

IDR Manager Software

User Guide



Version history

Table 1: Version history

Version	Date	Description
4.0	23.08.2021	Adaption to Version 4 of the IDR Manager Software
4.0.2	19.11.2021	Adaption to Version 4.0.216 of the Software
4.0.3	13.05.2022	Adaption to Version 4.0.391 of the Software
4.0.5	05.12.2022	Adaption to Version 4.0.509 of the Software
4.1.0	24.02.2023	Adaption to Version 4.1.0 of the Software

Disclaimer

The information in this document may change without further notice.

Trademarks and copyright

The trademarks used in this document are the property of integrative management solutions or corresponding owner.

Intellectual property rights protect © 2023 IDR concept and IDR Manager.

Content

- Introduction..... 10
- What is IDR Manager?..... 10
- System requirements 12
- Where can IDR Manager be hosted? 13
 - Windows Server 13
 - Update TLS Certificate..... 18
- Update IDR Manager..... 18
- Open the IDR Manager Website 18
- Views 20
 - Tile view..... 22
 - Table view..... 23
 - Service view..... 24
 - Business view 25
 - Recovery plan view..... 26
 - Gantt view 26
- Tenants..... 28
 - Create tenants..... 28
 - Update tenants..... 29
 - Delete tenants..... 30
 - Clone tenants 30
- Users..... 32
 - Create users..... 32
 - Update user 34
 - Delete user 35
- Audit Logs 36
- Business Processes 38
 - Create business processes..... 38
 - Update business processes 39
 - Delete business processes..... 39
- IT services 41
 - Create IT services..... 41
 - Update IT services 42
 - Delete IT services..... 42
- Applications 44
 - Create applications..... 44

Update applications	45
Delete applications.....	46
On premises assets.....	47
Create on premises assets.....	47
Update on premises assets	48
Delete on premises assets.....	48
Cloud assets.....	50
Create cloud assets.....	50
Update cloud assets	51
Delete cloud assets.....	51
Remote assets	53
Create remote assets	53
Update remote asset.....	54
Delete remote asset	54
Task Items.....	56
Create task items.....	56
Update task items.....	57
Delete task items.....	58
Scenarios	59
Create scenarios	59
Update scenarios.....	60
Delete scenarios	60
Roles	62
Create roles	62
Update roles.....	62
Delete roles	63
Persons	64
Create persons	64
Update persons	65
Delete persons.....	65
Working with IDR Manager	67
Version history from updates.....	67
Download User Guide	67
Check of consistency	68
Collaboration within IDR Manager	68
Create objects.....	68

Update objects	68
Delete objects.....	69
Conclusion of a recovery plan	69
Recovery plan	70
Create a recovery plan	70
Update a recovery plan	71
View recovery plan information.....	73
Update recovery plan	73
Conclude recovery plan.....	74
Delete recovery plan	75
Personal menu.....	76
Change password	76
2-Factor-Authentication	77
Reports	80
General handbook.....	80
Business view.....	82
Service view	84
Role view	86
Asset history	87
Orphaned elements.....	88
BCM documents	90
Importing.....	91
Exporting	92
Attachments	93
Dependencies RPO, MTPD and RTO.....	93

Register of figures and tables

Figure 1: Explanation of the parameters MTPD, RTO, RPO and emergency operation level (BSI standard 200-4 S.90)	10
Figure 2: Login	18
Figure 3: Forgot password.....	19
Figure 4: IDR Manager user interface	20
Figure 5: Change view of a business process	21
Figure 6: Tile view.....	22
Figure 7: Searching in the tile view	22
Figure 8: Table view.....	23
Figure 9: Searching in the table view	23
Figure 10: Service view.....	24
Figure 11: Note sum RTO service view.....	24

Figure 12: Service as tree structure.....	24
Figure 13: Business view	25
Figure 14: Business processes in general overview	25
Figure 15: recovery plan view	26
Figure 16: Gantt view	27
Figure 17: Gantt warning.....	27
Figure 18: Manage menu	28
Figure 19: Create tenant (1/2).....	28
Figure 20: Create tenant (2/2).....	29
Figure 21: Update tenant	30
Figure 22: Delete tenant.....	30
Figure 23: Clone tenant.....	31
Figure 24: User overview.....	32
Figure 25: Create user	33
Figure 26: Add user to a tenant.....	34
Figure 27: Update user	35
Figure 28: Delete user	35
Figure 29: Audit log	36
Figure 30: Detailed audit log entry.....	37
Figure 31: Filter audit logs.....	37
Figure 32: Create business process	38
Figure 33: Update business process.....	39
Figure 34: Delete business process	40
Figure 35: Create IT services.....	41
Figure 36: Update IT services	42
Figure 37: Delete IT service	43
Figure 38: Create application	44
Figure 39: Note RTO	45
Figure 40: Update application	45
Figure 41: Delete application	46
Figure 42: Create on premises asset	47
Figure 43: Update on premises asset	48
Figure 44: Delete on premises assets.....	49
Figure 45: Create cloud assets.....	50
Figure 46: Update cloud assets	51
Figure 47: Delete cloud asset	52
Figure 48: Create remote asset	53
Figure 49: Update remote asset.....	54
Figure 50: Delete remote asset	55
Figure 51: Create task item	56
Figure 52: Upload assets	57
Figure 53: Update task item	57
Figure 54: Delete task item	58
Figure 55: Create scenario.....	59
Figure 56: Update scenario	60
Figure 57: Delete scenario.....	61
Figure 58: Create role	62
Figure 59: Update role.....	63
Figure 60: Delete role	63

Figure 61: Create person	64
Figure 62: Update person.....	65
Figure 63: Delete person	66
Figure 64: Changelog IDR Manager.....	67
Figure 65: Check of the consistency.....	68
Figure 66: Creation of an IT service through another user	68
Figure 67: Update it service through another user.....	69
Figure 68: Delete IT service through other user.....	69
Figure 69: Message when concluding a recovery plan	69
Figure 70: Create recovery plan	70
Figure 71: Active disaster case	71
Figure 72: Note recovery plan.....	71
Figure 73: Update status in a recovery plan.....	72
Figure 74: Close a disaster case.....	72
Figure 75: Recovery plan menu.....	73
Figure 76: Show plan info.....	73
Figure 77: Update recovery plan.....	74
Figure 78: Conclude recovery plan.....	74
Figure 79: Time differences recovery plan.....	75
Figure 80: Personal menu.....	76
Figure 81: Password change.....	76
Figure 82: Configure 2FA.....	77
Figure 83: Recovery codes.....	78
Figure 84: Disable 2FA.....	79
Figure 85: Report overview	80
Figure 86: Choice of business processes for the general handbook.....	80
Figure 87: Business process overview general handbook.....	81
Figure 88: Snippet of a general handbook	82
Figure 89: Choice of business processes for the business view	83
Figure 90: Snippet of a business view	83
Figure 91: Choice of IT services for the service view.....	84
Figure 92: Overview IT services	85
Figure 93: Snippet of a service view.....	85
Figure 94: Create role view	86
Figure 95: Snippet of a role view.....	87
Figure 96: Create asset history.....	88
Figure 97: Snippet of an asset history	88
Figure 98: Create orphaned elements.....	89
Figure 99: Snippet of orphaned elements.....	89
Figure 100: BCM documents	90
Figure 101: Import business process.....	91
Figure 102: Match properties on import.....	92
Figure 103: Overview on new and modified objects.....	92
Figure 104: Export business processes.....	93
Figure 105: Snippet of an export.....	93
Figure 106: Explanation of the parameters MTPD, RTO, RPO and emergency operation level (BSI Standard 200-4 S.90)	94

Table 1: Version history..... 2
Table 2: Navigation bar 21

List of Abbreviations

BCM	Business Continuity Management
CSV	Comma Separated Value
DR	Disaster Recovery
GUID	Globally Unique Identifier
IDR	Integrative Disaster Recovery
IIS	Internet Information Services
KPI	Key Performance Indicators
ITSCM	IT Service Continuity Management
MTPD	Maximum Tolerable Period of Disruption
QR Code	Quick Response Code
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SQL	Structured Query Language
TLS	Transport Layer Security

Introduction

The IDR Manager is one element of the concept „Integrative Disaster Recovery“ (IDR) Management. IDR Manager helps organize and streamline the access of recovery procedures, which are part of a Disaster Recovery plan. IDR Manager allows a structured creation and organization of a Disaster Recovery (DR) Handbook.

The IDR Manager is based on standards 100-4 and 200-4 of the German Federal Office for Information Security, formal known as Bundesamt für Sicherheit in der Informationstechnik (BSI); therefore, the Audit Log is BSI compliant.

What is IDR Manager?

With the usage of “IDR Manager”, you gain an immediate and comprehensive view over the entire IT infrastructure. IDR Manager is a central repository, which grants fast access to the recovery procedures, should a disaster occur. IDR Manager is not specifically designed to automatically trigger recovery plans.

When starting IDR Manager, you will first find all business processes, IT services, applications, infrastructure assets located on premise, in the cloud, or remotely, as well as task items, roles and personnel. This information is required to recover systems and data, in case of a disaster.

IDR Manager helps IT personnel to act quickly and access recovery steps and procedures. Users can easily identify dependencies between layers of the DR plan. The recovery plans and processes are stored as task items and linked to the concerned application(s) or IT service(s).

All required applications and tasks in the event of a disaster can be recorded and retrieved in terms of their recovery time objectives (RTO) and mutual dependencies.

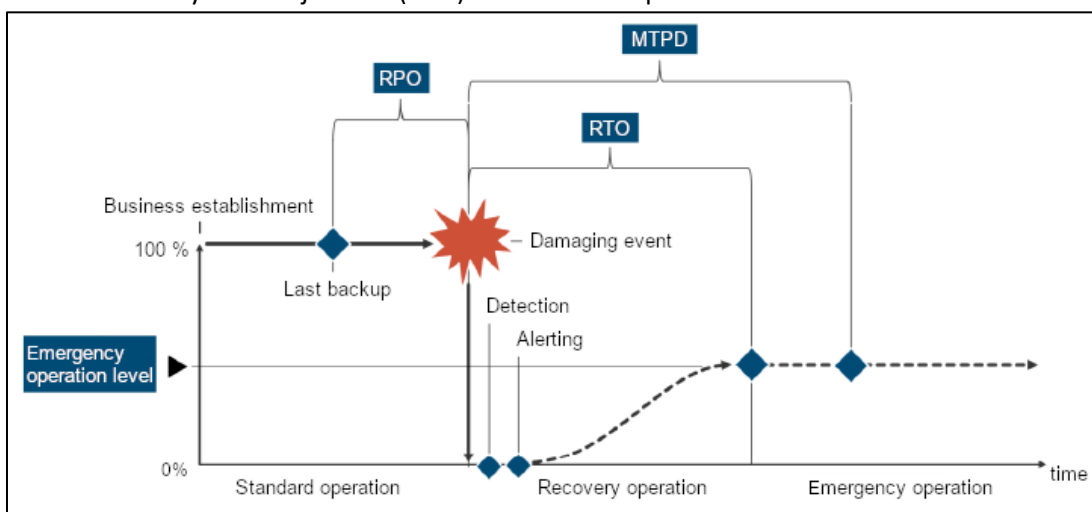


Figure 1: Explanation of the parameters MTPD, RTO, RPO and emergency operation level (BSI standard 200-4 S.90)

Updating IDR Manager is pretty straight forward. It enables a fast and automatized change management, which allows to work with up-to-date DR handbooks as hardcopy version. This is sometimes needed for documentation and certification purposes.

Technical changes, such as additional DR tasks, or organizational personnel changes can be edited.

IDR Manager Admins can grant access and write permissions. This ensures, that only authorized users are able to modify the information. These permissions are assigned through roles and only the IDR Manager tenant or global admin can adjust these permissions. Therefore, all users involved in a disaster recovery activity will be able to work on their tasks and have access to the relevant information in the DR handbook. IDR Manager is a cloud-based solution and thus independent of a datacenter.

It is possible to export the stored information in PDF format. This way you can access the information in other tools, or store it for compliance workflows.

System requirements

Operating System:

- Windows Server 2016 64 Bit
- Windows Server 2019 64 Bit

Hardware:

- 2 CPU Cores (virtual or physical)
- At least 4 GB RAM
- At least 15GB free Disk Space for the installation
- Additional Disk Space for Assets needed (An additional storage device is recommended)

Software:

- .Net Framework 4.6.1
- SQL Server Express 2017 (is included)
- .NET Core Hosting Bundle 5.0.0 (is included)
- Windows IIS feature (automatically installed)

Permissions needed on the Operation System:

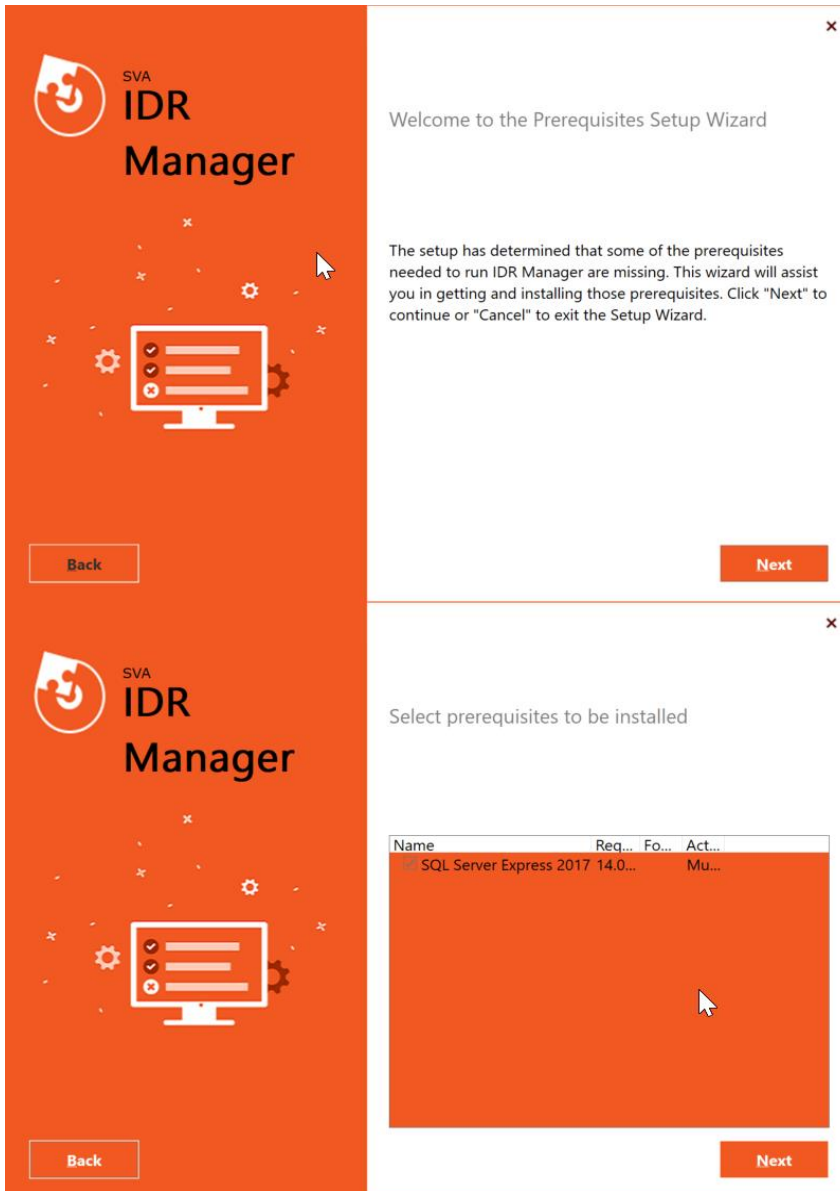
Local administration permissions are required for the installation. During the installation process, the software will create a local service user, which will run the software.

Where can IDR Manager be hosted?

IDR Manager can be hosted in an on premise environment or as a service using the SVA IDR Manager Cloud service.

Windows Server

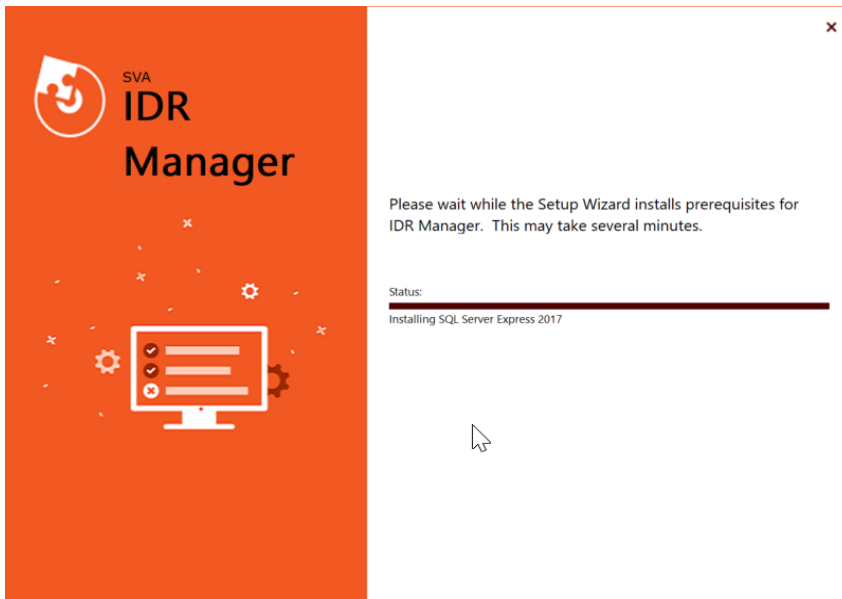
When installed on Windows Server, IDR Manager runs as an IIS website. Required features and software will be installed during the setup. It is possible to edit the IIS site subsequently, for example to update the IP address or a TLS certificate.



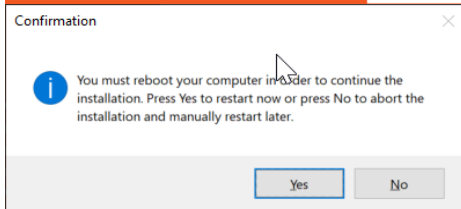
Launch the installation window.

If SQL Server Express 2017 is missing, you will be prompted for installation.

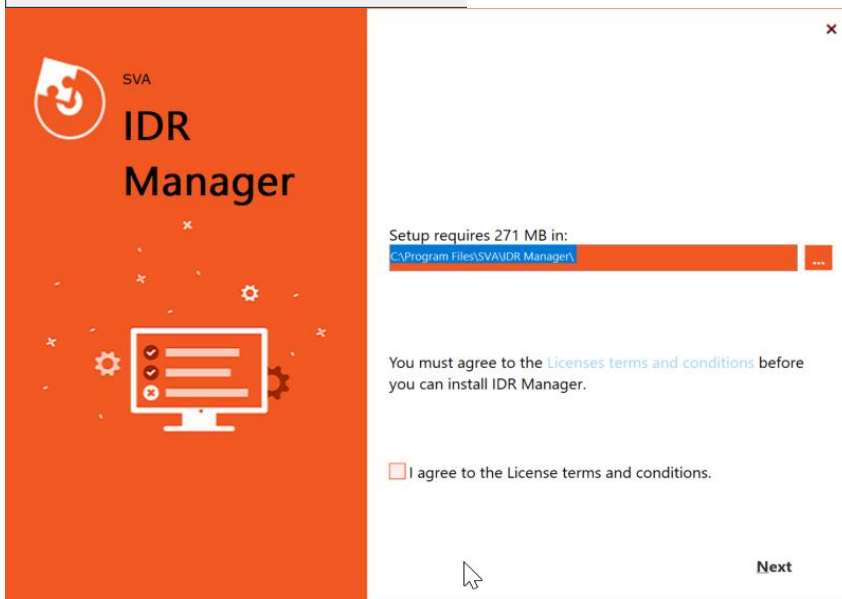
Important: Windows has to be up-to-date at this point.



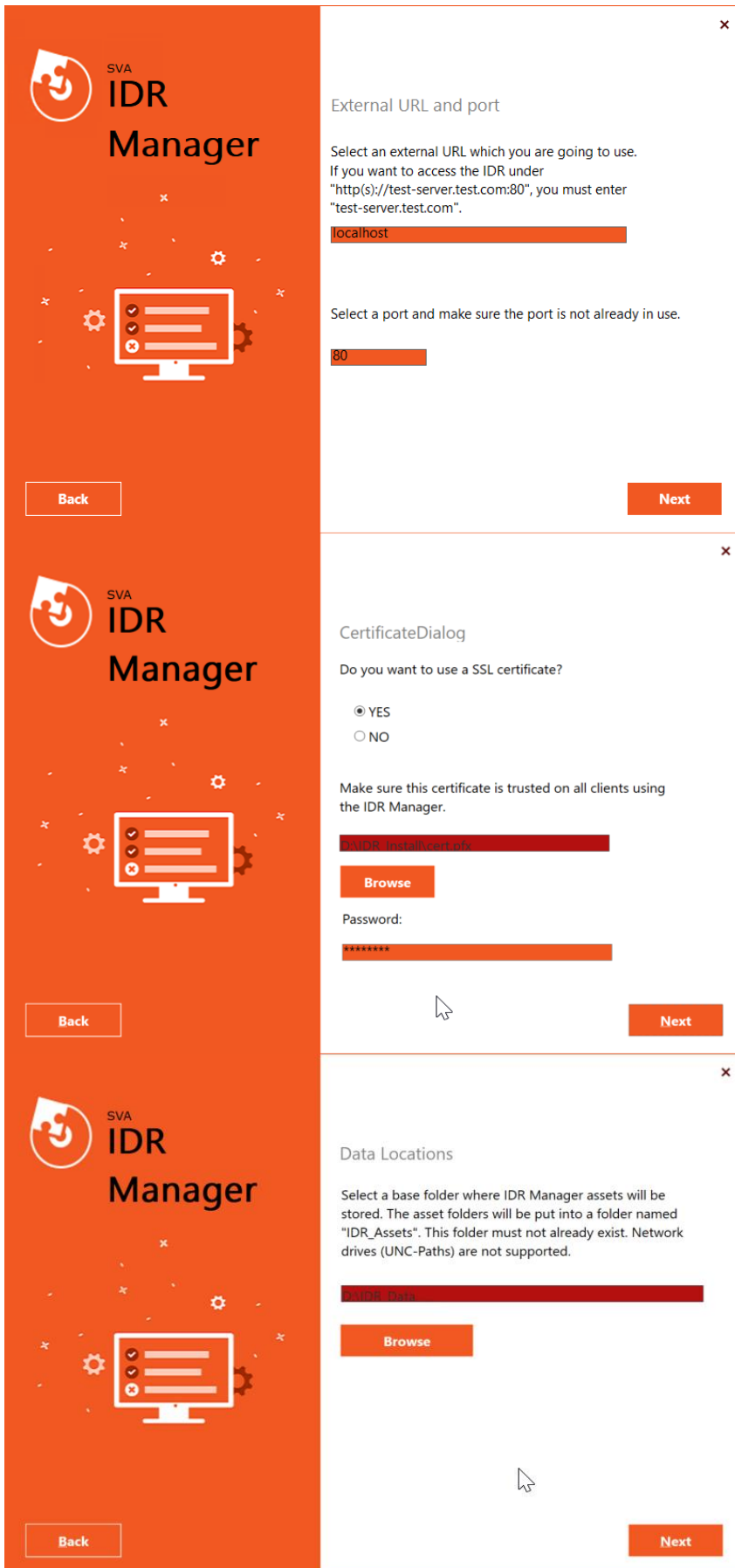
Installation of SQL Server Express 2017.



A restart is required after installing SQL Server.



Setting the installation path.



Setting an external hostname and port.

Important: when using a firewall or reverse proxy, type in the external IP address.

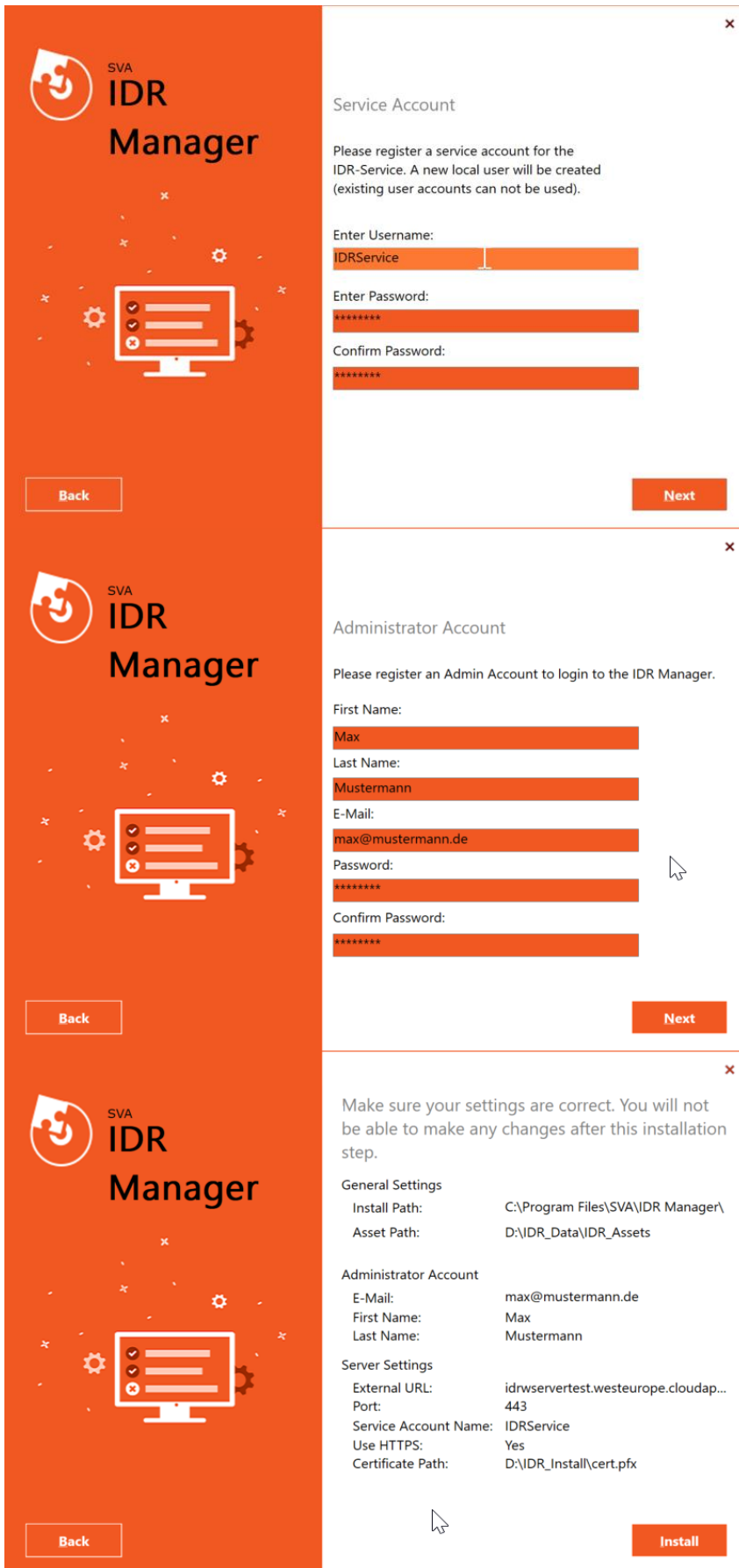
It is also possible to update these settings in IIS Manager after installation at a later stage.

Configuring a TLS certificate.

The certificate is automatically saved in the Windows Certificate Store.

Defining the IDR data path to store assets.

An additional storage disk is recommended.



Registration of IDR Manager Windows service account. The account runs the Application Pool.

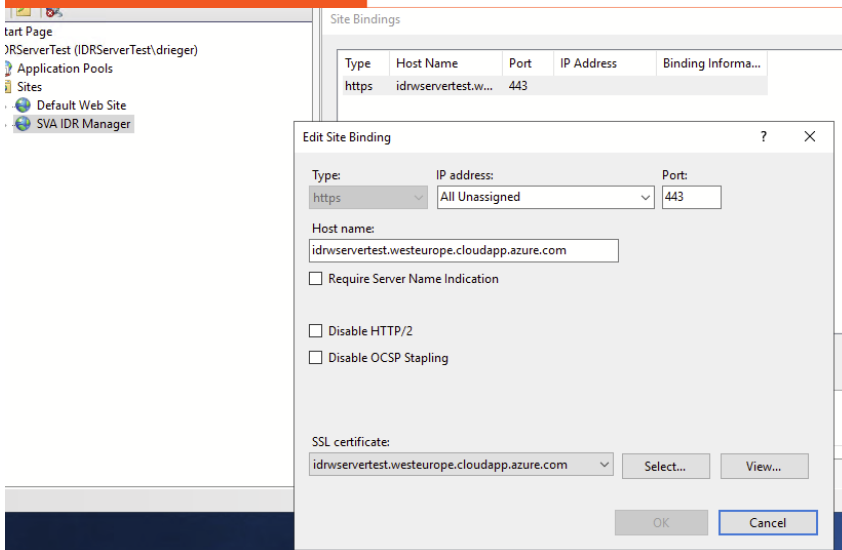
Registering the administrator account of IDR Manager.

Confirming the entered administrator data.



Execution of installation process.

IDR Manager has been successfully installed.



The installation creates an IIS instance. There you can change the settings, if needed.

Update TLS Certificate

To update the Transport Layer Security (TLS) certificate of IDR Manager, use the IIS Manager administration console. Import the new certificate to the Windows Certificate Store. After that, it is possible to change the certificate in the binding setting of IIS Manager.

Update IDR Manager

When updating IDR Manager, the old version will be completely replaced by the new one. To ensure that no data is lost, the old data will be stored in a backup folder, located on the installation path. The backup folder stores the installation files, assets and certificate. The name of the backup folder will be assigned by the system. The naming convention of the folder is represented by the Globally Unique Identifier (GUID) followed by the date, as such: “{GUID}yy-MM-dd_HH-mm-ss”.

Important: After uninstalling IDR Manager all data will be lost. During the uninstallation, the system will prompt you to confirm, whether the used assets should be further stored or deleted.

All data, except assets is stored in SQL Server Express. The name of the database is „IDR-Manager“. Uninstalling the software will not delete the database files.

Open the IDR Manager Website

For those who purchased the SVA IDR Manager cloud service, an initial tenant will be created. In the following use case, the Website URL is:

- <https://idr.sva.de/>



The screenshot shows a login form with the following elements:

- Title: Login
- Field 1: User Email * (input type="text")
- Field 2: User Password * (input type="password" with a toggle icon)
- Link: [Forgot Password?](#)
- Button: LOGIN

Figure 2: Login

SVA initially creates a username (e-mail address) and password and sends it to the defined e-mail address. The password will only be valid for the first login. It is required to change the password, when logging in for the first time.

For the installation of the on premise version of IDR Manager, an IP address or hostname and port will be needed. The IP address or hostname are used to open IDR Manager in a browser.

These are the standard website address formats:

- <https://<ip>:<port>> or
- <https://<hostname>:<port>> or
- <https://<hostname or ip>> with default port (80 or 8080)

For example, <https://10.200.200.2/> is a correct website address.

The login window will open, when the website is accessed, see Figure 2: Login. The e-mail address and password are required to log in. At this point, the login information of the administrator account was already set during the installation of IDR Manager.

It is possible to reset forgotten passwords. To do this, users need to click on “forgot password?”. They will receive a new one-time password on the configured e-mail address, when the system recognizes the e-mail address, as being linked to an account.

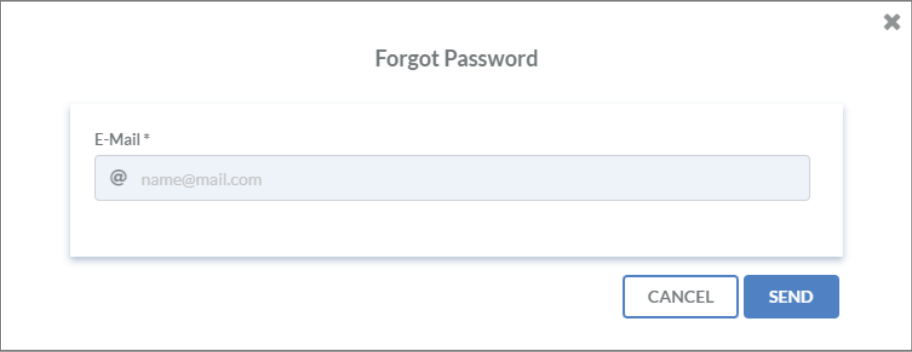


Figure 3: Forgot password

Views

The user interface displays all disaster recovery relevant information. The information is arranged in different tiles. The default view is the table view.

The information shown is split as follows:

- Business processes
- IT services
- Applications
- On premise assets
- Cloud assets
- Remote assets
- Task items
- Roles
- Persons

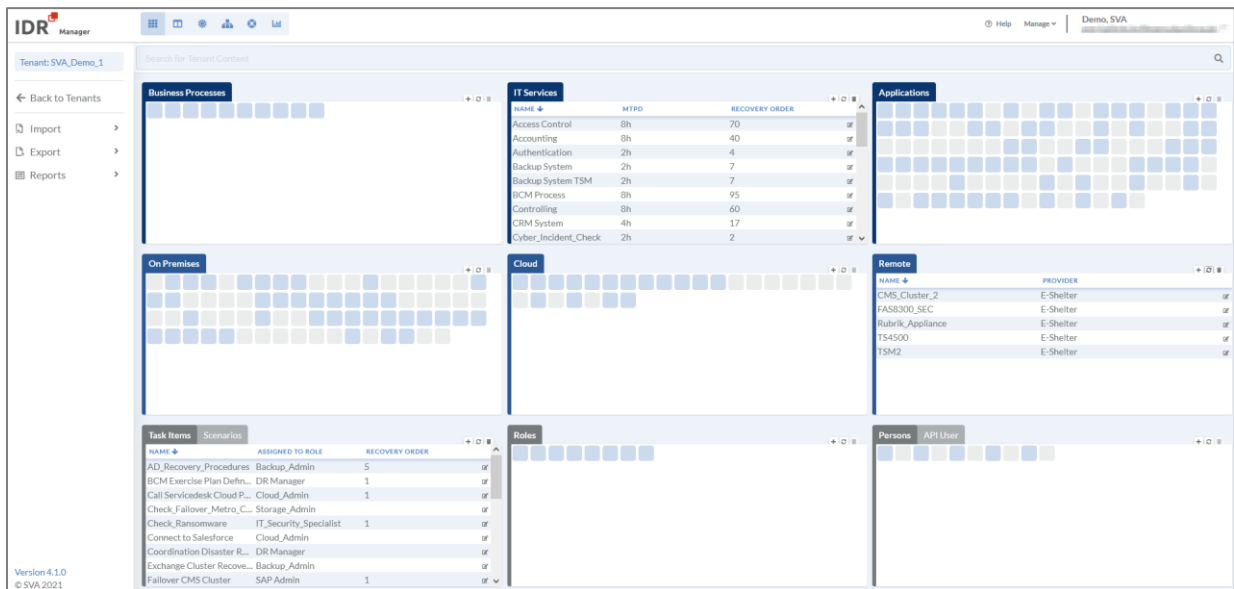







Figure 4: IDR Manager user interface

The information can be viewed either as tiles and tables, or you can select and isolate data for services or business processes. The different colors of tiles show, whether the element is linked to another element or is orphaned.

To change the view, there is a navigation bar on the upper left, see the following table.

Table 2: Navigation bar

Tile view 	In this view, the information is presented in tiles. If you click or hover over a tile, you'll see dependencies between elements, for example IT services.
Table view 	Here, the information is presented in tables.
Service view 	In the service view, you'll directly see dependencies between IT services and applications.
Business view 	In this view, various types of information of business processes will be presented in a tree structure.
Recovery view 	In this view, it is possible to view and create a recovery plan for each IT service.


As preferred, the view can be changed between tile and table view. To change the view, click the  button in a tile.



Figure 5: Change view of a business process

Tile view

In this view, all information is structured in tiles. If a tile is blue, then it has a relationship to at least another element.

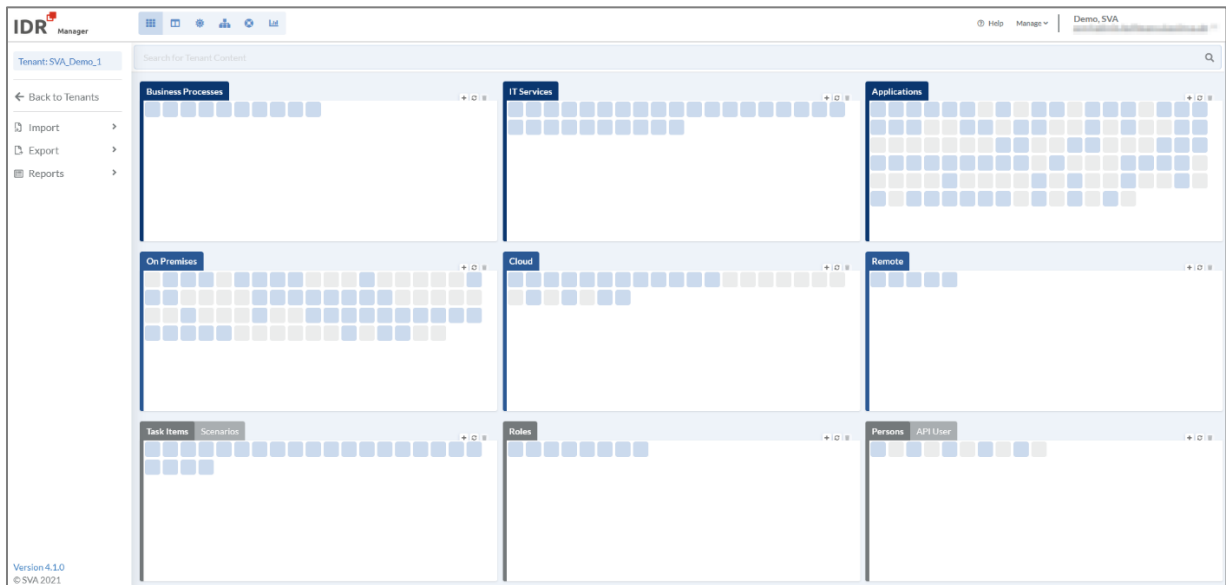


Figure 6: Tile view

When you hover over a tile, dependencies will be highlighted in blue. You can find more information on page 67.

You can also find a search bar, which might come in handy. To search, type the name of an element in the search bar. If an element exists, the associated tiles will be highlighted, see Figure 7: Searching in the tile view.

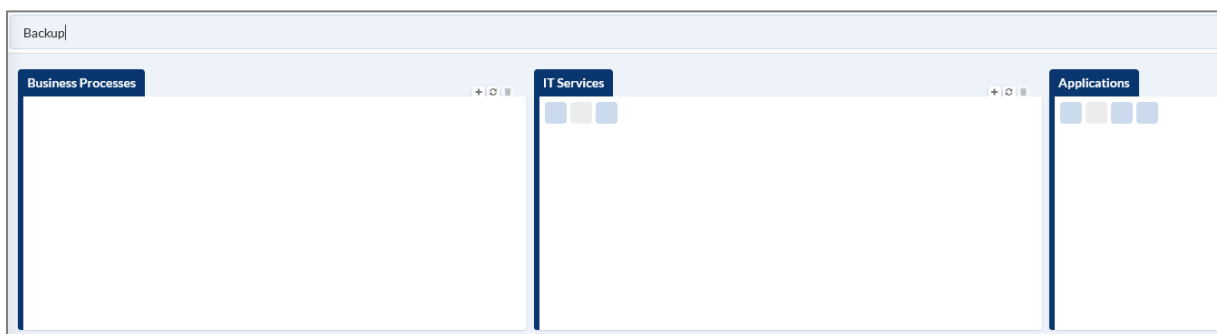


Figure 7: Searching in the tile view

Table view

In this view, the information is shown in a table.

The screenshot shows the IDR Manager interface with a search bar at the top containing 'Tenant: SVA_Demo_1'. The main content area displays several tables:

- Business Processes:** A table with columns NAME, OWNER, and RECOVERY ORDER. It lists various processes like BCM_S, Corporate Management, Customer_Service, etc.
- IT Services:** A table with columns NAME, MTPD, and RECOVERY ORDER. It lists services like Access Control, Accounting, Authentication, etc.
- Applications:** A table with columns NAME, RTO, and RECOVERY ORDER. It lists applications like Access_Points_Office, Access_Points_Workshop, etc.
- On Premises:** A table with columns NAME and LOCATION. It lists items like Artec_Appliance, ASX_DC01, etc.
- Cloud:** A table with columns NAME and CLOUD PROVIDER. It lists services like Analytics_1, Analytics_2, etc.
- Remote:** A table with columns NAME and PROVIDER. It lists items like CMS_Cluster_2, IAS300_SEC, etc.
- Task Items:** A table with columns NAME, ASSIGNED TO ROLE, and RECOVERY ORDER. It lists tasks like AD_Recovery_Procedures, BCM_Exercise_Plan_Defin..., etc.
- Roles:** A table with columns NAME and RESPONSIBILITY. It lists roles like Backup_Admin, Cloud_Admin, Database_Admin, etc.
- Persons:** A table with columns NAME and COMPANY. It lists individuals like Todt, Michael, Alan Adam, Tenant, etc.

Version 4.0.509 © SVA 2021

Figure 8: Table view

It is also possible to search for elements in the search bar, see Figure 9: Searching in the table view.

The screenshot shows the IDR Manager interface with a search bar containing 'Backup'. The main content area displays the following tables:

- Business Processes:** Empty table.
- IT Services:** A table with columns NAME, MTPD, and RECOVERY ORDER. It lists Backup System (2h, 7) and Backup System TSM (2h, 7).
- Applications:** A table with columns NAME and RTO. It lists Backup_VM (0:00), Rubrik Cluster (4:00), Rubrik_Cloud_Backup (2:00), and TSM (2:00).

Figure 9: Searching in the table view

Service view

In this view, all information of services and their corresponding applications is shown, see Figure 10: Service view.

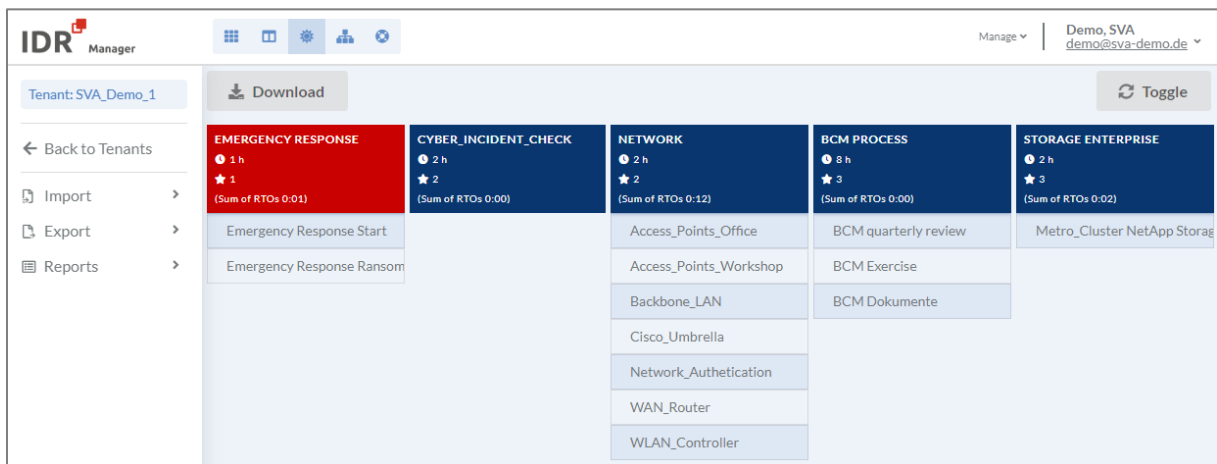


Figure 10: Service view

By default, all applications are colored blue. If a disaster case has been created for a service, the service will be colored red.

If the sum of all RTOs of an application is higher than or equal to the MTPD of the IT service, users will receive a notification on that service, see Figure 11: Note sum RTO service view.

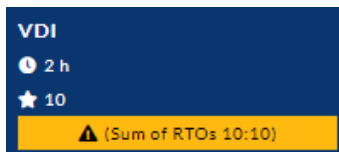




Figure 11: Note sum RTO service view

To download the service view for other documents, click on the  **Download** button. Afterwards the overview will be downloaded as PNG file.

With the  **Toggle** button it is possible to switch between total overview and tree structure. To see the services in tree structure, you need to select the specific service you want to examine in the search bar, see Figure 12: Service as tree structure.

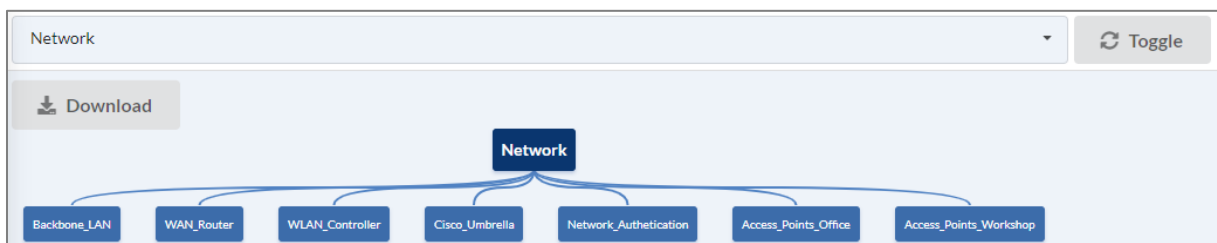


Figure 12: Service as tree structure

Business view

In this view, a business process can be selected via search bar. After selecting a process, all related applications and IT services will be shown in a tree structure. It offers a great view over applications and IT services, that are part of a disaster case.

The search bar is empty by default. When typing in the search bar, the system will recommend relevant results based on names of business processes.

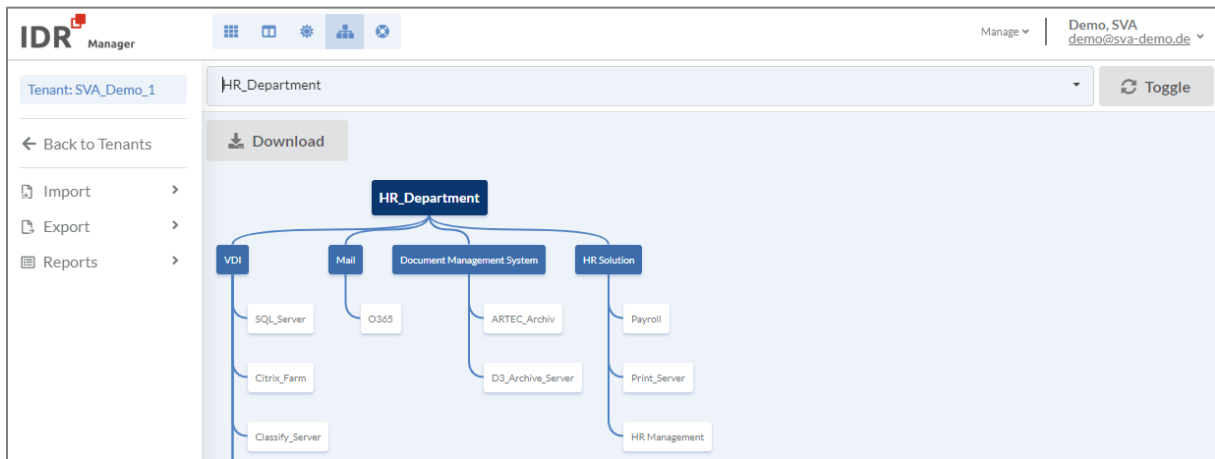


Figure 13: Business view

To download the business processes in a tree structure for other documents, click on the

Download button. The tree structure will then be downloaded as PNG file.

The **Toggle** button enables switching between tree structure and general overview, see Figure 14: Business processes in general overview.

IT SERVICE CONTINUITY MAN.		CORPORATE MANAGEMENT		IT DEPARTMENT		CUSTOMER_SERVICE		SALES_DEPARTMENT	
★ 1	CIO	★ 3	CEO	★ 5	CIO	★ 10	COO	★ 20	CFO
Emergency Response		BCM Process		Network		VDI		CRM System	
Cyber_Incident_Check		VDI		Storage Enterprise		CRM System		SAP BI	
BCM Process		SAP BI		Authentication		Mail		Mail	
DR Testing Mode		Mail		Backup System		Dealer Management System		Accounting	
				Storage		Partner Portal		Dealer Management System	
				Backup System TSM		Document Management System		Printservice	
				VDI				Telephone System	
				Database_Systems					

Figure 14: Business processes in general overview

Recovery plan view

When an IT service is threatened by a disaster, at least one recovery procedure is needed. To create a recovery plan, you first need to switch to the recovery plan view, see Figure 15: recovery plan view.

In the recovery plan view, you can also use the select bar, to browse through existing recovery plans.

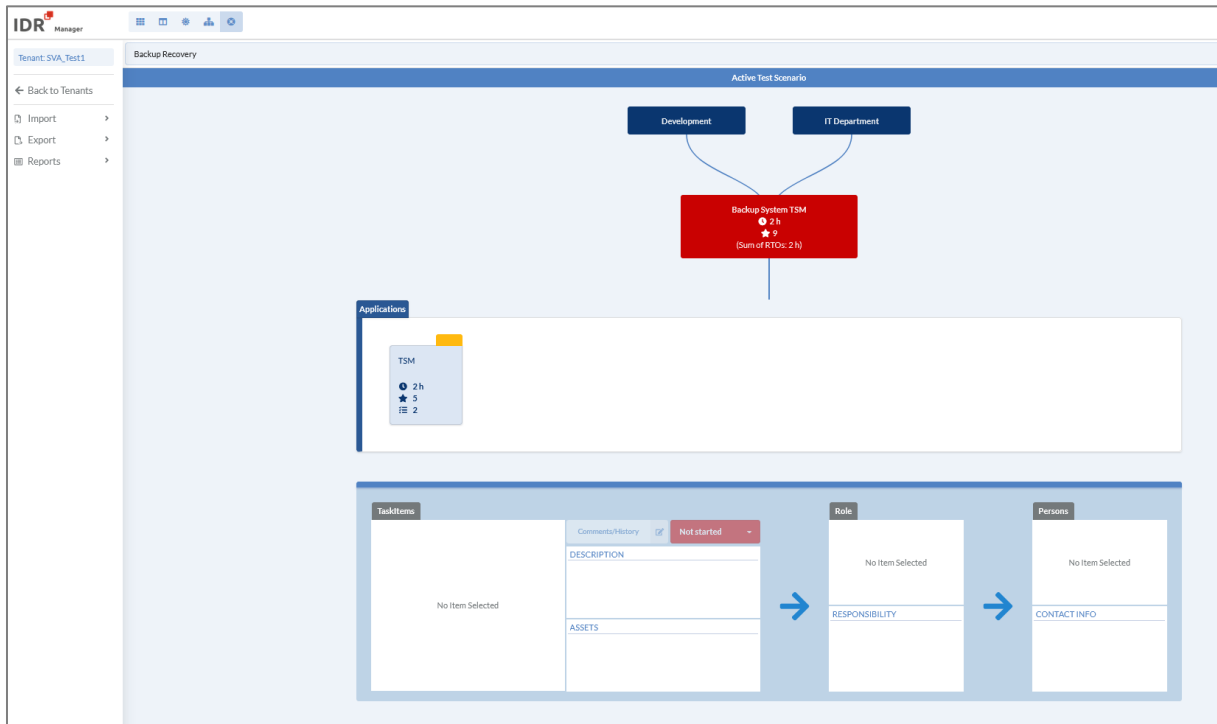


Figure 15: recovery plan view

You can find more information on how to work with the recovery plan view in chapter Recovery plan on page 70.

Gantt view

When working on a disaster case, being able to view all dependencies between business processes, IT services and applications can prove to be very useful. IDR Manager's Gantt Chart provides this functionality very accurately. The Gantt view displays three types of diagrams:

- Business processes
This diagram points out all time relevant dependencies from the selected business process.
- IT services
Within this view you can see time relevant dependencies on the selected IT service.

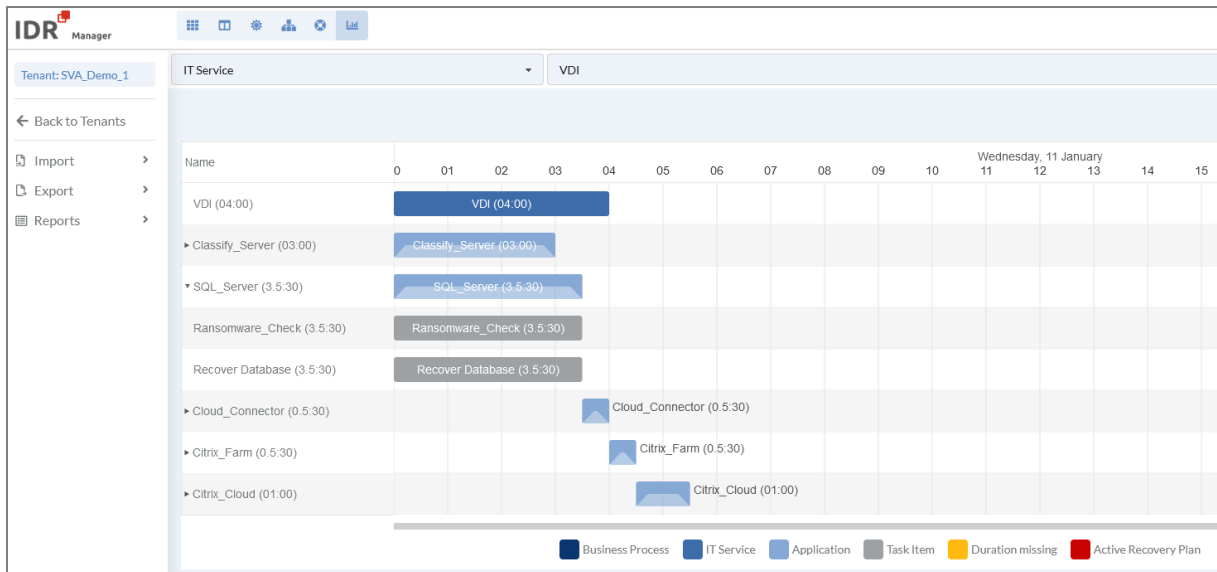


Figure 16: Gantt view

IDR refers to the actual date when presenting the time dependencies. The predefined items will be presented according to the selected diagram type. Regardless of the selected diagram type, applications and task items will be presented for the IT service that needs to be recovered. The displayed timeline length reflects the MTPD of the IT service or RTO of an application.

The Gantt view also enables editing IT services, applications and task items by clicking twice on the object and opening the edit window of the concerned object.

When the MTPD of an IT service or RTO of an application is missing, there will be a warning shown on the top of the Gantt view, see Figure 17: Gantt .

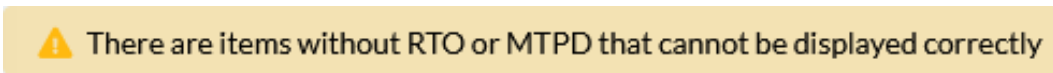


Figure 17: Gantt warning

Tenants

In order to separate complex structures, IDR Manager is split into tenants. They can be used to divide domains or branches of the company, if required. Within a tenant, it is possible to define user permissions through roles.

Create tenants

When creating a tenant, we first need to switch to the overview of all tenants. To switch overviews use the manage menu, as shown in the following figure.

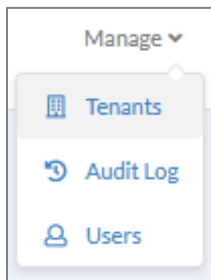


Figure 18: Manage menu

To create a new tenant click on the **+** button.

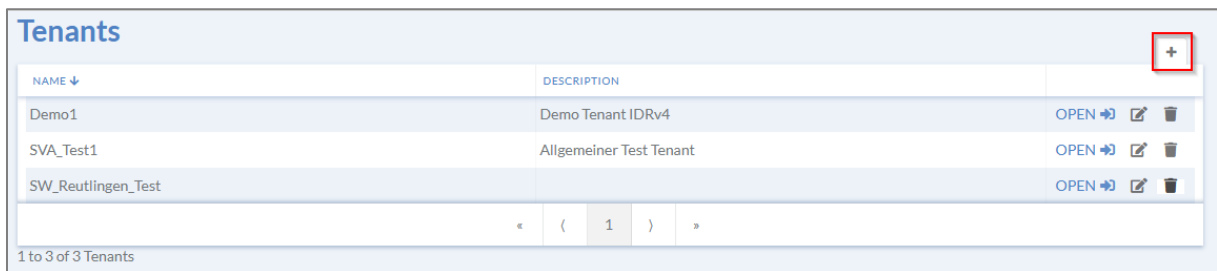


Figure 19: Create tenant (1/2)

Type in a name for the new tenant. A description is optional. To submit, click the **CREATE** button.

Figure 20: Create tenant (2/2)



It is possible to force 2-factor-authentication (2FA) upon all users of the tenant. To do so, you need to mark “enforce 2FA for all users”.

Furthermore, it is necessary to define a routine for checking files. The system will remind users to update their files in the tenant, based on the defined routine. This includes all uploaded files within the tenant. You need to define the desired cycle, by setting a value between 30 and 365 days in the “file outdated period” field.

Unlike for the field “file outdated period”, it is possible to leave the field “file check interval” empty. Nevertheless, it is recommended to define an interval, to check the validity of the documents before they expire. The interval is based on Business Continuity Management (BCM) or Service Continuity Management (ITSCM) principles of the company.

As soon as the deadline for “file outdated period” or “file check interval” has been reached, the uploaders will be notified via e-mail to check their corresponding documents.

Update tenants

To update a tenant, switch to the tenant overview and click the  button next to that tenant. An edit window will open, where you can update the name, description, 2FA settings, “file outdated period” or “file check interval” of that tenant. To finish, click the  button.

Update Tenant [Close]

Name *
Demo_1

Description
Demo Tenant für User Guide

2FA Settings
You can enforce 2FA for all user accounts with access to this tenant.
 Enforce 2FA for all Users

File Outdated Settings
If you want to receive email notifications about outdated assets and BCM files, please define a lifetime period (in days) and a check interval (in months) down below. Set interval to 0 to disable this check.



File Outdated Period (days)
365

File Check Interval (months)
0

[CANCEL] [UPDATE]

Figure 21: Update tenant

Delete tenants

To delete a tenant, select the  button next to that tenant. A notification will ask you to confirm your actions. To finish the deletion, click the  button.


Delete Tenant [Close]

Are you sure you want to delete Demo1?

[CANCEL] [DELETE]

Figure 22: Delete tenant

Clone tenants

To clone a tenant, switch to the tenant overview and click on the corresponding clone button . An edit window will open, where setting a new name will be mandatory, see Figure 23: Clone tenant.

Clone Tenant ✕

Name *

Description

2FA Settings
You can enforce 2FA for all user accounts with access to this tenant.

Enforce 2FA for all Users

File Outdated Settings
If you want to receive email notifications about outdated assets and BCM files, please define a lifetime period (in days) and a check interval (in months) down below. Set interval to 0 to disable this check.

File Outdated Period (days)

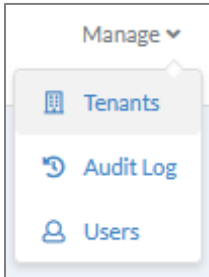
File Check Interval (months)

Figure 23: Clone tenant

Users

Create users

To create users, switch to the manage menu.



Select “users” in the drop-down menu to switch to the user overview. Click on the **+** button, to create a new user.

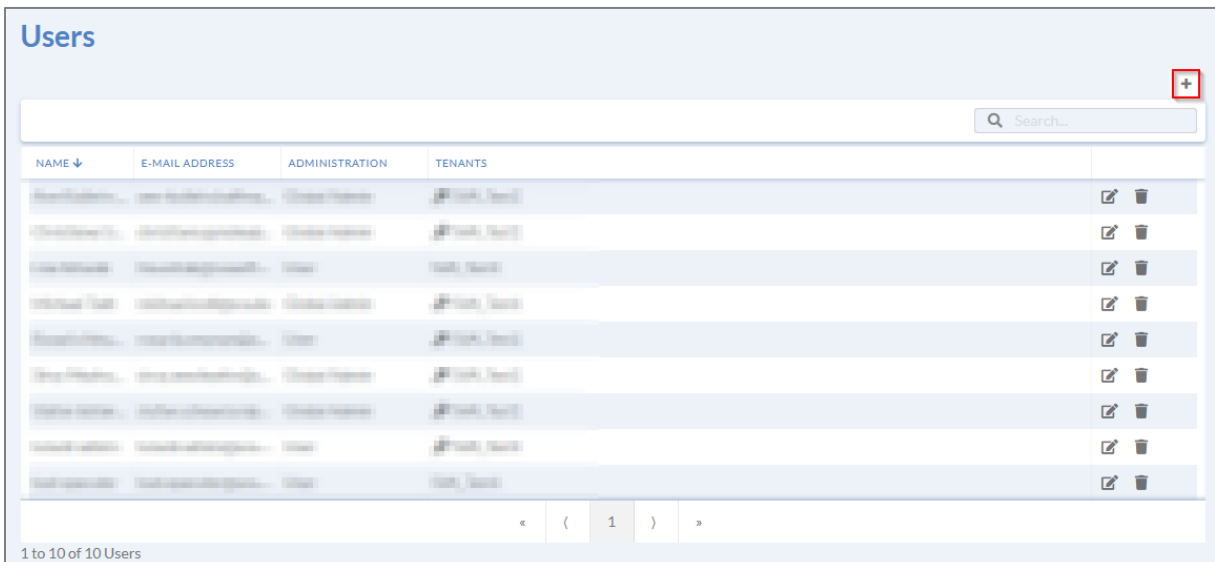
A screenshot of the 'Users' overview page. The page has a header with the title 'Users' and a search bar on the right. Below the header is a table with columns: NAME, E-MAIL ADDRESS, ADMINISTRATION, and TENANTS. The table contains 10 rows of user data. At the bottom of the table, there is a pagination control showing '1 to 10 of 10 Users' and a page number '1'. A red box highlights a '+' button in the top right corner of the table area.

Figure 24: User overview

An edit window will open, containing the following fields:

- First name*
- Last name*
- E-mail address*
- Password*
- Password verification*
- Company
- Work phone
- Private phone
- Mobile phone

All fields marked with * are mandatory.

The screenshot shows a 'Create User' form with the following fields and controls:


- First Name ***: Input field with placeholder 'First Name'.
- Last Name ***: Input field with placeholder 'last Name'.
- E-Mail ***: Input field with placeholder 'E-Mail'.
- Password ***: Input field with placeholder 'Password' and an eye icon for visibility toggle.
- Verify Password ***: Input field with placeholder 'Verify Password' and an eye icon for visibility toggle.
- Company**: Input field with placeholder 'Company'.
- Work phone**: Input field with placeholder 'Work phone'.
- Private phone**: Input field with placeholder 'Private phone'.
- Mobile**: Input field with placeholder 'Mobile'.
- Global Admin**: A checkbox for granting global administration permissions.
- CANCEL** and **CREATE** buttons at the bottom right.

Figure 25: Create user

To submit, click on the  button.

After submitting the creation, the credentials need to be sent manually to the concerned user. There will be no automated e-mail sent to the created user.

Important: Global administration permissions should be granted carefully. These permissions allow users to view and delete all assets, users and tenants.

To enable working within a certain tenant, it is necessary to assign the user to that tenant. To assign the user, open the tenant and click on the  button in the tile “persons”. On the “find” tab, it is possible to search for an existing user and add it to the selected tenant.

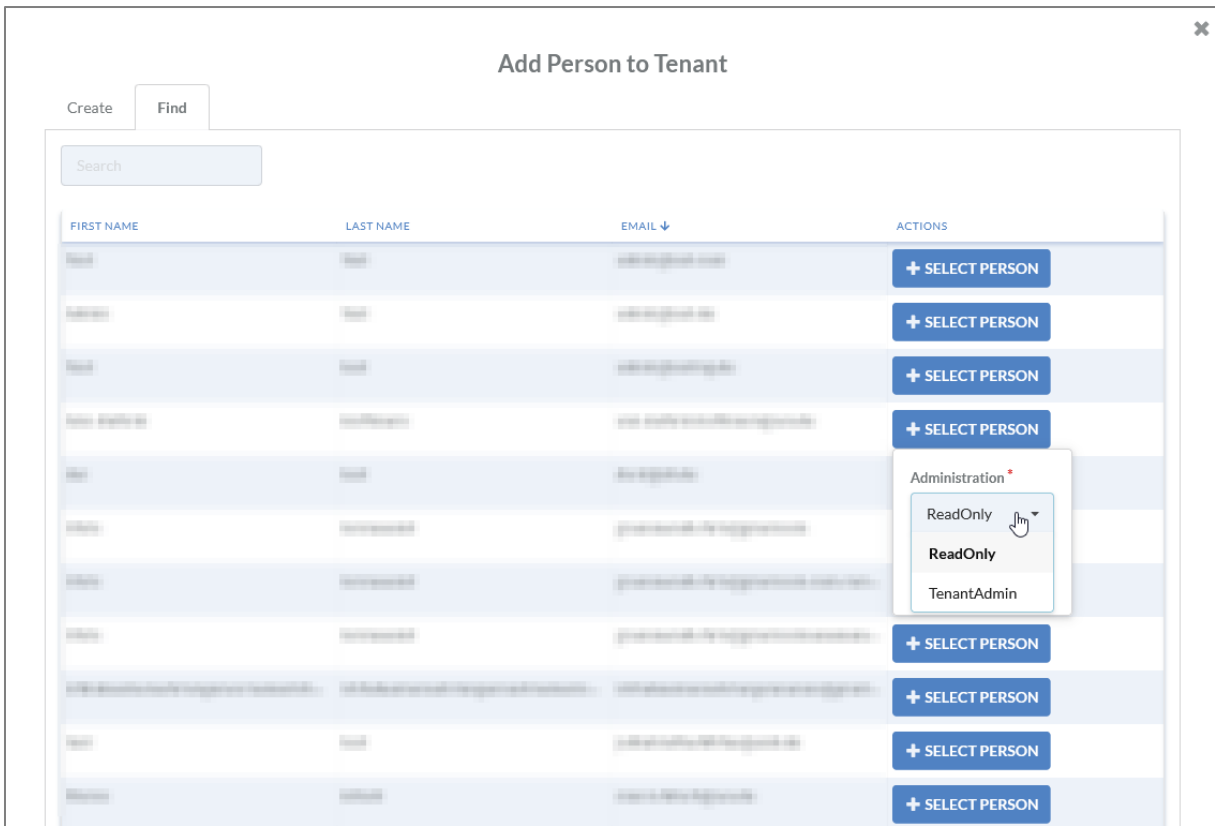



Figure 26: Add user to a tenant

The users may be granted one of the following permissions:

- **ReadOnly:** Read permission on the tenant.
- **TenantAdmin:** Read and write permission on the tenant.

Update user

To update a user click the  button next to the concerned user. An edit window will open and show editable information of that user.

The 'Update User' dialog box is titled 'Update User' and has a close button (X) in the top right corner. It contains the following fields:


- First Name * (text input)
- Last Name * (text input)
- E-Mail * (text input)
- Company (text input)
- Work phone (text input)
- Private phone (text input)
- Mobile (text input)
- Global Admin

At the bottom right, there are two buttons: 'CANCEL' and 'UPDATE'.

Figure 27: Update user

To finish, click the  button.

Delete user

To delete a user, click the  button next to that user. You will then be prompted for confirmation.

The 'Delete User' dialog box is titled 'Delete User' and has a close button (X) in the top right corner. It contains the following text and elements:

- Are you sure you want to delete this User?
- John D. Smith

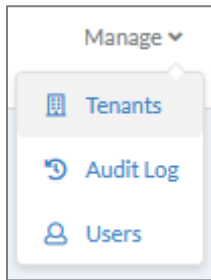
At the bottom right, there are two buttons: 'CANCEL' and 'DELETE'.

Figure 28: Delete user

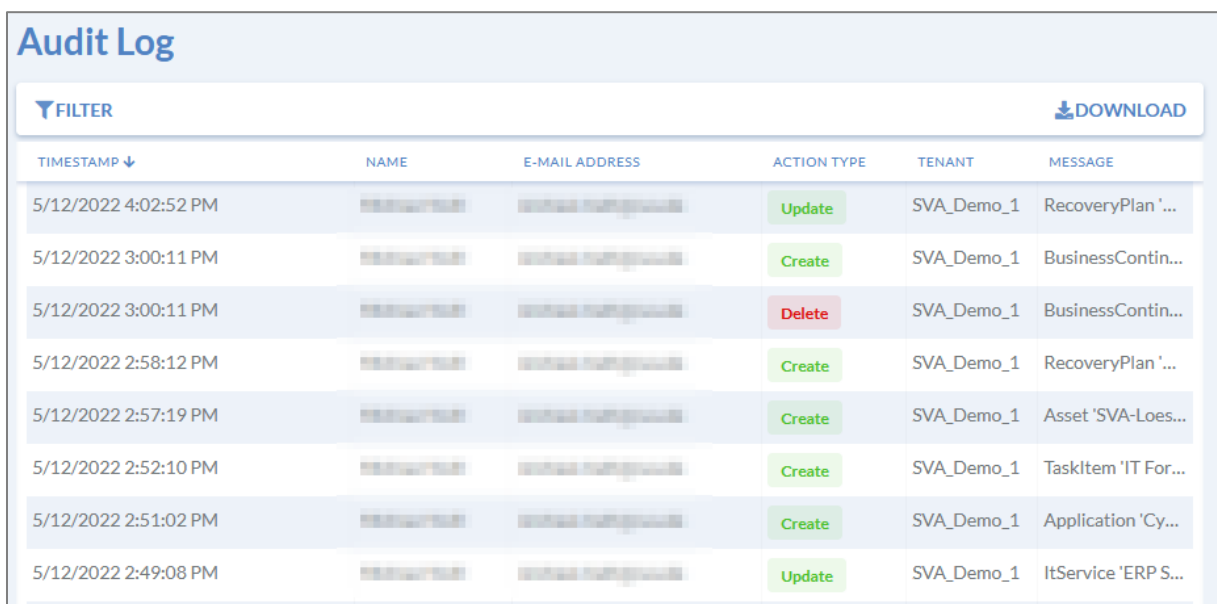
To finish, click the  button.

Audit Logs

To open audit logs, switch to the manage menu.



An integrated audit log gives an overview on all performed activities in IDR Manager. It can only be viewed with global administrator permissions.



Audit Log					
FILTER					DOWNLOAD
TIMESTAMP ↓	NAME	E-MAIL ADDRESS	ACTION TYPE	TENANT	MESSAGE
5/12/2022 4:02:52 PM	[REDACTED]	[REDACTED]	Update	SVA_Demo_1	RecoveryPlan '...
5/12/2022 3:00:11 PM	[REDACTED]	[REDACTED]	Create	SVA_Demo_1	BusinessContin...
5/12/2022 3:00:11 PM	[REDACTED]	[REDACTED]	Delete	SVA_Demo_1	BusinessContin...
5/12/2022 2:58:12 PM	[REDACTED]	[REDACTED]	Create	SVA_Demo_1	RecoveryPlan '...
5/12/2022 2:57:19 PM	[REDACTED]	[REDACTED]	Create	SVA_Demo_1	Asset 'SVA-Loes...
5/12/2022 2:52:10 PM	[REDACTED]	[REDACTED]	Create	SVA_Demo_1	TaskItem 'IT For...
5/12/2022 2:51:02 PM	[REDACTED]	[REDACTED]	Create	SVA_Demo_1	Application 'Cy...
5/12/2022 2:49:08 PM	[REDACTED]	[REDACTED]	Update	SVA_Demo_1	ItService 'ERP S...

Figure 29: Audit log

Furthermore, it is possible to download the logs for an auditor or reviewer. For that, you need to click the **DOWNLOAD** button. The resulting PDF document containing all entries will be downloaded and opened automatically.

By clicking on a row, you will get more detailed information on the selected row in a pop-up window.

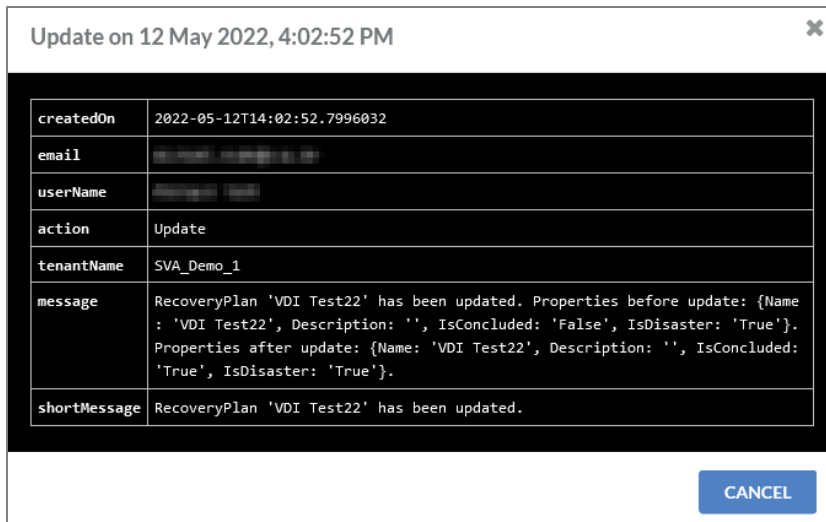


Figure 30: Detailed audit log entry

The log content can be adjusted by clicking the **FILTER** button. An edit window will open, where you can select or deselect required content. You can also define a time frame for the log.

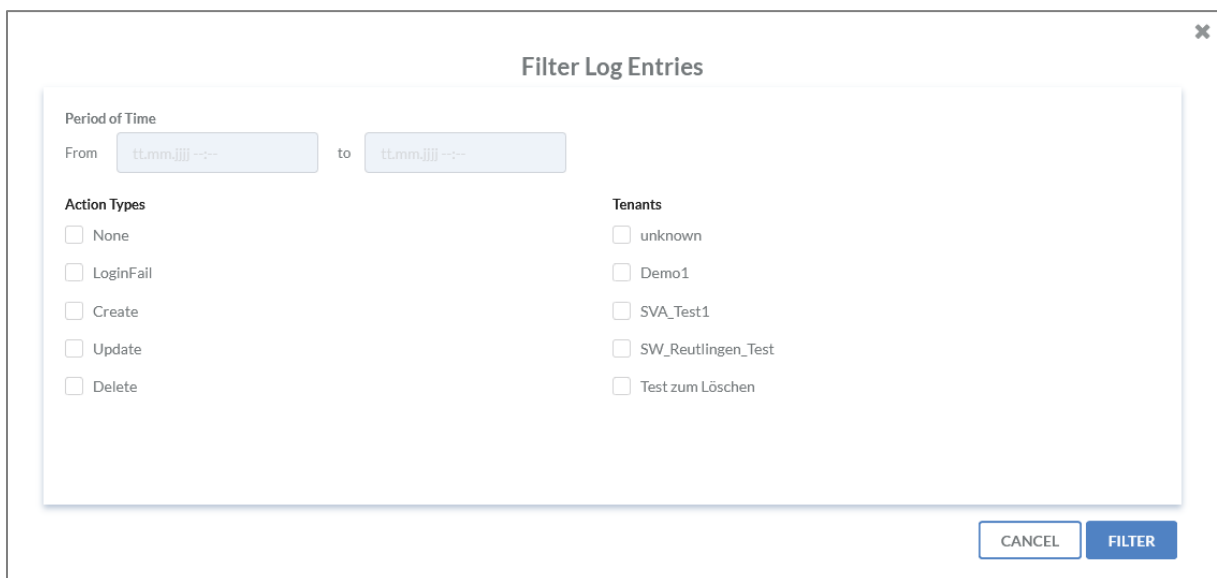



Figure 31: Filter audit logs

Click on the **FILTER** button to finish

It is not possible to delete logs on the web interface.

Business Processes

Create business processes

To create a business process, click on the  button. An edit window will open.

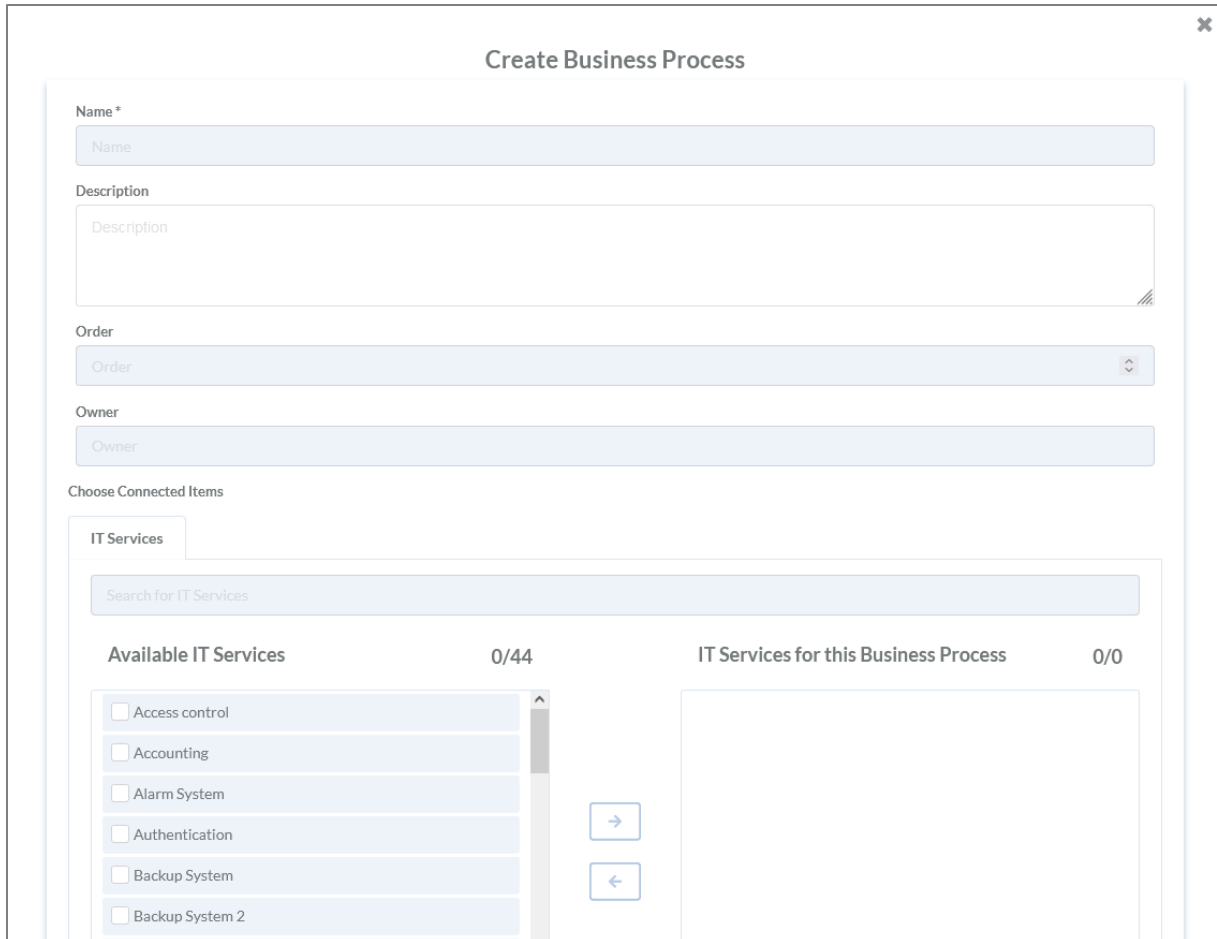




Figure 32: Create business process

The processing window contains the following fields:


- Name of the business process*
- Description
- Order
The entered order has no impact on the tile or table view. The order is used for informative prioritization.
- Owner
- Link to IT services

All fields marked with * are mandatory.

To create a link between a business process and an IT service, select the service from the list  and add it with the  button.

Click the  button to save changes.

Update business processes

Use the table view, to update a business process. To change from tile view to table view, click the  button.

To update a specific process, click the  button next to that process. An edit window will open.

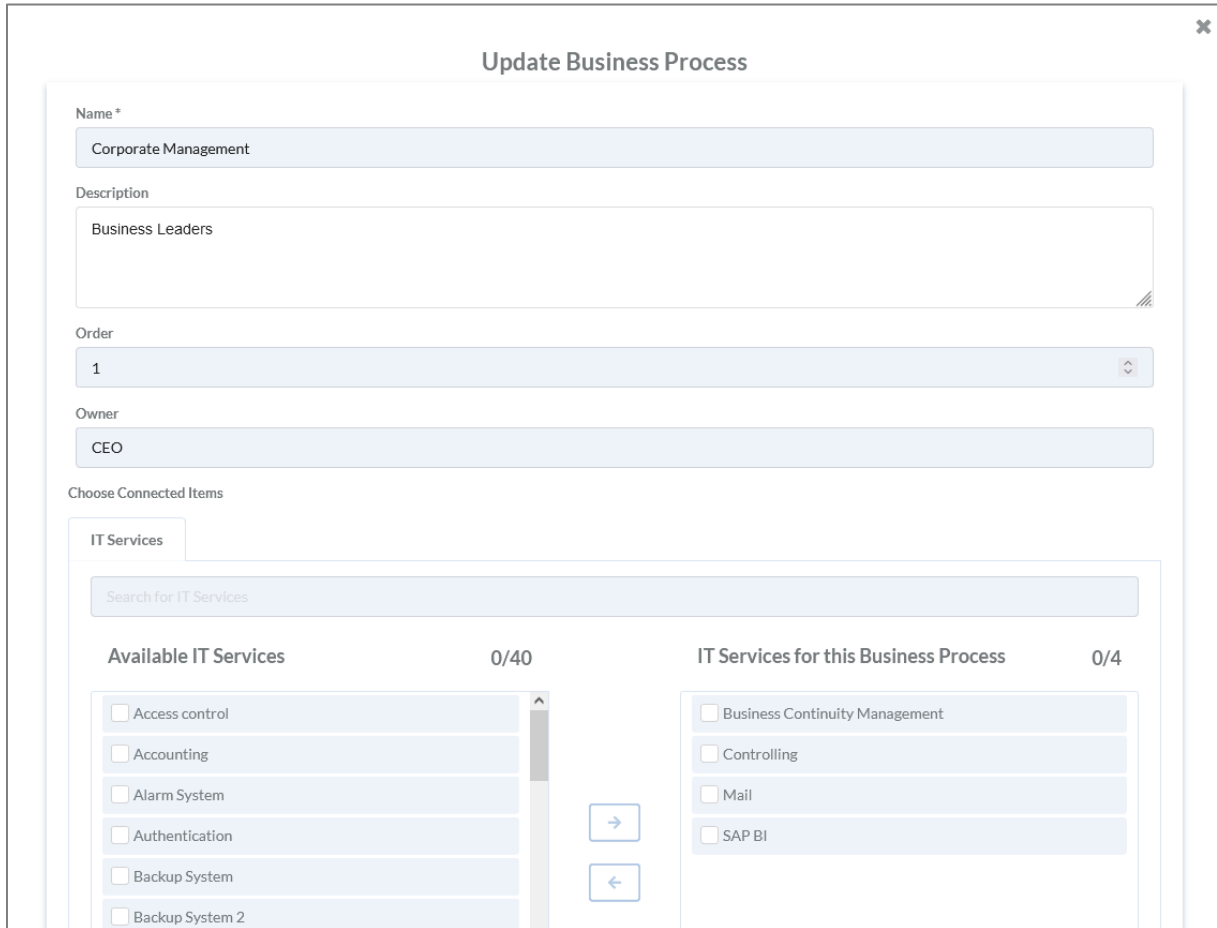










Figure 33: Update business process

To add a link to IT services, select the service from the list  and add it with a click on the  button. To remove a service, select it  and remove it with a click on the  button. To finish, click the  button.

Delete business processes

Delete a business process from the table view. To change from tile view to table view, click the  button. To delete a business process, click the corresponding  button next to the concerned process. Now you can select all processes you wish to delete. To finish, click the  button again.

A notification window will list the selected processes and prompt for confirmation, see Figure 34: Delete business process.

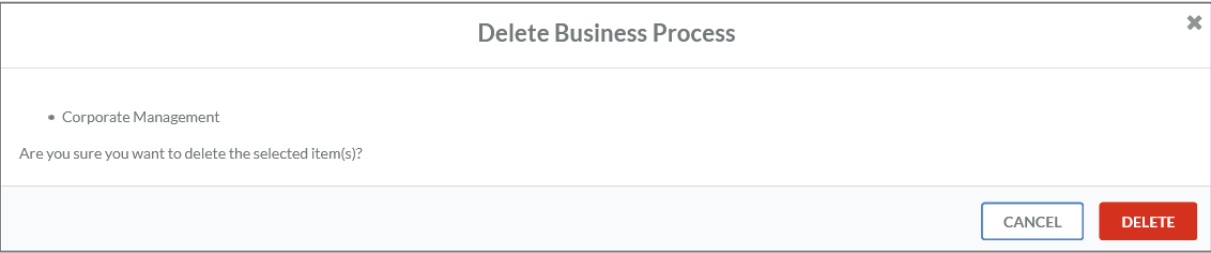


Figure 34: Delete business process

To finish, click the  button.

IT services

Create IT services

To create a new service, click the **+** button. The following edit window will open:

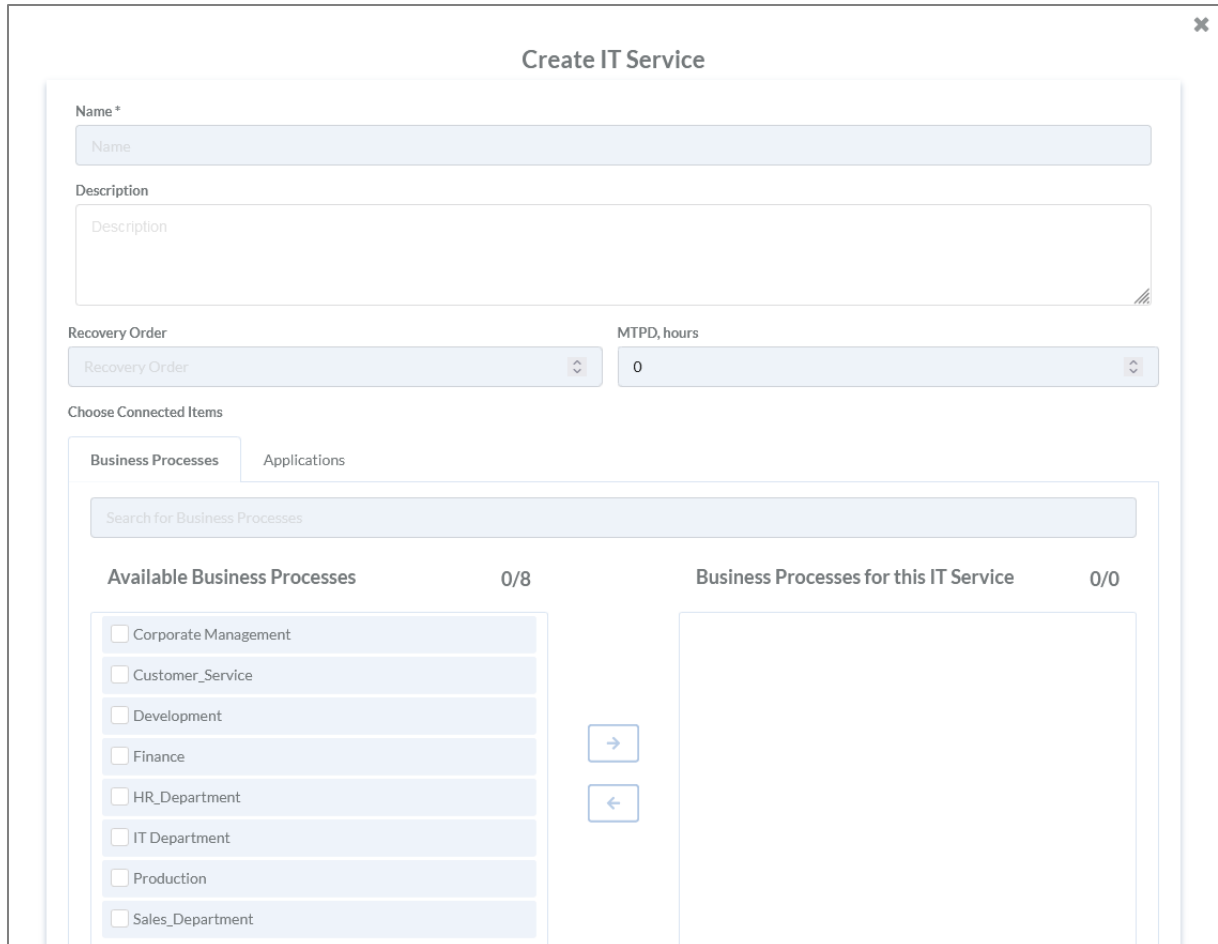


Figure 35: Create IT services

The edit view contains the following fields:

- Name of IT service*
- Description
- Recovery order
The defined order has impact on the arrangement of the elements in tile or table view. Critical elements will rank higher and be arranged to the left. (Ranking from 1 upwards, 1 being the highest value).
- Maximum Tolerable Period of Disruption (MTPD) in hours
- Link to business processes
- Link to applications

All fields marked with * are mandatory.

To link the IT service to existing business processes or applications, select them and add them with the button. To finish, click the button.

Update IT services

Updating an IT service requires using the table view.

To update an IT service, click the  button next to that service. A processing window will open:

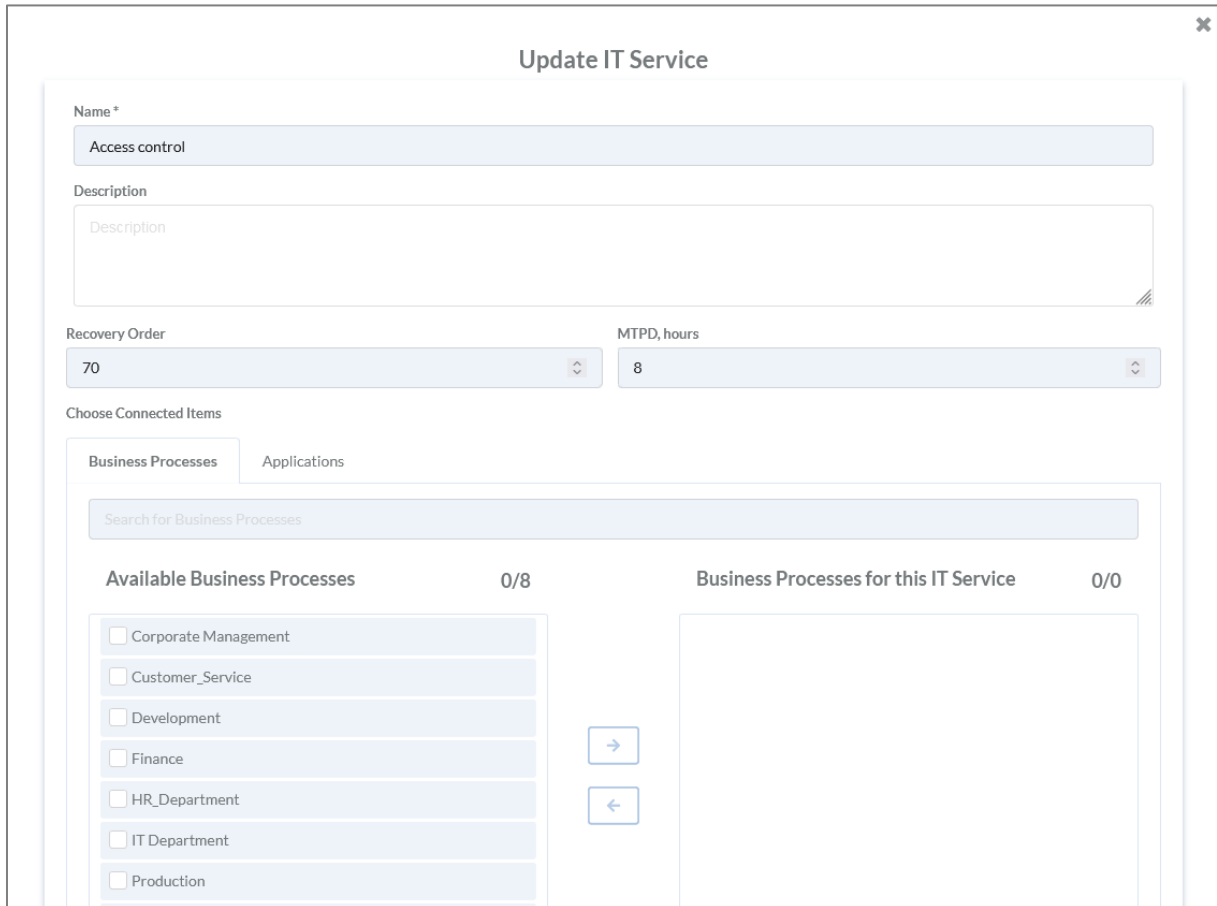










Figure 36: Update IT services

To link business processes or applications, select the process or application  and add it with the  button. To remove the process or application, select it  and click the  button. To finish click the  button.

Delete IT services

Deletion of an IT service requires using the table view.

To delete an IT service, click the  button, then select each service that you want to remove . To finish click again the  button. A notification window will list all selected elements and request confirmation, as shown in Figure 37: Delete IT service.

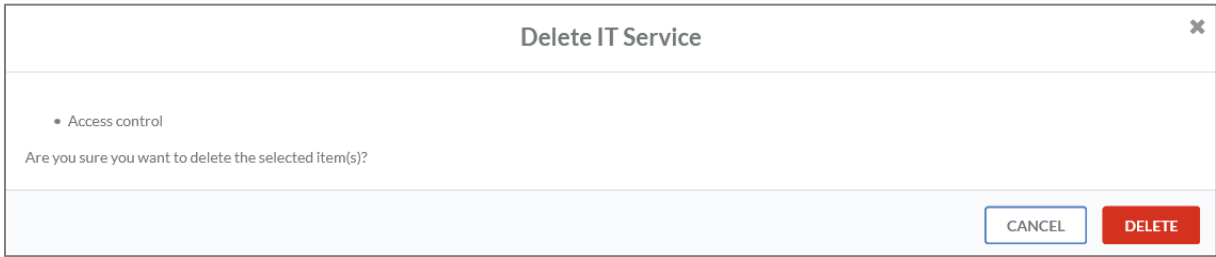


Figure 37: Delete IT service

Applications

Create applications

New applications can be created with a click of the **+** button. The following edit window will open:

The screenshot shows a 'Create Application' window with the following fields and sections:




- Name ***: A text input field.
- Description**: A large text area.
- Recovery Order**: A numeric input field with the value 0.
- RTO, hours : minutes**: A numeric input field with the value 0.
- RPO, hours**: A numeric input field with the value 0.
- Choose Connected Items**: A section with tabs for 'IT Services', 'On Premises', 'Cloud', 'Remote', and 'Task Items'. The 'IT Services' tab is selected.
- Search for IT Services**: A search bar.
- Available IT Services**: A list of services with checkboxes, showing 0/31 items. The list includes: Access Control, Accounting, Authentication, Backup System, Backup System 2, and Backup System TSM.
- IT Services for this Application**: An empty list showing 0/0 items.
- Navigation arrows (right and left) are located between the two lists.

Figure 38: Create application

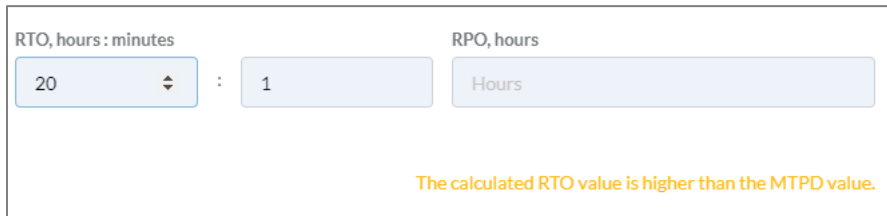
The edit view contains the following fields:

- Name of application*
- Description
- Order
The defined order has impact on the arrangement of the elements in tile or table view. Critical elements will rank higher and be arranged to the left. (Ranking from 1 upwards, 1 being the highest value).
- Recovery Time Objective (RTO) in hours and minutes
- Link to IT services
- Link to on premises assets
- Link to cloud assets
- Link to remote assets
- Link to task items

All fields marked with * are mandatory.

To add a link to an IT service, select the element  and add it with a click on the  button. To finish click on the  button.


When the RTO of an application is higher than or equal to the MTPD of the IT service, a notification will be displayed, see Figure 39: Note RTO. That notification will be replicated in the service view, business view and recovery plan view.

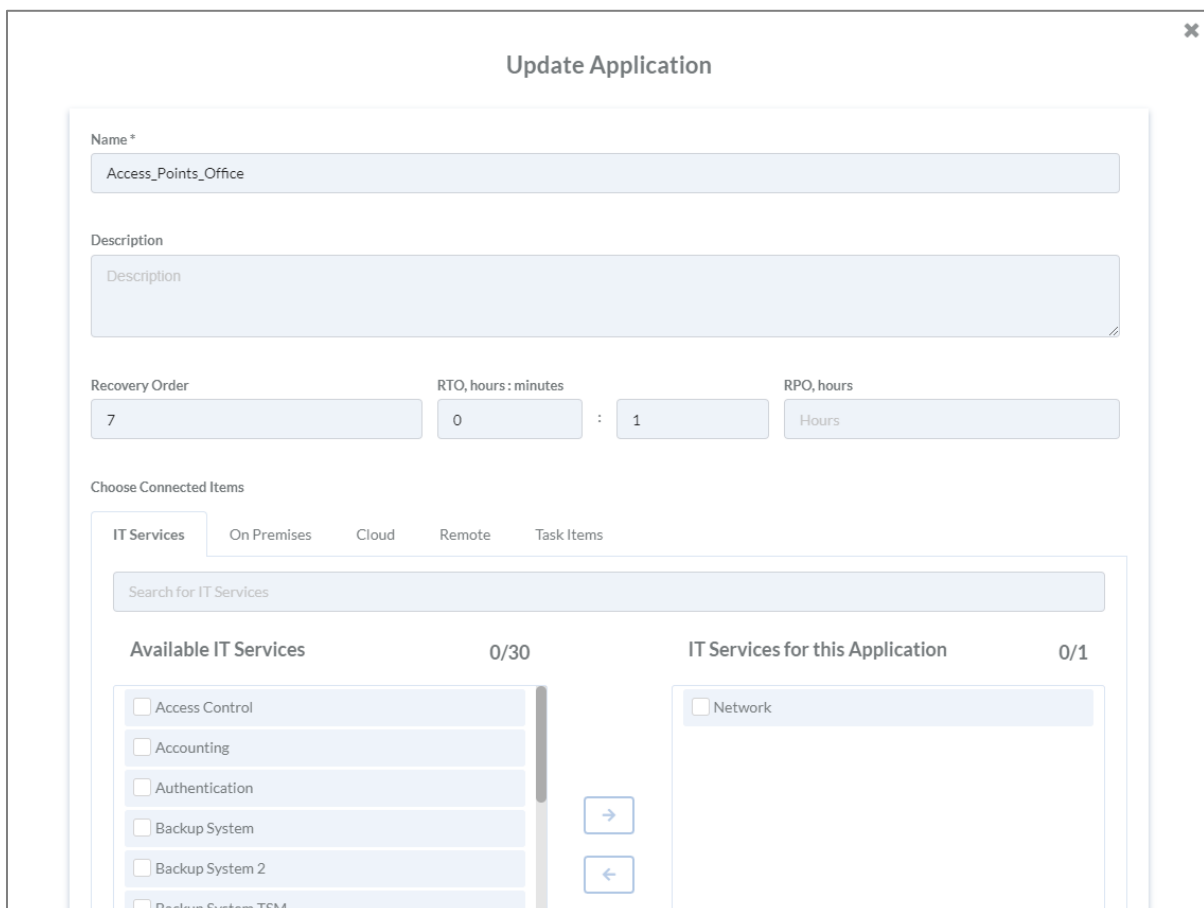


The screenshot shows two input fields: 'RTO, hours : minutes' with a value of '20' and 'RPO, hours' with a value of '1'. Below these fields, a yellow warning message states: 'The calculated RTO value is higher than the MTPD value.'

Figure 39: Note RTO

Update applications

To update an application, click on the  button next to it. The following processing window will be shown:








The 'Update Application' dialog box contains the following fields and sections:

- Name ***: Access_Points_Office
- Description**: Description
- Recovery Order**: 7
- RTO, hours : minutes**: 0 : 1
- RPO, hours**: Hours
- Choose Connected Items**:
 - IT Services (selected)
 - On Premises
 - Cloud
 - Remote
 - Task Items
- Search for IT Services**: Search bar
- Available IT Services** (0/30):
 - Access Control
 - Accounting
 - Authentication
 - Backup System
 - Backup System 2
 - Backup System TSM
- IT Services for this Application** (0/1):
 - Network





Navigation arrows (right and left) are located between the two lists of IT services.

Figure 40: Update application

To link IT services to an application, select the concerned services  and add them with a click on the  button. To unlink services, select them  and remove them with a click on the  button. To finish click the  button.

Delete applications

Deletion of an application requires using the table view.

To delete an application, click the  button. Now select each application  you want to delete. After selecting the applications, you can submit the deletion by clicking the  button again. To finish, check the notification and confirm deletion with a click on the  button, see Figure 41: Delete application.

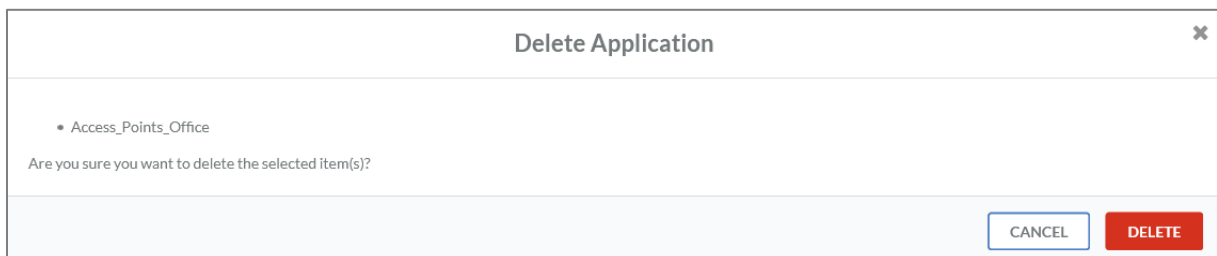


Figure 41: Delete application

On premises assets

Create on premises assets

To create on premises assets, click the **+** button. The following edit window will open:

The screenshot shows a web-based form titled "Create On Premises". The form is enclosed in a light blue border with a close button (X) in the top right corner. The form fields are as follows:

- Name ***: A text input field with a light blue background.
- Description**: A larger text input area with a light blue background.
- Location**: A text input field with a light blue background.
- Room**: A text input field with a light blue background.
- Network Address**: A text input field with a light blue background.
- Storage Capacity**: A text input field with a light blue background.
- Choose Connected Items**: A section with a sub-tab labeled "Applications". It contains a search bar "Search for Applications". Below the search bar, there are two columns: "Available Applications" (0/89) and "Applications for this On Premises" (0/0). Under "Available Applications", there is a list of items with checkboxes: "Access_Points_Office" and "Access_Points_Workshop".

Figure 42: Create on premises asset


The edit view contains the following fields:

- Name of the on premises asset*
- Description
- Location
- Room
- Network address
- Storage capacity
- Link to applications

All fields marked with * are mandatory.

To link applications, select them and add them with a click on the button. To finish, click the Button.

Update on premises assets

To update an on premises asset, click the  button next to the asset. The following edit window will be opened:

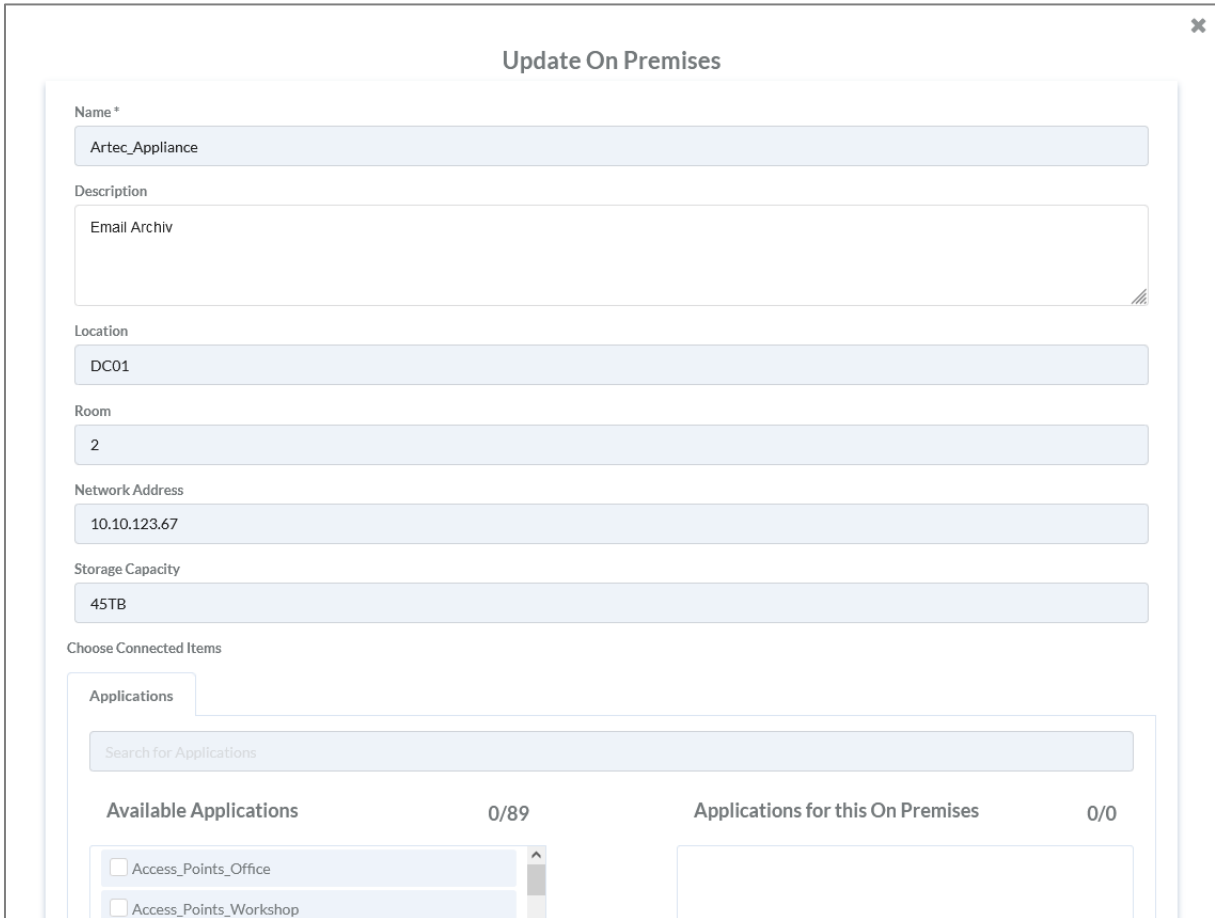











Figure 43: Update on premises asset

To link applications to an on premises asset, select them  and add them with a click on the  button. To remove an application, select it  and click the  button. To finish, click the  button.

Delete on premises assets

Deletion of an on premises asset requires using the table view.

To delete click the  button. Now select  the on premises asset you would like to delete and click again the  button. In order to delete the selected assets, check the notification and confirm the selection with a click on the  button, see Figure 44: Delete on premises.

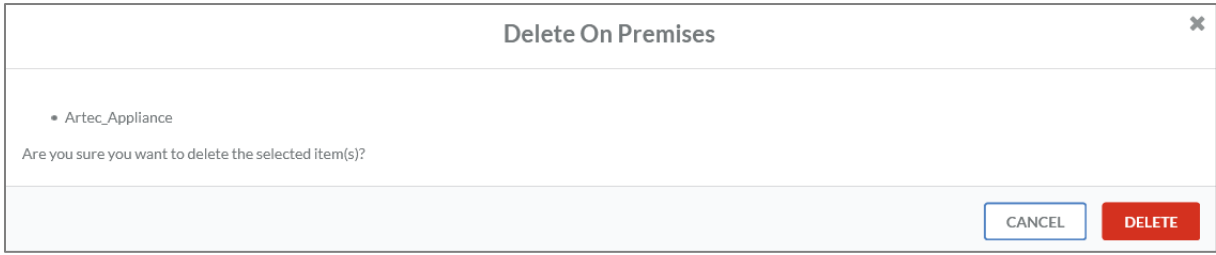
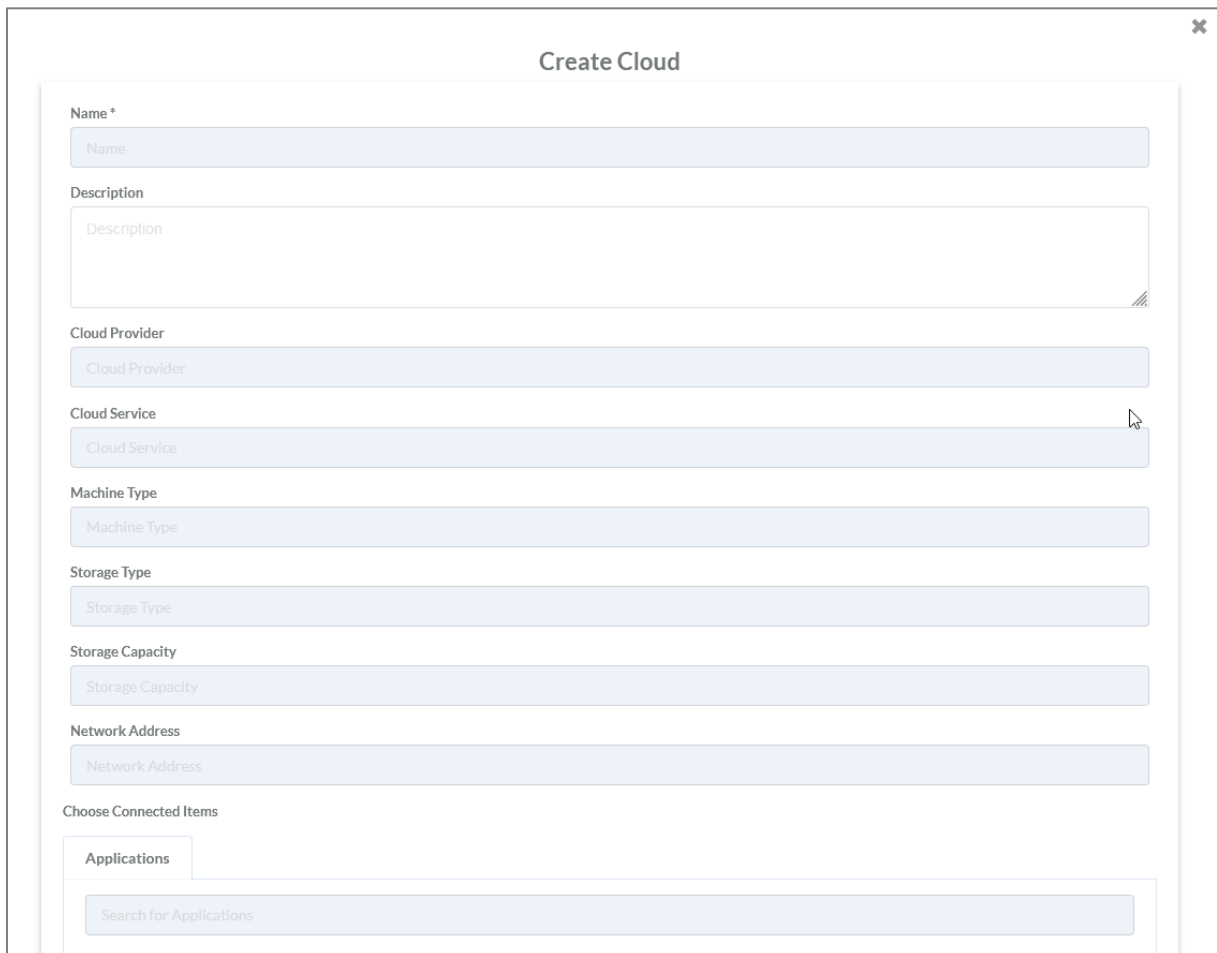


Figure 44: Delete on premises assets

Cloud assets

Create cloud assets

Systems that are operated by a cloud service provider (e.g. Microsoft Azure), are stored as cloud assets in IDR Manager. To create a new cloud asset, click the **+** button. The following window will be opened:



The screenshot shows a window titled "Create Cloud" with a close button in the top right corner. The form contains the following fields:

- Name***: A text input field with a red asterisk indicating it is mandatory.
- Description**: A larger text input field.
- Cloud Provider**: A text input field.
- Cloud Service**: A text input field.
- Machine Type**: A text input field.
- Storage Type**: A text input field.
- Storage Capacity**: A text input field.
- Network Address**: A text input field.
- Choose Connected Items**: A section with a tab labeled "Applications" and a search bar labeled "Search for Applications".

Figure 45: Create cloud assets

The edit view contains the following fields:

- Name of the cloud asset*
- Description
- Cloud provider
- Cloud service
- Machine type
- Storage type
- Storage capacity
- Network address
- Link to applications

All fields marked with * are mandatory.

To link applications, select them and add them with a click on the button. To finish, click the button.

Update cloud assets

To update a cloud asset, click the button next to it. The following edit window will open:

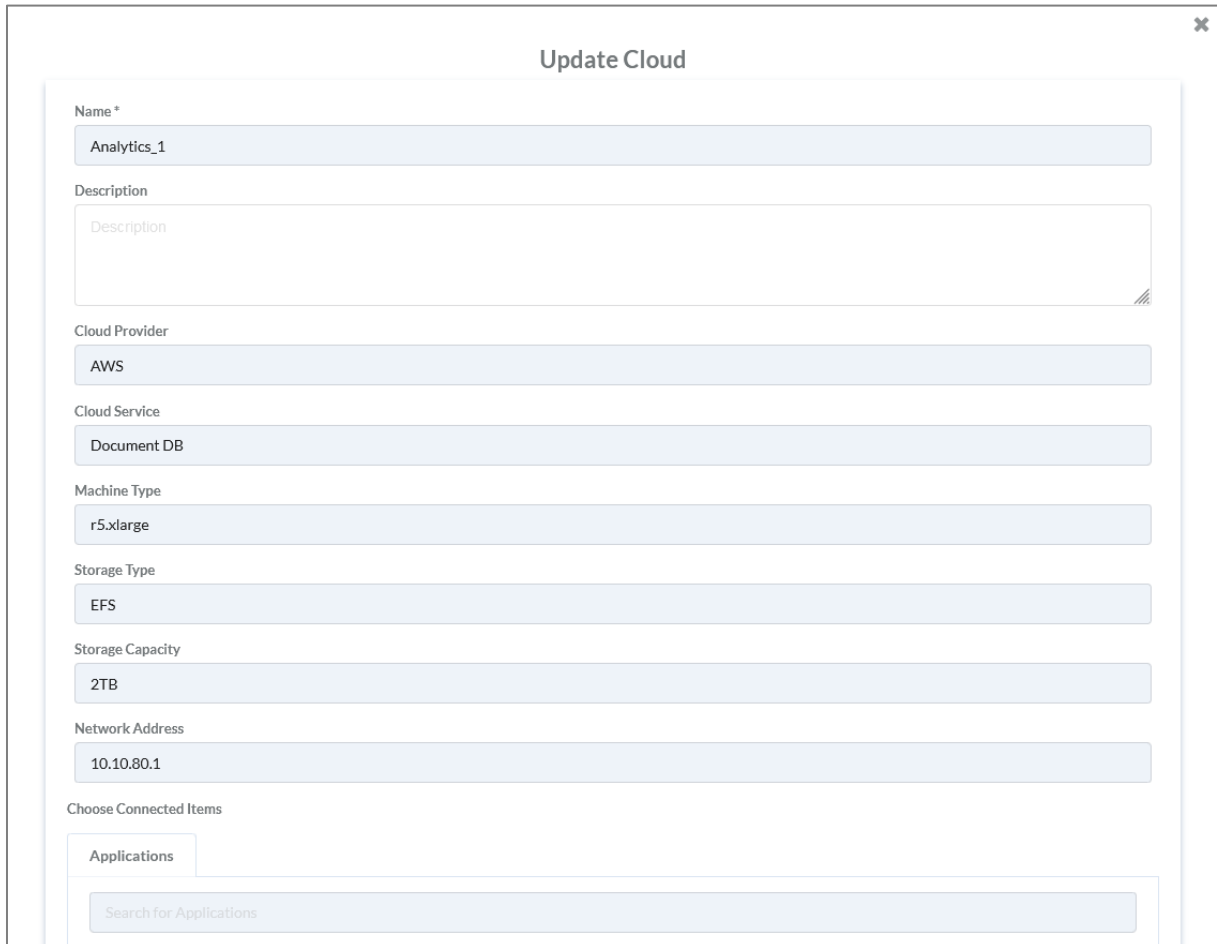


Figure 46: Update cloud assets

To link one or more applications to a cloud asset, select the applications and add them with a click on the button. To remove the application, select it and click the button. To finish click the button.

Delete cloud assets

Deletion of a cloud asset requires using the table view.

To delete cloud assets, click the button. Now select the cloud assets you would like to delete and click the button again. To delete the selection, check the notification and confirm the deletion windows with a click on the button, see Figure 47: Delete cloud asset.

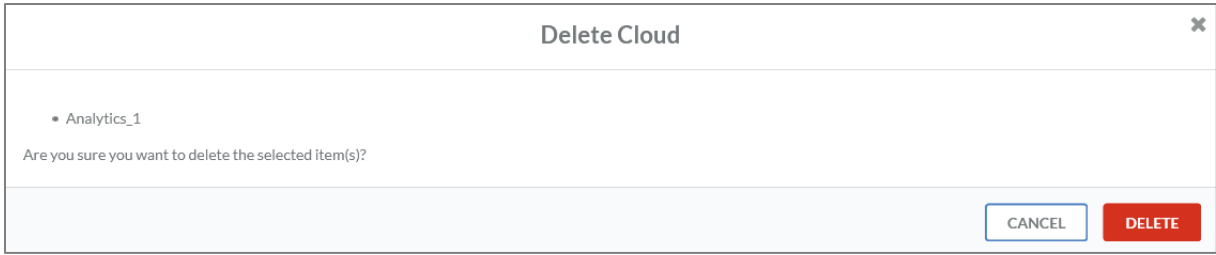
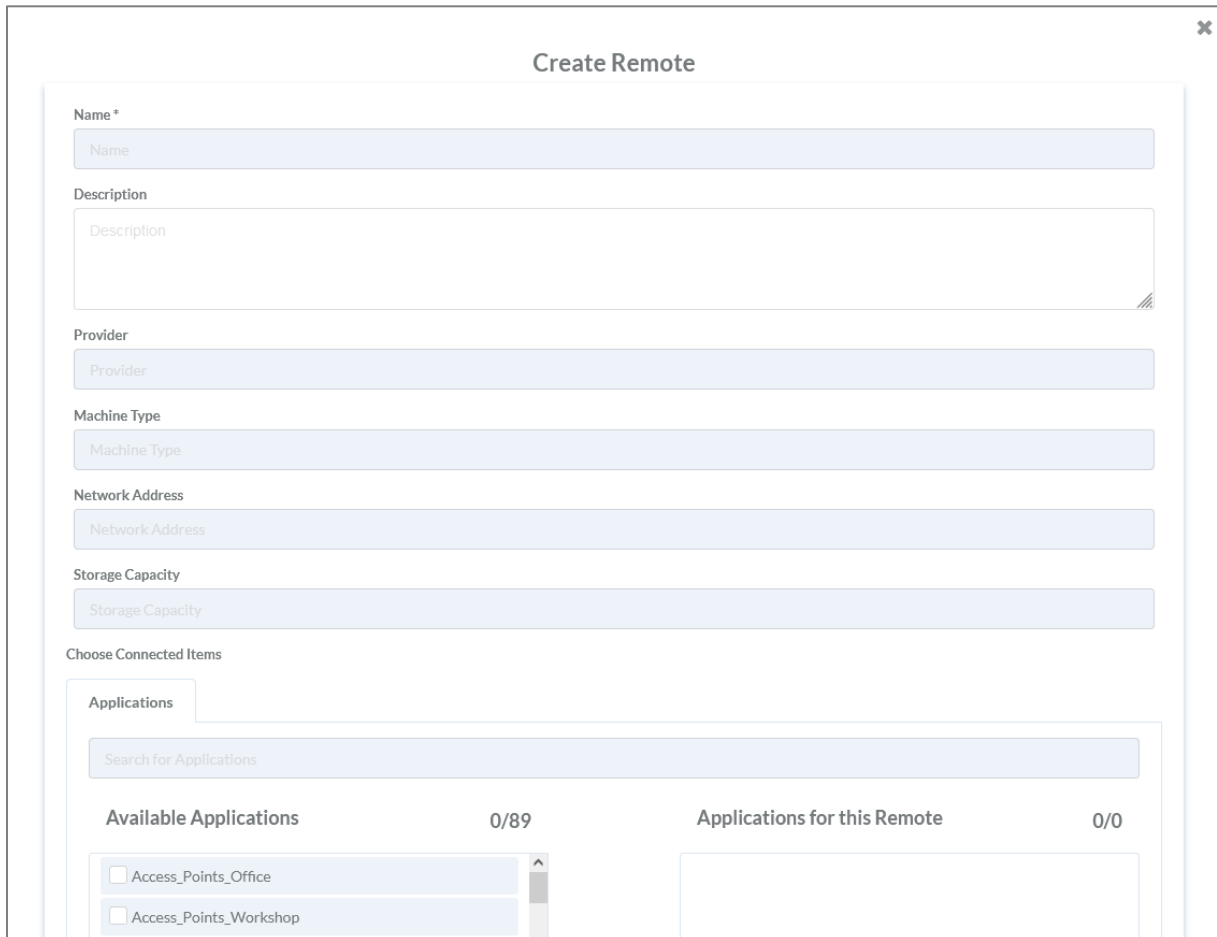


Figure 47: Delete cloud asset

Remote assets

Create remote assets

Some systems are running remotely, for example, they are operated by service operator or on another site as a secondary site. These are stored as a remote assets in IDR Manager. To create a new remote asset, click the **+** button. The following edit window will open:



The screenshot shows a 'Create Remote' dialog box with the following fields and sections:

- Name ***: A text input field with the placeholder 'Name'.
- Description**: A larger text input field with the placeholder 'Description'.
- Provider**: A text input field with the placeholder 'Provider'.
- Machine Type**: A text input field with the placeholder 'Machine Type'.
- Network Address**: A text input field with the placeholder 'Network Address'.
- Storage Capacity**: A text input field with the placeholder 'Storage Capacity'.
- Choose Connected Items**: A section containing:
 - A search bar labeled 'Search for Applications'.
 - Two columns: 'Available Applications' (0/89) and 'Applications for this Remote' (0/0).
 - Under 'Available Applications', there are two items: 'Access_Points_Office' and 'Access_Points_Workshop', each with an unchecked checkbox.

Figure 48: Create remote asset


The edit view contains the following fields:

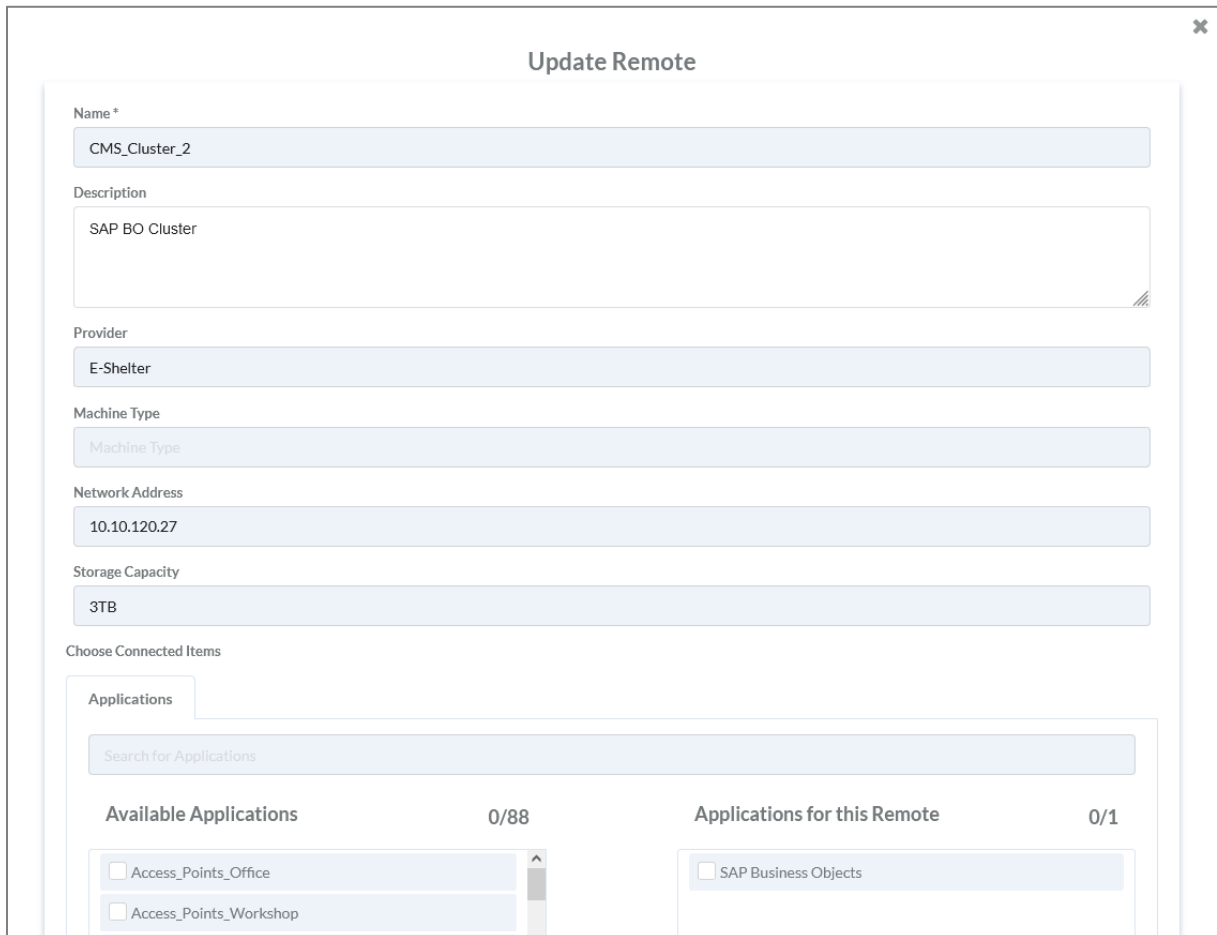
- Name of the remote assets*
- Description
- Provider
- Machine type
- Network address
- Storage capacity
- Link to applications

All fields marked with * are mandatory.

To link an application to a remote asset, select the application and add it with a click on the button.

Update remote asset






To update a remote asset, click the  button next to it. The following edit window will open:



The screenshot shows the 'Update Remote' dialog box. It contains the following fields and sections:





- Name ***: CMS_Cluster_2
- Description**: SAP BO Cluster
- Provider**: E-Shelter
- Machine Type**: Machine Type
- Network Address**: 10.10.120.27
- Storage Capacity**: 3TB
- Choose Connected Items**:
 - Applications**: Search for Applications
 - Available Applications** (0/88):
 - Access_Points_Office
 - Access_Points_Workshop
 - Applications for this Remote** (0/1):
 - SAP Business Objects

Figure 49: Update remote asset

To link an application to a remote asset, select the application  and add it with a click on the  button. To remove the application, select it  and click the  button. To finish, click the  button.

Delete remote asset

Deletion of an application requires using the table view.

To delete remote assets, click the  button. Now select  the assets you would like to delete and click the  button again. To delete the selection, check the notification and confirm the deletion windows with a click on the  button, see Figure 50: Delete remote asset.

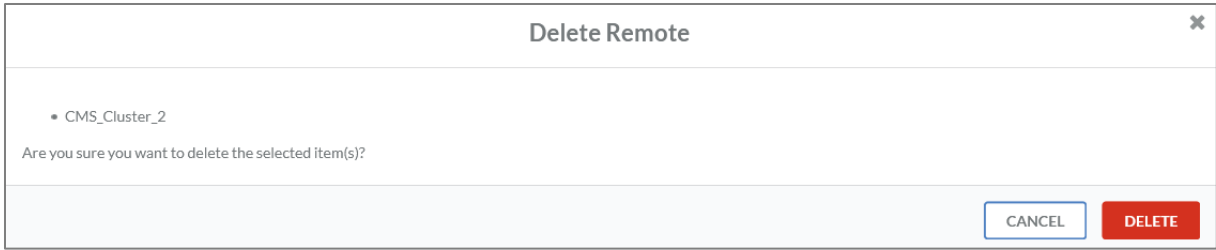


Figure 50: Delete remote asset

Task Items

Create task items

Task Items store recovery documents. These documents contain the recovery procedures, to bring IT systems back up in case of a disaster. These can range from step by step guides/procedures to workflows and diagrams. Each Task Item is linked to an application; therefore, you are storing any recovery procedure pertaining to an application. To create a new task item, click the **+** button. The following edit window will open:

The screenshot shows a dialog box titled "Add Task Item". It contains the following fields and sections:

- Name***: A text input field with a required asterisk.
- Description**: A larger text input area.
- Order**: A dropdown menu.
- Role**: A dropdown menu.
- Choose Connected Items**: A section with two tabs: "Applications" (selected) and "Assets".
- Search for Applications**: A search bar.
- Available Applications**: A list of applications with checkboxes, showing 0/89 items. The list includes: Access_Points_Office, Access_Points_Workshop, Active_Directory, ADFS, Alpha+, and Application_Server.
- Applications for this Task Item**: An empty list showing 0/0 items.
- Navigation arrows (right and left) are located between the two application lists.

Figure 51: Create task item

The edit view contains the following fields:

- Name of the task items*
- Description
- Order
- Role
- Link to applications
- Link to assets

All fields marked with * are mandatory fields.

To link an application, select the application and add it with a click on the button.

The file containing the procedures, guides and diagrams are uploaded under the tab “assets”, see Figure 52: Upload assets.

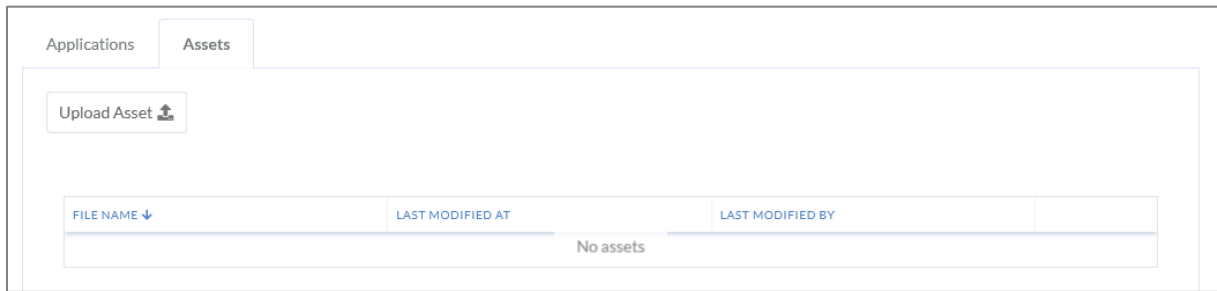



Figure 52: Upload assets

Update task items

To update a task, click the  button next to it. The following edit window will open:

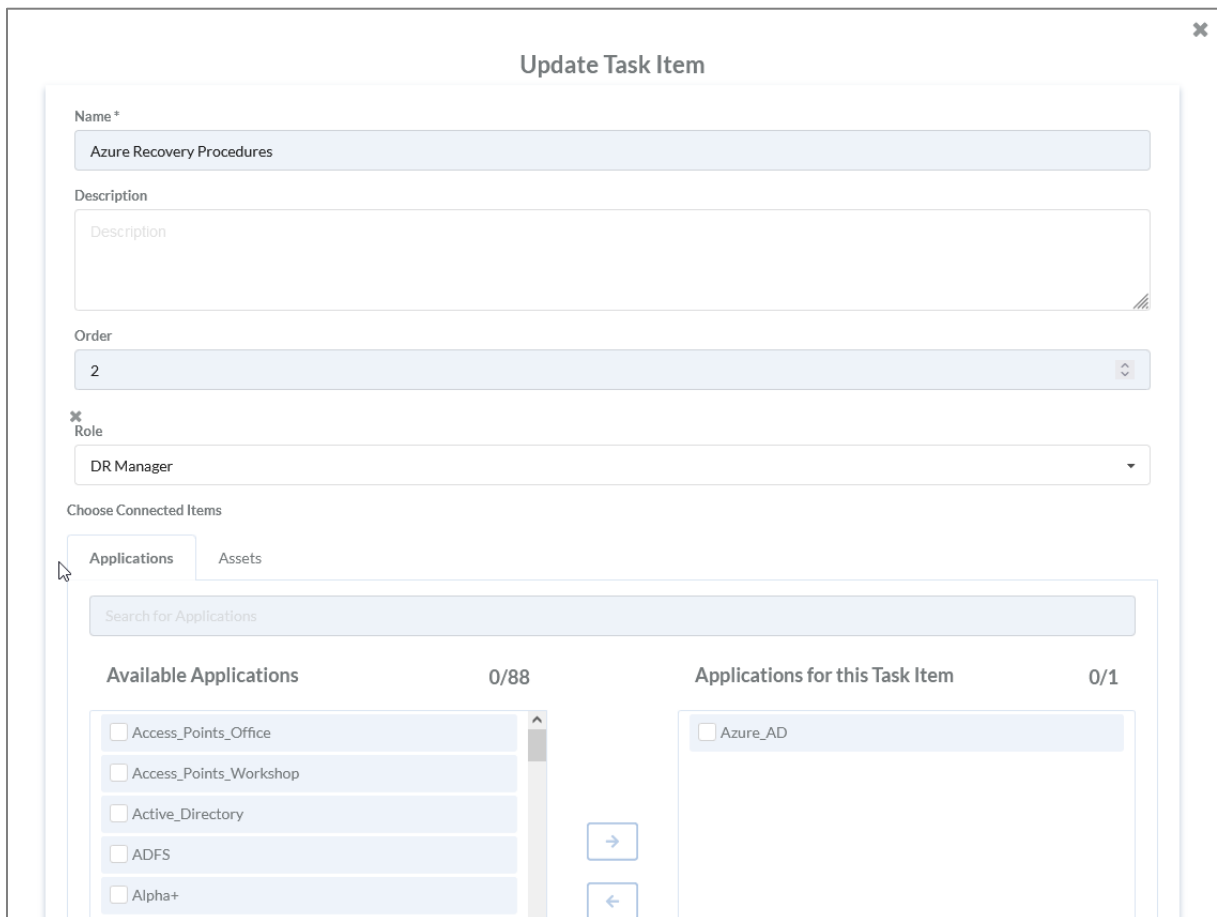









Figure 53: Update task item

To link an application to a task item, select the application and add it with a click on the  button. To remove the application, select it and click the  button. To finish, click the  button.

Delete task items

Deletion of a task item requires using the table view.

To delete task items click the  button. Now select  the items, you would like to delete and click the  button again. To delete the selection, check the notification and confirm the deletion windows with a click on the  button, see Figure 54: Delete task item.

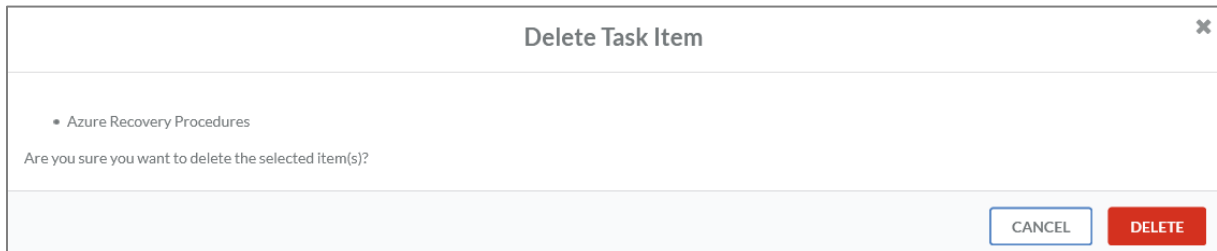


Figure 54: Delete task item

Scenarios

Create scenarios

Outage scenarios are referenced upon when creating use cases for task items. Possible use cases can be for example blackouts, fire or ransomware. When the use cases are categorized together, they can be purposefully processed on basis of needs and recovery plans.

To create a new scenario, click the **+** button. The following edit window will open:

The screenshot shows a 'Create Scenario' dialog box with the following fields and sections:

- Name ***: A text input field.
- Description**: A larger text area for entering details.
- Choose Connected Items**: A section with a 'Task Items' tab and a search bar labeled 'Search for Task Items'.
- Available Task items**: A list of 7 items with checkboxes, showing 0/23 items selected. The items are:
 - AD_Recovery_Procedures
 - BCM Exercise Plan Definition
 - Call Servicedesk Cloud Provider
 - Check_Failover_Metro_Cluster
 - Check_Ransomware
 - Connect to Salesforce
 - Coordination Disaster Recovery Process
- Task items for this Task Item**: An empty list area showing 0/0 items, with right and left arrow buttons between the columns.

Figure 55: Create scenario

The edit view contains the following fields:


- Name of the scenario*
- Description
- Link to task items

All fields marked with * are mandatory.

To link a task item, select the item and add it with a click on the button. To finish, click the

button

Update scenarios

To update a scenario, click the  button next to it. The following edit window will open:

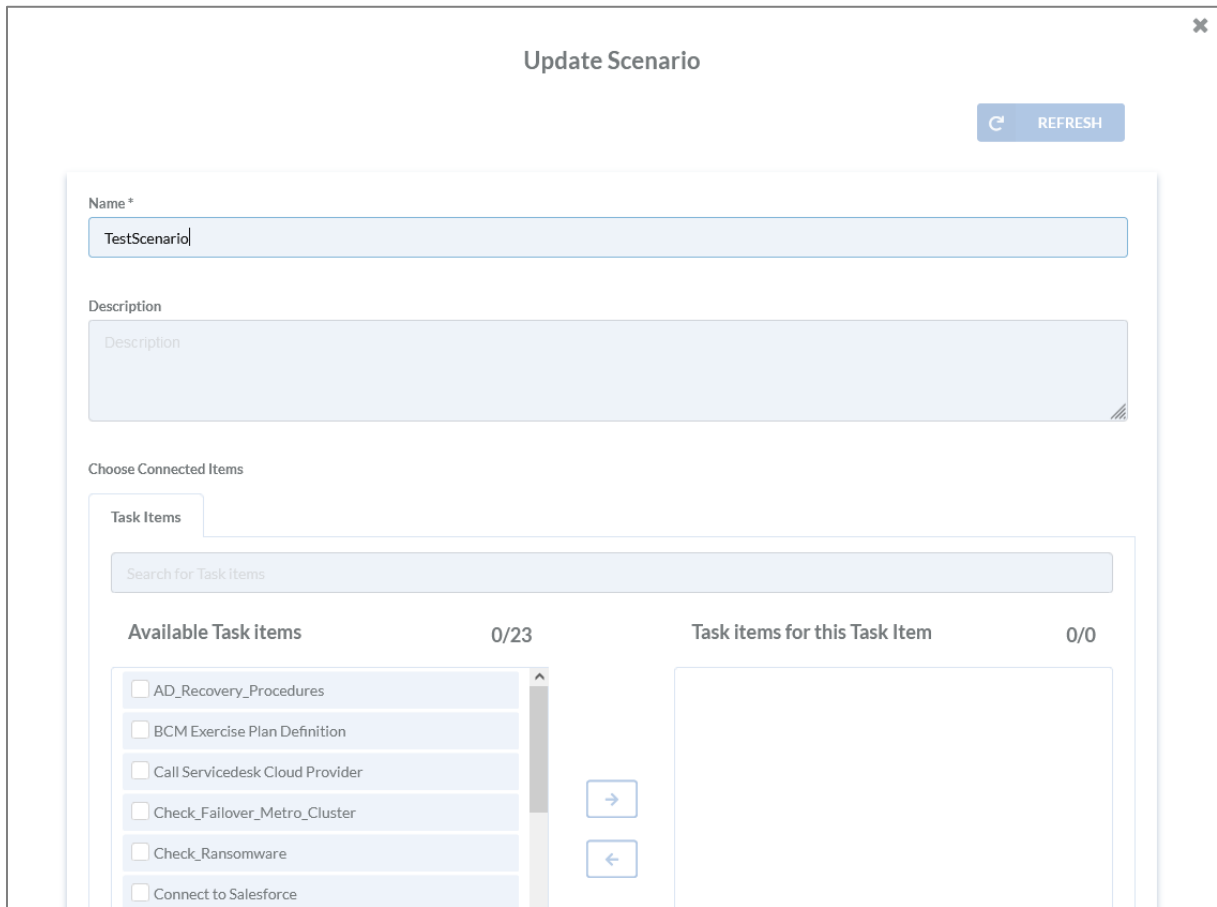








Figure 56: Update scenario

To link a task item to a scenario, select the application and add it with a click on the  button. To remove the item, select it and click the  button. To finish, click the  button.

Delete scenarios

Deletion of a scenario requires using the table view.

To delete scenarios click the  button. Now select the scenario you would like to delete and click the  button again. To delete the selection, check the notification and confirm the deletion windows with a click on the  button, see Figure 54: Delete task item.

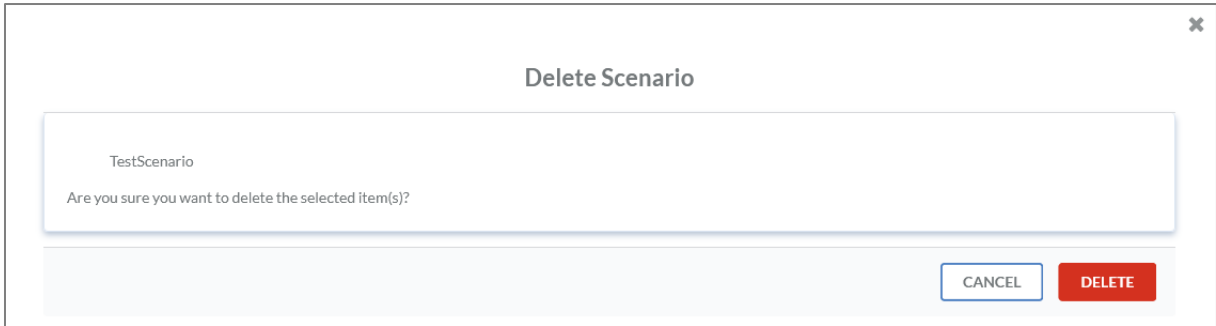


Figure 57: Delete scenario

Roles

Create roles

Using roles allow the assignment of tasks to different people. To create a new role, click the **+** button. The following edit window will open:

Figure 58: Create role

The edit view contains the following fields:

- Name of the role*
- Description
- Responsibility
- Link to task items
- Link to persons

All fields marked with * are mandatory.

To add a task item, select the item and add it with a click on the button. To remove the task item, select it and click the button. To finish, click the button.

Update roles

To update a role click the  button next to it. An edit window will open.

Figure 59: Update role

To link a task item to a role, select the item and add it with a click the button. To remove the task item, select it and click the button. To finish, click the button.

Delete roles

Deletion of a role requires using the table view.

To delete click the button. Now select all roles you would like to delete and hit the button again. To delete the selection, check the notification and confirm the deletion windows with a click on the button, see Figure 60: Delete role.

Figure 60: Delete role

Persons

Create persons

The disaster recovery information is processed by team members, referred to as persons in the tool.

To register a new person click the **+** button. The following edit window will open:

Figure 61: Create person

The edit view contains the following fields:

- First name*
- Last name *
- E-mail address*
- Password*
- Verify password*
- Company
- Work phone
- Private phone
- Mobile phone
- Administration*
 - Read only
 - Tenant admin
- Description
- Link to roles

All fields marked with * are mandatory.

To add role, select the role and add it with a click on the button. To remove the role, select it and click the button. To finish, click the button.

Update persons




To update a person click the  button next to it. The following edit window will open

Figure 62: Update person

To link a role to a person, select the role and add it with a click on the button. To remove the role, select it and click the button. To finish, click the button.

Delete persons

Deletion of team members requires using the table view.

To delete, click the  button. Select all persons you would like to delete and hit again  button. To delete the selection, check the notification and confirm the deletion windows with a click on the button, see Figure 63: Delete person.

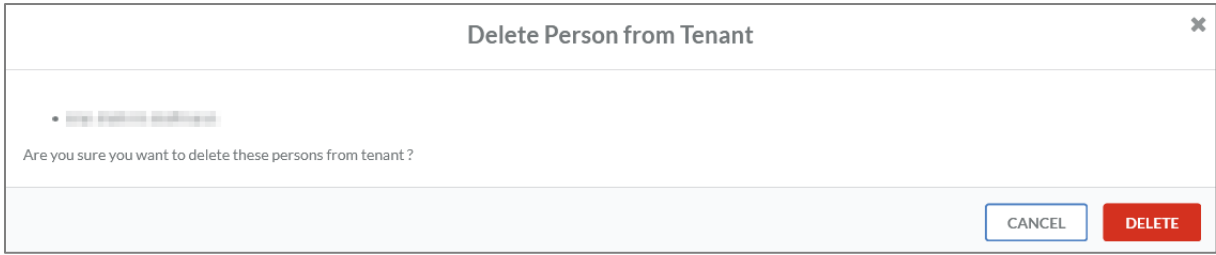


Figure 63: Delete person

Working with IDR Manager

Version history from updates

The current version of the IDR Manager is shown at the bottom of the left side.

Version 4.0.509
© SVA 2021

The changelog can be opened by clicking on the version, see Figure 64: Changelog IDR Manager. A list of every version since IDR Manager version 4 with its changes will open.

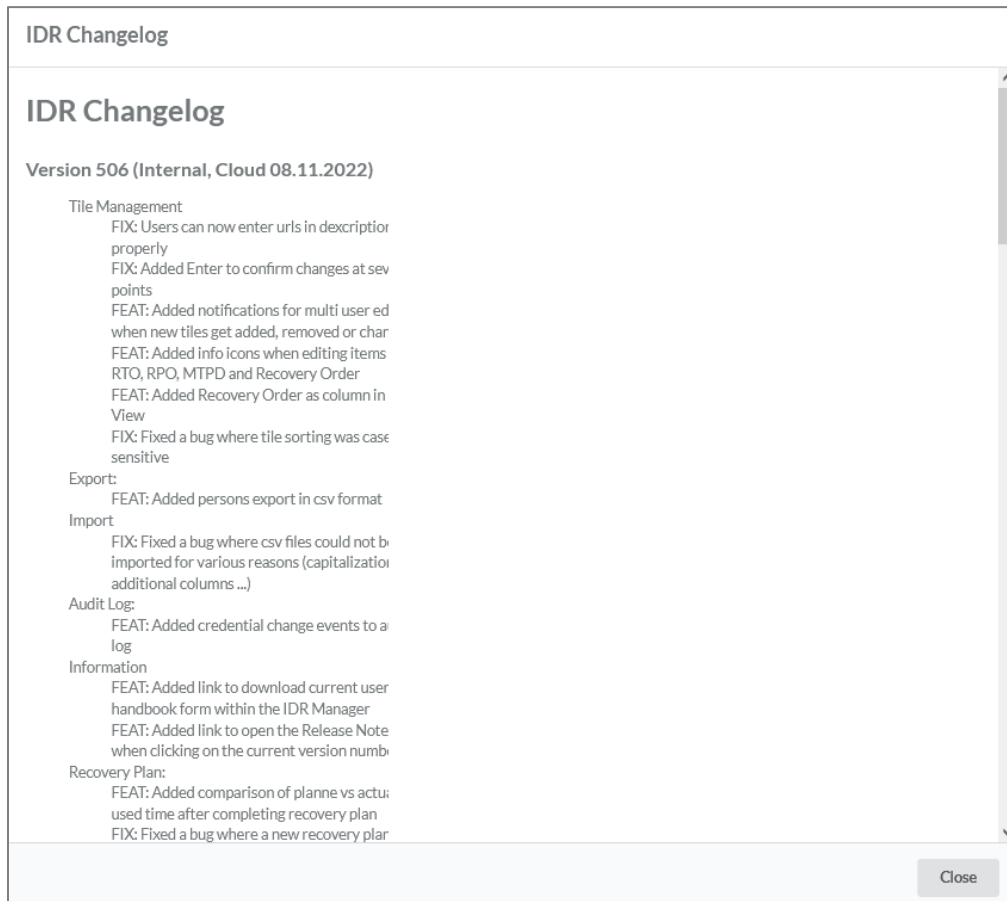


Figure 64: Changelog IDR Manager

Download User Guide

You can find a download link for the user guide in IDR Manager under "Help".



Check of consistency

The tile view allows checking data consistency in IDR Manager. When hovering the mouse over tiles, the system will highlight all tiles with a link to that tile in blue. With this function, it is possible to quickly check for existing dependencies. This also allows you to check, if a role has personnel linked to it as well as task items. The following figure displays an example for IT services:

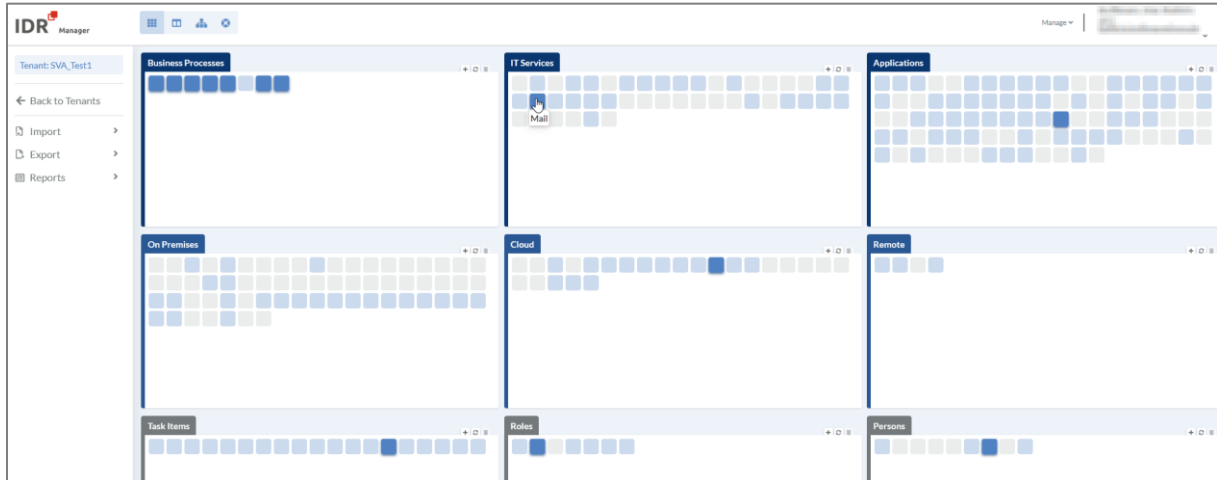


Figure 65: Check of the consistency

This is not the only method to check for consistency in the IDR Manager. Tiles with missing links are marked grey. It is also possible to export a list of all grey tiles, see chapter “Reports” – “Orphaned Elements”.

Collaboration within IDR Manager

Create objects

The collaboration within IDR Manager works with information boxes. When an object is created by another user, every other user using the tile or table view will get a notification at the top on the right side, see Figure 66: Creation of an IT service through another user. The IDR Manager will then automatically reload the page in the background, to display the latest changes.

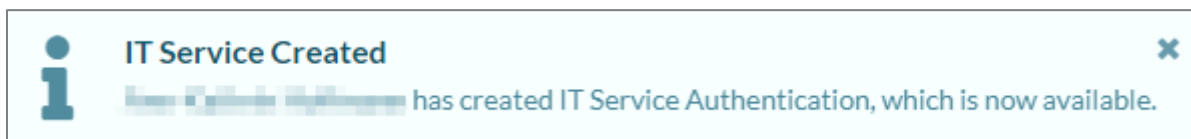


Figure 66: Creation of an IT service through another user

Update objects

When a different users change the same object, a yellow note appears on the update window of each, see Figure 67: Update it service through another user. Additionally, an info box appears at the top right to inform about the change of the object.

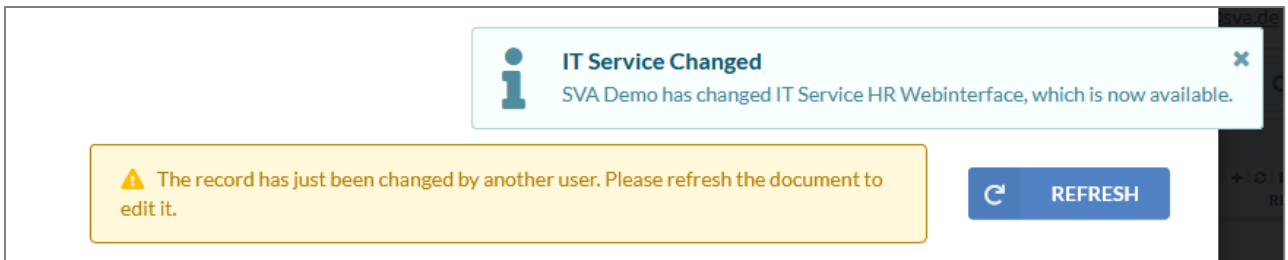


Figure 67: Update it service through another user

When a change takes place, the user interface will not refresh, because otherwise the changes will be overwritten by the other user. The user needs to click on the **REFRESH** button, to refresh the window and see the changes. Without a refresh, it is not possible to save changes to the object.

Delete objects

When an object is deleted by another user, the other users will be notified about it with an info box, see Figure 68: Delete IT service through other user.

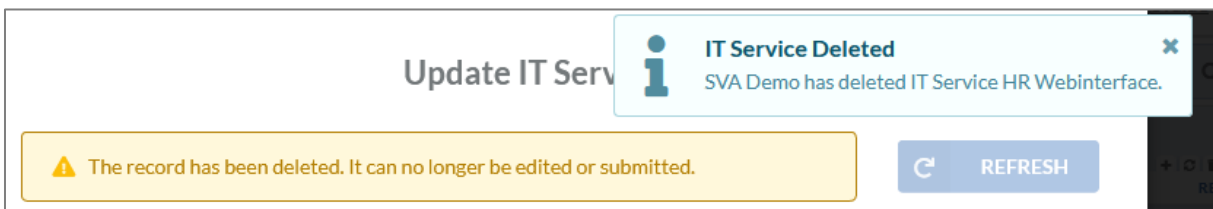


Figure 68: Delete IT service through other user

When an object is deleted, it is not possible to change or save the object in the update window.

Conclusion of a recovery plan

If a user is using the service view, while another user closes a recovery plan, a notification box will appear, informing about the final statement of the recovery plan. The info box will appear on the top right corner, see Figure 69: Message when concluding a recovery plan. This helps a lot while working as a team within the IDR Manager.



Figure 69: Message when concluding a recovery plan

Recovery plan

Create a recovery plan

You can create a new recovery plan in the recovery plan view. Click on the **+** button next to the search bar. The following edit window will open:

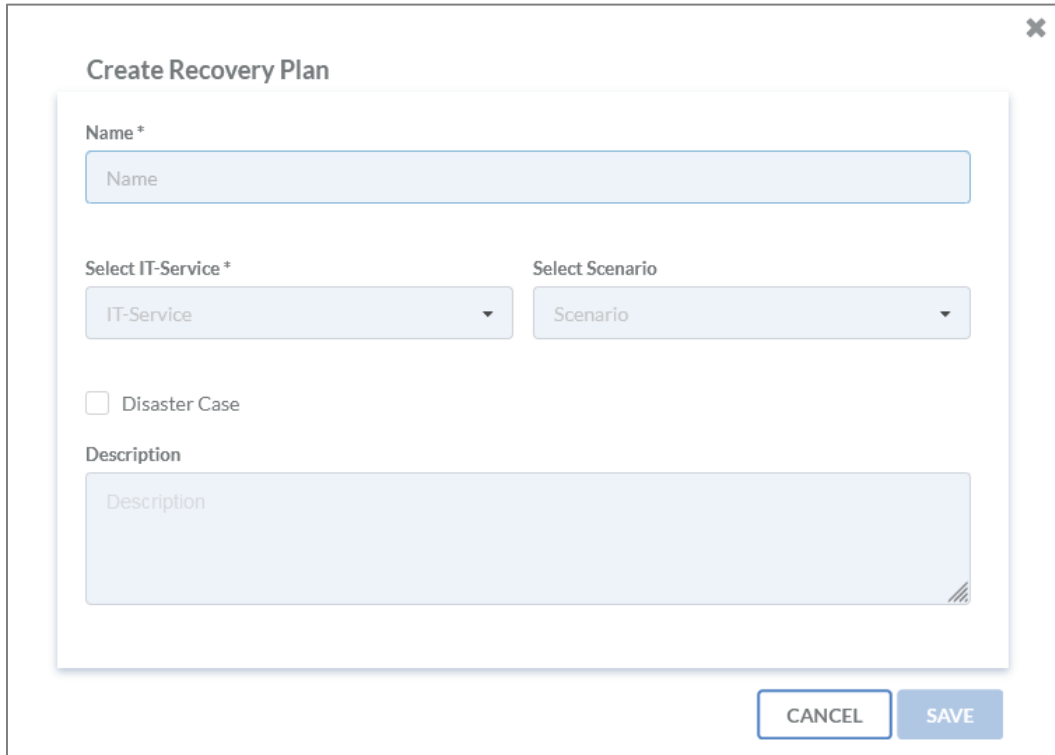


Figure 70: Create recovery plan

The recovery plan needs a name and the selection of corresponding scenario that occurred. It is possible to choose between the one of the stored scenarios or a full recovery. Full recovery implies, that all task items connected to the IT service will be considered.

To create an emergency case, select “Disaster Case”. Otherwise, a test case will be created. Beneath the search bar you will find a tag, showing whether the created scenario is a test or emergency case. If a disaster case has been created, this will be shown in the service view. The service will then be colored red. All other services will be colored blue.



Figure 71: Active disaster case

This interface shows all information on the recovery process. It shows every task in the correct order. After completing a task, you can mark it as done, see Figure 73: Update status in a recovery plan.

If the sum of the RTOs of an application is higher or equal to the MTPD of the IT service, a note will be displayed in the recovery plan, see Figure 72: Note recovery plan.

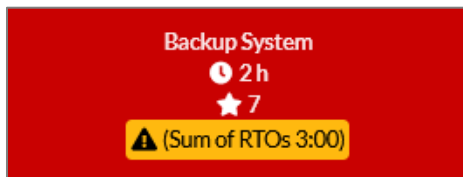


Figure 72: Note recovery plan

Please note: When creating a recovery plan, the current RTO values will be used. Changing these values will not update the values in other existing recovery plans.

Update a recovery plan

A recovery plan shows all tasks, which need to be processed when handling the disaster case. Task status can be updated at any point in time. There are three available states: “not started”, “in progress” and “done”. To update the status of a task, click the object in applications whose task is completed. Now click the task you want to modify (1), modify the status (2) and mark it done (3).

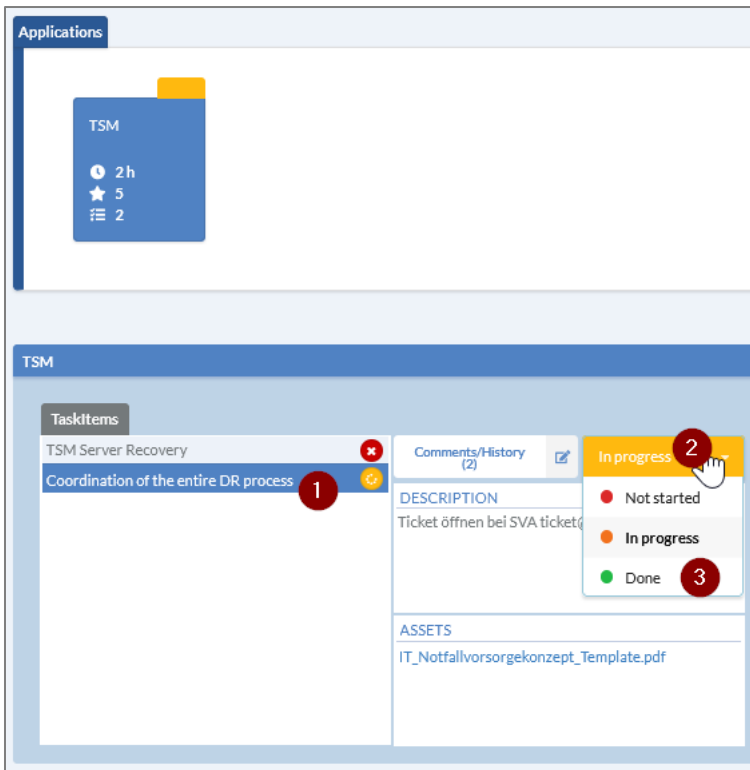


Figure 73: Update status in a recovery plan

As soon as all tasks are completed, the application will be shown as completed. If there is more than one application, the case will be displayed as available, as soon as all applications are completed. This gives you a complete overview on the status of a recovery process. If all tasks are closed, the service will remain red until the recovery plan is concluded.

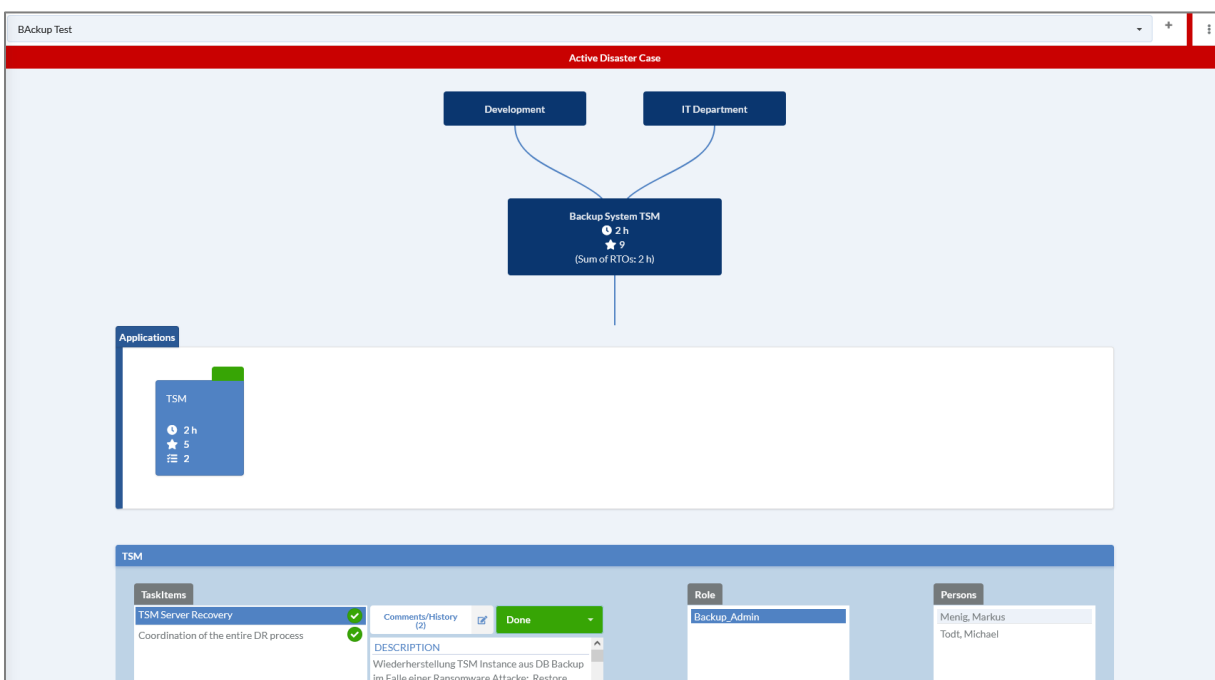



Figure 74: Close a disaster case

View recovery plan information

The recovery plan can be edited, as soon as it has been completed. To edit the plan, open its menu with a click on the  button.

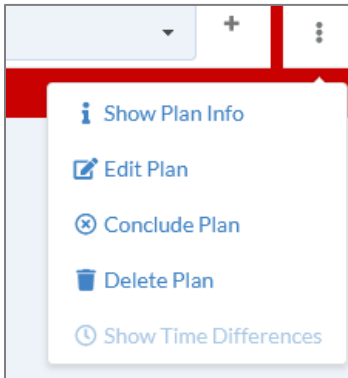


Figure 75: Recovery plan menu

Here the plan can be closed (conclude plan), deleted (delete plan) or updated (edit plan). If more information on a recovery plan will be needed, it is possible to click on “show plan info”. The following windows will open:

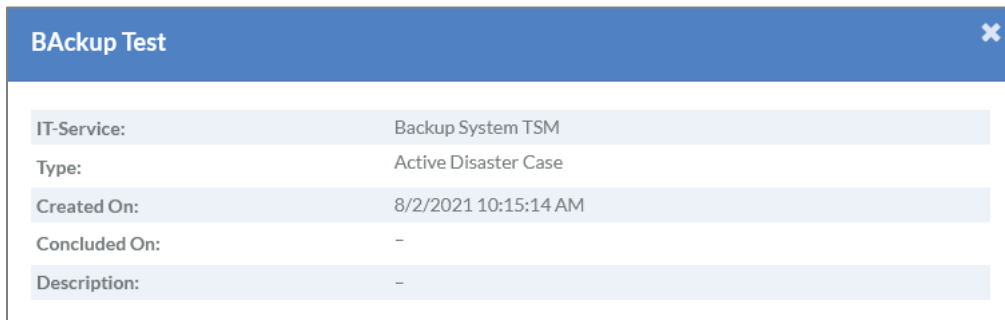


Figure 76: Show plan info

Update recovery plan



To update a recovery plan, click the  button and click “edit plan” to open the following window:

Figure 77: Update recovery plan

By clicking the  button, all changes will be saved.

Conclude recovery plan


When the created recovery plan is updated and the disaster case can be closed, it is recommended to store the recovery plan for a short period of time for documentation and evaluation purposes. After evaluation, the recovery plan will be marked as concluded. To conclude a recovery plan click the

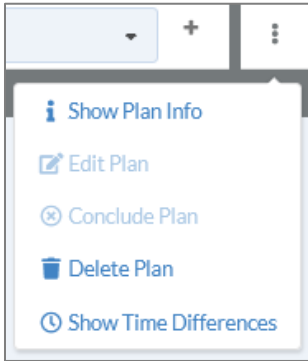
menu  and choose “conclude plan”. The following window will open:

Figure 78: Conclude recovery plan

To finish click the  button.

Please note: While another user is using the service view, the person will be notified when a recovery plan is concluded, note chapter Conclusion of a recovery plan. This is a very useful feature that helps when working as a team within the IDR Manager. When multiple users are using the service view simultaneously, they will be prompted, as soon as the recovery plan is concluded.

When a recovery plan is concluded, it is possible to compare the planned RTO with the actual needed RTO. To open the overview click on the  button and then on “show time differences”.



A window will open, and show the gap between the planned and needed time, see Figure 79: Time differences recovery plan. That helps to adapt the time afterwards to be more precise in a disaster. For the feature to work, the state at the recovery plan need to be set on “in progress” when the recovery for an application starts.

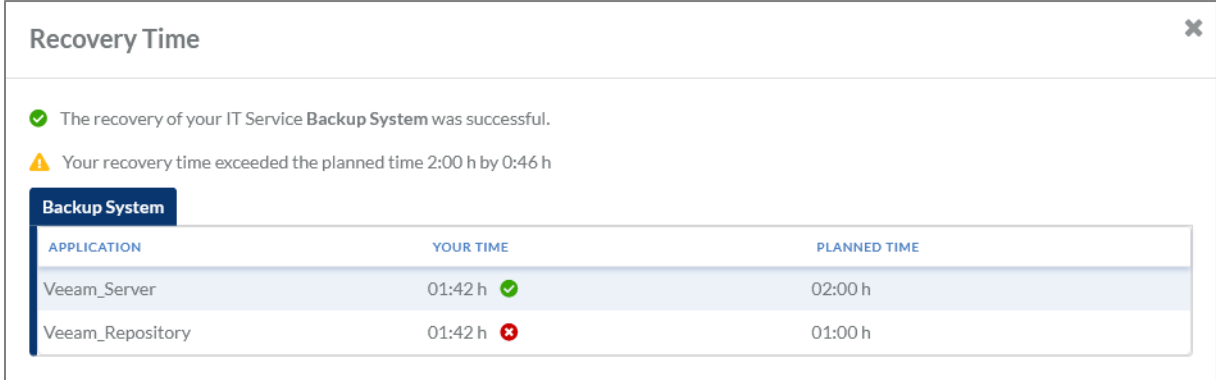

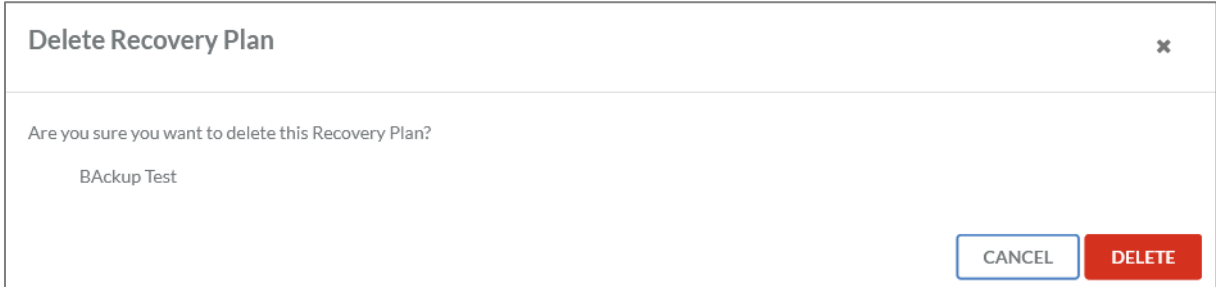


Figure 79: Time differences recovery plan

Delete recovery plan

If a recovery plan is not needed any longer, it can be deleted with a click on the menu  and then choose “delete plan”. The following window will open:



To finish click the  button.

Personal menu

After the login, the name of the user is displayed on the top right corner. After clicking on the name of the user, a personal menu will open.

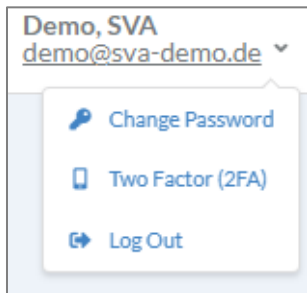
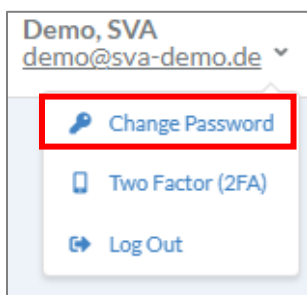


Figure 80: Personal menu

Change password

To change the password, you need to click on “change password” within the personal menu.



A pop-up window will appear, allowing you to set your new password.

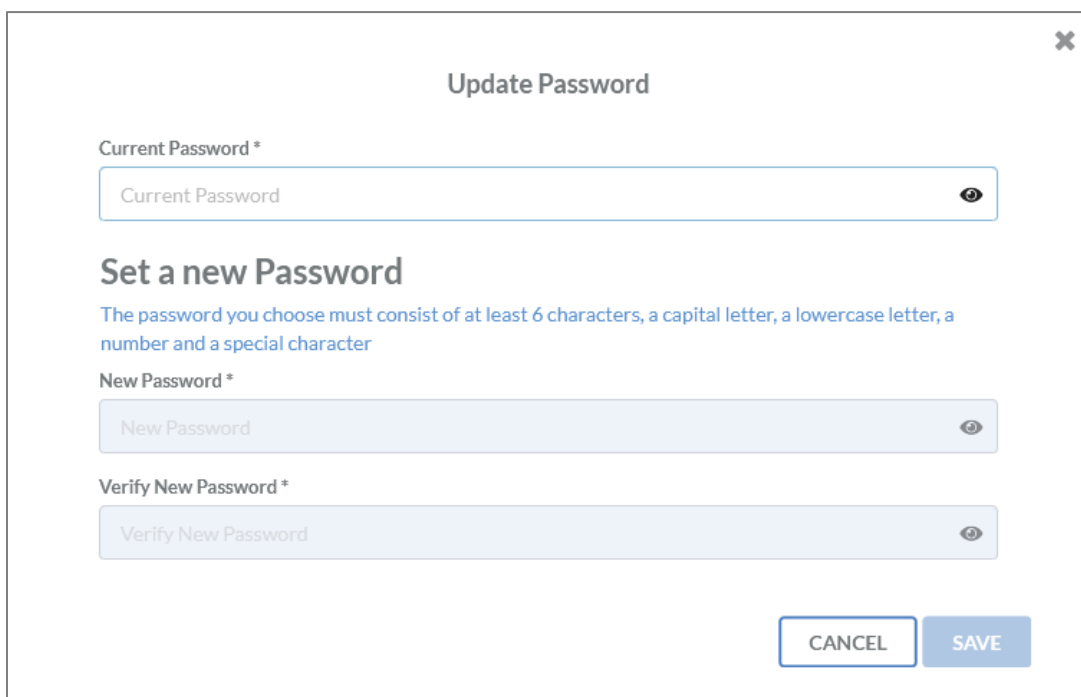
A screenshot of a 'Update Password' pop-up window. The window has a title bar with a close button (X) in the top right corner. The main heading is 'Update Password'. Below the heading, there is a form with three input fields: 'Current Password *', 'New Password *', and 'Verify New Password *'. Each field has a placeholder text and a toggle icon for visibility. Below the input fields, there are two buttons: 'CANCEL' and 'SAVE'.

Figure 81: Password change

To change the password you need to satisfy the following password policy:

- At least 6 characters,

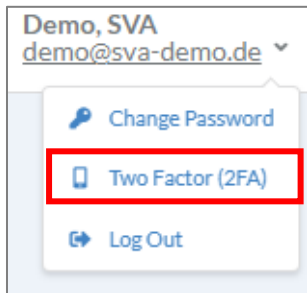
- A capital letter
- A lowercase letter
- A number
- A special character

To finish, click the  button.

2-Factor-Authentication

Configuration

To configure 2-Factor-Authentication (2FA) you need to click on “two factor” in the personal menu.



Afterwards the following edit window will open, see Figure 82: Configure 2FA.

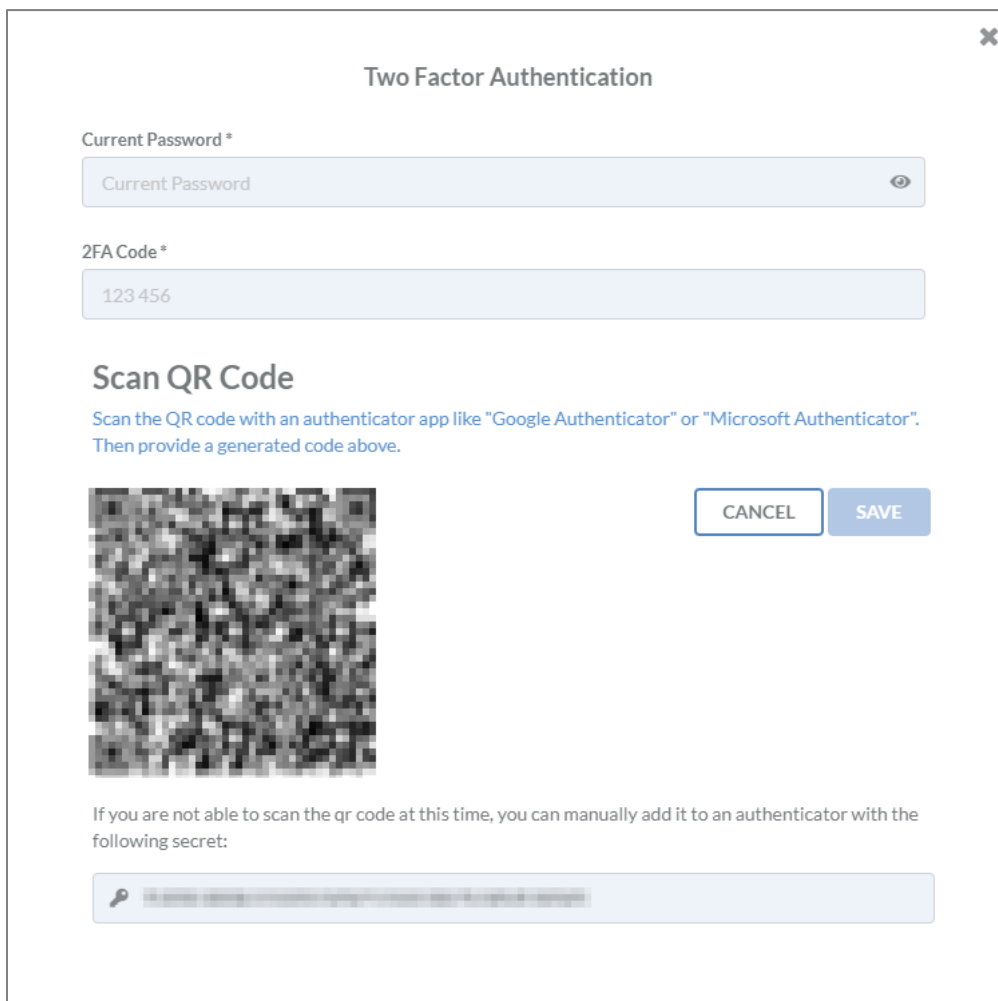
A screenshot of a 'Two Factor Authentication' configuration window. The window has a title bar with a close button (X) in the top right corner. The main content area is titled 'Two Factor Authentication'. It contains two input fields: 'Current Password *' with a placeholder 'Current Password' and an eye icon for toggling visibility, and '2FA Code *' with a placeholder '123 456'. Below these fields is a section titled 'Scan QR Code' with instructions: 'Scan the QR code with an authenticator app like "Google Authenticator" or "Microsoft Authenticator". Then provide a generated code above.' To the right of the QR code is a 'CANCEL' button and a 'SAVE' button. Below the QR code, there is a note: 'If you are not able to scan the qr code at this time, you can manually add it to an authenticator with the following secret:' followed by a text input field containing a secret key.

Figure 82: Configure 2FA

The QR code in the processing windows needs to be read by an authenticator app. It is also possible to type the displayed secret on the bottom side of the screen within the app, if the smartphone camera is unavailable.

The following apps are compatible with the IDR Manager:

- Microsoft authenticator
- Google authenticator
- FreeOTP+ (2FA authenticator)
- Yubico authenticator

Please note: It is possible to use other apps. These apps need the 2FA standard to be compatible with IDR Manager.

After reading the QR code, the app will show a one-time password. That password is required in the field “2FA code”. In addition to the 2FA code, users need to type their current password. To finish, click on **SAVE**.

After saving, you find a set of recovery codes, as shown in, Figure 83: Recovery codes.

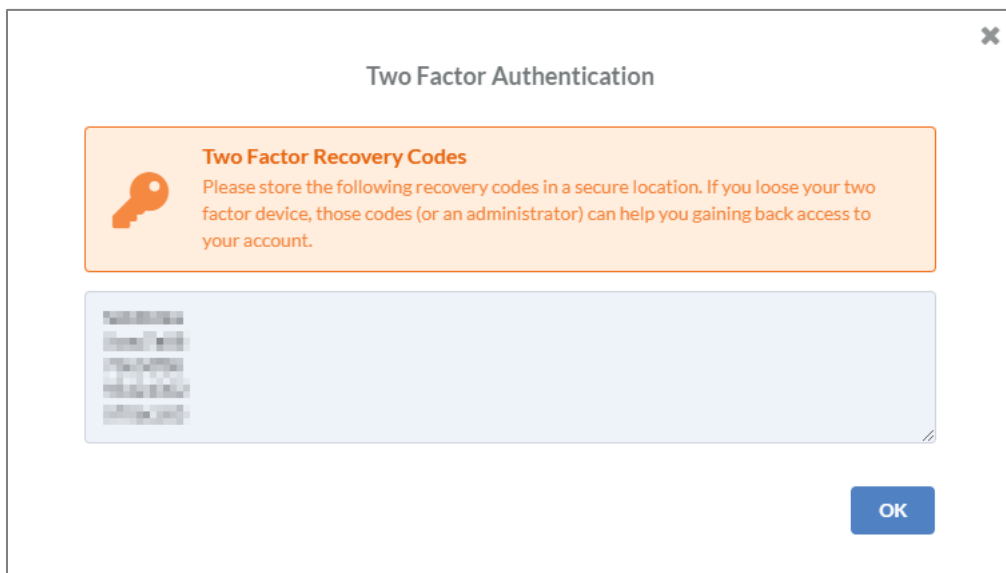
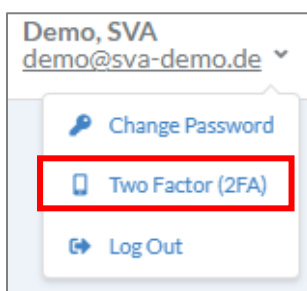


Figure 83: Recovery codes

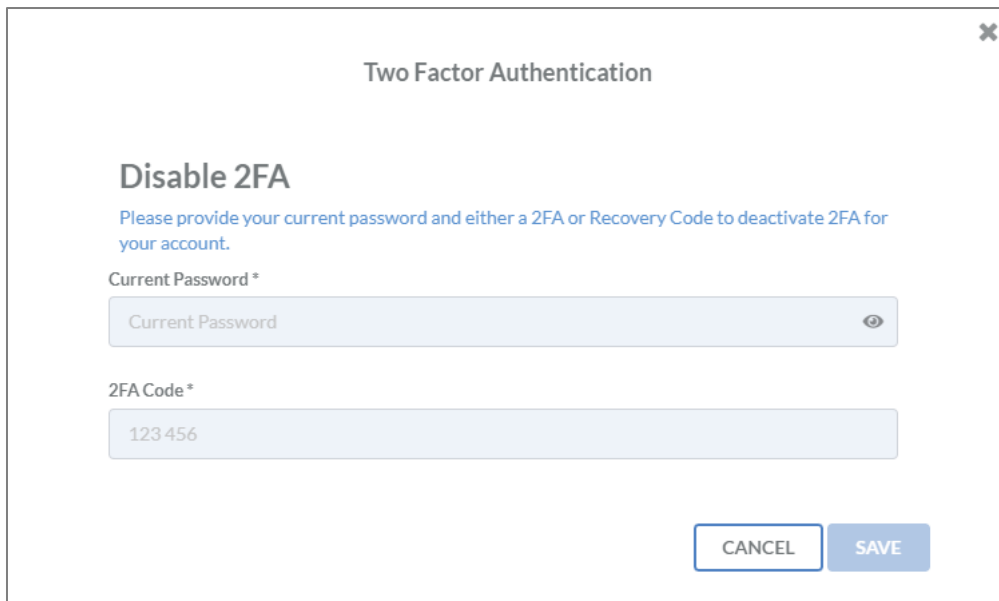
It is recommended to store these codes safely, for example in a password manager. These codes are needed, in case, for instance, users lose their smartphones, where they have their authenticator app installed. One of those codes will enable them to login and register a new authenticator app.

Disable

To delete a second factor, you need to click on “two factor” in the personal menu.



Now an edit window will open, see Figure 84: Disable 2FA.



The screenshot shows a dialog box titled "Two Factor Authentication" with a close button (X) in the top right corner. Inside the dialog, the heading "Disable 2FA" is displayed. Below the heading is a blue instruction: "Please provide your current password and either a 2FA or Recovery Code to deactivate 2FA for your account." There are two input fields: "Current Password *" and "2FA Code *". The "Current Password" field contains the text "Current Password" and has an eye icon on the right. The "2FA Code" field contains the text "123456". At the bottom right of the dialog are two buttons: "CANCEL" and "SAVE".

Figure 84: Disable 2FA

To confirm that step, users need to enter their current password and a 2FA code from the authenticator app. To finally disable the second factor, click the **SAVE** button.

Please note: It is not possible to disable the second factor if the user has been assigned to a tenant with the enforcement of 2FA.

Reports

General handbook

To create an overview on all business cases including all IT services, applications, task items and the deployment of IT services you need to create a general handbook report. To create this report, expand the reports on the left hand side and click on general handbook.

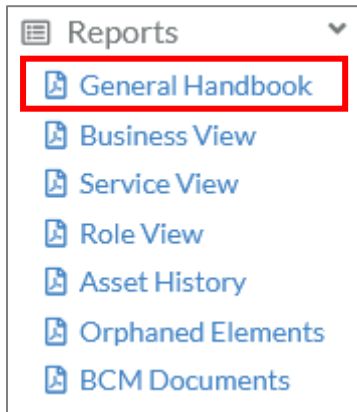


Figure 85: Report overview

The following edit window will open. There you can select each business process you need to be part of the report.

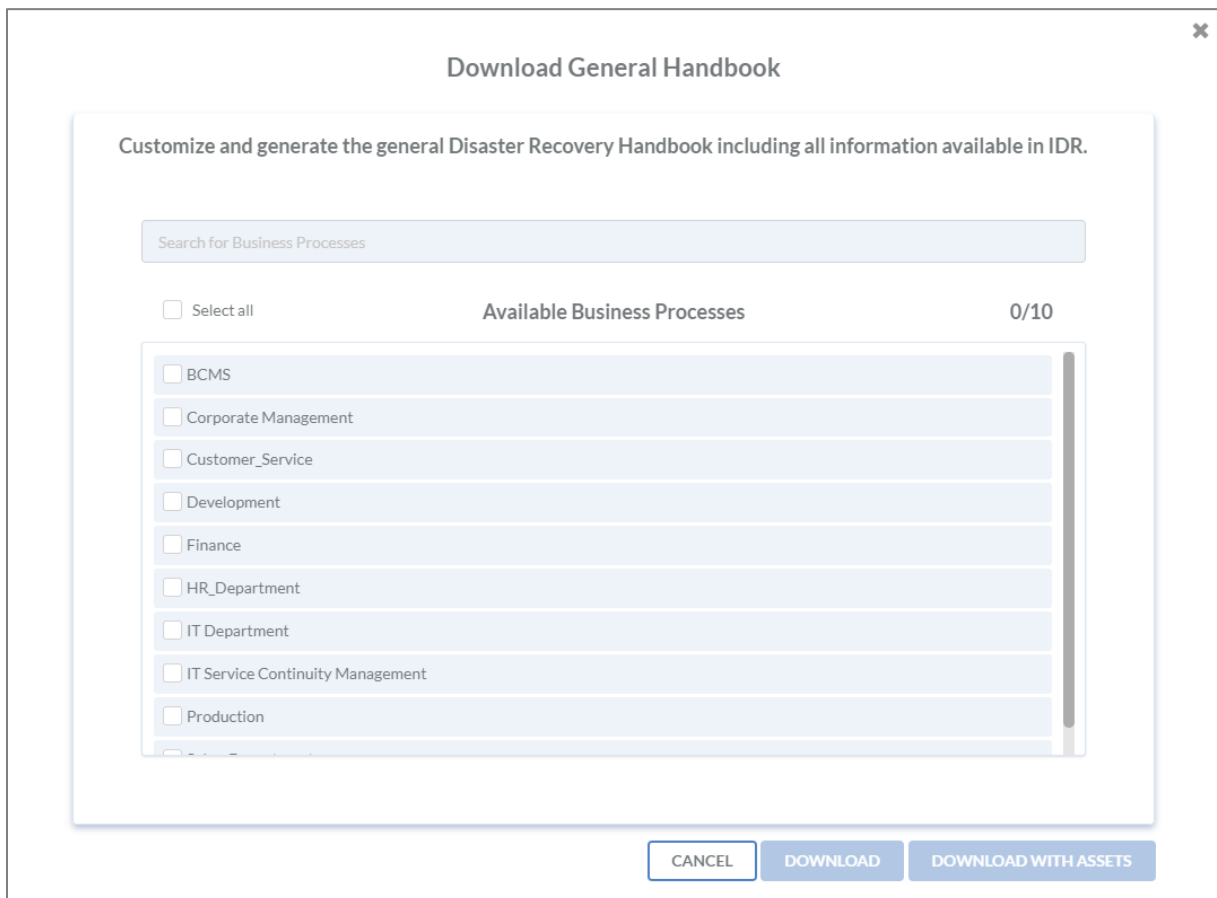


Figure 86: Choice of business processes for the general handbook

To download task items, click the

DOWNLOAD WITH ASSETS

button. Otherwise click the

DOWNLOAD

The general handbook provides an overview on all business processes of the tenant with their IT services and applications, see Figure 87: Business process overview general handbook.

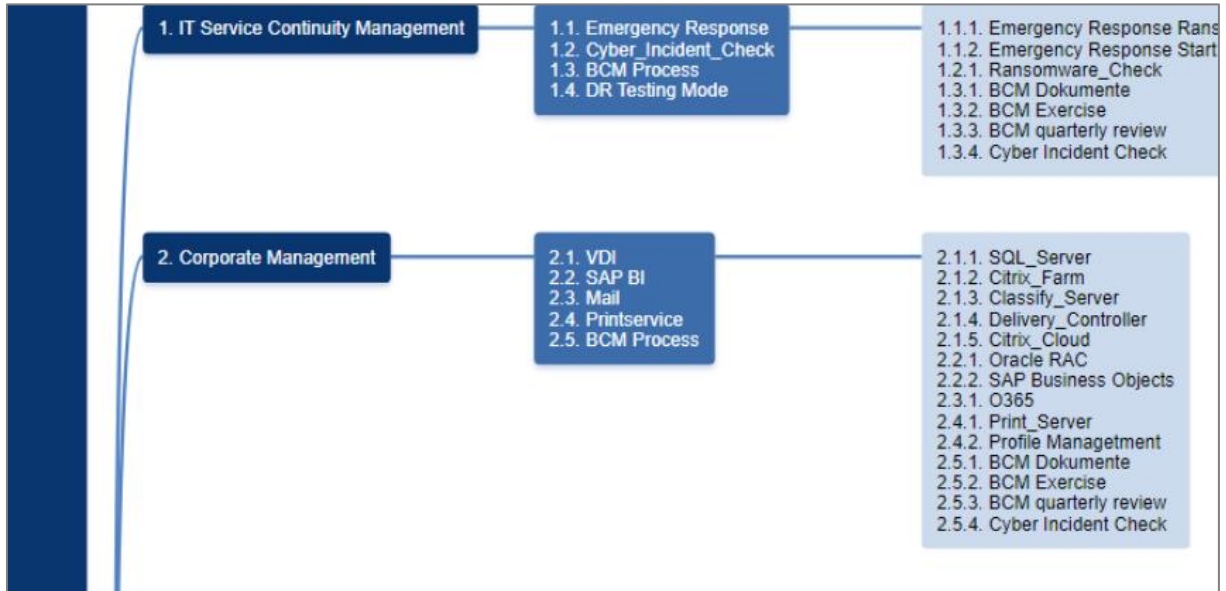


Figure 87: Business process overview general handbook

At Figure 88: Snippet of a general handbook is a snippet of the general handbook

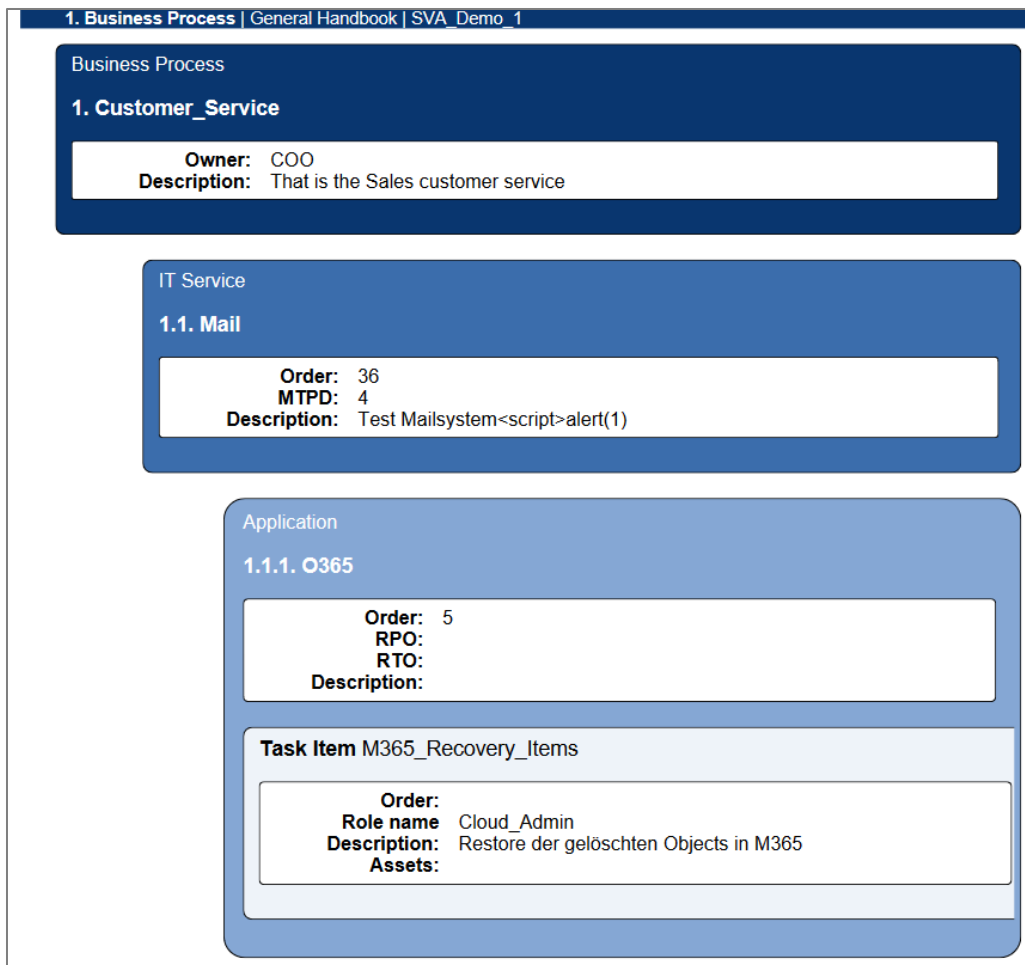
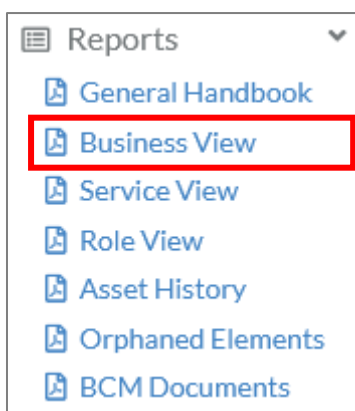


Figure 88: Snippet of a general handbook

Business view

To create an overview on all business cases, including all IT services, applications and task items, you need to create a business view report. To create this report, expand the reports section on the left-hand side and click on business view.



The following edit window will open. Here you can select each business process, you need to include in the report.

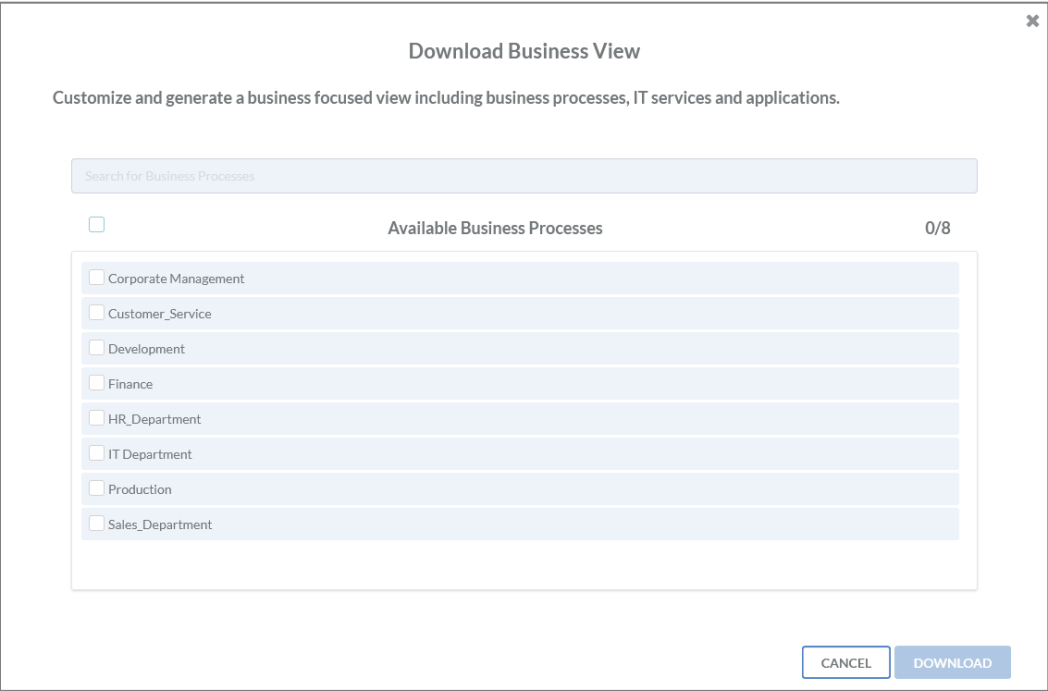


Figure 89: Choice of business processes for the business view

To finish, click the **DOWNLOAD** button.

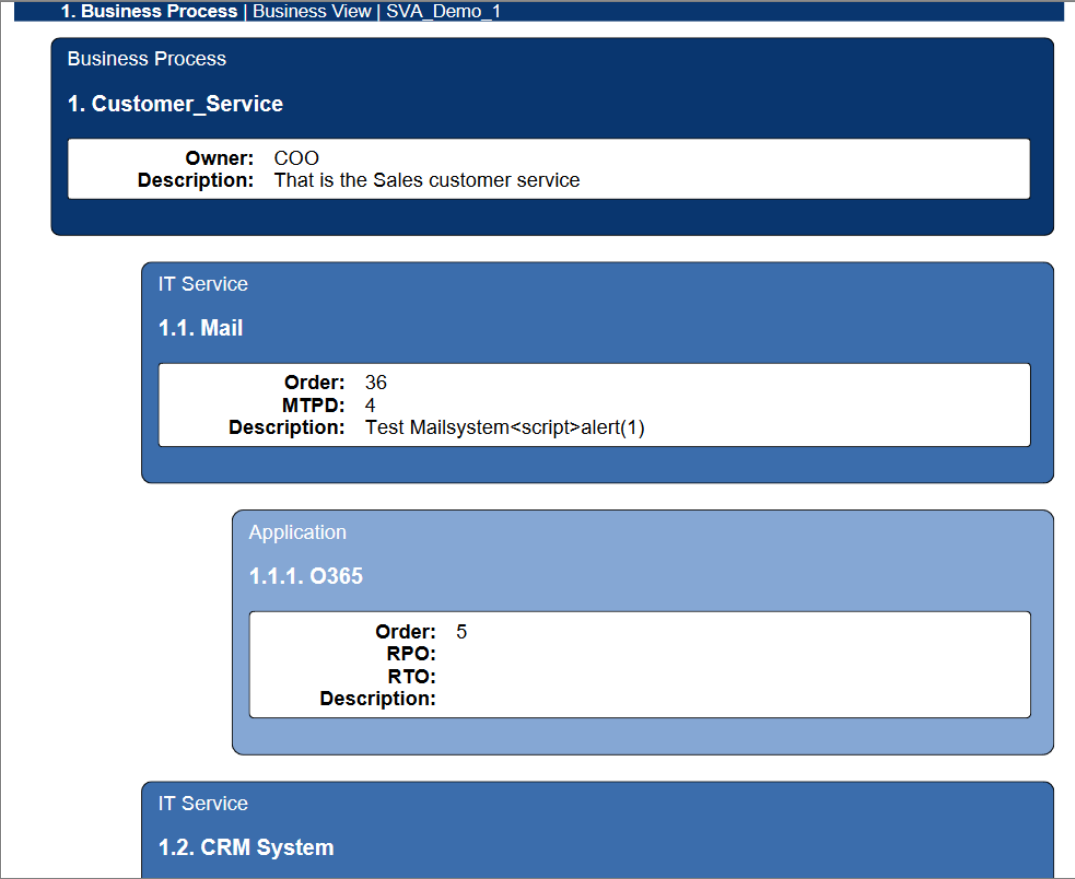
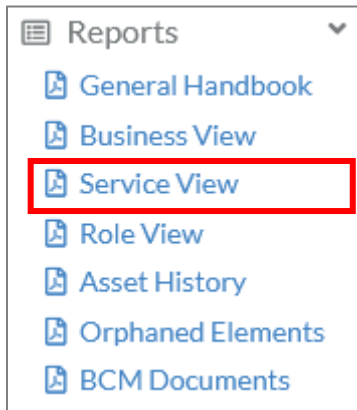


Figure 90: Snippet of a business view

Service view

To provide an overview on all IT services, including all applications and their deployment, you need to create a service view report. To create this report, expand the reports on the left hand side and click on service view.



The following edit window will open. Here you can select each IT service, you need in the report.

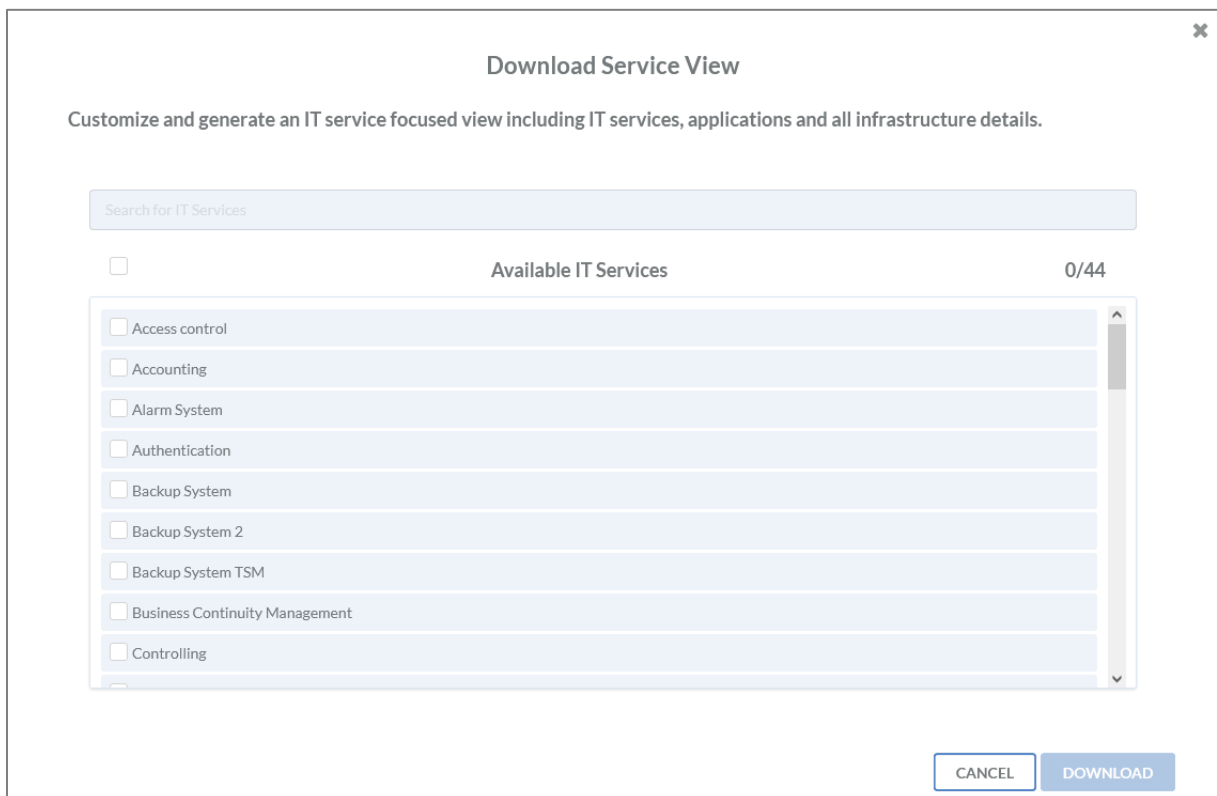


Figure 91: Choice of IT services for the service view

To finish click the  button.

For every listed IT service, there is a section within the document which lists all applications, see

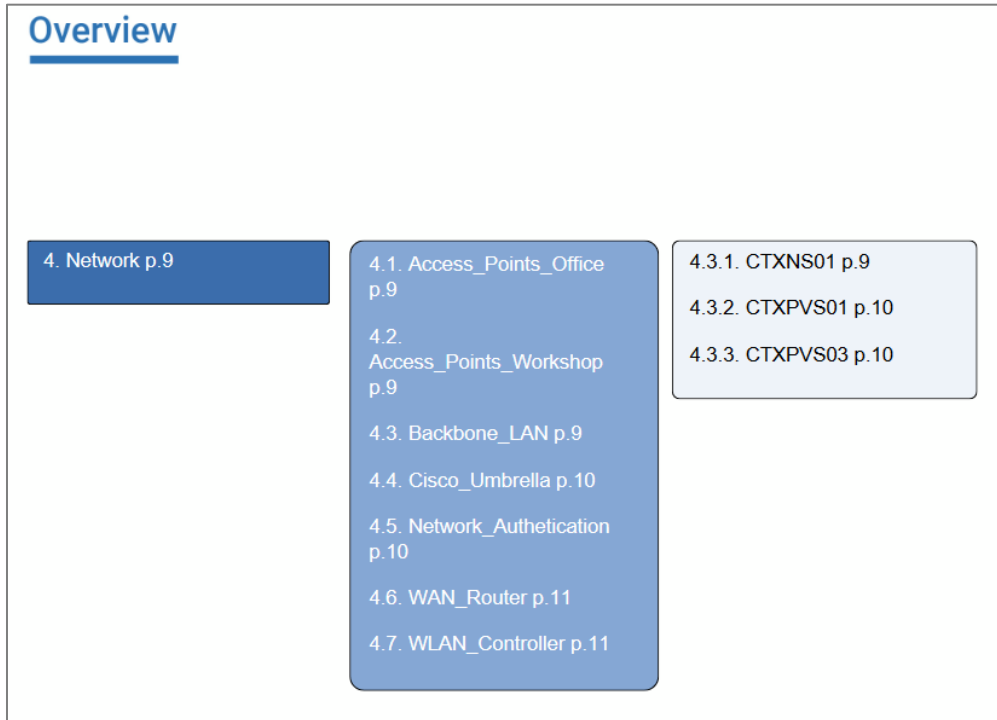


Figure 92: Overview IT services

The below section is a listing of all IT services with detailed information.

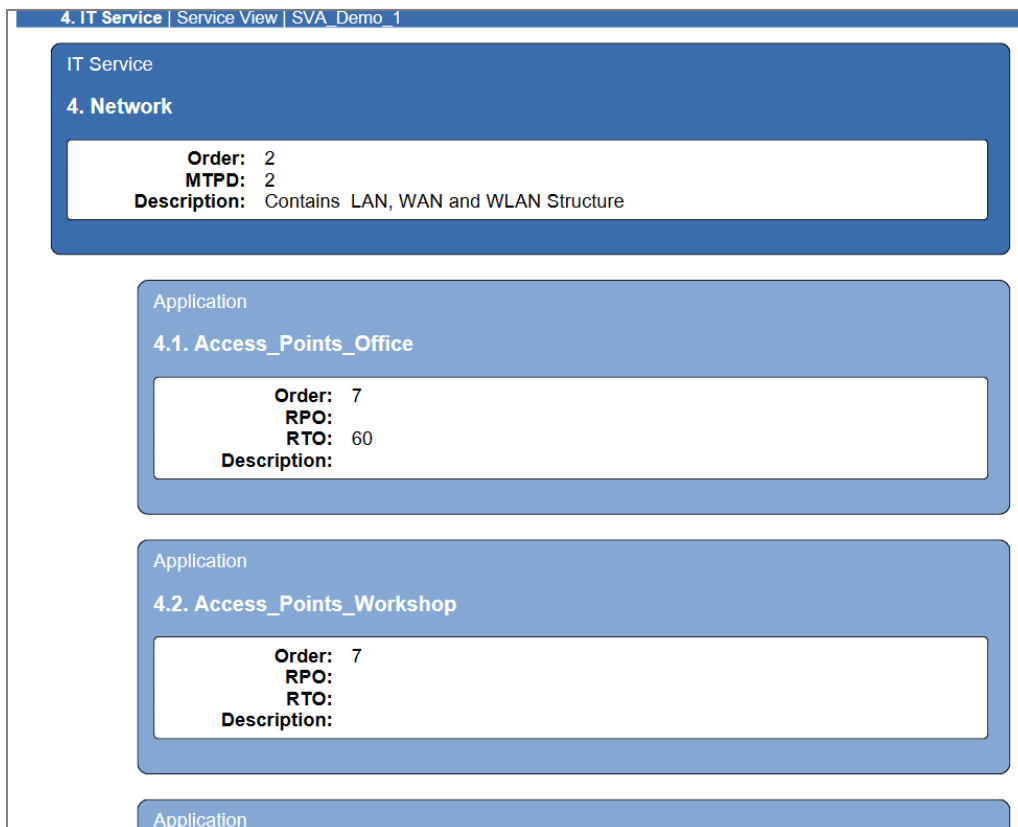
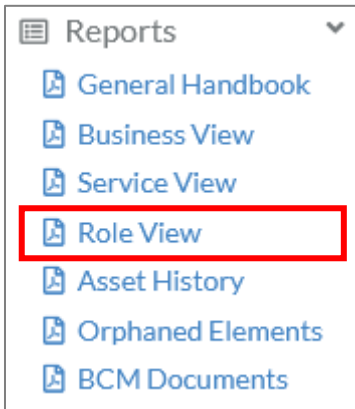


Figure 93: Snippet of a service view

Role view

To create an overview on all roles including carriers, you need to create a role view report. To build this report, expand the reports section on the left hand side and click on role view.



The following processing window will open. Here you can select each role, you need in the report.

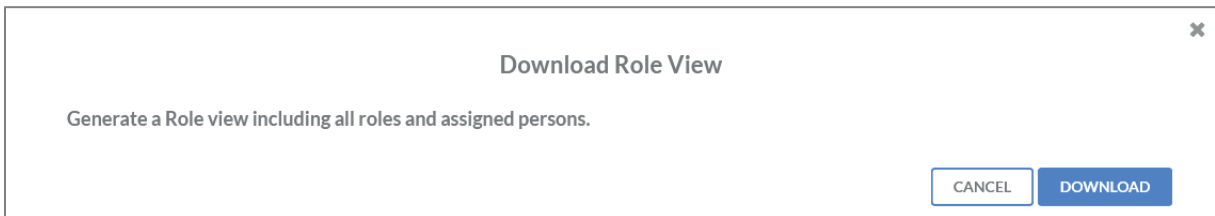


Figure 94: Create role view

To finish, click the  button.

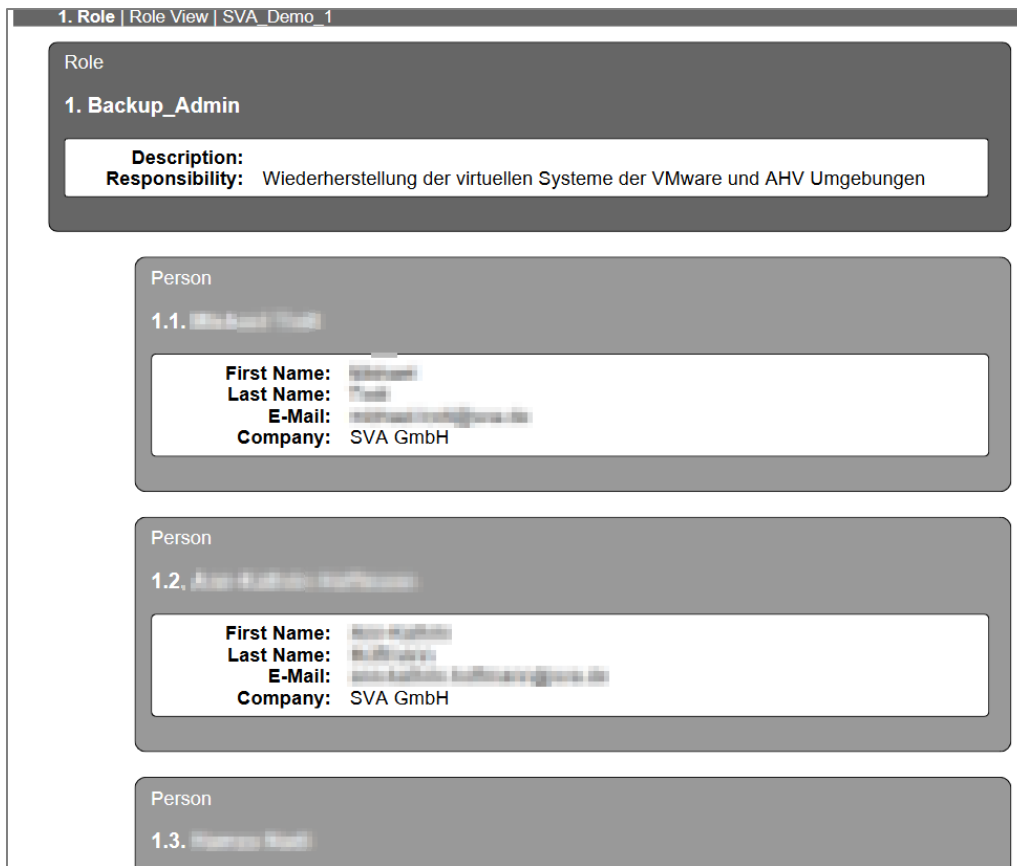
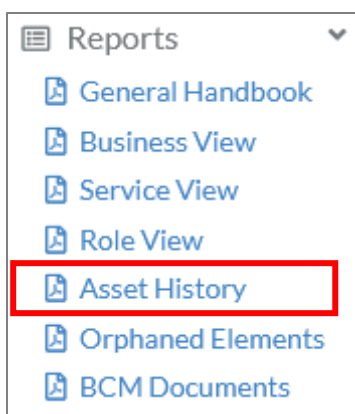


Figure 95: Snippet of a role view

Asset history

To create an overview on all task items, that have been consistent for a defined period of time, you need to create an asset history report. To create this report, expand the reports section on the left hand side and click on asset history.



The following edit window will open. There you can select the date.

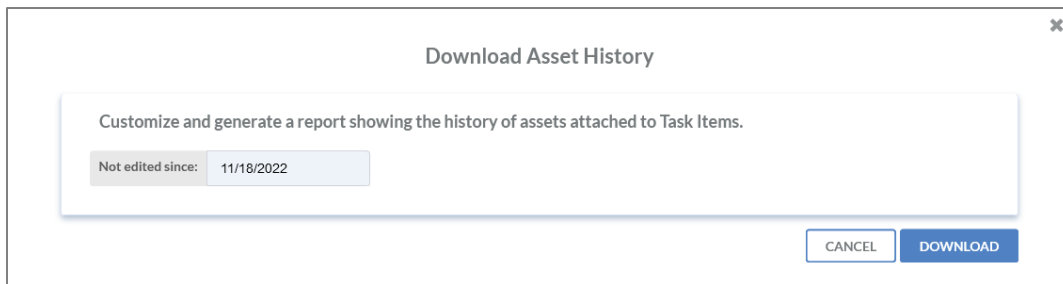


Figure 96: Create asset history

To finish, click the **DOWNLOAD** button.

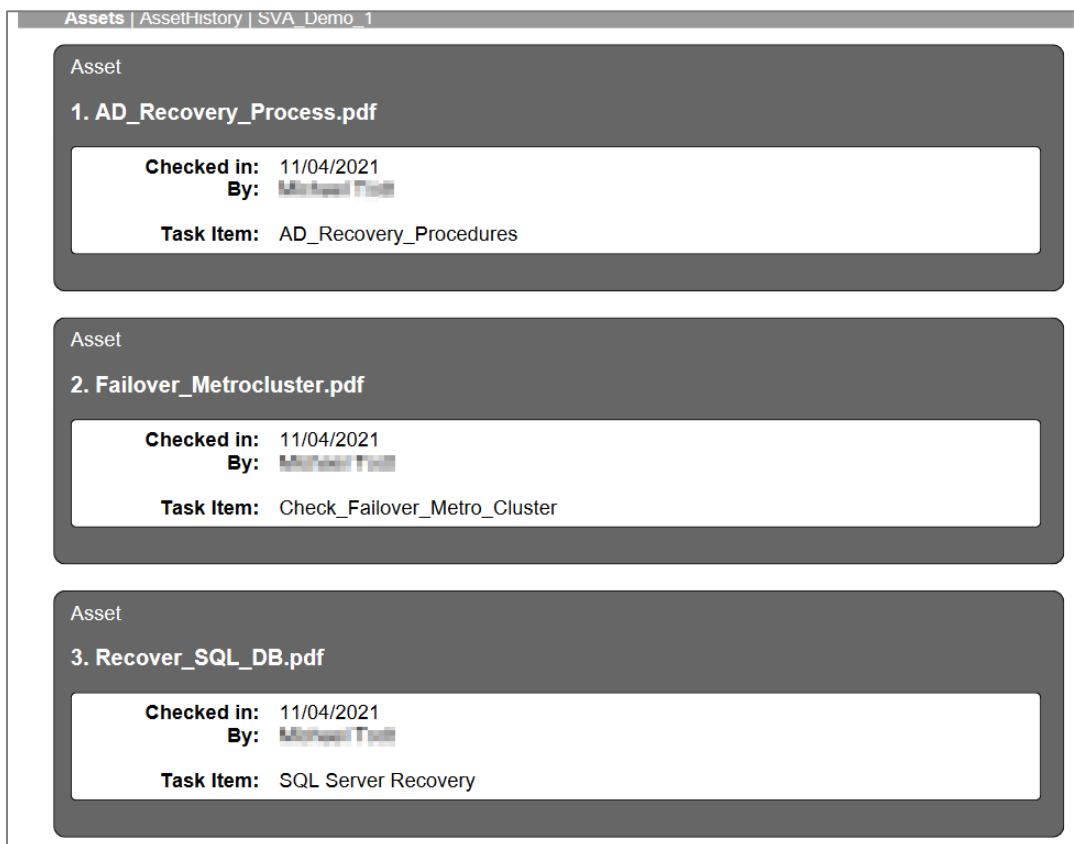
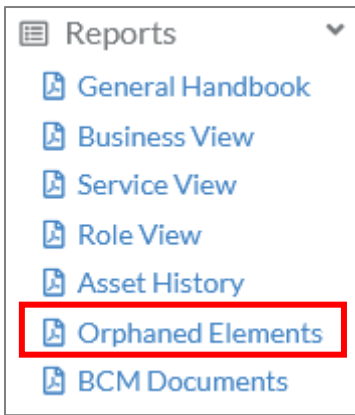


Figure 97: Snippet of an asset history

Orphaned elements

To evaluate all orphaned elements including all business cases, IT services, applications, task items and the deployment of IT services; you need to create an orphaned elements report. To create this report, expand the reports section on the left side and click on orphaned elements.



The following processing window will open, where you can download the orphaned elements.

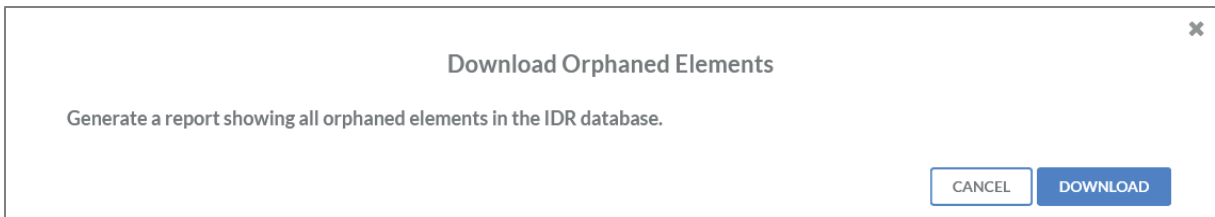


Figure 98: Create orphaned elements

To finish, click the  button.

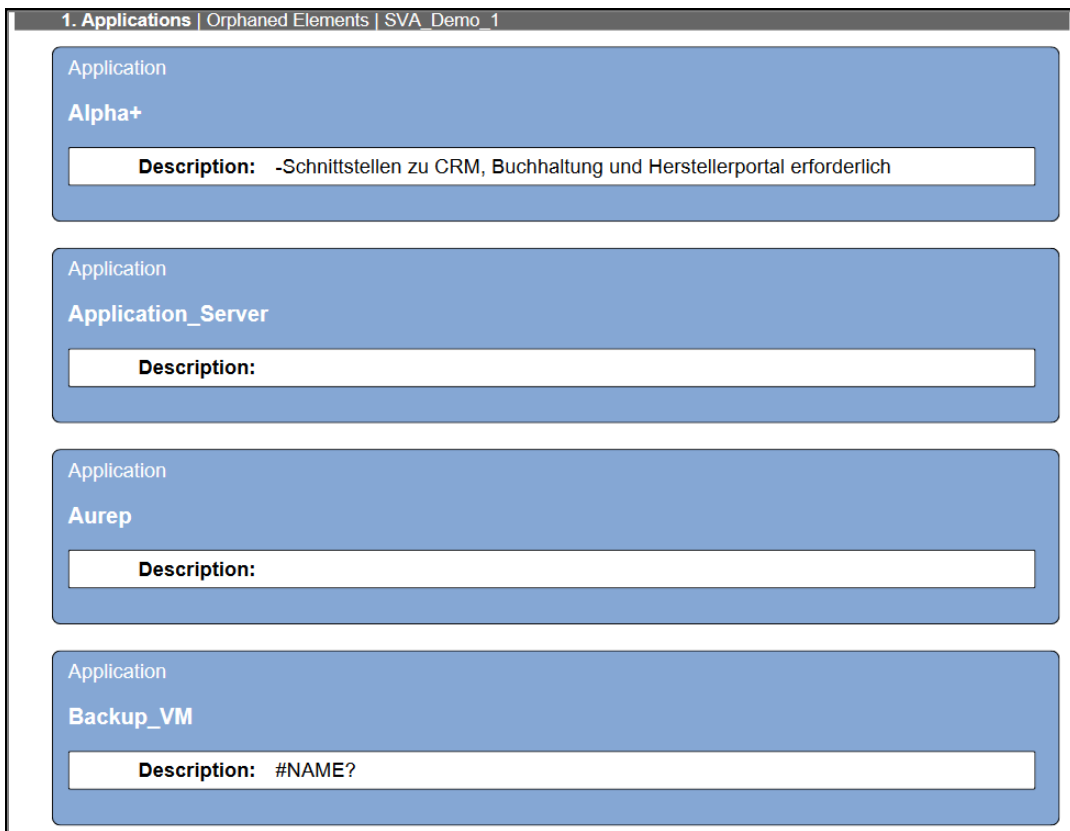
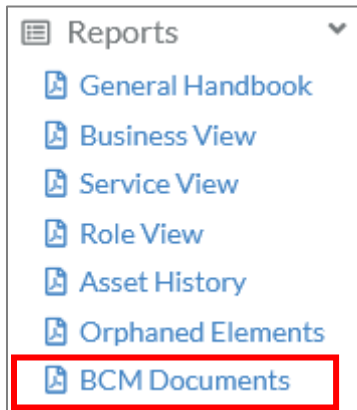


Figure 99: Snippet of orphaned elements

BCM documents

It is possible to store documents needed for the BCM process. Users can add, replace, download and delete these documents according to their permissions. To open this section, click on reports and then on BCM documents.



A window will open, showing all stored BCM documents, see Figure 100: BCM documents.

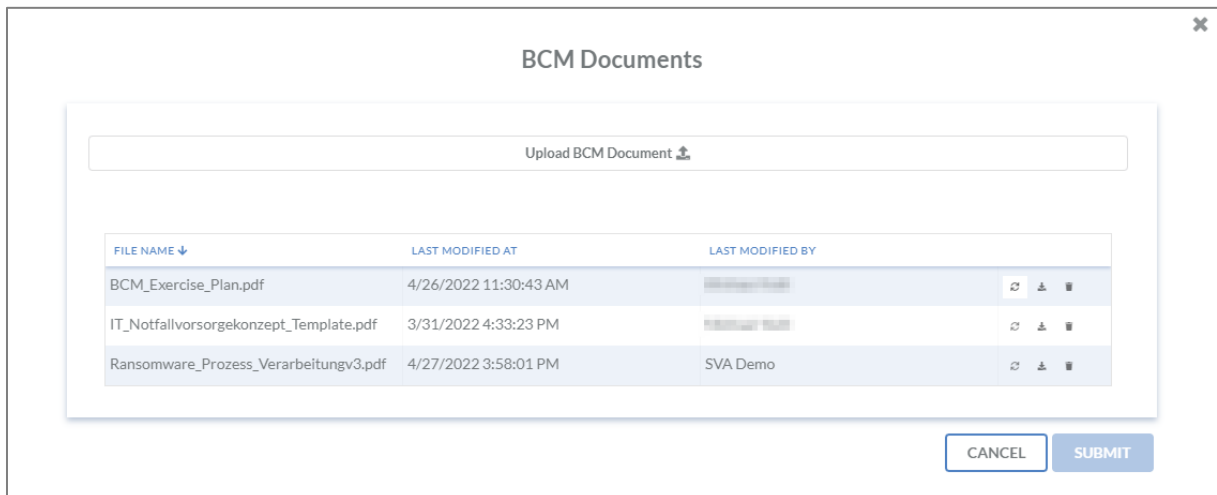



Figure 100: BCM documents

Add BCM document

To add a document, click the  button.





Replace document

To replace existing documents, click the  button next to the document. Afterwards, a new pop-up window will open, where you can select the needed document.

Download document

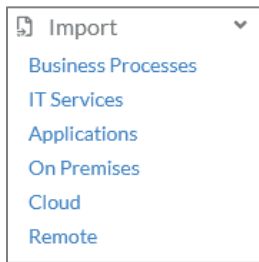
To download a document, click on  next to the concerned document.

Delete document

To delete a document, click the  button next to it. To confirm deletion click on the  button. To discard the changes, click  and then .

Importing

The import menu can be found on the left-hand side of the screen, above “Reports”. To expand the menu, click on “Import”.



The expanded menu shows all available assets that can be imported. To initiate an import, click on the needed section. An edit window will prompt for selecting the concerned list of assets in CSV format. The example below shows a use case on how to upload business processes.

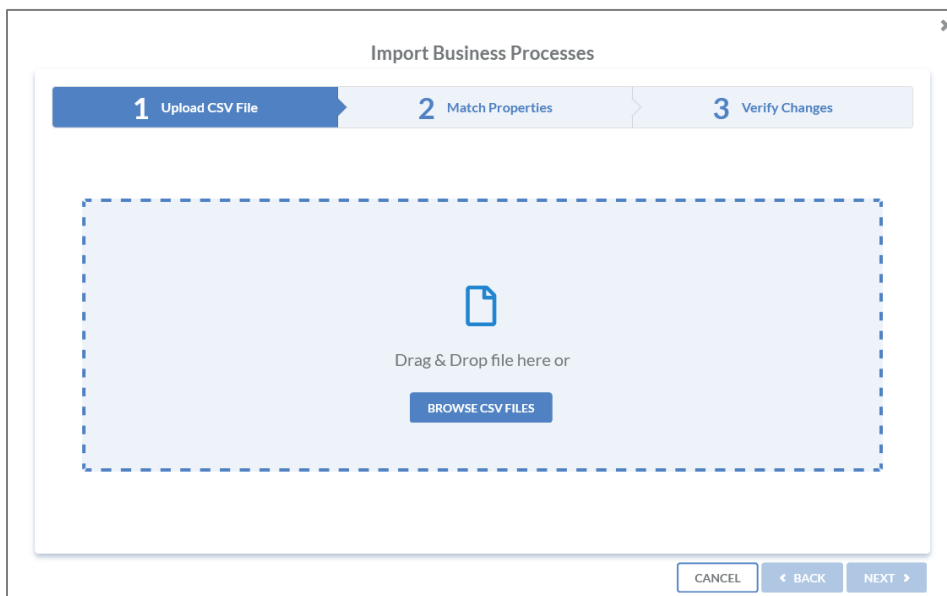


Figure 101: Import business process

When importing a CSV file, you will be prompted to match the criteria in the CSV file with the predefined criteria in IDR Manager.

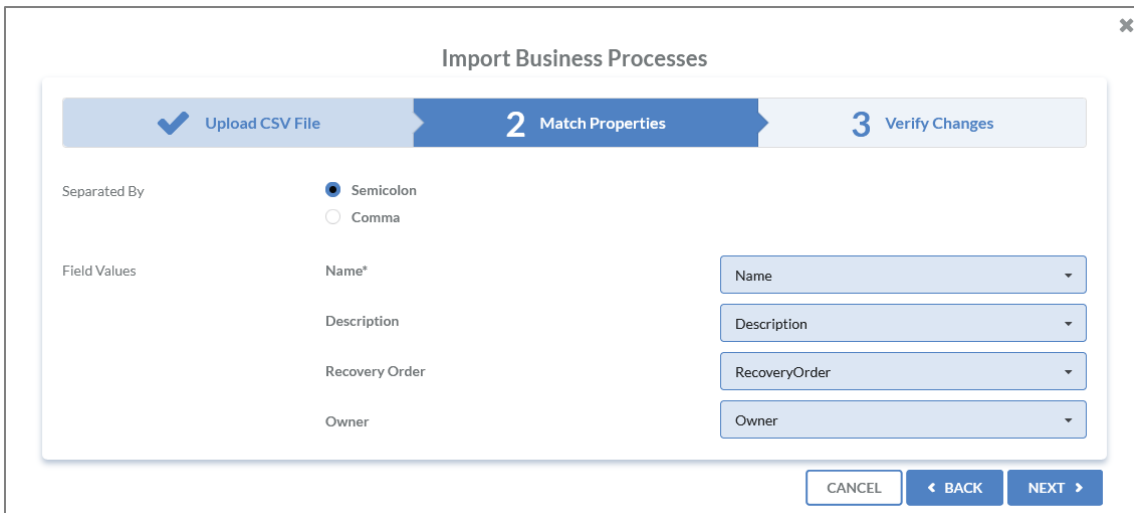


Figure 102: Match properties on import

Once the matching has been finished, a new dialog window will open, showing all objects, that are either new or to be modified.

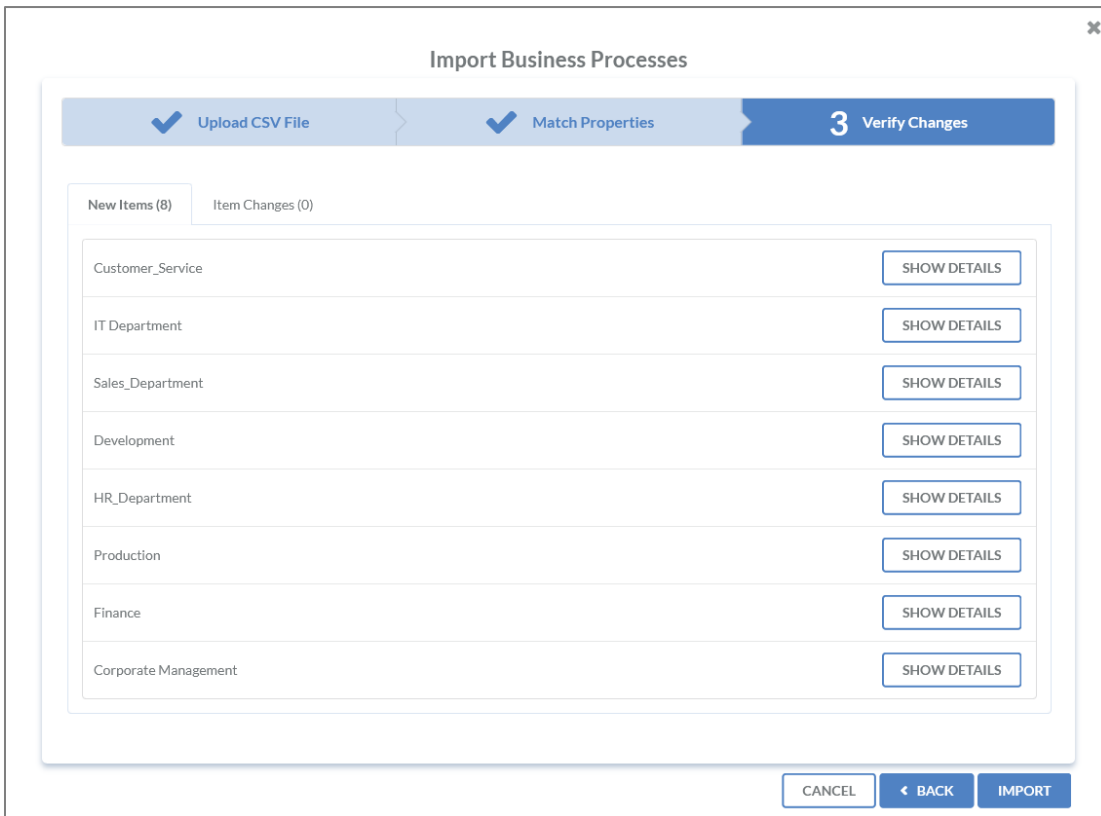
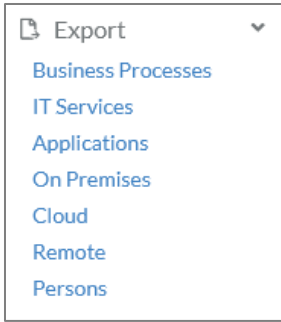


Figure 103: Overview on new and modified objects

Exporting

To export elements out of IDR Manager, click and expand the “Export” section on the left-hand side, which will expand the export menu.



Now you can choose which elements you want to export. The following example show the export of business processes:



Figure 104: Export business processes

To finish, click the **DOWNLOAD** button.

	A	B	C	D	E	F	G
1	Name	RecoveryOrc	Owner	Description			
2	Customer_Service	10	COO	Das ist die Kundenbetreuung des Autohauses			
3	IT_Department	5	CIO				
4	Sales_Department	20	CFO				
5	Development	90	CEO				
6	HR_Department	80	COO				
7	Production	30	CEO				
8	Finance	60	CFO				
9	Corporate Management	1	CEO	Business Leaders			
10							

Figure 105: Snippet of an export

Attachments

Dependencies RPO, MTPD and RTO

On IT services and applications level, the disaster recovery parameters RTO and MTPD are needed. To understand the connection between these parameters, the German Bundesamt für Sicherheit in der Informationstechnik (BSI) created the following figure in accordance with their 200-4 norm:

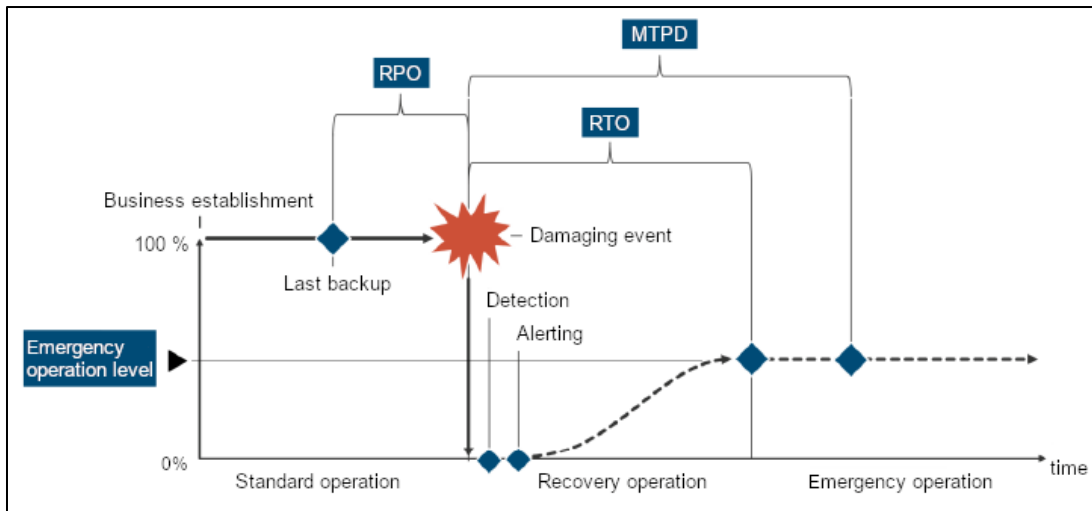


Figure 106: Explanation of the parameters MTPD, RTO, RPO and emergency operation level (BSI Standard 200-4 S.90)

It is critical to understand the significance of the KPIs before defining them. To understand the difference, an explanation about the parameters and their interdependencies will follow. You can find more information on the BSI norm 200-4 on page 90. The norm is currently only available in German.

Below you can find a brief definition of the KPIs:

The Recovery Point Objective (RPO) represents the time period between the last backup and a trigger event. It is important to determine the limit of a loss tolerance of the company.

If an outage scenario occurs, it is important to acknowledge the available time until the potential damage could threaten the existence of the company. This is known as Maximum Tolerable Period of Disruption (MTPD).

The Recovery Time Objective (RTO) determines the expected time to recover systems and is included within the MTPD. It is important to note that the RTO will always be shorter than the MTPD. The RTO comprises the time frames for detection, alarming and recovery. The narrower the RTO, the higher the expected costs.