Bringing Potential to Life

ingentis

# System Reference Guide

| | |
|---|---|
| Projekt: | **org.manager for SAP SuccessFactors** |
| Klassifizierung: | **PUBLIC** |
| Version: | **1.2** |
| Stand: | **15.01.2026** |

Ingentis Softwareentwicklung GmbH · Raudtener Str. 7 · 90475 Nürnberg / Germany · +49 (0) 911 98 97 59-0 · mail@ingentis.com · www.ingentis.de
Geschäftsführer: Joachim Rotzinger (CEO) · Tobias Weiß (COO)
USt-IdNr: DE186953155 · Steuer-Nr.: 241/129/31461 · Amtsgericht Nürnberg · HRB: 14491

# Contents

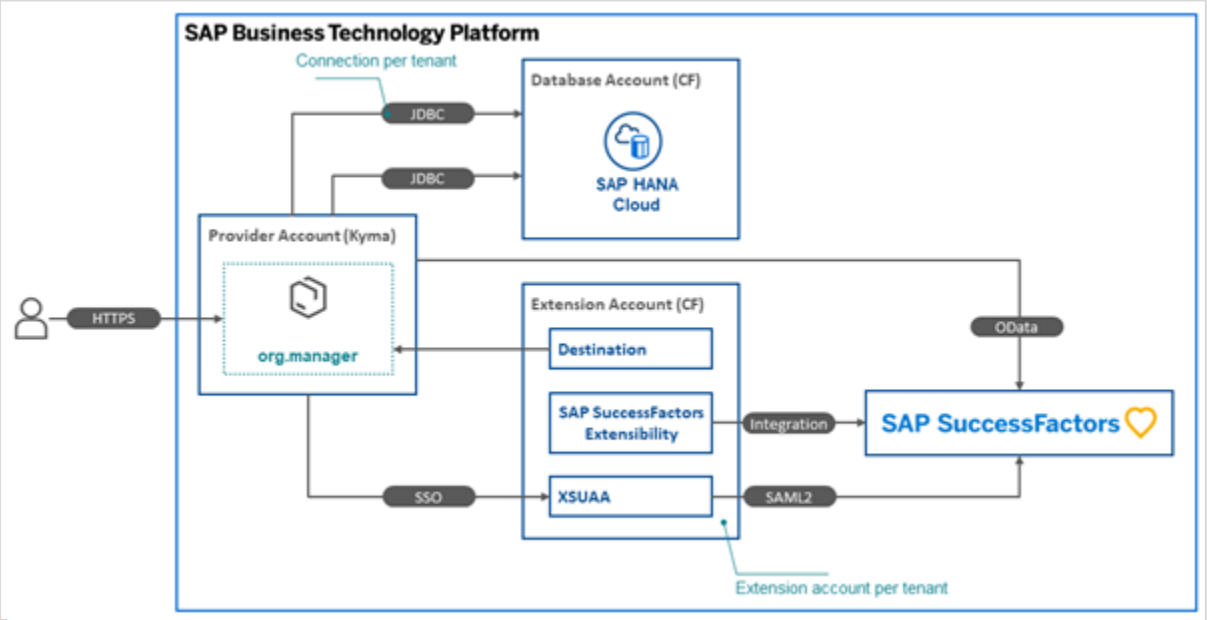
# Product Overview

Ingentis is a software company, specializing in the development of add-ons to leading HR systems such as SAP and SAP SuccessFactors. The flagship product is Ingentis org.manager, a tool that enables anybody to create and publish individual, data-rich organizational charts within minutes.

The software org.manager for SAP SuccessFactors is an extension to SAP SuccessFactors. Benefiting from over 25 years of experience in the segment of organizational charts, the solution is designed for the swift creation of custom organizational charts for SAP SuccessFactors. Ingentis org.manager for SAP SuccessFactors runs on SAP Business Technology Platform and is integrated in SAP SuccessFactors. The tool is certified by SAP as SAP SuccessFactors Extension build on SAP Business Technology Platform.

Ingentis org.manager for SAP SuccessFactors distinguishes from the built-in organizational charts of SAP SuccessFactors in terms of flexibility, design and the capability of displaying any hierarchy including any object maintained in SAP SuccessFactors. The configuration can easily be adapted to the customer's requirements.

# System Architecture




Ingentis org.manager for SAP SuccessFactors Architecture

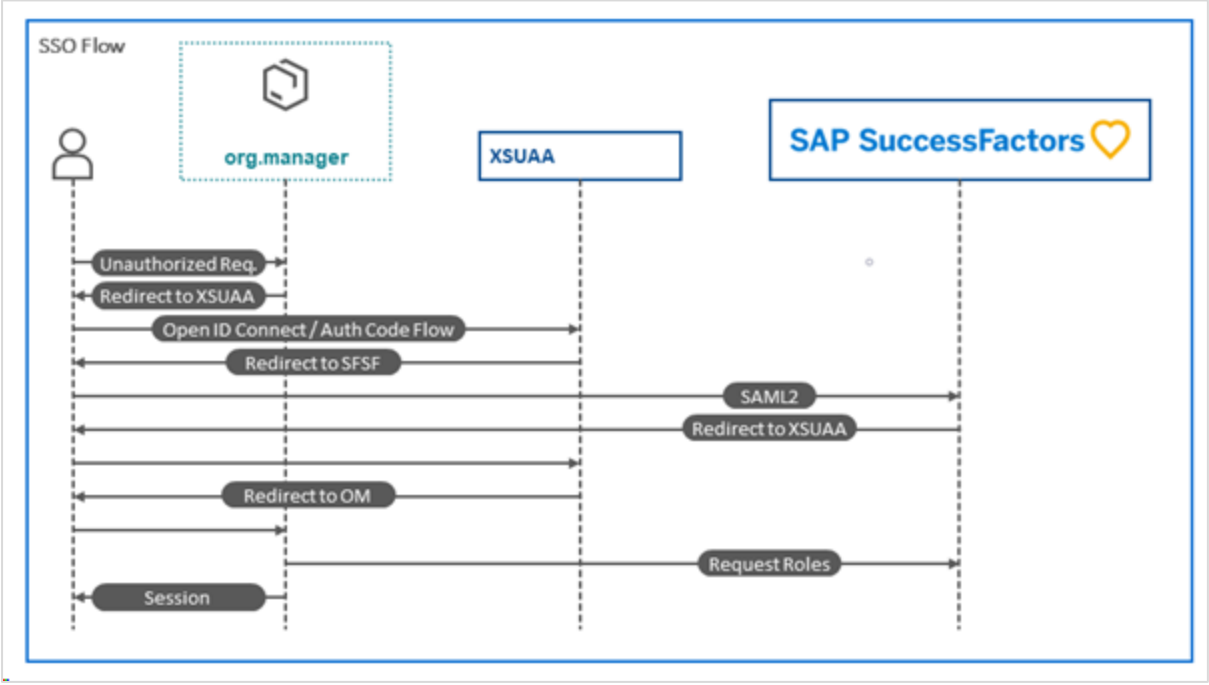
SAP Business Technology Platform (BTP). It is written in JAVA and hosted by Kyma runtime. In addition, several BTP Cloud Foundry (CF) services complement org.manager.

- **Provider Account:** The Kyma runtime is instantiated within the provider account. It is the overall runtime for all tenants.
- **Extension Account:** The extension account is used for integrating the customers SuccessFactors (SFSF) system with org.manager. Therefore, the SAP SuccessFactors Extensibility service is used to connect the SFSF system via an OData destination. The OData destination then is used to access the OData API of the connected SFSF system. For single sign on (SSO) purpose, the XSUAA service of the extension account is configured to perform SSO with the connected SFSF system via saml2. One extension account is created for every registered tenant.
- **Database Account:** An SAP HANA Cloud database is instantiated within the database account. A separate scheme, user and password is generated for every tenant, so that every tenant has its separate JDBC connection to the database. In addition, a main connection exists with a separate user and scheme, so non tenant specific information can be stored.

# Security

## User Security

org.manager is secured via SSO and requests roles from the SFSF system, so that no access to the application is possible without being authenticated against SFSF, and no data can be seen, or actions done, without being in the correct role. The SSO configuration is stored within a tenant specific extension account. When accessing org.manager configuration frontend, an automated redirect to the underlying identity provider (IDP) is done. After being correctly authenticated, the user roles are requested from SFSF, so the final permissions of the end user can be determined. The following diagram shows a short version of how SSO works with org.manager.




org.manager for SAP SuccessFactors - SSO Architecture

After being authenticated and authorized, the user and its permissions will be identified via a session. Sessions have an idle timeout of 30 minutes and exist for a maximum of 12 hours. After that, the user must authenticate again. When a user gets assigned new roles, a logout and login is required to take effect.

## Data Residency

org.manager and all used SAP technologies are hosted on the SAP Business technology platform. New tenants will be onboarded in the nearest environment to the underlying SFSF system.

## Data Access to SAP SuccessFactors

org.manager reads and writes data from and to SFSF via the integrated OData API. Communication is done via HTTPS. The credentials to access the OData API are generated by the SAP SuccessFactors Extensibility service within a tenant specific extension account within the global account where org.manager is hosted. The extensibility service creates an HTTP Destination using OAuth2SAMLBearerAssertion as authentication type. This destination will then be consumed by org.manager to access the connected SFSF system. To be able to access data within SFSF, a technical user must be created. This user may only need access to the fields that have to be read and written.

## Data Access to SAP HANA Cloud

org.manager has two types of connection to the database:

- **Global connection:** This connection accesses data, that are relevant for org.manager to work in general and accesses information like the existing tenants.
- **Tenant specific connection:** Every tenant has its own connection to access tenant specific data.

Every tenant connection and the global connection has its own credentials and accesses its own database schema. The credentials are stored as uniquely per tenant identifiable Kubernetes secret.

The connections are secured via TLS 1.2 and encrypted with the TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256 cipher suite.

org.manager does not implement any manual certificate or public/private key handling. All encryption mechanics are managed by the BTP.

## Data Encryption in SAP HANA Cloud

To protect data saved to disk from unauthorized access at operating system level, the SAP HANA Cloud, SAP HANA database uses native SAP HANA data encryption in the persistence layer. Data volume encryption protects the data area on disk, while redo log encryption protects the log area on disk.

The SAP HANA database holds the bulk of its data in memory for maximum performance, but it still uses persistent disk storage to provide a fallback in case of failure. During normal operation, data is automatically saved from memory to disk at regular savepoints. Additionally, all data changes are recorded in redo logs. A redo log entry is written to disk with each committed database transaction. If a fault occurs, the SAP HANA database can be restarted in the same way as any disk-based database and returns to its last consistent state by replaying the redo log entries from the last savepoint.

- **Data volume encryption:** All pages that reside in the data area on disk are encrypted using the AES-256-CBC algorithm. Pages are transparently decrypted as part of the load process into memory. Therefore, when pages reside in memory they are not encrypted and there is no performance overhead for in-memory page accesses. When changes to data are persisted to disk, the relevant pages are automatically encrypted as part of the write operation. Pages are encrypted and decrypted using 256-bit page encryption keys. Page keys are valid for a certain range of savepoints and can be changed by executing SQL statements. After data volume encryption has been enabled, an initial page key is automatically generated. Page keys are never readable in plain text, but are encrypted themselves using a dedicated data volume encryption root key, which is generated randomly during instance creation.
- **Redo log encryption:** Log entries are encrypted using the AES-256-CBC algorithm before they are written to disk. Log entries are encrypted and decrypted using a 256-bit long root key, which is generated randomly during instance creation.

# Monitoring and Logging

## Monitoring

To be able to maintain technical availability, the systems of org.manager for SAP SuccessFactors are monitored automatically by SAP as platform provider.

Additionally to the technical availability, Ingentis is monitoring the application for the following:

- CPU usage
- Memory usage
- Disk usage
- Network transfer rate
- Database availability
- Database memory/cpu usage
- Requests per minute to the application
- Users per minute
- Errors per minute
- Feature usage

The availability of the infrastructure can be checked at status.ingentis.com

## Logging

Application logs are securely stored within SAP BTP for 90 days. When the logs are generated, the internal system clock of SAP BTP is used. The logs are protected against manual modifications even by the administrator.

Following application events are being logged:

- Application errors
- Application starts/shutdowns
- HTTP access log

Configuration logs are securely stored till termination of the contract. When the logs are generated, the internal system clock of SAP BTP is used.

Following configuration events are being logged:

- Configuration changes
- Metadata refreshes
- Configuration replaced by another configuration
- License file changes
- Configuration resets
- Data in use resets
- Secret created/deleted (for SFTP)

All login attempts are redirected to the customer's SuccessFactors system and only valid attempts are processed by the application. The authentication is handled by customer's SuccessFactors system and thereby the access logs are in the responsibility of the customer.

**Attention**: System logs of the SAP BTP are not handled by Ingentis.

## User Management

All users are authenticated via the SuccessFactors system or another identity provider to the application. The creation of users, user changes, the deactivation of users and the definition and administration of roles and rights is thus done via the SuccessFactors system or at the customer's IdP.

**Attention**: A technical user account is required for the system to work properly, and a configuration user is recommended. You can find more information about these two special users in the Deployment chapter.

## Organizational & Administrative Security

### Information Security Policies

We maintain internal information security policies, including incident response plans, and regularly review and update them.

Our applications are developed and operated in house. All our staff is bound to the strict rules of §5, Bundesdatenschutzgesetz (German Data Protection Law).

## Information Security Management

We are bound by the EU General Data Protection Regulation and use the ISMS standard “ISIS 12”. An external data protection officer verifies our compliance.

## Training

We provide periodical security and technology use training for employees.

# Software Development Practices

## Coding Practices

Our engineers use best practices and industry-standard secure coding guidelines, which align with the OWASP Top 10.

# Data Center

## Data Center Locations

The Kyma runtime for org.manager is provided directly by SAP, with the option to have AZURE, AWS or GCP as the hosting hyperscaler. org.manager is currently hosted in the following Kyma regions:

| Region | Hyperscaler | Location | SAP Regional Name | SAP Regional Identifier | Hyperscaler Regional Name |
|---|---|---|---|---|---|
| **Europe** | Microsoft Azure | Amsterdam (Netherlands) | Europe (Netherlands) | eu-20 | West Europe |
| **USA (West)** | Microsoft Azure | Quincy (Washington) | US West (WA) | us-20 | West US 2 |
| **USA (East)** | Microsoft Azure | Virginia | US East (VA) | us-21 | East US 2 |
| **Canada** | Amazon Web Services | Montreal | Canada (Montreal) | ca-10 | ca-central-1 |
| **Australia** | Amazon Web Services | Sydney | Australia (Sydney) | ap-10 | ap-southeast-2 |
| **Kingdom of Saudi Arabia** | Google Cloud Platform | Dammam | KSA (Dammam) | sa-31 | me-central2 |

**Europe**

- IP address for Demo: 4.245.12.17
- IP addresses for Test: 20.224.27.157, 4.231.36.126, 108.143.216.65
- IP addresses for Production: 20.13.19.221, 51.124.187.119, 20.123.217.41

**USA (West)**

- IP addresses for Test: 20.9.144.243, 20.3.136.120, 20.80.160.196
- IP addresses for Production: 20.3.149.134, 172.179.240.134, 20.80.162.243

**USA (East)**

- IP address for Demo: 20.102.42.187
- IP addresses for Test: 20.163.173.82, 20.42.111.133, 20.55.28.99
- IP addresses for Production: 135.222.208.90, 172.191.171.149, 20.127.172.123

**Canada**

- IP addresses for Test: 15.223.104.146, 52.60.52.118, 15.156.137.134
- IP addresses for Production: 99.79.147.4, 15.222.218.40, 3.98.201.131

**Australia**

- IP addresses for Test: 52.62.41.199, 54.153.202.148, 13.236.220.23
- IP addresses for Production: 52.65.20.196, 52.64.42.76, 13.211.63.17

**Kingdom of Saudi Arabia**

- IP address for Test: 34.166.29.244
- IP address for Production: 34.166.148.137

### Data Center Certifications

org.manager only runs on SAP Business Technology Platform data centers. SAP ensures that the same or equivalent certificates are valid at every data center where cloud solutions are run:

- ISO 27001
- SOC 1 / SSAE 16
- SOC 2
- ISO 22301

Information provided without guarantee. For more detailed information have a look at the official compliance documentation of the data center in use.

### SAP Business Technology Platform Penetration Tests

SAP have the Penetration Testing by internal and external ethical hackers as part of the security standards. The Penetration Test report cannot be provided to customers since it contains sensitive information.

# Technical Information

## Browser

### Configuration Requirements

org.manager requires browsers to be configured with these attributes:

| | |
|---|---|
| Caching | We recommend allowing browser caching because we use it heavily for static content such as Image files, CSS files, and JavaScript files. If you clear your cache, the browser does not perform as well until the deleted files are downloaded again to the browser and cached for use next time. |
| HTTP/2 | Browser must support the HTTP/2 standard |
| Javascript | Javascript must be enabled |
| Cookies | Cookies must be enabled |

## Supported Browsers

The following browsers are supported:

- Microsoft Edge (Chromium Version)
- Mozilla Firefox
- Google Chrome

The legacy version of Microsoft Edge is not supported.

Google and Mozilla release continuous updates to their Chrome and Firefox browsers. We make every effort to fully test and support the latest versions as they are released. However, if defects appear with OEM-specific browser software, we cannot guarantee fixes in all cases.

## Proxies

If your browser accesses org.manager via a proxy, the proxy must support the same features as the browser:

- HTTP/2
- Cookies

A proxy must forward all headers to the application.

# Integration between SuccessFactors and SAP BTP

## OData API

org.manager automatically integrates with the OData API of SuccessFactors, via SAP BTP integration mechanism.

That means, the moment the application is deployed, the integration mechanism on SAP BTP automatically generates an **OAuth 2 Client Application** in SuccessFactors. You can find this OAuth client in SuccessFactors in the **Admin Center** under **Manage OAuth Client Applications**.

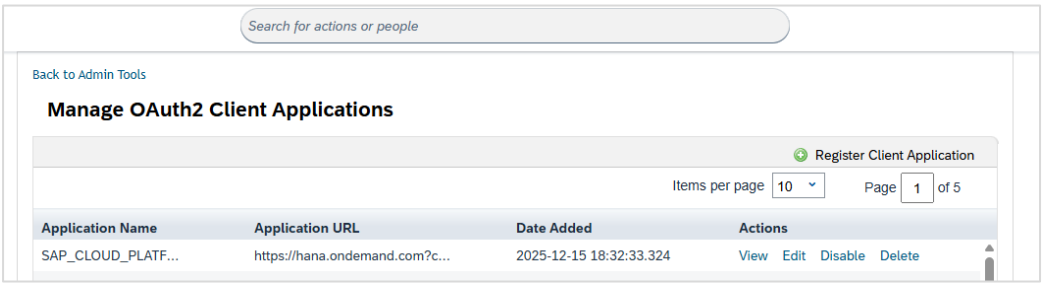
The integration follows the following naming convention:

- SAP_CLOUD_PLATFORM-SYSTEM-NAME-<YOUR_COMPANY_ID>-<TIMESTAMP_OF_CREATION>

Do not **Delete**, **Disable** or change the **Bind to Users**, **User IDs** or **X.509 Certificate** settings on this client application. This will break the integration between org.manager and SuccessFactors. Our application will lose access to the OData API, users will no longer be able to log in to our application, and we will no longer be able to load data from SuccessFactors.

The OAuth 2 Client Application contains a X.509 certificate which is limited to a specific time (typically 2 years). Our application automatically generates a new OAuth 2 Client application, via the BTP integration mechanism, once the certificate is going to expire. This is an automated process; there is no manual intervention needed here.

**Do not generate new certificates by yourself! This will break the integration between our application and SuccessFactors!**



# Status

The website **https://status.ingentis.com/** is available to all customers. Here we inform about upcoming maintenance, but also about unplanned downtimes, and the current status of the clusters is always visible.

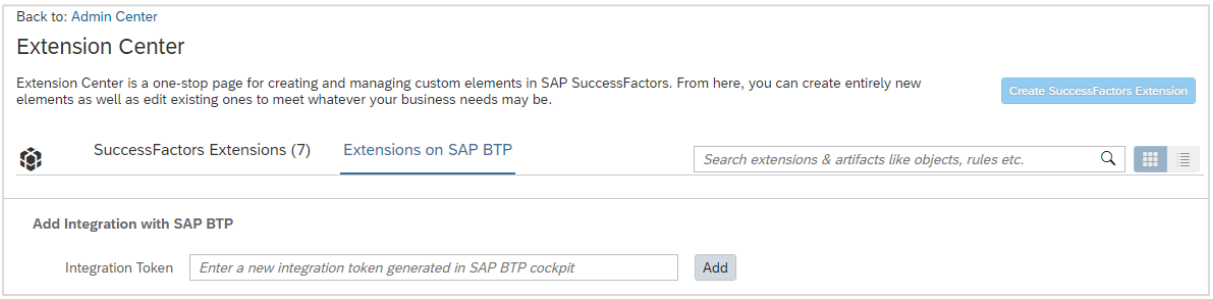
# Deployment

## Activate Integration Token in SFSF

The following steps must be done for all SAP SuccessFactors instances to integrate (test, production, etc.):

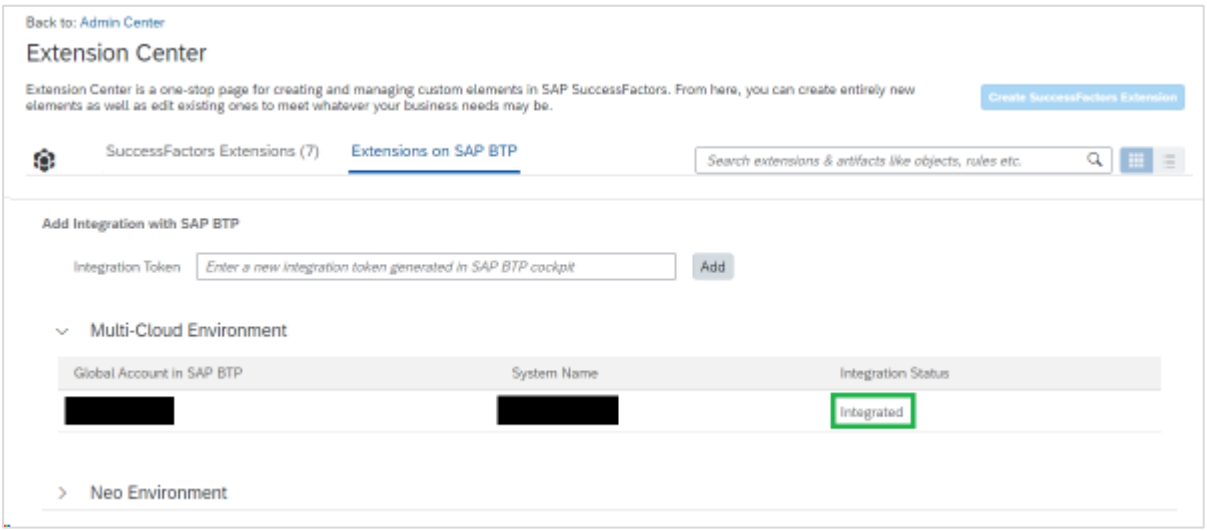
After logging into the SAP SuccessFactors, go to action “Extension Center” and select the tab “Extensions on SAP BTP”.

Under “Add Integration with SAP BTP” enter the integration token provided by Ingentis and click on “Add”.




SAP SuccessFactors - Extension Center

Wait until the linked sub account appears as “Integrated”




Integrated Token in SFSF.

## Technical User

A technical user is required to access the OData API to read and write data. Therefore, no login to the SFSF admin panel is required. The technical user needs read and write access to all objects and fields that should be surveilled and written to. The following permissions are required so that the org.manager can run correctly:

| Required Permissions (via Manage Permission Roles) | |
|---|---|
| **Manage Integration Tools** | **OData API To-Do External Categories Import**<br>(Required to create notifications within SFSF, e.g., when a user was invited to a simulation.) |
| **Manage System Properties** | **Picklist Management and Picklists Mappings SetUp**<br>(This permission is required to show possible picklist values) |
| **Metadata Framework** | **Access to non-secured objects**<br>(This permission is required to show possible picklist values)<br><br>**Admin access to MDF OData API**<br>(This permission is required to make use of the snapshot pagination parameter. Without that parameter, invalid data may be caught from SFSF on large data sets) |

## Configuration User

A configuration user is recommended to setup org.manager and to see and verify the output. It can also help to find errors appearing on SFSF side. Login into the SFSF admin panel is required. The following permissions are recommended:

| Recommended Permissions (via Manage Permission Roles) | |
|---|---|
| **Manage Integration Tools** | **Access to OData API Audit Log**<br>(Recommended for diagnosing faulty calls to the OData API.)<br><br>**Access to OData API Metadata Refresh and Export**<br>(Recommended for executing a metadata refresh and exporting the metadata from SFSF.)<br><br>**Access to OData API Data Dictionary**<br>(Recommended to be able to see the object definitions exposed by the OData API.) |
| **Metadata Framework (Employee Central only)** | **Configure Object Definitions**<br>(Recommended to be able to see the object definitions.)<br><br>**Access to non-secured objects**<br>(Recommended to be able to see the picklist definitions.) |

## Create and Assign Users to Appropriate Roles

org.manager can handle different users with different roles and can assign the roles to different permissions of org.manager. To be able to access org.manager, create and send us at least one role name that will be authorized to access org.manager. For compatibility reasons to the configuration of the legacy NEO version, the default role name to access org.manager is 'Ingentis-org.manager'.

## Final Deployment Requirements Checklist

Please ensure that the following tasks have been accomplished:

□ One integration token for each SFSF system was activated
□ One technical user for each SFSF system is available
□ The technical user has sufficient permissions
□ A role was created and assigned to the authorized users

Please provide Ingentis the following information for every relevant SFSF system:

- The user ID of the technical user. It is important that we get the user ID and not the login name or username, because the technical user is used to authenticate against the OData API via an OAuth2 flow, that only works with the user ID.
- The login URL to the SFSF system

**Only if you have checked all the Ingentis is able to start deploying and configuring the application.**