Setting a Master Password

- Specifying a Master Password
- Changing a Master Password
- Resetting the Master Password
- Connecting with a Master Password specified
- Manually Requesting the Master Password for New Connections
- Showing the Encrypted Password in Cleartext
- Declaring a Master Password Rule

When you use **Save Between Sessions** for database passwords and SSH passwords or pass-phrases, they are by default encrypted using a static key. The same is true for the Proxy password if you have specified one. For better security, you can specify a Master Password that is then used instead of the static key to encrypt all passwords and pass-phrases. This way, only you know the information needed to decrypt the data. The algorithms used for encryption with a Master Password are also more advanced, minimizing the risk that the data can be decrypted by brute force.

Using a Master Password does, however, mean that if you forget it, there is no way to retrieve it and therefore no way to decrypt the saved passwords. It also means that the encrypted passwords cannot be read by a DbVisualizer version earlier than 9.2.

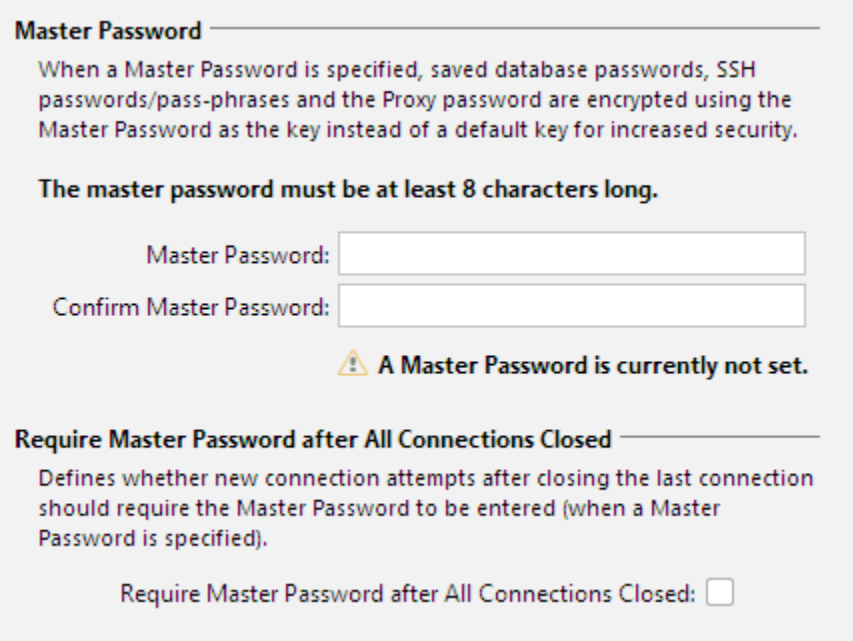
If you forget the Master Password, it cannot be recovered. The only way forward is to reset the Master Password, which also clears all passwords encrypted with it.

Passwords encrypted with a Master Passwords cannot be used in DbVisualizer version earlier than 9.2. If you set a Master Password in 9.2 and then use an earlier version, you will get "invalid password" errors when trying to connect with a saved password. You must enter the database or SSH password again in the earlier version, or go back to using DbVisualizer version 9.2 or later.

Specifying a Master Password

To use a Master Password for encoding of passwords saved between sessions:

1. Open **Tools->Tool Properties** and select the **General/Master Password** category,
2. Enter a password matching the described rules in both the **New Password** and **Confirm New Password** fields,
3. Click **Apply** and then confirm that you want to do this after reading the warning about what it implies.

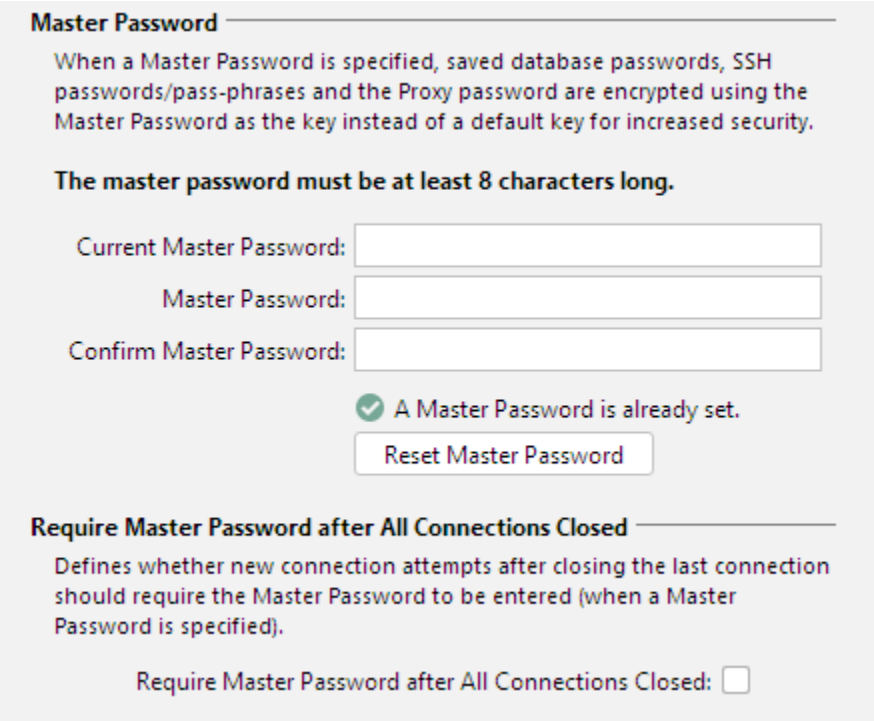


The passwords for all connections with **Save Between Sessions** chosen for the password are now encrypted with the Master Password. The same goes for the SSH passwords/pass-phrases if you have selected to have them saved between sessions, as well as the proxy password, if any.

Changing a Master Password

If you want to change the Master Password:

1. Open **Tools->Tool Properties** and select the **General/Master Password** category,
2. Enter the current password in the **Current Password** field and the new password in both the **New Password** and **Confirm New Password** fields,
3. Click Apply.



The saved passwords are then decrypted with the current Master Password and re-encrypted with the new.

Resetting the Master Password

If you have forgotten the Master Password, or simply no longer want to use one, you can reset it:

1. Open **Tools->Tool Properties** and select the **General/Master Password** category,
2. Click the **Reset Master Password** button and confirm that you want to do this.

Note that all passwords encoded with the Master Password are then immediately cleared and there is no way to recover them.

Connecting with a Master Password specified

When you have a Master Password specified, you will be prompted to enter it the first time within a DbVisualizer session that you need to connect with a saved password. From then on, you can make other connections with saved passwords without being prompted until you restart DbVisualizer.

Manually Requesting the Master Password for New Connections

You have two options to manually require being prompted for the Master Password again after entering it once within a DbVisualizer session:

1. Select **Database->Require Master Password at Next Connect**,
2. Open **Tools->Tool Properties**, select the **General/Master Password** category and enable **Require Master Password after All Connections Closed**.

Showing the Encrypted Password in Cleartext

When you have specified a Master Password, you can view the saved database password or SSH password/pass-phrase in cleartext.

1. Right-click on the password field label and select **Show Password**,
2. Enter the Master Password when prompted.

Declaring a Master Password Rule

A Master Password must have at least eight characters of any kind by default, but you can declare your own rule using a regular expression in an installation configuration file:

1. Open the *DBVIS-HOME/resources/dbvis-custom.prefs* file,
2. Enter a regular expression as the value of the `dbvis.-MasterPasswordRule` property,
3. Enter a description of the rule for showing the user in Tool Properties as the value of the `dbvis.-MasterPasswordRuleDescr` property.

The regular expression for the default rule is `.{8,}`. It is easy to change the number in this expression to any number you want. There are regular expressions that can describe pretty much any rule you can come up with. For instance, this rule requires at least nine characters, with at least one symbol, one digit, one uppercase character, and one lowercase character:

```
(?=.{9,})(?=.*?[^\\w\\s])(?=.*?[0-9])(?=.*?[A-Z]).*?[a-z].*
```

If you cannot adopt these examples to your own policy, you can search the Internet for other examples of "regular expressions for password validations".