

Confidential storage agenda



When you install new instance of CzechIdM, **is required generate new key** for crypt all values in confidential storage. The key can be changed by long running task **ChangeConfidentialStorageKey**, the LRT you must start after change crypt key, as parameter will be given old confidential storage key.

Agenda in Settings (left menu), where confidential storage values are readable. It is in **read only mode**, so values cannot be changed, removed or added some more. **Confidential storage** permission is needed, otherwise you cannot get in confidential storage agenda. You have to create new role and in tab **Permissions** add permission (entity type = Confidential storage, permission = READ). Now any user with this role assigned has access to Confidential storage agenda.

The confidential storage is currently used for:

- saving the confidentials values from EAV forms
- saving sensitive configuration items

Key	Owner Id	Owner type	Id
eav:fb10fe4a-1452-4089-9ac2-0f475d08e923	8d17c93	eu.bcvolutions.idm.acc.entity.SysSystemFormValue	744ccb0
eav:389119ca-6167-4ff4-9e79-63d32a899dc5	181fc08	eu.bcvolutions.idm.core.model.entity.eav.idmidentityFormValue	7e62a9c
eav:389119ca-6167-4ff4-9e79-63d32a899dc5	4c09a93	eu.bcvolutions.idm.core.model.entity.eav.idmidentityFormValue	e44d121
remoteServerPassword	2b0b0a9	eu.bcvolutions.idm.acc.entity.SysSystem	a9179a

1 - 4 of 4 records

The storage detail shows these information:

- Owner Id - Identifier of entity, which owns confidential storage value.
- Owner type - It's entity type of owner. If system entity has saved value, owner type is SysSystem. But if value is in extended attribute of system, it is saved by extended attribute of system, so owner type would be SysSystemFormValue. It is shown on previous picture.
- Key - It defines value. It is one third of identifier of value. To find one value, exact which we want, is needed key, owner id and owner type.
- Value - It is decrypted password.
- Creator - Identity, which created confidential value.

- Created - Date, when confidential storage value was created.

The screenshot shows the 'Detail encrypted value' page in the czechidm application. The left sidebar contains a navigation menu with items like Examples, Profile, Tasks, Users, Organization, Roles, Systems, Virtual systems, Audit, Notifications, Settings (selected), Configuration, Workflow definitions, Script definitions, Form definitions, Modules, Task scheduler, Password policies, Confidential storage, Tree structures, and Role catalog. The main content area displays the details of an encrypted value with the following fields:

Field	Value
Owner Id	181fc089-57ed-48f5-af55-df471d2a911a
Owner type	eu.bcvolutions.idm.core.model.entity.eav.IdentityFormValue
Key	eav:389119ca-6167-4ff4-9e79-63d32a899dc5
Value	123
Creator	Administrator (admin)
Created	03.11.2017 12:21:04

At the bottom of the page, there is a footer with the text: 'BCV solutions s.r.o. | Help | ServiceDesk | About app'.

Admin guide

- [Confidential storage](#)

Devel guide

- [Confidential storage](#)

From:
<https://wiki.czechidm.com/> - IdStory Identity Manager

Permanent link:
https://wiki.czechidm.com/devel/documentation/confidential_storage

Last update: **2020/06/23 12:24**

