BIS - Access Engine (ACE) 5.0

- Sistem distribuit de control al accesului, cu management grafic al alarmelor
- Integrare și interacțiune fără întreruperi cu sisteme video, anti-incendiu, anti-intruziune și PA/VA prin intermediul platformei comune BIS
- Rezilienţă ridicată datorită unei arhitecturi de sistem pe 4 niveluri și implementării redundante a componentelor critice
- Integrarea produselor terțe prin protocoale deschise și securizate și SDK
- Proces de înscriere eficient, care face integrarea mai rapidă și mai sigură

Controlul accesului a devenit, în prezent, una dintre cele mai importante tehnologii pentru creșterea securității persoanelor, a proprietăților și a activelor. BIS Access Engine și produse de control sofisticate oferă o gamă largă de funcții de control al accesului. Combinați pachetul de bază Access Engine cu funcții opționale pentru a construi un sistem personalizat de control al accesului care să vă satisfacă exact necesitățile. Apoi, utilizați software-ul Building Integration System pentru a integra Access Engine cu echipamentul dvs. de detectare a intruziunilor și de securitate video.

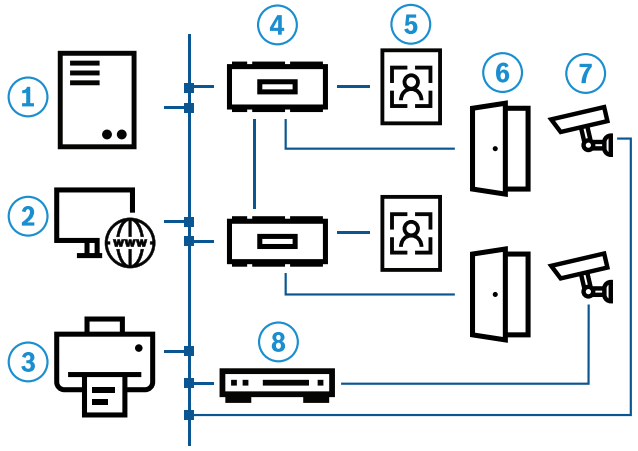
Prezentare generală a sistemului

Software-ul Access Engine (ACE), alături de componentele hardware de acces Bosch, este un sistem complet de control al accesului în cadrul Building Integration System (BIS). Acesta cuprinde toate caracteristicile esențiale ale oricărui sistem autonom de control al accesului, plus o gamă largă de îmbunătățiri opționale.

La fel ca alte motoare BIS, ACE beneficiază din plin de toate caracteristicile suplimentare BIS, cum ar fi hărți interactive de locație și planuri de acțiune pentru un management puternic, complet integrat al alarmelor. Mesajele de alarmă și evenimentele de control al accesului pot fi afișate cu informații grafice despre locație și instrucțiuni privind fluxul de lucru.

ACE folosește interfețele standard de utilizator BIS și flexibilitatea de personalizare a acestora. În plus, ACE oferă interfețe specifice de configurare a accesului pentru deținătorii de carduri, hardware de acces și reguli de acces.

Principalul beneficiu al familiei Building Integration System este integrarea unei game largi de sisteme de securitate și siguranță în aceeași sediu. Prin combinarea ACE cu alte motoare BIS (de exemplu, Automation și Video), puteți proiecta soluții inteligente de securitate, adaptate exact cerințelor licitației dvs.
Access Engine rulează pe o singură stație de lucru, într-un sistem client-server sau într-un mediu distribuit cu un server central și servere locale sau regionale. În mediul distribuit cu mai multe servere, toate dispozitivele, deținătorii de carduri și autorizațiile pot fi gestionate de pe serverul de nivel superior.
Pentru a asigura un nivel maxim de securitate și integritate a datelor, BIS ACE poate gestiona controlere RS485 de înaltă securitate cu protocol OSDP v2 pentru comunicații criptate autentificate și supravegherea cititorului.



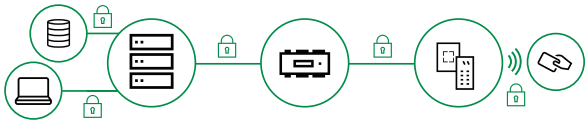
Poz.	Descriere (sistem cu un singur server)
1	Server BIS central cu Access Engine și software Video Engine
2	Stații de lucru multiple pentru gestionarea alarmelor sau înregistrare
3	Dispozitive de înregistrare, cum ar fi imprimantă de carduri, scanner de semnătură, cititor de înregistrare, cameră pentru fotografii de identitate
4	Controlere de acces
5	Cititoare de acces
6	Zăvoare electrice
7	Cameră IP
8	Recorder video digital, de ex. DIVAR, pentru înregistrarea alarmelor

Funcții

Pachetul de bază Access Engine, alături de controlerele de acces AMC, oferă următoarele caracteristici:

- O gamă largă de modele intuitive de uși șablon, care permit o configurare hardware rapidă și ușoară (de exemplu, ușă standard, turnichet, lift cu cititoare de timp și prezență etc.).
- Dialogul de configurare a modelului de ușă generează un plan de cablare pentru instalatorul hardware.
- Proces de integrare fluent, care include înregistrarea cardului și înregistrarea biometrică.
- Dialoguri personalizabile pentru a colecta doar informațiile personale necesare.
- Modele de timp pentru controlul accesului bazat pe timp, inclusiv definiția zilelor speciale, a sărbătorilor legale repetitive etc.
- Modele de timp pentru activarea/dezactivarea automată a conturilor deținătorilor de card, a codurilor PIN etc.
- Modele de timp pentru activarea/dezactivarea automată a setărilor sistemului, cum ar fi deblocarea unei uși de birou între orele 9:00 și 17:00
- Cod PIN suplimentar pentru armarea/dezarmarea alarmelor de intruși.
- Blocarea/deblocarea temporară a deținătorilor de carduri, fie manual, fie controlat în timp.
- Înscrierea cardurilor pe o listă neagră.
- Anti-revenire.
- Echilibrarea zonei de acces, inclusiv verificarea secvenței de acces, oferă un mijloc de limitare a numărului de persoane dintr-o anumită zonă, armând/dezarmând automat alarmele dacă o zonă este goală/nu este goală și generând liste de adunare.
- Autorizarea de tip N-Persons va acorda acces la o ușă numai atunci când un număr definit (N) de deținători de carduri autorizați prezintă ecusoanele la un cititor configurat corespunzător. Setarea poate fi efectuată pentru fiecare cititor în parte, pentru un număr de persoane de la 2 la N (nelimitat).
- Funcție Uși capcană pentru gestionarea a două uși cooperante cu două perechi de cititoare; recomandat pentru niveluri de securitate ridicate, de ex. intrări în sălile serverelor sau în departamente de cercetare.
- Tur de gardă: un sistem de ultimă generație de urmărire a patrulei, care utilizează cititoare existente de control al accesului, verificarea secvenței de acces și a timpului de acces. Orice încălcare a secvenței sau a timpului de patrulare provoacă o alarmă, care este apoi urmărită de

caracteristicile sofisticate BIS de gestionare a alarmelor. Rapoartele turului de gardă pot fi generate din jurnalul de evenimente BIS.

- Funcție de verificare aleatorie: deținătorii de carduri care accesează sau părăsesc locația pot fi opriți la întâmplare și îndrumați către personalul de securitate pentru o inspecție mai atentă. Cardurile aparținând „VIP”-urilor desemnate pot fi excluse de la verificarea aleatorie.
- Managementul vizitatorilor: cardurile vizitatorilor pot fi urmărite și gestionate separat în ceea ce privește perioadele de valabilitate și o potențială nevoie de escortă.
- Interfață pentru armarea/dezarmarea unui IDS (sistem de detecție a intruziunilor), inclusiv gestionarea autorizațiilor și alocarea cardurilor.
- Importul și exportul pe web a datelor deținătorilor de carduri stocate în sisteme terțe sau pe un server de director, cum ar fi Microsoft Active Directory sau Apache Directory.
- Toate informațiile personale, inclusiv fotografiile și semnăturile, sunt stocate într-o bază de date SQL securizată.
- Managementul nivelului de amenințare pentru a preconfigura până la 15 scenarii, inclusiv situații de blocare și evacuare.
- Interfață de lift pentru controlul a până la 64 de etaje, prin intermediul unui cititor de carduri intern al liftului, și pentru atribuirea de autorizații de etaj către deținătorii de carduri.
- Interfață cu sisteme de management al destinației, capabilă să autorizeze până la 255 de etaje, cu ușă frontală și posterioară într-un sistem lift.
- Interfață pentru importarea datelor de personal dintr-un sistem HR sau exportarea informațiilor respective de la ACE la acest sistem.
- Personalizare îmbunătățită a cardului pentru importarea imaginilor deținătorilor de carduri și crearea de modele personalizate de ecusoane de companie imprimabile la imprimante standard de carduri.
- Funcția de deblocare de la distanță a ușii, de ex. prin clic cu mouse-ul pe o pictogramă dintr-o hartă interactivă de locație BIS.
- Crearea de zone logice, de ex. camere individuale, grupuri de camere, etaje sau parcări, cărora li se pot atribui puncte speciale de control al accesului.
- Gestionarea flexibilă a alarmelor pentru o gamă largă de condiții de alarmă (de exemplu, acces refuzat, detectarea modificărilor neautorizate, ecuson pe lista neagră, alarmă de constrângere etc.) opțional combinabilă cu funcții BIS, cum ar fi hărți interactive de locație și planuri de acțiune.
- Utilizarea dispozitivelor I/O digitale monitorizate din familia de controlere Bosch pentru funcții suplimentare de control și monitorizare, inclusiv detectarea intruziunilor și a modificărilor neautorizate.
- Comunicarea dintre controlerele de acces locale și cititoare este asigurată de OSDP V2 (canal securizat OSDP).
- Comunicația dintre sistemul principal de control al accesului și controlerele de acces locale este securizată prin DTLS (cu criptare AES-256).
- 
- Înregistrare detaliată a evenimentelor de acces și a alarmelor pentru respectarea prevederilor legale și anchete criminalistice.
  - Pistă de audit pentru modificări aduse înregistrărilor principale și autorizațiilor, inclusiv crearea, modificarea și ștergerea înregistrărilor.
  - Raportare integrată, cu funcție de filtrare.
- Permite până la opt formate diferite de carduri simultan.
- Editarea en-gros a autorizațiilor și a altor date.

Verificare video

Verificarea video extinde nivelul de securitate al sistemului de control al accesului prin intermediul tehnologiei video. Când un cititor se află în modul de verificare video, titularul cardului nu este acceptat direct. Cititorul efectuează o solicitare de intrare care apare ca mesaj pe ecranul operatorului.

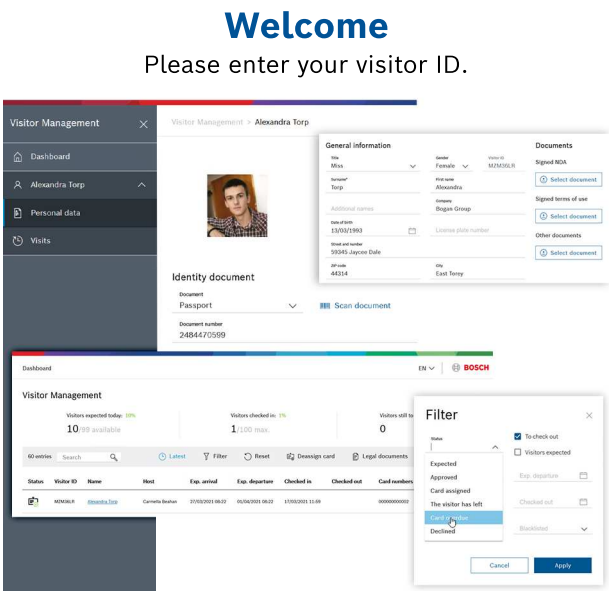
Un plan de acțiune (consultați accesoriile opționale BIS) afișează operatorului imaginea deținătorului cardului stocată în baza de date ACE, împreună cu o imagine live de la o cameră din apropierea intrării/cititorului care a trimis solicitarea. Operatorul compară imaginile și decide dacă deschide sau nu ușa.

Gestionarea parcărilor

Această caracteristică permite definirea și utilizarea modelului de ușă „parcare”, model care conține controlul a două bariere de intrare și ieșire și a semafoarelor acestora, care împiedică accesul atunci când parcarea a atins capacitatea maximă.
Accesul în parcări poate fi reglementat printr-un cititor cu rază lungă și carte de identitate, sau folosind o cameră și plăcuța de înmatriculare.
Fiecare parcare poate fi împărțită în zone logice, cu un număr maxim de vehicule definit pentru fiecare zonă.
Autorizația de a trece de barieră și de a parca într-o zonă logică poate fi atribuită deținătorilor de carduri în casetele de dialog standard. De asemenea, este posibilă echilibrarea ocupării parcărilor, cu ajutorul unor informații despre capacitatea curentă afișate pe ecranul operatorului. Echilibrarea ocupării cu mașini (parcări) și a cu persoane (zone de acces) este gestionată separat, astfel încât să fie posibilă urmărirea simultană a locației deținătorului cardului și a vehiculului acestuia.

Visitor Management

- Preînregistrați programările în sistem, pentru a scurta timpul de procesare.
- Permiteți vizitatorilor să-și creeze propriile profiluri în modul chioșc, pentru a evita cozile la recepție.
- Folosiți un tablou de bord pentru a monitoriza vizitele așteptate în ziua respectivă, numărul vizitatorilor din locație, ce acreditări sunt utilizate și ce acreditări mai trebuie să fie colectate.
- Setați date de expirare pentru profilurile vizitatorilor și atașările acestora pentru a respecta reglementările naționale privind confidențialitatea datelor, cum ar fi Regulamentul european general privind protecția datelor (RGPD).



Integrarea panourilor de intruziune

Permisiunile de operare a panourilor de intruziune Bosch B Series și G Series pot fi atribuite deținătorilor de carduri în mod centralizat, permițându-le acestora să armeze și să dezarmeze zonele cu funcția de control al intruziunii.
Dacă deține autorizația corespunzătoare, un posesor de card poate dezarma o zonă și debloca ușa acestuia cu o singură glisare a cardului la un cititor simplu.

Controlul accesului pentru controlul bolilor

- Noile cititoare contactless de amprentă digitală și cu recunoaștere facială elimină o sursă periculoasă de contaminare. Pentru un plus de securitate, sistemul poate solicita opțional un card contactless sau o altă acreditare biometrică pentru autentificare.
- Controlul secvenței de acces ajută la aplicarea fluxului unidirecțional de public, reducând riscul de infecție prin eliminarea întâlnirilor față în față.
- Managementul ACE la nivel de amenințare oferă modalități de a comuta instantaneu de la o schemă de flux de public la alta, în caz de urgență.
- Zonele ACE de control al accesului sunt ideale pentru implementarea rapidă a restricțiilor de igienă privind numărul de persoane dintr-un spațiu definit.
- Cititoarele contactless elimină nevoia de butoane fizice ale liftului.
- Armarea și dezarmarea contactless a zonelor de intruziune reduce suplimentar sursele de contaminare.

- Utilizarea telefoanelor mobile pentru acces promovează igiena prin reducerea numărului de acreditări fizice partajate - o soluție comună dezvoltată cu partenerii **HID** și **STiD**.
- Sistemele de recunoaștere a plăcuțelor de înmatriculare reduc nevoia unor cabine de control cu personal, tastaturi și butoane, sau necesitatea de a ieși din vehicul cu acreditări fizice.

Accesorii pentru BIS Access Engine

Managementul extins al parcărilor
Asigură managementul parcării oaspeților, inclusiv generarea de vouchere de parcare și notificări despre vizitatorii care depășesc întâlnirile programate.

Interfață de programare a aplicației
Un kit de dezvoltare software (SDK) pentru integrarea Access Engine cu aplicații terțe, cum ar fi Identity Management, Time & Attendance și sisteme avansate de Visitor Management.

Integrarea dulapurilor cu cheie
Integrarea dulapurilor cu cheie **Deister** și **Kemas** pentru securizarea cheilor fizice și monitorizarea utilizării acestora. Disponibilitate numai în anumite țări.

Integrarea încuietorilor online wireless
Integrarea încuietorilor online wireless **SimonsVoss SmartIntego** (cilindri de broască, clanțe și lacăte) pentru uși, care necesită securitate de nivel mediu, cum ar fi birourile și sălile de clasă. Disponibilitate numai în anumite țări.

Integrarea încuietorilor offline de la distanță
Integrarea **încuietorilor offline conforme OSS-SO** sau a încuietorilor offline **Normbau (Pegasys)** pentru uși la distanță, pentru care nu este posibilă conexiunea prin cablu din cauza distanței, a condițiilor de construcție sau a costului. Sistemul de blocare offline constă din software, hardware și accesorii. Componentele hardware sunt disponibile liber pe piața deschisă de la partenerii Bosch. Licența software oferă o serie de dialoguri în BIS și ACE. Disponibilitate numai în anumite țări.

Creșterea capacității de control al accesului
ACE se adaptează cu ușurință la necesitățile extinse ale locațiilor dvs. Licențele suplimentare MAC (Main Access Controller) permit creșterea acoperirii geografice sau a performanțelor. Un număr tot mai mare de angajați sau vizitatori pot fi cazați prin licențe suplimentare pentru titularii de card.
Licențele pentru creșterea numărului de intrări sunt disponibile în trepte de 32, 128 sau 512. O intrare în acest sens este echivalentă cu un model de ușă ACE, ceea ce facilitează calculul cerințelor.
Exemplu: locația dvs. are 2 intrări principale, fiecare cu un cititor de intrare și un cititor de ieșire, 26 de uși de birou cu cititor de intrare și 1 ușă capcană pentru camera serverului. Numărul total de modele de uși/ intrări este 29, indiferent de numărul de cititoare implicate. Un total de 32 de intrări sunt deja acoperite de licența de bază a pachetului ACE.

Note despre instalare/configurare

Access Engine în cifre
Următoarele valori maxime se aplică sistemului de referință descris mai jos.

Număr maxim de carduri active per sistem	400,000
Număr maxim de cititoare per server	10,000
Număr maxim de controlere MAC (controlere principale de acces) per server	40
Număr maxim de autorizații de acces per MAC	1,000
Număr maxim de AMC per MAC	125 Pentru sisteme de înaltă performanță: 60
Număr maxim de autorizații de acces per ACE	40,000
Număr maxim de divizii per ACE	400
Număr maxim de ronduri de pază per ACE	200
Număr maxim de ronduri de pază simultane	8
Număr maxim de panouri de intruziune B/G pentru sincronizarea titularului de card cu ACE	500

Sisteme de referință pentru server și client

	Sistem server (fără client care rulează)	Sistem client
CPU	Intel Xeon E-2144G la 3,6 GHz (4 nuclee, 8 unități logice)	Intel Core i7-8700 la 3,2 GHz (6 nuclee, 12 unități logice)
RAM	32 GB (2667 MHz)	8 GB (2667 MHz)
GPU	Grafică integrată de la CPU	Intel UHD Graphics 630 (memorie GPU de 4 GB)
Disc de sistem	NVMe Viteză de scriere: 1440 MB/s Viteză de citire: 2250 MB/s Timp mediu de răspuns 10 ms	Disc SSD
Disc pe care se instalează AMS	SSD Viteză de scriere: 1000 MB/s Viteză de citire: 1100 MB/s Timp mediu de răspuns 10 ms	

	Sistem server (fără client care rulează)	Sistem client
Sistem de operare	Microsoft Server 2019 Standard Edition	Microsoft 10 Pro Edition

Versiuni de browser pentru programe de completare bazate pe web

Browser web	Versiune
Google Chrome	112 sau mai recent
Microsoft Edge	111 sau mai recent
Mozilla Firefox	102 sau mai recent

Specificații tehnice

Consultați specificațiile pentru versiunea respectivă a pachetului de bază BIS.

Informații pentru comandă

Licență BIS-FACE-API50 pentru API
Licență BIS Access Engine pentru API
Număr comandă **BIS-FACE-API50 | F.01U.415.274**

Licență de bază BIS-FACE-BPA50
Licență de bază pentru BIS Access Engine
Număr comandă **BIS-FACE-BPA50 | F.01U.415.273**

Licență BIS-FACE-OFFL50 pentru pachet de bază offline
Licență pentru pachet de bază offline (ACE)
Număr comandă **BIS-FACE-OFFL50 | F.01U.415.275**

BIS-FACE-PRK50 Licență pentru managementul parcărilor auto
Licență pentru managementul parcărilor auto (ACE)
Număr comandă **BIS-FACE-PRK50 | F.01U.415.277**

BIS-FACE-VISWEB50 Licență pentru managementul vizitatorilor
Licență pentru managementul vizitatorilor (ACE)
Număr comandă **BIS-FACE-VISWEB50 | F.01U.415.276**

BIS-XACE-100C50 Licență pentru 100 de carduri de identitate
=Licență pentru 100 de carduri de identitate (ACE)
Număr comandă **BIS-XACE-100C50 | F.01U.415.290**

BIS-XACE-10KC50 Licență pentru 10.000 de carduri de identitate
=Licență pentru 10.000 de carduri de identitate (ACE)
Număr comandă **BIS-XACE-10KC50 | F.01U.415.292**

BIS-XACE-10MC50 Licență pentru 10 MAC
Licență pentru 10 MAC (ACE)
Număr comandă **BIS-XACE-10MC50 | F.01U.415.285**

BIS-XACE-128D50 Licență pentru 128 de uși
Licență pentru 128 de uși (ACE)
Număr comandă **BIS-XACE-128D50 | F.01U.415.288**

BIS-XACE-1KC50 Licență pentru 1.000 de carduri de identitate
Licență pentru 1.000 de carduri de identitate
Număr comandă **BIS-XACE-1KC50 | F.01U.415.291**

BIS-XACE-1KEY50 Licență pentru 1 dulap cu cheie
Licență pentru 1 dulap cu cheie
Număr comandă **BIS-XACE-1KEY50 | F.01U.415.295**

BIS-XACE-1MAC50 Licență pentru 1 MAC
Licență pentru 1 MAC
Număr comandă **BIS-XACE-1MAC50 | F.01U.415.284**

BIS-XACE-25OF50 Licență pentru 25 de uși offline
Licență pentru 25 de uși offline
Număr comandă **BIS-XACE-25OF50 | F.01U.415.286**

BIS-XACE-25ON50 Licență pentru 25 de uși online wireless
Licență pentru 25 de uși online wireless
Număr comandă **BIS-XACE-25ON50 | F.01U.415.294**

BIS-XACE-32DR50 Licență pentru 32 de uși
Licență pentru 32 de uși
Număr comandă **BIS-XACE-32DR50 | F.01U.415.287**

BIS-XACE-50KC50 Licență pentru 50.000 de carduri de identitate
Licență pentru 50.000 de carduri de identitate
Număr comandă **BIS-XACE-50KC50 | F.01U.415.293**

BIS-XACE-512D50 Licență pentru 512 de uși
Licență pentru 512 de uși
Număr comandă **BIS-XACE-512D50 | F.01U.415.289**

BIS-XACE-25OS50 Licență pentru 25 de uși offline OSS-SO
Licență pentru 25 de uși offline OSS-SO
Număr comandă **BIS-XACE-25OS50 | F.01U.415.309**

Reprezentat de:

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