UKG Workforce Central in the Cloud

Introduction

This technical paper is specific to the UKG Workforce Central™ suite hosted in either the U.S. or European Union (EU) UKG Private Cloud data center locations. Workforce management solutions from UKG (Ultimate Kronos Group) provide the complete automation and high-quality information you need to help control labor costs, minimize compliance risk, and improve workforce productivity. But your UKG™ solution can deliver continuous value only if it is available and managed properly over time. That's why more and more customers are choosing UKG in the cloud for deploying their workforce management solutions.

UKG can manage your workforce management solution in our private cloud, where users can access the applications over the web at any time, from anywhere.

You get 24/7 access to your solution without having to purchase additional hardware, operating systems, or RDBMS licenses. You also gain valuable peace of mind knowing that experienced UKG technical consultants are managing your applications and employee data. It is the ideal choice for organizations seeking to achieve their workforce management goals without exceeding their capital equipment budgets or placing additional demands on their in-house IT staff.

UKG provides comprehensive maintenance and support of your workforce management solution, including complete support of IT infrastructure comprising the server hardware, operating systems, and database systems required to run your UKG application(s) in the UKG Private Cloud:

- Server security and management
- Service pack installation
- Legislative update installation
- Software version installation
- Daily system and data backups
- Guaranteed 99.75% service-level agreement (SLA)

When evaluating any vendor's cloud services, you need to be confident that your application(s) and database are being maintained at a world-class data center facility engineered to incorporate multiple levels of security and redundancy, thereby ensuring maximum availability of your workforce management solution.

This document is intended to describe the infrastructure, services, processes, and policies behind the UKG Private Cloud, including:

- Data center specifications related to physical infrastructure, network connectivity, data communications, security, and more
- System backup and recovery processes
- Security policies and controls
- Change control
- Integration with customer data and application environment
- SLA policies and management
- Certifications and accreditations
- Technical support

Cloud offering – UKG Workforce Central

The following applies to single-tenant applications within the UKG Private Cloud.

Cloud Offering	
Environments: One standard production and one development (nonproduction) environment.	Included; more nonproduction environments are available for additional fees
Environment restoration: Restoration of production to one nonproduction environment once per week.	Included; more frequent restores or additional environments require a time-and-materials fee
Connectivity to service: The customer's users connect to the application via a secure connection over the internet. Cooperative efforts with customer IT staff may be required to enable access. UKG will assist with validating site connectivity, but assumes no responsibility for the customer's internet connection or ISP relationships. UKG-related internet traffic cannot be filtered by proxy or caching devices on the client network. Exclusions must be added for the fully qualified domain names and public IP addresses assigned to the environments.	Included
Device-initiated terminal connectivity: In the device-initiated mode of communication, the UKG terminal initiates all communications with the device manager server at the UKG Private Cloud over the internet. For this method, it is required that the customer open port 443 outbound. In cases where network address translation is required for terminals, the customer is responsible for applying the translations on its network.	Included
Remote access to non-web applications: Remote access to non-web applications (e.g., UKG Workforce Integration Manager™) using a remote access tool such as a Citrix receiver. Limited UKG applications require the use of these remote access accounts.	Two named users included
SFTP accounts: Provided to the customer to push files to the UKG Private Cloud and to pull files from the UKG Private Cloud for designated integration points (e.g., UKG Workforce Integration Manager input/output folders). This location is not designed for long-term storage, and files may be deleted after 30 days after creation.	Two logins included
Operating system and database software management: Includes application of critical security patches, service packs, and hot fixes; and maintenance of servers.	Included
Server maintenance: Repair and replacement of defective or failed hardware and the installation of hardware upgrades.	Included
Application updates: Application service packs, legislative updates (if applicable), point releases, and version upgrades.	Included
Backup: Customer data is backed up daily. Database backups are replicated via encrypted connections to a second UKG Private Cloud data center within the applicable region; either the EU or the U.S. backups are retained for the prior 28 days on a rotating basis. All historical employee and configuration data is stored in the rotating backups.	Included
Encryption at rest of customer content at storage level: For each of the customer's production and nonproduction environments in a data center in the U.S. or the EU, customer content will be encrypted at rest at the storage level. Encryption at rest is defined as customer content being made unreadable on disk via encryption technology when the UKG Private Cloud computing environment hardware is powered off.	If selected on order form

UKG Workforce Central upgrade services

These include services for UKG to execute tasks to apply point releases and version upgrades to the customer's UKG applications in the UKG Private Cloud. Services are limited to those tasks that apply these updates to the applications.

Included Upgrade Tasks	
Project coordination: project manager coordinates the upgrade project by: • Making up to eight 30-minute weekly status calls (one per week) • Coordinating UKG resources • Sending meeting invitations • Providing project timeline and expected customer commitment at the start of the project • Providing initial project schedule and communicating progress during weekly status calls • Providing communication plan and contact list	Included
Initiate Phase	
Customer/UKG introduction call — up to one hour.	Included
Technical readiness and architecture review — UKG Private Cloud environment.	Included
Collaborate Phase	
Assessment of interface upgrade.	Included
Assessment of new features or changes to configuration.	Not included
Assessment of customs and custom reports and development activities related thereto.	Not included
One restore of production database to preproduction environment for the purpose of upgrade testing. Additional restores, if requested, shall be subject to additional time and material fees.	Included
Upgrade of nonproduction and production environments to new point release or version.	Included
Upgrade of UKG Workforce Integration Manager interfaces due to product changes introduced as part of the technical upgrade as defined in product documentation. For UKG Workforce Central 8, this includes XML export/imports and database views as defined in the UKG Workforce Central Import User Guide and the UKG Workforce Central Data View Reference Guide.	Included
Upgrade of non-UKG Workforce Integration Manager interfaces in nonproduction environment and production environment.	Not included
Upgrade of customs and custom reports. This includes the upgrade of UKG Workforce Integration Manager interfaces that use table import batch functionality, read/write directly to database tables, or require changes due to new/changed customer requirements.	Not included
Upgrade of interfaces and reports created or provided by customer.	Not included
Update of terminal firmware managed by UKG.	Not included
Configuration of new features or functionality or changes to existing configuration.	Available for purchase
System testing of upgraded environments by verifying a user can log in.	Included
User acceptance testing of upgraded environments, interfaces, custom reports, new features, etc.	Not included
Development of customer-specific test cases.	Not included
Sign-off on upgraded nonproduction and production environments.	Customer
Adopt	
Deployment readiness call — up to one hour.	Included

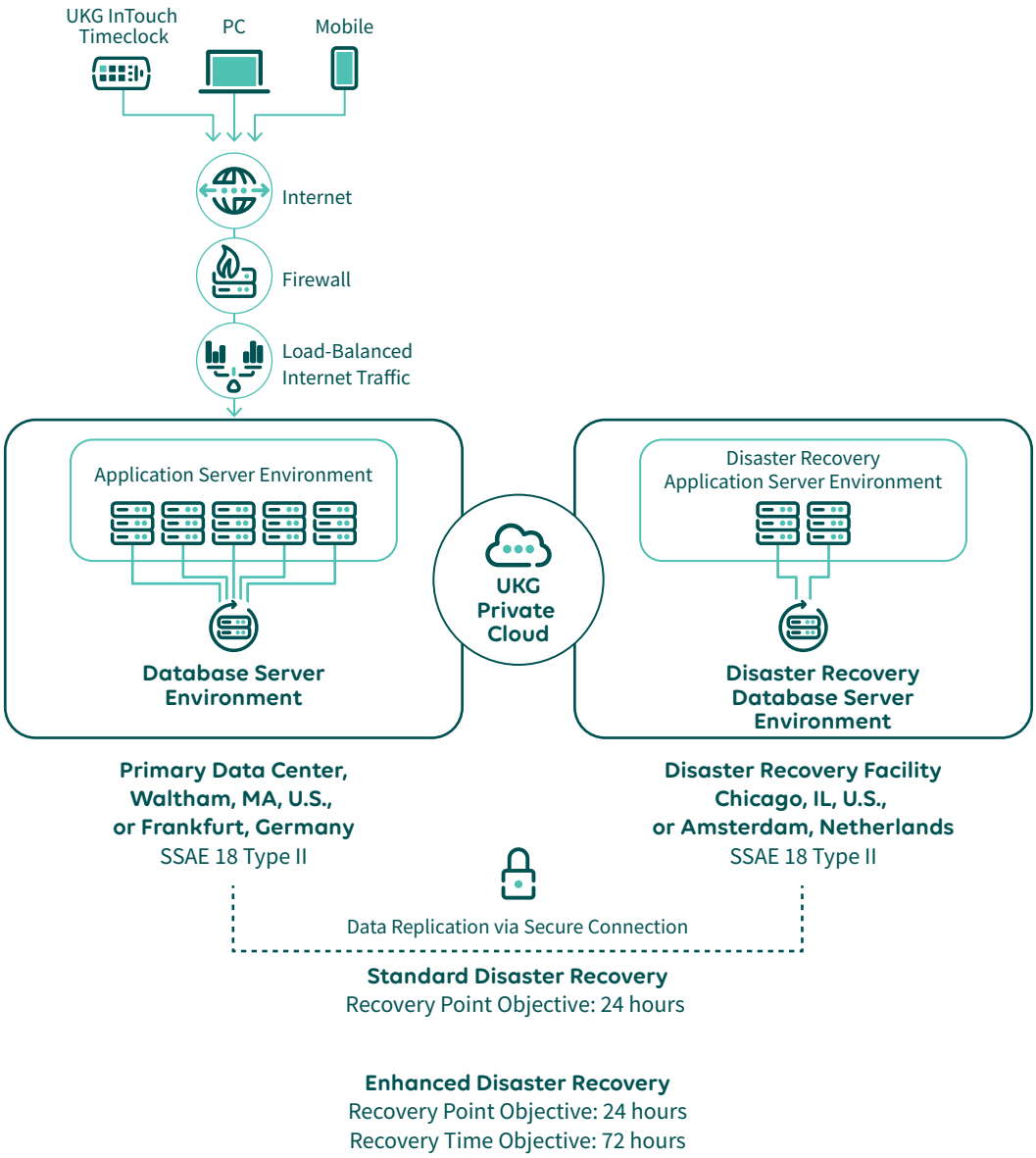
Note that new feature configuration, project management services, and other professional, managed, and educational services and training are not included as part of upgrade services, but may be purchased independently if desired.

Project coordination lasts for no more than eight weeks. At the end of this time, UKG will complete the production upgrade. If for any reason UKG cannot complete the technical upgrade steps within eight weeks due to a UKG-caused delay, project coordination will continue proportionally to cover the UKG-caused delay. For example, if UKG causes a two-week delay due to UKG resource unavailability, project coordination will last no more than 10 weeks.

If not specifically noted, the customer should assume responsibility for the task and/or deliverable.

Data center overview

Architecture/system design:



The UKG Private Cloud data centers offer world-class facilities for power management, heating/ventilation/air-conditioning (HVAC), fire detection and suppression, physical security, and Tier 1 internet connectivity. The facilities are designed to meet the stringent requirements of customers who require the highest availability of critical IT assets, including workforce management applications and data. The environmental conditions are closely monitored and controlled. In the U.S., UKG Private Cloud offers data centers located in Waltham, Massachusetts, and Chicago, Illinois. In the EU, UKG Private Cloud offers data centers located in Frankfurt, Germany, and Amsterdam, Netherlands.

Cloud data flow:

Type of Data	Method of Flow
Terminal traffic	Initial certificate via port 444 (secure HTTP/TLS), if required for older terminals. Ongoing communication is device-initiated via port 443.
End-user web traffic	All traffic is via secure HTTP (TLS) via the internet and directly through UKG core infrastructure (includes UKG-owned and managed firewalls, routers, and switches).
Batch interfaces	Outbound and inbound interfaces to the customer are initiated by the customer and transmitted securely via SFTP. Optionally, PGP encryption can be implemented for an additional fee.
XML-API interfaces	HTTPS (TLS)
Interface and report development	HTTPS (TLS)
Authentication method	One of three methods: native application authentication; LDAPS authentication; single sign-on using Security Assertion Markup Language(SAML) 2.0.
Outbound-initiated sessions	Not permitted.
Direct database access	Read only. ODBC access services available for additional fees.

Maintenance windows:

Scheduled maintenance windows are established by UKG to maintain and update the services when necessary. During these maintenance periods, the services are available to UKG to perform periodic maintenance services, which include vital software updates. UKG will make commercially reasonable efforts during the maintenance period to ensure the services are available to the customer. UKG provides customers flexibility in selecting their maintenance period based on location and day-of-the-week preference.

Customer-specific maintenance periods:

- Customer will choose one of the following time zones for its maintenance period:
  - United States Eastern Standard Time
  - Greenwich Mean Time (GMT)/UTC
  - Australian Eastern Standard Time (AEST)
  - Central European Time
- Customer will choose one of the following days of the week for its maintenance period: Saturday, Sunday, Wednesday, or Thursday.
- UKG will use up to six hours in any two consecutive months to perform customer-specific maintenance, excluding any customer-requested application updates.
- Customer-specific maintenance will occur between midnight and 6:00 a.m. in the customer's selected time zone.
- Excluding any customer-requested application updates, UKG will provide notice of planned downtime via an email notice to the primary customer contact at least seven days in advance of any known downtime so that planning can be facilitated by the customer. If emergency maintenance is required, UKG will provide as much notice as reasonably possible.
- Customer-specific maintenance windows also include additional maintenance windows mutually agreed upon by the customer and UKG.
- In the absence of instruction from the customer, UKG will by default perform maintenance per the time zone where the data center is located.

Non-customer-specific maintenance period

UKG anticipates non-customer-specific maintenance to be performed with no or little (less than three hours per month) customer downtime. If for any reason non-customer-specific maintenance requires downtime, UKG will provide as much notice as reasonably possible of the expected window in which this will occur. Downtime in excess of three hours per month for non-customer-specific maintenance will be deemed to be an outage.

Maintenance:

UKG maintains the equipment specifically related to your UKG workforce management solution to help ensure high availability. In addition, we provide 24/7 monitoring of network communications, server disk space, CPU utilization, and other factors that can significantly impact your solution, and therefore, the end-user experience.

UKG also provides software-related maintenance services. We install application updates, service packs, new software versions, and legislative updates (if applicable), allowing you to take advantage of the latest software features and enhancements while minimizing your risk of noncompliance.

To help ensure exceptional service and ongoing customer satisfaction, you'll be:

- Proactively contacted on a regular schedule to inform you of service packs, legislative updates, and other key system application updates
- Provided with reporting on SLA uptime and root-cause analysis as well as incident response documents as appropriate

System backup and recovery processes

UKG conducts weekly full and daily incremental backups of customer applications and data. All database backups are replicated via secure transmissions to a secondary UKG Private Cloud environment in an alternate data center. Backups are retained for the prior 28 days. UKG conducts formal tests on a quarterly basis to validate that the backup infrastructure is functioning correctly and that the data can be restored.

Optional enhanced disaster recovery

The Enhanced Disaster Recovery service provides customers with a disaster recovery (DR) environment at a secondary UKG Private Cloud facility, to which the customer's application configuration files and data will be replicated. This DR service has a recovery time objective (RTO) of 72 hours and a recovery point objective (RPO) of 24 hours. This DR environment does not include any nonproduction instances, UKG Workforce Analytics™, UKG Workforce Record Manager™, or telephony solutions.

Services include:

- Deployment of the DR system(s) in the UKG disaster recovery data center
- Configuration of data backup(s) and replication from the primary data center to the DR site
- Enabling of replication of the customer's primary system(s) to the DR site

In the unlikely event that UKG declares a disaster in the primary data center, UKG will notify the customer and activate the DR steps necessary to restore application availability within the defined RTO.

Security policies and processes

At UKG, data security is a top priority. Our corporate security officer is the designated management representative responsible for implementing policies and procedures designed to protect and safeguard the customer's workforce data. Employees who require remote access to the customer's private cloud must use two-factor authentication to gain access to the environment. Physical and logical access to the cloud environment is limited to authorized employees based on their business role. Privileged access is further restricted to a subset of the authorized employees (such as system administrators), and logical access is granted with a named user ID and unique complex password.

To reinforce our commitment to security, UKG employees are required to complete security and privacy awareness training within 60 days of hire and annually thereafter.

UKG maintains a hosting environment that undergoes examinations by an independent auditor in accordance with the American Institute of Certified Public Accountants SSAE 18 (i.e., SOC 1) and the AICPA Trust Services Principles Section 100a, Trust Services for Security, Availability, Processing Integrity, Confidentiality, and Privacy (i.e., SOC 2). The UKG Private Cloud is evaluated for the principles of Security, Availability, Privacy, and Confidentiality by the independent auditor. The UKG Private Cloud is located in data centers that undergo SSAE 18 examinations. Management access to the UKG Private Cloud is limited to authorized UKG support staff and customer-authorized integrations. The security architecture has been designed to control appropriate logical access to the UKG Private Cloud to meet the Trust Services Principles of Security, Availability, Privacy, and Confidentiality. The applications provide the customer with the ability to configure application security and logical access per the customer's business processes.

The customer agrees not to upload payment card information as the service is not certified for PCI DSS. Extensions for Health Care (EHC — formerly Optlink) is now hosted in the UKG Private Cloud (in U.S. data centers only) and allows ePHI to be stored when encrypted at rest.

Customer access:

Customers will access the UKG web application via encrypted TLS sessions. The application provides the customer with the ability to configure application security and logical access per the customer's business process. In the event the customer identifies an issue related to the security, availability, or confidentiality of the data or system, the customer will notify UKG.

The customer may require file transfers to populate or extract UKG application data. This shall be accomplished using SFTP to send or retrieve files from the customer's application server. In addition, each customer has a unique named user account and associated password.

UKG management access:

Management access to the environment is limited to authorized UKG support staff and customer-authorized integrations.

A centralized secure file transfer solution facilitates data transfers between the customer and its cloud environment. This solution provides for an encrypted transmission and logging of all files transferred into or out of a customer environment.

UKG performs continuous monitoring in the cloud environment.

Change control

UKG has a formal process in place, backed by automated tools and systems, to help ensure change planning, execution, and follow-through are executed in a controlled and coordinated manner that minimizes disruption to cloud services and ensures timely change management for customers.

The UKG Change Control team coordinates all planned changes, including installation of new software versions, point releases, and legislatives updates, with our UKG Private Cloud consultants. UKG Global Support, in the course of troubleshooting a customer issue, may also identify unplanned changes that require prompt attention to bring the issue to resolution.

Once a change request is submitted to the Change Control team, all planned and unplanned changes are categorized as minor, standard, major, or critical based on risk level and are reviewed by Change Control management. Once approved, the changes are developed, tested, and implemented within the timeframe specified for each category. Standard changes are typically implemented within a five-day period. UKG follows standard operating procedures for all planned changes. Changes are generally applied to the nonproduction environment prior to a production change request.

Certain changes impact more than one customer. In those instances, UKG issues a broadcast message to the affected customers.

UKG also performs changes required to maintain operating systems and other third-party applications that form the base of the UKG workforce management platform. Implementation of these changes is carefully scheduled to minimize service disruption, especially during critical periods in the customer's payroll cycle. Furthermore, UKG reviews vendor and third-party security bulletins to identify and recommend necessary patches and apply those that will protect the customer's security.

Integration with customer data and application environment

If you are having UKG Workforce Integration Manager interfaces developed, data integration between cloud-based UKG applications and other third-party systems is achieved via customer-initiated SFTP file transfers. These transfers enable you to seamlessly and securely move data between systems, such as uploading an employee master file for import into the UKG workforce management system or downloading a payroll data file each pay period. Although many UKG Private Cloud customers automate these processes, automation is not required. Other customized integration options are available at an additional cost.

UKG-based username and password authentication is provided. Integration with Active Directory/LDAP may be available depending on your network configuration.

UKG support for single sign-on:

Single sign-on (SSO) allows users to access authorized network resources seamlessly, on the basis of a single login or user authentication that is performed when they initially access the network. SSO can improve the productivity of network users, reduce the cost of network operations, and improve network security. Specific benefits include:

- Ease of administration: Login credentials are stored and maintained in a single location using a single mechanism (such as LDAP).
- Increased user productivity: Users are not burdened with the chore of logging in to multiple systems. In addition, users are relieved of the manual task of synchronizing username and password combinations for each application.
- Better security: For example, disabling a user account ensures that the account is disabled across all applications in the entire network. Since a user has a single password, it is less likely that the need exists to write down the password.

UKG supports SSO enabled by SAML 2.0.

SLA policies and management

The purpose of the SLA, a service guarantee between UKG and your organization, is to set clear customer expectations for service uptime and availability of workforce management solutions delivered by UKG and to establish financial penalties should we fail to meet those availability promises. The standard UKG Private Cloud SLA stipulates 99.75% availability of a customer's workforce management solution(s) and specifies credits paid to the customer if these terms are not met per the SLA.

To maintain transparency and ensure adherence to the SLA, each UKG Private Cloud customer receives availability metrics.

UKG Workforce Central 8 compatibility requirements

Browser			Operating System	
Vendor	**Product**	**Version**	**Vendor**	**Product**
Microsoft	Internet Explorer	11	Microsoft	Windows 10
				Windows 8
Google	Chrome	56+		Windows 7 — 32- and 64-bit
Mozilla	Firefox 32-bit	51+		Windows Server 2012
				Windows Server 2012R2
Apple	Safari	7.x and 8.x	Apple	Mac OS-X 10.9 and 10.10

Note: For Safari browser/OS-X clients, JRE is provided by Oracle.

Chrome and Firefox — Only recent versions supported (i.e., current version and two previous versions)

CPU	Intel-based Pentium 4 or AMD equivalent; 2 GHz+ recommended
RAM	2GB minimum; 4GB recommended
Cache	256KB/L2 recommended
Display	1,024 x 768 with 256 colors recommended; 128MB minimum graphics memory
Hard disk space	Minimum free disk space: 100MB
Network protocol	HTTPS
Network bandwidth	LAN connection: Gigabit network recommended WAN connection: Fractional T1, or T1+ recommended

UKG Workforce Timekeeper™ 8 requires cookies to be enabled.

Navigator User Interface			
Vendor	**Product**	**Version**	**Operating System**
Adobe	Flash	17+	Same as supported browsers

Java Plug-in			
Vendor	**Product**	**Version**	**Operating System**
Oracle	Java plug-in (JRE)	Supports JRE 1.8 or JRE 1.8_71+ (ships with product)	Same as supported browsers

Mobile	
Device Type	**Platform**
Apple	iPad, iPhone, and iPod Touch — running iOS 8.0
Android	OS 4.4 of the Google-distributed Android operating system

Tablet	
Device Type	**Platform**
Apple	iPad running iOS 8.0+

Timeclock		
Device Type	**Part Number**	**Software / Firmware**
4500 Timeclock	8602000-0xx	Not supported in UKG Private Cloud
4500 Timeclock	8602004-xxx	02.03.16 and greater
4500 Timeclock	8602800-0xx through -4xx	02.03.16 and greater
4500 Timeclock	8602800-5xx through -9xx	03.00.16 and greater
UKG InTouch™ Timeclock	All	1.1.1 and greater

Desktop Virtualization			
Product	**Platform Operating System**	**Product**	**Platform Operating System**
Citrix XenApp v6	Microsoft Windows 2012 Server 64-bit	Terminal services	Microsoft Windows Server 2012 SE
	Microsoft Windows 2012 R2 Server 64-bit		Microsoft Windows Server 2012 SE

About UKG

At UKG (Ultimate Kronos Group), our purpose is people™. Built from a merger that created one of the largest cloud companies in the world, UKG believes organizations succeed when they focus on their people. As a leading global provider of HCM, payroll, HR service delivery, and workforce management solutions, UKG delivers award-winning Pro, Dimensions, and Ready solutions to help tens of thousands of organizations across geographies and in every industry drive better business outcomes, improve HR effectiveness, streamline the payroll process, and help make work a better, more connected experience for everyone. UKG has more than 12,000 employees around the globe and is known for an inclusive workplace culture. The company has earned numerous awards for culture, products, and services, including consecutive years on Fortune's *100 Best Companies to Work For* list. To learn more, visit ukg.com.

Our purpose is people