CBS-RM-DIP4 Remote System Management DIP 4000 1jahr

Remote Portal

- Zentralisierte Bestandsverwaltung mit schnellem Fernzugriff auf das gesamte System durch Verbindung mit dem Remote Portal
- Optimierte Systemverwaltung und -wartung für die Implementierung von Updates und Patches, damit Ihr gesamtes System jederzeit aktuell und geschützt ist
- Detaillierte Zustands- und Alarmüberwachung liefern Echtzeitinformationen zu einzelnen Geräten und dem gesamten System
- Cloud-Verbindung mit Fokus auf Datenschutz

Mit dem Remote System Management Service von Bosch können Sie das Internet der Dinge (IoT) für sich nutzen. Mit dem benutzerfreundlichen Toolset erhalten Sie Funktionen für sichere, transparente und kosteneffiziente Geräteverwaltung während der gesamten Nutzungsdauer eines Geräts oder Systems. Dieser Service ermöglicht Benutzern die Bestands- und Update-Verwaltung sowie Zustandsüberwachung für das gesamte System über eine zentrale Remote Portal-Plattform.

Funktionen

Bestandsverwaltung
Verbinden Sie Ihr System einfach mit Remote Portal, um eine sichere Geräteverbindung und überprüfbare Geräteregistrierung sicherzustellen. Diese zentralisierte Verwaltungsplattform bietet einen durchgehenden Echtzeit-Überblick über den Systembestand, einschließlich Informationen über aktuelle Software- und Firmware-Versionen.

Update-Verwaltung
Die Update-Verwaltungsfunktion ermöglicht die Remote-Verwaltung und -Implementierung von Updates für ein Gerät oder das gesamte System an einem oder mehreren Standorten.

- Sicherheits-Patches und Firmware-/Software-Updates können schnell implementiert werden.
- Anhand automatisch generierter Update-Berichte erhalten Sie eine detaillierte Zusammenfassung der Änderungen, die durch ein Update implementiert wurden.

Zustandsüberwachung
Mithilfe der Zustandsüberwachungsfunktionen des Remote System Management Services können Sie fundierte Entscheidungen treffen sowie Fehler proaktiv beheben. Dies sorgt für eine hohe Systemverfügbarkeit und Sie müssen weniger Zeit am Standort verbringen.

- Überwachen Sie Verbindungen, Update-Verfügbarkeit und die Berechtigungsstatus von Geräten.
- Erhalten Sie detaillierte Einblicke zu Hardware- und Aufzeichnungszustand.
- Definieren Sie, welche Zustandsmeldungen per E-Mail gesendet werden.

Unterstützter Betriebsmodus
Die DIVAR IP Verbindung mit Remote Portal und der Remote System Management Service unterstützen alle Betriebsmodi – BVMS, Video Recording Manager (VRM) und iSCSI-Target. Die Modi VRM und iSCSI bieten nur die Verwaltung des DIVAR IP Geräts. Zur Verwaltung eines kompletten Systems, einschließlich Kameras, muss DIVAR IP im BVMS Modus verwendet werden. Im Kontext von Remote System Management

sind die Modi VRM und iSCSI effektiv bei Verwendung als Subsysteme, die ein übergreifendes Videosystem integrieren. Dies beinhaltet ein DIVAR IP Hauptsystem, das im BVMS Modus betrieben wird.
Hinweis: Jedes DIVAR IP Gerät verbindet sich für alle Betriebsmodi einzeln mit Remote Portal. DIVAR IP Geräte, die zu einem übergeordneten Videosystem gehören, müssen innerhalb des jeweiligen Unternehmenskontos entsprechend gruppiert werden.

Datensicherheit
Die höchstmögliche Sicherheit für Remote-Gerätezugriff und Datenübertragung wird gewährleistet.
Durch ein integriertes Trusted Platform Module (TPM) und die Public-Key-Infrastruktur (PKI) erhalten Sie einen hervorragenden Identitätsnachweis und Manipulationsschutz. Dies ermöglicht die gegenseitige zertifikatbasierte Authentifizierung zwischen Gerät und Cloud sowie eine sichere Verbindung für Remote-Gerätezugriff.
Die lokale Gerätesicherheit wird durch mehrschichtige Konfigurationen zum Härten der Sicherheit und Verwendung der Windows Server-Sicherheitsfunktionen gewährleistet, darunter:

- Windows Defender Device Guard, um sicherzustellen, dass nur vertrauenswürdige Software auf dem Server ausgeführt wird.
- Control Flow Guard für integrierten Schutz vor Angriffen, die auf Speicherbeschädigung abzielen.
- Windows Defender Antivirus, eine integrierte Antischadsoftware-Lösung, die Sicherheits- und Antischadsoftware-Verwaltung bietet.
- Windows Defender Credential Guard, das virtualisierungsbasierte Sicherheit zum Isolieren von Anmeldeinformationen verwendet und verhindert, dass Kennworthashes oder Kerberos-Tickets abgefangen werden.
- Local Security Authority (LSA), das sich im LSASS-Prozess (Local Security Authority Security Service) befindet, überprüft Benutzer für lokale und Remote-Anmeldungen und setzt lokale Sicherheitsrichtlinien durch.

Datenschutz
Datenschutz bei Kunden- und Benutzerdaten wird von Remote System Management durch die folgenden Maßnahmen gewährleistet:

- Dedizierte Cloud-Verbindung ausschließlich zu Wartungs- und Überwachungszwecken (basierend auf dem MQTTS-Protokoll).
- Kein Remote-Videozugriff, aber rund um die Uhr transparente Informationen zum Systemzustand.
- Video- und Wartungsdaten werden für DIVAR IP Geräte getrennt: Fernverbindung für Systemwartungsdienste ohne die Gefahr eines unbefugten Videozugriffs.

Vereinfachte Firewall-Verwaltung
DIVAR IP Geräte konsolidieren die gesamte Kamerakommunikation für ein Videosystem in einer einzelnen ausgehenden Verbindung zu Remote Portal. Mit nur einer ausgehenden Verbindung wird der Aufwand für IT-Firewall-Verwaltungsaufgaben deutlich reduziert.

Remote Portal-Integration
Der Remote System Management Service ist nahtlos in das Remote Portal integriert.
Die erste Verbindung mit dem Remote Portal ist kostenfrei.
Mit der entsprechenden Lizenz können die Remote System Management Servicefunktionen online in Remote Portal aktiviert werden.

Hinweis
Funktionalität und Services können je nach Gerät variieren.
Weitere Informationen zu den entsprechenden Systemanforderungen finden Sie in der Dokumentation der jeweiligen Geräte.

Registrieren Sie sich kostenlos:
https://remote.boschsecurity.com

Hinweis: Remote System Management bietet einen kostenlosen Testzeitraum. Nach dessen Ablauf können Benutzer weiterhin die folgenden Funktionen nutzen:

- Remote Portal-Verbindung.
- Grundlegende Bestandsverwaltung zur Anzeige und Verwaltung der installierten Geräte.
- Überwachung von Verbindung, Update-Verfügbarkeit und Berechtigungs-/Lizenzstatus.

Hinweis
Servicedetails
Zusätzliche Servicedetails werden im Servicebeschreibungsdokument für Remote System Management beschrieben, das im Produktkatalog heruntergeladen werden kann.

Im Lieferumfang enthaltene Teile

Menge	Komponente
1	Remote System Management Lizenz für 1 Jahr

Technische Daten

Konnektivität

Netzwerk	Für optimale Leistung sollte eine feste Internetanbindung für die Verbindung von Geräten mit der Bosch Security Cloud verwendet werden. Mobile Internetverbindungen können

	verwendet werden, dies kann sich jedoch auf Leistung und Verfügbarkeit auswirken.
Browser	Die browserbasierten Schnittstellen von Remote Portal lassen sich am besten mit modernen Browsern darstellen: • Google Chrome • Firefox • Microsoft Edge **Hinweis**: JavaScript muss aktiviert sein.

Datensicherheit

Sicherer Kryptoprozessor (TPM)	TPM v2.0, RSA 2048 Bit, ECC256, SHA-256
PKI	X.509 Zertifikate
Netzwerksicherheit	TLS v1.2 oder höher, DTLS 1.2 oder höher
Lokale Verschlüsselung	BitLocker Geräteverschlüsselung, AES-256

Kompatibilität

Gerät	Minimale Firmware-/Software-Version
DIVAR IP all-in-one 4000	DIVAR IP System Manager 2.0
Bosch IP-Kameras (angeschlossen an das lizenzierte DIVAR IP all-in-one Gerät)	Firmware-Version 6.5

Bestellinformationen

CBS-RM-DIP4 Remote System Management DIP 4000 1jahr
Lizenz zum Aktivieren der Remote System Management Services für ein DIVAR IP all-in-one 4000 Gerät für den Zeitraum von 1 Jahr
Bestellnummer **CBS-RM-DIP4 | F.01U.410.890**

Vertreten von:

Europe, Middle East, Africa:
Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven, The Netherlands
Phone: + 31 40 2577 284
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com

Germany:
Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Tel.: +49 (0)89 6290 0
Fax:+49 (0)89 6290 1020
de.securitysystems@bosch.com
www.boschsecurity.com