



TruPortal™

GUÍA DEL USUARIO DEL SOFTWARE

Interlogix® TruPortal™ Software Guía del Usuario, versión del producto 1.5. Esta guía es el ítem número 461047001A, de fecha 25 de Julio, 2013.

Copyright

© 2013 United Technologies Corporation.

Interlogix es parte de UTC Climate Controls & Security, una subsidiaria de United Technologies Corporation. Todos los derechos reservados.

Marcas registradas y patentes

Los nombres Interlogix, TruPortal, TruVision, y sus logos son marcas registradas de United Technologies Corporation. Microsoft, Internet Explorer, y Windows, son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países. Apple, iPad, iPhone, y iTunes son marcas registradas de Apple Inc. Android es una marca registrada de Google, Inc. Otros nombres comerciales usados en este documento pueden ser marcas comerciales o marcas registradas de los fabricantes o distribuidores de los productos respectivos.

Fabricante

Interlogix
3211 Progress Drive, Lincolnton, NC 28092, EE.UU.
Representante autorizado de fabricación en la UE:
UTC Climate, Controls & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Países Bajos

Versión

Este documento se aplica a la versión 1.5 de TruPortal.

Certificación



Conformidad FCC

Este dispositivo cumple con la parte 15 de las Normas de la FCC. La operación está sujeta a las siguientes condiciones: (1) Este dispositivo no puede causar interferencias perjudiciales y (2) este dispositivo debe aceptar cualquier interferencia que reciba, incluidas interferencias que puedan causar un funcionamiento no deseado.

Clase A: Se ha comprobado que este equipo cumple los límites para dispositivos digitales de clase A, de acuerdo con la parte 15 de las Normas de la FCC. Estos límites han sido establecidos para proporcionar una protección razonable contra interferencias perjudiciales cuando el equipo funciona en un entorno comercial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con el manual de instrucciones, puede causar interferencias perjudiciales en las comunicaciones de radio. El funcionamiento de este equipo en un área residencial puede causar interferencias perjudiciales, en cuyo caso el usuario deberá corregir la interferencia por sus propios medios.

Clase B: Se ha comprobado que este equipo cumple los límites para dispositivos digitales de clase B, de acuerdo con la parte 15 de las Normas de la FCC. Estos límites han sido establecidos para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con las instrucciones, puede causar interferencias perjudiciales en las comunicaciones de radio.

No hay garantía de que no se produzcan interferencias en una instalación particular. Si este equipo causa interferencias perjudiciales en la recepción de radio o televisión, lo cual puede determinarse apagando y prendiendo el equipo, se recomienda al usuario que intente corregir la interferencia tomando las siguientes medidas:

- Reorientar o re-colocar la antena de recepción.
- Aumentar la distancia entre el equipo y el receptor.
- Conectar el equipo a una toma corriente de un circuito diferente al que está conectado el receptor.
- Consultar al distribuidor o técnico de radio/TV para obtener ayuda.

Conformidad con ACMA

¡Aviso! Este es un producto clase A. En un entorno doméstico este producto puede causar interferencias de radio, en cuyo caso el usuario deberá tomar las medidas adecuadas.

Canadá

Este aparato digital clase A cumple con la norma canadiense ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

Directivas de la Unión Europea

12004/108/CE (Directiva CEM): Por la presente, United Technologies declara que este dispositivo cumple con los requisitos esenciales y otras disposiciones pertinentes de la Directiva 2004/108/CE.



2002/96/CE (Directiva RAEE): En la Unión Europea, los productos marcados con este símbolo no se pueden descartar entre los residuos municipales sin clasificar. Para su correcto reciclaje, devolver este producto a su proveedor local al comprar un nuevo equipo equivalente, o entregarlo en puntos especiales de recolección. Para más información consultar: www.recyclethis.info.



2006/66/CE (directiva relativa a las pilas): Este producto contiene una pila que, en la Unión Europea, no se puede descartar entre los residuos municipales sin clasificar. Consultar la documentación del producto para obtener información específica sobre la pila. La pila está marcada con este símbolo, que puede incluir letras para indicar que contiene cadmio (Cd), plomo (Pb) o mercurio (Hg). Para su correcto reciclaje, devolver la batería a su proveedor o entregarla en un punto de recolección. Para más información consultar: www.recyclethis.info.

Información de contacto

www.interlogix.com

Atención al cliente

www.interlogix.com/support

Licencias públicas GNU

Linux Kernel 2.6.30, Pthreads, Larry Doolittle, Flex Builder, Yubikey Buildroot están bajo la Licencia Pública General de GNU, versión 2. Una copia de la licencia se encuentra en <http://www.gnu.org/licenses/gpl-2.0.html>.

YAFFS2 y la tar de GNU están bajo la Licencia Pública General de GNU, versión 3. Una copia de la licencia se encuentra en <http://www.gnu.org/licenses/gpl-3.0.html>.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy están bajo la Licencia Pública General Menor de GNU, versión 3. Una copia de la licencia se encuentra en <http://www.gnu.org/licenses/lgpl-3.0.html>.

OpenSSL, Componentes AstraFlex y LIGHTTPD están bajo una licencia BSD modificada

Copyright © 1998-2011 The OpenSSL Project. Todos los derechos reservados.

Copyright © 2008, Yahoo! Inc. Todos los derechos reservados.

Copyright © 2004, Jan Kneschke, incremental. Todos los derechos reservados.

LOS TITULARES DE LOS DERECHOS DE AUTOR Y COLABORADORES OFRECEN ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO LOS AUTORES O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRA CONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

CMockery and Google Protocol Buffers (C) están bajo la licencia Apache, Versión 2.0 (en lo sucesivo, la "Licencia")

No se puede usar este archivo excepto de conformidad con la licencia. Se puede obtener una copia de la Licencia en <http://www.apache.org/licenses/LICENSE-2.0>

A menos que así lo exija la ley aplicable o se acuerde lo contrario por escrito, el software distribuido bajo la Licencia se distribuye en base a "TAL CUAL ES", SIN GARANTÍAS O CONDICIONES DE NINGÚN TIPO, ya sean expresas o implícitas. Consultar la Licencia para obtener información sobre las condiciones que rigen los permisos y las limitaciones vigentes en virtud de la Licencia.

Flex-IFrame

Se concede permiso, de forma gratuita, a cualquier persona que obtenga una copia de este software Flex-IFrame y los archivos de documentación asociados (en lo sucesivo el "Software"), para trabajar con el Software sin restricciones, incluidos, sin limitación, los derechos para usar, copiar, modificar, fusionar, publicar, distribuir, sublicenciar y vender copias del Software, y permitir que las personas a quienes se proporcione el Software también lo hagan.

Google Protocol Buffers (C++) está bajo la nueva licencia BSD.

LOS TITULARES DE LOS DERECHOS DE AUTOR Y COLABORADORES OFRECEN ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO LOS TITULARES DE LOS DERECHOS DE AUTOR O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRA CONTRACTUAL (POR

NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

gSOAP está bajo la licencia pública gSOAP (Licencia MPL modificada)

Copyright © 2001-2009 Robert A. van Engelen, Genivia Inc. Todos los derechos reservados.

EL PROGRAMA DE ESTE PRODUCTO FUE PROVISTO, EN PARTE, POR GENIVIA INC, SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO EL AUTOR SERÁ RESPONSABLE POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRA CONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

mini_httpd está licenciado bajo la licencia freeware de Acme Labs.

La redistribución y en uso en formato fuente y binario de mini_httpd, con o sin modificaciones, están permitidos siempre que se cumplan las siguientes condiciones:

1. La redistribución del código fuente debe conservar el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia.
2. Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia en la documentación u otros materiales suministrados con la distribución.

EL AUTOR OFRECE ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO EL AUTOR O LOS CONTRIBUIDORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRA CONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

Apache log4Net está bajo la licencia Apache versión 2.0.

Una copia de la licencia se encuentra en <http://logging.apache.org/log4net/license.html>.

Non-English versions of Interlogix documents are offered as a service to our global audiences. We have attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

El programa de este producto contiene software con derechos de autor que está licenciado bajo la GPL. Se puede obtener todo el código fuente correspondiente durante un período de tres años después de nuestro último envío de este producto, que será no antes de 30/09/2013, mediante el envío de un giro postal o cheque de \$5 dólares a la siguiente dirección:

Interlogix
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820

Escribir "source for TruPortal" en la línea de memo del pago. Se puede obtener una copia de la Licencia en www.interlogix.com. Esta oferta es válida para cualquier persona que reciba esta información.

CAPITULO 1	<i>Introducción</i>	1
	Convenciones usadas en esta documentación	2
CAPITULO 2	<i>Instalación de hardware</i>	3
	Descripción de la arquitectura del sistema	4
	Documentación de la ubicación física de cada dispositivo	5
	Conexión a una estación de trabajo cliente local o LAN	6
	Instalación de una lectora de enrolamiento	6
CAPITULO 3	<i>Preparación de la configuración</i>	7
	Determinando Ajustes de Red	8
	Uso del Asistente de instalación	9
	Uso del Asistente de actualización	11
CAPITULO 4	<i>Configuración del sistema</i>	13
	Iniciar sesión en el sistema	15
	Ajustar Fecha y hora	15
	Configuración de seguridad de la red	16
	<i>Crear una solicitud de firma de certificado</i>	16
	<i>Importar un Certificado de seguridad</i>	17
	<i>Configurar los Ajustes de red</i>	17
	Configuración de seguridad	18
	<i>Configurar la seguridad de las instalaciones</i>	20
	Configurar el idioma principal del sistema	20
	<i>Ajustar el idioma del sistema</i>	21
	Configuración de los formatos de tarjeta	21
	<i>Añadir un formato de tarjeta</i>	22
	<i>Eliminar un Formato de tarjeta</i>	22
	Configuración de dispositivos	22
	<i>Antes de comenzar</i>	22
	<i>Configurar el controlador del sistema</i>	24
	<i>Configurar entradas y salidas</i>	25
	<i>Configurar un controlador de puerta</i>	25
	<i>Reemplazar un controlador de puerta</i>	26
	<i>Configurar puertas</i>	26
	<i>Configurar las lectoras</i>	33
	<i>Configurar los módulos de expansión de E/S</i>	34
	Configuración de dispositivos de video	34
	<i>Añadir una DVR/NVR</i>	35
	<i>Añadir una cámara de video</i>	35
	<i>Añadir plantillas de video</i>	36
	<i>Enlazar las cámaras a los dispositivos de rastreo de video de eventos</i> ..	36
	Configurar Áreas	36
	<i>Agregar una área</i>	37
	<i>Asignar lectoras a las áreas</i>	37

<i>Remover una Área</i>	37
ConfigurarAnti-passback	38
<i>Configurar el Anti-passback</i>	38
Creación de grupos de feriados.....	39
<i>Añadir un grupo de feriados</i>	40
<i>Agregar un feriado a un grupo de feriados</i>	40
<i>Copiar un grupo de feriados</i>	41
<i>Remover un grupo de feriados</i>	41
Creación de programas	41
<i>Agregar un programa</i>	42
<i>Agregar un intervalo a un programa</i>	42
<i>Eliminar un intervalo de un programa</i>	43
<i>Copiar un programa</i>	43
<i>Remover un programa</i>	43
Crear Grupos de lectoras	43
<i>Añadir un grupo de lectoras</i>	43
<i>Copiar un grupo de lectoras</i>	44
<i>Remover un grupo de lectoras</i>	44
Configuración de los niveles de acceso	44
<i>Añadir un nivel de acceso</i>	44
<i>Copiar un nivel de acceso</i>	45
<i>Remover un nivel de acceso</i>	45
Configuración de roles de operador.....	45
<i>Añadir un rol de operador</i>	46
<i>Modificar un rol de operador</i>	46
<i>Copiar un rol de operador</i>	46
<i>Remover un rol de operador</i>	47
Configurar Correo electrónico	47
<i>Configurar un servido de correo electrónico</i>	47
<i>Modificar una lista de correo electrónico</i>	48
<i>Añadir una lista de correo electrónico</i>	49
<i>Remover una lista de correo electrónico</i>	49
<i>Desactivar notificaciones por correo electrónico</i>	49
Configuración de los Campos definidos por el usuario	50
<i>Agregar campos definidos por el usuario</i>	50
<i>Reorganizar los campos definidos por el usuario</i>	51
<i>Remover un campo definido por el usuario</i>	51
Comportamiento programación de puertas y lectoras	51
Importar Personas y credenciales de un archivo CSV	52
Configuración de Disparadores de acciones	52
<i>Entendiendo los disparadores</i>	53
<i>Entendiendo las acciones</i>	61
<i>Añadir un Registro de disparadores de acciones</i>	66
<i>Copiar un Registro de disparador de acciones</i>	67
<i>Remover un registro disparadores de acciones</i>	67
Configurando un compartido de red	67
<i>Añadir un compartido de red</i>	67
<i>Copiar un compartido de red</i>	68
<i>Remover un compartido de red</i>	68
Crear un respaldo y un punto de restauración.....	68

CAPITULO 5

Administración de acceso69

Administración de personas.....	70
<i>Añadir una persona</i>	<i>70</i>
<i>Remover una persona</i>	<i>71</i>
<i>Cargar foto ID de una Persona</i>	<i>71</i>
<i>Remover foto IDde una Persona</i>	<i>72</i>
Administración de credenciales.....	72
<i>Instalar una lectora de enrolamiento</i>	<i>72</i>
<i>Añadir una credencial</i>	<i>72</i>
<i>Remover una credencial</i>	<i>73</i>
Administración de credenciales perdidas o robadas.....	74
<i>Evitar el uso de una credencial perdida o robada</i>	<i>74</i>
<i>Restablecer una credencial encontrada</i>	<i>74</i>
Administración Cuentas de usuarios.....	75
<i>Añadir una cuenta de usuario</i>	<i>75</i>
<i>Cambiar un nombre de usuario y contraseña</i>	<i>75</i>
<i>Desactivar una cuenta de usuario</i>	<i>75</i>
Crear Reportes.....	76
<i>Crear un reporte</i>	<i>77</i>
Búsqueda de personas.....	77
<i>Buscar personas</i>	<i>77</i>
<i>Cancelar la búsqueda</i>	<i>77</i>

CAPITULO 6

Monitoreo del acceso79

Monitoreo de eventos y alarmas.....	80
<i>Ver últimos eventos</i>	<i>80</i>
<i>Cargar más eventos</i>	<i>81</i>
<i>Cargar todos los eventos</i>	<i>81</i>
<i>Buscar eventos</i>	<i>81</i>
<i>Exportar eventos</i>	<i>81</i>
Monitoreo de eventos de video.....	82
<i>Antes de comenzar.....</i>	<i>82</i>
<i>Reproducir video de eventos</i>	<i>83</i>
<i>Monitorear video</i>	<i>83</i>
<i>Descargar un clip de video</i>	<i>84</i>
<i>Referencia controles de video.....</i>	<i>85</i>
Control de puertas.....	87
<i>Abrir una puerta</i>	<i>87</i>
<i>Desbloquear una puerta</i>	<i>87</i>
<i>Restablecer una puerta</i>	<i>87</i>
<i>Bloquear una puerta</i>	<i>87</i>
<i>Asegurar una puerta</i>	<i>88</i>
<i>Restablecer todas las puertas</i>	<i>88</i>
<i>Bloquear todas las puertas</i>	<i>88</i>
<i>Desbloquear todas las puertas</i>	<i>89</i>
<i>Menús Comandos de puertas</i>	<i>89</i>
<i>Etiqueta Ver eventos</i>	<i>90</i>
<i>Etiqueta Ver horarios</i>	<i>90</i>
<i>Salvar modo fallback de puerta.....</i>	<i>91</i>
Control de entradas y salidas.....	91
<i>Activar o desactivar una salida</i>	<i>91</i>

	Controlar disparadores de acciones	92
	<i>Ejecutar un registro de disparadores de acciones Manualmente</i>	92
	Reajustar Anti-passback	93
CAPITULO 7	<i>Mantenimiento</i>	95
	Respaldo de Datos	95
	<i>Crear una copia de Respaldo</i>	96
	<i>Programar respaldos automáticos</i>	96
	<i>Respaldar Eventos</i>	97
	<i>Restablecer a partir de un respaldo</i>	97
	Salvar y Restablecer los ajustes personalizados	98
	<i>Salvar Datos y ajustes personalizados</i>	98
	<i>Restablecer ajustes personalizados</i>	98
	<i>Reajustar ajustes de fábrica</i>	99
	Actualización del Firmware.....	99
	<i>Antes de comenzar</i>	99
	<i>Verificar actualizaciones de firmware</i>	100
	Administración de paquetes de idiomas	101
	<i>Añadir un paquete de idioma</i>	102
	<i>Remover un Paquete de idioma</i>	102
CAPITULO 8	<i>Solución de problemas</i>	103
	Resolver problemas del navegador	103
	Reiniciar el controlador del sistema.....	104
	Diagnósticos.....	104
	<i>Fusibles</i>	107
	<i>Estados problemas de hardware</i>	107
	<i>Solución de problemas lectoras</i>	108
	<i>Solución de problemas Programas</i>	108
	Mensajes de error, advertencia y eventos	108
	<i>Estados de sabotaje</i>	108
	<i>Eventos de alimentación y baterías</i>	108
	<i>Eventos batería de respaldo</i>	109
	<i>Eventos dispositivos</i>	110
	<i>Eventos sabotaje de puerta</i>	110
	<i>Eventos de entrada auxiliar</i>	111
	<i>Eventos de salida auxiliar</i>	111
	<i>Advertencia "Objetos han cambiado"</i>	111
	<i>Evento "Falló sinc. NTP"</i>	111
	Errores reproductora de video	112
	<i>Ninguna conexión de video activa</i>	112
CAPITULO 9	<i>Referencia</i>	113
	Capacidades del sistema	114
	Configurar Controladores de puerta sencilla basados en IP (IPSDC)	115

<i>Preparar estaciones de trabajo cliente para usar la herramienta de configuración integrada (ICT)</i>	116
<i>Uso de la Herramienta de configuración integrada</i>	118
Permisos de roles de operador predeterminados	121
Uso de puerto.....	124
Exactitud de duración de Pulso	125

TruPortal™ es una sofisticada solución de control de acceso basada en la web que se ha diseñado para ser fácil de usar. Es compatible con una variedad de componentes de hardware de control de acceso, incluyendo:

- Los dispositivos de entrada que detectan las condiciones o eventos, tales como timbres o alarmas.
- Los dispositivos de salida tales como luces y cerraduras que respondan a los dispositivos de entrada y / o disparadores de acciones.
- TruVision™ Grabadoras de video digital (DVRs) y Grabadoras de video en red (NVRs).

El software de interfaz de usuario TruPortal está integrado en el controlador del sistema y se puede utilizar para:

- Controlar el acceso de hasta 64 puertas, en función de programas de acceso definidos por el usuario.
- Configurar los programas para incluir feriados recurrentes.
- Agregar al sistema hasta 10,000 usuarios y tarjetas ID.
- Añadir programas a las lectoras para ayudar a automatizar el sistema.
- Aplicar Anti-passback (APB).
- Crear grupos de lectoras.
- Monitorear los eventos a distancia y automatizar la enlace de los eventos al video grabado.
- Abrir, bloquear y restablecer las puertas, a distancia.

Nota: Para una instalación s319-listada por Underwriters Laboratories of Canada (ULC), las características de acceso remoto son suplementarias.

Las versiones móviles de la interfaz de usuario están disponibles para dispositivos iOS6 y Android™. Estas apps de acompañamiento se pueden usar para monitoreo de la actividad del sistema en forma remota y ejecutar administración básica. Referirse a las *Notas de la versión TruPortal* para detalles.

Además del software de interfaz de usuario, el sistema incluye los siguientes programas:

- El **Asistente de instalación** puede utilizarse para detectar el controlador del sistema en una red, sincronizar la hora en el controlador del sistema con el tiempo en la estación de trabajo cliente local y configurar los ajustes de red. El Asistente de instalación también puede usarse para determinar la nueva dirección IP de un controlador del sistema si la dirección IP ha cambiado. Ver [Uso del Asistente de instalación](#) en pág. 9.
- El **Asistente de actualización** se puede utilizar para actualizar el controlador del sistema desde una versión anterior. *Los clientes existentes TruPortal 1.0 y goEntry 3.0 deberían usar el asistente de Actualización en lugar del asistente de instalación para actualizar el controlador del sistema.* Ver [Uso del Asistente de actualización](#) en pág. 11.
- El **Asistente de importación/exportación** se puede utilizar para importar datos de las personas y las credenciales de una base de datos existente de valores separados por comas (CSV), así como los datos de exportación. También se puede utilizar para borrar personas y los datos de credenciales en el modo por lotes y eventos de exportación. Ver la *Guía del usuario importación/exportación* incluida en el disco utilitarios para detalles.

Convenciones usadas en esta documentación

La documentación TruPortal está incluida en el disco del producto y el texto en cada documento está formateado para hacer fácil la identificación de lo que se describe.

- Cuando un término se define, la palabra está en *cursiva*.
- Los nombres de los campos se muestran en **negritas**.
- Los menús y opciones de menú aparecen en **negritas cursivas**. Todas las opciones del menú tienen teclas de aceleración que permiten seleccionar las opciones del menú por medio del teclado. La letra subrayada indica la tecla de aceleración correspondiente a la opción de menú. Las teclas de aceleración se escriben, por ejemplo, <Alt>, <C>.
- Las teclas del teclado se presentan entre paréntesis angulares. Por ejemplo: <Tab>, <Ctrl>.
- Las combinaciones de teclas se escriben de dos maneras:
<Ctrl> + <Z> significa mantener presionada la primera tecla y presionar la segunda
<Alt>, <C> significa presionar la primera tecla y, luego, presionar la segunda
- Los botones de la pantalla se muestran entre corchetes, por ejemplo: [Modificar], [Cancelar].

Hacer clic en el botón **Ver Ayuda** (?) en la esquina superior derecha de la interfaz de usuario de TruPortal para acceder a la versión electrónica localizable de la *Guía del Usuario de software TruPortal* a través del sistema de ayuda en línea.

Hacer clic en el botón **Mostrar herramienta de consejos** (i) para mostrar información contextual al desplazarse sobre los campos y los iconos en la interfaz de usuario TruPortal. La herramienta de consejos se puede activar y desactivar haciendo clic en el mismo botón. Maximizar la ventana del navegador para mostrar todas las herramientas de consejos; la herramienta de consejos puede no aparecer si la ventana del navegador es demasiado pequeña.

El primer paso en la configuración del sistema es la instalación de los componentes de hardware que serán utilizados por el sistema (entradas, salidas, puertas, lectoras, cámaras, etc.) de acuerdo con las instrucciones del fabricante. Asegurarse de registrar datos sobre configuraciones de la puerta que se pueden utilizar más adelante en el nombramiento de los dispositivos, grupos de lectoras, y las áreas en las que los dispositivos se configuran en la interfaz de usuario.

Nota: Clientes existentes TruPortal 1.0 ó goEntry 3.0 que ya tienen instalado y configurado todo el hardware pueden saltar este paso y usar el **Asistente de Actualización** para actualizar el controlador del sistema. Ver [Uso del Asistente de actualización](#) en pág. 11.

Después de instalar los componentes de hardware, conectar el controlador del sistema a una estación de trabajo cliente local o en una Red de área local (LAN), y luego usar el Asistente de Instalación para detectar el controlador del sistema en la red, como se describe en [Preparación de la configuración](#) en pág. 7.

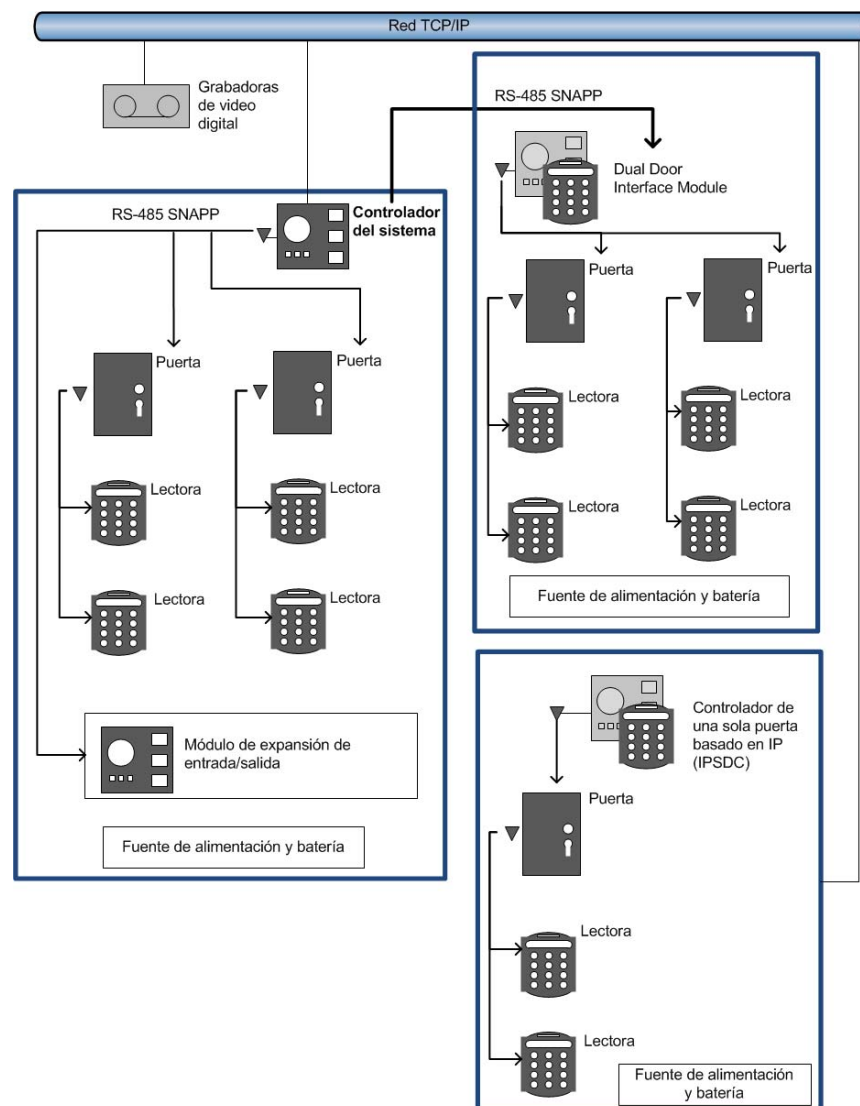
Los temas en este capítulo incluyen:

- [Descripción de la arquitectura del sistema](#) en pág. 4
- [Documentación de la ubicación física de cada dispositivo](#) en pág. 5
- [Conexión a una estación de trabajo cliente local o LAN](#) en pág. 6
- [Instalación de una lectora de enrolamiento](#) en pág. 6

Descripción de la arquitectura del sistema

Las funciones del controlador del sistema como el cerebro del sistema que recibe y envía la información. Contiene la base de datos que almacena todos los datos de los dispositivos, programas, personas, etc., así como el software de interfaz de usuario que se puede acceder desde una computadora a través de un navegador web, un iPhone o un iPad.

Diversos componentes se pueden conectar al controlador del sistema, incluyendo controladores de puerta, lectoras, módulos de expansión de entrada/salida, relés de sirena, relés de estrobo y relés de apertura. Estos componentes pueden ser considerados los brazos del sistema, que se alimentan de datos en el sistema y también llevan a cabo las acciones solicitadas por el sistema.



Además de los componentes de lógica cableada, el controlador del sistema se puede comunicar con el protocolo de Internet propietario Controladores de puerta sencilla basados en IP. Además, las apps companion iPad®, iPhone®, y Android™ permiten a los usuarios el monitoreo remoto de actividad del sistema y ejecutar tareas administrativas básicas, como añadir o borrar usuarios.

Documentación de la ubicación física de cada dispositivo

A medida que se instala cada dispositivo para cada puerta (cerraduras, sensores, lectoras), proporcionar una descripción de cada dispositivo, y una lista de los números de serie de los dispositivos asociados a cada puerta en una gráfica de instalación como la que se proporciona a continuación. Estos datos pueden ser utilizados más tarde, cuando los dispositivos se configuran en la interfaz de usuario.

Descripción de la puerta	Número de serie de las lectoras	Controlador de puerta Número de serie	Expansión E/S Número de serie	Cámara enlazada
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			

Descripción de la puerta	Número de serie de las lectoras	Controlador de puerta Número de serie	Expansión E/S Número de serie	Cámara enlazada
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			

Conexión a una estación de trabajo cliente local o LAN

El controlador del sistema se puede conectar directamente a una estación de trabajo cliente local o en una red de área local (LAN). Hay dos tomas Ethernet RJ-45 100BaseT en el controlador de sistema. El puerto 1 es configurable y el puerto 2 tiene una dirección IP (protocolo de Internet) fija, 169.254.1.200. Consultar la Guía de Referencia rápida del controlador del sistema para identificar las tomas.

Si se conecta el controlador del sistema directamente a una estación de trabajo local, utilizar la toma Ethernet estática y un cable Ethernet Categoría 6 (CAT6). Si se conecta a una LAN, utilizar el conector Ethernet configurable y un cable Ethernet CAT6. Consultar al administrador de la red del sitio para determinar cómo se debe configurar el controlador del sistema, como se explica en [Determinando Ajustes de Red](#) en pág. 8.

Nota: Si se cuenta con varios dispositivos de red con una conexión única a la red a través de un conmutador o un enrutador pequeño, verificar que no haya más que un interruptor o enrutador entre el controlador del sistema y la conexión a la red.

Instalación de una lectora de enrolamiento

Si se planea utilizar la lectora de enrolamiento opcional (TP-RDR-LRN) para leer los datos en tarjetas credencial, instalar y configurar la lectora en una estación de trabajo cliente de acuerdo con las instrucciones del fabricante. Ver [Instalar una lectora de enrolamiento](#) en pág. 78 para más detalles.

Preparación de la configuración

Después de instalar los dispositivos de hardware, se deben ejecutar los siguientes pasos antes de lanzar la Interfaz de usuario para ejecutar una configuración completa del Sistema:

1. Consultar con el administrador de la red localidad para decidir cómo se debe configurar los ajustes de la red. Ver [Determinando Ajustes de Red](#) en pág. 8.
2. *Si se trata de un cliente existente de TruPortal 1.0 ó goEntry 3.0 y todo el hardware está ya instalado y configurado*, usar el Asistente de actualización para actualizar el controlador del sistema en lugar de usar el Asistente de instalación. Ver [Uso del Asistente de actualización](#) en pág. 11.

Si se trata de un usuario nuevo de TruPortal seguir los pasos en [Uso del Asistente de instalación](#) en pág. 9 para:

- Detectar el controlador del sistema en la red de área local.
 - Cambiar la contraseña por default para la cuenta de Administrador principal para mejorar la seguridad.
 - Sincronizar la fecha/hora en el controlador del sistema con la estación de trabajo del cliente local.
 - Configurar los ajustes de red del controlador del sistema.
3. Configurar cualquier controlador de puerta sencilla basado en IP instalado, para que reconozca la dirección IP del controlador del sistema *antes* de configurar el controlador de puerta sencilla basado en IP en la interfaz de usuario. Al establecer esta conexión de red se asegura que los controladores de puerta sencilla basados en IP serán detectados cuando el controlador del sistema escanea para cambios de hardware. Para obtener más información, ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.

Determinando Ajustes de Red

Antes de usar el Asistente de instalación para ejecutar una configuración inicial del controlador del sistema, consultar con el administrador de la red del sitio para determinar las respuestas a las siguientes preguntas:

- **¿La dirección IP del controlador del sistema debe ser estática o dinámica?** Los operadores accederán a la interfaz de usuario escribiendo la dirección IP del controlador del sistema en el campo de dirección del navegador web. Si la dirección IP del controlador del sistema usa el Protocolo de configuración de Anfitrión Dinámico (DHCP), entonces los operadores deben usar una URL virtual u otro alias para acceder al controlador del sistema. Si la asignación de dirección IP actual es cambiada por la red, los operadores no podrán encontrarla.
- **¿Deberá cambiarse el Puerto de Servicio?** El Puerto de servicio por default para una conexión HTTPS es 443; el valor por default para una conexión HTTP es 80. Típicamente, este puerto sólo necesita cambiar si está en conflicto con un puerto existente en uso en la red. Si el puerto es cambiado, los usuarios necesitarán incluir el número de puerto con la dirección IP del controlador del sistema para iniciar sesión en el sistema (p.ej., `https://IPaddress:port`).

Nota: Los puertos 0 al 1024 (p.ej., *puertos bien conocidos*) están reservados para servicios privilegiados. Se recomienda que esos puertos no se usen como puertos de servicio.

- **Si se usa una dirección IP estática, ¿cuáles son los valores de las máscaras de sub-red, puerta de enlace y nombre del servidor de dominio (DNS) para la red?** Esta información será necesaria para configurar las propiedades de la red para el controlador del sistema.
- **¿Debe usarse una conexión Segura de Protocolo de Transferencia Hipertexto (HTTPS)?** Se recomienda usar la conexión HTTPS para evitar el acceso no autorizado al sistema. Este protocolo de hipertexto seguro encripta los paquetes entre los navegadores de los clientes y el controlador del sistema e impide que alguien recopile información del usuario espiando el tráfico de la red. Puede haber casos en los que es necesario usar el protocolo de hipertexto no seguro (HTTP). Por ejemplo, si se accede al controlador del sistema a través de un servidor de red proxy no compatible con HTTPS, la única opción es desactivar HTTPS.

Después de la instalación, el sistema también puede ser configurado para usar una conexión segura Secure Shell (SSH) que autentica las estación de trabajo de clientes remotos y permite a los usuarios remotos iniciar sesión en el sistema (incluyendo a los representantes de soporte técnico). Referirse a [Configuración de seguridad de la red](#) en pág. 16.

Uso del Asistente de instalación

Esta sección describe cómo usar el Asistente de instalación para:

- Detectar el controlador del sistema en la red de área local.
- Cambiar la contraseña por default para la cuenta de Administrador principal para mejorar la seguridad.
- Sincronizar la fecha/hora en el controlador del sistema con la estación de trabajo del cliente local.
- Configurar los ajustes de red del controlador del sistema.

Nota: Si se trata de un usuario existente de TruPortal o goEntry, ejecutar el **Asistente de actualización** para actualizar el controlador del sistema de una versión anterior en vez de usar el Asistente de instalación. Ver [Uso del Asistente de actualización](#) en pág. 11.

El Asistente de instalación también puede usarse para determinar la nueva dirección IP de un controlador del sistema si la dirección IP ha cambiado.

Nota: El Asistente de instalación no es compatible con Microsoft® Windows® XP.

Para usar el Asistente de instalación:

1. Verificar que el controlador del sistema esté conectado a la red de área local para que pueda ser detectado por el Asistente de instalación.
2. Insertar el disco del producto en el drive CD/DVD de la estación de trabajo del cliente.

Nota: Si se descargó la imagen del disco y se extrajo al disco duro de la estación de trabajo del cliente, abrir Windows Explorer, navegar a la imagen del disco en el disco duro y hacer clic doble en **start.hta** de la aplicación para lanzar el software Utilitarios.

El software Utilitarios determinará si la estación de trabajo del cliente incluye los programas requeridos para ejecutar la interfaz del usuario.

3. Si se indica, hacer clic en **.NET 4.5 Framework** y/o en **Bonjour** para instalar el software.
4. Hacer clic en el icono **Asistente de instalación**.
5. Cuando aparece la página de introducción, seleccionar un **idioma** y hacer clic en [Siguiente].
El asistente de instalación buscará cualesquier controladores del sistema en la red.
6. Seleccionar el controlador del sistema en la lista y hacer clic en [Siguiente].
7. En la página de iniciar sesión, escribir la actual **Contraseña** para la cuenta del the Administrador.
El default de **Nombre de Usuario** para la cuenta del Administrador es `admin`.
El default de **Contraseña** para la cuenta del administrador es `admin`.

IMPORTANTE: La cuenta del administrador tiene acceso a todos los aspectos del sistema. Es peligroso dejar la contraseña por default sin cambiar. Todos los que están familiarizados con el producto conocen los valores por default.

8. Escribir la contraseña nueva en los campos **Nueva contraseña** y **Confirmar contraseña**, y hacer clic en [Siguiente].
9. En la página Fecha/hora, seleccionar la **Zona horaria del controlador del sistema**.
10. Si los valores **Fecha y hora del controlador** y **Fecha y hora de cliente** aparecen en rojo, la zona horaria ajustada en el controlador del sistema es diferente a la zona horaria en la estación de trabajo del cliente, o la hora varía entre los dos dispositivos por más de 10 segundos.

Hacer clic en [Sync hora] para sincronizar la zona horaria y hora en el controlador del sistema con la zona horaria y hora de la estación de trabajo del cliente.

Nota: Después de completar la configuración inicial, el sistema puede ser sincronizado con un servidor de Protocolo Hora de Red (NTP). Ver [Ajustar Fecha y hora](#) en pág. 15

11. Hacer clic en [Siguiente] para continuar a la página de Configuración de la red.

12. Seleccionar **Estático** o **Dinámico** como el tipo de conexión para el controlador.

Para configurar una dirección IP estática:

- a. Escribir la **dirección IP** para el controlador que los usuarios escribirán en el navegador de web para conectarse al sistema.
- b. (Opcional) Cambiar el **Puerto de servicio** para el controlador del sistema.

Nota: El Puerto de servicio por default para una conexión HTTPS es 443; el valor por default para una conexión HTTP es 80. Los puertos 0 al 1024 (p.ej., *puertos bien conocidos*) están reservados para servicios privilegiados. Se recomienda que esos puertos no se usen como el puerto de servicio. Si el puerto se cambia a un valor diferente, los usuarios necesitarán incluir el número de puerto a la dirección IP del controlador del sistema para iniciar sesión en el sistema (p.ej., `https://IPaddress:port`).

- c. Escribir la **Máscara de sub-red** para la red en que está conectado el controlador.
- d. Escribir la **Puerta de enlace predeterminada** para la red.
- e. Escribir el **Servidor DNS** para la red.

13. Seleccionar **Activar Conexión HTTPS** para usar un protocolo de hipertexto seguro

IMPORTANTE: Se recomienda usar la conexión HTTPS para evitar el acceso no autorizado al sistema.

14. Hace clic en [Aplicar] para salvar la configuración de la red.

15. Para experimentar con diferentes configuraciones de la red, hacer clic en [Reiniciar el controlador].

La página descubrimiento de controlador aparecerá y detectará el controlador del sistema nuevamente. Regresar a la página de Configuración de red para editar los ajustes como se necesite.

16. Para acceder a la interfaz de usuario principal e iniciar la configuración del sistema, hacer clic en el hiperenlace que muestra la dirección IP del controlador. Ver [Configuración del sistema](#) en pág. 13 para más detalles.

17. Hacer clic en [Finalizar] para cerrar el Asistente de instalación.

18. Si hay controladores de puerta sencilla basado en IP instalados, se deben configurar para que reconozcan la dirección IP del controlador del sistema *antes* de configurar el controlador de puerta sencilla basado en IP en la interfaz de usuario. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.

19. Proceder con [Configuración del sistema](#) en pág. 13.

Uso del Asistente de actualización

Los clientes de TruPortal 1.0 ó goEntry 3.0 puede usar el **asistente de actualización** para actualizar el controlador del sistema en forma remota desde la estación de trabajo de un cliente local de una versión del producto a otra versión (por ejemplo, de la versión 1.0 a la versión 1.5). Este proceso consiste en la descarga de archivos desde el sitio web del producto, y luego usando el Asistente de actualización para respaldo de datos, actualizar el firmware y el código del núcleo en el controlador del sistema y restaurar los datos.

Antes de usar el Asistente de actualización, notar los siguientes detalles:

- IMPORTANTE:** No solo apagar y encender el controlador del sistema (se debe apagar y desenchufar la alimentación) durante una actualización.
- IMPORTANTE:** La *Actualización* es diferente a la *actualización del firmware*. Una actualización de firmware impacta al firmware mientras que una actualización afecta tanto al firmware como al código central del controlador del sistema. No usar la página **Administración del Sistema > Actualizaciones firmware**, para actualizar el controlador del sistema, usar el asistente de actualización en su lugar.
- Después de una actualización, el controlador del sistema no puede degradarse a la versión anterior.
- El Asistente de actualización no es compatible con Microsoft Windows XP.
- **(Se recomienda)** ejecutar el asistente de actualización directamente desde la DVD física TruPortal, contrario al montaje de una imagen ISO.
- Aunque el Asistente de actualización proporciona una opción para realizar respaldos de datos, un archivo de respaldo extra puede ser creado como medida de precaución (ver [Crear una copia de Respaldo](#) en pág. 102). Los valores de configuración también se pueden respaldar (ver [Salvar y Restablecer los ajustes personalizados](#) en pág. 104). Para salvar un registro histórico de eventos, usar el asistente de importación/exportación de eventos en formato CSV.
- Si está actualizando desde goEntry a TruPortal, se conservará la información de formato de tarjeta.
- Asegurar que todos los usuarios registren su salida del sistema antes de usar el asistente de actualización.
- Asegurarse de que todos los procesos de respaldo y restablecimiento hayan terminado.
- La actualización será más rápida y más fiable si el controlador del sistema utiliza una dirección IP estática. (Para cambiar este ajuste, ver [Configurar los Ajustes de red](#) en pág. 17.) Si se usa una dirección IP dinámica, la dirección IP puede cambiar durante la actualización y el proceso para. Si ocurre esto, usar el Asistente de instalación para obtener la nueva dirección IP y entonces reiniciar el Asistente de actualización.
- Un botón [Finalizar] aparece en muchas páginas del asistente, hacer clic en él para detener la actualización, si es necesario.

Para usar el Asistente de actualización:

1. Iniciar sesión en el sitio web del producto y descargar los siguientes archivos en una estación de trabajo local:
 - La imagen ISO de la última versión del disco de Utilitarios.
 - El archivo de fuente NGP.bin que se utiliza para actualizar el firmware.

IMPORTANTE: No cambiar el nombre de los archivos descargados.

2. Utilizar una aplicación de terceros para montar (por ejemplo, añadir) la imagen ISO descargada en el equipo cliente local.
3. En el Explorador de Windows, navegar a la carpeta \PanelUpgradeWizard en la imagen ISO.
4. Hacer clic doble en **PanelUpgradeWizard.exe**.
El asistente creará una carpeta llamada <documentos locales>\PanelUpgradeWizard que incluye dos subcarpetas: \Backups y \Logs.
5. Cuando aparece la página de introducción, seleccionar un **idioma** y hacer clic en [Siguiente].
6. Iniciar sesión como un usuario con permisos de ejecución para la característica Actualizaciones de firmware y hacer clic en [Siguiente].
La página de archivo de origen muestra detalles sobre el firmware en el controlador del sistema.
7. Hacer clic en [...] para navegar a la carpeta donde se descargó el archivo NGP.bin.
8. En la caja de diálogo Abrir que aparece, hacer clic en el archivo NGP.bin para seleccionarlo, y luego hacer clic en [Abrir].
La página del archivo de origen muestra los detalles sobre el archivo NGP.bin.
9. Hacer clic en [Siguiente].
10. En la página de respaldo, escribir la ruta en la que se copiarán los datos de arriba, o navegar a su ubicación.

Nota: Aún cuando la casilla de verificación **Crear archivo de respaldo** se puede borrar para evitar el respaldar datos, se recomienda que los usuarios la dejen activada para respaldar los datos antes de la actualización. Esta opción es sólo para uso de la fábrica.

IMPORTANTE: Si no se crea un archivo de respaldo mediante el uso del asistente de actualización, las fotos no se conservarán y tendrán que ser restablecidas a partir de una copia de respaldo anterior.

11. Hacer clic en [Respalidar].
12. Cuando aparezca el mensaje "Respaldo exitoso", hacer clic en [Siguiente].
13. En la siguiente página, hacer clic en [Actualización del firmware].
Aparece un resumen del progreso del Asistente de actualización. Este proceso puede tardar entre cinco y diez minutos. Aparecerán cuadrados rojos junto a los errores que se produjeron.
14. Cuando la actualización se haya completado, hacer clic en [Siguiente].
15. Si los datos están respaldados en [paso 11](#), la página Restaurar muestra la localización a la cual se respaldaron los archivos.
 - a. Hacer clic en [Restaurar] para cargar los datos del respaldo de nuevo en el controlador del sistema.
 - b. Cuando aparece el mensaje "Restaurar exitoso" hacer clic en [Siguiente] para comprobar que la actualización se produjo en la página Resultados de la actualización.
16. Cuando aparezca la página Resultados de la actualización, hacer clic en [Finalizar] para salir del asistente.
17. Si un sistema goEntry se actualizó a TruPortal, revisar las descripciones de formato de tarjeta en la página **administración del sistema > formatos de tarjetas** y actualizarlos, si es necesario. (Las descripciones de formato de tarjeta se actualizan sólo en inglés.)
18. Si hay controladores de puerta sencilla basado en IP instalados, se deben configurar para que reconozcan la dirección IP del controlador del sistema *antes* de configurar el controlador de puerta sencilla basado en IP en la interfaz de usuario. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.

Configuración del sistema

TruPortal está diseñado para que, una vez configurado, se puedan añadir y remover rápidamente personas y credenciales así como gestionar el acceso a una localidad. Durante su configuración, se define la siguiente información:

- Las áreas, puertas, lectoras de credenciales, video de vigilancia y los sistemas auxiliares de seguridad en una localidad.
- Los niveles de acceso necesarios para los varios grupos de personas que trabajan en una localidad.
- Los programas de acceso para días hábiles y feriados.
- Las funciones de operador de las personas que vayan a administrar y a monitorear el sistema.

Este capítulo está organizado de forma secuencial, con las tareas dispuestas en el orden en que deben ejecutarse para configurar el software.

IMPORTANTE:

Si hay cualesquier controladores de puerta sencilla basados en IP instalados, se deben configurar para que reconozcan la dirección IP del controlador del sistema *antes* de configurarlos en la interfaz del usuario. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.

1. [Iniciar sesión en el sistema.](#)
2. [Ajustar Fecha y hora.](#)
3. [Crear una solicitud de firma de certificado.](#)
4. [Importar un Certificado de seguridad.](#)
5. [Configurar los Ajustes de red.](#)
6. [Configurar la seguridad de las instalaciones.](#)
7. [Ajustar el idioma del sistema.](#)
8. [Añadir un formato de tarjeta.](#)
9. [Escanear para cambios de hardware.](#)
10. [Asignar nombres significativos al hardware.](#)

11. **Configurar el controlador del sistema.**
12. Opcional: **Configurar los módulos de expansión de E/S.**
13. **Configurar un controlador de puerta.**
14. **Desbloquear una puerta.**
15. **Configurar las lectoras.**
16. Opcional: **Añadir una DVR/NVR.**
17. Opcional: **Añadir una cámara de video.**
18. Opcional: **Enlazar las cámaras a los dispositivos de rastreo de video de eventos.**
19. Opcional: **Agregar una área.**
20. Opcional: **Configurar el Anti-passback.**
21. Opcional: **Asignar lectoras a las áreas.**
22. Opcional: **Añadir un grupo de feriados.**
23. Opcional: **Agregar un programa.**
24. Opcional: **Añadir un grupo de lectoras.**
25. **Añadir un nivel de acceso.**
26. Opcional: **Añadir un rol de operador.**
27. Opcional: **Configurar un servido de correo electrónico.**
28. Opcional: **Añadir una lista de correo electrónico.**
29. Opcional: **Agregar campos definidos por el usuario.**
30. Opcional: **Comportamiento programación de puertas y lectoras.**
31. **Importar Personas y credenciales de un archivo CSV.**
32. Opcional: **Configuración de Disparadores de acciones.**
33. Opcional: **Configurando un compartido de red.**
34. **Crear un respaldo y un punto de restauración.**
35. Opcional: **Añadir un Registro de disparadores de acciones.**
36. Opcional: **Añadir un paquete de idioma.**

Iniciar sesión en el sistema

1. Lanzar un navegador de Internet.
2. Escribir la dirección IP para el sistema en la barra direcciones del navegador.

Nota: Si el puerto de servicio por default para el sistema se ha cambiado, anexar el número de puerto a la dirección IP (p. ej., `https://IP address:port`).

3. Si al usar Internet Explorer® recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
4. Escribir **Nombre usuario**.
5. Escribir **Contraseña**.
6. (Opcional) Seleccionar un **idioma** diferente para la interfaz de usuario.
Por default, el sistema incluye cinco idiomas — inglés, español, francés, holandés y portugués — pero es posible añadir más. Ver [Administración de paquetes de idiomas](#) en pág. 107.
7. Hacer clic en [Iniciar sesión].
8. Si es la primera vez que se usará la Interfaz de usuario en la estación de trabajo del cliente, hacer clic en **Aceptar** cuando aparezca la página de Contrato de Licencia.

La página **Inicio** muestra varios asistentes que pueden usarse para añadir rápidamente personas, credenciales, niveles de acceso, programas y feriados. Hacer clic en un icono de asistente y seguir las instrucciones en la pantalla para añadir nuevos objetos, o referirse a la sección relevante de este documento para instrucciones detalladas.

Para salir del sistema más tarde hacer clic en el icono **Terminar sesión** en la parte superior derecha de la interfaz de usuario

Ajustar Fecha y hora

El sistema soporta sincronización de hora con un servidor Protocolo de Hora en Red (NTP). Si está activada esta opción tanto en la interfaz de usuario como en una DVR/NVR, la DVR/NVR y el sistema se mantienen sincronizados a tiempo. Sin esta opción, la hora del sistema puede variar con relación a la hora de la DVR/NVR lo cual puede impactar a los programas y causar dificultades en la obtención de video relativo a un evento de acceso.

Notar los detalles siguientes acerca del tiempo de sincronización NTP:

- El cliente NTP trata de sincronizarse cada hora.
- Para usar esta opción, el controlador del sistema debe poder acceder al servidor NTP a través del Protocolo Usuario Datagram (UDP) puerto 123. Si este puerto no está accesible, la hora del sistema no se sincroniza con el servidor NTP y se registran eventos de «Error de sinc NTP». Consultar con el administrador de la red de la localidad.
- Si la hora del sistema se cambia manualmente a menos de un minuto antes del comienzo de un horario asignado a una puerta, el modo horario de la puerta surte efecto de inmediato.

Para ajustar la fecha y la hora:

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Fecha y hora**.

3. Seleccionar la **zona horaria**.
4. Seleccionar la **fecha y hora** local.
5. (Opcional) Sincronizar hora:
 - a. Seleccionar la caja de selección **Sincronizar con servidor NTP**.
 - b. Hacer clic en [Aceptar cambios].
 - c. Escribir la dirección IP del servidor NTP.
 - d. Hacer clic en [Aceptar cambios].
 - e. Hacer clic en [Sincronizar ahora].
6. Hacer clic en [Aceptar cambios].

Configuración de seguridad de la red

La etiqueta Configuración de red de la página **Administración del sistema > Ajustes del sistema** muestra varios ajustes de la red que pueden ser usados para asignar un certificado de seguridad y configurar las propiedades de la red, incluida la navegación segura.

Crear una solicitud de firma de certificado

Secure Sockets Layer (SSL) es una tecnología de encriptación que protege los datos que se están transmitiendo entre el servidor web y los navegadores de web de los usuarios para evitar espionaje, sabotaje de datos, etc. El uso de SSL en un sitio web se indica en general con un icono de candado en los navegadores de web, pero también puede ser indicado con una barra de direcciones verde.

Para activar SSL en el sistema, crear una solicitud de firma de certificado (también conocida como *CSR* o como *solicitud de certificación*), someterla a una autoridad de certificación y después importar el certificado firmado. Un certificado auto-firmado también se puede instalar. Este bloque de texto encriptado se genera en el servidor en el que se usa el certificado, contiene información como el nombre de la organización, nombre común (i.e. nombre del dominio), localidad y país.

Para crear una solicitud de firma de certificado:

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Configuración de red**.
3. Hacer clic en [Crear solicitud firma de certificado].
Aparece la caja de diálogo Solicitud de firma de certificado.
4. Escribir la información solicitada y hacer clic en [Generar].

Nota: Escribir ya sea la dirección IP o el nombre del dominio calificado completamente (FQDN) del servidor en el campo **Nombre común**. Si el controlador está configurado para usar una dirección IP DHCP-asignada, entonces es muy recomendable que el servidor DHCP se configure para que asigne siempre esta dirección IP al controlador. De lo contrario, cada vez que se asigna una dirección IP diferente al controlador, se tendrá que generar e instalar un nuevo certificado.

El texto de la solicitud de firma de certificado (CSR) aparece en la caja de texto al lado derecho de la caja de diálogo.

5. Para usar un certificado autofirmado, hacer clic en [Instalar certificado autofirmado].
El controlador del sistema se reiniciará automáticamente.

6. Para usar un certificado firmado:
 - a. Copiar el texto del CSR y salvarlo en un archivo local para enviar a una autoridad de certificación.
 - b. Cerrar la caja de diálogo Solicitud de firma de certificado.
 - c. Ver [Importar un Certificado de seguridad en la página 17](#).

Importar un Certificado de seguridad

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Configuración de red**.
3. Hacer clic en [Importar certificado]. Aparece la caja de diálogo Cargar certificado.
4. Hacer clic en [Seleccionar archivo].
5. Buscar y seleccionar el archivo del certificado.
6. Hacer clic en [Abrir].
7. Hacer clic en [Cargar].

El controlador del sistema se reiniciará automáticamente.

Configurar los Ajustes de red

Los ajustes de red para el sistema se configuran inicialmente en el Asistente de instalación, pero se pueden actualizar en la etiqueta Configuración de red de la página de **Administración del sistema > Ajustes del sistema** como se describe a continuación. Consultar [Determinando Ajustes de Red](#) en pág. 8 para obtener más información acerca de las opciones de configuración.

1. Iniciar sesión como usuario con permisos de modificación para la función de configuración de red.
2. Seleccionar **Administración del sistema > Ajustes del sistema**.
3. Hacer clic en la etiqueta **Configuración de red**.
4. Hacer clic en [Configurar].
Aparece la caja de diálogo Propiedades de red.
5. Para utilizar una conexión dinámica, seleccionar **Obtener una dirección IP automáticamente mediante DHCP**.
6. Para utilizar una conexión estática, seleccionar **Usar la siguiente dirección IP** y escribir.
Para configurar una dirección IP estática:
 - a. Escribir la **Dirección IP** del controlador del sistema.
 - b. Escribir la **Máscara sub-red**.
 - c. Escribir el **Portal por default**.
 - d. Escribir el **Servidor DNS**.
7. (Opcional) Cambiar el **Puerto de Servicio** para el controlador del sistema.

Nota: El Puerto de servicio por default para una conexión HTTPS es 443; el valor por default para una conexión HTTP es 80. Los puertos 0 al 1024 (p.ej., *puertos bien conocidos*) están reservados para servicios privilegiados. Se recomienda que esos puertos no se usen como el puerto de servicio.

Si el puerto se cambia a un valor diferente, comunicará dicha información a los usuarios, ya que tendrá que añadir el número de puerto a la dirección IP del controlador

del sistema (por ejemplo, <https://IPaddress:port>) para iniciar sesión de nuevo después de que se reinicie el sistema.

8. Seleccionar **Activar Conexión HTTPS** para usar un protocolo de hipertexto seguro.

IMPORTANTE: Se recomienda usar la conexión HTTPS para evitar el acceso no autorizado al sistema.

9. Si se cambia la configuración de HTTPS, desactivar la caché del navegador, especialmente si se utiliza Firefox o Chrome.
10. Para utilizar una conexión SSH que autentifica las estaciones de trabajo remotas y permite a los usuarios remotos (incluyendo representantes de soporte técnico) iniciar sesión, seleccionar **activar conexión SSH**.

Nota: Consultar [Configuración de seguridad](#) en pág. 18 para información sobre cómo configurar una contraseña para una cuenta de servicio SSH.

11. Hace clic en [Salvar] para aceptar los cambios a la configuración de red.
Aparecerá un mensaje para indicar que el controlador del sistema se debe reiniciar para aplicar los cambios a la configuración de la red.
12. Hacer clic en [Salvar cambios].
El sistema se reiniciará. Los usuarios que están registrados actualmente perderán su conexión y deberán iniciar sesión nuevamente. Si la dirección IP del controlador del sistema ha cambiado, actualizar cualesquier controladores de puerta sencilla basados en IP en el sistema para que reconozcan la nueva dirección IP. Ver [Usar el ICT para configurar los controladores de puerta sencilla basados en IP](#) en pág. 125.

Configuración de seguridad

La etiqueta Seguridad de la página **Administración del sistema > Ajustes del sistema** permite configurar aspectos relativos a la seguridad física de las instalaciones.

Códigos PIN

El sistema puede ser configurado para el acceso solo con una credencial o con una credencial y un número de identificación personal (PIN). Exigir que las personas presenten una tarjeta de identificación (credencial) y escriban un código PIN, aumenta la seguridad al impedir el acceso con una tarjeta de identificación encontrada o robada. Las lectoras pueden configurarse para Solo credencial o Credencial y PIN, según los horarios. (Ver [Comportamiento programación de puertas y lectoras en la página 55.](#))

Longitud máxima del PIN

El PIN puede tener 4, 6 ó 9 dígitos.

Máximo intentos PIN

Permite a las personas cierto número de intentos para introducir su PIN correctamente.

Tiempo de bloqueo de PIN

Si una persona ingresa un PIN incorrecto demasiadas veces, se impide el acceso de la ID de credencial a esa lectora durante el tiempo especificado en esta opción. Una vez transcurrido el tiempo de bloqueo, se restauran los privilegios de acceso de la ID de credencial.

Salvar modo fallback de puerta

La información de las credenciales se almacena en el controlador del sistema. Si un controlador de puerta dual pierde la comunicación con el controlador del sistema, las credenciales escaneadas a una lectora no pueden ser verificadas. En tal caso, el controlador de puertas debe validar las solicitudes de acceso si alguien ha de entrar en las instalaciones.

Nota: Los controladores de puerta sencilla basados en IP cuentan con un modo fallback separado.

Entrada terminaciones fin de línea

Las puertas pueden ser cableadas para detectar si están abiertas o cerradas, forzadas y saboteadas. A estas puertas se las llama *supervisadas*. A las puertas sin circuitos de detección se las llama no supervisadas, aunque tengan una lectora y una cerradura eléctrica o un bloqueo magnético. Para puertas supervisadas, esta opción describe el tipo de resistencia(s) que se usan y cómo se cablea el circuito. Hay dos tipos principales monitoreados por: circuitos de 1,000 y de 4,700 ohmios. Pueden cablearse con resistencias dobles o con una sola resistencia conectada en serie o en paralelo en relación con el sensor de la puerta.

Nota: Los controladores de puerta sencilla basados en IP soportan sólo supervisión 1K/Doble, como se ha configurado mediante el ajuste de los interruptores en el controlador. Consultar la *Referencia rápida del controlador de una sola puerta basada en IP* para detalles.

Ajustar contraseña SSH para la cuenta de servicio

Una conexión SSH se puede activar en la etiqueta **Seguridad** de la de la página **Administración del sistema > Ajustes del sistema** para autenticar a los usuarios remotos (incluyendo los representantes de soporte técnico) que inician su sesión. Usar el botón [Ajustar contraseña SSH para cuenta de servicio] para ajustar la contraseña.

Modo fallback del controlador de puerta sencilla basado en IP

La información de las credenciales se almacena en el controlador del sistema. Si un controlador de puerta sencilla basado en IP pierde la comunicación con el controlador del sistema, las credenciales escaneadas a una lectora no pueden ser verificadas. Seleccionar **Usar tabla caché local** para conceder acceso si la tarjeta coincide con una de las últimas 50 credenciales usadas para obtener acceso exitosamente, según se hayan almacenado en la memoria caché local del controlador de puerta sencilla basado en IP.

Notar los siguientes detalles sobre el modo fallback del controlador de puerta sencilla basado en IP:

- Durante los primeros 40—60 segundos de pérdida de conectividad de red, el controlador de puerta sencilla basado en IP continuará intentando verificar las credenciales a través del controlador del sistema. Debido a que el controlador del sistema no puede alcanzarse, las credenciales se rechazarán hasta que inicie el modo fallback del controlador de puerta sencilla basado en IP.
- Si las credenciales se cambian o se borran, todos los datos en memoria caché de los controladores de puerta sencilla basados en IP se despejarán.

Encriptar comunicaciones del controlador de puerta sencilla basado en IP

Por default, esta caja de selección se selecciona para encriptar las comunicaciones entre el controlador del sistema y los controladores de puerta sencilla basados en IP para mejorar la seguridad de los datos.

Configurar la seguridad de las instalaciones

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Seguridad**.
3. Seleccionar la **longitud máxima de PIN**.

IMPORTANTE: Cuando se salva una nueva longitud máxima de PIN y existen credenciales con números de PIN más largos que la nueva longitud máxima, aparece una advertencia diciendo que los números de PIN existentes se truncarán para adaptarlos a la nueva longitud. El mensaje del sistema permite continuar o cancelar la operación de salvar.

4. Seleccionar el número **máximo de intentos de PIN**.
5. Seleccionar un **tiempo de bloqueo de PIN**.
6. Seleccionar un **Modo fallback de puerta**:
 - **Sin acceso:** No se autoriza ningún acceso.
 - **Acceso código de sitio:** Se autoriza el acceso si la credencial coincide con uno de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta** y el código de instalación en la tarjeta coincide con el definido para el formato.
 - **Todo el acceso:** Se autoriza el acceso si la tarjeta coincide con cualquiera de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta**.
7. Seleccionar una opción de **Terminaciones de EOL entrada**.
8. Si una conexión SSH se ha activado en la etiqueta Configuración de red, hacer clic en **Ajustar contraseña para la cuenta de servicio de SSH** para ajustar una contraseña para que los usuarios remotos puedan acceder al sistema.
9. Seleccionar un **Controlador de puerta sencilla basado en IP Modo fallback**.
 - **Sin acceso:** No se autoriza ningún acceso
 - **Acceso código de sitio:** Se autoriza el acceso si la credencial coincide con uno de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta** y el código de instalación en la tarjeta coincide con el definido para el formato
 - **Todo el acceso:** Se autoriza el acceso si la tarjeta coincide con cualquiera de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta**.
 - **Usar tabla caché local:** El acceso se concede si la tarjeta coincide con una de las últimas 50 credenciales utilizadas para obtener con éxito el acceso.
10. (Recomendado) Dejar que la caja de selección **Encriptar las terminaciones de controladores de puerta sencilla basados en IP** encripte las comunicaciones entre el controlador del sistema y los controladores de puerta sencilla basados en IP y mejore la seguridad de datos
11. Hacer clic en [Aceptar cambios].

Configurar el idioma principal del sistema

Un idioma principal del sistema se puede definir en las etiqueta opciones del sistema de la página **Administración de sistema > Ajustes de sistema** para determinar el idioma usado para las funciones ejecutadas por el sistema, tales como la asignación de nombres para dispositivos por default, respaldos programados y correos electrónicos automatizados.

El idioma del sistema también se utiliza si una persona se conecta y selecciona un idioma que no está disponible actualmente, o si un usuario realiza una acción relacionada con el lenguaje (por ejemplo, la

carga de eventos en la página de **eventos**) y el idioma con el que el usuario se conectó ya no está disponible. Esto puede ocurrir si se remueve un paquete de idioma, cuando los usuarios están todavía registrados en el sistema.

Ajustar el idioma del sistema

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Opciones del sistema**.
3. Seleccionar un **Idioma del sistema**.
4. Hacer clic en [Aceptar cambios].

Configuración de los formatos de tarjeta

Las credenciales (tarjetas de identificación) que se usan para el control de acceso electrónico almacenan los datos en diferentes formatos. Para leer correctamente los datos, es necesario agregar el formato de tarjeta a la configuración. La ID de credencial almacenada en la tarjeta incluye un número de tarjeta, un código de instalación y un código de emisión.

Antes de que una credencial pueda ser reconocida, el sistema debe estar configurado para reconocer el formato de la tarjeta, es decir, la forma en que los datos se formatean en la ID de credencial. Se proporcionan cuatro formatos de tarjeta por default y más se pueden añadir. Sin embargo, el sistema debe ser configurado para reconocer sólo los formatos que se usen activamente.

Los formato de tarjeta por default que se proporcionan incluyen:

- 26 Bit (H10301) Wiegand código de instalación 200
- 32 Bits 14443 cascada 1
- 37 Bits (I10304) instalación 40
- 40 Bits CASI 4002

Notar los siguientes detalles sobre los formato de tarjeta:

- Si el sistema se actualiza de una versión anterior, los formatos de tarjeta existentes se conservan.
- El sistema está pre configurado para reconocer varios formatos de tarjeta comerciales y soporta hasta ocho formatos de tarjeta activos al mismo tiempo. Si un formato de tarjeta que se desea no está en la lista, se puede añadir como un tipo personalizado.
- Un *formato de tarjeta en bruto* no incluye el código de instalaciones, sino que trata todos los bits de datos de la tarjeta como parte de la credencial de acceso. Por consiguiente, las credenciales con formato sin procesar son más fáciles de configurar que las tarjetas que incluyen el código de instalación.
- Muchos formatos estándar incluyen el código de las instalaciones como parte de la ID de credencial. Esto permite una configuración de seguridad del lugar más sofisticada, pero también aumenta la complejidad de la configuración. Por ejemplo, si se usa un código de instalación y una puerta entra en modo fallback porque no puede comunicarse con el controlador del sistema, la puerta puede ser configurada para abrirse si una tarjeta con un código de instalación válido se escanea en la lectora. Esto se debe a que el controlador de las puertas no almacena la base de datos completa de las personas, pero puede almacenar el código de instalación.

Añadir un formato de tarjeta

1. Seleccionar **Administración del sistema > Formatos de tarjeta**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del formato**.
4. Seleccionar un **tipo de formato**.
5. Tipo de **código de instalación**, si es necesario.
6. Para un formato personalizado, escribir otros datos, según sea necesario.
7. Hacer clic en [Aceptar cambios].

Eliminar un Formato de tarjeta

1. Seleccionar **Administración del sistema > Formatos de tarjeta**.
2. Seleccionar el formato de tarjeta por remover.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configuración de dispositivos

Esta sección describe cómo configurar los siguientes dispositivos:

- Controlador del sistema
- Entradas y salidas
- Controladores de puertas
- Puertas
- Lectoras
- Módulos de expansión de entrada/salida

Para información sobre cómo configurar DVRs/NVRs y cámaras, consultar [Configuración de dispositivos de video](#) en pág. 35.

Antes de comenzar

Antes de configurar dispositivos en la página **Administración del sistema > Dispositivos**, completar los siguientes pasos:

1. Si hay controladores de puerta sencilla basados en IP instalados, se deben configurar para que reconozcan la dirección IP del controlador *antes* de configurar los controladores de puerta sencilla basados en IP en la interfaz del usuario. Al establecer esta conexión de red se asegura que el controlador de puerta sencilla basado en IP será detectado cuando el controlador del sistema escanea para cambios de hardware. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.
2. Usar el botón [Escanear para cambios de Hardware] para descubrir dispositivos, como se describe a continuación.
3. (Opcional, pero recomendado) Remplazar los nombres genéricos de dispositivos. Ver [Asignar nombres significativos al hardware](#) en pág. 24.

Escanear para cambios de hardware

Antes de configurar los dispositivos, hacer clic en el botón [Escanear para cambios de hardware] en la página **Administración del sistema > dispositivos** para descubrir los siguientes tipos de dispositivos propietarios localizados downstream del controlador del sistema y añadirlos automáticamente al árbol de dispositivos:

- Módulos de interfaz dual para puertas
- Módulos de expansión de entrada/salida
- Los controladores de puerta sencilla basados en IP que ya se han configurado para reconocer al controlador del sistema

Otra forma de agregar controladores de puertas en la página **Dispositivos** es seleccionar el controlador del sistema y hacer clic en [Añadir]. Seleccionar el tipo de controlador por añadir, llenar los campos restantes y hacer clic en [Aceptar cambios].

El sistema asignará nombres genéricos por default a los dispositivos que pueden ser personalizados más tarde (ver [Asignar nombres significativos al hardware](#) en pág. 24) y mostrar dispositivos en una jerarquía de árbol en la página **Administración del sistema > Dispositivos**. Algunos nombres por default se presentan en secuencia (por ejemplo, entrada11, entrada12, etc.). Las puertas y lectoras heredan el número de serie del controlador de puerta padre. Por ejemplo, si un controlador de puerta tiene el número de serie 1234, las puertas localizadas downstream del controlador de la puerta se nombrarán Puerta 1234-1, Puerta 1234-2, etc.

Nota: Si el número de serie de un controlador de puerta cambia (por ejemplo, si un controlador de puerta se reemplaza), todos los objetos hijos (puertas y lectoras) que aún usen los nombres por default deberán actualizarse para reflejar el nuevo número de serie del controlador de la puerta padre. Ver [Reemplazar un controlador de puerta](#) en pág. 27.

Para detectar dispositivos de hardware en el sistema:

IMPORTANTE: Los controladores de puerta estarán fuera línea durante el escaneo, que generalmente toma varios minutos.

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Seleccionar el controlador del sistema.
3. Hacer clic en [Escanear para cambios de hardware].
4. Hacer clic en [Aceptar cambios].

Si el sistema detecta cualquier problema (por ejemplo, si no hay una batería de respaldo instalada), aparecerá una notificación en una caja negra en la parte superior de la interfaz del usuario; hacer clic dentro de la caja para abrir la página **Administración del sistema > Diagnósticos** para más información sobre este problema. Ver [Diagnósticos](#) en pág. 110.

Asignar nombres significativos al hardware

Independientemente de si el sistema tiene pocos o muchos dispositivos de varios tipos, es necesario tener convenciones de nomenclatura eficaces para una implementación exitosa. El uso de nombres significativos y bien estructurados para entradas, salidas, controles de puertas, lectoras, etc. ayudará a:

- Identificar la ubicación y función de cada dispositivo.
- Organizar los dispositivos en grupos significativos.
- Ayudar al monitoreo de los eventos de acceso.

En lugar de utilizar nombres genéricos asignados a los dispositivos por el Asistente de instalación (por ejemplo, *controlador de puerta 8888*), utiliza los elementos pertinentes en cada nombre del dispositivo para proporcionar un marco de referencia sobre el tipo de dispositivo, ubicación u otra categoría significativa para una instalación, por ejemplo para un controlador de puerta *Vestíbulo principal, puertas en la pared al este*.

Nota: Si los nombres por default no se personalizan, recordar que cualquier cambio que se haga al nombre del objeto padre deberá hacerse a los objetos hijo (por ejemplo, las puertas y lectoras conectadas a un controlador de puerta) para evitar inconsistencias en los nombres de los dispositivos.

Antes de iniciar esta tarea, consultar la tabla de instalación creada cuando los dispositivos se instalaron, como se describe en [Documentación de la ubicación física de cada dispositivo](#) en pág. 5.

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Seleccionar el controlador del sistema.
3. Escribir un **Nombre del dispositivo** descriptivo.
4. Hacer clic en [Aceptar cambios].
5. Seleccionar el primer controlador de puertas de la lista.
6. Comparar el **Número de serie** con la tabla de instalación para confirmar que se haya seleccionado el dispositivo correcto en la interfaz del usuario.
7. Escribir un **Nombre del dispositivo** descriptivo.
8. Hacer clic en [Aceptar cambios].
9. Repetir el procedimiento para cada uno de los dispositivos en la jerarquía.

Configurar el controlador del sistema

El controlador del sistema puede aceptar cuatro entradas auxiliares de uso general y producir dos señales de salida de uso general, que deben activarse manualmente. Las entradas se pueden usar para accesorios tales como un detector de movimiento o para entradas de otros sistemas como, por ejemplo, un sistema de alarma de incendio. Se trata de configuraciones opcionales y solo deben activarse si están instaladas. Las entradas de uso general pueden configurarse para abrir todas las puertas automáticamente al ser disparadas, como en el caso de una alarma de incendio u otra emergencia.

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Seleccionar el controlador del sistema.
3. Hacer clic en la etiqueta **General**.
4. Seleccionar una **cámara enlazada**, si se ha configurado una para monitorear la ubicación física del controlador del sistema,
5. Hacer clic en la etiqueta **Entradas**.
6. Para cada entrada auxiliar de uso general que se conecta:
 - a. Seleccionar **Activado**.
 - b. Escribir un nombre significativo.
 - c. Seleccionar el **Tipo**.
 - d. (Opcional) Seleccionar **Desbloquear todas las puertas**, si la entrada pertenece a un sistema de alarma o emergencia.
 - e. (Opcional) Seleccionar una **Cámara enlazada**, si hay una asociada a la fuente de entrada (por ejemplo, una cámara asociada al detector de movimiento en un cuarto).

7. Hacer clic en la etiqueta **Salidas**.
8. Para cada salida auxiliar de uso general que se conecta:
 - a. Seleccionar **Activado**.
 - b. Escribir un nombre significativo.
 - c. Seleccionar **Encendido/apagado activo**, si el relé se energiza cuando la salida está apagada, de lo contrario, despejar la caja de selección.
 - d. (Opcional) Seleccionar una **Cámara enlazada** si hay una asociada con la salida.
9. Hacer clic en [Aceptar cambios].
10. Hacer clic en [Reiniciar controlador] para reiniciar el controlador del sistema.

Configurar entradas y salidas

Las entradas y salidas son las opciones de propósito general que pueden configurarse para satisfacer las necesidades de un sitio. Una entrada puede ser la señal de un detector de movimiento, por ejemplo. Una salida es un impulso eléctrico enviado por el controlador del sistema a algún dispositivo.

Usar la página **Administración del sistema > Dispositivos** para configurar entradas y salidas. Las entradas y salidas se monitorean desde la página **Monitoreo > Entradas/salidas**, desde donde se pueden activar manualmente las salidas. Las salidas también pueden controlarse por disparadores de acciones.

Configurar un controlador de puerta

Nota: Si hay cualesquier controladores de puerta sencilla basados en IP instalados, se deben configurar para que reconozcan la dirección IP del controlador del sistema *antes* de configurarlos en la interfaz del usuario. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.

Los controladores de puertas duales se pueden conectar a un máximo de cuatro lectoras en dos puertas. Los controladores de puerta sencilla basados en IP pueden conectarse a dos lectoras en una sola puerta. Cada puerta puede tener dos lectoras, una para entrar y una para salir, generalmente usadas con Anti-passback.

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Expandir el árbol debajo del controlador del sistema.
3. Seleccionar el Controlador de puertas.
4. Seleccionar la **Cantidad de puertas** conectadas a este controlador.
5. (Opcional) Seleccionar una **cámara enlazada**, si hay una asociada al panel del controlador de puertas.
6. Hacer clic en [Aceptar cambios].

Nota: Aunque todas las puertas estén bloqueadas al agregar un nuevo controlador de puerta, éste permanecerá desbloqueado. Para bloquearlo, se deben restablecer todas las puertas y entonces bloquearlas a todas nuevamente.

Reemplazar un controlador de puerta

IMPORTANTE: Si se reemplaza un controlador de puerta, asegurarse de actualizar los objetos hijos (puertas y lectoras) para que reflejen el número de serie nuevo del controlador de la puerta padre antes de usar el botón [Buscar cambios de hardware] en la página **Administración del sistema > Dispositivos**, como se describe a continuación. De otro modo, la información de configuración será sobrescrita.

Para reemplazar el controlador de puerta y conservar su información de configuración:

1. Respalidar la base de datos como se describe en [Crear una copia de Respaldo](#) en pág. 102.
2. Reemplazar la tarjeta de controlador de puerta.
3. (SÓLO PARA CONTROLADORES DE PUERTA SENCILLA BASADOS EN IP) Usar la herramienta de configuración integrada (ICT) para configurar el nuevo controlador de puerta sencilla basado en IP para que reconozca la dirección IP del controlador del sistema. Ver [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 121.
4. Actualizar el número de serie de la puerta del controlador en la página **Administración del sistema > Dispositivos**.
5. Si los objetos hijo (puertas y lectoras) aún usan los nombres por default, actualizarlos para que reflejen el número de serie nuevo del controlador de la puerta padre.
6. Reiniciar el controlador del sistema. Ver [Reiniciar el controlador del sistema](#) en pág. 110.
7. Reiniciar sesión después de que el controlador del sistema reinicie.
El controlador de puerta puede aparecer como fuera de línea hasta que logre conectarse con el controlador del sistema.
8. (Se recomienda) respaldar la base de datos y salvar la configuración actualizada con el número de serie nuevo después de que el controlador esté en línea. Ver [Respaldo de Datos](#) en pág. 101 y [Salvar y Restablecer los ajustes personalizados](#) en pág. 104.

Configurar puertas

Para cada puerta debe configurarse:

- El período de tiempo que debe permanecer desbloqueada cuando se presenta una credencial válida.
- El período de tiempo que se la puede mantener abierta antes de disparar una alarma.
- El tipo de cerradura usada (ya sea eléctrica estándar o con bloqueo magnético).
- Si se requiere una lectora solo para entrar o para entrar y salir.
- Los tipos de eventos y alarmas monitoreados por los circuitos de la puerta.
- Entradas y relés auxiliares. Por ejemplo, una puerta configurada con apertura automática y solicitud de salida (RTE) extendida, para facilitar el acceso de discapacitados.

Desbloquear una puerta

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Expandir el árbol debajo del controlador del sistema.
3. Expandir el árbol debajo del controlador de puertas.
4. Seleccionar la puerta por configurar.

Nota: Algunos campos no aparecerán en la página de **dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP, que no soporta los tipos de entrada/salida auxiliar o sabotaje de los puntos de entrada. Consultar la *referencia rápida de controlador de puerta sencilla basado en IP* para saber cómo modificar la configuración de los interruptores DIP para los tipos de entrada. Después de cambiar los ajustes del interruptor DIP, reiniciar el controlador de puerta sencilla basado en IP.

5. Seleccionar un **Período de acceso normal concedido**.
6. (Opcional) Seleccionar un **Periodo de acceso extendido concedido**.
7. Seleccionar el **Tiempo de puerta mantenida abierta**.
8. (Opcional) Seleccionar **Ampliación del tiempo de puerta mantenida abierta**.
9. Seleccionar un **Modo de cerradura de puerta**.
 - **Desbloqueo programado**
 - **Bloquear al cerrar**
10. (Opcional) Seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
11. Seleccionar un **Modo de acceso**.
12. (Opcional) Seleccionar **Solicitud de salida activada**, si la puerta está cableada al efecto.
13. (Opcional) Si está seleccionada **Solicitud de salida activada**, seleccionar **No activar apertura en RTE** para evitar que la cerradura de puerta se energice cuando se cierre el contacto de solicitud de salida.
14. (Opcional) Seleccionar las alarmas conectadas a la puerta:
 - **Puerta mantenida abierta**
 - **Puerta forzada abierta**
 - **Sabotaje**
15. (Opcional) Si se ha conectado una alarma visual o auditiva a la puerta, seleccionar "Puerta Mantenida/forzada" en la lista de **Relés auxiliares**.
16. Configurar los sensores **Tipos de entrada** para:
 - Sensor de **contacto de la puerta**
 - Botón o sensor de **Solicitud de salida**
 - Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
 - Circuitos **antisabotaje**

Nota: Las entradas auxiliares y de sabotaje listadas arriba no aplican a puertas conectadas a controladores de puerta sencilla basados en IP.

17. Hacer clic en [Aceptar cambios].
18. Repetir este procedimiento para cada puerta.

Configurar una puerta para el Acceso de discapacitados

Se registran eventos cada vez que las puertas se mantienen abiertas durante demasiado tiempo y cuando se autoriza el acceso, pero la puerta no se abre. Con una alarma visual o auditiva opcional, el sistema puede disparar una alarma física si se fuerza la puerta o se la mantiene abierta durante demasiado tiempo.

Para adaptarse a las necesidades de las personas que necesitan más tiempo para abrir o pasar a través de una puerta, el sistema permite a los usuarios identificar las credenciales autorizadas al efecto y configurar características opcionales en una puerta, tales como apertura automática y tiempo extra para los sensores de solicitud de salida. Esto se realiza de credencial en credencial, para preservar la

seguridad de las instalaciones, puesto que cuanto más tiempo una puerta se mantiene abierta, más fácil es que alguien entre sin presentar una credencial. Ver [Añadir una credencial en la página 79](#).

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Expandir el árbol debajo del controlador del sistema.
3. Expandir el árbol bajo controlador de puertas.
4. Seleccionar la puerta a configurar.

Nota: Algunos campos no aparecerán en la página de **dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP, que no soporta los tipos de entrada/salida auxiliar o sabotaje de los puntos de entrada. Consultar la *referencia rápida de controlador de una sola puerta basado en IP* para saber cómo modificar la configuración de los puentes para los tipos de entrada.

5. Seleccionar un [Período de acceso normal concedido](#).
6. Seleccionar una [Extensión del período de acceso concedido](#).
Este es el período de tiempo que la puerta permanece desbloqueada para que la persona la pueda abrir.
7. Seleccionar el [Tiempo de puerta mantenida abierta](#).
8. Seleccionar una [Extensión del tiempo de puerta mantenida abierta](#).
Este es el período de tiempo que la puerta puede permanecer abierta para que la persona la atraviese.
9. Seleccionar un **Modo de cerradura**.
 - [Desbloqueo programado](#)
 - [Bloquear al cerrar](#)
10. (Opcional) Seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
11. Seleccionar un [Modo de acceso](#).
12. (Opcional) Seleccionar [Solicitud de salida activada](#), si la puerta está cableada al efecto.
13. (Opcional) Si está seleccionada [Solicitud de salida activada](#), seleccionar [No activar apertura en RTE](#) para evitar que la cerradura de puerta se energice cuando se cierre el contacto de solicitud de salida.
14. (Opcional) Seleccionar las alarmas conectadas a la puerta:
 - [Puerta mantenida abierta](#)
 - [Puerta forzada abierta](#)
 - [Sabotaje](#)
15. Si la puerta está conectada a un dispositivo de apertura automática:
 - a. Seleccionar "RTE Extendido" en la lista de [Entradas auxiliares](#).
 - b. Seleccionar "[Apertura automática](#)" en la lista de [Entradas auxiliares](#).
 - c. Seleccionar un [Tiempo de activación del relé auxiliar](#).
16. Configurar los sensores [Tipos de entrada](#) para:
 - Sensor de **Contacto de la puerta**
 - Botón o sensor de **Solicitud de salida**
 - Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
 - Circuitos **Antisabotaje**

Nota: Las entradas auxiliares y de sabotaje listadas arriba no aplican a puertas conectadas a controladores de puerta sencilla basados en IP.

17. Hacer clic en [Aceptar cambios].
18. Repetir este procedimiento para cada puerta.

Configurar una puerta con bloqueo magnético

- **ADVERTENCIA!** • Al configurar una puerta con bloqueo magnético, es importante usar la opción "Sensor de conexión del bloqueo magnético" para evitar que los imanes de la puerta se activen antes de tiempo y cierren la puerta de golpe, lo que puede causar lesiones.

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Expandir el árbol debajo del controlador del sistema.
3. Expandir el árbol bajo controlador de puertas.
4. Seleccionar la puerta a configurar.

Nota: Algunos campos no aparecerán en la página de **dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP, que no soporta los tipos de entrada/salida auxiliar o sabotaje de los puntos de entrada. Consultar la *referencia rápida de controlador de una sola puerta basado en IP* para saber cómo modificar la configuración de los puentes para los tipos de entrada.

5. Seleccionar un **Período de acceso normal concedido**.
6. Seleccionar una **Extensión del período de acceso concedido**.
Este es el período de tiempo que la puerta permanece desbloqueada para que la persona la pueda abrir.
7. Seleccionar el **Tiempo de puerta mantenida abierta**.
8. Seleccionar una **Extensión del tiempo de puerta mantenida abierta**.
Este es el período de tiempo que la puerta puede permanecer abierta para que la persona la atraviese.
9. Seleccionar un **Modo de cerradura**.
 - **Desbloqueo programado**
 - **Bloquear al cerrar**
10. (Opcional) Seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
11. Seleccionar un **Modo de acceso**.
12. (Opcional) Seleccionar **Solicitud de salida activada**, si la puerta está cableada al efecto.
13. (Opcional) Si está seleccionada **Solicitud de salida activada**, seleccionar **No activar apertura en RTE** para evitar que la cerradura de puerta se energice cuando se cierre el contacto de solicitud de salida.
14. (Opcional) Seleccionar las alarmas conectadas a la puerta:
 - **Puerta mantenida abierta**
 - **Puerta forzada abierta**
 - **Sabotaje**
15. Seleccionar "**Sensor de conexión del bloqueo magnético**" en la lista de **Entradas auxiliares**.
16. (Opcional) Si una luz de alarma o claxon está conectada a la puerta, seleccionar "Puerta mantenida/forzada" desde la lista **Aux de relé**.
17. Configurar los sensores **Tipos de entrada** para:
 - Sensor de **Contacto de la puerta**
 - Botón o sensor de **Solicitud de salida**

- Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
- Circuitos **Antisabotaje**

Nota: Las entradas auxiliares y de sabotaje listadas arriba no aplican a puertas conectadas a controladores de puerta sencilla basados en IP.

18. Hacer clic en [Aceptar cambios].

19. Repetir este procedimiento para cada puerta.

Opciones de configuración de puertas

Período Normal de Acceso Autorizado

Cuando una lectora escanea una credencial válida, la puerta se desbloquea durante el tiempo seleccionado.

Nota: Las cerraduras inalámbricas Schlage AD-400 ignoran este ajuste. Configurar el valor **Volver a bloquear después** en el software del utilitario Software en su lugar. Ver la *Referencia rápida cerraduras inalámbricas TruPortal* para más detalles.

Ampliación del período de acceso autorizado

Cuando se selecciona una credencial válida con la opción **Usar tiempo extendido de apertura/mantenido abierto** (de acuerdo a la configuración en la página **Administración de acceso > Personas**) y es escaneada por la lectora, la puerta se desbloqueará para el **Tiempo de acceso concedido normal** más el **Tiempo de acceso concedido extendido**. Esto permite configurar el sistema de modo de cumplir la legislación y los reglamentos que rigen el acceso de personas con discapacidad.

Nota: Las cerraduras inalámbricas Schlage AD-400 ignoran este ajuste. Configurar esta característica en el utilitario software Schlage en su lugar. Ver la *Referencia rápida de cerraduras inalámbricas TruPortal* para más detalles.

Tiempo de puerta mantenida abierta

Cuando una lectora escanea una credencial válida, la puerta se puede mantener abierta durante el **Tiempo de acceso concedido normal** más el **Tiempo puerta mantenida abierta** allí seleccionado. Si una puerta se mantiene abierta durante más tiempo que el especificado, se registra un evento y se selecciona la opción alarma **Puerta mantenida abierta**.

Tiempo ampliado de puerta mantenida abierta

Cuando se selecciona una credencial válida con la opción **Usar tiempo extendido de apertura/mantenido abierto** (de acuerdo a la configuración en la página **Administración de acceso > Personas**) y la credencial es escaneada por la lectora, la puerta se puede mantener abierta para el **Tiempo de acceso concedido normal** más el **Tiempo de puerta mantenida abierta extendido**. Si una puerta se mantiene abierta durante más tiempo que el especificado, se registra un evento y se selecciona la opción alarma **Puerta mantenida abierta**. Esto permite configurar el sistema de modo de cumplir la legislación y los reglamentos que rigen el acceso de personas con discapacidad.

Solicitud de salida activada

Si la puerta cuenta con alarma por violación, mantenida abierta demasiado tiempo y sabotaje, se debe usar Solicitud de salida (RTE), conjuntamente con un botón que se presiona para salir, una lectora de salida o algún tipo de sensor que detecta la aproximación a la puerta desde el interior. De lo contrario, cada vez que alguien sale, se dispara una alarma de puerta forzada.

No activar apertura en solicitud de salida RTE

Un contacto de solicitud de salida RTE generalmente es un botón localizado cerca de la puerta asociada. Seleccionar para evitar que la apertura de puerta se energice al cerrarse el contacto de solicitud de salida RTE. Cuando una tarjeta habiente presiona el botón, se envía una RTE al controlador del sistema. (Las solicitudes RTE también se conocen como REX.)

Si esta caja está seleccionada, la apertura de puerta NO se energiza cuando se cierra el contacto de solicitud de salida. Si esta caja no está seleccionada, la apertura de puerta se energiza cuando se cierra la solicitud de salida RTE.

Modo de cerradura de puerta**Desbloqueo programado**

La puerta se desbloquea cuando se autoriza el acceso y permanece desbloqueada hasta que expira el período especificado en **Período normal de acceso autorizado**.

Si la **entrada auxiliar** de la puerta está configurada con Sensor de conexión del bloqueo magnético, el relé de apertura permanece activo hasta que se activa el sensor de conexión magnética, se cierra el contacto de la puerta y expira el tiempo de desbloqueo.

Nota: Los controladores de puerta sencilla basados en IP no soportan entrada y salida Aux. Las cerraduras inalámbricas Schlage AD-400 ignoran este ajuste.

Bloquear al cerrar

La puerta se desbloquea cuando se autoriza el acceso y permanece desbloqueada hasta que expira el período especificado en **Período normal de acceso autorizado** o se abre y cierra la puerta, lo que tenga lugar primero.

Si la **entrada auxiliar** de la puerta está configurada con *Sensor de conexión del bloqueo magnético*, el relé de apertura permanece activo hasta que se activa el sensor de conexión magnética y se cierra el contacto de la puerta, independientemente del tiempo de desbloqueo.

Nota: Los controladores de puerta sencilla basados en IP no soportan entrada y salida Aux. Las cerraduras inalámbricas Schlage AD-400 ignoran este ajuste.

Modo de acceso**Lectora solo para entrar**

La puerta tiene una lectora para escanear credenciales para entrar, pero no requiere la presentación de credenciales para salir.

Lectora para entrar y lectora para salir

La puerta tiene lectoras para escanear credenciales para entrar y para salir. Esta configuración es necesaria para la función Anti-passback.

Alarma activada**Puerta mantenida abierta**

Seleccionar esta opción si la puerta está cableada de modo de detectar que está abierta. Si se mantiene abierta durante más tiempo que el seleccionado en **Tiempo de puerta mantenida abierta**, se registra un evento en la página **Eventos**.

Puerta forzada abierta

Seleccionar esta opción si la puerta está cableada para detectar una entrada forzada. Si una persona abre la puerta, sin presentar una credencial con acceso autorizado, se registra un evento en la página **Eventos**. Si se desea que se dispare una alarma física cuando la puerta es forzada, configurarla con una alarma visual o auditiva cableada al **relé auxiliar**.

Sabotaje

Seleccionar esta opción si la puerta está cableada para detectar sabotaje de lectora. En caso de sabotaje, se registra un evento en la página **Eventos**.

Nota: La opción de **sabotaje** solamente controla el punto de entrada de sabotaje, no el contacto de puerta, solicitud de salida o puntos de entrada auxiliar. También esta opción no aparecerá en la página del **Sistema Administración > Dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP, que no soporta sabotaje de entrada de lectora.

Entrada auxiliar

Nota: Este campo no aparecerá en la página del **Sistema Administración > Dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP, que no soporta tipos de entrada/salida auxiliar. Consultar la *referencia rápida de controlador de una sola puerta basado en IP* para saber cómo modificar la configuración de los puentes para los tipos de entrada.

Ninguno

Indica que la entrada no se usa ni se monitorea.

Solicitud de salida extendida

Concebida para uso únicamente con la opción Apertura automática seleccionada en **Relés auxiliares**.

Sensor de conexión del bloqueo magnético

Diseñada para puertas que usan una cerradura magnética en lugar de apertura de puerta. Detecta la señal de salida del bloqueo magnético que indica que la puerta se ha conectado con el imán. El sistema no activa el imán hasta que el sensor de conexión de la puerta envía una señal que indica que la puerta se conectó con el imán y el sensor de contacto de la puerta indica que la puerta está cerrada. De este modo se evita que el imán se active antes de tiempo y la puerta se cierre de golpe.

Si "Desbloqueo programado" es el **Modo de cerradura de puerta** seleccionado, el imán permanece inactivo hasta que expira el período determinado. De cualquier modo, no se activa hasta que se reciben las señales del sensor de conexión magnética y del sensor de contacto de la puerta, indicando que la puerta está cerrada y conectada al imán.

Relé auxiliar

Nota: Este campo no aparecerá en la página del **Sistema Administración > Dispositivos** si una puerta está conectada a un controlador de puerta sencilla basado en IP que no soporta tipos de entrada/salida auxiliar. Consultar la *Referencia rápida de controlador de una sola puerta basado en IP* para saber cómo modificar la configuración de los puentes para los tipos de entrada.

Ninguno

Indica que el relé no se usa ni se energiza.

Puerta mantenida/forzada

Un uso típico de esta opción es hacer que el relé dispare una alarma física, visual o auditiva, cuando se sujeta o se viola la puerta.

Abridor de puerta

Por lo general, se usa con una puerta configurada con una sola lectora de entrada y un dispositivo manual de liberación cableado para Solicitud de salida (RTE) y un pulsador para apertura automática de RTE extendida. La entrada de RTE abre la puerta durante el tiempo que el dispositivo manual de liberación está activo, suficiente para que una persona salga con normalidad. La entrada auxiliar (RTE extendida) activa el relé auxiliar durante el Tiempo especificado de activación del relé auxiliar. Esta salida de relé activa el dispositivo de apertura automática de la puerta, que la desbloquea y la abre para dejar pasar a una persona con necesidades especiales.

Esta configuración solo tiene sentido si la **entrada auxiliar** está configurada para RTE extendida.

Tipos de entrada**NA (normalmente abierto)**

El contacto del sensor está normalmente abierto.

NC (normalmente cerrado)

El contacto del sensor está normalmente cerrado.

No supervisado

El circuito no está cableado con un circuito de continuidad para detectar sabotaje.

Supervisada

El circuito está cableado con un circuito de continuidad para detectar sabotaje.

Nota: Para controladores de puerta sencilla basados en IP, consultar la *Referencia rápida del controlador de una sola puerta basado en IP* para información sobre cómo configurar los ajustes del puente sobre la base de la selección del tipo de entrada.

Configurar las lectoras

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Expandir el árbol debajo del controlador del sistema.
3. Expandir el árbol bajo controlador de puertas.
4. Expandir el árbol debajo de la puerta.
5. Seleccionar la lectora a configurar.
6. Seleccionar un **Método de acceso**.
 - **Solo credencial**
 - **Credencial y PIN**
7. Seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta y la lectora.
8. Hacer clic en [Aceptar cambios].
9. Repetir este procedimiento para las otras lectoras.

Configuración lectora Opciones**Solo Credencial**

Para acceder, solo es necesario presentar una credencial válida (ID de credencial).

Credencial y PIN

Para acceder, es necesario presentar una credencial válida y un número de identificación personal. Esto impide el acceso con una credencial robada o encontrada. Algunas instalaciones

usan el modo **Solo credencial** durante el día y **Credencial y PIN** fuera del horario laboral, cuando las instalaciones están vacías.

Configurar los módulos de expansión de E/S

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Seleccionar expansor de E/S.
3. Hacer clic en la etiqueta **General**.
4. Seleccionar una **cámara enlazada**, si se ha configurado una para monitorear la ubicación física del controlador del sistema,
5. Seleccionar **Alarma de sabotaje activada**, si el gabinete está cableado para detectar sabotajes.
6. Hacer clic en la etiqueta **Entradas**.
7. Para cada entrada auxiliar de uso general que se conecta:
 - a. Seleccionar **Activado**.
 - b. Escribir un nombre significativo.
 - c. Seleccionar el **Tipo**.
 - d. (Opcional) Seleccionar **Desbloquear todas las puertas**, si la entrada pertenece a un sistema de alarma o emergencia.
 - e. (Opcional) Seleccionar una **cámara enlazada**, si hay una asociada a la fuente de entrada (por ejemplo, una cámara asociada al detector de movimiento en un cuarto).
8. Para cada salida auxiliar de uso general que se conecta:
 - a. Seleccionar **Activado**.
 - b. Escribir un nombre significativo.
 - c. Seleccionar **Encendido/apagado activo**, si el relé se energiza cuando la salida está apagada, de lo contrario, despejar la caja de selección.
 - d. (Opcional) Seleccionar una **Cámara enlazada** si hay una asociada con la salida.
9. Hacer clic en [Aceptar cambios].

Configuración de dispositivos de video

Las grabaciones de video de eventos de acceso pueden ser revisados por el acceso al video grabado en una DVR / NVR de las cámaras asociadas a un dispositivo conectado al controlador del sistema. Cuando se produce un evento en un dispositivo, el sistema mantiene un registro de la fecha y hora del evento. Si hay una cámara enlazada a ese dispositivo, el sistema usa la fecha y hora del evento para crear un hipervínculo a un video grabado por la DVR/ conectada a la cámara.

Enlazar una cámara a un dispositivo permite que el sistema asocie un evento producido en tal dispositivo al video grabado a través de la cámara durante el tiempo del evento. El sistema no controla la cámara ni la DVR/NVR directamente, sino que usa la información para transmitir a la DVR/NVR la fecha, la hora y la cámara que grabó el video, para reproducirlo.

Las cámaras de video vigilancia pueden ser de dos tipos generales: fija o con movimiento horizontal, vertical y zoom (PTZ). Los usuarios pueden controlar las cámaras PTZ cameras si:

- Se está usando Internet Explorer como navegador,
- Microsoft .NET Framework 4.5 (o más reciente) está instalado,
- Los controles ActiveX están activados en el navegador y
- La cámara está conectada a una DVR/NVR.

Añadir una DVR/NVR

Antes de añadir una DVR/NVR, consultar las notas de la versión para determinar la revisión mínima requerida del firmware. Consultar la documentación de la DVR/NVR para instrucciones de cómo actualizar el firmware.

1. Seleccionar **Administración de Sistema > Dispositivos > Dispositivos de Video**.
2. Hacer clic en [Agregar] y seleccionar el modelo adecuado de DVR/NVR.
3. Escribir un nombre descriptivo en el campo **Nombre del dispositivo**.
4. Escribir la **dirección IP** del dispositivo.
5. Escribir el **nombre de usuario** para iniciar sesión en el dispositivo.
6. Escribir la **contraseña** para iniciar sesión en el dispositivo.
7. Hacer clic en [Aceptar cambios].
8. Hacer clic en el siguiente enlace **Configuración y control del navegador web** para confirmar la conexión y comprobar la configuración de las cámaras conectadas al dispositivo.

Añadir una cámara de video

Antes de llevar a cabo esta tarea, se debe añadir una DVR/NVR al sistema.

1. Seleccionar **Administración de Sistema > Dispositivos > Dispositivos de Video**.
2. Seleccionar la DVR/NVR con la cámara por añadir.
3. Seleccionar **Añadir > cámara**.
4. Escribir un nombre descriptivo en el campo **Nombre del dispositivo**.
Por ejemplo, "Cámara del vestíbulo principal".
5. Seleccionar la **Entrada de DVR** correcta.
Es el canal en la DVR/NVR al que se conecta físicamente la cámara.
6. Seleccionar un **Ancho de banda del flujo de video**.
Si se desconoce el ancho de banda, iniciar sesión en la interfaz basada en navegador de la DVR/NVR y examinar los ajustes para la cámara.
7. Escribir la **Duración de la reproducción previa al evento** deseada.
Es la cantidad de tiempo previo al evento que desea ver en la reproducción. Por ejemplo, un evento de puerta forzada se registra en el sistema al forzar la puerta, sin embargo, la persona que forzó la puerta puede haberla saboteado durante varios segundos antes de lograr forzarla.

También se puede ajustar una cámara para monitoreo de la ubicación física en el controlador del sistema. Referirse a [Configurar el controlador del sistema](#) en pág. 25.

Añadir plantillas video

Las plantillas de video determinan cuántas entradas de cámara se pueden monitorear simultáneamente desde la pantalla de la computadora.

1. Seleccionar **Monitoreo > Plantillas video**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre diseño de video**.
Por ejemplo, si hay cuatro cámaras vigilando la zona de la plataforma de carga, es posible crear una plantilla 2x2 y llamarla "Cámaras de la plataforma de carga".
4. Seleccionar un **Tipo diseño de video**.
5. Seleccionar una cámara para cada celda de la plantilla.
6. Hacer clic en [Aceptar cambios].

Enlazar las cámaras a los dispositivos de rastreo de video de eventos

Las lectoras generan eventos de acceso autorizado y acceso denegado, por lo que, si se vincula una cámara a una lectora, los usuarios tienen un registro visual de cada persona que entró (o a la cual se le denegó la entrada) por esa lectora.

Las puertas generan eventos si se las fuerza, se las mantiene abiertas durante demasiado tiempo y en caso de desbloqueo momentáneo, por lo que, si se enlaza una cámara a una puerta, los usuarios tienen un registro de cada incidente de seguridad de acceso.

Entradas y salidas auxiliares son dispositivos opcionales conectados al controlador del sistema o a un módulo de expansión de E/S. Para enlazar una cámara a estos dispositivos, se debe hacerlo a través de la etiqueta Entrada o Salida del controlador del sistema correspondiente.

1. Conectar el sistema (a través de la red TCP/IP) a la DVR/NVR y a la cámara.
 - a. Ver [Añadir una DVR/NVR en la página 36](#).
 - b. Ver [Añadir una cámara de video en la página 36](#).
2. Seleccionar **Administración del sistema > Dispositivos**.
3. Seleccionar el dispositivo desde el árbol por jerarquía.
4. Seleccionar la cámara adecuada en la lista **cámara enlazada**.

Configurar Áreas

Las zonas representan espacios en el plano físico de las instalaciones, específicamente las entradas y salidas a esos espacios. La definición de áreas permite a los usuarios identificar cuáles lectoras conducen al interior de esos espacios y cuáles lectoras conducen al exterior de esos espacios y al interior de las áreas adyacentes. Las áreas se usan para rastrear la ubicación física de las personas en las instalaciones, lo que puede verse en el Informe de nómina, y para rastrear el Anti-passback (APB) de las credenciales.

Agregar una área

Antes de asignar lectoras a un área, se debe crear el área.

1. Seleccionar **Administración de acceso > Áreas > Definición de áreas**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del área**.
4. Seleccionar una opción **Reajuste automático anti-passback**.
Si “Nunca” está seleccionado, se ajustará una violación de Anti-passback manualmente.
5. Hacer clic en [Aceptar cambios].

Asignar lectoras a las áreas

La asignación de lectoras a las áreas es lo que define las áreas en el sistema. El sistema registra qué lectora escanea una credencial y, sobre la base de la asignación de zonas, señala la zona en que la persona con esa credencial debe estar y por cuáles lectoras debe pasar antes de trasladarse a otra zona.

IMPORTANTE: Comprobar la correcta asignación de las lectoras. Si se detecta una credencial en una lectora que no es contigua a la última lectora, se dispara una violación de Anti-passback. Por ejemplo, si el laboratorio A da al pasillo principal y está físicamente configurado de modo que la lectora 1 autoriza el acceso y la lectora 2, la salida, pero, por error un usuario, asigna la lectora 3 para salida, cada persona que intente salir del laboratorio A violará el Anti-passback.

1. Seleccionar **Administración de acceso > Áreas > Asignación de lectoras**.
2. Para cada lectora:
 - a. Seleccionar el **Área de partida**. Esta es el área en la que se encuentra la lectora.
 - b. Seleccionar el **Área de llegada**. Esta es el área en la que la persona va a entrar, una vez que la lectora acepte su credencial.
 - c. Seleccionar **Anti-passback**:
 - Ninguno
 - Tolerante
 - Riguroso
3. Hacer clic en [Aceptar cambios].

Remover una Área

Nota: No se puede eliminar la zona predeterminada.

1. Seleccionar **Administración de acceso > Áreas > Definición de áreas**.
2. Seleccionar área por remover.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configurar Anti-passback

El Anti-passback requiere que se use una credencial para entrar y salir del área de tal manera que el sistema sepa cuál área está ocupando actualmente el tarjeta habiente. El sistema mantiene un registro de los movimientos de personal en las áreas de seguridad, y evita el paso a las áreas que son lógicamente imposibles.

Si una persona usa una credencial para entrar en una área configurada como Anti-passback y, luego, sale sin usar la credencial (a través de una puerta mantenida abierta por otra persona, por ejemplo), el controlador no sabe que la persona ha salido de esa área específica. Como resultado, si el sistema está configurado para imponer el Anti-passback obligatorio, impide que esa credencial se use para entrar en otra área, incluyendo la que recién se dejó, hasta que la ubicación de la credencial se restablezca a una área neutra o por default.

Opciones de Anti-passback

Una violación de Anti-passback tiene lugar cuando una persona presenta una credencial (tarjeta de identificación) para entrar en una zona, pero de algún modo sale de la zona sin presentar la identificación. El evento se dispara cuando la persona trata de entrar en otra zona, no conectada físicamente a la última zona en la que se sabe que estuvo.

Ninguno

No se usa la función Anti-passback.

Tolerante

Se registra un evento cuando una credencial viola las reglas del Anti-passback.

Riguroso

La credencial que infringe el Anti-passback no puede acceder a ninguna área, hasta que la ubicación de la credencial se restablece a una área neutra o por default.

Configurar el Anti-passback

Para configurar el Anti-passback, hay que añadir al sistema áreas que coinciden con las áreas de las instalaciones, asignar las lectoras a esas áreas y añadir credenciales.

1. Ver [Agregar una área en la página 39](#).
2. Ver [Asignar lectoras a las áreas en la página 39](#).
3. Ver [Añadir una credencial en la página 79](#).

Nota: El panel Credenciales de la página Personas (**Administración de acceso > Personas**) permite exceptuar de los requisitos de Anti-passback a credenciales individuales.

Creación de grupos de feriados

Los feriados son excepciones en los horarios del lugar de trabajo. La creación de un grupo de estos días dará lugar a que el sistema anule el horario normal durante esos días. Si un feriado no debe sobrescribir cierto programa, entonces el grupo de feriados debe incluirse en ese programa.

Por ejemplo, las instalaciones pueden abrir de lunes a viernes a excepción de ciertos feriados anuales, cuando solo el personal de limpieza y los administradores de red deben tener acceso a las instalaciones. El personal de limpieza puede hacer una limpieza a fondo cuando las instalaciones están cerradas para las actividades normales. Los administradores de red pueden usar los feriados para hacer servicios de mantenimiento y actualización que causarían trastornos en un día normal de trabajo.

Para adaptarse a estas necesidades, crear un grupo de feriados para esos días en los que el personal regular no trabaja. Es decir, hay que crear dos programas y dos niveles de acceso, uno para el personal de oficina y otro para el personal de apoyo (personal de limpieza y administradores de red). Incluir el grupo de feriados en el horario del personal de apoyo, pero no en el horario regular del personal de oficina. Por default, cuando un grupo de feriados se crea, automáticamente se "excluye" de los programas y durante ese feriado el programa no opera.

Al configurar el nivel de acceso del personal de apoyo, asignar el horario del personal de apoyo a las lectoras y los grupos de lectoras que el personal de apoyo va a usar. (Recordar "incluir" el grupo de feriados seleccionándolo en el programa de manera que este grupo de personas tendrá acceso concedido durante el feriado.) Al configurar el nivel de acceso del personal regular, asignar el horario del personal regular a las lectoras y los grupos de lectoras que el personal regular de oficina va a usar.

Tomar nota de los detalles a continuación sobre cómo impactan los feriados a los programas:

- Cuando la fecha se designa como feriado, el sistema hace una excepción a todas las operaciones normales en esa fecha en particular o conjunto de fechas a menos de que se haya creado una programación personalizada para surtir efecto en la misma fecha.
Por ejemplo, si una puerta está programada para abrir automáticamente todos los días de 8:00 am a 5:00 pm, esa puerta permanecerá cerrada en un día feriado en vez de desbloquearse como lo haría normalmente. Otro ejemplo se produce cuando una persona normalmente tiene acceso con tarjeta a una puerta especial los miércoles y un feriado programado se produce en un miércoles, esa persona no puede acceder a la puerta ese día.
- Para hacer una excepción para una persona que necesita acceso al edificio en un día festivo, esa persona debe estar asignada a un programa que está excluido del grupo de feriados.
Por ejemplo, para conceder a una persona el acceso al edificio el día de Navidad, ajustar el nivel de acceso de la persona (por ejemplo, un nivel de acceso denominado "personal de apoyo"), enlazar el nivel de acceso a un programa específico (por ejemplo, un programa de llamado "24/7"), y luego ajustar el horario 24/7 para incluir el feriado día de Navidad.
- Para realizar un desbloqueo programado en un feriado, añadir el feriado a un programa que se asigna a una puerta en particular.

Añadir un grupo de feriados

IMPORTANTE: La creación de un grupo de feriados tendrá efecto inmediatamente. Los feriados añadidos a este grupo serán excluidos de TODOS los programas removiendo así los días especificados de las operaciones normales en esa fecha en particular o conjuntos de fechas y causando que el sistema sobrescriba el programa regular. Referirse a [Creación de grupos de feriados](#) en pág. 41 para más información.

1. Seleccionar **Administración de acceso > Feriados**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del grupo de feriados**.
Por default, un grupo nuevo de feriados contiene un feriado.
 - a. Eligir la fecha y el patrón del feriado:
 - **Único:** un evento que se produce una sola vez.
 - **Se repite todos los años:** un evento que ocurre en la misma fecha todos años, tal como el 25 de diciembre.
 - **Personalizados:** un evento que se repite anualmente en un patrón específico, como el Viernes Santo.
 - b. Para un feriado único o uno que se repite, escribir el día de inicio en el campo **Fecha**, o hacer clic en el icono **Calendario** junto al campo **Fecha** para seleccionar una fecha de la ventana temporal Calendario.
 - c. Escribir el tipo y número de días que dura el feriado en el campo **Duración**. (Por default, un feriado nuevo dura un día. Valores válidos son de 1 a 366.)
4. Para agregar un feriado al grupo, hacer clic en [Añadir] en el panel Lista de feriados y repetir los pasos [paso a](#) al [paso c](#).
5. Hacer clic en [Aceptar cambios].

Agregar un feriado a un grupo de feriados

1. Seleccionar **Administración de acceso > Feriados**.
2. Seleccionar un grupo de feriados por modificar.
3. Agregar un feriado al grupo:
 - a. Hacer clic en [Agregar] en el panel Lista de feriados.
4. Crear intervalos para el horario.
 - a. Para crear intervalos adicionales, hacer clic en [Añadir] en el panel Lista de intervalos.
 - b. Hacer clic en la caja de selección correspondiente a cada día por añadir al intervalo.
 - c. Escribir los valores de la hora de inicio y de fin.
 - d. Para un feriado único o uno que se repite, escribir el día de inicio en el campo **Fecha**, o hacer clic en el icono **Calendario** junto al campo **Fecha** para seleccionar una fecha de la ventana temporal Calendario.
 - e. Escribir el tipo y número de días que dura el feriado en el campo **Duración**.
5. Hacer clic en [Aceptar cambios].

Copiar un grupo de feriados

1. Seleccionar **Administración de acceso > Feriados**.
2. Seleccionar un grupo de feriados por copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del grupo de feriados**.
5. Hacer los cambios necesarios en los feriados en el grupo copiado.
6. Hacer clic en [Aceptar cambios].

Remover un grupo de feriados

Nota: No se puede eliminar un grupo de feriados en uso.

1. Seleccionar **Administración de acceso > Feriados**.
2. Seleccionar un grupo de feriados por remover.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Creación de programas

Los programas se usan para determinar cuándo una lectora le autorizará el acceso a una persona, o cuándo una puerta se bloquea o desbloquea automáticamente. Es posible crear hasta 64 programas y usrls en el sistema, incluyendo los programas predeterminados a continuación:

- Todos los días las 24 horas del día
- Lunes a viernes 8AM-5PM (8.00 a 17.00)
- Lunes a viernes 9AM-6PM (9.00 a 18.00)
- Fines de semana 7AM-7PM (7.00 a 19.00)

Un *intervalo* es el período de tiempo durante el cual un horario está activo. Los programas pueden incluir múltiples intervalos. Por ejemplo, si el personal de limpieza de la oficina lava y aspira los pisos los miércoles, pero los demás días de la semana solo limpia los baños y los cestos de basura, necesitan tener acceso durante más horas el miércoles que los otros días de la semana. En este caso, se crea un intervalo para el miércoles y otro para los demás días de la semana.

Notar los siguientes detalles sobre los programas:

- En los programas, el tiempo se expresa en horas y minutos, sin segundos, pero la hora de inicio de un período corresponde al comienzo del minuto (0 segundos) y la hora de término de un período corresponde al final del minuto (59 segundos). En el programa predefinido 24/7, se nota que la hora de inicio es 12:00 AM (24.00) y la hora de término es 11:59 PM (23.59). Expresado en segundos, la hora de inicio es 12:00:00 AM y la hora de término es 11:59:59 PM, con una

diferencia de un segundo. Un programa que pasa la medianoche debe ser configurado de esta manera, porque si se introduce 12:00 AM como hora de inicio y fin, el programa se activa durante solo 59 segundos (de 12:00:00 a 12:00:59).

- Los disparadores de acciones, programas y control manual pueden impactar el estado de los dispositivos y son tratados igualmente por el sistema. La última operación ejecutada determina el estado del dispositivo.
- Cuando la fecha se designa como feriado, el sistema hace una excepción a todas las operaciones normales en esa fecha en particular o conjunto de fechas a menos de que se haya creado una programación personalizada para surtir efecto en la misma fecha. Referirse a [Creación de grupos de feriados](#) para información sobre cómo impactan los feriados a los programas.
- Los programas para controlar los períodos de acceso de las lectoras se asignan a través de la página **Administración de acceso > Niveles de acceso**.
- Los programas para controlar el bloqueo de las puertas se asignan a través de la página **Monitoreo > Puertas**.

Agregar un programa

1. Seleccionar **Administración de acceso programas**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del programa**.
4. Hacer clic en **Grupos de feriados**.
5. Seleccionar los grupos de feriados incluidos en este programa.

Nota: Los feriados son excepciones de los programas normales de acceso. Al incluir un grupo de feriados en un programa se evita que el grupo de feriados lo anule. Por ejemplo, si se crea un grupo de feriados para feriados bancarios y la oficina está cerrada esos días, el grupo de feriados no deberá estar seleccionado para el programa para el nivel de acceso de los trabajadores de la oficina. Sin embargo, si el departamento de despacho trabaja los feriados, se podría seleccionar el grupo de feriados bancarios para el horario relativo al nivel de acceso del personal de despacho, a fin de evitar que el grupo de feriados bancarios anule el horario del departamento de despacho.

6. Hacer clic en [Aceptar cambios].

Agregar un intervalo a un programa

1. Seleccionar **Administración de acceso programas**.
2. Seleccionar el horario a modificar.
3. Crear intervalos para el programa.
 - a. Para crear intervalos adicionales, hacer clic en [Añadir] en el panel Lista de intervalos.
 - b. Hacer clic en la caja de selección correspondiente a cada día por añadir al intervalo.
 - c. Escribir los valores de la hora de inicio y de fin.
4. Hacer clic en [Aceptar cambios].

Eliminar un intervalo de un programa

1. Seleccionar **Administración de acceso programas**.
2. Seleccionar el horario a modificar.
3. Seleccionar el intervalo a eliminar.
4. Hacer clic en [Remover] en el panel Lista de intervalos.
5. Hacer clic en [Aceptar cambios].

Copiar un programa

1. Seleccionar **Administración de acceso programas**.
2. Seleccionar el programa a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del programa**.
5. Agregar, eliminar o modificar los intervalos de tiempo según sea necesario.
6. Hacer clic en [Aceptar cambios].

Remover un programa

1. Seleccionar **Administración de acceso programas**.
2. Seleccionar el programa a eliminar.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Crear Grupos de lectoras

Los grupos de lectoras son útiles cuando se tiene una gran cantidad de lectoras y puertas en las instalaciones. Los grupos de lectoras permiten a los usuarios agrupar varias lectoras según una característica en común y asignarlas, como un grupo, a los niveles de acceso. Por ejemplo, todas las lectoras en el sótano de un edificio pueden agregarse a un grupo.

El agrupamiento no necesita estar relacionado con una zona física. Por ejemplo, un grupo de lectoras llamado limpieza se puede usar en un nivel de acceso que autoriza el acceso a todos los armarios de almacenamiento de suministros de limpieza.

Los grupos de lectoras aparecen en la página **Administración de acceso > Niveles de acceso** lo que permite autorizar el acceso a todas las lectoras de un grupo con una sola selección, en vez de una por una.

Añadir un grupo de lectoras

1. Seleccionar **Administración de acceso > Grupos de lectoras**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del grupo de lectoras**.
4. Seleccionar cada lectora del grupo.
5. Hacer clic en [Aceptar cambios].

Copiar un grupo de lectoras

1. Seleccionar **Administración de acceso > Grupos de lectoras**.
2. Seleccionar el grupo de lectoras a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del grupo de lectoras**.
5. Agregar o modificar la asignación de lectoras según las necesidades.
6. Hacer clic en [Aceptar cambios].

Remover un grupo de lectoras

1. Seleccionar **Administración de acceso > Grupos de lectoras**.
2. Seleccionar el grupo de lectoras a eliminar.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configuración de los niveles de acceso

Los niveles de acceso determinan a qué puertas y cuándo una credencial tiene acceso. Por ejemplo, si las instalaciones cuentan con una oficina y un almacén, y no se permite que el personal de oficina entre al almacén, se crea un nivel de acceso para el personal de oficina, que incluye solo las puertas de la zona de las oficinas.

La página **Administración de acceso > Niveles de acceso** se usa para asignar programas a lectoras y a grupos de lectoras. Luego, los niveles de acceso se asignan a las credenciales, determinando los días y horas en que la persona con esa credencial puede entrar a través de las lectoras en ese nivel de acceso.

Añadir un nivel de acceso

1. Seleccionar **Administración de acceso > Niveles de acceso**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del nivel de acceso**.
4. Seleccionar las lectoras y los grupos de lectoras a incluir en este nivel de acceso.
5. Seleccionar un horario para cada lectora seleccionada.
6. Hacer clic en [Aceptar cambios].

Copiar un nivel de acceso

Si hay una gran cantidad de lectoras, la creación de un nuevo nivel de acceso puede tardar mucho tiempo. Copiar un nivel de acceso permite volver a usar una configuración similar y hacer solo unas cuantas modificaciones para adaptarla al nuevo nivel de acceso.

1. Seleccionar **Administración de acceso > Niveles de acceso**.
2. Hacer clic en el nivel de acceso por copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del nivel de acceso**.
5. Modificar según sea necesario las lectoras y los grupos de lectoras de este nivel de acceso.
6. Borrar la caja de selección próxima a cualquier lectora que no se deba incluir en este nivel de acceso.
7. Hacer clic en [Aceptar cambios].

Remover un nivel de acceso

1. Seleccionar **Administración de acceso > Niveles de acceso**.
2. Hacer clic en el nivel de acceso por remover.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configuración de roles de operador

Un rol de operador es una directiva de permisos de grupo. Cuando se añade una persona y se le concede el permiso para iniciar sesión y operar el sistema, a ese operador se le otorgan permisos para cambiar, ejecutar o sólo ver características y datos. En lugar de configurar manualmente el acceso a cada recurso o dato para cada operador individual, el recurso de funciones de operador permite a los usuarios asignar privilegios de acceso comunes a cada tipo de operador, según sus funciones laborales específicas.

Notar los siguientes detalles sobre los formatos de tarjeta:

- Los ajustes predefinidos no pueden ser cambiados por el rol de administrador.
- Solo un administrador puede modificar los ajustes de roles para el operador, guardia, sólo ver y distribuidor.
- La función de administrador no puede borrarse.
- El rol de operador no puede borrarse si está asignado actualmente a una o más personas.

Los ejemplos de cómo varios roles de operador pueden usarse incluyen:

- **Administrador:** El usuario principal responsable por la administración del sistema.
- **Operador:** Especialistas en tecnología de información que usan el sistema para llevar a cabo tareas tales como respaldo de bases de datos, asignación de niveles de acceso, etc.
- **Guardia:** Personal de seguridad responsable por el monitoreo de la instalación que usa el sistema para controlar cámaras PTZ, puertas, entradas, etc., así como reproducir video, correr reportes, y ejecutar registro de disparo de acciones en forma manual.
- **Solo ver:** Supervisores que necesitan acceso al sistema solo para leer para efectos administrativos.
- **Distribuidor:** Los distribuidores y consultores responsables de la instalación inicial del sistema.

Los varios niveles de permisos incluyen:

- **Ninguno:** El operador no puede visitar ni ver esta página.
- **Visión:** El operador puede ver la página o los datos, pero no puede hacer cambios ni ejecutar comandos.
- **Modificación:** El operador puede cambiar los ajustes.
- **Ejecutar:** El operador puede cambiar los comandos.

Para mostrar una lista de los niveles de permisos por default asignados a los roles de operador, ver [Permisos de roles de operador predeterminados](#) en pág. 127.

Añadir un rol de operador

1. Seleccionar **Administración del sistema > Roles de operador**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre de rol**.
4. Seleccionar un **permiso** para cada recurso.
5. Hacer clic en [Aceptar cambios].

Modificar un rol de operador

Nota: La función de administrador no puede modificarse.

1. Seleccionar **Administración del sistema > Roles de operador**.
2. Para cambiar el nombre, escribir un nombre descriptivo en el campo **Nombre de rol**.
3. Cambiar el **permiso** para cada característica, según sea necesario.
4. Hacer clic en [Aceptar cambios].

Copiar un rol de operador

Copiar un rol de operador existente permite a los usuarios volver a usar una configuración similar y hacer sólo unos cuantos cambios requeridos para el nuevo rol.

1. Seleccionar **Administración del sistema > Roles de operador**.
2. Seleccionar el rol por copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre de rol**.
5. Cambiar el **permiso** para cada característica, según sea necesario.

6. Hacer clic en [Aceptar cambios].

Remover un rol de operador

Nota: Roles que están asignados actualmente a usuarios no pueden borrarse.

1. Seleccionar **Administración del sistema > Roles de operador**.
2. Seleccionar el rol por remover.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configurar Correo electrónico

El sistema puede configurarse para enviar correos electrónicos automáticos cuando ocurran ciertos eventos, tales como un respaldo de base de datos, o cuando un disparador de acción es ejecutado.

El sistema incluye una lista de correos electrónicos predefinidos a la cual se pueden añadir destinatarios de mensajes de correo electrónico automáticos. Hasta diez listas de correos electrónicos, cada una de las cuales contiene hasta diez receptores, puede ser creada para usarse con correos electrónicos automáticos.

Para usar la característica de correos electrónicos automáticos, configurar el sistema para usar ya sea un servidor Simple Mail Transfer Protocol (SMTP) interno o externo y añadir al menos un destinatario de correo electrónico a la lista de correos electrónicos predefinida, como se describe en esta sección.

Configurar un servido de correo electrónico

El sistema puede ser configurado para acceder ya sea un servidor de correo electrónico enterprise SMTP interno, o un servidor SMTP externo (como un Gmail) para enviar correos electrónicos automáticos.

Consultar con el proveedor de servicios de Internet (ISP) o proveedor de servicios de correo electrónico para determinar la dirección IP o nombre de anfitrión para el servidor de correo electrónico y su número de puerto. También preguntar si el servidor de correo electrónico usa el protocolo SSL (Secure Sockets Layer) para encriptación de datos.

Nota: Algunos proveedores de servicios de Internet y de correo electrónico limitan la cantidad de mensajes de correo electrónico que pueden ser enviados cada día y pueden cobrar extra por cualquier cantidad por encima de esa cantidad. En algunos casos, un proveedor bloqueará la cuenta cuando si se supera la cantidad máxima. Si estos temas son restrictivos, considerar el uso de un servicio de retransmisión SMTP pagado o ser anfitrión de un servidor de correo interno.

1. Seleccionar **Administración del sistema > correo electrónico> ServidorAjustes**.
2. Seleccionar **Activar notificaciones de correo electrónico**.
3. Si se conecta a un servidor de correo electrónico seguro, seleccionar la caja de selección **permitir autenticación**.

- a. Escribir la dirección IP o nombre del anfitrión del servidor de correo electrónico en el campo **servidor de correo electrónico**.
 - b. Escribir el número de puerto del servidor de correo electrónico en el campo **puerto**.
Si el servidor de correo electrónico usa el protocolo SSL, el valor por default es 465, de otra manera, el valor por default es 25.
 - c. Si el servidor de correo electrónico usa el protocolo SSL, seleccionar la caja de selección **Requiere SSL**.
 - d. Escribir el nombre de usuario para la cuenta de servicio de correo electrónico en el campo **Usuario**.
 - e. Escribir la contraseña para la cuenta de servicio de correo electrónico en el campo **contraseña**.
4. Si se conecta a un servidor de correo electrónico que no requiere un nombre de usuario y contraseña, dejar sin seleccionar la caja de selección **Permitir autenticación**.
- a. Escribir la dirección IP o nombre del anfitrión del servidor de correo electrónico en el campo **servidor de correo electrónico**.
 - b. Escribir el número de puerto del servidor de correo electrónico en el campo **puerto**.
Si el servidor de correo electrónico usa el protocolo SSL, el valor por default es 465, de otra manera, el valor por default es 25.
 - c. Si el servidor de correo electrónico usa el protocolo SSL, seleccionar la caja de selección **Requiere SSL**.
 - d. Escribir el nombre que aparecerá en los correos electrónicos automáticos en el campo **nombre del remitente**.
 - e. Escribir el nombre que aparecerá en los correos electrónicos automáticos en el campo **correo electrónico del remitente**.
Si los destinatarios no deben responder a correos electrónicos automáticos, considerar crear una cuenta de correo electrónico "no responder" por ejemplo "noresponder@nombrededominio.com".
5. Hacer clic en [Aceptar cambios].
6. Hacer clic en [Probar servidor correo electrónico] para verificar los ajustes del servidor de correo electrónico.

Modificar una lista de correo electrónico

Los destinatarios pueden añadirse y removerse de una lista de correo electrónico y el nombre de la lista puede cambiarse como se describe a continuación. El sistema incluye una lista de correos electrónicos predefinidos a la cual se debe añadir al menos un destinatario para mensajes de correo electrónico automáticos.

1. Seleccionar **Administración del sistema > Correo electrónico > Listas de correo electrónico**.
2. Hacer clic en la lista de correo electrónico para seleccionarla.
3. Para cambiar el nombre de una lista de correos electrónicos, escribir un nombre descriptivo de la lista en el campo **Nombre de lista de correos electrónicos**.
4. Para añadir una persona a la lista:
 - a. Escribir el nombre de la persona en el campo **Mostrar nombre**.
 - b. Escribir la dirección de correo electrónico de la persona en el campo **Dirección de correo electrónico**.
 - c. Hacer clic en [Añadir].
5. Para remover una persona de la lista:

- a. Hacer clic en el nombre de la persona para seleccionarla.
 - b. Hacer clic en [Remover].
6. Hacer clic en [Aceptar cambios].

Añadir una lista de correo electrónico

El sistema incluye una lista de correos electrónicos predefinidos a la cual se debe añadir al menos un destinatario para soportar mensajes de correo electrónico automáticos. Se pueden crear hasta diez listas de correos electrónicos, cada una de las cuales puede contener hasta diez destinatarios. Una lista existente de correos electrónicos puede copiarse y modificarse según se necesite.

1. Seleccionar **Administración del sistema > Correo electrónico> Listas de correo electrónico**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo de la lista de correo electrónico en el campo **Nombre de la lista de correo electrónico**.
4. Para cada persona que se añade a la lista de correo electrónico:
 - a. Hacer clic en [Añadir].
 - b. Escribir el nombre de la persona en el campo **Mostrar nombre**.
 - c. Escribir la dirección de correo electrónico de la persona en el campo **Dirección de correo electrónico**.
5. Cuando se hayan añadido los destinatarios a la lista de correo electrónico, hacer clic en [Aceptar Cambios].

Remover una lista de correo electrónico

Nota: No es posible borrar una lista de correo electrónico si está siendo usada por el sistema.

1. Seleccionar **Administración del sistema > Correo electrónico> Listas de correo electrónico**.
2. Hacer clic en la lista de correo electrónico para seleccionarla.
3. Hacer clic en [Remover].

Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Desactivar notificaciones por correo electrónico

Para desactivar rápidamente las notificaciones de correo electrónico, limpiar la caja de selección **Activar notificaciones de correo electrónico** en la página **ajustes del servidor**. Notar, sin embargo, que esto impacta cualquier detonador de acción que involucra correos electrónicos automáticos.

1. Seleccionar **Administración del sistema > correo electrónico> Ajustes del servidor**.
2. Limpiar la caja de selección **Activar notificaciones de correo electrónico**.
3. Hacer clic en [Aceptar cambios].

Configuración de los Campos definidos por el usuario

Los registros de la persona en la base de datos pueden ser campos definidos por el usuario asociado con ellos que pueden usarse para ingresar datos personales acerca del personal, tal como placas del auto o número telefónico del domicilio. Un campo debe estar activado para aparecer en la página **Administración de acceso > Personas**. Si se desactiva un campo, se remueve de la base de datos y se pierden los datos contenidos en ese campo para cada persona.

Todas las bases de datos deben poder distinguir un registro de otro. Ya que algunos nombres son muy comunes, usar los apellidos de los empleados como identificador exclusivo de los registros de la base de datos no funciona. Por consiguiente, las organizaciones asignan a cada empleado un número de identificación exclusivo.

IMPORTANTE: Para obtener los mejores resultados, usar un identificador de registros personales, como un número de empleado, exclusivo para cada persona en la organización. Si no se tiene una forma de identificar cada registro como exclusivo, las acciones de mantenimiento de la base de datos, tales como actualizaciones, importaciones, exportaciones y otras acciones pueden dar lugar a que se modifique un registro incorrecto.

Cuando se crean campos definidos por el usuario, pueden ser designados como protegidos. La configuración de esta opción determina si los campos definidos por el usuario con la característica Protegido seleccionada son visibles o modificables por diferentes roles de operador. De este modo se aumenta el nivel de protección de la información confidencial, tal como números de teléfono particular. Por ejemplo, si se desea que los usuarios con el rol de operador vean toda la información personal y los usuarios con el rol de guardia vean solo la información personal no protegida, es necesario cambiar la configuración de los roles de operador como se muestra en la siguiente tabla:

Rol	Ajustes de campos definidos por usuario	Ajustes campos de usuario protegidos
Operador	Solo ver	Solo ver
Guarda	Solo ver	Ninguna

Agregar campos definidos por el usuario

Los campos definidos por usuario forman parte de los registros personales en la base de datos. Un campo debe estar activado para aparecer en la página **Administración de acceso > Personas**.

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Para cada campo:
 - a. Seleccionar **Activado**.
 - b. Escribir una **Etiqueta**.
 - c. (Opcional) seleccionar **Obligatorio**.
 - d. (Opcional) seleccionar **Protegido**.
4. Hacer clic en [Aceptar cambios].

Reorganizar los campos definidos por el usuario

Los campos definidos por usuario forman parte de los registros personales en la base de datos. Un campo debe estar activado para aparecer en la página **Administración de acceso > Personas**. Si se desactiva un campo, se remueve de la base de datos y se pierden los datos contenidos en ese campo para cada persona.

IMPORTANTE: No se modifican las etiquetas de los campos para tratar de cambiar su orden. Los datos están asociados al campo, no a la etiqueta del campo. Cambiar la etiqueta no cambia el orden, pero da lugar a que los datos estén mal etiquetados.

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Usar las flechas Ordenar para mover los campos hacia arriba o hacia abajo.
El orden de los campos en esta etiqueta coincide con el orden de los campos **Administración de acceso > Personas**.

Remover un campo definido por el usuario

Un campo debe estar activado para aparecer en la página **Administración de acceso > Personas**. Si se desactiva un campo, se remueve de la base de datos y se pierden los datos contenidos en ese campo para cada persona.

1. Seleccionar **Administración del sistema > Ajustes del sistema**.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Despejar la caja **activado** correspondiente al campo y los datos a borrar.
4. Hacer clic en [Aceptar cambios].

Comportamiento programación de puertas y lectoras

La pestaña Ver programa de la página **Monitoreo > Puertas**, se usa para anular el comportamiento de las puertas y lectoras, determinado de acuerdo con un programa. Por ejemplo, durante el horario comercial, una puerta debe permanecer desbloqueada para el acceso del público a la sala de exposición o al local de ventas al por menor. Después del horario comercial normal, puede ser necesario que ciertas lectoras se ajusten para requerir una credencial y un PIN (útil para impedir el acceso con tarjetas perdidas o robadas), de modo que se configura la lectora para solicitar, por default, solo una credencial (**Administración del sistema > Dispositivos**) y solicitar una credencial y un PIN después del horario comercial (**Monitoreo > Puertas > Ver horarios**).

Nota: No confundir el comportamiento de la puerta y la lectora con el acceso. La página **Administración de acceso > Niveles de acceso** se usa para asignar programas a lectoras y a grupos de lectoras. Luego, los niveles de acceso se asignan a las credenciales, determinando los días y horas en que la persona con esa credencial puede entrar a través de las lectoras en ese nivel de acceso. El modo de acceso, solo credencial o credencial y PIN, no es relevante para el nivel de acceso. (Ver [Configuración de seguridad en la página 18](#).)

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver horarios**.
3. Para cada combinación de puerta y lectora:

- a. Seleccionar un **Programa**.
- b. Seleccionar un **Modo de programa**.

Para las puertas, los modos de programa son:

- **Desbloqueada**
- **Primera entrada con tarjeta**
- **Bloqueada**

Para las lectoras, los modos de horario son:

- **Solo credencial**
- **Credencial y PIN**

Importar Personas y credenciales de un archivo CSV

El asistente de importación/exportación proporcionado en el disco de utilitarios puede usarse para añadir o borrar conjuntos de personas y datos de credenciales en modo de lotes desde otra fuente, tal como una base de datos de recursos humanos o de otro sistema de control de acceso.

Nota: Las personas también pueden tener una cuenta de usuario en el sistema, que les permite iniciar sesión y usar el sistema. La información de cuenta de usuario no es procesada por el asistente de importación/exportación.

El asistente de importación/exportación puede ser usado para mapear los campos de un archivo CSV a la tabla de base de datos del sistema e importar personas y datos de credenciales desde otra fuente, tal como una base de datos de recursos humanos o de otro sistema de control de acceso. Referirse a la guía *Asistente de importación/exportación* para más detalles.

Nota: Un registro personal se compone de campos definidos por el usuario para la información personal, las credenciales de acceso (tarjeta de ID, PIN, nivel de acceso) e información opcional sobre la cuenta de usuario que permite iniciar sesión en el sistema. Es imposible importar/exportar datos de cuenta de usuario. Solo se pueden importar y exportar datos personales y de credenciales definidos por el usuario.

Los registros de persona pueden añadirse en forma individual como se describe en [Administración de personas](#) en pág. 76.

Configuración de Disparadores de acciones

Con la característica Disparadores de acciones, se pueden definir las condiciones para disparar junto con las acciones correspondientes que serán ejecutadas cuando las condiciones para iniciarlas se hayan satisfecho. Por ejemplo, si una puerta exterior es forzada abierta entre las horas de 7 p.m. a 7 a.m., un disparador de acción puede ser ejecutado causando que las sirenas suenen, que las luces se activen y que un correo electrónico automático sea enviado a todos los supervisores del sitio.

La página **Administración del sistema > Disparadores de acciones** contiene dos etiquetas, **disparadores** y **acciones** como se describe a continuación.

Entendiendo los disparadores

Usar la etiqueta **Disparadores** en la página **Disparadores de acciones** para definir las condiciones de disparador que ejecutarán acciones. Un disparador consiste de uno o más grupos de condiciones y un grupo de condiciones consiste de uno o más instrucciones de condición.

Cada instrucción de condición incluye cuatro lista de caída abajo en donde los usuarios pueden:

- Especificar un tipo de entidad, tal como una **Puerta** o un **Programa**.
- Especificar un calificador relacionado con el tipo de entidad seleccionado. Si se ha seleccionado **Puerta** como el tipo de entidad, las opciones en esta caja de lista incluyen **Cualquiera**, **Todas**, y una lista de puertas definidas en el sistema.
- Especificar si la condición debe ser falsa o verdadera.
- Seleccionar una condición que detonaría una acción. Si se ha seleccionado **Puerta** como el tipo de entidad, las opciones incluyen **Segura**, **Desbloqueada**, **Bloqueada**, **Mantenida abierta**, **Forzada abierta**, **Saboteada**, **Abierta** y **Mag Problema de sensor**.

La siguiente tabla lista las condiciones de disparador disponibles para cada tipo de entrada:

Entidad	Condiciones de disparar	Notas
Área	Desbloqueada - cualquier puerta	Una puerta pertenece a una área si cualquiera de sus lectoras está configurada para entrar o salir del área en la página Administración de acceso > Áreas > Asignaciones de lectoras. La sola excepción es "Bloqueado afuera – Cualquier puerta", que solo considera lectoras que entran al área seleccionada. Dispara como verdadera cuando las puertas en el área reúnen las condiciones. Dispara como falsa cuando las puertas no cumplen las condiciones. Las áreas exteriores no son soportadas. Ver el disparador de puerta para detalles de condición. Si una área no está asociada con ninguna puerta, las condiciones de "ninguna puerta" siempre serán falsas, y las condiciones de "todas las puertas" siempre son verdaderas.
	Bloqueada - cualquier puerta	
	Mantenida abierta - cualquier puerta	
	Forzada abierta - cualquier puerta	
	Sabotaje - cualquier puerta	
	Abierta - cualquier puerta	
	Asegurar - todas las puertas	
	Problema sensor magnético - cualquier puerta	

Entidad	Condiciones de disparar	Notas
Puerta	Desbloqueada	Dispara como verdadera cuando se activa apertura de puerta. Dispara como falsa cuando se desactiva apertura de puerta.
	Bloqueada	Dispara como verdadera cuando se bloquea la puerta. Dispara como falsa cuando el bloqueo de la puerta no está más activo
	Mantenida abierta	Dispara como verdadera cuando una alarma de puerta mantenida abierta está activa. Dispara como falsa cuando una alarma de puerta mantenida abierta es restablecida.
	Forzada abierta	Dispara como verdadera cuando una alarma de puerta mantenida abierta está activa. Dispara como falsa cuando una alarma de puerta mantenida abierta es restablecida.
	Sabotaje	Dispara como verdadera cuando una alarma de sabotaje de puerta está activa. Dispara como falsa cuando una alarma de sabotaje de puerta es restablecida. Incluye sabotaje en contacto de puerta, solicitud de salida, entrada auxiliar y sabotaje.
	Abrir	Dispara como verdadera cuando la puerta está abierta. Dispara como falsa cuando la puerta está cerrada. Incluye condiciones de puerta forzada y mantenida abierta.
	Seguro	Dispara como verdadera cuando la apertura de puerta está inactiva y la puerta está cerrada. Dispara como falsa cuando la apertura de puerta está inactiva y la puerta está abierta.
	Problema sensor magnética	Dispara como verdadera cuando una alarma de sensor magnético está activa. Dispara como falsa cuando una alarma de sensor magnético es restablecida.
Entrada	Inactiva	Dispara como verdadera cuando la entrada está inactiva. Dispara como falsa cuando la entrada está inactiva.
	Activa	Dispara como verdadera cuando la entrada está activa. Dispara como falsa cuando la entrada está inactiva.
	Saboteada	Dispara como verdadera cuando la entrada está saboteada. Dispara como falsa cuando la entrada no está saboteada.
Salida	Encendido	Dispara como verdadera cuando la salida está encendida. Dispara como falsa cuando la entrada no está encendida.
	Apagada	Dispara como verdadera cuando la salida está apagada. Dispara como falsa cuando la entrada no está apagada.

Entidad	Condiciones de disparar	Notas
Módulo	Saboteada	Dispara como verdadera cuando los periféricos reportan condición de sabotaje. Dispara como falsa cuando los periféricos reportan condición de sabotaje restablecida.
	Error comunicaciones	Dispara como verdadera cuando se pierde la comunicación con el periférico. Dispara como falsa cuando se restablece la comunicación.

Entidad	Condiciones de disparar	Notas
Lectora	Concedido	Dispara como verdadera/falsa para cualquier tipo de evento de acceso concedido. Será seguida por otro evento de acceso concedido.
	Concedido - sin entrada	Dispara como verdadera/falsa cuando la puerta no está abierta y no ocurre una violación de APB.
	Concedido - entrada hecha	Dispara como verdadera cuando la puerta está abierta y la lectora conduce a área no exterior.
	Concedido - entrada hecha APB con acceso	Dispara como verdadera/falsa cuando la puerta está abierta y la lectora conduce a un área no exterior, y a una violación de APB con acceso.
	Concedido - sin entrada APB con acceso	Dispara como verdadera/falsa si la puerta no está abierta y la lectora conduce a un área no exterior, y violación de APB con acceso.
	Concedido - egreso hecho	Dispara como verdadera/falsa si la puerta está abierta y la lectora conduce a un área no exterior, y sin violación de APB.
	Concedido - egreso hecho APB con acceso	Dispara como verdadera/falsa si la puerta está abierta y la lectora conduce a un área exterior, y a violación de APB con acceso.
	Concedido - sin egreso APB con acceso	Dispara como verdadera/falsa si la puerta no está abierta y la lectora conduce a un área no exterior, y violación de APB con acceso.
	Negado - cualquier razón	Dispara como verdadera/falsa cuando se niega el acceso por cualquier razón.
	Negado - credencial inválida	Dispara como verdadera/falsa cuando se niega el acceso por credencial desconocida.
	Negado - código de instalación	Dispara como verdadera/falsa cuando se niega el acceso por código de instalación inválido.
	Negado - código de expedición	Dispara como verdadera/falsa cuando se niega el acceso por código de expedición inválido.
	Negado - PIN	Dispara como verdadera/falsa cuando se niega el acceso por PIN inválido. No hay disparador explícito para cuando se alcance el máximo de intentos inválidos de PIN y se bloquee la salida del tarjeta habiente.
	Negado - no autorizado	Dispara como verdadera/falsa cuando se niega el acceso por no haber nivel de acceso.
	Negado - APB sin acceso	Dispara como verdadera/falsa cuando se niega el acceso por violación de APB sin acceso
	Negado - puerta bloqueada	Dispara como verdadera/falsa cuando se niega el acceso debido a puerta bloqueada.
	Negado - inactivo	Dispara como verdadera/falsa cuando se niega el acceso debido a credencial activa de/a fuera de rango.

Entidad	Condiciones de disparar	Notas
Programa	En efecto	Dispara como verdadera cuando comienza el programa. Dispara como falsa cuando termina el programa.
	Feriado en efecto	Dispara como verdadera cuando un programa no está en efecto debido a un feriado. (Las horas del día en que el disparador está activo basado en el programa.) Dispara como falso cuando termina el feriado. Ver Consideraciones para Registros disparadores de acciones basados en programas en pág. 63.
	15 minutos antes inicio	Dispara como verdadero cuando inicia 15 minutos antes del programa. Dispara como falsa cuando inicia el programa.
	15 minutos antes del fin	Dispara como verdadero cuando termina 15 minutos antes del programa. Dispara como falsa cuando termina el programa.
Sistema	Bloquear todas las puertas - comando	Dispara como verdadera cuando el bloqueo está activo. Dispara como falso cuando el bloqueo de la puerta no está más activo.
	Desbloquear todas las puertas - comando	Dispara como verdadera cuando el desbloqueo está activo. Dispara como falso cuando el desbloqueo no está más activo.
	Problema	Dispara como verdadera cuando está activo el sabotaje pared/externa. Dispara como falsa cuando la condición de sabotaje está inactiva.
	Batería de respaldo baja	Dispara como verdadera cuando el voltaje de la batería es menos de 11.7 VCD. Dispara como falsa cuando el voltaje de la batería es mayor de 11.7 VCD.
	Memoria batería baja	Dispara como verdadera cuando el voltaje de la batería es menos de 2.0 VCD. Dispara como falsa cuando el voltaje de la batería es mayor de 2.0 VCD. Solo verificado cada seis horas.
	Falló alimentación CA	Dispara como verdadera cuando se remueve la alimentación CA. Dispara como falsa cuando se restablece la alimentación CA.
	Fusible cortado	Dispara como verdadera cuando se corta cualquier fusible. Dispara como falsa cuando se restablecen todos los fusibles.
	Hora cambiada	Dispara como verdadera cuando cambia la hora. No se vuelve a armar durante un minuto. Dispara como falsa automáticamente después de un minuto.

Notar los siguientes detalles sobre los disparadores:

- Pueden crearse hasta diez grupos de expresiones de condición, con hasta diez expresiones de condición a través de todos los grupos (por ejemplo dos grupos podrían tener cinco condiciones cada uno).
- Para iniciar un nuevo grupo de expresiones de condición, hacer clic en el botón [+] que aparece arriba de la expresión de condición en un grupo existente. Hacer clic en el botón [-] para remover un grupo de expresiones de condición.
- Un segundo nivel de botones de [+] y [-] aparece junto a cada expresión de condición individual. Hace clic en el botón [+] para añadir una nueva expresión de condición; hacer clic en el botón [-] para remover una expresión de condición única.
- Ya sea para un grupo específico de expresiones de condición o para todos los grupos de expresiones de condición, deben seleccionarse **Cualquiera puede ocurrir** o **Todos deben ocurrir**.
- Si se selecciona **Cualquiera** o **Todo** como el calificador de una entidad en una expresión de condición, cualquier objeto nuevo que se añada al sistema del mismo tipo de entidad será incluido automáticamente en la evaluación de condición. Por ejemplo, si una expresión de condición se crea para monitoreo de todas las lectoras y se instala una lectora, la lectora nueva se añade automáticamente al grupo de lectoras que se está monitoreando.
- Condiciones de disparo para lectoras siempre disparan como falsas inmediatamente después de disparar como verdaderas. También las acciones de desactivación no son usadas generalmente con las condiciones de disparar lectora.
- Si una entidad del sistema (por ejemplo, una lectora) es definida en una expresión de condición y entonces la entidad se borra del sistema, la expresión de condición correspondiente también será borrada. Si la entidad se vuelve a crear, una expresión de condición nueva puede ser creada para esa entidad.
- Un evento es registrado siempre que una expresión de condición dispara y cambia el estado de verdadero a falso.
- Expresiones de condición duplicadas pueden ser incluidas en el mismo grupo de condiciones.
- Las entradas desactivadas y salidas pueden ser incluidas en la expresión de disparo, pero no habrá efecto en la evaluación de disparo.
- Los registros de disparar acción pueden ser configurados para ocurrir cuando un disparador es desactivado.
- Los registro de disparar acción pueden incluir condiciones de disparo sin ningún resultado de las acciones.

Además, se presume que las condiciones de disparo están en un estado indeterminado y que harán la transición a falso o verdadero para ejecutar las acciones correspondientes:

- Para todos los registros cuando el sistema inicia.
- Para cada registro cuando se configura y un registro se salva.
- Para registros afectados cuando se borra una entidad de referencia.

Consideraciones para Registros disparadores de acciones basados en programas

Cuando se crean las expresiones de condiciones para registros disparadores de acciones que involucran programas, recordar que los grupos de feriados pueden incluirse o excluirse de un programa, dependiendo de cómo el grupo de feriados se haya configurado en la página

Administración de Acceso > Programas.

- Si un grupo de feriados es *incluido* en un programa, (por ejemplo si se selecciona la caja de selección), entonces el programa será activo en los días definidos en el grupo de feriados durante las horas definidas en el programa. Esto es independiente de cuales días de la semana están seleccionados para el programa.
- Si la caja de selección de un grupo de feriados está *excluido* de un programa (por ejemplo si la caja de selección está despejada), entonces el programa no estará activo en ningún momento durante los días definidos en el grupo de feriados. Esto es independiente de cuales días de la semana están seleccionados para el programa.
- Si el mismo día es parte de un grupo de feriados que está *incluido* en un programa y también es parte de otro grupo de feriados que está *excluido* del mismo programa, el día será *incluido* en el horario.

Para garantizar que una acción sea disparada sin importar si se trata de un feriado o no, crear una expresión "o" con las condiciones de disparar usando la opción "Cualquiera puede ocurrir". Por ejemplo, añadir una condición de disparo que será verdadera cuando esté en efecto un programa para los días de la semana de 9AM - 6PM y una condición de disparo coincidente que será verdadera cuando los feriados estén en efecto.

El siguiente ejemplo muestra cuando un disparador de feriado en efecto está activo si un feriado impacta negativamente un programa para el horario de los días de la semana de 7AM - 7PM:

	Miér. 2/13 7AM - 7PM	Jue. 2/14 7AM - 7PM	Vie. 2/15 7AM - 7PM	Sáb. 2/16 7AM - 7PM	Dom. 2/17 7AM - 7PM	Lun. 2/18 7AM - 7PM	Mar. 2/19 7AM - 7PM
Sin feriados definidos							
En ventana	Activa	Activa	Activa			Activa	Activa
Feriado en efecto							
Feriado 1 (2/14-2/16) la caja de selección está despejada							
Feriado 2 (2/15-2/18) la caja de selección está despejada							
En ventana	Activa						Activa
Feriado en efecto		Activa	Activa			Activa	
Feriado 1 (2/14-2/16) la caja de selección está seleccionada							
Feriado 2 (2/15-2/18) la caja de selección está despejada							
En ventana	Activa	Activa	Activa	Activa			Activa
Feriado en efecto						Activa	

Entendiendo las acciones

Usar la etiqueta **Acciones** en la página **Administración del sistema > Disparadores de acciones** para definir las acciones que se ejecutarán cuando una condición de disparar acción se vuelve verdadera o falsa. (Los disparadores de acciones también pueden ejecutarse en la página **Monitoreo > Disparadores de acciones**. Ver [Controlar disparadores de acciones](#) en pág. 98.)

Por ejemplo, una expresión de condición pueden ser definidos en la etiqueta disparadores para especificar que una acción ocurrirá si cualquier puerta está forzada abierta. Entonces una acción puede ser configurada en la etiqueta acciones cuando la expresión de condición se vuelve verdadera, un correo electrónico automático será enviado a todos los supervisores. Si una puerta está forzada abierta después de la creación del registro disparadores de acciones, se enviará un correo electrónico automático a todos los supervisores.

Hasta 32 registros de disparo de acción pueden ser creados para resultar en dos tipos de acciones:

- Las acciones de activación se ejecutan cuando una condición de disparo se vuelve verdadera, y
- las acciones de desactivación se ejecutan cuando una condición de disparo se vuelve falsa.

Registros de disparo de acción múltiple pueden ser configuradas para ejecutar la misma acción o controlar la misma entidad del sistema. Por ejemplo, un registro puede ser configurado para prender una salida de sirena y enviar un correo electrónico automático cuando cualquiera de las varias entradas de emergencia se active, y otro registro puede configurarse para apagar la sirena y enviar un correo electrónico cuando se haya restablecido la emergencia.

La siguiente tabla lista las acciones disponibles:

Entidad	Acciones	Notas
Controlador del sistema	Reajustar APB	Reajusta el Anti-passback de todas las credenciales a un estado neutral (p. ej. paso libre).

Entidad	Acciones	Notas
Puertas/ lectoras	Bloquear	Bloquea la puerta. Nota: No afecta lectoras en modo de acceso.
	Desbloquear	Desbloquea puerta. Nota: No afecta lectoras en modo de acceso.
	Abrir	Desbloquea apertura de puerta para el periodo de acceso concedido. Nota: No afecta lectoras en modo de acceso.
	Abrir extendido	Desbloquea apertura de puerta para el periodo de acceso extendido. Nota: No afecta lectoras en modo de acceso.
	Primera entrada con tarjeta	Ajusta el modo de puerta a Primer usuario pendiente.
	Relé aux encendido	Enciende el relé aux de puerta.
	Relé aux apagado	Enciende el relé aux de puerta.
	Buzzer de puerta encendido	Enciende el buzzer salida de puerta. Nota: Los controladores de puerta sencilla basados en IP no soportan esta acción.
	Buzzer de puerta apagado	Apaga el buzzer de salida de puerta. Nota: Los controladores de puerta sencilla basados en IP no soportan esta acción.
	Puerta Bloqueada	Puerta bloqueada (afecta apertura y lectoras entrada/salida).
	Restablecer puerta	Restablecer puerta (afecta apertura y lectoras entrada/salida).
	Tarjeta+PIN - lectora entrada	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.
	Tarjeta+PIN - lectora salida	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.
	Tarjeta+PIN - lectoras entrada/salida	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.
	Solo tarjeta - lectora entrada	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.
	Solo tarjeta - lectora salida	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.
	Solo tarjeta - lectoras entrada/salida	Ajusta la lectora a modo de acceso Credencial y PIN. Nota: No afecta apertura de puerta.

Entidad	Acciones	Notas
Salida	Encendido	Enciende salida.
	Apagado	Apaga salida.
	Pulsar encendido	Pulsa la salida a encendida, después a apagada por la duración seleccionada. Nota: La exactitud del pulso de duración varía dependiendo de la longitud del pulso. Ver Exactitud de duración de Pulso en pág. 133.
	Pulsar apagado	Pulsa la salida a apagada, después a encendida por la duración seleccionada. Nota: La exactitud del pulso de duración varía dependiendo de la longitud del pulso. Ver Exactitud de duración de Pulso en pág. 133.

Entidad	Acciones	Notas
Área	Reajustar APB	Reajusta APB para todas las credenciales que están en áreas a neutral (p.ej. paso libre).
	Desbloquear - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Bloquear - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Relé aux encendido - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Relé aux apagado - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Buzzer encendido - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área. Nota: Los controladores de puerta sencilla basados en IP no soportan esta acción.
	Buzzer apagado - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área. Nota: Los controladores de puerta sencilla basados en IP no soportan esta acción.
	Primera entrada con tarjeta - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Bloquear - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Reinstalar - puertas	Ver el comando de puerta correspondiente. Afecta todas las puertas con lectoras de entrada o salida asociadas con el área.
	Credencial y PIN - lectoras entrada	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden entrar al área.
	Solo credencial - lectoras salida	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden salir del área.
	Solo credencial - todas lectoras	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden entrar o salir del área.
	Solo credencial - lectoras entrada	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden entrar al área.
	Solo credencial - lectoras salida	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden salir del área.
	Solo credencial - todas lectoras	Ver el comando de puerta correspondiente. Afecta todas las lectoras que pueden entrar o salir del área.

Entidad	Acciones	Notas
Notificación por correo electrónico	Enviar correo electrónico	Ver los requerimientos explícitos abajo.

Notar los siguientes detalles sobre los registros disparadores:

- Se pueden incluir hasta diez acciones por registro de disparador de acciones. Estas acciones pueden ser una combinación de acciones de activación y o desactivación.
- Las acciones pueden ser configuradas para ocurrir cuando un disparador es desactivado.
- Usar el campo **Estado** en la parte superior de la página **Administración del sistema > Disparadores de acciones** para activar o desactivar los registros disparadores.
- Los disparadores de acciones también pueden ejecutarse en la página **Monitoreo > Disparadores de acciones**. Ver [Controlar disparadores de acciones](#) en pág. 98.

Nota: Para proporcionar una forma rápida de asegurar todas las puertas en la instalación, crear un registro de disparadores de acciones para bloquear todas las puertas y entonces dispararla manualmente en la página **Monitoreo > disparadores de acciones** cuando sea necesario.

- Las entradas y salidas desactivadas pueden incluirse como una acción, pero no tendrán que ser implementadas hasta que la entrada o salida esté activada.
- Los disparadores de acciones, programas y control manual pueden impactar el estado de los dispositivos y son tratados igualmente por el sistema. La última operación ejecutada determina el estado del dispositivo.
- Los disparadores de acciones no sobrescriben los estados de puerta Bloquear todas las puertas o Desbloquear todas las puertas.
- Si una entidad (por ejemplo, una lectora) es definida en un registro de disparadores de acciones y entonces la entidad se borra del sistema, la expresión de condición correspondiente también será borrada. Si la entidad se vuelve a crear, una expresión de condición nueva puede crearse para esa entidad.
- Si el sistema está configurado para enviar correos electrónicos automáticos, un registro de disparadores de acciones puede crearse para enviar una notificación a una lista de correos electrónicos cuando cambie una condición de disparador. La entrega de correo electrónico se intentará durante el límite de reintentos seleccionado relativo a cuando se disparó la acción.
- Los controladores de puerta sencilla basados en IP no soportan acciones de Buzzer encendido y Buzzer apagado.
- Si un disparador de acción está dirigido a una entidad cuyo módulo padre está fuera de línea, la acción no tendrá efecto en esa entidad cuando el módulo vuelva a estar en línea. En otras palabras, las acciones no persisten ni quedan en cola.
- Las acciones de salida no registran un evento de salida encendida o salida apagada a menos de que el estado cambie físicamente la salida. Por ejemplo, si una salida está encendida y ocurre una acción de disparo para encender esa salida, no se generará un evento de salida encendida.

Además, se presume que las condiciones de disparo están en un estado indeterminado y que harán la transición a falso o verdadero para ejecutar las acciones correspondientes:

- Para todos los registros cuando el sistema inicia.
- Para cada registro cuando se configura y un registro se salva.
- Para registros afectados cuando se borra una entidad de referencia.

Añadir un Registro de disparadores de acciones

1. Seleccionar **Administración del sistema > Disparadores de acciones**.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo para el registro de hasta 64 caracteres de longitud, en el campo **Nombre disparador de acciones**.
4. Seleccionar valores en las cuatro cajas de caída abajo para crear la primera expresión de condición que dispara una acción.
5. Para crear expresiones de condiciones adicionales en el mismo grupo:
 - a. Hacer clic en el botón [+] en la misma línea que la última expresión de condición.
 - b. Seleccionar valores en las cuatro lista de caída abajo.
 - c. Repetir **paso a** y **paso b** para cada expresión de condición nueva.
 - d. Si es necesario, hacer clic en el botón [-] para remover una expresión de condición.
6. Para crear un grupo de expresión de condición nueva, hacer clic en el botón [+] que aparece en la misma línea que la lista de caída abajo **Cualquiera puede ocurrir**.
7. Ajustar las cajas de la lista de caída abajo **Cualquiera puede ocurrir** para crear operadores lógicos (p. ej. expresiones Y/O) para las expresiones de condiciones en cada grupo.
8. Hacer clic en [Aceptar cambios].
9. Después, hacer clic en [Acciones] para configurar las acciones que ocurrirán cuando una o todas las expresiones de condiciones sean verdaderas, dependiendo de cómo se configuren los disparadores.
 La etiqueta acciones incluye dos secciones: Acciones de activación y acciones de desactivación. Las acciones pueden añadirse ya sea a una o ambas secciones según se necesite.
10. Para añadir acciones de sistema, área, salida o puerta:
 - a. Hacer clic en [Añadir] bajo la sección acciones de activación o acciones de desactivación.
 - b. Seleccionar el tipo de acción por añadir.
 - c. En la caja de diálogo configurar acciones, seleccionar cada entidad y la acción que ocurrirá.
 - d. Hacer clic en [OK] para cerrar la caja de diálogo configurar acciones.
11. Para añadir acciones de correo electrónico:

Nota: Evitar la adición de grandes cantidades de acciones de correo electrónico para evitar destinatarios "spamming".

- a. Hacer clic en [Añadir] bajo la sección acciones de activación o acciones de desactivación.
 - b. Seleccionar **Acciones de correo electrónico**.
 - c. En la caja de diálogo configurar acciones, seleccionar cada lista de distribución de correo electrónico a la que se enviará un mensaje cuando las condiciones de disparo cambien. También se puede enviar mensajes a todas las listas.
 - d. Escribir **Texto correo electrónico**.
 - e. Seleccionar un valor **Interrupción reintento**. Si el correo electrónico inicial falla debido a un error de conexión, el sistema intentará enviar el mensaje nuevamente, duplicando el tiempo de duración entre cada intento hasta que el valor de interrupción de reintento se alcance.
 - f. Hacer clic en [OK] para cerrar la caja de diálogo configurar acciones.
12. Hacer clic en [Aceptar cambios].

Copiar un Registro de disparador de acciones

1. Seleccionar **Administración del sistema > Disparadores de acciones**.
2. Hacer clic en registro disparador de acciones para seleccionarla.
3. Hacer clic en [Copiar].
4. Editar el registro, según se necesite.
5. Hacer clic en [Aceptar cambios].

Remover un registro disparadores de acciones

1. Seleccionar **Administración del sistema > Disparadores de acciones**.
2. Hacer clic en registro disparador de acciones para seleccionarla.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Configurando un compartido de red

Como se describe en [Respaldo de Datos](#) en pág. 101, es posible programar respaldos automáticos y que se envíe el archivo de respaldo resultante a un recurso compartido en la red, conocido como un *compartido de red*.

Los compartidos de red pueden configurarse para una carpeta en la red, o para un sistema de archivos remoto que usa uno de los siguientes protocolos de comunicación:

- File Transfer Protocol (FTP)
- File Transfer Protocol Secure (FTPS)
- Common Internet File System (CIFS)

Añadir un compartido de red

Para configurar un compartido de red para respaldos programados:

1. Seleccionar **Administración del sistema > Compartido de red**.
2. Hacer clic en [Añadir].
3. Seleccionar un protocolo de comunicaciones en el campo **Protocolo** para conexión a un sistema de archivo remoto, o seleccionar *Ninguno* para usar una carpeta de red.

Nota: A medida que se ingresan datos en los campos en la página compartido de red el campo **Nombre del compartido** se cambia para reflejar la nueva información.

4. Si FTP o FTPS fueron seleccionados en el [paso 3](#), escribir el número del puerto de la conexión en el campo **Puerto**.
5. Escribir la dirección IP o nombre del anfitrión del compartido de red en el campo **anfitrión**.
6. Escribir la dirección del directorio en el compartido de red en el campo **anfitrión**.
7. Si un protocolo de sistema de archivo remoto fue seleccionado en el [paso 3](#), escribir el nombre de usuario que se necesita para iniciar sesión en el sistema en el campo **usuario**.

8. Si un protocolo de sistema de archivo remoto fue seleccionado en el [paso 3](#), escribir el la contraseña que se necesita para iniciar sesión en el sistema en el campo **contraseña**.
9. Hacer clic en [Aceptar cambios].

Copiar un compartido de red

1. Seleccionar **Administración del sistema > Compartido de red**.
2. Hacer clic en el compartido de red para seleccionarla.
3. Hacer clic en [Copiar].
4. Editar el compartido de red, según se necesite.
5. Hacer clic en [Aceptar cambios].

Remover un compartido de red

1. Seleccionar **Administración del sistema > Compartido de red**.
2. Hacer clic en el compartido de red para seleccionarla.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Crear un respaldo y un punto de restauración

Después de configurar el sistema, es importante:

- Crear un archivo de respaldo que incluya todos los registros, fotos y ajustes configurados en el sistema. Ver [Respaldo de Datos](#) en pág. 101.
- Crear un punto de restauración que incluya todos los datos normalmente salvados en un archivo de respaldo más los ajustes personalizados del controlador del sistema. Esta información se salvará en el controlador del sistema y puede restablecerse más tarde para regresar el sistema a su estado de operación inicial. Ver [Salvar y Restablecer los ajustes personalizados](#) en pág. 104.

El acceso a las instalaciones y la interfaz de usuario pueden ser administradas para:

- Añadir y remover personas,
- Añadir, desactivar, reactivar y remover credenciales y
- Añadir y remover cuentas de usuario.

Los temas en este capítulo incluyen:

- [Administración de personas](#) en pág. 70
- [Administración de credenciales](#) en pág. 72
- [Administración de credenciales perdidas o robadas](#) en pág. 74
- [Administración Cuentas de usuarios](#) en pág. 75
- [Crear Reportes](#) en pág. 76
- [Búsqueda de personas](#) en pág. 77

Administración de personas

Cada persona en la organización puede tener acceso al edificio y al sistema. El acceso a las instalaciones físicas se controla con una credencial (tarjeta de identificación). El acceso al sistema se controla por medio de una cuenta de usuario para iniciar sesión en el controlador. Para mantener organizadas las credenciales y cuentas de usuario, el sistema las asocia con el registro de cada persona que forma parte de la organización. Este registro individual en la base de datos se llama "persona", porque corresponde a una persona real.

Es importante distinguir entre las personas, las credenciales y las cuentas de usuario. En primer lugar, todos los que necesitan entrar en las instalaciones necesitan una credencial (una tarjeta de identificación con un número codificado que el sistema reconoce). Sin embargo, no todos los que necesitan tener acceso a las instalaciones necesitan también tener acceso al sistema con una cuenta de usuario. En segundo lugar, solo los que operan y administran el sistema necesitan cuentas de usuario. En tercer lugar, en algunos casos, los operadores del sistema se encuentran fuera de las instalaciones en una estación central y, por lo tanto, no necesitan una credencial para acceder a las instalaciones físicas, a pesar de que tienen una cuenta de usuario.

Los registros de la base de datos, "personas", permite a los usuarios administrar convenientemente las credenciales y cuentas de usuario desde un registro, en lugar de mantener bases de datos separadas para los usuarios del sistema y credenciales de acceso a instalaciones.

Añadir una persona

Antes de añadir registros de personas, asegurarse de:

- Asignar a cada registro personal un número de identificación individual de algún tipo. Puede ser el número de empleado, por ejemplo.
- Añadir los campos definidos por el usuario necesarios que pueden usarse para ingresar los datos personales de los empleados, tales como las placas del auto o el número telefónico del domicilio. Ver [Configuración de los Campos definidos por el usuario](#) en pág. 53.

Hay varias formas de añadir registros de personas:

- Por medio de la página **Administración de acceso > Personas**, como se describe a continuación.
- Usando el asistente Añadir persona disponible en la página **Inicio**.
- El Asistente de importación/exportación proporcionado en el disco Utilitarios puede usarse para importar registros de personas y datos de credencial que ya existen en formato CSV (por ejemplo, si estos datos se exportaron desde otro sistema de control de acceso o desde la base de datos de empleados). Referirse a la guía *Asistente de importación/exportación* para más detalles.
- Usando la Lectora de entrada opcional. Ver [Instalar una lectora de enrolamiento](#) en pág. 78.

Para añadir registros de personas en la página **Administración de acceso > Personas**:

1. Hacer clic en **Administración de acceso > Personas**.
2. Hacer clic en [Añadir].
3. Escribir un **nombre** y un **apellido**.
4. Hacer clic en la etiqueta **Detalles**.
5. Escribir la información solicitada en los campos definidos por el usuario.
6. Si la persona va a usar el software del sistema, hacer clic en la etiqueta **cuentas de usuario** y crear la cuenta. Ver [Añadir una cuenta de usuario en la página 82](#).
7. Hacer clic en [Aceptar cambios].

8. Si la persona requiere una credencial de acceso a las instalaciones físicas, consultar **Añadir una credencial** página 79.

Remover una persona

El sistema puede almacenar hasta 10.000 registros de personas. Sin embargo, las personas que ya no requieren acceso a las instalaciones o al sistema deben removerse de la base de datos.

Nota: Para eliminar varias personas en un solo lote, usar el Asistente de importación/exportación proporcionado en el disco Utilitarios.

1. Hacer clic en **Administración de acceso > Personas**.
2. En la lista de personas, seleccionar la persona.
3. Hacer clic en [Remover].
Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

Cargar foto ID de una Persona

Las personas pueden tener una foto de identificación asociada a su registro. Una miniatura de esta foto aparecerá cada vez que se produce un evento de acceso relativo a la credencial de la persona.

Notar los siguientes detalles sobre cómo cargar fotos:

- Los formatos de archivo soportados incluyen GIF, JPG y PNG.
- Fotos de hasta 200 KB de tamaño se pueden cargar, pero el tamaño se ajustará automáticamente a 10 KB o menos, en formato JPG.
- El total de almacenaje de fotos está limitado a 40 MB.
- Si se cargan fotos más grandes, el tamaño máximo de 40 MB puede agotarse antes de alcanzar la capacidad de 10,000.

Para cargar una foto:

1. Hacer clic en **Administración de acceso > Personas**.
2. En la lista de personas, seleccionar la persona.
3. Hacer clic en el icono de la foto de identificación que se encuentra al lado del nombre de la persona.
Aparece el cuadro de diálogo Cargar foto.
4. Hacer clic en **Seleccionar archivo**.
Aparece la caja de diálogo Seleccionar archivo.
5. Seleccionar la foto a cargar y hacer clic en **Abrir**.
6. Hacer clic en **Cargar**.
7. Desaparece la caja de diálogo Seleccionar archivo.
8. Hacer clic en [Aceptar cambios].

Nota: Para cargar una foto existente, hacer clic en la foto existente y repetir los pasos siguientes.

Remover foto ID de una Persona

1. Hacer clic en **Administración de acceso > Personas**.
2. En la lista de personas, seleccionar la persona.
3. Hacer clic en el icono de la foto de identificación que se encuentra al lado del nombre de la persona.
Aparece el cuadro de diálogo Cargar foto.
4. Hacer clic en **Remover**.
5. Cuando aparece el mensaje de confirmación, hacer clic en **Remover**.

Administración de credenciales

En primer lugar, todos los que necesitan entrar en las instalaciones necesitan una credencial (una tarjeta de ID con un número codificado que el sistema reconoce). Antes de asignar una credencial, añadir la persona a la base de datos. Ver [Añadir una persona en la página 76](#).

Nota: Siempre que se cambien o se borren credenciales, la caché local en controlador de puerta sencilla basado en IP se despeja para evitar acceso no autorizado en caso de que se utilice el modo fallback del controlador de puerta sencilla basado en IP. Ver [Modo fallback del controlador de puerta sencilla basado en IP](#) en pág. 19.

Instalar una lectora de enrolamiento

La lectora de enrolamiento opcional (TP-RDR-LRN) se puede conectar con una estación de trabajo de cliente local y usarse para leer credenciales. Los datos de credenciales se insertarán automáticamente en el campo **ID de credencial** en la página **Administración de acceso > Personas**. Este dispositivo puede ahorrar tiempo si se está añadiendo un número considerable de credenciales.

Instalar y configurar la lectora en la estación de trabajo del cliente de acuerdo a las instrucciones del fabricante, que están disponibles en línea en www.rfideas.com. Descargar el utilitario de configuración pcProx, que incluye documentación para la lectora pcProx Plus (i.e., la TP-RDR-LRN).

Notar los siguientes detalles sobre la configuración de lectora de enrolamiento:

- Si se usan las credenciales con un código de instalación, configurar la lectora RF para separar el código de instalación del código de credencial en la credencial.
- El utilitario de configuración pcProx usa archivos .hwg para configurar la lectora de enrolamiento. Usar el archivo de configuración Casi_card.hwg configuration para reconocer las credenciales CASI Prox.

Añadir una credencial

Antes de agregar una credencial a una persona, es necesario crear un registro de esa persona. Ver [Añadir una persona en la página 76](#).

1. Seleccionar **Administración de acceso > Personas**.
2. Seleccionar la persona que necesita la credencial.
3. Hacer clic en [Credenciales].
4. Hacer clic en [Añadir credencial].

5. Hacer clic en la etiqueta **General**.

6. Escribir la **ID de credencial**.

Si se anexa una lectora de enrolamiento opcional a la estación de trabajo del cliente local, hacer clic dentro del campo **ID de credencial** después deslizar la tarjeta de la persona través de la lectora para llenar el campo.

7. (Opcional) escribir el código **PIN**.

Nota: Utilizar un signo de numeral (#) al final de cada PIN, sobre todo si la longitud del PIN es menor que la **Longitud máxima de PIN** definida en la etiqueta Seguridad de la página **Administración del sistema > Ajustes del sistema**. Se requieren signos de numeral para los PINs utilizados en los dispositivos conectados a los controladores de puerta sencilla basados en IP.

8. (Opcional) seleccionar **Usar tiempo ampliado de apertura/mantener abierto** si la persona titular de la credencial necesita más tiempo para abrir y pasar por las puertas.

9. (Opcional) seleccionar **Exento de Anti-passback**, si se usa la función Anti-passback y esta credencial no ha de rastrearse.

10. (Opcional) seleccionar una fecha de **activa desde** y **activa hasta**, si la credencial tiene validez temporal.

11. Hacer clic en la etiqueta **Niveles de acceso**.

12. Seleccionar los niveles de acceso correspondientes a la credencial.

13. Hacer clic en [Aceptar cambios].

Remover una credencial

No es necesario que se remueva una credencial para evitar su uso. Por ejemplo, si una persona reporta la pérdida de una credencial, en lugar de eliminar la credencial de inmediato, se puede desactivar hasta que la persona haya tenido tiempo de buscarla. Si no se la encuentra, entonces, cuando la persona solicita una nueva credencial, se puede remover la credencial perdida. Ver [Evitar el uso de una credencial perdida o robada en la página 81](#).

1. Seleccionar **Administración de acceso > Personas**.

2. Seleccionar la Persona titular de la credencial por borrar.

3. Hacer clic en [Credenciales].

4. Hacer clic en la credencial por borrar.

5. Hacer clic en [Remover credencial].

6. Hacer clic en [Remover].

7. Cuando aparece la caja de diálogo Remover Objeto, hacer clic en [Remover].

Administración de credenciales perdidas o robadas

Si una persona reporta la pérdida de una credencial, en lugar de eliminar la credencial de inmediato, se puede desactivar hasta que la persona haya tenido tiempo de buscarla. Si no se la encuentra, entonces, cuando la persona solicita una nueva credencial, se puede remover la credencial perdida.

La desactivación de una credencial tiene otra ventaja. Dado que cualquier credencial no válida que pase por una lectora genera un evento, si la credencial todavía está asignada a una persona, el evento indica específicamente tal persona como tratando de usar una credencial no válida. Si hay cámaras de video que monitorean los eventos de las puertas y las lectoras, existe una imagen de la persona que intentó usar la credencial después que fue reportada como robada. Una búsqueda en la base de datos de eventos de la persona que perdió la credencial muestra todos los incidentes relacionados con esa persona antes y después de que la credencial fuera reportada como perdida. De esta manera, se puede establecer una asociación entre la víctima y el autor del robo.

Evitar el uso de una credencial perdida o robada

Usar esta tarea para desactivar una credencial en vez de eliminarla.

1. Seleccionar **Administración de acceso > Personas**.
2. Seleccionar la persona titular de la credencial a desactivar.
3. Hacer clic en [Credenciales].
4. Hacer clic en la credencial a desactivar.
5. Hacer clic en el campo **Activo hasta**.
Aparece la ventana emergente del calendario.
6. Seleccionar una fecha pasada.
7. Hacer clic en [Aceptar cambios].

Restablecer una credencial encontrada

1. Seleccionar **Administración de acceso > Personas**.
2. Seleccionar la persona titular de la credencial a desactivar.
3. Hacer clic en [Credenciales].
4. Hacer clic en la credencial a reactivar.
5. Borrar el campo **Activo hasta**.
6. Hacer clic en [Aceptar cambios].

Administración Cuentas de usuarios

Las cuentas de usuarios permiten iniciar sesión en el sistema. Una cuenta de usuario está asociada con el registro de una persona en la base de datos, al igual que una credencial. Sin embargo, las personas no necesitan tener una cuenta de usuario para tener acceso a las instalaciones con una credencial.

Añadir una cuenta de usuario

Antes de agregar una credencial a una persona, es necesario crear un registro de esa persona. Ver [Añadir una persona en la página 76](#).

1. Iniciar sesión como administrador o distribuidor. (Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.)
2. Seleccionar **Administración de acceso > Personas**.
3. Seleccionar la persona por modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Seleccionar **Puede iniciar sesión**.
6. Escribir un **Nombre de usuario**.
7. Hacer clic en [Ajustar contraseña].
8. Escribir la nueva contraseña en los campos **Ingresar nueva contraseña** y **Confirmar contraseña**.
9. Hacer clic en [OK].
10. Seleccionar un **Rol**.
11. Hacer clic en [Aceptar cambios].

Cambiar un nombre de usuario y contraseña

1. Iniciar sesión como administrador o distribuidor. (Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.)
2. Seleccionar **Administración de acceso > Personas**.
3. Seleccionar la persona por modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Escribir un nuevo **Nombre de usuario**.
6. Hacer clic en [Ajustar contraseña].
7. Escribir la nueva contraseña en los campos **Ingresar nueva contraseña** y **Confirmar contraseña**.
8. Hacer clic en [OK].
9. Hacer clic en [Aceptar cambios].

Desactivar una cuenta de usuario

1. Iniciar sesión como administrador o distribuidor. (Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.)
2. Seleccionar **Administración de acceso > Personas**.
3. Seleccionar la persona por modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Limpiar la casilla **Se puede iniciar sesión**.

6. Hacer clic en [Aceptar cambios].

Crear Reportes

Cinco reportes predefinidos que permiten ver la información almacenada en la base de datos del servidor:

Historial de acceso

Permite ver un resumen de los intentos de acceso por persona, filtrados por intervalo de fechas, nombre de persona (comodín), lectora, área y respuesta de autorizado o denegado.

Credencial

Permite ver una lista de credenciales asignadas, filtrada por nombre de persona (comodín), identificación de la credencial (comodín), nivel de acceso, y estado activa o inactiva.

Acceso a lectoras

Permite ver una lista de personas con acceso a cada lectora, filtrada por nombre de persona (comodín) y lectora.

Lista de asistencia

Permite ver una lista de personas por área actual o última lectora, filtrada por nombre de persona (comodín), área, lectora y eventos. Seleccionar **Incluir eventos "Acceso/egreso concedido - sin entrada** para incluir los eventos que ocurrieron pero no se puede determinar si ocurrió el acceso o egreso.

Nómina

Permite ver una lista de todas las personas en la base de datos, filtrada por nombre de persona (comodín) y privilegios de inicio de sesión.

Notar los siguientes detalles sobre los reportes:

- Los reportes se muestran en formato HTML, en una ventana del navegador de Internet. Si se usa Internet Explorer 7 o anterior, el logo del producto en la esquina superior derecha no se muestra bien. Esta es una limitación de las versiones anteriores de Internet Explorer.
- Si los nombres de entidad (p. ej., nombres de dispositivos, nombres de personas) cambian, el nombre actualizado de la entidad se refleja en el siguiente reporte.

Crear un reporte

1. Seleccionar **Reportes**.
2. Seleccionar el tipo de reporte por añadir.
3. Llenar los campos específicos del reporte como se necesite.
4. Hacer clic en [Ver] para mostrar el reporte en una ventana de navegador nueva.
5. Para exportar un reporte:
 - a. Hacer clic en [Exportar].
 - b. Cuando se indique, hacer clic en [Salvar].
 - c. En la caja de diálogo que aparece, navegar a la ubicación en donde se salvará el reporte en formato CSV.
 - d. Hacer clic en [Salvar].

Nota: Si continúa apareciendo la notificación "Generando reportes" y se opaca la interfaz de usuario principal, la estación de trabajo local está baja de memoria. Cerrar la ventana del navegador y terminar la sesión, cerrar los programas abiertos que no se necesiten en el momento, volver a iniciar sesión e intentar crear el reporte de nuevo.

Búsqueda de personas

La función de búsqueda filtra la base de datos y genera una lista de los registros de personas con un campo que coincide en todo o en parte con los requisitos de la búsqueda.

Buscar personas

1. Seleccionar **Administración de acceso > Personas**.
2. Hacer clic en [Buscar] y seleccionar un campo por buscar.

El botón [Buscar] aparece junto a la caja de texto Buscar y se muestra como una lupa. Cuando se hace clic, una lista de los campos que se pueden buscar aparecen abajo del botón.
3. Escribir el término por buscar.
4. Presionar <Ingresar>.

Cancelar la búsqueda

Los resultados de la búsqueda continúan el filtrado de la base de datos, incluso si se pasa a otra página y se vuelve a la página **Personas**, hasta que se cancela la búsqueda.

1. Seleccionar **Administración de acceso > Personas**.
2. Hacer clic en la **X** para borrar el campo de búsqueda.

Durante las operaciones cotidianas, el acceso a las instalaciones puede ser monitoreado y controlado por medio de:

- Visualización de eventos.
- La visualización de video de las cámaras de seguridad, si se han instalado cámaras.
- La anulación del comportamiento programado de las puertas, para abrirlas, desbloquearlas, bloquearlas o restablecerlas.
- Respuesta a las alarmas.

Los temas en este capítulo incluyen:

- [Monitoreo de eventos y alarmas](#) en pág. 80
- [Monitoreo de eventos de video](#) en pág. 82
- [Control de puertas](#) en pág. 87
- [Control de entradas y salidas](#) en pág. 91
- [Controlar disparadores de acciones](#) en pág. 92
- [Reajustar Anti-passback](#) en pág. 93

Monitoreo de eventos y alarmas

La página **Eventos** proporciona un registro de:

- Problemas de acceso
 - Acceso no autorizado
 - Violación de Anti-passback
 - Puertas mantenidas abiertas demasiado tiempo
 - Inicio de sesión en el sistema
- Mensajes de estado del sistema y los dispositivos
 - Cambios en el estado del sistema, tales como actualizaciones de la hora y fecha
 - Cambios de modo de los dispositivos
 - Cambios en el estado de disparadores de acciones
 - Respaldos de base de datos y eventos
- Alarmas
 - Sabotaje de puertas
 - Puertas apertura forzada
 - Fallas o problemas del sistema

Notar los siguientes detalles sobre la página **Eventos**:

- Todo evento asociado a un dispositivo conectado a una cámara tiene un registro en video del evento.
- Para ordenar los eventos, hacer clic en un encabezado de columna.
- La página **Eventos** se desplegará automáticamente cuando se genera un evento nuevo. Si la lista está ordenada por fecha y hora mostrando el evento más reciente arriba, la lista se reorganizará para mostrar un evento nuevo siempre en la parte de arriba.
- Hacer clic en la columna Dispositivo para acceso a la página **Monitoreo > Puertas** y mostrar detalles sobre el dispositivo.

Hacer clic en un evento para mostrar un panel de detalles que muestra la fecha y hora del evento, junto con una descripción del mismo. Adicionalmente se proporciona información sobre el evento dependiendo de si el evento se relaciona con una persona (por ejemplo, Acceso concedido) o dispositivo específico (por ejemplo, Puerta desbloqueada):

- Para eventos relacionado con personas, el panel de detalles también incluye el nombre, credencial y foto de la persona, si están disponibles. Hacer clic doble en la foto para acceder la página **Administración de acceso > Personas** y mostrar los detalles del individuo.
- Para eventos con dispositivos específicos, el panel de detalles incluye una descripción del evento, fecha, hora, y la información del dispositivo y del video relativo al evento, de estar disponible.

Hacer clic en el botón [Cerrar] en el panel detalles al terminar la revisión de la información del evento.

Ver últimos eventos

Los últimos eventos se muestran en la esquina inferior izquierda de la página. Si se produce un evento mientras se está trabajando en otra página, pasando el cursor sobre el evento, se puede mostrar un resumen del evento, que incluye una foto en miniatura de la persona implicada.

La ventana emergente muestra la fecha y hora del evento, una descripción del evento y la credencial. Debajo de eso aparece la foto y el nombre de la persona.

Cargar más eventos

La página **Eventos** muestra los eventos más recientes. Para ver eventos más antiguos que los que se muestran, primero hay que cargarlos al navegador desde el sistema. El comando Cargar más eventos cargará los próximos 500 eventos (o menos, si hay menos de 500).

1. Seleccionar **Eventos**.
2. Hacer clic en el botón de mando [Eventos].
3. Seleccionar **Cargar más eventos**.
4. (Opcional) para detener la operación, hacer clic en **Cancelar** , cuando aparezca.

Cargar todos los eventos

La página **Eventos** muestra los eventos más recientes. Para ver eventos más antiguos que los que se muestran, primero hay que cargarlos al navegador desde el sistema. El comando Cargar todos los eventos carga todos los eventos del controlador del sistema al navegador y puede tardar varios minutos en completarse.

1. Seleccionar **Eventos**.
2. Hacer clic en el botón de mando [Eventos].
3. Seleccionar **Cargar más eventos**.
4. (Opcional) para detener la operación, hacer clic en **Cancelar** , cuando aparezca.

Buscar eventos

Usar la función de búsqueda para filtrar la lista de eventos exhibidos por una o más facetas.

1. Seleccionar **Eventos**.
2. Hacer clic en el icono **Filtro**, que se encuentra en el lado derecho de la página.
3. Escribir los criterios de búsqueda en los campos correspondientes.
Cuanto más criterios se usan, más preciso es el resultado de la búsqueda.
4. Presionar <Ingresar>.

Exportar eventos

El sistema puede almacenar hasta 65.535 eventos. Una vez que se alcanza este límite, se eliminan los eventos más antiguos, según sea necesario para hacer espacio. Usar el comando Exportar eventos para almacenar un registro de eventos en formato de valores separados por comas (CSV).

1. Seleccionar **Eventos**.
2. Hacer clic en el botón de mando [Eventos].
3. Seleccionar **Exportar eventos**.
4. Seleccionar la ubicación en la estación de trabajo del cliente en donde se salvó el archivo.
5. Escribir un nombre descriptivo con la extensión **.csv**.
6. Hacer clic en **Salvar**.

Monitoreo de eventos de video

El sistema puede mostrar el video en vivo (o grabado) de cámaras específicas y asociar el video grabado a eventos registrados de dispositivos específicos, tales como lectoras y puertas. (Ver [Configuración de dispositivos de video](#) en pág. 35.)

Los enlaces a video de eventos específicos se encuentran en la página **Eventos**. La página **Monitorear > Video** permite monitorear en directo el video de una o más cámaras. Los clips de video en vivo o grabado pueden descargarse a una estación de trabajo de cliente local.

Antes de comenzar

Antes de reproducir video ya sea en la página **Eventos** o en **Monitorear > Video**, verificar que los ajustes de seguridad para Internet Explorer estén ajustados en forma adecuada, como se describe a continuación.

1. Abrir Internet Explorer.
2. En el menú Herramientas, hacer clic en **opciones de Internet**.
3. Cambiar a la etiqueta Seguridad y hacer clic en [Nivel de personalización...].

Nota: Si el botón **Nivel de personalización...** no está activado, se deben establecer políticas de seguridad para evitar que los usuarios puedan cambiar los ajustes de Internet Explorer. Contactar al administrador de la red o ejecutar Internet Explorer como administrador.

4. Desplazarse por la lista de configuración de seguridad para mostrar los controles ActiveX y la configuración de plug-ins.
5. Para *Pedir automáticamente los controles ActiveX*, hacer clic en **Activar**.
6. Para *Descargar controles ActiveX firmados*, hacer clic en **Activar** o en **Pedir**.
7. Para *Inicializar y controles de secuencia de comandos ActiveX que no están marcados como seguros para secuencia de comandos*, hacer clic en **Activar** o en **Pedir**.
8. Para *Ejecutar controles ActiveX y plug-ins*, hacer clic en **Activar** o en **Pedir**.
9. Para los *Controles de secuencia de comandos ActiveX marcados como seguros para secuencia de comandos*, hacer clic en **Activar** o en **Pedir**.
10. Desplazarse por la lista de configuración de seguridad para mostrar los ajustes varios.
11. Para *Secuencias de comandos ActiveX*, hacer clic en **Activar** o en **Pedir**.
12. Desplazarse por la lista de configuración de seguridad para mostrar los ajustes de secuencias de comandos.
13. Para *Usar el bloqueador de pop-up*, hacer clic en **Desactivar**.
14. Hacer clic en **OK**, y después hacer clic en **OK** de nuevo para salvar los ajustes.

También la primera vez que se accede el video, aparecerá un mensaje que indica que se debe instalar un reproductor de video propietario. Hacer clic en [Descargar e instalar] para instalar el software. (Si las políticas de seguridad de la red bloquean la descarga, contactar al administrador de la red o ejecutar Internet Explorer como administrador.) Después de que aparezca un mensaje que indica que la reproductora de video se ha instalado correctamente, salir del sistema y reiniciar sesión para acceder a video.

IMPORTANTE: Los usuarios existentes TruPortal 1.0 o goEntry 3.0 deben desinstalar (si procede) la versión actual del control TruPortal ActiveX a través de la opción **Panel de control > Programas y características > Desinstalar un**

programa antes de instalar el reproductor de video de propiedad actualizado.

Reproducir video de eventos

En la página **Eventos**, los eventos con video grabado asociado tienen un icono hipervinculado de una cámara () al lado de la descripción del evento.

1. Seleccionar **Eventos**.
2. Desplazarse o buscar el evento.
3. Hacer clic en el icono de la **cámara** que aparece junto a la descripción del evento.
El panel Detalle de eventos aparece en la parte inferior de la página junto con un cuadro de video.
4. Hacer clic en [Reproducir video del evento].
5. Desplazarse sobre la parte inferior del cuadro de video para mostrar los controles que se pueden usar para reproducir y grabar video. Ver [Referencia controles de video](#) en pág. 90.

Monitorear video

Mientras que la página **Eventos** permite ver video grabado de eventos vinculados a dispositivos específicos, la página **Monitorear > Video** permite a los usuarios monitorear la seguridad general de las instalaciones. Por ejemplo, si una persona sospechosa estuviera acechando el estacionamiento, no daría lugar a un evento de puerta o lectora, pero si hay una cámara de vigilancia en el estacionamiento, un usuario podría detectar la presencia de tal persona mirando el video de dicha cámara.

Nota: Antes de que se pueda monitorear el video grabado añadir al menos una plantilla de video. Ver [Añadir plantillas video](#) en pág. 38.

Para monitorear video:

1. Seleccionar **Monitorear > Video**.

Nota: Si aparece un mensaje que indica que la reproductora de video tiene que ser instalada, hacer clic en [Descargar e Instalar]. Al finalizar la instalación, cerrar la sesión y reiniciarla para ver el video del evento. Ver [Antes de comenzar](#) en pág. 88 para más detalles.

2. Seleccionar una **plantilla**.
3. Para ver video en vivo, pulsar el botón [En vivo].
4. Para ver el video grabado, hacer clic en [Reproducir] y seleccionar una opción en el menú que aparece.
5. (Opcional) Para reposicionar una cámara con movimiento horizontal, vertical y zoom, hacer clic en el botón **PTZ** para abrir y ajustar los controles de PTZ.

Descargar un clip de video

Los clips de video pueden descargarse desde las páginas **Eventos** y **Monitorear > Video**, como se describe a continuación.

1. Desplazarse sobre la parte inferior del cuadro de video para mostrar los controles que se pueden usar para reproducir y grabar video. Ver [Referencia controles de video](#) en pág. 90.
2. Para descargar un clip de video en vivo:
 - a. Hacer clic en [Reproducir].
 - b. Seleccionar **En vivo** desde el menú que aparece.
 - c. Hacer clic en el botón **Grabar/reproducir video en vivo**.
 - d. Navegar hasta una carpeta en la caja de dialogo que aparece, y hacer clic en **OK**.
 - e. Hacer clic en el botón **Grabar/reproducir video en vivo** de nuevo para parar la grabación de video en vivo.

Nota: Cambiar al modo reproducción mientras el video se está descargando detendrá el proceso de descarga.

El clip de video se descarga en la carpeta seleccionada.

3. Para descargar un clip de video en vivo:
 - a. Hacer clic en el botón **Reproducir**.
 - b. Seleccionar *2 minutos* desde el menú Reproducir que aparece.
 - c. Esperar durante 30 segundos.
 - d. Hacer clic en el botón **Grabar/reproducir video en vivo**.
Una barra de tiempo aparece en el cuadro de video.
 - e. Mover el control deslizante a la marca de 1 minuto y hacer clic en **OK**.
 - f. Navegar hasta una carpeta en la caja de dialogo que aparece, y hacer clic en **OK**.
El clip de video se descarga en la carpeta seleccionada.

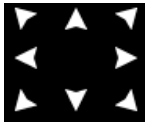
Nota: Si el video no se puede descargar desde una cámara conectada a un TVR31, intentar ajustar la configuración del acelerador de ancho de banda en la TVR31.

Para ver los clips de video descargados, utilizar TruVision Navigator Player proporcionado en el disco del producto en la carpeta \ VideoPlayer.

Referencia controles de video

FIGURA 1. Controles de video



Icono	Característica	Función
	Control del iris	Abre o cierra el iris de la cámara para ajustarlo a la cantidad de luz disponible
	Control del foco	Ajusta el foco de la imagen.
	Control de zoom	Ajusta el zoom de la cámara.
	Controles de movimiento horizontal y vertical	Mueve la cámara en la dirección indicada por la flecha correspondiente.
	Control de retroceso cuadro a cuadro	Retrocede un cuadro el video grabado.

Icono	Característica	Función
	Control de retroceso	Retrocede el video.
	Control de reproducción	Reproduce la transmisión de video (en vivo o grabado).
	Control de pausa	Detiene la transmisión de video (en vivo o grabado).
	Control de avance	Avanza el video grabado en avance rápido.
	Control de avance cuadro a cuadro	Avanza un cuadro el video grabado.
	Control de video	Cambia de reproducción de video grabado a visualización de video en vivo.
	Control de reproducción	Menú de selección de opciones de reproducción, desde en vivo a varios minutos anteriores.
	Control de preajustes	Mueve la cámara rápidamente a la posición preajustar.
	Activar control PTZ	Abre los controles de movimiento horizontal, vertical y zoom (solo funciona con cámaras PTZ).
	Control de video grabar en vivo/ reproducir	Graba video.

Control de puertas

La página **Monitorear > Puertas** muestra el estado de las puertas, las lectoras asignadas, los eventos recientes en esas puertas y los programas asignados. Esta página permite que los operadores bloqueen, abran, restablezcan y desbloqueen las puertas.

Abrir una puerta

Usar el comando Abrir puerta para abrir una puerta para alguien sin credencial.

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Hacer clic en el botón de acción **Comandos de puerta individual** correspondiente a la puerta que se desea abrir.
4. Seleccionar **Abrir puerta**.

Desbloquear una puerta

Usar el comando Desbloquear puerta para anular la seguridad de la puerta, permitiendo que cualquiera pueda salir o entrar sin presentar una credencial válida.

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Hacer clic en el botón de acción **Comandos de puerta individual** correspondiente a la puerta que se desea desbloquear.
4. Seleccionar **Desbloquear puerta**.

Restablecer una puerta

Usar el comando Restablecer puerta para volver la puerta a su modo normal de funcionamiento, tras bloquearla o desbloquearla.

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Hacer clic en el botón de acción **Comandos de puerta individual** correspondiente a la puerta que se desea restablecer.
4. Seleccionar **Restablecer puerta**.

Bloquear una puerta

Usar el comando Bloquear puerta para bloquear una puerta y cambiar el modo de la lectora para evitar que se conceda acceso a cualquiera de las credenciales en la puerta.

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Hacer clic en el botón de acción **Comandos de puerta individual** correspondiente a la puerta que se desea bloquear.
4. Seleccionar **Bloquear puerta**.

Asegurar una puerta

Usar el comando Asegurar puerta para asegurar una puerta.

1. Seleccionar **Monitoreo > Puertas**.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Hacer clic en el botón de acción **Comandos de puerta individual** correspondiente a la puerta que se desea asegurar.
4. Seleccionar **Asegurar puerta**.

Nota: Para proporcionar una forma rápida de asegurar todas las puertas en la instalación, crear un registro de disparadores de acciones para bloquear todas las puertas y entonces dispararla manualmente en la página **Monitoreo > disparadores de acciones** cuando sea necesario. Ver [Configuración de Disparadores de acciones](#) en pág. 56.

Restablecer todas las puertas

Usar el comando Restablecer todas las puertas para volver las lectoras conectadas a puertas a su modo normal de funcionamiento, tras bloquear o desbloquear todas las puertas a menos de que esté activa una **entrada** de desbloqueo designada. Se configura una entrada de desbloqueo en la página **Administración del sistema > Dispositivos > Controlador**.

1. Seleccionar **Monitoreo > Puertas**.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Restablecer todas las puertas**.

Un evento reinstalado de lectora se genera para cada lectora que se encontraba en estado de Bloqueo, junto con un sólo evento reinstalado de Todas las puertas para el controlador del sistema. Un evento Modo lectora de entrada sólo tarjeta o un evento Modo lectora de entrada tarjeta + PIN también se genera para cada puerta, en función de cómo esté configurada la lectora en la página de **Administración del sistema > Dispositivos**.

Bloquear todas las puertas

Usar comandos de Bloquear todas las puertas para bloquear las puerta y cambiar el modo de la lectora para evitar que se conceda acceso a cualquiera de las credenciales en las puertas. Cualesquier acciones que puedan impactar la apertura de puerta no tendrán ningún efecto hasta que se ejecute el comando global Restaurar todas las puertas.

1. Seleccionar **Monitoreo > Puertas**.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Bloquear todas las puertas**.

Un evento "Lectora bloqueada" se genera para cada lectora que se encontraba en estado de Bloqueo, junto con un sólo evento "Todas las puertas bloqueadas" para el controlador del sistema.

Nota: Aunque todas las puertas estén bloqueadas al agregar un nuevo controlador de puerta, éste permanecerá desbloqueado. Para bloquearlo, se deben restablecer todas las puertas y entonces bloquearlas a todas nuevamente.

Desbloquear todas las puertas

Usar el comando Desbloquear todas las puertas para anular la seguridad de todas las instalaciones, permitiendo que cualquiera pueda salir o entrar sin presentar una credencial válida. Cualesquier acciones que puedan impactar la apertura de puerta no tendrán ningún efecto hasta que se ejecute el comando global Restaurar todas las puertas.

1. Seleccionar **Monitoreo > Puertas**.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Desbloquear todas las puertas**.

Un evento "Lectora reinstalada" se generará para cada lectora que se encontraba bloqueada, junto con un sólo evento "Todas las puertas desbloqueadas" para el controlador del sistema

Menús Comandos de puertas

En ocasiones es necesario sobrescribir el comportamiento normal programado para una puerta específica (por ejemplo para dar acceso a un mensajero) o a un sitio completo (por ejemplo durante un simulacro de incendio). Si un desastre o situación de emergencia ocurre cerca de las instalaciones, todas las puertas pueden necesitar bloquearse. Se pueden controlar puertas individuales desde la etiqueta **Ver eventos** en la página **Monitoreo > Puertas**. Los comandos globales de puertas permiten cambiar con un solo clic el estado de todas las puertas de las instalaciones.

Menú Comandos globales de puertas

Nota: Después de bloquear o desbloquear todas las puertas, se debe usar el comando **Restablecer todas las puertas**, antes de tratar de controlar cualquier puerta de forma individual.

Desbloquear todas las puertas

Libera las cerraduras de todas las puertas, permitiendo entrar y salir libremente. Esto se registra como Evento 14644. Después de expedir este comando, reinstalar todas las puertas de manera que las puertas individuales puedan ser controladas en forma directa.

Bloquear todas las puertas

Bloquea todas las puertas e ignora las credenciales, de modo que nadie puede entrar ni salir. Esto se registra como Evento 14646. Después de expedir este comando, reinstalar todas las puertas de manera que las puertas individuales puedan ser controladas en forma directa.

Restablecer todas las puertas

Restablece todas las puertas a su estado normal, a menos que esté activa una **entrada** de desbloqueo asignada. Se configura una entrada de desbloqueo en la página **Administración del sistema > Dispositivos > Controlador**.

Menú Comandos de puerta individual

Abrir puerta

Desbloquea la puerta durante el período especificado en **Hora de acceso normal autorizado**, en la página **Administración del sistema > Dispositivos**.

Desbloquear puerta.

Libera la cerradura de la puerta, permitiendo entrar y salir libremente, hasta que se cambia el estado de la puerta, ya sea por un programa de lectora o por un comando global (para todas las puertas).

Restablecer puerta.

Restaura la puerta al comportamiento predeterminado según el horario establecido.

Bloquear puerta

Bloquea la puerta e ignora las credenciales, de modo que nadie puede entrar ni salir.

Asegurar puerta

Bloquea la puerta.

Etiqueta Ver eventos

La etiqueta **Ver eventos** de la página **Monitoreo > Puertas** muestra el último evento de la puerta y las lectoras asociadas, y el estado actual de cada puerta y sus lectoras. Se pueden controlar puertas individuales desde la etiqueta **Ver eventos** de la página **Monitoreo > Puertas**.

Etiqueta Ver horarios

La etiqueta **Ver horarios** de la página **Monitoreo > Puertas** permite modificar el comportamiento de las lectoras y las puertas de acuerdo con los horarios establecidos, en vez de manualmente como en la etiqueta **Ver eventos**.

Por ejemplo, si una sala de exposición para clientes tiene una puerta para acceso desde el estacionamiento que debe permanecer bloqueada fuera del horario comercial, pero desbloqueada durante el horario de atención al público, o cuando un vendedor está en la sala de exposición, de modo que los clientes puedan entrar sin dificultad al edificio. En este caso, es posible seleccionar un horario de 9.00 a 17.00 para la puerta y elegir la opción "Primera entrada con tarjeta" para el **Modo de programa**, si se desea que la sala de exposiciones esté desbloqueada solo después de que un vendedor usa una credencial para entrar en la sala.

Programa

En esta lista, seleccionar un programa (los programas se crean en **Administración de acceso > Programas**) para indicar cuándo el Modo de programa seleccionado debe estar activo.

Modo de programa (puerta)

Seleccionar una opción de esta lista para configurar el comportamiento de la puerta específica durante el programa especificado.

Desbloqueado

La puerta permanecerá desbloqueada y accesible sin la presentación de una credencial durante el programa seleccionado.

Primera entrada con tarjeta

La puerta estará bloqueada al principio del programa y permanecerá en este estado hasta que se pase una credencial válida. En ese momento, la puerta cambiará al estado desbloqueado.

Bloqueada

Durante el programa seleccionado, la puerta permanece cerrada y es necesario pasar una credencial válida para entrar.

Modo de horario (lectora)

Seleccionar una opción de esta lista para configurar el comportamiento de la lectora específica durante el horario especificado.

Solo Credencial

Para acceder, solo es necesario presentar una credencial válida (ID de credencial).

Credencial y PIN

Para acceder, es necesario presentar una credencial válida y un número de identificación personal. Esto impide el acceso con una credencial robada o encontrada. Algunas instalaciones usan el modo **Solo credencial** durante el día y **Credencial y PIN** fuera del horario laboral, cuando las instalaciones están vacías.

Salvar modo fallback de puerta

La información de las credenciales se almacena en el controlador del sistema. Si un controlador de puertas no puede comunicarse con el controlador para determinar si debe autorizar el acceso (por ejemplo, debido a una mala conexión), las puertas conectadas a ese controlador de puertas funcionarán en modo fallback:

Restringido

No se autoriza ningún acceso.

Código de Instalación

Se autoriza el acceso si la credencial coincide con uno de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta** y el código de instalación en la tarjeta coincide con el definido para el formato. No se verifica la identidad de la credencial.

Todos

Se autoriza el acceso si la tarjeta coincide con cualquiera de los formatos definidos en la página **Administración del sistema > Formatos de tarjeta**, independientemente del código de instalación y la ID de credencial.

Control de entradas y salidas

Las entradas y salidas se monitorean desde la página **Monitoreo > Entradas/salidas**, desde donde se pueden activar o desactivar manualmente. Las salidas también pueden controlarse por disparadores de acciones. Para obtener más información acerca de entradas y salidas, ver [Configurar entradas y salidas](#) en pág. 25

Activar o desactivar una salida

1. Seleccionar **Monitoreo > Entradas/salidas**.
2. Hacer clic en el botón **Activar/desactivar** correspondiente a la salida.
El estado de la salida cambia.

Controlar disparadores de acciones

En la página **Administración de sistema > Disparadores de acciones**, los disparadores de acciones se pueden configurar para monitorear una o más condiciones de disparadores de acciones junto con las acciones correspondientes que se ejecutarán cuando se satisfacen las condiciones de los disparadores de acciones descritos en [Configuración de Disparadores de acciones](#) en pág. 56.

Dependiendo de cómo se hayan configurado, los registros de disparadores de acciones pueden resultar en dos tipos de acciones:

- Las acciones de activación se ejecutan cuando una condición de disparo se vuelve verdadera, y
- las acciones de desactivación se ejecutan cuando una condición de disparo se vuelve falsa.

Una vez creados, los disparadores de acciones pueden ejecutarse en forma manual en la página **Monitorear > Disparadores de acciones** para lograr que la acción correspondiente sea ejecutada.

Notar los siguientes detalles sobre el control de los disparadores de acciones:

- Los disparadores de acciones que no tienen una acción definida para ellos no aparecerán en la página **Monitorear > disparadores de acciones**.
- Hacer los disparos manualmente no tiene prioridad alguna sobre hacer los disparos por el sistema, ni persiste el estado de disparo. Una vez que se dispara una acción en forma manual, cualquier cambio de estado futuro de la condición disparo del sistema causará que las acciones se ejecuten nuevamente.
- Para proporcionar una forma rápida de asegurar todas las puertas en la instalación, crear un registro de disparadores de acciones para bloquear todas las puertas y entonces dispararla manualmente en la página **Monitoreo > disparadores de acciones** cuando sea necesario.

Ejecutar un registro de disparadores de acciones Manualmente

1. Seleccionar **Monitorear > Disparadores de acciones**.
2. Hacer clic en el botón de acción **Disparar manualmente** para el registro de disparar acciones.
3. Seleccionar **Ejecutar acciones de activación** o **Ejecutar acciones de desactivación**.

Reajustar Anti-passback

La opción Anti-passback requiere el uso de una credencial para entrar y salir de un área. De esta forma, el sistema rastrea en qué área se encuentra el portador de la credencial, mantiene un registro de los movimientos del personal en áreas protegidas e impide el paso a las áreas lógicamente imposibles. Si una persona usa una credencial para entrar en una área configurada como Anti-passback y, luego, sale sin usar la credencial (a través de una puerta mantenida abierta por otra persona, por ejemplo), el sistema no registra la salida del área específica de esa persona. Como resultado, si el sistema está configurado para imponer el Anti-passback obligatorio, impide que esa credencial se use para entrar en otra área, incluyendo la que recién se dejó, hasta que la ubicación de la credencial se reajuste a una área neutra o por default.

1. Seleccionar **Monitoreo > Reajustar Anti-passback**.
2. Para restablecer todas las personas:
 - a. Hacer clic en [Reajustar todo].
 - b. Seleccionar un área de la lista.
3. Para reajustar a personas seleccionadas:
 - a. Seleccionar un rango de personas haciendo clic en el primer nombre de la lista y, luego, mantener apretada la tecla <Shift>, mientras se hace clic en la última persona. El rango de nombres se resalta.
 - b. Seleccionar personas individuales haciendo clic en el primer nombre deseado y, luego, mantener apretada la tecla <Ctrl>, mientras se hace clic en los otros nombres para seleccionarlos.
 - c. Hacer clic en [Reajustar lo seleccionado].
 - d. Seleccionar un área de la lista.

CAPITULO 7 *Mantenimiento*

Unas actividades simples de mantenimiento ayudan a garantizar que el sistema funcione en forma eficiente con un mínimo de problemas e interrupciones. Estos incluyen respaldos de la base de datos y comprobar si hay actualizaciones de firmware.

Los temas en este capítulo incluyen:

- [Respaldo de Datos](#) en pág. 95
- [Salvar y Restablecer los ajustes personalizados](#) en pág. 98
- [Actualización del Firmware](#) en pág. 99
- [Administración de paquetes de idiomas](#) en pág. 101

Respaldo de Datos

Se recomienda respaldar periódicamente la base de datos del sistema, para asegurar la recuperación rápida de sus necesidades de seguridad tras un desastre. El sistema salva las copias de respaldo a la estación de trabajo cliente local, por lo que existe una copia que no está en el controlador del sistema. El archivo de respaldo encriptado incluye todos los registros, las fotos, y los ajustes configurados en el sistema, con la excepción de:

- Los estados puerta/lectora se ajustan manualmente a través de la página **Monitoreo > Puertas** y
- Eventos.

Respaldos de bases de datos también se pueden programar para que ocurran automáticamente, con los correos electrónicos enviados después de los respaldos correctos o incorrectos. Los eventos también se pueden respaldar en un archivo CSV.

Crear una copia de Respaldo

En esta sección se describe cómo crear un archivo de respaldo y descargarlo en una estación de trabajo local. Los datos del sistema se pueden copiar a un archivo en la estación de trabajo cliente (como se describe aquí) o se pueden programar respaldos automáticos, tal como se describe en la siguiente sección. (Para respaldar eventos, consultar [Respaldar Eventos](#) en pág. 103.)

1. Iniciar sesión en el sistema como usuario con permisos de ejecución para la función de respaldo de base de datos.
2. Seleccionar **Administración del sistema > respaldo/restablecimiento**.
3. Hacer clic en [Descargar archivo de respaldo].
Aparece la caja de diálogo respaldo base de datos.
4. Hacer clic en [Descargar archivo de respaldo].
5. Seleccionar una ubicación para el archivo de respaldo.
6. Hacer clic en [Salvar].

IMPORTANTE: El nombre del archivo de respaldo de la base de datos contiene una suma de verificación requerida para restablecer el sistema (por ejemplo, backup_1926651153.bak). No editar los caracteres que aparecen después del carácter de subrayado (_) en el nombre del archivo.

Programar respaldos automáticos

Respaldos automáticos pueden ser programados para ocurrir hasta siete veces por semana, con el archivo de respaldo resultante enviado a un recurso de red compartido (ver [Configurando un compartido de red](#) en pág. 72). Si el sistema está configurado para enviar correos electrónicos automáticos, una notificación se envía después de que ocurren respaldos programados.

Nota: Los respaldos programados deben separarse al menos por 30 minutos.

1. Iniciar sesión en el sistema como usuario con permisos de ejecución para la función de respaldos programados.
2. Seleccionar **Administración del sistema > respaldo/restablecimiento**.
3. Hacer clic en [Respaldar programa].
4. Para crear una programación para un respaldo de base de datos:
 - a. En el área de configuración de programa de base de datos de la página, seleccionar **Programa activado**.
 - b. Seleccionar los días en que el programa será respaldado.
 - c. Seleccionar una hora para el respaldo.
 - d. Seleccionar la ubicación a donde se enviará el archivo de respaldo en el campo de recursos **compartidos de red**.
 - e. (Opcional) Hacer clic en [Respaldar ahora] para iniciar el respaldo inmediatamente.
5. Para crear un programa para un evento de respaldo:
 - a. En el área Configuración de programa de evento de la página, seleccionar **Programa activado**.
 - b. Seleccionar **Programa incrementado** para respaldar solo aquellos eventos que ocurrieron desde el ultimo respaldo.
 - c. Seleccionar los días en que el programa será respaldado.
 - d. Seleccionar una hora para el respaldo.

- e. Seleccionar la ubicación a donde se enviará el archivo de respaldo en el campo de recursos **compartidos de red**.
 - f. (Opcional) Hacer clic en [Respaldar ahora] para iniciar el respaldo inmediatamente.
6. (Opcional) Para enviar un correo electrónico automático después del respaldo programado:
 - a. Seleccionar **Enviar si hay éxito**, **Enviar si fracasa** o ambas casillas de verificación.
 - b. Seleccionar una **lista de correo electrónico**.
7. Hacer clic en [Aceptar cambios].

Respaldar Eventos

Notar los siguientes detalles sobre los eventos:

- Los eventos no se pueden restablecer desde un archivo de respaldo. El archivo se destina sólo a fines de mantenimiento de registros.
- Los eventos pueden ser exportados utilizando el asistente de importación/exportación provisto en el disco Utilitarios, como se describe en la *Guía del usuario del asistente de importación/exportación*.

Para respaldar los eventos:

1. Iniciar sesión en el sistema como usuario con permisos de ejecución para la función de respaldo de base de datos.
2. Seleccionar **Administración del sistema > respaldo/restablecimiento**.
3. Hacer clic en [Respaldar programa].
4. En el área Configuración del programa de eventos de la página, hacer clic en [Respaldar ahora]. La caja de diálogo Ejecutar respaldo programado muestra los resultados de la operación.

Restablecer a partir de un respaldo

IMPORTANTE: El restablecimiento del respaldo sobrescribe la base de datos y se pierden todos los cambios realizados desde la fecha del respaldo.

1. Iniciar sesión en el sistema como usuario con permisos de ejecución para la característica Restablecer base de datos.
2. Seleccionar **Administración del sistema > respaldo/restablecimiento**.
3. Hacer clic en [Buscar].
4. Ir al archivo de respaldo.
5. Seleccionar el archivo y hacer clic en [Abrir].
6. Hacer clic en [Cargar archivo de respaldo].

Salvar y Restablecer los ajustes personalizados

Usar la página **Administración de sistema > Salvar/reajustar ajustes** para crear un punto de restablecimiento que incluye todos los datos normalmente salvados en un archivo de respaldo y los ajustes personalizados al controlador del sistema. Es como un estado personalizado por default.

En lugar de regresar el controlador del sistema a los ajustes de fábrica, que luego tendría que reconfigurarse a las necesidades específicas del sistema, se puede salvar la configuración básica de las instalaciones como una configuración personalizada y reiniciar con esa configuración de ser necesario. La información se guarda en el sistema y puede almacenarse después usando la frase de seguridad preestablecida.

Salvar Datos y ajustes personalizados

Esta tarea crea un archivo con todos los datos y ajustes de configuración del sistema presentes, almacenados en el controlador del sistema.

1. Seleccionar **Administración del sistema > Salvar/restablecer ajustes**.
2. Seleccionar **Salvar ajustes personalizados**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña**.
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Salvar ajustes personalizados**.

Restablecer ajustes personalizados

IMPORTANTE: Al usar esta característica, se borran todos los datos y ajustes configurados y se restablece la configuración almacenada en el archivo de ajustes personalizados. Antes de restablecer los ajustes personalizados, comprobar que hay una copia de respaldo actualizada.

IMPORTANTE: Tras el restablecimiento de los ajustes personalizados, el controlador del sistema se reiniciará. Durante este tiempo estará fuera de línea durante unos minutos. Por lo tanto, es mejor usar esta función durante los períodos de poca actividad de acceso, o los tarjeta habientes se verán obligados a esperar para poder entrar, si no se ha configurado un **modo Fallback de puerta** que permita el acceso cuando el controlador no está en línea.

1. Seleccionar **Administración del sistema > Salvar/reajustar ajustes**.
2. Seleccionar **Restablecer ajustes personalizados**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña**.
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Restablecer ajustes personalizados**.

Aparece el siguiente mensaje de advertencia: «Se está reiniciando el dispositivo» y se muestra una barra de progreso.

Cuando la barra de progreso llega a su fin, el servidor sale de línea y el navegador muestra la página por default cuando no puede conectarse a una dirección web.

7. Borrar la caché del navegador. (In Internet Explorer 8+, presionar <Ctrl>+<Shift>+<Borrar>.)

Reajustar ajustes de fábrica

IMPORTANTE: Esta característica borra todos los ajustes y datos (excepto los ajustes de configuración de red) y reajusta el controlador a los valores de fábrica. Antes de restablecer los ajustes de fábrica, comprobar que hay una copia de respaldo actualizada.

1. Seleccionar **Administración del sistema > Salvar/restablecer ajustes**.
2. Seleccionar **Restablecer ajustes de fábrica**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña**.
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Restablecer ajustes de fábrica**.
Aparece el siguiente mensaje de advertencia: «Se está reiniciando el dispositivo» y se muestra una barra de progreso.
Cuando la barra de progreso llega a su fin, el servidor sale de línea y el navegador muestra la página por default cuando no puede conectarse a una dirección web.
7. Borrar la caché del navegador. (In Internet Explorer 8 o más reciente, presionar <Ctrl>+<Shift>+<Borrar>.)
Cuando el servidor está nuevamente en línea, aparece el Formulario de aceptación de licencia de software de usuario final (EULA).
8. Hacer clic en **Aceptar**.

Actualización del Firmware

Las mejoras a las características se ofrecen ocasionalmente en el sitio web del producto en forma de actualizaciones de firmware que pueden descargarse y aplicarse al controlador del sistema y otros controladores de puerta sencilla basados en IP que puedan estar instalados.

Nota: La *actualización* del firmware del controlador es un proceso diferente a la *actualización* del sistema, lo cual afecta el código del núcleo del controlador del sistema, además de afectar el firmware. Para cambiar de una versión de TruPortal a una versión posterior (por ejemplo, de la versión 1.0 a la versión 1.5) o para actualizar de goEntry a TruPortal, ver [Uso del Asistente de actualización](#) en pág. 11.

Antes de comenzar

Antes de realizar una actualización de firmware, notar los siguientes detalles importantes:

IMPORTANTE: Conectar una batería de repuesto completamente cargada al controlador del sistema antes de actualizar el firmware. El controlador del sistema puede ser inutilizado y requerir reemplazo si se pierde la alimentación durante la actualización del firmware. Consultar la *referencia rápida del controlador del sistema* para información de la batería.

IMPORTANTE: No restablecer o reiniciar el controlador de puerta sencilla basado en IP durante la actualización del firmware o el controlador de puerta sencilla basado en IP no funcionará.

- Respalidar la base de datos antes de actualizar el firmware del controlador. Ver [Respaldo de Datos](#) en pág. 101.
- Los eventos almacenados en el controlador del sistema son purgados durante una actualización de firmware. Para mantener un registro de los eventos existentes, respaldar los eventos (ver [Respaldo de Eventos](#) en pág. 103) o exportar eventos (ver la *Guía del usuario del asistente de importación/exportación*).
- Una vez iniciado, el proceso de actualización no se puede cancelar.
- El firmware no se puede revertirse después de una actualización del firmware.
- Durante una actualización de firmware del controlador del sistema, habrá dos períodos breves cuando las credenciales no se pueden utilizar para acceder a las puertas. Después de que se completa la actualización y se reinicia el controlador del sistema, la operación normal se reanudará.

Verificar actualizaciones de firmware

1. Descargar los archivos de actualización de firmware desde el sitio web del producto.
 - Los archivos de actualización de firmware del controlador tienen una extensión LFF.
 - Los archivos de actualización de firmware para controladores de puerta sencilla basados en IP utilizan este nombre de archivo: IPSDCU.bin.
2. Iniciar sesión en el sistema como usuario con permisos de ejecución para la característica actualizar firmware.
3. Comparar las actualizaciones de firmware disponibles en el sitio web con el número de revisión del firmware del controlador del sistema y otros controladores de puerta sencilla basados en IP, como aparecen en la página de **administración del sistema > Configuración del sistema**.
4. Descargar las actualizaciones de firmware que son más recientes que el firmware del controlador del sistema y los controladores de puerta sencilla basados en IP.
5. Seleccionar **Administración del sistema > Actualizaciones firmware**.
6. Seleccionar **Actualizar firmware TruPortal** o **Actualizar firmware del controlador de puerta IP**.
7. En el campo **Archivo nuevo de firmware**, buscar y seleccionar el archivo de actualización de firmware.
8. Hacer clic en [Siguiente].
9. Hacer clic en [Actualizar].

Después de una actualización de firmware del controlador del sistema, el controlador del sistema se reiniciará. Volver a entrar y cambiar a la página **Monitoreo > Diagnósticos** (consultar [Diagnósticos](#) en pág. 110) para comprobar si hay problemas con las puertas, controladores y otro hardware recién instalado.

Administración de paquetes de idiomas

El sistema proporciona la siguiente flexibilidad en referencia a los idiomas:

- Un idioma del sistema determina el idioma utilizado para las funciones realizadas por el sistema, tales como la asignación de nombres por default del dispositivo, respaldos programados y correos electrónicos automatizados.
- Los usuarios individuales pueden seleccionar un lenguaje a nivel de usuario diferente al iniciar sesión en el sistema.

Se proporcionan cinco idiomas - Inglés, español, francés, holandés, y portugués con el sistema y los usuarios pueden cambiar el idioma de la interfaz de usuario al inicial sesión. ([Iniciar sesión en el sistema](#) en pág. 15.)

Se proporcionan idiomas adicionales en forma de *paquetes de idiomas* que están disponibles en el sitio web del producto. Estos paquetes de idiomas se pueden descargar y se agregan al sistema. También se pueden remover los paquetes de idiomas.

Notar los siguientes detalles sobre los paquetes de idiomas:

- Solo cinco idiomas pueden estar activos en cualquier momento.
- Antes de añadir un idioma nuevo a una instalación nueva, un lenguaje existente deberá ser removido.

Nota: No es posible remover inglés ni el paquete del idioma del sistema actual.

- Después de añadir un idioma nuevo, el idioma está disponible la próxima vez que el usuario firme su entrada.
- Si se remueve el idioma actualmente activo (por ejemplo, español), el usuario debe terminar la sesión del sistema y volver a iniciarla en el nuevo idioma.
- Los paquetes de idiomas se crean para las versiones específicas del firmware del controlador del sistema. Los dos primeros dígitos del número de versión del paquete de idioma (por ejemplo, 3.5x.xxxx) deben coincidir con los dos primeros dígitos de la versión de firmware actual, que se muestra en la página administración del sistema> paquetes de idiomas.
- Cuando el firmware del controlador del sistema se actualiza, el inglés y cualquier otro paquete de idiomas por default (español, francés, holandés, y portugués) que esté aún instalados también se actualizan. Para actualizar cualquier otro paquete de idioma, descargar e instalar el paquete de idioma correspondiente del sitio web del producto.
- Las actualizaciones de paquetes de servicio no afectan los paquetes de idioma.

Añadir un paquete de idioma

1. Lanzar un navegador de Internet soportado.
2. Descargar el paquete de idioma que desee en la página web del producto para una estación de trabajo cliente local o en un sistema de archivos compartidos.
3. Iniciar sesión en el sistema como usuario con permisos de Modificar.
4. Seleccionar **Administración del sistema > Paquetes de idiomas**.
5. Hacer clic en [Añadir].

Nota: El botón [Añadir] se activa solamente si se han instalado menos de cinco paquetes de idiomas. Si es necesario, remover un paquete de idioma (excepto inglés y el paquete de idioma actual a nivel del sistema) antes de agregar un nuevo paquete de idioma. Ver [Remover un Paquete de idioma en la página 108](#).

6. En el cuadro de diálogo Abrir que aparece, navegar a la carpeta en la que se ha descargado el paquete de idioma (el archivo tiene una extensión de NLS.), seleccionar el archivo y, hacer clic en [Abrir].
7. Cuando aparece la ventana Add-On del paquete de idioma, hacer clic en [Instalar].
8. Cuando la instalación se haya completado, hacer clic en [Finalizar].
9. Para comenzar a usar un idioma nuevo:
 - a. Salir del sistema con clic en el icono **terminar sesión** en la parte superior derecha de la interfaz de usuario.
 - b. Seguir los pasos [Iniciar sesión en el sistema](#) en pág. 15 y seleccionar el nuevo idioma en el campo **idioma**.

Remover un Paquete de idioma

Nota: No es posible remover el inglés ni el paquete del idioma actual a nivel del sistema.

1. Seleccionar **Administración del sistema > Paquetes de idiomas**.
2. Hacer clic en el paquete de idiomas para seleccionarlo.
3. Hacer clic en [Remover].

Aparece la caja de diálogo Remover objeto.
4. Hacer clic en [Remover].

CAPITULO 8

Solución de problemas

Los temas en este capítulo incluyen:

- [Resolver problemas del navegador](#) en pág. 103
- [Reiniciar el controlador del sistema](#) en pág. 104
- [Diagnósticos](#) en pág. 104
- [Mensajes de error, advertencia y eventos](#) en pág. 108
- [Errores reproductora de video](#) en pág. 112

Resolver problemas del navegador

Borrar la memoria caché y reiniciar el navegador puede resolver muchos problemas aparentes, tales como un repentino comportamiento extraño de la interfaz de usuario. Los pasos específicos varían según la marca y versión del navegador.

1. Terminar sesión del sistema y volver a iniciar sesión en la página de **Inicio**.
2. Despejar historial y caché del navegador.
3. Cerrar el navegador y volver a abrirlo.
4. Iniciar sesión en el sistema.

Nota: Tras activar o desactivar HTTPS/SSL, verificar que se limpió la caché del navegador, especialmente si se usa Firefox o Chrome.

Aquí hay algunos consejos para eliminar problemas del navegador:

- Si el controlador del sistema se reajusta o la base de datos es restablecida, Internet Explorer puede mostrar temporalmente una página XML en lugar de una página de inicio de sesión. Si ocurre, refrescar la página del navegador hasta que aparezca la página de inicio de sesión.
- El sistema soporta el uso de los botones del navegador Atrás y Adelante, sin embargo ocasionalmente puede aparecer una página en blanco mientras se navega hacia atrás o hacia adelante. Si esto ocurre, refrescar la página del navegador.
- Para navegadores diferentes a Internet Explorer, los botones Atrás y Adelante pueden no funcionar como se espera cuando se trata de navegar entre etiquetas de una página (por ejemplo, cuando se cambia de la etiqueta detalles a cuenta de usuario en la página **Administración de acceso > Personas**. Si esto ocurre, hacer clic de ratón en la etiqueta deseada.
- Maximizar la ventana del navegador para mostrar todas las herramientas de consejos. Las herramientas de consejos pueden no aparecer si la ventana del navegador es demasiado pequeña.
- Cuando la seguridad HTTPS está activada o desactivada en la página **Ajustes del sistema > Configuración de red**, la página de inicio de sesión deberá aparecer automáticamente. Si no aparece la página de inicio de sesión, despejar manualmente el navegador y reiniciar el navegador para acceder la página de inicio de sesión.
- Los ajustes del proxy del navegador pueden afectar la conectividad al controlador del sistema (que usa los puertos 80 y 443) cuando HTTPS está desactivado. Para resolver este problema, configurar proxys de servidores para permitir el tráfico HTTP sobre el puerto 443 ya sea en forma explícita (1) especificando el puerto 443 en the panel URL (por ejemplo, <http://192.168.1.10:443>), (2) añadiendo una excepción a los ajustes del proxy en el cliente, o (3) configurando un puerto de servicio que es desbloqueado por el cortafuegos. Ver [Configurar los Ajustes de red](#) en pág. 17.

Reiniciar el controlador del sistema

1. Seleccionar **Administración del sistema > Dispositivos**.
2. Seleccionar el controlador del sistema desde el árbol de dispositivos por jerarquía.
3. Hacer clic en [Reiniciar controlador].

Cuando el controlador del sistema se alimenta sólo por una batería y el voltaje cae a menos de 10.2 V, la tarjeta se apaga hasta que la fuente de poder AC/DC principal se restablece.

Diagnósticos

Errores detectados en el sistema se muestran en la página **Monitoreo > Diagnósticos**, junto con las estadísticas del sistema, tales como los números de entradas. Toda la información se puede consultar desde el momento de inicio de sesión y en cualquier momento a partir de entonces. Para refrescar manualmente los datos hacer clic en [Refrescar].

Para acceder a la página **Diagnósticos**:

- Seleccionar **Monitoreo > Diagnósticos**, o
- Hacer clic en el indicador de estado que aparece en la parte superior al centro de la interfaz de usuario cuando ocurren errores o hay advertencias.

Notar los siguientes detalles sobre la página de **Diagnósticos**:

- El color rojo indica un mal funcionamiento, tal como dispositivos fuera de línea. El color amarillo indica una advertencia, tal como una condición de sabotaje.
- Una elipse (...) aparece si hay información disponible sobre una categoría en una herramientas de consejos que puede mostrarse desplazándose sobre la elipse.
- El sistema no incluye acciones para ejecutar pruebas de diagnósticos específicas.
- Hacer clic en [Descargar archivo diagnósticos] para crear un archivo encriptado sencillo que incluye datos y bitácoras de configuración. No se incluye información personal específica en el archivo (como nombres o números de Seguro Social), referirse a las notas de la versión para detalles. Este archivo puede salvarse localmente y enviarse a soporte técnico para usar en la solución de problemas.
- Una lectura exacta para corriente DC no puede mostrarse cuando el controlador está alimentado por una fuente de DC. La información de la DC solo se mostrará cuando el controlador del sistema se alimenta con AC.

Diagnóstico	Valor mostrado	Estado
Alimentación de AC	OK Baja Falla	INF = OK WRN = Baja ERR = Falla
Alimentación DC	Tensión, Intensidad	INF >= 10.0 VWRN < 10.0 V WRN = sobrecarga de intensidad
Batería de respaldo	Tensión, intensidad, carga descarga	INF >= 11.7 VWRN < 11.7 V ERR < 11.4 V, Sin batería
Batería de la memoria	Tensión	INF >= 2.3 V WRN < 2.3 V ERR < 2.0 V
Fusibles	OK <i>Nombre del fusible,...</i>	INF = Todos OK ERR = Si alguno no está correcto
Controlador	OK <i>Problemas,...</i>	INF = OK WRN = Si no está correcto
Módulos	OK <i>ModuleName problema,...</i>	INF = Todos OK WRN = Si hay sabotaje ERR = Si fuera de línea
Puertas	OK <i>DoorName problema,...</i>	INF = Todos OK WRN = Si sujeta, forzada, sabotada ERR – Si fuera de línea

Diagnóstico	Valor mostrado	Estado
Entradas digitales	OK <i>InputName problema,...</i>	INF = Todos OK WRN = Si hay sabotaje ERR – Si fuera de línea
Tiempo en actividad	Hora del último arranque, días funcionando	INF = Siempre
Carga prom. CPU	1 m, 5 m, 15 m	INF 15m < 0.80 WRN 15 m = 0.80 ERR 15 m = 0.95
Uso de memoria	Usado, total	INF < 95% WRN >= 95% ERR = 100%
Almacenamiento principal	Porcentual	INF < 90% WRN >= 90% ERR = 100%
Almacenamiento imágenes y respaldo	Usado, total	INF < 50% WRN >= 50% ERR >= 95%
Tarjetas ADP	Usado, total	INF = Siempre
Puertas	Usado, total	INF = Siempre
Lectoras	Usado, total	INF = Siempre
Tarjetas E/S mejorada	Usado, total	INF = Siempre
Entradas	Usado, total	INF = Siempre
Salidas	Usado, total	INF = Siempre
DVRs	Usado, total	INF = Siempre
Cámaras	Usado, total	INF = Siempre
Persona	Usado, total	INF = Siempre
Credenciales	Usado, total	INF = Siempre
Niveles de acceso	Usado, total	INF – Siempre
Programas	Usado, total	INF – Siempre
Grupos de feriados	Usado, total	INF – Siempre
Feridos	Usado, total	INF = Siempre
Áreas	Usado, total	INF = Siempre

Diagnóstico	Valor mostrado	Estado
Grupos de lectoras	Usado, total	INF = Siempre
Funciones de operador	Usado, total	INF = Siempre
Plantillas video	Usado, total	INF = Siempre
Formatos de tarjeta	Usado, total	INF = Siempre

Fusibles

Los fusibles protegen la alimentación de CC suministrada por la tarjeta del controlador del sistema para su uso por los periféricos externos.

Fusible	+V	0V
Aux. 1	CN3.1	CN3.2
Aux. 2	CN3.3	CN3.4
Controlador de puerta	CN10.2 CN17.2	CN11.4 CN18.4
Entrada auxiliar	CN21.1	CN21.3 CN22.2

Estados problemas de hardware

Los items de hardware pueden tener los siguientes problemas:

Controlador

- Sabotaje

Módulos

- Fuera de línea
- Sabotaje

Puertas

- Fuera de línea
- Forzadas
- Sujetadas
- Sabotaje solicitud de salida
- Sabotaje contacto puerta
- Sabotaje auxiliar puerta
- Sabotaje puerta

Entrada digital

- Fuera de línea
- Sabotaje

Solución de problemas lectoras

Si una lectora no responde como se desea, usar, usar el botón [Escanear para cambios de hardware] (ver [Escanear para cambios de hardware](#) en pág. 23), verificar que la lectora aparezca en jerarquía del árbol de dispositivos en la página **Administración del sistema > Dispositivos** y verificar la configuración de la lectora. Ver [Configurar las lectoras](#) en pág. 34.

Si ocurren eventos inesperados para puertas o lectoras conectadas a un controlador de puerta sencilla basado en IP, verificar el puente del controlador de puerta sencilla basado en IP y cambiar los ajustes para asegurarse que el hardware esté configurado correctamente. Por ejemplo, el puerto de entrada de dispositivo (DI) de la lectora, J2, tiene dos entradas digitales que se usan para dispositivos de estado de puerta (contactos de puerta y entrada de solicitud de salida) y pueden ser configurados como entradas digitales supervisadas o no supervisadas. Si se configuran las entradas como entradas digitales supervisadas en la interfaz del usuario de TruPortal, requieren resistencias EOL. Consultar la *Referencia rápida del controlador de puerta sencilla basado en IP* para detalles.

Solución de problemas Programas

Si un programa no se comporta como se espera revisar las siguientes secciones:

- [Creación de grupos de feriados](#) en pág. 41
- [Creación de programas](#) en pág. 43
- [Consideraciones para Registros disparadores de acciones basados en programas](#) en pág. 63

Mensajes de error, advertencia y eventos

Estados de sabotaje

El controlador del sistema no distingue cuál de las cuatro entradas de puerta está en estado de sabotaje, al registrar los eventos de sabotaje. El estado de las entradas en tiempo real se puede ver en la página **Monitoreo > Diagnósticos**.

Eventos de alimentación y baterías

El controlador del sistema se apaga cuando el sistema está alimentado por batería

Si el controlador se alimenta exclusivamente de la batería y el voltaje de la batería cae a menos de 10.2 voltios, el controlador se apaga hasta que se restaura la alimentación de AC.

Eventos batería de respaldo

Los eventos de la batería de respaldo se producen cuando el voltaje de la batería de respaldo cae por debajo de determinados umbrales.

Código evento	Descripción evento	Causa
Evento 14612	Batería de respaldo crítica	El voltaje cae a menos de 11.4V o sube a más de 10.2V
Evento 14613	Corte de batería de respaldo	El voltaje cae a menos de 10.2V o sube a más de 9.0V
Evento 14624	Batería de respaldo baja	El voltaje cae a menos de 11.7V o sube a más de 11.4V
Evento 14625	Batería de respaldo restaurada	El voltaje sube a más de 11.7V
Evento 14649	No se detecta batería de respaldo	La tensión cae a menos de 9.0 V

Nota: Si el sistema se alimenta exclusivamente de una batería de respaldo, se apagará a 10.2V y no se generarán los eventos de corte y de no detección.

Evento batería de memoria

Código evento	Descripción evento
Evento 14618	Batería respaldo de memoria baja

Eventos fusibles

Código evento	Descripción evento
Evento 14651	Fusible cortado
Evento 14652	Fusible restaurado

Eventos dispositivos

Código evento	Descripción evento	Dispositivo
Evento 4105	Comunicaciones del dispositivo en falla	Controlador de puerta, expansor de E/S
Evento 4106	Comunicaciones dispositivo restauradas	Controlador de puerta, expansor de E/S
Evento 4107	Alarma de sabotaje*	Controlador, controlador puerta, expansor de E/S
Evento 14622	Problema de sistema	Controlador
Evento 14623	Sistema restaurado	Controlador
Evento 14628	Dispositivo falló	Controlador
Evento 14629	Dispositivo restaurado	Controlador
Evento 14643	Sabotaje restaurado*	Controlador, controlador puerta, expansor de E/S

* No se aplica a controladores de puerta integrados

Comunicaciones del dispositivo en falla/restauradas

Se usa para indicar los errores de comunicación con dispositivos instalados más adelante. Ocurre cuando las comunicaciones entre el bus RS-485 SNAPP y un dispositivo downstream configurado se pierden o se restablecen. El dispositivo siempre muestra cuál es el módulo afectado.

Dispositivo en falla/restaurado

Se usa para indicar problemas en general de los dispositivos instalados más adelante. Se produce cuando cualquier entrada de sabotaje del dispositivo cambia de estado (incluido el sabotaje externo/pared, pero no el sabotaje a la puerta), o cuando se detecta un error de comunicación por VBUS. El dispositivo siempre indica el controlador. Para cada evento de sabotaje, habrá un evento de sabotaje correspondiente para el dispositivo. Para los eventos de error de VBUS, no hay forma de informar cuál dispositivo tiene el error de VBUS, por lo que no hay ningún evento correspondiente que muestre cuál es el dispositivo afectado.

Problema de sistema/restaurado

Se usa para indicar problemas en general del sistema. Se produce cuando el **sabotaje externo/a la pared** cambia de estado. El **Dispositivo** siempre indica el controlador. Este evento puede usarse en el futuro para identificar otras condiciones de problemas.

Eventos sabotaje de puerta

Código evento	Descripción evento
Evento 14633	Sabotaje de puerta restaurado
Evento 14632	Alarma sabotaje de puerta

Alarma sabotaje de puerta/restaurada

Se usa para indicar la condición de sabotaje de cualquiera de las cuatro entradas de las puertas: DR, RTE, TR, AUX. El evento de alarma de sabotaje se genera al detectar una condición de

sabotaje en cualquiera de las entradas, o cuando TR está activo. No se generarán otros eventos de alarma de sabotaje para RTE, TR y AUX hasta que todas las condiciones de sabotaje que se resuelvan, pero se generarán otros eventos de alarma de sabotaje para DR, aunque las otras condiciones de sabotaje se mantengan. El evento de sabotaje restaurado solo se genera cuando se resuelve la condición de sabotaje de las cuatro entradas y TR está inactivo

Eventos de entrada auxiliar

Código evento	Descripción evento
Evento 14640	Entrada activa
Evento 14641	Alarma de sabotaje de entrada
Evento 14642	Entrada inactiva
Evento 4170	Entrada desactivada

Eventos de salida auxiliar

Código evento	Descripción evento
Evento 10240	Salida activada
Evento 11264	Salida desactivada

Advertencia "Objetos han cambiado"

De vez en cuando la caché del navegador local puede perder la sincronización con el sistema. En este caso, la interfaz se desactiva y aparece el mensaje de advertencia.

Hacer clic en el texto de la advertencia para recargar la página.

Evento "Falló sinc. NTP"

La capacidad de sincronizar el sistema con un servidor NTP, como se discute en [Ajustar Fecha y hora](#) en pág. 15, requiere que el sistema pueda acceder el NTP a través del puerto 123 UDP. Si este puerto no está abierto (por ejemplo, si está bloqueado por un cortafuegos), se registrará un evento "Falló sinc. NTP". Consultar con el administrador del sitio de la red para resolver este problema.

Errores reproductora de video

Si se presentan problemas para reproducir video, revisar [Antes de comenzar](#) en pág. 88 además de la siguiente información.

Ninguna conexión de video activa

Este mensaje aparece en la página Monitoreo > **Video** y el panel Detalle de eventos de la página **Eventos**.

El mensaje puede significar lo siguiente:

- No se ha configurado un dispositivo de cámara,
- El sistema perdió comunicación con una DVR/NVR o
- La reproductora de video no está instalada o está obsoleta Ver [Antes de comenzar](#) en pág. 88.

Nota: El video solo puede verse en Internet Explorer. Referirse a las *Notas de la versión* para detalles.

Si el mensaje de error aparece al hacer clic en el icono de una cámara al lado de un evento:

1. Hacer clic en [Reproducir video del evento].
2. El video se exhibe o el control ActiveX no está instalado. Ver [Antes de comenzar](#) en pág. 88.
3. Si no sucede nada y el mensaje permanece, verificar el funcionamiento de la DVR/NVR:
 - a. Ver [Configuración de dispositivos de video en la página 35](#).
 - b. Ver [Enlazar las cámaras a los dispositivos de rastreo de video de eventos en la página 38](#).

Si se muestra el mensaje de error cuando se selecciona **Monitoreo > Video**:

1. Hacer doble clic en el panel de video que muestra el mensaje de error.
2. Si el video no aparece:
 - a. Seleccionar **Monitoreo > Plantillas de video**.
 - b. Seleccionar la plantilla de video que se estaba viendo.
 - c. Comprobar que se selecciona la cámara correcta en cada lista desplegable de cada panel de la plantilla de video.
3. Si la cámara correcta no figura en la lista, verificar que la cámara se agregó a la página **Administración de sistemas >Dispositivos** y que está funcionando:
 - a. Ver [Configuración de dispositivos de video en la página 35](#).
 - b. Ver [Añadir una cámara de video en la página 36](#).
 - c. Ver [Añadir plantillas video en la página 38](#).

Los temas en este capitulo incluyen:

- [Capacidades del sistema](#) en pág. 114
- [Configurar Controladores de puerta sencilla basados en IP \(IPSDC\)](#) en pág. 115
- [Permisos de roles de operador predeterminados](#) en pág. 121
- [Uso de puerto](#) en pág. 124
- [Exactitud de duración de Pulso](#) en pág. 125

Capacidades del sistema

Atributo	Capacidad
Número de personas	10.000
Cantidad de credenciales individuales	10.000
Credenciales por persona	5
Niveles de acceso	64
Niveles de acceso por credencial	8
Programas	64
Intervalos de tiempo por programa	6
Grupos de feriados por programa	8
Grupos de feriados	8
Feriados por grupo de feriados	32
Feriados (total)	255
Áreas	64
Grupos de lectoras	64
Roles de operador	32
Campos definidos por el usuario	10
Plantillas de video	64
Formatos de tarjeta	8
Listas correo electrónico	10
Disparadores de acciones	32
Cantidad de eventos mantenidos en bitácora de eventos	65.000
Capacidades dispositivo	
Cantidad de puertas (controladores de puertas, de tarjeta básica o dual) con lectores de entrada/ cantidad de puertas con lectores de entrada y salida	64 / 32
Cantidad total de Módulos de interfaz dual para puertas (incluidos los incorporados)	32
Cantidad total de controladores de puerta sencilla basados en IP (IPSDCs)	62
Lectoras (total)	64
Entradas/salidas	
Cantidad total de entradas al sistema (incluido el controlador del sistema)	132

Atributo	Capacidad
Cantidad total de salidas del sistema (incluido el controlador del sistema)	66
Cantidad total de Add-ons de expansión entrada/salida o tarjetas add-on de expansión entrada/salida	8
DVRs/NVRs	4
Cámaras	64
Puertos Ethernet	2
Puertos de bus de SNAPP RS-485	4

Configurar Controladores de puerta sencilla basados en IP (IPSDC)

Antes de configurar los controladores de puerta sencilla basados en IP en la interfaz de usuario, cada controlador de puerta sencilla basado en IP debe ser configurado para reconocer la dirección IP del controlador del sistema. Establecer esta conexión de la red asegura que el IPSDC será detectado cuando el botón [Escanear para cambios de hardware] se usa en la página **Administración de sistema > Dispositivos**.

A continuación se ofrece una vista general de los pasos involucrados en la configuración de un controlador de puerta sencilla basado en IP:

1. Instalar el controlador de puerta sencilla basado en IP. Ver la *Referencia rápida del controlador TruPortal de puerta sencilla basada en IP* para detalles.
2. Seguir los pasos en [Preparar estaciones de trabajo cliente para usar la herramienta de configuración integrada \(ICT\)](#) en pág. 122. Antes de configurar un controlador de puerta sencilla basado en IP, la dirección IP de una estación de trabajo del cliente local debe prepararse para estar en la misma sub-red del controlador de puerta sencilla basado en IP.
3. Consultar [Antes de comenzar](#) en pág. 124 para obtener más información acerca de las opciones de la herramienta ICT.
4. Seguir los pasos en [Usar el ICT para configurar los controladores de puerta sencilla basados en IP](#) en pág. 125.
5. Iniciar sesión en el acceso e interfaz de usuario TruPortal y acceder la página **Administración de sistema > Dispositivos**.
6. Usar el botón [Escanear para cambios de hardware] para que el controlador del sistema pueda descubrir el controlador de puerta sencilla basado en IP y añadirlo al Árbol de dispositivos. Ver [Escanear para cambios de hardware](#) en pág. 23.
7. Configurar el controlador de puerta sencilla basado en IP en la TruPortal interfaz de usuario. Ver [Configurar un controlador de puerta](#) en pág. 26.

En seguida algunos detalles adicionales sobre los controladores de puerta sencilla basados en IP:

- Ocasionalmente las mejoras de características para los controladores de puerta sencilla basados en IP están disponibles en el sitio web del producto en forma de actualizaciones de firmware. Ver [Actualización del Firmware](#) en pág. 105.
- Los controladores de puerta sencilla basados en IP pueden configurarse para usar un modo fallback si la conectividad con el controlador del sistema se pierde. Un caché local que almacena hasta 50 credenciales exitosas puede conceder acceso. Ver [Configuración de seguridad](#) en pág. 18.
- Los controladores de puerta sencilla basados en IP no soportan acciones Buzzer encendido y Buzzer apagado configuradas para disparadores de acciones, sabotaje puntos de entrada, o tipos de entradas auxiliares. Consultar la *Referencia rápida de controlador de una sola puerta basado en IP TruPortal* para saber cómo modificar la configuración de los puentes para tipos de entrada.
- Para reemplazar un controlador de puerta sencilla basado en IP, referirse a [Reemplazar un controlador de puerta](#) en pág. 27.

Preparar estaciones de trabajo cliente para usar la herramienta de configuración integrada (ICT)

La *Herramienta de configuración integrada (ICT)* es un programa basado en navegador construido en cada controlador de puerta sencilla basado en IP que puede usarse para configurar un controlador de puerta sencilla basado en IP para que reconozca el controlador del sistema.

La dirección IP por default de un controlador de puerta sencilla basado en IP es 192.168.6.6. Antes de usar la herramienta ICT para configurar un controlador de puerta sencilla basado en IP, la estación de trabajo del cliente local debe prepararse para estar en la misma sub-red del controlador de puerta sencilla basado en IP. Estos pasos varían dependiendo de cuál sistema operativo se usa como se describe a continuación.

Para preparar una estación de trabajo de cliente Windows XP:

1. Hacer clic en **Iniciar**, **Panel de Control**, después en **Conexiones de red**.
2. Hacer clic derecho en **Conexión de Área Local**. Si la primera opción en la caja de la lista de caída abajo es:
 - **Desactivar**, entonces la conexión está activada. Ir a [paso 3](#).
 - **Activar**, entonces seleccionarlo para activar la conexión. Regresar a [paso 1](#).
3. Seleccionar **Propiedades** en la lista de caída abajo.
4. En la sección **Esta conexión usa los siguientes objetos:**, seleccionar **Protocolo Internet TCP/IP**.
5. Seleccionar **Propiedades**.
6. Si esta computadora está ajustada para:
 - **DHCP**, entonces **Obtener una dirección IP automáticamente** ya está seleccionada. Seleccionar **Usar la siguiente dirección IP**.
 - **Estática**, entonces escribir la dirección IP y el número de sub-red. Reajustar la computadora a esos valores después de completar la configuración del controlador.
7. Ingresar la dirección IP 192.168.6.1, o una dirección IP válida similar (p. ej., 192.168.6.x en donde x es cualquier número entre 1 y 254 excepto 6).
8. Cambiar la sub-red a 255.255.255.0.
La puerta por default no necesita cambiarse.
9. Hacer clic en **OK** hasta que todas las ventanas abiertas se cierren.
10. Si está activado un cortafuegos, desactivar el cortafuegos antes de iniciar la herramienta ICT.

11. Proceder con [Usar el ICT para configurar los controladores de puerta sencilla basados en IP](#) en pág. 125.

Para preparar una estación de trabajo de cliente Windows 7:

1. Hacer clic en el botón **Iniciar**, seleccionar el **Panel de control Red e Internet** y después **Red y Centro compartido**.
2. En la sección de la forma **Ver redes activas**, hacer clic en el enlace **Conexión de área local**.
3. En el diálogo **Conexión área local** hacer clic en **Propiedades**.
4. En la caja del diálogo Conexión de área local, seleccionar ya sea **Protocolo Internet versión 4 (TCP/IPv4)** o **Protocolo Internet versión 6 (TCP/IPv6)**.
5. Hacer clic en **Propiedades**.
 - Si se ha seleccionado **Obtener automáticamente una Dirección/IPvx Usar IPvx Dirección**, en donde x es la versión del protocolo Internet que se está usando (4 ó 6).
 - Si la conexión es estática, escribir la dirección IP y número de máscara de sub-red. Reajustar la computadora a esos valores después de completar la configuración del controlador.
6. Ingresar la dirección IP 192 . 168 . 6 . 1, o una dirección IP válida similar (p. ej., 192 . 168 . 6 . x en donde x es cualquier número entre 1 y 254 excepto 6).
7. Cambiar el valor de Longitud de prefijo de sub-red a 255 . 255 . 255 . 0.
La puerta por default no necesita cambiarse.
8. Hacer clic en **OK** y **Cerrar** hasta que todas las ventanas abiertas se cierren.
9. Si está activado un cortafuegos, desactivar el cortafuegos antes de iniciar la herramienta ICT.
10. Proceder con [Usar el ICT para configurar los controladores de puerta sencilla basados en IP](#) en pág. 125.

Para preparar una estación de trabajo de cliente Windows 8:

1. Hacer clic en el icono **Red** para abrir la Red y Centro de compartido.
2. Hacer clic **Cambiar los ajustes de adaptador**.
3. En la ventana conexiones de red, hacer clic derecho en el icono **Conexión de área local** y seleccionar **Propiedades** en el menú.
4. En la caja del diálogo Conexión de área local, seleccionar ya sea **Protocolo Internet versión 4 (TCP/IPv4)** o **Protocolo Internet versión 6 (TCP/IPv6)**.
5. Hacer clic en **Propiedades**.
 - Si se ha seleccionado **Obtener automáticamente una Dirección/IPvx Usar IPvx Dirección**, en donde x es la versión del protocolo Internet que se está usando (4 ó 6).
 - Si la conexión es estática, escribir la dirección IP y número de máscara de sub-red. Reajustar la computadora a esos valores después de completar la configuración del controlador.
6. Ingresar la dirección IP 192 . 168 . 6 . 1, o una dirección IP válida similar (p. ej., 192.168.6.x en donde x es cualquier número entre 1 y 254 excepto 6).
7. Cambiar el valor de **Longitud de prefijo de sub-red** a 255 . 255 . 255 . 0.
La puerta por default no necesita cambiarse.
8. Hacer clic en **OK** y **Cerrar** hasta que todas las ventanas abiertas se cierren.
9. Si está activado un cortafuegos, desactivar el cortafuegos antes de iniciar la herramienta ICT.
10. Proceder con [Usar el ICT para configurar los controladores de puerta sencilla basados en IP](#) en pág. 125.

Uso de la Herramienta de configuración integrada

Esta sección describe cómo usar la herramienta ICT para configurar un controlador de puerta sencilla basado en IP para que reconozca la dirección IP del controlador del sistema de manera que el controlador de puerta sencilla basado en IP pueda ser detectado cuando se use el botón [Escanear para cambios de hardware] en la página **Administración del sistema > Dispositivos**.

Antes de comenzar

Antes de usar la herramienta ICT, notar los siguientes detalles:

- La estación de trabajo del cliente que será usada para acceder la herramienta ICT debe configurarse en forma apropiada. Referirse a [Preparar estaciones de trabajo cliente para usar la herramienta de configuración integrada \(ICT\)](#) en pág. 122.
- Si un cortafuegos está activado en la estación de trabajo del cliente local, desactivar el cortafuegos antes de iniciar la herramienta ICT.
- Si una instalación requiere que un controlador de puerta sencilla basado en IP y su anfitrión correspondiente se comuniquen a través de un cortafuegos, usar la herramienta ICT para configurar el cortafuegos del controlador de puerta sencilla basado en IP para que permita conexiones a través del puerto 3001.
- Desactivar o pasar por alto cualquier proxy de red durante el uso de las ICT.
- Después de completar la configuración, la ICT se puede desactivar para evitar el acceso no autorizado. Ver [Activar y Desactivar la herramienta ICT](#) en pág. 127.
- Si se cambian las opciones en un formulario de ICT, hacer clic en **Salvar** en la parte inferior de la forma de salvar los cambios antes de cambiar a otro. Esta acción salva los últimos cambios realizados en un archivo de configuración temporal.
- Después de completar todos los formularios, hacer clic en **Aplicar cambios** y entonces hacer clic en **Reiniciar la aplicación** para que los cambios se efectúen. Los cambios se salvarán a la base de datos de la configuración en el controlador de puerta sencilla basado en IP.

La tabla siguiente describe los botones disponibles en la interfaz ICT:

Botón	Uso	Resultado
Salvar	Después de cambiar valores en cualquier forma	Salva los cambios a un archivo de configuración temporal.
Aplicar cambios	Después de completar todos los cambios	Salvar los cambios del archivo de configuración temporal a la base de datos de configuración.
Reiniciar la aplicación	Después de seleccionar Aplicar cambios	La herramienta ICT recoge los últimos cambios de la base de datos de configuración y vuelve a iniciar.
Reiniciar el controlador	Después de seleccionar Aplicar cambios	El controlador de puerta sencilla basado en IP aplica los últimos cambios y vuelve a iniciar.

Botón	Uso	Resultado
Defaults de fábrica ^a	Para restablecer los ajustes por default del controlador de puerta sencilla basado en IP	Los ajustes del controlador de puerta sencilla basado en IP se han restablecido a los defaults de fábrica. Los ajustes de dirección IP se retienen.
Cambiar Usuario/contraseña	Para ajustar la ID de usuario y/o contraseña para iniciar sesión en la herramienta ICT.	Cambia la ID de usuario y/o contraseña por la herramienta ICT. Los valores por default son <i>instalar</i> , <i>instalar</i> . Para mayor seguridad, cambiar los valores por default.

- a. Si los parámetros de red por default son restablecidos usando el botón SW7, entonces todos los parámetros (incluyendo la dirección IP del controlador de puerta sencilla basado en IP) serán modificados.

Usar el ICT para configurar los controladores de puerta sencilla basados en IP

Seguir estos pasos para configurar un IPSDC para que reconozca la dirección IP del controlador. Estos pasos también pueden ser utilizados para reconfigurar un IPSDC si cambia la dirección IP del controlador.

- Utilizar uno de los siguientes navegadores de Internet para abrir una ventana del navegador en la estación de trabajo cliente:
 - Microsoft Internet Explorer 7.0 o más reciente
 - Netscape 7.0 o más reciente
 - Mozilla Firefox 12.0 o más reciente
- En el campo **Dirección** del navegador, introducir la dirección IP del IPSDC.
La dirección IP por default de fábrica de un IPSDC es 192.168.6.6. De no estar seguro de cuál es la dirección IP de un IPSDC, presionar y mantener presionado el botón Restaurar valores por default (SW7) en el IPSDC durante al menos 5 segundos para restaurar la configuración a los valores por default de fábrica.
- Cuando inicia la ICT, escribir la **ID de usuario** y la **Contraseña** para la ICT.
Los valores por default son *instalar* e *instalar*.
- Hacer clic en [Iniciar sesión].
La página de información del controlador muestra el formulario de parámetros.
- (Recomendado) Cambiar la contraseña por default para mejorar la seguridad:
 - Hace clic en [Cambiar usuario/Contraseña] para abrir el formulario de cambio de usuario / contraseña.
 - Escribir la **ID de usuario**.
 - Escribir la **Nueva contraseña**.
 - Volver a escribir la contraseña en el campo **Confirmar contraseña**.
 - Hacer clic en [Cambiar credenciales].
- Hacer clic en el menú parámetros de controlador para abrir la forma Red principal.
- Para usar una conexión dinámica para el controlador de puerta sencilla basado en IP, seleccionar **Usar DHCP**. (Usar esta opción si un servidor DHCP está en la red y si el controlador de puerta sencilla basado en IP puede alcanzarse a través del puerto de la consola.)

Para usar una conexión estática (p.ej., una dirección IP ajustada):

- a. Escribir el **Controlador IP**.
 - b. Escribir el **Portal IP**.
 - c. Escribir la **Máscara sub-red**.
8. Escribir el nombre del controlador de puerta sencilla basado en IP en el campo **Nombre del controlador**.
 9. (Recomendado) Registrar esta información en la tabla de instalación. Ver [Documentación de la ubicación física de cada dispositivo](#) en pág. 5.
 10. Hacer clic en **Salvar**.
 11. Cambiar a la ficha Configuración del panel y escribir la dirección IP del controlador en el campo **Dirección IP del panel**.
 12. Hacer clic en **Salvar**.
 13. Si esto completa la configuración del controlador de puerta sencilla basado en IP usando la ICT, hacer clic en **Aplicar cambios**, entonces **Reiniciar la aplicación**.
 14. Si la estación de trabajo cliente local utilizada para acceder a la TIC originalmente tenía una dirección IP estática, reiniciar la estación de trabajo para utilizar la dirección original. Ver [Preparar estaciones de trabajo cliente para usar la herramienta de configuración integrada \(ICT\)](#) en pág. 122.
 15. Después de que un controlador de puerta sencilla basado en IP está configurado para reconocer la dirección IP del controlador del sistema, se puede añadir al sistema de dos maneras:
 - Usar el botón [Escanear para cambios de Hardware] para descubrir dispositivos. Ver [Escanear para cambios de hardware](#) en pág. 23, o
 - Agregar el controlador de puerta sencilla basado en IP manualmente seleccionando el controlador del sistema en la página **Administración del sistema > Dispositivos**, hacer clic en [Añadir] y seleccionar *Controlador IP 1 puerta 2 lectoras*. Hacer clic en [Aceptar cambios] al terminar.
 16. Para completar la configuración de un controlador de puerta sencilla basado en IP en la interfaz de usuario:
 - Configurar las opciones del sistema completo del controlador de puerta sencilla basado en IP en la etiqueta Seguridad de la página **Administración del sistema > Ajustes del sistema**. Ver [Configuración de seguridad](#) en pág. 18 y
 - Configurar opciones específicas del controlador en la página **Administración del sistema > Dispositivos**. Ver [Configurar un controlador de puerta](#) en pág. 26.

Activar y Desactivar la herramienta ICT

Controlar acceso a la ICT seleccionando una de las siguientes opciones:

- **Temporal:** Permite acceso a la herramienta ICT hasta que se reajuste el controlador de puerta sencilla basado en IP
- **Permanente:** Permite acceso hasta que la ICT se desactiva nuevamente en forma manual.

IMPORTANTE: Antes de comenzar, se **debe** tener acceso físico al controlador.

Para activar la ICT temporalmente:

1. Presionar y sostener SW4 hasta que D19 (p.ej., el LED Watchdog) se encienda ON. Permitir hasta cinco (5) segundos para que se encienda el D19. (Ver la *Referencia rápida del controlador de puerta sencilla basada en IP* para localizar los interruptores.)
2. Después de que D19 esté encendido, liberar SW4.

3. D19 se apaga cuando se activa manualmente la herramienta ICT.
La herramienta ICT ahora está activada hasta que se reinicie el controlador.

Para activar la herramienta ICT permanentemente:

1. Completar los pasos para activar la herramienta ICT temporalmente, como se describe arriba.
2. Registrarse a la herramienta ICT.
3. Desde el menú **Parámetros de controlador**, seleccionar **Otros parámetros**.
4. Deseleccionar **Desactivar Herramienta de Configuración Integrada** y hacer clic en **OK**.
5. Para que esta selección sea permanente, hacer clic en **Salvar, Aplicar cambios**, después **Reiniciar el controlador**.

El controlador de puerta sencilla basado en IP ejecuta un reinicio del sistema automático y la herramienta ICT se activa de forma permanente.

Para desactivar la ICT:

1. Registrarse a la herramienta ICT.
2. Desde el menú **Parámetros de controlador**, seleccionar **Otros parámetros**.
3. Seleccionar **Desactivar Herramienta de Configuración Integrada** y hacer clic en **OK**.
4. Para que esta selección sea permanente, hacer clic en **Salvar, Aplicar cambios**, después **Reiniciar el controlador**. El controlador ejecuta un reinicio del sistema automático y la herramienta ICT se desactiva en forma permanente.

Permisos de roles de operador predeterminados

Como se comenta en [Configuración de roles de operador](#) en pág. 48, un rol de operador es una política de grupo de permisos que puede usarse para expandir o limitar las páginas de interfaz de usuarios que pueden ver los usuarios, así como las acciones que los usuarios pueden ejecutar en el sistema.

Los varios niveles de permisos incluyen:

- **Ninguno:** El operador no puede visitar ni ver esta página.
- **Visión:** El operador puede ver la página o los datos, pero no puede hacer cambios ni ejecutar comandos.
- **Modificación:** El operador puede cambiar los ajustes.
- **Ejecutar:** El operador puede cambiar los comandos.

La siguiente tabla proporciona los niveles de permiso por default para el sistema.-

Característica	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Niveles de acceso	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Disparadores de acciones: Administración	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación

Característica	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Disparadores de acciones: Monitorear	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Ver	Ejecutar
Reajustar el Anti-passback	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Ver	Ejecutar
Áreas	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación
Respaldar base de datos	Ninguno, ejecutar	Ejecutar	Ejecutar	Ninguna	Ninguna	Ejecutar
Control PTZ de cámaras	Ninguno, ejecutar	Ejecutar	Ejecutar	Ejecutar	Ninguna	Ninguna
Formatos de tarjeta	Ninguno, visualización, modificación	Modificación	Ver	Ninguna	Ninguna	Modificación
Credenciales	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ninguna	Modificación
Fecha y hora	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Dispositivos	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación
Diagnósticos	Ninguno, visualización	Ver	Ver	Ver	Ver	Ver
Puertas (incluyendo controlador de puerta sencilla basado en IP)	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Ver	Ejecutar
Configuración correo electrónico	Ninguno, visualización, modificación	Modificación	Ver	Ninguna	Ver	Modificación
Eventos	Ninguno, visualización	Ver	Ver	Ver	Ver	Ver
Actualización de firmware	Ninguno, ejecutar	Ejecutar	Ninguna	Ninguna	Ninguna	Ejecutar
Feridos	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación

Característica	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Entrada/Salida	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Ver	Ejecutar
Paquetes de idiomas	Ninguno, visualización, modificación	Modificación	Ninguna	Ninguna	Ninguna	Modificación
Configuración de la red	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación
Compartidos de red	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación
Funciones de operador	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Ver
Personas	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Campos de usuario protegidos	Ninguno, visualización, modificación	Modificación	Ninguna	Ninguna	Ninguna	Ninguna
Grupos de lectoras	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Reportes	Ninguno, ejecutar	Ejecutar	Ejecutar	Ejecutar	Ejecutar	Ejecutar
Restablecer base de datos	Ninguno, ejecutar	Ejecutar	Ninguna	Ninguna	Ninguna	Ejecutar
Salvar/restablecer ajustes	Ninguno, ejecutar	Ejecutar	Ninguna	Ninguna	Ninguna	Ejecutar
RespalDOS programados	Ninguno, visualización, modificación	Modificación	Ver	Ninguna	Ninguna	Modificación
Programas	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Seguridad	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación
Opciones del sistema	Ninguno, visualización, modificación	Modificación	Ver	Ver	Ver	Modificación

Característica	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Cuentas usuarios	Ninguno, visualización, modificación	Modificación	Ver	Ninguna	Ninguna	Modificación
Campos definidos por usuario	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación
Video	Ninguno, visualización	Ver	Ver	Ver	Ver	Ninguna
Plantillas video	Ninguno, visualización, modificación	Modificación	Modificación	Ver	Ver	Modificación

Uso de puerto

Los dispositivos de hardware usan puertos para permitir que las aplicaciones de hardware compartan características sin interferir con las demás.

La tabla a continuación proporciona información de puerto para varios dispositivos en el sistema:

Dispositivo	Puerto	Uso
Controlador del sistema	TCP/22	Conexión Secure Shell (SSH)
Controlador del sistema	TCP/80	TruPortal Interfaz de usuario y utilitarios
Controlador del sistema	TCP/443	TruPortal Interfaz de usuario y utilitarios
Controlador del sistema	TCP/3001	Actualizaciones de firmware de bajo nivel
Controlador del sistema	UDP/5353	Escanear para descubrimiento de cambios de hardware
TruVision TVN 20	TCP/8000	Puerto por default de flujo de video
TruVision TVN 21	TCP/8000	Puerto por default de flujo de video
TruVision TVN 50	TCP/8000	Puerto por default de flujo de video
TruVision TVR 10	TCP/8000	Puerto por default de flujo de video
TruVision TVR 11	TCP/8000	Puerto por default de flujo de video
TruVision TVR 30	TCP/80	Puerto por default de flujo de video
TruVision TVR 31	TCP/80	Puerto por default de flujo de video
TruVision TVR 41	TCP/8000	Puerto por default de flujo de video
TruVision TVR 60	TCP/8000	Puerto por default de flujo de video

Exactitud de duración de Pulso

Cuando se configuran disparadores de acciones que encienden o apagan un pulso, notar que la exactitud de variación del pulso depende de la longitud de pulso, como se detalla en la siguiente tabla:

Duración	Rango de exactitud
1 segundo	1
2 segundos	2
3 segundos	3
5 segundos	5
10 segundos	10
15 segundos	15
20 segundos	00:19 – 00:20
30 segundos	0:29 – 0:30
45 segundos	0:45 – 0:46
60 segundos	0:59 – 1:00
90 segundos	1:23 – 1:32
2 minutos	1:53 – 2:02
3 minutos	2:53 – 3:02
5 minutos	4:43 – 5:12
10 minutos	9:43 – 10:12
15 minutos	14:43 – 15:12
20 minutos	19:43 – 20:12
30 minutos	29:43 – 30:12
45 minutos	44:43 – 45:12
60 minutos	0:59:43 – 1:00:12
90 minutos	1:20:43 – 1:40:42
2 horas	1:40:43 – 2:00:42
4 horas	3:40:32 – 4:00:42
6 horas	6:00:43 – 6:20:42
8 horas	8:00:43 – 8:20:42
10 horas	10:00:43 – 10:20:42
12 horas	12:00:43 – 12:20:42
16 horas	16:00:43 – 16:20:42

20 horas	20:00:43 – 20:20:42
1 día	0d:23:40:43 – 1d:00:00:42
7 días	7d:00:20:43 – 7d:16:20:42

Glosario

ANSI

Siglas de American National Standards Institute, una organización voluntaria que establece normas para la industria informática.

Anti-passback

Anti-passback se puede usar para establecer una secuencia específica en la cual las credenciales deben usarse para obtener acceso a un área.

Apertura de puerta

Dispositivo eléctrico o magnético que se usa para mantener la puerta en la posición cerrada. La apertura de una cerradura eléctrica requiere algún tipo de carga eléctrica generada por otro dispositivo, tal como una lectora de tarjetas.

Área APB

Las áreas son definidas por las lectoras que entran y salen de ellas. Se registra el Área actual en la que se encuentra una tarjeta. Cuando una tarjeta trata de entrar en una área determinada a través de una lectora determinada, se niega el acceso si no está registrada como presente en el área de la lectora en la que está configurada su salida.

Asistente

Programa utilitario que se usa como guía para trabajar paso a paso a través de un proceso.

Credencial

Una ID de credencial con un número codificado que puede añadirse al sistema y usarse para conceder o negar el acceso.

DHCP

Siglas de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de anfitrión). Protocolo de comunicaciones que permite a los administradores de red administrar de forma centralizada y automatizar la asignación de direcciones de Protocolo de Internet en la red de una organización.

Cámara IP

Videocámara digital que se conecta directamente a la red con su propia dirección IP y tiene capacidad para transmitir imágenes usando protocolos de comunicación normalizados, tales como TCP/IP. Una cámara IP no necesita estar conectada a una PC ni a una tarjeta de captura de video.

Código de instalación

Campo opcional en la tarjeta que identifica inequívocamente un lugar. Los proveedores de tarjetas Wiegand suelen proporcionar el código de instalación y lo almacenan en las tarjetas. En otras tarjetas, el usuario define el código de instalación. Una lectora de tarjetas puede ponerse en modo de Sólo código de instalación, lo que requiere el código de instalación antes de que se autorice el acceso.

Compartidos de red

Un recurso compartido de red, tal como un sitio FTP o una carpeta de red.

Contacto de puerta

Dispositivo de dos piezas usado por un sistema de acceso por tarjeta para indicar si una puerta está abierta o cerrada. Por lo general, una pieza está montada en la puerta y la otra en una posición similar en el marco de la puerta.

Controlador de puerta sencilla basado en IP

Acrónimo para controlador de una sola puerta basado en IP.

Dirección IP

Identificador de una computadora en una red TCP/IP. El formato de una dirección IP es una dirección numérica de 32 bits, escrita como cuatro números separados por puntos. Cada número puede estar entre cero y 255. Por ejemplo, 1.120.4.72 podría ser una dirección IP.

Enrutador

"Concentrador" inteligente que permite que varias sub-redes se conectan entre sí para compartir datos y recursos

Ethernet

Norma de redes de comunicación LAN que usan cable coaxial o par trenzado. IEEE 802.3 es la norma para Ethernet. Existen los siguientes tipos de Ethernet: 10 Mbps (Mega [millones] bits por segundo), 100 Mbps, 1 Gbps (Giga [mil millones] bits por segundo)

Evento

Un registro histórico de actividad rastreado por el sistema, tal como individuos a quienes se les concedió o negó el acceso, violaciones de Anti-passback, y alarmas que ocurrieron.

Hora UTC

Siglas de horario universal coordinado, una escala de tiempo que une la hora del meridiano de Greenwich (GMT) que se basa en la tasa inconsistente de rotación de la Tierra, con la hora atómica exacta. Cuando la hora atómica y la hora de la Tierra se aproximan a un segundo de diferencia, se añade un segundo de salto a la hora UTC.

HTTP

Siglas de Hyper Text Transfer Protocol (Protocolo de transferencia de hipertexto). Define la forma en que se formatean y transmiten los mensajes y controla las acciones que los servidores y navegadores web deben ejecutar en respuesta a distintos comandos.

IP

Siglas de Internet Protocol (Protocolo de Internet), que especifica el formato de los paquetes y el esquema de direccionamiento en una red.

LAN

Siglas de Local Area Network (red de área local). Una LAN enlaza las estaciones de trabajo cliente dentro de un área limitada, por medio de cables de alto rendimiento para que los usuarios puedan intercambiar información, compartir periféricos y usar los recursos de una unidad de almacenamiento secundario llamado servidor de archivos.

LDAP

Siglas del Protocolo Ligero de Acceso a Directorios. LDAP, es un protocolo de software usado comúnmente para hablar con los servidores que almacenan la información de usuario, incluidos los certificados digitales. Permite la localización de organizaciones, personas y otros recursos, tales como archivos y dispositivos en una red, ya sea por Internet o en una Intranet corporativa. La conexión a un servidor LDAP puede ser no encriptada o encriptada con SSL.

National Television Standards Committee

Comúnmente conocida como NTSC, es la señal de televisión usada en los Estados Unidos y Japón.

Nivel de acceso

Una o más combinaciones de lectora/programa, que se usa para controlar el acceso de los tarjeta habientes al hardware. Los niveles de acceso pueden asignarse a tarjetas de identificación activas para definir a qué lectoras y en qué horario la tarjeta tiene acceso.

No supervisado

Puerta o gabinete que no está cableado con un circuito de continuidad para detectar intentos de sabotaje.

PAL

Norma de video usada en Europa, Australia y Nueva Zelanda. El sistema PAL transmite 625 líneas por 1/25 segundos.

PIN

Siglas de Personal Identification Number (número de identificación personal), un número generalmente asociado con una persona y usado en el control de acceso

PTZ

Siglas de Pan-Tilt-Zoom (movimiento horizontal, vertical y zoom). Una característica de las cámaras cuyo movimiento horizontal, vertical y zoom se puede controlar por computadora. PTZ permite aumentar el área de visualización de una cámara porque es posible girarla en diferentes direcciones.

Puerto TCP/IP

Cada proceso que quiere comunicarse con otro proceso se identifica al conjunto de protocolos TCP/IP a través de uno o más puertos. Un puerto es un número de 16 bits, usado por el protocolo anfitrión a anfitrión para identificar a qué protocolo de nivel superior o programa de aplicación (proceso) debe entregar los mensajes entrantes.

SMTP

Siglas de Simple Network Management Protocol (Protocolo simple de administración de redes). Un estándar para la transmisión de correo electrónico a través de redes IP.

SNMP

Siglas del Protocolo de transferencia de correo electrónico sencillo. Método de gestión de varios elementos de hardware, por ejemplo, una impresora, conectada a la red.

Solicitud de salida

Los dispositivos de solicitud de salida (RTE) se usan para permitir el paso a través de puertas bloqueadas desde el lado protegido de puntos de entrada controlados. Un contacto de solicitud de salida (RTE) generalmente es un botón localizado cerca de la puerta asociada. Cuando un tarjeta

habiente presiona el botón, se envía una RTE al controlador.

SSL

Siglas de Secure Sockets Layer (Capa de sockets seguros), un protocolo común para la autenticación y comunicación cifrada a través de Internet. SSL se usa en la comunicación con servidores web (HTTP) y LDAP.

Subred

Grupo de computadoras que comparten las mismas propiedades y recursos de red

Sujetador de puerta

Dispositivo que sujeta la puerta en la posición abierta hasta que el sistema lo instruye a cambiar de estado.

Supervisada

Puerta o gabinete cableado con un circuito de continuidad, de modo de detectar intentos de sabotaje.

TCP/IP

Siglas de Transmission Control Protocol/ Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). Conjunto de protocolos de comunicación usados para conectar servidores a través de Internet.

Tipo de tarjeta

Clasifica las tecnologías de codificación de las tarjetas, tales como Magnética, Wiegand, Tarjeta inteligente, First Access, etc.

URL

Siglas de Uniform Resource Locator (Localizador uniforme de recursos). URL es la dirección de un recurso o un archivo disponible en una red TCP/IP, tal como Internet.

Wiegand

Tecnología de control de acceso mediante tarjetas que contienen cables de tungsteno cargados magnéticamente, cortados en tiras y montados verticalmente en columnas.

Índice

A

Accediendo a ayuda en línea	2
Acceso de discapacitados	27
Activa desde	73
Activa hasta	73
Activado/desactivado	34
Activar conexión HTTPS	10, 18
Activar credenciales	74
ActiveX	35
Actualizaciones de firmware	99
Administrador	
cambiar la contraseña para	9
cuenta usuario	9
Advertencias	
Objetos han cambiado	111
Se está reiniciando el dispositivo ..	98, 99
Ajustes personalizados, salvar y restablecer ..	98
Alarma de sabotaje activada	34
Alarma sabotaje de puerta	110
Alimentación DC	107
Añadir	
áreas	37
cámaras de video	35
compartido de red	67
Controladores de puerta sencilla	
basados en IP	115, 120
credenciales	70
cuentas usuario	70
dispositivos	23
Formatos de tarjeta	21
fotos	71
grabadoras de video digital	35
grupos de feriados	39
grupos de lectoras	43
Listas correo electrónico	49
niveles de acceso	44
paquetes de idiomas	102
plantillas de video	36
programas	41
roles de operador	45
Ancho de banda del flujo de video	35
Anti-passback	31, 36, 37, 93, 127
configuración	38
Apertura automática	32
Apertura de puerta	127
archivos CSV	52
Área APB	127
Área por default	37
Asistente de actualización	2, 11
Asistente de importación/exportación	2, 52
Asistente de instalación	2, 3, 9
Asistentes	2, 127
Asistente de actualización	11
Asistente de instalación	9

Asistente de página de Inicio	15
-------------------------------------	----

B

Bloquear al cerrar	31
Bloqueo magnético	19, 29
Botón escanear para cambios de hardware ..	23

C

Caja de diálogo Respaldo de la base	
de datos	96
Caja de selección Desbloquear todas las	
puertas	24, 34
Caja de selección protegida	50
Cámara enlazada	24, 28, 29, 33, 34, 36
Cámaras PTZ	35
Cambiando contraseña	75
Cambiar contraseñas	75
Campo exclusivo	50
Campos definidos por el usuario	
añadir	50
configuración	50
protegidos	50
remoción	51
reorganizar	51
Cargar fotos	71
Casilla Usar tiempo ampliado de apertura/	
mantener abierto	73
Certificados de seguridad	17
Código de emisión	21
Código de instalación	21, 22, 128
Compartidos de red	129
Conexión Secure Shell (SSH)	8, 18
Configuración de formatos de tarjeta	21
configuración de servidor de correo	
electrónico externo SMTP	48
configuración de servidor de correo	
electrónico interno SMTP	47
Configuración y control del	
navegador web	35
Configurar	
Anti-passback	38
áreas	36, 37
cámaras de video	34, 35
campos definidos por el usuario	50
compartido de red	67
Controlador del sistema	9
Controladores de puerta sencilla	
basados en IP	115
controladores de puertas	25
correo electrónico	47
credenciales	70
cuentas usuario	70
disparadores de acciones	52
dispositivos	36
DVRs/NVRs	34, 35
fecha y hora	111
Formatos de tarjeta	21

grupos de lectoras	43	administración	70
Idioma del sistema	21	crear reportes	76
lectoras	33	de duración limitada	74
niveles de acceso	44	definición	127
opciones de puerta	30	desactivación	74
personas	70	Importando	52
plantillas de video	36	instalación de una lectora	
programas	41	de enrolamiento	72
puertas	26, 27	perdida o robada	74
registros de disparadores de acciones ..	66	CSV	52
roles de operador	45	Cuentas de usuario	
servidor de correo electrónico		administración	70
externo SMTP	48	fecha	52
servidor de correo electrónico		permisos de grupo	50
interno SMTP	47		
Sincronización temporal con el		D	
servidor NTP	15, 111	De uso general	
video de evento	36	entradas	25
Contacto de puerta	28, 29, 128	salidas	25
Contraseña Secure Shell (SSH)	19	Desactivar credenciales	74
Controlador del sistema		Desbloqueo programado	32
conexión	6	Descargar un archivo de diagnósticos	105
descripción	4	DHCP	8, 127
Controladores de puerta sencilla		Dirección IP	6, 16
basados en IP	4, 7	configuración de controladores de puerta	
actualizaciones de firmware	99	sencilla basados en IP	119
configuración	115	configurado una dirección	
encriptación	19	IP dinámica	10, 17
Herramienta de		configurado una dirección	
configuración integrada	119	IP estática	10, 17
modo fallback	19	determinando la nueva dirección IP	9
reemplazar	26	estática vs. dinámica	8
Controladores de puertas		incluyendo números de puertos	8
configuración	25	Disparadores	53
reemplazar	26	Disparadores de acciones	52
Copiar		configuración	66
compartido de red	68	controlado manualmente	92
grupos de lectoras	44	disparando manualmente	67
programas	43	ejecutar manualmente	92
registros de disparadores de acciones ..	67	Entendiendo las acciones	61
roles de operador	46	entendiendo los disparadores	53
correo electrónico, desactivar	49	exactitud de duración de pulso	125
Credencial ID	52	instrucciones de condición	53
Credencial y PIN	33, 91	Dispositivos de video	35
Credenciales	52		

Drive CD/DVD	9
Duración de la reproducción	
previa al evento	35
Duración de pulso	125
DVRs y NVRs, ajustando la hora y la fecha	15

E

Encriptar comunicaciones de controlador de	
puerta sencilla basado en IP	19
Entrada auxiliar	32
Entrada terminaciones fin de línea	19, 20
Entradas	
auxiliares	91
monitoreo	91
Entradas/Salidas de uso general	24
Ethernet	128
Etiqueta Campos definidos por usuario	50
Etiqueta Configuración de red	16, 17
Etiqueta Cuenta de usuario	75
Etiqueta entradas	34
Etiqueta General	24
Etiqueta listas de distribución	48, 49
Etiqueta Respaldo programa	96, 97
Etiqueta Seguridad	18, 120
Etiqueta servidor de correo electrónico	47
Etiqueta Ver horarios	51
Evento 10240	111
Evento 11264	111
Evento 14618	109
Evento 14640	111
Evento 14641	111
Evento 14642	111
Evento 14644	89
Evento 14646	89
Evento 14651	109
Evento 14652	109
Evento 4170	111
Eventos	
credenciales perdidas o robadas	74
definición	128
exportación	81
Falló sinc NTP	15, 111
respaldos	97
video	36, 82
visualización	80
Eventos batería de respaldo	109
Eventos de entrada auxiliar	
14640	111
14641	111
14642	111
4170	111
Eventos de salida auxiliar	
10240	111
11264	111
Eventos dispositivos	110
Eventos sabotaje de puerta	
Evento 14632	110

Evento 14633	110
Exento de Anti-passback	73
Exportar eventos	81

F

Falló sinc NTP	15, 111
Fecha, ajuste	9, 15
Feridos	
impacto en disparadores de acciones ..	59
personalizados	40
que se repitan todos los años	40
únicos	40
First Access	130
Fotos	71, 72
remoción	72
Fusibles	107

H

Hardware	
asignación de nombres	23
Descubrimiento	7
Escanear para cambios de hardware ...	23
instalación	3
Herramienta de configuración integrada	
activar y desactivar	120
configuración de controladores de puerta	
sencilla basados en IP	119
descripción	118
preparando las estaciones de trabajo ..	118
Herramienta de consejos	2
Hoja de propiedades Propiedades de red ...	17
Hora UTC	128
Hora, ajuste	9, 15
HTTP	128
HTTPS	8, 130

I

ID credencial	52
ID de persona	50
Idioma del sistema	20
Idiomas	
administración de paquetes de idiomas	101
ajustar el idioma del sistema	20
cambiar idiomas durante inicio	
de sesión	15, 102
IEEE 802.3	128
Importar	
certificados de seguridad	17
personas y credenciales	52
Instrucciones de condición	53
Internet Explorer	98, 99, 112
ajustes recomendados	82
versiones anteriores a 8.0	76

L

LAN	3, 6, 128, 129
LDAP	129, 130

Lectora para entrar y lectora para salir	31
Lectora solo para entrar	31
Lectoras de enrolamiento	6, 72
Longitud máxima del PIN	18, 20

M

Máscara de sub-red	10
Máximo intentos de PIN	18
Mensajes	
Alarma de sabotaje	110
Alarma de sabotaje de entrada	111
Batería de respaldo baja	109
Batería de respaldo crítica	109
Batería de respaldo restaurada	109
Comunicaciones del dispositivo	
en falla	110
Comunicaciones dispositivo	
restauradas	110
Corte de batería de respaldo	109
Dispositivo falló	110
Dispositivo restaurado	110
Entrada activa	111
Entrada desactivada	111
Entrada inactiva	111
Falló sinc NTP	15, 111
Fusible cortado	109
Fusible restaurado	109
Memoria batería de respaldo baja	109
Ninguna conexión de video activa	112
No se detecta batería de respaldo	109
Objetos han cambiado	111
Problema del sistema	110
Sabotaje restaurado	110
Salida activada	111
Salida desactivada	111
Se está reiniciando el dispositivo ..	98, 99
Sistema restaurado	110
Modo de cerradura de puerta	27, 32
Modo de Programa	52
Bloqueada	52
Credencial y PIN	52
Desbloqueada	52
lectora	90
Primera entrada con tarjeta	52

puerta	90
Sólo credencial	52
Modo fallback del controlador de	
puerta sencilla basado en IP	19
Monitorear	
disparadores de acciones	92
entradas	91
puertas	51
salidas	91
Video de eventos	82

N

Nivel de acceso	52
Niveles de permiso	121
No supervisado	33, 129
Nombre del dispositivo	24
Normalmente abierto	33
Normalmente cerrado	33
Número de empleado	50
Número de ID	50
Número de identificación exclusivo	50
Número de identificación personal (PIN) ..	18
Número de registro en base de datos	50
Número de serie	24

O

Opciones de lectoras	33
credencial y PIN	33
solo credencial	33

P

Página Asignación de lectoras	37
Página compartido de red	67
Página correo electrónico	47
Página Definición de áreas	37
Página Diagnósticos	104
Página Disparadores de acciones	92
Página Dispositivos	26, 28, 29, 51, 104
Página Entradas/salidas	91
Página eventos	80, 82, 112
Página Feriados	39
Página Formatos de tarjeta	21, 91
Página Grupos de lectoras	43
Página Niveles de acceso	42, 43, 44, 51

Página paquetes de idiomas	101	grupos de lectoras	44
Página Personas	50, 70, 75	Listas correo electrónico	49
Panel Credenciales	38	niveles de acceso	45
Página Plantillas de video	36	paquetes de idiomas	102
Página programas	41, 43, 90	personas	71
Página Puertas	42	programas	43
Etiqueta Ver horarios	51	roles de operador	47
Página Roles de operador	45, 50	Reporte Acceso a lectoras	76
Página Salvar/restablecer ajustes	98, 99	Reporte de nómina	36, 76
Página Video	82, 83, 85, 112	Reporte Historial de acceso	76
Panel Credenciales	38	Reporte lista de asistencia	76
Período de acceso normal		Reportes	
concedido	27, 28, 29, 31	Acceso a lectoras	76
Personas	52	crear	77
credenciales	70	Credencial	76
cuentas usuario	70	Historial de acceso	76
fotos	71, 72	Lista de asistencia	76
Importando	52	Nómina	76
remoción	71	Respaldo/restablecer página	95
Personas con discapacidad	73	Respaldo	68
PINs	52, 129	ajustes personalizados	98
Problemas del navegador	103	crear una copia de respaldo	96
Programas, impacto en disparadores		programar respaldos automáticos	96
de acciones	59	respaldo de eventos	97
PTZ	129	Respaldo, restablecimiento de datos	97
Puerta		Restablecer ajustes personalizados	98
no supervisada	129	RJ-45	6
supervisada	130		
Puerta de enlace predeterminada	10	S	
Puerta mantenida abierta	30	Sabotaje	28, 30
Puerta mantenida/forzada	27, 29, 32	Sabotaje de puerta restaurado	110
Puertas		Salidas	
Etiqueta Ver eventos	90	auxiliares	91
Etiqueta Ver horarios	90	monitoreo	91
menús de comandos	89	Salvar modo fallback de puerta	19
monitoreo	51	Código de Instalación	20
Puerto de servicio	8, 10, 17	Restringido	20
Puerto TCP/IP	129	Todos	20
Puerto UDP	15	Secure Sockets Layer (SSL)	16
Punto de restablecimiento	68, 98	Seguridad	20
R		Sensor de conexión del bloqueo mag ...	29, 31
Reajustar el Anti-passback	93	Servidor de nombres de dominio (DNS)	10
Red		Servidor NTP	16
enrutador	6	servidor SMTP	47
Red de área local	3, 6	SMTP	129
Reiniciar el controlador del sistema	104	SNMP	129
Relé auxiliar	27, 31	Solicitud de firma de certificado (CSR)	16
Remove		Solicitud de salida (RTE) 27, 28, 29, 30, 129	
áreas	37	Solicitud de salida (RTE)	
campos definidos por el usuario	51	extendida	27, 28, 30, 32
compartido de red	68	Sólo credencial	33, 91
credenciales	73	Solución de problemas	
disparadores de acciones	67	crear un archivo de diagnósticos	105
Formatos de tarjeta	22	Diagnósticos	104
fotos	72	Errores reproductora de video	112
grupos de feriados	41	lectoras	108

mensajes de error,	
advertencia y eventos	108
problemas del navegador	103
programas	108
Reiniciar el controlador del sistema ..	104
Solución de problemas, lectoras	108
SSL	129
start.hta	9
Subred	130
Sujetador de puerta	130
Supervisada	33, 130

T

Tarjeta inteligente	130
Tensión	109
Tiempo activación relé auxiliar	28, 33
Tiempo de bloqueo de PIN	18
Tiempo extendido mantenido/abierto	30
tiempo extendido mantenido/abierto	30
Tipo de tarjeta	130
Tipos de entrada	
no supervisada	33
normalmente abierto	33
normalmente cerrado	33
supervisada	33

U

UDP	111
URL	130

V

Valores Separados por Comas	52
Ver botón de ayuda	2
Video	
controles del reproductor	85
descargar clips de video	84
reproducción	83
Solución de problemas	112
visualización de eventos	82
Video en directo	83
Video grabado	83

W

Wiegand	130
---------------	-----

Z

zona	37
------------	----