

## BIS - Access Engine (ACE) 5.0



O controle de acesso é hoje uma das tecnologias mais importantes no aumento da segurança de pessoas, bens e ativos. O BIS Access Engine e os sofisticados produtos controladores fornecem uma ampla variedade de recursos de controle de acesso. Combine o pacote básico do Access Engine com os recursos opcionais a fim de desenvolver um sistema de controle de acesso personalizado capaz de atender às suas necessidades específicas. Utilize, então, o software Building Integration System (BIS) para integrar o Access Engine aos equipamentos de segurança de vídeo e detecção de intrusão.

### Visão geral do sistema

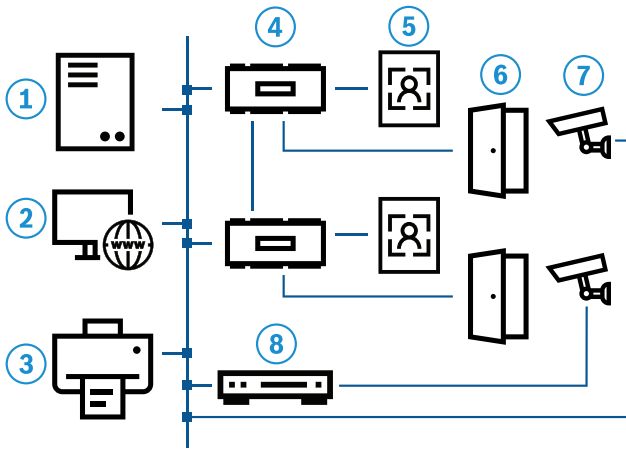
O software do Access Engine (ACE), juntamente com o hardware de acesso da Bosch, é um sistema de controle de acesso completo no Building Integration System (BIS). Ele inclui todos os recursos essenciais encontrados em qualquer sistema de controle de acesso autônomo, além de uma ampla variedade de recursos opcionais.

Como os outros engines do BIS, o ACE se beneficia integralmente de todos os recursos adicionais do BIS, como mapas de localização interativos e planos de ação, proporcionando o gerenciamento de alarmes totalmente eficaz e integrado. As mensagens de alarme e os eventos de controle de acesso podem ser exibidos com informações de localização gráfica e instruções de fluxo de trabalho.

- ▶ Sistema de controle de acesso distribuído com gerenciamento de alarmes gráficos
- ▶ Integração e interação perfeitas com sistemas de vídeo, incêndio, intrusão e PA/VA por meio da plataforma comum do BIS
- ▶ Resiliência elevada graças a uma arquitetura de sistema com 4 camadas e implantação de redundância de componentes críticos
- ▶ Integração de produtos de terceiros via protocolos abertos e seguros e um SDK
- ▶ Processo de inscrição eficiente que torna a integração mais rápida e segura

O ACE utiliza as interfaces de usuário padrão do BIS e sua flexibilidade de personalização. Além disso, o ACE oferece interfaces de configuração de acesso específicos para usuários com cartão, hardware de acesso e regras de acesso.

A principal vantagem da família Building Integration System é a integração de uma ampla gama de sistemas de segurança e proteção na mesma instalação. Por meio da combinação do ACE com outros motores do BIS (por exemplo, Automation e Vídeo), é possível desenvolver soluções de segurança inteligentes e personalizadas para satisfazer com exatidão os requisitos específicos de um projeto. O Access Engine pode ser executado em uma estação de trabalho individual, em um sistema cliente-servidor ou em um ambiente distribuído com um servidor central e servidores locais ou regionais. No ambiente de multisservidor distribuído, todos os dispositivos, titulares de cartão e autorizações podem ser gerenciados a partir do servidor de nível superior. Para garantir os níveis mais altos de segurança e integridade dos dados, o BIS ACE pode gerenciar controladores RS485 de alta segurança com protocolo OSDP v2 para comunicação criptografada autenticada e supervisão de leitores.



### Pos. Descrição (sistema monosservidor)

Pos.	Descrição (sistema monosservidor)
1	Servidor BIS central com software do Access Engine e Video Engine
2	Diversas estações de trabalho para gerenciamento de alarme e inclusão
3	Dispositivos de inclusão, como impressora de cartão, leitor de assinaturas, leitor de inclusão e câmera para fotos de identificação
4	Controladores de acesso
5	Leitores de acesso
6	Fechaduras de porta
7	Câmera IP
8	Gravador de vídeo digital, como, por exemplo, DIVAR, para registro de alarmes

- Modelos de tempo para ativação/desativação automática de contas de usuários de cartão, códigos PIN etc.
- Modelos de tempo para a ativação/desativação automática de configurações do sistema, como por exemplo configurar uma porta do escritório para ficar destrancada das 9:00 às 17:00
- Código PIN adicional para armar/desarmar alarmes de intrusão.
- Bloqueio/desbloqueio temporário de usuários de cartão, de forma manual ou controlado por tempo.
- Inclusão de cartões na lista negra.
- Antidupla entrada.
- O balanceamento das áreas de acesso, incluindo as verificações das sequências de acessos, oferece uma forma de limitar o número de pessoas em determinada área, automaticamente armando/desarmando alarmes caso a área esteja vazia/não vazia, e gerando listas de agrupamentos.
- As autorizações para números definidos de pessoas concederão acesso em determinada porta apenas quando o número definido (N) de usuários de cartão autorizados apresentar o crachá em um leitor configurado de maneira correspondente. A configuração pode ser feita individualmente em cada leitor, de 2 a N pessoas (sem limite).
- Recurso de barreira de segurança ("mantrap") para gerenciamento de duas portas conjugadas com dois pares de leitores; recomendado para altos níveis de segurança, como, por exemplo, entrada em centros de informática ou departamentos de pesquisa.
- Ronda: sistema de rastreamento de patrulha de última geração que utiliza os leitores de controle de acesso existentes, sequência de acesso e verificação de horário de acesso. Qualquer violação da sequência de patrulhamento ou da programação de tempo gera um alarme e este é rastreado por

### Funções

O pacote básico do Access Engine, juntamente com os controladores de acesso AMC, oferecem os seguintes recursos:

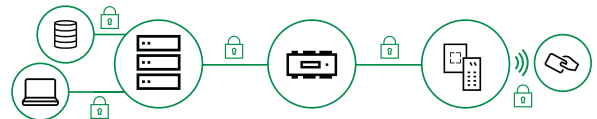
- Uma ampla gama de modelos de portas intuitivos que permitem uma configuração rápida e fácil de hardware (por exemplo, porta padrão, catraca, elevador com leitores de hora e presença etc.).
- É aberta uma caixa de diálogo para a configuração do modelo da porta, gerando um esquema de conexão de cabos para o instalador de hardware.
- Processo de integração contínuo incluindo cadastramento biométrico e de cartão.
- Diálogos personalizáveis para coletar apenas as informações pessoais necessárias.
- Modelos de horário para controle de acesso baseado em tempo, incluindo definição de dias especiais, feriados públicos recorrentes etc.

sofisticados recursos de gerenciamento de alarme no BIS. Relatórios de ronda de segurança podem ser gerados no registro de eventos do BIS.



- Recurso de revista aleatória: os usuários de cartão que entram ou saem das instalações podem ser barrados aleatoriamente e direcionados ao pessoal de segurança para uma inspeção mais detalhada. Cartões pertencentes a "VIPs" designados podem ser excluídos da revista aleatória.
- Visitor Management: os cartões de visitantes podem ser rastreados e gerenciados separadamente quanto aos períodos de validade e à possível necessidade de um acompanhante.
- Interface para arme/desarme do IDS (Sistema de detecção de intrusão), incluindo gerenciamento de autorizações e atribuição de cartões.
- Importação e exportação online de dados de titulares do cartão armazenados em sistemas de terceiros ou em um servidor de diretório, como Microsoft Active Directory ou Apache Directory.
- Todas as informações pessoais, inclusive fotos e assinaturas, são armazenadas em um banco de dados SQL protegido.
- Gestão de nível de ameaça, para pré-configurar até 15 cenários, inclusive situações de bloqueio e evacuação.
- Interface de elevador para controle de até 64 andares via leitor de cartão no elevador e para atribuição de autorizações por andar aos usuários de cartão.
- Interface para sistemas de gerenciamento de destino capaz de autorizar até 255 andares com porta dianteira e traseira em um sistema de elevadores.
- Interface para importação de dados pessoais de um sistema de RH ou exportação desse tipo de informação do ACE para esse sistema.

- Personalização de cartões aprimorada para importação de imagens do usuário do cartão e criação personalizada de layouts de crachás corporativos, que podem ser impressos em impressoras de cartão padrão.
- Recurso de desbloqueio remoto de portas, como, por exemplo, clicar com o mouse em um ícone de um mapa de localização interativo do BIS.
- Criação de áreas lógicas, como, por exemplo, salas individuais, grupos de salas, andares inteiros ou estacionamentos, para as quais podem ser atribuídos pontos de controle de acesso especiais.
- Gerenciamento flexível de alarmes para uma vasta gama de condições de alarme (como, por exemplo, acesso negado, detecção de violação, crachás na lista negra, alarme de coação etc.) que podem ser combinadas opcionalmente com recursos do BIS, como mapas de localização interativos e planos de ação.
- Utilização das E/S (entradas/saídas) digitais e monitoradas da família de controladores da Bosch para funções adicionais de monitoramento e controle, incluindo detecção de intrusão e violação.
- A comunicação entre os controladores de acesso locais e os leitores é protegida por OSDP V2 (OSDP Secure Channel).
- A comunicação entre o sistema principal de controle de acesso e os controladores de acesso locais é protegida por DTLS (com criptografia AES-256).



- Registro detalhado de eventos de acesso e alarmes para conformidade legal e investigação forense.
  - Trilha de auditoria para mudanças nas autorizações e registros mestres, incluindo criação, modificação e exclusão de registros.
  - Relatórios integrados com recurso de filtragem.
- Suporte para até oito diferentes formatos de cartão simultaneamente.
- Edição em massa de autorizações e outros dados.

#### Verificação por vídeo

A verificação por vídeo estende o nível de segurança do sistema de controle de acesso por meio de tecnologia de vídeo. Quando um leitor está no modo de verificação por vídeo, o usuário de cartão não tem ingresso direto. Em vez disso, o leitor faz uma solicitação de entrada a qual é exibida como mensagem na tela do operador.

Um Plano de Ação (consulte também os acessórios opcionais do BIS) exibe para o operador as imagens do usuário do cartão, conforme armazenadas no banco de dados do ACE, juntamente com uma imagem ao vivo gerada pela câmera próxima da entrada/leitor

que enviou a solicitação de acesso. O operador compara ambas as imagens e decide abrir ou não a porta.

### Gerenciamento de estacionamento



Este recurso permite definir e utilizar o modelo de porta para “estacionamento”. Este modelo contém o controle de duas barreiras (para entrada e saída) e seus semáforos, as quais impedem o acesso quando o estacionamento atinge a capacidade máxima. O acesso a estacionamentos pode ser regulamentado por um leitor de longa distância e cartão de ID, ou por câmera e placas veiculares.

Cada estacionamento pode ser dividido em áreas lógicas, com um número máximo de carros definido para cada uma delas. A autorização para transpor a barreira e estacionar em uma área lógica pode ser atribuída a usuários com cartões nas caixas de diálogo padrão. O gerenciamento de utilização dos estacionamentos é igualmente possível, com as informações sobre a capacidade atual exibida na tela do operador. A utilização de vagas de carros (estacionamento) e acesso de pessoas (áreas de acesso) é gerenciado separadamente; dessa forma, é possível rastrear a localização do usuário do cartão e do carro ao mesmo tempo.

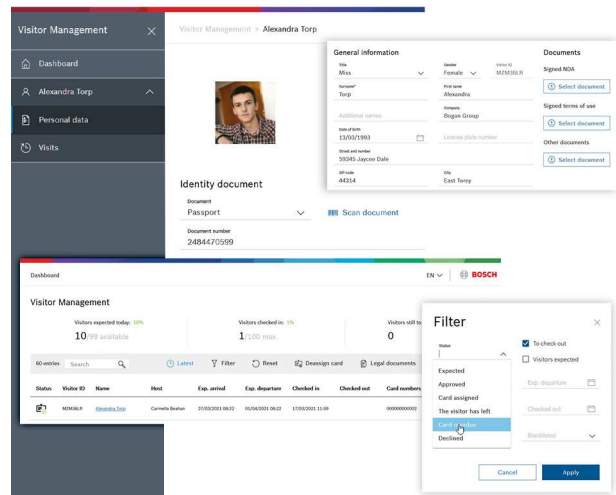
### Gerenciamento de visitantes

- Pré-registre compromissos no sistema para reduzir o tempo de processamento.
- Permita que os visitantes criem seus próprios perfis no modo de quiosque para evitar filas na recepção.
- Use um painel para monitorar as visitas esperadas do dia, quantos visitantes estão no local, quais credenciais estão em uso e quais credenciais ainda precisam ser coletadas.

- Defina datas de vencimento para os perfis de visitantes e os respectivos anexos a fim de cumprir os regulamentos nacionais de privacidade de dados, como o RGPD da Europa.

## Welcome

Please enter your visitor ID.



### Integração dos painéis de intrusão

As permissões para operar painéis de intrusão B Series e G Series da Bosch podem ser atribuídas centralmente aos portadores de cartões, permitindo que eles armem e desarmem áreas onde existe controle de intrusão.

Com a devida autorização, o portador do cartão pode desarmar uma área e destravar a porta com uma única passada de cartão em um leitor simples.

### Controle de acesso para controle de doenças

- Novos leitores de digital e reconhecimento facial sem contato eliminam uma perigosa fonte de contaminação. Para uma segurança ainda maior, o sistema pode opcionalmente exigir um cartão sem contato ou outra credencial biométrica para autenticação.
- O controle da sequência de acesso ajuda no fluxo unidirecional da multidão – reduzindo o risco de infecção ao eliminar encontros frontais.
- O gerenciamento do nível de ameaça do ACE apresenta maneiras de alternar instantaneamente de um esquema de fluxo de multidão para outro, em caso de emergências.
- As áreas de controle de acesso do ACE são ideais para implementar sem demora restrições higiênicas quanto ao número de pessoas em um espaço definido.
- Leitores sem contato eliminam a necessidade de botões físicos do elevador.
- O arme e desarme sem contato das áreas de intrusão reduz ainda mais as fontes de contaminação.

- O uso de celulares para acesso proporciona higiene, pois reduz o número de credenciais físicas compartilhadas – uma solução de cooperação desenvolvida com as parceiras **HID** e **STiD**.
- Os sistemas de reconhecimento de placas veiculares reduz a necessidade de cabines de controle com guardas, teclados e botões; ou a necessidade de sair do veículo com credenciais físicas.

### Acessórios para o Access Engine do BIS

#### Gerenciamento de estacionamento estendido

Fornece gerenciamento de estacionamento de convidados, incluindo a geração de cartões de estacionamento e notificação sobre os visitantes que permanecem após seus compromissos agendados.

#### Interface de programação de aplicativos

Um kit de desenvolvimento de software (SDK) para integrar o Access Engine com aplicativos de terceiros, como sistemas avançados de Gerenciamento de Identidades, Hora & Presença e gestão de visitantes.

#### Integração de armários de chaves

Integração de armários de chaves **Deister** e **Kemas** para armazenamento de chaves físicas e monitoração do seu uso. Disponível apenas em alguns países.

#### Integração de bloqueios online sem fio

Integração de bloqueios online sem fio **SimonsVoss SmartIntego** (cilindros de fechadura, maçanetas e fechaduras) para portas que exigem nível de segurança médio, como escritórios e salas de aula. Disponível apenas em alguns países.

#### Integração de bloqueios offline remotos

Integração dos **bloqueios offline OSS-SO** ou **Normbau (Pegasys)** para portas remotas, cuja conexão por meio de cabeamento não é possível devido a distância, condições de construção ou custo. O sistema de bloqueio off-line consiste em software, hardware e acessórios. O hardware está disponível gratuitamente no mercado em geral a partir de parceiros da Bosch. A licença de software permite uma série de diálogos no BIS e ACE (Access Engine, Mecanismo de Acesso). Disponível apenas em alguns países.

#### Aumento da capacidade de controle de acesso

O ACE é facilmente escalonado para atender às necessidades crescentes de seus lugares. Licenças adicionais MAC (Main Access Controller, Controlador de Acesso Principal) permitem aumentar a cobertura geográfica ou o desempenho. Um número crescente de funcionários e visitantes podem ser acomodados por licenças do titular do cartão adicional. Licenças para aumentar o número de entradas estão disponíveis em incrementos de 32, 128 ou 512. Nessa concepção, uma entrada equivale a um modelo de porta do ACE; isso facilita o cálculo das necessidades.

Exemplo: a instalação possui duas entradas principais com um leitor de entrada e um de saída em cada uma delas, 26 portas de escritório com leitor de entrada e uma área de inspeção (eclusa) para a sala de servidores. O número total de entradas/modelos de porta é 29, independentemente do número de leitores envolvidos. A licença do pacote básico do ACE já oferece cobertura para um total de 32 entradas.

### Notas de instalação/configuração

#### Access Engine em números

A seguinte máxima aplica-se ao sistema de referência descrito abaixo.

Número máx. de cartões ativos por sistema	400,000
Número máximo de leitores por servidor	10,000
Número máx. de MACs (Master Access Controllers) por servidor	40
Número máx. de autorizações de acesso por MAC	1,000
Número máx. de AMCs por MAC	125
	Para sistemas de alto desempenho: 60
Número máx. de autorizações de acesso por ACE	40,000
Número máximo de divisões por ACE	400
Número máximo de rondas de segurança por ACE	200
Número máximo de rondas de segurança simultâneas	8
Número máx. de painéis de intrusão B/G para sincronização do titular do cartão com ACE	500

#### Sistemas de referência para servidor e cliente

	Sistema de servidor (sem nenhum cliente em execução)	Sistema cliente
CPU	Intel Xeon E-2144G a 3,6 GHz (4 núcleos, 8 lógicos)	Intel Core i7-8700 a 3,2 GHz (6 núcleos, 12 lógicos)
RAM	32 GB (2667 MHz)	8 GB (2667 MHz)
GPU	Placa gráfica integrada da CPU	Intel UHD Graphics 630 (memória da GPU de 4 GB)
Disco do sistema	NVMe	Disco SSD

	Sistema de servidor (sem nenhum cliente em execução)	Sistema cliente
	Velocidade de gravação: 1440MB/s Velocidade de leitura: 2250MB/s Tempo médio de resposta 10ms	
Disco onde o AMS está instalado	SSD Velocidade de gravação: 1000MB/s Velocidade de leitura: 1100MB/s Tempo médio de resposta 10ms	
Sistema operacional	Microsoft Server 2019 Standard Edition	Microsoft 10 Pro Edition

**Versões do navegador para programas complementares baseados na Web**

Navegador da Web	Versão
Google Chrome	112 ou superior
Microsoft Edge	111 ou superior
Mozilla Firefox	102 ou superior

**Especificações técnicas**

Consulte as especificações da versão respectiva do Pacote básico do BIS.

**Informações sobre pedidos**

**Licença do BIS-FACE-API50 para API (Application Programming Interface, Interface de Programação de Aplicativos)**

Licença do BIS Access Engine para API  
Número do pedido **BIS-FACE-API50 | F.01U.415.274**

**Licença Básica do BIS-FACE-BPA50**

Licença básica para o BIS Access Engine  
Número do pedido **BIS-FACE-BPA50 | F.01U.415.273**

**Licença do BIS-FACE-OFFL50 para pacote básico off-line**

Licença para pacote básico off-line (ACE)  
Número do pedido **BIS-FACE-OFFL50 | F.01U.415.275**

**Representado por:**

**North America:**  
Bosch Security Systems, LLC  
130 Perinton Parkway  
Fairport, New York, 14450, USA  
Phone: +1 800 289 0096  
Fax: +1 585 223 9180  
onlinehelp@us.bosch.com  
www.boschsecurity.com

**Latin America and Caribbean:**  
Robert Bosch Ltda  
Security Systems Division  
Via Anhanguera, Km 98  
CEP 13065-900  
Campinas, Sao Paulo, Brazil  
Phone: +55 19 2103 2860  
Fax: +55 19 2103 2862  
LatAm.boschsecurity@bosch.com  
www.boschsecurity.com

**Licença do BIS-FACE-PRK50 para gerenciar estacionamento**

Licença para gerenciar estacionamento (ACE)  
Número do pedido **BIS-FACE-PRK50 | F.01U.415.277**

**Licença do BIS-FACE-VISWEB50 para Visitor Management**

Licença para Visitor Management (ACE)  
Número do pedido **BIS-FACE-VISWEB50 | F.01U.415.276**

**Licença do BIS-XACE-100C50 para 100 cartões de ID**

Licença para 100 cartões de ID (ACE)  
Número do pedido **BIS-XACE-100C50 | F.01U.415.290**

**Licença do BIS-XACE-10KC50 para 10.000 cartões de ID**

Licença para 10.000 cartões de ID (ACE)  
Número do pedido **BIS-XACE-10KC50 | F.01U.415.292**

**Licença do BIS-XACE-10MC50 para 10 MAC**

Licença para 10 MAC (ACE)  
Número do pedido **BIS-XACE-10MC50 | F.01U.415.285**

**Licença do BIS-XACE-128D50 para 128 portas**

Licença para 128 portas (ACE)  
Número do pedido **BIS-XACE-128D50 | F.01U.415.288**

**Licença do BIS-XACE-1KC50 para 1.000 cartões de ID**

Licença para 1.000 cartões de ID  
Número do pedido **BIS-XACE-1KC50 | F.01U.415.291**

**Licença do BIS-XACE-1KEY50 para 1 gabinete com chave**

Licença para 1 gabinete com chave  
Número do pedido **BIS-XACE-1KEY50 | F.01U.415.295**

**Licença do BIS-XACE-1MAC50 para 1 MAC**

Licença para 1 MAC  
Número do pedido **BIS-XACE-1MAC50 | F.01U.415.284**

**Licença do BIS-XACE-25OF50 para 25 portas off-line**

Licença para 25 portas offline  
Número do pedido **BIS-XACE-25OF50 | F.01U.415.286**

**Licença do BIS-XACE-25ON50 para 25 portas online sem fio**

Licença para 25 portas on-line sem fio  
Número do pedido **BIS-XACE-25ON50 | F.01U.415.294**

**Licença do BIS-XACE-32DR50 para 32 portas**

Licença para 32 portas  
Número do pedido **BIS-XACE-32DR50 | F.01U.415.287**

**Licença do BIS-XACE-50KC50 para 50.000 cartões de ID**

Licença para 50.000 cartões de ID  
Número do pedido **BIS-XACE-50KC50 | F.01U.415.293**

**Licença do BIS-XACE-512D50 para 512 portas**

Licença para 512 portas  
Número do pedido **BIS-XACE-512D50 | F.01U.415.289**

**Licença do BIS-XACE-25OS50 para 25 portas OSS-SO off-line**

Licença para 25 portas OSS-SO offline  
Número do pedido **BIS-XACE-25OS50 | F.01U.415.309**