



Unit4 FP&A

Cloud Service Description

Version 1.4

May 2020



CONTENT

CONTENT	1
1. Description.....	2
2. Data centers & data residency	3
3. Service model	5
4. Environments.....	6
5. Reporting and monitoring.....	8
6. Releases and updates	8
7. Planned and unplanned maintenance.....	10
8. Customer permissions and responsibilities	10
9. Customizations, integrations, custom reports and fields.....	13
10. Technical operations	14
11. Data considerations.....	16

1. Description

Unit4 FP&A provides everything you need to transform disparate sources of financial data into actionable business intelligence. An extensive library of template-driven content makes it easy for power-users and end-users to create bespoke analyses, reports, charts, KPI dashboards and simulation models for particular sectors or specialist fields with speed and agility.

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

Unit4 provides a complete technically-managed solution for Unit4 FP&A 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 FP&A is available as a shared option (default), where compute resources are shared between customers without any interference and a dedicated option (on Microsoft Azure only) where compute resources are dedicated to a single customer.

In summary, Unit4 provides the following:

- Full deployment of Unit4 Products, including any required administration desktop, web client and mobile web sites and API's/web services.
- All user access to Unit4 FP&A is over secure internet connections (HTTPS). A variety of browsers and mobile platforms are supported. There is an Azure ExpressRoute option to provide a private communications channel.
- Comprehensive integration options available, including the use of Unit4 API's/Web Services, batch file-based interfacing and SQL read-only access to data (Dedicated option).
- Infrastructure is fully scalable, in a high availability environment with redundancy in critical aspects such as power, hardware, network communications.
- Firewalls, anti-virus and access controls.
- 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 in service performance indicators and see the status of services.

- Various Azure regions leveraged to enable Unit4 to meet your data residency needs; your data always resides within a specified a geo-political zone (except where explicitly stated otherwise).
- Formal policies in place for: Information Security, Data Processing, Disaster Recovery and Business Continuity and Acceptable Use

2. Data centers & data residency

Unit4 Global Cloud Services use the Microsoft Azure infrastructure and platform services, and Nordic data center (Conapto AB) 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 and Nordic data center (Conapto AB) details on www.conapto.se.

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 Iowa (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	Victoria and New South Wales (DR)	AEDT/AEST
Norway	Microsoft Azure	Stavanger and Oslo (DR TBD)	CET/CEST
Sweden	Nordic data center (Conapto AB)	Sätra and Sollentuna (DR)	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
APAC	Asia	All
Australia/New Zealand	Australia	All
Canada	Canada – Azure	All
EU	EU – Azure	All
Sweden	Nordic data center (Conapto AB)	Unit4 ERP 7 and Unit4 FP&A
Norway/ Denmark	Norway – Azure	All
UK	UK – Azure	All
US	US – Azure	All

In the unlikely event the primary and secondary redundancy of the network in a Geopolitical zone fails, connections are rerouted using tertiary redundancy in the following way.

Primary	Secondary	Tertiary
Geopolitical zone EU	Geopolitical zone EU	Geopolitical zone UK
Geopolitical zone UK	Geopolitical zone UK	Geopolitical zone EU
Geopolitical zone USA	Geopolitical zone USA	Geopolitical zone Canada
Geopolitical zone Canada	Geopolitical zone Canada	None
Geopolitical zone Asia	Geopolitical zone Asia	Geopolitical zone Australia
Geopolitical zone Australia	Geopolitical zone Australia	Geopolitical zone Asia
Geopolitical zone Norway	Geopolitical zone Norway	TBD

3. Service model

Unit4 FP&A is available in 2 main models:

1. Unit4 FP&A SaaS shared in a shared deployment model; and
2. Unit4 FP&A SaaS dedicated in a dedicated deployment model.

Unit4 FP&A SaaS dedicated provides the same service offering as the shared cloud option with the distinction that computing resources are not shared with other Unit4 customers, such that computing resources are dedicated to a single customer. The dedicated deployment option is not available for the Unit4 people platform services, these are always shared (Unit4 People Platform services are multi tenant).

Category	Component	Shared	Dedicated
SOLUTION	Release Upgrade elasticity: Ability to defer a Release for 6 months (maximum)	Yes	
	All patching, updates of the standard solution (technical)	Included and automatic	Included and automatic
INFRASTRUCTURE	Environments included	Preview + Production	Preview + Production
	Storage (Documents)	250GB	250 GB
	Availability guarantee	Yes	Yes
	Response time guarantee	No	No
	Data Centers	Microsoft Azure and Nordic data center (Conapto AB)	Microsoft Azure
	Dedicated deployment	No	Yes
SERVICES	Releases will commence	Automatically	Automatically
	On-going technical operations, performance management, maintenance of all	Yes	Yes

Category	Component	Shared	Dedicated
	infrastructure components, monitoring alert response and issue resolution		
	Backup & Restore services	Yes	Yes
	Disaster Recovery	Yes	Yes
	Monitoring program of infrastructure and application	Yes	Yes

4. Environments

Unit4 FP&A

Two (2) environments are provided, including:

- one Cloud Production Environment (or “live” environment) being the environment that the Customer uses in day to day (live) operation; and
- one non-production environment (or “preview” environment) which can be used as test, QA, pre-production or acceptance environment or for training purposes).

A Customer's preview environment always contains the latest updates for the Unit4 Product in use by the Customer. Additional environments can be provided at an extra charge.

People Platform Services

Unit4 People Platform services are multitenant, 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 Cloud Production Environment (PE) is subject to the Service Level Agreement.

4.2 Non-Production Environments Characteristics

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

Definition of an NPE refresh from or to PE

A refresh of an NPE from PE encompasses:

- The restore of transactional database(s)
- The restore of non-transaction data store
- Copy of most recent 90 days of documents or the most recent 2Gb of documents, whichever results in greater amount of documents (blob store)
- Custom report templates (e.g. Purchase order template, invoice template, etc.)
- Report output from last 90 days. There is no NPE refresh option for Unit4 People Platform Services.

Point in time used

The NPE refresh is from a point in time prior to the current business day. The specific point in time is selected by Unit4.

Frequency of NPE refresh from or to PE

Where the PE and NPE environment are at the same Release level or at the different Release levels, one refresh per NPE per month is included.

Additional requests will give an extra charge per refresh per NPE.

How to request a refresh?

Refreshes must be submitted to Unit4 by a Named Support Contact using a Service Request on Unit4 Community4U.

Throughput time

A NPE refresh from PE will be available for use at the start of the second business day following the Service Request acceptance (depends on the contracted support level).

Users accessing an NPE

NPEs are configured to handle 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 environment will be erased and replaced with a fresh copy from PE; same reports as in PE, same data as in PE, etc.

Update of an NPE to a new Update

The Preview (NPE) 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 geo-political 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 on 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.

5. Reporting and monitoring

5.1 Reporting on Service Performance

Unit4 provides operational information regarding Unit4 FP&A on Unit4 Community4U. That information includes:

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

5.2 Monitoring program

A continuous 24x7x52 monitoring and resolution program is in place to detect and resolve incidents to meet the Service availability and response time targets.

The monitoring covers availability.

6. Releases and updates

Periodically, Unit4 introduces new features in Unit4 FP&A 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 and Hotfixes, as deemed necessary by Unit4 in order to maintain the existing features of the Service 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 the Unit4 FP&A Service and would be chargeable.
- Where any Release or Update 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 charge a reasonable fee to provide assistance to the Customer to the extent any such Release or Update replaces or updates any Customisation or non-standard functionality utilised by Customer and Customer wishes to maintain the previous Customisation or non-standard functionality.

6.1 Release deployment

Releases may take place approximately each quarter. 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 of Unit4 FP&A in use by the customer. Unit4 will use reasonable endeavours 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 Update Deployment

Updates are applied as deemed necessary by Unit4 in order to maintain the existing features of Unit4 FP&A as well as maintaining service level commitments and security.

An update calendar per Geopolitical zone will be released at least 4 weeks before an update commences on preview. The Production environment will follow no sooner than 9 weeks after the update announcement. Updates are not capable of being deferred.

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.

6.3 Hotfix Deployment

Hotfixes are applied as deemed necessary by Unit4 in order to maintain the existing features of the Unit4 FP&A 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

Currently, the Planned Maintenance window is from Saturday 18:00 to Sunday 06:00 CET/CEST on the 4th week of every month. For Nordic Data Center the Planned Maintenance window is Monday from 20:00 to Tuesday 03:00 CET/CEST every week. Next to that a Planned Maintenance Window might be planned twice (2x) in a 12 months period to deploy a software Release from Saturday 18:00 to Sunday 06:00 CET/CEST. The Production Service may be periodically unavailable at this time. Planned Maintenance windows are subject to change upon reasonable notice.

The exact dates of Planned Maintenance windows are communicated in the Unit4 Customer Portal.

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 penalty.

7.2 Unplanned Preventative Maintenance

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

8. Customer permissions and responsibilities

8.1 Customer permissions

Customer has the right to:

- 1) Monitor PE availability and Service Response Time on an active basis using a third-party monitoring service. Monitoring acts as a consumer of Unit4 FP&A and is subject to any and all present and future Usage Restrictions of Unit4 FP&A.

Customer and Unit4 must agree, prior to monitoring, on monitoring details in order to ensure that the monitoring does not interfere with the Unit4 FP&A offering and that Unit4 security tooling does not block the monitoring service.

- 2) 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.
- 3) 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 FP&A and tasks that are the responsibility of the Customer (or by Unit4 Professional Services at an extra charge):

Task	Included	Customer Responsibility
Project Planning		
<ul style="list-style-type: none"> • Publishing general availability schedule of Releases on the Unit4 Community4U 	✓	
<ul style="list-style-type: none"> • Managing timelines, outline goals, roles and responsibilities 		✓
<ul style="list-style-type: none"> • Business analysis and discovery 		✓
<ul style="list-style-type: none"> • Creating test plans 		✓
Release deployment in Preview environment		
<ul style="list-style-type: none"> • Update Preview environment with Release 	✓	
<ul style="list-style-type: none"> • User training on changes 		✓
<ul style="list-style-type: none"> • Test: conducting basic Release testing 		✓
<ul style="list-style-type: none"> • Training support to assist with testing 		✓

Task	Included	Customer Responsibility
<ul style="list-style-type: none"> Functional and user acceptance testing as desired 		✓
<ul style="list-style-type: none"> Training, implementation and Configuration for new features 		✓
<ul style="list-style-type: none"> Reviewing test scripts and testing outcome for issues resolution 		✓
<ul style="list-style-type: none"> Go/No-go criteria's and agreement on Production Release deployment timing 		✓
Release deployment in Production		
<ul style="list-style-type: none"> 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. 	✓	✓
<ul style="list-style-type: none"> 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 (see Unit4 Solution Specific Service Description Connectivity section).
- 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 FP&A 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 the Service and managing Customer’s Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer’s behalf concerning the Unit4 FP&A, 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 in Unit4 FP&A SaaS or its Users’ Accounts, and will provide all information and take all steps requested by Unit4.

9. Customizations, integrations, custom reports and fields

9.1 Customizations and customer reports

Unit4 FP&A does not support any customizations, only configuration is applicable.

9.2 Integrations

Integrations, defined as any solution capability that shares data with an external, are permitted according to the guidelines described below. Interface methods not explicitly stated below are not permitted. In general, no direct database access is permitted at all.

Integration Type	Permitted?
Integration with Unit4 ERP 7 where Unit4 ERP 7 financial data, intercompany data, cash data and metadata are extracted by Unit4 FP&A	Yes
Integration with latest Unit4 Financials supported version, where transactions at detail or summary level from Unit4 FP&A with drill-back to Unit4 Financials.	Yes

Integration Type	Permitted?
Integration with Unit4 Student Management	Yes

10. Technical operations

10.1 Printing

All printing is carried out on the client side.

10.2 Connectivity

Unit4 FP&A is accessed via the OneClient and RichClient over the public internet using an HTTPS connection (RSA 2048 bits - SHA256 with RSA and/or EC 256 bits SHA256 with ECDSA).

The Unit4 FP&A RichClient and the Microsoft Office Add-Ins needs to be installed locally on site.

Internet bandwidth suggestions*

- Unit4 FP&A OneClient – 32 Kbps per user
- Unit4 FP&A RichClient – 128 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.

** For more information, please refer to Unit4 FP&A System Requirements document.

Virtual Private Network

Unit4 can provide an optional VPN (IPsec) connection as an option only for Microsoft Azure deployments.

Client device terminating the VPN connection has to fulfil following requirements:

- Be on the list of supported hardware for Route Based VPN:
<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices>
- Support Network Address Translation (NAT) to limit the networks on customer side to one network with maximum 24-bit mask
- Provide, at minimum, support for VPN settings listed below:

IKE version	IKE v2
IPSec Keying Mode	PSK
IKE Phase 1 – Encryption Algorithm	AES 256
IKE Phase 1 - Authentication	SHA 256
IKE Phase 1 – DH Group	At minimum DH14

IKE version	IKE v2
IPSec Phase 2 – Encryption	AES 256
IPSec Phase 2- Authentication	SHA 256

10.3 Technical overview

Topic	Description
FTP	
Protocol	SFTP (SSH FTP) protocol is used
Credentials	Two sets of credentials are provided per environment (e.g. 2 username/passwords for production, 2 username/password for each NPE)
Email	
Domain	Unit4 FP&A needs an SMTP Server to send eMails. By default, Unit4 mailsystem can be used, but the sender email address is limited to noreply@FP&A.cloud. Optionally the customers SMTP Server can be used.
Protocol	SMTP over TLS
Authentication	
Protocols supported	By default, authentication for Unit4 FP&A (OneClient) is carried out using application-based username and password authentication. Management of users and passwords within Unit4 FP&A application is the responsibility of the customer. Unit4 FP&A supports authentication via Unit4 Identity Services (IDS). IDS is a federated authentication gateway, authentication is performed at the customer's own IdP. Unit4 IDS supports WS-Federation, SAML-P and OpenID Connect support (see Unit4 IDS Service Description).
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 FP&A

Unit4 deploys 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 Unit4 Global Cloud Service.

When customer requests to copy a database snapshot from outside of Unit4 Cloud environment 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 Production Service 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 Customer Portal using a Service Request. Example:

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

11.3 Data Security

Data in transit

Customer Data in transit is protected with latest TLS encryption levels.

Customer Data at rest

Except for Unit4 FP&A SaaS Dedicated and cloud delivery in the Nordic data center (Conapto AB), data at rest is protected using transparent, whole database encryption (e.g. transparent data encryption, and/or whole disk data encryption). When selecting Unit4 FP&A SaaS Dedicated or deployment in the Nordic data center an extra fee will be applied to have

whole database encryption. Please see the Unit4 Information Security Policy, which is available at www.unit4.com/terms.

Whitelisting

IP Whitelisting is offered as an option that will come at an additional cost in the Unit4 Global Cloud Service, as a means to gain an extended level of control on who has access to their environment. An IP whitelist is a list of IP addresses that are granted access to a certain Service. When an IP whitelist is used, all IP addresses are denied access, except those included in the IP whitelist.

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

Whitelisting	Product	Data center	Cloud Type	Available?
Web endpoints	U4FP&A	Azure,	All	Yes
Web endpoints	U4FP&A	Nordic	All	No
When using People Platform Services whitelisting will not work due to dynamic URLs.				

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 Whitelisting is not supported for any combination of Global products with any People Platform Services.

11.4 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:

- Unit4 FP&A (OneClient), accessed via a supported web browser
- Unit4 FP&A (RichClient), can be setup:
 - - locally, setup files can be requested via Support Portal. access via Citrix
 - - optional service via Citrix

11.5 Data staging area

Staging database is a separate service provided based on the Microsoft Azure SQL database engine. That database can be used for storing any kind of staging data. Unit4 FP&A can query data via a SQL dynamic area and present it within the application. The database will be open to access for uploading to and downloading from UNIT4 FP&A.

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.

Size(performance):

It is offered as single database for each environment with 50 database transaction units (DTUs) and 250GB storage included.

User Management:

Unit4 offers the database and the necessary access and credentials to work with this database. One administration account will be created and credentials will be shared with a customer. The ~~customer~~ customer can create more users, if required. SQL database user management is a customer responsibility.