Centrally Secure Passwords

Overview

Page Contents

Some tools use cleartext passwords, which can pose a security risk. The security risk is even greater if you use LDAP or other external authentication, since you expose your SSO password in cleartext and that password is likely to be used for other services.

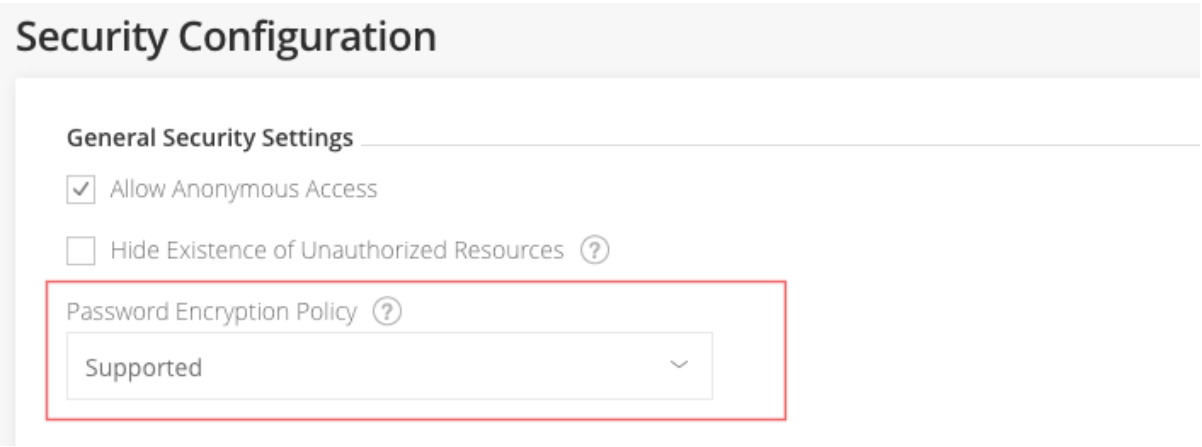
For example, Maven uses cleartext passwords in the `settings.xml` file by default.

Using Maven's built-in support for encrypted passwords and generating passwords on the client side does not overcome the security risks for the following reasons:

1. The login password is decrypted on the client side and ends up as cleartext in memory, and then transmitted over the wire (unless forcing SSL too).
2. The master password used for decryption is stored in clear text on the file system.
3. Password encryption is left to the good will of the end-user and there is no way to centrally mandate it.

A unique solution is provided for this problem by generating encrypted passwords for users based on secret keys stored in the system. You can ensure users' shared passwords are never stored or transmitted as clear text.

You can set a central policy for using or accepting encrypted passwords in the **Administration** module under **Security | Settings** by setting the **Password Encryption Policy** field.



The behavior according to the **Password Encryption Policy** setting is as follows:

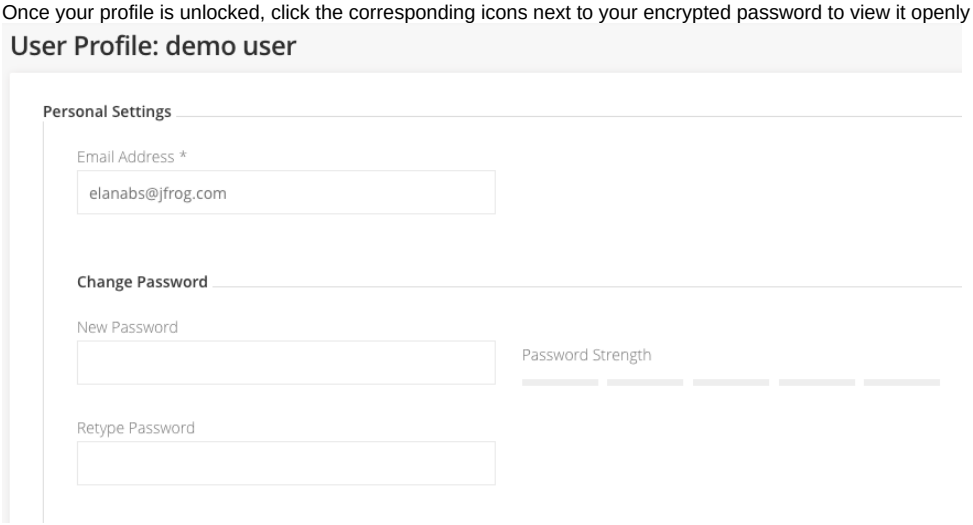
Supported	The system can receive requests with encrypted password (default).
Required	The system requires an encrypted password for every authenticated request.
Unsupported	The system rejects requests with encrypted password.

Using Your Secure Password

To secure your password:

1. Open your profile page (click on your login name on the upper-right corner and select Edit Profile), type-in your password in the **Current Password** field and click **Unlock**.

2. Once your profile is unlocked, click the corresponding icons next to your encrypted password to view it openly or copy it to the clipboard.



Different encryption mechanisms

The encryption mechanisms of the Oracle and IBM JDKs are not identical. Switching from one to another will make your encrypted password obsolete.

IBM JDK Encryption Restrictions

Some of the IBM JRE/JDK are shipped with a restriction on the encryption key size (mostly for countries outside the US); This restriction can be officially removed by downloading unrestricted policy files from IBM and overriding the existing ones:

1. Register and download the unrestricted JCE policy files from the IBM website.
2. Select the correct zip that matches your JAVA version.
3. The downloaded zip file contains 2 jar files - *`local_policy.jar`* and *`US_export_policy.jar`*. Backup the existing files in *`$IBM_JDK_HOME/jre/lib/security`* and extract the jars from the zip file to this location
4. Restart the system.