UNIT4
In business for people

Unit4 FPM

Unit4 Cloud Service Description

VERSION 1.3

March 2024

CONTENT

1. Introduction

Unit4 FPM is a powerful corporate reporting system that handles consolidation, liquidity planning, reporting and analysis. The product has a desktop and a web interface that both uses the same SQL Server data source.

The purpose of this document is to describe the cloud service composition provided to the Customer.

Unit4 provides a complete technically managed solution for Unit4 FPM 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 Software as a Service: Unit4 SaaS - a software as a service delivery model deployed on Microsoft Azure. This model leverages of Microsoft Azure's scale and experience of running highly secure and compliant cloud services around the globe. Microsoft Azure's infrastructure is second to none in terms of physical and electronic security, and it adheres to industry standards such as ISO 27001, SOC 1 & 2, PCI DSS and many more.

Unit4 FPM is available as a shared option, where computing resources are shared between Customers without any interferences.

In summary, Unit4 provides the following:

- Full deployment of Unit4 Products, including any required administration desktop client (optional), web client and Unit4 FPM API/web services.
- All user access to Unit4 FPM is over secure internet connections (HTTPS). A variety of browsers are supported.
- Comprehensive integration options available, including the use of Unit4 FPM batch file-based interfacing, and API (for export of data).
- Relevant security level.
- Continuous monitoring is in place, covering servers, services and applications, feeding alerts and continuous improvement.
- Application of all updates, patches, Hot Fixes to Unit4 and other supporting software.
- Production and Non-Production Environments with a separate database for your data.
- Forgiveness restores (where applicable), plus disaster recovery in a physically separate secondary site.
- Service Level Agreement, with service credits based on service availability.
- Unit4 Community4U to engage with Unit4 directly, giving insight in the service performance indicators and see the status of services.
- *Formal policies in place for: information security, data processing, disaster recovery, business continuity and acceptable / fair use.*

2. Data centers & data residency

Unit4 SaaS use the Microsoft Azure infrastructure and platform services to deliver the Unit4 SaaS. These services are delivered from within different geo-political 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 geo-political zones, along with the data center locations. For more information, see Azure region details: azure.microsoft.com/regions

Geopolitical zone	Provider	Data location (Countries/City's/Regions)	Time zone
Sweden	Microsoft Azure	Gävle and Staffanstorp	CET/CEST

Unless agreed in a deviation schedule the chosen deployment of the Customer will be as follows:

Customer residence	Geopolitical zone used	Available solutions
Sweden Norway Denmark Finland	Sweden - Azure	All

3. Service model

Unit4 FPM is available in one main model:

- in a shared deployment model

In summary form the characteristics of the model is as per table below:

Category	Component	Characteristics
SOLUTION	All patching, updates of the standard solution (technical)	Included and automatic
INFRASTRUCTURE	Environments included	1 Production + 1 Non-Production
	Transactional storage (e.g., database)	50 GB
	Availability guarantee	Yes
SERVICES	Releases will commence	Automatically, with possibility to defer
	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

Category	Component	Characteristics
COMPLIANCE	Compliance certificates and assurance documents – Microsoft Azure	SOC1 Type II (ISAE 3402), SOC2 type II (ISAE 3000), ISO27001, ISO27017[1]

4. Environments

Two (2) environments are provided, including:

- One Production Environment (PE) called alternatively "live" environment, being the environment that the Customer uses to run the day to day (live) operation; and
- One Non-Production Environment (NPE) called alternatively test environment, being the Customer's Preview environment always containing the latest updates for the Unit4 Product in use by the Customer

Unit4 assigns to every Customer a unique 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. The Customer ID codes are created at Unit4 discretion during the early stage of the implementation and are not a subject to change.

People Platform Services

Unit4 People Platform services are Multi-Tenant, shared services. Except where explicitly stated in the service's Service Description, each Unit4 People Platform service has a Preview instance and a Production instance; there is no concept of Customer specific instances of Unit4 People Platform services. As such, no additional instances of Unit4 People Platform services are provided.

4.1 Production Environments

Only the Production Environment (PE) is subject to the Service Level Agreement.

[1] Unit4 FPM is compliant with mentioned standards to give Customers confidence that the highest levels of security and data protection practices will be met and allows Customers to streamline their own compliance with regulatory and industry standards. 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.

4.2 Non-Production Environments Characteristics

Although a Non-Production Environment (NPE) is not a subject to the SLA, NPEs have some characteristics as described below.

Users accessing an NPE

NPEs are configured to handle a maximum of 15 concurrent Users.

Customer responsibilities

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 PE.

Update of an NPE to a new Update

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

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.

Restores

A restore request can be made by issuing a Service Request in the Unit4 Community4U. Throughput time, amount of included restores and the charge is same to a refresh of a NPE. Please note there is no Customer specific restore option for Unit4 People Platform Services.

Suspension

NPE which is not actively used will be suspended. Suspended NPE may be reactivated at any point in time. In order to reactivate suspended NPE Customer needs to initiate re-activation, which may take up to 15 minutes.

4.3 Database refresh

Definition of Database Refresh Between Environments

A refresh between environments (e.g., from NPE to PE) is a full copy of Customer database between the environments. Refresh of the data stored outside of the database has to be explicitly specified in the Service Request.

There is no database refresh option for Unit4 People Platform Services.

Point in time used

The database refresh is from a point in time prior to the current Business Day. The specific point in time is selected by Unit4.

Frequency of database refresh

One refresh per environment per month is included. Additional refreshes would be extra charged.

Different environment Release versions

Database refresh is possible when:

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

How to request a refresh?

Customers can use self-service to proceed with refresh.

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

5. Reporting and monitoring

5.1 Reporting on Service Performance

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

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

6. Releases and updates

Periodically, Unit4 introduces new features in Unit4 FPM including enhanced features and functionality across applications. Features and functionality will be made available as part of a Release. As part of regular maintenance Unit4 will apply Updates, Patches and Hot Fixes, as deemed necessary by Unit4 to maintain the existing features of Unit4 SaaS and to maintain service level commitments and security.

Releases and Updates will be provided free of charge as part of the Service. However, it should be noted:

- Any Releases or Updates 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 Unit4 SaaS and would be chargeable.

6.1 Release deployment

Releases take place 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 of that time (such unavailability shall not be counted as service downtime for the calculation of Service Availability). A schedule of planned deployment of Releases to the Production environment will be published on the Unit4 Community4U. A Customer's Preview Environment always contains the latest updates for the Unit4 SaaS solution in use by the Customer. Unit4 will use reasonable endeavors to ensure that Releases will be carried out during the Planned Maintenance window.

[APPLICABLE FOR UNIT4 PEOPLE PLATFORM SERVICES]

Given the foundational nature of the Unit4 People Platform services, releases of Unit4 People Platform services occur more frequently than end user facing aspects of Unit4 business solutions. Unit4 People Platform service releases are deployed in a transparent manner and result in no downtime. As such, Unit4 People Platform service releases can be deployed outside of Planned Maintenance windows. In rare cases when downtime is necessary, the release will be performed during a Planned Maintenance window. Details regarding changes contained in a Unit4 People Platform service release can be found on the Unit4 Community4U as soon as the release has been deployed. Releases of Unit4 People Platform services cannot be deferred.

6.2 Hot Fix and Patch Deployment

Hot Fixes and patches are applied as deemed necessary by Unit4 in order to maintain the existing features of Unit4 SaaS as well as maintaining service level commitments and security.

Please note there is no concept of an update to Unit4 People Platform services. All changes to a Unit4 People Platform service are considered a release of the service.

7. Planned and unplanned maintenance

7.1 Planned Maintenance

Planned Maintenance windows are dedicated to apply to all the respective changes to the Service provided e.g. updates, hot-fixes 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)** *Releases, Hot-Fixes and Infrastructure updates*	**Additional** **Planned Maintenance windows (PMW)** *Releases*
All regions (except Azure US, Azure Canada)	12 per year, 3rd or 4th week of each month From: Sat 4PM To: Sun 4AM UTC	4 per year according to time interval specific for given region *(unless communicated otherwise)*

Time of Planned Maintenance window is a subject of a change (+/- 1hr), 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 6hrs, unless they are promoted to extended Planned Maintenance windows, these take up to 12hrs.

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 endeavors 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 paying 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 off, or the security of 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:

Monitor PE availability and Service Response Time on an active basis using a third-party monitoring service. Monitoring acts as a consumer of Unit4 SaaS and is subject to any and all present and future Usage Restrictions of Unit4 SaaS. Customer and Unit4 must agree, prior to monitoring, on monitoring details in order to ensure that the monitoring does not interfere with Unit4 SaaS offering and that Unit4 SaaS security tooling does not block the monitoring service.

1. Conduct an external security vulnerability scan on an annual basis. Details of the planned scan must be provided to Unit4 at least 30 days in advance of each scan using a Service Request.

2. Conduct a security penetration test on an annual basis. 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

Release and Service Updates

The following list summarizes typical Release and/or Update tasks and indicates services included as part of Unit4 SaaS and tasks that are the responsibility of the Customer (or by Unit4 Professional Services/partner at 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's 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	✓	✓

Technical & functional responsibilities

Technical Environment responsibilities:

- Supply, administration and maintenance of customer-side client 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.

Functional Environment responsibilities:

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

8.3 Customer Obligations

Account Set-up

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 requirement to comply with Unit4's acceptable use policy (www.unit4.com/terms). Where applicable each individual User must establish an Account. 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 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 SaaS and managing Customer's Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer's behalf concerning 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 his or her 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 Unit4 SaaS or its Users' Accounts and will provide all information and take all steps requested by Unit4.

9. Customisations and integrations

Integrations are permitted and can be written by Unit4 or Unit4 partners and to some extend by the Customers themselves. Maintenance, support, implementation and update considerations for integrations are not included in the Service fee. The Customer has sole responsibility for the 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. If any assistance is required regarding integration work, Unit4 may be able to assist with resolving issues, but this will be subject to review and extra charge. Customer will be required to purchase Professional Services at Unit4's or partner's Prevailing Rates.

9.1 Customisations

Unit4 FPM does not support any Customisations, only configuration is applicable.

9.2 Permitted tools

The following Custom report tools are permitted:

- Unit4 FPM Excel add-in - Installed on local desktop of the Customer.

9.3 Unit4 APIs backward compatibility

Unit4 recommends using the most recent version of the Unit4 FPM APIs in order to receive optimum performance and stability. Unit4 FPM API's always follow the current version. All breaking changes in the Unit4 FPM API's will be noted in the Unit4 FPM release notes, a document published for each new release on the Unit4 Community.

9.4 Integrations

Integrations are permitted according to the supported integration methods described below. Integration methods not explicitly stated below are not permitted.

Integration Type	Available?
Integration with Unit4 ERPx, where Unit4 ERPx financial and meta data are extracted by Unit4 FPM.	Yes
Integration with Unit4 ERP 7, where Unit4 ERP 7 financial and meta data are extracted by Unit4 FPM.	Yes
Integration with latest Unit4 Financials, where Unit4 Financials financial and meta data are extracted by Unit4 FPM.	Yes

Other integration options:

Integration Type	Permitted?
Integrations using Unit4 FPM Export API	Yes
Integration using import files over SFTP imported by Unit4 FPM integration modules or batch jobs [1]	Yes

Notes:

1. (Paid option) Achievable also via folder access on remote desktop client that is restricted to nominated administrative users(Data Export, Data Import and Logs folders).

10. Technical operations

10.1 Printing

All printing is carried out on the client side.

10.2 Direct Database access

Direct database access cannot be provided.

10.3 Connectivity

Access to the web client is delivered over the public internet using an HTTPS connection (RSA 2048 bits - SHA256 with RSA and/or EC 256 bits SHA256 with ECDSA). Access to the Desktop client is carried out using a 2048 bit encrypted thin client connection over TLS with SHA-2 RSA Encryption Algorithm over the public internet.

Internet bandwidth suggestions*

Unit4 FPM web client – 512 Kbps per User
Unit4 FPM desktop client – 512 Kbps per User

- Latency Recommended: at most 50 ms

* Rough guidance only based on simulation testing. Response times will be dependent upon a variety of factors such as number of Users, type of web processing initiated, Customer-side internet line capacity and infrastructure set-up such as use of proxies.

10.4 Solution access

The Unit4 FPM solution is accessed in the following manner:

- Unit4 FPM web client accessed via a supported web browser.
- Unit4 FPM desktop client installed on user's workstation (default offering).
- Unit4 FPM desktop client accessed as a remote application via a remote access solution (e.g. Citrix Workspace APP) as a paid option.
- Programmatic access to Unit4 FPM API

10.5 Authentication

By default, authentication for Unit4 FPM (desktop and web client) is carried out using application-based username and password authentication. Management of users and passwords within Unit4 FPM application is the responsibility of the Customer.

The Unit4 Cloud Services 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. In case the customer is using any other Unit4 Services which uses Unit4 IDS for authentication purpose, Unit4 IDS is required to use for Unit4 FPM.

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 IDS Service Description at www.unit4.com/terms.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 of Unit4 IDS.

Unit4 FPM desktop client (via Citrix Workspace Application) authentication involves two steps; first step is to authenticate using Unit4 Cloud specific credentials against a Unit4 Cloud operated Active Directory and second step using either Basic or Federated Authentication. FPM desktop client accounts are managed by the customer through Citrix self-service and Unit4 FPM users are managed by the customer within the application. Currently, federated authentication is not supported for Unit4 Property Management desktop client on Unit4 Cloud.

10.6 FPM Desktop client

Desktop Client, understood as Unit4 Services is a desktop client installed on user's workstation (default offering) or accessed as a remote application delivered via a remote access solution (e.g. Citrix Workspace Application) as a paid option.

10.6.1 Microsoft office components

Unit4 Cloud provide an access (as a paid option) for Unit4 FPM users to selected Microsoft Office products in order to:

- open attachments from within Unit4 FPM desktop client
- export to Excel within Unit4 FPM desktop client
- edit Other Data Reports in Excel format stored in Unit4 FPM
- open documents/files from data import

The products in scope are as follows:

- Microsoft Excel (English) – Included in the "Extra Desktop Client" subscription option if purchased (license per purchased user).

10.6.2 Supported extensions on Citrix

Unit4 Cloud supports following files to be opened via Citrix:

- Excel spreadsheets (.xls .xlsx .csv) via Microsoft Excel;
- Images (.png .jpg .bmp) via Microsoft Paint
- Text files (.txt .log) via Microsoft Notepad
- PDFs (.pdf) via Adobe Reader

Any other file types not described here must be copied over and opened on local workstation.

10.6.3 Citrix Self-Service

Citrix self-service gives Customers ability to create, activate and deactivate accounts, manage accounts permissions and resetting passwords. It enables Customers to manage their Citrix Users without a need to request Unit4 assistance. Access to Citrix self-service is limited to Users with User Manager role.

For security reasons, accounts inactive for 60 days are automatically disabled, but can be reactivated in the Self-Service portal. After 360 days of inactivity accounts are permanently deleted and have to be recreated if needed.

10.7 Technical overview

Topic	Description
FTP	
Protocol	SFTP protocol is used with AES256-SHA2 cipher
Credentials	One set of credentials are provided per environment (e.g. 1 username/password for production, 1 username/password for each NPE)
Email	
Domain	Unit4 FPM provides basic e-mail functionality for sending messages to recipients with default Unit4 domain, which on request can be configured with custom domain. In case the Customer requires more advanced features (e.g., bounce back emails, DKIM support, IMAP support), Unit4 products can use Customer's own email servers, if they are reachable by Unit4 SaaS.
Protocol	SMTP over TLS
Authentication	
Protocols supported	WS-Federation, SAML-P and OpenID Connect support (see Unit4 IDS Service Description) and application specific credentials
Internet communication	
Protocols supported	HTTPS secured with TLS with RSA SHA256withRSA encryption and/or EC SHA256 with ECDSA

11. Data considerations

11.1 Transfers of Customer Data to Unit4 FPM

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 Unit4 SaaS.

When Customer requests to copy a database snapshot from outside of Unit4 Cloud to either PE or NPE then it should be free of any Customization objects. These objects should be sent in a separate Service request and will follow standard Customization review process.

11.2 Backup and Restore Services

Customers are given the option of a “forgiveness” restore, where a recent PE 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 in 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.

There is no “forgiveness” restore option for Unit4 People Platform Services.

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

Customer may request a Service Restore report no more frequently than once per month via the Unit4 Community4U using a Service Request. Example:

11.3 Data Security

Data in transit

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

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

IP Allowlisting is offered as an option that will come at an additional cost in Unit4 SaaS, as a means to gain an extended level of control on who 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.

IP Allowlisting is available for the following product – data center – cloud type combinations.

Whitelisting	Data center	Available?
Web endpoints	Azure	Yes

Customer needs to provide VPN access to their own network for Partners or Unit4 consultants working off network (to allow remote working).

The People Platform Services like Unit4 Identity Services, Unit4 Wanda and Unit4 Extension Kit use dynamic IP addresses, there for IP Allowlisting is not supported for any combination of Global products with any People Platform Services.

Security

Connection is secured via TLS and firewall rules that limit connectivity by IP address. Firewall rules are maintained by Unit4 and each change must be requested via Service Request in support portal.

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 shared resources. When a limit is exceeded, corrective measures will be taken.

Please see Unit4 Fair Usage Policy at www.unit4.com/terms for more details.

Limit – API (Export of data)

To ensure smooth service performance and provide all customers with a consistent experience, Export API requests have a maximum timeout of 5 minutes. If an API request doesn't receive a response within this period, it will be automatically terminated.

Limit – Saving actions

It is recommended to not have more than 60 saving actions by concurrent users per minute. One saving action is:

for Administration modules: one "Save" per user/module
for Data Input and Consolidation modules: one "Save" per user/module/ company/version/period

This can be monitored in the Activity Report – Log Report.

11.5 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 clients, desktop client).
Application reporting tools.
Application functionality to export to file.
Export API.
Upon Agreement termination Customer Data can be retrieved by Customer in accordance with the Agreement.

SCHEDULE A
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).

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 Customer identifier.
Customisation Object	the product of any Customisation being any code change (for example AG16 or ACT) or other database object not created using the changing of standard Unit4 Product menus and functionality.
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 it takes Unit4 to perform the restoration of a recent Production Environment back-up (at the request of the Customer).
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
FTP	File Transfer Protocol
HTML	Hyper Text Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IdP	Identity Provider
Kbps	Kilobits Per Second
NPE	Non-Production Environment

Acronym	Full Name
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
TLS	Transport Layer Security Encryption
URL	Uniform Resource Locator (a web address)
VPN	Virtual Private Network
WIP	Work In Progress
XML	Extensible Markup Language