Recast

LOCAL

Last Modified on 04.16.26

The LOCAL identity source is a built-in identity source which contains the default admin account.

Authentication screen

Enable/disable the methods available to authenticate. The following options are available:

Form authentication – Allow the user to login via the Application Workspace login page (http/https).
Basic authentication – Enable basic login for the identity source.

Contacts screen

Enable contacts – If enabled, contacts from this identity source will be used.
Requires Email – If enabled, all objects without a email address will be hidden.
Show attributes – If you enable the **Description** and **User mail** you allow those attributes to be exposed to Application Workspace.

Account Lockout Policy screen

An account can be locked for a specific time period after too many authentication attempts within a time span.

Invalid logon reset interval – The period of time during which the **Invalid logon threshold** must be reached before the lockout will be applied.
Invalid logon threshold – How many invalid login attempts are allowed before the lockout will be applied.
Lockout duration – The amount of time that an account is locked for.

Password Policy screen

Configure the complexity requirements of the password policy by inserting the minimal number of letters, numbers and special characters (non-alphanumeric character) the password should contain or the password's minimal length.

> Disable a complexity requirement
> If you want to disable one of the complexity requirements, you just have to insert 0 in the corresponding field.