DataFlux Authentication Server

DataFlux
A sas COMPANY

YOUR DATA.
YOUR BUSINESS.
ONE SOLUTION.

This page is intentionally blank

DataFlux
A SAS COMPANY

DataFlux Authentication Server

Administrator's Guide

Version 2.1

January 8, 2010

This page is intentionally blank

Contact DataFlux

Corporate Headquarters

DataFlux Corporation

940 NW Cary Parkway, Suite 201
Cary, NC 27513-2792
Toll Free Phone: 877-846-FLUX (3589)
Toll Free Fax: 877-769-FLUX (3589)
Local Phone: 1-919-447-3000
Local Fax: 919-447-3100
Web: http://www.dataflux.com

DataFlux United Kingdom

Enterprise House
1-2 Hatfields
London
SE1 9PG
Phone: +44 (0) 20 3176 0025

DataFlux Germany

In der Neckarhelle 162
69118 Heidelberg
Germany
Phone: +49 (0) 6221 4150

DataFlux France

Immeuble Danica B
21, avenue Georges Pompidou
Lyon Cedex 03
69486 Lyon
France
Phone: +33 (0) 4 72 91 31 42

Technical Support

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

Documentation Support

Email: docs@dataflux.com

Legal Information

DataFlux Legal Statements

Apache Portable Runtime License Disclosure

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 1.1

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.

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.

Tele Atlas North American Copyright Disclosure

Portions copyright © 2006 Tele Atlas North American, Inc. All rights reserved. This material is proprietary and the subject of copyright protection and other intellectual property rights owned by or licensed to Tele Atlas North America, Inc. The use of this material is subject to the terms of a license agreement. You will be held liable for any unauthorized copying or disclosure of this material.

USPS Copyright Disclosure

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

DataFlux 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.

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.

Table of Contents

Introduction

Conventions Used in this Document

This document uses several conventions for special terms and actions.

Typographical Conventions

The following typographical conventions are used in this document:

Typeface	Description
Bold	Text in bold signifies a button or action
italic	Identifies document and topic titles
`monospace`	Typeface used to indicate filenames, directory paths, and examples of code

Syntax Conventions

The following syntax conventions are used in this document:

Syntax	Description
[]	Brackets [] are used to indicate variable text, such as version numbers
#	The pound # sign at the beginning of example code indicates a comment that is not part of the code
>	The greater than symbol is used to show a browse path, for example **Start** > **Programs** > **DataFlux Data Management Studio** 1.0 > **Documentation**.

References

DataFlux Authentication Server User's Guide

DataFlux Data Management Studio User's Guide

DataFlux Data Management Server Administrator's Guide

DataFlux Data Management Server User's Guide

DataFlux Federation Server Administrator's Guide

DataFlux Federation Server User's Guide

DataFlux Expression Language Reference Guide

DataFlux Quality Knowledge Base Online Help

Overview

Purpose

The Authentication Server provides a central point of authentication management across multiple domains and multiple operating environments. Specific features include:

Centralized Authentication - the server accesses native authentication mechanisms, such as Windows Active Directory or LDAP, to verify the identity of the users of DataFlux client applications.

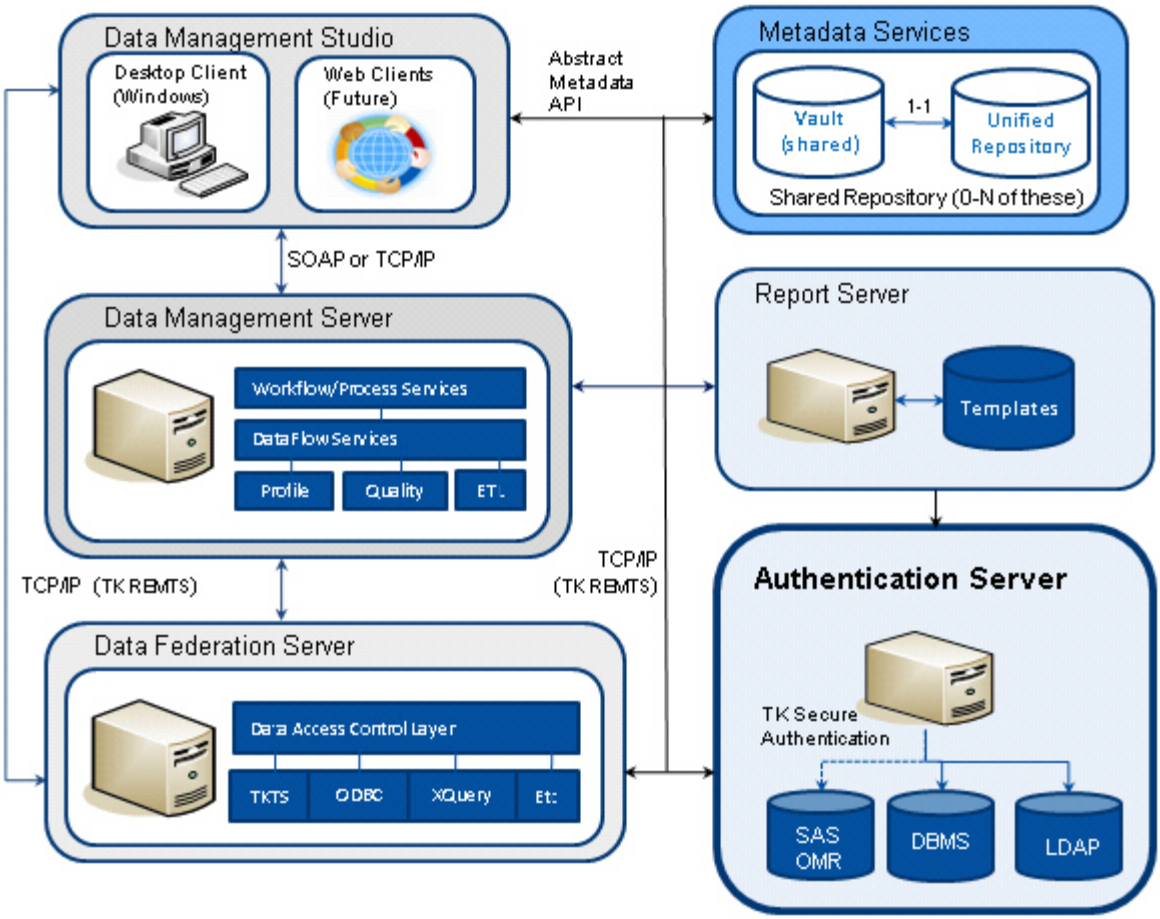
Centralized Management of Users and Groups - the server manages user and group definitions that form the basis for authorization on DataFlux servers.

Single or Reduced Sign-On - the server enables authenticated users to connect across domains to DataFlux servers and databases without submitting additional credentials.

Platform Architecture

The DataFlux Authentication Server is part of the DataFlux Data Management Platform. The platform provides centralized data access and data analysis for the data that is stored in DataFlux servers and databases across your enterprise, as shown in the following diagram:

The Authentication Server in the Data Management Platform



The DataFlux Authentication Server is required in all deployments that include a DataFlux Federation Server. Otherwise, the Authentication Server is optional. Your deployment may include more than one Authentication Server.

Authentication Servers are managed from the Administration riser in DataFlux Data Management Studio.

How it Works

Connect to a Federation Server

The following process describes how the Authentication Sever helps you connect to a Federation Server. After you connect to a Federation Server, you can open connections to databases.

1. An Administrator creates your user definition on Authentication Server and adds the user definition to groups and shared logins.
2. If necessary, you add to y our user definition a login for the domain of the Federation Server.

3. You open a connection to the Authentication Server. The Authentication Server authenticates your login. The Authentication Server sends a handle to Data Management Studio so that it can read the logins in your user definition.
4. You open a connection to the Federation Server.
5. Data Management Studio retrieves from the Authentication Server your login for the Federation Server domain.
6. Studio connects to the Federation Server using the login from the Authentication Server.
7. The Federation Server connects to Authentication Server using your login.
8. The Authentication Server authenticates the login and returns a handle to the Federation Server. At this point, you can open connections to databases.

 **Note:** If you connect to a Federation Server without first connecting to an Authentication Server, you are asked to supply credentials to the Federation Server.

Connect to a Database

After you connect to a Federation Server, you can open a connection to database using the following process:

1. You open a connection to a database.
2. The Federation Server uses your handle to retrieve from the Authentication Server a login to the database.

   Depending on the DSN configuration for that database, the login that is retrieved can be a personal login (from your user definition, for that domain), or a shared login (for which your user definition has been designated as a consumer).
3. The Federation Server uses the login from the Authentication Server to connect to the database, without asking you to enter another login.

System Requirements

Supported Operating Systems and Required Host Hardware

Operating System	Bits	OS Versions and Patches	Memory	Min. Disk Space*	CPU
AIX®	64	IBM® AIX 5.3 Technology Level 6 or AIX 6.1, with the runtime package `xlcpp.rte.10.1.0.aix.base`. Note that you can run the 32-bit system if required by third-party software.	96MB per concurrent user	694MB	Power CPU or RS64 architecture
HP-UX®	64	HP-UX 11i version 2 or 3, operating system release identifier `B.11.23` and above, with June 2007 patch bundle. If you authenticate with the Pluggable Authentication Module, install patches `PHCO_40361` and `PHCO_4036`, which make the Itanium patches 40360 and 40361 available on PA-RISC. Also install the Atomic APIs from the AtomicAPI optional software pack. See also Enable Streams on HP-UX.	96MB per concurrent user	793MB	PA-RISC 2.0
HP-UX Itanium® Processor Family Architecture	64	HP-UX 11i version 2 or 3, operating system release identifier `B.11.23` and above, with the June 2007 patch bundle and the `PHKL_36853` patch. If you authenticate with the Pluggable Authentication Module, install patches `PHCO_40360` and `PHCO_40361`. Also install the Atomic APIs from the AtomicAPI optional software pack. See also Enable Streams on HP-UX.	96MB per concurrent user	1063 MB	IA64-compliant
Red Hat Linux®	32 or 64	Red Hat Enterprise Linux 5.3, with version 2.6.11 or higher of the Linux kernel (see also the kernel information in the Red Hat Knowledge Base. Install all default packages. For x64, install both the 32-bit and 64-bit versions of the `libXp.so` library, which is included in the `libXp` package. Install the RPM package `compat□libstdc++□33□3.2.3□61`. The Unicode libraries depend upon the installation of a compatible standard C++ library, which is located in `/usr/lib/libstdc++.so.5` and/or `/usr/lib64/libstdc++.so.5`. The Native Posix Thread Library is supported. Linux threads are not supported. glibc 2.4 is required during the build.	64MB plus 8MB per concurrent user	722MB (32) or 784MB (64)	Pentium 4 or Xeon-class processors

SuSE Linux	32 or 64	Open SuSE 10.2 or 11.0 with version 2.6.11 or higher of the Linux kernel. SuSE 11.0 has better thread support. Install all default packages. For SuSE 10.2, install RPM package compat□libstdc++□5.0.7□22.2. The Unicode libraries depend upon the installation of a compatible standard C++ library, which is located in /usr/lib/libstdc++.so.5 and/or /usr/lib64/libstdc++.so.5. The Native Posix Thread Library is supported. Linux threads are not supported. glibc 2.4 is required during the build.	64MB plus 8MB per concurrent user	722MB (32) or 784MB (64)	Pentium 4 or Xeon-class processors
Solaris®	64	Solaris S64 or SAX, Version 9 or Version 10 Update 1 and higher, with patch 120037□09 for LDAP authentication.	96 MB per user	883MB	All that support Solaris 10 for x64, Intel 64, or AMD 64
Windows®	32 or 64	Microsoft® Windows® Server 2008 Standard Edition Microsoft® Windows® Server 2008 Enterprise Edition Microsoft® Windows® Server 2008 Datacenter Edition Microsoft® Windows® Server 2003, Standard Edition updated with Service Pack 1* Microsoft® Windows® Server 2003, Enterprise Edition updated with Service Pack 1* Microsoft® Windows® Server 2003, Datacenter Edition updated with Service Pack 1* * Install this update: http://www.microsoft.com/downloads/details.aspx?familyid=17c36612-632e-4c04-9382-987622ed1d64&displaylang=en. Microsoft® Windows® Server 2003 for x64 systems, Standard Edition Microsoft® Windows® Server 2003 for x64 systems, Enterprise Edition Microsoft® Windows® Server 2003 for x64 systems, Datacenter Edition Microsoft® Windows® XP Professional, updated with Service Pack 2 Microsoft® Windows® Vista □ Enterprise, Business, and Ultimate Editions Microsoft® Windows® XP Professional for x64 systems Microsoft® Windows® Vista for x64 systems □ Enterprise, Business, and Ultimate Editions	1GB plus 1GB swap space. For XP, 512MB plus 512MB swap space.	830MB	Pentium 4 or later

* An additional 30MB of disk space is required during installation for temporary storage.

Enable Streams on HP-UX

Follow these steps to ensure that Streams is installed and enabled on HP-UX:

1. The HP-UX Streams product is generally installed by default. Issue the following command to verify that Streams has been installed:
   ```
   /usr/sbin/swlist –l product | grep Streams
   ```
2. If necessary, install Streams from the HP-UX installation media. You will need tp log in as a Superuser.
3. To ensure that Streams is enabled, issue the following command
   ```
   /usr/sbin/kctune –v streampipes
   ```
4. If the current value of the `streampipes` variable is 1, then Streams is enabled and this procedure is complete.
5. If the current value is 0, issue the following command to change the `streampipes` variable:
   ```
   /usr/sbin/kctune streampipes=1
   ```
6. Restart HP-UX to enable Streams.

Oracle Database Prerequisites

Each Authentication Server maintains an authentication data store. The data store is located on the Authentication Server host by default. If you choose to do so, you can locate the authentication data store in an Oracle database. If you use Oracle to store your authentication data, please configure your Oracle database as directed in this section.

The Authentication Server has separate prerequisites for the native Oracle driver or for the Oracle ODBC driver.

Prerequisites for the Native Oracle Driver

In order to use the native Oracle driver to connect to the Oracle server, install the Oracle 10g R1 or R2 (10.1 and 10.2) client on the Authentication Server host.

If your Authentication Server runs in UNIX, then enter the following commands so that the Authentication Server can access shared libraries (also known as shared objects):

```
cd installation_directory/as/lib
cp tkeora10.so tkeora.so
```

Note: for Oracle 11, use `tkeora11` in place of `tkeora10`.

Note: for HP64, use `sl` in place of `so`.

In UNIX, to allow the Authentication Server to find the shared libraries, you need to set the ORACLE_HOME environment variable to the home directory of the native driver, then set a value for the LIBPATH environment variable to specify the path to the shared library directory:

```
setenv LIBPATH $ORACLE_HOME/lib:$LIBPATH
```

Prerequisites for the Oracle ODBC Driver

If you use the DataFlux ODBC Wire Protocol ODBC driver, then you are not required to install the Oracle client on the Authentication Server host.

In UNIX, to enable the Authentication Server to use shared libraries, first set one environment variable to identify the home directory of the ODBC driver. Next, set another environment variable to identify the path to the share libraries. Using the C shell, enter the command from the following list that applies to your operating system:

Linux
```
setenv LD_LIBRARY_PATH=$ODBCHOME/lib:$LD_LIBRARY_PATH
```

Solaris
```
setenv LD_LIBRARY_PATH $ODBCHOME/lib:${LD_LIBRARY_PATH}
```

AIX
```
setenv LIBPATH $ODBCHOME/lib:${LIBPATH}
```

HP/UX
```
setenv SHLIB_PATH $ODBCHOME/lib:${SHLIB_PATH}
```

In UNIX, to configure data sources, you may need to edit the file `.odbc.ini` in your home directory. If `.odbc.ini` is maintained at a central location at your site, then you need to set the path to that file in the environment variable ODBCINI.

Installing the Authentication Server

Windows

Follow these steps to install an Authentication Server on a host that runs the Windows operating system:

1. Download the DataFlux Authentication Server from the download section at http://www.dataflux.com/Customer-Care/.
2. In a DOC prompt or Run window, enter:
   ```
   df21-as-win32.exe
   ```
3. In the **Welcome** window, click **Next**.
4. In the **Select Additional Components** window, select the components you want to install, then click **Next**.
5. In the **Choose Destination Location** window, accept the default installation directory, or click **Browse** to choose a different directory, then click **Next**.
6. In the **Select Program Manager Group** window, accept the default Program Manager group or type a new group name, then click **Next**.
7. In the **Start Installation** window, click **Next** to begin the installation.The **Installing** window shows the progress of the installation. To cancel the installation, click **Cancel**.
8. In the **Installation Complete** window, click **Finish** to exit. If you want to view the Release Notes, click **View Release Notes**.

The default installation directory for the Authentication Server is:

```
C:\Program Files\DataFlux\Authentication Server\version
```

UNIX and Linux

Follow these steps to install an Authentication Server on a host that runs one of the supported versions of the UNIX or Linux operating systems. Supported operating systems are listed in the System Requirements.

1. Download the DataFlux Authentication Server from the download section at http://www.dataflux.com/Customer-Care/.
2. Copy the DataFlux Authentication Server installer and `README.txt` file that correspond to your operating system to an accessible directory.
3. At the command prompt, connect to the location where you are installing the Authentication Server.
4. Specify the directory where you will be installing Authentication Server, and navigate to that directory.
5. Enter the following command to uncompress the installation file.
   ```
   gzip -c -d auth-server-home/df21-as-operating-system.tar.gz | tar xvf -
   ```
6. Run the installer:
   ```
   perl as/install.pl
   ```

Configuring the Authentication Server

Configure Your License

Overview

A license file is provided when you install an Authentication Server. The license remains valid for one year after installation, with no service limits.

A message is written to the server log when the license expires.

DataFlux Data Management Studio automatically displays windows that help you track the status of your licenses.

Configure Your License in Windows

Follow these steps to configure your license file in Windows:

1. Obtain a Host ID by selecting **Start** > **Programs** > **DataFlux Authentication Server *version-number*** >**DataFlux Host ID**. Make note of the Host ID for future reference.
2. Contact your DataFlux representative and provide the Host ID to obtain your license file.
3. Save the license file on the Authentication Server host. The default license location is:
   `C:\Program Files\DataFlux\Authentication Server\`*`version`*`\etc\license`
4. If you changed the license file location during installation, the License option in the Authentication Server configuration file as_serv_aspsql.xml will display the new location. Save the license file to this location.

Configure Your License in UNIX

Follow these steps to configure your license file in UNIX:

1. To generate a Host ID, run the following command and write down the Host ID that is returned.
   ```
   /bin/lmhostid
   ```
2. Log onto the MyDataFlux Portal at http://www.dataflux.com/Customer-Care.
3. Click **Request License Unlock Codes** to open the License Request Form page.
4. Fill out the form and enter the Host ID.
5. When you receive your new license file, save it on the UNIX server in the `etc/license` directory. License files must have a `.lic` file name extension in order to be considered.

About the Authentication Server Configuration Files

The Authentication Server configuration files work with the options on the server invocation command to tailor the server to meet your needs. The options in the configuration files determine the server's operational parameters, such as authentication mechanisms and domains, administrative user IDs, log level, and encryption level.

The default server configuration is set during installation. The default configuration is fully operational. Default authentication uses the current authentication mechanism and domain of the server host.

Most of the configuration files are stored by default in `C:\Program Files\DataFlux\Authentication Server\`*version-number*`\etc`, or in a similar path in UNIX or Linux. Files with other locations are listed below.

It is recommended that you set authorizations to protect these files from general access, as described in Configure Authorizations in the Operating System

as_log.xml - defines the log level for the Authentication Server. The Authentication Server generates a log file by default. The default log file records user connections and server errors. You can configure the log file as needed to capture additional information, as described in Logging Events on the Authentication Server.

as_serv_aspsql.xml - defines values for the majority of the configuration options.

as_serv_aspsql_schema_trans.xml - when you install the Authentication Server, and when you choose to store your authentication data in the internal transactional database on the Authentication Server host, this file tells the server how to build the schema and tables of the authentication data store. This file is not intended to be edited.

as_serv_aspsql_schema_ora.xml - when you install the Authentication Server, and when you choose to store your authentication data in an Oracle database, and when you

specify the location of the Oracle database server using a path (rather than a ODBC DSN), this file tells the server how to build the schema and tables of the authentication data store. This file is not intended to be edited.

as_serv_aspsql_schema_odbc_ora.xml - when you install the Authentication Server, and when you choose to store your authentication data in an Oracle database, and when you specify the location of the Oracle database server using a an ODBC DSN (rather than a path), this file tells the server how to build the Oracle schema and tables of the authentication data store. This file is not intended to be edited.

as_serv_aspsql_scf.dat – optionally stores the Oracle credentials that are used by the Authentication Server to access authentication data when that data is stored in an Oracle database. If you use this file to store your Oracle credentials, set the values of the options CredentialsLocation and ConnectionString accordingly in the file as_serv_aspsql.xml. This file is stored by default in `C:\Program Files\DataFlux\Authentication Server\`*version-number*`\var`, or in a similar directory in UNIX or Linux.

sasauth.conf - configures the SASAUTH software on UNIX and Linux hosts, as described in Configure Authentication Mechanisms in UNIX and Linux. This file is stored by default in *auth-server-home*`/utilities/bin`.

Note that the `*.xml` configuration files are accompanied by `*.template` files, which are used as a reference to the default configuration.

If you edit a configuration file, you need to restart the Authentication Server to put your changes into effect.

Identify Administrators

Authentication Server administrators are authorized to add, edit, and delete most of the objects in the authentication data store. Administrators cannot read the passwords of users and shared logins.

Administrators are initially identified when you install an Authentication Server. The installer is the default administrator unless another individual is identified at that time.

After installation, you can add or delete administrators by editing the SystemUsers option in the as_serv_aspsql.xml configuration file.

Configure Encryption

By default, the DataFlux Authentication Server encrypts all of the data that is transferred between clients and the Authentication Server. You can change the default encryption level by changing the value of the Clientencryptionlevel option in the configuration file as_serv_aspsql.xml.You can choose between no encryption, login encryption, or all encryption.

The Authentication Server uses either SASProprietary encryption or AES encryption. SASProprietary is used by default. AES is optionally available from the DataFlux download section of the DataFlux Customer Care Portal, at http://www.dataflux.com/Customer-Care/.

The server's encryption algorithm is identified in the option NetworkEncryptAlgorithm option in the configuration file as_serv_aspsql.xml. Valid values are SASProprietary and AES. The value of the NetworkEncryptionAlgorithm option is set automatically when you install the Authentication Server.

If you install AES encryption on your Authentication Server, you also need to install AES security patches on the clients that connect to the Authentciation Server.

Configure Authorizations in the Operating System

The following tables recommend that you set read, write, and execute authorizations for certain users in certain directories. Deny directory access to all users other than those listed below.

Recommended Authorizations for Windows

Directories	User Role	Authorizations
DataFlux-home *DataFlux-home**Authentication Server*	Installer	Full control
	Process user	Read, execute, list folder contents
DataFlux-home\ *Authentication Server* *version*\var	Installer	Full control
	Process user	Read, execute, list folder contents
	Person who backs up the Authentication Server	Read, list folder contents

Recommended Authorizations for UNIX and Linux

Directories	User Role	Authorizations
DataFlux-home *DataFlux-home*/Authentication Server	Installer	Read, write execute
	Process user	Read, execute
DataFlux-home/Authentication Server /*version*/var	Installer	Read, write execute
	Process user	Read, write execute
	Person who backs up the Authentication Server	Read, execute

Configure Authentication

About Authentication

Authentication takes place when a client requests a connection to a DataFlux server (such as a Federation Server or Data Management Server). The client's default Authentication Server authenticates the user in the DataFlux server's domain, using the authentication mechanism that was specified for that domain. Successful authentication enables the client to establish a connection to the DataFlux server.

When an Authentication Server authenticates a client user, the authentication mechanism can be Active Directory, LDAP, Host, or PAM:

Active Directory - a Windows-based authentication mechanism.

LDAP - authenticates against an LDAP authentication provider, and can also enable UNIX and Linux servers to authenticate against a Windows authentication provider.

Host - authenticates using the host's default authentication mechanism.

PAM - a UNIX/Linux authentication mechanism that enables connections to LDAP and Active Directory authentication providers, including providers running in Windows.

About SIMPLE and SASAUTH

Authentication Severs running in UNIX or Linux can use the SIMPLE or SASAUTH programs to manage host authentication. Choose SIMPLE to use the default host authentication mechanism, without having to assign root authorizations to the SIMPLE process. Choose SASAUTH to use LDAP or PAM authentication, or to configure an ordered list of authentication mechanisms. The SASAUTH process requires root authorizations.

SASAUTH is used by default. You can also choose to define environment variables to configure Active Directory or LDAP authentication, without using SASAUTH or SIMPLE.

To select or to switch between SIMPLE and SASAUTH, see Select SIMPLE Authentication or SASAUTH Authentication.

Configure Authentication Mechanisms in Windows

Follow these steps to configuration an authentication mechanism when your Authentication Server is running in the Windows operating environment.

1. Open the configuration file as_serv_aspsql.xml.
2. Locate the AuthProviderDomain option set.
3. Enter the server's domain name and specify either ADIR, LDAP, or HOST as the authentication mechanism.
4. If the Authentication Server will authenticate in multiple domains, you can specify one unique domain for each of the three authentication mechanisms.
5. Use the SetEnv option set to specify environment variables for each authentication mechanism.
6. For ADIR, specify AD_HOST and AD_PORT.
7. For HOST, specify values for HOSTUSER_HOST and HOSTUSER_PORT.
8. For LDAP, specify values for LDAP_BASE, LDAP_HOST, and LDAP_PORT.
9. If users will authenticate with LDAP by sumitting user IDs rather than distinguished names, specify values for LDAP_PRIV_DN, and LDAP_PRIV_PW. These options are not needed if your LDAP server supports anonymous binds.
10. Save and close the configuration file.

Configure Authentication in UNIX and Linux

- Select SIMPLE or SASAUTH Authentication
- Configure SIMPLE Authentication
- Configure SASAUTH Authentication
- Configure SASAUTH for LDAP
- Configure SASAUTH for PAM

Select SIMPLE or SASAUTH Authentication

In UNIX and Linux, the DataFlux Authentication Server can use the SIMPLE or SASAUTH host authentication process, as described in About Authentication.

Follow these steps to select or to switch between SIMPLE and SASAUTH authentication:

1. If the Authentication Server is running, stop the Authentication Server.
2. To switch from SASAUTH to SIMPLE, execute `set_auth` as follows:

```
bin/set_auth simple
```

3. To switch from SIMPLE to SASAUTH, execute `set_auth` as follows:
```
bin/set_auth sasauth
```

4. Before you restart your Authentication Server, refer to one of the following topics:

   Configure SIMPLE Authentication
   Configure SASAUTH Authentication

5. Restart the Authentication Server.

Configure SIMPLE Authentication

After you run set_auth to select SIMPLE authentication, follow these steps to configure SIMPLE authentication:

1. Open the configuration file as_serv_aspsql.xml.
2. Locate the entries for the AuthProviderDomain option set.
3. Ensure that all UNIX and Linux domains specify only HOSTUSER as their authentication mechanism. Delete or replace any instances of LDAP or PAM.
4. Use the SetEnv option set to specify values for the environment variables HOSTUSER_HOST and HOSTUSER_PORT.
5. Save and close the configuration file.
6. Restart the Authentication Server.

Configure SASAUTH Authentication

You configure SASAUTH authentication after you select SASAUTH using set_auth.

Follow these steps to configure SASAUTH:

1. Open the configuration file as_serv_aspsql.xml.
2. Locate the entries for the AuthProviderDomain option set.
3. Ensure that all UNIX and Linux domains specify only HOSTUSER as their authentication mechanism.
4. Use the SetEnv option set to specify values for the environment variables HOSTUSER_HOST and HOSTUSER_PORT.
5. Save and close the configuration file as_server_aspsql.xml.

6. Set the owner of SASAUTH to `root`. This step is required so that SASAUTH can read encrypted passwords. On the command line, enter the following:

```
$ su root
# cd auth-server-home/lib/utilities/bin
# mv setuid/* .
# chown root sasauth
# chmod 4755 sasauth
# exit
```

7. Edit the configuration file *auth-server-home*`/lib/utilities/bin/sasauth.conf`.

8. For the variable `methods`, specify one authentication mechanism, or specify an ordered list of two or three authentication mechanisms, as shown in these examples:

```
methods=pw
```

or

```
methods=ldap pw
```

or

```
methods=pam ldap pw
```

Where:
`pw` - host authentication
`ldap` - LDAP authentication
`pam` - authentication using programmable authentication modules

When you specify multiple authentication mechanisms, SASAUTH attempts to authenticate with the first mechanism in the list. If authentication fails, then SASAUTH attempt to authenticate with the second mechanism, and so on with a third mechanism if one is specified, until authentication succeeds.

9. Activate and configure the SASAUTH log files by removing the comment character and inserting a path for the debug log, the access log, and the error log, as needed. Use the debug log only when testing or diagnosing errors. The default `logOwner` is `root`, and the default `debugNoPasswords` value is `true`, to prevent passwords from appearing in the debug log.

10. Set the parameters for the number of repeated authentication attempts by the user, in the values `maxtries`, `maxtriesPeriod`, and `maxtriesWait`. The default is 5 attempts in 60 seconds, following by a waiting period of 5 minutes.

11. If you specified `ldap` in the value of the `method` variable above, then configure the LDAP authentication method as described in Configure SASAUTH for LDAP.

12. If you specified `pam` in the value of the `method` variable above, then configure the PAM authentication method as described in Configure SASAUTH for PAM.

13. If you specified `pw` in the value of the method variable above, then there is no need for further configuration for that authentication mechanism.

14. Save and close the sasauth.conf configuration file.

Configure SASAUTH for LDAP Authentication

Follow these steps to configure LDAP authentication in UNIX or Linux.

Prerequisites for this procedure include the selection of SASAUTH with set_auth, and the initial configuration of SASAUTH.

1. In the configuration file: *auth-server-home*`/utilities/bin/sasauth.conf`, in the section entitled LDAP Configuration, specify the name of your LDAP server host for the variable LDAP_HOST.
2. If your LDAP server uses a specific port, enter the number of that port as the value of the variable LDAP_HOST_PORT.
3. For the variable LDAP_AUTH_METHOD, specify a value of BIND or MATCH. Choosing BIND is advantageous because that method does not write encrypted passwords into the sasauth.conf configuration file. BIND is less advantageous because that method does not capture bind failure information in the SASAUTH log files. Choose MATCH to capture bind failure information. MATCH is less advantageous because user-entered passwords and matching passwords from the LDAP server are stored in the sasauth.conf configuration file. If you specify MATCH, make sure that the sasauth.conf configuration file can be read only by the root user.
4. For the variables LDAP_HOST_DN and LDAP_HOST_PW, leave the default values (`"ldaplogin"` and `"ldappasswd"`) if you specified a value of BIND for LDAP_AUTH_METHOD. If you specified MATCH, replace the default values with the user ID and password of an administrative user. Administrative privileges are required to read passwords.
5. For the variable LDAP_SEARCHBASE, specify the domain containers in your LDAP tree that identify the starting point for your authentication searches. Note that SASAUTH expects user names in the form user@domain, as in steveb@stevesco.com.
6. For the variable LDAP_USERBASE, specify the location of the organizational unit that contains the names of your Data Management Studio users.
7. For the varialble LDAP_SCHEMA, retain the default value of RFC2307 or choose a value of AD2, AD3, or OTHER. Choose a value of OTHER if you want to define your own variables for attributes such as the user name, user ID, group ID, and password. To see the values that are applied for RFC2307, AD2, or AD3, see the values at the bottom of the sasauth.conf configuration file. You should not change the values of RFC2307, AD2, or AD3.
8. If you specified LDAP_SCHEMA= OTHER, specify new values for LDAP_USERNAME_ATTRIBUTE. LDAP_UID_ATTRIBUTE, LDAP_GID_ATTRIBUTE, and LDAP_PASSWD_ATTRBUTE. Also confirm the suitability of the other default values that are supplied for that group of variables in the configuration file.
9. If you need to configure PAM authentication, see Configure SASAUTH for PAM Authentication. Otherwise, save and close the sasauth.conf configuration file.

Configure SASAUTH for PAM Authentication

Configure PAM authentication in UNIX or Linux as follows.

Prerequisites for this procedure include the selection of SASAUTH with set_auth, and the initial configuration of SASAUTH.

On the Authentication Server, open the configuration file `/etc/pam.conf`. Add or edit the PAM authentication services that are used by SASAUTH. The services are specified in the following format:

```
service-name module-type control-flag module-path options
```

Examples for Solaris:

```
sasauth auth requisite pam_authtok_get.so.1
sasauth auth required pam_dhkeys.so.1
sasauth auth required pam_unix_auth.so.1
sasauth account required pam_unix_account.so.1
```

Examples for HP/UX:

```
Sasauth account required /usr/lib/security/$ISA/libpam_unix.so.1
Sasauth auth required /usr/lib/security/$ISA/libpam_unix.so.1
```

If your system uses PAM and LDAP, then your entries in pam.conf need to define your LDAP service. The `man` page for `/etc/pam.d` will help you determine the syntax of these entries.

Solaris Details

If your system uses PAM and LDAP on Solaris, then you need to configure PAM to communicate with your LDAP server with the `ldapclient(1m)` command. Refer to the ldapclient man page for more information.

The Solaris LDAP client does not treat numeric user names as user names. Instead, Solaris assumes that a user name that is numeric is actually a UID, and converts the user name directly to the UID instead of querying the LDAP database. Since Solaris recommends that user names begin with an alphabetic character, this is unlikely to change. If your site uses Solaris as an LDAP client, then user names in LDAP cannot be numeric.

AIX Details

On AIX, PAM is not activated by default. To activate PAM, refer to the IBM document *Security Guide – Authentication Module* (http://www16.boulder.ibm.com/pseries/en_US/aixbman/security/pam_overview).

IBM does not provide an LDAP module for PAM. The open source package OpenLDAP can be used to build an LDAP module, but this is not recommended for production environments since it is not a solution supported by IBM. Instead, sites that need LDAP authentication should configure the AIX system for LDAP authentication. Refer to the IBM Redbook

Integrating AIX into Heterogeneous LDAP Environments for instructions on how to configure AIX as an LDAP client.

Linux Details

For Linux, the directory `/etc/pam.d` contains one configuration file for each program that authenticates using PAM. The file `/etc/pam.d/sasauth` needs to contain entries in the following form:

```
module-type control-flag module-path options
```

For example, the file might contain the following entries:

```
#%PAM-1.0
auth sufficient pam_rootok.so
auth required pam_unix2.so nullok
account required pam_unix_acct.so
```

Configure Oracle to Store Authentication Data

Overview

When you install an Authentication Server, you can choose to locate the authentication data store on Oracle. During the install, you select an Oracle database server and a database driver. Two database drivers are available, one uses a path to access the database, the other uses an ODBC database source name (DSN) to access the database.

After installation you update the primary Authentication Server configuration file to register the location of the data store and configure the management of Oracle credentials.

If your Authentication Server runs in UNIX or Linux, and if you choose the ODBC driver, then you need to Configure ODBC in Unix or Linux.

Note that if you have two or more Authentication Servers, you can choose to configure them alike, so that the servers share a single authentication data store in Oracle.

Edit the Authentication Server Configuration File

After installation, edit the configuration file as_serv_aspsql.xml to record the name and path of the authentication data store in Oracle, and to configure the management of Oracle credentials.

1. Edit the Authentication Server configuration file shown in this Windows path:
   ```
   C:\Programs\DataFlux\Authentication Server\version-number\etc\as_serv_aspsql.xml
   ```
2. Enter the Oracle schema name that corresponds to your Oracle data store as the value of ASPSQL_SCHEMA.
   ```
   <!ENTITY ASPSQL_SCHEMA "oracle-schema-name">
   ```

3. Add the ASPSQL_ORAPATH tag to your configuration file. The value for ASPSQL_ORAPATH should be your Oracle path if you are using the Oracle driver or your ODBC DSN if you are using the ODBC driver.

```
<!ENTITY ASPSQL_ORAPATH "oracle-path-or-DSN">
```

4. Change the value of ASPSQL_CONFIG_DBMS SYSTEM to point to the appropriate Oracle configuration file. This configuration file tells the server how to create the tables in the Oracle data store.

```
<!ENTITY ASPSQL_CONFIG_DBMS SYSTEM "as_serv_aspsql_schema_ora.xml">
```

Or:

```
<!ENTITY ASPSQL_CONFIG_DBMS SYSTEM "as_serv_aspsql_schema_odbc_ora.xml">
```

5. If you plan to store Oracle credentials on disk, you can choose to add the credentials to a file. Or, if your site security policy forbids you to store Oracle credentials on disk, jump ahead to the next step.

   To add Oracle credentials to a file, add the ASPSQL_CREDENTIALS_LOC tag. to the configuraiton file:

```
<!ENTITY ASPSQL_CREDENTIALS_LOC "C:\Program Files\DataFlux\Authentication
Server\2.1\var\as_serv_aspsql_scf.dat">
```

   Be sure to use an absolute path rather than a relative path.

   DataFlux recommends that you keep the file in the `var` directory, because that directory is recommended to receive access restrictions in the operating environment, as specified in Configure Authorizations in the Operating System.

   Add Oracle credentials to the credentials file in the following format:

```
UID=myuser;PWD=mypwd
```

   The credentials in the file will be encrypted when you start or restart the Authentication Server.

6. To enter Oracle credentials manually, rather than storing them disk, use **Set Provider Credentials** or write a script that runs when you start the server. The script prompts you to enter credentials, which are maintained in memory until the server is restarted.

   To use **Tools ->** **Set Provider Credentials** in Data Management Studio to manually enter credentials, and to not save those credentials to disk, set a blank value for ASPSQL_CREDENTIALS_LOC, as follows:

```
<!ENTITY ASPSQL_CREDENTIALS_LOC "">
```

To use a script to capture Oracle credentials, set two environment variables in the script:

```
DFAS_PROVIDER_SOURCE_UID=my-Oracle-UID
DFAS_PROVIDER_SOURCE_PWD=my-Oracle-PWD
```

7. Regardless of how you manage Oracle credentials, set the following value in the configuration file:

```
<Option name="CredentialsLocation">&ASPSQL_CREDENTIALS_LOC;</Option>
```

8. Save and close the configuration file.
9. Start or restart the Authentication Server.

This completes the Oracle configuration process.

Example Configuration File

The following text illustrates a version of the as_serv_aspsql.xml configuration file that has been updated to configure the storage of authentication data in Oracle.

```
<?xml version="1.0"?>
<!DOCTYPE Config [
<!-- ASPSQL Provider DBMS independent content -->
<!ENTITY ASPSQL_CATALOG "AS">
<!ENTITY ASPSQL_CATALOG_QUALIFIER "&ASPSQL_CATALOG;.">
<!ENTITY ASPSQL_SCHEMA "TKTSTST5">
<!ENTITY ASPSQL_SCHEMA_QUALIFIER '"&ASPSQL_SCHEMA;".'>
<!ENTITY ASPSQL_BT_DOMAINS "DOMAINS">
<!ENTITY ASPSQL_BT_SUBJECTS "SUBJECTS">
<!ENTITY ASPSQL_BT_GROUPS "GROUPS">
<!ENTITY ASPSQL_BT_SUBJECT_GROUPS "SUBJECT_GROUPS">
<!ENTITY ASPSQL_BT_GROUP_GROUPS "GROUP_GROUPS">
<!ENTITY ASPSQL_BT_PRINCIPALS "PRINCIPALS">
<!ENTITY ASPSQL_BT_PRINCIPAL_MAPS "PRINCIPAL_MAPS">
<!ENTITY ASPSQL_BT_GROUP_MAP_MGRS "GROUP_MAP_MGRS">
<!ENTITY ASPSQL_BT_GROUP_MAP_USERS "GROUP_MAP_USERS">
<!ENTITY ASPSQL_BT_SUBJECT_MAP_MGRS "SUBJECT_MAP_MGRS">
<!ENTITY ASPSQL_BT_SUBJECT_MAP_USERS "SUBJECT_MAP_USERS">
<!ENTITY ASPSQL_BT_VERSION "VERSION">
<!ENTITY ASPSQL_BT_SENTINEL "SENTINEL">
<!-- ASPSQL Provider DBMS dependent content - Oracle -->
<!ENTITY ASPSQL_ORAPATH "TKTSORA">
<!ENTITY ASPSQL_CONFIG_DBMS SYSTEM "as_serv_aspsql_schema_ora.xml">
<!ENTITY ASPSQL_CREDENTIALS_LOC "C:\Program
Files\DataFlux\Authentication Server\2.1\var\as_serv_aspsql_scf.dat">
]>
<Config name="ASConfig">
<!-- Provider common elements -->
<!-- Port to listen on -->
<Option name="Port">21030</Option>
<!-- Provider common elements -->
<OptionSet name="SystemUsers">
<Option name="Account">DATAFLUX\admin1</Option>
<Option name="Account">DATAFLUX\admin2</Option>
</OptionSet>
<OptionSet name="SetEnv">
<Option name="FIREBIRD">C:\Program Files\DataFlux\Authentication
Server\2.1\lib\fbembed</Option>
```

```
<Option name="SAS_FB_FBEMBED">1</Option>
</OptionSet>
<OptionSet name="License">
<OptionSet name="Primary">
<Option name="Provider">DATAFLUX</Option>
<Option name="Location">C:\TableServer\license\license.lic</Option>
</OptionSet>
<OptionSet name="Secondary">
</OptionSet>
</OptionSet>
<Option name="NetworkEncryptAlgorithm">SASProprietary</Option>
<Option name="ObjectServerParms">CLIENTENCRYPTIONLEVEL=EVERYTHING</Option>
<!-- Provider name -->
<Option name="AuthenticationProvider">ASPSQL</Option>
<!-- Provider specific root element -->
<OptionSet name="ASPSQLProvider">
<!-- System catalog and schema names -->
<Option name="SystemCatalog">&ASPSQL_CATALOG;</Option>
<Option name="SystemSchema">&ASPSQL_SCHEMA;</Option>
<Option name="MinConnections">1</Option>
<Option name="MaxConnections">2</Option>
<Option name="CredentialsLocation">&ASPSQL_CREDENTIALS_LOC;</Option>
&ASPSQL_CONFIG_DBMS;
</OptionSet>
</Config>
```

Configure ODBC for Oracle in Unix or Linux

Follow these steps to configure your Oracle ODBC driver and define data sources.

1. Run the DataFlux ODBC Configuration tool:

   ```
   bin/dfdbconf
   ```

2. For the location of odbc.ini, enter:

   ```
   auth-server-home/etc/odbc.ini
   ```

3. For the location of the ODBC template file, enter:

   ```
   auth-server-home/etc/odbc.ini.template
   ```

4. Enter **A** to add a new data source.
5. In the **Available Templates** list, choose item **4**, **Oracle Wire Protocol [DataDirect 5.3 Oracle Wire Protocol]**.
6. Press **Enter** to choose default values for the initial data source parameters. At **Hostname**, enter the name of the host of the Oracle database server in the field.
7. Continue to accept default values, then enter a gateway system identifier in the **SID** field.
8. Accept the remaining default data source parameters.
9. Enter a name for the new data source.
10. Enter **X** to exit dbdfconf.

Administering the Authentication Server

Start or Stop the Authentication Server on Windows

Follow these steps to start or stop an Authentication Server on a Windows host.

1. On the Authentication Server host, click **Start** > **Settings** > **Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Computer Management**.
4. Expand the **Services and Applications** folder.
5. Double-click **Services**.
6. Right-click **DataFlux Authentication Server** and select **Stop** or **Start**. It is recommended that you ask all users to disconnect from the server before you stop it.

Start or Stop the Authentication Server on UNIX or Linux

To start or stop an Authentication Server on a host that runs UNIX or Linux, enter the following command:

```
./bin/asadmin start
```

The asadmin application accepts the following options:

start - starts the Authentication Server.

stop - stops the server.

status - displays the operational status of the server.

help - displays the options that supported by asadmin.

version - dsiplays version information for asadmin.

Backup and Restore the Authentication Server

Overview

To protect your data and executables, you need to back up your server files and your authentication data store. The data store is located in one of two places: on the Authentication Server host (internal database), or on an Oracle database.

Backup Server Files

To back up your Authentication Server executable files, stop the server and make copies of the following directories and subdirectories.

On Windows, copy the following directories or the equivalent directories at your site:

```
C:\Documents and Settings\admin-id\Application Data\DataFlux\AuthServer
```

Or, in Windows 7:

```
C:\Users\admin-id\Application Data\DataFlux\AuthServer
```

And:

```
C:\Programs\DataFlux\AuthenticationServer
```

On UNIX or Linux, copy the Authentication Server's home directory, and all of its contents.

Backup and Restore with GBAK

Use the GBAK tool to backup and restore the authentication data store in Windows, UNIX, or Linux. In Windows, GBAK is stored by default in the directory *auth-server-home*`\bin\fbembed`. In UNIX and Linux, the directory is *auth-server-home*`/lib/bin/fbembed`.

Backup and Restore an Internal Database

Backup command:

```
gbak -b internal-database backup-database -user SYSDBA -pas MASTERKEY
```

Example backup commands:

```
cd C:\Program Files\DataFlux\Authentication Server\2.1\var
..\bin\fbembed\gbak -b asdb.tdb C:\backup\asdb.tbk -user SYSDBA -pas MASTERKEY
```

Restore command

```
gbak -r internal-database backup-database -user SYSDBA -pas MASTERKEY
```

Example restore commands:

```
cd C:\Program Files\DataFlux\Authentication Server\2.1\var
..\bin\fbembed\gbak -r C:\backup\asdb.tbk C:\backup\asdb.tdb -user SYSDBA -pas
MASTERKEY
```

Backup and Restore an Oracle Database

If your authentication data store is located in Oracle, backup the following Oracle tables:

SUBJECT_GROUPS

GROUP_GROUPS

PRINCIPALS

GROUP_MAP_MGRS

GROUP_MAP_USERS

SUBJECT_MAP_MGRS

SUBJECT_MAP_USERS

VERSION

SENTINEL

PRINCIPAL_MAPS

GROUPS

SUBJECTS

DOMAINS

Administer Log Files

Overview

By default, the DataFlux Authentication Server records a selected set of events in a file that is stored on the local host. In Windows, the default path to the log file is:

```
C:\Program Files\DataFlux\Authentication
Server\version\var\log\as_%d_%S{pid}.log
```

Where *version* represents the software version, d becomes the date, S becomes the server hostname, and *pid* represents the process ID.

In UNIX and Linux, the default path to the log file is:

```
$DM_HOME$/DataFlux/DatatManagementPlatformversion/AuthenticationServer/var/log/
as_%d_%S{pid}.log
```

Log events and thresholds are specified in the log configuration file as_log.xml. In Windows, the default location of that file is:

```
C:\Program Files\DataFlux\Authentication Server\2.1\etc\as_log.xml
```

About Appenders and Loggers

As shown in the log configuration file as_log.xml, the default log configuration consists of one appender and nine loggers. The appender specify a log output destination. The loggers specify log event types and thresholds.

The RollingFileAppender is configured by default to generate a new log file each day and for each invocation of the Authentication Server.

Loggers define the log events that are monitored. Loggers also define a threshold level for each monitored log event. The threshold levels determine the amount of information that is recorded in the log for each event.

The following list of threshold levels is ordered from least-information at the top, to most-information at the bottom:

OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE
ALL

The default loggers and thresholds are defined in the following table.

Default Loggers and Thresholds

Logger	Description	Threshold
Cradle	records cradle messages	Info
DataFlux.licensing	records license checks	Warn
Admin	records administrative activity	Info
App	records messages from the Studio client	Info
Audit	records file reads, writes, and deletes	Info
IOM	records messages from other servers	Info
root	threshold applies to all unspecified log events	Error
App.TableServices. SQLDriver	INACTIVE, records database transactions, for use with tech support only	Trace
App.Statement.Statement. ExecDirect	INACTIVE, records statements input from Studio	Trace
App.Statement.Statement. Prepare	INACTIVE, records statements output to Studio	Trace

Note: the three inactive loggers should be enabled only when you are directed to do so by DataFlux technical support.

Change Log Events and Thresholds

The default log configuration captures most of the events that you will need to diagnose server problems. You can change the default log configuration at any time by changing log events and threshold levels. Log changes are generally used to help diagnose errors.

Note that if you opt to receive additional log messages, by using a threshold level of DEBUG, TRACE, or ALL, you may experience a reduction in server performance. In general, it is recommended that you not select a threshold below INFO when the server is operational in a production environment.

Also note that the logging facility can be adapted to use other appenders and loggers. Please contact DataFlux Technical Support for further information.

To disable a logger or change a logger's threshold level, follow these steps:

1. Open in a text editor the log configuration file as_log.xml.
2. To prevent any further collection of log events for a given logger, enclose the logger in comment tags, as in:

```
<!-- Administration message logger -->
 <!--<logger name="Admin"> -->
  <!--<level value="Info"/> -->
<!--</logger> -->
```

3. To change the threshold of a logger, replace the existing level value with OFF, FATAL, ERROR, WARN, INFO, DEBUG, TRACE,or ALL, as in:

```
<!-- Administration message logger -->
 <logger name="Admin">
  <!-- DEFAULT <level value="Info"/> -->
  <level value="Warn"/>
</logger>
```

4. Save and close the log file.
5. Restart the Authentication Server.

About Authentication Server Objects

Overview

Authentication objects are records in an authentication data store. Authentication objects include logins, domains, users, groups, and shared logins.

Authentication objects are created, displayed, edited, and deleted using the Administration riser in DataFlux Data Management Studio. To connect to an Authentication Server and see it's authentication objects, open the Administration riser, expand Authentication Servers, right-click a server, and select **Open**.

The number and type of authentication objects that you will be able to display depends on your role. Passwords cannot be seen or displayed by anyone. Administrators can add, edit, and delete all objects other than passwords, and can update the passwords of shared logins. Owners and managers of groups and shared logins can add and delete members. Users can see their logins. Everyone can see all users and groups.

DataFlux clients and servers query the authentication data store for user and group membership information. User and group information is used by the clients and servers to manage access to data and software features.

During operation, updates to authentication objects are immediately available to DataFlux clients and servers. Changes and deletions of authentication objects can result in changes to existing connections between DataFlux clients and DataFlux servers.

Each DataFlux Authentication Server generally maintains one complete authentication data store. The data store is generally located on the same host as the Authentication Server, and data is not shared between servers.

When you install an Authentication Server, you can choose to store authentication data in an Oracle database, as described in Configure Oracle as the Authentication Data Store. Using Oracle, you can define one database per Authentication Server, or you can configure more than one Authentication Server to share a single authentication data store in Oracle, with available TCP optimizations between servers.

Domains

A domain is named collection of logins that share an authentication mechanism. The Authentication Server defines domains so that Data Management Studio users can connect to DataFlux servers and database servers in those domains. The domains are associated with logins for authentication.

As an example of how domains are implemented, assume that you have a DataFlux Federation Server that runs on a Windows host in a domain named CHICAGO. To enable a DataFlux Data Management Studio user to connect to that server, you would follow these general steps:

1. You, the administrator, connect to an Authentication Server to create the CHICAGO domain, using the Domains riser. Use the same format that is used in Windows, such as CHICAGO/myLogin or us.ourcorp.chicago.com.
2. Identify the authentication mechanism of the CHICAGO domain in the Authentication Server's configuration file as_serv_aspsql.xml, as a added value for the option AuthProviderDomain.
3. The Studio user adds a CHICAGO login to his or her user definition.

At this point, the user can request a connection to the Federation Server, authenticate in the CHICAGO domain, and access data based on his or her user definition and group memberships.

When users add logins to a new domain, they can create no more than one login per domain for their one user definition.

If a Studio user logs in without a domain, a default domain is supplied. The default comes from the PrimaryProviderDomain option. If that value is not defined, then the default comes from the AutoAddDefaultDomain option. If that option has no value, then the Authentication Server uses host authentication.

Domains have properties that determine how they will be submitted for authentication. Domains can be defined as user-name only (userid), user-principal-name (userid@domain), or down-level (userid\domain). Additionally, domains can be case-sensitive (mixed-case), or case-insensitive (domain entries from users are converted to uppercase before authentication).

Logins

Logins consist of a combination of a user ID and a password. The Authentication Server works with three types of logins:

Inbound logins - are sent from Data Management Studio to the Authentication Server to verify the identity of the user when the user starts the Studio application or when the user connects to the Authentication Server. Inbound logins are also used to establish connections to DataFlux servers. When a Studio user requests a connection to a DataFlux server, the Authentication Server forwards that user's inbound login to the DataFlux server's domain for authentication. If the user authenticates successfully, the Authentication Server notifies the DataFlux server, and the DataFlux server accepts the connection.

Outbound logins - are submitted to database servers to validate the identity of the users whom request connections to those databases. Outbound logins are defined for each shared login. A shared login enables consumers (users or groups) to access the database using a shared database account. When a user requests a connection to a database server, the Authentication Server confirms that the user is a consumer, and sends the login to the client. The client sends the login to the database to establish the connection. The outbound login is not displayed to the user.

Oracle login - if you choose to locate your authentication data store in Oracle, the Authentication Server uses an outbound Oracle login to connect to that database, as described in Configure Oracle to Store Authentication Data.

Administrators define one initial inbound login when they create a new user definition. The user can then add unique logins to his or her user definition. A user definition can have no more than one login for each domain.

Administrators cannot display passwords and they cannot edit another user's logins. However, administrators can edit the outbound logins of shared logins, including the passwords.

Logins can be shared by multiple Authentication Servers if those servers share a single authentication data store in Oracle. Otherwise, each Authentication Server maintains a separate set of logins.

Users

User definitions, or simply "users", are objects that defined in the authentication data store. The object consists of a user name and a collection of one or more logins. Each login consists of a unique combination of a user ID and a domain.

A user can be added as a member of a group or added as a consumer of a shared login.

Groups

Groups are collections of users that form categories, often according to work role, such as Payroll, Accounting, and Human Resources. Groups are used to structure authorization to the jobs and data that are stored on DataFlux Federation Servers, Data Integration Servers, and Report Servers. The DataFlux servers query the Authentication Servers as needed to determine group membership.

Groups can be members of other groups.

Groups can be consumers of shared logins.

Groups can be managers of shared logins.

Each group has an owner. The group owner can edit the group definition, add and delete members, and assign a new owner.The owner is defined from the existing set of user definitions. A group is required to have an owner at all times

Administrators can add and delete groups, add and delete members, and reassign owners.

Shared Logins

Shared logins are collections of users and groups that use outbound logins to connect to database servers. When a Studio user requests a connection to a database, if that user is a *consumer* of a shared login for that database, then the Authentication Server sends the outbound login (database credentials) to the Studio client, and the client connects to the database. The Studio user sees no information about the outbound login.

Consumers of shared logins do not need individual accounts on the respective database servers.

The passwords for outbound logins cannot be displayed. Only administrators can update outbound logins.

Each shared login has a designated owner. The owner can add and delete consumers and shared login managers. The shared login owner can add, delete, and modify the outbound login and password. The owner can also change his login and reassign ownership to another user.

Users that are designated as managers can add and delete memberships in the shared login.

Appendix: Reference for as_serv_aspsql.xml

The options in the main Authentication Server configuration file, as_serv_aspsql.xml, are defined as follows.

In Windows, the default location of the file is:

```
C:\Programs\DataFlux\Authentication Server\version-
number\etc\as_serv_aspsql.xml
```

For information about other configuration files, see About the Authentication Server Configuration Files.

AppendEnv

```
<OptionSet name="AppendEnv">
 <Option name="your-variable">your-append-value</Option>
</OptionSet>
```

The AppendEnv option will find the indicated OS environment variable and append the option value to the end of the existing value. If the environment variable does not exist, then it will be created and set to the option value. The AppendEnv option will not add a delimiter of any sort between the existing and new environment variable value. If a semi-colon (;) is needed, then it must appear as the first character in the option value.

PrependEnv

```
<OptionSet name="PrependEnv">
 <Option name="your-variable">your-prepend-value</Option>
</OptionSet>
```

The PrependEnv option will find the indicated OS environment variable and prepend the option value to the beginning of the existing value. If the environment variable does not exist, it will be created and set to the option value. The PrependEnv option will not add a delimiter of any sort between the existing and new environment variable value. If a semi-colon (;) is needed, then it must appear as the last character in the option value.

SetEnv

```
<OptionSet name="SetEnv">
 <Option name="your-variable">your-value</Option>
</OptionSet>
```

The SetEnv option defines environment variables and assign values to those variables. Use this option to set environment variables that are required for Active Directory and LDAP authentication on the host of the Authentication Server. See AuthProviderDomain.

Port

```
<Option name=”Port”>21030</Option>
```

The Port option identifies the port that the server runs on. 21030 is the default value.

SystemUsers

```
<SystemUsers>
 <Option name="Account">domain\uid1</Option>
 <Option name="Account">domain\uid2</Option>
</SystemUsers>
```

The SystemUsers option defines administrative accounts for the Authentication Server. The user IDs must represent existing accounts in the specified domains.

License

```
<OptionSet name="License">
 <OptionSet name="Primary">
 <Option name="Provider">license-provider-name</Option>
 <Option name="Location">path-to-provider</Option>
  </OptionSet>
 <OptionSet name="Secondary">
 <Option name="Provider">license-provider-name</Option>
 <Option name="Location">path-to-provider</Option>
 </OptionSet>
 </OptionSet>
```

The License option provides information about the types of license checks that are performed by the Authentication Server. Provider choices include SAS and DATAFLUX. Both license methods may be enabled. One method will be identified as the primary license provider, while the other will be the secondary license provider.

AuthenticationProvider

```
<Option name=”AuthenticationProvider”>ASPSQL</Option>
```

The AuthenticationProvider option identifies the authentication process in the Authentication Server. The named process accesses the authentication data store. `ASPSQL` is the only valid value.

ASPSQLProvider

```
<OptionSet name=”ASPSQLProvider”>
 <Option name=”SystemCatalog”>AS</Option>
 <Option name=”SystemSchema”>”schema-name”</Option>
 <Option name=”MinConnections”>1</Option>
 <Option name=”MaxConnections”>4</Option>
 <Option name=”CredentialsLocation”>file-path</Option>
 <Option name=”ConnectionString”>connection-string</Option>
 </OptionSet>
```

The SystemCatalog option specifies the name of the catalog of the authentication data store.

The SystemSchema option specifies the name of the schema of the authentication data store.

The MinConnections option specifies the minimum number of connections to keep open to the authentication data store.

The MaxConnections option specifies the maximum number of connections to keep open to the authentication data store. In highly concurrent environments, this value should be raised.Generally speaking, a value of 4 should meet most needs.

The CredentialsLocation option specifies the location of the credentials file that is used to connect to the database that stores authentication data. This option is not required when you locate the autentication data store on the Authentication Server host. When you locate the data store on Oracle, this option can be used to store the encrypted credentials that the Authentication Server uses to connect to the authentication data store. If your site security policy forbids the storage of database credentials, you can enter credentials manually at server startup, or store the credentials in environment variables, as described in Configure Oracle to Store Authentication Data.

The ConnectionString option specifies the connection string to use to connect to the database that stores authentication data. If you locate your authentication data store on the Authentication Server host, the connection string is generated based on the specified location of the database file. When you locate the authentication data store in Oracle, this connection string contains Oracle connection information. The connection information is initially collected at install time. Oracle connections can consist of an ODBC DSN or a path.

ObjectServerParms

```
<Option name="ObjectServerParms">
 Clientencryptionlevel=everything
</Option>
```

The ObjectServerParms option specifies Authentication Server parameters. server parameters. Valid values include Clientencryptionlevel.

Clientencryptonlevel

The Clientencryptionlevel value is specified in the ObjectServerParms option. Valid values include:

none - nothing is encrypted.

credentials - login credentials are encrypted. These credentials are used to authenticate to the Authentication Server. This is the default value.

everything - encrypts all client-server communications.

NetworkEncryptAlgorithm

```
<Option name="NetworkEncryptAlgorithm">algorithm</Option>
```

The NetworkEncryptAlgorithm option specifies the encryption algorithm that is used to encrypt network data transfers between clients and the Authentication Server. Valid values for `algorithm` are SASProprietary and AES. AES encryption is available from the DataFlux customer portal. For more information, see Configure Encryption.

AuthProviderDomain

```
<OptionSet name="AuthProviderDomain">
 <Option name="provider-domain">domain-name</Option>
</OptionSet>
```

Or:

```
<Option name="AuthProviderDomain">provider-domain:domain-name</Option>
```

The AuthProviderDomain option associates authentication mechanisms with authentication domains. Authentication types are mapped to authentication providers (hosts) using environment variables, as described below.

You can associate a maximum of one authentication mechanism with one domain.

The `provider-domain` value determines the authentication mechanism. Valid values for *`provider-domain`* are:

ADIR. - .specifies that the authentication provider be a Microsoft Active Directory server that accepts a bind containing user names and passwords for authentication.

HOSTUSER - specifies that user names and passwords be authenticated by using the authentication processing that is provided by the host operating system.

LDAP - specifies that the authentication provider use a directory server to specify the bind distinguished name (BINDDN) and a password for authentication.

For the `domain-name`value, be sure to duplicate the capitalization of context-sensitive domains. If the domain name contains spaces, use quotation marks around the name.

The maximum length of the option values is 1,024 characters.

For UNIX and Linux domains, specify a provider-domain of HOSTUSER if you authenticate with SIMPLE or SASAUTH, as described in Configure SASAUTH Authentication in UNIX or Linux.

Set the following environment variables to identify authentication providers as required by your Authentication Server:

Microsoft Active Directory Server:

AD_HOST=*Microsoft-Active-Directory-host-name*

AD_PORT=*Microsoft-Active-Directory-port-number*

Host Authentication:

HOSTUSER_HOST=*host-name*

HOSTUSER_PORT=*port-number*

LDAP Server:

LDAP_BASE=*base-distinguished-name*

LDAP_HOST=*LDAP-host-name*

LDAP_PORT=*LDAP-port-number*

LDAP Server for users connecting with a user ID instead of a distinguished name (DN):

LDAP_PRIV_DN=*privileged-DN*

LDAP_PRIV_PW=*password-for-privileged-DN*

The *privileged-DN* needs to be authorized to search for users.

If the LDAP server allows anonymous binds, then LDAP_PRIV_DN and LDAP_PRIV_PW are not required.

To create the required environment variables, use the SetEnv option set, as shown:

```
<OptionSet name="SetEnv">
 <!-- specify a host for Active Directory authentication-->
 <Option name="AD_HOST"> myhost </Option>
 <Option name="AD_PORT"> myport </Option>

 <!-- specify a host for LDAP authentication -->
 <!-- BASE parameters are site-specific -->
 <Option name="LDAP_HOST"> myhost </Option>
 <Option name="LDAP_PORT"> myport </Option>
 <Option name="LDAP_BASE"> ou=myorgunit, o=myorg </Option>

 <!-- specify a host for host authentication -->
 <Option name="HOSTUSER_HOST"> myhost </Option>
 <Option name="HOSTUSER_pofg"> myport </Option>
</OptionSet>
```

PrimaryProviderDomain

```
<Option name="PrimaryProviderDomain">your-domain</Option>
```

The PrimaryProviderDomain option specifies the authentication provider that is used first by default.

If `your-domain` contains spaces, then enclose the name in quotation marks.

AutoAddDefaultDomain

```
 <Option name="AutoAddDefaultDomain"/>
```

The AutoAddDefaultDomain option specifies that you want to use the Authentication Server's host domain as the default domain. The default domain is applied if a client

authenticates without supplying a domain. When you specify this option, the server automatically creates an entry for it's host domain in the authentication data store.

The AutoAddDefaultDomain option is valid only if you set the PrimaryProviderDomain and AuthProviderDomain values as shown:

```
<Option name="AuthProviderDomain">HOSTUSER:auth-server-domain-name</Option>
<Option name="PrimaryProviderDomain">auth-server-domain-name</Option>
```

For example, if the domain of the Authentication Server was DATAFLUX, then the required option values would be:

```
<Option name="AuthProviderDomain">HOSTUSER:DATAFLUX</Option>
<Option name="PrimaryProviderDomain">DATAFLUX</Option>
```

The domain object that is created in the authentication data store receives attributes based on the following table:

Attributes of the Default Domain

	Authentication Server OS	
Domain Attribute	**Windows**	**UNIX and Linux**
Use as part of login	Yes	No
Logins are case-sensitive	No	Yes

Glossary

A

Active Directory

an authentication mechanism in the Windows operating environment, with LDAP-like directory services and DNS-based naming.

administrator

an individual who has been granted access to all authentication objects except for passwords in the configuration file as_server_aspsql.xml.

AES encryption

the advanced encryption standard is optionally available on Authentication Servers to encrypt specified network traffic using 256-bit keys.

authentication

the process of verifying the identity of an individual.

authentication data store

a database that contains definitions of domains, users, groups, and shared logins. The database is accessed by an Authentication Server.

authentication mechanism

a program that authenticates users who login to that mechanism's domain.

Authentication Server

a component of the Data Management Platform that provides a central location for the management of connections between the Data Management Studio client, the DataFlux Federation and Data Management Servers, and native database servers.

authorization

the process of determining which users have which permissions for which resources. The outcome of the authorization process is an authorization decision that either permits or denies a specific action on a specific resource, based on the requesting user's identity and group memberships.

C

consumer

a user or group who is allowed to use a shared login to connect to a database.

D

DNS

the Domain Name System uses authoritative servers to assign names in domains and sub-domains. DNS provides translation services between domain names and IP addresses.

domain

a collection of logins designated to be authenticated using the same or like authentication mechanism.

DSN

Database Source Names enable ODBC drivers to connect to data sources.

E

encryption
the act or process of converting data to a form that only the intended recipient can read or use.

G

group
an object in the authentication data store that represents a collection of users and other groups. A group can be a consumer and/or manager of a shared login.

H

host authentication
a process in which a server sends credentials to its host operating system for verification.

L

LDAP
the lightweight directory access protocol is used to access directories or folders. LDAP servers provide an authentication mechanism that can be accessed by Authentication Servers.

login
a DataFlux copy of information about an external account. Each login includes a user ID and belongs to one user or group. Most logins do not include a password.

M

manager
a user or group in the authentication data store that has been granted permission to add and delete consumers from a shared login.

member
a user or group who has been added to a group.

O

ODBC
The Open Database Connectivity Standard is an application programming interface that enables applications to access data from a variety of database management systems.

owner
a user in the authentication data store that has been given permission to add and delete the members of a group. Each group is required to have one and only one owner at all times.

P

PAM
in UNIX and Linux, programmable authentication modules in the operating environment enable authentication across a network.

PUBLIC

this default group, which cannot be edited, contains all users who have authenticated in the host environment of the Authentication Server, but do not have a user definition on the server.

pw

the default authentication mechanism in UNIX and Linux.

S

SASProprietary encryption

the default encryption algorithm for the Authentication Server.

shared login

an object in the authentication data store that associates a colleciton of users and groups with an outbound login that connects the consumers of that shared login to a databas server.

U

user

an object in the authentication data store that associates one or more logins with one individual. A user can be a member of a group, a consumer of a shared login, or be granted access on a DataFlux server.

user definition

same as user. This term is used to differentiate objects in the authentication data store from the individuals who run client applications.

USERS

a default group that includes all individuals who have a user definition and have logged in at least once.