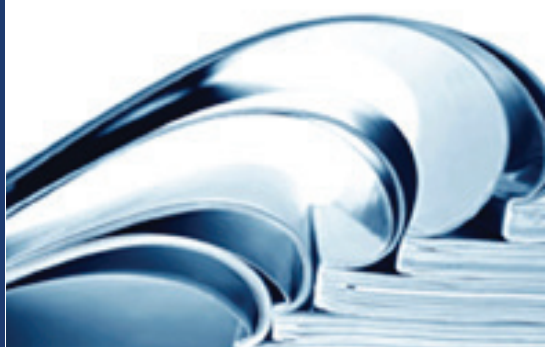
DataFlux Authentication Server

DataFlux
A sas COMPANY

YOUR DATA.
YOUR BUSINESS.
ONE SOLUTION.



This page is intentionally blank

DataFlux Authentication Server

User's Guide

Version 2.1.1

September 3, 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.

VMware

DataFlux Corporation LLC technical support service levels should not vary for products running in a VMware® virtual environment provided those products faithfully replicate the native hardware and provided the native hardware is one supported in the applicable DataFlux product documentation. All DataFlux technical support is provided under the terms of a written license agreement signed by the DataFlux customer.

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

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

Solutions and Accelerators Legal Statements

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

Apache

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.

This page left intentionally blank

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 Secure Administrator's Guide

DataFlux Expression Language Reference Guide

DataFlux Quality Knowledge Base Online Help

Overview

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 an authentication data store. The data store contains definitions of the domains, users, groups, and shared logins that are needed to support authentication.

The server responds to queries from Data Management Studio clients. The clients request user status information. The status information consists of the user's memberships and roles. For example, a given user could be the owner of a group and a manager of a shared login. The client needs the status information to determine the visibility of authentication data and the availability of administration features in the client.

The Authentication Server also supplies membership and role information to DataFlux servers such as the Federation Server. The DataFlux servers use the status information to authorize access to data and software features.

The authentication data store manages the following authentication objects:

Logins consist of a user ID, domain, and password, which together authenticate successfully in the specified domain.

Domains identify existing authentication domains in your network

Users consist of one or more logins, all of which define an individual.

Groups consist of a collection of users and other groups. Groups can be consumers of shared logins. Each group has a user who is the designated owner of that group. Owners can add and delete members and reassign ownership.

Shared Logins - consists of consumers (users and groups) and an outbound login. The outbound login allows consumers to connect to database servers. Shared logins have an owner and can have one or more managers. Managers are users that can add or delete consumers.

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 provide access to that server's domains, users, groups, and shared logins. Users that are designated as owners or managers can add and delete members for their respective groups and shared logins.

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.

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 data store. 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:

- Select a default Authentication Server.
- Log in to the default Authentication Server at the invocation of the Studio client.
- Submit logins to the server (transparently), when connecting to database servers.
- Connect to an Authentication Server to display the user definition and memberships. Users can also add logins to their user definition. Owners and managers 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 data.
- Back-up and restore the authentication data store.
- 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 mechanism in the database server's domain. The authentication mechanism returns authentication success or failure.

The authentication mechanisms that are used by the Authentication Server are the same mechanisms that are used every day outside of the Data Management Platform. Using existing user accounts and authentication mechanisms simplifies security in. and administration of, the Authentication Server. For example, if your computer runs in a Windows domain, your Windows login might be authentication by an instance of the Active Directory authentication mechanism. You would use that same login and mechanism to connect to a Federation Server in the same domain.

The Authentication Server can communicate with a list of supported authentication mechanisms in the Windows, UNIX, and Linux operating environments. For details, see the *Authentication Server Administrator's Guide*. Administrators configure one or more authentication mechanisms for each domain that is accessed as part of the Data Management deployment.

Using the Authentication Server

For information on adding, editing, and deleting users, groups, domains, ad 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. If the local
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 `asaadmin` 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 the optional AES encryption package, 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 - 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.

Owner of Group - 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).
- reassign ownership to another user.

Owner of Shared Login - each shared login has one required 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.

Manager 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.

Managing Domains, Users, Groups, and 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 has been created, and after the individual has connected to the Authentication Server, that individual can add logins to the respective user definition. Administrators can also add logins to existing user definitions.

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.

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.

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.

Manage Groups on the Authentication Server

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, and display a list of owned groups. 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, and 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, edit, and delete shared logins. Administrators add and delete the consumers of shared logins. Owners of shared logins add and delete consumers for the shared logins that they own.

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 colleciton 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.