Unit4 T&E v7

Unit4 Cloud Service Description

Version 7

2026

Contents

1. Notice 2
2. Introduction 2
3. Data centres & data residency 3
4. Service Model 3
5. Environments 4
6. Reporting and monitoring 6
7. Releases and updates 6
8. Planned and Unplanned Maintenance 7
9. Customer permissions and responsibilities 8
10. Technical operations 11
11. Data considerations 12

SCHEDULE A 14

1. Notice

Please note that Unit4 T&E v7 is approaching end-of-life. From September 1, 2026, Unit4 T&E v7 will no longer be supported or maintained by Unit4.

2. Introduction

Unit4 T&E v7 is a software-as-a-service ("**SaaS**") build solution designed for people-centric organizations. It provides a fully integrated data model, processing model and reporting model, enabling our customers to manage their business processes related to time management, travel and expense management, and people planning.

The purpose of this Service Description is to describe the T&E v7 core Service. Details about additional Services, such as Unit4 Platform Services, can be found in relevant documents published on our website (www.unit4.com/terms).

Unit4 provides a complete technically managed solution for Unit4 T&E v7 deployed in the public cloud. This end-to-end service includes cloud infrastructure, system software, monitoring, management and maintenance, disaster recovery and Service updates.

Unit4 offers cloud enterprise solutions as a SaaS delivery model deployed in the TietoEvry Data Center. Unit4 T&E v7 operates efficiently within this framework, utilizing a shared model to optimize resource allocation.

In summary, Unit4 provides the following:

- Access to Unit4 T&E v7 over secure internet connections (HTTPS). A variety of browsers and mobile platforms are supported.
- Comprehensive integration options can be provided using the T&E v7 Public REST APIs
- Production and Non-Production Environments with a separate database for Customer Data.
- Service levels, with Service Credits based on Service Availability.
- Access to Unit4 Community (Community4U).

3. Data centres & data residency

T&E v7 is delivered using TietoEvry hosting services. These services are delivered from Norway, using a primary and a secondary location, in the locations detailed below, to meet service level commitments and disaster recovery needs. The specific location within Norway is at the discretion of Unit4 and can change from time to time. The table below contains details of the geopolitical zone, along with the data centre locations.

Geopolitical Zone	Provider	Data Location (Countries/Cities/Regions)	Time Zone
Norway	TietoEvry	Oslo, Gjøvik and Fetsund	CET/CEST

4. Service Model

Unit4 T&E is available in a shared deployment model. This means computing resources such as the web server and SQL server are shared with other Unit4 customers.

Category	Component	Shared
SOLUTION	Application releases and updates	No new features will be deployed. Only P1 defects will be addressed via updates.
	All patching and security updates	Automatic
INFRASTRUCTURE	Environments included	1 Production and 1 Non-Production
	Storage (Documents)	250GB

Category	Component	Shared
	Availability guarantee	Yes
	Data centres	TietoEvry Data Centre
	Dedicated deployment	No
SERVICES	Releases will commence	None, this Service is end-of-life
	Updates will commence	Automatically, but only updates addressing P1 defects will be made available
	On-going technical operations, performance management, maintenance of all infrastructure components, monitoring alert response and issue resolution	Yes
	Backup & Restore services	Yes
	Disaster Recovery	Yes
	Monitoring program of infrastructure and application	Yes

5. Environments

Two (2) environments are provided[1], including:

- One Production Environment called alternatively “live” environment, being the environment that the Customer uses to run the day to day (live) operations; and
- One Non-Production Environment:
    - Test – which can be used according to the Customer needs as “Test” / “Quality” / “Development” / “Pre-Production”.

Additional environments can be provided at an extra charge.

Production Environments

Only the Production Environment is subject to the service levels detailed in the Unit4 Service Terms – SaaS, available at www.unit4.com/terms. Production environment backups are made daily in the time zone of the geopolitical zone in use. Backups of the Production Environment are kept for 30 calendar days.

Non-Production Environments Characteristics

Although the Non-Production Environment does not benefit from the service levels noted above, the Non-Production Environment has some characteristics as described below. Backups of the Non-Production Environment are made daily in the time zone of the geopolitical zone in use. Backups of the Non-Production Environment are kept for 30 calendar days.

Database refresh

A database refresh between environments (e.g. from the Production Environment to the Non-Production Environment) is a full copy of the Customer database between the environments.

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

Customers are entitled to up to 12 database refreshes per environment in each calendar year.

Users accessing the NPE

The Non-Production Environment supports testing and UAT activities with limited concurrent user activity, and data processing volumes that are expected to be approximately 5% of the production workload. They are intentionally sized and configured differently from the Production Environment and are not designed to support production workloads, sustained high traffic, or business-critical operations.

6. Reporting and monitoring

Reporting on Service Performance

Unit4 provides operational information regarding the Unit4 T&E v7 via Community4U. This information includes:

- Scheduled Maintenance (times, dates per region)
- Release information and deployment schedules
- Incident(s) overview
- Site recovery status (in the event of disaster recovery plan initiation)

Monitoring Program

A continuous 24x7x52 monitoring and resolution program is in place to detect incidents to meet Service Availability.

7. Releases and updates

Unit4 T&E v7 is no longer actively maintained. Only P1 application bugs are addressed. Hotfixes are applied as deemed necessary by Unit4 in order to maintain the existing features of Unit4 T&E v7, as well as maintain service levels and security.

Update deployment

Updates are applied as deemed necessary by Unit4 to maintain the existing features of Unit4 T&E v7 as well as maintaining service levels and security. Service Updates may take place approximately twice per year. The frequency of Updates may be increased or decreased at Unit4's discretion. Updates may take up to twelve (12) hours to deploy, resulting in the Service being unavailable for some or all that time (such unavailability shall not be counted as Service downtime for the calculation of Service Availability).

A schedule of planned deployment of Updates to the Production Environment will be published on Community4U. Unit4 will use reasonable endeavours to ensure that Updates will be carried out during the Planned Maintenance Window (detailed below).

8. Planned and Unplanned Maintenance

Planned Maintenance

Infrastructure:

The infrastructure Planned Maintenance Window is scheduled for the second Thursday of each month.

Start Time: Thursday, 22:00 CET
End Time: Friday, 01:00 CET

Applications:

There is currently no recurring Planned Maintenance Window for applications. If a Priority 1 (P1) defect is identified, a maintenance schedule will be published on Community4U, and customers will be notified accordingly.

Unplanned Preventative Maintenance

Unit4 may carry out unplanned preventative maintenance if there is an urgent requirement to secure the stability or security of Unit4 T&E v7. Such action may be taken at the discretion of Unit4 in unforeseen and exceptional circumstances that require immediate resolution and cannot be postponed until the next Planned Maintenance Window. Unplanned preventative maintenance is counted as a Service Outage.

Service Notifications and Customer Communication

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

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

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

Unplanned incidents (such as outages) are communicated via email and Community4U. During global outages, components responsible for email delivery may be affected. If the service is unavailable, customers should check Community4U first—any active incident will be posted there.

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

9. Customer permissions and responsibilities

Customer permissions

Customer has the right to:

1. Monitor Production Environment Service Availability on an active basis using a third-party monitoring service. Any such third party is subject to any and all present and future usage restrictions of Unit4 T&E v7. Customer and Unit4 must agree, prior to monitoring, on monitoring details in order to ensure that the monitoring does not interfere with the Unit4 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.

Customer Responsibilities

Release and Service Updates

The following list summarizes typical Release and/or Update tasks and indicates services included as part of Unit4 T&E v7, as well as tasks that are the responsibility of the Customer:

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		✓
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		✓
Release deployment in Production		
• Update existing application Configuration, being all activities undertaken to set up application provided by the service which involve the use of standard menus and	✓	✓

functionality. There may be rare cases where it is not technically possible to determine the correct business Configuration; in these rare cases any tasks that must be completed manually are the responsibility of the Customer.		
• Update Production Environment with Release	✓	✓

Customisation update responsibilities

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

Technical & functional 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.

Functional Environment responsibilities:

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

Customer Obligations

Customisations, custom reports and integrations are permitted and can be written by Unit4, Unit4 partners or the Customer. Maintenance, support, implementation and update considerations for these custom components are not included in the Unit4 Charges. Customisations are not supported by Unit4. The Customer has sole responsibility for the Customisations, custom reports and integrations, as well as their maintenance and Unit4 has no responsibility to maintain compatibility or fix any problems resulting from the use of non-standard software. This includes any custom development or Customisation (including Unit4 delivered Customisation as part of a project implementation, bespoke code written by Unit4). If any assistance is required regarding Customisations and/or bespoke work, Unit4 may be able to assist with resolving issues or with upgrades of the Customisation, but this will be

subject to review and extra charges. The Customer will be required to purchase additional Services at Unit4's Prevailing Rates.

Account Set-up

Customer is responsible for designating its Authorised Users, and for ensuring that all Authorised Users are adequately trained and understand Customer's remote access. Where applicable each individual Authorised User must establish an account. Customer is responsible for managing its accounts and disabling an Authorised User's account when Unit4 T&E v7 access is no longer required, including immediately upon termination of such Authorised User's affiliation with Customer. Customer is responsible for its Authorised Users' acts and omissions and for all activities occurring under its Authorised Users' accounts.

Account Security

Each Authorised User is responsible for keeping his or her account credentials confidential. Authorised 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 T&E v7 or its Authorised Users' accounts and will provide all information and take all steps requested by Unit4.

10. Technical operations

Printing

All printing is carried out on the Customer's side.

Direct Database access

Direct database access cannot be provided.

Connectivity

Access to the web client is delivered over the public internet using an HTTPS connection.

Solution access

Unit4 T&E v7 is accessed in the following manner:

- Unit4 T&E v7 (web client) accessed via a supported web browser
- Programmatic access to Unit4 API

Authentication

Available Unit4 T&E v7 authentication options:

- Unit4 T&E v7 application credentials
- OAuth 2.0 authorisation
- SAML authentication

11. Data considerations

Backup and Restore Services

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

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

There is no “forgiveness” restore option available for other infrastructure components, such as data files or bin folders. The restore process is limited to the database itself.

Data Security

Data in transit

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

Customer Data at rest

Customer Data at rest is protected using disk data encryption.

Component lifecycle and security dependencies

All products, platform services, and infrastructure components used within the Unit4 ecosystem are subject to a defined product and component lifecycle. This applies to both Unit4-developed components and third-party technologies used to deliver the Service.

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

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

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.

Access to my data

The Customer Data is owned and controlled by the Customer and in accordance with Applicable Law.

To ensure the Customer has access to their Customer Data, the following options are available:

- Application functionality (Web client).
- Application reporting tools.
- Application functionality to export to file.
- APIs/web services.
- On termination of the agreement between Unit4 and the Customer, Customer Data can be retrieved by Customer in accordance with the Agreement (see the Service Terms – SaaS available at www.unit4.com/terms).

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

Term	Definition
Account Administrator	An appropriate and qualified representative of the Customer who will have administrative level control for creation, maintenance and deletion of accounts providing access to the Service.
Customisation Object	A T&E v7 customisation is any non-standard Unit4 T&E v7 solution configuration including its data queries and solution specific database objects such as tables, views, AG16 etc.
Localisation	A Service developed for strategic territories and verticals that secures legal, statutory and market standard requirements in that territory or vertical.
Multi-Tenant	A single instance of Unit4 T&E v7 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.

Acronym	Meaning
ACT	Advanced Customisation Tools (Unit4 ERP only)
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
API	Application Program Interface (e.g. Web Services)

ARC	Agresso Reporting Tool (Unit4 ERP only)
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
HTML	Hyper Text Markup Language
HTTPS	Hypertext Transfer Protocol Secure
Kbps	Kilobits Per Second
NPE	Non-Production Environment
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