

BIS: Access Engine (ACE) 5.0



El control de accesos se ha convertido en la actualidad en una de las principales tecnologías para aumentar la seguridad de las personas, las propiedades y los bienes. Access Engine de BIS y los sofisticados productos controladores proporcionan una gama completa de funciones de control de accesos.

Combine el paquete básico de Access Engine con funciones opcionales para crear un sistema de control de accesos personalizado que cumpla con sus necesidades concretas. A continuación, utilice el software del Sistema de Integración para integrar Access Engine con su equipo de detección de intrusión y seguridad por vídeo.

Descripción del sistema

El software de Access Engine (ACE), junto con el hardware de acceso de Bosch, es un completo sistema de control de accesos del Sistema de Integración (BIS). Contiene todas las funciones fundamentales de cualquier sistema de control de accesos independiente, a las que añade una completa gama de mejoras opcionales.

Al igual que el resto de los engines de BIS, ACE aprovecha al máximo todas las funciones adicionales de BIS, como los mapas de ubicaciones interactivos y los planes de acción, para proporcionar una administración de alarmas de gran potencia y totalmente integrada. Los mensajes de alarmas y los

- ▶ Sistema de control de accesos distribuido con gestión gráfica de alarmas
- ▶ Integración e interacción perfectas con sistemas de vídeo, incendios, intrusión y PA/VA mediante la plataforma BIS común
- ▶ Gran resistencia gracias a la arquitectura del sistema en 4 capas y la implantación redundante de los componentes críticos
- ▶ Integración de productos de terceros mediante protocolos abiertos y seguros y SDK
- ▶ Proceso de registro eficaz que facilita una inscripción más rápida y segura

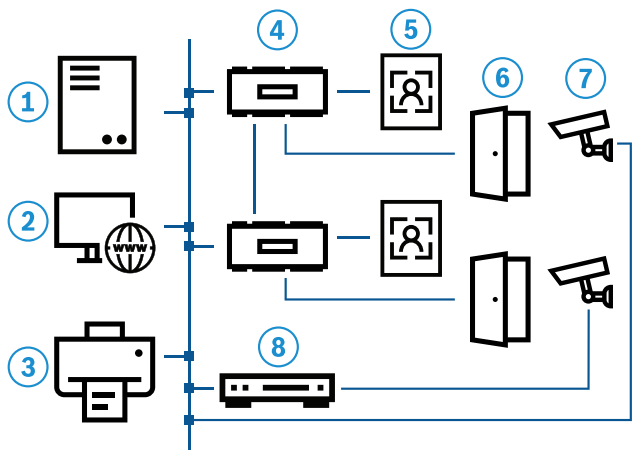
eventos de control de alarmas se pueden visualizar con información gráfica sobre las ubicaciones e instrucciones sobre el flujo de trabajo.

ACE emplea las interfaces de usuario de BIS estándar y su flexibilidad para la personalización. Además, provee interfaces de configuración de accesos específicas para usuarios de tarjetas, hardware de acceso y reglas de acceso.

La principal ventaja de la gama de BIS es la integración de una gran variedad de sistemas de seguridad y protección dentro de unas mismas instalaciones. Mediante la combinación del ACE con otros motores de BIS (por ejemplo, los de automatización y vídeo), es posible diseñar soluciones de seguridad inteligentes a la medida exacta de sus necesidades.

Access Engine funciona en una sola estación de trabajo en un sistema cliente-servidor, o en un sistema distribuido con un servidor central y otros locales o regionales.

En el entorno distribuido con varios servidores, todos los dispositivos, los titulares y las autorizaciones se pueden gestionar desde el nivel del máximo nivel. Para garantizar la máxima seguridad e integridad de los datos, BIS ACE puede administrar controladores RS485 de alta seguridad con el protocolo OSDP v2 para la comunicación cifrada autenticada y la supervisión de lectores.



Posicion Descripción (sistema de un solo servidor)

1	Servidor de BIS central con software de Access Engine y Video Engine
2	Varias estaciones de trabajo para gestión de alarmas o inscripción
3	Dispositivos de inscripción como impresora de tarjetas, escáner de firmas, lector de inscripciones, cámara para fotos para Id.
4	Controladores de accesos
5	Lectores de acceso
6	Pasadores de puerta
7	Cámara IP
8	Grabador de video digital, p. ej., DIVAR para la grabación de alarmas

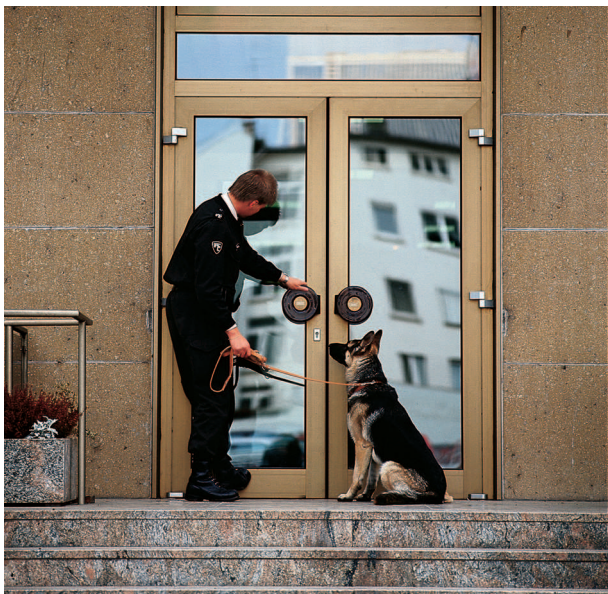
Funciones

El paquete básico de Access Engine, junto con los controladores de acceso de AMC, ofrece las siguientes características:

- Una amplia gama de modelos de puertas mediante plantillas que permite configurar el hardware de forma rápida y fácil (por ejemplo, puerta estándar, giratoria, ascensor con tiempo, relojes de fichar, etc.).
- El cuadro de diálogo de configuración de modelos de puertas genera un diseño de cableado para la instalación del hardware.
- Proceso de incorporación totalmente integrado, incluida la inscripción biométrica y de tarjetas.
- Cuadros de diálogo personalizables para recopilar solo la información personal necesaria.
- Modelos de tiempo para control de accesos basado en el tiempo, que incluyen la definición de días especiales, festivos recurrentes, etc.

- Modelos de tiempo para la activación/desactivación de cuentas de titulares de tarjeta, códigos PIN, etc.
- Modelos de hora para la activación/desactivación automática de la configuración del sistema, como el configurar una puerta de unas oficinas para que se mantenga desbloqueada de 9:00 a 17:00.
- Código PIN adicional para armar/desarmar alarmas de intrusos.
- Bloqueo o desbloqueo temporal de soportes para tarjetas, ya sea de forma manual o mediante control de tiempo.
- Inclusión de tarjetas en la lista negra.
- Función antirretorno.
- El equilibrio de áreas de acceso, incluida la comprobación de la secuencia de accesos, proporciona una forma de limitar el número de personas que hay en un área determinada, el armado o desarmado automático de las alarmas si un área está vacía/no está vacía y generar listas de reunión.
- La autorización para N personas otorgará acceso en cada puerta sólo cuando un número definido (N) de usuarios de tarjetas autorizados presenten sus credenciales en una lectora configurada de forma correspondiente. La configuración se puede realizar de lectora en lectora y desde 2 a N personas (ilimitado).
- La función de trampa para gestionar dos puertas cooperativas con dos pares de lectores; recomendada para elevados niveles de seguridad, por ejemplo, entradas a salas del servidor o departamentos de investigación.
- Ronda de guardia: sofisticado sistema seguimiento mediante patrulla que emplea las lectoras de control de accesos existentes y la comprobación de secuencias y horas de acceso. Cualquier infracción de la secuencia o del horario de la patrulla provoca una alarma, de la que se realiza un seguimiento mediante las avanzadas funciones de

administración de alarmas de BIS. Los reportes de la ronda de guardia se pueden generar desde el registro de eventos de BIS.



- Función de comprobación aleatoria: se puede detener a usuarios de tarjetas que accedan o abandonen el lugar de forma aleatoria y enviarlos al personal de seguridad para que realicen una inspección más exhaustiva. Es posible excluir de la comprobación las tarjetas pertenecientes a usuarios designados como VIP.
- Administración de visitantes: las tarjetas de visitante se pueden controlar y gestionar de forma independiente en función de sus plazos de validez y de la posible necesidad de escolta.
- Interfaz de armado o desarmado de un IDS (sistema de detección de intrusos), como el manejo de autorizaciones y la asignación de tarjetas.
- Importación y exportación basada en web de datos de titulares de tarjetas almacenados en sistemas de terceros o en un servidor de directorios, como Microsoft Active Directory o Apache Directory.
- Toda la información personal, incluidas fotos y firmas, se almacena en una base de datos SQL protegida.
- Gestión de niveles de amenazas para preconfigurar hasta 15 escenarios, incluidas las situaciones de bloqueo y evacuación.
- Interfaz de ascensor para controlar hasta 64 plantas mediante un lector de tarjetas interno de un ascensor, así como para asignar las asignaciones de autorizaciones de plantas a los soportes de tarjetas.
- Interfaz con sistemas de gestión de destinos capaces de autorizar hasta 255 plantas con puerta delantera y trasera en un sistema de ascensores.
- Interfaz para importar datos personales a partir de un sistema de administración personal o exportarlos desde ACE a tal sistema.

- Personalización de tarjetas mejorada para importar imágenes de soportes para tarjetas y crear diseños personalizados de marcas corporativas que pueden imprimirse mediante impresoras de tarjetas estándar.
- Función de desbloqueo remoto de puertas (por ejemplo, mediante un clic del mouse en un icono del mapa de ubicaciones interactivo de BIS).
- Creación de zonas lógicas (por ejemplo, habitaciones individuales, grupos de habitaciones, plantas completas o zonas de estacionamiento) a las que se pueden asignar puntos de control de accesos especiales.
- Gestión flexible de alarmas para una amplia gama de condiciones de alarmas (por ejemplo, acceso denegado, detección de sabotaje, marcas en lista negra, alarma de coacción, etc.), que puede combinarse opcionalmente con funciones de BIS como los mapas de ubicación interactivos y los planes de acción.
- Uso de las funciones digitales, de seguimiento de E/S para mayor control y de seguimiento de la gama de controladores de Bosch (incluida la detección de intrusiones y sabotajes).
- La comunicación entre los controladores de acceso local y los lectores está protegida por OSDP V2 (OSDP Secure Channel).
- La comunicación entre el sistema de control de acceso principal y los controladores de acceso locales está protegida por DTLS (con codificación AES-256).



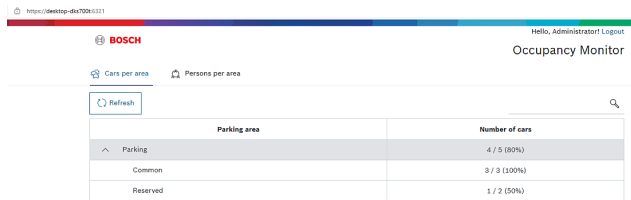
- Registro detallado de los eventos de acceso y las alarmas para cumplimiento legal e investigación científica.
 - Pista de auditoría que recoge los cambios en los registros y autorizaciones maestros, incluida la creación, modificación y eliminación de registros.
 - Capacidad de generación de reportes con filtrado.
- Soporte para hasta ocho formatos diferentes de tarjetas de forma simultánea.
- Edición masiva de autorizaciones y otros datos.

Verificación mediante vídeo

La verificación mediante vídeo amplía el nivel de seguridad del sistema de control de accesos mediante tecnología de vídeo. Si un lector está en modo de verificación de vídeo, no se admite al usuario de tarjeta de forma automática. En su lugar, el lector realiza una solicitud de entrada que aparece en forma de mensaje en la pantalla del operador.

Un plan de acción (consulte los accesorios opcionales de BIS) muestra al operador la imagen del usuario de tarjeta almacenada en la base de datos del ACE, así como una imagen en directo de una cámara cercana a la entrada/lectora que envía la solicitud. El operador compara ambas imágenes y decide si abrir o no la puerta.

Administración de zonas de estacionamiento



Con esta función se puede definir y utilizar el modelo de puerta de zona de estacionamiento, que permite controlar dos barreras de entrada y salida y sus semáforos correspondientes, que impiden el acceso cuando la zona ha alcanzado su capacidad máxima. El acceso a las zonas de estacionamiento se puede regular mediante lector de largo alcance y tarjeta de identificación o por cámara y matrícula. Cada zona de estacionamiento puede dividirse en zonas lógicas y definirse un número de vehículos máximo para cada una. Los cuadros de diálogo estándar permiten asignar la autorización para pasar la barrera y estacionar en un área lógica a los usuarios de tarjeta. También se puede realizar un equilibrio de carga de las zonas de estacionamiento y que aparezca información sobre la capacidad actual en la pantalla del operador. El equilibrio de carga de los vehículos (zonas de estacionamiento) y personas (áreas de acceso) se gestiona por separado, por lo que es posible realizar un seguimiento simultáneo de la ubicación del titular de tarjeta y del vehículo.

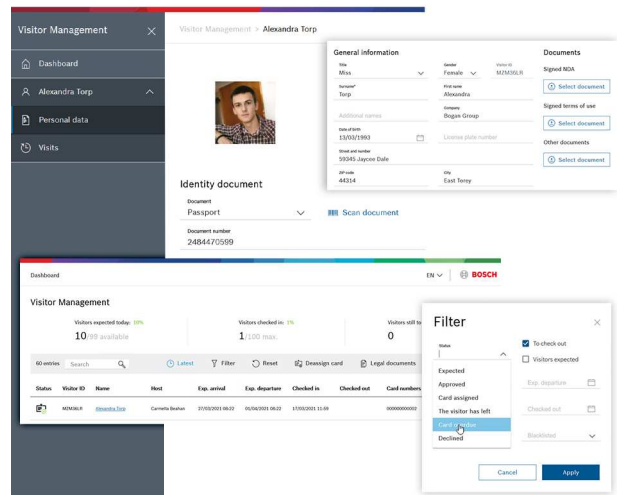
Gestión de visitantes

- Registre previamente las citas en el sistema para acortar el tiempo de procesamiento.
- Permita a los visitantes crear sus propios perfiles en modo quiosco para evitar que se formen colas en la recepción.
- Utilice un panel para supervisar las visitas esperadas del día, cuántos visitantes hay en las instalaciones, qué credenciales están en uso y qué credenciales están pendientes de recogida.

- Establezca fechas de caducidad de los perfiles de visitantes y sus archivos adjuntos para cumplir con las normas nacionales de privacidad de datos, como el RGPD europeo.

Welcome

Please enter your visitor ID.



Integración de paneles de intrusión

Los permisos para utilizar los paneles de intrusión B Series y G Series de Bosch se pueden asignar a los titulares de tarjetas de forma centralizada, lo que les permite armar y desarmar áreas controladas por intrusión.

Con la autorización adecuada, un titular de tarjeta puede desarmar un área y abrir su puerta con solo pasar la tarjeta en un simple lector.

Control de accesos para el control de enfermedades

- Los nuevos lectores de huellas dactilares y reconocimiento facial sin contacto eliminan una peligrosa fuente de contaminación. Para una seguridad aún mayor, el sistema puede exigir opcionalmente una tarjeta sin contacto o una credencial biométrica adicional para la autenticación.
- El control de secuencia de acceso ayuda a aplicar el flujo de multitudes unidireccional, lo que reduce el riesgo de infección al eliminar los encuentros cara a cara.
- La gestión del nivel de amenaza de ACE proporciona maneras de cambiar instantáneamente de un esquema de flujo de multitudes a otro, en caso de emergencia.
- Las áreas de control de acceso de ACE son ideales para implementar rápidamente restricciones higiénicas en el número de personas en un espacio definido.
- Los lectores sin contacto eliminan la necesidad de botones físicos en el ascensor.
- El armado y desarmado sin contacto de las áreas de intrusión reduce aún más las fuentes de contaminación.

- El uso de teléfonos móviles para el acceso promueve la higiene al reducir el número de credenciales físicas compartidas: una solución cooperativa desarrollada con los socios de **HID y STiD**.
- Los sistemas de reconocimiento de matrículas reducen la necesidad de cabinas de control, teclados y botones con personal; o de salir fuera del vehículo con las credenciales físicas.

Accesorios para BIS Access Engine

Administración de estacionamiento extendido

Proporciona administración de estacionamiento de invitados, incluida la generación de tiques de aparcamiento y la notificación de los visitantes que superan las citas programadas.

Interfaz de programación de aplicaciones

Un kit de desarrollo de software (SDK) para integrar Access Engine con aplicaciones de terceros como sistemas de administración de identidades, horarios y asistencia y administración de visitantes.

Integración de armarios de llaves

Integración de armarios de llaves **Deister y Kemas** para proteger llaves físicas y monitorizar su utilización. Disponible solo en ciertos países.

Integración de bloqueos en línea inalámbricos

Integración de los bloqueos en línea inalámbricos **SimonsVoss SmartIntego** (cilindros de cierre, picaportes y candados) para puertas, que requieren un nivel medio de seguridad, como oficinas y aulas. Disponible solo en ciertos países.

Integración de cierres remotos sin conexión

Integración de **cerraduras tipo "offline" (fuera de línea) OSS-SO o Normbau (Pegasys)** para puertas remotas, donde la conexión a través de cableado no es posible debido a la distancia, las condiciones de construcción o el coste. El sistema de bloqueo sin conexión se compone de software, hardware y accesorios. El hardware está disponible de forma gratuita en el mercado libre de socios de Bosch. La licencia de software activa un determinado número de diálogos en BIS y ACE. Disponible solo en ciertos países.

Aumenta la capacidad de control de accesos

ACE se escala fácilmente conforme a las necesidades de sus centros. Licencias adicionales de MAC (Main Access Controller) permiten aumentar la cobertura geográfica o el rendimiento. Es posible acomodar un número creciente de personal o visitantes utilizando licencias adicionales de titular de tarjeta.

Las licencias para aumentar el número de entradas están disponibles en pasos de 32, 128 o 512. En este sentido, una entrada equivale a un modelo de puerta ACE, lo cual facilita el cálculo de los requisitos.

Ejemplo: sus instalaciones tienen dos entradas principales con una lectora de entrada y de salida en cada una, 26 puertas de oficina con lectora de entrada y una esclusa para la sala de servidores. El número total de modelos de puerta/entradas es 29, independientemente del número de lectores empleados. La licencia del paquete de ACE básico ya cubre un total de 32 entradas.

Notas de configuración/instalación

Access Engine en cifras

Los siguientes máximos se aplican al sistema de referencia que se describe a continuación.

Número máximo de tarjetas activas por sistema	400,000
Número máximo de lectores por servidor	10,000
Número máximo de MAC (Master Access Controllers) por servidor	40
Número máx. de autorizaciones de acceso por MAC	1,000
Número máximo de AMC por MAC	125
	Para sistemas de alto rendimiento: 60
Número máx. de autorizaciones de acceso por ACE	40,000
Número máximo de divisiones por ACE	400
Número máximo de rondas de guardia por ACE	200
Número máximo de rondas de guardia simultáneas	8
Número máximo de paneles de intrusión B/G para la sincronización del titular de la tarjeta con ACE	500

Sistemas de referencia para servidor y cliente

	Sistema de servidor (sin cliente en funcionamiento)	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	Gráficos integrados desde la CPU	Gráficos Intel UHD 630 (memoria GPU de 4 GB)
Disco del sistema	NVMe	Disco SSD

	Sistema de servidor (sin cliente en funcionamiento)	Sistema cliente
	Velocidad de escritura: 1440 MB/s Velocidad de lectura: 2250 MB/s Tiempo medio de respuesta: 10 ms	
Disco donde está instalado AMS	SSD Velocidad de escritura: 1000 MB/s Velocidad de lectura: 1100 MB/s Tiempo medio de respuesta: 10 ms	
Sistema operativo	Microsoft Server 2019 Standard Edition	Microsoft 10 Pro Edition

Versiones del navegador para programas de complementos basados en web

Navegador web	Versión
Google Chrome	112 o superior
Microsoft Edge	111 o superior
Mozilla Firefox	102 o superior

Especificaciones técnicas

Consulte las especificaciones de la versión correspondiente de BIS Basic Package.

Información para pedidos

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

Licencia básica BIS-FACE-BPA50
 Licencia básica para BIS Access Engine
 Número de pedido **BIS-FACE-BPA50 | F.01U.415.273**

Licencia del paquete básico sin conexión BIS-FACE-OFFL50
 Licencia del paquete básico sin conexión (ACE)
 Número de pedido **BIS-FACE-OFFL50 | F.01U.415.275**

Licencia para gestión de estacionamiento BIS-FACE-PRK50

Licencia para gestión de estacionamiento (ACE)
 Número de pedido **BIS-FACE-PRK50 | F.01U.415.277**

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

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

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

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

Licencia para 128 puertas BIS-XACE-128D50
 Licencia para 128 puertas (ACE)
 Número de pedido **BIS-XACE-128D50 | F.01U.415.288**

BIS-XACE-1KC50 Licencia para 1000 tarjetas ID
 Licencia para 1000 tarjetas ID
 Número de pedido **BIS-XACE-1KC50 | F.01U.415.291**

Licencia para 1 armario de llaves BIS-XACE-1KEY50
 Licencia para 1 armario de llaves
 Número de pedido **BIS-XACE-1KEY50 | F.01U.415.295**

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

Licencia para 25 puertas sin conexión BIS-XACE-25OF50
 Licencia para 25 puertas sin conexión
 Número de pedido **BIS-XACE-25OF50 | F.01U.415.286**

Licencia para 25 puertas online inalámbricas BIS-XACE-25ON50
 Licencia para 25 puertas online inalámbricas
 Número de pedido **BIS-XACE-25ON50 | F.01U.415.294**

Licencia para 32 puertas BIS-XACE-32DR50
 Licencia para 32 puertas
 Número de pedido **BIS-XACE-32DR50 | F.01U.415.287**

BIS-XACE-50KC50 Licencia para 50.000 tarjetas ID
 Licencia para 50.000 tarjetas ID
 Número de pedido **BIS-XACE-50KC50 | F.01U.415.293**

Licencia para 512 puertas BIS-XACE-512D50
 Licencia para 512 puertas
 Número de pedido **BIS-XACE-512D50 | F.01U.415.289**

Licencia para 25 puertas sin conexión OSS-SO BIS-XACE-25OS50
 Licencia 25 puertas sin conexión OSS-SO
 Número de pedido **BIS-XACE-25OS50 | F.01U.415.309**

Representado por:

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