

Database Password Manager

- Background of the problem
- Introducing a solution
- Getting Started
- Add Database User Account
- Modify Database User Account
- Remove Database User Account
- View Passwords
- Run Automatic Password Rotation
- Modify Password Strength Criteria
- Configure Account Associations
 - Add Account Association
 - Add Database Server
 - Add Password Container
 - Remove Account Association
 - Update Account Association
- ColdFusion Integration
- Using Stored Passwords In Database Applications
 - Using Database Passwords in Spring Applications
 - Using Database Passwords in All Other Applications
- Security Information
 - Network Diagram
 - Database Diagram

Background of the problem

Goals: Securing and maintaining application passwords.

Unlike user passwords which should solely be stored in ones head, application passwords must be stored and made accessible to the application process at run-time. Most applications retrieve such passwords from configurations files stored locally on disk. Configuration files, in turn, are secured with file-based access controls limiting which processes (and users) can read or write said files.

In order to add an additional level of protection, plain-text passwords can be encrypted. If the cryptographic keys remain secret, leaked files containing encrypted passwords are less likely to be useful to an attacker.

In areas such as the Graduate Division and the Office of Research, there are dozens of separate application passwords for each application and for each of development, test and production environments. All of these passwords must be changed periodically. Manually changing this many password represents significant workload and introduces risk of service interruption due to human error.

Introducing a solution

Goals: Encrypting passwords with a strong algorithm and using a sufficiently long key length to achieve current computational security. Controlling, automating and auditing access to the password stores.

This is nothing new; other OIT groups have already devised password security [solutions](#) around such ideas.

Although the existing solutions may work well for one group, other groups cannot always take advantage of them due to unique infrastructural needs:

- The majority of existing GD/OR applications are hosted on servers running a different operating system.
 - Maintaining a secure shared file space might add security issues and would certainly add complexity.
- Many of our applications run on different application stacks and are written in unsupported languages .
 - No Coldfusion API exists for the existing solutions.

- No Visual Basic 6 API exists for the existing solutions.

The Database Password Manager tool referenced here provides the same basic functionality as existing solutions:

- Management of secure password stores
 - create, read, update, and delete encrypted passwords

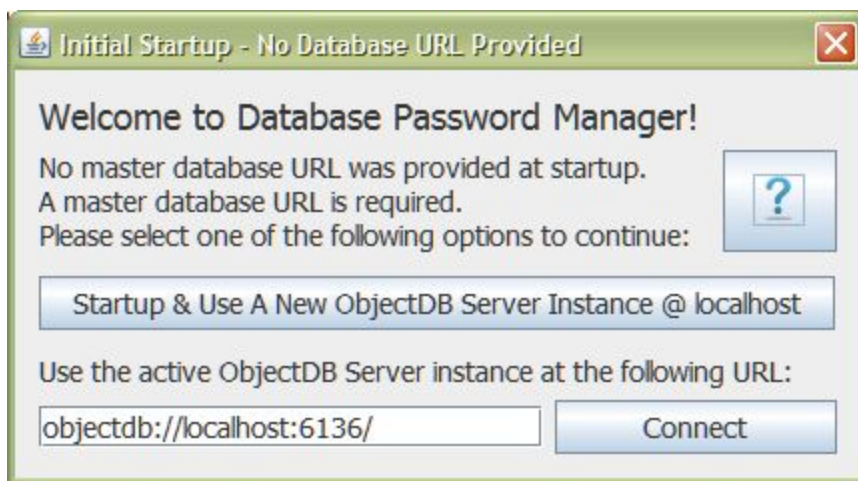
Additionally, it provides the ability to:

- Store multiple passwords in a single file if desired (simplifying file ACL management).
- Facilitates password rotation
 - Update one or more passwords at the database server-level and well as the password store for individual software applications from one tool with very few steps.


Getting Started

Note that DBPM has its own integrated help system that should be able to get you through understanding all aspects of the system. Almost every window in DBPM has one or more help icons that, when clicked, take the user to the part of DBPM's help document that is relevant to the action being performed. This wiki, however, gives a softer introduction to the system and therefore may still be helpful. This wiki document should perhaps be read first as an introduction to the system functionality as a whole and then the in-system help can be used as reference documentation. The system also has a link to this wiki document. You can access this document through the system at any time by clicking Help (In the file menu) -> About -> Open Product Page.

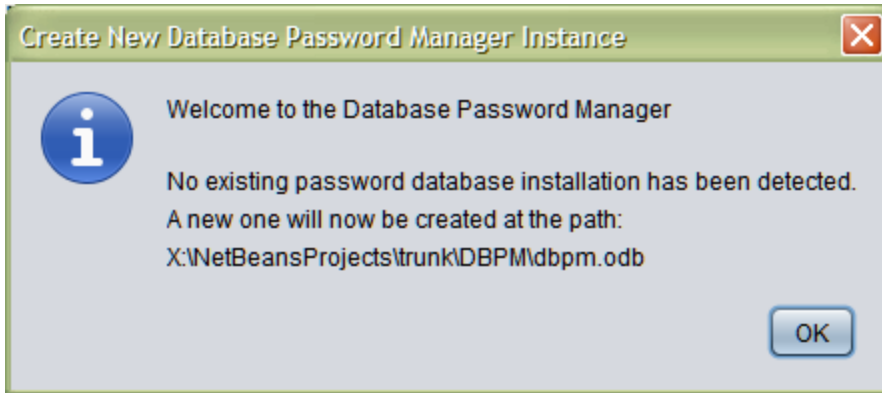
To begin using the system, click on the DBPM.jar file or launch it with command prompt using the `java -jar` command (JRE6 or greater). The following screen should be presented:



This message is essentially asking you where you want to store all that password and other information that the system needs to function. The most common option is usually to **Startup & Use A New ObjectDB Server Instance @ localhost**. Clicking this button will launch a relatively small process called `server.exe` that, by default, accepts database connections through port 6136. ObjectDB is a lightweight embeddable database chosen for its simple file-based storage which allows for the trivial application file-based security.

When the server is running, you should see the following icon in your system tray: . If ObjectDB Server is already running or you would like to connect to another (possible remote) server instance that is different from the default, enter the URL for that instance and click **Connect**.

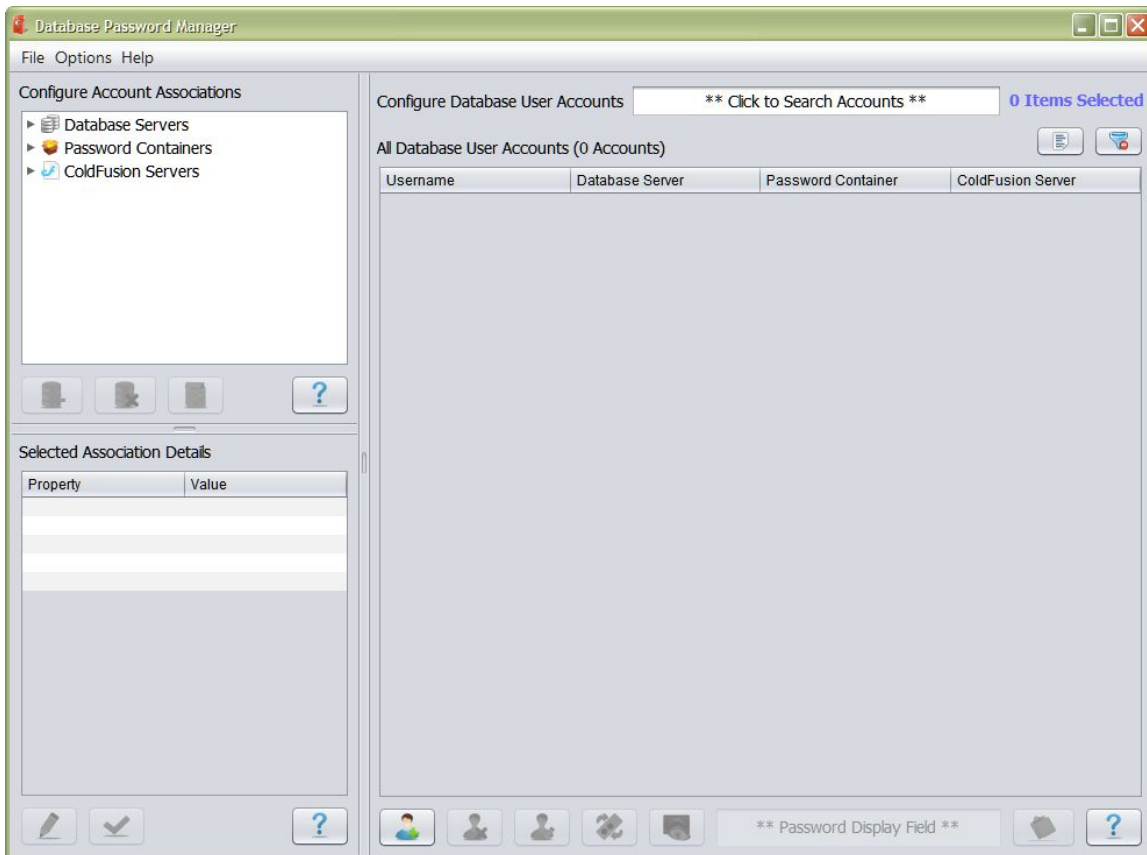
If this is your first time running the Database Password Manager, you will be presented with the following message:



What this message is telling you is that there is no current DBPM "installation" has been detected at the server URL that you specified. An installation involves nothing more than creating a new database file at the specified ObjectDB server URL and this operation happens automatically once you click the **OK** button. The installation file that is created will hold all the information that is entered into the system except the actual encrypted passwords. Encrypted passwords will be stored in user-defined password containers. The user of password containers is discussed later in this document.

Add Database User Account

When you launch the Database Password Manager for the first time, you will be presented with the following window:



You will notice that the only buttons on the GUI that are currently enabled are the blue "help with this section" buttons and the green plus sign button.


Click on the green plus sign to add a database user account to the system. Doing this will present the following

screen:


Add Database User Account


Fill in the following fields to add a new database user account:

Username:


Password: 

Confirm Password:

Database Server: 




Password Container: 

☐ Used by ColdFusion Application Server

 Configure ColdFusion Server Integration

Username field cannot be blank.

This screen has the following fields which must be populated before you can add the new account.

- Username
 - Enter the username of the database user account.
 - This username should be the same as it is on the database server system.
- Password
 - Enter the password for this username.
 - Leave this field blank if you would like to generate a password.
 - A password can be generated by clicking on .
- Confirm Password
 - Re-enter the password for confirmation.
 - Again, leave this field blank if you would like to generate a password.
- Database
 - Select the database connection that will be used to reset passwords on the RDBMS.
 - Database connections can be added by clicking on . (See the section on account associations for more info)
- Password Container
 - Select the password container that will hold the password for this account.
 - Each password container will be implemented by a separate .odb file the stores all the encrypted passwords that are associated with that container. User permissions can then be customized on this container file through the operating system.
 - Password containers can be added by clicking on . (See the section on account associations for more info)
 - **WARNING:** If you manually move a password container file, the system will not be able to locate and retrieve passwords that are stored in that password container. It is recommended that you store all password containers as well as the main system database in the same directory.

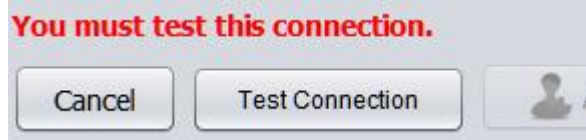
The "Used By ColdFusion Application Server" check box should be selected if the password being added is used in a ColdFusion server. Selecting this option will require additional configuration of ColdFusion server information that

must be specified by clicking on



Once ColdFusion server configuration is complete, the system will be able to modify the password on a ColdFusion server when it is changed by this tool. See the section on ColdFusion integration for more information.

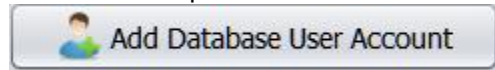
Once all the fields are filled in, you will be required to test the database connection. You should see the following



situation on the bottom of this add user dialog window:

Click "Test Connection" and the connection will be tested. If you filled in all the correct database connection credentials, the test should pass.

Once all the required fields are filled in and the database connection has been tested, the




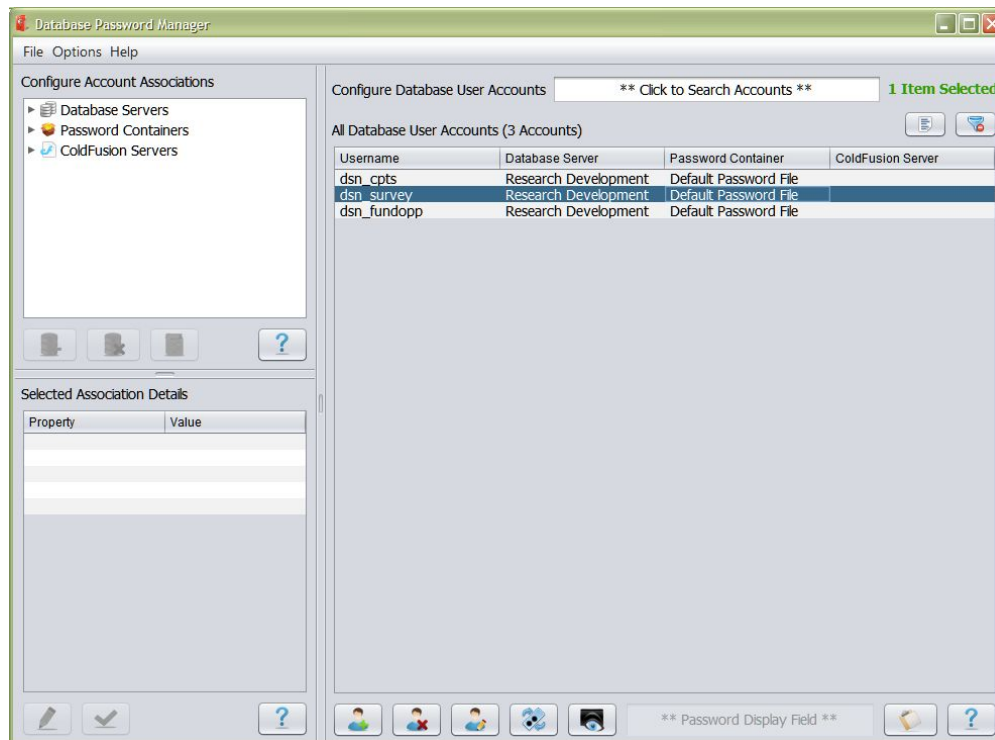
button should become enabled. Click on this button to add the user account to the system.

Note: If you plan to change a password for a database user that is not yet in the system, first add the user to the system with the current old password. You can then use the "Modify" tab to change the password on the system as well as on the actual RDBMS.

Modify Database User Account

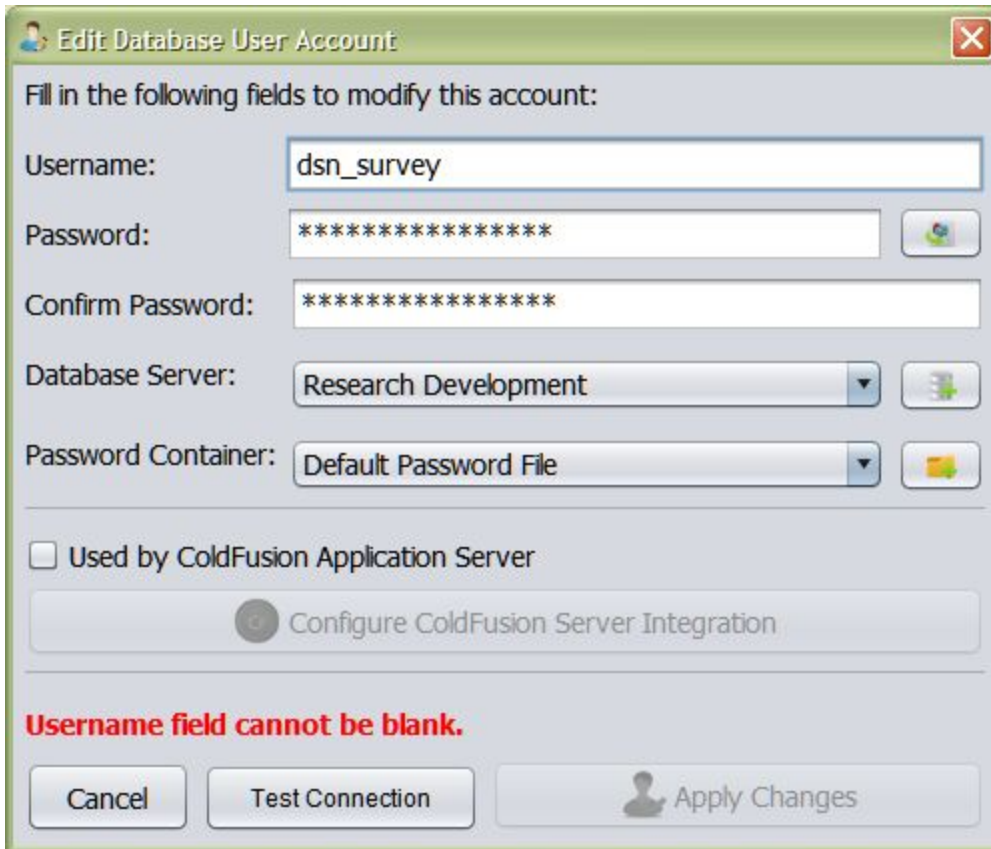
Once a database user account is entered into the system, you can modify it by selecting its row in the accounts

table and then clicking on .



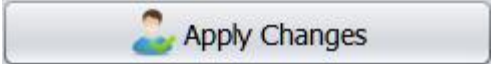
Once you do this, you will be presented with essentially the same window as was used to add the account in the first

place but with minor verbiage and icon changes.



The screenshot shows a dialog box titled "Edit Database User Account" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

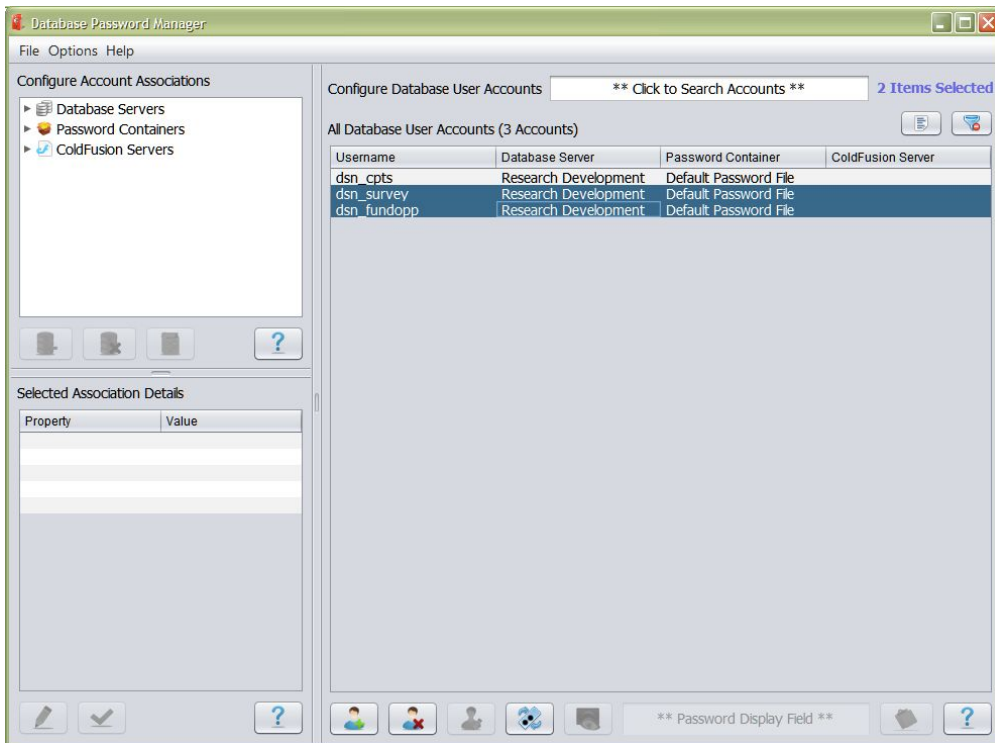
- Username:** A text field containing "dsn_survey".
- Password:** A password field with masked characters "*****" and a small icon to its right.
- Confirm Password:** A password field with masked characters "*****".
- Database Server:** A dropdown menu showing "Research Development" and a small icon to its right.
- Password Container:** A dropdown menu showing "Default Password File" and a small icon to its right.
- ☐ **Used by ColdFusion Application Server**
- A button labeled "Configure ColdFusion Server Integration" with a circular icon to its left.
- A red error message: "Username field cannot be blank."
- At the bottom, there are three buttons: "Cancel", "Test Connection", and "Apply Changes" (which includes a user icon).



Behavior of this form is the same as described in the "Adding a Database User Account" section above. When you are done modifying this account and testing the connection, click .

Remove Database User Account

You can remove a database user account by selecting its row in the accounts table and then clicking on .

You can also select and remove multiple rows (if using Windows) by holding down the Ctrl key and clicking on each desired entry as shown below:




Helpful Tip: Click  to remove any filters that may be active on the accounts list. This will insure that all accounts that are in the system are displayed on the list. Click  to select all accounts in the list.

View Passwords

If you would like to view the password for a database user account, select a single account from the accounts list


and click on .



Doing so will display the password in the "Password Display Field" that is directly to the right of the button. The password will display for 5 seconds and then disappear.

If you need the password copied to the clipboard, click on .

Run Automatic Password Rotation

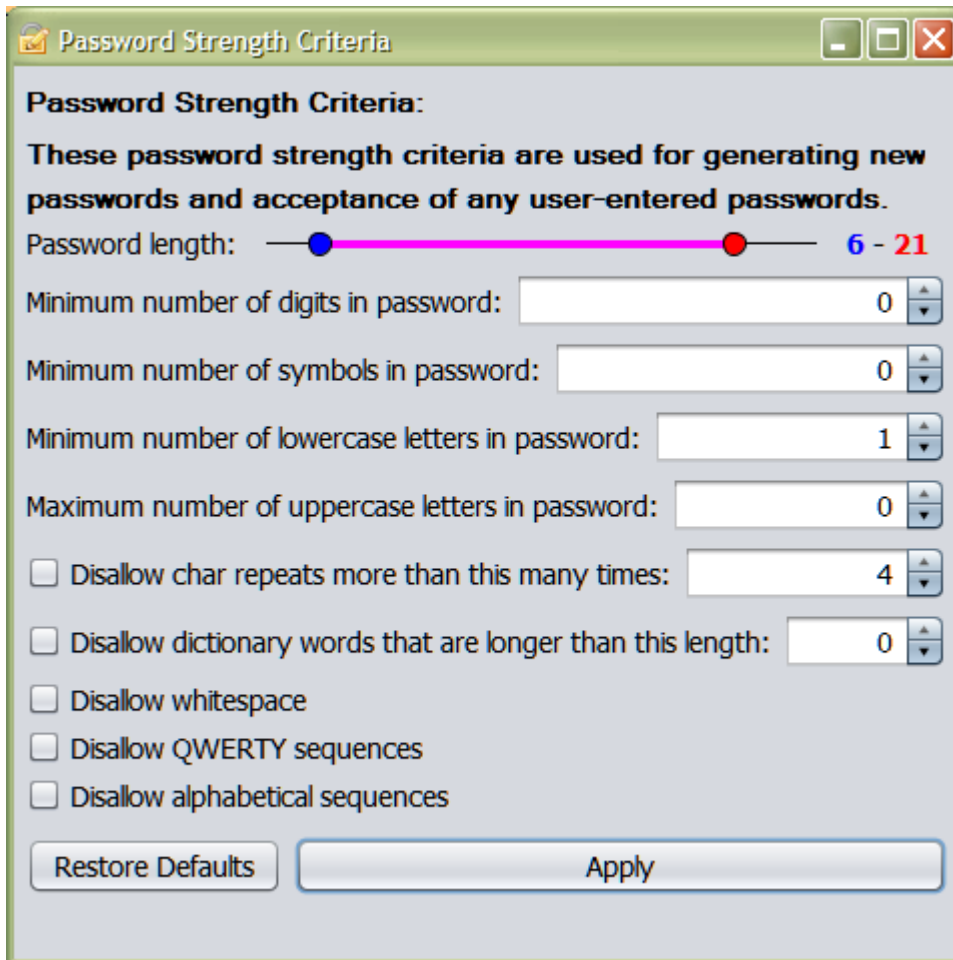
The Database Password Manager offers the ability to run an automatic password rotation. This action will change the database passwords on all selected database accounts with a single click. A password rotation will change the password in the DBPM and any associated servers. To perform a password rotation, select all of the accounts that

you would like to change and then click on .

Helpful Tip: Click  to remove any filters that may be active on the accounts list. This will insure that all accounts that are in the system are displayed on the list. Click  to select all accounts in the list.

Modify Password Strength Criteria

The password strength criteria are a set of password constraints that you can set. Both generated and user-defined passwords will then be forced to comply with these criteria. To view or modify these criteria, click "Options" from the file menu and then select the "Password Strength Criteria". Doing so should pop-up the window shown below:



The screenshot shows a window titled "Password Strength Criteria" with a green title bar. Inside, there's a section titled "Password Strength Criteria:" followed by a descriptive sentence: "These password strength criteria are used for generating new passwords and acceptance of any user-entered passwords." Below this, there's a "Password length:" slider with a blue circle at 6 and a red circle at 21, with the text "6 - 21" to the right. Following the slider are five input fields with up/down arrows: "Minimum number of digits in password:" (0), "Minimum number of symbols in password:" (0), "Minimum number of lowercase letters in password:" (1), "Maximum number of uppercase letters in password:" (0), and "Disallow char repeats more than this many times:" (4). Below these are three unchecked checkboxes: "Disallow dictionary words that are longer than this length:" (0), "Disallow whitespace", "Disallow QWERTY sequences", and "Disallow alphabetical sequences". At the bottom are two buttons: "Restore Defaults" and "Apply".

There are 13 fields in this window:

- Password Length Slider
 - Use the blue circle to select the minimum required password length.
 - Use the red circle to select the maximum allowable password length.
 - The password length range is displayed on the label to the right of the slider.
- Minimum number of digits in password
 - Enter the minimum number of digits that a password needs to contain.
 - A digit is a number between 0-9 and is a single character.
 - Input must be a number
- Minimum number of symbols in password
 - Enter the minimum number of non-alphanumeric symbols that a password must contain.
 - Input must be a number.
- Minimum number of lowercase letters in password
 - Enter the minimum number of lowercase letters that a password must contain.
 - Input must be a number.
- Minimum number of uppercase letters in password
 - Enter the minimum number of uppercase letters that a password must contain.
 - Input must be a number.

- Disallow char repeats more than this many times []
 - Do not allow any character to repeat more times than the number specified in the adjacent text field.
- Disallow dictionary words that are longer than this length []
 - Dictionary words that have more characters than the number specified in the adjacent text field will not be accepted.
- Disallow whitespace
 - Do not allow spaces or tabs in passwords.
- Disallow QWERTY sequences
 - Do not allow passwords to have characters in the same order as on a QWERTY keyboard
- Disallow alphabetical sequences.
 - Do not allow passwords to have alphabetical sequences.
 - abcd is an example alphabetical sequence that will be denied.

There are two buttons on this window:

- Restore Defaults
 - Set password criteria to the default settings and close the window.
 - Default settings can be configured in the PasswordToolConstants class.
- Apply
 - Use the password strength criteria that is shown in this window as the active password strength criteria.

Configure Account Associations

One of the greatest features of this system is its ability to automatically change passwords on database management systems, ColdFusion servers, and password containers. Each of these is known as an **account association**.

Account associations are established when the account is created.

You can change an account's association when you edit the account as described in the "Modify Database User Account" section.

A single association can be used by many accounts.

Modifying settings on an association will affect all accounts that are linked to that association.

DBPM currently handles 3 different types of account associations:

1. Database Servers
2. Password Containers
3. ColdFusion Servers

CRUD operations on these associations are all handled in mostly the same way.

Add Account Association

Account associations are usually added when a new account is added which uses a server that is currently not on the DBPM instance. The same windows that are explained in the following sections will be shown in this case. The text before the screenshot in each association addition instructions describes how to add an association from the associations tree. Skip these instructions and continue to the text after the screenshot if you are adding a new association from the add account dialog window.

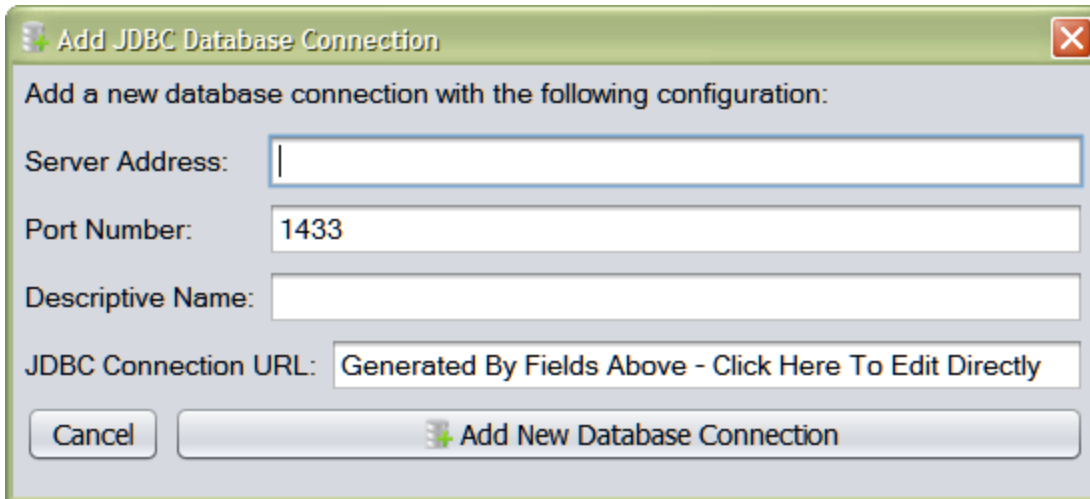
Add Database Server

To add a database server from the account associations table, select the "Database Servers" node and click



. (You can also right-click on the node and select "Add Database Server"). You will then be presented with

the following window:




The dialog box is titled "Add JDBC Database Connection" and contains the following fields and buttons:

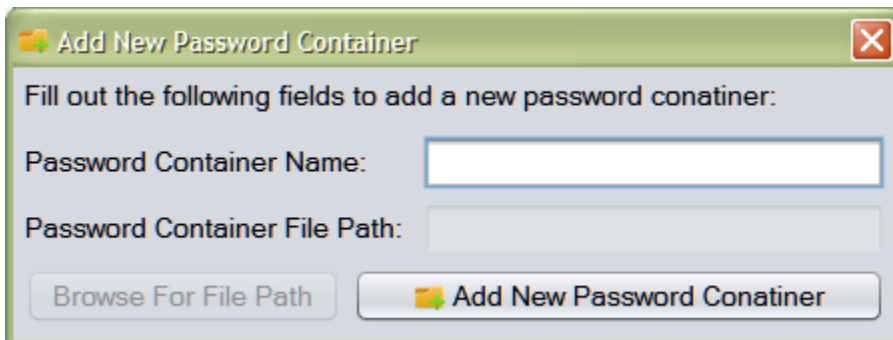
- Server Address:** A text input field.
- Port Number:** A text input field with the value "1433" entered.
- Descriptive Name:** A text input field.
- JDBC Connection URL:** A text input field containing the text "Generated By Fields Above - Click Here To Edit Directly".
- Buttons:** "Cancel" and "Add New Database Connection".

- Entering a Server Address and Port Number (1433 populated by default) will cause the JDBC Connection URL field to be populated automatically.
- If desired, you may also manually enter the JDBC Connection URL string by clicking on the greyed out "JDBC Connection URL" text field.

You must also enter a descriptive name for the database connection. This provides a user-friendly way to identify the database that this connection references.

Add Password Container

To add a password container from the account associations table, select the "Password Containers" node and click . (You can also right-click on the node and select "Add Password Container"). You will then be presented with the following window:



The dialog box is titled "Add New Password Container" and contains the following fields and buttons:

- Password Container Name:** A text input field.
- Password Container File Path:** A text input field.
- Buttons:** "Browse For File Path" and "Add New Password Container".

A descriptive name needs to be provided to identify the password container. This name may be different from the file name but does not have to be. Next, provide a file path to the password container. One is automatically generated when you enter the container name but it can be changed by either directly editing the "Password Container File Path" field or browsing for a file path.

Remove Account Association

Removing account associations is done by selecting the association to remove and then clicking on the respective "Remove Association" button:





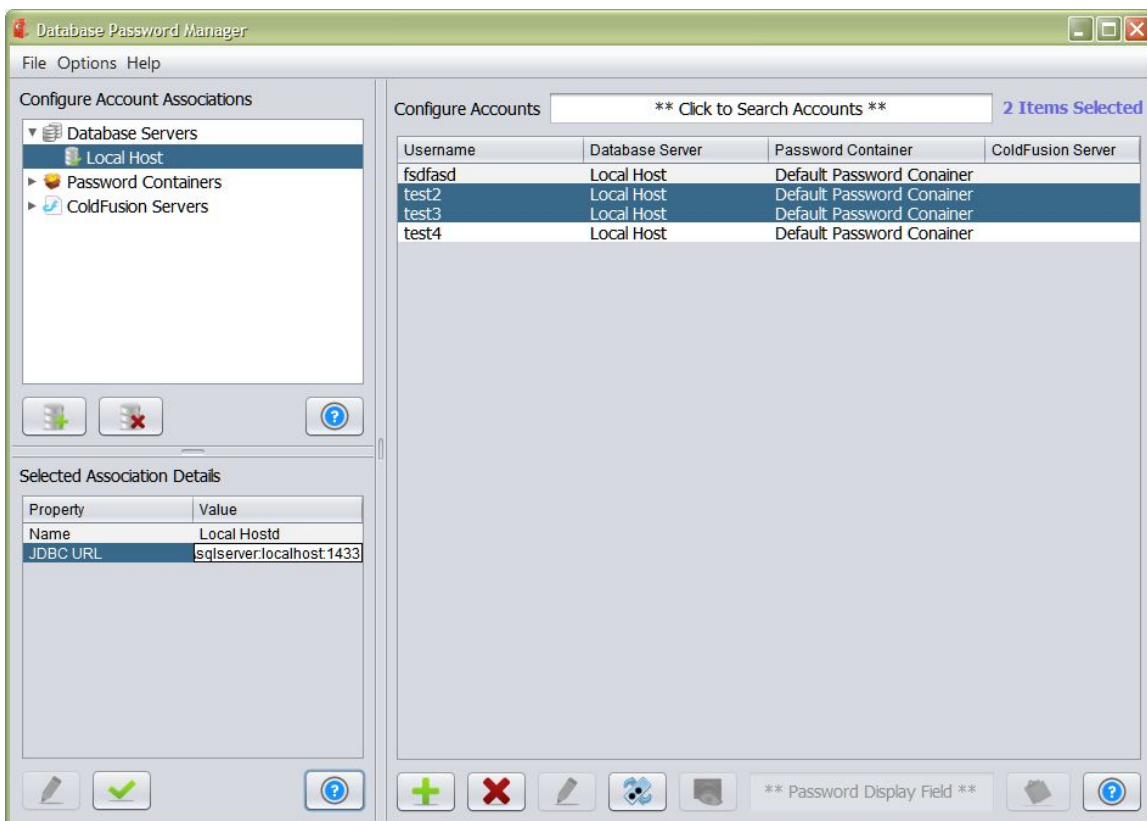
You can also right-click on the association and select the remove option.

Note: When removing an association, all accounts that are linked to that association will be removed as well. To prevent an account's removal, change it to another association before deleting the association of interest. You can view all accounts linked to an association by right-clicking on the association and selecting "Display Linked Accounts".

Update Account Association

Updates of each type of association follow the same process:

1. Select an association from the associations tree.
2. Select the field of this association that you would like to edit from the "Selected Association Details" table.
3. Click  to begin editing the field. (you can also double-click the value cell for that property to begin editing)
4. Click  to apply the changes on this field (you can also hit Enter or simply click on another cell to apply the changes)



ColdFusion Integration

Sets default ColdFusion configuration settings.

Using Stored Passwords In Database Applications

The Database Password Manager provides an API that developers can use to retrieve database application

passwords for use in applications. There are two primary ways that this is handled depending on if your application uses the Spring Framework or not.

Using Database Passwords in Spring Applications

The Spring Framework makes it easy to import passwords from any source. Since many developers are familiar with how Adcom's CryptoJCE interfaces with Spring security, the DBPM has been built to interface with Spring in the same way.

Using Database Passwords in All Other Applications

If your application does not use the Spring Framework, you can still get your database passwords from the GDOR Passwords API. The recommended way of doing this is to move all database configuration into tomcat's context.xml. Your configuration should look something like this:

TomcatExampleDBPMResource

```
<!-- Database for FundOpps -->
<Resource name="uci_fundopp"
username="dsn_fundopp"
factory="edu.uci.security.EncryptedDataSourceFactory.java"
auth="Container"
type="javax.sql.DataSource"
maxActive="20"
maxIdle="30"
maxWait="10000"
minIdle="0"
minEvictableIdleTimeMillis="3600000"
timeBetweenEvictionRunsMillis="1800000"
removeAbandoned="true"
removeAbandonedTimeout="120"
/>
```

The first two attributes are the required and most important ones. Note that only a username is required because the password is filled in by DBPM. Other attributes of the Resource tag like `driverClassName` and `url` are also filled in by DBPM.

Note: If you have a DBPM installation at a location different than the default (localhost at port 6136). The URL to the password file of the password should be provided in the "password" attribute.

Security Information

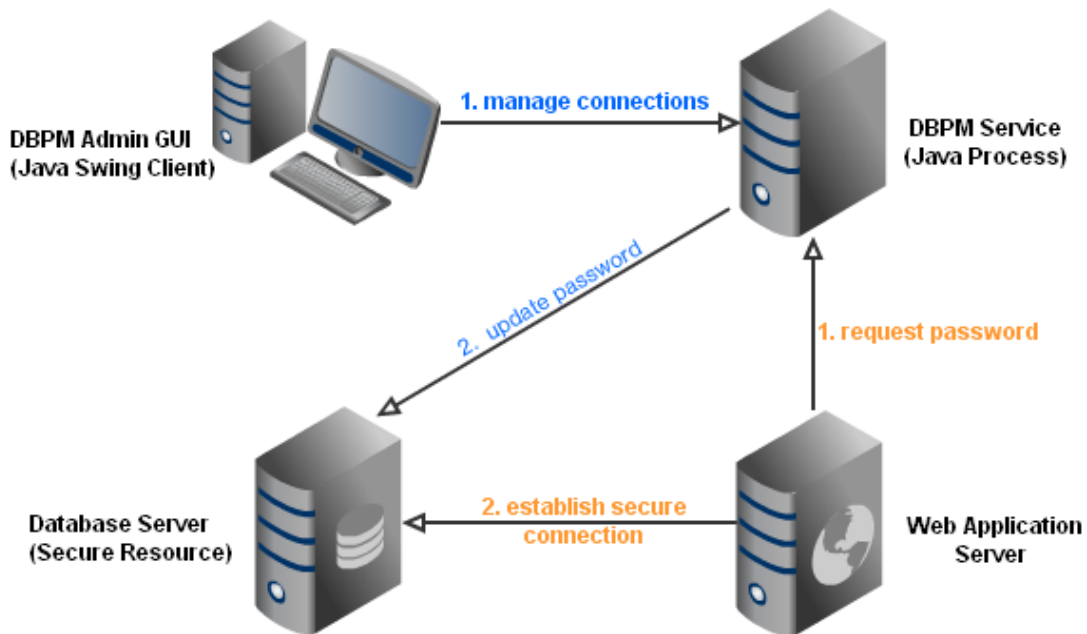
The Database Password Manager uses AES Encryption to encrypt and decrypt passwords. This cryptography relies on a secret Key and IV stored somewhere on the file system where the Database Password Manager is running. The actual encrypted passwords are stored in database files protected with file-based security.

In addition to this, the Database Password Manager relies on a password policy configuration file that is used to specify password strength criteria. The criteria is enforced by the tool for password generation to ensure that newly created or updated passwords are strong.

Security for the current GD/OR implementation relies on Windows filesystem security which is made sufficient since both DBPM components (Admin GUI, Service) run locally on the web application server.

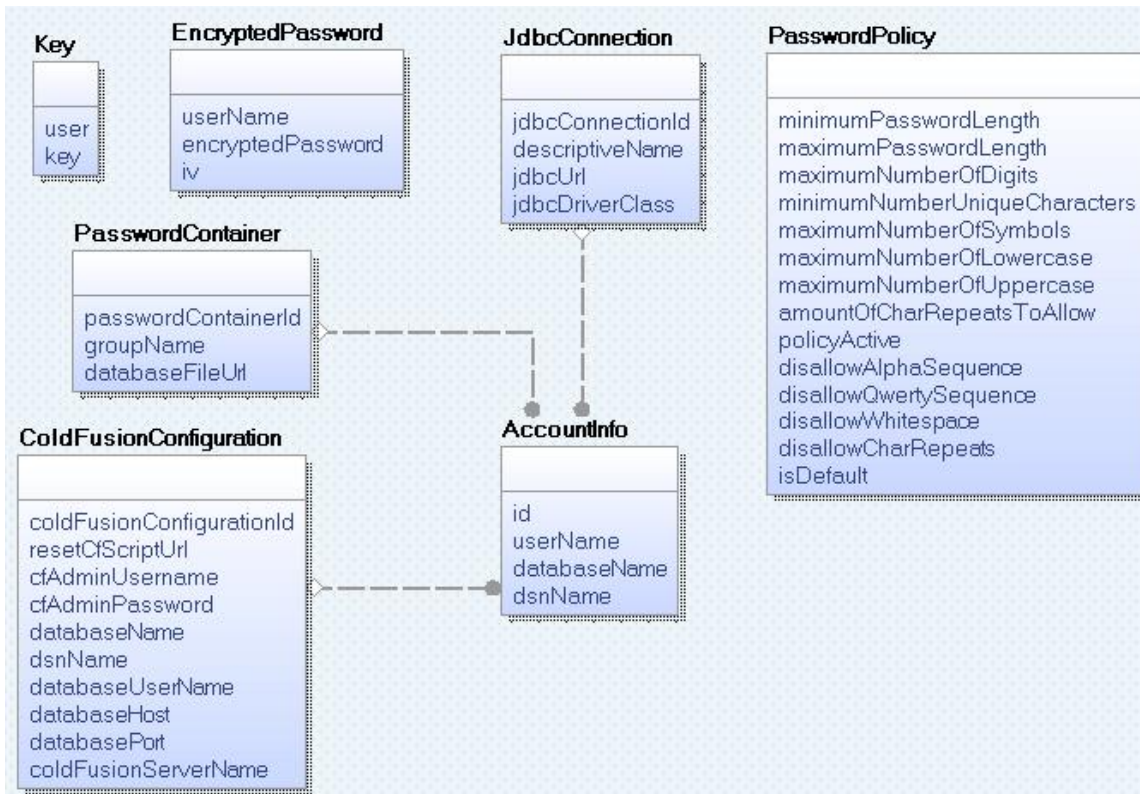
- The DBPM Service itself only allowed to listen/service local requests.
- More importantly, encrypted passwords which DBPM work upon are stored in separate files, each with individualized security permissions.
 - An unwarranted user executing the Admin GUI would not be able to take harmful actions without read/write access to the underlying files.

Network Diagram



- The DBPM Admin GUI interacts with the DBPM Service to manage connections.
- Operations such as updating passwords will update the target server keeping the credentials in secured repository in sync with those on the database itself.
- Applications request credentials from the Password Service and in turn connect to the associated Database Server.

Database Diagram



- The Key and EncryptedPassword tables are stored in different database files to increase the flexibility of the system to future security enhancements.
- The Key and EncryptedPassword tables have no database level constraints on AccountInfo but the system insures that for every userName, there exists exactly one Key and EncryptedPassword record.
- The database system used to store this information is Object-DB, a JPA compliant high speed object database.
- All database queries are in JPQL.