Documentation: Configuring Domain Manager Password Policies in Ambience 4.6.4

This is an example of how to configure the different Domain Manager Password Policies in Ambience 4.6.4

Configuring Domain Manager's Lockout

1. Go to application.config in Ambience Server's /etc directory.
2. Add in the following in application.config:

```
elixir.web.domain-controller.domain-manager {
        max-inactive-interval = 5 minutes
        lockout {
                fail-count: 5
                interval: 2 minutes
        }
}
```

3. Save the configurations.
4. Restart the Ambience Server.

Additional Details:
max-inactive-interval: represents the amount of time a user can be inactive for before the user's session time times out and logs off.
fail-count: represents the number of failed login attempts before the user is locked out.
interval: represents the time the user has to wait after the failed attempts.

Configuring Domain Manager's Password (Must **Have** Symbol Set)

1. 1.Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "mustHaveSymbolSet":" to:
   e.g.
   "mustHaveSymbolSet":",~^*()"

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
Symbol sets can be added based on preferences. In the example above, Domain Manager's password would at least need to have either one of the symbols ,~^*() on the next password change.

Configuring Domain Manager's Password (Must **Not** Have Symbol Set)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "mustNotHaveSymbolSet":" to:
   e.g.
   "mustNotHaveSymbolSet":",~^*()"

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
Symbol sets can be added based on preferences. In the example above, Domain Manager's password must not have any of the symbols ,~^*() on the next password change.

<u>Configuring Domain Manager's Password (Minimum Length)</u>

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "minLength":1 to:
   e.g.
   "minLength":4

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
Minimum length of password can be added based on preference. In the example above, Domain Manager's password needs to be more than 4 characters long on the next password change.

For example,

Example	Output
"pas"	Password change is unsuccessful & would output an error.
"password"	Password change successful.

Configuring Domain Manager's Password (Maximum Length)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "maxLength":0 to:
   e.g.
   "maxLength":10

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
Maximum Length of password can be added based on preference. In the example above, Domain Manager's password needs to be less than 10 characters long on the next password change.

For example,

"password123"	Password change is unsuccessful & would output an error.
"password12"	*Password change successful.*

Configuring Domain Manager's Password (Must Have Digit)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "mustHaveDigit":false to:
   e.g.
   "mustHaveDigit":true

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
The need of having numeric values in Domain Manager's password can be added based on preference. In the example above, the Domain Manager's password needs to have numeric values in the next password change.

Configuring Domain Manager's Password (Must Have Upper Case)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "mustHaveUpperCase":false to:
   e.g.
   "mustHaveUpperCase":true

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
The need of having upper case values in Domain Manager's password can be added based on preference. In the example above, the Domain Manager's password needs to have upper case values in the next password change.

For example,

password	Password change is unsuccessful & would output an error.
Password	Password change is successful

Configuring Domain Manager's Password (Must Have Lower Case)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "mustHaveLowerCase":false to:
   e.g.
   "mustHaveLowerCase":true

4. Save the changes.
5. Restart Ambience Server.

Additional Details:
The need of having lower case values in Domain Manager's password can be added based on preference. In the example above, the Domain Manager's password needs to have lower case values in the next password change.

For example,

PASSWORD	Password change is unsuccessful & would output an error.
pASSWORD	Password change is successful.

Configuring Domain Manager's Password (Not Same As Logon)

1. Login Ambience Server's Domain Manager Page.
2. Click on the 'Configuration' tab & navigate to /module/usergroupsdb/password-policy
3. Edit the contents for "notSameAsLogon":false to:
   e.g.
   "notSameAsLogon":true

4. Save the changes.
5. Restart Ambience Server.

Additional Details:

In the example above, the Domain Manager's password could not be the same as it's logon name.