Remote System Management

CBS-RM-DIPx

it Descrizione del servizio

Sommario

1 Funzioni principali

Il servizio Remote System Management di Bosch consente di sfruttare le potenzialità dell'Internet delle cose (IoT) per fornire una gestione sicura, trasparente e conveniente delle risorse per tutto il ciclo di vita di un sistema video. Questo servizio consente agli utenti finali, agli integratori di sistema e agli installatori di eseguire la gestione dell'inventario e degli aggiornamenti nonché attività di monitoraggio dell'integrità di un intero sistema video Bosch (DIVAR IP + BVMS + telecamere) da una piattaforma Remote Portal centralizzata.

Il servizio fornisce la massima tranquillità ai clienti finali, consentendo il monitoraggio sicuro del sistema 24 ore su 24, 7 giorni su 7. Ciò consente all'utente di intervenire attivamente in caso di problemi e di risolverli, ad esempio, prima che le registrazioni video vadano perse a causa di un errore del disco rigido. La connessione MQTTS sicura garantisce inoltre la privacy dei dati, poiché nessuno può accedere al materiale video tramite questa connessione a causa del fatto che il trasferimento dei dati video e delle immagini non è supportato da questo protocollo. Inoltre, il servizio consente l'implementazione di software e firmware in remoto, mantenendo il sistema aggiornato e sicuro. La connettività cloud si basa su una singola connessione in uscita da DIVAR IP a Remote Portal, dove DIVAR IP consolida tutte le comunicazioni in entrata e in uscita per l'intero sistema video.

Il servizio è progettato per essere utilizzato da organizzazioni di clienti finali di maggiori dimensioni che effettuano la manutenzione del sistema da più luoghi distanti tra loro o da installatori che offrono tali servizi a molti clienti finali diversi. I vantaggi dell'utilizzo di Remote System Management sono costituiti principalmente da una maggiore efficienza durante l'esecuzione di operazioni di manutenzione del sistema, evitando di doversi recare in loco quando non necessario grazie alle funzionalità di manutenzione in remoto, ad esempio l'implementazione di aggiornamenti in caso di un avviso di sicurezza, o dalla disponibilità di informazioni più aggiornate sul sistema, che consentono una migliore preparazione degli interventi in loco. Effetto collaterale positivo: servizio completo con emissioni di CO_2 minime. Inoltre, gli utenti possono migliorare l'esperienza del servizio che forniscono agendo in modo proattivo e cogliendo l'opportunità di risolvere problemi sul campo addirittura prima che i clienti (interni) si rendano conto di avere un problema.
Per i dettagli funzionali, fare riferimento alle rispettive schede tecniche del servizio.

Avviso!

Le schede tecniche sono disponibili nel catalogo dei prodotti relativo al proprio Paese o area geografica.

2 Requisiti di sistema

Requisiti software

L'interfaccia Web Remote Portal può essere utilizzata con i moderni browser Web che supportano HTML5. Per usufruire dell'esperienza ottimale, Bosch consiglia l'utilizzo di Google Chrome.

Requisiti del dispositivo

Per utilizzare tutte le funzionalità di Remote System Management, sulle telecamere IP di Bosch deve essere in esecuzione firmware versione 6.50 o successive.
Come indicato nella scheda tecnica, sono supportati solo modelli DIVAR IP specifici. Per questi modelli, il requisito minimo per il software è il supporto di DIVAR IP System Manager 2.0 o versioni successive. Per dettagli, consultare la rispettiva scheda tecnica.
La larghezza di banda richiesta dipende dalle specifiche del sistema video e dalla struttura del sito, ovvero dal numero di telecamere e dai dispositivi DIVAR IP in loco. Bosch consiglia una larghezza di banda minima di 11 Mbps o 1,31 Mbps per DIVAR IP, poiché DIVAR IP consolida le comunicazioni in entrata e in uscita per sé e per le telecamere collegate. Questa raccomandazione è derivata dal caso di utilizzo più impegnativo in termini di larghezza di banda, ovvero dal download di file di aggiornamento di maggiori dimensioni che creano un picco della richiesta di larghezza di banda ogni volta che tali aggiornamenti vengono attivati da Remote Portal. La maggior parte del tempo di funzionamento non di picco richiederà larghezze di banda di circa 10 Kbps, ad esempio per il monitoraggio dei parametri di integrità e altri scambi di dati di telemetria.

Avviso!

Questi requisiti di larghezza di banda possono variare e l'utente deve verificare che la larghezza di banda disponibile soddisfi i requisiti dell'applicazione. Bosch fornisce numerosi strumenti per il calcolo della larghezza di banda richiesta, senza alcuna responsabilità per la disponibilità effettiva della larghezza di banda e la corretta configurazione.

3 Applicazione Web

Remote System Management è integrato con Remote Portal, che funge da piattaforma centrale basata sul Web per l'attivazione del servizio e funzionalità generali aggiuntive, indipendentemente dall'offerta del servizio, come descritto di seguito.

Gestione del sistema e dei dispositivi (Device Management) con una vista dashboard
I sistemi e i singoli dispositivi possono essere raggruppati in ordine gerarchico per corrispondenza con la posizione di installazione o del cliente, per limitare l'accesso per un gruppo di dispositivi o aggregare lo stato di più dispositivi.

Panoramica del servizio
La sezione "Servizi" in Remote Portal fornisce una panoramica di tutti i servizi disponibili sui tipi di dispositivi. Ciascun servizio fornisce un elenco di una panoramica consolidata di tutti i dispositivi e sistemi su cui è attivo.

Gestione delle licenze dei servizi
I servizi possono essere attivati visitando Remote Portal dopo la messa in servizio iniziale di DIVAR IP su Remote Portal.
Per l'attivazione del servizio Remote System Management, è necessario disporre di licenze. In base al modello di DIVAR IP e alla relativa modalità operativa, si applicano licenze diverse. Per dettagli, consultare le schede tecniche. Le licenze vengono gestite e attivate in Remote Portal nella sezione "Licenze di servizio".

Gestione utenti
Remote Portal consente un controllo minuzioso dell'accesso a dispositivi e servizi. Tramite gli *amministratori* di gestione dei ruoli, i *tecnici* e gli *utenti finali* possono essere associati singolarmente a sistemi, gruppi e servizi.

Avviso!

Per ulteriori informazioni su Remote Portal, visitare la relativa pagina di prodotto disponibile all'indirizzo: https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/

4 Documentazione

La documentazione e le schede tecniche per tutti i singoli sistemi basati su DIVAR IP sono disponibili qui:

Formazione tecnica:	https://academy.boschsecurity.com/

NOTA: sarà disponibile un corso introduttivo autonomo su Remote System Management. Questo corso di formazione verrà successivamente integrato nel corso di formazione per la certificazione di DIVAR IP all-in-one.

Procedure/note sulla configurazione:	https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt
Schede tecniche/note di applicazione:	https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip

5 Componenti del software open source

I componenti del software open source inclusi nella piattaforma Remote Portal sono disponibili qui: https://remote.boschsecurity.com/open_source/open_source_licenses.txt

6 Hosting dei servizi

I servizi elencati in questa sezione sono ospitati sull'infrastruttura distribuita come servizio AWS.
L'applicazione Remote Portal è una piattaforma multi-tenant globale. Questa piattaforma, il relativo database, il back-end e il front-end sono ospitati nell'AWS nella regione di Francoforte, in Germania.

7 Manutenzione e livello di servizio

Bosch offre un accordo sul livello di assistenza (SLA) dedicato per i rivenditori con firma di Remote System Management di Bosch. Questo SLA illustra in dettaglio il processo di supporto, manutenzione e disponibilità in garanzia per Remote System Management di Bosch e contiene dettagli di contatto per hotline di emergenza, clausole penali, ecc.
Per ulteriori informazioni, contattare il rappresentante di vendita locale.

8 Obblighi dei clienti e degli utenti

Per i clienti diretti di Bosch è necessaria l'accettazione dei Termini e condizioni per rivenditori di software come servizio al fine di ottenere abbonamenti o licenze per Remote System Management. Per l'attivazione di licenze di servizi o abbonamenti, gli utenti devono accettare i termini e le condizioni di Remote Portal. Ulteriori obblighi includono:

- 8.1. Il collegamento Internet tra clienti, il rispettivo centro di monitoraggio/sala di controllo e la sede di installazione dei dispositivi compatibili (incluse le telecamere video, definite di seguito "Dispositivi") fino all'interfaccia Internet del data center utilizzata da Bosch, nonché il rapporto dei clienti finali tra il cliente e i suoi partner contrattuali sono a esclusiva responsabilità dei clienti.
- 8.2. L'installazione, l'utilizzo, la manutenzione e, se necessario, la riparazione dei dispositivi sono a esclusiva responsabilità dei clienti.
- 8.3. L'applicazione non è progettata né garantita per l'utilizzo in applicazioni ad alto rischio che richiedono prestazioni fail-safe speciali, ad esempio negli ambiti di operatività di impianti nucleari, controllo del traffico aereo, supporto alla vita o altri dispositivi, sistemi o applicazioni in cui il guasto di un dispositivo o di un'applicazione potrebbe provocare direttamente il decesso, infortuni, lesioni fisiche o danni ambientali gravi ("attività ad alto rischio"). In deroga a qualsiasi altra disposizione, i clienti non sono autorizzati a utilizzare l'Applicazione, né a permetterne l'utilizzo a terze parti, nell'ambito di attività ad alto rischio.
- 8.4. Ottenere il consenso necessario delle persone interessate in conformità alle normative su sicurezza e protezione dei dati, poiché i dati personali vengono raccolti, elaborati o utilizzati nel corso dell'utilizzo dell'applicazione da parte delle suddette persone e la legislazione non permette tale raccolta, elaborazione o utilizzo senza la necessità di ottenere il consenso, ciò si applica al caso in questione.
- 8.5. Prima di inviare i dati e le informazioni a Bosch, verificare che nei dati o nelle informazioni non siano presenti virus o altro malware e che i programmi antivirus soddisfino i requisiti più recenti.
- 8.6. Segnalare eventuali difetti dei servizi contrattuali a Bosch subito dopo aver rilevato tali difetti. In caso di ritardo nell'invio della notifica o se la notifica non viene fornita nonostante il cliente sia a conoscenza del difetto, si esclude la riduzione unilaterale del pagamento della tariffa, la sospensione da parte del cliente, nonché la conclusione straordinaria.
- 8.7. I seguenti ruoli e attività sono a esclusiva responsabilità del cliente:
  - 8.7.1. L'assegnazione di ruoli e autorizzazioni alle persone o unità corrispondenti per i ruoli utente disponibili nel Remote Portal e la gestione di tali ruoli e autorizzazioni.
  - 8.7.2. L'assegnazione di dispositivi a partner contrattuali del cliente e ai siti dei partner contrattuali.
  - 8.7.3. La fornitura, l'installazione e il collegamento di dispositivi adeguati per il funzionamento in conformità ai requisiti di sistema. L'Applicazione supporta il funzionamento dei dispositivi da parte del cliente mediante le funzioni illustrate.

9 Informazioni correlate al GDPR

Finalità dell'elaborazione dei dati

Bosch elabora i dati personali solo nella misura in cui ciò sia necessario e nelle modalità richieste:

1. al fine di soddisfare gli obblighi di Bosch ai sensi dell'accordo/dei termini di utilizzo dell'offerta del servizio Remote System Management; e
2. per conformità alle istruzioni del cliente fornite di volta in volta (che possono essere istruzioni specifiche o generiche, come specificato nel presente accordo o altrimenti comunicate dal cliente a Bosch); e
3. non elabora i dati personali per nessun'altra finalità.

Categorie dei dati

- Dati dei dispositivi: dati immessi dal titolare del trattamento dei dati o trasferiti dal dispositivo del titolare del trattamento dei dati - dati master del dispositivo, dati di telemetria sull'integrità del dispositivo e metadati delle versioni software. Posizione e persona di contatto di un dispositivo. Dati utilizzati per abilitare il servizio Remote System Management fornito al titolare del trattamento dei dati.
- Registri relativi ai dispositivi: le attività dei dispositivi vengono registrate per abilitare la risoluzione dei problemi del sistema.
- Dati di configurazione utente: dati immessi dal titolare del trattamento dei dati durante l'utilizzo della soluzione, ad esempio informazioni sull'accesso degli utenti, inclusi indirizzo IP, azienda, nome, cognome e indirizzo e-mail necessari per fornire all'utente l'accesso all'applicazione.
- Registri delle operazioni degli utenti: documentazione dell'utilizzo del sistema degli utenti, incluse le operazioni eseguite e i relativi contrassegni orari. Utilizzati per aiutare a risolvere i casi di manutenzione e per migliorare l'esperienza utente.
- Dati non personali, ad esempio dati su siti, account cliente e di configurazione del servizio, inclusi tipi e flussi.

Soggetti dei dati

- Dipendenti del cliente
- Utenti finali o partner contrattuali del cliente ("cliente del cliente")

Subcontraenti

Tutti i subcontraenti sono elencati nella **Tabella 1**.

	Nome e indirizzo del subcontraente e nome del responsabile della privacy dei dati/della persona di contatto per domande relative alla privacy	**Ambito del servizio (ambito dell'ordine effettuato dal contraente)**	**Luogo dell'elaborazione dei dati**	**Trasferimento/ accesso ai dati personali del cliente (tipo di dati e gruppo di soggetti dei dati)**
1	Servizi Web Amazon (AWS)	Provider di infrastruttura/hosting (come delineato nel concetto di sicurezza) e provider di servizi	Regioni dell'infrastruttura AWS (vedere la sezione 6)	Tutte le categorie e i soggetti dei dati elencati in dati 9

	Nome e indirizzo del subcontraente e nome del responsabile della privacy dei dati/della persona di contatto per domande relative alla privacy	Ambito del servizio (ambito dell'ordine effettuato dal contraente)	Luogo dell'elaborazione dei dati	Trasferimento/ accesso ai dati personali del cliente (tipo di dati e gruppo di soggetti dei dati)
		gestiti per archiviazione, manipolazione e recupero dei dati, nonché per la connettività cloud		
2	Robert Bosch India Incaricato della protezione dei dati di Bosch India (RBEI/ DSO) DPO.India@in.bosch.com	Gruppo limitato di supporto operativo tecnico	No.123, Industrial Layout, Hosur Road, Koraman-galaBengaluru-560 095 Karnataka, India	Tutte le categorie e i soggetti dei dati elencati in dati 9 Il team OPs può accedere solo a livello di sistema operativo all'applicazione e all'archiviazione, non a livello di account o di sito
3	Bosch.IO GmbH https://www.bosch-digital.com/imprint/	Funzionamento e manutenzione del database Digital Device Twin (https://eclipse.dev/ditto/) per archiviazione, manipolazione e recupero dei dati del dispositivo	Regioni dell'infrastruttura AWS (vedere la sezione 6)	Dati dei dispositivi per categoria dei dati

Tabella 1

Misure tecniche e organizzative

Le seguenti misure tecniche e organizzative sono accettate tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati e specificate nel presente singolo caso. Vedere l'elenco dei modelli di esempio.

- I. Misure per garantire la riservatezza (art. 32 par. 1 lit. b del GDPR)
  - I. Controllo degli accessi fisici: nessun accesso non autorizzato ai sistemi di elaborazione dei dati.
  - II. Controllo degli accessi logici: nessun utilizzo non autorizzato del sistema tramite password (sicure), meccanismi di blocco automatico, autenticazione a due fattori e crittografia dei dati.

  - III. Controllo degli accessi ai dati: nessuna lettura, copia, modifica o rimozione non autorizzata nel sistema tramite concetti di autorizzazione, diritti di accesso specifici dell'utente e registrazione dell'accesso.
  - IV. Controllo mediante separazione: elaborazione separata dei dati raccolti per finalità varie.

- II. Misure che garantiscono l'integrità (art. 32 par. 1 lit. b del GDPR)
  - I. Controllo dei trasferimenti: nessuna lettura, copia, modifica o rimozione non autorizzata durante la trasmissione o il trasporto elettronico tramite crittografia, reti private virtuali (VPN) e firma elettronica.
  - II. Controllo degli inserimenti: determinazione se e da chi i dati personali sono stati inseriti, modificati o rimossi nei sistemi di elaborazione dei dati tramite registrazione e gestione dei documenti.

- III. Misure per garantire disponibilità e resilienza (art. 32 par. 1 lit. b del GDPR), ad es.:
  - I. Controllo della disponibilità: protezione da danni accidentali o distruzione o perdita tramite strategia di backup.
  - II. Controllo dell'ordine: nessuna elaborazione dei dati in fase di messa in funzione in conformità all'art. 28 del GDPR senza istruzioni corrispondenti da parte del titolare del trattamento dei dati mediante progettazione esplicita del contratto, gestione degli ordini formalizzata, selezione rigorosa del fornitore del servizio, obbligo di convincimento preventivo e ispezioni di follow-up.
  - III. Resilienza: i sistemi e servizi (ad es. archiviazione, accesso, funzionalità di linea, ecc.) sono progettati in modo da garantire anche elevate sollecitazioni intermittenti o carichi elevati costanti delle elaborazioni.

- IV. Misure per la presentazione con l'uso di pseudonimi dei dati personali mediante:
  - I. Separazione dei dati master del titolare del trattamento dei dati del cliente e dei dati del cliente
  - II. Utilizzo di ID di personale, clienti e fornitori anziché dei relativi nomi

- V. Misure per la crittografia dei dati personali mediante:
  - I. Crittografia simmetrica
  - II. Crittografia asimmetrica
  - III. Hashing

- VI. Misure per ripristinare rapidamente la disponibilità dei dati personali dopo un incidente fisico o tecnico mediante il concetto di backup.

- VII. Procedure di revisione, valutazione ed esame in modo periodico (art. 32 par. 1 lit. d del GDPR; art. 25 par. 1 del GDPR) tramite:
  - I. Gestione della privacy
  - II. Gestione delle risposte agli incidenti
  - III. Protezione dei dati per impostazione predefinita (art. 25 par. 2 del GDPR)
  - IV. Valutazione mediante DSO, controlli IT
  - V. Valutazione, certificazioni, controlli esterni

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309141013