THE POWER TO KNOW.

DataFlux® Authentication Server 4.1

Administrator's Guide

Second Edition

SAS® Documentation

Contact SAS

SAS Institute Inc.
100 SAS Campus Drive
Cary, NC 27513-2414, USA

Phone: 919-677-8000
Fax: 919-677-4444

SAS Technical Support

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

SAS Documentation Support

Email: yourturn@sas.com

Legal Notices

For additional legal notices, see Appendix 3.

Table of Contents

What's New in DataFlux Authentication Server 4.1 vi

Recommended Reading vii

Overview of DataFlux Authentication Server 1

Purpose 1

How to Use this Document 1

Architecture 3

How it Works 4

Export Domains, Logins, Users, and Groups to SAS Metadata Server 5

About the Export Process 5

Export Using SAS Deployment Wizard 7

Export Manually 9

Troubleshoot the Export Process 11

Configuring DataFlux Authentication Server 15

Upgrade Notes 15

Promote Server Content to a New Release 16

Add, Edit, or Delete a Server Definition 16

Select a Default Server 16

Connect to a Server 17

About the Server Configuration Files 17

Identify Administrators 18

Configure Encryption 19

Configure the Shared Login Manager on SAS Federation Server 19

Configure Authorizations in the Operating Environment 20

Configure Authentication Providers 20

Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins 30

Add a New Default Server 35

Administering DataFlux Authentication Server 37

Start or Stop a Server in Windows 37

Start, Stop, or Display Server Information in UNIX or Linux 37

Connect to a Server 38

Select a Default Server 39

Backup or Restore DataFlux Authentication Server 39

Administer Log Files 41

Administering Users, Groups, Domains, Logins, and Shared Logins 47

Overview 47

Use the Administration Riser 47

Access User Logins 48

Update in Batch with ASBATCH 49

About Users, Groups, Domains, Logins, and Shared Logins 62

Overview 62

Domains 63

Logins 63

Users 64

Groups 64

Shared Logins 65

Appendix 1: PROC ASEXPORT Syntax Reference 66

Overview: ASEXPORT Procedure 66

Concepts: ASEXPORT Procedure 66

Syntax: ASEXPORT Procedure 72

Appendix 2: Configuration File Reference 88

Appendix 3: Legal Notices 98

Glossary 103

What's New in DataFlux Authentication Server 4.1

Overview

The *DataFlux Authentication Server 4.1: Administrator's Guide, Second Edition* contains the following changes and enhancements:

- PROC ASEXPORT exports domains, logins, users, and groups to SAS Metadata Server.
- SASAUTH is now configured during installation in UNIX and Linux.
- Login management is now configured during installation.
- Server log entries can now be upgraded to include literal user names and metatadata IDs.

PROC ASEXPORT Exports User Definitions to SAS Metadata Server

A PROC ASEXPORT program and a validation program now run automatically under the direction of the SAS Deployment Wizard. The programs export domains, logins, users, and groups from DataFlux Authentication Server to SAS Metadata Server. You can run the programs manually after deployment. Further information is available in How to Use this Document and in Chapter 2.

SASAUTH Configured During Installation

The SASAUTH utility is now configured for host authentication by default during the installation of DataFlux Authentication Server. In previous releases, SASAUTH was configured after installation.

You can reconfigure SASAUTH authentication providers after installation.

Login Management Configured During Installation

The configuration option that configures login management for administrators is now set during installation. Administrators can add, delete, or update logins by default after installation. This permission can be rescinded by updating the value of the configuration option AdminLoginManagementPolicy.

Available Server Log Update for User and Group Names

By default, user and group log file messages identify the modified entities by metadata ID. You can now update your log configuration file to enable the addition of literal user and group names. See Upgrade Audit Log Messages to Include User and Group Names.

All of the documentation for DataFlux products is provided by SAS Customer Support, at the following locations:

- Documentation
- Install Center
- System Requirements

Recommended Reading

This document might reference other publications including:

DataFlux Data Management Studio: User's Guide
DataFlux Data Management Studio: Installation and Configuration Guide
DataFlux Data Management Server: Administrator's Guide
DataFlux Secure: Administrator's Guide
DataFlux Web Studio: User's Guide
DataFlux Web Studio: Installation and Configuration Guide
SAS Federation Server: Administrator's Guide
SAS Drivers for Federation Server: User's Guide

See also the Help for the preceding products and the Help for SAS Federation Server Manager.

For a complete list of SAS publications, go to support.sas.com/bookstore. If you have questions about which titles you need, please contact a SAS Publishing Sales Representative:

SAS Publishing Sales
SAS Campus Drive
Cary, NC 27513-2414
Telephone: 1-800-727-3228
Fax: 1-919-677-8166
E-mail: sasbook@sas.com
Web address: support.sas.com/bookstore

Overview of DataFlux Authentication Server

- Purpose
- How to Use This Document
- Architecture
- How it Works

Purpose

DataFlux Authentication Server provides a central point of support for authentication and authorization for data management products such as DataFlux Web Studio. Features include:

Centralized Authentication - DataFlux Authentication Server accesses native authentication providers, such as Windows Active Directory or LDAP, to verify the credentials of the users who create jobs, run jobs, administer servers, or access data collections.

Centralized Management of Users and Groups - DataFlux Authentication Server manages a database of domains, logins, users, groups, and shared logins.

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

How to Use this Document

The following table defines the chapters of this document apply to you, based on the release numbers of the DataFlux data management software. The table defines when authentication support shifts from DataFlux Authentication Server to SAS Metadata Server.

When all of your data management software supports the SAS Metadata Server, use Chapter 2 of this document only. Chapter 2 describes how to export domains, users, and groups from DataFlux Authentication Server to SAS Metadata Server.

Table 1 – How to Use this Document

If You Have...	Release	Use All Chapters Except Chapter 2	Use Chapter 2 Only	Use When...
DataFlux Data Management Studio	2.5 and earlier	•		
	2.6 and later		•	All DataFlux Authentication Server clients are migrating to SAS Metadata Server.
	2.6	•		Supporting SAS Federation Server 4.1 or earlier, or any release of DataFlux Web Studio.
	All	•		Supporting DataFlux Web Studio.
DataFlux Data Management Server	2.5 and earlier	•		
	2.6 and later		•	
DataFlux Web Studio	All	•		
SAS Federation Server	4.1 and earlier	•		
	4.2 and later		•	
SAS Business Data Network	3.0 and earlier	•		
	3.1 and later		•	
SAS Lineage	3.0 and earlier	•		
	3.1 and later		•	

Architecture

DataFlux Authentication Server works with your existing network authentication providers to validate submitted logins. Supported types of authentication include LDAP, Active Directory, and the host authentication providers in the Windows, UNIX, and Linux operating environments.

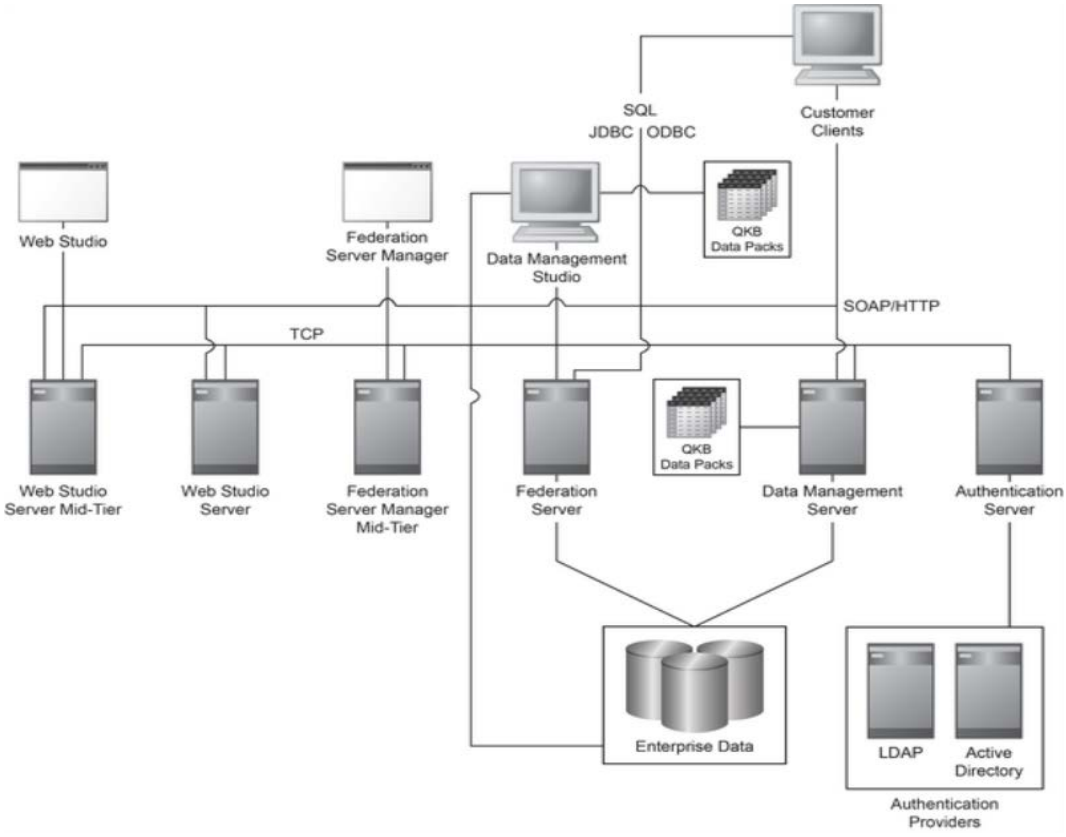
DataFlux Authentication Server maintains a transactional database that manages centralized definitions of users, groups, domains, logins, and shared logins. The transactional database resides by default on the server host. Users, groups, domains, logins, and shared logins can also be maintained in the Oracle relational database.

Shared logins are used by SAS Federation Server to provide restricted access to relational databases.

To support authorization, DataFlux Authentication Server provides group membership information to requesting data management software such as DataFlux Data Management Server.

The following diagram shows how DataFlux Authentication Server connects to clients and servers.

Recent releases of most DataFlux data management software replace support for DataFlux Authentication Server with support for SAS Metadata Server.



DataFlux Secure: Encryption, SSL, and FIPS Compliance

Starting with DataFlux Authentication Server 3.2, DataFlux Secure is installed by default. The additional security features that are provided by DataFlux Secure must be enabled after installation. The encryption algorithm SASProprietary is enabled by default. To enable enhanced security, you configure DataFlux Authentication Server as directed in the *DataFlux Secure: Administrator's Guide*.

DataFlux Secure provides the following features:

- 256-bit AES encryption for network traffic and password storage.
- Secure Sockets Layer protection for communication with SSL-enabled authentication providers.
- Optional compliance with Federal Information Processing Standard FIPS 140-2.

How it Works

Configuration, authentication, and authorization in DataFlux Authentication Server proceeds as follows.

After installation, administrators edit configuration files to accomplish the following tasks:

- identify administrators and trusted users.
- identify network authentication providers.
- configure security features.

After configuring the server, administrators use the Administration riser in DataFlux Data Management Studio.

Individual instances of data management products such as DataFlux Web Studio define a default DataFlux Authentication Server.

When a user is asked to authenticate, DataFlux Authentication Server passes the user's credentials to the specified network authentication provider and reports success or failure to the client.

Authorization is managed by individual data management products such as DataFlux Web Studio. The individual products maintain permissions for access to their respective jobs, data, commands, and services. To determine if an authenticated user is permitted access to a requested object, the application requests group membership information from DataFlux Authentication Server. Permission is granted if the user is authorized or if the user is a member of a group that is authorized.

In recent releases, SAS Metadata Server manages the preceding tasks.

Export Domains, Logins, Users, and Groups to SAS Metadata Server

- About the Export Process
- Export Using SAS Deployment Wizard
- Export Manually
- Troubleshoot the Export Process

About the Export Process

Introduction

The export process transfers domains, logins, users, and groups from DataFlux Authentication Server 4.1M1 or later to SAS Metadata Server 9.4M3 or later. When the export process has been validated, you can rely entirely on SAS Metadata Server for all of the services that were formerly provided by DataFlux Authentication Server.

During the installation of DataFlux Authentication Server 4.1M1, a new instance of the server software is created alongside the existing server. The new server instance is used to run the export process.

Why Export?

Exporting domains, logins, users, and groups to SAS Metadata Server consolidates SAS authentication processes and resources across your enterprise. Administrators can learn and use a single administrative application, SAS Management Console.

Only one SAS data management application requires the use of DataFlux Authentication Server in its latest release. All of the other SAS data management applications are configured by default during deployment to use SAS Metadata Server. To learn which releases apply to DataFlux Authentication Server, see How to Use this Document.

Export Manually or with SAS Deployment Wizard

The export process consists of a SAS export program and a SAS export validation program. The programs are either run manually in a SAS session, or they are run under the direction of the SAS Deployment Wizard.

The SAS Deployment Wizard runs the export and export validation programs in the following deployment scenarios:

- SAS Federation Server 4.1 to 4.2 (migration and upgrade-in-place scenarios)

- SAS Federation Server 3.2 to 4.2 (upgrade-in-place scenario only)
- DataFlux Data Management Server 2.6 to 2.7 (migration and upgrade-in-place scenarios)

For all other data management installation scenarios, you run the export process manually. To run the export and validation programs manually, see Export Manually.

To run the export process in SAS Deployment Wizard, see Export Using SAS Deployment Wizard.

Prerequisites

Meet the following prerequisites before running the export process:

- Install Foundation SAS on the host of DataFlux Authentication Server 4.1M1.
- Gather network host names and port numbers for SAS Metadata Server 9.4M3 or later, your previous instance of DataFlux Authentication Server, and DataFlux Authentication Server 4.1M1.
- Obtain an administrator user ID and password for SAS Metadata Server.
- Obtain a user ID and password that will authenticate on the local domain of DataFlux Data Management Server 4.1M1.

Possible Manual Assignment of Group Memberships

All domains, logins, users, and groups should be exported in the initial run of the export process. Completing the export process in a single run ensures that group memberships are properly affiliated in SAS Metadata Server. If you need to run the export process a second time, then you will have to manually assign group memberships on SAS Metadata Server for any users and groups that were added in the initial run.

To examine user profiles in SAS Metadata Server, use SAS Management Console.

How the Export Process Matches Users

The export process attempts to match the user IDs in the logins from DataFlux Authentication Server to the user IDs in SAS Metadata Server. Domains are matched between DataFlux Authentication Server's Domain object and the domains in the logins on SAS Metadata Server. If a match is found for user IDs and domains, then any new logins or group memberships are added to the matching user profile.

Nothing is changed in the original user profile in SAS Metadata Server.

If a match is not found, then a new user account is added to SAS Metadata Server.

About Shared Logins

Shared logins are not exported. Shared logins are used by SAS Federation Server to access relational databases. Shared logins on DataFlux Authentication Server need to

be manually replicated on SAS Metadata Server. To create shared login accounts on SAS Metadata Server, see the *SAS Federation Server Manager: User's Guide*.

About PROC ASEXPORT

The export process is implemented in PROC ASEXPORT. For syntax information regarding this procedure, see Appendix 1: PROC ASEXPORT Syntax Reference.

Export Using SAS Deployment Wizard

The SAS Deployment Wizard prompts you through the export process when you are deploying a supported data management product. Supported products are listed in Export Manually or with SAS Deployment Wizard.

Meet the prerequisites before you run the export process.

After you run the export process, the export validation program updates one of the following files. The content of the file is displayed by SAS Deployment Wizard:

```
<configuration-
directory>\Lev[n]\Documents\Instructions.html
```

or:

```
<configuration-
directory>\Lev[n]\Documents\UpdateInstructions.html
```

Any export errors are logged and recorded in a separate export validation results list.

If you need to resolve errors, you probably need to run the export program and the export validation program again to complete the export process. To run the programs manually, see Export Manually.

Review the Export Validation Result List

If the export process ran without errors, then the export validation result list indicates success. If errors were logged, then SAS Deployment Wizard refers you to the following export validation result list:

```
<configuration-directory>\Lev[n]\Logs\Configure\
   dfauthsvrc_acproc.validation_result.txt
```

The list indicates all domains, logins, users, and groups that were not exported, as shown in the following example:

```
Unexported logins          12:05 Monday, December 21, 2015   4

AS_USER_ID                          AS_FQLN_N
------------------------------------------------------------------
000E23E689C85E11E9DF0005650AA5E1  demouser
0002F6DFA33A5E115B020005650AA5E1  test010
00020C8C76985E11D8F40005650AA5E1  test011
```

Review the Export Log

Each time it is run, the export program generates a separate log file of the form `dfauthsvrc_updateConfigure_<datetime-stamp>.log`. The log is stored in the following location:

> *<configuration-directory>*\Lev[*n*]\Logs\Configure\dfauthsvrc_asproc.result.log

To resolve common errors in the log, see Troubleshoot the Export Process.

Export Again, After Export Using SAS Deployment Wizard

After you run the export process in SAS Deployment Wizard, and after you resolve errors, follow these steps to run the export process manually:

1. On the host of DataFlux Authentication Server 4.1M1, confirm or set the following environment variables:

    a. In UNIX or Linux, open a shell and enter the following:

    ```
    export metapasesword=sas-metadata-server-admin-password

    export aspassword=dataflux-authentication-server-admin-password
    ```

    a. In Windows, open a command shell and enter the following:

    ```
    set metapassword=sas-metadata-server-admin-password

    set aspassword=dataflux-authentication-server-admin-password
    ```

2. Run the following export program:
   <install-path>\SASHome\DataFluxAuthenticationServer*<version-number>*\authserver\data\install\Config\dfauthsvrc\Deployment\Metadata\asexport_default.sas

3. In the same directory, run the export validation program asexport_default_validation.sas.

4. Review the Export Validation Result List:
   <*configuration-directory*>\Lev[n]\Logs\Configure\
   dfauthsvrc_acproc.validation_result.txt

5. In the same directory, review the export log dfauthsvrc_asproc.result.log.

Export Manually

Follow these steps to run the export process manually, without using SAS Deployment Wizard.

To see a list of data management software upgrades that can run the export process using SAS Deployment Wizard, see Export Manually or with SAS Deployment Wizard.

Meet the prerequisites before you run the manual export process.

1. On the host of DataFlux Authentication Server 4.1M1, download the export program and the export validation program using SAS Note 58881.

   Store the downloaded files asexport_default.sas.orig and asexport_default_validate.sas.orig in the following location:

   <*install-path*>\SASHome\DataFluxAuthenticationServer\<*version-number*>\authserver\data\install\Config\dfauthsvrc\Deployment\Metadata

2. If the newly installed DataFlux Authentication Server 4.1M1 or later is running, issue the following stop command: DataFlux Authentication Server:

   <*install-path*>\SASHome\DataFluxAuthenticationServer\<*version-number*>\authserver\bin\dasadmin stop

3. Change to the directory <*install-path*>\etc\. Back-up the file as_serv_aspsql.xml by copying it to as_serv_aspsql.xml.bak.

4. Edit the configuration file as_serv_aspsql.xml. In the file, locate the SystemUser and TrustedUser option sets. As needed, copy the SystemUser value and paste that value as a new option of the TrustedUser option set, as shown:

   ```
   <OptionSet name="TrustedUsers">
   <Option name="Account">domain\trusted-user</Option>
   <Option name="Account">domain\system-user</Option>
   </OptionSet>
   ```

5. Start DataFlux Authentication Server using the following command:
   <*install-path*>\SASHome\DataFluxAuthenticationServer\
   <*version-number*>\authserver\bin\dasadmin start

6. Change to the following directory:
   <*install-path*>\SASHome\DataFluxAuthenticationServer\<*version-number*>\authserver\data\install\Config\dfauthsvrc\Deployment\Metadata

7. Edit the file asexport_default.sas.orig. Save the file to the new filename asexport_default.sas.

8. In the program file, set the values in the asexport macro as follows:

    a. Specify the hostname or network IP address of SAS Metadata Server:
    ```
    meta_server=my-sas-metadata-server.domain.com,
    ```

    b. Specify the administrator user ID of SAS Metadata Server:
    ```
    meta_user=userid,
    ```

    c. Enter or verify the following token:
    ```
    meta_password=%nrbquote(%sysget(metapassword)),
    ```

    This token will obtain the administrator password for SAS Metadata Server from an environment variable. You will create the environment variable in a subsequent step.

    d. Confirm or change the default port number for SAS Metadata Server:
    ```
    meta_port=8561,
    ```

    e. Specify the hostname or network IP address of your newly installed DataFlux Authentication Server:
    ```
    as_server=localhost,
    ```

    or

    ```
    as_server=my-new-df-auth-server.domain.com,
    ```

    f. Specify the administrative user ID of the previous instance of DataFlux Authentication Server:
    ```
    as_user=userid,
    ```

    g. Enter or verify the following token:
    ```
    as_password=%nrbquote(%sysget(aspassword)),
    ```

    This token will specify the administrator password for DataFlux Authentication Server.

    h. Confirm or change the default port number of your newly installed DataFlux Authentication Server:
    ```
    as_port=21030,
    ```

    i. Set the hostname or network IP address of the previous instance of DataFlux Authentication Server (from which you will export domains, logins, users, and groups):

    ```
    as_server_src=my-previous-authentication-server.domain.com,
    ```

    j. Confirm or change the default port number of the previous instance of DataFlux Authentication Server:
    ```
    as_port_src=21030,
    ```

k. Save and close asexport_default.sas.

9. To specify environment variables for administrator passwords, follow these steps:

   a. In UNIX or Linux, open a shell and enter the following:
      ```
      export metapassword=sas-metadata-server-admin-password
      export aspassword=dataflux-authentication-server-admin-password
      ```

   b. In Windows, open a command shell and enter the following:
      ```
      set metapassword=sas-metadata-server-admin-password
      set aspassword=dataflux-authentication-server-admin-password
      ```

10. In the shell, start a SAS session. Run asexport_default.sas and check the SAS log.

11. In a text editor, open the following export validation program:
    ```
    <install-path>\SASHome\DataFluxAuthenticationServer\<version-number>\authserver\data\install\Config\dfauthsvrc\Deployment\Metadata\asexport_default_validate.sas.orig
    ```

12. Save the file as asexport_default_validate.sas.

13. In the program file, edit the values in the asexport macro to match the values in asexport_default.sas. Save and close asexport_default_validate.sas.

14. In SAS, run asexport_validate.sas.

15. Review the Export Validation Result List. The list either indicates that the export is complete, or it lists all objects that were not exported:
    ```
    <configuration-directory>\Lev[n]\Logs\Configure\dfauthsvrc_acproc.validation_result.txt
    ```

16. In the same directory, review the export log dfauthsvrc_asproc.result.log.

17. As needed, resolve any export errors, then run the manual export process again to confirm that the export is complete.

18. Stop DataFlux Authentication Server. In <*install-path*>\etc\, delete or rename as_serv_aspsql.xml. Rename as_serv_aspqsl.xml.bak to as_serv_aspsql.xml. Start DataFlux Authentication Server.

Troubleshoot the Export Process

The following table provides resolutions for common export errors.

Log Entry	Possible Cause	Resolution

A problem was encountered while initializing the install for: DataFlux Authentication Server
 	
LOG: SEVERE: Install Status: -1000 Sep 02, 2015 6:48:45 PM com.sas.ssn.Chaining install SEVERE: Install failure for: DataFlux Authentication Server Sep 02, 2015 6:48:45 PM com.sas.ssn.Chaining install
	The SAS deployment installation is failing when the program tries to extract a tar file, because the sasauth file is owned by root, not the installer ID.	When you see this message, do not dismiss the Install Failure dialog box. Take the following steps:
		
		1. Stop DataFlux Authentication Server process.
		
		2. Change the ownership of the file to the install user:
		
		`cd <SASHome>\DataFluxAuthenticationServer\4.1\authserver\lib`
		`su`
		`mv sasauth sasauth.root`
		`exit` *(back to your SAS installer ID)*
		`cp -f sasauth.root sasauth`
		
		3. Click **Retry** in the error dialog box in SAS Deployment Wizard to continue.
		
		SAS Deployment Wizard should install DataFlux Authentication Server successfully and should proceed with the next step in the deployment process.

Execute failed: java.io.IOException: Cannot run program "${sas.exec.file}" : CreateProcess error=2, The system cannot find the file specified. Check to make sure that SAS Foundation is installed on the system.	SAS Foundation, also referred to as Base SAS, is not installed with DataFlux Authentication Server.	You should install Base SAS 9.4M3 or later, with all of the associated hotfixes. • For a migration, install SAS Foundation where DataFlux Authentication Server resides on the target machine. • For an upgrade, install SAS Foundation on the source machine where DataFlux Authentication Server is installed.
ERROR: The requested method can only be	System user not defined as trusted user, or administrator permissions not granted to account	Open as_server_aspsql.xml or as_serv_aspsql.xml.asproc and add the appropriate SystemUser account to the TrustedUser option set.

Log Entry	Possible Cause	Resolution
called by a trusted user or the user owner. ERROR: Critical TK KERNEL error ERROR: User does not have sufficient authorization to perform requested operation: IMPERSONATE(AS:User\(auth ID). NOTE: No rows returned.	that is running PROC ASEXPORT.	
ERROR: The symbolic reference for (object) did not resolve. ERROR: IOMI:DoRequest function failed. ERROR: Cannot associate a Login with UserID USRDEMO to Identity usrdemo because this UserID is already assigned to a Login for Identity sasdemo. ERROR: IOMI:DoRequestfunction failed	User object failed to resolve in SAS Metadata Server because of domain mismatch with existing user account. Domains must match for login accounts.	Using SAS Management Console, add an additional login on the accounts tab with the authentication domain that matches the authdomain exported from DataFlux Authentication Server. A user object may have two entries on the accounts tab, one for each authentication domain.
ERROR: The symbolic reference for $G0005A7726985E11D8F40005650AA5E1 did not resolve. ERROR: IOMI:DoRequest function failed.	In this case, the system user was also a user in metadata, but a specific user ID is not presented. You have to identify the user object before taking action.	During deployment, use the dfauthsvrc_asproc.result.log in conjunction with dfauthsvrc_asproc.validation_result.lst to match the object value to a username. After deployment, refer to the SAS log of the session used to run PROC ASEXPORT.
Shared Login account(s) was not exported.	ASEXPORT does not export shared logins.	Shared login accounts must be recreated in SAS Metadata Server. See the *SAS Federation Server: Administrators Guide* for procedures to create shared login accounts.

Log Entry	Possible Cause	Resolution
Unresolved authentication identifier (auth ID), also referred to as an 'orphaned ID'.	The user or group account no longer exists.	SAS Federation Server: Use the DROP AUTH ID DDL statement to drop the identifier or transfer the object ownership to another user. Here is an example: `DROP { AUTHID | AUTHORIZATION [IDENTIFIER] } "ID" [TRANSFER TO name]`

Configuring DataFlux Authentication Server

- Upgrade Notes
- Promote Server Content to a New Release
- Add, Edit, or Delete a Server Definition
- Select a Default Server
- Connect to a Server
- About the Server Configuration Files
- Identify Administrators
- Configure Encryption
- Configure the Shared Login Manager on SAS Federation Server
- Configure Authorizations in the Operating System
- Configure Authentication Providers
- Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins
- Add a New Default Server

Upgrade Notes

If you are upgrading an existing DataFlux Authentication Server to a new release, be sure to follow these general steps:

1. Install the new server alongside your existing server.
2. Migrate your existing users, groups, domains, logins, and shared logins to the new release.
3. Promote your server configuration, including authentication providers.
4. Test your new server.
5. Uninstall your old server.

> **Note:** The uninstall process for the DataFlyx Authentication Server removes all installed files, including the file ASDB.TDB, which contains the system tables for the default transactional database.

Promote Server Content to a New Release

Follow these steps to promote DataFlux Authentication Server to the latest release:

1. Stop DataFlux Authentication Server in the latest release and in the previous release.
2. Copy the ASDB.TDB file to the new installation location. See <*install-path*>/var.
3. Compare the configuration files in the previous release, update the configuration files as needed in the current release, and then close all of the configuration files.
4. Start DataFlux Authentication Server in the latest release and in the previous release. Validate that the database and server configuration in the latest release contain the content that was promoted from the previous release.

Add, Edit, or Delete a Server Definition

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

1. In DataFlux Data Management Studio, expand the **Administration** riser. If you do not have an **Administration** riser, disconnect from your current DataFlux 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 **Authentication Servers** and select **Edit** or **Delete**.

Select a Default Server

When you select a default DataFlux Authentication Server, you will be prompted to log in when you start DataFlux Data Management Studio.

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 a Server

Connect to DataFlux Authentication Server to view and edit logins, users, groups, domains, and shared logins.

Before you can connect, you must first create a server definition.

Follow these steps to connect to DataFlux Authentication Server:

1. In DataFlux Data Management Studio, expand the **Authentication Servers** riser.
2. Right-click the server name.
3. Select **Open**.
4. In the Login dialog box, 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 host of DataFlux Authentication Server.

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.

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.

About the Server Configuration Files

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

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

Most of the configuration files are stored by default in `<install-path>\etc` or in a similar path on UNIX or Linux. Files with other locations are listed below.

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

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

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

as_serv_aspsql_schema_trans.xml - describes how to build system tables for the default transactional database. This file is not intended to be edited.

as_serv_aspsql_schema_ora.xml - describes how to build the schema and system tables for an Oracle database. This file is not intended to be edited.

as_serv_aspsql_schema_odbc_ora.xml - when you use an Oracle database, and when you specify the location of the Oracle database server using an ODBC DSN (rather than a path), this file tells the server how to build the Oracle schema and and system tables. This file is not intended to be edited.

as_serv_aspsql_scf.dat - optionally stores the Oracle credentials that are used by DataFlux Authentication Server to access users, groups, domains, logins, and shared logins on Oracle. If you use this file to store your Oracle credentials, set the values of the option CredentialsLocation accordingly in the file as_serv_aspsql.xml. This file is stored by default in `<install-path>\var`.

sasauth.conf - configures the SASAUTH software on UNIX and Linux hosts, as described in Configure the SASAUTH Authentication Utility. This file is stored by default in `<install-path>/lib`.

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

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

Identify Administrators

DataFlux Authentication Server administrators are authorized to add, edit, and delete users, groups, domains, and shared logins.

An administrator is initially identified when you install DataFlux Authentication Server. The individual who executed the installation application becomes the administrator by default unless you specify another individual (by user ID) at that time.

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

Configure Encryption

By default, DataFlux Authentication Server encrypts all network traffic. You can change the default encryption level by changing the value of the Clientencryptionlevel option in the configuration file as_serv_aspsql.xml. You can choose between no encryption, login encryption, and all encryption. The default value is EVERYTHING, which encrypts all network traffic.

By default, DataFlux Authentication Server uses the SASProprietary encryption algorithm. SASProprietary uses 56-bit keys. If you enable DataFlux Secure, you can upgrade to AES encryption. AES encryption uses 256-bit keys.

DataFlux Secure enables DataFlux Authentication Server to use SSL (HTTPS) and FIPS compliance, as described in the *DataFlux Secure Administrator's Guide*.

Installing DataFlux Secure affects two server configuration options in as_serv_aspsql.xml: NetworkEncryptionAlgorithm and EncryptFIPS.

Configure the Shared Login Manager on SAS Federation Server

On SAS Federation Server, the Shared Login Manager requests outbound logins from DataFlux Authentication Server. The outbound logins enable SAS Federation Server to authenticate users on databases such as Oracle.

To configure the Shared Login Manager, you specify a login and a shared login key. The key grants the Shared Login Manager access to all of the shared logins that were assigned that particular key.

If you assign the Shared Login Manager a non-administrative login, access is granted only to the subset of shared logins that list the non-administrative login as a shared login manager.

To display shared login managers and shared login keys, open SAS Federation Server Manager.

To assign a login to the Shared Login Manager on SAS Federation Server, follow these steps:

1. Open SAS Federation Server Manager.
2. Connect to SAS Federation Server.
3. In the **Options** dialog, click the **Advanced** tab.
4. Enter the user ID and password of the login of the Shared Login Manager, as well as an optional shared login key.
5. Click **OK** to save your entries.

Configure Authorizations in the Operating Environment

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

Recommended Authorizations for Windows

Directories	User Role	Authorizations
<*install-path*>\ AuthServer	Installer	Full control
	Process user	Read, write, execute, list folder contents
<*install-path*>\var	Installer	Full control
	Process user	Read, write, execute, list folder contents
	Person who backs up DataFlux Authentication Server	Read, list folder contents

Recommended Authorizations for UNIX and Linux

Directories	User Role	Authorizations
<*install-path*>/authserver	Installer	Read, write execute
	Process user	Read, execute
<*install-path*>/authserver/var	Installer	Read, write execute
	Process user	Read, write execute
	Person who backs up DataFlux Authentication Server	Read, execute

Configure Authentication Providers

- About Authentication Providers
- Configure Authentication in Windows
- Configure Authentication in UNIX and Linux

About Authentication Providers

Authentication takes place when a client such as DataFlux Data Management Studio requests a connection to SAS Federation Server or DataFlux Data Management

Server. To authenticate, the client's DataFlux Authentication Server works with an authentication provider in the operating environment, in the domain that is specified in the login. Successful authentication enables the client to establish a connection to the server.

You can configure as many as three authentication providers for each DataFlux Authentication Server, one of each of the following types. Each provider needs to have its own domain.

AD - Windows Active Directory authentication.

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

Host - Host authentication uses the authentication provider of the host of DataFlux Authentication Server. Host authentication is configured by default during installation.

To reconfigure authentication providers, see Configure Authentication in Windows or Configure Authentication in UNIX/Linux.

Configure Authentication in Windows

Follow these steps to configure authentication providers when DataFlux Authentication Server is running in the Windows operating environment. You can specify up to three authentication providers, one of each type (LDAP, Active Directory, and Host), in unique domains.

1. If DataFlux Authentication Server is running, then stop the server.
2. Open the configuration file as_serv_aspsql.xml. The default path of that file is `<install-path>\etc\as_serv_aspsql.xml`.
3. In the configuration file, locate the **AuthProviderDomain** option. This option associates the types of authentication providers with your domains. To learn more about this option, see Appendix: Configuration File Reference.
4. To configure a single authentication provider of the type Host, specify a domain for the HOSTUSER keyword:
   ```
   <Option name="AuthProviderDomain">HOSTUSER:your-domain-name</Option>
   ```
   The HOSTUSER domain is used by default if the login being authenticated does not contain a domain. If this option is not specified in the configuration file, then the default domain name is HOSTUSER.
5. To configure a single Active Directory authentication provider, specify a domain for the ADIR keyword:
   ```
   <Option name="AuthProviderDomain">ADIR:your-AD-domain</Option>
   ```
6. To configure a single LDAP authentication provider, specify a domain for the LDAP keyword:

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

7. To specify two or three authentication providers, use the following syntax:

```
<Option
name="AuthProviderDomain">(provider1:domain1,provider2:domain2,
   provider3:domain3)</Option>
```

For example:

```
<Option
name="AuthProviderDomain">(HOSTUSER:NYCWIN,ADIR:BRONXAD,LDAP:BROO
KLYNKLDAP)</Option>
```

Note: You can specify a maximum of one provider of each type, and the domains must be unique.

8. If you specified an Active Directory authentication provider, then use the SetEnv option set to specify AD_HOST and AD_PORT:

```
<OptionSet name="SetEnv">
    <!-- specify a host for Active Directory authentication-->
   <Option name="AD_HOST">yoursite.yourcompany.com</Option>
   <Option name="AD_PORT">host-port-number-for-AD</Option>
</OptionSet>
```

If you did not configure an LDAP authentication provider, you can proceed to step 12.

9. If you specified an LDAP authentication provider, then specify the environment variables LDAP_BASE, LDAP_HOST, and LDAP_PORT:

```
<OptionSet name="SetEnv">
    <!-- specify envars for LDAP authentication -->
   <Option
name="LDAP_HOST">yourldaphost.yousite.mycompany.com</Option>
   <Option name="LDAP_PORT">host-port</Option>
   <Option name="LDAP_BASE">ou=yourorgunit,o=yourorg</Option>
</OptionSet>
```

The environment variable LDAP_BASE defines the default base DN (Distinguished Name). The values for LDAP_BASE are site-specific.

10. If you specified an LDAP authentication provider, and if that provider does not allow anonymous binds, then specify the privileged DN in the environment variables LDAP_PRIV_DN, and LDAP_PRIV_PW:

```
<OptionSet name="SetEnv">
   <!-- specify an authorized LDAP user for simple binds -->
   <Option name="LDAP_PRIV_DN">user-name</Option>
   <Option name="LDAP_PRIV_PW">password</Option>
</OptionSet>
```

The user that you specify must be authorized to search for users.

11. If you specified an LDAP authentication provider, and if the LDAP server is configured to use a value other than DN for authentication, then specify an alternate value in the environment variable LDAP_IDATTR:

```
<OptionSet name="SetEnv">
   <!-- specify an LDAP authentication attribute other than DN --
>
   <Option name="LDAP_IDATTR">CN</Option>
</OptionSet>
```

CN is an example value. The value at your site may differ. The default value of LDAP_IDATTR is `userid`.

Contact your site administrator to determine if additional configuration steps are required for your LDAP implementation.

12. Save and close the configuration file.
13. Start DataFlux Authentication Server.

Configure Authentication in UNIX and Linux

- About Authentication in UNIX and Linux
- Configure LDAP Authentication
- Configure AD Authentication
- Configure SASAUTH Authentication
- Configure SASAUTH for PAM

About Authentication in UNIX and Linux

Starting in DataFlux Authentication Server 3.2, the server installation process prompts you through the process of configuring an authentication provider. The server is started at the conclusion of the installation process, so you can begin using your server immediately.

The installation process configures DataFlux Authentication Server to use host authentication. This means that the server will authenticate in the domain of the host on which the server is installed.

After installation, you can change host authentication to point to a different UNIX or Linux domain. You can also use . You can configure one LDAP, one Active Directory, and one Host authentication provider. This feature enables you to authenticate users in as many as three domains on a single DataFlux Authentication Server.

To revise your post-installation authentication provider, you will need input from your network administrator so that you can apply site-specific values. Using site-specific values, you configure your LDAP and AD providers in DataFlux Authentication Server's configuration file.

Host authentication is provided by your UNIX or Linux operating environment. To interact with the host authentication provider, DataFlux Authentication Server uses the SASAUTH utility. SASAUTH:

1. Looks up the submitted userid in a user database.
2. Compares the submitted password to the password in a password database.
3. Retrieves the UID number for the user and apply the access controls that are associated with that UID.

If your host authentication provider uses pluggable authentication modules (PAM), SASAUTH can be configured accordingly.

Configure LDAP Authentication

When DataFlux Authentication Server is installed on a UNIX or Linux host, follow these steps to configure an LDAP authentication provider:

1. Begin by ensuring that your LDAP authentication provider is properly configured to authenticate UNIX users. In order for DataFlux Authentication Server to connect directly to the LDAP database, the database must include the required UNIX/Posix user attributes, such as UID. Most LDAP servers provide an LDAP schema that contains this information. Your LDAP database must conform to the RFC 2307 standard for UNIX user attributes.
2. If DataFlux Authentication Server is running, then stop the server.
3. Open the configuration file *<install-path>*/etc/as_serv_aspsql.xml.
4. In the option AuthProviderDomain, change the single authentication provider to LDAP or add the LDAP provider and domain to your existing authentication providers:

```
<!-- single-provider syntax -->
<Option name="AuthProviderDomain">LDAP:your-ldap-domain</Option>


<!-- multi-provider syntax -->
<Option name="AuthProviderDomain">ADIR:domain1,HOSTUSER:domain2,
   LDAP:domain3</Option>
```

5. Use the SetEnv Option Set to configure the following LDAP environment variables:

   LDAP_HOST - identifies the LDAP server host.

   LDAP_PORT – the port number of the LDAP service. If LD_PORT is not defined, then the default port value is used.

   LDAP_BASE – specifies the default base DN (Distinguished Name) to use when performing LDAP operations.

```
<OptionSet name="SetEnv">
  <Option
name="LDAP_HOST">myldaphost.mysite.mycompany.com</Option>
  <Option name="LDAP_PORT">myport</Option>
  <Option name="LDAP_BASE">ou=myorgunit,o=myorg</Option>
</OptionSet>
```

6. If the LDAP server does not allow anonymous binds, then LDAP_PRIV_DN and LDAP_PRIV_PW are required. The LDAP_PRIV_DN user needs to be authorized to search for users:

   LDAP_PRIV_DN=*privileged-DN*

   DN LDAP_PRIV_PW=*password-for-privileged-DN*

   ```
   <OptionSet name="SetEnv">
     <Option name="LDAP_PRIV_DN">user1</Option>
     <Option name="LDAP_PRIV_PW">passwword1</Option>
   </OptionSet>
   ```

7. If the LDAP server is configured to use a value other than DN (Distinguished Name) for authentication, then specify the alternate value using LDAP_IDATTR. The default value of LDAP_IDATTR is `userid`.

   LDAP_IDATTR=*attribute-name*

   ```
   <OptionSet name="SetEnv">
     <Option name="LDAP_IDATTR">CN</Option>
   </OptionSet>
   ```

8. Consult with your network administrator to determine if any additional site-specific LDAP settings are required.
9. Save and close the configuration file.
10. Start DataFlux Authentication Server.

Configure AD Authentication

When DataFlux Authentication Server is installed on a UNIX or Linux host, follow these steps to configure Active Directory (AD) authentication:

1. Begin by ensuring that your AD authentication provider is properly configured to authenticate UNIX users. In order for DataFlux Authentication Server to connect directly to the AD database, the database must include the required UNIX/Posix user attributes, such as UID. Most AD servers provide an AD schema that contains this information. To enable connections, install Microsoft Services for UNIX (SFU) 2 or 3 on the hosts of your AD repositories.
2. If DataFlux Authentication Server is running, then stop the server.

3. Open the configuration file <*install-path*>/etc/as_serv_aspsql.xml.

4. In the option AuthProviderDomain, change the single authentication provider to ADIR or add the AD provider and domain to your existing authentication providers:

```
<!-- single-provider syntax -->
<Option name="AuthProviderDomain">ADIR:your-ldap-domain</Option>

<!-- multi-provider example -->
<Option name="AuthProviderDomain">HOSTUSER:domain2,LDAP:domain2,
   ADIR:domain3</Option>
```

5. Use the SetEnv Option Set to configure the following LDAP environment variables:

   AD_HOST - identifies the Active Directory server host.

   AD_PORT – specifies the port number for Active Directory.

```
<OptionSet name="SetEnv">
  <Option name="AD_HOST">your-AD-network-hostname</Option>
  <Option name="AD_PORT">port-number-on-AD-host</Option>
</OptionSet>
```

6. Save and close the configuration file.

7. Start DataFlux Authentication Server.

Configure SASAUTH Authentication

The SASAUTH authentication utility is used to implement host authentication in the UNIX and Linux operating environments. Host authentication uses the authentication domain of the computer that hosts the DataFlux Authentication Server.

Beginning in DataFlux Authentication Server 4.1, SASAUTH is configured for host authentication during the installation process. Before DataFlux Authentication Server 4.1, SASAUTH configuration was a post-installation procedure.

The post-installation procedure for configuration SASAUTH remains valid if you need to change the default authentication domain or authentication provider.

SASAUTH can be configured to use default authentication (known as pw) or pluggable authentication modules (PAM), or even both methods in series. SASAUTH also provides three levels of logging, and a configurable response to invalid authentications. All of these features are configured in the file sasauth.conf.

Note: The SASAUTH utility requires root authorizations.

Follow these steps to reconfigure the SASAUTH utility:

1. If DataFlux Authentication Server is running, then stop the server.

2. Login with root privileges, or contact your network administrator, to run the following script, which establishes root privileges for the SASAUTH utility:
   ```
   sh> <install-path>/lib/sasauth.inst.sh
   ```

3. Execute the following script to enable the SASAUTH utility:
   ```
   sh> <install-path>/bin/set_auth sasauth
   ```

4. Edit the SASAUTH configuration file.
   ```
   <install-path>/lib/sasauth.conf
   ```

5. In the configuration file, the methods variable specifies authentication methods for the SASAUTH utility. The methods variable accepts the values `pw` and `pam`. Use the `pw` value for authentication via `<install-path>/etc/passwd`. On some hosts, `pw` provides non-traditional authentication using protected password databases or other enhancements. Use the `pam` value if your site uses pluggable authentication modules.

   You can specify `pw`, `pam`, or both. If you specify both, then SASAUTH will authenticate with the first method, then attempt to authenticate with the second method if necessary.

   Specify one of the following values for the methods variable:

   ```
   methods=pw
   methods=pam
   methods=pw pam
   methods=pam pw
   ```

   If you specify `pam`, then you need to configure that method. See Configure SASAUTH for PAM.

6. As needed, you can activate and configure the SASAUTH logging facility by enabling a log file. In the configuration file, remove a comment character and insert a path for one of the three log files, as shown in the following example.

   The following example enables the Access Log and populates a log file at the specified location:

   ```
   #debugLog=
   accessLog=/tmp/sasauth.log
   #errorLog=
   ```

   Enable the `debugLog` only when testing or diagnosing errors.

   Note: You may need to configure the syslog on the host of DataFlux Authentication Server in order to collect log messages from SASAUTH.

7. To configure repeated authentication attempts, edit the options `maxtries`, `maxtriesPeriod`, and `maxtriesWait`.

`maxtries` - specifies the number of authentication attempts allowed before a waiting period is imposed.

`maxtriesPeriod` - specifies the number of seconds that can elapse before the termination of the authentication process.

`maxtriesWait` - specifies the number of seconds that a user must wait if that user exceeds the `maxtries` value within the time limit of `maxtriesPeriod`. After the waiting period, the `maxtries` count is reset to zero.

The default values specify 5 attempts in 60 seconds, following by a waiting period of 5 minutes:

```
maxtries=5
maxtriesPeriod=60
maxtriesWait=300
```

To disable the limits on authentication retries, insert comment characters in front of each variable:

```
# maxtries=5
# maxtriesPeriod=60
# maxtriesWait=300
```

8. Save and close the sasauth.conf configuration file.
9. When it is installed on UNIX or Linux, DataFlux Authentication Server is configured by default to authenticate with the UNIXUSER domain. If you wish to change the name of the domain, open the configuration file as_serv_aspsql.xml. In that file, edit the UNIXUSER domain name in the following entry:

   ```
   <Option name="AuthProviderDomain">HOSTUSER:UNIXUSER</Option>
   ```

   Save and close the configuration file.
10. Start DataFlux Authentication Server.

Configure SASAUTH for PAM

If you configured the SASAUTH utility for host authentication, and if you specified PAM as an authentication method, then use this topic to configure PAM authentication.

PAM requires you to register the applications that use authentication services. In the operating environment, upgrade your PAM configuration to register SASAUTH. In the HP-UX, Solaris, and AIX operating environments, the PAM configuration is stored in `/etc/pam.conf`. In that file, you need to specify the authentication services that are used by SASAUTH, and you need to specify when SASAUTH performs authentication. These specifications are made in the module types `account` and `auth`.

Caution: *PAM allows you to register* other*, which permits any application to use authentication services. The use of* other *is not recommended.*

PAM supports applications that run in both 32–bit and 64–bit environments. The SASAUTH utility has a 64-bit format. In the pam.conf configuration file, make sure that the modules that you associate with SASAUTH also have a 64–bit format.

PAM modules are usually provided in separate directories for 32–bit and 64–bit libraries. The pam.conf configuration file contains pathnames that are either relative (Solaris and AIX) or that contain a symbolic variable (HP-UX).

The entries in pam.conf that are used to register applications have the following form:

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

Examples for Solaris:

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

Examples for HP/UX:

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

Refer to the man page for PAM to ensure that you correctly register SASAUTH.

Note: On AIX, PAM is not activated by default. To activate PAM, refer to the IBM document *Security Guide - Authentication Module*.

In Linux operating environments, the directory /etc/pam.d contains one configuration file for each application that is authorized to use PAM. The name of the configuration file matches the name of the application. For SASAUTH, the configuration file is /etc/pam.d/sasauth. The SASAUTH configuration file needs to contain entries in the following form:

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

Examples for Linux:

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

```
account required pam_unix_acct.so
```

Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins

Overview

By default, DataFlux Authentication Server uses a transactional database to store users, groups, domains, logins, and shared logins. You can choose to configure DataFlux Authentication Server to store these objects on an Oracle relational database. The Oracle configuration uses an Oracle driver, or one of two available ODBC drivers. The Oracle driver uses a path to access the database. The ODBC drivers use a data source name (DSN) to access the database.

After you install DataFlux Authentication Server, you update the primary server configuration file to configure the Oracle database. If you choose an ODBC driver, you may also need to add an ODBC data source, as described later in this topic.

Note: If you already have an ODBC data source, make sure that your odbc.ini file contains the required value `EnableNcharSupport=1`.

Configure the Oracle Database

1. Edit the configuration file shown in this Windows path:
   `<install-path>\etc\as_serv_aspsql.xml`

2. For the entity ASPSQL_SCHEMA, enter the name of the Oracle schema for DataFlux Authentication Server's transactional database.
   `<!ENTITY ASPSQL_SCHEMA "oracle-schema-name">`

3. Add comment tags as follows to prevent the creation of these two entities:
   ```
   <!-- <!ENTITY ASPSQL_TRANDBF "C:\Program
   Files\DataFlux\AuthServer\server1\var\asdb.tdb"> -->
   <!-- <!ENTITY ASPSQL_CONFIG_DBMS SYSTEM
   "as_serv_aspsql_schema_tran.xml"> -->
   ```

4. Remove comment tags as follows to create these three entities:
   ```
   <!ENTITY ASPSQL_ORAPATH "{TNSNames entry for your Authentication
   Server database}">
   <!ENTITY ASPSQL_CONFIG_DBMS SYSTEM
   "as_serv_aspsql_schema_ora.xml">
   <!ENTITY ASPSQL_CREDENTIALS_LOC "<install-
   path>\var\as_serv_aspsql_scf.dat">
   ```

5. Remove comment tags around the following option:
   ```
   <Option
   name="CredentialsLocation">&ASPSQL_CREDENTIALS_LOC;</Option>
   ```

6. If you plan to store Oracle credentials on disk, then continue with this step to create an Oracle credentials file. If you plan to enter Oracle credentials manually, then jump ahead to the next step.

   DataFlux recommends that you store the Oracle credentials file in the `var` directory, as indicated in the default value of the entity ASPSQL_CREDENTIALS_LOC. The `var` directory is recommended to receive access restrictions in the operating environment, as specified in Configure Authorizations in the Operating System. If you use a non-default storage location, be sure to specify an absolute path for the entity, rather than a relative path.

   Open the Oracle credentials file. Add Oracle credentials in the following format:

   `UID=myuser;PWD=mypwd`

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

7. If you plan to enter Oracle credentials manually, rather than storing them on disk, you can use **Set Provider Credentials**, or you can write a script that runs when you start the server. If you write a script, then the script will need to prompt the user for credentials, which would then be maintained in memory until the server is restarted.

   To use **Tools ->** **Set Provider Credentials** in DataFlux Data Management Studio to manually enter credentials, set a blank value for the entity ASPSQL_CREDENTIALS_LOC:

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

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

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

8. If it is still open, save and close the configuration file as_aspsql.xml
9. Start or restart DataFlux Authentication Server.

Example Configuration File

The following version of the file as_serv_aspsql.xml shows typical values for a configuration that uses Oracle to store users, groups, domains, logins, and shared logins.

```
<?xml version="1.0"?>

<!--
```

```
     HOW TO CONFIGURE AN ORACLE DATA STORE:
     In order to configure DataFlux Authentication Server to use
an Oracle data store,
     search for the word "Oracle" in this file and follow the
instructions in the comments. -->

<!DOCTYPE Config [
<!-- ASPSQL Provider DBMS independent content -->
<!ENTITY ASPSQL_CATALOG "AS">
<!-- When configuring an Oracle data store, specify a valid
Oracle schema for ASPSQL_SCHEMA below -->
<!ENTITY ASPSQL_SCHEMA "">

<!ENTITY ASPSQL_SCHEMA_QUALIFIER "">
<!ENTITY ASPSQL_BT_DOMAINS "DOMAINS">
<!ENTITY ASPSQL_BT_SUBJECTS "SUBJECTS">
<!ENTITY ASPSQL_BT_GROUPS "GROUPS">
<!ENTITY ASPSQL_BT_SUBJECT_GROUPS "SUBJECT_GROUPS">
<!ENTITY ASPSQL_BT_GROUP_GROUPS "GROUP_GROUPS">
<!ENTITY ASPSQL_BT_PRINCIPALS "PRINCIPALS">
<!ENTITY ASPSQL_BT_PRINCIPAL_MAPS "PRINCIPAL_MAPS">
<!ENTITY ASPSQL_BT_GROUP_MAP_MGRS "GROUP_MAP_MGRS">
<!ENTITY ASPSQL_BT_GROUP_MAP_USERS "GROUP_MAP_USERS">
<!ENTITY ASPSQL_BT_SUBJECT_MAP_MGRS "SUBJECT_MAP_MGRS">
<!ENTITY ASPSQL_BT_SUBJECT_MAP_USERS "SUBJECT_MAP_USERS">
<!ENTITY ASPSQL_BT_VERSION "VERSION">
<!ENTITY ASPSQL_BT_SENTINEL "SENTINEL">

<!-- Transactional data store used by default -->

<!--
     Add comment tags around the following lines when configuring
an Oracle data store
-->
<!ENTITY ASPSQL_TRANDBF "C:\Program
Files\DataFlux\AuthServer\server1\var\asdb.tdb">
<!ENTITY ASPSQL_CONFIG_DBMS SYSTEM
"as_serv_aspsql_schema_tran.xml">

<!--
     Remove comment tags from the following lines to configure an
Oracle data store
     and supply a valid Oracle Path
 -->
```

```
<!-- <!ENTITY ASPSQL_ORAPATH "{TNSNames entry for your
Authentication Server database}"> -->
<!-- <!ENTITY ASPSQL_CONFIG_DBMS SYSTEM
"as_serv_aspsql_schema_ora.xml"> -->
<!-- <!ENTITY ASPSQL_CREDENTIALS_LOC "<install-
path>\var\as_serv_aspsql_scf.dat"> -->

]>
<Config name="ASConfig">
                <!-- Port to listen on -->
                <Option name="Port">21030</Option>

           <!-- Administrative account -->
     <OptionSet name="SystemUsers">
           <Option name="Account">LOCAL\tsadm</Option>
     </OptionSet>

           <OptionSet name="SetEnv">
          <Option name="FIREBIRD">C:\Program
Files\DataFlux\AuthServer\server1\lib\fbembed</Option>
          <Option name="FIREBIRD_LOG">C:\Program
Files\DataFlux\AuthServer\server1\var\log</Option>
     </OptionSet>

     <OptionSet name="PrependEnv">
                              <Option name="Path">C:\Program
Files\DataFlux\AuthServer\server1\lib\fbembed;</Option>
     </OptionSet>

     <!-- Encryption Algorithm -->
     <Option
name="NetworkEncryptAlgorithm">SASProprietary</Option>
     <Option
name="ObjectServerParms">CLIENTENCRYPTIONLEVEL=EVERYTHING</Option
>

     <OptionSet name="License">
          <OptionSet name="Primary">
               <Option name="Provider">SAS</Option>
                                                  <Option
name="Location"><install-path>\etc\license</Option>
          </OptionSet>
                <!-- </OptionSet> -->

     <OptionSet name="TrustedUsers">
```

```
            <Option name="Account">DATAFLUX\dfcnn19</Option>
        </OptionSet>

        <!-- Provider name -->
        <Option name="AuthenticationProvider">ASPSQL</Option>

             <!-- Provider-specific root element -->
        <OptionSet name="ASPSQLProvider">
             <!-- System catalog and schema names -->
            <Option name="SystemCatalog">&ASPSQL_CATALOG;</Option>
            <Option name="SystemSchema">&ASPSQL_SCHEMA;</Option>
            <Option name="MinConnections">1</Option>
            <Option name="MaxConnections">2</Option>

            <!-- Remove comment tags from the following line to
    configure an Oracle data store -->
            <!-- <Option
    name="CredentialsLocation">&ASPSQL_CREDENTIALS_LOC;</Option> -->

             &ASPSQL_CONFIG_DBMS;
        </OptionSet>
    </Config>
```

Add an ODBC Data Source on Windows

If DataFlux Authentication Server runs on Windows, follow these steps to add an ODBC data source:

1. Open the Windows application ODBC Data Source Administrator:
    a. Select **Start** > **Settings** > **Control Panel**, or use the current Windows equivalent path.
    b. Double-click **Administrative Tools**.
    c. Double-click **Data Sources (ODBC)**.
2. In the ODBC Data Source Administrator, click the **System DSN** tab, and then click **Add**.
3. In the Create New Data Source dialog, select **DATAFLUX 32-BIT Oracle**, or select **DATAFLUX 32-BIT Oracle Wire Protocol**. Click **Finish**.
4. In the driver setup dialog, enter your data source properties in the provided fields and tabs.
5. Click the **Advanced** tab, and then click **Enable N-CHAR Support**, to display a check mark for that property. This selection is required.
6. Click **OK** twice to save your changes.

Add an ODBC Data Source on UNIX or Linux

If DataFlux Authentication Server runs on UNIX or Linux, follow these steps to add an ODBC data source.

1. Run the DataFlux ODBC Configuration tool:
   ```
   bin/dfdbconf
   ```
2. Enter **A** to add a new data source.
3. In the **Available Templates** list, choose **Oracle Wire Protocol [DataDirect 6.0 Oracle Wire Protocol]**. On certain versions of UNIX, you can choose **Oracle [DataDirect 6.0 Oracle]** instead.
4. Enter a value of 1 for the property **Enable N-CHAR Support**. This entry is required.
5. Enter your site's data source parameters, or press **Enter** to select default values.
6. Enter a name for the new data source.

Add a New Default Server

After you install, configure, and start a new DataFlux Authentication Server, you and other users follow these steps to create a new server definition and select the new server as their default. The default server authenticates your login when you start DataFlux Data Management Studio.

1. In DataFlux Data Management Studio, click the **Administration** riser.
2. Right-click DataFlux Authentication Server and select **New Authentication Server Connection**.
3. In the window Add Authentication Server Definition, create the server definition and test the connection.
4. In the Administration riser, right-click the new server definition and select **Set as Default**.

When you select a default DataFlux Authentication Server, the client creates the following configuration file:

```
C:\Documents and Settings\userid\Application
Data\DataFlux\DMStudio\instance\etc\app.cfg
```

In this user-specific instance of app.cfg, DataFlux Data Management Studio stores the following option/value pair:

```
BASE/AUTH_SERVER_LOC=auth-server-network-host-name:port
```

```
Example: BASE/AUTH_SERVER_LOC=d14885.ourCompany.com:21030
```

Note: If your user-specific instance of the app.cfg file is not removed before you upgrade DataFlux Data Management Studio, the new version of DataFlux Data Management Studio will attempt to authenticate with your previous default server.

You can change your default DataFlux Authentication Server at any time by selecting **Set as Default**.

Administering DataFlux Authentication Server

- Start or Stop a Server in Windows
- Start, Stop, or Display Server Information in UNIX or Linux
- Connect to DataFlux Authentication Server
- Select a Default Server
- Backup or Restore DataFlux Authentication Server
- Administer Log Files

Start or Stop a Server in Windows

Follow these steps to start or stop a DataFlux Authentication Server that is running on a Windows host.

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

   Note: Version number differences between DataFlux Authentication Server database schema and DataFlux Authentication Server itself can terminate the start process. Major version numbers must match. The minor version number of the schema can be 1 less than the minor version number of the server.

   Note: The DataFlux Authentication Server will not start if the default port number is not specified for the Port option in the configuration file as_serv_aspsql.xml.

Start, Stop, or Display Server Information in UNIX or Linux

Use the script dasadmin to start, stop, and display information for DataFlux Authentication Server in the UNIX or Linux operating environment.

The dasadmin script accepts the following commands:

start - starts DataFlux Authentication Server.

stop - stops DataFlux Authentication Server.

status - displays the operational status (running, not running) of DataFlux Authentication Server.

help - displays usage information for the dfsadmin script.

version - displays version information for DataFlux Authentication Server and records the same information in the log file for DataFlux Authentication Server.

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

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

To stop DataFlux Authentication Server, use:

```
<install-path>/bin/dasadmin stop
```

Note: Version number differences between DataFlux Authentication Server database schema and DataFlux Authentication Server itself can terminate the start process. Major version numbers must match. The minor version number of the schema can be 1 less than the minor version number of the server.

Note: DataFlux Authentication Server will not start if the default port number is not specified for the Port option in the configuration file as_serv_aspsql.xml.

Connect to a Server

Connect to DataFlux Authentication Server to view and edit logins, users, groups, domains, and shared logins.

Before you can connect, you must first create a server definition.

Follow these steps to connect to DataFlux Authentication Server:

1. In DataFlux Data Management Studio, expand the **Authentication Servers** riser.
2. Right-click the server name.
3. Select **Open**.

4. In the Login dialog box, 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 host of DataFlux Authentication Server.

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.

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.

Select a Default Server

When you select a default DataFlux Authentication Server, you will be prompted to log in when you start DataFlux Data Management Studio.

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**.

Backup or Restore DataFlux Authentication Server

Overview

Use this section to backup or restore your users, groups, domains, logins, and shared logins, either in the default transactional database or on Oracle. Also use this section to backup the executable files of DataFlux Authentication Server.

Backup Server Files

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

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

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

Or, on Windows 7:

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

And:

```
C:\Program Files\DataFlux\AuthServer
```

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

Backup or Restore a Transactional Database

DataFlux Authentication Server uses a transactional database by default to store users, groups, domains, logins, and shared logins. The database is implemented in a file. The file is required to be stored locally, on the host of DataFlux Authentication Server. The name and location of the database file are specified in the configuration file as_serv_aspsql.xml. The location is specifed for the entity ASPSQL_TRANDBF, as follows:

```
ENTITY ASPSQL_TRANDBF "<install-path>\var\asdb.tdb">
```

To back up the transactional database file, enter the following command :

```
<install-path>\bin\dasutil backup full-path-to-transdb-backup-file
```

In the UNIX or Linux operation environment, the command and the install path are the same.

To restore the transactional database, enter:

```
<install-path>\bin\dasutil restore full-path-to-transdb-backup-file
```

The full path points to a backup file, not to the file that you are backing up, as shown in the following Windows examples:

```
dasutil backup \\myBackupHost\myBackupPath\120831asdb.tdb
```

```
dasutil restore \\myBackupHost\myBackupPath\120831asdb.tdb
```

 **Note:** If you backup your transactional database with dasutil, then you are required to restore your database with dasutil.

Backup or Restore an Oracle Database

If you use Oracle to store your users, groups, domains, logins, and shared logins, then locate the Oracle schema that contains the tables for DataFlux Authentication Server. The schema is identified in the configuration file as_serv_aspsql.xml.

Copy the following tables into a new schema, or copy these tables into the same schema using a different name:

DOMAINS

GROUPS

SUBJECTS

SUBJECT_GROUPS

GROUP_GROUPS

PRINCIPALS

PRINCIPAL_MAPS

GROUP_MAP_MGRS

GROUP_MAP_USERS

SUBJECT_MAP_MGRS

SUBJECT_MAP_USERS

VERSION

SENTINEL

 **Note:** These are the default table names. If you changed the names of the tables in the as_serv_aspsql.xml configuration file, use the customized names.

Administer Log Files

- Overview
- About Appenders and Loggers
- Change Log Events and Thresholds
- Upgrade Audit Log Messages to Include User and Group Names
- Initial Log File

Overview

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

`<install-path>\var\log\as_%d_%S {pid}.log`

The d value becomes the date, the S value becomes the server hostname, and *pid* represents the process ID.

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

`<install-path>/var/log/das_yyyy-mm-dd_process-id.log`

Example:

`<install-path>/var/log/das_2013-05-31_24426.log`

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

`<install-path>\etc\as_log.xml`

About Appenders and Loggers

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

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

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

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

OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE
ALL

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

Default Loggers and Thresholds

Logger	Description	Threshold
Cradle	records cradle messages	Info
DataFlux.licensing	records license checks	Warn
Admin	records administrative activity	Info
App	records messages from the DataFlux Data Management Studio	Info

Logger	Description	Threshold
Audit	records database file reads, writes, and deletes.	Info
IOM	records messages from other servers	Info
root	threshold applies to all unspecified log events	Error
App.TableServices. SQLDriver	INACTIVE, records database transactions, for use with Tech Support only	Trace
App.Statement.Statement. ExecDirect	INACTIVE, records statements input from DataFlux Data Management Studio	Trace
App.Statement.Statement. Prepare	INACTIVE, records statements output to DataFlux Data Management Studio	Trace

 **Note:** The three inactive loggers should be enabled only when you are directed to do so by a SAS Technical Support representative.

Change Log Events and Thresholds

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

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

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

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

1. Open in a text editor the log configuration file as_log.xml.

2. To prevent any further collection of log events for a given logger, enclose the logger in comment tags, as in:

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

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

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

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

Initial Log File

Here is the default content of XML log file <*install-path*>\etc\as_log.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<logging:configuration
xmlns:logging="http://www.sas.com/xml/logging/1.0/">

     <!-- Rolling log file with default rollover of midnight -->
     <appender class="RollingFileAppender"
name="TimeBasedRollingFile">
          <param name="Append" value="true"/>
          <param name="ImmediateFlush" value="true"/>
          <rollingPolicy
class="TimeBasedRollingPolicy">               <param
name="fileNamePattern"
                    value="$home\var\log\as_%d_%S{pid}.log"/>
          </rollingPolicy>
          <layout>
               <param name="HeaderPattern" value="Host:
'%S{hostname}',
                    OS: '%S{os_family}',
                    Release: '%S{os_release}',
                    SAS Version: '%S{sup_ver_long2}',
                    Command: '%S{startup_cmd}'"/>
                <param name="ConversionPattern"
                    value="%d %-5p [%t] %c %X{Client.ID}:%u -
%m"/>
          </layout>
     </appender>

     <!-- Cradle message logger -->
     <logger name="Cradle">
          <level value="Info"/>
     </logger>

     <!-- DataFlux licensing message logger -->
     <logger name="DataFlux.Licensing">
          <level value="Warn"/>
     </logger>

     <!-- Administration message logger -->
```

```
    <logger name="Admin">
        <level value="Info"/>
    </logger>

    <!-- Application message logger -->
    <logger name="App">
        <level value="Info"/>
    </logger>

    <!-- Audit message logger -->
    <logger name="Audit">
        <level value="Info"/>
    </logger>

    <!-- IOM protocol message logger -->
    <logger name="IOM">
        <level value="Info"/>
    </logger>

    <root>
        <level value="Error"/>
        <appender-ref ref="TimeBasedRollingFile"/>
    </root>

    <!-- Perf -->
    <logger name="Perf.ARM.SQLServices">
        <level value="Warn"/>
    </logger>

</logging:configuration>
```

Upgrade Audit Log Messages to Include User and Group Names

The Audit logger generates log messages for all changes to DataFlux Authentication Server's transactional database. By default, when users and groups that are the subject of the Audit logger messages, they are identified by metadata ID. To add literal user and group names to the metadata IDs, add the following lines to the log configuration file <*install-path*>\etc\as_log.xml.

```
    <!-- CSV format object ID/name mappings: <count>, <id>, <name>
    Example: FBAB079DFA5841E41B41FAB4D4BD4DD9, Shared_Login_Manager -
    ->

    <logger name="Audit.DFAuthServer.Map">
        <level value="debug"/>
    </logger>

    <!-- Subject <subject-name> (<subject-id>) added -->
    <logger name="Audit.DFAuthServer.AddSubject">
```

```
    <level value="debug"/>
 </logger>

<!-- Group <group-name> (<group-id>) added -->
 <logger name="Audit.DFAuthServer.AddGroup">
     <level value="debug"/>
 </logger>

<!-- PrincipalMap <map-name> (<map-id>) added -->
 <logger name="Audit.DFAuthServer.AddPrincipalMap">
    <level value="debug"/>
</logger>
```

Administering Users, Groups, Domains, Logins, and Shared Logins

- Overview
- Use the Administration Riser
- Access User Logins
- Update in Batch with ASBATCH

Overview

By default, DataFlux Authentication Server maintains a database of users, groups, domains, logins, and shared logins, as defined in About Users, Groups, Domains, Logins, and Shared Logins. The database is used for authentication and authorization. DataFlux Authentication Servers use logins and shared logins to authenticate connection requests for SAS Federation Servers, DataFlux Data Management Server, and relational databases. Authorization is implemented in DataFlux Data Management Server and SAS Federation Server. These servers authorize access to data collections and jobs based on group membership information that is provided by DataFlux Authentication Server.

Two interfaces enable you to create and maintain users, groups, domains, logins, and shared logins: the **Administration** riser in DataFlux Data Management Studio, and the ASBATCH utility.

The **Administration** riser provides administrators with read/write access to the transactional database used by DataFlux Authentication Server. Passwords cannot be displayed, and logins cannot be accessed by default. Non-administrative users can use the **Administration** riser to display authorized information and add logins to their user definitions.

The ASBATCH utility provides a scripting interface that enables you to update the transactional database during off-peak hours. In the script file that drives the updates, you can use filters to update multiple rows with a single command.

Use the Administration Riser

Follow these steps to use the **Administration** riser to create and maintain users, groups, domains, logins, and shared logins on a DataFlux Authentication Server:

1. Open DataFlux Data Management Studio 2.5.*x* or earlier.
2. Click the **Administration** riser on the lower left.

3. Expand **Authentication Server** in the tree, right-click a DataFlux Authentication Server, and select **Open**.

4. Enter a user ID and password.

   To create or edit users, groups, domains, logins, or shared logins, you need a login that is listed as an administrator for the current DataFlux Authentication Server. Administrators cannot add or delete logins other than their own.

   If you connect with a login that is not administrative, you can add logins to your user, view memberships in groups, and view the consumers of shared logins.

5. Click a riser to display users, domains, groups, and shared logins. To add or view logins, click the **User** riser.

6. Click icons or right-click to create or maintain users, groups, domains, logins, or shared logins.

   Note: When you create users, groups, domains, logins, and shared logins, DataFlux Authentication Server may accept special characters that are not accepted in your operating environment. Be sure to follow the naming conventions of your operating environment.

Access User Logins

After an administrator creates a new user definition, the individual who is identified in that user definition adds a password and can also add more logins. Normally, and by default, administrators cannot add, delete, or modify logins. If such access is necessary on a temporary basis, you can enable access, make changes, and then disable access to logins. Similar capabilities are also available in the ASBATCH utility.

Follow these steps to access user logins in the **Administration** riser:

1. Stop DataFlux Authentication Server and edit the configuration file as_serv_aspsql.xml.

2. Add the following option to the configuration file:

   ```
   <Option name="AdminLoginManagementPolicy">
   ADD REMOVE UPDATE</AdminLoginManagementPolicy>
   ```

   You can specify any combination of ADD, REMOVE, or MODIFY. When you modify a login, you change the password.

3. Save and close the configuration file.

4. Start DataFlux Authentication Server and change logins.

5. Stop DataFlux Authentication Server and edit the configuration file.

6. To preserve security, delete the option AdminLoginManagementPolicy, and then save and close the file.
7. Restart DataFlux Authentication Server.

To query the status of the login management policy, use the following read-only Boolean category items:

- Server.LoginManagementPolicy.Add
- Server.LoginManagementPolicy.Remove
- Server.LoginManagementPolicy.Update

Update in Batch with ASBATCH

- ASBATCH Overview
- Use ASBATCH
- Sample XML and CSV Files for ASBATCH
- ASBATCH Operators and Options for XML and CSV Files
- ASBATCH Command-Line Options
- Use the ASBATCH Audit File and Undo File
- Use the ASBATCH Log File

ASBATCH Overview

The ASBATCH utility is installed as a selectable component of SAS Federation Server Manager 4.1 and earlier.

The ASBATCH utility enables you to update the transactional database used by DataFlux Authentication Server. You run ASBATCH using a script and an XML or CMV file. You can execute the script at times of minimal server access.

When you invoke asbatch.exe, command-line options point to an XML or CSV file. In the XML or CSV file, operators and options cause ASBATCH to add, modify, or delete users, groups, domains, and logins.

> **Note:** ASBATCH does not add, modify, or delete shared logins. Use the Administration riser in DataFlux Data Management Studio for that purpose.

> **Note:** CSV files do not add, modify, or delete groups. Use an XML file for that purpose.

The ASBATCH utility generates an audit file that lists all changes made, and also generates an undo file that enables you to remove newly added users, groups, domains and logins.

You can create a log configuration file that will cause ASBATCH to generate log entries at a specified level of detail.

To execute ASBATCH, you need to log in with an account that is specified separately from the accounts of Authentication Server administrators. You also need to set an option that specifies explicit permission to add, delete, and/or update the data.

Use ASBATCH

Follow these steps to use the ASBATCH utility:

1. If you prefer to not include an administrative login in the command that executes asbatch.exe, then set the following environment variables in the operating environment:

   set ASBATCH_UID=*asbatch-username*
   set ASBATCH_PWD=*asbatch-password*

    **Note:** The ASBATCH password will be available in plaintext. To minimize risk, do not set these variables as defaults, and remove the variables or quit your session after you complete your update.

2. Stop DataFlux Authentication Server and edit the configuration file <*install-path*>\etc\as_serv_aspsql.xml. Add the following option to the bottom of the file to permit access to logins. Specify the type of access that you require.

   <Option name="AdminLoginManagementPolicy">ADD REMOVE UPDATE </Option>

   You can specify any combination of ADD, REMOVE, and UPDATE. When you update a login, you replace the password.

   To enable the AdminLoginManagementPolicy option, the value of the following option in the configuration file is required to be y:

   <Option name="ADMIN_LOGIN_MGMT"> y </Option>

3. Save and close the configuration file.

4. Open a text editor to create your ASBATCH script file. The script file is executed when you run ASBATCH. The script file specifies operators and options for the ASBATCH utility. The name and location of the script file is specified in the command that invokes asbatch.exe. The script file uses either XML or CSV format. To create your script file, see Sample XML and CSV Files for ASBATCH and ASBATCH Operators and Options for XML and CSV Files.

5. Save and close the script file.

6. Optionally create a configuration file that will cause ASBATCH to generate a log file. See Generate a Log File for ASBATCH.

7. Start ASBATCH by specifying options for asbatch.cmd in Windows, or for asbatch in UNIX or Linux. Specify the -help option as follows to display a list of available options:

   ```
   <install-path>\bin> asbatch.cmd -help

   csh> asbatch -help
   ```

   Note: Be sure to specify filenames for the audit file, undo file, and log file.

   To learn more, see ASBATCH Command-Line Options.

8. Review the contents of the audit file and optional log file.

9. To remove the additions that were made by the most recent run of ASBATCH, use the undo file.

10. To preserve security and prevent impersonation, stop DataFlux Authentication Server, open the configuration file as_serv_aspsql.xml, and delete the option AdminLoginManagementPolicy. Save and close the configuration file.

11. In the operating environment, either quit your current session or remove the environment variables ASBATCH_UID and ASBATCH_PWD.

12. Start DataFlux Authentication Server and announce availability to users.

Sample XML and CSV Files for ASBATCH

ASBATCH updates DataFlux Authentication Server's database based on the operators and options that are specified in an XML or CSV file.

The XML or CSV file is opened and read when you invoke asbatch.exe.

Sample XML File

In the following example file in XML format, the first line is required, as are the opening and closing ASBatch tags.

```
<?xml version="1.0" encoding="utf-8"?>
<ASBatch major="major-release-num" minor="minor-num"
delta="delta-num">
   <Add>
      <User name="user-name" login="principal-name"
domain="domain-name"
           desc="description" />
      <Domain name="ASTEST" desc="Used for testing."
           isLogin="false"
           isCase="false"
           isUPN="false"/>
       <Group name="group-name" owner="group-owner"
```

```
desc="Group description" />
   </Add>
   <Update>
      <Domain name="domain-name" desc="New domain name" />
      <Group name="group-name" newname="new-group-name" />
      <Group name="group-name" owner="new-group-owner" />
      <Group name="group-name" desc="New description for
new group" />
      <User name="old-name" newname="new-name" />
        <User name="name" desc="New description for new
name" />
      <User filter="description='user description'"
desc="New description" />
      <User name="name" isEnabled="false" />
      <User filter="isEnabled='true'" isEnabled="false" />
       <User name="name">
         <Add>
            <Login name="principal-name" domain="domain-
name" password="password" />
         </Add>
         <Remove>
            <Login domain="domain-name" />
         </Remove>
         <Update>
            <Login domain="domain-name" password="new-
password" />
         </Update>
      </User>
      <Group name="group-name">
         <Add>
            <User name="user-name"/>
            <Group name="group-name"/>
         </Add>
         <Remove>
            <User name="user-name"/>
            <Group name="user-group"/>
         </Remove>
      </Group>
   </Update>
   <Remove>
      <User name="name"/>
      <User filter="description='User description'"/>
      <Domain name="dname"/>
      <Domain name="dname" isCascade="TRUE"/>
      <Domain filter="description='Domain description'" />
      <Group name="group-name"/>
      <Group filter="description='Group description'" />
   </Remove>
</ASBatch>
```

Sample CSV File

The following example of a comma-separated file shows the required descriptor on the first line.

```
TITLE:,ASBATCH,major=version-major,minor=version-
minor,delta=version-delta
ADD_USER:,name=uname,domain=dname,login=lname,desc=User
description
ADD_DOMAIN:,name=dname,desc=Domain
description,isLogin=TRUE,isCase=FALSE,isUPN=NO
UPDATE_USER:,name=uname,desc=New description
UPDATE_USER:,filter=description='User description',desc=New
description
UPDATE_USER:,name=uname,IsEnabled=FALSE
UPDATE_USER:,filter=description='User
description',IsEnabled=FALSE
UPDATE_DOMAIN:,name=dname,desc=New description
UPDATE_USER_ADD_LOGIN:,name=uname,domain=dname,password=pas
sword
UPDATE_USER_REMOVE_LOGIN:,domain=dname
UPDATE_USER_UPDATE_LOGIN:,name=uname,domain=dname,password=
new-password
REMOVE_USER:,name=uname
REMOVE_USER:,filter=description='User description'
REMOVE_DOMAIN:,name=dname
REMOVE_DOMAIN:,filter=description='Domain description'
REMOVE_DOMAIN:,name=dname,isCascade=TRUE
```

ASBATCH Operators and Options for XML and CSV Files

Using an XML file, you can add, update, and remove users, groups, and domains. Using a CSV file, you can add, update, and remove users and domains. Use the Administration riser to maintain shared logins.

For information on valid values for options that take boolean values, see Valid Values for Boolean Options in ASBATCH.

Operator - Description	Options	Option Description and Syntax
Add User	name	Name of new user. XML: <Add> <User name="user-name" login="user-id" domain="domain-name" desc="user-description" /> </Add>

Operator - Description	Options	Option Description and Syntax
		CSV: `ADD_USER:,name=user-name,domain=domain-name,login=user-id,desc=user-description`
	login	User's login for authentication.
	domain	Name of domain that authenticates the login
	desc	User description, 0-256 bytes
	isEnabled	Boolean value of 1 or true enables authentication for the user.

Add Domain	name	Domain name.
		
		XML:
		`<Add>`
		`  <Domain name="domain-name"`
		`  desc="domain-description"`
		`isLogin="boolean"`
		`  isCase="boolean" isUPN="boolean"`
		`/>`
		
		CSV:
		`ADD_DOMAIN:,name=domain-name,desc=domain-description,isLogin=boolean,isCase=boolean,isUPN=boolean`

	desc	Domain description, 0-256 bytes
	isLogin	Boolean value 1 or true indicates the default domain, user enters login only.
	isCase	Boolean value 1 or true indicates a case-sensitive domain name. A value of 0 or false indicates an all-caps domain name.
	isUPN	Boolean value 1 or true indicates up-level domain (login@domain). A value of 0 or false indicates a down-level domain (domain\login).

Add Group - add a new group, in XML only.	name	Group name.
		
		XML:
		`<Add>`
		`  <Group name="group-name"`
		`owner="owner-name"`
		`  desc="group-description" />`
		`</Add>`

	owner	Existing user name of group owner.
	desc	Group description, 0-256 bytes.

Operator - Description	Options	Option Description and Syntax

Remove User, Remove Domain, Remove Group - remove existing entry. Remove group is available in XML only.	name	Name of user, domain, or group to be removed. Use name or filter but not both.
		
		XML:
		`<Remove>`
		`  <User|Domain|Group`
		`  filter="option-name='option-value'"/>`
		`</Remove>`
		
		CSV:
		`REMOVE_GROUP:,filter=match-option-name='match-option-value',isCascade=True`

	filter	Removes multiple users, domains, or groups, based on matching option values.
	isCascade	For Remove Groups, 1 or True indicates that any users who belong to the removed group will have that group membership removed. When isCascade=False, the group remove operation fails if any users are still members of that group.

Update User - change descriptions and/or enablement for existing user(s).	name	Name of user.
		
		XML 1 of 3 -for one user, change description and/or enablement):
		`<Update>`
		`  <User name="user-name"`
		`  isEnabled="boolean-auth-enable-or-disable"`
		`  desc="new-description" />`
		`</Update>`
		
		XML 2 of 3 - change description and/or enablement for all users with matching strings in the description option:
		`<Update>`
		`  <User filter="description='desc-match-string'"`
		`  desc=”new-description"`
		`  isEnabled=boolean />`
		`</Update>`
		
		XML 3 of 3 (change descriptions for all matching enablements):
		`<Update>`
		`  <User filter="isEnabled='boolean'"`
		`  desc=”new-description" />`
		`</Update>`

Operator - Description	Options	Option Description and Syntax
		CSV 1 of 3: UPDATE_USER:,name=user-name,isEnabled=boolean,desc=new-desc CSV 2 of 3: UPDATE_USER:,filter=description='desc-match-string',desc=new-description CSV 3 of 3: UPDATE_USER:,filter=isEnabled=boolean,desc=new-value
	desc	Description of user, 0-256 bytes.
	filter	For matching user options, make the specified change.
	isEnabled	Boolean value of 1 or true enables authentication for the user.
Update User Add Login - add login to existing user.	login	User ID for authentication. XML: <Update> <User name=existing-user-name> <Add> <login=new-login domain=new-domain password=new-pwd /> </User> </Update> CSV: UPDATE_USER_ADD_LOGIN:,name=existing-user-name,login=new-login,domain=new-domain,password=new-pwd
	domain	Domain used for authentication.
	password	Password that accompanies the user ID.
Update User Update Login - change existing login, without changing the user ID.	name	Name of an existing login. XML: <Update> <User name="username" domain="new-domain" password="new-password" /> </Update> CSV: UPDATE_USER_UPDATE_LOGIN:,name=existing-

Operator - Description	Options	Option Description and Syntax
		user-name,domain=new-domain,password=new-pwd
	domain	New domain value for existing login.
	password	New password for existing login.
Update User Remove Login - remove a login from an existing user.	domain	Domain of login to be removed. XML: <Update> <User name=existing-user-name> <Remove> <Login domain=domain-name/> </Remove> </User> </Update> CSV: UPDATE_USER_REMOVE_LOGIN:name=existing-user-name,domain=domain
Update Domain - change the description of a domain.	name	Name of domain to be updated. XML: <Update> <Domain name=existing-domain-name desc=new-domain-description /> </Update> CSV: UPDATE_DOMAIN:,name=existing-domain-name, desc=new-domain-description
	desc	New description for domain, 0-256 bytes.
Update Group - change the name, description, or owner of an existing group, in XML only.	name	Name of group to be updated. XML: <Update> <Group name="existing-group-name" desc="new-description" newname="new-group-name" owner="new-group-owner" </Group> <Update />
	desc	New group description, 0-256 bytes.
	newname	New group name
	owner	New group owner.

Operator - Description	Options	Option Description and Syntax
Update Group Add or Remove - add or remove a user or group from an existing group, in XML only.	name	Name of group to be updated, name of user or group to be added or removed. XML: <Update> <Group name="group-name"> <Add | Remove> <User name="user-name" /> <Group name="group-name" /> </Add | Remove> </Group> </Update>
	user	Add or remove a user.
	group	Add or remove a group.

Valid Values for Boolean Options in ASBATCH

ASBATCH accepts the following values for boolean options:

Valid values for "true:" TRUE, true, YES, yes, 1, T, t, Y, y

Valid values for "false:" FALSE, false, NO, no, 0, F, f, N, n

ASBATCH Command-Line Options

Use the following command-line options to execute asbatch.exe:

-a | --audit *audit-file-path*

Specifies the name and path of the file that ASBATCH generates to record all database changes.

-h | --help *help-file-path*

Displays a list of available command line options and exits.

-i | --input *path-to-XML-or-CMV-file*

Specifies the name and location of the XML or CSV file that contains ASBATCH operators and options.

-lc | --log-config-loc *path-to-asbatch-log-config-file*

Specifies the name and location of the file that configures logging for ASBATCH.

-p | --port *auth-server-port-number*

Specifies the port number used by the target Authentication Server.

-pw | password *plaintext-password*

Specifies the password of the user definition that will be used along with the user and domain options to authenticate ASBATCH. Specify this value only if you choose not to set the environment variable ASBATCH_PWD, as described in Use ASBATCH. This password is displayed in plaintext.

-r | --uri *connection-string*

Specifies an IOM connection string that is used only when the port option is not specified.

-s | --server *server-identifier*

Specifies the name of the host of the target Authentication Server. Valid values are a network name, an IP address, or `localhost`.

-t | --type *type-of-changes-file*

Specifies the format of the input file that specifies database changes. Valid values are XML or CSV. XML is the default.

- us | --user *user-name*

Specifies the name of the user defintion that will be used to authenticate ASBATCH, along with the values of the password and domain options. Specify this value only if you choose not to set the environment variable ASBATCH_UID, as described in Use ASBATCH.

-v | --version

Displays ASBATCH version information and exits.

Sample ASBATCH Command

```
<install-path>\bin\asbatch.exe
   --input
c:\ProgramFiles\DataFlux\AuthServer\server1\etc\XMLfile1.xml
   --audit asboutfile.xml
   --port 21030
   --server localhost
   --user LOCAL\ADMIN -password ADMIN_PASS
   --type XML
   --logconfigloc <install-path>\etc\asbatch_log4sas.xml
```

Use the ASBATCH Audit File and Undo File

When you run ASBATCH, the utility generates an audit file and an undo file. The audit file records all of the changes that ASBATCH makes to DataFlux Authentication Server's transactional database. The undo file enables you to remove new entries that were added by the last run of ASBATCH.

The names and paths of the audit and undo files are specified by the `audit` option of the command that executes asbatch.exe. The name of the audit file determines the name of the undo file. The name of the undo file ends with u.xml.

To remove new additions with the undo file, edit the `input` option in the previous ASBATCH command. Replace the name and path of the input XML or CSV file with the name and path of the undo file, and then execute the command. ASBATCH generates a new audit to confirm the removals.

The undo file does not replace database entries that were modified or removed. To see a list of modifications and removals, refer to the audit file.

Use the ASBATCH Log File

Default Log Configuration

The default log file is named asbatch.log. The default path for that file is one of the following:

```
<install-path>\var\log\asbatch.log
```

The default path and name of the ASBATCH log configuration file is as follows:

```
<install-path>/etc/asbatch_log.xml
```

Changing the Default Logging Behavior

To change the default logging behavior of ASBATCH, edit your existing log configuration file or create a new log configuration file. The new log configuration file points to a new log file in a different location on the local host. For information on setting logging levels, see About Appenders and Loggers.

Initial ASBATCH Log Configuration File

The following XML content is delivered in asbatch_log.xml when you install ASBATCH:

```
<?xml version="1.0"?>

<log4sas:configuration
xmlns:log4sas="http://www.sas.com/rnd/Log4SAS/">

   <appender name="LOG" class="FileAppender">
      <param name="File"
value="/home/eredwa/asbatch/asbatch.log"/>
      <param name="ImmediateFlush" value="true"/>
      <param name="Append" value="false"/>
      <layout>
           <param name="ConversionPattern" value="%d %-5p [%t] %u
%c - %m (%F@%L)"/>
      </layout>
```

```
   </appender>

 <root>
      <level value="ERROR"/>
      <appender-ref ref="LOG"/>
 </root>

</log4sas:configuration>
```

About Users, Groups, Domains, Logins, and Shared Logins

- Overview
- Domains
- Logins
- Users
- Groups
- Shared Logins

Overview

Users, groups, domains, logins, and shared logins are records in a transactional database that is maintained by DataFlux Authentication Server. By default, the transactional database resides on the host of DataFlux Authentication Server.

Each instance of DataFlux Authentication Server maintains a distinct transactional database, and records are not shared between databases.

As an alternative to the default configuration, you can configure DataFlux Authentication Server to maintain users, groups, domains, logins, and shared logins in Oracle. Using Oracle, multiple DataFlux Authentication Servers can share a single set of system tables, with available TCP optimizations between servers. For further information about using Oracle to store authentication objects, see Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins.

Database records are created, displayed, edited, and deleted using the **Administration** riser in DataFlux Data Management Studio. You can also update the database in batch using an XML or CMV file and the ASBATCH utility.

Access to users, groups, domains, logins, and shared logins depends on your role. Passwords cannot be displayed regardless of your role. Administrators can add, edit, and delete all records other than logins, and can update the passwords of shared logins. Owners and managers of groups and shared logins can add and delete members. Users can see their logins. Everyone can see all users and groups.

DataFlux clients and servers query the transactional database for user and group membership information, as part of the authorization process.

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

Note that when you create or rename records, DataFlux Authentication Server may accept special characters that are not accepted in the operating environment. Be sure to follow the naming conventions of your operating environment.

Domains

A domain is named collection of logins that share an authentication provider. The DataFlux Authentication Server defines domains so that users can connect to DataFlux Data Management Server, SAS Federation Server, DataFlux Web Studio Server, and relational database servers in those domains.

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

If a user logs in without a domain, a default domain is supplied. The default domain comes from the PrimaryProviderDomain option. If that option has no value, then DataFlux Authentication Server uses host authentication.

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

Logins

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

Inbound logins - are sent from DataFlux Data Management Studio to DataFlux Authentication Server to verify the identity of the user at client start or when the user connects to DataFlux Authentication Server. Inbound logins are also used to establish connections to SAS or DataFlux server software such as DataFlux Data Management Server or SAS Federation Server. When a user requests a connection to a SAS or DataFlux server, DataFlux Authentication Server authenticates the user's inbound login in the server's domain. If the user authenticates successfully, then DataFlux Authentication Server notifies the SAS DataFlux server, and the SAS or DataFlux server accepts the user's connection.

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

Oracle login - if you choose to store your users, groups, domains, logins, and shared logins in Oracle, DataFlux Authentication Server uses an outbound Oracle login to connect to that database, as described in Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins.

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

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

Logins can be shared by multiple instances of DataFlux Authentication Server if those servers share a single set of system tables in Oracle. Otherwise, each DataFlux Authentication Server maintains a separate set of logins.

Users

User definitions, or simply "users", are database entries that associate a platform name with one or more logins in the operating environment. Each login consists of a unique combination of a domain, user ID, and password.

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

User passwords are not displayed. By default, administrators cannot add or delete logins, or change passwords in a user definitions.

Groups

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

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

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

Groups can be members of other groups.

Groups can be designated as consumers of shared logins.

Groups can be designated as managers of shared logins.

Two top-level groups, PUBLIC and USERS, are continuously maintained by DataFlux Authentication Server. The PUBLIC group includes all users who successfully authenticate in the host operating environment of DataFlux Authentication Server. PUBLIC users are not required to have a registered user definition in DataFlux 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 DataFlux 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 have read access to the group membership information that is displayed in DataFlux Data Management Studio. You can remove this read access by changing the value of the option PublicUserGroupManagementPolicy.

Shared Logins

A shared login is a collection of users and groups that is associated with an account on a relational database. DataFlux Authentication Server enables the consumers of shared logins to connect to relational databases using the credentials that are stored with the shared logins in the transactional database.

When a user (or job, which is associated with a user) connects to SAS Federation Server, that user can then request a connection to a relational database. SAS Federation Server passes that request to DataFlux Authentication Server. In response, DataFlux Authentication Server determines whether the user is a consumer of a shared login for the requested database. If the user is a consumer, then DataFlux Authentication Server sends the credentials of the relational database account (from the shared login) to SAS Federation Server. The client uses the supplied credentials (known as an outbound login) to open a connection to the database. Users see no information about the outbound login.

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

The passwords for outbound logins cannot be displayed.

Administrators can add and delete shared logins and add and delete consumers of shared logins. Administrators cannot delete or replace the outbound login.

Each shared login has a designated owner. The designated owner can be a user or a group. The owner has full access to the shared login, including the ability to read and replace the outbound user ID and password. The owner can also change his login and reassign his or her ownership to another user.

Shared logins have designated managers as well as owners. Managers can be users or groups. Managers can add and delete consumers and read the outbound login. Users that are designated as managers can add and delete memberships in the shared login. Manager logins are configured on SAS Federation Server to read the outbound login without revealing that login to the connecting client.

Each shared login has a required key value. You can assign the same key to multiple shared logins. Keys are used by the Shared Login Manager on SAS Federation Server. The Shared Login Manager uses a login and key value to gain access to one or more shared logins. The Shared Login Manager uses the accessible shared logins to make connections to relational databases.

Appendix 1: PROC ASEXPORT Syntax Reference

Overview: ASEXPORT Procedure

PROC ASEXPORT migrates metadata from DataFlux Authentication Server to SAS Metadata Server. The procedure supports direct object migration through the SAS Open Metadata Interface. It also supports the creation of an export package that is compatible with PROC METADATA.

The following steps illustrate the workings of the ASEXPORT procedure:

1. The META= connection and filter parameters are used to connect to SAS Metadata Server.
2. The AS= connection and filter parameters are used to connect to DataFlux Authentication Server.
3. The MATCH, MATCH SINGLETON, ADD, and DELETE statements use these working sets to build up the mappings between DataFlux Authentication Server and SAS Metadata Server objects.
4. The LIST statement lists them.
5. The EXPORT statement exports them to a file, forwards them to SAS Metadata Server, or both.
6. The file created by the EXPORT statement can be used directly by the METADATA procedure as its IN= procedure option.

Concepts: ASEXPORT Procedure

The matches between DataFlux Authentication Server and SAS Metadata Server objects are managed internally by the relationships in the tabular data represented in the following three schemas:

- AS Schema
- META Schema
- X Schema

Note that the maximal set of working objects available for export is controlled by the various filters specified on the procedure statement.

AS Schema

The AS schema includes the working set of DataFlux Authentication Server objects that are extracted using the initial filters specified in the AS(FILTER) procedure suboptions. The AS schema is a one-to-one tabular snapshot of Authentication Server objects read in using the META/FILTER options.

This schema consists of the following tables:

DOMAINS

extracted using the AS(FILTER(DOMAINS)) suboption.

USERS

extracted using the AS(FILTER(USERS)) suboption.

GROUPS

extracted using the AS(FILTER(GROUPS)) suboption.

LOGINS

extracted using the AS(FILTER(LOGINS)) suboption.

The AS schema contains a representation of DataFlux Authentication Server objects that are currently in the working set of source objects. These objects are available for selection into the working set of export mappings in the X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP tables. The schema is displayed in the following sample:

```
create table AS.DOMAINS
(

   NAME NVARCHAR(256) NOT NULL,
   NAME_N NVARCHAR(256) NOT NULL,
   "DESC" NVARCHAR(256) NOT NULL,
      IS_CS_USERID NCHAR(1) NOT NULL,
   IS_DQ_USERID NCHAR(1) NOT NULL,
    IS_UPN_USERID NCHAR(1) NOT NULL
);
create table AS.USERS
 (
   ID NCHAR(32) NOT NULL,
   NAME NVARCHAR(256) NOT NULL,
   NAME_N NVARCHAR(256) NOT NULL,
   "DESC" NVARCHAR(256) NOT NULL,
   ENABLED NCHAR(1) NOT NULL
);
create table AS.LOGINS (
   FQLN NVARCHAR(256) NOT NULL,
   DOMAIN_N NVARCHAR(256) NOT NULL,
   NAME NVARCHAR(256) NOT NULL,
   USER_ID NCHAR(32) NOT NULL
);
```

```
create table AS.GROUPS (
   ID NCHAR(32) NOT NULL,
   NAME NVARCHAR(256) NOT NULL,
   NAME_N NVARCHAR(256) NOT NULL,
   "DESC" NVARCHAR(256) NOT NULL,
   OWNER_ID NCHAR(32)
);
```

META Schema

The META schema includes the working set of SAS Metadata Server objects extracted using the initial filters specified in the META(FILTER) procedure suboptions.

This schema consists of the following tables:

DOMAINS

extracted using the META(FILTER(DOMAINS)) suboption.

USERS

extracted using the META(FILTER(GROUPS)) suboption.

GROUPS

extracted using the META(FILTER(GROUPS)) suboption.

LOGINS

extracted using the META(FILTER(LOGINS)) suboption.

The META schema contains a representation of SAS Metadata Server objects currently in the working set of destination objects. These objects are available for selection into the working set of export mappings in the X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP tables. The schema is displayed in the following sample:

```
create table META.DOMAINS
 (
   ID NCHAR(17) NOT NULL,
   AS_ID NVARCHAR(128),
   NAME NVARCHAR(60) NOT NULL,
   NAME_N NVARCHAR(60) NOT NULL,
   "DESC" NVARCHAR(200) NOT NULL,
       OUTBOUND_ONLY NCHAR(1) NOT NULL,
    TRUSTED_ONLY NCHAR(1) NOT NULL
);
create table META.USERS (
   ID NCHAR(17) NOT NULL,
```

```
   AS_ID NCHAR(32),
   NAME NVARCHAR(60) NOT NULL,
   NAME_N NVARCHAR(60) NOT NULL,
   "DESC" NVARCHAR(200) NOT NULL
);
create table META.LOGINS (
   ID NCHAR(17) NOT NULL,
   AS_ID NVARCHAR(128),
   FQLN NVARCHAR(128) NOT NULL,
   NAME NVARCHAR(60) NOT NULL,
   "DESC" NVARCHAR(200) NOT NULL,
   DOMAIN_ID NCHAR(17) NOT NULL,
   OWNER_ID NCHAR(17) NOT NULL,
    TRUSTED_ONLY NCHAR(1) NOT NULL
);
create table META.GROUPS (
   ID NCHAR(17) NOT NULL,
   AS_ID NVARCHAR(32),
   NAME NVARCHAR(60) NOT NULL,
   NAME_N NVARCHAR(60) NOT NULL,
   "DESC" NVARCHAR(200) NOT NULL
);
```

X Schema

The X schema includes normalized content, views, and joined result sets produced from matches between objects represented in the AS and META schemas.

This schema consists of the following tables or views:

audit-file-path

contains the working set of (AS:Domain, OMSOBJ:AuthenticationDomain) domain mappings currently queued for export.

USER_MAP

contains the working set of (AS:Group, OMSOBJ:IdentityGroup) group mappings currently queued for export.

GROUP_MAP

contains the working set of (AS:Group, OMSOBJ:IdentityGroup) group mappings currently queued for export.

AS_LOGINS_N

contains views of AS.LOGINS with additional FQLN_N column where the column contains a normalized fully qualified login name that can be matched with logins in MS.LOGINS. Login name qualification and normalization is governed by the naming rules inferred from the AS.DOMAINS(IS_CS_USERID, IS_DQ_USERID, IS_UPN_USERID) columns.

MS_LOGINS_N

contains views of MS.LOGINS with additional FQLN_N column where the column contains a normalized fully qualified login name that can be matched with logins in AS.LOGINS. Login name qualification and normalization is governed by the naming rules inferred from the AS.DOMAINS(IS_CS_USERID, IS_DQ_USERID, IS_UPN_USERID) columns.

The X schema contains the working set of export mappings from DataFlux Authentication Server to SAS Metadata Server. These mappings are used along with utility tables to assist in matching and selection criteria when using the MATCH, MATCH SINGLETON, ADD, and REMOVE statements.

The contents of the schema are listed in following table:

Table or View	Description
X.DOMAIN_MAP	Current working set of domain object mappings.
X.USER_MAP	Current working set of user object mappings.
X.GROUP_MAP	Current working set of group object mappings.
X.AS_LOGINS_N	View of AS.LOGINS with normalized fully qualified login name column, FQLN_N.
X.MS_LOGINS_N	View of META.LOGINS with normalized fully qualified login name, FQLN_N.

The schema is displayed in the following sample:

```
create table X.DOMAIN_MAP (
   AS_NAME NVARCHAR(256) NOT NULL,
   AS_NAME_N NVARCHAR(256) NOT NULL,
   AS_DESC NVARCHAR(256) NOT NULL,
    AS_IS_CS_USERID NCHAR(1) NOT NULL,
    AS_IS_DQ_USERID NCHAR(1) NOT NULL,
    AS_IS_UPN_USERID NCHAR(1) NOT NULL,
    META_ID NCHAR(17),
   META_AS_ID NVARCHAR(128),
   META_NAME NVARCHAR(60) NOT NULL,
   META_NAME_N NVARCHAR(60) NOT NULL,
   META_DESC NVARCHAR(200) NOT NULL,
    META_OUTBOUND_ONLY NCHAR(1) NOT NULL,
    META_TRUSTED_ONLY NCHAR(1) NOT NULL
);
```

```
create table X.USER_MAP (
   AS_ID NCHAR(32) NOT NULL,
   AS_NAME NVARCHAR(256) NOT NULL,
   AS_NAME_N NVARCHAR(256) NOT NULL,
   AS_DESC NVARCHAR(256) NOT NULL,
   AS_ENABLED NCHAR(1) NOT NULL,
   META_ID NCHAR(17),
   META_AS_ID NCHAR(32),
   META_NAME NVARCHAR(60) NOT NULL,
   META_NAME_N NVARCHAR(60) NOT NULL,
   META_DESC NVARCHAR(200) NOT NULL
);
create table X.GROUP_MAP (
AS_ID NCHAR(32) NOT NULL,
AS_NAME NVARCHAR(256) NOT NULL,
AS_NAME_N NVARCHAR(256) NOT NULL,
AS_DESC NVARCHAR(256) NOT NULL,
AS_OWNER_ID NCHAR(32),
META_ID NCHAR(17),
META_AS_ID NCHAR(32),
META_NAME NVARCHAR(60) NOT NULL,
META_NAME_N NVARCHAR(60) NOT NULL,
META_DESC NVARCHAR(200) NOT NULL
);
create view X.AS_LOGINS_N as select AL.*,
case
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FF' then
upper(AL.NAME)
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FT' then
AL.NAME
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'TF' then
upper(AL.NAME) || '@' || AL.DOMAIN_N
else
AL.NAME || '@' || AL.DOMAIN_N
end as "FQLN_N" from AS.LOGINS AL,
X.DOMAIN_MAP_ALL DX
where AL.DOMAIN_N = DX.AS_NAME_N
;
create view X.MS_LOGINS_N as select ML.*,
case
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FF' then
upper(ML.NAME)
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FT' then
ML.NAME
```

```
when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'TF' then
upper(ML.NAME) || '@' || DX.AS_NAME_N
else
ML.NAME || '@' || DX.AS_NAME_N
end as "FQLN_N" from META.LOGINS ML,
X.DOMAIN_MAP_ALL DX
where ML.DOMAIN_ID = DX.META_ID
;
```

Syntax: ASEXPORT Procedure

Requirement: The target SAS Metadata Server and the source DataFlux Authentication Server must be running. Connection information for these servers must be available. A trusted user must also be available/

Tip: PROC ASEXPORT supports RUN-group processing.

See: Open Metadata Interface in *SAS Language Interfaces to Metadata/*

```
PROC ASEXPORT<proc-options>;
MATCH DOMAIN | USER | GROUP / <match-options>;
MATCH SINGLETON DOMAIN | USER | GROUP / <match-options>;
ADD DOMAIN | USER | GROUP / <add-options>; REMOVE DOMAIN | USER |
GROUP / <remove-options>;
 LIST <type-list> / <list-options>;
EXPORT / <export-options>;
UNDO;
```

Statement	Task
PROC ASEXPORT	Export or migrate DataFlux Authentication Server content.
MATCH	Match DataFlux Authentication Server objects with an equivalent SAS Metadata Server objects and place the matches into the working set of export mappings.
MATCH SINGLETON	Match a single DataFlux Authentication Server object with an equivalent SAS Metadata Server object and place the match into the working set of export mappings.
ADD	Add DataFlux Authentication Server objects that are unmatched in the working set of SAS Metadata Server objects to the working set of export mappings.
REMOVE	Remove objects matching the specified criteria from the working set of export mappings.

Statement	Task
LIST	List the current working set of export mappings in the SAS log.
EXPORT	Export the working set of export mappings and clear the mapping tables, X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP.
UNDO	Undo changes to the working set of export mappings. These mappings result from the most recent MATCH, MATCH SINGLETON, ADD, or REMOVE statement that was not followed by a RUN or EXPORT statement.

PROC ASEXPORT Statement

Exports or migrates DataFlux Authentication Server content.

Syntax

PROC ASEXPORT

<METACON=(*SAS-Metadata-Server-connection-arguments*)>
<ASCON=(*DataFlux-Authentication-Server-connection-arguments*)>
<OUT=*fileref*>
<HEADER=NONE | SIMPLE | FULL>
<VERBOSE>
;

Optional Arguments

METACON=(*SAS-metadata-server-connection-arguments*)

Alias: META=

Server connection arguments establish communication with SAS Metadata Server. The metadata system options are used in place of omitted attributes.

FILTER=(*filter-strings*)

is the set of filter strings used to retrieve the working set of SAS Metadata Server objects using a templated GetMetadataObjects query with a XMLSelect search criteria. There is one filter per object type. If a filter is "*" or is omitted, then no subsetting is done when retrieving the objects and all objects of the associated metadata type are retrieved. METACON uses the following filter strings:

DOMAINS="*XMLSelect-search-filter*"

specifies a valid XMLSelect search= string used to match objects of type AuthenticationDomain.

USERS="*XMLSelect-search-filter*"

specifies a valid XMLSelect search= string used to match objects of type Person.

GROUPS="XMLSelect-search-filter"

specifies a valid XMLSelect search= string used to match objects of type IdentityGroup.

Restriction: The GROUPS option is not supported for SAS Business Data Network.

LOGINS="*Select-filter*"

specifies the search criteria used to match objects of type Login. The filter is the value of the Search= attribute of the Logins association specified in the query template.

PASSWORD="password"

is the password for the authenticated user ID on SAS Metadata Server.

Alias: PW= or METAPASS=

PORT=*number*

is the TCP port that SAS Metadata Server listens to for requests. This port number was used to start SAS Metadata Server.

Alias: METAPORT=

Requirement: Do not enclose the port number in quotation marks.

REPOSITORY=*repository-name*

is the name of the repository to use for all SAS Metadata Server requests. The repository name must be foundation.

Alias: METAREPOSITORY=

SERVER="*host-name*"

is the host name or network IP address of the computer that hosts SAS Metadata Server. The value LOCALHOST can be used if the SAS session is connecting to SAS Metadata Server on the same computer.

Alias: METASERVER= or HOST= or IPADDR=

USER="*authenticated-user-ID*"

is an authenticated user ID on SAS Metadata Server. SAS Metadata Server supports several authentication providers.

Alias: METAUSER= or ID= or USERID=

ASCON=(*authentication-server-connection-arguments*)

server connection arguments establish communication with DataFlux Authentication Server.

FILTER=(*filter-strings*)

is the set of filter strings used to retrieve the working set of DataFlux Authentication Server objects. Filter strings are simple name and value pairs or value lists where values are ODBC pattern strings or constants. There is one filter per object type. If a filter is "*" or is omitted, then no subsetting is done when retrieving the objects and all objects of the associated type are retrieved. ASCON uses the following filter strings:

DOMAINS="*domains-filter*"

specifies one of the following domain search filters:

caseSensitivity=TRUE|T|YES|1|FALSE|F|NO|0

selects domains with principal identities that match the specified case sensitivity. The specified value is compared as case insensitive.

description=*domain-description*

selects domains that match the specified description. The specified value is compared as case insensitive and should be quoted.

domain=*domain-name*|(*domain-name1, domain-name2* …)

selects domains with names that match the specified name or a name in the list. Values are compared as case insensitive and can be quoted.

partOfLogin=TRUE|T|YES|1|FALSE|F|NO|0

selects domains that are or are not specified as part of a login. The specified value is compared as case insensitive.

isUPN=TRUE|T|YES|1|FALSE|F|NO|0

selects domains that are or are not specified as a User Principal Name. The specified value is compared as case insensitive.

USERS="*XMLSelect-search-filter*"

specifies one of the following user search filters:

subject=*user-name*|(*user-name1, user-name2* …)

selects users that match the specified name or a name in the list. Values are compared case insensitive and can be quoted.

identifier=*user-identifier*|(*user-identifier1, user-identifier2* …)

selects users that match the specified user ID or a user ID in the list. Values are compared case insensitive.

description=*user-description*)

selects users with descriptions that contain the specified search string. Values are compared case insensitive and should be quoted.

enabled=TRUE|T|YES|1|FALSE|F|NO|0

selects users with the specified state of enablement. descriptions that contain the specified search string.

GROUPS="XMLSelect-search-filter"

specifies one of the following group search filters:

group=*group-name*|(*group-name1, group-name2* …)

selects groups that match the specified name or a name in the list. Values are compared as case insensitive and can be quoted.

identifier=*group-identifier*|(*group-identifier1, group-identifier2* …)

selects groups that match the specified group ID or a group ID in the list. Values are compared as case insensitive.

description=*group-description*)

selects groups with descriptions that contain the specified search string. Values are compared case insensitive and should be quoted.

ownerName=*owner-name*

selects groups with the specified group owner name. Values are compared case insensitive and can be quoted.

Restriction: The GROUPS option is not supported for SAS Business Data Network.

LOGINS="select-filter"

specifies a valid user login search filter. The filter is the value of the Search= attribute of the Logins association specified in the query template. The select filter is a domain name or list of domain names, specified as follows:

domain-name | (domain-name1, domain-name2 …)

PASSWORD="password"

is the password for the authenticated user ID on DataFlux Authentication Server.

Alias: PW=

PORT=number

is the TCP port that DataFlux Authentication Server listens to for requests. This port number was used to start DataFlux Authentication Server.

Requirement: Do not enclose the port number in quotation marks.

SERVER="host-name"

is the host name or network IP address of the computer that hosts DataFlux Authentication Server. The value LOCALHOST can be used if SAS session is connecting to DataFlux Authentication Server on the same computer.

Alias: HOST= or IPADDR=

URI="IOM-uri"

is the complete IOM uri specification of DataFlux Authentication Server. A URI can be specified instead of the server and port.

USER="authenticated-user-ID"

is an authenticated user ID on DataFlux Authentication Server. DataFlux Authentication Server can support several authentication providers.

Alias: ID= or USERID=

OUT=*fileref*

specifies an XML file used by the EXPORT statement to store either the output result returned by SAS Metadata Server or the input that would have been submitted to SAS Metadata Server when exported using the NOFORWARD option. The value must be a fileref, not a pathname. Therefore, you must first submit a FILENAME statement to assign a fileref to a pathname. In most cases, the output XML string is identical to the input XML string, with the addition of the requested values within the XML elements.

If the OUT= argument is omitted and the VERBOSE option is specified, PROC ASEXPORT output is written to the SAS log.

Note: PROC ASEXPORT can generate large XML output. You might need to specify a large LRECL value or RECFM=N (streaming output) to avoid truncation of long output lines.

Note: In the z/OS operating environment, fixed-length records in the XML method call are not supported by PROC METADATA. Specify RECFM=V (or RECFM=N as suggested above) when you create the XML method call.

Alias: OUTFILE=

Restriction: SAS Business Data Network does not support z/OS connections.

HEADER= NONE|SIMPLE|FULL

specifies whether to include an XML header in the output FILE= and OUT= XML files. The declaration specifies the character-set encoding for web browsers and XML parsers to use when processing national language characters in the output XML file. Valid values are defined as follows:

NONE

omits an encoding declaration. Web browsers and parsers might not handle national language characters appropriately.

SIMPLE

inserts an XML header that specifies the XML version number: This is the default value when the HEADER= argument is not specified.

FULL

inserts an XML declaration that represents the encoding that was specified when creating the output XML file. The source for the encoding varies, depending on the operating environment. In general, the encoding value is taken from the ENCODING= option specified in the FILENAME statement, or from the ENCODING= system option.

SAS attempts to use that encoding for the output XML file (and in the XML header). The encoding can vary. A single encoding can have multiple names or aliases that can appear in the XML header. These names might not be valid or recognized in all XML parsers. When generating the encoding attribute in the XML header, SAS attempts to use an alias that will be recognized by Internet Explorer. If the alias is not found, SAS attempts to use a name that will be recognized by Java XML parsers. If the name is not found, SAS uses an alias by which SAS will recognize the encoding. For information about encoding and transcoding, see *SAS National Language Support (NLS): Reference Guide*.

VERBOSE

specifies to print input or output XML strings to SAS log.

Match Statement

Matches DataFlux Authentication Server objects with equivalent SAS Metadata Server objects and places the matches into the working set of export mappings. The

MATCH statement name is followed by the type of object being matched for export. This object type can be DOMAIN, USER, or GROUP. The MATCH statement has two options, CRITERIA= and LOG.

Syntax

```
MATCH <type> / <match-options>;
<CRITERIA="match-criteria">
<LOG>
```

Optional Arguments

CRITERIA="*match-criteria*"

specifies match criteria used to associate DataFlux Authentication Server objects and SAS Metadata Server objects for insertion into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table 1.2 MATCH Entities

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS and META.DOMAINS
USERS	All columns in AS.USERS, META.USERS, X.AS_LOGINS_N, and X.MS_LOGINS_N
GROUPS	All columns in AS.GROUPS and META.GROUPS

The MATCH statement always joins objects using the default matching criteria per object type and then subsets based on the CRITERIA= WHERE clause specified. If omitted, a CRITERIA= value of “1=1” is implied so that no further subsetting occurs.

The following table documents the default match criteria per object type:

Table 1.3 MATCH Criteria

Type	Default CRITERIA= value
DOMAINS	(AS.DOMAINS.NAME_N=META.DOMAINS.NA ME_N) and (META.DOMAINS.AS_ID is NULL)
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and (X.MS_LOGINS_N.FQLN_N=X.AS_LOGINS_N. FQLN_N) and (META.USERS.ID=X.MS_LOGINS_N.OWNER_I D) and (META.USERS.AS_ID is NULL)
GROUPS	(AS.GROUPS.NAME_N=META.GROUPS.NAM E_N) and (META.GROUPS.AS_ID is NULL)

LOG

specifies to print match results in the SAS log.

MATCH SINGLETON Statement

Matches a single DataFlux Authentication Server object with an equivalent SAS Metadata Server object and places the match into the working set of export mappings. The MATCH SINGLETON statement name is followed by the type of object being matched for eventual export. The object type can be DOMAIN, USER, or GROUP. The MATCH SINGLETON statement has two options, CRITERIA and LOG.

Syntax

```
MATCH SINGLETON <type> / <match-singleton-options>;
<CRITERIA="match-criteria">
<LOG>
```

Optional Arguments

CRITERIA="*match-criteria*"

specifies match criteria used to associate a single DataFlux Authentication Server object with a single SAS Metadata Server object for insertion into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table 1.4 MATCH SINGLETON Entities

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS and META.DOMAINS
USERS	All columns in AS.USERS, META.USERS, X.AS_LOGINS_N, and X.MS_LOGINS_N
GROUPS	All columns in AS.GROUPS and META.GROUPS

The MATCH SINGLETON statement always joins objects using the default matching criteria per object type and then subsets based on the user's CRITERIA= WHERE clause. If omitted, a CRITERIA= value of "1=1" is implied such that no further subsetting occurs. Specifying criteria that produces more than one match results in an error, and no additional mapping is queued for export. The following table documents the default match singleton criteria per object type:

The following table documents the default match singleton criteria per object type:

Table 1.5 MATCH SINGLESTON Criteria

Type	Default CRITERIA= value
DOMAINS	The domain is neither already exported nor queued for export in the current working set of export mappings.
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and (X.MS_LOGINS_N.OWNER_ID= META.USERS.ID) and the user is neither already exported nor queued for export in the current working set of export mappings.
GROUPS	The group is neither already exported nor queued for export in the current working set of export mappings.

LOG

specifies to print match results in the SAS log.

ADD Statement

Adds DataFlux Authentication Server objects that are unmatched in the working set of SAS Metadata Server objects to the working set of export mappings. The ADD statement name is followed by the type of object being added for export. The object type can be DOMAIN, USER, or GROUP. The ADD statement has two options, CRITERIA and LOG.

Syntax

```
ADD <type> / <add-options>;
<CRITERIA="match-criteria">
<LOG>
```

Optional Arguments

CRITERIA="*match-criteria*"

specifies criteria used to select DataFlux Authentication Server objects into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table 1.6 ADD Entities

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS
USERS	All columns in AS.USERS, X.AS_LOGINS_N
GROUPS	All columns in AS.GROUPS

The ADD statement always selects AS objects using the default criteria per object type and then subsets based on the CRITERIA= WHERE clause specified. If omitted, a CRITERIA= value of “1=1” is implied such that no further subsetting occurs.

The following table documents the default add criteria per object type:

Table 1.7 ADD Criteria

Type	Default CRITERIA= value
DOMAINS	The domain is neither already exported nor queued for export in the current working set of export mappings.
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and The user is neither already exported nor queued for export in the current working set of export mappings.
GROUPS	The group is neither already exported nor queued for export in the current working set of export mappings.

LOG

specifies to print ADD statement results in the SAS log.

REMOVE Statement

Removes objects matching the specified criteria from the working set of export mappings. The REMOVE statement name is followed by the type of objects being removed from the working set of export mappings. The object type can be DOMAIN, USER, or GROUP. The REMOVE statement has two options, CRITERIA and LOG.

Syntax

REMOVE <*type*> / <*remove-options*>;
<CRITERIA="*match-criteria*">
<LOG>

Optional Arguments

CRITERIA="*match-criteria*"

specifies criteria used to select DataFlux Authentication Server objects into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched:

```
remove domains / criteria="x.domain_map.as_name_n='EURNET'" log;
```

The following table lists those entities per object type:

Table 1.8 REMOVE Criteria

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in X.DOMAIN_MAP
USERS	All columns in X.USER_MAP
GROUPS	All columns in X.GROUP_MAP

The MATCH statement always selects objects mapped for export (those accumulated via the prior MATCH, MATCH SINGLETON, and ADD statements) using the specified criteria. The default CRITERIA= value is always "1=1" such that all export mappings are cleared.

LOG

specifies to print REMOVE statement results in the SAS log.

LIST Statement

Lists the current working set of export mappings in the SAS log. The LIST statement name is optionally followed by the type of objects being listed. The object type can be DOMAIN, USER, or GROUP. The LIST statement has one option, VERBOSE.

Syntax

LIST <*type*> / <*list-options*>;
<VERBOSE>

Optional Argument

VERBOSE

verbose output.

EXPORT Statement

Exports the working set of export mappings and clears the mapping tables, which are X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP. EXPORT. EXPORT has four options, NOFORWARD, VERBOSE, NOVERBOSE, and NEWGROUPSUFFIX.

Syntax

EXPORT <*export-options*>;
<NOFORWARD>
<VERBOSE>
<NOVERBOSE>
<NEWGROUPSUFFIX='*suffix-value*'>

Optional Arguments

NOFORWARD

prevents forwarding of generated XML to the metadata server. When NOFORWARD is specified, the OUT= file will contain SAS Metadata Server input XML. Otherwise, it will contain output response XML.

VERBOSE

specifies to print generated input or output response XML to the SAS log. The VERBOSE option is ignored if the NOVERBOSE is also specified. The VERBOSE option is implied if the procedure's OUT= option is omitted because the log becomes the destination for generated or response XML.

NOVERBOSE

specifies to not print generated input or output response XML to the SAS log. The NOVERBOSE option overrides the VERBOSE option of the procedure and EXPORT statements. The NOVERBOSE option is ignored if the procedure's OUT= option is omitted.

NEWGROUPSUFFIX='*suffix-value*'

allows export of all groups into SAS Metadata Server without matching. Exports objects that have been added and matched, adding the specified string to the name of each new group exported. Care should be taken to avoid producing target group names exceeding 60 characters in length, which is the limit of the Name attribute of IdentityGroup objects.

Details

The EXPORT statement exports all export mappings and clears the mapping tables, which are X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP.

Each new exported object and existing matched object is mapped in metadata using the ExternalIdentities association to an ExternalIdentity object with the following attributes:

- For new objects, ImportType='AuthenticationServer.Import'
- For matched or "tagged" objects, ImportType='AuthenticationServer.Match'
- Context='AuthenticationServer.ID'
- Name='AS:Server/server-name', where the server name consists of the fixed 'AS:Server/' prefix followed by the PUBLIC group identifier of the source DataFlux Authentication Server.

The export process creates mappings between source DataFlux Authentication Server objects and target SAS Metadata Server objects. Multiple DataFlux Authentication Server domains can map to the same SAS Metadata Server AuthenticationDomain object. Other object types map 1:1 in the two stores. However, exports from multiple DataFlux Authentication Server instances can also produce n:1 mappings.

The Name attribute of the ExternalIdentity objects used in the mappings uniquely identifies the source DataFlux Authentication Server.

The EXPORT statement writes SAS Metadata Server output into the file specified by the OUT option or the SAS log if the VERBOSE procedure statement option is specified and the OUT= option is omitted. If the NOFORWARD option is specified, then the statement unconditionally writes input XML into the file specified by the OUT= option or the SAS log if OUT= is omitted. If the OUT= option is specified, then the XML is also written to the SAS log if the EXPORT statement's NOVERBOSE option is omitted and either the procedure's

UNDO Statement

Undoes changes to the working set of export mappings. These changes result from the most recent MATCH, MATCH SINGLETON, ADD, or REMOVE statement that was not followed by a RUN or EXPORT statement.

Syntax

```
UNDO;
```

Example: Exporting from a DataFlux Authentication Server to a SAS Metadata Server

Features:

PROC ASEXPORT statement

MATCH SINGLETON statement

MATCH statement

ADD statement

LIST statement

EXPORT statement

Details

This example demonstrates the following actions:

- specify metadata values
- create explicit singleton matches between these two domains
- auto-match domains by name
- add remaining unmatched domains
- perform explicit user matching

- auto-match users by FQLN
- add remaining unmatched users
- list everything for review
- create an input file (per noforward) for PROC METADATA that we can review

Assign a file reference.

The FILENAME statement assigns a libref to an external SAS library that contains a permanent SAS catalog.

```
filename asx 'C:\TableServer\asexport.xml';
```

Specify metadata values.

```
proc ASEXPORT meta=
                              (
                                  user='username'
password='password'
                                   server='localhost'
                                  port=port_number
                                   repos='repositoryID'
                                   filter=(DOMAINS "*"
                                                 USERS "*"
                                                  GROUPS "*"
                                                 LOGINS
"Login[Domain/AuthenticationDomain
[@OutboundOnly='0']]")
                               )
             as=
                               (
                  server='localhost'
                   user='username'
                   pass='password'
                   port=port_number
                  filter=(DOMAINS "domain=(domain_names)"
                          USERS "enabled=TRUE subject=(ADMUSER,
Shared_Login_Manager, tsadm, 'USER%')"
                          LOGINS "(login IDs for included
domains)")
              )
              verbose
              tracefile='C:\TableServer\asexport.trace'
traceloc=SQL traceflags='319'
              retain
               out=asx
```

```
                ;
```

Create explicit singleton matches between these two domains.

```
match singleton DOMAIN / criteria="as.domains.name_n='LOCAL' and
 meta.domains.name_n='domain_name'" log;
match singleton DOMAIN / criteria="as.domains.name_n='UNIX' and
 meta.domains.name_n='domain_name'" log;
```

Auto-match domains by name.

```
match DOMAINS / log;
```

Add remaining unmatched domains.

```
add DOMAINS / log;
```

Perform explicit user matching.

Attempt at least one user that has a matching Login. Nothing should match.

```
match singleton USER /
criteria="as.users.name_n='SHARED_LOGIN_MANAGER' and
 meta.users.name_n='FEDERATION SERVER SHARED LOGIN MANAGER'" log;
match singleton USER / criteria="as.users.name_n='USER1' and
 meta.users.name_n='TSADM'" log;
match singleton USER / criteria="as.users.name_n='TSADM' and
 meta.users.name_n='TSADM'" log;
```

Auto-match users by FQLN.

```
match USERS / log;
```

Add remaining unmatched users.

```
add USERS / log;
```

List everything for review.

```
list DOMAINS USERS;
```

Create an input file (per noforward) for proc METADATA that we can review.

```
export / noforward noverbose;
```

End processing of PROC ASEXPORT.

```
quit;
```

Appendix 2: Configuration File Reference

The options in DataFlux Authentication Server configuration file as_serv_aspsql.xml are defined as follows.

In the Windows operating environment, the default location of the file is:

```
<install-path>\etc\as_serv_aspsql.xml
```

Note that when you install DataFlux Authentication Server, the default configuration file does not contain default entries for all of the following options.

To specify a value for an option that does not have a default entry, simply add that option as a new entry.

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

Valid Values for Boolean Options

Options such as AddUser and AutoAddDefaultDomain accept Boolean values. The valid values for all Boolean options in this configuration file consist of: TRUE, FALSE, YES, NO, Y, and N. Other Boolean values, such as `y`, `n`, `t`, `f`, `1`, or `0`, are inapplicable.

About ENTITY Declarations

In the configuration file, ENTITY declarations are used to define the transactional database that DataFlux Authentication Server uses to manage users, groups, domains, logins, and shared logins. DataFlux recommends that you retain the default values of these entities.

If you decide to configure your database on Oracle, then you should comment-out the entity declarations for the transactional database, as directed in Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins.

If you use the default transactional database, then you are required to locate the database on DataFlux Authentication Server host and specify a full, non-relative, path as the value of the entity ASPSQL_TRANDBF.

Options in the Configuration File

AdminLoginManagementPolicy
AppendEnv
ASPSQLProvider
AuthenticationProvider
AuthProviderDomain
AutoAddDefaultDomain
AutoAddUsers
Clientencryptionlevel

CredentialsLocation	Dnsname
EncryptFIPS	FIREBIRD
FIREBIRD_LOG	License
Location	MaxConnections
MinConnections	NetworkEncryptAlgorithm
ObjectServerParms	PrependEnv
Port	Primary
PrimaryProviderDomain	PublicUserGroupManagementPolicy
Secondary	SetEnv
SystemCatalog	SystemSchema
SystemUsers	TrustedUsers

AdminLoginManagementPolicy

```
<Option name="AdminLoginManagementPolicy">keywords</Option>
```

All administrators are authorized to add users and create one login per user. By default, only users can change their logins. The AdminLoginManagementPolicy option allows administrators to add logins, delete logins, and update logins. Specify any of the following keywords in any order:

ADD – administrators can add user logins
REMOVE – administrators can remove user logins
UPDATE – administrators can reset user passwords.

Example:

```
<Option name="AdminLoginManagementPolicy">ADD REMOVE
UPDATE</Option>
```

You can specify any combination of ADD, REMOVE, and/or UPDATE.

None of these values are specified by default.

Specifying this option poses a security risk. As such, you should specify this option only when you need to make a specific change. After the change is made, you should remove this option from the configuration file.

AppendEnv

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

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

ASPSQLProvider

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

SystemCatalog - specifies the name of the catalog of DataFlux Authentication Server's database.

SystemSchema - specifies the name of the schema of DataFlux Authentication Server's database.

MinConnections - specifies the minimum number of connections to keep open to DataFlux Authentication Server's database.

MaxConnections - specifies the maximum number of connections to keep open to DataFlux Authentication Server's database. In highly concurrent environments, this value should be raised. Generally speaking, a value of 4 should meet most needs.

CredentialsLocation - specifies the location of the credentials file that is used to connect toDataFlux Authentication Server's database. This option is not required when you use the default transactional database. When you use Oracle, this option can be used to store the encrypted credentials that DataFlux Authentication Server uses to connect to that database. If your site security policy forbids the storage of database credentials, you can enter credentials manually at server startup, or store the credentials in environment variables, as described in Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins.

AuthenticationProvider

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

The AuthenticationProvider option identifies the authentication process in DataFlux Authentication Server. The named process accesses DataFlux Authentication Server's database. ASPSQL is the only valid value.

AuthProviderDomain

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

Or, for two or a maximum of three domains:

```
<Option name="AuthProviderDomain">(provider1:domain1,
     provider2:domain2,
     provider3:domain3)
```

```
</Option>
```

The AuthProviderDomain option associates authentication providers with domains. You can specify a maximum of one authentication provider for each domain, and all domain values must be unique. Also, you can specify a maximum of one authentication provider of each type. Valid values for *authentication-provider* are as follows:

ADIR - specifies that authentication is provided by a Microsoft Active Directory server.

HOSTUSER - specifies that authentication is provided by the host operating system of DataFlux Authentication Server.

LDAP - specifies that authentication is provided by an LDAP directory server.

For Windows, the domain-name value should be a case-sensitive name that is recognized on your network. If a domain name contains spaces, use quotation marks around the name. See also PrimaryProviderDomain.

Adding an authentication provider requires additional configuration. The configuration process depends on the provider type and on the host operating environment of DataFlux Authentication Server. To configure your new authentication provider, see About Authentication Providers.

AutoAddDefaultDomain

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

or

```
<OptionSet name="AutoAddDefaultDomain">
     <Option name="Enabled">boolean</Option>
</OptionSet>
```

For valid values, see Valid Values for Boolean Options.

The AutoAddDefaultDomain option instructs DataFlux Authentication Server to automatically register the host domain if that domain has not already been registered, at server start time, as shown in the following examples:

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

or

```
<OptionSet name="AutoAddDefaultDomain">
     <Option name="Enabled">TRUE</Option>
</OptionSet>
```

When it is enabled, the AutoAddDefaultDomain option creates a domain definition using the value of the option PrimaryProviderDomain. The domain is created only if the PrimaryProviderDomain is mapped to host authentication in the option AuthProviderDomain. For example, on Windows, the AutoAddDefaultDomain option is

valid when you set the PrimaryProviderDomain and AuthProviderDomain options as shown:

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

If the domain of DataFlux Authentication Server was DATAFLUX, then the option values would be:

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

On UNIX and Linux, the following option values are specified in the configuration file by default after the installation of DataFlux Authentication Server:

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

DataFlux Authentication Server uses the UNIXUSER domain during authentication if the supplied login does not specify a domain.

The AutoAddDefaultDomain option is not specified by default. Add the option to the configuration file as needed. To summarize the default behavior, when a domain is not specified, DataFlux Authentication Server uses the PrimaryProviderDomain if AutoAddDefaultDomain is enabled. Otherwise, the server uses the host authentication provider.

The domain object that is created receives attributes based on the following table:

Attributes of the Default Domain

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

AutoAddUsers

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

or

```
<OptionSet name="AutoAddUsers">
     <Option name="Enabled">boolean</Option>
     <Option name="DomainFilter">filter-string</Option>
     <Option name="UserIDFilter">filter-string</Option>
</OptionSet>
```

When enabled, the AutoAddUsers option specifies that Authentication Server automatically adds users as they authenticate based on the domain and user ID that they use to connect. Automatically added users receive a single login composed of the inbound user ID, in the domain specified.


Note: The AutoAddUsers option does not automatically add domains.

By default the value of the Enabled option is TRUE.

The shorthand Option element form activates the auto-add feature for all users in all domains. The longer OptionSet element activates the auto-add feature for specified users in specified domains.

For example, to automatically add user definitions for any and all users who login from the BOULDERNT and OURCO domains, add the following specification to the configuration file:

```
<OptionSet name="AutoAddUsers">
     <Option name="DomainFilter">BOULDERNT OURCO</Option>
</OptionSet>
```

The values of the UserIDFilter and DomainFilter options are case-insensitive when they are compared against the logins of connecting users.

Filter option values may contain the wildcard characters, % (percent) and _ (underscore), matching zero or more characters or any one character, respectively.

Clientencryptionlevel

```
<Option name="ObjectServerParms">
     clientencryptionlevel=none | credentials | everything
</Option>
```

This parameter of the ObjectServerParms option determines how DataFlux Authentication Server data is encrypted for transmission on your network. Valid values include:

none - nothing is encrypted.

credentials - login credentials are encrypted. These credentials are used to authenticate to DataFlux Authentication Server.

everything - all client-server network communications are encrypted. This is the default value.

Dnsname

```
<Option name="ObjectServerParms">
     dnsname=dns-ip-address
</Option>
```

This parameter of the ObjectServerParms option specifies the IP address of the Domain Name Servers that is used for authentication. Specify this parameter when the operating environment of DataFlux Authentication Server uses Internet Protocol Version 6 (IPv6) addresses.

EnableFIPS

```
<Option name="EncryptFIPS">FALSE</Option>
```

This option enables DataFlux Authentication Server to run in compliance with Federal Information Processing Standard 140-2. The default value is FALSE. After you install DataFlux Authentication Server with the DataFlux Secure software, the configuration process can be directed to change the value to TRUE.

FIREBIRD and FIREBIRD_LOG

```
<OptionSet name="SetEnv">
     <Option name="FIREBIRD"><install-path>\lib\fbembed</Option>
     <Option name="FIREBIRD_LOG"><install-path>\var\log</Option>
</OptionSet>
```

The FIREBIRD environment variable specifies the installation path of the default transactional database. The transactional database is required to be stored on the host of DataFlux Authentication Server.

You can reconfigure DataFlux Authentication Server to use an Oracle database rather than the transactional database, as described in Configure Oracle to Store Users, Groups, Domains, Logins, and Shared Logins. The Oracle database does not use the options FIREBIRD or FIREBIRD_LOG.

The FIREBIRD_LOG environment variable identifies the directory that stores the log files that are generated by the transactional database.

In the Windows operating environment, the default values for FIREBIRD and FIREBIRD_LOG are set in the configuration file by DataFlux Authentication Server's installation process. In the UNIX and Linux operating environments, DataFlux Authentication Server's startup script dasadmin sets the environment variable FIREBIRD_LOG.

License

```
<OptionSet name="License">
     <OptionSet name="Primary">
          <Option name="Provider">SAS</Option>
          <Option name="Location">depot-path</Option>
     </OptionSet>
</OptionSet>
```

The License option provides information about the types of license checks that are performed by DataFlux Authentication Server. The value of the Provider option is SAS, and uppercase is required. The value of the Location option specifies the path to the SAS SETINIT. The default path is as follows:

depot-path\sid_files*site-filename*.txt

In the Windows operating environment, a typical entry for the Location option is as follows:

```
<Option name="Location">C:\my-user\Depot_release-week\sid_files\
     DMPversion_09CRZD_70142972_Win_X64_Wrkstn_Srv.txt</Option>
```

The default value for the License option is set into the configuration file when you install DataFlux Authentication Server.

Each product receives a unique "site" file, as specified in your Software Order E-Mail. Multiple site files can share a single sid-files directory.

NetworkEncryptAlgorithm

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

The NetworkEncryptAlgorithm option specifies the encryption algorithm that is used to encrypt network data transfers between clients and DataFlux Authentication Server. Valid values for this option are SASProprietary and AES. The default SASProprietary encryption algorithm uses 56-bit keys. You can upgrade to the 256-bit keys of the AES encryption algorithm by installing the DataFlux Secure software with DataFlux Authentication Server. The configuration process for DataFlux Secure changes the value of this option to AES. For more information, see Configure Encryption.

ObjectServerParms

```
<Option name="ObjectServerParms">
     auth-server-parameter-options
</Option>
```

The ObjectServerParms option specifies a series of DataFlux Authentication Server parameters. The parameters can be specified in any order. The parameters are delimited by blank spaces.

PrependEnv

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

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

Port

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

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

PrimaryProviderDomain

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

The PrimaryProviderDomain option specifies the domain that is used first by default when a user submits credentials without a domain. The value of the option must be a domain name that is included in the AuthProviderDomain option set.

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

PublicUserGroupManagementPolicy

```
<Option name="PublicUserGroupManagementPolicy">READ</Option>
```

The PublicUserGroupManagementPolicy option specifies the access permission that is applied to members of the PUBLIC group. By default, members of the PUBLIC group have read access to the group membership information that is displayed in DataFlux Data Management Studio. Groups are displayed after PUBLIC members connect to DataFlux Authentication Server and select the **Groups** riser. To remove read access, either add comment characters around the option above, remove the option text entirely, or remove the READ value. READ is the only valid value for this option.

SetEnv

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

The SetEnv option defines environment variables and assigns values to those variables. Use this option to set environment variables that are required for Active Directory and LDAP authentication on the host of DataFlux Authentication Server. See the following options FIREBIRD and FIREBIRD_LOG. See also the environment variables that are set for AuthProviderDomain.

SystemUsers

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

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

TrustedUsers

```
<OptionSet name="TrustedUsers">
     <Option name="Account">domain\userid1</Option>
     <Option name="Account">domain\userid2</Option>
</OptionSet>
```

The TrustedUsers option set defines the user accounts that are privileged to act on behalf of other users, for the purpose of retrieving information from DataFlux Authentication Server. Trusted users are authorized to read DataFlux Authentication Server data, but not to add, modify, or delete that data.

 **Note:** Because of their differing permissions, trusted users should not also be system users.

Trusted user accounts enable SAS Federation Server to query relational databases. To execute a relational query, SAS Federation Server must first obtain group membership information from DataFlux Authentication Server for the user who defined the query. This is necessary because the user who defined the query must be authorized on SAS Federation Server to submit the query and store retrieved data. The user who requested the query only needs permission to make the request.

If the defining user is authorized, then SAS Federation Server connects to the relational database and submits the query. The relational query is authenticated and authorized on the relational database using a shared login that SAS Federation Server obtains from DataFlux Authentication Server.

Appendix 3: Legal Notices

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 3.1

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.

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.

Canada Post Copyright Disclosure

The Data for areas of Canada includes information taken with permission from Canadian authorities, including: © Her Majesty the Queen in Right of Canada, © Queen's Printer for Ontario, © Canada Post Corporation, GeoBase®, © Department of Natural Resources Canada. All rights reserved.

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 [as used in DataFlux clients and servers.]

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.

Informatica Address Doctor Copyright Disclosure

AddressDoctor® Software, © 1994-2015 Platon Data Technology GmbH

Loqate Copyright Disclosure

The Customer hereby acknowledges the following Copyright notices may apply to reference data.

Australia: Copyright. Based on data provided under license from PSMA Australia Limited (www.psma.corn.au)

Austria: © Bundesamt für Eich- und Vermessungswesen

Brazil: Conteudo firnecido por MapLink. Brazil POIs may not be used in publically accessible, internet-based web sites whereby consumers obtain POI data for their personal use.

Canada:

Copyright Notice: This data includes information taken with permission from Canadian authorities, including © Her Majesty, © Queen's Printer for Ontario, © Canada Post, GeoBase ®.

End User Terms: The Data may include or reflect data of licensors including Her Majesty and Canada Post. Such data is licensed on an "as is" basis. The licensors, including Her Majesty and Canada Post, make no guarantees, representation, or warranties respecting such data, either express or implied, arising by law or otherwise, including but not limited to, effectiveness, completeness, accuracy, or fitness for a purpose.

The licensors, including Her Majesty and Canada Post, shall not be liable in respect of any claim, demand or action, irrespective of the nature of the cause of the claim, demand or action alleging any loss, injury or damages, direct or indirect, which may result from the use or possession of the data or the Data. The licensors, including Her Majesty and Canada Post, shall not be liable in any way for loss of revenues or contracts, or any other consequential loss of any kind resulting from any defect in the data or in the Data.

End User shall indemnify and save harmless the licensors, including Her Majesty the Queen, the Minister of Natural Resources of Canada and Canada Post, and their officers, employees and agents from and against any claim, demand or action, irrespective of the nature of the cause of the claim, demand or action, alleging loss, costs, expenses, damages, or injuries (including injuries resulting in death) arising out of the use of possession of the data or the Data.

Croatia, Cyprus, Estonia, Latvia, Lithuania, Moldova, Poland, Slovenia, and/or Ukraine: © EuroGeographics

France: source: Géoroute® IGN France & BD Carto® IGN France

Germany: Die Grundlagendaten wurden mit Genehmigung der zuständigen Behörden entnommen

Great Britain: Based upon Crown Copyright material.

Greece: Copyright Geomatics Ltd.

Hungary: Copyright © 2003; Top-Map Ltd.

Italy: La Banca Dati Italiana è stata prodotta usando quale riferimento anche cartografia numerica ed al tratto prodotta e fornita dalla Regione Toscana.

Norway: Copyright © 2000; Norwegian Mapping Authority

Portugal: Source: IgeoE – Portugal

Spain: Información geográfica propiedad del CNIG

Sweden: Based upon electronic data © National Land Survey Sweden.

Switzerland: Topografische Grundlage © Bundesamt für Landestopographie.

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

SQLite Copyright Disclosure

Sun Microsystems Copyright Disclosure

TomTom Copyright Disclosure

USPS Copyright Disclosure

VMware Copyright Disclosure

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 DataFlux 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 DataFlux 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.