

ICONO 93

SISTEMA DE CONTROL DE ACCESO

REDES Y PROYECTOS DE ENERGIA SAS EMA

ABRIL 2018

TABLA DE CONTENIDO

Contenido

1. GENERALIDADES DEL SISTEMA....4
   1.1 DESCRIPCIÓN GENERAL DE CONTROL DE ACCESO. 4
2. ARQUITECTURA DEL SISTEMA 4
3. LISTADO DE EQUIPOS....6
   3.1 DESCRIPCIÓN GENERAL DE LOS EQUIPOS. 6
      3.1.1 CONTROLADOR PRINCIPAL. 7
      3.1.2 EXPANSORES. 7
      3.1.3 FUENTE DE ALIMENTACIÓN....8
      3.1.4 LECTORAS DE PROXIMIDAD.....9
      3.1.5 PASILLOS MOTORIZADOS. 9
4. OPERACIÓN DEL SECURITY EXPERT. 10
   4.1 DESCRIPCIÓN DE LA INTERFAZ. 11
      4.1.1 GLOBAL....11
      4.1.2 SITES. 12
      4.1.3 USERS. 13
      4.1.4 EVENTS. 13
      4.1.5 REPORTS. 14
      4.1.6 MONITORING. 15
      4.1.7 ABOUT. 16
   4.2 CREACIÓN DE USUARIOS Y ASIGNACIÓN DE TARJETAS. 16
      4.2.1 CREACIÓN DE USUARIOS DESDE LA OPCIÓN USERS. 17
      4.2.2 IMPORTAR USUARIOS....19
   4.3 EVENTOS Y REPORTES. 22
      4.3.1 REPORTES. 23
      4.3.2 EVENTOS....24
5. MANUAL DE MANTENIMIENTO PREVENTIVO. 25
6. REGISTRO FOTOGRÁFICO. 26

7. MANUAL DE SOLUCIÓN DE PROBLEMAS FRECUENTES. 30

1. GENERALIDADES DEL SISTEMA

1.1 DESCRIPCIÓN GENERAL DE CONTROL DE ACCESO.

El sistema de Control de acceso implementado en el proyecto ICONO 93 es en su totalidad de marca SCHNEIDER con su solución Security Expert, es un sistema que combina software y hardware innovador con la última tecnología IP para ayudar a enfrentar los desafíos de seguridad del edificio. La tecnología de Security Expert proporciona visualización y control de todo el edificio y asegura que los sistemas de seguridad funcionen de manera precisa y sin interrupciones. La información está disponible; el riesgo se reduce y la eficiencia se maximiza. La solución integrada de Security Expert une aplicaciones dispares de una infraestructura de seguridad para ofrecer una única plataforma inteligente, una que garantice una seguridad óptima con información accionable en tiempo real que crea el entorno empresarial más seguro posible.

El cableado se encuentra totalmente canalizado desde los respectivos gabinetes hasta el dispositivo final por medio de tubería conduit EMT de diferentes calibres, respetando el porcentaje de llenado de tubería que establece el RETIE para los cables utilizados.

2. ARQUITECTURA DEL SISTEMA

El sistema está controlando un total de 24 puertas y 4 molinetes en todo el edificio. El edificio cuenta con tres centros de concentración de cableado de las los elementos periféricos (Contactos magnéticos, botones de salida y lectoras de tarjetas). El tablero principal está ubicado en el cuarto de control del sótano 1, el segundo se encuentra en el cuarto eléctrico del piso 4 y el tercero en el cuarto eléctrico del piso 7.que está ubicado en el cuarto eléctrico del piso 4. Los controladores principales están distribuidos en estos gabinetes y se conectan por medio de una red LAN dedicada para los sistemas de seguridad y automatización; a su vez, los controladores principales se comunican con los expansores por medio de un enlace RS485.

Tanto los controladores como los expansores cuentan con capacidad para manipular dos puertas, teniendo en cuenta que virtualmente un molinete cuenta como un espacio de dos puertas (una a la que se asocia la entrada y una a la que se asocia la salida) cada dispositivo podrá manipular un solo molinete.

A continuación se podrán ver los siguientes diagramas:

- **Arquitectura del sistema de Control de acceso:** Diagrama de conexión y componentes del sistema con sus respectivas ubicaciones y la topología correspodiente.
- **Distribución del sistema de Control de acceso:** Distribución lógica del sistema especificando los equipos principales como controladores y expansores que hacen parte del sistema y sus respectivas direcciones IP, direcciones MAC, seriales y puertas asociadas.

DISTRIBUCIÓN DEL SISTEMA CONTROL DE ACCESO CORTEZZA 93

Nº CONTRATO: FECHA: 7/22/2018		DIRECTOR: ING. CARLOS ANDRES VARGAS RESIDENTE: ING. NESTOR CORTES		CLIENTE / SUCURSAL: CORTEZZA 93 PC DE INSTALACIÓN: SERVIDOR						
ITEM	NOMBRE	REFERENCIA	MARCA	UBICACIÓN	CONFIGURADO / PROBADO	NÚMERO DE SERIE	DIRECCIÓN MAC	DIRECCIÓN IP	PUERTA 1 (READER 1)	PUERTA 2 (READER 2)
1	CONTROLADOR 1	SP-C 1	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	C2B7DA6A	00:1B:C2:B7:DA:6A	10.40.65.15	MOLINETE 4 - SALIDA	MOLINETE 4 - ENTRADA
2	EXPANSOR 1	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	0700E6D5	NA	NA	MOLINETE 2 - SALIDA	MOLINETE 2 - ENTRADA
3	EXPANSOR 2	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	B881CE5F	NA	NA	MOLINETE 1 - SALIDA	MOLINETE 1 - ENTRADA
4	EXPANSOR 3	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	E7FC39A8	NA	NA	BANDEROLA - SALIDA	BANDEROLA - ENTRADA
5	EXPANSOR 4	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	BD99D654	NA	NA	CUARTO BAJA TENSIÓN	CUARTO DE CONTROL
6	CONTROLADOR 2	SP-C 2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	C294B630	00:1B:C2:94:B6:30	10.40.65.16	MOLINETE 3 - SALIDA	MOLINETE 3 - ENTRADA
7	EXPANSOR 5	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	49DE2CC3	NA	NA	HVAC - SÓTANO 1	SUBESTACIÓN
8	EXPANSOR 6	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	6050EF19	NA	NA	HVAC - SÓTANO 2	PLANTA ELÉCTRICA
9	EXPANSOR 7	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	0A8193C4	NA	NA	AGUA POTABLE	CUARTO RCI
10	EXPANSOR 8	RDM2	SCHNEIDER	SÓTANO 1 - CUARTO DE CONTROL	OK	20BBCA77	NA	NA	MOLINETE 4 - CAPTURADOR	HVAC - SÓTANO 3

Imagen No 1. Ejemplo de tabla de distribución del sistema.

3. LISTADO DE EQUIPOS

En la tabla No 1 se encuentras relacionados todos los equipos utilizados para el sistema de Control de acceso y su respectiva referencia y la cantidad utilizada en el proyecto.

DESCRIPCIÓN	MARCA	REFERENCIA	CANTIDAD
Fuente de alimentación inteligente 12V – 4A	SCHNEIDER	SP-PSU-4A	1
Controlador principal Security Expert	SCHNEIDER	SP-C	4
Expansor 2 puertas con RS485	SCHNEIDER	SP-RDM2	14
Lectora de proximidad 26Bits	APTIQ	APTIQ-SM10	33
Brazo hidráulico No 4	ZEBRA	RH4	7
Brazo hidráulico para puerta 120K	YALE	3005	10
Torniquete bidireccional	GUNNEBO	SLIMSTEELV	4
Capturador de tarjetas	GUNNEBO	CPT-GR	1
Banderola motorizada	GUNNEBO	ECO	1
Electroimán 600lbs	SAC	EI-600-LBS-SAC	24
Pulsador de pánico alambrado	SECOLARM	SS-077Q	2
Botón de salida	SECOLARM	SD-7201RCPE1Q	24
Fuentes 12V 5A	SECOLARM	ST-2606-5AQ	3
Transformador 24-28VAC/100VA	SECOLARM	ST-UVDA-W100Q	3
Batería 12VDC – 7A	KEYKO	BAT127	3
Servidor PowerEdge	DELL	R540	1
Contacto magnético liviano	SECOLARM	SM200Q/W	24
Licencia de visitantes	EASYLOBBY	EL-96000-SVM10	1
Licencia de integración	EASYLOBBY	EL-ACI-TACC	1
Tarjeta estándar de proximidad	APTIQ	9558-SCHALAGE	1000
Cámara para estaciones de trabajo	QUICKCAM	C920	2
Computador para control de visitantes	LENOVO	P310	2
Monitor 32”	SAMSUNG		4

Tabla No 1. Listado de equipos del sistema de control de acceso.

3.1 DESCRIPCIÓN GENERAL DE LOS EQUIPOS.

Cada uno de los equipos tiene una función específica dentro del sistema Security Expert de SCHNEIDER, a continuación se realizará una breve descripción de cada uno de los elementos principales con el fin de hacer una introducción al sistema y que el usuario se familiarice con los términos y funcionalidades de cada uno de ellos dentro del conjunto, previo a la explicación de la operación de la plataforma.

3.1.1 CONTROLADOR PRINCIPAL.



Imagen No 2. Controlador principal SP-C.

El controlador principal de Security Expert es la unidad de procesamiento central del sistema. Se comunica con todos los módulos del sistema, almacena toda la información de configuración y transacción, procesa todas las comunicaciones e informa alarmas y actividad del sistema a una estación de monitoreo o computadora remota.

3.1.2 EXPANSORES.



Imagen No 3. Expansor de lectoras SP-RDM2

Security Expert 2 Door Expander amplía el número de entradas del lector de tarjetas en el sistema en 2 o 4 al usar el modo Lector Múltiple, el número de entradas de zona en 8

(cuatro entradas utilizadas para control y control de puertas y hasta ocho se pueden usar para funcionalidad extendida) y el número de salidas PGM por 8 (incluye 2 salidas de control de bloqueo de relé). La arquitectura de red de módulo flexible permite conectar grandes cantidades de módulos a la red del módulo RS-485. Se pueden conectar hasta 250 módulos al sistema Security Expert en cualquier combinación con la red, a una distancia de hasta 900m (3000ft). Se puede lograr un mayor alcance con el uso de un módulo de repetidor de red.

3.1.3 FUENTE DE ALIMENTACIÓN.



Imagen No 4. Fuente de alimentación SP-PSU-4A

La fuente de alimentación proporciona 12VDC de potencia adecuada para alimentar dispositivos de seguridad, control de acceso o automatización junto con una gran cantidad de módulos potenciados por la red de Security Expert, y permite un monitoreo simple y potente de las corrientes y tensiones de suministro. La arquitectura de red de módulo flexible permite conectar grandes cantidades de módulos a la red del módulo RS-485. Se pueden conectar hasta 250 módulos al sistema Security Expert en cualquier combinación con la red, a una distancia de hasta 900M (3000ft). Se puede lograr un mayor alcance con el uso de un módulo de repetidor de red.

3.1.4 LECTORAS DE PROXIMIDAD.



Imagen No 5. Lectoras de proximidad.

El aptiQ mini mullion SM10 es un lector inteligente, ideal para nuevas instalaciones o para aquellas que ya han transicionado a tecnología inteligente. Con un atractivo diseño, el lector aptiQ SM10 se adecúa fácilmente con la línea de lectores multi-tecnología aptiQ. Este pequeño, pero potente lector incorpora estándares ISO (14443A, 14443B, 15693), es compatible con FIPS 201-1.

3.1.5 PASILLOS MOTORIZADOS.



Imagen No 6. Pasillos motorizados SlimStyle EV.

Los torniquetes tripode son soluciones de entrada compactas y rentables diseñadas para un funcionamiento suave y silencioso, menos desgaste y menor consumo de energía. adecuado para áreas donde hay un gran flujo de personas. SlimStile EV ofrece una carcasa de dos patas bien diseñada, fabricada en acero inoxidable, ideal para sitios donde hay grandes flujos de personas y robustez. Disponible una versión de acero inoxidable grado 316 y una versión exterior IP44, acero inoxidable 316. Una versión doble también está disponible. En recibir una señal del sistema de control de acceso, o botón pulsador, permite el paso de una persona a una hora.

4. OPERACIÓN DEL SECURITY EXPERT.

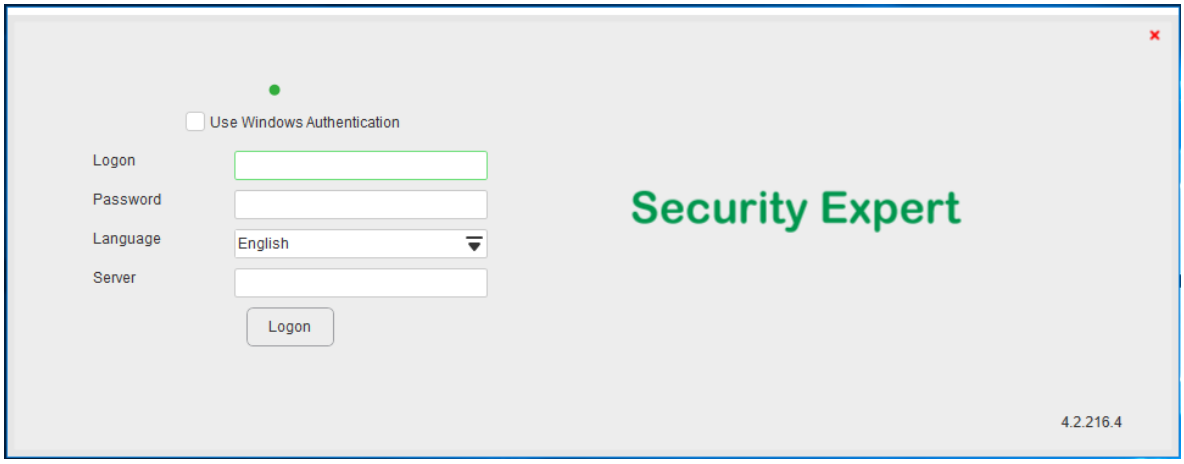


Imagen No. 7 Interfaz de ingreso a la plataforma.

Al ingresar al sistema se muestra la interfaz de ingreso de la imagen No 7, para ingresar se deben registrar las siguientes credenciales:

Username: Operador

Password: Cortezza93

La plataforma da la opción de seleccionar el lenguaje de operación, en este manual se realizará la explicación con el lenguaje nativo que es inglés y se realizarán los tutoriales

de esta misma manera, sin embargo el operador puede elegir manejar el software en español.

4.1 DESCRIPCIÓN DE LA INTERFAZ.

En la imagen No 8 se observa la imagen del centro de operaciones de la plataforma de Security Expert; en ella se podrá realizar la visualización de los eventos, creación de usuarios y asignación de tarjetas.

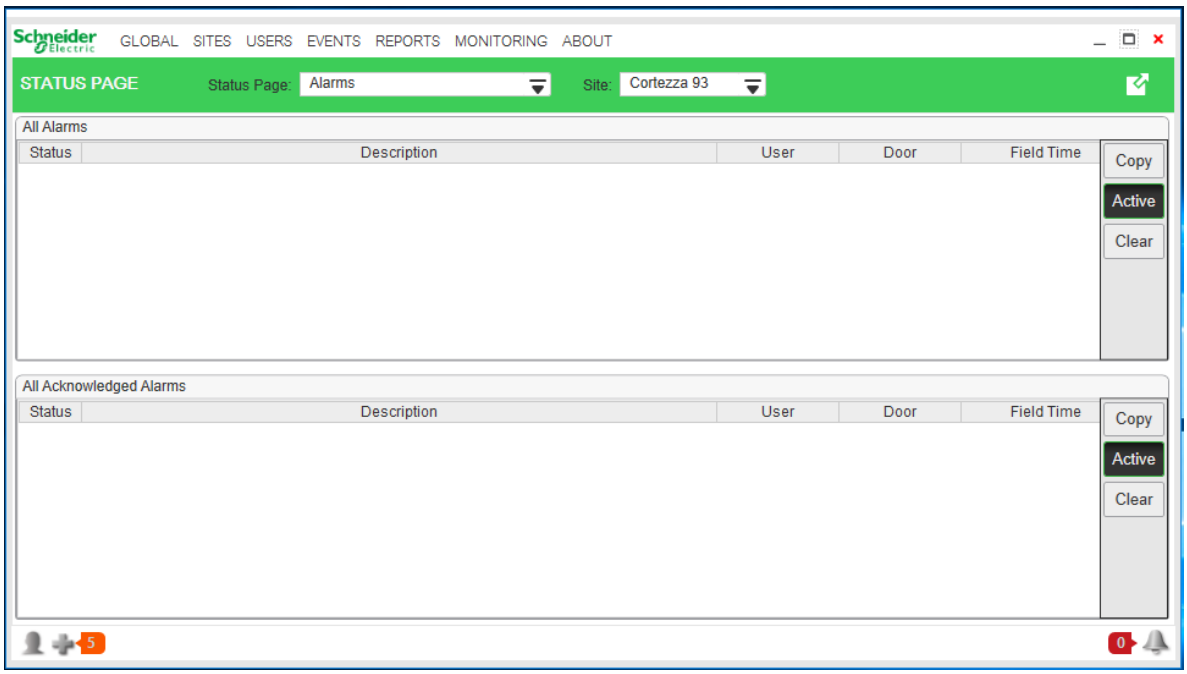


Imagen No 8. Interfaz de usuario del Ops center.

4.1.1 GLOBAL

Dentro de la pestaña **GLOBAL** el operador va a encontrar una única opción que es la de **HOME**, está opción despliega la ventana principal de la interfaz en donde se encontrará información general del sistema tal como detalles del usuario actual, fecha y hora del último ingreso, sitio que se está monitoreando, logout y cambio de contraseña.

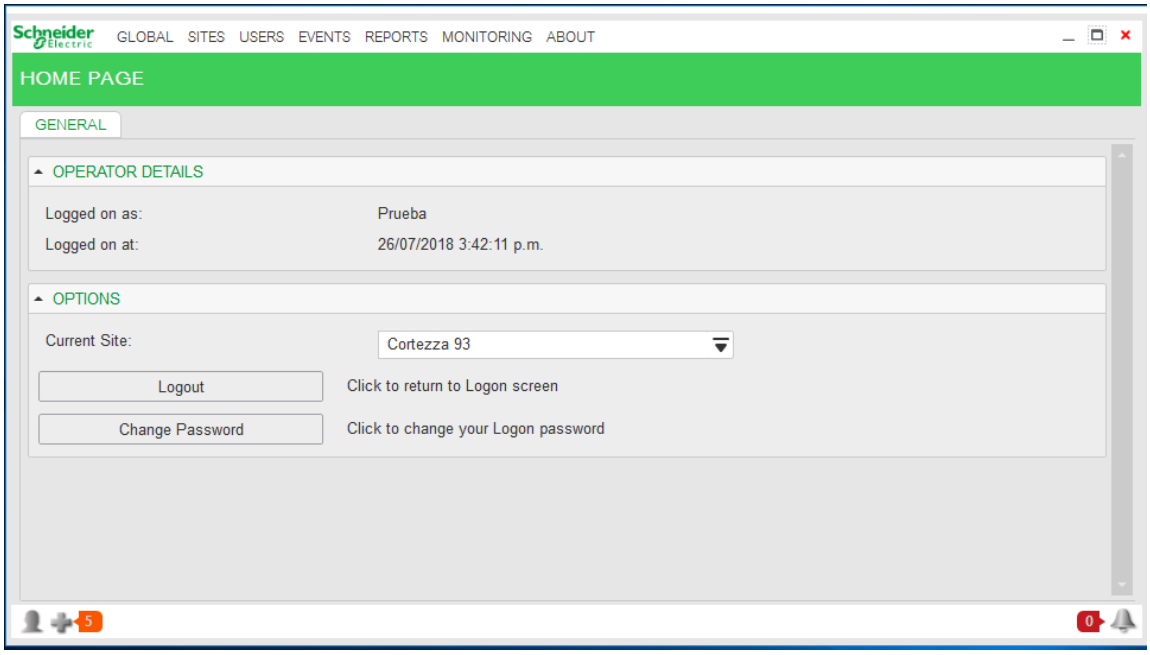


Imagen No 9. Home Page.

4.1.2 SITES.

En la ventana Sites el operador va a encontrar tres opciones, FUNCTION CODES, IMPORT USERS y BATCH ADD USERS. La primera opción está bloqueada porque el perfil del operador no cuenta con permisos para accedes a las funciones de código y las opciones de usuarios son para agregar usuarios de forma masiva por medio de archivos planos .CSV, esto se explicará más adelante en el capítulo de agregar usuarios.

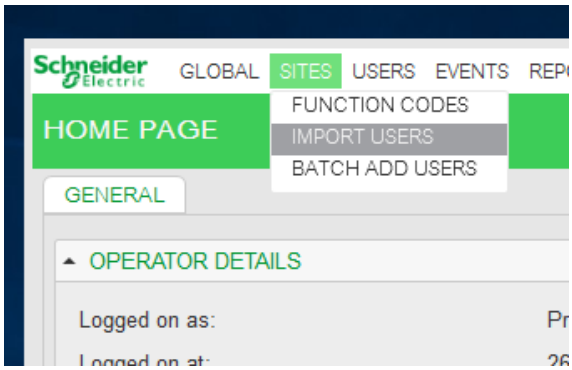


Imagen No 10. Opciones de la pestaña Sites.

4.1.3 USERS.

La ventana de usuarios es donde se puede navegar a través de todos los usuarios que están creados en el sistema y se pueden modificar diferentes opciones de cada uno, como evadir el Antipassback o generarle acceso a otras puertas, entre otros; también se pueden agregar usuarios manualmente uno a uno diligenciando la información en los campos que la requieren.

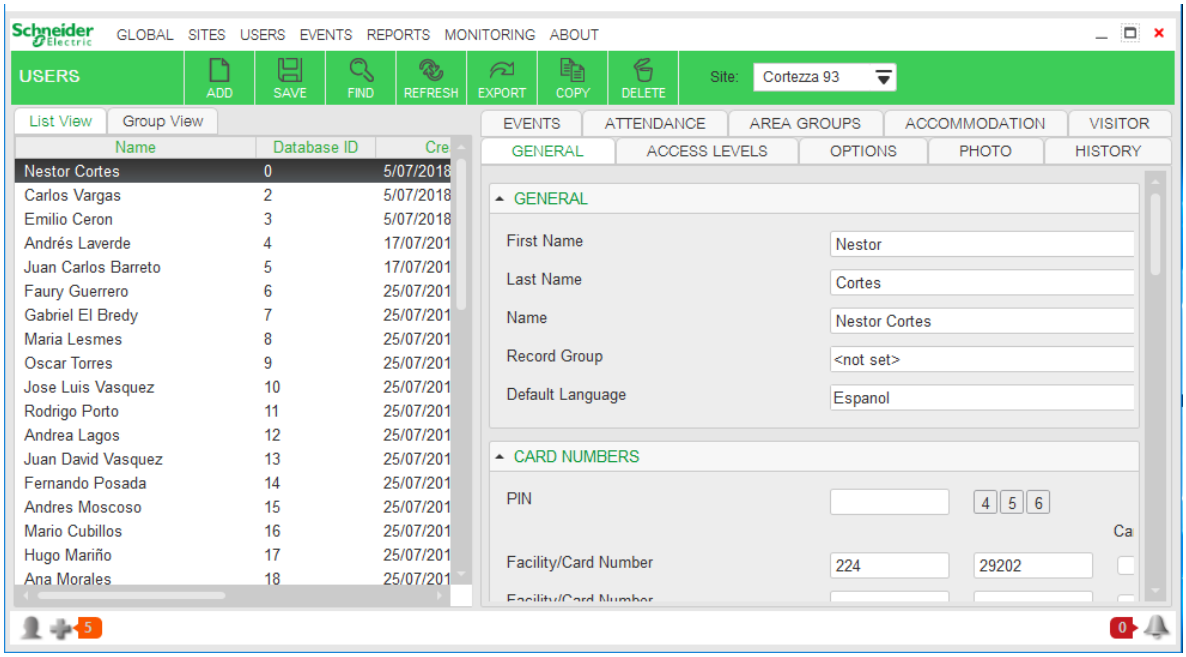


Imagen No 11. Pestaña Users con todas las diferentes opciones.

4.1.4 EVENTS.

Esta es una ventana que me permite generar log de eventos detallados, sin embargo para el perfil de operador se encuentra bloqueado debido a que estos son privilegios de administrador del sistema, por lo tanto cuando intenta ingresar a esta opción se va a mostrar una ventana como la de la imagen No 12, allí se puede apreciar el mensaje de ACCES DENIED.

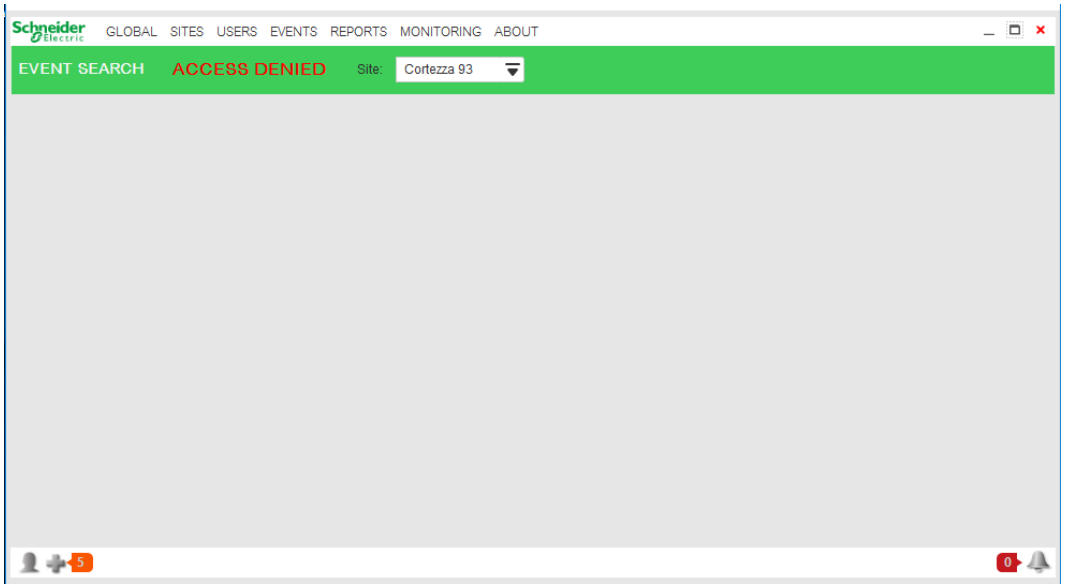


Imagen No 12. Ventana Users dentro de la interfaz del sistema.

4.1.5 REPORTS.

La pestaña reportes despliega dos opciones, EVENT y CENTRAL STATION REPORT, en la pestaña Event se pueden filtrar los eventos de acuerdo a los requerimientos del operador, se puede buscar por fecha o por controlador y guardar los reportes generados.

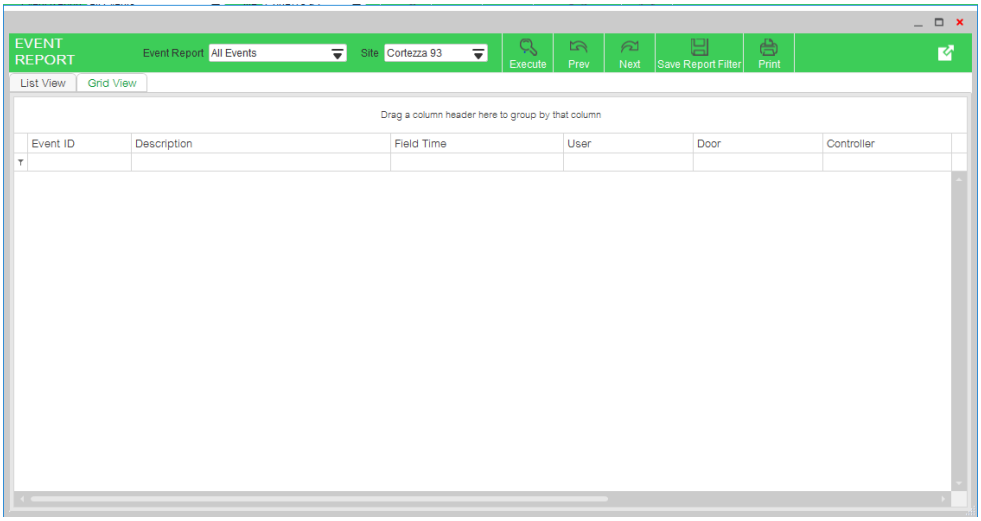


Imagen No 13. Ventana events desplegada.

Es importante tener en cuenta que la opción Central Station report no tiene ninguna utilidad para esta aplicación debido a que se integra un sistema de intrusión o alarma al Security Expert, por lo tanto se recomienda no darle ningún tipo de uso a esta opción.

4.1.6 MONITORING.

La pestaña Monitoring despliega tres opciones, la primera es STATUS PAGE VIEW que se utiliza para realizar un seguimiento de los eventos discriminados por alarmas ocurridas y alarmas reconocidas; la segunda es FLOOR PAN VIEW que se utiliza para realizar una revisión un poco más gráfica de los eventos que están ocurriendo en tiempo real con las puertas configuradas; y por último se encuentra la opción de SETUP que se utiliza para cargar más vistas de planta y listas de estado, esta opción no es apta para monitoreo por lo que se recomienda no generar uso con esta utilidad para evitar errores de funcionamiento.

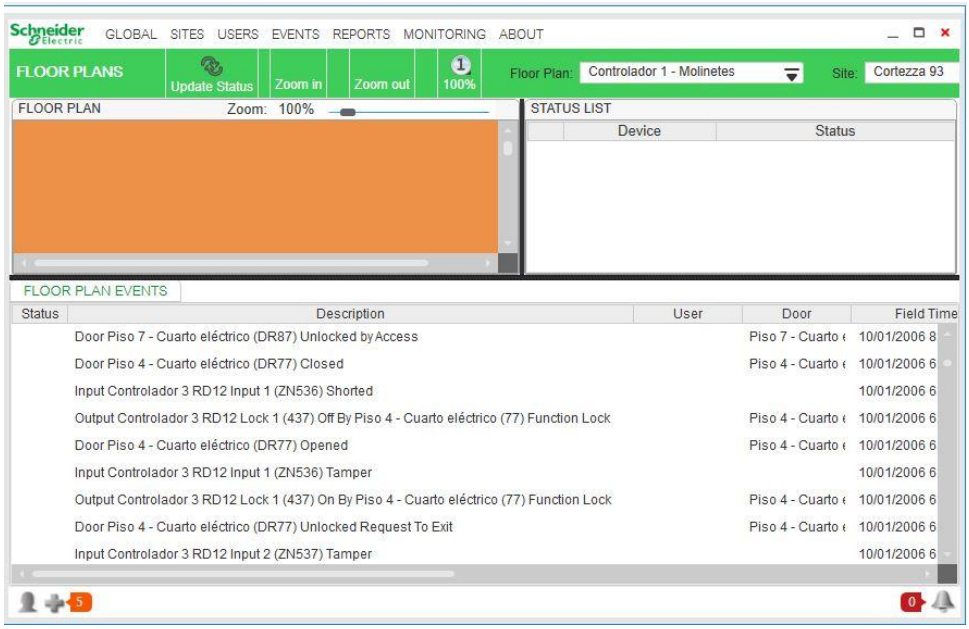


Imagen No 14. Ventana Floor Plan View.

4.1.7 ABOUT.

La pestaña About despliega tres opciones, la primera es HELP que es un link al manual de usuario de fábrica del sistema Security Expert, el usuario puede acudir a esta herramienta cuando se encuentre con preguntas o inconvenientes con respecto a la operación del sistema, cabe resaltar que el usuario encontrará ayuda con respecto a utilidades que no son de la competencia de la operación sino de la configuración del sistema; la segunda pestaña es LICENSE y en ella se encuentra la información de la licencia del sistema, esta opción está bloqueada para el perfil operacional, por lo tanto no será de ningún uso; por último la tercera opción es la de VERSION, esta opción abre una ventana emergente como la información de la versión del software y el nombre del equipo en la que se encuentra instalado el Security Expert.

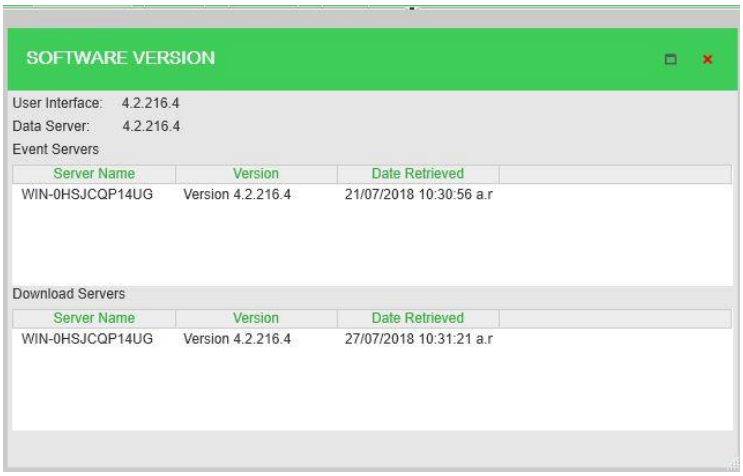


Imagen No 15. Ventana versión desplegada.

4.2 CREACIÓN DE USUARIOS Y ASIGNACIÓN DE TARJETAS.

Hay dos maneras de crear usuarios en la plataforma y asignarles su respectiva tarjeta, la prima es uno a uno diligenciando los datos de cada uno de los usuarios, la segunda es realizar una importación masiva desde un archivo plano .CSV, a continuación se explicará detalladamente de qué manera realizar cada procedimiento.

4.2.1 CREACIÓN DE USUARIOS DESDE LA OPCIÓN USERS.

En el panel de opciones se va a dirigir a la pestaña que dice USER y hace clic en la opción USERS, se desplegará una ventana como la que se muestra en la imagen No. 16 en donde se podrán ver todos los usuarios creados y una serie de opciones para darle a los usuarios un perfil personalizado. Una vez se encuentre en la ventana de usuarios le da click en ADD, notará que los espacios de la pestaña GENERAL se ponen en blanco, proceda a diligenciar los datos de la persona que va a vincular al sistema, asegúrese de diligenciar los 3 primeros campos y de diligenciar los datos de la tarjeta que va a manejar el usuario, los datos que se requieren son el Facility Code y los últimos números de la tarjeta.

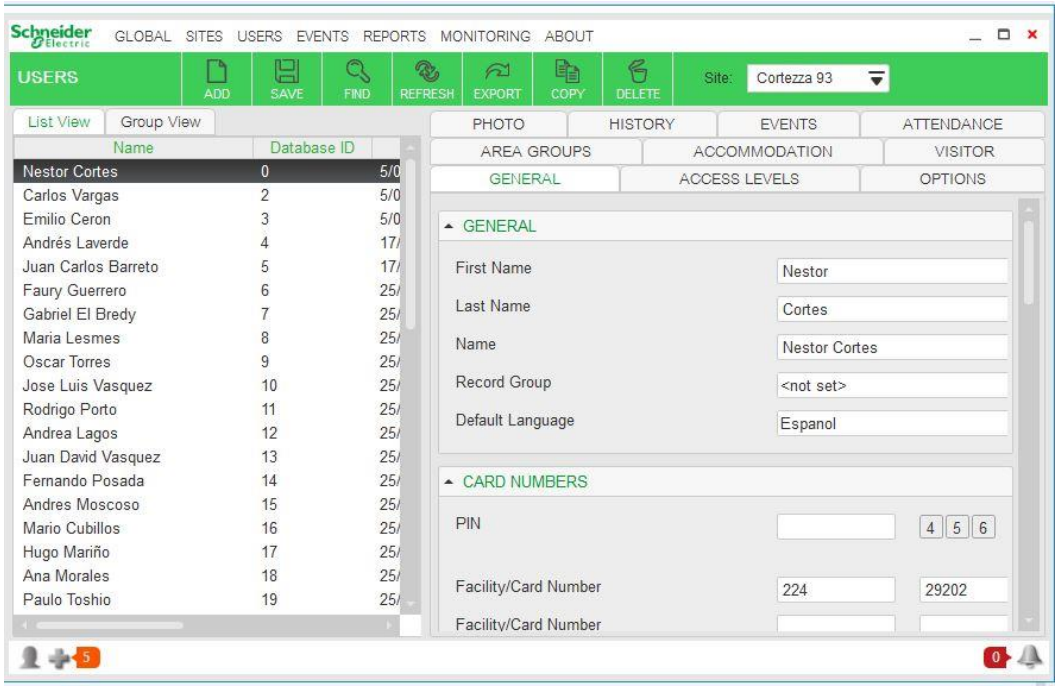


Imagen No 16. Ventana Users.

El operador notará que puede seleccionar un Récord Group o grupo de registro, esto es para agrupar los usuarios de acuerdo a la empresa a la que pertenecen, seleccione el menú desplegable y dele click en la opción que corresponda.

Una vez esos datos están diligenciados va a proceder a asignarle un nivel de acceso a dicho usuario, para esto tendrá que darle click en la pestaña ACCESS LEVELS que se encuentra en la ventana USERS, después click en ADD y seleccione el nivel de acceso que corresponde al usuario que está creando. Los niveles de acceso están creados de la según se describe en la tabla No 2.

Nivel de acceso	Descripción
Administrador	Acceso a todas las puertas del edificio. Full Access.
Ingreso peatonal	Habilita la tarjeta para ingresar y salir por cualquier molinete.
Personal de mantenimiento	Habilita la tarjeta para ingresar a todos los cuartos técnicos.
Personal de seguridad	Habilita la tarjeta para el ingreso al cuarto de control.
Visitante	Habilita la tarjeta para ingresar por cualquier molinete pero sólo permite salir depositando la tarjeta por el capturador.

Tabla No 2. Descripción de los niveles de acceso.

Una vez seleccionado el nivel de acceso le da click en guardar y el usuario aparecerá en la parte derecha en el listado de los demás usuarios.

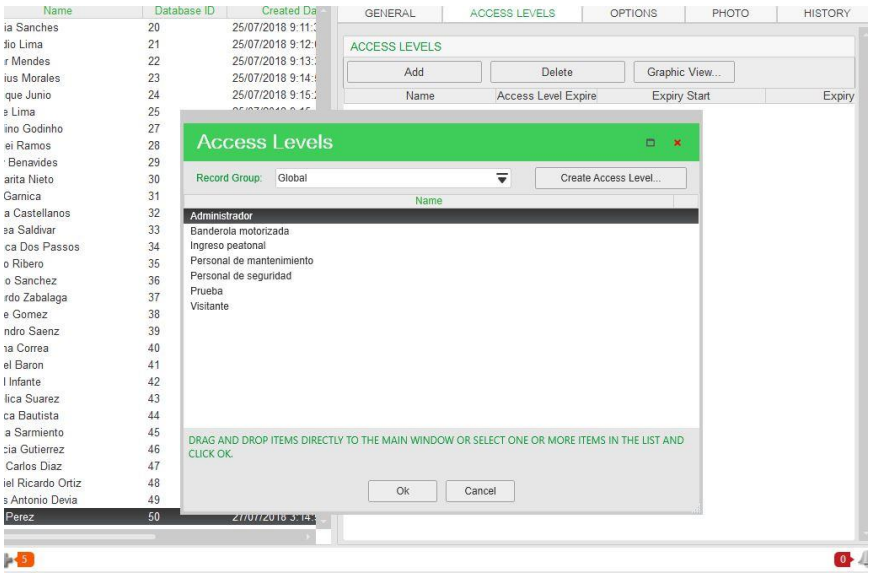


Imagen No 17. Ventana Access levels.

Para el caso de este ejemplo de creó el usuario Juan Pérez con número de tarjeta 123456 y en el grupo de registro de clientes JLR, podemos observarlo en la lista o en la pestaña GROUP VIEW desplegando el record group de clientes JLR como muestra en la imagen No 18.



Imagen No 18. Usuario creado.

4.2.2 IMPORTAR USUARIOS.

Para importar usuarios de manera masiva lo primero que se tiene que hacer en generar un archivo plano .CSV donde se diligenciaran los datos del personal a registrar, se realizará un ejemplo con los usuarios de la tabla No 3 y se realizará el paso a paso para registrarlos por medio de la herramienta importar usuarios.

First Name	Last Name	Name	Facility	Card	Access Level
Juan	Perez	Juan Perez	224	1234	Visitante
Josefina	Ramirez	Josefina Ramirez	224	3456	Ingreso peatonal
Andres	Martinez	Andres Martinez	224	1678	Administrador

Tabla No 3. Datos de los usuarios a registrar por medio de archivo plano.

El primer paso será diligenciar los datos dentro del archivo, es importante aclarar que el campo de Access Level debe diligenciarse tal cual como está registrado en la plataforma, respetando espacios y caracteres, es decir que si por ejemplo el nivel de acceso tiene mayúsculas, en el archivo plano se debe escribir el nivel de acceso en mayúsculas, de lo contrario no se podrá realizar la creación del usuario con éxito. En la imagen No 19 se muestra la forma en la que están diligenciados los usuarios en el archivo plano; también es muy importante que la información esté delimitada por comas, de lo contrario el Security Expert interpretar que toda la información corresponde a una sola columna; una vez diligenciados los datos de todas las personas a ingresar guarda el archivo.

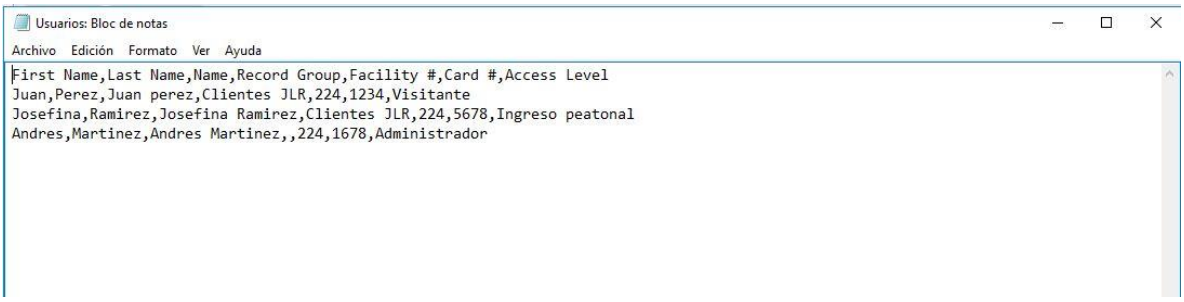


Imagen No 19. Archivo plano .CSV con datos diligenciados.

Una vez completado el paso anterior, diríjase a la pestaña **Sites** y luego seleccione la opción **Import Users**, se desplegará una ventana en la que usted podrá navegar hacia el archivo que acaba de guardar; seleccione el archivo plano y dele click en Next. Dado que en el ejemplo que se está realizando la primera fila del archivo corresponde a la descripción del campo, en la opción que dice **Start import at line** va a seleccionar la opción 2, esto quiere decir que el archivo empezará a tomar la información a partir de la línea 2, deje la opción de delimitador de texto en comillas y seleccione Next.

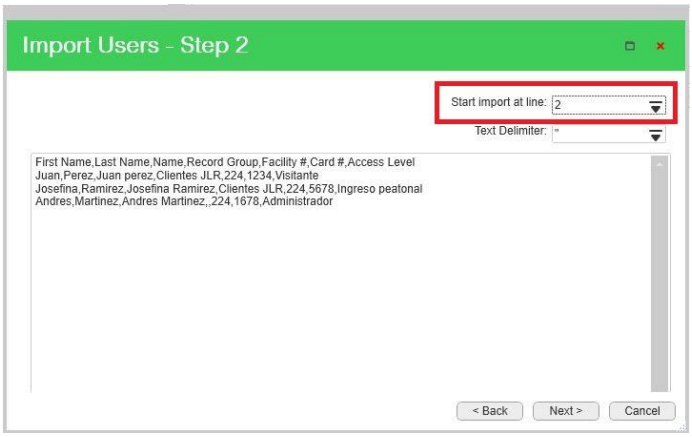


Imagen No 20. Start import at line.

La siguiente ventana mostrará los datos que fueron diligenciados en el archivo plano y desplegará la cantidad de columnas que el software detectó, esto sirve para que el operador valide que la información fue diligenciada de manera correcta. ***Si la cantidad de columnas que arroja el software no coincide con las columnas que fueron diligenciadas debe revisar el archivo plano para encontrar el error***. En este punto lo que se debe hacer es asignar el orden de las columnas, para el ejemplo First Name es la primera columna, Last Name es la segunda, Name (First and Last) la tercera, como el software no nos da la posibilidad de asignar el record group le damos Skip a esa columna y continuamos asignando el orden, de esa manera queda organizado como se ve en la imagen No 21. Dele click en Next.

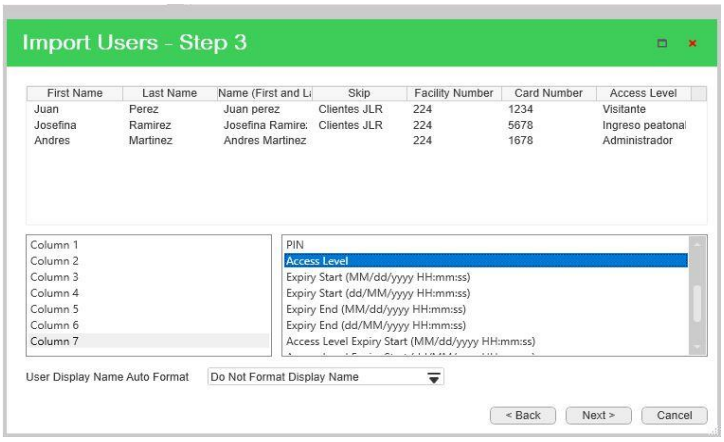


Imagen No 21. Asignación de columnas en la ventana de importar usuarios.

Debido a que ya se le están asignando tarjetas a los usuarios, la siguiente ventana no tendrá ningún uso, así que volvemos a darle click en Next. Por último le damos click en Finish y el procedimiento habrá terminado. Valide que los usuarios hayan sido creados y que los datos correspondan a los que fueron ingresados en el archivo plano.

Si se presentan errores durante el proceso, cuando le de click en Finish saldrá una ventana emergente llamada User Import Errors en donde le listará los errores que encontró durante el proceso, en la imagen No se ve un ejemplo de la ventana de errores donde está diciendo que no puede crear usuarios duplicados.

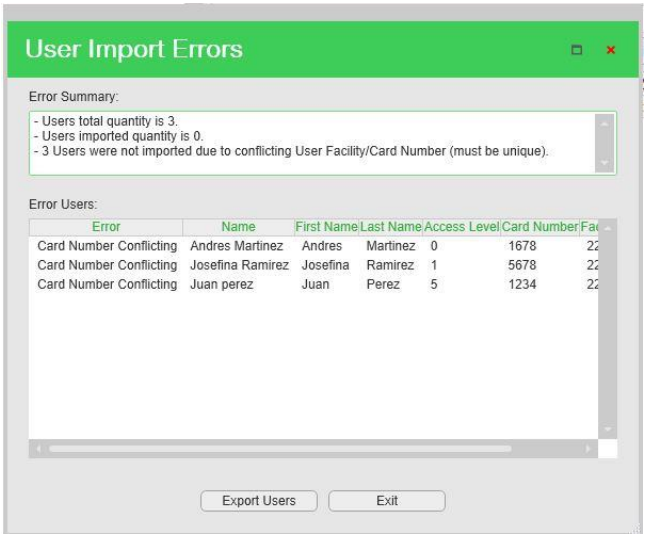


Imagen No 22. Despliegue de errores en la importación de usuarios.

4.3 EVENTOS Y REPORTES.

Los eventos y los reportes son la opción que da el Security Expert para generar un informe de lo que está sucediendo en las puertas que se encuentran controladas, este informe se genera en tiempo real siempre y cuando los controladores se encuentren en línea.

4.3.1 REPORTES.

Para realizar reportes lo que se debe hacer es dirigirse a la ventana **Reports** y seleccionar la opción **Event.** Aparecerá la ventana Event Report, en la parte superior derecha de esta ventana se encontrara un panel de opciones dentro de los cuales está Execute, Prev, Next, Save report filter y Print; Seleccionaremos la opción Excute, que tiene el ícono de una lupa, se desplegará una ventana como se muestra en la imagen No 23. Es importante aclarar que antes de seleccionar la opción Execute se debe especificar si el operador desea un reporte de las alarmas reconocidas, o de las alarmas o de los eventos.

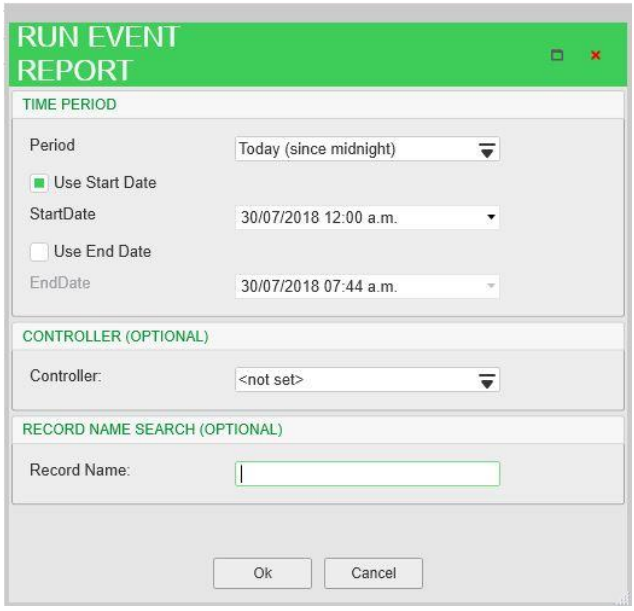


Imagen No 23. Run Event Report.

Dentro de esta ventana el operador contará con tres opciones para elaborar su búsqueda, la primera es el periodo de tiempo en el que desea recibir su reporte, por ejemplo desde media noche del mismo día o de los últimos días, dando click en el menú desplegable Perio encontrará una gran variedad de opciones. O lo puede realizar de manera más específica estableciendo una fecha y hora exacta de inicio y una fecha y hora exacta de

fin para su reporte. La segunda opción le permite escoger la controladora sobre la cual quiere realizar el reporte, recuerde que la lista de puertas asociadas a cada controladora se encuentra en el documento adjunto a este manual y se llama “Distribución control de acceso” así que si desea realizar el reporte sobre una puerta específica puede identificar a qué controladora pertenece esa puerta y de esa manera generar un reporte aún más detallado. La tercera opción es implemente el nombre que el operador le quiera asignar al reporte que va a generar, una vez tenga esta información completamente diligenciada le da click en OK. En ese momento el reporte se habrá generado.

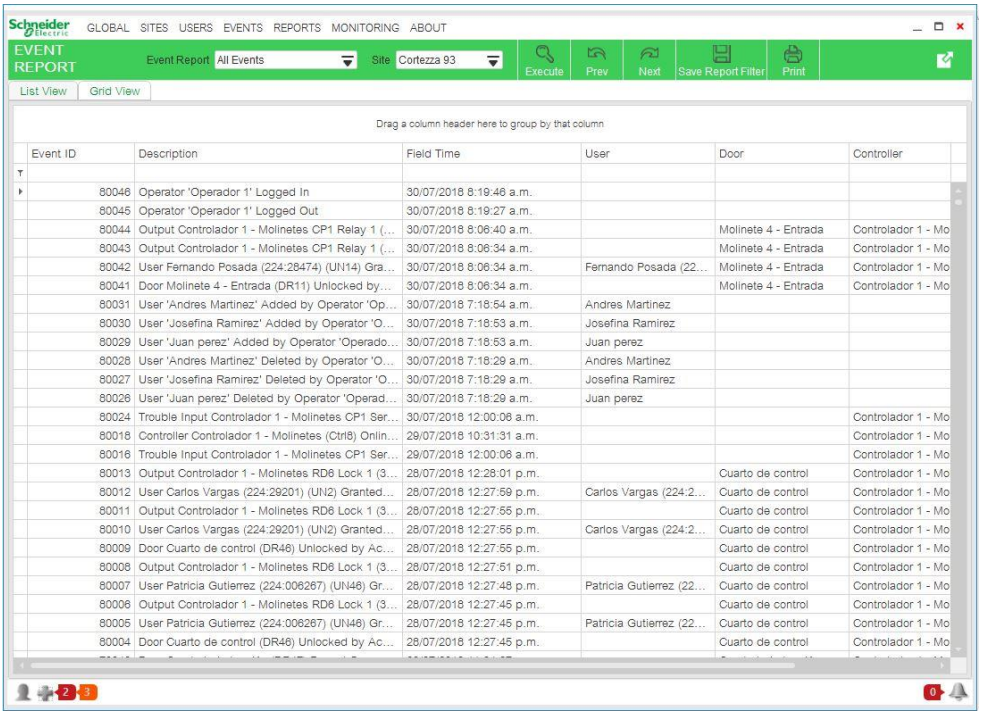


Imagen No 24. Reporte generado.

4.3.2 EVENTOS.

La manera más sencilla y útil de revisar el listado de eventos en tiempo real es dando click en la pestaña **Monitorging** y después seleccionando la opción **Floor Plan View** de esta manera se despliega una ventana en la que se listan todos los eventos que están ocurriendo en tiempo real. Se puede observar en la imagen No 25.

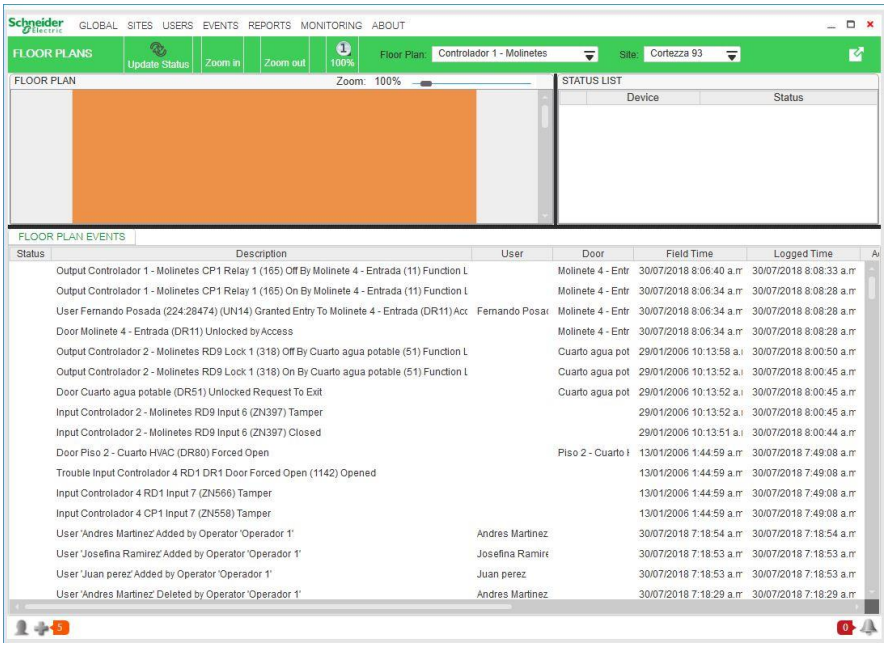


Imagen No 25. Floor Plan View, Eventos en tiempo real.

5. MANUAL DE MANTENIMIENTO PREVENTIVO.

Redes y Proyectos de Energía, en consideración de las buenas prácticas de implementación y mantenimiento de las redes de cableado e instalación de soluciones de control de acceso recomienda tener en cuenta las siguientes observaciones para el óptimo funcionamiento del sistema.

Realizar un MANTENIMIENTO PREVENTIVO al sistema cada tres meses o cada que lo estipule el personal de operación encargado de la administración del edificio, en dicho mantenimiento se deberán tener en cuenta los siguientes puntos:

Revisión del estado de cable de cobre (Cable dúplex, cable UTP Cat. 6). Esta revisión consiste en inspeccionar todos los elementos periféricos del sistema, garantizando que se encuentren en adecuadas condiciones de limpieza y que estén bien anclados a la pared, este procedimiento aplica para lectoras de proximidad, electroimanes y contactos magnéticos, en caso de que se encuentren elementos sueltos, caídos o con deficiencias en el anclaje se debe revisar que el estado de las conexiones y los empalmes se encuentre en buenas condiciones, sin que los empalmes se encuentren sueltos o las

conexiones abiertas. En caso que las conexiones estén sueltas se deben comunicar con el personal autorizado para realizar este tipo de conexiones.

Revisión de los gabinetes de consolidación de equipos, el gabinete principal se encuentra ubicado en el cuarto de control del sótano 1 y hay dos gabinetes secundarios, uno instalado en el cuarto eléctrico del piso 4 y el otro en el cuarto eléctrico del piso 7, hay que procurar que las condiciones de aseo de estos gabinetes siempre sean óptimas ya que es donde se encuentran ubicadas las controladoras del sistema, por lo tanto se debe garantizar que los gabinetes estén limpios y cuidar el exceso de polvo y material particulado, no se deberán realizar desconexiones de ninguna índole, ni desmontar los equipos de los rieles, apagar fuentes ni bajar breakers sin previa autorización del personal correspondiente.

Para el mantenimiento de los electroimanes se recomienda limitarse a realizar limpieza de las terminales de conexión y limpieza física del equipo, no se recomienda desmontar el electroimán ni realizar ningún tipo de acción invasiva dentro del equipo.

6. REGISTRO FOTOGRÁFICO.



Imagen No 26. Controladoras en el gabinete principal de sótano 1.



Imagen No 27. Controladoras en gabinetes secundarios de Piso 4 (Der) y Piso 7(Izq).



Imagen No 28. Electroimán y contactos magnéticos instalados en puerta de cuarto de baja tensión.



Imagen No 29. Ejemplo de instalación de botón de salida y lectora de proximidad.



Imagen No 30. Ejemplo de instalación de control de acceso en puerta sencilla, electroimán magnético y brazo hidráulico.



Imagen No 31. Pasillos motorizados instalados.



Imagen No 32. Banderola motorizada instalada y botones de apertura remota desde el mueble de la recepción.

7. MANUAL DE SOLUCIÓN DE PROBLEMAS FRECUENTES.

Cualquier tipo de anormalidad que se presente en el sistema de control de acceso debe ser revisado por el personal de mantenimiento u operaciones que esté capacitado y tenga el conocimiento básico de sistemas de control de acceso, lectura de tablas de administración y manejo de equipos periféricos como los que están instalados en el proyecto, preferiblemente el personal que haya sido capacitado por REDES Y PROYECTOS DE ENERGÍA SAS EMA; esto debido a que los elementos que componen el sistema son equipos especiales que requieren de un manejo adecuado.

ACTIVIDAD INUSUAL	ACCIÓN A TOMAR
Los controladores se encuentran Offline.	• Verificar que esté bien conectado el patch cord al controlador y al punto de red. Revisar la distribución de los racks para saber en qué punto se encuentran los controladores. • Revisar estado físico del patch cord, si se ve afectado, deteriorado o roto, proceder a cambiarlo. • Realizar ping para prueba de conectividad a la dirección IP del controlador. • Ubicar según la tabla de administración el puerto del switch asociado al punto de red y verificar funcionalidad según el link. • Verificar la conexión del patch cord del switch al punto del patch panel. • Contactar a personal de Redes y Proyectos para asesoría y revisión especializada.
No hay fluido eléctrico en los racks y los equipos pasivos	• Si hubo corte de energía o desconexión desprogramada del fluido eléctrico, el sistema de control de acceso está conectado al regulado (UPS), así que tendrá energía 10 minutos inmediatamente después del corte antes que se apaguen los equipos.

	• Si el fluido eléctrico falla antes de los 10 minutos se debe revisar que el breaker del circuito asociado al sistema Control de acceso esté en estado ON. • Conectar al personal de mantenimiento o al personal de Fleischmann para una revisión del sistema eléctrico.
El electroimán no está funcionando, la puerta queda abierta.	• Revisar con un elemento metálico que el electroimán esté imantando, puede que lo haga con poca fuerza. • Revisar que las conexiones no estén sueltas, sin intervenir los empalmes, sólo realizar una revisión visual. • Contactar a personal de Redes y Proyectos para asesoría y revisión especializada.