



Notas de versión del software Sigur

Revisión del 16/07/2026

Tabla de contenido

1.	Versión 1.6.8.131 (añadido en julio de 2026)	3
2.	Contactos	17

1. Versión 1.6.8.131 (añadido en julio de 2026)

Sistema:

- Se ha implementado protección del servidor contra ataques DoS y contra la suplantación de direcciones IP utilizada en ataques de amplificación, de acuerdo con el protocolo DTLSv1.2.
- Se ha corregido un fallo que provocaba el cierre inesperado del módulo del servidor durante la identificación facial (cámara IP) al utilizar la lógica «Permitir acceso solo acompañado».
- Se ha corregido un error de inicio del módulo del servidor que se producía cuando la contraseña de la base de datos comenzaba con el símbolo \$.
- Se ha corregido un problema que podía provocar el cierre inesperado del módulo del servidor durante la ejecución de copias de seguridad automáticas de la base de datos.
- Se ha mejorado la estabilidad del módulo del servidor cuando el reconocimiento facial de Sigur está habilitado y se establece una conexión al puerto TLS sin intercambio posterior de certificados.
- Se ha corregido un bloqueo del servidor que impedía la conexión de las estaciones de trabajo cliente.
- Se ha corregido el funcionamiento del comando exit en la utilidad AdminCLI.
- Se ha corregido un error en la visualización del número permitido de identificadores en la licencia, que provocaba falsas alertas de superación del límite.

Instalación y actualización del software. Durante la desinstalación silenciosa del software con el parámetro /S, todas las ventanas gráficas se cierran correctamente. Antes de la desinstalación en el servidor, el módulo del servidor y el servidor de bases de datos se detienen automáticamente.

Software «Cliente»:

- Se ha mejorado el rendimiento y se han corregido errores en la pestaña «Personal» durante la generación continua de un gran volumen de eventos.
- Se ha corregido un problema que provocaba el cierre inesperado del software «Cliente» al restablecer la conexión con el servidor.
- Se ha corregido un problema por el que, al instalar una estación de trabajo cliente en Windows, no se creaban los accesos directos en el menú «Inicio» ni en el escritorio.
- Se ha corregido un problema que provocaba el bloqueo del software «Cliente» al intentar iniciar sesión.
- Se ha corregido un problema que provocaba el bloqueo del sistema al trabajar con los modos de acceso cuando se utilizaba el módulo «Cuarentena».
- Se han corregido los problemas que se producían en el software «Cliente» en Linux al enviar un correo electrónico de prueba durante la configuración del servidor SMTP.

Controladores:

- Se ha añadido compatibilidad con los controladores E2 Lite, E2 Pro, E4 Lite y E4 Pro.
- En la pestaña «Dispositivos OSDP» de la configuración de los controladores se han añadido las columnas «Modelo del dispositivo», que muestra el modelo del lector Sigur conectado, y «Configuración» para asignar funciones a los modos de funcionamiento principal y secundario del lector MK100.
- Se ha actualizado el campo «Retardo de activación del sistema de seguridad (ms)» en la configuración del controlador. Ahora el valor se establece mediante un control deslizante en lugar de introducirse manualmente. El valor máximo es de 60 000 ms. También se ha corregido un problema relacionado con el guardado incorrecto del tiempo de armado.
- Se ha añadido al instalador del software un archivo con las versiones actuales del firmware de los controladores. A partir de ahora, para los controladores de la gama actual ya no es necesario descargar el firmware desde el sitio web.
- Se ha mejorado la estabilidad de la conexión entre el controlador y el servidor. Anteriormente, en algunos casos podía producirse una pérdida de comunicación. Ahora el servidor consulta los controladores cada 30 segundos en lugar de cada 600 segundos.
- Se ha refactorizado el proceso de carga de datos de los controladores, lo que ha permitido acelerar la sincronización de los datos y reducir el consumo de memoria RAM.
- Se ha corregido un problema por el que la configuración personalizada del punto de acceso en un controlador con firmware versión 0.x.x se reemplazaba por la configuración estándar al cambiar el método de armado.
- Se ha corregido un problema que podía provocar el error «No se ha podido iniciar la actualización» durante la actualización del firmware del controlador.
- Se ha corregido un problema de sincronización lenta de los datos en la memoria del controlador al crear un nuevo empleado.
- Ahora, al configurar un controlador, la lista de salidas para «Línea de indicación LED3 del lector N» solo muestra las salidas disponibles para ese modelo de controlador.
- Se ha corregido un error en el funcionamiento del botón para cambiar el perfil de cifrado.
- Se ha corregido un problema por el que, al seleccionar la configuración estándar del controlador E510 «Dos torniquetes, control potencial», se aplicaban parámetros incorrectos para «Botón de solicitud de acceso "Entrada"/"Salida"».
- Se ha ampliado la aplicación del tiempo de espera «Tiempo de espera del acompañante», que ahora también se utiliza para esperar al segundo sujeto de acceso. Este cambio es aplicable a los controladores con firmware 1.24.0 o superior.

Lectores:

- Se ha añadido compatibilidad con las nuevas gamas de lectores Sigur MK100 y MR100 v2.
- Se ha añadido compatibilidad con el lector SR100 EMB en los modos USB PC/SC y USB HID.

Indicaciones de los lectores:

- Se ha corregido el comportamiento de la ventana de configuración de las indicaciones de los lectores en el software «Cliente». Ahora, al cancelar el guardado de los cambios, los perfiles de indicación ya no desaparecen y la ventana se cierra correctamente al primer intento en todas las pestañas.
- Se ha prohibido crear perfiles de indicación personalizados cuyos nombres comiencen por «\$!».
- Se ha corregido el funcionamiento incorrecto de la indicación «Cambiar color», que provocaba un único parpadeo del indicador del lector en lugar de cambiar su color.
- Se ha corregido un error en la generación del nombre del archivo adjunto del perfil de indicación al enviarlo por correo electrónico. Anteriormente, cuando se utilizaban caracteres cirílicos, algunos clientes de correo mostraban el nombre del archivo en forma codificada.

Tarjetas Mifare:

- Se han corregido errores de lectura y escritura en determinadas tarjetas Mifare Classic en modo protegido.
- Se ha corregido un problema al convertir tarjetas Mifare Plus al modo SL3 utilizando el lector ACR1252U.

Personal:

- Se ha corregido un problema por el que los cambios en los permisos de acceso a un punto de acceso no se aplicaban si en ese momento no existía comunicación con el controlador.
- En Windows se ha añadido un límite para el tamaño de las imágenes cargadas en las pestañas «Personal» y «Planos». Ahora se admite una resolución máxima de 4K (3840 × 2160).
- Se ha corregido un problema por el que la ventana de importación de personal desde una hoja de cálculo de MS Excel se cerraba si el archivo seleccionado contenía fórmulas.
- Se ha corregido un error que se producía tras eliminar un departamento cuando el operador tenía configurado un límite de capacidad para dicho departamento.
- Se ha corregido un problema que podía provocar un error de acceso a la base de datos al cambiar el tipo de sujeto de acceso y pasar a otro sin guardar los cambios.
- Se ha eliminado la posibilidad de editar el tipo Wiegand para los códigos QR en la pestaña «Personal».
- Ahora, al cambiar el tipo de identificador asignado a un empleado por un código QR, se utiliza automáticamente el formato configurado en «Archivo» – «Configuración» – «Códigos PIN y QR». La lista desplegable de formatos ya no es editable.
- Se ha añadido el bloqueo de la lista desplegable de formatos al añadir un código PIN.
- Se ha añadido una nueva propiedad del pase: «Tipo de pase». Esta propiedad

se muestra en la ficha del sujeto de acceso y se selecciona manualmente al emitir un nuevo pase desde la interfaz del software «Cliente». Ahora es posible añadir para los empleados tarjetas, identificadores móviles, códigos PIN y códigos QR. El tipo de pase también puede especificarse al importar personal desde un archivo XLS.

- Tras la actualización del software, todos los pases con formatos W26, W34, W36, W37, W42, W58 y W58Dec tendrán establecido el tipo «Tarjeta». Si es necesario, el tipo de pase puede modificarse manualmente o mediante la utilidad de sobrescritura masiva del tipo de pase mediante comentario.
- La imagen del código QR del empleado puede visualizarse y copiarse desde la pestaña «Personal», así como añadirse a las plantillas de impresión de pases.
- Se ha corregido la ordenación incorrecta de las plantillas de pases durante su creación y eliminación.
- Se ha corregido un problema por el que, al limitar la validez de un pase, se rellenaban automáticamente la fecha y la hora utilizadas anteriormente para otro pase.
- Se ha corregido un problema relacionado con el guardado incorrecto de la fotografía en la ficha del sujeto de acceso.
- Se ha corregido un error al guardar los cambios en el plazo de validez del pase y del acceso durante la edición masiva.
- Se ha corregido un error de acceso a la base de datos al intentar imprimir el pase de un empleado.
- Se ha corregido un problema por el que, al crear varios nuevos sujetos de acceso de forma consecutiva, el último podía heredar el número de teléfono del anterior.
- Se ha corregido un problema por el que, al copiar una plantilla gráfica de pase, los datos no se transferían a la nueva plantilla.
- Se ha corregido un error de acceso a la base de datos que podía producirse al añadir un nuevo cargo. Ahora, si se intenta crear un cargo cuyo nombre solo difiere por el uso de mayúsculas/minúsculas, las letras «e»/«ë» o un espacio final, el sistema muestra un aviso indicando que dicho cargo ya existe.
- Se ha corregido un problema por el que el botón «Eliminar elemento seleccionado» permanecía activo al seleccionar el departamento raíz «Objeto».

Videovigilancia:

- Se ha restablecido la recepción de matrículas reconocidas desde el servidor ISS (SecurOS) en las estaciones de cliente de Sigur con Linux.
- Se ha corregido un problema de registro duplicado del evento de denegación de acceso durante el reconocimiento de la matrícula de un sujeto con un período de validez limitado.
- HikCentral. Se ha mejorado y optimizado la integración. Se ha publicado una nueva versión del servicio de integración: 1.1.0.
- Trassir. Se ha corregido un problema que podía provocar el cierre inesperado del módulo del servidor al intentar realizar un paso por un punto de acceso en modo de identificación facial.
- Macroscop. Se ha corregido un problema que provocaba el cierre inesperado del módulo del servidor cuando la integración estaba activa.
- Domination. Se ha corregido la visualización incorrecta de los canales

- importados desde el sistema Domination en el software Sigur.
- Se ha corregido un problema por el que, al modificar la fotografía de un empleado mediante la API REST, la imagen no se sincronizaba con el sistema de videovigilancia.
 - Se ha corregido un error de autorización al abrir vídeo archivado en la pestaña «Archivo» del software «Cliente» que se producía al seleccionar un evento, cuando la contraseña del operador contenía caracteres especiales.

Monitoreo:

- Se ha corregido un problema por el que el software «Cliente» no se iniciaba tras reiniciarse si la vista de monitoreo contenía el elemento «Matriz de objetos de seguridad».
- Se ha añadido la posibilidad de mostrar el departamento del sujeto de acceso para el objeto «Localización de empleados» en la pestaña «Monitoreo».
- En la ventana modal «Mostrar eventos» de la pestaña «Monitoreo» del software «Cliente» se ha eliminado el filtro del evento «Se ha acercado la tarjeta», ya que este evento no se muestra en dicha pestaña.
- Se ha corregido el bloqueo del software «Cliente» cuando el flujo RTSP no está disponible en la pestaña «Monitoreo».
- Se ha corregido la visualización incorrecta de la información en la pestaña «Monitoreo» al crear una vista con un panel de texto que utiliza codificación HTML y una lista de eventos.
- Se ha corregido un problema por el que, al pulsar el botón «Actualizar» en la pestaña «Monitoreo», no se actualizaban los datos del personal en la ventana «Selección de empleados» al intentar autorizar el paso a través de un plano.

Modos:

- Se ha añadido un filtro por puntos de acceso en la pestaña «Modos».
- Se ha corregido la visualización incorrecta de las zonas en la configuración de los modos con cálculo del tiempo de trabajo basado en la presencia en las zonas especificadas.
- Se ha corregido un problema por el que el modo de nivel 1 se aplicaba incorrectamente al asignar modos de forma masiva desde la pestaña «Personal».
- Se han corregido varios problemas que se producían al copiar modos.
- Se ha eliminado la variable CODEKEY_DESC («Comentario del pase») de la lista de variables disponibles para configurar las condiciones de aplicación de los modos.

Pasos repetidos. Se ha corregido un problema por el que, durante la sincronización de datos de nuevos empleados, la regla de prohibición de pasos repetidos se aplicaba incorrectamente, lo que provocaba que se añadieran automáticamente a las listas de restricción independientemente de la configuración.

Archivo. A partir de ahora, el inicio del período se establece automáticamente con la fecha actual y la hora «Desde»: 00:00.

Informes:

- Se ha añadido un nuevo «Informe de disciplina laboral», que permite obtener información básica sobre las horas de entrada y salida de los empleados. El informe está disponible desde la versión gratuita del software. Este informe también puede adjuntarse a un correo electrónico como parte de una reacción ante eventos del sistema.
- El informe «Lista del personal» ahora incluye información sobre el tipo de pase.
- El «Informe de tarjetas no utilizadas» pasa a llamarse «Informe de pases no utilizados».
- Se ha corregido el formato de las celdas que contienen fechas u horas en las plantillas de informes.
- Se ha corregido un problema que modificaba el formato del fondo de las celdas en los informes exportados.
- Se ha corregido un filtrado incorrecto por empleados al exportar la planilla a 1C.
- «Informe unificado del tiempo de trabajo»:
 - Se ha corregido un problema por el que el informe no se generaba si el modo asignado al empleado contenía dos períodos de trabajo.
 - Se ha corregido un error en el informe por el que, al activar la opción «Incluir el día de la semana en las fechas», no se mostraban valores en la columna «Fecha».
- «Duración de presencia en las zonas de acceso»:
 - Se ha corregido el cálculo incorrecto del tiempo de permanencia en la zona actual al generar el informe.
 - Se ha corregido un problema por el que el informe incluía registros con fechas anteriores a la creación del empleado.
- «Registro de eventos del sistema»:
 - Se ha corregido la visualización incorrecta de la hora inicial en el informe.
 - Se ha corregido un problema por el que el informe incluía sujetos de acceso a los que el operador no tenía permisos.
- «Registro de acciones de operadores»:
 - Se ha corregido un problema por el que, al generar el informe «Registro de acciones de operadores», el filtrado por sujetos de acceso funcionaba incorrectamente. Asimismo la ventana de generación del informe muestra ahora el número de registros procesados desde la base de datos y el número de registros incluidos en el informe final.
 - Se ha corregido la generación incorrecta del informe «Registro de acciones de operadores» para operadores con restricciones de acceso a departamentos y puntos de acceso.
 - Se ha corregido un problema por el que el período previamente solicitado para el «Informe de pases no utilizados» podía mostrarse de forma incorrecta.
 - A partir de ahora, la eliminación de un modo queda registrada correctamente en el registro de acciones de los operadores.

- Se ha corregido un error en el informe «Registro de eventos de seguridad» por el que se mostraban eventos correspondientes a zonas de seguridad eliminadas.

Operadores:

- Se ha actualizado el texto de la información emergente correspondiente al permiso «Inicio de sesión con tarjeta».
- El parámetro «Identificador en SUDIR» ahora solo se muestra en los permisos del operador cuando existe la licencia correspondiente.
- Se ha corregido un problema por el que un operador podía editar el texto de las notificaciones en la pestaña «Personal» – «Notificaciones», incluso cuando el envío de notificaciones de aprobación de solicitudes estaba deshabilitado.
- Se ha corregido un problema que impedía eliminar el límite de capacidad de un departamento en la configuración de permisos del operador.
- Se ha eliminado la posibilidad de editar el texto de las notificaciones en la pestaña «Personal» – «Notificaciones» para operadores que no disponen de los permisos correspondientes.
- Se ha corregido un problema por el que, para los operadores del sistema con acceso restringido a puntos de acceso, el filtro de puntos de acceso de la pestaña «Personal» no mostraba los grupos de puntos de acceso.
- Se ha corregido un problema por el que un operador con permisos únicamente de visualización del personal podía asignar y eliminar modos de acceso.
- Se ha corregido un problema por el que un operador sin permisos para modificar la configuración de los equipos podía cambiar los ajustes en la pestaña «Equipos» – «Biometría».

Reacción ante eventos:

- El botón «Seleccionar todo» vuelve a funcionar correctamente al seleccionar eventos durante la creación de una reacción basada en un evento unificado.
- Se ha corregido un error por el que, al configurar una reacción para eventos de tipo «Tras el acceso» y «Tras la denegación de acceso», no se ejecutaba la acción «Establecer la duración del pase».
- Se ha implementado la comprobación de permisos del operador al configurar una reacción que envía informes por correo electrónico. Los informes se muestran ahora de acuerdo con las restricciones de acceso del operador. Si un operador no dispone de permisos para acceder a los informes asociados a reacciones creadas previamente, los eventos vinculados a dichas reacciones no se muestran en la pestaña «Eventos».
- Se ha corregido un problema que podía afectar al envío de informes por correo electrónico cuando el idioma de la estación de trabajo cliente era diferente del idioma del servidor.
- Se ha corregido un error por el que, al eliminar un evento con cambios no guardados en la reacción, la confirmación del guardado aplicaba los cambios, pero el evento se eliminaba igualmente.
- Se ha corregido un error al enviar por correo electrónico el Informe de disciplina laboral, que provocaba que el archivo se generase con un formato incorrecto.

Gestión de pases temporales de visitantes:

- Se ha corregido un problema por el que, al crear un código QR o un pase de visitante mediante la API REST, no se establecían puntos de acceso, lo que impedía conceder acceso posteriormente.
- Se ha corregido un problema en el tratamiento de códigos QR por el que las fotografías e imágenes adicionales no se procesaban correctamente: los archivos adjuntos no se mostraban en la pestaña «Personal» ni en la plantilla gráfica del pase.
- Se ha corregido un problema por el que no se realizaba el envío automático y manual de correos electrónicos con códigos QR para visitantes desde Sigur cuando el visitante había sido creado mediante la API REST.
- Se ha corregido la ausencia de un valor en el campo «Visitando a» al enviar un pase QR por correo electrónico. Anteriormente, el campo podía permanecer vacío si no existía una solicitud asociada.
- Se ha corregido un problema por el que la fecha de inicio de validez y la fecha efectiva de emisión del código QR no coincidían con los valores especificados en la solicitud.
- Se ha corregido un error en la gestión del período de validez de los pases de visitante: al editar o modificar personal de forma masiva, los cambios en el período de validez y en las restricciones del plazo se aplicaban incorrectamente, provocando discrepancias entre las pestañas «Visitantes» y «Personal». Se han añadido comprobaciones de los pases emitidos y se ha sincronizado la disponibilidad de los parámetros relacionados con el período de validez.
- Se ha corregido un problema por el que, al modificar el período de validez de un pase de visitante en la pestaña «Visitantes», desaparecía el registro de su emisión.
- Se ha corregido un problema relacionado con el guardado de los valores de los parámetros adicionales al emitir un pase de visitante utilizando información ya existente del visitante.
- Se ha corregido un problema por el que los cambios en el nombre completo de un visitante con código QR no se sincronizaban con la sección «Personal», incluso después de actualizar las pestañas o reiniciar el software «Cliente».
- Se ha corregido el funcionamiento incorrecto del procedimiento de eliminación de datos del visitante seleccionado.
- Se ha corregido un error que se producía al crear una solicitud sin especificar el tipo de documento en el servicio web de solicitudes.
- Se ha corregido la visualización incorrecta de la versión del software en el servicio web de solicitudes.
- Se ha corregido un problema por el que no se abría la página con el número de solicitud y el código QR al crear una solicitud con aprobación automática mediante el servicio web.
- Se ha corregido un problema por el que, al consultar una solicitud creada desde el software «Cliente» con varios visitantes, en el servicio de solicitudes solo se mostraba el código QR del primer visitante, incluso si se introducía el número de documento de otro participante de la solicitud.
- Se ha corregido un problema en el servicio web de solicitudes por el que el mensaje de notificación sobre el reenvío del código QR aparecía en inglés.

- Se ha añadido la validación de los campos «Inicio de vigencia» y «Fin de vigencia» al crear una solicitud de visita.
- Se ha añadido un nuevo valor del sistema «No seleccionado» para el tipo de documento del visitante.
- Se ha añadido la comprobación de unicidad del nombre del documento durante la edición. Los espacios en blanco al principio y al final del nombre se eliminan automáticamente y ya no se guardan.
- Se ha corregido la visualización incorrecta del valor del parámetro «Visitando a» en la ventana de información del código QR emitido al visitante. Ahora, si el empleado visitado ha sido dado de baja o eliminado del sistema, su nombre completo se muestra con el prefijo «[Y]».
- Se ha corregido un problema por el que, al emitir un pase para un visitante, el campo Email se rellenaba automáticamente con el valor example@ex.com.

Reconocimiento de documentos:

- Se ha añadido compatibilidad para la integración con Content AI PassportReader SDK 1.5.5.
- Se ha restablecido la compatibilidad con ABBYY PassportReader SDK. Para garantizar el funcionamiento correcto durante la configuración inicial, es necesario ejecutar el software «Cliente» con privilegios de administrador.

Terminal móvil Sigur:

- Se ha implementado la posibilidad de escanear códigos de barras de formato Code 128, así como pases de tipo «Código QR», mediante la aplicación «Terminal móvil». Como parte de esta funcionalidad, se ha añadido un nuevo permiso de operador en el software «Cliente». Además, el «Archivo» y los informes registran ahora el nuevo evento «Código leído: <cadena leída>».
- El software «Cliente» registra ahora el evento «Acceso denegado. Número de pase desconocido.» cuando se presenta una tarjeta desconocida en un terminal Sigur sin conexión.
- Se ha corregido un error por el que, al escanear un código QR de visitante en la aplicación «Terminal móvil», se mostraba el mensaje «Número de pase desconocido», aunque el pase hubiera sido emitido correctamente mediante el servicio web de solicitudes.

Sincronización de datos:

- Se ha refactorizado la funcionalidad de sincronización de datos desde fuentes externas hacia la base de datos de Sigur, lo que ha permitido acelerar el proceso de sincronización.
- Se han corregido errores y bloqueos del software «Cliente» que se producían durante la sincronización de sujetos de acceso con formatos de fecha incorrectos.
- Se ha corregido un problema por el que distintos sujetos de acceso podían recibir el mismo pase durante la sincronización de los datos desde fuentes externas.
- Se ha corregido un problema por el que la sincronización desde una base de

datos externa no se ejecutaba si el campo «Período de validez del pase» de los empleados se quedaba sin rellenar (NULL).

- Se ha corregido un problema por el que un empleado cuyo campo «Período de validez del pase» estaba sin rellenar (NULL) se eliminaba o se trasladaba a la carpeta «Despedidos» durante la sincronización desde una base de datos externa.

Active Directory: Se ha corregido un problema por el que, al configurar el bloqueo de cuentas de Active Directory, la lista de zonas permitidas no se mostraba hasta reiniciar el software «Cliente».

Sistema de pago:

- Se ha corregido un bloqueo del software «Cliente» al añadir o modificar de forma masiva la cuenta de varios sujetos de acceso.
- Se ha corregido la visualización incorrecta del importe de una transacción al recibir una notificación de cambio de saldo de la cuenta.
- Se ha corregido un error al guardar el valor de la cuenta asociada a un código QR de visitante.

Sistema de detección y alarma de incendio:

- Se ha corregido un problema que provocaba una inicialización prolongada del software «Cliente» cuando existía un gran número de puntos de acceso y el operador tenía acceso a la pestaña «Seguridad».
- Se ha corregido un problema por el que era necesario reiniciar el módulo del servidor para mostrar correctamente el estado de una nueva zona de seguridad.
- Se ha añadido la visualización de tres nuevos eventos relacionados con las zonas de seguridad de Sigur: «No se pudo armar la zona. La línea de alarma no está configurada», «... El lector está ocupado» y «...La seguridad de la zona ya se está activando». Estos eventos están disponibles en los informes del sistema, en el «Archivo» y en la pestaña «Monitoreo», y también pueden utilizarse para configurar reacciones ante eventos.
- Los eventos de las zonas de seguridad de los controladores Sigur se muestran ahora no solo en el «Registro de eventos de seguridad», sino también en el «Archivo» y en el «Registro de eventos del sistema». Este cambio solo afecta a nuevos eventos registrados.
- Se ha corregido un problema por el que no era posible obtener el estado de una zona de seguridad de Sigur ni armarla.

Biometría:

- Se ha corregido un problema relacionado con la generación y el guardado de las plantillas de venas de la palma de Biosmart.
- Se ha corregido la aparición de advertencias sobre cambios no guardados en la configuración de biometría de Vzor cuando en realidad no existían modificaciones.
- Se ha corregido un problema relacionado con la generación de plantillas

biométricas de Biosmart Quasar que se producía cuando el nombre de usuario del sistema operativo contenía caracteres cirílicos.

Integración con terminales de reconocimiento facial Suprema:

- Se ha optimizado el rendimiento y la estabilidad del servicio de integración.
- Se ha añadido compatibilidad para la integración con servidores Sigur que se ejecutan en Debian Linux y RHEL.
- Se ha añadido compatibilidad con PostgreSQL como base de datos externa del sistema de control de acceso.
- Se ha validado el funcionamiento con dispositivos Suprema mediante el protocolo OSDP.
- Se ha corregido un problema que provocaba bloqueos del software «Cliente» y errores en los registros después de habilitar la integración con Suprema desde «Archivo» – «Configuración» – «Biometría».
- Se ha corregido un problema por el que el proceso supremaservice no finalizaba y el software «Cliente» quedaba bloqueado tras deshabilitar la integración en Linux.
- Se ha corregido un problema por el que la integración con Suprema continuaba funcionando tras el vencimiento de la licencia.
- Se ha corregido la visualización incorrecta del campo «Tipo de código de pase para generar» en «Archivo» – «Configuración» – «Biometría» – «Suprema».
- Se ha corregido un problema por el que las plantillas biométricas no se cargaban en los terminales Suprema cuando el sistema contenía plantillas Biosmart Quasar.
- Se ha corregido un problema que podía provocar el cierre inesperado del módulo del servidor al intentar añadir una huella dactilar mediante dispositivos Suprema.
- Se ha corregido un problema relacionado con la sincronización de tarjetas en terminales Suprema cuando se eliminaba simultáneamente la restricción del período de validez de las tarjetas para varios empleados.

Integración con terminales de reconocimiento facial Hikvision:

- Se ha optimizado la integración, reduciendo la carga del servidor y acelerando la sincronización de los datos.
- Se ha corregido un error de sincronización de los datos con terminales Hikvision al utilizar la versión 1.5 del servicio de integración en sistemas Linux con PostgreSQL.

Integración con BAS-IP:

- Se ha corregido un problema por el que la información del personal no se sincronizaba con la memoria de los paneles de entrada.
- Se ha corregido un problema relacionado con la sincronización de pases de tipo «ID móvil» con la memoria de los paneles de entrada.

Integración con la caja de llaves Keyguard:

- Se ha eliminado la solicitud permanente de guardar cambios al seleccionar reglas de acceso en el software «Cliente», que aparecía incluso cuando no se había realizado ninguna modificación.
- Se ha corregido la visualización incorrecta de la lista de reglas de acceso a las llaves al asignar permisos a los empleados.

Integración con Dormakaba. Se ha corregido un problema por el que la lista de puntos de acceso y los eventos de paso no se sincronizaban desde el software Matrix.

Protocolo de integración WebDel. Se ha corregido un error por el que, cuando un sistema externo denegaba el acceso, se generaba el evento «Acceso denegado. El modo no permite el paso.».

REST API:

- Se han añadido nuevos tipos de eventos devueltos por las solicitudes GET /api/v1/events, GET /api/v1/events/types y GET /api/v1/events/parsed:
 - «Cambio del estado de alimentación del controlador» (DC_STATUS);
 - «Cambio del estado de la batería del controlador» (BATTERY_STATUS);
 - «No se pudo cambiar el modo del punto de acceso» (AP_MODE_DENY).
- El tipo de evento VOLTAGE_STATUS deja de utilizarse.
- Se ha añadido el atributo armingMethod al evento «Estado de la zona de seguridad» (ALARM_LINE_STATUS). Este atributo se devuelve en la respuesta de GET /api/v1/events/parsed cuando la zona ha sido armada mediante un lector Sigur MK100.
- Se han añadido nuevos motivos para determinados eventos devueltos por la solicitud GET /api/v1/events/parsed:
 - Para el evento PASS_DENY:
 - «Access period expired or not started» («Acceso denegado. El período de acceso no ha comenzado o ya ha terminado»);
 - «Waiting for confirmation of access point mode change» («Acceso denegado. En espera de confirmación del cambio de modo del punto de acceso»);
 - Para el evento WAITING_FOR_RULE_STAGE:
 - «Waiting for second access object» («Esperando al segundo sujeto para el acceso»);
 - «Waiting for confirmation of access point mode change» («En espera de confirmación del cambio de modo del punto de acceso»);
 - Para el evento MNG_STATE_CHANGED:
 - «PIN» y «PIN AND PASS» (cambio del modo del punto de acceso mediante el código PIN o mediante el código PIN con confirmación mediante el pase).
- Se han añadido nuevos tipos de eventos devueltos por las solicitudes GET /api/v1/events, GET /api/v1/events/types y GET /api/v1/events/parsed:
 - «No se pudo armar la zona» (ALARM_LINE_DENY);

- «Evento de estado de la zona de seguridad» (ALARM_LINE_STATUS).
- Se ha añadido un nuevo motivo para WAITING_FOR_RULE_STAGE: «Esperando confirmación de activación de la seguridad de la zona» («Waiting for confirmation of zone arming»). Se ha añadido el atributo alarmZoneId al objeto data, así como el objeto alarmZone dentro de additionalData.
- Se han añadido nuevos endpoints para gestionar tarjetas de visitante y códigos QR, administrar los registros de emisión de tarjetas de visitante y gestionar códigos QR y códigos PIN de empleados.
- Se ha añadido el campo tabid (número del departamento) al objeto departments, disponible también durante la creación y edición de departamentos.
- Se ha añadido la posibilidad de crear, modificar y eliminar el MFUID de las tarjetas.
- Se han actualizado las solicitudes de los grupos Employees y Official Vehicles:
 - el período de acceso del sujeto de acceso y el PIN de verificación pueden especificarse al crear un sujeto de acceso, modificarse y obtenerse mediante API REST (se han añadido los atributos accessStartTime, accessEndTime y verificationPin);
 - se ha añadido el objeto identifiers a los cuerpos de determinadas solicitudes y respuestas, que contiene todos los identificadores del sujeto de acceso;
 - se ha ampliado el conjunto de filtros: la solicitud GET /api/v1/employees admite ahora los operadores IN, NEQ, IS_NULL, IS_NOT_NULL y CONTAINS para filtrar por parámetros adicionales.
- Se ha modificado la lógica de funcionamiento de las tarjetas con el atributo guestApplicable=true.
- A partir de ahora, GET /api/v1/cards y GET /api/v1/cards/{id} devuelven únicamente pases de tipo «Tarjeta». Para consultar identificadores móviles, códigos QR y códigos PIN de los sujetos de acceso, deben utilizarse GET /api/v1/employees y GET /api/v1/employees/{id}.
- Se ha optimizado el procesamiento de GET /api/v1/events/parsed y GET /api/v1/events cuando se utiliza filtrado por tiempo.
- Se han corregido errores que se producían al generar un código QR de visitante mediante PUT /api/v1/guests/{id}/QR.
- Se ha corregido un problema por el que la respuesta a la solicitud GET /api/v1/guests incluía el atributo guestCardId para visitantes de tipo «QR», permitiendo acceder a la información mediante GET /api/v1/guestcards/{id}.
- Se ha corregido la representación incorrecta de los campos value y formattedValue en la respuesta de GET /api/v1/guestcards/{id}.
- Se ha corregido un problema por el que DELETE /api/v1/accessrules/{id} permitía eliminar los modos predeterminados.
- Se ha corregido el tratamiento incorrecto de GET /api/v1/bindings/employees-guestcards al utilizar los parámetros includeFields, excludeFields, limit y offset.
- Se ha corregido un error HTTP 500 al ejecutar GET /api/v1/guestcards con los parámetros value y sortBy. La ordenación por los campos assigned y formattedValue ya no está soportada para esta solicitud.
- Se ha corregido un error HTTP 500 que se producía al intentar eliminar el valor de un parámetro adicional obligatorio mediante PUT /api/v1/employees/{id}.

- Se ha corregido la validación de los valores de las tarjetas creadas mediante API REST . Ya no es posible crear una tarjeta o un código QR con un código igual a cero.
- Se ha corregido un problema en el procesamiento de eventos por el que GET /api/v1/events/parsed podía devolver una respuesta vacía.
- Se ha corregido un error HTTP 500 al ejecutar GET /api/v1/events cuando el servidor del sistema de control de acceso se ejecutaba sobre Linux.
- Se ha corregido un problema por el que GET /api/v1/employees devolvía todos los empleados cuando la búsqueda utilizaba un parámetro adicional inexistente. Ahora, en estos casos, el servidor devuelve el estado HTTP 422.
- Se ha corregido un problema por el que el filtrado por accessObjectId en GET /api/v1/events/parsed no funcionaba al utilizar PostgreSQL.
- A partir de ahora, GET /api/v1/employees, ejecutado por un operador con acceso completamente restringido a los departamentos, devuelve 200 OK con un resultado vacío.
- Se ha corregido el funcionamiento del filtro tabid en GET /api/v1/employees.

Otras correcciones y optimización del funcionamiento del sistema:

- Se ha corregido un problema por el que no se iniciaba el software «Gestión del servidor».
- Se han eliminado otras causas que podían provocar bloqueos y una disminución del rendimiento del sistema.
- Se ha corregido un problema que podía provocar el bloqueo de la pestaña «Configuración de dispositivos» – «Configurar dispositivos IP» en el software «Gestión del servidor».
- Se ha mejorado el rendimiento de la pestaña «Personal» al utilizar la integración con Biosmart.
- Se han corregido errores relacionados con la actualización tardía de la información de la licencia cargada en el software «Cliente».
- Se ha aclarado la descripción de ayuda para el parámetro «Multiplicador del resultado del alcoholímetro» en la configuración de los alcoholímetros conectados a los controladores Sigur mediante la interfaz Wiegand.

2. Contactos

Para cualquier consulta o asistencia, por favor contáctenos utilizando la información proporcionada:

Sitio web: www.sigur.com

Consultas generales: info@sigur.com

Soporte técnico: support@sigur.com