

UKG

UKG Ready: infrastructuur,
beveiliging en support van
wereldklasse

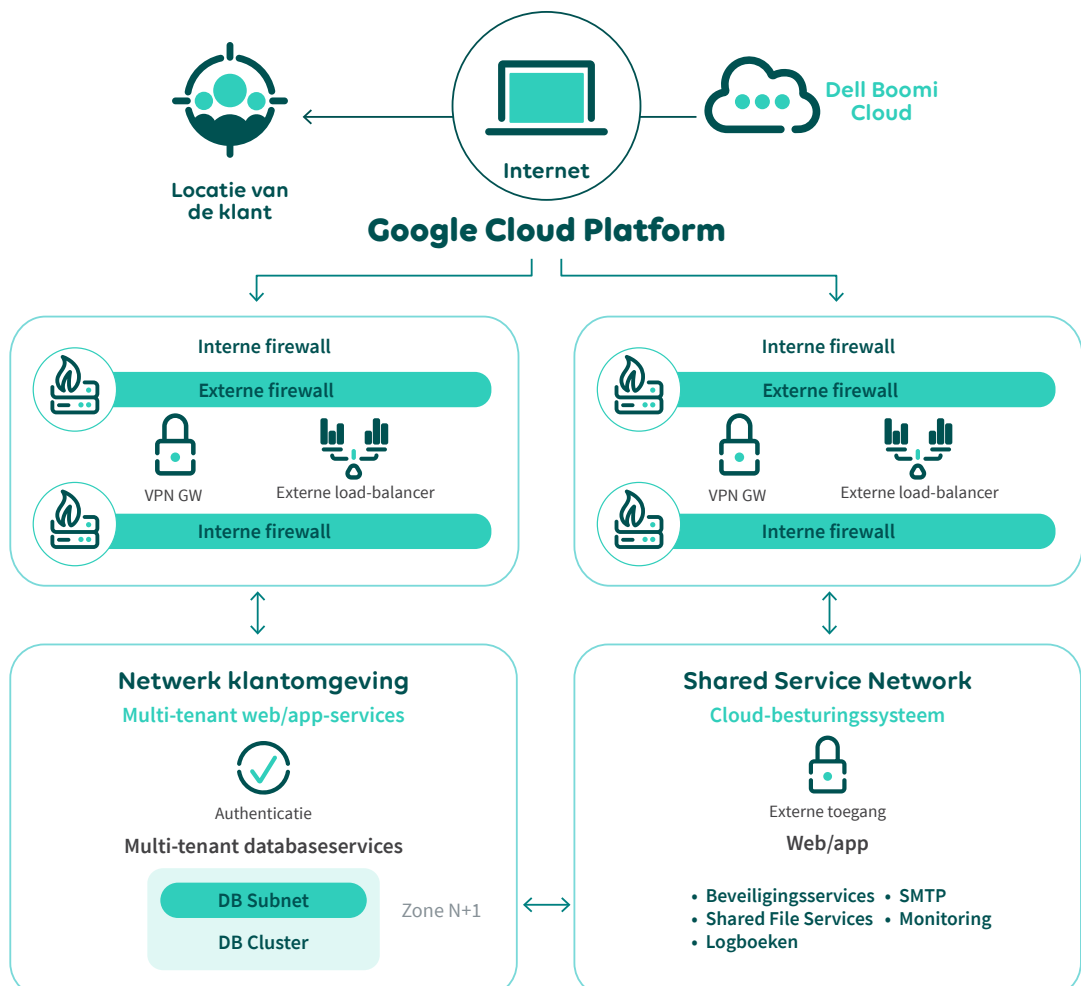


Inleiding

UKG Ready™ is een complete cloudsuite voor human capital management (HCM) waarmee u uw volledige personeelsbestand kunt beheren, van werving tot pensioering. De geïntegreerde tools van deze suite verzorgen HR, salarisadministratie, werving en selectie, beheer van personeelsvoorzieningen, workforce management en nog veel meer, zodat u de meest waardevolle succesfactor van uw organisatie optimaal kunt beheren. Uw managers krijgen via één bron toegang tot realtime personeelsgegevens om huidige werknemers te motiveren, nieuw talent aan te trekken en beter geïnformeerde zakelijke beslissingen te nemen. UKG Ready wordt exclusief aangeboden als SaaS-oplossing (Software as a Service). Elke module kan afzonderlijk worden gebruikt als onderdeel van een complete, geïntegreerde oplossing, of in combinatie met applicaties, content en/of services van externe leveranciers. UKG™ (Ultimate Kronos Group) levert UKG Ready als een complete HCM-applicatie die altijd en overal toegankelijk is voor de gebruikers van de klant.

De cloudgebaseerde UKG Ready-oplossing is de ideale keuze voor organisaties die hun HCM-doelstellingen willen bereiken zonder hun kapitaalbudget te overschrijden of de eigen IT-medewerkers extra te belasten. Omdat UKG Ready wordt gehost in de Google Cloud, krijgt u 24 uur per dag toegang tot uw oplossing zonder dat u extra hardware, besturingssystemen of databaselicenties hoeft aan te schaffen. U kunt gerust zijn in de wetenschap dat de ervaren specialisten van UKG zorgen voor het beheer van de complete infrastructuur, inclusief uw applicaties en personeelsgegevens, om hoge beschikbaarheid, betrouwbare prestaties en gelaagde beveiliging te garanderen. Omdat upgrades en uitbreidingen in de cloud worden toegepast, profiteert u bovendien onmiddellijk van de nieuwste softwareverbeteringen voor optimaal beheer van uw personeelsbestand.

Het ecosysteem van UKG Ready



Architectuur/systeemontwerp

Bij UKG begrijpen we dat SaaS-oplossingen moeten worden ondersteund door hoogwaardige IT-infrastructuren waarop onze klanten elke dag opnieuw kunnen vertrouwen. Daarom heeft de cloudinfrastructuur van UKG Ready een multi-tenant architectuur met de best mogelijke gegevensbeveiliging, maximale uptime en ingebouwde redundantie.

Beveiliging en auditing

De UKG Ready-omgeving voldoet aan de criteria van het American Institute of Certified Public Accountants (AICPA) SOC 1 Type II en AT101 SOC 2 Type II voor beveiliging, beschikbaarheid en vertrouwelijkheid. De cloudomgeving wordt jaarlijks onderworpen aan een audit door een onafhankelijke Tier 1-auditfirma, die SOC Type II-rapporten publiceert om de geschiktheid en de werkzaamheid van de controlemaatregelen te bevestigen. UKG heeft verklaard dat wordt voldaan aan de privacyvoorschriften van het EU/US Privacy Shield Framework.

Systeemuptime

UKG werkt nauw samen met Google om zowel de fysieke beveiliging als de consistente beschikbaarheid van uw UKG Ready-applicaties en de bijbehorende data te garanderen. Hierdoor bedraagt de historische maandelijkse uptime van UKG Ready voor wat betreft niet-geplande uitval meer dan 99,79%.

Architectuur en calamiteitenherstel

De beschikbaarheidsstrategie voor de UKG Ready-database berust op synchronisatie om kopieën van de productiedatabase te bewaren op vier verschillende servers. Deze strategie zorgt dat uw gegevens, applicatieaanpassingen en programmacode beschikbaar blijven, zelfs als een databaseserver of een Google Cloud-site uitvalt. De primaire database wordt in realtime gesynchroniseerd met een secundaire database. Deze secundaire database wordt weer met twee andere databases gesynchroniseerd om onmiddellijke redundantie te bieden voor het geval een server uitvalt.

Wekelijks wordt een complete backup van de database gemaakt, met dagelijkse incrementele backups om het risico nog verder te beperken.

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

Berichtgeving over systeemupdates

UKG Global Support houdt systeembeheerders op de hoogte van alle systeemupdates. Deze berichten worden ook in de UKG Kronos Community geplaatst.

- Servicepacks: wekelijks – updates meestal op woensdag
- Systeemversies: tweemaandelijks – updates meestal op donderdag
- Systeemonderhoud: 24 uur van tevoren – updates meestal in het weekend

Beleid en processen voor beveiliging

Bij UKG staat gegevensbeveiliging altijd bovenaan. Onze Chief Information Security Officer is verantwoordelijk voor de implementatie van beleid en procedures om de data van onze klanten te beveiligen en te beschermen.

Opties voor gegevensverzameling en encryptie

De gebruikers van uw organisatie krijgen vanaf een webbrowser of een mobiel apparaat toegang tot de UKG Ready-cloudomgeving via versleutelde TLS-sessies op poort 443. UKG InTouch®-terminals maken verbinding via Ethernet en gebruiken poort 80 of 443. Deze terminals kunnen de gegevensoverdracht met behulp van TLS versleutelen wanneer u beschikt over een digitaal ID-certificaat van een externe provider. In de hele UKG Ready-omgeving worden data in rust versleuteld door middel van Transparent Data Encryption (TDE).

Beveiligde systeemlogin

Eindgebruikers van UKG Ready kunnen zich authenticeren met een uniek wachtwoord. UKG maakt gebruik van moderne, industriestandaard hashing-algoritmen voor de beveiliging van deze wachtwoorden, die nooit in tekstvorm worden opgeslagen.

Eindgebruikers kunnen single sign-on (SSO) gebruiken om toegang te krijgen tot UKG Ready. Voor implementatie van SAML 2.0 (Security Assertion Markup Language) hebben wij van u een X.509-certificaat nodig, dat zelfondertekend mag zijn. Daarnaast moet u de entiteits-ID van uw Identity Provider (bijvoorbeeld ADFS 2.0) en een omleidings-URL voor de inlogpagina opgeven. Nadat een gebruiker via SSO is ingelogd, worden de rolafhankelijke functionele en informatietoegangsrechten van medewerkers en leidinggevendenden bepaald aan de hand van een beveiligingsprofiel.

Browserondersteuning

Eindgebruikers kunnen UKG Ready-applicaties gebruiken vanaf webbrowsers of mobiele apps die aan de volgende vereisten voldoen:

- Edge
- Chrome™/Firefox®/Safari®: nieuwste versies
- Mobiel: beperkte ondersteuning voor mobiele platforms met de hierboven vermelde browsers

Ondersteuning voor mobiele apps

De mobiele app van UKG Ready werkt op de volgende mobiele apparaten van Apple of Android met een data-abonnement of wifi:

- Apple® iOS: nieuwste versies
- Android™ OS: 5.0 en hoger

Fysieke en logische beveiliging

UKG host en beheert UKG Ready op het Google Cloud Platform, dat voldoet aan de criteria van ISO 27001 en SSAE 18 Type II en beschikt over meerdere lagen met fysieke en logische beveiligingsfuncties, waaronder:

Intrusion Prevention System (IPS)/Intrusion Detection System (IDS): UKG gebruikt firewalls van de nieuwste generatie, die uitsluitend geautoriseerd netwerkverkeer doorlaten.

Beveiligde sessies: TLS 1.2 en hogere protocolversies worden ondersteund.

Virtuele-codeverificatie: UKG Ready vereist verificatie van virtuele code aan de hand van een gebruikersnaam, een wachtwoord en een door het systeem gegenereerde code. De wachtwoorden moeten voldoende complexiteit hebben, een minimum aantal tekens bevatten en na een bepaalde periode vervallen.

Best practices voor programmacode: UKG maakt bij de applicatieontwikkeling en het softwareonderhoud gebruik van veilige programmeermethoden en controleprocedures. Programmacode wordt regelmatig opnieuw beoordeeld om mogelijke veiligheidslekken op te sporen.

Penetratietests: UKG schakelt jaarlijks een gekwalificeerde externe partner in om penetratietests uit te voeren.

Kwetsbaarhedescans: UKG voert kwetsbaarhedescans uit met een speciale tool, analyseert de gevonden risico's en ontwikkelt reparatie- of beheersplannen om kwetsbaarheden te verhelpen.

Antivirussoftware: UKG implementeert een commerciële antivirusoplossing van een externe leverancier om te voorkomen dat virussen of andere malware in de cloudomgeving binnendringen.

Patchbeheer: UKG past regelmatig patches toe op de UKG Ready-omgeving als onderdeel van routinematig onderhoud voor een beveiligde cloudinfrastructuur. De door de softwareleveranciers aangeleverde patches worden door specialisten van UKG gecontroleerd. Goedgekeurde patches worden eerst getest en daarna in de cloudomgeving geïmplementeerd volgens het UKG-beleid voor wijzigingsbeheer.

Risicobeoordeling: UKG voert een jaarlijkse risicobeoordeling van de UKG Ready-cloudomgeving uit om te bepalen of het controlekader voldoet aan de criteria voor gegevensprivacy en gegevensbeveiliging.

Beheer van beveiligingsincidenten: UKG hanteert een escalatieprocedure om de verantwoordelijke UKG-managers en de contactpersonen bij de klant te informeren in het geval van een beveiligingsincident. Het incident wordt onderzocht en opgelost en vervolgens vindt een oorzakenanalyse plaats.

Trainingen voor beveiliging en gegevensbescherming

UKG geeft bewustmakingstrainingen over beveiliging en gegevensbescherming aan zowel huidige als nieuwe medewerkers. Nieuwe werknemers van UKG volgen deze training verplicht binnen 60 dagen na indiensttreding, en daarna jaarlijks. Medewerkers leren op de training wat precies persoonsgegevens zijn, hoe ze vertrouwelijke informatie en persoonsgegevens moeten beschermen en welke actuele beveiligingstrends er zijn. Na afloop van de trainingssessie maken de medewerkers een toets om aan te tonen dat ze voldoende inzicht hebben in gegevensbescherming, beveiliging en gegevensprivacy.

Antecedentenonderzoek

Voordat een kandidaat in dienst genomen, voert UKG een antecedentenonderzoek uit om na te gaan of de kandidaat voor een betrekking in aanmerking komt. Bij dit onderzoek verifiëren we de gevolgde opleidingen en het arbeidsverleden. Voor zover dit wettelijk toegestaan en vereist is voor de desbetreffende functie, controleren we ook op strafblad en kredietverleden.

Certificeringen

De specialisten in het UKG Cloud Services-team beschikken in de breedte en de diepte over alle IT-ervaring, technische vaardigheden en kennis van UKG applicaties die ze nodig hebben om uw cloudgebaseerde HCM-systeem te beheren, te ondersteunen en te onderhouden. Onze mensen hebben een breed scala aan technische en beveiligingscertificaten behaald, zodat ze aantoonbaar de ervaring en de vaardigheden hebben opgedaan om betrouwbare, hoogwaardige cloudhostingdiensten te kunnen ondersteunen.

Onze specialisten hebben onder meer de volgende certificaten behaald:

- Microsoft® Certified Professional
- Microsoft Certified Technology Specialist (MCTS)
- Microsoft Certified Solution Developer (MCSD)
- PMI Project Management Professional (PMP)®
- ITIL v3 (Foundation)
- CompTIA A+ (2008), Computer-Communications Systems Supervisor – 7 level (militair)
- Microsoft Certified Professional (MCP Server 2003)
- 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)



Wijzigingsbeheer

UKG heeft een formeel proces voor wijzigingsbeheer ontwikkeld om het aanvragen, ontwikkelen, testen, goedkeuren en implementeren van wijzigingen (inclusief urgente aanpassingen) in de UKG Ready-omgeving te begeleiden. In dit proces maken we onderscheid tussen infrastructuurwijzigingen, applicatiewijzigingen en klantspecifieke configuratiewijzigingen, die elk volgens een vastgelegd stappenplan worden afgehandeld.

Wanneer een wijziging gewenst is in de UKG Ready-omgeving, dient de aanvrager (meestal een lid van het UKG Cloud Services-team) een wijzigingsverzoek in. Dit verzoek bevat informatie over het type wijziging, de prioriteit, de beschrijving, het testplan, de implementatie-instructies, het backout-plan, het validatieplan, de effecten op klanten en de risicobeoordeling. Het type wijziging en de prioriteit ervan bepalen welke goedkeuringen vereist zijn om de wijziging te implementeren. Na goedkeuring doorloopt een wijzigingsverzoek het proces voor wijzigingsbeheer, waarna het in productie wordt genomen tijdens de geplande onderhoudsvensters op woensdag van 0.01 uur tot 4.00 uur en op zaterdag van 0.01 uur tot 6.00 uur.

Wijzigingen in de code van de UKG Ready-omgeving doorlopen een SDLC-proces (System Development Lifecycle). UKG volgt een Agile ontwikkelingsmethodiek met maandelijks sprints. Aan het eind van elke sprint brengt UKG een nieuwe UKG Ready-release uit tijdens een van de vensters voor gepland onderhoud. Codewijzigingen moeten voorafgaand aan de ontwikkeling worden goedgekeurd en kwaliteitstests ondergaan voordat ze in productie worden genomen. Alle stappen in het SDLC-proces worden gedocumenteerd in een ticket.

Systeemintegratie

Integratie van bestaande applicaties met uw HCM-oplossing is van cruciaal belang voor een succesvolle implementatie. De UKG Ready Integration Hub, onderdeel van de UKG Ready-suite, versnelt en vereenvoudigt de integratie tussen UKG Ready en elke combinatie van cloud-, SaaS- en on-premise applicaties. Met deze hub kan het UKG Services-team of een gecertificeerde UKG Services Partner snel en efficiënt integraties tussen UKG Ready en externe systemen bouwen en implementeren (met beproefde, industriestandaard integratietools) voor optimale gegevensintegriteit en een kortere time-to-value.

Het UKG Services-team of de gecertificeerde UKG Services Partner beoordeelt uw specifieke vereisten en bepaalt de beste integratiestrategie om in uw behoeften te voorzien. De specialisten van UKG gebruiken één of meer van de volgende technieken (als onderdeel van de UKG Ready Integration Hub) om uw integraties te bouwen en te implementeren:

UKG Ready-middleware: deze integratietechniek kan worden gebruikt om UKG Ready-applicaties te koppelen aan on-premise legacy-systemen, zodat u bijvoorbeeld bestanden naar een lokale netwerkprinter kunt sturen, bestanden van een lokaal netwerk kunt uploaden naar de cloud en bestanden vanuit de cloud kunt downloaden naar een lokale computer. Het UKG Services-team of uw UKG Services Partner kan middleware ook gebruiken voor het geautomatiseerd uploaden van informatie (werknemersgegevens, opgebouwde tegoeden, kostenplaatsen, in- en uitklokdata en dergelijke) van uw lokale netwerk naar centrale servers.

REST API's: de REST-architectuur, die wordt gebruikt door marktleiders zoals Google, Yahoo, Amazon en Twitter, is een populaire standaard voor integratie tussen systemen via een reeks bidirectionele API's. De REST-architectuur fungeert als een onderliggende laag voor gegevenstoegang en stelt openbare XML API's beschikbaar (ingebed in een webservice), die meestal worden aangeroepen met GET- en POST-commando's. UKG heeft voor UKG Ready een robuuste bibliotheek met REST API's aangelegd, die bij elke productupdate verder wordt uitgebreid.

Import/export: door middel van importeersjablonen voor verschillende functies en situaties kunnen klanten rechtstreeks data importeren in UKG Ready. Geautoriseerde gebruikers kunnen een sjabloonstijl voor het gewenste importtype kiezen, zoals een Excel-versie om vanuit andere systemen informatie te importeren over personeelsvoorzieningen, historische salarisgegevens, verlofaanvragen en vaardigheden of werkvoorkeuren van medewerkers. Daarnaast kunnen geautoriseerde gebruikers instellen welke informatie en welke bestandsnaamconventies worden gebruikt voor een gegevensexportbestand. Ze kunnen ook aangepaste formulieren exporteren door de gewenste bestandsindeling voor het exportbestand te kiezen (bijvoorbeeld CSV, vaste kolombreedte of aangepast) en het exportbestand te configureren. Voorbeelden van standaard exportbestanden zijn loonlijsten, regelingen voor personeelsvoorzieningen, opleidingen en certificeringen.

Dell® Boomi™: dankzij dit flexibele integratieplatform-as-a-service (iPaaS) kan het UKG Services-team of een gecertificeerde UKG Services Partner een bibliotheek met kant-en-klare connectors gebruiken voor eenvoudige integratie met een steeds breder aanbod van industriestandaard systemen van externe leveranciers. Geautoriseerde eindgebruikers kunnen deze integratieprocessen rechtstreeks vanuit de UKG Ready-interface uitvoeren. Daarnaast kunnen ze integratieprocessen inplannen voor uitvoering met een bepaalde frequentie of op een bepaalde tijd. Bovendien kunnen ze rapporten over de uitvoeringsgeschiedenis genereren en de logboeken filteren op proces, uitvoeringstype, uitvoeringstijd en/of status. Uitvoeringsbevoegdheden voor integraties worden geconfigureerd in het UKG Ready-beveiligingsprofiel van de eindgebruiker.*

Services

Support

UKG levert bekroonde supportservices om te waarborgen dat u de gebruikerservaring krijgt die u mag verwachten. UKG Support Services geeft u toegang tot waardevolle tools en informatie om u te helpen eventuele problemen snel en efficiënt te diagnosticeren en op te lossen, zodat u de productiviteit snel weer kunt herstellen. Als de zelfhulptools niet toereikend zijn, staan onze deskundige en ervaren supportspecialisten (met gemiddeld bijna 10 jaar ervaring in dit vakgebied) klaar om u met raad en daad bij te staan.

Met het UKG Standard Support Plan heeft uw organisatie recht op:

- Beschikbaarheid tijdens normale kantooruren: Maandag t/m vrijdag tussen 08.00 en 17.00 uur
- Onbeperkt cases (incidenten) genereren en beheren
- Escalatie, oplossing en bevestiging van cases
- Online toegang tot de UKG Kronos Community voor:
 - Proactieve systeemberichten via de groepen
 - Webgebaseerde registratie en tracering van cases
 - Uitgebreide, doorzoekbare kennisbank
 - Klantengroepen
 - Systeemdocumentatie
 - Technische tips
 - Trainingen

Met het UKG Plus Support Plan (verkrijgbaar tegen meerprijs) krijgt uw organisatie alle voordelen van het Standard Support Plan, aangevuld met:

- 24/7 live telefonische en online support
- Proactieve en preventieve ondersteuning
- Complete tracement en beheer van problemen

UKG Support Services reageert doorgaans binnen één uur op noodgevallen, zoals problemen die gevolgen hebben voor de toegang tot het systeem, de gegevensbeveiliging of de salarisverwerking. U wordt aangeraden om spoedgevallen te melden via het gratis telefoonnummer, zodat de prioriteit van de case kan worden verhoogd. Het team van Support Services reageert op niet-dringende gevallen meestal binnen vier tot acht werkuren.

Referenties:

*Omdat de uitvoering van Dell Boomi-integraties door eindgebruikers rechtstreeks vanuit de gebruikersinterface van UKG Ready wordt beheerd, moeten klanten van Dell Boomi met hun eigen ontwikkelaars toch gebruikmaken van de UKG Ready Integration Hub. Alle UKG Ready-integraties op basis van Dell Boomi moeten door UKG Services-specialisten of gecertificeerde UKG Services Partners worden gebouwd.



Our purpose is people

© 2020 UKG Inc. Alle rechten voorbehouden.

Ga voor een volledig overzicht van alle UKG-handelsmerken naar ukg.com/nl-NL/handelsmerken.

Alle overige genoemde handelsmerken zijn eigendom van de desbetreffende eigenaren.

Alle specificaties kunnen zonder voorafgaande kennisgeving worden gewijzigd. SV0534-NLv12