Logi Ad Hoc Reporting
Troubleshooting Authentication Failure

Standard Authentication

Version 11
Last Updated: March 2014

Table of Contents

Troubleshooting “Standard” Authentication

This guide tries to address the most common user authentication problems in Logi Ad Hoc when configured to use the “standard” security model. Some of the concepts apply to all of the security models (“NT”, “Session”, “Database” and “SecureKey”), however, these will be specifically covered in other guides.

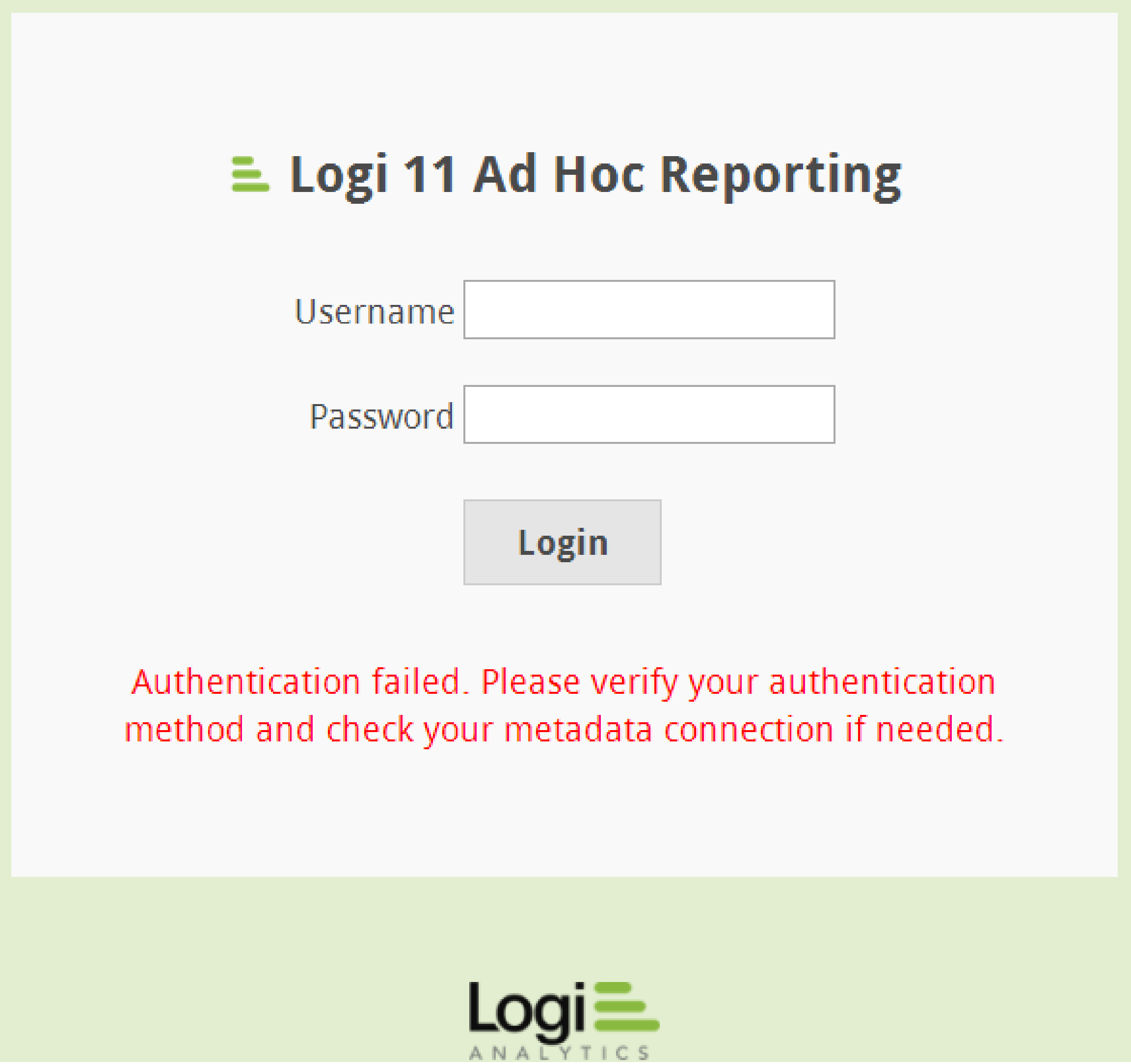
The “Standard” authentication model is the default for all new instances created by the Management Console for Logi Ad Hoc.

Many of the causes for an authentication failure are simple configuration problems and usually come down to the content of the metadata database or the connection to the metadata database. It is expected that the System Administrator will have knowledge of User configuration via the Ad Hoc interface and Application configuration via the Management Console. There is no attempt in this guide to provide “how-to” instructions.

Consult *the Management Console Usage Guide* or the *System Administration Guide* for detailed administration instructions.

What Is an Authentication Failure?

Very simply, if the credentials supplied via the login page do not grant access to the Ad Hoc application you have an authentication failure. The following picture is the typical result.



Authentication failed. Please verify your authentication method and check your metadata connection if needed.

Troubleshooting

The following table can be used as a brief troubleshooting guide. The entries in the table are organized according to their frequency of occurrence. Each of the entries in the table is described in greater detail in later sections of this document.

Quick Troubleshooting Guide

Brief Cause	Logic	Things to Check
Invalid Credentials	The Username and Password do not exist in the metadata database	Try to login with “Admin/password”. If this permits access, verify the User credentials that failed
No reporting database for the User	At least one of the User’s roles must grant access to a reporting database	Login with “Admin/password” and adjust the User’s roles to access a reporting database
No Reporting Database	There must be a reporting database schema in the metadata	If the “Admin/password” credentials do not allow access, use the Management Console to import the schema from a reporting database
Metadata Access	Ad Hoc needs to have “administrator” access to a metadata database	Using the Management Console, verify that the metadata connection string is still valid. Verify that the credentials supplied in the metadata connection string grant administrator privileges to the metadata database Is the DBMS online?
Folder Permissions	The Network Service and machine/ASPNET accounts should have Full control of various folders and files	Check the properties of the _Definitions/_Reports folder (as a test). The simplest remedy for this is to set the account permissions on the root folder of the Ad Hoc instance

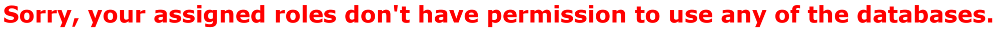
Invalid Credentials

This is the most frequent reason that users can't be authenticated. Usually it's a typographical error in the username or password, but it is possible that the user has forgotten their credentials. The Administrator can verify the username and reset the user's password.

Note: *For case-sensitive metadata databases, the username must match precisely the name stored in the metadata database. In other words, "Admin" and "admin" are not the same.*

No Reporting Database for the User

A user will not be granted access if their assigned role(s) do not grant reporting privileges to at least one reporting database. The following message will be issued on the login page:



Sorry, your assigned roles don't have permission to use any of the databases.

The Administrator should use the Ad Hoc user interface to either associate a reporting database to one of the user's roles or create a role that grants access to a reporting database and assign it to the user.

No Reporting Database

Ad Hoc requires at least one reporting database to be connected to the Ad Hoc instance and for some part of the schema to be imported into the metadata database for any user to be able to login. To resolve this issue, the System Administrator should use the Management Console to establish a reporting database connection and import the schema of the reporting database into the metadata database.

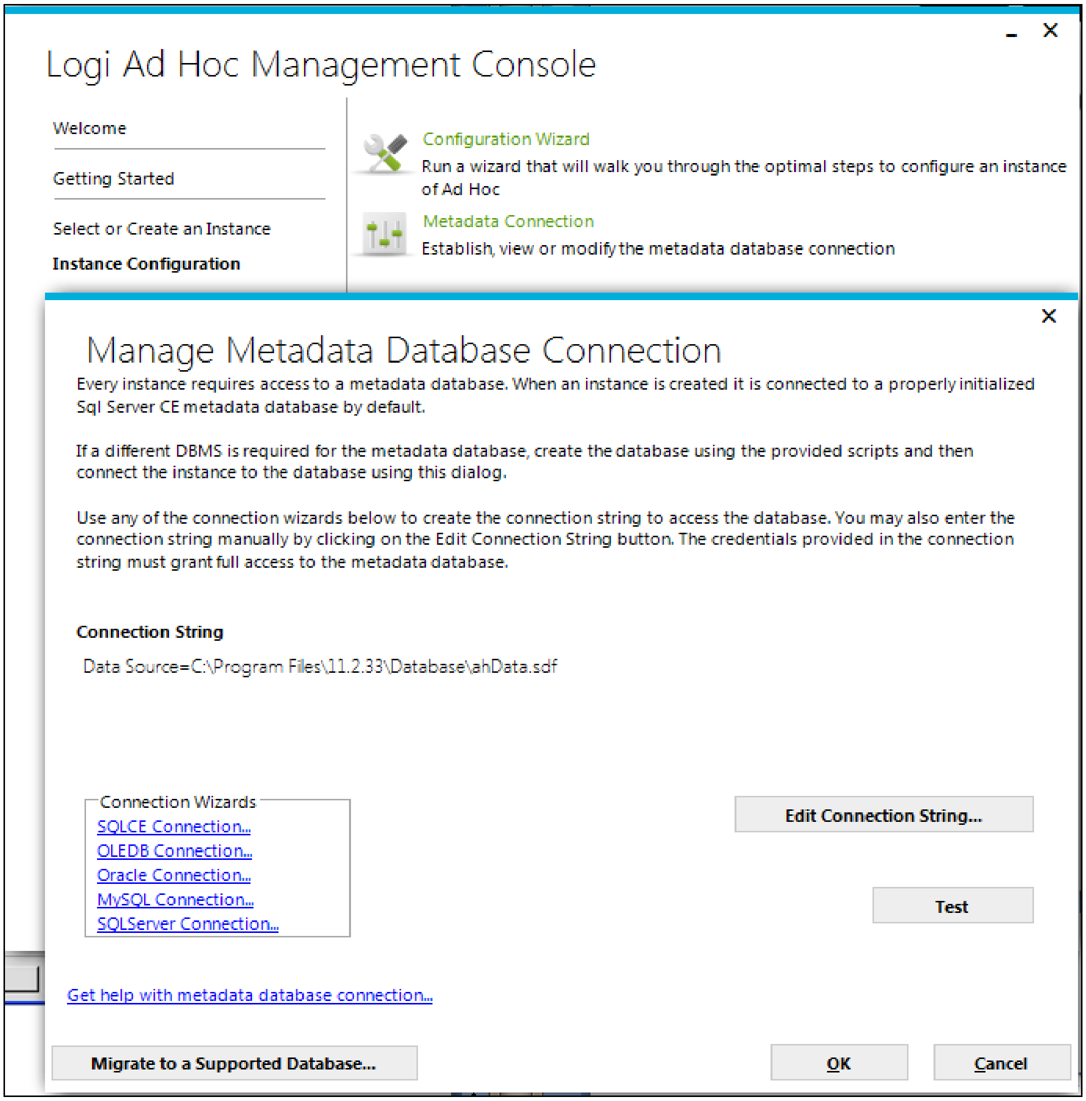
Note: *In the* ***Import Schema*** *dialog, the process is to highlight the objects that should be imported and then click the* ***Add Selected*** *button to include the objects in the schema import process. Just highlighting the objects is not sufficient to complete the process.*

Metadata Access

Every Ad Hoc instance relies on “administrator” level access to a metadata database. The metadata database is specific to each instance of Ad Hoc. The default metadata database is a SQL Compact Edition database distributed with Ad Hoc. The System Administrator may have elected to create an Oracle, SQL Server, or MySQL metadata database.

Ad Hoc needs the ability to insert, update and delete records from the metadata database as well as modify the metadata database schema.

To diagnose and fix various metadata problems, the Management Console offers the **Metadata Connection** action. The following dialog is used to manage the metadata connections:



Logi Ad Hoc Management Console

Run a wizard that will walk you through the optimal steps to configure an instance of Ad Hoc

Establish, view or modify the metadata database connection

Manage Metadata Database Connection

Every instance requires access to a metadata database. When an instance is created it is connected to a properly initialized Sql Server CE metadata database by default.

If a different DBMS is required for the metadata database, create the database using the provided scripts and then connect the instance to the database using this dialog.

Use any of the connection wizards below to create the connection string to access the database. You may also enter the connection string manually by clicking on the Edit Connection String button. The credentials provided in the connection string must grant full access to the metadata database.

Connection String

Data Source=C:\Program Files\11.2.33\Database\ahData.sdf

To verify if the connection string shown is valid and allows access to the metadata database, the **Test** button is provided.

The **Test** button **does not** verify that the credentials grant “administrator” privileges. These privileges are built into the default SQL CE metadata database, but must be verified by the DBA for the alternate DBMS’s.

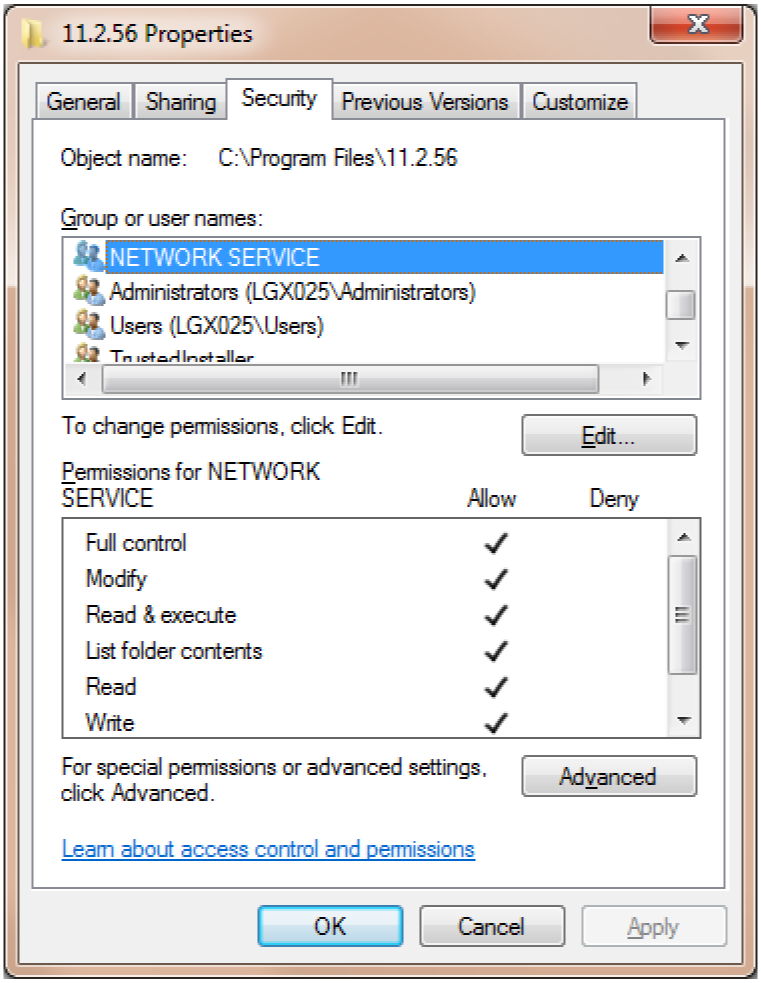
The connection can fail for a variety of reasons. The database could be offline, the provider doesn’t match the database version, or the connection string simply does not grant access to the proper metadata database.

In older versions of Ad Hoc, for example, the default metadata database was Microsoft Access. Customers have tried to migrate a 32-bit instance of Ad Hoc to a 64-bit platform where there are no data providers for MS Access. In this case, the metadata should be migrated to a DBMS that is supported in the 64-bit environment prior to attempting the migration of the Ad Hoc instance.

Folder/File Permissions

Ad Hoc uses the NETWORK SERVICE, the machine/ASPNET or the machine/IIS_IUSRS accounts (depending on the operating system) to manage certain folder contents and the default metadata database. When an instance is created, these accounts are given “Full” permission to the necessary folders and files. If these permissions were lost, as they would be if the folder structure were copied, they would need to be re-established.

The simplest method to establish the permissions on the folders is to adjust the security on the root folder of the instance. This may be accomplished by [Right-Click] on the root folder and selecting Properties. The following dialog should be displayed.



11.2.56 Properties

Object name: C:\Program Files\11.2.56

Group or user names:

- NETWORK SERVICE
- Administrators (LGX025\Administrators)
- Users (LGX025\Users)
- TrustedInstaller

To change permissions, click Edit.

Permissions for NETWORK SERVICE	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

The default metadata database security properties may also be verified by locating the database (ahData.mdb for MS Access or ahData.sdf for SQL CE) in the *Database* folder of the instance and checking the properties of the file. The permissions need to be as described above.

What If I Still Can’t Find The Cause?

If the problem is not remedied by any of the above suggestions, additional diagnosis of the instance may be in order.

Upgrade Manager
From the Management Console, the **Manage an Instance** action group contains the **Upgrade Manager** action. Click on the **Upgrade Manager** and review the dialog. There may be an indication that the metadata schema does not match the required schema for the instance or that the Rights may need to be updated.

Diagnostic Tool
From the Management Console, the **Tools** action group contains the **Diagnostic** action. Running the **Diagnostic** may provide additional information regarding the instance configuration that might prevent the user from accessing the application. It is advisable to enable all of the options available.

Log Errors
The failure of a user to login may be captured in an error log, providing the instance is configured to capture the error. Error logging is enabled by adding a LogErrors attribute to the **<General>** element found in the *_Definitions/_Settings.lgx* file of the instance. This is an XML file that may be edited with any plain text editor (Notepad for example).

Example: `<General LogErrors="True" />`

When this is done, errors will be recorded in a file located in the *Log* folder of the instance.

Event Viewer
Microsoft Windows provides an Event Viewer, where the administrator can determine if there are any error messages by going into the Applications dialog window and looking to see if there are any warning symbols. The error messages generated in the Event Viewer can indicate if there are any machine-level issues.

The Event Viewer can be found under the Control Panel / Administrative Tools.

Contact Us

For more information about other Logi Analytics products or assistance beyond this user manual, please contact Logi Analytics in the following ways:

Corporate Headquarters

Phone: 1-888-LOGIXML (1-888-564-4965)
(703) 752-9700

Fax: (703) 995-4811

Email: info@logianalytics.com

Address: 7900 Westpark Drive, Suite A200
McLean, VA 22102

Web Site: www.logianalytics.com

Sales Department

Phone: 1-888-LOGIXML (1-888-564-4965)
(703) 752-9700

Email: sales@logianalytics.com

Customer Support

Phone: 1-888-LOGIXML (1-888-564-4965)
(703) 752-9700

Link: http://www.logianalytics.com/support/