Password Encryption

Components that are required to authenticate against a database or another repository need to have user credentials specified in configuration files. Such sensitive information can be encrypted so that the actual value of the password will be known only during runtime, protecting Aspire from potential malicious attacks.

On this page

Admin Interface

In general, when using pre-packaged applications and the standard Aspire Admin interface (i.e. http://localhost:50505), all password encryption will be handled automatically. All passwords will be encrypted when stored in configuration files on disk, ZooKeeper, MongoDB or HBase.

Create the Main Password

All password encryption / decryption is based on a main password. Use the following steps to create a new one:

1. Go to ASPIRE_HOME
2. Run *bin\aspire.bat - create_master*. This script creates an encrypted main password file (in the config/passwords directory). This file will contain a random key used to decrypt passwords inside Aspire.

Notes:

- The main password file must be secured by the operating system. This means that administrators should grant read access only to the user running Aspire.
- The main password file path value is stored inside the settings file as a property called "masterPasswordFilePath"

Important security concern

If you skip this step, all the **encryption on Aspire will use the default main password**, which comes with all Aspire Distributions. All of your encrypted passwords will be exposed (to be decrypted in any other Aspire Distribution). **Using a Master Password is *extremely important* to prevent this exposure.**

Password Encryption Aspire Administration UI

If you want to secure Aspire access to the Administration UI using the ConfigFile method, the best and most secure way is by encrypting the passwords. Complete the following steps.

1. Run *bin\aspire.bat -set_passwords.* This script will prompt for the passwords of the "administrator" and "developer" users to be encrypted inside the *settings.xml* file. (For Linux, *bin\aspire.sh* should be used.)
2. Enable the ConfigFile authentication on the *settings.xml* file:

settings.xml

```
<authentication>
  <type>ConfigFile</type>
</authentication>
```

3. Start Aspire and use the "administrator" or "developer" users to log in using the recently added passwords.

Change passwords

If you need to create a new set of passwords, you must go to the *settings.xml* file and remove the *"adminPassword"* and *"developerPassword"* properties from the System Properties section before re-running the bin\aspire.bat -set_passwords script.

Password Encryption for Custom Applications

If you are creating a custom application which requires password encryption, you may need to use the "encryptPassword" script.

- The encrypted password will be stored as a property in the settings.xml file.
- The property should be specified to the appropriate component's configuration in the application.xml file.

To use password encryption, complete the following steps.

1. Run *bin\aspire.bat -encrypt_password*. This script will prompt for the password you need to encrypt, and a property name where the encrypted password will be stored. This property is written to the Aspire settings.xml file.
2. Reference the created property from the component's configuration using ${propertyName} syntax.
3. Make sure your component allows password encryption.

Important Notes

- Operating systems: This functionality has been tested on Windows only.
- By default, Aspire uses a secret pre-configured main password unless an administrator uses **aspire.bat -create_master** to create a new one.