

VAX

Control del Acceso VAX ver. 3.1

XX274-30-09



Vicon Industries Inc. no garantiza que las funciones contenidas en este equipo cumplan con sus requisitos o que la operación esté completamente libre de errores o se realice exactamente como se describe en la documentación. Este sistema no ha sido diseñado para usarse en situaciones críticas para la vida y no debe usarse para este propósito.

Número de documento: 8009-8274-30-08 Las especificaciones del producto están sujetas a cambios sin previo aviso. Publicado: 4/23 Copyright © 2023 Vicon Industries Inc. Todos los derechos reservados.

Vicon Industries Inc.

Tel: +1 631-952-2288

Fax: +1 631-951-2288

Sin costo USA: 800-645-9116

UK: 44/(0) 1489-566300

www.vicon-security.com

Guía técnica del control de acceso VAX

Guía técnica de control de acceso VAX de Vicon

Copyright © 2021 Vicon Industries

Nota: Algunas imágenes podrían estar en Inglés debido a la disponibilidad en el código madre

Tabla de Contenido

Introducción	xi
Vicon Software - Acuerdo de licencia de usuario final	xii
Copyright	xiv
1. Resumen	1
Requisitos del Servidor	1
Sistemas operativos compatibles	2
Procedimientos de instalación	2
Nueva instalación VAX	2
Actualización VAX.....	7
Monitoreo del sistema.....	7
Preguntas Frecuentes.....	8
Instalación del cliente.....	9
Navegadores compatibles	9
Acceso al servidor.....	10
Preguntas frecuentes.....	10
2. Actualización del VAX	12
Actualizaciones de software	12
Descargue la última versión de VAX	12
Requisitos previos a la instalación.....	12
Instalación de actualización	12
Actualizaciones de firmware del panel.....	12
Solución de problemas de actualización de firmware	14
Preguntas Frecuentes.....	15
3. Configuración inicial	16
Configuración inicial del software de control de acceso de Vicon.....	16
Configuración de conexión	17
Configuración del Cliente.....	17
Información del distribuidor.....	18
Administrador inicial.....	18
Ajustes del correo electrónico.....	18
Inicio de sesión en la interfaz web de VAX.....	19
Recuperación de contraseña en VAX.....	19
Configuración inicial del panel	20
Navegación por la interfaz del panel	21
Configuración del modo de comunicación: Servidor IP.....	22
Configuración del Modo de Comunicación: Nombre del Servidor (DNS).....	24
Configuración de IP del panel: DHCP	25
Configuración de IP del panel: IP estática.....	27
Reinicio de un panel	30
Prueba de Entradas/Salidas en la Puerta.....	31
Interfaz de configuración HTTP del panel	39
Adición de un panel al control de acceso VAX	40
Método 1: agregar un panel a través de la pantalla Paneles desconocidos	41
Método 2: Adición manual de un panel con dirección MAC	42
Adición de un panel: configuración básica	42
A dónde ir desde aquí	44
4. Licencias de software	45
Licencia de su software	45
Formatos de tarjeta admitidos	47
Preguntas frecuentes sobre licencias de software	47
5. Interfaz de usuario del administrador del sistema.....	49
Acceso a la interfaz de usuario del administrador del sistema.....	49
Cambiar la contraseña de la interfaz de usuario del administrador del sistema	50
Copia de seguridad de la base de datos	51
Restauración de su base de datos	53
Gestión de servicios y sistemas.....	54

Gestión de servicios.....	54
Apagar o reiniciar su servidor	54
Ajustes de red en System Manager.....	55
Certificados SSL	57
Introducción a los Certificados	57
Certificados autofirmados.....	58
Certificados PEM.....	58
Certificados PFX	59
Almacenamiento de certificado	59
Instalación de un certificado en el almacén de certificados.....	60
Multi-usuario.....	62
6. Planificación de la implementación de control de acceso.....	56
Hardware.....	56
Especificaciones de hardware	57
Topología de comunicación.....	62
Cables, Estándares y Mejores Prácticas	64
Requisitos de alimentación del VAX-MDK Door Master.....	64
Identificación de un panel	65
Software	66
Orden de Operaciones.....	66
Particiones	68
Sitios	69
Zonas horarias de puerta.....	70
Zonas horarias del usuario	72
Grupos de privilegios de acceso.....	73
Feriados	81
7. Configuración de su Panel	77
Configuración avanzada del panel.....	77
Pestaña General.....	77
Opciones.....	78
Configuración de entrada/salida	79
Actualización de su panel	85
Actualización automática del panel	86
Actualizaciones de firmware del panel.....	87
Solución de problemas de actualización de firmware	89
8. Configuración de una puerta	90
Agregar una puerta	90
Configuración avanzada de puertas	92
General	92
Opciones.....	93
Configuración del Lector	96
Áreas.....	98
9. Configuración de la zona horaria de la puerta	99
Agregar una zona horaria de la puerta	99
10. Zonas horarias del usuario.....	102
11. Acceder a grupos de privilegios.....	104
12. Configuración de usuario/titular de tarjeta.....	106
Agregar un usuario.....	106
Privilegios de usuario.....	107
Imágenes del titular de la tarjeta de usuario.....	108
Campos personalizados	108
Credenciales de usuario	109
Grupos de acceso.....	110
Plantillas de usuario	110
Inscripción de titulares de tarjetas mediante notificación	111
Importación de usuarios y titulares de tarjetas	112
Adición de campos personalizados	114
13. Configuración de días festivos	117

Orden de las festivos de operaciones.....	117
Zonas horarias de festivos del usuario	118
Grupos de festivos de usuario	119
Zonas horarias de festivos de la puerta.....	120
Grupos de días festivos de la puerta	121
Zonas horarias de festivos para piso.....	122
Grupo de festivos para pisos	123
Agregar un día festivo	124
Ejemplo de festivo.....	125
14. Zonas de ejecución única.....	129
Adición de una zona horaria de ejecución única	129
15. Niveles de crisis.....	131
Cambios en los niveles de crisis.....	131
Configuración de los niveles de seguridad del usuario	132
Aplicación de niveles de crisis a las puertas	132
Aplicación de niveles de crisis en el control de acceso VAX.....	132
Aplicar Niveles de Crisis con una Entrada Aux	133
16. Funciones de anulación del control de acceso de Vicon	134
Cancelar puertas.....	134
Cancelar pisos	135
Invalidar salidas	146
Invalidar entradas.....	147
Invalidar particiones de alarma	148
17. Funciones de deslizamiento triple	138
Requisitos del usuario para usar el triple deslizamiento.....	138
Lista de opciones de deslizamiento triple	138
Configuración de triple deslizamiento.....	140
Ejemplos de triple deslizamiento	141
18. Descripción del sistema.....	143
19. Configuración de particiones y sitios.....	146
Agregar particiones.....	146
Agregar sitios y áreas	147
Editar Sitios y Áreas: Áreas	148
Editar Sitios y Áreas: Formatos de Tarjeta	148
20. Administradores y Privilegios	150
Administradores	160
Agregar una cuenta de administrador	150
Ejemplos de administrador	154
Administradores de Cuentas de Servicio para Servicios de Terceros	165
Privilegios de administrador.....	166
Terminología	166
Resumen de privilegios	167
Asignación de privilegios.....	168
Grupos de seguridad.....	169
Ejemplos de privilegios.....	170
Informe de privilegios	171
Permisos	172
Permisos de administrador del sistema	173
Permisos de usuarios y programación.....	173
Permisos del sistema	174
Permisos de dispositivos.....	175
Permisos de programación	176
Permisos de días festivos	177
Permisos especiales	179
Permisos de informes.....	179
Permisos globales	180
Permisos de notificación	181
Autenticación.....	182

Autenticación local	182
Autenticación OAuth.....	183
Autenticación de dos factores	185
21. Áreas y Anti-Passback	159
Hardware.....	159
Módulo de memoria APB	159
Configuración del software anti-passback	160
Agregar áreas	160
Configuración Anti-Passback.....	161
Asignación de áreas a los lectores	162
Estado APB y Violaciones	163
22. Configuración de trampa de hombre	166
Configuración del hardware de trampa.....	166
23. Reportes	169
Registro Administrativo	169
Actividad del usuario	170
Actividad de la puerta	172
Reporte de Actividad de Piso.....	174
Reporte de actividad del ascensor.....	176
Lista de usuarios	178
Reporte de Notificaciones.....	180
Reporte de asamblea (Muster)	182
Reportes de Configuración	185
Actividad de entrada	187
Actividad de salida	189
Actividad del plan de acción	191
Seguimiento del tiempo	193
Actividad de alerta.....	226
Particiones de alarma	231
24. Notificaciones	196
Destinos	196
Tiempo real.....	196
Correo electrónico	196
Web Push	196
Base de datos	198
Configuración de Página de notificaciones.....	198
Reglas de Notificación	198
Tipos.....	198
Grupos	198
Acceso a la pantalla de configuración de notificaciones	198
Lista de reglas.....	199
Creación de una regla de notificación	199
Estilos de notificación	200
Creación de una regla de estilo de notificación.....	201
Reglas de cámara en vivo	202
Crear una regla de cámara en vivo	202
Barra lateral de notificaciones.....	202
Controles de la barra lateral.....	203
Pantalla de Monitoreo	204
Acceso a la pantalla de monitoreo.....	204
Personalización de las notificaciones mostradas	205
Opciones de monitoreo.....	205
Opciones de notificación seleccionadas.....	206
25. Base de datos	208
Depuración de notificaciones.....	208
Depuración del registro del administrador	209
Advertencia sobre el tamaño de la base de datos.....	209
26. Configuración del sistema	211

Configuración general	211
Dirección del servidor	211
Seguridad.....	212
Seguridad mejorada con PIN manual.....	212
Configuración de correo electrónico	212
Configuración de correo electrónico	212
Notificaciones por correo electrónico.....	213
Configuración de la aplicación móvil.....	251
Generación de un código QR.....	251
Solicitudes de servicio	251
Purgar notificación	252
27. Hardware para ascensores	214
Conexión del panel Elevator-Master a la placa de E/S	215
Configuración de direcciones de placa de E/S	216
Prueba de entrada/salida de la placa E/S	218
Sensor de sabotaje de placa de E/S	218
28. Componentes del software del ascensor	219
Agregar un panel de elevador.....	220
Agregar un elevador	222
Botón de detección	224
Mapa de E/S por piso	225
Zonas horarias de piso	225
Asignación de acceso de usuario a pisos.....	227
29. Protocolo abierto de dispositivo supervisado (OSDP V2)	228
Beneficios de usar OSDP	228
Modelos de controlador de puerta compatibles.....	228
Cómo comprobar si el firmware es compatible con OSDP	228
Cableado de un lector OSDP.....	229
Puntos de conexión OSDP	229
Resistores de terminación	230
Configuración de la comunicación OSDP.....	270
Configuración de la dirección del lector OSDP a través del menú LCD	271
Ajustes de comunicación del software OSDP.....	272
Configuración del modo de canal seguro OSDP	273
Configuración de claves de cifrado	273
Habilitación del modo de canal seguro en lectores OSDP	274
Software: restricción de la comunicación OSDP al modo de canal seguro	275
30. Tableros de Entrada / Salida.....	277
Introducción	277
Números de pieza de la placa de E/S.....	277
Configuración de hardware.....	277
Conexión del placas Master E/S a las placas E/S	278
Configuración de direcciones de placa de E/S	279
Configuración del software de E/S.....	280
Adición del panel maestro E/S a VAX.....	281
Configuración de entradas y salidas	283
Programaciones de entrada y salida.....	287
Puertas no administradas y monitoreadas con placas E/S.....	292
Aplicaciones del mundo real para entradas y salidas	294
31. Integración del sistema de cámara	297
Navegadores compatibles	297
Habilitar el servidor web/móvil	298
Habilitar servidor web: Valerus Configuration	298
Habilitar servidor web: ViconNet	298
Habilitar servidor web: Milestone XProtect Mobile.....	299
Habilitar servidor web: Exacq exacqVision Web Services	299
Habilitar servidor web: Digital Watchdog DW Spectrum.....	300
Adición de un sistema de cámara.....	300

Administrar sistemas de cámara.....	301
Purgar cámaras.....	302
Aceleración GPU.....	303
WebSockets.....	303
Usar Proxy.....	303
Visualización de cámaras sincronizadas.....	303
Visualización de video en vivo.....	304
Visualización de reproducción de vídeo.....	305
Asociación de cámaras con puertas y ascensores.....	306
Asociaciones de cámara: puerta.....	307
Asociaciones de cámaras: Ascensor.....	307
Notificaciones de cámara.....	307
Configuración de alertas de cámara en vivos.....	308
Adición de certificados de sitio web para la integración de cámaras.....	309
Importación de certificación en Internet Explorer.....	310
Importación de Certificación enGoogle Chrome.....	311
Importación de certificados con el Asistente de importación de certificados..	313
Matriz de cámaras de varios proveedores.....	315
Visualización de cámaras en Matrix.....	317
32. Integración de directorio activo.....	318
Descripción general de la integración.....	318
AD Integración Orden de Operaciones.....	318
Planificación: qué información de AD se sincronizará.....	319
Grupos AD, Membresía y Estructura.....	320
Credenciales de usuario.....	320
Configuración de cuentas de servicio.....	322
Crear y configurar cuentas de servicio.....	322
Instalar VAX.....	323
Configuración de integración LDAP en VAX.....	325
User Credenciales de Usuarios LDAP.....	325
Campos personalizados de usuarios LDAP.....	326
Crear asociaciones entre grupos de AD y grupos de privilegios de acceso.....	327
Sincronizar usuarios desde.....	329
Autenticación del administrador LDAP.....	330
Solución de problemas de integración LDAP.....	332
Conflictos LDAP.....	332
Los servicios VAX no se inician.....	327
Sincronizar usuarios desde AD.....	329
Autenticación del administrador LDAP.....	330
Solución de problemas de integración LDAP.....	332
Conflictos LDAP.....	332
Los servicios VAX no se inician.....	327
Sincronizar usuarios desde AD.....	329
Autenticación del administrador LDAP.....	330
Solución de problemas de integración LDAP.....	332
Conflictos LDAP.....	332
Los servicios VAX no se inician.....	332
33. Motor de control de acción.....	334
Introducción.....	334
Casos de uso de ACE.....	334
Componentes ACE.....	334
Planes de acción.....	334
Disparadores de acción.....	338
Conceptos de acción avanzados.....	341
Variables en los Planes de Acción.....	341
Expresiones en Planes de Acción.....	343
Si Acción.....	344
cada acción.....	344

Acción HTTP	346
Exportación e importación de planes de acción.....	348
34. Mapas interactivos.....	350
Agregar un mapa	350
Mapas adyacentes	351
Agregar objetos a los mapas	352
Dibujar un área.....	354
Ver y monitorear con mapas.....	355
Barra lateral de objetos del mapa	357
Barra lateral de detalles del objeto.....	357
35. Third Party IntegrationIntegración de terceros.....	359
Assa Abloy® Aperio™ Lock Sistemas	359
Requisitos de software/hardware	359
Configuración de hardware	359
Configuración del software: Aplicación de programación Aperio.....	360
Configuración del software: paneles y puertas VAX Aperio	363
36. Información para administradores de red y dominio	365
Configuración del acceso remoto avanzado a través de Internet	365
Cómo se comunican los paneles	365
Cómo se comunican los clientes web con VAX.....	365
Acceso remoto: requisitos de red.....	365
Realización de una copia de seguridad y restauración	367
Realización de una copia de seguridad y restauración manual con MSSQL Command-Line	367
Copia de seguridad de la base de datos SQL	368
Restauración de base de datos SQL	368
Copia de seguridad/restauración de la base de datos: Preguntas frecuentes	370
Realización de la migración de datos con Data Migrator	371
Exportación de datos de partición.....	371
Importación de datos de partición	371
Integración API.....	372
REST API.....	372
API en tiempo real.....	372
Acceso a la documentación de la API.....	373
Configuración del modo multiusuario.....	373
Configuración del modo multiusuario.....	373
Adición de inquilinos.....	374
37. Apoyo	375
37. Soporte	377
38. Integración de alarma IP DSC.....	378
Funciones de integración de DSC	378
Descripción general de alto nivel de los pasos de integración.....	378
Configuración de comunicación del panel DSC	379
39. Tablero.....	381
Introducción a los tableros	381
Creación de tableros	381
Grupo de navegación.....	383
Graficas	384
Estadística.....	384
Estadística.....	385
Reporte.....	386
Reporte de Muster	387
.....	388
Barra lateral de notificaciones.....	388
40. Impresión de credencial	390
Descripción general de la impresión de distintivos.....	390
Nuevo editor de tarjetas.....	390
Impresión de una tarjeta	394

41. Integración Schlage.....	396
Descripción general de Schlage	396
Allegion ENGAGE App	396
Adición de un sitio ENGAGE 396	396
Conexión de una puerta de enlace ENGAGE a la aplicación	397
Adición de un juego de cerraduras Schlage a VAX.....	397
Adición de juego de cerradura a una puerta	398
Supervisión y anulación de Schlage	398
Solución de problemas de Schlage	398
42. Monitoreo de Salud en VAX.....	400
Introducción a la Vigilancia del funcionamiento	400
Historial de funcionamiento.....	400
Herramientas de historial defuncionamiento.....	400
Configuraciones de funcionamiento.....	404
Introducción a la configuración de funciones	404
Conclusion	407
43. Solución de problemas en VAX.....	408
Herramientas comunes: Menú LED del panel	408
Solución de problemas del instalador	408
Nota importante	409
Sistemas operativos no admitidos y requisitos previos	409
Herramienta de configuración	409
Solución de problemas de SQL Server.....	409
No se puede instalar/desinstalar VAX - Error 1316	
La cuenta especificada ya existe	410
Guía de instalación de Windows 11 SQL para unidades NVME 410	410
Mover VAX a una nueva computadora	411
Mover VAX a una nueva computadora	411
Solución de problemas de comunicación	413
Diagnóstico del servidor	413
Diagnóstico del panel.....	413
No se puede conectar a VAX.....	414
VAX se niega a conectarse.....	415
VAX obtiene el tiempo de espera de conexión a la base de datos (3.0+)	415
Triple deslizamiento no funciona en lectores de tarjetas	416
Periféricos de entrada, salida y salida	416
Resolución de problemas de entrada, salida y periféricos	417
Solución de problemas de acceso denegado.....	418
¿Funcionarán mis tarjetas existentes con VAX?	419
El teclado no envía PIN.....	419
Lista de posibles motivos de acceso denegado.....	419
Tipos de acceso denegado	420
Solución de problemas del lector.....	421
Metodología de resolución de problemas	421
El lector no responde a la credencial	421
El lector no se enciende	422
El lector emite un pitido erróneo	423
El número de tarjeta no coincide con el número esperado.....	423
El software muestra un formato de tarjeta desconocido al presentar la credencial	423
El lector responde a la credencial pero no a la notificación en el software	425
Lectores y Configuración.....	425
Lectura de tarjeta incorrecta.....	425
Lectores de tarjetas que se apagan de forma intermitente en un panel VAX-MDK	425
Problemas de cableado.....	426
Especificaciones de energía	426
Lectores:	426
Salidas:	426

Introducción

Vicon se enorgullece en presentar el control de acceso VAX. Esta guía está diseñada para ayudarlo a planificar, instalar y configurar su nuevo sistema de control de acceso. Aunque hemos hecho todo lo posible para garantizar que el proceso de instalación sea intuitivo y sencillo, recomendamos leer esta guía en su totalidad antes de instalar un sistema de acceso Vicon.

Software Vicon - Acuerdo de Licencia de Usuario Final

IMPORTANTE - LEER CON CUIDADO:

Este Acuerdo de Licencia de Usuario Final ("EULA – siglas en Ingles) es un acuerdo legal entre usted (ya sea un individuo o una sola entidad legal) y Vicon con el cual adquirió los productos de software de Vicon identificados anteriormente ("SOFTWARE"). El SOFTWARE incluye software Vicon, y puede incluir asociado medios de comunicación, impreso materiales, "en línea", o electrónico documentación y servicios basados en Internet. Nota: cualquier software, documentación o servicio web que se incluya en el SOFTWARE, o accesible a través del SOFTWARE, y están acompañados por sus propios acuerdos de licencia o términos de uso; se rigen por dichos acuerdos en lugar de este EULA. Este EULA es válido y otorga derechos de usuario final ÚNICAMENTE si el SOFTWARE es genuino. Al instalar, copiar, descargar, acceder o utilizar el SOFTWARE, usted acepta estar sujeto a los términos de este CLUF. Si usted no acepta los términos de este EULA, usted no podrá usar o Copiar el SOFTWARE, y debe comunicarse de inmediato con Vicon para obtener instrucciones sobre la devolución de los productos no utilizados de acuerdo con las políticas de devolución de Vicon.

1. LICENCIA DEL PRODUCTO DE SOFTWARE

El término "COMPUTADORA" como se usa en este documento significará el HARDWARE, si el HARDWARE es un solo computador o deberá significar la computadora del sistema con cual el HARDWARE funciona, si el HARDWARE es un componente del sistema informático

2. CONCESIÓN DE LICENCIA

Vicon le otorga los siguientes derechos, siempre que cumpla con todos los términos y condiciones de este EULA:

Instalación y uso: Salvo que se indique expresamente lo contrario en este EULA, puede instalar, usar, acceder, mostrar y ejecutar solo una (1) copia del SOFTWARE en la COMPUTADORA. El SOFTWARE no puede ser utilizado por más de la cantidad de copias genuinas con licencia registradas con Vicon.

Activación Obligatoria: ESTE SOFTWARE CONTIENE MEDIDAS TECNOLÓGICAS DISEÑADAS PARA EVITAR EL USO SIN LICENCIA O ILEGAL DEL SOFTWARE. Los derechos de licencia otorgados en virtud de este EULA se limitan al primer año (1 año) después de ejecutar el SOFTWARE por primera vez, a menos que proporcione la información requerida para activar su copia con licencia de la manera descrita durante la secuencia de configuración (a menos que Vicon lo haya activado por usted). Puede activar el SOFTWARE mediante el uso del teléfono; se pueden aplicar cargos de peaje. Es posible que también deba reactivar el SOFTWARE si modifica su HARDWARE o altera el SOFTWARE.

Copia de Seguridad: Usted puede utilizar la copia de seguridad únicamente para fines de archivo y para reinstalar el SOFTWARE en la COMPUTADORA. Salvo que se indique expresamente en este EULA o en la legislación local, no puede realizar copias del SOFTWARE, incluidos los materiales impresos que acompañan al SOFTWARE. No puede prestar, alquilar, arrendar, prestar o transferir de otro modo el DVD o la copia de seguridad a otro Usuario.

Reserva de Derechos: Vicon reserva todos los derechos no expresamente otorgados a usted en este EULA.

3. DESCRIPCIÓN DE OTRO DERECHOS Y LIMITACIONES

Consentimiento para el uso de datos: acepta que Vicon puede recopilar y utilizar la información técnica recopilada de cualquier manera como parte de los servicios de soporte del producto que se le brindan, si corresponde, en relación con el SOFTWARE. Vicon puede usar esta información únicamente para mejorar sus productos o para brindarle servicios o tecnologías personalizados. Vicon puede divulgar esta información a otros, pero no en una forma que lo identifique personalmente.

Información de la base de datos: solo se puede acceder a la información almacenada en la base de datos y/o en los archivos de respaldo de la base de datos a través del SOFTWARE con

licencia de Vicon. Cualquier intento de acceder a la información de la base de datos a través de un acceso sin licencia y/o rescindiré este acuerdo de licencia. Vicon no proporciona acceso directo a la información de la base de datos.

Software/servicios adicionales: los términos de este EULA se aplican a las actualizaciones, complementos y componentes complementarios del SOFTWARE de Vicon que Vicon pueda proporcionarle o poner a su disposición después de la fecha en que obtenga su copia inicial del SOFTWARE, a menos que otros términos se proporcionan junto con dichos Componentes Suplementarios. Limitaciones en ingeniería inversa, de compilación y desensamble. No puede aplicar ingeniería inversa, descompilar o desensamblar el SOFTWARE.

Separación de Componentes: El SOFTWARE se licencia como un solo producto. Sus componentes no pueden separarse para su uso en más de una computadora. EULA único: el paquete del SOFTWARE puede contener múltiples versiones de este EULA, como múltiples traducciones y/o múltiples versiones multimedia (p. ej., en la documentación del usuario y en el software). En este caso, solo tiene licencia para usar una (1) copia del SOFTWARE.

Terminación: Sin perjuicio de cualquier otro derecho, Vicon puede cancelar este EULA si no cumple con los términos y condiciones aquí contenidos. En tal caso, deberá destruir todas las copias del SOFTWARE y todos sus componentes. Marcas comerciales: este EULA no le otorga ningún derecho en relación con las marcas comerciales o marcas de servicio de Vicon o sus proveedores.

4. ACTUALIZACIONES

Si el SOFTWARE está etiquetado como una actualización, debe tener la licencia adecuada para usar un producto identificado por Vicon como elegible para la actualización a fin de usar el SOFTWARE ("Producto elegible"). Únicamente a los efectos de la(s) actualización(es), "HARDWARE" significará el sistema informático o el componente del sistema informático con el que recibió el Producto elegible. El SOFTWARE etiquetado como una actualización reemplaza y/o complementa (y puede deshabilitar, si se actualiza un producto de software de Vicon) el Producto elegible que vino con el HARDWARE. Después de la actualización, ya no podrá usar el SOFTWARE que formó la base para su elegibilidad para la actualización (a menos que se indique lo contrario). Puede usar el producto actualizado resultante solo de acuerdo con los términos de este EULA y solo con el HARDWARE. Si el SOFTWARE es una actualización de un componente de un paquete de programas de software cuya licencia obtuvo como un solo producto, el SOFTWARE se puede usar y transferir solo como parte de ese paquete de producto único y no se puede separar para usar en más de una computadora.

5. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los títulos y derechos de propiedad intelectual sobre el SOFTWARE (incluidos, entre otros, imágenes, fotografías, animaciones, videos, audio, música, texto e incorporados al SOFTWARE), los materiales impresos que lo acompañan y cualquier copia del SOFTWARE, son propiedad de Vicon o de sus proveedores. El software es con licencia, no vendido. Todos los títulos y derechos de propiedad intelectual sobre el contenido que no está incluido en el SOFTWARE, pero al que se puede acceder mediante el uso del SOFTWARE son propiedad del propietario del contenido respectivo y pueden estar protegidos por derechos de autor aplicables u otras leyes de propiedad intelectual y tratados. El uso de cualquier servicio en línea al que se pueda acceder a través del SOFTWARE puede regirse por los respectivos términos de uso relacionados con dichos servicios.

6. RESTRICCIONES A LA EXPORTACIÓN

Usted reconoce que el SOFTWARE está sujeto a la jurisdicción de exportación de EE. UU. y Canadá. Usted acepta cumplir con todas las leyes internacionales y nacionales aplicables que se aplican a los productos, incluidas las Regulaciones de la Administración de Exportaciones de EE. UU. y Canadá, así como las restricciones de destino, uso final y usuario final emitidas por los gobiernos de EE. UU., Canadá y otros.

7. DISPOSICIONES ADICIONALES

PARA LAS GARANTÍAS LIMITADAS, LA LIMITACIÓN DE RESPONSABILIDAD Y OTRAS DISPOSICIONES ESPECIALES, CONSULTE LAS DISPOSICIONES ADICIONALES PROPORCIONADAS Y/O DE OTRO MODO CON EL SOFTWARE. DICHAS GARANTÍAS LIMITADAS, LIMITACIÓN DE RESPONSABILIDAD Y DISPOSICIONES ESPECIALES SON PARTE INTEGRAL DE ESTE EULA.

Copyright

Copyright © 1998 - 2023 Vicon Todos los derechos reservados.

La información de este documento está sujeta a cambios sin previo aviso. El software descrito en este documento se proporciona bajo acuerdo de licencia. El software solo se puede utilizar de acuerdo con los términos expresados por Vicon.

Ninguna parte de esta documentación puede reproducirse o transmitirse de ninguna forma o por ningún medio, excepto para el beneficio del usuario de operar el software sin el permiso expreso por escrito de Vicon.

Vicon Industries Inc.

Telefono:
+1 631-952-2288

Website: www.vicon-security.com

Capítulo 1. Primeros pasos


Descripción general

VAX es un moderno sistema de control de acceso de cliente/servidor basado en web HTML5. La aplicación del servidor está diseñada a ser instalado en a ser único ordenador personal y puede ser accedido usando uno o más clientela a través de a navegador web. El software del servidor VAX consta de:


- **Servidor web VAX** : la responsabilidad del servidor web es alojar la aplicación web y facilitar el acceso del cliente para administrar su sistema de control de acceso.
- **VAX Gestor del Sistema:** Sistema del gerente responsabilidad es a administrar apoyo arriba y restaurando la base de datos, así como administrar la configuración de múltiples inquilinos, la configuración general del servidor.
- **VAX Monitoreo del Sistema:** El Sistema Monitor permite tú a vista el estado y ofertas limitado control sobre el servidor web y las utilidades de copia de seguridad/restauración.
- **Base de datos Proveedor** VAX usos a relacional base de datos a almacenar el configuración y notificaciones del sistema de control de acceso. Se puede configurar para usar cualquiera de las siguientes bases de datos:
 - **Base de datos de Microsoft SQL Server:** El software VAX se puede configurar para usar un servidor Microsoft local o remoto. sql Base de datos. Tú puede optar a usar el gratis (incluido) sql Expresar 2019 o su propia instancia preinstalada de Microsoft SQL. Tenga en cuenta: Se requiere una versión mínima de 2008.
 - **Postgres:** El VAX software poder ser configurado a usar a local o remoto postgresql base de datos. usted puede optar para el instalador a instalar él, o usar su propio existente instancia. Por favor Nota: A Se requiere un mínimo de Postgres v12.

Requisitos del Servidor

El servidor de aplicaciones VAX está diseñado para ejecutarse en una PC moderna con Microsoft Windows 10 o superior; también se recomienda Windows Server 2016 o superior para un rendimiento óptimo.

 **Nota:** Es posible instalar el software VAX en una PC compartida; sin embargo, cuando sea posible, recomendamos una instalación independiente para obtener un rendimiento y una confiabilidad óptimos. También es posible instalar VAX en una máquina virtual, fuera del sitio o en la nube. Para obtener más información sobre los paneles que se comunican con el panel a través de Internet, consulte la sección correspondiente en la guía técnica principal.

- 2GHz o un procesador más rápido de 32 bits (x86) o 64 bits (x64). Se recomiendan dos o más núcleos.
- 4GB RAM para 32-bit y 64-bit .
- 10 GB de espacio libre en disco duro (se requiere espacio adicional para la base de datos).
- Windows 10 Home o superior (Windows 7 no compatible). Compatible con Windows 10/11.
- Microsoft .Net Framework 4.8.1.
- Microsoft SQL Server 2016 o SQL Server 2016 Express o superior (instalación de SQL Express disponible desde el instalador de VAX).

 **Nota:** Las especificaciones de la computadora son los estándares mínimos para un sistema básico. Cuando un sistema incluye una gran cantidad de clientes (más de 10), controladores (más de 50) y/o usuarios (más de 2000), se recomienda enfáticamente potencia de servidor adicional.

Sistemas operativos compatibles

Nota

Tenga en cuenta que esto se refiere a los sistemas operativos capaces de ejecutar el software del servidor. Los clientes son compatibles independientemente de la versión del sistema operativo, siempre que sea compatible con HTML5. Para obtener más información sobre los navegadores web de clientes compatibles, consulte la sección denominada "Navegadores compatibles".

Tabla 1.1. Sistemas operativos compatibles

Sistema Operativo	Nota
Windows 11 Professional (32 y 64 bit)	
Windows 11 Home (32 y 64 bit)	
Windows 10 Professional (32 y 64 bit)	
Windows 10 Home (32 y 64 bit)	
Windows Server 2016 (Cualquier Versión)	
Windows 8 Professional (32 y 64 bit)	
Windows 8 Home (32 y 64 bit)	
Windows Server 2016	

No se admiten los siguientes sistemas operativos. VAX no puede instalarse correctamente en estos sistemas operativos:

Tabla 1.2. Sistemas operativos no compatibles

Sistemas operativos no compatibles	Notas
Windows XP (Cualquier Versión)	Falta el núcleo web alojable
Windows Vista (Cualquier Versión)	Falta el núcleo web alojable
Windows 8/7 Starter Edition	Componentes faltantes
Windows 7 Home Basic	Componentes faltantes
Windows Server 2003 (Cualquier Versión)	Falta el núcleo web alojable
Windows RT	Específico para ARM

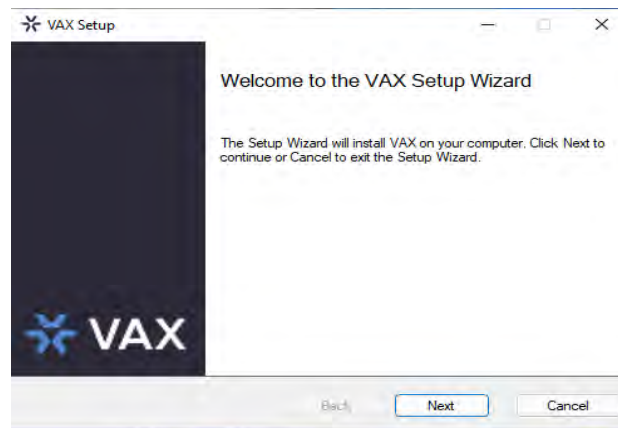
Procedimientos de Instalación

Esta sección cubre la instalación de VAX y algunas frecuentemente preguntadas.

Nueva Instalación VAX

1. Localice y ejecute el archivo llamado "VAX.exe" en su medio de instalación o descargue y ejecute el instalador desde nuestro sitio web.
2. En sistemas operativos más antiguos, el instalador puede requerir una instalación de .NET Framework 4.5.1. Si es necesario, el instalador ejecutará el instalador de .NET Framework incluido antes de iniciar el instalador de VAX. Una vez instalado el requisito previo necesario, el instalador iniciará automáticamente el instalador de la aplicación VAX.

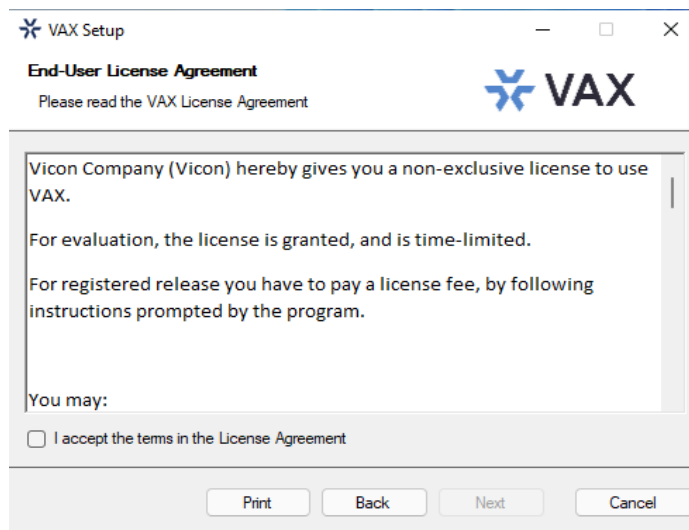
Figura 1.1. Instalador de aplicaciones VAX



Después de que se haya cargado el instalador de VAX, haga clic en el botón Siguiente para continuar.

3. En la siguiente pantalla, lea y acepte el Acuerdo de licencia. Este acuerdo debe aceptarse para proceder con la instalación del VAX. Haga clic en Siguiente.

Figura 1.2. Acuerdo de licencia VAX

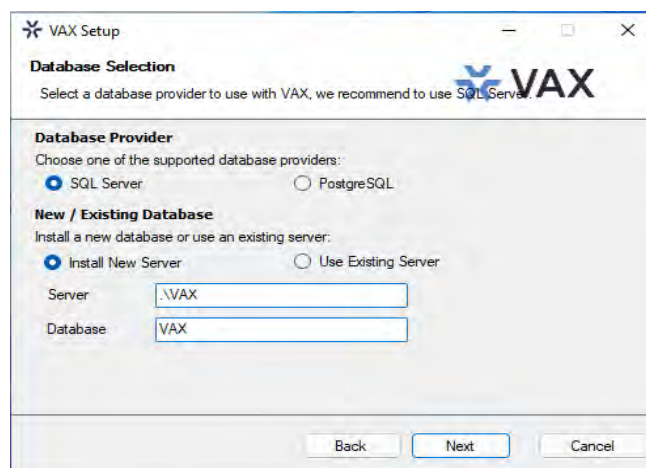


4. El siguiente paso es elegir el tipo de instalación:


- **Instalación típica:** Se recomienda una para instalaciones normales. Utiliza la configuración predeterminada para los puertos de escucha, usa las cuentas de SERVICIO NT locales para los servicios, crea reglas de entrada para los puertos de escucha en el Firewall de Windows y genera un certificado autofirmado..
- **Instalación Avanzada:** Se recomienda para usuarios que deseen utilizar un servidor SQL externo o que necesiten opciones de configuración avanzadas para entornos de dominio. Tiene mucho más control sobre varias opciones de configuración de VAX.

5. La página de selección de base de datos le permite seleccionar qué proveedor de base de datos instalar o usar y le permite configurar los ajustes de conexión que VAX usará para acceder a la base de datos.

Figura 1.3. VAX selección de base de datos



- **Proveedor de base de datos** Se puede utilizar SQL Server o PostgreSQL como base de datos. Para instalaciones nuevas, recomendamos utilizar SQL Server. Si actualiza una instalación existente, estos campos deben completarse automáticamente.

 **Nota:** Se recomienda utilizar SQL Server cuando se hospeda la base de datos en la misma máquina que el software VAX.

- **Instalar un nuevo servidor/Usar servidor existente:** Si tiene una instalación existente del proveedor de la base de datos, puede seleccionarla en el campo desplegable Servidor. De lo contrario, puede seleccionar **Instalar** nuevo servidor para instalar el proveedor de base de datos seleccionado y configurarlo para su uso con VAX.
- **Servidor** El campo Servidor le permite ingresar la dirección del servidor de la base de datos. Si se selecciona SQL Server y Usar servidor existente, el menú desplegable del campo Servidor mostrará una lista de instancias detectadas de SQL Server. Si está actualizando una instalación existente, el campo Servidor se completará con el servidor SQL configurado existente.
- **Base de datos** El nombre de la base de datos es el nombre único que se le da a la base de datos dentro del servidor de la base de datos. El menú desplegable mostrará una lista de bases de datos que detectó en el servidor seleccionado.
- **Nombre de usuario** Un campo opcional para el nombre de usuario para autorizar el software para acceder a la base de datos. Este campo no es necesario para la instalación básica y se utiliza para autorizar su propio proveedor de base de datos externo.
- **Contraseña:** Un campo opcional para autorizar al software a acceder a la base de datos. Este campo no es necesario para la instalación básica y se utiliza para autorizar su propio proveedor de base de datos externo.

6. **[Solo instalación avanzada]** La configuración de comunicación le permite modificar los puertos utilizados por el software para alojar servicios web y servidores de comunicación.

Servidor web: El servicio del servidor web es responsable de proporcionar la interfaz basada en web y las API. El **puerto HTTPS** es el puerto en el que el servidor escuchará las comunicaciones web, de forma predeterminada es **11001**.

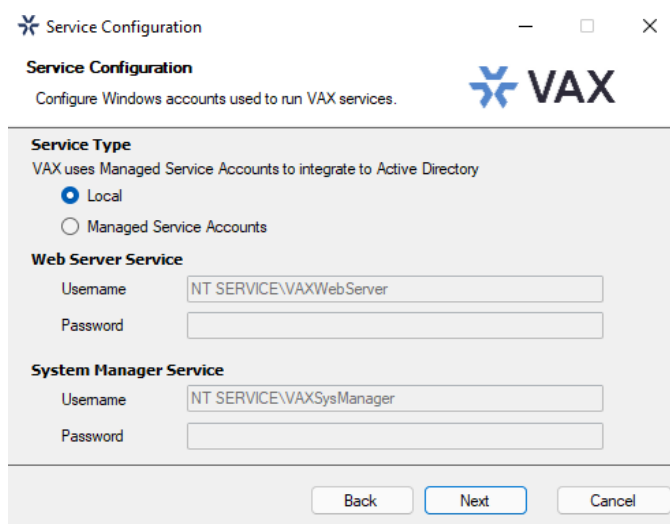
Panel de Comunicación: El servicio de servidor web alberga un servidor para comunicarse con nuestros paneles. El **puerto TCP/UDP** es el puerto que el servidor escuchará las conexiones del panel, por defecto es **9876**.

Administrador de sistemas: El servicio de administrador del sistema es responsable de administrar las copias de seguridad de la base de datos y la configuración del servidor. El **puerto**

HTTPS es el puerto en el que el servidor escuchará la comunicación de administración; de manera predeterminada, es **11002**.

7. **[Solo para la instalación avanzada]** La configuración del servicio le permite configurar las cuentas utilizadas para alojar los servicios del servidor web y del administrador del sistema. La opción **Local** utilizará cuentas NT SERVICE, cual son especial virtual ventanas cuentas usado a anfitrión servicios. La opción **Cuenta de servicio administrada** se usa para la integración de Active Directory para permitir el acceso a los servicios para consultar el dominio. La creación de cuentas de servicio administradas está fuera del alcance de este manual de instalación.

Figura 1.4. VAX Configuración del servicio

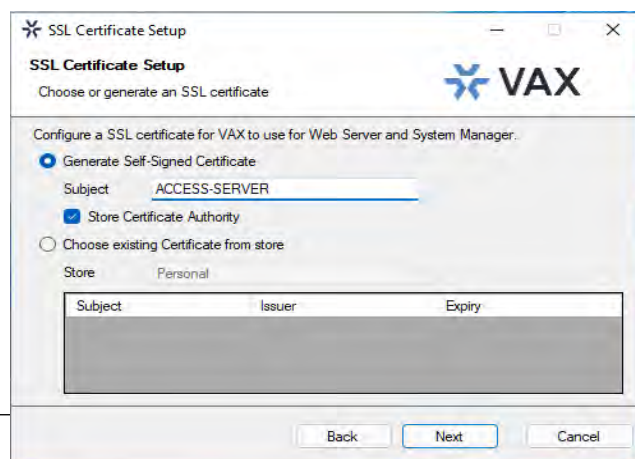


8. **[Solo para la instalación avanzada]** La configuración del certificado SSL le permite generar o seleccionar un certificado SSL para usarlo para alojar los servicios web del servidor web y del administrador del sistema. La opción **Generar certificado autofirmado** generará un nuevo certificado con el sujeto especificado para su uso. Los certificados autofirmados generarán una advertencia al buscar el software, ya que el navegador no puede validar al emisor del certificado. Al seleccionar **Almacenar Certificado Autoridad**, se eliminará esta advertencia solo en la computadora de instalación, al almacenar el certificado de firma como un certificado raíz.

La opción **Elegir un certificado existente** de la tienda le permitirá seleccionar un certificado de la tienda de certificados de Windows que tenga una clave privada válida. Los certificados que se han importado a Windows se mostrarán aquí.

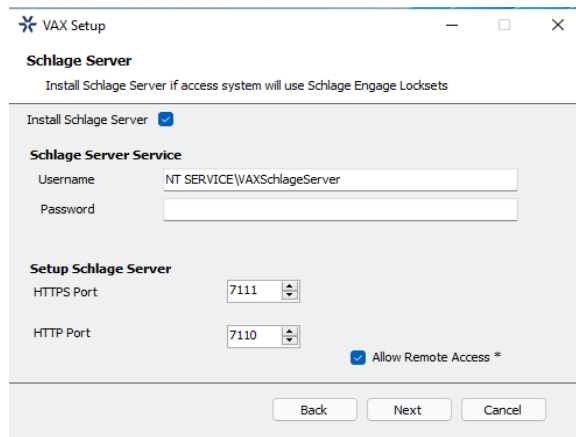
Los certificados SSL se pueden administrar después de la instalación en System Manager en Configuración → Certificados.

Figura 1.5. VAX Configuración del certificado SSL



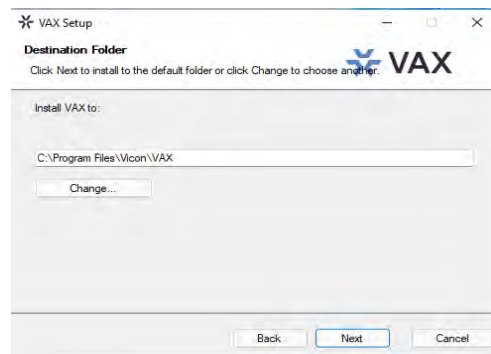
9. **[Solo para la instalación avanzada]** Schlage Server es un servicio independiente que se comunica con las puertas de enlace y las cerraduras de Schlage Engage. Si necesita el uso de la integración de cerraduras Schlage, marque la opción Instalar servidor Schlage y personalice los puertos del servidor Schlage o las cuentas de servicio según sea necesario.

Figura 1.6. VAX Servidor Schlage



10. El siguiente paso es seleccionar el directorio de instalación donde desea que se instale la aplicación VAX.

Figura 1.7. VAX Carpeta de destino



11. Ahora ha completado la parte de configuración del instalador. Haga clic en Instalar para realizar la instalación de VAX y Finalizar cuando finalice la instalación.

Actualización VAX

Se lanzan actualizaciones periódicas a VAX para mejorar las funciones, corregir errores o mejorar la compatibilidad. VAX no ofrece paquetes de actualización por separado. Nuestro instalador independiente es capaz de instalar una nueva instancia de software o actualizar una instancia existente del software VAX.

Actualización de instalación

Dependiendo de cómo haya instalado VAX, el procedimiento para actualizar el software VAX puede requerir algunos pasos que no se describen en esta sección. Consulte el Capítulo 2, Actualización de VAX para obtener más detalles sobre estos pasos adicionales. Recomendamos hacer una copia de seguridad de su base de datos VAX antes de actualizar. Para obtener más información sobre cómo realizar una copia de seguridad de su base de datos, consulte la sección correspondiente en la guía técnica principal. También recomendamos detener el servicio VAX a través de System Monitor antes de la instalación. Tenga en cuenta que si el instalador no contiene una versión más nueva que la versión instalada actualmente, no tendrá la opción de realizar una actualización.

Actualización del Firmware

En algunos casos, para utilizar la última versión de VAX, también se requiere una actualización de firmware en los paneles (consulte la sección correspondiente en la guía técnica principal).

Monitor del Sistema

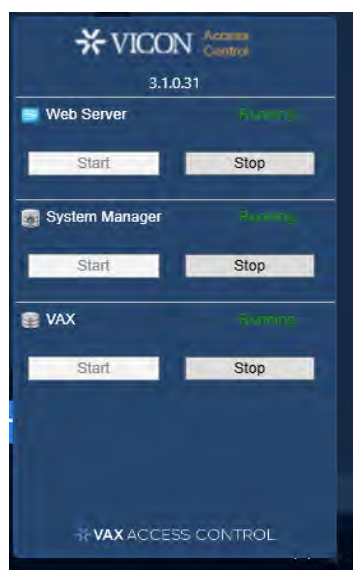
Monitor del Sistema (System Monitor) es una aplicación de bandeja que le muestra el estado y ofrece un control limitado sobre el proceso del servidor web. Puede brindarle varios atajos útiles cuando se hace clic con el botón derecho en el icono. También le mostrará la versión actual de su software VAX.

Una vez que VAX esté instalado en el servidor, el ícono del monitor del sistema se ubicará en la bandeja del sistema (junto al reloj, resaltado a continuación). Si no ve este icono, es posible que esté oculto. Puede utilizar el icono de flecha en la bandeja del sistema para mostrar iconos ocultos. También puede iniciar System Monitor desde el menú de inicio de la computadora en la que está instalado VAX.



Para ver el Monitor del sistema, simplemente haga clic en el icono y aparecerá una pequeña ventana cerca de la bandeja del sistema (en la imagen a continuación).

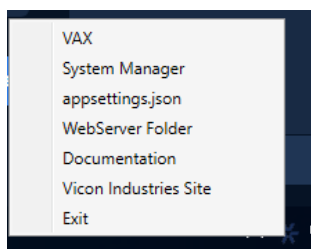
Figura 1.8. Ventana del monitor del sistema



Una vez que se abre la ventana Monitor del sistema, puede usar los botones Iniciar y Detener para iniciar y detener los Servicios utilizados por VAX. Esto puede ser útil si la base de datos o el servicio web no se inician automáticamente.

Consejo

Si hace clic con el botón derecho en el icono del Monitor del sistema, obtendrá varios accesos directos útiles.



Preguntas frecuentes

P: ¿Tengo que usar SQL Express 2019 o puedo usar mi propio software de base de datos?

R: Admitimos cualquier Microsoft SQL Server desde 2016 hasta el presente o Postgres v12 o posterior; sin embargo, al usar nuestro software para instalar SQL Express, puede estar seguro de que está configurado de manera óptima para nuestro sistema. Si elige usar su propia instancia de servidor de base de datos, deberá asegurarse de que los privilegios y protocolos correctos estén disponibles para la conexión. Esto es algo que generalmente solo recomendamos para técnicos o administradores de red que estén bien versados en la instalación y configuración de SQL Server. También tenga en cuenta que las diferentes versiones de SQL tienen diferentes requisitos de sistema operativo y PC. Si elige usar una versión diferente, asegúrese de que su PC cumpla con los requisitos para esa versión.

P: ¿Es compatible con los sistemas operativos Windows Vista o Windows XP??

R: En este momento no hay ningún plan para admitir sistemas operativos anteriores a Microsoft Windows 10. Nos comprometemos a garantizar que el software funcione con futuras versiones de Microsoft Windows.

P: Recibí un error de SQL durante la instalación de VAX. ¿Qué tengo que hacer?

R: Como parte de la instalación de VAX, debe proporcionar la información de SQL correcta que el instalador utiliza para configurar una serie de opciones de seguridad y base de datos de VAX. Si esta información es incorrecta, deberá corregirse antes de que pueda instalar correctamente el software VAX. Si ha elegido instalar SQL Express como parte de la instalación de VAX, la configuración debe completarse automáticamente. Sin embargo, si ha elegido usar una versión y/o instancia de base de datos personalizada, deberá completar manualmente esta configuración.

P: ¿Cuál es el tamaño máximo de base de datos admitido?

R: Si está utilizando Postgres, no hay un tamaño máximo de base de datos. Si utiliza Microsoft SQL Server
tamaño máximo de la base de datos es una limitación directa de la versión de SQL instalada, no del software VAX. Si ha utilizado la instalación predeterminada de SQL Express 2019, el tamaño máximo de la base de datos es de 10 GB. Las versiones anteriores de SQL Express anteriores a 2008 generalmente tenían una limitación de 2 GB.

P: ¿VAX es de 32 bits o de 64 bits?

R: VAX es una aplicación de 32 bits diseñada para ejecutarse tanto en sistemas operativos nativos de 32 bits como en sistemas operativos de 64 bits con capacidad de emulación de 32 bits (x64). No hay ningún plan para admitir una instalación nativa de 64 bits, ya que el software VAX no se beneficiará del aumento de direccionamiento que proporciona 64 bits.

Instalación del Cliente

VAX admite la conectividad del cliente a través del acceso basado en web. Como resultado, no es necesario instalar ningún software de cliente VAX; más bien usa su navegador web para acceder al servidor VAX.

Navegadores Soportados

La lista de navegadores admitidos no es una lista exhaustiva. Estos son navegadores que reciben pruebas de Vicon Industries. Aunque otros navegadores pueden funcionar, no brindamos asistencia técnica con ellos. Siempre buscamos los comentarios de los usuarios para decidir qué navegadores brindar soporte de primera clase y ampliaremos la lista de navegadores compatibles según lo dicte su participación en el mercado.

Tabla 1.3. VAX Navegadores soportados

Navegador	Version	Soportados	Notas
Google Chrome	24.0+	Sí	El navegador elegido por Vicon Industries
Mozilla Firefox	20.0+	Sí	
Microsoft Internet Explorer	11	Sí	Nota: se requiere IE11 para ciertas integraciones de cámara.
Microsoft Internet Explorer	6.0 to 10	No	Sin compatibilidad con HTML5 moderno
Microsoft Edge	20.0+	Sí	Nota: algunos problemas con la navegación a la dirección localhost a través del nombre DNS. La dirección IP o el cliente remoto funcionan bien.
Apple Safari	6.0+ (Mac/iOS)	Sí	

Accediendo el Servidor

Una vez que se haya asegurado de tener un navegador compatible con el software VAX, acceder al software VAX es muy simple. Si está accediendo al servidor desde la PC en la que se instaló, se proporciona un enlace al menú de inicio; de lo contrario, deberá ingresar la dirección manualmente en su navegador web.

Acceso a VAX desde la PC en la que está instalado el software del servidor:

Durante la instalación, se coloca un acceso directo en su menú de inicio para VAX. El enlace para VAX se puede ubicar haciendo clic en Inicio -> Todos los programas -> VAX y finalmente haciendo clic en "Iniciar VAX."

Acceso a VAX desde una PC remota:

Abra su navegador web y dentro de la barra de direcciones ingrese la dirección del Servidor VAX usando el formato: **https://NombredeLacomputadora:11001**

Alternativamente, puede usar la dirección IP del servidor si el servidor está usando una dirección IP estática usando el formato: **https://192.168.1.100:11001**

Ejemplo 1.1. Acceder al servidor VAX de forma remota

https:// ComputerName: 11001 (el puerto predeterminado es 11001)



Una vez que haya ingresado la dirección, presione Entrar para navegar al software VAX

Preguntas frecuentes

P: ¿Por qué el navegador XXX no es compatible?

R: Los navegadores web, aunque similares en apariencia, difieren mucho en términos de características. Como mínimo, requerimos compatibilidad con HTML5 y muchos navegadores compatibles con estándares que no figuran en nuestra lista admitida funcionarán bien con nuestro software. Para brindar la mejor experiencia posible, proporcionamos un conjunto de navegadores recomendados. Los navegadores que no se mencionan en la lista recomendada pueden funcionar bien, pero en caso de que surjan problemas, solo brindamos asistencia técnica para los navegadores enumerados como admitidos..

P: ¿Necesito Windows 7 o posterior en el cliente?

R: No. Uno de los beneficios del software basado en web es la flexibilidad que ofrece para la conectividad. El software del cliente no está limitado por el sistema operativo sino por el navegador instalado en la máquina del cliente. Windows XP es generalmente la versión más antigua de Windows que recomendaríamos y las plataformas Mac y Mobile son totalmente compatibles siempre que se use un navegador web compatible.

P ¿Puedo acceder a VAX sin utilizar SSL (protocolo HTTPS)?

R: No. En aras de la seguridad, no admitimos conexiones sin cifrar.

P: Estoy usando un navegador no compatible y hay anomalías gráficas o problemas al intentar Usar el software VAX. ¿Cómo resuelvo?

R: Utilice un navegador compatible. No brindamos asistencia para ningún navegador que no aparezca como compatible. Sin embargo, si cree que sería beneficioso admitir un navegador que no está en nuestra lista admitida, nos encantaría saber de usted. Como mínima, siempre se requiere HTML5.

P: Uso Internet Explorer 10, que aparece como compatible, pero sigo experimentando anomalías gráficas o problemas con el software VAX. ¿Cómo resuelvo?

R: Internet Explorer tiene una función llamada Modo de compatibilidad que está habilitada de forma predeterminada para sitios de Intranet (no públicos). Para lograr la mejor experiencia en los navegadores Internet Explorer, recomendamos que esta función esté deshabilitada para nuestra aplicación.

Para deshabilitar el modo de compatibilidad en Internet Explorer 10, consulte los siguientes pasos:

1. Abra Internet Explorer y presione F12 para abrir las herramientas de desarrollo.
2. En la parte superior de la nueva ventana, verá dos listas desplegables, una etiquetada como 'Modo de navegador' y otra etiquetada como 'Modo de documento'. Asegúrese de que el modo de navegador sea IE10 (o superior) y el modo de documento sea el estándar IE10 (o superior).
3. En Internet Explorer 11, haga clic en el ícono de ajustes en la parte superior derecha de la ventana del navegador web.
4. Seleccione "Configuración de vista de compatibilidad".
5. Asegúrese de que la casilla de verificación "Mostrar sitios de intranet en Vista de compatibilidad" no esté seleccionada.

Capítulo 2. Actualización VAX

Este capítulo cubre el proceso de actualización del VAX, los requisitos previos para la actualización y cómo actualizar el firmware en los Paneles (los tableros de control de puertas y ascensores).

Actualizaciones del Software

Periódicamente, se lanzan actualizaciones a VAX para mejorar las funciones, corregir errores o mejorar la compatibilidad. VAX no ofrece paquetes de actualización por separado. Nuestro instalador independiente es capaz de instalar una nueva instancia de software o actualizar una instancia existente del software VAX. Todas las instancias con licencia de VAX tienen derecho a actualizaciones de software a medida que se lanzan.

Descargue la última versión de VAX

Visite nuestra página de descargas de VAX en:

<https://www.vicon-security.com/software-downloads-library/vax-access-control-software/>

Se le solicitarán las credenciales para descargar; por favor contacte a Vicon Industries para estos detalles.


Requisitos previos a la Instalación

Para actualizar VAX, se deberán cumplir los siguientes requisitos.

- La actualización debe realizarse desde la computadora en la que está instalado VAX actualmente.
- Debe iniciar sesión con el mismo inicio de sesión de Windows que instaló VAX (debido a los permisos de la base de datos).
- Si la actualización incluye una actualización de firmware para los paneles, el puerto UDP 9876 no debe bloquearse.

Actualización de instalación

El procedimiento para actualizar el software VAX es idéntico al de una instalación nueva. (Consulte la sección llamada "Procedimientos de instalación"). Recomendamos hacer una copia de seguridad de su base de datos VAX antes de actualizar. Para obtener más información sobre cómo realizar una copia de seguridad de su base de datos, consulte la sección correspondiente en la guía técnica principal. También recomendamos detener el servicio VAX a través de System Monitor antes de la instalación.

-  **Nota:** Durante la instalación, se recomienda que haga clic en "Avanzado" y se asegure de que la información, como la conexión a la base de datos, sea correcta.

Actualizaciones de firmware del panel

Periódicamente, cuando mejoramos VAX, se requerirán actualizaciones de firmware para sus paneles con las actualizaciones de software. Actualizar el firmware de un panel es un proceso relativamente sencillo.



Aviso:

Mientras está en modo de actualización de firmware, los paneles no funcionan. No responderán a las presentaciones de tarjetas, no generarán notificaciones y colocarán la Puerta en un estado de bloqueo. Para limitar el impacto que esto tiene en su sitio, sugerimos colocar solo 1 panel a la vez en el modo de actualización de firmware.

1. Cuando un Panel intenta conectarse a la aplicación VAX y se descubre que el firmware no está actualizado, verá un indicador en la parte inferior del panel de notificación en el lado derecho de la pantalla.

- Para que un Panel tenga su firmware actualizado debemos ponerlo en Modo de Actualización de Firmware. Para ello, navegaremos a la página de descripción general del sistema en el software. Haga clic en el cuadro "**x/x Paneles En línea**" arriba del área de Notificaciones o en el menú de navegación izquierdo, haga clic en Descripción general del sistema.

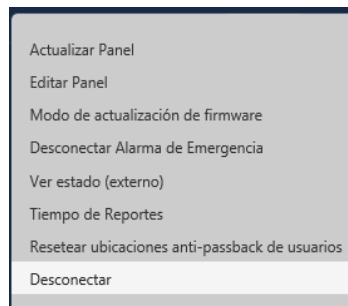


- En la Descripción general del sistema, verá una lista de todos los paneles en su sistema. Cualquier panel que requiera una actualización de firmware mostrará un estado Crítico y, si lo expande, la **Versión de firmware** mostrará Obsoleto.

Figura 2.1. Descripción general del sistema que muestra el mensaje de firmware desactualizado



- El siguiente paso es colocar sus paneles en el modo de actualización de firmware. Esto se puede lograr en la página de Descripción general del sistema.
 - En el lado derecho del Panel, haga clic en el icono de engranaje azul, que se muestra a continuación. Aparecerá un menú contextual.



- Seleccione 'Modo de actualización de firmware' en el menú contextual.
- El Panel ahora se desconectará e intentará actualizar su firmware.

 **Nota:** Puede realizar múltiples actualizaciones de firmware al mismo tiempo si es necesario.

- El servidor VAX aceptará las conexiones entrantes de los paneles en el modo de actualización de firmware en el puerto UDP 9876 y aplicará automáticamente el firmware más reciente para su panel. Una vez completado, el servidor indicará al Panel que se reinicie en modo normal, momento en el que el Panel reanudará el funcionamiento normal. Si el panel no se conecta al servidor en UDP 9876 dentro de los 60 segundos, el panel se reiniciará.

- Repita el proceso anterior en todos los paneles que indiquen que requieren una actualización de firmware. Después de que se haya actualizado el firmware de todos los Paneles, recomendamos actualizar todos sus Paneles. El icono de estado 'Modo de actualización' en el Tablero en el menú Dispositivos desaparecerá automáticamente, o puede actualizar la página.

Solución de problemas de actualización de firmware

El panel continúa mostrando el firmware desactualizado después de colocarlo en el modo de actualización de firmware. Si un Panel continúa mostrando que requiere una actualización de firmware después de colocar el panel en el modo de actualización de firmware y volver a estar en línea, asegúrese de que no haya ningún firewall de terceros que bloquee el puerto UDP 9876. Asegúrese de que no haya soluciones de firewall empresariales entre el servidor y el Panel en la red bloqueando el puerto UDP 9876.

El panel no vuelve a estar en línea después de pasar al modo de actualización de firmware. Si un panel no vuelve a estar en línea después de varios minutos, recomendamos verificar físicamente la pantalla LCD del panel.

- Si la pantalla LCD muestra el mensaje "Run Application Timeout", apague el panel desconectando el Cat5 del lado izquierdo de la placa. Mantenga presionado el botón con la etiqueta Enter (SW3) mientras conecta el cat5. Esto colocará el panel nuevamente en el modo de actualización de firmware.
- La pantalla LCD del panel mostrará la dirección del servidor actual desde la que desea actualizar su firmware. Si ve este conjunto como 192.168.2.10, podría indicar que tuvo un problema durante la actualización. Pruebe la sugerencia anterior o cambie la dirección IP del servidor VAX temporalmente a 192.168.2.10 con una máscara de subred 255.255.255.0.

Preguntas frecuentes

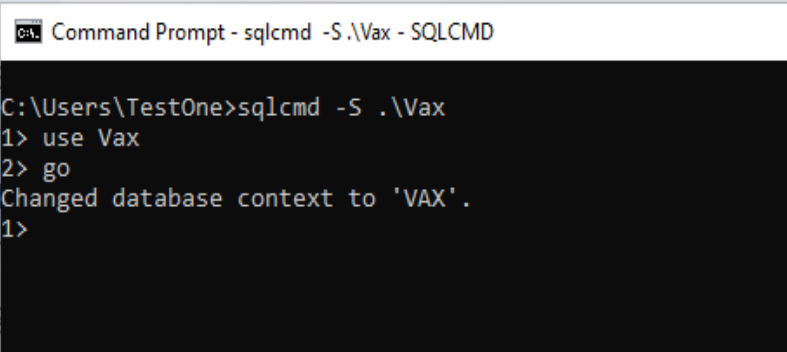
P: ¿Cómo puedo verificar si mi inicio de sesión de Windows puede actualizar VAX?

R: Para verificar si su cuenta tiene los permisos correctos, simplemente podemos hacer una conexión a la base de datos VAX y ver si se nos niega o se nos otorga el acceso. Esto puede requerir la asistencia del personal de TI o de Vicon Industries.

1. Abra una línea de comando con privilegios de administrador (haga clic con el botón derecho en cmd.exe, 'Ejecutar como administrador').
2. En la línea de comando, escriba: 'SQLCMD -S .\Vax' (su nombre de instancia puede ser diferente). Haga clic en 'ENTRAR'.
3. En el '1>', tipo 'USAR VAX' y prensa 'INGRESAR'.
4. En el '2>', tipo 'IR' y presione 'ENTRAR'.

Si ve el mensaje "Contexto de base de datos cambiado a 'VAX'", su cuenta de Windows tiene permiso para actualizar VAX.

Figura 2.2. Command Prompt: copia de seguridad



```
cmd Command Prompt - sqlcmd -S .\Vax - SQLCMD
C:\Users\TestOne>sqlcmd -S .\Vax
1> use Vax
2> go
Changed database context to 'VAX'.
1>
```

Si ve el mensaje "El servidor principal "computadora/usuario" no puede acceder a la base de datos "VAX" en el contexto de seguridad actual", su cuenta de Windows no tiene permiso para actualizar VAX.

P: Mi inicio de sesión de Windows no tiene permiso para actualizar VAX; ¿Cómo puedo saber qué cuenta tiene?

R: Debido a la forma en que funcionan los permisos de la base de datos SQL, cuando VAX se instala inicialmente, el inicio de sesión de Windows que instala el software obtiene un permiso implícito para acceder a la base de datos. Probablemente (pero no siempre), podemos encontrar este nombre de cuenta de usuario comprobando un archivo de registro generado por el instalador de MS SQL.

1. Navegar a su instalación directorio de sql servidor (generalmente situado en "C:\Programa archivos\Microsoft sql Servidor
2. Usar el buscar bar a buscar todo carpetas para a archivo llamado "sql_common_core_Cpu64_1.log" o "sql_common_core_Cpu32_1.log". Abra el archivo en el bloc de notas.
3. Una vez que haya abierto el archivo, use la función 'buscar' y busque la cadena "apdata". El primer resultado debería mostrar la ruta al directorio de usuario del inicio de sesión de Windows correcto.

Si el inicio de sesión de Windows no está disponible o ya no existe, comuníquese con Vicon Industries.

Capítulo 3. Configuración inicial

Este capítulo cubrirá la configuración inicial de los elementos de software y hardware de VAX. Esto incluye la configuración inicial del software, la configuración inicial de los Paneles y cómo asociar un Panel con VAX.

Configuración inicial del software

Esta sección cubrirá la configuración inicial de su sistema de control de acceso. Esto es simplemente una cuestión de proporcionar al software VAX suficiente información para que construya su base de datos inicial.

Acceda al servidor VAX a través del navegador HTML5 de su elección. (Para obtener más información sobre cómo acceder al servidor, consulte la sección llamada "Acceso al servidor".) Una vez que su navegador llegue al servidor, es posible que vea una ventana emergente que indica que la conexión al servidor es 'No confiable' o 'No privada'.

Debido a la naturaleza dinámica de nuestro software, no podemos crear un Certificado firmado con una Autoridad de certificación. Las comunicaciones con el servidor están encriptadas con SSL de 128 bits. En Google Chrome, haga clic en 'Avanzado' y 'continuar con...'. En otros navegadores, haga clic en 'Continuar de todos modos' o 'Agregar excepción' (dependiendo de su navegador).

Una vez que llegue al servidor y pase las advertencias del navegador, se le presentará una pantalla de bienvenida, seguida del asistente de configuración inicial. Se divide en cuatro pasos: EULA, configuración del cliente, dirección del servidor y administrador inicial.

EULA

1. Lea el Acuerdo de licencia de usuario final y luego marque la casilla de verificación **Acepto el Acuerdo de licencia de usuario final** en la parte inferior.
2. Haga clic en el botón Siguiente en la parte inferior derecha de la página.

Configuración del cliente

1. Ingrese un Nombre para el cliente y establezca la Zona horaria del sitio inicial del sistema.
2. Opcionalmente, ingrese información sobre el distribuidor que administra el sistema para que el usuario final pueda comunicarse fácilmente para obtener asistencia.
3. Opcionalmente, ingrese la configuración de correo electrónico para habilitar el restablecimiento de contraseña y las notificaciones por correo electrónico y las alertas del sistema.
4. Haga clic en el botón Siguiente en la parte inferior derecha de la página.

Figura 3.1. Configuración del cliente

Configuración del cliente	
Nombre	Vicon Demo
Descripción	Descripción Opcional
Número de cuenta	1060
Nombre del Integrador	Nombre del Integrador
Número de teléfono del distribuidor	XXXXXXXXXX
Sitio web del distribuidor	URL del sitio web
Email del distribuidor	Integrador@Email.Com

Tabla 3.1. Campos de configuración del cliente

Campo	Breve descripción
Nombre	Este es el nombre del host, el cliente o el nombre de la empresa (no un sitio específico).
Descripción	Una descripción opcional del anfitrión, cliente o empresa.
Zona horaria del sitio inicial	Esta es la zona horaria principal en la que opera su primer sitio. Posteriormente se pueden agregar sitios adicionales con diferentes zonas horarias.

Información del integrador

Figura 3.2. Información del integrador

 **Nota:** La información del integrador es opcional, pero se recomienda.

Figura 3.2. Información del integrador

Campo	Breve descripción
Nombre del integrador	Este es el nombre del integrador que instala el sistema y/o responsable de brindar soporte al usuario final del sistema.
Número de teléfono del integrador	Este es el número de teléfono de contacto principal del integrador que instala el sistema y/o responsable de brindar soporte al usuario final del sistema. Sin guiones entre las secciones del número (p. ej.: 800-348-4266)
Sitio web del integrador	Esta es la dirección del sitio web del integrador que instala el sistema y/o responsable de brindar soporte al usuario final del sistema. Introduzca la URL completa del sitio web del distribuidor. Ejemplo: https://www.vicon-security.com
Correo electrónico del integrador	Esta es la dirección de correo electrónico de contacto principal del integrador que instala el sistema y/o responsable de brindar asistencia al usuario final del sistema

Configuración del Correo Electrónico

Figura 3.3. Ajustes del correo electrónico

Configuración de correo electrónico

Servidor SMTP: Requerido si usa SMTP

Puerto del servidor SMTP: 25

Requiere SSL:

Dirección de respuesta: usuario@email.com

Nombre de Usuario: Opcional

Contraseña: Contraseña SMTP

Enviar test al Guardar:

- **Nota:** La configuración del correo electrónico es opcional, pero se recomienda. Estos pueden usarse para recuperar una contraseña olvidada y para recibir correos electrónicos de notificación.

Tabla 3.3. Configuración de correo electrónico Campos

Campo	Breve descripción
Servidor SMTP	Este es el nombre del servidor SMTP requerido para enviar correos electrónicos (por ejemplo: mail.ISPdomain.com).
Puerto del servidor SMTP	Este es el puerto utilizado para enviar correos electrónicos a través de SMTP (el puerto 25 es común, sin embargo, su configuración puede variar).
Requiere SSL	Marque la casilla de verificación Secure Socket Layer si su cliente de correo electrónico requiere y usa SSL para cifrar mensajes de correo electrónico.
Dirección de respuesta	Esta es la dirección de correo electrónico desde la que se enviarán las notificaciones y la recuperación de correo electrónico. Puede ser la misma que la dirección de correo electrónico del remitente.
Nombre de usuario	Este es el nombre de usuario necesario para autenticar y enviar correos electrónicos a través de SMTP.
Contraseña	Esta es la contraseña necesaria para la autenticación y el envío de correo electrónico a través de SMTP.

Dirección del Servidor

Figura 3.4. Reestablecer Dirección del servidor

Server Address

How to Choose

- If all panels are on the same network as the server, select Ethernet Adapter or Computer Name.
- If panels are connecting over the internet, select Public IP Address
- If you're using a domain name or dynamic DNS, select DNS Name

Type	Address
<input checked="" type="radio"/> Ethernet	192.168.2.139
<input type="radio"/> Loopback Pseudo-Interface 1	127.0.0.1
<input type="radio"/> Public IP Address	209.91.167.223
<input type="radio"/> Computer Name	TESTONE
<input type="radio"/> DNS Name	TESTONE

* Server Address field can be changed later under System Settings.

Los paneles VAX inician la conexión con el servidor y, por lo tanto, deben configurarse con la dirección para llegar al servidor. Cuando a un panel se le envía nueva configuración, es decir se le actualizan sus tablas, se le envía esta dirección de servidor. Esta configuración dependerá de en qué parte de la red se encuentren los paneles en relación con el servidor.

1. Revise las opciones que se muestran en la siguiente tabla y seleccione la opción que mejor describa el diseño de su red.
2. Haga clic en el botón **Siguiente** en la parte inferior derecha de la página.

Tabla 3.4. Tipos de direcciones de servidor

Campo	Breve descripción
Adaptador de Ethernet	Cada adaptador de red que tenga una dirección IPv4 se mostrará en la tabla. Si los paneles están en la misma red local que el adaptador, seleccione esta opción. Nota: puede mostrar una advertencia de que DHCP está habilitado cuando se selecciona, si es así, recomendamos usar el nombre de la computadora, configurar una IP estática o una reserva de DHCP para garantizar que la dirección IP no cambie.
Dirección IP pública	Esta es la dirección IP pública de la puerta de enlace predeterminada del servidor, si corresponde. Si los paneles se conectan a través de Internet al servidor, seleccione esta opción. Nota: La conexión de paneles a través de Internet generalmente requerirá el reenvío de puertos en el enrutador. Además, dependiendo de su proveedor de Internet, su dirección IP pública puede ser dinámica y podría cambiar. Si ha determinado que su dirección IP pública es dinámica, le recomendamos que utilice un servicio de DNS dinámico y seleccione la opción Personalizada.
Nombre de la computadora	Por defecto, se instaló el nombre de la PC VAX. Los paneles en la misma red local que el servidor pueden resolver el nombre de la computadora usando la resolución DNS o NetBIOS. Recomendamos esta opción si la PC está usando DHCP para obtener una dirección IP.
Personalizado	Puede ingresar una dirección IPv4 o DNS personalizada para que los paneles la usen para conectarse al servidor. Seleccione esta opción si tiene su propia dirección DNS que se resuelve en el servidor o está utilizando un servicio de DNS dinámico.

Administrator

Figura 3.5. Administrador inicial

1. Introduzca una **dirección de correo electrónico, un nombre, un apellido y una contraseña** para el administrador del sistema inicial.

2. Una vez configurados todos los campos, haga clic en Crear cliente para continuar.

Tabla 3.5. Campos iniciales del administrador

Campo	Breve descripción
Dirección de correo electrónico	Esta es la dirección de correo electrónico/nombre de usuario del administrador principal de VAX. Esta dirección de correo electrónico se utilizará para iniciar sesión en el sitio inicialmente.
Nombre de usuario	De manera predeterminada, este campo se completará con la dirección de correo electrónico establecida arriba. Sin embargo, puede cambiar el nombre de usuario a algo que no sea el correo electrónico. Debe tener entre 5 y 255 caracteres.
Nombre de pila	El primer nombre del administrador principal de VAX. Acepta de 2 a 64 caracteres y no puede contener caracteres especiales.
Apellido	El apellido del administrador principal de VAX. Acepta de 2 a 64 caracteres y no puede contener caracteres especiales.
Idioma	El idioma que se muestra en la interfaz de usuario y de los mensajes enviados al administrador principal de VAX. Esto se establece por administrador.
Contraseña	Introduzca y confirme la contraseña que utilizará el administrador principal. Acepta de 6 a 16 caracteres. Esto se puede cambiar en un momento posterior.

Si todo lo que ingresó fue válido, VAX creará y configurará automáticamente su base de datos para su uso.

¡Felicidades! Ahora está listo para comenzar a configurar su sistema de control de acceso. Ahora podemos pasar a configurar los paneles para comunicarse con el servidor.

Inicio de sesión en la interfaz web de VAX

Una vez que haya completado la configuración inicial, o el sistema haya sido preconfigurado para usted, ahora puede iniciar sesión en la interfaz web de VAX.

En la página de inicio de sesión, ingrese la dirección de correo electrónico y la contraseña que ingresó en la página de configuración inicial o el correo electrónico y la contraseña que le proporcionó el instalador del sistema. Haga clic en el botón Iniciar sesión en esta pantalla. Ahora será llevado a la página de inicio de la interfaz web de VAX.

Figura 3.6. Inicio de sesión de VAX



Recuperación de contraseña en VAX

En caso de que no pueda recordar o extravié su contraseña para iniciar sesión en VAX, puede pasar por el proceso de recuperación de contraseña haciendo clic en el botón azul Restablecer contraseña en la parte inferior de la página.

Advertencia

Debido a la naturaleza de alta seguridad de este producto, las contraseñas solo se pueden restablecer si la configuración de correo electrónico se ha programado en el software. Si no se ha programado, póngase en contacto con Vicon Industries – más información en el Capítulo 37 Apoyo.

Para obtener información sobre la configuración de correo electrónico para usar con alertas de correo electrónico y recuperación de contraseña, consulte la sección llamada "Configuración de correo electrónico".

En la página Restablecer contraseña, complete el correo electrónico de la cuenta de administrador para la que desea restablecer la contraseña. Haga clic en el botón Solicitar reinicio. Si la configuración del correo electrónico es correcta, recibirá un código de confirmación por correo electrónico en el correo electrónico del administrador proporcionado. Ingrese este código en el campo Código de confirmación e ingrese su nueva contraseña. Haga clic en Confirmar reinicio; ahora volverá a la página de inicio de sesión.

Restablecer la contraseña

Nombre de Usuario

Volver a Iniciar sesión Restablecer Solicitud

Restablecer confirmación de contraseña

Nombre de Usuario

Código de confirmación

Contraseña

Confirmar contraseña

Volver a Iniciar sesión Confirmar Reinicio

Configuración inicial del panel

Esta sección cubrirá la configuración inicial común de VAX PoE y controladores de puerta, elevador y entrada/salida con alimentación de 12 VDC. Esta sección se enfoca en configurar la información de comunicación manualmente en el Panel para que pueda conectarse al software del servidor VAX. El aspecto del software para configurar un panel entrará en más detalles en el Capítulo 7, Configuración de su panel.

Este aspecto de la configuración requiere que el software VAX esté instalado en una PC o servidor con la Configuración inicial completada con un nombre de cuenta de correo electrónico asignado y una contraseña válida. Nos referiremos a la PC con VAX instalado como el Servidor VAX. Anote la dirección IP o el nombre del servidor VAX; esto es necesario durante la configuración del panel.

Todavía se puede acceder a los diagnósticos incorporados, incluso cuando el servidor no está disponible o aún no está instalado.

Desde una perspectiva de hardware, los paneles con alimentación VAX PoE deben montarse en su ubicación prevista o ser accesibles físicamente de forma temporal cerca del servidor VAX con un cable Cat5e/6 (no cruzado) conectado directamente a un inyector PoE o a un conmutador de red alimentado (Nota: El recorrido máximo del cable desde el VAX VAX-1D-1 hasta el inyector o el interruptor alimentado es de 100 metros o 330 pies). En el caso de un controlador con alimentación de 12 VDC, como los paneles VAX-MDK, se debe enchufar una alimentación de 12 a 13,5 VDC y el Cat5 se debe conectar a una red que pueda llegar al servidor VAX localmente o a través de Internet.

⚠ Advertencia

Si está a punto de realizar una instalación del Panel, le recomendamos que lea el Capítulo 6, Planificación de una implementación de control de acceso junto con este capítulo en su totalidad antes de la configuración.

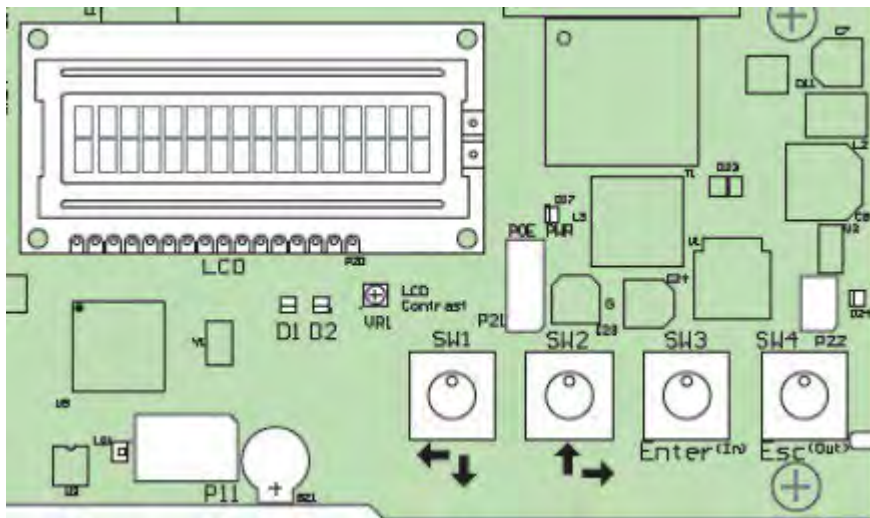
Información para recopilar antes de la configuración

- La IP estática o el nombre del servidor del servidor VAX.
- ¿Usará este panel DHCP o una dirección estática para la dirección IP? Si es estático, ¿qué IP, subred, puerta de enlace y DNS se deben usar?
 - ¿El personal de TI en la ubicación está al tanto de los nuevos dispositivos que se agregan a la red (si corresponde)?

Navegación por la interfaz del panel

Hay 4 botones ubicados en la esquina inferior derecha de un controlador VAX para acceder, ver y configurar un Panel.

Figura 3.8. Botones del panel (mismo diseño de botones en paneles alimentados por PoE y 12 VDC)



Los dos botones blancos (SW1 y SW2) se usan para moverse hacia arriba y hacia abajo a través de los menús cuando no se está editando un elemento específico. Y para moverse hacia la izquierda y hacia la derecha sobre los datos de valor cuando se está editando un elemento específico del menú.

Los dos botones negros (SW3 = Enter, SW4 = Esc) se utilizan para seleccionar un elemento del menú, colocar un valor particular en modo de edición y no edición, guardar o cancelar cambios y guardar cambios en la memoria.

El estado predeterminado del panel es un menú desplegable que muestra lo siguiente:

- Estado(s) de la puerta
- Horario de puerta
- Nombre de red
- Nombre del panel y asociación del sitio
- Fecha y hora
- Modo de conexión del servidor
- Modo de comunicación del panel

Nota: Puede presionar la tecla Enter (SW3) mientras está en el menú predeterminado para pausar el desplazamiento y hacer que permanezca en el mismo elemento.

Para ver rápidamente cómo está configurado actualmente el Panel (SOLO LECTURA), mantenga presionado el botón ESC (SW4) durante 4 segundos o hasta que el Panel emita dos pitidos. Ahora puede usar los

botones de navegación (SW1 y SW2) para ver la configuración actual.

Tabla 3.6. Vista de configuración de solo lectura

01 Nombre del panel	02 Nombre del área
03 Identificación del dispositivo del panel	04 Modo de funcionamiento del panel
05 Dirección de panel predeterminada	06 Dirección IP real
07 Dirección MAC del panel	08 Máscara de subred del panel
09 Puerta de enlace del panel	DNS de 10 paneles
11 Modo de comunicación del panel	12 Dirección IP del servidor
13 Nombre del servidor	14 Puerto del servidor
15 Modo de conexión del servidor	16 Versión de firmware
17 Modo de servidor HTTP	

Algunos de los campos más importantes/útiles para tener en cuenta son los siguientes:

07 Dirección MAC del Panel: Esta es la dirección MAC del Panel. Anote la dirección para cuando agregue el Panel a VAX o si el personal de TI lo necesita para la seguridad del puerto.

06 Dirección IP real: De manera predeterminada, el Panel intentará usar DHCP para obtener una dirección IP; si tiene éxito, esta dirección estará aquí. Puede usar esta dirección para acceder a la página de configuración web del panel; sin embargo, esta dirección podría cambiar según la configuración del servidor DHCP.

15 Modo de conexión del servidor: este campo muestra el método de conexión que el panel intenta usar para comunicarse con el servidor (dirección IP o nombre del servidor).

Configuración del modo de comunicación: IP del servidor

Esta sección cubre cómo configurar el Panel para comunicarse con la dirección IP estática del servidor VAX.

Nota: La comunicación entre el Panel y el servidor solo puede ocurrir cuando ambos lados tienen direcciones IP válidas. De manera predeterminada, el Panel intentará obtener una dirección a través de DHCP. Si el Panel necesita tener una IP estática configurada manualmente, consulte la sección llamada "Configuración de IP del Panel: IP Estática".

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca '¿CONFIGURAR CONTRASEÑA?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED (acceso Concedido)'. Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'SERVER CONN MODE' y luego presione el botón

Configuración inicial

ENTER. Esta configuración define el modo de comunicación del servidor (Modo de conexión del servidor deletreado debido a limitaciones de espacio de caracteres).



4. Ahora, en la pantalla SERVER CONN MODE ', presione los botones blancos hacia arriba o hacia abajo hasta que la flecha en la pantalla LCD indique que se ha seleccionado '1: IP del servidor' y presione el botón ESC.



5. Se le presentará un mensaje que dice ' CHANGE CONFIRM?' y tiene dos opciones: Sí presionando el botón ENTER o NO presionando el botón ESC. Si desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NO CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, el proceso de cambio expirará y deberá iniciarlo nuevamente).



6. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD a 'SERVER IP ADDR' y luego presione el botón ENTER.



7. Usando los botones blancos para el movimiento hacia la izquierda y hacia la derecha, así como para cambiar los valores numéricos para cada posición de la dirección IP del servidor y usando el botón ENTER para cambiar entre el modo EDIT (posición parpadeando entre el valor y negro sólido) y el modo VIEW (posición parpadeando entre valor y en blanco), ingrese la dirección IP completa del servidor.



8. Con la dirección IP completa completada en la pantalla LCD, asegúrese de estar en el modo VER (indicado por el valor posicional que parpadea entre el valor y el espacio en blanco) y luego presione el botón ESC.
9. Aparecerá un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: Sí presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NO CHANGED'. Nota: si no se realiza ninguna selección en 20 segundos, el proceso de cambio se agotará y tendrá que iniciarlo de nuevo)



10. Presione ESC una vez más para guardar la configuración en la memoria flash. Se le presentará con 'Setup Saved'.



Configuración del modo de comunicación: Nombre del Servidor (DNS)

Esta sección cubre cómo configurar el Panel para comunicarse con el servidor a través del nombre DNS. Esto es útil cuando el servidor VAX está en una computadora portátil o no puede tener una IP estática. El Panel utilizará un servidor DNS local para traducir el Nombre del servidor a la IP del servidor que está utilizando actualmente. Aconsejamos a nuestros distribuidores/clientes que sean conscientes de que los enrutadores domésticos se pueden usar como un servidor DNS, pero a menudo funcionan mal o solo actúan como repetidores DNS, lo que no funcionará con nuestros paneles.

Nota: La comunicación entre el Panel y el servidor solo puede ocurrir cuando ambos lados tienen direcciones IP válidas. De manera predeterminada, el Panel intentará obtener una dirección a través de DHCP. Si el Panel necesita tener una IP estática configurada manualmente, consulte la sección llamada "Configuración de IP del Panel: IP Estática"

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique "ACCESS GRANTED". Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'SERVER CONN MODE' y luego presione el botón ENTER. Esta configuración define el modo de comunicación del servidor (Modo de conexión del servidor deletreado debido a limitaciones de espacio de caracteres).



4. Ahora, en la pantalla 'SERVER CONN MODE' presione los botones blancos hacia arriba o hacia abajo hasta que la flecha en la pantalla LCD indique que se ha seleccionado '2: nombre del servidor' y presione el botón ESC.

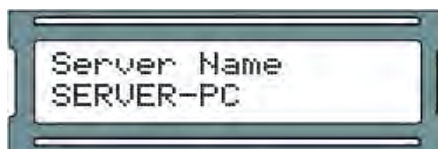
Configuración inicial



5. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice y establezca la flecha indicadora en la pantalla LCD en 'Nombre del servidor' y luego presione el botón ENTER.



6. Usando los botones blancos para el movimiento hacia la izquierda y hacia la derecha, así como para cambiar los valores alfabéticos, numéricos y de símbolos para cada posición del nombre del servidor y usando el botón ENTER para cambiar entre el modo EDIT (posición parpadeando entre el valor y negro sólido) y Modo VER (posición parpadeando entre valor y en blanco), ingrese el nombre completo del servidor (hasta 16 caracteres).




7. Con el nombre completo del servidor completado en la pantalla LCD, asegúrese de estar en el modo VER (indicado por el valor posicional que parpadea entre el valor y el espacio en blanco) y luego presione el botón ESC.
8. Se le presentará un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: Sí presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, el proceso de cambio se agotará y tendrá que iniciarlo de nuevo.)



9. Presione ESC una vez más para guardar la configuración en la memoria flash. Se le presentará con 'Configuración guardada'



 **Nota:** A menudo es más fácil hacer la conexión inicial con la IP del servidor y luego cambiar el modo de conexión a Nombre del servidor desde la configuración de Configuración del sistema titulada Dirección del servidor en la interfaz web de VAX.

Configuración de IP del panel: DHCP

Esta sección cubre cómo configurar el Panel para obtener una dirección IP automáticamente usando DHCP. Esta es la configuración predeterminada con la que se envía el panel.

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado)



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice y configure la flecha indicadora en la pantalla LCD en 'Panel Comm mode' y luego presione el botón ENTER.



4. Ahora, en la pantalla 'Panel Comm mode', presione los botones blancos hacia arriba o hacia abajo hasta que la flecha en la pantalla LCD indique que '1: DHCP client' está seleccionado y presione el botón ESC.



5. Aparecerá un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: YES via pressing the ENTER button or NO via pressing the ESC button.

Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, se agotará el tiempo de espera del proceso de cambio y tendrá que volver a iniciarlo).



6. Presione ESC una vez más para guardar la configuración en la memoria flash. Se le presentará con 'Setup Saved'.



Configuración de IP del panel: IP estática

Esta sección cubre cómo configurar el Panel con una IP estática. Esto se usa cuando un servidor DHCP no está disponible o el personal de TI ya ha designado una IP para el Panel.

Necesitará la siguiente información (del personal de TI o equivalente) antes de configurar una dirección estática:

- Dirección IP del Panel.
- Máscara de subred asociada a la IP del Panel.
- Puerta de enlace predeterminada (solo aplicable si viaja a través de WAN o enlaces de Internet al servidor).

Una vez que tenga esta información, use los siguientes pasos para asignar una dirección IP estática en el panel.

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice y configure la flecha indicadora en la pantalla LCD en 'Panel Comm mode' y luego presione el botón ENTER.



4. Ahora, en la pantalla 'Panel Comm mode', presione los botones blancos hacia arriba o hacia abajo hasta que la flecha en la pantalla LCD indique '0: Static IP' y presione el botón ESC.



5. Se le presentará un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: Sí presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica ' CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, el proceso de cambio expirará y tendrá que iniciarlo de nuevo.)



Configuración inicial

- Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'Panel IP Addr' y luego presione el botón ENTER.



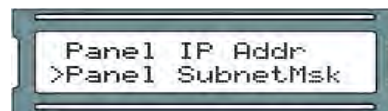
- Usando los botones blancos para el movimiento hacia la izquierda y hacia la derecha, así como para cambiar los valores numéricos para cada posición de la dirección IP del Panel y usando el botón ENTER para cambiar entre el modo EDIT (posición parpadeando entre el valor y negro sólido) y el modo VIEW (posición parpadeando entre el valor y en blanco), ingrese la dirección IP completa del Panel.



- Con la dirección IP completa completada en la pantalla LCD, asegúrese de estar en el modo VIEW (indicado por el valor posicional que parpadea entre el valor y el espacio en blanco) y luego presione el botón ESC.
- Aparecerá un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: YES presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, se agotará el tiempo de espera del proceso de cambio y tendrá que volver a iniciarlo).



- Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'Panel Subnetmsk' y luego presione el botón ENTER.



- Usando los botones blancos para el movimiento hacia la izquierda y hacia la derecha, así como para cambiar los valores numéricos para cada posición de la máscara de subred del panel y usando el botón ENTER para cambiar entre el modo EDIT (posición parpadeando entre el valor y negro sólido) y el modo VIEW (posición parpadeando entre el valor y en blanco), ingrese la máscara de subred completa del Panel.



- Con la máscara de subred completa completada en la pantalla LCD, asegúrese de estar en el modo VIEW (indicado por el valor posicional parpadeando entre el valor y el espacio en blanco) y luego presione el botón ESC.
- Aparecerá un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: YES presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón

Configuración inicial

ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, se agotará el tiempo de espera del proceso de cambio y tendrá que volver a iniciarlo.)



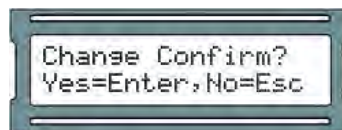
- Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD a 'Panel Gateway' y luego presione el botón ENTER.



- Usar los botones blancos para el movimiento hacia la izquierda y hacia la derecha, así como usarlos para cambiar los valores numéricos para cada posición de la puerta de enlace del Panel y usar el botón ENTER para cambiar entre el modo EDIT (posición parpadeando entre el valor y negro sólido) y el modo VIEW (posición parpadeando entre el valor y en blanco), ingrese la puerta de enlace completa del Panel.



- Con la puerta de enlace del panel completo completada en la pantalla LCD, asegúrese de estar en el modo VER (indicado por el valor posicional que parpadea entre el valor y el espacio en blanco) y luego presione el botón ESC.
- Aparecerá un mensaje que dice 'CHANGE CONFIRM?' y tiene dos opciones: YES presionando el botón ENTER o NO presionando el botón ESC. Si la dirección IP del servidor es correcta y desea confirmar esa configuración en el panel, presione el botón ENTER. Ahora se le presentará un mensaje que indica 'CHANGED'. Presionar el botón ESC cancelará la operación y presentará un mensaje que indica 'NOT CHANGED'. (Nota: si no se realiza ninguna selección en 20 segundos, se agotará el tiempo de espera del proceso de cambio y tendrá que volver a iniciarlo)



- Presione ESC una vez más para guardar la configuración en la memoria flash. Se le presentará con 'Setup Saved'



Restablecer un Panel

Esta sección cubrirá cómo restablecer un panel a un estado predeterminado. Si en algún momento necesita restablecer el Panel a los valores predeterminados de fábrica, consulte estos pasos:

- Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



- Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. ((Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado)



- Usando los botones blancos hacia arriba y hacia abajo en el panel, ubique y configure la flecha indicadora en la pantalla LCD para 'Erase Flash Mem' y luego presione el botón ENTER.



- parecerá un mensaje que dice 'Erase Flash Mem?' y tiene dos opciones: Sí presionando el botón ENTER o NO presionando el botón ESC.



- Aparecerá brevemente un mensaje que indica 'ERASING FLASH' seguido por 'ERASED' y luego la pantalla LCD regresará a la pantalla 'ERASE FLASH MEM' . (Nota: el proceso de borrado expirará si no hay actividad dentro de los 60 segundos.)
- El Panel ahora se reiniciará y ahora estará en un estado predeterminado. Ya puede configurar el Panel.

Prueba para Entradas / Salidas en la Puerta

Esta sección cubre los métodos que los técnicos pueden usar para probar el panel una vez que se ha montado en la puerta.

Tabla 3.7. Prueba en la puerta

Nombre de la prueba	Descripción/uso común
Prueba de salida	Se usa para probar los 3 relés de salida, generalmente se usa para verificar si la cerradura de la puerta se conectó correctamente.
Prueba de entrada	Se usa para probar las 4 entradas, generalmente se usa para verificar si el contacto de la puerta y/o el botón de salida estaban correctamente cableados.
Prueba de lector	Se usa para probar los 2 puertos del Lector, generalmente se usa para verificar si el Lector se conectó correctamente y para verificar el formato de bits de las tarjetas.

Prueba de salida (modelos PoE)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de salida en controladores de puerta alimentados por PoE

- Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4

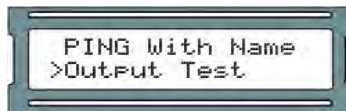
segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado)



3. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la flecha indicadora en la pantalla LCD en 'Output Test' y luego presione el botón ENTER.



4. Presione los botones blancos hacia arriba o hacia abajo para mover el cursor sobre la salida que desea probar. Presione ENTER y el cero resaltado cambiará a 1, y se activará la salida. Presione ENTER nuevamente para desactivar la salida. Cuando haya terminado de probar, presione el botón ESC.



5. Después de presionar ESC, verá un mensaje que dice 'Cancelado'. Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales.



Prueba de Salida (VAX-MDK)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de salida en controladores de puerta, ascensor o E/S alimentados con 12 VDC.

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.

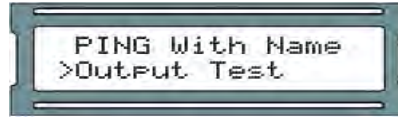


2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado)



3. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la

flecha indicadora en la pantalla LCD en 'Output Test' y luego presione el botón ENTER.



4. En los modelos con alimentación de 12 VDC, deberá seleccionar un tipo de placa. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique la opción que mejor se adapte a lo que necesita y presione el botón Enter. Estas opciones se describen a continuación:



Tabla 3.8. Categorías de acción

Opción de menú	Descripción
1: Use Preset DB	La prueba de salida detectará automáticamente qué tipo de placa está configurada en función de la configuración actual de la base de datos.
2: PRS_IO8	Seleccione esta opción si las tarjetas de expansión conectadas son expansores de E/S (VAX-IO-EXP8-PCB).
3: PRS_TDM	Seleccione esta opción si las tarjetas de expansión conectadas son de dos puertas (VAX-EXP-2D).
4: PRS_IO8_All	Esta opción le permitirá probar relés en varios expansores de E/S a la vez (VAX-IO-EXP8-PCB).
5: PRS_TDM_All	Esta opción le permitirá probar relés en múltiples expansores de dos puertas (VAX-EXP-2D).

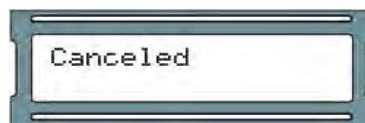
5. Después de seleccionar un tipo de tablero, ahora elegirá una dirección de tablero. Las direcciones admitidas actualmente son 1-4 para expansores VAX-EXP-2D y 1-8 para expansores VAX-IO-EXP8-PCB. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice la dirección del expansor que desea probar y presione el botón Enter.



6. Presione los botones blancos hacia arriba o hacia abajo para mover el cursor sobre la salida que desea probar. Presione ENTER y el cero resaltado cambiará a 1, y se activará la salida. Presione ENTER nuevamente para desactivar la salida. Cuando haya terminado de probar, presione el botón ESC.



7. Después de presionar ESC, verá un mensaje que dice 'Canceled'. Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales.



Prueba de entrada (modelos PoE VAX-1D-1)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de entrada en controladores de puerta alimentados por PoE.

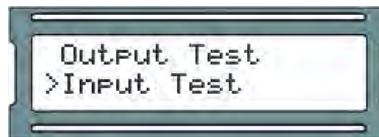
1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.)



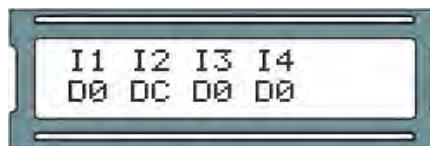
3. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la flecha indicadora en la pantalla LCD en "Input Test" y luego presione el botón ENTER.



4. Se le mostrará brevemente una leyenda sobre los estados de entrada.



5. Si tiene algún dispositivo de entrada, como contactos de puerta o dispositivos REX, el panel emitirá un pitido y le mostrará qué entradas están activas. Las entradas inactivas son 'DO' y las entradas activas son 'DC'. Si está probando un contacto de puerta, abra y cierre la puerta y controle el cambio de entrada. Cuando haya terminado de probar, presione el botón ESC.



6. Después de presionar ESC, verá un mensaje que dice "Cancelado". Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales.



Prueba de Entrada (modelos VAX-MDK)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de entrada en controladores de puerta, ascensor o E/S alimentados con 12 VDC.

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.

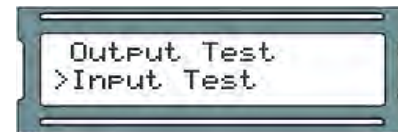
Configuración inicial



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.)



3. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la flecha indicadora en la pantalla LCD en "Input Test" y luego presione el botón ENTER.



4. En los controladores con alimentación de 12 VDC, deberá seleccionar un tipo de placa. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique la opción que mejor se adapte a lo que necesita y presione el botón Enter. Estas opciones se describen a continuación:



Tabla 3.9. Categorías de acción

Opción de menú	Descripción
1: Use Preset DB	La prueba de entrada detectará automáticamente qué tipo de placa está configurada según la configuración actual de la base de datos.
2: PRS_IO8	Seleccione esta opción si las tarjetas de expansión conectadas son expansores de E/S (VAX-IO-EXP8-PCB).
3: PRS_TDM	Seleccione esta opción si las tarjetas de expansión conectadas son de dos puertas (VAX-EXP-2D).

5. Después de seleccionar un tipo de tablero, ahora elegirá una dirección de tablero. Las direcciones admitidas actualmente son 1-4 para expansores VAX-EXP-2D y 1-8 para expansores VAX-IO-EXP8-PCB. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice la dirección del expansor que desea probar y presione el botón Enter.



6. Se le mostrará brevemente una leyenda sobre los estados de entrada.



7. Si tiene algún dispositivo de entrada, como contactos de puerta o dispositivos REX, el panel emitirá un pitido y le mostrará qué entradas están activas. Las entradas inactivas son 'Do' y las entradas activas son 'Dc'. Si está probando un contacto de puerta, abra y cierre la puerta y controle el cambio de entrada. Cuando haya terminado de probar, presione el botón ESC.



- Después de presionar ESC, verá un mensaje que dice "Canceled". Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales..



Prueba de lector (modelo PoE VAX-1D-1)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de Reader en controladores de puerta alimentados por PoE.

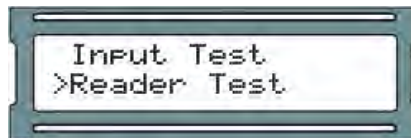
- Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



- Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.)



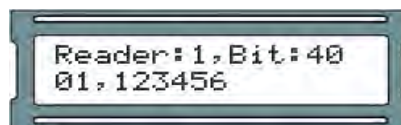
- Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la flecha indicadora en la pantalla LCD en "Reader Test" y luego presione el botón ENTER.



- Se le mostrará una pantalla que dice 'No Card Input'. Ahora puede presentar una tarjeta de proximidad o fob a uno de los Lectores adjuntos.



- Si el Lector está cableado correctamente y se presenta una tarjeta de 40 o 26 bits, verá información sobre la tarjeta y el Lector en la pantalla. Si está utilizando un segundo Reader, puede realizar la prueba en ese Reader de la misma manera. Cuando haya terminado de probar, presione el botón ESC.



- Después de presionar ESC, verá un mensaje que dice "Canceled". Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales.



Prueba de Lector (Modelos VAX-MDK)

Esta sección incluye instrucciones detalladas sobre cómo realizar una prueba de Reader en controladores de ascensores y puertas alimentados con 12 VDC.

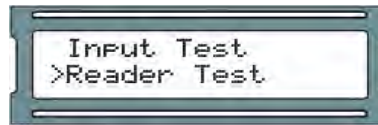
1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca 'SETUP PASSWORD?' en la pantalla LCD y '0000'.



2. Presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESS GRANTED'. (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado.)



3. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice y configure la flecha indicadora en la pantalla LCD en 'Prueba de lector' y luego presione el botón ENTER.



4. En los controladores con alimentación de 12 VDC, deberá seleccionar un tipo de placa. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique la opción que mejor se adapte a lo que necesita y presione el botón Enter. Estas opciones se describen a continuación:



Tabla 3.10. Categorías de acción

Opción de menú	Descripción
1: Use Preset DB	La prueba de entrada detectará automáticamente qué tipo de placa está configurada según la configuración actual de la base de datos.
3: PRS_TDM	Seleccione esta opción si las tarjetas de expansión conectadas son de dos puertas (VAX-EXP-2D).
5: PRS_TDM_All	Esta opción le permitirá probar lectores en múltiples expansores de dos puertas (VAX-EXP-2D) al mismo tiempo.

5. Después de seleccionar un tipo de tablero, ahora elegirá una dirección de tablero. Las direcciones admitidas actualmente son 1-4 para expansores VAX-EXP-2D y 1-8 para expansores VAX-IO-EXP8-PCB.



6. Usando los botones blancos hacia arriba y hacia abajo en el Panel, localice la dirección para el expander desea probar y presione el botón Enter.
7. Se le mostrará una pantalla que dice 'Sin entrada de tarjeta'. Ahora puede presentar una tarjeta de proximidad o fob a uno de los Lectores adjuntos.



8. Si el Lector está cableado correctamente y se presenta una tarjeta de 40 o 26 bits, verá información sobre la tarjeta y el Lector en la pantalla. Si está utilizando un segundo Reader, puede realizar la prueba en ese Reader de la misma manera. Cuando haya terminado de probar, presione el botón ESC.




9. Después de presionar ESC, verá un mensaje que dice "Canceled". Volverá al menú de opciones. Ahora puede continuar con pruebas adicionales.



Interfaz de configuración HTTP del panel

Esta sección cubrirá cómo acceder a la interfaz web de configuración HTTP del Panel y cómo realizar cambios en esta interfaz.

 **Nota:** La interfaz HTTP del panel actualmente no es compatible con algunos modelos, como los paneles de ascensores PoE

Cada Panel tiene una interfaz web de configuración a la que se puede acceder a través de un navegador web, siempre que el cliente que se conecte a esta interfaz esté en la misma red. En esta interfaz se pueden configurar muchos de los ajustes que podemos configurar manualmente. Si el Panel tiene una dirección IP válida a través de DHCP o una dirección estática ingresada manualmente, puede usar esa dirección a través de un navegador web para acceder a esta interfaz.

1. Obtenga la dirección IP del Panel manteniendo presionado SW4 durante 4 segundos en el Panel y usando SW1 y SW2 para buscar '06 Actual IP Add'. Si ha asignado una dirección estática al Panel, esa será la dirección que utilice. Alternativamente, si el Panel se ha comunicado con el servidor, es probable que pueda encontrar la dirección haciendo lo siguiente: Abra un símbolo del sistema en el servidor, escriba 'arp -a' y presione Entrar. Una vez que encuentre la dirección MAC, busque la entrada adyacente en la columna a la izquierda de la dirección MAC; verá la dirección IP asociada con esa dirección MAC.
2. Abra un navegador web y escriba la dirección IP del Panel por sí mismo, no se requieren números de puerto, 'http' o 'www'. Si la conexión es exitosa, se le solicitará un nombre de usuario y una contraseña. El nombre de usuario es 'usuario' y la contraseña es la contraseña de 4 dígitos que se utiliza para acceder a la interfaz del Panel a bordo, por defecto es '0000'. Una vez que inicie sesión, verá la descripción general del panel de acceso a la puerta (Door Access Panel Overview).

Figura 3.9. Descripción general de la configuración HTTP del panel

ODM PANEL
PANEL1771

Door Access Panel
Overview

Overview

Panel Setup

Panel

Name: No Panel Name
Area: No Area Name
Time: 2019,06,21 09:27:35
Firmware Version: ODM V19022107
Run Mode: Normal
Communication Mode: DHCP Client
Connection Type: Wired
Assigned IP: 192.168.002.041
MAC Address: 001EC0EE26EB

Server

Name: SERVER-PC
IP Address: 192.168.002.192
Port: 9876
Connection Mode: Server IP

Door 1

Mode: Lockdown
State: Closed
Lock State: Locked
Internal Motion: Enabled
External Motion: Disabled
Outside Reader: Reader 1
Inside Reader: Reader 2

* Press F5 to update or click:

Hay dos páginas en la interfaz web a las que se puede acceder con el panel de navegación en el lado izquierdo de la página. La descripción general (la página principal) muestra información del panel de solo lectura. La configuración del panel es donde puede anular la configuración de comunicación del panel.

Descripción general: en la página de descripción general, puede ver el estado y la configuración del panel. Algunas de las secciones destacadas incluyen: el nombre del panel, la versión del firmware, el modo de comunicación (cómo obtiene su dirección IP), la dirección IP asignada, la dirección MAC, el nombre del servidor, la IP del servidor y el modo de conexión del servidor (IP o nombre) el Panel está utilizando para conectarse al servidor. Para cada puerta: el modo de la puerta (en cuál de los 8 estados de la puerta se encuentra actualmente la puerta), el estado (abierto o cerrado, si la puerta tiene un contacto de puerta) y el estado de bloqueo (bloqueado o desbloqueado).

Configuración del panel: En la pantalla de configuración del Panel, podrá cambiar la configuración de comunicación en el Panel: el Modo de comunicación del Panel (cómo obtiene el Panel su dirección IP), IP del Panel (no se configurará a menos que el modo de comunicación del Panel sea una IP estática), Servidor Nombre (si se comunica con el servidor por nombre), IP del servidor (si se comunica con el servidor por dirección IP), Modo de conexión del servidor (el método de comunicación que utilizará el Panel para encontrar el servidor) y Modo de servidor HTTP (habilita el Panel interfaz web). Una vez que haya ingresado los cambios, puede presionar **Set Panel Configuration** para guardar los cambios.

Advertencia

Los cambios en esta interfaz que se guarden anularán cualquier información ingresada manualmente o la configuración obtenida del software VAX. Si cambia los métodos de comunicación en la interfaz, le recomendamos que realice esos mismos cambios en el software VAX. La pantalla Configuración del panel solo debe usarse para la configuración inicial o cuando la información del servidor ha cambiado.

Agregar un panel al control de acceso VAX

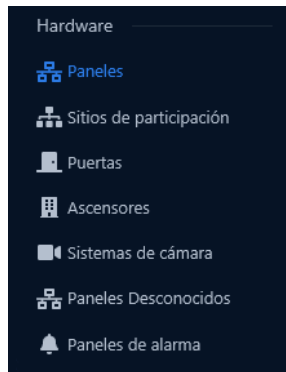
Esta sección cubrirá el proceso básico de agregar un Panel en VAX Access Control. En la mayoría de las implementaciones, es un proceso bastante fácil y se puede realizar de dos maneras diferentes.

Método 1: Agregar un panel desconocidos en la ventana de paneles

Esta sección cubrirá la adición de un Panel al software después de que el Panel haya sido configurado para buscar el servidor.

El Panel está configurado para encontrar el servidor por Nombre o Dirección IP. (Consulte la sección llamada "Configuración de IP del panel: IP estática" y la sección llamada "Configuración del modo de comunicación: Nombre del servidor (DNS)" para obtener detalles sobre cómo configurar un panel para encontrar un servidor de control de acceso VAX).

1. Acceda a su sistema de control de acceso VAX a través de su navegador HTML5 de elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en **Paneles desconocidos** en la sección Hardware en la parte inferior del menú de navegación..



4. En la pantalla Paneles desconocidos, cualquier Panel que se comunice correctamente con el servidor y que aún no se haya agregado aparecerá en esta lista. Se mostrará el nombre, la dirección MAC, la dirección IP, el tipo de panel y la versión del firmware..

Unknown Panels							
Name	MAC	IP Address	Type	Firmware	First Attempt	Last Attempt	
+ TEST-POE-ODM	5410ECB4D00E	192.168.2.192	ODM	11/24/2020	11/29/2022 12:57:30 AM	11/29/2022 1:06:06 AM	✖

Consejo


Si no está seguro de qué dirección MAC pertenece a qué controlador, puede acceder al menú de solo lectura en un panel manteniendo presionada la tecla ESC durante 4 segundos. Use los botones blancos para encontrar el elemento 7, dirección MAC del panel.

5. Cuando haya identificado el panel que desea agregar, haga clic en el botón + a la izquierda del nombre del panel. Accederá a la pantalla **Add Panel** con la dirección MAC, el modelo del panel y los campos de información de IP rellenos previamente..
6. Continúe con la sección llamada "**Agregar un panel: configuración básica**" para obtener instrucciones continuas sobre cómo agregar un panel.

Método 2: Agregar un panel manualmente con dirección MAC

Esta sección cubrirá cómo agregar un Panel manualmente en VAX Access Control. Puede elegir este método por las siguientes razones:

- Aún no ha configurado el Panel para comunicarse con el servidor.
- Está preconfigurando el software antes de la implementación de los paneles.
- Se debe recopilar la siguiente información antes de agregar paneles manualmente:
 - El modelo del Panel (en la caja en la que vino el Panel) para cada Panel (para ver la lista completa de modelos, consulte la sección correspondiente dentro de la guía técnica principal).
 - Dirección MAC de cada Panel.
 - Si los paneles utilizarán DHCP o direcciones estáticas.
 - Ubicación de los Paneles (generalmente se usa para nombrar los Paneles).
 - Si el Panel es un Panel de Puerta, ¿usará un contacto de Puerta?

 **Nota:** Si toda esta información no está disponible, puede usar valores de marcador de posición para las direcciones MAC y los nombres.

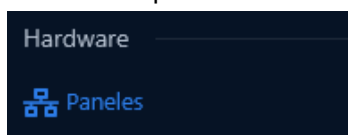
Una vez que haya recopilado esta información, ahora podemos comenzar a agregar los paneles. Continúe con la sección llamada "Agregar un panel: configuración básica".

Agregar un Panel: Configuración Básica

Esta sección cubrirá los diversos campos que deben completarse para agregar un Panel en VAX Access Control. Se recomienda completarlos en el orden en que se muestran en la pantalla, con la excepción de la dirección MAC si se completa previamente.

Si aún no está en la pantalla Agregar paneles:

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en Paneles en la sección Hardware en la parte inferior del menú de navegación.



4. En la **pantalla Paneles**, haga clic en el botón **Agregar**.

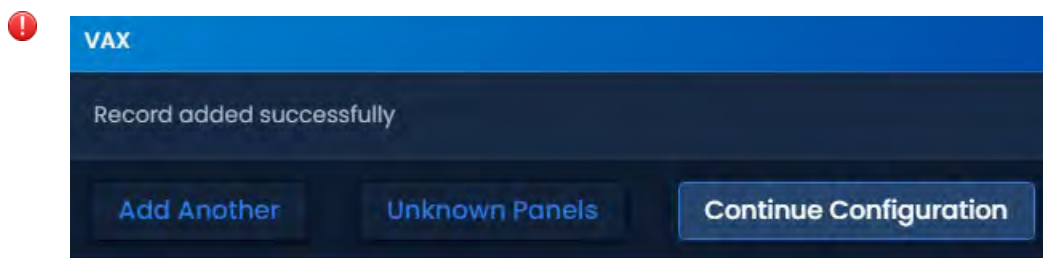
En la pantalla **Agregar panel**, se le presentarán varios menús desplegables, campos de texto y casillas de verificación para completar. Si navegó a esta página desde la pantalla Paneles desconocidos, la mayor parte de la información se completará automáticamente.

Figura 3.10. Pantalla de Agregar Panel

Tabla.11. Agregar campos de panel

Desplegable/cuadro de texto/casilla de verificación	Descripción
Modelo de panel	Seleccione el modelo de Panel usando este menú desplegable; según el modelo que elija, es posible que se muestren opciones adicionales.
Nombre	El nombre del Panel; Recomendamos nombrar el Panel según su ubicación en el sitio. Acepta de 4 a 60 caracteres.
Descripción	Descripción opcional del Panel. Acepta de 0 a 255 caracteres.
Sitio	Seleccione el sitio en el que residirá el Panel. Esto no se puede cambiar una vez que se agrega el Panel.
Dirección MAC	La dirección de red única integrada en cada Panel. Puede completarse previamente si está agregando el panel a través de una notificación de conexión desconocida desde el panel. Debe tener 12 caracteres.
Contraseña del panel	La contraseña es necesaria para acceder al menú de administración integrado en el Panel. Los valores válidos son de 0 a 9999. El valor predeterminado es '0000'.
Instalado	Establece si el panel y sus dispositivos deben aparecer en la Descripción general del sistema o en otras páginas de estado.
sensor de manipulación	Desmarque para deshabilitar automáticamente el sensor de manipulación integrado una vez que se agregue el Panel.
Contactos de puerta	Desmarque si no hay contactos de puerta conectados al panel.
Agregar puertas automáticamente	Marque si desea agregar Puertas automáticamente a este Panel. Serán nombrados en base al nombre del Panel. Por ejemplo, el nombre "Panel frontal" agregará una puerta llamada "Puerta frontal".
Expansores (solo en algunos modelos)	Número de módulos expansores. Módulos de E/S o de puerta. Ingrese la cantidad correcta (1-8 para módulos IO, 1-4 para módulos de puerta).
Modo de conexión	Método en el que el Panel obtendrá su dirección IPv4. Si configuró manualmente una dirección IP en el panel, deberá establecerla en IP estática y completar los detalles de la red.

Ahora puede hacer clic en **Guardar**; se le pedirá que corrija cualquier información que falte o que no sea válida. Una vez corregido pulsa **Guardar** de nuevo. Aparecerá un cuadro de mensaje que dirá Registro agregado con éxito con las opciones **Agregar otro** (que lo llevará de regreso a la pantalla Agregar panel), **Continuar configuración** (que lo llevará a la pantalla **Editar panel** donde puede configurar opciones adicionales que son cubierto en la sección llamada "Configuración avanzada del panel") o **Paneles desconocidos** que lo llevarán a la lista de Paneles desconocidos.



Advertencia

Antes de su primera actualización de los Paneles, le recomendamos configurar los ajustes avanzados de sus Paneles. Esto se puede encontrar en la sección llamada "Configuración avanzada del panel".

A dónde ir desde aquí

Ya ha completado los dos capítulos más importantes del libro.

Si acaba de completar una instalación del software, le recomendamos que se tome un momento para explorar y cambiar la contraseña predeterminada de la interfaz de usuario de System Manager. Para obtener más información, consulte el Capítulo 5, *Interfaz de usuario del administrador del Sistema*

Para obtener información sobre la licencia VAX e información sobre la licencia de su software, consulte el *Capítulo 4, Licencias de software*.

Si está listo para continuar con la configuración de un panel, consulte la sección denominada "Configuración avanzada del panel".

Si no tiene experiencia con el control de acceso o desea repasar la terminología específica de VAX, consulte el *Capítulo 6, Planificación de una implementación de control de acceso*. Contiene más información para planificar con éxito una implementación, junto con vínculos a muchas partes diferentes de esta guía.

Para obtener información de contacto de soporte, consulte el *Capítulo 37, Soporte*.

Capítulo 4. Licencias de software

Este capítulo cubrirá el aspecto de la licencia de software de VAX, información sobre el proceso de licencia, cómo funcionan los formatos de tarjeta con nuestra licencia de producto y preguntas frecuentes sobre la licencia de su software.

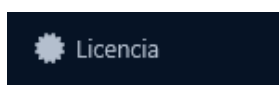
VAX es un producto con licencia. Las licencias nos ayudan a continuar desarrollando y agregando nuevas funciones a VAX. También ayuda a los integradores a mantener buenas relaciones con los usuarios finales, realizar el mantenimiento de los herrajes de las puertas y puede facilitar los ingresos recurrentes para el instalador. El software con licencia brinda a los distribuidores y usuarios finales el beneficio de costos iniciales bajos. Con una licencia VAX válida, su sistema también tiene derecho a actualizaciones de software básicas gratuitas.

 **Nota:** VAX incluye una licencia de prueba de 15 días después de la instalación inicial.

Licencia de su software

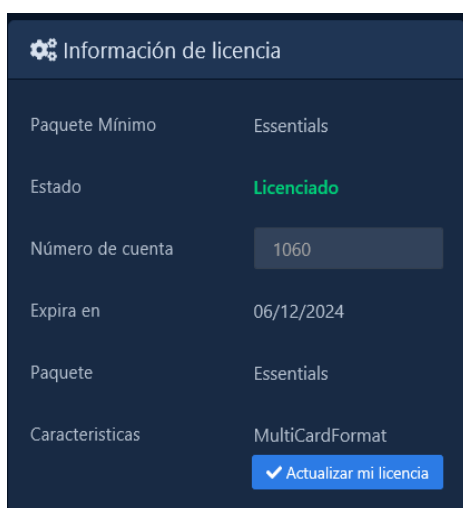
La activación de la licencia de software en su VAX es simple por diseño. La sección Opciones de licencia también se incluye para facilitar su elección del nivel de licencia, ya que le proporcionará el paquete necesario para conservar las funciones de su configuración actual..

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en **Licencias** en la sección Administración en la parte inferior del menú de navegación.



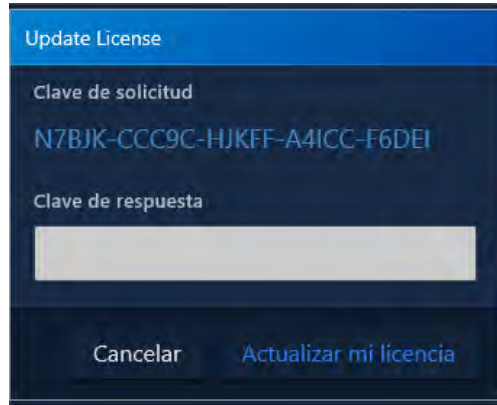
4. Asegúrese de tener un número de cuenta válido en el campo '**Número de cuenta**'. Si no es así, puede obtenerlo poniéndose en contacto con su distribuidor o instalador..

Figura 4.1. Pantalla de licencia VAX




5. El siguiente paso es tomar nota de su 'Caducacion!' para determinar si se requiere una licencia en este momento y tomar nota de su paquete de software.
6. A menos que esté dentro de los últimos 30 días de su licencia de software o desee cambiar su paquete de software, no es necesario actualizar su licencia. Si determina que la licencia debe actualizarse, continúe con el siguiente paso.

7. Para generar una nueva licencia, haga clic en el botón '**Actualizar mi licencia**' en la parte inferior de la pantalla.
8. Se le presentará su nueva **clave de solicitud**. Póngase en contacto con su distribuidor, instalador o Industrias Vicon (consulte el Capítulo 37, Soporte) con esta clave de solicitud (solo válida el día en que se generó). Se revisarán sus opciones de licencia para determinar la mejor duración de la licencia y el mejor paquete de software para sus necesidades y luego se le proporcionará una clave de respuesta que activará su software.



9. Una vez que haya ingresado la **clave de respuesta** proporcionada por Vicon Industries, haga clic en '**Actualizar**' para activar su licencia.

 **Nota:** La clave de respuesta debe ingresarse en mayúsculas con guiones entre cada 5 caracteres.


Formatos de tarjeta admitidos

VAX es compatible con una variedad de formatos de bit de tarjeta; sin embargo, para simplificar y aumentar la seguridad, recomendamos usar nuestras credenciales de alta seguridad de 40 bits cuando sea posible. Como parte de su licencia VAX, puede bloquear formatos de tarjetas de terceros. Esto puede agregar seguridad adicional a sus sistemas al restringir el uso de credenciales de menor seguridad. Para obtener más información sobre otros formatos de tarjeta y habilitarlos en su licencia de software (sin cargo), comuníquese con Vicon Industries. *Consulte el Capítulo 37, Soporte.*

Preguntas frecuentes sobre licencias de software

P: ¿Recibiré un aviso antes de que caduque mi licencia?

R: Absolutamente. Dentro de los últimos 30 días del período de su licencia, el software VAX le informará que el software está a punto de caducar y le proporcionará la fecha exacta de caducidad.

 **Nota:** Si la configuración de correo electrónico está configurada, VAX intentará enviar un correo electrónico a los administradores del sistema y al distribuidor para informarles que la licencia vencerá pronto.

P: ¿Qué sucede cuando mi software caduca?

R: En el primer inicio de sesión después de que caduque una licencia, comenzará un período de gracia de 10 días. Durante este período de gracia, todas las funciones estarán disponibles. Todas las funciones críticas y las configuraciones existentes continuarán ejecutándose después de que el software caduque y el período de gracia de 10 días haya terminado. Consulte las preguntas a continuación para saber qué estará disponible y qué no estará disponible cuando el software caduque.

P: ¿Qué características estarán disponibles una vez que mi licencia haya expirado y mi período de gracia de 10 días haya terminado?

R: Después de que la licencia haya expirado y haya terminado el período de gracia de 10 días; un subconjunto muy pequeño de funciones está disponible:

- La mayoría de las pantallas están disponibles en modo de solo lectura, incluidos los usuarios de visualización, días festivos, grupos de acceso, etc.
- Las características que afectan la seguridad personal se mantienen para su seguridad. Esto incluye:
 - Puertas Pulsantes
 - Eliminación de usuarios/credenciales
 - Anulación de Puertas, Pisos, Entradas y Salidas
 - Anular al nivel de crisis
 - Eliminación de administradores, cambio de contraseñas y modificación de permisos
 - Comandos del panel (incluidos Actualizar paneles, Restablecer Anti-Passback, Obtener hora, Desconectar panel, Colocar panel en modo de actualización de firmware)
 - Estado del Sistema
 - Actualización de la información de la licencia

P: ¿Qué características no estarán disponibles después de que mi licencia haya expirado y mi período de gracia de 10 días haya terminado?

R: La mayoría de los cambios en su sistema están deshabilitados. Esto incluye (pero no se limita a):

- Agregar Usuarios/Credenciales
- Agregar/Modificar días festivos
- Cambio de horarios
- Visualización de cámaras
- Visualización de informes

P: ¿Por qué VAX requiere una licencia?

R: Al principio del desarrollo, decidimos optar por un enfoque con licencia por varias razones.

- Proporcionar un costo inicial de software significativamente más bajo en comparación con nuestros competidores.
- Ofrecer a los usuarios finales la capacidad de pagar por las funciones que necesitan, asegurando que los sitios más pequeños que no puedan aprovechar el conjunto completo de funciones de VAX reciban un precio acorde con lo que necesitan.
- Permitirnos continuar actualizando y mejorando el conjunto básico de características VAX y ofrecer estas actualizaciones sin cargo adicional para el usuario final.
- Reducir la piratería de software.

P: ¿Qué términos de licencia están disponibles?

R: Hay varios niveles de licencias de software que son válidas por 1 año o 3 años de licencia. Cada nivel aumenta ciertos aspectos, como el número de puertas/cámaras. Comuníquese con Vicon Industries para obtener más información sobre estos paquetes. (Consulte el Capítulo 37, Soporte).

P: ¿A qué me da derecho una licencia VAX?

R: Siempre se requiere una licencia VAX activa para usar el software VAX y esta licencia le dará derecho a todas las actualizaciones de software durante el plazo de la licencia. Esto incluye cualquier característica adicional y mejoras agregadas dentro de su paquete de software..

P: ¿Sigue siendo válida mi licencia de software si cambio la computadora que aloja el software VAX?

R: Al restaurar una base de datos VAX en una computadora diferente, automáticamente invalidará su licencia. Sin embargo, no se le cobra una tarifa por la licencia de la nueva computadora. Comuníquese con Vicon Industries para que vuelva a armar su licencia, lo que le proporcionará una licencia de software válida para su nueva PC que transferirá el tiempo restante de su licencia anterior y su paquete de software con licencia.

Capítulo 5. Interfaz de usuario del administrador del sistema

La interfaz de usuario del administrador del sistema es una interfaz web separada que se utiliza con fines de administración, como ejecutar copias de seguridad de la base de datos, iniciar o detener el servicio web de la aplicación principal, cambiar la configuración de la red, etc..

Acceso a la interfaz de usuario del administrador del sistema

Acceder a la interfaz de usuario de System Manager es un procedimiento muy similar al acceso a la interfaz web de VAX; la principal diferencia es que está alojado en un puerto diferente (11002).

1. Acceder a la interfaz de usuario de System Manager desde la PC en la que está instalado el servidor

Durante la instalación, se coloca un acceso directo en el menú Inicio para la **interfaz de usuario de System Manager**. El enlace para la interfaz de usuario de System Manager se puede ubicar haciendo clic en Inicio -> Todos los programas -> VAX y finalmente haciendo clic en "Iniciar VAX System Manager".

Acceso a la interfaz de usuario de System Manager desde una PC remota

Abra su navegador web y dentro de la barra de direcciones ingrese la dirección del software de **interfaz de usuario de System Manager** usando el formato:
https://NameOfTheComputer:PortNumber .

Alternativamente, también puede acceder a la interfaz de usuario de administración del sistema a través de la dirección IP usando el formato: ***https://192.168.0.100:PortNumber***.

Ejemplo 5.1. Acceso a la interfaz de usuario de System Manager de forma remota

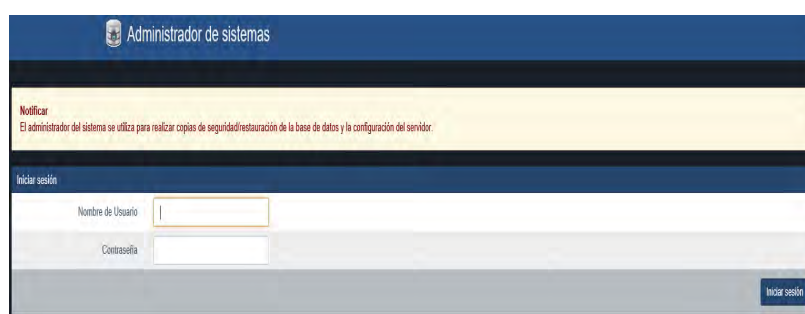
https://ComputerName:11002 (default port is 11002)



Una vez que haya ingresado la dirección, presione enter para navegar a la interfaz de usuario de **VAX System Manager**.

2. Verá una pantalla de inicio temporal y luego se le presentará la ventana de inicio de sesión.

Figura 5.1. System Manager UI Ventana de inicio



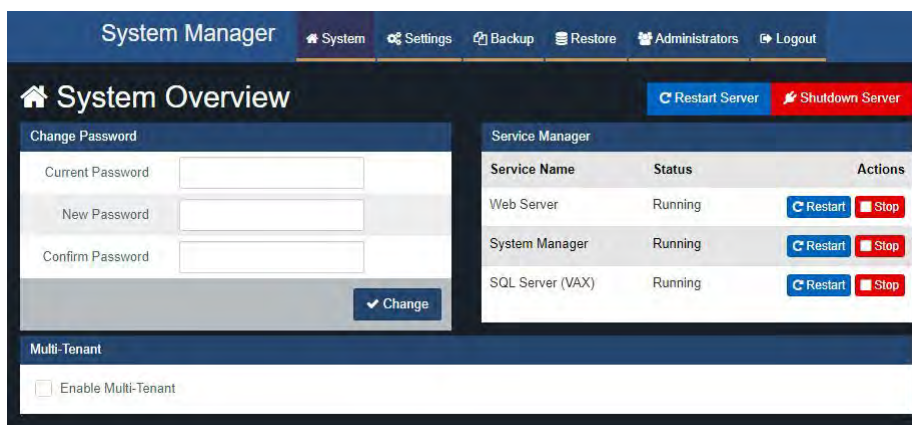
Nombre de usuario y contraseña predeterminados para System Manager UI

El nombre de usuario predeterminado es 'vax' y la contraseña predeterminada es 'vaxaccess' (se distingue entre mayúsculas y minúsculas y sin comillas).

- ⚠ **Precaución:** Recomendamos cambiar la contraseña predeterminada de la interfaz de usuario del administrador del sistema lo antes posible.

3. Al iniciar sesión, se le presentará la pantalla del sistema.

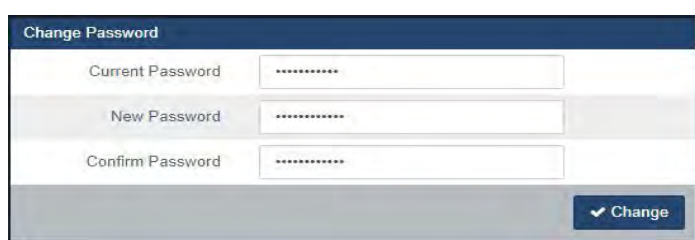
Figura 5.2. System Manager UI - Pantalla del sistema



Cambiar la contraseña de la interfaz de usuario del administrador del sistema

- Haga clic en 'Sistema' en el menú superior cuando inicie sesión en **la interfaz de usuario del administrador del sistema**.
- En la pantalla del sistema, habrá una sección Cambiar contraseña en el lado izquierdo de la pantalla.

Figura 5.3. Sección de cambio de contraseña



- Ingrese su contraseña actual (la predeterminada es 'vaxaccess') seguida de la nueva contraseña dos veces.
- Haga clic en **'Cambiar'** para completar el procedimiento de cambio de contraseña.

Copia de seguridad de su base de datos VAX

- Acceda a la interfaz de usuario del administrador del sistema. (Consulte la sección llamada "Acceder a la **interfaz de usuario del administrador del sistema**".)
- Haga clic en **'Copia de seguridad'** en el menú superior.
- Seleccione los elementos que desea respaldar (se recomienda la configuración predeterminada).

- **Base de Datos:** La base de datos VAX (recomendado)
 - **Fotos de perfil:** Imágenes asociadas a tus Usuarios (titulares) (recomendado).
 - **Mapas:** Imágenes asociadas con cualquier mapa gráfico
4. Seleccione sus opciones de copia de seguridad (se recomienda la configuración predeterminada).
- **Comprimir copia de Seguridad:** Determina si el archivo de copia de seguridad se comprime después de una copia de seguridad correcta (recomendado).
 - **Eliminar archivos anteriores a X días:** Elimina automáticamente los archivos **.prbak** de la ubicación de la copia de seguridad si la antigüedad supera el número de días especificado. Elija mantener más copias de seguridad o desmarque para mantener todas las copias de seguridad hasta que se eliminen manualmente
 - **Copia de seguridad cifrada con contraseña:** Marque si desea que se solicite una contraseña para restaurar la copia de seguridad.
5. Determine dónde se guardará su copia de seguridad. Ofrecemos soporte para una unidad local, una unidad USB o un recurso compartido de red.

 **Precaución:**

El usuario de Windows que ejecuta el servicio System Manager debe tener acceso adecuado a la carpeta de salida deseada. La cuenta de servicio predeterminada de Windows es "NT SERVICE\VAXSysManager". En el caso de realizar una copia de seguridad en una unidad de red, es posible que no pueda otorgar acceso de lectura y escritura a la cuenta de servicio predeterminada con la que se ejecuta el servicio System Manager. En este caso, deberá reinstalar el software y especificar una cuenta de Windows diferente que tenga acceso a esa unidad de red. Consulte la sección correspondiente dentro de la guía técnica principal para obtener más información.

Copia de seguridad en unidad local o USB

El siguiente cuadro de texto ahora se puede completar con una ruta a una ubicación de copia de seguridad, incluida una unidad local o USB. El formato de la ruta es similar a: "**C:\Backup**"

 **Nota:** Si la carpeta que ingresó en el campo de texto 'output a' no existe, se creará

Copia de seguridad en recurso compartido de red: Ingrese la ruta de su recurso compartido de red.

Ejemplo 5.2. Ejemplo de recurso compartido de red

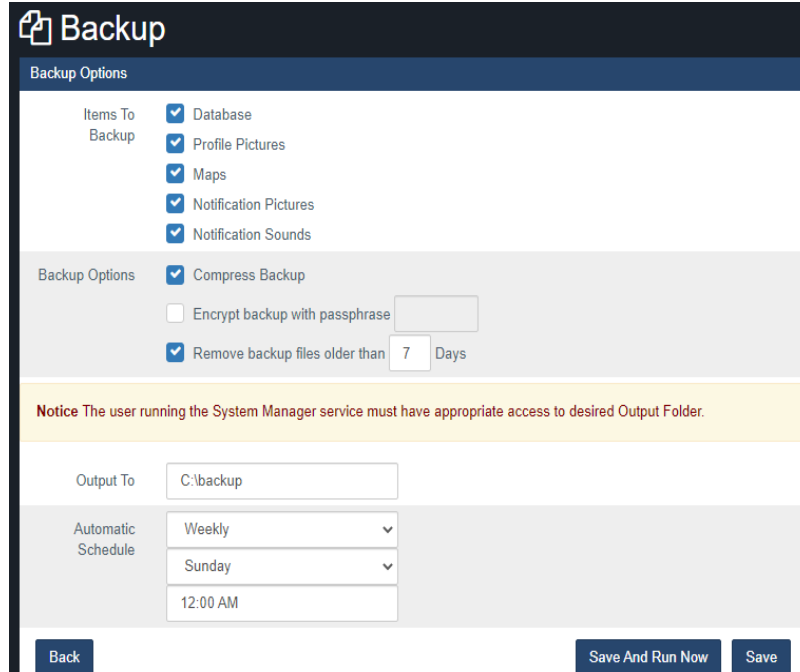
`\\Servername\PathToMyBackupShare`

6. Seleccione un programa de copia de seguridad.
- **Deshabilitado:** Sin programación automática. La copia de seguridad se inicia presionando el botón 'Guardar y ejecutar ahora'.
 - **Diariamente:** la copia de seguridad se realiza una vez al día a la hora especificada.
 - **Semanalmente:** la copia de seguridad se realiza una vez a la semana en el día de la semana y la hora especificada.
7. Si desea ejecutar la copia de seguridad inmediatamente, haga clic en el botón '**Guardar y ejecutar ahora**'. Alternativamente, haga clic en el botón '**Guardar**' para guardar la

configuración de la copia de seguridad y ejecutarla en la próxima hora programada (si se define una programación).

Si los permisos de carpeta o red impidieron que se escribiera la copia de seguridad, verá un error. Al realizar su primera copia de seguridad, debe buscar la salida y verificar que se haya escrito la copia de seguridad. Esto puede tardar varios minutos para bases de datos más grandes..

Figura 5.4. Pantalla de copia de seguridad del administrador del sistema



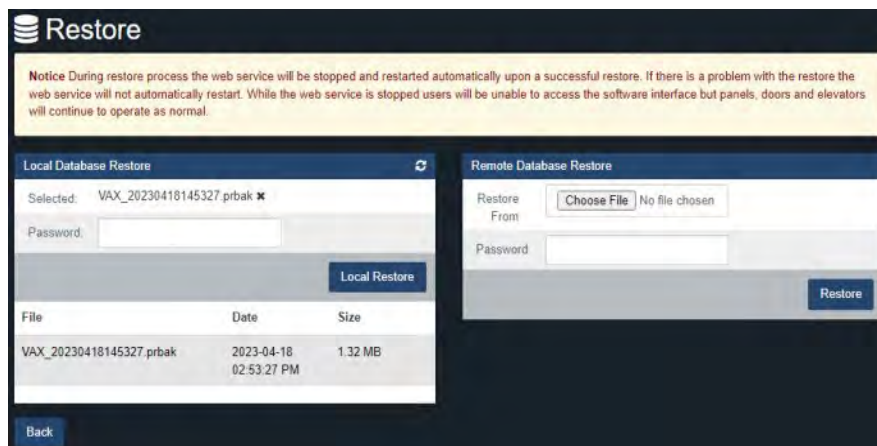
 **Nota**

Si tiene problemas para realizar una copia de seguridad de su base de datos utilizando la interfaz de usuario de **System Manager**, hay un método manual para realizar copias de seguridad que se detalla en la sección llamada "**Realización de una copia de seguridad y restauración manual con la línea de comandos de MSSQL**".

Restauración de su base de datos VAX

1. Acceda a la interfaz de usuario del administrador del sistema (consulte la sección llamada "Accessing the System Manager UI").
2. Haga clic en '**Restore**' en el menú superior.

Figura 5.5. Restaurar la base de datos



3. En el lado izquierdo de la pantalla, verá los archivos de copia de seguridad existentes que se encuentran en la carpeta de copia de seguridad configurada.
4. Puede restaurar seleccionando directamente una copia de seguridad de la base de datos de la lista o usar el botón Elegir archivo para seleccionar manualmente un archivo de copia de seguridad de la base de datos. Una copia de seguridad que se realizó el 25 de marzo de 2022 se llamaría "VAXfullbackup_20220325010349.prbak".

Restauración desde un archivo de copia de seguridad

- Opcionalmente ingrese la contraseña si se usó una contraseña durante la copia de seguridad.
 - Haga clic en el botón **'Restore'** o botón **Local Restore**.
5. Ahora se restaurará la base de datos. Si el proceso de restauración falla, recomendamos intentarlo de nuevo. Si continúa fallando, hay un método manual para realizar la restauración de la base de datos que se detalla en la sección llamada "Realización de una copia de seguridad y restauración manual con la línea de comandos de MSSQL".

⚠ Advertencia

Durante el proceso de restauración, el servicio web se dejará y se reiniciará automáticamente después de una restauración exitosa. Si hay un problema con la restauración, el servicio web no se reiniciará automáticamente. Mientras el servicio web esté detenido, los usuarios no podrán acceder a la interfaz del software, pero los paneles, las puertas y los ascensores seguirán funcionando con normalidad.

Servicio y Gestión de Sistemas

El **System Manager UI** permite controlar el servicio del servidor web VAX y el servicio SQL Server que utiliza VAX. Además de brindar la capacidad de reiniciar o apagar su sistema, esto es útil cuando no se puede acceder fácilmente a la PC y brinda un método rápido para reiniciar los servicios o verificar si se está ejecutando.

Gestión de servicios

1. Haga clic en **'System'** en el menú superior al iniciar sesión en el system manager UI.
2. Verá una sección del Service Manager para el servidor web VAX y el servidor SQL

Figura 5.6. Gestión de servicios

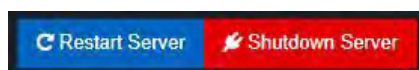
Service Name	Status	Actions
Web Server	Running	Restart Stop
System Manager	Running	Restart Stop
SQL Server (VAX)	Running	Restart Stop

3. Desde aquí puede iniciar/detener/reiniciar y ver el estado de los servicios.

Apagar o reiniciar su servidor

1. Haga clic en **'System'** en el menú superior al iniciar sesión en el System Manager UI.

Figura 5.7. Apagar o reiniciar su servidor.



2. Verá dos botones correspondientes a reiniciar o apagar su sistema.

Configuración de red en el System Manager

El **System Manager** ahora brinda soporte limitado para configurar su red. Esto no pretende reemplazar las opciones de configuración de red dentro de Windows, sino proporcionar una interfaz más simple para cambiar o verificar la configuración básica de la red. Para una configuración avanzada, le recomendamos que utilice las opciones de red tradicionales de Windows.

⚠ Precaución

Cambiar la configuración de la red puede causar una pérdida de conexión con el administrador del sistema y el software VAX. Asegúrese de ingresar opciones de configuración de red válidas. Si no está seguro de los valores correctos, póngase en contacto con el administrador del sistema.

Configuración de red

1. Haga clic en **'Networking'** en el menú superior al iniciar sesión en el System Manager UI.
2. Ahora se le presentará la página de configuración de la red.

Figura 5.8. Página de configuración de red



📌 **Nota :** Cambiar su nombre del host requerirá un reinicio del sistema.

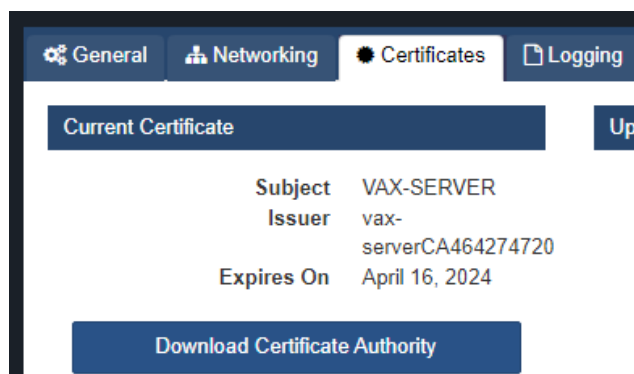
Certificados SSL

Esta sección del manual cubrirá los **certificados SSL** y cómo instalarlos/administrarlos dentro de System Manager. Esto cubrirá el certificado autofirmado predeterminado, así como también cómo importar el suyo propio a System Manager. Además, brindará una guía general sobre cómo exportar su certificado autofirmado y cómo instalarlo en el Almacén de certificados de la computadora, lo que permite omitir el mensaje "La conexión no es segura".

Introducción a los Certificados

Dentro de la página **System Manager** de **VAX**, el usuario puede navegar a la subpestaña **Certificados** en la pestaña **Configuración**. Al usuario se le presentarán 2 elementos. **Certificado actual**, que mostrará el certificado actual instalado, su asunto, el emisor y cuándo caduca. La segunda es la sección **Actualizar certificado**, que permite al usuario elegir qué tipo de certificado/método desea instalar y utilizar. Seleccionar opciones aquí cambiará dinámicamente la sección a continuación que se utiliza para la generación del certificado autofirmado, las opciones para cargar e instalar certificados **PEM** o **PFX** y, por último, una lista de certificados en el almacén de certificados de su PC.

Figura 5.9. Certificados



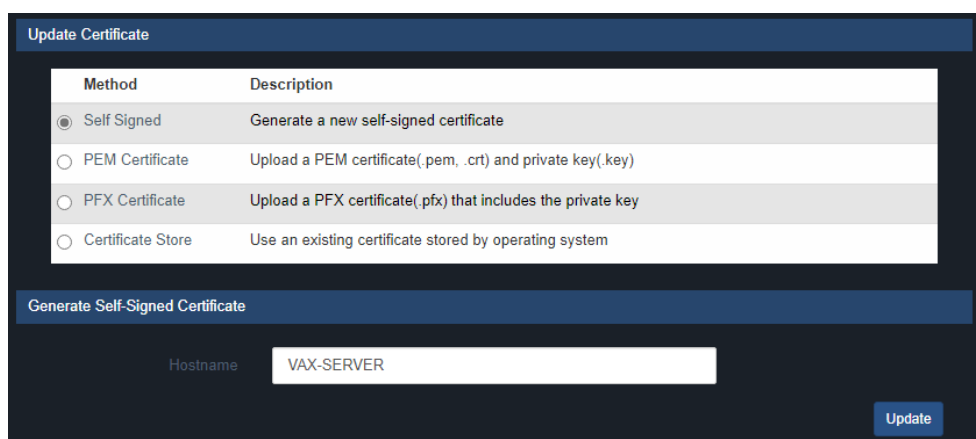
Certificados Autofirmados

Durante la instalación inicial de VAX, al usuario se le presentará una opción para generar un **certificado autofirmado**. Sin embargo, este no es el único lugar donde se puede hacer esto. Después de la instalación, el usuario puede generar uno nuevo a través del administrador del sistema. Los casos de uso para esto incluyen el vencimiento del certificado, así como cambios como cambios en el nombre de host de la computadora que podrían afectar la accesibilidad. Al usuario se le presentará un cuadro que debe completarse automáticamente con el nombre de host de la computadora. Esto se puede cambiar según sea necesario. Al hacer clic en **Actualizar**, se cerrarán los servicios VAX e instalará el certificado recién generado.

Consejo

El uso de un certificado autofirmado dará como resultado que el usuario reciba un mensaje de advertencia de **Conexión no segura** al navegar al servidor, ya que no está firmado por una autoridad de certificación válida y reconocida. Omitir esto se tratará en otra sección.

Figura 5.10.



Certificados PEM

Los Certificados PEM son un par que viene con dos archivos. El archivo de certificado (ya sea **.pem** o **.crt**) y el **archivo de clave privada (.key)**. Ambos son necesarios ya que la clave privada esencialmente confirma que el certificado es un certificado válido de una **Autoridad de certificación (CA) verificada**. El proceso para obtenerlos está más allá del alcance de este manual; para obtener más información sobre cómo obtenerlos, comuníquese con su especialista en TI o con el proveedor del que se compró el certificado. El proceso real de la instalación es simple. Simplemente cargue los dos archivos en los respectivos cuadros de carga y haga clic en actualizar. Los servicios se reiniciarán y, una vez que estén en funcionamiento, el usuario puede verificar navegando hasta el servidor en un navegador web y verificando si el certificado se muestra como válido en el navegador web.

Figura 5.11.

The screenshot shows a web interface titled "Update Certificate". It features a table with the following content:

Method	Description
<input type="radio"/> Self Signed	Generate a new self-signed certificate
<input checked="" type="radio"/> PEM Certificate	Upload a PEM certificate(.pem, .crt) and private key(.key)
<input type="radio"/> PFX Certificate	Upload a PFX certificate(.pfx) that includes the private key
<input type="radio"/> Certificate Store	Use an existing certificate stored by operating system

Below the table is the "Upload PEM Certificate" section, which includes two file upload fields:

- Certificate (.pem, .crt) with a "Choose File" button and "No file chosen" text.
- Private Key (.key) with a "Choose File" button and "No file chosen" text.

An "Update" button is located at the bottom right of the form.

Certificados PFX

Los **certificados PFX** son un poco diferentes a los PEM. En lugar de tener el archivo de certificado y el archivo de clave, se ha combinado en un solo archivo protegido con contraseña. Por lo general, esta contraseña se establece al generar la CSR en IIS o en una herramienta de terceros como Digicert. ***Esta parte queda fuera del alcance del manual y se recomienda comunicarse con su especialista en TI o proveedor de certificados.*** Para instalar el certificado, simplemente cargue el **archivo .pfx** en el cuadro de carga y proporcione la contraseña utilizada para cifrarlo.

Haga clic en actualizar y los servicios se reiniciarán una vez que se instale el certificado. Los usuarios pueden verificar que el certificado esté funcionando navegando al servidor en un navegador web y comprobando si el certificado se muestra como válido en el navegador web.

Figura 5.12.

The screenshot shows a web interface titled "Update Certificate". It features a table with the following content:

Method	Description
<input type="radio"/> Self Signed	Generate a new self-signed certificate
<input type="radio"/> PEM Certificate	Upload a PEM certificate(.pem, .crt) and private key(.key)
<input checked="" type="radio"/> PFX Certificate	Upload a PFX certificate(.pfx) that includes the private key
<input type="radio"/> Certificate Store	Use an existing certificate stored by operating system

Below the table is the "Upload PFX Certificate" section, which includes two input fields:

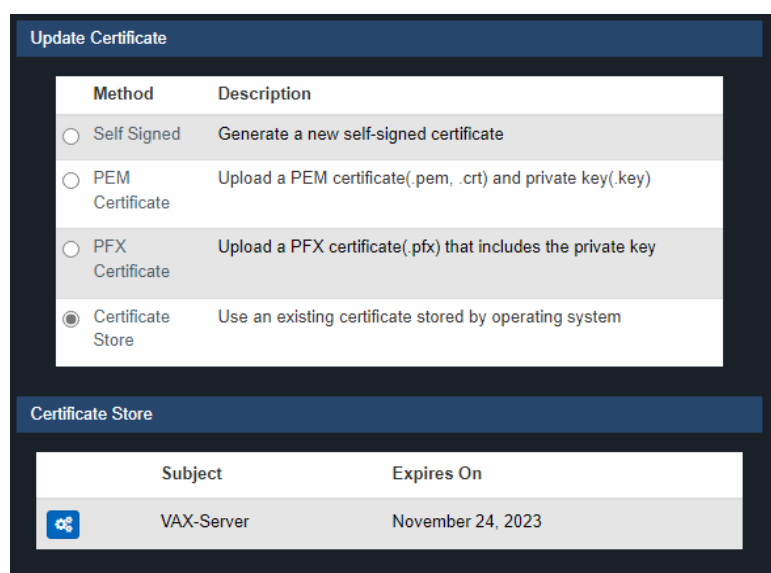
- Certificate (.pfx) with a "Choose File" button and "No file chosen" text.
- Password with an empty text input field.

An "Update" button is located at the bottom right of the form.

Almacenamiento de Certificados


En muchos casos, si la empresa que ejecuta el servidor tiene su propio certificado SSL en uso, también se puede usar para VAX. Es probable que estos certificados ya estén instalados en la PC o en el almacén de certificados de usuario y se puedan seleccionar y aplicar. Al igual que los otros métodos, los servicios se reiniciarán una vez que se complete la instalación del certificado. Los usuarios pueden verificar que el certificado esté funcionando navegando al servidor en un navegador web y verificando si el certificado se muestra como válido en el navegador web..

Figura 5.13.



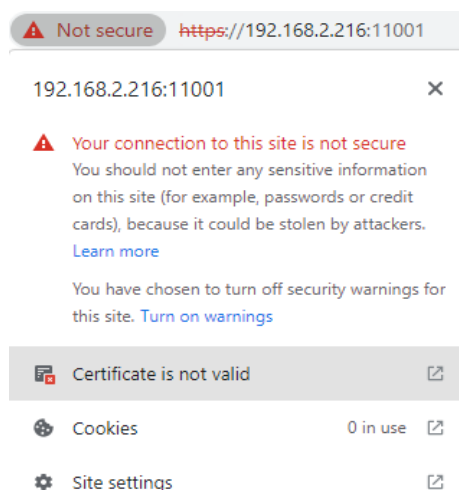
Instalación de un certificado en el almacén de certificados

Al usar un certificado auto firmado, como se mencionó anteriormente, al usuario se le presentará una página de Conexión no segura cuando navegue al servidor en un navegador web. Hay un método que se detallará a continuación para evitar.

 **Nota:** En realidad, esto no asegura la conexión ni valida el certificado. Este proceso difiere ligeramente entre navegadores web. La siguiente guía usará Google Chrome como plantilla.

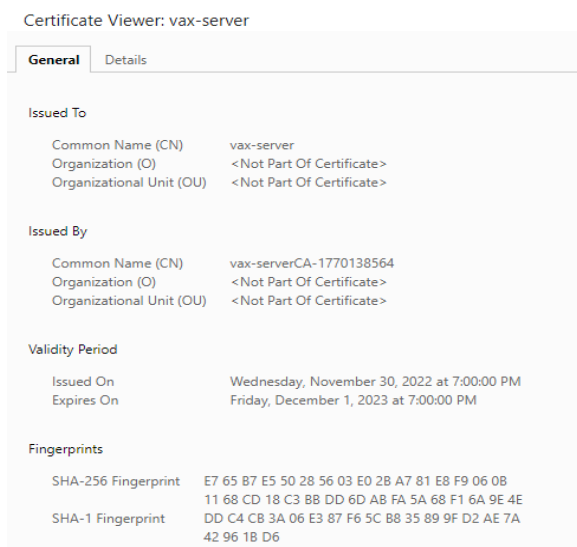
1. Busque el servidor en cuestión y haga clic donde dice **"Not Secure"** a la izquierda de la URL y haga clic en **"Certificate is not Valid"**

Figura 5.14.



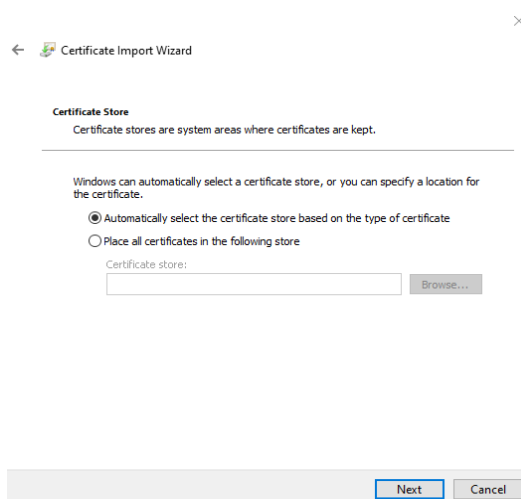
2. Aparecerá una nueva ventana, en la esquina inferior derecha habrá un botón "Exportar". Haga clic aquí y seleccione una ubicación para guardar el archivo del certificado.

Figura 5.15.



3. Haga doble clic en el archivo de certificado recién guardado. Esto presentará al usuario un asistente de importación de certificados SSL. Haga clic en "Instalar certificado" para comenzar el proceso. Al usuario se le presentará la ubicación de una tienda: elija "Máquina local" y haga clic en Siguiente.
4. Deje la opción predeterminada para permitir que Windows elija automáticamente la tienda en la que lo estamos instalando y haga clic en Siguiente. Esta última página le dará un resumen de los cambios, el usuario puede hacer clic en Finalizar aquí. Para ver esto en efecto, reinicie el navegador web y borre el caché del navegador. Ya no debería haber ningún mensaje sobre una conexión no segura. Para una mayor resolución de problemas, se recomienda comunicarse con su especialista de TI, ya que cualquier cosa más allá de esto queda fuera del alcance del soporte de Vicon

Figura 5.16.



Multi- Usuario

Multiusuario se configura desde la interfaz de usuario de System Manager. Consulte la sección llamada "Configuración del modo multiusuario" para obtener más información sobre esta función.

Capítulo 6. Planificación de una implementación de control de acceso

Este capítulo está destinado a ayudar a los técnicos en las etapas de planificación de las implementaciones de VAX y también puede ayudar a los usuarios finales y a los instaladores a comprender la terminología o los conceptos específicos de nuestro software. La sección de hardware cubrirá la topología de cómo se comunica nuestro producto, los cables y estándares comúnmente utilizados con nuestro producto y las referencias a los diagramas en otros capítulos de este libro. Las secciones de software repasarán el orden de las operaciones y los conceptos de los principales componentes del software.

Hardware

Esta sección repasará las especificaciones de hardware, la topología de comunicación de cómo nuestros paneles interactúan con el servidor VAX y cómo identificar un modelo de panel en el panel físico.

Hay 4 piezas principales de hardware que se utilizan en diferentes combinaciones. La siguiente tabla los describe.


 **Nota :** La siguiente tabla es una lista de subensamblajes. Al realizar el pedido, utilizará números de pieza separados que contendrán 1 o más de estos subconjuntos junto con accesorios, carcasas y otras piezas necesarias.

Tabla 6.1. Hardware – Placas controladoras

Hardware	Descripción
VAX-1D-1/ VAX-2D-1	Controlador de puerta alimentado por PoE con alimentación de cerradura integrada, relés auxiliares y entradas. Se comunica a través de Ethernet. Se puede pedir con varias opciones y configuraciones de firmware. Controla 1-2 puertas según el firmware cargado.
VAX-EXP-2D	Controlador de 1-2 puertas con alimentación de 12 V CC. Requiere VAX-MDK para comunicación y distribución de energía. Se comunica en bus RS485.
VAX-IO-EXP8- PCB	Controlador de entrada/salida con alimentación de 12 V CC. Requiere VAX-MDK para comunicación y distribución de energía. Se comunica en bus RS485.
VAX-MDK	Controlador con alimentación de 12-13,5 VCC. Comunica y distribuye energía a hasta 4 módulos VAX-EXP-2D como un controlador de 8 puertas o con hasta 8 módulos VAX-IO-EXP8-PCB para controlar hasta 64 entradas y salidas o hasta 64 pisos de ascensores (un VAX adicional -EXP-2D requerido para puertos de lectores de ascensores).

Especificaciones de Hardware

Figura 6.1. VAX-1D-1/VAX-2D-1

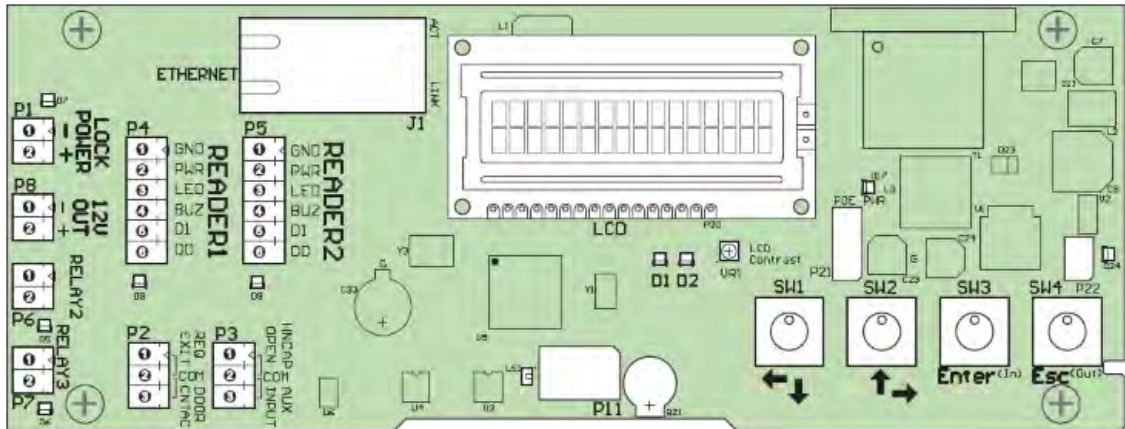


Tabla 6.2. Especificaciones de Hardware VAX-1D-1/VAX-2D-1

Categoría	Dispositivo y descripción
Voltaje - Alimentación	
Suministro	802.3af PoE (proporcionando hasta 20 W)
Alimentación de Cerradura	Estado sólido 12 VDC 500 mA / 24 VDC 250 mA (con convertidor opcional) con protección contra sobrecorriente
Salida auxiliar	12 VDC 500mA (compartido con los puertos del lector actual)
Red	
Velocidad	10/100 Mbps
Modos	Estática o DHCP
MAC	Única
Salidas / Entradas	
Relé de Puerta	1 relé de estado sólido de contacto húmedo.
Relés auxiliares	2 relés de estado sólido de contacto seco (límite de 24 V CC 1 A)
Entradas	4 x supervisor o digital (REX, contacto de puerta, abridor HDCP, auxiliar)
Lector	
Puerto del Lector	2 x Wiegand (D0, D1, BUZ, LED, VCC 12VDC 500mA, GND)
Interfaz de usuario	
LEDs	2 indicadores de alimentación. 2 indicadores de flujo de datos del lector 3 indicadores de estado del relé 2 indicadores de estado de Ethernet 2 x información a bordo 3 x información externa (PIR)
Pantalla LCD	1 x 16 canales, LCD de 2 líneas con retroiluminación
Pulsadores	4 interruptores táctiles.

Categoría	Dispositivo y descripción
Sonido	1 x 90 db Piezo
Movimiento Integrado	
Pasivos PIRs	Rendimiento de detección de 5.0m 94° Horizontal / 82° Vertical Área de Detección 64 Zona de Detección Consumo 170uA LED tricolor (rojo, verde, naranja)
Protección	
PoE	Límite de corriente de irrupción y límite de corriente general
Sobrecorriente	Cerradero de puerta, relés, salida de 12 VDC
Sobretensión	Cerradero de puerta, Lectores, Entradas
Sabotaje	Foto Sensor de manipulación
Mantenimiento del tiempo	
Fecha y hora	1 x reloj en tiempo real a bordo (no requiere batería; se mantiene hasta 1 mes sin energía)
Memoria	
Memoria Flash	8.0 Mb
Carcasa y placa trasera	
Plástico ABS moldeado	Cubierta extraíble para acceso rápido Placa posterior de montaje en superficie plana con puerto de cableado Disponible en acabado negro mate; Blanco o pintable
Opciones	
Zumbador ruidoso	100 db a 100 cm (3 pies)
Convertidor de contacto seco	Convierte el contacto húmedo en seco
Tarjetas de Expansión	Memoria adicional, paneles de expansión del elevador, E/S (para capacidad de expansión futura)
Módulo enchufable RS-485	Se utiliza para comunicarse con los productos Assa Abloy Aperio y las placas de expansión de ascensores

Figura 6.2. VAX-EXP-2D

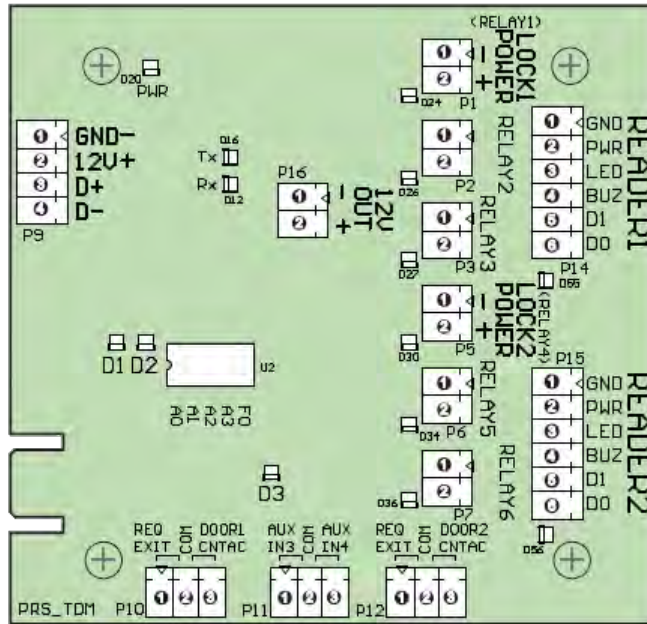


Table 6.3. Especificaciones de Hardware VAX-EXP-2D

Categoría	Dispositivo y descripción
Alimentación	
Suministro	1 entrada de alimentación de 12 VDC proporcionada por VAX-MDK o desde una fuente de alimentación externa. Hasta 1,25A aproximadamente.
Alimentación de Cerradura	2 x estado sólido 12 VDC 500 mA / 24 VDC 250 mA (con convertidor opcional) con protección contra sobrecorriente
Salida auxiliar	1 x 12 VDC 350mA (compartido con los puertos del lector de corriente)
Red	
Comunicación	Bus RS485 comunicándose con VAX-MDK. Compatible con configuración estrella o en cadena
Entradas / Salidas	
Relé de Puerta	2 relés de estado sólido de contacto húmedo 12 VDC 500 mA
Relés auxiliares	4 relés de estado sólido de contacto seco (límite de 24 VDC 1 A)
Entradas	6 x supervisor o digital (REX, contacto de puerta, abridor HDCP, auxiliar)
Lector	
Puerto de lector	2 x Wiegand (D0, D1, BUZ, LED, VCC 12VDC 350mA, GND)
Interfaz de usuario	
LEDs	2 indicadores de potencia. 2 indicadores de flujo de datos del lector 6 indicadores de estado del relé 2 indicadores de estado RS485 2 x información a bordo
Protección	
Entrada 12VDC	Límite de corriente de arranque y límite de corriente general

Categoría	Dispositivo y descripción
Sobrecorriente	Cerradero de puerta, relés, salida de 12 VDC
Sobretensión	Cerradero de puerta, Lectores, Entradas
Sabotaje	Foto Sensor de manipulación
Dimensiones	
Caja de acero	29 cm (ancho) x 43,5 cm (alto) x 7,5 cm (profundidad) (11,41" x 17,41" x 2,95")
Dimensiones de PCB	9,5 cm (ancho) x 9 cm (alto) (3,740" x 3,543").
Opciones	
Zumbador ruidoso	100 db a 100 cm (3 pies)
Convertidor de 24 VDC	Convierte 12 VCC a 24 VCC
Convertidor de contacto seco	Convierte el contacto húmedo en seco

Figura 6.3. VAX-IO-EXP8-PCB

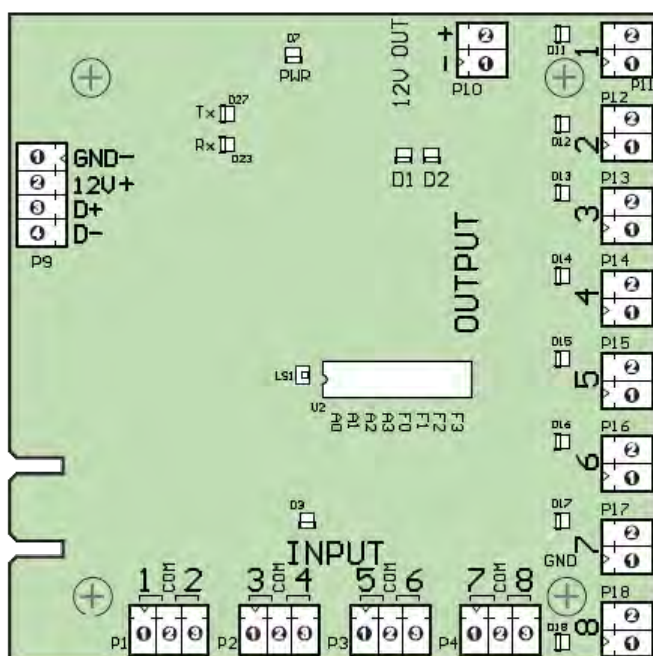


Table 6.4. Hardware Specifications VAX-IO-EXP8-PCB

Categoría	Dispositivo y descripción
Alimentación	
Suministro	1 entrada de alimentación de 12 VDC proporcionada por VAX-MDK o desde una fuente de alimentación externa. Hasta 0.35A aproximadamente.
Salida auxiliar	1 x 12 VDC 350mA
Red	
Comunicación	Bus RS485 comunicándose con VAX-MDK. Compatible con configuración estrelal o en cadena
Entradas / Salidas	
Relés auxiliares	8 relés de estado sólido de contacto seco (límite de 30 VDC 1 A)
Entradas	8 x Supervisor o Digital
Interfaz de usuario	

Categoría	Dispositivo y descripción
LEDs	1 indicador de potencia.
	8 indicadores de estado de relé.
	2 indicadores de estado RS485
	2 información integrada
	1 actividad de entrada
Proteccion	
Entrada 12VDC	Límite de corriente de arranque y límite de corriente general
Sabotaje	Foto sensor de manipulación
Dimensiones	
Caja de acero	29 cm (ancho) x 43,5 cm (alto) x 7,5 cm (profundidad) (11,41" x 17,41" x 2,95")
Dimensiones de PCB	9,5 cm (ancho) x 9,5 cm (alto) (3,740" x 3,740").
Options	
Zumbador ruidoso	100 db a 100 cm (3 pies)
Convertidor de contacto seco	Convierte el contacto húmedo en seco

Figura 6.4. VAX-MDK

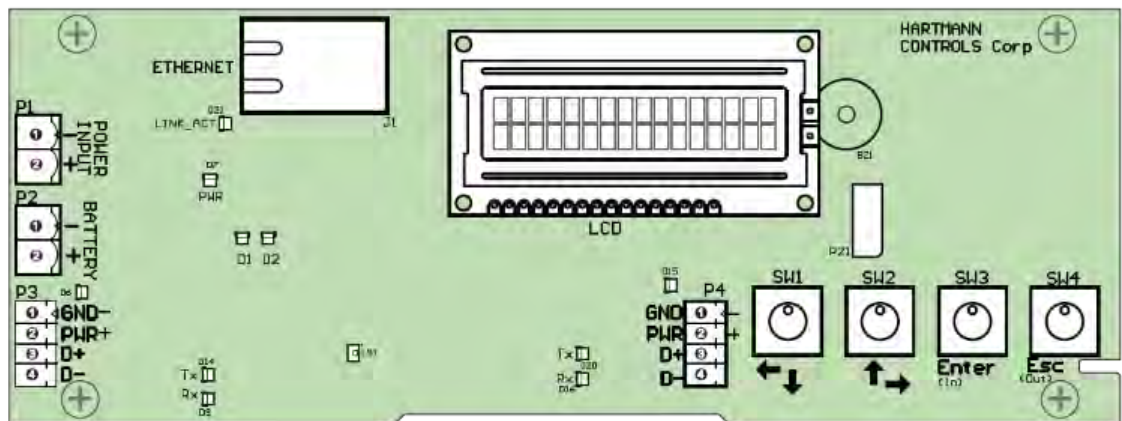


Tabla 6.5. Especificaciones de hardware VAX-MDK

Categoría	Dispositivo y descripción
Alimentacion	
Suministro	1 entrada de 12-13,8 VDC. Hasta 6A de corriente. 5A típico.
Batería de reserva	1 x conexión a respaldo de batería externa suplementaria (12-13.8VDC in). La energía de respaldo principal debe ubicarse en una fuente de alimentación externa.
Potencia de salida	2 salidas de 12 VDC para conexión a módulos VAX-IO-EXP8-PCB o VAX-EXP-2D. Hasta 2,5A por salida. 5A totales.
Red	
Velocidad	10/100 Mbps
Modos	Estática o DHCP
MAC	Única
Comunicacion	2 x salidas RS485 para comunicación con hasta 4 módulos VAX-EXP-2D u 8 módulos VAX-IO-EXP8-PCB

Categoría	Dispositivo y descripción
Interfaz de usuario	
LEDs	3 indicadores de potencia. 1 indicador de estado de Ethernet 2 x información a bordo 4 indicadores de estado RS485
Pantalla LCD	1 x 16 canales, LCD de 2 líneas con retroiluminación
Pulsadores	4 interruptores táctiles.
Sonido	1 piezoeléctrico de 90 db
Protección	
Sobrecorriente	Salidas de 12 VCC
Sobretensión	Entrada de 12-13,8 VDC
Sabotaje	Foto sensor de manipulación
Mantenimiento del tiempo	
Fecha y hora	1 x reloj en tiempo real a bordo mantiene hasta 1 mes sin energía)
Dimensiones	
Caja de acero	29 cm (ancho) x 43,5 cm (alto) x 7,5 cm (profundidad) (11,41" x 17,41" x 2,95")
Dimensiones de PCB	9,5 cm (ancho) x 9,5 cm (alto) (3,740" x 3,740").

Topología de comunicación

Esta sección repasa la topología de comunicación general de una implementación de VAX.

Los controladores de puerta VAX-1D-1 y VAX-2D-1 de Vicon Industries funcionan con Power-over-Ethernet (PoE). Esta energía se proporciona a través de un conmutador de red PoE o un inyector PoE. Los controladores se comunican por TCP/IP a través de un cable Cat5e/Cat6, a menudo a través del mismo cable del que recibe energía.

Los controladores de puertas, E/S y ascensores con alimentación de 12 VDC, como el VAX-MDK, no utilizan PoE, pero la topología de la red es la misma.

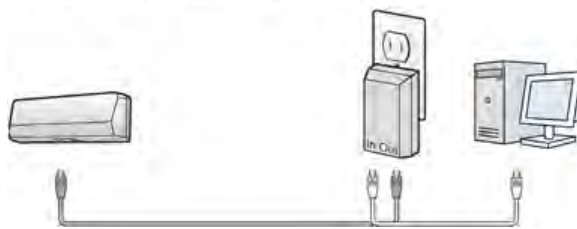
A continuación, tenemos varios ejemplos de configuración de cómo los controladores pueden comunicarse a través de una variedad de infraestructuras de red.

Alimentación PoE: puede suministrarse directamente mediante un conmutador o, alternativamente, inyectarse a través de un inyector de un solo puerto entre el conmutador/enrutador y el controlador.



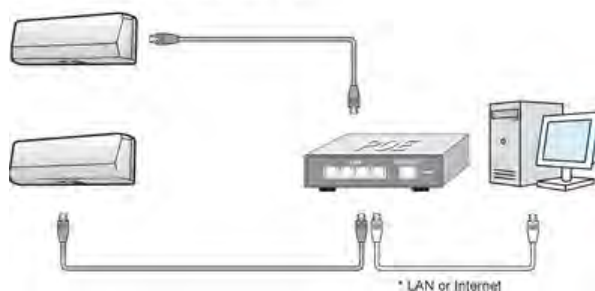
Controlador - Inyector PoE - PC (directo). En este escenario, el controlador está alimentado por un inyector PoE que está conectado directamente al servidor VAX. Escenarios como este suceden mucho cuando no hay mucha infraestructura de red para trabajar.

Controller - POE Injector - PC (Direct)



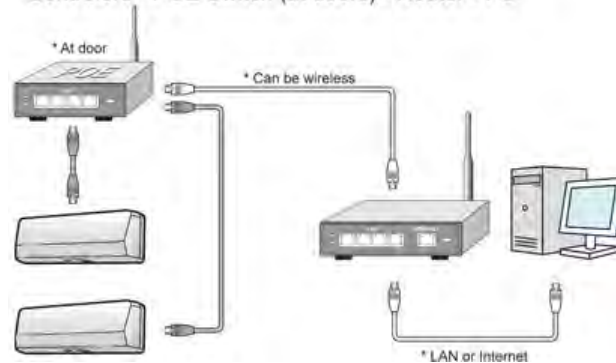
Controladores - Switch/Router PoE - PC. Este es un escenario más típico y se ve con bastante frecuencia en el campo. Los controladores están alimentados por un conmutador PoE (ubicado en un armario o sala eléctrica), que se conecta al servidor en el sitio utilizando la infraestructura de red existente del sitio, o un servidor externo a través de una conexión a Internet.

Controllers - POE Router - PC

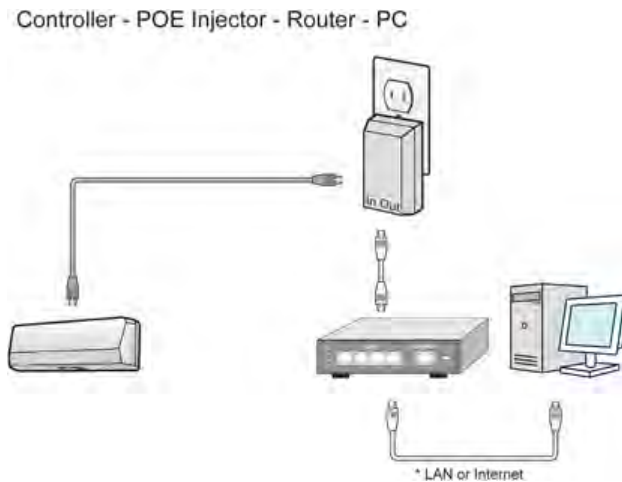


Controladores - Switch PoE (en puertas) - Router/Switch - PC. En este escenario, los controladores están alimentados por un conmutador PoE (encima/cerca de la puerta), que se conecta (de forma inalámbrica o con un solo cable) a la infraestructura de red existente del sitio o a un servidor externo a través de una conexión a Internet. Esta topología se usa cuando es difícil llevar Cat5e a la puerta o cuando las puertas están muy cerca una de la otra.

Controllers - POE Switch (at doors) - Router - PC



Controlador - Inyector PoE - Router/Switch - PC. En este escenario, el VAX-1D está alimentado por un inyector PoE que está conectado a la infraestructura de red del sitio. Este ejemplo se ve mucho en sitios de una sola puerta donde no es rentable comprar un conmutador PoE.



Como puede ver, el VAX-1D-1 puede ser muy flexible en la forma en que se implementa en un sitio, y se pueden implementar varios paneles en cualquier combinación de los ejemplos anteriores.

Cables, Estándares y Mejores Prácticas

Esta sección incluye una lista de especificaciones de cables que se utilizan con nuestro hardware, referencias a diagramas visuales y algunas mejores prácticas para implementaciones de sistemas Vicon VAX.

Especificaciones y estándares de cables

Esta sección contiene información sobre varios estándares de cable utilizados con nuestros productos.

Tabla 6.6. Estándares de cables

Nombre	Max. Distancia	Tipo de cable (use un calibre más grueso para recorridos más largos)	Codigo
Cable PoE	100 m (328')	Par trenzado, 4 pares	Cat5 100Base-T o mejor
cable del lector	152 m (500')	6 conductores trenzados (no trenzados), 24 AWG o más gruesos. En general blindado.	Belden 9537 o equivalente
Cable de cerradura de puerta	152 m (500')	2 conductores trenzados 18 AWG	Belden 9740 o equivalente
cable de salida	152 m (500')	2 conductores trenzados 22 AWG	Belden 8740 o equivalente
cable de entrada	152 m (500')	2 conductores trenzados 22 AWG	Belden 8740 o equivalente
Cable RS-485 con alimentación	600 m (2000')	4 conductores trenzados, par trenzado, 2 pares, 22 ~ 16 AWG, blindado	Belden 9402 o equivalente

VAX-MDK Requisitos de energía

Esta sección repasará los requisitos de alimentación de los paneles de estilo de 12 VDC.

El VAX-MDK requerirá entre 1,5 A y 6 A a 12-13,8 VDC de la fuente de alimentación externa.

A continuación, se describe la distribución de energía desde un controlador VAX-MDK a los módulos de expansión VAX-EX-P-2D conectados a través de los puertos PVAX-MDK P3 y P4 en una configuración de puerta (hasta 4 VAX-EXP-2D que equivalen a 8 puertas). /lectores, que es la configuración máxima) y qué pasos se deben seguir para garantizar que haya suficiente corriente disponible para los periféricos conectados, como lectores, cerraduras electrificadas y consumo de salida de 12 VCC utilizado opcionalmente.

El único controlador VAX-MDK y los cuatro módulos VAX-EXP-2D requieren un total de 50 mA para el funcionamiento de la placa. Esto excluye cualquier dispositivo conectado y alimentado desde el puerto de salida de 12 VDC P16 de un VAX-EXP-2D. También se considera un porcentaje actual disponible del 10%.

Cada punto de distribución de energía en un VAX-MDK (puerto de salida P3 y P4) puede proporcionar hasta 2,5 A máx. a su banco de módulos de expansión conectados mediante cableado directo o interconexión de datos y regletas. Ni el consumo del banco n.º 1 ni el del banco n.º 2 pueden superar los 2,5 A cada uno. En el caso de que se requiera corriente adicional para alimentar un dispositivo conectado, es posible que se requiera la implementación de un suministro limitado de energía secundario de clase 2 de bajo voltaje listado por UL para reducir la carga de corriente del banco a 2,5 A o menos.

Each power bank should be calculated as:

(Cantidad de VAX-EXP-2D x 10 mA) + (Cantidad de lectores x Valor nominal máximo del lector en mA) + (N.º de impulsos activados x Cantidad de impulsos de impulso en mA) + (Cantidad de dispositivos conectados a una salida de 12 VDC x Valor nominal del dispositivo en mA)

Ejemplo 6.1. Ejemplo de cálculo de energía

En sistema de ocho puertas que usa cerraduras con clasificación de 380 mA en todas las puertas, ocho puertas que usan un lector de proximidad estándar con clasificación de 80 mA sin dispositivos adicionales conectados a la alimentación.

Banco #1: (2 VAX-EXP-2D x 10mA) + (4 lectores x 80mA) (4 disparos x 380mA) + (0 dispositivos x 0mA) = 1860mA (1.86A)

Banco #2: (2 VAX-EXP-2D x 10mA) + (4 lectores x 80mA) (4 disparos x 380mA) + (0 dispositivos x 0mA) = 1860mA (1.86A)

Ahora que se determina el consumo de cada banco, la disponibilidad de corriente de fuente de alimentación externa mínima estimada que figura en la lista de UL para aVAX-MDK se calcula como se indica a continuación: (Banco n.º 1 + Banco n.º 2) + ((Banco n.º 1 + Banco n.º 2) x 10 %) + 10mA

Corriente nominal mínima de la fuente de alimentación = (1,86 + 1,86) + ((1,86 + 1,86) x 10 %) = 4092 mA (4,09 A)

Identificación de un Panel

Esta sección cubre cómo identificar el modelo de un Panel físicamente y en el software.

Vicon Industries diseña y fabrica una variedad de modelos de paneles para satisfacer las necesidades de una variedad de implementaciones. La siguiente tabla enumera cada modelo y las características únicas de cada modelo.

Tabla 6.7. Referencia del modelo de panel

Modelo	Max. Puertas	Max Lector	Movimiento REX	Breve explicación
VAX-MDK-Door-Master-OSDP (MDK_MASTER)	8	8	No	Controlador de 1 a 8 puertas de estilo tradicional montado en una caja de acero compatible con OSDP V2. Hasta 8 puertas por controlador VAX-MDK con la cantidad adecuada de tarjetas de expansión de dos puertas VAX-EXP-2D. Alimentado a través de una fuente de alimentación externa de 12 VDCC
VAX-MDK-Door-Master (MDK_MASTER)	8	8	No	Controlador de 1-8 puertas estilo tradicional montado en una caja de acero. Hasta 8 puertas por controlador VAX-MDK con la cantidad adecuada de tarjetas de expansión de dos puertas VAX-EXP-2D. Alimentado a través de una fuente de alimentación externa de 12 VDC
VAX-IO-STR-2	N/A	N/A	N/A	Admite dispositivos generales de entrada/salida en varios casos de uso y configuraciones. Hasta 64 entradas / salidas por panel VAX-MDK con 8 placas E/S. Alimentado por una fuente externa de 12 VDC.
VAX-IO-STR	N/A	N/A	N/A	VAX-IO-STR-2 recomendado para nuevas instalaciones. Admite dispositivos generales de entrada/salida en varios casos de uso y configuraciones. Hasta 64 Entradas / Salidas con 8 placas de E/S. Alimentación PoE.
VAX-ELV-STR-2	N/A	N/A	N/A	Admite control de acceso a cabinas de ascensores en varias configuraciones con tarjetas de expansión. Hasta 64 Pisos por cabina con la cantidad adecuada de Placas de Expansión. Alimentado a través de una fuente de alimentación externa de 12 VDC.
POE-Elevator-64	N/A	N/A	N/A	Se recomienda VAX-ELV-STR-2 para nuevas instalaciones. Admite control de acceso a cabinas de ascensores en varias configuraciones con tarjetas de expansión. Hasta 64 Pisos por cabina con la cantidad adecuada de Placas de Expansión. Alimentación PoE.
POE-APERIO-8	8	8	No	Controlador maestro ASSA ABLOY Aperio capaz de controlar hasta 8 dispositivos Aperio a través de 1 a 8 concentradores Aperio con alimentación PoE
VAX-2D-1	2	2	No	Controlador de dos puertas con alimentación PoE
VAX-2D-1-REX	2	2	Si	Controlador de dos puertas con alimentación PoE y movimiento integrado
VAX-1D-1	1	2	No	Controlador de puerta única con alimentación PoE
VAX-1D-REX-1	1	1	Si	Controlador de puerta única con alimentación PoE y movimiento integrado

Todos los paneles de Vicon Industries se prueban por completo antes del envío y, una vez que la prueba es exitosa, el panel recibe el sello de aprobación de Vicon Industries en forma de una etiqueta en el panel a la derecha de la pantalla LCD. Esta etiqueta contiene el modelo y el número de serie, que se utiliza para fines de garantía.

Si no se puede acceder fácilmente al Panel, pero está conectado a la red, puede identificar el Panel iniciando sesión en la interfaz web del Panel y verificando la versión del firmware. Para obtener más información sobre cómo acceder a la interfaz web del Panel, consulte la sección llamada "Interfaz de configuración HTTP del Panel".

Software

Este capítulo entra en gran detalle sobre los conceptos de configuración de software específicos para VAX. Cada sección de configuración también proporciona enlaces a los capítulos de configuración asociados con el concepto del tema. Ya sea que sea nuevo o esté bien versado en el control de acceso, este es el capítulo más importante de este libro.

Orden de Operaciones

La configuración de VAX es bastante flexible, sin embargo, hay un orden general de operaciones que se debe cumplir.

Esta tabla pretende ser una descripción y una guía general para el orden de configuración. Cada elemento entrará en más detalle más adelante en este capítulo.

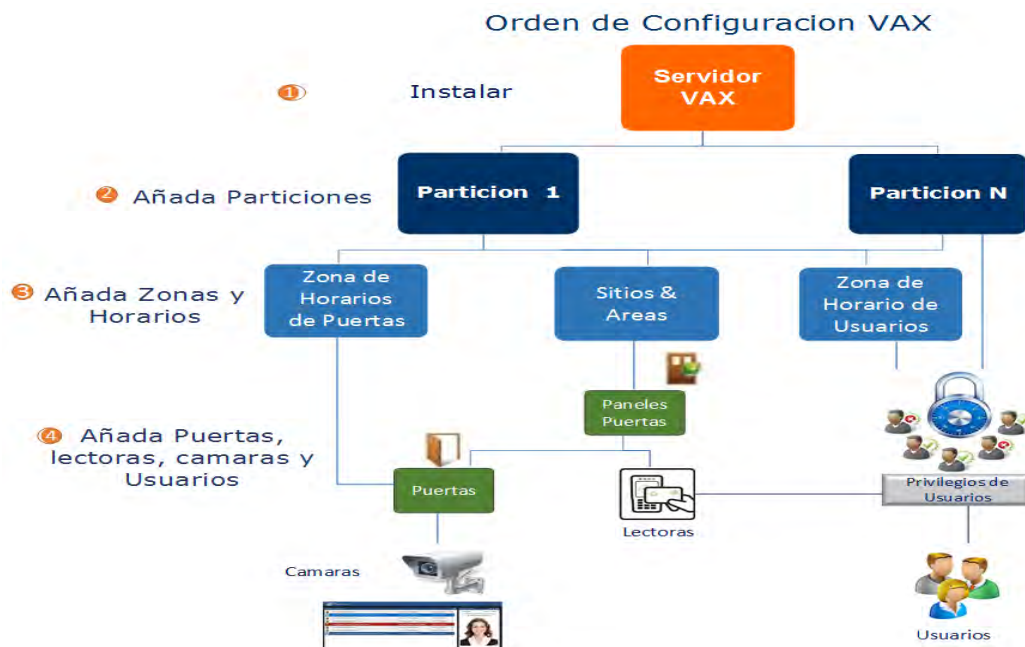
Tabla 6.8. Orden de Operaciones: Configuración del Software

#	Elemento de configuración	Orden de configuración	Notas adicionales
1	Particiones	La base de cualquier configuración debe completarse primero.	La partición predeterminada se puede usar de manera efectiva en sitios pequeños, implementaciones de una sola puerta o instancias donde no se requiere un control administrativo detallado.
2	Sitios	Debe configurarse después de finalizar las particiones.	El sitio predeterminado se puede usar de manera efectiva en implementaciones pequeñas; recomendamos cambiar el nombre del Sitio a su ubicación para una mejor comprensión visual.
3	Paneles	Debe configurarse después de finalizar los sitios. Una vez asociado con un sitio, puede cambiar con qué sitio está asociado el panel (solo dentro de la misma partición).	Si se configura antes de estar en el sitio: si no puede obtener las direcciones MAC de los paneles, use direcciones MAC de marcador de posición como "123456789123".
4	Horarios de puerta/piso	Configure cronogramas de puerta / piso adicionales si es necesario; se puede hacer antes o después de agregar Puertas y Ascensores. Recomendamos hacerlo antes.	Los horarios de puerta predeterminados "Acceso siempre con tarjeta", "Siempre desbloqueado", "Bloqueado", "Acceso con tarjeta 9-5" se pueden renombrar y enviar mensajes para adaptarse a las necesidades de implementación.
5	Puertas / Ascensores	Las puertas/elevadores deben configurarse después de que se hayan finalizado los cronogramas de puertas/pisos y deben configurarse después de agregar los paneles.	Los lectores (que se encuentran en Configuración de la puerta) también deben configurarse antes de los siguientes pasos.

6	Horarios de usuario	Los horarios de usuario deben configurarse después de las particiones y antes del grupo de privilegios de acceso.	Los horarios de usuario predeterminados "Acceso siempre", "Sin acceso" y "Acceso de 9:00 a. m. a 5:00 p. m." se pueden renombrar y enviar mensajes para adaptarse a las necesidades de implementación.
7	Grupos de privilegios de acceso	Las particiones, los horarios de usuario, las puertas y los lectores deben configurarse previamente.	Debe planificarse/configurarse con el cliente.
8	Usuarios	Debe configurarse después de Particiones, Grupos de privilegios de acceso, Puertas/ Lectores y Grupo de privilegios de acceso.	Si no tiene ningún grupo de privilegios de acceso, puede asignar un usuario a una partición.

La siguiente es una visualización de la tabla.

Figura 6.5. Orden de configuración VAX



Particiones

En esta sección cubriremos los conceptos básicos del particionamiento dentro del VAX. También cubriremos algunos ejemplos básicos de cómo se ha utilizado el particionamiento en el campo. Para la configuración de particiones, consulte el Capítulo 19, Configuración de particiones y sitios.

Conceptos

La palabra "**Particiones**" tiene varios significados literales y figurativos en muchos aspectos de la seguridad, la tecnología de la información, el derecho e incluso las matemáticas. En el contexto de VAX, el particionamiento es un método para separar lógicamente el sistema de control de acceso en distintas secciones y definir permisos específicos para los administradores. Para obtener más información sobre la **configuración del administrador**, visite el *Capítulo 20, Administradores y privilegios*.

Factores para tener en cuenta al planificar una implementación de VAX que pueden afectar si la implementación utilizará particiones:

- ¿La implementación abarcará varios edificios/sitios?
- ¿Quién administrará el sistema una vez implementado? (Recepcionista, personal de seguridad, encargados del edificio, etc.)
- ¿Podría la implementación beneficiarse de la segregación de partes del sistema?
- Si es un distribuidor certificado de Vicon Industries, tómese un momento para consultar al cliente y escuchar su opinión sobre si sería apropiado segregar el sistema.

Esquema de nombres para particiones. Durante la planificación de la implementación, deberá tener en cuenta un esquema de nomenclatura coherente para sus particiones y sitios. Puede nombrar las particiones como desee, siempre que pueda comprender qué son exactamente. En muchos casos, los sitios se nombran exactamente o de manera muy similar a la partición a la que están asignados.

Ejemplos

Esta sección cubrirá varios ejemplos del uso de la característica de partición. Los nombres y empresas en estos ejemplos son arbitrarios.

Ejemplo 1: Sistema Escolar. Una junta escolar tiene Paneles VAX configurados en tres escuelas diferentes (A, B y C), con un solo servidor VAX en la oficina central. En un sistema plano tradicional, un administrador en el software de control de acceso tendría acceso a todas las puertas en las tres escuelas. Usando el Particionamiento, podemos tener tres Particiones diferentes (A, B y C) y crear una cuenta de Administrador para cada escuela. Ahora cada escuela solo tiene control sobre su propio sistema, lo que reduce el riesgo de problemas de configuración y limpia la interfaz de cada cuenta de administrador con solo información relevante para ellos.

Ejemplo 2: Compañía de administración de condominios. Una empresa de administración de condominios está utilizando VAX para administrar varios sitios de condominios en varias ubicaciones. Las puertas que administran incluyen entradas principales, puertas de estacionamiento, cuartos de lavado, almacenamiento y basura/reciclaje en cada edificio. Mediante el uso de particiones, pueden crear un esquema de nomenclatura consistente y agilizar la gestión de particiones individuales.

Ejemplo 3: Oficina/Centro de datos. Una oficina con un centro de datos en el sitio está utilizando el controlador de puertas de Vicon Industries para administrar el centro de datos y la entrada pública. Usando Particiones, el propietario puede crear dos Particiones. Uno para la puerta principal y otro para la entrada del centro de datos. Ahora el propietario puede crear una cuenta administrativa para la puerta principal para dársela a la recepcionista. Esto le da al propietario más control sobre a quién se le puede otorgar acceso al centro de datos. También podría darle a la cuenta de administrador de la recepcionista la capacidad de ver eventos para la entrada del centro de datos, pero no darle control sobre agregar usuarios o anular la puerta del centro de datos.

Sitios

En esta sección, repasaremos los sitios y cómo interactúan con las particiones, los paneles y otros aspectos de VAX.

Los sitios son el método en el que los paneles se asocian con las particiones. No puede asignar directamente un Panel a una Partición; primero debe crear un sitio en la partición y luego asignar el panel al sitio asignado a la partición en la que debe estar el panel. Si usa una sola partición, los sitios pueden ser útiles para separar su implementación en secciones para facilitar la administración. los ojos, especialmente cuando tiene varias puertas de entrada en varios edificios. Si los Paneles residirán en Programaciones diferentes, se recomienda separar esos Paneles en Sitios separados; esto asegurará que los Paneles siempre informen eventos en el Programa aplicable a su ubicación.

Ejemplos

Esta sección cubrirá varios ejemplos de Sitios que se utilizan. Los nombres y empresas en estos ejemplos son arbitrarios.

Ejemplo 1: Hospital. Un hospital con varios edificios en un área pequeña utiliza paneles de puerta VAX. Al utilizar Sitios, cada edificio puede ser su propio Sitio y los objetos tales como Horarios de Usuario, Horarios de Puertas, Días Festivos y Grupos de Privilegios de Acceso pueden usarse en todo el sistema de control de acceso. Quizás en este mismo escenario, un administrador crea una partición separada para el personal administrativo. Estos usuarios se pueden compartir en varias particiones, pero requerirían sus propios horarios de usuario y grupos de privilegios de acceso.

Ejemplo 2: Gobierno Municipal. El gobierno de una ciudad ha optado por utilizar VAX para gestionar sus puertas en oficinas e instalaciones. Con Sites, el administrador del edificio crea un Site para el ayuntamiento, los edificios de gestión del agua, las estaciones de bomberos e incluso los centros comunitarios. Los sitios y las particiones se pueden usar en este escenario para simplificar la administración y crear separadores lógicos. Por ejemplo, el centro comunitario probablemente sería su propia partición y podría ser administrado por personal en el sitio mientras se mantiene una autoridad central en el ayuntamiento.

Horarios de Puertas

En esta sección, cubriremos los conceptos de **Horarios de puerta** dentro de VAX y un par de ejemplos de Horarios de puerta que se utilizan en el campo. Para la configuración de Horarios de puertas, consulte el *Capítulo 9, Configuración de Horarios de puertas*.

Conceptos

Los horarios de las puertas son cómo podemos configurar las puertas para que se comporten y cuándo queremos que se comporten así. Los horarios de las puertas en VAX son muy flexibles. Las puertas actualmente tienen 8 estados diferentes en los que pueden estar, y existen varios métodos para cambiar estos estados, que incluyen: **anulaciones de puertas, zonas de ejecución única (OTR) y acciones de deslizamiento triple**. Un horario de puerta puede cambiar hasta 20 veces al día, sin incluir anulaciones, OTR y acciones de deslizamiento triple. La siguiente sección muestra los 8 estados de puerta y una breve explicación de lo que significan.

Cierre de emergencia. Cuando se usa el **rojo** para definir un período o una zona dentro de un horario, la acción resultante es que la Puerta que usa este Horario ahora está en un estado seguro (bloqueado). No se permite ningún acceso a través de credencial o que el titular de tarjeta atraviese una puerta en un estado de bloqueo, a menos que el titular de la tarjeta tenga su configuración 'es *Master*' activada dentro de su cuenta.

Solo Tarjeta. Cuando se usa el **amarillo** para definir un período o una zona dentro de un horario, la acción resultante es que la puerta que usa este horario ahora está en un estado seguro (bloqueada). Junto con una combinación de lector de proximidad / teclado o lector de proximidad estándar, requiere la presentación de una *tarjeta válida* para permitir el acceso a través de la puerta.

Pin Solo. Cuando se usa el **azul** para definir un período o una zona dentro de un horario, la acción resultante es que la Puerta que usa este Horario ahora está en un estado seguro (bloqueado). Junto con una combinación de Lector de proximidad/teclado o Lector solo de teclado, requiere una *entrada de PIN válida* en el teclado para permitir el acceso a través de la Puerta.

Tarjeta o Pin. Cuando se usa **agua** para definir un período o una zona dentro de un horario, la acción resultante es que la Puerta que usa este Horario ahora está en un estado seguro (bloqueado). Junto con una combinación de Lector de proximidad / teclado, solo de teclado o Lector de proximidad estándar, requiere la presentación de una *tarjeta válida o la entrada de PIN* en el teclado para permitir el acceso a través de la puerta.

Tarjeta y Pin. Cuando se usa el **violeta** para definir un período o una zona dentro de un horario, la acción resultante es que la puerta que usa este horario ahora está en un estado seguro (bloqueado). Junto con una combinación de lector de proximidad / teclado, requiere la presentación de una *tarjeta válida y la entrada del PIN en el teclado (en ese orden)* para permitir el acceso a través de la puerta.

Desbloqueado - Cuando se usa **verde** para definir un período o una zona dentro de un horario de horario, la acción resultante es que la puerta que usa este horario ahora está en un estado público (desbloqueado), y *no requiere una credencial válida* para otorgar acceso a través de la puerta.

Entrada de la primera credencial. Cuando se usa **verde claro** para definir un período o una zona dentro de un horario, la acción resultante es que la puerta que usa este horario ahora está en un estado seguro (bloqueado) en un modo de '**Esperando credencial**', esperando que se presente una *tarjeta válida o entrada de PIN* válida antes de cambiar el estado a un estado público (o desbloqueado).

Solo los tarjetahabientes con la opción '*Primera entrada de tarjeta habilitada*' incluida en su perfil de usuario cambiarán el estado del Horario a Público. Se puede otorgar acceso a otros titulares de tarjetas en función de su regla de privilegio de acceso particular, pero la puerta permanecerá en un modo seguro: en espera de credencial.

El uso típico de "Entrada de la primera credencial" es evitar la entrada no autorizada a una instalación en función de un horario de puerta pública. Por ejemplo, no querrá que la puerta se abra a menos que haya un empleado dentro del edificio.

Doble Credencial. Cuando se usa el **gris** para definir un período o una zona dentro de un horario, la acción resultante es que la Puerta que usa este Horario ahora está en un estado seguro (bloqueado). Para que se otorgue el acceso, se deben presentar *dos credenciales válidas al lector dentro de los 5 segundos de diferencia antes de que la puerta se desbloquee y otorgue el acceso*. Para mayor seguridad, puede configurar la puerta para que solo acepte una credencial dual si la primera credencial presentada tiene el privilegio de usuario '**Supervisor**'. Esta opción se puede configurar en la pestaña **Opciones de la pantalla Editar puerta**.

Factores de horario de la puerta. Los factores para tener en cuenta al planificar sus horarios de puerta incluyen los siguientes:

- ¿Tendrá la implementación una Puerta pública? Si es así, ¿cuándo debería esa puerta cambiar a un estado bloqueado? ¿Debe esa puerta usar la **primera tarjeta en entrar**?
- ¿La implementación utiliza una combinación de proximidad/teclados numéricos? ¿Alguna de estas puertas requiere **tarjeta y PIN / Tarjeta o PIN / Pin solamente**?
- ¿Hay ubicaciones ultra seguras dentro de las implementaciones (centros de datos, bóvedas, etc.)? ¿Se beneficiarían de un horario de puerta con **tarjeta y PIN o credencial doble**?

Planificación de un horario de puerta. Al planificar su implementación de control de acceso, deberá preguntarse a sí mismo (y/o al cliente) cómo les gustaría que se comportaran sus puertas. Cualquier combinación de estados de puerta se puede programar en un programa de puerta y se puede aplicar a varias puertas.

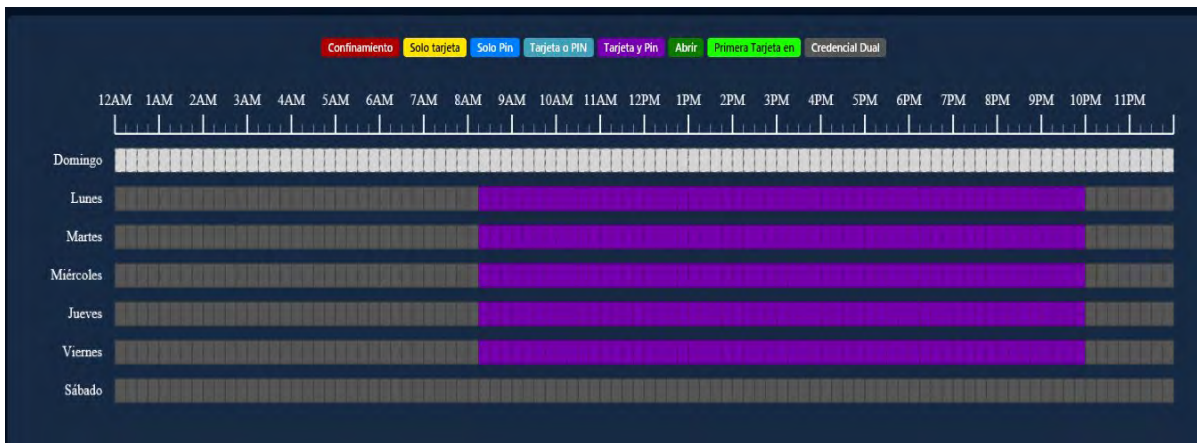
Ejemplos

Esta sección repasará algunos ejemplos del mundo real de horarios de puertas y puede ayudarlo a visualizar cómo se ven estos horarios de puertas en el software.

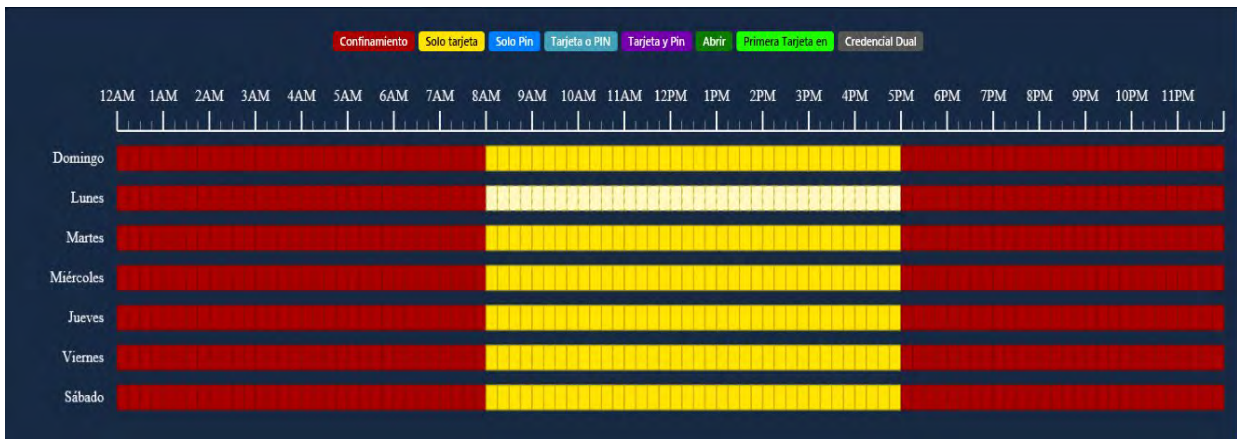
Ejemplo 1: Entrada pública de una tienda de comestibles. En este ejemplo, tenemos un horario de puerta que se asignará a la puerta pública principal de una tienda de comestibles; está configurada para **Desbloquear** durante el horario de atención de la tienda y, de lo contrario, la tarjeta solo para el personal.



Ejemplo 2: Puerta del centro de datos. En este ejemplo, tenemos un horario de puerta de alta seguridad que se asignará a la entrada del centro de datos; este Horario utiliza **Tarjeta y PIN** durante el horario de oficina, y **Doble Credencial** fuera del horario laboral



Ejemplo 3: Entrada de empleados de oficina. En este ejemplo, tenemos una tarjeta de acceso Horario de 9 a 5 Puertas que será asignada a la Puerta principal de una oficina. Este es uno de los horarios de puerta predeterminados incluidos en VAX.



Horarios de usuarios

En esta sección, cubriremos los conceptos de horarios de usuario dentro de VAX y un ejemplo de un horario de usuario. Para la configuración de Horarios de usuario, *consulte el Capítulo 10, Horarios de usuario*.

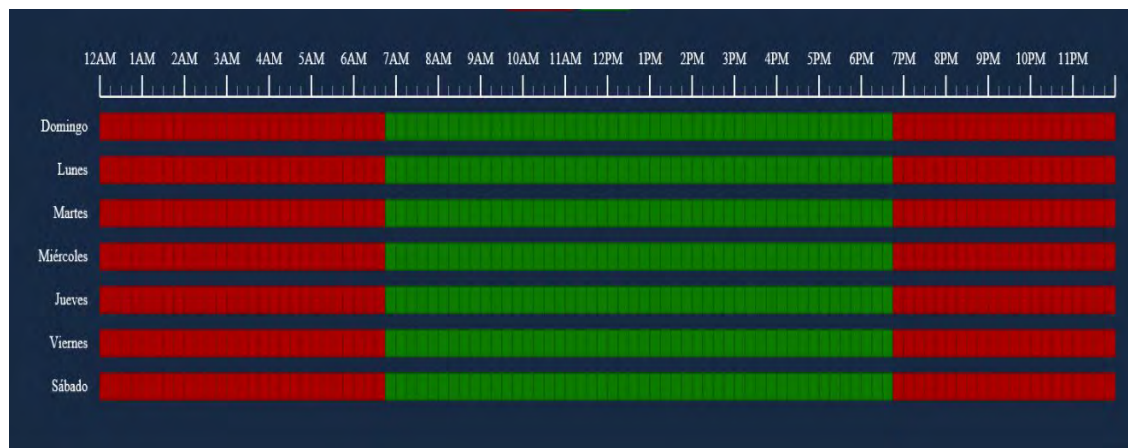
Conceptos

Similar a los Horarios de Puerta, los Horarios de Usuario son el método en el cual los Usuarios son validados si tienen acceso a un Lector específico (**Acceso o Sin Acceso**). La única excepción que afectaría un acceso Permitido y evitaría que se le otorgue acceso al titular de la tarjeta es cuando la Puerta en particular se encuentra actualmente en un estado de Bloqueo, por lo que solo se otorgará acceso a los Usuarios con el conjunto de **Privilegios Maestros**. Los horarios de usuario se aplican a los grupos de **privilegios de acceso**, a diferencia de los **horarios de puertas**, que se aplican a las **puertas**.

Nota: De forma predeterminada, VAX viene con 3 horarios de usuario predeterminados ('Sin acceso', 'Acceso siempre' y 'Acceso de 9 a. m. a 5 p. m.'). Estos horarios de usuario se pueden editar o eliminar según sea necesario, pero en la mayoría de los casos serán suficientes para implementaciones más pequeñas.

Ejemplos

En este ejemplo, tenemos una versión ligeramente modificada del Horario de usuario predeterminado "Acceso de 9 a. m. a 5 p. m.". Lo hemos modificado para un horario más flexible de 7 am a 6 pm.



Acceder a grupos de privilegios

En esta sección, repasaremos los conceptos de Grupos de privilegios de acceso (APG) y cuál es su función en VAX. Para obtener instrucciones sobre cómo configurar los grupos de privilegios de acceso, consulte el Capítulo 11, Grupos de privilegios de acceso

Conceptos

Los Grupos de Privilegios de Acceso en VAX son el enlace que permite el acceso de un **Usuario** a un **Lector** o **Piso** basado en el **Horario del Usuario** y el **Horario de la Puerta/Piso**. Los grupos de privilegios de acceso generalmente se configuran una vez que se cumplen los siguientes requisitos:

- **Paneles, Puertas y Lectores** han sido configurados
- Se han configurado los **horarios de las puertas**

- Se han configurado **los Horarios de usuario**
- Se han configurado los **Horarios de piso** (si se usa el Panel de elevador)

Planificación de sus Grupos de Privilegios de Acceso

Un concepto importante que hace que VAX sea único de otros sistemas es que los Usuarios pueden ser parte de más de un Grupo de Acceso. Esto nos da la flexibilidad de crear APG basados en puertas similares y asignar un usuario individual a múltiples APG según las puertas que necesitará el usuario. Los factores a tener en cuenta para determinar cuántos grupos de acceso necesitará incluyen los siguientes:

- ¿Están los usuarios divididos en diferentes grupos que requerirán diferentes privilegios de acceso (por ejemplo, ingeniería, personal de recursos humanos, gerentes, etc.)?
- ¿Necesitan algunos usuarios más acceso que otros?
- ¿Es necesario que el grupo de privilegios de acceso que está agregando esté en más de una partición?
- ¿Los Grupos de Privilegios de Acceso deben estar agrupados por Usuarios o en base a diferentes tipos de Puertas/ Pisos (Puertas exteriores, Puertas de I+D, grupos de Pisos de ascensores)?

Estilo Estructura de APG (Grupos de Privilegios de Acceso): Grupos basados en usuarios

La estructura tradicional de los grupos de acceso suele implicar un grupo con muchas Puertas/Pisos en el sistema (en algunos casos, todos). Este estilo de grupos se basa en el tipo de Usuarios del grupo, como por ejemplo:

Tabla 6.9. APG ejemplo: 1

Nombre APG	Puertas asignadas APG
Personal de ingeniería	Tendría acceso a Puertas de ingeniería, Puerta principal, Puerta de sala de producción.
Personal de recursos humanos	Tendría acceso a las puertas de la oficina, puerta principal.
Personal de TI	Tendría acceso a closets de red, Puertas de oficina, Puerta principal.
Ventas	Tendría puertas de oficina de acceso, puerta de entrada.

Ventajas de los grupos basados en usuarios:

- Más rápido de configurar inicialmente (debido a que cada usuario está en un solo grupo).
- Funciona bien si la mayoría de los usuarios necesitan los mismos permisos. En el ejemplo anterior, tenemos 4 grupos, con potencialmente cientos de Usuarios en cada uno.

Desventajas de los grupos basados en usuarios:

- Dificultades para cambiar los permisos de usuarios específicos. En el ejemplo anterior, si alguien de Ventas necesitara acceso a las Puertas de Ingeniería, necesitaría su propio grupo separado porque colocar a ese Usuario en el APG de Ingeniería daría lugar a un conflicto debido a que la Puerta Frontal está en ambos grupos.
- No se puede otorgar fácilmente acceso adicional a un usuario sin brindar acceso adicional a la APG.

Estilo Estructura APG (Grupos de Privilegios de Acceso): Grupos basados en puertas / pisos

Esta estructura de grupos de acceso, exclusiva de VAX, aprovecha que los Usuarios pueden formar parte de más de una APG. Estos grupos implican grupos más pequeños y más específicos que se basan en unas pocas Puertas, generalmente de tipo similar, como Puertas exteriores, Puertas de ingeniería. Los usuarios se colocarían en varios grupos en función de las Puertas/Pisos a los que necesitan acceso (y en qué momento necesitan acceso a esas Puertas/Pisos), como:

Tabla 6.10. APG Ejemplo: 2


Nombre del APG	Puertas asignadas por APG
Puertas de ingeniería	Tendría acceso a puertas de ingeniería, puerta de sala de producción.
Puertas de oficina	Tendría acceso a las puertas de la oficina.
Armarios de red	Tendría acceso a la red Puertas de closet.
Puertas exteriores/comunes	Puerta principal y cualquier otra puerta común

Ventajas de los Grupos Basados en Puertas/Pisos:

- Más fácil de mantener a largo plazo ya que se puede especificar un acceso de usuario más específico.
- Los permisos de usuario pueden ser más específicos y es más fácil realizar cambios en las puertas/pisos a los que tiene acceso un usuario. En el ejemplo anterior, si alguien en Ventas necesitaba acceso a las Puertas de ingeniería, ese usuario simplemente puede ubicarse en ambos grupos.

Desventajas de los Grupos Basados en Puertas/Pisos:

- Más tiempo para configurar inicialmente (dependiendo de la cantidad de usuarios).

 **Nota:** En algunas situaciones, puede ser beneficioso hacer un enfoque híbrido, donde las Puertas exteriores y los Pisos comunes tienen sus propios grupos separados, mientras se mantienen otros APG como basados en el Usuario. La parte importante es comunicarle a su cliente sus necesidades y construir APG efectivos juntos.

Nombrar sus grupos de privilegios de acceso

Se recomienda enfáticamente un nombre consistente para sus grupos de acceso. Generalmente, la mejor práctica es nombrar el grupo según el tipo de Usuario dentro del grupo, o según las Puertas/Pisos que están en el grupo.

Festivos / Feriados


Esta sección cubrirá los días **festivos** en VAX. Esta sección cubrirá conceptos y algunos ejemplos. Para la configuración de días festivos, consulte el *Capítulo 13, Configuración de días festivos*.

Los días festivos dentro de VAX se utilizan para definir excepciones al horario de acceso diario regular en respuesta a una ocurrencia de calendario específica. Esta ocurrencia puede ser un día específico o, alternativamente, configurarse para que ocurra anualmente.

A cada feriado se le asigna una fecha, así como uno o más grupos de feriados de usuario o grupos de feriados de puerta, y el horario que seguirá cada grupo en la fecha dada.

Conceptos

Los días festivos requieren algunos pasos de configuración debido a la forma en que interactúan con los usuarios y las puertas. Así como las Puertas y los Usuarios tienen Horarios separados (**Horarios de Usuario y Horarios de Puerta**), los Días Festivos tienen 2 Horarios llamados Horarios de Días Festivos de Puerta y Horarios de Días Festivos de Usuario. En implementaciones grandes, como aquellas que abarcan varios países, puede ser muy flexible.

 **Nota:** En el día del feriado, los cronogramas de feriados de puertas y los cronogramas de feriados de usuarios anularán lo que las puertas y los grupos de privilegios de acceso harían normalmente en las puertas y los grupos de privilegios de acceso a los que están asignados los grupos de feriados.

Hay 5 componentes en los días festivos; cada uno se explicará a continuación:


Horarios de puertas en días festivos. Definen el horario que seguirá una Puerta en un Día Festivo. La configuración del horario es muy similar a la configuración del horario de una puerta regular. Todos los estados normales de la puerta están presentes y pueden cambiar hasta 4 veces en un horario. De forma predeterminada, VAX viene instalado con un Horario de días festivos de la puerta llamado '**Cerrado durante los días festivos**' con un horario de bloqueo todo el día.

Grupos de días festivos de puertas. son una colección de puertas que seguirán el mismo horario en un día festivo. Esto se puede asignar a una puerta cuando se crea o se edita. De forma predeterminada, VAX viene instalado con dos grupos de festivos de una puerta: '**Festivos estándar**' y '**Sin Festivos**'.

Programaciones de días festivos del usuario. Los calendarios de días festivos de los usuarios definen un horario que seguirá una cuenta de usuario en un día festivo. La configuración del horario es muy similar a la configuración normal del horario del usuario. Los modos de usuario disponibles incluyen: '**No permitido**' y '**Permitido**'. De forma predeterminada, VAX viene instalado con dos grupos de usuarios de festivos: '**Acceso en festivos de 9 a. m. a 5 p. m.**' y '**Festivos sin acceso**'.

Grupos de días festivos de usuarios. Son una colección de programaciones de calendario de festivos que los usuarios seguirán en un día festivo. Esto se asigna a los usuarios a través del grupo de privilegios de acceso cuando se crea o edita. De forma predeterminada, VAX viene instalado con dos grupos de festivos de usuario: '**Festivos estándar**' y '**Sin festivos**'.

Festivos: La página Festivos reside en el menú '**Inicio/Día a día**'. Aquí es donde agrega los días festivos, define la fecha y asigna el día festivo a grupos de días festivos de puerta, grupos de días festivos de usuario o ambos.

 **Nota:** Si su implementación utilizará controladores de elevadores para administrar el acceso a los pisos, hay dos componentes adicionales de Festivos:

- Grupos de días festivos de piso (similares a los grupos de días festivos de puerta)
- Cronogramas de feriados de piso (similares a los cronogramas de feriados de puerta)

Ejemplos

Esta sección repasará algunos ejemplos de días festivos que se utilizan en el campo, junto con algunos de los componentes y la toma de decisiones que se incluyeron en cada día festivo. Al agregar un feriado, se puede asignar a grupos de feriados de puerta, grupos de feriados de piso y grupos de feriados de usuarios (con los calendarios de feriados apropiados). Por defecto, VAX viene instalado con dos días festivos: '**Navidad**' y '**Año Nuevo**'.

Algunas preguntas que puede hacerse al agregar un día festivo pueden incluir las siguientes:

- ¿Qué quiero que hagan mis puertas en este día festivo?

- ¿Deberían estar bloqueadas, solo con tarjeta, abiertas, etc.?
- ¿Todos mis Sitios/Particiones deberían verse afectados por este Día festivo (por ejemplo, Sitios en otros países donde el Día festivo puede no estar presente)?
-
- ¿Estos festivo deberían afectar a mis Usuarios, mis Puertas, Pisos o ambos?
- Si utiliza controladores de ascensores, ¿estas vacaciones deberían afectar también su comportamiento?
- ¿Hay algún Usuario que necesite acceso a la(s) Puerta(s) en el Día Festivo?


Ejemplo 1: Día de la Independencia. A una pequeña empresa le gustaría cerrar este día; quieren que la Puerta se cierre con llave en esta festividad. Simplemente pueden asegurarse de que todas sus puertas utilicen las "**festivos estándar**" del grupo de festivos de la puerta. Agregan el feriado en la **página de feriados** y lo adjuntan al **grupo de puertas de feriados estándar** con el **cronograma de feriados de la puerta configurado como 'Cerrado durante los feriados'**. Como puede ver, los grupos de puertas y horarios predeterminados funcionan bien para la mayoría de las situaciones.

Ejemplo 2: Día de Canadá: Gran empresa. Una gran empresa con oficinas en los EE. UU. y Canadá quisiera cerrar sus oficinas en Canadá, pero no en los EE. UU. Si su sistema utiliza particiones, simplemente puede agregar el Día de Canadá al grupo de días festivos de puerta predeterminado en la partición con las oficinas canadienses.

Capítulo 7. Configuración de su Panel

Adición de un panel a VAX

Esta sección cubrirá el proceso básico de agregar un Panel en VAX, en la mayoría de las implementaciones es un proceso bastante fácil y se puede hacer de dos maneras diferentes.

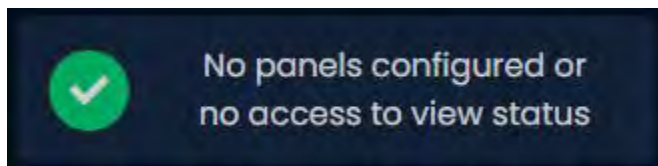
 **Nota:** Esta sección aparece en un capítulo anterior de esta guía. Si ya ha agregado un Panel, puede continuar con la sección llamada "Configuración avanzada del panel".

Método 1: agregar un panel a través de una notificación

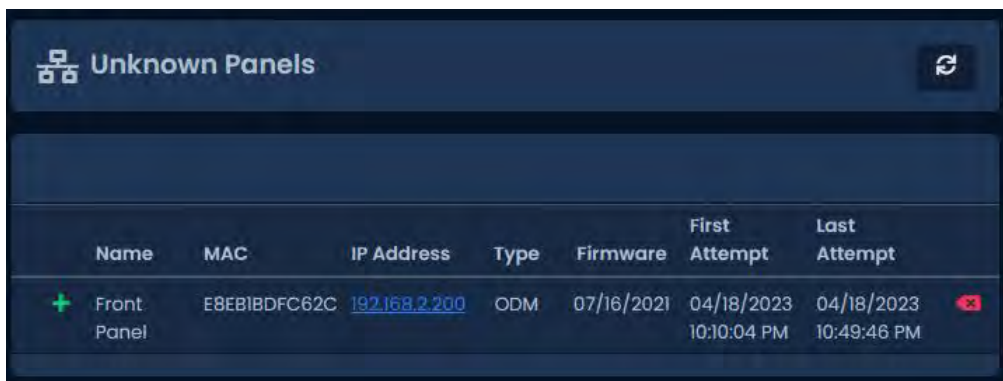
Esta sección cubrirá la adición de un Panel al software después de que el Panel haya sido configurado para buscar el servidor.

El Panel está configurado para encontrar el servidor por **Nombre o Dirección IP**. (Consulte la sección llamada "Configuración de IP del panel: IP estática" y la sección llamada "Configuración del modo de comunicación: nombre del servidor (DNS)" para obtener detalles sobre cómo configurar un panel para encontrar un servidor VAX)

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador
3. En la **barra lateral**, preste atención a la sección **Notificaciones** en el lado derecho de la página.



4. Después de unos momentos, si el Panel está configurado correctamente y no hay firewalls de terceros que bloqueen el puerto TCP 9876, el Panel se conectará al servidor y aparecerá una Notificación (en la imagen a continuación).

A screenshot of a notification titled "Unknown Panels" with a refresh icon. Below the title is a table with columns: Name, MAC, IP Address, Type, Firmware, First Attempt, and Last Attempt. One row is visible with a green plus icon in the Name column and a red X icon in the Last Attempt column.

Name	MAC	IP Address	Type	Firmware	First Attempt	Last Attempt
+ Front Panel	EBEB1BDFC62C	192.168.2.200	ODM	07/16/2021	04/18/2023 10:10:04 PM	04/18/2023 10:49:46 PM

5. Esta Notificación indica que el servidor fue contactado por un Panel que el servidor no conoce. La Notificación mostrará la dirección mac del Panel que intenta conectarse. Si esta dirección coincide con un Panel que le gustaría configurar, haga clic en Notificación.
6. Una vez que haga clic en la Notificación del panel desconocido, se lo llevará a la pantalla **Agregar panel de la puerta** con el campo **Dirección Mac** rellenado previamente con la dirección mac que se muestra en la Notificación.

7. Continúe con la sección llamada "Agregar un panel: configuración básica" para obtener instrucciones continuas sobre cómo agregar un panel..


Método 2: agregar un panel manualmente con la dirección Mac

Esta sección cubrirá la adición de un Panel manualmente en VAX. Puede elegir este método por las siguientes razones:

- Aún no ha configurado el Panel para comunicarse con el servidor.
- Está preconfigurando el software antes de la implementación de los paneles.
- Si la implementación es grande, agregar los paneles a través de notificaciones puede ser difícil

Se debe recopilar la siguiente información antes de agregar paneles manualmente:

- El modelo del Panel (se puede encontrar en el Panel físico a la derecha de la pantalla LCD) para cada Panel.
- Dirección Mac de cada Panel.
- Si los paneles utilizarán DHCP o direcciones estáticas.
- Ubicación de los Paneles (generalmente se usa para nombrar los Paneles).
- Si el Panel es un Panel de Puerta, ¿usará un contacto de Puerta?

 **Nota:** Si no toda esta información está disponible, puede usar valores de marcador de posición para las direcciones Mac y nombres.

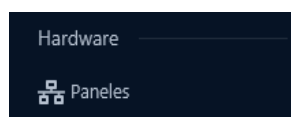
Una vez que haya recopilado esta información, ahora podemos comenzar a agregar los paneles. Continúe con la sección llamada "Agregar un panel: configuración básica"

Agregar un panel: configuración básica

Esta sección cubrirá los diversos campos que deben completarse para agregar un Panel en VAX. Se recomienda completarlos en el orden en que se muestran en la pantalla, con la excepción de la dirección mac si se completa previamente..

Si aún no se encuentra en la pantalla **Agregar paneles de puertas**:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**, haga clic en el icono **Paneles** de puerta (en la imagen de abajo).



4. En la pantalla **Paneles** de puerta, haga clic en el botón **Agregar**.
5. En la pantalla **Agregar paneles** de puerta, se le presentarán varios menús desplegables, campos de texto y casillas de verificación para completar.

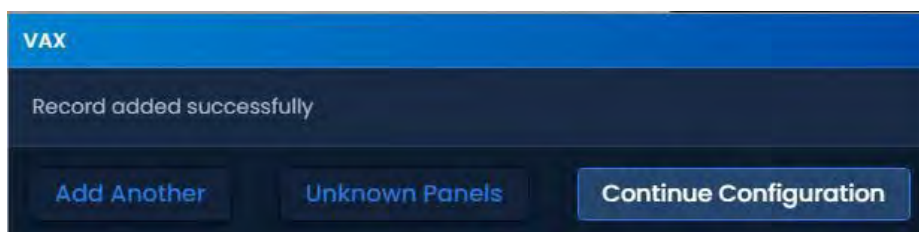
La siguiente tabla describe los campos comunes.

Tabla 7.1. Agregar un Panel

Desplegable/Cuadro de texto/Casilla de verificación	Descripción
Modelo de panel	Seleccione el modelo de Panel usando este menú desplegable, dependiendo del modelo que elija; es posible que se muestren opciones adicionales.
Nombre	El nombre del Panel, recomendamos nombrar el Panel en función de su ubicación en el sitio. Acepta de 4 a 60 caracteres.
Descripción	Descripción opcional del Panel. Acepta de 0 a 255 caracteres.
Sitio	Seleccione el sitio en el que residirá el Panel. Esto no se puede cambiar una vez que se agrega el Panel.
Dirección MAC	La dirección de red única integrada en cada Panel. Puede completarse previamente si está agregando el panel a través de una notificación de conexión desconocida desde el panel. Debe tener 12 caracteres.
Contraseña del panel	La contraseña necesaria para acceder al menú de administración integrado en el Panel. Los valores válidos son de 0 a 9999. El valor predeterminado es '0000'.
Conexión TCP: modo de conexión	El método en el que el Panel recibe su dirección IP, DHCP o Estática. Al seleccionar estático, aparecerán campos adicionales para completar.

Nota : Si ya configuró el Panel con una dirección IP estática, también deberá ingresarla en el software.

- Ahora puede hacer clic en **Guardar**, se le pedirá que corrija cualquier información que falte o que no sea válida. Una vez corregido pulsa **Guardar** de nuevo. Aparecerá un cuadro de mensaje que dirá **Panel de puerta agregado con éxito**.



Advertencia

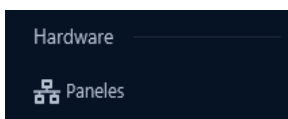
Antes de su primera actualización de los Paneles, le recomendamos configurar los ajustes avanzados de sus Paneles. Esto se puede encontrar en la sección llamada "Configuración avanzada del panel".

Configuración avanzada del panel


Esta sección cubre los aspectos de configuración de los Paneles después de que el Panel se haya agregado al software. Una vez que se agrega el panel, hay opciones de configuración adicionales disponibles, como la configuración de entrada/salida.

Para acceder a la configuración avanzada del Panel:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**, haga clic en el icono **Paneles** de puerta (en la imagen de abajo).



4. En la pantalla **Paneles**, verá los Paneles que ya haya agregado al software. Haga clic en el botón **azul** (Configuración avanzada) junto al Panel que desea configurar.
5. En la pantalla **Editar panel**, hay cuatro pestañas. Las pestañas **General y Conectividad** son las que configuramos al agregar el Panel. La mayoría de estas opciones se pueden modificar según las necesidades. Las pestañas **Opciones y E/S** se rellenan automáticamente en función del modelo de Panel que seleccionó al agregar el Panel. Esta configuración se tratará en la siguiente sección.

 **Nota:** Es posible que algunas opciones no estén disponibles dependiendo del modelo de panel que se esté configurando.

Pestaña General

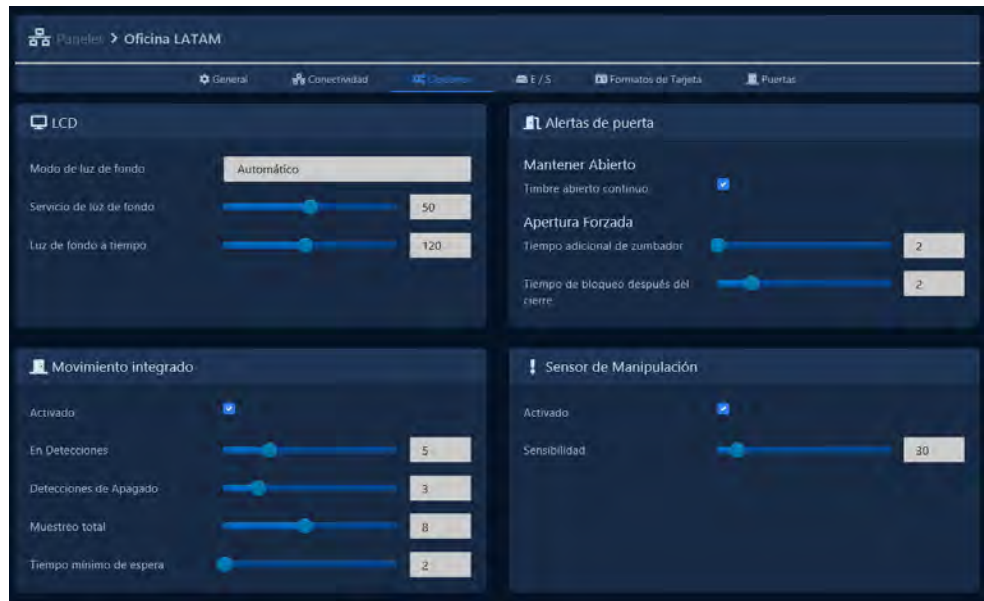
La pestaña General le permite cambiar cualquier información proporcionada cuando se agregó el Panel. Las opciones de cifrado también aparecen en esta pestaña. Se pueden cambiar los siguientes elementos:

Tabla 7.2. Agregar un Panel

Desplegable/Cuadro de texto/Casilla de verificación	Descripción
Nombre	El nombre del Panel. Acepta de 4 a 60 caracteres.
Descripción	Descripción opcional del Panel. Acepta de 0 a 255 caracteres.
Sitio	El sitio en el que residirá el Panel se encuentra. Se puede cambiar a un sitio diferente en la misma partición.
Dirección MAC	La dirección de red única integrada en cada Panel.
Contraseña del panel	La contraseña necesaria para acceder al menú de administración integrado en el Panel. Los valores válidos son de 0 a 9999. El valor predeterminado es '0000'.
Instalado	Habilita si el panel está instalado y configurado para comunicarse. Desmarcar evitará que el panel contribuya al conteo de paneles en la parte superior derecha en la mayoría de las pantallas.
Expansores (solo en algunos modelos)	Cantidad de módulos expansores. Módulos de E/S o de puerta. Ingrese la cantidad correcta (1-8 para módulos IO, 1-4 para módulos de puerta).
Firmware automático	Habilita si el panel recibirá actualizaciones de firmware automáticamente (solo se admite en modelos seleccionados).
Actualizar (solo en algunos modelos)	Se puede configurar como 'AES de 256 bits' cuando se requiere mayor seguridad. Define el método de cifrado entre el servidor VAX y el Panel.

Opciones

Esta sección cubrirá los elementos de configuración en la pestaña de opciones al configurar un Panel.



La pestaña **Opciones** se divide en 6 secciones: **LCD**, **Apertura forzada**, **Sensor de manipulación** y **Movimiento integrado**. Cada sección tiene varias barras deslizantes que se utilizan para cambiar fácilmente los ajustes. También puede utilizar el cuadro de texto junto al control deslizante para introducir manualmente un valor.

Tabla 7.3. Pestaña de opciones

Elemento de configuración	Descripción
LCD	
Modo de luz de fondo	El modo de funcionamiento de la pantalla LCD integrada del Panel. Los valores son Automático, Siempre encendido, Siempre apagado.
Servicio de retroiluminación	El nivel de luz de la pantalla LCD integrada del Panel. Incrementa en 1. Los valores válidos son de 0 a 100.
Retroiluminación a tiempo	El tiempo que la retroiluminación de la pantalla LCD integrada del panel permanecerá activa después de recibir la entrada del usuario. Incrementos de 1 s. Los valores válidos son de 0 s a 255 s.
Mantener abierto	
Zumbador abierto continuo	Determina si la alarma mantenida abierta conectada a un zumbador externo o global estará en un estado cerrado continuo o si emitirá un pulso en el zumbador. Por defecto es pulso.
Forzado abierto	
Tiempo de zumbador adicional	El tiempo adicional que se activará un zumbador de apertura forzada después de que se produzca un evento de apertura forzada. Incrementos de 1 s. Los valores válidos son de 0 s a 255 s.
Tiempo de bloqueo después del cierre	Tiempo total de bloqueo después de un evento de apertura forzada. Incrementos de 1s. Los valores válidos son de 0 s a 10 s. Este es un tiempo intermedio para evitar una alarma de apertura forzada justo después de que una puerta se abra y se cierre. Esto ocurre si una persona válida pasa por una puerta, pero inmediatamente vuelve a salir por la puerta
Sensor de manipulación / sabotaje	
Activado	Activar/Desactivar el sensor de manipulación integrado. El sensor de manipulación emitirá una alarma audible si detecta que se ha quitado la cubierta del panel. Algunos instaladores desactivan esto durante la instalación y las pruebas.

Configuración de su panel

Sensibilidad	La sensibilidad del sensor de manipulación integrado. Un valor más alto permite que se exponga más luz al sensor antes de activar una alarma. Un valor más alto es útil en situaciones en las que el panel está expuesto a la luz solar. Incrementa en 1. Los valores válidos son de 0 a 255
Movimiento Integrado	
Activado	Activar/desactivar el sensor de movimiento integrado (si corresponde).
Por detecciones	Movimiento en detecciones. Incrementa en 1 . Los valores válidos son del 1 al 16.
Detecciones desahabilitadas	Detecciones de movimiento desactivado. Incrementos de 1. Los valores válidos son de 0 a 15.
Muestreo total de movimiento	Muestreo total de movimiento. Incrementa en 1 . Los valores válidos son del 1 al 16.
Tiempo mínimo de espera	Tiempo de espera mínimo de movimiento. Incrementos de 1 s. Los valores válidos son de 0 s a 255 s.
Anti-passback	
Restablecer Anti-passback a medianoche	Si está habilitado, el Anti-passback local se restablecerá a la medianoche.

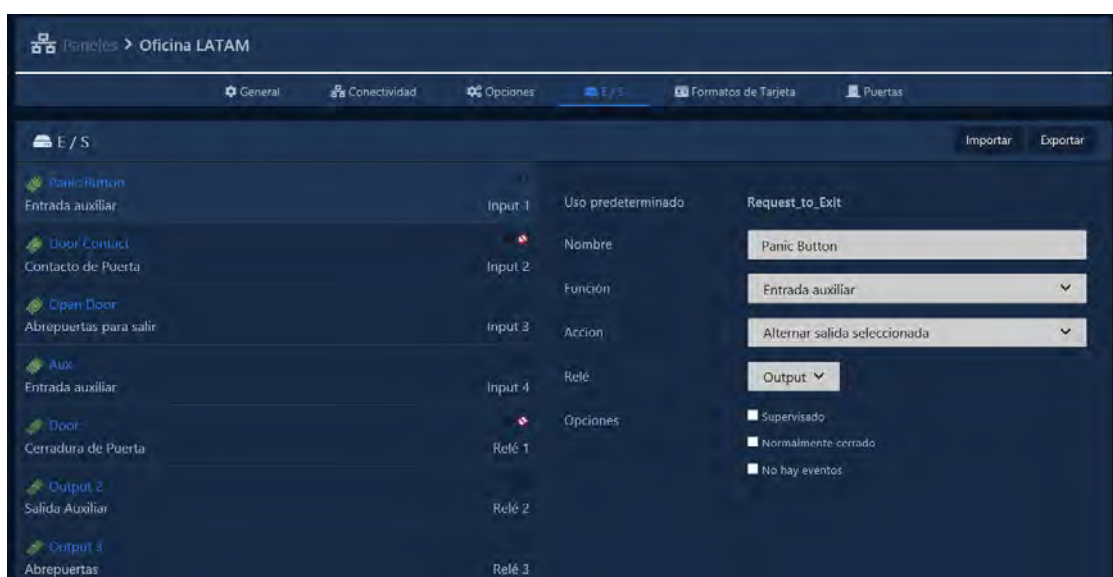
Nota: En la mayoría de los casos, los valores predeterminados para las opciones de movimiento integrado funcionan bien; sin embargo, si necesita disminuir o aumentar la sensibilidad del sensor, consulte la sección llamada "Movimiento integrado: cambio de sensibilidad".

Configuración de entradas / salidas

Esta sección cubre las opciones de configuración en la pestaña Entrada/Salida (E/S). Dependiendo del modelo de panel seleccionado al agregar el panel, el software cambiará los valores predeterminados. Por ejemplo: si agrega un VAX-2D-1; La salida 1 y la salida 2 se asignarán como golpes de puerta. La pestaña de E/S no está disponible en los paneles de elevador. Los paneles VAX-MDK tendrán un menú desplegable para acceder a la configuración de E/S para varios expansores.

Figura 7.1. VAX-1D-1 Pestaña de E/S típica

En la pestaña E/S, la columna de la izquierda muestra cada Entrada y Salida junto con la función actual debajo de ella. La Salida/Entrada seleccionada actualmente (sombreada en gris) tendrá su información mostrada en el lado derecho. Esta información incluye:



- El Nombre de la Entrada/Salida (a mostrar en las notificaciones)
- Puerta asociada (utilizada para determinar a qué puerta corresponde una entrada o salida)

- Función, ver más abajo
- Si la salida/entrada está normalmente cerrada/abierta
- Eventos deshabilitados/habilitados para esta salida/entrada

La siguiente tabla repasará las 10 funciones de entrada diferentes y las 8 funciones de salida diferentes en los controladores alimentados por PoE.

Tabla 7.4. Funciones de entrada/salida VAX-1D-1

Función	Descripción
Funciones de entrada	
Desactivado	La entrada está deshabilitada y no reaccionará a ningún cambio de estado de entrada en la entrada seleccionada.
Solicitud de salida	Permite utilizar la entrada como REX. Esto permitirá que un botón pulsador u otra entrada de contacto seco desbloquee la puerta asociada.
Contacto de puerta	Esta función de entrada se usa para entradas que rastrean si la puerta está abierta o cerrada. También conocido como interruptor de posición de puerta. Debe estar deshabilitado si no está en uso.
Abridor de puerta para salir	Este tipo de entrada se usa generalmente para operadores discapacitados para activar abrepuertas automáticos. El Abridor Automático debe estar habilitado en las Opciones de Configuración de la Puerta.
Sensor de movimiento	Esta función de entrada se utiliza para sensores de movimiento externos. Desbloquear por movimiento debe estar desmarcado en las Opciones de configuración de la puerta para que el sensor de movimiento desbloquee la puerta. Por defecto, el sensor de movimiento evitará la alarma de apertura forzada. El movimiento integrado debe deshabilitarse en la pestaña Opciones de configuración del panel.
Entrada auxiliar	Esta función de Entrada tiene la mayoría de las opciones configurables, incluidas acciones de Entrada como Salidas pulsantes, anulación de Puertas, activación de alarmas. Las acciones de entrada auxiliar se cubren con más detalle en la sección llamada "Acciones de entrada auxiliar"
Alarma de emergencia	Esta función de entrada se utiliza para recibir comandos de los sistemas de alarma de emergencia. Por ejemplo, puede configurar esta entrada para desbloquear la puerta y reproducir un timbre cuando se active una alarma de incendio.
Estado de alarma externa	Esta función de entrada se utiliza para monitorear el estado de un sistema de alarma. Cuando la alarma se considera "Activada", los Lectores no aceptarán Credenciales a menos que el Usuario asociado con esa Credencial tenga el privilegio de Usuario "Desconectar alarma" activado
Abrepuertas para entrar	Este tipo de entrada se usa generalmente para operadores discapacitados para activar abrepuertas automáticos. El Abridor Automático debe estar habilitado en las Opciones de Configuración de la Puerta.
Puerta desbloqueada o abierta/evitar desbloquear	Se utiliza en configuraciones de Mantrampa. Cuando la puerta está abierta o desbloqueada, esta salida se activará, generalmente está conectada a una entrada en otro panel que controla el acceso a la misma área. Conéctese a una entrada con la función "Puerta Evitar Desbloquear".
Funciones de salida	
Desactivado	La salida está deshabilitada y no se activará, incluso si se le indica que lo haga por anulación.

Configuración de su panel

Cerradura de puerta	Se usa para definir una salida como conectada a un cerradero de puerta/cerradura magnética. Nota: La salida 1 es el único contacto húmedo, por lo tanto, las cerraduras de puerta en las salidas 2 y 3 requerirían una fuente de alimentación externa para cerraduras.
Abridor de puerta	Se utiliza para definir una salida que está conectada a la entrada del disparador en un dispositivo de apertura de puerta automático.
Zumbador externo	Se utiliza para altavoces externos. Activará el relé cuando la puerta se fuerza o se mantiene abierta. La opción de zumbador global permitirá que todas las puertas conectadas en el mismo panel activen la misma salida.
Interfaz de alarma	Esta Salida está conectada a una Entrada en el panel de alarma capaz de armar el sistema de alarma; la alarma ahora se puede armar usando un comando de triple deslizamiento. Para obtener más información sobre escenarios de triple deslizamiento, consulte el <i>Capítulo 17, Funciones de triple deslizamiento</i> .
Salida auxiliar	Una salida que se puede activar a partir de cambios de entrada o a través de comandos de triple deslizamiento
Cerradura de puerta secundaria	Configurar una salida para esta función dará como resultado que la salida se dispare cada vez que se dispare la cerradura de la puerta principal. Si la puerta está desbloqueada, la salida permanecerá encendida hasta que cambie el estado de la puerta.
Evitar el desbloqueo de la puerta	Se usa en configuraciones de Mantrap para evitar el acceso a un área si la entrada es activada por una fuente externa (por lo general, otro panel que controla el acceso a la misma área). Se puede usar en otras aplicaciones, como bucles de tierra para puertas de estacionamiento

Advertencia : Si su panel no está usando un contacto de puerta, seleccione las entradas de contacto de puerta y cambie la función desplegable a 'Deshabilitado'.

Acciones de entrada auxiliar

Esta sección cubre acciones adicionales que se pueden programar en una **entrada auxiliar** en VAX. La siguiente tabla son acciones admitidas en los modelos de panel con alimentación PoE.

Tabla 7.5. Acciones de entradas auxiliar

Acción de entrada	Descripción
Activar salida seleccionada	Permite que la entrada active una salida (seleccionable en el menú desplegable). La salida permanecerá activada hasta que sea anulada en el software o por otra acción de entrada auxiliar.
Desactivar salida seleccionada	Permite que la entrada desactive una salida (seleccionable en el menú desplegable).
Alternar salida seleccionada	Permite que la entrada alterne una salida (seleccionable en el menú desplegable). Alternar cambiará el estado del estado actual de la salida. La entrada deberá volver a su estado normal y luego cambiar nuevamente para que cambie el estado de la salida
Salida seleccionada de pulso	Permite que la entrada active una salida (seleccionable en el menú desplegable) durante 1,5 segundos, después de lo cual la salida se desactivará.
Activar salida seleccionada con sonido	Permite que la entrada active una salida (seleccionable en el menú desplegable) con una alerta audible de que la salida se activó. La salida permanecerá activada hasta que se anule en el software o por otra acción de entrada auxiliar.
Desactivar salida seleccionada con sonido	Permite que la entrada desactive una salida (seleccionable en el menú desplegable) con una alerta audible de que la salida se desactivó.

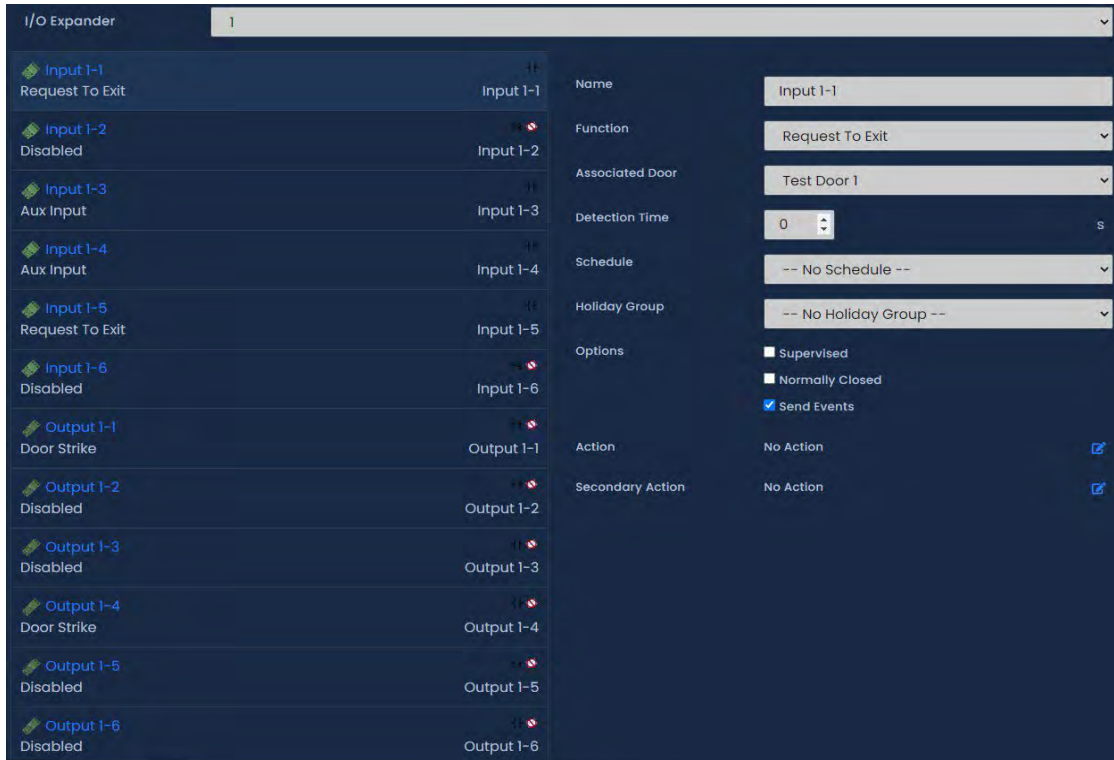
Configuración de su panel

Alternar salida seleccionada con sonido	Permite que la entrada alterne una salida (seleccionable en el menú desplegable) con una alerta sonora de que la salida se activó. Alternar cambiará el estado del estado actual de la salida. Cada cambio de estado irá acompañado de una alerta sonora de que se cambió el estado de salida. La entrada deberá volver a su estado normal y luego cambiar de nuevo para que cambie el estado de la salida.
Salida de pulso seleccionada con sonido	Permite que la entrada active una salida (seleccionable en el menú desplegable) durante 1,5 segundos con una alerta audible de que la salida se activó, después de lo cual la salida se desactivará.
Activar interfaz de alarma	Permite que una Entrada (como un botón) active una Salida que está asignada como una interfaz de alarma. El circuito cambia a un estado cerrado durante
Desactivar interfaz de alarma	Permite que una entrada (como un botón) desactive una salida asignada como interfaz de alarma.
Alternar interfaz de alarma	Permite que una entrada (como un botón) active una salida asignada como interfaz de alarma. El circuito cambia a un estado cerrado durante 1,5 segundos antes de cambiar a un estado abierto. En la mayoría de los casos, esto se puede usar para armar un sistema de alarma.
Activar interfaz de alarma con sonido	Permite que una Entrada (como un botón) active una Salida que se asigna como una interfaz de alarma con una alerta audible. El contacto seco cambia a un estado cerrado durante 1,5 segundos antes de cambiar a un estado abierto. En la mayoría de los casos, esto se puede usar para armar un sistema de alarma.
Desactivar interfaz de alarma con sonido	Permite que una Entrada (como un botón) desactive una Salida que está asignada como una interfaz de alarma con una alerta audible.
Alternar interfaz de alarma con sonido	Permite que una Entrada (como un botón) active una Salida que se asigna como una interfaz de alarma con una alerta audible. El contacto seco cambia a un estado cerrado durante 1,5 segundos antes de cambiar a un estado abierto. En
Reproducir sonido 0-4	la mayoría de los casos esto se puede usar para armar un sistema de alarma
Reproducir sonido de advertencia	Permita que una Entrada dispare un sonido en el Panel; permite un menú desplegable con varias opciones.
Anular puertas con nivel de crisis	Permita que una entrada reproduzca un sonido de advertencia.
Sin acción	Permite que una entrada cambie el nivel de crisis de la puerta a un valor asignable de una lista desplegable.

! **Advertencia;** Las entradas conectadas al panel deben estar secas, sin energía. El incumplimiento de esta instrucción podría provocar daños en el panel

Una vez que haya realizado los cambios deseados en la configuración del Panel, ahora puede hacer clic en el botón Guardar en la parte inferior de la página. Una vez que haya agregado y configurado sus otros paneles, probablemente querrá continuar con la actualización de su panel. Consulte la sección llamada "Actualización de su panel".

VAX-MDK



Los controladores con alimentación de 12 V CC tienen algunas características adicionales de entrada/salida que se mencionarán en esta sección. Algunas diferencias específicas incluyen:

- El menú desplegable Expansor de E/S selecciona qué entradas y salidas del expansor mostrar.
- El tiempo de detección se puede configurar en las entradas para que la función y/o acción ocurra solo si el estado de la entrada se mantiene durante el número de segundos definido.
- A las entradas se les puede asignar un programa de entrada, que restringirá cuándo funcionará la función de la entrada o las acciones asignadas. Por ejemplo, es posible que desee programar un sensor de movimiento externo. Admite horarios de festivos.
- A las salidas configuradas con la función Salida Aux se les puede asignar un Programa de salida. Admite horarios de festivos.
- A todas las entradas se les puede asignar una acción similar a las acciones de entrada auxiliar en otros tipos de paneles. La acción puede ocurrir independientemente de la función de entrada.
- A todas las entradas se les puede asignar una segunda acción similar a las acciones de entrada auxiliar en otros tipos de paneles denominada acción de encendido. La acción de encendido puede ocurrir independientemente de la función de entrada además de la acción establecida

La siguiente tabla contiene una lista de Acciones.

Tabla 7.6. Acciones de entrada del panel VAX-MDK

Acciones de triple deslizamiento	Breve explicación
Sin acción	Las acciones son opcionales; aún se generará un evento cuando se cumplan las condiciones de entrada y aún se puedan ejecutar los activadores de secuencias de comandos del lado del servidor.
Activar salida	Activa una salida, seleccionable a través de la lista desplegable.
Alternar salida	Cambia una salida al estado opuesto, seleccionable a través de la lista desplegable.

Configuración de su panel

Acciones de triple deslizamiento	Breve explicación
Desactivar salida	Desactivar la salida seleccionada, seleccionable a través de la lista desplegable.
Salida de pulso alta	Pulse una salida para cerrar, configure un retraso y la duración del pulso.
Salida Pulso Bajo	Pulse una salida para abrir, configure un retardo y la duración del pulso.
Pulso de salida opuesto	Pulse una salida al contrario de su estado actual, configure un retraso y la duración del pulso.
Activar salida múltiple	Active múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Desactivar Salida Múltiple	Desactive múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Alternar salida múltiple	Alterne múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Inhabilitar entrada	Deshabilitar una entrada seleccionada. Seleccionable de una lista desplegable con retraso y duración.
Anular <Modo de puerta>	Esta acción de deslizamiento triple anulará el estado de la puerta según la selección que configure en el software. Estas anulaciones de puerta se deben reanudar desde el software o una acción separada que reanude el estado de la puerta. Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta. Puerta y modo seleccionable de la lista desplegable
anular <Modo de puerta> con reanudación automática	Esta acción de triple deslizamiento anulará el estado de la puerta dependiendo de la selección que configure en el software. Estas Anulaciones de puerta le indican a la puerta que reanude el horario normal cuando el horario de puerta asignado a esta puerta está programado para cambiar. También se puede reanudar desde el software o una acción separada que reanudará el estado de la puerta. Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta. Puerta y modo seleccionables de la lista desplegable
Anulación de reanudación de puerta	Reanuda una puerta desde un estado anulado. Seleccionable a través de la lista desplegable.
Nivel de crisis del conjunto de puerta	Inicia el nivel de crisis en una puerta. Seleccionable a través de la lista desplegable para puerta y modo.
Nivel de crisis de restablecimiento de puerta	Vuelva a establecer el nivel de crisis por defecto en la puerta seleccionada. Seleccionable a través de la lista desplegable.
Desactivación de puerta con zumbador abierto	Desactive temporalmente una alarma/zumbador abierto mantenido en la puerta seleccionada. Seleccionable a través de una lista desplegable para puerta y duración (1-600 segundos).
Desconexión de alarma de emergencia	Desactiva la función de alarma de emergencia que reanudará cualquier anulación causada por la función de alarma de emergencia.
Alarma de emergencia (silenciosa) - Desbloqueo de puertas	Activa la función de alarma de emergencia. Los lectores no emitirán un pitido (silencioso). No excluirá las puertas con la opción "Desbloquear en alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia (silencio) - Desbloqueo de puertas sin protección	Activa la función de alarma de emergencia. El panel no emitirá un pitido (silencioso). Excluirá las puertas con la opción "Desbloquear en alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia - Sonido	Activa la función de alarma de emergencia. El panel emitirá un pitido hasta que se active la función de desconexión de alarma de emergencia. No afectará el estado de la puerta.

Configuración de su panel

Alarma de emergencia: desbloquear puertas	Activa la función de alarma de emergencia. El panel emitirá un pitido hasta que se active la función de desconexión de alarma de emergencia. No excluirá las puertas con la opción "Desbloquear en caso de alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia - Desbloqueo de puertas no protegidas	Activa la función de alarma de emergencia. El panel no emitirá un pitido (silencioso). Excluirá las puertas con la opción "Desbloquear en alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Zumbador	Proporciona varias opciones para desactivar los zumbadores del lector o las salidas configuradas como zumbadores externos. El zumbador se reactivará si otro evento activa el zumbador, como una puerta que se abre a la fuerza.
Activar interfaz de alarma	Se utiliza para activar una salida que se asigna como interfaz de alarma. En la mayoría de los casos, esto se puede usar para armar un sistema de alarma.
Desactivación de la interfaz de alarma	Se utiliza para desactivar una salida asignada como interfaz de alarma. En la mayoría de los casos, esto se puede usar para desarmar un sistema de alarma

Pestaña de formatos de tarjeta

La pestaña Formatos de tarjeta tiene varias configuraciones de formato de tarjeta misceláneas. Esta pestaña también muestra las combinaciones disponibles de formatos de tarjeta. Para obtener más información sobre los formatos de tarjeta, consulte la sección llamada "Editar sitios y áreas: formatos de tarjeta". Esta sección describirá las otras opciones disponibles en esta pestaña.

Tabla 7.7. Opciones de formato de tarjeta

Opción	Descripción
Utilice el código de sitio fijo de 60000	Cuando está marcada, todas las credenciales presentadas a los lectores en este panel informarán un código de sitio de 60000. Esto es útil en sitios donde hay demasiados códigos de sitio o no hay código de sitio.
Reasignar código de sitio 0 a 60000	Cuando se marca, todas las credenciales presentadas a los lectores en este panel informarán un código de sitio de 60000 si el código de sitio original era 0 y el formato de los datos de la credencial es diferente a una ráfaga de 8 bits. Esto es útil en sitios donde no se desea tratar el código de sitio 0 como un PIN.
Option	Description
Suprimir eventos de formato de tarjeta inválidos	Cuando está marcado, este panel no informará eventos relacionados con formatos de tarjeta no válidos.
Suprimir eventos con formato de tarjeta desconocido	Cuando está marcado, este panel no informará eventos relacionados con formatos de tarjeta desconocidos. Útil cuando hay ruido frecuente en las líneas del lector que no se puede resolver.

Movimiento Integrado: Cambio de Sensibilidad

Esta sección cubre cómo aumentar o disminuir la sensibilidad del movimiento integrado. Asegúrese de que "**Desbloquear por movimiento**" no esté deshabilitado en la pestaña **Opciones** de la pantalla **Editar puerta**.

Bajar la sensibilidad. Para disminuir el tiempo de sensibilidad del sensor, aumente el valor de **Muestreo total de movimiento** y reduzca el valor de **Detección activada**.

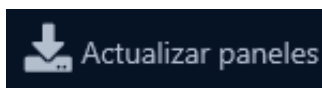
Elevando la Sensibilidad. Para aumentar el tiempo de sensibilidad del sensor, reduzca el valor de **Muestreo total de movimiento** y reduzca el valor de **Detecciones desactivadas**.

Actualización de su panel

Esta sección cubrirá el proceso de actualización de sus Paneles. La actualización de sus paneles envía información relevante a la memoria flash de los paneles. Se deben actualizar los paneles para que los cambios en el software se apliquen a los paneles. Por ejemplo: si agrega un nuevo usuario al software, el Panel no reconocerá a ese usuario hasta que se actualice.

Puede actualizar todos los paneles desde cualquier página del software VAX. Simplemente haga clic en el botón Actualizar paneles en la parte superior derecha de la página (en la imagen a continuación).

Figura 7.2. Botón para Actualizar paneles

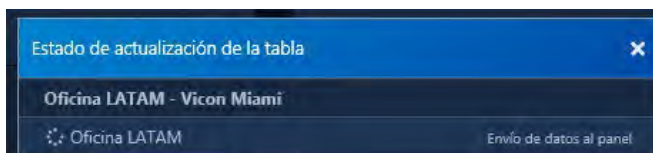


Actualización del primer panel. Siempre que realice la primera actualización de sus paneles después de conectarlos con éxito por primera vez, hay un par de elementos que debe revisar para asegurarse de que sus paneles vuelvan a estar en línea después de la actualización.

- ¿Está la dirección o el nombre del servidor correcto en "Inicio>Configuración del sistema>Dirección del servidor"?
- ¿Están sus paneles utilizando contactos de puerta? De no ser así, ¿se han deshabilitado en la pestaña de E/S de configuración del panel?
- Si está realizando trabajo adicional en el panel físico, puede ser útil desactivar temporalmente el sensor de manipulación, que se puede cambiar en "Inicio>Hardware>Paneles>Opciones>".

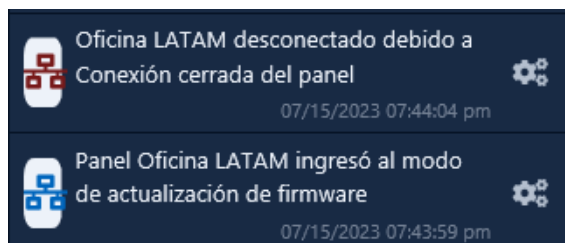
Cuando haga clic en Actualizar paneles, su navegador le preguntará si está seguro de que desea realizar esta acción. Haga clic en **Sí/Continuar/Aceptar**. Aparecerá una ventana en el medio de la pantalla que mostrará el estado de las actualizaciones que se envían al Panel.

Figura 7.3. Ventana de estado de actualización del panel



Después de que el Panel reciba toda esta información, se desconectará de VAX por un par de momentos y luego intentará volver a conectarse a VAX.

Figura 7.4. Notificación típica de actualización del panel



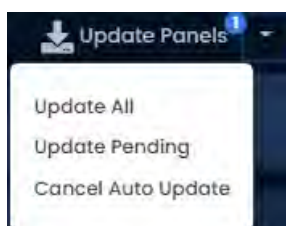
Mi panel no vuelve a estar en línea después de mi primera actualización. Si su Panel no vuelve a estar en línea después de su primera actualización, consulte "Inicio>Configuración del sistema>Dirección del servidor". Si se trata de un nombre, es posible que el Panel tenga problemas para convertir el nombre en una IP mediante DNS. Consultar al personal de TI; si un servidor DNS estable no está disponible, es posible que deba cambiar el modo de comunicación de su servidor a IP estática.

Actualización automática del Panel

VAX es capaz de actualizar sus paneles automáticamente después de realizar cambios. Este comportamiento está habilitado de forma predeterminada.

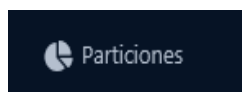
Cada vez que realice un cambio en una partición, un temporizador configurable comenzará la cuenta regresiva. Se mostrará una notificación en la parte inferior superior de cualquier pantalla. Una vez que este temporizador llegue a 0, el servidor VAX actualizará automáticamente los paneles adjuntos a las particiones que hayan tenido cambios. Si realiza cambios adicionales después de que el temporizador haya comenzado, restablecerá el temporizador al valor predeterminado configurado y comenzará de nuevo.

Figura 7.5. Mensaje de actualización automática



El temporizador de actualización automática es una configuración a nivel de partición. Para cambiar los ajustes de actualización automática:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono **Particiones** (en la imagen a continuación).



2. En la pantalla Particiones, verá una lista de todas las particiones del sistema. Haga clic en el botón azul Editar junto a las particiones en las que desea configurar la actualización automática.
3. En la página Editar partición, habrá una casilla de verificación llamada "Actualización automática del panel". Si desea habilitar la actualización automática, asegúrese de que esta casilla de verificación esté marcada.

También puede configurar el temporizador de actualización automática. 15 minutos es el valor predeterminado, pero se puede configurar entre 5 minutos y 1440 minutos. Si realizó algún cambio, haga clic en Guardar.

Figura 7.6. Configuración de actualización automática



Actualizaciones de firmware del Panel

Periódicamente, cuando mejoramos VAX, se requerirán actualizaciones de firmware para sus paneles

con las actualizaciones de software. Actualizar el firmware de un panel es un proceso relativamente sencillo.

! Advertencia

Mientras está en modo de actualización de firmware, los paneles no funcionan. No responderán a las presentaciones de tarjetas, no generarán notificaciones y pondrán la puerta en un estado de bloqueo. Para limitar el impacto que esto tiene en su sitio, sugerimos colocar solo 1 panel a la vez en modo de actualización de firmware.

Config actualización p92

1. Cuando un Panel intenta conectarse a la aplicación VAX y se encuentra que el firmware está desactualizado, verá un indicador cerca de la parte superior de la pantalla que indica que 1 o más Paneles requieren una actualización de firmware (junto al indicador de Paneles en línea).

Figura 7.7. Notificación de firmware desactualizado

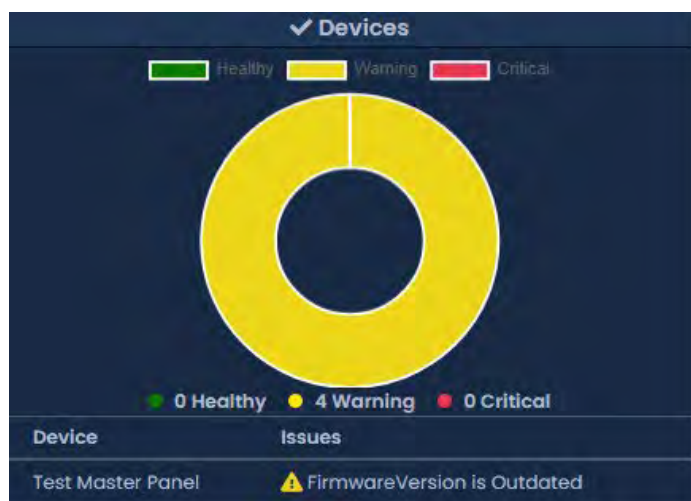


Figura 7.8. Notificación de firmware desactualizado



2. Para que un Panel tenga su firmware actualizado debemos ponerlo en Modo de Actualización de Firmware. Para hacer esto, navegaremos a la página de Descripción general del sistema en el software. Haga clic en el cuadro "x/x Panels Online" arriba del área de Notificaciones o en la página de inicio, desplácese hacia abajo hasta la sección titulada **Sistema y** haga clic en Descripción general del **sistema**.

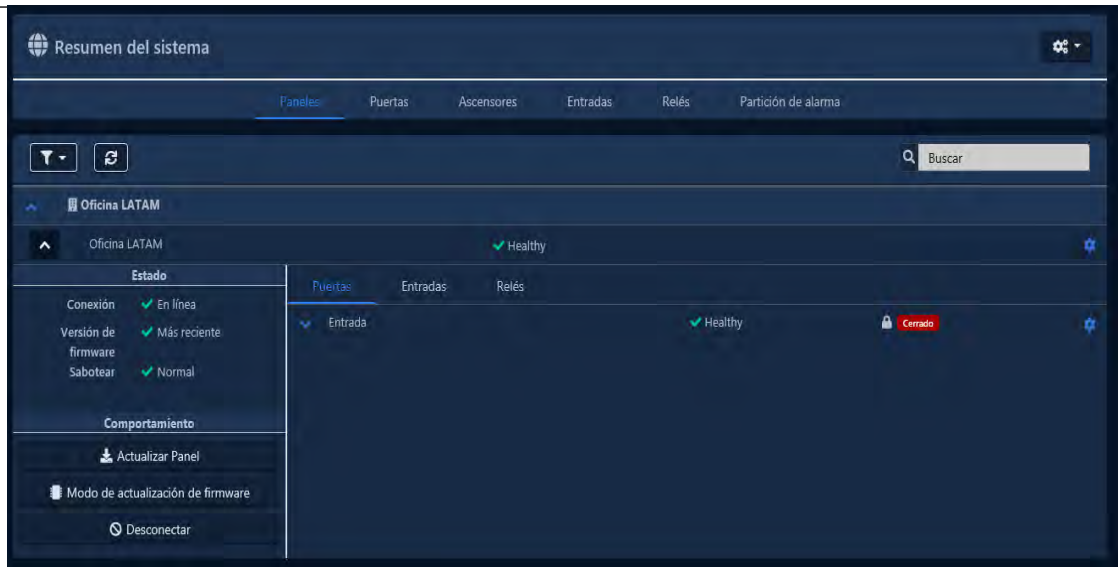


3. En la Descripción general del sistema, verá una lista de todos los paneles de su sistema. Todos los paneles que requieran una actualización de firmware tendrán un mensaje junto a su nombre.

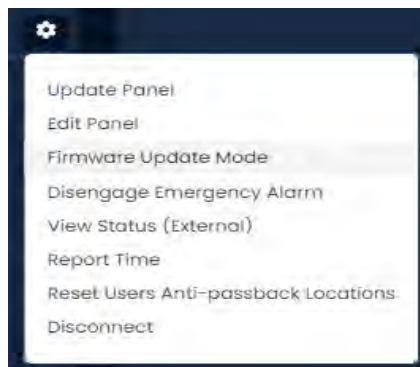
Figura 7.9. Descripción general del sistema que muestra el mensaje de firmware desactualizado

4. El siguiente paso es colocar sus paneles en el modo de actualización de firmware. Esto se puede lograr en la página de **Descripción general del sistema**.
 - a. En el lado derecho del Panel, haga clic en el icono de engranaje, que se muestra arriba. Aparecerá un menú contextual como se muestra a continuación.

Configuración de su panel



b. Seleccione '**Modo de actualización de firmware**' en el menú contextual.



c. El Panel ahora se desconectará e intentará actualizar su firmware.

5. El servidor VAX aceptará conexiones entrantes de paneles en modo de actualización de firmware en el **puerto UDP 9876** y aplicará automáticamente el último firmware coincidente para su panel. Una vez completado, el servidor le indicará al Panel que se reinicie en modo normal, momento en el que el Panel reanudará el funcionamiento normal. Si el panel no se conecta al servidor en UDP 9876 dentro de los 60 segundos, el panel se reiniciará.
6. Repita el proceso anterior en todos los paneles que indiquen que requieren una actualización de firmware. Después de que se haya actualizado el firmware de todos los Paneles, recomendamos actualizar todos sus Paneles. El ícono de estado 'Modo de actualización' sobre la ventana de notificaciones desaparecerá automáticamente, o puede actualizar la página.

Solución de problemas de actualización de firmware

El panel continúa mostrando el firmware desactualizado después de colocarlo en el modo de actualización de firmware. Si un panel continúa mostrando que requiere una actualización de firmware después de colocar el panel en el modo de actualización de firmware y volver a estar en línea, asegúrese de que no haya ningún firewall de terceros que bloquee el puerto UDP 9876. Asegúrese de que no haya soluciones de firewall empresariales entre el servidor y el Panel en la red bloqueando el puerto UDP 9876.

El panel no vuelve a estar en línea después de colocarlo en el modo de actualización de firmware. Si un panel no vuelve a estar en línea después de varios minutos, recomendamos verificar físicamente la pantalla LCD del panel.

Configuración de su panel

- Si la pantalla LCD muestra el mensaje "Run Application Timeout", apague el panel desconectando el Cat5 del lado izquierdo de la placa. Mantenga presionado el botón con la etiqueta Enter (SW3) mientras conecta el cat5. Esto colocará el panel nuevamente en el modo de actualización de firmware..
- La pantalla LCD del panel mostrará la dirección del servidor actual desde la que desea actualizar su firmware. Si ve este conjunto como 192.168.2.10, podría indicar que tuvo un problema durante la actualización. Pruebe la sugerencia anterior o cambie la dirección IP del servidor VAX temporalmente a 192.168.2.10 con una máscara de subred 255.255.255.0.

Capítulo 8. Configuración de una puerta

Este capítulo repasará todos los aspectos de configuración de una puerta. Agregar una Puerta es el siguiente paso lógico después de configurar sus Paneles de Puerta; Si durante las etapas de planificación decidió que necesitaba Horarios de puertas adicionales, le recomendamos que los cree antes de agregar sus Puertas. *Consulte el Capítulo 9, Configuración de horarios de puertas.*

Agregar una puerta

Esta sección repasará el proceso de agregar una puerta. Al agregar una puerta, no todos los aspectos son configurables. Después de agregar la puerta, habrá más ajustes y configuraciones disponibles.

1. . Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**, haga clic en el icono **Puertas** (que se muestra a continuación).



4. En la pantalla **Puertas**, verá que las Puertas que ya ha configurado se enumeran aquí. Haga clic en el botón **Agregar** en esta pantalla.
5. En la pantalla **Agregar puerta**, tendrá varios campos para completar.

Consejo: También puede acceder a la pantalla Agregar puerta desde la pestaña Puertas en la pantalla Editar panel

Figura 8.1. Pantalla de agregar puerta



Tabla 8.1. Agregar una puerta

Cuadro de texto / Menú desplegable	Descripción
Tipo de puerta	Seleccione Administrado para puertas con cerraduras y lectores. Para obtener más información sobre puertas no administradas, consulte la sección denominada "Puertas no administradas y monitoreadas con IO-Boards".
Nombre	Nombre único de su Puerta. Acepta de 4 a 255 caracteres. Recomendamos nombrar su Puerta por su ubicación o función.

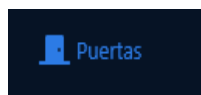
Cuadro de texto / Menú desplegable	Descripción
Descripción	Descripción opcional de la Puerta. Acepta de 4 a 255 caracteres.
Panel	Una vez que seleccione un Panel con puertos abiertos, aparecerán opciones de configuración adicionales en la pantalla. Seleccione el panel al que se adjuntará esta puerta.
Puerto en el panel	Este puerto representa el índice de las clasificaciones de Entrada/Salida. Por lo general, lo aumentará secuencialmente.
Horario	Este es el aspecto de configuración más importante al agregar una puerta. Seleccione el horario de puerta deseado (predeterminado o personalizado). Esto se puede cambiar después de agregar la puerta.
Grupo de vacaciones de puerta	Aquí puede seleccionar un grupo de festivos de puerta. La selección predeterminada es 'Sin festivos'. Esto se puede cambiar después de agregar la puerta.
Lector 1 Nombre	Nombre único de su Lector. Acepta de 4 a 255 caracteres. Recomendamos nombrar su Lector por su ubicación, incluso si es un Lector de ENTRADA o SALIDA.
Lector 1 Descripción	Descripción opcional de su Reader. Acepta de 4 a 255 caracteres.
Lector 1 puerto en panel	Seleccione un puerto para el Lector. El número de puerto refleja el puerto del Lector físico en el Panel.
Lector 2	Lector 2 no es compatible cuando se ha habilitado el controlador de movimiento en el panel. Si desea utilizar un lector interno y externo, deshabilite el movimiento en la configuración avanzada del Panel. Una vez deshabilitado, complete los campos del Lector 2.

- Una vez que haya completado todos los campos obligatorios, haga clic en el botón Guardar para agregar la puerta. Se le indicarán las opciones para agregar una puerta adicional o **continuar con la configuración**, lo que lo llevará a la **configuración avanzada de la puerta** para la puerta que acaba de agregar.

Configuración avanzada de puertas

Esta sección cubrirá las opciones avanzadas de configuración de puertas. Estos ajustes solo se pueden configurar después de agregar una puerta. Para obtener información sobre cómo agregar una puerta, consulte la sección llamada "Agregar una puerta".

- Si aún no está en la pantalla Editar puerta, desplácese hacia abajo en la **barra lateral**, hasta la sección titulada **Hardware**, haga clic en el icono **Puertas** (en la imagen a continuación).



- En la pantalla **Puertas**, verá que las Puertas que ya ha configurado se enumeran aquí. Haga clic en el botón azul junto a la puerta que desea configurar.
- En la pantalla **Editar** puerta, verá 5 pestañas, cada una con sus propios elementos de configuración. Algunas opciones no están disponibles en modelos o tipos de puertas específicos.

General

Esta sección cubrirá los elementos de configuración en la pestaña General de **Configuración de la puerta**.

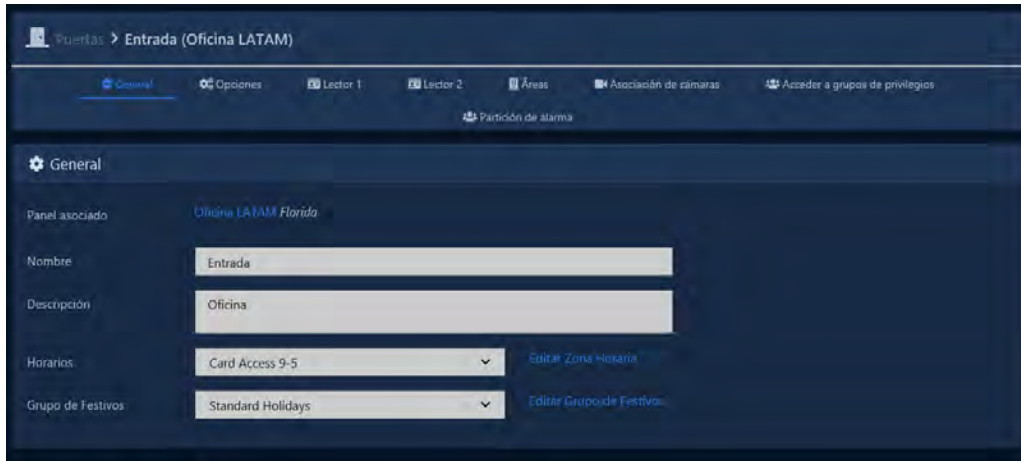


Figura 8.2. Pestaña General

Cuadro de texto/Menú desplegable	Descripción
Nombre	Nombre único de su Puerta. Acepta de 4 a 255 caracteres. Recomendamos nombrar su Puerta por su ubicación o función.
Descripción	Descripción opcional de la Puerta. Acepta de 4 a 255 caracteres.
Cronograma	Este es el aspecto de configuración más importante de una puerta. Seleccione el programa de puerta deseado (predeterminado o personalizado). También puede editar el horario de puerta seleccionado haciendo clic en el enlace "Editar horario" a la derecha del menú desplegable.
Grupo de festivos de puerta	Aquí puede seleccionar un grupo de festivos de puerta. La selección predeterminada es 'Sin festivos'.

Opciones

Esta sección cubrirá los elementos de configuración en la pestaña Opciones de Configuración de la puerta. Las primeras 5 opciones son misceláneas:

Figure 8.3: Pestaña de opciones

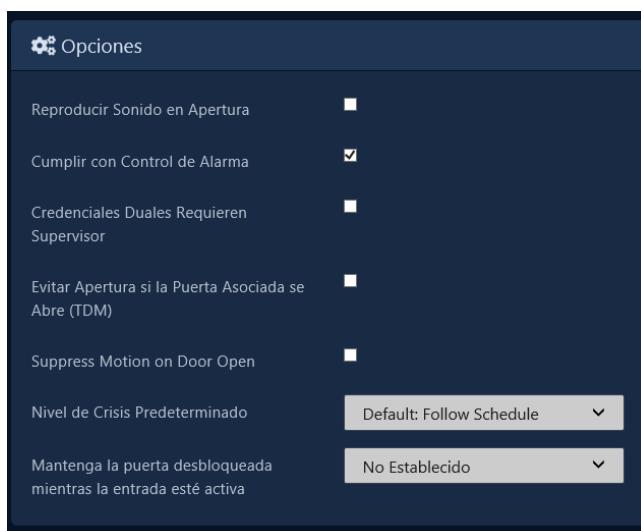


Tabla 8.3. Pestaña de opciones de puerta

Cuadro de texto/Menú desplegable	Descripción
Reproducir sonido al abrir	Si está marcado, el panel reproducirá un indicador audible cuando la puerta se abra (requiere contacto de puerta).
Cumple con el control de alarma	Si se marca, la puerta cambiará de comportamiento cuando se active una entrada configurada con la función Estado de alarma externa.
Credenciales duales requiere supervisor	Cuando el Horario de la puerta indica que se requieren Credenciales dobles, esta configuración activa/desactiva el requisito de que la Credencial inicial presentada tenga el privilegio de supervisor.
Prevenir el desbloqueo si la puerta emparejada está abierta	Esta configuración activa la lógica interna de Mantrap en los controladores de dos puertas; Para más información sobre la configuración de Mantrap, consulte el <i>Capítulo 22, Configuración de Mantrap</i> .
Suprimir movimiento al abrir la puerta	Suprime el sensor de movimiento una vez que la puerta está abierta, evita que el movimiento destrabe la puerta o active el abridor de puerta cuando cualquiera de las funciones está habilitada.
Nivel de Crisis por Defecto	Establece el nivel de crisis predeterminado para la puerta en funcionamiento normal.
Mantenga la puerta desbloqueada mientras la entrada esté activa	Seleccione una entrada que mantendrá la puerta desbloqueada mientras se mantenga el estado de la entrada (cerrada o abierta).

Temporizadores

La sección de temporizadores de la página de opciones tiene varios temporizadores con controles deslizantes para ajustar.

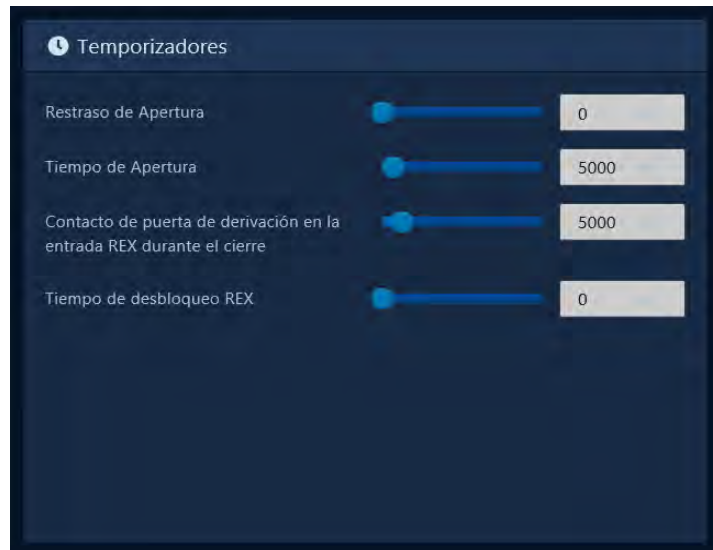


Tabla 8.4. Temporizadores

Nombre del temporizador	Descripción
Retardo de desbloqueo	El tiempo de demora (en ms) entre la autorización de una credencial y el desbloqueo de la puerta. Incrementos de 100 ms. Los valores válidos son de 0 ms a 60000 ms.
Desbloquear tiempo	El tiempo (en ms) que la puerta permanecerá desbloqueada después de que se haya autorizado una credencial. Incrementos de 100 ms. Los

Configuración de horarios de puertas

	valores válidos son de 700 ms a 60000 ms.
Tiempo permitido de apertura	El tiempo (en ms) que una puerta puede permanecer abierta antes de que se active una alarma. Incrementos de 100 ms. Los valores válidos son de 1000 ms a 300000 ms.
Derivar Contacto de puerta en la entrada REX durante el cierre	Tiempo (en ms) que puede abrir una puerta después de activar un botón REX, Movimiento o Abridor mientras la puerta está en Bloqueo antes de que se considere una Apertura forzada. Incrementos de 100 ms. Los valores válidos son de 2000 ms a 25500 ms.
Tiempo de desbloqueo de REX	Tiempo de desbloqueo alternativo para las activaciones de Solicitud de salida o Abridor de puerta para salir. Si se establece en 0, se utilizará el tiempo de desbloqueo normal. Incrementos de 500 ms. Los valores válidos son de 0 ms a 100000 ms.

Alarma de apertura mantenida

La sección Alarma de apertura mantenida de la página de opciones tiene varias opciones para configurar Alarmas de apertura mantenida.

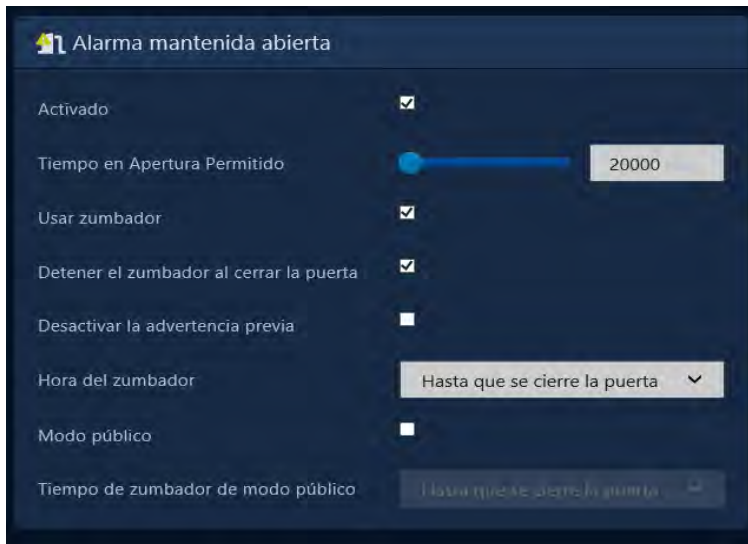


Table 8.5. Alarma de apertura mantenida

Ajuste de alarma de apertura mantenida	Descripción
Activado	Habilita la notificación y las funciones de alarma de apertura retenida. Habilitado por defecto.
Tiempo permitido de apertura	El tiempo (en ms) que la puerta puede permanecer abierta después del tiempo de desbloqueo antes de que se produzca un evento de apertura retenida. Incrementos de 100 ms. Los valores válidos son de 1000 ms a 300000 ms.
Usar zumbador	Permite que se mantenga abierto para activar una salida de zumbador externo asociada y disparar el zumbador interno en paneles POE. Habilitado por defecto
Detener zumbador al cerrar puerta	Cuando está habilitada, esta función detendrá un evento Retenido abierto una vez que se cierre la puerta. Habilitado por defecto. Cuando está deshabilitado, requiere pasar una tarjeta válida para detener un evento abierto retenido.
Desactivar advertencia previa	Una activación del zumbador de preaviso que ocurre durante el tiempo abierto permitido. Desmarcado por defecto.

Configuración de horarios de puertas

Hora del zumbador	Menú desplegable con varias opciones sobre cuánto tiempo debería durar el zumbador de apertura mantenida. Las distintas opciones son: Hasta puerta cerrada, 5 segundos, 1 minuto, 10 minutos
Modo público	Cuando está habilitado, permite que ocurran eventos de Mantenido abierta cuando la puerta está en un horario desbloqueado. Desmarcado por defecto
Hora del zumbador en modo público	Menú desplegable similar con opciones sobre cuánto tiempo debería durar el zumbador de apertura mantenida. Ocurre solo cuando la puerta está desbloqueada. Las distintas opciones son: Hasta que se cierre la puerta, 5 segundos, 1 minuto, 10 minutos

Abridor Automático

La sección Abrepuertas automático de la página de opciones tiene varias casillas de verificación y controles deslizantes para la configuración con abridores automáticos de puertas. Si su implementación no utiliza una apertura automática, puede pasar a la siguiente sección.

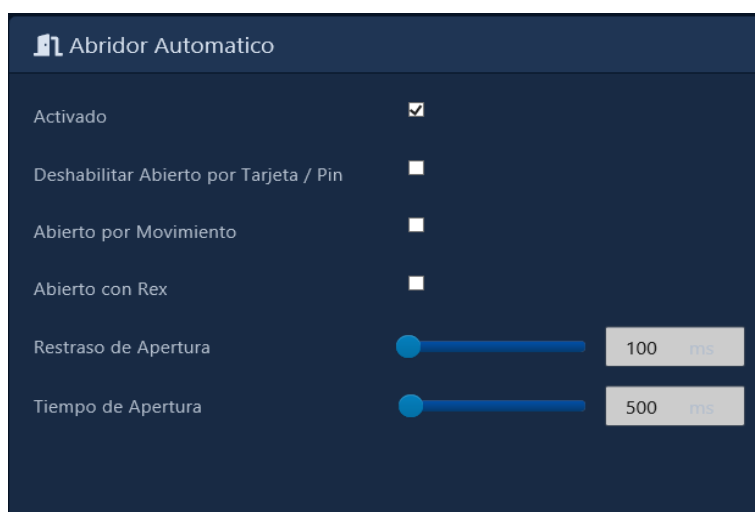


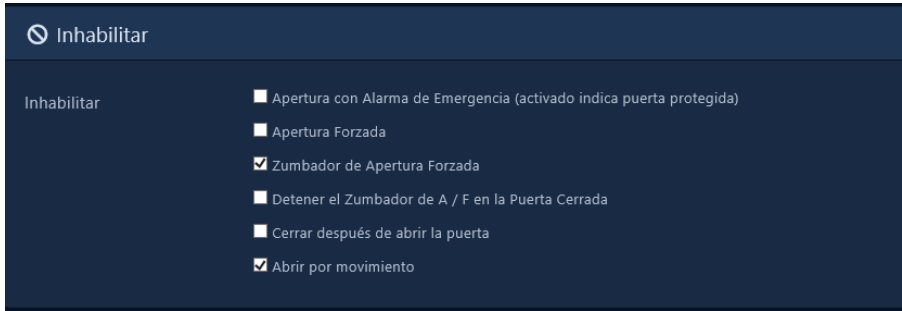
Tabla 8.6. Abridor Automático

Nombre de la casilla de verificación/temporizador	Descripción
Activado	Compruebe si hay un abrepuertas automático conectado a esta puerta. Debe configurarse en la configuración de entrada/salida del panel.
Desactivar abierto por tarjeta	Si está marcada, evita que la presentación de la tarjeta active la apertura automática. El usuario requiere que el atributo "Auto Opener" esté habilitado.
Abierto con movimiento	Si está marcado, permitirá que el movimiento active el abridor automático.
Abierto con REX	Si está marcado, permitirá que REX active el abridor automático.
Retraso del abridor	Retardo antes de la activación de la salida Abre Automático. Incrementos de 100 ms. Los valores válidos son de 100 ms a 20000 ms.
Apertura a tiempo	Tiempo durante el cual estará activada la salida Abre Automático. Incrementos de 100 ms. Los valores válidos son de 100 ms a 20000 ms.

Desactivar

La sección Desactivar de la página de opciones tiene varias casillas de verificación. Cuando se marca una casilla de verificación, ese elemento está deshabilitado. Por ejemplo, si se marca Desbloquear por movimiento, el sensor de movimiento no desbloqueará la puerta.

Tabla 8.7. Desactivar



Casilla de verificación	Descripción
Desbloquear en Alarma de Emergencia	Evite que la puerta se desbloquee cuando se active la alarma de emergencia.
Apertura forzada	Deshabilite los eventos de apertura forzada desde esta puerta.
Zumbador de apertura forzada	Deshabilitar el zumbador de apertura forzada.
Detener zumbador F/O al cerrar la puerta	De forma predeterminada, un evento de apertura forzada se detiene cuando se cierra la puerta; cuando está deshabilitado, el evento de apertura forzada continúa hasta que se presenta una credencial válida.
Bloquear después de abrir la puerta	Deshabilite el bloqueo de la puerta después de que la puerta se abra. Requiere un contacto de puerta.
Desbloquear por movimiento	Desactive el desbloqueo cuando se active el movimiento

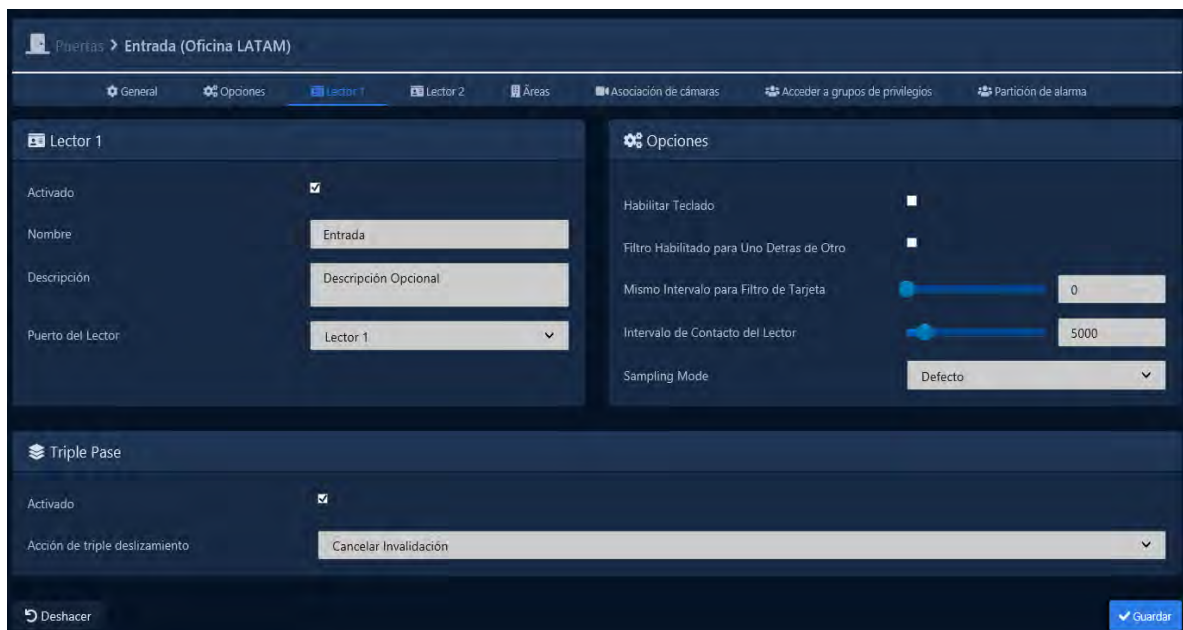
Una vez que haya realizado los cambios deseados, presione el botón **Guardar** en la parte inferior de la página.

Configuración del lector

Las pestañas del Lector tienen varias configuraciones para cada uno de los Lectores adjuntos al Panel. El nombre, la descripción y el número de puerto se pueden reconfigurar. Hay un par de elementos de configuración que no estaban disponibles al agregar la puerta.

Figura 8.4. Configuración del lector

Table 8.8. Opciones de configuración del lector



Configuración de horarios de puertas

Elemento de configuración	Descripción
* Acción (solo modelos de 12 VDC)	Se puede configurar una acción opcional cuando se presenta una credencial al lector. Las acciones disponibles son las mismas que se pueden configurar para triple deslizamiento. La lista de acciones se puede ver en el Capítulo 17, Funciones de triple deslizamiento.
*Realizar acción solo en acceso concedido (solo modelos de 12 V CC)	Cuando está marcado, cualquier acción en el menú anterior solo ocurrirá si la credencial tiene acceso. Cuando no se seleccionan, las credenciales a las que se les deniega el acceso seguirán activando la acción.
Activar teclado	Agrega la funcionalidad del teclado con triple deslizamiento para brindar más opciones. También se requiere para que los calendarios de tarjeta y PIN funcionen como se espera. Esto no es obligatorio para que funcionen los horarios de Tarjeta o PIN o los horarios de PIN solamente.
Intervalo del Teclado	El tiempo permitido entre pulsaciones de teclas en un teclado antes de que se considere que la entrada está completa. Incrementos de 100 ms. Los valores válidos son de 100 ms a 10000 ms.
Filtro activado lector adosado	Habilitar/deshabilitar el temporizador de interferencia del lector adosado. Principalmente en configuraciones de lectores con un Reader de entrada y salida que están lado a lado en la pared. Evita que las tarjetas sean escaneadas por ambos lectores.
Intervalo de interferencia lector consecutivos	Cuando se usan Lectores consecutivos, el tiempo total después de que un Lector recibe una Credencial antes de que el Lector opuesto acepte la misma Credencial. Incrementos de 100 ms. Los valores válidos son de 500 ms a 5000 ms.
Mismo intervalo de filtro de tarjeta	Las credenciales múltiples del mismo valor se ignorarán durante la duración especificada. Útil con puertas donde una credencial de largo alcance puede leer varias veces rápidamente. Incrementos de 100 ms. Los valores válidos son de 0 ms a 25000 ms.
Intervalo de entrada del lector	Tiempo entre deslizamientos antes de varias acciones, como el triple deslizamiento.
Modo de muestreo	Este valor afecta si se utiliza un algoritmo de interferencia en la entrada del lector Wiegand con el objetivo de reducir o eliminar lecturas de tarjetas defectuosas causadas por interferencias como EMI. Los valores son Predeterminado, Modo 1, Modo 2, Modo 4 y Modo 4. El modo de muestreo se puede cambiar en el menú del panel LCD para realizar pruebas más rápidas

Una vez que haya hecho los cambios deseados, presione el botón Guardar en la parte inferior de la página. Si desea obtener información sobre la función Triple deslizamiento, consulte la siguiente sección.

Introducción al triple deslizamiento

El deslizamiento triple se configura en el nivel del Lector en la parte inferior de cada pestaña del Lector. Para ver ejemplos de acciones de triple deslizamiento y escenarios específicos, consulte el Capítulo 17, Funciones de triple deslizamiento.

Solo los usuarios con el privilegio de usuario "*Triple deslizamiento*" o "*Maestro*" pueden realizar acciones de triple deslizamiento. Estas acciones pueden permitir a los tarjetahabientes cerrar la puerta antes de tiempo, armar el sistema de alarma y otras funciones útiles. Para obtener más información sobre la configuración del usuario, consulte la sección denominada "*Privilegios del usuario*".

Áreas

La pestaña Áreas contiene los ajustes de configuración para la configuración del *Área* y *Anti-passback*. Para obtener más información sobre áreas/Anti-passback y requisitos de configuración, consulte el *Capítulo 21, Áreas y Anti-Passback*.

Figura 8.5. Pestaña de áreas

The screenshot shows a configuration window titled 'Áreas'. At the top, there is a note: 'Nota: Las puertas que participarán en las decisiones anti-passback requieren un módulo de memoria opcional. Las puertas que informarán las ubicaciones de los usuarios pero que no participarán en las decisiones anti-passback no necesitan un módulo de memoria. Anti-Passback admite un máximo de 32 códigos de sitio.' Below the note, there are several configuration options:

- 'Agregar área a Oficina LATAM' with a text input field and a green '+' button.
- 'Lector 1 Otorga Acceso al área' with a dropdown menu showing 'Office'.
- 'Lector 2 Otorga Acceso al área' with a dropdown menu showing 'No Area'.
- 'Seguimiento de la ubicación del usuario (sin APB)' with an unchecked checkbox.
- 'Habilitar Anti-passback' with a checked checkbox.
- 'Invalidar configuración de APB de los sitios' with an unchecked checkbox.

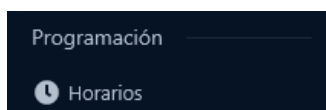
Capítulo 9. Configuración de horarios de puertas

Este capítulo cubre la configuración de Horarios de Puertas en VAX. Para obtener información sobre planificación, conceptos y ejemplos de horarios de puerta, consulte la sección llamada "*Horarios de puerta*".

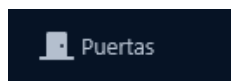
Agregar un horario de puerta

Agregar un horario de puertas en VAX es un proceso optimizado que aprovecha al máximo HTML5. El cronograma de puerta predeterminado 'Acceso siempre con tarjeta' es el cronograma más utilizado en el campo, sin embargo, hay cientos de combinaciones posibles de estados de puerta que pueden adaptarse a muchas situaciones únicas. Los horarios de puerta pueden admitir hasta 40 períodos de tiempo en un día. Esta sección cubre cómo agregar un nuevo horario de puerta.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono **Horarios** y seleccione la pestaña **Puertas**. (en la foto de abajo).



4. En el menú superior, seleccione la sección titulada Puertas.



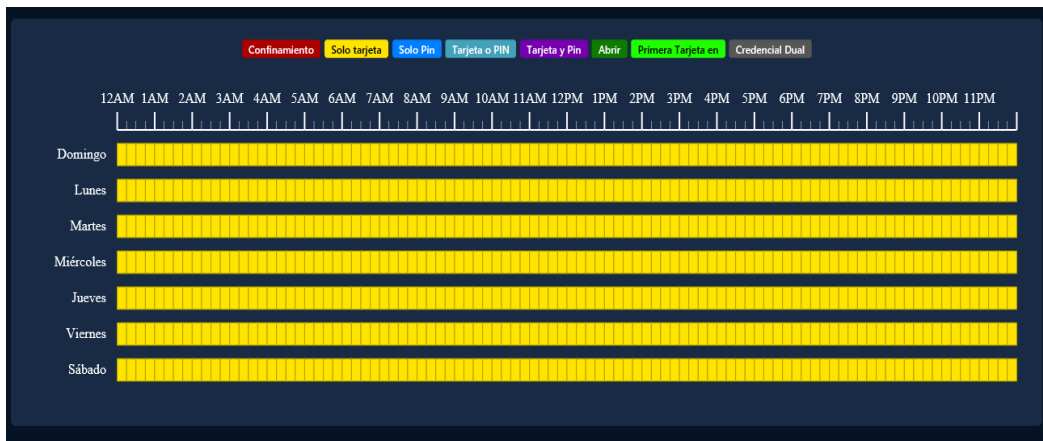
5. En la pantalla Horarios de puerta, verá los Horarios predeterminados. En muchos casos estos Horarios satisfacen las necesidades del sistema; sin embargo, si durante la etapa de planificación usted (el instalador o el usuario final) decidió que se necesitan Programaciones de puerta adicionales, haga clic en el botón Agregar en esta pantalla.
6. En la pantalla **Agregar horario de puertas**, tendrá un par de cuadros de texto para completar.

Tabla 9.1. Agregar horario de puertas

Cuadro de texto	Descripción
Nombre	Nombre único de su Horario. Acepta de 4 a 255 caracteres. Se recomienda nombrar sus Programaciones según la función de la Programación.
Descripción	Descripción opcional del Horario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este horario. Si se selecciona más de uno, se creará una copia para cada partición.

7. Crear el horario es el último paso para crear un horario de puerta. La sección Programación de la página Agregar programación de puerta se muestra a continuación.

Figura 9.1. Editor de horarios de puertas



8. Seleccione el **modo de intervalo** deseado de las opciones en la parte superior. Desde aquí, el usuario ahora puede hacer clic y arrastrar en cualquier lugar de la cuadrícula para crear un nuevo intervalo. Alternativamente, el usuario puede desplazarse hacia abajo simplemente haciendo clic en cualquier intervalo de días y desplazarse hacia abajo para editar intervalos en el widget **Editor de programación** que proporciona una lista de todos los intervalos para el día seleccionado y un segundo widget para realizar cambios

Figura 9.2. Editor de intervalo



9. Utilice el menú desplegable **Selector de día** para seleccionar el día deseado y obtener una lista de todos los períodos de ese día. El usuario puede hacer clic en el **botón + b** para agregar un nuevo lapso y puede usar el botón **Copiar** para copiar el cronograma de días completos a otros días individuales o lapsos de varios días como **Semana, Fin de semana o Días de la semana**. Esto es útil para definir el estado de la Puerta. estará en todo el día, o cambiando el modo para tramos ya presentes. (Para obtener más información sobre los estados de las puertas, consulte la sección denominada "Conceptos.)
10. La sección **Agregar intervalo** del editor de horarios tiene 3 campos que se usan para agregar un tramo de horario de puerta. Cuando se hace clic en los campos Iniciar y Detener, aparecerá un widget de reloj para configurar estos valores. El menú desplegable Modo dictará qué estado de puerta seguirá el horario durante el período de tiempo definido. Una vez que haya completado estos campos, haga clic en el botón **Agregar intervalo**.
11. Ahora debería ver la barra que seleccionó codificada por color según el período de tiempo que agregó. Agregue períodos de tiempo adicionales a ese día si es necesario.

Si desea que el **horario** que ha creado se use para varios días diferentes, puede hacer clic en la lista desplegable **Copiar** y seleccionar la **semana, el fin de semana, los días de semana o los días de la semana** que se requieren para el intervalo creado.

Figura 9.3. Agregar widget de intervalo



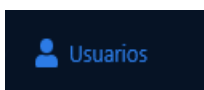
- Una vez que su horario de puerta para los 7 días sea el deseado, ahora puede presionar Guardar para crear el horario de puerta en las particiones seleccionadas. Para obtener información sobre cómo asignar calendarios de puertas a puertas, consulte la sección llamada "Agregar una puerta".

Capítulo 10. Horarios de usuarios

Este capítulo cubre cómo agregar horarios de usuario adicionales a VAX. Para obtener más información sobre qué es un Horario de Usuario, consulte la sección denominada “Conceptos”.

Agregar un **Horario de usuario** en VAX se parece mucho a cómo agregamos otros **Horarios** en el software, como **Horarios de puertas** y **Horarios de piso**. La principal diferencia es que estos Horarios se aplican a los Usuarios a través de **Grupos de Privilegios de Acceso** y solo tienen dos estados posibles, **Permitido** y **No Permitido**. Los horarios de usuario admiten hasta 8 intervalos de tiempo en un día

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono **Horarios** y seleccione la pestaña **Usuarios**. (en la foto de abajo).



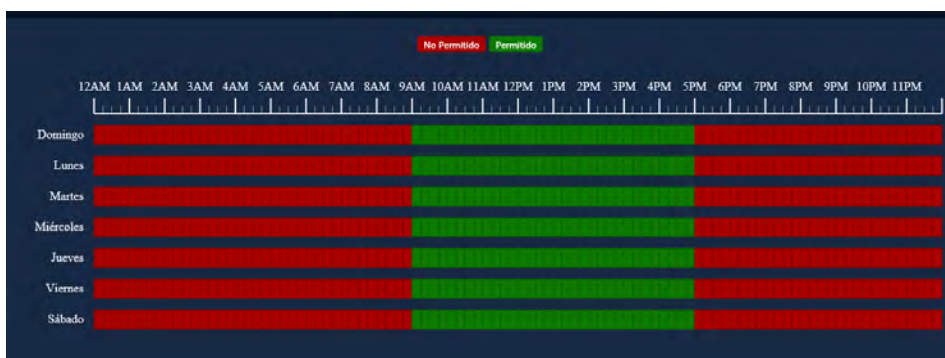
4. En la pantalla Horarios de usuario, verá los Horarios predeterminados. Estos Programas se pueden renombrar y modificar para adaptarse a las necesidades de implementación. Si durante la etapa de planificación usted (el instalador o el usuario final) decidió que se necesitan horarios de usuario adicionales, haga clic en el botón **Agregar** en esta pantalla.
5. En la pantalla **Agregar horario de usuario**, tendrá algunos cuadros de texto para completa.

Tabla 10.1. Agregar un horario de usuario

Cuadros de texto	Descripción
Nombre	Nombre único de su horario de usuario. Acepta de 2 a 60 caracteres. Recomendamos nombrar sus Horarios por la función del Horario.
Descripción	Descripción opcional de su horario de usuario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este programa. Si se selecciona más de una, se creará una copia para cada partición.

6. Programación: la creación de la programación es el último paso para crear una programación de usuario. A continuación se muestra el aspecto de la parte de programación de la página Agregar programación.

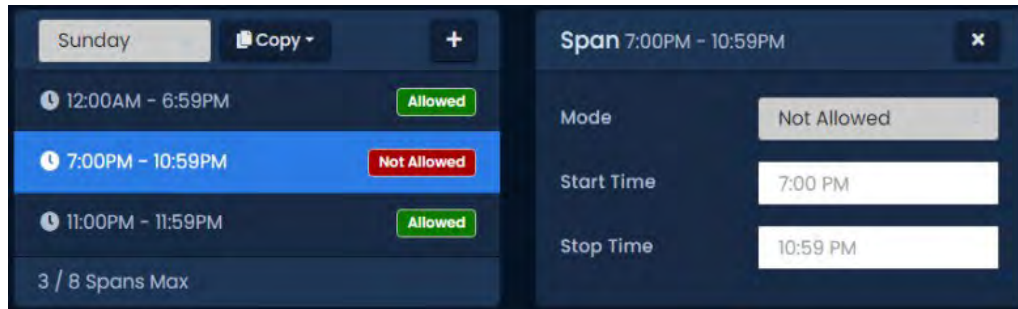
Figura 10.1. Editor de programación de usuario



7. Seleccione el modo de intervalo deseado de las opciones en la parte superior. Desde aquí, el usuario ahora puede hacer clic y arrastrar en cualquier parte de la cuadrícula para crear un nuevo tramo. Alternativamente, el usuario puede desplazarse hacia abajo simplemente haciendo clic en

cualquier intervalo de días y desplazarse hacia abajo para editar intervalos en el widget Editor de programación que proporciona una lista de todos los intervalos para el día seleccionado y un segundo widget para realizar cambios.

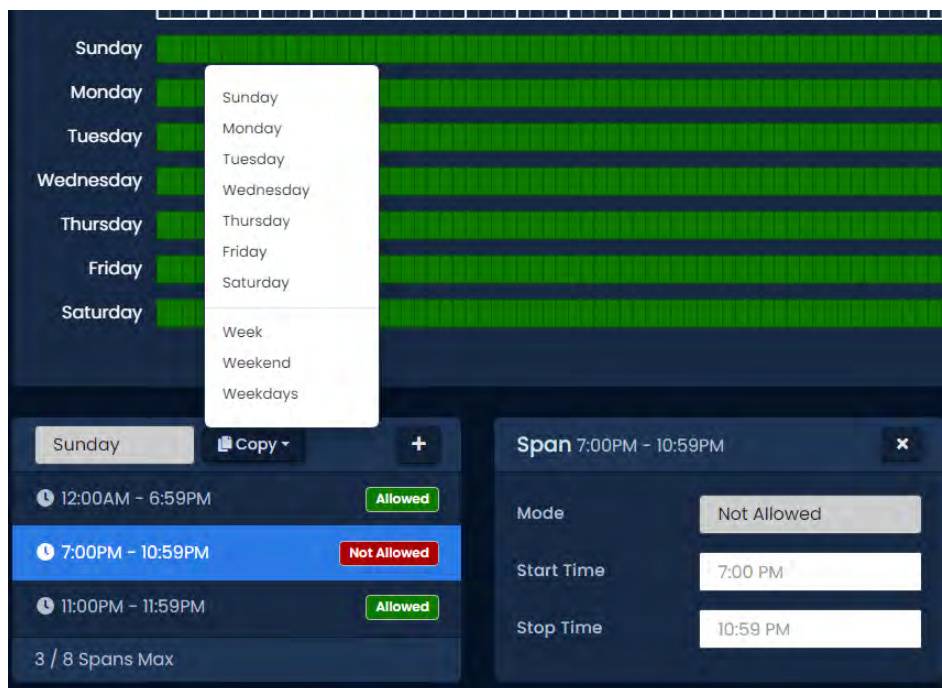
Figura 10.2. Editor de horarios



8. Utilice el menú desplegable **Modo** para seleccionar el estado de acceso del usuario para el tramo seleccionado. Solo **Permitido y No Permitido** están disponibles.
9. La sección **Agregar un intervalo** del editor horarios tiene 3 campos que se usan para agregar un intervalo de programación de usuario. Cuando se hace clic en los campos **Iniciar y Detener**, aparecerá un widget de reloj para configurar estos valores. El menú desplegable **Modo** dictará qué estado de acceso de usuario seguirá el programa durante el período de tiempo definido. Una vez que haya completado estos campos, haga clic en el botón **Agregar intervalo**.
10. Ahora debería ver la barra que seleccionó codificada por color según el período de tiempo que agregó. Agregue períodos de tiempo adicionales a ese día si es necesario.

Si desea que el horario que ha creado se use para varios días diferentes, puede hacer clic en la lista desplegable **Copiar y seleccionar la semana, el fin de semana, los días de semana o los días de la semana** que se requieren para el intervalo creado.

Figura 10.3. Agregar widget de intervalo



11. Una vez que su horario de usuario para los 7 días sea el deseado, ahora puede presionar Guardar para crear el horario de usuario en las particiones seleccionadas. Para obtener información sobre cómo asignar horarios de usuario a los usuarios, consulte el *Capítulo 11, Grupos de privilegios de acceso*.

Capítulo 11. Grupos de privilegios de acceso

Este capítulo cubrirá cómo agregar un **grupo de privilegios de acceso** en VAX. Si desea obtener más información sobre la planificación de un grupo de privilegios de acceso y escenarios de ejemplo, consulte la sección denominada "Conceptos".

Como se mencionó en el Capítulo 5; Los Grupos de Privilegios de Acceso son el método que damos a los **Usuarios Acceso o No Acceso a Lector(es)/Pisos**. Los usuarios que necesitan el mismo nivel de acceso se colocan en un grupo, mientras que los usuarios con necesidades de acceso adicionales se colocan en un grupo diferente.

Alternativamente, podemos crear nuestros Grupos de Privilegios de Acceso basados en las Puertas/Puertas en el grupo, dándonos un control adicional sobre a qué Puertas/Pisos pueden acceder los Usuarios.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**, haga clic en **Grupos de privilegios de acceso** icono (en la foto de abajo icon)




4. En la pantalla Grupos de privilegios de acceso, notará cualquier grupo que ya haya creado. Haga clic en el botón **Agregar** en esta pantalla.
5. En la pantalla **Agregar grupo de privilegios** de acceso, tendrá algunos campos para completar.

Grupo


Tabla 11.1. Agregar un grupo de privilegios de acceso

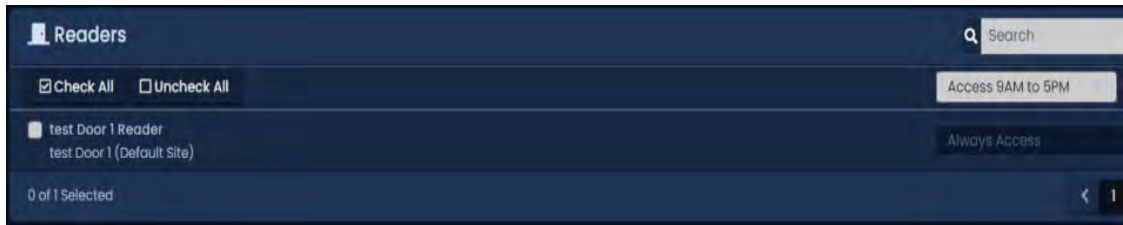
Cuadros de texto	Descripción
Nombre	Nombre único de su grupo de privilegios de acceso. Acepta de 2 a 60 caracteres. Recomendamos nombrar el grupo por el tipo de Usuarios que estarán en el grupo.
Descripción	Descripción opcional de su grupo de privilegios de acceso. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este grupo de privilegios de acceso. Solo se podrán asignar lectores de esa partición.

6. Una vez que haya seleccionado una **Partición, Usuarios, Lectores y Pisos** que hayan sido configurados, esa Partición aparecerá en las tres secciones inferiores de la página.

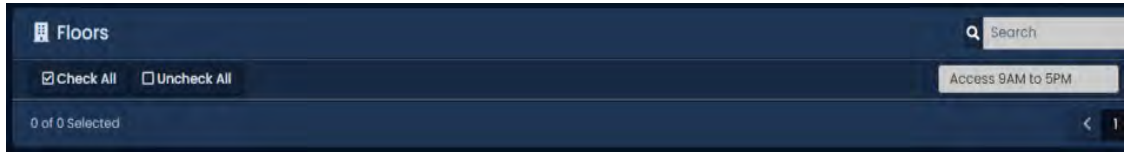
 **Nota:** Los usuarios son opcionales al crear un grupo de privilegios de acceso. Se pueden agregar más tarde según sea necesario.

7. En la sección Lectores: Seleccione la casilla de verificación a la izquierda de cualquier Lector al que el grupo de acceso requiera acceso. Utilice el menú desplegable del lado derecho para seleccionar el Programa de usuario que se aplicará a este grupo en ese Lector. Si un Lector no está marcado, a los Usuarios del grupo se les negará el acceso a los Lectores no marcados (a menos que un Usuario sea parte de un Grupo de Privilegios de Acceso diferente que les otorga acceso).

 **Nota:** Si ninguno de los horarios de usuario coincide con los requisitos del grupo de acceso, puede crear un nuevo horario de usuario, consulte el Capítulo 10, Horarios de usuario.



8. En la sección Pisos: Seleccione la casilla de verificación a la izquierda de cualquier Piso al que el grupo de acceso requiera acceso. Utilice el menú desplegable del lado derecho para seleccionar el horario de usuario que se aplicará a este grupo en ese piso. Si un Piso no está marcado, a los Usuarios del grupo se les negará el acceso a los Pisos no marcados (a menos que un Usuario sea parte de un Grupo de Privilegios de Acceso diferente que les otorga acceso).



9. . Una vez que haya seleccionado los Lectores y Horarios de usuario asociados con cada Lector; puede crear el grupo de privilegios de acceso. Si hay usuarios en otros grupos de acceso en la misma partición, puede agregarlos al grupo en esta pantalla (siempre que su grupo de privilegios de acceso no entre en conflicto con uno que se está creando).
10. Una vez que esté satisfecho con la configuración (que se puede editar más tarde según sea necesario), haga clic en el botón verde **Crear**.

Capítulo 12. Configuración de usuarios/titulares de tarjetas

Este capítulo cubrirá la adición de **usuarios/titulares de tarjetas** en VAX, cómo aplicar privilegios de usuario especiales, agregar credenciales (como tarjetas, fobs, PIN y pucks), agregar imágenes de titulares de tarjetas, cómo importar usuarios desde archivos de texto y cómo agregar campos a los usuarios.

Agregar un usuario en VAX es un proceso bastante simple, sin embargo, hay una variedad de opciones que aprovechan las diversas características de nuestro software.

Antes de agregar Usuarios a VAX, por lo general querrá alguna información sobre el rol de cada Usuario. Si no toda esta información está disponible, puede agregar esta información más tarde.

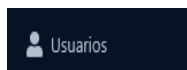
- Nombre y apellido del Usuario.
- Cualquier privilegio especial que el Usuario pueda necesitar, como el acceso de triple deslizamiento; estos privilegios se explicarán en la siguiente sección.
- Credenciales de las tarjetas/fobs que se le asignarán al Usuario. Si esto no está disponible, se puede agregar más tarde.
- A qué **grupos de privilegios de acceso** pertenecerá este usuario.

Una vez que se haya recopilado esta información, ahora podemos comenzar a agregar usuarios/titulares de tarjetas a VAX. La adición de usuarios/titulares de tarjetas se puede hacer de varias maneras diferentes:

- Agregue cada usuario de uno en uno.
- Importe grandes cantidades de usuarios a la vez utilizando una importación CSV.
- Inscriba al usuario haciendo clic en la notificación "Acceso denegado de usuario desconocido" que se genera cuando se presenta una credencial desconocida a un lector.
- Sincronice VAX con un proveedor de LDAP como Active Directory (consulte el *Capítulo 32, Integración de Active Directory* para obtener más información sobre la integración de LDAP).

Agregar un usuario: un usuario a la vez

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**; haga clic en el ícono de **Usuarios** (en la imagen a continuación).



4. En la pantalla Usuarios, verá los Usuarios que ya haya creado. Haga clic en el botón Agregar en esta pantalla.

Privilegios de usuario

En la página **Agregar usuario**, habrá varios cuadros de texto y casillas de verificación para completar, incluidos **Privilegios especiales de usuario**. El siguiente cuadro brinda una breve explicación de cada elemento en la sección **General de la página Agregar usuarios**. Todas las configuraciones generales son opcionales excepto Nombre y Apellido.

Tabla 12.1. Agregar usuario: configuración general

Cuadros de texto / casilla de verificación	Descripción
Nombre	El nombre del Usuario. Acepta de 1 a 60 caracteres.
Apellido	El apellido del Usuario. Acepta de 1 a 60 caracteres.
Empieza el	La fecha en que el Usuario se vuelve activo. Antes de esta fecha, se negará el acceso al Usuario independientemente del Horario o privilegio (opcional). El tiempo tiene una precisión de 10 minutos. Los modelos de paneles Aperio son precisos al día.
Expira el	La fecha en que se revocará automáticamente el acceso de los Usuarios. Útil para contratistas y trabajadores temporales (opcional). El tiempo tiene una precisión de 10 minutos. Los modelos de paneles Aperio son precisos al día.
Nivel de crisis	El nivel de seguridad que se le otorga al usuario cuando se inicializa el modo Crisis. Si el nivel de seguridad es igual o mayor que el Nivel de Crisis, se le otorgará acceso al Usuario. Para obtener más información sobre los niveles de crisis, consulte el Capítulo 15, Niveles de crisis
Maestro	Habilitar/deshabilitar el privilegio de usuario maestro. Los Usuarios Maestros tienen acceso completo a todas las Puertas y Pisos, sin importar el horario u otros privilegios. Habilita implícitamente los permisos de triple deslizamiento para el usuario. Útil para el personal de seguridad o personal de emergencias.
Supervisor	Habilitar/deshabilitar el privilegio de usuario supervisor. Los usuarios supervisores se pueden utilizar para otorgar acceso a otros usuarios a las puertas donde la credencial doble es el estado de la puerta y se requiere supervisor. Los supervisores pueden tener acceso a las puertas cuando están bloqueadas, pero solo si su grupo de privilegios de acceso lo permite
Primera tarjeta en	Habilite o deshabilite el privilegio Primera credencial de entrada para este usuario. Esto le permite al usuario activar un modo de desbloqueo de la puerta cuando la puerta sigue una primera credencial en horario.
Triple deslizamiento	Habilite/desactive el privilegio del usuario para activar cualquier acción de deslizamiento triple preconfigurada en la puerta. Para obtener más información sobre las opciones de triple deslizamiento, consulte el Capítulo 17, Funciones de triple deslizamiento.
Desactivar alarma	Habilite/desactive el privilegio del usuario para desactivar la alarma de emergencia mediante un doble deslizamiento..
Abridor automático	¿Este usuario requiere que se active un abridor automático (si está disponible)?

Nota

El nombre y el apellido son los únicos campos obligatorios en la sección General de la página para agregar un usuario.

Figura 12.1. Ejemplos de configuración general

The screenshot displays two panels for user configuration. The left panel, titled 'General', contains the following fields: 'Primer Nombre' (First Name) with the value 'Angie', 'Apellido' (Last Name) with the value 'Belíco', and 'Email'. Below these are two empty text boxes for 'Comienza en' (Starts on) and 'Expira en' (Expires on). The right panel, titled 'Permissions', includes a 'Nivel de Crisis' (Crisis Level) dropdown menu set to 'Default: Follow Schedule'. Under 'Privilegios' (Privileges), there are several toggle switches: 'Master' (checked), 'Supervisor' (unchecked), 'Primera Tarjeta en' (unchecked), 'Triple Pase' (unchecked), 'Desconectar Alarma' (checked), and 'Abridor automático' (unchecked). At the bottom of the permissions section is a 'Desahabilitado' (Disabled) toggle switch, which is currently turned off.

Imágenes del titular de la tarjeta

La siguiente sección es Imágenes. Puedes subir hasta 3 imágenes por Usuario. La imagen del Titular de la Tarjeta es la imagen principal que aparecerá en las notificaciones para ese Usuario. Los accesorios 1 y 2 se pueden usar para imágenes adicionales de credencialización fotográfica. También puede tomar fotografías directamente desde el navegador web si un dispositivo de imágenes está conectado a la computadora y está usando Google Chrome.

Las imágenes se almacenan en el servidor VAX en: "<Installation Directory>\VAX\WebServer\content\Uploads\UserProfilePictures".

No se requiere una imagen del titular de la tarjeta para agregar un usuario. Se puede agregar/editar una imagen en cualquier momento.

Figura 12.2. Ejemplo de imágenes

The screenshot shows the 'Imágenes' (Images) section of the user configuration interface. It features a 'Titular de la tarjeta' (Cardholder) field with a small profile picture of a man. Below this are two 'Accesorio' (Accessory) fields, labeled 'Accesorio 1' and 'Accesorio 2'. Each accessory field has an 'Escoger...' (Choose...) button and a 'Browse' button to the right, indicating that users can upload additional photos for identification purposes.

Campos Personalizados

La siguiente sección es Campos personalizados. Si se han creado previamente campos personalizados, se pueden completar en esta pantalla para cada usuario. Si necesita crear campos personalizados adicionales, consulte la sección llamada "Agregar campos personalizados".


Figura 12.3. Campos personalizados: Ejemplo

The screenshot shows the 'Agregar Campo Personalizado' (Add Custom Field) interface. The breadcrumb path is 'Campos Personalizados > Agregar Campo Personalizado'. The 'General' section includes the following fields: 'Nombre' (Name) with the value 'Necesario', 'Tipo de Campo' (Field Type) with a dropdown menu set to 'Escoger...' (Choose...), and three checkboxes: 'Mandatorio' (Mandatory), 'Aparece en Monitoreo' (Appears in Monitoring), and 'Aparece en la página de usuarios' (Appears in the user page), all of which are currently unchecked. At the bottom left is a 'Borrar' (Delete) button, and at the bottom right is a '+ Crear' (Create) button.

Credenciales de usuario

The next section is **Credentials**. Here you can add a variety of Credentials such as cards, fobs, PINs or a combinations of these credentials.

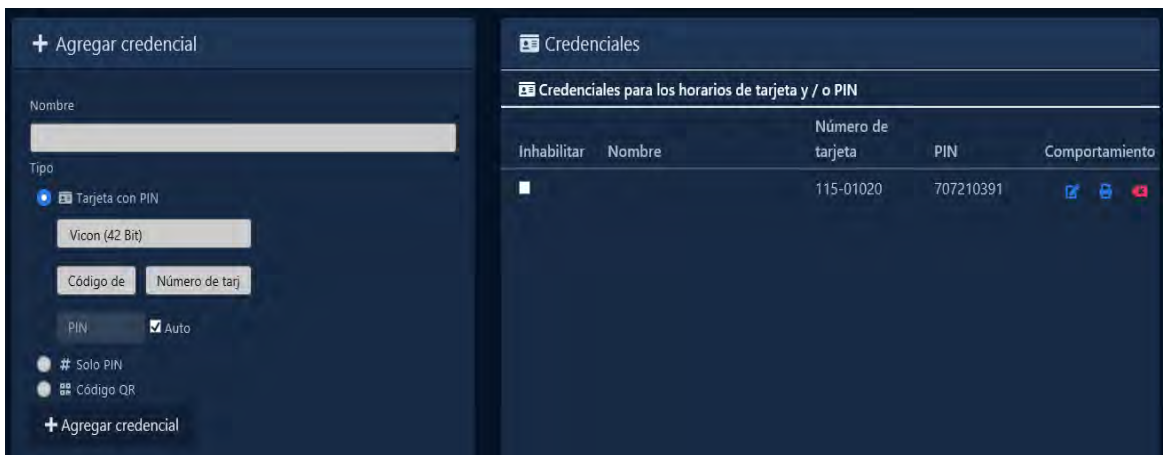
1. Ingrese el **código de sitio** (también conocido como código de instalación) y el número de tarjeta de la Credencial en los cuadros de texto **Código de sitio y Número de tarjeta**. Se generará automáticamente un número de **PIN** asociado con la Credencial para los horarios de Tarjeta y PIN, a menos que la casilla de verificación Auto no esté marcada.

 **Nota:** Si su sitio no utiliza programaciones de PIN, se ignorará el PIN generado automáticamente

2. Una vez que haya ingresado la información de la credencial, haga clic en el botón **Agregar credencial**. La credencial que ingresó se moverá al lado derecho de la pantalla, lo que indica que se realizó correctamente.
3. Para agregar credenciales de PIN para programaciones de **solo PIN**, haga clic en el botón de opción Pin Only e ingrese un PIN (de forma predeterminada, se generará uno automáticamente). Una vez ingresado, haga clic en el botón **Agregar credencial**.

Ahora puede ingresar cualquier Credencial adicional asociada con el Usuario.

Figura 12.4. Credenciales: Ejemplo




Dependiendo del Horario de la Puerta, el lector esperará diferentes tipos de credenciales del Usuario.

Horarios de la tarjeta. El lector esperará una presentación de tarjeta/fob del Usuario.

Horarios de Tarjeta y Pin. El lector esperará una presentación de tarjeta/fob, seguida de una entrada de PIN que coincida con la tarjeta asociada. En el ejemplo anterior, un Usuario presenta su tarjeta '025-23847'. El lector esperará el PIN '1234' después de la presentación de la tarjeta.

Horarios de Tarjeta o Pin. El lector esperará una presentación de tarjeta/fob o PIN. En el ejemplo anterior, el Usuario puede presentar una de sus dos tarjetas o ingresar el PIN '59278'. El PIN '1234' no funcionará con este horario porque está adjunto a una tarjeta.


Pin Solo Horarios. El lector solo esperará PIN en este horario. En el ejemplo anterior, el PIN '59278' otorgará acceso. Los números PIN adjuntos a las tarjetas no funcionarán con este horario.

 **Nota:** Las credenciales no son obligatorias para agregar un usuario y se pueden agregar después de que se crea el usuario.

Grupos de Acceso

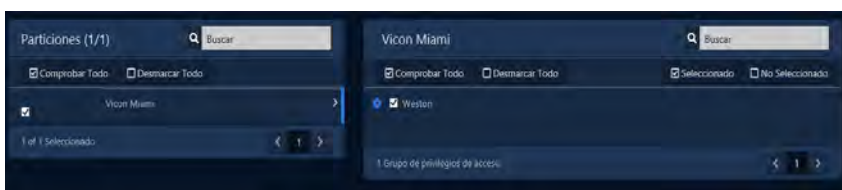
La última sección para agregar un usuario es asignar el usuario a **grupos de privilegios de acceso**. Si no ha creado uno, consulte el *Capítulo 11, Grupos de privilegios de acceso*


Todas las particiones para las que tiene permiso para ver tendrán sus grupos de privilegios de acceso asociados mostrados aquí. Seleccione los grupos de acceso a los que el usuario debe pertenecer.

 **Nota:** Si no hay un grupo de privilegios de acceso disponible en la partición seleccionada, el usuario puede asignarse a esa partición y agregarse a un grupo de privilegios de acceso en un momento posterior.

Una vez que haya seleccionado el grupo de privilegios de acceso y/o la partición a la que debe pertenecer el usuario, ahora puede hacer clic en **Crear** para crear el usuario.

Figura 12.5. Grupo de acceso: ejemplo

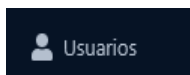


 **Nota:** Para que los controladores de puerta conozcan las nuevas credenciales y usuarios, debe realizar una actualización del panel. Consulte la sección llamada "Actualización de su panel".

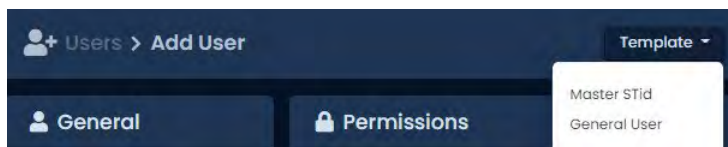
Plantillas de Usuario

Los administradores pueden crear plantillas de usuario para agregar más rápidamente tipos comunes de usuarios. Agregar y actualizar plantillas de usuario es simple:

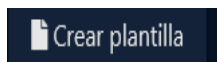
1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**; haga clic en el ícono de **Usuarios** (en la imagen a continuación).



2. En la pantalla Usuarios, haga clic en el botón **Agregar**.
3. En la parte superior de la pantalla Agregar usuario, el menú desplegable Plantilla contendrá las plantillas existentes. Seleccione una plantilla para usarla o para actualizarla. Déjalo en blanco si está creando uno nuevo.




4. Complete los privilegios (triple deslizamiento, Primera entrada de tarjeta, etc.), Comienza el, Caduca el, Particiones y Grupos de acceso que desea incluir en la plantilla.
5. Haga clic en Crear plantilla o Actualizar plantilla en la parte inferior izquierda de la pantalla.



6. Se le pedirá que asigne un nombre a la plantilla de usuario. De forma predeterminada, las plantillas solo las verá el administrador que las crea. Establecer la plantilla como Global hace que aparezca para todos los administradores, independientemente de las particiones.

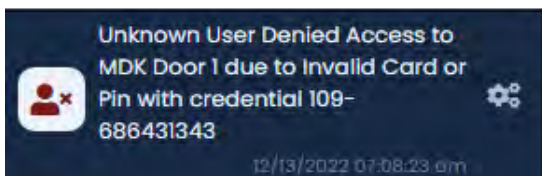
7. Haga clic en Guardar. La plantilla se creará y ahora aparecerá en el menú desplegable Plantillas al agregar un usuario.

 **Nota:** Si una plantilla proporciona acceso a una partición para la que un administrador no tiene permiso, el usuario creado no formará parte de esa partición.

Inscripción de titulares de tarjetas mediante notificación

Es posible inscribir usuarios/titulares de tarjetas sin escribir ninguna información de credenciales en el software. Esta sección cubre cómo podemos inscribir a un Usuario/ Titular de tarjeta simplemente presentando su nueva Credencial en un lector disponible.

1. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
2. En la página principal de VAX, preste mucha atención al área de notificación en el lado derecho de la pantalla.
3. Obtenga la nueva Credencial que actualmente no está asignada a ningún Usuario/Titular de tarjeta en VAX.



4. En un Lector cercano, presente la nueva Credencial. Se denegará el acceso a la Credencial y aparecerá una notificación en el software.
5. Haga clic en la notificación "Usuario desconocido acceso denegado a <nombre del lector> debido a tarjeta o PIN no válidos con credencial <código del sitio>-<número de tarjeta>"
Esto nos llevará a la pantalla Agregar usuario, con la credencial rellena previamente en función de la credencial correspondiente a la notificación en la que hizo clic.
6. Complete los campos necesarios adicionales.

Consejo

Si el sitio está muy ocupado, puede hacer clic en el botón "Detener" que se encuentra justo encima del área de notificación para pausar las notificaciones en vivo; esto le dará tiempo adicional para buscar y hacer clic en la notificación correcta para agregar el nuevo usuario/titular de la tarjeta.

Importación de usuarios y titulares de tarjetas

Esta sección cubre cómo importar grandes cantidades de usuarios y credenciales a VAX. Esto se usa a menudo cuando hay una gran cantidad de titulares de tarjetas para agregar.

La importación de tarjetas funciona mediante el análisis de un archivo CSV (valores separados por comas) que tiene datos de usuario de manera consistente y predefinida. Por lo general, será una hoja de cálculo o incluso un archivo de texto. El archivo de texto deberá completarse antes de la importación, y el formato del archivo se verá generalmente así:

Brandon, Riley, 24, 6338

Christine, Payne, 24, 7568

Judy, Lawson, 24, 6496

Patricia, Wright, 24, 7674

Kevin, Turner, 24, 8797

Theresa, Sims, 24, 8688

También se pueden agregar tarjetas adicionales, PIN y valores personalizados aquí en este archivo.

! **Advertencia:**

Los nombres y apellidos no deben contener ninguno de los siguientes caracteres; ?, #, \$, %, ^, &, *, (,), @, !, <, >, +, =, \, /, :, ;, ", ~

Guarde el archivo como **Import.CSV**. También puede usar un programa de hoja de cálculo, siempre que los usuarios estén separados por líneas y el archivo se guarde como un archivo CSV.

Para importar el archivo, sigue estos pasos:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**; haga clic en el ícono **Importar tarjetas** (en la imagen a continuación).



4. En la pantalla **Importar tarjetas**, haga clic en el botón Elegir archivo en el medio de la pantalla. Aparecerá una ventana del Explorador de Windows; navegue y seleccione el **archivo CSV**.
5. Una vez que haya seleccionado el archivo, haga clic en el botón **Analizar** en el lado derecho de la pantalla. VAX ahora escaneará el archivo y procederá al paso 2.

Figura 12.6. Opciones de importación

6. Utilice el menú desplegable **Grupo de acceso** y seleccione los **grupos de privilegios de acceso** en los que se ubicarán estos usuarios. Puede seleccionar más de 1 grupo.

Nota: Será necesario seleccionar al menos 1 grupo de acceso existente en el menú desplegable, incluso al importar los grupos de privilegios de acceso de los usuarios como una columna.

7. Utilice el menú desplegable **Nivel de crisis** y seleccione el nivel de seguridad apropiado para los usuarios que se están importando.
8. Utilice el menú desplegable **Credencial n.º 1:** y seleccione el tipo de credencial que se importa con cada usuario. Haga clic en el botón + para agregar más de una credencial.
9. Se mostrará un registro de usuario de muestra y todas las columnas encontradas. El tipo de datos debe seleccionarse para cada columna. Complete estas selecciones para cada columna (la selección mínima requerida es Nombre, Apellido, Credencial n.º 1, Código del sitio, Credencial n.º 1, Número de tarjeta).

Tabla 12.2. Importación de tipos de datos de usuario

Tipos de datos	Ejemplo
Nombre	Alice
Apellido	Pierce
Empieza el	2014-12-16
Expira el	2014-12-24
Maestro, Supervisor, Entrada de la primera tarjeta, Deslizamiento triple, Alarma de desactivación, Abridor con desventaja	Verdadero, 1, Sí o ENCENDIDO habilitarán el atributo para el usuario. Cualquier otra cosa será considerada 'falsa'
Credencial # Código del sitio	33
Credencial # Número de tarjeta	48503
Credencial # PIN	1234

10. Haga clic en Validar en la parte inferior de la página una vez que haya completado todas las columnas y grupos de acceso.

11. VAX ahora validará los registros. Puede usar esta oportunidad para revisar cualquier error. Los registros que no se pueden importar se resaltarán en rojo.

Figura 12.7. Vista previa de importación

Record #	First Name	Last Name	Don't Import	Credential #1 Site Code	Credential #1 Card Number	Pin Number	Don't Import	Don't Import	Don't Import	Don't Import	Don't Import
1	User First Name	User Last Name	Classification	Site Code	Card Number	Pin Number	Crisis Level	Start Date	Expires On	User Disabled	Card Disabled
<input checked="" type="checkbox"/>	Alisha	Jagir	Standard	22	12007	745442690	Default: Follow Schedule			False	False
<input checked="" type="checkbox"/>	AnneCorinne	Vilma	Standard	22	12024	556347757	Default: Follow Schedule			False	False
<input checked="" type="checkbox"/>	Brandise	Vanni	Standard	22	12017	253623682	Default: Follow Schedule			False	False
<input checked="" type="checkbox"/>	Carol-Jean	Chauncey	Standard	22	12005	214730559	Default: Follow Schedule			False	False

12. Haga clic en **Importar archivo** para importar los usuarios. Los usuarios que cambiaron a rojo no se importaron debido a un error.

Ahora puede editar esos usuarios y agregar privilegios de usuario adicionales o agregar valores de campo personalizados.

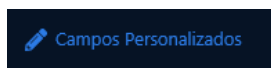
Agregar campos personalizados

Esta sección demostrará cómo agregar campos personalizados adicionales a VAX.

El propósito de los campos personalizados es permitir que los administradores agreguen información personalizada a los usuarios/titulares de tarjetas que sea específica para sus necesidades. Pueden usar la información personalizada para ordenar y buscar usuarios. Puede agregar tantos campos personalizados como necesite.

Para crear campos personalizados adicionales, siga estos pasos:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**; haga clic en el ícono de **Campos personalizados** (en la imagen a continuación).



2. En la pantalla **Campos personalizados**, verá los campos personalizados que ya haya creado. Para agregar un campo adicional, haga clic en el botón **Agregar**.

Figura 12.8. Campos Personalizados

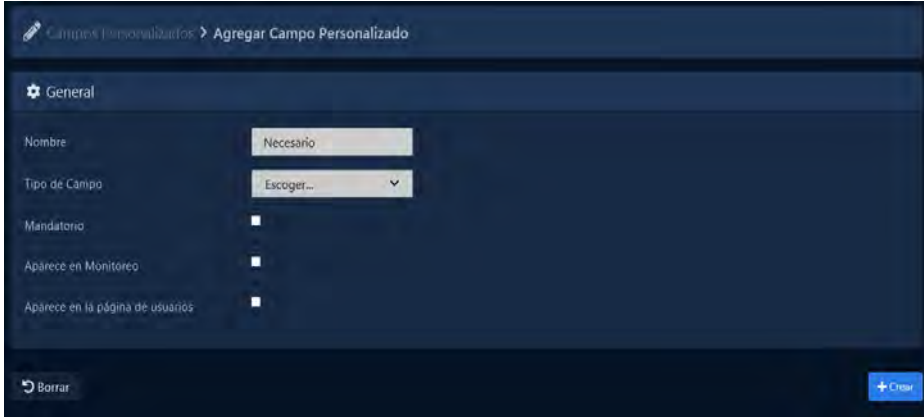
Nombre	Tipo	Mandatorio
No se encontró ningún registro.		

Consejo

Puede cambiar el orden en que aparecen los campos personalizados haciendo clic y arrastrando el icono a la izquierda del nombre del campo personalizado.

Figura 12.9. Agregar Campos Personalizados

3. En la pantalla **Agregar campos personalizados**, complete el Nombre de su campo personalizado.



4. Elija un **Tipo de campo**. Los tipos de campo se describen en la siguiente tabla.

Tabla 12.3. Tipo de campo

Tipo de campo	Descripción
Cadena	Valores de campo personalizados para ser una serie de texto y/o números. Utiliza un cuadro de texto al introducir valores.
Casilla de verificación	El valor del campo personalizado se muestra como una casilla de verificación. Simboliza Verdadero/Falso.
Desplegable	El valor del campo personalizado se muestra como un menú desplegable. Al agregar el campo, seleccionará qué valores están disponibles en el menú desplegable.
Fecha	El valor del campo personalizado se muestra como un selector de fecha de estilo de calendario.

5. Al marcar la casilla de verificación **Obligatorio**, el campo personalizado será obligatorio cuando se agregue un usuario.
6. Al marcar la casilla de verificación **Aparece** en el monitoreo, el valor del campo personalizado aparecerá en la pantalla Monitoreo VAX cuando se seleccione un registro de usuario.
7. Si el tipo de campo es una cadena, se puede ingresar una cadena de formato para agregar una validación adicional al ingresar valores. Por ejemplo, ingresar 'd' sin las comillas restringirá una cadena a solo números. Consulte la referencia rápida de Microsoft [[https://msdn.microsoft.com/en-us/library/az24scfc\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx)] sobre expresiones regulares.
8. Si el Tipo de campo es Fecha, se puede usar una cadena de formato para definir cómo se debe mostrar/ingresar la fecha (AAAA-MM-DD). Consulte esta página [<http://momentjs.com/docs/#/parsing/string-format/>] como referencia.
9. Haga clic en Guardar, el campo personalizado ahora estará disponible en la pantalla Agregar/Editar usuario, así como en la pantalla Usuarios al seleccionar Personalizado como la opción de clasificación.

Capítulo 13. Configuración de días festivos

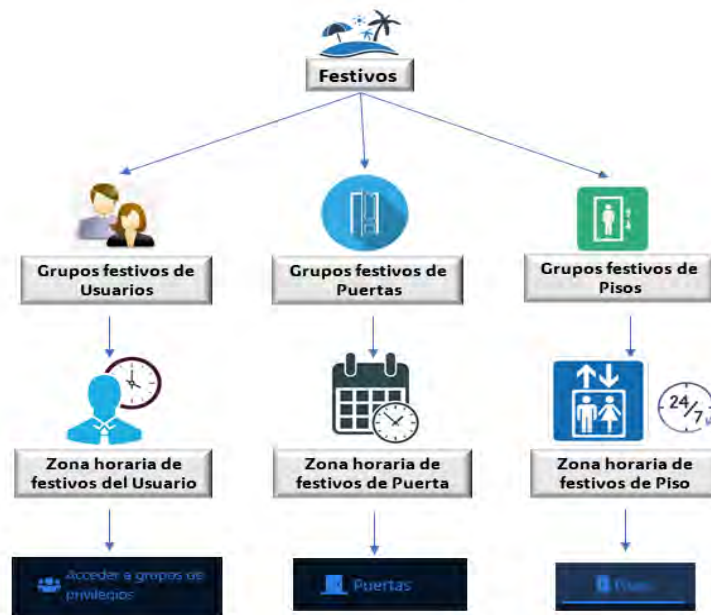
Este capítulo cubrirá la configuración de varios componentes de vacaciones en VAX. Le recomendamos que lea la sección llamada "Días festivos" antes de leer este capítulo para planificar cómo un día festivo debería afectar su sistema y una explicación de los componentes involucrados.

Los 8 componentes de Festivos en VAX son:

- Programaciones de días festivos del usuario
- Grupos de días festivos de usuarios
- Horarios de días festivos de la puerta
- Grupos de días festivos en puerta
- Horarios de Feriados de Piso
- Grupos de festivos de piso
- Días festivos

A continuación se muestra una visualización de cómo estos componentes se aplican entre sí.

Figura 13.1. Diagrama de configuración de días festivos



Orden de operaciones de días festivos

Aunque estos componentes de festivos pueden ser componentes en cualquier orden, hay un orden general de configuración que debe cumplirse

1. Calendario de días festivos de usuario/puerta/piso:

Después de planificar cómo deben comportarse las Puertas/Pisos/Usuarios durante un día festivo, cree estos Cronogramas de días festivos apropiados en función de los cronogramas que deben desviarse de sus cronogramas normales.

2. Grupo de días festivos de usuario/puerta/piso: si se necesitan más grupos de días festivos que los predeterminados, agréguelos.

3. **Festivos:** Agregue el feriado y seleccione qué grupos de usuarios/puertas/pisos deben verse afectados por el feriado y qué cronogramas de feriado se deben cumplir en ese feriado.
4. **Asignación de Usuario/Puerta/Piso a Grupos de Festivos:** La última parte de un festivo es la asignación de Puertas, Pisos y Grupos de Privilegios de Acceso a sus Grupos de festivos correspondientes.

Programaciones de días festivos del usuario

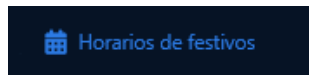
Esta sección cubrirá la configuración de los **calendarios de días festivos de los usuarios**. Por defecto, VAX viene instalado con 2 Programaciones de festivos de usuario predeterminadas:

Acceso Festivo 9AM a 5PM: con horario de 'Permitido' de 8am a 5pm y 'No Permitido' en cualquier otro horario del día.

Festivo Sin Acceso: con horario de 'No Permitido' todo el día.

Aunque esto a menudo es suficiente para la mayoría de las configuraciones de días festivos, es bastante fácil agregar horarios adicionales de días festivos del usuario o editar los horarios predeterminados.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la barra lateral, desplácese hacia abajo hasta la sección titulada Programación; haga clic en el icono Horarios de días festivos (en la imagen a continuación).



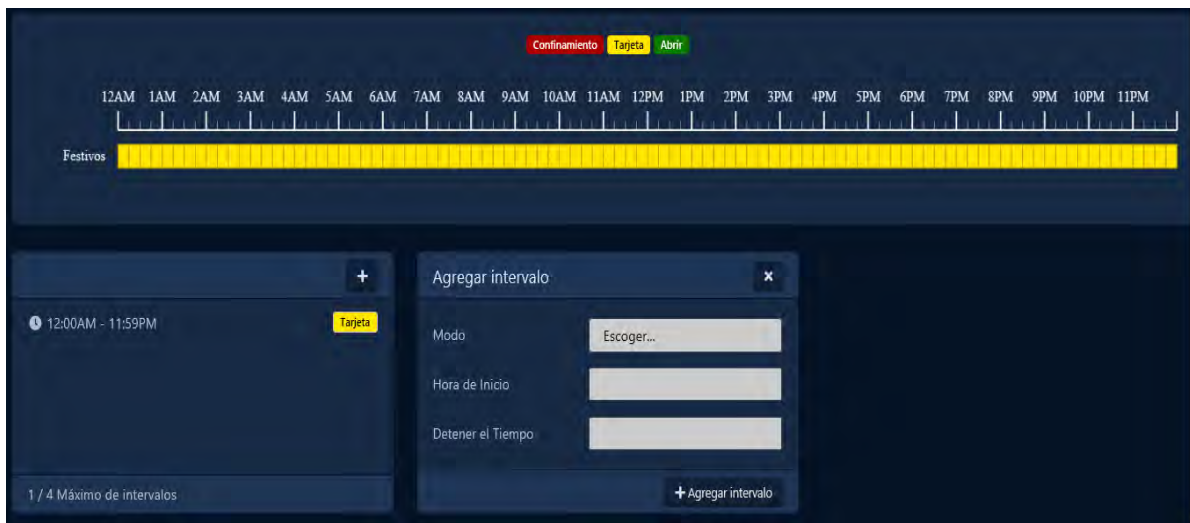
4. En la pantalla **Horarios de días festivos del usuario**, verá los Horarios de días festivos predeterminados del usuario, si necesita Horarios adicionales; haga clic en el botón **Agregar**.
5. En la pantalla **Agregar Horarios de días festivos del usuario**, verá que se ve casi exactamente como otros horarios que ha agregado en el sistema. Rellene los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.1. Agregar Horarios de días festivos del usuario

Casilla de verificación	Descripción
Nombre	Nombre único de su horario de usuario de festivos. Acepta de 2 a 60 caracteres. Recomendamos nombrar el Horario como su función para facilitar la lectura.
Descripción	Descripción opcional de su horario de vacaciones de usuario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este horario; si se selecciona más de uno, se crearán varias copias del Programa.

6. Ahora puede configurar la programación en función de lo que desea que tenga acceso un grupo de usuarios durante un feriado. Puede hacer clic en el estado de acceso deseado desde la parte superior y luego hacer clic y arrastrar la línea de tiempo deseada para el lapso seleccionado. Alternativamente, puede hacer clic en la barra roja al lado de **Día festivo en** la mitad de la página Programar. Esto abrirá el **widget del editor de horarios**.

Figure 13.2. Editor de Horarios



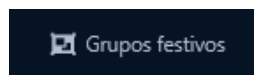
7. En el **Editor de horarios**, verá los intervalos de horarios ya existentes. Puede hacer clic en el botón + para agregar un nuevo lapso que abrirá el cuadro Agregar lapso. Puede usar el menú desplegable Modo para seleccionar un modo de acceso para todo el feriado si ya ha seleccionado un tramo existente. Si necesita más personalización, use la sección de agregar tramos para cambiar el programa de festivos del usuario hasta 4 veces en un día.
8. Una vez que haya completado la programación, haga clic en el botón Guardar. Ahora ha agregado un programa de vacaciones de usuario.

Grupos de días festivos de usuarios

Esta sección cubrirá la configuración de los grupos de festivos de usuario. Por defecto, VAX viene instalado con 2 grupos de vacaciones de usuario predeterminados:

Días festivos estándar: **grupo predeterminado y sin días festivos**. Aunque esto suele ser suficiente para la mayoría de las configuraciones de festivos, es bastante fácil agregar grupos de festivos de usuario adicionales.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**, haga clic en el icono **Grupos de días festivos** (en la imagen a continuación).



4. En la pantalla **Grupos de festivos del usuario**, verá los Grupos de festivos del usuario predeterminados. Si necesita grupos adicionales, haga clic en el botón **Agregar**.
5. En la página **Añadir grupos de días festivos de usuarios**. Rellene los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.2. Añadir grupos de días festivos de usuarios

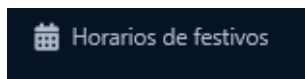
Casilla de verificación	Descripción
Nombre	Nombre único para su grupo de festivos de usuario. Acepta de 2 a 60 caracteres. Recomendamos nombrar el grupo según el tipo de vacaciones que contendrá o el grupo de usuarios para facilitar la lectura.
Descripción	Descripción opcional de su Grupo de festivos de Usuario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este grupo; si se selecciona más de uno, se crearán varias copias del grupo.

- Una vez que haya completado el llenado de los campos, haga clic en el botón **Guardar**. Ahora ha agregado un grupo de festivos de usuario, que ahora se podrá asignar en los **grupos de privilegios de acceso** y aparecerá al **agregar festivos**.

Horarios de días festivos de puertas

Esta sección cubrirá la configuración de los cronogramas de días festivos de la puerta. De forma predeterminada, VAX viene instalado con 1 horario de festivos de una puerta predeterminado: Significa que Cerrado durante los días festivos con un horario de cierre todo el día. Aunque esto a menudo es suficiente para la mayoría de las configuraciones de días festivos, es bastante fácil agregar horarios de días festivos de puerta adicionales o editar los horarios predeterminados.

- Acceda a su sistema VAX a través del navegador HTML5 de su elección.
- Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en icono de los **horarios de festivos** (en la foto de abajo).



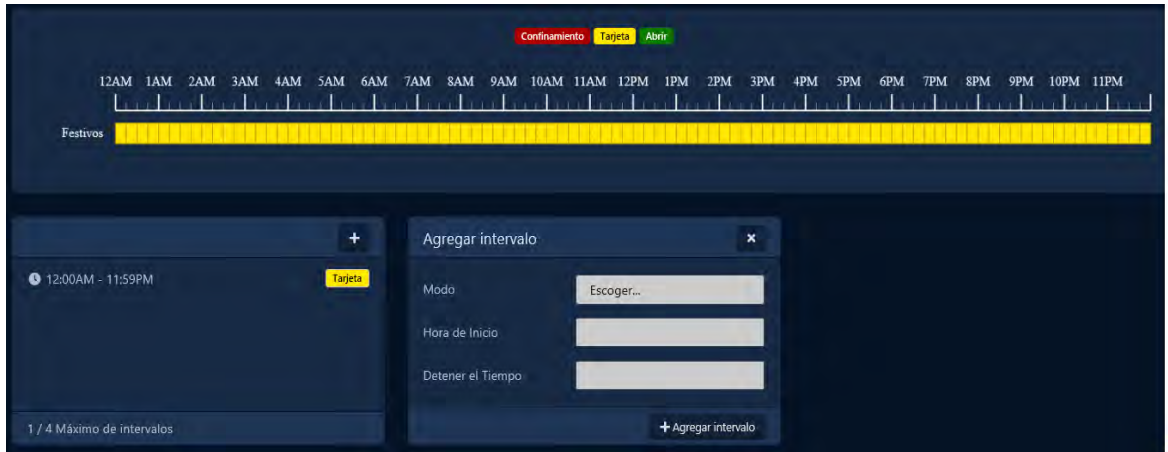
- En la pantalla **Horarios de días festivos de la puerta**, verá el Horario de días festivos predeterminado de la puerta; si necesita Programaciones adicionales, haga clic en el botón **Agregar**.
- En la pantalla **Agregar calendario de días festivos en la puerta**, verá que se ve casi exactamente como otros horarios que ha agregado en el sistema. Rellene los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.3. Agregar calendario de días festivos en la Puerta

Casilla de verificación	Descripción
Nombre	Nombre único de la programación de días festivos de la puerta. Acepta de 2 a 60 caracteres. Recomendamos nombrar el Horario como su función para facilitar la lectura.
Descripción	Descripción opcional de su horario de festivos de la puerta. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este horario; si se selecciona más de uno, se crearán varias copias del Programa.

- Ahora puede configurar el horario en función de lo que desea que haga una puerta durante un día festivo. Puede hacer clic en el estado de la puerta deseado desde la parte superior y luego hacer clic y arrastrar la línea de tiempo deseada para el lapso seleccionado. Alternativamente, puede hacer clic en la barra amarilla al lado de **Día festivo** en la mitad de la página **Programar**. Esto abrirá el editor de horarios a continuación

Figura 13.3. Editor de horarios

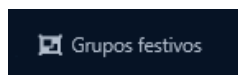


- En el **Editor de horarios**, verá los intervalos de horarios ya existentes. Puede hacer clic en el botón + para agregar un nuevo lapso que abrirá el cuadro Agregar lapso. Puede usar el menú desplegable Modo para seleccionar un modo de puerta para todo el día si ya ha seleccionado un tramo existente. Si necesita más personalización, use la sección Agregar intervalo para cambiar el estado de la puerta hasta 4 veces en un día.
- Una vez que haya completado la programación, haga clic en el botón Guardar. Ahora ha agregado un cronograma de vacaciones de la puerta.

Grupos de días festivos de las puertas

Esta sección cubrirá la configuración de los grupos de días festivos de puerta. De forma predeterminada, VAX viene instalado con 2 grupos de días festivos de puerta predeterminados: cerrado durante los días festivos y sin días festivos. Aunque esto a menudo es suficiente para la mayoría de las configuraciones de días festivos, es bastante fácil agregar grupos de días festivos de puerta adicionales.

- Acceda a su sistema VAX a través del navegador HTML5 de su elección.
- Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono de **grupos de festivos** (imagen abajo).



- En la pestaña **Puertas**, verá los Grupos de días festivos de puerta predeterminados; si necesita grupos adicionales, haga clic en el botón **Agregar**
- En la página **Agregar grupos de días festivos de puertas**, complete los cuadros de texto y marque las casillas con los valores apropiados.

Tabla 13.4. Añadir grupo de días festivos de puerta

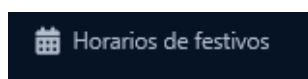
Casilla de verificación	Descripción
Nombre	Nombre único para su grupo de días festivos de la puerta. Acepta de 2 a 60 caracteres. Recomendamos nombrar el grupo según el tipo de festivos que contendrá o el grupo de usuarios para facilitar la lectura.
Descripción	Descripción opcional de su grupo de días festivos de la puerta. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este grupo; si se selecciona más de uno, se crearán varias copias del grupo

- Una vez que haya completado el llenado de los campos, haga clic en el botón **Guardar**. Ahora ha agregado un grupo de festivos de la puerta. que ahora será asignable en la **configuración de la puerta** y aparecerá al **agregar días festivo**.

Horarios de días festivos para pisos

Esta sección cubrirá la configuración de Horarios de días festivos para pisos. De forma predeterminada, VAX viene instalado con 1 horario de festivos para piso predeterminado: Cerrado durante los festivos con un horario de cierre todo el día. Aunque esto a menudo es suficiente para la mayoría de las configuraciones de días festivos, es bastante fácil agregar cronogramas de feriados de planta adicionales o editar los cronogramas predeterminados.

- Acceda a su sistema VAX a través del navegador HTML5 de su elección.
- Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono **Horarios de días festivos** (en la imagen a continuación).



- En la pantalla **Horarios de días festivos de piso**, verá el Horario de días festivos de piso predeterminado; si necesita Programaciones adicionales, haga clic en el botón **Agregar**.
- En la pantalla **Agregar horario de festivos de piso**, verá que se ve casi exactamente como otros horarios que ha agregado en el sistema. Rellene los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.5. Agregar horario de festivos de piso

Casilla de verificación	Descripción
Nombre	Nombre único de su horario de festivos de piso. Acepta de 2 a 60 caracteres. Recomendamos nombrar el Horario como su función para facilitar la lectura.
Descripción	Descripción opcional de su horario de festivos de piso. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este horario; si se selecciona más de uno, se crearán varias copias del Programa

- Ahora puede configurar el horario en función de lo que desea que haga un piso durante un feriado. Puede hacer clic en el estado del piso deseado desde la parte superior y luego hacer clic y arrastrar la línea de tiempo deseada para el lapso seleccionado. Alternativamente, puede hacer clic en la barra amarilla junto a Vacaciones en la mitad de la página **Programar**. Esto abrirá el **editor de horarios** a continuación.

Figura 13.4. Editor de horarios



7. En el **Editor de horarios**, verá los intervalos de horarios ya existentes. Puede hacer clic en el botón + para agregar un nuevo lapso que abrirá el cuadro Agregar lapso. Puede usar el menú desplegable Modo para seleccionar un modo de piso para todo el día si ya ha seleccionado un lapso existente. Si necesita más personalización, use la sección Agregar intervalo para cambiar el estado de la puerta hasta 4 veces en un día.
8. Una vez que haya completado la programación, haga clic en el botón **Guardar**. Ahora ha agregado un horario de feriado de piso.

Grupo de Festivos de Piso

Esta sección cubrirá la configuración de los grupos de festivos de piso. De forma predeterminada, VAX viene instalado con 1 Grupos de festivos de piso predeterminados: Grupo de festivos predeterminado. Aunque esto suele ser suficiente para la mayoría de las configuraciones de festivos, es bastante fácil agregar grupos de festivos de piso adicionales.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el ícono de **Grupos de festivos** (en la imagen a continuación).



4. En la **pestaña Pisos**, verá los Grupos de vacaciones de piso predeterminados; si necesita grupos adicionales, haga clic en el botón **Agregar**.
5. En la página **Agregar grupos de festivos de piso**, complete los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.6. Agregar grupo de días festivos de piso

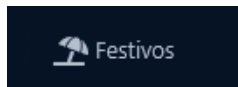
Casilla de verificación	Descripción
Nombre	Nombre único para su Grupo de festivos de piso. Acepta de 2 a 60 caracteres. Recomendamos nombrar el grupo según el tipo de feriados que contendrá o el grupo de usuarios para facilitar la lectura.
Descripción	Descripción opcional de su Grupo de festivos en Piso. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que desea crear este grupo; si se selecciona más de uno, se crearán varias copias del grupo

6. Una vez que haya completado el llenado de los campos, haga clic en el botón **Guardar**. Ahora ha agregado un grupo de festivos de piso, que ahora se podrá asignar en la **configuración de pisos** y aparecerá al **agregar feriados**.

Añadir un día festivo

This section will go over how to add additional Holidays to VAX. This section assumes you have planned out how this Holiday should affect your system. For more information on planning your Holidays, please see the section called "Holidays".

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **programación**; haga clic en el icono de **festivos** (en la imagen de abajo).



4. En la pantalla de **días festivos**, verá los días festivos (Navidad y Año Nuevo). Si necesita feriados adicionales, haga clic en el botón **Agregar**.
5. En la página **Agregar festivos**, complete los cuadros de texto y las casillas de verificación con los valores apropiados.

Tabla 13.7. Añadir un día festivo

Cuadro de texto / Casilla de verificación	Descripción
Nombre	Nombre único para su día de fiesta. Acepta de 2 a 60 caracteres.
Descripción	Descripción opcional de sus feriados. Acepta de 4 a 255 caracteres.
Fecha de inicio	La fecha inicial de la festividad, seleccionada en el widget de selección de fechas.
Ocurre anualmente	Cuando esta opción está habilitada, este feriado se observa todos los años en la misma fecha.
Usar días festivos preestablecidos	Cuando esta opción está habilitada, los días festivos canadienses, estadounidenses y judíos serán opciones seleccionables con una lista desplegable de los días festivos preestablecidos asociados. Al seleccionar el feriado de la lista desplegable, también se completarán los campos Nombre y Fecha inicial.
Grupos de Usuarios	Utilice la casilla de verificación para seleccionar los grupos de vacaciones de usuario con los que desea asociar las vacaciones. Una vez marcado, use el menú desplegable junto al grupo para seleccionar el Programa de vacaciones del usuario que se aplicará a ese grupo

Cuadro de texto / Casilla de verificación	Descripción
Grupos de puertas	Utilice la casilla de verificación para seleccionar con qué Grupos de festivos de puerta le gustaría asociar el festivo. Una vez marcado, utilice el menú desplegable junto al grupo para seleccionar el horario de festivos de la puerta que se aplicará a ese grupo.
Grupos de piso	Utilice la casilla de verificación para seleccionar con qué grupos de festivos de piso le gustaría asociar los feriados. Una vez marcado, utilice el menú desplegable junto al grupo para seleccionar el horario de feriado de piso que se aplicará a ese grupo.

- Una vez que haya completado el llenado de los campos, haga clic en el botón Guardar. Ahora ha añadido un feriado.

 **Nota :**

Recuerda realizar una Actualización a tus Paneles para que estén al tanto de los nuevos feriados.

Ejemplo de un feriado

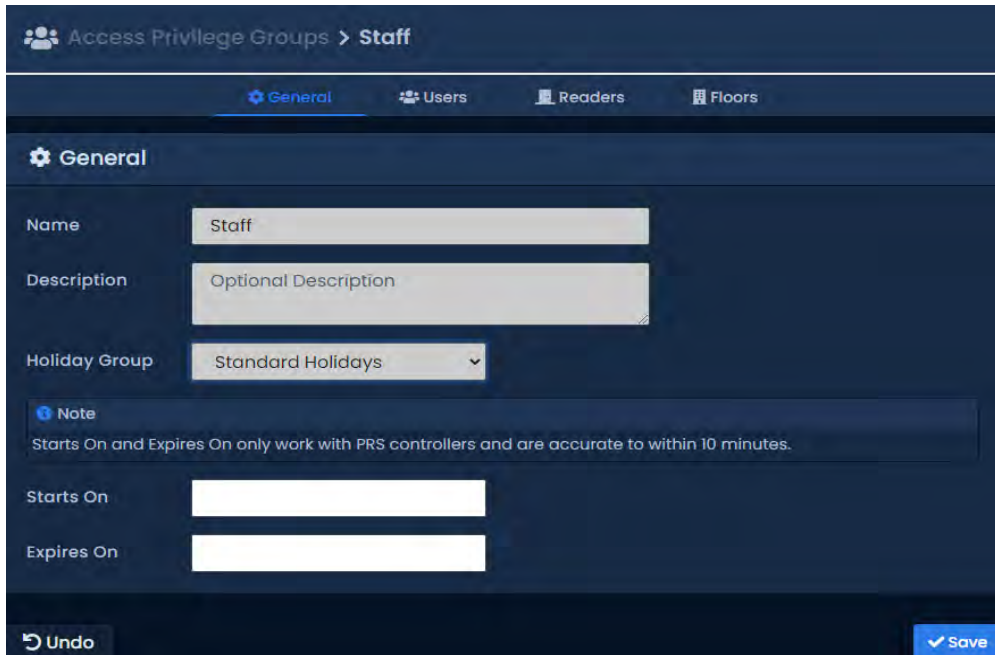
Esta sección contiene el ejemplo del Viernes santo que se agrega como feriado en VAX.

En este ejemplo, utilizaremos los **calendarios de días festivos** y los **grupos de días festivos** predeterminados. Simplemente agregamos el Día festivo y nos aseguramos de que las **Puertas** tengan aplicado el **Grupo de días festivos de puerta**, los Grupos de privilegios de acceso tengan el **Grupo de días festivos de usuario** aplicado y los Pisos tengan el **Grupo de días festivos de piso** aplicado

Figura 13.5. Agregar Viernes Santo

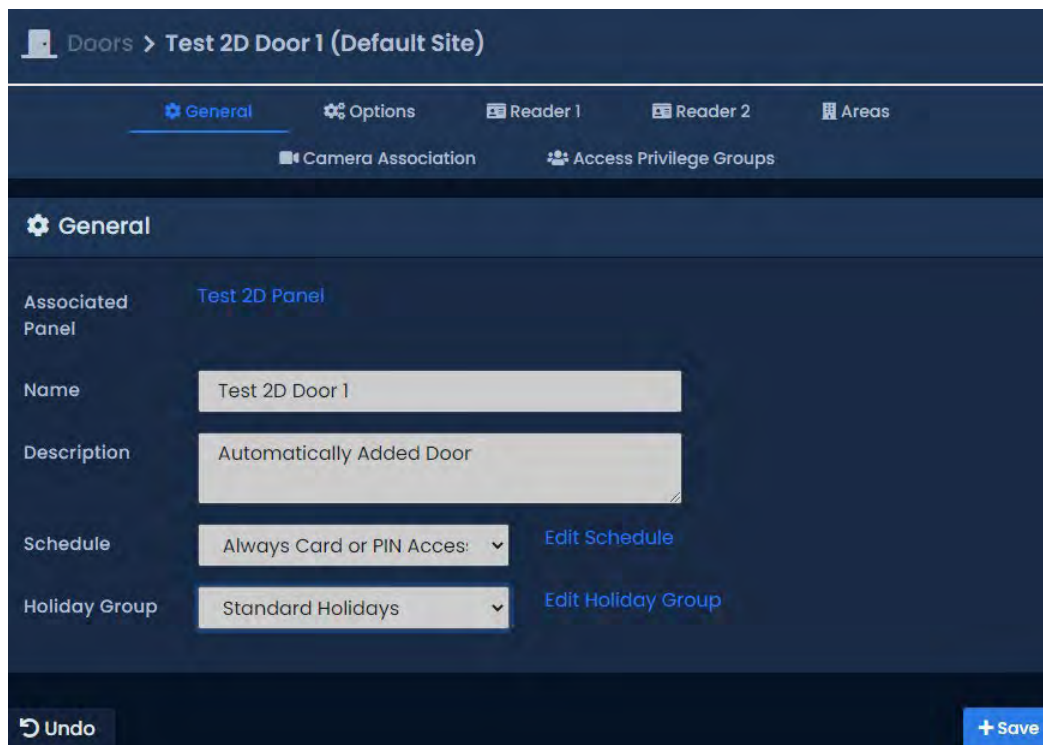
Después de agregar el feriado anterior, tendremos que asegurarnos de que los **grupos de privilegios de acceso**, las **puertas** y los **pisos** a los que debería afectar el feriado tengan los **grupos de feriados adecuados**.

Figura 13.6. Grupos de privilegios de acceso: grupo festivo

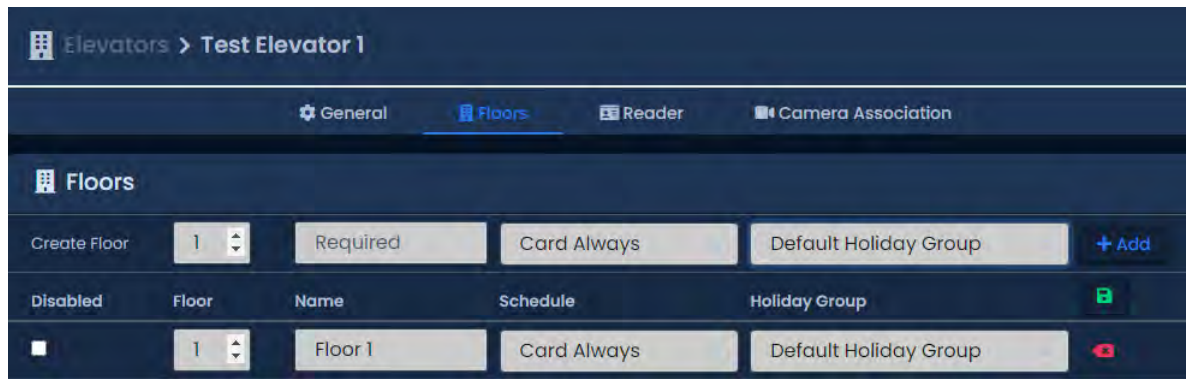


En la captura de pantalla anterior, verá que hemos cambiado el menú desplegable **Grupo de días festivos** al Grupo de días festivos del usuario de días festivos estándar, que es el grupo de usuarios al que hemos agregado el día festivo anteriormente.

Figura 13.7. Puerta: Grupo de festivos



En la captura de pantalla anterior, puede ver que hemos cambiado el menú desplegable **Grupo de días festivos** a **Grupo de días festivos de puerta de días festivos estándar**, que es el grupo de puertas al que hemos agregado el Día festivo anteriormente.

Figura 13.8. Piso: Grupo de festivos

En la captura de pantalla anterior, puede ver que hemos cambiado el menú desplegable **Grupo de días festivos** para cada piso al grupo de días festivos de piso predeterminado, que es el grupo de pisos al que hemos agregado el día festivo anteriormente. Tenga en cuenta que podemos tener pisos con diferentes grupos de feriados.

Capítulo 14. Zonas de ejecución única

Las zonas de ejecución única (OTR) se utilizan para crear eventos únicos en los que el estado de una puerta o piso cambia en un día específico durante un período de tiempo predeterminado.

Esta característica puede ser útil para eventos que requieren que la Puerta/Piso se desvíe de su horario normal.

Adición de zonas de ejecución única

Esta sección cubre los pasos para agregar un OTR en VAX.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**. Seleccione el icono de **ejecucion única**. (Imagen debajo)



4. En la parte superior de la pantalla **Ejecuciones únicas, Puertas y Pisos** serán las dos opciones disponibles para agregar una Ejecución única)



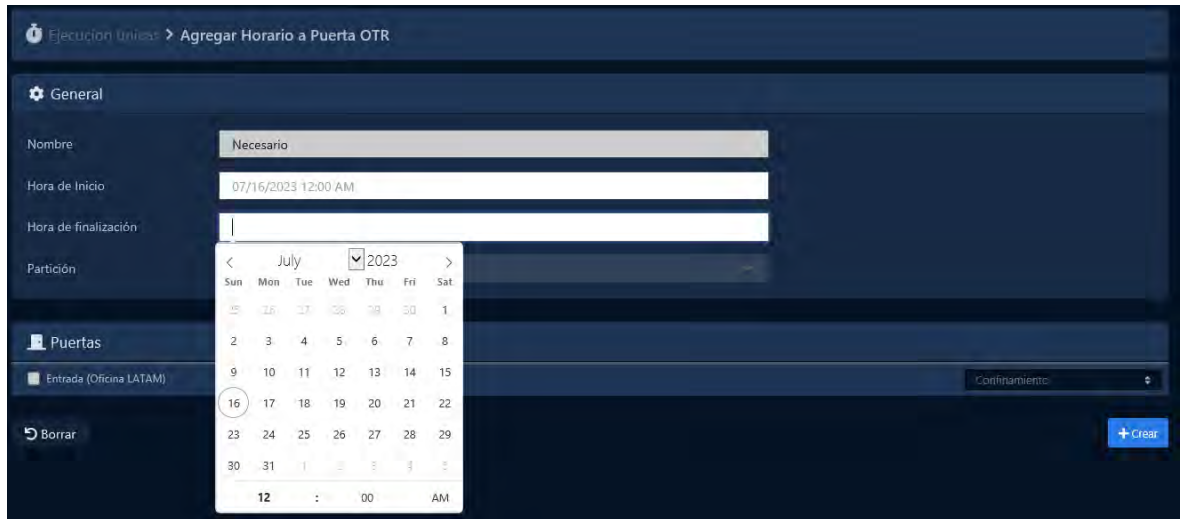
5. En la pantalla OTR, verá los OTR anteriores que se han creado, haga clic en el botón Agregar en esta pantalla.
6. . En la pantalla **Agregar OTR**, tendrá un par de cuadros de texto para completar.

Tabla 14.1. Agregar un programa de ejecución única

Cuadro de texto	Descripción
Nombre	Nombre único para su programa de ejecución única. Acepta de 2 a 60 caracteres. Recomendamos nombrar su OTR según la razón por la que se creó, como mantenimiento de emergencia, vacaciones prolongadas, fiesta de cumpleaños.
Hora de inicio/fin	La fecha y hora en que comienza el Horario. Al hacer clic, aparecerá el widget del selector de fecha. Utilice el selector de calendario y hora para seleccionar la fecha y la hora de inicio/fin de la OTR.
Partición	Utilice el menú desplegable Partición para cambiar qué puertas se pueden seleccionar para este OTR.
Pisos / Puertas Afectadas	Seleccione las puertas/pisos a los que desea que afecte esta OTR y use el menú desplegable en el lado derecho para seleccionar cuál de los 8 estados de puerta o 3 estados de piso se aplicará durante esta OTR.

7. Una vez que haya seleccionado el nombre, la hora de inicio, la hora de finalización, la partición, las puertas/pisos y el estado de la puerta/piso, ahora puede hacer clic en **Crear** para crear el OTR. Si se selecciona más de una partición, se creará un OTR para cada una.

Figura 14.1. Widget de selector de fecha



Consejo

Puede configurar un OTR para abarcar varios días. Esto puede ser útil para feriados que duran más de un día.

Capítulo 15. Niveles de crisis

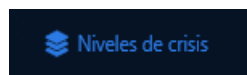
Este capítulo cubrirá cómo funcionan los niveles de crisis en VAX, junto con cómo personalizarlos y usarlos de manera efectiva.

Los niveles de crisis brindan a los administradores la capacidad de cambiar el comportamiento de las puertas rápidamente durante situaciones de emergencia con una variedad de niveles de gravedad configurables. Se pueden configurar hasta 16 niveles de crisis; por defecto solo 4 están activos.

Cambios en los niveles de crisis

Esta sección cubrirá cómo hacer ajustes a los nombres y el comportamiento de los niveles de crisis. Para ver y realizar cambios en el comportamiento de cada nivel de crisis, siga los siguientes pasos:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada Administración; haga clic en el ícono de Niveles de crisis (en la imagen a continuación)



4. En la pantalla Niveles de crisis, verá los 16 niveles disponibles.

Figura 15.1. Pantalla de niveles de crisis

Deshabilitado	Nombre	Nivel	Estado de la Puerta
	Default: Follow Schedule	1	
No	Code Yellow	2	Solo tarjeta
No	Level 3	3	Solo tarjeta
No	Level 4	4	Solo tarjeta
No	Level 5	5	Solo tarjeta
No	Level 6	6	Solo tarjeta
No	Level 7	7	Solo tarjeta
No	Code Orange	8	Solo tarjeta
No	Level 9	9	Solo tarjeta
No	Level 10	10	Solo tarjeta
No	Level 11	11	Solo tarjeta
No	Level 12	12	Solo tarjeta
No	Level 13	13	Solo tarjeta
No	Level 14	14	Solo tarjeta
No	Level 15	15	Solo tarjeta
No	Code Red	16	Solo tarjeta

1 = seguridad más baja 16 = máxima seguridad

5. Todos los elementos subrayados con puntos se pueden editar haciendo clic en ellos. Puede personalizar el nombre de cada nivel de crisis, si el nivel está deshabilitado y con qué estado de puerta está asociado un nivel de crisis. Una vez que realice un cambio, se guardará automáticamente.

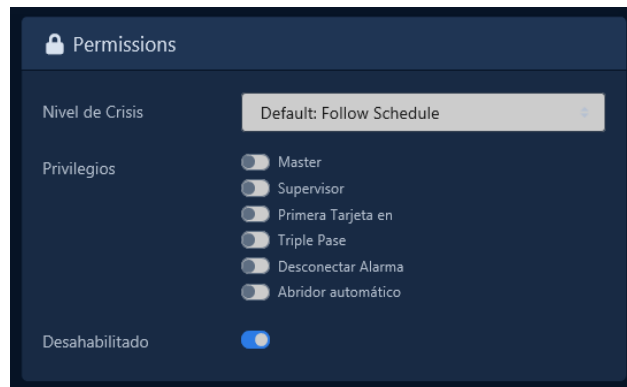
Configuración de los niveles de seguridad del usuario

Cuando se aplica un Nivel de Crisis a una Puerta con un Estado de Puerta aplicado de Solo Tarjeta, **NO** se otorgará acceso a los Usuarios al presentar su Credencial a menos que el **Nivel de Seguridad del Usuario** sea igual o mayor que el Nivel de Crisis que se está aplicando, con la excepción de que el usuario tiene el privilegio **Maestro** activado.

Los niveles de seguridad del usuario se pueden cambiar en la pantalla Editar usuario.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Usuarios**; haga clic en el icono **Usuarios**.
2. En la pantalla Usuarios, haga clic en el botón azul (editar) junto al usuario que desea cambiar.
3. . En la pestaña **General del Usuario**, el menú desplegable Nivel de crisis representa el nivel de seguridad de ese Usuario. De manera predeterminada, un Nivel de crisis de usuario se establece en el nivel 1, Predeterminado: Seguir programación.
4. Si ha cambiado el Nivel de crisis del usuario, haga clic en **Guardar**. Los paneles deberán actualizarse antes de que el cambio surta efecto.

Figura 15.2. Cambio de un nivel de crisis de usuario



Aplicación de niveles de crisis a las puertas

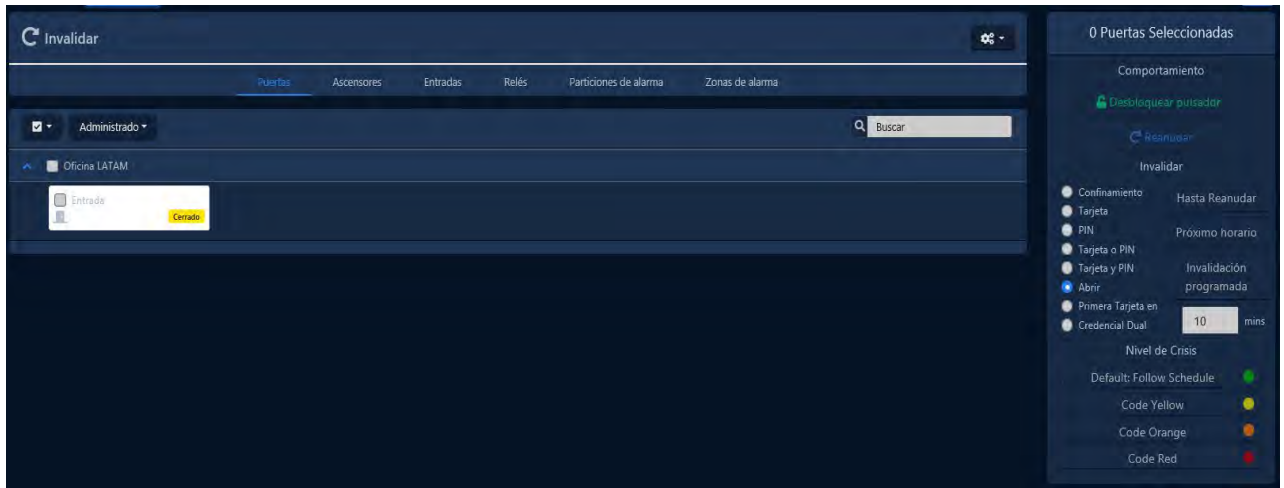
Esta sección cubrirá los dos métodos que se pueden usar para aplicar niveles de crisis a las puertas. El primer método es a través del software VAX; el segundo método es mediante el uso de entradas AUX en los paneles.

Aplicación de niveles de crisis en VAX

La aplicación de un nivel de crisis en VAX se puede hacer desde cualquier página en la interfaz de VAX. El menú Niveles de crisis se encuentra en la esquina superior derecha (en la imagen a continuación).



Haga clic en el icono Niveles de crisis para abrir el menú Niveles de crisis. Aquí verá todos los sitios en el sistema y las puertas adjuntas a cada sitio.

Figura 15.3. Menú de niveles de crisis

Al hacer clic en la casilla de verificación junto a un sitio, se seleccionarán todas las puertas en ese sitio. Alternativamente, puede seleccionar Puertas individuales. Una vez que haya seleccionado las Puertas, haga clic en el Nivel de crisis en el lado derecho que mejor se adapte a cómo desea que se comporte la Puerta (en función de cómo haya configurado sus Niveles de crisis), teniendo en cuenta que esto puede bloquear el acceso a los Usuarios si su nivel de seguridad es demasiado bajo.

Para reanudar la puerta desde el modo de crisis, seleccione las puertas y haga clic en el **valor predeterminado de nivel de crisis: Seguir programa**.

Aplicación de niveles de crisis con una entrada auxiliar

El segundo método para aplicar un nivel de crisis a una puerta es a través de una entrada auxiliar. Para obtener más información sobre la configuración de Entrada/Salida, consulte la sección denominada "Configuración de Entrada/Salida".

Una vez que se configura una entrada auxiliar para iniciar un nivel de crisis, esa entrada puede activarse mediante un botón o un contacto seco de algún otro sistema, como una alarma contra incendios. Cuando se activa la entrada, solo el panel con la entrada auxiliar configurada se colocará en el modo de crisis. Iniciar un nivel de crisis a través de una entrada auxiliar no cambia el estado de la puerta, solo el nivel de crisis.

Advertencia

Una vez que una entrada auxiliar activa un modo de crisis, la forma de reanudar el horario normal es a través de la interfaz del software VAX, o al tener una entrada adicional con un activador de entrada auxiliar que coloca la puerta en el modo predeterminado: Seguir horario.

Capítulo 16. Funciones de invalidación / anulación de VAX

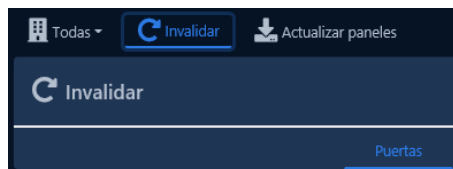
Este capítulo cubrirá las diversas funciones de anulación en VAX, incluida la forma de invalidar una puerta, una salida o un piso de ascensor a través del software en tiempo real.

! Advertencia

Las invalidaciones son el nivel más alto de estado al que obedecerá una puerta, una salida o un piso. Las invalidaciones reemplazan los días festivos, los OTR, los niveles de crisis y los horarios de puerta (con la excepción de la anulación hasta el próximo horario).

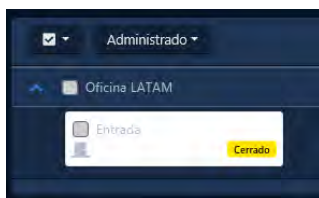
Invalidar Puertas

Esta sección cubre cómo invalidar una puerta en VAX usando el menú **Invalidar puertas**. Se puede invalidar una puerta desde cualquier página del software haciendo clic en el botón **Invalidar** y luego en el botón **Puertas** en la parte superior de la página (en la imagen a continuación).



Haga clic en el icono Invalidar puertas para abrir el menú Invalidar puertas. Aquí verá todos los sitios del sistema y las puertas adjuntas a cada sitio. Solo se mostrarán las Puertas que están en línea y conectadas a VAX; Las puertas que están fuera de línea aparecerán atenuadas.

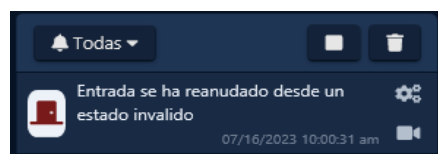
Figura 16.1. Menú de Invalidación de puertas



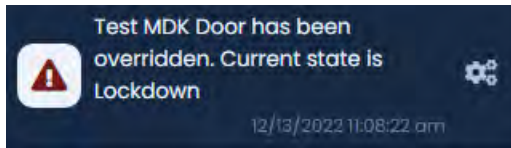
Al hacer clic en la casilla de verificación junto a un sitio, se seleccionarán todas las puertas en ese sitio. Alternativamente, puede seleccionar Puertas individuales. Una vez que haya seleccionado las Puertas, los botones en el lado derecho se pueden usar para manipular el estado de la Puerta instantáneamente.

El menú Invalidar puertas se divide en 3 secciones, **Acciones, Invalidar y Nivel de crisis**.

General. La invalidación más común es la acción de **desbloqueo por pulso**, que desbloqueará una puerta y luego volverá a su horario normal un momento después. La acción **Reanudar** se puede utilizar en cualquier tipo de invalidación de puerta para devolver la puerta a su horario normal. Cuando se reanuda una puerta, verá la notificación: La puerta se ha reanudado desde un estado invalido.



Invalidar hasta reanudar. Las 4 invalidaciones momentáneas se pueden usar para cambiar el estado de la puerta (bloqueo, desbloqueo, tarjeta, PIN). Una vez que se invalida la puerta, permanecerá en ese estado hasta que la puerta se reanude con el botón **Reanudar**. En Descripción general del sistema, puede ver el estado de la puerta y si la puerta está invalida.



Invaldar hasta el próximo horario. El comportamiento de estas invalidaciones difiere ligeramente de Invaldar hasta reanudar. Estas invalidaciones cambiarán el estado de la puerta, y la puerta permanecerá invalida hasta que la puerta esté programada para cambiar de estado; momento en el que la puerta reanudará su horario normal. Reanudar la puerta con el botón de reanudar también cambiará el estado de la puerta a su horario normal.

Ejemplo: una empresa tiene una puerta pública que está abierta de 9 a 5 y la tarjeta solo fuera del horario de atención. Es un día lento y el gerente decide cerrar temprano. Navega hasta VAX usando su teléfono inteligente e inicia una invalidación hasta el próximo horario, con un estado de puerta de solo tarjeta. La puerta permanecerá en este estado hasta las 5 p. m. de esa noche, cuando reanudará su horario normal

Nota : Las invalidaciones de puerta también se pueden realizar configurando acciones de deslizamiento triple. Esto puede ser útil para una variedad de situaciones, como cerrar temprano. Para obtener más información sobre las opciones de triple deslizamiento, consulte el *Capítulo 17, Funciones de triple deslizamiento*.

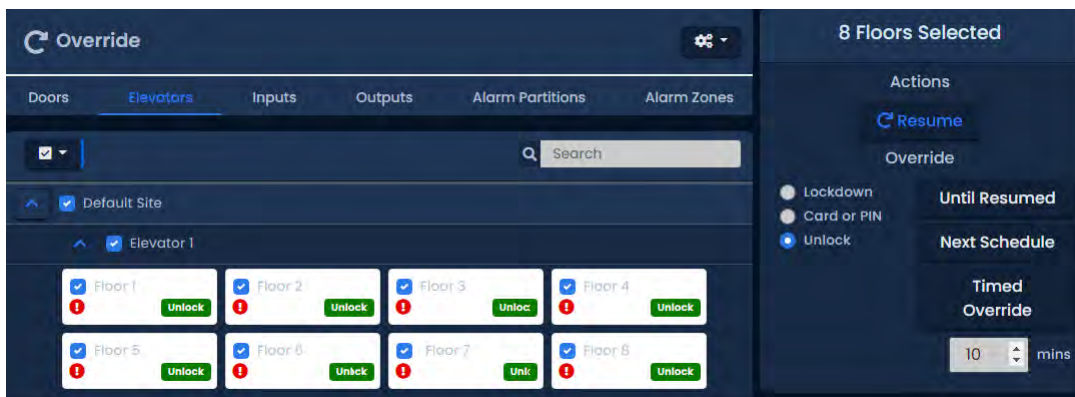
Invaldar pisos

Esta sección cubre cómo **invalidar los pisos** de un elevador en VAX usando el menú **Invaldar elevador**. Se puede anular un piso desde cualquier página del software haciendo clic en el **botón Invaldar pisos** en la parte superior derecha de la página (en la imagen a continuación)



Haga clic en el icono Invalidar para abrir el menú **Invaldar**. Haga clic en el ícono de **Elevadores** para abrir el menú de invalidación de piso. Aquí verá todos los Sitios en el sistema y los Elevadores y Pisos adjuntos a cada Sitio. Haga clic en el icono desplegable de un ascensor para mostrar los pisos. Solo se mostrarán los Pisos que están en línea y conectados a VAX; Los pisos que están fuera de línea aparecerán atenuados.

Figura 16.2. Menú de invalidación de piso

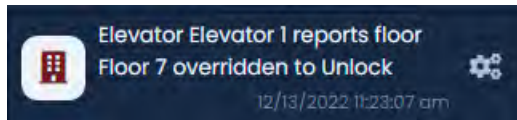


Al hacer clic en la casilla de verificación junto a un sitio, se seleccionarán todos los pisos en ese sitio. Al hacer clic en un Elevador, se seleccionarán todos los Pisos adjuntos a ese Elevador. Alternativamente, puede seleccionar Pisos individuales. Una vez que haya seleccionado los Pisos, los botones en el lado derecho se pueden usar para manipular el estado del Piso instantáneamente.

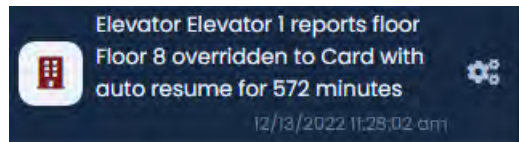
El menú Invalidar pisos se divide en 3 secciones: **General**, **Invalidar hasta reanudar** e **Invalidar hasta el próximo horario**.

General. La acción **Reanudar** se puede usar en cualquier tipo de invalidación de piso para devolver el **Piso** a su horario normal. Cuando se reanude un piso, verá la notificación: **invalidación de piso deshabilitada**.

Invalidar hasta reanudar. Estas invalidaciones se pueden usar para cambiar el estado del piso (bloqueo, desbloqueo, tarjeta). Una vez que se invalida el piso, permanecerá en ese estado hasta que se reanude el piso con el botón Reanudar. En Descripción general del sistema, puede ver el estado del piso y si el piso está anulado.



Invalidar hasta el próximo horario. El comportamiento de estas invalidaciones difiere ligeramente de Invalidar hasta reanudar. Estas invalidaciones cambiarán el estado del Piso, y el Piso permanecerá invalido hasta que el Piso esté programado para cambiar de estado, momento en el cual el Piso reanudará su horario normal. Reanudar el piso con el botón Reanudar también cambiará el estado del piso a su horario normal.



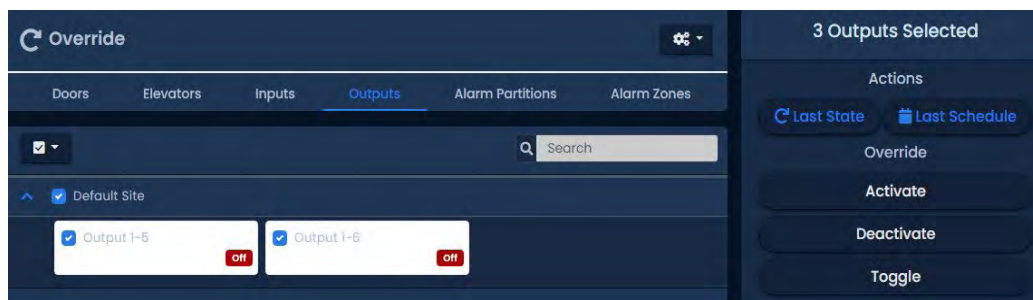
Invalidar Salidas

Esta sección cubre cómo invalidar las salidas en VAX. El proceso es muy similar a Invalidar Puertas. Se puede invalidar una salida desde cualquier página del software haciendo clic en el botón **Invalidar salidas** en la parte superior derecha de la página (en la imagen a continuación).



Haga clic en el icono Invalidar salidas para abrir el menú invalidar salidas. Aquí verá todos los sitios en el sistema y las salidas disponibles adjuntas a cada sitio; Las salidas conectadas a los paneles que están fuera de línea aparecerán atenuadas.

Figura 16.3. Menú de invalidación de salidas



Al hacer clic en la casilla de verificación junto a un sitio, se seleccionarán todas las puertas en ese sitio. Alternativamente, puede seleccionar salidas individuales. Una vez que haya seleccionado la Salida, los botones en el lado derecho se pueden usar para manipular el estado de la Salida instantáneamente.

Activar. Cambia la salida a un estado activo, también conocido como estado cerrado.



Deactivar. Cambia la salida a un estado inactivo, también conocido como estado abierto.



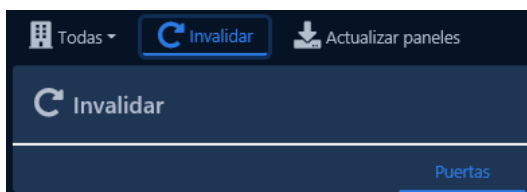
Resumir. Reanuda la salida a su estado natural (definido en la configuración de E/S del panel como normalmente cerrado o normalmente abierto)

Nota

Las invalidaciones de salida también se pueden realizar configurando acciones de triple deslizamiento. Esto puede ser útil para una variedad de situaciones, como cerrar temprano. Para obtener más información sobre las opciones de triple deslizamiento, consulte el *Capítulo 17, Funciones de triple deslizamiento*

Invalidar Entradas

This section covers how to Override Inputs in VAX. The process is very similar to Overriding Outputs. Overriding an input can be done from any page in the software by clicking on the Override button on the top of the page (pictured below).



Haga clic en el icono **invalidar** para abrir el menú **Invalidar entradas**. Aquí verá todos los sitios en el sistema y las entradas disponibles adjuntas a cada sitio; Las entradas conectadas a los paneles que están fuera de línea aparecerán atenuadas.

Figura 16.4. Menú de invalidación de entradas



Al hacer clic en la casilla de verificación junto a un sitio, se seleccionarán todas las puertas en ese sitio. Alternativamente, puede seleccionar Entradas individuales. Una vez que haya seleccionado la **Entrada**, los botones del lado derecho se pueden usar para manipular el estado de la Entrada instantáneamente.

Resumir. Reanuda la entrada a su estado natural. Reanuda su horario habitual.

Nota:

Las invalidaciones de entrada también se pueden realizar configurando acciones de deslizamiento triple. Esto puede ser útil para una variedad de situaciones, como activar un plan de acción ACE. Para obtener más información sobre las opciones de triple deslizamiento, consulte el *Capítulo 17, Funciones de triple deslizamiento*

Figura 16.5. Menú de invalidación de entradas

12/14/2022 07:49:16 am Test Master Test Master requested Input Input 1-4 resume from overridden state.

Denegado. Rechazar solicitudes de anulación para la entrada e ignora todos los intentos de cambiar la entrada mientras está en Rechazar invalidación. Si se reanudara, la entrada volvería a su estado natural.

Figura 16.6. Menú de invalidación de entradas

12/14/2022 07:48:58 am Test Master Test Master requested Input Input 1-4 override to ignore status changes.

Permitir. Permitir invalida las solicitudes de entrada para monitorear y permitir los intentos de cambiar las entradas mientras se encuentran en Permitir invalidación. La entrada reanudaría su programación natural si se reanuda desde este estado.

Figura 16.7. Menú de invalidación de entradas

12/14/2022 07:48:59 am Test Master Test Master requested Input Input 1-4 override to monitor status changes.

Invalidar particiones de alarmas

Las secciones de Invalidación de alarma en el menú Invalidar permiten invalidar alarmas de sitios y sus respectivas alarmas. Para obtener más información sobre estas secciones, consulte el *Capítulo 38, Integración de alarma IP DSC*.

Capítulo 17. Funciones de triple deslizamiento (pase)

Triple Deslizamiento es una función en VAX que permite **presentar una Credencial a un Lector 3 veces** en concesión para realizar acciones predefinidas. Estas acciones incluyen invalidar el estado de la puerta, activar salidas en el panel y activar interfaces de alarma. Este capítulo cubrirá las opciones disponibles y ejemplos comunes de cómo se utilizan en el campo. Las salidas que se activan mediante acciones de triple deslizamiento también se pueden conectar a una entrada auxiliar en el panel para acciones adicionales.

Requisitos del usuario para usar el triple pase

Para que un usuario pueda realizar una acción de Triple deslizamiento, se debe seleccionar el atributo de usuario Triple deslizamiento al agregar o editar el usuario. Se requiere el atributo de usuario *Supervisor cuando se utiliza Triple deslizamiento con Horarios de Puerta de alta seguridad Doble Credencial y Tarjeta y PIN*. Las credenciales de PIN pueden activar acciones de triple deslizamiento presionando '#' en el teclado 3 veces después de ingresar el PIN. Para obtener más información sobre los atributos de usuario, consulte la sección llamada "Privilegios de usuario".

Lista de opciones de triple deslizamiento o pase

Esta lista contiene las acciones de deslizamiento triple actualmente configurables. Los modelos de panel con alimentación de 12 VDC tienen un conjunto diferente de opciones de deslizamiento triple; se muestran en la siguiente sección. Solo los usuarios/tarjetas con el atributo de usuario de triple deslizamiento podrán realizar un triple pase. Para obtener más información sobre los atributos de usuario, consulte el *Capítulo 12, Configuración de usuario/titular de tarjeta*.

Tabla 17.1. Funciones de triple deslizamiento

Acciones de triple deslizamiento	Breve explicacion
Activar salida auxiliar	Activa la salida seleccionada.
Desactivar salida auxiliar	Desactiva la Salida seleccionada.
Alternar salida auxiliar	Alterna la Salida seleccionada (si la Salida está activada, esta acción desactivará la Salida).
Salida auxiliar de pulso	Activa la salida seleccionada durante aproximadamente un segundo ante de desactivarla nuevamente.
Activar interfaz de alarma	Activa la salida que tiene una función asignada de interfaz de alarma durante aproximadamente un segundo ante de desactivarla nuevamente.
Desactivar interfaz de alarma	Desactiva la Salida que tiene asignada una función de Interfaz de Alarma (si la interfaz está actualmente activa).
Alternar interfaz de alarma	Activa la salida que tiene una función asignada de interfaz de alarma durante aproximadamente un segundo ante de desactivarla nuevamente.
Desactivar la alarma de emergencia	Si un panel tiene una entrada configurada como alarma de emergencia, si la alarma está activada, esta acción de triple deslizamiento restablecerá el panel a su estado normal.
Invaldar <Modo de puerta>	Esta acción de deslizamiento triple anulará el estado de la puerta según la selección que configure en el software. Estas anulaciones de puertas se deben reanudar desde el software o con la acción de triple deslizamiento "Cancelar invalidación". Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta.

Acciones de triple deslizamiento	Breve explicacion
Invalidar <Modo de puerta> con reanudación automática	Esta acción de triple deslizamiento anulará el estado de la puerta dependiendo de la selección que configure en el software. Estas Anulaciones de puerta le indican a la puerta que reanude el horario normal cuando el horario de puerta asignado a esta puerta está programado para cambiar. También se puede reanudar desde el software o con la acción de triple deslizamiento "Cancelar anulación". Los modos incluyen: Bloqueo, Tarjeta, PIN, Tarjeta o PIN, Tarjeta y PIN, Desbloqueo, primera entrada de tarjeta
Invalidar alternar <Modo de puerta>	Esta acción de deslizamiento triple anulará el estado de la puerta según la selección que configure en el software. Estas anulaciones de puertas deben reanudarse desde el software, con la acción de triple deslizamiento "Cancelar anulación" o realizando un segundo triple deslizamiento que "alternará" el estado de regreso a la normalidad. Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta.
Cancelar invalidación	Reanuda cualquier puerta desde un estado invalido.
Cancelar invalidación de salida	Reanuda cualquier salida desde un estado invalido.

 **Nota:**

Si está utilizando un teclado, puede configurar hasta 7 acciones de deslizamiento triple basadas en una pulsación de tecla después de un triple pase. Debe presionar # 3 veces después de haber presentado sus credenciales seguido del número correspondiente a la acción que desea ejecutar. Debe presionar # una última vez para ejecutar la acción.

Tabla 17.2. Características de deslizamiento triple del panel VAX-MDK

Acciones de triple deslizamiento	Breve explicacion
Sin acción	Las acciones son opcionales; aún se generará un evento cuando se cumplan las condiciones de entrada y los activadores de secuencias de comandos del lado del servidor aún se puedan ejecutar.
Activar salida	Activa una salida, seleccionable a través de la lista desplegable.
Desactivar salida	Desactiva una salida, seleccionable a través de la lista desplegable.
Alternar salida	Cambia una salida al estado opuesto, seleccionable a través de la lista desplegable.
Desactivar salida	Desactivar la salida seleccionada, seleccionable a través de la lista desplegable.
Salida de pulso alta	Pulse una salida para cerrar, configure un lapso y duración del pulso.
Salida Pulso Baja	Pulse una salida para abrir, configure un lapso y duración del pulso.
Pulso de salida opuesta	Pulse una salida al contrario de su estado actual, configure un retraso y la duración del pulso.
Activar salida múltiple	Active múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Desactivar Salida Múltiple	Desactive múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Alternar salida múltiple	Alterne múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.

Funciones de triple deslizamiento

Acciones de triple deslizamiento	Breve explicación
Entrada deshabilitada	Deshabilitar una entrada seleccionada. Seleccionable de una lista desplegable con retraso y duración.
Anular <Modo de puerta>	Esta acción de triple deslizamiento invalidará el estado de la puerta dependiendo de la selección que configure en el software. Estas invalidaciones de puerta deben reanudarse desde el software o con la acción de triple deslizamiento "Cancelar invalidación". Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta. Puerta y modo seleccionable de la lista desplegable
Anular <Modo de puerta> con reanudación automática	Esta acción de triple deslizamiento invalidará el estado de la puerta dependiendo de la selección que configure en el software. Estas invalidaciones de puerta deben reanudarse desde el software o con la acción de triple deslizamiento "Cancelar invalidación". Los modos incluyen: bloqueo, tarjeta, pin, tarjeta o pin, tarjeta y pin, desbloqueo, primera entrada de tarjeta. Puerta y modo seleccionable de la lista desplegable
Alternar anulación <Modo de puerta>	This Triple Swipe Action will toggle override the state of the Door depending on the selection you configure in the software. This option allows a triple swipe to toggle the door into and out of an overridden state. Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Credential In, Dual Credential. Door and mode selectable from drop-down list
Anulación de reanudación de puerta	Reanuda una puerta desde un estado invalido. Seleccionable a través de la lista desplegable.
Nivel de crisis del conjunto de puerta	Inicia el nivel de crisis en una puerta. Seleccionable a través de la lista desplegable para puerta y modo.
Nivel de crisis de restablecimiento de puerta	Vuelva a establecer el nivel de crisis por defecto en la puerta seleccionada. Seleccionable a través de la lista desplegable.
Desactivación de puerta con zumbador abierto	Desactive temporalmente una alarma/zumbador abierto mantenido en la puerta seleccionada. Seleccionable a través de una lista desplegable para puerta y duración (1-600 segundos).
Desconexión de alarma de emergencia	Desactiva la función de alarma de emergencia, que reanudará cualquier anulación provocada por la función de alarma de emergencia.
Alarma de emergencia (silenciosa) - Desbloqueo de puertas	Activa la función de alarma de emergencia. Los lectores no sonarán (silenciosos). No excluirá puertas con la opción "Desbloquear en alarma de emergencia" desactivada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia (silenciosa): desbloqueo de puertas desprotegidas	Activa la función de alarma de emergencia. El panel no emitirá un pitido (silencioso). Excluirá las puertas con la opción "Desbloquear en alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia - Sonido	Activa la función de alarma de emergencia. El panel emitirá un pitido hasta que se active la función de desactivación de la alarma de emergencia. No afectará el estado de la puerta.
Alarma de emergencia: desbloquear puertas	Activa la función de alarma de emergencia. El panel emitirá un pitido hasta que se active la función de desconexión de alarma de emergencia. No excluirá las puertas con la opción "Desbloquear en caso de alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.
Alarma de emergencia - Desbloqueo de puertas no protegidas	Activa la función de alarma de emergencia. El panel no emitirá un pitido (silencioso). Excluirá las puertas con la opción "Desbloquear en alarma de emergencia" deshabilitada. Puertas afectadas seleccionables vía lista.

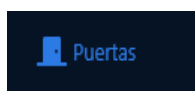
Acciones de triple deslizamiento	Breve explicacion
Zumbador	Proporciona varias opciones para desactivar los zumbadores del lector o las salidas configuradas como zumbadores externos. El zumbador se reactivará si otro evento activa el zumbador, como una puerta que se abre a la fuerza.
Activar interfaz de alarma	Se utiliza para activar una salida que se asigna como interfaz de alarma. En la mayoría de los casos, esto se puede usar para armar un sistema de alarma.
Interfaz de alarma Desactivar	Se utiliza para desactivar una salida asignada como interfaz de alarma. En la mayoría de los casos, esto se puede usar para desarmar un sistema de alarma.

Configuración de triple deslizamiento - pase

Como se explicó anteriormente en esta guía, las acciones de deslizamiento triple se configuran en la pestaña **Lector** de la pantalla **Editar puerta**.

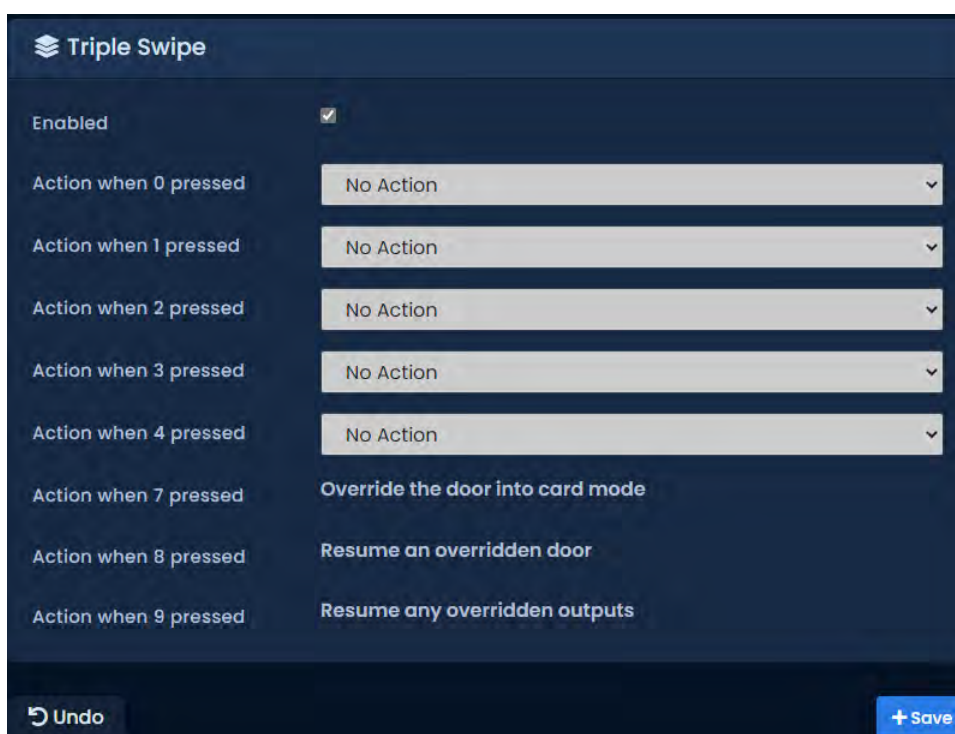
Para llegar a esta pantalla:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada Hardware; haga clic en el icono de Puertas (en la imagen de abajo).



2. En la pantalla **Puertas**, se enumerarán las Puertas configuradas. Haga clic en el botón azul junto a la puerta que desea configurar.
3. En la pantalla **Editar puerta**, verá 4 pestañas. Haga clic en la pestaña **Lector**, desplácese hacia abajo hasta la parte inferior de la pestaña Lector y verá las opciones **para Acciones de triple deslizamiento**.

Figura 17.1. Pestaña Lector: Deslizamiento triple con opciones de teclado



Ejemplos de triple deslizamiento / pase

Esta sección contiene ejemplos del mundo real de cómo nuestros distribuidores/usuarios finales pueden utilizar Triple deslizamiento / pase.

Armar/Desarmar Sistema de Alarma. Muchos usuarios de nuestro producto utilizan nuestro sistema para armar/desarmar sus sistemas de alarma. Es tan fácil como pasar tres veces la tarjeta al salir de la oficina para armar el sistema y hacer lo mismo al día siguiente para desarmarlo. Para obtener más información sobre la interfaz con los sistemas de alarma, consulte la sección correspondiente de la guía técnica principal.

Cierre una puerta pública temprano. Algunas instalaciones tienen Puertas Públicas, Puertas que se desbloquean durante un período del día (9 am a 5 pm). Si la Puerta debe cerrarse antes de tiempo, puede Anularla a Solo tarjeta hasta el próximo horario. La puerta ahora será solo tarjeta hasta el día siguiente, cuando reanudará su horario normal de desbloqueo.

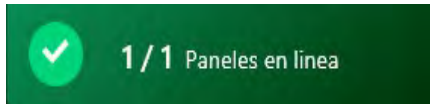
También podemos lograr lo anterior a través de la acción de Triple pase. A continuación se encuentran las instrucciones para cerrar la puerta temprano, pero también para indicarle a la puerta que reanude el horario normal al día siguiente cuando esté programada para abrirse.

1. Vaya a "Inicio/Hardware/Paneles de puertas".
2. Elija la puerta que desea poder bloquear antes y haga clic en el botón azul (editar).
3. Haga clic en la pestaña **Lector 1** o **Lector 2** según el Lector que requiera esta función.
4. Habilite el triple deslizamiento marcando la casilla de verificación..
5. Desde el menú desplegable de la acción **Triple pase**; elija **invalidar tarjeta** de reanudación automática y luego haga clic en **Guardar lector** en la parte inferior derecha.
6. Vaya a "Inicio/Usuarios".
7. En la pestaña General, vaya hacia abajo en la lista marcando la opción **Triple deslizamiento** para los usuarios que le gustaría tener esta capacidad y haga clic en **Guardar** a la derecha de ese usuario.
8. Actualizar paneles.

Capítulo 18. Descripción general del sistema

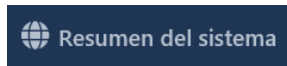
Este capítulo cubrirá la pantalla de descripción general del sistema en VAX y cómo se puede usar para simplificar las acciones, incluida la actualización de los paneles individualmente, colocar los paneles en el modo de actualización de firmware, ver todas las puertas y salidas en el sistema y ver el estado de los ascensores y pisos.

Se puede acceder a la página Resumen del sistema desde cualquier página de nuestro software. Simplemente puede hacer clic en el ícono de Paneles en línea arriba de la barra de notificaciones en el lado derecho donde se muestra el estado de su Panel.



Alternativamente, puede navegar al Administrador del sistema siguiendo los siguientes pasos:

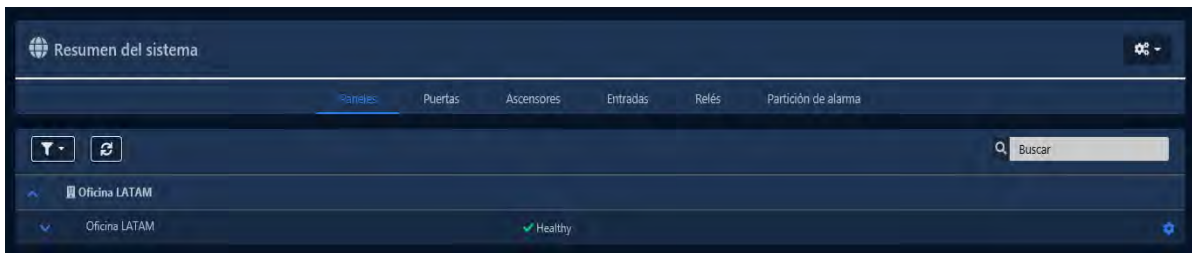
1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Inicio**; haga clic en el ícono de **Descripción general del sistema** (en la imagen a continuación).




Una vez en la pantalla de **Descripción general del sistema**, verá todas las particiones y sitios creados en su sistema y cada uno de los paneles conectados a ellos, junto con:

- Si el Panel está en línea o fuera de línea.
- Si el Panel requiere una Actualización de Firmware.

Figura 18.1. Pantalla de descripción general del sistema: vista predeterminada







Puede usar el botón  para expandir cada Panel y revelar las Puertas/Pisos asociados con sus Paneles. Esto mostrará si la Puerta/Piso está en un estado anulado o siguiendo un horario, o si la Puerta está abierta o cerrada (si hay un contacto de Puerta disponible). Las puertas están codificadas por colores para mostrar en cuál de los 8 estados de la puerta se encuentra actualmente.

Puede cambiar su vista en Descripción general del sistema con el menú en la parte superior. Seleccione **Puertas** para ver solo las Puertas en su sistema. Seleccione **Entradas** para ver solo las Entradas en su sistema. Seleccione **Salidas** para ver solo las Salidas en su sistema. Seleccione **Ascensores** para ver **Ascensores** y Pisos en su sistema.



A la derecha de cada objeto en la Vista general del sistema hay un icono con forma de engranaje. Si hace clic en este icono, aparecerá un menú desplegable con varias opciones. Dependiendo del tipo de objeto, el menú tendrá diferentes opciones disponibles. El siguiente cuadro explica cada uno de estos objetos y opciones.

Tabla 18.1. Elementos del menú de descripción general del sistema

Opción del menú	Descripción
 Opciones del menú de objetos del panel	
Actualizar panel	Realiza una actualización de Panel para ese Panel individual. Útil para probar y solucionar problemas.
Editar panel	Abre la pantalla Editar panel para el panel seleccionado.
Modo de actualización de firmware	Pone el Panel en modo de actualización de firmware.
Ver el estado	Muestra el estado de conexión del Panel en una nueva ventana.
Hora del informe	El Panel informará lo que cree que es la hora actual. Aparecerá una notificación con el resultado.
Restablecer las ubicaciones anti-passback de los usuarios	El Panel cambiará la ubicación actual de cualquier credencial a 'Sin área'.
Desconectar (por un minuto)	El Panel se desconectará del servidor y esperará 1 minuto antes de intentar volver a conectarse.
 Opciones del menú de objetos de puerta	
Pulsar Puerta	Pulsa la puerta desbloqueada; funciona igual que la acción Pulse Unlock en el menú Door Overrides.
Reanudar	Reanuda la Puerta desde un estado anulado; funciona igual que la acción Reanudar en el menú Anulaciones de puerta.
Editar puerta	Navega a la página de edición de puertas.
 Opciones del menú de Salidas	
Editar Panel	Vaya a la página de edición del panel.
 Opciones del menú de Ascensores	
Reanudar piso	Reanuda el Piso desde un estado anulado; funciona igual que la acción Reanudar en el menú Anulaciones de piso.

Capítulo 19. Configuración de particiones y sitios

Este capítulo cubrirá los aspectos del software para configurar particiones y sitios en VAX. Si no está completamente seguro de qué es una partición, visite la sección denominada "Particiones" antes de leer este capítulo.

La mayor parte de la complejidad de las particiones es el resultado de cómo ciertos objetos se comparten entre múltiples particiones, mientras que otros son por partición. El siguiente cuadro podría ayudarlo a tener una idea de cómo estos objetos interactúan con las particiones.

Tabla 19.1. Cómo los objetos interactúan con las particiones

Tipo de objeto	Partición
Horarios (Puerta, Usuario, Festivo, etc)	Por Partición
Horarios de ejecución única	por partición
Días festivos	por partición
Sitios	por partición
Grupos de privilegios de acceso	por partición
Paneles de puerta	Partición única por sitio
puertas	Partición única por sitio
Ascensores	Partición Única por Ascensor
Pisos	Partición única por sitio
Lectores	Partición única por sitio
Usuarios	Múltiples particiones
Administradores	Múltiples particiones
Niveles de crisis	Múltiples particiones
Campos Personalizados	Múltiples particiones

Agregar particiones

Aunque los conceptos detrás de las particiones VAX son complejos, la configuración es relativamente simple y directa.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono **Particiones** (en la imagen a continuación).



4. En la pantalla Particiones, verá 'Partición predeterminada' que se crea de forma predeterminada. En la mayoría de los casos, una sola partición satisface las necesidades del sistema; sin embargo, si durante la etapa de planificación usted (el instalador o el usuario final) decide que utilizar particiones beneficiaría su implementación, haga clic en el botón **Agregar** en esta pantalla.
5. En la pantalla **Agregar partición**, tendrá dos cuadros de texto para completar.

Tabla 19.2. Agregar una partición

Cuadro de texto	Descripción
Nombre	Nombre único de su partición. Acepta de 4 a 255 caracteres.
Descripción	Descripción opcional de la partición. Acepta de 4 a 255 caracteres.

Figura 19.1. Agregar pantalla de partición

- Una vez que haya completado el nombre y la descripción de su partición, haga clic en el botón **Guardar** para crear la partición. El siguiente paso es crear Sitios asociados con esas Particiones.

Agregar sitios y áreas

Agregar sitios en VAX es similar a agregar particiones, ya que van de la mano entre sí. Si no está completamente seguro de qué es un "Sitio", consulte la sección llamada "Sitios".

- Acceda a su sistema VAX a través del navegador HTML5 de su elección.
- Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de **Sitios y Áreas** (en la imagen a continuación).



- En la pantalla **Sitios y áreas**, verá el sitio predeterminado denominado **Sitio predeterminado**, al igual que con las particiones; las implementaciones pequeñas generalmente solo usan un sitio.
- Si su implementación requiere más de un sitio, o utilizará múltiples particiones, deberá agregar más sitios. Haga clic en el botón **Agregar** en esta página. En la pantalla **Agregar sitio**, tendrá varios campos para completar.

Tabla 19.3. Agregar un sitio

Cuadro de texto/Opción	Descripción
Nombre	Nombre único de su sitio. Acepta de 4 a 255 caracteres.
Descripción	Descripción opcional del Sitio. Acepta de 4 a 255 caracteres.
Zona horaria	La zona horaria local en la que reside el Sitio.
Dividir	Seleccione la partición en la que desea que resida ese sitio.

- Una vez que haya completado los campos obligatorios, haga clic en el botón **Guardar** para crear el sitio.
- Después de haber agregado sus Sitios y Áreas, probablemente querrá agregar sus **Paneles**; consulte la sección llamada "Agregar un panel a VAX Access Control".
- Al editar un sitio, tendrá varias opciones que no están disponibles al agregar un sitio. La siguiente sección cubrirá esas opciones adicionales.

Editar Sitios y Áreas: Áreas

Las áreas se crean y se asignan a las puertas para que el sistema pueda saber qué lectores dan acceso a qué áreas. Se utiliza principalmente para Anti-passback y rastreo de ubicación de Usuario (Informe de Reunión). Para agregar áreas adicionales:

- En la pantalla Editar sitio, haga clic en la pestaña **Áreas**.
- En la pestaña **Áreas**, ingrese un nombre para su nueva área y haga clic en el botón **Agregar área** en el lado derecho.



 **Nota:** El área predeterminada 'Sin área' no se puede eliminar. Ahora ha agregado un área al VAX.

Figura 19.2. Agregar un área


Para obtener más información sobre Anti-passback, consulte el *Capítulo 21, Áreas y Anti-Passback*.

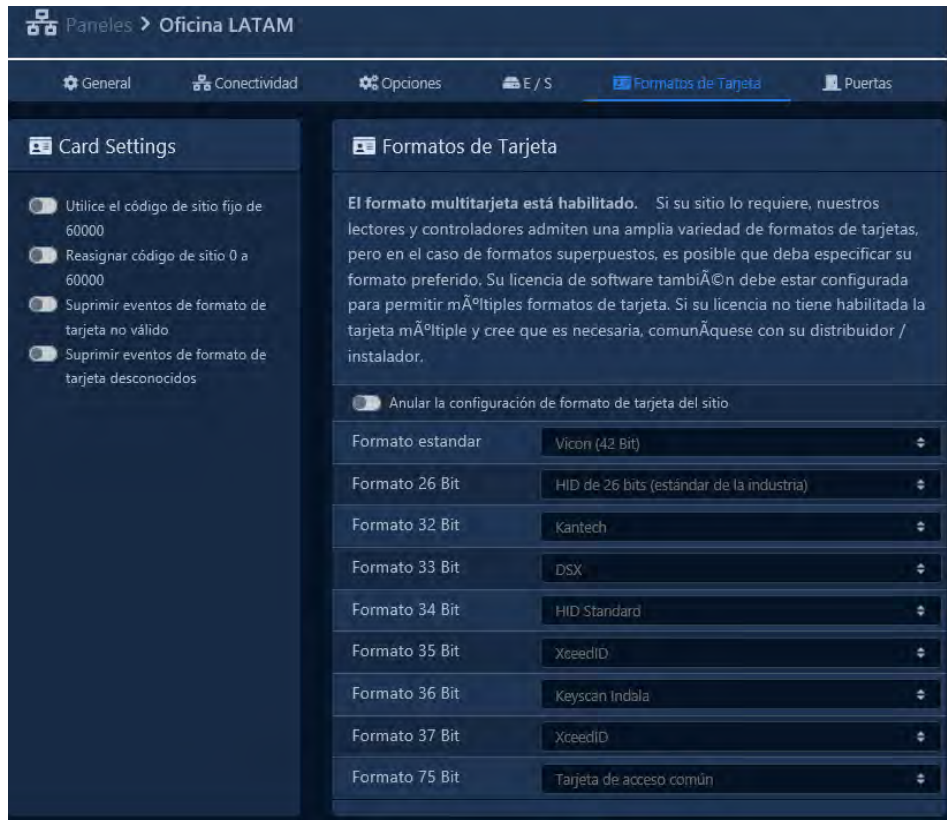
Editar Sitios y Áreas: Formatos de Tarjeta

VAX admite una variedad de formatos de tarjeta. El uso de formatos de tarjeta de terceros (cualquier formato que no sea Vicon de 40 bits) requiere que su licencia VAX habilite la característica Multi tarjetas. Si está en un período de prueba, Multicard estará habilitado de forma predeterminada. Si su licencia no tiene Multi tarjetas habilitada y cree que es necesaria, consulte el *Capítulo 4, Licencias de software*.

Los formatos de tarjeta se configuran a nivel del sitio, también se pueden anular por panel. En el caso de formatos superpuestos, es posible que deba especificar su formato preferido.

1. En la pantalla Editar sitio, haga clic en la pestaña **Formatos de tarjeta**.
2. En la pestaña **Formatos de tarjeta**, puede revisar los formatos actuales. Especifique su **formato preferido** cuando sea necesario.
3. Haga clic en el botón Guardar en la parte inferior derecha una vez que haya realizado los cambios.

Figura 19.3. Formatos de tarjeta



Capítulo 20. Administradores y privilegios

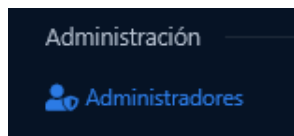
VAX Este capítulo cubrirá cómo agregar la creación y administración de cuentas de administrador, explicará cómo funcionan los grupos de seguridad y los privilegios y las opciones de autenticación avanzada disponibles. Las cuentas de administrador son especialmente útiles con varias particiones; para obtener más información acerca de las particiones, consulte la sección denominada "Conceptos" y el *Capítulo 19, Configuración de particiones y sitios*.

Administradores


Los administradores gestionan y supervisan todos los aspectos del sistema de control de acceso desde la interfaz web o mediante la aplicación móvil. Los administradores pueden tener diversos privilegios para una o todas las particiones, lo que permite otorgar acceso limitado. Esta sección cubrirá cómo crear una cuenta de administrador, cómo los administradores pueden administrar su propia configuración y cómo los administradores del sistema pueden administrar a otros administradores y generar claves API.

Agregar una cuenta de administrador

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en **Administradores** en la sección Administración cerca de la mitad del menú de navegación.



4. En la pantalla de **administradores**, verá la cuenta de administrador inicial que se creó durante la configuración inicial. Haga clic en el botón **Agregar** en esta pantalla.
5. En la sección Administrador, seleccione el tipo de autenticación que usarán. Dependiendo de la configuración de autenticación, tendrá las siguientes opciones:
 - **Local:** Las credenciales del administrador se gestionan localmente dentro del sistema.
 - **LDAP:** El correo electrónico y el nombre del administrador se sincronizan y las credenciales se autentican desde el servidor LDAP configurado. Esta opción solo aparecerá si LDAP está configurado.
 - **Cuenta de servicio:** El administrador solo accede al sistema usando una clave API y no tiene credenciales.
 - **OAuth :** El correo electrónico y el nombre del administrador se sincronizan y las credenciales se autentican desde uno de los proveedores de OAuth configurados, como Google o Microsoft.

 **Nota :** El OAuth debe agregarse en Configuración del sistema para que aparezca esta opción. Ver la sección llamada "Autenticación OAuth"
6. Según el Tipo seleccionado, complete los campos que se muestran en la sección Administrador.

Administrador

Tipo: Local Cuenta de servicio

Dirección de correo electrónico: Dirección de email única

Nombre de Usuario: Nombre de usuario único

Nombre: Primer Nombre, Apellido

Administrador del Sistema:

Idioma: English

Opciones de credenciales: Introducir contraseña Contraseña temporal Invitación

Contraseña: Ingrese una contraseña, Confirmar la contraseña

✘ La contraseña y la contraseña de confirmación deben coincidir.
 ✘ La contraseña debe tener una longitud de entre 5 y 255 caracteres.
 ✘ La contraseña requiere un carácter en mayúsculas (A-Z).
 ✘ La contraseña requiere un carácter en minúscula (a-z).

Tabla 20.1. Agregar un administrador: Opciones

Cuadro de texto/Menú desplegable/ Casilla de verificación	Descripción
Tipo	El método de autenticación para autorizar al Administrador. Las opciones son: Local, Cuenta de servicio, OAuth y LDAP (si LDAP está configurado; consulte el Capítulo 32, Integración con Active Directory).
Dirección de correo electrónico	Dirección de correo electrónico única del Administrador. Por defecto es el mismo que el nombre de usuario, pero el nombre de usuario puede ser único.
Nombre de usuario	Nombre de usuario único del administrador. Acepta de 5 a 255 caracteres.
Nombre	Nombre de los administradores. Acepta de 2 a 64 caracteres.
Apellido	Apellido de los administradores. Acepta de 2 a 64 caracteres.
Administrador del sistema	Habilita el administrador del sistema, lo que le da al administrador acceso completo a todas las funciones. Las acciones que requieren administrador del sistema se tratan en la sección de privilegios.
Idioma	Idioma que se muestra en la interfaz de usuario para el administrador.
Opciones de credenciales	Para los administradores locales, seleccione cómo se crearán sus credenciales. Introducir contraseña: especifique ahora la contraseña para el administrador. Contraseña temporal: especifique una contraseña que debe cambiarse al iniciar sesión. Invitación: si está configurado, envía una invitación por correo electrónico al administrador para que especifique una contraseña.
Contraseña	Contraseña de administradores. Acepta de 6 a 16 caracteres.
confirmar Contraseña	Contraseña de administradores. Acepta de 6 a 16 caracteres.

Nota

Los **administradores** con el administrador del sistema marcado no están sujetos a permisos de **partición**; tienen acceso ilimitado a todos los aspectos del sistema.

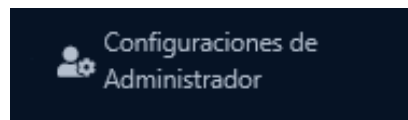
7. La segunda parte de agregar un administrador es asignar **acceso y privilegios a la partición**. Los privilegios dictan lo que un Administrador puede hacer dentro del sistema. Un administrador puede tener privilegios en varias particiones, sin embargo, algunas acciones están limitadas solo a los administradores del sistema y no estarán accesibles para los administradores normales, independientemente de los privilegios de la partición. Consulte la sección denominada "**Asignación de privilegios**" para obtener más información sobre la asignación de privilegios.
8. Como alternativa o adicionalmente, puede asignar el Administrador a uno o más Grupos de Seguridad. Los grupos de seguridad son una forma de asignar privilegios a un grupo de administradores.
9. Después de seleccionar los permisos, ahora puede hacer clic en Guardar para agregar el Administrador. Ahora puede iniciar sesión en la cuenta que ha creado y verificar que los permisos son los esperados. Si realiza cambios en una cuenta de administrador que ha iniciado sesión, es posible que el administrador deba cerrar sesión e iniciar sesión para que los cambios surtan efecto.

Configuración del administrador

Esta sección cubrirá las diversas cosas que un administrador puede hacer en la página **Configuración del administrador** que está disponible para todos los administradores.

Actualización de la configuración del administrador

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del administrador** cerca del final de la sección Administración.



Alternativamente, puede hacer clic en el menú desplegable en la parte superior derecha de la página donde se muestra el nombre del administrador y hacer clic en **Configuración**.

4. En la sección **Administrador**, puede actualizar las siguientes configuraciones.

Una captura de pantalla de la interfaz de configuración del administrador. El título es "Administrador". Hay campos de texto para "Primer Nombre" (contiene "Maria") y "Apellido" (contiene "Bustamante"). Hay menús desplegables para "Idioma" (contiene "Spanish") y "Formato de fecha y hora" (contiene "MM/DD/YYYY"). Hay un interruptor para "Tiempo militar" (está desactivado) y un campo de selección para "Reproducir sonidos de notificación" (está activado). Hay un menú desplegable para "Panel predeterminado" (contiene "-Usar sistema predeterminado-"). Hay un botón azul "Guardar" en la esquina inferior derecha.

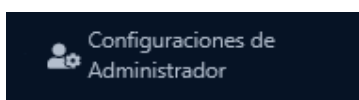
Tabla 20.2. Ajustes de Administradores

Cuadro de texto/Menú desplegable / Casilla de verificación	Descripción
Nombre de pila	Nombre de los administradores. Acepta de 2 a 64 caracteres.
Apellido	Apellido de los administradores. Acepta de 2 a 64 caracteres.
Idioma	Idioma que se muestra en la interfaz de usuario para el administrador.
Formato de fecha y hora	El formato utilizado para mostrar la fecha dentro de la interfaz de usuario.
Tiempo militar	Si mostrar la hora en horario militar de 12 a. m./p. m. o de 24 horas.
Reproducir sonidos de notificación	Configure si desea permitir que VAX reproduzca sonidos de notificación cuando se reciban ciertas notificaciones.
Panel predeterminado	El panel predeterminado que se muestra al iniciar sesión en VAX.

Haga clic en Guardar para guardar los cambios que haya realizado.

Cambiar la contraseña

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del administrador** cerca del final de la sección Administración.



Alternativamente, puede hacer clic en el menú desplegable en la parte superior derecha de la página donde se muestra el nombre del administrador y hacer clic en **Configuración**.

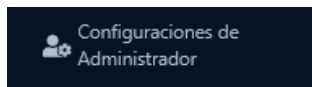
4. En la sección **Cambiar contraseña**, ingrese su **contraseña actual**.

 Una captura de pantalla de un formulario web con el título "* Cambiar contraseña". Hay tres campos de entrada de texto etiquetados como "Contraseña actual", "Nueva contraseña" y "Confirmar contraseña". Debajo de los campos hay cuatro mensajes de error con un ícono de 'x' roja: "La contraseña y la contraseña de confirmación deben coincidir.", "La contraseña debe tener una longitud de entre 5 y 255 caracteres.", "La contraseña requiere un carácter en mayúsculas (A-Z).", "La contraseña requiere un carácter en minúscula (a-z).". En la parte inferior derecha hay un botón azul que dice "Cambiar contraseña".

5. Ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Asegúrese de que su nueva contraseña cumpla con los requisitos que se muestran.
6. Haga clic en **Cambiar contraseña** para actualizar su contraseña.

Registro de autenticación de dos factores

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del administrador** cerca del final de la sección Administración.



Alternativamente, puede hacer clic en el menú desplegable en la parte superior derecha de la página donde se muestra el nombre del administrador y hacer clic en **Configuración**.

4. En la sección **Autenticación de dos factores**, puede ver dos opciones:
 - **Contraseña de un solo uso (TOTP)** Inscriba VAX en una aplicación de autenticación de terceros, como Google Authenticator o Microsoft Authenticator. La aplicación generará un código de seis dígitos que cambiará cada treinta segundos. Este código de seis dígitos debe ingresarse al iniciar sesión cuando para validar tiene acceso a la segunda forma de autenticación.
 - **Token de seguridad (FIDO)** Inscriba VAX con un autenticador de seguridad, como un teléfono inteligente o una clave de seguridad de hardware con un navegador compatible. Al iniciar sesión, el navegador le pedirá al sistema operativo que le indique que use su autenticador para validar que tiene acceso a la segunda forma de autenticación.

Registro de contraseña de un solo uso (TOTP)TFA

1. Haga clic en el botón **Contraseña de un solo uso (TOTP)** en la página Configuración del administrador.
2. Abra su autenticador TOTP preferido e inscriba un nuevo sitio utilizando el código QR. La forma de realizar esto variará dependiendo de la aplicación utilizada.
3. Escanee el código QR que se muestra en el modal de inscripción de **autenticación de dos factores**. Una vez que haya inscrito el sitio, ingrese el **Código TFA** actual en el modal para confirmar la inscripción.
4. Haga clic en Inscribirse para completar la inscripción de la autenticación de dos factores TOTP.

Registro de Token de Seguridad (FIDO)

1. Haga clic en el botón **Token de seguridad (FIDO)** en la página Configuración del administrador.
2. El navegador le indicará las opciones de autenticación disponibles. Dependiendo de su dispositivo y navegador, varias opciones pueden estar disponibles para usted, incluyendo:
 - **Clave de seguridad externa o sensor integrado:** Seleccione una clave de seguridad externa, como Yubikey, o un sensor integrado como Windows Hello o un sensor biométrico integrado en su dispositivo. La llave de seguridad externa debe conectarse o puede usar NFC para dispositivos móviles cuando sea compatible.
 - **Agregar un nuevo teléfono Android:** En los navegadores Chrome, puede usar un teléfono Android como segundo factor. Esto requerirá que abra una notificación en el teléfono y la coloque cerca de su dispositivo para realizar la autenticación de dos factores.
3. Siga las instrucciones que muestra su navegador para completar el proceso de inscripción.

Administradores de cuentas de servicio para servicios de terceros

La cuenta de servicio está disponible como tipo de cuenta cuando se agrega un administrador. El propósito de esta cuenta es permitir que los servicios de terceros interactúen con la API REST de VAX. Las cuentas de servicio del administrador usan el mismo sistema de permisos que un administrador normal; esto le permite limitar los permisos de un servicio de terceros solo a lo que ese servicio necesita (por ejemplo, un servicio como un sistema de entrada telefónica normalmente solo necesitaría el permiso Pulsar puerta)

Generación de clave API

1. Después de agregar el administrador, vaya a la pantalla Editar administrador para el administrador de la cuenta de servicio.
2. Navegue a la pestaña Clave API

Figura 20.1. Pestaña Clave API en Editar administrador

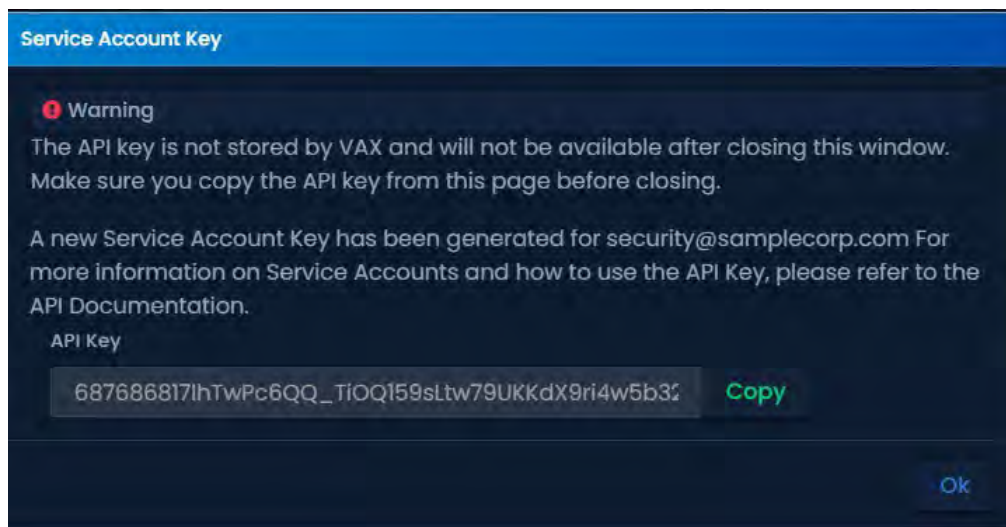


3. Haga clic en el botón Generar para generar la clave API.
4. Ahora aparecerá la clave API y se puede copiar en algún lugar para guardarla de forma segura. La clave API tendrá una validez de 1 año a partir de la fecha en que se genere. Cuando la clave API caduca, debe regenerarse y volver a ingresarse en cualquier dispositivo o servicio que la use. La clave API se puede regenerar o deshabilitar en cualquier momento.

⚠ Advertencia

VAX no almacena la clave API y no estará disponible después de cerrar esta ventana. Asegúrese de copiar la clave API de esta página antes de cerrar.

Figura 20.2. clave de API generada



Lista blanca de IPs

Todos los dispositivos y servicios que vayan a utilizar una clave API a través de un administrador de cuenta de servicio deben incluirse en la lista blanca por su dirección IP. Esta es una función de seguridad para mitigar el riesgo de que una clave de API extraviada se utilice con fines malintencionados.

Utilice los siguientes pasos para agregar direcciones IP a la lista blanca de IP:

1. Después de agregar el administrador, vaya a la pantalla Editar administrador para el administrador de la cuenta de servicio.
2. Navegue a la pestaña Clave API.
3. En la mitad inferior de la pantalla, ingrese la dirección IP del dispositivo o servicio que usará la clave API. Se admiten comodines como 192.168.2.* o 10.*.*. Se admiten varias direcciones.
4. Haga clic en el botón Agregar. La dirección IP ingresada se agregará a la lista blanca de IP.
5. Repita los pasos anteriores si se necesita más de 1 dirección IP en la lista blanca de IP.
6. Haga clic en Guardar en la parte inferior de la pantalla.

Figura 20.3. Lista blanca de IPs



Uso de una clave API

La clave API se utiliza al enviar comandos a la API REST de VAX. Los detalles sobre cómo usar la clave de API se tratan en la documentación de la API. Consulte la sección llamada "Integración de la API" para obtener información sobre cómo acceder a la documentación de la API.

Privilegios de administrador

VAX ofrece un sistema de permisos muy granular, combinado con particiones, lo que le permite otorgar acceso restringido a varias partes interesadas y tener la seguridad de que solo pueden ver y administrar lo que sea necesario. Esta sección explicará cómo funciona el sistema de permisos, cómo asignar privilegios a los administradores y grupos de seguridad y una lista de permisos disponibles.

Terminología

Administrador del sistema	Un administrador que tiene permisos completos para realizar cualquier acción en el sistema.
Asignación de privilegios	Un permiso otorgado globalmente o para una partición específica a un Administrador o un Grupo de Seguridad. Por ejemplo, permitir Agregar usuarios en la partición predeterminada.
Permisos	Consentimiento para que un Administrador visualice información o realice una acción. Por ejemplo: Ver usuarios, Agregar paneles, Anular puertas.
Alcance	Un permiso puede aplicarse o aplicarse a tres objetivos diferentes: Global, Partición y Actor.

Alcance global se aplica a todas las particiones o es una acción que se realiza a nivel global. Por ejemplo: agregar campos personalizados, administrar la configuración de LDAP.

Alcance de partición aplica el privilegio a una partición específica. Por ejemplo: Permitir agregar días festivos en la partición 1.

Alcance Actor aplica el privilegio para un actor específico (Usuario, Puerta, Panel, etc.). Por ejemplo: Excluir Editar usuarios para CEO

Resumen de Privilegios

Todos los administradores que no son administradores del sistema necesitan uno o más permisos para ver información y realizar acciones. Los permisos se otorgan asignando privilegios directamente a un administrador o indirectamente a través de la pertenencia a un grupo de seguridad.

Un privilegio permite o deniega un permiso para un administrador o grupo de seguridad. El privilegio especifica si se aplica globalmente a todas las particiones, para una partición específica o para uno o más actores específicos. Se pueden otorgar múltiples privilegios para el mismo permiso al mismo administrador, ya sea con diferentes alcances o por pertenencia al grupo de seguridad.

Al realizar la autorización para un administrador puede realizar una acción, todas las asignaciones de privilegios para el permiso dado. Dado que los administradores pueden tener múltiples privilegios para el mismo permiso, se clasifican en el siguiente:

Denegar Global

Denegar Actor

Denegar partición

Permitir Actor

Permitir partición

Permitir Global

La verificación de autorización compilará una lista de particiones y actores permitidos y denegados en función de la lista de privilegios ordenados y filtrará los resultados en consecuencia. De hecho, la denegación explícita del permiso tiene prioridad sobre la concesión explícita de permisos si hay privilegios en conflicto.

Por ejemplo, un administrador tiene dos privilegios: permitir ver usuarios en la partición A y denegar ver usuarios secretos. Verían a todos los usuarios de la partición A, excepto al usuario secreto (suponiendo que sean miembros de la partición A). Dado que el privilegio Denegar actor está clasificado más alto que el privilegio Permitir partición, el usuario secreto está oculto.

Efectivamente, una verificación de permisos dará como resultado uno de los cuatro resultados:

- **Ninguno:** No se encontraron privilegios para el Administrador, o se le denegaron privilegios, impidiéndole realizar el permiso.
- **Solo particiones/actores específicos:** Se encontraron privilegios Permitir actor o Permitir partición para el administrador, lo que les otorga acceso para ejecutar el permiso en particiones o actores específicos únicamente.
- **Todos excepto:** Se encontraron todos excepto un permiso global y uno o más privilegios de denegar actor o denegar partición para el administrador, lo que le otorga acceso para ejecutar el permiso en todas las particiones, excepto en las particiones o actores denegados especificados.
- **Permitir global:** Solo se encontró un privilegio Permitir global para el administrador, lo que les otorga acceso para realizar el permiso en todas las particiones

Asignación de privilegios

Los privilegios se pueden otorgar a los administradores de forma individual o a un grupo de administradores mediante grupos de seguridad mediante la interfaz de usuario de privilegios y acceso a particiones. Solo los administradores del sistema pueden asignar privilegios en las páginas Agregar o Editar de los administradores y grupos de seguridad.

En la parte superior de la lista, hay un menú desplegable Alcance. Esto puede establecerse en Global, que aplicará los permisos seleccionados a continuación a cada partición, o establecerse en una partición específica.


 **Nota:** *Ciertos permisos solo aparecerán en el ámbito Global, como la sección Global y Agregar partición.*

Figura 20.4. Interfaz de acceso y privilegios de partición del usuario

1. En la parte superior, seleccione el **Alcance** al que desea otorgar privilegios de Administrador o Grupo de seguridad.



2. Haga clic en la flecha derecha de la categoría que tiene el permiso que desea otorgar.
3. Puede seleccionar todos los permisos para un actor haciendo clic en la casilla de verificación o haciendo clic en la flecha izquierda para ver todos los permisos individuales disponibles para el actor.
4. Para cada permiso seleccionado, puede ampliar el alcance del privilegio seleccionando el menú desplegable **Todo** a la derecha del permiso.
5. Según el alcance del permiso, aparecerán las siguientes opciones en el menú desplegable:
 - **Todo:** El privilegio permitirá el permiso para todos los actores bajo el alcance. Por ejemplo, permitir que un administrador vea todos los usuarios en una partición.
 - **Incluye:** El privilegio permitirá el permiso solo a los actores seleccionados, en lugar de todo el alcance. Por ejemplo, permitir que un administrador solo vea y edite la puerta de su oficina.

- **Excluye:** El privilegio denegará explícitamente el permiso a los actores seleccionados, en lugar de a todo el ámbito. Por ejemplo, negarle a un grupo de seguridad la visualización de ciertos usuarios.
 - **Excepto:** El privilegio permitirá a todos los actores bajo el alcance excepto a los actores seleccionados. Por ejemplo, permitir que un administrador vea todos los mapas excepto el mapa del búnker subterráneo secreto.
 - **Denegar:** El privilegio negará explícitamente el permiso para todos los actores bajo el alcance. Por ejemplo, denegar explícitamente que un grupo de seguridad anule la puerta de la bóveda.
6. Si se seleccionan Incluir, Excluir o Excepto, aparecerá un botón a la derecha del menú desplegable. Al hacer clic en el botón, podrá seleccionar qué actores se ven afectados por el privilegio.

Para ayudar en la asignación de privilegios, hay algunas opciones para ayudar:

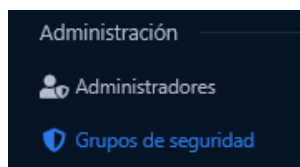
- **Buscar:** en la esquina superior derecha de la interfaz de usuario, hay un campo de búsqueda que filtrará y expandirá cualquier permiso que coincida con el término buscado. Al presionar enter en la búsqueda, se seleccionarán todos los permisos mostrados.
- **Marcar todo/Desmarcar todo:** Debajo del menú desplegable Ámbito, hay botones que seleccionan o anulan la selección de todos los permisos en el ámbito seleccionado.
- **Importar:** en la parte superior derecha debajo de la búsqueda, hay un botón Importar que le permitirá seleccionar un Administrador o Grupo de seguridad para importar todos sus privilegios y reemplazar la selección existente.

Grupos de Seguridad

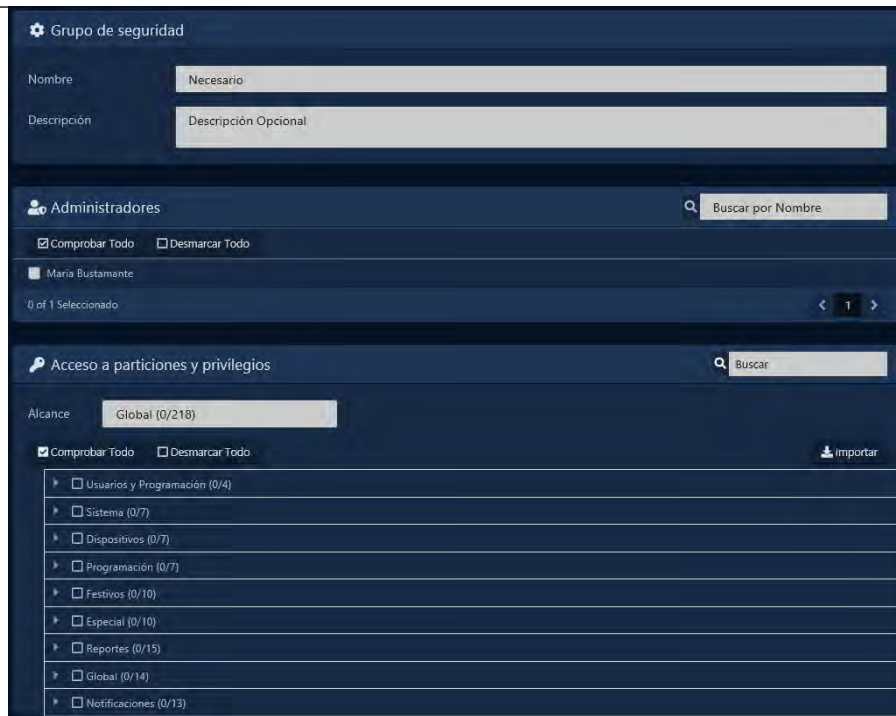
Los Grupos de Seguridad son una forma de asignar privilegios a un grupo de Administradores sin tener que editar individualmente cada uno. Además, los administradores que no son del sistema utilizan los grupos de seguridad al crear administradores para otorgar privilegios predefinidos por los administradores del sistema. Los grupos de seguridad solo pueden ser administrados por los administradores del sistema, aunque a los administradores que no son del sistema se les pueden otorgar privilegios de visualización de los grupos de seguridad para poder otorgárselos a los nuevos administradores.

Crear un nuevo grupo de seguridad

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en **Grupos de seguridad** en la sección Administración cerca de la mitad del menú de navegación.



4. En la página Grupos de seguridad, haga clic en el botón **Agregar**.



5. Introduzca un **Nombre** y una **Descripción** en la sección Grupo de seguridad..
6. Seleccione a qué **administradores** desea otorgar privilegios con el grupo.
7. En la sección **Privilegios y acceso a la partición**, seleccione los privilegios que desea asignar a los administradores seleccionados anteriormente. Para obtener más información, consulte la sección denominada "Asignación de privilegios".
8. Una vez que haya seleccionado sus administradores y sus nuevos privilegios, haga clic en **Crear**.

Ejemplos de privilegios

Dependiendo de los permisos que le otorgue a un administrador, la cantidad de iconos y secciones del software a los que pueden acceder será diferente. Esta sección mostrará un par de ejemplos de cómo se pueden usar estos permisos para ayudar a los usuarios finales del sistema a ser más eficientes.

Ejemplo: Secretaria

Una vez que se pone en marcha el sistema, el integrador de seguridad entrega una cuenta de administrador a la organización que compró el sistema. El personal de seguridad otorga una cuenta de administrador a la secretaria en la recepción con los siguientes permisos:

- Ver, agregar y editar grupos de privilegios de acceso, administrar la pertenencia a grupos de privilegios de acceso
- Ver, agregar y editar usuarios, administrar credenciales de usuario
- Informes de la actividad del usuario
- Panel de actualización
- Ver el estado de

Una vez que el nuevo administrador inicie sesión, solo verá iconos según sus permisos de administrador. Este administrador podrá cambiar/agregar usuarios, cambiar a qué puertas tienen acceso a través de grupos de privilegios de acceso, ejecutar informes de actividad de usuario y actualizar paneles cada vez que realice cambios. El privilegio de ver el estado le permitirá al administrador ver cualquier notificación si está conectado y ver si algún controlador está fuera de línea.

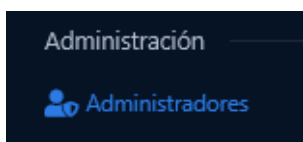
Figura 20.5. Administrador con permisos limitados

Privilege Report		
Permission	Global	Default Partition
▼ Users & Scheduling		
View Access Privilege Groups	✓	
Add Access Privilege Groups	✓	
Edit Access Privilege Groups	✓	
Delete Access Privilege Groups	✓	
Manage Access Privilege Group Membership	✓	
View Users		All
Add Users		All
Edit Users		All
Delete Users		All
Manage Users Custom Fields		All
Manage Users Images		All
Manage Users Credentials		All
Manage Users Actions		All
View Users PINs		All
Manage Users AntiPassback		All

Reporte de privilegios

El informe de privilegios en la página **Editar administradores** le permite ver fácilmente el resultado final de todos los privilegios aplicados a un administrador. Enumera todos los permisos en secciones colapsables, con cada alcance, Global y cada Partición, como columnas.

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación de la izquierda, haga clic en **Administradores** en la sección Administración cerca de la mitad del menú de navegación.



4. En la pantalla de administradores, busque al administrador que no es del sistema y desea ver su **reporte de privilegios** y haga clic en el **botón de engranaje** a la izquierda de su nombre para abrir la página Editar administradores.
5. Seleccione la pestaña **Reporte de privilegios** en la parte superior de la página.

Figura 20.6. Ejemplo de reporte de privilegios

Privilege Report		
Permission	Global	Default Partition
▼ Users & Scheduling		
View Access Privilege Groups	✓	
Add Access Privilege Groups	✓	
Edit Access Privilege Groups	✓	
Delete Access Privilege Groups	✓	
Manage Access Privilege Group Membership	✓	
View Users		All
Add Users		All
Edit Users		All
Delete Users		All
Manage Users Custom Fields		All
Manage Users Images		All
Manage Users Credentials		All
Manage Users Actions		All
View Users PINs		All
Manage Users AntiPassback		All

Las flechas izquierdas se pueden expandir y contraer para mostrar todos los permisos en cada sección.

Permisos

VAX ofrece una extensa lista de permisos para realizar todas las acciones en el sistema. Hay algunas cosas importantes que debe saber sobre cómo funcionan los permisos.

Para reducir la complejidad y mantener la comparabilidad con versiones anteriores, ciertos permisos permiten que un administrador vea otra información que se requiere para usar el permiso. Por ejemplo, el permiso Agregar grupo de privilegios de acceso permitirá a un administrador consultar una lista de lectores y pisos, entre otras cosas que se requieren.

Los permisos de visualización cumplen un par de funciones diferentes. Se requiere un permiso de visualización para utilizar los permisos correspondientes de Agregar, Editar o Eliminar, ya que se accede a todos ellos desde la página de lista. Un permiso de visualización le permite abrir las páginas de edición como de solo lectura para ver información adicional que no se muestra en la página de lista.

Los permisos de visualización también se pueden usar para evitar que el actor se asigne como un valor. Por ejemplo, excluir una puerta de la visualización impedirá que sus lectores aparezcan para ser asignados a un grupo de privilegios de acceso.

Algunas otras cosas a tener en cuenta con respecto a los permisos:

- Los privilegios de todas las particiones de las que un usuario es miembro se tienen en cuenta al realizar comprobaciones de permisos de usuario, ya que los usuarios pueden pertenecer a varias particiones.
- Excluir la visualización de un panel no oculta los dispositivos adjuntos a un panel, como Puertas y Ascensores, que tienen sus propios permisos.

- Editar plan de acción es uno de los permisos más poderosos que se pueden otorgar. Como las acciones de los planes de acción no realizan ninguna verificación de permisos, este permiso brinda efectivamente la capacidad de realizar la mayoría de las acciones en el sistema.

Permisos de administrador del sistema

La mayoría de las habilidades que antes eran exclusivas del administrador del sistema se han convertido en permisos globales. Sin embargo, todavía hay algunas cosas que siguen siendo exclusivas para los administradores del sistema, que incluyen:

- **Agregar, editar o eliminar grupos de Seguridad:** Los administradores que no sean del sistema solo pueden ver los grupos de seguridad para poder asignarlos a nuevos administradores.
- **Agregar o editar privilegios de administrador:** los administradores que no sean del sistema solo pueden asignar grupos de seguridad para otorgar privilegios si están permitidos.
- **Restablecer el bloqueo del administrador:** el restablecimiento del bloqueo de otros administradores debido a demasiados intentos de contraseña incorrectos solo lo pueden realizar los administradores del sistema
- **Configurar la autenticación:** dado que la configuración incorrecta de la autenticación podría evitar que los administradores del sistema accedan al sistema, la configuración de la autenticación está restringida a los administradores del sistema.
- **Aprobar cuentas de servicio:** dado que las cuentas de servicio solicitan sus propios permisos, esta acción solo la pueden realizar los administradores del sistema.
- **Establecer permiso maestro en los usuarios:** Dada la capacidad única de los usuarios de pertenecer a varias particiones, permitir que los administradores que no sean administradores del sistema establezcan un permiso maestro puede permitirles obtener acceso a otras particiones para las que el administrador no tenga permiso.
- **Cambiar otras credenciales de administrador o claves de API:** para evitar que los que no sean administradores del sistema obtengan acceso a cuentas con más privilegios, solo los administradores del sistema pueden cambiar las contraseñas de otros administradores, eliminar TFA de su cuenta o generar claves de API.

Permisos de usuarios y programación

Tabla 20.3. Permisos de usuarios y programación

Permisos	Alcance	Descripción
Ver privilegios de acceso a grupos	Actor	Ver la lista de Grupos de privilegios de acceso y sus asignaciones de usuarios y lectores.
Agregar privilegio de grupos de acceso	Partición	Agregar nuevos Grupos de Privilegios de Acceso con permisos de Lector y Piso. Nota: Se requiere el permiso Administrar membresía para asignar usuarios a nuevos grupos.
Editar privilegios de grupos de acceso	Actor	Edite los detalles sobre los grupos de privilegios de acceso existentes, incluidas sus asignaciones de Lector y Piso.
Eliminar grupos de privilegios de acceso	Actor	Elimine los grupos de privilegios de acceso existentes del sistema.
Ver usuarios	Actor	Ver la lista de Usuarios y sus permisos y credenciales.
Agregar usuarios	Partición	Agregue nuevos usuarios con credenciales y asignaciones de grupos de acceso.
Editar usuarios	Actor	Edite la configuración y los permisos generales de un usuario

Administradores y privilegios

Permisos	Alcance	Descripción
Administrar campos personalizados de usuarios	Actor	Edite los valores de los campos personalizados de los usuarios.
Administrar imágenes de usuarios	Actor	Agregue y elimine imágenes de perfil y accesorios para los usuarios.
Administrar credenciales de usuarios	Actor	Agregue, edite y elimine credenciales, PIN y credenciales móviles para los usuarios.
Administrar acciones de usuarios	Actor	Asigne acciones para realizar al obtener acceso a lectores específicos para los usuarios.
Ver PIN de usuarios	Actor	Capacidad para ver los PIN asignados a los usuarios.
Administrar Usuarios Anti Passback	Actor	Capacidad para ver y restablecer la posición anti-passback para los usuarios.
Ver plantillas de tarjetas	Actor	Ver la lista de plantillas de tarjetas en la partición o el sistema.
Agregar plantillas de tarjetas	Partición	Agregue nuevas plantillas de tarjetas al sistema.
Editar plantillas de tarjetas	Actor	Edite los detalles de la plantilla de tarjeta existente y su diseño y disposición.
Eliminar plantillas de tarjetas	Actor	Elimine las plantillas de tarjetas existentes de la partición o el sistema.
Ver imágenes de plantillas de tarjetas	Partición	Ver imágenes cargadas para plantillas de tarjetas en la partición o el sistema.
Eliminar imágenes de plantilla de tarjeta	Partición	Elimine las imágenes de plantillas de tarjetas existentes del sistema

Permisos del Sistema

Tabla 20.4. Permisos del Sistema

Permisos	Alcance	Descripción
Ver particiones	Actor	Ver la lista de particiones en el sistema y su configuración.
Agregar particiones	Global	Agregue nuevas particiones al sistema.
Editar particiones	Actor	Edite el nombre, la descripción y la configuración de actualización automática para las particiones existentes.
Eliminar particiones	Actor	Elimine las particiones existentes del sistema.
Ver estado de salud	Partición	Ver el estado de salud de la partición.
Ver sitios	Actor	Vea la lista de sitios y sus configuraciones de área y anti-passback.
Agregar sitios	Partición	Agregue nuevos sitios a las particiones existentes.
Editar sitios	Actor	Configura los detalles del sitio, los formatos de tarjeta, las áreas y la configuración de APB.
Eliminar sitios	Actor	Eliminar sitios del sistema.
Administrar Sitios Antipassback	Actor	Capacidad para restablecer la posición APB para todos en el sitio
Ver sitios de participación	Actor	Vea la lista de sitios de Schlage Engage y su configuración.
Agregar sitios de participación	Partición	Agregue nuevos sitios de Schlage Engage al sistema.
Editar sitios de participación	Actor	Edite los detalles sobre los sitios de Engage existentes.
Eliminar sitios de participación	Actor	Eliminar sitios de Engage del sistema.

Administradores y privilegios

Permisos	Alcance	Descripción
Ver lista de mapas	Actor	Ver la lista de mapas en la partición o sistema y su configuración.
Agregar mapas	Partición	Agregue nuevos mapas a particiones o sitios.
Editar mapas	Actor	Edite los detalles del mapa, la imagen y los objetos que se muestran en el mapa.
Eliminar mapas	Actor	Eliminar mapas del sistema.
Ver el mapa	Actor	Vea el mapa real y sus objetos representados en él.
Ver disparadores de acción	Actor	Vea la lista de activadores de acción en la partición o sistema y su configuración.
Agregar activadores de acción	Partición	Agregue nuevos disparadores de acción al sistema.
Editar activadores de acción	Actor	Edite los detalles sobre los activadores de acción existentes.
Eliminar activadores de acción	Actor	Eliminar activadores de acción del sistema.
Ver planes de acción	Actor	Ver la lista de planes de acción pero no el contenido real.
Agregar planes de acción	Partición	Agregar nuevos planes de acción al sistema.
Editar planes de acción	Actor	Edite el contenido de los planes de acción existentes. Nota: este permiso otorga efectivamente la capacidad de hacer muchas cosas, ya que los planes de acción no tienen verificación de permisos.
Eliminar planes de acción	Actor	Eliminar planes de acción del sistema.
Ejecutar planes de acción	Actor	Ejecutar planes de acción normales del sistema de seguridad.
Ejecutar Planes de Acción de Alta Seguridad	Actor	Ejecutar planes de acción del sistema de alta seguridad.
Ver Tableros	Actor	Vea la lista de tableros y el tablero real en sí.
Agregar tableros	Partición	Agregar nuevos tableros al sistema.
Editar tableros	Actor	Edite los paneles existentes y sus widgets.
Eliminar tableros	Actor	Eliminar tableros del sistema

Permisos de dispositivos

Tabla 20.5. Permisos de dispositivo

Permisos	Alcance	Descripción
Ver puertas	Actor	Ver la lista de Puertas y su configuración en la partición o sistema.
Agregar puertas	Partición	Agregue nuevas Puertas a la Partición o al sistema.
Editar puertas	Actor	Edite la configuración de Puertas en la partición o sistema, excepto sus lectores o la asignación de cámaras.
Eliminar puertas	Actor	Eliminar Puertas de la partición o sistema.
Administrar Lectores de Puertas	Actor	Asignar y configurar el lector interior y exterior de puertas en la partición o sistema.
Gestionar Puertas Anti Passback	Actor	Configurar áreas y ajustes anti-passback de puertas en la partición o sistema.
Administrar las cámaras de las puertas	Actor	Configure la asociación de cámaras y presets PTZ de puertas en la partición o sistema.
Ver ascensores	Actor	Ver la lista de ascensores y su configuración en la partición o sistema.
Agregar elevadores	Partición	Agregue nuevos ascensores a la partición o al sistema.

Administradores y privilegios

Permisos	Alcance	Descripción
Editar ascensores	Actor	Edite la configuración de los ascensores existentes en la partición o sistema excepto sus plantas, asignación de lectores y cámaras.
Eliminar ascensores	Actor	Eliminar ascensores de la partición o sistema.
Administrar pisos de ascensores	Actor	Configure detalles de piso y asignaciones de Horarios para ascensores en la partición o sistema.
Administrar lector de elevador	Actor	Asignar y configurar el lector en cabina de ascensores en la partición o sistema.
Administrar cámaras de ascensor	Actor	Configurar asociación de cámaras de ascensores en la partición o sistema.
Ver paneles	Actor	Ver la lista de paneles y su configuración en la partición o sistema.
Agregar paneles	Partición	Agregue nuevos paneles a la partición o al sistema
Editar paneles	Actor	Edite la configuración de los paneles en la partición o el sistema excepto su E/S y la contraseña del panel.
Eliminar paneles	Actor	Elimine los paneles y sus dispositivos adjuntos de la partición o el sistema.
Administrar E/S del panel	Actor	Configure las entradas y salidas de los paneles en la partición del sistema.
Administrar contraseña del panel	Actor	Ver y editar la contraseña utilizada para acceder a la interfaz del panel.
Ejecutar comandos del panel	Actor	Envíe varios comandos al panel, incluida la hora del informe, y desconecte el panel del servidor.
Actualización del firmware del panel	Actor	Ordene al panel que actualice al último firmware disponible del servidor.
Ver integradores de cámaras	Actor	Vea la lista de integradores de cámaras en la partición o el sistema.
Agregar integradores de cámara	Partición	Agregue nuevos integradores de cámara a la partición o al sistema.
Editar integradores de cámara	Actor	Edite la configuración de integradores de cámaras en la partición o sistema, sincronice y asigne cámaras al software.
Eliminar integradores de cámara	Actor	Eliminar integradores de cámara de la partición o sistema.
Ver cámaras	Actor	Vea video en vivo o grabado de las cámaras asociadas a la partición o sistema.
Ver paneles de alarma	Actor	Ver la lista de paneles de alarma en la partición o sistema.
Agregar Paneles de Alarma	Partición	Agregue nuevos paneles de alarma a la partición o al sistema.
Editar paneles de alarma	Actor	Edite la configuración de los paneles de alarma en la partición o sistema.
Eliminar paneles de alarma	Actor	Elimine los paneles de alarma y sus particiones y zonas de la partición o sistema.
Ver particiones de alarma	Actor	Ver la lista de particiones de alarma en la partición o sistema.
Editar particiones de alarma	Actor	Edite la configuración de las particiones de alarma en la partición o sistema.
Armar/Desarmar Particiones de Alarma	Actor	Armar o desarmar la partición de alarma para asegurar el área u obtener acceso.
Realizar acciones de alarma	Actor	Realice acciones como fuego o pánico auxiliar y silencie los pitidos de problemas.
Zonas de anulación	Actor	Anular zonas para permitir el armado de particiones con una zona abierta.

Programación de permisos

Tabla 20.6. Programación de permisos

Permisos	Alcance	Descripción
Ver Horarios de Puertas	Actor	Ver la lista de horarios de puerta en la partición o sistema.
Agregar horarios de puertas	Partición	Agregue nuevos calendarios de puertas a la partición o al sistema.
Editar horarios de puerta	Actor	Edite los calendarios de puerta existentes y su configuración de intervalo de tiempo.
Eliminar horarios de puerta	Actor	Elimine los horarios de puerta existentes de la partición o el sistema.
Ver horarios de piso	Actor	Ver la lista de Programaciones de piso en la partición o sistema.
Agregar horarios de piso	Partición	Agregue nuevos horarios de piso a la partición o sistema.
Editar horarios de piso	Actor	Edite los horarios de piso existentes y su configuración de intervalo de tiempo.
Eliminar horarios de piso	Actor	Elimine los Horarios de planta existentes de la partición o el sistema.
Ver puertas de ejecución única	Actor	Ver la lista de puertas de ejecución única en la partición o sistema.
Agregar puertas de ejecución única	Partición	Agregue puertas de ejecución única a la partición o al sistema.
Editar puertas de ejecución única	Actor	Edite las ejecuciones únicas de puerta existentes y su configuración de intervalo de tiempo.
Eliminar ejecuciones únicas de puerta	Actor	Elimine las ejecuciones únicas de puerta existentes de la partición o el sistema
Ver pisos de ejecución única	Actor	Ver la lista de pisos de ejecución única en la partición o sistema.
Agregar pisos de ejecución única	Partición	Agregue nuevas ejecuciones únicas de piso a la partición o al sistema.
Editar pisos de ejecución única	Actor	Edite las ejecuciones de tiempo de planta existentes y su configuración de intervalo de tiempo.
Eliminar pisos de ejecución única	Actor	Elimine las ejecuciones únicas del piso existentes de la partición o el sistema.
Ver horarios de usuario	Actor	Ver la lista de programaciones de usuario en la partición o el sistema.
Añadir horarios de usuario	Partición	Agregue nuevos horarios de usuario a la partición o al sistema.
Editar horarios de usuario	Actor	Edite los horarios de usuario existentes y su configuración de intervalo de tiempo.
Eliminar horarios de usuario	Actor	Elimine Programaciones de usuario existentes de la partición o el sistema.
Ver horarios de entrada	Actor	Ver la lista de Horarios de Entrada en la partición o sistema.
Agregar horarios de entrada	Partición	Agregue nuevos horarios de entrada a la partición o al sistema.
Editar horarios de entrada	Actor	Edite los horarios de entrada existentes y su configuración de intervalo de tiempo.
Eliminar programaciones de entrada	Actor	Elimine los horarios de entrada existentes de la partición o el sistema.
Ver programaciones de salida	Actor	Ver la lista de programaciones de salida en la partición o el sistema.
Agregar programaciones de salida	Partición	Agregue nuevos horarios de salida a la partición o al sistema.

Administradores y privilegios

Permisos	Alcance	Descripción
Editar programaciones de salida	Actor	Edite los programas de salida existentes y su configuración de intervalo de tiempo.
Eliminar programaciones de salida	Actor	Elimine los programas de salida existentes de la partición o el sistema.

Permisos de días festivos

Tabla 20.7. Permisos de días festivos

Permisos	Alcance	Descripción
Ver días festivos	Actor	Vea la lista de Días festivos y los grupos a los que afectan en la partición o el sistema.
Agregar días festivos	Partición	Agregue nuevos días festivos a la partición o al sistema.
Editar días festivos	Actor	Edite los días festivos existentes en la partición o el sistema.
Eliminar días festivos	Actor	Elimine los días festivos existentes de la partición o el sistema.
Ver grupos días festivos de puerta	Actor	Vea la lista de grupos de días festivos de puerta en la partición o el sistema.
Agregar grupos de días festivos de puertas	Partición	Agregue nuevos grupos de días festivos de puerta a la partición o sistema.
Editar grupos de días festivos de puertas	Actor	Edite los grupos de días festivos de puertas existentes en la partición o el sistema.
Eliminar grupos de días festivos de puertas	Actor	Elimine los grupos de días festivos de puerta existentes de la partición o sistema.
Ver horarios de días festivos	Actor	Ver la lista de programaciones de días festivos de la puerta en la partición o el sistema.
Agregar horarios de días festivos en la puerta	Partición	Agregue nuevos horarios de días festivos de puerta a la partición o sistema
Editar horarios de días festivos de la puerta	Actor	Edite horarios de días festivos de puerta existentes en la partición o el sistema.
Eliminar horarios de días festivos de la puerta	Actor	Elimine los horarios de días festivos de la puerta existentes de la partición o el sistema.
Ver grupos de días festivos de Piso	Actor	Ver la lista de grupos de días festivos de piso en la partición o el sistema.
Agregar grupos días festivos de piso	Partición	Agregue nuevos grupos de días festivos de piso a la partición o sistema.
Editar grupos de días festivos de piso	Actor	Edite los grupos de días festivos de piso existentes en la partición o el sistema.
Eliminar grupos de días festivos de piso	Actor	Elimine los grupos de días festivos de piso existentes de la partición o el sistema.
Ver horarios de feriados de piso	Actor	Ver la lista de horarios de días festivos de piso en la partición o el sistema
Agregar horarios de días festivos de piso	Partición	Agregue nuevos horarios de días festivos de piso a la partición o al sistema.
Editar horarios de días festivos de piso	Actor	Edite los horarios de días festivos de piso existentes en la partición o el sistema.
Eliminar horarios de días festivos de piso	Actor	Elimine los horarios de días festivos de piso existentes de la partición o el sistema.
Ver grupos de días festivos del usuario	Actor	Ver la lista de grupos de días festivos de usuarios en la partición o el sistema.
Agregar grupos de días festivos de usuarios	Partición	Agregue nuevos grupos de días festivos de usuarios a la partición o al sistema.

Administradores y privilegios

Permisos	Alcance	Descripción
Editar grupos de días festivos de usuarios	Actor	Edite los grupos de días festivos de usuarios existentes en la partición o el sistema.
Eliminar grupos de días festivos de usuarios	Actor	Elimine los grupos de días festivos de usuarios existentes de la partición o el sistema.
Ver calendarios de días festivos de los usuarios	Actor	Ver la lista de horarios de días festivos del usuario en la partición o el sistema.
Agregar horarios días festivos de usuario	Partición	Agregue nuevos horarios de días festivos de usuario a la partición o al sistema.
Editar horarios días festivos de usuario	Actor	Edite los horarios de días festivos del usuario existentes en la partición o el sistema.
Eliminar horarios de días festivos de usuario	Actor	Elimine los horarios de días festivos del usuario existentes de la partición o el sistema.
Ver grupos de días festivos del dispositivo	Actor	Ver la lista de grupos de días festivos de dispositivos en la partición o el sistema.
Agregar grupos de días festivos de dispositivos	Partición	Agregue nuevos grupos de días festivos de dispositivos a la partición o al sistema.
Editar grupos de días festivos del dispositivo	Actor	Edite los grupos de días festivos de dispositivos existentes en la partición o el sistema.
Eliminar grupos de días festivos del dispositivo	Actor	Elimine los grupos de días festivos de dispositivos existentes de la partición o el sistema.
Ver horarios de días festivos de entrada	Actor	Agregue nuevos horarios de días festivos de entrada a la partición o al sistema.
Agregar horarios de días festivos de entrada	Partición	Edite horarios de días festivos de entrada existentes en la partición o el sistema.
Editar calendarios de días festivos de entrada	Actor	Elimine horarios de días festivos de entrada existentes de la partición o sistema.
Eliminar programaciones de días festivos de entrada	Actor	Ver la lista de horarios de días festivos de salida en la partición o el sistema.
Ver los horarios de salida de vacaciones	Actor	Agregue nuevos horarios de días festivos de salida a la partición o sistema.
Agregar horarios de días festivos de salida	Partición	Edite los horarios de días festivos de salida existentes en la partición o el sistema.
Editar horarios de días festivos de salida	Actor	Elimine horarios de días festivos de salida existentes de la partición o el sistema.
Eliminar horarios de días festivos de salida	Actor	Agregue nuevos horarios de días festivos de entrada a la partición o al sistema.

Permisos especiales

Tabla 20.8. Permisos especiales

Permisos	Alcance	Descripción
Pulsar Puerta	Actor	Abrir momentáneamente las puertas en la partición o el sistema.
Invaldar puerta	Actor	Invaldar puertas a diferentes modos en la partición o sistema.
Invaldar bloqueo de puerta	Actor	Invalde las puertas para cerradas en la partición o el sistema.
Invaldar el nivel de crisis de la puerta	Actor	Invaldar puertas a un nivel de crisis en la partición o sistema.
Invaldar piso	Actor	Invaldar pisos a diferentes modos en la partición o sistema.

Administradores y privilegios

Permisos	Alcance	Descripción
Invaldar entrada	Actor	Invaldar entradas a diferentes modos en la partición o sistema.
Invaldar salida	Actor	Invaldar las salidas a diferentes modos en la partición o el sistema.
Desactivar la alarma de emergencia	Actor	Desconecte las alarmas de emergencia que se hayan disparado en los paneles de la partición o sistema.
Ver el estado de	Partición	Vea el estado en tiempo real de los dispositivos en la partición o el sistema.
Actualizar panel	Actor	Actualizar la configuración de paneles en la partición o sistema

Permisos a Reportes

Tabla 20.9. Permisos a reportes

Permisos	Alcance	Descripción
Lista de usuarios	Actor	Vea la lista de las credenciales de cada usuario en la partición o el sistema.
Actividad de la puerta	Actor	Ver informe histórico de notificaciones de puerta en la partición o sistema.
Actividad del usuario	Actor	Ver informe histórico de notificaciones de usuario en la partición o sistema.
Actividad de piso	Actor	Ver informe histórico de notificaciones de piso en la partición o sistema.
Configuración	Partición	Ver configuración de dispositivos y programación en la partición o sistema.
E/S	Partición	Ver informe histórico de notificaciones de entrada y salida en la partición o sistema.
Seguimiento del tiempo del usuario	Actor	Ver la duración del tiempo que los usuarios han pasado dentro de las áreas de la partición o el sistema.
Plan de acción	Actor	Vea el informe histórico de las notificaciones del plan de acción en la partición o el sistema.
Supervisión	Partición	Ver la página de monitoreo de notificaciones a pantalla completa.
Actividad del ascensor	Actor	Ver informe histórico de notificaciones de ascensores en la partición o sistema
APB	Partición	Vea las posiciones en tiempo real de los usuarios para anti-passback en la partición o sistema.
Historial de alertas	Partición	Vea el informe histórico de las notificaciones que se configuraron como alertas y el reconocimiento de las alertas en la partición o el sistema.
Notificaciones	Partición	Ver informe histórico de todas las notificaciones en la partición o sistema.
Registro administrativo	Actor	Ver la actividad histórica de todas las acciones realizadas por los administradores en el sistema.
Actividad de alarma DSC	Actor	Ver informe histórico de notificaciones de alarma en la partición o sistema.

Permisos Globales

Tabla 20.10. Permisos Globales

Permisos	Alcance	Descripción
Ver administradores	Actor	Ver la lista de administradores en la partición o sistema.
Agregar administradores	Global	Agregue nuevos administradores que no sean del sistema al sistema mediante grupos de seguridad para asignar privilegios.
Editar administradores	Actor	Edite detalles sobre otros administradores en el sistema.
Eliminar administradores	Actor	Elimine los administradores existentes del sistema.
Ver grupos de seguridad	Actor	Ver la lista de grupos de seguridad en el sistema. La membresía de los grupos de seguridad se puede cambiar cuando se le otorga el permiso Agregar administrador o Editar administrador.
Ver campos personalizados	Actor	Ver la lista de todos los campos personalizados en el sistema.
Agregar campos personalizados	Global	Agregue nuevos campos personalizados al sistema.
Editar campos personalizados	Actor	Edite los campos personalizados existentes y sus opciones en el sistema.
Eliminar campos personalizados	Actor	Elimine los campos personalizados existentes del sistema.
Niveles de crisis	Global	Administre los niveles de los niveles de crisis que están disponibles y qué modo de programación realizan.
LDAP	Global	Configure los ajustes de LDAP y la asignación de atributos de LDAP a credenciales o campos personalizados.
Administrar cliente	Global	Configure los ajustes globales del cliente, como la dirección del servidor y la información del distribuidor.
Ajustes del correo electrónico	Global	Configure los ajustes de SMTP utilizados para enviar correos electrónicos desde VAX.
Licencia	Global	Permita que los administradores actualicen la información de la licencia.
Base de datos	Global	Ver totales y purgar notificaciones y registros administrativos de VAX.
Migrador de datos	Global	Capacidad para exportar e importar datos al software. Nota: este permiso otorga la capacidad de agregar o actualizar la mayoría de los valores en el software y debe otorgarse de forma selectiva cuando sea necesario.
Credenciales STID	Global	Cuando se integre al portal de STid, el permiso permitirá a los administradores ver e inscribir las credenciales de pago de STid.
Ver configuración de funcionamiento del sistema	Global	Vea los problemas de salud configurados y sus umbrales y acciones en el sistema.
Editar configuración de funcionamiento del sistema	Global	Configure problemas de salud, umbrales y acciones realizadas en el sistema.
Reportes de problemas en funcionamiento del sistema	Global	Ver informe histórico de problemas de salud que registran el problema en el sistema.

Permisos de notificación

Tabla 20.11. Permisos de notificación

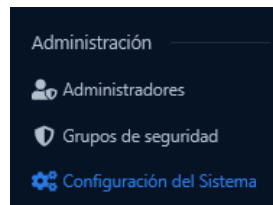
Permisos	Alcance	Descripción
Ver reglas	Partición	Vea la lista de reglas de notificación que determina dónde se envían las notificaciones procesadas en la partición o el sistema.
Administrar reglas de administración	Partición	Configure las reglas de notificación para afectar cómo se envían las notificaciones al administrador desde la partición o el sistema.
Administrar reglas globales	Partición	Configure reglas de notificación para afectar cómo se procesan globalmente las notificaciones para todos los administradores en la partición o el sistema.
Administrar reglas de base de datos	Partición	Configure las reglas de notificación de la base de datos que afectan qué notificaciones se almacenan en la base de datos para informes y su política de retención.
Administrar estilos de administración	Partición	Configure estilos para afectar cómo aparecen las notificaciones en tiempo real en la interfaz de usuario para el administrador desde la partición o el sistema.
Administrar estilos globales	Partición	Configure estilos para afectar la forma en que las notificaciones en tiempo real aparecen globalmente para todos los administradores en la partición o el sistema.
Administrar las reglas de administración de la cámara en vivo	Partición	Configure qué notificaciones activarán la cámara en vivo para que aparezca en la IU para el administrador de la partición o el sistema.
Administrar reglas globales de cámara en vivo	Partición	Configure qué notificaciones activarán la cámara en vivo para que aparezca globalmente para todos los administradores en la partición o el sistema.
Administrar reglas de alerta	Partición	Configure qué notificaciones deben considerarse alertas y requieren reconocimiento en la partición o el sistema.
Administrar grupos de reglas	Partición	Configurar grupos de reglas, lo que le permite configurar un grupo de administradores que pueden reconocer una alerta en la partición o el sistema.
Alerta de reconocimiento	Partición	Capacidad para reconocer una alerta estándar en la partición o el sistema.
Confirmar alerta de supervisor	Partición	Capacidad para reconocer una alerta de supervisor en la partición o el sistema.
Notificaciones push	Partición	Permita que se envíen notificaciones a los administradores mediante web push.

Autenticación

VAX ofrece varias formas diferentes de autenticar a los administradores para acceder al software. En esta sección se explicará cómo configurar estas diversas opciones de autenticación. Como cambiar la configuración de autenticación podría impedir que los administradores del sistema inicien sesión, ver y editar esta configuración está restringida solo a los administradores del sistema.

Autenticación Local

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del sistema** cerca del final de la sección Administración.



4. Haga clic en la pestaña **Autenticación** en la parte superior de la página Configuración del sistema.
5. En **Configuración de autenticación local**, puede actualizar las siguientes configuraciones.

Configuración de autenticación local

- Permitir autenticación local
- Longitud mínima de la contraseña: 5
- Longitud máxima de la contraseña: 255
- Requisitos de contraseña:
 - Minúscula
 - Carácter en mayúscula
 - Número
 - Símbolo
 - Sin contraseñas comunes
- Caducidad de la contraseña: 0 **Días**
- Intentos de contraseña antes del bloqueo: 5
- Tiempo de bloqueo: 10 **Minutos**

Configuración de la invitación

- Habilitar invitaciones de administrador
- Duración de la invitación: 1 **Semanas**

Contraseñas Prohibidas

Contraseña	Acción
12345	[X]
123456	[X]
1234567	[X]
12345678	[X]
123456789	[X]
123123	[X]
password	[X]
password1	[X]
test123	[X]
abc123	[X]
admin	[X]
qwerty	[X]
qwerty123	[X]
demo	[X]
demoadmin	[X]
VAX	[X]
Vicon Industries	[X]
admin	[X]

Tabla 20.12. Configuración de autenticación local

Cuadro de texto/Menú desplegable/ Casilla de verificación	Descripción
Permitir autenticación local	Establece si los administradores pueden iniciar sesión mediante la autenticación local.
Longitud mínima de la contraseña	Longitud mínima de la contraseña requerida.
Longitud máxima de la contraseña	Longitud máxima de la contraseña permitida.
Requisitos de contraseña	Requisitos de complejidad para garantizar que las contraseñas sean seguras. <ul style="list-style-type: none"> • Carácter en minúsculas: se requiere un carácter en minúsculas (a-z). • Carácter en mayúsculas: Se requiere un carácter en mayúsculas (A-Z). • Número: se requiere un número (0-9). • Símbolo: Se requiere un símbolo no alfanumérico (!, #, \$, etc.) • Sin contraseñas comunes: no se permiten las contraseñas de la lista de contraseñas prohibidas.
Caducidad de la contraseña	Un tiempo opcional en días antes de que caduque una contraseña y será necesario cambiarla para iniciar sesión. Establecer este valor en 0 deshabilita la caducidad de la contraseña. Un administrador puede configurar la contraseña Nunca caduca en Editar administrador para ignorar este requisito
Intentos de contraseña antes del bloqueo	Número de intentos de contraseña incorrectos en una cuenta de administrador antes de bloquear los intentos de inicio de sesión durante un tiempo específico.
Tiempo de bloqueo	Tiempo en minutos para bloquear una cuenta de administrador después de demasiados intentos incorrectos de contraseña.
Habilitar invitaciones de administrador	Habilite el envío de un correo electrónico de invitación a los nuevos administradores para que se inscriban y establezcan una contraseña.
Duración de la invitación	Duración en días de vigencia de la invitación al nuevo Administrador.
Contraseñas Prohibidas	Lista de contraseñas cuyo establecimiento está prohibido cuando No hay contraseñas comunes habilitadas

6. Haga clic en **Guardar** en la parte inferior derecha una vez que haya actualizado su configuración.

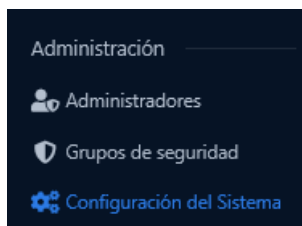
Autenticación OAuth

La autenticación OAuth usa proveedores de autenticación de terceros, como Google o Microsoft, para autorizar a los administradores a VAX. Cuando el Administrador desee iniciar sesión, VAX lo redirigirá al proveedor externo donde ingresará sus credenciales existentes. Una vez que el proveedor externo autentica sus credenciales, lo redirige a VAX con un código único que utiliza para recuperar un token de seguridad que valida la autorización del administrador.

Para realizar la autenticación, el proveedor de OAuth requerirá un URI de redirección para redirigir de nuevo a VAX. Esta URL debe ser válida dondequiera que se acceda al software, lo que generalmente requerirá que sea una dirección DNS válida que se resuelva en el servidor.

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.

2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del sistema** cerca del final de la sección Administración.



4. Haga clic en la pestaña **Autenticación** en la parte superior de la página Configuración del sistema.
5. Haga clic en la pestaña OAuth en el menú de la izquierda. En Configuración de **OAuth**, puede agregar y administrar **proveedores de OAuth de terceros** existentes.
6. Haga clic en el menú desplegable Agregar para seleccionar uno de los proveedores admitidos (**Google, Microsoft**) o un proveedor personalizado.
7. Según el proveedor seleccionado, se mostrarán diferentes campos para configurar el proveedor de OAuth. Para todos los proveedores, deberá registrarse en su sistema para recuperar una identificación de cliente y un secreto de cliente. También deberían tener una sección con más información para completar los otros campos si usan un proveedor personalizado.

Tabla 20.13. Configuración de OAuth



Cuadro de texto/Menú desplegable/ Casilla de verificación	Descripción
Activado	Establece si este proveedor de OAuth puede autenticar administradores.
Nombre	Nombre del proveedor de OAuth que se muestra en la página de inicio de sesión.
Identificación del cliente	Identificador único proporcionado por el proveedor de OAuth para identificar el servidor VAX ante el proveedor de OAuth.
Secreto del cliente	Secreto proporcionado por el proveedor de OAuth para autenticar el servidor VAX al obtener tokens de acceso.
URL de redireccionamiento	URI que el proveedor de OAuth redirigirá al Administrador de regreso a VAX con el código de autenticación. Debe seguir la siguiente sintaxis: https://[ServerAddress]:11001/oauth/[OAuthId] . OAuthId será Google o Microsoft para los proveedores compatibles, o un GUID para los proveedores personalizados.

Cuadro de texto/Menú desplegable/ Casilla de verificación	Descripción
Alcances *	Alcances solicitados al proveedor de OAuth para recuperar el correo electrónico y la información del suscriptor.
URL de autenticación *	URL del proveedor de OAuth para redirigir al administrador para realizar la solicitud de inicio de sesión.
URL del token *	URL para solicitar el token de acceso del proveedor de OAuth utilizando el código de autenticación enviado de vuelta a VAX en el URI de redirección.
Correo electrónico de reclamación *	Reclamación en el token de acceso que representa la dirección de correo electrónico del Administrador
Reclamación de identificador *	Reclamación en el token de acceso que representa el identificador único de la cuenta OAuth.
Cargar metadatos *	Establece si sincronizar las notificaciones de Nombre, Apellido e Idioma del proveedor de OAuth al iniciar sesión.
Reclamación de nombre *	Reclamación en el token de acceso que representa el nombre del Administrador.
Reclamo de apellido *	Reclamo en el token de acceso que representa el apellido del Administrador.
Reclamación de idioma *	Reclamo en el token de acceso que representa el idioma del Administrador.

8. Haga clic en **Guardar** en la parte inferior derecha una vez que haya actualizado su configuración.

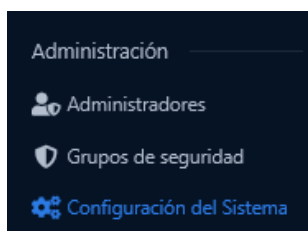
Autenticación de dos factores

La autenticación de dos factores requiere que un administrador presente una segunda forma de autenticación además de su contraseña. Esta forma de autenticación puede ser un token TOTP de seis dígitos o usar un autenticador de hardware, como una clave de seguridad o un teléfono móvil.

! Advertencia

El uso de la autenticación de dos factores FIDO requiere que la URL utilizada para acceder a VAX coincida con el campo Dirección web en Configuración del sistema para poder autenticarse. Además, se requiere un certificado SSL válido para utilizar estas funciones de mayor seguridad.

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En el menú de navegación izquierdo, haga clic en **Configuración del sistema** cerca del final de la sección Administración.



4. Haga clic en la pestaña **Autenticación** en la parte superior de la página Configuración del sistema.

5. Haga clic en la pestaña **Autenticación de dos factores** en el menú de la izquierda. En **Autenticación de dos factores**, puede configurar qué opciones de TFA están disponibles.

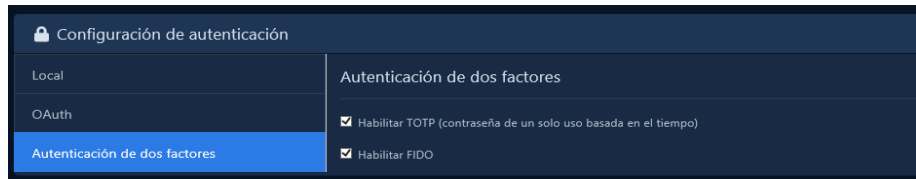


Tabla 20.14. Configuración de autenticación de dos factores

Cuadro de texto / Menú desplegable / Casilla de verificación	Descripción
Habilitar TOTP (contraseña de un solo uso basada en el tiempo)	Permita que los administradores registren autenticadores de contraseña de un solo uso basados en el tiempo como su segunda forma de autenticación.
Habilitar FIDO	Permita que el administrador registre autenticadores FIDO, como tokens de seguridad como Yubikeys, como su segunda forma de autenticación.

6. Haga clic en **Guardar** en la parte inferior derecha para guardar los cambios.


Capítulo 21. Áreas y Anti-Passback

Este capítulo cubre la configuración de Anti-Passback en VAX.

Anti-passback es una función que evitará que una Credencial (tarjeta / llavero / PIN) se use dos veces para acceder a un área sin salir primero del área monitoreada. VAX es compatible con anti-passback global y local.

Anti-passback local: funciona por controlador operando con solo dos áreas (entrada y salida). Puede operar sin el servidor VAX.

Anti-passback global: Funciona en múltiples controladores, requerido cuando hay más de una entrada a un área o cuando las áreas están anidadas dentro de áreas como estructuras de estacionamiento de varios niveles. Requiere que el servidor VAX esté disponible para que las ubicaciones de los usuarios se actualicen entre los controladores.

 **Nota:** *Anti-passback se abreviará como 'APB' en el resto de este capítulo.*

Hardware

Esta sección describirá los requisitos de hardware para anti-passback.

- El panel debe ser un controlador de puerta. Otros modelos de paneles, como elevadores y paneles IO, no admiten esta función.
- Si un Panel debe tomar decisiones anti-passback, requerirá un **Módulo de Memoria**. Consulte la siguiente sección sobre el módulo de memoria APB.
- Cada Sitio no puede tener más de 4 Códigos de Sitio / Facilidades diferentes para que anti-passback funcione completamente. Los PIN no contribuyen a este límite.

Módulo de memoria APB

Para que un controlador tome decisiones anti-passback, debe tener un módulo de memoria instalado. Los paneles sin un módulo de memoria no podrán generar violaciones anti-passback, pero pueden informar al servidor cuando un usuario ingresa a un área, que se puede reenviar a otros paneles asignados a las mismas áreas.

Especificaciones de hardware:

- Tamaño de la memoria: 512 KBKB
- Indicador LED de encendido
- Parte #: APB-MEM



Instalación del módulo de memoria

El módulo de memoria APB se inserta en el puerto P21 con la esquina con muesca del módulo hacia la parte superior izquierda cuando se enfrenta directamente al panel, de modo que la muesca rodee la esquina inferior derecha de la pantalla LCD. Asegúrese de que todas las clavijas estén bien asentadas en el zócalo y que ninguna esté doblada.

⚠ Advertencia

El módulo de memoria solo debe insertarse en el puerto 21 de un controlador cuando el controlador no está encendido; de lo contrario, el módulo podría dañarse.

Figura 21.1. Módulo de memoria instalado



Configuración del software Anti-passback

Hay tres componentes principales para configurar APB. Esta sección los cubrirá todos.

Áreas: Creadas y asignadas a puertas para que el sistema pueda saber qué lectores dan acceso a qué áreas y en qué área debe estar un usuario antes de que se le otorgue acceso a otra área.

Configuración de APB: configuración de APB a nivel del sitio. Se puede invalidar a nivel del panel.

Estado de APB: pantalla de estado que le brinda una descripción general de dónde se encuentran los usuarios en el sistema, en qué áreas estuvieron, última actividad, etc.

La configuración de anti-passback debe hacerse en el siguiente orden:

- Agregue las áreas requeridas
- Configurar los ajustes de APB a nivel del sitio
- Asigne Áreas y habilite APB en cualquier Puerta que requiera APB
- Probar y monitorear el estado de APB

📄 **Nota:** Hay un límite máximo de 32 códigos de sitio admitidos por APB

Agregar Areas

Las áreas son un elemento de configuración que se utiliza con APB. Se debe crear al menos un Área para configurar APB. Para agregar un área:

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la barra lateral, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de **Sitios y Áreas** (en la imagen a continuación)).

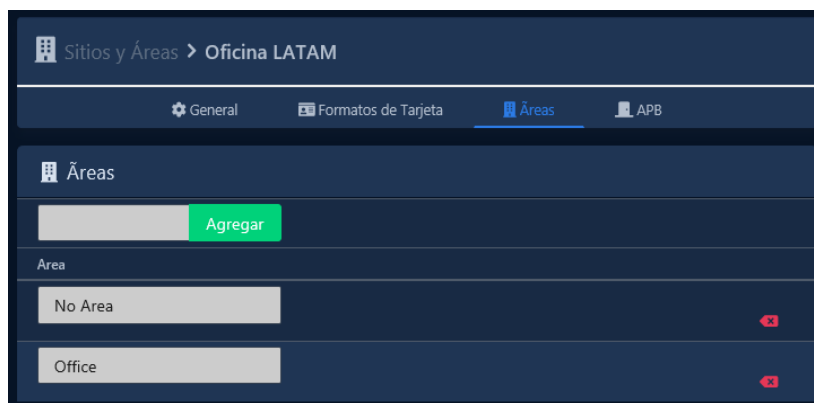


4. En la pantalla **Sitios y áreas**, verá los sitios que haya creado. Haga clic en el botón azul (configuración avanzada) junto al sitio con el que usará APB.
5. En la pantalla Editar sitio, haga clic en la pestaña **Áreas**.
6. En la pestaña **Áreas**, ingrese un nombre para su nueva área y haga clic en el botón **Agregar área** en el lado derecho.

 **Nota:** El área predeterminada 'Sin área' no se puede eliminar.

Ahora ha agregado con éxito un Área a VAX y puede continuar configurando APB.

Figura 21.2. Agregar un área



Configuración Anti-Passback

Los ajustes específicos de APB, como Tiempo de espera, APB suave y Caducidad, se configuran en el nivel del sitio. Todas las puertas adjuntas a los paneles en el sitio se adherirán a esta configuración, pero se pueden anular en la pestaña APB de la pantalla Editar puerta.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de Sitios y Áreas (en la imagen a continuación)).



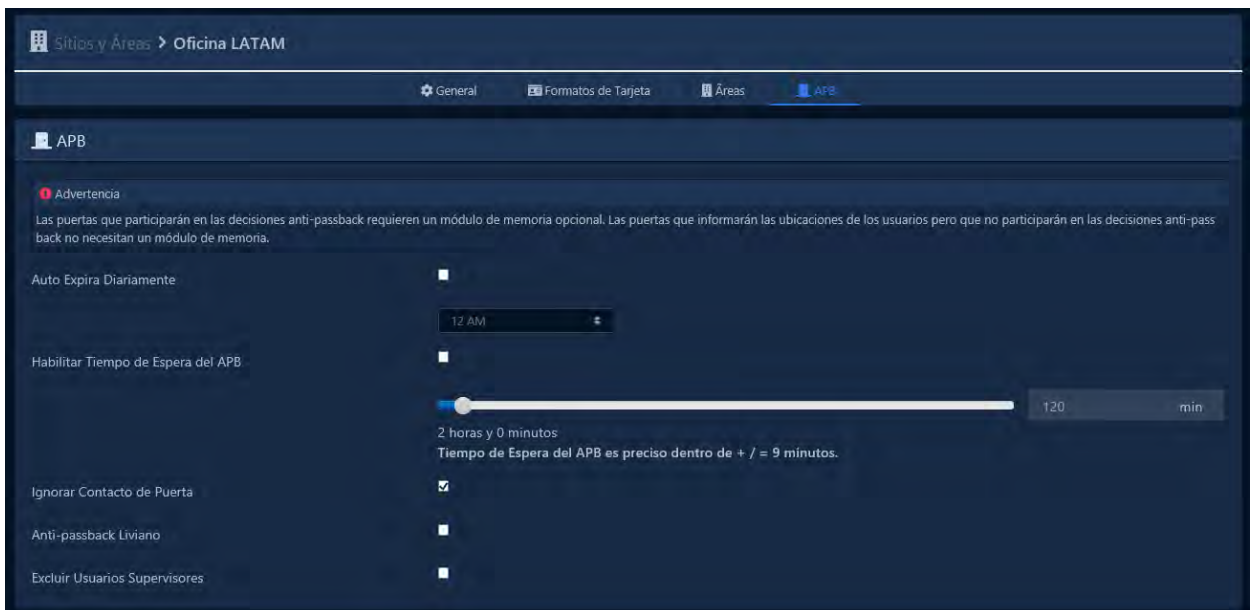
2. En la pantalla **Sitios y áreas**, verá los sitios que haya creado. Haga clic en el **botón azul** (configuración avanzada) junto al sitio con el que usará APB.
3. En la pantalla Editar sitio, haga clic en la **pestaña APB**.

- Configure los siguientes ajustes según los requisitos del sitio. Si tiene algunas puertas que requieren configuraciones diferentes en comparación con la mayoría de las puertas en el sitio, puede establecer individualmente estas mismas configuraciones desde la pantalla Editar puerta.

Tabla 21.1. Elementos de configuración anti-passback

Elementos de configuración	Descripción
Auto Caducidad Diaria	Habilite si necesita que las Áreas de usuario en el sitio se restablezcan a una hora específica cada día. Habilite y seleccione una hora del día en la que los usuarios del sitio se restablecerán a 'Sin área'.
Tiempo de espera de APB	La cantidad de tiempo (en minutos) después de que a un Usuario se le otorga acceso a un área que se le permitirá al Usuario atravesar la Puerta/Portón sin generar una infracción de APB. El tiempo de espera de APB tiene una precisión de +/- 9 minutos. Soporta de 30 a 2550 minutos.
Ignorar contacto de puerta	Si está marcado, APB ignorará el contacto de puerta. Una presentación de Credencial contará como el Usuario moviéndose al Área configurada. Si no se marca, una presentación de Credencial de usuario solo contará como movida al Área configurada si el contacto de la Puerta detecta la apertura de la Puerta.
Anti-passback suave	Cuando se marca, se informarán las infracciones de APB, pero se otorgará el acceso. Si no se marca, una violación de APB da como resultado que se le niegue el acceso al usuario.
Excluir usuarios supervisores	Los usuarios con el Privilegio de Usuario "Supervisor" estarán exentos de violaciones de APB.

Figura 21.3. Configuración APB

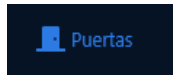


Haga clic en el botón **Guardar** una vez que se complete la configuración.

Asignación de áreas a los lectores

Esta sección demostrará cómo activar APB en una Puerta y asignar cada lector a un Área.

- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el icono de **Puertas** (en la imagen de abajo).



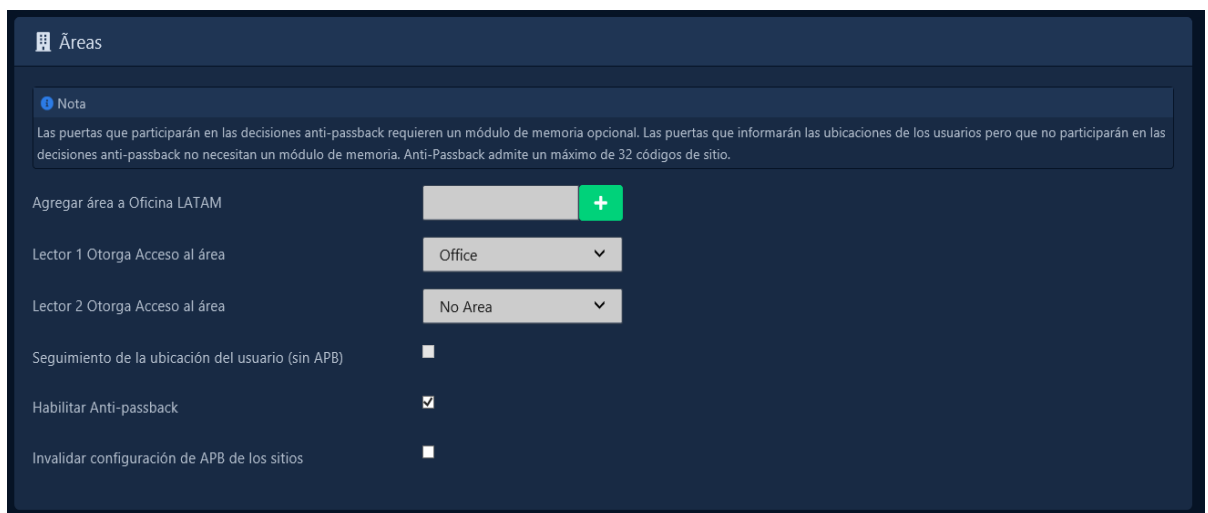
2. En la pantalla **Puertas**, verá las Puertas que ya ha configurado enumeradas aquí. Haga clic en el botón azul al lado de la puerta en la que le gustaría configurar APB.
3. En la pantalla **Editar** puerta, verá 5 pestañas. Haga clic en la pestaña **Áreas**. Los elementos de configuración de esta pantalla se explican a continuación:

Tabla 21.2. Elementos de configuración Anti-passback

Elementos de configuración	Descripción
Lector 1 otorga acceso al área	El Área a la que Lector 1 concede acceso. Seleccione un área personalizada o 'Sin área'.
Reader 2 otorga acceso al área	El Área a la que Lector 2 otorga acceso. Seleccione un área personalizada o 'Sin área'. Si no hay Reader 2, aún se debe seleccionar un área.
Habilitar Anti-Passback	Al seleccionar esta opción, se habilitará Anti-Passback. Las puertas sin paneles con módulos de memoria informarán sobre los cambios de ubicación del área de usuario cuando estén habilitadas, pero no tomarán decisiones de APB.
Anular la configuración de APB de los sitios	Seleccione si la configuración de APB en esta puerta debe ser diferente a la configuración de APB definida en la pantalla Editar sitio

Figura 21.4. Pestaña de Áreas en Editar Puerta

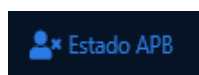
4. Haga clic en el botón **Guardar** una vez completada la configuración.
5. Los paneles deben actualizarse después de estos cambios. Ahora puede comenzar a probar y monitorear APB.



Estado y violaciones de APB

This section will outline the monitoring options for APB and how violations work. Most monitoring of APB can be done from the APB Status screen.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el icono de **estado de APB** (en la imagen a continuación).



2. Se mostrará la página de estado de APB. Aquí puede ver el estado en vivo de las áreas en las que se encuentran actualmente los usuarios. Si un usuario está en el área '**Sin área**', no se mostrará aquí.

Figura 21.5. Pantalla del estado APB



Esta pantalla se refrescará automáticamente en pocos segundos; el temporizador de actualización se puede ajustar usando el ícono de ajustes sobre la cuadrícula de ubicación del usuario. Puede alternar qué áreas se muestran a través de la lista en el lado izquierdo.

Restablecer ubicaciones de Anti-passback de usuario

En algunas circunstancias, puede ser necesario restablecer la ubicación de un Usuario. Esto puede ocurrir si un Usuario ingresó a un Área o no pudo leer fuera de un área. Hay varias formas de restablecer la ubicación de un usuario. Puede restablecer todo el sitio, un usuario individual o un solo controlador de puerta. Esta sección describirá estos métodos.

Nota:

Cuando se restablece la ubicación de un Usuario, el Usuario no generará infracciones en la siguiente tarjeta válida. Tenga cuidado al restablecer ubicaciones cuando utilice áreas anidadas (áreas dentro de áreas).

- **Restablecer usuario individual:** en la pantalla de estado de APB, haga clic en el icono de engranaje azul a la derecha de cualquier usuario. En el menú contextual, puede seleccionar 'Restablecer ubicación del usuario' para restablecer el usuario. También puede restablecer el usuario desde la pestaña Anti-passback de la pantalla Editar usuario (si el menú contextual desaparece, esto se debe a que la lista se actualiza según el temporizador de actualización).
- **Restablecer todas las ubicaciones de los sitios:** en la pantalla Estado de APB, puede hacer clic en el ícono de ajustes junto a cualquier nombre de sitio en el lado izquierdo de la pantalla. Desde el menú contextual, puede seleccionar 'Restablecer todas las ubicaciones del sitio' para restablecer todas las ubicaciones de los usuarios que se encuentran actualmente en cualquier área del sitio seleccionado.
- **Expiración automática diaria:** si es necesario, se puede configurar un sitio individual para restablecer todas las ubicaciones de los usuarios a una hora específica del día. Consulte la sección llamada "Configuración Anti-Passback" para conocer las opciones de configuración.

APB Violaciones

Una violación de APB ocurre cuando un Usuario intenta ingresar a un Área en la que ya se encuentra o intenta ingresar a un Área albergada sin ingresar al Área anterior.

De manera predeterminada, una violación de APB dará como resultado que se le niegue el acceso al usuario. Si Soft Anti-passback está habilitado, se generará una infracción, pero se otorgará al usuario acceso al Área.

Las infracciones de APB se pueden configurar para enviar un correo electrónico y/o activar una vista de cámara. Para obtener más información, consulte la sección denominada "Notificaciones por correo electrónico."

Figura 21.6. Violaciones APB

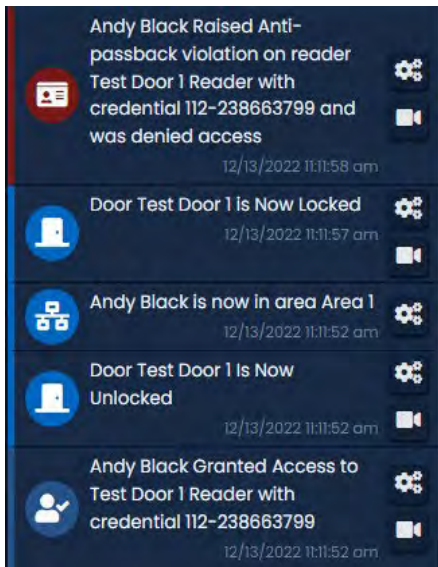
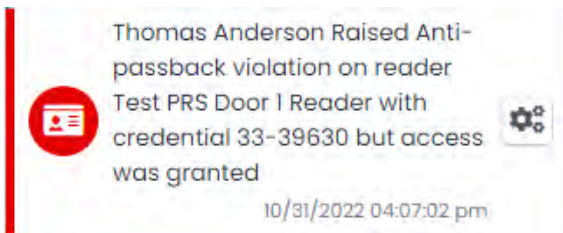


Figura 21.7. Violaciones Soft APB



Capítulo 22. Configuración de Mantrap

Este capítulo cubre la configuración de Mantraps en VAX. Esta función está disponible en la versión 3.1+ y solo se admite en modelos de panel seleccionados y puede requerir cableado adicional para funcionar.

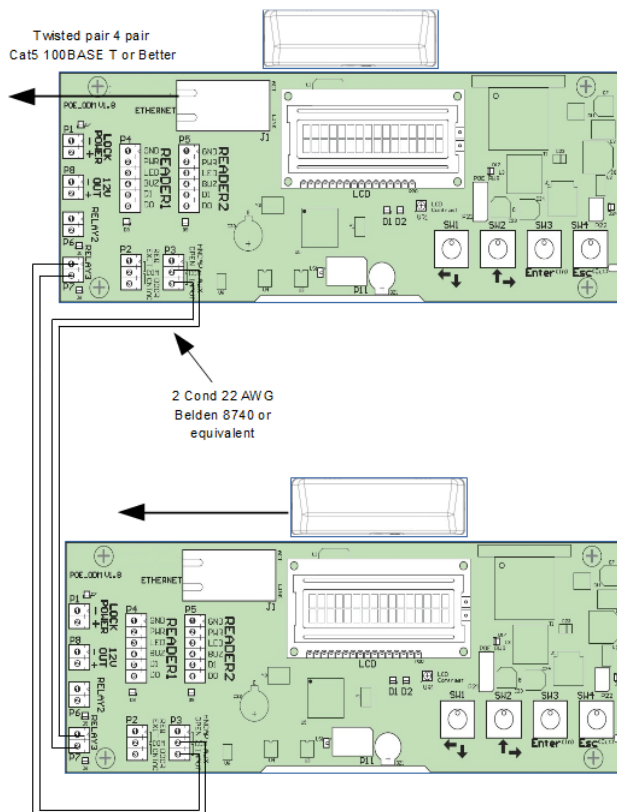
Mantrap (también llamado esclusa de aire o vestíbulo de control de acceso) se usa comúnmente en áreas de alta seguridad donde un titular de tarjeta ingresa a un espacio cerrado entre dos (o más) puertas. Cuando se abre o desbloquea la primera puerta, la segunda puerta recibirá una señal de la puerta abierta indicándole que no abra ni desbloquee. La segunda puerta no permitirá el paso hasta que la primera puerta esté cerrada. Esto también funciona a la inversa.

Configuración del hardware Mantrap

La configuración de mantrap es compatible con múltiples controladores (2 x VAX-1D-1 o controladores de puerta de 12 VCC) y entre dos puertas en un solo panel de dos puertas (1 x VAX-2D-1).

Panel separado: Esta configuración requiere que ambos paneles con puertas en la trampa tengan 1 salida disponible y 1 entrada disponible. Una Salida de cada Panel se conectará a una Entrada en el otro Panel en la configuración de Mantrap. Por favor vea el diagrama de abajo.

Figura 22.1. Controlador separado para Mantrap

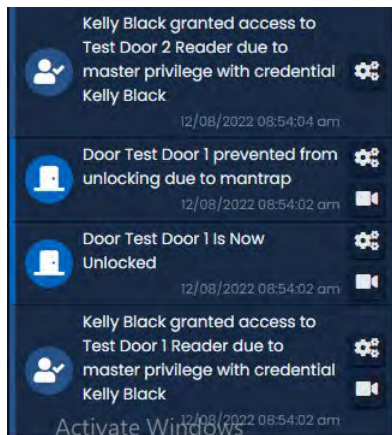


Una vez implementado el diagrama anterior, utilice los siguientes pasos para configurar las Entradas/Salidas.

1. Acceda a su sistema de control de acceso VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono **Paneles** (en la imagen a continuación).



4. Haga clic en el botón **azul** (Configuración avanzada) junto al Panel que desea configurar.
5. En la pantalla **Editar** panel, verá 4 pestañas. Haga clic en la pestaña **E/S**. Ahora podemos configurar la Entrada que indicará a la puerta que no se abra o no permita el acceso, y la Salida que indicará a la otra puerta que la puerta de este Panel está abierta o desbloqueada.
6. Seleccione la Entrada que recibirá una señal del Panel cuando otra Puerta en la configuración Mantrap esté desbloqueada o abierta. Cambie el menú desplegable Función a "Evitar desbloqueo de puerta".
7. Seleccione la Salida del Panel que estará señalando al otro Panel. Cambie el menú desplegable Función a "Puerta desbloqueada o abierta".
8. Su pantalla de E/S debería verse muy similar al ejemplo a continuación:



9. Presione el botón **Guardar** en la parte inferior de la pantalla. Realice una actualización del panel y comience la prueba.

Repita este proceso en cualquier panel adicional que participará en Mantrap.

Ambas puertas en la misma configuración de VAX-2D-1: esta configuración no requiere ninguna entrada o salida adicional para funcionar cuando se utiliza un panel de dos puertas. Solo necesitamos configurar una configuración de software para que ambas puertas se comporten de la misma manera que dos controladores de puerta única conectados entre sí.

Una vez que se hayan agregado ambas puertas al panel, utilice los siguientes pasos para habilitar la funcionalidad Mantrap.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el icono de **Puertas** (en la imagen de abajo).



2. En la pantalla **Puertas**, verá las Puertas que ya ha configurado enumeradas aquí. Haga clic en el botón azul al lado de una de las puertas que usará el Mantrap.
3. En la pantalla **Editar** puerta, verá 5 pestañas. Haga clic en la pestaña **Opciones**.
4. En la pestaña **Opciones**, habrá una casilla de verificación con la etiqueta "Evitar desbloquear si la puerta emparejada está abierta". Asegúrese de que esté marcado.
5. Presione el botón **Guardar** en la parte inferior de la pantalla. Realice una actualización del panel y comience a probar.

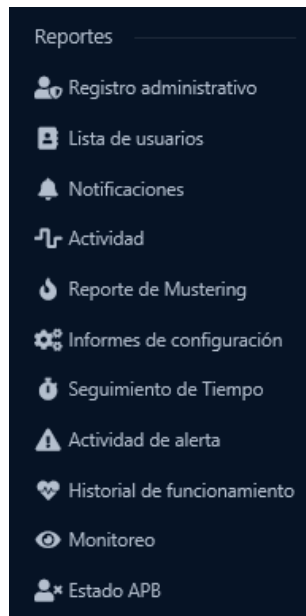
Capítulo 23. Reportes

Este capítulo será una descripción general de las diversas funciones de informes en VAX. Estos informes pueden ser útiles para rastrear usuarios, puertas, pisos, notificaciones pasadas y administradores. Cada sección de este capítulo cubrirá uno de los elementos de la categoría de informes en la página de inicio.

Tabla 23.1. Reportes en VAX

Reporte de registro administrativo	Reporte de lista de usuarios
Reporte de Notificaciones	Reporte de actividad de la puerta
Reporte de reunion (mustering)	Reporte de actividad de piso
Reporte de actividad del ascensor	Reporte de actividad del usuario
Reporte de actividad de entradas	Reporte de actividad de salida
Reportes de Configuración	Reporte de actividad del plan de acción
Reporte de actividad de alertas	Reportes de Actividad de Particiones de Alarma

Figura 23.1. Opciones de Reportes



Registro administrativo

Esta sección cubre qué es el registro administrativo y cómo ejecutarlo en VAX.

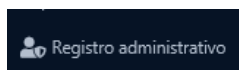
El registro administrativo es un informe que se utiliza para realizar un seguimiento de las actividades de otros administradores en VAX. Este informe le permite ver qué configuraciones han cambiado otros administradores y cuándo el administrador realizó ese cambio. Las opciones para exportar el informe también están disponibles.

Nota

Solo las cuentas de administrador con privilegios de administrador del sistema tendrán acceso para ejecutar este informe. Para obtener más información sobre los privilegios de administrador del sistema, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para ejecutar un informe de registro del administrador:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **registro administrativo** (en la imagen a continuación).



2. Una vez en la pantalla **Registro administrativo**, tendrá 3 secciones para completar:
 - a. **Intervalo de fechas:** seleccione la **hora de inicio y la hora de finalización** con las que desea ejecutar el reporte. Aparecerá el **widget Selector de fecha**. Utilice el selector de calendario y hora para seleccionar la fecha y hora para iniciar/detener el reporte.

También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.2. Widget Selector de fecha

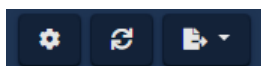
- b. **Administradores:** Seleccione los administradores con los que desea ejecutar el informe. Puede seleccionar más de uno a la vez, o solo un administrador individual.



- c. **Resultados:** Elija el formato de salida del informe. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

3. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar Reporte** en la parte inferior de la página. Accederás a los resultados del informe.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el informe de los resultados en línea usando el botón de exportación.



Nota: Depending on the size of the report, it may take several minutes to generate.

Actividad del usuario

Esta sección cubre qué es el Informe de actividad del usuario y cómo ejecutarlo en VAX.

Este informe le permite ver con qué Puertas, Pisos y Lectores ha estado en contacto una cuenta de Usuario, incluido el acceso otorgado y el acceso denegado. Las opciones para filtrar, clasificar y exportar el informe también están disponibles.

Nota

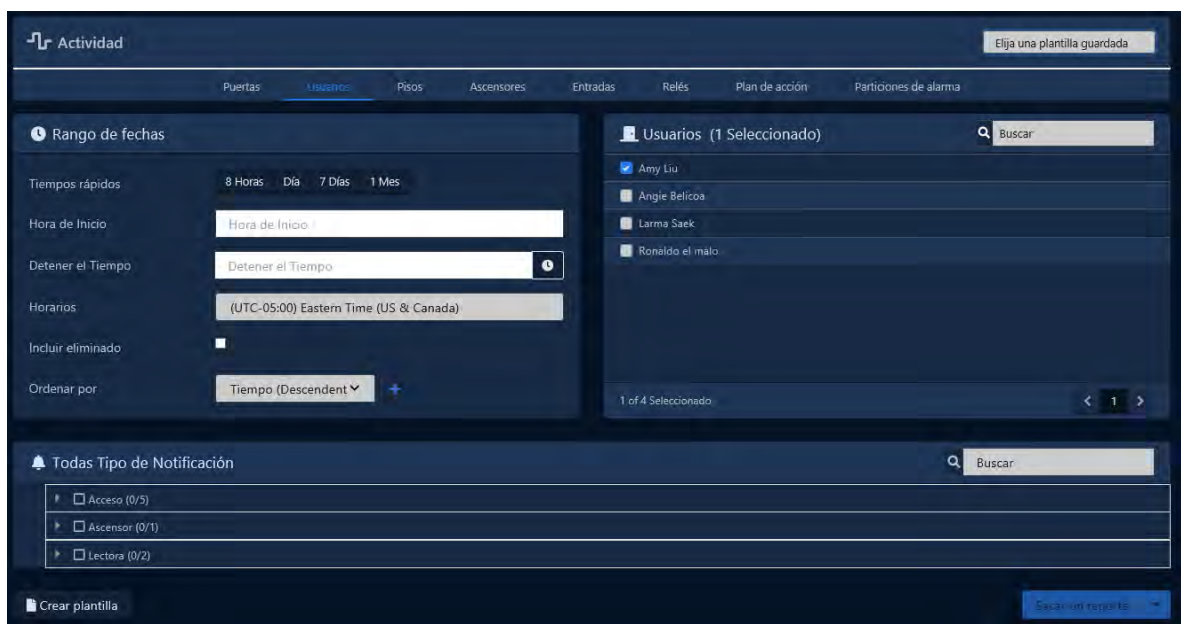
Los administradores que no sean administradores del sistema requerirán que se active el privilegio de administrador de actividad de usuario; solo los Usuarios en esa Partición serán visibles para el administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Use los siguientes pasos para ejecutar un Informe de actividad del usuario:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



2. Seleccione **Usuarios** de la lista de opciones en la parte superior de la página Actividad.
3. Una vez en la pantalla de actividad del usuario, tendrá 5 secciones para completar.



Intervalo de fechas: seleccione la **hora de inicio y la hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el **widget Selector de fecha**. Utilice el selector de calendario y hora para seleccionar la fecha y hora para iniciar/detener el reporte.

También puede seleccionar a qué **zona horaria** se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.3. Widget selector de fecha

- b. **Usuarios:** seleccione los usuarios con los que desea ejecutar el reporte. Puede seleccionar más de uno a la vez, o solo un usuario individual. La barra de búsqueda se puede utilizar para encontrar usuarios rápidamente.
- c. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el reporte en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar acceso denegado, infracciones anti-passback y muchos otros filtros.

Figura 23.4. Tipos de notificaciones

- i. **Clasificación:** puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.5. Clasificar

Generar de reporte: elija el formato de salida del reporte de la lista desplegable Ejecutar reporte. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figura 23.6. Correr reporte

- d. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte

Si desea cambiar los parámetros del informe, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los reportes de actividad de usuario exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Sitio:** sitio en el que ocurrió el evento.
- **Usuario:** nombre y apellido del Usuario al que está asociado el evento.
- **Número de Tarjeta:** Credencial (PIN o Tarjeta) que el Usuario utilizó con el evento.
- **Dispositivo 1:** Lector o Piso en el que ocurrió el evento.
- **Dispositivo 2:** Puerta o Ascensor adjunto al Dispositivo 1.
- **Mensaje:** Información adicional sobre el evento, como Acceso Concedido/Acceso Denegado, el Usuario, Credencial, Lector o Piso.

Actividad de Puerta

Esta sección cubre qué es el reporte de actividad de la puerta y cómo ejecutarlo en VAX.

El reporte de actividad de la puerta se utiliza para rastrear las actividades de las puertas en VAX. Este reporte le permite ver qué han estado haciendo las puertas, cuándo se abrieron, cuándo se desbloquearon y a qué usuarios se les otorgó o denegó acceso a estas puertas. Las opciones para exportar el reporte también están disponibles.

Nota

Los administradores que no sean administradores del sistema requerirán que el **privilegio de administrador** de reportes de actividad de puertas esté activado; solo las Puertas adjuntas a los Paneles en esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

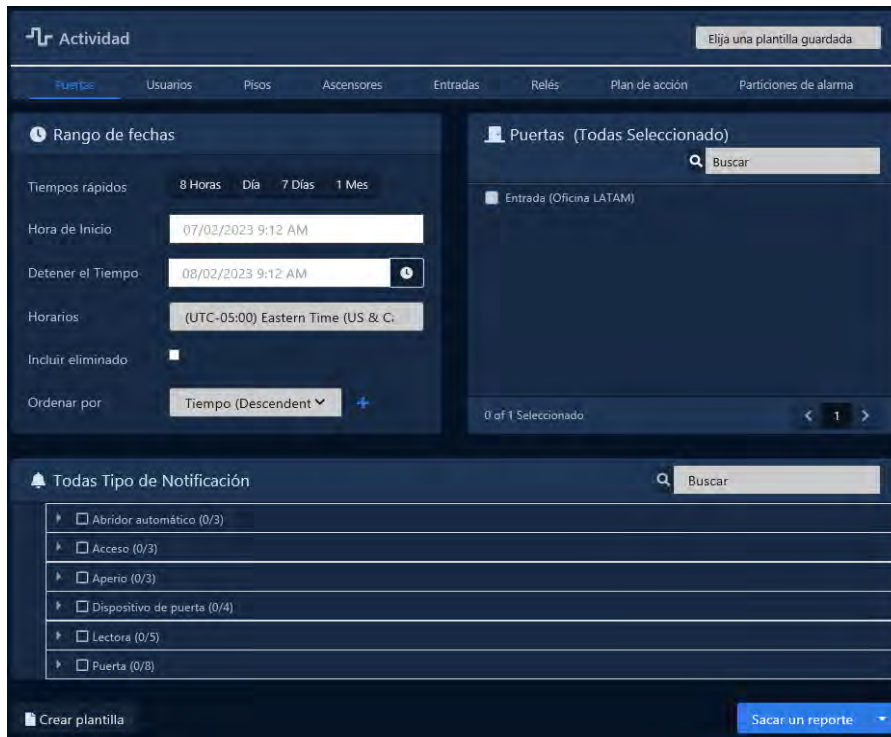
Actividad 196

Utilice los siguientes pasos para ejecutar un reporte de actividad de puerta:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



2. Seleccione **Puertas** de la lista de opciones en la parte superior de la página Actividad.



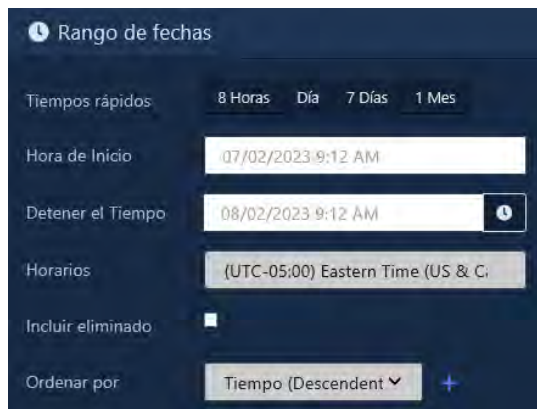
3. Una vez en la pantalla **Actividad de la puerta**, tendrá 5 secciones para completar.

a. **Intervalo de fechas:** seleccione la hora de **inicio** y la hora de **finalización** con las que desea ejecutar reporte. Aparecerá el widget Selector de fecha. Use el selector de calendario y hora para elegir la fecha y la hora para iniciar/detener el reporte.

a

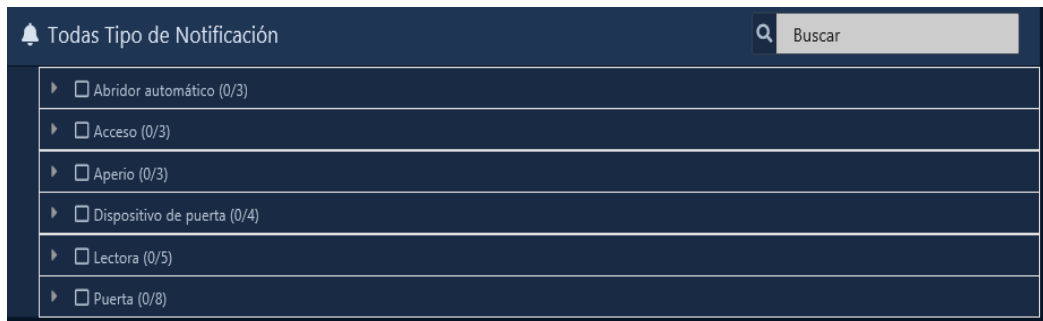
También puede seleccionar a qué zona horaria se convertirá el reporte exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.7. Widget selector de fecha

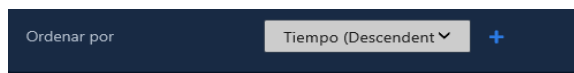


b. **Puertas:** seleccione las puertas contra las que desea ejecutar el reporte. Puede seleccionar más de una a la vez, o solo una puerta individual. La barra de búsqueda se puede utilizar para encontrar Puertas rápidamente.

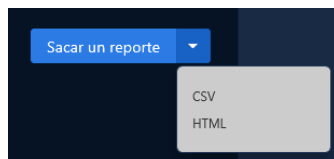
c. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el reporte en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar Puerta forzada abierta, mantenida abierta y muchos otros filtros.

Figura 23.8. Tipos de notificaciones

- d. **Clasificación:** puede configurar cómo se ordenarán los resultados del reporte. El valor predeterminado es **Tiempo** descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.9. Clasificación

- e. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable Ejecutar reporte. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figura 23.10. Generar un Reporte

- f. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en Ejecutar reporte en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del informe, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los reportes de actividad de puerta exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Sitio:** sitio en el que ocurrió el evento.
- **Puerta:** nombre de la Puerta a la que está asociado el evento.
- **Lector:** Lector al que está asociado el evento.
- **Usuario:** si un usuario está asociado con el evento, el nombre y el apellido se mostrarán aquí.
- **Número de tarjeta:** si una credencial estuvo involucrada en el evento, se mostrará aquí.

- **Mensaje:** Información adicional sobre el evento, como Acceso Concedido/Acceso Denegado, el Usuario, Credencial, Lector y Piso.

Nota: Las invalidaciones, los botones de salida y los OTR no tendrán una entrada en la categoría de Lector, Usuario y Número de Tarjeta.

Reporte de actividad de piso

Esta sección cubre qué es el Reporte de actividad del piso y cómo ejecutarlo en VAX.

El informe de actividad de los pisos se utiliza para realizar un seguimiento de las actividades de los pisos en VAX. Este Reporte le permite ver qué han estado haciendo los pisos, cuándo se accedió a ellos y a qué usuarios se les otorgó o denegó el acceso a estos pisos. Las opciones para exportar el Reporte también están disponibles. Este Reporte difiere del reporte de actividad de ascensores en que se centra en los pisos en lugar de en las cabinas de ascensores individuales. No verá la actividad de los usuarios en este informe si no utilizan la detección de botones.

Este reporte se enfoca en pisos individuales y no mostrará la actividad del usuario si el ascensor no está utilizando la detección de botones. Utilice el informe de actividad del ascensor en su lugar si el ascensor no utiliza la detección de botones. *Ver reporte de Actividad del Ascensor.*

Nota

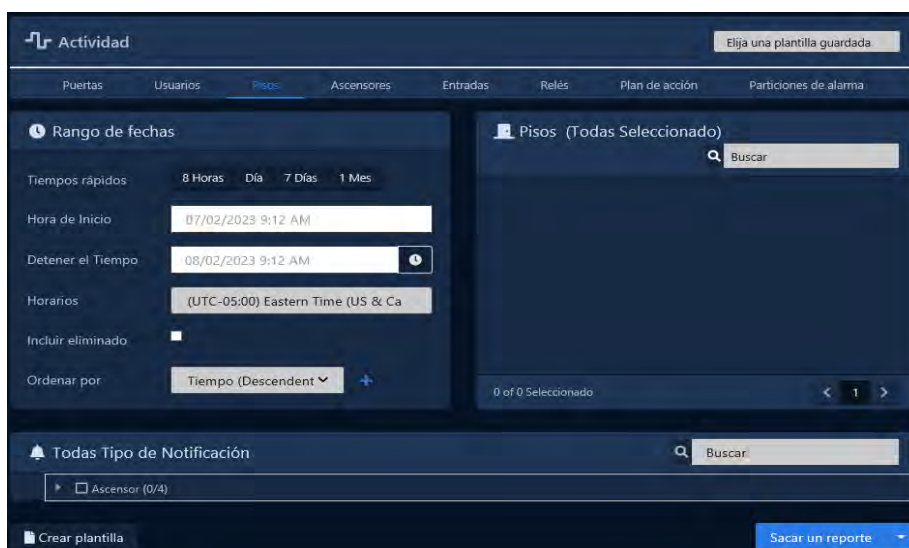
Los administradores que no sean administradores del sistema requerirán que se active **el privilegio de administrador de actividades** en reportes de pisos; solo los Pisos adjuntos a los Paneles en esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios.*

Utilice los siguientes pasos para ejecutar un reportes de actividad de piso:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



2. Seleccione **Pisos** de la lista de opciones en la parte superior de la página Actividad.



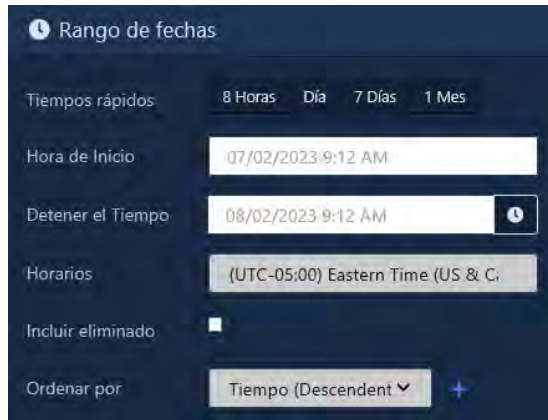
3. Una vez que esté en la pantalla **Actividad de piso**, tendrá 5 secciones para completar.

- a. **Intervalo de fechas:** seleccione la hora de **inicio** y la hora de **finalización** con las que desea ejecutar reporte. Aparecerá el widget Selector de fecha. Use el selector de

calendario y hora para elegir la fecha y la hora para iniciar/detener el reporte.

También puede seleccionar a qué zona horaria se convertirá el reporte exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.11 Widget selector de fecha



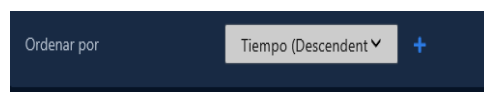
- b. **Pisos:** seleccione los pisos en los que desea ejecutar el reporte. Puede seleccionar más de uno a la vez, o solo un piso individual. La barra de búsqueda se puede utilizar para encontrar pisos rápidamente.
- c. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el reporte en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar Acceso denegado, Piso anulado y muchos otros filtros.

Figura 23.12. Tipos de notificaciones (más disponibles)



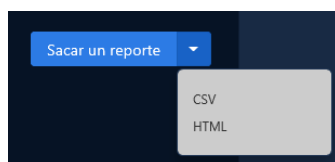
- d. **Clasificación:** puede configurar cómo se ordenarán los resultados del reporte. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.13. Clasificación



- e. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.14. Run Report



- f. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del informe, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los informes de actividad de isos exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Sitio:** el sitio en el que ocurrió el evento.
- **Ascensor:** nombre del Ascensor al que está asociado el evento.
- **Piso:** nombre del Piso al que está asociado el evento.
- **Usuario:** si un usuario está asociado con el evento, el nombre y el apellido se mostrarán aquí.
- **Número de tarjeta:** si una credencial estuvo involucrada en el evento, se mostrará aquí.
- **Mensaje:** Información adicional sobre el evento, como Acceso Concedido/Acceso Denegado, el Usuario, Credencial, Lector y Piso.

Nota : Las invalidaciones y los OTR no tendrán una entrada en la categoría Usuario y número de tarjeta.

Reporte de actividad del ascensor

Esta sección cubre qué es el reporte de actividad del elevador y cómo ejecutarlo en VAX.

El reporte de actividad del ascensor se utiliza para realizar un seguimiento de las actividades de las cabinas de los ascensores en VAX. Este reporte le permite ver qué han estado haciendo las cabinas, cuándo se accedió a ellos y a qué usuarios se les otorgó o denegó el acceso a ellas. Las opciones para exportar el reporte también están disponibles. Este informe difiere del reporte de actividad de piso en que se centra en las cabinas de los ascensores en lugar de en los pisos individuales.

Nota

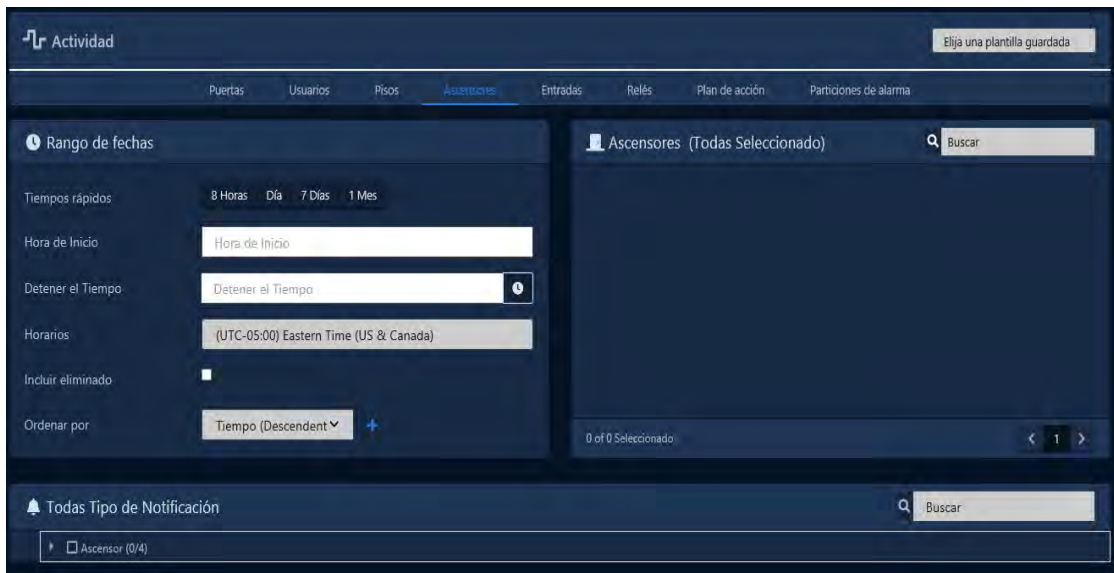
Los administradores que no sean administradores del sistema requerirán que se active el **privilegio de administrador de reportes de actividad del elevador**; solo los ascensores adjuntos a los paneles en esa partición serán visibles para el administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para ejecutar un informe de actividad del ascensor:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



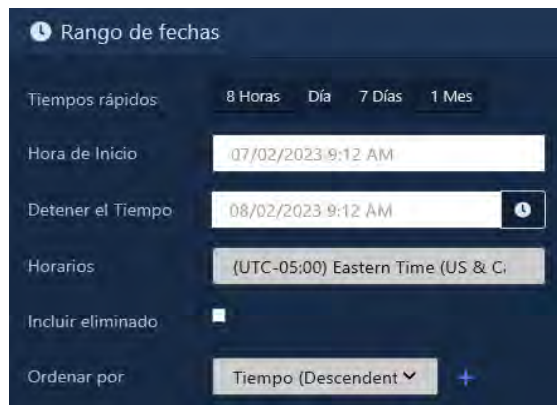
2. Seleccione **Ascensores** de la lista de opciones en la parte superior de la página Actividad.
3. Una vez en la pantalla **Actividad del ascensor**, tendrá 5 secciones para completar.



- a. **Intervalo de fechas:** seleccione la hora de **inicio** y la hora de **finalización** con las que desea ejecutar reporte. Aparecerá el widget Selector de fecha. Use el selector de calendario y hora para elegir la fecha y la hora para iniciar/detener el reporte.

También puede seleccionar a qué zona horaria se convertirá el reporte exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.15. Widget Selector de fecha



- a. **Ascensores:** seleccione los ascensores con los que desea ejecutar el reporte. Puede seleccionar más de uno a la vez, o solo una cabina individual. La barra de búsqueda se puede utilizar para encontrar ascensores rápidamente.
- b. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma **predeterminada**.

Figura 23.16. Tipos de Notificaciones



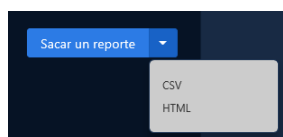
- c. **Clasificación:** puede configurar cómo se ordenarán los resultados del reporte. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.13. Clasificación



- d. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figura 23.18. Generar reporte



- a. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del informe, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los informes de actividad de ascensores exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Sitio:** el sitio en el que ocurrió el evento.
- **Ascensor:** nombre del Ascensor al que está asociado el evento.
- **Piso:** nombre del Piso al que está asociado el evento.
- **Usuario:** si un usuario está asociado con el evento, el nombre y el apellido se mostrarán aquí.
- **Número de tarjeta:** si una credencial estuvo involucrada en el evento, se mostrará aquí.
- **Mensaje:** Información adicional sobre el evento, como Acceso Concedido/Acceso Denegado, el Usuario, Credencial, Lector y Piso.

Nota: Las anulaciones y los OTR no tendrán una entrada en la categoría Usuario y número de tarjeta

Lista de usuarios

Esta sección cubre qué es el reporte de la lista de usuarios y cómo ejecutarlo en VAX.

El reporte de lista de usuarios se utiliza para ver todos los usuarios en el sistema (que tiene permiso para ver). Esto incluye campos personalizados, permisos, grupos de acceso y más. Las opciones para exportar el reporte también están disponibles.

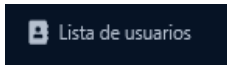
Nota

Los administradores que no son administradores del sistema requerirán que el privilegio de administrador de la lista de usuarios de informes esté activado. Solo los usuarios de esa partición serán visibles para el

administrador en la lista de usuarios. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

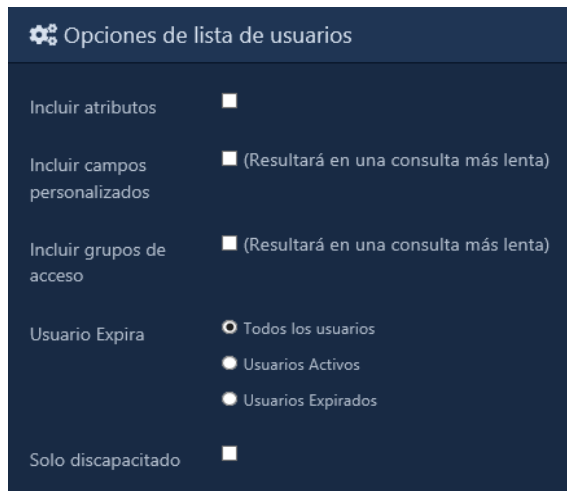
Use los siguientes pasos para ejecutar el Reporte de lista de usuarios:

1. **En la barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el icono **Lista de usuarios** (en la imagen a continuación).



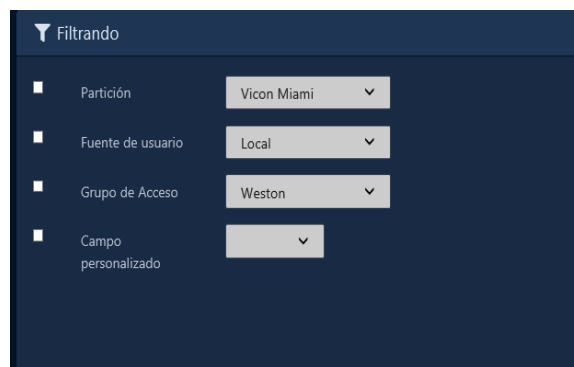
2. Una vez en la pantalla **Lista de usuarios**, tendrá 4 secciones para completar.
 - a. Opciones de la **lista de usuarios**: se puede seleccionar información opcional para incluirla en los resultados del informe.

Figura 23.19. Opciones de la lista de usuarios



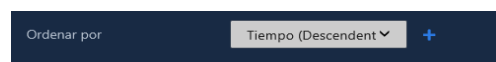
- b. **Filtrado**: Puede filtrar aún más los usuarios que aparecen en los resultados del informe aquí.

Figura 23.20. Filtrado de listas de usuarios

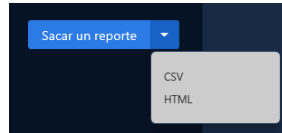


- c. **Clasificación**: puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Nombre, Apellido, Número de tarjeta. Puede ordenar por múltiples factores simultáneamente.

Figura 23.21. Clasificación



- e. **Generar reporte**: elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figura 23.22 Generar reporte

- b. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del informe, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

Reporte de Notificaciones

Esta sección cubrirá qué es el Informe de notificaciones y cómo ejecutarlo en VAX.

El informe de notificaciones se utiliza para ver notificaciones anteriores, como la conexión de paneles, la apertura de puertas, el acceso concedido o denegado a los usuarios y muchos otros tipos de notificaciones. Las opciones para exportar el informe también están disponibles.

Utilice los siguientes pasos para ejecutar un informe de notificaciones:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Notificaciones** (en la imagen a continuación).



2. Una vez en la pantalla de **Notificaciones**, tendrá 3 secciones para completar.
 - a. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el informe**.

También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.23. Widget Selector de fecha

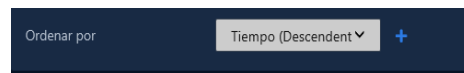
- b. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada.

Figura 23.24. Tipos de notificación



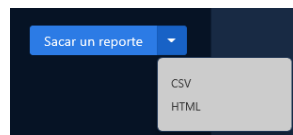
- d. **Clasificación:** puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Nombre, Apellido, Número de tarjeta. Puede ordenar por múltiples factores simultáneamente.

Figura 23.25. Clasificación



- f. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figura 23.26 Generar reporte



- c. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los reportes de notificaciones exportados incluye lo siguiente:

- **Hora:** fecha y hora de la Notificación.
- **Evento:** Tipo de evento de la Notificación.
- **Mensaje:** Mensaje asociado al evento.

Reporte de reunion (Mustering)

Esta sección cubre qué es el reporte Muster y cómo ejecutarlo en VAX.

El reporte Muster obtiene una lista de Usuarios que se encuentran en áreas particulares en función de qué puertas dan acceso a esas áreas. Este reporte requiere que las áreas se configuren en cada sitio y que los campos "Lector 1 otorga acceso al área" y "Lector 2 otorga acceso al área" en la pantalla **Editar puerta** se completen para cualquier puerta en la que exista la necesidad potencial de ejecutar este reporte. Las opciones para exportar el reporte también están disponibles.

Nota

Los administradores que no sean administradores del sistema requerirán que se active el **privilegio de administrador de reportes Muster (reunión)**; solo las Puertas adjuntas a los Paneles en esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Use los siguientes pasos para configurar Áreas y asignarlas a Puertas:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de **Sitios y Áreas** (en la imagen a continuación).



2. En la pantalla **Sitios y áreas**, verá los sitios que haya creado. Haga clic en el botón azul (configuración avanzada) junto al sitio al que desea agregar áreas.
3. En la pantalla Editar sitio, haga clic en la pestaña **Áreas**.
4. En la pestaña **Áreas**, **ingrese un nombre** para su nueva área y haga clic en el botón **Agregar** área en el lado derecho. Agregue áreas adicionales según sea necesario.
5. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono de **Puertas** (en la imagen de abajo).



6. En la pantalla **Puertas**, verá las Puertas que ya ha configurado enumeradas aquí. Haga clic en el botón azul junto a la puerta en la que desea configurar las áreas.
7. En la pantalla **Editar puerta**, verá 5 pestañas. Haga clic en la pestaña **Áreas**. Los elementos de configuración de esta pantalla se explican a continuación.

Figura 23.27. Configuración de área

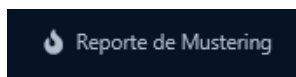
8. **Lector 1 concede acceso al área:** el área a la que el Lector 1 concede acceso. Seleccione un área personalizada o 'Sin área'.

Lector 2 concede acceso al área: el área a la que Lector 2 concede acceso. Seleccione un área personalizada o 'Sin área'. Si no hay Reader 2, aún se debe seleccionar un área.

9. Una vez que configure las áreas en cualquier puerta adicional, debe actualizar los controladores o esperar a que el temporizador de actualización automática los actualice automáticamente.

Utilice los siguientes pasos para ejecutar un reporte de Muster:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono Reporte de Muster (en la imagen a continuación).



2. Una vez en la pantalla Reporte de Muster, tendrá 4 secciones para completar.

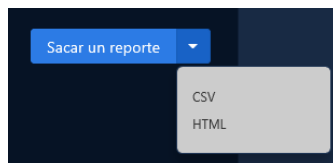
3. **Intervalo de fechas:**

- a. Seleccione la **hora de inicio** en la que le gustaría ejecutar el informe. Aparecerá el widget Selector de fecha. Utilice el **selector de calendario y hora** para seleccionar la fecha y hora para iniciar el reporte. El reporte solicitará datos entre la hora de inicio y la hora actual.
- b. Seleccione la **hora de inicio** para indicar el marco de tiempo para que se ejecute el informe.
- c. Seleccione a qué **zona horaria** se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.
- d. Seleccione la **partición** en la que residen las áreas en las que desea ejecutar el informe.
- e. Seleccione los **sitios** en los que residen las áreas en las que desea ejecutar el informe.

Figura 23.28. Widget selector de fecha

4. **Áreas:** seleccione las áreas en las que desea ejecutar el informe. Puede seleccionar más de uno a la vez, o solo un Área individual. La barra de búsqueda se puede utilizar para encontrar áreas rápidamente. De forma predeterminada, si no se eligen áreas, el informe se ejecutará en todas las áreas de la partición y el sitio seleccionados.
5. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.29. Generar Reporte



6. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en Ejecutar reporte en la parte inferior de la página. Accederás a los resultados del reporte.

La información que se presenta en los informes de actividad de puertas exportados incluye lo siguiente:

- **Áreas:** nombre del área en la que se encuentra actualmente el usuario en función de la última actividad del lector.
- **Usuario:** nombre del Usuario.
- **Lector:** nombre del último Lector al que el Usuario tuvo acceso.
- **Última actividad:** la fecha y la hora de la última actividad conocida que involucró al usuario.

Reportes de Configuración

Los informes de configuración son una serie de informes en VAX que le permiten exportar información del sistema. Esto puede incluir información de red para todos sus paneles, nombres y horarios para todas sus puertas, cómo están configurados sus horarios y mucho más.

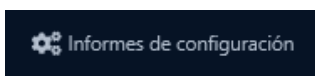
Esta sección cubrirá dónde y cómo ejecutar estos informes y alguna información sobre cada informe de configuración individual.

Nota

Solo las cuentas de administrador con el privilegio de configuración de reportes tendrán acceso para ejecutar este reporte. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para ejecutar cualquiera de los informes de configuración:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el icono **reportes de configuración** (en la imagen a continuación).



2. Una vez en la pantalla **Reporte de configuración**, elegirá en qué partición le gustaría ejecutar el reporte (puede seleccionar más de 1) y qué tipo de informe le gustaría ejecutar.

La siguiente tabla describe cada uno de los informes de configuración:

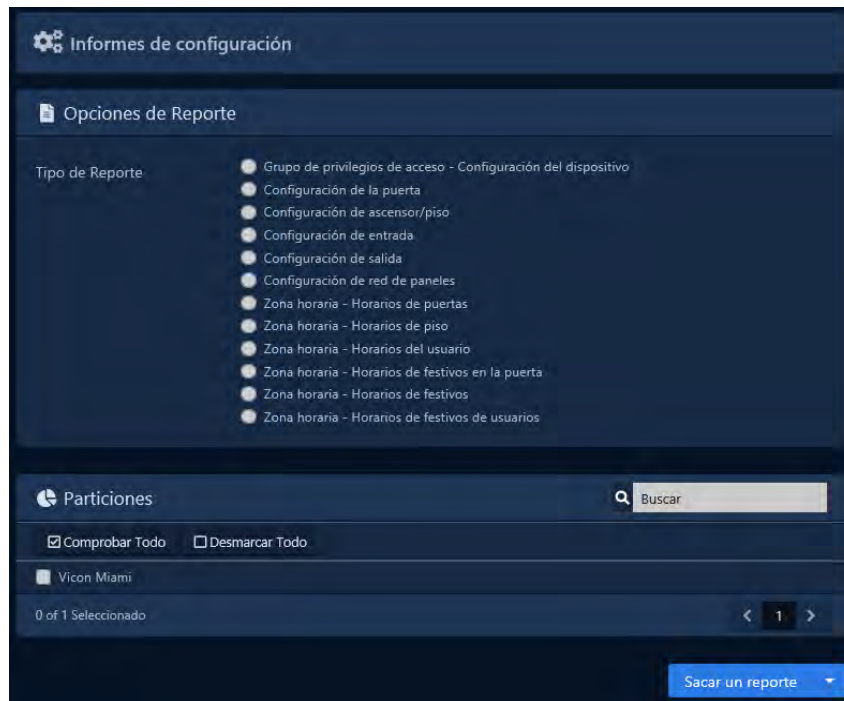
Tabla 23.4. Reportes de Configuración

Reporte	Descripción
Configuración del dispositivo del grupo de privilegios de acceso	Crearé una lista exportable de todos los Grupos de Privilegios de Acceso en las Particiones seleccionadas, junto con los Lectores o pisos de Elevador en cada grupo y el nombre del Horario de Usuario asociado con cada Lector/Piso.
Configuración de la puerta	Crearé una lista exportable de todas las puertas en las particiones seleccionadas junto con el nombre del cronograma de puertas y el grupo de días festivos que usa cada puerta. Incluye los nombres de los lectores asociados con cada puerta y el nombre del controlador de puerta al que está conectada cada puerta
Configuración de ascensor/piso	Crearé una lista exportable de todos los pisos de ascensores en las particiones seleccionadas junto con el nombre del cronograma de piso y el grupo de días festivos que usa cada puerta. Incluye los nombres de los Lectores asociados con cada Ascensor y el nombre del Panel de Ascensor al que está conectado cada Ascensor.
Configuración de entrada	Crearé una lista exportable de todas las Entradas adjuntas a todos los Paneles en las Particiones seleccionadas, incluidos los Paneles de puerta y las Tarjetas IO. Enumerará el uso de la función de entrada, el nombre, los horarios de entrada, los grupos de días festivos y las acciones para las entradas de la placa E/S.
Configuración de salida	Crearé una lista exportable de todas las Salidas adjuntas a todos los Paneles en las Particiones seleccionadas, incluidos los Paneles de Puerta y las Placas IO. Enumerará la función de salida, el nombre, el programa de salida en los tableros IO y los grupos de vacaciones.
Configuración de red de paneles	Crearé una lista exportable de todos los Paneles en las Particiones seleccionadas junto con su configuración de red y el nombre del modelo, que incluye: Modo de conexión, Dirección IP, Máscara de subred, Puerta de enlace y DNS
Horario - Horarios de puerta	Crearé una lista exportable de todos los Horarios de Puertas en las Particiones seleccionadas junto con los intervalos de tiempo configurados y los modos asociados para cada día de la semana.
Horario - Horarios de piso	Crearé una lista exportable de todos los cronogramas de piso en las particiones seleccionadas junto con los períodos de tiempo configurados y los modos asociados para cada día de la semana

Reportes

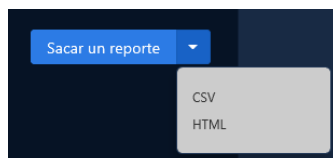
Reporte	Descripción
Horario - Horarios de usuario	Crear una lista exportable de todos los horarios de usuario en las particiones seleccionadas junto con los períodos de tiempo configurados y los modos asociados para cada día de la semana.
Horario - Horarios de puerta Festivos	Crear una lista exportable de todos los calendarios de puertas de vacaciones en las particiones seleccionadas junto con los intervalos de tiempo configurados y los modos asociados para cada día de la semana.
Horario - Horarios de piso de festivos	Crear una lista exportable de todos los horarios de pisos de festivos en las particiones seleccionadas junto con los períodos de tiempo configurados y los modos asociados para cada día de la semana.
Horario - Horarios de usuario de festivos	Crear una lista exportable de todos los calendarios de usuarios de días festivos en las particiones seleccionadas junto con los períodos de tiempo configurados y los modos asociados para cada día de la semana.

Figura 23.30. Pantalla de reportes de configuración



- 3. Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.


Figure 23.31. Generar Reporte



- 4.** Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a **Parámetros** haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón **Actualizar**. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



 **Nota:** Según el tamaño del reporte, puede tardar varios minutos en generarse

Actividad de entrada

Esta sección cubre qué es el reporte de actividad de entrada y cómo ejecutarlo en VAX.

El reporte de actividad de entrada se utiliza para realizar un seguimiento de las actividades de las entradas auxiliares en VAX. Este informe le permite ver cuándo cambiaron de estado entradas específicas, incluidas las entradas auxiliares en los paneles de puerta y los paneles E/S. Las opciones para exportar el informe también están disponibles.

Nota

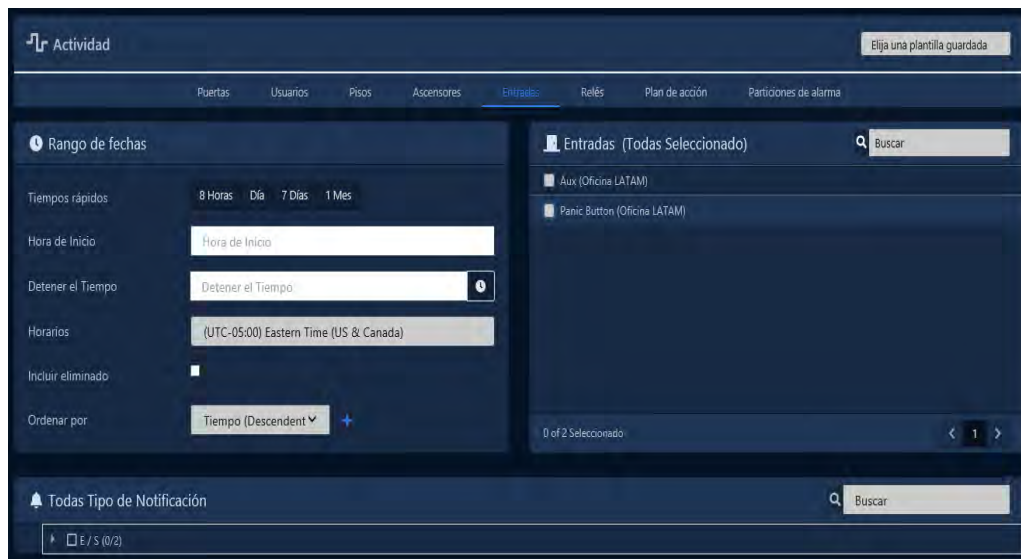
Los administradores que no sean administradores del sistema requerirán que **el privilegio de administrador para reportes de actividad de entrada** esté activado; solo las Entradas adjuntas a los Paneles en esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para ejecutar un informe de actividad de entrada:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



2. Seleccione **Entradas** de la lista de opciones en la parte superior de la página Actividad.



3. Una vez en la pantalla **Actividad de entrada**, tendrá 5 secciones para completar.

- a. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el informe**.

También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.32 Widget selector de fecha

- b. **Entradas:** seleccione las entradas con las que desea ejecutar el reporte. Puede seleccionar más de uno a la vez, o solo una entrada individual. La barra de búsqueda se puede utilizar para encontrar **Entradas** rápidamente.
- c. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar el estado de entrada cambiado y varios otros filtros.

Figura 23.33. Tipos de notificación

- d. **Clasificación:** puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.34. Clasificación


- e. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.35. Generar Reporte

- f. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.


Si desea cambiar los parámetros del reporte, puede volver a **Parámetros** haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón **Actualizar**. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



 **Nota:** Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los informes de actividad de entrada exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Entrada:** nombre de la Entrada con la que está asociado el evento.
- **Mensaje:** información adicional sobre el evento, como "La entrada 1 de informes de la placa de E/S cambió a desactivada".

 **Nota:** Solo las entradas definidas como "Entrada auxiliar" aparecerán en la lista de entradas seleccionables.

Actividad de salidas

Esta sección cubre qué es el reporte de actividad de salida y cómo ejecutarlo en VAX.

El reporte de actividad de salida se utiliza para realizar un seguimiento de las actividades de las salidas auxiliares en VAX. Este reporte le permite ver cuándo cambiaron de estado las salidas específicas, incluidas las salidas auxiliares en los paneles de puerta y los paneles de E/S. Las opciones para exportar el reporte también están disponibles.

Nota

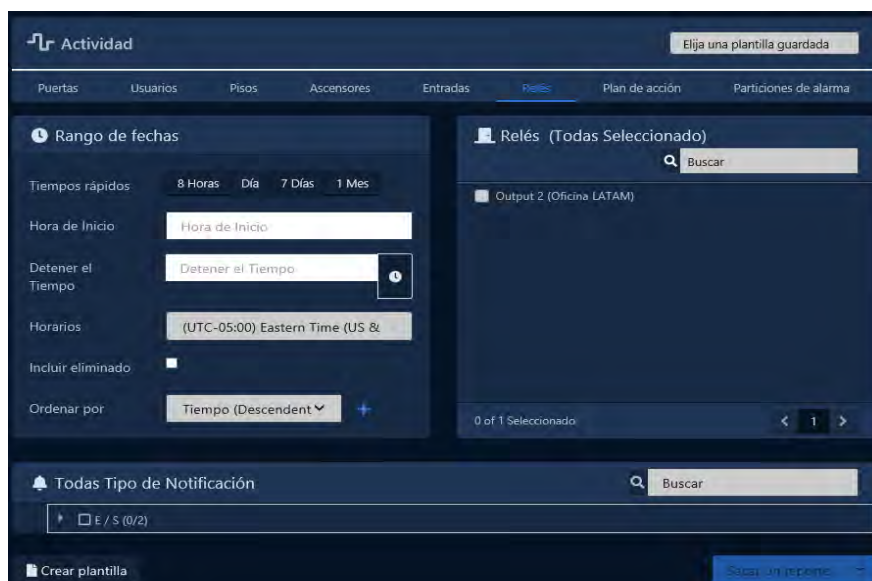
Los administradores que no sean administradores del sistema requerirán que se active el **privilegio de administrador de reportes de actividad de salida**; solo las Salidas adjuntas a los Paneles en esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para ejecutar un reporte de actividad de salida:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **reportes**; haga clic en el ícono de **Actividad** (en la imagen a continuación).



2. Seleccione **Salidas** de la lista de opciones en la parte superior de la página Actividad.



3. Una vez en la pantalla Actividad de salida, tendrá 5 secciones para completar.

- a. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el informe**.

También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.36. Widget selector de fecha



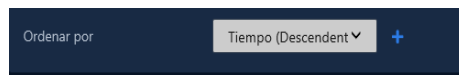
- b. **Salidas:** seleccione las salidas con las que desea ejecutar el informe. Puede seleccionar más de una a la vez, o solo una salida individual. La barra de búsqueda se puede utilizar para encontrar Salidas rápidamente.
- c. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar Cambio de estado de salida, Cambio de programa de salida y varios otros filtros.

Figure 23.37. Tipos de notificación



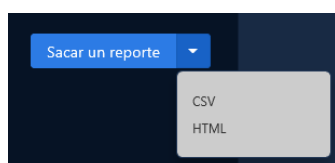
- a. **Clasificación:** puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.38. Clasificación



- b. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.39. Generar Reporte



- c. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en **Ejecutar reporte** en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los informes de actividad de salida exportada incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Salida:** nombre de la Salida con la que está asociado el evento.
- **Mensaje:** información adicional sobre el evento, como "La salida 1 de los informes de la placa de E/S cambió a desactivada"

Nota: Solo las salidas definidas como "Salida auxiliar" aparecerán en la lista de salidas seleccionables.

Actividad del plan de acción

Esta sección cubre qué es el Informe de actividad del plan de acción y cómo ejecutarlo en VAX.

El Informe de actividad del plan de acción se utiliza para ver las notificaciones generadas por los planes de acción utilizados por ACE. Las opciones para exportar el reporte también están disponibles.

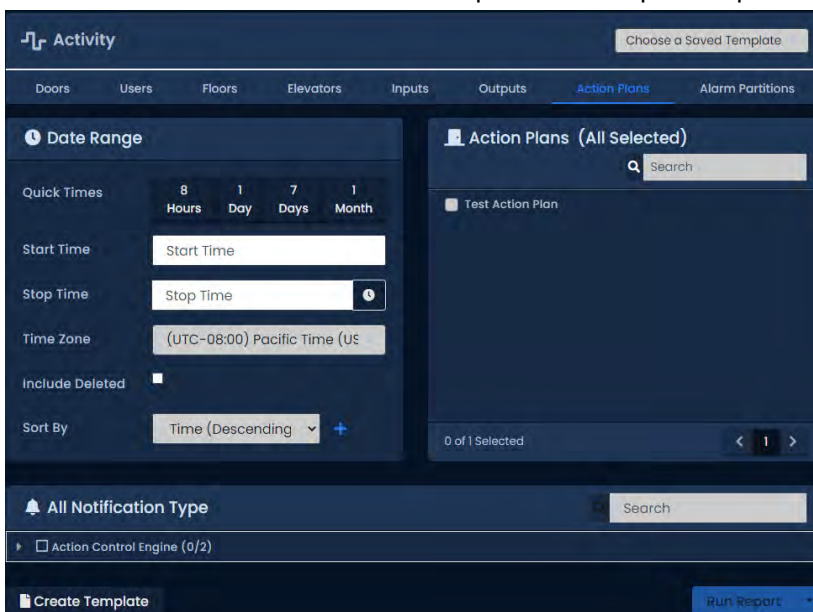
Nota: Solo los administradores que son administradores del sistema pueden ejecutar este informe.

Utilice los siguientes pasos para ejecutar un reporte de actividad del plan de acción:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **reportes**; haga clic en el icono de **Actividad** (en la imagen a continuación).



2. Seleccione **Planes de acción** de la lista de opciones en la parte superior de la página **Actividad**.



3. Una vez en la pantalla **Actividad del plan de acción**, tendrá 5 secciones para completar.

- a. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el informe**.

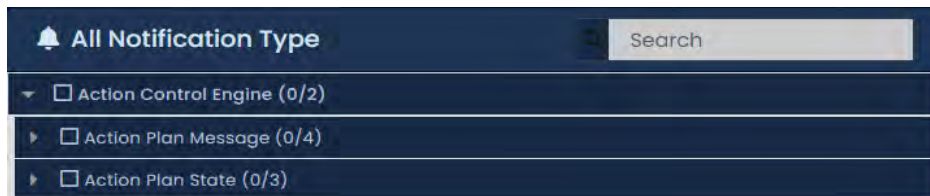
También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.40. Widget selector de fecha



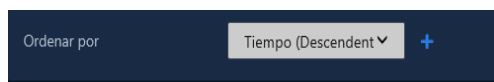
- a. **Planes de acción:** seleccione los planes de acción con los que desea ejecutar el informe. Puede seleccionar más de uno a la vez, o solo un plan de acción individual. La barra de búsqueda se puede utilizar para encontrar planes de acción rápidamente. Todos están seleccionados por defecto
- b. **Tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada. Puede filtrar el estado del plan de acción cambiado y varios otros filtros.

Figure 23.41. Tipos de notificación



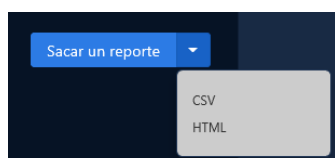
4. **Clasificación:** puede configurar cómo se ordenarán los resultados del informe. El valor predeterminado es Tiempo descendente. Puede ordenar por múltiples factores simultáneamente.

Figura 23.38. Clasificación



5. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.39. Generar Reporte



6. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en Ejecutar reporte en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

La información que se presenta en los informes de actividad del plan de acción exportados incluye lo siguiente:

- **Hora:** fecha y hora del evento.
- **Plan de Acción:** nombre del Plan de Acción al que está asociado el evento.
- **Mensaje:** información adicional sobre el evento, como el contenido de un mensaje de acción de registro.

Seguimiento del tiempo

Esta sección cubre qué es el reporte de seguimiento de tiempo y cómo ejecutarlo en VAX.

El reporte de seguimiento de tiempo se usa para rastrear cuánto tiempo los usuarios están en un área según las credenciales de usuario que se usan en lectores específicos. Esta información se puede utilizar para la nómina y otros fines. Las opciones para exportar el reporte también están disponibles.

Nota

Los administradores que no sean administradores del sistema requerirán que el privilegio de **administrador de reporte de seguimiento de tiempo del usuario** esté activado; solo los Usuarios que son miembros de esa Partición serán visibles para el Administrador. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Para utilizar correctamente el seguimiento de tiempo, asegúrese de que haya dos lectores de credenciales ubicados de tal manera que los usuarios puedan presentar sus credenciales (tarjetas, fobs, PIN) al entrar o salir de las instalaciones. Esto es importante si planea usar el reporte de seguimiento de tiempo para fines de nómina.

Utilice los siguientes pasos para ejecutar un informe de seguimiento de tiempo:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada Reportes; haga clic en el icono de **seguimiento de tiempo** (en la imagen de abajo).

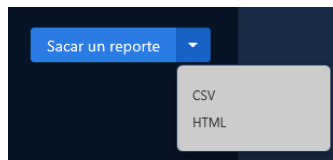


2. Una vez en la pantalla de **seguimiento de tiempo**, tendrá 4 secciones para completar.
 - a. **Los reportes guardados (plantillas):** la configuración del reporte se puede guardar y recuperar desde este menú desplegable. Esto puede ahorrarle tener que volver a seleccionar opciones al ejecutar un reporte. Deje en blanco o seleccione una plantilla guardada.
 - b. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el reporte**.

Figura 23.44. Widget selector de fecha

- c. **En Lectores:** Seleccione uno o más lectores de la lista. Se hará referencia a los lectores seleccionados para rastrear el tiempo de entrada de cualquier usuario al que se le haya otorgado acceso.
- d. **Lectores salientes:** Seleccione uno o más lectores de la lista. Se hará referencia a los lectores seleccionados para rastrear el tiempo de salida de cualquier usuario al que se le haya otorgado acceso.
3. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.45. Generar Reporte



- Una vez que haya completado los campos obligatorios, ahora puede hacer clic en Ejecutar reporte en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota: Según el tamaño del reporte, puede tardar varios minutos en generarse.

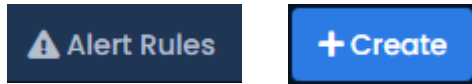
Actividad de alertas


Actividad de alerta se utiliza para rastrear la actividad de alertas del sistema en VAX. Este reporte proporcionará al administrador una lista de mensajes con fechas que reflejan las reglas de notificación de alertas que se establecieron antes del evento de alerta. Se pueden agregar mensajes a las alertas para reconocimiento y registros personales del administrador.

Nota

Los administradores que no sean administradores del sistema requerirán que se active el **privilegio de administrador de reporte de actividad de alerta**. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*.

Utilice los siguientes pasos para configurar una regla de notificación de actividad de alerta:

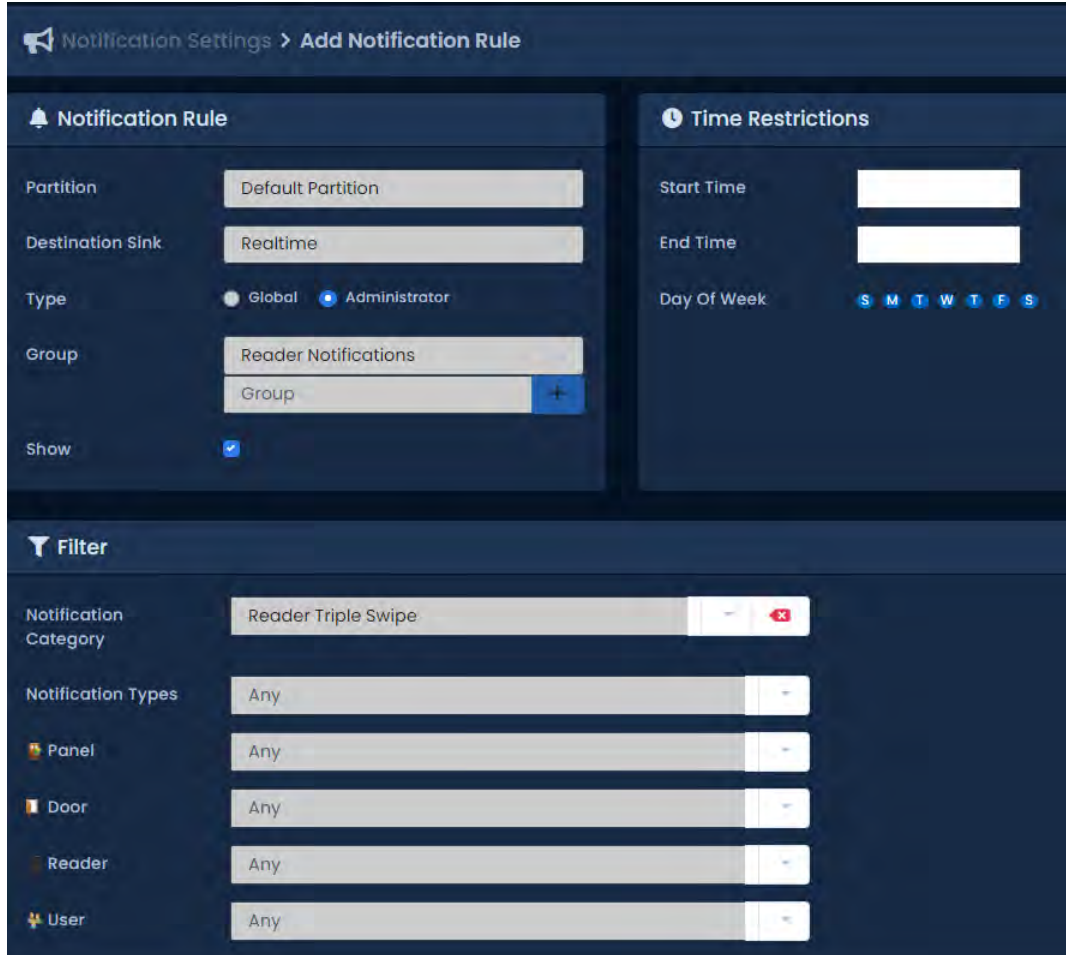



 **Nota:** Actividad de alerta solo se completará después de que se creen las reglas de notificación de alerta.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el ícono de **Configuración de notificaciones** (en la imagen a continuación).



2. En la parte superior de la página habrá 5 opciones de configuración para elegir. Seleccione **Reglas de alerta** (en la imagen a continuación).
3. Seleccione el botón **+** para agregar una nueva regla.
4. Una vez en la pantalla **Agregar regla de alerta**, es necesario completar la sección **Regla de alerta** y la sección **Reconocimientos**. Las secciones Regla y Restricciones de tiempo se pueden completar según sea necesario.



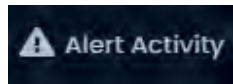
 **Nota :** Se pueden crear reconocimientos múltiples seleccionando el botón + Nuevo reconocimiento. Cada reconocimiento tendrá la opción de seleccionar: Cualquiera, Grupo, Administrador y si se requiere un supervisor.

5. Una vez completadas todas las secciones, se puede crear la regla seleccionando **+ botón + Crear**.

Utilice los siguientes pasos para ejecutar un informe de actividad de alerta:

Una vez en la pantalla **Actividad de alerta**, tendrá 3 secciones para completar.

- a. En la barra lateral, desplácese hacia abajo hasta la sección titulada **Reportes**; haga clic en el icono de **actividad de alerta** (en la imagen de abajo).

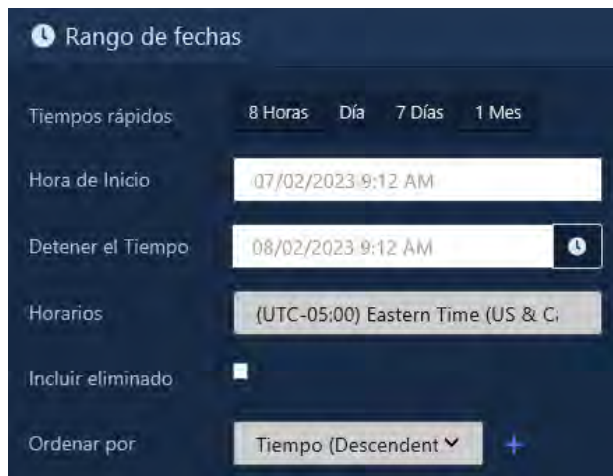


La información que se enumera en un informe generado es la siguiente:

- **Fecha:** fecha y hora de la Alerta.
 - **Mensaje:** notificación inicial junto con el mensaje de reconocimiento.
- b. **Intervalo de fechas:** seleccione la **hora de inicio** y la **hora de finalización** con las que desea ejecutar el **reporte**. Aparecerá el widget Selector de fecha. Utilice el selector de calendario y hora para **seleccionar la fecha y hora para iniciar/detener el reporte**.

También puede seleccionar a qué zona horaria se convertirá el informe exportado. Esto es útil cuando partes de su implementación están en diferentes zonas horarias.

Figura 23.46. Widget Selector de fechas


 A dark blue widget titled "Rango de fechas" (Date Range). It features several controls:

- Tiempos rápidos:** Four buttons labeled "8 Horas", "Día", "7 Días", and "1 Mes".
- Hora de Inicio:** A text input field containing "07/02/2023 9:12 AM".
- Detener el Tiempo:** A text input field containing "08/02/2023 9:12 AM" with a small clock icon to its right.
- Horarios:** A dropdown menu showing "(UTC-05:00) Eastern Time (US & C)".
- Incluir eliminado:** A checkbox that is currently unchecked.
- Ordenar por:** A dropdown menu showing "Tiempo (Descendent)" with a plus sign to its right.

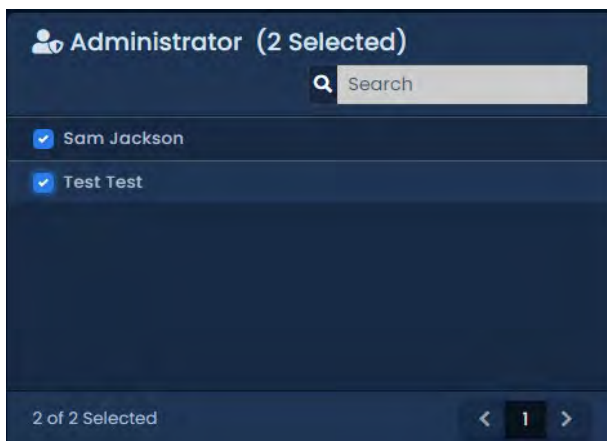
6. **Todos los tipos de notificación:** puede filtrar qué notificaciones aparecen en el informe en esta sección. Todos los tipos de notificación se seleccionan de forma predeterminada.

Figura 23.47. Todos los tipos de notificación



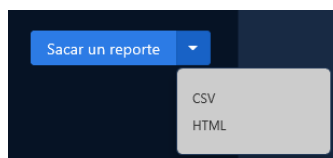
7. **Administradores:** Puede seleccionar qué administrador inició sesión para el informe. Todos están seleccionados por defecto

Figura 23.48. Administradores:



8. **Generar reporte:** elija el formato de salida del reporte de la lista desplegable **Ejecutar reporte**. En línea (resultados que se muestran en el navegador web) es el valor predeterminado. CSV y HTML también se pueden seleccionar.

Figure 23.49. Generar Reporte



9. Una vez que haya completado los campos obligatorios, ahora puede hacer clic en Ejecutar reporte en la parte inferior de la página. Accederás a los resultados del reporte.

Si desea cambiar los parámetros del reporte, puede volver a Parámetros haciendo clic en el icono de engranaje. Puede actualizar los resultados del reporte con el botón Actualizar. Puede exportar el reporte de los resultados en línea usando el botón de exportación.



Nota:

Se pueden ver los acuses de recibo y se puede crear un mensaje en la pantalla de Alertas seleccionando el ícono de Alertas en la parte superior de la escena VAX. (en la imagen a continuación)



Particiones de Alarmas

La actividad de las particiones de alarma se utiliza para rastrear el sistema de alarma que está integrado en VAX

Nota

Solo las cuentas de administrador con el privilegio de configuración de informes tendrán acceso para ejecutar este informe. Para obtener más información sobre los privilegios de administrador, consulte el *Capítulo 20, Administradores y privilegios*

Capítulo 24. Notificaciones

Los dispositivos en VAX como Paneles, Puertas o Lectores generan notificaciones sobre varios cambios de estado y acciones que ocurren. Las notificaciones se envían en tiempo real desde el panel al servidor. Los paneles fuera de línea almacenarán hasta 50,000 eventos, y se eliminarán por orden de entrada una vez que estén llenos. VAX procesa cada notificación a través de una serie de reglas para que cada destino la acepte o la rechace. Las notificaciones se pueden configurar para que se muestren en tiempo real en la interfaz web, se envíen por correo electrónico a los administradores, se envíen a los dispositivos mediante Web Push y se almacenen en la base de datos para generar reportes

Destinos

Hay cuatro destinos que aceptan notificaciones: tiempo real, correo electrónico, Web Push y base de datos. Cada destino tiene su propio conjunto de reglas que determinan si una notificación será aceptada o rechazada.

Tiempo Real:

En la interfaz web de VAX, a los administradores se les muestran notificaciones en tiempo real a medida que se reciben. Dependiendo del tamaño de la pantalla, se muestran en la barra lateral derecha, desde un menú desplegable en la parte superior de la página o en una página dedicada en el móvil. La pantalla de monitoreo proporciona una vista de pantalla completa de las notificaciones en tiempo real, lo que permite una fácil verificación fotográfica en las estaciones de guardia o en los mostradores de conserjería

Email

Cuando VAX recibe una notificación, se puede configurar para enviar esa notificación en un correo electrónico a todos o a administradores específicos. Se envía un único correo electrónico por notificación, y cada destinatario se dirige mediante BCC (copia oculta). Un ejemplo del correo electrónico enviado se muestra a continuación.

Web Push

Web Push le permite a VAX enviar notificaciones a su navegador web, incluso cuando no está enfocado o incluso abierto en el navegador. Web Push requiere confirmación en el navegador para permitir que el permiso VAX envíe notificaciones automáticas. VAX encripta la notificación y la envía a un servidor push del fabricante del navegador (Google, Mozilla, Microsoft). El servidor push envía la notificación al navegador, que muestra la notificación. La notificación aparece en el sistema o en la bandeja de notificaciones del navegador según el dispositivo y el navegador.

Prerequisitos

Web Push requiere un certificado SSL válido para funcionar; Los certificados autofirmados solo son compatibles con Firefox. Los siguientes navegadores web actualmente son compatibles con Web Push:

Tabla 24.1. Navegadores compatibles

Navegador	Versión mínima
Windows	
Chrome	Versión 50 o superior
Firefox	Versión 44 o superior
Edge	Versión 17 o superior
Opera	Versión 42 o superior
Mac/Linux	
Chrome	Versión 50 o superior

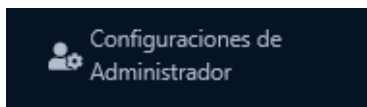
Android	
Chrome	Versión 81 o superior
Firefox	Versión 68 o superior

Suscripción a Web Push

Los administradores pueden suscribirse a uno o más navegadores web para recibir notificaciones Web Push en la pestaña Web Push de la página Configuración del administrador.

Para suscribir un navegador web para recibir notificaciones automáticas:

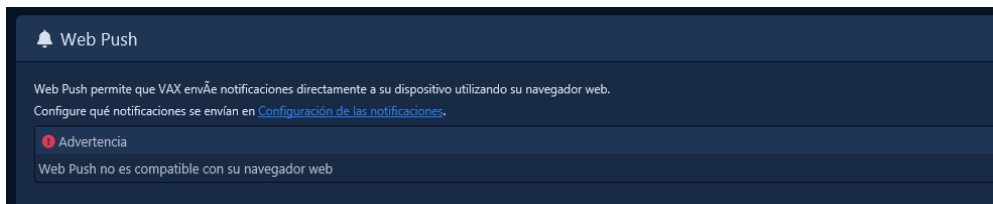
1. Abra **Configuración del administrador** en la sección Sistema de la página de inicio.



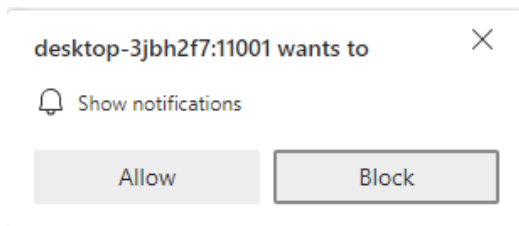
2. Abra la pestaña **Web Push** en la parte superior de la página.



3. Puede ingresar un **nombre de dispositivo** para ayudar a identificar las suscripciones del navegador en la lista a continuación.



4. Clic **Suscribir**
5. El navegador le pedirá que permita que VAX envíe notificaciones automáticas.



6. Una vez permitidas, sus suscripciones se agregarán a la lista a continuación y en su lugar aparecerá una opción para cancelar la suscripción.

Base de datos

Cuando VAX recibe una notificación, por defecto almacenará todos los tipos de notificación excepto los errores de credencial de lector en la base de datos para permitir informes históricos.

Página de configuración de notificaciones

La página **Configuración de notificaciones** le permite administrar las reglas que deciden dónde se envían, almacenan y diseñan las notificaciones. Los administradores requieren el permiso Administrar reglas de notificación para ver esta sección. Agregar o editar reglas globales requiere permiso de administrador del sistema.

Reglas de notificación

Every notification is processed against a list of Notification Rules for each destination. The first rule that matches the notification for each destination determines whether the destination should accept or reject the notification.

Destinos

En VAX, las notificaciones se pueden enviar o almacenar a diferentes destinos. Cada destino tiene su propio conjunto de reglas que decide si acepta o rechaza cada notificación.

- **Tiempo real:** se muestra en tiempo real en la interfaz web.
- **Email:** Enviado por correo electrónico a todos los administradores en específicos.
- **Web Push:** enviado a los navegadores de todos o de administradores específicos.
- **Base de datos:** Almacenado en la base de datos para reportes históricos.

Tipos

Las reglas de notificación se pueden aplicar a todos los administradores de la partición o a un administrador específico.

- **Global:** la regla se aplica a todos los administradores de la partición.
- **Administrador:** la regla se aplica al administrador específico que creó la regla.

Las reglas de tipo de administrador tienen mayor prioridad y se procesan antes que cualquier regla de tipo global.

Nota:

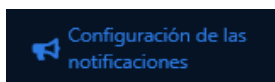
Esto no se aplica a las reglas de la base de datos, que siempre son globales.

Grupos

Las reglas de notificación para el destino en tiempo real se pueden anular mediante grupos de reglas. Los grupos de reglas se pueden seleccionar en la barra lateral de notificaciones y en la página Monitoreo de alertas. Una vez seleccionadas, las notificaciones nuevas se procesan según las reglas del grupo para determinar si se mostrarán en esa página.

Acceso a la pantalla de configuración de notificaciones

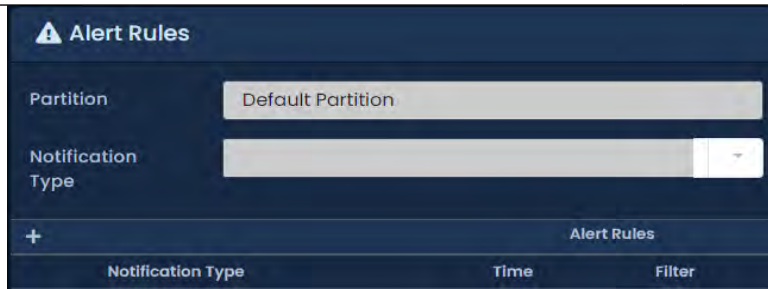
En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de **Configuración de notificaciones** (en la imagen a continuación).



Hay tres secciones en la página Configuración de notificaciones:

- **Reglas:** Lista de reglas para cada destino.
- **Estilos:** Reglas que personalizan sonido, color e imagen en las notificaciones en tiempo real.
- **Live Camera:** Rules that determine whether live camera stream should be shown.

Las opciones **Partición y Tipo de notificación** le permiten seleccionar un tipo de notificación que se mostrará y de qué partición. Con el Tipo de notificación en blanco, se mostrarán todas las notificaciones. (en la foto de abajo)



Lista de reglas

En la sección Reglas, hay una lista de reglas para cada destino de una notificación. Cada lista de reglas se muestra en el orden en que se procesan. La prioridad de la regla se puede cambiar haciendo clic y arrastrando una regla encima o debajo de otra regla.

Nota: Las reglas de administrador siempre tendrán mayor prioridad que las reglas globales y no se pueden reordenar debajo de las reglas globales y viceversa.

Creación de una regla de notificación

1. Use el botón **+ Agregar** (que se muestra a continuación) junto al destino que desea crear. Las opciones disponibles son **Tiempo real**, **Correo electrónico**, **Web Push** y **Base de datos**. Esto lo llevará a la pantalla **Agregar regla de notificación**.

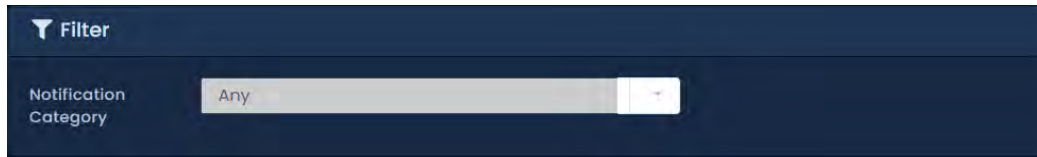


2. La **partición** y la **partición y receptor de data** ya deberían estar seleccionados según la pantalla anterior. Una regla debe estar asociada a una **Partición** y un **Destino**.
3. Elija si la nueva regla afectará a todos los Administradores en la Partición (Global) o al Administrador específico que agrega la regla (el Administrador)

Nota: Solo los administradores del sistema pueden crear reglas globales.

4. Para las reglas en tiempo real, se puede seleccionar o crear un **grupo**. Se pueden seleccionar grupos para filtrar las notificaciones que se muestran en la interfaz en tiempo real.
5. El campo Aceptar decide si esta regla debe permitir el envío de la notificación al Destino o si debe rechazarla. Desmarcar Aceptar significará que el destino no recibirá la notificación si coincide.

6. Las reglas de notificación pueden especificar determinadas notificaciones o dispositivos para que coincidan. De manera predeterminada, se aplicará una regla a todas las notificaciones, a menos que se especifique un filtro. Una **categoría de notificación** se puede seleccionar en el menú desplegable. Cuando se selecciona una categoría de notificación, pueden aparecer opciones de filtro adicionales para limitar aún más la regla.



7. Se pueden implementar restricciones de tiempo para restringir cuándo debe estar activa la regla. La regla solo coincidirá con las notificaciones que ocurran dentro del marco de tiempo especificado.



8. Seleccione Guardar para guardar su configuración. Ahora podrá ver su **regla de notificación** en la pantalla **Configuración de notificaciones**. La nueva regla se aplicará de inmediato a todas las notificaciones posteriores que se reciban. Las notificaciones anteriores no se verán afectadas por la nueva regla.

Estilos de notificación

Los estilos de notificación cambian la forma en que aparecen las notificaciones en las páginas Notificaciones de la barra lateral y Supervisión de alertas. Los estilos pueden cambiar varios aspectos de una notificación, incluidos:

- **Color de fondo:** cambie el color de fondo de la notificación.
- **Sonido de notificación:** cargue un MP3 para que se reproduzca cuando ocurra una notificación.
- **Imagen de notificación:** cargue una imagen para que se muestre cuando ocurra una notificación.

Los estilos de notificación son de tipo global o de administrador. Esto define si el estilo debe aplicarse globalmente a todos los administradores o específicamente al administrador que creó el estilo. Los estilos de administrador siempre tendrán prioridad sobre los estilos globales. Los estilos globales solo pueden ser agregados/editados por los administradores del sistema.

Por defecto, hay 3 tipos de Notificaciones:

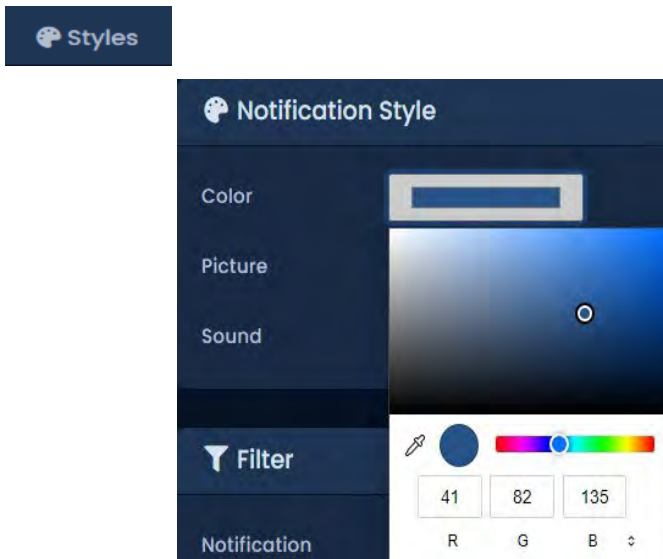
- **Neutral (azul):** Notificaciones que no son positivas ni negativas. Esto incluye inicios de sesión del panel, cambio de estado de entradas y salidas y más.
- **Positivo (verde):** Notificaciones que son positivas. Esto incluye los mensajes de acceso concedido para los usuarios.
- **Alertas (rojo):** Notificaciones que son negativas. Esto incluye apertura forzada de la puerta, activación del sensor de sabotaje y desconexiones del panel. Cualquier tipo de notificación puede convertirse en una alerta.

Creación de una regla de estilo de notificación

1. Use el botón + Agregar (que se muestra a continuación) junto a los tipos **Administrador** o **Global**. Esto lo llevará a la pantalla **Agregar estilo de notificación**.



2. El campo **Partición** se preseleccionará en la página **Configuración de notificaciones**. El campo **Tipo** se preseleccionará según el botón Agregar que se presione.
3. Si desea cambiar el color de fondo de la notificación, elija el color AA seleccionando el cuadro de color o ingresando un código de color HTML. (en la foto de abajo)



4. Si desea cargar una imagen personalizada para mostrarla, haga clic en Elegir archivo y seleccione un archivo PNG, JPG o BMP con un tamaño máximo de 5 MB.
5. Si desea que se reproduzca un sonido cuando se muestra la notificación, haga clic en Seleccionar archivo y seleccione un archivo MP3 con un tamaño máximo de 2 MB.
6. Los estilos de notificación pueden especificar determinadas notificaciones o dispositivos para que coincidan. De forma predeterminada, se aplicará un estilo a todas las notificaciones a menos que se especifique un filtro. Se puede seleccionar una categoría de notificación en el menú desplegable. Cuando se selecciona una categoría de notificación, es posible que aparezcan opciones de filtro adicionales para limitar aún más el estilo.
7. Se pueden implementar restricciones de tiempo para restringir cuándo debe estar activo el estilo. El estilo solo será utilizado por notificaciones que ocurran dentro del marco de tiempo especificado.
8. Seleccione Guardar para guardar su configuración. Ahora podrá ver su estilo de notificación en la pantalla Configuración de notificaciones. El nuevo estilo se aplicará inmediatamente a todas las notificaciones nuevas a medida que se produzcan.

Reglas de la cámara en vivo

Las reglas de cámara en vivo especifican qué notificaciones deben disparar una transmisión de una cámara en vivo en el panel de notificación de la barra lateral y en la página de monitoreo de alerta. La transmisión de una cámara en vivo solo se muestra cuando una regla coincide y el dispositivo que genera la notificación tiene una cámara asociada.

Las reglas de cámara en vivo son de tipo global o de administrador. Esto define si a todos los administradores se les debe mostrar la transmisión de la cámara o si la regla es específica del administrador que creó la regla.

Las reglas del administrador siempre tendrán prioridad sobre las reglas globales.

Crear una regla de cámara en vivo

1. Use el botón + Agregar (que se muestra a continuación) junto a los tipos **Administrador o Global**. Esto lo llevará a la pantalla **Agregar estilo de notificación**.



2. El campo **Partición** se preseleccionará en la página **Configuración de notificaciones**. El campo **Tipo** se preseleccionará según el botón Agregar que se presione.
3. Las reglas de cámara en vivo pueden especificar ciertas notificaciones o dispositivos para que coincidan. De forma predeterminada, la regla se aplicará a todas las notificaciones a menos que se especifique un Filtro. Una **categoría de notificación** se puede seleccionar en el menú desplegable. Cuando se selecciona una categoría de notificación, pueden aparecer opciones de **filtro adicionales** para limitar aún más la regla.
4. Se pueden implementar restricciones de tiempo para restringir cuándo debe estar activo el estilo. El estilo solo será utilizado por notificaciones que ocurran dentro del marco de tiempo especificado.
5. Haga clic en **Guardar** para almacenar la nueva regla de cámara en vivo. La regla se aplicará inmediatamente a todas las nuevas notificaciones entrantes.

Barra de notificaciones

En pantallas de gran tamaño, verá la barra lateral de notificaciones en el lado derecho de la pantalla. La barra lateral de notificaciones muestra las 20 notificaciones más recientes recibidas en tiempo real. Se puede configurar una transmisión de cámara en vivo de la notificación más reciente para que se muestre en la parte superior de la barra lateral.

Figura 24.1. Barra de notificaciones



Consejo

En tamaños de pantalla más pequeños, la barra lateral de notificaciones desaparecerá. Se puede acceder haciendo clic en el icono de flechas en la parte superior de la pantalla, que se muestra a continuación.



Controles de la barra lateral

La barra lateral de notificaciones tiene una fila de botones en la parte superior que permiten un fácil control de la barra lateral.

Figura 24.2. Controles de la barra lateral de notificaciones



Grupos de reglas

El menú desplegable Grupo de reglas permite un filtrado sencillo de las notificaciones en tiempo real. Cuando se selecciona un grupo de reglas, todas las notificaciones posteriores se procesarán a través del grupo de reglas para determinar si deben mostrarse. Los grupos de reglas se pueden configurar en la página Configuración de notificaciones; vea la sección llamada "Grupos" para más detalles. El grupo de reglas seleccionado será recordado por el navegador en las siguientes cargas de página.

Vista de cámara externa

El botón Vista de cámara externa moverá la transmisión de la cámara en vivo desde la parte superior de la barra lateral a su propia página en una ventana nueva. La vista de cámara externa se actualizará a medida que se reciban nuevas notificaciones en la barra lateral. Mientras la vista de cámara externa esté abierta, la barra lateral no mostrará la transmisión de la cámara en la parte superior.

Pausa / Reproducir

El botón Pausa/Reproducir evitará que la barra lateral muestre nuevas notificaciones. La barra lateral se puede reanudar mostrando nuevas notificaciones haciendo clic en el botón Reproducir. Las notificaciones que ocurrieron mientras estaba en pausa no se mostrarán, solo las notificaciones nuevas.

Borrar

El botón Borrar eliminará todas las notificaciones de la barra lateral

Cámara en vivo

Se puede configurar una transmisión de cámara en vivo para que se muestre en la parte superior de la barra lateral cuando ocurren ciertas notificaciones. Las notificaciones de dispositivos como puertas o ascensores que tienen cámaras asociadas mostrarán un ícono de cámara en la notificación que, al hacer clic, **mostrará** un video histórico en una ventana emergente. Una secuencia de cámara se puede mover a su propia ventana haciendo clic en el botón **Vista de cámara externa**. Las reglas para las cuales las notificaciones mostrarán una cámara en vivo se pueden configurar en la página Configuración de notificaciones; *consulte la sección llamada "Reglas de la cámara en vivo" para obtener más detalles.*

Reglas rápidas

Las notificaciones en la barra lateral tienen un botón de engranaje en la esquina inferior izquierda que abre un menú contextual. El menú contextual muestra el tipo de notificación y las opciones para crear rápidamente reglas que afecten las notificaciones futuras.

Cada opción abrirá la página Agregar regla adecuada con la categoría de notificación, la partición, la aceptación y receptor de data (si corresponde) establecidos en función de la notificación y la opción seleccionada de la siguiente manera:

- **Ocultar:** Agregar regla en tiempo real con Aceptar sin marcar.
- **Notificar:** Agregar regla de envío por correo electrónico/web con Aceptar marcado.
- **Mostrar cámara en vivo:** Agregar regla de cámara en vivo.
- **Personalizar:** agregue un estilo de notificación.

Consulte la sección Configuración de notificaciones para obtener más información de cómo agregar reglas

Pantalla de monitoreo

La Pantalla de Monitoreo es una página dedicada en VAX con capacidades de visualización de notificaciones mejoradas. Los guardias y el personal de seguridad suelen utilizar esta página para monitorear tipos específicos de notificaciones o para la verificación de videos/fotos. Esta sección cubrirá dónde encontrar la pantalla de monitoreo y cómo personalizarla.

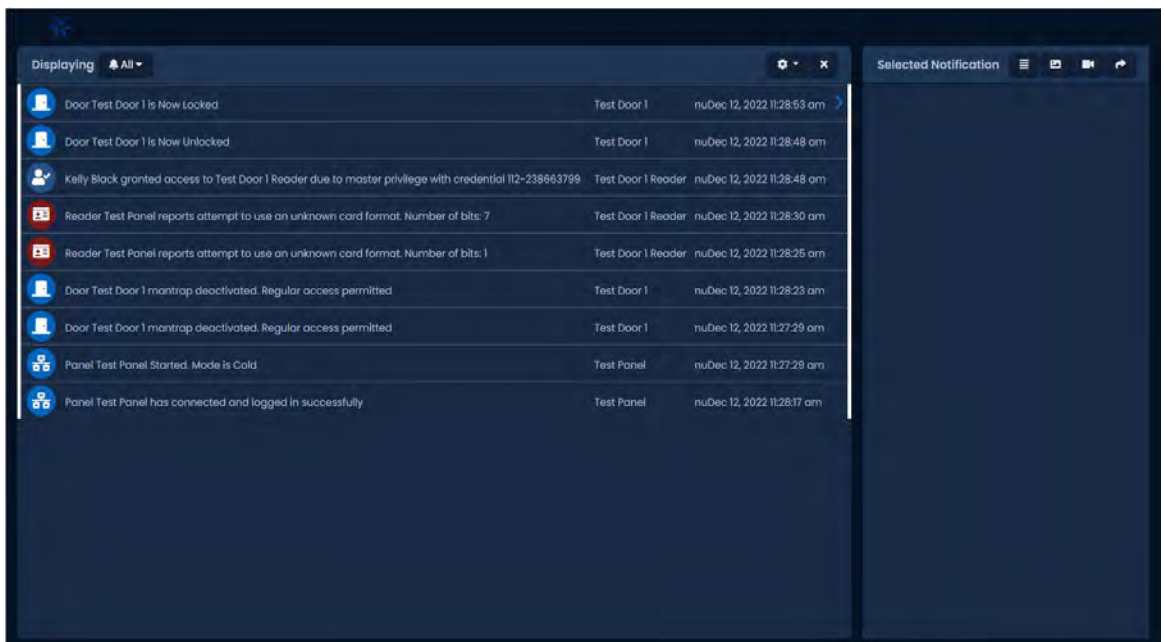
Acceder a la pantalla de monitoreo

1. En la **barra lateral**, desplácese hacia abajo hasta la sección superior titulada **Día a día**; haga clic en el ícono de **Monitoreo** (en la imagen a continuación)).



2. Al hacer clic en el ícono de Monitoreo, se abrirá una ventana/pestaña separada..

Figura 24.3. Pantalla de monitoreo



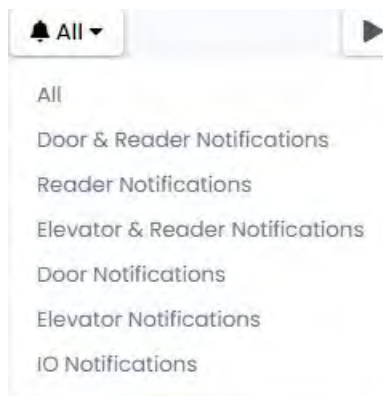
Personalización de las notificaciones mostradas


De manera predeterminada, todas las notificaciones aceptadas por las reglas de notificación en tiempo real aparecerán en la pantalla de monitoreo. Se pueden crear grupos de reglas para cambiar qué notificaciones se mostrarán.

Para cambiar qué tipos de notificaciones apareceran:

1. En la pantalla de monitoreo, haga clic en **"Mostrar: todas las notificaciones"** en el lado izquierdo. Aparecerá un menú desplegable con los grupos de notificación que se han creado en **Configuración de notificaciones**.
2. Seleccione qué grupo de filtros de notificación le gustaría aplicar. Este filtro afectará solo a las notificaciones futuras; no cambiará las notificaciones que se muestran actualmente.

Figura 24.4. Filtros de notificación



 **Nota:** Para agregar grupos de filtros de notificación adicionales, consulte la sección llamada "Grupos".

Opciones de monitoreo

Esta sección explicará las opciones de configuración adicionales que afectan la forma en que se muestran las notificaciones.

En el lado derecho del área de notificación principal hay dos iconos. El basurero borrará la cuadrícula de notificaciones. El otro le mostrará opciones adicionales.

Figura 24.5. Opciones de monitoreo

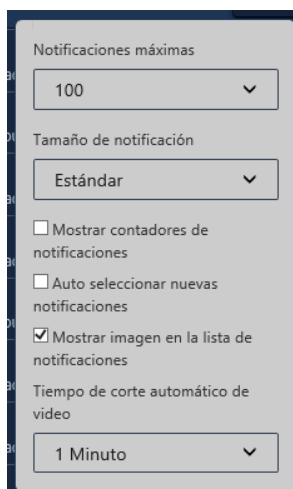
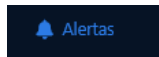


Tabla 24.2. Opciones de monitoreo

Casilla de verificación/menú desplegable	Descripción
Máximo de notificaciones	El número máximo de notificaciones que se pueden mostrar a la vez. Las opciones son 25, 50, 100, 500.
Tamaño de notificación	Cuánto espacio ocupará cada Notificación en el área de Notificación. Las opciones son mosaicos estándar, grandes, horizontales y verticales. Grande puede hacer que sea más fácil de leer. Los mosaicos son mejores cuando necesita la capacidad de revisar rápidamente las imágenes de perfil de muchos usuarios.
Mostrar contadores de notificaciones	Si está marcado, aparecerá un contador de notificaciones sobre el área de notificaciones seleccionadas. Mostrará el total de notificaciones recibidas, el total visto y el total perdido.
Selección automática de nueva notificación	Si está marcada, las nuevas notificaciones se seleccionarán automáticamente.
Mostrar imagen en la lista de notificaciones	Si hay una imagen asociada con una Notificación, se mostrará en el área de Notificación con la notificación.
Tiempo de corte de video automático	Si hay una cámara asociada con una Notificación seleccionada, puede aparecer en el área de Notificación seleccionada. Esta configuración influirá si se reproduce un video histórico o un video en vivo

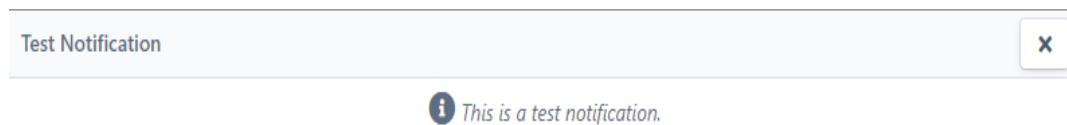
Confirmación de Alerta

Figura 24.6. Icono de alerta



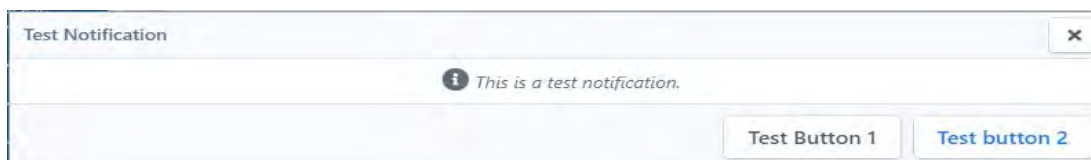
En esta sección se tratará el reconocimiento de alertas. Las alertas se pueden enviar a un administrador con un estado en línea. Las alertas presentarán una ventana con una acción.

Figura 24.7. Icono de Alerta



Si la notificación es producida por un plan de acción, algunas de estas acciones pueden modificarse en el plan de acción relacionado con la notificación. Otras notificaciones se relacionarán con el estado del sistema. Para este tipo de notificación, consulte el *Capítulo 40, Supervisión del funcionamiento* y *Capítulo 42, Supervisión del funcionamiento en VAX*. Puede cerrar una ventana de notificación presionando una acción. El cierre de la ventana también se considerará como un reconocimiento de la alerta sin acción. Al reconocer la acción, la ventana desaparecerá, pero se podrá volver a ver mediante informes.

Figura 24.8. Icono de Alerta



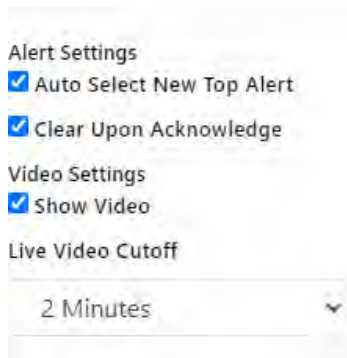
Para navegar a la sección Alerta, desplácese hasta la parte superior de la barra lateral. La sección Alertas mostrará una lista de alertas no reconocidas. Estas alertas se emitieron sin un administrador en línea o no fueron manejadas por un administrador. Haga clic en el icono de engranaje desplegable para ver la configuración de alertas.

Figura 24.9. Icono de Alerta



Aquí puede **alternar Selección automática** de nueva alerta principal, Borrar al confirmar. La configuración de video en el mismo menú desplegable incluye **Mostrar corte de video y video en vivo** con un selector de limitador de tiempo entre 2 y 10 minutos.

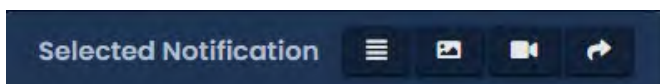
Figura 24.10. Icono de Alerta



Opciones de notificación seleccionadas

La sección Notificación seleccionada está en el lado derecho y mostrará información relevante para la Notificación seleccionada actualmente. Esto puede incluir el dispositivo, el usuario asociado, la credencial, la imagen de perfil o las cámaras asociadas.

Figura 24.11. Opciones de monitoreo



Los siguientes ajustes son muy simples y están activados o desactivados. Cuando una configuración está activada, el icono será blanco. Cuando la configuración está desactivada, el icono será gris. La siguiente tabla explica lo que hace cada configuración.

Tabla 24.3. Monitoring Options

Elemento de configuración	Descripción
	Muestra el mensaje de notificación de la notificación seleccionada cuando está habilitado.
	Muestra la imagen asociada con la Notificación cuando está habilitada (si está disponible).
	Muestra cualquier cámara asociada con la Notificación cuando está habilitada (si está disponible).

Notificaciones



Esta opción alternará las cámaras mostradas para que aparezcan en una ventana separada.

Capítulo 25. Base de Datos

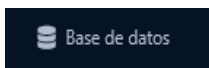
Este capítulo cubrirá las opciones disponibles en la pantalla Base de datos en VAX, Control, específicamente la depuración de Notificaciones y entradas de registros administrativos para reducir el tamaño de la base de datos y conservar el rendimiento. Las configuraciones están disponibles para alertar a los administradores cuando la base de datos alcanza un tamaño determinado.

Depuración de notificaciones

Esta sección cubrirá cómo purgar notificaciones en VAX Access Control. Grandes cantidades de notificaciones a lo largo del tiempo pueden dañar el rendimiento de VAX Access Control, especialmente con implementaciones con cientos de paneles activos y miles de usuarios.

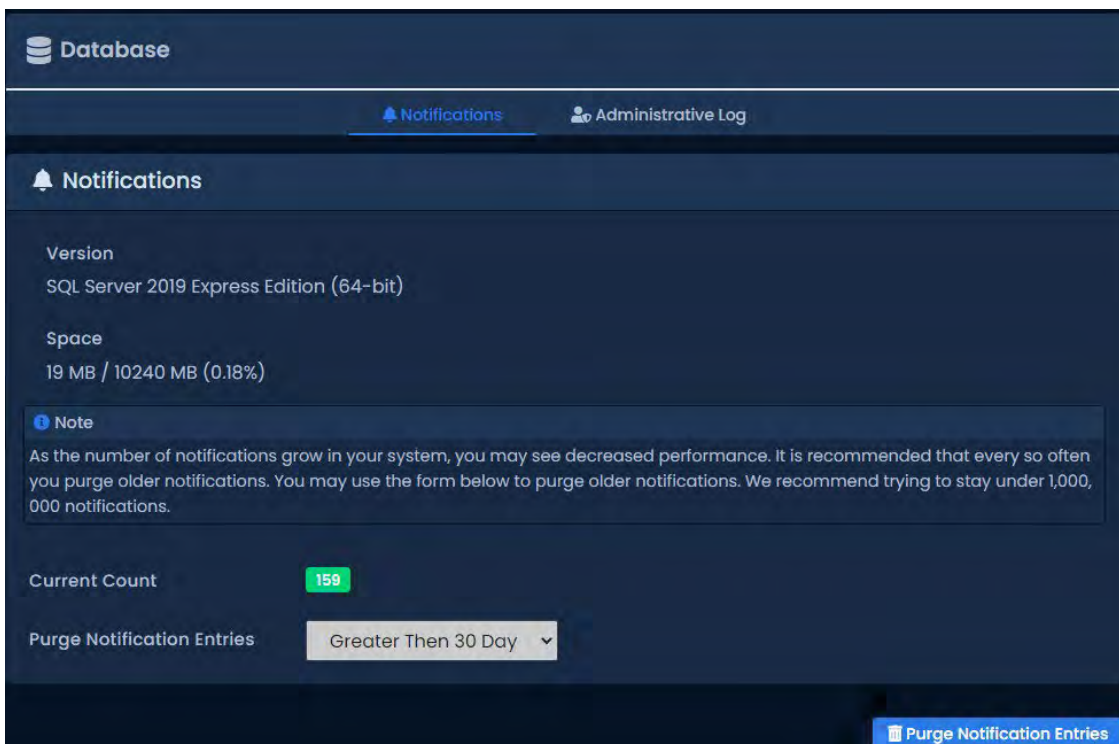
Utilice los siguientes pasos para acceder al formulario de depuración de notificaciones de la base de datos en VAX Access Control:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el icono de la **base de datos** (en la imagen de abajo).



2. Una vez en la pantalla de la **base de datos**, verá la cantidad de notificaciones actualmente en la base de datos.

Figura 25.1. Pantalla de depuración de la base de datos



3. Recomendamos tratar de permanecer por debajo de 1,000,000 de notificaciones. Para implementaciones más pequeñas, esto podría demorar varios años, pero para las más grandes, podría tomar algunos meses.
4. Para depurar las notificaciones, use el menú desplegable **depurar notificaciones** y cambie la antigüedad que deben tener las notificaciones para poder eliminarlas. La fecha va desde Notificaciones con más de 5 años hasta Notificaciones con más de 30 días. También puede seleccionar depurar todas las notificaciones.

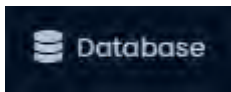
- Una vez que haya hecho su selección, haga clic en el botón **depurar notificaciones** en la parte inferior derecha. Las notificaciones que coincidan con el parámetro de fecha se eliminarán. El conteo actual se actualizará una vez que se complete la depuración.

Depuración del registro de administrador

Esta sección cubrirá cómo depurar las entradas en el registro del administrador en el control de acceso VAX. La mayoría de los cambios en VAX (como agregar un usuario) agregarán una entrada al registro administrativo. Estos registros deben depurarse periódicamente para mantener el rendimiento.

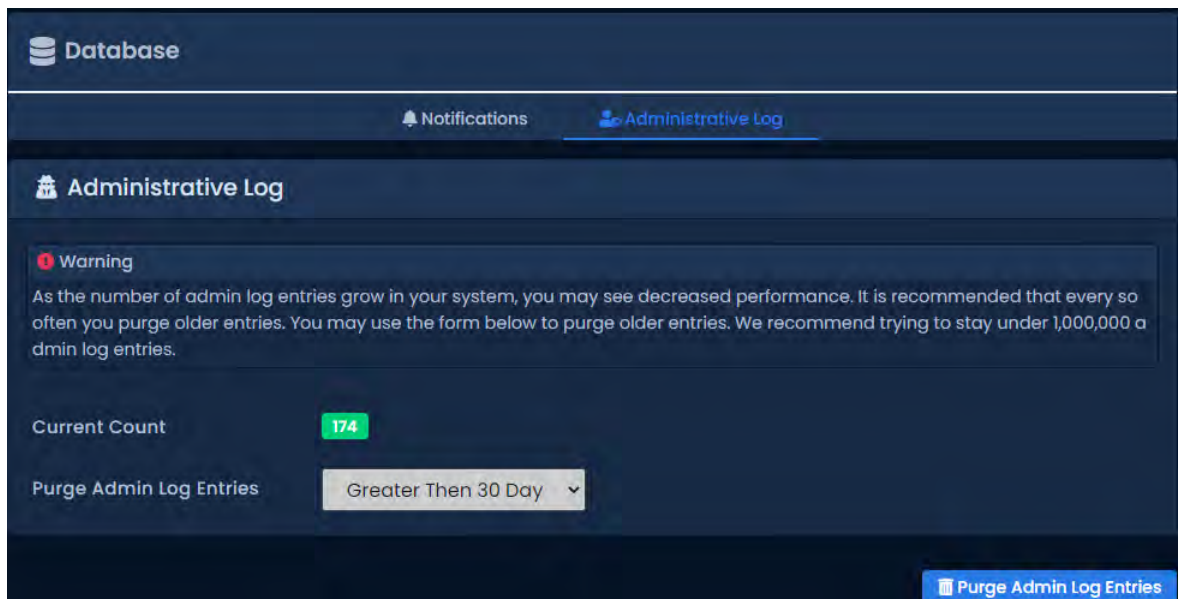
Utilice los siguientes pasos para acceder al formulario de depuración del registro administrativo de la base de datos en el control de acceso VAX:

- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el icono de la **base de datos** (en la imagen de abajo).



- Una vez en la página de la base de datos, haga clic en la pestaña titulada **Registro administrativo**.
- Una vez en la pestaña **Registro administrativo**, verá la cantidad de entradas de registro administrativo actualmente en la base de datos.

Figura 25.2. Pantalla de depuración de la base de datos



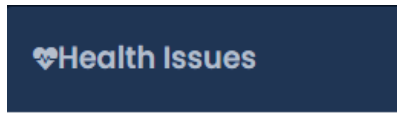
- Recomendamos tratar de permanecer por debajo de 1,000,000 de entradas del registro administrativo. Para implementaciones más pequeñas, esto podría demorar varios años, pero para las más grandes, podría tomar algunos meses.
- Para depurar las entradas del registro administrativo, use el menú desplegable **depurar entradas del registro administrativo** y cambie la antigüedad que deben tener las entradas del registro para poder eliminarlas. La fecha varía desde entradas con más de 5 años hasta entradas con más de 30 días. También puede seleccionar depurar todas las entradas.
- Una vez que haya hecho su selección, haga clic en el botón depurar entradas de registro de administrador en la parte inferior derecha. Las entradas que coincidan con el parámetro de fecha ahora se eliminarán. El conteo actual se actualizará una vez que se complete la depuración.

Advertencia de tamaño de base de datos

Esta sección cubrirá cómo configurar una notificación de advertencia de tamaño de base de datos en VAX. Grandes cantidades de notificaciones y registros de administración a lo largo del tiempo pueden dificultar el rendimiento de VAX, lo que implica específicamente implementaciones con cientos de paneles activos y miles de usuarios. Esta sección le permitirá notificar a los administradores y usuarios del sistema cuando una base de datos se acerque al tamaño máximo.

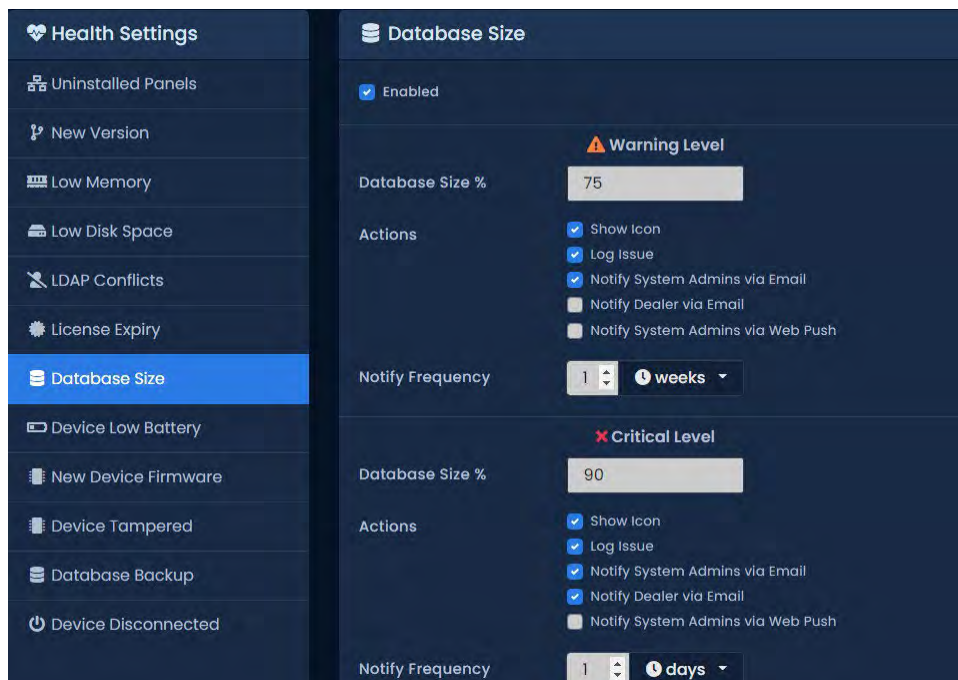
Use los siguientes pasos para acceder al formulario de advertencia de tamaño de la base de datos en VAX:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el ícono de **Configuración de salud (en la imagen a continuación)**.



2. Una vez en la pantalla **Problemas de salud**, verá en la lista del lado izquierdo titulada **Configuración de funcionamiento**, la opción Tamaño de la base de datos.

Figura 25.3. Página de advertencia de tamaño



3. Seleccione el porcentaje de advertencia ingresando la **cantidad deseada** o use las flechas arriba/abajo provistas dentro del cuadro de texto.
4. Seleccione opciones que incluyen, entre otras, Mostrar ícono, Problema de registro, Notificar a los administradores del sistema por correo electrónico, Notificar al distribuidor por correo electrónico y Notificar a los administradores del sistema a través de Web Push.
5. Una vez que haya hecho su selección, haga clic en el botón **Guardar** en la parte inferior derecha.

Capítulo 26. Configuración del Sistema

Este capítulo cubre la configuración del sistema de VAX. La mayoría de estas configuraciones son los mismos campos que se configuran durante la configuración inicial de VAX. Incluyen la información del distribuidor, la dirección del servidor, los puertos de comunicación, la seguridad y la configuración del correo electrónico para las alertas por correo electrónico.

Para acceder a la página de configuración del sistema:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la barra lateral, desplácese hasta la sección titulada **Administración**; haga clic en el icono **Configuración del sistema**. (en la foto de abajo)



En la pantalla Configuración del sistema, habrá cinco pestañas de configuración. Son **Configuración general**, **Seguridad**, **Configuración de correo electrónico**, **Solicitudes de servicio** y **Notificación de depuración**.

Configuración general

Esta sección cubrirá la pestaña Configuración general en la configuración del sistema VAX. Estos ajustes y una descripción se incluyen en la siguiente tabla:

Tabla 26.1. Campos generales de configuración

Campo	Breve descripción
Nombre	Este es el nombre del host, cliente o nombre de la empresa (no un sitio específico).
Descripción	Una descripción opcional del anfitrión, cliente o empresa.
Número de cuenta	Su número de cuenta de Industrias Vicon. Esto lo proporciona Vicon en la activación inicial. Acepta de 2 a 30 caracteres.
Nombre del distribuidor	Este es el nombre del distribuidor que instala el sistema y/o responsable de brindar soporte al usuario final del sistema.
Número de teléfono del distribuidor	Este es el número de teléfono de contacto principal del distribuidor que instala el sistema y/o responsable de brindar soporte al usuario final del sistema. Sin guiones entre las secciones del número (por ejemplo: 800-348-4266).
Sitio web del distribuidor	Esta es la dirección del sitio web del distribuidor que instala el sistema y/o responsable de brindar soporte al usuario final del sistema. Formato como "www.dealerwebsite.com"
Correo electrónico del distribuidor	Esta es la dirección de correo electrónico de contacto principal del distribuidor que instala el sistema y/o responsable de brindar soporte al usuario final del sistema

Dirección del servidor

La dirección del servidor se configura en la parte inferior de la pestaña General; estos campos se envían al Panel durante una actualización del Panel y dictan cómo los Paneles se comunican con el

servidor VAX.

Tabla 26.2. Campos de configuración de conexión

Campo	Breve descripción
Dirección del servidor	Por defecto, el nombre de la PC en la que está instalado VAX. Este campo es lo que se envía a sus paneles y dictará cómo se comunican con el servidor. Puede mantener esto como un nombre si el DNS está activo, o cambiarlo por la IP estática del servidor.
Dirección web	La dirección URL utilizada para enviar enlaces para la inscripción de credenciales móviles, el código QR de la aplicación de administración y los correos electrónicos de restablecimiento de contraseña. De forma predeterminada, si no se establece, el servidor utilizará la URL de referencia
Formato de tarjeta predeterminado	El formato de tarjeta a utilizar. Por defecto estándar HID (26 bits).
Código de sitio predeterminado	El ID de sitio predeterminado.
IdST predeterminado	El token de acceso predeterminado para dispositivos STid.
Tablero de control predeterminado	El formato de tablero predeterminado que se usará.

Una vez que haya realizado los cambios deseados en su configuración, haga clic en el botón Guardar en la parte inferior derecha de la pantalla.

Seguridad

Esta sección cubrirá la pestaña Configuración de seguridad en la configuración del sistema VAX.

Seguridad mejorada con PIN manual

La seguridad de PIN manual mejorada a menudo se habilita en implementaciones donde se utilizan horarios de puerta **solo PIN**. Cuando está habilitado, el sistema rechazará los números de PIN manuales que sean demasiado similares a los números de PIN existentes, lo que reduce en gran medida los cambios de acceso no autorizado debido a la similitud de PIN.

Para habilitar, simplemente marque la casilla de **verificación Seguridad de PIN manual mejorada** en la **Sección general de Configuración del sistema**.

Configuración de correo electrónico

Esta sección cubrirá la configuración de correo electrónico en VAX. La pestaña Configuración de correo electrónico se usa para configurar una dirección de correo electrónico para enviar correos electrónicos para recuperación de contraseña y alertas de notificación.

Figura 26.3 configuración de correo electrónico



Ajustes del correo electrónico

Complete los siguientes campos en la pestaña Configuración de correo electrónico de la Configuración del

sistema.


 **Nota:** Email Settings are optional, but recommended. Can be used to recover a forgotten password and to receive notification emails.


Tabla 26.3. Campos de configuración de correo electrónico

Campo	Breve descripción
Servidor SMTP	Este es el nombre del servidor SMTP requerido para enviar correos electrónicos (por ejemplo: mail.ISPdomain.com).
Puerto del servidor SMTP	Este es el puerto utilizado para enviar correos electrónicos a través de SMTP (el puerto 25 es común, sin embargo, su configuración puede variar).
Requiere SSL	Marque la casilla de verificación Secure Socket Layer si su cliente de correo electrónico requiere y utiliza SSL para cifrar los mensajes de correo electrónico.
Dirección de respuesta	Esta es la dirección de correo electrónico desde la que se enviarán las alertas de correo electrónico y la recuperación de correo electrónico. Puede ser la misma que la dirección de correo electrónico del remitente.
Nombre de usuario	Este es el nombre de usuario necesario para la autenticación y el envío de correo electrónico a través de SMTP.
Contraseña	Esta es la contraseña necesaria para la autenticación y el envío de correo electrónico a través de SMTP.
Enviar prueba al guardar	Si está marcado, se enviará un correo electrónico de prueba desde la dirección de respuesta para verificar que la configuración sea correcta

Una vez que se hayan configurado todos los campos obligatorios, haga clic en **Guardar**. Si se marcó la casilla de verificación **Enviar prueba al guardar**, se enviará un correo electrónico de prueba a la dirección de respuesta desde la dirección de respuesta.

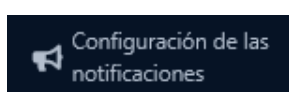
Notificaciones por Correo Electrónico

Las notificaciones por correo electrónico son una característica de VAX que le permite recibir correos electrónicos cuando ocurren ciertos eventos en su sistema de control de acceso. Por ejemplo, si a alguien se le negó el acceso a un lector, es posible que desee recibir una alerta por correo electrónico al respecto.

 **Nota:** Para que las notificaciones por correo electrónico funcionen, debe configurar correctamente la configuración de correo electrónico de VAX.

Para configurar las notificaciones por correo electrónico, siga estos pasos:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la barra lateral, haga clic en el ícono **Configuración de notificaciones**.



4. En la pantalla de configuración de notificaciones, verá 16 secciones y 3 columnas. Cada sección contiene un encabezado sobre el tipo de notificación debajo de ella.
5. Cada notificación tiene un botón de alerta, correo electrónico y cámara en vivo en el lado

izquierdo. Cuando el botón Correo electrónico junto a una notificación está activado, se enviará un correo electrónico al administrador conectado cuando se produzca esta notificación, junto con información sobre la notificación, como el usuario/puerta/lector/hora involucrados.

Cuando se selecciona el botón Alerta, esa notificación aparecerá en rojo en las notificaciones en vivo y opcionalmente producirá un sonido en el navegador web.

Cuando se selecciona Video en vivo, se generará una transmisión de video en línea si la notificación está relacionada con una puerta o ascensor con cámaras asociadas.

Configuración de la aplicación móvil

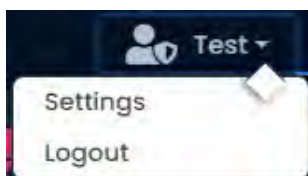
Esta sección cubrirá cómo generar un Código QR en VAX para configurar su aplicación móvil. El código QR se puede escanear con su aplicación móvil para facilitar la integración del servidor.

Generación de un código QR

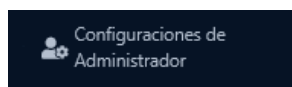
Una versión móvil de VAX está disponible para descargar a través de su dispositivo móvil. Los archivos de descarga se pueden encontrar a través de la tienda de aplicaciones de su dispositivo. Con la aplicación instalada, puede usar un código QR para agregar la configuración del servidor VAX existente a la aplicación en su dispositivo móvil.

Para generar un código QR, siga estos pasos:


1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la pantalla de inicio, haga clic en el icono **Configuración administrativa** en la parte superior de la pantalla. Aparecerá un menú desplegable. Seleccione **Configuración**.



4. Alternativamente, también se puede acceder a la **pestaña móvil en la barra lateral**. Desplácese a la sección titulada **Administración**; haga clic en el ícono de **Configuración del administrador** (en la imagen a continuación)).



5. En la página **Configuración del administrador**, estarán disponibles una pestaña Notificaciones y una pestaña Móvil. Seleccione la pestaña **Móvil**.
6. Escanee el código QR generado dentro de su aplicación VAX con la cámara de su dispositivo móvil.

 **Nota:** El código QR generado representará la dirección actual que se utiliza para acceder a VAX. (es decir, host local, nombre de PC, dirección IP, IP pública). Asegúrese de que actualmente está accediendo a VAX con una dirección que se puede encontrar a través de su dispositivo móvil.

Solicitudes de servicio

Esta sección cubrirá la pestaña Solicitudes de servicio en la configuración del sistema VAX. Solicitudes de servicio muestra una lista de solicitudes de servicio de terceros para una clave de API. Las aplicaciones de terceros solicitan claves API para integrarse con VAX. La información sobre estas aplicaciones de terceros se muestra y describe mediante la siguiente información que se muestra en esta tabla:

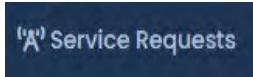


Tabla 26.4. Solicitudes de servicio

Nombre	Breve descripción
Nombre	Nombre de la aplicación.
Solicitado	Fecha solicitada.
Dirección IP	Dirección IP de la aplicación de terceros.
URL de devolución de llamada	URL Enlace a la información de devolución de llamada directa

Para obtener más información sobre la integración de terceros, consulte el *Capítulo 35, Integración de terceros*.

Notificación de Depuracion

Esta sección de Configuración del sistema maneja la **eliminación de notificaciones**. Consulte el *Capítulo 25, la sección denominada "Depuración de notificaciones"* para obtener más información sobre la depuración de notificaciones.

Figura 26.4.

Purge Notification

Automatic Purge

Configure a time of the day that VAX should automatically purge all notifications that have exceeded their retention policy configured above.

Enable Purge Notifications

Time

Day of Week Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Sat...

Notification Limit

Configure a maximum notification count that will automatically trigger a purge of the configured number of oldest notifications from the database.

Notification Limit 2500000

Purge Size 100000

Store Purged Notifications in CSV File

Capítulo 27. Hardware del Elevador

Este capítulo cubrirá los componentes de hardware de control de acceso necesarios para configurar Elevadores en VAX.

Se requieren los siguientes elementos:

Tabla 27.1. Hardware del Elevador

Número de parte	Descripción
Panel maestro del elevador	El panel maestro del elevador. Un controlador con firmware especial para interactuar con los Expansores de Elevadores de a través de una conexión RS-485.
Placa de expansión de E/S del elevador (VAX-IO-EXP8-PCB)	Tarjetas adicionales con 8 Entradas y 8 Salidas. Controlado desde el Panel Maestro del Elevador a través de una conexión RS-485. Direcciones de interruptores DIP 1-8.
Placa de expansión del lector (VAX-EXP-2D)	Placas secundarias con 2 puertos de lector wiegand, 4 salidas secas, 2 salidas húmedas y 6 entradas. Se utiliza principalmente en el contexto de los ascensores para los puertos de lectura. Dirección del microinterruptor 9

Conexión del panel maestro del elevador a las tarjetas de expansion

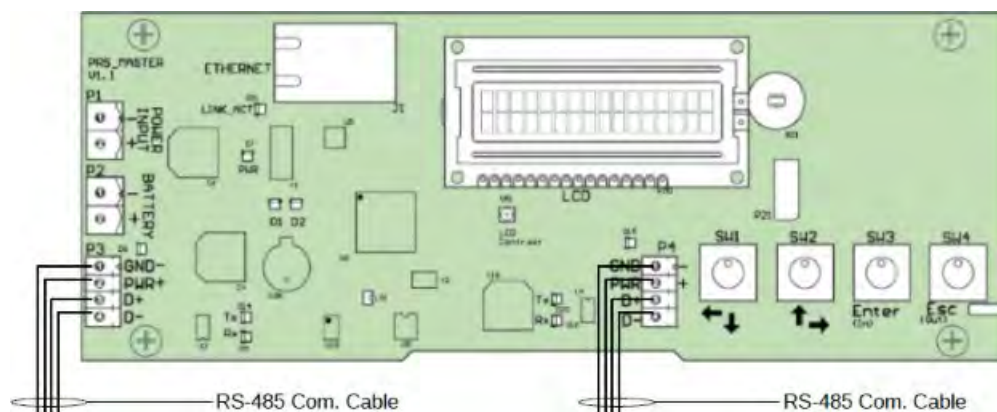
The **Elevator Master Panel** communicates with the **Expander Boards** using **RS-485 interconnect strip(s) or wiring**. When choosing to wire the expander boards to the VAX-ELV-STR-2 instead of the interconnect strips, it is recommend to use 2-pair twisted shielded 18 AWG.

Elevator kits such as the VAX-ELV-STR will typically come pre-wired and include interconnect strips. The Elevator Master Panel will plug into either the P3 or P4 header connection to the expanders P9 header connection. Use the follwing instructions of wiring the Elevator Master to the expanders via 2-pair twisted.

1. El controlador maestro tendrá dos puertos RS-485 + puertos de alimentación dedicados (P3, P4) y, si se usan tiras de interconexión, 2 puertos cerca de la parte inferior de cada tira (EP2). Conecte las conexiones de alimentación a través de 2 conductores 18 AWG (GND, PWR+) y conecte las conexiones de datos a través de 2 conductores trenzados 18-22 AWG (D+, D-) al punto correspondiente en el expansor IO (P9).

El panel se verá de la siguiente manera:

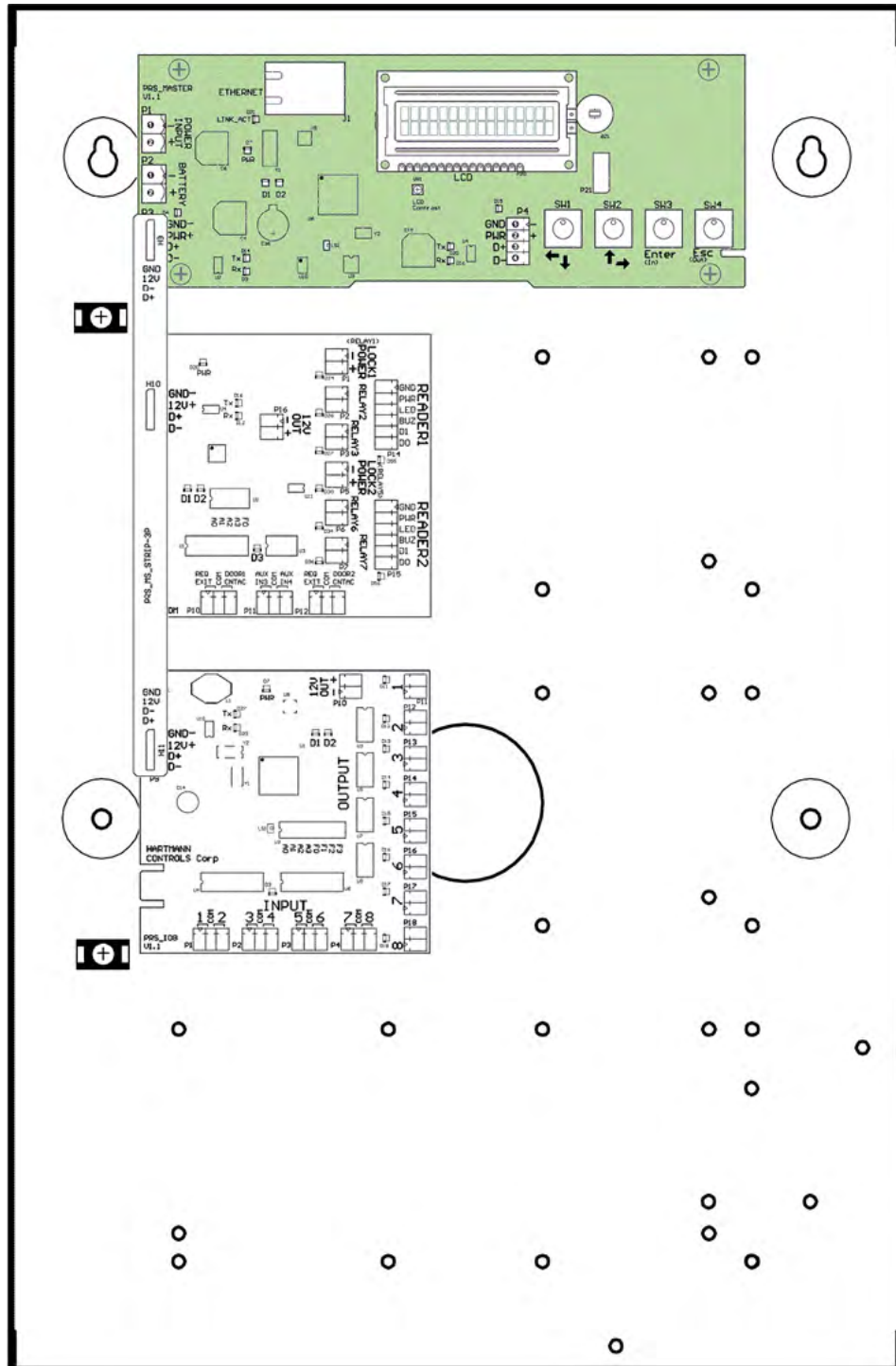
Figura 27.1. Conexión RS-485 para ascensor



En el primer expansor:

1. Conecte el otro extremo del par de '12 V' del Elevator Master a 'GND-' y '12V+' en el conector de 4 pines en el lado izquierdo de la primera placa de expansión. Asegúrese de que la polaridad coincida.
2. Se instalará un cable RS-485 adicional desde la primera **placa de expansión** hasta la segunda utilizando el mismo bloque de cabecera. Asegúrese de que la polaridad coincida. Continúe esta cadena para todas las **tarjetas de expansión** adicionales.

Figura 27.2. Panel maestro de Elevador

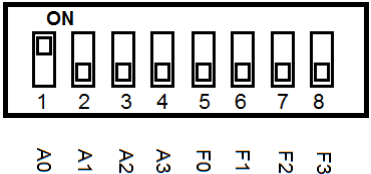
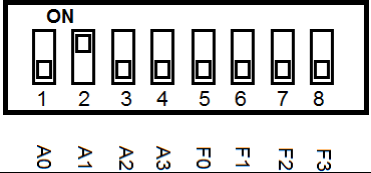
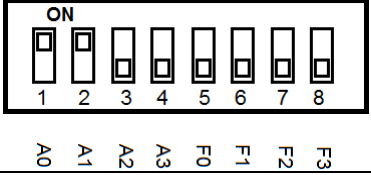
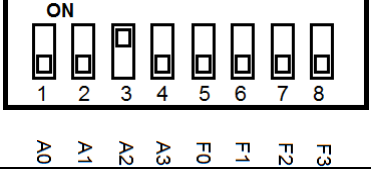
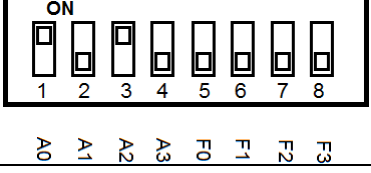
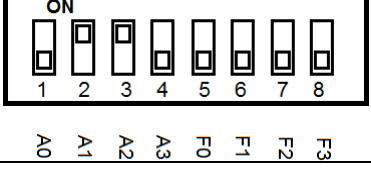
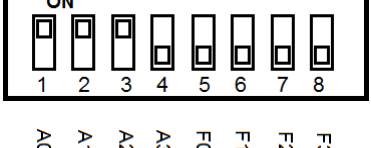


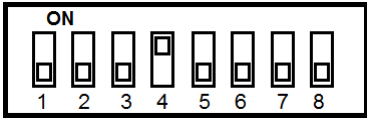
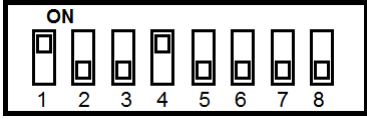
Configuración de direcciones de tarjetas de expansión

Cada **tarjeta de expansión** en el bus RS-485 requiere una dirección de panel secuencial. La dirección se configura usando los primeros 4 interruptores DIP en las tarjetas de expansión. El expansor de lectores para los kits de elevador debe establecerse en 9. La primera **tarjeta de expansión de E/S** necesita una dirección de '1', la segunda una dirección de '2' y así sucesivamente.

El siguiente cuadro demostrará las posiciones de los interruptores DIP y la dirección de la placa de expansión correspondiente:

Tabla 27.2. Dirección del interruptor DIP del panel de expansión

Posición del interruptor DIP	Dirección de Panel resultante
	Dirección del panel: 1 A3 ~ A0: 0001
	Dirección del panel: 2 A3 ~ A0: 0010
	Dirección del panel: 3 A3 ~ A0: 0011
	Dirección del panel: 4 A3 ~ A0: 0100
	Dirección del panel: 5 A3 ~ A0: 0101
	Dirección del panel: 6 A3 ~ A0: 0110
	Dirección del panel: 7 A3 ~ A0: 0111

Posición del interruptor DIP	Dirección de Panel resultante
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 8 A3 ~ A0: 1000
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 9 A3 ~ A0: 1001

Una vez que haya conectado sus **tarjetas de expansión** al panel **maestro del elevador** y haya configurado las **direcciones del panel del interruptor DIP**, ahora puede encender la tarjeta maestra del elevador a través de una fuente de alimentación de 12-13,5 VDC.

⚠ Advertencia

Antes de cablear las Entradas/Salidas en la Tarjeta de Expansión en su sistema de elevador, recomendamos configurar el software antes de esto. *Consulte el Capítulo 28, Componentes del software del elevador.*

Prueba de entrada/salida de la tarjeta de expansión

La exploración de la placa del expansor de E/S se coloca en modo de prueba a través de una configuración de interruptores DIP predefinidos (todos los interruptores están en APAGADO excepto F3, consulte la figura a continuación). En el modo de prueba, la Tarjeta de Expansión activará secuencialmente sus 8 Salidas. Después de probar las 8 salidas, se apagarán y las entradas estarán disponibles para la prueba. Para probar una Entrada, simplemente cortocircuite la Entrada y la Salida correspondiente se activará. Si alguna de estas pruebas falla, comuníquese con Vicon Industries. *Consulte el Capítulo 37, Soporte.*

Figura 27.3. Interruptor DIP: Prueba de entrada/salida



Sensor de manipulación de la placa de expansión

a placa del Expansor tiene un sensor de manipulación incorporado. Este sensor enviará una notificación a VAX si detecta un cambio en el nivel de luz. Si las tarjetas de expansión están ubicadas en el mismo contenedor que el panel maestro del elevador, es probable que no necesite habilitar el sensor de manipulación de la tarjeta de expansión. Si las Tarjetas Expansoras están en una ubicación diferente, al menos una Tarjeta Expansora debería tenerlo habilitado. Para habilitar el sensor de manipulación, simplemente gire F2 a ON. Mantenga A0 - A3 igual. Vea abajo.

Figura 27.4. Interruptor DIP: Sensor de manipulación



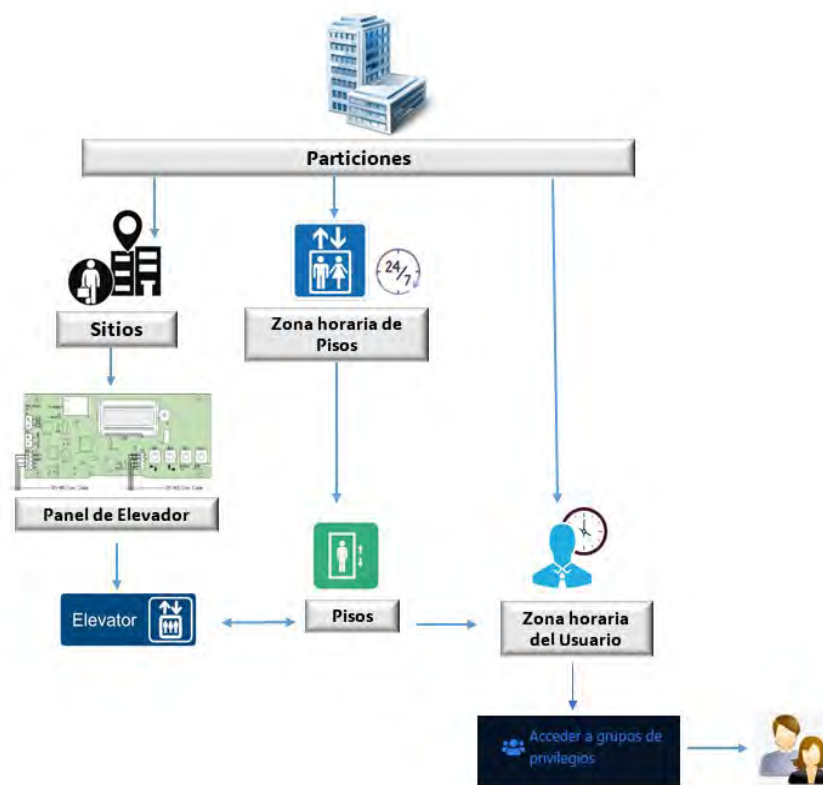
Capítulo 28. Componentes del software de Elevador

Este capítulo será una descripción general de los diversos componentes del ascensor dentro de VAX 2.1.0+. Los componentes del software Elevator son los siguientes:

- Paneles de ascensor (el VAX-ELV-STR-2)
- Elevadores
- Pisos
- Horarios de piso
- Zonas de ejecución única en el piso (OTR en el piso)
- Grupos de festivos de piso
- Horarios de Festivos de piso

El siguiente diagrama demuestra los componentes principales de los ascensores y cómo interactúan con los elementos de software ya existentes de VAX.

Figura 28.1. Elementos de configuración del Elevador



Agregar un panel de elevador

Agregar un panel de elevador a VAX es muy similar a agregar un panel de puerta. Esta sección repasa este proceso.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.

2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono **Paneles** (en la imagen a continuación).



4. En la pantalla **Ver paneles**, haga clic en el botón **Agregar**.

En la pantalla **Agregar paneles**, se le presentarán varios menús desplegables, campos de texto y casillas de verificación para completar. Asegúrese de que el menú desplegable Modelo de panel esté configurado en: **VAX-ELV-STR-2**.

Figura 28.2. Pantalla Agregar paneles

 Una interfaz de usuario con un fondo oscuro. Encabezado: 'Panel' con un ícono de configuración. Campos de formulario:

- Panel Model: Menú desplegable con 'VAX-ELV-STR-2' seleccionado y 'PRS Elevator Panel' como subtítulo.
- Name: Campo de texto con 'Elevator Test'.
- Description: Campo de texto con 'Optional Description'.
- Site: Menú desplegable con 'Default Site'.
- MAC Address: Campo de texto con '988888888888'.
- Panel Password: Campo de texto con '0000'.
- Installed: Casilla de verificación marcada.
- Tamper Sensor: Casilla de verificación no marcada.
- Expanders: Campo de texto con '2'.

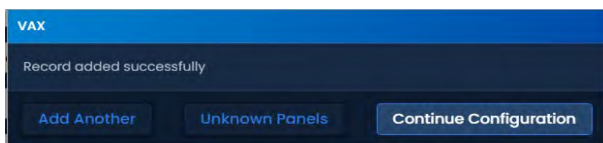
En la siguiente tabla se describen los campos a completar.

Tabla 28.1. Agregar Panel

Desplegable/Cuadro de texto / Casilla de verificación	Descripción
Modelo de panel	Seleccione VAX-ELV-STR-2.
Nombre	El nombre del Panel; Recomendamos nombrar el Panel según su ubicación en el sitio. Acepta de 4 a 60 caracteres.
Descripción	Descripción opcional del Panel. Acepta de 0 a 255 caracteres.
Sitio	Seleccione el sitio en el que residirá el Panel. Esto no se puede cambiar una vez que se agrega el Panel.
Dirección MAC	La dirección de red única integrada en cada Panel. Puede completarse previamente si está agregando el panel a través de una notificación de conexión desconocida desde el panel. Debe tener 12 caracteres.
Contraseña del panel	La contraseña necesaria para acceder al menú de administración integrado en el Panel. Los valores válidos son de 0 a 9999.
Expansores	La cantidad de Placas de Expansión adjuntas al Panel del Elevador. Los valores válidos son del 1 al 8.
Conexión TCP: modo de conexión	El método en el que el Panel recibe su dirección IP, DHCP o Estática. Al seleccionar estático, aparecerán campos adicionales para completar.

Una vez que haya completado los campos obligatorios, haga clic en el botón Crear en la parte inferior de la pantalla.

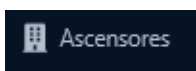
Si tiene éxito, se le mostrará el mensaje: 'Panel agregado con éxito' con las opciones para agregar un Panel adicional, o para continuar con la pantalla de edición del Panel que acabamos de agregar.



Agregar un Elevador

Después de agregar un panel de elevador, el siguiente paso es agregar un elevador. Este objeto contendrá la configuración para los pisos, incluidos los horarios de piso y los grupos de días festivos.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono de Elevadores (en la imagen a continuación).



4. En la pantalla Ver elevadores, haga clic en el botón **Agregar**. En la pantalla Agregar elevador, se le presentarán varios menús desplegables, campos de texto y casillas de verificación para completar.
5. En la siguiente tabla se describen los campos a completar.

Tabla 28.2. Agregar Elevador

Desplegable / Cuadro de texto / Casilla de verificación	Descripción
Nombre	Un nombre único para su Ascensor. Acepta de 2 a 60 caracteres.
Descripción	Una descripción opcional para su Ascensor. Acepta de 0 a 255 caracteres.
Panel	Seleccione el panel del elevador al que se adjuntará este elevador
Detección de botones	Deshabilitar/Habilitar si la detección de botones está disponible. Para obtener más información sobre la detección de botones, consulte la sección denominada "Detección de botones".
Número de piso inicial	Número de piso inicial. Los valores válidos son -55 a 200.
Numero de pisos	Numero de pisos. Los valores válidos son de 0 a 255. Si hay más de 8 Pisos, se requerirán más de un Tablero Expansor. Si no hay puertos disponibles, se le notificará al guardar.

Una vez que haya completado los campos obligatorios, haga clic en el botón Guardar en la parte inferior de la pantalla.

Si tiene éxito, se le mostrará el mensaje: '**Elevador agregado con éxito**' con las opciones para agregar un Ascensor adicional, o para continuar a la pantalla **Editar Elevador** del ascensor que acabamos de agregar.

En la pantalla **Editar Elevador**, hay tres pestañas: **General, Pisos, Lectores**. Se describen a continuación:

General. En la pestaña **General**, puede cambiar el nombre del **elevador**, **agregar/editar** la descripción y habilitar/deshabilitar la detección de botones. (Para obtener más información sobre la detección de botones, consulte la sección denominada "Detección de botones".)

Solo hay dos opciones disponibles en la pestaña General después de agregar el Elevador:

Figura 28.3. Pestaña General

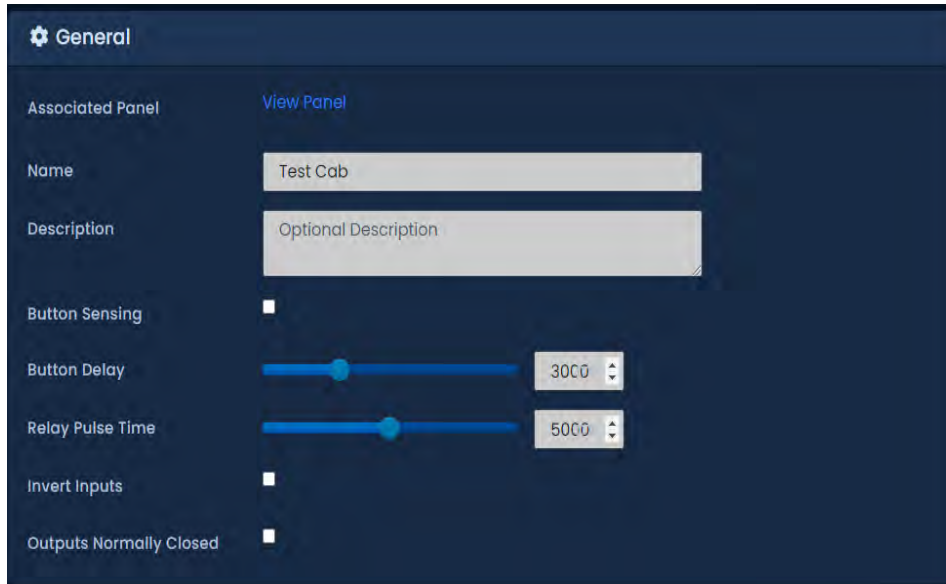


Table 28.3. Pestaña General

Desplegable / Cuadro de texto / Casilla de verificación	Descripción
Botón de retraso	Si se utiliza la detección de botones, cuánto tiempo entre la presentación de una credencial y la pulsación de un botón se considera válida. Incrementos de 100 ms. Los valores válidos son de 0 ms a 10000 ms.
Tiempo de pulso de relé	Cuánto tiempo permanecerán cerrados los relés una vez que se haya concedido acceso a un piso o grupo de pisos en particular. Incrementos de 100 ms. Los valores válidos son de 100 ms a 2000 ms

Pestaña de Piso

La pestaña **Pisos** es donde puede editar, **agregar o eliminar Pisos**. Es donde usted asigna los **horarios de Piso y el Grupo de festivos de Piso**.

Figura 28.4. pestaña Pisos

Output	Status	Elevator	Floor
Expander 1			
Elevator: Test Cab			
Address: 1			
1	Enabled	Test Cab	[1] Floor 1
2	Enabled	Test Cab	[2] Floor 2
3	Enabled	Test Cab	[3] Floor 3
4	Enabled	Test Cab	[4] Floor 4
5	Enabled	Test Cab	[5] Floor 5
6	Enabled	Test Cab	[6] Floor 6
7	Enabled	Test Cab	[7] Floor 7
8	Enabled	Test Cab	[8] Floor 8
Expander 2			
Elevator: None			
Address: 2			
1	Not Used		
2	Not Used		
3	Not Used		
4	Not Used		
5	Not Used		
6	Not Used		
7	Not Used		
8	Not Used		

Lector

La **pestaña Lector** es donde puede habilitar el Lector, nombrar/cambiar el nombre del Lector y asignar a qué puerto del Lector está conectado. Se requiere un lector para un control de piso adecuado. Las cabinas de ascensor sin lectores solo pueden operar en horarios.

Figura 28.5. pestaña Lector

Elevators > Cab 1

General Floors **Reader** Camera Association

Reader

Enabled

Name

Reader Port

Action [+](#)

Perform action only on Access Granted

[Undo](#) [Save](#)

Detección de botones

Esta sección cubrirá los conceptos de detección de botones. La detección de botones está habilitada/deshabilitada en la pestaña General al editar un Elevador o al crear un Elevador.

Detección de botón: Habilitado. Debe habilitarse cuando los botones de un ascensor (correspondientes a un Piso) están conectados a las **Entradas** en la **Tarjeta Expansora**. Cuando se presiona un botón en el elevador sin que se presente una Credencial autorizada, la **Salida** correspondiente permanecerá apagada (con la excepción de que el Piso correspondiente tenga un modo de **Horario de Piso Desbloqueado**)

Cuando se presiona un botón en la cabina del ascensor después de que se haya presentado una Credencial autorizada (el **Usuario** tiene un **Grupo de Privilegios de Acceso** que le da acceso a ese Piso específico), se **activará la Salida** correspondiente.

El beneficio principal de la **detección de botones** es que los **administradores** en VAX pueden ver exactamente a qué **piso seleccionó el usuario** para ir (en vivo a través de **notificaciones** o a través del **informe de actividad del piso/informe de actividad del usuario**).

Detección de botón: deshabilitado. Debe deshabilitarse cuando no es posible conectar los botones en la cabina del ascensor a la **entrada** en la **tarjeta de expansión**. En este escenario, las **salidas** en la **tarjeta de expansión** estarán entre el intérprete de botones y el controlador lógico del elevador.

Dado que la **Tarjeta Expansora** no puede interpretar qué Piso desea seleccionar el Usuario, cuando se ha presentado una Credencial autorizada (el Usuario tiene un **Grupo de Privilegios de Acceso** que le da acceso a Pisos específicos), todas las **Salidas asociadas con los Pisos** a los que el Usuario tiene acceso se cerrará. Los botones en la cabina del elevador que están asociados con una de las salidas cerradas fluirán normalmente al controlador lógico del elevador.

La desventaja de no tener **detección de botones** es que los **administradores** en VAX no podrán ver qué **piso seleccionó el usuario**. Se podrá ver un registro del **Usuario** presentando su Credencial al **Lector en la cabina** en Informes de **Actividad de Piso/Actividad del Usuario**.

Mapa de E/S por piso

El mapa de E/S por piso es una pestaña en la pantalla del panel de edición que muestra un mapa de todas las salidas en la tarjeta de expansión y los pisos y elevadores correspondientes según la configuración actual. El mapa de E/S de piso es extremadamente útil para una referencia de cableado. Esta pantalla mostrará las Direcciones de la Tarjeta de Expansión de cada Expansor, con qué Elevador está asociado el Expansor y la Salida con la que está asociado cada Piso.

Figura 28.6. Mapa de E/S por piso

Output	Status	Elevator	Floor
Expander 1			
Elevator: Test Cab			
Address: 1			
1	Enabled	Test Cab	[1] Floor 1
2	Enabled	Test Cab	[2] Floor 2
3	Enabled	Test Cab	[3] Floor 3
4	Enabled	Test Cab	[4] Floor 4
5	Enabled	Test Cab	[5] Floor 5
6	Enabled	Test Cab	[6] Floor 6
7	Enabled	Test Cab	[7] Floor 7
8	Enabled	Test Cab	[8] Floor 8
Expander 2			
Elevator: None			
Address: 2			
1	Not Used		
2	Not Used		
3	Not Used		
4	Not Used		
5	Not Used		
6	Not Used		
7	Not Used		
8	Not Used		

Horarios de piso

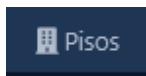
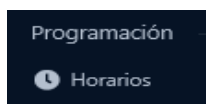
Esta sección cubre la adición de cronogramas de piso adicionales a VAX.

Los **horarios de Pisos** se aplican a los **Pisos** en la **Pestaña de Pisos** de la Pantalla **Editar Elevadores**. A diferencia de los **Horarios de Puerta**, los **Horarios de Piso** solo tienen tres estados posibles: **Tarjeta**, **Desbloqueo y Bloqueo**. De forma predeterminada, hay 3 Horarios de piso

- Card Always
- Locked Always
- Unlocked Always

Para agregar más horarios de piso:

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono **Horarios** (en la imagen a continuación). **Seleccione la pestaña del piso**,



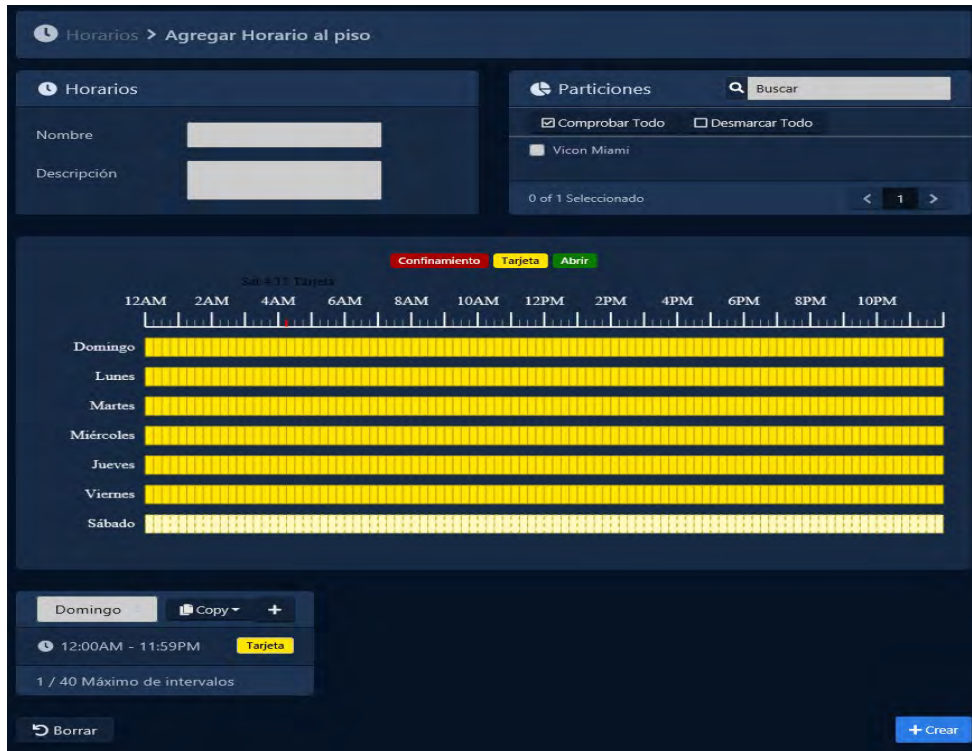
4. En la pantalla **Horarios de piso**, verá los Horarios predeterminados. Para agregar horarios, haga clic en el botón **Agregar** en esta pantalla.
5. En la pantalla Horarios de planta, verá los Horarios predeterminados. Para agregar horarios, haga clic en el botón Agregar en esta pantalla.
6. En la pantalla **Agregar horario de piso**, tendrá algunos cuadros de texto para completar.

Tabla 28.4. Agregar Horario

Texto	Descripción
Nombre	Nombre único de su Horario de planta. Acepta de 2 a 60 caracteres. Recomendamos nombrar sus Horarios por la función del Horario.
Descripción	Descripción opcional de su Horario de planta. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este programa. Si se selecciona más de una, se creará una copia para cada partición

7. Horario: La creación del horario es el último paso para crear un **horario de piso**.

Figura 28.7. Horario de piso

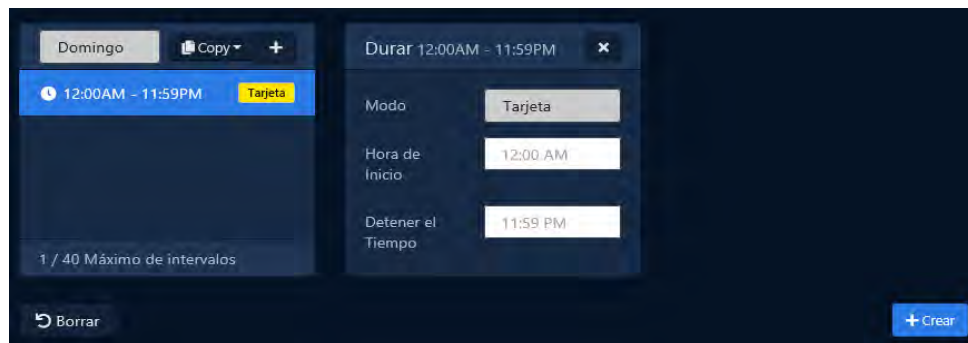


Nota: En Horarios de piso, puede tener hasta 8 intervalos de tiempo, lo que significa que el estado del piso puede cambiar hasta 8 veces en un horario.

8. Haga clic en cualquiera de las barras horizontales en el horario para que aparezca el widget Editor de horarios. El widget del editor de Horarios es una herramienta simple y poderosa para crear **Horarios**.

Figura 28.8. Editor de Horarios

9. Utilice el menú desplegable **Modo** para seleccionar el estado de acceso al piso para el tramo. Solo están disponibles **Tarjeta**, **Desbloqueo** y **Bloqueo**.
10. La sección **Agregar tramo del editor de horarios** tiene 3 campos que se usan para agregar un horario de piso. Cuando se hace clic en el campo Iniciar y detener, aparecerá un menú deslizante para seleccionar la hora de inicio y finalización. El segundo menú desplegable **Modo** dictará qué estado de acceso al piso seguirá el horario durante el lapso de tiempo definido. Una vez que haya completado estos campos, haga clic en el botón Agregar.



11. Ahora debería ver la barra que seleccionó codificada por colores para el período de tiempo que agregó. Agregue intervalos de tiempo a ese día si es necesario.

Si desea que el horario que ha creado se use para varios días diferentes, puede hacer clic en la barra con su horario completo y seleccionar la lista desplegable Copiar para seleccionar en qué día de la semana se debe copiar el horario. El cronograma se replicará en función de la opción de fecha seleccionada.

12. 12. Una vez que su horario para los 7 días sea el deseado, ahora puede presionar Guardar para crear el horario de piso en las particiones seleccionadas.

Asignación de acceso de usuario a pisos

Esta sección cubrirá cómo asignar permisos de Usuario para acceder a Pisos específicos usando Grupos de Privilegios de Acceso. Este proceso es bastante sencillo y funciona con componentes VAX con los que quizás ya esté familiarizado.

Una vez que haya agregado su(s) elevador(es) y asignado horarios de piso a cada piso, ahora puede asignar permisos de usuarios a estos pisos usando grupos de privilegios de acceso y horarios de usuarios de la misma manera que asignaría un permiso de usuario a un lector.

Para obtener más detalles sobre la asignación de pisos a grupos con privilegios de acceso, consulte el Capítulo 11, Grupos con privilegios de acceso.

Capítulo 29. Protocolo abierto de dispositivo supervisado (OSDP V2)

OSDP es un protocolo de comunicaciones desarrollado por la Security Industry Association (SIA). El caso de uso principal en el contexto de VAX es mejorar la seguridad con dispositivos periféricos como lectores de tarjetas.

Este capítulo cubrirá los beneficios de OSDP, los modelos de panel compatibles de Vicon Industries y cómo configurar los lectores OSDP para que funcionen con nuestros controladores desde una perspectiva de hardware y software.

Beneficios de usar OSDP

OSDP tiene varios beneficios sobre los protocolos de comunicación de lectores tradicionales (Wiegand, reloj y datos). Los resumiremos aquí:

- **Cableado simplificado:** los lectores que se comunican con los lectores OSDP utilizan menos conductores que otros métodos. Por lo general, puede usar un par trenzado de cuatro (4) conductores, como Belden 3107A o incluso un cable CAT6. Cualquier cable que cumpla con la especificación TIA485/EIA-RS-485 debería poder funcionar.
- **Cifrado:** OSDP admite comunicación cifrada bidireccional a través de AES-128. Esto evita vectores de ataque específicos, como la caída fácil y la suplantación de identidad.
- **Detección de manipulación y desconexión:** los lectores tradicionales normalmente no vienen con una forma de detectar la manipulación o la desconexión (como que alguien retire el lector de su posición montada). Los que lo hacían requerían pares adicionales para lograr esto y generalmente tenían costos adicionales. Debido a que OSDP es una comunicación bidireccional, el panel de control de acceso puede detectar si el lector está desconectado o retirado de su posición de montaje.
- **Distancias más largas:** los lectores Wiegand generalmente solo admitían una longitud máxima de 500'. OSDP usa RS-485, que teóricamente admite hasta 2000' (siempre que tenga alimentación de CC más cercana a 500').

Modelos de controlador de puerta compatibles

Actualmente, OSDP es compatible con los controladores de puerta VAX-MDK con firmware específico OSDP. Al pedir controladores de puerta, debe especificar que necesita firmware OSDP. Los módulos VAX-EXP-2D también requieren un firmware específico para admitir OSDP. No hay interoperabilidad entre el hardware OSDP y el hardware que no es OSDP. Los lectores Wiegand todavía se pueden usar en paneles OSDP.

Cómo comprobar si el firmware es compatible con OSDP

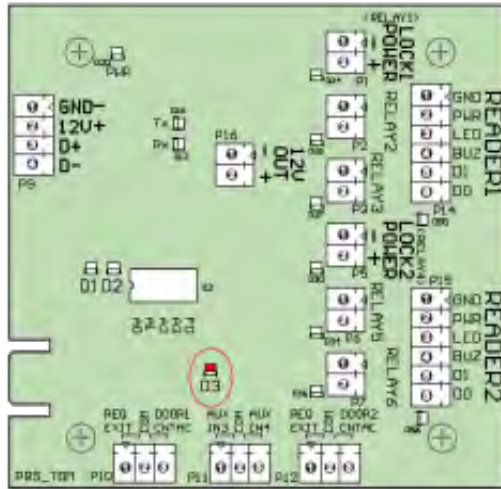
VAX-MDK: Utilice los siguientes pasos para comprobar la versión del firmware:

1. En el controlador físico, mantenga presionado el botón ESC (SW4) en el panel durante aproximadamente 3-4 segundos hasta que el panel emita dos pitidos.
2. Usando los botones blancos hacia arriba y hacia abajo en el panel, localice la opción titulada Versión de firmware (opción 16).



3. Si el controlador usa firmware OSDP, la versión de firmware comenzará con PMO. Si el controlador usa firmware Wiegand, comenzará con PMS.

VAX-EXP-2D: cuando se enciende un VAX-EXP-2D con firmware OSDP, el LED con la etiqueta D3 parpadeará 3 veces. El LED también parpadeará cada 30 segundos. Este LED también se encenderá cuando cambie el estado de la entrada, eliminando temporalmente las entradas que pueden ser necesarias para una identificación **adecuada**.



Cableado de un lector OSDP

El fabricante del lector proporcionará su propia documentación sobre cómo conectar el lector. El cableado recomendado es de 4 conductores de par trenzado blindado como Belden 3107A. Otros tipos de par trenzado pueden ser adecuados, como CAT6.

Puntos de conexión OSDP

Hay varios puntos donde puede conectar lectores OSDP en controladores OSDP VAX-MDK. El controlador VAX-MDK tiene dos conexiones de bus RS-485. Ambos buses RS-485 también se utilizan para comunicarse con los módulos de expansión VAX-EXP-2D. Cuando se utilizan tiras de interconexión, la parte inferior de la tira también tendrá un punto de conexión.

Figura 29.1. Puntos de conexión OSDP (RS-485) en VAX-MDK

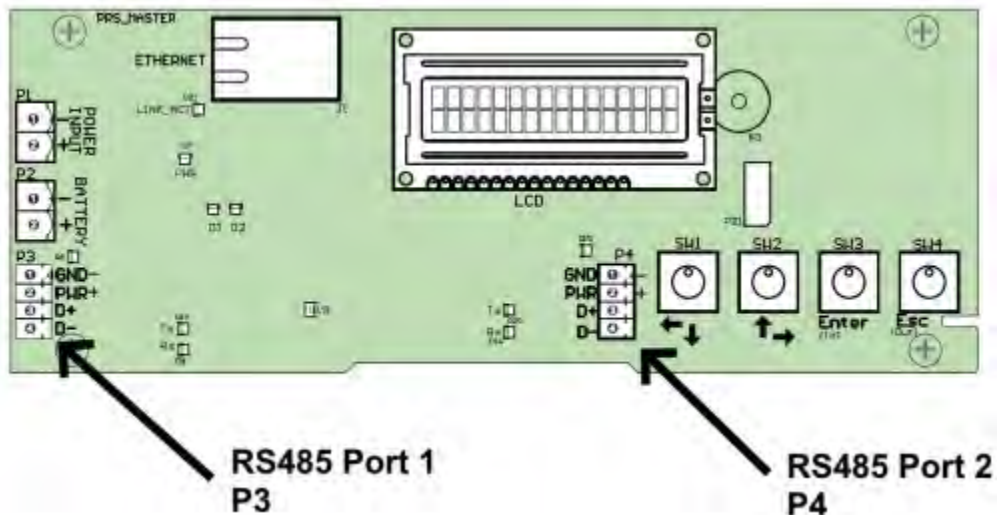
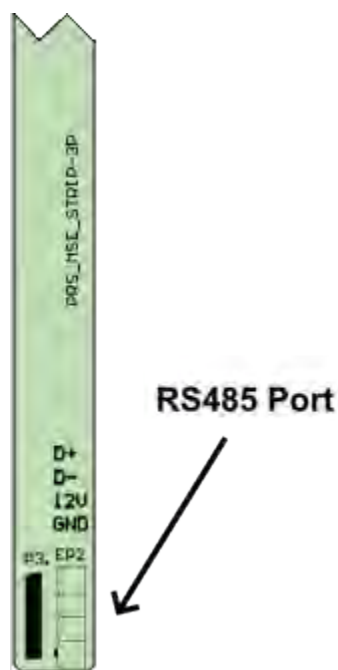


Figura 29.2. Puntos de conexión OSDP (RS-485) en tira de interconexión



⚠ Advertencia

Debido a la protección contra cortocircuitos en las conexiones del bus RS-485, un cortocircuito entre PWR y GND en cualquier conexión RS-485 hará que el controlador de la puerta se encienda y desconecte la alimentación de todos los expansores en el mismo bus. Por este motivo, puede resultar adecuado alimentar externamente lectores OSDP con su propia fuente de alimentación. La conexión GND y PWR en 12V OUT (P15) en un VAX-EXP-2D individual tiene su propia protección contra cortocircuitos y puede ser adecuada cuando la alimentación externa no es una opción.

⚠ Advertencia

Un cortocircuito entre D+ y D- o GND en cualquier conexión RS-485 hará que cualquier dispositivo conectado en el mismo bus (como VAX-EXP-2D) deje de comunicarse. Por esta razón, puede ser adecuado conectar la comunicación a lectores OSDP y otros dispositivos RS-485 de tal manera que los lectores no estén en el mismo bus RS-485 que los otros dispositivos.

Resistores de terminación

Algunos fabricantes de lectores OSDP recomendarán que se coloquen una o más resistencias en el bus RS-485 y posiblemente una resistencia de terminación en el último dispositivo del bus RS-485. Consulte la documentación del lector para obtener instrucciones específicas sobre el uso de la resistencia.

Configuración de la comunicación OSDP

Cada dispositivo OSDP tendrá una dirección. La mayoría de los dispositivos vendrán con una dirección de dispositivo predeterminada de 0. A través del menú LCD hay opciones para cambiar una dirección, probar la comunicación y habilitar el modo de comunicación segura. A veces es posible usar software de terceros para cambiar esta configuración en el lector o puede solicitar el lector preconfigurado con una dirección específica. Las direcciones 1 a 4 están reservadas para expansores. Las direcciones 5-16 están disponibles para lectores OSDP.

📄 Nota

Debe conectar un lector a la vez al configurar las direcciones, ya que varios lectores con la misma dirección causarán problemas de comunicación.

Configuración de la dirección del lector OSDP a través del menú LCD

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca '¿CONFIGURAR CONTRASEÑA?' en la pantalla LCD y '0000'.



2. Si el panel está utilizando la contraseña predeterminada ('0000'), presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESO CONCEDIDO'. Si el panel ya tiene una contraseña, la ingresará ahora usando los botones blancos arriba y abajo y el botón ENTER (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado).



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'OSDP' y luego presione el botón ENTER.



4. Ahora elegirá una dirección OSDP para realizar cambios o pruebas. Si no está seguro de cuál es la dirección, debe comenzar con 00. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique la dirección que desea cambiar o probar y presione el botón Enter.



5. La opción predeterminada en el siguiente menú es Sondear el dispositivo. Se recomienda encarecidamente que sondee el dispositivo (con éxito) antes de intentar cambiar la dirección. Para sondear el dispositivo, presione el botón Enter.



6. Ahora se mostrará el resultado de la encuesta. Verá Ack si hubo un dispositivo con dirección RS-485 que seleccionó en el menú anterior que puede responder. Se mostrará el tiempo de espera si no hay dispositivos conectados con la dirección seleccionada.

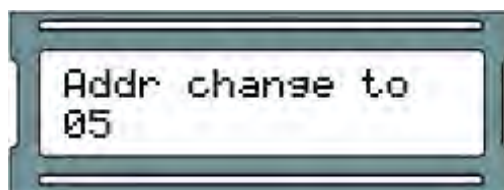




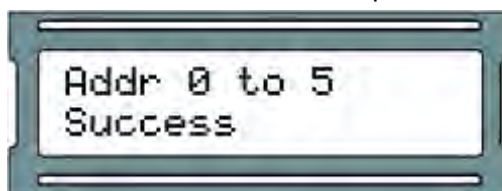
7. Pulse el botón ESC para volver al menú anterior.
8. Si necesita cambiar la dirección del dispositivo actual, use los botones blancos hacia arriba y hacia abajo en el Panel para ubicar la opción de menú Cambiar dirección. Pulse la tecla ENTER para entrar en el menú de cambio de dirección.



9. Ahora puede elegir la nueva dirección. Use los botones blancos hacia arriba y hacia abajo en el Panel para aumentar/disminuir la dirección. Cuando esté listo para elegir la dirección, presione el botón ENTER.



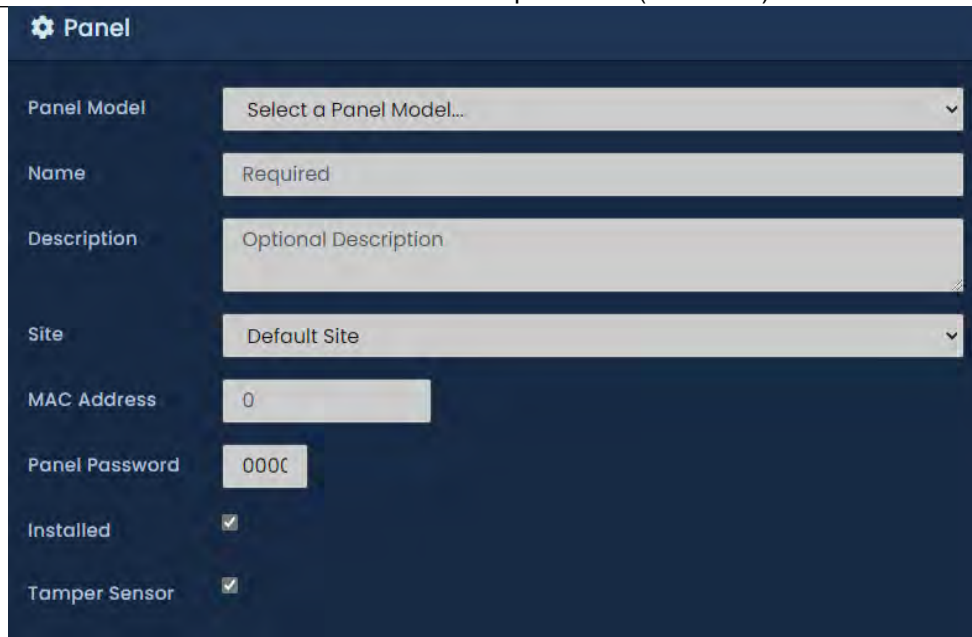
10. Si tiene éxito, verá la dirección antigua y la nueva con el mensaje Éxito. Registre la nueva dirección y presione el botón ESC para salir de este menú. Se mostrará el tiempo de espera si no se puede acceder a la dirección desde la que intentaba cambiar.



Configuración de comunicación del software OSDP

Esta sección resumirá la configuración del software requerida para la comunicación OSDP. La configuración de cifrado se tratará más adelante en este capítulo.

1. Configure la comunicación TCP entre el controlador de puerta y el software VAX como se describe en la sección llamada "Configuración inicial del panel".
2. Agregue el controlador al software como se describe en la sección llamada "Agregar un panel a VAX Access Control", asegurándose de seleccionar VAX-MDK-Master-OSDP como modelo de panel.
3. Al agregar una puerta (como se describe en la sección llamada "Agregar una puerta") a un panel OSDP, habrá una casilla de radio que le permitirá seleccionar OSDP como la interfaz del lector. Ingrese la dirección OSDP del lector que desea asociar a esta puerta.



Panel

Panel Model: Select a Panel Model...

Name: Required

Description: Optional Description

Site: Default Site

MAC Address: 0

Panel Password: 000C

Installed:

Tamper Sensor:

Configuración del modo de canal seguro OSDP

El modo de canal seguro es una función de OSDP que le permite utilizar el cifrado AES de 128 bits entre el controlador y el lector. La configuración del modo de canal seguro no es obligatoria para que OSDP funcione, pero se recomienda para obtener la máxima seguridad. Las claves de cifrado se configuran en la interfaz del software VAX. Los controladores de puerta VAX-MDK OSDP tienen una opción a través de la pantalla LCD para habilitar el modo de canal seguro en un lector adjunto. Según el lector, puede optar por permitir solo comunicaciones seguras.

Según el fabricante del lector, el modo de canal seguro se puede habilitar mediante una tarjeta de programación o una aplicación móvil de configuración del lector específica para el lector. Esta sección mostrará la configuración del software relacionada con el cifrado OSDP y mostrará cómo habilitar el modo de canal seguro a través de la interfaz LCD en el panel.

Advertencia

El modo de canal seguro no debe activarse hasta que se hayan enviado claves/códigos de cifrado al lector. VAX tiene la capacidad de hacer esto desde el software y se tratará en la siguiente sección.

Configuración de claves de cifrado

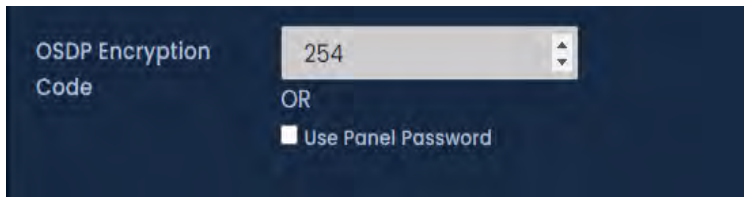
Esta sección cubre cómo configurar claves de cifrado para lectores OSDP desde el software VAX. Esto debe hacerse antes de habilitar el modo de canal seguro a través de la interfaz LCD del panel. El panel debe agregarse al sistema antes de poder seguir estos pasos. Para obtener información sobre cómo agregar un panel, consulte la sección llamada "Agregar un panel al control de acceso VAX".

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la barra lateral, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono **Paneles** (en la imagen a continuación).



4. En la pantalla Paneles, verá los Paneles que ya haya agregado al software. Haga clic en el botón azul (Configuración avanzada) junto al Panel que desea configurar.

5. En la pantalla **Editar panel**, estará en la pestaña General. Desplácese hacia abajo para ver la configuración OSDP. Estas opciones solo aparecerán si el controlador tiene firmware OSDP.



6. El código de cifrado OSDP admite 255 claves de cifrado predefinidas que se pueden usar con el modo de canal seguro. Este campo aceptará 0-254.

Como alternativa, la contraseña del panel se puede utilizar como clave de cifrado. Marque la casilla de verificación Usar contraseña del panel si desea usar la contraseña del panel como clave de cifrado o ingrese el valor de la clave de cifrado que le gustaría usar.

7. Actualice sus paneles para enviarles las claves de cifrado. No se usarán hasta que el Modo de canal seguro esté habilitado como se describe en las siguientes secciones.

Activación del modo de canal seguro en los lectores OSDP

Una vez que haya enviado las claves de cifrado al controlador, debe habilitar el modo de canal seguro en el propio lector. Puede hacerlo desde el menú LCD del panel o, en algunos casos, el fabricante del lector puede tener otros medios para hacerlo, como la tarjeta de programación o la aplicación de configuración.

1. Mantenga presionado el botón ENTER (SW3) en el panel durante aproximadamente 3 a 4 segundos hasta que aparezca '¿CONFIGURAR CONTRASEÑA?' en la pantalla LCD y '0000'.



2. Si el panel está utilizando la contraseña predeterminada ('0000'), presione el botón ESC. A continuación, debería aparecer un mensaje en la pantalla LCD que indique 'ACCESO CONCEDIDO'. Si el panel ya tiene una contraseña, la ingresará ahora usando los botones blancos arriba y abajo y el botón ENTER (Nota: si no hay actividad de configuración durante 60 segundos, el Panel realizará un cierre de sesión forzado).



3. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique y configure la flecha indicadora en la pantalla LCD en 'OSDP' y luego presione el botón ENTER.



4. Ahora elegirá una dirección OSDP para realizar cambios o pruebas. Si no está seguro de cuál es la dirección, debe comenzar con 00. Usando los botones blancos hacia arriba y hacia abajo en el Panel, ubique la dirección que desea cambiar o probar y presione el botón Enter.



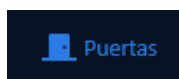
5. En el menú OSDP para la dirección que seleccionó, use los botones blancos hacia arriba y hacia abajo en el Panel para ubicar la opción de menú 4 Habilitar modo SC y presione la tecla ENTER.

Software: restricción de la comunicación OSDP al modo de canal seguro

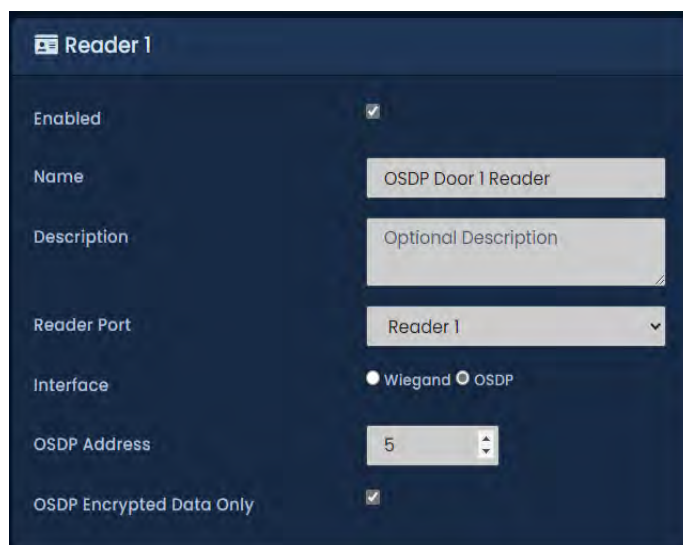


El último paso para asegurar sus lectores OSDP es configurar los ajustes del lector (desde el software) para restringir cualquier comunicación no segura. Utilice los siguientes pasos solo si las claves de cifrado ya se han enviado al controlador y los lectores se han cambiado al modo de canal seguro desde el menú LCD del panel.

1. Desde la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**, haga clic en el icono **Puertas** (en la imagen de abajo).



2. En la pantalla **Puertas**, verá que las Puertas que ya ha configurado se enumeran aquí. Haga clic en el botón azul junto a la puerta para la que está listo para terminar de configurar el modo de canal seguro.
3. En la pantalla **Editar puerta**, vaya a la pestaña **Lector 1** (es posible que deba repetir estos pasos para la pestaña Lector 2 si usa lectores consecutivos).
4. En la pestaña **Lector**, hay una casilla de verificación titulada **Solo datos cifrados OSDP**. Marque la casilla de verificación y haga clic en **Guardar** en la parte interior de la página.



5. Habilite solo datos cifrados OSDP en cualquier otro lector que deba configurarse y actualice sus paneles.

Capítulo 30. Placas de entradas / salidas

La placa de entrada/salida (IO-Board) es un controlador de entrada/salida de propósito general. Tiene la capacidad de conmutar sus relés de estado sólido integrados en función de programas o acciones predefinidas basadas en entradas de contacto seco. Se puede usar para monitorear hasta 16 puertas no administradas (puertas con cerraduras, contactos de puerta, entradas, pero sin lector) por controlador maestro o hasta 64 puertas monitoreadas (puertas que solo tienen contactos de puerta) por controlador maestro.

Este capítulo está diseñado para ayudarlo a planificar y configurar nuestras placas de entrada/salida.

Consejo

Si no planea usar ninguna placa de entrada/salida, puede omitir este capítulo con seguridad.

Números de pieza de la placa de E/S

Esta sección contiene números de pieza relevantes y sus descripciones. Los números de pieza generalmente tendrán una combinación de subconjuntos que se tratan con más detalle en la siguiente sección.

Tabla 30.1. Números de pieza de la placa de E/S

Número de parte	Descripción
VAX-IO	Kit básico de entrada/salida con VAX-MDK y módulo de expansión VAX-IO-EXP8-PCB. 12VDC alimentado con fuente de alimentación externa. Completo en caja de acero ventilada y con cerradura. Agregue hasta 7 expansores más para controlar hasta 64 E/S por controlador maestro.
VAX-IO-EXP8-PCB (IO-Board)	Placa de expansión de 8 pisos (o expansión de E/S de 8 puertos) solo sin gabinete (requiere el kit VAX-ELV-STR o VAX-IO para funcionar)

Configuración de Hardware

Esta sección cubre una descripción general de los componentes involucrados, la configuración del hardware para conectar las placas IO al controlador IO-Master y algunos ejemplos de hardware externo típico.

Lista de componentes:

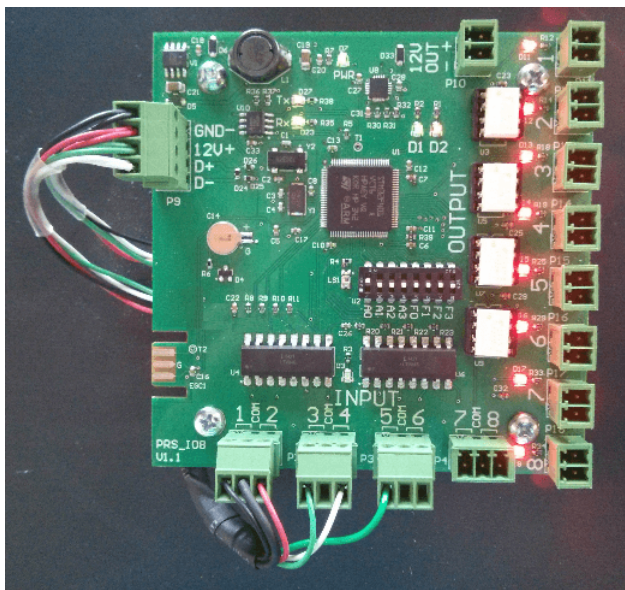
IO Master: Un controlador maestro, alimentado por energía de 12 VDC. Proporciona alimentación y comunicación a hasta 8 IO-Boards a través del bus RS-485 que proporciona hasta 64 entradas y 64 salidas.

IO-Board: placas secuenciales alimentadas y controladas por el panel IO-Master. Cada IO-Board está equipado con:

- 8 salidas de estado sólido:
- Contacto seco de relé de estado sólido, 30 VDC, límite de 500 mA, totalmente configurable, sin piezas mecánicas.
- Puede colocarse en horarios, cambiar de estado hasta 11 veces en un solo día.
- Configurable como normalmente cerrado o normalmente abierto.

- Se puede colocar en un horario de días festivos, cambiar de estado hasta 5 veces en un solo día festivo.
- Se puede manipular desde cualquier entrada en el mismo controlador IO-Master.
- 8 entradas de contacto seco:
- Puede activarse a través de botones, contactos de puerta, entradas de alarma, relés, sistemas externos.
- Se puede colocar en horarios para monitorear solo las entradas durante horas específicas. Hasta 5 cambios de horario en un solo día.
- Configurable como normalmente cerrado o normalmente abierto.
- Se puede configurar para activar varios eventos en cualquier salida en el mismo controlador IO-Master.

Figura 30.1. IO-Board



Si compra el controlador/placas IO en un kit, la comunicación y la alimentación entre el maestro IO y las placas IO estarán precableadas con tiras/rieles de interconexión.

Conexión del IO-Master a las IO-Boards

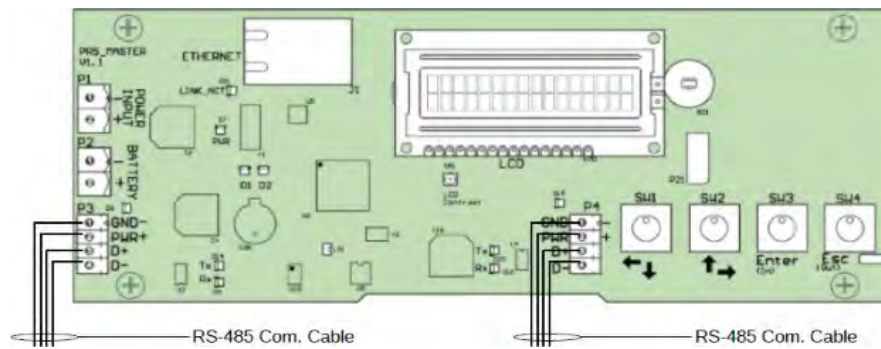
Los kits de E/S vendrán con las placas de E/S precableadas con cableado estándar o a través de tiras de interconexión convenientes. Esta sección se puede omitir si no planea conectar las placas IO de forma remota.

Conexión VAX-MDK RS-485

1. El controlador maestro tendrá dos puertos RS-485 + de alimentación dedicados (P3, P4) y, si se usan tiras de interconexión, 2 puertos cerca de la parte inferior de cada tira (EP2). Conecte las conexiones de alimentación a través de 2 conductores 18 AWG (GND, PWR+) y conecte las conexiones de datos a través de 2 conductores trenzados 18-22 AWG (D+, D-) al punto correspondiente en el expansor IO (P9).

Su panel debe verse exactamente como sigue:

Figura 30.2. Controlador maestro IO Conexiones RS-485



En la **primera placa IO**:

1. Conecte el otro extremo del par '12V a 'GND-' y '12V+' en el conector de 4 pines en el lado izquierdo de la placa IO. Asegúrese de que la polaridad coincida.
2. Si se utiliza más de una **placa de E/S**, se instalará un cable RS-485 adicional desde la primera placa de E/S hasta la segunda utilizando el mismo bloque de cabecera. Asegúrese de que la polaridad coincida. Continúe esta cadena para todas las tarjetas de expansión adicionales.

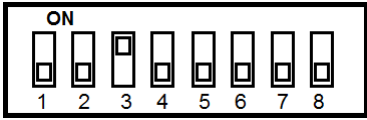
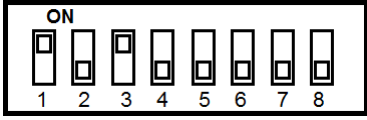
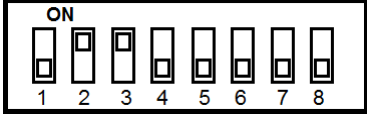
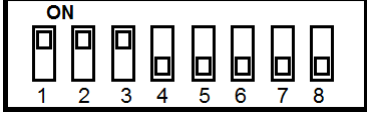
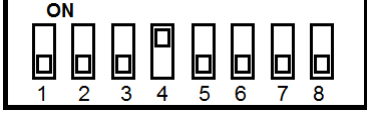
Configuración de las direcciones de la placa de E/S (I/O)

Cada **placa de IO (E/S)** en el bus **RS-485** requiere una dirección de panel secuencial. La dirección se configura usando los primeros **4 interruptores DIP en la placa E/S**. El primer IO-Board necesita una dirección de '1', el segundo una dirección de '2' y así sucesivamente.

El siguiente cuadro demostrará las posiciones de los **interruptores DIP** y la dirección de la **placa de E/S** correspondiente:

Tabla 30.2. Dirección del interruptor DIP del panel de expansión

Posición del interruptor DIP	Dirección del panel resultante
	Dirección del panel: 1 A3 ~ A0: 0001
	Dirección del panel: 2 A3 ~ A0: 0010
	Dirección del panel: 3 A3 ~ A0: 0011

Posición del interruptor DIP	Dirección del panel resultante
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 4 A3 ~ A0: 0100
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 5 A3 ~ A0: 0101
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 6 A3 ~ A0: 0110
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 7 A3 ~ A0: 0111
 A0 A1 A2 A3 F0 F1 F2 F3	Dirección del panel: 8 A3 ~ A0: 1000

Una vez que haya conectado sus placas de expansión al **panel maestro E/S** y configurado las **direcciones del panel** del interruptor DIP, ahora puede encender la **placa maestra E/S** a través de una fuente de alimentación de **12-13,7 VDC**. Puede cambiar los valores de los interruptores DIP mientras los controladores están encendidos.

Prueba de entrada/salida de la placa IO

La placa E/S se puede poner en modo de prueba a través de una configuración de interruptor DIP predefinida (todos los interruptores están en APAGADO excepto F3, consulte la figura a continuación). En el modo de prueba, la placa IO activará secuencialmente sus 8 salidas. Después de que se hayan probado las 8 salidas, se apagarán y las entradas estarán disponibles para la prueba. Para probar una entrada, simplemente cortocircuite la entrada y se activará la salida correspondiente. Si alguna de estas pruebas falla, comuníquese con Vicon Industries. *Consulte el Capítulo 37, Soporte.*

Figura 30.3. Interruptor DIP: Prueba de entrada/salida



Configuración del software de E/S

Esta sección cubrirá las diversas configuraciones de software necesarias para planificar e implementar con éxito un panel IO-Master y sus IO-Boards conectados.

La siguiente lista contiene cada uno de los componentes de software relevantes para la configuración de la placa E/S:

- Configuración de entrada/salida en la pantalla del panel de edición
- Horarios de entrada
- Programaciones de vacaciones de entrada
- Horarios de salida
- Programaciones de vacaciones de salida
- Grupos de vacaciones IO
- Puertas no administradas
- Puertas Monitoreadas


Agregar el panel maestro E/S a VAX

Agregar un panel maestro E/S a VAX es muy similar a agregar un panel de puerta. Esta sección repasa este proceso.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono **Paneles** (en la imagen a continuación).



4. En la pantalla **Ver paneles**, haga clic en el botón **Agregar**.

 **Consejo:** También puede acceder a la pantalla Agregar paneles desde la pantalla Paneles desconocidos, que completará automáticamente la mayor parte de la información.

En la pantalla **Agregar paneles**, se le presentarán varios menús desplegables, campos de texto y casillas de verificación para completar.

Asegúrese de que el menú desplegable Modelo de panel esté configurado en **VAX-IO-STR-2**.

Figura 30.4. Agregar pantalla de paneles

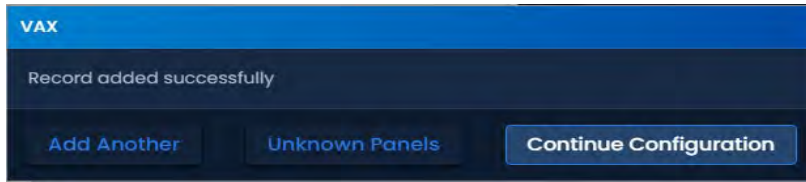
En la siguiente tabla se describen los campos a completar.

Tabla 30.3. Agregar Panel

Desplegable/Cuadro de texto/Casilla de verificación	Descripción
Modelo de panel	Seleccione VAX-IO-STR-2
Nombre	El nombre del Panel; Recomendamos nombrar el Panel según su ubicación en el sitio. Acepta de 4 a 60 caracteres.
Descripción	Descripción opcional del Panel. Acepta de 0 a 255 caracteres.
Sitio	Seleccione el sitio en el que residirá el Panel. Esto no se puede cambiar una vez que se agrega el Panel.
Dirección MAC	La dirección de red única integrada en cada Panel. Puede completarse previamente si está agregando el panel a través de una notificación de conexión desconocida desde el panel. Debe tener 12 caracteres.
Contraseña del panel	La contraseña necesaria para acceder al menú de administración integrado en el Panel. Los valores válidos son de 0 a 9999.
Expansores	La cantidad de IO-Boards conectadas al panel maestro de IO. Los valores válidos son del 1 al 8.
Conexión TCP: modo de conexión	El método en el que el Panel recibe su dirección IP, DHCP o Estática. Al seleccionar estático, aparecerán campos adicionales para completar

Una vez que haya completado los campos obligatorios, haga clic en el botón **Guardar** en la parte inferior de la pantalla.

Si tiene éxito, se le mostrará el mensaje: **'Panel agregado con éxito'** con las opciones para agregar un Panel adicional, o para continuar con la pantalla de edición del Panel que acabamos de agregar.



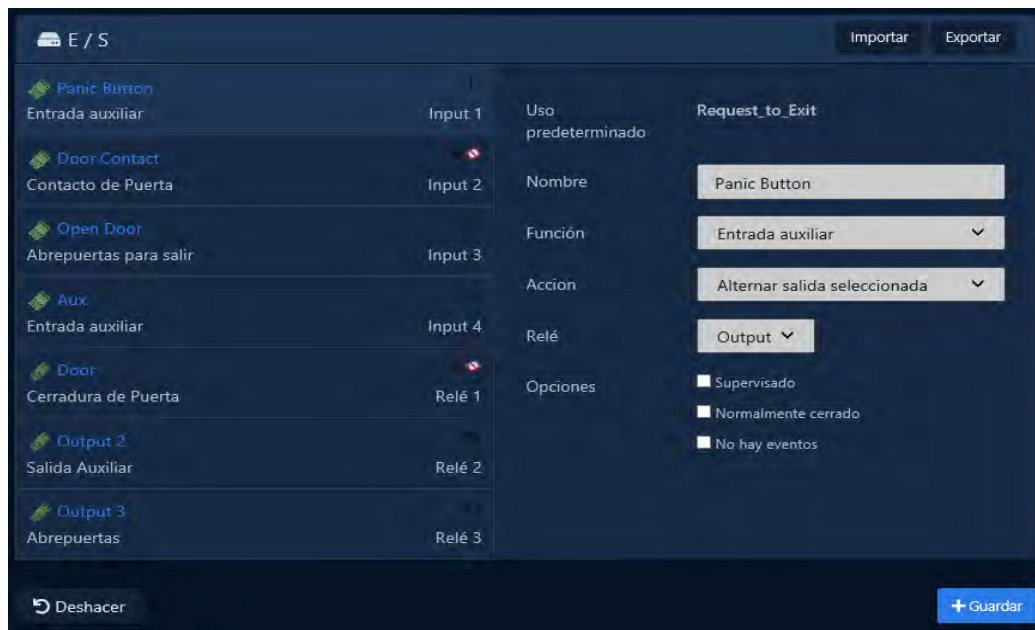
Configuración de entradas y salidas

Una vez que haya agregado el panel maestro IO, podrá editar las entradas y salidas en las placas E/S en el software.

1. Navegue a la pantalla Editar panel para el controlador maestro E/S.
2. Haga clic en la pestaña E/S en la pantalla Editar panel.
3. De manera predeterminada, todas las Entradas y Salidas estarán deshabilitadas. Puede cambiar entre qué placa de E/S está editando con el menú desplegable "Expansor de E/S" cerca de la parte superior.

Las entradas y salidas se enumeran en el lado izquierdo de la pantalla. La entrada / salida seleccionada será gris y sus opciones se mostrarán en el lado derecho.

Figura 30.5. Pestaña de E/S



La siguiente tabla muestra cada uno de los campos disponibles cuando se selecciona una Entrada:

Tabla 30.4. Opciones de entrada

Función	Descripción
Nombre	Nombre único de su Entrada. Acepta de 4 a 60 caracteres. Recomendamos nombrar su entrada según su función o dispositivo que se conectará a ella.
Función	La función dictará qué opciones de entrada están disponibles.

Función	Descripción
Tiempo de detección	Cuánto tiempo (en segundos) que la entrada debe cambiar de estado antes de que se considere "activada". Las acciones y alertas asociadas con la entrada no ocurrirán hasta que haya pasado el tiempo de detección.
Cronograma	Opcional. Seleccione un Programa de entrada de la lista desplegable. Este cronograma le indicará al Master E/S que solo monitoree esta entrada durante un tiempo específico.
Grupo de vacaciones	Opcional. Seleccione un Grupo de vacaciones de la lista desplegable. Esta opción le indicará al Master E/S que use un horario alternativo que se puede definir al agregar días festivos al sistema.
Acción	Elija de la lista de acciones disponibles. Las acciones disponibles se cubrirán en la siguiente tabla.
Opción: Supervisado	Elija si está utilizando resistencias para supervisar la entrada de manipulación (se puede ignorar en la mayoría de los casos).
Opción: Normalmente Cerrado/Invertido	Elija si la entrada está normalmente cerrada. Este es el caso a menudo con contactos de puerta

Funciones de entrada VAX-IO-STR-2

Los paneles VAX-IO-STR-2 tienen funciones de entrada adicionales debido a una mayor potencia de procesamiento. Se utilizan para puertas no gestionadas y supervisadas. Consulte la sección llamada "Puertas no administradas y monitoreadas con placas E/S" para obtener más información.

Tabla 30.5. Funciones de entrada VAX-IO-STR-2

Función	Descripción
Contacto de puerta	Esta función de entrada se usa para entradas que rastrean si la puerta está abierta o cerrada, como los contactos magnéticos de la puerta. También conocido como interruptor de posición de puerta.
Solicitud de salida	Permite utilizar la entrada como REX. Esto permitirá que un botón pulsador u otra entrada de contacto seco desbloquee la puerta asociada.
Sensor de movimiento	Esta función de entrada se utiliza para sensores de movimiento externos. Desbloquear por movimiento debe estar desmarcado en Opciones de configuración de puerta para que el sensor de movimiento desbloquee la puerta. De forma predeterminada, el sensor de movimiento evitará la alarma de apertura forzada.
Entrada auxiliar	Esta función de entrada tiene la mayoría de las opciones configurables, incluidas acciones de entrada, como salidas pulsantes, anulación de puertas, activación de alarmas.

Acciones:

Las acciones son opcionales al configurar Entradas; estas acciones pueden apuntar a una sola o hasta 5 salidas conectadas al mismo panel maestro E/S. Solo las salidas configuradas como salidas auxiliares pueden ser objeto de una acción. Las siguientes son las diversas acciones que puede realizar con Entradas.

Tabla 30.6. Acciones de entrada VAX-IO-STR-2

Acción	Descripción
Sin acción	Las acciones son opcionales; aún se generará un evento cuando se cumplan las condiciones de entrada y aún se puedan ejecutar los activadores de secuencias de comandos del lado del servidor.
Activar salida	Activa una salida, seleccionable a través de la lista desplegable.
Alternar salida	Cambia una salida al estado opuesto, seleccionable a través de la lista desplegable.
Desactivar salida	Desactivar la salida seleccionada, seleccionable a través de la lista desplegable.
Salida de pulso alta	Pulse una salida para cerrar, configure un retraso y la duración del pulso
Salida Pulso Bajo	Pulse una salida para abrir, configure un retardo y la duración del pulso.
Pulso de salida opuesto	Pulse una salida al contrario de su estado actual, configure un retraso y la duración del pulso.
Activar salida múltiple	Active múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Desactivar Salida Múltiple	Desactive múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista
Alternar salida múltiple	Alterne múltiples salidas desde una sola entrada. Se pueden seleccionar hasta 5 salidas. Utilice la tecla CTRL cuando haga clic en Salidas de la lista.
Inhabilitar entrada	Deshabilitar una entrada seleccionada. Seleccionable de una lista desplegable con retraso y duración.
Puerta no administrada - Resumir	Reanuda una puerta no administrada a su programación normal en función de su programación de salida.
Puerta no administrada - Invalidar bloqueo	Anular una puerta no administrada seleccionada a un estado bloqueado. El estado permanecerá hasta que se reanude el comando
Puerta no gestionada - Invalidar desbloqueo	Anular una puerta no administrada seleccionada a un estado desbloqueado. El estado permanecerá hasta que se reanude el comando.
Puerta no administrada: Invalidar bloqueo con reanudación automática	Anular una puerta no administrada seleccionada a un estado bloqueado. El estado reanudará su horario normal en la próxima transición programada en el Horario de salida.
Puerta no administrada: Invalidar el desbloqueo con reanudación automática	Anular una puerta no administrada seleccionada a un estado desbloqueado. El estado reanudará su horario normal en la próxima transición programada en el Horario de salida.

 **Consejo**

Los paneles VAX-IO-STR-2 tienen una acción de entrada adicional llamada "Activar". Le permite elegir que ocurra una acción adicional y se puede combinar con otras funciones de entrada, como el contacto de la puerta y la solicitud de salida.

Figura 30.6. Opciones de Entradas

La siguiente tabla muestra cada uno de los campos disponibles cuando se selecciona una Salida:

Table 30.7. Output Options

Función	Descripción
Nombre	Nombre único de su Salida. Acepta de 4 a 60 caracteres. Recomendamos nombrar su salida según su función o el dispositivo que se conectará a ella.
Función	La función dictará qué opciones de salida están disponibles.
Puerta asociada	Seleccione a qué puertos de puerta o nombre de puerta se asociará la salida.
Horario	Opcional. Seleccione un programa de salida de la lista desplegable. Este programa le indicará al IO-Master que solo monitoree esta entrada durante un tiempo específico.
Grupo de Festivos	Opcional. Seleccione un Grupo de festivos de la lista desplegable. Esta opción le indicará al Master E/S que use un horario alternativo que se puede definir al agregar días festivos al sistema.
Opción: Normalmente Cerrado	Elija si la salida está normalmente cerrada.
Opciones: Sin eventos	Las salidas con esta opción seleccionada no generarán eventos cuando la salida cambie de estado.
Opciones: Protegido	Las salidas con esta opción seleccionada no pueden ser objeto de ninguna acción de entrada.
Opciones: inicialmente activado (si no se seleccionó ningún horario)	La Salida comenzará como "activada" (cerrada) hasta que se vea afectada por una acción de Entrada o Anulación del servidor.

Funciones de Salidas VAX-IO-STR-2

Los paneles VAX-IO-STR-2 tienen funciones de entrada adicionales debido a una mayor potencia de procesamiento. Se utilizan para puertas no gestionadas y supervisadas. Consulte la sección llamada "Puertas no administradas y monitoreadas con IO-Boards" para obtener más información.

Table 30.8. funciones de entrada VAX-IO-STR-2

Función	Descripción
Cerradura de la puerta	Configura la salida para que actúe como si hubiera una cerradura conectada, como una cerradura de puerta, una cerradura magnética, un portón, etc. Utiliza el programa de salida establecido en las opciones de salida.
Cerradura de puerta secundaria	Configura la salida para seguir el estado del cerradero asociado a la misma puerta.
Puerta desbloqueada o abierta	Configura la salida para que se active cuando la puerta asociada está abierta a través del estado de contacto de la puerta o abierta desbloqueada según el estado de contacto de la puerta
Zumbador externo	Configura la salida para que se active cuando la puerta asociada se fuerza o se mantiene abierta.
Zumbador global	Configura la salida para que se active cuando cualquier puerta en el mismo panel VAX-IO-STR-2 se fuerza o se mantiene abierta. Configurable qué puertas harán esto.
Salida auxiliar	Salida de uso general que puede tener una programación basada en la programación de salida. Puede cambiar el estado en función de anulaciones o acciones de entrada

Figura 30.7. Opciones de Salidas

The screenshot shows a configuration window with a dark blue background. It contains the following fields and options:

- Name:** A text input field containing "Output 1-1".
- Function:** A dropdown menu with "Door Strike" selected.
- Associated Door:** A dropdown menu with "Test Panel 2 Door 1" selected.
- Options:** Two checkboxes: "Normally Closed" (unchecked) and "No Events" (checked).

Horarios de entradas y salidas

Esta sección cubrirá los horarios de entrada y salida. Las entradas y salidas en las placas E/S se pueden colocar en un horario.

Horarios de entradas

Los horarios de entrada son horarios que puede colocar en las entradas para dictar cuándo se monitoreará y cuándo se ignorará la entrada.

Hay dos modos disponibles: No supervisado y Supervisado. En un solo día, puede cambiar entre estos modos hasta 5 veces.

Para agregar un programa de entrada:

1. En la **barra lateral**, desplácese hacia abajo hasta **Programación**; haga clic en el icono **Horarios** (en la imagen a continuación). Seleccione la pestaña **Entradas** (en la imagen a continuación).



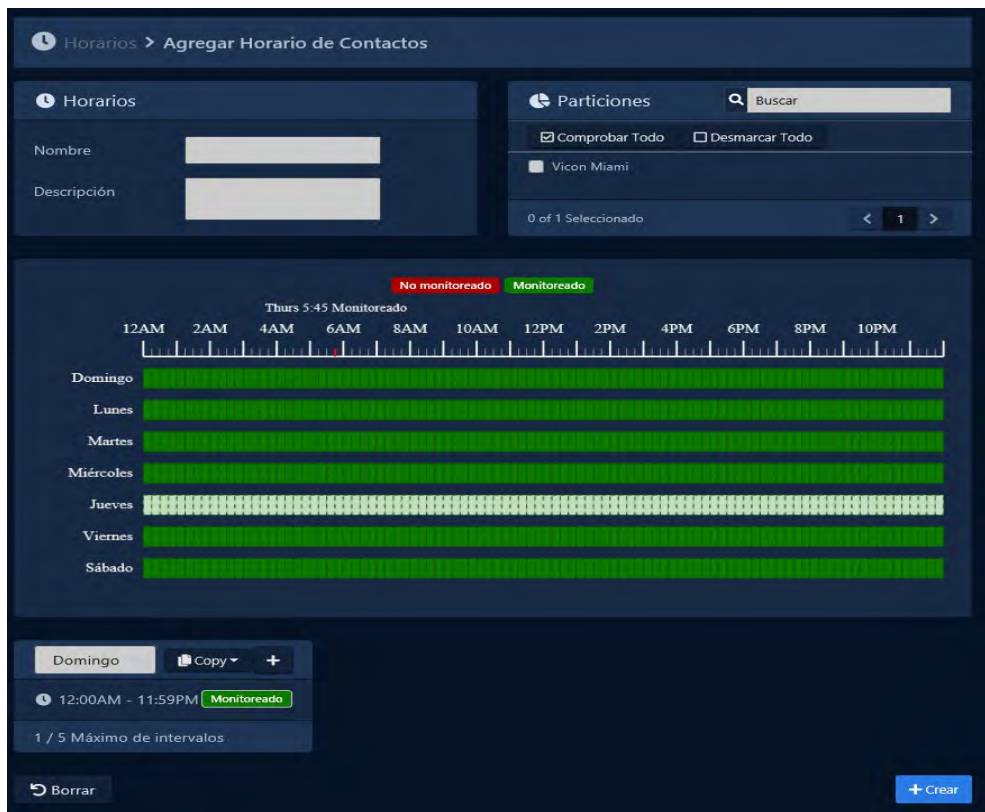
2. En la pantalla **Ingresar** horarios, verá los horarios predeterminados. Si se necesitan horarios de entradas adicionales, haga clic en el botón **Agregar** en esta pantalla.
3. En la pantalla Agregar horario de entrada, tendrá un par de cuadros de texto para completar.

Tabla 30.9. Agregar horario de entrada

Texto	Descripción
Nombre	Nombre único de su Horario. Acepta de 4 a 255 caracteres. Recomendamos nombrar sus Horarios por la función de los horarios.
Descripción	Descripción opcional del Horario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este programa. Si se selecciona más de una, se creará una copia para cada partición.

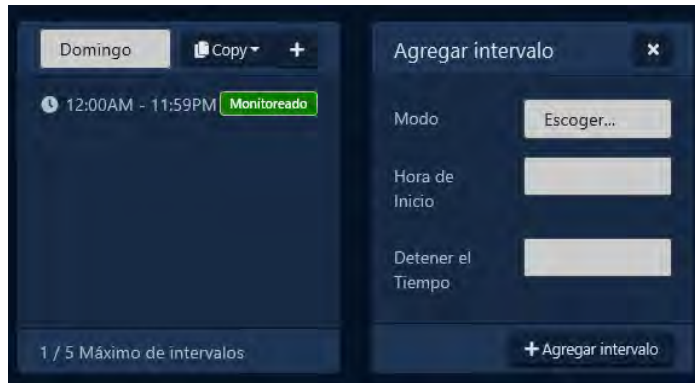
4. Crear el **Horario** es el último paso para crear un Horario de Entrada. A continuación se muestra el aspecto de la parte de programación de la página Agregar programación.

Figura 30.8. Horario de Entrada



- Haga clic en cualquiera de las barras horizontales en el cronograma para que aparezca el **widget Editor de horario**. El widget del editor de horarios es una herramienta simple y poderosa para crear horarios.

Figura 30.9. Editor de Horario



- Utilice el menú desplegable **Modo** para seleccionar el estado de entrada para el período de tiempo seleccionado. Esto es útil para definir en qué estado estará la entrada durante todo el día, o cambiar el modo para intervalos ya presentes.
- La sección **Agregar intervalo** del editor de horarios tiene 3 campos que se usan para agregar un intervalo de horario de entrada. Cuando se hace clic en los campos **Inicio y Parada**, aparecerá un menú deslizante para seleccionar las horas de inicio y parada. El segundo menú desplegable **Modo** dictará qué estado de entrada seguirá el programa durante el período de tiempo definido. Una vez que haya completado estos campos, haga clic en el botón **Agregar**.
- Ahora debería ver la barra que seleccionó codificada por colores según el período de tiempo que agregó. Agregue períodos de tiempo adicionales a ese día si es necesario.

Si desea que el horario que ha creado se use para varios días diferentes, puede hacer clic en la barra con su horario completo y seleccionar la lista desplegable Copiar para seleccionar en qué día de la semana se debe copiar el horario. El cronograma se replicará en función de la opción de fecha seleccionada.

- Una vez que su horario de entrada para los 7 días sea el deseado, ahora puede presionar **Guardar** para crear el Calendario de entrada en las particiones seleccionadas. El programa de entrada ahora se puede asignar a las entradas al agregar o crear paneles Master E/S.

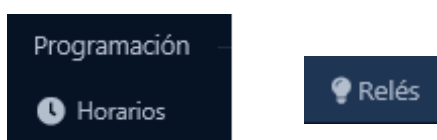
Horarios de Salidas

Los horarios de salida son horarios que puede colocar en las salidas para dictar cuándo se abrirán o cerrarán (activadas o desactivadas).

Hay dos modos disponibles: encendido y apagado. En un solo día, puede cambiar entre estos modos hasta 11 veces.

Para agregar un programa de salida:

- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en el icono **Horarios** (en la imagen a continuación). Seleccione la pestaña **Salida**, (en la imagen a continuación).



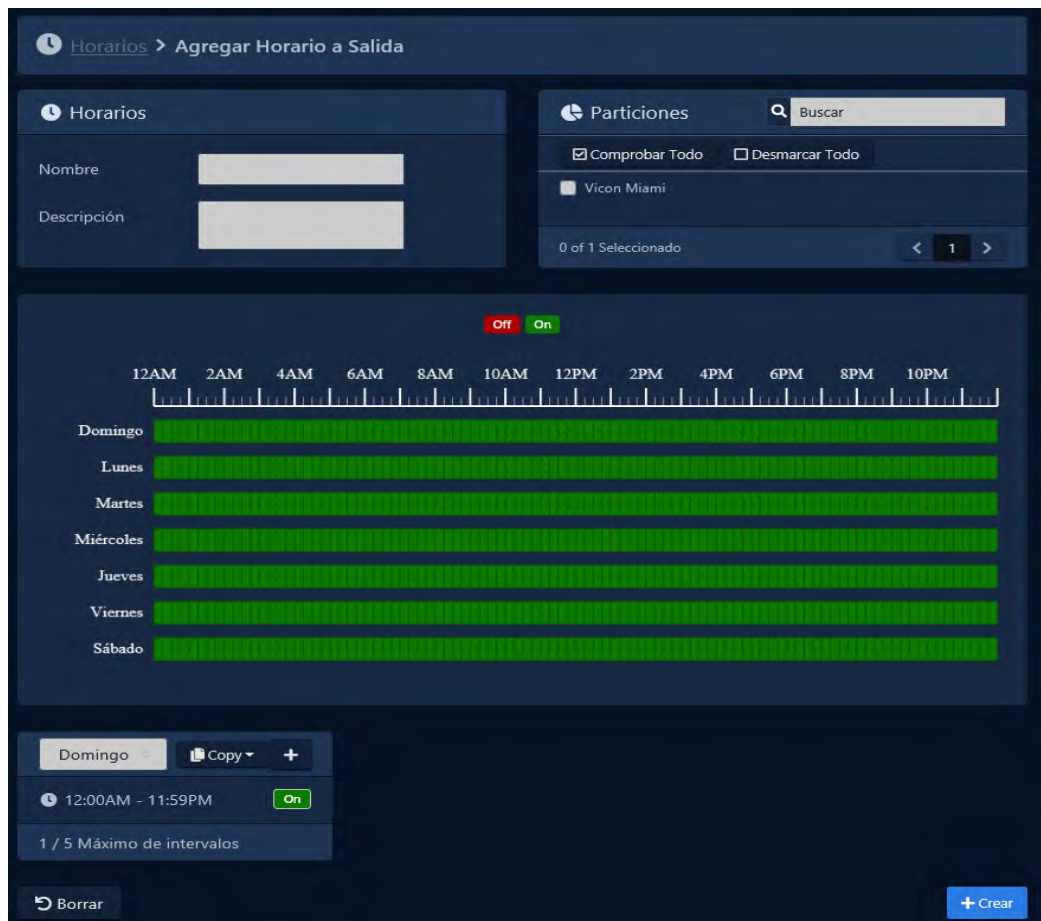
2. En la pantalla **Horarios de salida**, verá los Horarios predeterminados. Si se necesitan horarios de salida adicionales, haga clic en el botón **Agregar** en esta pantalla.
3. En la pantalla Agregar programa de salida, tendrá un par de cuadros de texto para completar.

Tabla 30.10. Agregar horario de salida

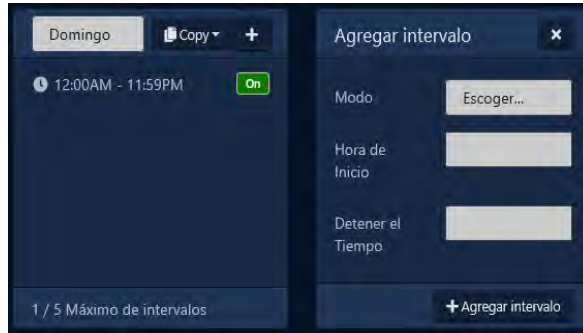
Texto	Descripción
Nombre	Nombre único de su Horario. Acepta de 4 a 255 caracteres. Recomendamos nombrar sus Horarios por la función de los horarios.
Descripción	Descripción opcional del Horario. Acepta de 4 a 255 caracteres.
Particiones	Seleccione las particiones en las que le gustaría crear este programa. Si se selecciona más de una, se creará una copia para cada partición

4. 4. Crear el Horario es el último paso para crear un **Horario de Entrada**. A continuación se muestra el aspecto de la parte de programación de la página **Agregar**.

Figura 30.10. Horario de Salidas



5. Haga clic en cualquiera de las barras horizontales en el Horario para que aparezca el **widget Editor de horario**. El widget del editor de horarios es una herramienta simple y poderosa para crear horarios.

Figura 30.11. Widget del editor

6. Utilice el menú desplegable **Modo** para seleccionar el estado de la salida para el período de tiempo seleccionado. Esto es útil para definir en qué estado estará la salida durante todo el día, o cambiar el modo para intervalos ya presentes.
7. La sección **Agregar intervalo** del editor de horarios tiene 3 campos que se usan para agregar un intervalo de horario de salida. Cuando se hace clic en los campos **Inicio y Parada**, aparecerá un menú deslizante para seleccionar las horas de inicio y parada. El segundo menú desplegable **Modo** dictará qué estado de entrada seguirá el programa durante el período de tiempo definido. Una vez que haya completado estos campos, haga clic en el botón **Agregar**.
8. Ahora debería ver la barra que seleccionó codificada por colores según el período de tiempo que agregó. Agregue períodos de tiempo adicionales a ese día si es necesario.

Si desea que el horario que ha creado se use para varios días diferentes, puede hacer clic en la barra con su horario completo y seleccionar la lista desplegable Copiar para seleccionar en qué día de la semana se debe copiar el horario. El cronograma se replicará en función de la opción de fecha seleccionada.
9. Una vez que su horario de salida para los 7 días sea el deseado, ahora puede presionar **Guardar** para crear el Calendario de entrada en las particiones seleccionadas. El programa de salida ahora se puede asignar a las entradas al agregar o crear paneles Master E/S.

Puertas no administradas y monitoreadas con las Placas E/S

Las puertas no administradas y monitoreadas son aberturas que no tienen acceso controlado (lector o método de control de acceso) pero sí tienen otros herrajes de puerta, como contactos de puerta como cerrojos de puerta. La entrada del contacto de la puerta se usa para determinar si la puerta está abierta o cerrada. Se pueden configurar acciones adicionales para que ocurran cuando se abre la puerta. Esta sección revisará cómo agregar este tipo de puertas.

El siguiente cuadro define la diferencia entre estos tipos de puertas:

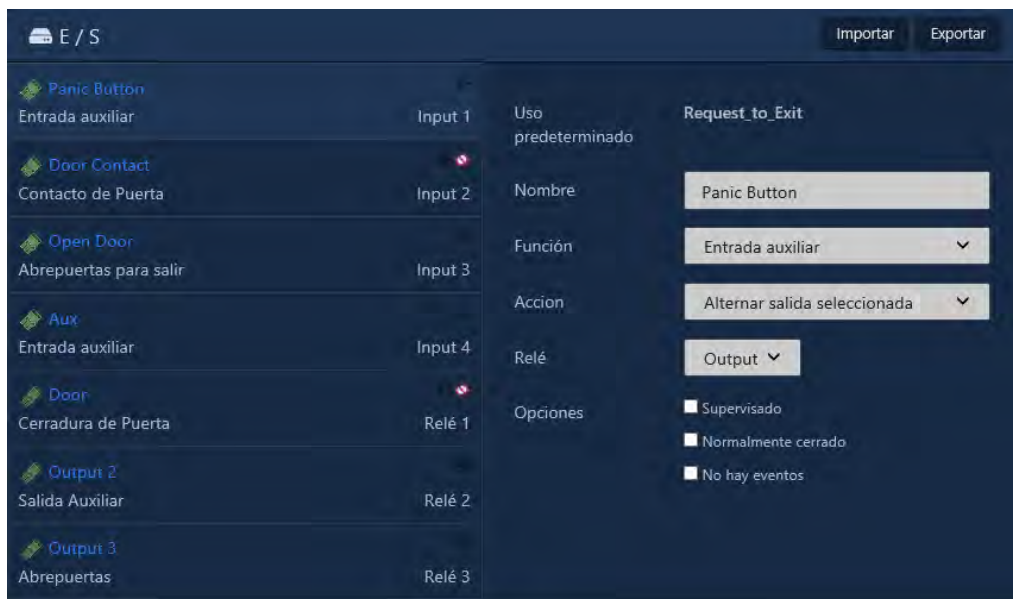
Tabla 30.11. Tipos de puertas E/S y características

Tipo de puerta	Tipo de panel admitido	Características
monitoreado	VAX-IO-STR-2	Solo admite asociaciones de contacto de puerta y cámara. Funciones de salida limitadas. 64 Límite de puerta por VAX-IO-STR-2
no administrado	VAX-IO-STR-2	Admite contacto de puerta, golpe de puerta, REX, sensor de movimiento, asociaciones de cámara, anulación remota y funciones de salida adicionales. Límite de 16 puertas por VAX-IO-STR-2

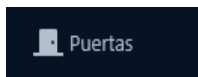
Use los siguientes pasos para configurar una puerta no administrada o monitoreada.

1. Navegue a la pantalla **Editar panel** para el controlador Master E/S al que está conectando su puerta no administrada (Inicio, Paneles, Editar panel) .
2. Haga clic en la **pestaña E/S** en la pantalla Editar panel. Utilice el menú desplegable **Expansor de E/S** y seleccione el expansor apropiado al que está conectado el hardware de su puerta.
3. Seleccione la entrada a la que está conectado el hardware de su puerta en el lado izquierdo de la página.
4. Puede cambiar el nombre de la entrada para que el sistema sea más fácil de entender.
5. Cambie el menú desplegable Función a Contacto de puerta o la función adecuada. El contacto de la puerta debe configurarse antes de poder agregar una puerta supervisada.
6. Opcionalmente, puede configurar la entrada para realizar otras acciones como lo haría con cualquier otra entrada. Es posible que desee configurar la entrada como normalmente cerrada si la función es un contacto de puerta.

Figura 30.12. Contacto de puerta de placa de E/S



7. Para las entradas y salidas de VAX-IO-EXP8-PCB, debe seleccionar una puerta asociada para que la entrada funcione. Repita el proceso anterior para cualquier entrada y salida conectada al hardware de la puerta.
8. Después de cambiar las entradas requeridas a los contactos de la puerta u otras funciones de entrada y salida, haga clic en Guardar en la parte inferior de la página.
9. Desde la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**, haga clic en el icono **Puertas** (en la imagen de abajo).



10. En la pantalla Puertas, verá que las Puertas que ya ha configurado se enumeran aquí. Haga clic en **Agregar** botón en esta pantalla.

11. En la pantalla **Agregar puerta**, seleccione **Sin administrar** como Tipo de puerta.
12. Seleccione la placa de E/S a la que está conectado su contacto de puerta en el menú desplegable **Panel**.
13. Seleccione la entrada a la que está conectado el contacto de su puerta en el menú desplegable **Entrada**.

Figura 30.13. Agregar pantalla de puerta

Tipo de Puerta	Tipo	Paneles soportados	Características
<input checked="" type="radio"/>	Administrado	1D, 2D, MDK	Soporta hasta 2 lectores, Abridor Automático, Anti-Passback, Cámaras
<input type="radio"/>	Monitoreado	IO-STR, IO-STR-2	Solo Admite Contacto de Puerta y Cámaras
<input type="radio"/>	No		
<input type="radio"/>	Administrado	IO-STR-2	Soporta Contacto de Puerta, Chapa y Cámaras

Nombre:

Descripción:

Panel:

El maximo de Puertas ya estan configuradas o no se han definido suficientes chapas en el panel

14. Haga clic en **Guardar**.
15. Una vez agregado, podrá cambiar la configuración específica de la puerta, asociar una cámara a la puerta y ver el estado de la puerta en la página de descripción general del sistema, el visor de mapas y otros. Las notificaciones relacionadas con la puerta aparecerán como otras notificaciones de puertas.

Aplicaciones de la vida real para entradas y salidas

Al utilizar múltiples funciones de entrada y salida, las tarjetas de E/S se pueden usar para una gran variedad de propósitos. A continuación se presentan varias situaciones comunes en las que los integradores de seguridad han utilizado nuestras placas de E/S.

Disparador de acción del sistema de cámaras:

La mayoría de los sistemas NVR/DVR de cámara modernos admiten entradas de contacto seco que pueden desencadenar acciones específicas como "comenzar a grabar la cámara abajo" o "cambiar la posición de la cámara a la ubicación B". Al utilizar ciertas funciones de salida de nuestros controladores de puerta regulares, puede conectar uno de los relés adicionales a una entrada en una placa IO. Los controladores de puerta ahora se pueden configurar para enviar una señal a los sistemas de cámara a través de las placas IO en función de parámetros específicos como:

- Puerta forzada o mantenida abierta
- Puerta desbloqueada o abierta

Dispositivos/Sistemas Externos:

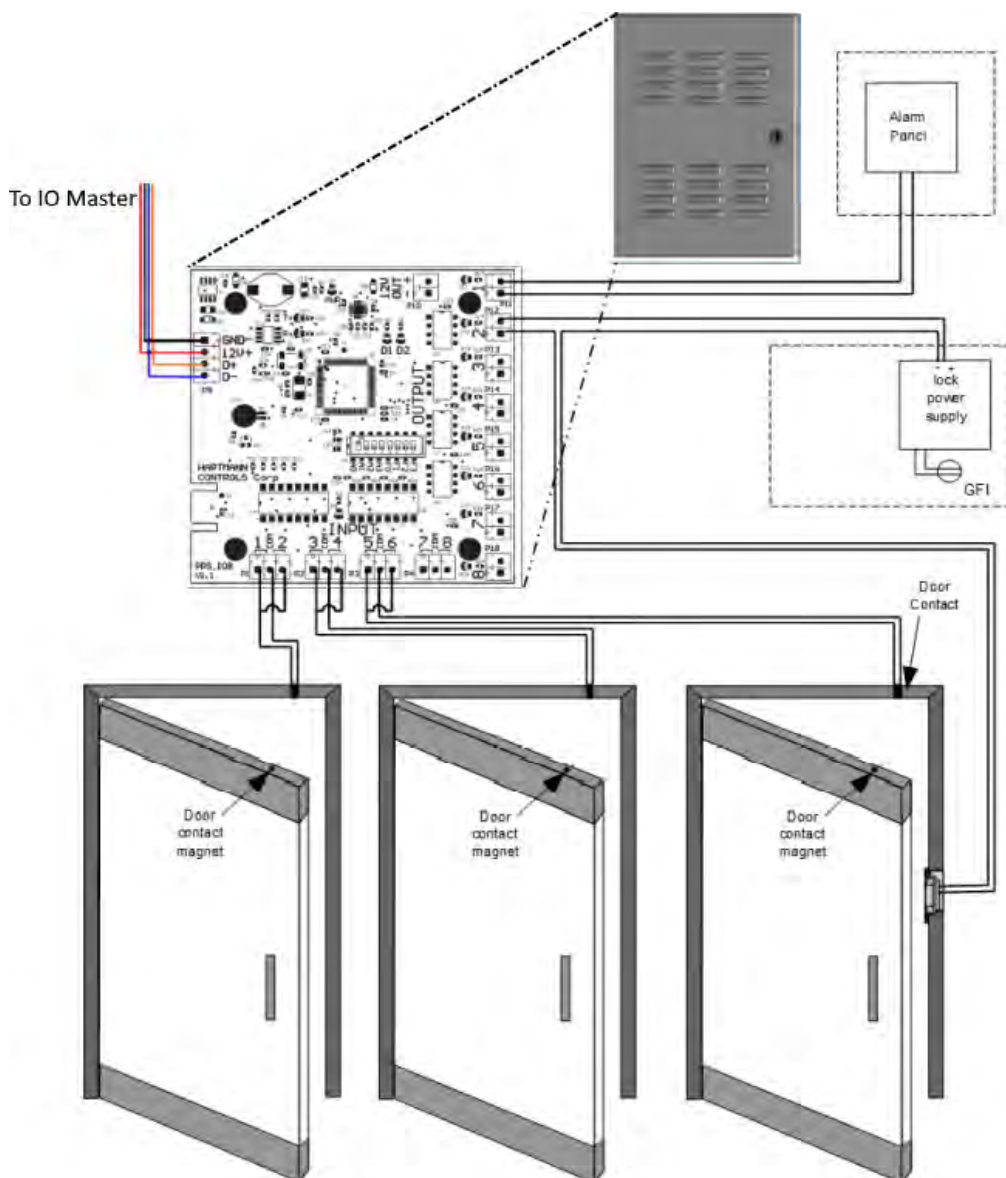
Es posible que otros sistemas y dispositivos externos interactúen con las placas de E/S, siempre que puedan proporcionar a la placa de E/S un contacto seco para cerrar la entrada a una de las conexiones a tierra comunes en la placa de E/S. Esto puede incluir varias entradas, como sensores, botones, interruptores o dispositivos de salida, como motores o luces. La siguiente tabla muestra algunos ejemplos de dispositivos externos que pueden interactuar con la placa E/S:

Tabla 30.12. Dispositivos Externos

Dispositivos	Descripción
Detector de rotura de cristal	Nombre único de su Salida. Acepta de 4 a 60 caracteres. Recomendamos nombrar su salida según su función o el dispositivo que se conectará a ella.
Detector de rotura de cristal	Conecte múltiples detectores de rotura de cristales para recibir rápidamente una notificación de un evento de rotura de cristales y notificar al sistema de alarma.
Rayos fotoeléctricos	Supervise estos haces fuera del horario comercial para detectar intrusos. Utilice salidas para avisar al sistema de alarma y activar sirenas/luces.
Sensores de movimiento	Supervise los sensores de movimiento fuera del horario comercial para detectar intrusos. Utilice salidas para avisar al sistema de alarma y activar sirenas/luces.
Detectores de choque	Se puede utilizar en una gran variedad de aplicaciones.
Sensor de temperatura	Configure el sensor para que solo se active cuando se cumplan los criterios de temperatura específicos.
Botones/Interruptores	Los botones y los interruptores de llave pueden activar fácilmente una entrada en la placa E/S.

Los siguientes diagramas demuestran cómo se pueden conectar algunos dispositivos externos a la placa E/S.

Figura 30.14. Ejemplo de Placa E/S



Capítulo 31. Integración del sistema de cámaras

VAX es capaz de integrarse con una variedad de software de gestión de video (VMS) y algunas grabadoras de video en red (NVR). La integración con los sistemas VMS le permite realizar las siguientes funciones:

- Integrar con cámaras de múltiples sistemas VMS, incluidas instancias a través de LAN/WAN/Internet.
- El monitoreo de video en tiempo real muestra las cámaras importadas desde el VMS directamente en su navegador web. El video en tiempo real se puede mostrar en función de alertas predefinidas, como puerta abierta, puerta abierta forzada, etc.
- Asociar cámaras a Puertas y Ascensores. Asocie las cámaras PTZ en función de las posiciones preestablecidas de la cámara.
- Vinculación de video y notificaciones basadas en eventos predefinidos proporcionados por el software de control de acceso.

VAX actualmente se integra con los siguientes sistemas de gestión de video:

Tabla 31.1. Sistemas de gestión de video

Sistema	Versión Mínima	Notas
ViconNet	8.0	El servidor web debe estar habilitado.
Milestone xProtect	2016	El servidor web debe estar habilitado.
Exacq exacqVision	7.4.3	El servidor web debe estar habilitado. Se necesita generar certificado SSL.
Digital Watchdog DW Spectrum	2.4	El servidor web debe estar habilitado.
Vicon Valerus	1.2	Es posible que sea necesario generar un certificado SSL.

Navegadores soportados

Esta sección mostrará qué sistemas de cámara son compatibles con qué navegadores web.

Table 31.2. Sistemas de gestión de video

Sistema	Versión Mínima	Notas
Vicon Valerus	Internet Explorer 11	<ul style="list-style-type: none">• Requiere Valerus Plug-in.• Soporta múltiples cámaras en matriz.• Buena calidad de video y rendimiento.• Latencia de video muy baja.• Sin soporte móvil.
Vicon ViconNet	Internet Explorer 11	<ul style="list-style-type: none">• Requiere Silverlight Plug-in.• Soporta múltiples cámaras en matriz.• Admite ajustes de iris y enfoque.• Buena calidad de video y rendimiento.• Sin soporte móvil.

Sistema	Versión Mínima	Notas
Milestone xProtect	Internet Explorer 11 Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	<ul style="list-style-type: none"> • Utiliza HTML5, compatible con muchas plataformas. • Stream utiliza JPEG, rendimiento y calidad medios. • Aparece en pantalla cuando se detecta grabación o movimiento. • Compatible con dispositivos móviles.
Exacq exac-qVision	Internet Explorer 11 Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	<ul style="list-style-type: none"> • Utiliza HTML5, compatible con muchas plataformas. • Stream utiliza JPEG, rendimiento y calidad medios. • Soporta Web Sockets. • Compatible con dispositivos móviles.
Digital Watchdog DW Spectrum	Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	<ul style="list-style-type: none"> • Utiliza transmisión HTML5 a través del protocolo WebM. • Buena calidad de video y rendimiento. • Almacena la transmisión en vivo, lo que provoca un retraso de 5 a 10 segundos para el video en tiempo real. • Soporte móvil limitado.

Habilitar el servidor web/móvil del VMS

Esta sección describirá lo que se requiere antes de que VAX pueda sincronizar y ver cámaras en el VMS.

Cada sistema necesitará su respectivo servidor web VMS habilitado. Para obtener detalles más específicos sobre cómo habilitar y configurar el servidor web en un VMS específico, comuníquese con el distribuidor/instalador del VMS o el fabricante del VMS.

Habilitar servidor web: configuración de Valerus

1. Valerus tendrá habilitado el servidor HTTP de forma predeterminada.
2. Importe o cree un certificado SSL autofirmado como se describe en la documentación de Valerus o en el soporte de Vicon.
3. Continúe con la sección llamada "Agregar un sistema de cámara".

Habilitar servidor web: configuración de ViconNet

1. Inicie sesión en un Núcleo ViconNet.
2. Habilite el servidor web y móvil de ViconNet como se describe en la Guía de instalación y configuración de ViconNet.
3. Si está utilizando HTTPS (recomendado), use un navegador web y busque la URL del servidor ViconNet. Acepte las advertencias del certificado y continúe.

4. Debe agregar el certificado Self-Signed ViconNet SSL; este proceso se describe en la sección llamada "Agregar certificados de sitio web para la integración de la cámara".
5. Continúe con la sección llamada "Agregar un sistema de cámara".

Habilitar servidor web: Milestone XProtect Mobile

1. Inicie sesión en el servidor que aloja Milestone XProtect.
2. Instale el componente Milestone Mobile Server como se describe en el Manual del administrador de XProtect Mobile.
3. Cree un certificado SSL autofirmado a través del administrador de certificación XProtect Mobile.
4. Configure la configuración de IFrame con los siguientes pasos:
 - a. Vaya a "C:\Program Files\Milestone\Milestone Mobile Server\Web" en el servidor de Milestone Mobile.
 - b. Copie y pegue la carpeta "C:\Archivos de programa (x86)\Vicon\VAX\WebServer\milestone" del servidor web VAX en la carpeta web del paso anterior. Cambie el nombre de la carpeta de hitos a VAX.
 - c. En el servidor Milestone Mobile, abra VideoOS.MobileServer.Service.exe.config desde el directorio de instalación con privilegios administrativos. Puede utilizar un programa de edición de archivos como el bloc de notas.
 - d. Busque la clave "Content-Security-Policy". Agregue "https://computer:11001" al final de "frame-src 'self'". debería verse como:

```
<add key="Content-Security-Policy" value="default-src 'self'; script-src 'self'; connect-src 'self' ws://* wss://*; img-src 'self' data: blob;; style-src 'self' 'unsafe-inline'; frame-src 'self' https://VAX:11001" />
```
 - e. Busque la clave "PlainTextAuthenticationEnabled". Establezca el valor como "Verdadero".
 - f. Busque la clave "X-Frame-Options". Elimine "DENY" del valor. Deje el valor en blanco o configúrelo en "ALLOW-FROM https://servername:11001".
5. Utilice un navegador web y busque la URL del servidor de XProtect Mobile. Acepte las advertencias del certificado y continúe.
6. Debe agregar el certificado Self-Signed XProtect Mobile SSL; este proceso se describe en la sección denominada "Adición de certificados de sitios web para la integración de la cámara".
7. Continúe con la sección llamada "Agregar un sistema de cámara".

Habilitar servidor web: Exacq exacqVision Web Services

1. Inicie sesión en el servidor que aloja exacqVision.
2. Habilite el servicio web de exacqVision como se describe en el Manual del usuario del servicio web.
3. Use un navegador web y busque la URL de la interfaz web de exacqVision. Acepte las advertencias del certificado y continúe.
4. Debe agregar el certificado SSL autofirmado exacqVision; este proceso se describe en la sección denominada "Adición de certificados de sitios web para la integración de la cámara".
5. Continúe con la sección llamada "Agregar un sistema de cámara".

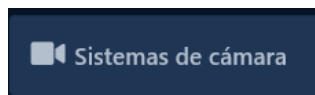
Habilitar servidor web: Digital Watchdog DW Spectrum

1. El servidor web de DW Spectrum debe estar habilitado de forma predeterminada.
2. Si está utilizando HTTPS (recomendado), use un navegador web y busque la URL de la interfaz web de DW Spectrum. Acepte las advertencias del certificado y continúe.
3. Debe agregar el certificado SSL de DW Spectrum autofirmado; este proceso se describe en la sección denominada "Adición de certificados de sitios web para la integración de la cámara".
4. Continúe con la sección llamada "Agregar un sistema de cámara".

Agregar un sistema de cámaras

Agregar un sistema de cámara (VMS) le permite asociar cámaras a puertas/ascensores y ver reproducción histórica y video en tiempo real.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el icono de **sistemas de cámara** (en la imagen a continuación).



4. En la pantalla **Sistemas de cámara**, verá cualquier otro sistema de cámara que ya haya agregado. Puede conectarse a múltiples sistemas de cámara si es necesario. Haga clic en el botón **Agregar** en esta pantalla.

Figura 31.1. Pantalla para agregar un sistema de cámaras

 Una captura de pantalla de la interfaz de usuario de un sistema de cámaras. El título de la ventana es "Integrador de cámara". Hay una advertencia roja que indica que VAX requiere el uso de HTTPS. Abajo hay un formulario con los siguientes campos:

Nombre	Necesario
Tipo de Integrador	Escoger...
Dirección	ex. https://localhost
Nombre de Usuario	Nombre de Usuario
Contraseña	
Horarios	(UTC-05:00) Eastern Time (US & Canada)
Partición	Vicon Miami
Retraso de reproducción	-10

 En la parte inferior izquierda hay un botón "Borrar" y en la parte inferior derecha un botón "+ Crear".

5. En la pantalla **Agregar sistema de cámara**, tendrá algunos cuadros de texto para completar.

Tabla 31.3. Agregar sistema de cámara

Texto	Descripción
Nombre	Nombre único de su sistema de cámara. Acepta de 2 a 255 caracteres. Recomendamos nombrar su sistema de cámara según la ubicación o la función.
Tipo de integrador	Elija el tipo de integrador correcto según el VMS con el que desea integrarse.
DIRECCIÓN	La dirección del servidor/computadora que aloja el VMS. Puede ser un nombre o una dirección IP. Incluya el encabezado http/https. Incluya el número de puerto que usa el software de administración de video si no usa el puerto predeterminado 80. El número de puerto solo es necesario si no usa el puerto predeterminado 80 (http) o 443 (https).
Nombre de usuario	El nombre de usuario que se utilizará para acceder al VMS. Esto se puede ubicar en el software de administración de su cámara.
Contraseña	La contraseña de la cuenta VMS que accederá al VMS. Esto se puede ubicar en el software de administración de su cámara.
Zona horaria	La zona horaria local en la que residirá el sistema de la cámara.
Particion	La partición en la que se ubicará el sistema de la cámara.
Retraso de reproducción	Número de segundos de diferencia para sincronizar el tiempo de notificación con el tiempo de grabación

6. Una vez que haya completado los campos obligatorios, ahora puede presionar **Guardar** para crear el sistema de cámara en la partición seleccionada. Se le pedirá que agregue otro sistema o que continúe con la configuración del sistema de cámara que acaba de agregar.

Advertencia

Si el VMS usa HTTPS (recomendado), es probable que deba agregar el certificado SSL del VMS a cualquier computadora cliente que esté viendo cámaras a través de VAX. Consulte la sección llamada "Agregar certificados de sitio web para la integración de la cámara" para obtener más detalles sobre este proceso.

Gestionar sistemas de cámaras

Una vez que haya agregado un sistema de cámara, el siguiente paso es sincronizar las cámaras disponibles desde el VMS y habilitar qué cámaras le gustaría integrar con VAX.

Si acaba de agregar un sistema de cámara, al hacer clic en "**Continuar con la configuración**" accederá a la pantalla **Administrar cámaras**; de lo contrario:


1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el icono de **sistemas de cámara** (en la imagen a continuación).



2. En la pantalla **Sistemas de cámara**, verá cualquier sistema de cámara que ya haya agregado. Haga clic en el botón azul de edición junto al sistema de cámara que desea modificar.

Una vez en la pantalla **Administrar sistemas de cámara** para un sistema de cámara específico, el siguiente paso es sincronizar las cámaras (recuperar una lista de cámaras o grupos de cámaras disponibles) y seleccionar a qué cámaras desea que el Sistema de control de acceso tenga acceso.

- Haga clic en el botón desplegable "**Sincronizar cámaras**" y elija si desea sincronizar todas las cámaras en el sistema de cámaras o por ciertos grupos de cámaras (si el VMS lo admite). La sincronización de cámaras por grupos le permite importar grupos predefinidos desde el software de administración de cámaras; esto es útil en sitios con una gran cantidad de cámaras.

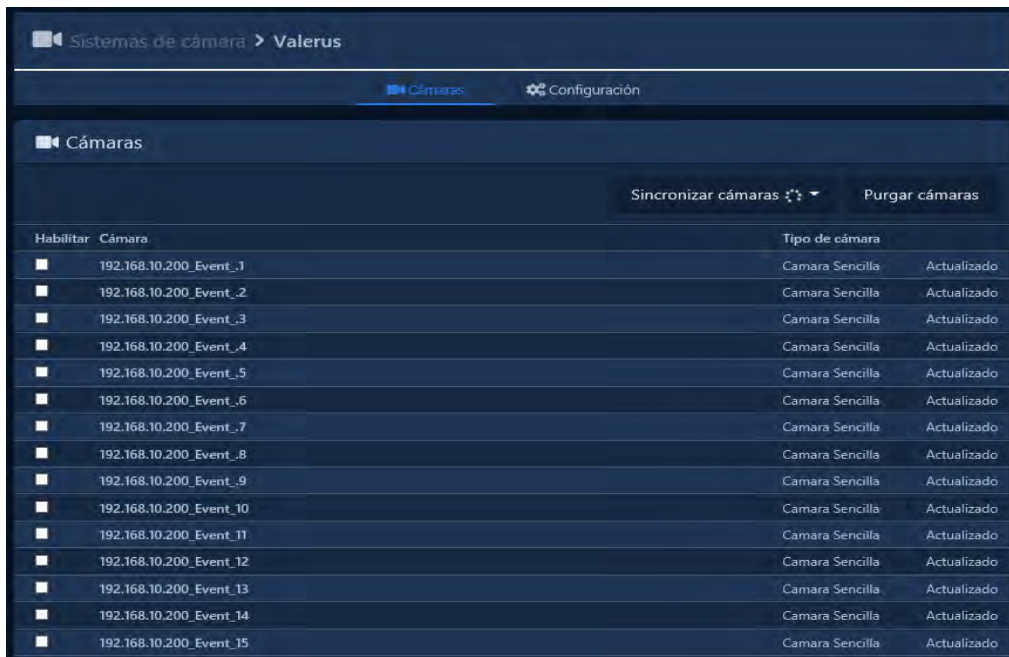
 **Nota:** Dependiendo de la cantidad de cámaras en el software de administración de video, este proceso puede demorar algunos minutos. El proceso también le permitirá saber si falla al comunicarse con el servidor.

- Una vez que se complete el proceso de sincronización, verá una lista de cámaras disponibles que se recuperó del sistema VMS.
- Cada cámara en la lista contendrá el nombre de la cámara importada del VMS, el tipo de cámara, si es una cámara nueva o faltante y si la cámara está habilitada.
- La casilla de verificación Habilitar al lado de cada cámara dicta si la cámara está disponible para el Sistema de control de acceso para asociación o visualización de puertas.

Advertencia

Una vez que se habilita una cámara, esto contará para el límite de cámaras impuesto por la licencia de su producto.

Figura 31.2. Pantalla de gestion de camaras




Habilitar	Cámara	Tipo de cámara	
<input type="checkbox"/>	192.168.10.200_Event_1	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_2	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_3	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_4	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_5	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_6	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_7	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_8	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_9	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_10	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_11	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_12	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_13	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_14	Camara Sencilla	Actualizado
<input type="checkbox"/>	192.168.10.200_Event_15	Camara Sencilla	Actualizado

Depurar Cámaras

Cuando se elimina o cambia el nombre de una cámara en el software de gestión de cámaras, será necesario volver a sincronizar las cámaras. Si el software de control de acceso detecta que una cámara que estaba disponible previamente ya no existe, se etiquetará como "No encontrada". Cuando esto sucede, y no se espera que la cámara vuelva a estar disponible, podemos purgar la cámara del sistema. Esto eliminará la cámara y todas las asociaciones que la cámara tiene con Puertas y Ascensores.

Para eliminar cámaras que ya no existen, simplemente sincronice las cámaras para detectar cuáles ya no están disponibles; haga clic en el botón "**Depurar cámaras**" una vez si ve alguna cámara que está "No encontrada".

Figura 31.3. Depurar cámaras

Purgar cámaras


Aceleración de GPU

En la pestaña de configuración de la página **Editar sistema de cámara**, hay una opción titulada **Aceleración de GPU** que puede aparecer si el VMS lo admite. Esta opción se usa para tomar prestada potencia de procesamiento de la tarjeta de video de la computadora cuando los clientes están viendo las cámaras; esto puede ayudar a descargar la carga de la CPU en la computadora cliente.

 **Nota:** Esta característica requiere una tarjeta de video compatible y un navegador web.

WebSockets

La opción de configuración Use WebSockets puede aparecer si el VMS lo admite. Esta opción se usa para usar el protocolo de transporte WebSocket y puede hacer que el transporte de la reproducción de la cámara sea más eficiente.

 **Nota:** Esta característica requiere sistemas operativos compatibles (Windows 8 o superior).

Uso de Proxy

Esta es una opción exclusiva para Valerus. Cuando está habilitado, las solicitudes para ver y los comandos a las cámaras utilizarán el servidor web VAX como un proxy para las solicitudes web. Esto evitará algunos errores de certificado SSL cuando se utilice HTTPS.

Visualización de cámaras sincronizadas

La visualización de cámaras en VAX se puede realizar de varias formas; también admitimos la vista de cámara en línea que se puede activar en función de eventos como Acceso denegado o Puerta forzada abierta. Esta sección cubrirá la visualización de video en vivo y la reproducción de video.

Advertencia

Para ver las cámaras en VAX a través de la comunicación HTTPS, primero debe crear una relación de confianza entre la computadora cliente que busca VAX y el servidor web VMS. Para hacer esto, debemos importar un certificado del servidor VMS o la certificación SSL debe registrarse con una Autoridad de certificación válida. Consulte la sección llamada "Adición de certificados de sitio web para la integración de la cámara" para obtener más detalles sobre este proceso.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**; haga clic en el ícono **Visor de cámaras** (en la imagen a continuación).



En la pantalla Visor de cámara, tendrá varias opciones para ver las cámaras en su sistema.

Figura 31.4. Visor de camaras



 **Consejo**

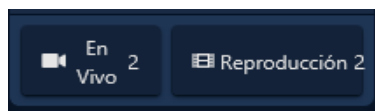
Puede ver rápidamente la transmisión en vivo de una sola cámara haciendo clic directamente en el ícono de la cámara junto al nombre de cada cámara en esta pantalla.

Visualización de vídeo en Vivo

To view live video on the View Cameras screen, input the following parameters:


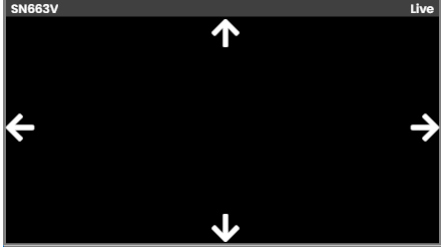

1. **Sistema de cámara:** seleccione el sistema de cámara que le gustaría ver.
2. **Tamaño de matriz:** si el VMS admite una matriz de video, puede seleccionar un tamaño de matriz. De forma predeterminada, el sistema elegirá automáticamente el mejor tamaño para la cantidad de cámaras que está viendo.
3. **Modo:** seleccione Vídeo en directo como modo.
4. **Cámaras:** Seleccione qué cámaras le gustaría ver. Puede seleccionar varias cámaras si el VMS admite una matriz de video.
5. Una vez que haya seleccionado la(s) cámara(s), ahora puede hacer clic en el botón "**Ver video en vivo**" en esta pantalla.

Figura 31.5. Visor de camaras



6. Aparecerá una nueva ventana sobre su pantalla actual. Este es el visor de la cámara. Mostrará video en vivo de la cámara que seleccionó. Tendrás varias opciones en esta pantalla; algunos dependerán del tipo de cámara o VMS que esté viendo:

Tabla 31.4. Ver opciones de cámara

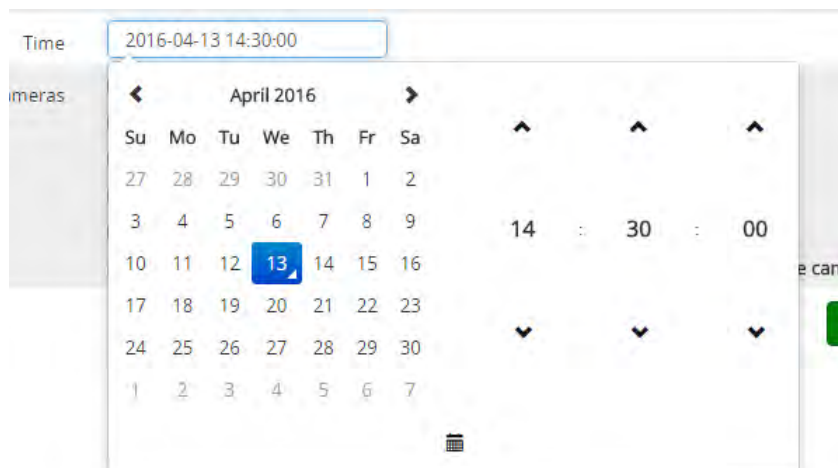
Opción	Descripción
	Este botón cambiará el modo de cámara a reproducción. Puede usar la flecha hacia arriba para seleccionar dónde comenzar la reproducción en función de la hora actual o seleccionar una hora con el selector de fecha y hora.
	Solo PTZ. Pan Speed influirá en la rapidez con la que se moverá una cámara PTZ al cambiar de posición manualmente o con paneo automático
	Solo PTZ. El botón Aplicar moverá la cámara a la posición predeterminada seleccionada; esto también le permite establecer valores predeterminados basados en la posición actual de la cámara con el botón Configurar.
Calidad de la cámara	Sólo ExacQ. Se puede seleccionar baja calidad para ahorrar ancho de banda a expensas de la calidad de la transmisión.

7. Si su pantalla está negra o tiene algún error en la parte inferior, como "Error al recuperar el video" o "fuente", consulte el capítulo correspondiente en nuestra Guía técnica.


Visualización de reproducción de video

Para ver la reproducción del video en la pantalla **Ver cámaras**, ingrese los siguientes parámetros o haga clic en:

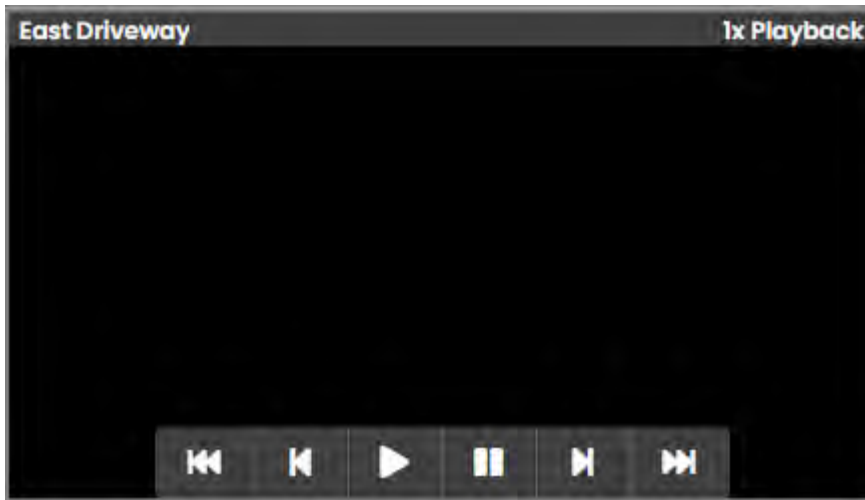
- Sistema de cámara:** Seleccione el sistema VMS que le gustaría ver.
- Tamaño de matriz:** si el VMS admite una matriz de video, puede seleccionar un tamaño de matriz. De forma predeterminada, el sistema elegirá automáticamente el mejor tamaño para la cantidad de cámaras que está viendo.
- Modo:** seleccione Reproducir video como el modo.
- Hora:** cuando se selecciona el modo Reproducción de video, se deberá completar el campo Hora. Al hacer clic en el cuadro de texto, se presentará el widget de fecha y hora; seleccione la hora a la que le gustaría ver la reproducción del video.



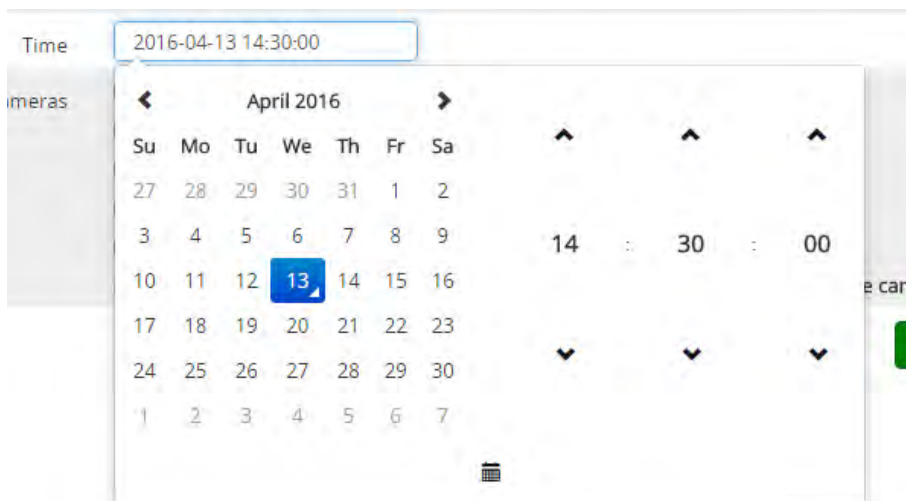
5. **Cámaras:** Seleccione qué cámaras le gustaría ver.
6. Una vez que haya seleccionado las cámaras, ahora puede hacer clic en el botón "Ver video de reproducción" en esta pantalla.
7. Aparecerá una nueva ventana; este es el visor de la cámara de reproducción. Comenzará la reproducción a la hora seleccionada.

 **Consejo:** Puede volver al video en vivo en cualquier momento presionando el botón Video en vivo en el visor de la cámara.

8. En el visor de la cámara, tendrá opciones específicas para la reproducción de video.



9. Puede elegir un nuevo tiempo para la reproducción del video haciendo clic en el botón que se muestra a continuación:



Asociación de cámaras con puertas y elevadores

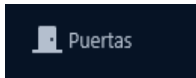
VAX permite que el soporte para cámaras se asocie con puertas/ascensores. Esto es para que las notificaciones se puedan vincular a la reproducción de video.

Las asociaciones de puerta/ascensor con cámaras también nos permiten mostrar una vista de cámara en línea cuando se producen alertas en una puerta asociada con esa cámara, como Puerta abierta forzada y Puerta mantenida abierta.

Use los siguientes pasos una vez que sus cámaras hayan sido sincronizadas y habilitadas en el sistema:

Asociaciones de cámara: Puerta

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el icono de **Puertas** (en la imagen de abajo).



2. En la pantalla **Puertas**, verá las Puertas que ya ha configurado enumeradas aquí. Haga clic en el botón azul junto a la puerta para la que desea configurar una asociación de cámara.
3. En la pantalla **Editar puerta**, verá que hay 6 pestañas, cada una con sus propios elementos de configuración. Haga clic en la pestaña **Asociación de cámaras**; aquí es donde configuraremos asociaciones de cámaras para esta puerta.

Figura 31.6. Pestaña de asociación de cámara en la pantalla Editar puerta



4. Select the camera you would like to associate with the door. If the VMS supports matrix views, you may select more than one.

Consejo : Puede asociar una cámara con una posición preestablecida si la cámara es una cámara PTZ

Asociaciones de cámara: Elevador

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Hardware**; haga clic en el ícono de **Elevadores** (en la imagen a continuación).



2. En la pantalla **ascensores**, verá los ascensores que ya ha configurado enumerados aquí. Haga clic en el botón azul junto al ascensor para el que desea configurar una asociación de cámara.
3. En la pantalla **Editar Elevador**, verá que hay 4 pestañas, cada una con sus propios elementos de configuración. Haga clic en la pestaña **Asociación de cámaras**; aquí es donde configuraremos asociaciones de cámaras para este ascensor.

Figura 31.7. Pestaña de asociación de cámara en la pantalla Editar Elevador.

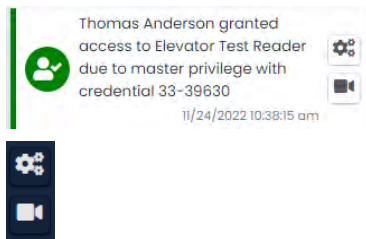
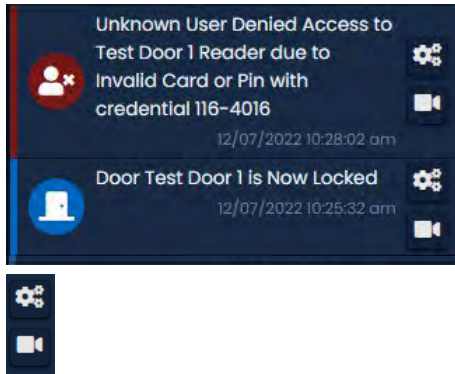


4. Seleccione las cámaras que le gustaría asociar con el elevador.

Consejo : Puede asociar una cámara con una posición preestablecida si la cámara es una cámara PTZ

Notificaciones de cámaras

Una vez que una cámara se asocia con una puerta/ascensor, aparecerá un ícono junto a todas las notificaciones relacionadas con ese dispositivo, incluido el video en vivo y la reproducción. Al hacer clic en el ícono de la cámara, aparecerá un visor de cámara de reproducción que coincidirá con la hora del evento. Todos los informes también tendrán un enlace de cámara junto a cada entrada que incluya un dispositivo con una cámara asociada.

Figura 31.8. Notificaciones de puerta con enlace de cámara**Figura 31.9. Notificaciones de Elevador con enlace de cámara****Figura 31.10. Informe de actividad de puerta con enlace de cámara**

11/24/2022 09:41:21 am	Default Site	Test Door 1 Reader 1	Test User 1 Test1 34-55892	Test User 1 Test1 granted access to Reader 1 due to master privilege with credential 34-55892
------------------------	--------------	----------------------	----------------------------	---

Configuración de alertas de cámara en vivo

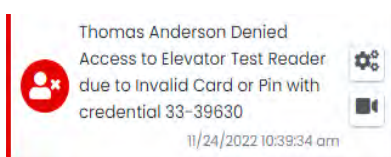
Una vez que las puertas y los ascensores tienen asociaciones de cámaras, VAX admite la configuración de mensajes de eventos para mostrar una transmisión de video en línea sobre el área de notificaciones.

Esto es útil para eventos de tiempo crítico, como puerta forzada abierta, puerta abierta o tarjetas a las que se le niega el acceso a un área segura. Esta sección repasará la configuración de estas alertas.

Figura 31.11. Vista de cámara en línea basada en acceso denegado

La **configuración de notificaciones** específicas para su uso con el visor de cámara en línea se cubre en la sección llamada "**Reglas de cámara en vivo**".

Podemos abrir una pantalla externa para notificaciones de video en vivo usando el botón resaltado a continuación.



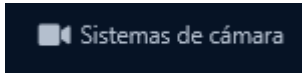
Mientras esta pantalla externa esté abierta, las notificaciones con la opción de video en vivo se mostrarán en la nueva ventana, no en la barra de notificaciones.

Adición de certificados de sitio web para la integración de cámaras

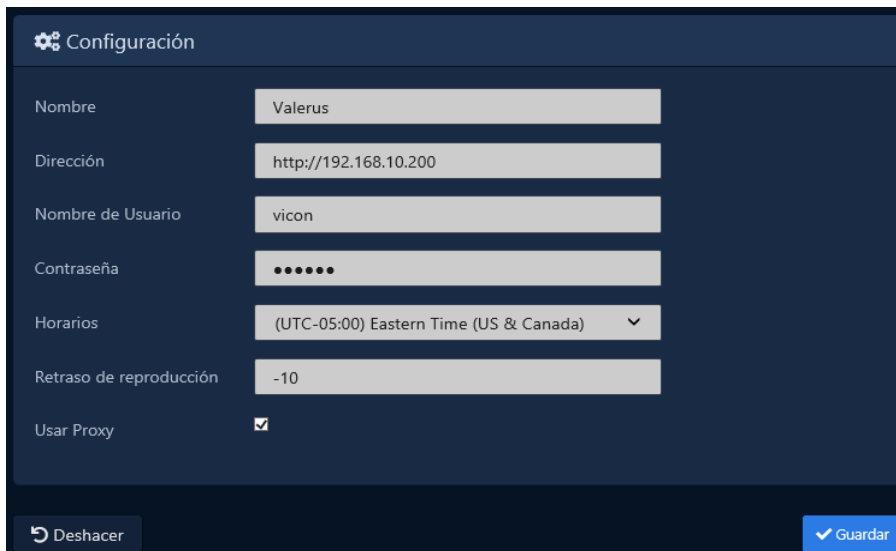
VAX utiliza comunicación segura HTTPS segura. Si el VMS también usa HTTPS, debemos crear una "confianza" entre la PC cliente y el VMS. Si el servidor web de VMS utiliza un certificado autofirmado (a diferencia de un certificado oficial comprado a una empresa, como godaddy.com), debe agregar la certificación autofirmada generada por el servidor web de VMS. Esto no se aplica si está utilizando una comunicación HTTP normal.

Las siguientes instrucciones funcionarán en la mayoría de los sistemas operativos y navegadores web.

1. **Inicie sesión en VAX.** En la página principal, desplácese hacia abajo hasta la sección titulada "**Hardware**"; haga clic en el icono de **sistemas de cámara**.



2. admin Haga clic en el botón azul de edición junto al sistema de cámara para el que desea **agregar una certificación**. Haga clic en la pestaña "**Configuración**".

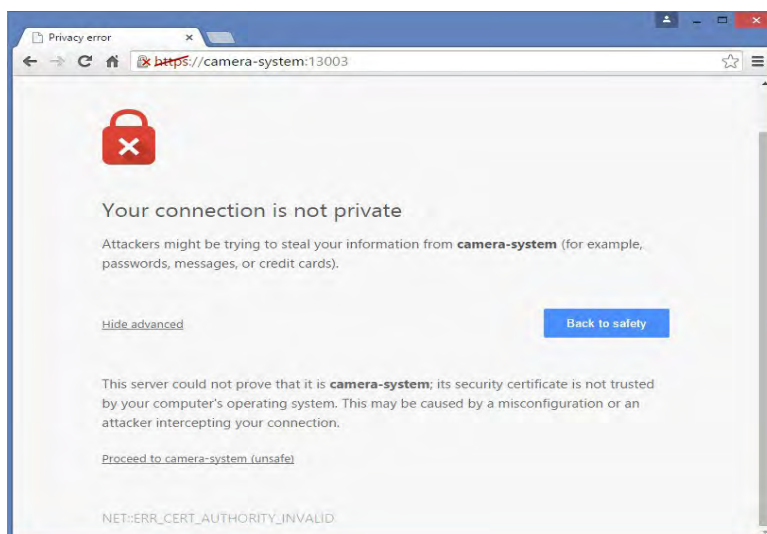


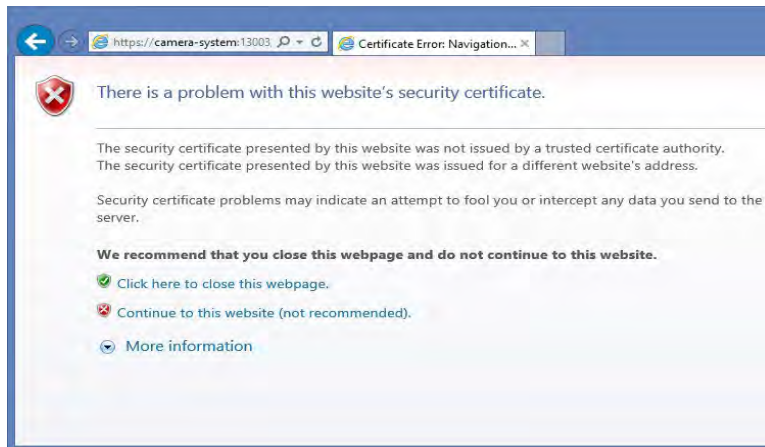
Configuración

Nombre	Valerus
Dirección	http://192.168.10.200
Nombre de Usuario	vicon
Contraseña	•••••
Horarios	(UTC-05:00) Eastern Time (US & Canada) ▼
Retraso de reproducción	-10
Usar Proxy	<input checked="" type="checkbox"/>

Deshacer Guardar

3. En la pestaña de configuración, copie el cuadro de texto titulado "Dirección". Tendremos que buscar esta dirección en otra pestaña de nuestro navegador web para recuperar el archivo de certificación. Copie la URL y colóquela en la barra de direcciones del navegador web. Presione **enter** y debería ver el siguiente mensaje (dependiendo de su navegador).

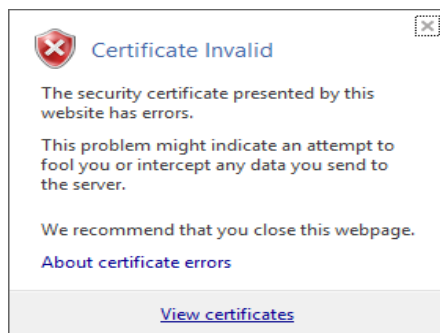




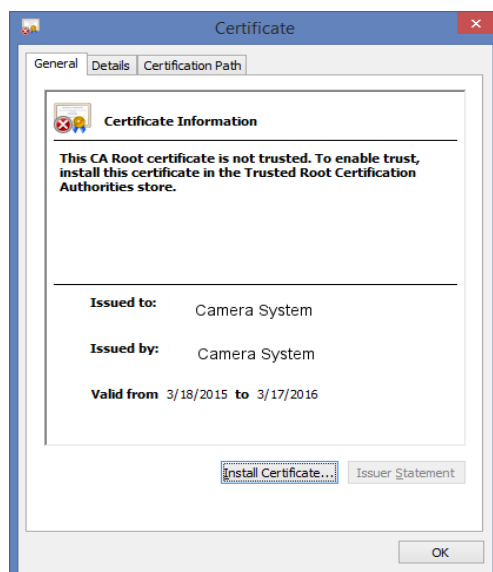
4. El siguiente paso es extraer la certificación para que podamos instalarla en nuestro equipo.

Importación de certificación en Internet Explorer

1. En Internet Explorer, haga clic en "**Continuar a este sitio web**"; una vez que se cargue el sitio, verá un botón rojo en la URL titulado "**Error de certificado**". Haga clic en este botón; aparecerá una pequeña ventana emergente. Haga clic en "**ver certificados**".

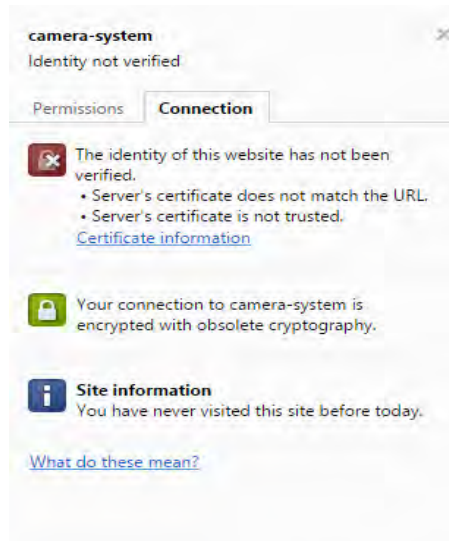


2. En la **ventana de certificados**, haga clic en "**instalar certificado**" en la parte inferior de la ventana. Aparecerá el asistente de importación de certificados. Vaya a la sección llamada "**Importación de certificados** con el asistente de importación de certificados" para continuar con el proceso de importación de certificados.



Importación de certificación en Google Chrome.

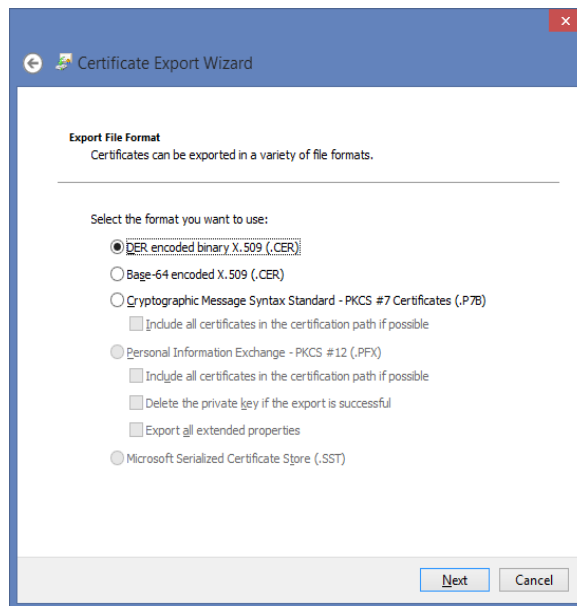
1. In Google Chrome: Once you see the message "Your connection is not private", click on the icon that looks like a padlock in the URL with an "X" through it. A small window will appear.



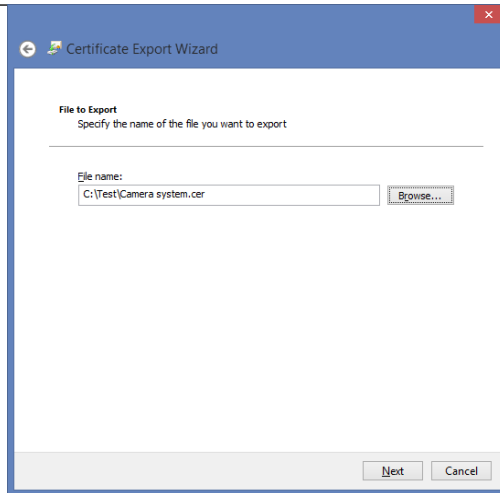
2. En esta ventana, haga clic en el enlace titulado "**Información del certificado**". Una ventana nueva aparecerá. Haga clic en la pestaña **Detalles** de esta ventana.

Click on the "Copy to File" button on this screen. This will launch the Certificate Export Wizard

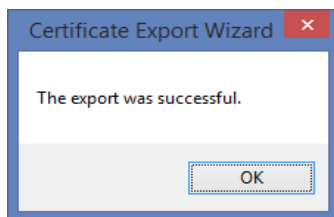
3. En la primera página del asistente de exportación de certificados, haga clic en "**Siguiente**". En la pantalla "**Exportar formato de archivo**", haga clic en "Siguiente".



4. En la pantalla "Archivo para exportar", busque la ubicación en la que desea guardar el certificado. También debe nombrar el archivo. Haga clic en Siguiente".



5. En la última pantalla, haga clic en "Finalizar". La certificación archivada ahora se exportará a la ubicación seleccionada.

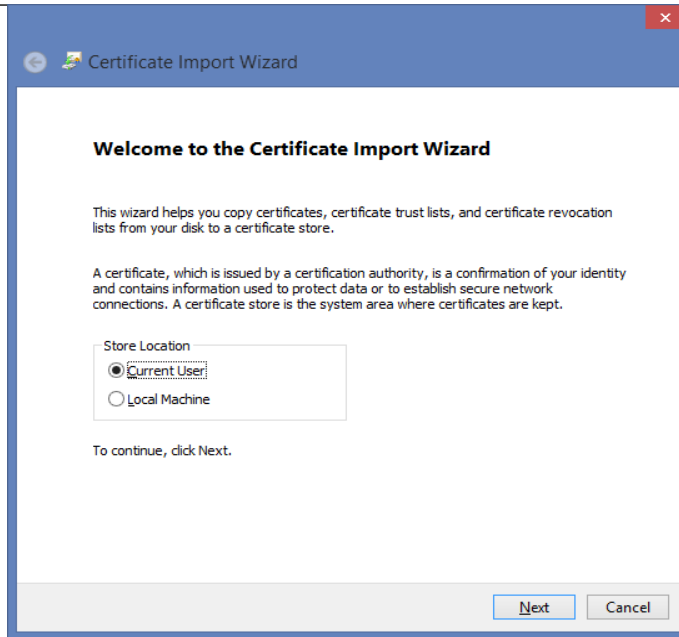


6. Vaya a la ubicación donde exportó el archivo de certificación. Haga clic derecho en el archivo y seleccione "Instalar certificado". Esto ahora iniciará el Asistente de importación de certificados. Vaya a la sección llamada "Importación de certificados con el asistente de importación de certificados" para obtener más instrucciones.

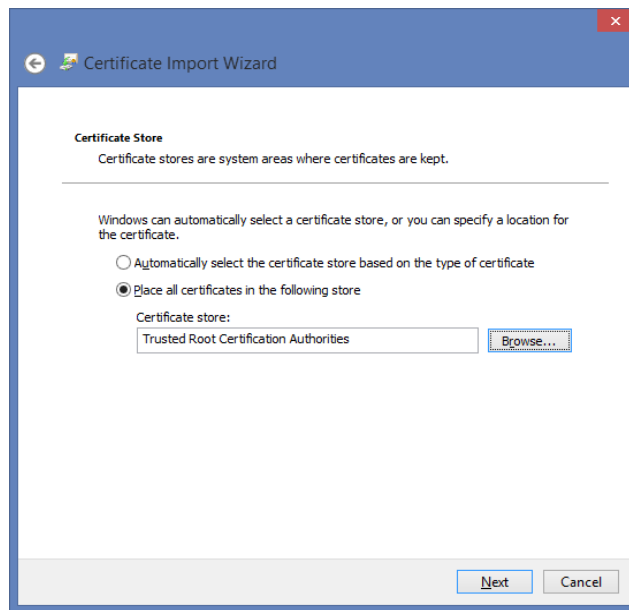
Importación de certificados con el asistente Wizard de importación de certificados

Esta sección cubre cómo proceder una vez que abra el asistente de importación de certificados. Se puede acceder a esto haciendo clic en "Instalar certificado" en Internet Explorer, o después de exportar un certificado desde Google Chrome y hacer doble clic en el archivo guardado.

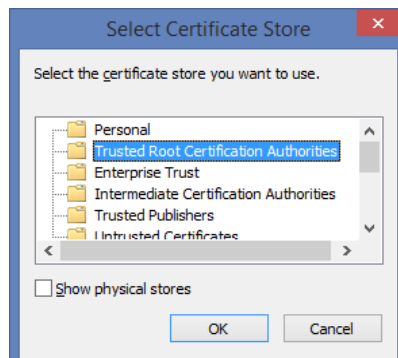
1. En la primera pantalla del asistente de importación, seleccione "Usuario actual" como Ubicación de la tienda; si más de un usuario de Windows utilizará la interfaz web de VAX, seleccione "Máquina local". Haga clic en Siguiente.




2. En la siguiente pantalla, seleccione "Colocar todos los certificados en la siguiente tienda" y haga clic en el botón de exploración.



3. Aparecerá una pequeña ventana con varias carpetas; seleccione "Autoridades de certificación raíz de confianza" como almacén de certificados. Haga clic en Aceptar". Haga clic en "Siguiente" de nuevo.



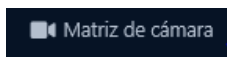
4. En la última pantalla, haga clic en "Finalizar". Se le indicará que está a punto de instalar un certificado. Haga clic en "Sí" para instalar el certificado.
5. Debe reiniciar sus navegadores web y borrar el caché de su navegador antes de que la nueva configuración surta efecto.

 **Nota:** Este proceso debe realizarse en todas las computadoras cliente que verán los sistemas de cámara a través de VAX a través del protocolo HTTPS. Si no lo hace, aparecerá el error "Error al cargar la lista de sitios".

Matriz de cámaras de varios proveedores

Camera Matrix es una pantalla completa en VAX dedicada a ver cámaras en una vista de cuadrícula. Las cámaras de múltiples proveedores se pueden ver simultáneamente. Se admite un tamaño de matriz máximo de 4 x 4.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**; haga clic en el ícono **Camera Matrix** (en la imagen a continuación).



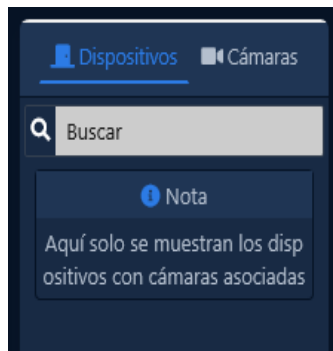
La pantalla Camera Matrix se abrirá en otra pestaña o ventana externa.

Figura 31.12. Matriz de cámara con cámaras



2. En el lado izquierdo de la pantalla está la lista de **dispositivos** y la lista de **cámaras**.

Figura 31.13. lista de dispositivos

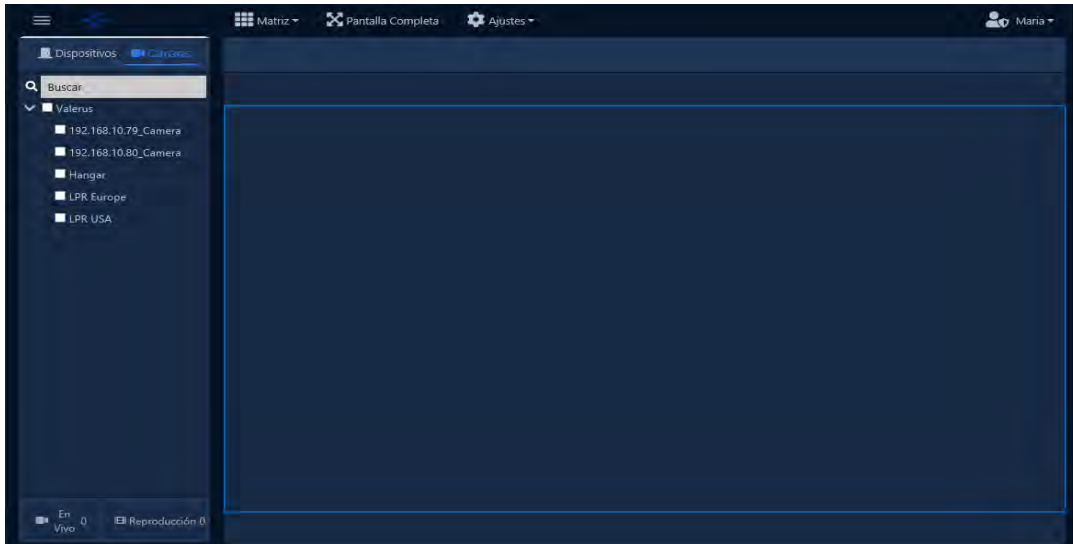


3. Cuando se seleccione Dispositivos, obtendrá una lista de Puertas y Ascensores con cámaras asociadas a ellos. Cuando se selecciona Cámaras, obtendrá una lista de sistemas de cámaras y cámaras.

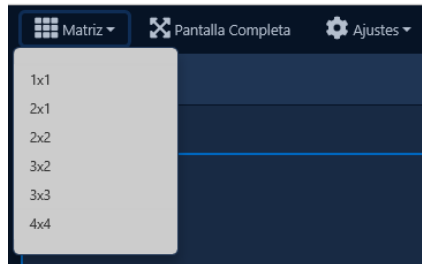
En la parte superior izquierda de la pantalla hay varias opciones de página.

Figura 31.14. lista de opciones





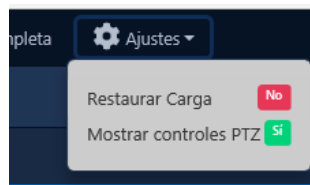
4. Haga clic en **Dispositivos** para alternar la lista de dispositivos en el lado izquierdo. Use esto para maximizar el espacio de la pantalla para ver las cámaras.
5. Haga clic en **Matriz** para seleccionar un tamaño de Matriz. 1x1 a 4x4 están disponibles.



6. Haga clic en **Pantalla completa** para que el navegador web actual pase al modo de pantalla completa. Use esto para maximizar el espacio de la pantalla para ver las cámaras.



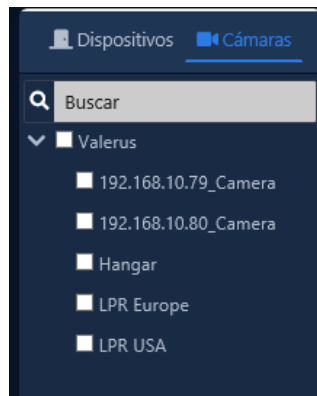
7. Haga clic en **Configuración** para revelar la configuración específica de la página. Habilite Restaurar al cargar para permitir que la página recuerde qué cámaras se mostraban al recargar. Mostrar controles PTZ se puede alternar para eliminar los controles PTZ de la ventana interior cuando se visualizan cámaras PTZ.



Visualización de cámaras en Matrix

Para ver video en vivo o reproducción, haga lo siguiente:

1. Haga clic en Configuración en la parte superior de la página. Seleccione el tamaño de matriz apropiado.
2. En la lista Dispositivos y cámaras, expanda la vista de árbol. Cuando desee ver una cámara, simplemente haga clic y arrastre una cámara o dispositivo a una de las ventanas de video en el medio de la pantalla. Puede marcar varias cámaras y hacer clic en Directo o Reproducción en la parte inferior de la pantalla.



3. Cuando se está viendo una cámara, puede hacer clic con el botón derecho en la ventana interior cuando esté viendo una cámara para cambiar rápidamente entre reproducción y video en vivo. También puede acceder a los ajustes preestablecidos de PTZ de esta manera.



Capítulo 32. Integración con Active Directory

Este capítulo describirá los beneficios y los pasos necesarios para integrar VAX con un proveedor LDAP como **Microsoft Active Directory (AD)**. Se recomienda encarecidamente un administrador de TI y es probable que se requiera para una integración exitosa. Este capítulo debe revisarse en su totalidad antes de intentar la integración de AD.

Descripción general de la integración

La integración de Active Directory permite que VAX haga lo siguiente:

- Importar usuarios de un servidor Active Directory (AD) existente y otorgarles acceso a puertas/pisos en función de los grupos de seguridad de AD en los que se encuentren.
- Sincronice los usuarios de VAX con los usuarios de AD según un temporizador o activado manualmente desde VAX.
- A los usuarios en AD que estén deshabilitados se les quitarán sus derechos de acceso a puertas/pisos (según el tiempo de sondeo de AD).
- Asociar campos personalizados en VAX con campos de atributo de usuario de AD.
- Importar información de Credencial (Tarjeta/Mando/PIN) desde los campos de Atributo de usuario de AD.
- Permitir la autenticación LDAP para los administradores de VAX. Permite a los administradores de VAX iniciar sesión en VAX con credenciales de dominio AD.

Orden de operaciones de integración de AD

Para maximizar la eficiencia y minimizar el tiempo de configuración, recomendamos el orden de operaciones descrito en esta guía. Cada elemento de esta lista se detallará en su propia sección.

1. Planificación: qué información de AD se sincronizará

- Grupos (opcional): Cree o elija Grupos en AD que VAX monitoreará. Tenga en cuenta la cadena de unidades organizativas (OU) necesaria para reducir el alcance a esos grupos. VAX solo sincronizará los usuarios de AD que sean miembros de los grupos seleccionados.
- Credenciales (opcional): la información de credenciales (Tarjetas/Mandos/PIN) se puede importar desde Atributos de usuario de AD en Active Directory. Requiere uno o más campos de atributos de usuario disponibles.
- Campos personalizados (opcional): los atributos de usuario de AD como la dirección, el número de teléfono y muchos otros se pueden asociar con campos personalizados en VAX.
- Autenticación LDAP (opcional): si está habilitado, agregar nuevos administradores en VAX le dará la opción de usar la autenticación LDAP en lugar de crear un nombre de usuario y una contraseña. No se necesita configuración especial en AD.

2. Configurar cuentas de servicio para VAX

- Elija o cree una cuenta de servicio en Active Directory.
- Agregue la cuenta de servicio como miembro del grupo AD "Controladores de dominio de solo lectura" o un grupo equivalente que le dé acceso a la cuenta de servicio para leer usuarios y grupos de Active Directory.

- Agregar la política local "Iniciar sesión como derecho de servicio" a la cuenta de servicio VAX se ejecutará en el servidor en el que se instalará VAX.
3. Instalar VAX
 - Instalar VAX en una computadora que sea parte del dominio; asegúrese de que los servicios estén configurados para ejecutarse como la cuenta de servicio creada en Active Directory.
 - Si es necesario, cambie los permisos de la base de datos localmente en SQL para que la cuenta de servicio tenga acceso para crear/modificar la base de datos VAX MSSQL.
 4. Configuración de integración LDAP en VAX
 - Realice la configuración inicial de VAX e inicie sesión con el Administrador inicial (si aún no lo ha hecho).
 - Ingrese el nombre de dominio completo en la configuración de integración de LDAP.
 - Elija un tiempo de sondeo en la configuración de integración de LDAP (con qué frecuencia VAX verificará los cambios de AD).
 - Introduzca la unidad organizativa del grupo raíz (opcional). Esto reducirá el alcance a la unidad organizativa que contiene los grupos que VAX sincronizará y monitoreará para los usuarios.
 5. Crear asociaciones entre grupos de AD y grupos de privilegios de acceso
 - Cree Asociaciones entre Grupos AD y Reglas que definirán a qué Puertas/Pisos los Usuarios en esos Grupos tendrán acceso.
 6. Importación de credenciales desde AD (Opcional):
 - Crear asociaciones entre los atributos de usuario de AD y un tipo de credencial.
 7. Importación de campos personalizados desde AD (Opcional):
 - Crear Campos Personalizados en VAX.
 - Crear asociaciones entre los atributos de usuario de AD y los campos personalizados de VAX.
 8. Sincronizar AD: realizar la primera sincronización LDAP.
 - Una vez que haya completado todos los pasos anteriores, realice su primera sincronización.

Planificación: ¿Qué información de AD se sincronizará?

Esta sección describirá los factores que se deben considerar en las fases de planificación de la integración de LDAP.

La siguiente lista contiene información que se sincroniza automáticamente para los usuarios de AD:

- Nombre y apellido
- Fecha de caducidad del usuario (los usuarios caducados ya no tendrán derechos de acceso)
- Estado del usuario (deshabilitado/habilitado)
- Membresía de grupo (solo grupos que se han agregado en VAX)

Toda la demás información (credenciales, campos personalizados) es opcional y se describe a continuación.

Grupos AD, Membresía y Estructura

VAX sincroniza a los usuarios en función de los grupos de seguridad de AD de los que son miembros. Elegirá los grupos de seguridad de AD desde los que desea monitorear/sincronizar usuarios.

Opcionalmente, se puede otorgar acceso a puertas/pisos en función de los grupos de seguridad de AD de los que son miembros los usuarios.

Los siguientes son factores que deben ser considerados durante este proceso:

- a. ¿Qué nivel de granularidad deben tener los permisos para Puertas/Pisos?
- b. Cualquier persona en AD debe tener acceso a todas las puertas/pisos:
 - o Se puede usar un grupo existente (como 'Personal' o 'Usuarios de dominio') para dar acceso a los empleados a todas las puertas/pisos del sistema.
- c. Grupos muy específicos de personas requieren diferentes accesos en diferentes momentos:
 - o Si no hay Grupos de seguridad de AD dedicados para cada tipo de usuario (RRHH, TI, Oficina, etc.): Se deben crear Grupos de seguridad dedicados en AD para dar acceso a Puertas/Pisos. Los usuarios de AD deben asignarse a los grupos de AD apropiados antes de la implementación.
- d. ¿Se debe dar a los empleados acceso a Puertas/Pisos desde Active Directory o VAX??
- e. Active Directory:
 - o En este caso, debe haber uno o más Grupos AD creados específicamente para el Control de Acceso. Los empleados existentes se colocarán en uno o más de estos grupos. VAX se configurará para dar acceso a puertas/pisos en función de la pertenencia al grupo AD.
 - o La mayor parte de la administración se realizará en AD. Los nuevos empleados se colocarán en grupos AD de control de acceso y se les otorgarán automáticamente permisos para puertas/pisos.
- f. VAX:
 - o En este caso, los usuarios de AD se sincronizarán en función de uno o más grupos. Una vez sincronizado, un administrador de VAX dará acceso a puertas/pisos en función de los grupos de VAX.

Credenciales de usuarios

Las credenciales de usuario (tarjetas, llaveros, datos biométricos, PIN) son lo que utilizan los usuarios de VAX para acceder a puertas/pisos.

La información de credenciales se puede agregar a los usuarios en VAX después de que se hayan sincronizado desde AD o la información de credenciales se puede almacenar en los campos de atributos de usuario de AD e importarse con el usuario.

Los beneficios de almacenar información de credenciales en Atributos de usuario de AD incluyen:

- Centralización de la gestión de usuarios de control de acceso.
- Se realiza una copia de seguridad de las credenciales y se pueden volver a importar fácilmente si se destruye la base de datos VAX.

Cuando los Usuarios en AD están deshabilitados, se revocarán los derechos de acceso a Puertas/Pisos de cualquier credencial correspondiente.

Almacenamiento de credenciales de usuario en atributos de usuario de AD

Podemos importar varios tipos de credenciales de uno o más campos de atributos de usuario de AD.

- o Credencial Wiegand de un solo campo de atributo de AD:

La credencial comenzará con un Código de sitio o un Código de instalación, seguido del Número de credencial y el PIN correspondiente (opcional). Cada entrada debe estar separada por una coma. (ejemplo: 33,1528,1234 o 33,1529)

- o Credencial Wiegand con código de sitio fijo:

El código del sitio o el código de la instalación se establecerá como un valor específico en VAX. El número de credencial estará en un solo campo de atributo de usuario de AD. El PIN opcional también estará en su propio campo.

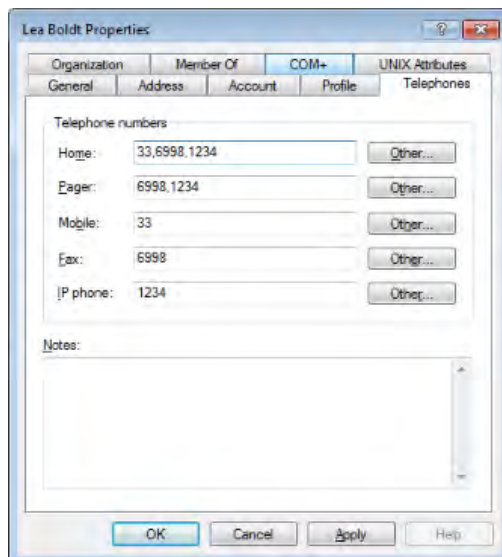
- o Credencial Wiegand de tres campos individuales:

El código del sitio o el código de la instalación estará en un solo campo de atributo de usuario de AD. Tanto el número de credencial como el PIN opcional estarán en un único campo de atributo de usuario de AD.

- o PIN:

El código del sitio o el código de la instalación estará en un solo campo de atributo de usuario de AD.

Figura 32.1. Ejemplo de todos los tipos de credenciales almacenadas en campos de atributo de usuario de AD

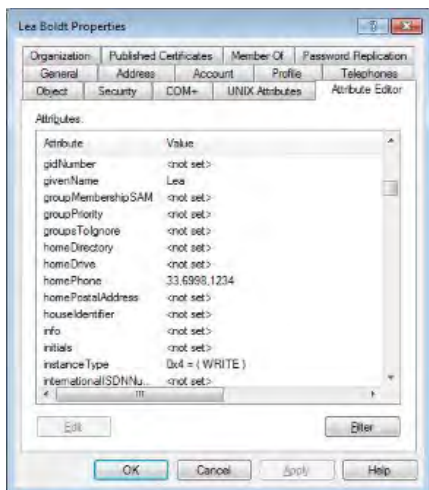


Puede editar los atributos de usuario de AD en una vista de lista; Los campos de atributos de usuario de AD ocultos y comúnmente no utilizados se pueden encontrar en esta vista.

En usuarios y equipos de Active Directory:

1. Haga clic en Ver en el menú superior.
2. Haga clic en Funciones avanzadas. La ventana se actualizará.

- Al editar un usuario de AD, aparecerá una nueva pestaña titulada Editor de atributos.



Configuración de cuentas de servicio

Esta sección describirá los pasos necesarios para permitir que VAX acceda a los recursos del dominio, incluido el acceso a Microsoft Active Directory a través del protocolo LDAP. VAX se ejecuta como un servicio de Windows. Deberá ejecutarse como una cuenta de Windows que tenga permiso para leer información LDAP.

Un administrador de TI puede crear una cuenta de servicio administrada (una cuenta especial de Windows creada especialmente para ejecutar servicios en un dominio) o una cuenta de dominio normal de Windows con permisos de dominio y cuenta de servicio.

Crear y configurar cuentas de servicio

- Inicie sesión en un controlador de dominio de Windows con un administrador de dominio.
- Abra Usuarios y equipos de Active Directory.
- Navegue a una unidad organizativa donde creará la cuenta de servicio. Recomendamos usar la unidad organizativa Cuentas de servicio administradas.
- Haga clic con el botón derecho en la unidad organizativa y seleccione Nuevo, seguido de Usuario.
- Cree el nuevo Usuario. Puede llamarlo VAXService para que pueda encontrarlo fácilmente más tarde. Registre el nombre de inicio de sesión. Establezca una contraseña. Asegúrese de que "El usuario debe cambiar la contraseña al iniciar sesión" no esté marcado.
- Después de crear el Usuario, vaya a sus Propiedades.
- Agregue el usuario al grupo de seguridad de AD "Controladores de dominio de solo lectura". Este permiso es necesario para que VAX realice consultas LDAP.

A continuación, debemos otorgar a la cuenta de servicio que creamos permiso local para iniciar sesión como un servicio.

- Inicie sesión en la computadora con Windows en la que se instalará VAX con una cuenta de administrador de dominio o un administrador local.
- Abra "Política de seguridad local". También puede encontrarlo buscando o ingresando "secpol.msc" en una ventana Ejecutar.
- En la ventana Política de seguridad local, expanda las "Políticas locales" del lado izquierdo y seleccione "Asignación de derechos de usuario".

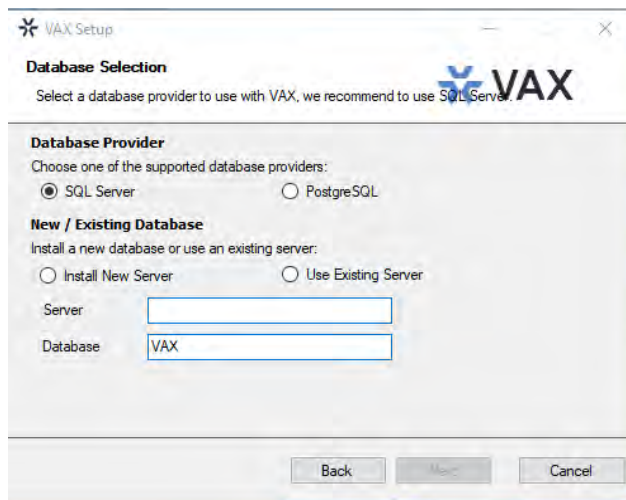
4. En la lista de políticas, haga clic con el botón derecho en "Iniciar sesión como servicio" y seleccione Propiedades en el menú contextual.
5. En la ventana de propiedades, haga clic en 'Agregar usuario o grupo'.
6. Busque y seleccione la cuenta de dominio de Windows creada anteriormente en el dominio. Esto permitirá que esta cuenta inicie sesión como un servicio.
7. Haga clic en Aceptar y Aceptar de nuevo en la página anterior para aplicar esta configuración.

La configuración de la cuenta de servicio ahora está completa; ahora puede continuar con la instalación del software del servidor VAX.

Installer VAX

Esta sección describirá la instalación del software. El instalador del software VAX es inteligente. Detectará los componentes faltantes y los instalará por usted. La siguiente es una breve descripción general del procedimiento de instalación. Para una mejor comprensión o uso de la configuración avanzada, consulte la Guía de instalación/actualización.

1. Ejecute VAX.exe desde el medio de instalación o después de descargarlo de la web.
2. Verá una lista de los componentes necesarios. Aparecerá una casilla de verificación junto a los componentes que faltan.

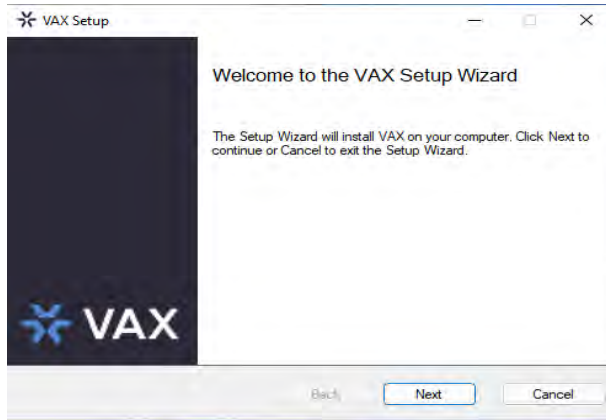


3. Haga clic en Instalar, se instalarán todos los componentes marcados. Si está instalando desde un medio de instalación VAX; los componentes faltantes se instalarán localmente. Si instala desde una descarga web, el instalador intentará instalar esos elementos desde Internet.


Nota

Si algún componente no se instala, intente reiniciar la computadora y ejecute el instalador nuevamente. Si los componentes continúan fallando en la instalación, comuníquese con el soporte técnico de Vicon Industries. Consulte el Capítulo 37, Soporte.


4. Una vez que se hayan instalado los componentes faltantes, comenzará la configuración del VAX.



- a. Haga clic en Siguiente.
- b. Acepte el EULA y haga clic en Siguiente.
- c. Seleccione Avanzado.
- d. Haga clic en Siguiente.
- e. En la pantalla Configuración del servicio, ingrese el dominio y el nombre de usuario de la cuenta de servicio que se creó en las secciones anteriores (ejemplo, "corp\VAXService"). Introduzca la contraseña de la cuenta de servicio. Repita esto para la sección Administrador del sistema.

 **Precaución:** No incluya un sufijo de dominio en los campos "Ejecutar como usuario" de la cuenta de servicio

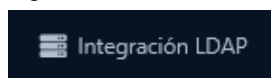
- f. Haga clic en Siguiente.
- g. Haga clic en Siguiente.
- h. Haga clic en Instalar.

 **Nota:** Si alguno de los servicios no se instala o no se inicia, consulte la sección denominada "Error en el inicio de los servicios VAX".

Configuración de integración LDAP en VAX

Esta sección cubrirá la configuración de integración LDAP en VAX.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador creada durante la configuración inicial o proporcionada por su distribuidor/instalador.
3. En la barra lateral, desplácese hacia abajo hasta la sección titulada Programación; haga clic en Integración LDAP icono (en la foto de abajo).



4. Complete los siguientes campos en la pantalla Integración LDAP:

Tabla 32.1. Configuración de LDAP

Cuadro de texto/Casilla de verificación	Descripción
Nombre de dominio completo	Ingrese el nombre de dominio asociado con el controlador de dominio (Ejemplo: Corp.local).
Tiempo de sondeo LDAP	Ingrese la cantidad de tiempo (en minutos) que VAX esperará entre la revisión del servidor AD para ver si hay cambios en los usuarios adjuntos a los grupos que están siendo monitoreados.
Unidad organizativa del grupo raíz (opcional)	Puede reducir el alcance en el que VAX le permitirá agregar/ver grupos de AD. Ingrese la cadena de unidades organizativas requerida para llegar a la unidad organizativa que contendrá los grupos de AD que desea sincronizar/supervisar. (Ejemplo: OU=Ubicación de Nueva York,OU=Control de acceso,OU=Grupos)
Permitir autenticación LDAP	Marque para habilitar el inicio de sesión único a través de las credenciales de dominio de AD.
Permitir sincronización de grupo/usuario LDAP	Marque para habilitar la sincronización de grupo/usuario LDAP


! Aviso

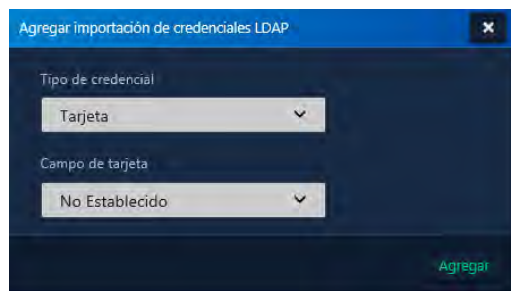
No haga clic en el botón **Forzar sincronización** o en el botón **Forzar actualización** (inicia la sincronización inicial) hasta que la asignación de credenciales de usuario, la asignación de campos personalizados y todos los grupos AD requeridos se hayan agregado como grupos de privilegios de acceso. Esto se tratará en las siguientes secciones.

5. Haga clic en el botón **Guardar** en la parte inferior de la pantalla.

Credenciales de usuario LDAP

Si se decidió durante las fases de planificación que las Credenciales se obtendrán de Active Directory, siga el resto de esta sección.

1. En la pantalla Integración LDAP, vaya a la pestaña Credenciales de usuario.
2. Haga clic en el icono  para abrir las opciones de importación de credenciales LDAP.
3. Seleccione un Tipo de credencial de la lista desplegable.
4. Si seleccionó Tarjeta como Tipo de credencial, debe seleccionar un Tipo de importación. Esto ayudará a VAX a saber si la información de la credencial estará en un solo campo o en múltiples atributos de usuario de AD.



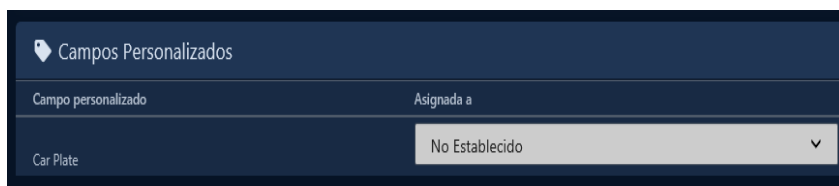
5. Seleccione el campo de atributo de usuario de AD de cualquier menú desplegable requerido.

Nota: Si alguno de los campos de PIN se deja como "No establecido", generaremos automáticamente los PIN correspondientes para los horarios de tarjeta y PIN. Si el campo está configurado, pero está vacío en AD, también se generará automáticamente. En el caso de importar una credencial de un solo campo, generaremos automáticamente un PIN si no hay una entrada separada por comas después del Código del sitio y el Número de tarjeta.

Campos personalizados de usuario de LDAP

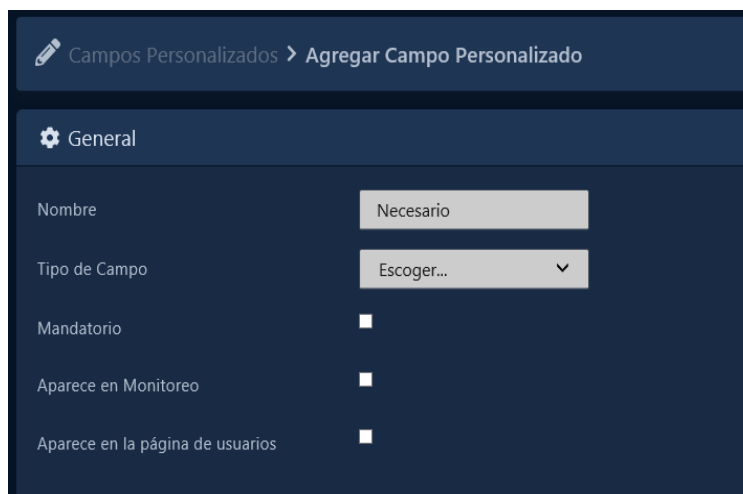
Si se decidió durante las fases de planificación que uno o más atributos de usuario de AD deben sincronizarse con VAX desde Active Directory, siga el resto de esta sección.

1. Los campos personalizados deben agregarse en VAX antes de que se asocien con los atributos de AD.
2. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**; haga clic en el ícono de **Campos personalizados** (en la imagen a continuación).

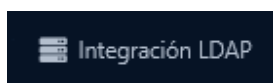


3. En la pantalla Campos personalizados, verá los campos personalizados ya creados. Para agregar un campo adicional, complete el cuadro de texto titulado Nombre del campo y haga clic en el botón Agregar.

Figura 32.1. Campos personalizados: Ejemplo



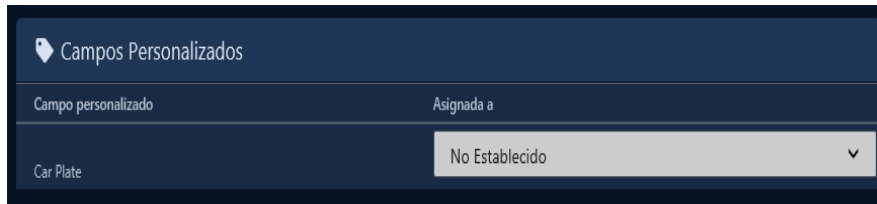
4. Una vez que haya agregado sus campos personalizados, debemos asociar los campos personalizados de VAX a los atributos de usuario de AD.
5. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Programación**; haga clic en icono **Integración LDAP** (en la foto de abajo)



6. En la pantalla Integración LDAP, vaya a la pestaña Campos personalizados.
7. Verá los campos personalizados agregados en los pasos anteriores. Utilice el menú desplegable Asignado a para seleccionar un atributo de usuario de AD para asociarlo a cada campo personalizado. Puede dejar el menú desplegable como No configurado; VAX

tratará el campo personalizado como lo haría normalmente.

Figura 32.2. LDAP Campos personalizados



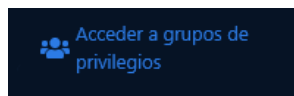
8. Ahora puede pasar a la siguiente sección para crear asociaciones de grupos de privilegios de acceso a grupos de seguridad de AD.

Crear asociaciones entre grupos de AD y grupos de privilegios de acceso

Para que un usuario de AD se sincronice, debemos decirle a VAX qué grupos de seguridad de AD monitorear y sincronizar usuarios. Para obtener más información sobre la planificación de la estructura del grupo, consulte la sección llamada "Grupos AD, membresía y estructura".

Esta sección demostrará cómo agregar un grupo de seguridad de AD como un grupo de privilegios de acceso en VAX.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**; haga clic en el icono **Grupos de privilegios de acceso** (en la imagen a continuación).




2. En la pantalla Grupos de privilegios de acceso, verá los grupos ya creados. Haga clic en el botón Agregar en esta pantalla.
3. Seleccione LDAP como Tipo de grupo. Si desea crear grupos de privilegios de acceso sin LDAP, puede seleccionar Local.
4. El menú desplegable Grupo le dará una lista de los grupos de seguridad de AD que VAX pudo ver. Seleccione un grupo de AD del que le gustaría monitorear/sincronizar usuarios.

Consejo

Puede reducir el alcance de lo que VAX de AD Groups puede ver completando la sección de OU raíz en la pantalla de configuración de LDAP.

5. (Opcional) Complete una descripción para ayudar a otros administradores a comprender el rol / propósito de este grupo.
6. Seleccione una partición para crear este grupo de privilegios de acceso.

 **Nota:** Puede asociar el mismo grupo de seguridad de AD a varias particiones agregando el grupo varias veces y cambiando la partición seleccionada.

7. Si anticipa que los horarios de usuario en este grupo se comportarán de manera diferente en un día festivo, seleccione Días festivos estándar para el grupo de días festivos. De lo contrario, seleccione Sin días festivos.

Figura 32.3. Adición de un grupo de seguridad de AD como grupo de privilegios de acceso

8. Lectores / pisos:

Si se han configurado Paneles, Puertas, Elevadores y Lectores, opcionalmente puede dar acceso a Puertas/Pisos y seleccionar un Horario. Los usuarios de AD que estén sincronizados tendrán acceso a las puertas/pisos especificados en función del horario de usuario seleccionado. Marque las Puertas/Pisos correspondientes y seleccione un programa del menú desplegable.

Figura 32.4. Selección de lectores/pisos

Una vez que esté satisfecho con la configuración (que se puede editar más tarde según sea necesario), haga clic en el botón verde **Crear**.

9. Repita este proceso para cualquier grupo de seguridad de AD adicional que desee agregar.

Sincronizar usuarios de AD

Before the first LDAP synchronization, please ensure the following have been complete:

- Se ha ingresado un nombre de dominio completo en la configuración de LDAP.
- Si es necesario, las credenciales de usuario se han asignado a los campos de atributo de usuario de AD. Las credenciales deben ingresarse en los campos de atributos de usuario seleccionados en Active Directory.
- Si es necesario, se agregaron campos personalizados y se asignaron a campos de atributo de usuario de AD.

- Todos los grupos de seguridad de AD requeridos se agregaron como grupos de privilegios de acceso. Ahora está listo para realizar la sincronización inicial de AD.
- 1. En la barra lateral, desplácese hacia abajo hasta la sección titulada Programación; haga clic en el ícono de Integración LDAP (en la imagen a continuación).



- 2. Para la primera sincronización inicial, presione el botón **Forzar actualización**.



El botón Forzar sincronización eliminará cualquier usuario LDAP existente de VAX y luego intentará sincronizar esos usuarios en función de la configuración y los grupos LDAP actuales.

⚠ Advertencia

Según el rendimiento o la carga en el controlador de dominio (servidor AD), una actualización forzada puede tardar entre unos minutos y más de una hora. Force Refresh solo debe usarse para la sincronización inicial o si se cambia la asignación de credenciales y/o la asignación de campos personalizados o si se agregan grupos de seguridad de AD adicionales como grupos de privilegios de acceso.

- 3. Una vez completada la primera sincronización, VAX comprobará si hay cambios en AD en función del tiempo de sondeo de LDAP. También puede forzar a VAX a sincronizar antes presionando el botón Forzar sincronización.



Autenticación del administrador LDAP

Con LDAP configurado, VAX puede permitir la autenticación de administrador con proveedores de LDAP como Active Directory para administradores que inician sesión en VAX para administrar el sistema y realizar cambios.

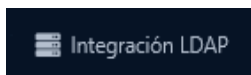
Los beneficios de usar la autenticación LDAP con VAX incluyen:

- El inicio de sesión único permite a los administradores usar su Active Directory o credenciales de dominio para acceder a VAX.
- Las contraseñas se autentican con Active Directory. En el caso de que la contraseña cambie en Active Directory, VAX requerirá la nueva contraseña para que el Administrador inicie sesión.

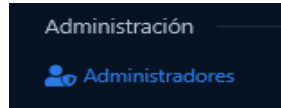
Algunas de las desventajas de usar la autenticación LDAP con VAX incluyen:

- Si el proveedor de LDAP está fuera de línea, los administradores no pueden iniciar sesión para realizar cambios en VAX.
- Si las credenciales de LDAP están comprometidas, VAX también puede estarlo. Para configurar la autenticación LDAP para administradores:


- 1. En la barra lateral, desplácese hacia abajo hasta la sección titulada Programación; haga clic en el ícono de Integración LDAP (en la imagen a continuación).



2. Complete el nombre de dominio completo y marque la casilla de verificación "Permitir autenticación LDAP".
3. Haga clic en 'Guardar' en la parte inferior de la pantalla.
4. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el ícono **Administradores** (en la imagen a continuación).



5. Haga clic en el botón **"Agregar"** en esta pantalla.
6. Seleccione **LDAP** en el menú desplegable Autenticación.
7. Complete el Nombre de usuario con el **'Nombre de inicio de sesión del usuario'** del proveedor LDAP.

 **Nota:** El prefijo del nombre de dominio no es necesario en la mayoría de los casos en el campo Nombre de usuario.

8. Rellene los permisos necesarios para el nuevo administrador. Para obtener más detalles sobre estos permisos, consulte el *Capítulo 20, Administradores y privilegios*.
9. Haga clic en el botón **"Guardar"** en esta pantalla.
10. El administrador podrá iniciar sesión en VAX utilizando las credenciales de dominio

Figura 32.5. Acceso de administrador con credenciales de dominio



Solución de problemas de integración LDAP

Esta sección describirá la resolución de problemas específicos de la integración LDAP.

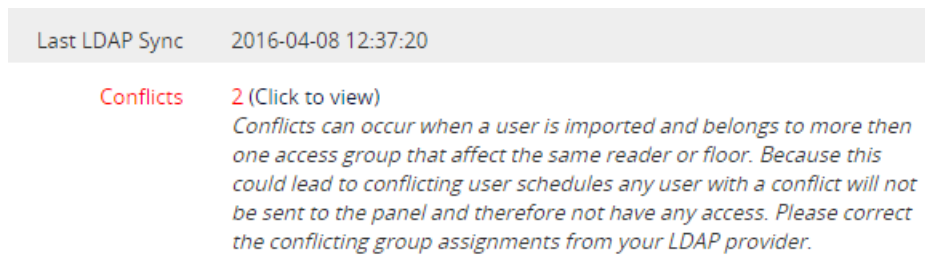
LDAP Conflictos

Una vez que VAX se integra a un servidor de Active Directory, es posible que se produzcan conflictos de configuración entre los usuarios.

Pueden ocurrir conflictos cuando un usuario es importado y pertenece a más de un Grupo de Privilegios de Acceso que afectan al mismo Lector o Piso. Debido a que esto podría generar conflictos en los horarios de los usuarios, cualquier usuario con un conflicto no será enviado al Panel y, por lo tanto, no tendrá ningún acceso. El problema debe corregirse desde el proveedor de LDAP.

Cuando ocurre un conflicto, verá un banner rojo en la parte superior de la página y una sección en la pantalla Integración LDAP.

Figura 32.6. Mensaje de conflicto



Puede hacer clic en "Hacer clic aquí" para ver más detalles sobre los conflictos. Aparecerá una ventana con los detalles del conflicto..

Figura 32.7. Ejemplo de conflictos de usuarios de LDAP



En nuestro ejemplo, Lea Boldt se colocó accidentalmente en los grupos de seguridad de AD "Acceso a la puerta principal 9 a 5" y "Acceso a la puerta principal Acceso siempre". La solución en este caso es modificar el usuario de AD Lea Boldt y eliminar al usuario de uno de los dos grupos. Una vez transcurrido el tiempo de sondeo, el conflicto se resolverá. También puede realizar una sincronización forzada para resolver el conflicto antes.

Los servicios VAX no se inicia

Durante la instalación, puede haber circunstancias en las que uno o ambos servicios VAX no se inicien o no se instalen. Los motivos y posibles soluciones se detallarán en este apartado.

Verificación de archivos de registro

Si el servicio que no pudo iniciarse fue VAXServer, es posible que podamos verificar los archivos de registro para obtener información adicional.

1. Navegar a:

C:\Program Files(x86)\Vicon Industries\VAX\WebServer\Logs

2. Su ruta de instalación puede ser diferente.

3. Abra Application.txt en el bloc de notas.

4. Verifique las últimas entradas en el archivo de registro. La siguiente tabla se puede utilizar para comparar con posibles resoluciones.

Tabla 32.2. Servicio no pudo iniciarse

Entrada de registro	Posibles Resoluciones
ERROR VAX. Servicios web. HCAuth-Provider [(null)] - Error de autenticación LDAP: (VAXwebservice) Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta	La cuenta de servicio especificada en el instalador tiene credenciales incorrectas, verifique el nombre de usuario y la contraseña. Esto también podría indicar que la contraseña de la cuenta ha caducado. El Visor de eventos de Windows también puede brindar más información. Póngase en contacto con su administrador de dominio.
"Verificando las migraciones de la base de datos" aparece repetidamente hasta que se detiene el servicio.	No se pudo acceder a la base de datos. Es posible que el servicio no se haya iniciado automáticamente. Abra Services.MSC y verifique que el servicio titulado "SQL Server (VAX)" se esté ejecutando. Puede hacer clic derecho en el servicio y seleccionar Iniciar.
ERROR VAX. StartupHelpers.D-bSetupHelper [(null)] - System.Data.SqlClient. SqlException (0x80131904): CREAR BASE DE DATOS	La cuenta de servicio especificada en el instalador no tiene permisos para crear bases de datos. Solicite a un administrador de SQL que agregue el rol de SQL Server 'dbcreator' a la cuenta de servicio especificada en el instalador y haga clic en 'reintentar' en la ventana del instalador.

Si aún no puede iniciar/installar con éxito ningún servicio VAX, consulte el *Capítulo 37, Soporte*.

Capítulo 33. Motor de control de acción

Introducción

El motor de control de acción, al que nos referiremos como ACE.

ACE es un potente motor de secuencias de comandos laterales dentro del software VAX. Permite a los administradores definir un conjunto de condiciones que activan una serie de acciones que ocurrirán cuando se cumplan estas condiciones.

Advertencia

No recomendamos utilizar el motor de control de acción para ninguna función de seguridad humana. ACE no funcionará si el servidor VAX no está disponible o la conectividad de la red no funciona.

Casos de uso de ACE

ACE se puede configurar para lograr lo siguiente:

- Bloqueo de lectura de un solo botón/tarjeta
- Tour de guardia personalizado
- Desbloquee las puertas exteriores con una sola lectura de tarjeta
- Correo electrónico programado del conteo de ocupación del área o edificio
- SMS/correo electrónico basado en una condición/disparador
- Disparar el relé en otro edificio en función de una condición/disparador
- Enviar solicitudes HTTP a sistemas de terceros
- Envíe instantáneas de la cámara a los administradores en función de la condición/disparador
- Deshabilitar una tarjeta si se usa más de una cantidad específica
- Envío automático de informes por correo electrónico
- -y muchos más.

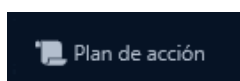
ACE Componentes

Hay dos componentes principales para ACE, **planes de acción** y **disparadores de acción**. Los planes de acción deben crearse primerot.

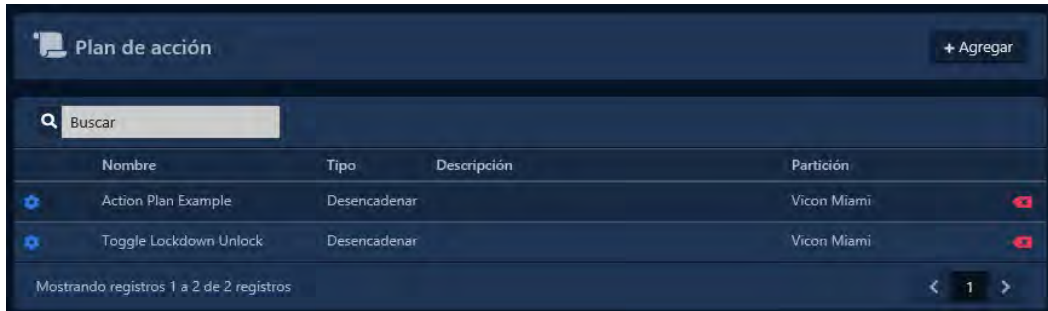
Plan de acción

Los planes de acción son una serie de acciones encadenadas para realizar una tarea. Hay más de 40 acciones que se pueden encadenar. Use los siguientes pasos para crear un plan de acción:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono de **Planes de acción** (en la imagen a continuación)



- En la pantalla Planes de acción, se le presentarán los planes de acción existentes. Cualquier plan de acción que se pueda ejecutar tendrá un botón naranja de ejecución a la izquierda. Haga clic en el botón **Agregar** para crear un nuevo plan.



- En la pantalla **Agregar** plan de acción, complete el nombre del plan.

Consejo :

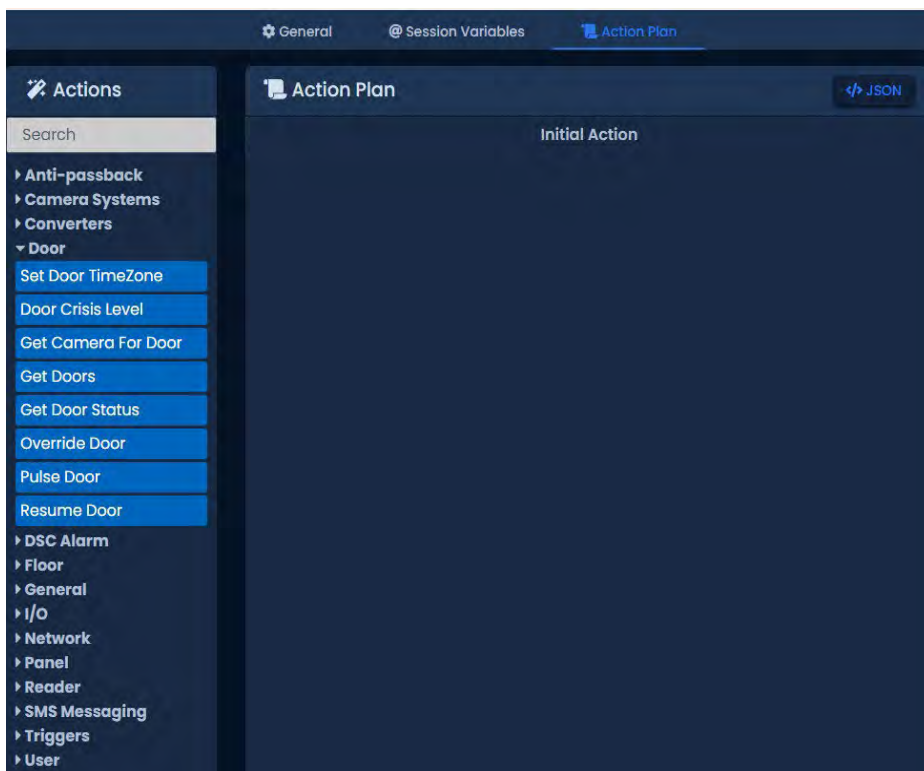
El nombre debe representar lo que hará el plan de acción o su propósito. La descripción es opcional.

- Seleccione una **partición** para colocar este plan.

- Seleccione un Tipo** de plan. A continuación se explica cada tipo de plan:

- Tipo de plan de activación: el plan se ejecuta a través de una activación de acción. Cuando se cumplan las condiciones del activador de la acción, este plan se ejecutará.
- Tipo de plan de sistema: el plan se ejecuta presionando el botón de ejecución mientras se visualiza el plan de acción o en la pantalla de planes de acción; también se puede ejecutar a través de la API web. Estos planes también pueden ser utilizados por otros planes.

- Haz clic en **Crear**. Accederá a la pantalla Editar plan de acción. Vaya a la pestaña Plan de acción.



Acciones

En la pestaña Plan de acción, puede configurar una o varias acciones para ejecutar. Hay más de 40 acciones agrupadas en categorías a la izquierda de la página. Algunas acciones pueden resolverse en una cadena de condiciones de Éxito o Fallo. Esto significa que puede crear una cadena de acciones independiente en función del éxito o el fracaso de la acción anterior.

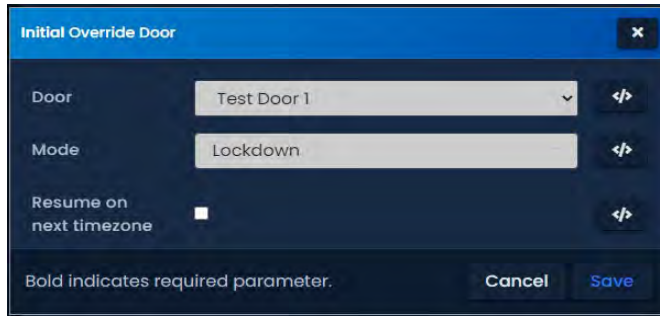
La siguiente tabla describe las acciones disponibles en cada sección. Para obtener más detalles sobre todas las acciones, consulte la sección correspondiente dentro de la guía técnica principal para obtener una lista completa de acciones.

Tabla 33.1. Categorías de acción

Categorías de acción	Descripción
Anti-passback	Le permite restablecer el área y las ubicaciones de los usuarios en el sistema, comúnmente utilizado para restablecer las ubicaciones anti-passback
Sistemas de cámara	Acciones que están diseñadas para interactuar con un sistema VMS
Convertidores	Acciones que pueden convertir números/cadenas en hashes como MD5 o Base64. Comúnmente utilizado durante la autenticación con sistemas de terceros.
Puerta	Acciones relacionadas con la puerta, como iniciar invalidaciones y niveles de crisis
Piso	Acciones relacionadas con el piso del elevador, como iniciar invalidaciones
General	Contiene acciones como registro, temporizadores, configuración de variables, declaraciones si/o y cada declaración
E/S	Acciones utilizadas para iniciar comandos de invalidación de entradas o salidas
Red	Acciones que tienen lugar a través de la red. Esto incluye el envío de correos electrónicos, solicitudes HTTP y solicitudes PING.
Panel	Acciones específicas del panel, como iniciar la alarma de emergencia, activar el altavoz piezoeléctrico y actualizar los paneles
Lector	Acciones específicas del lector, como controlar el LED del lector o el altavoz piezoeléctrico incorporado
Mensajería SMS	Acciones que pueden enviar mensajes SMS. Los proveedores actuales de SMS son Clickatell y Twilio.
disparadores	Acciones que esperarán un período de tiempo específico para que suceda algo, como la apertura de una puerta o la pulsación de un botón.
Usuario	Acciones específicas del usuario, como deshabilitar a un usuario o verificar si un usuario es miembro de un grupo de privilegios de acceso específico

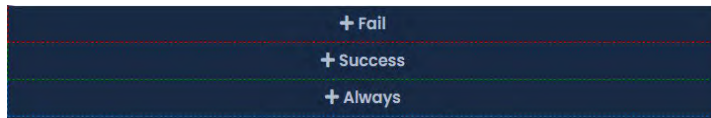
Utilice estos pasos para agregar una acción a su plan de acción:

1. Abra la categoría correspondiente a la izquierda haciendo clic en ella.
2. Haga clic izquierdo y mantenga presionada la acción que desea agregar. Ahora puede arrastrar esta acción al área central de la pantalla.
3. Si es la primera acción del plan de acción, arrástrela hasta el cuadro Acción inicial en la sección central. Suelte y debería aparecer una ventana donde puede ingresar opciones (parámetros) en la acción.
4. Rellene los parámetros necesarios. En este ejemplo, hemos seleccionado Anular puerta para nuestra acción inicial. Se debe seleccionar una Puerta y un Modo. Haga clic en Aceptar.



Use estos pasos para encadenar acciones adicionales juntas:

1. Abra la categoría correspondiente a la izquierda haciendo clic en ella.
2. Haga clic con el botón izquierdo y mantenga presionado con el mouse o el trackpad en la siguiente acción que desea agregar. Ahora puede arrastrar esta acción al área central de la pantalla.
3. Arrastre la acción sobre una acción existente en el medio de la pantalla. Dependiendo de la acción, es posible que vea un cuadro Siempre, un cuadro de éxito y un cuadro de error.



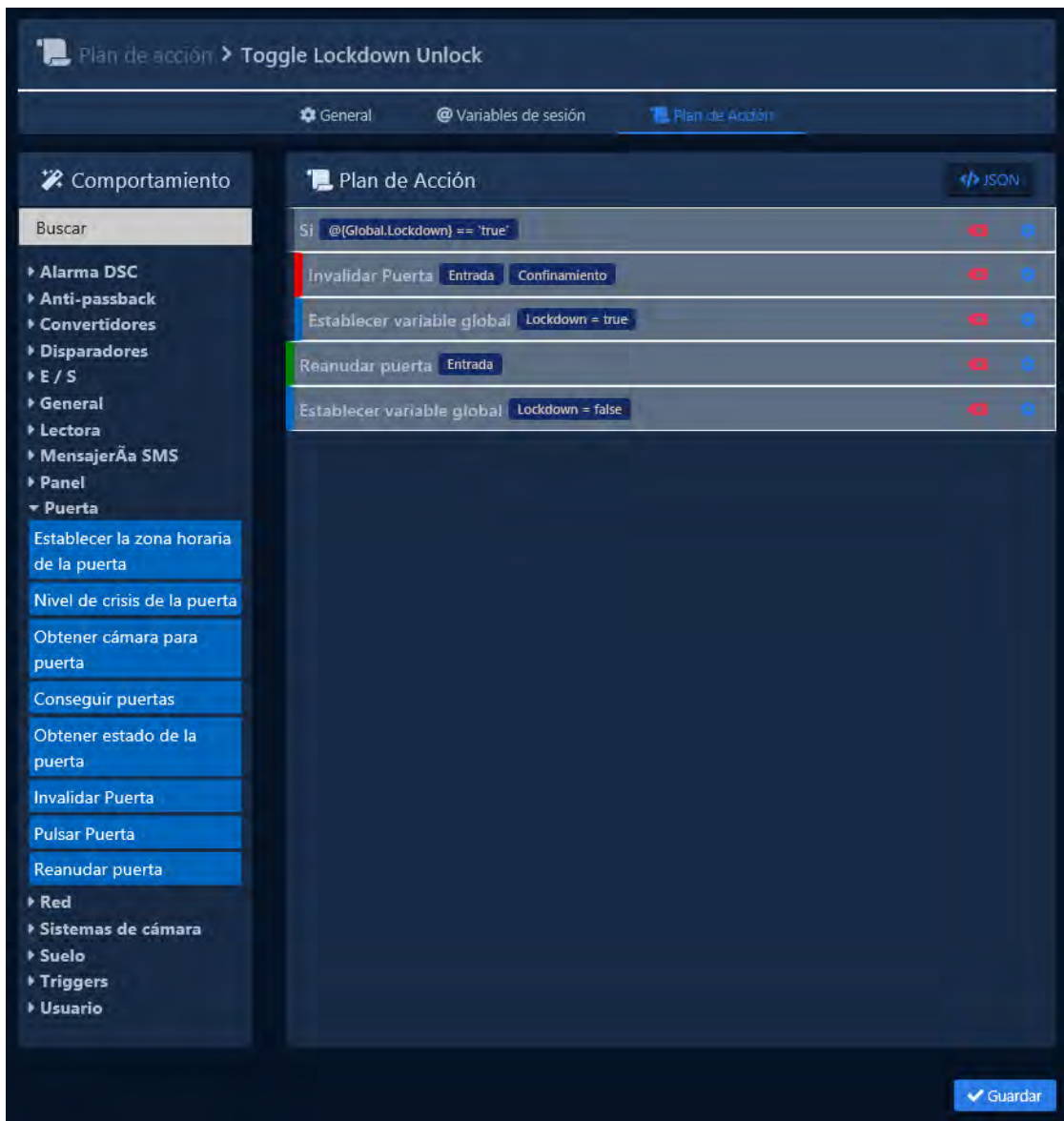
- Si necesita que su nueva acción ocurra después de que la acción anterior se haya completado con éxito, arrastre y suelte la nueva acción en el cuadro Éxito.
- Si necesita que su acción ocurra si la acción anterior no tiene éxito, arrastre y suelte la nueva acción en el cuadro de error.

Puede hacer que se produzcan acciones separadas si la acción anterior falla o tiene éxito. Las cadenas de acciones se requisarán y colorearán.

 **Consejo**

Una acción encadenada en el cuadro Siempre se ejecutará independientemente de si la acción anterior se resolvió como Éxito o Fallo. Normalmente se ejecutará inmediatamente y no tendrá acceso a variables o resultados de la acción anterior.

Figura 33.1. Plan de acción de cierre de edificios

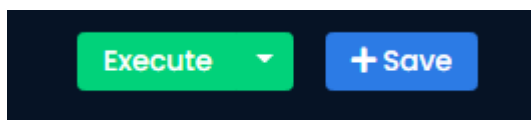


4. Haga clic en Guardar una vez que haya completado su plan de acción. Ejecutar también guardará el plan de acción.

Ejecución de un plan de acción

Si el Tipo de plan de acción se configuró como Sistema, se puede ejecutar de una de las tres formas:

1. Haga clic en el botón **naranja** en la pantalla **Planes de acción** para ejecutarlo inmediatamente.
2. Haga clic en el botón verde **Ejecutar** en la pantalla **Editar plan de acción**.



3. Ejecute la acción a través de VAX Web API a través de una solicitud HTTP POST.

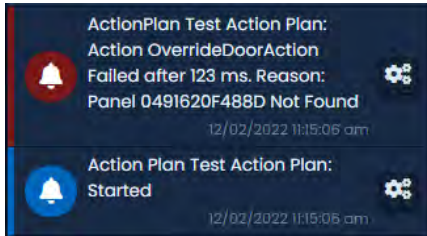
Example: <https://localhost:11001/api/ActionPlans/10/Exec>

Si el Tipo de plan de acción se configuró como Desencadenador, se debe crear y configurar un Desencadenador de acción para ejecutar ese plan de acción.

Supervisión de la ejecución de la acción

Cuando se ejecuta un plan de acción, se generan varias notificaciones cuando ocurre la acción. Dependiendo del plan de acción, se pueden generar más notificaciones. Las acciones de registro también generarán una notificación titulada Mensaje del plan de acción.


Figura 33.2. Plan de acción en ejecución



Consejo

Al monitorear planes de acción más complicados, la pantalla Monitoreo puede mostrar cientos de notificaciones. Consulte el *Capítulo 24, Notificaciones*.

Para ver las notificaciones del plan de acción que ya se han producido, puede ejecutar el informe de actividad del plan de acción. Para obtener más información sobre cómo ejecutar este informe, consulte el Informe de actividad del plan de acción.

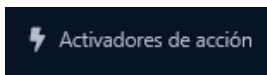
 **Nota:** Los planes de acción pueden lograr mucho más de lo que se muestra en este ejemplo básico. Puede combinar cientos de acciones para satisfacer su necesidad específica

Activadores de acción

Los activadores de acciones son conjuntos de condiciones configurables que ejecutan un plan de acción cuando se cumplen las condiciones. Un plan de acción debe ser del tipo Desencadenador para que un Desencadenador de acción lo ejecute. Estos disparadores son extremadamente flexibles. Puede crear tantos como necesite y hacerlos tan específicos o genéricos como desee.

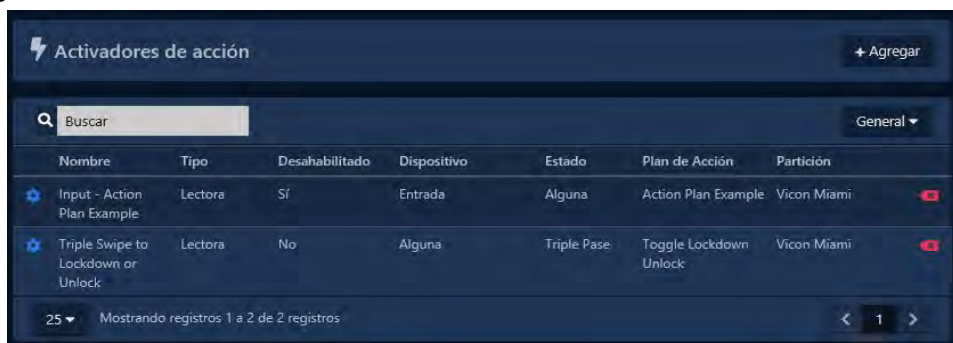
Pasos para agregar un disparador de acción:

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**; haga clic en el ícono **Activadores de acción** (en la imagen a continuación).



2. En la pantalla Activadores de acción, se le presentarán los activadores existentes. Haga clic en el botón Agregar para crear un nuevo disparador.

Figura 33.3. Pantalla de activadores de acción




- En la pantalla Agregar disparador, definirá las condiciones bajo las cuales ejecutar un plan de acción.
- Complete la sección Ubicación del activador. Un activador de acción solo puede pertenecer a una única partición. Seleccione un sitio. Puede seleccionar Cualquiera para incluir todos los sitios en la partición o un sitio específico.

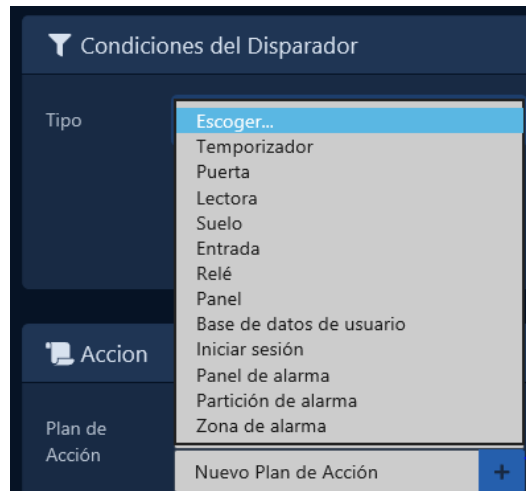
- En la sección **Condiciones de activación**, seleccione un **Tipo**. La mayoría de los tipos de condiciones tendrán un estado. Puede dejar esto como Cualquiera o seleccionar un Estado específico para cumplir con la condición de este disparador.

Tabla 33.2. Tipos y estados

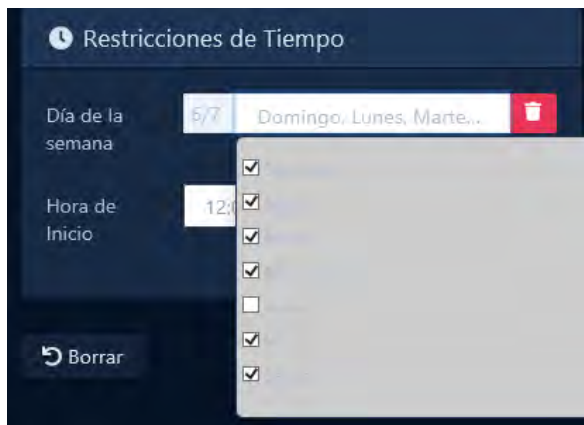
Tipo	Estados disponibles	Parámetros
Temporizador	n/a	Restricciones de tiempo: hora de inicio, intervalo, día de la semana
Puerta	Cualquiera, Abierto, Cerrado, Desbloqueado, Bloqueado, Apertura forzada, Mantenido abierto, Activación / desactivación de movimiento externo, Activación / desactivación de REX	Cualquier Puerta o una Puerta específica.
Lector	Acceso concedido, Acceso denegado, Entrada de primera tarjeta, Deslizamiento triple, Violación suave de APB, Violación dura de APB	Cualquier Lector o un Lector específico. Cualquier Usuario o un Usuario específico.
Piso	desbloqueado	Cualquier Usuario o un Usuario específico.
Entrada	Activado, Desactivado, Cortocircuitado, Desconectado	Cualquier entrada o una entrada específica.
Salida	Encendido apagado	Cualquier salida o una salida específica.
Panel	Desconectado, Conectado, Sensor de sabotaje, Alarma de emergencia	Cualquier Panel o un Panel específico.
UsuarioDb	Agregado, actualizado, eliminado	n / A
Iniciar sesión	Cualquiera, Éxito, Fracaso, Bloqueo	n / A

 **Nota:** Se puede configurar un temporizador de disparo para que se repita diariamente; la configuración de Intervalo se puede establecer en 1440 minutos.

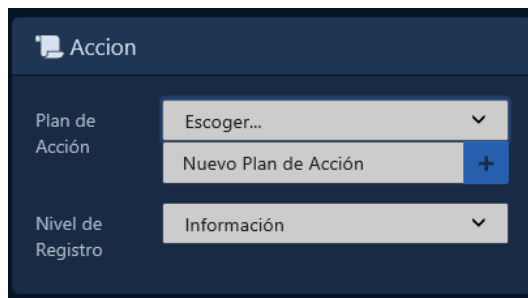
- Si es necesario, seleccione un estado. De forma predeterminada, se establecerá como Cualquiera. Algunos disparadores pueden tener opcionalmente uno o más parámetros. Esto le permitirá especificar un dispositivo específico (lector, puerta, piso, entrada, salida) o un usuario específico para cumplir con las Condiciones de disparo.



7. Complete la sección Restricciones de tiempo. Puede especificar qué días de la semana puede ocurrir el disparador y qué horas del día a través de Hora de inicio y Hora de finalización. Desviación de tiempo permitirá que las notificaciones (como las de apertura forzada o mantenida abierta) que no estén activas (es decir, provengan de un panel que estuvo fuera de línea durante un período de tiempo) sigan cumpliendo las condiciones del disparador si la hora de la notificación está por debajo de la deriva de tiempo permitida.



8. La última sección a llenar es la Acción. Seleccione un plan de acción del menú desplegable Plan de acción que se ejecutará cuando se cumplan las condiciones del desencadenante de la acción.



9. Haga clic en Crear. El disparador ahora ejecutará el plan de acción si se cumplen sus condiciones.

Conceptos de acción avanzados

Esta sección describirá las opciones más avanzadas disponibles al crear un plan de acción, por ejemplo, cómo usar variables, expresiones, cada acción, acciones If y el uso de la acción HTTP.

Variables en Planes de Acción

Los planes de acción tienen soporte para variables. Las variables se utilizan para almacenar información, a la que se puede hacer referencia o utilizar cuando se ejecuta un plan de acción. También puede permitirle etiquetar la información para que pueda leerse fácilmente.

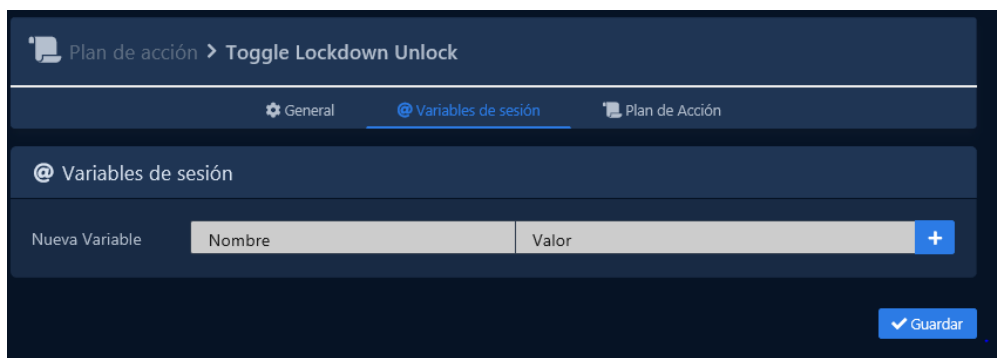
Hay cuatro tipos de variables disponibles:

- **Variables de sesión:** creadas durante el plan de acción o como parte del plan de acción. Puede contener números, cadenas, matrices, objetos, otras variables o el resultado de una expresión.
- **Variables de activación:** Variables que están disponibles para ser referenciadas o utilizadas en el plan de acción que se basan en el activador que lo ejecuta. Los ejemplos pueden incluir información sobre el administrador para ejecutar el plan o el nombre de la puerta/lector/usuario que activó el activador.
- **Variables de último resultado:** Variables que solo están disponibles para ser referenciadas en la acción inmediatamente después de una acción HTTP, PING o Cada acción. Estas variables contendrán los resultados de la acción anterior. Un ejemplo podría ser una solicitud HTTP GET que tendría los resultados de la acción almacenados en una variable llamada 'LastResult.Content'.
- **Variables globales:** variables que están disponibles para ser referenciadas globalmente a través de planes de acción dentro de la misma partición. Estas variables pueden contener números, matrices, objetos, otras variables o el resultado de una expresión que se puede leer, actualizar o borrar.

Crear una variable

There are two ways to create variables that can be used during an action plan:

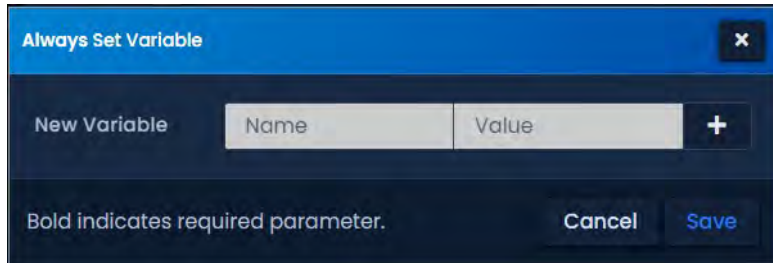
1. En la pantalla Editar plan de acción, vaya a la pestaña Variables de sesión.
 - En la pestaña Variables de sesión, verá las variables existentes. Coloque un nombre y un valor junto a la etiqueta Nueva variable.



- Haga clic en el botón '+' a la derecha del nuevo valor de la variable. También puede editar las variables de sesión existentes en esta página.
- Clic en Guardar. Ahora se puede hacer referencia a la variable de sesión como @{Session.VariableName} como cualquier parámetro en cualquier acción.

2. En la pantalla Editar plan de acción, vaya a la pestaña Plan de acción.

- En la lista de acciones de la izquierda, expanda la sección General.
- Haga clic y arrastre la acción Establecer variable a la Acción inicial o conéctela a la condición Éxito, Fallo o Siempre de cualquier acción existente.



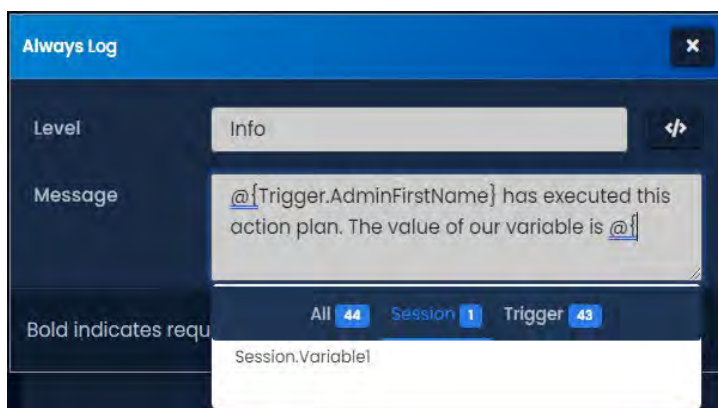
- Coloque un nombre y un valor junto a la etiqueta Nueva variable. El valor puede contener una expresión, otra variable o un valor bruto.
- Haga clic en el botón '+' a la derecha del nuevo valor de la variable. Puede agregar tantas variables como necesite durante una acción de establecer variable. También puede editar las variables de sesión existentes desde aquí.
- Haga clic en Aceptar. Ahora se puede hacer referencia a la variable de sesión como @{Session.VariableName} como cualquier parámetro en cualquiera de las siguientes acciones.

Uso de variables en acciones

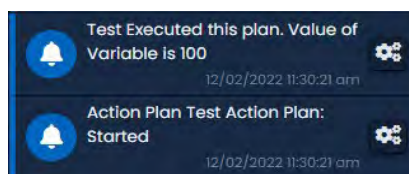
Las variables de todo tipo se utilizan principalmente como parámetros en las acciones.

Al agregar una acción (como la acción Registrar), puede usar una variable escribiendo '{@Variable-Type.VariableName}'. Si escribe '@{' verá una lista de variables disponibles de todos los tipos. Puede usar esto en lugar de escribir el nombre de la variable.

Figura 33.4. Lista de autocompletar variables



Cuando se ejecuta el plan de acción, cualquier variable se sustituirá o se calculará en el valor (como se ve en nuestro ejemplo a continuación).



Expresiones en planes de acción

Los Planes de Acción tienen soporte para Expresiones. Una expresión es una unidad de código que se evalúa como un valor. Esto se puede usar para determinar verdadero o falso (usado con la acción If) a través de un operador de comparación. También puedes hacer operaciones aritméticas u operaciones con cadenas.

Al agregar parámetros a una acción (como la acción Registrar), puede usar una expresión escribiendo '@[]'. Cualquier cosa dentro de los corchetes se evaluará como una expresión. Puede usar variables dentro de expresiones y usar expresiones para asignar un valor a una variable. El siguiente cuadro demostrará varios ejemplos.

Tabla 33.3. Ejemplos de expresiones

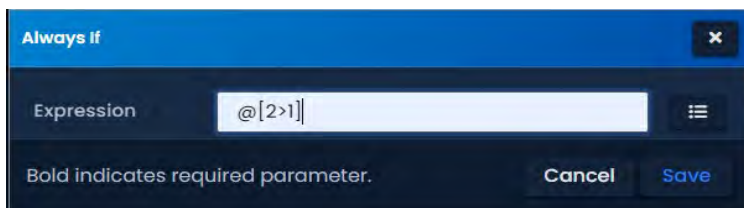
Expresión	Evaluación
@[100+50]	150
@[1>4]	Falsa
@["TestString".length]	10
@["Test"+"String"]	TestString
@[@{LastResult.Index}+1]	Índice variable de la acción anterior + 1
@[100==100]	Verdadera
@[100/25]	4

El uso de expresiones puede hacer que sus planes de acción sean más poderosos y permitir operaciones lógicas como la acción Si.

Si acción

La acción SI le permite hacer cadenas condicionales de acciones. La acción SI utilizará una expresión como su único parámetro. Si la expresión se evalúa como verdadera, la siguiente acción que se ejecuta después de la acción SI será la acción en la condición Éxito. Si la expresión se evalúa como cualquier cosa menos verdadera, se considerará falsa y se ejecutará la acción en la condición de falla.

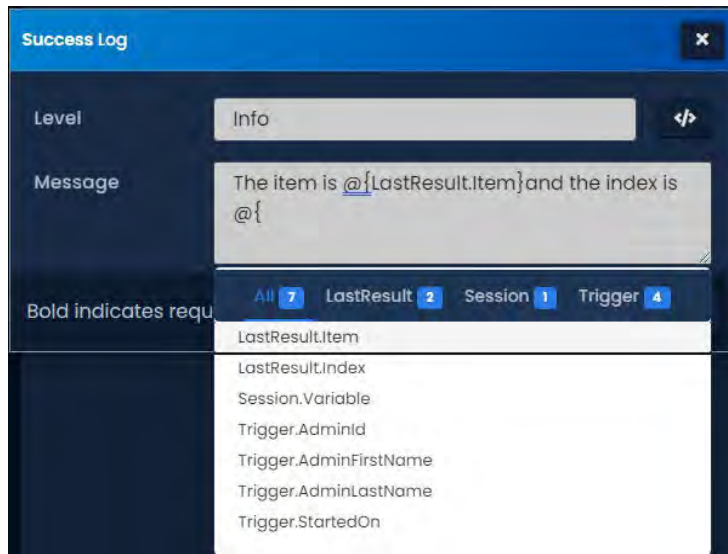
En nuestro ejemplo, hemos arrastrado una acción Si de la sección general a nuestro cuadro de acción inicial.



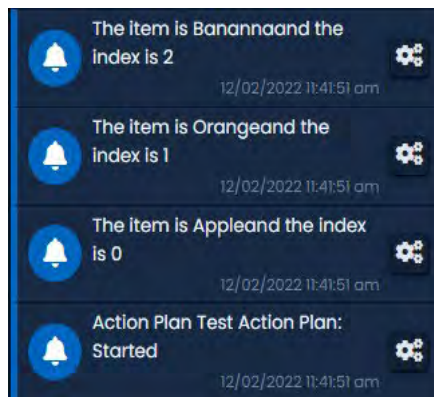
'@[2>1]' se evaluará como verdadero porque 2 es más que 1. Configuraremos acciones de registro en la condición Éxito (verdadero), Fallo (falso) y siempre. Ahora nuestro plan de acción se ve así:

La acción Si es una herramienta poderosa que puede hacer que los planes de acción sean más personalizables y más reactivos a diferentes circunstancias.



Figura 33.7. Cada acción Últimas variables de resultado

Cuando se ejecuta la acción Cada, todos los elementos se procesarán individualmente en la cadena de éxito. Las acciones adicionales se ejecutarán independientemente de las acciones de otros elementos y no tendrán acceso a sus variables. No se ejecutarán en ningún orden específico. Puede usar la acción del temporizador junto con la variable LastResult.Index si necesita que cada elemento se ejecute en diferentes intervalos.

Figura 33.8. Cada Acción Ejecutada

Acción HTTP

La acción HTTP le permite hacer que el servidor VAX envíe solicitudes HTTP a sistemas de terceros, incluidas otras API web. También puede enviar solicitudes HTTP a VAX a través de la API web VAX REST. Una vez que el destino procesa la solicitud, la respuesta también puede ser analizada y utilizada por otras acciones.

Use los siguientes pasos para crear una acción HTTP:

1. En la pantalla Editar plan de acción, vaya a la pestaña Plan de acción.
2. En la lista de acciones de la izquierda, expanda la sección Red.

- Haga clic y arrastre la acción de solicitud HTTP a la acción inicial o conéctela a la condición Correcto, Incorrecto o Siempre de cualquier acción existente.

- Defina el tiempo de espera (60 segundos por defecto). Cantidad de tiempo después de que se envía la solicitud antes de que la acción se encadene a la condición de error.
- Defina la dirección a la que se enviará la solicitud HTTP (ejemplo: `https://localhost:11001/api/users`).
- Defina el método HTTP (GET, PUT, POST, OPTIONS, DELETE). El método que elija dependerá del sistema de terceros. La mayoría de las solicitudes de información utilizarán el método GET.
- De ser requerido, complete el Cuerpo de la solicitud. Aquí es donde puede incluir parámetros que utilizará el sistema receptor.
- Establezca el Tipo de contenido según los requisitos del sistema de terceros (Cualquiera, Cadena, JOSN, XML). Las llamadas web a VAX usarán JSON.

Consejo : El tipo de contenido 'Archivo' debe usarse si el resultado de la solicitud es un archivo. Esto se puede usar para enviar informes e imágenes por correo electrónico.

- Si se requieren encabezados específicos, ingrese el nombre y el valor del encabezado y haga clic en el botón "+". Puede agregar varios encabezados si es necesario.
- Marque Omitir validación de certificado si el sistema de terceros o el servidor VAX está utilizando un certificado SSL no válido.
- Marque Usar contenedor de cookies si desea que el VAX administre las cookies correspondientes a esta solicitud HTTP o solicitudes posteriores. Esto es útil si inicia sesión en otros sistemas.
- Haga clic en Aceptar.

Si hay una acción dentro de la condición Éxito o Fallo de la acción de solicitud HTTP, tendrá acceso a 2 variables únicas.

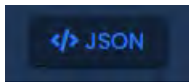
- '{@LastResult.StatusCode}': Esta variable contendrá el código de estado HTTP devuelto por la dirección de destino.
- '{@LastResult.Content}': Esta variable contendrá la respuesta devuelta por la dirección de destino. Puede guardar esta variable como una variable de sesión para su uso posterior o usar esta variable en la acción que sigue a la acción de solicitud HTTP. Si necesita acceder a una propiedad específica, puede usar '{@LastResult.Content.PropertyName}'

Exportación e importación de planes de acción

Esta sección describirá cómo exportar e importar un plan de acción.

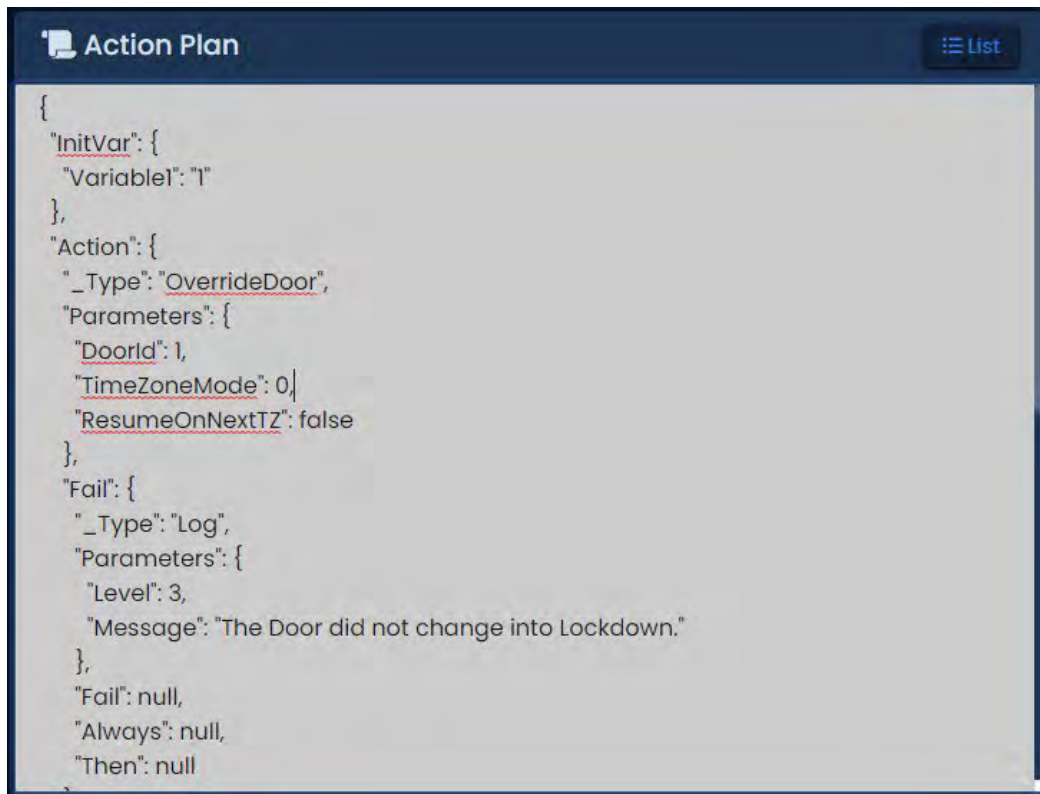
Los planes de acción en VAX se pueden exportar e importar como cadenas JSON. Use los siguientes pasos para exportar e importar un plan de acción:

1. En la pantalla Editar plan de acción, vaya a la pestaña Plan de acción.
2. Haga clic en el botón JSON en el lado derecho de la pantalla. El plan de acción actual ahora mostrará la vista JSON de su plan de acción.



3. En la vista JSON del plan de acción, seleccione todo el contenido de la vista JSON.
4. Haga clic derecho en la pantalla después de seleccionar la vista JSON completa y seleccione 'copiar' en el menú contextual. El contenido del Plan de Acción está ahora en su portapapeles.
5. Navegue a la pantalla Editar para un Plan de acción existente o cree uno nuevo.
6. Haga clic en la pestaña Plan de acción.
7. Haga clic en el botón JSON en el lado derecho de la pantalla. Seleccione todo el contenido de la vista JSON.
8. Haga clic con el botón derecho en la pantalla después de seleccionar la vista JSON completa y seleccione "pegar" en el menú contextual. El Plan de acción ahora se parecerá al Plan de acción que copió de.

Figura 33.9. Vista JSON del plan de acción



```
{
  "InitVar": {
    "Variable": "1"
  },
  "Action": {
    "_Type": "OverrideDoor",
    "Parameters": {
      "DoorId": 1,
      "TimeZoneMode": 0,
      "ResumeOnNextTZ": false
    },
    "Fail": {
      "_Type": "Log",
      "Parameters": {
        "Level": 3,
        "Message": "The Door did not change into Lockdown."
      },
      "Fail": null,
      "Always": null,
      "Then": null
    }
  }
}
```

Capítulo 34. Mapas interactivos

Este capítulo demostrará cómo configurar y ver mapas interactivos dentro de VAX.

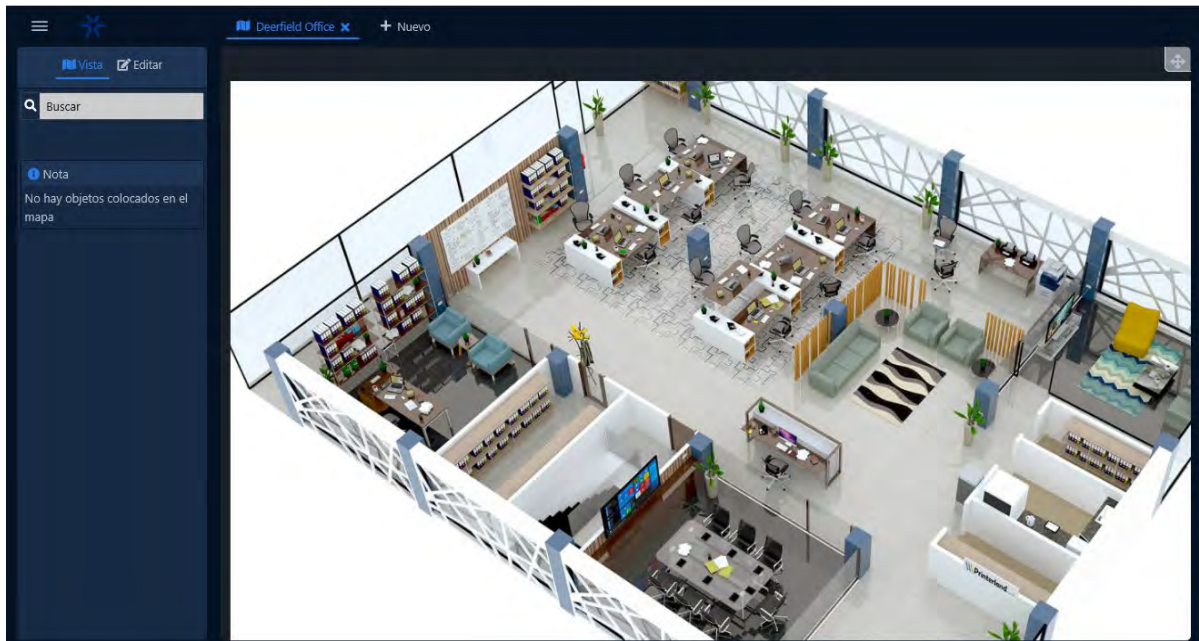
Los mapas interactivos se utilizan para crear una representación visual de un edificio o sitio con fines de monitoreo. Los componentes del sistema de control de acceso se colocan en la parte superior de un diseño del edificio. Esto incluye:

- Puertas
- Pisos de ascensor
- Entradas
- Salidas
- Cámaras
- Áreas

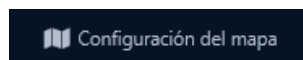
Figura 34.1. Visor de mapas

Agregar un Mapa

Siga estos pasos para agregar un mapa a VAX.



1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Sistema**, haga clic en el icono **Configuración del mapa** (en la imagen a continuación).



2. En la pantalla **Configuración del mapa**, todos los **mapas** que ya haya configurado se enumeran aquí. Haga clic en el botón **Agregar** en esta pantalla.
3. En la pantalla **Agregar mapa**, tendrá varios campos para completar.

Figura 34.2. Pantalla de Agregar mapas

Tabla 34.1. Agregar un Mapa

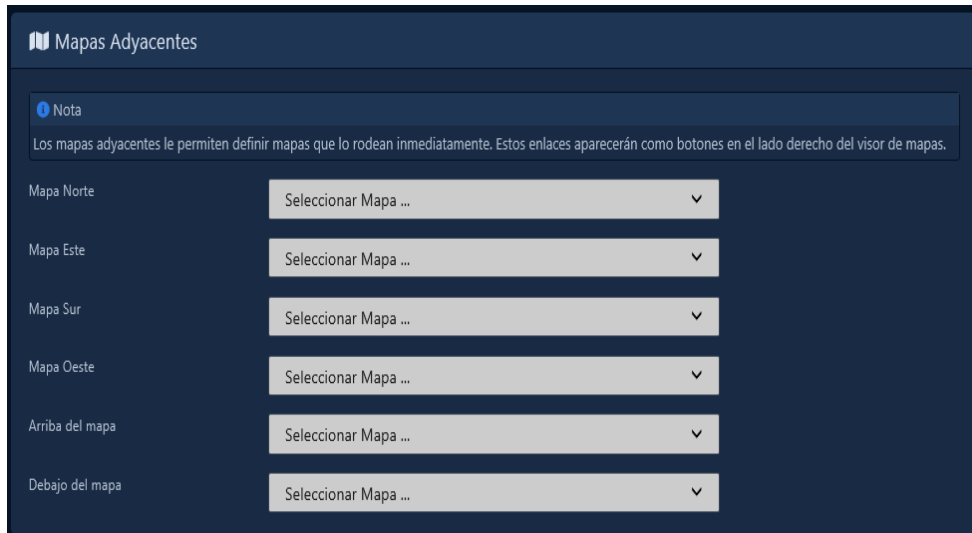
Cuadro de texto/Menú desplegable	Descripción
Nombre	Nombre único de su mapa. Acepta de 2 a 100 caracteres. Recomendamos nombrar su mapa por su ubicación o contenido.
Descripción	Descripción opcional del mapa. Acepta hasta 255 caracteres.
Imagen	Elija una imagen local para cargarla como fondo del mapa. Se admiten PNG, GIF, JPG y BMP. La imagen se convertirá a PNG.
Particion	Elija una partición a la que esté asociado este mapa. Esto influirá en qué objetos se pueden colocar en el mapa según el alcance de la partición.
Sitio	Campo opcional donde se puede asociar un Sitio al mapa. Esto influirá en qué objetos se pueden colocar en el mapa según el alcance del sitio.

- Una vez que haya completado todos los campos obligatorios, haga clic en el botón **Guardar** para agregar el mapa. Se le solicitarán las opciones para agregar un mapa adicional o para Continuar la configuración, lo que lo llevará a la pantalla **Configuración** del mapa para el mapa que acaba de agregar.

Mapas adyacentes

En sistemas con varios pisos o edificios para monitorear, puede ser beneficioso configurar dónde está cada mapa en relación con otros mapas. Si el edificio tiene varios pisos, puede configurar el piso 2 como si estuviera sobre el piso 1. Esto puede acelerar la navegación entre los mapas.

Al editar un mapa, puede asignar enlaces entre mapas en la pestaña Mapas adyacentes. Simplemente complete cualquier menú desplegable con el nombre de otro mapa.

Figura 34.3. Mapas Adyacentes

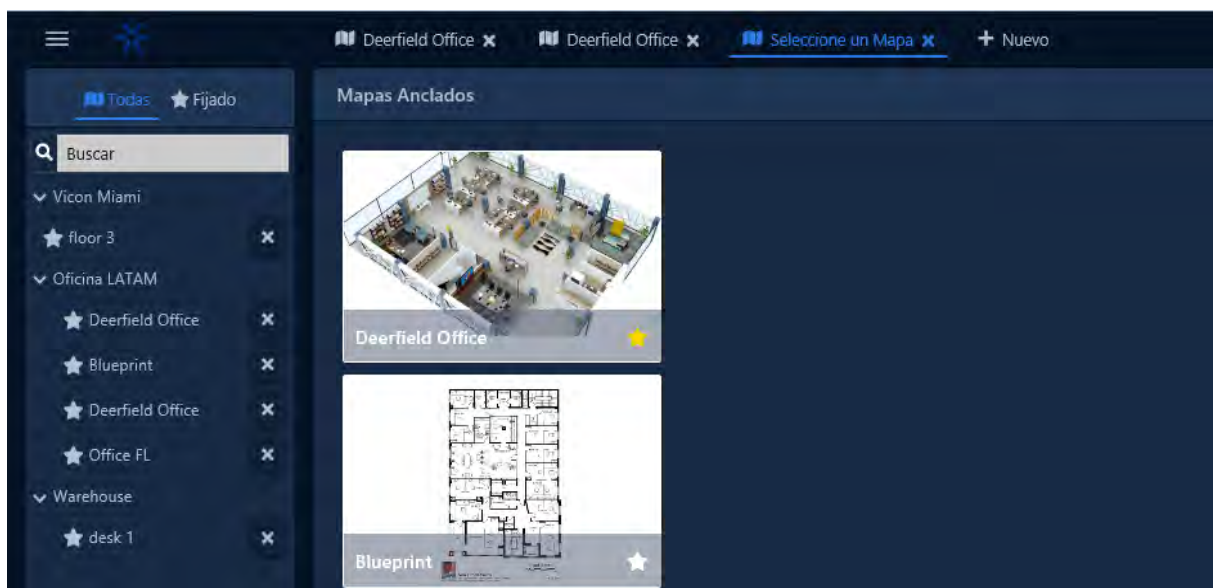
Agregar objetos a los mapas

Esta sección cubrirá cómo agregar varios objetos de control de acceso a un mapa, como puertas, pisos, entradas, salidas y cámaras.

1. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**, haga clic en el ícono **Mapas** (en la imagen a continuación). Se abrirá una nueva ventana en su navegador web.



2. En Visor de mapas, se le mostrará la pestaña **Seleccionar un mapa**. Todos los mapas que ya haya configurado se enumeran aquí. Aparecerá una miniatura de cada mapa con su título.

Figura 34.4. Seleccionar un Mapa

Consejo: Al hacer clic en el ícono de estrella a la derecha del nombre del mapa, se fijará el mapa al frente de la lista de miniaturas.

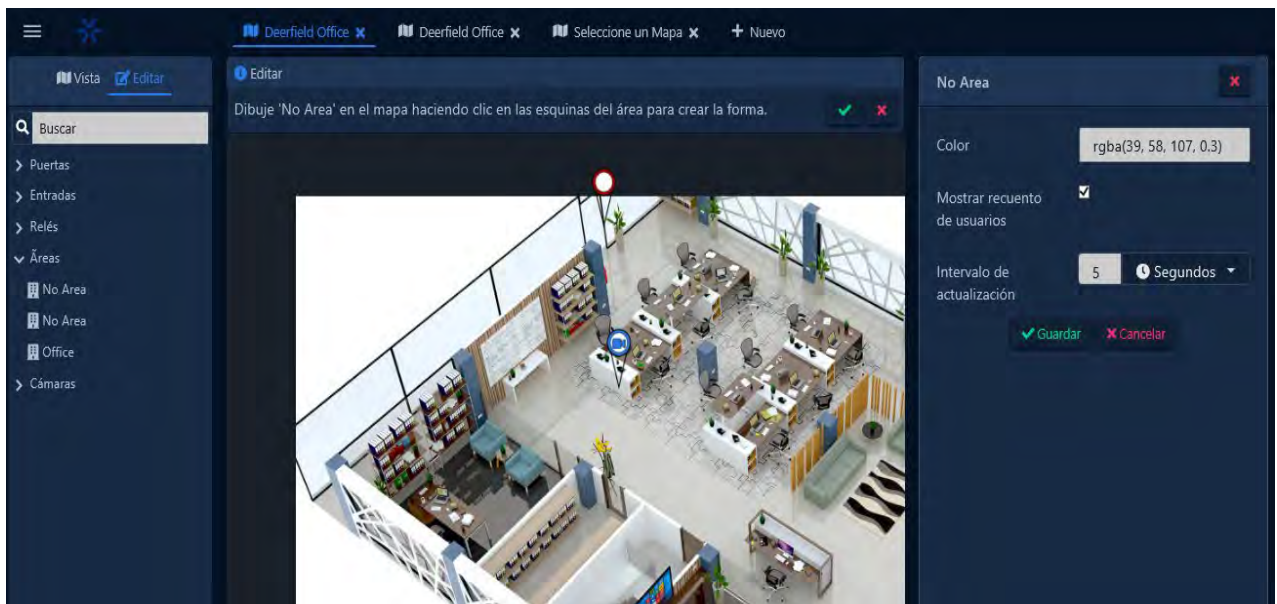
3. Seleccione un mapa haciendo clic en él. Ahora se mostrará el mapa.

4. Debe hacer clic en el botón Editar cerca de la parte superior izquierda de la pantalla para agregar objetos al mapa.
5. Después de hacer clic en el botón Editar, ahora se muestra una lista de tipos de objetos disponibles en el lado izquierdo de la página. Haga clic en el nombre del tipo de objeto (Puertas, Elevadores, etc.) para expandir los objetos de ese tipo. Al hacer clic en Puertas, se mostrarán los objetos de puerta que se pueden mostrar en el mapa.

Nota: Solo los objetos que aún no están colocados en el mapa aparecerán en la lista de objetos

6. Para colocar un objeto en el mapa, haga clic y arrastre el objeto desde el lado izquierdo de la pantalla hasta el mapa que se muestra en el centro. Ahora puede colocar el objeto en relación con su posición en el mundo real.

Figure 34.5. Adding Objects to a Map



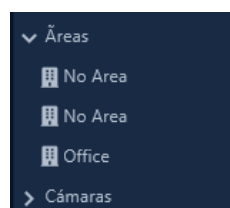
7. Para eliminar un objeto del mapa, haga clic en el objeto del mapa que desea eliminar. Aparecerá un menú en el lado derecho que le permitirá eliminar el objeto del mapa.
8. Una vez que haya agregado los objetos requeridos al mapa, haga clic en el botón Ver en la parte superior izquierda.

Dibujar un área

Las áreas se pueden dibujar en el mapa para mostrar visualmente la separación entre áreas y mostrar quién está en cada área. Puede encontrar más información sobre las áreas en la sección llamada "Editar sitios y áreas: Áreas".

Nota: Las áreas de dibujo no son compatibles con los navegadores web móviles.

1. Al editar un mapa, expanda los tipos de objetos de Áreas haciendo clic en Áreas en el lado izquierdo de la página.

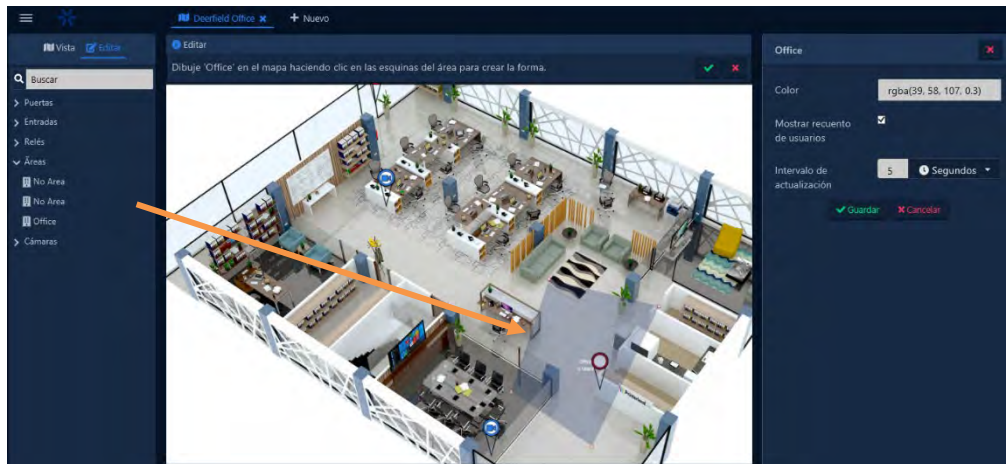


- Haga clic en el área que desea dibujar en el mapa. Aparecerá un menú en el lado derecho de la pantalla.
- Ahora puede dibujar el área en el mapa haciendo clic en las esquinas del área para crear una forma.

Controles al dibujar el mapa:

- Agregar punto: clic izquierdo
 - Quitar punto: clic derecho
 - Mover punto (snap): clic izquierdo + arrastrar
 - Mover punto (arrastré libre): Mayús + Clic izquierdo + Arrastrar
- El color y la transparencia del área se pueden modificar en el menú del lado derecho de la pantalla si es necesario.
 - Haga clic en Guardar para guardar el lugar donde se dibujó el área. Haga clic en cancelar para comenzar de nuevo.

Figura 34.6. Dibujar un área



Visualización y seguimiento con mapas

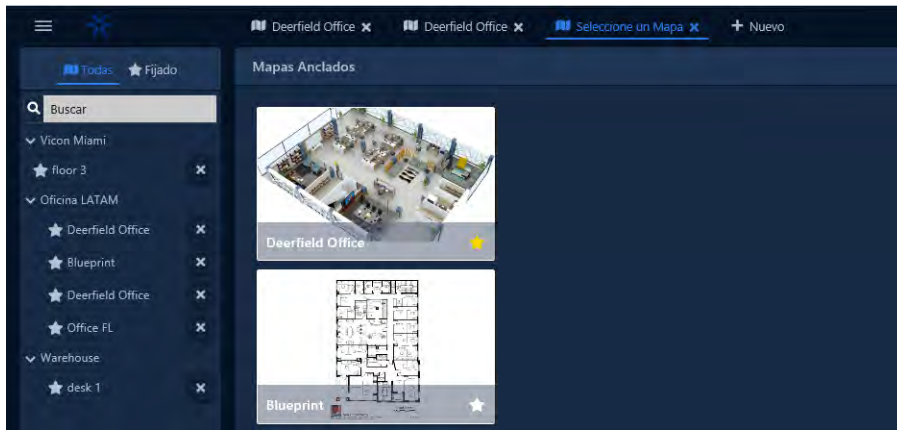
Esta sección repasará las opciones disponibles al ver un mapa. Use los siguientes pasos para ver un mapa.

- En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Día a día**, haga clic en el ícono **Mapas** (en la imagen a continuación). Se abrirá una nueva ventana en su navegador web.



- En el Visor de mapas, se le mostrará la pestaña **Seleccionar un mapa**, todos los mapas que ya haya configurado se enumeran aquí. Aparecerá una miniatura de cada mapa con su título.

Figura 34.7. Seleccionar un Mapa



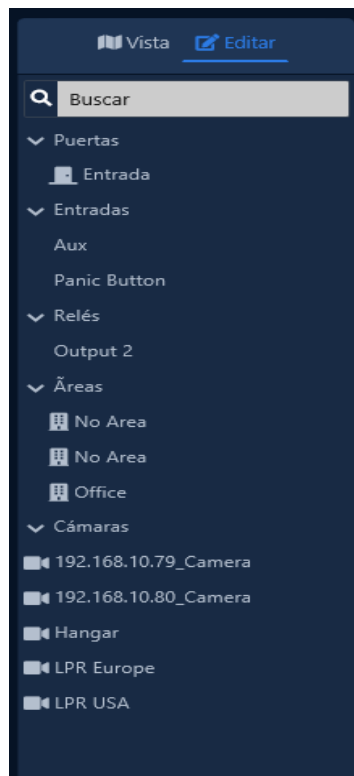
3. Seleccione un mapa haciendo clic en él. El mapa ahora se mostrará junto con cualquier objeto que se haya colocado en el mapa.

Consejo: Puede tener más de un mapa abierto a la vez haciendo clic en el botón Nuevo en la parte superior de la pantalla. Los mapas abiertos se mostrarán como pestañas en la parte superior de la página

Barra lateral de objetos del mapa

El lado izquierdo de la página incluirá una lista de objetos que se han colocado en el mapa. Los objetos se separan en categorías. Puede expandir la categoría haciendo clic en el nombre de la categoría (Puertas, Ascensores, Cámaras, Áreas, Entradas, Salidas, Acciones).

Figura 34.9. Barra lateral de objetos del mapa



En la barra lateral de objetos de mapa, puede ver el estado en tiempo real de los objetos. El mismo estado se muestra en el mapa.

- Las puertas mostrarán en qué modo están según el código de colores.

- Las puertas con contactos de puerta mostrarán si están abiertas o cerradas.
- El color de las puertas que se mantienen abiertas o forzadas se cambiará a rojo y mostrarán el texto de alerta a la derecha del nombre.
- Los objetos que han sido anulados mostrarán su nombre en rojo.
- Los objetos conectados a los paneles que están desconectados aparecerán en gris.
- Al hacer clic con el botón izquierdo en un objeto de la lista, se mostrará su menú contextual correspondiente en el lado derecho de la página y se moverá el visor de mapas al objeto en el mapa.
- Al hacer clic con el botón derecho en un objeto de la lista, se mostrará un menú contextual para el objeto. Puede usar esto para pulsar una puerta, ver una cámara y más.

Barra lateral de detalles del objeto

Cuando se selecciona un objeto en el mapa o desde la barra lateral de objetos del mapa, aparecerá una barra lateral en el lado derecho de la página con detalles y opciones para el objeto seleccionado.

El contenido de los detalles del objeto dependerá del tipo de objeto seleccionado.

Figura 34.10. Ejemplos de barra lateral de detalles de objeto



Consejo:

Si hay una cámara asociada con el objeto seleccionado, aparecerá una ventana de cámara en vivo en la barra lateral.

Capítulo 35. Integración de terceros

Este capítulo incluye información sobre cómo VAX se integra con sistemas de software de terceros. Esto incluye el software de credencialización fotográfica cardPresso® y los sistemas de bloqueo inalámbrico ASSA ABLOY.

Lock Systems Abloy® Aperio™

Este capítulo cubre la configuración y los requisitos de software/hardware del uso de los sistemas Assa Abloy Aperio Lock con los controladores PoE de Vicon Industries. Para obtener más información sobre los sistemas Assa Abloy Aperio, visite <http://www.assaabloy.ca/en/local/ca/Products/New-Innovative-Product/Aperio-wireless/>

Requisitos de Software / Hardware

⚠ Advertencia

Debe estar certificado por el distribuidor de Assa Abloy para pedir productos de Assa Abloy de Vicon Industries. Vicon Industries es un distribuidor certificado de productos Assa Abloy.

Asegúrese de tener los siguientes elementos antes de proceder a la instalación:

- Panel VAX Aperio (2, 4 u 8 puertas) con módulo Plug in de interfaz RS-485
- Assa Abloy AH30R12/Aperio Hub Comm RS-485*
- Herramienta de aplicación de programación de dongle de radio USB Assa Abloy*
- Aplicación de programación Aperio*
- Archivo de clave de licencia de Aperio*
- Cerraduras inalámbricas Aperio
- * Incluido en el Kit Aperio

Configuración de Hardware

Esta sección cubrirá el aspecto del hardware de la conexión del concentrador Aperio al panel VAX Aperio. Esta sección incluye referencias visuales y especificaciones de cables.

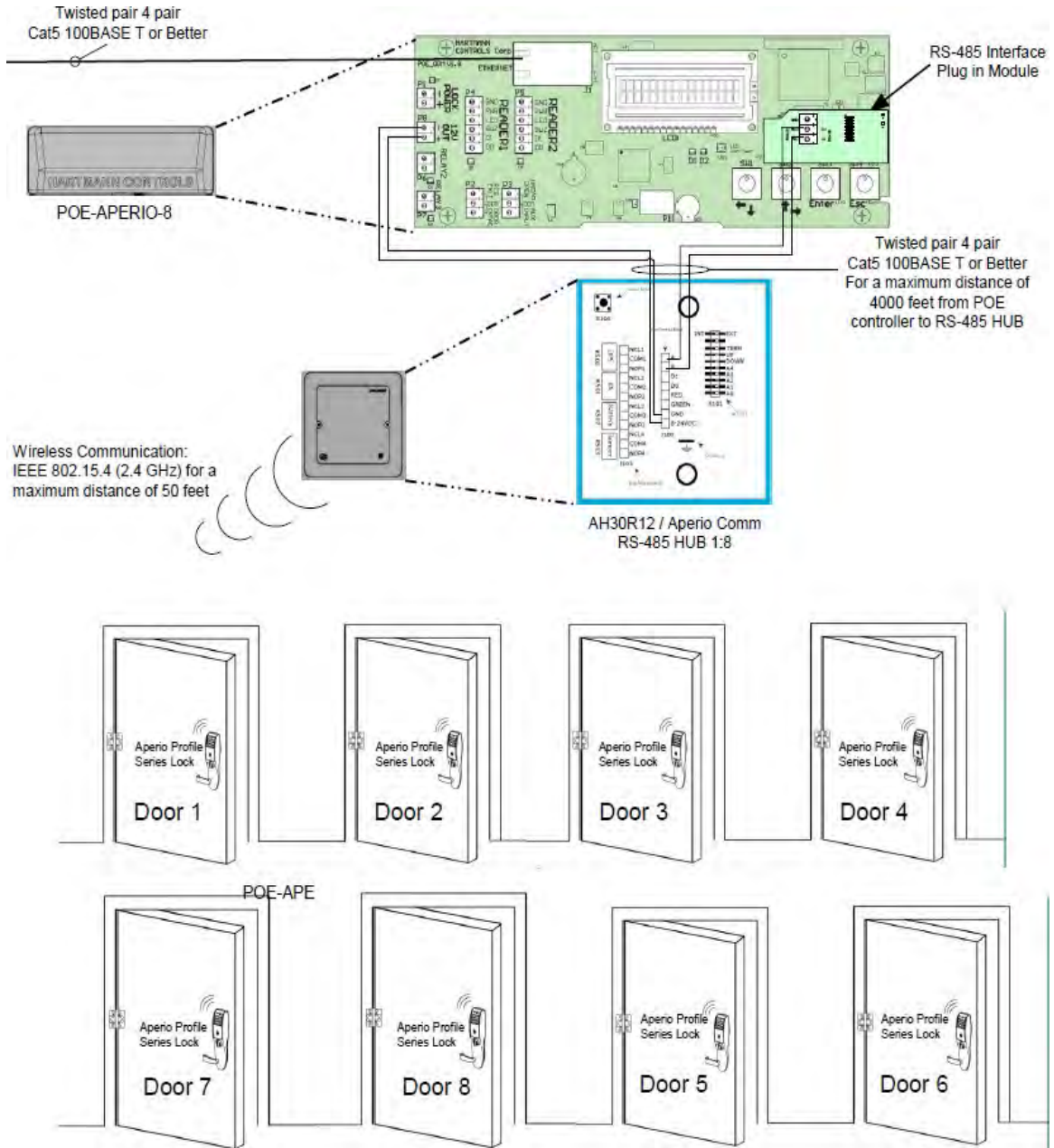
El panel VAX Aperio se comunica con el concentrador Aperio a través de una conexión RS-485. Se incluye e instala un módulo de conexión RS-485 en todos los paneles Aperio.

Para conectar el Aperio Panel al Aperio Hub, siga estos pasos:

1. Designe un par de hilos de cable RS-485 que proporcionarán alimentación al concentrador Aperio desde el panel Aperio.
2. En el lado del panel del RS-485, conecte el cable negativo y positivo al bloque de cabecera 12V OUT en el lado izquierdo del panel.
3. En el concentrador Aperio, conecte el otro lado de los cables de alimentación designados al bloque de encabezado etiquetado como 9-24 VDC y GND. Asegúrese de que la polaridad coincida con lo que está conectado al panel.
4. Designe un par de hilos de cable RS-485 que proporcionarán comunicación al concentrador Aperio desde el panel Aperio.
5. En el lado del panel del cable RS-485, conecte los cables de datos al bloque de encabezado del módulo enchufable RS-485 en RX+(D+) y RX-(D-).

- En el concentrador Aperio, conecte el otro lado de los cables de comunicación designados al bloque de encabezado etiquetado como A y B. RX+ (D+) del panel se conectará a A en el concentrador Aperio. RX- (D-) del Panel se conectará a B en el Aperio Hub.

El siguiente diagrama demuestra visualmente la topología de comunicación del panel Aperio con el concentrador Aperio.

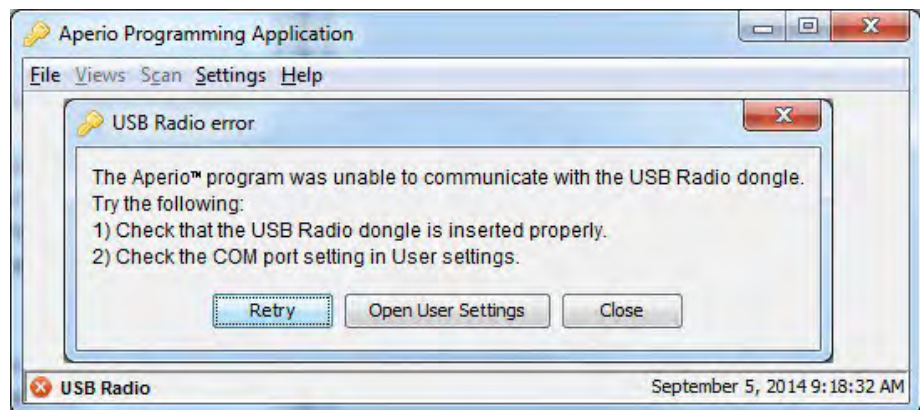
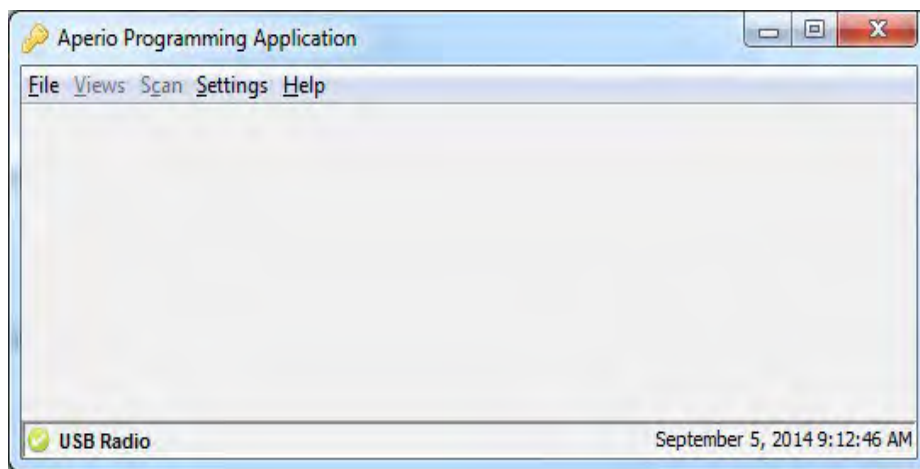


Configuración del software: aplicación de programación Aperio

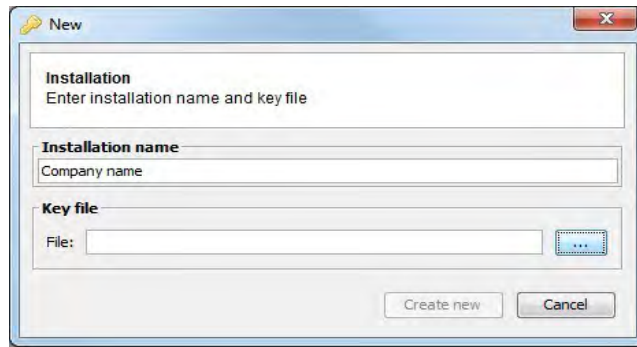
Esta sección cubrirá los aspectos de software de la configuración del concentrador Aperio para comunicarse con las cerraduras Aperio a través de la aplicación de programación Aperio. Es importante emparejar todas sus cerraduras con Aperio Hub antes de agregar las puertas en VAX.

- En la computadora portátil o PC programará Aperio Hub, descargue la aplicación de programación Aperio desde su kit Aperio o desde http://www.assaabloyresources.com.au/downloads/eac/Aperio_Common.zip

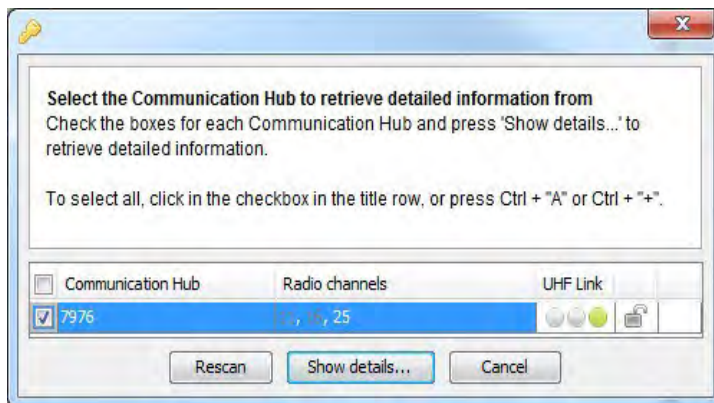
2. Descomprima Aperio_Common.zip en su computadora e instale la aplicación.
3. Conecte su Assa Abloy USB Radio Dongle e instale el controlador (ubicado en el directorio de instalación de la aplicación de programación Aperio)).
Nota: Si tiene problemas para instalar el controlador de dongle o la aplicación de programación Aperio, comuníquese con el soporte técnico interno o con el soporte de Assa Abloy.
4. Asegúrese de que en el Administrador de dispositivos de Windows se reconozca y funcione "Tritech TriBee USB".
5. Inicie la aplicación de programación Aperio desde su menú de inicio. Si Tritech Tribee está correctamente instalado y enchufado, verá un círculo verde en la parte inferior izquierda de la aplicación junto a USB Radio. Si el dongle USB no está instalado correctamente o no está conectado a la PC/Laptop, recibirá un error.



6. Una vez que la aplicación de programación Aperio haya detectado su radio USB, haga clic en Archivo y luego en Nuevo en el menú superior.
7. Introduzca un nombre de instalación (ejemplo: nombre de la empresa). Examine y seleccione el archivo clave proporcionado en su kit Aperio o recibido de Assa Abloy. Haga clic en Crear nuevo; se le pedirá que introduzca una contraseña para la instalación. Se requieren al menos 8 caracteres.



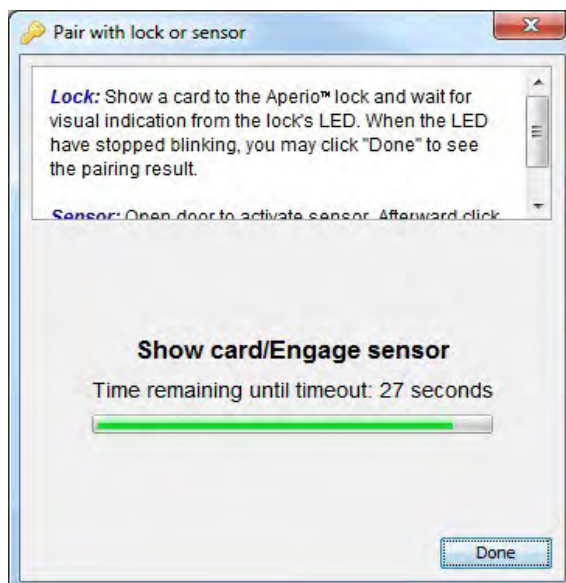
8. Una vez que ingrese su contraseña, iniciará sesión y la aplicación comenzará a buscar automáticamente Centros de comunicación. Haga clic en la casilla de verificación junto al centro de comunicaciones que desea configurar; haga clic en Mostrar detalles.



9. Ahora podemos comenzar a emparejar nuestras cerraduras con el centro de comunicación. Haga clic derecho en el centro de comunicación que desea configurar. Haga clic en el submenú del concentrador de comunicaciones en el concentrador con el que desea vincular cerraduras y haga clic en "vincular con cerradura o sensor".

Nota: Asegúrese de que el número del centro de comunicaciones coincida con el número del centro físico; esto es especialmente útil cuando se configuran varios concentradores al mismo tiempo.

10. Ahora aparecerá la ventana Emparejar con candado o sensor; tendrá 30 segundos para presentar una tarjeta a la cerradura que desea emparejar. Espere hasta que el LED de bloqueo deje de parpadear antes de hacer clic en "Listo".



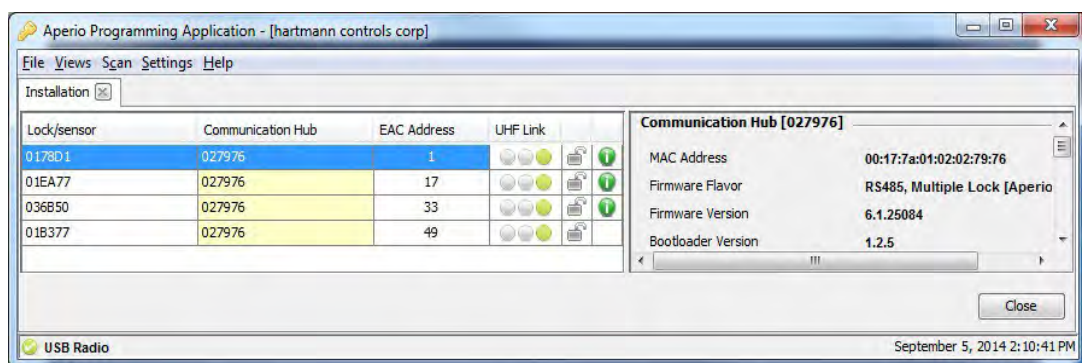
11. Si el emparejamiento es exitoso, verá "Communication Hub emparejado correctamente con lo siguiente: XXXXXX" en la ventana de emparejamiento con candado o sensor, donde XXXXXX es el número impreso en la parte posterior de la cerradura.

 **Nota**

Algunos modelos de cerradura requieren que el lado de salida libre de la manija de la puerta esté hacia abajo y que la tarjeta presentada antes se sincronice con el Centro de comunicaciones. Si su emparejamiento falla, intente esto antes de solucionar otros aspectos

12. Repite el proceso de emparejamiento con todas las cerraduras que quieras configurar. Una vez completo; tome nota de la dirección EAC de cada cerradura y la ID del sensor de cerradura en la ventana de instalación, necesitaremos la dirección EAC de cada cerradura para configurar la puerta en VAX

Ejemplos de 4 cerraduras sincronizadas dentro de la aplicación de programación Aperio



Configuración del software: Paneles y Puertas VAX Aperio

Esta sección cubrirá el aspecto del software de agregar paneles VAX Aperio a VAX y configurar cerraduras Aperio en VAX que se configuraron en la aplicación de programación Aperio. Para obtener más información sobre el emparejamiento de cerraduras con Aperio Hub, consulte la sección llamada "Configuración del software: aplicación de programación Aperio".

Lo siguiente debe completarse antes de agregar el panel VAX Aperio (2, 4 u 8 puertas):

- El hardware se ha instalado, cableado y funciona (controlador Aperio y concentrador de comunicación Aperio).
 - Las cerraduras Aperio se programaron mediante la aplicación de programación Aperio.
 - Las direcciones EAC y los ID de bloqueo se han anotado desde la aplicación de programación Aperio.
 - Los candados están instalados o en espera de instalación dentro de los 50 pies del centro de comunicación.
1. Una vez que se hayan cumplido los requisitos anteriores, agregue el Panel de la misma manera que agregaría un Panel de puerta normal, asegurándose de seleccionar el modelo de Panel apropiado al agregarlo. Para obtener información más detallada sobre cómo agregar un panel, consulte la sección llamada "Agregar un panel al control de acceso VAX".
 2. En la barra lateral, desplácese hacia abajo hasta la sección titulada Hardware; haga clic en el icono Puertas.
 3. En la pantalla Puertas, haga clic en Agregar. En la pantalla Agregar puerta, ingrese los campos como lo haría en una puerta normal. Notará que cuando cambie el menú desplegable del Panel

al Panel de Aperio, aparecerá un nuevo cuadro de texto llamado Dirección de Aperio. Este campo es donde ingresaremos la dirección EAC del bloqueo que recibimos de la aplicación de programación Aperio.

4. Una vez que haya completado los campos obligatorios, incluida la dirección Aperio/EAC correspondiente, haga clic en Guardar. Para obtener información adicional sobre cómo agregar una puerta y configurar lectores, consulte el Capítulo 8, Configuración de una puerta.
5. Repita el proceso de adición de puertas en todas las cerraduras; Al agregar puertas Aperio adicionales, notará que el puerto en el panel se incrementará automáticamente en el menú desplegable..
6. Una vez que todas sus puertas estén configuradas, agregue un usuario de prueba y colóquelo en un grupo de privilegios de acceso que tenga acceso a los lectores que creó en sus puertas Aperio. Realice una actualización de todos los paneles y pruebe la tarjeta asociada con el usuario de prueba.

Capítulo 36. Información para administradores de red y dominio

Configuración del acceso remoto avanzado a través de Internet

Esta sección cubrirá cómo conectar un panel de Vicon Industries de cualquier tipo a un servidor VAX a través de Internet. Esta sección también cubrirá cómo conectar un cliente de navegación web al servidor VAX a través de Internet.

Cómo se comunican los paneles

El servidor VAX es un dispositivo de escucha que escucha en el puerto TCP/UDP 9876 para conexiones del Panel. Los paneles se comunican con el servidor ya sea por nombre DNS o IP en el puerto TCP/UDP 9876.

Después de configurar el Panel con la dirección IP del servidor, el Panel envía un "paquete" de datos introductorios dirigido a la IP del servidor. El conmutador o enrutador busca el destino IP de este paquete y aplica cierta lógica. Primero verificará su tabla de enrutamiento y comparará la dirección con los dispositivos o redes que conoce. Si el servidor estuviera en la misma red, reenviaría ese paquete al conmutador más cercano a ese servidor. Si el paquete no tiene una dirección en la red local, lo reenviará a su **puerta de enlace predeterminada** y, probablemente, desde allí vaya a Internet.

Una vez a través de Internet, el paquete llegará a la dirección IP pública de la red donde reside el servidor VAX. Un administrador de TI habría configurado una **regla de reenvío de puertos** para reenviar cualquier tráfico con un puerto **TCP/UDP de destino de 9876** a la dirección interna del servidor VAX. Una vez que se establece la comunicación y se agrega el Panel en el software VAX, el Panel y el servidor se comunicarán en ambos sentidos entre sí y ocasionalmente verificarán si el otro extremo aún está activo..

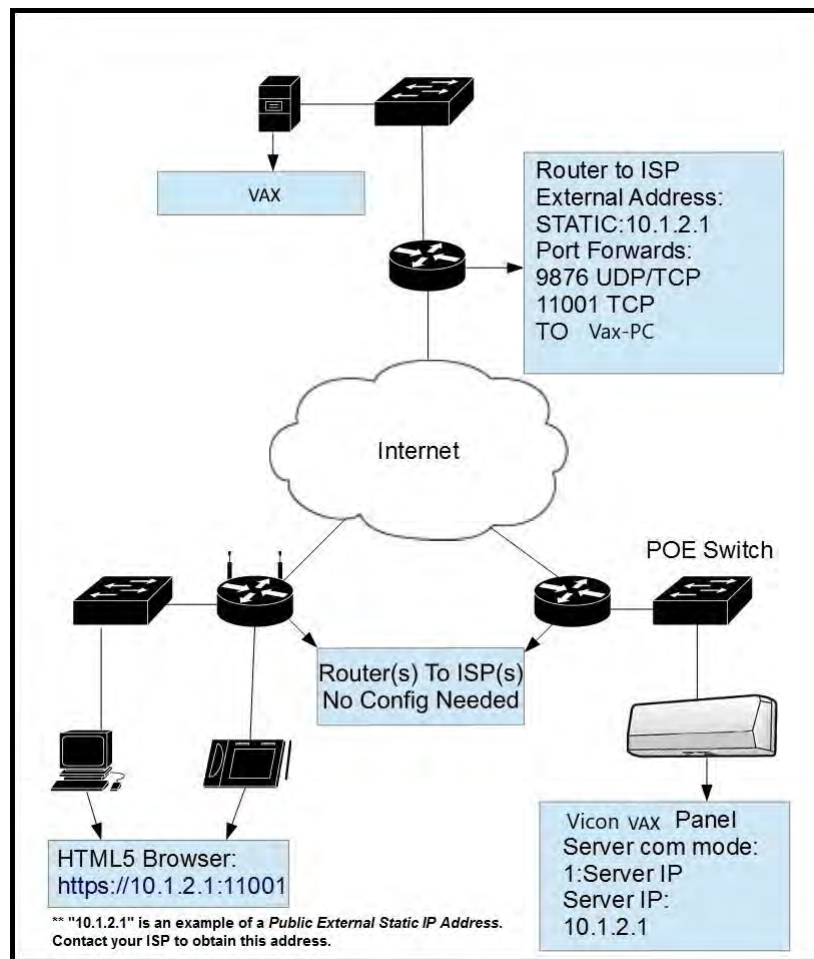
Cómo se comunican los clientes web con VAX

El servicio web VAX escucha en el puerto **TCP 11001** las conexiones entrantes del cliente web. Los clientes en la misma red pueden usar un navegador web dirigido a la dirección IP del servidor o el nombre. Los clientes a través de Internet que deseen comunicarse con el servidor VAX deberán **navegar utilizando la dirección IP estática** pública del enrutador conectado a la red privada en la que reside el servidor VAX. El puerto TCP de destino 11001 deberá reenviarse a la dirección interna del servidor VAX a través de una configuración de regla de reenvío de puerto en el enrutador. Si el cliente requiere acceso a la interfaz de usuario de System Manager, el puerto TCP de destino 11002 también necesitará una regla de reenvío de puerto.

Acceso remoto: requisitos de red

Esta sección cubre los requisitos de red para que un servidor reciba conexiones de clientes web o Paneles a través de Internet. Esta sección incluye diagramas visuales para ayudarlo a comprender el flujo de datos.

Figura 36.1. Topología de Red: Paneles y Clientes Remotos



Requisitos de red

- El sitio con el servidor VAX debe tener una dirección IP estática pública que les haya proporcionado su ISP. Llame a su ISP para obtener detalles y costos asociados con el arrendamiento de una IP pública.
- La PC VAX debe tener una dirección interna estática.
- El enrutador principal en el sitio con el servidor VAX debe ser capaz de reenviar puertos. Consulte el manual de su enrutador para obtener más detalles.
- Los puertos de destino TCP/UDP 9876 deben tener una regla de reenvío de puerto a la dirección interna del servidor para que los paneles se comuniquen a través de Internet. Los puertos de destino TCP 11001 y 11002 (si es necesario) deben tener reglas de reenvío de puertos a la dirección interna del servidor para que los clientes accedan a la interfaz web a través de Internet.

DNS Dinámica

Cuando obtener una dirección IP estática de un ISP es demasiado costoso o no es factible, la alternativa es utilizar un servicio de DNS dinámico. Varios proveedores de servicios de Internet ofrecen este servicio (a veces es gratuito, pero puede ser de pago). Estos servicios crean un nombre de dominio que está asociado con su dirección IP pública dinámica; la dirección IP con la que está asociado el dominio se actualiza automáticamente mediante algún software de cliente o alguna configuración especial del enrutador. Industrias Vicon no proporciona este tipo de servicio; para obtener más información sobre el DNS dinámico, hable con el personal de TI local o consulte los recursos disponibles en Internet.

 **Nota**

El sitio en el que residen el cliente y los paneles no necesita reenvíos de puertos ni direcciones estáticas (en la mayoría de los casos) porque están llamando al servidor mediante puertos de origen dinámicos. Solo el sitio con el servidor VAX requiere configuración adicional.

 **Advertencia**

Una vez que haya obtenido la IP pública estática de su ISP, debe ingresar esta dirección en el campo Dirección del servidor en el software VAX en Inicio>Configuración del sistema>Configuración general: Dirección del servidor. Una vez que realice una actualización del Panel, esta será la dirección que usarán sus Paneles para encontrar el servidor, anulando cualquier valor configurado manualmente.

Tabla 36.1. Referencia de terminología

Término	Descripción
Servidor VAX	La computadora (también puede ser una máquina virtual) en la que se ejecuta el servicio web VAX. Se puede buscar en esta computadora a través de la red o Internet/WAN para configurar y ver su sistema de control de acceso.
Dirección IP estática pública	Esta es la dirección que representa su red doméstica en Internet. Normalmente, su ISP le proporciona dinámicamente una dirección externa pública, lo que significa que cambiará cada pocos días más o menos. Se requiere una IP pública estática para una conexión estable y consistente a nuestro software.
Reenvío de puertos	El reenvío de puertos se utiliza para permitir que hosts externos (clientes y paneles) se conecten a servicios alojados en una red interna. Esto nos permite mapear los puertos de destino 9876, 11001 y 11002 a la dirección interna del servidor.

Ejemplos de acceso remoto

Esta sección incluirá escenarios de ejemplo de acceso remoto, incluidos escenarios en los que los distribuidores/instaladores alojarán el servidor VAX..

Ejemplo 1: expansión a la segunda oficina.

Una empresa se ha expandido a una segunda oficina e instala paneles de puertos de Vicon Industries en su segunda ubicación. En lugar de comprar un segundo servidor y una licencia para el segundo sitio, pueden configurar los Paneles en el nuevo sitio para conectarse al servidor de la oficina principal. El personal de TI obtiene de su ISP una dirección pública estática para la oficina principal. También configuraron reglas de reenvío de puertos para el puerto TCP/UDP 9876, el puerto TCP 11001 y el puerto TCP 11002 a la dirección interna del servidor VAX. También se aseguran de que el software VAX haya sido configurado para enviar la nueva dirección en 'Inicio>Configuración del sistema>Dirección del servidor'. El personal de TI configurará cualquier regla de firewall adicional si es necesario. Los paneles y clientes ahora pueden comunicarse libremente con el servidor VAX.

Ejemplo 2: servidor VAX alojado por el distribuidor.

A un distribuidor/instalador le gustaría alojar los servidores VAX de sus clientes en su oficina para brindar mantenimiento y garantizar copias de seguridad y actualizaciones de software adecuadas. La empresa distribuidora obtiene una IP estática para su oficina y crea las reglas de reenvío de puertos adecuadas para dirigir el tráfico del panel y del cliente al servidor internamente en su red. Cuando el distribuidor implementa nuevos clientes, puede preconfigurar los paneles y probarlos en su oficina. Es probable que el distribuidor utilice particiones y tenga una partición separada para cada cliente junto con una cuenta de administrador que solo puede administrar la partición de ese cliente. De esta manera, el distribuidor puede alojar información de varios clientes en una instalación de software.

Realización de una copia de seguridad y restauración manual con la línea de comandos de MSSQL

Esta sección cubre los procedimientos avanzados de respaldo y restauración en VAX. Esto cubre la realización de copias de seguridad de bases de datos y la restauración de bases de datos con SQL Command-Line.

⚠ Advertencia

Estas instrucciones solo deben ser realizadas por profesionales de TI e instaladores calificados de Vicon Industries. Si tiene problemas para realizar copias de seguridad y restauraciones con la interfaz de usuario del administrador del sistema, entregue este documento a su personal interno de TI o comuníquese con Vicon Industries. *Consulte el Capítulo 37, Soporte.*

Copia de seguridad de la base de datos SQL

Esta sección cubre cómo realizar una copia de seguridad de la base de datos a través de la línea de comandos SQL.

1. En la computadora con VAX instalado, abra un símbolo del sistema (search cmd.exe o ubicado en C:\Windows\system32) con privilegios de administrador. (Para hacerlo, haga clic derecho en cmd.exe y seleccione "Run as Administrator".)
2. En el símbolo del sistema, escriba **'SQLCMD -S .\VAX'** y presione **Enter**. (VAX es el nombre predeterminado para la instancia de la base de datos, el nombre de su instancia puede variar. Para encontrar el nombre de su instancia, consulte la sección llamada "Copia de seguridad/restauración de la base de datos: Preguntas frecuentes".)
3. Escriba **'use [master]'** y presione **Enter**. Escriba **'Go'** y presione **Enter**.
4. Recomendamos crear una carpeta de respaldo ubicada en la raíz de **"C:/"** drive. En el siguiente ejemplo usamos **"C:\backup"** como la carpeta en la que se realiza la copia de seguridad de la base de datos.
5. Escriba **'BACKUP DATABASE [VAX] TO DISK = N'C:\backup\VAXbackup' WITH NOFORMAT, NOINIT, NAME = N'VAX-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10'** y presione **Enter**.
6. Escriba **'Go'** y presione **Enter**. La copia de seguridad ahora se realizará si el nombre de la base de datos y la ubicación de la copia de seguridad son correctos.

Figura 36.2. Command Prompt: Copia de seguridad

```

C:\Users\davevm>SQLCMD -S .\VAX
1> use master
2> go
Changed database context to 'master'.
1> BACKUP DATABASE [VAX] TO DISK = N'C:\backup\ViconBackup' WITH NOFORMAT, NOI
T, NAME = N'VAX-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10
2> go
10 percent processed.
20 percent processed.
30 percent processed.
40 percent processed.
51 percent processed.
60 percent processed.
70 percent processed.
80 percent processed.
90 percent processed.
Processed 688 pages for database 'VAX', file 'VAX' on file 2.
100 percent processed.
Processed 2 pages for database 'VAX', file 'VAX_log' on file 2.
BACKUP DATABASE successfully processed 690 pages in 0.313 seconds <17.199 MB/s
>
1>
    
```

Restauración de base de datos SQL

Esta sección cubre cómo realizar una restauración de base de datos a través de la línea de comandos SQL.

1. Instale VAX en la computadora en la que se restaurará la base de datos. Asegúrese de que la versión de VAX instalada sea la misma versión o más reciente que la versión de la que se realizó la copia de seguridad de la base de datos.
2. Si la copia de seguridad se realizó por línea de comando, mueva el archivo de copia de seguridad a la computadora (a través de una unidad USB o correo electrónico) a una carpeta en "C:/" nombrar "**backup**".
3. Si la copia de seguridad fue realizada por la interfaz de usuario del administrador del sistema:

"VAX_<dateofbackup>.prbak" tendrá que ser renombrado a: "VAX_<dateofbackup>.zip".

Extraiga el archivo y copie el archivo "VAXFullBackup.bak" al "C:\backup".
4. Detenga el servicio web VAX a través del Monitor del sistema (consulte la sección correspondiente dentro de la guía técnica principal) o a través de la IU de administración del sistema (consulte el *Capítulo 5, IU del administrador del sistema*)
5. En la computadora con VAX instalado, abra una Command Prompt (búsque cmd.exe o located in C:\Windows\system32) con privilegios de administrador. (Para hacerlo, haga clic con el botón derecho en cmd.exe y seleccione "Run as Administrator".)
6. En el Command Prompt, escriba **'SQLCMD -S .\VAX'** y presione **Enter**. (VAX es el nombre predeterminado para la instancia de la base de datos, el nombre de su instancia puede variar. Para encontrar el nombre de su instancia, consulte la sección llamada "Copia de seguridad/restauración de la base de datos: Preguntas frecuentes".)
7. Escriba **'use [master]'** y presione **Enter**. Escriba **'Go'** y presione **Enter**.
8. Escriba:

'RESTORE DATABASE [VAX] FROM DISK = N'C:\backup\VAXbackup' WITH FILE = 1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'VAX' TO 'C:\Program Files\Microsoft SQL Server\MSSQL11.VAX\MSSQL\DATA\VAX.mdf', MOVE 'VAX_log' TO 'C:\Program Files\Microsoft SQL Server\MSSQL11.VAX\MSSQL\DATA\VAX_log.LDF' y presione **Enter**.
9. Escriba **'Go'** y presione **Enter**. La restauración ahora se realizará si el nombre de la base de datos y la ruta de la base de datos son correctos.
10. Inicie el servicio web VAX e inicie sesión para confirmar que la copia de seguridad se realizó correctamente.

Figura 36.3. Command Prompt: Restaurar

```

C:\Users\davevm>SQLCMD -S .\UAX
1> USE MASTER
2> GO
Changed database context to 'master'.
1> RESTORE DATABASE [UAX] FROM DISK = N'C:\backup\UAXFullBackup.bak' WITH FILE
1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'UAX' TO 'C:\Program Files\Microsoft SQ
Server\MSSQL11.UAX\MSSQL\DATA\UAX.mdf', MOVE 'UAX_log' TO 'C:\Program Files\Mi
rosoft SQL Server\MSSQL11.UAX\MSSQL\DATA\UAX_log.LDF'
2> GO
5 percent processed.
10 percent processed.
15 percent processed.
20 percent processed.
25 percent processed.
30 percent processed.
35 percent processed.
40 percent processed.
45 percent processed.
51 percent processed.
55 percent processed.
60 percent processed.
65 percent processed.
70 percent processed.
75 percent processed.
80 percent processed.
85 percent processed.
90 percent processed.
95 percent processed.
100 percent processed.
Processed 688 pages for database 'UAX', file 'UAX' on file 1.
Processed 2 pages for database 'UAX', file 'UAX_log' on file 1.
RESTORE DATABASE successfully processed 690 pages in 0.131 seconds (41.093 MB/s)
c>.
1>
    
```

Copia de seguridad/restauración de la base de datos: Preguntas frecuentes

P: ¿Por qué no funcionó la utilidad de restauración integrada?

R: Microsoft SQL Server es una pieza de software bastante sofisticada, sin embargo, las ubicaciones y el comportamiento de sus bases de datos asociadas cambian según el sistema operativo de la computadora, la versión del servidor SQL instalada y la arquitectura del sistema (32 o 64 bits). Al restaurar una base de datos VAX en una computadora diferente, si alguno de estos factores cambia, el archivo de la base de datos no puede encontrar la ruta de la base de datos y requiere ayuda adicional..

P: ¿Dónde puedo encontrar el nombre de mi instancia de base de datos?

R: Puede encontrar el nombre de su instancia de base de datos en una instalación VAX existente siguiendo los siguientes pasos:

1. Vaya a la carpeta WebServer de su directorio de instalación de VAX (generalmente ubicado en "C:\Program Files (x86)\Vicon Industries\VAX\WebServer").
2. Abra el archivo llamado "VAX.exe.config" en un editor de texto como el bloc de notas.
3. Busca la línea: 'connectionString="Data Source=pcname\VAX;' donde 'pcname' es el nombre de su computadora/servidor. El nombre después de la PC es el nombre de la instancia de base de datos que VAX está usando actualmente.

Migración de datos

Esta sección cubre la importación y exportación de datos en VAX entre particiones.

Exportación de datos de partición

Esta sección cubre cómo realizar una exportación de datos de partición a través del migrador de datos.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el **Migrador de datos** icono (en la foto de abajo)

Figura 36.4. Icono de Migrador de datos



4. Asegúrese de que la pestaña **Exportar** esté seleccionada.
5. Seleccione la(s) partición(es) que desea exportar.
6. Seleccione las Opciones para exportar.
7. Seleccione Exportar y seleccione una ubicación para guardar su archivo de datos.

Figura 36.5. Migrador de datos: opciones para exportar



Importing Partition Data

This section covers how to perform an *import* of partition data via data migrator.

1. Acceda a su sistema VAX a través del navegador HTML5 de su elección.
2. Inicie sesión con la cuenta de administrador que creó durante la configuración inicial o que le proporcionó su distribuidor/instalador.
3. En la **barra lateral**, desplácese hacia abajo hasta la sección titulada **Administración**; haga clic en el **Migrador de datos** icono (en la foto de abajo)

Figure 36.6. Icono de Migrador de datos



4. Asegúrese de que la pestaña **Importar** esté seleccionada.



5. Haga clic en Elegir archivo. Busque la ubicación del archivo de datos, seleccione el archivo y haga clic en abrir.
6. Seleccione **Analizar (Parse)**.
7. Verifique el contenido de la importación y seleccione la partición que desea importar. Cree y asigne un nombre a una nueva partición o use los menús desplegables para seleccionar una partición existente.
8. Utilice las casillas de verificación para seleccionar los datos que desea importar a la partición.
9. Seleccione **Importar**

Figure 36.7. Data Migrator: Import



Tabla 36.2. Estrategia de conflicto

Estrategia	Breve explicacion
Duplicar	No haga coincidir con los usuarios existentes, duplique cada usuario en la partición asignada.
Tarjetas credenciales	Use el usuario existente si todas las credenciales coinciden con el usuario importado.
Nombre	Utilice el usuario existente si el nombre y el apellido coinciden exactamente
Ambos	Utilice el usuario existente si todas las credenciales y el nombre coinciden con el usuario importado.

Integración API

Este capítulo revisará los recursos disponibles para acceder a la API Restful y Real-time en VAX VAX cuenta con una API REST HTTP que permite una integración simplificada con sistemas de terceros.

Advertencia

Todas las API se proporcionan tal cual sin garantía expresa o implícita de Vicon Industries. Vicon Industries no brinda soporte para ninguna aplicación o proyecto desarrollado utilizando estas API..

REST API

La API REST proporciona una plataforma de integración web REST-FUL. Este servicio brinda acceso a la mayoría de las funciones de administración de datos dentro de VAX, incluidas las consultas y la adición de registros a la base de datos. Las solicitudes se envían al servidor VAX utilizando HTTP y el formato de datos JSON. La API REST se usa ampliamente dentro de la aplicación VAX.

Tiempo real API

La API en tiempo real proporciona un subconjunto de operaciones más pequeño que la API REST y sus operaciones están orientadas principalmente a obtener información de estado en vivo de su sistema. Esto incluye cosas como el estado actual de un dispositivo o la obtención de eventos en tiempo real de su sistema. La API en tiempo real utiliza

SignalR [<http://signalr.net/>] y requiere la disponibilidad de una biblioteca de cliente en el lenguaje de desarrollo de su elección.

Acceso a la documentación de la API

La documentación de la API REST y en tiempo real está disponible en cualquier versión de VAX 2.7 o posterior. Si tiene un sistema existente, puede acceder a él con lo siguiente:

<https://NameOrIPoFServer:11001/apidocs>

Si no tiene un sistema en vivo para ver la documentación, puede verlo en línea en nuestro sistema de demostración. <https://VAXdemo.com:11001/apidocs>

Configuración del modo multiusuario

Multi-inquilino es una función disponible en VAX que permite a las empresas de TI o distribuidores/instaladores almacenar múltiples bases de datos VAX en un solo sistema.

El modo multi-inquilino permite que cada inquilino tenga una base de datos separada y un punto de entrada a VAX. El servidor reforzará un nombre de dominio adecuado, ya que a cada inquilino se le aumentarán uno o más subdominios, es decir, <https://client1.dealname.com:11001>

Cuando el modo multi-inquilino está habilitado, hay algunos aspectos que deben tenerse en cuenta:

- Se requiere un nombre de dominio completo con un 'Registro A de DNS' para cada arrendatario.
- Se creará una base de datos separada para cada arrendatario. Pueden estar en la misma instancia o separados.
- Cada inquilino requerirá su propia licencia VAX.
- Los paneles desconocidos no generarán una notificación de panel desconocido hasta que se cree una asociación desde la interfaz de usuario de System Manager.
- La interfaz de usuario del administrador del sistema permitirá que se configuren varios administradores.
- Las copias de seguridad de la base de datos ahora se configurarán y programarán por base de datos.

Advertencia

La habilitación de múltiples inquilinos no se puede revertir. Considere esto cuidadosamente antes de habilitar esta característica.

Habilitación del modo multiusuario

El modo multiusuario está habilitado desde la interfaz de usuario del administrador del sistema. Los registros DNS A y los punteros deben configurarse antes de habilitar el multiinquilino. Use los siguientes pasos para habilitar multiusuario:

1. Acceda a la interfaz de usuario del administrador del sistema VAX como se describe en la sección llamada "Acceder a la interfaz de usuario del administrador del sistema".
2. En la página Sistema de la interfaz de usuario del administrador del sistema, marque la casilla de verificación Multiusuario en la parte inferior de la pantalla.

Multi-Tenant

Enable Multi-Tenant

3. Aparecerá un mensaje informativo. Léalo y haga clic en Aceptar. Multi-inquilino ahora estará habilitado. Los servicios web de VAX se reiniciarán durante este proceso.
4. Vuelva a iniciar sesión en la interfaz de usuario de System Manager o actualice la página.
5. La base de datos VAX existente se cambiará a su primer inquilino. Todos los inquilinos se mostrarán en la parte inferior de la interfaz de usuario de System Manager. Se pueden editar con el botón de edición azul a la izquierda del nombre del inquilino.

Figura 36.8. Lista de inquilinos

Tenant	Status	Database	Backup Schedule	Account #	License	License Expiry	Actions
Test Customer	Enabled	Odyssey	Not Scheduled	7945	Enterprise	November 1, 2027	License Backup Restore Delete
Test Customer	Enabled	Odyssey	Not Scheduled	7945	Enterprise	November 1, 2027	License Backup Restore Delete

Agregar inquilinos

Esta sección describe la adición de inquilinos adicionales una vez que se haya habilitado el modo de múltiples inquilinos.

1. En la interfaz de usuario del administrador del sistema, haga clic en el botón Agregar inquilino.
2. En la pantalla Crear inquilino, complete el nombre de su inquilino. Por lo general, será el nombre de la empresa o el nombre del cliente.
3. Introduzca una cadena de conexión de base de datos válida. Esto se usará para crear la base de datos para este arrendatario.

Ejemplo 36.1. Cadena de conexión de la base de datos:

Data Source=VAXSERVER\VAX; Initial Catalog=Client1;Integrated Security=true

En el ejemplo anterior, VAXServer es el nombre de la computadora en la que residirá la base de datos. VAX es el nombre de la instancia de la base de datos en la que residirá la base de datos. Esto puede ser el mismo para todos los inquilinos. Client1 es el nombre de la base de datos que se creará para el arrendatario. esto debe ser unico.

Nota

El servicio web VAX debe ejecutarse como una cuenta de servicio que tenga permiso para crear bases de datos en las instancias de bases de datos especificadas.

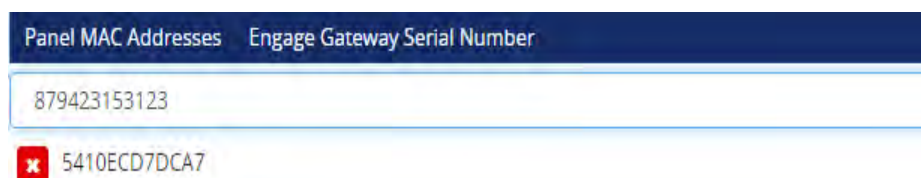
Tenant Information

Enabled

Name

Connection String

4. Opcionalmente, puede configurar qué paneles se asociarán a este arrendatario. Puede ingresar la dirección MAC del panel y hacer clic en el botón Agregar para cada panel. También se mostrará una lista de paneles no asociados en la parte inferior de la página. Si ve que se agrega un panel que debería pertenecer al arrendatario, haga clic en el signo "+" junto al nombre del panel. Puede agregar más paneles después de crear el arrendatario.



5. Ingrese cualquier punto final. Un punto final es el subdominio que usará un arrendatario para acceder a su instancia VAX. Solo necesita proporcionar la parte del subdominio. Haga clic en el botón Agregar junto al nombre del punto final.



6. Haga clic en Guardar una vez que haya completado la información del arrendatario. Ahora puede acceder al inquilino a través del punto final configurado.

Gestión de inquilinos

Mientras edita un arrendatario, puede editar todas las configuraciones disponibles al agregar un arrendatario. Esto incluye asociar paneles adicionales y agregar puntos finales.

Copia de seguridad de bases de datos de inquilinos

Cada arrendatario tendrá su propia copia de seguridad de base de datos y programa de copia de seguridad. Utilice los siguientes pasos para hacer una copia de seguridad de una base de datos de inquilinos:

1. En la página de inicio de la interfaz de usuario de System Manager, haga clic en el botón Copia de seguridad a la izquierda de un arrendatario existente.

O bien, al editar un arrendatario, haga clic en el botón Copia de seguridad en la parte superior derecha de la pantalla.



2. Ahora estará en las Opciones de respaldo para esa base de datos específica. Estas opciones están completamente cubiertas en la sección llamada "Copia de seguridad de su base de datos VAX".
3. Le recomendamos que establezca una programación automática para sus copias de seguridad. Las copias de seguridad de un arrendatario individual incluirán el nombre del arrendatario en el archivo de copia de seguridad.

Restauración de bases de datos de inquilinos

Each tenant database can be restored individually from a previous backup.

Advertencia

La restauración de cualquier base de datos de inquilinos reiniciará temporalmente el servicio web VAX.

Utilice los siguientes pasos para hacer una copia de seguridad de una base de datos de inquilinos:

1. En la página de inicio de la interfaz de usuario de System Manager, haga clic en el botón Restaurar a la izquierda de un arrendatario existente.

O cuando edite un arrendatario, haga clic en el botón Restaurar en la parte superior derecha de la pantalla.



2. Ahora estará en la pantalla Restaurar base de datos para ese arrendatario específico. Estas opciones están completamente cubiertas en la sección correspondiente dentro de la guía técnica maestra.

Acceso a la interfaz web de inquilino con un subdominio

Después de que se crea el arrendatario y se le asigna un Endpoint; debe acceder a la interfaz web del arrendatario para crear un inicio de sesión e ingresar la información inicial.

Se accede a cada inquilino a través de un subdominio DNS único. No olvide incluir el encabezado HTTPS y el puerto (el valor predeterminado es 11001).

`https://client1.dealname.com:11001`

Consejo

Después de agregar un subdominio al registro DNS, pueden pasar hasta 24 horas antes de que todos los servidores DNS reconozcan y puedan resolver el nuevo subdominio.

Una vez que acceda a la interfaz web, configurará el sistema como lo haría normalmente. Consulte el Capítulo 3, Configuración inicial para obtener detalles sobre la pantalla de configuración inicial.

Acceder a la interfaz web del arrendatario sin un subdominio

En el caso de que su sistema multiinquilino no sea público o desee probar multiinquilino sin obtener un subdominio oficial; use las siguientes instrucciones para permitir que el servidor acceda localmente a inquilinos individuales.

1. Abra el Bloc de notas como administrador.
2. Abra el archivo titulado hosts en "C:\Windows\System32\drivers\etc". Es posible que deba ajustar el menú desplegable de tipo de archivo a "Todos los archivos" para ver el archivo de hosts.
3. Para cada inquilino que haya agregado, deberá agregar una nueva entrada (1 por línea) al archivo. debería verse como:

```
127.0.0.1 client1.computername
```

127.0.0.1 se puede reemplazar con la IP del VAX en computadoras remotas. Agregue entradas según sea necesario.

4. Guarde el archivo y ahora puede acceder a la interfaz web de un arrendatario. No olvide incluir el encabezado HTTPS y el puerto (el valor predeterminado es 11001).

`https://client1.computername:11001`

5. Una vez que acceda a la interfaz web, configurará el sistema como lo haría normalmente. Consulte el Capítulo 3, Configuración inicial para obtener detalles sobre la pantalla de configuración inicial.

Capítulo 37. Soporte

Usuarios finales:

Por lo general, Vicon Industries no brinda asistencia directa a los usuarios finales, ya que dependemos de nuestra amplia red de distribuidores e instaladores capacitados para brindar servicio a nuestros productos en el campo. Si su sistema requiere servicio, le recomendamos que se comunique con su distribuidor / instalador. Si no sabe quién es su distribuidor, puede comunicarse con Vicon Industries y lo ayudaremos a encontrar un distribuidor/instalador local.

Distribuidor / Instalador:

El soporte de Vicon Industries está disponible para los distribuidores de lunes a viernes entre las 9 a. m. y las 5 p. m. EST para ayudarlo con cualquier problema relacionado con la instalación que pueda tener.

Website

Vicon Industries ofrece una serie de guías técnicas y recursos a través de nuestro sitio web: <https://www.vi-con-security.com>

Email

El soporte por correo electrónico está disponible a través de nuestro sitio web en <https://www.vicon-security.com/learn-and-sup-port/support-and-sales-contacts/>. Espere de 24 a 48 horas hábiles para obtener una respuesta..

Teléfono

Si se requiere soporte urgente, ofrecemos números de soporte locales y gratuitos durante el horario comercial normal. Fuera de nuestro horario laboral habitual, espere de 24 a 48 horas laborales para recibir una respuesta. Puede comunicarse con nosotros en:

Llamada gratuita (solo en América del Norte): 800-348-4266
Int: +1 631 952-2288

Capítulo 38. Integración de alarma IP DSC

Los paneles de alarma/intrusión DSC Power Series están integrados en VAX a través de una comunicación basada en red basada en el protocolo UDP. Este capítulo cubrirá las características generales de la integración, cómo configurar la comunicación, cómo usar funcionalmente la integración y casos de uso.

⚠ Precaución

Este capítulo asume que el lector está familiarizado con los paneles de intrusión DSC. Consulte su documentación para obtener más detalles.

Funciones de integración de DSC

La integración permite las siguientes opciones:

- Ver el estado de las particiones de alarma y las zonas de alarma a través de la interfaz web de VAX mediante notificaciones o descripción general del sistema
- Armar (Armar En Casa, Armar Ausente, Armar Noche) y desarmar a través de la interfaz web de VAX, la aplicación móvil, los planes de acción o a través de la API de VAX
- Omitir zonas, ponerse en contacto con los servicios de emergencia, silenciar pitidos de problemas
- Configurar notificaciones relacionadas con alarmas como disparadores dentro de disparadores de acción
- Ejecutar informes contra particiones de alarma, zonas y notificaciones específicas de intrusión

Descripción general de alto nivel de los pasos de integración

La integración exitosa implica la configuración dentro del teclado del panel de intrusión y la interfaz web del VAX. Esta sección resumirá esos pasos. Más detalles sobre los pasos individuales están cubiertos en las secciones de procedimiento.

1. Instale y realice la configuración inicial del software VAX.
2. Asegúrese de que el servidor tenga una IP estática o un nombre DNS confiable y que el puerto UDP 3073 esté permitido en cualquier firewall relevante o reglas de reenvío de puertos (si el servidor VAX es remoto desde el panel de intrusión).
3. Las definiciones de particiones y zonas se configuran dentro del panel de intrusión, como los nombres de las zonas y particiones, y se conecta a la red.
4. Establezca la IP estática del servidor VAX en el menú IP del servidor de integración de la sesión 1 dentro del panel de intrusión ([*][8][código del instalador][851][428]) o establezca el nombre DNS del servidor VAX en el menú DNS del servidor de integración de sesión 1 dentro del panel de intrusión ([*][8][código del instalador][851][431]).
5. Si el puerto predeterminado (UDP 3073) no es factible, puede cambiar el puerto a través del menú Puerto saliente de integración de la Sesión 1 dentro del Panel de intrusión ([*][8][código del instalador][851][432]).
6. Si se requiere una IP estática para el panel de intrusión (DHCP por defecto); estas opciones se pueden configurar dentro de [*][8][código de instalador][851][001], [*][8][código de instalador][851][002], [*][8][código de instalador] [851][003] y [*][8][código de instalador][851][007].
7. Establezca el Retardo de comunicación dentro del panel de intrusión en 60 segundos ([*][8][código de instalador][377] [002]).

8. Establezca el Comunicador alternativo dentro del panel de intrusión en Sí ([*][8][código del instalador][382][5]).
9. Establezca las opciones de alternancia de integración de la sesión 1 2 para que se configuren 3 y 5 (03: integración a través de Ethernet, 05: protocolo de integración) dentro del panel de intrusión ([*][8][código del instalador][851][425]) . La pantalla LCD debe mostrar "--3-5--".
10. Establezca las opciones de alternancia de integración de la sesión 1 3 para que se establezcan 1, 3 y 4 (01: sondeo UDP, 03: notificación en tiempo real, 04: la notificación sigue al grupo) dentro del panel de intrusión ([*][8][instalador código][851][426]). La pantalla LCD debe mostrar "1-34".
11. El ID de integración se configura/obtiene del panel de intrusión ([*][8][código del instalador][851][422]).
El número tendrá 12 dígitos.
12. El código de acceso de integración se configura/obtiene del panel de intrusión ([*][8][código de instalador] [851][423]). El código predeterminado es 12345678.
13. El código de instalador se configura/obtiene del panel de intrusión ([*][8][código de instalador][006][001]). El código predeterminado es 5555.
14. El código maestro se configura/obtiene del panel de intrusión ([*][8][código del instalador][006][002]). El código predeterminado es 1234.
15. Dentro de la interfaz web de VAX, agregue el Panel de intrusión a través de la sección Paneles de alarma con Nombre, Tipo, Sitio, ID de integración, Código de acceso de integración, Código de instalador y Código maestro.
16. Espere hasta que reciba una notificación con el texto "El panel de alarma ahora está en línea".
17. Configure los ajustes de notificación, los activadores de acción y los planes de acción para cumplir con cualquier objetivo específico de integración.

Además de estos pasos, la integración cableada aún se puede usar a través de conexiones de entrada/relé de contacto seco.

Configuración de comunicación del panel DSC

Esta sección describe los pasos y la información requerida antes de agregar el panel DSC a VAX.

La arquitectura de comunicación entre el Panel de Intrusión y VAX es cliente-servidor. El panel de intrusión se comunica con una dirección IP específica mediante el puerto UDP 3073 de forma predeterminada.

Los paneles DSC pueden comunicarse con hasta 4 servicios de terceros. Los ajustes específicos de integración tienen una sesión asociada a ellos. Esta sección está escrita asumiendo que la Sesión 1 es la sesión disponible. Consulte la documentación de DSC para obtener aclaraciones sobre qué subsecciones se utilizan para las sesiones 2, 3 y 4.

Estos pasos deben realizarse después de que se haya instalado el software VAX, se haya completado la configuración inicial y se hayan configurado las particiones y zonas en el panel de intrusión a través del teclado LCD cableado. Para obtener ayuda con los pasos específicos del panel de intrusión, comuníquese con el soporte de DSC.

Las instrucciones para navegar a menús específicos a través del teclado LCD se mostrarán de la misma manera que se muestran en la documentación de DSC.

1. Anote la dirección IP estática o el nombre DNS asignado al servidor VAX. Si el servidor VAX está en una red diferente a la del panel de intrusión, es posible que se requieran reglas de reenvío de puertos, enrutamiento y firewall.
2. Si se eligió una dirección IP estática como método de comunicación: a través de la interfaz del teclado LCD DSC, navegue hasta el menú IP del servidor de integración usando [*][8][código de instalador][851][428]. Use las teclas para ingresar la dirección IP local del servidor VAX o la dirección IP pública del enrutador al que está conectado el servidor VAX.
3. Si se eligió un nombre DNS como método de comunicación: a través de la interfaz del teclado LCD DSC, navegue hasta el menú DNS del servidor de integración usando [*][8][código del instalador][851][431]. Use las teclas para ingresar el nombre DNS del servidor VAX o la dirección de dominio resoluble.
4. El puerto predeterminado utilizado para la integración es UDP 3073. Puede cambiar este puerto si es necesario a través del menú Puerto saliente de integración a través de la interfaz del teclado LCD DSC navegando a [*][8] [código de instalador][851][428] y utilizando las teclas numéricas para seleccionar el puerto.
5. Si se requiere una IP estática para el panel de intrusión (DHCP por defecto); estas opciones se pueden configurar a través de la interfaz del teclado LCD DSC dentro de:
 - Dirección IP Ethernet: [*][8][installer code][851][001]
 - Dirección IP Subnet Mask: [*][8][installer code][851][002]
 - Dirección IP Gateway : [*][8][installer code][851][003]
 - Ethernet principal DNS IP: [*][8][installer code][851][007]
6. Set Communication Delay to 60 seconds through DSC LCD Keypad interface using [*][8][installer code][377][002] and using the number keys to set the seconds to 60.
7. Establezca el comunicador alternativo dentro del panel de intrusión en Y (Sí) a través de la interfaz del teclado LCD DSC usando [*][8][código de instalador][382][5] y usando la tecla [*] para establecer el valor.
8. Será necesario configurar varias configuraciones de alternar específicas de integración en dos menús separados:
 - a. Navegue a la opción 2 de alternar la integración de la sesión 1 a través de la interfaz del teclado LCD DSC usando [*][8][código del instalador][851][425]. Será necesario configurar la opción 3 (03: integración a través de Ethernet) y la opción 5 (05: protocolo de integración). Para configurar estas opciones, utilice las teclas numéricas presionando 3 y 5; estas opciones deben estar activadas. Cuando se complete, la pantalla LCD debe mostrar la pantalla LCD debe mostrar "--3-5---".
 - b. Navegue a la opción 3 de alternar la integración de la sesión 1 a través de la interfaz del teclado LCD DSC usando [*][8][código del instalador][851][426]. Será necesario configurar la opción 1 (01: sondeo UDP), la opción 3 (03: notificación en tiempo real) y la opción 4 (04: la notificación sigue al grupo). Para configurar estas opciones, use las teclas numéricas presionando 1,3 y 4; estas opciones deben estar activadas. Cuando se complete, la pantalla LCD debe mostrar la pantalla LCD debe mostrar "1-34".
9. Establezca o anote el ID de integración a través de la interfaz del teclado LCD DSC usando [*][8][código de instalador][851][422]. Use las teclas numéricas para ajustar la ID de integración si es necesario. Deberá desplazarse con las teclas de flecha para ver el valor completo de 12 dígitos.

10. Establezca o anote el código de acceso de integración a través de la interfaz del teclado LCD DSC usando [*][8] [código de instalador][851][423]. Use las teclas numéricas para ajustar el código de acceso de integración si es necesario. Deberá desplazarse con las teclas de flecha para ver el valor completo de 8 dígitos. El valor predeterminado es 12345678.

11. Establezca o anote el código de instalador a través de la interfaz del teclado LCD DSC usando [*][8][código de instalador] [851][011]. El código de instalador predeterminado es 5555.

Capítulo 39. Tablero

VAX proporciona un panel extremadamente personalizable que permite al usuario tener la información más importante para sus operaciones diarias en la parte superior de la página de inicio. El contenido de los paneles también se escala y reajusta dinámicamente en función de la resolución de pantalla del dispositivo que lo visualiza. El usuario también puede **guardar Tableros** como perfiles que se pueden cambiar sobre la marcha, lo que permite un acceso rápido a cualquier información que necesite. Este capítulo cubrirá la creación y personalización de los Tableros en profundidad con toda la información relevante para las operaciones diarias.

Introducción a los tableros

De manera predeterminada, cuando se instala VAX por primera vez, el Tablero viene preconfigurado y se puede ver desde la página de inicio. Es probable que esta configuración predeterminada esté bien para la mayoría de los usuarios, ya que proporciona **estadísticas básicas, estado del sistema, alarmas recientes, actividad del usuario e historial de acceso diario**. Sin embargo, algunos usuarios pueden querer ajustar la ubicación de estos widgets, eliminar widgets o agregar más. Esto se puede lograr mediante una sencilla interfaz de **arrastrar y soltar** que permite al usuario adaptar el Tablero a sus necesidades y preferencias.

Figure 39.1. Tablero inicial



Crear Tableros

Para editar el panel, el usuario deberá hacer clic en el botón Editar en la parte superior de la pantalla junto al indicador de estado de los paneles. Esto se aplicará a cualquier Tablero que esté activo actualmente. Para crear un panel, seleccione la barra desplegable en la parte superior. Por defecto, estará marcado como "Inicio". Habrá una opción para Crear nuevo; haga clic aquí para ir a la página de creación.

Justo en la parte superior, puede darle un nombre al nuevo Tablero haciendo clic en el cuadro e ingresando un nombre. A partir de ahí, en el lado derecho de la página estará el menú Widget. Esta sección repasará qué opciones y cómo se pueden personalizar un poco más adelante. Para traer un widget a la pantalla, simplemente haga clic y arrástrelo a donde debe colocarse. Mientras lo arrastra, habrá una línea de puntos que indica dónde terminará el widget, que se puede ajustar después arrastrándolo a otro lugar o haciendo clic en la esquina y arrastrándolo para cambiar su tamaño. Para eliminar un widget, simplemente presione el botón de edición en el widget y elija la opción Eliminar, o arrástrelo a la papelera en la esquina inferior derecha.

Figura 39.2.

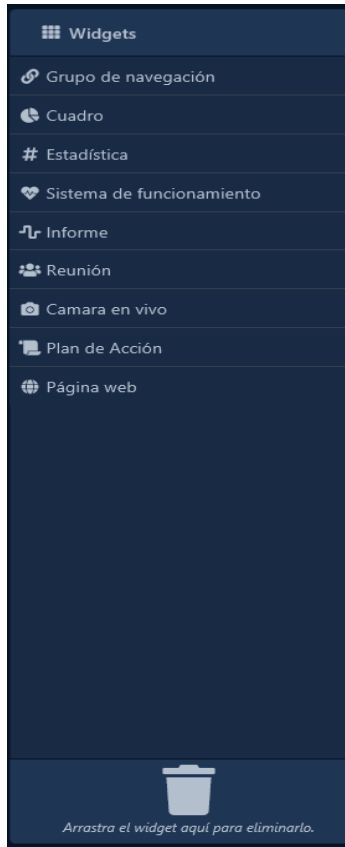


Figura 39.3.

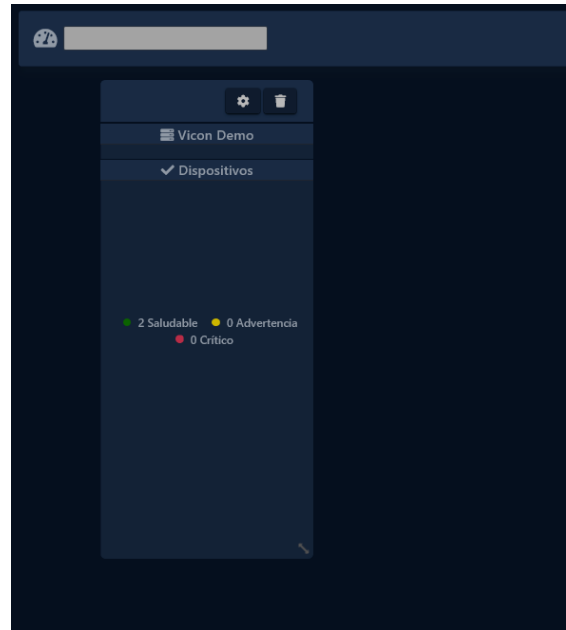


Table 39.1.

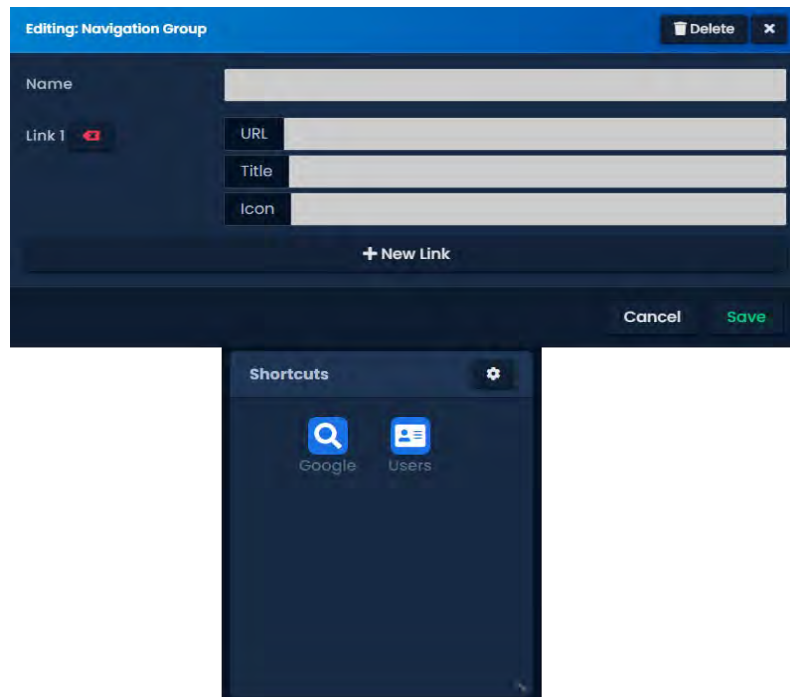
Widget	Descripción
Grupo de navegación	Un widget personalizable que le permite crear un botón de acceso directo que se vincula a otra página interna o externamente.
Cuadro	Un widget que permite al usuario elegir entre múltiples gráficos diferentes que pueden mostrar información de conjuntos de datos seleccionados por el usuario.
Estadística	Un widget que permite al usuario colocar una pequeña pantalla de ciertas estadísticas para una referencia rápida.
Funcionamiento del Sistema	Un widget personalizable que permite al usuario ver rápidamente cualquier problema de salud relacionado con el servidor o el panel.
Informe	Un widget que muestra un informe de la elección de los usuarios con intervalos de fechas preestablecidos y filtros específicos de tipo de notificación.
Reunión – Muster	Un widget que muestra un informe de las áreas en las que se encuentran los usuarios y cuándo ingresaron

Grupo de navegación

Tabla 39.2. Widget de estadísticas

Opción	Descripción
Nombre	Nombre del widget
URL	Dirección web del sitio/página que desea vincular al botón creado por el widget
Título	Título de la URL
Icono	Enlaces a un icono para usar desde la biblioteca FA. (Ejemplo fa-search.) Para encontrar la biblioteca completa de opciones, consulte la biblioteca Font-Awesome en línea.

Figura 39.4.



Gráfica

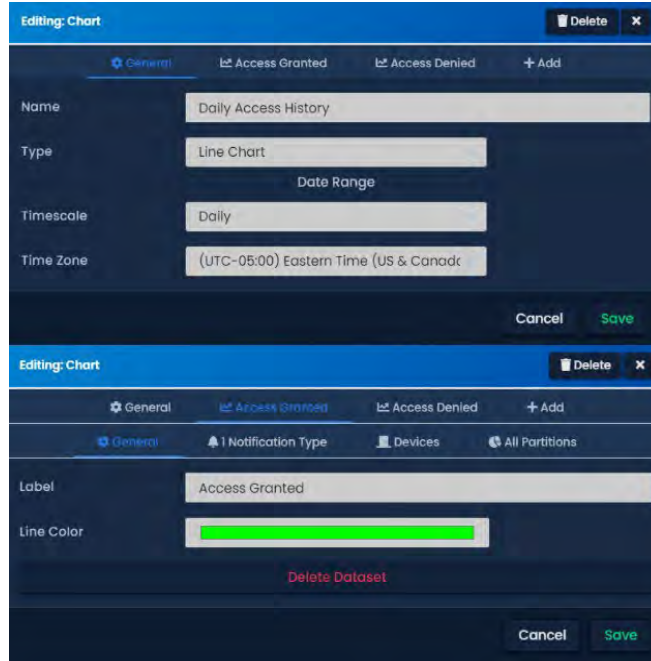
Tabla 39.3. Pestaña General del widget de gráfico

Opción	Descripción
Nombre	Nombre del widget.
Tipo	Un menú desplegable de tipos de gráficos. Esto incluye gráfico de barras vertical/horizontal, gráfico de líneas y gráfico de burbujas.
escala de tiempo	Un menú desplegable para ventanas de fecha predefinidas para extraer datos. Esto incluye por hora, por día, por semana, por mes y por año.
Zona horaria	Un menú desplegable que contiene diferentes zonas horarias para elegir.

Tabla 39.4. Ficha Conjuntos de datos del widget de gráfico

Opción	Descripción
General	Una sección que permite al usuario nombrar la etiqueta del gráfico y el color de la línea.
Tipo de notificación	Una lista de tipos de notificación para extraer. Solo puede seleccionar un tipo de notificación por conjunto de datos o, de lo contrario, no funcionará.
Dispositivos	Una lista de tipos de dispositivos para extraer datos y filtrar.
Particion	Una lista de particiones para extraer datos y filtrar

Figura 39.5.



Estadística

Tabla 39.5. Widget de estadísticas

Opción	Descripción
Usuarios	Presenta un valor numérico para el número de usuarios en el sistema.
Particiones	Presenta un valor numérico para el número de particiones en el sistema.
Paneles	Presenta un valor numérico para el número de paneles en el sistema.
puertas	Presenta un valor numérico para el número de puertas en el sistema.
Ascensores	Presenta un valor numérico para el número de ascensores en el sistema.
Plan de acción	Presenta un valor numérico para el número de planes de acción en el sistema.
Cámaras	Presenta un valor numérico para el número de cámaras en el sistema.
Paneles en línea	Presenta un valor numérico para el número de paneles en línea en el sistema

Funcionamiento del Sistema

Table 39.6.

Opción	Descripción
Nombre	Nombre del mosaico del widget que se coloca en la parte superior del widget.
Mostrar uso de memoria	Una estadística relacionada con el servidor para mostrar el uso actual de la memoria.
Mostrar uso de disco	Una estadística relacionada con el servidor para mostrar el uso actual del disco.
Mostrar dirección del servidor	Muestra la dirección IP actual del servidor VAX
Mostrar problemas	proporciona una lista con marcas de tiempo de cuándo se detectan problemas de estado del servidor en el servidor. Esto incluye el estado de la copia de seguridad, los dispositivos sin conexión, la caducidad de la licencia y cualquiera de las opciones antes mencionadas en este widget.
Mostrar gráfico de salud del dispositivo	Presenta un gráfico que muestra el porcentaje de estado de los dispositivos en función de los estados Correcto, Advertencia y Crítico.
Mostrar lista de salud del dispositivo	Presenta una lista de dispositivos y problemas de salud que tienen.
Mostrar paginación	Agrega un contador de páginas en la parte inferior del widget que permite al usuario ver un historial más antiguo de los problemas de salud del dispositivo

Figura 39.6.

Editing: System Health Delete X

Name

Server Issues

- Show Memory Usage
- Show Disk Usage
- Show Server Address
- Show Issues

Device Issues

- Show Device Health Chart
- Show Device Health List
- Show Pagination

Per Page

Cancel Save

Reportes

La generación de informes es una de las opciones más detalladas, por lo que junto con una tabla que presenta algunas opciones, esta sección analizará un poco más en detalle. Algunos de los menús serán sensibles al contexto del tipo de informe seleccionado en términos de qué notificaciones filtrar y qué conjuntos de datos se podrán seleccionar, como puertas, usuarios, etc.

Tabla 39.7.

Opción	Descripción
Informe de actividad de la puerta	Proporciona un informe de la actividad reciente de las puertas. Puede filtrar por tipo de notificación, puertas y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite clasificar por hora, nombre de la puerta o nombre del lector.
Informe de actividad del usuario	Proporciona un informe de actividad reciente para los usuarios. Puede filtrar por tipo de notificación, usuario y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por hora, nombre, código de sitio o número de tarjeta.
Option	Description
Informe de actividad de piso	Proporciona un informe de la actividad reciente de pisos y ascensores. Puede filtrar por tipo de notificación, piso y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por hora, nombre del piso, nombre del lector o nombre del ascensor.
Informe de actividad del ascensor	Proporciona un informe de la actividad reciente de pisos y ascensores. Puede filtrar por tipo de notificación, piso y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por hora, nombre del piso, nombre del lector o nombre del ascensor.
Informe de actividad de entrada	Proporciona un informe de la actividad reciente de las entradas. Puede filtrar por tipo de notificación, entrada (solo auxiliar) y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por hora y nombre de entrada.
Informe de actividad de salida	Proporciona un informe de actividad reciente para las salidas. Puede filtrar por tipo de notificación, salida (solo auxiliar) y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por hora y nombre de salida.
Informe de actividad del plan de acción	Proporciona un informe de la actividad reciente para los planes de acción. Puede filtrar por tipo de notificación, plan de acción y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar por tiempo y nombre del plan de acción.
Informe de actividad de alarma DSC	Proporciona un informe de actividad reciente con alarmas DSC integradas en VAX. Puede filtrar por tipo de notificación, partición y especificar un rango de fechas desde un menú desplegable con opciones preconfiguradas. También permite ordenar solo por tiempo

Figura 39.7.

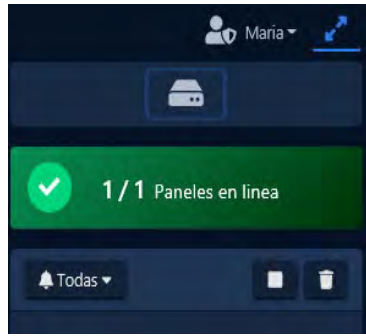
Reporte de Muster – Reunión

El informe Muster es similar al widget de actividad del usuario, pero en su lugar muestra solo el último lector que escaneó un usuario. El usuario también puede filtrar en función de un campo personalizado y se pueden especificar áreas específicas si lo desea. Al igual que con todos los demás widgets, hay opciones para la paginación y la configuración de la hora de inicio del informe desde una lista desplegable con opciones preconfiguradas

Figura 39.8.

Barra lateral de notificaciones

Esta breve sección cubrirá el widget de descripción general del panel y la barra de notificación a lo largo del lado derecho de la pantalla. A diferencia de los widgets anteriores, estos no se pueden arrastrar y soltar y permanecerán estáticos en la barra lateral. Justo en la parte superior está nuestra descripción general de Paneles. Esto mostrará el conteo actual de paneles en vivo y se actualizará dinámicamente a medida que los paneles se conecten o desconecten. Al hacer clic en esto, accederá a la página de descripción general del sistema. Puede leer más sobre esta página en la sección Descripción general del sistema del manual, *Capítulo 18, Descripción general del sistema*.

Figure 39.9.

Debajo de la descripción general del panel se encuentra la barra de notificaciones. Esto proporciona notificaciones en vivo a medida que ocurren en el sistema. Aquí hay algunas opciones que pueden ayudar a mejorar la experiencia o proporcionar información importante del sistema.

A lo largo de la parte superior de la barra de notificaciones hay tres botones. Un menú desplegable para filtrar los tipos de notificación que se puede modificar a través de la Configuración de notificaciones. A la derecha de esto hay un botón de pausa/reanudar para pausar el flujo de notificaciones y un botón de notificación clara. Estos pueden ser útiles para recopilar datos/eventos necesarios para la resolución de problemas.

Finalmente, en la parte inferior de la barra de notificaciones, habrá algunos íconos junto con la versión del software. Estos iconos representan alertas activas de nivel de advertencia o de nivel crítico. Esto proporciona una vista rápida de lo que puede ser necesario resolver para garantizar un rendimiento óptimo del sistema. Los umbrales para estas advertencias se pueden configurar en la sección Configuración de salud de VAX.

Figura 39.10.

Capítulo 40. Impresión de credencial

Impresión de credenciales dentro de VAX otorga al administrador la capacidad de imprimir varios diseños en credenciales de tarjetas imprimibles.

Impresión de credenciales General

La impresión de credenciales se puede encontrar en la sección Usuarios y está etiquetada como Plantillas de tarjeta. Se puede crear una cantidad ilimitada de plantillas de tarjetas para que las utilicen los administradores. Las plantillas de tarjetas se pueden usar para titulares de tarjetas en diferentes particiones, pero deben residir en una única partición y solo pueden acceder a ellas los administradores asignados a esa partición. La impresión de credenciales incluye las siguientes características:

- Capacidad para diseñar varias plantillas para el anverso y reverso de las tarjetas.
- Imprima en cualquier impresora de tarjetas disponible en la red.
- Plantillas separadas por partición.
- Genere códigos de barras y códigos QR de varios campos de titulares de tarjetas, que luego se pueden imprimir en las tarjetas.
- Descargar diseños de tarjetas como imagen PNG.

Nuevo editor de tarjetas

Para comenzar a diseñar, el administrador primero deberá navegar hasta el editor de Nueva tarjeta que se encuentra dentro de Plantillas de tarjeta..

1. En la **barra lateral** izquierda, haga clic en **Plantillas de tarjetas**. Ahora aparecerá el panel de identificación de **fotos**.



2. Haga clic en el botón **+ Agregar** ubicado en la parte superior derecha de la página.
3. Mediante el menú desplegable, **seleccione una partición** para que resida la tarjeta y, a continuación, haga clic en **Crear**.

Inmediatamente presente en el medio de la pantalla hay una tarjeta en blanco, con íconos a la derecha de la tarjeta. El editor es una interfaz de arrastrar y soltar, donde se pueden arrastrar varias formas, herramientas e información a la tarjeta o arrastrarla fuera de la tarjeta para eliminarla.


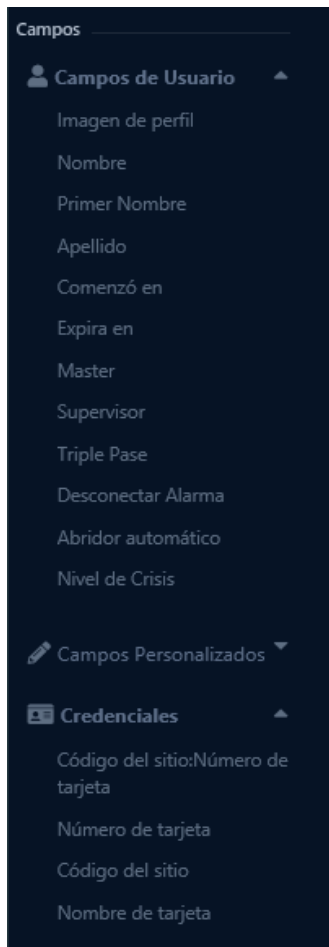
 **Nota:** Para cambiar el tamaño de un elemento, primero se debe deseleccionar el elemento. El administrador puede pasar el cursor sobre el elemento para cambiar su tamaño.



Figura 40.1. Campos del titular de la tarjetas



En el lado izquierdo (Figura 40.1), hay un menú que se puede ocultar o mostrar a través del botón de menú de la esquina superior izquierda. La información del usuario, los campos personalizados y la información de credenciales se pueden extraer automáticamente del software e imprimir en la tarjeta arrastrando el elemento correspondiente a la tarjeta en la pantalla. Los ejemplos incluyen la imagen de perfil del titular de la tarjeta, el nombre, el número de tarjeta y cualquier campo personalizado que se haya creado y asociado con el usuario

Tabla 40.1. Opciones de campos de usuario

Campo de usuario	Descripción
Imagen de perfil	Toma la foto de perfil del titular de la tarjeta, si corresponde.
Nombre	Toma el nombre completo del titular de la tarjeta (tanto el nombre como el apellido combinados).
Nombre de pila	Toma solo el primer nombre del titular de la tarjeta
Apellido	Toma solo el apellido del titular de la tarjeta
Comenzó en	Tira los inicios en la propiedad del titular de la tarjeta.
Expira el	Tira el caduca en propiedad del titular de la tarjeta.
Maestro	Muestra si el titular de la tarjeta es un usuario Maestro.
Supervisor	Muestra si el titular de la tarjeta es un Supervisor.
Triple deslizamiento	Muestra si el titular de la tarjeta tiene habilitado el permiso de triple deslizamiento.
Desactivar alarma	Muestra si el titular de la tarjeta tiene permiso para anular y desactivar alarmas.
Abridor automático	Muestra si el titular de la tarjeta tiene permiso para disparar automáticamente el abridor de puertas al deslizar la tarjeta.
Nivel de crisis	Mostrar el permiso de nivel de crisis del usuario.

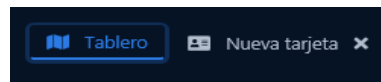
Tabla 40.2. Campos personalizados

Campo personalizado	Descripción
Campos personalizados de texto	Muestra los valores de texto del campo personalizado seleccionado para un titular de tarjeta.
Casilla de verificación Campos personalizados	Muestra el valor de texto de la casilla de verificación (verdadero o falso) para un titular de tarjeta.
Campos personalizados desplegados	Muestra el valor de texto del elemento desplegable seleccionado para un titular de tarjeta.
Campos personalizados de fecha	Muestra el campo personalizado de fecha de un titular de tarjeta, en el formato especificado. De manera predeterminada, se mostrará como mm/dd/aaaa H:MM:SS AM.

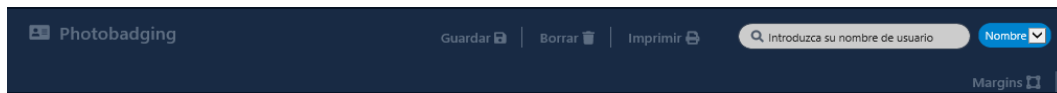
Tabla 40.3. Campos de credenciales

Campos de credenciales	Descripción
Número de tarjeta	Mostrar el número de cédula de la credencial del titular de la tarjeta.
Código del sitio	Muestra el Código de sitio/Código de instalación de la credencial del titular de la tarjeta.
Nombre de tarjeta	Muestre el nombre de la credencial en la tarjeta.

En la parte superior del editor se encuentran las distintas pestañas, ya que VAX le brinda al administrador la capacidad de tener varias tarjetas abiertas en diferentes pestañas para editarlas o imprimirlas al mismo tiempo.



Justo debajo de esa barra superior está el nombre de la plantilla, junto con botones para guardar la plantilla, borrarla y comenzar desde cero, imprimir la tarjeta o buscar usuarios.



La búsqueda se puede realizar por nombre (nombre o apellido) o número de tarjeta/credencial PIN. Después de buscar un usuario y seleccionar del menú desplegable, la plantilla de la tarjeta se actualizará con su información respectiva para que el administrador pueda ver una vista previa de cómo se vería la tarjeta, así como imprimir la tarjeta individual inmediatamente desde el editor con la información del usuario.

A la derecha del lienzo de la tarjeta se encuentra el menú Tarjeta, Herramientas y Formas. Las opciones de la tarjeta cambian la orientación de la tarjeta, así como qué lado de la tarjeta está actualmente seleccionado para editar. Los menús de herramientas y formas ofrecen las siguientes opciones:

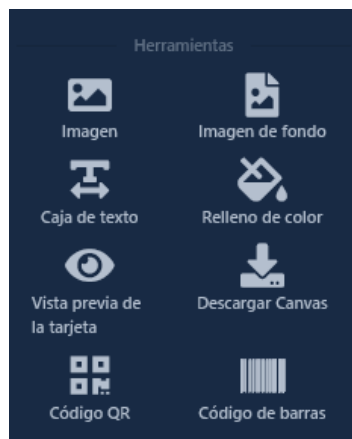


Tabla 40.4. Menú de herramientas

Herramientas	Descripción
Imagen	Cargue una imagen en la tarjeta que se puede mover y cambiar de tamaño.
Imagen de fondo	Cargue una imagen estática para usarla como fondo de la tarjeta. La imagen se estirará para llenar toda la tarjeta.
Caja de texto	Coloca un cuadro de texto editable para contener cualquier texto.
Relleno de color	Rellena el fondo con un color específico de elección, o usando una de las imágenes de fondo preestablecidas.
Vista previa de la tarjeta	Muestra la tarjeta sola. Haga clic en "Salir de vista previa de la tarjeta" para seguir editando la tarjeta.
Descargar lienzo	Descarga el lienzo y el lateral de la tarjeta actual como una única imagen JPEG.
Código QR	Genere un código QR para colocarlo en la tarjeta con información que contenga los campos de usuario, los campos personalizados o la información de credencial del titular de la tarjeta. Solo se puede seleccionar y generar 1 campo por código QR.
Código de barras	Genere un código de barras para colocarlo en la tarjeta con información que contenga los campos de usuario, los campos personalizados o la información de credencial del titular de la tarjeta. Solo se puede seleccionar y generar 1 campo por código de barras

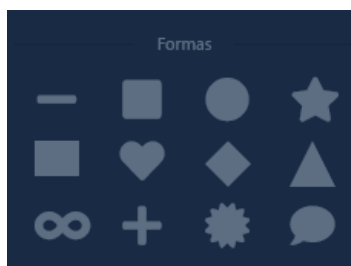


Table 40.5. Menu de formas

Figuras	Descripción
Línea	Coloque una sola línea sólida en la tarjeta.
Cuadrado	Coloca un cuadrado de relleno sólido en la tarjeta.
Círculo	Coloca un círculo de relleno sólido en la tarjeta.
Estrella	Coloca una estrella de relleno sólido en la tarjeta.
Rectángulo	Coloca un rectángulo de relleno sólido en la tarjeta que se puede cambiar de tamaño en diversos grados.
Corazón	Coloca un objeto con forma de corazón de relleno sólido en la tarjeta.
Diamante	Coloca un objeto de diamante de relleno sólido en la tarjeta.
Triángulo	Coloca un objeto de triángulo de relleno sólido en la tarjeta.
Símbolo infinito	Coloca un objeto de símbolo de infinito en la tarjeta.
símbolo más	Coloca un objeto de símbolo más en la tarjeta.
Certificado	Coloca un objeto de certificado en la tarjeta.
Burbuja de chat	Coloca una forma de burbuja de chat de relleno sólido en la tarjeta

Cada elemento tiene un conjunto de propiedades que son muy similares entre elementos similares. A continuación se muestra una tabla de las diversas propiedades de cada elemento.

Tabla 40.6. Tabla de propiedades de campo

propiedades de campo	Descripción
Propiedades de imagen	<ul style="list-style-type: none"> • Desenfocar: ajuste el control deslizante/cuadro de texto para aumentar el desenfocar general de la imagen. Valores entre 0 - 5 para la intensidad del desenfocar. • Brillo: ajuste el control deslizante/cuadro de texto para aumentar o disminuir el brillo de la imagen. Valores entre 0 - 200. • Contraste: ajuste el control deslizante/cuadro de texto para aumentar o disminuir el contraste de la imagen. Valores entre 0 - 200. • Escala de grises: ajuste el control deslizante/cuadro de texto para disminuir la cantidad de color en la imagen. Valores entre 0 - 100. • Invertir: ajuste el control deslizante/cuadro de texto para invertir los colores de la imagen. Valores entre 0 - 100. • Opacidad: ajuste el control deslizante/cuadro de texto para cambiar la transparencia de la imagen. Valores entre 0 - 100. • Saturar: ajuste el control deslizante/cuadro de texto para aumentar o disminuir la saturación de los colores de la imagen. Valores entre 0 - 200. • Sepia: ajuste el control deslizante/cuadro de texto para aumentar el filtro sepia y hacer que la imagen sea más cálida. Valores entre 0 - 100. • Propiedades predeterminadas: restablecer todos los valores a sus valores predeterminados.
Propiedades de texto	<ul style="list-style-type: none"> • Negrita: casilla de verificación para poner en negrita todo el nombre. • Cursiva: casilla de verificación para establecer el nombre en cursiva. • Subrayado: casilla de verificación para subrayar todo el campo del nombre. • Tachado: casilla de verificación para aplicar una línea de izquierda a derecha en todo el campo de nombre. • Tamaño del texto: control deslizante/cuadro de texto ajustable para aumentar o disminuir el tamaño del texto. Valores entre 0 - 300. • Color del texto: cambia el color del texto, usando valores RGB o seleccionando de la paleta configurable • Opacidad: ajuste el control deslizante/cuadro de texto para cambiar la transparencia de la imagen. Valores entre 0 - 100. • Sombra: agregue un efecto de sombra en la tarjeta

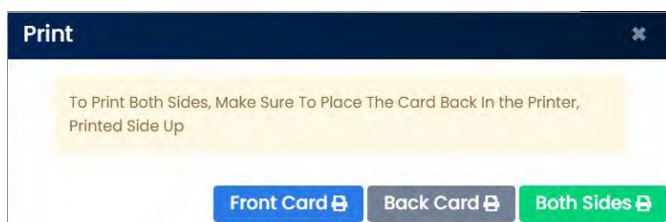
<p>Propiedades de forma</p>	<ul style="list-style-type: none"> • Desenfoco: ajuste el control deslizante/cuadro de texto para aumentar el desenfoco general de la imagen. Valores entre 0 - 5 para la intensidad del desenfoco. • Brillo: ajuste el control deslizante/cuadro de texto para aumentar o disminuir el brillo de la imagen. Valores entre 0 - 200. • Contraste: ajuste el control deslizante/cuadro de texto para aumentar o disminuir el contraste de la imagen. Valores entre 0 - 200. • Escala de grises: ajuste el control deslizante/cuadro de texto para disminuir la cantidad de color en la imagen. Valores entre 0 - 100. • Invertir: ajuste el control deslizante/cuadro de texto para invertir los colores de la imagen. Valores entre 0 - 100. • Opacidad: ajuste el control deslizante/cuadro de texto para cambiar la transparencia de la imagen. Valores entre 0 - 100. • Saturar: ajuste el control deslizante/cuadro de texto para aumentar o disminuir la saturación de los colores de la imagen. Valores entre 0 - 200. • Sepia: ajuste el control deslizante/cuadro de texto para aumentar el filtro sepia y hacer que la imagen sea más cálida. Valores entre 0 - 100. • Propiedades predeterminadas: restablecer todos los valores a sus valores predeterminados.
------------------------------------	--

Impresión de una tarjeta

La impresión en impresoras de tarjetas dentro de VAX se puede hacer a través del editor de Nueva Tarjeta o las páginas individuales de Editar Usuario. Vaya a la página de edición de usuario y haga clic en la pestaña Credenciales. Junto a la credencial habrá un icono de impresora. Haga clic en este icono para abrir la ventana emergente Plantillas de tarjeta, donde ahora aparecerán las plantillas guardadas disponibles. Seleccione la plantilla que desea usar para el anverso o el reverso. Ahora aparecerán las opciones de la impresora..



Al imprimir desde el editor de tarjetas, aparecerá una ventana emergente en la que el administrador puede seleccionar imprimir el anverso, el reverso o ambos lados de la tarjeta. A continuación, se puede seleccionar una impresora como destino.



Capítulo 41. Integración de Schlage

Las cerraduras inalámbricas Allegion Schlage se pueden integrar con VAX. Después de la configuración inicial, habrá muy poca diferencia entre la funcionalidad de una cerradura Schlage en comparación con una puerta administrada típica en el software VAX..

Nota

El servidor Schlage para que VAX se comunice con la puerta de enlace deberá agregarse durante la instalación. Si VAX ya está instalado sin el servidor Schlage agregado, será necesario desinstalar y volver a instalar VAX. *La desinstalación y la reinstalación no borrarán la base de datos y es seguro realizarla para agregar el servicio Schlage adicional.*

Note

El complemento Lockset se debe comprar en la licencia de **Obsidian** para que los candados se vinculen al sistema.

Schlage Overview

VAX puede integrarse con cerraduras inalámbricas Schlage a través de ENGAGE Gateway.

- Ver el estado de las particiones de alarma y las zonas de alarma
- Armar (Armar En Casa, Armar Ausente, Armar Noche) y desarmar a través de la interfaz web de VAX, la aplicación móvil, los planes de acción o a través de la API de VAX
- Omitir zonas, ponerse en contacto con los servicios de emergencia, silenciar los pitidos de problemas Hay 3 componentes externos para integrar Schlage Locksets con VAX:
 - ENGAGE Gateway: actúa como un "Panel" dentro de VAX
 - Schlage Lockset: actúa como una "Puerta" dentro de VAX
 - Allegion ENGAGE: para registrar aplicaciones y dispositivos en un sistema Schlage.

Allegion ENGAGE App

La aplicación de teléfono Allegion ENGAGE se usa para conectar cerraduras Schlage a una puerta de enlace Schlage. Se requiere una cuenta de Allegion para comenzar a agregar cerraduras y puertas de enlace a un sitio.

La aplicación **Allegion ENGAGE** se puede descargar desde Google Play Store para dispositivos Android o Apple App Store para dispositivos Apple.

Adición de un sitio ENGAGE

1. En el menú de la barra lateral izquierda, ubique y haga clic en Engage Sites que se encuentra en la sección HARDWARE.
2. Haga clic en Agregar para crear un nuevo sitio de Engage.
3. Proporcione un nombre para el sitio de Engage. Seleccione la partición y el sitio en VAX en el que residirá el sitio de Engage.

Nota

Cualquier dispositivo futuro que se agregue a este sitio de Engage se agregará a la partición y el sitio seleccionados en VAX.

4. Ingrese las credenciales de correo electrónico y contraseña para una cuenta de Engage, luego haga clic en Crear nuevo sitio de Engage. Si se ingresaron las credenciales adecuadas, el sitio de Engage se agregará correctamente. De lo contrario, vuelva a ingresar las credenciales y haga clic en el botón Crear nuevamente.
5. Verifique que el sitio exista abriendo la aplicación Allegion ENGAGE en un dispositivo móvil y vea los sitios.

Conexión a ENGAGE Gateway de la App

1. Encienda la puerta de enlace.
2. Tome nota del número de serie de la puerta de enlace. Esto se puede encontrar en la parte inferior del Gateway.
3. Restablecimiento de fábrica de la puerta de enlace. Consulte el manual de la puerta de enlace para obtener instrucciones sobre cómo restablecer (generalmente un botón en la parte posterior).
4. Dentro de la aplicación Allegion ENGAGE Mobile, seleccione el sitio de Engage creado anteriormente y toque "Seleccionar". Esto abrirá la página Dispositivos.
5. Toque el botón + ubicado en la parte inferior derecha de la pantalla para agregar un dispositivo.
6. En la lista, seleccione Puerta de enlace para agregar la puerta de enlace ENGAGE. La siguiente página mostrará una lista de todas las puertas de enlace cercanas listas para conectarse, diferenciadas por números de serie.
7. Seleccione la puerta de enlace con el número de serie como se indicó anteriormente para agregarlo.
8. Asigne un nombre a la puerta de enlace y seleccione Siguiente.
9. Seleccione IP como Modo de comunicación de puerta de enlace y haga clic en Siguiente.
10. Cambie "IP detrás del cortafuegos" a ON y seleccione DHCP para la configuración de IP. Haga clic en Siguiente.
11. La dirección del servidor ahora buscará la configuración del servidor Schlage configurada durante la instalación inicial (avanzada). Establezca los siguientes parámetros:

Tabla 41.1. Gateway parámetros

Server URL	https://<your server address>:7111/engage_wss
CA Server URL	http://<Your server address>:7110/engage/newCA/current
Keep Alive (in seconds)	300

El dispositivo comenzará a conectarse y notificará una vez completado.

12. Hay 2 métodos para agregar el Gateway a VAX una vez que se haya agregado al sitio ENGAGE.
 - En Paneles desconocidos, la puerta de enlace aparecerá con su número de serie como dirección MAC.
 - Cuando esté en la página de edición de Engage Sites, vaya a la pestaña Puertas de enlace y haga clic en el botón Sincronizar.
13. La puerta de enlace ahora aparecerá en los paneles y el administrador ahora puede editarla desde la página Paneles o la página Editar sitios de Engage.

Adición de un juego de cerraduras Schlage a VAX

1. El juego de cerradura requerirá baterías. Asegúrese de que las baterías nuevas o completamente cargadas estén instaladas en la cerradura. Una presentación de credenciales al lector de Lockset responderá si se proporciona suficiente energía.

Nota

Por lo general, las pilas AA se utilizan en cerraduras. Consulte el manual de la cerradura para conocer el tipo de batería recomendado.

2. En la aplicación Allegion ENGAGE, seleccione el **sitio ENGAGE** en uso y seleccione el **botón +**.
3. En la pantalla de **selección de tipo de dispositivo**, seleccione ND si la cerradura es de la serie NDE o seleccione LE si la cerradura es de la serie LE.
4. Complete la adición del dispositivo Lockset al sitio ENGAGE siguiendo las instrucciones restantes en la aplicación. La sección wifi se puede omitir.
5. Desde VAX, en la **sección Hardware** de la **barra lateral**, **seleccione Engage Sitios**. Seleccione el sitio de Engage al que se agregó el dispositivo. Seleccione la pestaña **Dispositivos** y seleccione el botón **Sincronizar**. El nuevo Lockset debe verse en la pestaña **Locks**.

Adición de juego de cerradura a una puerta

1. Desde VAX, en la sección **Hardware** de la barra lateral, seleccione **Engage Sites**.
2. Edite el sitio de Engage donde se agregó Lockset. Seleccione la pestaña **Gateway** y seleccione el botón **Editar** puerta de enlace.
3. Seleccione la pestaña **Puertas** y seleccione el **botón + Agregar nuevas puertas**. Esto hará que la puerta de enlace busque todas las cerraduras disponibles cercanas..

Nota

El escaneo puede tomar hasta 30 segundos, también puede tomar algunos intentos. Si la cerradura está demasiado lejos de la puerta de enlace seleccionada, es posible que se deba seleccionar una puerta de enlace más cercana de los pasos anteriores.

4. Después del escaneo, seleccione el botón **Agregar** en el juego de cerraduras requerido.
5. El Schlage Lockset ahora se agrega como una puerta en el VAX

Nota

Si es necesario cambiar una cerradura a una puerta de enlace diferente en el mismo sitio de Engage, la puerta se puede desvincular de la puerta de enlace en la página Editar puerta de enlace en la pestaña Candados vinculados en la pestaña Candados.

Precaución

Si un bloqueo necesita cambiar los sitios de Engage, entonces el bloqueo debe eliminarse del sitio de Engage, restablecerse de fábrica y luego agregarse a un sitio de Engage diferente.

Supervisión y anulación de Schlage

Las cerraduras inalámbricas Schlage se pueden tratar como una puerta dentro de VAX. Consulte la sección Supervisión e invalidación de puertas para obtener información sobre cómo anular o supervisar el estado de las cerraduras.

Solución de problemas de Schlage

Se permite un total de 10 dispositivos habilitados para ENGAGE por puerta de enlace.

El rango de comunicación de la puerta de enlace a las esclusas es de 30' a 50' en una ubicación ideal

Asegúrese de no vincular dispositivos en la aplicación. La aplicación es solo para agregar la cerradura y la puerta de enlace. Aplicación que muestra que no se encontraron dispositivos. Mantenga presionado el botón de reinicio hasta que el dispositivo se vuelva verde.

Apague y encienda la puerta de enlace si los problemas persisten con la conexión en la aplicación.

Capítulo 42. Supervisión del Funcionamiento en VAX

Este capítulo cubrirá los fundamentos de los **sistemas de monitoreo de funcionamiento** en VAX y explicará cómo utilizar las herramientas disponibles para mantener la salud del sistema VAX.

Introducción al Monitoreo de funcionamiento

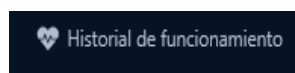
Es importante entender cómo mantener un sistema VAX. Las herramientas de informes de VAX permiten a los administradores revisar los eventos que el sistema VAX ha manejado y el historial del sistema. El **funcionamiento del sistema** VAX se puede monitorear usando las herramientas en Historial de funcionamiento y mantenerse usando las diferentes selecciones de Configuraciones de Funcion. La configuración permite a los administradores establecer notificaciones o registros para que aparezcan cuando ocurre un evento, notificándolos en tiempo real.

El **historial de funcionamiento** es una herramienta de generación de informes que permite al administrador ver eventos relacionados con el funcionamiento y el mantenimiento del sistema. **Configuración de funciones** es una sección de configuración que contiene una lista de eventos relacionados con las funciones del sistema VAX que se pueden monitorear y configurar para notificar a los administradores cuando ocurran. La herramienta Historial de Funcionamiento recopila registros sobre el estado de salud del sistema VAX entre una hora de inicio y una hora de finalización. Estos registros se pueden filtrar aún más por Problemas de funcionamiento y la gravedad o naturaleza del registro, como los niveles **Saludable, Advertencia y Crítico**. Debajo de Configuración de funcionamiento hay opciones para mostrar íconos, registros y notificaciones cuando un evento relacionado con el funcionamiento del sistema VAX activa una acción, incluidas nuevas versiones de software, paneles desinstalados, batería baja en los dispositivos y más. La siguiente sección repasará las herramientas de historial de funcionamiento de VAX.

Historial de Funcionamiento

La sección Historial de funcionamiento de Reportes contiene opciones para ejecutar informes sobre la función y el estado del sistema VAX. Como un tipo de Informe, esta herramienta ejecuta un reporte para compilar una lista de eventos que ha manejado el sistema VAX. Este capítulo explicará sus características y herramientas y cómo usar estas herramientas para limitar la búsqueda de informes para resultados personalizables.

Figura 42.1. Icono Historial de funcionamiento

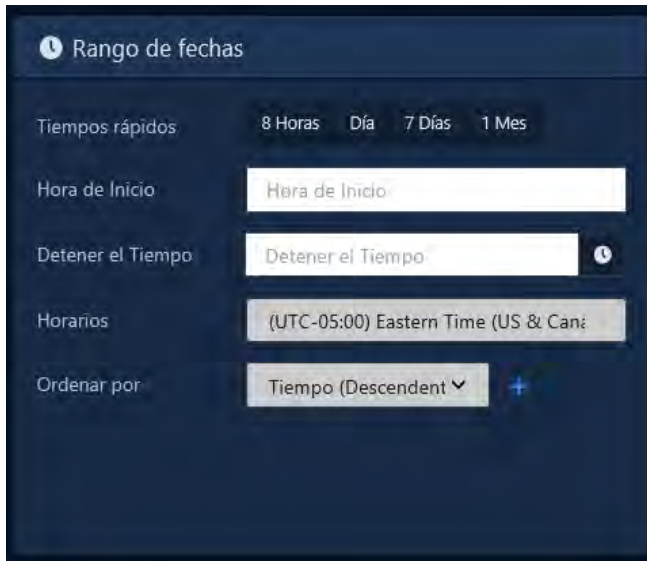


Herramientas de historial de funcionamiento

Historial de Funcionamiento: intervalo de fechas

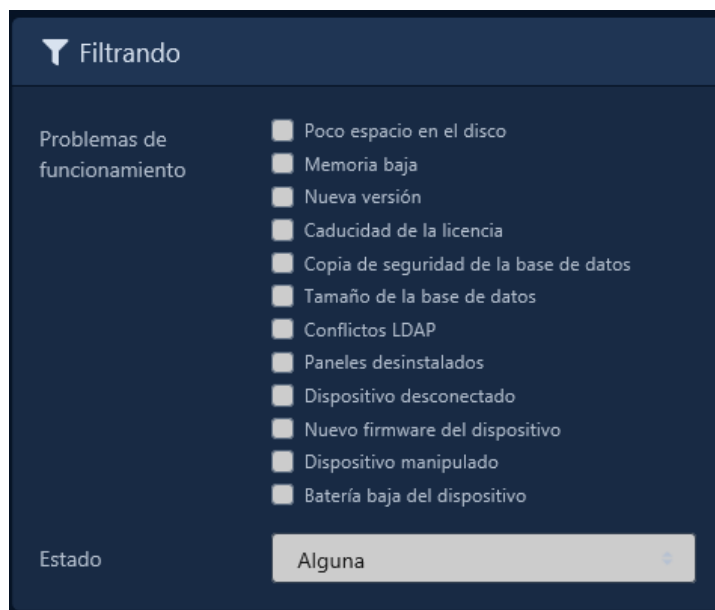
Historial de funcionamiento que se encuentra en la sección **Reportes** de la **barra de herramientas**, muestra informes sobre la salud del sistema VAX. Esta función permite a los administradores elegir una hora y fecha de inicio y una hora y fecha de finalización para filtrar las notificaciones. Los tiempos se establecen utilizando la herramienta de calendario para ayudar a configurarlos rápidamente. Luego, el sistema compilará todos los registros creados entre los tiempos establecidos que coincidan con una lista de especificaciones de filtro seleccionadas. Hay opciones de tiempo rápido que permiten la selección de 8 horas, 1 día, 7 días y 1 mes sin configuración manual. Los administradores pueden elegir un método Ordenar por que ordena los registros por Ascendente o Descendente, por ocurrencia. Hay un selector de zona horaria que puede calibrar las marcas de tiempo para diferentes zonas horarias.

Figura 42.2 Icono Historial de funcionamiento



Filtros

Figura 42.3. Icono de filtros



Hay selecciones de filtro por problemas de salud y el estado del problema. Estos problemas de salud son rastreados automáticamente por VAX y filtran los problemas de salud para reducir la selección y eliminar los problemas no seleccionados de la lista de informes. Si no se selecciona ningún problema, VAX incluirá todos los problemas de forma predeterminada. Las opciones de filtro para problemas de salud incluyen:

1. Poco espacio en disco
2. Memoria baja
3. Nueva versión
4. Caducidad de la licencia
5. Copia de seguridad de la base de datos

6. Tamaño de la base de datos
7. Conflictos LDAP
8. Paneles desinstalados
9. Dispositivo desconectado
10. Nuevo firmware del dispositivo
11. Dispositivo manipulado
12. Baja Batería en dispositivo

Algunos de estos problemas son tan simples como registrar si el software se actualizó a una nueva versión, mientras que otros, como memoria baja o batería baja del dispositivo, se monitorean e informarán sobre sus cambios..

Poco espacio en disco

La opción Espacio en disco bajo alterna la selección del registro del valor monitoreado por el sistema de informes del historial de salud. Al seleccionar la opción Poco espacio en disco, se reducirá la lista de informes para incluir registros de Poco espacio en disco. El sistema mostrará un registro de espacio en disco bajo cuando el disco en el que está instalado el sistema VAX alcance un umbral porcentual de espacio en disco restante. Este valor de umbral se puede establecer y cambiar en Configuración de salud. Se puede establecer un umbral para los niveles de advertencia y críticos y el VAX mostrará el nivel apropiado y el porcentaje de espacio en disco restante. El espacio en disco restante predeterminado para el nivel de advertencia es del 70 % y para el crítico es del 90 %.

Memoria baja

La opción Memoria baja alterna la selección del registro del valor monitoreado por el sistema de informes del historial de salud. Cuando el sistema utiliza un alto porcentaje de la memoria disponible para el sistema, se crean registros. De manera predeterminada, el nivel de advertencia notificará cuando se use el 70 % o más de la memoria y el nivel crítico sea el 90 % o más. Estos valores se pueden cambiar en Configuración de salud.

Nueva versión

La opción Nueva versión alterna la selección de los registros que supervisan la disponibilidad de una nueva versión del software. El sistema creará un registro basado en la cantidad de días desde el lanzamiento. El valor predeterminado para el nivel de advertencia es 0 días. Estos valores se pueden cambiar en Configuración de salud.

Caducidad de Licencia

The License Expiry option toggles selection of the logs monitoring the expiration of the license of the La opción Caducidad de la licencia alterna la selección de los registros que supervisan la caducidad de la licencia del sistema VAX. El sistema registrará un nivel de advertencia cuando quede una cantidad de días hasta el vencimiento. El número predeterminado de días es 0. Estos valores se pueden cambiar en Configuración de salud.

Copia de seguridad de la base de datos

La opción Copia de seguridad de la base de datos alterna la selección de los registros que supervisan los días desde que se realizó una copia de seguridad. De forma predeterminada, el sistema registrará un nivel de advertencia cuando los días desde que se realizó una copia de seguridad alcancen los 75 días. El nivel crítico es de 80 días desde la copia de seguridad. Estos valores se pueden cambiar en Configuración de funcionamiento

Tamaño de la base de datos

La opción Tamaño de la base de datos alterna la selección de los registros que monitorean el tamaño de la base de datos del sistema VAX. Por defecto, el Nivel de Aviso registrará un Aviso cuando la Base de Datos alcance el 1% y seguirá notificando semanalmente sobre el crecimiento del sistema. De forma predeterminada, el nivel crítico se establece en el 90 % del tamaño de la base de datos. Estos valores se pueden cambiar en Configuración de funcionamiento.

Conflictos LDAP

La opción Conflictos de LDAP alterna la selección de los Conflictos de LDAP del sistema de supervisión de registros. VAX creará un registro después de un número de horas desde que ocurrió el último conflicto. De forma predeterminada, el nivel de advertencia se establece en 0 horas después de un conflicto. El nivel crítico se establece en 0 horas de forma predeterminada. Estos valores se pueden cambiar en Configuración de funcionamiento.

Paneles desinstalados

La opción Paneles desinstalados alterna la selección de los registros que supervisan el estado de los paneles. El sistema VAX creará un registro después de desinstalar una serie de paneles. De forma predeterminada, el nivel de advertencia creará un registro si se desinstalan más de 0 paneles. Estos valores se pueden cambiar en Configuración de funcionamiento.

Dispositivo desconectado

La opción Dispositivo desconectado alterna la selección de los registros que monitorean la cantidad de dispositivos que se desconectan. El sistema VAX creará un registro después de que más del 1 % de los dispositivos se hayan desconectado.

Nuevo firmware del dispositivo

La opción Nuevo firmware del dispositivo alterna la selección de los registros que monitorean el lanzamiento de un nuevo firmware para los dispositivos conectados al sistema VAX. De manera predeterminada, el sistema creará un registro si más del 0 % de los dispositivos tienen una actualización de firmware disponible. Estos valores se pueden cambiar en Configuración de funcionamiento.

Dispositivo manipulado

La opción Dispositivo manipulado alterna la selección de los registros que supervisan la manipulación de dispositivos. De forma predeterminada, si se han manipulado más del 0 % de los dispositivos, el nivel de advertencia creará un registro. Estos valores se pueden cambiar en Configuración de funcionamiento.

Dispositivo con batería baja

La opción de batería baja del dispositivo alterna la selección de los registros que monitorean el nivel de batería de los dispositivos inalámbricos. Por defecto, el sistema crea un registro si más del 0% de las baterías llega al 0%. Estos valores se pueden cambiar en Configuración de funcionamiento.

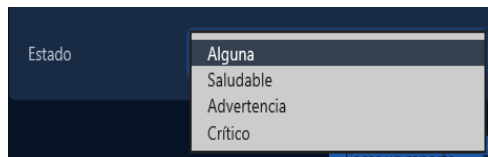
Estado

A continuación hay diferentes opciones para filtrar los registros por estado y gravedad. Estos tipos de estado pueden filtrar por cambios de salud positivos y cambios negativos por las siguientes selecciones:

1. Cualquiera
2. Saludable

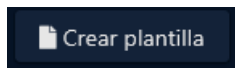
3. Advertencia
4. Crítico

Figure 42.4. Icono de Estado



Utilice una combinación de las opciones de filtros, estados y rango de fechas para restringir la búsqueda a problemas específicos, tipo de estado y hora o fechas de ocurrencia. También hay un botón para guardar estas búsquedas filtradas como una plantilla que se puede llamar para uso repetido, modificar y volver a guardar en el futuro o guardar como una nueva plantilla. Las opciones de formato incluyen CSV y HTML. Después de ejecutar un reporte de **historial de funcionamiento** hay un botón Volver a la configuración, un botón Actualizar informe y un botón Exportar. El botón Exportar proporcionará dos opciones, CSV o HTML. El archivo CSV se puede descargar y abrir en hojas de cálculo y programas de edición de texto como Microsoft Excel o Notepad. Los archivos HTML se pueden descargar y abrir en un navegador HTML para verlos en una nueva ventana. Las flechas en la parte superior e inferior de los resultados se pueden usar para avanzar a la página siguiente para ver más registros.

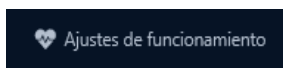
Figura 42.5. Icono de plantilla



Configuración de funcionamiento

La Configuración de funcionamiento en la sección Administración es una herramienta para activar las notificaciones de eventos relacionados con la salud del sistema. Los diferentes Ajustes de Salud y sus usos serán discutidos en este capítulo

Figura 42.6. Icono de Configuración de funcionamiento



Introducción a la configuración de funcionamiento

La **configuración de funcionamiento** se puede encontrar navegando a la sección **Administración** en la barra de tareas. Esta herramienta le permite al usuario **seleccionar una acción** para tomar en caso de que haya un cambio en el valor que está monitoreando la configuración de funcionamiento.

Acciones

Se puede seleccionar cualquier cantidad de acciones para que ocurran para cada evento que la configuración de funcionamiento pueda monitorear. Después de seleccionar una configuración de funcion para trabajar, se pueden seleccionar varias acciones para cada configuración de funcionamiento seleccionando la casilla de verificación de cada acción. Estas acciones se pueden deseleccionar desmarcando la casilla. Estas acciones incluyen:

1. Mostrar icono
2. Problema de registro
3. Notifique a los administradores del sistema por correo electrónico

4. Notificar al distribuidor por correo electrónico
5. Notificar a los administradores del sistema a través de Web Push

Figura 42.7 Problemas de funcionamiento



Frecuencia de notificación

El formato de frecuencia de notificación permite un número de entrada equivalente a una selección de horas, días, semanas o meses entre notificaciones. El usuario puede dictar un aumento o disminución en el nivel de advertencia en función de un valor que los administradores pueden establecer para cada tipo de configuración de funcionamiento.



El administrador también puede cambiar el valor de frecuencia de notificación para aumentar o disminuir el tiempo entre las notificaciones enviadas durante el nivel de advertencia activo para una configuración de funcionamiento. Por ejemplo, "1" días después del lanzamiento de una nueva versión establece el nivel de advertencia en 1.

Durante este período, los administradores pueden realizar las acciones "Registrar problema" cada "12" horas hasta que cambie el nivel de advertencia. Después de "7" días después del lanzamiento, el nivel de advertencia aumenta al nivel de advertencia 2/nivel crítico, cambiando los tipos de acción a "Mostrar icono" y/o "Notificar al distribuidor por correo electrónico", y cambiando la frecuencia de notificación a cada "2" horas según en la configuración realizada en la sección Nivel de advertencia 2/Nivel crítico para esa **configuración de funcionamiento**

Niveles de advertencia

Figura 42.8. Icono de Niveles de advertencia



Figura 42.9. Icono de nivel crítico

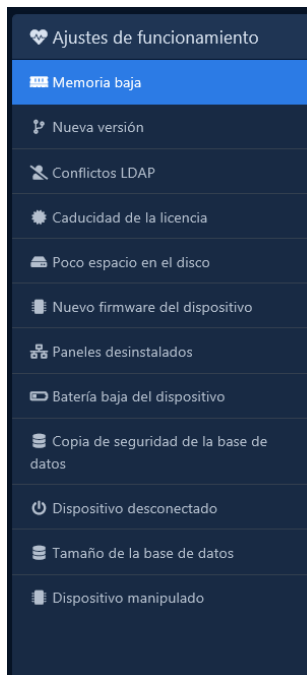


Cada una de estas **configuraciones de funcionamiento** se puede habilitar seleccionando la casilla Habilitar en la parte superior de cada página de configuración de funcionamiento. De forma predeterminada, esta configuración está habilitada. Cada configuración de estado tiene un evento diferente observado y un valor de umbral que activará un cambio en el nivel de advertencia si se alcanza. Para cada nivel de advertencia, se puede asignar y cambiar cualquier cantidad de acciones y la frecuencia de las notificaciones.

Establecer este valor de umbral determinará cuándo se llevarán a cabo las acciones. Se pueden asignar acciones para activar si cambia el nivel de advertencia. Durante el tiempo que el nivel de advertencia esté activo, las acciones se activarán con la frecuencia designada por la selección de frecuencia de notificación. Se pueden asignar hasta dos niveles de advertencia para cada configuración de funcionamiento. Si se alcanza el segundo umbral, el nivel de advertencia cambia y el segundo conjunto de configuraciones de acciones y frecuencia de notificación anulan el nivel de advertencia anterior. El nivel crítico se puede configurar con parámetros de frecuencia de notificación y acción crecientes, decrecientes o iguales.

Configuraciones de funcionamiento: Opciones

Figura 42.10. Configuraciones de funcionamiento



Esta sección repasará los diferentes tipos de configuraciones de funcionamiento y lo que cada una de las configuraciones monitorea. Los ajustes de funcionamiento que se pueden configurar para desencadenar acciones incluyen:

1. Dispositivo manipulado
2. Caducidad de la licencia
3. Dispositivo desconectado
4. Paneles desinstalados
5. Tamaño de la base de datos

6. Nueva versión
7. Nuevo firmware del dispositivo
8. Batería baja del dispositivo
9. Copia de seguridad de la base de datos
10. Memoria baja
11. Poco espacio en disco
12. Conflictos LDAP

Poco espacio en el disco

Cuando el disco en el que está instalado el sistema VAX alcanza un umbral porcentual del espacio restante en disco. Este valor de umbral se puede establecer y cambiar en Configuración de funcionamiento. El espacio en disco restante predeterminado para el nivel de advertencia es del 70 % y para el crítico es del 90 %.

Memoria baja

Cuando el sistema utiliza un alto porcentaje de la memoria disponible para el sistema, se crea un registro. De manera predeterminada, el nivel de advertencia notificará cuando se use el 70 % o más de la memoria y el nivel crítico sea el 90 % o más.

Nueva versión

El sistema creará un registro basado en la cantidad de días desde el lanzamiento. El valor predeterminado para el nivel de advertencia es 0 días. Estos valores se pueden cambiar en Configuración de funcionamiento.

Caducidad de la licencia

El sistema registrará un nivel de advertencia cuando quede una cantidad de días hasta el vencimiento. La cantidad predeterminada de días es 0. Estos valores se pueden cambiar en Configuración de funcionamiento.

Copia de seguridad de la base de datos

La copia de seguridad de la base de datos registra los días desde que se realizó una copia de seguridad. De forma predeterminada, el sistema registrará un nivel de advertencia cuando los días transcurridos desde que se realizó una copia de seguridad alcancen los 75 días. El nivel crítico es de 80 días desde la copia de seguridad. Estos valores se pueden cambiar en Configuración de funcionamiento.

Tamaño de la base de datos

Tamaño de la base de datos registra el tamaño de la base de datos del sistema VAX. Por defecto, el Nivel de Aviso registrará un Aviso cuando la Base de Datos alcance el 1% y seguirá notificando semanalmente sobre el crecimiento del sistema. De forma predeterminada, el nivel crítico se establece

en el 90 % del tamaño de la base de datos.

Conflictos LDAP

Conflictos LDAP registra los conflictos LDAP del sistema. VAX creará un registro después de un número de horas desde que ocurrió el último conflicto.

Paneles desinstalados

Los paneles desinstalados monitorean el estado de conexión de los paneles. El sistema VAX creará un registro después de desinstalar una serie de paneles.

Dispositivo desconectado

Dispositivo desconectado supervisa la cantidad de dispositivos que se desconectan.

Nuevo firmware del dispositivo

El nuevo firmware del dispositivo supervisa el lanzamiento de un nuevo firmware para los dispositivos conectados al sistema VAX. Estos valores se pueden cambiar en Configuración de funcionamiento.

Dispositivo manipulado

Dispositivo manipulado supervisa la manipulación de dispositivos.

Dispositivo con batería baja

La opción de batería baja del dispositivo monitorea el nivel de batería de los dispositivos inalámbricos.

Conclusion

Es importante entender y mantener la salud del sistema VAX; saber que su sistema está actualizado, respaldado, tiene suficiente espacio de almacenamiento y la energía de la batería pueden ser cosas vitales para monitorear al mantener y solucionar problemas del sistema VAX.

Combine el uso de las herramientas de **Configuración e Historial de funcionamiento** para mantenerse informado sobre el historial y la salud actual del sistema VAX. Esto permite a los administradores mirar hacia atrás para solucionar problemas y ver las actualizaciones de estado del sistema a medida que suceden en tiempo real.

Capítulo 43. Solución de problemas en VAX

A veces, una instalación sale mal, faltan archivos o están dañados. Las comunicaciones no se conectan, las entradas y salidas no responden correctamente y las tarjetas devuelven acceso denegado cuando no deberían hacerlo. Este capítulo cubrirá cómo solucionar problemas comunes para encontrar una solución.

Herramientas comunes: Menús LED de Panel

Alguna información importante sobre la solución de problemas del panel: Usando el LED en el panel podemos acceder a un menú de edición y un menú de solo lectura. A continuación encontrará instrucciones sobre cómo utilizar estos menús.

Para acceder al menú Editar en el panel LED:

1. Mantenga presionado el botón [Entrar]
2. Introduzca la contraseña del panel, por defecto es 0000
3. Presione [ESC] para ingresar la contraseña
4. Desplácese hacia arriba y hacia abajo con los botones blancos (SW1, SW2)
5. Presione [Enter] para seleccionar un modo para cambiar/ver
6. Usa los botones blancos para desplazarte entre las opciones
6. Presione [ESC] para salir del modo de edición

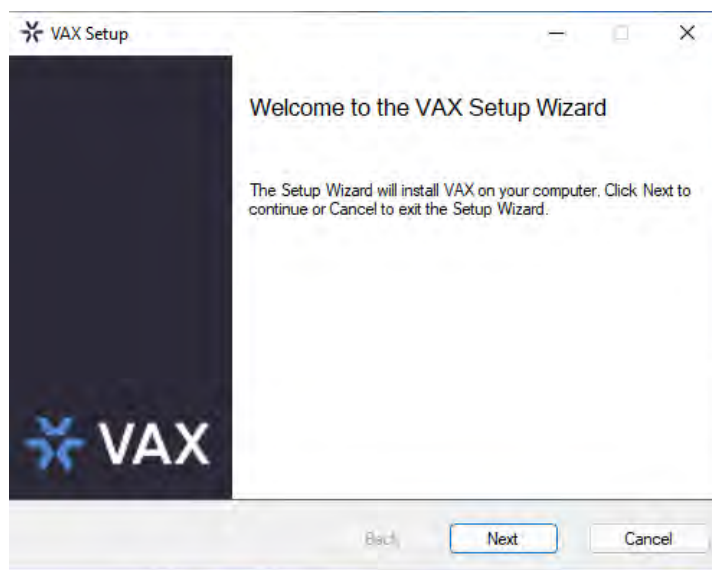
El menú de sólo lectura en el panel LED:

1. Mantenga presionado el botón [ESC]
2. Desplácese hacia arriba y hacia abajo usando los botones blancos para ver (SW1, SW2)
3. Presione [ESC] para salir de Solo lectura

Estos menús son útiles para solucionar problemas de paneles, conectividad y encontrar información sobre su panel. *Consulte el Capítulo 3, Configuración inicial* para obtener más información e imágenes.

Solución de problemas del instalador

El proceso de instalación puede tardar algunos pasos en completarse y, en cada paso, algo puede salir mal. Esta sección cubrirá problemas comunes con la instalación y cómo solucionar problemas para encontrar el problema y resolverlo.

Figura 43.1. Instalador de aplicaciones VAX

Nota IMPORTANTE

Al actualizar o migrar a un nuevo servidor, asegúrese de leer detenidamente las notas del instalador. En algunos casos, la instalación de la versión más reciente puede causar daños si las versiones son incompatibles. Recuerde verificar si la versión de VAX instalada en el servidor y la versión de actualización o migración de VAX son compatibles. También hay casos en los que las versiones del servidor SQL son incompatibles con otra versión de SQL. Recuerde leer atentamente las notas del instalador para obtener información al respecto, consulte la Guía del usuario o llame a nuestra línea de soporte para obtener ayuda al actualizar o migrar.

Sistemas operativos no admitidos y requisitos previos

El sistema VAX requiere una PC moderna que funcione como mínimo con Microsoft Windows 10, Microsoft Windows Server 2016. Se recomienda Windows 10/11 o Windows Server 2019 para un rendimiento óptimo. Por favor vea el Capítulo 1:

[Getting Started](#) y Capítulo 3:
[Initial Config](#)

para obtener una lista de los requisitos del sistema y los sistemas operativos compatibles.

Los sistemas operativos no compatibles o los dispositivos que no tienen todos los requisitos del sistema pueden ser incompatibles con VAX; considere actualizar a un dispositivo compatible. Use la herramienta "Acerca de su PC" en la configuración de Windows para encontrar las especificaciones de un dispositivo.

Herramienta de configuración

Ejecutar la herramienta de configuración de VAX permite realizar cambios en el sistema, eliminar un sistema y reparar un sistema. Si aparece un mensaje de error que indica que faltan archivos o se han perdido, la ejecución de una reparación puede encontrar y reemplazar algunos de los archivos perdidos. En algunos casos, eliminar y reinstalar VAX resolverá el problema. Es importante ejecutar una copia de seguridad antes de reparar o reinstalar para que haya una copia de la base de datos SQL. Al reinstalar/actualizar, 'pruebe' la ruta predeterminada para el servidor SQL o la ruta personalizada al servidor SQL antes de reinstalar o actualizar.

Solución de problemas del servidor SQL

Múltiples instancias de SQL pueden ejecutarse en una sola máquina. SQL Server 2008, 2012 y 2019 pueden ejecutarse simultáneamente en la misma máquina. Al instalar VAX, aparecerá un mensaje para instalar un servidor SQL si aún no está presente. Se recomienda el nombre y la ubicación predeterminados de esta carpeta. Si se configuran copias de seguridad periódicas después de la instalación y hay una base de datos perdida, se puede restaurar una copia de seguridad con la herramienta Administrador del sistema. Además, al reinstalar o actualizar, hay una opción para probar la ruta del servidor SQL para encontrar un servidor SQL existente.

 MSSQL15.VAX	2022-09-06 7:14 AM	File folder
 MSSQL15.VAX1	2022-11-28 9:56 AM	File folder

No se puede instalar/desinstalar VAX - Error 1316 La cuenta especificada ya existe

Causa: Esto suele deberse a claves de registro corruptas.

Solución: elimine VAX dentro de Regedit, luego instale 3.1 y elija "Reparar".

1. Abra el Editor del Registro.
2. Navegue a Computadora > HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node.
3. Busque Vicon.
4. Haga clic derecho en "Vicon" y Eliminar.
5. Descargue el archivo de instalación de VAX (se recomienda la misma versión).
6. Ejecute el instalador.
7. Siga las indicaciones. *Solo puede dar la opción de reparación. Seleccione Reparar si no hay opción para una nueva instalación*

Guía de instalación de Windows 11 SQL para unidades NVME

Al instalar SQL de cualquier versión en una máquina con Windows 11, existe la posibilidad de que la instalación no funcione en circunstancias normales. Esto se debe a que Microsoft ya no emula la configuración del sector del disco duro "PhysicalBytesPerSectorForAtomity" como 4096 (4kb).

Es un problema conocido con las unidades NVME que ya no emulará esto y en su lugar lo establecerá en lo que el fabricante tenga a bordo, en algunos casos 16kb-32kb. Hay dos formas de manejar esto:

1. Bajar a Windows 10
2. Ejecute los siguientes comandos en una ventana elevada del símbolo del sistema para forzar un nivel de registro de emulación de 4 kb
 - REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\stornvme\Parameters\Device" /v "ForcedPhysicalSectorSizeInBytes" /t REG_MULTI_SZ /d "*" 4095" /f
 - REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\stornvme\Parameters\Device" /v "ForcedPhysicalSectorSizeInBytes" /t REG_MULTI_SZ /d "*" 4095" /f

Ejecute este comando también en el símbolo del sistema para verificar qué se está ejecutando actualmente; se requiere reiniciar para que esto surta efecto visual y funcionalmente.

- “fsutil fsinfo sectorinfo C:”

La respuesta debe ser 4096 o inferior después de ejecutar esos comandos. Source:

<Source> <https://docs.microsoft.com/en-us/troubleshoot/sql/admin/troubleshoot-os-4kb-disk-sector-size></Source>

Moving VAX to a New Computer

Mover VAX a una computadora nueva puede ser muy simple. Los pasos importantes a tener en cuenta son los siguientes:

- Método de migraciones de bases de datos
- Ubicación de la red
- Modo de conexión
- Reinicio de licencia

El método de migración de la base de datos se refiere a cómo se moverá la información de la base de datos. El movimiento entre implementaciones locales se puede realizar a través de la utilidad de migración de datos o la opción de copia de seguridad/restauración del administrador del sistema.

1. La herramienta Data Migrator toma los datos de las particiones y los exporta como un archivo YAML. Este archivo se puede importar a otra instancia de VAX.
 - **Migrador de data no exporta Notificaciones, Registros, Imágenes de perfil, Plantillas, Mapas, Administradores, Sitio y Áreas
2. Copia de seguridad/restauración del administrador del sistema realiza una base de datos del sistema completo. Esto luego se puede restaurar en un nuevo sistema VAX.
3. **Los sonidos y los registros del sistema no se transfieren
4. **Las soluciones alojadas solo se pueden transferir mediante la utilidad Migrador de data.

La ubicación de la red se refiere a si el nuevo servidor está en la misma red que el antiguo. Estos son factores importantes, ya que es posible que los Paneles no puedan conectarse si está en una red diferente, o los Administradores no podrán acceder desde sus dispositivos.

El modo de conexión es la forma en que los usuarios y los paneles se conectan al servidor. Si el servidor usa una dirección IP, puede ser tan simple como configurar el nuevo servidor en la dirección IP anterior (asegúrese de que esto no genere un conflicto de IP). El nombre del servidor será diferente, ya que esto podría ser una cuestión de cambiar la resolución de nombre del servidor DNS.

Reinicio de licencia. Será necesario volver a armar la licencia para asociarla con la nueva computadora.

Alternar I-Frames en VAX

En algunos casos, es posible que sea necesario mejorar la seguridad de I-Frame de VAX. Consulte la siguiente guía para alternar una mejora de configuración de I-Frame. En las versiones 3.0.1.26 y posteriores, esta configuración ya está habilitada. Para alternar esta configuración, siga estos pasos para editar el archivo Appsettings. Tenga en cuenta que cambiar la siguiente configuración a falso habilitará la configuración; cambiar a verdadero desactivará la configuración de I-Frame.

1. Comience abriendo la unidad C: en el Explorador de archivos
2. Navegue a Archivos de programa (x86)
3. Navegue a las carpetas VAX
4. Navegue a la carpeta WebServer
5. . Busque el archivo llamado appsettings y ábralo en el Bloc de notas (Ejecute el Bloc de notas como administrador; esto puede requerir que abra el Bloc de notas como administrador primero, luego use File > Open File y abra el archivo Appsettings)
6. Desplácese hacia abajo hasta la parte inferior del código donde verá el bloque de código Autenticación en la parte inferior del bloque principal de Autenticación; busque:
"CookieSameSitePolicy": "Lax"
7. Cree una nueva línea y agregue esta línea: "AllowIFrames": false
8. Además, deberá agregar una coma al final de la línea anterior: "CookieSameSitePolicy":
"Lax",

La parte inferior del archivo de configuración de la aplicación (desde la sección Autenticación hacia abajo) debería verse así:

```
"Authentication": {  
  
  "MaxPasswordAttemptLockoutTime":  
  10,  
  
  "MaxPasswordAttempts": 5,  
  
  "UniquePINByPartition": false,  
  
  "MobileCredentialSiteCode":  
  61000,  
  
  "SlidingSessionExpiryInMinutes":  
  600, "CrossOriginURLs": [],  
  
  "CookieSameSitePolicy": "Lax",  
  
  "AllowIFrames": false  
},  
  
"AllowedHosts": "**"  
}
```

Nota:

Es posible que deba ejecutar el Bloc de notas como administrador antes de abrir Appsettings. Para hacer esto, debe abrir el Bloc de notas escribiendo Bloc de notas en la búsqueda de Windows o encontrando su ícono en el menú Inicio y haga clic con el botón derecho para Ejecutar como administrador. Luego use File > Open File en el Bloc de notas para navegar hasta el archivo Appsettings. Una vez que esté dentro de la carpeta correcta, es posible que deba cambiar el tipo de archivo que se muestra a Todos los archivos en lugar de solo .txt. Haga clic en el archivo appsettings para abrir. En este punto, consulte la sección anterior para realizar los cambios necesarios.

Figura 43.2.

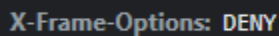
```

"Authentication": {
  "MaxPasswordAttemptLockoutTime": 10,
  "MaxPasswordAttempts": 5,
  "UniquePINByPartition": false,
  "MobileCredentialSiteCode": 61000,
  "SlidingSessionExpiryInMinutes": 600,
  "CrossOriginURLs": [],
  "CookieSameSitePolicy": "Lax",
  "AllowIframes": false
},
"AllowedHosts": "*"
}

```

Esta configuración debe establecerse en falso si desea protegerse de las vulnerabilidades. Si desea deshabilitar esta función de seguridad, reemplace "AllowIFrames": falso con "AllowIFrames": verdadero. De forma predeterminada, esta configuración se establece en falso y se puede observar en las herramientas de desarrollo de VAX. Para ver el estado, ingrese las herramientas para desarrolladores en una página con VAX abierto y navegue hasta la pestaña Red y la pestaña Encabezado. En Encabezado de respuesta, observe Opciones de marco I: DENEGAR. Esto indica que el software está protegiendo contra las vulnerabilidades de I-Frame.

Figura 43.3.



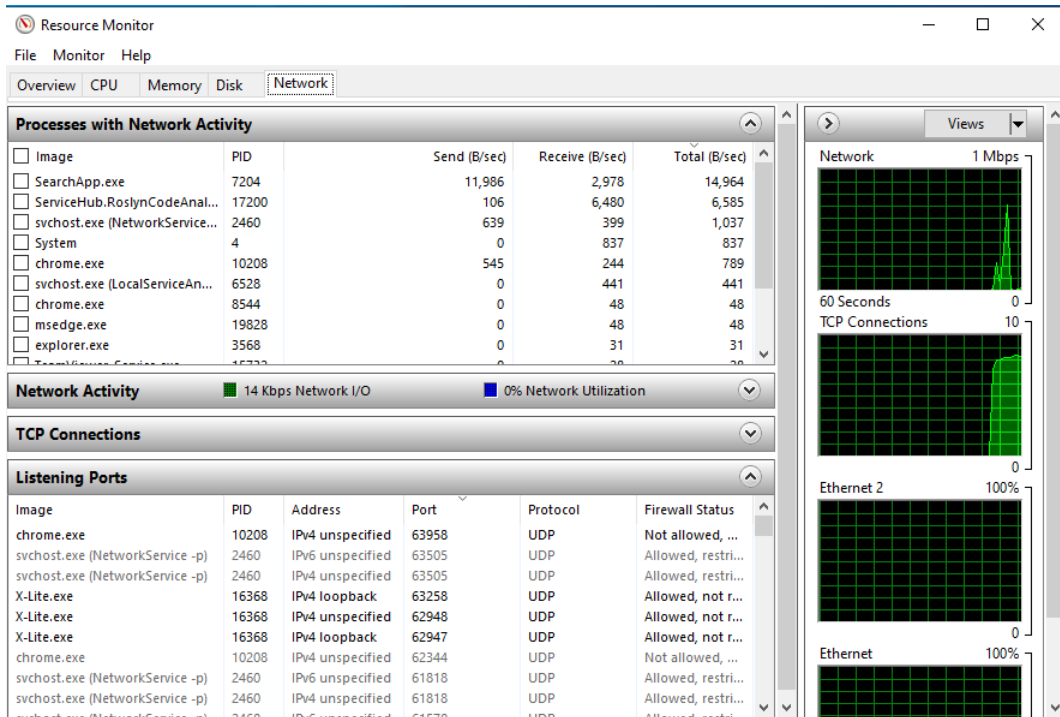
X-Frame-Options: DENY

Solución de problemas de comunicación

Un panel puede desconectarse y permanecer desconectado por una amplia variedad de razones, desde el lado del servidor hasta el lado del panel y todo lo demás. Esta guía ayudará a proporcionar información sobre dónde comenzar a solucionar problemas de conectividad..

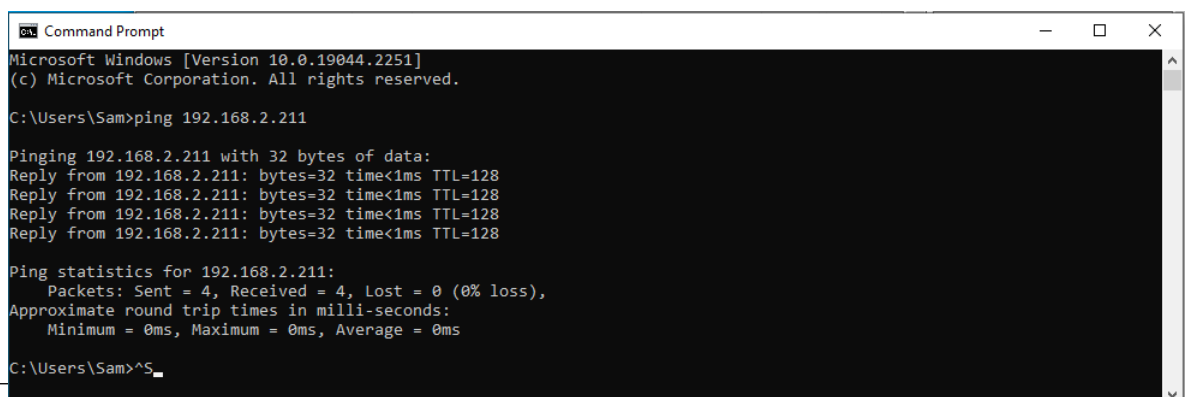
Diagnóstico del servidor

1. Compruebe si la dirección IP del servidor es correcta. Dentro de VAX, verifique si el campo Dirección del servidor (que se encuentra en Configuración del sistema) es consistente con la dirección IP real del servidor. Los paneles inician la comunicación con el servidor y, por lo tanto, buscarán una dirección de servidor definida, que debe resolverse en la máquina donde está alojado VAX.
2. Compruebe si los puertos están desbloqueados o en uso (Estado del cortafuegos y Monitor de recursos). Los cortafuegos como McAfee son culpables comunes cuando se requiere desbloquear los puertos manualmente a través de su interfaz. Además, otro proceso puede estar utilizando los puertos utilizados por VAX. Resource Monitor es una herramienta útil para comprobar rápidamente si los puertos están ocupados o bloqueados.



Diagnóstico del panel

- Comience por verificar si el Panel ha obtenido una dirección IP. De forma predeterminada, los paneles buscan adquirir una dirección DHCP, y esta dirección se puede ver en la pantalla LCD de cada panel en el menú desplegable.
Para cambiar el panel para que tenga una dirección IP estática, consulte "Establecer información de IP del panel" en las preguntas frecuentes. También se puede ver en el menú de sólo lectura:
 - Mantenga presionado el botón ESC en el Panel (SW4)
 - Una vez en el menú de solo lectura, navegue a la opción 6: Dirección IP real usando los botones SW1 y SW2
- Desde el servidor o una máquina local, compruebe si se puede acceder a la dirección IP del paso anterior mediante un ping o un navegador web. Todos los paneles, excepto el ascensor POE, tienen una interfaz web a la que se puede acceder mediante un navegador web.
- Si no está disponible, verifique la integridad de los cables y dispositivos de la red. Esto se puede probar utilizando otro dispositivo, como una computadora portátil u otro dispositivo, o intercambiando los componentes con otros cables o dispositivos de red (es decir, cambiando del conmutador POE al inyector POE).
- Compruebe si el conmutador o dispositivo al que está conectado el panel es un conmutador gestionado o no gestionado. Vicon Panels no aceptará información de etiquetado de VLAN.



No puede conectar a VAX

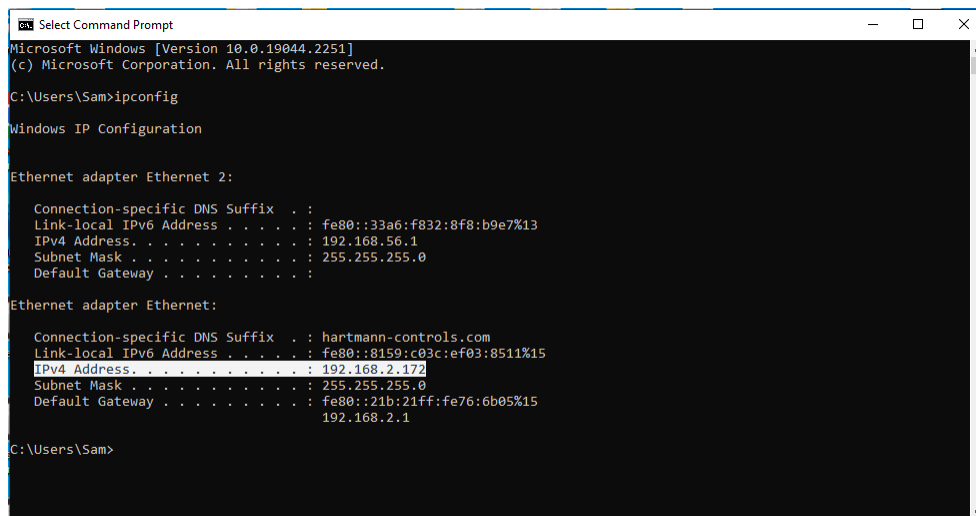
VAX requiere HTTPS:// para conectarse al servidor. El siguiente paso es ver cómo se conecta el usuario.

- ¿Están utilizando una dirección IP?
- ¿Nombre de la computadora/DNS?
- * Debe coincidir con el método realizado en la configuración inicial *

Si el administrador está utilizando el método de navegación correcto (IP o nombre del servidor) para conectarse, verifique la configuración del servidor para asegurarse de que la dirección IP configurada en "Dirección del servidor" coincida con la dirección IP de la computadora. Esto se puede cruzar abriendo un indicador de CMD e ingresando 'ipconfig' para comparar las direcciones IPv4.

Si la dirección del servidor y la dirección de la computadora coinciden y el navegador aún tiene problemas, esto puede deberse a un error de red. Verifique la conectividad haciendo ping al servidor remoto desde la computadora. Una falla de ping puede determinar si se puede acceder al servidor desde el host. Para hacer ping, abra un indicador de CMD e ingrese 'ping' y la dirección IPv4 del servidor o el nombre del servidor (es decir, ping 192.168.2.172). Si se agota el tiempo de espera de la solicitud de ping, no se puede acceder al servidor. Si se devuelve el ping, hay una conexión..

*** IMPORTANTE *** La falla del ping no siempre determina los errores de conectividad, ya que una configuración de firewall en la máquina del servidor puede rechazar las solicitudes ICMP (ping). Intente hacer ping desde el servidor a la computadora host, o intente hacer ping al enrutador desde el servidor y la computadora host.



```

Select Command Prompt
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sam>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::33a6:f832:8f8:b9e7%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : hartmann-controls.com
    Link-local IPv6 Address . . . . . : fe80::8159:c03c:ef03:8511%15
    IPv4 Address. . . . . : 192.168.2.172
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::21b:21ff:fe76:6b05%15
                                192.168.2.1

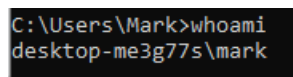
C:\Users\Sam>
  
```

VAX se niega a conectarse

Una de las razones más comunes por las que esto ocurre es debido a un error de migración de datos. El error se puede observar en los registros de la aplicación. Por lo general, System Manager y el servidor SQL aún se ejecutarán correctamente. Sin embargo, el servidor web VAX no puede ubicar el servidor SQL y, debido a que no puede acceder a él, el servidor web no se ejecutará. Puede permanecer activo y seguir funcionando durante unos minutos, pero finalmente se detendrá.

Para remediar este problema, realice las siguientes acciones.

Figura 43.4. whoami



```

Select Command Prompt
C:\Users\Mark>whoami
desktop-me3g77s\mark
  
```

1. 1. Abra CMD y escriba "whoami"
2. 2. A continuación, dentro del CMD, intente acceder al servidor ingresando los siguientes comandos:
 - a. sqlcmd -S .\VAX
 - b. Use VAX
 - c. Go
3. Una vez que se confirme el acceso, verifique el archivo appsettings.json/VAX.exe.conf. Cambie la siguiente línea para reflejar a continuación:
 - a. ...Data Source=.\VAX;...
4. 4. Luego verifique el Registro para verificar el registro del instalador y, si está lleno, límpielo.

VAX obtiene tiempo de espera de conexión a la base de datos (3.0+)

1. Abra appsettings.json
2. Modifique la cadena de conexión de la base de datos y agregue un nuevo elemento al final para que se vea así:

```
"MainDatabaseContext": "Data Source=.\VAX;Initial Catalog=VAX;Integrated Security=True;Connection Timeout=600"
```

3. Guardar y reiniciar el servicio
Si usa varios arrendatarios, se debe agregar el tiempo de espera de conexión a la cadena de conexión de cada arrendatario.

Triple deslizamiento no funciona en lectores de tarjetas

El deslizamiento triple es una función útil que permite la programación con lectores de tarjetas para realizar funciones específicas. Las razones comunes por las que el deslizamiento triple no funciona son las siguientes:

- Configuración: El triple deslizamiento debe estar habilitado en el lector de tarjetas y en la cuenta de usuario.
- Para usar el deslizamiento triple con un lector de tarjetas SOLAMENTE, toque 3 veces con el lector de tarjetas.
- Para teclados, toque 3 veces O ingrese el PIN y luego presione # 3 veces para simular tocar 3 veces (es decir, 1 2 3 4 # # #).
- Los teclados tienen más opciones, después de "deslizar" tres veces, presione inmediatamente la tecla deseada y luego presione #. hay un tiempo de espera.

Periféricos de entrada, salida y salida

Los periféricos de salida pueden incluir, entre otros,:

- Cerraduras de puerta
- Cerraduras magnéticas
- Abridores de puertas

- Torniquetes
- Relés Externos
- Sirenas
- Luces estroboscópicas
- Abridores Automáticos
- Sistemas de alarma/intrusión
- PLC Ascensor
- Entrada de PLC genérica
- Entrada de contacto seco en otro panel o panel de terceros

Las entradas y salidas pueden no funcionar según lo previsto. En algunos casos, las Entradas y Salidas controlan una función de la puerta. Un sistema de alarma que se supone que debe sonar no lo hace. En esta situación, la solución de problemas de entrada y salida puede resolver el problema. Al solucionar problemas, a menudo la conclusión es una de las siguientes:

- El cableado es incorrecto o está dañado (los puntos de falla también incluyen terminaciones de cables, empalmes/conectores B)
- El dispositivo en sí está dañado
- El dispositivo de salida requiere más potencia o voltaje de lo que permiten las especificaciones del panel
- La entrada/salida no está configurada para la función correcta (Salida 1-1, Salida 1-2)
- La entrada/salida está configurada incorrectamente (normalmente abierta/normalmente cerrada)
- Entrada o salida defectuosa

Identificar el problema de la entrada/salida requerirá un proceso de eliminación. Para dividir el problema en múltiples partes y verificar la funcionalidad de las partes individuales del sistema para finalmente descubrir qué parte es el problema. Estas piezas generalmente se pueden dividir en estas partes:

- La propia puerta/controlador IO
- El cableado hacia/desde el dispositivo
- El dispositivo de entrada/salida (golpe de puerta, contacto de puerta, botón de salida, etc.)
- La configuración del software

Solución de problemas de entrada, salida y periféricos

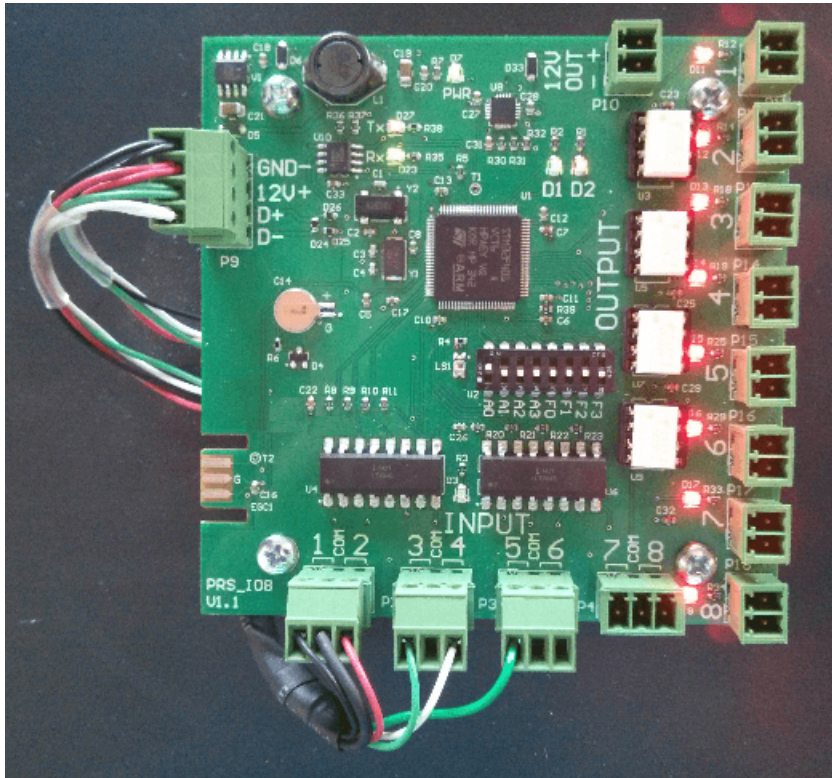
1. Es importante saber qué salidas de los paneles requieren una fuente de alimentación externa. Por favor vea el Capítulo 7

<Output_troubleshooting>Panel Setup</Output_troubleshooting>

En algunos casos, la salida requiere una fuente de alimentación externa; el Panel no proporcionará energía. Es importante saber cuánta energía usa la salida y si el POE puede suministrar suficiente energía.

- Los relés húmedos VAX-EXP-2D y VAX-1D-1 (bloqueo de potencia 1, bloqueo de potencia 2) están limitados a 550 mA a 12 VCC
 - Los relés de estado sólido VAX-EXP-2D y VAX-1D-1 (salida 2,3,5,6) están limitados a conmutar 24 VCC 1A
 - Los relés VAX-IO-EXP8-PCB están limitados a conmutar 30 VCC 500 mA
2. Las entradas en todos los controladores son de contacto seco. Cuando el Panel ve un cierre a tierra del pin de señal, considera que la entrada está activa.
 3. Si una salida no funciona, primero verifique el hardware físico de la salida. Si la cerradura de la puerta está siendo alimentada desde lockpower, use un multímetro en el panel para verificar si la cerradura está recibiendo voltaje y para verificar el estado del LED ámbar. Si hay un cortocircuito en la cerradura de la puerta o en el cable, el LED ámbar se apagará. Mida el voltaje en la salida de energía de la cerradura mientras la cerradura está conectada (invalítela para desbloquearla desde el software o utilice una prueba de salida en la pantalla LCD del panel) y mientras el bloque de cabecera está desconectado.
 4. Si la cerradura de la puerta recibe alimentación externa, retire el bloque de cabecera del relé y cambie el multímetro al modo de resistencia o conductividad y mida el relé mientras está encendido y apagado. Si no hay conductividad, el relé está dañado. Si hay conductividad, el siguiente paso sería sacar los cables del bloque de cabecera y cortocircuitarlos (para simular el relé). Si la huelga se dispara, implica que el problema es el relé (verifique las especificaciones de la huelga, ya que esto implica que la huelga dañó el relé con demasiado voltaje o demasiada corriente). Si parece estar bien, pruebe con un relé de repuesto (si está disponible) o cambie a un relé externo.
 5. Quitar los cables del relé del panel y conectarlos juntos verificará si los relés no funcionan. Si el dispositivo (cerradura, cerradura magnética, abridor automático) no funciona después de hacer un cortocircuito, entonces es el cableado, el dispositivo periférico en sí o la fuente de alimentación.
 6. Para medir el voltaje (o la conductividad) en el dispositivo mismo o descartar el cableado, desmonte la cerradura de la puerta o el cerrojo magnético y lleve el dispositivo directamente al Panel con un cable corto. Si funciona conectado directamente al Panel pero no con el cable más largo, entonces es probable que sea el cable. Un técnico debería poder verificar esto con un probador de cables o retorciendo un extremo del cableado, haciendo un corto y luego haciendo una prueba de conductividad con un multímetro..
 7. Verifique que el hardware y el panel funcionen antes de iniciar sesión en el software para verificar la configuración del relé, qué puerta está asociada, los temporizadores de las puertas, etc. Si la anulación de la puerta funciona pero la lectura de la tarjeta no; compruebe los temporizadores de la puerta en caso de que se haya configurado un temporizador de desbloqueo de 200 ms. Verifique si la Entrada/Salida está anulada en la Descripción general del sistema, desactivada o en la entrada/salida incorrecta en la configuración de E/S del panel.
 8. De manera similar, con una entrada, si la prueba de entrada (a través del panel LCD) funciona pero la acción (como desbloquear la puerta) no funciona, esto indica que la atención debe cambiar a la configuración de entrada en el software. . Si la entrada del Panel es funcional, entonces es hora de descartar el dispositivo o el cableado.

Figura 43.5.

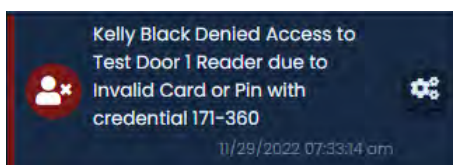


Solución de problemas de acceso denegado

Cuando las tarjetas y el PIN están configurados incorrectamente, normalmente falta un componente. Algunas de estas causas comunes son:

- Grupos de acceso: los usuarios pueden ubicarse en un grupo de privilegios de acceso diferente.
- Partición: Es posible que el Panel de la puerta se haya agregado a una partición diferente.
- Horarios: Los Horarios configurados en la puerta o grupo de acceso pueden estar negando el acceso en los horarios especificados. (Los horarios de usuario se aplican a lectores específicos dentro de un grupo de acceso).
- Horarios de puerta: los horarios de puerta se aplican a la puerta real. Un problema común puede ser usar un PIN en una puerta con acceso solo con tarjeta.
- La puerta/piso o las entradas/salidas conectadas pueden anularse. Verifique el resumen del sistema para el estado de la puerta/piso/entrada/salida.

Figura 43.6. Acceso denegado



¿Funcionarán mis tarjetas existentes con VAX?

Las tarjetas pueden variar de todo tipo de formatos de bits. Por ejemplo, las tarjetas Proxyll se pueden programar con cualquier cosa hasta 85 bits. Algunas cosas a comprobar para ver si es compatible:

1. ¿Pueden los lectores “leer” la tarjeta? ¿Hay un pitido?
2. ¿Qué ve VAX en la tarjeta? ¿La salida se muestra como se esperaba?
3. Algunos de los problemas anteriores también pueden deberse a un cableado incorrecto del lector de tarjetas, así que asegúrese de que el lector pueda escanear una tarjeta existente que se sabe que funciona con el sistema.
4. Realice una prueba de lectura y anote el formato de bit y el número de tarjeta. Compare esto con una prueba de lector de la misma credencial en otro lector.

Teclado no envía PINs

VAX requiere un modo de ráfaga de 8 bits para poder leer los PIN correctamente.

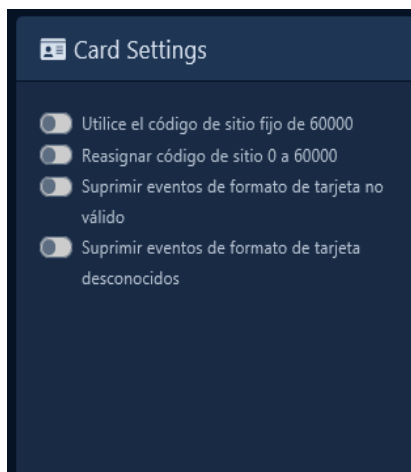
- En un Rosslare (AYC-Q65), realice las siguientes acciones:
- Ingrese al modo de programación (###) (a veces, mantener presionado # durante 4 segundos funciona)
- Introducir código de programación (1 2 3 4)
- Entrar en el menú 1 (1)
- Seleccione la Opción 3 (3), que es Wiegand Nibbles de 8 bits Complementada

Lista de posibles razones para el acceso denegado

- Una actualización de los paneles
 - Zona horaria incorrecta
 - Sin privilegios
 - Tarjeta no válida
 - Fecha de inicio de trabajo no válida
 - Fecha de fin de trabajo no válida
 - PIN esperado
 - PIN incorrecto
 - Nivel de seguridad no válido
 - Formato de tarjeta no válido
 - No en el grupo de privilegios de acceso
 - Niveles de autenticación
 - Invalidar
 - Evento de ejecución única
 - Día festivo
 - Zona horaria de la puerta
 - Zona horaria del usuario
 - Modo de crisis habilitado
 - Zona horaria configurada en modo tarjeta al ingresar un PIN
 - Los teclados Rosslare no admiten PIN superiores a 50999
-
- Si ve un error con 1 bit, vaya a Formatos de tarjeta en el Panel de edición y cambie Suprimir formato de tarjeta no válido y Suprimir eventos de formato de tarjeta desconocido.

- Si los códigos de sitio no funcionan, anule el código de sitio en Formatos de tarjeta en el Panel de edición y cambie Usar código de sitio fijo de 60000. Luego, cambie la credencial de cada usuario al código de sitio 60000.

Figura 43.7. Formatos de tarjetas



Tipos de acceso denegado

Tabla 43.1. Tipos de acceso denegado

Error	Descripción
Credencial inválida	Acceso denegado a la puerta porque el tipo de credencial no es válido para Reader.
Tarjeta o PIN no válido	Acceso denegado a la puerta porque el PIN o la credencial de la tarjeta no son válidos.
Zona horaria no válida	Acceso denegado a la puerta porque APG o Credencial no es válida para la zona horaria configurada actualmente.
Nivel de crisis no válido	Acceso denegado a la puerta porque el acceso al nivel de crisis está por debajo del nivel de crisis establecido actualmente.
Fecha de inicio no válida	Acceso denegado a la puerta porque la fecha actual no está dentro de la Fecha de inicio y la Fecha de finalización de la credencial.
Fecha de finalización no válida	Acceso denegado a la puerta porque la fecha actual no está dentro de la Fecha de inicio y la Fecha de finalización de la credencial.
APB no válido	Acceso denegado a la puerta porque la configuración de Anti-Passback muestra que el usuario ya está dentro del área.
Acceso no válido: Mantrap	Acceso denegado a la puerta porque la configuración de Mantrap muestra que la puerta 1 todavía está abierta antes de abrir la puerta 2.

Solución de problemas del lector

Resumen de posibles problemas

- El lector no responde (pitido, parpadeo) a una credencial
- El lector no se enciende

- El lector sigue sonando
- El número de tarjeta no coincide con lo esperado
- La presentación de la credencial muestra Formato de tarjeta desconocido dentro del software
- El lector responde a la credencial pero no a la notificación en el software
- Algunas credenciales abren la puerta pero otras no

Metodología de solución de problemas

La solución de problemas del lector puede ser un proceso similar a la solución de problemas de entradas/salidas; divida el problema en partes fácilmente comprobables para reducir el problema. Dependiendo del problema, puede o no ser fácilmente divisible.

El lector no responde a las credenciales

Sintoma(s)

- La persona presenta las credenciales de RFID a un lector, pero el lector no emite un pitido, parpadea ni responde. No aparece nada en el software.

Posibles Causas

- Desajuste entre la frecuencia del lector y la frecuencia de la tarjeta (como probar una tarjeta de 125 khz en un lector de tarjetas inteligentes)
- El lector no tiene suficiente voltaje/corriente (no común)
- (Solo tarjeta inteligente) Faltan claves de cifrado
- (Solo tarjeta inteligente) Lector no configurado para admitir tecnología específica (el lector puede responder a DESfire EV2 pero no a MIFARE Classic)

Información adicional

- Intente encontrar el modelo del lector, generalmente ubicado en la parte posterior, para verificar qué tecnología RFID admite
- Trate de encontrar la caja de donde vino la tarjeta para identificar la frecuencia.

Las frecuencias y tipos típicos incluyen:

- HID 125KHz
- AWID 125KHz
- EM 125KHz
- INDALA 125KHz
- IOPROX 125KHz
- 433MHZ UHF (WRR22, WRR44, etc)
- 902 to 928 MHz (UHF readers like Specre, LR-3000)
- 13.56MHz (ICLASS, ICLASS SEOS, MIFARE CLASSIC, MIFARE Desfire EV1/EV2/EV3)

El lector no se enciende

Sintomas:

- El lector no muestra ningún LED ni emite pitidos de inicio
- Es posible que el lector esté en un ciclo de encendido, lo que haría que emitiera pitidos de inicio cada cierto tiempo.

Posibles Causas:

- Voltaje o corriente insuficiente
- Corto a través de GND y POWER
- Alimentación no conectada (cable dañado, cableado incorrecto, conector B defectuoso, etc.)
- Lector dañado

Información adicional:

- Obtener el modelo del lector para consultar los requerimientos actuales. VAX-1D-1 tiene 500mA disponibles para lectores. VAX-EXP-2D tiene hasta 700 mA disponibles para lectores.
- Mida el voltaje que sale del puerto del lector en el lado del panel. No habrá voltaje si hay un corto o sobre corriente. Desconecte los lectores y vea si vuelve el voltaje.
- Medir la tensión en el propio lector (implica tener que desmontar parcialmente el lector de la pared).
- Si se sospecha de un exceso de corriente, conecte el lector a una fuente de alimentación alternativa de 12 V, como la conexión del bloque de cabecera inferior en las tiras de interconexión, una fuente de alimentación externa de 12 V CC o incluso una batería de 12 V CC.
- Conecte el lector directamente al Panel para descartar el cableado si no se dispone de un multímetro.

El lector está pitiendo erróneamente

Sintoma(s):

- El lector emite un pitido continuo (es decir, 'beeeee...')
- El lector emite varios pitidos seguidos (es decir, 'bip bip bip...')
- El lector emite pitidos continuamente, pero solo cuando la puerta está desbloqueada

Posibles Causas:

- Se puede producir un pitido continuo cuando la línea Buzz tiene un cortocircuito a tierra o si solo suena cuando la puerta está desbloqueada; Es probable que la línea de zumbido y LED se mezclen
- La puerta está abierta a la fuerza o se mantiene abierta

Información adicional:

- Para descartar que el propio lector decida emitir un pitido, desconecte el cable de zumbador del lado del panel para descartar que sea el panel el que le dice al lector que emita un pitido.

El número de tarjeta no coincide con el número esperado

Sintoma(s):

- El usuario presenta su credencial al lector, pero el número que se muestra en la pantalla LCD o el panel no coincide con el número de tarjeta esperado
- La credencial muestra un número de tarjeta correctamente en un lector, incorrectamente en otro.

Posibles Causas:

- Las líneas de datos (D1, D0) están al revés (Wiegand de 26 bits al revés mostrará 0-0; otras longitudes de bits solo mostrarán el número de tarjeta incorrecto)
- La configuración del formato de la tarjeta no coincide con el formato de la credencial. Realice una prueba de lector para verificar la longitud de bits e intente cambiar la configuración de longitud de bits aplicable en la pestaña Formatos de tarjeta del Panel de edición o Editar sitio
- Si la longitud de bits es de 32 bits, esto puede indicar que un lector de tarjetas inteligentes no pudo acceder al número de tarjeta cifrada y, en su lugar, leyó el CSN de la credencial.

Información adicional:

- Cuando los lectores de tarjetas inteligentes leen el CSN de una tarjeta, el propio lector (HID o STid) puede programarse para generar el CSN de una manera diferente. Entonces, un lector puede leerlo como se espera, mientras que el otro no.

El software muestra un formato de tarjeta desconocido al presentar la credencial

Sintoma(s):

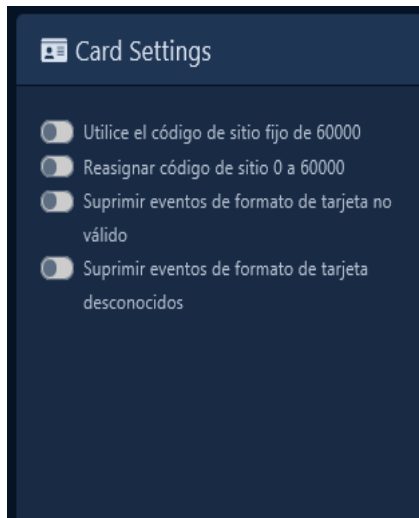
- El usuario presenta su credencial al lector pero el software muestra uno o más Formato de Tarjeta Desconocido, número de bits x
- Sin presentar credencial, el software muestra Formato de Tarjeta Desconocido, número de bits 1 o 2.

Posibles Causas:

- Una de las líneas de datos no está conectada (D1 o D0 desconectados devolverán varias notificaciones de formato de tarjeta desconocido de varias longitudes)
- EMF/EMI está causando que se envíen datos incorrectos al panel o podría estar afectando potencialmente la señal
- Se utilizó un cable incorrecto (sin blindaje o sin conexión a tierra del blindaje)
- Manipulación del lector (algunos lectores como STid escupirá un montón de bits individuales de la manipulación está activa)

Información adicional:

- Puede haber un cable incorrecto; use la configuración de muestreo del lector directamente en la pantalla LCD o en la pestaña Lector de la pantalla Editar puerta (el modo de muestreo LCD es un cambio temporal, pruebe todas las configuraciones; una vez que una configuración funcione, configure ese tipo en el software)



El lector responde a la credencial pero no a la notificación en el Software

Sintoma(s):

- El usuario presenta su credencial al lector y el lector responde, pero el software o la pantalla LCD no muestran ningún número de tarjeta ni mensajes relacionados.

Posibles Causas:

- Líneas de datos ambas completamente desconectadas
- VAX-EXP-2D no se comunica con VAX-MDK (podrían ser interruptores DIP o software no configurado con la cantidad correcta de expansores)
- No se ha agregado ninguna puerta al controlador (se puede descartar con Reader Test en LCD)
- La configuración de notificaciones tiene una regla en tiempo real establecida para no mostrar los eventos del lector (se puede descartar con la prueba del lector en la pantalla LCD)

Información adicional:

- Si un lector está en el modo de prueba del lector, no habrá notificaciones ni registros de lecturas de tarjetas hasta que vuelva a su estado normal.

Lectores y configuración

Para la configuración de HID Reader, consulte los siguientes recursos:

<https://configure.hidglobal.com/configure/configure>

Wiegand Keypad - 8-bit {Dorado}

<figures>

</figures>



Lectura de tarjeta incorrecta

Algunos problemas comunes de por qué las tarjetas se leen pero aparecen incorrectamente en nuestro software:

- Formato de bit incorrecto en VAX. Se puede cambiar dentro del software o se pueden enviar algunas tarjetas de muestra e intentaremos descifrarlas.
- Las líneas de datos están al revés. Cambiarlos puede solucionarlo.
- Las versiones anteriores del software no admitían números de tarjeta largos. Soporte agregado de la versión 2.10.18.

Lectores de tarjetas que se apagan intermitentemente en un panel VAX-MDK

Un Panel VAX-MDK con 3 módulos, 6 puertos y 6 lectores conectados. Algunos lectores se apagan intermitentemente y cuando están encendidos, transmiten identificaciones distorsionadas al servidor. El cableado es correcto, calibre 22 con una longitud máxima de 75 pies. Se transmite energía, las lecturas de voltaje son correctas.

El problema fue con la interferencia en la línea. Cambiar el modo de muestreo en los lectores solucionó el problema.

Problemas de cableado

Las ráfagas de acceso denegado con números de bits cortos son típicas de problemas de interferencia o conexión a tierra.

El lector está leyendo la tarjeta, pero regresar con un 0-0 o un formato de tarjeta impar diferente es típico de un orden incorrecto de los cables del lector blanco y verde.

Algunos cables Cat6/Cat5e funcionarán, pero en algunos casos los cables de par trenzado no están protegidos entre sí. Además, no use par trenzado (verde y blanco/verde para líneas de datos (D1 D0)). La distancia del panel al lector debe ser de un máximo de 500 pies desde el panel al lector cuando se instala correctamente con el cable correcto.

Especificaciones de energía

Lectores:

- VAX-1D-1 lector - 500mA / por puerto
- VAX-2D-1 lector 350mA / por puerto (700mA/per VAX-EXP-2D)
- 26 bit estándar / 125 khz frecuencia
- 8 bit ráfaga para teclado

Salidas:

- VAX-2D-1 Salida 12V, 500mA @ 12VDC (compartido con los puertos del lector)
- VAX-EXP-2D Salida 12V, 350mA @ 12VDC (compartido con los puertos del lector)
- VAX-EXP-2D / VAX-1D-1 relés húmedos (lvoltaje de cerradura 1,4) = 500mA @ 12VDC
- VAX-EXP-2D / VAX-1D-1 Relés de estado sólido (salida 2,3,5,6) conmutación 1A @ 24VDC
- VAX-IO-EXP8-PCB relés de conmutación 500mA @ 30VDC