

BIS - Access Engine (ACE) 4.5

www.boschsecurity.com.br



BOSCH

Tecnologia para a vida



- ▶ 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 redundância de componentes críticos
- ▶ Integração de produtos de terceiros via protocolos abertos e SDK
- ▶ Processo de inscrição eficiente que torna a integração mais rápida e segura

O controle de acesso é hoje uma das tecnologias mais importantes no aumento da segurança de pessoas, bens e ativos. O Access Engine e a série de sofisticados controladores do BIS oferecem uma grande 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. Utilize, então, o software Building Integration System (BIS) para integrar o Access Engine aos equipamentos de segurança de vídeo e 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.

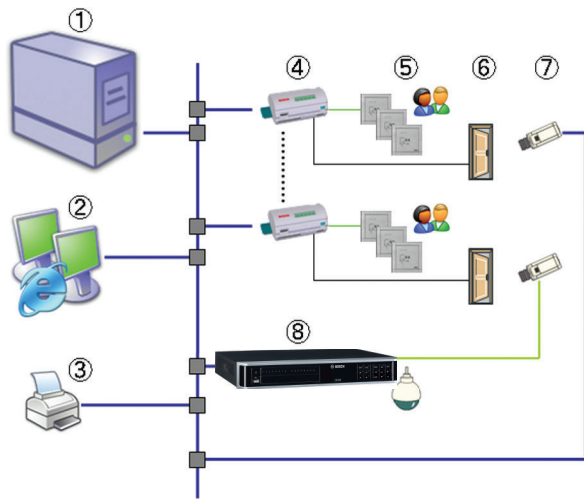
Como os outros engines do BIS, o ACE se beneficia integralmente de todos os recursos adicionais do BIS, como mapas de localização interativos e planos de

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.

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.



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

Funções

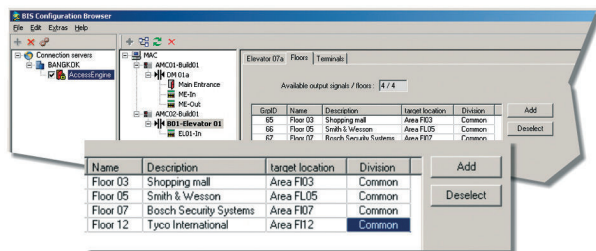
O pacote básico do Access Engine, juntamente com os controladores de acesso AMC, oferecem os seguintes recursos:

- Ampla gama de modelos intuitivos de portas que permitem uma configuração rápida e fácil do 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.
- Ativação imediata das configurações de leitores e usuários de cartão nos controladores de acesso.
- Modelos de horário para controle de acesso baseado em tempo, incluindo definição de dias especiais, feriados públicos recorrentes, etc.

- Modelos de tempo para ativação/desativação automática de contas de usuários de cartão, como regras de acesso, 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 09:00 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.
- Campos de entrada definíveis pelo usuário para informações complementares do usuário do cartão.
- Anti dupla entrada.
- O balanço de acesso em área, incluindo as verificações das sequências de acesso, oferece uma forma de limitar o número de pessoas em determinada área, arme/desarme automático caso a área esteja vazia/não vazia, além da geração de listas de agrupamento (mustering).
- 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.
- **Novo:** Ronda de guarda aprimorada: 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 sofisticados recursos de gerenciamento de alarme no BIS. Relatórios de ronda podem ser gerados no histórico de eventos do BIS.



- Recurso de revista aleatória: os usuários de cartão que entram ou saem das instalações podem ser barrados em intervalos aleatórios e direcionados ao pessoal de segurança para uma inspeção mais detalhada. Cartões pertencentes a "VIPs" designados podem ser excluídos da revista aleatória.
- Gerenciamento de visitantes: 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.



- 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 importação de dados pessoais de um sistema de RH ou exportação desse tipo de informação do ACE para esse sistema.
- **Novo:** 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 roteamento para garantir que os funcionários sigam as rotas estabelecidas nas instalações.
- 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.
- Capacidade de limitar o número de pessoas ou automóveis de acessar a determinada área lógica.
- Capacidade de arquivamento e restauração completa dos dados do sistema.
- Arquitetura cliente/servidor robusta baseada no servidor Web do BIS.
- Capacidade de personalizar os direitos de administrador do software, se necessário, utilizando caixas de diálogo.
- 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.
- Fácil integração com sistemas de vídeo da Bosch ou de terceiros, como centrais matriciais, DVRs, câmeras IP etc.
- Registro detalhado de eventos de acesso e alarmes para conformidade legal e investigação forense.
 - Histórico de auditoria para mudanças nas autorizações e registros mestres, incluindo criação, modificação e exclusão de registros.
 - Relatórios integrados com recurso de filtragem.
 - Exportação para formato CSV padrão para processamento adicional.
- Suporte para quatro formatos de cartão Wiegand diferentes ao mesmo tempo.
- Ajuda online abrangente.
- Alteração de dados em massa para 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.

BIS-XACE-512D45 Licença para 512 portas

Licença para 512 portas adicionais do BIS ACE

Número do pedido **BIS-XACE-512D45**

BIS-FACE-OFFL45 Licença para pacote básico offline

Licença para o pacote básico de portas offline do BIS ACE

Número do pedido **BIS-FACE-OFFL45**

BIS-XACE-25OF45 Licença para 25 portas offline

Licença para 25 portas offline adicionais do BIS ACE

Número do pedido **BIS-XACE-25OF45**

BIS-XACE-1MAC45 Licença para 1 MAC

Licença para 1 Controlador de Acesso Principal (MAC, Main Access Controller) adicional no BIS ACE

Número do pedido **BIS-XACE-1MAC45**

BIS-XACE-10MC45 Licença para 10 MAC

Licença para 10 Controladores de Acesso Principal (MACs, Main Access Controllers) adicionais no BIS ACE

Número do pedido **BIS-XACE-10MC45**

BIS-FACE-API45 Licença para API

Licença para a Interface de programação de aplicativos (API) no BIS ACE

Número do pedido **BIS-FACE-API45**

BIS-FACE-PRK45 Licença para gerenciar estacionamento

Licença para o gerenciamento de estacionamento de carros estendido no BIS ACE

Número do pedido **BIS-FACE-PRK45**

BIS-XACE-1KEY45 Licença para 1 gabinete chave

Licença para a conexão de 1 armário de chaves ao BIS ACE

Número do pedido **BIS-XACE-1KEY45**

Representado por:

North America:

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

Latin America and Caribbean:

Robert Bosch Ltda
Security Systems Division
Via Anhanguera, Km 98
CEP 13065-900
Campinas, São Paulo, Brazil
Phone: +55 19 2103 2860
Fax: +55 19 2103 2862
LatAm.boschsecurity@bosch.com
la.boschsecurity.com