

# DataFlux Authentication Server User's Guide



YOUR DATA.  
YOUR BUSINESS.  
ONE SOLUTION.



This page is intentionally blank



# DataFlux Authentication Server

## User's Guide

---

Version 3.1

July 12, 2012

This page is intentionally blank

# Contact DataFlux

## **DataFlux Corporate Headquarters**

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

## **DataFlux West**

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

## **Technical Support**

Phone: 1-919-531-9000  
Email: [techsupport@dataflux.com](mailto:techsupport@dataflux.com)  
Web: <http://dataflux.com/MyDataFlux-Portal.aspx>

## **Documentation Support**

Email: [docs@dataflux.com](mailto:docs@dataflux.com)

# Legal Information

Copyright © 1997 - 2012 DataFlux Corporation LLC, Cary, NC, USA. All Rights Reserved.

DataFlux and all other DataFlux Corporation LLC product or service names are registered trademarks or trademarks of, or licensed to, DataFlux Corporation LLC in the USA and other countries. ® indicates USA registration.

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

[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](mailto:apache@apache.org).
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

## **Boost Software License Disclosure**

Boost Software License - Version 1.0 - August 17, 2003

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

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

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

## **DataDirect Copyright Disclosure**

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

## **Expat Copyright Disclosure**

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

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

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

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

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

## **gSOAP Copyright Disclosure**

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

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

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

## **IBM Copyright Disclosure**

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

### **COPYRIGHT AND PERMISSION NOTICE**

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

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

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

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

## **Microsoft Copyright Disclosure**

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

## **Oracle Copyright Disclosure**

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

## **PCRE Copyright Disclosure**

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

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

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.



- Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

## **Red Hat Copyright Disclosure**

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

## **SAS Copyright Disclosure**

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

## **SQLite Copyright Disclosure**

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

## **Sun Microsystems Copyright Disclosure**

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

## **USPS Copyright Disclosure**

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

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

## **VMware**

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

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

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

## **Solutions and Accelerators Legal Statements**

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

## **Apache**

This product may contain software technology licensed from Apache.

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

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

See the License for the specific language governing permissions and limitations under the License.

## **Creative Commons Attribution**

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

## **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

<b>Introduction to DataFlux Documentation .....</b>	<b>1</b>
Accessibility .....	1
Audience for this Guide .....	1
Conventions Used In This Document .....	1
Reference Publications .....	2
<b>Overview of the Authentication Server.....</b>	<b>4</b>
<b>Using the Authentication Server.....</b>	<b>7</b>
Add, Edit, or Delete a Server Definition .....	7
Select a Default Server .....	7
Connect to an Authentication Server .....	8
Start, Stop, and Restart the Server.....	8
Access Limits in the Server Interface .....	9
<b>Managing Domains, Users, Groups, and Shared Logins .....</b>	<b>11</b>
About Domains .....	11
Manage Domains.....	12
About Users and Logins.....	12
Manage Users and Logins .....	13
About Groups.....	14
Manage Groups .....	14
About Shared Logins.....	15
Manage Shared Logins .....	16
<b>Glossary .....</b>	<b>17</b>



# Introduction to DataFlux Documentation

[Accessibility Features](#)

[Audience for This Document](#)

[Conventions Used in This Document](#)

[Reference Publications](#)

## Accessibility

The DataFlux Authentication Server 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](mailto:techsupport@dataflux.com).

## Audience for this Guide

Users of DataFlux Data Management Studio can use this guide to learn how to connect to an Authentication Server, display information on users, groups, domains, and shared logins, and manage the logins that are associated with their user definition.

Administrators of Authentication Servers can use this document to add, modify, and delete domains, users, groups, and shared logins. Administrators can also be introduced to server tasks, including installation, configuration, logging, and backup and restore. Administrative tasks are addressed in detail in the *DataFlux Authentication Server Administrator's Guide*.

Managers can use this document to learn how the Authentication Server provides a centralized gateway to network connectivity.

## 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:

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

## Path Conventions

In code examples in this document, the installation path of the Authentication Server is represented by the term *install-path*, as shown in this example:

```
install-path/bin/dasadmin start
```

The installation path depends on the operating environment.

### Windows XP

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

### Windows 7

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

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

### UNIX and Linux

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

The *instance-name* is specified when you install the Authentication Server. The default instance name is server1.

## Reference Publications

This document may reference other DataFlux publications including:

- DataFlux Authentication Server Administrator's Guide
- DataFlux Data Management Studio User's Guide
- DataFlux Data Management Studio Installation and Configuration Guide
- DataFlux Web 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 Secure Administrator's Guide
- DataFlux Drivers for ODBC and JDBC: User's Guide

DataFlux Expression Language Reference Guide  
DataFlux Quality Knowledge Base Online Help

Documentation provided with this software is located in the installation folder for DataFlux. For example, C:\Program Files\DataFlux\AuthServer\*instance-name*.

Many of the documents listed can be found on the MyDataFlux Portal at <http://www.dataflux.com/Resources/DataFlux-Resources/MyDataFlux-Portal.aspx> under **Documentation**.

# Overview of the Authentication Server

## Introducing the Authentication Server

The DataFlux Authentication Server acts as a central point of security for users of the Data Management Platform. By providing authentication services, the Authentication Server helps the users of Data Management Studio securely connect to database servers across your enterprise.

The Authentication Server maintains a database of users, groups, domains, logins, and shared logins. The data supports authentication as well as authorization. The server authenticates logins using your existing domains and authentication providers. Group data is queried by DataFlux Federation Servers and DataFlux Data Management Servers to authorize access to data, jobs, and services.

Shared logins are used by Federation Servers to enable users to access relational databases without needing to submit database credentials. This enables one user to create a schema for a database view, and another user to invoke that schema, while neither user needs to know the actual credentials that are used to connect to the relational database.

## Server User Interface

The Authentication Server is accessed from the DataFlux Data Management Studio application. You connect to Authentication Servers from the Administration riser.

After you connect to an Authentication Server, a new set of risers in the Studio client enable you to add logins to your user definition and to display accessible information for domains, users, groups, and shared logins.

If you are an administrator, you can read and write all objects by default except user logins and shared logins. Administrators can also update authentication objects using a script file and the ASBATCH utility, as described in the *DataFlux Authentication Server Administrator's Guide*.

If you are an owner of a group or shared login, you can add and delete users or change the change the outbound credentials of the shared login.

If you are a manager of a shared login, you can add and delete users and read the outbound credentials.

To disconnect from the Authentication Server user interface, click the **Close** icon in the tab at the top of the Studio client. Closing the connection restores the original risers.



## Server Network Deployment

You can install multiple Authentication Servers in your Data Management deployment, based on the terms of your software license. Each server maintains a distinct and separate authentication data store.

Each server can be configured to maintain an authentication data store in Oracle. The default is to maintain the data store on the Authentication Server host.

## Configuring DataFlux Secure

You can install the DataFlux Secure software with your Authentication Server to add 256-bit AES encryption, compliance with the Federal Information Processing Standard 140-2, and SSL protection for connections with non-platform clients and servers. After an administrator configures DataFlux Secure, the software runs transparently to increase security. For more information about DataFlux Secure, see the *DataFlux Secure Administrator's Guide*.

## About Administrators

The administrators of Authentication Servers are identified when the server is installed. After installation, a configuration file can be edited to add or delete administrators.

Administrator names are not stored in the Authentication Server database. Nor are administrators identified in any way in the server's graphical user interface in Data Management Studio.

## User Tasks

Users of DataFlux Data Management Studio perform the following Authentication Server tasks:

- Optionally select a default Authentication Server.
- Log in to the default Authentication Server at the invocation of the Studio client.
- Submit logins when connecting to Data Management Servers, Federation Servers, or your database servers.
- Add or change the logins that are associated with your user definition.
- Connect to an Authentication Server to display the user definition and memberships. If you are an owner or manager of groups or shared logins, you can add and delete members of groups and consumers of shared logins.

## Administrator Tasks

- Install the server.
- Configure the server.
- Start, stop, and restart the server.
- Add and maintain authentication objects.

- Back-up and restore authentication objects.
- Read and maintain log files.

## About Authentication

The Authentication Server manages the authentication of Data Management Studio users. When a Studio user requests a connection to a database server or a DataFlux server, the client sends a login to the Authentication Server. The Authentication Server sends the login to a designated authentication provider in the default domain, or in the domain that was supplied with the login. The authentication mechanism returns authentication success or failure.

The authentication providers that are used by the Authentication Server are the same providers that you use every day outside of the Data Management Platform. Using existing providers minimizes administration without decreasing security, while enabling access to authorized data, jobs, and services across your network.

The Authentication Server can communicate with a list of supported authentication providers in the Windows, UNIX, and Linux operating environments, as needed to support authentication for all users. For details, see the *DataFlux Authentication Server Administrator's Guide*.

# Using the Authentication Server

- [Add, Edit, or Delete a Server Definition](#)
- [Select a Default Server](#)
- [Connect to a Server](#)
- [Stop, Start, and Restart the Server](#)
- [Access Limits in the Server Interface](#)

For information on adding, editing, and deleting users, groups, domains, and shared logins, see [Managing Domains, Users, Groups, and Shared Logins](#).

## Add, Edit, or Delete a Server Definition

Follow these steps to add, edit, or delete a DataFlux Authentication Server definition in your instance of Data Management Studio. You need to add a server definition before you can choose a default server or connect to a server.

1. In Data Management Studio, expand the Administration riser. If you do not have an Administration riser, disconnect from your current Authentication Server. Click on the **X** icon in the file tab in the top left corner of the window.
2. In the Administration riser, to add a new server definition, right-click **Authentication Servers** and select **New**. Enter your personal name for the new server, along with a description, a server host name, and a port number.

The server host name needs to be fully qualified, with all of the domain information that is necessary for your local host to connect to the server. For example, if the local host is part of the same domain as the server host, then the server name might be d2251.us.myco.com.

3. To edit or delete an existing server definition, right-click the server definition in the Authentication Servers riser and select **Edit** or **Delete**.

## Select a Default Server

When you select a default Authentication Server, you will be prompted to log in when you start Data Management Studio. The log-in takes place before you connect to database servers.

Before you can select a default server, you must first create a [server definition](#).

To select a default server, right click the server definition in the Administration riser and select **Set as Default**.

You can also:

1. Click **Authentication Servers**

2. Select a server in the information pane.
3. Click the star symbol, which is entitled **Set the server as the default**.

## Connect to an Authentication Server

You connect to a DataFlux Authentication Server to view and edit the authentication data store that is maintained by that server.

To connect to an Authentication Server:

1. Expand the Authentication Servers riser.
2. Right-click the server name.
3. Select **Open**.
4. In the Login dialog, supply a user ID, domain, and password. Use either a login that has been associated with a user definition, or use a login that is valid on the Authentication Server host.

If you log in without a user definition, but with a host login, you can see all users, groups, and domains in that server's authentication data store.

If your login is associated with a user definition on that server, you can edit your logins in that user definition.

Other roles have different [access limits](#).

Before you can connect, you must first create a [server definition](#).

After you connect you will receive new risers: Domain, Users, Groups, and Shared Logins.

To disconnect from a server, click red **X** in the server tab in the top left corner.

## Start, Stop, and Restart the Server

In the Windows operating environment, administrators stop, start, and restart Authentication Servers using the Computer Management application, or by executing `services.msc`. In the UNIX and Linux environments, administrators control the server with the `asadmin` application. For further information on these tools, see the *DataFlux Authentication Server Administrator's Guide*.

## About License Checks

When you start an Authentication Server, the invocation process checks for valid licenses for all required and all optional software packages. For all packages except one, an expired license halts server invocation and writes error messages into the server log.

If your site uses DataFlux Secure, and if your license expires, the server will start and run with the default 56-bit encryption key. The server log file will receive entries that record the error.

Note that an expired AES encryption license will be problematic if the AES licenses have not expired on the Data Management Studio clients or on the DataFlux servers that communicate with the Authentication Server. The encryption types must be the same for the Authentication Server, the Studio clients, and the DataFlux servers.

## Access Limits in the Server Interface

When you open a connection to an Authentication Server, you gain access to the authentication data store that is maintained by that server. Your access to the authentication data store is determined by your role. Roles and access limits are defined as follows:

**Public** - this role represents Data Management Studio users who connect with a host login (without a user definition). Members of the public group can display all users, groups, and domains.

**Users** - represents all of the Studio users whose login is associated with a user definition. In addition to Public permissions, users can:

- add, edit, and delete their logins in their user definitions.
- display the consumers and managers of the shared logins to which the users have been added.

**Members of Groups** - consist of users and other groups, for the purpose of collective authorization to Federation Servers and Data Management Servers. Groups can also be managers of shared logins, to share administrative responsibilities between users.

The names of group members are displayed to all users. When a shared login is a member of a group, the consumers of that shared login are displayed only to Authentication Server administrators, the owner or managers of the shared login, or a member of a group that is the owner or a manager of the shared login.

**Owners of Groups** - each group receives one required owner. An owner is a user who has been granted the following permissions, in addition to those of the User role:

- add and delete members and owners of owned groups.
- display the Member of Groups tab for owned groups (in the group's information pane).
- display the Responsibilities tab for the users of owned groups (in the user's information pane).
- can reassign ownership to another user.

**Consumers of Shared Logins** - are users who are authorized to use an outbound login to connect to a relational database. The consumers of a shared login are displayed only to administrators, consumers, the owner of that shared login, and to the managers of that shared login.

**Owner of Shared Login** - each shared login requires one owner. An owner is a user with the following additional privileges:

- display the consumers and managers of the shared logins that are owned by that user.
- add and delete the consumers and managers of owned shared logins.
- display the Member of Shared Login tab for owned shared logins
- display the Responsibilities tab for the users of owned shared logins.

**Managers of Shared Login** - each shared login can have one or more managers. A manager is a user or group that has the following additional privileges:

- display the consumers and managers of managed shared logins
- add and delete consumers of managed shared logins.
- display the outbound login of the shared login.
- display the Responsibilities tab for the users of managed shared logins.

**Administrators** - are designated during the installation of the Authentication Server, and managed thereafter in a configuration file, as specified in the *Authentication Server Administrator's Guide*. Administrators have all available permissions to display, add, edit, and delete nearly every object in the authentication data store. Administrators cannot display passwords for users or shared logins. Administrators cannot, by default, add, remove, or update the logins that are associated with user definitions.

# Managing Domains, Users, Groups, and Shared Logins

- [About Domains](#)
- [Manage Domains](#)
- [About Users and Logins](#)
- [Manage Users and Logins](#)
- [About Groups](#)
- [Manage Groups](#)
- [About Shared Logins](#)
- [Manage Shared Logins](#)

## About Domains

For the purposes of the Authentication Server, domains are collections of servers and client applications that share an authentication mechanism. An authentication mechanism is a computer that runs a particular type of authentication software. In the native operating environment, if you have a user account in a given domain, then you can log in to gain access to your desktop. In the DataFlux Data Management Platform, you log in to gain access to a particular database server in a particular domain.

Administrators define domains in the authentication data store. The domains in the data store exactly match the domains in your existing network. Administrators use a configuration file to associate domains with authentication mechanisms, as described in the *DataFlux Authentication Server Administrator's Guide*.

When you, as a Data Management Studio user, request a connection to a server, or when you invoke your client, you submit a domain, user ID, and password. The Authentication Server sends these credentials to the specified authentication mechanism for the specified domain. If you successfully authenticate, then you either open the client or open a connection to the database server.

The Authentication Server can be configured to provide a default domain. The default domain enables users to authenticate with the authentication mechanism that supports the host of the Authentication Server, even if a domain is not provided by the user. The benefits of configuring a default domain include the ability for users to connect to the Authentication Server without having their login associated in advance with a user definition in the authentication data store. Another benefit is that users do not have to specify a domain to connect to database servers in the Authentication Server's domain.

To display, add, edit, and delete domains, see [Managing Domains](#).

# Manage Domains

Administrators can add, edit, and delete domains in the Domains riser. Users can display all domains.

To add a new domain, select All Domains in the Domains riser. In the All Domains pane, click **New Domain**.

To configure a new domain, administrators edit an Authentication Server configuration file to associate an authentication mechanism with that domain, as described in the configuration chapter of the *Authentication Server Administrator's Guide*.

To edit a domain, expand All Domains in the Domains Riser, right-click the domain, and select **Edit**.

To delete a domain, right-click in the Domains riser and select **Delete**. Any logins that include the deleted domain will be deleted from the authentication data store.

**Note:** before you delete a domain, you might want to check the logins in the Users riser to make note of the logins that include the domain that you intend to delete. You might need to replace these logins with others that include different domains.

## About Users and Logins

The term *user* refers to a user definition in an authentication data store. Users can be members of groups. Users can also be consumers of shared logins. A user consists of one or more logins.

A login is a combination of a user ID, domain, and password that enables a user to authenticate in the specified domain. Each login must represent a valid account in the specified domain on your network. Individuals can have one login for each domain that they need to access. That same individual can have additional logins within a single domain, with different user IDs, as needed for that individual to connect to database servers with [shared logins](#).

Each login on a particular Authentication Server must consist of a unique combination of user ID and domain.

If Data Management Studio users have selected a default Authentication Server, they submit a login when they start the Studio application. The default Authentication Server associates a user with that login. The server then manages subsequent authentications as the Studio user requests connections to DataFlux servers and database servers.

The passwords in the logins that are associated with users are not stored on the Authentication Server host. Nor are user passwords maintained by the Authentication Server. Instead, Studio users supply a password when they log in.

After a user definition has been created, and after the individual has connected to the Authentication Server, that individual can add logins to that user definition. Administrators cannot, by default, read, add, modify, or delete logins.



Administrators can be given permission to add or remove user logins, or to update passwords. This permissions should be granted only temporarily, and only as needed, and then removed, to prevent impersonation.

One method of accessing user logins is to assert the option `AdminLoginManagementPolicy` in an Authentication Server configuration file. A second method of accessing user logins is to grant access to the ASBATCH utility. The ASBATCH utility runs scripts that update the Authentication Server's database. Both of these methods are described in the *Authentication Server Administrator's Guide*.

The administrators of Authentication Servers are not identified with user definitions. Instead, administrators are specified when you install the server. After installation, you can add administrators by updating a configuration file, as discussed in the configuration chapter of the *Authentication Server Administrator's Guide*.

## Manage Users and Logins

Users and logins are managed from the Users riser.

Data Management Studio users who have connected to an Authentication Server can display all of the users and logins that have been defined on that server. (User passwords are not displayed or stored by the Authentication Server.) Users can edit their user definitions and display their memberships in groups and [shared logins](#).

Administrators can add, edit, and delete users. Administrators can add a login when they add users, but they cannot add, edit, or delete logins. Administrators can display the members of groups and the consumers of shared logins.

To add a new user, administrators expand the Users riser, right-click **All Users**, and select **New User**.

To edit an existing user, right-click the user in the Users riser and select **Edit User**.

To delete a user, right-click the user in the Users riser and select **Delete**. It is recommended that the individual named in the user definition close his or her connection before you delete the user. Also note that all of the user's memberships need to be deleted before you can delete the user. You may need to delete members, consumers, or managers, and reassign owners of groups or shared logins.

To display the logins that are associated with a user, expand All Users in the Users riser and click the user name. The logins are displayed in the information pane on the right.

To add a login to an existing user definition, the individual named in the user definition must have connected to the Authentication Server at least once. Right-click the user in the Users riser and select **New Login**.

# About Groups

Groups are collections of related users. Groups can be members of other groups, and groups can be consumers of shared logins. Groups can also be designated as managers of [shared logins](#).

Groups can be used to set data access permissions on DataFlux servers. When a user requests access to data on a DataFlux server, the DataFlux server (such as a Federation Server) queries the Authentication Server for that user's group membership information. If the user is a member of a group that has read or write access to the requested data, then the server grants the user access to that data.

For the purposes of authorization on DataFlux servers, groups that are members of other groups inherit the authorizations of their parent groups. For example, if a group B is a member of group A, then group B receives all of the authorizations of parent group A, along with other permissions that are unique to group B. Inheritance enables a structuring of groups, such that the largest groups have the fewest authorizations.

All groups are required to have a designated owner at all times. The owner is registered user who can add and delete members and reassign ownership. The owner can display all of the groups to which the owner's group is a member.

Two top-level groups, PUBLIC and USERS, are continuously maintained by the Authentication Server. The PUBLIC group includes all Data Management Studio users who successfully authenticate in the Authentication Server's host environment. PUBLIC users are not required to have a registered user definition on the Authentication Server. This all-inclusive group receives minimal access to data.

The USERS group is a member of the PUBLIC group. The USERS group consists of all PUBLIC users who do have user definitions on the Authentication Server. The USERS group inherits the minimal permissions of the PUBLIC group. Additionally, members of the USERS group can edit their user definitions and group memberships.

By default, members of the PUBLIC group are granted read access to the group membership information that is displayed in Data Management Studio. Administrators can remove read access by changing the value of the configuration option `PublicUserGroupManagementPolicy`. For further information, see the *DataFlux Authentication Server Administrator's Guide*.

# Manage Groups

Administrators can add, edit, and delete groups. Administrators can also add or delete members from a group, display group memberships, and reassign group owners. Group owners can also add or delete members in their groups, display user's memberships in other groups, display a list of owned groups, and reassign ownership. Users can display all members in all groups.

To add a new group, administrators open the Groups riser, click **All Groups** and click **New Groups**.

To edit a group (change the name, description, and owner), administrators expand All Groups in the Groups riser, right-click a group, and select **Edit**.

To delete a group, administrators right-click the group in the Groups riser and select **Delete**.

**Note:** deleting a group whose members are connected to servers can cause errors. It is recommended that you check the status of the members of the group before you delete that group.

To display the memberships of a group, you right-click the group in the Groups riser and select Membership. The Membership dialog displays the members of the group, the group's memberships in other groups, and the group's memberships in shared logins.

To add members, administrators and owners click the group in the Groups riser, then select **Add Members** in the information pane.

To delete a member, administrators and owners select the member in the group's information pane, then click the **X** icon.

To display a group's designations as a manager of shared logins, open the **Responsibilities** tab in the group's information pane.

To add or delete a group as a manager of a shared login, administrators and owners follow these steps:

1. Open the Shared Logins riser.
2. Expand **All Shared Logins**.
3. Click the shared login.
4. In the information pane, click the **Managers** tab.
5. To add a group as a manager, click **Add Managers** to display the Add Managers dialog.
6. To delete a group's manager designation, click the **Delete** icon.

## About Shared Logins

Shared logins enable consumers to connect to database servers and Federation Servers using an outbound login that is supplied by the Authentication Server. Consumers can be users or groups, but not other shared logins.

When a consumer attempts to connect to the server that is the target of the shared login, the Authentication Server first authenticates the consumer's inbound login. The Authentication Server then sends the outbound login to the consumer's instance of Data Management Studio. Data Management Studio uses the outbound login to connect to the database server or Federation Server.

Outbound logins are never displayed. Outbound logins are encrypted and stored in the authentication data store that is maintained by the Authentication Server. The default

encryption method uses 56-bit keys. Optional AES encryption uses 256-bit keys. Outbound logins are entered and edited only by administrators. For information on encryption, see the configuration chapter of the *Authentication Server Administrator's Guide*.

Each shared login has one owner. The owner is a user who was specified by the administrator who created the shared login. Owners can display, add, and delete the consumers and managers in their respective shared logins. Owners and administrators can reassign new owners, but owners cannot be deleted without reassignment. Owners cannot change the outbound login.

Managers are users who are added to shared logins so that they can display, add, and delete consumers. Managers cannot display a list of managers, add managers, reassign owners, or change the outbound login.

When administrators create shared logins, they have the option of defining a shared login key. The key is a character value that is used by DataFlux Federation Servers to specify the group of shared-login connections that are accepted by each Federation Server. The intent is to divide the shared login connections across the available Federation Servers. Administrators can display and edit shared login keys values.

## Manage Shared Logins

Administrators add and delete shared logins and the consumers of shared logins. Administrators can also read and replace the outbound login that is used to connect to the relational database, and replace the owner or managers.

The owner of a shared login can add and delete consumers, read and replace the outbound login, and specify a different user as owner. The owner can be designated as a user, not as a group.

The manager of a shared login can add and delete consumers, read the outbound login, and replace the manager. The manager can be designated as a user or as a group.

To add a new shared login, connect to the Authentication Server and expand the Shared Logins riser. Click the **New Shared Login** icon above the riser. Outbound logins need to represent valid accounts on the target data server.

To edit or delete a shared login, expand All Shared Logins, right-click a shared login, and select **Edit Shared Login** or **Delete**. Note that deleting a shared login does not terminate any ongoing connections that were established with the deleted shared login.

To add consumers, select a shared login in the Shared Logins riser. In the Information pane for that shared login, click **Add Consumers** or the **Delete** icon.

To display user memberships in groups and shared logins, select the **Membership** icon in the information pane.

To add and delete managers, click the **Managers** tab in the information pane.

# 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 collection of users and groups with an outbound login that connects the consumers of that shared login to a database 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.