File Access Manager Installation of Certificates and SSL

Version: 8.4

Revised: March 27, 2023

Copyright and Trademark Notices

Contents

Configuring File Access Manager to Use Local Certificates

File Access Manager uses a self-signed certificate for each of the services.

You can configure the system to use your own trusted certificates, using the procedure described in this chapter. To be trusted, server certificates must conform to the following guidelines:

- Certificates are signed by a Certificate Authority (CA), trusted by all servers in the organization, whether the CA is commercial or in-house.
- Certificates are issued to each server hosting one of the WCF hosting services (as described below).
- Certificates common name should be Fully Qualified Domain Name (FQDN) of the server.
- Certificate Subject Alternative Name (DNS) should be the short name (NetBios) of the server.
- The certificate must have the following extensions defined:
    - Key Usage: Digital Signature, Key Encipherment.
    - Enhanced Key Usage: Server Authentication, Client Authentication.

The certificate may have other key usages, but must have at minimum those mentioned above.

Changing Certificates for Elasticsearch

The Elasticsearch nodes in File Access Manager all use the same certificate as identification when other nodes or File Access Manager services communicate with them. The certificate is also used to encrypt communication between the nodes.

The Elasticsearch certificate is stored in a PKCS#12 file, which is a standard way of storing certificates and private keys. This is equivalent to the Windows Certificate Store. We will have to provide a certificate with its private key and the CA (Certificate Authority) certificate that signed it.

> Note: The commands below should be run in an elevated command line. If any of the paths contain spaces, surround them with quotation marks (").

High Level Steps

1. Choose an Elasticsearch node at random.
2. Delete the current certificate from the PKCS#12 file used by Elasticsearch.

3. Provide a certificate with a private key, import the new certificate's pfx/p12 file and change the certificate alias.
4. Provide the signing CA (Certificate Authority) certificate's .cer file and import it into Elasticsearch's PKCS#12 file to trust the certificate within Elasticsearch.
5. Restart the Elasticsearch service.
6. Copy the new PKCS#12 file to the other Elasticsearch nodes and restart them.
7. Insert the new PKCS#12 file into the File Access Manager database using the SailPoint FAMCertificateManager tool.

Detailed Steps

1. Choose one of the Elasticsearch nodes to perform the following steps on. It can be any of the currently installed nodes, no matter the order of installation.
2. Delete the current certificate from the PKCS#12 file used by Elasticsearch:

```
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\jdk\bin\keytool.exe" -delete -alias key -storepass "" -keystore
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12"
```

```
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\jdk\bin\keytool.exe" -delete -alias cert -storepass "" -
keystore "%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12"
```

3. Provide a new certificate with a private key, import the new certificate's pfx/p12 file and change the certificate alias:
    a. Provide a new certificate in a pfx/p12 format using your organization's standard method of obtaining server certificates. It should contain the certificate's private key.
    b. Use the following command to import the private key from the new pfx/p12 file into the one used by Elasticsearch:

```
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
```

```
8.2.2\jdk\bin\keytool.exe" -importkeystore -srckeystore <full
path to pfx/p12 file> -destkeystore
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12" -deststorepass
"" -srcstorepass <pfx/p12 file password>
```

c. The import process will generate a default alias for the private key, which is displayed in the last commands output. Set the private key's alias to "key" by running the following command:

```
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\jdk\bin\keytool.exe" -changealias -alias <default alias>
-destalias key -keystore
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12" -storepass ""
```

4. Provide the signing CA (Certificate Authority) certificate's .cer file and import it into Elasticsearch's PKCS#12 file to trust the certificate within Elasticsearch:

   a. Provide the signing CA (Certificate Authority) certificate's .cer file using your organization's standard method of obtaining CA certificates. It should not contain the private key, just the certificate itself.

   b. Import the certificate using the following command:

```
"%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\jdk\bin\keytool.exe" -importcert -file <full path to cer
file> -keystore "%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12" -storepass ""
-alias cert
```

5. Restart the Elasticsearch service.

6. Copy the new PKCS#12 file to the other Elasticsearch nodes and restart them as well.

   Make sure to copy the file to the same path as the first node, which according to the previous steps should be: %SAILPOINT_HOME%\Elasticsearch\elasticsearch-8.2.2\config\fileaccessmanager-elastic-cert.p12.

   > Note: This should also be done for the Elasticsearch nodes in Disaster Recovery as well.

7. Insert the new PKCS#12 file into the File Access Manager database, using the SailPoint FAMCertificateManager tool on just one of the nodes:

```
"%SAILPOINT_HOME%\FileAccessManager\Server
```

```
Installer\Tools\FAMCertificateManager\FAMCertificateManager.exe" 20 -
esCertFile="%SAILPOINT_HOME%\Elasticsearch\elasticsearch-
8.2.2\config\fileaccessmanager-elastic-cert.p12"
```

> Note: 20 is the ID of the first Elasticsearch node. Using the ID of any node will always assign this certificate to the other nodes as well.

Changing Certificates for RabbitMQ

To replace the RabbitMQ certificates with your own trusted certificates:

1. Provide the following certificate files and keys:
    a. The file containing the public key of the root Certificate Authorities that you wish to implicitly trust with the name: "*ca.cer*"
    b. The file containing the client's own certificate public key with the name: "*rabbitmq.cer*"
    c. The file containing the client's private key in PEM format: "*key.pem*"

    This can be done using OpenSSL. Examples commands below:

    openssl pkcs12 -in famcert.pfx -nokeys -out rabbitmq.cer

    openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
2. To configure the RabbitMQ certificate files:
    - Replace the files located under "%SAILPOINT_HOME%\RabbitMQ\certificates" with the certificates and key mentioned above.
    - Open the file %SAILPOINT_HOME%\RabbitMQ\data\rabbitmq.config with a text editor, and replace the current files path with the path of your own trusted certificates and key. Then save the file.
3. Delete the SailPoint RabbitMQ certificate from the certificate computer store. The certificate name is "File Access Manager RabbitMQ"
4. Restart the rabbitmq service, the Central Permission Collection Engine(s) and Collector(s) services and the Central Data Collection Engine(s) and Collector(s) services.

Changing the Certificates for Core Services

This process will replace the certificate for all the services except for Elasticsearch and RabbitMQ with your selected certificate.

All the SailPoint supplied certificates will be removed

To replace the certificates with your own:

1. Open an elevated command line

   ```
   "%SAILPOINT_HOME%\FileAccessManager\Server Installer-
   \Tools\FAMCertificateManager\FAMCertificateManager.exe" -a -existingCertificate
   ```

2. Select your certificate from the dropdown list.

3. Restart the services, or reboot the server.

> Note: You can change the certificate for a single service, using the SailPoint tool FAMCertificateManager.exe, using the service_id of that service.

Changing the Certificates for Collectors

Changing the certificates of the collectors (Activity Monitor, Permission Collector, Data Classification) using the *Collector Installation Manager* replaces the SailPoint self-signed certificates with your appointed certificate, and deletes the corresponding SailPoint certificate from the certificate store.

To replace the certificates for collectors using the Collector Installation Manager:

1. Run the Collector Installation Manager

   This will open a list of the collectors. You can update separate certificates per collector, or use the same certificate for all.

2. Click **Set Certificate for all Services**

   If this server does not have a server installer, you will have to update the watchdog certificate manually. See Installing Collectors on a Server Without Core Services .

3. Select your certificate from the dropdown list to update the certificate list.

4. Restart all the services, or simply reboot the server.

Installing Collectors on a Server Without Core Services

If you are installing collectors on a server without installing the server installer, the **Collector Installation Manager** will not replace the watchdog certificate. This must be done manually, as described below.

Verify that you have to perform this step

Check the certificate store (local computer store), after running the Collector Installation Manager. If there is a certificate called “File Access Manager WatchDog [servername],” the watchdog certificate has not been replaced.

1. Copy the thumbprint of your trusted certificate.
    a. Find the certificate you want to use. This should be in the certificate store (local computer store).
    b. Right click to read the certificate details, and copy the *thumbprint* value.
2. Update the thumbprint value in the watchdog configuration file.
    a. Locate the Watchdog configuration file

       %SAILPOINT_HOME%\%SAILPOINT_APP_NAME%\WBXWatchDogServiceHost.exe.config
    b. Open the configuration file with a text editor, and search for the “clientCertificateThumbprint.”
    c. Replace the value with the copied thumbprint from your trusted certificate in step 1.
    d. Save the file.
3. Restart the watchdog service.
4. Delete the SailPoint watchdog service certificate from the computer's personal certificate store.

File Access Manager Website SSL

The File Access Manager website is not affected by general SSL settings.

Setting the File Access Manager website to use SSL is not required, but is recommended.

To use SSL for Website communications, perform the following steps:

1. Install a certificate on the same server as the File Access Manager page (preferably with the same certificate criteria described above).
2. Open Internet Information Services Manager (inetmgr).
3. Navigate to the Default Web Site, and click “Bindings” on the panel to the right.
4. Click **Add**.
5. Select HTTPS on the Type dropdown menu.
6. Select **Select** on the SSL Certificate dropdown menu to use a trusted certificate, preferably one from your organization.
7. Click **OK**.
8. Click **Close**.
9. A manual update must be made in the DB to reflect the web site URL (check for fields with the URL in it for the SQL below):

```
update [whiteops].[system_configuration_value] set [value] = replace
([value],'http','https') where [name]='Web Site URL'
```

10. Set the "requireSSL" flag and SSL port in the configuration file.

    File: C:\inetpub\wwwroot\siqApi\SiqApi.dll.config

    <add key="requireSSL" value="true" />

    true

    require SSL

    false

    regular http protocol

    <add key="sslPort" value="443" />

ssl port

Change this value if you want to change the default

11. When securing cookies, ensure the following is in each web.config file for v1, v2, and siqapi.

    <httpCookies httpOnlyCookies="true" requireSSL="true" />”

    The web.config files are located at:

    V1 - "{website root folder} \identityiqfam\v1\web.config"

    V2 - "{website root folder}\identityiqfam\v2\web.config"

    SiqApi - "{website root folder} \siqApi\web.config"

    The default installation path for File Access Manager IIS application is “C:\inetpub\wwwroot”

To make browsing to the page using HTTPS mandatory, perform the following steps:

1. Double click on SSL Settings while on the Default Website.
2. Click **Require SSL**.
3. Leave “**Ignore**” on Client Certificates.
4. Click **Apply**.