UNIT4
In business for people

Unit4 Platform Services

Cloud Service Description

VERSION 2026Q1

March 2026

CONTENT

1. Introduction

Unit4 Platform Services are the foundational layer of Unit4 solutions. The Platform has a micro-Service based architecture where different Task Focused Applications run independently of each other. These Services are Multi-Tenant, shared Services that integrate with several Microsoft Azure PaaS Services. Unit4 checks availability of its Platform Services according to the SLA measuring individual micro service availability. The time to completion of a business action depends on the processing by one or more micro services which operate asynchronously.

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

Unit4 Platform Services runs on Microsoft Azure, leveraging Microsoft Azure's scale and experience of running highly secure and compliant cloud Services around the globe. Microsoft Azure certifications provide the building blocks for Unit4's compliance efforts. Unit4 delivers its own ISO 27001, ISO 27017, SOC 1, SOC 2.

In summary, Unit4 provides the following:

- Fully scalable Platform, in a high availability environment with redundancy
- Security by design
- Continuous monitoring is in place, feeding alerts and continuous improvement
- Application updates
- Production and Non-Production Environments with a separate database for Customer Data (if applicable)

2. Data centres & data residency

Unit4 Platform Services is built upon Microsoft Azure infrastructure and platform Services. The Unit4 Platform Services are 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 Azure region details: 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
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	New South Wales and Victoria (DR)	AEDT/AEST
Norway	Microsoft Azure	Oslo and Stavanger (DR)	CET/CEST

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

Customer head quarter residence	Geopolitical zone used
APAC	Asia
Australia/New Zealand	Australia
Canada	Canada
EU	EU
Norway/Sweden/Denmark	Norway
UK	UK
US	US

3. Service model

Unit4 Platform Services is a Multi-Tenant solution embedded in a cloud native / Service based platform. Unit4 Platform Services characteristics are as shown in the table below:

Category	Component	Characteristics
SOLUTION	Releases and Updates	Will be applied automatically and periodically
	Environments included	1 Production + 1 Non-Production (Preview)
	Availability guarantee	As per SLA
SERVICES	Releases will commence	Automatically
	Updates will commence	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 – Microsoft Azure	SOC1 Type II (ISAE 3402), SOC2 type II (ISAE 3000), ISO27001, ISO27017[1]

[1] 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. Environments

Customer's application environments connect to two discrete Unit4 Tenants in Unit4's Platform Services. The application Acceptance and Preview Environments connect to the Platform Preview environment while the application Production Environment connect to the Unit Platform Production environment where Unit4's Production SLA applies.

Customers' Preview Environments always contain the latest updates for the Unit4 Product in use by the Customer.

Unit4 assigns to every SaaS Customer a unique Cloud Customer ID code, which is visible in various elements of the Service (including environments) and it is used for Customer identification. The MS Azure Customers ID code is a 3-character acronym and for Norwegian DC Customers ID code consists of 6 digits. The Customer ID codes are created at Unit4 discretion during the early stage of the implementation and are not a subject to change. I

4.1 Production Environments

Only the Unit4 Platform Services Production Environment (PE) is subject to the Service Level Agreement. Customer accessible/visible platform services follow the general SLA. Platform Services unpinning other services that are customer accessible/visible are part of the Customer facing services.

4.2 Non-Production Environments characteristics

- A Non-Production Environment (NPE) is not subject to an SLA.
- For Platform Services there is no refresh from PE to NPE.
- NPE has reduced capacity and cannot be used to resemble PE throughput.
- All NPEs are updated as soon as an Update is available. Once an NPE has been updated to the latest Update, it is not possible to move back to the previous Update.

5. Releases and Updates

There is no concept of a Release to Unit4 Platform Services. All changes to a Unit4 Platform Service are considered an Update of the Service and will be applied automatically and continuously.

Unit4 Platform Service Updates are deployed in a transparent manner and result in no downtime. As such, Unit4 Platform Service Updates can be deployed outside of Planned

Maintenance windows. In rare cases when downtime is necessary, the Update will be performed during a Planned Maintenance Window.

6. Planned and Unplanned Maintenance

6.1 Planned Maintenance

Planned Maintenance Windows are dedicated to applying all the respective changes to the Service provided e.g. solution Updates and infrastructure changes. During Planned Maintenance Production, Service may be periodically unavailable. You can find more details on the schedule presented in the table below:

	Planned Maintenance Windows (PMW) *Updates and Infrastructure*
All regions (except Azure US and Azure Canada)	12 per year, **Regular PMW:** From: Sat 5PM To: Sat 11PM UTC* or **Extended PMW**: From: Sat 5PM To: Sun 5AM UTC*
Azure US and Azure Canada regions	12 per year, **Regular PMW:** From: Sun 5AM To: Sun 11AM UTC* or **Extended PMW**: From: Sat 11PM To: Sun 11AM UTC*

*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 the Maintenance page of the Cloud/SaaS Services section 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.

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 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.

6.2 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.

7. Customer permissions and responsibilities

7.1 Customer permissions

Customer has the right to:

1. Monitor Production Environment availability and Service Response Time on an active basis using a third-party monitoring service. Monitoring acts as a consumer of the Unit4 Platform Services. The Customer must 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. Conduct an external security vulnerability scan. Details of the planned scan can be provided to Unit4 at least 30 days in advance of each scan using a Service Request. Failure to so do may result in blocking the Customer to use the Service while testing.
3. Conduct a security penetration test. Details of the planned test can be provided to Unit4 at least 30 days in advance of each test, using a Service Request. Failure to so do may result in blocking the Customer to use the Service while testing.

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

7.2 Customer responsibilities

Customer has responsibility to configure the Customer assets according to the needs of specific Unit4 Services such as Extension Kit, AVA and IDS.

7.3 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.

8. Data Security

Data in transit

Customer Data in transit is over public networks is protected with TLS 1.2 and higher.

Customer Data at rest

Data at rest is protected using transparent, whole database encryption (e.g. transparent data encryption, and/or whole disk data encryption). Please see the Unit4 Information Security Policy, which is available at www.unit4.com/terms.

Allowlisting

The Platform Services use dynamic IP addresses and are not usable for IP allowlisting (a.k.a. IP filtering). Multi-layer authentication mechanisms based on SSO and M2M accounts are the data security mechanisms of choice. Static IP addresses can be purchased. Static IP address - Extension Kit

9. Data backup

Data is backed up with a retention of 7 days to support Disaster recovery scenarios. 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 the frequency to support RPO on a level of 1 hour.

10. Customer data criticality

There is no critical customer data in Platform Services.

11. Platform Services

The table below lists the Platform Services that support the technical health and operation of Unit4 SaaS. These Services run in the background and, while not always Customer-visible, are essential for ensuring stability, security, and ongoing platform performance.

#	Service Name	Additional Details	Available with ERP CR Azure/Nordic
1.	**API Services**	Appendix E	ERP CR Azure / Nordics
2.	**App Studio**	Appendix B	-
3.	**Data Hub (Bulk Data Access)**	Appendix F	-
4.	**Extension Kit**	Appendix A	ERP CR Azure
5.	**Identity Services**	Appendix C	ERP CR Azure / Nordics
6.	**Unit4 Advance Virtual Assistant (AVA)**	Appendix D	ERP CR Azure / Nordics

Appendix A: Extension Kit Services

Introduction

Unit4 Extension Kit (U4EK) is a cloud based; Multi-Tenant solution operated by Unit4 that provides a toolkit allowing Users to extend the capabilities of Unit4 Services. Unit4 Extension Kit gives Customers the opportunity to build or consume Extension Flows.

Extension Kit cannot be connected to two environments at the same time. A Customer needs to raise a Service Request with Unit4 every time a new environment is to be connected to one of these Services, whereas a Customer's Production Environment will be connected to the Production Environment of the Platform Service and each Customers Non-production Environment will be connected to the single preview instance on request.

Preconditions

- Unit4 Extension Kit requires Unit4 Identity Services (IDS) to be configured.
- Depending on the use case that Unit4 Extension Kit solves, it may require some web Services in the application to be publicly available to communicate with the business solution to perform certain tasks.

Restrictions

Unit4 Extension Kit only provides value when connected to any of the Unit4 Services. The ability of Unit4 Extension Kit to automate processes and resolve use cases is determined by the events that the Unit4 application publishes, and the endpoints made available.

Please read the product documentation of the respective Unit4 business solution connected to Unit4 Extension Kit for details about the endpoints and events available.

Customer responsibilities

Customers are responsible for creating, documenting, testing, maintaining, updating and managing the Extension Flow that was created in using Unit4 Extension Kit unless otherwise agreed especially after new Releases / Updates are made available.

Non Unit4 Services used

Unit4 Extension Kit uses the following services made available by a third party:

- Twilio - SendGrid Email Service
- Microsoft Azure Platform Services
    - ✓ Storage Account

- ✓ Event Grid
- ✓ Azure Functions
- ✓ Azure App Service
- ✓ API Management
- ✓ Microsoft CosmosDB
- ✓ Key Vault
- ✓ Application Insights

Specific terms and conditions and Data flow

When a User first logs in Extension Kit portal is asked for consent of usage of the Service. When and what data is sent to where is defined by the Extension Flow, which is created by the User. So, it is responsibility of the User where the data is being sent and the content of the data, which might contain Personal Data.

By default, Unit4 Extension Kit will store historical information about each Extension Flow run. This historical information is accessible by the Users that have access to the portal (this User access to the portal must be granted by another existing User with owner access rights). In this historical information, some parts are obfuscated so are not visible in the history. These parts are defined by the Actions definitions and cannot be chosen by the User.

The User can switch off this functionality by defining an Extension Flow as “Sensitive”, this way no information will be stored and only the result of the Extension Flow execution will be shown.

Extension Kit does not store any other User information or usage statistics beyond what is necessary for service improvement and security monitoring. Limited, anonymized telemetry data may be collected to help ensure service reliability, performance, and to improve the overall experience. This telemetry does not include any personal data from the content of your Flows.

Limits and regulators on usage

Extension Kit — Usage Limits

Unit4 Extension Kit enables Customers to create Extension Flows — automated processes that can range from simple to highly complex, depending on the volume of data processed, transformations applied, and the number of Actions executed.

Monthly Usage Allowance

Extension Kit operates in a Multi-Tenant environment, with a technical upper limit which is applied to ensure platform stability for all Customers.

Each Customer is entitled to 15,000 Actions started per calendar month ("Usage Limit"). Unused Actions do not roll over to the following month.

Customers may purchase additional Actions from Unit4 in blocks of 1,000, as required. Please contact your Unit4 account representative regarding the price.

Customers can monitor their Action consumption at any time via the Extension Kit Portal — Metrics. Extension Kit Portal > Metrics.

Service Limits

To ensure platform performance, individual Flows are subject to technical limits (e.g., maximum actions per flow, data size limits, execution timeouts). Full details are documented at: Extension Kit — Service Limits. These technical limits are enforced.

Appendix B: App Studio

Introduction

Unit4 App Studio is a low-code tool that enables teams to extend ERP with new screens and business apps, helping organizations tailor processes without deep technical expertise. It empowers users to operate more efficiently and adapt quickly by putting powerful configuration and app-building capabilities directly in their hands

Preconditions

- Unit4 App Studio requires Unit4 Identity Services (IDS) to be configured.
- Unit4 App Studio requires Unit4 Extension Kit to be configured
- Depending on the use case that Unit4 App Studio solves, it may require some web Services in the application to be publicly available to communicate with the business solution to perform certain tasks.

Customer responsibilities

Customers are responsible for designing apps efficiently to avoid unnecessary API consumption, managing lifecycle and cleanup of unused applications, validating that custom apps meet organizational standards, including compliance and localization, ensuring that users have proper ERP permissions for APIs and data access.

Limits and regulators on usage

App Studio operates within Unit4's Multi-Tenant cloud environment and therefore follows platform-wide usage controls designed to ensure fairness, stability, and predictable performance. Apps must comply with API rate limits, data-handling constraints, and resource governance rules inherent to ERP and Platform Services. Triggering Extension Kit flows and calling external APIs is subject to platform quotas and technical limits, and overly complex screens, large payloads, or heavy logic may be restricted or throttled to protect system performance. These safeguards ensure that no single app consumes disproportionate resources and that all tenants benefit from a reliable, consistent experience.

Specific terms and conditions and Data flow

App Studio apps process data dynamically and do not store business data locally; all information flows through authorized API calls, Extension Kit flows, or ERP resources using the customer's security context. Data submitted by users is transmitted directly to underlying services (ERPx, ERP CR, or third-party endpoints) following Unit4's secure cloud architecture. The platform ensures that data remains within approved boundaries, and customers must ensure that any external integrations comply with their internal data-handling policies.

Appendix C: Identity Services

Introduction

Unit4 Identity Services ("**U4IDS**") 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. U4IDS integrates with the organization's identity solution using industry standard protocols and is shared across Unit4 applications acting as a gateway for external authentication.

Environments

The Unit4 Identity Service is designed to ensure continuous availability, with no downtime during upgrades or updates. As a result, planned maintenance windows or refresh periods do not apply.

The disaster recovery strategy is designed to minimize service disruptions by leveraging Microsoft's cloud infrastructure for failover and high availability. Customers can expect seamless transitions in the event of infrastructure failures, ensuring continued access to authentication services without manual intervention. On U4IDS, the applied strategy is Geo-

Redundant Storage (GRS), which is the standard across all Platform Services. It replicates data to a secondary region, providing built-in disaster recovery capabilities. In the event of a regional failure, the Service automatically fails over to the secondary region, ensuring continuous Service availability. This geo-redundancy minimizes the risk of downtime, with traffic being dynamically rerouted to maintain Service continuity without manual intervention.

Data considerations

U4IDS does not store user information or credentials. Instead, it only retains the necessary details about the Tenant's Identity Provider (IdP) to facilitate a secure authentication process.

The Unit4ID serves as the identity field within the system. Customers should carefully consider the visibility of this field when selecting the corresponding attribute from their Identity Provider. For instance, using an email address as the Unit4ID is not recommended due to its identifiable nature.

All data is processed and stored in Azure Log Analytics Data Store (Log Analytics Workspace) and the IDS Database.

Before processing any Personal Data/Personally Identifiable Information (PII), the Service requests user consent during the first login. Sharing personal information is optional; however, consent to share the user identifier is mandatory. Without this consent, the application cannot function and will not be accessible.

It is the Customer's responsibility to ensure that their Identity Provider shares only the required information with IDS. U4IDS does not control or verify the data sent by the Customer's Identity Provider, and it is up to the Customer's IT team to ensure that only the necessary information is shared.

Customer responsibilities

Customers are responsible for configuring their Identity Provider (IdP) and providing the necessary information—whether required or requested—to Unit4 to enable the configuration of U4IDS. Support for configuring the Customer's IdP or troubleshooting related issues with U4IDS integration is available through Unit4 Professional Services as a chargeable service. The Customer IdP must be publicly accessible for Unit4 IDS to reach.

Non Unit4 Services used

Unit4 Identity Service uses the following Services/Products made available by a third party:

- Microsoft Azure Platform
- Duende Identity Server v7

Limits and regulators on usage

Unit4 Identity Services allows each Unit4 Customer to create up to 10 Machine-to-Machine (M2M) clients by default. If additional IDS clients are required, the Customer must identify this need and address it during the sales cycle to ensure the requirement is met. Additional clients may be subject to further assessment and potential costs.

Appendix D: Unit4 Advanced Virtual Assistant (AVA)

Introduction

Unit4 Advanced Virtual Assistant service (Ava) is a true enterprise digital assistant powered by AI, helping users take care of their administrative tasks in an intuitive way using a conversational dialog and managing discussions to effectively collaborate with their colleagues when solving an issue. Ava can also notify users of important tasks and activities. Ava has a skillset based on the Unit4 business solution it is connected to. The specific skills available on each business solution are describe in the Ava guideline.

Ava only works with Microsoft Teams chat application. As it is a 3rd party application, Microsoft Teams it has its own terms & conditions for usage and data privacy which are outside of Unit4's control. Unit4 is not responsible or involved in the procurement, configuration, usage or support of Microsoft Teams.

AVA is deployed as a global Service without storing data in one specific geopolitical zone (Data residency rules described in chapter 2 are not applicable)

Preconditions

- Ava requires Unit4 Identity Services (IDS) to be configured.
- Depending on the type of skills that are used, Ava may require several web services in the application to be publicly available to communicate with the business solution to perform tasks requested by the user.
- To make use of Ava the Unit4 business solution it connects to needs to be on a currently supported version. Please check the service description of your Unit4 business solution (e.g. U4ERP) for version dependencies.

Customer responsibilities

Customers are responsible for the configuration of the Unit4 business solution (e.g. Unit4 ERP). The steps required for configuration in the business solution that Ava connects to are available in the online implementation guide: https://ava-implementation-guide.u4pp.com. Assistance with this configuration is available from Unit4 Professional Services.
Customers are also responsible for the installation of the Ava Service App in Microsoft Teams. Additionally, some of the Ava functionalities require granting the app certain permissions. Check the implementation guideline for further knowledge https://ava-implementation-guide.u4pp.com.

Non Unit4 Services used

Unit4 Ava is integrated with different Services made available by a third party:

- Microsoft Graph API
- Microsoft Azure Platform Services
    - ✓ Azure AI Bot Service (formerly known as Microsoft Bot Framework) Azure AI Services
    - ✓ Azure AI Services
        - Azure AI Language: Conversational Language Understanding (CLU)
        - Azure OpenAI
    - ✓ Microsoft Teams

Specific terms and conditions and Data flow

When talking to Ava for the first-time, Customers and their end users must agree to the overall Ava Privacy Statement Unit4 Privacy Policy AVA Service September 2025. The Ava ecosystem makes use of several Microsoft Azure services. The use of these Azure services is governed by the terms and conditions of the agreement under which Unit4 obtained the services: https://azure.microsoft.com/en-us/support/legal/.

User's interactions with Ava are also subject to the MS Teams chat application's applicable terms of use, privacy and data collection policies. How personal information and other conversational content is transmitted, stored and processed by Microsoft Teams is outside Unit4's control: Microsoft Privacy Statement – Microsoft privacy

When connecting to Ava the first-time the user is asked for consent to store their messages and Ava's responses. If accepted messages are stored anonymously inside the Ava

ecosystem to improve Ava's "intelligence" (identify usage patterns, etc.). This data cannot be accessed by any user and only can be accessed by Unit4 personnel in accordance with applicable laws and in case customer needs support in relation with Unit4 Ava Service. Even though stored anonymously chat messages sent to Ava can include personal data. Provided data is solely used for the purpose of delivering Ava, where users can always ask Unit4 Ava to erase their Personal Data. Provided Data is never used nor submitted for AI model training purposes.

Appendix E: API Services

Integrations in API

When integrating via API, authentication is handled using machine-to-machine (M2M) clients, which are configured with a unique client ID and secret key. These credentials provide direct system-level access and are strictly tenant-specific. In a Mult-Ttenant environment like Unit4 platform, it's essential to understand that M2M keys are not interchangeable between customers. Sharing the key and secret of one tenant for another—even by accident—can result in serious data access issues. To protect our customers and ensure security, we only provide M2M credentials directly to the customer's designated administrator. These keys must not be shared with service partners, vendors, or internal consultants. Customers are responsible for managing them with care to avoid misuse or cross-tenant access.

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

Any non-standard Configuration (e.g., Integration and Extension flows), creation of custom reports, custom entities, fields, relationships, imports, exports, workflows, interaction plans, lookup data, and web styles 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. All Configurations must be carried out based on lean principles, to ensure ongoing performance and resilience of the Service.

Unit4 endeavours to provide API backwards compatibility. For further details on API lifecycle and versioning strategy, please refer to API technical documentation.

Integration Type	Permitted?
Integration using Unit4 Platform Services API	✓
Integration using Unit4 Extension Kit	✓

Integrations created by methods mentioned above, including Extension Flows created using Unit4 Extension Kit are not supported by Unit4 under Standard Support terms, unless agreed otherwise. The Customer has sole responsibility for any Integrations, including Extension Flows, 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 and/or Extension Flows, including Unit4 Integrations delivered as part of a Project implementation. If any assistance is required in regard to Extension Flows, 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.

Limits and regulators on usage

While the use of APIs within Unit4 platform is subject to certain usage limits and regulatory controls, it's important to note that these are defined at the product level, not centrally enforced by the platform itself. Each product integrated with the platform may apply its own rules regarding rate limits, data access, and operational boundaries. Therefore, to understand the specific API usage policies and constraints, Customers and partners must refer to the online help of the respective product. These documents provide detailed guidance on how the API can be used, including any applicable limits or conditions that ensure fair and secure usage.

Appendix F: Data Hub – Bulk Data Access

Introduction

Unit4 Data Hub — Bulk Data Access is a high-volume, batch-oriented data extraction capability built on top of the Unit4 Data Hub service. It enables organizations to access curated, analytics-ready ERPx data products at scale, without relying on API-based extraction or impacting operational workloads.

The Service exposes Customer-specific Delta tables through **Delta Sharing**, an open and secure data-sharing protocol supported by leading BI analytics and AI platforms. This

empowers data engineers, BI analysts, and AI teams to integrate ERPx data directly into their data warehouses, data lakes, machine learning pipelines, and enterprise reporting solutions.

Preconditions

- Data Hub – Bulk data access requires Unit4 Identity Services (IDS) to be configured.

Restrictions

- Data Hub – Bulk data access depends on Microsoft Databricks service, which cannot deploy secondary / disaster-recovery region in Norway East.

Customer Responsibilities

Customers are responsible for managing their own use of Bulk Data Access, including selecting and configuring the appropriate data products and refresh schedules in the Data Hub Portal, ensuring that all data extracted complies with their internal governance, retention, and data-handling policies, and designing efficient analytics pipelines that minimize unnecessary data movement by favouring incremental processing where supported. Customers must also securely store and manage their Delta Sharing credential files—which can only be downloaded once—and protected according to their security practices.

Non Unit4 Services used

Unit 4 Data Hub is integrated with different Services made available by a third party:

Microsoft Azure Platform Service:

- Storage Account
- Data Lake Gen2
- Storage tables
- Event Grid
- Azure Functions
- Key vault
- Application insights
- Spark
- Azure DataBricks

Limits and regulations of usage

Data Hub – Bulk data access depends on Microsoft Databricks service, which cannot deploy secondary / disaster-recovery region in Norway East.

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 appropriate and qualified Business User who will have administrative level control for creation, maintenance and deletion of Accounts providing access to the Unit4 Product.
Cloud Customer ID code	A unique Cloud Customer identifier.
ERPx Service User	Data Base User used for communication between Microservices.
ERPx Web Application	The main web application portal for Unit4 ERPx.
Extension	Automated workflow built using Extension Kit.
Extension Flow	Automated workflow that connects applications and Services together. Each Extension Flow consists of a trigger and one or more actions.
Extension Kit	Unit4 Extension Kit is a cloud based, Multi-Tenant solution operated by Unit4 that provides a toolkit allowing Users to extend the capabilities of Unit4 products and integrate with other systems.
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	Data Base User used for an early access enablement.

Term	Definition
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 Platform Services solution, housing multiple Tenants, where Tenants are physically integrated, but logically separated.
Platform Service	The Platform is a set of core services that underpins the application providing services such as workflow, reporting, secure data access and API framework.
Record	A data record stored within a Customer's database (for example a line in a timesheet).
Sendgrid Services	A Third-Party Service provider that Unit4 by default uses to send emails from Unit4 ERPx system. Sendgrid Services can be replaced by the Customer's SMTP configuration, on demand.
Task focused Applications (aka Task Focused Apps)	Applications delivered as Feature Services focused on accomplishing one or a set of concrete tasks.
Tenants	Customer logically separated spaces designed to fulfil Customer business needs via the Unit4 ERPx capabilities.
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)
ERP	Enterprise Resource Planning
FTE	Full Time Equivalent
HTTPS	Hypertext Transfer Protocol Secure
IDP	Identity Provider
Kbps	Kilobits Per Second
NPE	Non-Production Environment
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

*Notable Changes from V 2025Q2

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

- General functional and technical requirements and specifications added to Chapter 7
- Added Chapter 11 – List of Platform Services, including additional information for Customer visibility.