Bringing Potential to Life

ingentis

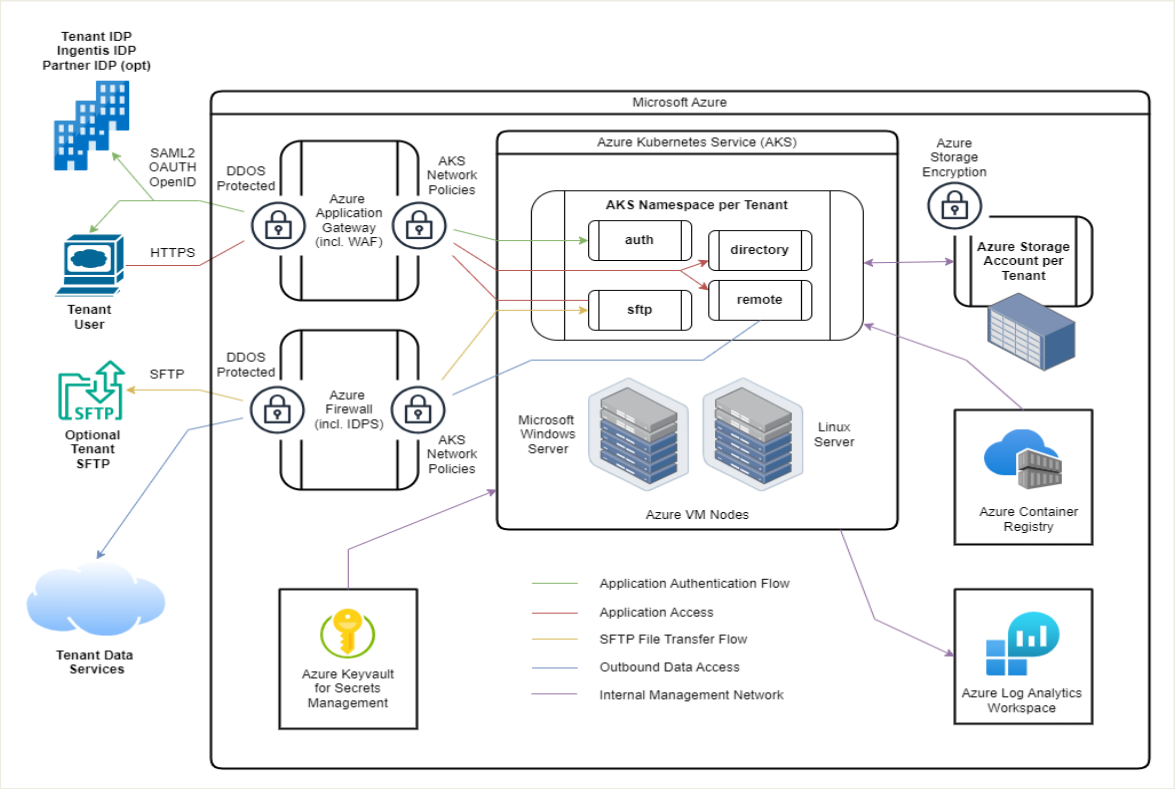
# System Reference Guide v2

| | |
|---|---|
| Project: | **org.manager [SaaS]** |
| Classification: | **PUBLIC** |
| Version: | **2.5** |
| As of: | **23.01.2026** |

Ingentis Softwareentwicklung GmbH · Raudtener Str. 7 · 90475 Nuremberg / Germany · +49 (0) 911 98 97 59-0 · mail@ingentis.com · www.ingentis.de
Managing Directors: Joachim Rotzinger (CEO) · Tobias Weiß (COO)
VAT ID: DE186953155 · Tax ID: 241/129/31461 · Nuremberg Local Court · HRB: 14491

# Contents

# System architecture




Logical architecture Ingentis org.manager [SaaS]

Ingentis org.manager [SaaS] is a specialized version of org.manager that is provided by Ingentis via the Internet and hosted in a regional data center of the MS Azure Cloud. It delivers the functionality of org.manager as software-as-a-service and can be accessed via the Internet in a browser. Access to the SaaS tenant is protected by single sign-on (SSO) authentication with the customer's identity provider (IDP). The configuration and customization of the charts is carried out by Ingentis Consulting; the customer only provides the data via an SFTP upload client or access to an externally accessible SFTP server. No installation is required at the customer's site.

**Note**:

- When using SAP HCM as the data source for org.manager, the org.manager SAP function module must be installed in SAP On-Prem in order to export the data in a fixed format.
- A local org.converter is required to configure the charts.

Ingentis org.manager [SaaS] uses some of the components that are also used in the "on-prem" version. It is a "shared-nothing architecture" and each tenant is physically separated from other tenants. Single sign-on with the client IDP can be implemented using a variety of standards such as SAML2, OAuth, or OpenID Connect.

**The components used in the SaaS version:**

- **org.server** - serves the current organizational chart
- **org.converter** - converts data and configuration (.ocv) into a format (.ows) that can be read by org.server
- **org.directory** - manages the organizational charts for org.server
- **org.remote** - manages the configuration files (OCV) and source data (CSV, SAP, etc.) in projects and jobs for org.converter
- **Authentication agent** - handles the authentication flow between the external IdP (customer, partner, consultant) and issues a JWT for Ingentis applications

# System requirements

System requirements (**cloud**):

- Identity provider with SAML2, OAuth 2.0, or OpenID Connect

System requirements (**clients**)

- Operating systems: Windows, Linux, macOS, iOS, Android, etc.
- Web browsers:
  - Microsoft Edge (Chromium)
  - Google Chrome
  - Mozilla Firefox
  - Apple Safari
- The browser must allow session cookies

Google, Mozilla, and Apple continuously release updates for their browsers. We strive to fully test and support the latest versions as soon as they are released. However, if errors occur in OEM-specific browser software, we cannot guarantee that we will be able to fix them in all cases.

# Updating data

org.remote manages file-based data within data groups. These files can be uploaded manually or via SFTP. This SFTP implementation offers both directions, whereby the customer can upload files to the client's SFTP server using an SFTP client of their choice, or the system can retrieve data via SFTP from an SFTP server provided by the customer.

In addition to this file-based update, various web services can also be used.

## SFTP

SFTP (Secure File Transfer Protocol) works via SSH (Secure Shell) and provides secure file transfer by encrypting the data during transfer, thus protecting it from interception or manipulation.

The SFTP service can be accessed via a separate URL and a user-defined port. The final port is specified when the tenant is created and is between 2222 and 3333. The default port 22 is

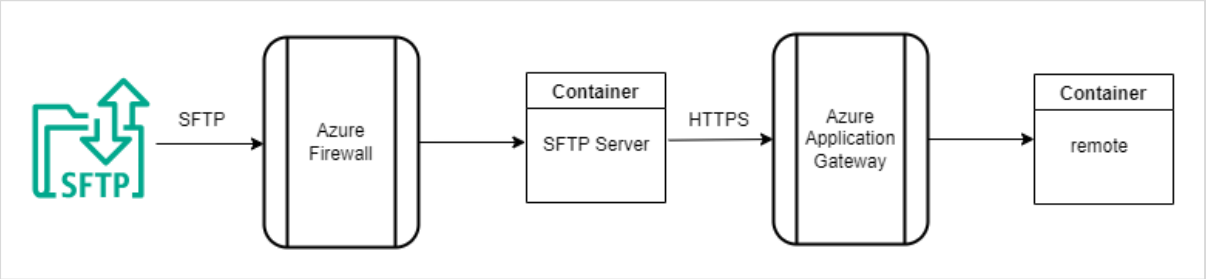
not available for security reasons. The following restrictions apply to connecting and uploading data:

- Authentication is limited to the use of an RSA certificate (self-created or provided by Ingentis). The RSA certificate must be at least 4096 bits.
- Username and password are not supported.
- If a ZIP archive is used, it must not be password-protected
- Image files can only be uploaded in a ZIP file

The data can be uploaded to the org.manager [SaaS] platform via an SFTP server. The SFTP server can be requested from Ingentis and is not provided automatically. Ingentis does not provide a specific SFTP client and does not recommend one. The data can be stored in a zipped folder (*.ZIP). It is also possible to upload CSV, TXT, OMS, and OMZ files. Images must be uploaded in a ZIP archive.

There is no limit to the amount of data or files that can be uploaded. However, it should be noted that uploading 1,000 individual files of 1 MB each takes significantly longer than uploading a single ZIP file of 1,000 MB. Existing data in the data groups will not be deleted, but existing files will be overwritten during the upload.

## Usage (SFTP file upload)




The file transfer architecture.

**SFTP upload:**

1. The customer should compile all required data, which should be in the same data group, preferably in a ZIP file (CSV, TXT, OMS, and OMZ files can also be uploaded).
   - The name of the file is irrelevant.
   - Multiple files can be uploaded to a data group.
     - Existing files will be overwritten.
     - New files will be added.
     - Old files will be retained.

2. The customer uploads the file via SFTP to the designated data group folder.
   - Data can only be stored in second-level folders (=data group folders; e.g., "/Charts/Pictures" from the image above).
   - The server "recognizes" the upload and immediately begins the next step as soon as the file upload is complete.

3. The file is transferred to org.remote via SFTP using an encrypted connection.
   - The "destination" of the file is determined by the upload folder.
     - The first level specifies the project.
     - The second level or the folder name itself specifies the data group.

4. After the file has been transferred to the remote station, it is immediately deleted from the SFTP server.
   - A ZIP file is automatically unzipped by org.remote.
   - "Synchronization" is not possible

## Usage

Ingentis provides the platform, the org.manager configuration including the promised functionalities (e.g., perspectives, layouts). Since the configuration is very complex and requires a local installation of org.converter, we recommend having Ingentis configure the system and only uploading the necessary HR data and initiating the organizational chart update process.

## Automation via scheduler

It is possible to use a time-based schedule for automatic conversion by org.converter. The schedule can only be set in the org.remote GUI.

# Licensing

## Master data

The number of data records processed by org.converter is decisive for licensing. If the number agreed in the license is exceeded, the conversion process (generation of the organizational chart) is terminated. The number of master records remaining in org.converter after data manipulation has been carried out is counted, not the number delivered by SAP. The data manipulation functionality allows you to clean up unclean source data by deleting unwanted objects.

In addition, the data volume in the SAP module itself can be limited by selecting the appropriate root node.

In this context, a master record is any SAP HR object. The object with the most elements is the limiting factor for licensing. In most cases, these are likely to be positions.

**Example 1:**
License with 5,000 master records, SAP export delivers 2,000 organizational units, 5,300 positions, and 4,700 employees, despite the restriction to the root node for Germany. → The number of positions exceeds the license scope, and org.converter aborts the conversion process.

**Example 2:**
As in example 1, except that org.converter creates a data manipulation that deletes all 400 positions assigned to the "Legacy" organizational unit→ 4,900 positions remain for further processing, so the license limit (5,000) is not exceeded and the conversion is carried out.

## Data sources

In general, Ingentis org.manager [SaaS] supports all existing data sources of org.manager with the exception of Excel (.xls and .xlsx) and local files. JPG and PNG are supported for image files (e.g., employee photos). Data files (e.g., in CSV file format) can be uploaded via org.remote and used as a data source. In most cases, however, the customer's data sources are not accessible from outside the company.

For this reason, Ingentis org.manager [SaaS] offers both an SFTP server endpoint for automatic file uploads and SFTP client functionality for retrieving customer data from an SFTP server provided by the customer. While SFTP works via SSH (Secure Shell) and thus ensures secure authentication, the file itself can also be optionally encrypted with PGP.

For SAP HCM, the "org.manager On-Prem" SAP function module can be used to extract data in structured ASCII files within the company network and then upload it to Ingentis org.manager [SaaS].

# Modules

The best practice for outputting org.converter (= the organizational chart) is HTML5, which can be displayed in common browser applications.

## SAP function module

Data is retrieved from SAP using an org.manager function module, which must be transferred to SAP via transporters. This function module is configured (definition of read fields, evaluation paths, etc.) in an IMG within SAP. The function module is able to provide the data as an export ("PUSH").

The following SAP objects can be exported via the function block as standard and without modification:

- O - Organizational unit
- S - Personnel position
- P - Personnel
- CP - Central person
- C - Center
- JF - Job group/job family
- Q - Qualification
- T - Task

Employee photos stored in SAP can also be extracted using an additional SAP report.

A detailed technical description of the function module can be found in our customer portal.

The org.manager SAP web service interface cannot be used for org.manager [SaaS] because the SAP system cannot be accessed from the Internet/cloud (where org.manager [SaaS] is located) within a company network.

## Access protection

Access protection is an additional module in org.manager [SaaS].

Unlike in org.manager [server], when using access protection, an organizational chart is created for each user, regardless of their permissions.

Permissions are controlled by configurable rules defined by org.converter. For example, it is possible to display only the structures below each user's respective organization. In order for the permission to be executed, the login of the employee in question must be included in the data. In the context of org.manager [SaaS], the "login" is the user's email address, which is provided in the access token.

## org.simulator

Web-based simulations can be run in org.manager [SaaS] Enterprise Edition via org.simulator. Based on the current structure, simulations can be started and saved without manipulating the data in the production system.

Objects can be moved, and new objects can be inserted into or deleted from the structure. The changes are made directly in the graphical structure. In addition, object attributes can be changed and change lists can be read. Furthermore, objects can be moved to a separate clipboard so that they can be inserted elsewhere later.

org.simulator can also be used in conjunction with access protection (not to be confused with the additional access protection module). This allows you to specify that all responsible persons may only perform simulations within their own area of responsibility.

## org.manager [mobile]

With the optional org.manager [mobile] module, organizational charts can also be displayed on mobile devices (iOS/Android). iOS is officially supported from version 9.0 and Android from version 6.0. No statement can be made about compatibility with earlier versions of these operating systems.

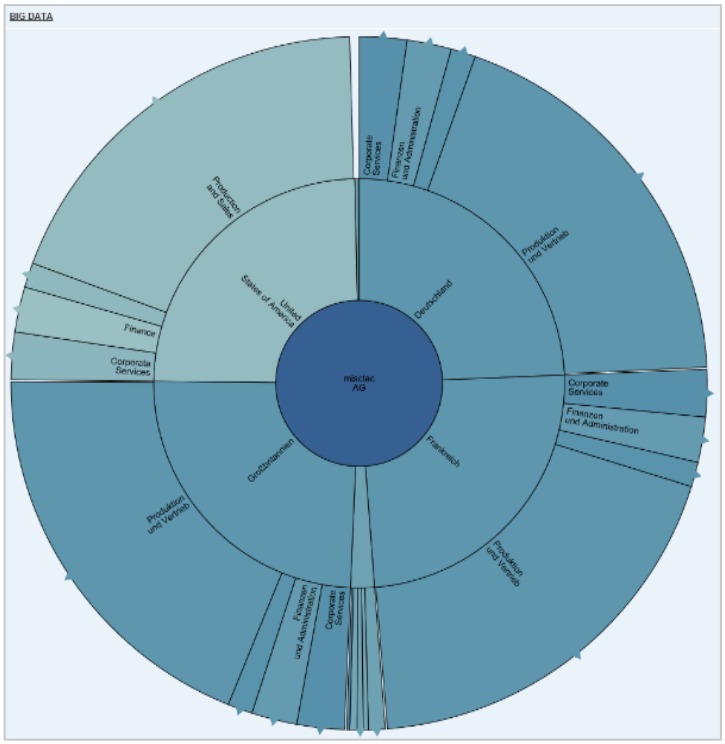
org.manager can also be used on MS Surface devices without the org.manager [mobile] module. The same applies to conventional notebooks running MS Windows.

## Edit mode

Edit mode allows you to make changes to any field in the organizational chart. Such changes include borders, colors, fonts, and even the text displayed. In other words, it is possible to overwrite the form of an attribute from the data source in the browser. The changes are not written back to the configuration file or the data pool. However, they can be saved locally by the client. The change file can be uploaded back to the organization chart later.

## Visualization of big data

When displaying large organizational structures with multiple levels, conventional tree views are usually not the best choice. The optional big data visualization module offers customers numerous alternative view types.



# Security

Ingentis org.manager [SaaS] runs in regional data centers of the Microsoft Azure Cloud and is operated entirely by Ingentis. The exceptions are Australia and New Zealand, where org.manager [SaaS] is operated by Navigo Pty Ltd. Ingentis and its service providers comply fully with the GDPR (General Data Protection Regulation). All data is stored in accordance with the GDPR and deleted 30 days after the end of the contract.

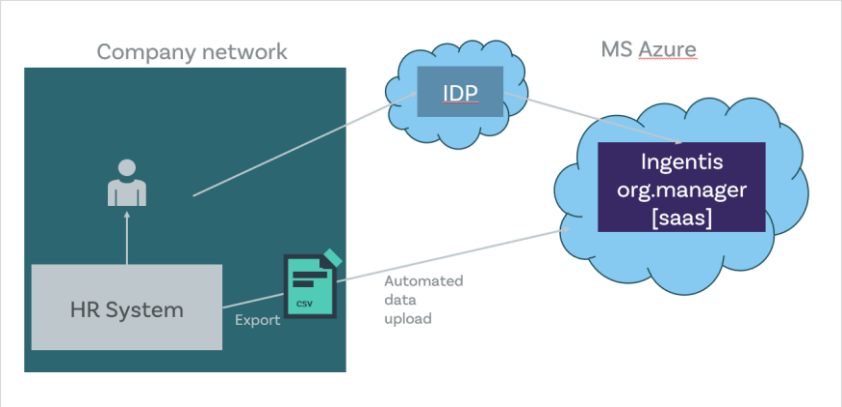
# Authentication

Authentication is required to access organizational charts. Ingentis org.manager [SaaS] supports authentication via SAML 2.0, OAuth, and OpenID Connect. All login attempts to org.charts are forwarded to the customer's IdP, and only valid attempts are processed. Validation is implemented in the authentication protocols. Since authentication is handled via the customer's IdP, the access logs are under the control and responsibility of the customer.

The use of an authentication provider is mandatory, and only one provider can be configured. It is neither provided by Ingentis nor included in any edition of org.manager [SaaS].

# Authorization

Based on the authentication of the user who wants to open an organizational chart, it is possible to assign access permissions at the person or group level.




Ingentis org.manager [SaaS] with SSO via IDP.

# Data Encryption

## Encryption at rest

Each client stores data in a dedicated Azure Storage account. This account is transparently encrypted and decrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is comparable to BitLocker encryption in Windows. The data in a storage account is encrypted with keys managed by Microsoft.

## Encryption in transit

### HTTPS

Access to the tenant application is protected by the Azure Application Gateway with integrated Web Application Firewall. The external IP of the Azure Application Gateway is protected by the Azure DDoS Protection Service. Encryption is performed using SSL with TLS 1.2 (best practice cipher suites) and TLS 1.3 (depending on the client browser). This can be verified by accessing your own tenant. The protocol actually used depends on the browser configuration and is therefore the responsibility of the customer.

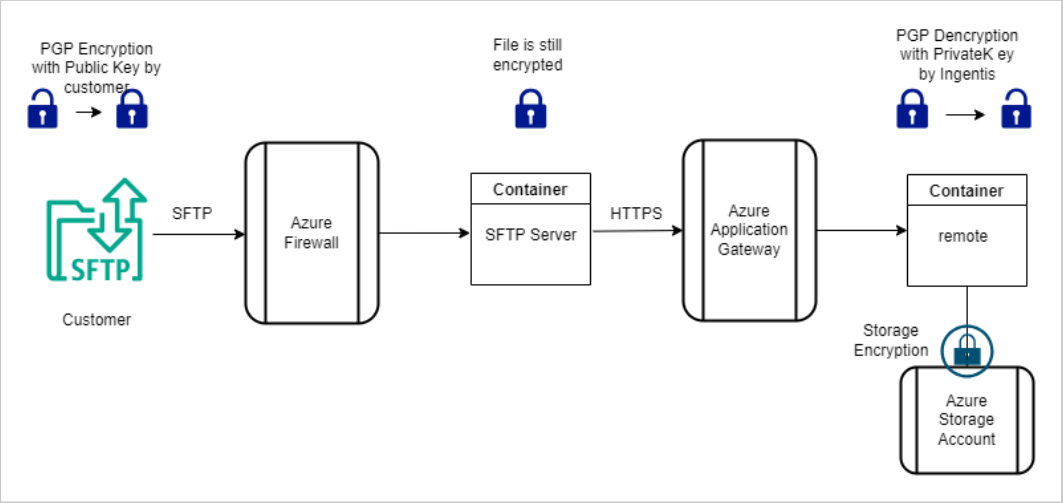
### SFTP

SFTP file uploads and outgoing data access within the tenant application are protected by the Azure firewall with integrated intrusion detection and prevention system (IDPS). The external IP of the Azure Application Gateway is protected by the Azure DDoS Protection Service.

## PGP file encryption (optional)

File encryption can supplement standard transport encryption but is optional.

- Two certificates are used. PGP is used for file encryption and SFTP/SSH for transmission encryption.
- For PGP encryption, Ingentis provides the customer with a public key via FTAPI.
- The key size can be 1024, 2018, 3072, or 4096; the decision is up to the customer.
- PGP encryption can be optionally activated for each file directory.
- For SFTP/SSH encryption, the customer must provide Ingentis with a public key.
- Stored private keys are protected by passphrases.




File transfer architecture with PGP encryption.

## Location of data

Microsoft Azure offers many locations around the world, but not all required services are available at these locations. The data centers used for Ingentis org.manager [SaaS] are ISO 27001 and SOC 2 & 3 compliant. In addition, the European data center is GDPR compliant.

The following locations are currently available, and additional (geographic) locations may be supported if they meet the requirements:

- **Australia** (operated by Navigo Pty Ltd)
  Australia East (New South Wales)
- **Europe**
  Western Europe (Netherlands)
- **USA**
  East Coast (Virginia)
- **Canada**
  Toronto

## Segregation

Each tenant is physically separated from other tenants by being deployed in its own K8s namespace with its own containers (process isolation). There are no shared components. This ensures that each customer has its own application instance and that data processing is strictly separated.

At the network level, each tenant is separated by its own virtual network. At the domain level, each tenant has its own subdomain. The subdomain is resolved by the Azure Application Gateway and Firewall Service, which forwards requests to the appropriate tenant application instance.

At the data storage level, tenant and application data are stored in a separate Azure Storage account that is not shared with other tenants. Therefore, the data is physically separated between tenants.

## Security tests

The security of Ingentis org.manager [SaaS] is tested once a year by an external company. Any problems are immediately rectified by Ingentis. Customers can request a summary of the results of the last "pentest." Customers can test their own tenant with two weeks' advance notice.

## VII Monitoring

In order to maintain technical availability, the systems of Ingentis org.manager [SaaS] are monitored both internally and externally. On the one hand, the underlying systems, such as the servers, are monitored for sufficient resources, and on the other hand, the application is monitored for availability.

Ingentis offers a service status portal with up-to-date information on availability, detected failures, or service degradation and plans maintenance work:

https://status.orgmanager.com

## Logging

All logs, especially security logs, are transferred to and stored in the Azure Logs Analytics Workspace. They are protected against manual changes, even by the administrator.

## Backup

The backup is stored with Azure Storage encryption on a geo-redundant Azure storage for 30 days. This means that the backup storage location is outside the operational data center. Data at rest is encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. In addition to encryption at rest, all your backup data is transferred via HTTPS. It always remains within the Azure backbone network.

For information about which regions host backups, see: https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions.

Backups are used for disaster recovery only; individual restore actions are not supported.

## Disaster recovery

In the event of a disaster, it is possible to create a new, completely independent cluster at any time. All the standard components required for this are included in Microsoft Azure and are therefore always available. The application is divided into several container images and can be restored by Ingentis at any time. Customer data can then be restored from the existing backup to the new cluster. Logs are stored as files with the respective tenant in the logging system and are therefore included in the backup.

# Maintenance

A monthly maintenance window is provided for the application of updates, upgrades, new versions, and/or other changes and maintenance work. This window takes place two weeks after the 1st of each month on the following Monday. Updates are performed in a European data center between 6:00 p.m. and 10:00 p.m. CET. Updates for a North American data center are performed between 10:00 a.m. and 4:00 p.m. CET.

During this time window, the respective tenant will be unavailable for several minutes. As this is defined in the SLAs with the customer, the downtime does not count as technical availability and does not need to be announced separately.

The effective downtime during this time window averages approximately 60 minutes.

The planned maintenance can also be viewed and subscribed to via the status page of Ingentis org.manager [SaaS]:

https://status.orgmanager.com

# Portal integration

## Linking

The easiest way to integrate the organizational chart into the company intranet is to save a link to the output page of Ingentis org.manager [SaaS].

The URL for the organizational chart (e.g., https://<company>.orgmanager.com/orgmanager) is saved in the desired location on the intranet page (e.g., under the name "Company Organizational Chart").

## Selective entry point

An entry point for a specific object is possible via call parameters in the URL. It is important that the attribute used for the entry point is also activated in the detailed search.

The following URL would search for an organizational unit with the ObjectID 12345678:

https://<company>.orgmanager.com/orgmanager**?goto=OE|(ObjectID,10,12345678)**

Please note that the **technical name** (in the "Types" section of org.converter) must be used for both the object name (in this case: OrgUnit) and the attribute name (in this case: ObjectID).

The 10 means that the ObjectID must be "12345678".

This object selection method also works for position and employee objects. The following examples are based on the SAP configuration of org.converter:

https://<company>.orgmanager.com/orgmanager/index.**html?goto=Position|(PositionID,10,12345678)**

https://<company>.orgmanager.com/orgmanager/index.**html?goto=Person|(PersonnelNumber,10,12345678)**

The following comparison operators are available:

| Data type | Operator ID | Description |
|---|---|---|
| **All** | 10 | = |
| **All** | 11 | <> |
| **Digit** | 20 | < |
| **Paragraph** | 21 | <= |
| **Paragraph** | 22 | > |
| **Number** | 23 | >= |
| **Character string** | 30 | Contains |
| **String** | 31 | Does not contain |
| **Character string** | 32 | Begins with |
| **Character string** | 33 | Does not begin with |
| **Character string** | 34 | Ends with |
| **character string** | 35 | Does not end with |

## Selecting the perspective

In addition, the desired perspective can be selected by its name.

&perspective=Name of perspective

**Example**:
https://<company>.orgmanager.com/orgmanager/orgmanager**?goto=OE|(ObjectID,10,12345678)&perspective=Standard**

## Selecting the language

The language in which the organizational chart is displayed is selected either as a default in the configuration file or when the organizational chart is called up.

**Example**:
https://<company>.orgmanager.com/orgmanager/orgmanager**?lang=en**

To do this, the output language must be licensed in org.converter (the default languages are German and English) and the terms in the data source must also be maintained in this language.

## Number of levels

The number of hierarchy levels can also be specified at the entry point:

?<technical name of the view>_layer=<number of levels>

**Example**:
https://<company>.orgmanager.com/orgmanager*?Organigram_layer=3*

**Important**: The name of the view must be specified, as a view can contain multiple graphical structures (e.g., organizational chart and staffing plan in parallel).