UKG

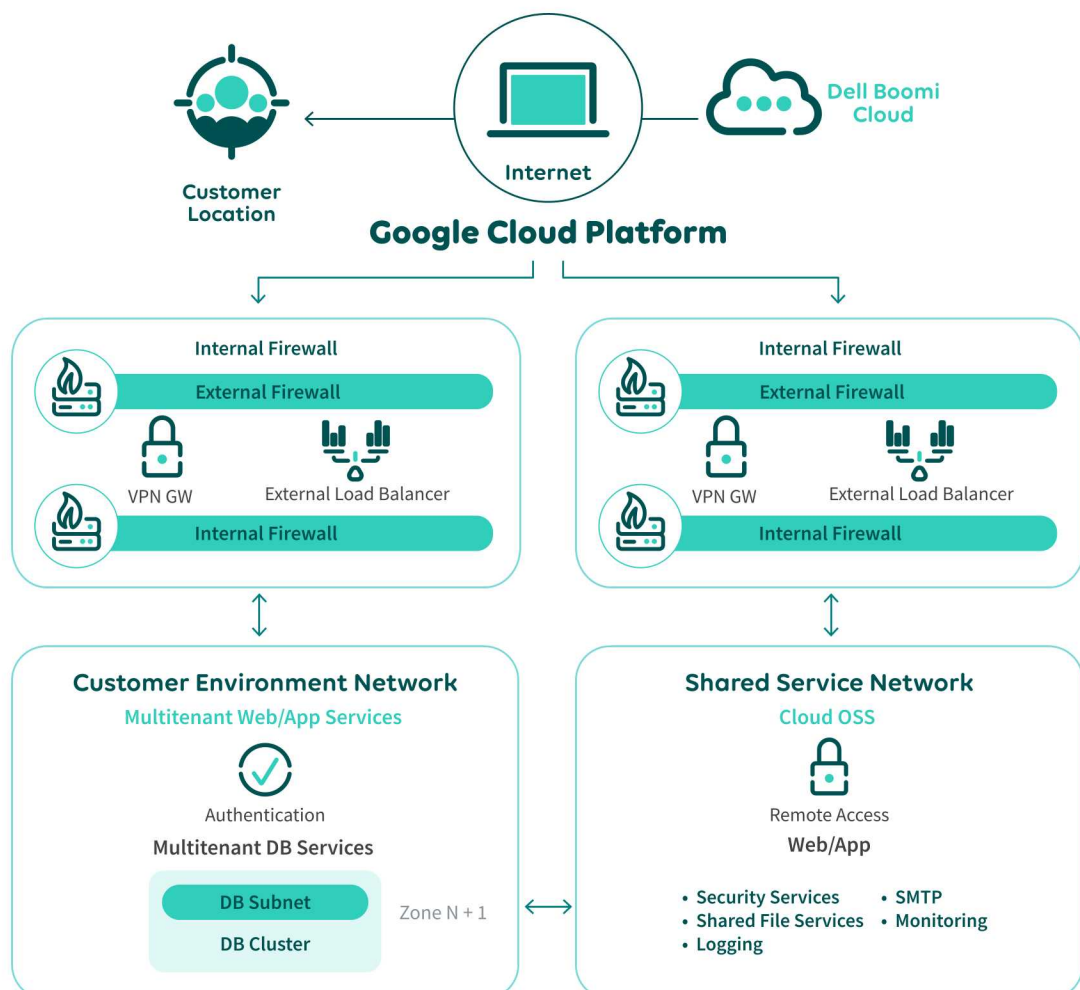# UKG Ready World-Class Infrastructure, Security, and Support

Introduction

UKG Ready™ is a full-suite human capital management (HCM) cloud solution that helps you manage your entire workforce from prehire to retire. Its comprehensive tool set integrates HR, payroll, recruiting, benefits administration, workforce management, and more so that you can manage and nurture your organization's most valuable asset, while giving managers single-source access to real-time employee data for engaging employees, attracting top talent, and making more informed business decisions. Offered exclusively as software as a service (SaaS), any module in UKG Ready can be used individually, as part of a complete, integrated solution, or in conjunction with other third-party applications, content, and/or services. UKG™ (Ultimate Kronos Group) delivers UKG Ready through a single HCM application that is available to customers at any time, from anywhere.

The cloud-based UKG Ready solution is the ideal choice for organizations looking to achieve their HCM goals without exceeding their capital equipment budget or placing additional demands on their busy in-house IT staff. Because UKG Ready is hosted in the Google Cloud, you get 24/7 access to your solution without having to purchase additional hardware, operating systems, or database licenses. You gain peace of mind knowing that experienced UKG technical consultants are managing the solution infrastructure, as well as your applications and employee data, to help ensure high availability, reliable performance, and multilayer security. In addition, because upgrades and add-ons take place in the cloud, you enjoy instant access to the latest software enhancements to help you manage your workforce for optimal results.

UKG Ready Ecosystem

Architecture/System Design

At UKG, we understand that SaaS offerings must be backed by a world-class technology infrastructure that customers can count on day in and day out. That's why the UKG Ready cloud infrastructure environment features a true multitenant architecture that provides the highest levels of data security, system uptime, and built-in redundancy.

Security and auditing

The UKG Ready environment has achieved the American Institute of Certified Public Accountants (AICPA) SOC 1 Type II and AT101 SOC 2 Type II criteria for security, availability, and confidentiality. The cloud environment undergoes an annual audit by an independent Tier 1 auditing firm that publishes the SOC Type II reports attesting to the suitability and operating effectiveness of the controls in place. UKG has certified its compliance with the EU/US Privacy Shield Framework.

System uptime

UKG works closely with Google to help ensure both the physical security and consistent availability of your UKG Ready data and applications. As a result of these efforts, UKG Ready uptime has historically measured 99.79% or greater monthly for unscheduled outages.

Uptime architecture and disaster recovery

The UKG Ready database availability strategy relies on synchronization to maintain copies of its production database on four different servers. This strategy helps ensure that your data, application customizations, and stored code continue to be available even if a database server or Google Cloud site experiences failure. The primary database syncs to a secondary database in real time, and the secondary database syncs to two other databases to provide instant redundancy in the event one server fails.

Full database backup is performed weekly — with incremental backups running daily — to further minimize risk.

- Recovery Point Objective (RPO): 6 hours
- Recovery Time Objective (RTO): 72 hours

System update communications

UKG Global Support will send system administrators a notification for all system updates. These notifications will also be posted in UKG Kronos Community.

- Service Packs: Weekly — updates typically occur on Wednesdays
- System Releases: Bimonthly — updates typically occur on Thursdays
- System Maintenance: 24-hour notice — updates typically occur during the weekend

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 customers' workforce data.

Data collection and encryption options

Your organization's users access the UKG Ready cloud environment from a web browser or mobile device via encrypted Transport Layer Security (TLS) sessions using port 443. UKG InTouch® terminal connections are Ethernet-based, using port 80 or 443. They can utilize TLS to encrypt data transmission when you provide a digital ID certificate from a third-party vendor. Data at rest is encrypted across the UKG Ready environment by utilizing Transparent Data Encryption.

Secure system login

UKG Ready end-users authenticate using a unique password. UKG uses industry-standard, modern hashing algorithms to secure these passwords, and they are never stored in clear text.

Your end-users may gain access to UKG Ready via Single Sign-On (SSO). To implement Security Assertion Markup Language (SAML) 2.0, UKG Ready requires an X.509 certificate, which may be self-signed. You will also need to provide the entity ID of your Identity Provider, such as ADFS 2.0, and a login redirect URL. Once a user is logged in via SSO, a multifaceted security profile controls the role-based functional and data access rights of supervisors and employees.

Browser support

End-users may access UKG Ready applications via a web browser or mobile app provided the following requirements are met:

- Internet Explorer®: Versions 10 or 11
- Edge
- Chrome™/Firefox®/Safari®: Current versions
- Mobile: We have limited support for mobile platforms using the browsers listed above

Mobile app support

The UKG Ready Mobile app runs on the following Apple or Android mobile devices with a data plan or Wi-Fi:

- Apple® iOS: Latest versions
- Android™ OS: 5.0 and higher

Physical and logical security features

UKG hosts and manages UKG Ready on the ISO 27001 and SSAE 18 Type II compliant Google Cloud Platform with multilevel physical and logical security features, including:

Intrusion Prevention System (IPS)/Intrusion Detection System (IDS): UKG deploys next-generation firewalls, which restrict network traffic to authorized traffic.

Secure Transmission Sessions: Secure protocol versions TLS 1.2 and above are supported.

Virtual Code Authentication: UKG Ready requires virtual code authentication — user name, password, and a system-generated code. Passwords are required to be complex, with a minimum number of characters and expiration at a predefined interval.

Best-Practice Coding: UKG employs secure coding practices and control processes across application development and software maintenance. Code reviews are conducted regularly to identify potential security flaws.

Penetration Testing: UKG uses a qualified third-party vendor to perform penetration testing annually.

Vulnerability Scanning: UKG conducts vulnerability scanning using a third-party tool, evaluates identified risks, and develops remediation and/or mitigation plans to address the vulnerability.

Antivirus Software: UKG deploys a third-party, commercially available antivirus solution on servers to prevent viruses and malware from being deployed in the cloud environment.

Patch Management: UKG patches the UKG Ready environment regularly as a routine part of maintaining a secure cloud infrastructure. Patches are reviewed by UKG engineers as they are released from the vendors. Approved patches are tested and then deployed to the environment in accordance with UKG change management policies.

Risk Assessment: UKG conducts an annual risk assessment of the UKG Ready cloud environment to determine whether the control framework achieves the data privacy and data security objectives.

Security Incident Management: UKG maintains an escalation procedure to notify appropriate UKG management staff and customer contacts in the event of a security incident. The event is worked to resolution and a root-cause analysis is performed.

Security and data protection training

UKG conducts Security and Data Protection Awareness Training for new and current employees. New UKG employees are required to complete training within 60 days of their date of hire and annually thereafter. This training focuses on teaching employees what information constitutes personal information, how to protect confidential data and personal information, and security trends of which UKG employees need to be aware. At the conclusion of the training session, employees must pass a test to demonstrate their understanding of data protection and security and privacy awareness issues.

Background checks

Before extending an offer of employment to a candidate, UKG conducts background checks to determine whether he or she is eligible for hire. These checks include education and employment history verification, and if permitted by law and authorized for the position in question, criminal background and credit check searches.

Certifications

The UKG Cloud Services team has the breadth and depth of IT experience, technical skills, and UKG application expertise required to manage, support, and maintain your cloud-hosted HCM system. Our team members have earned a wide range of technical and security certifications, which prove they have amassed the experience and mastered the skills needed to deliver reliable, high-performance cloud-hosting services.

These certifications include:

- Microsoft® Certified Professional
- Microsoft Certified Technology Specialist (MCTS)
- Microsoft Certified Solution Developer (MCSD)
- PMI's Project Management Professional (PMP)®
- ITIL v3 (Foundation)
- CompTIA A+ (2008), Computer-Communications Systems Supervisor – 7 level (military)
- Microsoft Certified Professional (MCP Server 2003) content_id:207963141
- Microsoft Certified System Administrator (MCSA Server 2003)
- Microsoft Certified Technology Specialist (MCTS SQL 2005)
- Juniper Certified – JNCIA-EX (Associate, Enterprise Switching)
- Juniper Certified – JNCIS-ER (Specialist, Enterprise Routing)
- Microsoft Certified DBA (MCDBA)
- VMware® Certification
- HP® 3Par Storage Certification
- HP Data Protector Certification
- Certified Information Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

Change Management

UKG has established a formal change management process to guide the request, development, testing, approval, and implementation of changes, including emergency changes, to the UKG Ready environment. This process differentiates among infrastructure changes, application changes, and customer-specific configuration changes, each of which is handled according to a specific set of predefined steps.

When a change is needed to the UKG Ready environment, the change requester — typically a member of the UKG Cloud Services team — completes a change request that includes the type of change, priority, description, test plan, deployment instructions, backout plan, validation plan, customer impact, and risk assessment. The type of change and its priority determine which approvals are needed to proceed. Upon approval, the change request is authorized to move through the change management process and into production during scheduled maintenance windows on Wednesdays from 12:01 a.m. to 4 a.m. and on Saturdays from 12:01 a.m. to 6 a.m.

Code changes to the UKG Ready environment follow a standard System Development Lifecycle (SDLC). UKG uses an Agile development methodology with monthly sprints. At the end of each sprint, UKG deploys a new UKG Ready release during a scheduled maintenance window. Code changes must be approved for development and undergo quality assurance testing before being deployed in production. All steps in the SDLC process are documented in a ticket.

System Integration

Integrating existing applications with your HCM solution is critical to a successful implementation. UKG Ready Integration Hub, part of the UKG Ready suite, speeds and simplifies integrations between UKG Ready and any combination of cloud, SaaS, or on-premises applications. It allows the UKG Services team or a certified UKG Services Partner to build and deploy integrations between UKG Ready and third-party systems — using industry-proven integration tools — quickly and efficiently, for improved data integrity and faster time to value.

The UKG Services team or a certified UKG Services Partner will assess your unique requirements and determine the best integration strategy to meet your needs. UKG experts will use one or more of the following technologies (included in UKG Ready Integration Hub) to build and deploy your integrations:

UKG Ready Middleware: This integration option may be used to connect UKG Ready applications to on-premises legacy systems, thereby enabling you to send files to a local network printer, upload files from a local network to the cloud, or download files from the cloud to a local computer. The UKG Services team or your UKG Services Partner may also use middleware to automate the upload of information — employee data, accrual balances, cost centers, time punches, and more — from your local network to central servers.

REST APIs: The REST architecture, used by technology leaders such as Google, Yahoo, Amazon, and Twitter, is now a common standard for achieving integration across systems through a series of bidirectional APIs. Working as an underlying layer for data access, the REST architecture provides public XML APIs — wrapped in a web service — which are generally executed using GET and POST commands. UKG has built a robust library of REST APIs for UKG Ready, which it continues to expand with each product update.

Import/export: Import templates, available for various functionality and settings, allow customers to import data directly into UKG Ready. Authorized users simply select the template style for the desired import type, such as an Excel version of an employee import, benefit plans, payroll history, employee skills or work preferences, or time-off requests from other systems. System data export allows authorized users to define the information and file-naming convention used for a data export file. They can also export custom forms by selecting the file format desired for the data export file, such as CSV, Fixed Width, and Custom Settings, and configuring the data export file as needed. Standard export files include payroll exports, benefit plans, training, certifications, and more.

Dell® Boomi™: This flexible integration platform-as-a-service allows the UKG Services team or a certified UKG Services Partner to leverage a library of prebuilt connectors to easily configure integrations with an ever-expanding set of industry-standard third-party systems. For optimal convenience and control, authorized end-users can execute these integration processes directly from the UKG Ready interface. They can also auto-schedule integration processes to execute at a specified frequency or time. In addition, they can run an execution history report and filter the logs by process, execution type, execution time, or status. Integration execution privileges are defined in the end-user's UKG Ready security profile.*

Cloud Services

Support

UKG offers award-winning Support Services to help you get the experience you expect. Our Support Services provide access to valuable tools and information to help you diagnose and resolve issues quickly and efficiently in order to optimize productivity and realize continuous value from your UKG investment. When our self-help tools aren't enough, our skilled, knowledgeable support professionals — with nearly 10 years of domain experience on average — are ready to put their expertise to work for you.

With the UKG Standard Support plan, your organization receives:

- Coverage during standard business hours: 8 a.m. – 5 p.m. Monday through Friday
- Unlimited case (incident) generation and management
- Case escalation, resolution, and confirmation
- Online access via the UKG Kronos Community for:
  - ➜ Proactive system messaging through groups
  - ➜ Cases for web-based case logging and tracking
  - ➜ Comprehensive, searchable knowledge base
  - ➜ Customer groups
  - ➜ System documentation
  - ➜ Technical tips
  - ➜ Training resources

UKG Support Services typically responds to emergency cases, such as those that impact system access, data security, or payroll processing, within one hour. We recommend that you report emergency issues via the toll-free support number so the case priority can be elevated accordingly. The Support Services team typically responds to nonemergency cases within an average of four to eight business hours.

References:

*Because end-user execution of Dell Boomi integrations is managed directly within the UKG Ready user interface, current Dell Boomi customers with their own developers still require UKG Ready Integration Hub. All UKG Ready integrations powered by Dell Boomi must be built by UKG Services professionals or certified UKG Services Partners.

ÜKG

Our purpose is people