Unit4 Financials by Coda

Cloud Service Description

VERSION 2026Q1

March 2026

Content

1. Introduction 2
2. Data centres & data residency 3
3. Service Model 6
4. Environments 7
5. Reporting and monitoring 10
6. Releases 10
7 Planned and Unplanned maintenance 11
8 Customer permissions and responsibilities 13
9 Localisations 17
10 Customisations, Integrations and Flexi Fields 18
11. Technical operations 22
12. Data considerations 24
SCHEDULE A Localisations by country 27
SCHEDULE B Unit4 Financials by Coda Tailored Solution 30
SCHEDULE C Other optional services 31
SCHEDULE D Glossary and Technical Acronyms 32
Notable Changes from V. 2025.2.1 33

1. Introduction

Unit4 Financials by Coda (U4FbC) SaaS delivers superior efficiency, consistency and accuracy to help your organization thrive amid the digital revolution. With business models transforming, new regulations emerging and change coming faster than ever, U4FbC helps you handle the most complex challenges with confidence.

U4FbC SaaS provides the original unified-ledger, global accounting system that gives your organization a single, real-time version of the truth. Embrace the best-of-breed financial solution that integrates with your existing systems for total freedom of choice and ongoing business agility.

The purpose of this U4FbC Service Description is to describe and detail the SaaS Service provided to the Customer.

Unit4 provides a complete technically managed solution for U4FbC SaaS deployed in the public cloud. This end-to-end Service includes infrastructure, hardware, system software, monitoring, management and maintenance of the entire solution (including backups), disaster recovery and service updates.

Unit4 offers cloud enterprise solutions as Unit4 SaaS - a Software as a Service delivery model deployed on Microsoft Azure. This model leverages Microsoft Azure's scale and experience of running highly secure and compliant cloud services around the globe. U4FbC operates efficiently within this framework, utilizing a shared model to optimize resource allocation.

In summary, Unit4 provides the following:

Access to U4FbC Web Client and API/web services.
All User access to U4FbC SaaS is over secure internet connections (HTTPS). A variety of browsers and mobile platforms are supported.
Comprehensive integration options available, including the use of Unit4 APIs and web services, batch file-based interfacing and optionally direct read-only access to a replicated production database.
Infrastructure is fully scalable, in a high availability environment with redundancy in critical aspects such as power, hardware and network communications.
Relevant security level.
Continuous monitoring is in place, covering servers, services and applications which is feeding alerts and continuous improvement.
Application of infrastructure updates, patches, and hotfixes.

Unit4 software and supporting software updates will be released four times a year. Optionally, there is a Maintenance Release if needed.

Production Environment and Non-Production Environments with a separate database for each Customer's data.

Disaster recovery in a physically separate secondary site.

Service Level Agreement, with Service Credits based on service availability.

- Unit4 Community (Community4U) to engage with Unit4 directly, giving insight into the service performance indicators and see the status of services.

Various Azure regions leveraged to enable Unit4 to meet Customers' data residency needs; Customers' data always resides within a specified geopolitical zone (except where explicitly stated otherwise).

Formal policies in place for information security, data processing, disaster recovery, and business continuity.

This document should be read in conjunction with the *Unit4 Cloud Technical Guidelines and Limits* document, available at www.unit4.com/service-descriptions under *Technical Documents*. This companion resource outlines detailed technical parameters, supported protocols, integration limits and service thresholds that apply to Unit4 Financials by Coda.

2. Data centres & data residency

Unit4 uses the Microsoft Azure infrastructure and platform Services, to deliver the U4FbC SaaS. These Services are delivered from within different geopolitical zones, using a primary and a secondary location in every zone to meet KPIs 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 Azure region details: www.azure.microsoft.com/regions.

Geopolitical zone	Provider	Data location (Countries/City's/Regions)	Time zone
EU	Microsoft Azure	Dublin, Ireland and Amsterdam (DR), Netherlands	CET/CEST
USA	Microsoft Azure	Texas and Illinois (DR)	CST/CDT

Geopolitical zone	Provider	Data location (Countries/City's/Regions)	Time zone
Canada	Microsoft Azure	Quebec City and Toronto (DR)	EST/EDT
United Kingdom	Microsoft Azure	London and Cardiff (DR)	GMT/BST
Asia	Microsoft Azure	Singapore and Hong Kong (DR)	SGT
Australia	Microsoft Azure	Victoria and New South Wales (DR)	AEDT/AEST
Norway	Microsoft Azure	Oslo and Stavanger (DR)	CET/CEST
Sweden	Microsoft Azure	Gävle and Staffanstorp (DR)	CET/CEST

Unless agreed otherwise in a Sales Order, the chosen deployment of the Customer will be as follows:

Customer residence	Geopolitical zone used
APAC	Asia
Australia/New Zealand	Australia
Canada	Canada
EU	EU
Sweden[1]	Sweden
Norway/ Denmark	Norway
UK	UK

[1] Platform Services will be delivered from Azure Norway data centre.

Customer residence	Geopolitical zone used
US	US

Primary	Secondary
Geopolitical zone EU	Geopolitical zone EU
Geopolitical zone UK	Geopolitical zone UK
Geopolitical zone USA	Geopolitical zone USA
Geopolitical zone Canada	Geopolitical zone Canada
Geopolitical zone Asia	Geopolitical zone Asia
Geopolitical zone Australia	Geopolitical zone Australia
Geopolitical zone Sweden	Geopolitical zone EU
Geopolitical zone Norway	Geopolitical zone EU

3. Service Model

Category	Component	Comments
SOLUTION	Environments included	1 Production + 2 Non-Production (Preview and Acceptance)
	All patching, updates of the standard solution (technical)	Included and automatic
INFRA-STRUC-TURE	Data Files storage	250GB[2]
	Transactional data storage	250GB[3]
	Availability guarantee	Yes
	Data centres	Microsoft Azure
	Updates will commence	Automatically
	On-going technical operations, performance management, maintenance of all infrastructure components, monitoring alert response and issue resolution	Yes
	Backup & Service Restore	Yes
	Disaster recovery	Yes
	Monitoring program of infrastructure and application	Yes

[2] Additional Data Files Storage is provisioned when needed and is subject to an extra charge. Operationally the system will not be halted when overage occurs.
[3] Additional Transactional Data Storage is provisioned when needed and is subject to an extra charge. Operationally the system will not be halted when overage occurs.

Category	Component	Comments
COMPLIANCE	Compliance certificates and assurance documents – Microsoft Azure	SOC1 Type II (ISAE 3402), SOC2 type II (ISAE 3000), ISO27001, ISO27017[4]

4. Environments

Three (3) environments are provided, including:

- **One Production Environmen**t (PE) - this is the environment that the Customer uses to run the day-to-day (live) operations,
- **Two Non-Production Environments (NPEs):**

  Preview – A Customer's Preview environment always contains the latest updates for the Unit4 Product in use by the Customer.

  Acceptance – It can be used according to Customer needs as “Test” /”Quality” /”Development” / ”Pre-Production”.

Additional Non-Production Environments are available for an additional charge.

Unit4 assigns to every Cloud Customer a unique Cloud Customer ID code, which is visible in various elements of the service (including environments) and is used for Customer identification. The MS Azure Customers ID code is a 3-character code. The Cloud Customer ID codes are created at Unit4's discretion during the early stage of the implementation and are not subject to change.

Platform Services

Unit4 Platform Services are multi-tenant, shared services. Except where explicitly stated in the service’s Service Description document, each Unit4 Platform Service has a Preview instance and a Production instance; there is no concept of Customer-specific instances of Unit4 Platform Services. As such, no additional instances of Unit4 Platform Services are provided. For more information, please refer to Unit4 Platform Services Service Description.

[4] It is Customers responsibility to ensure their own compliance with all applicable standards and compliance obligations. For more details around Information Security please see the Unit4 Information Security Policy, which is available at www.unit4.com/terms

4.1 Production Environments

Only the Production Environment (PE) is subject to the Service Level Agreement. Production environment backups are kept for 30 days to meet RPO.

4.2 Non-Production environments characteristics

While a Non-Production Environment (NPE) is not covered by the SLA or Disaster Recovery, it has the following characteristics:

Workload in NPE

NPEs support testing and user acceptance testing (UAT) activities with limited concurrent User activity, and data processing volumes that are expected to be approximately 5% of the Production Environment workload. They are intentionally sized and configured differently from Production Environments and are not designed to support production-like workloads, sustained high traffic, or business-critical operations. If volumes exceed those indicated the Customer will experience delays when running full loads in the Production Environment.

Customer responsibilities

The Customer needs to manage non-production WIP such as non-production report templates (e.g., in progress changes to purchase order report template) as refresh will replace WIP with copies from production.

What happens to the previous NPE details after a refresh?

Everything in NPE will be erased and replaced with a fresh copy from source environment.

Update of an NPE to a new update

The Preview environment is updated as soon as an update is available following a Unit4 announcement. Once an environment has been updated to the latest update, it is not possible to move back to the previous one.

Backups

Backups of NPE are made daily in the time zone of the geopolitical zone in use. Backups of NPE are kept for fourteen (14) calendar days.

Suspension

A NPE that is not actively used will be suspended. Suspended NPE may be reactivated at any point in time. To reactivate a suspended NPE, Customer needs to initiate re-activation, by accessing the environment through the web interface, which may take up to 15 minutes.

4.3 Database refresh

Definition of database refresh between environments

A database refresh between environments (e.g. from PE to NPE) is a full copy of the Customer database between the environments.

The scope of a standard database refresh is limited to the database content only. Activities outside this scope, including handling of data stored outside the database or additional related tasks, are not included in the standard service. Database refreshes are requested via a Service Request in Unit4 Community4U.

Customers are entitled to up to 12 database refreshes per environment in each calendar year. These are considered jointly, regardless of the source or target environment. For example, a Customer with three environments (e.g., PROD, PREV, ACCT) is entitled to a total of 36 refreshes per year. A Customer with four environments would have 48 refreshes per year.

Point in time used for refresh

A database refresh is performed using a restore from the most recent available backup of the source database. By default, this is the latest nightly backup, typically taken around 22:00 (local time) on the preceding day.

Requests for a **non-default point in time** for a database refresh are outside the scope of the standard service and may be subject to additional charges.

Frequency of database refresh

One refresh per environment per month is included.[7] Additional database refreshes are available at an additional charge.

Different environment update versions

Database refresh is possible when:

- Both environments are on the same update version or
- Target environment is on a higher update version.

How to request a refresh?

Customers can use self-service to request a refresh.

Refresh of the data stored outside of the database must be requested via the Service Request.

5. Reporting and monitoring

5.1 Reporting on Service performance

Unit4 provides operational information regarding the Unit4 SaaS on the Unit4 Community4U. That information includes:

- Service availability
- Scheduled maintenance (times, dates per region)
- Software update information and deployment schedules
- Incidents overview
- Site recovery status (in the event of the disaster plan initiation)

5.2 Monitoring program

A continuous 24x7 monitoring and resolution program is in place to detect and resolve incidents to meet the Unit4 Service Availability targets on Production Environment.

6. Releases

Unit4 will apply Releases, to make new features, functionality and updates available, also to maintain the existing features of the Service, KPIs and security. Releases will be provided free of charge as part of the Service. However, it should be noted:

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 U4FbC SaaS and will be a subject to additional charges. Where any Release replaces or updates any Customisation or non-standard functionality utilised by Customer, the Customer will be required to adopt the standard functionality. Unit4 reserves the right to invoice the Customer a reasonable charge to provide assistance if Customer wishes to maintain the previous Customisation or non-standard functionality.

6.1 Release deployment

Releases are applied approximately four times per year. The frequency of Releases may be increased or decreased at Unit4's discretion. Releases may take up to twelve (12) hours to deploy, resulting in the Service being unavailable for some or all that time (such unavailability shall not be counted as Service downtime for the calculation of Service Availability). Non-

production Environments are updated first, following a Unit4 Release announcement and according to the Release schedule.

A Customer's Preview environment always contains the latest Updates for the Unit4 SaaS solution in use by the Customer. The Production Environment will follow no sooner than 4 weeks after Preview deployment.

Unit4 will use reasonable endeavours to ensure that Production Releases will be applied during the Planned Maintenance window. Application of Releases cannot be deferred.[5]

7 Planned and Unplanned maintenance

7.1 Planned maintenance

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

	Standard Planned Maintenance windows (PMW) *Hotfixes, Localizations/Add-ons updates and Infrastructure*	**Additional Planned Maintenance windows (PMW)** *Release*
All regions (Except Azure US, Azure Canada.	Twelve per year, 3rd, or 4th week of each month From: Sat 4 PM To: Sun 4 AM UTC	Four per year according to time interval specific to a given region. *(Unless communicated otherwise)*
Regions Azure US and Azure Canada	Twelve per year, 3rd, or 4th week of each month **Shortened PMW** From: Sun 4 AM To: Sun 11 AM UTC Or **Full PMW***:	

[5] Release deployment details for Platform Services can be found in Unit4 Platform Services Description at www.unit4.com/service-descriptions.

	From: Sat 11 PM To: Sun 11 AM UTC **In rare cases when a downtime of all regions would be required*	

The time of a Planned Maintenance window is subject to change (+/- 1hr). This change is related to winter and summertime adjustments.

Planned Maintenance windows are subject to change upon reasonable notice. The exact dates of Planned Maintenance windows are communicated in Unit4 Community4U.

If actual downtime for scheduled or planned maintenance exceeds the time allotted for Planned Maintenance, it is considered part of the calculation for 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 / 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 a Service Outage. Unit4 needs to have the possibility to handle 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 U4FbC 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.

7.3 Service Notifications and Customer Communication

Unit4 communicates planned and unplanned activities through two channels: email notifications and Community4U.

Planned activities (such as Planned Maintenance Windows or Releases) are always published in advance on Community4U. Unit4 also issues email notifications to support visibility.

Planned patches are communicated by email and published on Community4U. Email remains the primary method due to shorter lead times, with the information consistently reflected on Community4U.

Unplanned Service Outages are communicated via email and Community4U. During global Service Outages, components responsible for email delivery may be affected. If the Service is unavailable, Customers should check Community4U first—any active incident will be posted there.

Email and Community4U are treated as equally valid communication channels. Customers should maintain up-to-date contacts in the system and regularly refer to Community4U for the latest status. Unit4 aims to deliver all messages by email as well; however, if email delivery is disrupted, Community4U remains the definitive source.

8 Customer permissions and responsibilities

8.1 Customer permissions

The Customer has the right to:

1. **Monitoring**

Track the availability of the Production Environment and monitor service responsiveness using an external monitoring tool. Such monitoring will consume Unit4 SaaS resources within the limits of current and future Usage constraints. Both Unit4 and the Customer must agree in advance on the details of the monitoring setup, to ensure it does not interfere with Unit4 SaaS operations or trigger security protections.

2. **Security Testing**

Perform external vulnerability scanning and penetration testing of their environments once per year. The Customer must submit a Service Request with full details of the planned activity at least 30 days in advance. Unit4 reserves the right to adjust the scope of such testing to protect the stability and integrity of shared infrastructure. Even if the activity is approved, Unit4 may suspend or terminate it without notice if it causes or risks causing disruption to the Customer or the stability or integrity of shared infrastructure. The Customer is solely responsible and liable for any resulting impact on the Service or recovery effort (which includes all efforts taken by Unit4 to restore the Service to a stable, secure and operational state).

3. **Performance Testing**

Carry out performance testing in the Production Environment, provided that the simulated load reflects typical Production Environment Usage patterns and is executed at the corresponding time of day (e.g. night jobs during nighttime hours). The Customer is not permitted to conduct testing designed to evaluate system behaviour under overload.

4. **Other Potentially Disruptive Activities**

Notify Unit4 in advance of any activity that may impact the behaviour, performance, or stability of Unit4 SaaS services. Unit4 may suspend or isolate affected systems—without prior notice—if an activity, whether authorized or not, is deemed to pose a risk to operational continuity or infrastructure health. Any investigation, mitigation, or remediation effort undertaken by Unit4 may be charged to the Customer.

Any effort by Unit4 to prepare for, coordinate, or manage the above activities is subject to additional charges, which can be immediately invoiced by Unit4 to the Customer.

8.2 Customer Responsibilities

Service releases

The following list summarizes typical update tasks and indicates services included as part of the Unit4 SaaS and tasks that are the responsibility of the Customer (or by utilising Unit4 Success Services for an extra charge):

Task	Included	Customer Responsibility
Project Planning		
• Publishing general availability schedule of Releases on the Unit4 Community4U	✓	
• Managing timelines, outline goals, roles and responsibilities		✓
• Business analysis and discovery		✓
• Creating test plans		✓

Task	Included	Customer Responsibility
Release deployment in Preview environment		
• Update Preview environment with Release	✓	
• User training on changes		✓
• Test: conducting basic Release testing		✓
• Training support to assist with testing		✓
• Functional and User acceptance testing as desired		✓
• Training, implementation and configuration for new features		✓
• Uplift and testing of all Customisations		✓
• Reviewing test scripts and testing outcome for issues resolution		✓
• Go/No-go criteria and agreement on Production Release deployment timing		✓
Release deployment in Production		
• Update existing application Configuration, being all activities undertaken to set up application provided by the Service which involve the use of standard menus and functionality. There may be rare cases where it is not technically possible to determine the correct business Configuration; in these rare cases any tasks that must be completed manually are the responsibility of the Customer.	✓	✓
• Update Production Environment with Release	✓	✓

Customisation update responsibilities

Unless agreed otherwise, Customer responsibilities include Customisation code lift and testing for compatibility, functional testing and any application (re)Configuration.

Unless agreed otherwise, any Customisations that are not updated to run on the current Release (n) in time for the production Release deployment will be disabled in the Production Environment prior to Release deployment.

Technical & Functional Responsibilities

The Customer's technical environment responsibilities include the supply, administration and maintenance of Customer-side devices and local printers.
Customer-side networking infrastructure, including connectivity to the internet.
Security of Customer-side network, devices and internet connectivity.
Ensuring sufficient bandwidth, including internet bandwidth.
All Customer initiated activities around penetration testing, security checks, Customer owned monitoring are in the sole responsibility of the Customer.
The Customer's functional environment responsibilities include:

- Customer is fully responsible for the Configuration and administration of the functional aspects of the Service, including User and role administration.

8.3 Customers Obligation

Account set-up

The Customer is responsible for designating its Users, and for ensuring that all Users are adequately trained and understand Customer's remote access and use obligations and requirements. Where applicable, each User must establish an Account. The Customer is responsible for managing its Accounts and disabling a User's Account when Unit4 SaaS access is no longer required, including immediately upon termination of such User's affiliation with the Customer. The Customer is responsible for its Users' acts and omissions and all activities occurring under its Users' Accounts.

Account Administrator

The Customer will designate one or more Account Administrator(s). The Account Administrator(s) responsibilities include, but are not limited to, coordinating with Unit4 regarding the Unit4 SaaS, and managing Customer's Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer's behalf concerning the

Unit4 SaaS, 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 the Customer may not reuse or recycle credentials when activating or disabling Accounts. The Customer will notify Unit4 without undue delay upon becoming aware of any known or suspected unauthorized access, misuse, or security breach affecting the Unit4 SaaS or any User Account and will provide all relevant information and take all reasonable steps requested by Unit4 to investigate and remediate the issue.

All Accounts used to access Unit4 Services and related applications must be secured in accordance with industry-standard security practices. At a minimum, password credentials must meet the following requirements:

- Minimum length of eight (8) characters
- Use of upper- and lower-case letters
- Inclusion of numbers
- Inclusion of special characters
- Credentials must be unique and not shared between Users

The Customer is responsible for enforcing appropriate password management practices, including timely access removal and credential changes where required.

8.4 General functional and technical requirements and specifications

Customer must comply with the functional and technical requirements and specifications, shared by Unit4 and available on **https://www.unit4.com/service-descriptions** and Community4U, which may be updated in accordance with the Unit4 General Terms of Business.

9 Localisations

The Service includes Localisations developed for our key strategic territories and verticals, securing legal, statutory and market standard requirements. Customer ordered Localisations will be made available to the Customer in the next available maintenance window. The

Localisations available depend on the Customer's home country and the version of U4FbC product. An overview of all available Localisations can be found in Schedule A.

10 Customisations, Integrations and Flexi Fields

Customisations and integrations are permitted and can be written by Unit4, Unit4 partners or the Customer. Maintenance, support, implementation, and update considerations for these custom components are not included in the SaaS Charges. Customisations are not supported by Unit4 under Standard Support. The Customer has sole responsibility for the Customisations and integrations, as well as their maintenance and Unit4 has no responsibility to maintain compatibility or fix any problems resulting from the use of non-standard software. This includes any custom development or Customisation (including Unit4 delivered Customisation as part of a project implementation, bespoke code written by Unit4). If any assistance is required regarding Customisations and/or bespoke work, Unit4 may be able to assist with resolving issues or with upgrades of the Customisation, but this will be subject to review and extra charges. The Customer will be required to purchase Success Services at Unit4's Prevailing Rates. Any Customisation can connect to the U4FbC Service using U4FbC APIs, but they require Customer or third-party vendor hosting, implementation, support and maintenance.

Note: U4FbC Integration Tool Kit (ITK) has been deprecated, the ITK processes are classed as customisations and therefore maintenance, support, implementation and update considerations for these processes are not included in the SaaS Charges.

New ITK processes are not permitted. Existing ITK processes must be reviewed and approved.

10.1 Unit4 created Customisations

Maintenance of Unit4 authored or created Customisations, including custom entities, fields, relationships, screens, reports, imports, exports, workflows, interaction plans, lookup data, localisation files, C# / Java /etc. code, database views, web styles and scripts, are outside the scope of Unit4 SaaS offerings. Maintenance, support, implementation and update considerations for these components are not included in the SaaS Charges.

10.2 Restrictions in Customisations

In general, there are restrictions regarding allowing Customisations in U4FbC SaaS including but not limited to:

No third-party applications, dll, jar and/or war files can be installed.
Unit4 provides the capability to bring custom SQL database objects from on-premises environments into Unit4 SaaS for continued operation of Customer-specific customizations. However, custom SQL database objects must comply with strict security, performance, and operational guidelines to be accepted.
Custom SQL database objects can be a security risk and may inadvertently lead to data leaks. Therefore, Customers must accept the risk of running their custom SQL database objects in Unit4 SaaS. Custom SQL database objects that do not meet security and performance requirements will not be permitted. Please review the Unit4 Cloud Customization Policy & Procedure for SQL Database Objects (available to partners, Customers and prospects via the Cloud Documentation in Community4U or at www.unit4.com/service-descriptions).
All Customers must self-certify custom SQL database objects (i.e., assessing the custom SQL database objects that they use and confirming to Unit4 that they are complying with the requirements set out in this section 10 and the Unit4 Cloud Customization Policy & Procedure for SQL Database Objects). Unit4 reserves the right to impose an additional charge on the Customer for the ongoing risks and management costs to Unit4 associated with retaining custom SQL database objects in Unit4 SaaS.
No direct access to local resources such as file system, network, etc., access must be indirect via approved methods that provide abstraction from specific infrastructure.
All customisations must be delivered fully documented.
Any code needs to be transparent and readable delivered to Unit4.
All customisations must include installation routines that require no manual interaction and allow for end Users to validate installation has been completed and the customisation ready for configuration or use via standard application capabilities.

10.3 Customisations – Review, Rejection, Removal

Unit4 requires spot check review of all Customisations submitted by Customers to ensure the security, stability, and performance of its services. Unit4 will request the source code of the Customisation to evaluate any potential risks to the service's stability, security, and/or performance.

For the adoption of new Customisations or updates to existing ones, Customers must submit a Service Request to Unit4. If Unit4 identifies any reasonable concerns, it reserves the right to reject the request upon review or remove existing Customisations from Customer environments.

10.4 Data Modification via Customisations

Customisations allow Customers to execute direct database modifications (e.g., directly changing, removing, or updating data in your database). Direct changes to the database are not normally permitted and Customisations can bypass standard built-in data controls in the application layer which protect both the confidentiality and integrity of Customer's information as well as impact system performance. By introducing Customisations, Customer accepts all the risks that are related to data consistency and integrity.

10.5 Data Modification via SQL Queries

Customers may request an execution of custom one-time SQL scripts in their databases. Such scripts may be subject to additional review by Unit4 and may be rejected due to a lack of compliance with Unit4 policies. Customers accept all the risks that are related to data consistency and integrity by requesting a Customer SQL script execution. With this Unit4 does not take any responsibility for the manual alteration of the database records.
Scripts to create objects in the Customer's database, such as views and tables, are treated as customisations and should follow the standard customisation review process.

10.6 Unit4 APIs Backward Compatibility

Unit4 recommends using the most recent version of the Unit4 APIs in order to receive optimum performance and stability. Prior versions of Unit4 APIs are updated to support backward compatibility for all prior versions of Unit4s APIs that have not reached an end-of-life status. End-of-life announcements will be made not less than eighteen (18) months before the end-of-life of each Unit4 API.

10.7 Robotic Process Automation (RPA)

Robotic Process Automation (RPA) is permitted in Unit4 SaaS under the following conditions:

No software can be installed on the Web server. The RPA must function entirely as a User, although it may optionally use APIs.
The RPA must operate like a human (e.g. similar pace and login frequency). Rapid, robotic keystrokes or excessive system interactions may cause timeouts or other issues, which could disrupt both the RPA's operation and the system itself.

10.8 Integrations

Integrations are defined as any type of interaction with U4FbC that are not classified as above defined Customisations. Integrations are permitted according to the supported integration methods described below. Integration methods not explicitly stated below are not permitted.

Integration Type	Permitted?
Integration using U4FbC API/web services SOAP	✓
Integration using U4FbC API/web services REST	✓[6]
Integration using U4FbC API/XMLi	✓[7]
U4FbC Integration Tool Kit (ITK) integrations	✓[8]
Integration using standard export/import files over SFTP	✓
Integration requiring read-only access to replicated dataset [9]	Additional Service offering – Data replication (read-only)

10.9 Maintenance of Customisations and Integrations

Maintenance, support, implementation and update considerations for these components is not included in the SaaS Charges except for Unit4 Engineering maintained Customisations listed above.

Customer or Unit4 partner authored Customisations, ITK processes, integrations are the full responsibility of the Customer for all aspects of deployment and maintenance. Customer responsibilities include code lift for release version compatibility, functional testing and Configuration and error resolution.

---

[6] Available with 2024 Q4 Release

[7] The .Net Router is deprecated.

[8] Existing ITK processes are allowed after review, new processes not allowed as ITK has been deprecated.

[9] Direct dataset read-only access is not included in the standard offering. Data replication is not subject to SLA and is not advised for production dependent processes. See "Data Replication (Read-Only) ".

Unit4 Success Services authored Customisations, ITK processes and integrations are outside the scope of for U4FbC SaaS. Maintenance of Customisations and integrations must be formally set up and included on an executed Sales Order to ensure that Unit4 takes responsibility. If Unit4 maintenance of Customisations and integrations has not been included on an executed Sales Order, responsibility for all aspects of deployment and maintenance will reside with the Customer.

11. Technical operations

11.1 Printing

Printing directly from U4FbC can be achieved using an Internet Printing Protocol (IPP/IPPS) printer over the Internet. Certificate management and management of the printer or print server is the Customer's responsibility.

The following authentication schemes are supported: -

No authentication
Basic authentication

11.2 Data replication (read-only)

Replicated database tables can be provided, at an additional recurring cost, as described in the Database Replica Service for U4FbC.

11.3 Connectivity

Unit4 uses static public IP addresses (both outgoing and incoming) for our services, providing reliable connectivity. However, please note that while we strive for consistency, these IP addresses are subject to change in the future and cannot be guaranteed as permanent.

Internet bandwidth suggestions

The web browser will use 12 to 20 Kbps per User unless large graphics are used.

Access scenarios

For U4FbC interfaces, the following access methods are available:

Interface type	Access method
Web endpoints	Internet
SFTP	Internet
Data replication (read-only)	Internet

11.4 SFTP Account Management

SFTP accounts are provisioned by Unit4 upon Customer request.

Following initial provisioning, password management and credential lifecycle (including resets and rotation) are performed by the Customer via the designated user management portal.

Customers are responsible for maintaining appropriate credential security in accordance with the minimum password requirements defined in the Unit4 Cloud Technical Guidelines and Limits document.

11.5 Authentication

By default, authentication for U4FbC (Web Client) is carried out using application-based username and password authentication. Management of Users and passwords within the Unit4 Financials application is the responsibility of the Customer.

The Unit4 SaaS have capabilities for federated authentication to allow Customers' Users to use their organizational credentials (e.g. domain username and password) when logging in to an Unit4 application using a web browser (web access). 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.

In order to use federated authentication, there is an optional Service called Unit4 Identity Services or Unit4 IDS. Unit4 IDS is a Multi-tenant Identity solution and architecture for the Unit4 ecosystem, that allows Users to have one single identity across multiple applications and provides a single sign-on experience. More details about Unit4 IDS can be found in Unit4 Platform Service Description at www.unit4.com/service-descriptions.

The Customer is responsible for Configuration of their identity provider (IdP) and for providing specific information (required or requested) to Unit4 that allows for configuration of Unit4 IDS. Authentication through IDS is preferred from a security perspective.

12. Data considerations

12.1 Transfers of Customer data to Unit4 Financials by Coda SaaS

Unit4 deploys a standard architecture and therefore, where Customer is an existing Unit4 Customer, it 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 U4FbC SaaS.

When Customer requests to copy a database snapshot from outside of Unit4 SaaS then it should be free of any Customisation objects. These objects should be sent in a separate Service Request and will follow standard Customisation review process.

Customer files transferred to Unit4 SaaS must be provided in an unencrypted format, as encryption in transit and at rest is handled by Unit4 SaaS.

12.2 Backup and Restore Services

Customers are given the option of a “forgiveness” restore, where a recent Production Service full back-up can be restored to the PE in case of a disastrous User mistake (e.g. running month end processing in “live” environment instead of Preview as intended).

Backups are performed to allow for forgiveness restores to be completed with a restoration point as shown below and no later than thirty (30) days prior to current time, to a resolution as shown below. Forgiveness restores should be initiated as a P1 incident and time to complete depends on data volume. The restore process is limited to the database itself.

Request restore point permitted
between 1 hour prior to the time the request is made and no later than 30 days prior to the time of request to a resolution of 5 minutes (see example below)

Current time	Restore Range	
15-03-2017 00:15	13-02-2017 00:15	14-03-2017 23:15
25-07-2017 14:25	25-06-2017 14:25	25-07-2017 13:25
22-09-2017 08:00	23-08-2017 08:00	22-09-2017 07:00

12.3 Data Security

Data in transit

Customer's Data in transit over public networks is protected with TLS 1.2.

Customer data at rest

The transparent data encryption and/or whole database encryption is used for U4FbC SaaS to protect Customer data at rest. More information can be found in Unit4 Information Security Policy at www.unit4.com/terms.

IP Allowlisting

IP Allowlisting is offered as an option that will come at an additional cost in the Unit4 SaaS, as a means to gain an extended level of control on what IP address has access to the Customers environment. An IP Allowlist is a list of IP addresses that are granted access to a certain Service. When an IP Allowlist is used, all IP addresses are denied access, except those included in the IP Allowlist. Unit4 does not support adding to Allowlist IP addresses which are changing frequently (e.g. dynamically assigned by your Internet Service Provider).

IP Allowlisting is available for the following product – data centre – service type combinations:

IP Allowlisting	Data centre	Service Type
Web endpoints	Azure	All
SFTP	Azure	All

Customers with enabled Allowlisting are responsible for providing VPN access to their own network for partners or Unit4 consultants working off-network (to keep the traffic originated from allowed IP addresses).

The Platform Services use dynamic IP addresses; therefore, IP Allowlisting is not supported for any combination of Financials by Coda with any Platform Services. As an exception IDS does support IP Allowlisting in combination with Financials by Coda, whereby the Customer IDP must be publicly accessible. For further details, please refer to Schedule C.

Component lifecycle and security dependencies

All Services, and infrastructure components used within the Unit4 ecosystem are subject to a defined product and component lifecycle. This applies to both Unit4-developed components and third-party technologies that form part of Unit4 Financials by Coda.

To maintain the security, integrity, availability, and performance of the Service, all components must remain within vendor-supported versions and lifecycle states (e.g. TLS versions, .NET frameworks, Unit4 add-ons, or statutory localisations).

When a component of Unit4 Financials by Coda reaches end-of-support or end-of-life, Unit4 will automatically replace, upgrade, or remediate the component as part of its standard operational and security processes. Customers cannot opt out of these changes, as the continued use of unsupported components of Unit4 Financials by Coda would introduce unacceptable security and stability risks to the Service.

12.4 Limits and regulations on usage

Unit4 operates within a multi-tenant environment and adheres to fair use policies to prevent any single process from monopolizing shared resources. Should these limits be exceeded, appropriate corrective actions will be implemented. For detailed guidelines related to service limits and regulations, please refer to the Unit4 Cloud Technical Guidelines and Limits document available at www.unit4.com/service-descriptions.

12.5 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. Web Client, Mobile Apps).
- API/web services.
- Read-only access to replicated dataset, see topic 11.2 Data replication (read-only).
- Upon Agreement termination Customer Data can be retrieved by Customer in accordance with the Agreement.
- SFTP access.

SCHEDULE A

Localisations by country

Localisations by Unit4 engineering

Localisations developed and/or maintained by Unit4 engineering are permitted as standard, and include the following:

Code	Name	Country	Description	Ownership
nlcommon	Common Extensions NL	Benelux	Common extensions for NL customisations	Unit4 Engineering
nladvpay	Advanced Payments	Benelux	Advanced Payments	Unit4 Engineering
nlintbal	Intray Balances	Benelux	Intray Balances	Unit4 Engineering
nlperass	Period Assistant	Benelux	Period assistant	Unit4 Engineering
nlstufbg	StUFBG Integration	Benelux	StUF BG Integration	Unit4 Engineering
nltranal	Transaction Allocation	Benelux	Transaction allocation	Unit4 Engineering
nlcolfee	Collection Fees	Benelux	Collection Fees	Unit4 Engineering
nlscanim	Scan Import	Benelux	Scan Import	Unit4 Engineering
nldocrep	Document Repeater[10]	Benelux	Document Repeater	Unit4 Engineering

[10] Not compatible with Unit4 Identity Services for U4FbC version 14 and 13.

Code	Name	Country	Description	Ownership
nlremhis	Reminder History	Benelux	Reminder History	Unit4 Engineering
einvoicing	E invoicing	Benelux	E invoicing	Unit4 Engineering
deelster	ELSTER[11]	Germany	Produce Files for German tax authority	Unit4 Engineering

Customization by third party or Unit4

Customization developed by third-party, partners or Unit4, via Success Services that have been reviewed in accordance with the customization review criteria are permitted. Updates are requested by Benelux and French Success Services that maintain the solution. It includes the following:

Benelux

Code	Name	Description	Ownership
nlassetudf	Assets-UserExtensions	Provides values for User Defined Fields in Assets	Unit4 Benelux Success Services
nlnotifypimusr	GLS_Notification-01.001.006-14000	Sends notifications to Users when assigning an invoice to another User in Invoice Matching	Unit4 Benelux Success Services

[11] Not compatible with Unit4 Identity Services.

France

Code	Name	Description	Ownership
frstmloader120	StmLoader (AFB120)	AFB120 bank statement format loading into statement table. NB: A shared FTPS folder will be used to securely upload the statement files from the client network	Unit4 France Success Services
frexportdata	ExportData	Produces the FEC file for French authorities: NB: a dedicated Uri will be provided to download each file via HTTPS access - FTPS could also be used to retrieve files	Unit4 France Success Services
fribanbankctrl	IBAN control CTRLBankAcc	IBAN and bank account format validation:	Unit4 France Success Services
frdbgateway	FRDbGateway (includes FRUtilities)	Common connectivity components	Unit4 France Success Services

SCHEDULE B

Unit4 Financials by Coda Tailored Solution

Unit4 Financials by Coda Tailored Solution provides the same service offering as the standard U4FbC standard solution with the distinction that computing resources such as web server, SQL server and business server, are not shared with other Unit4 Customers, and are dedicated to a single Customer. The tailored solution comes at an additional charge.

The tailored solution, formerly known as Dedicated, is a pre-requisite to order the Software Update Deferral Service.

The tailored solution is not available for the Unit4 Platform Services, these are always shared (Unit4 Platform Services are multi-tenant).

SCHEDULE C

Other optional services

All optional service description documents are available in Community4U.

Service name	Description	Version
Software Update Deployment Deferral	The service provides an option for Customers to delay the installation of the latest software update. It outlines specific conditions that must be met to request this service.	1.0
Downloadable Production Database Backup	Unit4 provides a weekly export of your Production Environment database to a secure Azure storage location, usable with the latest Microsoft SQL Server version, available for manual download and retained for four weeks.	1.0
Controlled EU Access	This service add-on ensures that Unit4 SaaS instances are hosted within the EEA or equivalent countries, safeguarding Customer data by regulating privileged access from outside these regions.	1.0
Web IP Allowlisting Service	The Unit4 IP Allowlisting Web service is an optional feature to enhance security and control over access to our Customers' environments via web interface. This document provides an overview of the service, detailing its benefits, limitations, and relevant information.	1.0
SFTP IP Allowlisting Service	The SFTP IP Allowlisting service enhances security by allowing Customers to specify up to 10 IP addresses for exclusive access to their U4 Cloud SFTP account, automatically blocking all others (excluding dynamic addresses).	1.1

SCHEDULE D

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 Service Terms (found on www.unit4.com/terms).

Glossary

Term	Definition
Account Administrator	An Account Administrator is an appropriate and qualified Business User who has administrative-level control over the creation, maintenance, and deletion of accounts that provide access to the Unit4 Product.
Cloud Customer ID code	A Cloud Customer ID code is a unique Cloud Customer identifier.
Customisation Object	The result of any Customisation, referring to any code change or other database object that is not created through modifications to the standard Unit4 Product menus and functionality.
Localisation	A Unit4 Product developed for strategic territories and verticals that secures legal, statutory and market standard requirements in that territory or vertical.
Maintenance Release	A Maintenance Release for Unit4 Financials by Coda is a full release of the product, used to deploy a software fix outside the standard release schedule.
Multi-Tenant	A single instance of Unit4 SaaS including its supporting infrastructure which serves multiple Customers.
Record	A data record stored within a Customer's database (for example a line in a timesheet).
Service Restore	The time required by Unit4 to restore a recent backup of the Production Environment, initiated at the Customer's request.
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)
DTU	Database Transaction Units
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IdP	Identity Provider
Kbps	Kilobits Per Second
KPIs	Key Performance Indicators
NPE	Non-Production Environment
PCI DSS	Payment Card Industry – Data Security Standard
PE	Production Environment
SFTP	Secure File Transfer Protocol
SHA-2 RSA	Secure Hash Algorithm (number 2) and RSA encryption Algorithm
SLA	Service Level Agreement
SOC	Service Organization Controls
SQL	Structured Query Language
TDS	Tabular Data Stream
TLS	Transport Layer Security Encryption
URL	Uniform Resource Locator (a web address)
U4FbC	Unit4 Financials by Coda
VPN	Virtual Private Network
WIP	Work In Progress

Notable Changes from V. 2025.2.1

These are the updates from the previous version incorporated into the current 2026Q1 release.

- General functional and technical requirements and specifications added to Chapter 8