Bringing Potential to Life

ingentis

System Reference Guide

Project:	**Business Rule Trigger**
Classification:	**PUBLIC**
Version:	**1.3**
As of:	**13.01.2026**

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

Table of Contents

Introduction

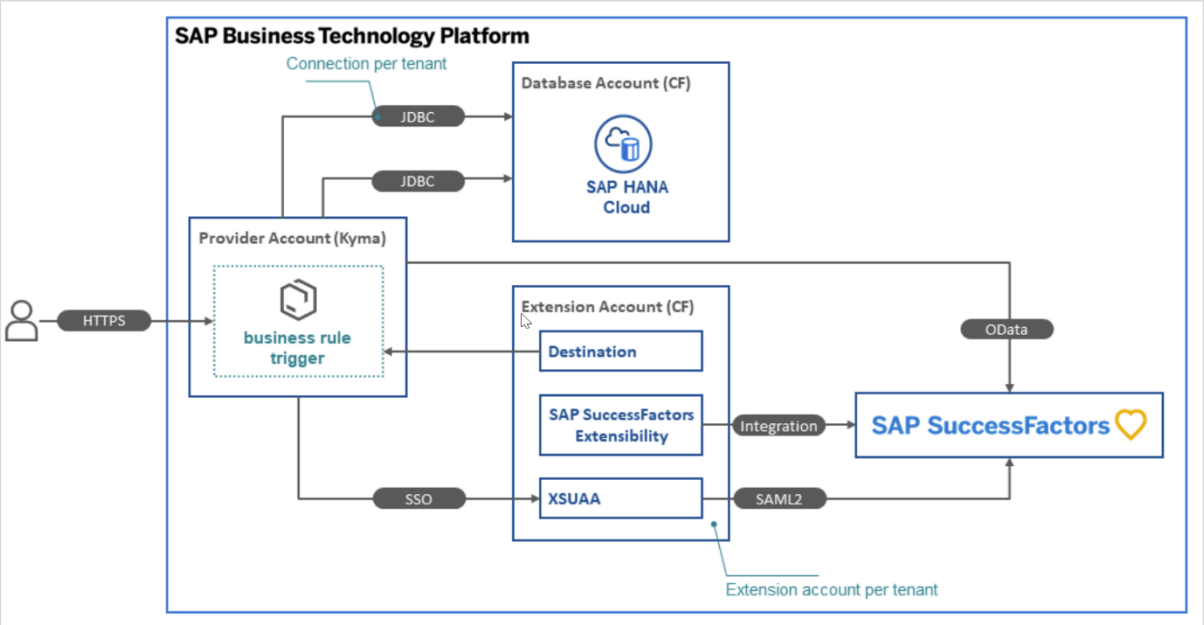
About Business Rule Trigger

Business Rule Trigger is an automatism that monitors changes made to data objects in SuccessFactors and stores dependent objects in SuccessFactors from the modified objects via an evaluation pathway, which results in these dependent objects, the business rules are triggered. In SuccessFactors itself, it is not possible to trigger business rules on any object if attribute Y has changed to object X.

Example

A popular example is the inheritance of the name of a BusinessUnit to a department: The customer would like to set the new business unit name when saving the name of the BusinessUnit at all departments hanging below. To do this, he has created a business rule at the Department, which automatically writes the name of the corresponding business unit to a specific attribute at the Department. The problem, however, is that this business rule only runs when the department is saved, but not when the BusinessUnit is saved. In other words, the current situation is that the customer has to manually press Save at all departments if the name of the business unit has changed to execute the business rule at the department, which automatically sets the name of the business unit at the department. Our Business Rule Trigger tool automates this annoying work

System Architecture



Business Rule Trigger - System Architecture

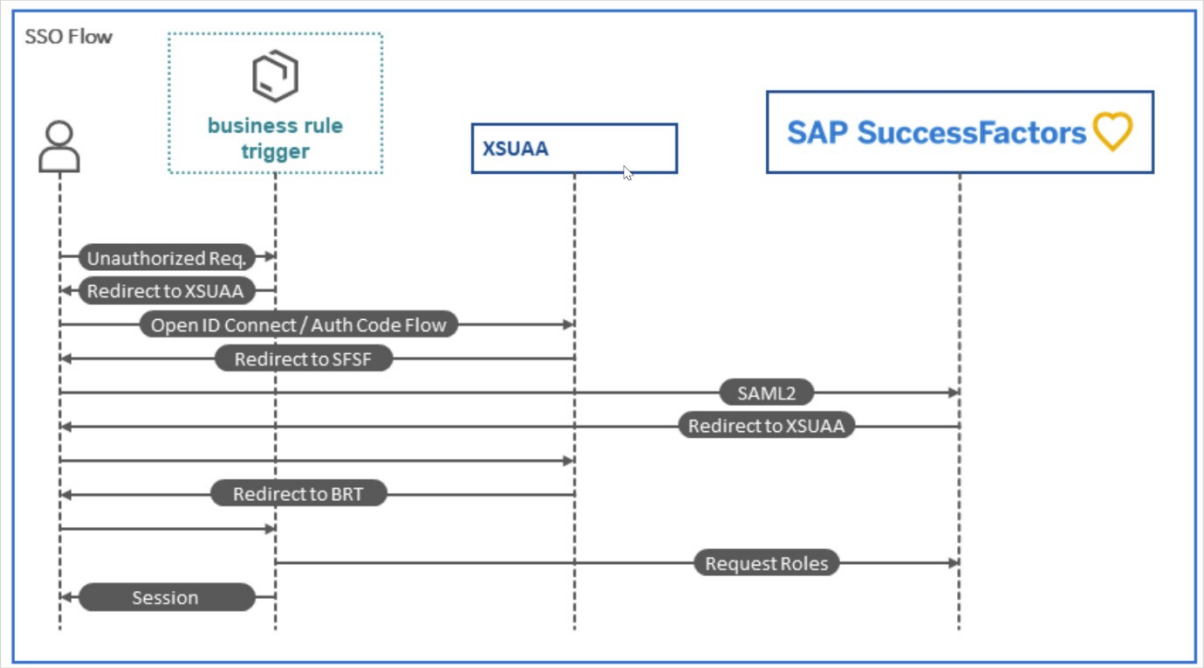
Ingentis business rule trigger (BRT) is a multi-tenant application, running on the SAP Business Technology Platform (BTP). It is written in JAVA and hosted by Kyma runtime. In addition, several BTP Cloud Foundry (CF) services complement BRT.

- 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 BRT. 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

BRT 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 the BRT 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 the BRT.



Business Rule Trigger - 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

BRT 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 SuccessFactors-System. BRT will not store sensitive information and will only work with object IDs and date values.

Data Access to SAP SuccessFactors

BRT 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 the BRT is hosted. The extensibility service creates an HTTP Destination, with OAuth2SAMLBearerAssertion as authentication type. This destination will then be consumed by the BRT to access the connected SFSF system. To be able to access the 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

BRT has two types of connection to the database:

- Global connection: This connection accesses data that are relevant for BRT 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 TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256 cipher suite.

BRT 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, 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 save points. 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 since the last save point.

- **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 have 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 save points 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.

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 the BRT is provided directly by SAP, with the option to have AZURE, AWS or GCP as the hosting hyperscaler. BRT 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

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

BRT 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 has 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

BRT 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 BRT 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

Business Rule Trigger 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**.

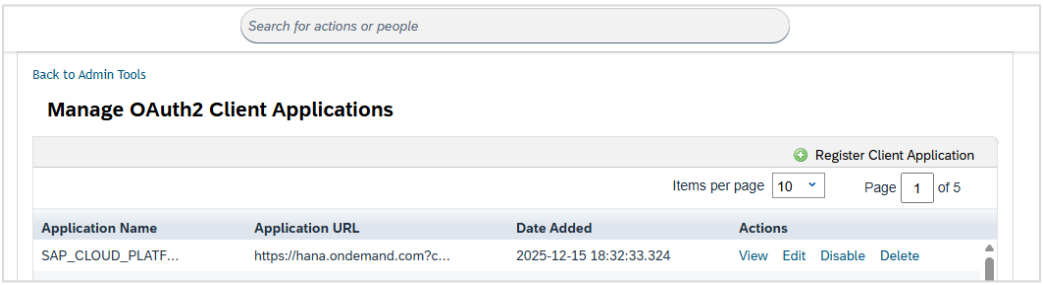
The integration follows the following naming convention:

- 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 Business Rule Trigger 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

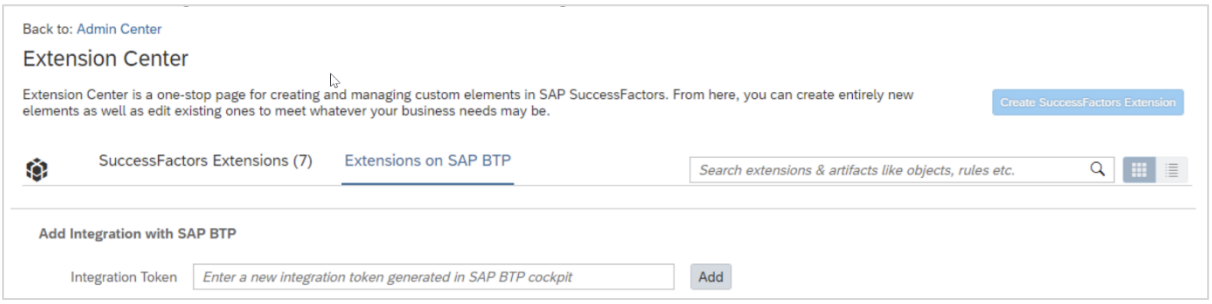
The website **https://status.ingentis.com/** is available to all customers. Here we inform about upcoming maintenance, but also about unplanned downtimes, and the current status of the clusters is always visible.

Deployment

Activate Integration Token in SuccessFactors

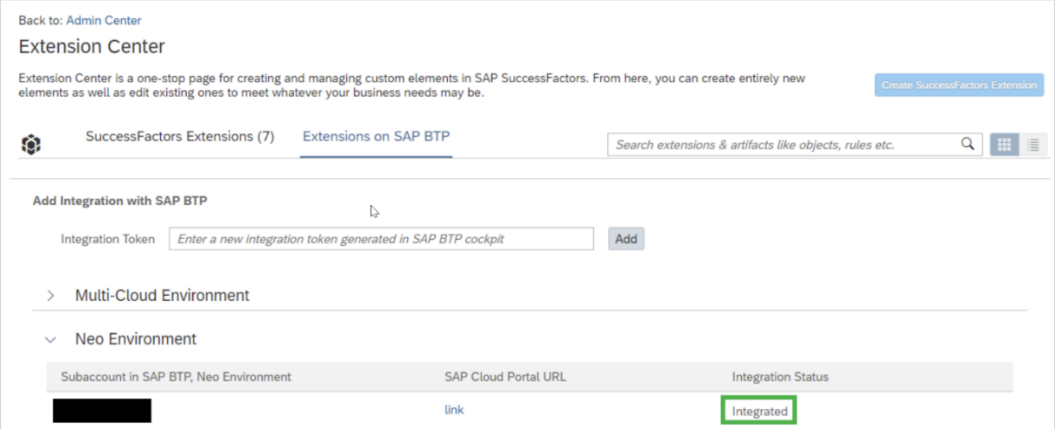
The following steps must be taken for all SAP SuccessFactors instances to integrate (test, production, etc.):

- 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 and click on “Add”.



SAP SuccessFactors – Extension Center.

Wait until the linked sub account appears as “Integrated”.



SAP SuccessFactors - Extension Center after integration.

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 BRT can run correctly:

Required Permissions (via Manage Permission Roles)	
Manage System Properties	Picklist Management and Picklists Mappings Set Up (This permission is required to show possible picklist values)

Required Permissions (via Manage Permission Roles)	
Metadata Framework	Access to non-secured objects (This permission is required to show possible picklist values) Admin access to MDF OData API (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

Create and Assign Users to Appropriate Roles

BRT can handle different users with different roles and can assign the roles to different permissions of the BRT. To be able to access BRT, create and send us at least one role name that should be authorized for access.

Final Deployment Requirements Checklist

Please ensure that the following tasks have been accomplished:

□ One integration token for each SuccessFactors system was activated
□ One technical user for each SuccessFactors 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 SuccessFactors 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 SuccessFactors system

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