UNIT4
In business for people

Unit4 Source to Contract

Service Description

VERSION 1.1

October 2023

CONTENTS

1. Introduction

Unit4 Source-to-contract (S2C) is a Software as a Service solution designed for people centric organizations. It provides a fully integrated data model, processing model and reporting model, enabling our customers to manage their key business areas.

The Unit4 Source-to-contract solution consists of core service and additional services such as Unit4 People Platform services, Feature services and more. The purpose of this service description is to describe Source-to-contract core service. Details about additional services can be found in the documents published on our website (www.unit4.com/terms).

Unit4 provides a complete technically managed solution for Unit4 Source-to-contract deployed in the public cloud. This end-to-end service includes infrastructure, hardware, system software, monitoring, management and maintenance, disaster recovery and service updates.

The Unit4 Source-to-contract solution is hosted with Amazon Web Services, which provides state-of-the-art technologies for flexible and secure hosting.

The hosting provider is ISO27001:2013, 27017:2015 and 27018:2014 certified and audited on a bi-yearly basis, following the SOC 2 standard. The latest certificates and audit reports can be provided upon request. AWS data centres are built to the highest standards with fully redundant power supply and cooling as well as strict access controls being in place to ensure a very secure environment. In summary, Unit4 provides the following:

- Access to Unit4 Source-to-contract over secure internet connections (HTTPS). Supported by a variety of browsers and mobile platforms.
- Comprehensive integration options can be provided using the Unit4 Extension Kit.
- Fully scalable solution, in a high availability environment with redundancy.
- Relevant security level.
- Ongoing surveillance, feeding alerts, and continuous development.
- Application of updates.
- Production environments with a single shared database multi-tenant for customer data.
- Service Level Agreement, with service credits based on service availability.
- Unit4 Community (Community4U) to engage with Unit4 directly, giving insight in the Roadmap.

2. Data centres & data residency

The Unit4 Source-to-contract solution is built upon Amazon Web Services. The Unit4 Source-to-contract service is delivered from within different geopolitical zones, using a primary and a secondary location in every zone to meet service level commitments and disaster recovery needs. The location within each geopolitical zone is at the discretion of Unit4 and can change from time to time. The table below contains details of the geopolitical zones, along with the data centre locations. For more information, see AWS region details:

Geopolitical zone	Provider	Data Location (Countries/City's/Regions)	Time Zone
EU	AWS	Dublin/ Ireland	CET/CEST
Asia	AWS	Singapore	SGT
Australia	AWS	Sydney, Australia	AEDT/AEST
EU	GCP	Holland	CET/CEST

Amazon Simple Cloud Storage Service (AWS S3) is used for file storage and files are contained within the same region as their respective environments.

GCP is used for Spend Analytics, Project Analytics, eSourcing Analytics, Contract Analytics and Supplier Analytics.

AWS is used for Project Management, eSourcing events, Contract management and Supply Base Management.

Unless agreed otherwise in an Order Form the chosen deployment of the customer will be as follows:

Customer residence	Geopolitical zone used
APAC	Asia
Australia/New Zealand	Australia
Canada	EU
EU	EU
Norway/ Denmark	EU
UK	EU
US	EU
Spend and Analytics is only hosted from EU geopolitical zone	

3. Service model

Unit4 Source-to-contract is a multi-tenant solution embedded in a cloud native / service-based platform. Unit4 Source-to-contract characteristics are as shown in the table below:

Category	Component	Characteristics
SOLUTION	Releases and updates	These will be applied automatically and periodically
	Environments included	Production
	Non-transactional storage (e.g., documents)	250GB[3]
	Transactional storage (e.g., database)	15 GB + 100 MB per each purchased FTE[4]
	Availability guarantee	Yes
SERVICES	Releases will start	Automatically
	Updates will start	Automatically
	On-going technical operations, performance management, maintenance of all infrastructure components, monitoring alert response and issue resolution	Yes
	Disaster Recovery	Yes
	Monitoring program of infrastructure and application	Yes
COMPLIANCE	Compliance certificates and assurance documents – Unit4	ISO27001

[3] Additional non-transactional storage can be requested by the customer and is going to be a subject of extra charge.

[4] Additional transactional storage can be requested by the customer and is going to be a subject of extra charge.

Category	Component	Characteristics
	Compliance certificates and assurance documents – Amazon Web Services Google Cloud Platform	ISO27001 ISO27017 ISO27018 SOC1 + SOC2 Type II

4. Environments

Only the Unit4 Source-to-contract Production Environment (PE) is subject to the Service Level Agreement.

Unit4 assigns to every cloud customer a unique Cloud Customer ID code, which is visible in various elements of the service (e.g. service now) and it is used for customer identification. The Customers ID code is a 3-character acronym. The Cloud Customer ID codes are created at Unit4 discretion during the early stage of the implementation and are not a subject to change.

4.1 People Platform services and Feature services

Unit4 People Platform services and Feature services are delivered with Unit4 Source-to-contract or as an option to support integration between S2C and UNIT4 ERP.

4.2 Production Environments

Backups

The Recovery Time Objective (RTO): Duration of time within which data must be restored.
The Recovery Point Objective (RPO): Maximum acceptable amount of data loss measured in time.

Server Backup	**VM Image Backup: Daily** **RTO: 1 day** **RPO: 12 hours**
SQL Database Backup	Full: Weekly Transactional Logs: Every 15 minutes RTO: 15 minutes RPO: 12 hours
AWS S3 File Storage	Real-time replication of all stored files

Backups are used for disaster recovery purposes. "Forgiveness" restores is not offered.

5. Reporting and monitoring

5.1 Reporting on service performance

Unit4 provides operational information regarding the Unit4 Source-to-contract on Unit4 Community4U. That information includes:

- Scheduled maintenance (times, dates per region).
- Release information.

5.2 Monitoring program

A continuous 24x7 monitoring and resolution program is in place to detect and resolve incidents to meet service availability metrics.

The utilization of Amazon CloudWatch and Unit4's internal alerting system provides us with the ability to monitor and respond to outages or degradation of the service in a timely manner.

During day-to-day operations single pane of glass dashboards, alerting mechanism and staff rotation practices enable Unit4 to stay on top of all service events that need intervention.

6. Releases and updates

Unit4 releases changes through a series of quarterly releases and ongoing updates.

Releases

Releases will be scheduled approximately 4 times per year (frequency to be increased or decreased at Unit4's discretion) to introduce new features, enhancements and solve lower priority deficiencies. Unit4 will use reasonable endeavours to ensure that releases will be carried out during the Planned Maintenance window.

A schedule of planned changes to the production environment will be published per geopolitical zone on Unit4 Community4U .

Updates

Updates will be applied on an ongoing basis to cater for bug fixes and off-cycle enhancements to maintain the existing features, as well as maintaining service level, security commitments and updates/revisions to its integration interfaces and user experience. Updates will be deployed to production environment.

7. Planned and Unplanned maintenance

7.1 Planned Maintenance

Planned Maintenance windows are dedicated to apply all the respective changes to the service provided e.g. solution updates, releases and infrastructure changes. During Planned Maintenance, production service may be periodically unavailable. You can find more details on schedule presented in the table below:

	Planned Maintenance windows (PMW) *Updates, releases and Infrastructure*
Feature Releases *All regions*	**Regular PMW:** From Sunday 19:00 to 23:00 CET One weekly planned maintenance window. *Utilized if necessary, quarterly release schedule.*
OS Patching *All regions*	**Regular PMW :** From Sunday 02:00 to 04:00 CET One weekly planned maintenance window. *Utilized if necessary, monthly patching schedule.*

*Time of Planned Maintenance window is a subject of a change (+/- 1h), which is related to winter and summer time adjustments.

Planned Maintenance windows are subject to change upon reasonable notice. The exact dates of Planned Maintenance windows are communicated in Unit4 Community4U. By default, all Planned Maintenance windows are regular and take up to 6h, unless they are promoted to extended Planned Maintenance windows, these take up to 12h.

Actual downtime for planned or scheduled maintenance that lasts longer than the allocated period is taken into account when determining the length of a service outage. If actual

downtime for scheduled or Planned Maintenance is less than time allotted for Planned Maintenance, that time is not applied as a credit to offset any service outage time for the month.

Planned Maintenance can also be carried out by Unit4 provided that the customer has received at least 8 hours' notice. This will occur in unforeseen or exceptional circumstances only (similar to emergency or unplanned preventative maintenance) to deal with a vital or critical issue and Unit4 will use its reasonable endeavours to do this outside business hours to cause minimal disruption to the customer. In this case, because Unit4 provides customer 8 hours' notice, this maintenance does not count as service outage. This is so that Unit4 is not encouraged to wait until the next Planned Maintenance window to deal with an urgent issue and avoid a service credit.

7.2 Unplanned Preventative Maintenance

Unit4 may carry out unplanned preventative maintenance if there is an urgent requirement to secure the stability or the security of the Unit4 SaaS. This action may be taken at the discretion of Unit4 for unforeseen and exceptional circumstances, which require immediate resolution that cannot wait until the next Planned Maintenance window. Unplanned preventative maintenance is counted as a service outage.

8. Customer permissions and responsibilities

8.1 Customer permissions

Customer has the right to:

1) Monitor PE availability and service response time on an active basis using a third-party monitoring service. Monitoring acts as a consumer of the Unit4 SaaS and is subject to all present and future usage restrictions of the Unit4 SaaS. Customer and Unit4 must agree, prior to monitoring, on monitoring details to ensure that the monitoring does not interfere with the Unit4 SaaS offering and that Unit4 SaaS security tooling does not block the monitoring service.

2) Unit4 provides a security penetration test on an annual basis, carried out by qualified third party. Customers are not allowed to perform penetration testing on the production environment. Customers may coordinate one yearly penetration test with Unit4, at the customer's expense. Details of the planned test must be provided to Unit4 at least 30 days in advance of each test, using a Service Request.

Any activities to prepare, coordinate or manage the above by Unit4 is subject to additional charges.

8.2 Customer responsibilities

Releases

Any releases may result in additional configuration and/or functional adjustments that are required to be made by either: (i) the customer; (ii) Unit4; or (iii) approved service partner consultants, which are not included in the service and would be chargeable.

The following list summarizes typical release tasks and indicates services included as part of the Unit4 Source-to-contract service and tasks that are the responsibility of the customer (or by Unit4 Professional Services at an extra charge):

Task	UNIT4 Responsibility	Customer Responsibility
Project Planning		
• Publishing general availability schedule of Releases on Unit4 Community4U	✓	
• Managing timelines, outline goals, roles and responsibilities		✓
• Business analysis and discovery		✓
• Creating test plans		✓
Release deployment in production environment		
• Apply release to production environment	✓	
• User awareness sessions in connection with major functionality releases	✓	
• Implementation and configuration for new features		✓
• Maintaining and testing of all integrations, extensions and customer configured screens, processes, reports, etc.		✓

Unless agreed otherwise, the customer responsibilities include configuration, and adjusting any Extension Kit flows, APIs in use and connected systems.

Technical and functional responsibilities

Technical environment responsibilities:

- Supply, administration, and maintenance of customer-side client devices.
- Customer-side networking infrastructure, including connectivity to the internet.
- Security of customer-side network, devices, and internet connectivity; and
- Ensuring sufficient bandwidth, including internet bandwidth.
- All customer initiated activities in penetration testing, security checks, Customer owned monitoring are in the sole responsibility of the Customer.

Functional environment responsibilities:

- Customer is fully responsible for the configuration and administration of the functional aspects of the service, including user and role administration after the initial implementation project has been signed-off.

Account setup

Customer is responsible for designating its users, The initial users will be created during the implementation project. The Customer is hereafter responsible for creating all future users and for ensuring that all users are adequately trained use obligations and requirement to comply with Unit4's Acceptable Use policy (www.unit4.com/terms). Customers are responsible for managing their accounts and disabling a users' accounts when Unit4 Source-to-contract access is no longer required, including immediately upon termination of that user's affiliation with customer. Customer is responsible for its users' acts and omissions and for all activities occurring under its users' accounts.

Account administrator

Customer will designate one or more Account Administrator's .The Account Administrator's responsibilities include, but are not limited to, coordinating with Unit4 regarding Unit4 Source-to-contract and managing customer's accounts. The customer guarantees that its Account Administrator(s) will maintain authority to act on customer's behalf concerning the Unit4 Source-to-contract service, and that Unit4 can rely on the Account Administrator's actions and instructions in connection therewith.

Account security

Each user is responsible for keeping their account credentials confidential. Users may not share account credentials, and customer may not recycle account credentials when activating or disabling accounts. Customer will notify Unit4 immediately upon discovering any known or suspected unauthorized access to, misuse of, or breach of security for the Unit4 SaaS or its users' accounts and will provide all information and take all steps requested by Unit4.

9. Configuration, extensions and integrations

Unit4 Source-to-contract gives customers great flexibility in adjusting the standard core application by Configuration to meet the needs of any specific customer requirements. In addition, there is the possibility to integrate with other applications.

9.1 Solution's flexibility

Any non-standard configuration (e.g., Integration), creation of custom reports, custom fields, imports, exports, can be performed by Unit4, Unit4 partners or the customer. Unless categorized as a product defect by Unit4, these are considered outside the scope of the standard service. Therefore, the maintenance, support, implementation, considerations for such components are not included in the Unit4 SaaS fees (unless agreed otherwise in an Order Form). Assistance may be sought from Unit4's Professional Services teams at Unit4's prevailing rates.

All configurations must be carried out based on lean principles, to ensure ongoing performance and resilience of the service.

9.2 Integrations

Integrations are permitted according to the supported integration methods described below:

Integration Type	Permitted?
Integration using Unit4 Source-to-contract API package	✓

Integrations created by methods mentioned above, are not supported by Unit4 under Standard Support terms, unless agreed otherwise. The customer has sole responsibility for any integrations, as well as their maintenance and Unit4 has no responsibility to maintain compatibility or fix any problems resulting from its use. This is applicable to any Integrations including Unit4 Integrations delivered as part of a Project implementation. Unit4 may be able to assist with resolving issues or with upgrades of the Integrations, but this will be a subject to review and extra charge. Customer will be required to purchase Professional Services at Unit4's prevailing rates.

10. Technical operations

10.1 Printing

All printing will be carried out on the client side.

10.2 Connectivity

Access to the Source to Contract Web Application is delivered over the public internet using an HTTPS connection (RSA 2048 bits - SHA256 with RSA and/or EC 256 bits SHA256 with ECDSA).

10.3 Solution access

The Unit4 Source-to-contract solution can be accessed via:

- A supported web browser.
- Programmatic access to API.

10.4 Predefined users

Unit4 reserves the right to create one predefined user in order to manage the implementation process, to make initial configurations to the platform during the implementation process, to provide the best possible support, and to update configurations on customers request.

Customers are not allowed to introduce any changes to predefined users settings without Unit4's written consent.

10.5 Authentication

Authentication for Unit4 Source-to-contract is carried out using a federated authentication. Management of users and passwords within the Unit4 Source-to-contract application is the responsibility of the customer.

Federated authentication allows customers' users to use their organizational credentials (e.g., domain username and password) when logging in to an Unit4 application. With federated authentication, the customer's authentication provider (e.g., ADFS, Azure Active Directory, etc.) performs authentication instead of an application-specific username and password that is validated by the Unit4 application.

The customer is responsible for configuration of their identity provider (IdP) and to provide specific information (required or requested) to Unit4 that allows for configuration.

10.6 Technical overview

Topic	Description
Email	
Domain	Unit4 provides basic e-mail functionality for sending messages to recipients with default S2C domain.

Topic	Description
Protocol	SMTP over TLS
Authentication	
Protocols supported	Web-based login with username and password as well as SSO following the SAML2 standard.
Internet communication	
Protocols supported	HTTPS (browsers supporting TLS >1.2 are required) secured with RSA 2048 bit keys and SHA256withRSA encryption and/or EC SHA256 with ECDSA .

11 Data considerations

11.1 Transfers of customer data to the Unit4 Source-to-contract

Unit4 deploys a standard architecture and therefore, where customer is an existing Unit4 customer, the customer is responsible for ensuring data consistency (i.e. that customer data to be inserted follows such standard architecture) and that any inconsistencies in customer data are appropriately cleansed before such data is inputted into the Unit4 SaaS.

11.2 Data backup

Transactional data is backed up with retention of 30 days. Non-transactional data (e.g., documents) are kept in encrypted storage account and in production environment transactional and non-transactional data are replicated to a segregated account. There is no "forgiveness" restore option available. Access to the backups is limited to the Global Cloud Operations engineers in case of disaster or malfunctioning of hardware/software. Backups are done with frequency to support RPO on level of <1 hour.

11.3 Data security

Data in transit

Customer data in transit over public networks is protected with TLS 1.2 (HTTPS).

Customer data at rest

All files and data media are encrypted at rest following current industry standards. (Currently AES).

11.4 Limits and regulators on usage

Unit4 runs in a multi-tenant environment and, as such, Unit4 observes fair use limits so that runaway processes do not monopolize resources.

To ensure the provision of a quality of Service to all our customers and to ensure that the behaviour of some does not disadvantage most of our customers, we have implemented several hard and soft limits in the application. In some cases, the application will warn users that their actions might impact performance - Unit4 reserves the right to intervene if such warnings are ignored and usage result in impact to server performance.

Detailed information describing how the fair usage policy applies to the Service including relevant hard limits and soft limits to ensure optimal performance is available in the User manuals.

11.5 Time to live

Transactional data, document storage and logfiles will be stored as long as the customer is willing to store data and has an active service agreement.

11.6 Access to my data

The customer's data is owned and controlled by the customer and in accordance with applicable law, customer shall be the data controller. Unit4 is the data processor.

To ensure the customer has access to their customer data, the following options are available:

- Application functionality (e.g. Source-to-contract web application).
- APIs.
- Upon agreement termination, customer data can be retrieved by the customer in accordance with the agreement.

12 Documentation and technical services

All Source-to-contract documentation made available (including Release notes) is published in English language only. Technical services being the support of the infrastructure or technical deployment of SaaS, are also provided in English.

Glossary and technical acronyms

Unless defined in the tables below, capitalised words and phrases have the meaning given to them in Unit4's General Terms of Business or Unit4 Support Terms (found on www.unit4.com/terms).

Glossary

Term	Definition
Account administrator	An appropriate and qualified business user who will have administrative level control for creation, maintenance, and deletion of accounts providing access to the Unit4 product also known as super user.
Cloud Customer ID code	A unique Cloud Customer identifier.
Source-to-contract service user	Database user used for communication between Microservices.
Source-to-contract *web application*	The main web application portal for Unit4 Source-to-contract solution.
Feature service	Features or solutions delivered as independently deployed and updated services.
IDP	An identity provider (IDP) is a service that stores and manages digital identities.
IDS system user	Database user used for an early access enablement.
Instance	Physical service infrastructure and software running on it, deployed in a specific region.
Integration	Inbound or outbound data exchange built and managed with Integration Kit.
Localisation services	Localisations delivered as Feature services, developed for our key strategic territories and verticals, securing legal, statutory and market standard requirements.
Multi-tenant	Architectural design of Unit4 Source-to-contract solution, housing multiple tenants, where tenants are physically integrated, but logically separated.

Term	Definition
Record	A data record stored within a customer's database (for example a line in a timesheet).
Transaction	The creation or modification of a Record.

Technical Acronyms

Acronym	Full Name
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
API	Application Program Interface (e.g., Web Services)
AWS	*Amazon Web Services*
ERP	Enterprise Resource Planning
FTE	Full Time Equivalent
GCP	*Google Cloud Platform*
HTTPS	Hypertext Transfer Protocol Secure
IDP	Identity Provider
Kbps	Kilobits Per Second
PE	Production Environment
SHA-2 RSA	Secure Hash Algorithm (number 2) and RSA encryption Algorithm
SLA	Service Level Agreement
SOC	Service Organization Controls
TDE	Transparent Data Encryption
TLS	Transport Layer Security Encryption
URL	Uniform Resource Locator (a web address)
WIP	Work In Progress