DataFlux® Secure Administrator's Guide

sas®

DATAFLUX®
data management

This page is intentionally blank

DataFlux® Secure

Administrator's Guide

Version 2.4

December 18, 2012

This page is intentionally blank

Contact DataFlux

DataFlux Corporate Headquarters
Toll Free: (877) 846-3589
Tel: (919) 447-3000
Fax: (919) 447-3100
940 NW Cary Parkway, Suite 201
Cary, NC 27513
USA

DataFlux West
Tel: (818) 906-7638
Fax: (818) 907-6012
15300 Ventura Boulevard, Suite 523
Sherman Oaks, CA 91403
USA

Technical Support

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

Documentation Support

Email: yourturn@sas.com

Legal Notices

Table of Contents

Introduction

Accessibility

The DataFlux Secure software includes features that improve usability of the product for users with disabilities. These features are related to accessibility 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 DataFlux products, send an e-mail to techsupport@dataflux.com.

Audience for this Guide

The primary audience for the *DataFlux Secure Administrator's Guide* consists of administrators who manage network servers, network security, and network authentication. The secondary audience for this document consists of managers who need to understand how DataFlux Secure is applied to the DataFlux Data Management Platform.

Conventions Used In This Document

This document uses several conventions for special terms and actions.

Typographical Conventions

The following typographical conventions may be used in this document:

Bold	A bold font represents the literal names of items that are displayed the graphical user interface.
italic	An italic font indicates non-literal, variable, or user-defined text, for subjects such as version numbers or option values.

Path Conventions

In code examples in this document, the installation path of a component of the DataFlux Data Management Platform is represented by the term *install-path*, as shown in this example:

```
    install-path/bin
```

The installation path depends on the operating environment, as shown in the following typical examples:

Windows XP

```
    drive:\Program Files\DataFlux\AuthServer\instance-name
```

Windows 7

```
    32-bit-drive:\Program Files (x86)\DataFlux\AuthServer\instance-name

    64-bit-drive:\Program Files\DataFlux\AuthServer\instance-name
```

UNIX and Linux

```
    /opt/dataflux/authserver/instance-name
```

The *instance-name* is specified when you install the server. The default instance name is either server1 or client1.

Reference Publications

Authentication Server Administrator's Guide
Data Management Server Administrator's Guide
Data Management Studio Installation and Configuration Guide
Data Management Studio User's Guide
Drivers for ODBC and JDBC User's Guide
Federation Server Administrator's Guide
Federation Server Manager User's Guide
Web Studio User's Guide (online help)
Web Studio Installation and Configuration Guide

What's New in DataFlux Secure 2.4

The main enhancements for DataFlux Secure 2.4 include the addition of support for the following components of the Data Management Platform:

- Web Studio
- Web Studio Server
- Federation Server Client

Also included is the addition of a password encryption utility.

Overview of DataFlux Secure

Features and Scope

The DataFlux Secure software provides three high-assurance features for your DataFlux Data Management Platform:

- AES encryption, to protect network communication and passwords.
- The Secure Sockets Layer (SSL), to protect SOAP/HTTP connections.
- FIPS compliance, to ensure that your platform meets stringent regulatory requirements.

In order to maintain interoperability, you need to install DataFlux Secure on all of your platform components. Components that lack a Secure configuration will be unable to communicate with Secure platform components.

DataFlux Secure is delivered as separate installable packages, one for each applicable platform component.

DataFlux Secure is installed as a series of dynamic linked libraries. DataFlux Secure does not provide a graphical user interface or run any daemon processes.

DataFlux Secure is implemented as follows for each component of the Data Management Platform.

Platform Component	Component Description	Secure Features Used
Authentication Server	Authenticates Data Management Studio users and platform services using native authentication providers. The server also maintains a database of users, groups, domains, logins, and shared logins. The database is queried by platform servers as part of their local authorization processes.	Uses AES, optional SSL, and optional FIPS compliance. The server can use SSL to communicate with your SSL-enabled authentication providers, in multiple domains.
Data Management Studio	Enables the creation of jobs and services that run on the client and on Data Management Servers, Federation Servers, and Web Studio Servers. Administers Data Management Servers and	Uses AES encryption and optional SSL. The Studio client can use SSL to communicate with SSL-enabled Data Management Servers and Web Studio Servers.

Platform Component	Component Description	Secure Features Used
	Authentication Servers. Displays information about Federation Servers.	
Data Management Server	Runs jobs and services created in Data Management Studio, stores job output and data collections, and implements access controls for data, jobs, and services. Optionally authenticates and uses group membership data from the Authentication Server. Server connections can be disabled by IP address. Enterprise version of server enables access by your client applications using SOAP or HTTP.	Uses AES encryption and optional SSL. The server can use SSL to communicate with SSL-enabled Web Studio Servers. Web Studio Clients, and your SSL-enabled SOAP clients. When SSL is enabled, the Data Management Server accepts only those connections that use HTTPS addresses.
Web Studio	Provides a user interface for data management tasks that transparently execute jobs on Web Studio Servers and Data Management Servers. Connects to the Authentication Server for user validation and group memberships.	Uses AES encryption and optional SSL. The client can use SSL to communicate with SSL-enabled Web Studio Servers and Data Management Servers.
Web Studio Server	Runs jobs and services created in Web Studio and Data Management Studio, stores job output and data collections, and implements access controls for local data, jobs, and services. Connects to the Authentication Server for user validation and group memberships.	Uses AES encryption and optional SSL. The server can use SSL to communicate with SSL-enabled Data Management Servers, Data Management Studio clients, Web Studio clients, and your SSL-enabled SOAP clients.
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 on the Authentication Server.	Uses AES and optional FIPS compliance. Your SQL clients can connect to the Federation Server using the DataFlux drivers for ODBC and JDBC. See also the Federation Server Client component.
Federation Server Manager	Provides a Web interface that administers data sources and access controls on Federation Servers.	Uses AES as needed to communicate with Secure Federation Servers.
Federation Server Client	This package provides the DataFlux drivers for ODBC and JDBC, which enable your non-platform applications to connect to data sources on Federation Servers. Also, this package optionally installs the ASBATCH utility, which is used for batch updates of the Authentication Server database.	These client components use AES and FIPS compliance as needed to communicate with similarly configured Federation Servers and Authentication Servers.

AES

When it is enabled, the AES (Advanced Encryption Standard) algorithm is implemented in DataFlux Secure with 256-bit keys. AES encryption and decryption protects:

- All platform passwords that are stored on disk. For information about platform passwords, see About Platform Passwords.
- All TCP communication between platform components.
- All network communication that uses SSL, including connections between your SOAP clients and your platform servers.

AES is separately enabled, so you can choose to retain the default encryption algorigthm and use DataFlux Secure for SSL only. The default encryption algorithm is SASPROPRIETARY, which uses 56-bit keys.

Administrators can manually encrypt passwords using AES to replace SASPROPRIETARY passwords, configure DSNs, provide a value for an opton, or supply a password as an argument to a command. To enable the encryption of passwords using AES, the platform servers are delivered with a password encryption tool.

SSL

Support for Secure Sockets Layer (SSL) connection protection is the second feature of the DataFlux Secure software. SSL uses private-key encryption and signed digital certificates to protect connections that have an HTTPS address. DataFlux Secure uses SSL to protect the following connections:

- Authentication Server connections to SSL-configured authentication providers such as Active Directory or LDAP.
- Data Management Server connections to your SSL-enabled SOAP applications.
- Data Management Studio connections to SSL-enabled Data Management Servers.

FIPS

This third feature of the DataFlux Secure software enables you to run your Federation Servers and Authentication Servers 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 Federation Server Manager and the Federation Server Client. In the client package, the DataFlux drivers for ODBC and JDBC and the ASBATCH utility are all FIPS-compliant.

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

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

About Platform Passwords

The DataFlux Data Management Platform stores a minimum number of passwords, and all passwords are encrypted for storage on disk. With DataFlux Secure, all passwords are encrypted for storage using 256-bit keys.

Platform passwords are limited in number because user passwords are not stored on platform components. Instead, user credentials are delivered from the Authentication Server to your existing authentication providers for validation. Because user passwords are not stored on platform components, the only passwords that are stored on the platform relate to shared logins and to platform server interconnections.

Shared logins are collections of users that share credentials for a given enterprise database. For example, if a 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 Server. If she is a consumer of that shared login, then the Authentication Server provides database credentials that allow the job to connect to the database, with specified permissions.

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

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

Passwords are not displayed in any graphical user interface.

AES: How It Works

When you install DataFlux Secure, and when you enable AES encryption, you encrypt the transmission of all logins using AES. AES uses public and private keys to encrypt and decrypt logins. The length of the keys is a strongly protective 256 bits.

AES can also be enabled to encrypt all TCP communication between all instances of the Authentication Server, the Federation Server, the Data Management Server, and the Web Studio Server. AES is also used to encrypt TCP communication between Data Management Studio and the Authentication Server and between Web Studio and the Federation Server. The Data Management Server does not use TCP communication, it uses SOAP/HTTP.

When SSL is enabled, and when AES is enabled, AES is used to encryupt all of the network communication that is transferred durin SSL connections. For connections between external SOAP clients and Data Management Servers, AES encryption can use keys with 128, 192, or 256 bits.

When AES encryption is not enabled, SASPROPRIETARY encryption is used by default, with a maximum key length of 56 bits.

With AES, any passwords that are stored on disk are stored in encrypted form using the 256-bit cipher.

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

SSL: How It Works

When SSL is enabled on an Authentication Server, SSL protects connections between the Authentication Server and any SSL-enabled authentication providers (LDAP or Active Directory.)

When SSL is enabled on a Data Management Server or a Web Studio Server, SSL is the sole means of connecting with these servers. SSL clients include Data Management Studio, Web Studio, and your SOAP clients.

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

Install and Configure

Installation Notes

DataFlux Secure is delivered in separate packages, one for each platform component.

DataFlux Secure is provided through SAS delivery channels. See your SAS Software Order Email (SOE) for information about installing this product.

The default installation path under Windows is: SASHome\product-instance-name

The default installation path under UNIX is: SASHome/*product-instance-name*

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

After you deploy a Secure package, refer to the other topics in this chapter to configure your server.

The system requirements for DataFlux Secure are the same as those of the ordinary platform components. To see the system requirements for platform components, refer to the SAS System Requirements page.

About Configuration

DataFlux Secure provides AES encryption, SSL connection protection, and FIPS compliance. These features require different levels of configuration after you install your Secure packages.

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

Configure SSL on the hosts of all clients and servers that will use SSL.

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

Configure OpenSSL

- About SSL
- Download and Deploy OpenSSL onto Windows Hosts
- Create SSL Certificates
- Create a Java Truststore on UNIX and Linux Hosts

About SSL

Configure OpenSSL on all of the clients and servers that will use SSL. Configure all relevant platform components, and configure any of your own SOAP clients that will use SSL to connect to Data Management Servers.

On UNIX or Linux hosts, OpenSSL is included by default in all supported operating environments. On Windows hosts, you download OpenSSL from a third-party and deploy it to your clients and servers.

After you deploy OpenSSL, you create and configure certificates and enable SSL on all hosts.

Download and Deploy OpenSSL onto Windows Hosts

Follow these steps to download and deploy OpenSSL onto all 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 platform 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 to configure their environment.

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 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 certfificates
   ```

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 will remain valid for three years. Windows will supply a value for `%COMPUTERNAME%`.

5. The command above will present 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/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 will present 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 Authentication Server

Enable AES and FIPS on Windows

After you install a DataFlux Authentication Server with DataFlux Secure, you 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 Data Management Studio, Data Management Server, and Web Studio use the

DataFlux drivers for ODBC or JDBC to communicate with the Authentication Server.

Note: Enabling AES encryption on an Authentication Server requires that you also enable 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

After you install a DataFlux Authentication Server with DataFlux Secure, you execute the set_secure command to enable AES encryption and, optionally, to 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 Data Management Studio, Data Management Server, and Web Studio use the DataFlux drivers for ODBC or JDBC to communicate with the Authentication Server.

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

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

```
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:

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

Configure SSL

Common Steps for All Operating Environments

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

1. Stop the 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, you can 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 Authentication Server is installed on Windows, then continue to the next topic. Otherwise, go to Configure SSL on UNIX/Linux.

Configure SSL on Windows

If your 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 you can save and close the configuration file and restart the 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 need not add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, you can 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. You can 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 you can 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 Authentication Server.

Configure SSL on UNIX or Linux

If your 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 you can skip these steps, save and close the configuration file, and restart your 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 need not add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, you can 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 you can 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 you can specify the protocol that is used at your site:

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

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

   NEVER
   The Authentication Server does not ask for a certificate.

   TRY
   The 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 Authentication Server uses an LDAP authentication provider, and if your site exchanges digital certificates, then you can 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, you can 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 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, you can 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 Authentication Server's certificate and private key, then you can specify the location of the 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 Authentication Server's certificate and private key, then you can 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 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 Data Management Studio

The DataFlux Secure software is required to be installed with Data Management Studio when that client connects to secured Data Management Servers, Web Studio Servers, Federation Servers, and Authentication Servers.

Data Management Studio requires the use of SSL when that client communicates with an SSL-enabled Data Management Server or 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 Data Management Studio needs to connect to a Federation Server or Authentication Server that is enabled for FIPS compliance, you need to configure Studio to communicate with the a DataFlux driver for ODBC or JDBC, rather than using a direct platform connection. For further information on the drivers, see the *DataFlux Drivers for ODBC and JDBC User's Guide*.

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

> Note: In Data Management Studio, when you define an SSL-enabled Web Studio Server or 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 Data Management Server

Overview

When configured with DataFlux Secure, the Data Management Server uses AES encryption as needed to increase security for proprietary interprocess communication with the clients and servers of the Data Management Platform.

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

Configure Access to FIPS-Compliant Servers

Federation Servers and Authentication Servers with DataFlux Secure can be enabled for compliance with FIPS 140-2. If your Data Management Server needs to connect to a FIPS-enabled server, then the Data Management Server needs to connect with a DataFlux driver, either ODBC or JDBC. Standard platform connections cannot be made when you enable FIPS compliance. For further information on the drivers, see the *DataFlux Drivers for ODBC and JDBC User's Guide*.

Configure SSL

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

1. If the 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 Data Management 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 Data Management Server.

Configure Federation Server

Enable AES and FIPS on Windows

After you install a DataFlux Federation Server with DataFlux Secure, you 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 Data Management Studio, Data Management Server, and Web Studio use the DataFlux drivers for ODBC or JDBC to communicate with the Federation Server.

> **Note:** Enabling AES encryption on a Federation Server requires that you also enable AES encryption on all associated instances of Authentication 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

After you install a DataFlux Federation Server with DataFlux Secure, you execute the set_secure command to enable AES encryption and, optionally, to 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 Data Management Studio, Data Management Server, and Web Studio use the DataFlux drivers for ODBC or JDBC to communicate with the Federation Server.

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

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

```
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:

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

Configure Federation Server Manager

Enable AES and FIPS on Windows

After you install a DataFlux Authentication Server with DataFlux Secure, you 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 Data Management Studio, Data Management Server, and Web Studio use the DataFlux drivers for ODBC or JDBC to communicate with the Authentication Server.

> **Note:** Enabling AES encryption on an Authentication Server requires that you also enable AES encryption on all associated instances of Federation Server, Data Management Server, and Data Management Studio, and Web 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 DataFlux Authentication Server with DataFlux Secure, you execute the set_secure command to enable AES encryption and, optionally, to 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 Data Management Studio, Data Management Server, and Web Studio use the DataFlux drivers for ODBC or JDBC to communicate with the Authentication Server.

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

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

```
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:

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

Configure SSL

Common Steps for All Operating Environments

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

1. Stop the 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, you can 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 Authentication Server is installed on Windows, then continue to the next topic. Otherwise, go to Configure SSL on UNIX/Linux.

Configure SSL on Windows

If your 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 you can save and close the configuration file and restart the 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 need not add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, you can 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. You can 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 you can 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 Authentication Server.

Configure SSL on UNIX or Linux

If your 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 you can skip these steps, save and close the configuration file, and restart your 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 need not add the options SSLCRLCHECK and SSLCRLLOC.

1. In the configuration file as_serv_aspsql.xml, you can 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 you can 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 you can specify the protocol that is used at your site:

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

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

   NEVER
   The Authentication Server does not ask for a certificate.

   TRY
   The 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 Authentication Server uses an LDAP authentication provider, and if your site exchanges digital certificates, then you can 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, you can 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 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, you can 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 Authentication Server's certificate and private key, then you can specify the location of the 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 Authentication Server's certificate and private key, then you can 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 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 Federation Server Client

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

- DataFlux Driver for ODBC
- DataFlux Driver for JDBC
- ASBATCH Utility

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

Configure Web Studio

The DataFlux Secure software is required to be installed with Web Studio when that client connects to secured Web Studio Servers, Data Management Server, Federation Servers, and Authentication Servers.

Web Studio requires the use of SSL when that client communicates with an SSL-enabled Web Studio Servers or Data Management Servers. 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, load server certificates into the Java TrustStore of Web Studio. Each instance of 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 is the only component of the Data Management Platform that requires you to load certificates, because Web Studio is the only component that uses Java SSL.

When Web Studio needs to connect to a Federation Server or Authentication Server that is enabled for FIPS compliance, you need to configure Web Studio to communicate with that server using a DataFlux driver for ODBC or JDBC, rather than using a direct platform connection. For further information on the drivers, see the *DataFlux Drivers for ODBC and JDBC User's Guide*.

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

> Note: In Web Studio, when you define an SSL-enabled Web Studio Server or Data Management Server (in the Management Server window), 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 Web Studio's Java TrustStore. You add one certificate for each of the SSL-enabled servers that will connect to a particular instance of Web Studio. If you are using trusted certificates (from a Certificate Authority such as VeriSign), then you do not need to load server certificates into Web Studio's 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 Web Studio Server

Overview

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

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

Configure Access to FIPS-Compliant Servers

Federation Servers and Authentication Servers with DataFlux Secure can be enabled for compliance with FIPS 140-2. If a Web Studio Server needs to connect to a FIPS-enabled server, then the Web Studio Server needs to connect with a DataFlux driver, either ODBC or JDBC. Standard platform connections cannot be made when you enable FIPS compliance. For further information on the drivers, see the *DataFlux Drivers for ODBC and JDBC User's Guide*.

Configure SSL

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

1. If the 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 (if you use certificates):
   ```
   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 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 Federation Servers or Authentication Servers. When you replace these passwords, they are stored on disk using AES encryption.

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

With appropriate privilege, 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 Data Management Studio.
3. Click the **Administration** riser in the lower left corner.
4. If your enterprise uses a 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 Federation Servers in your enterprise that were operational before you installed DataFlux Secure.
10. Right-click your Authentication Server and select **Open**.
11. Log on to your 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 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 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 Authentication Server. When you replace your passwords, you store them on disk using AES encryption.

1. Open Data Management Studio.
2. Click the **Administration** riser.
3. Right-click your 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, then click **OK**.

Encrypt Passwords

The Data Management Server is delivered with a utility that converts a plaintext 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.`.

Administer

After you install and configure DataFlux Secure on your Data Management Platform, 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, make sure that you also update or replace DataFlux Secure. Also be sure to retain or replace the DataFlux Secure license file as part of the upgrade.

Regarding the uninstall process; DataFlux Secure is an add-on product, so it does not appear by name on your computer as a separately removable program or process.

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

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 DataFlux Technical Support to temporarily increase the amount of data that is collected in the log files.

For additional information on logging, including the locations of the log files, refer to the *Data Management Studio User's Guide* and to the *Administrator's Guides* for the Federation Server, Data Management Server, and Authentication Server.

Appendixes

- Legal Notices

Legal Notices

DataFlux Legal Statements

DataFlux Solutions and Accelerators Legal Statements

DataFlux Legal Statements

Apache Portable Runtime License Disclosure

Copyright © 2008 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.

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 NONINFRINGEMENT. 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 [used in DataFlux Data Management Platform]

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.

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.

USPS Copyright Disclosure

National ZIP®, ZIP+4®, Delivery Point Barcode Information, DPV, RDI, and NCOA^{Link}®. © 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

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.

Solutions and Accelerators Legal Statements

Components of DataFlux Solutions and Accelerators may be licensed from other organizations or open source foundations.

Apache

This product may contain software technology licensed from Apache.

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.

Creative Commons Attribution

This product may include icons created by Mark James http://www.famfamfam.com/lab/icons/silk/ and licensed under a Creative Commons Attribution 2.5 License: http://creativecommons.org/licenses/by/2.5/.

Degrafa

This product may include software technology from Degrafa (Declarative Graphics Framework) licensed under the MIT License a copy of which can be found here: http://www.opensource.org/licenses/mit-license.php.

Copyright © 2008-2010 Degrafa. 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, 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 NONINFRINGEMENT. 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.

Google Web Toolkit

This product may include Google Web Toolkit software developed by Google and licensed under the Apache License 2.0.

JDOM Project

This product may include software developed by the JDOM Project (http://www.jdom.org/).

OpenSymphony

This product may include software technology from OpenSymphony. A copy of this license can be found here: http://www.opensymphony.com/osworkflow/license.action. It is derived from and fully compatible with the Apache license that can be found here: http://www.apache.org/licenses/.

Sun Microsystems

This product may include software copyrighted by Sun Microsystems, jaxrpc.jar and saaj.jar, whose use and distribution is subject to the Sun Binary code license.

This product may include Java Software technologies developed by Sun Microsystems,Inc. and licensed to Doug Lea.

The Java Software technologies are copyright © 1994-2000 Sun Microsystems, Inc. All rights reserved.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. DATAFLUX CORPORATION LLC, SUN MICROSYSTEMS, INC. AND THEIR RESPECTIVE LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Java Toolkit

This product includes the Web Services Description Language for Java Toolkit 1.5.1 (WSDL4J). The WSDL4J binary code is located in the file wsdl4j.jar.

Use of WSDL4J is governed by the terms and conditions of the Common Public License Version 1.0 (CPL). A copy of the CPL can be found here at http://www.opensource.org/licenses/cpl1.0.php.

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.