

AgentManager 1.0.7

Managing RDBAuth Server

Table of Contents

Overview	2
How RDBAuth works	2
Installing Agent Manager	2
Windows Installation	2
Macintosh Installation	3
Using Agent Manager	3
Getting Started	3
Creating a Connection	4
Editing a Connection	4
Deleting a Connection	4
Managing RDBAuth Server	4
Blocking	5
JDBC Pool	5
Admin Accounts	7
Status	8
Support Information	8

Overview

The Remote Database Authentication Server (RDBAuth) controls and manages user access privileges to database resources for Morris Digital Works' applications and utilities based on user-defined attributes, business rules, and security policies. AgentManager is an administration tool for applications built upon Morris Digital Works' Agent Framework. This tool gives administrators remote management capabilities such as stopping, starting, configuring and monitoring applications. AgentManager as of release 1.0.7 does not modify configuration files on the server. For any permanent configuration changes, you should modify the configuration files directly. This document explains how to use AgentManager to manage the RDBAuth Server.

How RDBAuth works

RDBAuth runs as a daemon and awaits requests from Morris Digital Works' clients. Each requesting client provides a service specific username and password, which RDBAuth will attempt to validate. If the username and password exist for the desired service, then RDBAuth relays to the client the connection string along with the database username and password for the access level of the requesting user. The client will then use the provided information to establish a connection directly to the database. This connection will be limited based upon the permissions setup for the user account provided.

Installing Agent Manager

First, you will need to insert the CD entitled "mdClassifieds Development Kit" in your CD drive. Once you've done this, navigate to the readme.txt file located at the root level of the CD drive. The readme.txt file will contain all the information you will need concerning the location of the product installer. Once you find the correct installer location, follow these installation instructions:

Windows Installation

System Requirements

- 300 MHz Pentium II
- 64 MB of RAM
- 25 MB of available hard disk space
- Microsoft Windows version: 98, 98 Second Edition, Millennium Edition, NT 4.0 with Service Pack 6 or later, 2000, or XP

Installation

Open the file "AgentManager\install.htm". Once you have selected the appropriate installer for your platform, the installer will automatically be downloaded to your desktop. After downloading, start the installer on your desktop by double-clicking on **install.exe**. This installer includes Java Virtual Machine (JVM), which is necessary for Agent Manager to run.

Macintosh Installation

System Requirements

- 350 MHz G3
- 64 MB of RAM
- 25 MB of available hard disk space
- Macintosh OS X

Installation

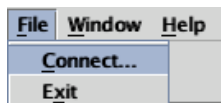
Open the file "AgentManager\install.htm". Once you have selected the appropriate installer for your platform, the installer will automatically be downloaded to your desktop. After downloading, start the installer on your desktop by double-clicking on **install**. This installer includes Macintosh Runtime Java (MRJ), which is necessary for Agent Manager to run.

This application requires OS X 10.0 or later. Upon downloading, the compressed installer should be recognized by Stuffit Expander and automatically expand. If it does not automatically expand, you can manually expand it using Stuffit Expander 6.0 or later. If you are still experiencing problems launching the installer once it has been expanded using Stuffit Expander, please contact technical support.

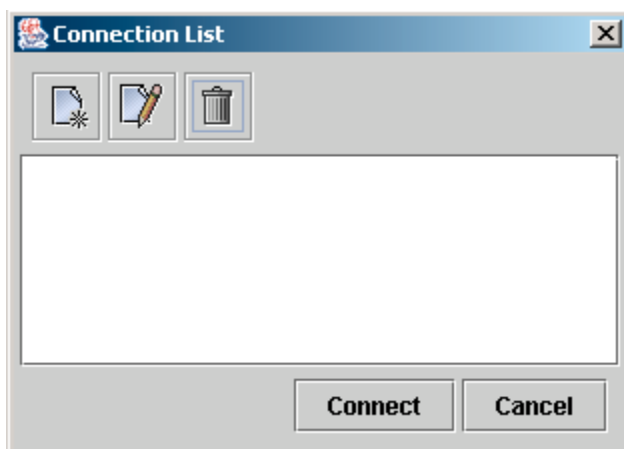
Using Agent Manager

Getting Started


To connect to an agent you must first click on the *Connect* button  or select the *Connect...* option from the File menu.

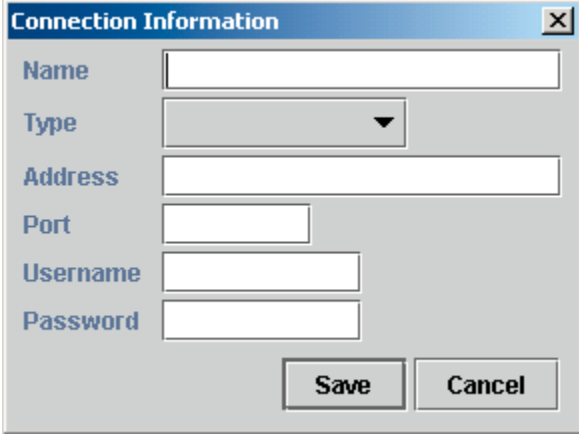


The *Connection List* dialog box will open and give a list of available connections. Select the agent that you want to open, and click on *Connect*.



Creating a Connection

Once you've opened the *Connection List* dialog box, click on the *New Connection* Button . This will bring up a *Connection Information* dialog box.



In the *Name* field, you will type the name of this agent as you would like it to appear in the *Connection List* dialog box. In the *Type* field, select “RDBAuth Server”. The *Address* and *Port* fields are the IP Address and Port number of the agent you wish to connect to. The *Username* and *Password* fields are the accounts you are logging in with. When finished, click 'Save'.

Editing a Connection

To edit a connection, open the *Connection List* dialog box by clicking on either the *Connect* button or the *Connect...* option from the File menu. Select the connection you wish to edit and click on the *Edit Connection* Button.



This will allow you to edit any of the fields in the *Connection Information* dialog box.

Deleting a Connection

To delete a connection, open the *Connection List* dialog box by clicking on either the *Connect* button or the *Connect...* option from the File menu. Select the connection you wish to edit and click on the *Delete Connection* Button.



This permanently deletes a connection, so make sure this is what you want to do before clicking on the button.

Managing RDBAuth Server

When you first connect to the RDBAuth Server, you will see a note at the top of the window. This note explains that the changes made in Agent Manager will remain in effect until the server is turned off. When the server is turned off, the server configurations will default back to the settings you created in *rdbauth.xml* (See *Remote Database Authentication Server (RDBAuth) Administrator Guide*). Therefore, if this is a permanent change, you will want to open *rdbauth.xml* and make the appropriate modifications.

Blocking

This is the panel where you'll find information about users who have failed to authenticate and thusly are blocked from repeatedly trying.

This panel is directly related to the `rdbauth.xml` configuration file. More information on `rdbauth.xml` can be found in *Remote Database Authentication Server (RDBAuth) Administrator Guide*.

There are two fields, *Maximum failed attempts* and *Expiration for block (sec)*, that determine how many failed authentication attempts can be made and how long the user will be blocked. The *Save* button commits any changes that have been made to the settings in this panel. For example, if the *Maximum failed* is set to 5 and *Expiration for block (sec)* is set to 600, then after the fifth failed attempt to authenticate, the user will have to wait 10 minutes before they are allowed to authenticate again. The last field, *Blocked IP Addresses*, is a list of the IP addresses belonging to blocked users. There is a *Refresh* button at the bottom of the screen that will allow you to refresh the list. The *Unblock* button allows you to unblock any selected IP address in the list.

The screenshot shows a web-based configuration interface for the RDBAuth server. At the top, there are four tabs: "Blocking" (selected), "JDBC Pool", "Admin Accounts", and "Status". Below the tabs, the "Blocking" panel contains two input fields: "Maximum failed attempts" and "Expiration for blocked (sec)". To the right of these fields is a "Save" button. Below the input fields is a large, empty rectangular area labeled "Blocked IP Addresses". At the bottom of the panel, there are two buttons: "Refresh" and "Unblock".

JDBC Pool

The RDBAuth server authenticates users via the database, so it needs to keep constant database connections. To connect to the database, the JDBC (Java DataBase Connectivity) library is used. A JDBC pool allows for multiple connections to the database to remain open and ready for use. When a user tries to login, the RDBAuth server gets a connection from the JDBC pool and uses it to authenticate the user. If more than one user is connecting to the RDBAuth server, it needs to be able to let all the users authenticate. To do this, the RDBAuth server grabs a connection for each user and uses it to authenticate. A feature of the JDBC pool is its ability to determine thresholds, such as the maximum number and the minimum number of connections to have open at all times. For example, let's set the max threshold to 5 and the min

threshold to 2. If 10 users attempted to authenticate, 2 connections will already be ready for them to use, however, new connections will be created for each user until the max threshold of 5 is reached. So, in our example, 3 new connections get established thusly accommodating 5 total users. The other 5 users must wait until a connection is available. Other features of the JDBC pool are described below.

This panel is directly related to the rdbauth.xml configuration file. More information on rdbauth.xml can be found in *Remote Database Authentication Server (RDBAuth) Administrator Guide*.

At the bottom of this screen, there are two buttons, *Refresh* and *Save*. The *Save* button saves all changes that have been made to the settings in this panel. The *Refresh* button reloads the current settings from the pool. You will lose new settings if you do not save the changes you made before refreshing.

The screenshot shows a web-based configuration interface for a JDBC pool. It features a tabbed interface with 'JDBC Pool' selected. The configuration is organized into two main sections: 'JDBC Settings' and 'Sizing'. The 'JDBC Settings' section includes three text input fields for 'JDBC Driver', 'Connection URL', and 'Stored Procedure'. The 'Sizing' section includes two spinners for 'Maximum Pool Size' and 'Minimum Pool Size', a dropdown menu for 'Waiting Scheme' (currently set to 'FIXED_WAIT'), and another dropdown menu for 'Cache Connections' (currently set to 'YES'). At the bottom of the configuration area are two buttons: 'Refresh' and 'Save'.

JDBC Driver: Defines the class name of the JDBC driver used to connect to the database.

Connection URL: JDBC URL used to connect to the database.

Stored Procedure: A function stored in the database. Stored procedures are dependent on what your database capabilities are. For example, using Oracle 8i, the stored procedures would be written in either Java or PL/SQL.

Maximum Pool Size: Maximum number of database connections allowed open at a single time.

Minimum Pool Size: Minimum number of database connections allowed open at a single time.

Waiting Scheme: Defines the action taken if a connection is not available upon request.

Actions available:

FIXED_WAIT: This waits until a connection is available.

FIXED_NO_WAIT: This returns null if no connection is available.

Cache Connections: Determines whether or not to cache the database.

Actions available:

YES - If set, this will cache database connections for reuse.

NO - If set, this will create a new connection for every request.

Admin Accounts

This panel allows an administrator to add or delete users and IP addresses. This panel is directly related to the http.xml configuration file. More information on http.xml can be found in *Remote Database Authentication Server (RDBAuth) Administrator Guide*.

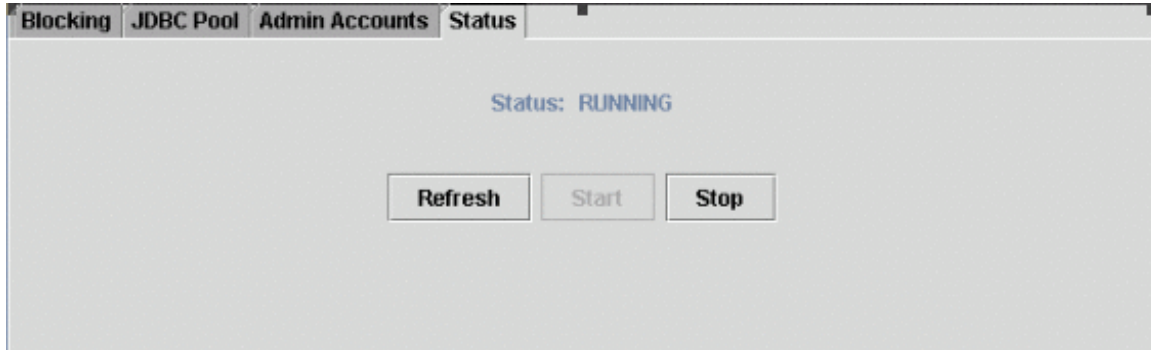
In the Users field, the New button allows for a new username and password to be added to the list. In the IP Addresses field, the New button allows for a new IP address or range of IP addresses to be added to the list. This is the field that allows admin access. The Delete buttons delete the selected user or IP address(es). When deleting a user or IP address, this revokes admin access. The Refresh buttons reload the list of users and IP addresses.

The screenshot shows a web interface with a tabbed menu at the top containing 'Blocking', 'JDBC Pool', 'Admin Accounts', and 'Status'. The 'Admin Accounts' tab is active. Below the tabs, there are two main sections: 'Users' and 'IP Addresses'. Each section contains a table with a header row and several empty rows. To the right of each table are three buttons: 'New', 'Delete', and 'Refresh'. The 'IP Addresses' table has a vertical scrollbar on its right side.

Status

This panel allows you to stop and start the rdbauth server.

The *Stop* button stops the rdbauth server. This only shuts down the rdbauth server. It does not shut down the entire system. If you stop the rdbauth server, users will not be able to authenticate until the server is restarted. The *Start* button starts the rdbauth server. The *Refresh* button reloads the current status of the rdbauth server.



Support Information

Morris Digital Works (MDW), a division of Morris Communications Co., provides tools, technologies, consulting and Web development services to Morris newspapers and external clients. MDW award winning technologies include; world-class hosting facilities, robust content management software, high performance application tools, site enhancement tools and comprehensive classified and display classified technology. Founded in 1995, Morris Digital Works has over 100 employees with offices in Topeka, KS, Joplin, MO, New York, NY and headquartered in Augusta, GA. An additional 250 MCC employees also participate in our Internet business and report directly to newspapers, magazines, book publishing and other internal organizations.

If you are experiencing problems with any of Morris Digital Works products, please contact customer support at (706) 828-2955 ext. 2.