CYGNUS electronics

MANUAL DE USUARIO
CENTRO DE SEGURIDAD 5

C.Nord

Contenido

1 Novedades

La versión 5 del software Security Center tiene una serie de novedades que permiten a la empresa de seguridad no solo aumentar la lista de servicios prestados a los clientes, sino también optimizar el trabajo del operador y los servicios de ingeniería.

1.1 Deshabilitación de sitios, canales de comunicación y eventos

Durante el mantenimiento o reparación del equipo instalado en el sitio, es conveniente utilizar la operación de desactivación temporal del sitio. Después de especificar la hora y el motivo de la desactivación, el operador de servicio puede desactivar el sitio del Centro de seguridad para no distraerse al recibir y manejar los mensajes recibidos desde el sitio. Después de la expiración del período especificado, el sitio se enciende automáticamente, sin embargo, el operador puede habilitar el sitio antes.

Durante el período de mantenimiento o reparación de los equipos utilizados para proporcionar canales de comunicación con el sitio, es posible desactivar los canales de comunicación. Después de especificar la hora y el motivo de la desactivación, el operador de servicio puede desactivar uno o varios canales de comunicación del sitio para no distraerse al recibir y manejar los mensajes que pasan a través de ellos. La desactivación de uno u otro canal de comunicación no obstaculiza la recepción de mensajes a través de otros canales de comunicación del sitio. Una vez transcurrido el período de desactivación, los canales de comunicación se activan automáticamente, sin embargo, el operador puede activar los canales de comunicación antes.

Si se producen deliberadamente falsas alarmas de sistemas de alarma contra incendios en el sitio (debido a un mal funcionamiento del equipo, vulnerabilidad técnica del sitio, movimiento de animales, etc.), es posible utilizar la operación de desactivación temporal del evento. Después de especificar la hora y el motivo de la desactivación, el operador de servicio puede desactivar el evento del sitio para no distraerse manejando la alarma. Después de la expiración del período de desactivación, el evento se enciende automáticamente, sin embargo, el operador puede activar el evento antes.

Consulte los detalles sobre cómo desconectar un sitio, canal de comunicación o evento, en el capítulo sobre el módulo "Operador de servicio".

1.2 Reconexión del sitio

Al manejar un mensaje de alarma recibido de un sitio, puede ser necesario volver a cerrar el sitio: abrir, inspeccionar y activar el sistema de seguridad nuevamente después de que se eliminó la causa de la alarma. El software Security Center brinda la oportunidad de notificar automáticamente a las personas responsables del sitio sobre la necesidad de volver a cerrar los sitios, así como sobre la negativa de la persona responsable a volver a cerrarlos.

Se notifica a la persona responsable de la necesidad de volver a cerrar el sitio, así como de la negativa de la persona responsable a volver a cerrar con mensajes SMS. Es posible informar a la persona responsable de esta y otras situaciones en el módulo “Administrador del sitio” en la pestaña [“Personas responsables”] (# site-manager-doorkeys).

El operador del Centro de seguridad puede notificar a la persona responsable sobre el reenganche del sitio mediante la aplicación "Alarm to Guard".

Para que el operador del Centro de Seguridad notifique a las personas responsables del reenganche del sitio, se permitirán acciones como “Solicitud de reenganche” y “Fallo de reenganche”. La configuración necesaria se puede establecer en el módulo "Configuración del sistema" en la pestaña "Acciones" (# system-setup-actions).

Informar a la persona responsable sobre el reenganche del sitio se realiza con la ayuda del controlador de eventos "Reenganche del sitio". Este manejador genera el texto de los mensajes correspondientes al tipo de acción en el formato dado y envía SMS a los responsables. Consulte la información sobre la configuración del controlador en el capítulo dedicado al módulo [“Administrador de eventos”] (# event-manager-reclosig).

1.3 Información sobre herramientas

El módulo "Operador de servicio" proporciona información sobre herramientas, que aparece al pasar el cursor sobre el sitio. Con la ayuda de la información sobre herramientas, el operador del Centro de seguridad puede obtener rápidamente la información requerida sobre el sitio, a saber: número, nombre y dirección del sitio, estado del sitio o sus secciones (bajo protección o sin protección) e información. sobre la primera y la última alarma en caso de una condición de alarma en el sitio.

1.4 Confirmaciones de video

Para reducir la probabilidad de respuesta a una falsa alarma, así como para coordinar las acciones de los guardias en el sitio, el operador puede ver video en vivo de las cámaras en el sitio durante el manejo de la alarma. Para hacer esto, un *enrutador de video* se instalará en el sitio. Es un dispositivo especial que puede transmitir video desde las cámaras conectadas al software Security Center.

Consulte la información sobre cómo agregar un enrutador de video instalado en el sitio a la tarjeta del sitio en el capítulo sobre la descripción del módulo [“Administrador del sitio”] (# site-manager-videorouter) para obtener información sobre cómo agregar un enrutador de video instalado en el sitio a la tarjeta del sitio.

En el capítulo sobre el módulo [“Operador de servicio”] (# duty-opertor-process-alarm), también se dice cómo el operador puede ver video en vivo desde el sitio durante el manejo de la alarma.

1.5 Servicios en la nube

Algunas características nuevas del software Security Center de la versión 5 se implementan como servicios en la nube: "Interfaz de programación remota", Aplicación móvil "MyAlarm", etc. A continuación se ofrece una breve descripción de las características de estos servicios y más detalles sobre cómo trabajar con se pueden encontrar en el capítulo "Servicios en la nube”.

1.5.1 Interfaz de programación remota

El servicio “Interfaz de programación remota” está destinado al control remoto de los equipos instalados en el sitio.

Para garantizar el acceso remoto en el sitio, se instalará el panel de control de C.Nord o PIMA Electronic Systems Ltd., y se utilizará el transmisor GSM “TR-100 GSM III” como comunicador.

Para acceder al servicio "Interfaz de programación remota", es necesario Registrarse el ingeniero en la "Nube", y también le da acceso a Manejo de sitio .

1.5.2 Aplicación móvil "MyAlarm"

La aplicación “MyAlarm” está destinada a clientes de empresas de seguridad privada. Con su ayuda, es posible acceder a la tarjeta del sitio, información sobre su estado y también la lista de personas responsables.

La aplicación se instalará en un dispositivo móvil (teléfono inteligente o tableta). Se puede utilizar Android o iOS como sistema operativo del dispositivo móvil.

La característica clave de la aplicación “MyAlarm” es la capacidad de proteger el sitio o quitarlo de la protección directamente desde la aplicación. Para ello se instalará el panel de control de C.Nord o PIMA Electronic Systems Ltd. y se utilizará como comunicador el transmisor GSM “TR-100 GSM III”. El usuario de la aplicación deberá ingresar el código de usuario que ingresa en el teclado del panel de control, este código se traduce al panel de control, luego de que el evento de tomar o quitar se transfiere a la aplicación “MyAlarm”. Debido a que los eventos en la aplicación “MyAlarm” se transmiten desde el Centro de Seguridad, luego de la toma bajo protección no es necesario monitorear el paso de la señal a una empresa de seguridad privada.

La capacidad de ver el registro de eventos del sitio es una característica importante de la aplicación "MyAlarm". Además, el registro de eventos de la aplicación “MyAlarm” muestra las acciones que realiza el operador del Centro de Seguridad durante el manejo de alarmas.

El operador del Centro de seguridad puede especificar qué eventos y acciones del operador se mostrarán en el registro de eventos de la aplicación "MyAlarm".

Cabe señalar que si se instala un enrutador de video en el sitio, además de las con fi rmaciones de video en el registro de eventos, es posible ver video en vivo de las cámaras instaladas en el sitio en la aplicación “MyAlarm”. La calidad de la transmisión de video depende del ancho de banda del canal de comunicación, que se utiliza para el acceso a Internet desde el dispositivo móvil.

Es necesario especificar el mismo nombre de usuario y contraseña, que se utilizan para acceder a los servicios de "Cuenta personal", para la autorización en la aplicación "MyAlarm".

1.5.3 Control de acceso al sitio desde la aplicación "MyAlarm"

La versión 5.3 del Centro de seguridad solo tenía una forma de otorgar acceso al sitio a la persona responsable desde la aplicación "MyAlarm": asignar a la persona responsable como administrador de la cuenta personal.

En la versión 5.4 del Security Center, apareció una nueva oportunidad: dar acceso a las personas responsables especi fi cadas en la tarjeta del sitio. Puede encontrar más información sobre cómo hacer esto en unartículo separado.

1.5.4 Permisos del operador durante el manejo de alarmas

En la versión 5.2.855, se han agregado nuevos permisos de operador relacionados con el manejo de alarmas en el módulo "Operador de servicio".

Suponga que los operadores de servicio en el receptor se dividen en dos grupos.

La tarea del primer grupo es tomar una decisión sobre si la respuesta requiere una respuesta (llamada de guardia) o no. Estos operadores deberán poder iniciar el manejo de la alarma inmediatamente, una vez recibida. Monitorizan los eventos desde el sitio, llaman a los responsables, etc. Y en algún momento deciden cancelar la alarma o reaccionar. Si se decide reaccionar, el operador registra la con fi rmación de la alarma.

Una vez confirmada la alarma, los operadores del segundo grupo, cuya tarea es la respuesta, comienzan su trabajo. Ellos “no ven” aquellas alarmas que no están con fi rmadas: el evento no aparece en la lista de “Alarmas”, no hay sonido de alarma, el sitio no se convierte en alarma. Todo esto ocurre solo en el momento en que se con fi rma la alarma: la alarma se vuelve “real”, los operadores que reaccionan la ven como si acabara de ser recibida y comienzan a reaccionar.

Con fi rmar alarmas Para que el operador del primer grupo con fi rme la alarma y la transmita a los operadores del segundo grupo, deberá tener el permiso “Con fi rmar alarmas”.

Administrar guardia Si el operador tiene permiso para "Administrar guardia", entonces tiene la oportunidad de registrar acciones con el tipo de "Llamada de guardia", "Llegada de guardia" y "Cancelar llamada de guardia".

Si los operadores del primer grupo no controlan realmente a Guard, no tendrán este permiso. Si el operador no tiene permiso para administrar la Guardia, las acciones de control de la Guardia no aparecen en la lista de posibles acciones para la alarma.

Los operadores del segundo grupo, por el contrario, tendrán dicho permiso.

Dado que se trata de un nuevo permiso, al actualizar a la versión 5.2.855, todos los operadores del Centro de seguridad que tenían permiso para procesar alarmas lo recibirán.

Procesar solo alarmas con fi rmadas / Cancelar solo alarmas con fi rmadas Estos son permisos para los operadores del segundo grupo. Si el operador tiene permisos solo para manejar alarmas con fi rmadas, él / ella “verá” la alarma solo después de que haya sido con fi rmada.

2. Introducción

El software Security Center fue desarrollado por la empresa científica y técnica C.Nord para su funcionamiento en el complejo sistema de transmisión de notificaciones “Andromeda”. El software Security Center está diseñado para los sistemas operativos Microsoft Windows 7/10. Se recomienda ejecutar el software Security Center en el sistema operativo Microsoft Windows Server 2008/2012.

Es necesario tener en cuenta las siguientes características del software Security Center:

- El software Security Center consta de partes funcionales independientes (módulos), cada una de las cuales está destinada a resolver un problema específico. Por un lado, permite proteger al máximo cada módulo frente a un posible fallo del otro, y por otro lado, permite instalar cada módulo en un ordenador independiente de la red.
- El software Security Center está orientado al funcionamiento en una red que admita el protocolo TCP / IP. Por lo tanto, los cambios realizados en el sistema en cualquier computadora de la red se aplican inmediatamente a todos los módulos de software que se ejecutan en esa red.

- Los derechos del operador en el software Security Center se definen en relación con una acción específica en un módulo de software específico. Así, los niveles de acceso de los operadores se implementan tanto al programa en su conjunto como a sus componentes individuales. Por ejemplo, es posible restringir el acceso del operador a todo el módulo "Administrador del sitio" y solo a la función de edición del programa de armado del sitio.

El equipo receptor de la estación central permite recibir y manejar eventos desde paneles de control (concentradores, unidades de sitio) con comunicadores incorporados (unidades de transmisión de mensajes digitales - módems especializados). Dependiendo del tipo de panel de control, sus capacidades funcionales y de servicio, es posible obtener de él alguna información sobre el estado del sitio. La mayoría de los paneles de control pueden transmitir una amplia gama de información. Por ejemplo, datos sobre el usuario que realizó el armado o desarmado; lugar (número de zona) de alarma o avería (rotura, cortocircuito); armado parcial con indicación de zonas no vigiladas y mucho más. Debido a esto, el operador de servicio tiene la información más completa sobre el estado del sitio (armado, desarmado, alarmado, etc.) y la condición técnica del equipo (batería baja, no 220V, línea telefónica defectuosa, etc.).

2.1 Requisitos de hardware para el sistema

Con fi guración mínima: Procesador Intel Core i3 2.6 GHz, RAM 2Gb, monitor SVGA de 17 ”, tarjeta de sonido, puerto USB para instalar llave electrónica de seguridad.

Configuración recomendada: Procesador Intel Core i5 3.0 GHz, RAM 4Gb, monitor SVGA de 19 ”, tarjeta de sonido y tarjeta de red para operar software en la red, puerto USB para instalar llave de seguridad electrónica.

2.2 Requisitos del sistema operativo

Se admiten los siguientes sistemas operativos:

- Microsoft Windows XP / Vista / 7/8/10 Microsoft Windows
- Server 2003/2008/2012/2016

El software Security Center, versión 5, está diseñado para funcionar en versiones de 32 y 64 bits de los sistemas operativos enumerados.

Antes de instalar Security Center, se recomienda verificar que el último paquete de actualización ofrecido por Microsoft esté instalado en el sistema operativo.

2.3 Llave de seguridad electrónica

El software Security Center está protegido contra copias ilegales mediante la clave de seguridad electrónica. Antes de usar Security Center, es necesario conectar la llave electrónica al puerto USB de la computadora e instalar su controlador.

2.4 Volumen de suministro

El software Security Center se entrega en el siguiente paquete:

- Disco compacto que contiene lo siguiente:
    - Paquete de distribución de la versión completa de Security Center destinado a su instalación en un equipo nuevo donde el software no estaba previamente instalado.
    - Paquete de actualización de distribución de Security Center destinado a actualizar el software Security Center ya instalado (o "Andromeda 2.8") a la versión 5 de Security Center.
    - Paquete de distribución de drivers para la llave electrónica de seguridad.
- Llave de seguridad electrónica para insertar en el puerto USB del ordenador.

3 Instalación

3.1 Selección del sistema operativo

Se recomienda ejecutar el software Security Center en el sistema operativo Microsoft Windows 10.

Si tiene la intención de utilizar el software Security Center en la red, es preferible instalar la parte del servidor del software Security Center (instalación completa) en una computadora con sistema operativo Microsoft Windows Server 2016.

Es mejor utilizar NTFS como sistema de archivos.

Se recomienda encarecidamente que actualice el sistema operativo actual instalando los últimos paquetes de servicio proporcionados por Microsoft.

3.2 Configuración del subsistema de disco de la computadora

Para asegurar un almacenamiento confiable de información y mejorar el rendimiento del sistema, se recomienda instalar dos discos duros en la computadora, en los cuales se instalará el software Security Center por completo. En este caso, instale el sistema operativo y los archivos ejecutables de Security Center en un disco duro y el directorio de la base de datos en el otro. Si es imposible instalar dos discos duros, se recomienda dividir el disco duro único en dos particiones e instalar el sistema operativo en una de ellas y la base de datos del Centro de seguridad en la otra.

Además, independientemente de la configuración del subsistema de disco, deberá configurar la copia de seguridad para la base de datos del software Security Center de modo que la copia de seguridad se cree en un disco duro adicional o en un recurso de red, que es un dispositivo de almacenamiento físicamente diferente.

3.3 Requisitos adicionales

Antes de instalar el software Security Center, debe asegurarse de que el software Andromeda Liberty o el software Andromeda anterior a la versión 2.8 no esté instalado en la computadora. Si se detecta uno de estos programas, elimínelo antes de instalar el software Security Center.

Para instalar Security Center, debe instalar Microsoft Internet Explorer 8.0 o superior. También se recomienda que el sistema tenga los siguientes componentes y programas:

- Para los sistemas operativos Microsoft Windows XP, Microsoft Windows Server 2003 y Microsoft Windows Server 2008:
  - Windows Installer 4.5 o posterior
  - Microsoft .NET Framework 3.5 SP1
- Componentes de acceso a datos de Microsoft (MDAC) 2.8 o superior
- Microsoft .NET Framework 2.0

Antes de instalar Security Center, debe asegurarse de que se cumplan todos los requisitos de hardware y del sistema operativo.

> Si se planea utilizar Security Center con enrutadores de video de la empresa C.Nord, entonces es necesario instalar la última versión de Adobe Flash Player en la computadora donde desea ejecutar el módulo “Operador de servicio”, que se puede cargar desde el sitio web oficial de Adobe.

3.4 Instalador

Al instalar el software Security Center, debe especificar valores para varias opciones de instalación. Inmediatamente después de que se inicie el instalador, debe especificar el idioma de la interfaz de usuario del instalador.

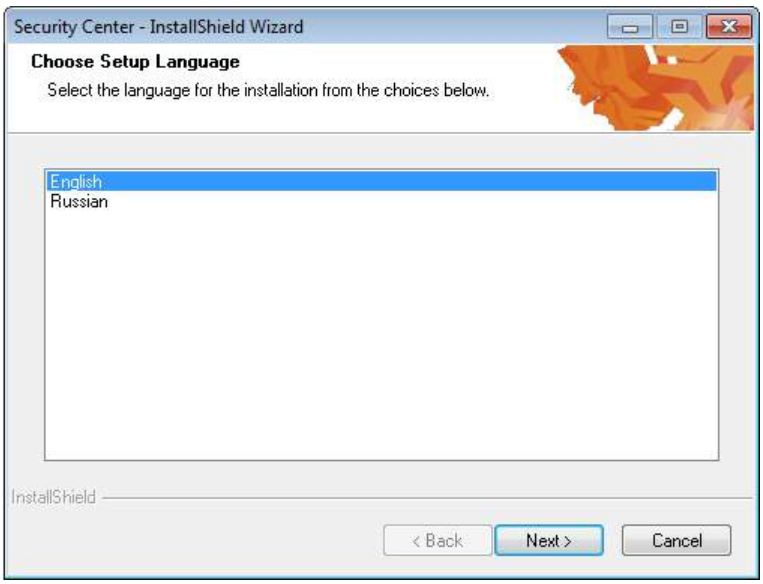


Figura 1: Selección del idioma del instalador

Después de eso, deberá seleccionar el idioma de la interfaz de usuario de Security Center de la siguiente lista:

- inglés
- ruso
- Español

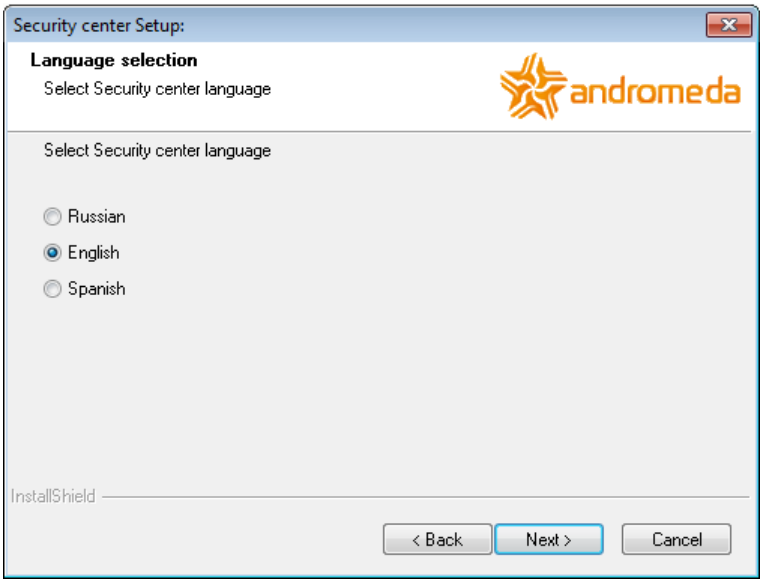


Figura 2: Selección del idioma del Centro de seguridad

Tenga cuidado: el idioma de la interfaz de usuario de Security Center no se puede cambiar después de la instalación. Si se comete un error al seleccionar el idioma de la interfaz de usuario, para corregirlo, deberá eliminar el Centro de seguridad y volver a instalarlo.

A continuación, el instalador le pedirá que especifique el directorio donde se ubicarán los archivos ejecutables del Centro de seguridad.

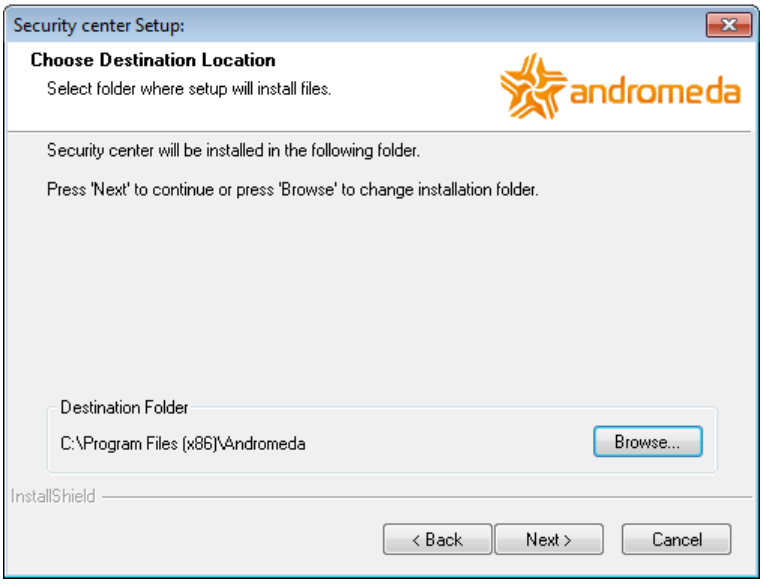


Figura 3: Seleccionar carpeta de instalación

Después de eso, deberá seleccionar el tipo de estación de trabajo en la que está instalando:

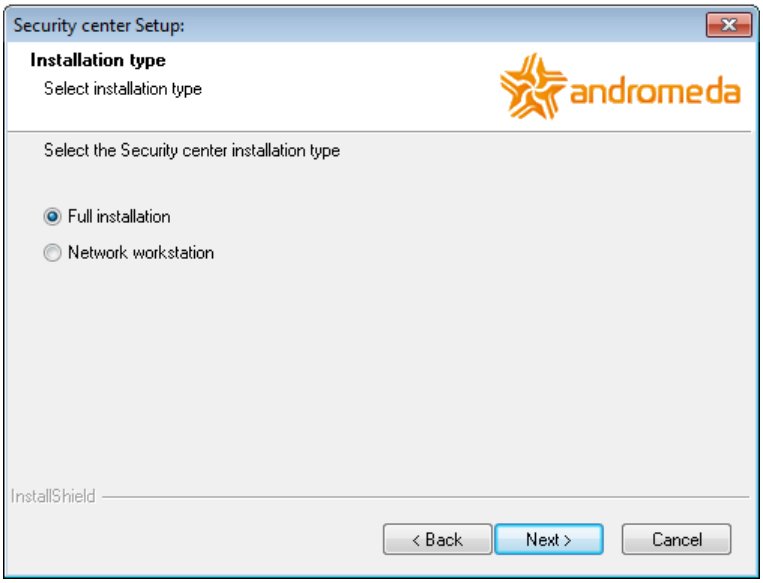


Figura 4: Selección del tipo de instalación

- Seleccione *Instalación completa* si la computadora actuará como servidor: almacenará la base de datos del Centro de seguridad y recibirá eventos.

  Seleccione la instalación completa si es la única computadora en la que se utilizará Security Center.

  En caso de instalación completa, la base de datos de Microsoft SQL Server y Security Center se instalará en la computadora. Además, se instalará en la computadora el módulo “Administrador de eventos” para recibir y procesar las notificaciones.

- Seleccione la instalación en *Estación de trabajo en red* si es necesario organizar un lugar de trabajo en la red informática local. Casi todas las funciones del programa están disponibles para el operador en la estación de trabajo de la red. Un ex

La opción es una serie de operaciones de servicio, como cambiar la configuración del módulo "Administrador de eventos" y la gestión de copias de seguridad.

Al realizar la instalación en una estación de trabajo en red, deberá especificar la computadora en la que se instaló previamente la versión completa.

3.4.1 Instalación completa

Al instalar la versión completa, deberá especificar el directorio en el que se almacenará la base de datos de Security Center.

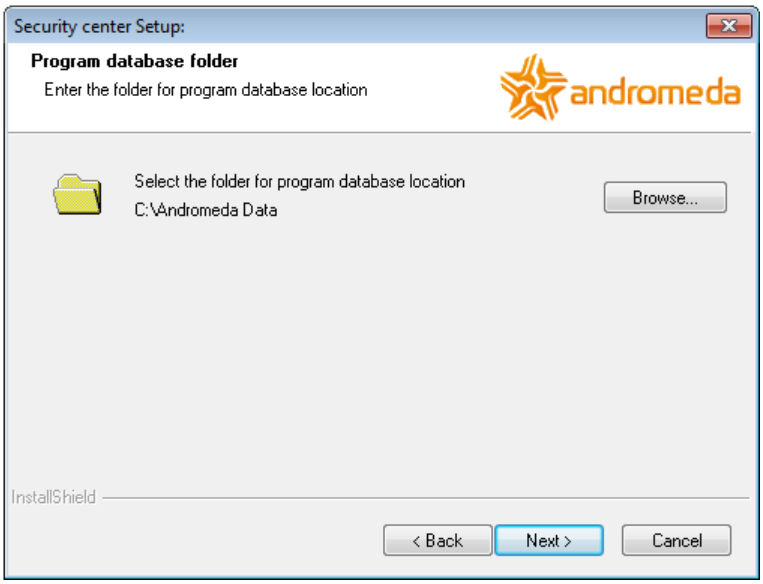


Figura 5: Instalación completa: selección de la carpeta de instalación de la base de datos

Para aumentar el rendimiento de Security Center, se recomienda colocar los archivos de la base de datos en un disco duro separado o al menos en una partición de disco duro separada. De forma predeterminada, el instalador le solicita que instale los archivos de la base de datos en una partición de disco que no sea la del sistema.

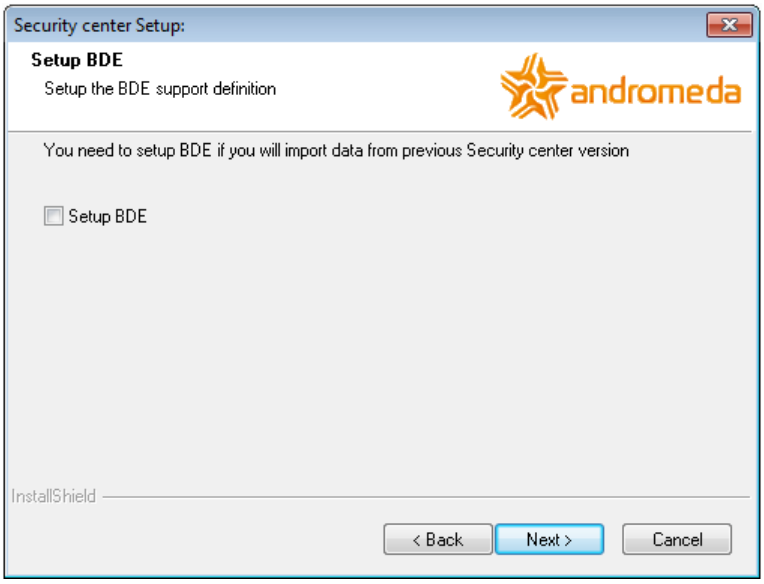


Figura 6: Instalación completa: seleccionando la configuración de BDE

También debe especificar la necesidad de configuración de BDE. El subsistema BDE ("Borland Database Engine") fue utilizado por Andromeda 1.0 - 2.76, así como por Andromeda Liberty para el acceso a la base de datos. Security Center utiliza el subsistema BDE solo al importar datos de las bases de datos de los programas enumerados. Si no necesita importar información de las bases de datos de Andromeda 2.6 - 2.76 o Andromeda Liberty, no es necesario instalar el subsistema BDE.

En caso de instalación completa, aparecerá una instancia con nombre de Microsoft SQL Server 2005 Express Edition en la computadora. El nombre de la instancia es "ANDROMEDA". Para realizar la instalación completa, la computadora no debe tener una instancia de Microsoft SQL Server con el mismo nombre.

Antes de que el instalador comience a instalar SQL Server 2005 y a copiar los archivos del Centro de seguridad en la computadora, puede ver su configuración para asegurarse de que todos los valores de todos los parámetros estén configurados correctamente.

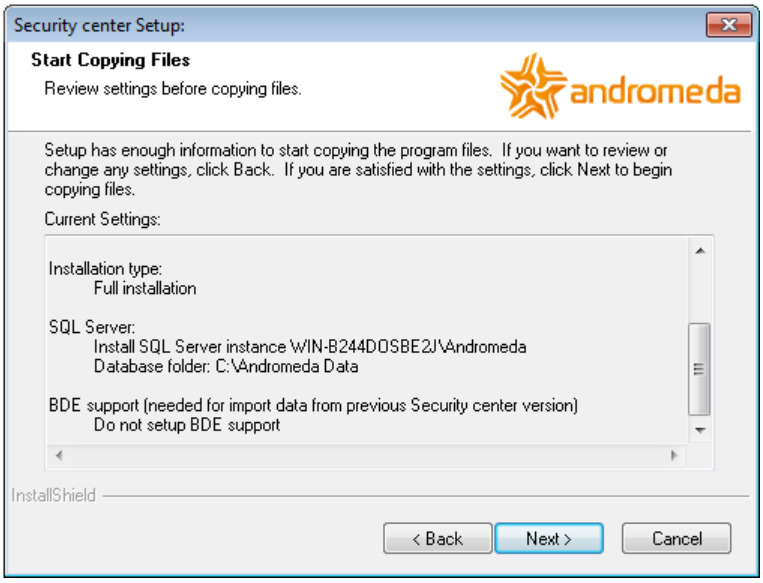


Figura 7: Instalación completa: lista de configuraciones del programa de instalación

3.4.2 Instalación en una estación de trabajo en red

Al instalar Security Center en una estación de trabajo de red, debe especificar una instancia de Microsoft SQL Server que se utiliza para almacenar la base de datos.

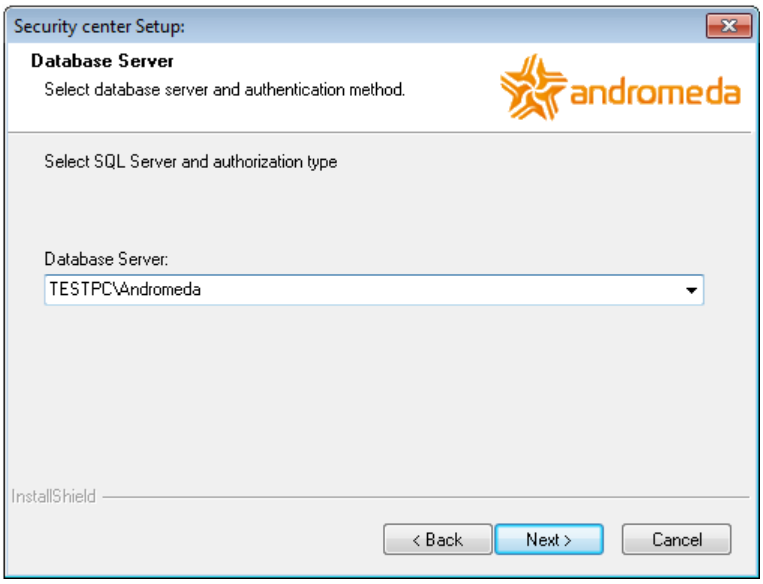


Figura 8: Instalación en la estación de trabajo de la red: selección del servidor SQL

Se instala una instancia de Microsoft SQL Server cuando se realiza una instalación completa de Security Center. El nombre de la instancia es "ANDROMEDA". Por lo tanto, debe seleccionar una línea del formulario "nombre del computador|ANDRÓMEDA"En la lista, donde nombre del computador es el nombre del equipo en el que se realizó la instalación completa de Security Center.

Si el instalador no puede encontrar la instancia de Microsoft SQL Server en la red local que se utiliza para almacenar la base de datos de Security Center, se recomienda especificar el nombre de la computadora y el nombre de la instancia manualmente.

Después de esto, debe ingresar el nombre o la dirección IP de la computadora en la que se inicia el módulo "Administrador de eventos". En la mayoría de los casos, esta es la misma computadora que se usa como servidor de Security Center.

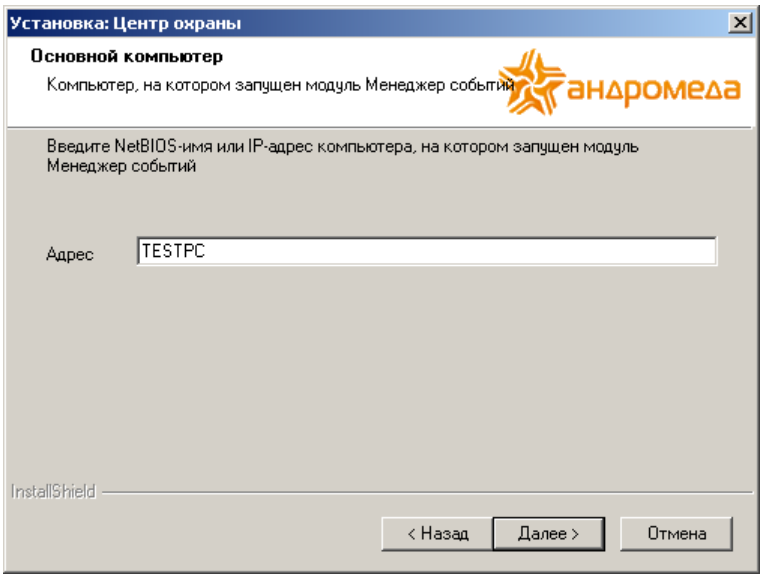


Figura 9: Instalación en la estación de trabajo en red: selección de la computadora con el módulo "Administrador de eventos"

La comunicación con el módulo “Administrador de eventos” es necesaria para que los módulos restantes de Security Center intercambien información y sincronicen acciones.

Antes de que el instalador comience a copiar los archivos en la computadora, puede ver su configuración para asegurarse de que todos los valores de todos los parámetros estén configurados correctamente.

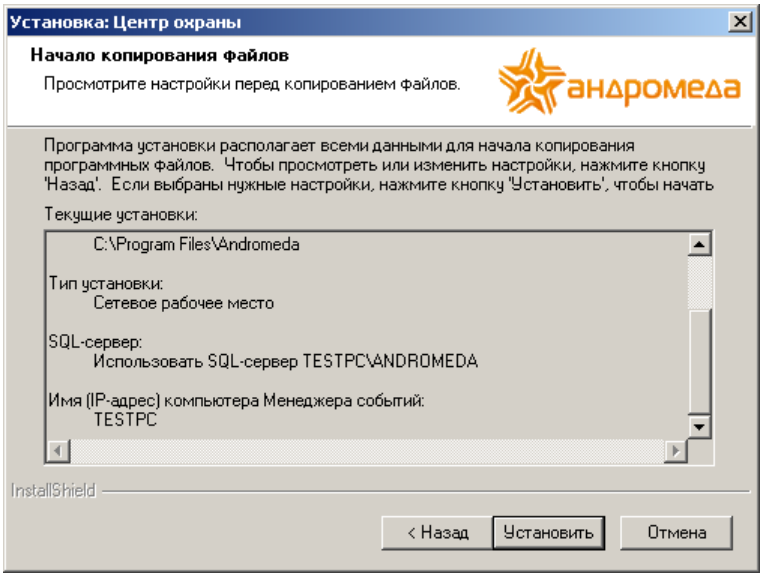


Figura 10: Instalación en una estación de trabajo en red: lista de configuraciones del instalador

3.5 Eliminación del centro de seguridad

Para desinstalar Security Center, deberá utilizar el elemento correspondiente en el Panel de control de Windows.

3.6 Problemas de instalación

Si hay algún problema con la instalación de Security Center, comuníquese con el servicio de soporte técnico de C.Nord por correo electrónico Soporte@cygnus.la

Cuando se comunique con el soporte técnico, especifique la versión de Security Center que se está instalando y describa el problema. En caso de solicitud por correo electrónico, se recomienda adjuntar el archivo que contiene los siguientes archivos:

- archivo C: |Andromeda_Install.log - Este archivo contiene el registro del instalador de Security Center
- archivos de la carpeta C: |Registro de Andrómeda - Los archivos contienen los registros de los módulos del Centro de seguridad.
- archivos de la carpeta C: |Archivos de programa |Microsoft SQL Server |90 |Configurar Bootstrap |INICIAR SESIÓN - Los archivos de este carpeta y sus subcarpetas contienen los registros del instalador de instalación de Microsoft SQL Server

Los archivos enumerados no contienen datos personales ni información confidencial.

4 Primeros pasos

4.1 Variantes del centro de seguridad

Las variantes del software Security Center difieren en el número máximo posible de sitios atendidos: 1000, 1500, 2000, etc.

No hay restricciones en el uso de fuentes de eventos, y las fuentes de eventos de paneles de monitoreo centralizados de terceros se comprarán por separado.

La variante inicial de Security Center es gratuita y permite proteger hasta 1000 sitios.

4.2 Propósito de los módulos

El software Security Center consta de módulos, cada uno de los cuales está destinado a resolver problemas específicos.

La "Administrador de eventoEl módulo ”está diseñado para recibir notificaciones del equipo receptor de la estación central, así como directamente de ciertos tipos de equipos del sitio, por ejemplo, a través de canales de comunicación GPRS y Ethernet.

Además, es en el módulo “Event manager” donde los eventos se manejan automáticamente: se monitorean las cadenas de eventos, se envían mensajes SMS y los eventos se transmiten a otros sistemas. Cabe señalar que el “Event Manager” es el enlace para todos los demás módulos de Security Center: primero se lanzará, porque es con su ayuda que los módulos intercambian información sobre nuevos eventos, acciones de los operadores y otros cambios ocurridos. durante el funcionamiento del módulo.

La "Administrador del sitioEl módulo ”se utiliza para la creación de nuevos sitios y cambiar la descripción de los sitios existentes.

La "Operador de servicioEl módulo ”es utilizado por el operador para manejar eventos. Las principales funciones del módulo son el monitoreo del estado operativo del sitio, la visualización de los últimos eventos recibidos, el registro de las acciones del operador para el manejo de la alarma recibida desde los sitios.

La "Mapas del sitioEl módulo ”está destinado a la creación de esquemas de acceso al sitio, planos de planta y ubicación de las coberturas de protección. Además, el módulo "Mapas del sitio" se utiliza para mostrar las zonas de alarma del sitio en el plano del piso durante el manejo de la alarma.

El listado de operadores de Security Center, así como sus derechos en cada uno de los módulos se configuran en el cuadro “ Gerente de personal”. En el mismo módulo, es posible cambiar la lista de guardias, así como la lista de computadoras en la red local en las que se operan las estaciones de trabajo de la red de Security Center.

La "Asistente de base de datos”Está diseñado para las siguientes operaciones:

- comprobación de la base de datos y recuperación de errores
- copia de seguridad de la base de datos
- restauración de la base de datos desde una copia de seguridad
- importación de datos de la base de datos del software "Andromeda", del software "Andromeda Liberty", del software "Strazh" y Software "CSM32"
- exportación de datos de la base de datos de Security Center para su uso en otros programas

En el Configuración del sistema módulo, es posible cambiar los directorios que se utilizan para describir los sitios: lista de plantillas de eventos, clases de eventos y acciones asociadas, tipos de sitios y lista de características adicionales.

4.3 Primer inicio

Para comenzar, es necesario iniciar el módulo “Administrador de eventos” y configurar las fuentes de eventos, componentes especiales del módulo, destinados a recibir eventos del equipo de la estación central.

Las fuentes de eventos se configuran en la ventana "Fuentes de eventos". Para acceder a él, seleccione “Fuentes de eventos. . . ”En el módulo“ Administrador de eventos ”(haga clic con el botón derecho en el icono en la bandeja del sistema de la barra de tareas).

Si Security Center se instala solo para familiarizarse, entonces para crear eventos desde sitios es posible usar la “Emulación de eventos. . . ”En el menú“ Administrador de eventos ”.

Una vez iniciado el módulo "Administrador de eventos", es posible comenzar a trabajar con otros módulos. Los sitios se ingresan al sistema con la ayuda del módulo "Administrador del sitio", y los eventos recibidos se monitorean y las alarmas se manejan con la ayuda del módulo "Operador de servicio".

4.4 Contraseña de administrador

Inmediatamente después de la instalación del software Security Center, solo un operador está presente en la lista de operadores: “Administrador”. La contraseña del operador "Administrador" por defecto es222222.

4.5 Importación de datos

El software Security Center implementa la función de importar información sobre sitios desde bases de datos de los siguientes programas:

- «Andrómeda» versiones 2.0 - 2.76
- «Tsentavr»
- «PCN6»
- «GuardNet»
- «Strazh»
- «CSM32»
- «Neman»
- «Mirazh»
- «Importar desde XML»

Si antes de la instalación de Security Center se utilizó el software de la lista anterior, entonces, para una transición cómoda a Security Center, es posible importar las descripciones de los sitios de la base de datos de estos programas.

Si se pretende importar datos del software "Andromeda" versión 2.0 - 2.76 o "Andromeda Liberty", entonces al instalar Security Center, es necesario especificar la necesidad de instalar BDE, el subsistema utilizado para acceder a los datos de estos programas. .

La importación de datos se realiza con la ayuda del módulo "Asistente de base de datos". En el caso de importar desde las versiones 2.0 - 2.76 del software “Andromeda” o “Andromeda Liberty”, se requerirán todos los archivos de la carpeta de la base de datos para ejecutarlo. Si hay una copia de seguridad de la base de datos en formato ZIP, es necesario extraer los archivos del archivo a cualquier carpeta del disco duro de la computadora.

5 Administrador de eventos

El módulo “Administrador de eventos” está destinado a recibir notificaciones del equipo receptor de la estación central, así como directamente de ciertos tipos de equipos del sitio, por ejemplo, vía GSM (CSD / GPRS) y canales de comunicación Ethernet.

Los eventos, que constituyen la base del software Security Center, son el resultado del manejo de las notificaciones recibidas por el módulo “Administrador de eventos”.

Los eventos se manejan automáticamente en el módulo “Administrador de eventos”: se monitorean las cadenas de eventos, se envían mensajes SMS y los eventos se transmiten a otros sistemas. Además, el “Event Manager” es el enlace para todos los demás módulos de Security Center: primero se lanzará, porque es con su ayuda que los módulos intercambian información sobre nuevos eventos, acciones de los operadores y otros cambios que ocurrieron durante el módulo. operación.

Una vez iniciado el módulo, aparece un icono en la bandeja del sistema de la barra de tareas de Windows, informándole del funcionamiento del módulo. Después de la recepción de eventos, el color del ícono cambia y cuando pasa el mouse sobre él, aparece información sobre la hora del último evento y el número total de eventos desde que se inició el módulo.

Si hace clic con el botón derecho del ratón en el icono del módulo, aparecerá un menú desplegable.

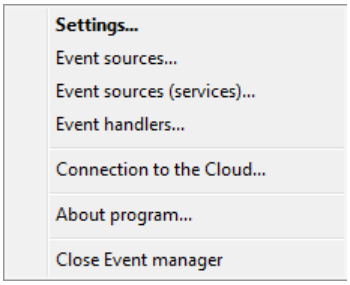


Figura 11: Menú desplegable del módulo "Administrador de eventos"

5.1 Configuración del módulo

Para acceder a la configuración, seleccione la opción “Configuración. . . ”En el menú desplegable del módulo.

Para acceder a la ventana "Configuración" y guardar los cambios realizados en ella, el usuario deberá tener permiso para "Cambiar configuración" para el módulo "Administrador de eventos".

5.1.1 Común

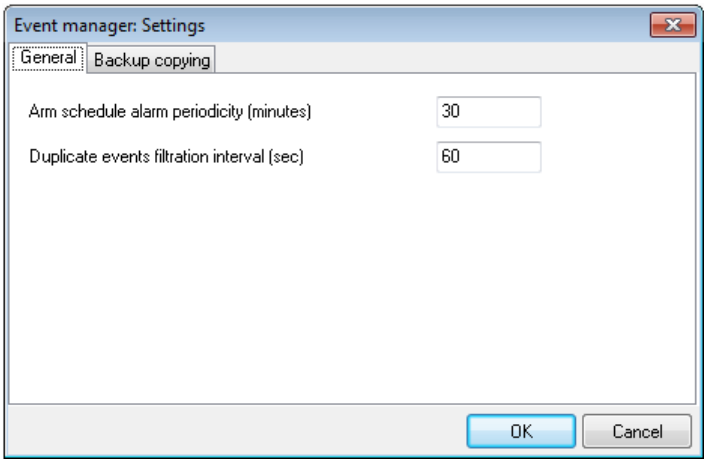


Figura 12: Ventana "Configuración", pestaña "Común"

El parámetro “Periodicidad de alarma de programación de armado” especifica el intervalo para generar eventos del sistema con los códigos ZZXB y ZZXC. Los eventos del sistema con estos códigos se crean cuando se viola el programa de armado diario del sitio y se viola el programa de armado a largo plazo del sitio, respectivamente. El horario de armado y el horario de armado a largo plazo del sitio se establecen individualmente para cada sitio en el módulo "Administrador del sitio".

El parámetro “Intervalo de filtración de eventos duplicados” especifica el intervalo durante el cual el segundo y los siguientes eventos idénticos recibidos a través de diferentes canales de comunicación se considerarán duplicados. Los eventos duplicados se manejan en los módulos de Security Center de una manera especial. Así, en el módulo “Operador de servicio” no se muestran en la lista general de eventos aceptados. En este caso, es posible habilitar su visualización en la pestaña de eventos del sitio. Además, los eventos duplicados no se incluyen en los informes a menos que se indique específicamente. El valor recomendado para esto El parámetro es de 60 segundos.

5.1.2 Respaldo

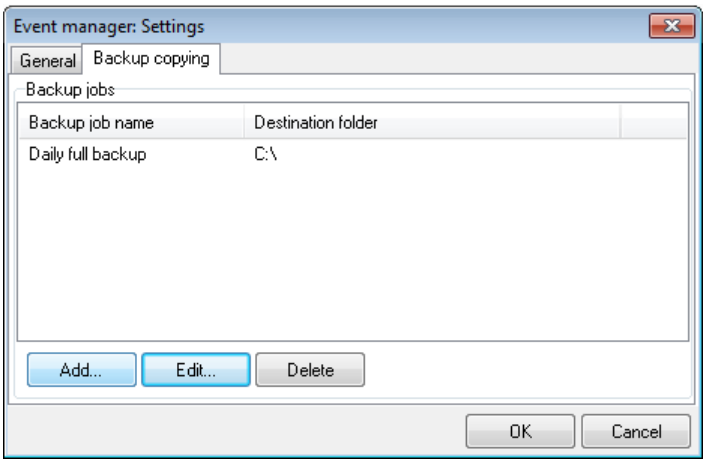


Figura 13: Ventana "Configuración", pestaña "Copia de seguridad"

La pestaña "Copia de seguridad" de la ventana de configuración del "Administrador de eventos" está diseñada para administrar las tareas de copia de seguridad.

Utilice la opción "Agregar. . . ”Para crear un nuevo trabajo de copia de seguridad y el botón“ Cambiar. . . ”Y los botones“ Eliminar ”para cambiar la configuración del trabajo existente o eliminarlo.

Al crear una nueva tarea de respaldo o cambiar una tarea de respaldo existente, es posible de fi nir los parámetros de la tarea en la ventana "Tarea de respaldo".

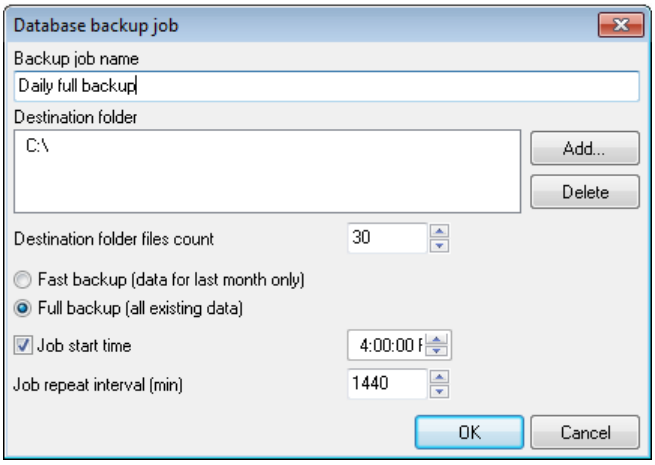


Figura 14: Ventana "Trabajo de copia de seguridad"

El parámetro "Nombre del trabajo" permite especificar un nombre para el trabajo de respaldo para distinguir un trabajo de otro en la lista.

Utilice el parámetro “Carpeta de destino” para de fi nir una o más carpetas en las que se copiará la copia de seguridad de la base de datos una vez creada. En este caso, se supervisará el número de archivos de la copia de seguridad de la base de datos de Security Center en cada carpeta de destino. Si el número de archivos de copia de seguridad es mayor que el número de archivos de la carpeta de destino, establecido por “Recuento de archivos de la carpeta de destino” al crear una copia de seguridad, se eliminará el archivo de copia de seguridad más antiguo.

Hay dos tipos de copias de seguridad de la base de datos de Security Center: rápida y completa.

- *Completo* La copia de la base de datos contiene toda la información almacenada en la base de datos en el momento de la copia, incluidos los eventos recibidos, las acciones del operador y los mensajes SMS enviados durante todo el período de funcionamiento del software.
- La cantidad de datos en el *rápido* La copia es mucho más pequeña: almacena eventos, acciones del operador y mensajes SMS solo del último mes.

En general, se recomienda utilizar copias rápidas para trabajos de respaldo. En cuanto a las copias de seguridad completas de la base de datos, se recomienda que se realicen manualmente o mediante las tareas del Programador de Windows. Consulte más información sobre cómo crear una copia de seguridad de la base de datos utilizando el Programador de Windows en la sección "Asistente de base de datos".

El parámetro “Intervalo de repetición del trabajo” especifica el intervalo para repetir el trabajo de respaldo.

Al marcar la casilla junto a la opción "Hora de inicio de la tarea" y especificar la hora, es posible configurar el inicio de la tarea de copia de seguridad al mismo tiempo. En este caso, si el valor del parámetro "Intervalo de repetición del trabajo" es cero, el trabajo se ejecutará una vez al día. Y si el parámetro "Intervalo de repetición del trabajo" se establece en un valor distinto de cero, se ejecutarán copias de seguridad periódicas todos los días a la misma hora.

Las copias de seguridad de la base de datos del software Security Center se crean mediante el módulo "Asistente de base de datos", incluidas las creadas por los trabajos de copia de seguridad. Para obtener más información sobre cómo realizar una copia de seguridad de la base de datos y realizar la restauración de la base de datos desde una copia de seguridad, consulte la sección "Asistente de base de datos" de esta guía.

5.2 Fuentes de eventos

El propósito principal del módulo "Administrador de eventos" es que recibe notificaciones del equipo receptor de la estación central, así como también directamente de ciertos tipos de equipos del sitio, por ejemplo, a través de canales de comunicación GPRS y Ethernet. Una variedad de métodos y protocolos. para la transmisión de notificaciones se apoya con la ayuda de componentes especiales del módulo "Administrador de eventos", que se denominan "fuentes de eventos".

Para acceder a la configuración de las fuentes de eventos, seleccione “Fuentes de eventos. . . ”En el menú del módulo que aparece después de hacer clic con el botón derecho en el icono del módulo en la bandeja del sistema de la barra de tareas.

Para acceder a la ventana "Fuentes de eventos" y guardar los cambios realizados en ella, el usuario debe tener permiso para "Cambiar configuración" para el módulo "Administrador de eventos".

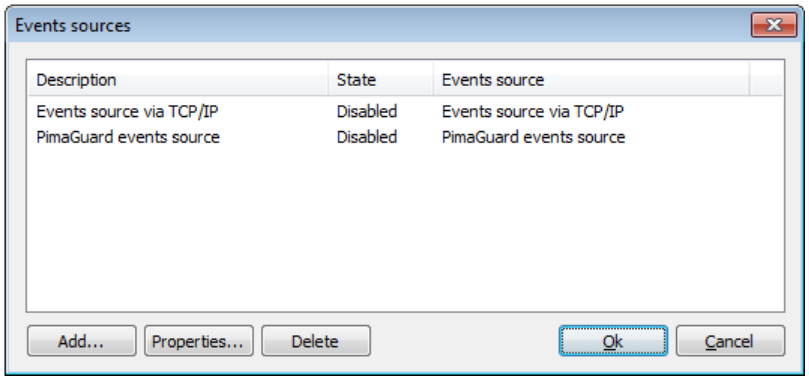


Figura 15: Ventana "Fuentes de eventos"

Haga clic en "Agregar. . . ”Para seleccionar la fuente de eventos deseada de la lista de las instaladas en el sistema.

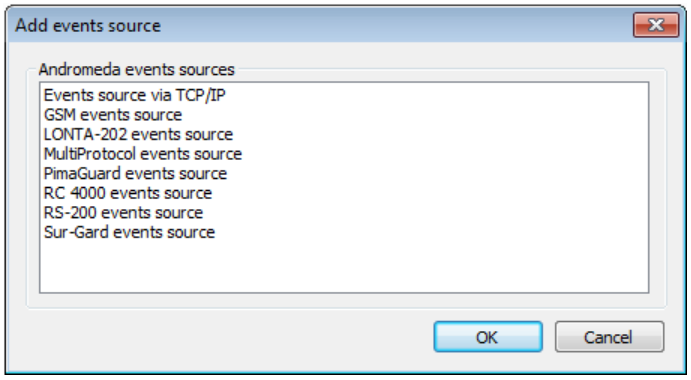


Figura 16: Ventana "Agregar fuente de evento"

Utilice las "Propiedades. . . ”Para cambiar la configuración de la fuente de evento seleccionada.

5.2.1 Configuración de origen de eventos común

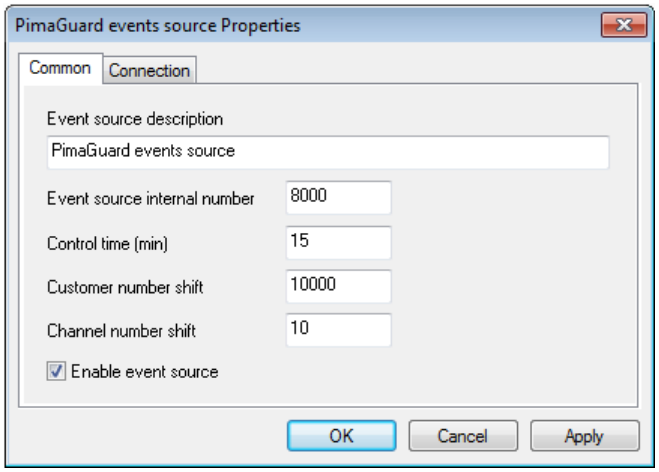


Figura 17: Ventana "Propiedades de la fuente de eventos", pestaña "Común"

Utilizar el Parámetro “Descripción del origen del evento” para especificar el nombre y los parámetros importantes del origen del evento, para en orden verlos en la lista de orígenes del evento utilizados.

El parámetro “Número interno de origen del evento” es necesario para que el Centro de seguridad y el usuario lo identifiquen. Primero, el número de la fuente del evento se usa para determinar desde qué fuente se recibe un evento. En segundo lugar, cuando la fuente del evento informa algo al usuario, el evento creado para este evento tendrá el mismo número de sitio que el número de fuente interna. Es muy recomendable crear sitios en el Centro de seguridad, cuyos números correspondan a los números internos de las fuentes de eventos; esto permitirá monitorear la ocurrencia de errores que ocurren durante la operación de la fuente, así como recibir información de servicio sobre su trabaja.

El parámetro “Tiempo de control” permite monitorear automáticamente el hecho de recibir eventos por parte de la fuente e informar al operador sobre los problemas encontrados durante la recepción. Si, por alguna razón, no se reciben eventos para el intervalo de eventos especificado por este parámetro, se creará un evento del sistema con el código “ZZXH” y el número de sitio correspondiente al número interno de la fuente del evento.

Utilice el parámetro "Cambio de número de cliente" para especificar un número entero positivo que se agregará automáticamente al número de sitio para cada evento aceptado por la fuente del evento. Se recomienda utilizar el cambio de números de sitio si se van a conectar varios paneles de monitoreo central, incluidos diferentes paneles, a una copia del software Security Center. Al establecer diferentes turnos de números de sitios para diferentes fuentes de eventos, es posible evitar el problema de superposición de los mismos números de diferentes sitios operados en diferentes paneles.

Por ejemplo, dos controladores remotos Lonta-202 están conectados al Centro de seguridad. Los rangos de números de sitios que se pueden conectar a los paneles son los mismos, de 1 a 600. Pero si el número de evento cambia igual a 1000 para una fuente de eventos y 2000 para la otra, entonces trabajaremos con los sitios 1001- 1600 para un panel y 2001-2600 para el otro en el Centro de seguridad.

“Cambio de número de canal” es un parámetro que especifica un número entero positivo que se agregará automáticamente al número de canal de recepción. Si el número de cambio de número de canal se establece en cero, los eventos recibidos por la fuente de eventos utilizarán el número de canal transmitido por el equipo receptor de la estación central o el primer número de canal si el equipo no transmite el número de canal. Al configurar diferentes cambios de número de canal para diferentes fuentes de eventos, es posible distinguir las fuentes de eventos (y los paneles conectados) para los eventos recibidos. El cambio de número de canal es especialmente relevante cuando se utilizan varias fuentes de eventos idénticas, ya que los tipos y números de los canales de comunicación utilizados por estas fuentes probablemente serán idénticos.

Es posible habilitar o deshabilitar la fuente de eventos usando el parámetro "Habilitar fuente de eventos". Cabe señalar que si se apaga la fuente del evento, se liberan todos los recursos utilizados por ella.

5.2.2 Fuente de evento de PimaGuard y Sentinel

La fuente de eventos de PimaGuard y Sentinel está diseñada para recibir eventos a través del puerto serie o la red Ethernet desde el software de la siguiente lista:

- “Mcard para MS-DOS”;
- «Pima NetSoft»,transmisores «GSM-200»y comunicadores «Net4Pro»;
- “Receptor IP Pima” (paneles de control “AlarmView” “Guardian”);
- “PimaGuard para Windows” (protocolo “Andromeda”).

Esta es la fuente más actualizada para recibir eventos del equipo de recepción de la estación central Pima, que incluye todas las funciones de la “Fuente de eventos de CMS-420”, que ya no se suministra como parte del Centro de seguridad. Si es necesario soportar las últimas características del equipo receptor de la estación central, así como la gama completa de protocolos y canales para la transmisión de noti fi caciones implementados por el equipo receptor Pima, es necesario utilizar las “Fuentes de eventos de PimaGuard y Sentinel ”.

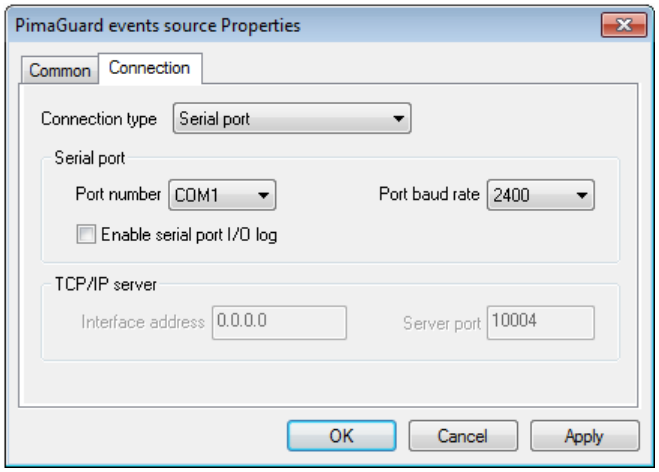


Figura 18: Ventana "Propiedades de fuentes de eventos PimaGuard", pestaña "Conexión", tipo de conexión "Puerto serie"

El parámetro “Método de conexión” especifica el método con el que el equipo receptor se conecta al Centro de seguridad: a través del puerto serie o una red que admita el protocolo TCP / IP.

Si se utiliza un puerto serie, utilice el parámetro "Número de puerto" para seleccionar el puerto serie al que está conectado el equipo receptor de la estación central, y utilice el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio.

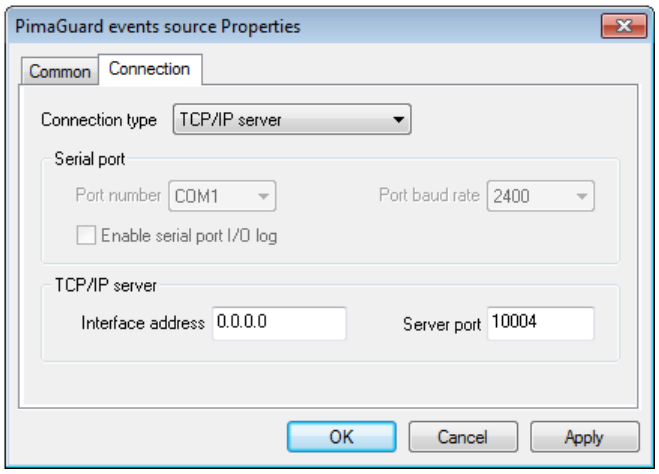


Figura 19: Ventana "Propiedades de fuentes de eventos de PimaGuard", pestaña "Conexión", tipo de conexión "Servidor TCP / IP"

Al conectar el equipo receptor vía Ethernet, se debe recordar que la “Fuente de eventos de PimaGuard y Sentinel” siempre actúa como servidor TCP / IP, es decir, espera las conexiones entrantes. Si varios

Los adaptadores de red están instalados en la computadora, o si un adaptador usa múltiples direcciones IP, use el parámetro “Dirección de interfaz” para especificar la dirección IP donde el origen del evento esperará las conexiones entrantes. El parámetro “Puerto del servidor” está destinado a indicar el puerto al que se conectará el equipo receptor de la estación central.

Al usar la fuente PimaGuard en el modo de recepción de eventos a través de Ethernet, se recomienda usar una instancia separada de la fuente de eventos para cada instancia del software de envío.

5.2.3 Origen del evento a través de TCP / IP

"Evento C.Nord source via TCP / IP ”está destinado a recibir eventos a través de una red compatible con TCP / IP desde los siguientes equipos:

- Transmisores GSM “TR-100 GSM” y “TR-100 GSM II” - vía GPRS
- Botón de pánico "Botón" - a través del canal GPRS
- Repetidor "Tsefei" - a través del canal Ethernet

Si se utiliza esta fuente de eventos, el panel de monitoreo central generalmente requiere una dirección IP dedicada en Internet. Además, se recomienda conectar diferentes tipos de equipos a diferentes instancias de la fuente de eventos, y al conectar el repetidor “Tsefei”, es mejor usar una instancia separada de la fuente de eventos para cada repetidor.

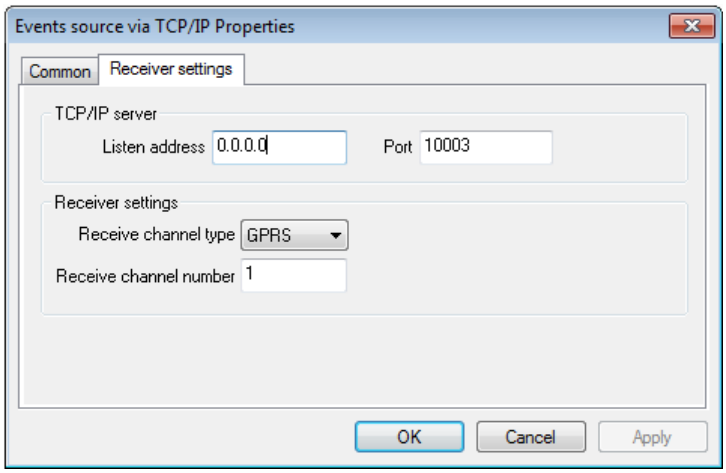


Figura 20: Origen del evento a través de la ventana de propiedades de TCP / IP, pestaña "Configuración del receptor"

El “origen de eventos a través de TCP / IP” siempre actúa como un servidor TCP / IP, es decir, espera las conexiones entrantes. Si hay varios adaptadores de red instalados en la computadora, o si un adaptador usa múltiples direcciones IP, use el parámetro “Dirección de interfaz” para especificar la dirección IP donde el origen del evento esperará las conexiones entrantes. El parámetro "Puerto del servidor" se utiliza para especificar el puerto al que se espera la conexión.

Utilice el parámetro "Tipo de canal de recepción" para especificar explícitamente el tipo de canal de comunicación que se utiliza al transmitir mensajes desde el equipo del sitio.
Por ejemplo, la “Fuente de eventos vía TCP / IP” puede recibir eventos de los transmisores TR-100 GSM a través del canal GPRS y de los repetidores “Tsefei” a través de Ethernet. La fuente del evento no puede identificar el canal de comunicación que se utiliza para la transmisión. Por lo tanto, al configurar esta fuente de eventos, es necesario especificar explícitamente el tipo de canal de comunicación que se utiliza para la transmisión: GPRS si la fuente está destinada a recibir eventos de TP-100GSM, y Ethernet, si la fuente recibe datos del “ Tsefei ”.

El parámetro "Número de canal de recepción" se utiliza para especificar el número que se utilizará para identificar el canal en el que se recibió el evento. El valor del parámetro es especialmente útil si se utilizan varias fuentes de eventos a través de TCP / IP: para distinguir entre las fuentes de las que se recibió el evento, es necesario establecer diferentes números de canal de recepción para ellas.

5.2.4 Fuente de eventos GSM

La “Fuente de Eventos GSM” está destinada a la recepción de eventos a través de los canales GSM SMS y CSD de “Nord GSM”, “Soyuz GSM” y “TR-100 GSM IV”, a través del canal CSD.

Cabe señalar que para utilizar la fuente de eventos GSM, es necesario conectar el módem GSM SonyEricsson GT-47, Siemens MC35 o compatible con ellos mediante el sistema de comando a la computadora.

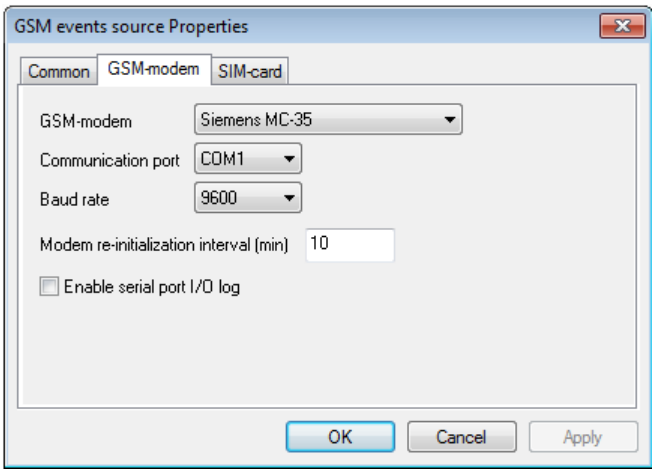


Figura 21: Ventana "Propiedades de la fuente de eventos GSM", pestaña "Módem GSM"

El parámetro “Módem GSM” de fi ne el tipo de módem GSM conectado a la fuente del evento.

Utilice el parámetro "Puerto de comunicación" para seleccionar el puerto serie al que está conectado el módem GSM y el parámetro "Velocidad en baudios" para establecer la tasa de cambio.

El parámetro “Intervalo de reinicialización del módem” permite reinicializar enérgicamente los eventos del módem GSM conectado a la fuente con un intervalo especificado.

Marque la opción “Habilitar registro de E / S del puerto serie” para guardar el protocolo de intercambio de la fuente del evento con el módem GSM en el disco duro. Esta información es útil para averiguar las causas de los problemas al conectarse a un módem GSM o enviar mensajes SMS a través de él. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

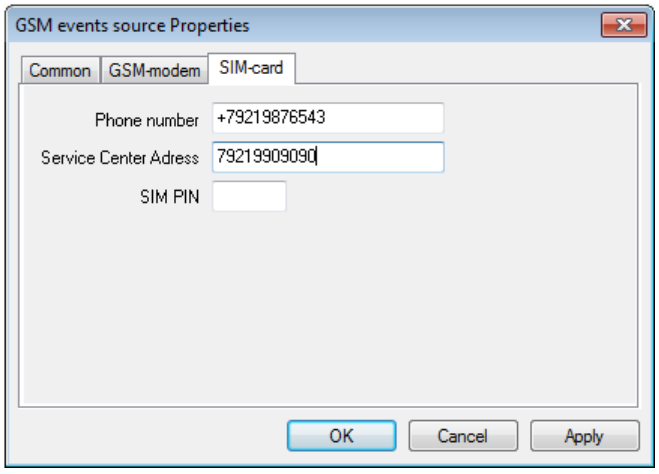


Figura 22: Ventana "Propiedades de la fuente de eventos GSM", pestaña "Tarjeta SIM"

Usando el parámetro "Número de teléfono" para especificar el número de teléfono de la tarjeta SIM instalada en el módem GSM. Este parámetro es necesario para generar comandos para los botones “PT-300” enviados vía SMS.

El parámetro "Dirección del centro de servicio" permite establecer el número de teléfono del centro de SMS del operador de telefonía móvil, cuya tarjeta SIM está instalada en el módem GSM. Algunos operadores de comunicaciones requieren que este parámetro sea

configurar para que la función de envío de mensajes SMS funcione correctamente. El número de teléfono que se utiliza como valor del parámetro "Dirección del centro de servicio" se especificará en formato internacional completo. El símbolo "+" no se utilizará al especificar este número.

Si la tarjeta SIM instalada en el módem GSM está protegida por un código de identificación personal, se puede configurar como el valor del parámetro "PIN de SIM". Se recomienda encarecidamente no utilizar tarjetas SIM protegidas por código PIN para evitar problemas asociados con la pérdida de códigos establecidos.

5.2.5 Fuente de eventos Sur-Gard

Está destinado a recibir eventos a través del puerto serie de los equipos de recepción de las estaciones centrales Sur-Gard fabricadas por DSC hasta System III inclusive. Dado que el formato de transmisión de datos utilizado por las estaciones centrales de Sur-Gard es el estándar de facto, esta fuente de eventos se puede utilizar para recibir eventos de hardware y software de una variedad de proveedores: "Ritm", "Proksima", Jablotron, etc.

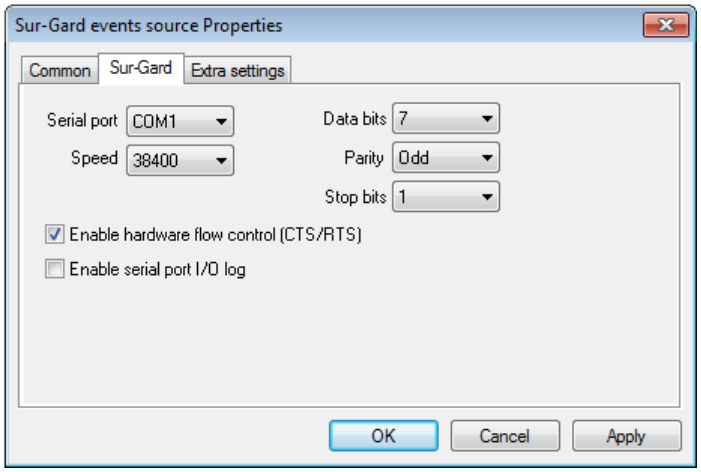


Figura 23: Ventana Propiedades de origen de eventos Sur-Gard, pestaña "Sur-Gard"

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el equipo receptor de la estación central, y utilice el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio. La cantidad de bits de datos en los bytes transmitidos se puede especificar con el parámetro "Bits de datos", la paridad de transmisión se puede especificar con el parámetro "Paridad" y el parámetro "Bits de parada" se utiliza para determinar la cantidad de bits de parada.

Si se utiliza el control por hardware del flujo de datos cuando se comunica a través de un puerto serie, es necesario marcar la casilla "Habilitar el control del flujo por hardware (CTS / RTS)".

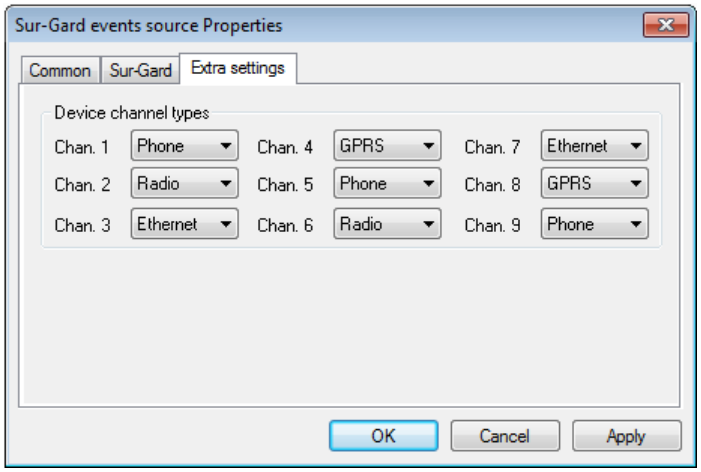


Figura 24: Ventana Propiedades de la fuente de eventos Sur-Gard, pestaña "Configuración adicional"

Utilice la pestaña "Configuración adicional" para especificar los tipos de canales de comunicación que utiliza el equipo receptor de la comunicación central cuando recibe señales del equipo del sitio.

5.2.6 Fuente de eventos LONTA-202

La “fuente de eventos LONTA-202” está destinada a recibir eventos a través del puerto serie de los paneles centrales de monitoreo Lonta PRO, Lonta Optima y LONTA-202 fabricados por Altonika.

Cabe señalar que si utiliza el software Sentinel junto con cualquier panel de Altonika y desea cambiar al software Security Center, debe conocer la posibilidad de importar datos automáticamente desde el software “Strazh”. Consulte la descripción del módulo “Asistente de base de datos”, con el que los datos son importantes, para obtener más información sobre esta función.

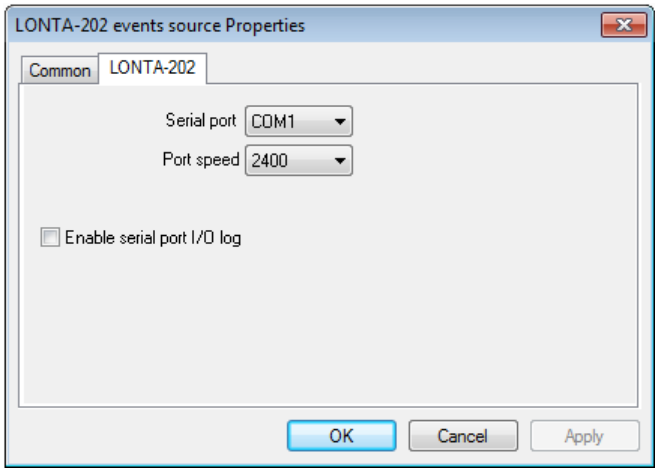


Figura 25: Ventana Propiedades de la fuente de eventos LONTA-202, pestaña "LONTA-202"

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el panel de monitoreo central, y el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio.

5.2.7 Fuente de eventos RS-200

La “fuente de eventos RS-200” está destinada a recibir eventos desde el panel de monitoreo central RS-200 fabricado por Altonika. Cabe señalar que la fuente de eventos admite todo el espectro de equipos que transmite señales al panel RS-200.

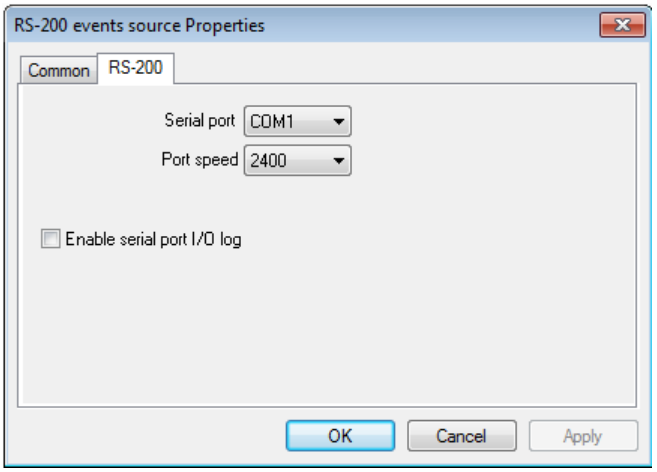


Figura 26: Ventana Propiedades de la fuente de eventos RS-200, pestaña "RS-200"

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el panel de monitoreo central, y el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio.

Cambio de número de sitio ”es un número entero positivo que se agrega automáticamente al número de sitio para cada evento aceptado por la fuente del evento.

5.2.8 Origen de eventos del RC 4000

La “fuente de eventos RC 4000” está destinada a recibir eventos a través del puerto serie desde el panel de monitoreo central RC 4000 fabricado por Visonic.

Si utiliza el panel RC 4000 junto con el software CSM32 y desea cambiar al software Security Center, debe conocer la posibilidad de importar datos automáticamente desde el software CSM32. Consulte la descripción del módulo “Asistente de base de datos”, con el que los datos son importantes, para obtener más información sobre esta función.

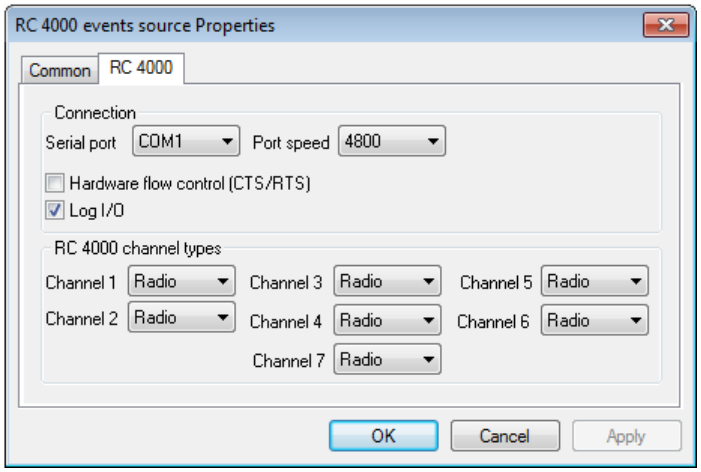


Figura 27: Ventana Propiedades de la fuente de eventos del RC 4000, pestaña "RC 4000"

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el panel, y el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio.

Si se utiliza el control por hardware del flujo de datos cuando se comunica a través de un puerto serie, es necesario marcar la casilla "Habilitar el control del flujo por hardware (CTS / RTS)".

Marque la opción “Registrar E / S” para guardar el protocolo de intercambio de la fuente del evento con el panel de monitoreo central en el disco duro. Esta información es útil para averiguar las causas de los problemas al recibir eventos del panel. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Utilice la pestaña “Tipos de canales RC 4000” para especificar los tipos de canales de comunicación que utiliza el panel cuando recibe señales del equipo del sitio.

5.2.9 Origen del evento multiprotocolo

La "fuente de eventos multiprotocolo" está diseñada para recibir eventos a través del puerto serie desde los siguientes paneles de monitoreo central

- Caballero silencioso 9500 (Honeywell)
- RCI4000 / RCI5000 / DTRCI5000 (KP Electronics)
- Blitz (canal de radio) (PKS)
- AES-Intellinet (canal de radio)

Además, esta fuente de eventos admite la recepción de datos a través de algunos otros protocolos comunes, por ejemplo, el protocolo Ademco 685.

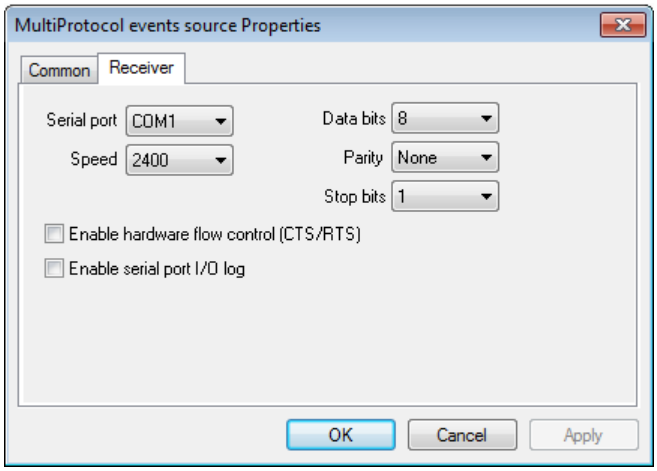


Figura 28: Ventana "Propiedades de origen de eventos multiprotocolo", pestaña "Receptor"

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el equipo receptor de la estación central, y utilice el parámetro "Velocidad en baudios del puerto" para establecer la tasa de cambio. La cantidad de bits de datos en los bytes transmitidos se puede especificar con el parámetro "Bits de datos", la paridad de transmisión se puede especificar con el parámetro "Paridad" y el parámetro "Bits de parada" se utiliza para determinar la cantidad de bits de parada.

Si se utiliza el control por hardware del flujo de datos cuando se comunica a través de un puerto serie, es necesario marcar la casilla "Habilitar el control del flujo por hardware (CTS / RTS)".

5.3 Controladores de eventos

Después de que el módulo “Administrador de eventos” acepta la notificación del panel de control o monitoreo central, decodifica y describe la notificación de acuerdo con la plantilla de evento especificada para el sitio desde el cual se recibió la notificación. El evento resultante de la decodificación de la notificación se puede manejar automáticamente en el módulo "Administrador de eventos" con la ayuda de componentes especiales del módulo llamados controladores de eventos.

Para acceder a la configuración de las fuentes de eventos, seleccione “Controladores de eventos. . . ”En el menú del módulo que aparece después de hacer clic con el botón derecho en el icono del módulo en la bandeja del sistema de la barra de tareas.

Para acceder a la ventana "Controladores de eventos", el usuario debe tener permiso para "Ver controladores de eventos" para el módulo "Administrador de eventos".

Para guardar los cambios, realizados en la ventana "Controladores de eventos", el usuario debe tener permiso para "Editar controladores de eventos" para el módulo "Administrador de eventos".

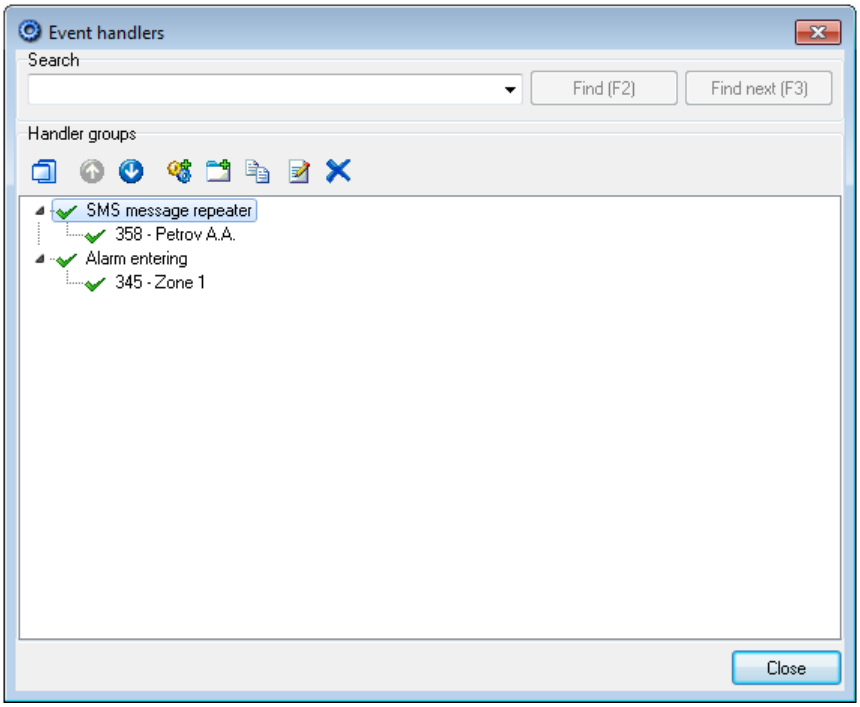


Figura 29: Ventana "Controladores de eventos"

El área "Buscar" de la ventana "Controladores de eventos" está destinada a buscar un grupo o controlador de eventos en la lista. Si hace clic en el botón "Inicio", la búsqueda se realizará desde el principio de la lista. Si hace clic en el botón "Buscar siguiente", la búsqueda comenzará desde el elemento seleccionado actualmente en la lista de controladores.

Los controladores de eventos del Centro de seguridad se controlan con los botones del panel de control, ubicado en la parte superior del área "Grupos de controladores" de la ventana "Controladores de eventos".

Haga clic en el botón "Mostrar grupos de controladores ocultos" para mostrar los controladores marcados como ocultos en la lista. Para habilitar la visualización de los grupos de controladores de eventos ocultos, el usuario debe tener permiso para "Ver controladores de eventos ocultos" para el módulo "Administrador de eventos". Cabe señalar que el permiso para "Editar controladores de eventos" se aplica solo a aquellos controladores de eventos que el usuario puede ver. De esta forma, se puede otorgar permiso al usuario para realizar cambios en los manejadores del “repetidor de mensajes SMS” y ocultar otros, críticos para el Centro de Seguridad, como “Red Pandora” o “Entrada de alarma”.

Utilice los botones "Subir en la lista" y "Bajar en la lista" para cambiar el orden de los controladores en la lista de visualización. Este orden es importante, ya que cada evento se envía a los controladores de eventos por turno, en el orden en que los controladores aparecen en la lista. Por ejemplo, si el controlador "Monitor de cadena de eventos" está configurado para monitorear el evento "Restablecimiento de alarma" después del evento "Alarma", entonces estará en la lista antes del controlador "Entrada de alarma", ya que este último puede cambiar la clase. del evento recibido.

El botón "Crear grupo" está destinado a agregar un nuevo grupo de controladores de eventos a la lista. Y el botón "Crear controlador" permite agregar un nuevo controlador al grupo. No hay restricciones sobre el número de grupos de manejadores en la lista o el número de manejadores en el grupo, se pueden crear tantos como sea necesario. El grupo de controladores de eventos de fi ne un algoritmo según el cual se manejará el evento. Además, la configuración del grupo define los recursos que se utilizarán durante el manejo. Por ejemplo, el dispositivo para el envío de SMS se especifica en el controlador de eventos "repetidor de mensajes SMS", y este dispositivo se utilizará para enviar mensajes a todos los controladores del grupo. En cuanto a los controladores del grupo, definen la configuración para el manejo de eventos que se realiza con respecto a sitios específicos. En este caso, los ajustes de los diferentes controladores no dependen unos de otros. Por ejemplo, los eventos del mismo sitio pueden ser manejados por diferentes manejadores del mismo grupo. La combinación de controladores en un grupo también es útil cuando los controladores de eventos deben estar ocultos o deshabilitados: el grupo se oculta junto con los controladores que incluye, y si el grupo de controladores de eventos está desactivado, los controladores incluidos en él no funcionarán, incluso si ellos mismos están habilitados.

Utilice el botón "Pegar copia del elemento seleccionado" para copiar el elemento actual seleccionado en la lista. Si se trata de un controlador de eventos, su copia se insertará en el mismo grupo de controladores de eventos, excepto que el nuevo controlador se desactivará. Si un

grupo de controladores está seleccionado en la lista, se insertará una copia del grupo en la lista. En este caso, se conservará el estado de los controladores de grupo, pero se desactivará el nuevo grupo de controladores de eventos.

Haga clic en el botón "Propiedades" para configurar el grupo de controladores de eventos o un controlador independiente.

El botón "Eliminar elemento seleccionado" permite eliminar el grupo seleccionado de controladores de eventos o un controlador separado en el grupo de la lista. Tenga cuidado, cuando elimine un grupo de controladores de eventos, todos los controladores de eventos incluidos en él serán eliminado. Debido al hecho de que la eliminación de controladores de eventos va acompañada de la limpieza de la base de datos de su configuración, algunos borrando grupos de controladores de eventos pueden llevar mucho tiempo.

La lista de los controladores de eventos admite varias operaciones que se pueden realizar con el mouse. Por ejemplo, se cambia posible el orden de los elementos de la lista y se mueven los controladores de eventos de un grupo a otro.

5.3.1 Configuración común para grupos de controladores de eventos

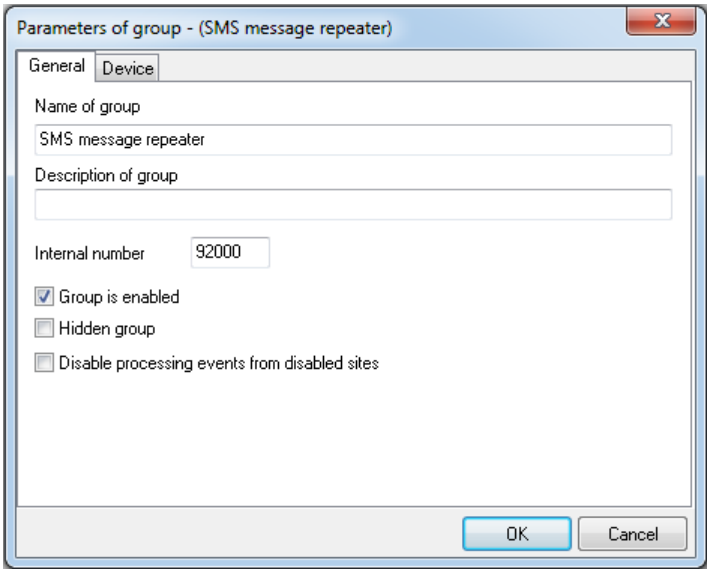


Figura 30: Ventana "Parámetros del grupo", pestaña "Común"

Como valor para el parámetro "Nombre del grupo", se permite especificar una cadena que se mostrará en la lista de controladores en la ventana "Controladores de eventos". En el nombre del grupo de los manejadores de eventos, se recomienda incluir información clave que caracterice al grupo para distinguir un grupo de otro, por ejemplo, los parámetros de los recursos utilizados por el grupo.

El parámetro "Descripción del grupo" se utiliza para almacenar información detallada sobre el grupo de controladores de eventos.

El parámetro "Número interno" es necesario para identificar el grupo de controladores de eventos por Security Center y el usuario. Cuando el grupo informa algo al usuario, el evento creado tendrá el mismo número de sitio que el número de grupo interno. Es muy recomendable crear sitios en el Centro de seguridad, cuyos números correspondan a los números internos del grupo de eventos; esto permitirá monitorear la ocurrencia de errores que ocurren durante la operación del controlador, así como recibir información de servicio sobre su trabaja. Como plantilla de eventos para sitios cuyos números corresponden a los números internos de los grupos de controladores de eventos, se recomienda utilizar la plantilla "Controladores de eventos".

Al buscar en la ventana "Controladores de eventos", la consulta de búsqueda examina los valores de los parámetros "Nombre del grupo", "Descripción del grupo" y "Número interno".

El grupo de controladores de eventos se puede habilitar o deshabilitar mediante el parámetro "El grupo está habilitado". Cabe señalar que si el grupo de controladores de eventos está desactivado, todos los recursos utilizados por él se liberan y el manejo de eventos por parte del grupo finaliza. En este caso, los manejadores incluidos en el grupo pueden habilitarse, ya que el estado del manejador no in fl uye en el manejo de eventos por parte del grupo inhabilitado.

Si el parámetro "Grupo oculto" está configurado para un grupo de controladores, es posible ocultar este grupo de controladores de la lista en la ventana "Controladores de eventos" para aquellos usuarios que no tienen permiso para ver los grupos ocultos de controladores de eventos.

Utilice la opción "Deshabilitar el manejo de eventos de sitios deshabilitados" para deshabilitar el manejo de eventos de sitios que están deshabilitados. Esta función puede ser útil para casi todos los manejadores, ya que permite excluir automáticamente del manejo los sitios deshabilitados. El sitio está deshabilitado en el módulo "Administrador del sitio" en la pestaña "Armar". Consulte la sección "Administrador del sitio" de este manual para obtener más información sobre cómo deshabilitar sitios.

5.3.2 Configuración del controlador de eventos común

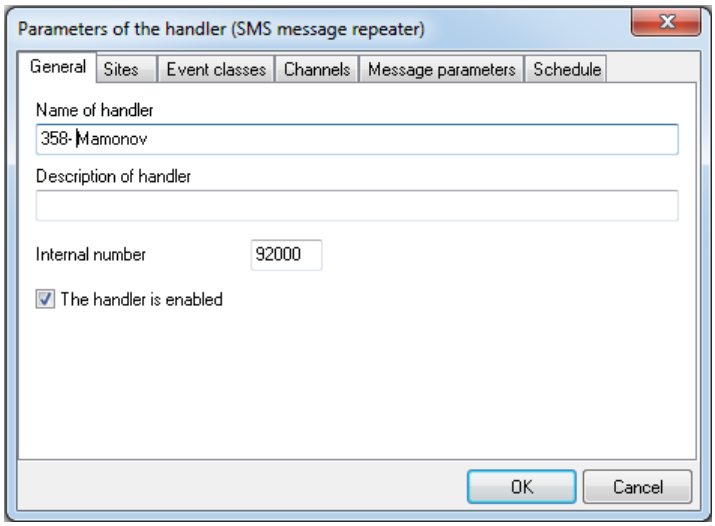


Figura 31: Ventana "Parámetros del controlador", pestaña "Común"

Como valor para el parámetro "Nombre del controlador", se permite especificar una cadena que se mostrará en la lista de controladores en la ventana "Controladores de eventos". En el nombre del manejador de eventos, se recomienda incluir información clave que lo caracterice y permita distinguir un manejador de otro, por ejemplo, el número del sitio, qué eventos maneja el manejador.

El parámetro "Descripción del controlador" está destinado a almacenar información detallada sobre el controlador de eventos.

El parámetro "Número interno" es necesario para identificar al controlador por Security Center y el usuario. Cuando el controlador informa algo al usuario, el evento creado tendrá el mismo número de sitio que el número de controlador interno.

El controlador de eventos se puede habilitar o deshabilitar mediante el parámetro "El controlador está habilitado". Cabe señalar que para el funcionamiento del controlador de eventos, es necesario que tanto el controlador como el grupo de controladores de eventos, en el que está incluido, estén habilitados.

Sitios

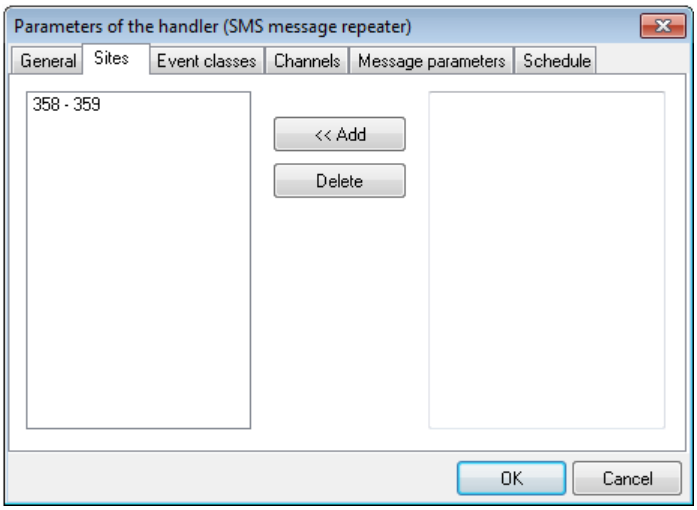


Figura 32: Ventana "Parámetros del controlador", pestaña "Sitios"

La pestaña "Sitios" se utiliza para especificar los números y los intervalos de los números de los sitios, qué eventos se manejarán. Para agregar un número o un intervalo de números de sitio a la lista de los manejados, es necesario ingresarlo en el campo de entrada en la parte derecha de la ventana y hacer clic en el botón “Agregar”. Al ingresar números de sitio, se permite enumerar varios números o números e intervalos de números separados por comas, por ejemplo: “100, 102, 104, 106-100, 200-299 ”. Para eliminar un número o un intervalo de números de sitio de la lista de los manejados, es necesario seleccionar la línea con el valor, que se eliminará en la lista, ubicada en la parte izquierda de la ventana, y hacer clic en el Botón "Eliminar".

Canales

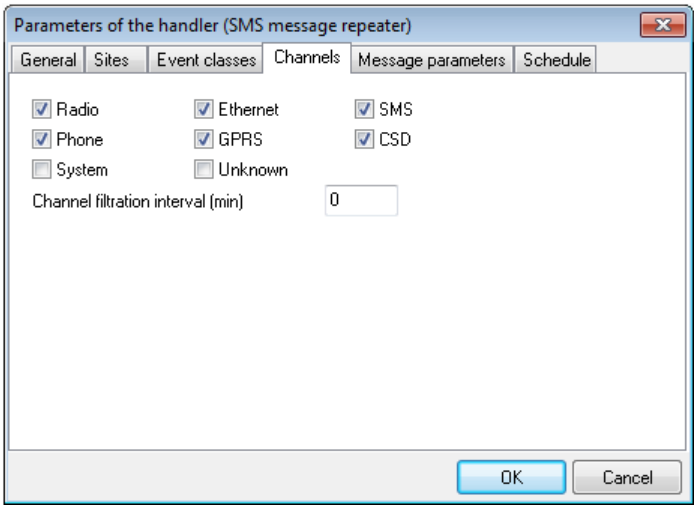


Figura 33: Ventana "Parámetros del controlador", pestaña "Canales"

La pestaña “Canales” está destinada a especificar los tipos de canales de comunicación a través de los cuales se recibirán los eventos a manejar. Para permitir el manejo de los eventos recibidos a través de un canal de comunicación en particular, es necesario verificar el nombre del canal apropiado.

El parámetro “Intervalo de filtración de canal” está destinado a excluir del manejo de eventos idénticos recibidos a través de diferentes canales de comunicación. Si el valor de este parámetro es mayor que cero, solo se manejará el primer evento recibido, todos los demás eventos, recibidos durante el intervalo especificado, serán ignorados. Por ejemplo, si se utilizan dos canales de comunicación para transmitir mensajes desde el sitio: radio y teléfono y el valor del parámetro "Intervalo de filtración de canal" es 1 minuto, se manejará el mensaje recibido por radio y el mensaje recibido por teléfono ser ignorado (si llega dentro de un minuto). El parámetro "Intervalo de filtración de canal" se recomienda para su uso en controladores de eventos "Repetidor de mensajes SMS".

Calendario

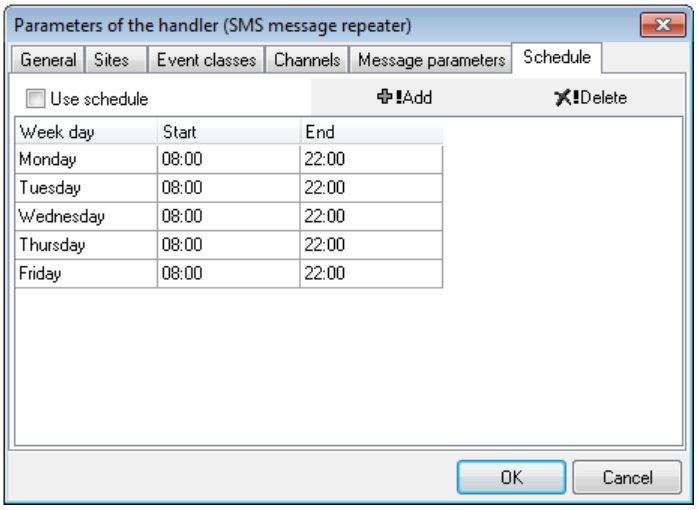


Figura 34: Ventana "Parámetros del controlador", pestaña "Programación"

Si el controlador de eventos debe configurarse de modo que el manejo de eventos se realice solo a una hora especificada, configure el programa del controlador en la pestaña "Programación".

Haga clic en el botón "Agregar" para agregar el intervalo del controlador de eventos a la lista. Para cada intervalo, es necesario especificar el día de la semana al que se refiere, así como la hora de inicio y finalización de su funcionamiento.

El botón "Eliminar" se utiliza para eliminar el intervalo del controlador de eventos de la lista.

Utilice la opción "Usar programa" para habilitar o deshabilitar el uso del programa por parte del administrador. Si el uso de la programación por parte del controlador de eventos está deshabilitado, entonces funciona constantemente. Si el uso de la programación está habilitado, pero no hay un solo intervalo para el trabajo, el controlador de eventos nunca se habilitará.

5.3.3 Monitoreo de eventos

Este manejador monitorea la recepción periódica del evento de una clase dada y genera un evento del sistema en su ausencia.

El controlador se puede utilizar para resolver las siguientes tareas:

- “Vigilancia de guardia”. La tarea de la vigilancia de la guardia se reduce a menudo a una simple vigilancia de la recepción periódica de un evento determinado. En este caso, a pesar de que la secuencia de recepción de eventos no está monitoreada, es posible monitorear a los guardias incluso en una ruta compleja seleccionando los intervalos para recibir eventos.
- “Monitoreo automático de prueba” A diferencia del tiempo de control de un sitio que implica la llegada de cualquier evento desde el sitio a través de cualquier canal de comunicación, es posible monitorear la llegada periódica de un evento en particular, y especificar el canal de comunicación a través del cual este evento es para ser recibido.

La configuración del grupo de manejadores de eventos “Monitoreo de eventos” coincide completamente con la configuración general de los grupos de manejadores de eventos, que se describen en detalle anteriormente.

La configuración del controlador de eventos "Monitoreo de eventos" también coincide en gran medida con la configuración general de los controladores de eventos discutidos anteriormente, excepto por la pestaña "Monitoreo de eventos".

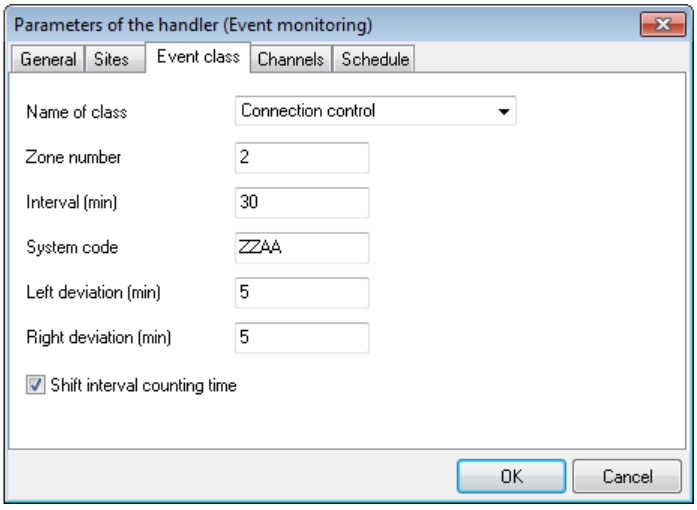


Figura 35: Ventana "Parámetros del controlador (supervisión de eventos)", pestaña "Clase de evento"

- El controlador de eventos, configurado como se muestra en la figura, monitoreará la llegada de la clase de evento “Control de conexión” cada 30 minutos. Un período de 25 a 34 minutos después de recibir el evento anterior se considerará válido para el próximo evento. *

El parámetro "Clase de evento" especifica la clase de evento que supervisa el controlador de eventos.

Utilice el parámetro "Número de zona" para limitar la lista de eventos monitoreados por el controlador. Si el valor de este parámetro no está establecido o es igual a cero, entonces el controlador monitorea la recepción de cualquier evento, cuya clase corresponde al valor del parámetro "Clase de evento". Si el parámetro “Número de zona” se establece en el valor de la zona, solo se monitorearán aquellos eventos que tengan un número de zona correspondiente a la zona especi fi cada.

El parámetro "Intervalo" define el intervalo durante el cual el manejador de eventos recibirá eventos monitoreados.

El parámetro "Código del sistema" especifica el código de evento del sistema que se creará si el controlador no recibe el siguiente evento. Al crear un evento del sistema, se utilizan el canal de comunicación “Sistema” y el número del sitio desde el cual no se recibe el evento monitoreado. El evento del sistema se decodificará de acuerdo con la plantilla de evento especificada para el sitio en el que se creó el evento.

Los parámetros “Desviación a la izquierda” y “Desviación a la derecha” están destinados a configurar el intervalo de monitoreo exacto para recibir los eventos monitoreados. Si el valor del parámetro “Desviación a la izquierda” no es igual a cero, entonces solo el evento, que se acepta no antes del valor del intervalo menos la desviación a la izquierda, se contará como recibido. Por ejemplo, si la llegada del evento se monitorea cada 30 minutos y la desviación a la izquierda es de 5 minutos, solo se contará como aceptado el evento que se reciba no antes de 25 minutos después del anterior. Si el valor del parámetro “Desviación a la derecha” no es cero, entonces el evento que se reciba más tarde que el valor del intervalo más la desviación a la derecha, pero no más, se contará como aceptado. Por ejemplo,

Si se establece el parámetro "Tiempo de recuento del intervalo de cambio", el nuevo intervalo de tiempo de espera del evento se contará desde el momento de la recepción del evento anterior. Si el parámetro no está configurado, entonces el recuento del intervalo está relacionado con el momento en que se habilita el controlador. Si los eventos monitoreados por el manejador son creados por la persona, se recomienda configurar el parámetro “Tiempo de recuento del intervalo de cambio”, para que el manejador de eventos ignore las inexactitudes y desviaciones relacionadas con la presencia del factor humano. Si se monitorean los eventos creados por el equipo, entonces no es necesario configurar el parámetro “Tiempo de recuento del intervalo de cambio”.

La configuración de las desviaciones permisibles y el cambio del comienzo del intervalo son más a menudo necesarios para tareas similares a la tarea de “Vigilancia de guardia”: hay un intervalo durante el cual se realiza una ronda, hay desviaciones permisibles. Si se presiona el botón de monitoreo antes de tiempo, se ignora y es posible presionarlo un poco más tarde. A su vez, el nuevo intervalo se contará desde el momento en que el guardia de seguridad con fi rmó la finalización del anterior.

5.3.4 Monitoreo de la cadena de eventos

Este controlador está destinado a monitorear la secuencia de tiempo (cadena) de los eventos recibidos y la generación de mensajes del sistema en caso de violación. El controlador está diseñado para resolver tareas como:

- “Seguimiento de eventos emparejados”. Por ejemplo, monitoreando la restauración de 220V u otras fallas en el sitio. Utilice el controlador de "Monitoreo de la cadena de eventos" para distinguir automáticamente entre fallas a corto plazo y fallas fatales, por ejemplo, para sitios de detección donde la fuente de alimentación no está disponible por mucho tiempo.
- “Vigilancia de guardia”. El uso de este manejador permite monitorear el movimiento de la guardia a lo largo de la ruta, teniendo en cuenta la secuencia correcta de la ronda.

La configuración del grupo de manejadores de eventos “Monitoreo de eventos” coincide completamente con la configuración general de los grupos de manejadores de eventos, que se describen en detalle anteriormente.

La configuración del controlador de eventos "Monitoreo de eventos" también coincide en gran medida con la configuración general de los controladores de eventos discutidos anteriormente, excepto por la pestaña "Cadena de clases".

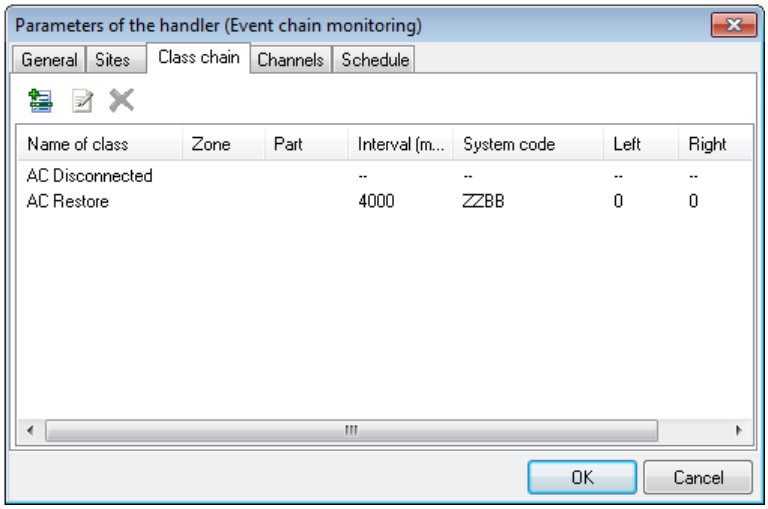


Figura 36: Ventana "Parámetros del controlador (supervisión de la cadena de eventos)", pestaña "Cadena de clases"

- El manejador de eventos, configurado como se muestra en la figura, está esperando un evento con la clase “AC desconectada”. Si dentro de las 5 horas (300 minutos) después de recibirlo del sitio, no se recibe el evento con la clase "AC Restore", el controlador creará un evento del sistema con el código "ZZBB". El manipulador configurado de esta manera permite advertir al personal de la estación de monitoreo sobre un corte prolongado de energía en el sitio. *

La pestaña "Cadena de clases" muestra una secuencia de clases de eventos, cuya recepción es supervisada por el controlador, y el controlador de eventos espera los eventos exactamente en el orden en que aparecen en la lista.

A diferencia del controlador de eventos “Control de eventos”, que inicia el intervalo de espera para el evento monitoreado inmediatamente después de habilitarlo, el controlador de eventos “Monitoreo de la cadena de eventos” se habilita solo después de que se recibe el primer evento de la cadena. El hecho de recibir el primer evento de la cadena por parte del manejador no es monitoreado de ninguna manera.

Utilice el botón "Agregar clase de evento a la cadena" para agregar una nueva clase de evento al final de la cadena de eventos monitoreados.

Haga clic en el botón "Propiedades de la clase de evento" para ver y cambiar los valores de los parámetros de la clase de evento seleccionada en la lista.

El botón "Eliminar" se utiliza para eliminar una clase de evento de la cadena.

Utilice la ventana "Propiedades de la clase de evento" para ver y cambiar las propiedades de la clase de evento:

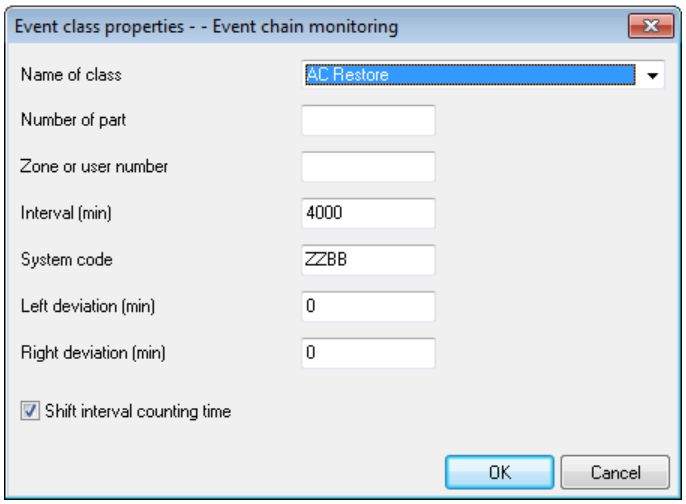


Figura 37: Ventana "Propiedades de la clase de evento - Supervisión de la cadena de eventos"

El parámetro "Nombre de la clase" especifica la clase de evento que supervisa el controlador de eventos.

Utilice el parámetro "Número de zona" para limitar la lista de eventos monitoreados por el controlador. Si el valor de este parámetro no está establecido o es igual a cero, entonces el controlador monitorea la recepción de cualquier evento, cuya clase corresponde al valor del parámetro "Clase de evento". Si el parámetro “Número de zona” se establece en el valor de la zona, solo se monitorearán aquellos eventos que tengan un número de zona correspondiente a la zona especi fi cada.

El parámetro "Intervalo" define el intervalo durante el cual el manejador de eventos recibirá eventos monitoreados.

El parámetro "Código del sistema" especifica el código de evento del sistema que se creará si el controlador no recibe el evento monitoreado. Cabe señalar que es posible especificar un código de evento del sistema separado para cada clase de evento en la cadena. Esto permite informar al operador sobre los detalles de la infracción y ofrecerle diferentes algoritmos para manejar la situación. Al crear un evento del sistema, se utilizan el canal de comunicación “Sistema” y el número del sitio desde el cual no se recibe el evento monitoreado. El evento del sistema se decodificará de acuerdo con la plantilla de evento especificada para el sitio en el que se creó el evento.

Los parámetros “Desviación a la izquierda” y “Desviación a la derecha” están destinados a configurar el intervalo de monitoreo exacto para recibir los eventos monitoreados. Si el valor del parámetro “Desviación a la izquierda” no es igual a cero, entonces solo el evento, que se acepta no antes del valor del intervalo menos la desviación a la izquierda, se contará como recibido. Por ejemplo, si la llegada del evento se monitorea en 30 minutos y la desviación a la izquierda es de 5 minutos, solo se contará como aceptado el evento que se reciba no antes de 25 minutos después del anterior. Si el valor del parámetro “Desviación a la derecha” no es cero, entonces el evento que se reciba más tarde que el valor del intervalo más la desviación a la derecha, pero no más, se contará como aceptado. Por ejemplo,

Si se establece el parámetro "Tiempo de recuento del intervalo de cambio", el nuevo intervalo de tiempo de espera del evento se contará desde el momento de la recepción del evento anterior. Si el parámetro no está configurado, entonces el recuento del intervalo está relacionado con el momento en que se habilita el controlador. Si los eventos monitoreados por el manejador son creados por la persona, se recomienda configurar el parámetro “Tiempo de recuento del intervalo de cambio”, para que el manejador de eventos ignore las inexactitudes y desviaciones relacionadas con la presencia del factor humano. Si se monitorean los eventos creados por el equipo, entonces no es necesario configurar el parámetro “Tiempo de recuento del intervalo de cambio”.

Al igual que el código de evento del sistema, los valores de los parámetros de desviación permitidos y el tiempo de recuento del intervalo de cambio se pueden especificar de forma independiente para cada clase de la cadena.

La configuración de las desviaciones permisibles y el cambio del comienzo del intervalo son más a menudo necesarios para tareas similares a la tarea de “Vigilancia de guardia”: hay un intervalo durante el cual se realiza una ronda, hay desviaciones permisibles. Si se presiona el botón de monitoreo antes de tiempo, se ignora y es posible presionarlo un poco más tarde. A su vez, el nuevo intervalo se contará desde el momento en que el guardia de seguridad con fi rmó la finalización del anterior.

Monitorización de la conexión con dispositivos GSM C.Nord

El controlador de eventos "Monitoreo de la cadena de eventos" se puede utilizar para monitorear la conexión a dispositivos que usan "C.Nord GSM (CML) ”.

Cuando el dispositivo está conectado a la fuente del evento, se crea un evento del sistema con el código "ZZWE", que por defecto se describe con la clase de evento "Conexión establecida". Cuando se desconecta el transmisor, se genera un evento del sistema con el código "ZZWF", que se describe con la clase de evento "Conexión perdida".

Así, existe toda la información necesaria para monitorear el canal de comunicación: si la conexión con el transmisor se pierde y no se restablece dentro de un período de tiempo determinado, es necesario obtener información al respecto.

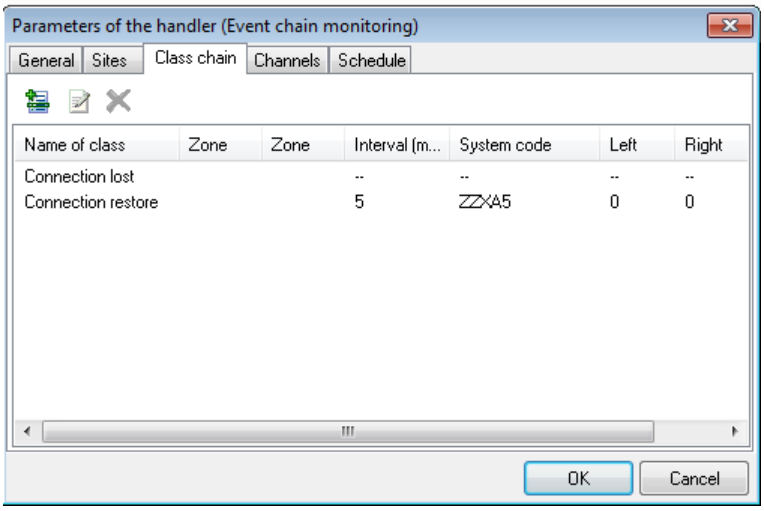


Figura 38: ”Parámetros del manejador (monitoreo de la cadena de eventos) para monitorear la ventana de conexión

El controlador de eventos, que está configurado como se muestra en la figura, creará un evento con el código "ZZXA5" (clase de evento - "Alarma de conexión", descripción del evento - "No hay eventos a través de GPRS"), si la conexión con el transmisor no es restaurado dentro de los 5 minutos posteriores a su pérdida.

5.3.5 Entrada de alarma

El manejador de eventos “Entrada de alarma” permite suspender el manejo de un evento de alarma por parte del módulo “Administrador de eventos” y esperar el desarmado, que se puede recibir inmediatamente después de la alarma.

El propósito de este controlador de eventos es evitar que el operador de servicio tenga que responder deliberadamente a falsas alarmas que ocurren cuando los sitios están desarmados.

Este controlador se utilizará para aquellos sitios donde se utilicen tácticas de seguridad, que excluyen el retraso de entrada. Además, el uso de este controlador está justificado para todos los sitios donde es posible un error de personal durante el desarmado.

La configuración del grupo de controladores de eventos "Entrada de alarma" coincide completamente con la configuración general de los grupos de controladores de eventos, que se describen en detalle anteriormente.

La configuración del controlador de eventos "Entrada de alarma" también coincide en gran medida con la configuración general de los controladores de eventos mencionados anteriormente, a excepción de la pestaña "Cadena de clases".

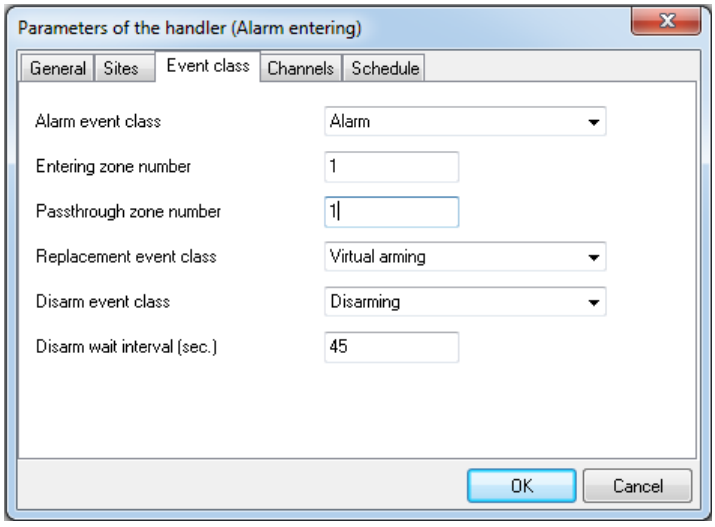


Figura 39: Ventana "Parámetros del controlador (entrada de alarma)"

- Si el controlador de eventos está configurado como se muestra en la figura, cuando se reciba un evento con la clase "Alarma" en la primera zona, el controlador se habilitará y reemplazará la clase del evento recibido con "Alarma retardada". Si después de eso el evento con la clase "Desarmado" no se recibe dentro de los 45 segundos, el evento con la clase "Alarma" será creado nuevamente por el manejador y enviado al operador para su manejo. Si se recibe el evento con la clase "Desarmado", el manejador dejará de trabajar hasta que se reciba el siguiente evento con la clase "Alarma". *

El parámetro “Clase de evento de alarma” especifica la clase del evento, cuyo manejo es suspendido por el operador y el Centro de Seguridad.

Utilice el parámetro "Número de zona" para determinar el evento que se manejará con precisión dentro de una zona: si el valor de este parámetro no está establecido o es igual a cero, entonces cualquier evento, cuya clase coincida con el valor del parámetro "Clase de evento de alarma", será aceptado para su manipulación. Si el parámetro “Número de zona” se establece en el valor de la zona, solo se manejará el evento con el número de zona correspondiente al especificado.

Para el evento aceptado para su manejo, se reemplaza la clase de evento. El valor del parámetro "Clase de evento de reemplazo" determina qué clase tendrá el evento después de su manejo.

Después de que el controlador de eventos "Entrada de alarma" recibe un evento de alarma y reemplaza la clase correspondiente, comienza la cuenta regresiva del intervalo de espera para el evento cuya clase está establecida por el valor de la clase de evento "Desarmado". Si el evento con dicha clase no se recibe durante el intervalo especificado por el valor del parámetro "Intervalo de espera de desarmado", el controlador creará un evento del sistema, en el que el código, la clase, el número de zona y la descripción se copiarán del evento, cuyo manejo fue suspendido. Solo diferirán la fecha y la hora del evento; corresponderán a la hora del evento del controlador y al canal de recepción del evento; el valor de este parámetro de evento se establecerá en “Sistema”.

5.3.6 Repetidor de mensajes SMS

El controlador "repetidor de mensajes SMS" permite enviar información sobre los eventos recibidos a un teléfono móvil en forma de mensajes SMS.

Con la ayuda del manejador “repetidor de mensajes SMS”, es posible brindar un servicio adicional a los clientes de la empresa de seguridad, por ejemplo, informar a las personas responsables sobre el armado y desarmado del sitio. Además, con la ayuda de este manipulador, es posible transmitir alarmas directamente al teléfono móvil de la Guardia en paralelo con el trabajo del operador de turno.

Además, este controlador puede simplificar enormemente la puesta en marcha de equipos en los sitios conectados. Si el ingeniero tiene un número personal del sitio que utilizará al momento de revisar el equipo en el sitio, y los mensajes SMS de los eventos recibidos de este sitio se envían a su teléfono móvil, permitirá realizar el equipo. configuración sin los operadores de servicio.

Dispositivo para enviar mensajes SMS

El manejador de eventos puede enviar mensajes SMS usando uno de los dispositivos conectados directamente a la computadora operativa:

- Módems GSM «iRZ TU31»
- Terminales GSM basados en módem GSM “Siemens MC35” o compatibles con él
- Módem GSM “SonyEricsson GM-22”
- Módem GSM «SonyEricsson GR-47»
- Teléfonos móviles Nokia

Para enviar mensajes SMS, se utilizan controladores de dispositivos especiales, que se denominan "transceptores". Cada dispositivo compatible tiene un transceptor apropiado, que está diseñado para conectarse al dispositivo.

Además de trabajar con dispositivos de hardware, el manipulador puede conectarse para enviar mensajes SMS al software "Phoenix" o directamente al servidor SMS del operador móvil a través del protocolo SMPP. También hay transceptores correspondientes para cada una de estas formas de enviar mensajes SMS.

Los ajustes en la pestaña "Dispositivo" permiten determinar la forma en que se enviarán los mensajes SMS, así como los parámetros necesarios.

Módem GSM

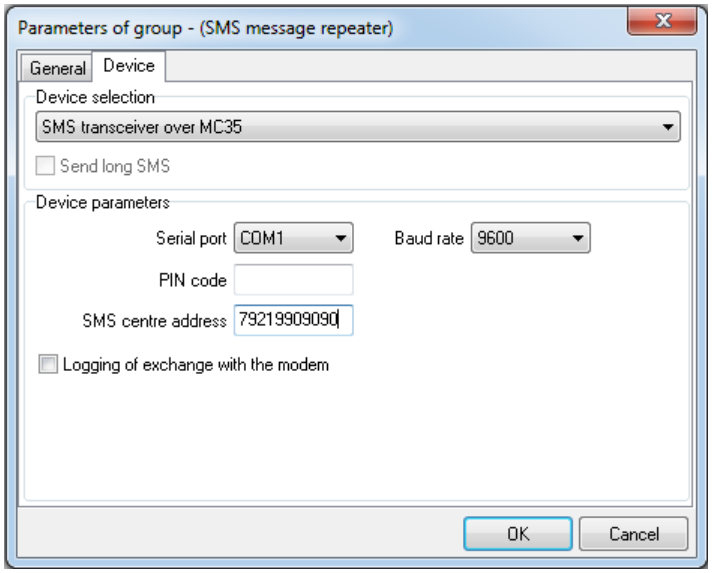


Figura 40: Ventana "Parámetros del grupo (repetidor de mensajes SMS)", pestaña "Dispositivo", parámetros del transceptor SMS a través del módem MC35

Utilice el parámetro "Puerto serie" para seleccionar el puerto serie al que está conectado el módem GSM, con el que se enviarán los mensajes SMS, y utilice el parámetro "Velocidad en baudios" para establecer la tasa de cambio.

Si la tarjeta SIM instalada en el módem GSM está protegida por un código de identificación personal, se puede configurar como el valor del parámetro "Código SIM". Se recomienda encarecidamente no utilizar tarjetas SIM protegidas por código PIN para evitar problemas asociados con la pérdida de códigos establecidos.

El parámetro "Dirección del centro de servicio" permite establecer el número de teléfono del centro de SMS del operador de telefonía móvil, cuya tarjeta SIM está instalada en el módem GSM. Algunos operadores de comunicaciones requieren que se configure este parámetro para que la función de envío de mensajes SMS funcione correctamente. El número de teléfono que se utiliza como valor del parámetro "Dirección del centro de servicio" se especificará en formato internacional completo. El símbolo "+" no se utilizará al especificar este número.

Marque el parámetro "Registro de intercambio con el módem" para guardar el protocolo de intercambio del controlador de eventos con el módem GSM en el disco duro de la computadora. Esta información es útil para averiguar las causas de los problemas al conectarse a un módem GSM o enviar mensajes SMS a través de él. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Los parámetros de los transceptores destinados a la conexión a los módems “SonyEricsson GM-22” y “SonyEricsson GR-47” son completamente similares a los parámetros de configuración del módem “Siemens MC35”.

Cabe señalar que varios grupos de controladores de eventos "repetidor de mensajes SMS" pueden utilizar el mismo módem GSM para enviar mensajes SMS. Por lo tanto, al determinar el número requerido de módems GSM, tenga en cuenta solo el ancho de banda del dispositivo utilizado. Para el módem “SonyEricsson GR-47” es posible tener en cuenta 5-7 mensajes SMS por minuto, y para el módem “Siemens MC35” este valor es de 10-12 mensajes SMS por minuto.

Software Phoenix

El software “Phoenix” fue desarrollado por C.Nord y está destinado a organizar un conjunto de canales para recibir y transmitir mensajes SMS. Se suministra como parte del software “Andromeda MS” y del software “Andromeda Persona”. La conexión al software “Phoenix” se realiza a través de una red que implementa el protocolo TCP / IP, mientras que una copia del software “Phoenix” actúa siempre como servidor TCP / IP, esperando la conexión. La característica del software “Phoenix” es la capacidad de reservar canales para el envío de mensajes SMS, por eso los parámetros del transceptor destinado al envío de mensajes SMS a través del software Phoenix se dividen en dos grupos idénticos. Un grupo de parámetros está destinado a configurar el canal principal para enviar mensajes SMS y el segundo para el canal de respaldo.

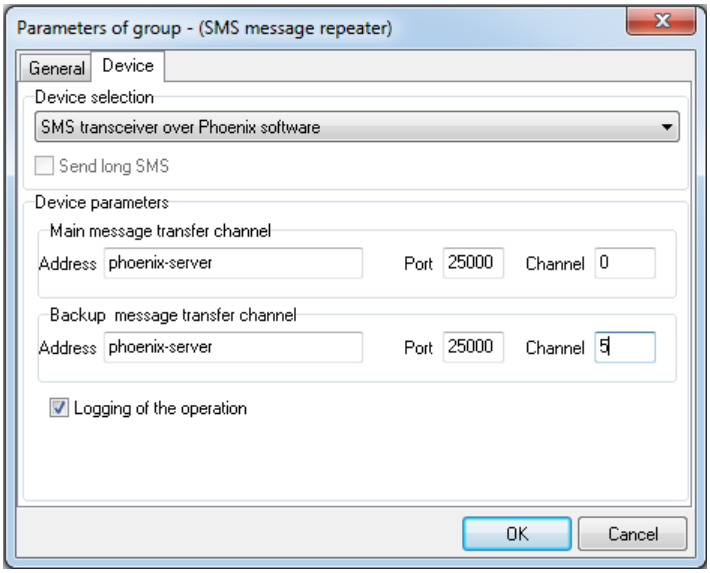


Figura 41: Ventana "Parámetros del grupo (repetidor de mensajes SMS)", pestaña "Dispositivo", parámetros del transceptor SMS sobre el software Phoenix

El parámetro "Dirección" se utiliza para especificar el nombre NetBIOS de la computadora, en la que se ejecuta la instancia del software Phoenix, a través de la cual es necesario enviar mensajes SMS. En lugar del nombre NetBIOS de la computadora, se le permite especificar su dirección IP. Utilice el parámetro "Puerto" para especificar el puerto al que desea conectarse.

Marque el parámetro "Registro de la operación" para guardar el protocolo de intercambio del controlador de eventos con el software "Phoenix" en el disco duro de la computadora. Esta información es útil para conocer las causas de los problemas al conectarse al software “Phoenix” o enviar mensajes SMS a través de él. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Teléfonos Nokia

El “transceptor de SMS en teléfonos Nokia” está diseñado para enviar mensajes SMS utilizando algunos modelos de teléfonos móviles Nokia.

Modelos de teléfono compatibles: 1100, 1220, 1260, 1261, 2100, 2270, 2275, 2280, 2285, 2300, 2600, 2650, 3100, 3105, 3108, 3200, 3205, 3210, 3220, 3300, 3310, 3320, 3330, 3350, 3360, 3390, 3395, 3410, 3510, 3510i, 3520, 3530, 3560, 3570, 3585, 3585i, 3586, 3586i, 3587i, 3588i, 3589i, 3590, 3595, 3610, 5100, 5110, 5130, 5140, 5190, 5210, 5510, 6100, 6108, 6110, 6130, 6150, 6190, 6200, 6210, 6220, 6225, 6230, 6250, 6310, 6310i, 6320, 6340, 6340i, 6360, 6370, 6385, 6500, 6510, 6560, 6585, 6590, 6610, 6610i, 6650, 6651, 6800, 6810, 6820, 7110, 7160, 7190, 7200, 7210, 7250, 7250i, 7260, 7600, 8210, 8250, 8290, 8310, 8390, 8810, 8850, 8855, 8890, 8910, 8910i.

Métodos admitidos para conectar teléfonos móviles a la computadora:

- Cable compatible con DAU-9P (modo FBUS);
- Cable DLR-3 (DLR-3P) (para los modelos 6210, 6250, 6310, 6310i, 7110, 7190);
- Puerto de infrarrojos;
- Bluetooth (para modelos 6310i con versión de firmware 5.50 y superior, 8910i);
- Cable DKU-5.

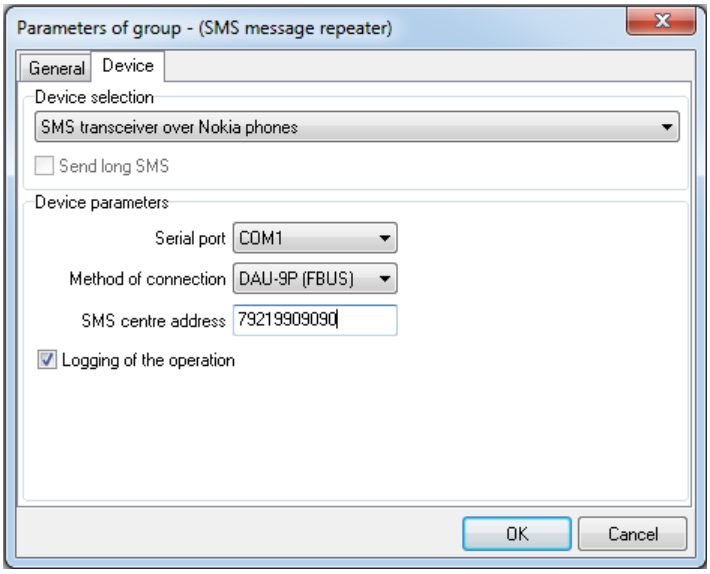


Figura 42: Ventana "Parámetros de grupo (repetidor de mensajes SMS)", pestaña "Dispositivo", parámetros del transceptor de SMS en teléfonos Nokia

Utilice la opción Puerto serie para seleccionar el puerto serie al que está conectado el teléfono móvil Nokia para enviar mensajes SMS, y utilice el parámetro "Método de conexión" para especificar la forma en que este teléfono está conectado a la computadora.

El parámetro "Dirección del centro de servicio" permite establecer el número de teléfono del centro de SMS del operador de telefonía móvil, cuya tarjeta SIM está instalada en el módem GSM. Algunos operadores de comunicaciones requieren que se configure este parámetro para que la función de envío de mensajes SMS funcione correctamente. El número de teléfono que se utiliza como valor del parámetro "Dirección del centro de servicio" se especificará en formato internacional completo. El símbolo "+" no se utilizará al especificar este número.

Marque el parámetro "Registro de la operación" para guardar el protocolo de intercambio del administrador de eventos con el teléfono Nokia en el disco duro de la computadora. Esta información es útil para averiguar las causas de los problemas al conectarse al teléfono Nokia o enviar mensajes SMS a través de él. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Protocolo SMPP sobre TCP / IP

El “Transceptor de SMS sobre SMPP (TCP / IP)” transmite mensajes SMS conectándose al servidor SMS del operador de comunicaciones móviles (SMSC) a través de SMPP versión 3.4. La conexión se realiza a través de una red que admite el protocolo TCP / IP.

La pestaña "SMSC" especifica los parámetros necesarios para conectar el transceptor al servidor SMS del operador de telefonía móvil.

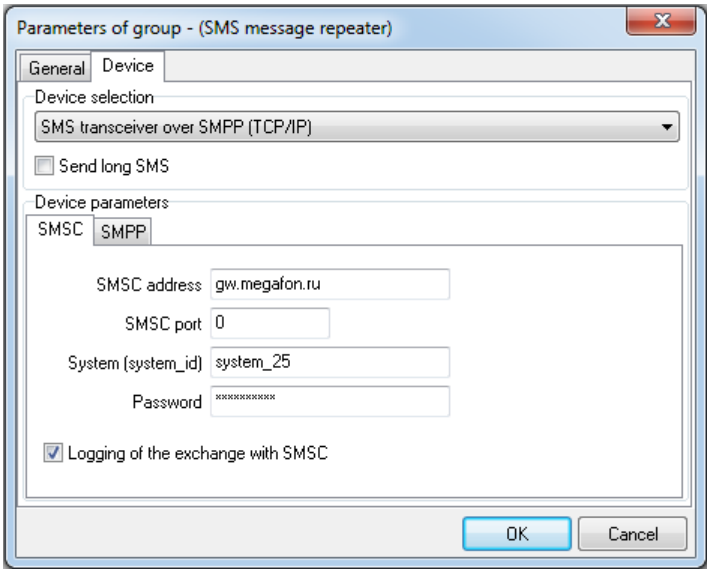


Figura 43: Ventana "Parámetros del grupo (repetidor de mensajes SMS)", pestaña "Dispositivo", parámetros del dispositivo "Transceptor SMS sobre SMPP (TCP / IP)", pestaña "SMSC"

El parámetro "Dirección SMSC" permite establecer la dirección IP o el nombre DNS de la computadora del servidor SMS del operador móvil al que se está conectando, y el parámetro "Puerto SMSC" permite especificar el puerto TCP / IP al que es necesario conectarse.

Los parámetros “Sistema (ID del sistema)” y “Contraseña” son los requisitos que identifican el sistema (suscriptor) que se está conectando al servidor SMS. Estos requisitos los proporciona el operador móvil durante la preparación del contrato para la organización de la conexión a su servidor SMS.

Marque el parámetro "Registro del intercambio con SMSC" para guardar el protocolo de intercambio del controlador de eventos con el servidor SMS del operador de comunicaciones móviles en el disco duro de la computadora. Esta información es útil para conocer las causas de los problemas a la hora de conectarse al servidor SMS del operador de comunicaciones móviles o enviar mensajes SMS a través de él. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Utilice la pestaña "SMPP" para especificar los parámetros específicos del protocolo SMPP. Se recomienda cambiar estos parámetros solo si el operador de comunicaciones móviles ha definido valores especiales para ellos durante la preparación del contrato para la organización de la conexión a su servidor SMS.

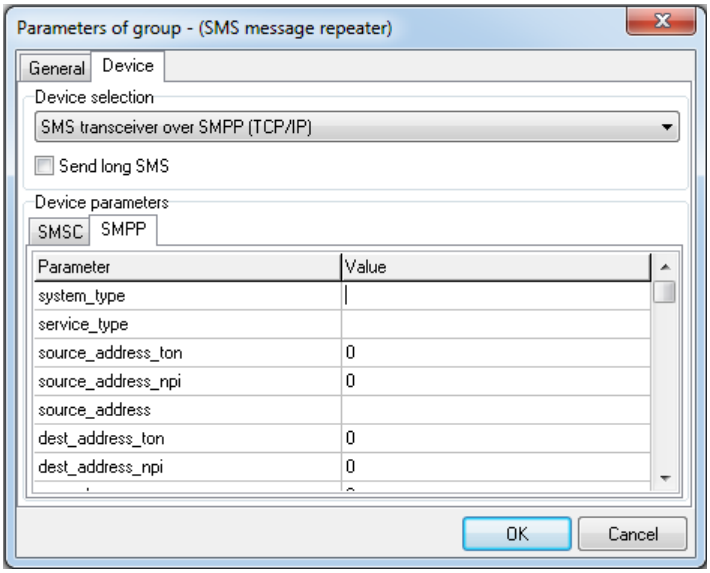


Figura 44: Ventana "Parámetros de grupo (repetidor de mensajes SMS)", pestaña "Dispositivo", parámetros del dispositivo "Transceptor SMS sobre SMPP (TCP / IP)", pestaña "SMPP"

Los nombres de todos los parámetros que se pueden cambiar en la pestaña “SMPP” corresponden a los campos en PDU SUBMIT SM. Puede encontrar una descripción detallada de los parámetros y su formato en la especificación del protocolo SMPP.

Pestaña "Clases de eventos"

En la pestaña "Clases de eventos", se muestra una lista de clases de eventos, tras la recepción de la cual el controlador generará un mensaje SMS para enviar.

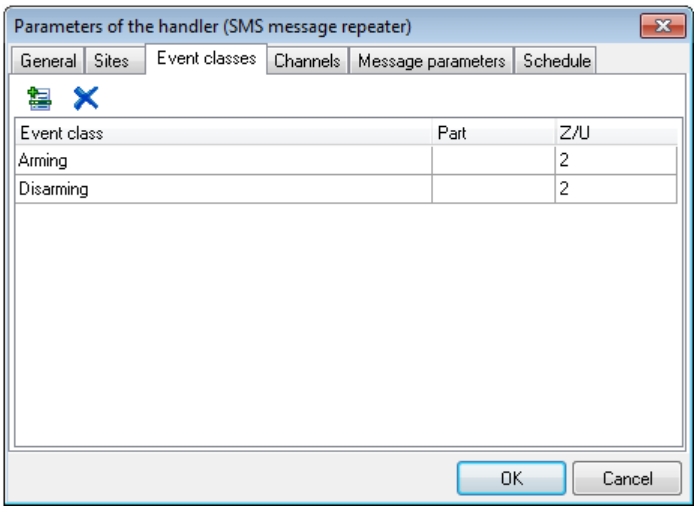


Figura 45: Ventana "Parámetros del controlador (repetidor de mensajes SMS)", pestaña "Clases de eventos"

Para cada clase de la clase en la lista es posible especificar el número de la pieza, así como el número de la zona o usuario; estos parámetros permiten determinar con mayor precisión los eventos que generarán mensajes SMS.

Si el valor de la columna "Parte" no se establece o es igual a cero, se gestionan todos los eventos cuya clase corresponde a la especificada en la columna "Clase". Si la columna "Parte" no se establece en cero, los mensajes SMS se generarán solo para esos eventos, cuyo número de parte corresponde al especificado.

Se aplica una regla similar al valor de la columna "Z / U" para especificar el número de zona o el usuario que desencadenó el evento.

Utilice el botón "Agregar clase de evento" para agregar una nueva clase de evento a la lista de clases de eventos

controladas. El botón "Eliminar" se utiliza para eliminar una clase de evento de la lista de eventos manejados.

Ficha "Parámetros de mensaje"

Utilice la pestaña "Parámetros de mensaje" para especificar los parámetros que determinan el destinatario, así como el formato y contenido de los mensajes SMS generados por el gestor.

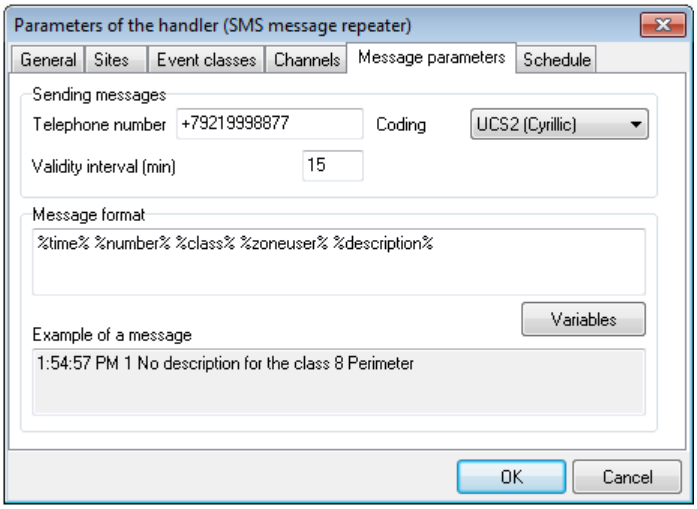


Figura 46: Ventana "Parámetros del gestor (repetidor de mensajes SMS)", pestaña "Parámetros del mensaje"

Utilice el parámetro "Número de teléfono" para configurar el número de teléfono del destinatario del mensaje SMS. Al especificar el valor de este parámetro, se recomienda especificar el número de teléfono en formato internacional, incluido el símbolo "+" al principio del número.

El parámetro "Codificación" se utiliza para seleccionar la codificación que se utilizará para generar mensajes SMS. Si el valor de este parámetro es “UCS2 (cirílico)”, los caracteres cirílicos que están presentes en los mensajes SMS se guardarán sin cambios. Si se especifica “Translit” como valor para este parámetro, los caracteres cirílicos del mensaje SMS serán transliterados, es decir, serán reemplazados por los correspondientes símbolos latinos.

Cabe señalar que el valor del parámetro "Codificación" está directamente relacionado con la longitud máxima del mensaje SMS que puede generar el controlador de eventos: el mensaje SMS en la codificación "UCS2" no puede contener más de 70 caracteres, mientras que la longitud máxima del mensaje en la codificación “Translit” es de 140 caracteres.

El tiempo máximo durante el cual el mensaje SMS está esperando su entrega al destinatario se especifica mediante el parámetro “Intervalo de validez”. Cabe señalar que este intervalo siempre se cuenta desde el momento en que el gestor genera el mensaje SMS. Además, no depende exactamente de dónde está esperando el mensaje SMS para ser entregado al suscriptor: en la lista de espera dentro del manejador de eventos o en el servidor del operador móvil: tan pronto como expire el intervalo de validez del mensaje SMS, intentos para enviarlo se detendrá.

El parámetro “Formato de mensaje” permite configurar una plantilla, según la cual se generarán los mensajes SMS enviados por el manejador. El valor correspondiente a los campos del evento recibido, como el nombre de la clase de evento o el número de sitio, se puede sustituir en mensajes SMS usando macros especiales; si se encuentra una macro mientras se maneja la cadena de formato del mensaje, se reemplazará con el valor del campo de evento correspondiente.

Lista de macros admitidas por el controlador de eventos:

- % date% - fecha de recepción del evento;
- % tiempo% - tiempo de recepción del evento;
- % número% - número de sitio;
- % name% - nombre del sitio;

- % address% - dirección del sitio;
- % phone% - números de teléfono del sitio;
- % channel%: nombre del canal a través del cual se recibió el evento;
- % code% - código de evento;
- % lass% - nombre de la clase del evento;
- % zoneuser% - número de zona o usuario que generó el evento;
- % description%: descripción del evento.

Haga clic en el botón "Variables" para mostrar el menú, desde el cual seleccionar el contenido de la macro que se agregará al valor del parámetro "Formato de mensaje". Por lo tanto, no es necesario recordar la ortografía correcta de la macro deseada, simplemente selecciónela en la lista y agréguela a la cadena de formato.

5.3.7 Reconexión del sitio

El controlador de "Reenganche del sitio" está diseñado para informar a las personas responsables sobre el reenganche del sitio a través de mensajes SMS. Con la ayuda de este manipulador, las personas responsables son informadas sobre la necesidad de volver a cerrar el sitio y sobre la falta de cierre de las personas responsables.

Si es necesario volver a cerrar el sitio, el manejador de eventos envía un mensaje SMS a todas las personas responsables, quienes serán noti fi cadas sobre la necesidad de volver a cerrar de acuerdo con la configuración del módulo “Administrador del sitio”. El mensaje SMS se crea en el formato especificado en la pestaña "Parámetros del mensaje" de la ventana "Parámetros del controlador". De forma predeterminada, el mensaje sobre la necesidad de volver a cerrar el sitio contiene el número, el nombre y la dirección del sitio.

Si la persona responsable se niega a volver a cerrar el sitio, el manejador del evento envía un mensaje SMS a todas las personas responsables, quienes serán noti fi cadas sobre la necesidad de volver a cerrar de acuerdo con la configuración del módulo “Administrador del sitio”. El mensaje SMS se crea en el formato especificado en la pestaña "Parámetros del mensaje" de la ventana "Parámetros del controlador". Por defecto, el mensaje sobre la negativa a volver a cerrar el sitio contiene el apellido y las iniciales de la persona responsable, así como el número del sitio, el nombre y la dirección.

Dispositivo para enviar mensajes SMS

Módem GSM

El gestor de eventos puede enviar mensajes SMS utilizando el terminal GSM basado en el módem GSM “Siemens MC35” (o compatible con él). El módem se conectará directamente a la computadora con el controlador de eventos.

Consulte los detalles sobre el envío de mensajes SMS utilizando el módem GSM en el capítulo sobre el controlador de eventos “Repetidor de mensajes SMS”.

Protocolo SMPP sobre TCP / IP

Para enviar mensajes SMS es posible utilizar la conexión al servidor SMS mediante el protocolo SMPP (TCP / IP).

Consulte los detalles sobre el envío de mensajes SMS a través del protocolo SMPP en el capítulo sobre el controlador de eventos “Repetidor de mensajes SMS”.

Ficha "Parámetros de mensaje"

La pestaña "Parámetros de mensaje" del controlador "Reenganche del sitio" es similar a la pestaña del controlador "Repetidor de mensajes SMS" del mismo nombre: aquí también se establecen los parámetros que definen el formato y el contenido de los mensajes SMS generados por el controlador. Sin embargo, un parámetro como "Número de teléfono" no se especifica para el controlador de eventos "Reenganche del sitio". El número de móvil de la persona responsable se utiliza como número de teléfono al que se enviará el mensaje SMS.

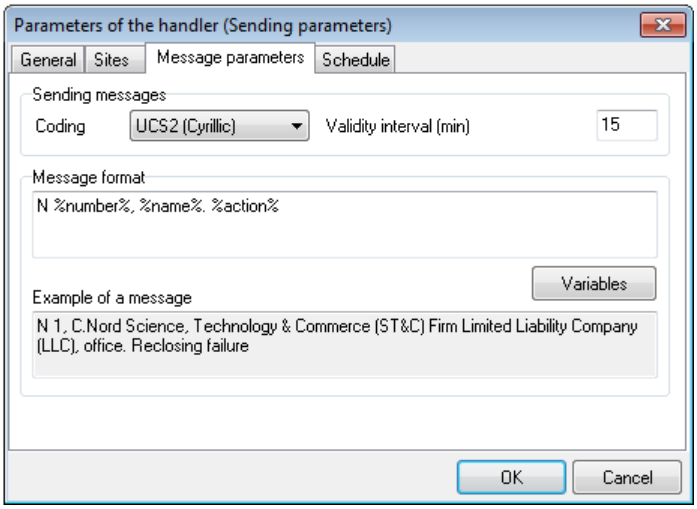


Figura 47: "Reenganche del sitio", ventana "Parámetros del manejador (parámetros de envío)", pestaña "Parámetros de mensaje"

Consulte los detalles sobre otros parámetros de mensajes en el capítulo sobre el controlador de eventos “Repetidor de mensajes SMS”.

5.3.8 Red Pandora

La tarea principal del controlador de eventos “Pandora Network” es organizar el intercambio de información entre instancias independientes del software Security Center. Los eventos, las acciones del operador y las descripciones del sitio se pueden transmitir de un Centro de seguridad a otro.

Cualquier canal que admita el protocolo TCP / IP se puede utilizar como canal de transferencia de información.

Es posible describir con precisión la cantidad de información que se transmitirá en la configuración del controlador de eventos. Por ejemplo, es posible especificar los números e intervalos de los números del sitio, los eventos desde los que se transmitirán, las clases de eventos requeridas para la transferencia, seleccionar las acciones de los operadores, que se transmitirán. Es posible la transmisión recíproca (simultánea) de información.

En primer lugar, el controlador de eventos se utiliza al crear sistemas de monitoreo distribuidos, cuando se combinan varios paneles de monitoreo central y es necesario recopilar información operativa en un solo centro de despacho unificado.

Parámetros de grupo

En la configuración del grupo de manejo de eventos “Red Pandora” es posible especificar la configuración para la conexión y la transmisión de información, así como la configuración que se aplica durante el manejo de la información recibida.

Pestaña "Números de sitio"

En la pestaña "Números de sitio" es posible especificar una lista de sitios, información sobre los cuales recibirá el grupo de controladores, así como los valores del cambio de número de sitio.

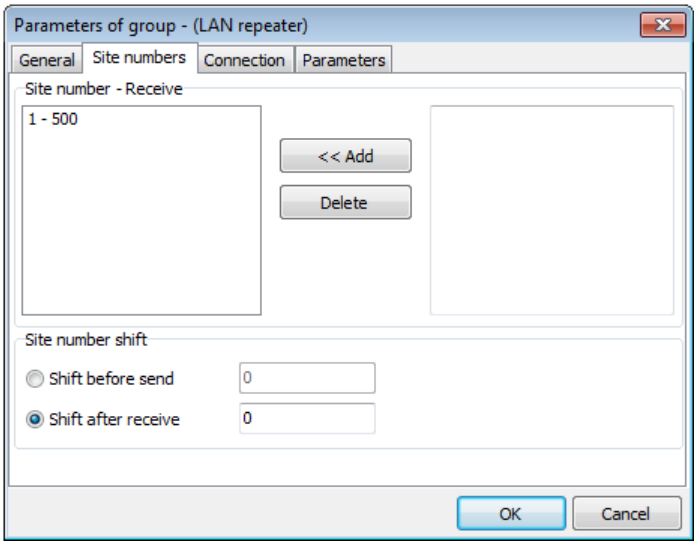


Figura 48: Ventana "Parámetros del grupo (red Pandora)", pestaña "Números de sitio"

El campo "Número de sitio - recibir" está destinado a indicar los números y los intervalos de los números de sitio, cuya información será aceptada por el controlador de eventos.

Para agregar un número o un intervalo de números de sitio a la lista de recibidos, es necesario ingresarlo en el campo de entrada en la parte derecha del campo y hacer clic en el botón “Agregar”. Para eliminar un número o un intervalo de números de sitios de la lista de recibidos, seleccione la línea con el valor que desea eliminar en la lista a la izquierda del campo y haga clic en el botón “Eliminar”.

Al ingresar números de sitio, se permite enumerar varios números o números e intervalos de números separados por comas, por ejemplo: “100, 102, 104, 106-100, 200-299”.

Se entenderá que “información del sitio” significa cualquier información transmitida por el manejador de la “red Pandora”: eventos, tarjetas del sitio, acciones del operador para alarmas. Por lo tanto, si se asume que el manejador de eventos de la “red Pandora” recibe información, los números del sitio en el que se recibe la información se indicarán en el campo “Número del sitio - recibir”.

El parámetro "Shift before send" especifica el valor del sumando que se agregará al número de sitio, antes de enviar información sobre el sitio.

El parámetro "Shift before send" especifica el valor del sumando que se agregará al número de sitio, después de recibir información sobre el sitio.

Se pueden especificar valores negativos para los parámetros “Desplazar antes de enviar” y “Desplazar después de recibir”.

El uso de cambios de número de sitio es especialmente útil si varios paneles de monitoreo central con el mismo número de sitios protegidos están conectados al centro de manejo unificado usando el manejador de eventos de la “red Pandora”. En este caso, es necesario seleccionar el cambio de número apropiado para cada panel, por ejemplo -10000, 20000 y 30 000, y así evitar conflictos.

Pestaña "Conexión"

Utilice la pestaña "Conexión" para especificar la configuración de conexión entre las instancias de los controladores de la "red Pandora".

Dado que el manejador de la “red Pandora” utiliza una red TCP / IP como canal de comunicación, para establecer la conexión entre las dos instancias del manejador, una de ellas actuará como servidor y la otra como cliente.

La función en la que actuará el controlador cuando se establezca la conexión se establece mediante el parámetro "Modo de inicialización de la conexión".

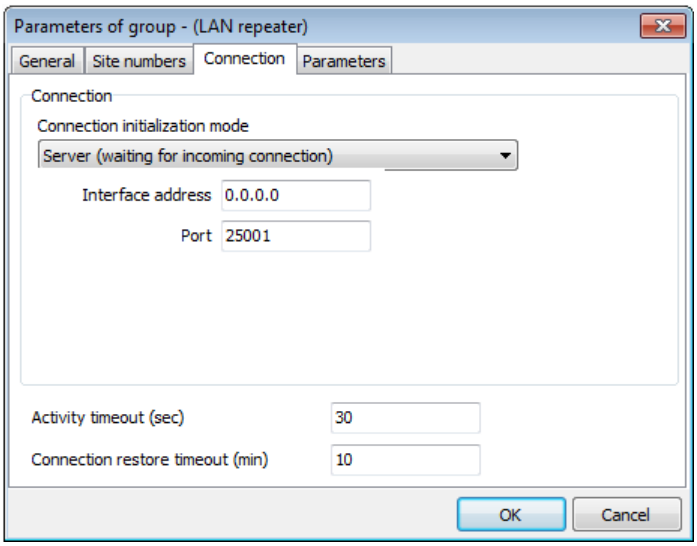


Figura 49: Ventana "Parámetros de grupo (red Pandora)", pestaña "Conexión", modo "Servidor"

Si el controlador de eventos actúa como un servidor y se utilizan varios adaptadores de red con la computadora, o si un adaptador usa varias direcciones IP, entonces usando el parámetro "Dirección de interfaz" es posible especificar la dirección IP en la que el controlador de eventos debe esperar. para la conexión entrante. El parámetro "Puerto del servidor" se utiliza para especificar el puerto al que se espera la conexión.

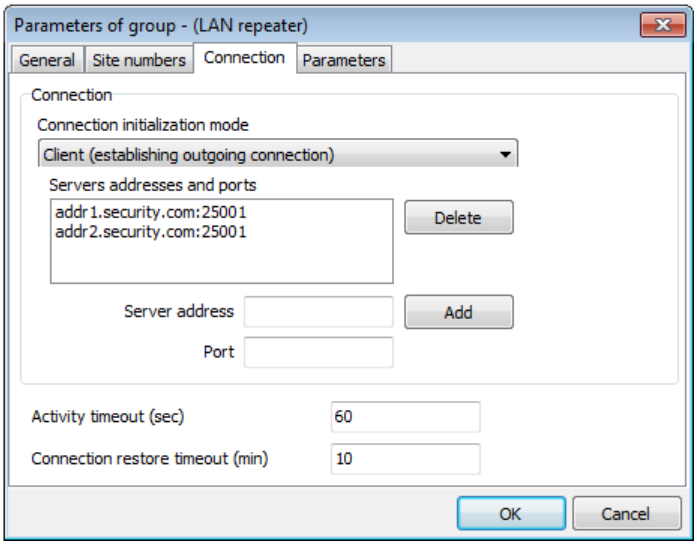


Figura 50: Ventana "Parámetros de grupo (red Pandora)", pestaña "Conexión", modo "Cliente"

Si el manejador de eventos actúa como cliente, es necesario especificar la dirección del servidor y el puerto al que es necesario establecer una conexión.

Cabe señalar que para el manejador de eventos de la “red Pandora” que actúa como cliente, es posible especificar varias direcciones de servidor: en el caso de que no sea posible establecer una conexión con la primera dirección de la lista, el manejador intente conectarse al siguiente y así sucesivamente.

Para agregar la dirección del servidor y el puerto a la lista, es necesario especificarlos como valores para los parámetros “Dirección del servidor” y “Puerto” y hacer clic en el botón “Agregar”.

Para eliminar el servidor, es necesario seleccionarlo en la lista de servidores y hacer clic en el botón “Eliminar”.

Para monitorear la presencia de una conexión en ausencia de información para la transmisión, el manejador de la “red Pandora” puede generar paquetes de prueba y monitorear su recepción. Al hacerlo, el manejador crea los paquetes de prueba, actuando como un servidor, y su recepción es monitoreada por el manejador, actuando como un cliente.

El parámetro “Tiempo de espera de actividad” está destinado a controlar el período de supervisión de la conexión en ausencia de información para la transmisión. Si el manejador actúa como servidor, este parámetro especifica el intervalo con el que el manejador forma el paquete de prueba. Si el manejador actúa como cliente, el parámetro “Tiempo de espera de actividad” especifica el intervalo durante el cual cualquier paquete, incluido un paquete de prueba, se recibirá del servidor. Si no hay paquetes del servidor durante el intervalo especificado en el parámetro "Tiempo de espera de actividad", el controlador que actúa como cliente cierra la conexión.

Al configurar el controlador de eventos de la “red Pandora”, es necesario seleccionar el valor del parámetro “Tiempo de espera de la actividad” en función del ancho de banda del canal de comunicación y su costo de operación. En general, para un controlador que actúa como cliente, se recomienda establecer el valor del parámetro "Tiempo de espera de actividad" aproximadamente dos veces y media más que para el controlador que actúa como servidor. En cuanto al valor del parámetro “Tiempo de espera de la actividad” para el manejador que actúa como servidor, el valor recomendado debe estar dentro del rango de 30 a 300 segundos.

Cuando se establece la conexión a través de un canal de comunicación, el controlador de eventos de la "red Pandora" crea un evento del sistema con el código "ZZYC". Si se pierde la conexión, se crea un evento del sistema con el código "ZZYB". Si el valor del parámetro "Tiempo de espera de restauración de conexión" no es igual a cero, en caso de ausencia prolongada de conexión, los eventos del sistema con el código "ZZYB" se crearán con el período especificado por este valor de parámetro.

Pestaña "Parámetros"

Utilice la pestaña "Parámetros" para configurar los parámetros para controlar la recepción y transmisión de información a través del canal de comunicación.

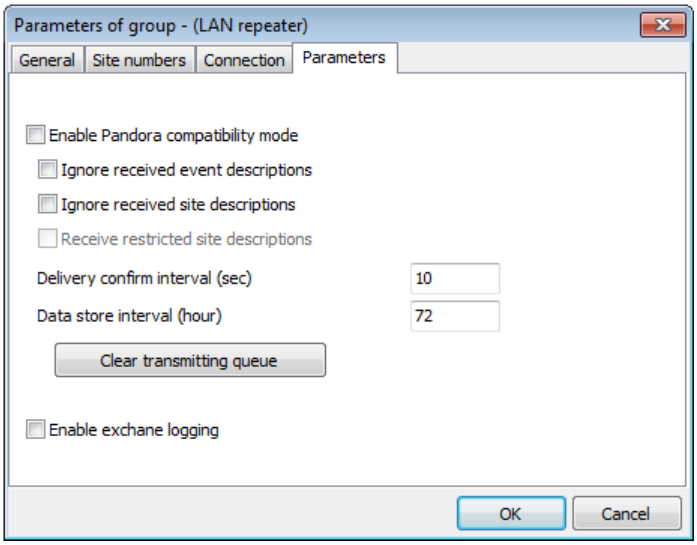


Figura 51: Ventana "Parámetros del grupo (red Pandora)", pestaña "Parámetros"

Si se selecciona el parámetro "Habilitar el modo de compatibilidad de Pandora", el controlador de eventos utilizará un protocolo obsoleto compatible con el software "Pandora" y "Andromeda - Remote Operator" para el intercambio de información. Este protocolo tiene una serie de deficiencias, en particular, no garantiza la entrega de información al destinatario. Se recomienda encarecidamente no habilitar el modo de compatibilidad con “Pandora” al establecer un canal de comunicación entre dos controladores de la “red Pandora”.

Utilice el parámetro "Ignorar descripciones de eventos recibidas" para controlar la recepción de descripciones de eventos. Si no se selecciona este parámetro, no se realiza la decodificación de los eventos recibidos a través del canal de comunicación: la clase de evento, los números de parte y zona y la descripción se almacenan como se recibieron. Si se selecciona este parámetro, solo se tomarán el canal y el código del evento recibido, después de lo cual se decodificará de acuerdo con la plantilla de evento establecida para el sitio como si se recibiera de una fuente de evento local.

El parámetro “Ignorar descripciones de sitio recibidas” permite deshabilitar la recepción a través del canal de comunicación y el almacenamiento en la base de datos de tarjetas de sitio. Si se selecciona este parámetro, se ignoran las descripciones del sitio, que se envían junto con los eventos, así como sus cambios en la instancia remota del Centro de seguridad. Si no se selecciona este parámetro, se sincronizarán las descripciones de los sitios cuya información se transmite a través del canal de comunicación.

Si el parámetro "Habilitar el modo de compatibilidad de Pandora" no está seleccionado, el controlador "Red de Pandora" garantiza la entrega de información al destinatario. Esto se logra con la ayuda de las con fi rmaciones que se envían desde el destinatario después de que la información que ha recibido se registre en la base de datos de Security Center. Utilice el parámetro “Intervalo de confirmación de entrega” para especificar el tiempo durante el cual el controlador de la “red Pandora” espera la confirmación del destinatario. Si no se recibe ninguna con fi rmación durante el intervalo especificado, el manejador de la “red Pandora” enviará la información, que no está con fi rmada, nuevamente.

El valor del parámetro “Intervalo de confirmación de entrega” depende del ancho de banda del canal de comunicación utilizado por el controlador de la “red Pandora” y del rendimiento de las computadoras en las que se está ejecutando el módulo “Administrador de eventos”. Por ejemplo, si se utiliza GPRS como canal de comunicación, para evitar un aumento de avalancha en la cantidad de información en la cola de transmisión, se recomienda aumentar el valor del parámetro “Intervalo de confirmación de entrega” a 90 segundos.

Si no hay conexión, el controlador de la “red Pandora” acumula la información en la cola de transmisión y, una vez que se restablece la conexión, transfiere la información acumulada en la cola. Utilice el parámetro "Intervalo de almacenamiento de datos" para controlar el volumen y la relevancia de los datos que se acumulan en la cola de transmisión. Si el período de almacenamiento de datos en la cola de transmisión es mayor que el valor de este parámetro, dichos datos se eliminarán automáticamente de la cola de transmisión. Además, si el ancho de banda del canal de comunicación se ha deteriorado y hay datos en la cola que no se pueden transmitir, haga clic en el botón “Borrar cola de transmisión” para eliminar forzosamente todos los datos acumulados en la cola para transmisión en el momento.

Marque el parámetro "Habilitar registro de intercambio" para guardar el protocolo de intercambio del controlador de eventos a través de la red TCP / IP en el disco duro de la computadora. Esta información es útil para averiguar las causas de los problemas al establecer una conexión o enviar información a través del canal de comunicación. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

Pestaña "Clases de eventos"

Utilice la pestaña "Clases de eventos" para seleccionar las clases de eventos que el controlador debe transmitir.

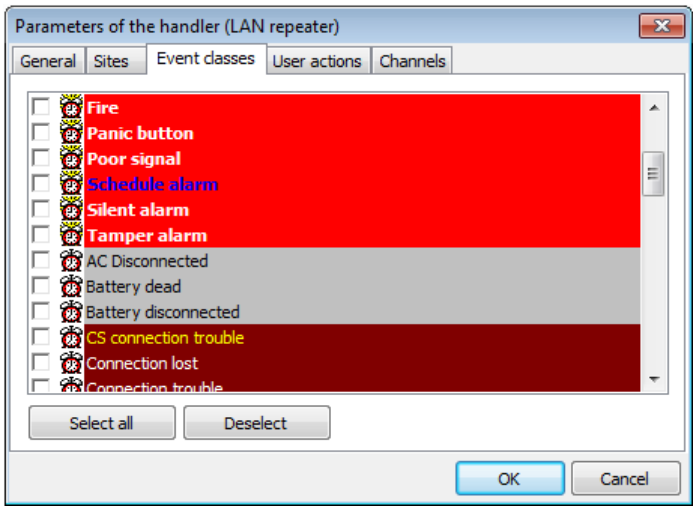


Figura 52: Ventana "Parámetros del controlador (repetidor LAN)", pestaña "Clases de eventos"

Para seleccionar la clase de evento para la transmisión, márquela en la lista. Utilice el botón "Seleccionar todo" para comprobar todas las clases de eventos en la lista. Utilice el botón "Deseleccionar" para deseleccionar todas las clases en la lista que están actualmente seleccionadas para transmisión.

Pestaña "Acciones del usuario"

Utilice la pestaña "Acciones del usuario" para seleccionar las acciones del operador y cancelar las alarmas que transmitirá el manipulador. Cabe señalar que las acciones y cancelaciones que son transmitidas por el manejador se relacionarán con aquellas alarmas cuyas clases se verifican en la pestaña “Clases de eventos”.

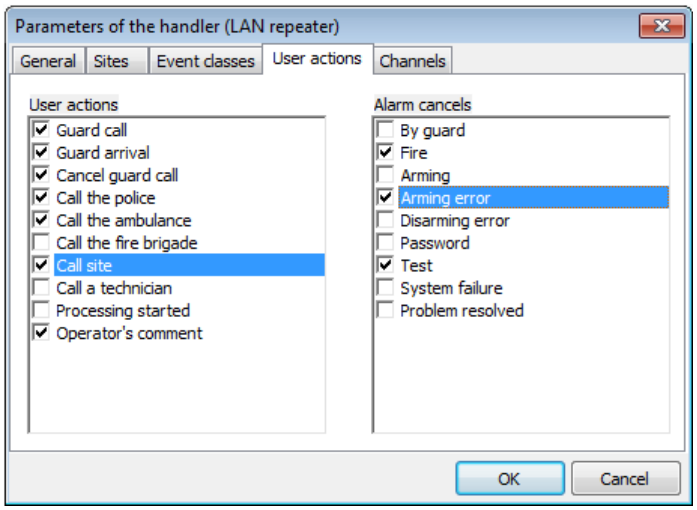


Figura 53: Ventana "Parámetros del controlador (repetidor LAN)", pestaña "Acciones del usuario"

Para seleccionar la acción o cancelar la transmisión, márquelas en la lista.

5.3.9 Repetidor a la nube

Este controlador de eventos está destinado a transmitir información sobre el Centro de seguridad, los sitios, los eventos recibidos, los guardias y las acciones del operador, los ingenieros y sus permisos, así como sobre los enrutadores de video instalados en el sitio, a la “Nube”. La "Nube" es un servicio que permite proporcionar acceso web a sitios y eventos para propietarios, organizaciones de instalación, operadores y guardias.

El controlador "Repeater to Cloud" proporciona la operación de servicios adicionales como el control remoto del equipo del sitio, la aplicación móvil "MyAlarm" y algunos otros. Con más detalle, todos estos servicios se describen en la sección "Servicios en la nube".

El funcionamiento de este manejador es importante para el correcto funcionamiento de todos los servicios en la nube, por eso editarlo es muy limitado. El grupo de controladores de eventos "Repetidor a la nube" y el controlador que contiene se crean durante el primer inicio del módulo "Administrador de eventos" y se habilitan automáticamente si el cuadro de diálogo "Comunicación en la nube" indica la necesidad de utilizar servicios en la nube.

Está prohibido eliminar, copiar o crear otro controlador "Repeater to Cloud". Es necesario cambiar los parámetros de conexión a la “Nube” solo si se utiliza la “Nube Privada”.

Pestaña "Común"

La configuración general del grupo de controladores de eventos "Repetidor a la nube" coincide completamente con la configuración general de los grupos de controladores de eventos, que se describen en detalle anteriormente. Cuando se crea un grupo, se establece automáticamente en "Grupo oculto".

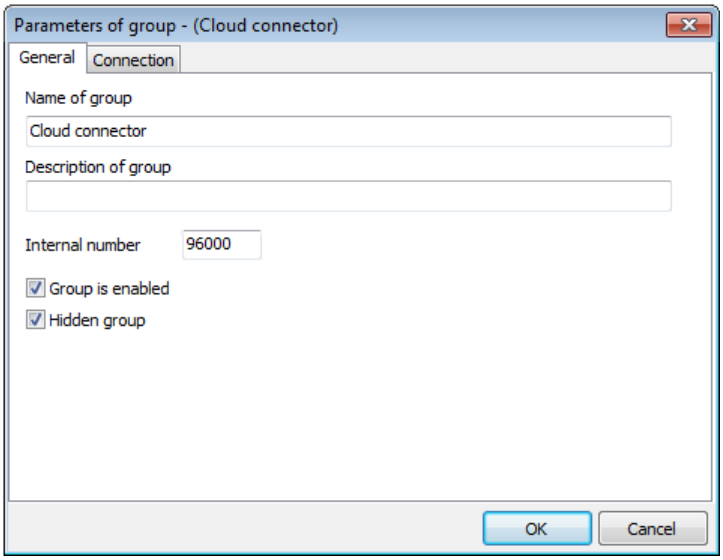


Figura 54: Ventana "Parámetros del controlador (repetidor a la nube)", pestaña "Común"

Pestaña "Canal"

La pestaña "Canal" muestra la dirección y el puerto del servidor, que se utilizan para la conexión a la "Nube". Para conectarse a la "Nube" utilice la siguiente configuración: dirección del servidor - disp.cnord.net, puerto del servidor - 1025. Es necesario cambiar los parámetros sólo si se utiliza "Nube privada".

Marque el parámetro "Habilitar registro de intercambio" para guardar el protocolo de intercambio del controlador de eventos en el disco duro de la computadora. Esta información es útil para averiguar las causas de los problemas al configurar una conexión o enviar información. No se recomienda incluir el registro de intercambio de forma independiente, sin una solicitud del servicio de soporte técnico de C.Nord.

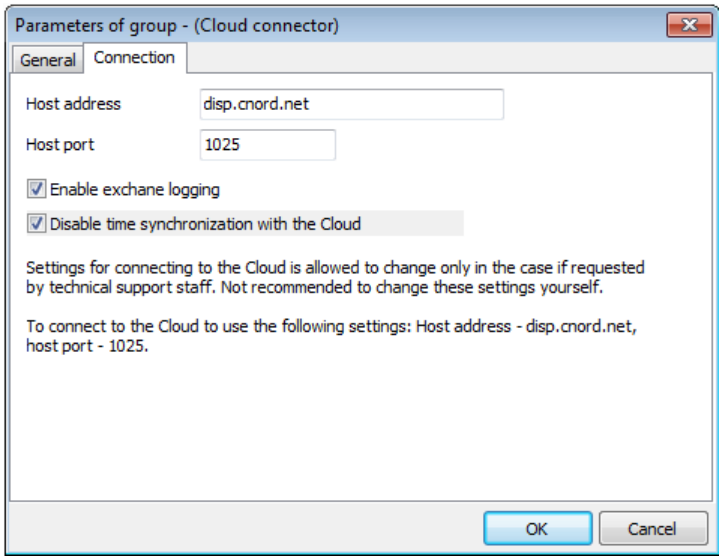


Figura 55: Ventana "Parámetros del controlador (repetidor a nube)", pestaña "Canal"

Si el usuario quiere evitar enviar información innecesaria a la “Nube”, el usuario puede elegir los servicios en la nube que utilizará, y también asegurarse de que solo se envíe a la “Nube” la información necesaria para los servicios seleccionados.

Para limitar la transmisión de información a la "Nube", seleccione "Conexión a la Nube" en el Administrador de eventos.

5.4 Conexión a la nube

Cuando se selecciona la opción "Conexión a la nube", el menú desplegable del mismo nombre aparece en el "Administrador de eventos".

El icono de "Nube" aparece en la barra de estado de la ventana. El color del icono cambia según el éxito de la conexión a la nube y la cantidad de mensajes en la cola de transmisión. Si se establece la conexión a la Nube y el número de mensajes en la cola de transmisión no supera los 100, la Nube será verde. De lo contrario, rojo.

Además, el estado de la conexión a la Nube se muestra en la línea “Comunicación con la Nube” y el número de mensajes en la cola de transmisión en la línea “Mensajes en la cola”.

Hay tres pestañas en la ventana "Conexión a la nube": "Modo de conexión", "Información de contacto" y "UID del Centro de seguridad".

5.4.1 Modo de conexión

Seleccione uno de los modos de conexión a la nube en la pestaña "Modo de conexión" de la ventana "Conexión a la nube". La selección del modo determina los servicios en la nube que se utilizarán y los datos que se transmitirán a la nube.

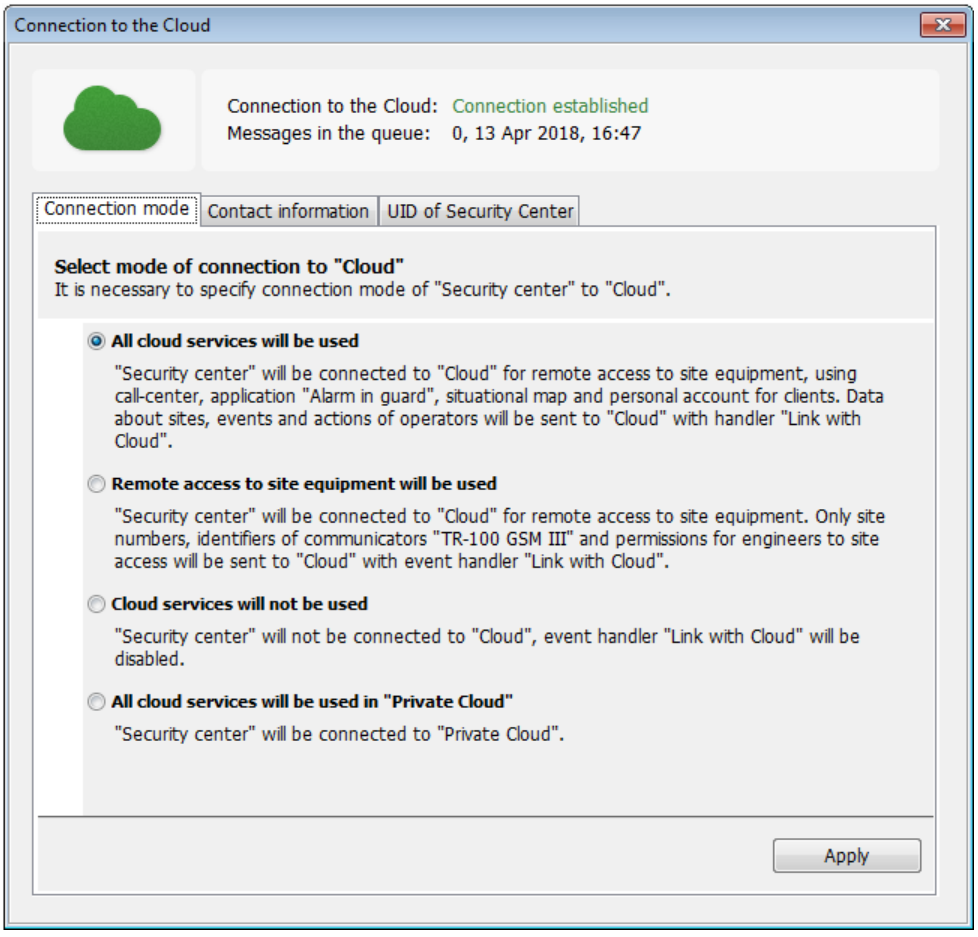


Figura 56: Ventana "Conexión a la nube", pestaña "Modo de conexión"

La integración completa con la nube permite utilizar el acceso remoto a los equipos del sitio, así como a los servicios en la nube disponibles. En este caso, todos los datos sobre sitios, eventos y acciones de los operadores se transmitirán a la “Nube”.

La conexión a la nube solo se puede utilizar para el acceso remoto al equipo del sitio. Este modo de conexión permite

envíe solo números de sitio, identificadores de comunicadores y permisos para que los ingenieros accedan a los sitios de la nube. Otros servicios en la nube se desactivarán y la información sobre ellos no se transmitirá a la nube.

También es posible deshabilitar todos los servicios en la nube y prohibir la transmisión de datos a la nube. Todos los servicios relacionados con el uso de la "Nube" no estarán disponibles. El controlador de eventos "Repeater to Cloud" se desactivará a la fuerza y no se podrá activar. No será posible acceder a la información de registro y UID de Security Center.

También es posible utilizar servicios en la nube en la “Nube privada”, seleccionando la conexión adecuada. Esto proporciona un mayor nivel de seguridad de la información debido a la instalación del software directamente en los servidores de una empresa de seguridad privada. Es posible especificar la dirección del administrador de "Nube privada" para el grupo de controladores "Repetidor a nube" en la pestaña "Canal" de la ventana "Parámetros del grupo".

5.4.2 Información de contacto

La pestaña “Información de contacto” permite cambiar los datos especificados al registrar el Centro de seguridad en la Nube.

Utilice la pestaña para rellenar campos como "Apellido", "Nombre", "Teléfono móvil", "Correo electrónico", "Nombre de la empresa", "Ciudad" y "Dirección". Se requieren campos marcados con un asterisco.

Después de cambiar los datos, haga clic en el botón "Aplicar". En este caso, la información ingresada será transmitida a la Nube.

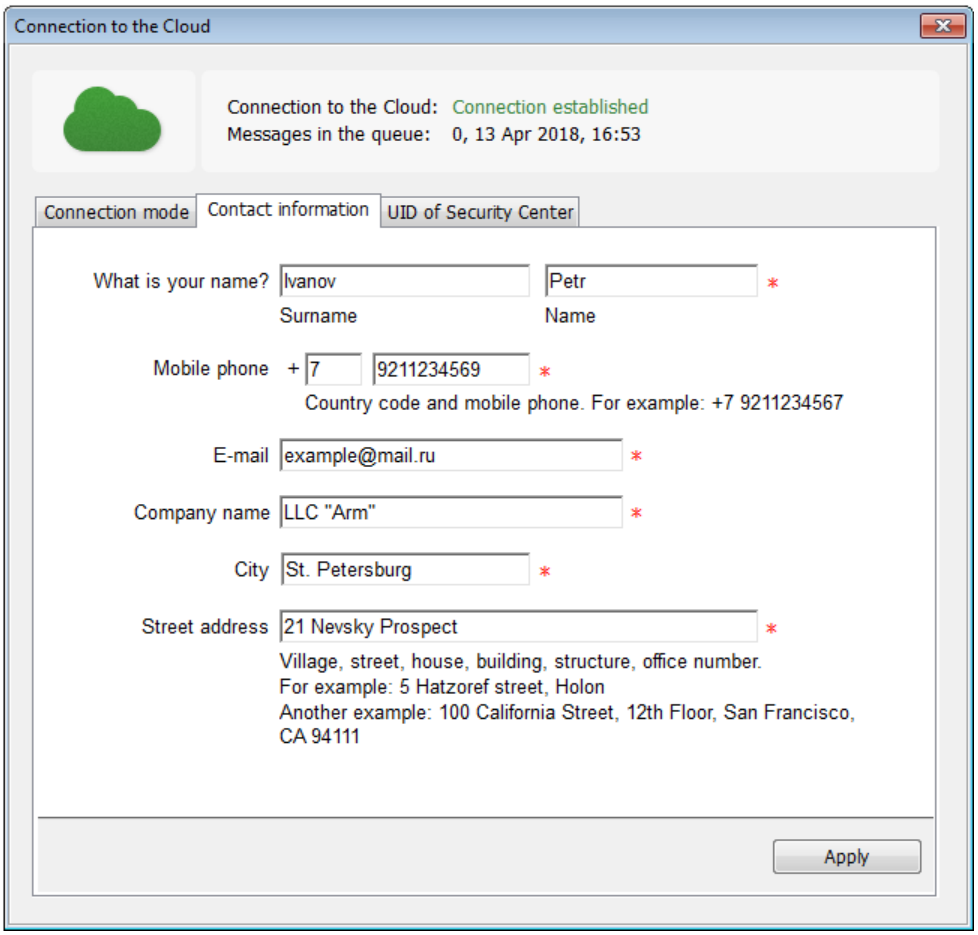


Figura 57: Ventana "Conexión a la nube", pestaña "Información de contacto"

5.4.3 UID del Centro de seguridad

Es posible encontrar el UID del Centro de seguridad utilizado en la pestaña "UID del Centro de seguridad". Para copiar el UID, selecciónelo y haga clic en el icono "Copiar". Esto es conveniente, por ejemplo, para el uso posterior de UID al registrar una cuenta de socio.

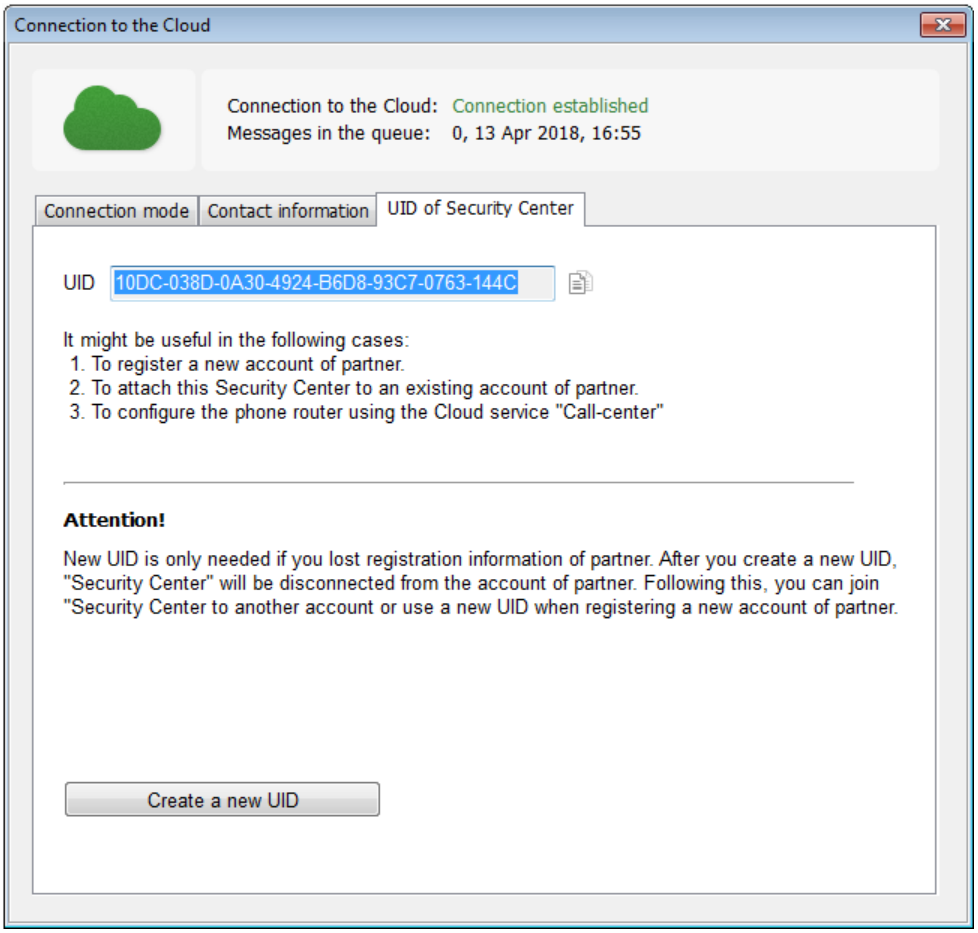


Figura 58: Ventana "Conexión a la nube", pestaña "UID del Centro de seguridad"

Si es necesario volver a registrar la cuenta de socio, cree un nuevo UID. Para hacer esto, haga clic en el botón "Crear un nuevo UID". Utilice el nuevo UID para agregar este Centro de seguridad a otra cuenta o cree una nueva cuenta de socio. Está permitido crear un nuevo UID no más de una vez al día.

5.5 Acerca del software

Cuando se selecciona la opción "Acerca del software", el menú desplegable del mismo nombre aparece en el "Administrador de eventos". Proporciona información sobre la versión del software Security Center, así como información sobre el modo de funcionamiento. El Centro de seguridad se puede utilizar con una llave de seguridad, una licencia temporal o en régimen de arrendamiento.

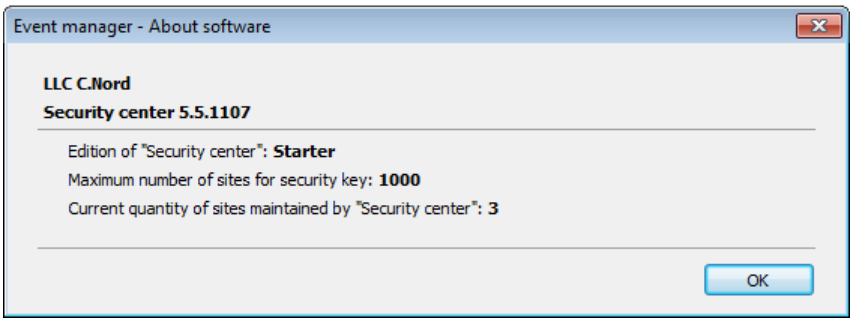


Figura 59: Ventana "Acerca del software"

Si se utiliza la clave de seguridad o la licencia, se indica lo siguiente en la ventana "Acerca del software":

- la edición Security Center;
- número máximo de sitios permitidos para usar;
- número actual de sitios mantenidos por el Centro de seguridad.

Si el Centro de seguridad se utiliza con una clave de seguridad, la información sobre la clave de seguridad también se muestra en la ventana "Acerca del software".

Si el software se utiliza con un archivo de licencia, aquí se indica la información sobre la licencia, así como la fecha de finalización.

6 Administrador del sitio

El módulo "Administrador de sitios" está destinado a administrar la descripción de los sitios disponibles en el software Security Center. Para iniciar el módulo "Administrador del sitio", el usuario debe tener el permiso "Iniciar sesión" para este módulo.

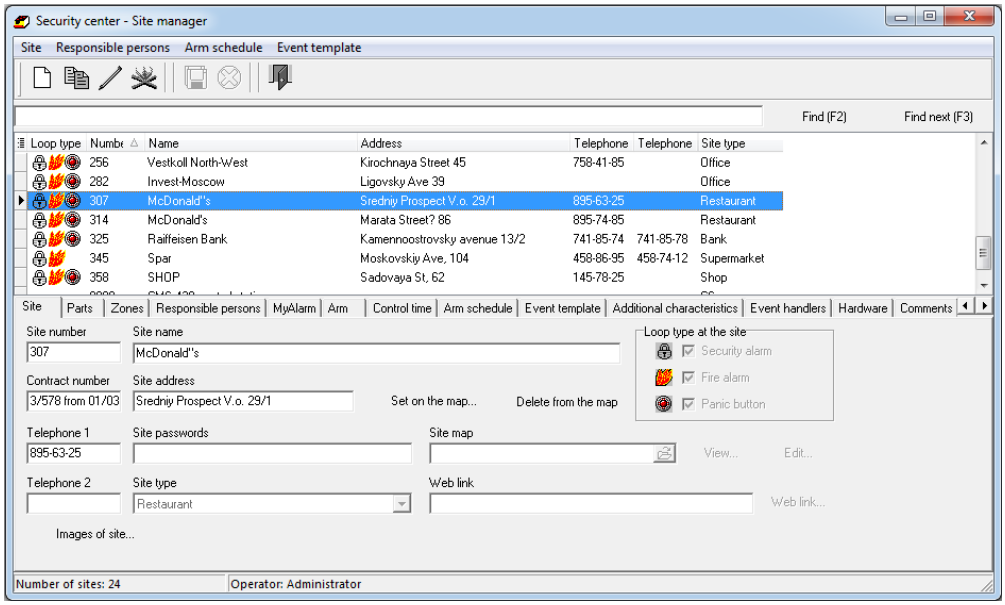


Figura 60: Ventana principal del módulo

La ventana principal del módulo "Administrador del sitio" muestra una lista de los sitios del Centro de seguridad y una tarjeta del sitio actual (seleccionado). Para realizar cualquier operación con el sitio, seleccione el elemento apropiado en el menú. Los elementos de menú más solicitados se duplican en el panel de control del módulo y los paneles de control en las pestañas en las que se agrupan los campos de la tarjeta del sitio.

6.1 Panel de control

Figura 61: Panel de control

Las operaciones, que se controlan mediante botones en el panel de control (enumerados en el orden de los botones):

- Utilice el botón "Crear sitio" para crear un nuevo sitio. Al sitio recién creado se le asigna el primer número de sitio gratuito, que se puede cambiar más tarde.
- El botón "Copiar sitio" tiene como objetivo crear un nuevo sitio y copiar toda la información del sitio actual (seleccionado) en él, excepto el número de sitio y el número de partes del sitio, si corresponde.

Para el número del sitio creado y para el número de partes del sitio, se utilizan los primeros números disponibles, que se pueden cambiar cuando el sitio se edite posteriormente.

- Después de hacer clic en el botón "Editar sitio", el módulo "Administrador del sitio" cambiará al modo de edición de la tarjeta del sitio actual. En el modo de edición, es posible cambiar el valor de los campos de la tarjeta del sitio.

Mientras que en el modo de edición no se permite seleccionar otro sitio de la lista de sitios, es necesario finalizar la edición de antemano, guardando los cambios realizados o descartándolos.

Para cambiar al modo de edición de la tarjeta del sitio, el usuario debe tener el permiso "Editar sitios" para el módulo "Administrador del sitio". Si esto no se especifica específicamente, entonces este permiso es suficiente para realizar cambios en la mayoría de los campos de la tarjeta del sitio.

- Para eliminar un sitio utilice el botón del mismo nombre. Cuando se elimina un sitio, se elimina toda la información asociada con este sitio, incluida la descripción de sus partes, zonas, personas responsables, etc.

Si existe la posibilidad de que se necesite la información sobre el sitio que se va a eliminar, se recomienda que el sitio no se elimine, sino que se cambie al número usando un desplazamiento al área de números de sitio obviamente no utilizados. Por ejemplo, si el sitio 567 ya no está protegido, pero la información en la tarjeta del sitio o los informes sobre eventos recibidos aún pueden ser necesarios, es posible cambiar el número usando el turno de 990000, es decir, el nuevo número de sitio será 990567. Para ocultar dichos sitios al operador de servicio, es posible utilizar el mecanismo de dividir el número de sitios en las computadoras. Ver más información sobre la configuración de este mecanismo, en el capítulo del módulo “Gestor de personal”, apartado “Ordenadores”.

- El botón "Guardar cambios" solo está disponible en el modo de edición del sitio. Presione este botón para guardar todos los cambios en la tarjeta del sitio que se realizaron durante la edición, después de lo cual saldrá del modo de edición.
- Además del botón anterior, el botón "Deshacer cambios" solo está disponible en el modo de edición del sitio. Presione este botón para cancelar todos los cambios realizados durante la edición del sitio, después de lo cual saldrá del modo de edición.
- Haga clic en el botón "Salir del programa" para salir del módulo "Administrador del sitio".

6.2 Lista de sitios

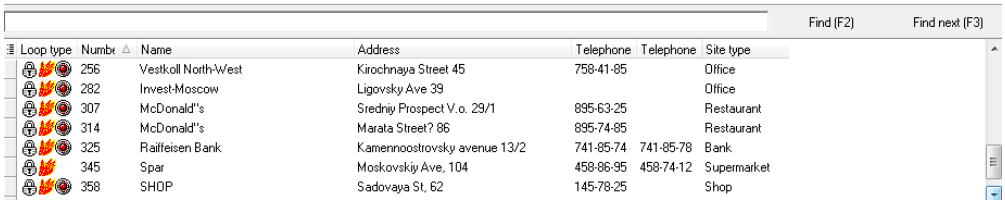


Figura 62: Lista de sitios

El propósito principal de la lista de sitios en el módulo “Administrador de sitios” es encontrar y seleccionar un sitio, información sobre cuál se verá o cambiará.

La búsqueda del sitio se realiza mediante la barra de búsqueda en la parte superior de la lista de sitios. Ingrese una subcadena en el campo de entrada, luego haga clic en el botón “Iniciar” para comenzar la búsqueda desde el principio de la lista de sitios mostrada. Si es necesario continuar la búsqueda, comenzando con el sitio actualmente seleccionado, luego haga clic en el botón "Continuar". Si un sitio que cumple la condición de búsqueda se encuentra en la lista, se seleccionará y se convertirá en el actual. La búsqueda de una subcadena determinada se realiza en todos los campos de uso frecuente de la tarjeta del sitio, como "Número del sitio", "Nombre del sitio", "Dirección del sitio", etc.

6.2.1 Selección de columnas mostradas

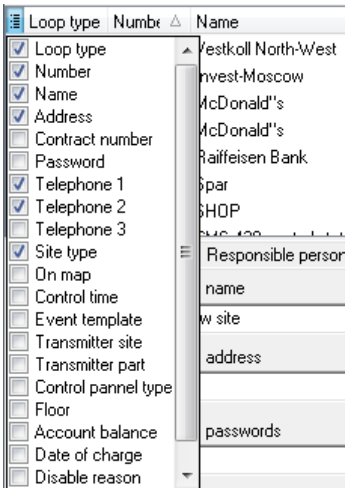


Figura 63: Lista de sitios: selección de columnas mostradas

Será Cabe señalar que es posible seleccionar las columnas que se mostrarán en la lista de sitios. Para hacer esto, haga clic con el botón izquierdo en el botón especial ubicado en la esquina superior izquierda de la lista de sitios y verifique las columnas necesarias en la lista que aparece.

6.2.2 Clasificación de sitios

Los sitios de la lista se pueden ordenar por cualquiera de las columnas mostradas. Para hacer esto, haga clic izquierdo en la columna necesaria. En el encabezado de la columna en la que se realiza la clasificación, se muestra un icono, que es una indicación de clasificación, también especifica el orden de clasificación: ascendente o descendente. Si es necesario ordenar en orden inverso, vuelva a hacer clic en la misma columna.

Es posible ordenar por varias columnas. Para hacer esto, haga clic en el encabezado de la columna, ordenando por qué desea agregar, y mantenga presionado el botón Control en el teclado al mismo tiempo.

6.2.3 Filtrado de sitios durante la visualización

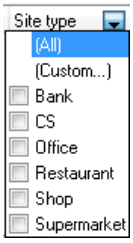


Figura 64: Lista de sitios: botón de filtrado

Otra función útil de la lista de sitios es filtrar por una característica determinada. Por ejemplo, si es necesario mostrar solo sitios del tipo "tienda", haga clic en la flecha que aparece en el encabezado de la columna cuando el cursor del mouse aparece sobre ella y seleccione el tipo de sitio en la lista desplegable.

O, por ejemplo, para asegurarse de que solo los sitios con la palabra "Dixie" se muestren en la lista. Para hacer esto, haga clic en la flecha de configuración de filtrado en la columna y seleccione “Filtro. . . " Articulo. En la ventana es necesario elegir la regla de comparación, dejar que sea "igual" e ingresar la referencia para la comparación - "Dixie".

Se consigue una flexibilidad de filtrado especial gracias a la regla de comparación "similar a". Usando la regla es posible filtrar la lista de sitios, ignorando discrepancias menores en los valores de los campos: para hacer esto, se puede usar un símbolo especial “%” en el valor de referencia, indicando el procedimiento de comparación, que en lugar de él cualquier Puede aparecer una subcadena, incluida una vacía.

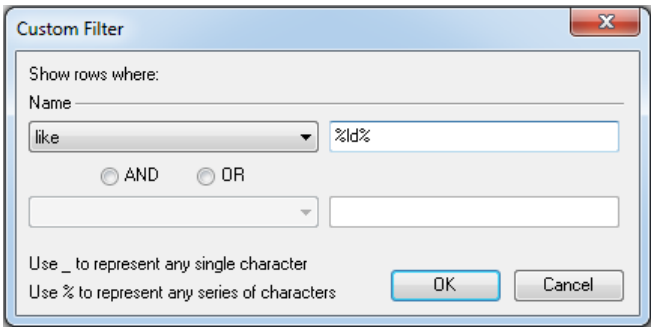


Figura 65: Lista de sitios: ventana de configuración de filtrado

La figura muestra el resultado de filtrar por comparación usando la regla "similar a% id%".

|imgcapt {img / ObjMngr-03-ObjectList-04.png} {Lista de sitios: resultado de filtrar comparando "similar a% ld%"}

6.3 Restauración del sitio eliminado

Para ver la tarjeta del sitio eliminado del Centro de seguridad o generar un informe sobre los eventos en el sitio eliminado, use la función de restaurar un sitio eliminado.

Para restaurar un sitio eliminado, el operador del Centro de seguridad, que tiene el permiso correspondiente, deberá seleccionar “Restaurar sitio eliminado. . . ”Del elemento“ Sitio ”en el menú del módulo“ Administrador del sitio ”.

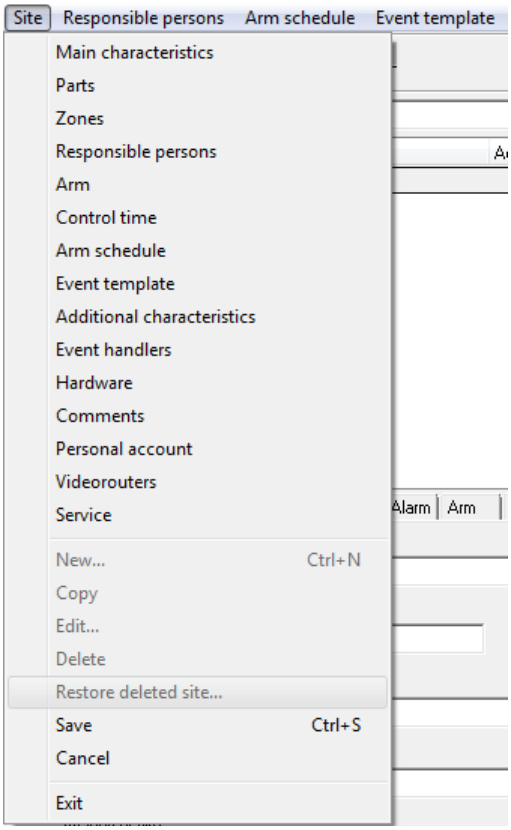


Figura 66: Restaurar el sitio eliminado

La ventana "Seleccionar sitio para restaurar" que se abre muestra los sitios que se eliminaron anteriormente. Para cada uno de ellos, el número de sitios (en el momento de la primera eliminación del sitio), el nombre y la dirección del sitio, el número de contrato, así como la fecha y hora de eliminación del sitio se indican en los campos correspondientes. Es conveniente buscar el sitio que se va a restaurar utilizando estos parámetros clasificando y filtrando los sitios por una característica específica.

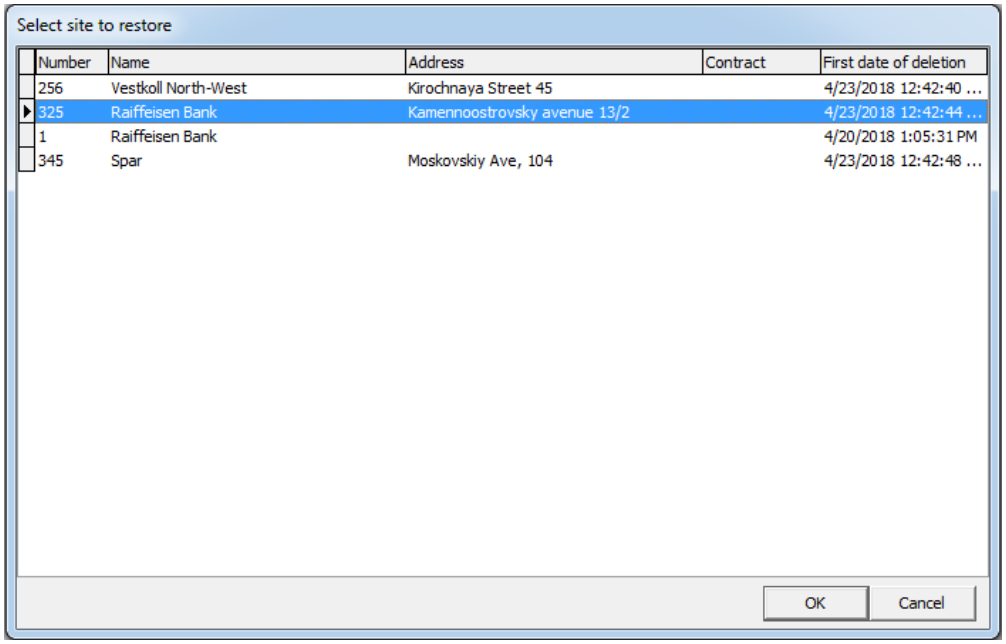


Figura 67: Seleccione el sitio para restaurar

Para restaurar, seleccione el sitio en la ventana "Seleccionar sitio para restaurar" y haga clic en el botón "Aceptar". Después de eso, el sitio

restaurarse y mostrarse en la lista de sitios en la ventana principal del módulo.

En este caso, el número del sitio restaurado cambia, si coincide con el número de sitio o parte ya existente. El cambio de número se logra agregando ciertos símbolos (de “A” a “F”): por ejemplo, el número de sitio “314” se cambia a “A314”. De la misma manera, el número de cualquier parte del sitio restaurado cambia si coincide con el número de sitio o parte ya existente. El número del sitio restaurado y el número de sus partes se informa en una ventana que se abre automáticamente inmediatamente después de que se restaura el sitio.

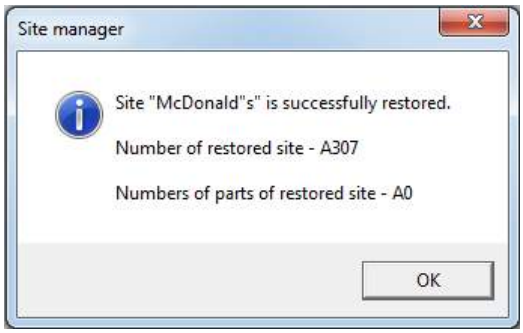


Figura 68: Información sobre el número de sitio restaurado y sus partes

Cabe señalar que para la computadora en la que se está restaurando el sitio, se puede establecer una restricción en los números de sitio disponibles. Si el número del sitio a restaurar excede los límites de esta restricción, el sitio se restaurará, pero aparecerá un mensaje informando al usuario sobre la necesidad de cambiar el número de sitio o cambiar la restricción en los números de sitio disponibles.

Para el sitio, parámetros como el identi fi cador del transmisor TP-100 GSM III, el identi fi cador y la clave de cifrado del dispositivo “Yupiter” no se restauran. Para que se restaure el sitio, el administrador del sitio también se elimina en la cuenta personal y se eliminan las suscripciones a las clases de eventos y las acciones del operador, que estaban disponibles en la aplicación "MyAlarm" antes de la eliminación del sitio. Además, para que el sitio sea restaurado, se cancelan los permisos otorgados a los ingenieros para el acceso remoto a este sitio.

Es importante recordar que la condición necesaria para la restauración del sitio es la capacidad de agregar un sitio a la base de datos del Centro de seguridad de acuerdo con las restricciones de licencia disponibles. Si se crea el número máximo posible de sitios en la base de datos, se muestra un mensaje de error y el procedimiento para restaurar el sitio finaliza.

6.4 Sitio

En la pestaña "Sitio" es posible especificar la información descriptiva básica sobre el sitio: número, nombre, dirección, números de teléfono, etc.

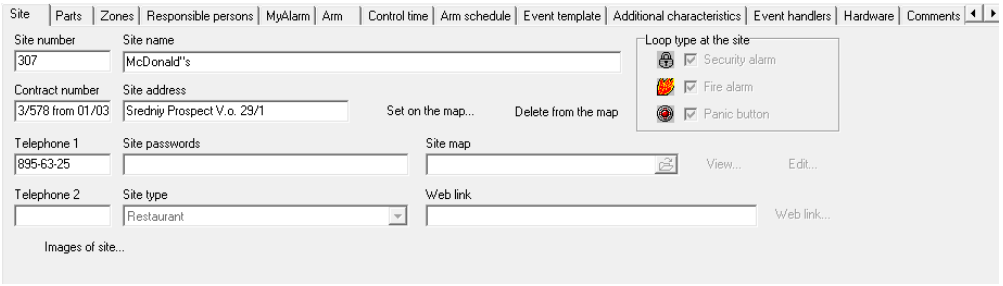


Figura 69: pestaña "Sitio"

6.4.1 Ubicación del sitio en el mapa

Para mostrar el sitio en el mapa de situación, es necesario especificar las coordenadas geográficas del sitio colocándolo en el mapa del terreno.

Para hacer esto, el operador del Centro de Seguridad deberá tener permiso para “Establecer en el mapa”.

Para ubicar el sitio, haga clic en “Establecer en el mapa. . . ”Junto al campo“ Dirección ”en la pestaña“ Sitio ”. No es necesario cambiar al modo de edición para hacer esto. La ventana "Mapa", llamada por esta acción, muestra "Google Maps". El marcador marca la ubicación del sitio. La ubicación se determina de acuerdo con el valor del campo "Ciudad" especificado al registrarse en la "Nube" y el campo "Dirección" especificado en la pestaña "Sitio". Además, la ventana proporciona una breve información sobre el sitio, a saber: número, nombre y dirección del sitio, así como un comentario para el Guardia, ingresado en la pestaña "Comentario".

Al pasar el cursor sobre él y mantener presionado el botón izquierdo del mouse, es posible mover el marcador para indicar una ubicación más precisa del sitio. Para acercar o alejar, use el control deslizante de zoom. Mueve el mapa con el cursor. La lista desplegable permite cambiar el tipo predeterminado de mapa "Esquema" a "Satélite", "Híbrido", "Mapa público", "Mapa público + satélite".

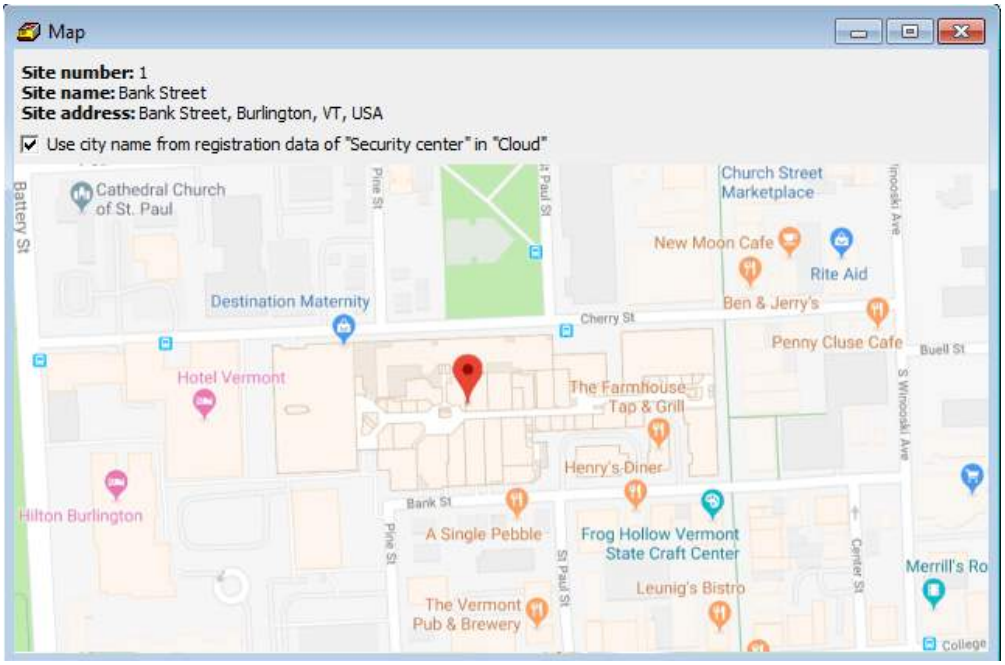


Figura 70: Pestaña "Sitio": configurada en el mapa

Una vez establecido el marcador, haga clic en el botón "Guardar" para guardar los cambios. Las coordenadas del sitio recibidas se almacenarán en la "Nube" y en la base de datos del Centro de seguridad. Una vez que las coordenadas se hayan guardado correctamente, el botón "Eliminar del mapa" estará activo. De lo contrario, será necesario repetir la operación de configurar el sitio en el mapa.

Importante: la configuración de sitios en el mapa es posible cuando se conecta a la nube y cuando los puertos 80 y 443 del protocolo TCP para la computadora, en la que se ejecuta el módulo “Administrador de sitios”, están abiertos.

Para eliminar las coordenadas guardadas del sitio del mapa, haga clic en el botón "Eliminar de la tarjeta" y con fi rme la eliminación. En este caso, la información sobre las coordenadas del sitio se eliminará tanto de la Nube como de la base de datos del Centro de Seguridad.

Si es necesario averiguar si el sitio está configurado en el mapa, consulte la información proporcionada en la lista de sitios del módulo "Administrador del sitio" en la columna "En el mapa". Si esta columna no se muestra en la lista, desactívela. Para hacer esto, marque la columna "En el mapa" en la lista de columnas que se muestran en la lista de sitios haciendo clic con el botón izquierdo en el botón especial ubicado en la esquina superior izquierda de la lista de sitios.

6.4.2 Mapa del sitio

Es posible especificar formatos de archivo BMP y JPG, así como archivos de mapa del sitio creados con el módulo "Mapas del sitio" como valor para el campo "Mapa del sitio". El cambio. . . El botón ”, ubicado junto al campo“ Mapa del sitio ”, está disponible para hacer clic solo si se especifica el archivo del mapa del sitio: cuando se hace clic en él, se iniciará el módulo“ Mapa del sitio ”para cambiar el mapa del sitio.

Al crear y guardar mapas del sitio mediante el módulo "Mapas del sitio", es necesario tener en cuenta que no se realiza la copia de información de los archivos del mapa del sitio a la base de datos del Centro de seguridad. Los archivos de origen se utilizan para mostrar los mapas. Esto es importante cuando se ejecuta el Centro de seguridad en la red local, ya que los archivos de mapa en este caso se almacenarán en un recurso de red accesible para todos los usuarios de la red del Centro de seguridad al menos para su lectura. Además, al crear copias de seguridad de la base de datos de Security Center, no se crea una copia de seguridad de los archivos del mapa del sitio: se solicita al usuario que organice la copia de seguridad de los archivos del mapa del sitio de forma independiente.

Consulte más información sobre la creación de mapas del sitio utilizando el módulo "Mapas del sitio" en la sección dedicada a este módulo.

6.4.3 Enlace web

A pesar del nombre, en el campo "Enlace web" es posible especificar *alguna* archivo y recurso ubicado en la computadora local, en la red local o en Internet, que se puede abrir usando las herramientas instaladas en la computadora.

Al hacer clic en el "Enlace. . . ”En el módulo“ Administrador del sitio ”, o el campo“ Enlace web ”en la tarjeta del sitio en el módulo“ Operador de servicio ”, el comando para abrir el recurso especificado se ejecutará por los medios registrados en el sistema operativo por defecto para este tipo de recurso.

Por ejemplo, en el campo “Enlace web” es posible especificar la dirección (URL) de la página web donde se muestra la transmisión de video desde la cámara instalada en el sitio. Haga clic en el enlace para ejecutar el navegador predeterminado, en el que se abrirá la página especificada.

Del mismo modo, en el campo "Enlace web" es posible especificar la ruta al archivo de descripción del sitio creado en un formato especial (AutoCad, 3D-Max). Haga clic en el enlace para iniciar el programa registrado en el sistema operativo para abrir dicho archivo.

6.4.4 Imágenes del sitio

En el módulo "Administrador del sitio", es posible descargar imágenes del sitio seleccionado desde el disco duro a la Nube o eliminarlo de la Nube.

La aplicación “Alarm to Guard” muestra las imágenes del sitio almacenadas en la Nube desde donde llegó la señal de alarma. Gracias a esto, los empleados de las empresas de seguridad pueden obtener la información necesaria sobre el tipo de sitio y las entradas más convenientes al mismo.

Para cargar y eliminar imágenes, el operador debe tener permiso para "Editar imagen del sitio".

Para trabajar con imágenes, es necesario hacer clic en el botón “Imagen del sitio. . . ”, Sin cambiar al modo de edición del sitio. Luego se abre la ventana del mismo nombre para descargar imágenes, así como para ver y eliminar archivos gráficos ya cargados.

Importante: es posible descargar imágenes a la Nube cuando se conecta a la Nube y cuando los puertos 80 y 443 del protocolo TCP para la computadora, en la que se está ejecutando el módulo “Administrador del sitio”, están abiertos.

Utilice el botón "Seleccionar" en la línea de dirección "Archivos" para seleccionar una o más imágenes del sitio en formatos PNG y JPEG para descargar. El tamaño de la imagen no debe exceder los 5 MB.

Para encontrarlas rápidamente en el disco duro y guardarlas correctamente en la Nube, es mejor poner las imágenes del sitio en la carpeta cuyo nombre corresponde al número del sitio. También es posible asignar los nombres, que comienzan con el número de sitio.

Después de seleccionar los archivos gráficos, haga clic en el botón "Enviar". En este caso, el tamaño de la imagen se reducirá automáticamente al óptimo para mostrar en la tableta en la aplicación móvil "Alarm to Guard". La barra de progreso en el campo "Progreso" muestra el estado de carga de las imágenes seleccionadas. No es posible cerrar la ventana "Imagen del sitio" o seleccionar nuevos archivos gráficos para cargarlos hasta que se complete la descarga.

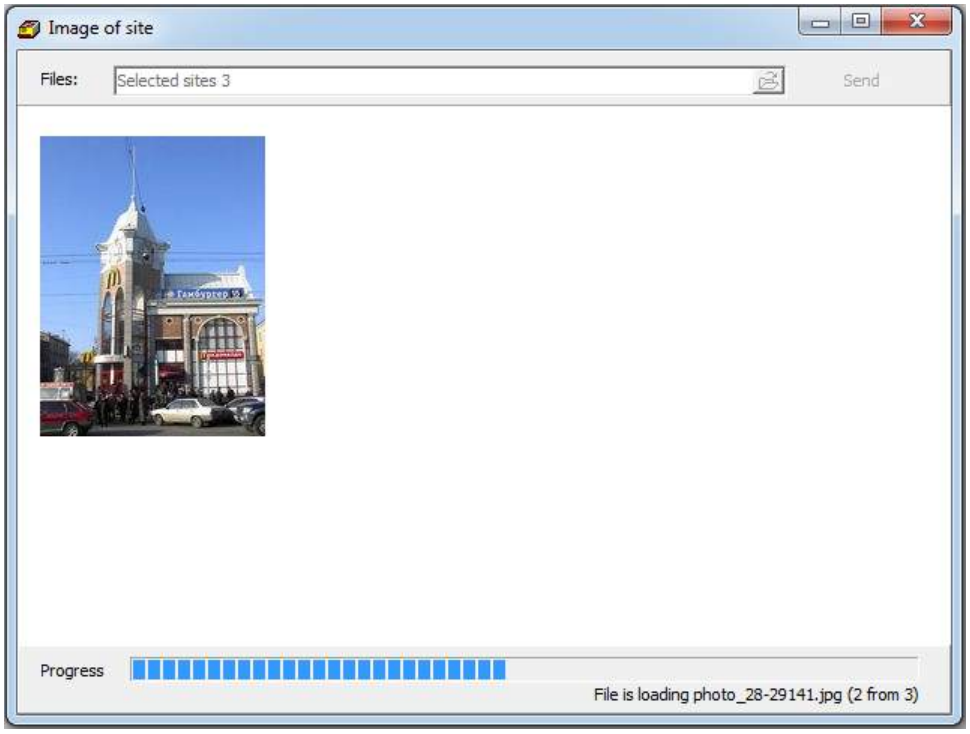


Figura 71: Pestaña "Sitio": imagen del sitio

Mover o eliminar los archivos gráficos, almacenados en la “Nube”, del disco duro no conduce a su pérdida en la Nube. Para eliminar la imagen descargada de la nube, coloque el cursor sobre su miniatura en la ventana "Imagen del sitio" y haga clic en el icono "Cesta" que aparece.

6.5 Particiones

La pestaña "Parts" permite guardar información sobre en qué partes (áreas) se divide el sitio y qué equipo se utiliza para organizar las partes en el sitio.

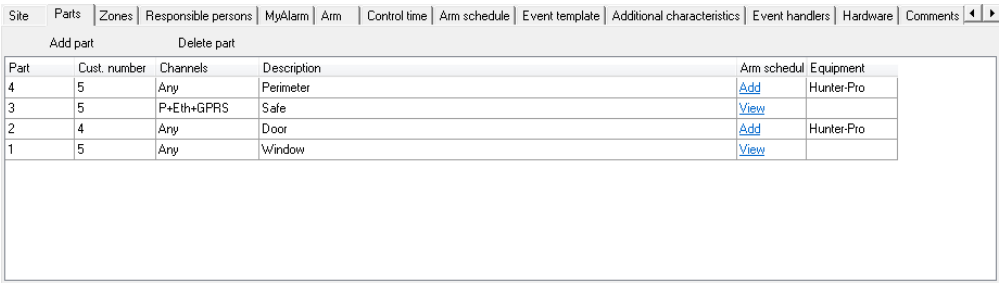


Figura 72: Pestaña "Piezas"

En varios casos, el término "Área" se utiliza en la documentación para los dispositivos del sitio en lugar del término "Parte". No existe una diferencia significativa entre estos términos, el término "Área" se utiliza por razones históricas: una vez que se utilizó en una de las traducciones de la documentación para los dispositivos del sitio y, desde entonces, a menudo se utiliza como sinónimo del término "Parte ”. Además, el término "Clave" es muy común en la literatura rusa, que también es sinónimo del término "Parte".

A veces, el término "Área" se utiliza especialmente para enfatizar la diferencia en el método de codificación de la información transmitida desde el dispositivo del sitio. Por ejemplo, el término "Parte" se utiliza para los dispositivos del sitio que transmiten información en el protocolo "Contact ID", que implica un número de sitio para todas las partes del dispositivo y números de secuencia individuales para cada parte.

A su vez, el término "Área" se utiliza para dispositivos que transmiten información a través de los protocolos de la familia "4/2" (por ejemplo, "EPAF"), donde no hay un campo separado para el número de pieza, y para identificar las piezas. es posible asignarles números de sitio individuales.

El software Security Center admite cualquiera de estos métodos de identificación de piezas en el sitio. Al describir las partes, es posible especificar tanto el número de secuencia como el número del sitio (clave).

Utilice los botones "Agregar parte" y "Eliminar parte" para agregar una nueva parte a la lista de secciones del sitio, o eliminar la parte seleccionada de la lista.

El campo "Parte" se completará si las partes en el dispositivo del sitio tienen números de serie y cuando se envían mensajes desde el sitio se utiliza el protocolo "ID de contacto". Como valor para el campo “Pieza”, se utilizará el número de secuencia de la pieza programada en el dispositivo del sitio.

Si no hay un número de pieza en la información recibida del sitio, entonces el valor del campo “Parte” no importa para Security Center y se puede completar arbitrariamente. Cuando se crea una pieza nueva, se le asigna un número que sigue al número máximo asignado a la pieza existente.

El “Cust. El campo "número" se completará si se utilizan números de sitios individuales para identificar las piezas. El valor de la "Cust. El campo number ”será el número de sitio programado para la pieza en el dispositivo de sitio.

Si no se utilizan números de sitio individuales para identificar partes en el sitio, el valor de la “Cust. El campo "número" puede estar vacío o puede llenarse con el número del sitio al que pertenece el sitio.

El campo "Canal" está destinado a realizar la identificación del sitio desde el cual se recibió el evento en combinación con el valor en el "Cust. campo "número". Por ejemplo, si especifica el número de sitio en el "Cust. número "que es diferente del número de sitio, y establece" Radio "como el valor para el campo" Canales ", entonces el evento recibido del sitio con tal número por radio será tratado como un evento, recibido para este sitio.

El uso de una descripción de partes de este tipo para los sitios puede ser útil en los casos en que se instalan comunicadores adicionales (por ejemplo, transmisores de radio) en sitios ya equipados, pero los números de los sitios en los que están instalados ya se utilizan en el canal de radio. . En este caso, es posible programar el panel para que se usen diferentes números de sitio por teléfono y radio, usando estos números y tipos de canales de comunicación al describir las partes del sitio.

Si el campo “Canal” en la configuración de la sección no se usa para identificar el sitio, se recomienda usar el valor “Cualquiera” como valor para este campo.

En el campo "Descripción", es posible especificar una línea arbitraria que describa la parte del sitio para los empleados del centro de monitoreo. Puede ser una descripción de las zonas o habitaciones incluidas en la pieza u otras características de la organización de la pieza.

Si el software Security Center puede identificar la parte en la que se recibió el evento, entonces la descripción de la parte se utilizará para formar una descripción de los eventos recibidos del sitio: el valor especificado en el campo "Descripción" se sustituirá en la descripción. del evento en lugar de la macro %% part %%.

En el campo "Programación de armado" de la pestaña "Partes" para cada una de las partes del sitio hay enlaces "Agregar" o "Ver". El enlace "Agregar intervalo" redirige a la pestaña "Programación de armado", donde ya se ha seleccionado la parte correspondiente para la programación. El enlace "Ver" está disponible cuando ya se ha creado el programa de armado de la pieza. Haga clic en el enlace "Ver" para abrir el programa creado en la pestaña "Programación de armado".

Como valor para el campo “Equipo”, es posible especificar el tipo de equipo del sitio que se utiliza para organizar la pieza. Esta función es útil si se instalan varios dispositivos de sitio en el sitio.

El valor del campo "Equipo" se puede seleccionar de la lista. Es posible cambiar el contenido de esta lista en el módulo "Configuración del sistema", en la pestaña "Campos del sitio", campo "Equipo de parte del cliente".

Para guardar los cambios realizados en los campos de descripción de las piezas, es necesario con fi rmarlos presionando el botón “Enter” después de completar la entrada de los valores.

6.6 Zonas

En la pestaña “Zonas”, es posible describir en detalle las coberturas de protección del sitio, incluyendo información sobre los equipos utilizados y la distribución de zonas en las partes del sitio.

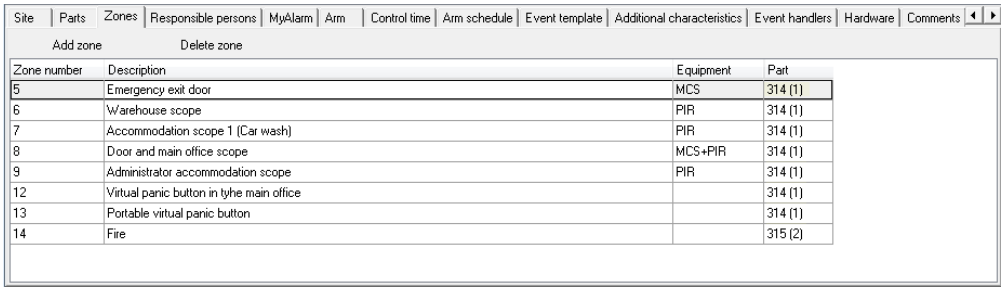


Figura 73: Pestaña "Zonas"

La información sobre las zonas es una parte muy importante de la descripción del sitio, ya que se utiliza al generar la descripción de los eventos recibidos del sitio. Por ejemplo, si se recibe una alerta del sitio en la zona uno, la descripción del evento, que será creada para su manejo por el operador del Centro de seguridad, será sustituida por la descripción de la zona uno de la tarjeta del sitio.

Utilice los botones "Agregar zona" y "Eliminar zona" para agregar una nueva zona a la lista de zonas del sitio, o eliminar la zona seleccionada de la lista.

El campo "Número de zona" está destinado a indicar el número de la zona descrita. El valor de este campo será el número de secuencia de la zona programada en el dispositivo del sitio.

En el campo "Descripción", es posible especificar una línea arbitraria que describa la zona del sitio para los empleados del centro de monitoreo. Como regla general, la descripción contiene un nombre de la habitación o la cobertura de protección a la que pertenece la zona.

Como valor para el campo “Equipo” es posible especificar la lista de equipo del sitio que se utiliza para organizar la zona.

El valor del campo "Equipo" se puede seleccionar de la lista. Es posible cambiar el contenido de esta lista en el módulo "Configuración del sistema" - en la pestaña "Campos del sitio", campo "Equipo de la zona del cliente".

Como valor para el campo “Clave” es posible especificar la parte a la que pertenece esta zona. Si el dispositivo del sitio está dividido en varias partes, entonces, al especificar partes en la descripción de las zonas, obtendremos información detallada.
sobre el organización de las coberturas de protección en el sitio.

6,7 Personas responsables

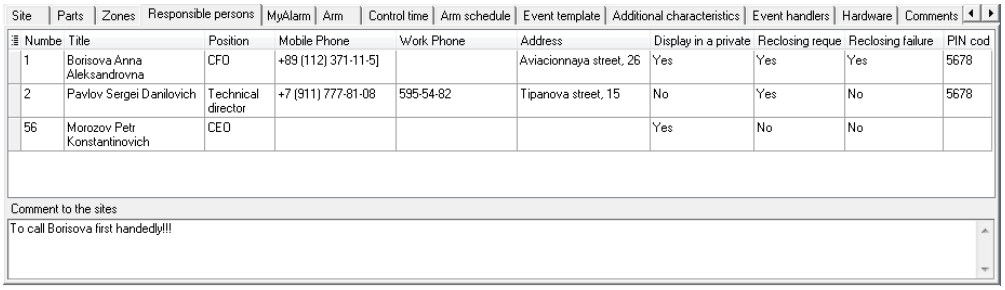


Figura 74: Pestaña "Personas responsables"

Utilice los botones "Nuevo" y "Eliminar" para agregar una persona nueva o eliminar a la persona seleccionada de la lista.

Utilice los botones "Arriba" y "Abajo" para cambiar el orden de las personas responsables en la lista. El orden de las personas responsables en la tarjeta del sitio en el módulo "Operador de servicio" corresponde al orden que se puede configurar en la pestaña "Personas responsables".

Haga clic en el botón "Editar" en el panel principal del módulo "Administrador del sitio" en la pestaña "Personas responsables" para editar los valores de campo de la persona responsable del sitio.

El campo “Número” se completará si el usuario, que tiene el código personal del armado / desarmado del sitio, se indica como la persona responsable. En este caso, el número de usuario programado en el dispositivo del sitio se especificará como el valor del campo "Número" para la persona responsable.

Si la persona responsable descrita no posee el código personal del armado / desarmado del sitio, entonces se puede usar un valor vacío para el campo “Número”.

Además del número de usuario de la persona responsable, es posible especificar otra información necesaria: nombre, cargo, números de teléfono móvil y particular, dirección.

Si el campo "Mostrar en una cuenta privada" tiene "Sí", la persona responsable se mostrará en la lista de personas responsables en la aplicación "Cuenta personal".

Con fi gure la noti fi cación automática de la persona responsable sobre la necesidad de volver a cerrar el sitio utilizando el campo "Reconexión". Si el valor es “Sí”, la persona responsable recibirá un SMS con información sobre el sitio que necesita ser abierto, inspeccionado y resguardado una vez eliminada la causa de la alarma.

Para que la persona responsable reciba SMS con información sobre la persona que se negó a llegar para el reenganche del sitio, es necesario establecer el valor en “Sí” en el campo “Fallo de reenganche”.

En el campo “Código PIN”, es posible cambiar el código PIN del responsable de la verificación del botón de pánico, así como confirmar el armado o desarmado del sitio (al solicitar el código PIN). Si antes de cambiar los códigos PIN de todas las personas responsables del sitio eran los mismos, aparecerá una ventana preguntando si es necesario cambiar el código PIN de todas las personas responsables del sitio.

El campo "Comentarios a las personas responsables" tiene como objetivo agregar información adicional sobre las personas responsables del sitio. Si es necesario, este campo se puede ocultar.

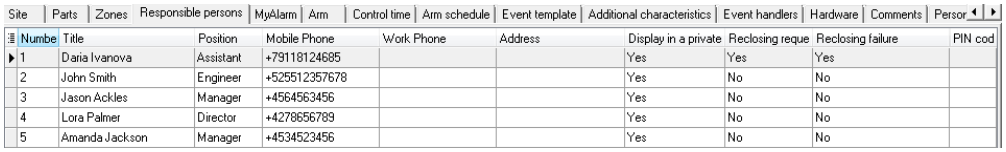
Si las personas responsables describen a los usuarios con los códigos personales de armado / desarmado, entonces la información sobre el usuario, que realizó el armado o desarmado, se incluirá en la descripción del evento manejado por el operador del Centro de Seguridad.

6.8 MyAlarm

La pestaña MyAlarm es necesaria para controlar el acceso de los usuarios a la aplicación MyAlarm.

Cuando ingresa a la aplicación, la información sobre el sitio no está disponible hasta que el usuario inicia sesión en el Centro de seguridad y no se le otorgará acceso a él.

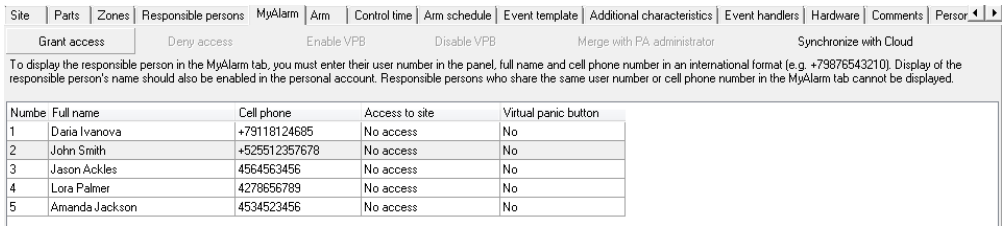
Para que la lista de usuarios aparezca en la pestaña “MyAlarm”, es necesario crearla en la pestaña “Responsables”. Es necesario especificar de forma obligatoria el número, nombre y apellidos, así como el teléfono móvil. En ausencia de uno de los valores, la línea con el usuario no aparecerá.



Numbe	Title	Position	Mobile Phone	Work Phone	Address	Display in a private	Reclosing reque	Reclosing failure	PIN cod
1	Daria Ivanova	Assistant	+79118124685			Yes	Yes	Yes	
2	John Smith	Engineer	+525512357678			Yes	No	No	
3	Jason Ackles	Manager	+4564563456			Yes	No	No	
4	Lora Palmer	Director	+4278656789			Yes	No	No	
5	Amanda Jackson	Manager	+4534523456			Yes	No	No	

Figura 75: Lista de personas responsables de la pestaña Myalarm

Los usuarios no pueden acceder a los sitios después de ser invitados a la aplicación. Para abrir el acceso, es necesario hacer clic en el botón "Permitir acceso", luego la aplicación mostrará el sitio.



Numbe	Full name	Cell phone	Access to site	Virtual panic button
1	Daria Ivanova	+79118124685	No access	No
2	John Smith	+525512357678	No access	No
3	Jason Ackles	4564563456	No access	No
4	Lora Palmer	4278656789	No access	No
5	Amanda Jackson	4534523456	No access	No

Figura 76: Botón "Permitir acceso"

Hay dos tipos de acceso:

- Usuario: ve el estado de todas las particiones y recibe notificaciones sobre el cambio de estado;
- Administrador del sitio: ve el estado de todas las particiones y recibe notificaciones sobre el cambio de estado, controla el estado del sitio. Puede invitar a otros usuarios a la aplicación MyAlarm sin el Centro de seguridad.

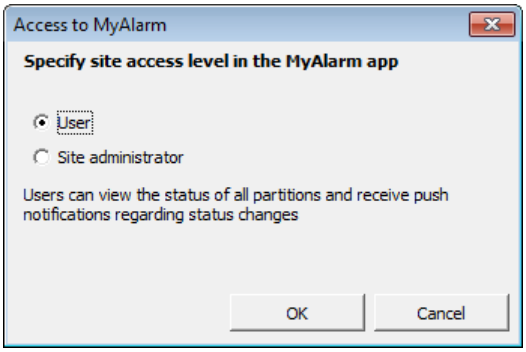


Figura 77: Tipos de acceso en MyAlarm

Para restringir el acceso, es necesario hacer clic en el botón "Denegar acceso". Después de eso, no se mostrará el sitio en la aplicación.

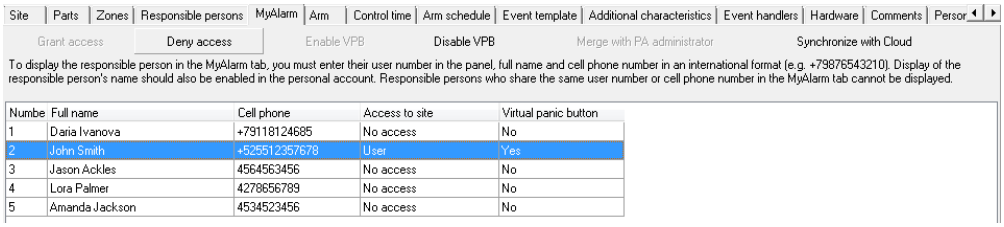


Figura 78: Botón "Denegar acceso"

* * “Activar botón de pánico” **. Muestra un botón de pánico virtual en MyAlarm, que se puede utilizar para llamadas de emergencia.
a un sitio. Funciona como un verdadero botón de pánico, pero está en el teléfono inteligente, lo que permite llamar a la ayuda independientemente de la ubicación del usuario. Una empresa de seguridad puede controlar el acceso al botón para cada usuario a través del Centro de seguridad.

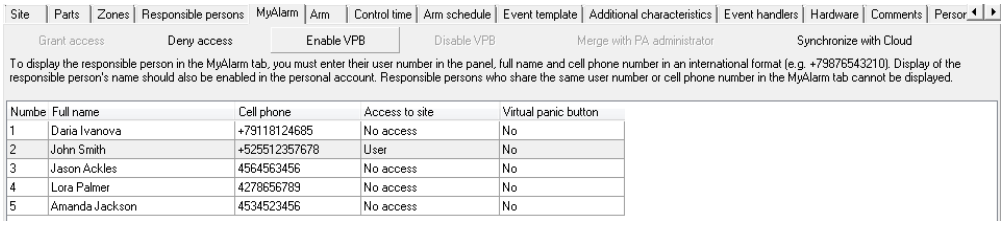


Figura 79: Botón "Permitir botón de pánico"

Para eliminar el botón de pánico de la aplicación, es necesario hacer clic en el botón "Desactivar botón de pánico".

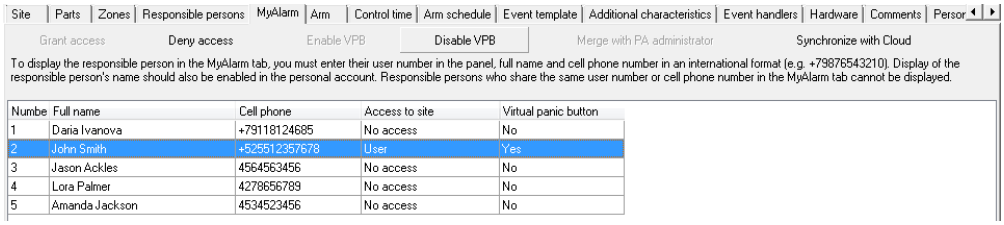


Figura 80: Botón "Desactivar botón de pánico"

“Sincronizar con la nube”. Usando el botón “Sincronizar con la Nube”, es posible solicitar la lista de usuarios de MyAlarm desde la Nube y sincronizarla con la lista de usuarios del sitio. El botón funciona solo si hay al menos un usuario en la pestaña MyAlarm.

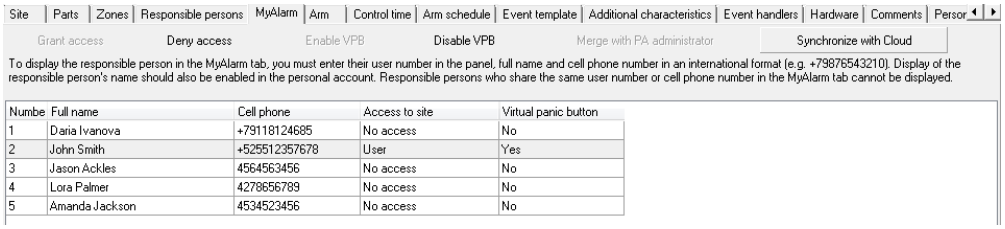


Figura 81: Botón "Sincronizar con la nube"

6.9 Armado

En la pestaña "Armar" es posible cambiar los parámetros asociados con las reglas de protección del sitio y la protección.

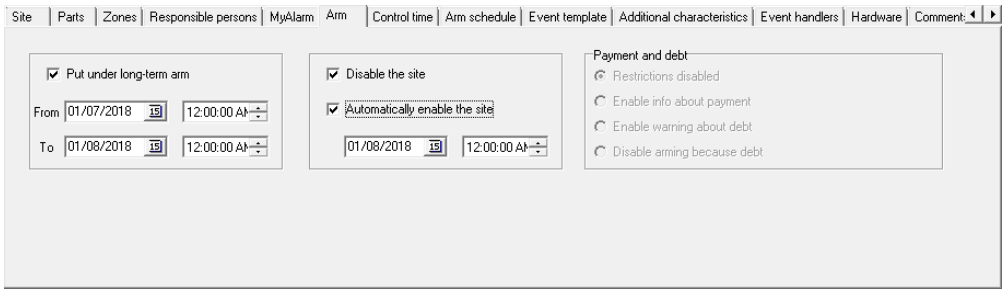


Figura 82: Pestaña "Armar"

6.9.1 Amado de larga duración

El campo "Poner bajo brazo a largo plazo" está diseñado para habilitar el modo de protección a largo plazo de un sitio e indicar la duración del modo. La protección a largo plazo está destinada a controlar situaciones en las que el sitio, por alguna razón, estará bajo protección durante mucho tiempo.

La protección a largo plazo del sitio se supervisa de la siguiente manera:

- al comienzo de la protección a largo plazo, se verifica el hecho del armado del sitio;
- si el sitio no está armado, se crea un evento del sistema con el código “ZZXC”. Si el sitio continúa no armado, el evento del sistema con el código "ZZXC" se repetirá con el intervalo especificado por el valor del parámetro "Periodicidad de alarma de programación de armado" especificado en la configuración del módulo "Administrador de eventos";
- Si durante el intervalo especificado como tiempo de protección a largo plazo, el sitio se desarma, se creará un evento del sistema con el código "ZZXE", después del cual el ciclo de monitoreo de la protección a largo plazo comenzará de nuevo - con la generación del evento del sistema con el código "ZZXC" y la expectativa del armado del sitio.

Para cambiar los parámetros de protección a largo plazo del sitio, el usuario deberá tener el permiso "Editar brazo a largo plazo" para el módulo "Administrador del sitio".

6.9.2 Deshabilitación del sitio

El campo "Deshabilitar sitio" está diseñado para deshabilitar el sitio, a partir de un momento determinado. Si el sitio está deshabilitado, los eventos recibidos de él se manejan de la siguiente manera:

- al recibir cualquier evento del sitio en el módulo "Operador de servicio", el sonido se apaga. Es decir, todos los eventos continúan mostrándose, los eventos con tipos de clases de “Armado” y “Desarmado” continúan cambiando el estado del sitio, pero no hay sonido al recibir eventos de este sitio;
- al recibir eventos con el tipo de la clase “Alarma”, se cancelan automáticamente. Es decir, si el sitio está deshabilitado y de él sale una alarma, además de que no hay sonido de alarma, esta alarma también se cancela automáticamente.

Si el sitio está deshabilitado, el parámetro “Habilitar el sitio automáticamente” permite encenderlo en el momento especificado sin la intervención del operador.

Para deshabilitar sitios, el usuario debe tener el permiso "Editar deshabilitación" para el módulo "Administrador del sitio".

6.9.3 Armado / Desarmado por Operador de Servicio

Si el equipo instalado en el sitio no implica la posibilidad de armar o desarmar, puede ser útil emular los eventos de armado o desarmado por parte del operador de servicio. Para habilitar esta función, configure el parámetro "Permitir armado y desarmado condicional por operador de servicio" en la configuración del sitio.

Una vez establecido este parámetro, aparecerá un elemento en el menú contextual de este sitio en el módulo "Operador de servicio", lo que permitirá crear un evento que cambiará el estado actual del sitio.

Por ejemplo, si el sitio está actualmente armado, el elemento del menú contextual se llamará "Desarmar" y cuando se seleccione, se creará un evento del sistema que tiene el tipo predeterminado de la clase "Desarmar".

6.10 Control de tiempo

La pestaña "Tiempo de control" está destinada al control de uno de los parámetros más importantes del control de la operación del sitio.

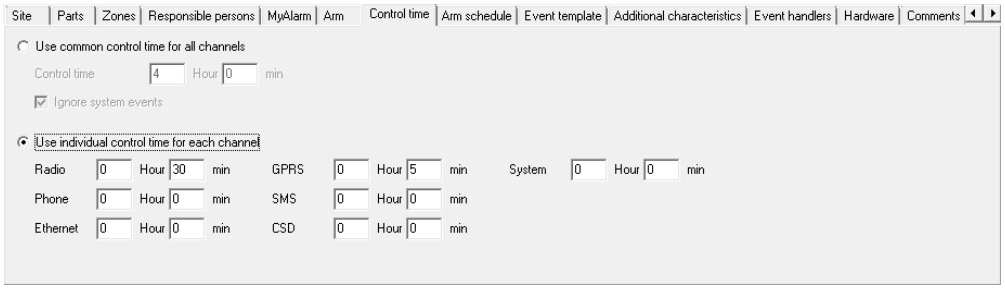


Figura 83: Pestaña "Control de tiempo"

El tiempo de control del sitio es el intervalo de tiempo durante el cual se recibirá cualquier evento del sitio. Se entenderá que el término "tiempo de control" difiere en significado del término "control de autotest". Durante el control de autotest, se espera que el sitio envíe eventos bastante específicos. Pero si estamos hablando del tiempo de control del sitio en el software Security Center, durante su manejo, se tienen en cuenta los eventos recibidos del sitio.

Si es necesario controlar la aprobación de la prueba o cualquier otro evento específico, es posible utilizar los controladores de eventos de “Monitoreo de eventos” o “Monitoreo de la cadena de eventos”. Puede encontrar más detalles sobre el propósito y cómo utilizar estos controladores de eventos en la sección del módulo "Administrador de eventos".

Es posible configurar el tiempo de control del sitio para monitorear por separado todos los canales de comunicación utilizados por el sitio.

Si se selecciona el elemento "Usar tiempo de control común para todos los canales", el software Security Center tomará en cuenta cualquier evento del sitio recibido a través de cualquier canal de comunicación al manejar el tiempo de control del sitio.

Este enfoque para establecer el tiempo de control del sitio es útil si el sitio usa solo un canal de comunicación para transmitir mensajes o si la transmisión de señales a través de canales de comunicación de respaldo no es periódica de alguna manera.

El parámetro “Tiempo de control” permite configurar las horas y minutos durante los cuales se recibirá un evento desde el sitio. Si durante el tiempo especificado no se reciben eventos del sitio, entonces un evento del sistema con el "ZZXA"

Se creará un código para este sitio. Si se recibe algún evento del sitio dentro del tiempo especificado, se reiniciará el intervalo de espera de eventos.

Si se especifica 0 como valor para el parámetro “Tiempo de control”, se desactivará el manejo del tiempo de control para este sitio.

El parámetro “Ignorar eventos del sistema” permite ignorar los eventos creados en el software Security Center al manejar el tiempo de control. No se recomienda deshabilitar este parámetro sin ninguna razón en particular cuando se monitorean eventos recibidos de sitios reales.

Seleccione el elemento "Usar tiempo de control individual para cada canal" si el sitio está equipado con comunicadores que funcionan a través de varios canales de comunicación y es necesario monitorear el funcionamiento de cada canal de comunicación independientemente del otro. Si se selecciona este elemento, es posible configurar el tiempo de control para cada tipo de canal de comunicación por separado. Al gestionar un tiempo de control individual, solo se tienen en cuenta los eventos recibidos a través del canal de comunicación controlado. Si no hay eventos dentro del intervalo especificado para el sitio, se creará un evento del sistema con el código “ZZXAx”, donde x será una cifra de 1 a 7 correspondiente al tipo de canal de comunicación monitoreado:

- "ZZXA1" - Sistema
- "ZZXA2" - Radio
- "ZZXA3": teléfono
- "ZZXA4": Ethernet
- "ZZXA5": GPRS
- "ZZXA6": SMS
- "ZZXA7" - CSD

Para los eventos que se crean para el sitio como resultado de la operación de los algoritmos del Centro de seguridad, "Sistema" siempre se especifica como el canal de recepción, es por eso que el parámetro "Ignorar eventos del sistema" no está presente al configurar el tiempo de control individual. para cada canal de comunicación: también se puede especificar el tiempo de control para el canal “Sistema”.

De forma predeterminada, los eventos con códigos “ZZXA” - “ZZXA7” se describen en todas las plantillas de eventos como alarmas, es decir, requieren el registro de las acciones del operador para su manejo y cancelación. Si es necesario, es posible cambiar la descripción del evento. Consulte la información sobre cómo hacer esto en el capítulo de esta descripción dedicado al módulo “Configuración del sistema”.

6.11 Programación de armado

En la pestaña "Programación de armado" es posible especificar los períodos de tiempo para cada día de la semana en que el sitio o sus partes serán armados, y también habilitar el monitoreo de esta regla por parte del Centro de Seguridad.

Para realizar cambios en la configuración del programa de armado, el usuario debe tener el permiso "Editar programa" para el módulo "Administrador del sitio".

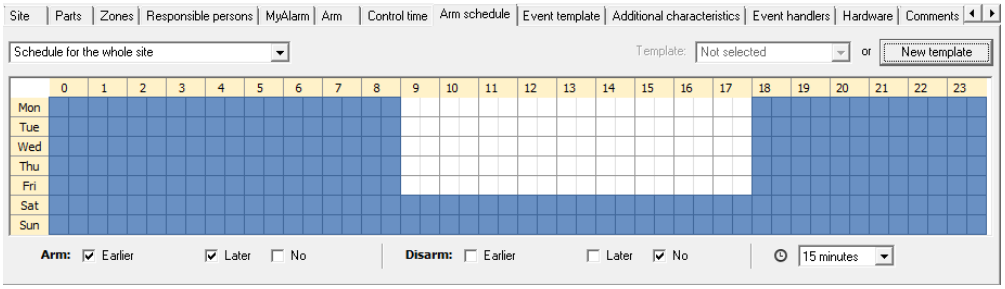


Figura 84: Pestaña "Programación de armado"

Es posible hacer un cronograma de brazos para todo el sitio y para cada una de sus partes. De forma predeterminada, la pestaña está configurada en el modo "Programar para todo el sitio". Este modo se utilizará al hacer un cronograma de armado para todo el sitio, es decir, para todas sus partes. Si es necesario crear un cronograma de armado para una o más partes del sitio, use el menú desplegable. Aquí están todas las partes creadas para el sitio, cada una de las cuales se puede seleccionar para hacer un cronograma separado.

En la tabla se indica el horario de armado del sitio o sus secciones, cuyas líneas corresponden a los días de la semana de lunes a domingo, y columnas a los intervalos de treinta minutos del día.

Las celdas de la mesa son de color azul, cuando indican el momento en que se armará el sitio o sus partes. Si la celda es blanca, el sitio o sus partes en el tiempo especificado serán desarmados.

Para agregar un intervalo durante el cual se armará un sitio o sus partes, es necesario dibujar un cuadrilátero correspondiente al intervalo deseado con el mouse. Para eliminar un intervalo del tiempo de protección de un sitio o sus partes, realice la misma operación.

Si el intervalo dibujado captura tanto el área azul como la blanca, aparecerá una ventana con dos botones: "Agregar intervalo" y "Eliminar intervalo". Si el sitio o sus partes se van a armar durante el intervalo de tiempo seleccionado, haga clic en el botón "Agregar intervalo". Si el sitio o sus partes deben desarmarse, haga clic en el botón "Eliminar".

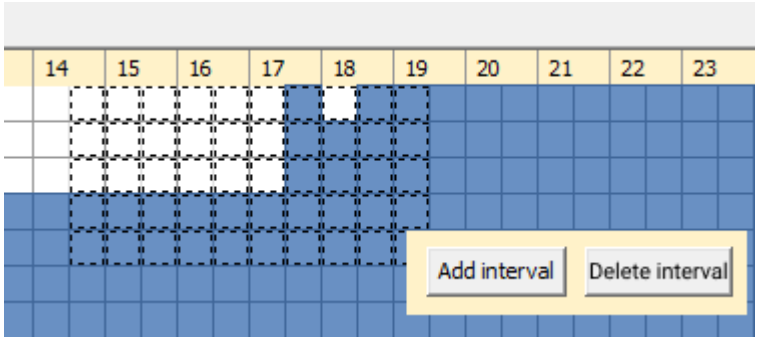


Figura 85: Pestaña "Programación de armado"

Es posible configurar los parámetros de control de programación utilizando las casillas de verificación ubicadas en la parte inferior de la pestaña. Al marcar las casillas necesarias, especifique los estados monitoreados del sitio armado.

Figura 86: Pestaña "Programación de armado": control de programación del sitio

El control de armado se configura usando los siguientes parámetros presentados en la línea "Armado":

- "Más temprano". Este parámetro permite obtener información sobre el hecho de que el sitio fue armado antes de lo indicado en el horario de armado. Si el sitio se armó antes, se genera un evento del sistema con el código "ZZWA". Por lo tanto, el jefe de la empresa protegida puede recibir una notificación por SMS de que los empleados abandonaron el lugar de trabajo antes de la hora prevista.
- "Mas tarde". Este parámetro permite obtener información sobre el hecho de que el sitio fue armado más tarde de lo indicado en el horario de armado. Si el sitio se armó más tarde, se genera un evento del sistema con el código "ZZWB". Por lo tanto, el jefe de una empresa protegida puede ser noti fi cado vía SMS sobre el retraso de tiempo de los empleados en el lugar de trabajo.
- "No". Este parámetro permite obtener información sobre el hecho de que el sitio está desarmado mientras que según el horario de armado estará armado. En este caso, se crea un evento del sistema “ZZXB”, que se repetirá con un intervalo especificado por el parámetro “Periodicidad de alarma de programación de armado”, antes de que se arme el sitio o hasta el momento en que se pueda desarmar el sitio. El parámetro "Periodicidad de alarma de programación de armado" se establece en la configuración del módulo "Administrador de eventos".

El control de desarmado se configura utilizando los siguientes parámetros presentados en la línea "Desarmar":

- "Más temprano". Este parámetro permite obtener información sobre el hecho de que el sitio fue desarmado antes de lo indicado en el horario de armado. Si el sitio se desarmó más tarde, se genera un evento del sistema con el código "ZZXD".

- "Mas tarde". Este parámetro permite obtener información sobre el hecho de que el sitio fue desarmado más tarde de lo indicado en el cronograma de armado. Si el sitio se desarmó más tarde, se genera un evento del sistema con el código "ZZWD". Así, el jefe de la empresa protegida puede ser noti fi cado vía SMS sobre el momento del desarme del sitio, es decir, el momento de llegada de los empleados al lugar de trabajo.
- "No". Este parámetro permite obtener información sobre el hecho de que el sitio está armado mientras que de acuerdo con el horario de armado debe estar desarmado. En este caso, se crea un evento del sistema con el código "ZZWC". Por lo tanto, el director de una empresa protegida puede recibir una notificación por SMS de que los empleados no llegan a tiempo al lugar de trabajo.

En el campo indicado por el ícono del temporizador, se establece el rango de tiempo, durante el cual se permite cualquier violación en el horario de los sitios (el valor máximo del parámetro es de 30 minutos). Por ejemplo, menos 15 minutos desde la hora de armado y más 15 minutos desde la hora de desarmado en la programación de sitios.

Supongamos que el horario de armado del sitio es de 21:45 a 09:15. Con una desviación aceptable de 15 minutos, se permite el armado de 21:30 a 21:45 y el desarmado de 09:15 a 09:30.

De forma predeterminada, los eventos con códigos “ZZXB” y “ZZXD” se describen en todas las plantillas de eventos como alarmas, es decir, requieren el registro de las acciones del operador para su manejo y cancelación. Si es necesario, es posible cambiar la descripción del evento. Consulte la información sobre cómo hacer esto en el capítulo de esta descripción dedicado al módulo “Configuración del sistema”.

Si en la versión anterior del Security Center se configuró el control de programación del sitio armado para el sitio, cuando se actualice el software, se habilitarán los parámetros “Sin armado programado” y “Desarmado temprano”. Los parámetros restantes para controlar la programación del sitio estarán deshabilitados.

Es posible crear una plantilla de programación de armado basada en la programación de armado. Para hacer esto, cree un horario de brazo para el sitio o su parte y haga clic en el botón "Nueva plantilla". Cabe señalar que el botón "Nueva plantilla" está disponible para hacer clic solo si se agrega al menos un intervalo de tiempo al programa.

En la ventana "Nueva plantilla de programación de armado" que se abre, se proporciona la programación de armado utilizada para crear la plantilla. Especifique el nombre de la plantilla y haga clic en el botón "Crear plantilla" en esta ventana.

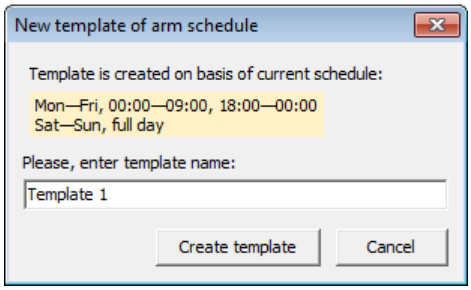


Figura 87: Pestaña "Programación de armado": nueva plantilla

Para aplicar una plantilla al sitio o su programa de armado parcial, haga lo siguiente:

seleccione la plantilla requerida en el menú desplegable en el campo "Plantilla".

El programa de armado se puede editar. Para hacer esto, seleccione el elemento "Editar" en el menú desplegable del campo "Plantilla". Todas las plantillas creadas se muestran en la ventana "Editar plantilla de programación de armado". Haga clic en la línea de la plantilla requerida para ingresar un nuevo nombre. Además, la plantilla se puede eliminar haciendo clic en el enlace "Eliminar" en la línea de la plantilla y con fi rmando la eliminación de la plantilla.

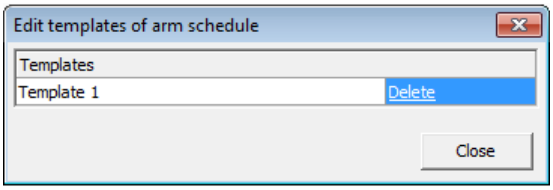


Figura 88: Pestaña "Programación de armado": edición de plantilla

6.12 Plantilla de evento

La pestaña "Plantilla de evento" está destinada a cambiar la plantilla de código de evento, que se utiliza para decodificar eventos recibidos del sitio, deshabilitar eventos de alarma y para cambiar las propiedades de un código de evento específico para este sitio.

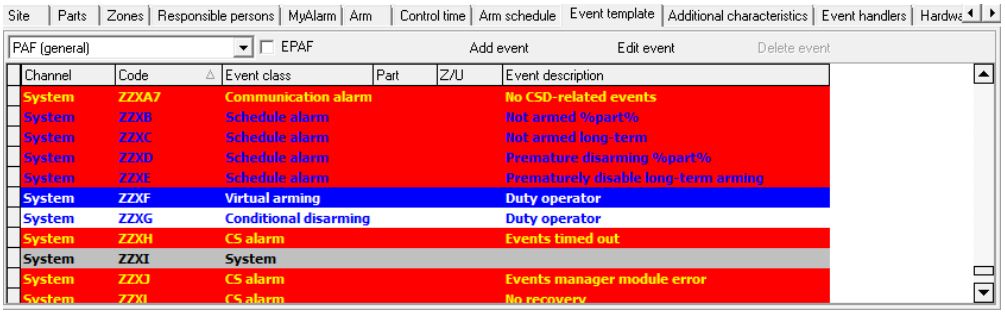


Figura 89: Pestaña "Plantilla de evento"

La plantilla de evento que se utilizará para decodificar eventos del sitio se puede seleccionar de la lista en la esquina superior izquierda de la pestaña.

Para cambiar la plantilla de evento utilizada por el sitio, el usuario debe tener el permiso "Cambiar plantilla de evento" para el módulo "Administrador del sitio".

Utilice el botón "Agregar evento" para agregar un nuevo evento a la plantilla de eventos del sitio. Utilice el botón "Cambiar evento" para cambiar la descripción del evento seleccionado. Se entenderá que los cambios realizados afectarán únicamente a este sitio y no se reflejarán ni en la plantilla de código de evento utilizada por el sitio ni en ningún otro sitio.

Haga clic en el botón "Eliminar" para eliminar un evento que se agregó a la plantilla de este sitio, o un evento, cuya descripción se modificó para este sitio. Los eventos que pertenecen a la plantilla de código de evento utilizada por el sitio no se pueden eliminar.

Para cambiar la descripción de los eventos, el usuario deberá tener el permiso "Editar plantilla de evento" para el módulo "Administrador del sitio". No es necesario ingresar al modo de edición para realizar cambios en la descripción de la plantilla de evento.

Si cambia los eventos de la plantilla, los cambios en la base de datos se guardan inmediatamente después de que el usuario haya realizado cambios en el evento de la plantilla. No es posible deshacer cambios.

Al crear un nuevo evento o cambiar un evento existente, es posible especificar todos los atributos del evento en la ventana "Editar evento".

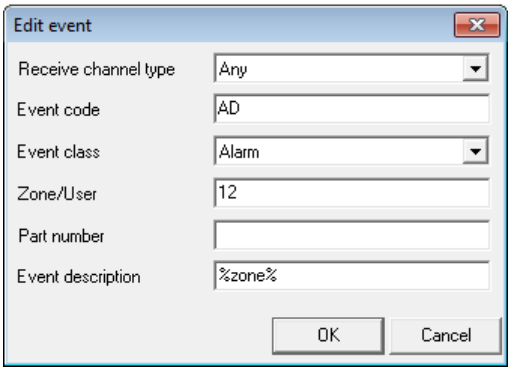


Figura 90: Ventana "Editar evento"

Se ofrece una descripción detallada de los campos de eventos en el capítulo sobre el módulo "Configuración del sistema" en la sección que describe la pestaña "Plantilla de eventos".

Debido al hecho de que los cambios en la plantilla de eventos para un sitio en particular son extremadamente difíciles de controlar, se recomienda no usarlos sin una necesidad especial.

La desactivación de un evento de alarma que se puede realizar mediante el botón "Desactivar evento", por su valor, es muy similar a la desactivación de un sitio, con la única diferencia de que se trata de un solo código de evento. Al recibir un evento de discapacidad en el

Módulo "Operador de servicio", no hay sonido para el evento, y el "Administrador de eventos" crea una cancelación automática para esta alarma. Se debe enfatizar que, a diferencia de cancelar una alarma para un sitio deshabilitado, cancelar una alarma para un evento deshabilitado cancelará solo este evento; el armado del sitio continúa en su totalidad, excepto por el código de evento deshabilitado.

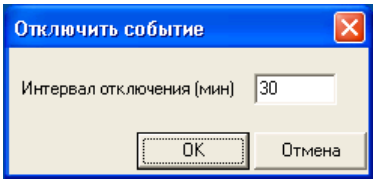


Figura 91: Ventana "Desactivar evento"

El evento se puede desactivar solo por un intervalo de tiempo limitado, que se indica cuando se realiza la desactivación. Después de este intervalo, el evento se habilitará automáticamente. Es posible habilitar el evento desactivado manualmente en cualquier momento haciendo clic en el botón "Activar evento".

Todas las operaciones para deshabilitar y habilitar el evento van acompañadas de la creación de eventos del sistema. Por ejemplo, cuando un evento está deshabilitado, se genera un evento del sistema con el código "ZZXM", cuando el evento se deshabilita automáticamente, se crea un evento del sistema con el código "ZZXN" y cuando el operador habilita el evento (habilitación manual), se genera un evento del sistema con el código “ZZXO”.

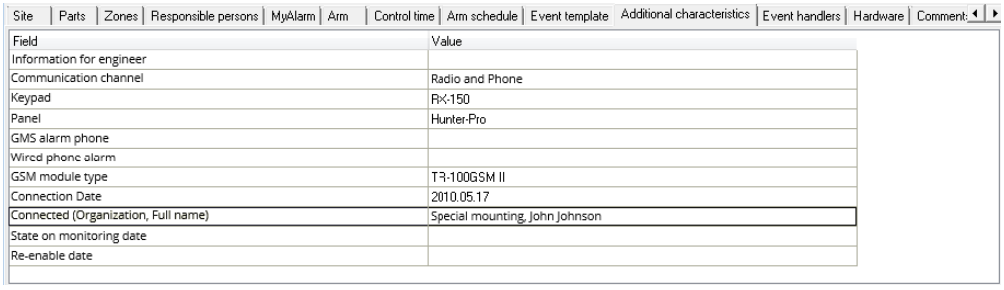
La generación de eventos del sistema permite realizar un seguimiento preciso de las operaciones para desactivar eventos.

Cabe señalar que la calidad de las plantillas de eventos suministradas con las nuevas versiones del Security Center está en constante mejora, por lo que al describir los sitios se recomienda utilizar las últimas versiones de las plantillas de eventos.

Para reemplazar la plantilla de evento desactualizada con su última versión, use la función de reemplazar la plantilla de evento implementada en el módulo "Configuración del sistema".

6.13 Características adicionales

En la pestaña "Características adicionales" es posible especificar valores para características adicionales de los sitios (campos personalizados). Agregue una nueva característica adicional o cambie una existente en el módulo "Configuración del sistema", en la pestaña "Campos del sitio".



Field	Value
Information for engineer	
Communication channel	Radio and Phone
Keypad	RX-150
Panel	Hunter-Pro
GMS alarm phone	
Wired phone alarm	
GSM module type	TR-100GSM II
Connection Date	2010.05.17
Connected (Organization, Full name)	Special mounting, John Johnson
State on monitoring date	
Re-enable date	

Figura 92: Pestaña "Características adicionales"

Para guardar los cambios realizados en las características adicionales, es necesario con fi rmarlos presionando el botón “Enter” después de completar la entrada de los valores.

Si no se define el valor de alguna característica adicional para el sitio, su valor puede dejarse en blanco. Cuando se muestran características adicionales en la tarjeta del sitio, solo aquellas cuyo valor se indica se enumeran en la lista de características.

Para que el usuario pueda cambiar los valores de las características adicionales del sitio, deberá contar con el permiso “Editar características adicionales” para el módulo “Administrador del sitio”.

6.14 Controladores de eventos

La pestaña "Controladores de eventos" está destinada a mostrar y cambiar los controladores de eventos asociados con el sitio. Lea más sobre la variedad y el propósito de los controladores de eventos suministrados con el software Security Center en el capítulo dedicado al módulo "Administrador de eventos" en la sección "Controladores de eventos".

Para que el usuario vea los grupos de controladores y controladores de eventos en esta pestaña, deberá tener el permiso "Ver controladores de eventos" para el módulo "Administrador de eventos".

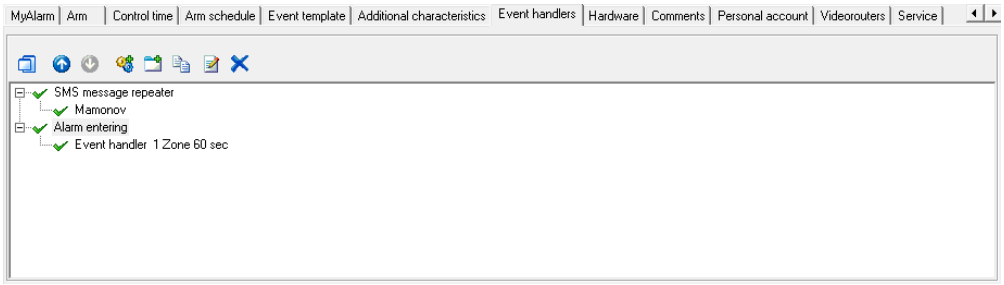


Figura 93: Pestaña "Controladores de eventos"

El propósito de los botones del panel de control para los controladores de eventos es el mismo que el del controlador de eventos en el módulo "Administrador de eventos".

Al configurar controladores de eventos en el módulo "Administrador del sitio", recuerde que no todos los grupos de controladores de eventos se muestran en la lista, sino sólo aquellos controladores en grupos cuyas configuraciones incluyen el número del sitio actual.

Para que el usuario pueda realizar cambios en los controladores de eventos asociados con el sitio, deberá tener el permiso "Editar controladores de eventos" para el módulo "Administrador de eventos".

6.15 Equipo

La pestaña "Equipo" del módulo "Administrador del sitio" está destinada a indicar el tipo de equipo utilizado en el sitio y realizar los ajustes necesarios. La introducción de información sobre el equipo proporciona el soporte correcto del Security Center instalado en los dispositivos del sitio.

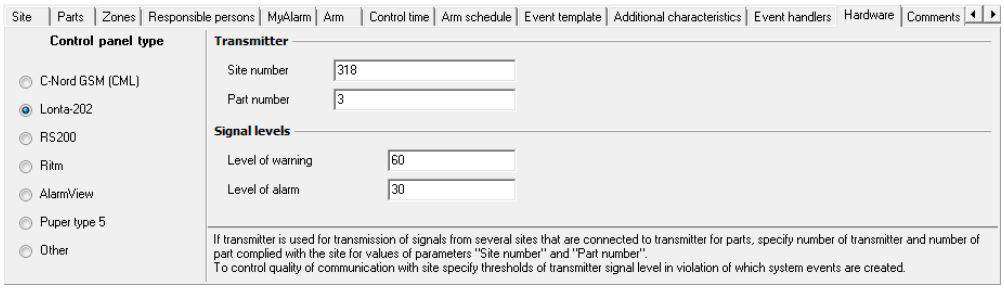


Figura 94: Pestaña "Equipo"

Para configurar el equipo, seleccione el sitio deseado y cambie al modo de edición. De la lista de sistemas presentados en la pestaña "Equipo", seleccione el tipo de equipo utilizado en el sitio: "TR-100 GSM III / Soyuz GSM", "AlarmView", "Lonta-202", "RS200", "Puper tipo 5 ”o“ Neman ”. Si el equipo de otro sistema está instalado en el sitio, especifique el tipo “Otro”.

Para los tipos de equipo “TR-100 GSM III / Soyuz GSM”, “Lonta-202” y “Otro”, especifique los parámetros para configurar el equipo. Recuerde que al copiar un sitio para un sitio nuevo, solo se copia la información sobre el tipo de equipo instalado, pero no los valores de los parámetros especificados.

6.15.1 "Otro"

Si la lista de tipos de equipos no incluye el sistema utilizado en el sitio, seleccione el tipo "Otro". En la sección "Transmisor", configure los valores para los parámetros "Número de sitio" y "Número de pieza".

Si el sitio es una de las partes del panel de control, entonces en el campo "Número de sitio" configure el número de sitio del panel de control, y en el campo "Número de parte" - el número de parte correspondiente al sitio.

6.15.2 "C-Nord GSM (CML)"

Este tipo de equipo se debe especificar para el sitio si uno de los siguientes dispositivos está instalado en él:

- "Nord GSM" o "Nord GSM (WRL)"
- "Serzhant GSM"
- "Soyuz GSM (OEM) o" Soyuz GSM (BOX) "
- Transmisor “TR-100 GSM III”, conectado al panel de control producido por C.Nord o PIMA Electronic Systems Ltd.

El campo "ID" se completará automáticamente después de que el dispositivo se conecte al Centro de seguridad por primera vez.

La ID del dispositivo es el número de identificación único del procesador instalado en el dispositivo. Al recibir eventos del sitio, se comprueba que los eventos se envían desde el dispositivo cuyo ID es el asignado al sitio. La protección contra la sustitución de equipos se realiza de esa manera.

Al reemplazar el equipo conectado al panel de control en el sitio, elimine el valor del parámetro "ID". Haga esto con el botón "Eliminar" ubicado frente al campo "ID". Después de eliminar el valor anterior, la ID del nuevo transmisor se determinará automáticamente en el campo "ID".

La eliminación del valor de este parámetro también es necesaria cuando el equipo se desmonta en el sitio o se cambia.

Es posible eliminar la identificación y cambiar el tipo de equipo para un sitio, así como para todos los sitios asignados a este identi fi cador. Para ello, utilice el cuadro de diálogo que aparece al cambiar el tipo de equipo. Al cambiar todos los sitios asignados a la ID, especifique cualquiera de los tipos de equipo enumerados en la lista para el sitio actual, y para otros sitios, el tipo "Otro" se especifica de forma predeterminada.

6.15.3 "Lonta-202"

Seleccione el tipo de equipo “Lonta-202” cuando utilice el sistema de seguridad por radio centralizado “Lonta-202” (antes llamado “Rif String RS202”) fabricado por Altonika.

En la sección "Transmisor", configure los valores para los parámetros "Número de sitio" y "Número de pieza". Si el sitio está conectado al transmisor de radio como una de las partes, entonces en el campo "Número de sitio" es necesario especificar el número de sitio del transmisor, y en el campo "Número de parte" - el número de parte correspondiente al sitio.

Los valores indicados en los campos “Número de sitio” y “Número de pieza” son prioritarios con respecto a los números estándar de los sitios del Centro de seguridad: al recibir eventos, los valores ingresados en la pestaña “Equipo” y primero de todos los valores del sitio los números se ven primero.

Para controlar la calidad de la comunicación con el sitio en el que se utiliza el equipo del sistema Lonta-202, es necesario establecer los niveles de umbral de la señal del transmisor. Haga esto en la sección "Niveles de señal", indicando los valores de los parámetros correspondientes en los campos "Nivel de advertencia" y "Nivel de alarma".

Si el nivel de la señal recibida del sitio es menor que el valor especificado en el campo "Nivel de advertencia", se creará un evento del sistema con el código "ZZXV". Si el nivel de la señal recibida del sitio es menor que el valor especificado en el campo "Nivel de alarma", se creará un evento del sistema con el código "ZZXU". Con la ayuda de eventos del sistema con códigos “ZZXV” y “ZZXU” es posible monitorear automáticamente el nivel de la señal recibida, atrayendo la atención del operador solo hacia aquellos sitios donde se requiere intervenir.

Cabe señalar que para los sitios en los que está instalado el equipo del sistema Lonta-202, la función de visualización del nivel de la señal recibida está disponible en el módulo “Operador de servicio”. La tarjeta del sitio tiene una pestaña que permite mostrar el nivel de la señal en forma de gráfico o como una tabla de valores.

6.15.4 "RS200"

Se seleccionará el tipo de equipo “RS200” cuando se utilice el sistema de protección radio centralizado “Rif String RS200” fabricado por Altonika.

6.16 Comentario

La pestaña "Comentarios" está diseñada para ingresar una descripción arbitraria del sitio.

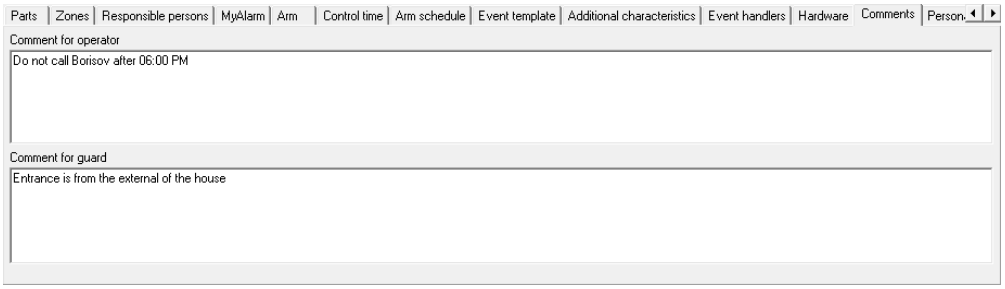


Figura 95: Pestaña "Comentarios"

En el campo "Comentario para el operador", se indica la información destinada al operador del Centro de seguridad. Esta información se muestra en la tarjeta del sitio en el módulo "Operador de servicio", por lo que a menudo se usa para almacenar notas en el sitio: solicitudes de las personas responsables, observaciones de los ingenieros que atienden el sitio, recomendaciones a los operadores, etc.

En el campo "Comentario para el guardia", se indica información para los guardias. En caso de alarma del sitio, se transfiere a la aplicación "Alarma a guardia".

6.17 Videorouters

La pestaña "Videorouters" en el módulo "Administrador del sitio" permite especificar los enrutadores de video para el sitio. Las cámaras de video, instaladas en el sitio, se conectarán a estos enrutadores de video.

Gracias a la instalación de cámaras de video, es posible el monitoreo remoto del sitio. La vigilancia puede ser realizada tanto por una persona responsable de la empresa protegida por medio de la interfaz web de la “Cuenta personal” o aplicación móvil, como por el operador de guardia de la compañía de seguridad en el módulo “Operador de guardia” mientras maneja una alarma.

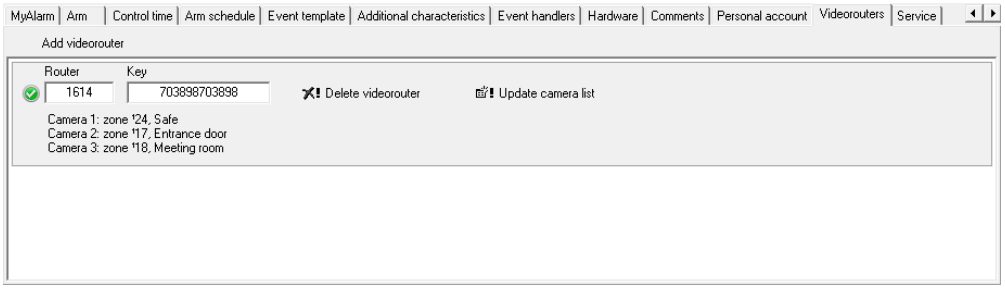


Figura 96: Pestaña "Videorouters"

Para agregar o cambiar datos sobre enrutadores de video, así como ver las claves de enrutadores de video instalados en el sitio, el usuario debe tener el permiso "Cambiar información sobre enrutadores de video" para el módulo "Administrador del sitio".

Para agregar el enrutador de video instalado en el sitio, haga clic en el botón "Agregar enrutador de video" en la pestaña "Enrutador de video". En el campo “Enrutador” ingrese la ID del enrutador de video, y en el campo “Clave”, la contraseña para su autorización. Los datos requeridos se indicarán en el dispositivo. Después de eso, presione el botón "Guardar" para guardar información sobre el enrutador de video o el botón "Cancelar" para cancelar el guardado. El icono de estado actual del enrutador de video muestra el estado de su conexión.

La tarjeta del sitio muestra información sobre la configuración del enrutador de video agregado. A saber: descripción de cada una de las cámaras de video conectadas y número de zonas en su campo de visión. Esta información se almacena en la base de datos del Security Center y en la “Nube”.

Para actualizar la información sobre las cámaras de video conectadas al enrutador de video, haga clic en el botón "Actualizar lista de cámaras".

Para eliminar información sobre el enrutador de video y las cámaras de video conectadas a él, haga clic en el botón "Eliminar enrutador de video".

6.18 Servicio

La pestaña "Servicio" está destinada a proporcionar a los ingenieros permisos para acceder a los sitios. El permiso recibido por el ingeniero le da la capacidad de programar remotamente el panel de control en el sitio durante el intervalo de tiempo especificado.

Cuando se selecciona el sitio en la lista de sitios en la pestaña, se muestra información sobre ingenieros, fecha y hora de inicio y finalización del permiso.

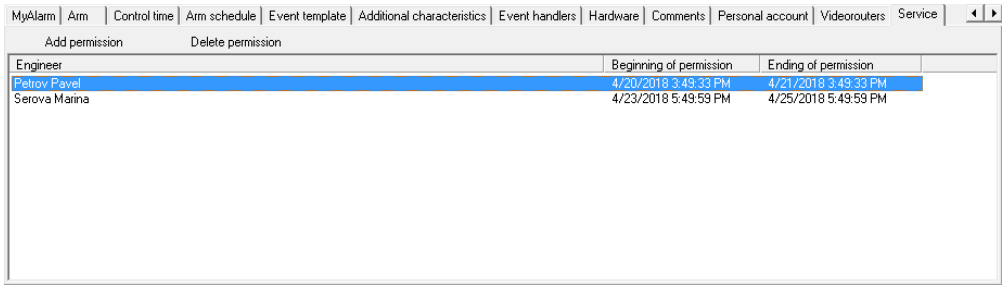


Figura 97: Pestaña "Servicio"

Solo el usuario con el permiso correspondiente puede otorgar acceso al sitio a los ingenieros.

Para emitir un permiso, seleccione el sitio deseado en la lista de sitios y haga clic en el botón "Agregar permiso".

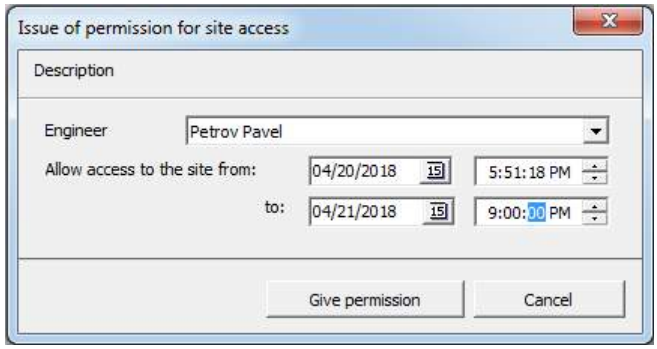


Figura 98: Ventana "Emitir permiso para acceder al sitio"

En la ventana "Emitir permiso para el acceso al sitio", complete los siguientes campos:

- “Ingeniero”: ingeniero de la lista desplegable. La lista muestra los ingenieros creados en el módulo "Administrador de personal". Los ingenieros que no hayan con fi rmado la dirección de correo electrónico para el registro en la nube también pueden seleccionarse de la lista, pero solo obtendrán acceso a los sitios después de que se complete el registro;

- “Permitir acceso al sitio desde” y “hasta”: fecha y hora de inicio y finalización del permiso, respectivamente. El permiso para acceder al sitio se puede emitir por no más de treinta días. Al emitir un permiso por más de tres días, la aplicación pedirá con fi rmación. Además, otorgarle a un ingeniero permiso para acceder al sitio cancelará el permiso otorgado a él / ella para acceder a este sitio anteriormente.

Después de ingresar los datos, haga clic en el botón "Dar permiso" para completar la operación. Para cancelarlo, haga clic en el botón "Cancelar".

Para eliminar el permiso de acceso al sitio, seleccione el permiso en la lista y haga clic en el botón "Eliminar permiso".

7 Configuración del sistema

El módulo "Configuración del sistema" está destinado a cambiar los directorios de servicios del Centro de seguridad, por ejemplo, plantillas de eventos o tipos de sitios.

7.1 Clases de eventos

En el Software Security Center, los eventos creados se dividen en varios tipos:

- A alarma
- Advertencia
- Armamento
- Encantador
- Culpa
- Restaurar
- Excepción
- Prueba
- Otro
- Resetear alarma

El tipo de evento determina el manejo. Por ejemplo, los eventos del tipo "Alarma" requieren acciones obligatorias del operador, llamadas manejo de alarmas. Además, las alarmas, cuyo manejo no se inicia o finaliza, cambian el estado actual de los sitios. Al manejar eventos que tienen el tipo "Armado" o "Desarmado", el estado del sitio también cambia.

La lista de tipos de eventos está predefinida y el usuario no puede cambiarla. Las clases de eventos están destinadas a agrupar los eventos y gestionarlos. La clase de evento de fi ne su tipo, en este caso es posible crear varias clases con el tipo “Alarma” y de fi nir listas de acciones individuales y cancelaciones para cada alarma.

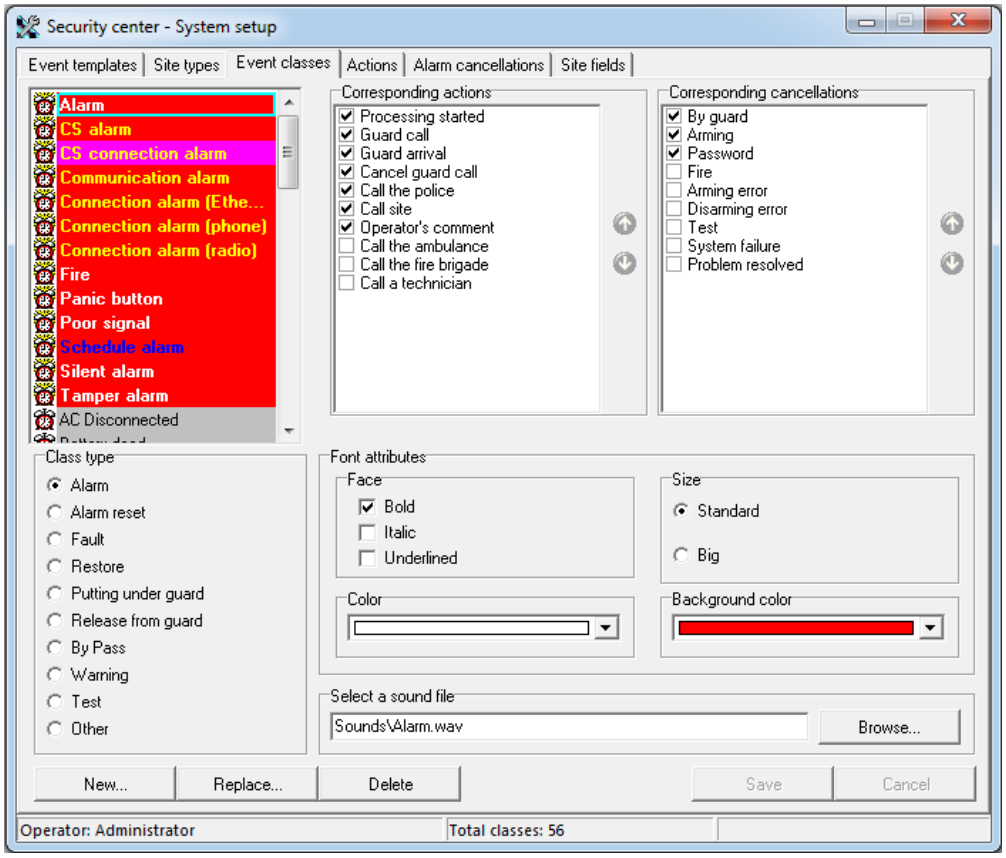


Figura 99: Pestaña "Clases de eventos"

Utilice la pestaña "Clases de eventos" para cambiar la lista de clases de eventos utilizadas.

Para guardar los cambios realizados en esta pestaña, el usuario deberá tener el permiso "Editar clases de eventos" para el módulo "Configuración del sistema".

La clase de evento define la aparición del evento en la lista de eventos recibidos del módulo "Operador de servicio". Color, fuente, color de fondo: todas estas propiedades de la clase de evento se pueden cambiar en el módulo "Configuración del sistema".

Además de los atributos responsables de mostrar eventos, es posible especificar un archivo de audio que se reproducirá cuando se reciba un evento.

Para las clases de eventos del tipo "Alarma", existen listas de acciones y cancelaciones, que el operador puede registrar durante el manejo de alarmas. Es importante que sea posible de fi nir no solo la lista de acciones, sino también su secuencia durante la visualización.

Dado que las clases de eventos definen la apariencia, el sonido y el script de alarma, el Centro de seguridad garantiza que estos parámetros permanezcan sin cambios para los eventos ya registrados. En otras palabras, los cambios e incluso la eliminación de clases de eventos no afectan a los eventos que ya están aceptados y registrados en la base de datos. Si se cambia el color o tamaño de la fuente que se utiliza para mostrar el evento o el tipo de evento, estos cambios solo se aplicarán a los nuevos eventos, los que se registrarán en la base de datos después de que se realicen los cambios.

Reemplazo de clase de evento

Si el Centro de seguridad ha estado en funcionamiento durante mucho tiempo, existe la posibilidad de que la lista de clases de eventos esté llena de basura. Por ejemplo, contiene clases duplicadas o información sobre clases que ya no se utilizan. Sin embargo, es imposible eliminar estas clases porque hay eventos descritos por estas clases. Para hacer frente a este problema, es posible reemplazar las clases de eventos duplicadas o no utilizadas con sus análogos actuales. Para reemplazar la clase de evento obsoleta con la que está actualmente en uso, use la opción “Reemplazar. . . " botón.

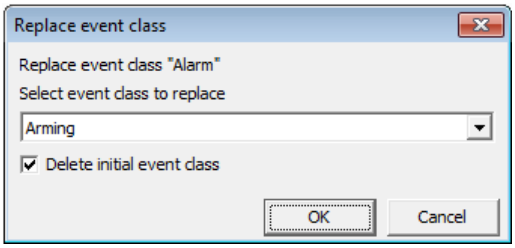


Figura 100: Ventana "Reemplazar clase de evento"

En la ventana que aparece, seleccione la clase de evento que se utilizará en lugar de la reemplazada y también especifique la necesidad de eliminar la clase de evento que se está reemplazando.

7.2 Plantillas de eventos

El mismo evento que ocurrió en el sitio se puede transmitir al Centro de seguridad de diferentes formas. El formato de notificación, en el que se recibirá la información sobre el evento, depende del tipo de equipo de transmisión y canal de comunicación.

Una plantilla de eventos es una lista de eventos que se pueden recibir al decodificar las notificaciones de un sitio.

La plantilla del evento es una característica integral del sitio. Es posible especificar la plantilla de evento que se utilizará para el sitio en el módulo "Administrador del sitio".

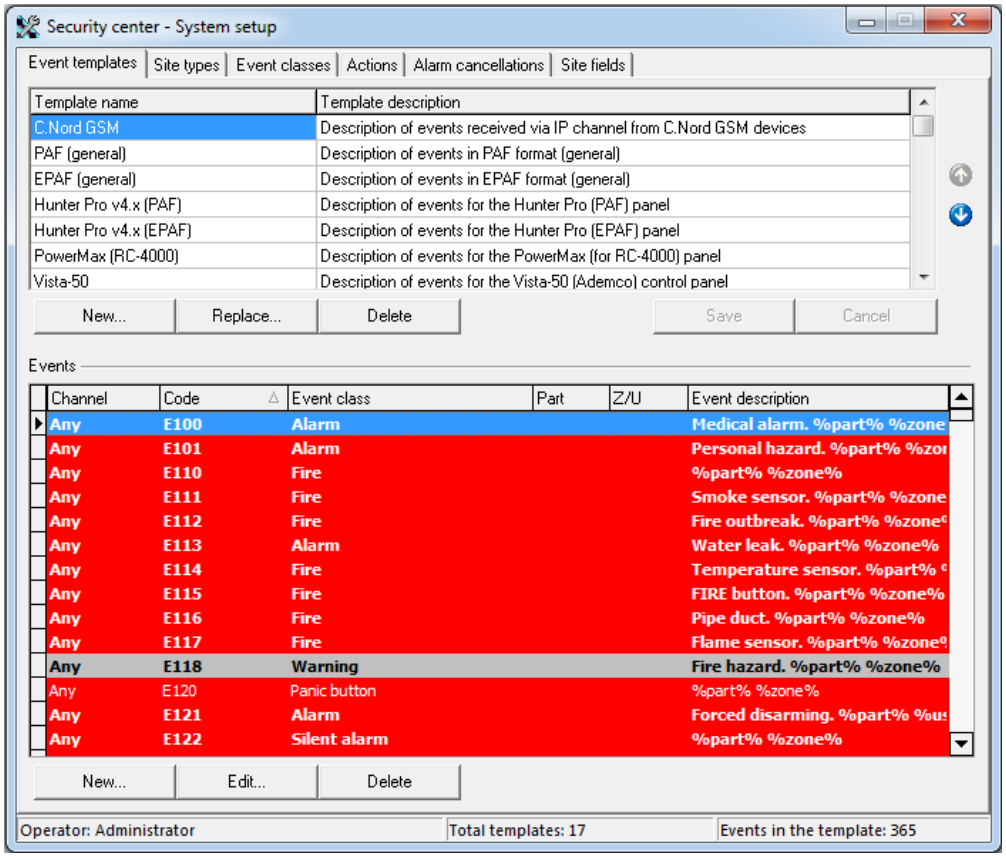


Figura 101: Pestaña "Plantillas de eventos"

Utilice la pestaña "Plantillas de eventos" para cambiar la lista de plantillas utilizadas por el Centro de seguridad. Además, es posible cambiar la descripción de los eventos en la plantilla.

Para guardar los cambios realizados en esta pestaña, el usuario debe tener el permiso "Editar plantillas de eventos" para el módulo "Configuración del sistema".

Los cambios que se realizan en la descripción de los eventos de la plantilla en la pestaña Configuración del sistema afectan a todos los sitios que utilizan esta plantilla de eventos. Se recomienda encarecidamente no realizar cambios en la plantilla de eventos del sitio sin una razón válida.

Es imposible eliminar la plantilla de evento utilizada en la descripción del sitio. Si la plantilla que el usuario desea eliminar se utiliza como plantilla de evento para un sitio, el intento de eliminar se completará con un error.

7.2.1 Reemplazo de la plantilla de evento

Cabe señalar que la calidad de las plantillas de eventos que se suministran con el Security Center mejora constantemente, por lo que al describir los sitios se recomienda utilizar las últimas versiones de las plantillas de eventos. Para reemplazar la plantilla obsoleta para sitios por otra, más relevante, use la función de reemplazar plantillas de eventos. Para reemplazar la plantilla de evento obsoleta con la que está actualmente en uso, use la opción “Reemplazar. . . " botón.

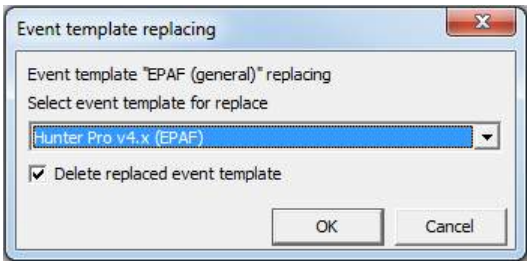


Figura 102: Ventana "Reemplazo de plantilla de evento"

En la ventana que aparece, seleccione una plantilla de evento que se utilizará en lugar de la reemplazada, y también especifique la necesidad de eliminar la plantilla de evento obsoleta.

Edición de eventos

Si cambia los eventos de la plantilla, los cambios en la base de datos se guardan inmediatamente después de que el usuario haya realizado cambios en el evento de la plantilla. No es posible deshacer cambios.

Al crear un nuevo evento o cambiar un evento existente, es posible especificar todos los atributos del evento en la ventana "Editar evento".

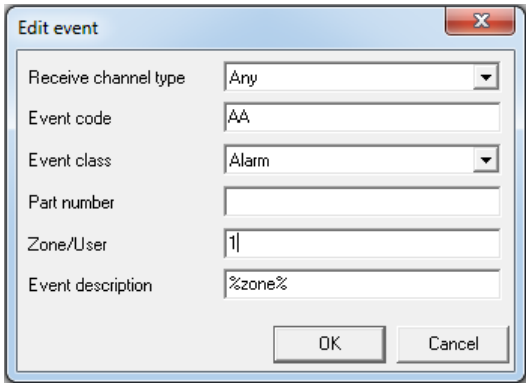


Figura 103: Ventana "Editar evento"

- “Tipo de canal de recepción”: al decodificar un evento, es importante qué canal se utilizó cuando el Centro de seguridad lo recibió. Por ejemplo, el mismo código de evento se puede decodificar de diferentes formas, para eventos recibidos por radio y teléfono. Si el código de evento se define para ambos canales de comunicación específicos y para el canal de comunicación "Cualquiera", la descodificación del canal de comunicación "Cualquiera" se aplica sólo si no se encuentra la descodificación de un canal de comunicación específico.

- El “código de evento” es la parte significativa del mensaje enviado desde el sitio. Es el código que identifica el cambio que se ha producido en el panel de control del sitio. Los códigos de evento pueden ser de diferentes longitudes, depende del formato (protocolo) y el canal de comunicación utilizado durante la transmisión de información desde el dispositivo del sitio a la estación central. El Centro de seguridad admite códigos de eventos de hasta 25 caracteres de longitud.
- La "clase de evento" es una clase de evento que se asignará al código recibido al decodificar un evento. La clase de evento define la aparición del evento en la lista de eventos, así como una lista de posibles acciones para su manejo, si la clase de evento es "Alarma".
- El "número de pieza" es un atributo que se puede utilizar para identificar mejor el evento durante la decodificación. Si el protocolo de intercambio con el dispositivo del sitio contiene el número de la parte a la que se refiere el evento, entonces el evento se identificará no solo por el código y el canal de recepción, sino también por el número de parte. Además, el número de pieza se utiliza cuando se genera la descripción del evento automáticamente: si el número de pieza no es cero y la descripción del evento contiene la macro%parte%, luego, en lugar de la macro, se insertará la descripción de la parte del sitio correspondiente al número de parte recibido del sitio.
- “Zona / Usuario” es un atributo que se puede utilizar dependiendo de cómo se utilice el formato informativo (protocolo) para transmitir información desde el panel de control al Centro de Seguridad.

  Supongamos que el panel, al transmitir a la estación, utiliza el protocolo ContactID, el cual, entre otras cosas, envía el número de la zona disparada o el número del usuario que realizó el desarmado del sitio. En este caso, el Centro de Seguridad ignora la zona o el número de usuario especificado en la descripción del evento y siempre usa el valor recibido del panel: el número de zona, que fue enviado desde el panel, se usará para decodificar el evento.

  Ahora consideremos la situación en la que el panel, al transmitir a la estación, usa el protocolo EPAF, en el que solo se transmiten el número de sitio y el código de evento. Los números de zona o de usuario no se transmiten explícitamente, pero se conoce la relación entre el código de evento y el número de zona o de usuario. En este caso, la zona o el número de usuario se especifica en la plantilla del evento, de acuerdo con el código del evento, y es el valor especificado en la plantilla el que se utilizará para formar la descripción del evento.

  Como ejemplo, consideremos un mensaje de alarma en la primera zona transmitido a través de diferentes protocolos. En el protocolo ContactID, este mensaje se transmitirá en forma de código E130 y número de zona 1. Al formar la descripción, el Centro de Seguridad realizará inmediatamente la sustitución de la descripción de la primera zona en la descripción del evento. Mientras que en el protocolo EPAF el mismo mensaje se transmitirá solo en forma de código AA y para obtener el número de la zona correspondiente a este código, el Centro de Seguridad tendrá que buscar en la plantilla del evento.

- "Descripción del evento" es una cadena de texto arbitraria que describe el evento.

  Al describir eventos, se recomienda utilizar las macros%usuario% y %zona%. Si se encuentra una macro en la descripción del evento durante su decodificación, un valor correspondiente al nombre de la zona (macro %zona%) o el nombre de la persona responsable (macro%usuario%) se insertará en la descripción. En este caso, la zona o el número de usuario se tomarán del evento en sí. La información sobre las zonas y las personas responsables en el sitio es muy importante. Es posible ingresar esta información para el sitio en el módulo "Administrador del sitio".

7.3 Acciones

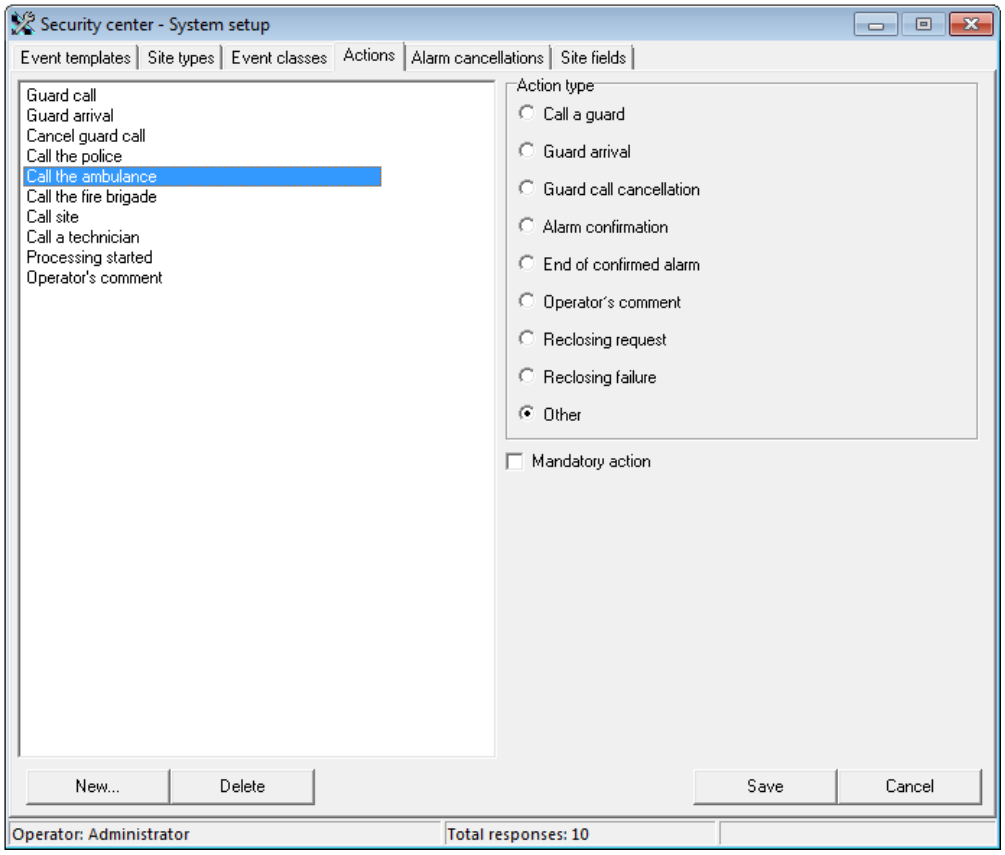


Figura 104: Pestaña "Acciones"

La pestaña "Acciones" está diseñada para cambiar la lista de acciones que un operador puede registrar durante el manejo de alarmas.

Para guardar los cambios realizados en esta pestaña, el usuario debe tener el permiso "Editar acciones del operador" para el módulo "Configuración del sistema".

Los siguientes tipos de acciones se definen en el software Security Center:

- “Llamar a un guardia”: al registrar este tipo de acción, el operador deberá especificar el guardia que fue llamado al sitio. Si se ha llamado a un guardia al sitio, la alarma del sitio se puede cancelar solo después de que el guardia llegue al sitio o se registre la cancelación de su llamada. La lista de guardias utilizados por el Centro de seguridad se puede cambiar en el módulo "Administrador de personal".
- "Llegada de guardia": la acción del tipo "Llegada de guardia" está disponible para el registro solo después de que se registre la llamada de guardia al sitio. Al registrar una acción con el tipo “Llegada guardia”, el operador deberá seleccionar la guardia cuya llegada está registrando.
- “Cancelación de llamada de guardia”: el registro de cancelación de una llamada de guardia está disponible solo después de que se registre su llamada al sitio. Al registrar una cancelación de llamada, el operador deberá seleccionar el guardia cuya cancelación de llamada está siendo realizada por el operador.
- “Comentario del operador”: este tipo de acción permite al operador ingresar texto arbitrario asociado con el manejo de la alarma. Las acciones de este tipo se pueden registrar en cualquier etapa del manejo de alarmas. Se recomienda incluir este tipo de acción en listas de acciones para todas las alarmas que están disponibles en el Centro de seguridad.
- “Solicitud de recierre”: este tipo de acción permite al operador informar automáticamente a las personas responsables sobre la necesidad de volver a cerrar el sitio. Al registrar este tipo de acción, se envía un mensaje SMS a los responsables, para quienes se configura una alerta de solicitud de reenganche en el módulo “Administrador del sitio”. El SMS contiene

el número, nombre y dirección del sitio que se abrirá, inspeccionará y volverá a cerrar una vez que se haya eliminado la causa de la alarma.

- “Fallo de reenganche”: este tipo de acción permite al operador informar automáticamente a las personas responsables sobre la negativa del responsable de reenganchar. Al registrar una acción de este tipo, el operador deberá seleccionar a la persona responsable del sitio que se ha negado a venir para el reenganche. La lista contiene solo a las personas responsables, a las que se les notifica sobre la necesidad de volver a cerrar de acuerdo con la configuración del módulo "Administrador del sitio". En este caso, el nombre completo de la persona responsable, que se negó a volver a cerrar, se muestra en el campo "Nota" cuando la acción se escribe en el registro de eventos. Al registrar este tipo de acción, se envía un mensaje SMS a los responsables, para quienes se configura una alerta sobre rechazo de reenganche en el módulo “Administrador del sitio”. El SMS contiene el nombre de la persona responsable, que se negó a volver a cerrar,

- “Otro”: las acciones del tipo “Otro” son de naturaleza informativa y se utilizan para el registro rápido de acciones que se utilizan a menudo durante el manejo de alarmas (llamar a la persona responsable, llamar a la policía, etc.). Las acciones de este tipo se pueden registrar en cualquier etapa del manejo de alarmas.

Se recomienda actualizar constantemente el listado de acciones con el tipo “Otro”, para que correspondan a las tácticas del guardia utilizadas en el momento. Una buena fuente de nuevas acciones con el tipo "Otro" pueden ser los comentarios del operador registrados.

Se puede hacer obligatoria la ejecución de cualquier tipo de acción durante la gestión de alarmas. Para hacer esto, seleccione la acción en la lista y marque la casilla "Acción obligatoria".

7.4 Cancelaciones de alarma

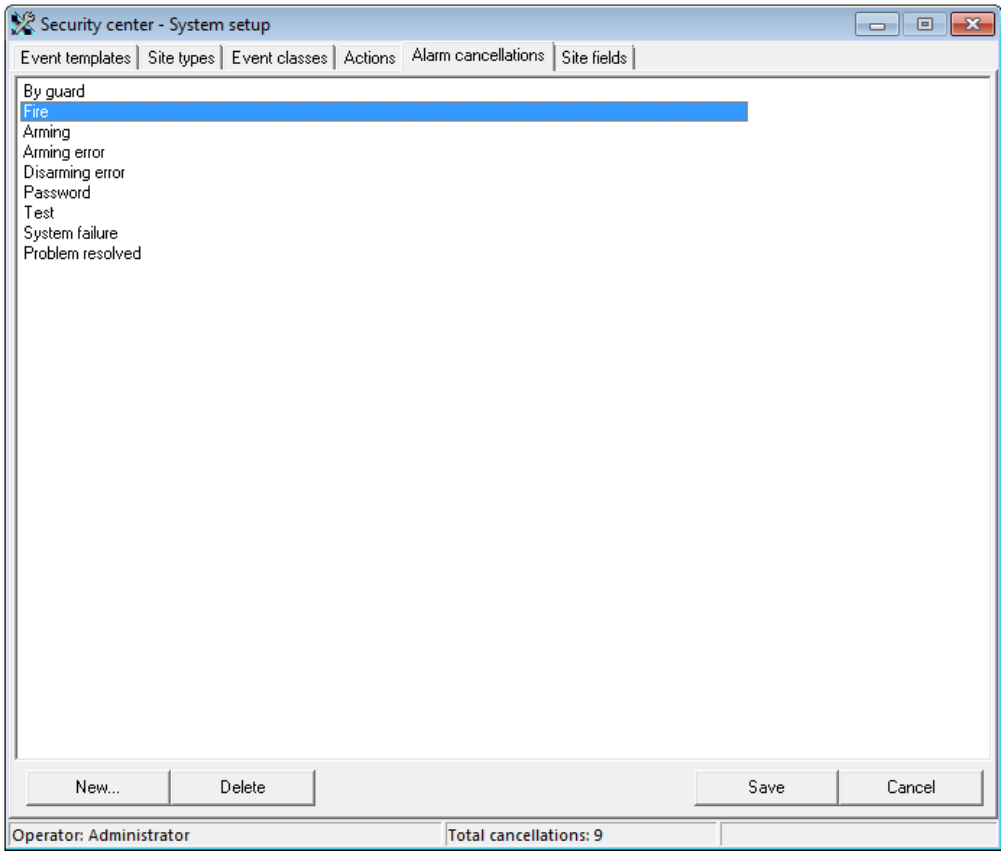


Figura 105: Pestaña "Cancelación de alarma"

Utilice la pestaña "Cancelación de alarma" para editar la lista de motivos registrados al cancelar alarmas.

Para guardar los cambios realizados en esta pestaña, el usuario deberá tener el permiso "Editar cancelaciones de alarma" para el módulo "Configuración del sistema".

La lista de cancelaciones de alarmas disponibles está estrechamente relacionada con las tácticas de protección del sitio y es de gran importancia para analizar el desempeño de la empresa.

El software Security Center contiene varios informes analíticos que garantizan la evaluación de las causas más comunes de cancelación de alarmas, incluso en el contexto de los sitios. Para utilizar estos informes, es necesario mantener una lista de cancelaciones de alarmas en el estado actual y regular claramente el uso de cada cancelación en las instrucciones del operador.

7.5 Tipos de sitios

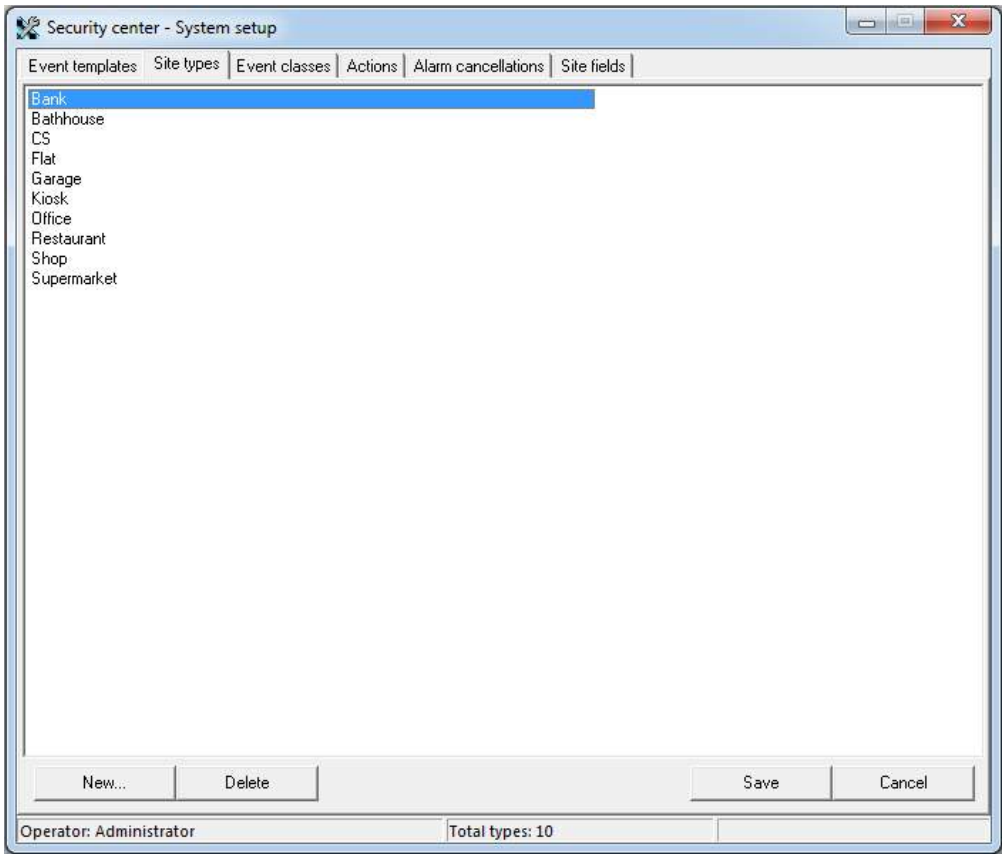


Figura 106: Pestaña "Tipos de sitios"

La pestaña "Tipos de sitios" se utiliza para administrar la lista de tipos de sitios.

Para guardar los cambios realizados en esta pestaña, el usuario debe tener el permiso "Editar tipos de sitios" para el módulo "Configuración del sistema".

El tipo de sitio es una propiedad obligatoria de un sitio. El tipo de sitio se utiliza para la conveniencia de organizar (ordenar, agrupar) la lista de sitios, por ejemplo, al ver las propiedades del sitio o al crear informes. Es posible especificar el tipo de un sitio en el módulo "Administrador del sitio".

7.6 Campos del sitio

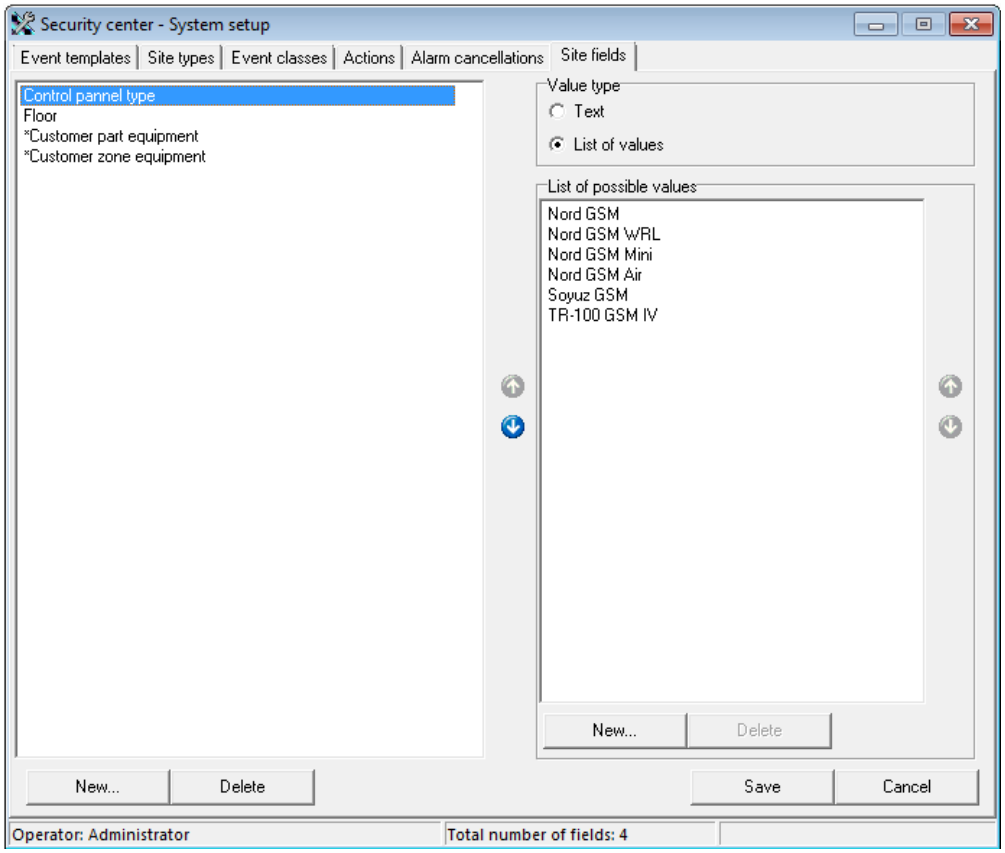


Figura 107: Pestaña "Campos del sitio"

Utilice la pestaña "Campos del sitio" para cambiar la lista de campos adicionales que estarán disponibles al completar la tarjeta del sitio.

Para guardar los cambios realizados en esta pestaña, el usuario debe tener el permiso "Editar campos del sitio" para el módulo "Configuración del sistema".

Al crear una lista de campos, es posible establecer su secuencia cuando se muestran en la tarjeta del sitio.

Si los valores de un campo son una lista de valores previamente conocidos, entonces es posible completar esta lista especificando el tipo apropiado para el campo. En este caso, la lista de valores no limita la capacidad de especificar un valor para el campo del sitio manualmente, si es necesario.

Hay dos campos en la lista de campos del sitio, para los cuales se recomienda cambiar solo la lista de valores posibles. Estos campos son "*Equipo de parte del cliente "y"*Equipamiento zona cliente ". Como sugieren sus nombres, están pensados para que sea más conveniente completar los valores del campo "Equipo" al editar partes y zonas de sitios en el módulo "Administrador de sitios".

8 Gerente de personal

En el módulo "Administrador de personal", es posible editar la lista de operadores y sus derechos - en los módulos del Centro de seguridad, guardias, que se utilizan en el Centro de seguridad, así como la lista de equipos en la red local, en que están permitidos los lugares de trabajo de la red Security Center.

8.1 Operadores

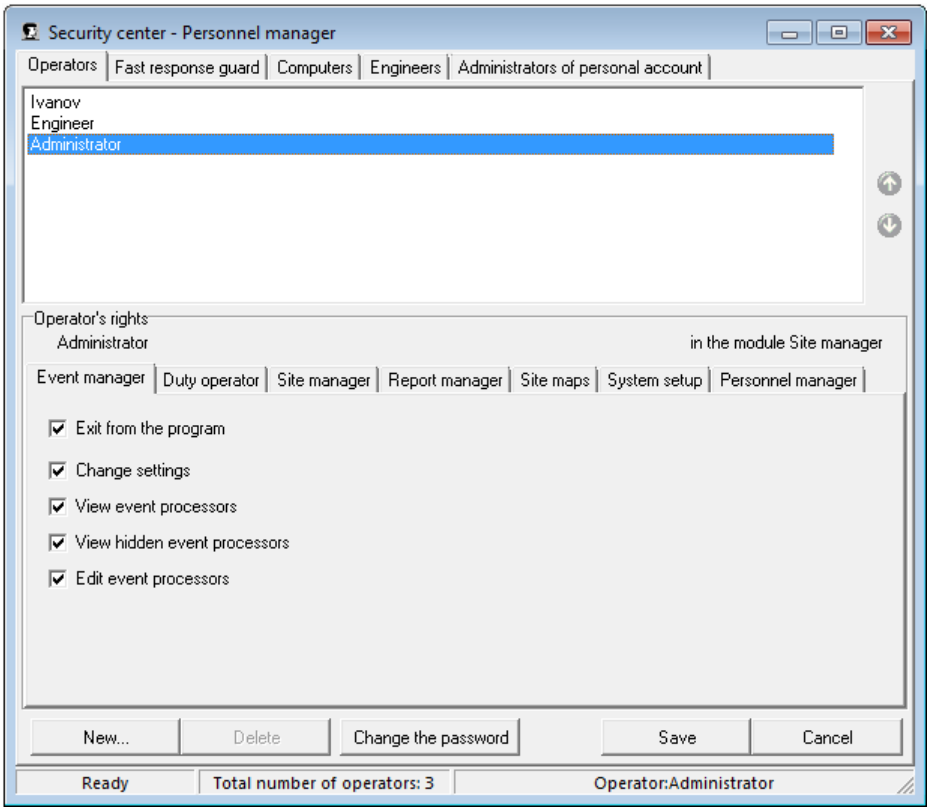


Figura 108: Pestaña Operadores

La pestaña "Operadores" está destinada a editar la lista de operadores de software y sus derechos en los módulos del Centro de seguridad.

Para guardar los cambios realizados en esta pestaña, el usuario deberá tener el permiso “Editar grupos” para el módulo “Administrador de personal”.

Los derechos de operador son individuales para cada módulo de Security Center. La disponibilidad de este o aquel derecho determina la lista de operaciones que se pueden realizar en el módulo.

Antes de determinar los derechos del operador en el módulo, permita que el operador ingrese a este módulo.

Al crear un nuevo operador, es posible asignarle los mismos derechos que uno de los existentes. Para ello, antes de crear un nuevo operador, en la lista de operadores seleccione el usuario, cuyos derechos se copiarán.

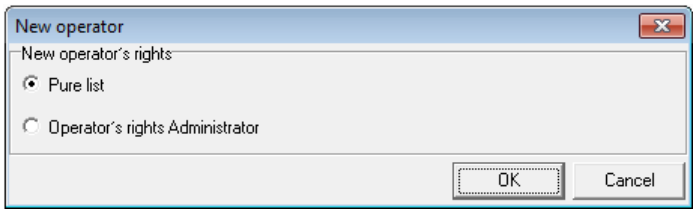


Figura 109: Selección de lista de derechos para nuevo operador

Se prohíbe editar el nombre y derechos del operador, que ingresó al módulo, así como “Administrador” en el módulo “Gerente de Personal”.

Para el operador actual del módulo “Administrador de personal” y el “Administrador”, solo se permite el cambio de contraseña.

8.1.1 Derechos del operador en el módulo "Administrador de eventos"

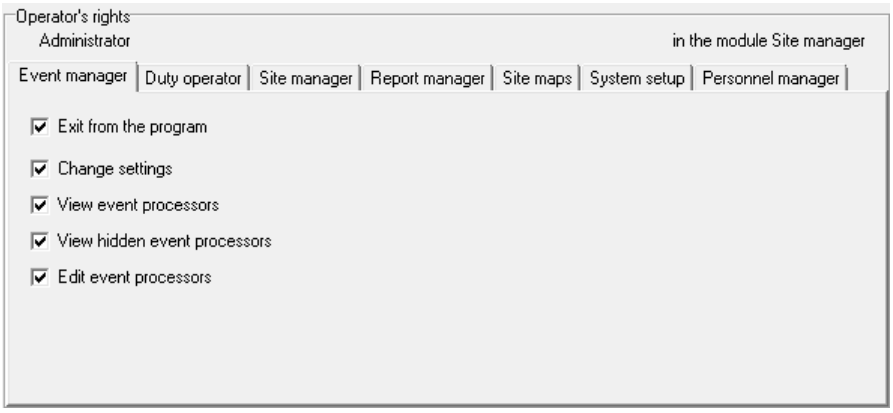


Figura 110: Derechos del operador en el módulo "Administrador de eventos"

- "Salir del programa": permiso para cerrar el módulo "Administrador de eventos".
- "Cambiar configuración": permiso para realizar cambios en la configuración del módulo "Administrador de eventos".
- "Ver controladores de eventos": permiso para ver (pero no cambiar) la configuración de los controladores de eventos. Este permiso también se aplica al módulo "Controladores de eventos".
- "Ver controladores de eventos ocultos": permiso para ver (pero no cambiar) la configuración de *oculto* controladores de eventos. Este permiso también se aplica al módulo "Controladores de eventos".
- "Editar controladores de eventos": permiso para realizar cambios en la configuración de los controladores de eventos permitidos. a vista. Este permiso también se aplica al módulo "Controladores de eventos".

8.1.2 Derechos del operador en el módulo "Operador de servicio"

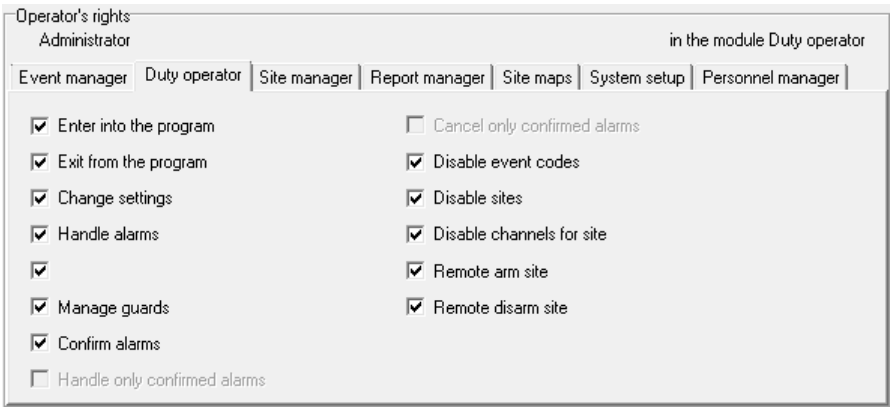


Figura 111: Derechos del operador en el módulo "Operador de servicio"

- "Entrar en el programa" - permiso para entrar en el módulo "Operador de servicio". Si el operador tiene que manejar las alarmas, tendrá este permiso.
- "Salir del programa": permiso para cerrar el módulo "Operador de servicio". La prohibición de cerrar el módulo "Operador de servicio" puede ser útil para operadores sin experiencia, como una advertencia sobre la salida del módulo por error.
- "Cambiar configuración": permiso para realizar cambios en la configuración del módulo "Operador de servicio". No se recomienda otorgar este permiso a los operadores de servicio, especialmente debido a que la configuración del "Servicio

operador ”módulo están asociados con la computadora en la que se está ejecutando el módulo, y no con el operador que inició el programa. De esta forma, el administrador puede realizar todos los ajustes necesarios del módulo en la computadora y cualquier operador que haya iniciado el módulo “Operador de servicio” trabajará con estos ajustes.

- "Manejar alarmas": permiso para manejar una alarma. El operador del Centro de seguridad con este derecho puede llamar a la ventana "Manejo de alarmas" y realizar todas las acciones posibles para manejar la alarma. Para cancelar la alarma, el operador también tendrá derecho a "Cancelar alarma".
- "Cancelar alarma": permiso para cancelar la alarma. El operador del Centro de seguridad con este derecho puede llamar a la ventana "Manejo de alarmas" y cancelar la alarma. Para manejar una alarma, el operador también tendrá derecho a "Manejar alarmas".
- "Deshabilitar códigos de eventos": permiso para deshabilitar eventos. El operador del Centro de Seguridad con este derecho puede llamar a la ventana “Desactivar evento” y desactivar el evento, especificando el tiempo durante el cual el evento se desactivará y el motivo de la desactivación.
- "Deshabilitar sitios": permiso para deshabilitar sitios. El operador del Centro de seguridad con este derecho puede llamar a la ventana "Deshabilitación del sitio" y deshabilitar el sitio, especificando el tiempo durante el cual el sitio estará deshabilitado y el motivo de la deshabilitación.
- "Desactivar canales para el sitio": permiso para desactivar los canales de comunicación del sitio. El operador del Centro de Seguridad con este derecho puede llamar a la ventana “Deshabilitación de canales del sitio” y deshabilitar uno o varios canales de comunicación, especificando el tiempo durante el cual los canales de comunicación serán deshabilitados y el motivo de deshabilitación.
- “Sitio de armado remoto / sitio de desarmado remoto”: permiso para armar / desarmar de manera remota los sitios. El operador del Centro de Seguridad con este derecho puede armar / desarmar el sitio, si el equipo con el tipo de transmisor “TR-100 GSM III” está instalado en el sitio.

8.1.3 Derechos del operador en el módulo "Administrador del sitio"

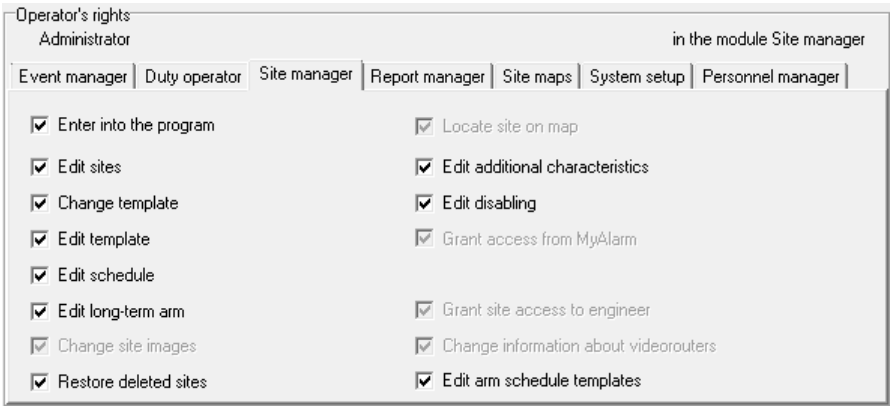


Figura 112: Derechos del operador en el módulo "Administrador del sitio"

- "Entrar en el programa" - permiso para entrar en el módulo "Administrador del sitio". Si el operador podrá ver y editar las tarjetas del sitio, entonces tendrá este permiso.
- "Editar sitios": permiso para editar tarjetas de sitio. Este permiso se aplica a la mayoría de los campos de la tarjeta del sitio, con la excepción de aquellos campos para los que se requieren los cambios de permisos adicionales que se describen a continuación. Con la ayuda de permisos adicionales, es posible proteger de cambios accidentales campos de tarjeta importantes o que rara vez se cambian.
- "Cambiar plantilla": permiso para cambiar la plantilla del evento del sitio. La plantilla de evento determina cómo se decodificarán los mensajes recibidos del equipo del sitio: qué mensajes se considerarán de alarma,

qué mensajes se considerarán armados, etc. La plantilla de evento en particular que se utilizará para un sitio depende del equipo instalado en el sitio, así como de los canales de comunicación a través de los cuales se transmiten los mensajes del sitio. Para la mayoría de los dispositivos de sitio modernos, la plantilla de evento “Radio (EPAF), DTMF, GPRS”, que se incluye en el paquete Security Center, es adecuada y se recomienda su uso.

- "Editar plantilla": permiso para editar descripciones de eventos incluidos en el conjunto de plantillas de eventos para el sitio. Se debe tener en cuenta que los cambios se aplicarán solo al sitio para el que se realizaron los cambios y la plantilla del evento en sí no se verá afectada de ninguna manera. Se recomienda encarecidamente no realizar cambios en la plantilla de eventos del sitio sin una razón válida.
- "Editar programa": permiso para editar los parámetros del programa de armado del sitio. Si el horario de armado está configurado para el sitio y su monitoreo está habilitado, entonces, si se viola el horario, el Centro de Seguridad creará los eventos del sistema apropiados (alarmas).
- "Editar brazo a largo plazo": permiso para editar los parámetros del brazo a largo plazo del sitio. Si el armado a largo plazo está habilitado para el sitio, cuando intente desarmar el sitio, el Centro de seguridad creará un evento del sistema (alarma).
- "Cambiar imágenes del sitio": permiso para cambiar las imágenes del sitio.
- "Restaurar sitios eliminados": permiso para restaurar sitios eliminados.
- "Ubicar el sitio en el mapa": permiso para cambiar la ubicación del sitio en el mapa.
- "Editar características adicionales": permiso para cambiar los valores de las características adicionales del sitio. La información importante se puede indicar en las características adicionales del sitio.
- “Editar inhabilitación”: permiso para cambiar los parámetros de inhabilitación del sitio. Para los sitios discapacitados, Security Center realiza la cancelación automática de las alarmas, sin noti fi car al operador de servicio sobre ellas.
- “Otorgar acceso al sitio al ingeniero”: permiso para otorgar acceso remoto a los sitios a los ingenieros.
- “Cambiar información sobre enrutadores de video”: permiso para cambiar información sobre enrutadores de video. Este permiso permite agregar y eliminar enrutadores de video, a los cuales están conectadas las cámaras en el sitio.
- “Editar plantillas de programación de armado”: permiso para editar plantillas de programación de armado. Con este permiso, es posible a cree, edite y elimine plantillas según el programa de armado seleccionado.

8.1.4 Derechos del operador en el módulo "Administrador de informes"

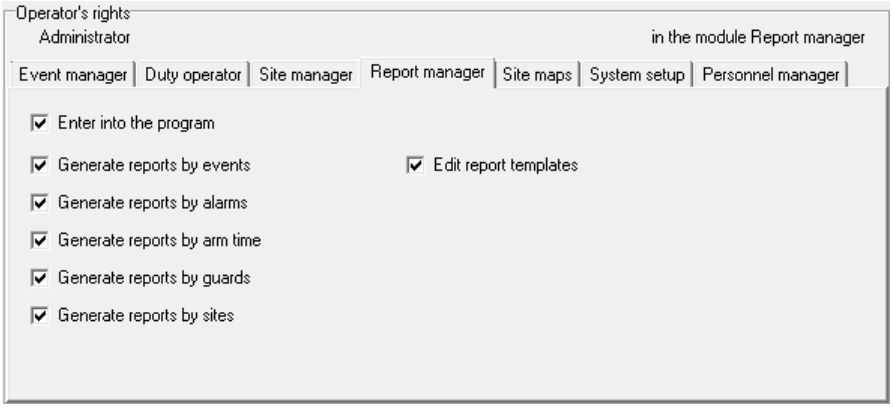


Figura 113: Derechos del operador en el módulo "Administrador de informes"

- "Entrar en el programa" - permiso para entrar en el módulo "Administrador de informes". Si el operador debe poder crear informes, entonces tendrá este permiso.

- "Generar informes por eventos": permiso para crear informes sobre los eventos recibidos. Al crear estos informes, el operador tiene acceso a la lista de sitios, así como a la lista de clases de eventos. Los informes generados contienen información sobre los eventos que se recibieron durante un período determinado, eventos de sitios no descritos y mensajes SMS enviados.
- "Generar informes por alarmas": permiso para crear informes sobre alarmas. Al crear estos informes, el operador tiene acceso a la lista de sitios, así como a la lista de clases de eventos y acciones del operador. Los informes generados contienen información sobre los eventos recibidos, las acciones del operador para manejar alarmas y respuestas de guardia. Además, algunos de los informes de alarmas proporcionan información sobre la base de la cual es posible identificar sitios problemáticos y analizar las causas de las alarmas.
- "Generar informes por tiempo de armado": permiso para crear informes de alarma. Al crear estos informes, el operador tiene acceso a la lista de sitios, así como a la lista de clases de eventos. Los informes creados contienen información sobre el tiempo durante el cual los sitios debían estar protegidos de acuerdo con su horario de armado, así como el tiempo durante el cual los sitios estaban realmente armados.
- "Crear informes por guardias": permiso para crear informes sobre guardias. Al crear estos informes, el operador tiene acceso a una lista de sitios, así como a listas de clases de eventos y guardias. Los informes generados contienen información sobre los eventos recibidos, las acciones del operador para manejar alarmas y respuestas de guardia.
- "Generar informes por sitios": permiso para crear informes por sitios. Al crear estos informes, el operador tiene acceso a la lista de sitios. Los informes creados pueden contener toda la información disponible en las tarjetas del sitio.
- “Editar plantillas de informes”: permiso para crear formularios nuevos y editar los existentes, a partir de los cuales se pueden crear informes en el módulo “Administrador de informes”. Se recomienda encarecidamente no conceder este permiso a los operadores y también realizar cambios en las plantillas de informes sin realizar una copia de seguridad de los datos modificados.

8.1.5 Derechos del operador en el módulo "Mapas del sitio"

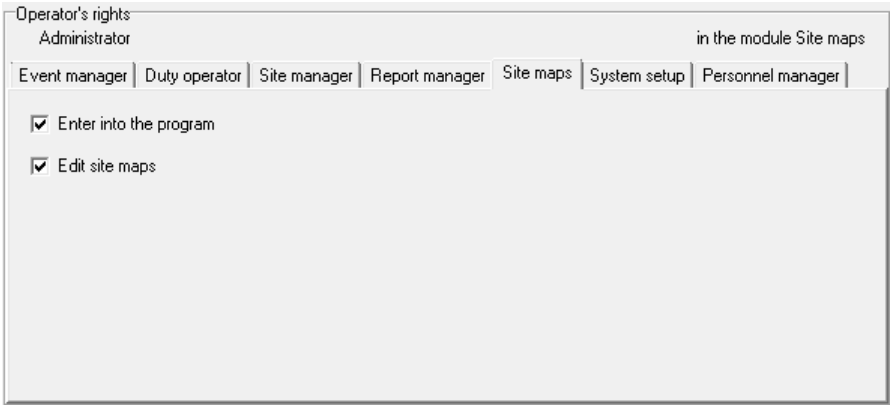


Figura 114: Derechos del operador en el módulo "Mapas del sitio"

- "Entrar en el programa" - permiso para entrar en el módulo "Mapas del sitio". Si el operador debe poder ver o editar mapas del sitio, incluyendo - para ver los mapas de los sitios cuando maneja una alarma, entonces él / ella tendrá este permiso.
- "Editar mapas del sitio": permiso para crear mapas del sitio nuevos y editar los existentes.

8.1.6 Derechos del operador en el módulo "Configuración del sistema"

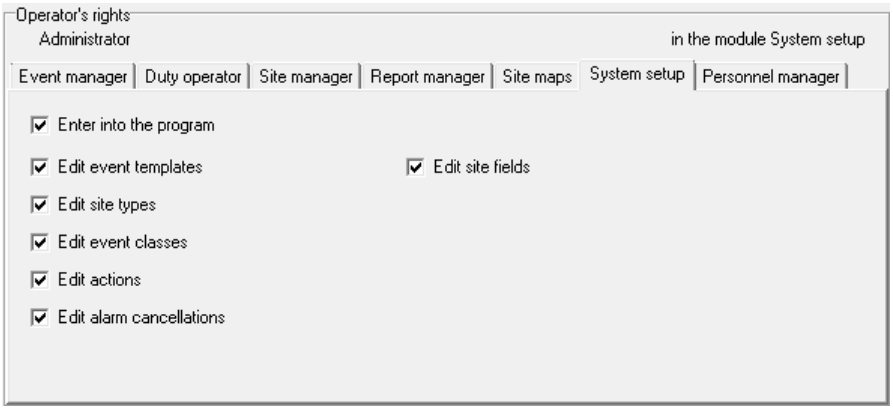


Figura 115: Derechos del operador en el módulo "Configuración del sistema"

- "Entrar en el programa" - permiso para entrar en el módulo "Configuración del sistema". Si el operador debe poder ver o cambiar la configuración de los directorios del sistema del Centro de seguridad, entonces tendrá este permiso.

- "Editar plantillas de eventos": permiso para crear nuevas y editar las plantillas de eventos existentes. La plantilla de eventos determina cómo se decodificarán los mensajes recibidos del equipo del sitio: qué mensajes se considerarán de alarma, qué mensajes se considerarán armados, etc. Cambios que se realizan en la descripción de la plantilla de eventos en la "Configuración del sistema" El módulo afectará a todos los sitios que utilicen la plantilla de evento editada. Se recomienda encarecidamente no realizar cambios en la plantilla de eventos del sitio sin una razón válida.
- "Editar tipos de sitios": permiso para crear nuevos tipos de sitios y editar los existentes. Los tipos son el mecanismo para agrupar y filtrar sitios en la lista. Si cambia, por ejemplo, cambia el nombre de un tipo de sitio en el módulo “Configuración del sistema”, este cambio afectará a todos los sitios para los que se estableció el tipo cambiado.
- "Editar clases de eventos": permiso para crear clases de eventos nuevas y editar las existentes. La clase de evento es una entidad clave para todos los procesos del software Security Center relacionados con el manejo de los eventos recibidos. La introducción de cambios en las clases de eventos se hará con cuidado y atención.
- “Editar acciones”: permiso para crear nuevas y editar las acciones del operador existentes, realizadas durante el manejo de alarmas. Para crear y editar scripts de manejo de alarmas, el usuario debe tener este permiso.
- “Editar cancelación de alarma”: permiso para crear nuevas y editar las causas existentes para cancelar alarmas. Para crear y editar scripts de manejo de alarmas, el usuario debe tener este permiso.
- “Editar campos del sitio”: permiso para editar los campos del sitio (características adicionales). Las características adicionales de los sitios son útiles en el evento, cuando es necesario agregar información a la tarjeta del sitio para la cual no hay un campo especial, y no es recomendable ingresarlo en notas. Este permiso puede ser necesario para aquellos usuarios del Centro de seguridad, cuya tarea es mantener la base de datos de las tarjetas del sitio.

8.1.7 Derechos del operador en el módulo "Configurador de claves Nord-LAN"

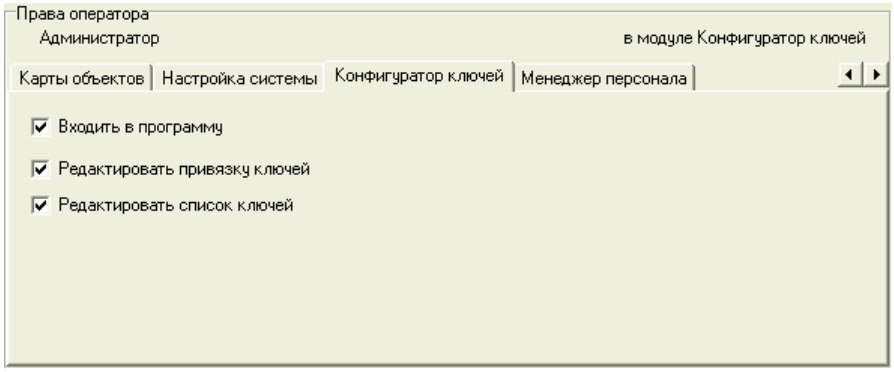


Figura 116: Derechos del operador en el módulo "Configurador de claves Nord-LAN"

- "Entrar en el programa" - permiso para iniciar el módulo "Configurador de claves Nord-LAN".
- "Editar asignación de claves": permiso para cambiar la lista de claves que le permiten armar o desarmar un sitio específico.
- "Editar lista de teclas" - permiso para editar la lista general de teclas Touch-memory, destinado a armar y desarmar sitios equipados con dispositivos de sitio "Nord-LAN".

8.1.8 Derechos del operador en el módulo "Administrador de personal"

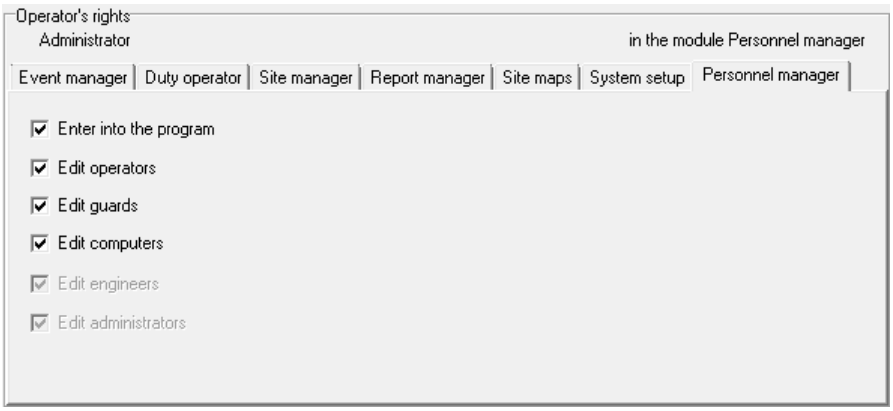


Figura 117: Derechos del operador en el módulo "Administrador de personal"

- "Entrar en el programa" - permiso para iniciar el módulo "Administrador de personal".
- "Editar operadores": permiso para indicar detalles de nuevos operadores, así como para cambiar la contraseña y los derechos de los operadores existentes. Un usuario con este permiso no puede cambiar sus propios derechos en los módulos del Centro de seguridad, así como los derechos del "Administrador".
- "Editar guardias": permiso para cambiar la lista de guardias. Los resguardos se utilizan para el manejo de alarmas: al registrar actividades relacionadas con un resguardo, el operador selecciona el resguardo, en relación con el cual se registra la acción, de la lista.
- "Editar equipos": permiso para editar la lista de equipos en los que se pueden iniciar los módulos del Centro de seguridad.
- "Editar ingenieros": permiso para editar la lista de ingenieros para otorgarles acceso remoto a los sitios.

8.2 guardias

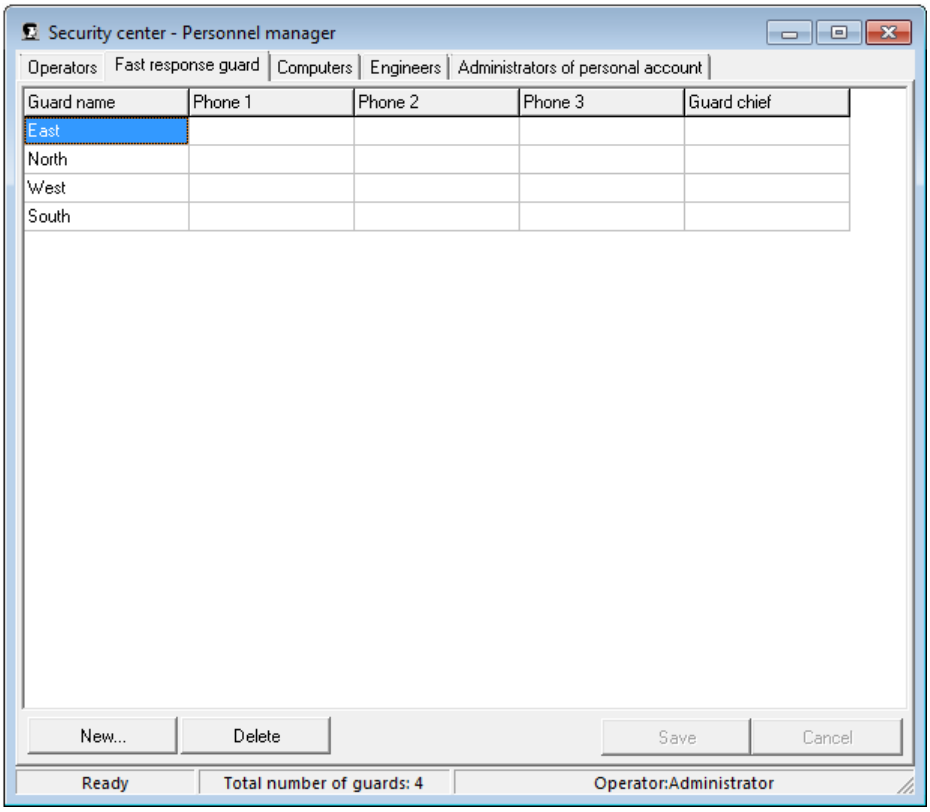


Figura 118: Pestaña "Guardias"

En la pestaña "Guardias" es posible editar la lista de guardias que se utilizan en el software Security Center.

Para guardar los cambios realizados en esta pestaña, el usuario deberá tener el permiso “Editar grupos” para el módulo “Administrador de personal”.

8.3 Ordenadores

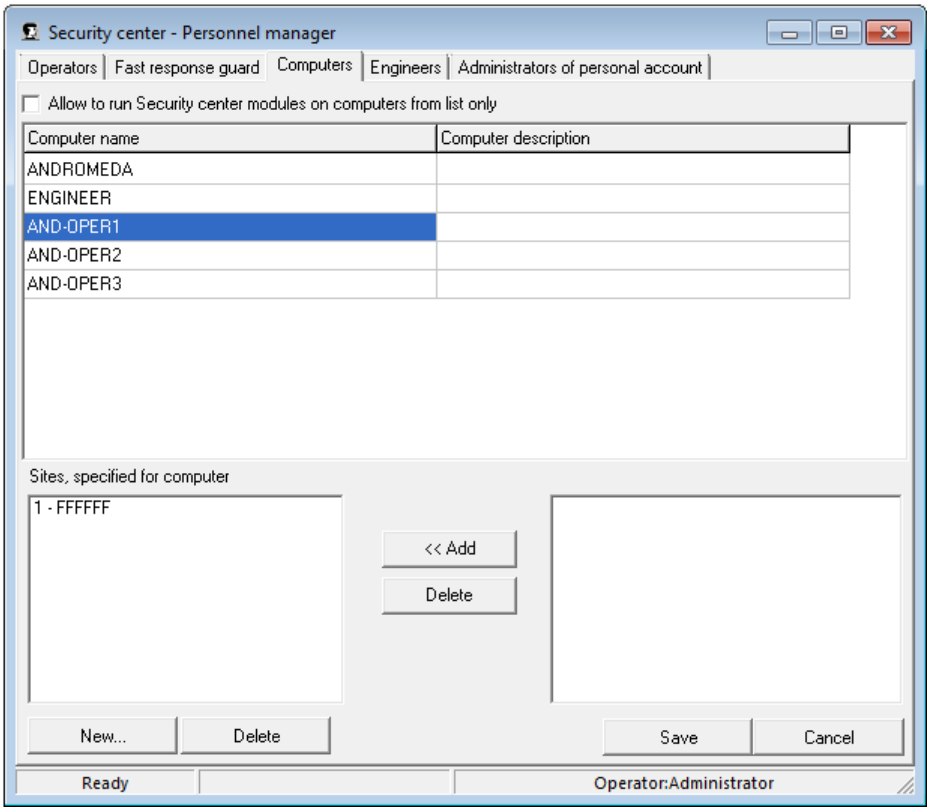


Figura 119: Pestaña "Ordenadores"

La pestaña "Computadoras" está destinada a administrar la lista de computadoras en las que se permiten los lugares de trabajo de red del software Security Center y a administrar la lista de sitios disponibles en estas computadoras.

Para guardar los cambios realizados en esta pestaña, el usuario deberá tener el permiso “Editar computadoras” para el módulo “Administrador de personal”.

8.3.1 Permitir ejecutar módulos de Security Center en equipos solo de la lista

Si esta opción está deshabilitada, los módulos del Centro de seguridad se pueden ejecutar en cualquier computadora de la red. En este caso, si el equipo en el que se ejecutan los módulos de Security Center no está incluido en la lista, se agregará allí automáticamente.

Si se incluye la restricción que permite que las estaciones de trabajo en red del Centro de seguridad se utilicen solo en aquellas computadoras que están incluidas en la lista, entonces el intento de iniciar cualquier módulo del Centro de seguridad en una computadora que no está en la lista. será rechazado. Las computadoras se agregarán a la lista manualmente.

8.3.2 Sitios especificados para computadora

Si es necesario, para cada computadora es posible de fi nir una lista de números de sitios que pueden ser descargados por los módulos del Centro de seguridad, que se inician en esta computadora.

Esta función es útil cuando los operadores de servicio utilizan el esquema de dividir los sitios entre los lugares de trabajo de la red. Por ejemplo, en una computadora, el operador trabaja con sitios desde el primer número hasta el tercer centésimo, en el siguiente - desde el número trescientos primero hasta el seiscientos y así sucesivamente.

8.4 Ingenieros {# staff-manager-engineer}

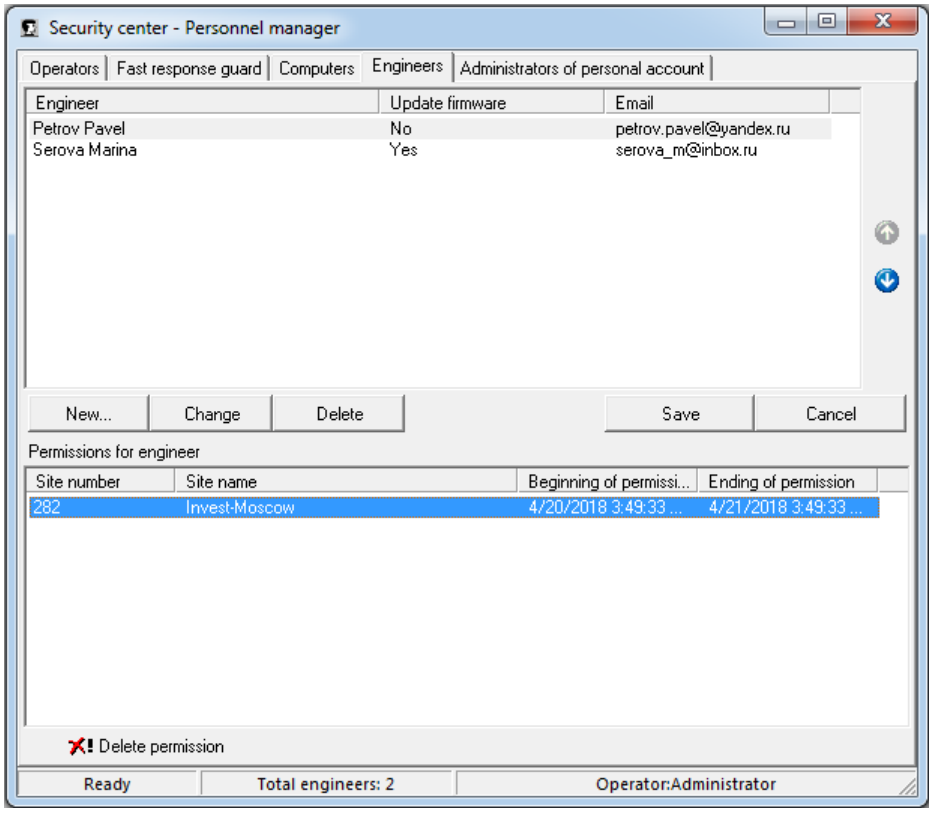


Figura 120: Pestaña "Ingenieros"

La pestaña "Ingenieros" se utiliza para administrar la lista de ingenieros a los que se les pueden otorgar permisos para acceder a la administración de sitios remotos.

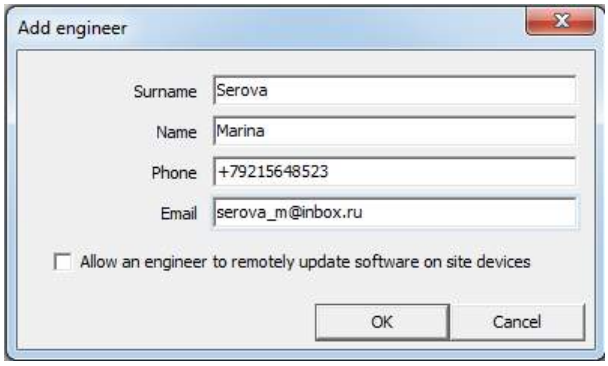


Figura 121: Agregar ingeniero

El usuario que tiene derecho a "Editar ingenieros" puede editar la lista de ingenieros.

Para agregar un ingeniero a la lista, haga clic en "Nuevo. . . " botón. Esto abre la ventana "Agregar ingeniero", en la que se llenarán los siguientes campos:

- "Apellido" es el apellido del ingeniero. El apellido y el nombre del ingeniero se ingresarán en letras rusas o latinas;
- "Nombre": el nombre del ingeniero;
- “Teléfono”: número de teléfono móvil en formato internacional;

- "Correo electrónico": la dirección de correo electrónico del ingeniero.

Después de ingresar los datos, haga clic en el botón "Agregar" para agregar el ingeniero. Al mismo tiempo, el apellido, el nombre y el correo electrónico del ingeniero creado se mostrarán en la lista de ingenieros. Para cancelar los cambios, haga clic en el botón "Cancelar".

Después de crear la cuenta de ingeniero, se le enviará una carta a su dirección de correo electrónico. El ingeniero deberá con fi rmar la dirección de correo electrónico para completar el registro en la Nube siguiendo el enlace en la carta y luego crear y con fi rmar la contraseña para acceder a la interfaz web para la programación del sitio remoto.

Para cambiar la información sobre el ingeniero, selecciónelo en la lista y haga clic en "Cambiar". Esto abre la ventana "Editar ingeniero". Es imposible cambiar el correo electrónico del ingeniero después de crear una cuenta en el sistema.

Para eliminar al ingeniero, selecciónelo en la lista y haga clic en “Eliminar”, luego con fi rme la eliminación en la nueva ventana.

Guarde los cambios en la lista de ingenieros haciendo clic en el botón "Guardar". De lo contrario, haga clic en el botón "Cancelar".

La información sobre los permisos otorgados al ingeniero para acceder a los sitios se muestra en la lista de "Permisos para ingeniero". Al seleccionar un ingeniero, la lista contiene información sobre el número de sitio, su nombre y la fecha y hora del inicio y finalización del permiso para acceder a él.

Para cancelar el permiso otorgado al ingeniero para acceder a un sitio, seleccione el permiso en la lista y haga clic en el botón "Eliminar permiso".

9 Mapas del sitio

Con la ayuda del módulo “Mapas del sitio”, es posible crear esquemas gráficos que describan el sitio: mapa del terreno con un mapa de posibles formas de acercarse al sitio, fotos del sitio, planos de planta, etc.

Una vez desarrollado el plano de las instalaciones del sitio, es posible colocar un diagrama de las coberturas de protección. Al

manejar una alarma, es posible ver las zonas de alarma en los mapas del sitio en el módulo "Operador de servicio".

No hay un editor gráfico incorporado en el módulo "Mapas del sitio", por lo que se recomienda crear esquemas utilizando herramientas de terceros. Las imágenes listas se pueden insertar en el mapa desde archivos BMP o JPG como imagen de fondo. Al preparar una imagen de fondo, seleccione su tamaño y resolución, teniendo en cuenta la posible impresión del mapa del sitio: no se realizan transformaciones, la imagen de fondo se imprime de acuerdo con sus parámetros.

Una vez seleccionada la imagen de fondo para el mapa, es posible colocar zonas en ella. Para cada zona, seleccione la ubicación y las dimensiones, así como la forma en que se muestra en el estado activo y pasivo. Luego, asocie el código de evento con la zona, cuyo registro significará la transición de la zona al estado activo. Normalmente, este código se selecciona como el código de alarma correspondiente a la zona.

Cuando se abre el archivo del sitio de alarma desde el módulo “Operador de servicio”, la tarjeta que contiene la zona en la que se recibió la alarma está activa. Además, la zona de alarma puede cambiar visualmente, mostrada alternativamente en el estado pasivo y activo.

También es posible especificar un archivo para la zona. Cuando se abre el archivo del sitio de alarma, el archivo asociado también se abrirá mediante los medios proporcionados en el sistema operativo para su tipo de archivo. Por ejemplo, si especifica un documento que contiene información importante sobre el sitio como archivo, este documento se abrirá junto con el archivo de mapa.

Si el software Security Center se utiliza en la red, el archivo del mapa del sitio se guardará en una carpeta que sea accesible para todos los usuarios de la red. Debe recordarse que incluso si esta carpeta es local para la computadora donde se editan los mapas del sitio, aún es necesario usar la ruta absoluta a la carpeta al guardar.

Al guardar un nuevo archivo de mapa del sitio o con un nombre diferente, el campo "Mapa del sitio" (su valor se puede ver y cambiar en el módulo "Administrador del sitio") se actualiza automáticamente.

Operador de 10 deber

El módulo "Operador de servicio" está diseñado para monitorear el estado operativo de los sitios, ver los eventos entrantes y registrar las acciones del operador mientras maneja las alarmas.

Antes de comenzar a trabajar en el módulo "Operador de servicio", asegúrese de que el módulo "Administrador de eventos" se esté ejecutando. Si durante el funcionamiento del módulo “Operador de servicio” se produce un error de conexión con el módulo “Gestor de eventos”, aparece una ventana con el error.

Figura 122: Mensaje de error de conexión con el módulo "Administrador de eventos"

Para iniciar el módulo "Operador de servicio", el usuario debe tener el permiso "Entrar en el programa" para este módulo.

Al igual que el resto de los módulos del Centro de seguridad, el módulo “Operador de servicio” descarga solo aquellos sitios, cuyo uso está permitido en la computadora en la que se está ejecutando. Es posible especificar los intervalos de los números de sitio. eso puede ser utilizado en un lugar de trabajo de red particular en el módulo "Administrador de personal".

10.1 Ventana principal del módulo

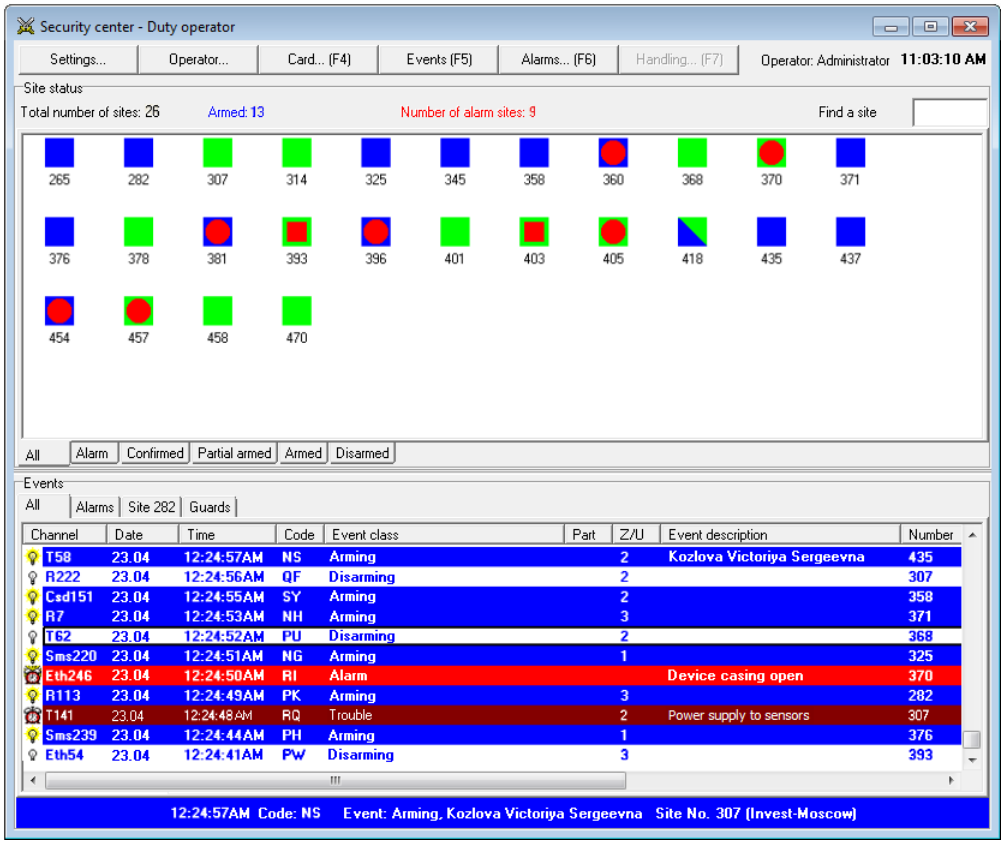


Figura 123: Ventana principal del módulo

La ventana principal del módulo "Operador de servicio" se divide en dos partes. La parte superior está destinada a mostrar sitios, la inferior para mostrar los eventos recibidos.

10.2 Barra de herramientas de acceso rápido

La barra de herramientas contiene botones que permiten acceder a las funciones más solicitadas del módulo “Operador de servicio”. Además del nombre de la función, se proporciona una tecla o una combinación de teclas entre paréntesis para acceder a la función desde el teclado.

Figura 124: Barra de herramientas de acceso rápido

Haga clic en el botón "Configuración" para abrir la ventana de configuración del módulo "Operador de servicio". Para que el usuario pueda realizar cambios en la configuración del módulo, deberá tener el permiso "Cambiar configuración" para el módulo "Operador de servicio".

Haga clic en el "Operador. . . ”Para cambiar el operador registrado en el módulo“ Operador de servicio ”. Después de hacer clic en el botón, se mostrará la ventana de registro del operador en el módulo, el módulo "Operador de servicio" no se detendrá: la recepción de eventos continuará y cuando se reciba una alarma, se mostrará la ventana de manejo de alarmas.

Haga clic en "Tarjeta. . . "Para acceder a la ventana" Tarjeta del sitio ". Se mostrará la ventana del sitio actual. El sitio actual será el sitio seleccionado en la lista de sitios, o el sitio cuyo evento está seleccionado en la lista de eventos, dependiendo de la ventana enfocada.

Haga clic en el botón "Eventos" para activar la pestaña "Eventos del sitio" en la ventana del evento y para mostrar los eventos del sitio actual en la lista de eventos en esta pestaña. Las reglas para seleccionar el sitio actual serán las mismas que al hacer clic en la “Tarjeta. . . " botón.

Haga clic en "Alarmas. . . ”Para acceder a la ventana“ Información de alarma ”. Una vez abierta la ventana, se cargarán en ella la tarjeta del sitio actual y el registro de manejo de la última alarma de este sitio.

Haga clic en "Manejo. . . ”Para abrir la ventana“ Manejo de alarmas ”. El botón está activo si el operador, que inició el módulo, tiene permiso para "Manejar alarmas" o "Cancelar alarma". Además, el botón solo está disponible si el sitio actual es un sitio de alarma.

10.3 Sitios

En la parte superior de la ventana "Estado del sitio", se indica el número total de sitios cargados por el módulo, el número de sitios que están actualmente armados y el número de sitios cuyo manejo de alarmas aún no se ha completado.

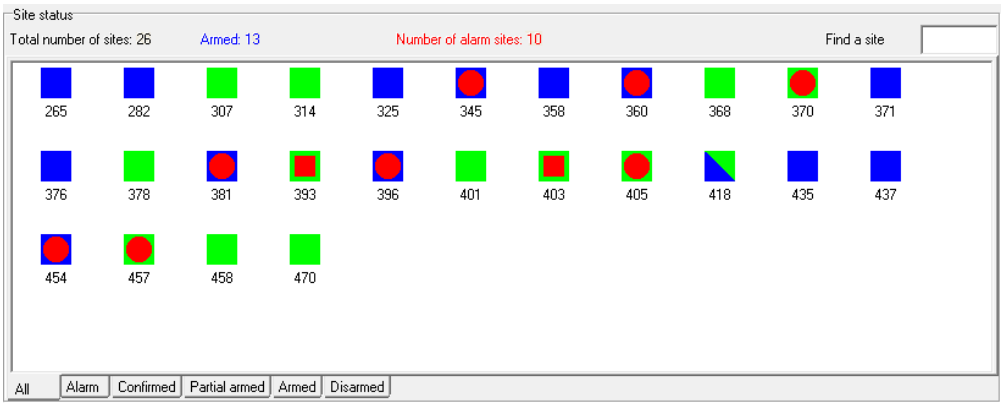


Figura 125: Ventana "Estado del sitio", pestaña "Todos"

Los sitios protegidos se muestran en el módulo "Operador de servicio" en forma de iconos en la ventana "Estado del sitio". El color del icono muestra el estado actual del sitio. Si es azul, entonces el sitio está armado, el verde está desarmado, gris - el sitio está deshabilitado. Si una parte del icono es azul y la otra es verde, el sitio está parcialmente armado. Un círculo o cuadrado rojo significa que hay una alarma en el sitio, que aún no se ha completado, mientras que un círculo rojo indica que no se ha registrado ninguna acción para esta alarma.

Debe recordarse que las alarmas recibidas desde sitios deshabilitados son manejadas por el sistema automáticamente, inmediatamente después de su recepción. Los eventos de armado y desarmado recibidos de sitios deshabilitados tampoco cambian su estado. Por lo tanto, el sitio deshabilitado no puede ser alarmante, armado o desarmado. Siempre se muestra con un icono gris.

Los iconos del sitio se muestran en pestañas que agrupan los sitios por estados básicos. El propósito de las pestañas es fácil de adivinar por sus nombres:

- la pestaña "Todos" muestra todos los sitios que pueden utilizarse en este lugar de trabajo;
- en la pestaña "Alarmas", se muestran los sitios para los que hay alarmas no controladas;
- la pestaña "Armado parcial" muestra los sitios que estaban armados parcialmente. En este caso, no todo el sitio está protegido, sino solo sus zonas particulares;
- la pestaña "Armado" muestra los sitios que están actualmente armados;
- la pestaña "Desarmado" muestra los sitios que están actualmente desarmados, o sitios cuyo estado no está definido, porque nunca han enviado ningún evento sobre el armado o desarmado.

Para encontrar rápidamente un sitio por número, utilice el campo para buscar un sitio en la esquina superior derecha del "Estado del sitio". ventana. La búsqueda de un sitio se lleva a cabo en la misma pestaña que está actualmente activa y se ejecuta "sobre la marcha", a partir los dígitos del número de sitio se ingresa en el campo de búsqueda.

10.3.1 Descripción emergente {# duty-opertor-tooltip}

Cuando pasa el cursor sobre un sitio en la ventana "Estado del sitio", aparece una información sobre herramientas con la que el operador del Centro de seguridad puede obtener rápidamente la información sobre el sitio requerido. La información sobre herramientas contiene la siguiente información:

- número, nombre y dirección del sitio;
- estado del sitio o sus partes (armado o desarmado);
- descripción de la situación de alarma en el sitio;
- información sobre los guardias llamados al sitio.

10.3.2 Estado del sitio

La información sobre herramientas contiene información sobre el estado del sitio si al menos un sitio está armado o desarmado.

Figura 126: Ventana "Estado del sitio", descripción emergente, estado del sitio

La información sobre herramientas indica la hora en que el sitio se armó o desarmó si el evento ocurrió dentro de las últimas 24 horas, o la fecha si el evento ocurrió antes. El color de fondo indica el estado actual del sitio: azul: el sitio está armado, el verde está desarmado. Cabe señalar que cuando se selecciona el parámetro "Mostrar color de estado al revés", los colores

que muestran el estado de los sitios protegidos están invertidos. Además, la información sobre herramientas informa sobre el usuario que completó el armado o desarmado del sitio.

Si el sitio está dividido en secciones, la información sobre herramientas proporciona información sobre el estado de cada parte del sitio. En este caso, la información sobre herramientas contiene la siguiente información: hora del último armado o desarmado, descripción de la pieza y el usuario que realizó la operación. El último evento registrado se muestra en negrita.

10.3.3 Alarma

Si se registra una situación de alarma en el sitio, la información sobre herramientas contiene información sobre la alarma. Si se registran varios eventos de alarma en el sitio, la información sobre herramientas muestra información sobre la primera y la última alarma registrada.

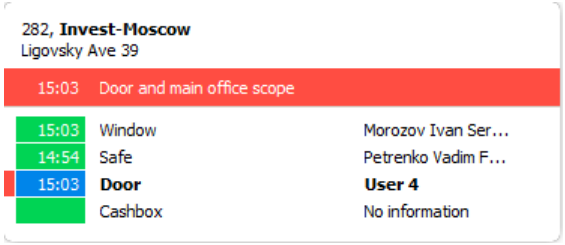


Figura 127: Ventana "Estado del sitio", información sobre herramientas, alarma

La información sobre herramientas indica la hora de la alarma si el evento ocurrió dentro de las últimas 24 horas, o la fecha si el evento ocurrió antes. El fondo rojo indica una situación de alarma en el sitio.

Si el sitio está dividido en partes, las partes de la alarma son rojas.

10.3.4 Guardias

La información sobre herramientas contiene información sobre la Guardia, si la Guardia es llamada al sitio ("Guardia en ruta") o está presente en el sitio ("Guardia en el sitio"). Si se cancela la llamada de Guardia al sitio, no se muestra la información de la llamada.

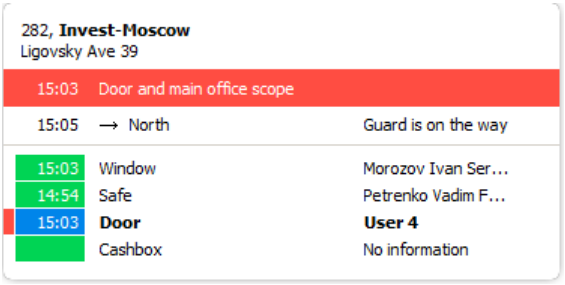


Figura 128: Ventana "Estado del sitio", información sobre herramientas, Guardia

La información sobre herramientas indica la hora de la llamada del Guardia o la llegada al sitio, si el evento ocurrió dentro de las últimas 24 horas, o la fecha si el evento ocurrió antes.

10.3.5 Menú contextual

Cuando hace clic con el botón derecho en el icono del sitio, se muestra un menú contextual con el que puede acceder rápidamente a la información sobre el sitio.

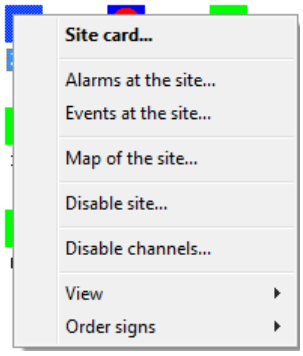


Figura 129: Ventana "Estado del sitio", menú contextual

Seleccionando la “Tarjeta del sitio. . . ”Para acceder a la ventana que muestra los campos de la tarjeta del sitio seleccionado. El aspecto de la ventana y su descripción se presentan a continuación, en la sección “Ventana de la tarjeta del sitio”.

Las “Alarmas en el sitio. . . El elemento ”está destinado al acceso a la ventana, mostrando información sobre las alarmas en el sitio, cuyo manejo se completa. Además de las alarmas en sí, esta ventana muestra el registro de manejo de alarmas del operador. Vea más información sobre esta ventana a continuación, en la sección “Ventana de alarmas”.

Seleccione el elemento del menú "Eventos en el sitio" para activar la pestaña "Sitio" en la parte inferior de la ventana principal del módulo "Operador de servicio". La pestaña está destinada a mostrar eventos para un sitio en particular y los eventos del sitio seleccionado se cargarán en ella.

Utilice el “Mapa del sitio. . . ”Para abrir el archivo de mapa (plano gráfico) del sitio. Si se especifica un archivo de formato gráfico (BMP o JPG) como mapa del sitio, se abrirá para su visualización en la ventana especial del módulo "Operador de servicio". Si el mapa del sitio se crea con la ayuda del módulo "Mapas del sitio", este módulo se abrirá para verlo.

El elemento "Deshabilitar sitio" en el menú contextual permite deshabilitar temporalmente cualquier sitio del Centro de seguridad, guardando toda la información sobre el sitio en el sistema. Esta característica es conveniente durante el mantenimiento de rutina o la reparación del equipo instalado en el sitio.

Los sitios del Security Center pueden ser deshabilitados por el operador con el permiso correspondiente. Seleccione el elemento "Desactivar sitio" para ver la ventana "Desactivación del sitio", que contiene información sobre el número y el nombre del sitio. Ingrese el tiempo durante el cual el sitio estará deshabilitado en el campo "Deshabilitar para" de esta ventana. Después de este tiempo, el sitio se habilitará automáticamente. Ingrese el tiempo en minutos, el valor máximo permitido es 180 minutos. Especifique el motivo de la desactivación temporal del sitio en el campo "Motivo de la desconexión". Este campo es obligatorio. Antes de hacer clic en el botón "Desactivar sitio", estudie la advertencia que alerta automáticamente sobre la hora en que el sitio se desactiva automáticamente (por ejemplo, "El sitio se habilitará automáticamente en 120 minutos, hoy a las 22:16").

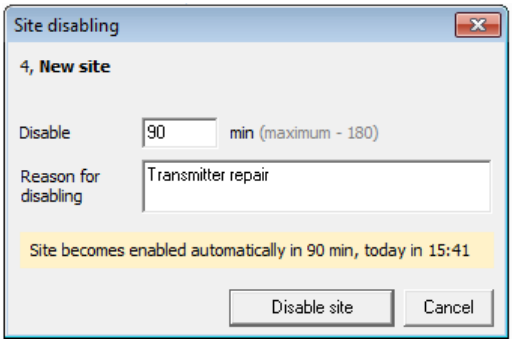


Figura 130: Ventana "Estado del sitio", ventana "Inhabilitación del sitio"

El registro de eventos muestra información sobre la desactivación del sitio, a saber: fecha y hora de la desactivación del sitio; operador que realizó la inhabilitación; tiempo y motivo de la inhabilitación.

El elemento "Habilitar sitio" permite habilitar el sitio de Security Center previamente deshabilitado antes de que expire el tiempo especificado durante la deshabilitación.

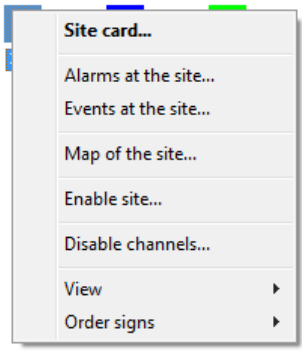


Figura 131: Ventana "Estado del sitio", menú contextual, elemento "Habilitar sitio"

Seleccione el elemento "Activar sitio" para ver la ventana "Activación del sitio", que contiene información sobre el número de sitio y el nombre y la hora de la desactivación automática del sitio. Para habilitar el sitio, haga clic en el botón "Habilitar sitio" de esta ventana.

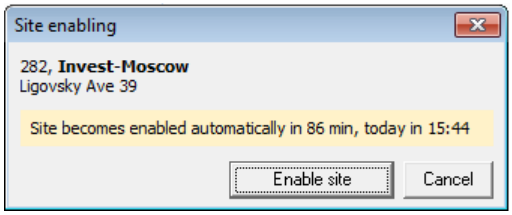


Figura 132: Ventana "Estado del sitio", ventana "Habilitación del sitio"

El registro de eventos muestra información sobre la habilitación del sitio, a saber: fecha y hora de la habilitación del sitio; modo de habilitación (automático o manual). Si el sitio se habilita manualmente, el operador que realizó la operación se especifica para el evento.

El elemento "Deshabilitar canales" en el menú contextual permite deshabilitar temporalmente cualquier canal del sitio, guardando toda la información sobre el canal en el sistema. Esta función es conveniente en caso de un mal funcionamiento del equipo utilizado para los canales de comunicación.

El canal de comunicación puede ser desactivado por el operador, que tiene derecho a "Desactivar canales para el sitio". Seleccione el elemento "Desactivar canales" para ver la ventana "Desactivación de canales del sitio", que contiene información sobre el número y el nombre del sitio. Seleccione uno o varios canales de comunicación para deshabilitar en la sección "Canales que se pueden deshabilitar": Radio, Teléfono, Sistema, Ethernet, GPRS, SMS y CSD. Ingrese el tiempo durante el cual los canales estarán deshabilitados en el campo “Deshabilitar por” de esta ventana. Pasado este tiempo, los canales se habilitarán automáticamente. Ingrese el tiempo en minutos, el valor máximo permitido es 180 minutos. Especifique el motivo de la desactivación temporal del canal en el campo "Motivo de la desconexión". Este campo es obligatorio. Antes de hacer clic en el botón "Desactivar canales",

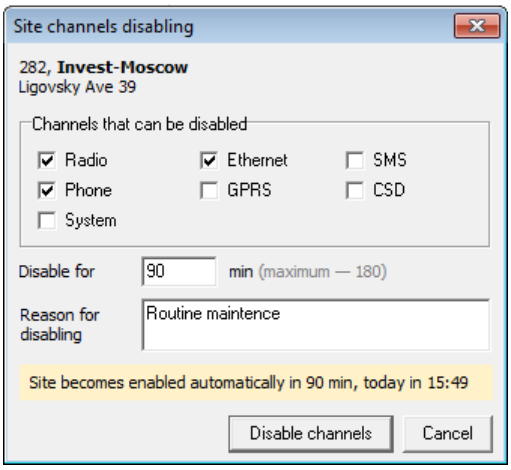


Figura 133: Ventana "Estado del sitio", ventana "Deshabilitación de canales del sitio"

El registro de eventos muestra información sobre la desactivación del canal, a saber: fecha y hora de la desactivación del canal; Nombre del Canal; período y motivo de la inhabilitación.

El elemento “Habilitar canales” permite habilitar los canales previamente deshabilitados antes de que expire el tiempo especificado durante la deshabilitación.

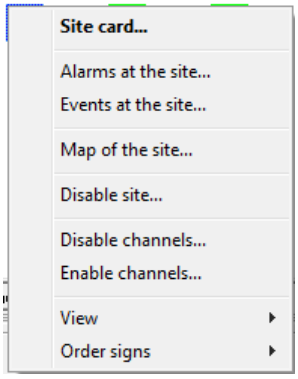


Figura 134: Ventana "Estado del sitio", menú contextual, elemento "Habilitación de canales del sitio"

Seleccione el elemento "Habilitar canales" para ver la ventana "Habilitación de canales del sitio", que contiene información sobre el número y el nombre del sitio. Seleccione uno o varios canales de comunicación para habilitar en la sección "Canales que se pueden deshabilitar" y haga clic en el botón "Habilitar canales":

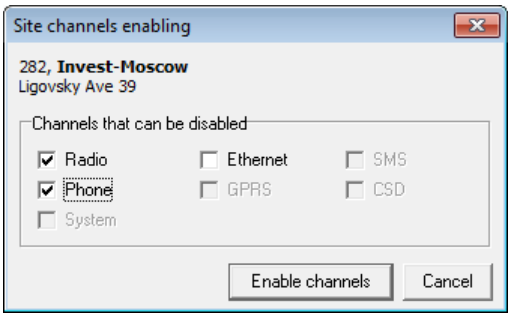


Figura 135: Ventana "Estado del sitio", ventana "Habilitación de canales del sitio"

El registro de eventos muestra información sobre la habilitación del canal, a saber: fecha y hora de la habilitación del canal; modo de habilitación (automático o manual). Si el canal se habilita manualmente, el operador que realizó la operación se especifica para el evento.

El elemento "Ver" está destinado a cambiar la forma en que se muestra la lista de sitios.

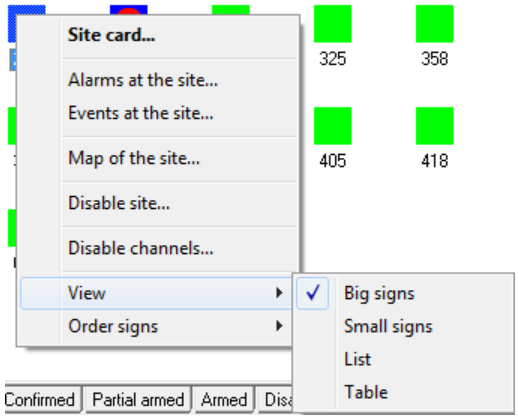


Figura 136: Ventana "Estado del sitio", menú contextual, elemento "Ver"

Los elementos “Iconos grandes”, “Iconos pequeños”, “Lista” difieren sólo en el tamaño del icono del sitio y en la forma en que se desplazan los elementos en la ventana. En cuanto al elemento "Tabla", si se selecciona en la ventana "Estado del sitio", se mostrará una lista de sitios similar a la lista de sitios utilizados en el módulo "Administrador del sitio".

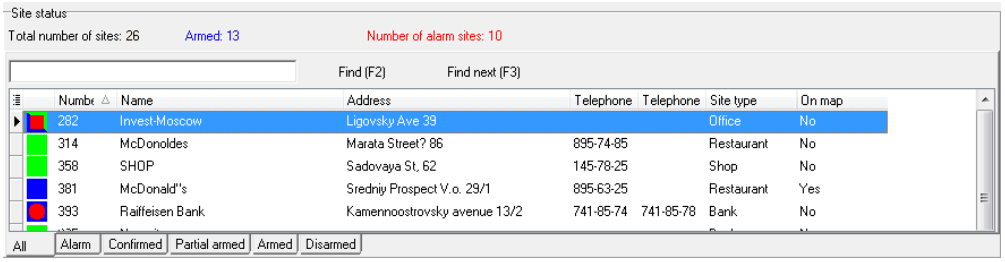


Figura 137: Ventana "Estado del sitio", pestaña "Todos", vista "Tabla"

En el capítulo dedicado al módulo "Administrador del sitio" se ofrece una descripción detallada de las funciones de dicha lista de sitios. Cabe señalar aquí que esta lista de sitios permite buscar un sitio utilizando la mayoría de los campos significativos, y no solo por número, y además, el operador puede ver los campos del sitio necesarios para él / ella sin abrir un ventana separada con la tarjeta del sitio.

El elemento del menú contextual "Organizar iconos" tiene como objetivo cambiar la forma en que se ordenan los iconos de los sitios cuando se muestran.

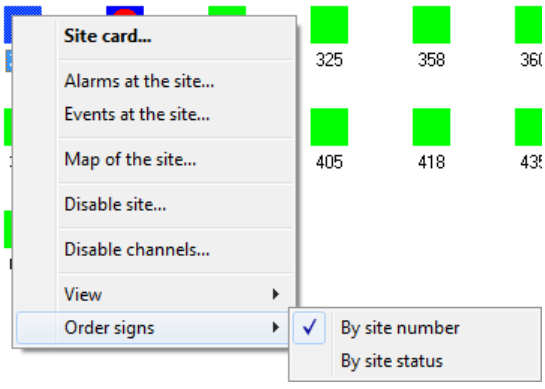


Figura 138: Ventana "Estado del sitio", menú contextual, elemento "Organizar iconos"

Si selecciona ordenar por número de sitio, los iconos de sitio en la lista se mostrarán en orden ascendente de números de sitio. Si selecciona ordenar por estado del sitio, el estado del sitio se tendrá en cuenta en primera instancia.

En este caso, primero se mostrarán los sitios para los que hay alarmas indefinidas, y los primeros en la lista serán aquellos sitios en los que aún no se ha iniciado el manejo de alarmas. Después de los sitios de alarma, se mostrarán los sitios que están armados.

Los sitios desarmados y deshabilitados más recientemente se mostrarán en la lista como último, así como los sitios cuyo estado no está definido.

Cabe señalar que el elemento resaltado en el menú contextual en negrita es el elemento predeterminado y se ejecutará en caso de hacer doble clic en el sitio con el botón izquierdo del mouse. Si no hay alarmas indefinidas para el sitio seleccionado, entonces el elemento “Tarjeta del sitio. . . ”Es el elemento predeterminado. Si se selecciona el sitio de la alarma, el elemento predeterminado es “Manejo de alarmas. . . ”, Después de seleccionarla, se abre una ventana destinada al manejo de alarmas del sitio:

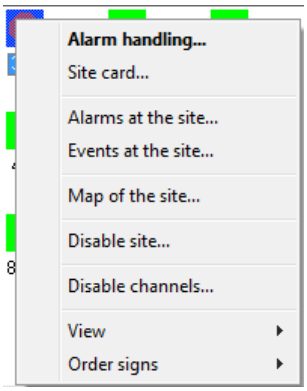


Figura 139: Ventana "Estado del sitio", menú contextual, elemento "Habilitar sitio"

10.4 Eventos

En la parte inferior de la ventana principal del módulo "Operador de servicio", se muestran los eventos recibidos y el estado de los guardias.

Los eventos se dividen en tres categorías, cada una de las cuales se muestra en una pestaña separada.

10.4.1 Todo

Figura 140: Ventana "Eventos", pestaña "Todos"

La pestaña "Todos" muestra todos los eventos significativos recibidos de los sitios cargados por el módulo "Operador de servicio". Para aclarar qué eventos se consideran significativos, se mencionará que se ha implementado un mecanismo de filtrado de eventos de prueba y duplicado, que permite que el operador del Centro de Seguridad sea liberado de manejar información que no le importa. en el software Security Center. El mecanismo de filtrado de eventos se controla con la configuración del módulo "Administrador de eventos". Consulte el capítulo dedicado a este módulo para familiarizarse con los detalles de este mecanismo. Aquí se mencionará que los eventos en los que los eventos significativos son aquellos que no se prueban ni se repiten, y solo se muestran en la pestaña “Todos”. Si el operador de servicio por alguna razón necesita ver todos los eventos recibidos de un sitio en particular,

La siguiente información se muestra en las columnas de la tabla de la ventana "Eventos":

- “Canal”: tipo y número del canal a través del cual se acepta el evento. El valor de este parámetro lo determina el origen del evento con el que se recibió el evento. Consulte más información sobre las fuentes de eventos existentes y su configuración en el capítulo sobre el módulo en la sección "Fuentes de eventos".
- “Fecha”, “Hora” - fecha y hora de la recepción del evento por el equipo de la estación de monitoreo. Si la información transmitida por el equipo receptor de la estación de monitoreo no contiene la fecha y hora de recepción del evento, entonces esta columna mostrará la fecha y hora de registro del evento en la base de datos del software Security Center.
- “Código”, “Clase de evento”, “Parte”, “Z / U”, “Descripción del evento” son los parámetros obtenidos como resultado de la decodificación del evento recibido de acuerdo con la descripción del sitio. Vea más detalles sobre los parámetros en los capítulos sobre los módulos “Configuración del sistema” y “Administrador del sitio”, en las secciones que describen las plantillas de eventos.
- “Número”, “Nombre”, “Dirección” son los campos del mismo nombre de la tarjeta del sitio desde donde se recibió el evento.

Los eventos de la lista se pueden ordenar por cualquiera de las columnas mostradas. Para hacer esto, haga clic izquierdo en la columna necesaria.

Al hacer clic con el botón derecho en el evento, se muestra un menú contextual con el que puede acceder rápidamente a información sobre el sitio.

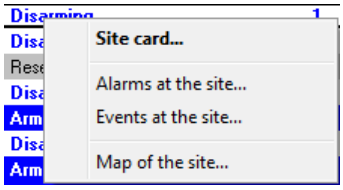


Figura 141: Ventana "Eventos", menú contextual

El propósito de los elementos del menú es completamente similar al del menú contextual que se muestra al hacer clic en el icono del sitio en la ventana "Estado del sitio".

10.4.2 Alarmas

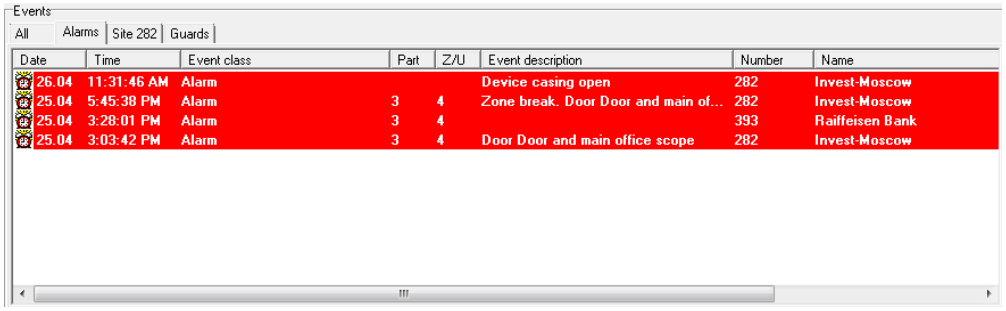


Figura 142: Ventana "Eventos", pestaña "Alarmas"

La pestaña "Alarmas" muestra los eventos de alarma que aún no se han completado.

10.4.3 Eventos en el sitio

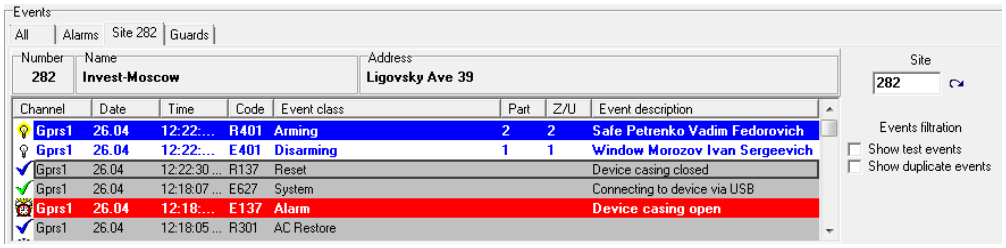


Figura 143: Ventana "Eventos", pestaña "Eventos en el sitio"

La pestaña "Eventos en el sitio" muestra un resumen del sitio seleccionado, así como los eventos recibidos de él.

Para cambiar un sitio, qué eventos se muestran en la pestaña "Eventos en el sitio", ingrese su número en el campo "Cambiar sitio" y presione la tecla "Enter" o el botón de flecha.

Utilice el parámetro "Mostrar pruebas" para habilitar o deshabilitar la visualización de eventos de prueba filtrados recibidos del sitio. De manera similar, use el parámetro "Mostrar duplicados" para habilitar o deshabilitar la visualización de eventos duplicados filtrados recibidos del sitio.

Haga clic con el botón derecho en el evento para mostrar el menú contextual, con el que puede deshabilitar temporalmente el evento.

El operador puede desactivar los eventos con el permiso "Desactivar códigos de eventos". Si selecciona la opción "Desactivar evento", aparece un cuadro de diálogo con información sobre el número, nombre y dirección del sitio. Además, se indica lo siguiente: código de evento; clase de evento; número de la parte en la que ocurrió el evento; número de la zona en la que ocurrió el evento; descripción del evento.

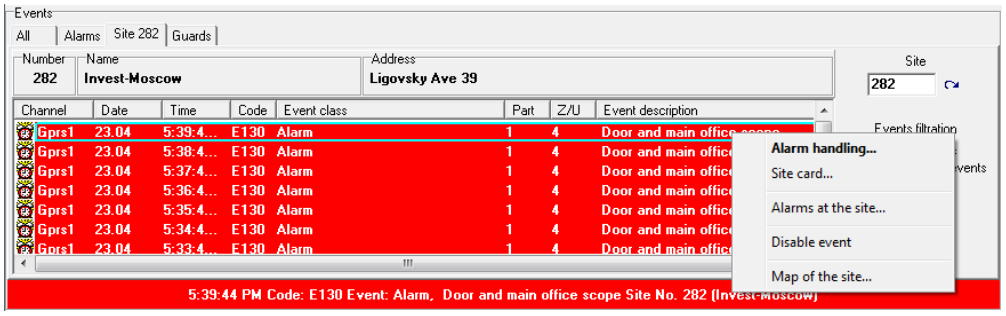


Figura 144: Ventana "Eventos", menú contextual, elemento "Desactivar evento"

Introduzca el tiempo durante el cual se desactivará el evento en el campo "Desactivar para" de esta ventana. Pasado este tiempo, el evento se habilitará automáticamente. Ingrese el tiempo en minutos, el valor máximo permitido es 90 minutos. Especifique el motivo de la desactivación temporal del evento en el campo "Motivo de la desconexión". Este campo es obligatorio. Antes de hacer clic en el botón "Desactivar evento", estudie la advertencia que alerta automáticamente sobre la hora en que el evento se desactiva automáticamente (por ejemplo, "El evento se activará automáticamente en 45 minutos, hoy a las 21:51").

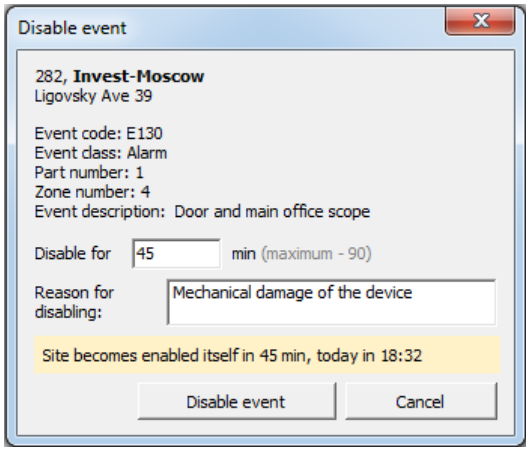


Figura 145: Ventana "Eventos", ventana "Desactivar evento"

El registro de eventos muestra información sobre la desactivación del evento, a saber: fecha y hora de la desactivación del evento; código de evento; números de pieza y zona, período y motivo de la desactivación.

El elemento "Habilitar evento" en el menú contextual permite habilitar un evento previamente deshabilitado antes de la expiración del período, especificado para deshabilitar.

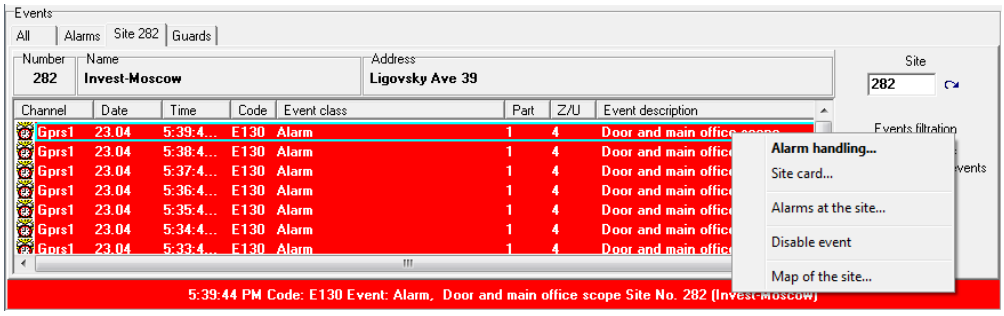


Figura 146: Ventana "Eventos", menú contextual, elemento "Habilitar evento"

Si selecciona el elemento "Activar evento", aparece un cuadro de diálogo con información sobre el número y el nombre del sitio. Además, se indica lo siguiente: código de evento; clase de evento; número de la pieza; número de la zona; descripción del evento. La ventana también indica la hora de la habilitación automática del evento. Para habilitar el evento, haga clic en el botón "Activar evento" de esta ventana.

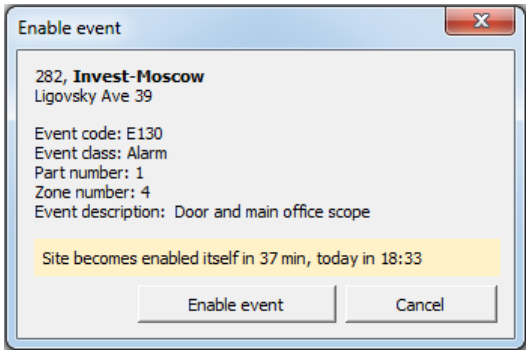


Figura 147: Ventana "Eventos", ventana "Activar evento"

El registro de eventos muestra información sobre la habilitación del evento, a saber: fecha y hora de la habilitación del evento; código de evento; números de pieza y zona; modo de habilitación (automático o manual). Si el evento se habilita manualmente, el operador que realizó la operación se especifica para el evento.

10.4.4 Estado de los guardias

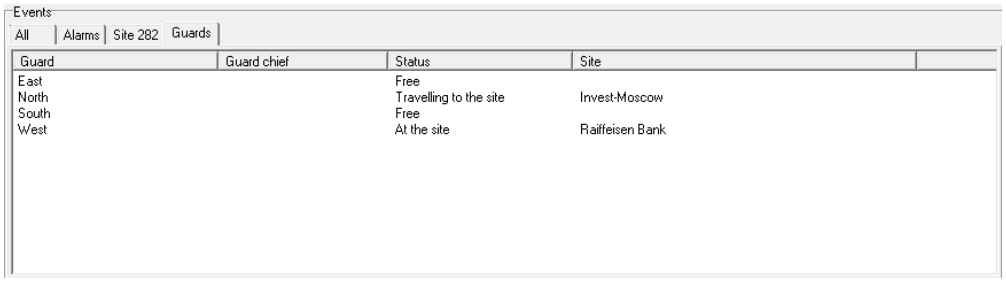


Figura 148: Pestaña "Eventos", pestaña "Guardia"

La pestaña "Guardias" muestra los guardias utilizados por el Centro de seguridad. Además de la información general sobre los guardias en la pestaña, se muestra su estado actual ("Gratis", "Viajando al sitio", "En el sitio") y el nombre del sitio al que se llama al guardia, si está ocupado actualmente.

10.5 Manejo de alarmas

La ventana está diseñada para manejar una alarma por parte del operador, que tiene el permiso de "Manejar alarma". El manejo de alarmas significa registrar las acciones realizadas por el operador en el registro de alarmas. Este registro se mantiene en el módulo "Operador de servicio", la información de este se puede imprimir en el módulo "Administrador de informes".

Cuando se recibe el evento de alarma, la ventana "Manejo de alarmas" se abre automáticamente. Esta función se puede desactivar en la configuración del módulo "Operador de servicio". Si necesita volver a abrir la ventana "Manejo de alarmas", haga doble clic en el sitio de alarma o evento de alarma que necesita manejar.

Al manejar una alarma, es importante comprender que si se recibe otra alarma del sitio durante el proceso de alarma, ambas alarmas se combinarán en un grupo y luego se manejarán juntas. De la misma manera, estos eventos se mostrarán juntos al visualizar las alarmas manejadas y al crear informes de alarmas en el módulo “Administrador de informes”.

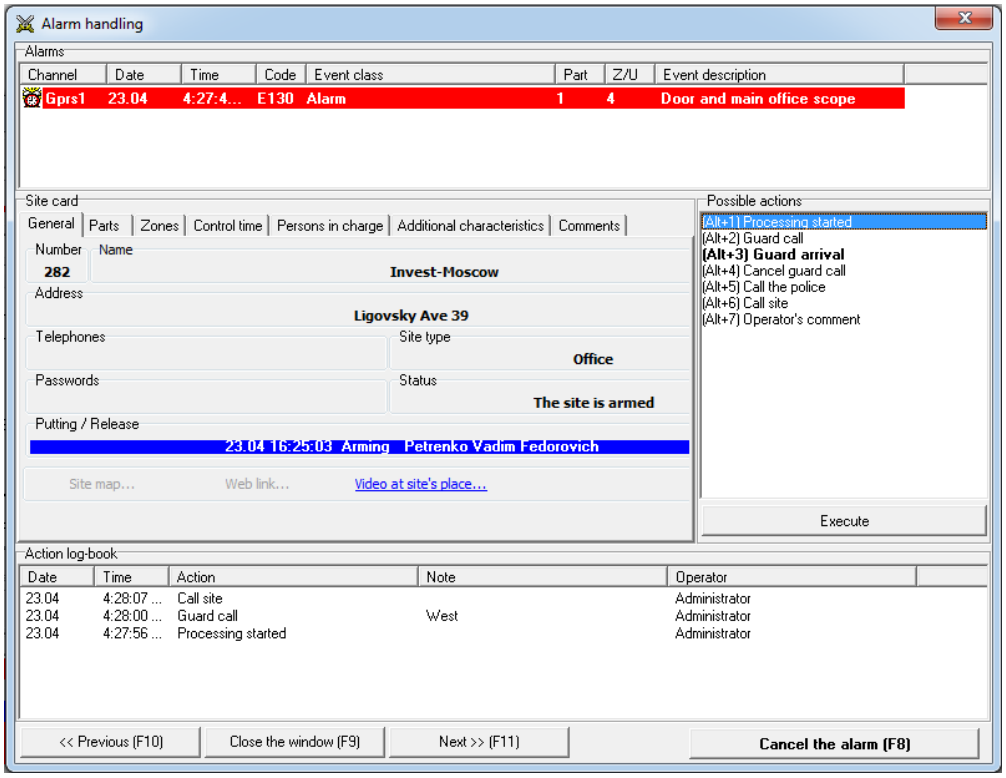


Figura 149: Ventana "Manejo de alarmas"

En la parte superior de la ventana "Manejo de alarmas", se muestran todas las alarmas del sitio que se deben manejar.

En la parte central de la ventana hay una tarjeta del sitio, en diferentes pestañas de las cuales se muestra información sobre el sitio. El propósito de los campos del sitio mostrados se analiza en detalle en el capítulo dedicado al módulo "Administrador del sitio".

El enlace “Video en el lugar del sitio” permite al operador ver el video transmitido por las cámaras instaladas en el sitio. Cuando se hace clic en el enlace, se abre una ventana, donde se muestra el video en vivo de todas las cámaras instaladas en el sitio conectadas al enrutador de video.

> Para ver videos de las cámaras, debe tener Adobe Flash Player instalado en la computadora con la última versión disponible que se puede descargar desde el sitio web oficial de Adobe.

A la derecha de la tarjeta del sitio se encuentra una lista de acciones que el operador puede realizar durante el manejo de una alarma. Esta lista incluye las acciones que se asignan a las clases de los eventos que se manejarán. Así, para diferentes alarmas, el operador ve varias acciones posibles, lo que permite ayudar y gestionar el trabajo del operador.

Las primeras diez acciones de la lista se pueden registrar utilizando las teclas numéricas del teclado como teclas de método abreviado. Si es necesario, en lugar de presionar una sola tecla numérica, es posible presionarla en combinación con la tecla “Alt”. La opción con la que es posible habilitar o deshabilitar el uso de la tecla “Alt” para un acceso rápido a las acciones está en la configuración del programa.

Vea más información sobre cómo crear posibles acciones durante el manejo de alarmas, así como cómo asignar acciones a clases de eventos, en el capítulo dedicado al módulo “Configuración del sistema”.

10.5.1 Llamar a un guardia al sitio

Al registrar una acción con el tipo "Llamar a un guardia", se muestra una ventana en la que el operador seleccionará el guardia que llamó en el sitio.

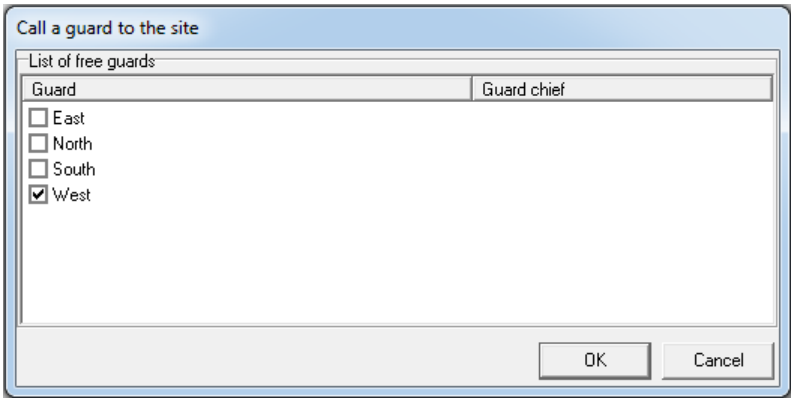


Figura 150: Ventana "Llamar a un guardia al sitio"

Para registrar una llamada de guardia, verifíquela en la lista de guardias y presione el botón "OK". Es posible marcar un guardia en la lista de dos formas: haciendo clic con el botón izquierdo en la casilla de verificación a la izquierda del nombre del grupo, o haciendo doble clic con el botón izquierdo del mouse en cualquier lugar de la línea, en el que el nombre del guardia y su se muestran senior.

Si el operador registra la llegada del guardia al sitio o la cancelación de la llamada de guardia, se muestra la misma ventana, pero solo los guardias que fueron llamados al sitio se mostrarán en la lista.

Es posible cambiar la lista de guardias en el módulo "Administrador de personal". Consulte más información sobre cómo hacer esto en el capítulo dedicado a este módulo.

10.5.2 Comentario del operador

Si el operador registra una acción con el tipo "Comentario del operador", entonces el texto del comentario se puede ingresar en una ventana especial.

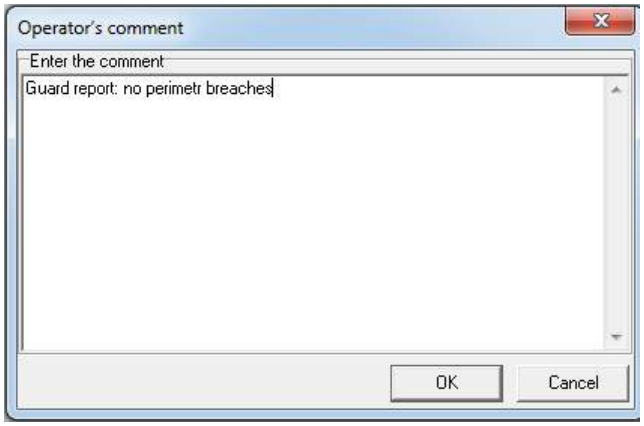


Figura 151: Ventana "Comentario del operador"

La longitud máxima del comentario del operador está limitada a cuatro mil caracteres.

Para terminar de ingresar el comentario desde el teclado, haga clic en el botón "Enter". Para ingresar una nueva línea al ingresar un comentario, presione la combinación de teclas “Control” + “Enter”.

10.5.3 Cancelación de alarma

Si se completa el manejo de la alarma y el operador debe registrarlo, deberá presionar el botón “Cancelar la alarma (F8)”. La alarma puede ser cancelada por el operador del Centro de Seguridad con el permiso correspondiente.

El operador puede seleccionar el breve resultado del manejo de la alarma o la causa de su cancelación en la ventana "Cancelación de alarma".

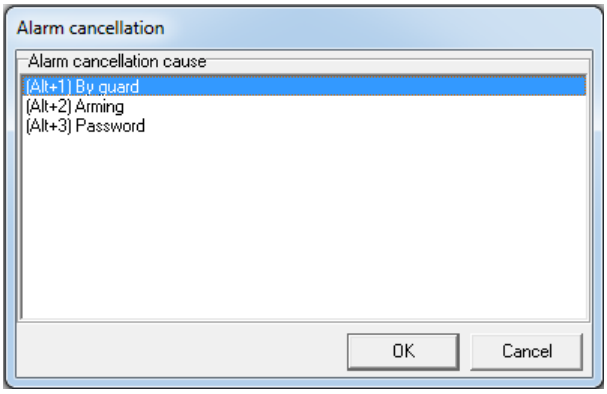


Figura 152: Ventana "Cancelación de alarma"

Las razones para la cancelación de la alarma, que se muestran en la lista, se asignan a las clases de eventos de alarma, para las cuales se registra la cancelación de la alarma.

Además, como en la lista de posibles acciones, las primeras diez razones para la cancelación de la alarma se pueden seleccionar con la ayuda de teclas numéricas o su combinación con el botón “Alt”.

Para analizar las causas de las alarmas y tomar decisiones encaminadas a optimizar el trabajo del personal de la estación de monitoreo, se recomienda mantener una lista de posibles cancelaciones de alarmas en el estado actual para cada tipo de alarma. Además, para la confiabilidad del análisis, el operador deberá registrar correctamente las razones reales para cancelar las alarmas. Una instrucción para el operador, que incluye alarmas típicas y situaciones que las conducen, esquema recomendado para el manejo de alarmas típicas y una indicación explícita del motivo de cancelación de la alarma, que el operador registrará en cada caso, es de gran utilidad para el análisis. confiabilidad, especialmente al principio.

10.6 Tarjeta de sitio

La ventana "Tarjeta del sitio" está diseñada para acceder a información sobre el sitio. Para abrirlo, haga doble clic en el ícono de un sitio que no sea alarmante, o haga clic con el botón derecho en el ícono de cualquier sitio y seleccione la “Tarjeta del sitio. . . ”En el menú, que aparece.

Además, la tarjeta del sitio también se puede abrir desde el menú que aparece cuando hace clic con el botón derecho en cualquier evento del sitio. Al hacer doble clic con el botón izquierdo del mouse en cualquier evento que no sea alarmante, se obtendrá un resultado similar.

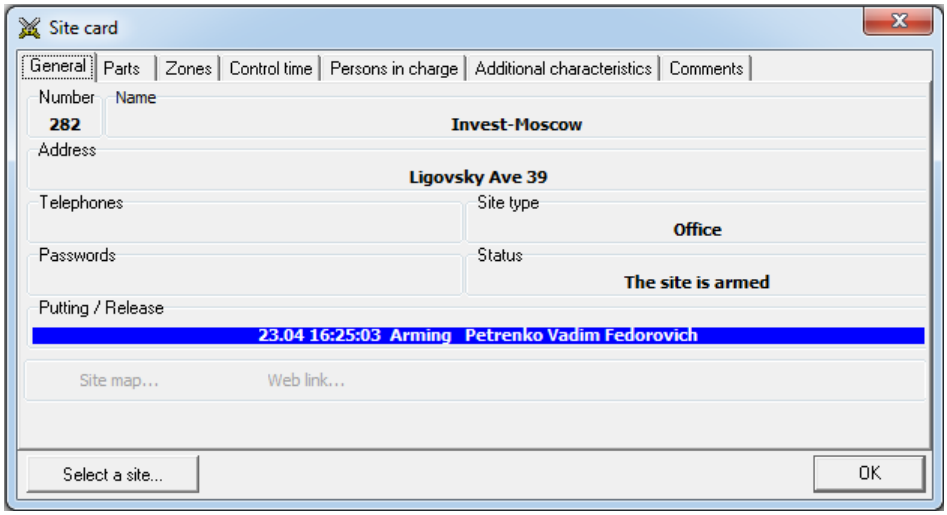


Figura 153: Ventana "Tarjeta del sitio"

Toda la información sobre el sitio que el operador de servicio pueda necesitar se muestra en las pestañas de la ventana "Tarjeta del sitio". El propósito de los campos del sitio mostrados se discute en detalle en el capítulo dedicado al módulo "Administrador del sitio".

10.7 Información sobre alarmas

La ventana "Información sobre alarmas" permite al operador ver el registro de manejo de alarmas, que fueron canceladas.

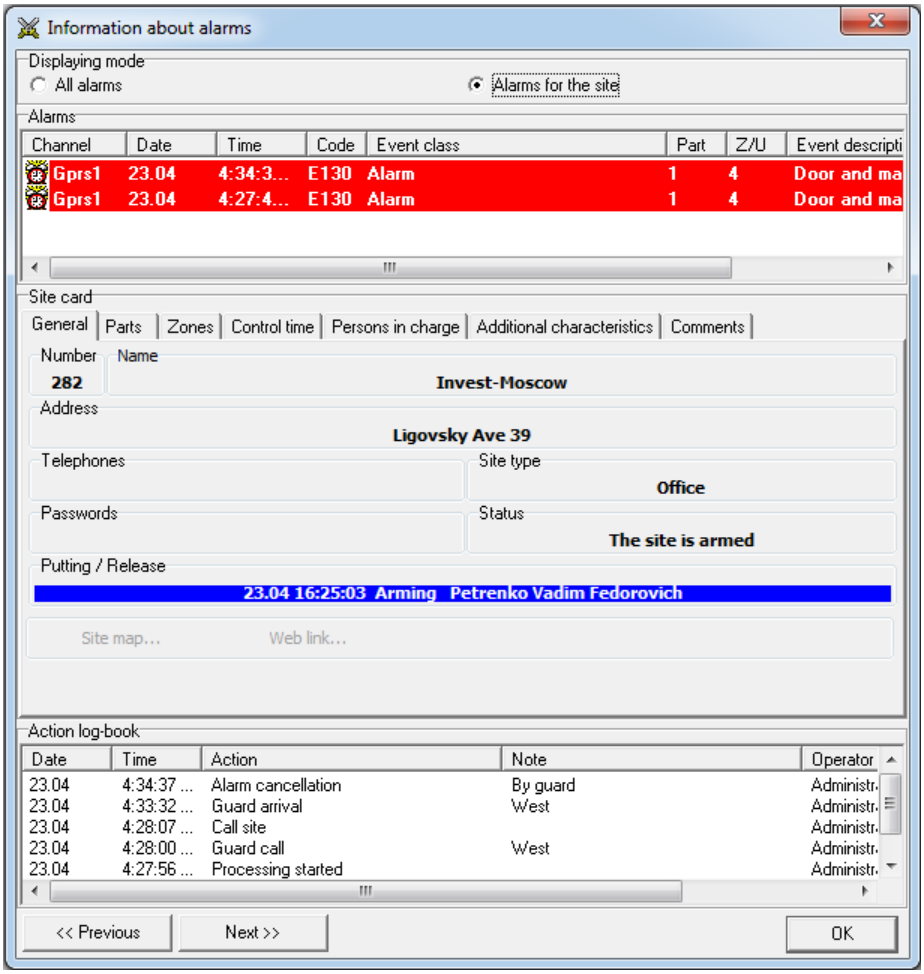


Figura 154: Ventana "Información sobre alarmas"

El cambio de modo de visualización de información al pasar a la alarma siguiente o anterior se encuentra en la parte superior de la ventana. En el modo “Todas las alarmas”, si presiona el botón “<< Anterior” o “Siguiente >>”, el programa cambiará a la alarma anterior o siguiente en orden cronológico. En el modo "Alarmas para el sitio", el programa cambiará a las alarmas para el sitio que se muestran en la ventana.

La lista de alarmas, para las cuales se muestra el registro, se encuentra debajo del interruptor de visualización de información. Consulte más información sobre la asignación de campos en la lista de alarmas anterior, en la sección de la ventana "Lista de eventos".

La tarjeta del sitio se muestra debajo de la lista, en el medio de la pantalla. El propósito de los campos del sitio mostrados se analiza en detalle en el capítulo dedicado al módulo “Administrador del sitio”.

La lista de acciones registradas por el operador durante el manejo de alarmas se muestra en la parte inferior de la pantalla. La lista se muestra en orden cronológico e incluye las acciones registradas por todos los operadores que participaron en el manejo de alarmas.

10.8 Configuración del módulo

El acceso a la configuración del módulo “Operador de servicio” está regulado por derechos que se pueden configurar en el módulo “Administrador de personal”. Además, que es posible limitar el acceso de un operador a la configuración del módulo, también es posible prohibir que el operador cierre el módulo "Operador de servicio". Estas restricciones pueden ser útiles no solo para

operadores sin experiencia, sino también para todos los operadores de servicio, ya que cerrar accidentalmente el módulo o bloquear la ventana principal del módulo con la ventana de configuración puede afectar negativamente el proceso de manejo de alarmas.

10.8.1 Común

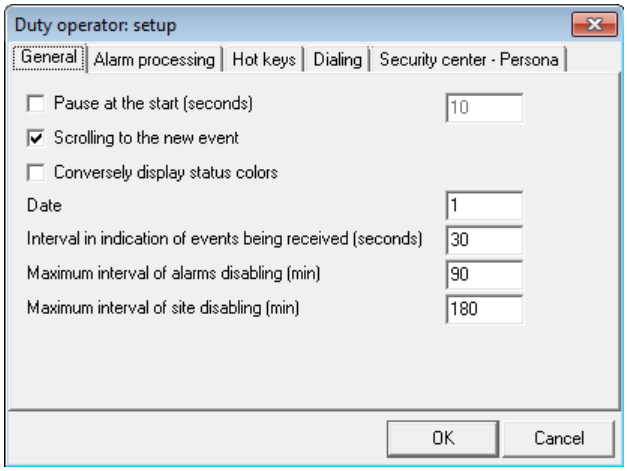


Figura 155: Ventana "Configuración", pestaña "Común"

El parámetro "Pausa al inicio" establece una pausa, durante la cual el módulo "Operador de servicio" se retrasará al inicio. El parámetro puede ser útil, si los iconos de los módulos “Event manager” y “Duty operator” se encuentran en la carpeta “Startup” o si se descargan automáticamente al inicio del sistema operativo de otra forma. Para iniciar el módulo "Operador de servicio", se necesita el módulo "Administrador de eventos" en ejecución, y puede llevar algún tiempo iniciar e inicializar completamente el módulo.

Si se establece el valor para el parámetro "Desplazarse al nuevo evento", cuando reciba nuevos eventos de los sitios, la lista de eventos en la ventana "Todos los eventos" se desplazará automáticamente para que el nuevo evento sea visible.

El parámetro “Mostrar colores de estado a la inversa” permite invertir los colores de los iconos, que representan el estado del sitio protegido. De forma predeterminada, el sitio del Centro de seguridad que está armado es azul y el sitio desarmado es verde. Si antes del trabajo con el Centro de Seguridad el operador utilizó el software de protección y monitoreo de sitios con configuraciones inversas a las propuestas, puede aplicar este parámetro. En este caso, los iconos del sitio se mostrarán en los colores invertidos a los originales: el sitio armado será verde y el sitio desarmado será azul. Para aplicar el parámetro "Mostrar colores de estado a la inversa", vuelva a cargar el módulo "Operador de servicio".

Es posible ajustar el número total de eventos que se muestran en el módulo "Operador de servicio" mediante el parámetro "Fecha". Debe recordarse que cuanto mayor sea el intervalo de eventos establecido, más tiempo se inicializará el módulo “Operador de servicio” y mayores serán los requisitos de este módulo para los recursos de la computadora.

Con el parámetro ”Intervalo de indicación de recepción de eventos” el operador puede monitorear continuamente el funcionamiento del software, lo cual es necesario para la detección oportuna de su mal funcionamiento. Este parámetro proporciona un control confiable del operador del Centro de seguridad, incluido el módulo "Operador de servicio", con la ayuda de la indicación sonora de la recepción del evento. Para que el operador tenga confianza en el funcionamiento estable del sistema, la recepción de eventos no sujeta a filtración se acompaña de una señal sonora. Si no hay eventos sin filtrar durante el intervalo de tiempo establecido por el parámetro, la señal de sonido se acompaña de la recepción del evento filtrado. Este evento se muestra en la línea del último evento recibido, pero no hay información sobre él en la lista general de eventos recibidos, ya sea en la lista de eventos de alarma o en la lista de eventos para el sitio (para mostrar el evento filtrado en la lista de eventos para el sitio habilite el modo “Mostrar duplicados”). Además, el evento filtrado recibido no se muestra en la tarjeta del sitio ni en la ventana de manejo de alarmas. Para habilitar la pantalla, configure el parámetro ”Intervalo de indicación de recepción de eventos” en un valor mayor que cero. Si este parámetro se establece en cero, la indicación de recepción de eventos se desactiva. El intervalo de visualización predeterminado es de 30 segundos. Si este parámetro se establece en cero, la indicación de recepción de eventos se desactiva. El intervalo de visualización predeterminado es de 30 segundos. Si este parámetro se establece en cero, la indicación de recepción de eventos se desactiva. El intervalo de visualización predeterminado es de 30 segundos.

El tiempo máximo de desactivación de eventos se establece en minutos mediante el parámetro “Intervalo máximo de desactivación de alarmas”. De forma predeterminada, el tiempo de desactivación del evento no debe exceder los 90 minutos.

El tiempo máximo para deshabilitar los sitios del Centro de seguridad se establece en minutos mediante el parámetro "Intervalo máximo de deshabilitación del sitio". De forma predeterminada, el tiempo de desactivación del sitio no debe exceder los 180 minutos.

10.8.2 Manejo de alarmas

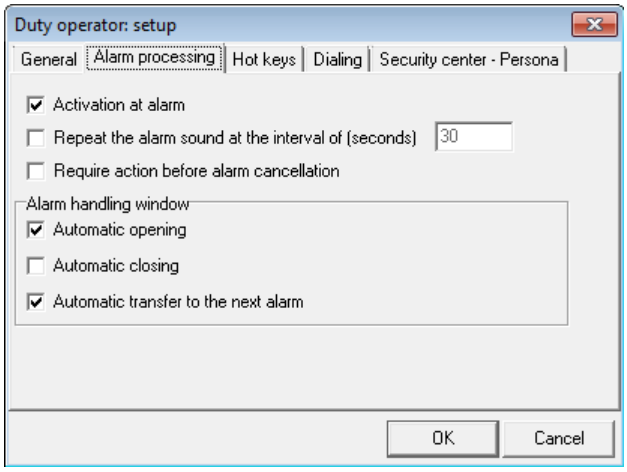


Figura 156: Ventana "Configuración", pestaña "Manejo de alarmas"

Si, al recibir un nuevo evento de alarma, es necesario que el módulo “Operador de servicio” atraiga la atención del operador, es necesario configurar el valor para el parámetro “Activación en alarma”.

En una situación en la que hay una alarma en el módulo "Operador de servicio", para la cual no se registran acciones durante demasiado tiempo, el parámetro "Repetir el sonido de la alarma en el intervalo de" puede ser útil. Si este parámetro se establece en un valor distinto de cero, entonces si no hay acciones de alarma durante el tiempo especificado, el "Operador de servicio" se comporta como si esta alarma se acabara de recibir: volverá a reproducir el sonido de la alarma y abrirá la alarma. ventana si está habilitado por el parámetro “Apertura automática” en la ventana de manejo de alarmas.

El elemento marcado "Apertura automática" de la ventana "Manejo de alarmas" permite que la ventana de alarma se abra automáticamente en caso de alarma. Los parámetros “Cierre automático” y “Transferencia automática a la siguiente alarma” determinan el comportamiento de la ventana de manejo de alarmas, en el momento en que se completa el manejo de alarmas actual. Si se establece el valor del primer parámetro, se cerrará la ventana de manejo de alarmas. Si se establece un valor para el segundo parámetro, la siguiente alarma recibida se cargará en la ventana de manejo de alarmas. Si se establecen valores para ambos parámetros, se intentará primero la siguiente alarma y, si no lo está, se cerrará la ventana de gestión de alarmas.

10.8.3 Teclas de acceso rápido

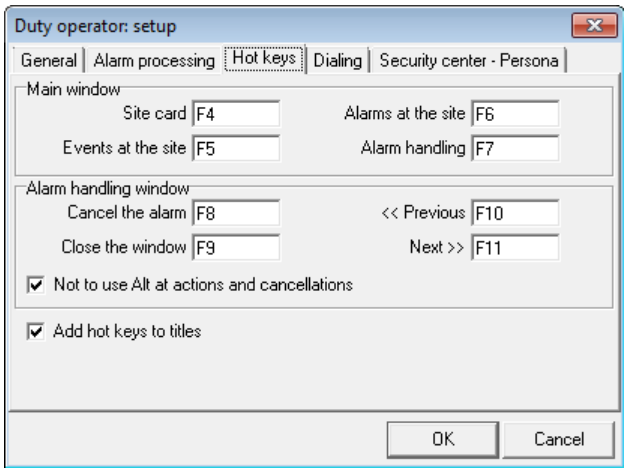


Figura 157: Ventana "Configuración", pestaña "Teclas de acceso rápido"

Utilice la pestaña "Teclas de acceso rápido" para asignar atajos de teclado para un acceso rápido a las funciones principales del módulo "Operador de servicio".

Cabe señalar que las teclas de acceso rápido para acciones y cancelaciones se asignan automáticamente, cuando se forma su lista. Pero con el parámetro “No usar Alt en acciones y cancelaciones” es posible prohibir la combinación de “Alt + Dígito” para un registro rápido de acciones o cancelaciones y usar solo dígitos.

El parámetro “Agregar teclas de acceso rápido a los títulos” permite mostrar las teclas de acceso rápido asignadas a las operaciones en los títulos de los botones.

10.8.4 Marcación

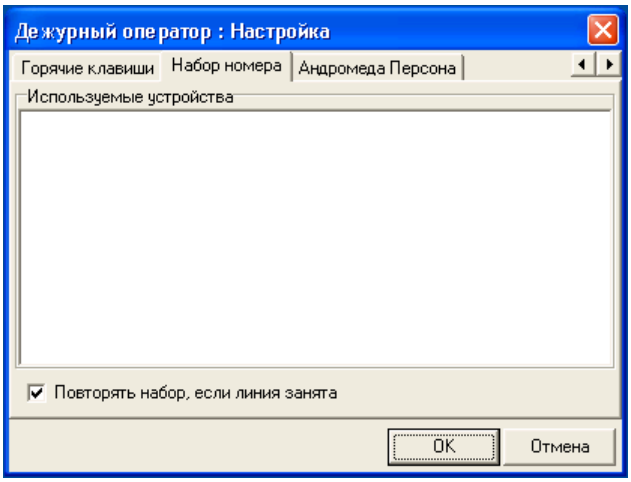


Figura 158: Ventana "Configuración", pestaña "Marcación"

Si hay un módem o cualquier dispositivo que admita la marcación a través de la interfaz TAPI conectado a la computadora, es posible especificar la lista de dispositivos que el módulo "Operador de servicio" puede usar para marcar en la pestaña "Marcación".

Para comenzar a marcar, haga clic con el botón izquierdo en cualquier número de teléfono del sitio que se muestra en la tarjeta del sitio.

Si el número marcado está ocupado, el módulo "Operador de servicio" puede volver a marcarlo si se establece el valor para "Marcación repetida, si la línea está ocupada".

10.8.5 Centro de seguridad: Persona

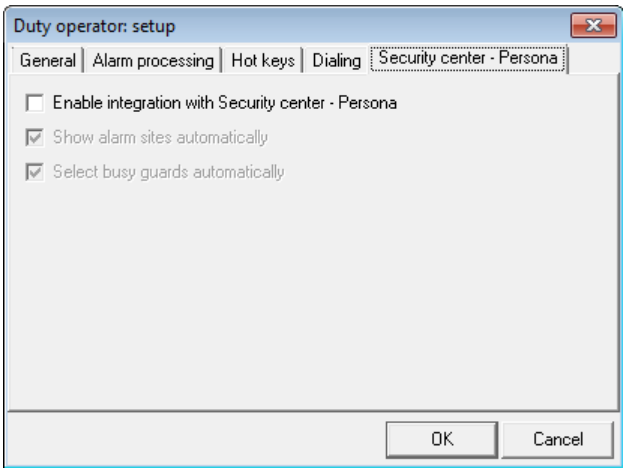


Figura 159: Ventana "Configuración", pestaña "Centro de seguridad - Persona"

El software Security Center se puede utilizar junto con el software “Andromeda Persona”. En particular, es posible descargar una lista de sitios del Centro de seguridad a la "Persona", después de lo cual se pueden colocar en el mapa del terreno.

Además, los cambios en el estado de los sitios y los guardias se pueden transferir del Centro de seguridad a "Persona" para que el "Persona" pueda mostrar automáticamente los sitios de alarma en el mapa y también mostrar el estado de los guardias que son llamados a los sitios.

En la pestaña "Andromeda Persona", es posible habilitar la integración del módulo "Duty operator" con el software "Andromeda Persona", y también permitir la visualización automática de los sitios de alarma y el estado de los guardias en la "Persona".

[id-09-03-06]: img / ShiftOp-Main-Event-06.png Ventana "Eventos", menú contextual del sitio de alarma "[id-09-04]: img / ShiftOp-Main-LastEvent.png" Línea del último evento recibido ”[id-09-10]: img / ShiftOp-Browse-01.png” Ventana “Seleccionar sitio” ”

11 Administrador de informes

El módulo "Administrador de informes" está destinado a crear informes sobre el funcionamiento de los sitios, el Centro de seguridad y el personal de la empresa de seguridad.

En el módulo “Administrador de informes” se construye un generador de formularios de informes, con el que es posible modificar los informes existentes o crear nuevos.

11.1 Informes de eventos

Al crear informes de eventos, recuerde los algoritmos de filtrado que se utilizan al registrar eventos. Ver más información sobre el filtrado de eventos en el apartado del módulo “Gestor de eventos”, aquí se debe tener en cuenta que si es necesario, es posible incluir los eventos filtrados en los informes generados.

A menos que se especifique lo contrario, todos los informes de eventos se crean teniendo en cuenta los sitios seleccionados y las clases de eventos. Debido a esto, se pueden crear informes para resolver diversas tareas, incluidas las específicas para una empresa de seguridad en particular.

Los primeros tres informes de eventos (“01 - Ordenar por hora”, “02 - Ordenar por sitios” y “03 - Agrupar por sitios”) están pensados para ver los eventos recibidos de los sitios en diferentes vistas. Cabe señalar que si se crean partes con sus propios números de sitio para un sitio, los eventos de estas partes se muestran en los informes de eventos. En este caso, el número de sitio de la pieza se indica entre paréntesis después del número de sitio.

11.1.1 Eventos de sitios no descritos

El informe "04 - De sitios no descritos" está diseñado para ver eventos que el Centro de seguridad no pudo asociar con ninguno de los sitios existentes. Al igual que el módulo "Eventos de sitios no descritos", este informe tiene como objetivo identificar errores cometidos durante la programación del equipo del sitio o al describir sitios en el Centro de seguridad. Por razones obvias, los sitios y las clases de eventos seleccionados durante su creación no importan para este informe.

11.1.2 Sitios sin eventos

El propósito del informe “05 - Lista de sitios sin eventos” es doble. Solía obtener una lista de sitios de los que no se recibían eventos dentro de un período de tiempo determinado de la manera más sencilla. Para hacer esto, seleccione todos los sitios de la lista de sitios y, en la lista de clases de eventos, seleccione todas las clases de eventos.

Otra tarea más interesante, para la que se puede utilizar el informe, es buscar, por ejemplo, todos los sitios del tipo “Banco”, de los cuales no ha habido fallas durante el último mes. Para hacer esto, seleccione todos los sitios del tipo deseado y clases de eventos que tengan el tipo "Fallo". El informe creado sobre la base de dichos parámetros contendrá solo los sitios deseados.

11.1.3 Desviación de tiempo

Utilizando el informe “06 - Por desviación de tiempo” para comprobar la correcta programación del intervalo de la prueba automática en el sitio y el correcto llenado del campo “Tiempo de control” en la tarjeta del sitio. Al crear el informe, se calcula el intervalo de tiempo promedio entre eventos del sitio, después de lo cual se compara con el tiempo objetivo del sitio.

Si la diferencia de valores es mayor que el umbral especificado en el momento de la creación del informe, dicho sitio se resaltará en la lista. Dependiendo de los algoritmos utilizados por los paneles de control para calcular el tiempo para la creación de la siguiente prueba automática, es posible excluir todos los eventos cuyo tipo de clase no sea "Prueba" al crear el informe.

11.1.4 Estadísticas por clase

El informe "07 - Estadísticas" es necesario para calcular el número de eventos de las clases dadas que se recibieron del sitio durante un período. En primer lugar, el informe es útil para identificar sitios con fallas de varios tipos. Por ejemplo, si selecciona la clase de evento "Fallo de CA" al crear el informe, puede calcular cuántas veces durante el período dado el sitio tuvo problemas de suministro de energía. Para incluir solo aquellos sitios a los que realmente necesita prestar atención en el informe, al crear un informe, es posible establecer el número mínimo de eventos para cada una de las clases especificadas que se recibirán para que el sitio se incluya en el informe.

Cabe señalar que para el uso efectivo de este informe, el usuario deberá crear clases separadas para aquellos eventos que sean de su interés.

11.1.5 SMS enviados

Los informes que pertenecen al grupo “08 - SMS enviados” - “12 - SMS, agrupación por sitios” están destinados a monitorear el funcionamiento del controlador de eventos “repetidor de mensajes SMS”. Utilice estos informes para obtener información sobre los mensajes SMS que se crearon al manejar eventos por sitios, así como la hora de entrega de estos mensajes SMS al destinatario.

11.1.6 Estadísticas por canales

Dependiendo de la configuración con la que se cree el informe “13 - Vía canales de comunicación”, se puede utilizar para resolver varias tareas. En primer lugar, es posible estimar qué canales de comunicación utiliza el sitio y en qué medida, después de calcular cuántos eventos se reciben de él en cada uno de los canales de comunicación. En segundo lugar, es posible estimar la carga de un canal de comunicación separado contando el número de eventos recibidos de todos los sitios seleccionados.

11.1.7 Estadísticas por estado

Utilice el informe "14 - Estado del sitio" para calcular el número y la duración de situaciones en las que el sitio tiene un determinado estado. Cada estado de un sitio dentro de este informe se caracteriza por dos eventos: el primer evento indica que el sitio ha pasado a un estado conocido, cuando se recibe el segundo evento, se considera que el sitio aún no se encuentra en este estado. Buenos ejemplos del estado del sitio son fallas en el canal de comunicación o de energía.

Por ejemplo, si hay una falla de energía en el sitio, se creará un evento que registre la falla y, una vez que se elimine la falla, se creará un evento sobre la restauración del suministro de energía. Si es necesario calcular cuántas veces el sitio estuvo en un estado de "falla de energía" y, además, cuál es la duración total de este estado, entonces al crear este informe, especifique las clases de eventos correspondientes a la falla y restauración de la fuente de poder.

Los estados de interés para los usuarios del Security Center pueden ser muy diferentes. Para que este informe se utilice activamente cuando se trabaja con el Centro de seguridad, es necesario crear clases separadas para aquellos eventos que registren el inicio y la finalización del estado, que sea de interés para el usuario.

11.2 Informes de alarma

Todos los eventos de alarma registrados por el Centro de seguridad requieren un manejo obligatorio por parte del operador. Si se registra un evento de alarma para el sitio en el momento en que hay otro evento no controlado en el mismo sitio, dichos eventos se combinan en un grupo y luego se manejan juntos. Las alarmas se manejan en el módulo "Operador de servicio". Al manejar una alarma, el operador registra las acciones que realizó durante el manejo de la alarma en el Centro de Seguridad. Después de la manipulación, el operador cancela la alarma registrando el tiempo de manipulación y el resultado.

Durante la creación, la mayoría de los informes de alarmas permiten especificar si se incluirán datos sobre las alarmas para las que no hubo llamadas de los guardias. Esto se debe al hecho de que muchas empresas de seguridad consideran que estas alarmas son temporales o falsas. Por tanto, en algunos informes no habrá tales alarmas, y en algunos, por el contrario, solo habrá tales alarmas.

Al crear informes de alarma, seleccione sitios y clases de eventos de alarma para incluirlos en el informe. Si, al crear un informe, es importante seleccionar solo aquellas alarmas para las que se registraron determinadas acciones, es posible especificar explícitamente las acciones de los operadores que se requieren.

11.2.1 Informe estándar e informe por operador

El informe "01 - Por operador" está diseñado para ver las alarmas que fueron manejadas por un determinado operador. Y con la ayuda del informe “02 - Estándar” es posible ver todas las alarmas y acciones registradas para ellas. Además, al crear este informe, es posible mostrar solo aquellas alarmas para las que no hubo llamadas de guardia.

11.2.2 Estadísticas por cancelaciones de alarma

Al crear el informe “03 - Por número de cancelaciones”, es posible especificar el número mínimo de cancelaciones que se registrarán durante un período. Si selecciona una cancelación específica, por ejemplo, "Fallo del equipo", y especifica que habrá al menos 5 cancelaciones de este tipo, puede obtener un informe que incluirá todos los sitios cuyas alarmas se han cancelado al menos 5 veces desde que se indicó la causa. de "Fallo del equipo".

El informe “03a - Estadísticas por cancelaciones” está destinado a calcular el número de cancelaciones seleccionadas registradas durante un período determinado. Con su ayuda, es posible ver qué causas de cancelación de alarma se registran con más frecuencia que otras y cuánto. Por ejemplo, es posible ver qué porcentaje de las alarmas canceladas son falsas. Además de contar el número total de cancelaciones para todos los sitios seleccionados, el informe permite detallar las cancelaciones del sitio para ver en qué sitios en particular hubo más falsas alarmas o alarmas en las que hubo llamadas de guardia.

Con la ayuda del informe "03b - Resumen por cancelaciones", es posible ver una opción más para detallar las cancelaciones del sitio. Es más conveniente ver el informe que el anterior, pero hay un límite: no puede incluir más de cuatro cancelaciones. Al igual que el anterior, este informe permite saber qué sitios se destacan en la lista común por las causas de las alarmas que se producen en ellos.

El informe “03c - Resumen por cancelaciones con comentario” permite seleccionar una causa para cancelar una alarma, calcular el número de alarmas, durante las cuales se indicó la causa de cancelación, y además - mostrar todos los comentarios que los operadores registraron cuando durante manejo de estas alarmas. Si el algoritmo de manejo de alarmas por parte de los operadores requiere comentarios al momento de registrar situaciones que acompañan al manejo, este informe será de gran utilidad para analizar las causas de las alarmas, así como los problemas que surgen cuando se manejan.

El último de los informes resumidos de cancelación de alarmas, “05 - Cancelaciones por día” permite seleccionar una causa para cancelar una alarma y calcular cuántas veces se utilizó esta causa en cada día durante el período seleccionado. Además, el informe permite seleccionar una característica adicional del sitio, que también se incluirá en el informe.

Supongamos que con la ayuda de informes anteriores se descubrió que hubo muchas falsas alarmas para el sitio durante un mes. Utilizando el informe “05 - Cancelaciones por día” es posible averiguar cómo se distribuyeron estas alarmas por días del mes: ocurrieron todos los días o durante turnos específicos de alguien.

11.2.3 Alarmas y eventos

El informe "04 - Con eventos" es una combinación de dos informes: informe de eventos e informe de alarma. Al crear este informe, es posible seleccionar no solo clases de eventos con el tipo "Alarma", sino también otras. En este caso, son los eventos con el tipo de clase “Alarma” y las acciones que se registraron durante su manejo, los que determinan qué sitios serán incluidos en el reporte. Los eventos con otros tipos de clases se incluirán en el informe después de que se cree el informe de alarma estándar.

Los eventos que se recibieron antes y después de una alarma pueden ser útiles para encontrar las causas de la ocurrencia de una alarma, por lo que este informe se usa con mayor frecuencia para este propósito.

11.3 Informes por tiempo de armado

El propósito de este grupo de informes es proporcionar información sobre el tiempo durante el cual el sitio estuvo armado, o especificar si el sitio estaba armado en un momento específico.

11.3.1 Hora de armado

El informe “01 - Con la cantidad de tiempo” permite ver el armado y desarmado diario del sitio durante un período, el tiempo durante el cual el sitio se armó y también el tiempo durante el cual el sitio tuvo que ser armado de acuerdo con el programa de armado.

Al mostrar el armado y desarmado del sitio, estos eventos son obligatorios filtrados: si se reciben varios armados uno por uno, solo el primero se incluirá en el informe. Si se reciben varios desarmados uno por uno, solo se incluirá en el informe el último desarmado.

El tiempo durante el cual se suponía que el sitio debía estar armado de acuerdo con el cronograma, no depende de si el monitoreo del cronograma de armado está incluido para el sitio. Por lo tanto, incluso si no se monitorea el programa de armado del sitio, aún se puede usar para comparar el período estimado y real del armado del sitio.

Con la ayuda del informe "02 - Brevemente" es posible obtener simplemente la cantidad de tiempo durante el cual el sitio estuvo armado durante un período determinado. Este informe puede ser útil en casos en los que el pago de los servicios de seguridad depende del tiempo durante el cual el sitio estuvo armado.

11.3.2 Estado de armado

A menudo, hay situaciones en las que es necesario averiguar en qué estado se encontraba el sitio en un día y una hora en particular. Para solucionar este problema, se utiliza el informe "03 - Estado de armado". Al crear un informe, seleccione la fecha, la hora y el estado de armado del sitio requerido.

11.4 Informes de los guardias

El análisis de la operación de los guardias permite evaluar la calidad de los servicios de seguridad prestados y la confiabilidad de los guardias. Además, al vincular las llamadas de los guardias a los sitios, es posible resaltar los sitios a los que se llama a los guardias con más frecuencia que al resto y sacar algunas conclusiones organizativas con respecto a estos sitios.

El informe sobre los guardias se asemeja a los informes de alarma, excepto que se centran en los aspectos específicos asociados con el trabajo de los guardias: contar la hora de llegada, la hora promedio de llegada, el número de llamadas, etc.

Para que los reportes de alarmas y los reportes de los guardias sean realmente útiles, el procedimiento de manejo de alarmas deberá estar vinculado a las acciones y causas de cancelación de las alarmas registradas por los operadores. Primero, es necesario identificar las situaciones típicas que son causantes de las alarmas. En segundo lugar, para manejar estas situaciones, es necesario crear acciones y cancelaciones de alarmas. En tercer lugar, es necesario capacitar al operador para identificar situaciones típicas, actuar de acuerdo con las reglas desarrolladas para él y registrar exactamente aquellas acciones y cancelaciones que correspondan a una determinada situación.

11.4.1 Desempeño de la guardia

El informe "01 - Rendimiento de guardia" está diseñado para mostrar todas las alarmas durante el período para el cual se registraron las llamadas de guardias seleccionados.

11.4.2 Estadísticas de respuestas

El siguiente informe, "02 - Estadísticas de respuestas", muestra las principales estadísticas relacionadas con el desempeño de los guardias sobre el un período: número total de llamadas grupales, el número de llamadas que se cancelaron, el tiempo que el guardia dedicó a las llamadas y tiempo medio de llegada de la guardia. El informe puede ser útil para estimar la carga de trabajo de un guardia, así como para identificar los guardias más y menos cargados.

11.4.3 Número medio de llamadas

Utilice el informe "03 - Número promedio de llamadas" para calcular el número total de llamadas de guardias a los sitios, así como el número promedio de llamadas de guardias al sitio por mes. Este informe se utiliza para identificar los sitios a los que se llama a los guardias con más frecuencia.

11.4.4 Tiempo de respuesta

El propósito del informe es “04 - Tiempo de respuesta” es estimar el tiempo que transcurre desde que se recibe la alarma hasta la llamada del guardia y su llegada al sitio. Al crear un informe, es posible especificar los valores máximos permitidos para estos intervalos, de modo que solo se incluyan en el informe aquellas alarmas donde se superaron estos valores.

11.4.5 Estadísticas por cancelaciones

Al igual que el informe de alarma similar, el informe “05 - Estadísticas por cancelaciones” permite calcular el número de causas registradas de cancelación de alarma durante un período, pero solo para los guardias seleccionados. Con la ayuda de este informe, es posible estimar cuántas de las alarmas a las que se llamó al guardia fueron falsas y por qué.

11.5 Informes del sitio

Un conjunto de informes de sitios está destinado a crear una copia impresa de los datos principales del Centro de seguridad: sitios, operadores, plantillas de eventos y controladores de eventos.

11.5.1 Sitios

Los informes “01 - Lista de sitios”, “02 - Tarjeta mínima”, “03 - Tarjeta corta” y “04 - Tarjeta completa” están pensados para ver e imprimir información sobre sitios en diferentes vistas y en diferentes volúmenes.

El informe “06 - Tiempo de control” permite visualizar los sitios cuyo tiempo de control se encuentra dentro de los límites definidos durante la creación del informe. El informe puede ser útil a la hora de clasificar sitios, si el tiempo de control del sitio se establece de acuerdo con su importancia.

11.5.2 Operadores

Utilice el informe “05 - Operadores” para imprimir una lista de usuarios del software Security Center y sus derechos en los módulos.

11.5.3 Plantillas de eventos

Se puede obtener una variedad de información sobre el uso de plantillas de eventos utilizando el informe "07 - Lista de plantillas de eventos". Dependiendo de los parámetros que se especificaron al crear el informe, es posible averiguar qué plantillas se utilizan para los sitios y cuáles no. Para aquellas plantillas que se utilizan, es posible contar el número de sitios que las utilizan.

Si además de la lista de plantillas de eventos es posible obtener descripciones de eventos que están incluidos en una plantilla en particular, utilice el informe "08 - Códigos de plantilla de eventos".

11.5.4 Controladores de eventos

El informe "09 - Repetidores de mensajes SMS" está destinado a visualizar e imprimir información sobre la configuración de los "repetidores de mensajes SMS" de los controladores de eventos. Se utiliza para obtener información sobre todos los controladores que se utilizan para los sitios seleccionados, o solo aquellos que tienen un número de destinatario específico.

12 Asistente de base de datos

El módulo "Asistente de base de datos" está destinado a realizar las siguientes operaciones:

- comprobación de la base de datos
- operación con copias de seguridad de la base de datos
- importación y exportación de datos

Después de iniciar el módulo "Asistente de base de datos", seleccione la operación requerida:

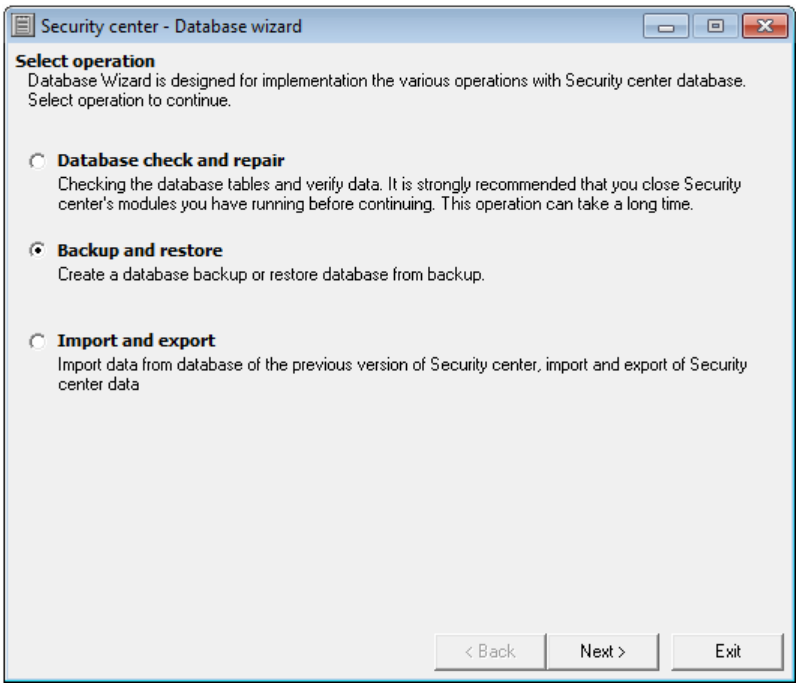


Figura 160: Ventana de inicio del módulo "Asistente de base de datos"

12.1 Verificación de la base de datos

Se recomienda realizar la operación de verificación de la base de datos al menos una vez al mes. Los procedimientos incluidos en la comprobación de la base de datos no tienen ninguna configuración y se realizan automáticamente.

Durante una verificación de la base de datos, no es necesario detener el funcionamiento de otros módulos. Una vez completada la verificación, se recomienda reiniciar el módulo "Operador de servicio".

12.2 Copia de seguridad

La copia de seguridad de la base de datos solo se puede realizar en la computadora en la que se realizó la instalación completa del Centro de seguridad.

El procedimiento de copia de seguridad no tiene un impacto crítico en el funcionamiento de otros módulos de Security Center. Sin embargo, al realizar una copia de seguridad de la base de datos, puede haber alguna degradación del rendimiento de la computadora en su conjunto. Este hecho se tendrá en cuenta a la hora de elegir el momento para realizar una copia de seguridad.

Al crear una copia de seguridad de la base de datos, establezca los valores para los parámetros que controlan la operación de copia de seguridad.

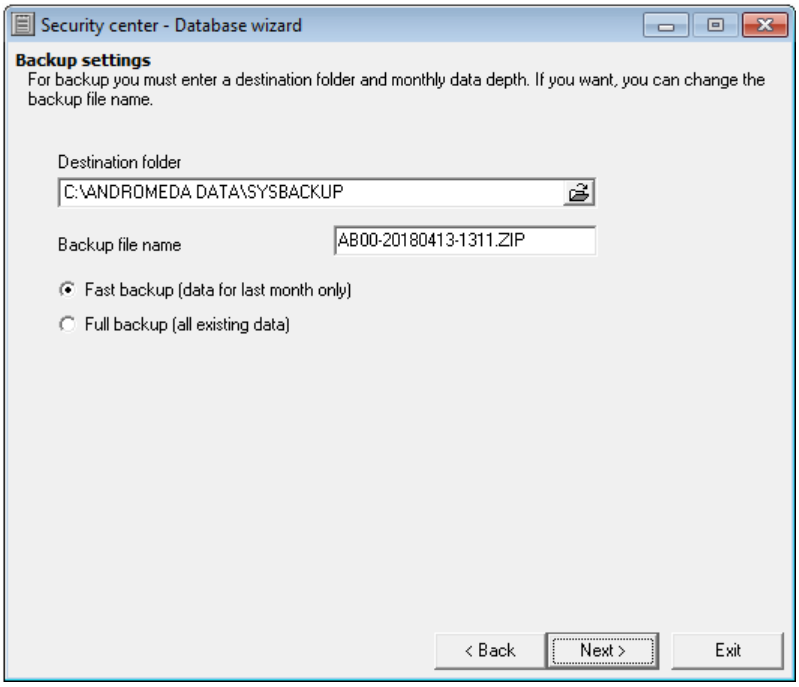


Figura 161: Ventana de configuración de la copia de seguridad

La opción Carpeta de destino especifica la carpeta en el disco duro de la computadora o recurso de red en la que se guardará la copia de seguridad de la base de datos.

El nombre del archivo de copia de seguridad se puede especificar mediante el parámetro del mismo nombre. A pesar de que no existen restricciones para nombrar el archivo de respaldo, es necesario recordar que para restaurar la base de datos del Security Center desde el respaldo usando la GUI del módulo "Asistente de base de datos", el nombre del archivo debe comenzar con los caracteres latinos " AB ".

Tenga en cuenta que la copia de seguridad de la base de datos del software Security Center se crea en forma de archivo ZIP, en el que se pueden incluir varios archivos que contienen datos de copia de seguridad. Si el tamaño del archivo de almacenamiento supera los 4 Gb, se creará un archivo de varios volúmenes, todos los archivos del cual serán necesarios para restaurar la base de datos desde la copia de seguridad.

Además del nombre del archivo de copia de seguridad y el nombre de la carpeta para su ubicación, especifique el tipo de copia de seguridad que desea crear. El tipo de copia de seguridad determina la cantidad de información que se incluirá en la copia de seguridad.

En caso de *copia de seguridad completa,* Toda la información almacenada en la base de datos en el momento de la copia, incluidos los eventos recibidos, las acciones del operador y los mensajes SMS enviados durante todo el período de funcionamiento del Centro de seguridad, se incluirán en la copia de seguridad de la base de datos.

En caso de *copia de seguridad rápida,* la cantidad de datos en la copia de seguridad será signi fi cativamente menor: guardará eventos, acciones del operador y mensajes SMS sólo durante el último mes.

Según la cantidad de información almacenada durante la copia de seguridad, se recomienda realizar una copia de seguridad completa al menos una vez al mes y copias de seguridad rápidas, al menos una vez al día.

Para almacenar copias de seguridad, se recomienda utilizar no uno, sino varios medios, y aquellos que no están conectados físicamente con el subsistema de disco de la computadora en la que está almacenada la base de datos de Security Center. Por ejemplo, puede ser un disco duro, una unidad flash o un recurso de red independientes.

Para aumentar la confiabilidad del sistema en su conjunto, Security Center realiza una copia de seguridad automática. Las copias rápidas de la base de datos se almacenan en el archivo “ANDROMEDA DATA |SYSBACKUP ”, el intervalo para crear copias de seguridad automáticas es de 24 horas por defecto.

12.3 Restaurar desde la copia de seguridad

La restauración de la base de datos a partir de una copia de seguridad solo se puede realizar en la computadora en la que se realizó la instalación completa del software Security Center.

Antes de restaurar la base de datos desde una copia de seguridad, detenga todos los módulos del Centro de seguridad, incluido el módulo "Administrador de eventos".

No importa la versión de la base de datos desde la que se realiza la restauración: inmediatamente después de la restauración, el módulo “Asistente de base de datos” comprobará la versión de los datos recuperados y, si es necesario, realizará la actualización.

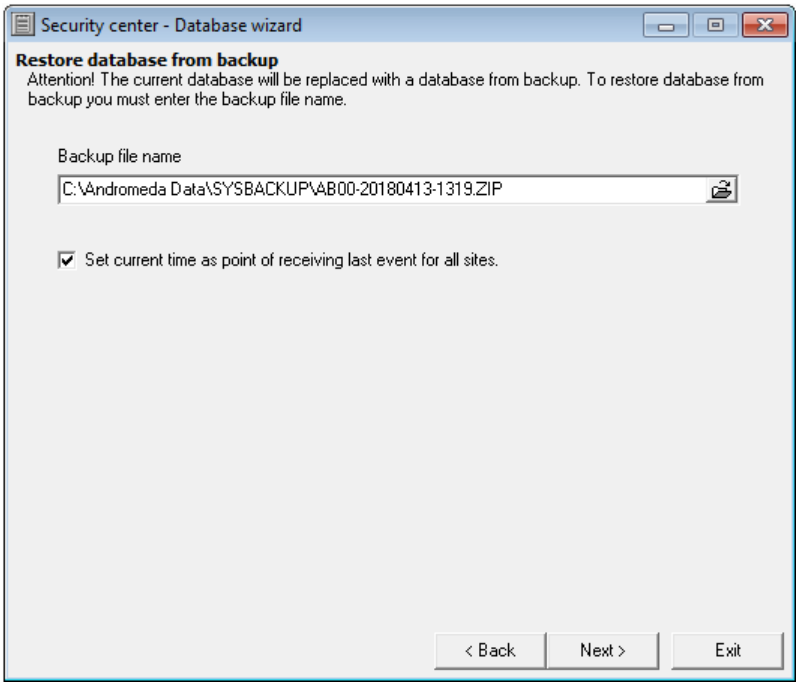


Figura 162: Ventana de configuración para restaurar desde una copia de seguridad

El nombre del archivo de respaldo desde el cual es necesario restaurar la base de datos se puede especificar usando el mismo parámetro. Si se creó una copia de seguridad de la base de datos en un archivo de varios volúmenes, entonces se requieren todos los archivos de almacenamiento cuando se recupera de dicha copia.

El parámetro "Establecer la hora actual como punto de recepción del último evento para todos los sitios" tiene como objetivo evitar la generación de eventos sobre la ausencia de un evento de control inmediatamente después de que la base de datos se restaure desde la copia de seguridad. Si esta bandera se establece al restaurar una base de datos desde una copia de seguridad, entonces para todos los sitios en la base de datos del software Security Center, el tiempo de referencia comienza a contar desde el momento en que la base de datos se restaura desde la copia de seguridad.

Ver más información sobre el parámetro “Tiempo de control del sitio” en el capítulo que describe el módulo “Administrador del sitio”, sección “Tiempo de control”.

Se recomienda restaurar la base de datos en dos pasos: primero, restaurar desde la copia completa más reciente de la base de datos y luego desde la copia rápida actual. Así, en la primera etapa, se restaurará todo el historial existente, y en la segunda etapa, se actualizará la información en constante cambio.

Cuando se completa la restauración de la base de datos desde una copia de seguridad, se recomienda realizar una verificación de la base de datos. Se debe recordar que la verificación de la base de datos no bloquea el funcionamiento de otros módulos del Security Center, por lo que se puede realizar después de que se inicien el “Administrador de eventos” y el “Operador de servicio”.

12.4 Importación de datos

Es posible importar datos solo en la computadora en la que se realizó la instalación completa del software Security Center.

Antes de iniciar la importación de datos, detenga todos los módulos del Centro de seguridad, incluido el módulo "Administrador de eventos".

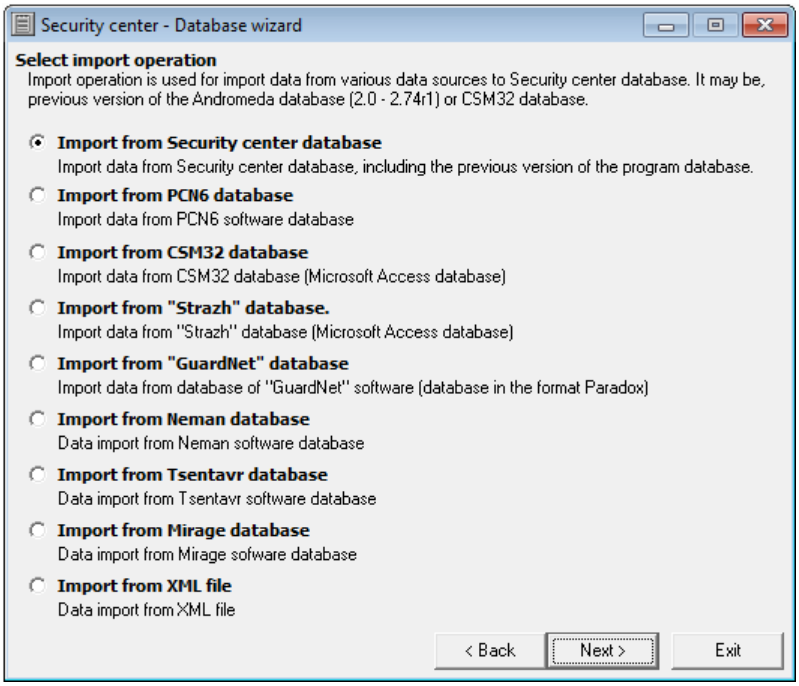


Figura 163: Ventana para seleccionar la fuente de datos para la operación de importación

En el Centro de seguridad, además de otras fuentes, es posible importar desde un archivo XML.

12.4.1 Importar desde archivo XML

Importando desde un archivo XML, es posible importar una base de datos del sitio del software Cobra al Security Center.

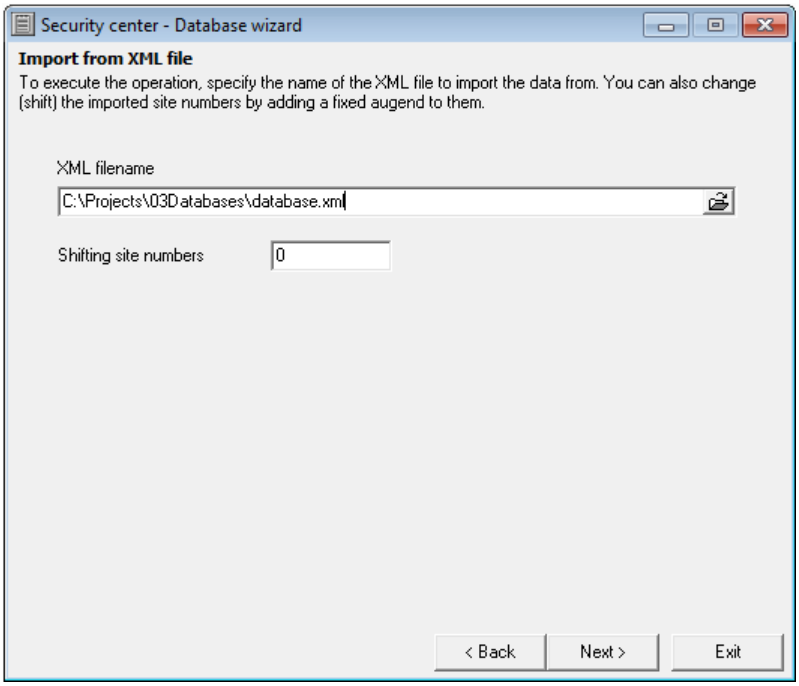


Figura 164: Ventana para configurar la importación desde un archivo XML

Utilice el parámetro "XML filename" para seleccionar el archivo de la base de datos especificando la ruta.

Al importar desde un archivo XML, es posible mover los números de los sitios importados. El cambio se realiza porque el sumatorio, especificado durante la configuración de la importación, se agrega a los números de sitio, información sobre la cual se transfiere al Centro de seguridad. Por ejemplo, si el valor del parámetro "Cambiar números de sitio" se establece en 10000, y los números de sitio en el archivo XML están dentro del rango de 1 a 2000, entonces en la base de datos del Centro de seguridad, estos sitios tendrán números dentro del rango de 10001 a 12000.

Consulte más información sobre la función de cambiar los números de sitio en las fuentes de eventos en el capítulo sobre el módulo "Administrador de eventos" en la sección "Fuentes de eventos".

12.5 Exportación de datos

El Centro de seguridad admite la exportación de información sobre sitios a un archivo de texto con un separador de valores.

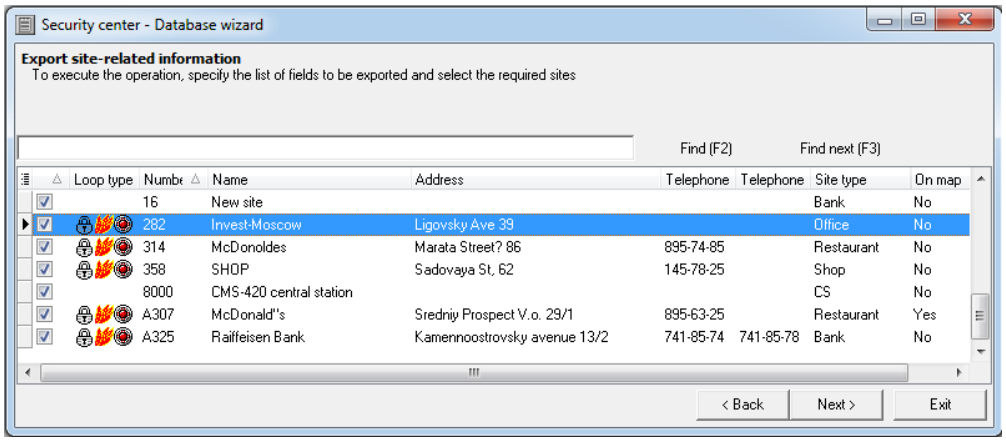


Figura 165: Ventana para seleccionar sitios y campos al configurar la exportación de información del sitio

Para exportar, seleccione sitios y campos (columnas) cuya información se escribirá en el archivo de exportación. Seleccione los sitios cuya información se exportará marcando las casillas de la primera columna de la línea cerca del sitio. Seleccione

campos, información desde la cual se escribirá en el archivo de exportación, habilitando o deshabilitando su visualización. El archivo de exportación incluirá información solo de los campos (columnas) que se muestran en la tabla.

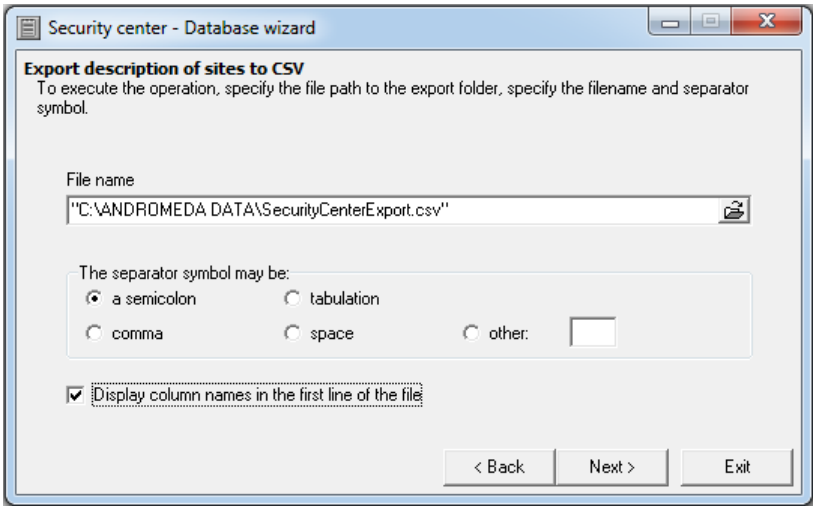


Figura 166: Ventana para configurar la exportación de información sobre sitios

Utilice el parámetro "Nombre de archivo" para especificar la carpeta y el nombre del archivo de exportación.

Utilice el parámetro "Símbolo de separador" para seleccionar el carácter que se utilizará como separador de campo en una línea del archivo de exportación. Debe recordarse que los valores del campo de línea en el archivo de exportación están entre comillas dobles, lo que excluye la posibilidad de un reconocimiento incorrecto del separador al abrir el archivo de exportación.

12.6 Opciones de la línea de comandos

Junto con la interfaz gráfica de usuario, el módulo "Asistente de base de datos" se puede utilizar para el control con la línea de comandos.

Esta función puede ser útil si el Programador de Windows, que tiene capacidades más avanzadas que el programador integrado en el módulo "Administrador de eventos", se utiliza como programador de tareas para realizar copias de seguridad de una base de datos o restaurar desde una copia de seguridad.

12.6.1 Copia de seguridad de la base de datos

AnDBWiz.exe
/ BACKUPDB
/ FOLDER: <Carpeta de destino 1>; <Carpeta de destino 2> / TIPO: <Tipo de copia de seguridad>
/ BACKUPCOUNT: <Número de archivos en la carpeta de destino>

/ BACKUPDB

Este parámetro especifica que el módulo "Asistente de base de datos" realizará una copia de seguridad de la base de datos. La configuración del procedimiento de copia de seguridad se establece mediante los parámetros de la línea de comandos que le siguen.

/ FOLDER: <Carpeta de destino 1>; <Carpeta de destino 2>

Una o varias carpetas en las que se guardará la copia de seguridad de la base de datos. Deberá especificarse al menos una carpeta. Los nombres de las carpetas se incluirán entre comillas. Si se especifican carpetas de sección, deben estar separadas por un punto y coma. Está permitido utilizar rutas absolutas en los nombres de las carpetas.

/ TIPO: <Tipo de copia de seguridad>

El tipo de copia de seguridad que se creará. Si este parámetro se establece en "0", indica una copia de seguridad rápida. Si este parámetro se establece en "1", indica una copia de seguridad completa. El parámetro es opcional. Si no se establece el valor del parámetro, se creará una copia de seguridad rápida.

/ BACKUPCOUNT: <Número de archivos en la carpeta de destino>

Este parámetro especifica el número máximo de archivos de respaldo de la base de datos en la carpeta de destino. Si encuentra que el número de archivos de copia de seguridad del mismo tipo excede el número máximo posible al crear una copia de seguridad, se eliminará el archivo de copia de seguridad más antiguo. El parámetro es opcional. Si no se especifica el valor del parámetro, el valor de este parámetro será 10.

12.6.2 Restauración de la base de datos desde la copia de seguridad

AnDBWiz.exe
/ RESTAURADOB
/ FOLDER: <Carpeta de origen> / TYPE:
<Tipo de copia de seguridad>

/ RESTAURADOB

Este parámetro especifica que el módulo "Asistente de base de datos" restaurará la base de datos a partir de una copia de seguridad. La configuración de restauración de la base de datos se establece mediante los parámetros de la línea de comandos que le siguen.

/ FOLDER: <carpeta de origen>

La carpeta en la que se restaurará la copia de seguridad de la base de datos. Si se encuentran varios archivos de copia de seguridad del tipo especificado en la carpeta especificada, se realizará la restauración desde la creación del archivo más reciente.

/ TIPO: <Tipo de copia de seguridad>

El tipo de copia de seguridad a partir del cual se restaurará la base de datos. Si este parámetro se establece en "0", indica una restauración rápida de la copia de seguridad. Si este parámetro se establece en "1", indica la restauración de la copia de seguridad completa. El parámetro es opcional. Si no se establece el valor del parámetro, se realizará la restauración desde la copia de seguridad rápida.

12.6.3 Ejemplo de uso de parámetros de la línea de comandos

AnDBWiz.exe
/ BACKUPDB
/ FOLDER: "E: \ Backup Data \ Operational"; "\\ Storage \ Andromeda Backup \ Operational" /
BACKUPCOUNT: 25

El conjunto de parámetros de la línea de comandos mencionado anteriormente significa que el módulo "Asistente de base de datos" creará una copia rápida de la base de datos y la copiará en las carpetas. MI: |Los datos de copia de seguridad |Operacional y ||Almacenamiento |Andrómeda Respaldo |Operacional.

Al copiar una copia de seguridad en la carpeta de destino, el módulo “Asistente de base de datos” debe verificar que el número total de archivos de copia de seguridad en línea en la carpeta de destino no exceda de 24, y si hay más, se eliminará el archivo de copia de seguridad más antiguo.

13 Servicios en la nube

La nube es un complejo de software y hardware de infraestructura. Brinda servicios para mejorar la calidad de los servicios que ofrece la empresa de seguridad privada.

La “Interfaz del ingeniero” muestra un sitio disponible para el control y brinda la capacidad de controlar remotamente el equipo en él.

El usuario del Security Center puede seleccionar uno de los modos de operación con los servicios en la nube, en función del grado de integración con la nube. La integración completa permite utilizar todos los servicios en la nube. Parcial significa solo un servicio que proporciona acceso remoto a equipos en un sitio. Al prohibir la transferencia de cualquier dato a la nube, el usuario se niega a utilizar todos los servicios en la nube.

13.1 Panel de ingeniería

La aplicación “Panel de ingeniería” está destinada a la configuración remota de los equipos instalados en el sitio, así como a la actualización de la versión de software de los dispositivos.

Para que el ingeniero pueda cambiar la configuración de forma remota, se debe instalar uno de los siguientes dispositivos en el sitio:

- Nord GSM o Nord GSM WRL
- Nord GSM Mini o Nord GSM Air
- Soyuz GSM
- TR-100 GSM IV

Para que un ingeniero pueda acceder al servicio, se le debe crear una cuenta.

Es posible crear una cuenta de ingeniero en la pestaña "Ingenieros" del módulo "Administrador de personal". Al crear una cuenta, se envía un correo electrónico a la dirección de correo electrónico del ingeniero. El ingeniero debe hacer clic en el enlace de la carta y crear y con fi rmar la contraseña para acceder al “Panel de ingeniería” en la página que se abre. Luego de ingresar los datos, es necesario hacer clic en el botón “Registrarse” para completar el registro en la Nube.

Para que el operador del Centro de seguridad cree una cuenta para el ingeniero o cambie su configuración, se le dará permiso para editar los ingenieros.

Después del registro exitoso, se mostrará un enlace en la página a la página principal del “Panel de ingeniería”. En esta página, los enlaces a las interfaces de programación remota de los sitios se proporcionarán en "Sitios disponibles", cuyo acceso está permitido al ingeniero. Cada enlace especifica el número de sitio y el tiempo de acceso permitido al sitio (por ejemplo, “Sitio No. 314, el acceso al sitio está permitido desde las 15:55 25.08.2013 hasta las 16:55 25.08.2013”).

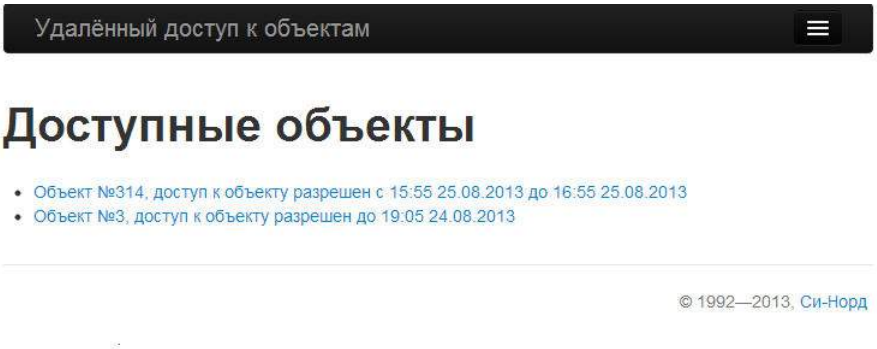


Figura 167: Panel de ingeniería

El usuario del Security Center, que tiene el permiso correspondiente, puede otorgar al ingeniero acceso a los sitios usando la pestaña "Mantenimiento" del módulo "Administrador del sitio".

El ingeniero puede ir a cualquiera de los enlaces especificados en la interfaz web solo en el momento en que se le permita acceder al sitio. Al mismo tiempo, ingresa a la página “Teclado remoto”. La página contiene la interfaz de

el teclado web, que es idéntico al instalado en el sitio. Así, la interfaz de programación remota implementa el comportamiento del teclado real conectado al dispositivo. La información sobre cómo se duplican los botones en el teclado se muestra en la interfaz web a la derecha del teclado.

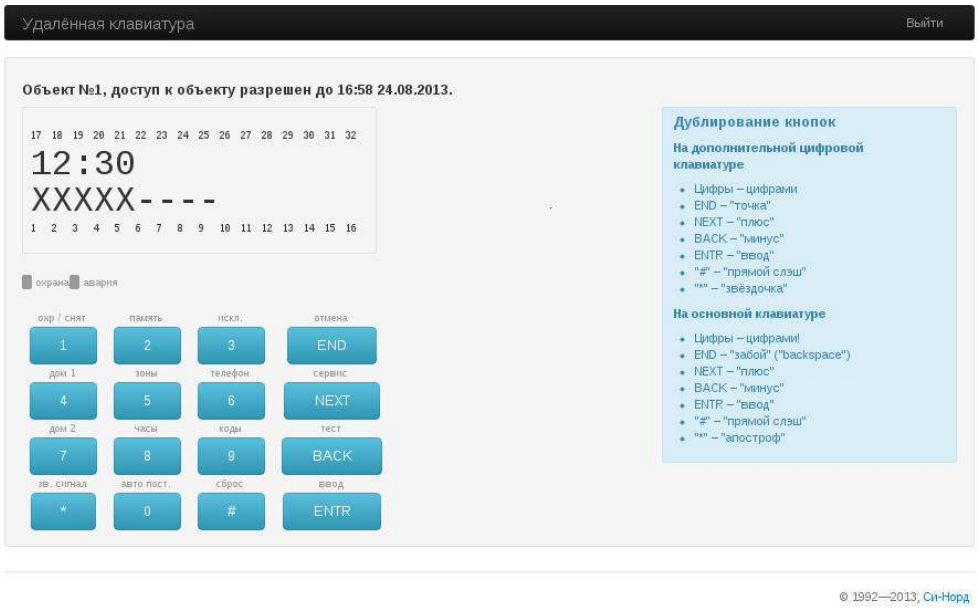


Figura 168: Teclado web

Cabe señalar que si se produce un error al trabajar con el teclado web, se muestra el texto del error y la interfaz va a la página principal con una lista de sitios. Por ejemplo, si el teclado web no se utiliza durante más de cinco minutos, se completa la sesión de comunicación con el sitio. Al mismo tiempo, se muestra el siguiente mensaje: “El período de espera para las acciones para configurar el dispositivo ha expirado. Para garantizar la seguridad, se completa la sesión de comunicación con el sitio No. 314 ”.

Si la conexión al sitio se pierde por cualquier motivo, el teclado del sitio se desactiva. En este caso, el texto del error es el siguiente: “El período de espera para la respuesta del dispositivo ha expirado. Para garantizar la seguridad, se completa la sesión de comunicación con el sitio No. 314 ”.

Si cuando se abre o usa el teclado web resulta que el sitio está armado, se muestra el siguiente mensaje: “El sitio No. 314 está armado actualmente. Para acceder al teclado web, desarme el sitio ”.

Una vez finalizado el trabajo, el ingeniero deberá salir del sistema haciendo clic en el enlace "Salir" ubicado en el panel principal de la página.

Para iniciar sesión en la interfaz web, vaya a keyboard.cnord.net e ingrese la dirección de correo electrónico y la contraseña que creó al registrarse. Después de eso, haga clic en el botón "Iniciar sesión". Para recuperar una contraseña, haga clic en el enlace "¿Olvidó su contraseña?". En la ventana que aparece es necesario ingresar la dirección de correo electrónico y presionar el botón “Restaurar contraseña”. Al mismo tiempo, se enviará una carta a la dirección especificada con un enlace para la restauración de la contraseña.

14 Soporte técnico

Si surgen problemas durante el funcionamiento del software Security Center, o si desea mejorarlo, comuníquese con el servicio de soporte técnico de Cygnus Electronics por correo electrónico a: soporte@cygnus.la

Cuando se comunique con el soporte técnico sobre un problema, especifique la versión de Security Center que se está instalando y describa el problema

En caso de solicitud por correo electrónico, se recomienda adjuntar el archivo que contiene los siguientes archivos:

- archivo C: Andromeda_Install.log - Este archivo contiene el registro del instalador de Security Center
- archivos de la carpeta C:|Registro de Andrómeda - Los archivos contienen los registros de los módulos del Centro de seguridad.
- archivos de la carpeta C:|Archivos de programa |Microsoft SQL Server |90 |Configurar Bootstrap |INICIAR SESIÓN - Los archivos de este carpeta y sus subcarpetas contienen los registros del instalador de instalación de Microsoft SQL Server

Los archivos enumerados no contienen datos personales ni información confidencial.


CYGNUS
electronics