UKG Dimensions in the Google Cloud

Security, privacy, and technology

Introduction

As more organizations move their core business technologies to the cloud, they need to know that providers are meeting or exceeding industry standards for securing their hosted applications. UKG™ (Ultimate Kronos Group) assures you that your hosted solution will be online and available, using today's latest technologies to secure and maintain the application.

UKG is committed to designing and deploying workforce management systems and processes to protect the privacy of personal information in all phases of the data lifecycle.

Certifications and controls

The UKG Dimensions™ solution from UKG is deployed in Google™ Cloud Platform (GCP), which has achieved ISO 27001, 27017, and 27018 certifications. On an annual basis, GCP is audited against the AICPA SSAE 18 SOC 2 criteria by an independent auditing firm and has received a FedRAMP high authority to operate. The UKG Dimensions application and service have achieved ISO 27001, 27018, and 27017 certifications. UKG Dimensions is also audited annually against the AICPA SSAE 18 Trust Principles for Security, Confidentiality, Availability, Processing Integrity, and Privacy. The UKG Dimensions SOC 2 Type II and Google Cloud Platform SOC 2 reports are available upon request with the execution of a mutual nondisclosure agreement.

Privacy

As a workforce solutions technology leader, UKG understands the regulatory pressures our customers face in the ever-evolving area of individual privacy. Consistent with our customer-first philosophy, UKG is committed to designing and deploying workforce management systems and processes to protect the privacy of personal information in all phases of the data lifecycle in accordance with our customers' instructions, our published privacy policy, and applicable laws.

Culture of privacy

Privacy starts at the top at UKG. Executive commitment and support have resulted in improved staff awareness and processes supporting data protection and privacy of personal information.

Records of processing

The UKG data inventory process is designed to achieve highly accurate reporting of processing activities conducted on behalf of our customers.

Data processing

UKG maintains technical and organizational measures in support of our customers' European Union General Data Protection Regulation (GDPR) security and compliance obligations.

Privacy impact assessments

As products and processes evolve, UKG will continue to assess privacy and identify risk areas using the UKG data inventory and classification system.

Vendor risk management

UKG vendor risk management includes oversight and contractual commitments to ensure third parties process data consistent with European Union GDPR principles.

Incident management

The UKG Cybersecurity Incident Response Plan treats incidents involving personal information with the highest severity level of response.

Encryption – protocols and cryptography

Data in transit: Web application, mobile, application programming interfaces (APIs), and terminal communications are protected with transport layer security (TLS), and UKG supports customer devices connecting with TLS 1.2.

Secure file transfer protocol (SFTP) services utilize secure shell transfer protocol to provide a generic endpoint for customers sending and receiving files to and from UKG Dimensions. In addition, PGP file encryption is standard for all flat-file integrations.

Data at rest: UKG secures data at the storage level for the customer's production and nonproduction environments for data in GCP using Advanced Encryption Standard 256-bit encryption.

Stringent security measures are taken to protect customer data by using encryption protocols and cryptography.

Network security

All internet connections traverse redundant firewalls to enforce access controls and provide monitoring and logging of traffic. UKG configures firewall rules to be deny-all by default. Required ports and protocols are opened based on a defined business purpose. Network proxies prohibit all unnecessary application traffic.

Network intrusion detection systems (IDS) and intrusion prevention systems are implemented to mitigate risks of intrusion and malicious software attacks. Vulnerability scans of the hosted environment and application are conducted, the results are reviewed, and the vulnerabilities are remediated per the UKG SOC 2 report.

Electronic file transmission between the environment and customers is permitted with the use of SFTP and APIs. Hardening settings on production servers are monitored against defined hardening standards.

Application access controls

UKG Dimensions utilizes a multitenant deployment strategy, where customer data is separated by database schema. All tenant access is controlled by a secure API gateway, and traffic is resolved by tenant ID.

A user's access to the UKG Dimensions system is controlled through configurable access profiles. The following access profiles determine what a user can see and do and are made up of two components, which allow you to precisely define access to the system based on your company's specific job requirements:

Function access profiles: This profile determines the functions that a user can perform within the system and what the user can do.

Data access and display profiles: These profiles not only determine the pay codes, work rules, and reports a user can use within the system but also the display controls, which affect how a user views the UKG Dimensions components. They also control which employees a manager can access.

Authentication

UKG Dimensions supports industry standard protocol SAML 2.0 for SSO integration.

The UKG Dimensions authentication service provides a highly available federated SSO service for user login to UKG Dimensions from the customer organization's desktops, work-from-home devices, and mobile devices.

The UKG Dimensions authentication service also supports basic authentication for customers that have not migrated to SSO. Usernames and password are stored in the UKG Dimensions system for customers using basic authentication. Customers may choose to have some (e.g., managers) make use of SSO and other users (non-managers) make use of basic authentication.

Access and authentication

User access to UKG Dimensions is controlled through configurable access profiles, while authentication service is provided by SSO.

Scalability

UKG Dimensions features a distributed service architecture and leverages micro-services in a multilayered platform.

UKG Dimensions offers automation and cloud management capabilities to provision and configure the infrastructure underlying the software solution. This provides the ability to scale services horizontally and/or vertically independently of each other, based on actual or projected utilization.

UKG gathers a significant volume of infrastructure and application metrics to evaluate the overall demand on services as well as the health and the performance of the environment. These metrics are leveraged both passively and actively for a variety of operational purposes.

UKG uses the cloud management capability on a regular basis and backs it with quantitative and qualitative data from monitoring. The services are scaled appropriately to the actual and anticipated load on the system.

Performance

UKG Dimensions undergoes a rigorous performance evaluation process during development, with industry-leading thresholds for interactive traffic, integration (API) traffic, and background computation and analytics. The solution is designed and built for high performance to meet the business needs of our customers in all industries and across a variety of workloads. This performance evaluation process is embedded in the software development lifecycle and applies equally to new and existing capabilities.

In customer-facing environments, response times are regularly monitored using a combination of synthetic transaction monitoring from multiple geographic locations (representing the customer base experience) as well as internal monitoring (representing the UKG portion of the experience).

Internal application performance monitoring tools provide visibility from the edge of the UKG cloud network through the data tier, allowing UKG engineers to precisely pinpoint any performance concerns. Aggregated data from both sources is regularly reviewed by dedicated engineering and operations teams to ensure UKG Dimensions is meeting or exceeding our customers' expectations and UKG's high standards for performance.

Performance evaluation process

UKG Dimensions undergoes a rigorous performance evaluation process during development. The solution is designed and built for high performance to meet the business needs of our customers in all industries and across a variety of workloads.

High availability

The UKG Dimensions architecture has high availability and resiliency built into the layers of the solution to support the UKG 99.75% SLA. All service components at the web, application, and middleware layers are mirrored across multiple server instances for redundancy. Load-balancing technologies and software clustering are implemented for increased availability.

UKG Dimensions leverages best-in-breed microservices to create a true distributed platform, ensuring high availability. These services allow better fault isolation; if one microservice fails, the others will continue to function. UKG can add more services, and they can be spread across multiple nodes or even data centers for increased demand.

All UKG Dimensions databases employ database clustering with streaming synchronous or asynchronous replication between database servers and Google zones.

Service and availability

UKG Dimensions services are designed to operate utilizing multiple cloud data centers (zones) within a geographic area (region). Should service be interrupted, the RTO is 24 hours, and the RPO is 4 hours.

Disaster recovery

The UKG Cloud Disaster Recovery Program has been developed and is maintained to ensure continued alignment with the UKG Business Continuity Management Program, which defines requirements for UKG disaster recovery plans and crisis management strategies.

UKG Dimensions services are designed to operate utilizing multiple cloud data centers (zones) within a geographic area (region). The UKG Cloud Disaster Recovery Program is based on an all-or-nothing failover strategy. In the event the customer's UKG Dimensions services are unavailable and cannot be restored within an acceptable timeframe, the entire stack would be switched over in a disaster situation to the disaster recovery (DR) region.

Once services have been successfully restored in the DR region, that environment will continue as the production region. To maintain continuity of the UKG Dimensions standard Disaster Recovery service, UKG will prepare a new DR region as part of the production failover recovery process.

Recovery time objective (RTO) is 24 hours, and the recovery point objective (RPO) is 4 hours.

State-of-the-art data centers

UKG Dimensions is deployed in GCP. Security and data protection are at the forefront of the design criteria and are an integral part of all Google operations. Physical security features of all Google data centers include a layered security model that uses safeguards such as alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Google data centers are monitored 24/7 by high-resolution interior and exterior cameras.

Security measures are further increased in areas that are closer to the data center floor. Less than 1% of Google employees will ever step foot in a Google data center, and only authorized Google employees with specific roles may enter floor areas. Access to the data center floor is possible only via a security corridor that utilizes a multifactor access control system that requires security badges and biometrics for entry.

The Google Cloud runs on a technology platform that was conceived, designed, and built to operate securely. Google is an innovator in hardware, software, network, and system management technologies. Using this expertise, it custom-designed its servers, proprietary operating system, and geographically distributed data centers with the principles of "defense in depth," resulting in an IT infrastructure that is more secure and easier to manage than more traditional technologies.

"Defense in depth" describes the multiple layers of defense that protect Google's network from external attacks. Only authorized services and protocols that meet Google's security requirements can traverse it, with everything else automatically dropped. Industry-standard firewalls and access control lists are used to enforce network segregation. All traffic is routed through custom Google Front End (GFE) servers to detect and stop malicious requests and distributed denial of service (DDoS) attacks. Additionally, GFE servers are allowed to communicate only with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to authorized personnel.

Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and an alternative power source, each with equal power. Diesel backup generators will provide enough emergency electrical power to run each data center at full capacity.

Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages.

Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms within affected zones, at security operations consoles, and at remote monitoring desks.

The Google Cloud

Google is an innovator in hardware, software, network, and system management technologies. The Google Cloud runs on a technology platform that was conceived, designed, and built to operate securely.

System monitoring and vulnerability management

UKG has deployed multiple layers of security, beginning at the system perimeter, including next-generation technology firewalls, intrusion prevention systems, intrusion detection systems (IDS), log monitoring, and anti-virus software. The environment is continuously monitored.

Security information and event management systems merge data sources (e.g., app logs, firewall logs, IDS logs) for granular analysis and alerting. In addition to IDS alerts that are generated, there is a security dashboard to assist in analysis and to be reviewed and available to UKG security personnel. Detective and preventative measures are applied at multiple layers.

Storage equipment and hardware

Google tracks the location and status of all storage equipment within its data centers. Google also upgrades obsolete hardware to improve processing speed and energy efficiency or to increase storage capacity.

Media sanitation and destruction of data

Google tracks the location and status of all storage equipment within its data centers through acquisition, installation, retirement, and destruction, via asset tags that are tracked in Google's asset database. Physical storage media may be decommissioned for a range of reasons. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google also upgrades obsolete hardware to improve processing speed and energy efficiency or to increase storage capacity.

Whether hardware is decommissioned due to failure, upgrade, or any other reason, storage media is decommissioned using appropriate safeguards. Google hard drives use technologies like full disk encryption to protect data at rest during decommission. When a hard drive is retired, authorized individuals will either: 1) verify that the disk is erased by overwriting the drive with zeros and performing a verification process to ensure the drive contains no data; or 2) use a tool to crush and deform the drive or shred the drive into small pieces.

The information in this document is subject to change without notice and should not be construed as a commitment by UKG.

UKG

Our purpose is people