



DATAFLUX
data management

DataFlux[®] Secure 2.7 Administrator's Guide

DataFlux[®] Secure 2.7

Administrator's Guide

Applies to these releases and later:

DataFlux Authentication Server 4.1

DataFlux Data Management Server 2.7

DataFlux Data Management Studio 2.7

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

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2017. *DataFlux® Secure 2.7: Administrator's Guide*. Cary, NC: SAS Institute Inc.

DataFlux® Secure 2.7: Administrator's Guide

Copyright © 2017, SAS Institute Inc., Cary, NC, USA

All rights reserved. Produced in the United States of America.

For a hard-copy book: No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute Inc.

For a web download or e-book: Your use of this publication shall be governed by the terms established by the vendor at the time you acquire this publication.

The scanning, uploading, and distribution of this book via the Internet or any other means without the permission of the publisher is illegal and punishable by law. Please purchase only authorized electronic editions and do not participate in or encourage electronic piracy of copyrighted materials. Your support of others' rights is appreciated.

U.S. Government Restricted Rights Notice: Use, duplication, or disclosure of this software and related documentation by the U.S. government is subject to the Agreement with SAS Institute and the restrictions set forth in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987).

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

June 2017

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.

SAS® and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are registered trademarks or trademarks of their respective companies. For additional information, see the [Legal Notices](#) appendix.

Table of Contents

Accessibility	iii
What's New in DataFlux Secure 2.7	iii
Recommended Reading	iii
Overview of DataFlux Secure	1
Applicability	1
Features and Scope	1
Install and Configure	7
Installation Notes	7
About Configuration	7
Configure OpenSSL	8
Configure DataFlux Data Management Studio	11
Configure DataFlux Data Management Server	12
Configure SAS Federation Server	14
Configure SAS Federation Server Client	14
Configure SAS Visual Process Orchestration Runtime Server	15
Configure SAS Visual Process Orchestration Web Client	16
Configure DataFlux Web Studio	16
Configure DataFlux Web Studio Server	17
Configure DataFlux Authentication Server	18
Encrypt Passwords	25
Administer DataFlux Secure	25
Troubleshoot DataFlux Secure	26
Appendixes	26
ODBC Drivers	26
Legal Notices	27

Glossary	32
Index	34

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 2.7

The main enhancements for DataFlux Secure 2.7 include the following:

- The June 2017 update for DataFlux Secure 2.7 provides performance, stability, and documentation enhancements.
- A new topic on ODBC Drivers including the SSL-encrypted drivers available in DataFlux Secure
- FIPS compliance for SOAP (HTTPS) connections to DataFlux Data Management Server
- The ASBATCH utility is no longer available on the SAS♦Federation Server Client

FIPS Compliance for SOAP Connections

Any SOAP client of DataFlux Data Management Server can benefit from the FIPS compliance. For more information, see the DataFlux Data Management Studio.

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 9.4 Intelligence Platform: Security Administration 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

- [Applicability](#)
- [Features and Scope](#)

Applicability

DataFlux Secure 2.7 is distributed with and can be enabled for the following products:

- DataFlux Data Management Studio 2.7
- DataFlux Data Management Server 2.7
- SAS Federation Server 4.2
- SAS Visual Process Orchestration 2.1 Runtime Server
- SAS Visual Process Orchestration 2.1 web client
- DataFlux Web Studio 2.5
- DataFlux Web Studio Server 2.5
- DataFlux Authentication Server 4.1M1

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](#)) protects HTTPS 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 Data Management Studio	Enables the creation of jobs and services that run on the client and	DataFlux Secure allows DataFlux Data

Client or Server	Description	DataFlux Secure Implementation
	<p>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 Management Server and DataFlux Authentication Server.</p>	<p>Management Studio to communicate with servers that are configured to use enhanced encryption. Without DataFlux Secure, DataFlux Data Management Studio is limited to using basic HTTP connections for SOAP communications and SAS Proprietary encryption for communication with the SAS Metadata Server.</p>
DataFlux Data Management Server	<p>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 SAS Metadata Server.</p> <p>Network clients can run jobs and services using a GSOAP interface. Server connections can be disabled by IP address, or by global ALLOW or DENY groups.</p>	<p>Uses configurable encryption, SSL, and available FIPS compliance to protect all network traffic, including GSOAP connections. Users and groups are defined and maintained on the SAS Metadata Server. The encryption algorithm is specified as part of the server definition on the SAS Metadata Server.</p>
SAS Federation Server	<p>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 on the SAS Metadata Server.</p>	<p>Uses configurable encryption and can use FIPS compliance to support connections to similarly configured clients and servers.</p>
SAS  Federation Server Client	<p>This package provides the SAS drivers for Federation Server, which enable your applications to connect to data sources on SAS Federation Server.</p>	<p>DataFlux Secure allows SAS Federation Server to communicate with servers that are configured to use enhanced encryption. Without DataFlux Secure, SAS Federation Server is limited to using basic HTTP connections for SOAP communications</p>

Client or Server	Description	DataFlux Secure Implementation
		and SAS Proprietary encryption for communication with the SAS Metadata 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 encryption and SSL. When SSL is enabled, the Runtime Server accepts only those connections that use HTTPS addresses. The SAS Metadata Server provides authentication support, specifies the encryption algorithm, and maintains user and group profiles. The Runtime Server maintains local authorizations.
SAS Visual Process Orchestration Web Client	The web client provides an environment for the creation and testing of orchestration jobs.	Uses configurable encryption and SSL to communicate with an SSL-enabled Runtime Server. The SAS Metadata Server provides support for authentication. The Runtime Server specifies the encryption algorithm.
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 authentication and for user and group profiles that are used for internal authorization.	Uses configurable enhanced encryption and SSL. SSL is used to communicate with an SSL-enabled DataFlux Web Studio Server or DataFlux Data Management Server. The DataFlux Authentication Server is required to support authentication and authorization.
DataFlux Web Studio Server	Runs jobs and services in support of Reference Data Manager, Monitor and Dashboard components of	Uses configurable encryption to communicate with

Client or Server	Description	DataFlux Secure Implementation
	DataFlux Web 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.	similarly configured clients and servers. The DataFlux Authentication Server is required to support authentication and authorization.
DataFlux Authentication Server	Authenticates DataFlux Data Management Studio users 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.	The DataFlux Authentication Server is used only to support legacy releases and DataFlux Web Studio. The default authentication provider is now the SAS Metadata Server. Like the SAS Metadata Server, the DataFlux Authentication Server uses configurable 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 Secure does not provide a graphical user interface or run any daemon processes.

AES

When enabled, AES (Advanced Encryption Standard) algorithms can be specified by the SAS Metadata Server. Several other encryption algorithms are available, as defined in the metadata definitions of the servers on the data management platform. The Web Studio client and server receive their encryption algorithm from the DataFlux Authentication Server.

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).

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.

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.

When a server is configured for SSL, it accepts only HTTPS connections. HTTP connections are not used or accepted.

SSL is implemented using OpenSSL. OpenSSL is downloaded and distributed across your site according to your company's existing security policies. Those policies address the tasks of requesting and installing the keys and digital certificates that are used by SSL.

The supported version of OpenSSL for all clients and servers is 1.0.x.

FIPS

Compliance with the Federal Information Processing Standard 140-2 is required by certain businesses and governmental entities.

FIPS compliance is optional, as are the other features in DataFlux Secure.

Like SSL, FIPS compliance is generally applied across all of the clients and servers that are part of a data management platform, including network clients.

Starting with the 2.7 release, FIPS compliance for the DataFlux Data Management Server includes full encryption support for all GSOAP connections. Clients use GSOAP connections to request the execution of jobs and services.

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 SAS Metadata Server or on the DataFlux Authentication Server. These servers are known as authentication providers.

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 authentication provider. If she is a consumer of that shared login, then the authentication provider provides DataFlux Web Studio with the credentials that are necessary to open the connection to the database.

The passwords for shared logins, along with the outbound credentials for databases, are stored only on the authentication provider.

The only other stored passwords are those that are used to open connections between servers. One such connection is used to connect a server to the authentication provider. Jobs running on the DataFlux Data Management Server can also use a stored password to open connections to the SAS Federation Server.

Passwords are not displayed in any graphical user interface.

For more information about using the SAS Metadata Server for passwords, see the Update a Managed Password section of the [SAS 9.4 Intelligence Platform: Security Administration Guide](#). For information about password maintenance, see the How to Re-Encrypt Stored Passwords section of the [SAS 9.4 Intelligence Platform: Security Administration Guide](#).

Install and Configure

- [Installation Notes](#)
- [About Configuration](#)
- [Configure OpenSSL](#)
- [Configure DataFlux Data Management Studio](#)
- [Configure DataFlux Data Management Server](#)
- [Configure SAS Federation Server](#)
- [Configure SAS Federation Server Client](#)
- [Configure SAS Visual Process Orchestration Runtime Server](#)
- [Configure SAS Visual Process Orchestration Web Client](#)
- [Configure DataFlux Web Studio](#)
- [Configure DataFlux Web Studio Server](#)
- [Configure DataFlux Authentication Server](#)
- [Encrypt Passwords](#)
- [Administer DataFlux Secure](#)

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 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](#)
- [Download and Deploy OpenSSL onto Windows Hosts](#)
- [Create SSL Certificates](#)

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 1.0.x.

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.x 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 (CA). 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 v1.0.x or later from a provider such as [Shining Light Productions](#).

DataFlux Data Management Studio is a 32-bit application. It requires the 32-bit OpenSSL even when installed on 64-bit operating systems.

Most modern server environments run with 64-bit operating systems. DataFlux Data Management Server, DataFlux Web Studio Server, and SAS Visual Process Orchestration Runtime Server will deploy to match their operating system. 64-bit servers require 64-bit OpenSSL. 32-bit OpenSSL and 64-bit OpenSSL can coexist on the same 64-bit system.

Install OpenSSL by executing the following:

```
Winbit-lengthOpenSSLversion-number.exe
```

For example:

```
Win64OpenSSL1.0.2.exe
```

1. Install OpenSSL to C:\OpenSSL-Win64 or C:\OpenSSL-Win32.
2. Select the installer option **Copy OpenSSL DLLs to the Windows System Directory**.
3. If you are installing OpenSSL on a client, the installation process is complete. Move on to [Create a Trusted Certificate](#).
4. 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
```

Create SSL Certificates

When a client requests an SSL connection, the server delivers a certificate containing the server's public 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 can be created with an OpenSSL command.

Privacy Enhanced Mail Format

The Privacy Enhanced Mail format or PEM, format contain the public certificate and the private key for servers such as DataFlux Data Management Server, DataFlux Web Studio Server, and SAS Visual Process Orchestration Runtime Server.

This PEM file is Base64 encoded and is easily read with a simple text editor.

However, do not edit with a robust editor such as WordPad, or Word, or to change the format to introduce Windows line termination characters, a Windows end-of-file character, or to use Unicode representation.

If you have a Base64 encoded certificate and private key from a CA, you can create a PEM by using the command line on these:

Windows: `copy myhost.crt+myhost.key myhost.pem`

Unix: `cat myhost.crt myhost.key >myhost.pem`

The OpenSSL commands below will create the PEM file containing a self-signed certificate.

The resulting PEM file should not be generally available. The server using the PEM will extract the public certificate and return it to requesting clients.

Create a Trusted Certificate

A trusted certificate certifies the ownership of a public key by the named subject of the certificate.

This allows clients to rely upon signatures or on assertions made by the private key that corresponds to the certified public key.

In this model of trust relationships, a CA is a trusted third party that is trusted both by the subject, who is the owner of the certificate, and by the party that is relying upon the certificate.

To create a trusted certificate on a host with OpenSSL, simply purchase the certificate from a CA.

Create a Self-Signed Certificate on Windows

A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies. Follow these steps to create a self-signed certificate on a Windows host that includes OpenSSL:

1. In the Run dialog box 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 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 OpenSSL 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 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.

Configure DataFlux Data Management Server

Overview

When configured with DataFlux Secure, the DataFlux Data Management Server can be enabled to use SSL to protect Internet connections. In addition, the server configuration can be further enhanced to comply with the FIPS standard 140-2.

When SSL is enabled, the DataFlux Data Management Server accepts only HTTPS connections. To send HTTPS requests, SSL must also be enabled on clients and other servers.

When configured for SSL, the DataFlux Data Management Server requires OpenSSL. Most modern server environments run with 64-bit operating systems. DataFlux Data Management Server deploys to match its operating system. 64-bit servers require 64-bit OpenSSL. 32-bit servers require [32-bit OpenSSL](#). 32-bit OpenSSL and 64-bit OpenSSL can coexist on the same 64-bit system.

The encryption level or algorithm for the DataFlux Data Management Server is determined by the server definition on the SAS Metadata Server.

Prerequisites

OpenSSL must be fully configured before security can be enabled on the DataFlux Data Management Server.

On the SAS Management Console, create a new HTTPS server metadata object for the DataFlux Data Management Server. In that metadata object, select the encryption algorithm that you want to apply to HTTPS connections.

If FIPS compliance is to be enabled, then FIPS-compliant OpenSSL DLL libraries must be deployed on the server host.

On UNIX platforms, SAS uses OpenSSL FIPS 140-2 module. The module must be compiled and installed by the customer to build the OpenSSL libraries in order to ensure FIPS 140-2 compliance. SAS uses OpenSSL 1.0.x and uses the FIPS 2.x module with a certificate number of 1747.

The only certified UNIX operating environments included are HP-UX for Itanium Processor, Solaris for SPARC Processor, Solaris for Intel 64 and AMD64 Processor, and Linux for Intel 64 and AMD64 Processor. AIX is not certified.

On Windows platforms, DataFlux Data Management Server uses OpenSSL 140-2 module. The module must be compiled and installed by the customer to build the OpenSSL libraries in order to ensure FIPS 140-2 compliance. SAS uses OpenSSL 1.0.x and uses the FIPS 2.x module with a certificate number of 1747.

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 and FIPS

Follow these steps to configure SSL and FIPS, if desired, 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 option or enter a value of YES to enable SSL on the DataFlux Data Management Server:

```
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 (if you use certificates):

```
DMSERVER/SOAP/SSL/CA_CERT_FILE = trusted-certificates-filename
```

```
DMSERVER/SOAP/SSL/CA_CERT_PATH = path-to-trusted-certif-file
```

6. If desired, set the following option to enable FIPS compliance.

```
DMSERVER/SOAP/SSL/FIPS = Yes
```

7. Enter one of the following commands to configure the SOAP DLL:

```
bin\set_soap ssl
```

```
bin\set_soap fips
```



Note: The `fips` option enables the FIPS DLLs and the SSL DLLs.

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

Configure Encryption

The encryption algorithm used by the DataFlux Data Management Server is determined by the server definition of the SAS Metadata Server. To view or change the encryption algorithm, edit the server definition in SAS Management Console. For specific instructions, see the [How to Change Over-the-Wire Encryption for IOM Servers](#) topic in the *SAS Intelligence Platform: Security Administration Guide*.

Configure SAS Federation Server

Enable or Disable FIPS

FIPS support is enabled during installation if FIPS is determined to be enabled on the SAS Metadata Server.

Follow these steps to disable and re-enable FIPS support:

1. Enable or disable FIPS on the SAS Metadata Server.
2. Open the file `fed-server-config-path/etc/dfs_serv.xml`.
3. Change the `EncryptFIPS` option to True or False:

```
<Option name="EncryptFIPS">TRUE</Option>
```

Or:

```
<Option name="EncryptFIPS">FALSE</Option>
```

4. Restart the DataFlux Data Management Server.

Configure Encryption

The encryption algorithm used by the DataFlux Data Management Server is determined by the server definition on the SAS Metadata Server. To view or change the encryption algorithm, edit the server definition in SAS Management Console. For specific instructions, see the [How to Change Over-the-Wire Encryption for IOM Servers](#) topic in the *SAS Intelligence Platform: Security Administration Guide*.

Configure SAS Federation Server Client

The SAS Federation Server Client software selectively installs the SAS Drivers for Federation Server. 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*.

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-nam
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-certif-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 OpenSSL 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 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, 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 requires OpenSSL. Most modern server environments run with 64-bit operating systems. DataFlux Web Studio Server deploys to match its operating system. 64-bit servers require 64-bit OpenSSL. 32-bit servers require [32-bit OpenSSL](#). 32-bit OpenSSL and 64-bit OpenSSL can coexist on the same 64-bit system.

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-certif-file`
6. Save and close the configuration file.
7. Start the DataFlux Web Studio Server.

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 a DataFlux Authentication Server to act as an SSL client for an external authentication provider 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 `SLLCERTISS` 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-certif-file</Option>
<Option name="SSLPVTKEYLOC">path-to-the-certif-file-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>
```

Replace Passwords

After you install and configure DataFlux Secure on your DataFlux Authentication Server, 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. Right-click your DataFlux Authentication Server and select **Open**.
5. Log on to your DataFlux Authentication Server with an account that has administrative privileges.
6. Click the **Shared Logins** riser.
7. Right-click a shared login and select **Edit**.
8. 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.
9. Repeat the preceding password replacement steps for all of your other shared logins.
10. Repeat the preceding steps for any other DataFlux Authentication Servers in your enterprise that were operational before you installed DataFlux Secure.
11. 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](#).

Appendixes

- [ODBC Drivers](#)
- [Legal Notices](#)

ODBC Drivers

Various Data Management products use Open Database Connectivity (ODBC) database drivers to link applications to a variety of database management systems. The ODBC drivers are deployed with those products without the secure components. As of the 2.7 release of DataFlux Secure, a secure component that enables encrypted connections to databases is available for some of these DataDirect 7.1 ODBC drivers. These drivers are enabled for Secure Sockets Layer (SSL) technology that establishes an encrypted link between the application and the database.

The current 64-bit branded ODBC drivers that are available with DataFlux Secure include the following:

DataDirect ODBC Drivers	Driver Enabled for SSL Encryption
Apache Hive Wire Protocol	x
DB2 Wire Protocol	x
Greenplum Wire Protocol	x
Impala Wire Protocol	
Informix Wire Protocol	
MySQL Wire Protocol	x
Oracle	
Oracle Wire Protocol	x
Postgres Wire Protocol	x
Progress OpenEdge Wire Protocol	x

DataDirect ODBC Drivers	Driver Enabled for SSL Encryption
Salesforce	x
SQL Server Legacy Wire Protocol	
SQL Server Wire Protocol	x
Sybase IQ Wire Protocol	
Sybase Wire Protocol	x
Teradata	

For more information about these drivers, see the documentation in the ODBC folder of your application.

Legal Notices

Apache Portable Runtime License Disclosure

Copyright © 2017 DataFlux Corporation LLC, Cary, NC USA.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Apache/Xerces Copyright Disclosure

The Apache Software License, Version 3.1

Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR

ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 1999, International Business Machines, Inc., <http://www.ibm.com>. For more information on the Apache Software Foundation, please see <http://www.apache.org>.

Boost Software License Disclosure

Boost Software License - Version 1.0 - August 17, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Canada Post Copyright Disclosure

The Data for areas of Canada includes information taken with permission from Canadian authorities, including: © Her Majesty the Queen in Right of Canada, © Queen's Printer for Ontario, © Canada Post Corporation, GeoBase©, © Department of Natural Resources Canada. All rights reserved.

DataDirect Copyright Disclosure

Portions of this software are copyrighted by DataDirect Technologies Corp., 1991 - 2008.

Expat Copyright Disclosure

Part of the software embedded in this product is Expat software.

Copyright © 1998, 1999, 2000 Thai Open Source Software Center Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

gSOAP Copyright Disclosure

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright © 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IBM Copyright Disclosure

ICU License - ICU 1.8.1 and later [as used in DataFlux clients and servers.]

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995-2005 International Business Machines Corporation and others. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Informatica Address Doctor Copyright Disclosure

AddressDoctor© Software, © 1994-2015 Platon Data Technology GmbH

Loqate Copyright Disclosure

The Customer hereby acknowledges the following Copyright notices may apply to reference data.

Australia: Copyright. Based on data provided under license from PSMA Australia Limited (www.pdma.com.au)

Austria: © Bundesamt für Eich- und Vermessungswesen

Brazil: Conteúdo fornecido por MapLink. Brazil POIs may not be used in publicly accessible, internet-based web sites whereby consumers obtain POI data for their personal use.

Canada:

Copyright Notice: This data includes information taken with permission from Canadian authorities, including © Her Majesty, © Queen's Printer for Ontario, © Canada Post, GeoBase ©.

End User Terms: The Data may include or reflect data of licensors including Her Majesty and Canada Post. Such data is licensed on an *as-is* basis. The licensors, including Her Majesty and Canada Post, make no guarantees, representation, or warranties respecting such data, either express or implied, arising by law or otherwise, including but not limited to, effectiveness, completeness, accuracy, or fitness for a purpose.

The licensors, including Her Majesty and Canada Post, shall not be liable in respect of any claim, demand or action, irrespective of the nature of the cause of the claim, demand or action alleging any loss, injury or damages, direct or indirect, which may result from the use or possession of the data or the Data. The licensors, including Her Majesty and Canada Post, shall not be liable in any way for loss of revenues or contracts, or any other consequential loss of any kind resulting from any defect in the data or in the Data.

End User shall indemnify and save harmless the licensors, including Her Majesty the Queen, the Minister of Natural Resources of Canada and Canada Post, and their officers, employees and agents from and against any claim, demand or action, irrespective of the nature of the cause of the claim, demand or action, alleging loss, costs, expenses, damages, or injuries (including injuries resulting in death) arising out of the use of possession of the data or the Data.

Croatia, Cyprus, Estonia, Latvia, Lithuania, Moldova, Poland, Slovenia, and/or Ukraine: © EuroGeographics

France: source: Georoute© IGN France & BD Carto© IGN France

Germany: Die Grundlagendaten wurden mit Genehmigung der zuständigen Behörden entnommen

Great Britain: Based upon Crown Copyright material.

Greece: Copyright Geomatics Ltd.

Hungary: Copyright © 2003; Top-Map Ltd.

Italy: La Banca Dati Italiana © stata prodotta usando quale riferimento anche cartografia numerica ed al tratto prodotta e fornita dalla Regione Toscana.

Norway: Copyright © 2000; Norwegian Mapping Authority

Portugal: Source: IgeoE © Portugal

Spain: Información geográfica propiedad del CNIG

Sweden: Based upon electronic data © National Land Survey Sweden.

Switzerland: Topografische Grundlage © Bundesamt für Landestopographie.

Microsoft Copyright Disclosure

Microsoft, Windows, NT, SQL Server, and Access, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle Copyright Disclosure

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates.

PCRE Copyright Disclosure

A modified version of the open source software PCRE library package, written by Philip Hazel and copyrighted by the University of Cambridge, England, has been used by DataFlux for regular expression support. More information on this library can be found at:
<ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>.

Copyright © 1997-2005 University of Cambridge. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Red Hat Copyright Disclosure

Red Hat Enterprise Linux and Red Hat Fedora are registered trademarks of Red Hat, Inc. in the United States and other countries.

SAS Copyright Disclosure

Portions of this software and documentation are copyrighted by SAS® Institute Inc., Cary, NC, USA, 2009. All Rights Reserved.

SQLite Copyright Disclosure

The original author of SQLite has dedicated the code to the public domain. Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

Sun Microsystems Copyright Disclosure

Java® is a trademark of Sun Microsystems, Inc. in the U.S. or other countries.

TomTom Copyright Disclosure

© 2006-2015 TomTom. All rights reserved. This material is proprietary and the subject of copyright protection, database right protection, and other intellectual property rights owned by TomTom or its suppliers. The use of this material is subject to the terms of a license agreement. Any unauthorized copying or disclosure of this material will lead to criminal and civil liabilities.

USPS Copyright Disclosure

National ZIP, ZIP+4, Delivery Point Barcode Information, DPV, RDI, and NCOA © United States Postal Service 2005. ZIP Code® and ZIP+4® are registered trademarks of the U.S. Postal Service.

DataFlux is a non-exclusive interface distributor of the United States Postal Service and holds a non-exclusive license from the United States Postal Service to publish and sell USPS CASS, DPV, and RDI information. This information is confidential and proprietary to the United States Postal Service. The price of these products is neither established, controlled, or approved by the United States Postal Service.

VMware Copyright Disclosure

VMware® virtual environment provided those products faithfully replicate the native hardware and provided the native hardware is one supported in the applicable DataFlux product documentation. All DataFlux technical support is provided under the terms of a written license agreement signed by the DataFlux customer.

The VMware virtual environment may affect certain functions in DataFlux products (for example, sizing and recommendations), and it may not be possible to fix all problems.

If DataFlux believes the virtualization layer is the root cause of an incident; the customer will be directed to contact the appropriate VMware support provider to resolve the VMware issue and DataFlux shall have no further obligation for the issue.

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

domain name

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

K

key

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

L

login

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

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

A

accessibility, 3
administer dataflux secure, 29
aes encryption, 8

D

dataflux authentication server, 22
dataflux data management server, 16
dataflux data management studio, 15
dataflux secure overview, 5
dataflux web studio, 20
dataflux web studio server, 21
dmsadmin utility, 29

E

encrypt passwords, 28

F

federal information process standard, 9
fips 140-2, 9
fips support, 9, 12, 22

I

installation notes, 11

J

java keytool utility, 21

java truststore, 21

O

openssl, 12
OpenSSL system requirements, 12
overview, dataflux secure, 5

P

password protection, 9
passwords, encrypt, 28

R

recommended reading, 3
replace passwords, 27

S

sas drivers for federation server, 18
sas federation server client, 18
sas visual process orchestration runtime server, 19
sas visual process orchestration web client, 20
ssl, 9, 13
supported clients and servers, 5
system requirements, 11

T

troubleshoot dataflux secure, 30

W

what's new, 3

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