kyoceradocumentsolutions.it

Kyocera Cloud Information Manager

White Paper sulla sicurezza

Versione 20211110

In questo documento

Il presente documento è riservato ed è ad esclusivo uso interno.

Questo documento descrive Kyocera Cloud Information Manager (KCIM) versione 1.0.

A chi si rivolge

Questo documento si rivolge ai membri del personale della sede centrale e alle società di vendita del gruppo Kyocera Document Solutions. Al di fuori del gruppo Kyocera Document Solutions, come partner di canale o utenti finali, si prevede che le società di vendita creino nuovi documenti pubblici ufficiali basati sui contenuti di questo manuale.

Storico delle revisioni

Data rilascio	Revisione	Capitolo	Dettagli
10 novembre 2021	1.0	-	Prima pubblicazione

Indice

1. In generale 4

2. Multitenancy - Multilocazione 5

3. Comunicazione sicura tra i moduli 8

4. Identificazione e autenticazione utente 9

4.1. Policy di blocco dell'account 9
4.2. Policy sulle password 9

5. Funzionalità di sicurezza di Keycloak 10

5.1. Funzionalità di Keycloak 10
5.2. Modello di mitigazione della minaccia 10

6. Protezione dati 12

6.1. Protezione dei dati archiviati 12
6.1.1. Controllo accessi 12
6.1.2. Autenticazione 12
6.1.3. Crittografia 12
6.1.4. Backup dati 12
6.2. Protezione dei dati di comunicazione 12
6.2.1. Accesso utenti 12
6.2.2. Token di accesso e token di aggiornamento 13
6.2.3. Protocollo HTTPS 13
6.3. Comunicazione sicura tra server KCIM e database 13
6.4. Test di vulnerabilità della sicurezza 13

7. Autenticazione dispositivo (MFP/Mobile) 14

8. Dettagli tecnici sulla sicurezza della piattaforma Google Cloud 15

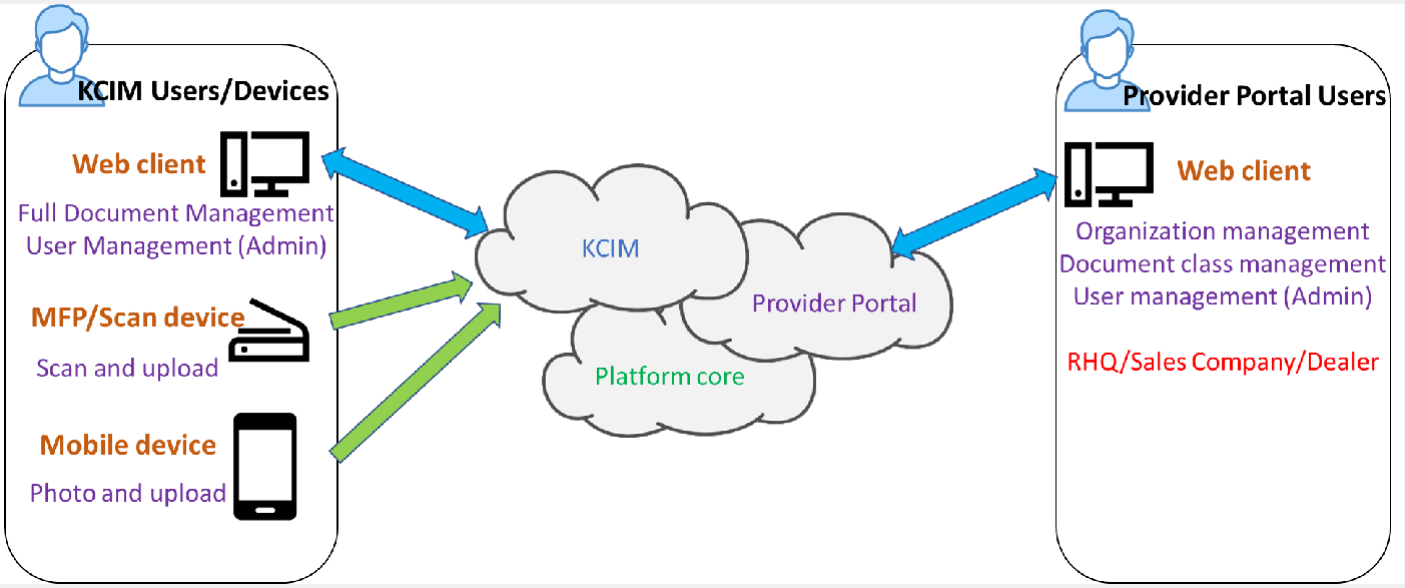
9. Informazioni di contatto 16

1. In generale

Kyocera Cloud Information Manager è un sistema di gestione documentale basato su cloud che consente agli utenti di gestire facilmente i documenti, scansire, caricare, indicizzare e archiviare i documenti.

Questo white paper informa i rivenditori sulle misure di sicurezza in KCIM. La priorità di Kyocera è fornire una protezione sicura delle risorse informative gestite da KCIM che sono rigorosamente protette dalla configurazione sicura e dalle funzionalità di sicurezza di KCIM.

KCIM è costituito dai seguenti componenti:



Portale provider: Il portale provider è un'applicazione che supporta la gestione dell'organizzazione KCIM, la gestione degli utenti e la gestione delle classi di documenti. Il provider (RHQ, SC, Dealer) può accedere al **portale provider** tramite un browser web. Si possono aggiungere, modificare o eliminare organizzazioni per fornitori secondari o per i loro clienti.

KCIM: L'amministratore del cliente o l'utente cliente possono accedere a **KCIM** utilizzando un browser web. L'amministratore del cliente può aggiungere account utente per la propria organizzazione e configurare le impostazioni relative ai diritti di accesso alle classi di documenti.
Gli utenti clienti possono gestire i documenti come scansione, caricamento, indicizzazione, ricerca, modifica, ecc.

Platform core: Il core della piattaforma è un componente fondamentale della piattaforma. KCIM è costruito su di esso. La piattaforma archivia in modo sicuro tutte le informazioni sui documenti di KCIM.

MFP client: Il client MFP si connette al server KCIM. Gli utenti possono caricare il documento scansito sul server KCIM.

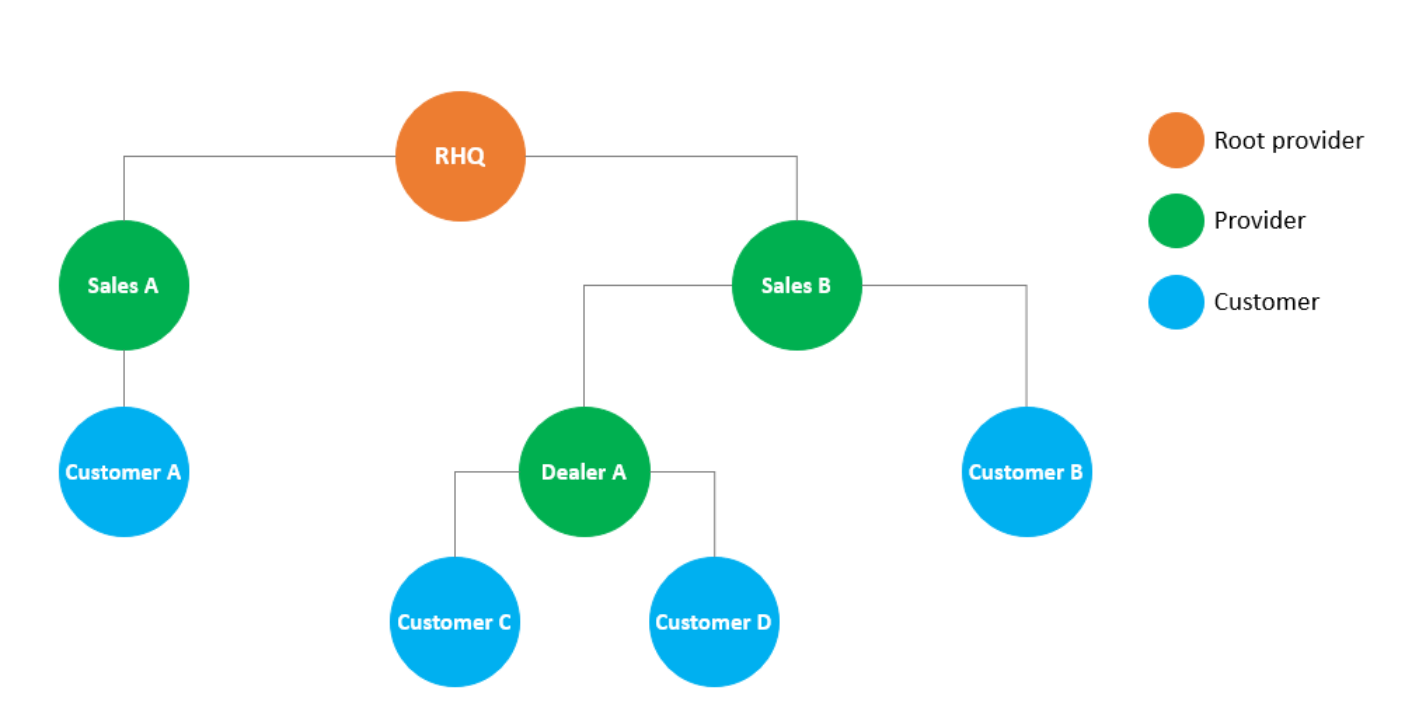
Mobile application: l'applicazione mobile si connette al server KCIM. I clienti possono scattare una foto dei loro documenti e caricarli sul server KCIM.

2. Multitenancy - Multilocazione

KCIM si avvale della multi-tenancy per ospitare un maggior numero di società di vendita, rivenditori e organizzazioni di clienti. Ogni società di vendita, rivenditore e cliente viene trattata come una organizzazione. Il controllo degli accessi viene imposto attraverso una struttura ad albero gerarchico (Fig. 2-1).

Le organizzazioni sono classificate in due tipi: un'organizzazione fornitore e un'organizzazione cliente. Un'organizzazione fornitore è focalizzata sulla gestione di una o più organizzazioni clienti. Le organizzazioni di fornitori dispongono di funzionalità di gestione dell'organizzazione/utente e di gestione delle licenze, mentre le organizzazioni clienti forniranno la funzionalità di gestione documentale.

La struttura gerarchica è modellata sulla struttura gerarchica di vendita comune utilizzata in KYOCERA. Una RHQ (sede regionale) è l'organizzazione madre (organizzazione principale del fornitore) con società di vendita sotto la RHQ come organizzazioni provider figlie. I clienti delle società di vendita sarebbero le organizzazioni dei clienti e i nodi foglia nella struttura gerarchica ad albero.



(Fig. 2-1) Struttura gerarchica delle organizzazioni KCIM

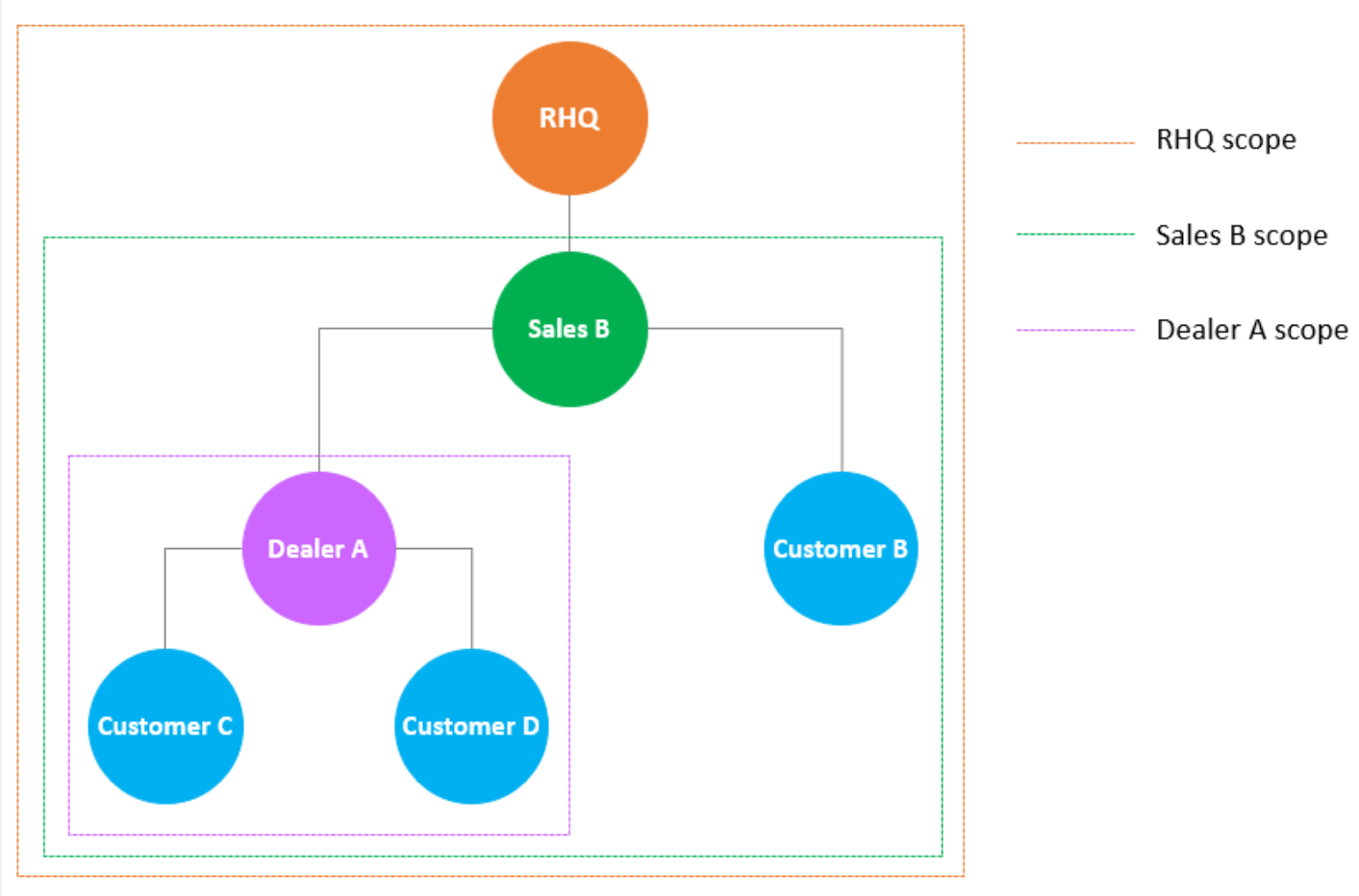
Nessuna organizzazione può visualizzare i dati di un'altra organizzazione ad eccezione dell'organizzazione madre. Solo il provider madre può ottenere dal cliente le informazioni sul contatore dell'utilizzo e le informazioni di contatto del rappresentante dell'organizzazione. Il conteggio dell'utilizzo è costituito dai dati relativi alle informazioni sulla licenza come la pagina OCR, il conteggio dei documenti, l'utilizzo delle dimensioni del documento e le informazioni sul contratto. I dati hanno un contesto e l'accesso ai dati è limitato (Tabella 2-1).

Tipo di utente	Utenti di aziende cliente	Documenti di aziende cliente	Informazioni sulla classe di documenti	Informazioni relative al contratto (conteggio OCR, conteggio e dimensione documenti)
Provider Admin/Support	Non accessibile	Non accessibile	Accessibile	Accessibile
Customer Admin	Accessibile	Accessibile	Accessibile Gestione diritti di accesso	Accessibile
Customer user	Non accessibile	Accessibile	Non accessibile	Accessibile Può visualizzare solo le informazioni sul contratto

(Tabella 2-1) Accesso ai dati dell'organizzazione e dell'utente per tipo di utente

I contesti sono presenti tra le organizzazioni madri e figlie. A livello di organizzazione, l'organizzazione madre/figlia può condividere i dati di definizione delle classi di documenti (classi di documenti e attributi delle classi di documenti).

Inoltre, l'organizzazione madre può gestire le informazioni relative alla licenza dell'organizzazione figlia cliente (ad es. quante pagine OCR, dimensioni del documento consentite) (Fig. 2-3).



(Fig. 2-3) Accesso alle informazioni relative alla licenza per ciascuna organizzazione

La visibilità diretta di questi dati è solo tra l'organizzazione madre e figlia. Ma RHQ può recuperare i dati di utilizzo dell'intera organizzazione figlia. Il portale del provider di KCIM può generare report sull'utilizzo dell'OCR dell'intera gerarchia dell'organizzazione, ma le informazioni dettagliate sull'organizzazione saranno rese anonime.

3. Comunicazione sicura tra i moduli

Secure Sockets Layer (SSL) è una tecnologia di sicurezza standard per stabilire un collegamento crittografato tra un server e un client. In KCIM, viene utilizzato TLS per rendere sicure e proteggere le informazioni sensibili condivise tra KCIM e un browser, dispositivo, dispositivo mobile o database. Queste informazioni includono:

- Credenziali e password utente KCIM
- Dati dell'utente
- Informazioni sul documento (documento, dati OCR, dati di indicizzazione, metadati, note, ecc.)
- Metriche di conteggio dei documenti (conteggio delle pagine OCR, dimensioni del documento, conteggio dei documenti, ecc.)

4. Identificazione e autenticazione utente

Quando si accede a KCIM, l'utente deve accedere con un account attivato. Un utente non autorizzato non può accedere a KCIM. Le seguenti funzioni sono supportate come funzioni di sicurezza per l'accesso. KCIM utilizza il metodo di autenticazione OAuth 2.0 tramite Keycloak. Keycloak è un software di gestione dell'autenticazione utente sponsorizzato da RedHat (si vedano i dettagli delle funzionalità di sicurezza di Keycloak in 5.Funzionalità di sicurezza di Keycloak).

4.1. Policy di blocco dell'account

La politica di blocco dell'account protegge KCIM dagli attacchi di cracking delle password. Quando un utente non riesce ad accedere per un numero predeterminato di volte, l'account utente viene bloccato per un certo periodo.

Come mostrato nella tabella seguente, quando si raggiunge la soglia di blocco dell'account per tre tentativi di accesso non riusciti, l'account viene bloccato. L'impostazione sbloccherà l'account dopo 30 minuti. L'account bloccato può anche essere sbloccato manualmente dall'amministratore.

Numero di tentativi di accesso continui non riusciti	3 tentativi in 15 minuti
Tempo di sblocco automatico	30 minuti

4.2. Policy sulle password

Un utente deve utilizzare una password complessa che sia difficile da analizzare e deve essere applicabile alla politica sulle password di KCIM.

Una password che non soddisfa la politica della password è vietata. Questo criterio impedisce agli utenti di impostare password semplici e protegge dall'accesso non autorizzato da parte di terzi.

Tutta l'autenticazione viene elaborata in modo sicuro in base a OAuth 2.0 tramite keycloak.

La lunghezza e la complessità della password sono definite nella tabella seguente.

Lunghezza password	Tra 8 e 64 caratteri
Complessità password	Deve includere almeno uno dei caratteri di ciascuna categoria: Maiuscolo (A ~ Z) Minuscolo (a ~ z) Numeri (0 ~ 9) Simboli (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

5. Funzionalità di sicurezza di Keycloak

KCIM utilizza Keycloak come servizio di gestione dell'identità/autenticazione. Keycloak è un sistema di gestione dell'autenticazione open source che supporta varie funzionalità di sicurezza.

5.1. Funzionalità di Keycloak

Keycloak fornisce le seguenti funzionalità:

- Supporto OAuth 2.0.
- Admin Console per la gestione centralizzata di utenti, ruoli, mappature dei ruoli, client e configurazione.
- Account Management console che consente agli utenti di gestire centralmente il proprio account.
- Supporto dei temi: personalizza tutte le pagine rivolte agli utenti per integrarle con le vostre applicazioni e il vostro marchio.
- Flussi di accesso: auto-registrazione utente opzionale, recupero password, verifica e-mail, richiesta aggiornamento password, ecc.
- Gestione delle sessioni: gli amministratori e gli utenti stessi possono visualizzare e gestire le sessioni utente.
- Mappatori di token: mappa gli attributi utente, i ruoli, ecc. come si desidera in token e istruzioni.
- Politiche di revoca non-precedenti per dominio, applicazione e utente.
- Supporto CORS - Gli adattatori client hanno il supporto integrato per CORS.
- Adattatori client per applicazioni JavaScript, WildFly, JBoss EAP, Fuse, Tomcat, Jetty, Spring, ecc.

5.2. Modello di mitigazione della minaccia

Keycloak mitiga le seguenti possibili vulnerabilità di sicurezza come server di autenticazione. In questo momento, KCIM configura la protezione dagli attacchi *brute force* e prevede di adottare un numero maggiore di funzionalità di sicurezza da keycloak.

- Restrizione IP
- Restrizione porte
- Password guess: attacchi *brute force*
- Attributi utente di sola lettura
- Clickjacking
- Requisiti SSL/HTTPS
- Attacchi di falsificazione di richieste tra siti (CSRF)
- URI di reindirizzamento non specifici
- Conformità FAPI
- Accesso compromesso e token di aggiornamento
- Codice di autorizzazione compromesso
- Reindirizzatori aperti
- Database delle password compromesso

- Limitazione di contesto
- Limitazione token di audience
- Limitazione sessioni di autenticazione

6. Protezione dati

6.1. Protezione dei dati archiviati

Le risorse informative di KCIM devono essere protette e non devono trapelare né venire perse. Kyocera Document Solutions implementa misure di protezione della sicurezza per le risorse di informazioni archiviate e un supporto per il recupero dei dati attraverso le funzionalità descritte di seguito.

6.1.1. Controllo accessi

Solo le persone con un adeguato controllo accessi avranno accesso a tutte le informazioni sui documenti KCIM (documento/contenuto/metadati). Gli utenti dovranno disporre di appropriati e definiti ruoli di accesso ai documenti per accedere a classi di documenti specifiche. Il ruolo di accesso ai documenti viene assegnato per classe di documenti e controllato dagli amministratori dell'organizzazione in KCIM.

6.1.2. Autenticazione

Il database KCIM richiede l'autenticazione dell'utente per ottenere l'accesso ai dati del database. Le credenziali di autenticazione vengono configurate durante il rilascio iniziale dell'istanza.

6.1.3. Crittografia

Il database KCIM utilizza l'algoritmo AES256 per la crittografia.

6.1.4. Backup dati

Il backup giornaliero del database KCIM viene eseguito automaticamente. È archiviato su Google Cloud Storage e crittografato tramite AES256.

6.2. Protezione dei dati di comunicazione

KCIM protegge i dati di comunicazione relativi all'accesso dell'utente per utilizzare KCIM e la comunicazione dati per trasferire i dati rispettivamente tra KCIM e i dispositivi.

Al fine di proteggere i dati di comunicazione KCIM dalla mascheratura, dalla manipolazione o dalla modifica dei dati, i dati di comunicazione vengono crittografati e i componenti KCIM vengono reciprocamente autenticati.

6.2.1. Accesso utenti

Quando un utente accede a KCIM da un'applicazione Web utilizzando un browser, viene stabilito un canale di comunicazione autenticato. L'utente KCIM può accedere al portale Web KCIM dall'interfaccia utente del browser Web client indipendentemente dal ruolo dell'utente. Quando un utente accede

al portale Web KCIM, viene sempre identificato e autenticato. Se questa identificazione e autenticazione hanno esito positivo, verrà emesso un token di accesso e l'utente potrà accedere al portale Web KCIM in base al suo ruolo. Il portale web KCIM protegge i dati di comunicazione tramite HTTPS.

6.2.2. Token di accesso e token di aggiornamento

Una volta completata l'autenticazione, verranno emessi un token di accesso e un token di aggiornamento e verrà mantenuta la sessione utente. La sessione utente verrà utilizzata per accedere a tutte le operazioni sui documenti. Il token di accesso verrà utilizzato per accedere alle operazioni di gestione degli utenti e dei contratti. La durata del token di accesso è di 5 minuti e può essere aggiornata utilizzando il token di aggiornamento ogni volta che si verifichi un accesso del BE API dopo la scadenza del token di accesso. L'interfaccia utente verrà disconnessa in caso di inattività di 15 minuti.

6.2.3. Protocollo HTTPS

HTTPS funziona sui protocolli protetti sottostanti (TLS 1.2) che crittografano tutto il traffico tra browser e server. SSL e TLS richiedono un certificato con una chiave privata, una chiave pubblica, informazioni sul dominio e una catena di firme da parte delle autorità di certificazione.

6.3. Comunicazione sicura tra server KCIM e database

KCIM stabilirà la connessione di rete al database utilizzando il traffico di rete crittografato TLS e AES 128.

6.4. Test di vulnerabilità della sicurezza

Al fine di mantenere l'applicazione KCIM aggiornata con le ultime misure di sicurezza, verrà seguito il seguente programma per la valutazione della vulnerabilità della sicurezza:

- Le valutazioni mensili saranno condotte dal team di sicurezza interno
- Una valutazione annuale sarà condotta da un fornitore esterno/di terzi specializzato in test di vulnerabilità della sicurezza per le applicazioni web

7. Autenticazione dispositivo (MFP/Mobile)

Per proteggere le informazioni sensibili trasmesse tra KCIM e i dispositivi, la sicurezza viene applicata tramite HTTPS. La versione utilizzata di TLS è 1.2.

L'utente deve autenticarsi tramite l'autenticazione KCIM dall'applicazione del dispositivo per stabilire la connessione di rete tra KCIM e il dispositivo.

L'autenticazione del client avverrà utilizzando user id, password, client-id e client-secret. Mobile e MFP hanno client-id e client-secret diversi.

8. Dettagli tecnici sulla sicurezza della piattaforma Google Cloud

KCIM è ospitato su Google Cloud Platform. GCP soddisfa l'ampia serie di controlli di sicurezza delle informazioni riconosciuti a livello internazionale e standard di conformità specifici del settore, come ISO 27001, HIPAA, FedRAMP, SOC 1/2/3, GDPR, CCPA (si veda l'elenco dettagliato degli standard conformi in GCP Cloud Compliance, https://cloud.google.com/security/compliance).

L'ambiente di hosting è progettato per utilizzare i servizi forniti da GCP e le funzionalità di sicurezza per proteggere e monitorare la nostra applicazione. Le varie funzionalità che vengono utilizzate includono:

- Varie credenziali GCP per login/accesso
- Log di sicurezza
- Instance isolation - Isolamento dell'istanza
- Firewall/API di accesso
- Punti di accesso HTTPS sicuri
- Sicurezza della rete (isolamento VPC, gruppi di sicurezza di rete, elenco di controllo dell'accesso alla rete, gateway Internet, ecc.),
- Archiviazione
- Simple Notification Service che monitora i log delle applicazioni CloudWatch

KCIM è presente sui seguenti data center GCP:

- Tokyo, Giappone (asia-northeast1)
- Saint-Ghislain, Belgio (europe-west1)
- Council Bluffs, Iowa, USA (us-central1)

KCIM utilizza l'archiviazione gestita e il database PostgreSQL ospitato su GCP.

9. Informazioni di contatto

In caso di domande o commenti, prego contattarci utilizzando le seguenti informazioni.

Indirizzo e-mail per richieste di tipo commerciale BSD:
bsd-product-inquiry@ml.kyods.com

Sito portale della community di vendita di soluzioni aziendali (modulo di richiesta):
https://globalsite.kyods.com/businesssolutions-salescommunityportal/inquiry/

KYOCERA Document Solutions Inc.

1-2-28 Tamatsukuri, Chuo-ku, Osaka 540-8585, Giappone
Tel.: +81-6-6764-3555

KYOCERA Document Solutions Italia S.p.A.
Via Monfalcone, 15
(MI)
Tel. +39 (02) 92179.1 – Fax +39 (02) 92179600
www.kyoceradocumentsolutions.it