Authenticates a user by querying a database consisting of user records. Resilient privacy enhancing policy evaluation mechanism avoids the passing around of the password through the network by requesting for the password only when the Database Authentication authority is invoked. The sensitive information is only exchanged between the user and the Database Authentication authority over TLS.

Configuring the Database Authentication Authority

To configure the authority, complete the following steps.

1. Sign into the Administrative Console
2. Click **Create New Authority.**
3. Select **Database Authentication** from the **Authority Type** drop down.
4. Type a name for the authority in the **Authority Name** box.
5. Type a description of the authority in the **Authority Description** box (optional).
6. Type he fully qualified URI location of the Resilient Access Authority Connector in the **Resilient Access Authority Connector Host** box, including the number of the port on the Resilient Access Authority Connector host that will accept incoming connections. To encrypt the communications between Resilient and the Resilient Access Authority Connector, type **https**.
   http[s]://*fully_qualified_domain_name*:*port_number*
7. Configure the connection to the Database server by entering:
   1. The fully qualified hostname of the database server in the **Database Host** box:
   2. The name of the database containing the user records in the **Database Name** box
   3. The database user name in the **Database User Name** box
   4. The password for the user account to connect to the Database server in the **Database Password** box.
8. Configure how the database will be queried to find the user and verify their password.
   1. Enter the table in the database that holds the user records in the **Authentication Table** box
   2. Enter the column name that has the user identity attribute that will be passed during database authentication in the **UserId Column Name** box
   3. Enter the column name that stores the password in the **Password Column Name** box.
   4. If Passwords are encoded as MD5 values before storing them in the database then the **Password encoded as MD5** checkbox should be checked.
   5. Resilient Access has integrated with Intensity Analytics Behavioral Biometric Authentication to seamlessly provide strong second factor authentication to policies created in Resilient Access. Intensity Analytics has a patented technology of calibrating the rhythm of a user's keystoke pattern and using that to create a unique user identity signature. This is then applied to detect if the person typing the password is the person being authenticated. As the user authenticates using their password the system calibrates and stores profiles of the keystroke rhythm until enough profiles have been created to accurately determine a user's keystroke rhythm. Subsequent authentication attempts will enforce the Intensity Analytics Behavioral Biometric Authentication as an additional authentication factor. To enable Intensity Analytics Behavioral Biometric Authentication click the **Include Intensity Analytics** checkbox.
9. Once you have finished configuring the Database Authentication authority, click **Create** or **Save**.