Remote System Management

CBS-RM-DIPx

de Servicebeschreibung

Inhaltsverzeichnis

1 Hauptfunktionen

Mit dem Service Remote System Management von Bosch können Sie das Internet der Dinge (IoT) für sich nutzen, um sichere, transparente und kosteneffiziente Geräteverwaltung während des gesamten Lebenszyklus eines Videosystems zu bieten. Dieser Service ermöglicht Endbenutzern, Systemintegratoren und Errichtern die Bestands- und Update-Verwaltung sowie Zustandsüberwachung für ein komplettes Bosch Videosystem (DIVAR IP + BVMS + Kameras) von einer zentralen Remote Portal-Plattform.

Mit diesem Service können sich Endkunden rund um die Uhr auf sichere Systemüberwachung verlassen. Der Benutzer kann bei Auftreten von Problemen proaktiv vorgehen und diese beheben, z. B. bevor Videoaufzeichnungen aufgrund eines Festplattenausfalls verloren gehen. Die sichere MQTTS-Verbindung sorgt zudem für Datenschutz: Über diese Verbindung ist kein Zugriff auf Videomaterial möglich, da dieses Protokoll keine Video- und Bilddatenübertragung unterstützt. Außerdem ermöglicht der Service die Installation von Software und Firmware aus der Ferne, damit das System jederzeit aktuell und geschützt ist. Die Cloud-Konnektivität basiert auf einer einzelnen ausgehenden Verbindung von DIVAR IP zu Remote Portal, wobei DIVAR IP die eingehende und ausgehende Kommunikation des gesamten Videosystems konsolidiert.

Der Service wurde für die Verwendung durch größere Endkundenunternehmen entwickelt, die ihre eigene Systemwartung an mehreren verteilten Standorten durchführen, und auch für Errichter, die solche Dienstleistungen für eine Reihe verschiedener Endkunden anbieten. Die Vorteile der Verwendung von Remote System Management sind eine effizientere Durchführung von Systemwartungsarbeiten, Vermeidung unnötiger Standortbesuche dank der Fernwartungsfunktionen, z. B. zur Installation von Updates im Falle von Security Advisories, und eine bessere Vorbereitung von Standortbesuchen dank aktueller Systeminformationen. Positiver Nebeneffekt: Umfassender Service bei minimalen CO_2-Emissionen. Darüber hinaus können Benutzer die Serviceerfahrungen noch weiter verbessern, indem sie proaktiv handeln und Konflikte im Einsatzbereich lösen, bevor (interne) Kunden überhaupt erkennen, dass ein Problem besteht.
Funktionsdetails können Sie den jeweiligen Servicedatenblättern entnehmen.

Hinweis!

Die Datenblätter finden Sie im entsprechenden Produktkatalog für Ihre Region oder Ihr Land.

2 Systemanforderungen

Anforderungen an die Software

Die Remote Portal-Webschnittstelle kann mit modernen Webbrowsern verwendet werden, die HTML5 unterstützen. Für beste Ergebnisse empfiehlt Bosch die Verwendung von Google Chrome.

Geräteanforderungen

Um Remote System Management in vollem Umfang nutzen zu können, muss auf Bosch IP Kameras die Firmware-Version 6.50 oder höher ausgeführt werden.
Nur bestimmte DIVAR IP Modelle werden unterstützt (siehe Datenblatt). Die Software-Mindestanforderung für diese Modelle ist die Unterstützung von DIVAR IP System Manager 2.0 oder höher. Details erhalten Sie im entsprechenden Datenblatt.
Die erforderliche Bandbreite ist abhängig von den Spezifikationen des Videosystems und der Standortstruktur, d. h. von der Anzahl der Kameras und DIVAR IP Geräte vor Ort. Bosch empfiehlt eine Mindestbandbreite von 11 Mbit/s bzw. 1,31 Mbit/s pro DIVAR IP, da DIVAR IP eingehende und ausgehende Kommunikation für sich selbst und verbundene Kameras konsolidiert. Diese Empfehlung basiert auf dem anspruchsvollsten Anwendungsfall hinsichtlich Bandbreite, nämlich dem Download größerer Update-Dateien, die immer dann einen hohen Bandbreitenbedarf erzeugen, wenn solche Updates von Remote Portal ausgelöst werden. Während der restlichen Betriebszeit ohne solche Spitzen sind üblicherweise Bandbreiten von ca. 10 Kbit/s erforderlich, z. B. für die Überwachung von Zustandsparametern und die Übermittlung anderer Telemetriedaten.

Hinweis!

Diese Bandbreitenanforderung kann variieren und der Benutzer muss überprüfen, ob die verfügbare Bandbreite den Anforderungen der Anwendung gerecht wird. Bosch stellt verschiedene Tools zur Berechnung der erforderlichen Bandbreite zur Verfügung, übernimmt jedoch keine Verantwortung für tatsächliche Bandbreitenverfügbarkeit und ordnungsgemäße Konfiguration.

3 Web-Anwendung

Remote System Management ist in Remote Portal integriert, das als zentrale webbasierte Plattform für die Serviceaktivierung und weitere allgemeine Funktionen dient, unabhängig vom unten beschriebenen Serviceangebot.

System- und Geräteverwaltung mit Dashboard-Ansicht
Systeme und einzelne Geräte können hierarchisch gruppiert werden, damit sie dem Kunden- oder Installationsort entsprechen, der Zugriff auf bestimmte Geräte eingeschränkt ist oder der Status mehrerer Geräte zusammengefasst wird.

Serviceübersicht
Im Bereich „Services“ im Remote Portal finden Sie eine Übersicht aller verfügbaren Services für die Gerätetypen. Jeder Service zeigt eine Zusammenfassung aller Geräte und Systeme, in denen er aktiv verwendet wird.

Servicelizenzverwaltung
Services können durch den Besuch des Remote Portal nach der Erstinbetriebnahme von DIVAR IP im Remote Portal aktiviert werden.
Der Remote System Management-Service erfordert Lizenzen für die Aktivierung. Je nach Modell und Betriebsmodus von DIVAR IP gelten verschiedene Lizenzen. Weitere Informationen finden Sie in den Datenblättern. Im Bereich „Servicelizenzierung“ von Remote Portal werden Lizenzen verwaltet und aktiviert.

Benutzerverwaltung
Mit Remote Portal kann der Zugriff auf Geräte und Services präzise gesteuert werden. Die Rollen *Administrator*, *Techniker* und *Endbenutzer* können anhand des Rollenmanagements individuell mit Systemen, Gruppen und Services verknüpft werden.

Hinweis!

Weitere Informationen zum Remote Portal finden Sie auf der jeweiligen Produktseite: https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/

4 Dokumentation

Benutzerdokumentation und Datenblätter aller einzelnen Systeme, die auf DIVAR IP basieren, finden Sie hier:

Technische Schulungen:	https://academy.boschsecurity.com/

Hinweis: Eine eigenständige Einführungsschulung für Remote System Management wird angeboten. Diese Schulung wird später in die Zertifizierungsschulung für DIVAR IP all-in-one integriert.

Anleitung/Konfigurationshinweise:	https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt
Datenblätter/ Anwendungshinweise:	https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip

5 Open-Source-Softwarekomponenten

Die Open-Source-Softwarekomponenten, die in der Remote Portal-Plattform enthalten sind, finden Sie hier: https://remote.boschsecurity.com/open_source/open_source_licenses.txt

6 Service-Hosting

Die hier aufgeführten Services werden in der AWS-Infrastruktur „as a Service“ gehostet.
Die Anwendung „Remote Portal“ ist eine globale mandantenfähige Plattform. Diese Plattform, ihre Datenbank, Backend und Frontend werden in der AWS-Region Frankfurt (Deutschland) gehostet.

7 Wartungs- und Service-Ebenen

Bosch bietet einen dedizierten Servicevertrag (SLA) für zertifizierte Händler von Remote System Management von Bosch. Dieser SLA enthält Details zur garantierten Verfügbarkeit, dem Wartungs- und Support-Prozess für Remote System Management von Bosch und Kontaktdetails für Notfall-Hotlines, Vertragsstrafen usw.
Weitere Informationen erhalten Sie bei Ihrem Vertriebsmitarbeiter vor Ort.

8 Kunden- und Benutzerverpflichtungen

Direktkunden von Bosch müssen die allgemeinen Geschäftsbedingungen für Software-as-a-Service-Händler akzeptieren, um Remote System Management-Lizenzen oder -Abonnements erhalten zu können. Für die Aktivierung von Servicelizenzen oder -abonnements müssen Benutzer die allgemeinen Geschäftsbedingungen von Remote Portal akzeptieren. Zu den weiteren Verpflichtungen zählen:

- 8.1. Für die Internetverbindung zwischen dem Kunden, seiner Leitstelle/seinem Kontrollraum und dem Installationsort kompatibler Geräte (inkl. Videokameras, nachfolgend „Geräte“ genannt) bis zur von Bosch verwendeten Internetschnittstelle des Rechenzentrums, sowie die Endkundenverbindung zwischen dem Kunden und seinen Vertragspartnern ist ausschließlich der Kunde verantwortlich.
- 8.2. Für die Installation, Bedienung, Wartung und – falls erforderlich – Reparatur von Geräten ist ausschließlich der Kunde verantwortlich.
- 8.3. Die Anwendung ist nicht ausgelegt und bietet keine Garantie für den Einsatz in Hochrisiko-Anwendungen, die eine besondere Ausfallsicherung erfordern, z. B. beim Betrieb von Kernanlagen, Flugverkehrskontrolle, Lebenserhaltung oder anderen Anwendungen, Geräten oder Systemen, bei denen ein Ausfall eines Geräts oder einer Anwendung direkt zu Tod, Personenschaden oder schweren Sach- oder Umweltschäden führen kann („Hochrisiko-Aktivitäten“). Ungeachtet anders lautender Bestimmungen dürfen Kunden die Anwendung nicht bei Hochrisiko-Aktivitäten verwenden und dies auch keiner dritten Partei erlauben.
- 8.4. Das Einholen der notwendigen Zustimmung der betroffenen Personen gemäß Datensicherheits- und Datenschutzvorschriften, wenn personenbezogene Daten beim Einsatz der Anwendung durch die erwähnten Personen erhoben, verarbeitet oder genutzt werden und kein Gesetz eine solche Erhebung, Verarbeitung oder Nutzung ohne erforderliche Einholung der Einwilligung zulässt, ist in diesem Fall anwendbar.
- 8.5. Prüfen Sie Daten und Informationen auf Viren oder andere Malware, bevor Sie sie an Bosch übermitteln, und stellen Sie sicher, dass Ihre Antiviren-Programme auf dem neuesten Stand sind.
- 8.6. Mängel bei Vertragsleistungen sind unmittelbar nach ihrer Kenntnisnahme an Bosch zu melden. Wenn ein Mangel verzögert oder nicht gemeldet wird, obwohl der Kunde Kenntnis des Mangels hatte, sind ein einseitiges Reduzieren oder Aussetzen der Gebühren durch den Kunden sowie eine außerordentliche Kündigung ausgeschlossen.
- 8.7. Für die folgenden Aufgaben ist ausschließlich der Kunde verantwortlich:
  - 8.7.1. Zuweisen von Rollen und Berechtigungen zu den entsprechenden Personen bzw. Geräten zu den verfügbaren Benutzerrollen im Remote Portal und Verwalten dieser Rollen und Berechtigungen.
  - 8.7.2. Zuordnung von Geräten zu Vertragspartnern des Kunden und zu den Standorten der Vertragspartner.
  - 8.7.3. Erwerben, Installieren und Anschließen geeigneter Geräte für den Betrieb gemäß den Systemanforderungen. Die Anwendung unterstützt den Betrieb der Geräte des Kunden mithilfe der beschriebenen Funktionen.

9 Informationen zur DSGVO

Zweck der Datenverarbeitung

Bosch verarbeitet personenbezogene Daten nur im jeweils erforderlichen Umfang und auf die jeweils erforderliche Weise:

1. Zur Erfüllung der Verpflichtungen von Bosch gemäß den allgemeinen Geschäftsbedingungen/Nutzungsbedingungen des Remote System Management-Serviceangebots.
2. Bisweilen zur Erfüllung von Anweisungen durch den Kunden (dies können spezifische oder allgemeine Anweisungen sein, die in dieser Vereinbarung festgelegt sind oder anderweitig vom Kunden an Bosch gemeldet wurden).
3. Bosch darf personenbezogene Daten nicht zu anderen Zwecken verarbeiten.

Datenkategorien

- Gerätedaten: Vom Datenverantwortlichen eingegebene oder vom Gerät des Datenverantwortlichen übertragene Daten – Gerätestammdaten, Telemetriedaten zum Gerätezustand und Metadaten der Softwareversionen. Standort und Ansprechpartner eines Geräts. Wird zum Aktivieren des bereitgestellten Remote System Management-Services für den Datenverantwortlichen verwendet.
- Gerätebezogene Protokolle: Geräteaktivitäten werden protokolliert, um eine Fehlerbehebung für das System zu ermöglichen.
- Benutzerkonfigurationsdaten: Vom Datenverantwortlichen während der Nutzung der Lösung eingegebene Daten, z. B. Benutzerzugangsinformationen, einschließlich IP-Adresse, Unternehmen, Vorname, Nachname und E-Mail-Adresse für den Benutzerzugriff auf die Anwendung.
- Benutzeraktionsprotokolle: Dokumentation der Systemnutzung der Benutzer einschließlich durchgeführter Aktionen und zugehöriger Zeitstempel. Dient zur Unterstützung von Wartungsarbeiten und zur Verbesserung der Benutzererfahrung.
- Nicht personenbezogene Daten wie Standort, Kundenkonto und Servicekonfigurationsdaten einschließlich Typen und Flows.

Betroffene Personen

- Mitarbeiter des Kunden
- Endbenutzer oder Vertragspartner des Kunden („Kunde des Kunden“)

Unterauftragnehmer

Alle Unterauftragnehmer sind in **Tabelle 1** aufgeführt.

	Name und Anschrift des Unterauftragnehmers und Name des Datenschutzbeauftragten/Ansprechpartners für Fragen zum Datenschutz	Leistungsumfang (Auftragsumfang des Auftragnehmers)	Ort der Datenverarbeitung	Übermittlung/ Zugriff auf personenbezogene Daten des Kunden (Datenart und Gruppe der betroffenen Personen)
1	Amazon Web Services (AWS)	Infrastruktur/Hosting-Provider (wie im Sicherheitskonzept beschrieben) sowie Managed Service Provider für die Speicherung, Bearbeitung und den Abruf von Daten und Cloud-Konnektivität	AWS-Infrastrukturregionen (siehe Abschnitt 6)	Alle unter Daten 9 aufgeführten Kategorien und betroffenen Personen
2	Robert Bosch India Datenschutzbeauftragter Bosch India (RBEI/DSO) DPO.India@in.bosch.com	Eingeschränkte Gruppe von Technical Operations Support	No. 123, Industrial Layout, Hosur Road, Koramangala, Bengaluru, 560095 Karnataka, India	Alle in Abschnitt 9 aufgeführten Kategorien und Betroffenen Das OPs-Team hat nur Zugriff auf Anwendung und Speicher auf BS-Ebene, nicht auf Konto- oder Standortebene
3	Bosch.IO GmbH https://www.bosch-digital.com/de/impressum/	Betrieb und Pflege der Digital Device Twin Datenbank (https://eclipse.dev/ditto/) zur Speicherung, Bearbeitung und Abfrage von Gerätedaten	AWS-Infrastrukturregionen (siehe Abschnitt 6)	Datenkategorie Gerätedaten

Tabelle 1

Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen (TOMs) sind vom Datenverantwortlichen und Auftragsverarbeiter vereinbart und im vorliegenden Einzelfall festgelegt. Siehe Musterliste.

- I. Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 Buchst. b der DSGVO)
  - I. Physische Zugriffskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungssystemen.

  - II. Logische Zugriffskontrolle: Keine unbefugte Systemnutzung durch Einsatz von (sicheren) Passwörtern, automatischen Sperrmechanismen, Zwei-Faktor-Authentifizierung und Datenverschlüsselung.
  - III. Datenzugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Ändern oder Entfernen innerhalb des Systems durch Einsatz von Berechtigungskonzepten, benutzerspezifischen Zugriffsrechten und Zugriffsprotokollierung.
  - IV. Trennungskontrolle: Getrennte Verarbeitung von erhobenen Daten für verschiedene Zwecke.

- II. Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 Buchst. b der DSGVO)
  - I. Übermittlungskontrolle: Kein unbefugtes Lesen, Kopieren, Ändern oder Entfernen bei elektronischer Übermittlung oder Transport durch Einsatz von Verschlüsselung, Virtual Private Networks (VPN) und elektronischer Signatur.
  - II. Eingangskontrolle: Bestimmung ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, geändert oder entfernt wurden durch Einsatz von Protokollierung und Dokumentenverwaltung.

- III. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b der DSGVO), z. B.:
  - I. Verfügbarkeitskontrolle: Schutz vor unbeabsichtigter Beschädigung, Vernichtung oder Verlust durch Einsatz einer Sicherungsstrategie.
  - II. Auftragskontrolle: Keine Datenverarbeitung bei Auftrag gemäß Art. 28 der DSGVO ohne entsprechende Anweisungen des Datenverantwortlichen durch Einsatz von expliziter Vertragsgestaltung, formalisiertem Auftragsmanagement, gründlicher Auswahl des Dienstleisters, Verpflichtung zur Vorabzustimmung und Nachkontrollen.
  - III. Belastbarkeit: Systeme und Services (z. B. Speicher, Zugriff, Leitungskapazitäten usw.) sind so ausgelegt, dass auch periodische hohe Belastungen oder hohe Dauerbelastungen bei Verarbeitungsvorgängen gewährleistet werden können.

- IV. Maßnahmen zur Pseudonymisierung von personenbezogenen Daten durch Einsatz von:
  - I. Trennung von Stammdaten des Datenverantwortlichen beim Kunden und Kundendaten
  - II. Einsatz von Personal-, Kunden- und Lieferantennummer anstelle von Namen

- V. Maßnahmen zur Verschlüsselung von personenbezogenen Daten durch Einsatz von:
  - I. Symmetrische Verschlüsselung
  - II. Asymmetrische Verschlüsselung
  - III. Hashen

- VI. Maßnahmen zur schnellen Wiederherstellung der Verfügbarkeit von personenbezogenen Daten nach einem physischen oder technischen Zwischenfall.

- VII. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d der DSGVO; Art. 25 Abs. 1 der DSGVO) durch Einsatz von:
  - I. Datenschutzmanagement
  - II. Vorfallsmanagement
  - III. Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 der DSGVO)
  - IV. Bewertung durch DSO, IT-Prüfungen

– V. Externe Bewertung, Prüfungen, Zertifizierungen

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

Building solutions for a better life.

202309141013