PASSWORDS SECURITY SETTINGS

WorldAPP allows you to set up the security regulations and to manage the password settings for all account types

User passwords expire in.

Allows you to manage the password validity term. The supported options are:

- Never Expires (by default);
- Expires in .. days (The value must be between 0 and 365).

Enforce password history.

Enables you to determine the number of unique new passwords that have to be associated with a user account before an old password can be reused. The possible options are:

- Is not logged (by default);
- Remember .. passwords (The value must be between 0 and 10).

Password complexity requirement.

This security setting requires the password to meet the complexity requirements. The possible options are:

- No Restriction (by default);
- Must mix alpha and numeric (the password must contain at least one numeral and one letter);
- Must contain special characters (the password must contain one of the following non-alphabetic character: !, ", #, $, %, &, ', (,), *, +, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~).

Minimum password length.

Enables you to set the minimum password length. The supported options are:

- Not Limited (by default);
- At least characters (The value must be between 0 and 16).

Account expiration requirement.

Allows you to limit the term the account can stay idle. The possible options are:

- Never Expires (by default);
- Expires if idle for .. days (The value must be between 0 and 365).

Account lockout policy.

This setting disables a user account if an incorrect password is entered a specified number of times over a specified period. You may set the following option:

- Do not lock accounts (by default);
- Lock accounts for .. minutes after .. invalid attempts (The value must be more than 0 for minutes and between 1 and 10 for attempts).