
# DataFlux® Secure 2.5
## Administrator's Guide
### Second Edition

SAS® Documentation

This page is intentionally blank

# DataFlux® Secure 2.5

## Administrator's Guide

### Second Edition

Applies to:
DataFlux Authentication Server 4.1
DataFlux Data Management Server 2.5
DataFlux Data Management Studio 2.5
DataFlux Web Studio 2.5
DataFlux Web Studio Server 2.5
SAS Federation Server 4.1
SAS Federation Server Manager 4.1
SAS Federation Server Client 4.1
SAS Visual Process Orchestration 2.1 Runtime Server
SAS Visual Process Orchestration 2.1 Web Client

May 1, 2014

This page is intentionally blank

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2014. *DataFlux® Secure 2.5: Administrator's Guide, Second Edition*. Cary, NC: SAS Institute Inc.

**DataFlux® Secure 2.5: Administrator's Guide, Second Edition**



SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

May 2014

SAS provides a complete selection of books and electronic products to help customers use SAS® software to its fullest potential. For more information about our e-books, e-learning products, CDs, and hard-copy books, visit **support.sas.com/bookstore** or call 1-800-727-3228.

# Table of Contents

# Accessibility

The DataFlux Secure software includes features that improve usability for the disabled. These accessibility features are related to standards for electronic information technology that were adopted by the United States (U.S.) Government under Section 508 of the U.S. Rehabilitation Act of 1973, as amended.

If you have questions or concerns about the accessibility of SAS products, please send an e-mail to techsupport@sas.com.

# What's New in DataFlux Secure 2.5

The main enhancements for DataFlux Secure 2.5 include the addition of support for the following clients and servers:

- SAS Visual Process Orchestration Web Client
- SAS Visual Process Orchestration Runtime Server
- SAS Federation Server Manager

# Recommended Reading

DataFlux Authentication Server Administrator's Guide
DataFlux Data Management Server Administrator's Guide
DataFlux Data Management Studio Installation and Configuration Guide
DataFlux Data Management Studio User's Guide
DataFlux Web Studio Installation and Configuration Guide
DataFlux Web Studio Server User's Guide
SAS Drivers for Federation Server User's Guide
SAS Federation Server Administrator's Guide
SAS Federation Server Manager User's Guide
SAS Visual Process Orchestration Server Administrator's Guide
SAS Visual Process Orchestration User's Guide

For a complete list of SAS publications, go to support.sas.com/bookstore. If you have questions about which titles you need, please contact a SAS Publishing Sales Representative:
SAS Publishing Sales
SAS Campus Drive
Cary, NC 27513-2414
Telephone: 1-800-727-3228
Fax: 1-919-677-8166
E-mail: sasbook@sas.com
Web address: support.sas.com/bookstore

# Overview of DataFlux Secure



## Features and Scope

The DataFlux Secure software provides three high-assurance features:

- Enhanced encryption for network communication and passwords. Multiple encryption algorithms are supported, up to and including the 256-bit private keys of AES.
- The Secure Sockets Layer (SSL) to protect SOAP (HTTP) connections.
- FIPS compliance to help ensure that your site meets regulatory requirements.

DataFlux Secure is installed by default, in a disabled state, alongside each supported client or server. You can enable the security enhancements at any time.

In order to maintain interoperability, you need to install, enable, and similarly configure DataFlux Secure on all of the clients and servers that interact at your site.

DataFlux Secure provides the following security enhancements for the following clients and servers:

| Client or Server | Description | DataFlux Secure Implementation |
|---|---|---|
| DataFlux Authentication Server | Authenticates DataFlux Data Management Studiousers and services using native authentication providers. The server also maintains a database of users, groups, domains, logins, and shared logins. The database is queried by servers as part of their local authorization processes. | Uses configurable enhanced encryption to communicate with data management clients and servers. The server uses SSL to communicate with SSL-enabled authentication providers. You can enable FIPS compliance to help meet regulatory requirements. |
| DataFlux Data Management Studio | Enables the creation of jobs and services that run on the client and on DataFlux Data Management Server, SAS Federation Server, and Dataflux Web Studio Server. DataFlux Data Management Studio also provides the administrative interface for DataFlux Data | Uses AES encryption to communicate with the DataFlux Authentication Server. Uses SSL to communicate with SSL-enabled DataFlux Data Management Server and Dataflux Web Studio Server. |

| Client or Server | Description | DataFlux Secure Implementation |
|---|---|---|
| | Management Server and DataFlux Authentication Server. | |
| DataFlux Data Management Server | Runs jobs and services created in DataFlux Data Management Studio, stores job output and data collections, and implements access controls for data, jobs, and services. It can authenticate and use group membership data from the DataFlux Authentication Server. Server connections can be disabled by IP address. Clients access the server using a SOAP interface. | Uses enhanced configurable encryption to protect passwords and to communicate with similarly configured SAS servers (using SAS/SECURE), SAS Federation Server, and DataFlux Authentication Server. The DataFlux Data Management Server can use SSL to communicate with SSL-enabled Dataflux Web Studio Server, the DataFlux Web Studio client, and your SSL-enabled SOAP clients. When SSL is enabled, the DataFlux Data Management Server accepts only those connections that use HTTPS addresses. |
| DataFlux Web Studio | Provides a user interface for data management tasks that transparently execute jobs on Dataflux Web Studio Server and DataFlux Data Management Server. Connects to the DataFlux Authentication Server for user authentication and group memberships. | Uses configurable enhanced encryption. Uses SSL to communicate with SSL-enabled Dataflux Web Studio Server ad DataFlux Data Management Server. |
| Dataflux Web Studio Server | Runs jobs and services created in DataFlux Web Studioand DataFlux Data Management Studio, stores job output and data collections, and implements access controls for local data, jobs, and services. Connects to the DataFlux Authentication Server for user validation and group memberships. | Uses configurable enhanced encryption to communicate with similarly configured clients and servers. The Dataflux Web Studio Server can use SSL to communicate with SSL-enabled DataFlux Data Management Server, DataFlux Data Management Studio, and your SSL-enabled SOAP clients. |
| SAS Federation Server | Runs jobs that collect data from multiple enterprise sources. Provides centralized access to collected data. Manages access to jobs and data collections using users and groups defined | Uses configurable enhanced encryption and can use FIPS compliance to support similarly configured clients and servers. |

| Client or Server | Description | DataFlux Secure Implementation |
|---|---|---|
| | on the DataFlux Authentication ServerAuthentication Server. | |
| SAS Federation Server Manager | Provides a web interface that administers data sources and access controls on SAS Federation Server. | Uses configurable enhanced encryption as needed to communicate with similarly configured SAS Federation Server and DataFlux Authentication Server. Uses SSL |
| SAS Federation Server Client | This package provides the SAS drivers for Federation Server, which enable your applications to connect to data sources on SAS Federation Server. Also, this package can be used to install the ASBATCH utility, which is used for batch updates of the DataFlux Authentication Server database. | These client components use configurable enhanced encryption and FIPS compliance as needed to communicate with similarly configured SAS Federation Server and DataFlux Authentication Server. |
| SAS Visual Process Orchestration Runtime Server | The Runtime Server executes orchestration jobs, which in turn execute jobs, real-time services, SAS programs, scripts, and other programs on servers across your enterprise. | The Runtime Server uses configurable enhanced encryption and can use SSL. When SSL is enabled, the Runtime Server accepts only those connections that use HTTPS addresses. Encryption can be configured to match the algorithm used by your other SAS servers. |
| SAS Visual Process Orchestration Web Client | The web client provides an environment for the creation and testing of orchestration jobs. | Uses configurable enhanced encryption and can use SSL to communicate with an SSL-enabled Runtime Server. Encryption can be SAS servers running SAS/SECURE. |

DataFlux Secure does not provide a graphical user interface or run any daemon processes.

## AES

When enabled, advanced encryption requires the use of AES (Advanced Encryption Standard) algorithms. AES encryption and decryption protects the following:

- All passwords that are stored on disk. For information about passwords, see About Password Protection.

- All interprocess communication between components that use the Integrated Object Model (IOM).
- All SSL communication between clients and servers.

AES is separately enabled, so you can choose to retain the default encryption algorithm and use DataFlux Secure for SSL only. The default encryption algorithm is SASPROPRIETARY, which uses 56-bit keys. Other encryption algorithms can be configured to match a SAS/SECURE implementation on your SAS servers.

Administrators manually encrypt passwords using AES to replace SASPROPRIETARY passwords using a password encryption tool.

## SSL

Support for Secure Sockets Layer (SSL) uses private-key encryption and signed digital certificates to protect HTTPS connections. DataFlux Secure uses SSL to protect the following connections:

- DataFlux Authentication Server connections to SSL-configured authentication providers such as Active Directory or LDAP.
- All client connections to the DataFlux Data Management Server, including connections from your own clients.
- DataFlux Data Management Studio connections to SSL-enabled DataFlux Data Management Server and DataFlux Authentication Server.
- DataFlux Web StudioWeb Studio connections to SSL-enabled DataFlux Authentication Server and DataFlux Data Management Server.
- SAS Visual Process Orchestration Runtime Serverconnections to SSL-enabled SAS Visual Process Orchestration Web Clients and DataFlux Data Management Server.
- SAS Federation Server Manager connections to SSL-enabled DataFlux Authentication Server.

## FIPS

FIPS compliance enables you to run your SAS Federation Server and DataFlux Authentication Server in compliance with FIPS 140–2. This Federal Information Processing Standard helps your company meet the security requirements of certain businesses and governmental entities.

FIPS compliance is also implemented in the Secure versions of the SAS Federation Server Manager and the SAS Federation Server Client. In the client package, the SAS drivers for Federation Server and the ASBATCH utility are all FIPS-compliant.

FIPS compliance prevents servers from connecting directly with clients that are not FIPS-compliant. If your DataFlux Authentication Server and SAS Federation Server are enabled for FIPS compliance, then your instances of DataFlux Data Management Studio and DataFlux Data Management Server need to connect to those servers with the SAS drivers for Federation Server.

For further information about FIPS 140-2, refer to the document Security Requirements for Cryptographic Modules.

### About Password Protection

The supported clients and servers store a minimum number of passwords, and all passwords are encrypted for storage on disk.

Passwords are limited in number because user passwords are not stored on the supported clients and servers. Instead, user credentials are delivered to your existing authentication providers for validation. Only stored login passwords are stored, in encrypted form, on the DataFlux Authentication Server.

Shared logins are collections of users that share credentials for a given enterprise database. For example, if a DataFlux Web Studio user wants to run a job that collects data from an Oracle database, she authenticates initially, and then she submits inbound credentials for a shared login to the DataFlux Authentication Server. If she is a consumer of that shared login, then the DataFlux Authentication Server provides database credentials that allow the job to connect to the database.

The passwords for shared logins, along with the outbound credentials for databases, are stored only on the host of the DataFlux Authentication Server, and always with AES encryption.

The only other stored passwords are thosese that are used to open connections between servers. One such connection is used to connect a server to the DataFlux Authentication Server for authentication or to obtain group membership information. Jobs running on the DataFlux Data Management Server can also open connections to the SAS Federation Server.

Passwords are not displayed in any graphical user interface.

# AES: How It Works

When you enable AES in DataFlux Secure, the client or server encrypts and decrypts using AES algorithms. Supported AES algorithms use private keys of 128, 192, or 256 bits.

When AES is not configured, the default algorithm is SASPROPRIETARY, which supports private keys of 56 bits.

When you install DataFlux Secure, and when you enable AES encryption, you encrypt the transmission of all logins . You also encrypt all network traffic that uses the SAS Integrated Object Model (IOM, an extension of TCP/IP.)

For HTTP servers that do not use IOM, AES encryption is implemented by SSL.

The process of encryption for network transmission takes place as follows in this typical example. When you connect to a SAS Federation Server from DataFlux Data Management Studio, the login that you submit is encrypted before it is transmitted. The SAS Federation Server then sends the encrypted login to the DataFlux Authentication Server for authentication.

# SSL: How It Works

When the Secure Sockets Layer is enabled on a DataFlux Authentication Server, it protects connections between the DataFlux Authentication Server and any SSL-enabled authentication providers (LDAP or Active Directory.) The DataFlux Authentication Server acts as an SSL client only.

When SSL is enabled on an HTTP server (DataFlux Data Management Server, Dataflux Web Studio Server, or SAS Visual Process Orchestration Runtime Server), SSL is the sole means of connecting with these servers.

SSL clients include DataFlux Data Management Studio, DataFlux Web Studio, SAS Visual Process Orchestration Web Client, SAS Federation Server Manager, SAS Drivers for Federation Server, and your SOAP clients.

To access a DataFlux Data Management Server using SSL, a SOAP client sends an HTTPS request to the server. The client can request a certificate from the server, which it compares to the certificate that the client stores locally. The client verifies the identity of the server and negotiates with the server to select a cipher (encryption method). The cipher that is selected is the first match between the ciphers that are supported on both the client and the server. All subsequent data transfers for the current request are then be encrypted using the selected encryption method.

# Install and Configure



## Installation Notes

For the 2.4.1 release and later, DataFlux Secure is installed and licensed by default when you install a client or server that supports DataFlux Secure.

DataFlux Secure is installed in a disabled state. You can enable the security enhancements that are provided by DataFlux Secure at any time.

DataFlux Secure is installed in the same default directory as the related client or server.

The system requirements for DataFlux Secure are the same as those of the clients and servers that use DataFlux Secure, as provided on the SAS System Requirements page.

In this document, the default installation path is indicated by the term *install-path*.

# About Configuration

DataFlux Secure provides configurable enhanced encryption, SSL connection protection, and FIPS compliance. These features require different levels of configuration after installation.

Configure encryption similarly on all instances of DataFlux Secure. First execute the command that enables encryption. Then replace all of your stored passwords with passwords that have been encrypted with the selected encryption algorithm.

When you configure SSL with DataFlux Secure, it is recommended that you enable SSL on all supported clients and servers. Most of the supported clients and servers requires you to install OpenSSL.

Configure FIPS compliance on the SAS Federation Servers and DataFlux Authentication Server by entering a command that enables the feature.

Clients that access FIPS-enabled servers need to connect with DataFlux device drivers, rather than SOAP or HTTP addresses. To learn about client-side drivers for the SAS Federation Server, see *SAS Drivers for Federation Server*.

# Configure OpenSSL



## OpenSSL System Requirements

OpenSSL is an open-source software package that enables HTTPS connections. OpenSSL is required on all of the hosts that run DataFlux Secure.

For all DataFlux Secure hosts, the system requirement for OpenSSL is 0.9.8.

On Windows hosts, deploy a supported version of OpenSSL from the provider of your choice.

On UNIX and Linux hosts, OpenSSL is delivered as part of the operating environment. Those libraries should be included in LD_LIBRARY_PATH.

To run DataFlux Secure on a Solaris 11 host, replace OpenSSL 1.0 with OpenSSL 0.9.8. Install OpenSSL 0.9.8 in /usr/sfw/lib.

After you deploy OpenSSL, request and add certificates from a Certificate Authority. Then enable SSL for DataFlux Secure, as described in this chapter.

## Download and Deploy OpenSSL onto Windows Hosts

Follow these steps to download and deploy OpenSSL onto all of the Windows hosts that will use SSL:

1. On your first Windows host, download OpenSSL v0.9.7 or later from a provider such as Shining Light Productions. Do not download a Light version.

   For servers that run on 64-bit hosts, be sure to download a 64-bit version of OpenSSL. If you install the 32-bit Data Management Studio on a 64-bit host, be sure to install the 32-bit OpenSSL. The 32-bit and 64-bit versions of Open SSL can reside on the same host without conflict. The 64-bit host can use the 64-bit version of OpenSSL for other purposes.

2. Also download the appropriate instance of the Visual C++ 2008 Redistributables.

3. Execute the following command to include the redistributables:

   `vcredist_x64.exe` or `vcredist_x32.exe`

4. Install OpenSLL by executing:

   `Win`*bit-length*`OpenSSL`*version-number*`.exe`
   For example:

   `Win64OpenSSL-1_0_1c.exe`

5. Install OpenSSL to `C:\OpenSSL-Win64` or `C:\OpenSSL-Win32`.

6. Select the installer option **Copy OpenSSL DLLs to the Windows System Directory**.

7. If you are installing OpenSSL on a client, the installation process is complete. Move on to Create a Trusted Certificate.

8. If you are installing OpenSSL on a server, either reboot the server or enter the following command before you create a certificate:

   ```
   set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg
   ```

   or:

   ```
   set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
   ```

9. To deploy OpenSSL to other applicable hosts, copy and paste the OpenSSL DLLs into the respective system directories, and restart the servers.

## Create SSL Certificates

When a client requests an SSL connection, the server delivers a certificate, which contains a key. The client uses the server's certificate to verify the identity of the server. Certificates can be trusted or self-signed. Trusted certificates are provided by

a Certificate Authority. Self-signed certificates are created with an OpenSSL command.

## Create a Trusted Certificate

Trusted certificates generally provide increased assurance in comparison to self-signed certificates. To create a trusted certificate on a host with OpenSSL, simply purchase the certificate from a certificate authority such as VeriSign and install the certificate as directed.

## Create a Self-Signed Certificate on Windows

Follow these steps to create a self-signed certificate on a Windows host that includes OpenSSL:

1. In the Run dialog dox or on a DOS command line, change to the OpenSSL directory:

   ```
   cd /d c:\openssl-win32
   ```
   or
   ```
   cd /d c:\openssl-win64
   ```

2. Create a directory named `certificates`:

   ```
   md certificates
   ```

3. Change to the `bin` directory:

   ```
   cd bin
   ```

4. Enter the command that creates the key file and the certificate file, and inserts the key file into the certificate:

   ```
   openssl req -x509 -nodes -days 1095 -newkey rsa:1024
    -keyout ..\certificates\%COMPUTERNAME%.pem
    -out ..\certificates\%COMPUTERNAME%.pem
   ```

   This command creates a certificate that remains valid for three years. Windows will supply a value for `%COMPUTERNAME%`.

5. The command above presents you with a number of prompts. The only significant prompt asks you for the host's common name. The common name is required to be a fully-qualified domain name, such as w64213.us.ourco.com.

## Create a Self-Signed Certificate on UNIX or Linux

1. Create a directory named certificates:

   ```
   mkdir /home/yourUserid/certificates
   ```

2. Change to the certificates directory:

   ```
   cd /home/yourUserid/certificates
   ```

3. Enter the command that creates the key file and the certificate file, and inserts the key file into the certificate:

   ```
   openssl req -x509 -nodes -days 1095 -newkey rsa:1024
   -keyout computerName.pem -out computerName.pem
   ```

4. The command above presents you with a number of prompts. The only significant prompt asks you for the host's common name. The common name is required to be a fully-qualified domain name, such as w64213.us.ourco.com.

# Configure DataFlux Authentication Server

## Enable AES and FIPS on Windows

To enable DataFlux Secure for DataFlux Authentication Server, select one shortcut to enable AES encryption and another shortcut to enable AES encryption and compliance with FIPS 140-2.

With the server stopped, double-click the following shortcut to enable AES encryption **with** FIPS compliance:

```
install-path/Set Security - FIPS
```

**Note:** Enabling compliance with FIPS 140-2 requires that DataFlux Data Management Studio, DataFlux Data Management Server, and DataFlux Web Studio use the SAS drivers for the SAS Federation Server to communicate with the DataFlux Authentication Server.

**Note:** Enabling AES encryption for the DataFlux Authentication Server also enables AES encryption on all associated instances of Federation Server, Data Management Server, and Data Management Studio.

To enable AES encryption **without** enabling FIPS compliance, double-click the following shortcut:

```
install-path/Set Security - AES
```

If, in the future, you need to disable FIPS compliance and AES encryption, and implement the default 56-bit SASPROPRIETARY encryption algorithm, double-click the following shortcut:

```
install-path/Set Security - SAS
```

## Enable AES and FIPS on UNIX or Linux

Execute the set_secure command to enable AES encryption. You can also enable compliance with FIPS 140-2.

With the server stopped, enter the following command to enable AES encryption **with** FIPS compliance:

```
install-path/bin/set_secure fips
```

**Note:** Enabling compliance with FIPS 140-2 requires that DataFlux Data Management Studio, DataFlux Data Management Server, and DataFlux Web Studio use the SAS drivers for the SAS Federation Server to communicate with the DataFlux Authentication Server.

**Note:** Enabling AES encryption for the DataFlux Authentication Server requires that you also enable AES encryption on all associated instances of SAS Federation Server, DataFlux Data Management Server, and DataFlux Data Management Studio.

To enable AES encryption **without** enabling FIPS compliance, enter the following command:

```
install-path/bin/set_secure aes
```

If, in the future, you need to disable FIPS compliance and AES encryption, and implement the default 56-bit SASPROPRIETARY encryption algorithm, enter the following command:

```
install-path/bin/set_secure sas
```

# Configure SSL

## Common Steps for All Operating Environments

Follow these steps to configure SSL on an DataFlux Authentication Server in the Windows, UNIX, or Linux operating environment:

1. Stop the DataFlux Authentication Server.
2. Open the configuration file as_serv_aspsql.xml.
3. To enable SSL communication with an LDAP authentication provider, add the following option to the SetEnv option set:
```
<OptionSet name="SetEnv">
   <Option name="LDAP_TLSMODE">1</Option>
</OptionSet>
```
4. To enable SSL communication with an Active Directory authentication provider, add the following option:
```
<OptionSet name="SetEnv">
   <Option name="AD_TLSMODE">1</Option>
</OptionSet>
```
5. In the configuration file, invoke client authentication by adding the following option, or by adding the following value if the option already exists:
```
<Option name="SSLCLIENTAUTH">1</Option>
```

If your DataFlux Authentication Server is installed on Windows, then continue to the next topic. Otherwise, go to Configure SSL on UNIX or Linux.

## Configure SSL on Windows

If your DataFlux Authentication Server is installed on Windows, and if your SSL implementation calls for the exchange of digital certificates, then follow these steps to complete the SSL configuration process. If your SSL configuration does not exchange digital certificates, then save and close the configuration file and restart the DataFlux Authentication Server.

If your SSL configuration does call for the exchange of digital certificates, then add only the options that apply to your site. For example, if your site does not check for revoked digital certificates, then you do not need to add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, add the following option or value to identify the issuer of the digital certificate:
   ```
   <Option name="SLLCERTISS">issuer-name</Option>
   ```
   The SSLCERTISS option is used with the SSLCERTSERIAL option to uniquely identify a digital certificate from the Microsoft Certificate Store.
2. Set the following option to specify the serial number of the digital certificate:
   ```
   <Option name="SSLCERTSERIAL">serial-number</Option>
   ```
3. If your SSL configuration checks a Certificate Revocation List (CRL) when a digital certificate is validated, then specify the following options:
   ```
   <Option name="SSLCRLCHECK">1</Option>
   <Option name="SSLCRLLOC">path-to-CRL-file</Option>
   ```
   A CRL is published by a Certificate Authority (CA). Each CRL contains only the revoked digital certificates that were issued by that particular CA.
4. Save and close the configuration file.
5. Start the DataFlux Authentication Server.

## Configure SSL on UNIX or Linux

If your DataFlux Authentication Server is installed on UNIX or Linux, then follow these steps to complete the SSL configuration process.

All of the following steps apply to the exchange of digital certificates. If your SSL configuration does not include the exchange digital certificates, then skip these steps, save and close the configuration file, and restart your DataFlux Authentication Server.

If your SSL configuration does call for the exchange of digital certificates, then add only the options that apply to your site. For example, if your site does not check for revoked digital certificates, then you do not need to add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, add the following option or value to specify the file that lists your trusted certificate authorities:
   ```
   <Option name="SSLCALISTLOC">file-path</Option>
   ```

The list in the file must be PEM-encoded (base64).

2. If your site checks a Certificate Revocation List (CRL) when a digital certificate is validated, then specify the following required options:

```
<Option name="SSLCRLCHECK">1</Option>
<Option name="SSLCRLLOC">path-to-CRL-file</Option>
```

   A CRL is published by a Certificate Authority (CA). Each CRL contains only the revoked digital certificates that were issued by that particular CA.

3. If your site exchanges digital certificates in the SSL validation process, then specify the protocol that is used at your site:

```
<Option name="SSLREQCERT">ALLOW|DEMAND|NEVER|TRY</Option>
```

   ALLOW
   The DataFlux Authentication Server asks for a certificate. If a certificate is not provided, then the session proceeds. If a certificate is provided and if it fails to validate, then the session proceeds.

   DEMAND
   The DataFlux Authentication Server asks for a certificate. If the certificate fails to validate, then the session is immediately terminated.

   NEVER
   The DataFlux Authentication Server does not ask for a certificate.

   TRY
   The DataFlux Authentication Server asks for a certificate. If a certificate is not provided, then the session proceeds. If a certificate is provided, and if the certificate fails to validate, then the session is immediately terminated.

   If you do not add the SSLREQCERT option to your configuration file, then the default value is DEMAND.

   If you specify SSLREQCERT and LDAP_SSLREQCERT, then the value of SSLREQCERT applies to all of your authentication providers except your LDAP authentication provider.

4. If your DataFlux Authentication Server uses an LDAP authentication provider, and if your site exchanges digital certificates, then specify a separate validation protocol for LDAP authentication provider:

```
<Option name="LDAP_SSLREQCERT">ALLOW|DEMAND|NEVER|TRY</Option>
```

   If you specify LDAP_SSLREQCERT and SSLREQCERT, then SSLREQCERT applies to all authentication providers other than LDAP. LDAP_SSLREQCERT applies to the LDAP provider only.

5. To enable or disable a subject name check in your SSL validation process, specify the SSLNameCheck option. The name check ensures that the subject name in the authentication provider's certificate matches the subject name that is expected by the DataFlux Authentication Server. The subject name that is expected is specified by the option LDAP_HOST or AD_HOST.

```
<Option name="SSLNameCheck">1</Option>
```

The SSLNameCheck option does not apply to your LDAP authentication provider if you also specify the option LDAP_SSLNameCheck.

The default value of SSLNameCheck is False (0) if SSLReqCert is set to NEVER or ALLOW, otherwise the default is True (1).

To disable subject name checks, specify a value of 0 (zero or FALSE for this binary option):

```
<Option name="SSLNameCheck">0</Option>
```

6. To separately enable or disable a subject name check for your LDAP authentication provider, add the option LDAP_SSLNameCheck:

   ```
   <Option name="LDAP_SSLNameCheck">1</Option>
   ```

   or

   ```
   <Option name="LDAP_SSLNameCheck">0</Option>
   ```

   The LDAP_SSLNameCheck option applies only to your LDAP authentication provider. All other subject name checks are governed by the option SSLNameCheck.

   The default value of LDAP_SSLNameCheck is False (0) if LDAP_SSLReqCert is set to NEVER or ALLOW, otherwise the default is True (1).

7. If your site *does not* use a PKCS #12 DER encoding package to store the DataFlux Authentication Server's certificate and private key, then specify the location of the DataFlux Authentication Server's certificate, private key, and password:

   ```
   <Option name="SSLCERTLOC">path-to-certificate-file</Option>
   <Option name="SSLPVTKEYLOC">path-to-the-certificate's-private-key-
   file</Option>
   <Option name="SSLPVTKEYPASS">encrypted-password-to-key-file</Option>
   ```

   The certificate and private key must be PEM-encoded (base64).

8. If your site does use a PKCS #12 DER encoding package file to store the DataFlux Authentication Server's certificate and private key, then specify the location of the package file and the decryption password for that package file:

   ```
   <Option name="SSLPKCS12LOC">path-to-certificate-file</Option>
   <Option name="SSLPKCS12PASS">encrypted-pwd-for-encoded-package-
   file</Option>
   ```

   If you specify SSLPKCS12LOC, then the SSLCERTLOC and SSLPVTKEYLOC options are ignored.

9. Save and close the configuration file.

10. In the operating environment, append the OpenSSL library path to include the path to the LD_LIBRARY_PATH environment variable.

11. Start the DataFlux Authentication Server.

The following example depicts typical SSL configuration options for an LDAP authentication provider:

```
<OptionSet name="SetEnv">
   <Option name="LDAP_HOST">sample1.sample.com</Option>
   <Option name="LDAP_PORT">636</Option>
   <Option name="LDAP_BASE">CN=Users,DC=SAMPLE,DC=com</Option>
   <Option name="LDAP_IDATTR">sample-account-name</Option>
            <Option name="LDAP_PRIV_DN">Administrator@sample.com</Option>
              <Option name="LDAP_PRIV_PW">DataFlux01</Option>
   <Option name="LDAP_TLSMODE">1</Option>
</OptionSet>
<Option name="SSLCALISTLOC">/home/certs/sample.pem </Option>
<Option name="AuthProviderDomain">LDAP:mydomain</Option>
<Option name="PrimaryProviderDomain">mydomain</Option>
```

The following example depicts typical SSL configuration options for an Active Directory authentication provider:

```
<OptionSet name="SetEnv">
         <Option name="AD_HOST">sample01.plt.rdc.sample.com</Option>
   <Option name="AD_PORT">636</Option>
   <Option name="AD_TLSMODE">1</Option>
 </OptionSet>
 <Option name="SSLCALISTLOC">/home/certs/sample.pem</Option>
 <Option name="AuthProviderDomain">ADIR:mydomain</Option>
<Option name="PrimaryProviderDomain">mydomain</Option>
```

# Configure DataFlux Data Management Studio

The DataFlux Secure software is installed in a disabled state on all instances of DataFlux Data Management Studio. The only time that DataFlux Secure is not installed by default is when export restrictions prevent the distribution of security software.

DataFlux Data Management Studio requires the use of SSL when that client communicates with an SSL-enabled DataFlux Data Management Server or DataFlux Web Studio Server. To configure SSL on a client host, install 32-bit OpenSSL. Note that you should install 32-bit OpenSLL even when the 32-bit client is installed on a 64-bit host. The 32-bit and 64-bit versions of OpenSSL can reside on the same host without conflict.

When you install DataFlux Data Management Studio, the SSL DLL is disabled unless the installation process finds OpenSSL in the system path. If you install OpenSSL after you install DataFlux Data Management Studio, then you need to enable the SSL DLL. Log in as an administrator and enter the following command:

```
bin\set_soap ssl
```

The SSL DLL remains enabled until you enter the following command:

```
bin\set_soap std
```

If you enable the SSL DLL, and if you do not install OpenSSL, then DataFlux Data Management Studio will not start. Use the Windows Task Manager to kill the process DMStudio.exe.

When DataFlux Data Management Studio needs to connect to a SAS Federation Server or DataFlux Authentication Server that is enabled for FIPS compliance, you need to configure DataFlux Data Management Studio to communicate using the DataFlux drivers for ODBC or JDBC, rather than using a direct connection. For more information about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

The configuration files for DataFlux Data Management Studio are not affected by the installation of DataFlux Secure.


Note: In DataFlux Data Management Studio, when you define an SSL-enabled DataFlux Web Studio Server or DataFlux Data Management Server (in the Management Server window), make sure that the **Server** field contains an HTTPS address, such as https://yourDMServer.yourcompany.com.

# Configure DataFlux Data Management Server

## Overview

When configured with DataFlux Secure, the DataFlux Data Management Server uses configurable enhanced encryption as needed to increase security for proprietary interprocess communication.

To communicate with a SAS Metadata Server, the DataFlux Data Management Server needs to be configured to use the same encryption algorithm as the SAS Metadata Server.

To add security to connections with SOAP clients, the DataFlux Data Management Server can be configured to use SSL. When configured with SSL, the DataFlux Data Management Server uses SSL exclusively. Non-SSL communication is rejected.

## Configure Access to FIPS-Compliant Servers

SAS Federation Servers and DataFlux Authentication Servers with DataFlux Secure can be enabled for compliance with FIPS 140-2. If your DataFlux Data Management Server needs to connect to a FIPS-enabled server, then the DataFlux Data Management Server needs to connect with a DataFlux driver, either ODBC or JDBC. For more information about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

## Configure SSL

Follow these steps to configure SSL on your DataFlux Data Management Server:

1. If the DataFlux Data Management Server is running, then stop the server.
2. Open the configuration file dmserver.cfg.
3. Add the following options to enable DataFlux Secure and SSL:

```
DMSERVER/SECURE = YES
DMSERVER/SOAP/SSL = YES
```

Enter a value of NO to disable SSL on the DataFlux Data Management Server.

4. Add the following options to identify your administrative group and identify your DataFlux Authentication Server:

```
DMSERVER/SECURE/GRP_ADMIN = your-group-name
DMSERVER/AUTH_SERVER_LOC = fully-qualified-path:port-number
```

5. To identify a key file and password, add these two options:

```
DMSERVER/SOAP/SSL/KEY_FILE = path-to-key-file
DMSERVER/SOAP/SSL/KEY_PASSWD = encrypted-password-for-key-file
```

To encrypt a password, see Encrypt Passwords.

6. To identify trusted certificates (if you use certificates):

```
DMSERVER/SOAP/SSL/CA_CERT_FILE = trusted-certificates-filename
DMSERVER/SOAP/SSL/CA_CERT_PATH = path-to-trusted-certificates-file
```

7. Save and close the configuration file.
8. Start the DataFlux Data Management Server.

# Configure SAS Federation Server

## Enable AES and FIPS on Windows

After you install a SAS Federation Server with DataFlux Secure, select one shortcut to enable encryption and another shortcut to enable encryption and compliance with FIPS 140-2.

With the server stopped, double-click the following shortcut to enable AES encryption **with** FIPS compliance:

```
install-path/Set Security - FIPS
```

**Note:** Enabling compliance with FIPS 140-2 requires that DataFlux Data Management Studio, DataFlux Data Management Server, and DataFlux Web Studio use the SAS drivers for Federation Server to communicate with the SAS Federation Server.

**Note:** Enabling AES encryption on a SAS Federation Server requires that you also enable AES encryption on all associated instances of DataFlux Authentication Server, DataFlux Data Management Server, and DataFlux Data Management Studio.

To enable AES encryption **without** enabling FIPS compliance, double-click the following shortcut:

```
install-path/Set Security - AES
```

If, in the future, you need to disable FIPS compliance and AES encryption, and implement the default 56-bit SASPROPRIETARY encryption algorithm, double-click the following shortcut:

```
install-path/Set Security - SAS
```

## Enable AES and FIPS on UNIX or Linux

After you install a SAS Federation Server with DataFlux Secure, execute the set_secure command to enable AES encryption. You can also enable compliance with FIPS 140-2.

With the server stopped, enter the following command to enable AES encryption **with** FIPS compliance:

```
install-path/bin/set_secure fips
```

**Note:** Enabling compliance with FIPS 140-2 requires that DataFlux Data Management Studio, DataFlux Data Management Server, and DataFlux Web Studio use the SAS drivers for Federation Server to communicate with the SAS Federation Server.

**Note:** Enabling AES encryption on a SAS Federation Server requires that you also enable AES encryption on all associated instances of DataFlux Authentication Server, DataFlux Data Management Server, and DataFlux Data Management Studio.

To enable AES encryption **without** enabling FIPS compliance, enter the following command:

```
install-path/bin/set_secure aes
```

If, in the future, you need to disable FIPS compliance and AES encryption, and implement the default 56-bit SASPROPRIETARY encryption algorithm, enter the following command:

```
install-path/bin/set_secure sas
```

# Configure SAS Federation Server Manager

The SAS Federation Server Manager implements advanced encryption and SSL using DataFlux Secure.

Advanced encryption is manually enabled, with or without the implementation of SSL.

The SAS Federation Server Manager is built on the Jetty HTTP server. Because SSL is installed with the Jetty server, there is no need to install OpenSSL on the host of the SAS Federation Server Manager.

# Configure SSL

## Overview

The SAS Federation Server Manager implements SSL using a *Java keystore* (JKS) to contain a *keystore entry*. The keystore entry contains a public key, a private key, and a certificate.

The certificate in the keystore entry can be signed or self-signed. A self-signed certificate is generated locally. It can be useful for testing purposes. A signed certificate is provided by a Certificate Authority. A signed certificate provides the trustworthiness and authentication that is required in SSL applications.

The SSL configuration process using the SAS keyconfig utility follows these steps:

1. Create a keystore, a keystore entry, and a self-signed certificate.
2. Request and import a signed certificate that replaces the self-signed certificate.
3. Update the configuration file fsmanager.cfg.
4. Restart the SAS Federation Server to enable SSL.

If you prefer, you can use the Java keytool utility or your own certificate management tool instead of the keyconfig utility. If you use a tool other than keyconfig, make sure that your keystore meets the following requirements:

- The keystore file must be in JKS format.
- The alias for the keystore entry must be `jetty`.
- The password must be the same for the keystore, the keystore entry, and the configuration option key_store_password (see Update the Configuration File.)

## Create a Keystore

Use the keyconfig utility to create a keystore with a self-signed certificate. The keyconfig utility is available in the bin directory of the SAS Federation Server Manager, as shown in the following examples:

```
 C:\Program
Files\SASHome\SASFederationServerManager\release\bin\keyconfig
 C:\Program Files\DataFlux\FSManager\app-instance\bin\keyconfig
 /opt/dataflux/fsmanager/bin/keyconfig
```

 Note: Refer to the example paths above when this section refers to the installation directory of the SAS Federation Server Manager.

Enter the following command to create a keystore, a keystore entry, and a self-signed certificate:

```
keyconfig create -ks "path\filename.keystore"
```

In the preceding command, the *path* can be absolute or relative. The following example uses a relative path:

```
keyconfig create -ks "..\keystore\fsmanager.keystore"
```

When the keyconfig utility prompts you to enter passwords for the keystore and for the keystore entry, be sure to enter the same password in both places. This same password is also used as the value of the configuration option key_store_password.

## Request and Import a Certificate

Use the keyconfig utility to generate a request for a signed certificate. Then package the request and send it to a Certificate Authority.

To generate the certificate request, enter the following command:

```
keyconfig request -ks keystore -file csr_file
```

In the preceding command, the *keystore* value specifies the path to the keystore that you created with the `keyconfig create` command. The *csr_file* value represents the path and name of the certificate request file.

Send the certificate request file to your Certificate Authority to receive a signed certificate.

When you receive your certification file from the Certificate Authority, use the following command to import the signed certificate into your keystore:

```
keyconfig import -ks keystore -cert certfile
```

In the preceding command, the *keystore* value specifies the path and name of the keystore that you originally generated with the `keyconfig create` command. The *certfile* value specifies the path and name of the certification file that you received from the Certificate Authority.

When the certificate has been imported into the keystore, you are ready to update the SAS Federation Server Manager configuration file.

## Update the Configuration File

Edit the configuration file fsmanager.cfg to specify the following option values. The file fsmanager.cfg is located in the etc directory of the SAS Federation Server Manager, as shown in the following examples:

```
 C:\Program Files\SASHome\SASFederationServerManager\release-number\etc
C:\Program Files\DataFlux\FSManager\app-instance\etc
/opt/dataflux/fsmanager/etc
```

The following example configuration file is provided at the following location:

```
FSManagerInstallPath\etc\fsmanager.ssl-example.cfg
```

Enter the following values into the configuration file:

**ssl_enabled = true**

Enables SSL on the SAS Federation Server Manager.

**ssl_port = 21077**

Specifies the port on which the SAS Federation Server Manager listens for SSL requests. The default port number 21077 is recommended. You can use a different number if the default number is in use.

**key_store_path = *full-path-and-filename***

Specifies an alternate storage location for the keystore. When this option is not specified, the default storage location is as follows:

```
FSManagerInstallPath/etc/jetty.keystore
```

Example:

```
C:\Program Files\SASHome\SASFederationServerManager\
      4.1\etc\jetty.keystore
```

Be sure to specify the full path and filename of your alternate storage location.

**key_store_password = *password***

Specifies the password that is used to extract the SSL certificate from the keystore. SAS recommends that you encrypt the password before you enter it into the configuration file. To encrypt the password, enter the following command:

```
FSManagerInstallPath\bin\pwutil clear-text-password
```

The pwutil command produces several encrypted values. Use the OBF value as the value of the configuration option, as shown in the following example:

```
key_store_password = OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4
```

Make sure that the value of key_store_password is the same password that is used in the signed certificate that you obtain from a Certificate Authority.

Save and close the configuration file. You can now restart the SAS Federation Server and begin using SSL.

# Enable AES

Enter the following command to enable AES:

```
FSManagerInstallPath\bin\update_secure
```

After you enable AES, you can authenticate on the SAS Federation Server Manager with the user ID SAS002 and password SAS003. Replace these default credentials immediately.

Until you enable AES, the SAS Federation Server Manager will encrypt with the default SASPROPPRIETARY encryption algorithm.

# Configure SAS Federation Server Client

The SAS Federation Server Client software selectively installs the following components:

- SAS Drivers for Federation Server
- ASBATCH Utility

The SAS Drivers for Federation Server are used by your applications to connect to data sources on SAS Federation Servers. The Secure drivers require no additional configuration to implement Secure features. The drivers are transparently configured to work with AES encryption and, if enabled, FIPS compliance. To learn more about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

The ASBATCH utility runs on any client, to enable administrators to make batch updates to the Authentication Server database. The database manages users, groups, domains, logins, and shared logins. The ASBATCH utility is documented in the *DataFlux Authentication Server Administrator's Guide*.

# Configure SAS Visual Process Orchestration Runtime Server

## Overview

When configured with DataFlux Secure, the SAS Visual Process Orchestration Runtime Server uses configurable enhanced encryption to store interprocess passwords and protect network communication.

To add security to connections with SOAP clients, the Runtime Server can be configured to use the Single Sockets Layer. When configured with SSL, the Runtime Server uses SSL exclusively. Non-SSL connections are rejected.

## Configure Access to FIPS-Compliant Servers

SAS Federation Servers and DataFlux Authentication Servers with DataFlux Secure can be enabled to run in compliance with FIPS 140-2. If your Runtime Server needs to connect to a FIPS-enabled server, then the Runtime Server needs to connect with a SAS driver for ODBC or JDBC. For more information about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

## Configure SSL

Follow these steps to configure SSL on your Runtime Servers:

1. If the DataFlux Data Management Server is running, then stop the server.
2. Open the configuration file dmserver.cfg.
3. Add the following options to enable DataFlux Secure and SSL:

```
DMSERVER/SECURE = YES
DMSERVER/SOAP/SSL = YES
```

Enter a value of NO to disable SSL on the Runtime Server.

4. Add the following options to identify your administrative group and identify your Authentication Server:

   ```
   DMSERVER/SECURE/GRP_ADMIN = your-group-name
   DMSERVER/AUTH_SERVER_LOC = fully-qualified-path:port-number
   ```

5. To identify a key file and password, add these two options:

   ```
   DMSERVER/SOAP/SSL/KEY_FILE = path-to-key-file
   DMSERVER/SOAP/SSL/KEY_PASSWD = encrypted-password-for-key-file
   ```

   To encrypt a password, see Encrypt Passwords.

6. To identify trusted certificates (if you use certificates):

   ```
   DMSERVER/SOAP/SSL/CA_CERT_FILE = trusted-certificates-filename
   DMSERVER/SOAP/SSL/CA_CERT_PATH = path-to-trusted-certificates-file
   ```

7. Save and close the configuration file.

8. Start the Runtime Server.

# Configure SAS Visual Process Orchestration Web Client

DataFlux Secure is required when the SAS Visual Process Orchestration Web Client connects to a similarly configured SAS Visual Process Orchestration Runtime Server. The encryption algorithm must also match the one that is implemented on the SAS Visual Process Orchestration Design Server.

The web client requires the use of SSL when that client communicates with an SSL-enabled Runtime Server. To configure SSL on a client host, install 32-bit OpenSSL. Note that you should install 32-bit OpenSLL even when the 32-bit client is installed on a 64-bit host. The 32-bit and 64-bit versions of OpenSSL can reside on the same host without conflict.

To complete the configuration of SSL, you first create certificates. You then load server certificates into the Java TrustStore of the web client. Each instance of the web client needs to store one certificate for each of its SSL-enabled servers. To load server certificates, see Add Server Certificates to the Java TrustStore.


Note: The web client requires you to load certificates because it uses Java SSL.

The configuration files for the web client are not affected by the installation of DataFlux Secure.

# Configure DataFlux Web Studio

The DataFlux Secure software is required to be enabled and configured on DataFlux Web Studio when that client connects to Secure-enabled DataFlux Web Studio

Servers, DataFlux Data Management Servers, SAS Federation Servers, and DataFlux Authentication Servers.

DataFlux Web Studio requires the use of SSL when that client communicates with an SSL-enabled DataFlux Web Studio Server or DataFlux Data Management Server. To configure SSL on a client host, install 32-bit OpenSSL. Note that you should install 32-bit OpenSLL even when the 32-bit client is installed on a 64-bit host. The 32-bit and 64-bit versions of OpenSSL can reside on the same host without conflict.

To complete the configuration of SSL, you first create certificates. You then load server certificates into the Java TrustStore of DataFlux Web Studio. Each instance of DataFlux Web Studio needs to store one certificate for each of its SSL-enabled servers. To load server certificates, see Add Server Certificates to the Java TrustStore.


Note: Web Studio requires you to load certificates because it uses Java SSL.

DataFlux Web Studio can be configured to connect to a SAS Federation Server or to a DataFlux Authentication Server. If those servers are configured for FIPS compliance, then you need to configure DataFlux Web Studio accordingly. DataFlux Web Studio needs to communicate with FIPS-enabled server using a DataFlux driver for ODBC or JDBC, rather than using a direct connection. For more information about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

The configuration files for DataFlux Web Studio are not affected by the installation of DataFlux Secure.


Note: When you define an SSL-enabled DataFlux Web Studio Server or DataFlux Data Management Server, make sure that the **Server** field contains an HTTPS address, such as https://yourDMServer.yourcompany.com.

## Add Server Certificates to the Java TrustStore

If you are using self-signed certificates, then you need to load server certificates into the Java TrustStore. You add one certificate for each of the SSL-enabled servers that will connect to a particular client or server. Note of course that self-signed certificates do not provide authentication or the level of trust of signed certificates.

If you are using trusted certificates (from a Certificate Authority such as VeriSign), then you do not need to load server certificates into the Java TrustStore.

To load certificates, use the keytool utility from Oracle, as directed in the following document:

http://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html

# Configure DataFlux Web Studio Server

## Overview

When configured with DataFlux Secure, the DataFlux Web Studio Server uses AES encryption to store passwords and to encrypt client connections.

When it is configured with SSL, the DataFlux Web Studio Server uses SSL exclusively. Non-SSL communication is rejected.

## Configure Access to FIPS-Compliant Servers

SAS Federation Servers and DataFlux Authentication Servers with DataFlux Secure can be enabled for compliance with FIPS 140-2. If a DataFlux Web Studio Server needs to connect to a FIPS-enabled server, then the Web Studio Server needs to connect with a SAS driver for ODBC or JDBC. For more information about the drivers, see the *SAS Drivers for Federation Server User's Guide*.

## Configure SSL

Follow these steps to configure SSL on a DataFlux Web Studio Server:

1. If the DataFlux Web Studio Server is running, then stop the server.
2. Open the configuration file *install-path*/etc/dmserver.cfg.
3. Add the following option to enable SSL (required):
   ```
   DMSERVER/SOAP/SSL = YES
   ```
   (Enter a value of NO to disable SSL.)
4. To identify a key file and password, add these two options:
   ```
   DMSERVER/SOAP/SSL/KEY_FILE = path-to-key-file
   DMSERVER/SOAP/SSL/KEY_PASSWD = encrypted-password-for-key-file
   ```
   To encrypt a password, see Encrypt Passwords.
5. To identify trusted certificates, add these two options:
   ```
   DMSERVER/SOAP/SSL/CA_CERT_FILE = trusted-certificates-filename
   DMSERVER/SOAP/SSL/CA_CERT_PATH = path-to-trusted-certificates-file
   ```
6. Save and close the configuration file.
7. Start the DataFlux Web Studio Server.

# Replace Passwords

After you install and configure DataFlux Secure on your clients and servers, follow these steps to replace any existing passwords on your clients or servers. When you replace these passwords, they are stored on disk using AES encryption.

Passwords that you do not replace remain functional, but they continue to be stored using the less-protective SASPROPRIETARY encryption algorithm.

With appropriate privileges, administrators can replace a SASPROPRIETARY password with a password that has been encrypted using the AES algorithm. To learn how to use the password encryption tool, see Encrypt Passwords.

Follow these steps to replace passwords:

1. Complete all of the configuration steps before you replace passwords.
2. Open DataFlux Data Management Studio.
3. Click the **Administration** riser in the lower left corner.
4. If your enterprise uses a SAS Federation Server, right-click that server, and then select **Open**.
5. Right-click the server again and select **Connect**.
6. Select **Tools -> Federation Server Options**.
7. Click the **Advanced** tab.
8. Replace the password for the Shared Login Manager and click **OK**.
9. Repeat the preceding steps for any other SAS Federation Servers in your enterprise that were operational before you installed DataFlux Secure.
10. Right-click your DataFlux Authentication Server and select **Open**.
11. Log on to your DataFlux Authentication Server with an account that has administrative privileges.
12. Click the **Shared Logins** riser.
13. Right-click a shared login and select **Edit**.
14. Replace the outgoing password for the shared login, and click **OK**. Note that the outgoing login is the one that establishes the connections to your network data source.
15. Repeat the preceding password replacement steps for all of your other shared logins.
16. Repeat the preceding steps for any other DataFlux Authentication Servers in your enterprise that were operational before you installed DataFlux Secure.
17. Refer to the next topic to replace all user passwords on any other DataFlux Authentication Servers in your enterprise.

## Replace User Passwords

If you were a user of DataFlux Data Management Studio before you installed DataFlux Secure, then follow these steps to replace your passwords on your DataFlux Authentication Server. When you replace your passwords, you store them on disk using AES encryption.

1. Open DataFlux Data Management Studio.
2. Click the **Administration** riser.
3. Right-click your DataFlux Authentication Server and select **Open**.
4. Click the **Users** riser.
5. Double-click your user name to display your logins.
6. For all of your logins that have passwords, right-click the login and click **Edit**.
7. In the **Edit** dialog box, replace the existing login with the same login,and then click **OK**.

# Encrypt Passwords

The DataFlux Data Management Server is delivered with a utility that converts a plain text password into an encrypted password. The password is encrypted with the 256-bit AES algorithm. You can copy the encrypted password into files and fields.

An encrypted password is required as the value of the option DMSERVER/SOAP/SSL/KEY_PASSWD.

In Windows, run *install-path*`\bin\EncryptPassword.exe`. Enter the password, confirm your initial entry, and receive the encrypted password.

In UNIX and Linux, run `dmsadmin crypt`.

A similar encryption tool is provided with the SAS drivers that are used by your clients to connect to data sources on SAS Federation Servers. For further information about this encryption utility, see the *SAS Drivers for Federation Server User's Guide*.

# Administer DataFlux Secure

After you install and configure DataFlux Secure, the software requires no maintenance other than the periodic replacement of the license file.

When you upgrade a client or server that uses DataFlux Secure, you need to reconfigure DataFlux Secure.

DataFlux Secure does not have a separate uninstall process. If you uninstall a client or server that uses DataFlux Secure, then DataFlux Secure is removed along with the client or server.

# Troubleshoot DataFlux Secure

If you cannot open a trusted connection between two hosts, then you should first ensure that DataFlux Secure has been installed on each host. Next, confirm that the configuration files on both hosts contain the option values and environment variables that are described in the Install and Configure chapter.

If DataFlux Secure has been installed and configured on both hosts, you can check the log files on the hosts to help isolate the error. To obtain additional information, contact SAS Technical Support to temporarily increase the amount of data that is collected in the log files.

For more information about logging, including the locations of the log files, refer to the user's guides and administrator's guides for your clients and servers, as listed in Recommended Reading.

# Glossary

## A

**Advanced Encryption Standard**

AES, from the US National Institute of Standards and Technology, defines symmetric-key encryption using key lengths of 128, 192, and 256 bits. DataFlux Secure uses 256-bit keys.

**authentication provider**

a software component that is used for identifying and authenticating users. For example, an LDAP server or the host operating system can provide authentication.

## C

**Certificate Revocation List**

a CRL contains a list of digital certificates that were revoked by a specific Certification Authority.

**Certification Authority**

CA, a commercial or private organization that provides security services to the e-commerce market. A Certification Authority creates and maintains digital certificates, which help to preserve the confidentiality of an identity. Microsoft, VeriSign, and Thawte are examples of commercial Certification Authorities.

## D

**decryption**

the process whereby a given algorithm is used to convert encrypted text into its original plan text.

**domain name**

identifies a collection of network devices. When supplied in a login, the domain name identifies an authentication provider.

## E

**encryption**

the process of encoding plain text into a format that can be decrypted with a specified algorithm, in this case, AES.

## F

**Federal Information Processing Standard**

a document that specifies how software must operate in order to meet standards set by the United States government.

**FIPS**

Federation Information Processing Standard

## K

**key**

provides the basis for the transformation of plaintext into ciphertext for encryption, and the reverse for decryption.

**keyconfig**

a DataFlux utility that enables the process of creating and installing trusted certificates.

**keytool**

a Java utility that enables the process of creating and installing trusted certificates.

## L

**login**

a combination of a user ID, password, and, if required, a domain name that is supplied by users for the purpose of authentication.

## O

**OpenSSL**

a publicly distributed software product that enables client/server communication using trusted certificates, authentication, and HTTPS addresses.

## P

**password replacement**

the process whereby existing passwords encrypted at a lower level of trust are replaced with newly encrypted passwords that provide a higher level of trust.

## S

**Secure Sockets Layer**

SSL is a protocol that provides network security and privacy. SSL uses encryption algorithms RC2, RC4, DES, TripleDES, and AES. SSL provides a high level of security. It was developed by Netscape Communications.

# Index

**T**



**V**



**W**

# Contact SAS

SAS Institute Inc.
100 SAS Campus Drive
Cary, NC 27513-2414, USA

Phone: 919-677-8000
Fax: 919-677-4444

## SAS Technical Support

Phone: 919-677-8008
Email: techsupport@sas.com
Web: http://support.sas.com/techsup/contact/

## SAS Documentation Support

Email: yourturn@sas.com