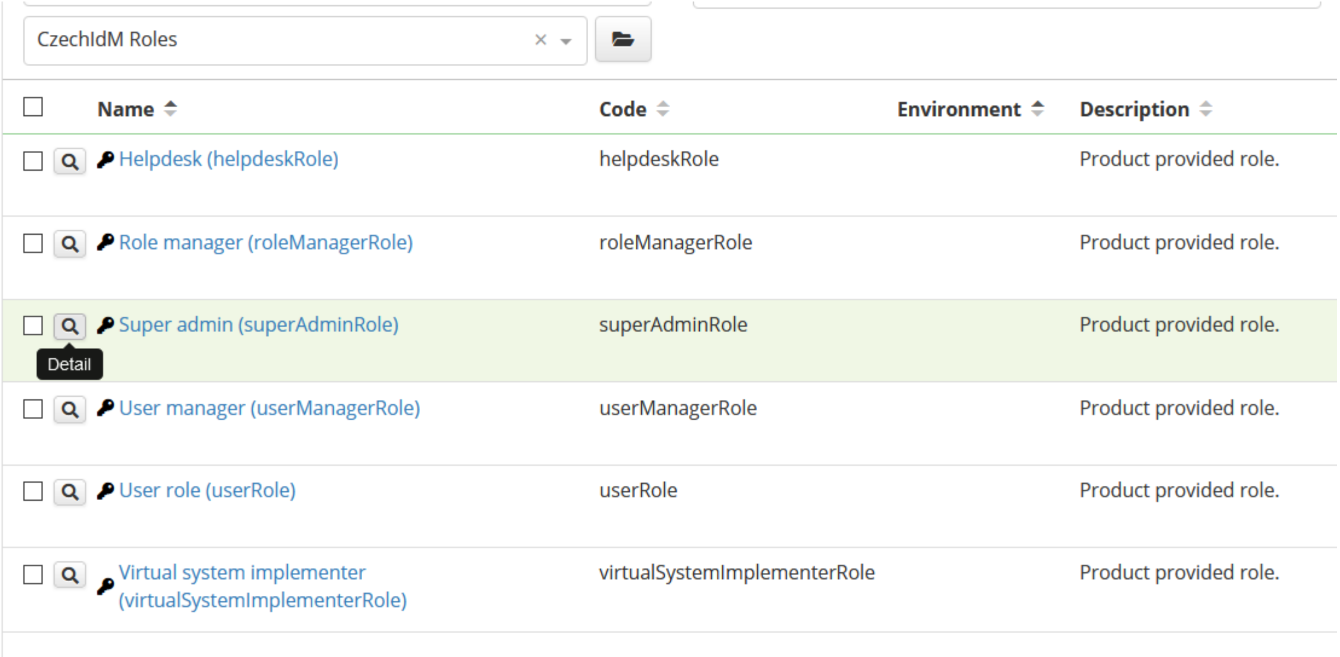
Init application and data

event, demo, init, data, processor

@since 10.5.0

Application init data are checked and created (updated), when application is started. Init data contains product provided roles, form definitions, value generators, password policies, codelist, scheduled task etc. to cover basic CzechIdM usage right after application is instaled or updated.

Application initialization and init data is created by registered processors. Init data is created, when application starts.



CzechIdM Roles

□	Name	Code	Environment	Description
□	Helpdesk (helpdeskRole)	helpdeskRole		Product provided role.
□	Role manager (roleManagerRole)	roleManagerRole		Product provided role.
□	Super admin (superAdminRole)	superAdminRole		Product provided role.
□	User manager (userManagerRole)	userManagerRole		Product provided role.
□	User role (userRole)	userRole		Product provided role.
□	Virtual system implementer (virtualSystemImplementerRole)	virtualSystemImplementerRole		Product provided role.

Product provided processors:

Module	Processor identifier	Description	Order	Disableable
acc	acc-init-synchronization-processor	Cancel synchronizations after server is restarted.	-10010	no
core	core-init-long-running-task-processor	Cancels all previously ran tasks etc. (tasks run, before server was restarted).	-10000	no
core	core-init-script-processor	Init scripts from classpath (file system).	-5200	no
core	core-init-notification-processor	Init notification templates from classpath (file system) and notification configuration from module descriptors.	-5100	no
ic	ic-init-data-processor	Initialize ic module - connector logging.	-5000	no
core	core-init-codelist-processor	Init base codelists (environment).	-300	no
core	core-init-form-definition-processor	Init default extended form definitions for formable types (identity, role, contract, tree node).	-200	no

Module	Processor identifier	Description	Order	Disableable
core	core-init-generator-processor	Init value generators for set default values of extended form attributes (for identity, role request concepts and assigned role attributes).	-100	no
core	core-init-role-catalogue-processor	Init product provided role catalogue item 'CzechIdM Roles'. This item will contain all product provided roles (by person). Catalogue item is created, when no other catalogue item exists.If this processor is disabled, then catalogue item will not be created and product provided roles will be created without catalogue relation.	-50	yes
core	core-init-admin-role-processor	Init administrator role (by configuration 'idm.sec.core.role.admin'). Role is created, when no other role exists (⇒ is the first role in application). Role will not be created, when is deleted and any other role exists. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).	0	no
core	core-init-user-role-processor	Init user role for core module (by configuration 'idm.sec.core.role.default'). Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	10	yes
acc	acc-init-user-role-processor	Init user role for acc module (by configuration 'idm.sec.core.role.default') - adds authorization policies for acc module	15	yes

Module	Processor identifier	Description	Order	Disableable
vs	vs-init-implementer-role-processor	Init implementer role for vs module (by configuration 'idm.sec.vs.role.implementer').Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	20	yes
core	core-init-helpdesk-role-processor	Init helpdesk role for core module (by configuration 'idm.sec.core.role.helpdesk'). Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	30	yes
acc	acc-init-helpdesk-role-processor	Init helpdesk role for acc module (by configuration 'idm.sec.core.role.helpdesk') - adds authorization policies for acc module.	35	yes
core	core-init-role-manager-role-processor	Init role manager role for core module (by configuration 'idm.sec.core.role.roleManager'). Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	40	yes
acc	acc-init-role-manager-role-processor	Init role manager role for acc module (by configuration 'idm.sec.core.role.roleManager') - adds authorization policies for acc module.	45	yes

Module	Processor identifier	Description	Order	Disableable
core	core-init-user-manager-role-processor	Init user manager role for core module (by configuration 'idm.sec.core.role.userManager'). Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated).Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	50	yes
core	core-init-delegation-role-processor	Init role with permissions for a delegations. Role is created, when not exist. Role will not be created, when configuration property is empty (defined, but empty string is given). Role is created with 'SYSTEM' role type - type is checked, when role authorities are created (or updated). Role is placed into role catalogue 'CzechIdM Roles' item, if item is defined.	60	yes
core	core-init-admin-identity-processor	Init administrator identity with 'admin' username. Admin identity is not created, when admin role is not created (not configured by property 'idm.sec.core.role.admin' or deleted). Admin identity is not created, when other identity with admin role (configured by property 'idm.sec.core.role.admin') exists. Admin identity is created with password with never ending expiration. Admin identity is created with profile with show system informaiton is enabled. Change admin password is recomended after identity is created.	100	no
core	core-init-organization-processor	Init default organization type 'Organization structure' with one root tree node 'Root organization'. Tree type and node is created, if no other tree type exists.	200	yes
core	core-init-demo-data-processor	Initialize demo data for application.	3000	has own additional property, see below

Module	Processor identifier	Description	Order	Disableable
core	core-init-password-policy-processor	Init base password policies for password validate and generate, when no other policy is defined. Validation policy set 30s fogin blocking time with 5 unsuccessful login attempts, minimum 8 char length passwords. Generate policy is configured to generate 8-12 char length passwords with 2 lower, 2 upper, 2 number and 2 special chars.	5000	yes
core	core-init-scheduled-task-processor	Schedule core long running tasks.	10000	no
acc	acc-init-scheduled-task-processor	Schedule acc long running tasks.	10100	no
core	core-init-monitoring-processor	Init monitoring manager and product provided monitoring evaluators.	11000	yes
acc	acc-init-monitoring-processor	Init product provided monitoring evaluators.	11010	yes
vs	vs-init-monitoring-processor	Init product provided monitoring evaluators.	11020	yes

Column disableable - processor can be disabled by additional property `idm.sec.core.init.data.enabled=false`. Each processor can be disabled by standard processor configuration with processor identifier usage.

Processors are registered to event type `INIT` for main IdM module (app). If you want to register you processor in custom module, then use prepared `AbstractInitApplicationProcessor` superclass. Processor order is designed to prepare all configurations (e.g. form definitions, password policies) before data is created ⇒ **admin role is created at first on 0 order**.

All registered processors are available in agenda (Settings - Modules - Processors - for ModuleDescriptorDto entity type).

Product provided roles

Roles to cover basic IdM usecases were designed and provided from product (~person). Product roles are checked, when application is started - they are created for new instalations and updated, when new IdM version is installed, or role definition is changed (e.g. when some required authorization policy has been deleted).

Configured role authorization policies are created or updated after application has started. Additional authorization policies can be configured. Authorization policy can be disabled, if is not needed - policy will be not enabled after application has started.

Role type enumeration is used now for product provided roles. Role type SYSTEM is used for all product provided roles and is checked before update role authorization policies, when new CzechIdM version is installed. **Authorization policies updates can be disabled by changing the role type to any other ⇒ role policies will not be updated** and vice versa, authorization policies updates for roles created before IdM version 10.5.0 can be enabled (e.g. for user role) by changing the role type to SYSTEM.

Configured **authorization policies are updated by** complex key - combination of **authorizable type and evaluator type**.

Examples:

- When authorization policy is removed - then is created again after application starts.
- When authorization policy is changed (permissions or additional configuration properties) - then is updated to product provided configuration again after application starts.
- When authorization policy is added to product provided role - it's preserved without change. **Be careful - different combination of authorizable type and evaluator type can be added only**.
- When authorization policy is disabled, then is updated to product provided configuration again after application starts, but it's still disabled.

Default user role can be changed three ways (best practice):

- Default user role supports sub roles @since 10.5.0 version - **new authorization policies can be configured to new role and role can be defined as sub role**,
- SYSTEM role type of default user role can be removed - when authorization policy has to be removed (~ prevent to update role policies after restart).
- If product provided role contains authorization policy, which is not needed ⇒ policy can be disabled and is not effective anymore.

Configuration property `idm.sec.core.init.data.enabled=false` disable creation and authorization policies updates at all (with other init processors above).

Product provided role codes can be changed by role configuration. When role is configured, but code is empty (empty string as value e.g. `idm.sec.core.role.default=`), then role will not be created (and used as default role in this example).

Product provided roles:

Person	Default role code	Description	Configuration property to change code	Processor
Super admin	superAdminRole	Application administrator - APP_ADMIN authority is configured only.	`idm.sec.core.role.admin`	core-init-admin-role-processor

Person	Default role code	Description	Configuration property to change code	Processor
User	userRole	Default role for all users - authorization policies configuration	`idm.sec.core.role.default`	core-init-user-role-processor
Helpdesk	helpdeskRole	Helpdesk user role - authorization policies configuration	`idm.sec.core.role.helpdesk`	core-init-helpdesk-role-processor
User manager	userManagerRole	User manager - authorization policies configuration	`idm.sec.core.role.userManager`	core-init-user-manager-role-processor
Role manager	roleManagerRole	Role manager - authorization policies configuration	`idm.sec.core.role.roleManager`	core-init-role-manager-role-processor
Virtual system implementer	virtualSystemImplementerRole	Approve requests for virtual system - authorization policies configuration	`idm.sec.vs.role.implementer`	vs-init-implementer-role-processor
Delegation	delegationRole	Default permissions for delegations - authorization policies configuration	`idm.sec.core.role.delegation`	core-init-delegation-role-processor

Roles are created by registered processors. Role is not created, when processor is disabled by configuration.

When role environment is used, when configuration properties has to contains environment too e.g. `superAdminRole|production`

Scheduled tasks

Module	Task	Parameters	Desrciption	Schedule
core	PasswordExpiredTaskExecutor		Send notification for user after password expired and publish PASSWORD_EXPIRED event.	00.05
core	SelectCurrentContractSliceTaskExecutor	-	Recalculate current using slices as contract. Find all slices which should be for actual date using as contract and copy their values to parent contracts.	0.30

Module	Task	Parameters	Desrcription	Schedule
core	HrEnableContractProcess	-	Start of contract validity - before end and expire.	0.35
core	IdentityRoleValidRequestTaskExecutor	-	Start of assigned role validity.	0.45
core	HrEndContractProcess	-	End of contract validity - scheduled before default contract expiration (this task works with disabled state too and set identity state by contract state).	0.50
core	HrContractExclusionProcess	-	Exclude contract.	0.55
core	IdentityContractExpirationTaskExecutor	-	Remove roles by expired identity contracts (⇒ removes assigned roles).	1.00
core	IdentityRoleExpirationTaskExecutor	-	Remove expired roles.	1.15
core	DeleteExecutedEventTaskExecutor	numberOfDays: 3	Delete executed entity events.	2.00
core	RemoveOldLogsTaskExecutor	removeRecordOlderThan: 90	Delete old logs from event logging tables (events, eventException and eventProperty).	2.05
acc	DeleteProvisioningArchiveTaskExecutor	numberOfDays: 90, operationState: EXECUTED, emptyProvisioning: true	Delete EXECUTED archived provisioning operation.	2.15
core	DeleteLongRunningTaskExecutor	numberOfDays: 90, operationState: EXECUTED	Delete old executed long running tasks.	2.20
core	DeleteNotificationTaskExecutor	numberOfDays: 180, sentOnly: true	Delete old sent notifications.	2.25
acc	DeleteSynchronizationLogTaskExecutor	numberOfDays: 180	Delete old synchronization logs.	2.35
acc	AccountProtectionExpirationTaskExecutor	-	Removes accounts with expired protection.	2.40
acc	RetryProvisioningTaskExecutor	-	Retry failed operation in provisioning queue.	every 5 minutes

Demo data

Demo data is created by registered processor `InitDemoDataProcessor` (`core-init-demo-data-processor` in table above). Demo data is created, when configuration property `idm.sec.core.demo.data.enabled=true` is set and processor is enabled.

Demo data creates:

- Example users with product provided roles assigned.
- Example tree nodes in product provided tree structure.
- Form projection for externe users.

From:
https://wiki.czechidm.com/ - **CzechIdM Identity Manager**

Permanent link:
https://wiki.czechidm.com/devel/documentation/architecture/dev/events/init-data

Last update: **2021/10/06 12:20**