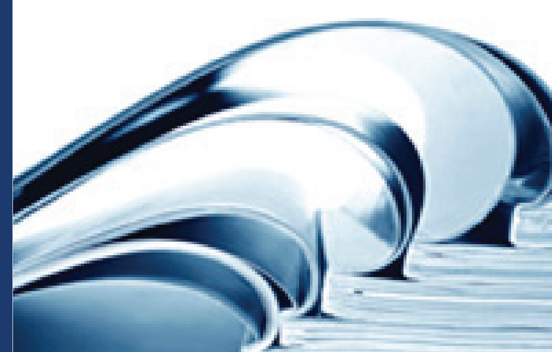
DataFlux Secure Administrator's Guide



DATAFLUX A sas COMPANY

YOUR DATA.
YOUR BUSINESS.
ONE SOLUTION.

This page is intentionally blank

DataFlux Secure

Administrator's Guide

Version 2.2

November 21, 2011

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

DataFlux United Kingdom

Tel: +44 (0) 20 3176 0025
Fax: +44 (0) 20 3411 8382
Enterprise House
1-2 Hatfields
London
SE1 9PG
United Kingdom

DataFlux France

Tel: +33 (0) 4 72 91 31 42

Immeuble Danica B
21, avenue Georges Pompidou
69003 Lyon
France

DataFlux Germany

Tel: +49 (0) 69 66 55 42 04
In der Neckarhelle 162
69118 Heidelberg
Germany

DataFlux Australia

Tel: +61 2 9428 0553
300 Burns Bay Road
Lane Cove, NSW 2066
Australia

Technical Support

Phone: 1-919-531-9000
Email: techsupport@dataflux.com
Web: http://dataflux.com/MyDataFlux-Portal.aspx

Documentation Support

Email: docs@dataflux.com

Legal Information

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.

DataDirect Copyright Disclosure

Expat Copyright Disclosure

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

gSOAP Copyright Disclosure

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

IBM Copyright Disclosure

ICU License - ICU 1.8.1 and later [used in DataFlux Data Management Platform]

Microsoft Copyright Disclosure

Oracle Copyright Disclosure

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/.

Red Hat Copyright Disclosure

VMware

DataFlux Corporation LLC technical support service levels should not vary for products running in a 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

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.

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.

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.

Table of Contents

Introduction

- Accessibility Features
- Audience for this Guide
- Conventions Used In This Document
- DataFlux Reference Publications

Accessibility Features

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	Text in bold signifies a button or action
italic	Identifies document and topic titles, variable syntax, and user-defined syntax
monospace	Typeface used to indicate examples of code

Path Conventions

Various products and operating systems may use different paths for default locations. This document uses the Windows 7 path in examples. The following examples display the differences in paths for three different operating systems:

Windows XP

drive:\Program Files\DataFlux\AuthenticationServer*version*

Windows 7

32bit – *drive*:\Program Files (x86)\DataFlux\AuthenticationServer*version*

64bit – *drive*:\Program Files\DataFlux\AuthenticationServer*version*

UNIX

/opt/dataflux/das

DataFlux Reference Publications

DataFlux Authentication Server Administrator's Guide
DataFlux Federation 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

Overview of DataFlux Secure

Features and Scope

The DataFlux Secure software enables high-assurance AES encryption and decryption for the following components of the DataFlux Data Management Platform:

- DataFlux Data Management Studio
- DataFlux Data Management Server
- DataFlux Authentication Server
- DataFlux Federation Server

The AES (Advanced Encryption Standard) software is implemented in DataFlux Secure with 256-bit keys. AES is used for connections between DataFlux Federation Servers, DataFlux Data Management Servers, and DataFlux Authentication Servers. AES is also used for connections between the Authentication Server and DataFlux Data Management Studio.

Secure Sockets Layer (SSL) is the second feature of DataFlux Secure. SSL uses private-key encryption to protect network connections. DataFlux Secure uses SSL to protect connections between Authentication Servers and the Windows Active Directory or LDAP authentication providers. SSL can also protect connections between SOAP clients and DataFlux Data Management Servers.

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

DataFlux Secure is intended to be installed on all of the instances of Data Management Studio, Authentication Server, Federation Server, and Data Management Server in your enterprise.

The DataFlux Secure installation process automatically modifies Windows configuration files to configure AES. In the UNIX and Linux operating environments, you run a script to configure AES. Additional configuration steps may be required to implement SSL, as described in the Install and Configure chapter.

AES: How it Works

When you install DataFlux Secure, you encrypt the transmission of all logins. AES uses public and private keys to encrypt and decrypt logins. The length of the keys is a strongly protective 256 bits. For connections between external SOAP clients and Data Management Servers, AES encryption can use keys with 128, 192, or 256 bits.

AES is used between the Authentication Server and the Federation and Data Management servers. AES is also used between Data Management Studio and the Authentication Server.

Without AES encryption, 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.

Passwords are not displayed in the Studio interface.

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 DataFlux Secure is installed on Authentication Servers, SSL encrypts and decrypts communication between the Authentication Server and any LDAP or Active Directory authentication providers that also use SSL.

When DataFlux Secure is installed on a Data Management Server, SSL is used to communicate with Data Management Studio and with enterprise SOAP clients.

To access a Data Management Server using SSL, a SOAP client sends an HTTPS request to the server. At that point, the server negotiates with the client 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
- Configure Data Management Studio
- Configure Data Management Server
- Configure Federation Server
- Configure Authentication Server'
- Replace Passwords

Installation Notes

DataFlux Secure uses separate installation processes for the following clients and servers: Data Management Studio, Data Management Server, Federation Server, and Authentication Server. For each client or server, the installation process follows these steps:

1. Contact your sales representative and let them know you are interested in DataFlux Secure. DataFlux will explain the relevant legal restrictions and eligibility requirements.
2. Receive an updated license file that contains the DataFlux Secure software as well as instructions on how to obtain the installers.
3. As needed, install or update the DataFlux client or server software that will receive DataFlux Secure. This step must take place before you install DataFlux Secure.
4. Stop any active instances of Studio, Data Management Server, Federation Server, and Authentication Server.
5. Install DataFlux Secure on your clients and servers.
6. Replace your current license file with the new license file that you received from DataFlux.
7. On the host computers in the Windows operating environment that run the Data Management Studio, Data Management Server, or Authentication Server software, download the OpenSSL software.

   OpenSSL is available from several suppliers, any of which are suitable for use with DataFlux Secure. One such supplier can be found at this Web site:

   http://www.slproweb.com/products/Win32OpenSSL.html

   In the UNIX and Linux operating environments, OpenSSL is delivered with the kernel.
8. In the UNIX and Linux operating environments, for the Authentication Server and Federation Server, run the set_secure script. See the applicable configuration topics.
9. Configure SSL.

10. Start your clients and servers.

11. Replace existing passwords to store them with AES encryption.

Configure Data Management Studio

The DataFlux Secure software is required to be installed with Data Management Studio when that client connects to secured servers in the Data Management Platform. The secured servers at your site can include the Data Management Server, the Federation Server, and the Authentication Server.

After you install DataFlux Secure, as described in Installation Notes, Data Management Studio requires no additional configuration steps. DataFlux Secure is enabled when you start Data Management Studio.

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

Configure Data Management Server

When configured with DataFlux Secure, the Data Management Server uses AES encryption as needed to manage proprietary interprocess communication with the clients and servers of the Data Management Platform. To communicate with external clients, the Data Management Server uses SSL exclusively. Non-SSL communication is rejected.

After you install DataFlux Secure as described in Installation Notes, 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 option to enable SSL (required):

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

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

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
   ```

   Client authentication is required with SSL.

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 Data Management Server.

Configure Federation Server

After you install DataFlux Secure on a Federation Server, as described in Installation Notes, you configure DataFlux Secure on that server as follows.

If your Federation Server is installed on a Windows host, then the configuration process consists of starting or restarting the Federation Server. Starting the server activates the configuration options that were added when you installed DataFlux Secure.

If your Federation Server is installed on a UNIX or Linux host, then you first stop the Federation Server if it is running. Next, run the following script to set the value of the NetworkEncryptAlgorithm option to **AES**:

```
fed-server-install-dir/bin/set_secure aes
```

The former value of the NetworkEncryptAlgorithm option was SASPROPRIETARY.

Now start the Federation Server to enable DataFlux Secure.

Configure Authentication Server

Configure AES

After you install DataFlux Secure on an Authentication Server, as described in Installation Notes, you configure DataFlux Secure on that server as follows.

If your Authentication Server is installed on a Windows host, then the configuration process consists of starting or restarting the server. Starting the server activates the configuration options that were added when you installed DataFlux Secure.

If your Authentication Server is installed on a UNIX or Linux host, then you first stop the server if it is running. Next, run the following script to set the value of the NetworkEncryptAlgorithm option to **AES**:

```
fed-server-install-dir/bin/set_secure aes
```

The former value of the NetworkEncryptAlgorithm option was SASPROPRIETARY.

Configure SSL

After you configure AES, follow these steps to configure SSL on an Authentication Server:

1. Stop the Authentication Server if necessary.
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.

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 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 et 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/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. 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>
```

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.

When you replace passwords, you should enter the same passwords that were already in use. By doing so, you avoid having to update accounts in the operating environment.

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**.

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.

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.