

Módulo de Control de Brivo Access para XProtect

Guía de instalación, configuración y uso

Brivo y Milestone han desarrollado esta integración para permitir que nuestros clientes se beneficien mutuamente de una comunicación más estrecha entre nuestros sistemas. A continuación, proporcionamos una guía, paso a paso, para los distribuidores en la que se detallan los requisitos previos para habilitar esta integración.



Prerrequisitos

Software y Licencias	2
Requisitos del sistema Milestone XProtect.....	2
Brivo Access.....	3
Orbnet Systems.....	3
Instalación de Brivo para XProtect Access.....	4



Configuración

Control de Brivo Access	6
Configuración de un nuevo administrador	6
Configuración del rol de administrador personalizado	10
Configuración de la aplicación API.....	12
Clave API	13
Respondedor de llamadas para el acceso desde el exterior (Event Callback).....	14
Esquema de la red	14
Protección con Windows Security software	15
Configuración del cortafuegos (Firewall) de la red	17
Gestión de la lista de comprobación de Milestone	20
Configuración del control de acceso	21
Información de control de acceso/Otras configuraciones	25
Vinculación de cámaras y puertas	26
Eventos de control de acceso.....	26
Notificaciones de solicitud de acceso.....	27
Titulares autorizados de tarjetas de acceso (Cardholders)	27
Configuración de las alarmas.....	28
Configuración de las reglas y los eventos.....	30
Configuración de eventos definidos por el usuario	32
Configuración de acceso de los usuarios a Smart Client	33
Configuración de funciones y de Smart Client.....	34
Configuración de monitor de acceso	34
Configuración de mapas de Smart Client	36
Configuración de la pestaña de control de acceso.....	39
Configuración de eventos definidos por el usuario	41
Solución de problemas	42

Prerrequisitos

Software y licencias

- Microsoft® Windows® 10 Pro (64 bits)
- Microsoft® Windows® 10 Enterprise (64 bits)
- Microsoft® Windows® 10 Enterprise LTSB 2016 (versión 1607 o posterior)
- Microsoft® Windows® 10 IoT Enterprise, versión 1803 o posterior (64 bits), IoT Core
- Microsoft® Windows® Server 2016 (64 bits): Essentials, Standard y Datacenter
- Microsoft® Windows® Server 2019 (64 bits): Essentials, Standard y Datacenter

Requisitos del sistema Milestone XProtect

- Debe ser un distribuidor autorizado de Milestone
- XProtect Express+, Professional+, Expert, Corporate 2020 R1 (20.1a) o superior
- Servidor de eventos Milestone - El servidor de eventos se incluye como parte de la instalación de Milestone

Nota: Si este componente no se ha instalado con su versión, siga los pasos que se encuentran en el apartado: Solución de Problemas, al final de este documento.

- Las licencias de acceso “Milestone Access” aplican como licencia base para su XProtect – Sin embargo, XProtect Access no se ejecuta como una licencia de prueba predeterminada. Si desea agregar una licencia de prueba por defecto. Si desea añadir una licencia de prueba a su licencia de XProtect, debe consultar al soporte de ventas de Milestone a través de purchase@milestonesys.com o enviar una solicitud de compra directamente al sitio web de Milestone. De lo contrario, realice la compra a un socio de Milestone, tal y como se indica a continuación.

Licencias

SKU ID	Nombre	MSRP (USD)
XPABL	Licencia básica de XProtect Access (BL)	142.00
XPADL	Licencia de puertas de XProtect Access (DL)	43.00

Previo a la instalación de un sistema de prueba de ORBNET, revise el Manual de Gestión del Cliente de Milestone (Milestone Management Client) y asegúrese de que tiene las licencias de XProtect Access asociadas con la versión de Milestone instalada. Si no aparecen mencionadas allí, no podrá utilizar el ORBNET Systems Plugin ya que XProtect Access no está habilitado como parte de la versión de prueba instalada de ORBNET, para ello, debe solicitar una licencia de prueba o comprarla previamente a Milestone.

◆ milestone | XProtect®

Licencia concedida a:

N/D

United Kingdom

[Modificar detalles...](#)

[Acuerdo de licencia de usuario final](#)

Milestone Care

Su nivel actual: Basic

[Acceso al portal Milestone Care...](#)

[Infomación sobre Milestone Care...](#)

Productos instalados

Versión de producto	Código de licencia de software	Fecha de caducidad	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2021 R2 Test	M01-C01-212-02-6C4BAA	12/14/2022	N/D	N/D
Milestone XProtect Smart Wall	M01-P03-100-02-6C1FDF	Ilimitado	Ilimitado	
Milestone XProtect Access	M01-P01-100-02-6C2B92	12/21/2022	12/21/2022	

Brivo Access

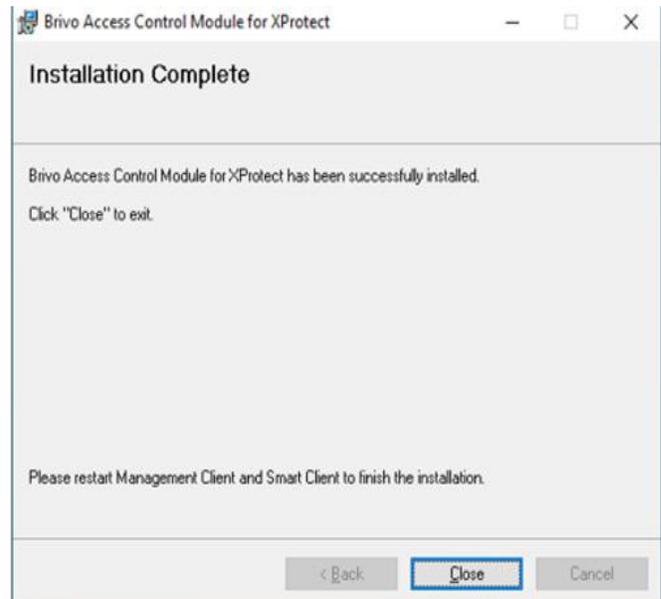
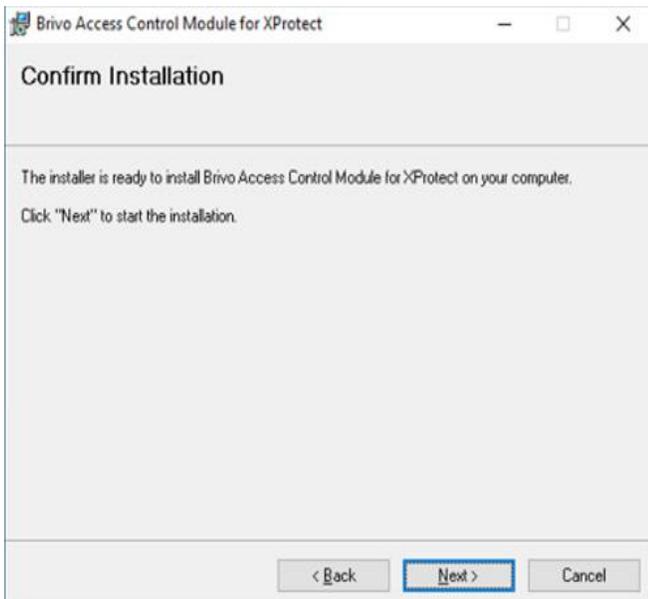
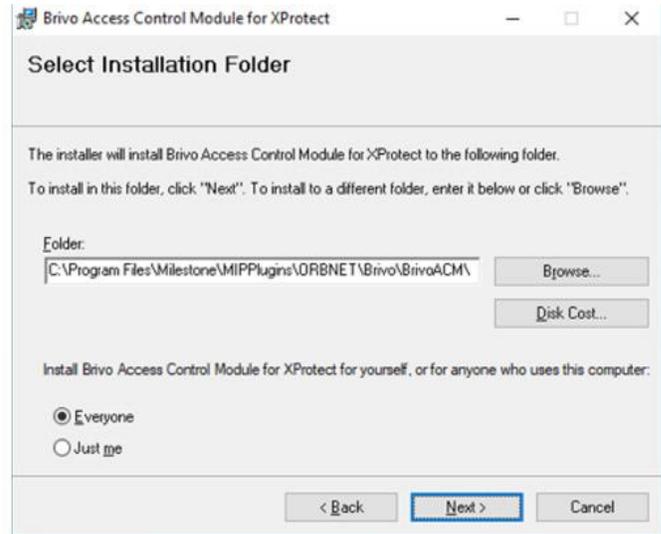
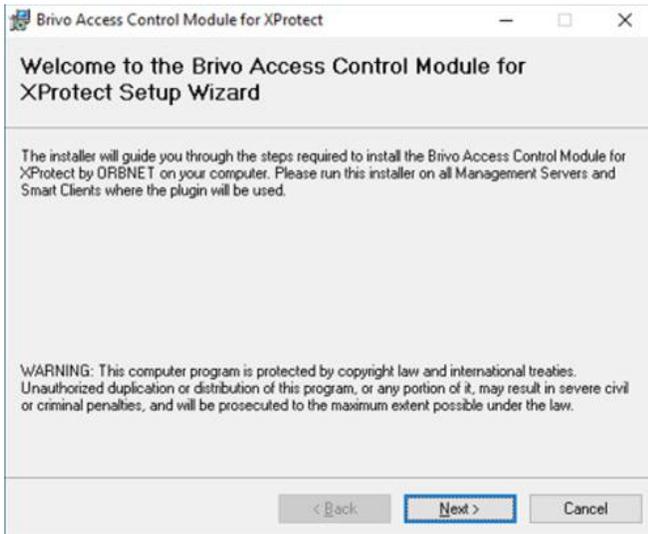
- Acceso de la cuenta de administrador supervisor a Brivo Access
- Administrador creado para Brivo Access para coordinar la integración y el acceso a puertas
- Clave API que debe solicitarse a Brivo
- Aplicación API: "Client ID" (Identidad del cliente) y "Client Secret" (Cliente secreto) generada por Brivo Onair
- Suscripción a Brivo Access para la integración de Milestone XProtect Access

Orbnet Systems

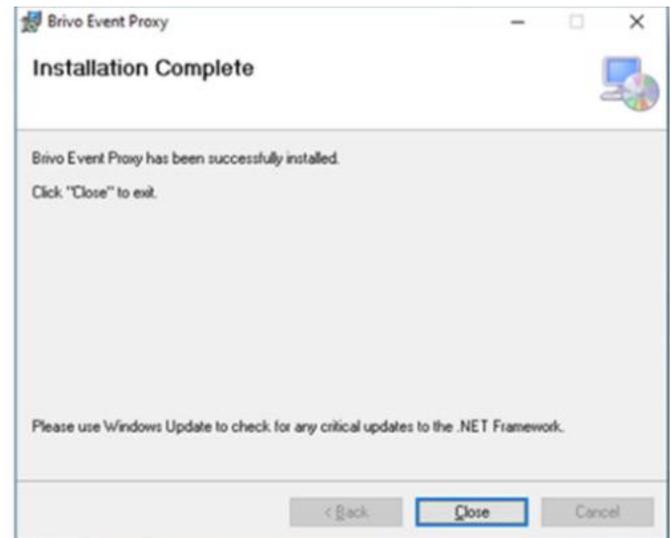
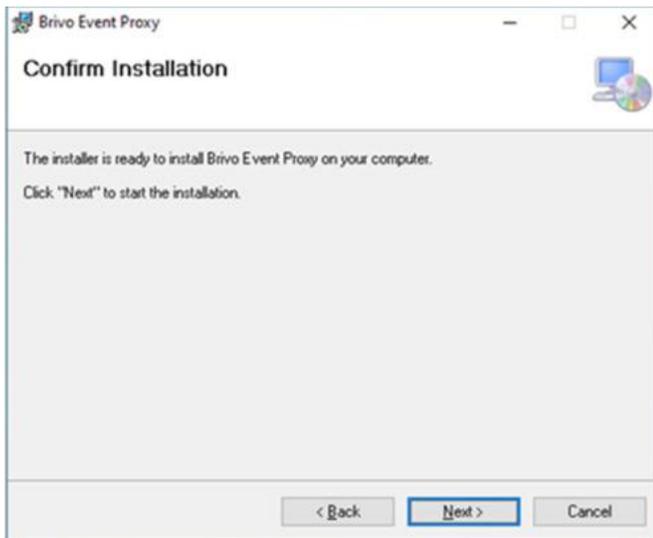
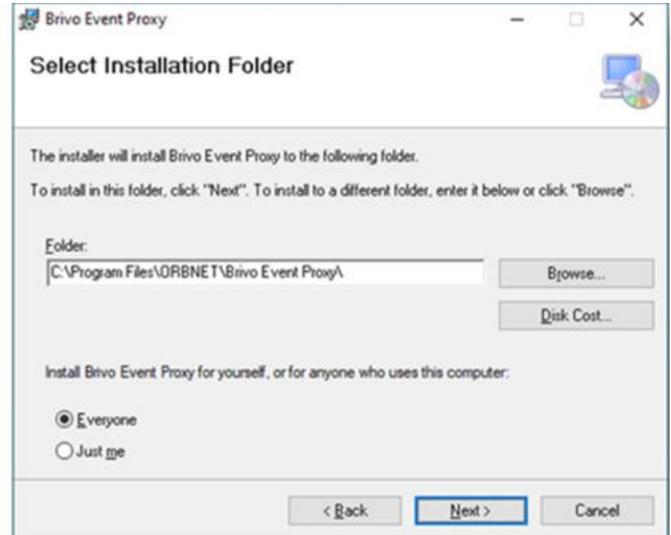
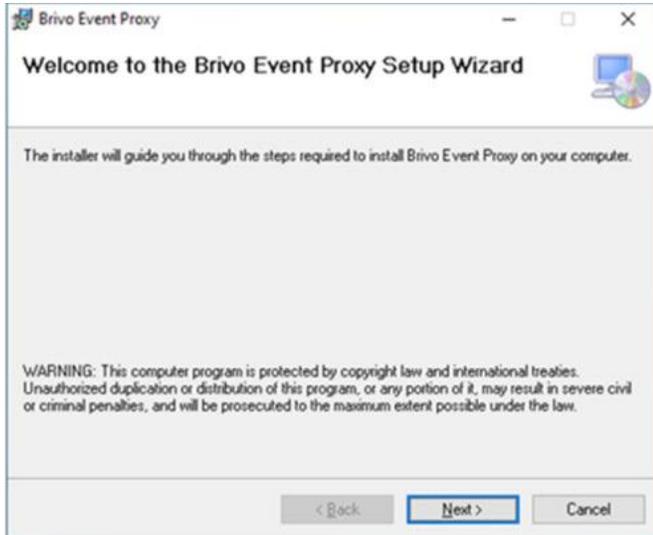
- Instalador - "Brivo Access for XProtect Setup.msi"
Brivo le proporcionará los enlaces de descarga con su clave API
- Instalador - "Brivo Event Proxy Setup.msi"
Brivo le proporcionará los enlaces de descarga con su clave API

Instalación de Brivo para XProtect Access

Inicie con el servidor o la máquina que ejecuta XProtect Management and Event Server (el servidor de gestión y eventos de XProtect). Primero cierre todos los Milestone Smart que estén abiertos y luego coloque el “Brivo Access for XProtect Setup. msi” en una carpeta del escritorio y haga doble clic para iniciar la instalación.



Una vez finalizada, ejecute el instalador "Brivo Event ProxySetup.msi" para completar la conexión del proxy de eventos. La instalación se realizará de manera predeterminada con "NT AUTHORITY\Network Service". Si el sistema de Milestone no tiene acceso a Internet, instálelo en un servidor accesible con acceso a Internet.



Configuración

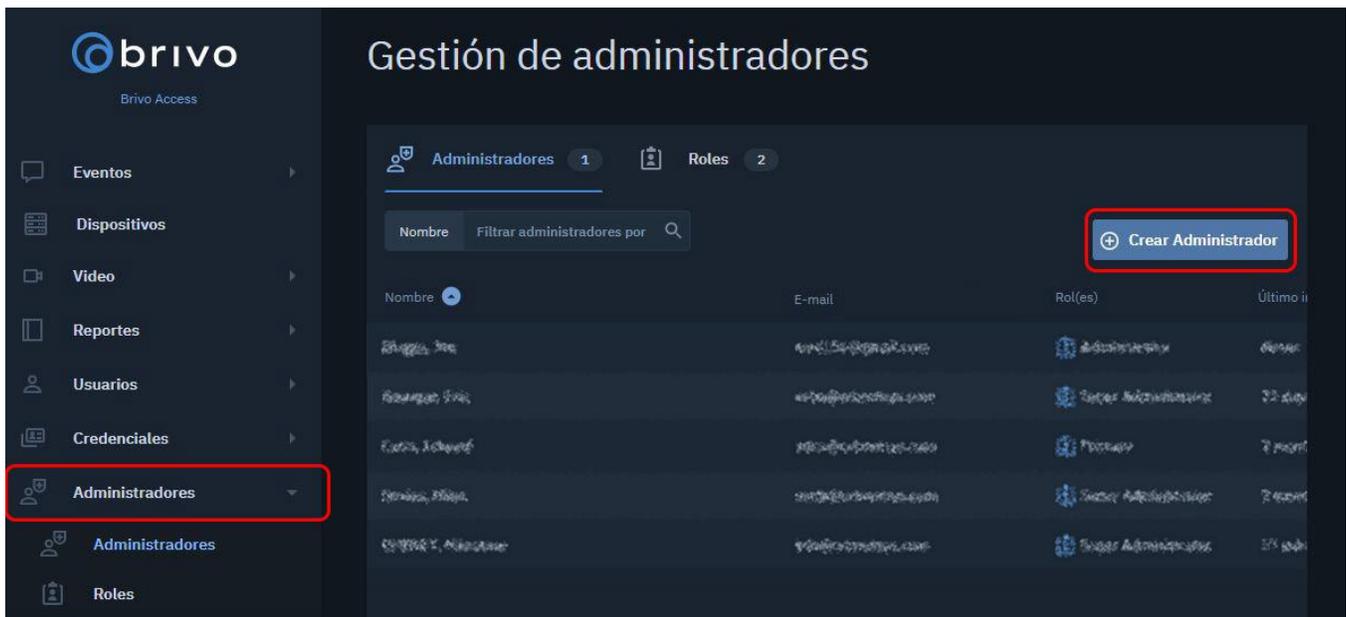
Control de Brivo Access

Configuración de un nuevo administrador

Se recomienda crear una nueva cuenta de usuario en Brivo para la conexión con el módulo Milestone Access. Esto permitirá una mejor gestión de las puertas a incluir y controlar.

En este ejemplo, se creó un usuario llamado "Milestone ORBNET" con acceso a todas las puertas que se pretenden incluir en Milestone al cual se le asignó el rol de **administrador**. Este es el nivel más bajo de administrador de cuentas que se recomienda para esta integración.

Para crear una nueva cuenta de administrador, seleccione **Administradores** en el menú principal. En la página que enumera los detalles de usuarios de los administradores actuales, busque y seleccione el botón **Crear Administrador**.



En **Gestión de administradores**, agregue los detalles relevantes para esta nueva cuenta.

Respecto a la sección **Roles**, recomendamos el perfil por defecto **Administrador**. En la siguiente sección se indicará cómo crear un rol personalizado, si es necesario.

En la sección **Asignaciones**, seleccione todos los sitios y grupos relevantes para la integración de Milestone.



Para finalizar, haga clic en **Crear Administrador** en la parte inferior de la página para terminar.



Se enviará un correo electrónico a la dirección de correo electrónico utilizada para establecer la contraseña de esta cuenta. Seleccione **COMENZAR**.

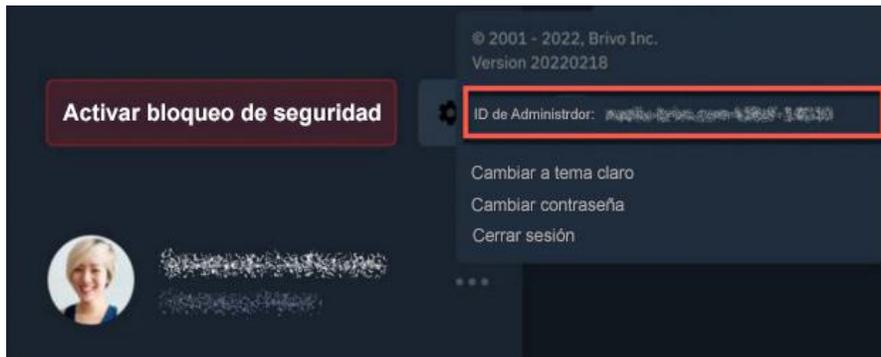


Esto le llevara a una página web para establecer la contraseña de este usuario.
 Tome nota de la **Contraseña** del usuario para el siguiente paso de la instalación.



Una vez configurada, deberá iniciar la sesión con esta cuenta para acceder a la cuenta **ID de administrador**. En la parte inferior izquierda de la página de Brivo Access, pulse los tres puntos para ver más opciones de la cuenta. Aquí se mostrará el **ID de administrador**.

Anote el **ID de administrador** para el siguiente paso de la instalación.



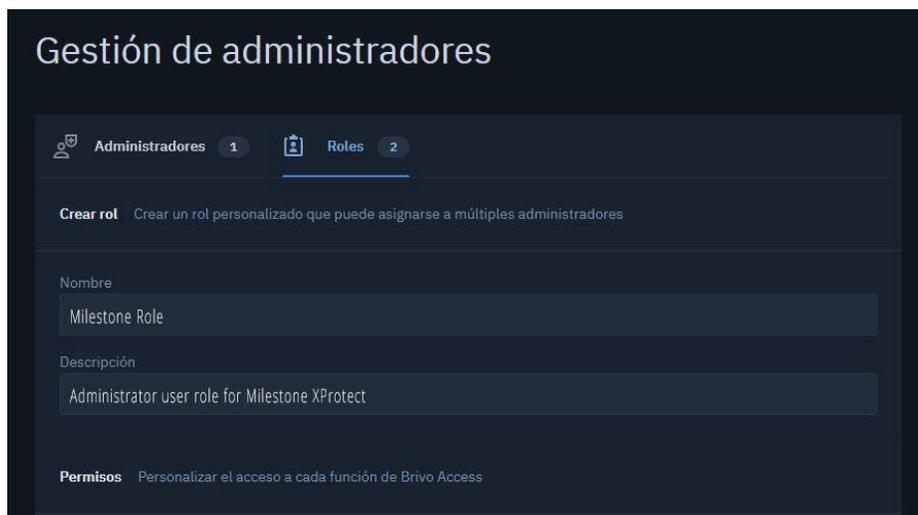
Configuración del rol de administrador personalizado

Este paso es opcional; para **Roles** recomendamos el perfil de Administrador predeterminado. Si prefiere tener un rol personalizado para limitar el acceso, siga los pasos que se indican a continuación para proporcionar el nivel mínimo de acceso a la cuenta.

En Brivo Access, seleccione **Roles** en la pestaña **Administradores**. A continuación, seleccione **Crear Rol** en la parte inferior derecha.



Agregue un **Nombre** y **Descripción** para este nuevo **Rol**.



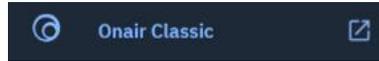
Actualice los **Permisos** para este rol, tal y como se indica a continuación.
Crear rol y aplicar a la nueva cuenta de administrador.

Permisos Personalizar el acceso a cada función de Brivo Access

Onair Classic	Sin acceso	Completo		
Tabla de seguimiento de eventos	Sin acceso	Completo		
Registro	Sin acceso	Completo		
Registro de instantáneas	Sin acceso	Completo		
Estado del dispositivo	Sin acceso	Limitado	Completo	Personalizado
Anular puertas	Deshabilitado	Habilitado		
Ver dispositivos	Deshabilitado	Habilitado		
Establecer horario	Deshabilitado	Habilitado		
Desbloquear puertas	Deshabilitado	Habilitado		
Vídeo en vivo	Sin acceso	Limitado	Completo	Personalizado
Ver vídeo en vivo (todos los sitios)	Deshabilitado	Habilitado		
Crear diseño personalizado	Deshabilitado	Habilitado		
Eliminar diseño personalizado	Deshabilitado	Habilitado		
Ver vídeo en vivo (diseño personalizado)	Deshabilitado	Habilitado		
Editar diseño personalizado	Deshabilitado	Habilitado		
Ver vídeo grabado	Deshabilitado	Habilitado		

Configuración de la aplicación API

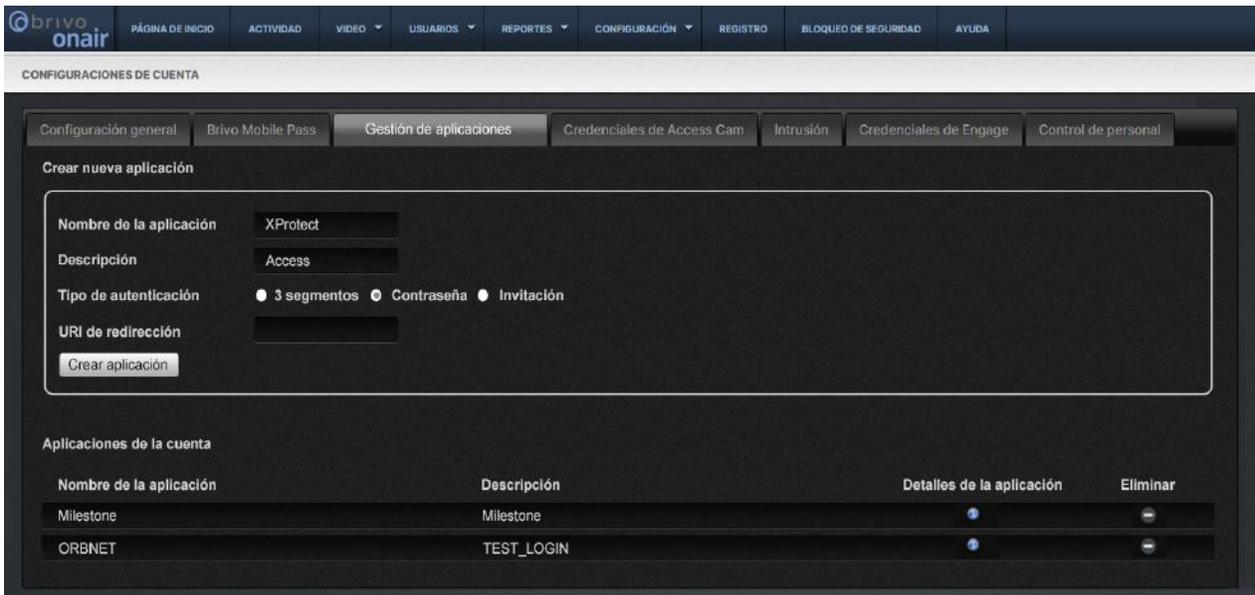
Actualmente, algunas configuraciones para este módulo solo están disponibles en Brivo Onair. Para los usuarios de Brivo Access, seleccione Onair Classic para acceder a esta sección desde el menú.



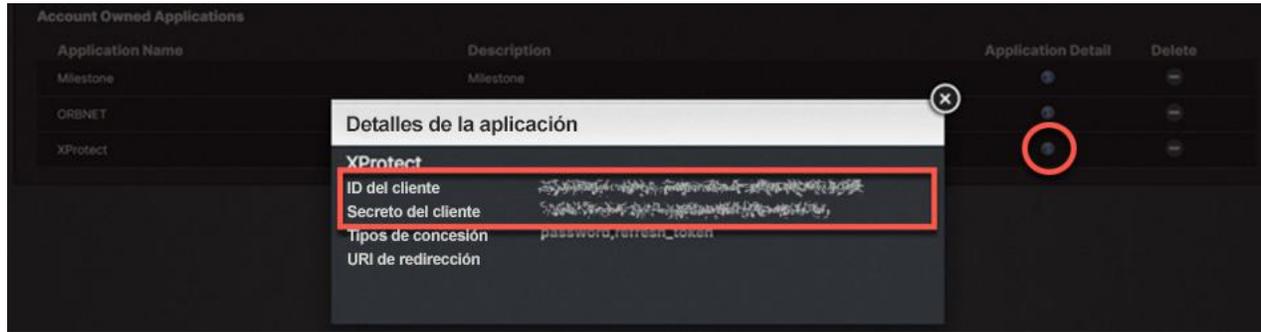
Dentro de Onair, como administrador principal o supervisor, vaya a **Configuración > Cuenta > Configuración de cuenta** y, a continuación, seleccione **Gestión de aplicaciones**.



En **Gestión de aplicaciones**, vaya a la sección **Crear una nueva aplicación**, agregue un **Nombre de la aplicación** y una **Descripción** y seleccione **Contraseña** para **Tipo de autenticación**. Seguidamente, pulse el botón **Crear aplicación**.



La nueva aplicación se añadirá a la lista, luego seleccione el ícono **Detalles de la aplicación**.



Tome nota del **ID del cliente** y del **Secreto del cliente** para el siguiente paso de la instalación.

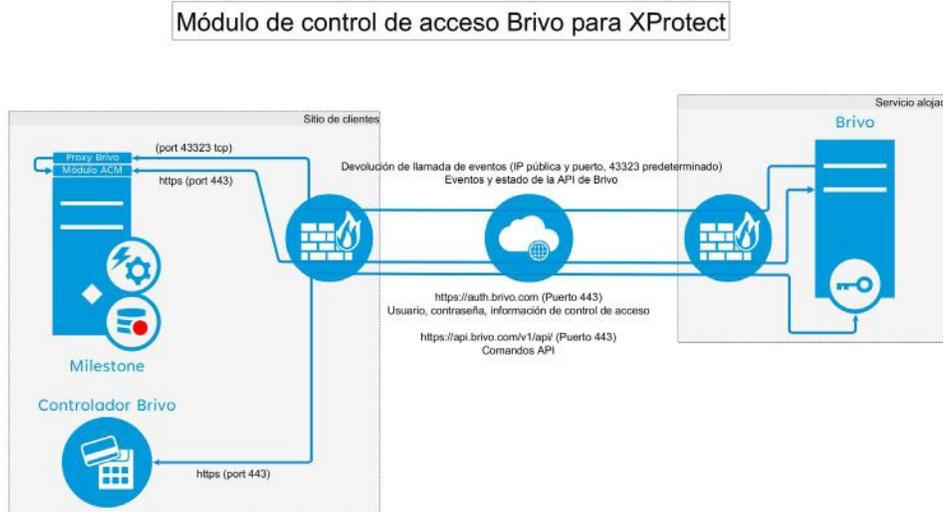
Clave API

Complete el **Formulario de acuerdo de acceso a la cuenta API** de su distribuidor de Brivo para poder obtener acceso a la Clave API.

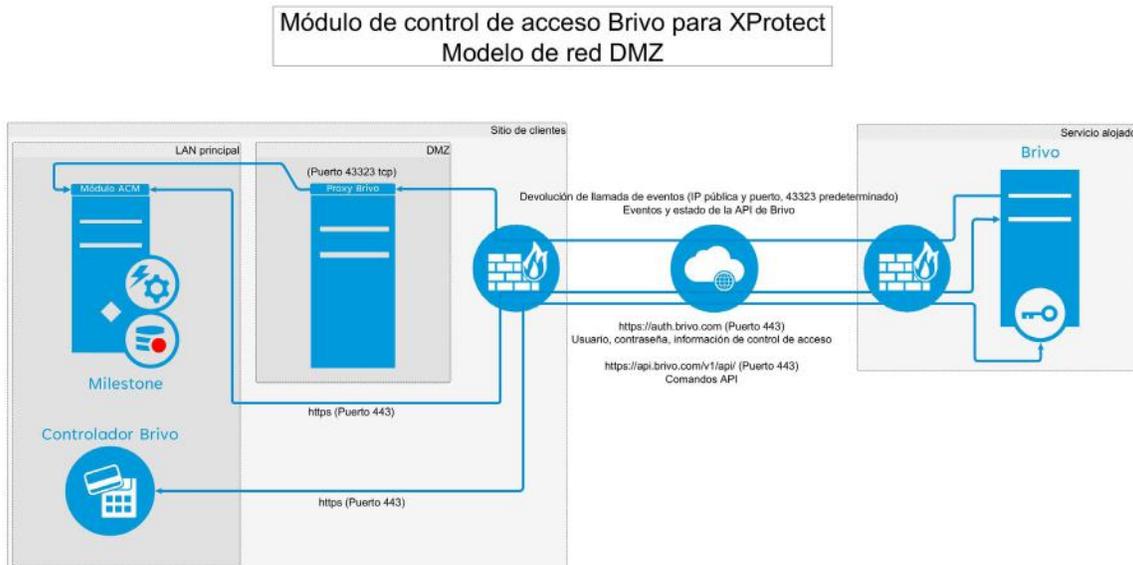
Respondedor de llamadas para el acceso desde el exterior (Event Callback)

Esquema de la red

En una instalación estándar, tanto el **Brivo Event Proxy** (utilizado para Brivo Event Callback) como la **Gestión de Milestone** residirían en el mismo servidor. Esto funcionara en un sistema en el que el servidor de Milestone tiene conexión a Internet.



En una instalación en la que el servidor de Milestone no tenga acceso a Internet, se utilizaría una máquina secundaria para enlazar la conexión a Internet. Generalmente, esto se hace en una zona desmilitarizada (DMZ), pero ello dependerá de la instalación de la red del sitio. Así sería como se instalaría el **Brivo Event Proxy**.



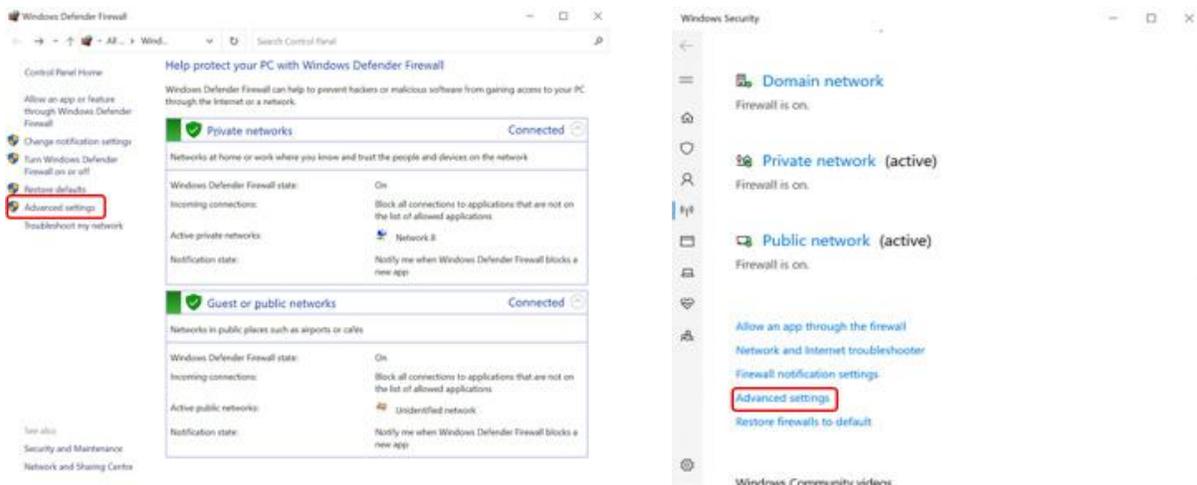
Protección con Windows Security software

Solicite autorización de la organización antes de implementar cualquier cambio de seguridad. Es posible que el equipo de seguridad informática quiera realizar esta tarea o una similar en un sistema gestionado de forma centralizada.

En este ejemplo se utiliza la interfaz predeterminada del cortafuegos (Firewall) de software de Windows Defender. Las funciones de los cortafuegos de software difieren, por lo que la configuración probablemente será diferente para el cortafuegos de software utilizado en su instalación. Consulte la guía de usuario de su cortafuegos para obtener más información.

Esta integración requiere un servicio externo basado en Internet para comunicarse con el servidor de Milestone en un puerto del protocolo de control de transmisión (TCP). Este se comunicará directamente con el Brivo Event Proxy instalado en el servidor o enlazado a un servidor en una zona desmilitarizada (DMZ). Ambos métodos requerirán que se configure un puerto TCP de entrada para permitir el acceso en uno o ambos servidores.

Vaya a **Firewall de Windows Defender** o **Seguridad de Windows** y luego seleccione **Configuración avanzada**.

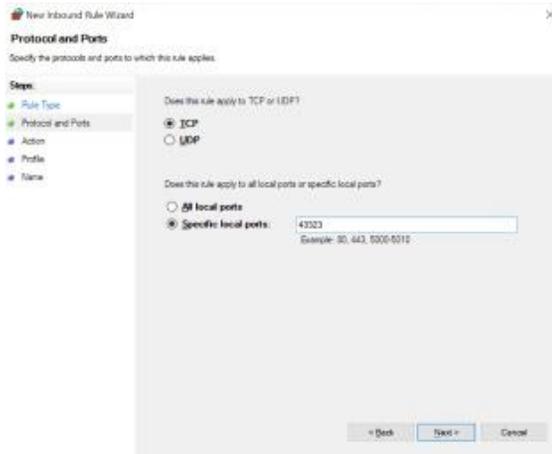
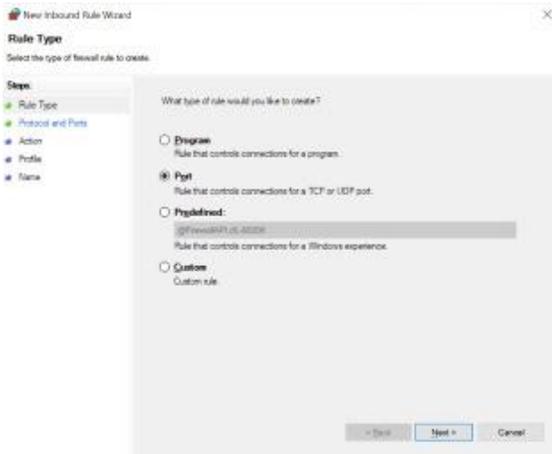


Seleccione **Inbound Rules (Ordenes de entrada)** y luego haga clic con el botón derecho para seleccionar **New Rule (Nueva orden)**.



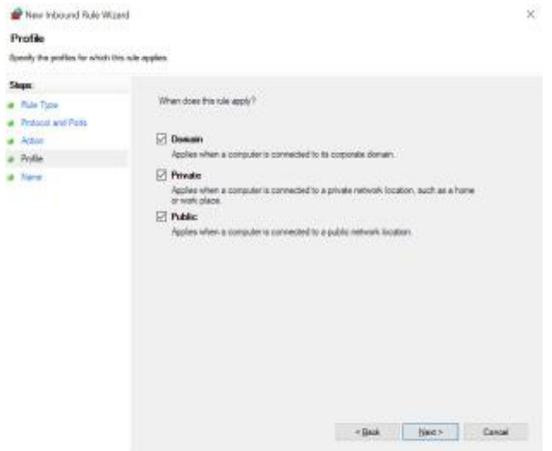
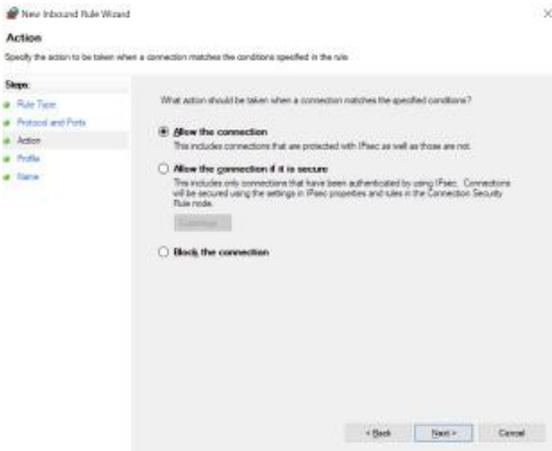
Tipo de regla = **Port (Puerto)**

Protocolo y puertos = **TCP, 43323**

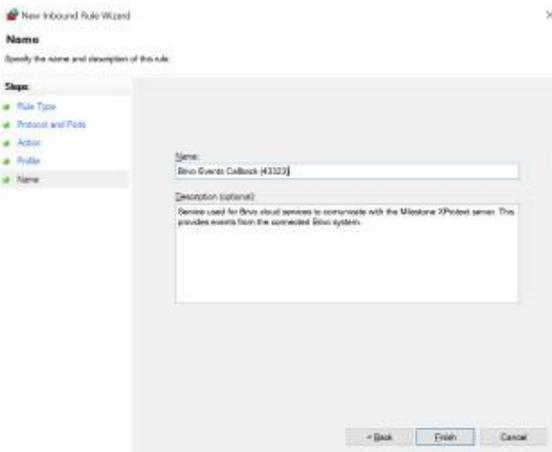


Acción = **Permitir la conexión**

Perfil = **Seleccionar todas las que correspondan**



Nombre = **Brivo Events Callback (43323)**



Configuración del cortafuegos (Firewall) de la red

Solicite autorización a la organización antes de implementar cualquier cambio de seguridad. Es posible que el equipo de seguridad informática quiera realizar esta tarea o una similar en un sistema gestionado de forma centralizada.

En este ejemplo se utiliza una interfaz básica estándar de router/cortafuegos de un fabricante conocido. Las funciones de los cortafuegos difieren, por lo que la configuración probablemente sea diferente para el cortafuegos utilizado en su instalación. Consulte la guía del usuario de su cortafuegos para obtener más información.

Agregue una restricción de IP de entrada (opcional pero recomendada).

Vaya a **Configuración de objetos > Objeto IP** y haga clic en el primer número de la lista, disponible:

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> Next >>

Establezca un nombre para este servicio y deje la interfaz predeterminada a menos que su configuración requiera que se cambie.

En el objeto IP, hay tres opciones de tipo de dirección:

Dirección única, Dirección de intervalo y Dirección de subred.

Para este ejemplo, se seleccionaría **Dirección de subred**. Los servicios de Brivo abarcan varios rangos de direcciones IP y subredes, dependiendo del lugar del mundo en el que se encuentre la instalación de este sitio, y el servidor que ejecute el servicio en ese momento dependerá de la IP que se comunique con su sistema Milestone XProtect.

This service will fall into 64.35.160.0/24 registered to Brivo Systems, LLC (Listed in ARIN).

REF: <https://rdap.arin.net/registry/entity/BRIVO-1>

REF: <https://who.is/whois-ip/ip-address/64.35.160.0>

Como se trata de una subred /24, hay 256 direcciones IP utilizables. La primera dirección IP utilizable es 64.35.160.1 con la subred añadida como 255.255.255.0.

Profile Index : 1

Name:	Brivo API
Interface:	Any
Address Type:	Subnet Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	64.35.160.1
End IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
Invert Selection:	<input type="checkbox"/>

Añada una **Redirección de puertos / Enrutamiento de puertos (Obligatorio)**.

Para configurar una regla NAT de redirección de puertos en el router, vaya a **NAT > Redirección de puertos** y haga clic en el primer número de la lista, disponible:

NAT >> Port Redirection

Port Redirection | [Set to Factory Default](#)

Index	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP	Status
1.		All					x
2.		All					x
3.		All					x
4.		All					x
5.		All					x
6.		All					x
7.		All					x
8.		All					x
9.		All					x
10.		All					x

<< 1-10 | 11-20 | 21-30 | 31-40 >> [Next >>](#)

En la entrada **Redirección de puertos**, configure las siguientes opciones:

- **Modo:** Configúrelo en Single (Individual) para abrir un solo puerto.
- **Nombre del servicio:** Se utiliza para identificar la orden NAT.
- **Protocolo:** Seleccione TCP.
- **Interfaz WAN:** La conexión a Internet en la que se abrirá el puerto.
- **Puerto público:** Este es el puerto externo. En este ejemplo, el puerto enrutado es el mismo tanto externa como internamente.
- **IP de origen:** Si ya está configurada, seleccione el objeto IP creado para la API de Brivo; de lo contrario, seleccione cualquiera.
- **IP privada:** Esta es la IP de la LAN del servidor que responderá (por ejemplo, servidor de Milestone o DMZ).
- **Puerto privado:** Este es el número de puerto del servicio que el router enviará a la IP de la LAN.

Auto Logout IP6

Dashboard
 Wizards
 Online Status

WAN
 LAN
 Load-Balance/Route Policy
 NAT
Port Redirection
 DMZ Host
 Open Ports
 Port Triggering
 Hardware Acceleration
 Firewall
 User Management
 Objects Setting
 CSM
 Bandwidth Management

NAT >> Port Redirection

Index No. 1

<input checked="" type="checkbox"/> Enable	
Mode	Single
Service Name	Brivo to Milestone
Protocol	TCP
WAN Interface	ALL
Public Port	43323
Source IP	Brivo API IP Object
Private IP	<Milestone-IP>
Private Port	43323

Haga clic en **Aceptar (OK)** para guardar la orden, y esta aparecerá como habilitada en la lista de órdenes. El router/cortafuegos ahora reenviará las solicitudes recibidas en ese puerto al servidor interno si la dirección IP coincide con la IP de origen.

Si está configurada, la IP de origen se mostrará con el servicio Brivo creado; de lo contrario, se mostrará como **Cualquiera**.

NAT >> Port Redirection

Port Redirection							Set to Factory Default
Index	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP	Status
1.	Brivo to Milestone	All	TCP	43323	Brivo API	<Milestone-IP>	✓
2.		All					✗
3.		All					✗
4.		All					✗
5.		All					✗
6.		All					✗
7.		All					✗
8.		All					✗
9.		All					✗
10.		All					✗

<< 1-10 | 11-20 | 21-30 | 31-40 >>
Next >>

Utilice un servicio de prueba como <https://www.whatismyip.com/port-scanner/> para confirmar que el puerto está accesible. La IP de origen deberá estar configurada en **Cualquiera** para poder utilizar esta herramienta, así que asegúrese de volver a cambiarla una vez completada.

Para el siguiente paso de la instalación, tome nota de la **IP pública** y del **Puerto externo** utilizados para el siguiente paso de la instalación.

Gestión de la lista de comprobación de Milestone

Lista de comprobación

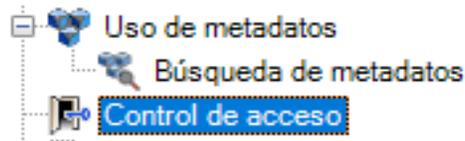
Antes de iniciar la configuración de la Lista de Comprobación (Checklist) de Milestone, revise esta lista y marque cada elemento para asegurarse de que todo está listo para que el módulo de integración funcione de inmediato. Se ha proporcionado enlaces a las secciones pertinentes.

Paso	✓	Enlace
Anotar el número de puertas que se utilizarán con Milestone		n/a
Enumerar las puertas con la(s) cámara(s) asociada(s) en Milestone		n/a
Licencia de acceso a Milestone adquirida o demostración		Acceso a Milestone
Licencia de acceso a Milestone aplicada a su servidor de Milestone		Acceso a Milestone
Módulo de control de acceso de Brivo para XProtect adquirido		Brivo Access
Creación de una nueva cuenta de administrador principal de Brivo		Configuración del administrador de Brivo
Ingreso de ID de administrador de Brivo y contraseña de la nueva cuenta		Configuración del administrador de Brivo
Creación de aplicación API de Brivo		Aplicación API
Ingreso de ID del cliente de la API de Brivo y secreto del cliente		Aplicación API
Creación o solicitud de la clave API de Brivo		Clave API
Ingreso de la clave API de Brivo		Clave API
Configuración de la orden del cortafuegos de Windows para Brivo Event Proxy		Seguridad de Windows
Configuración de la orden del cortafuegos de red para Brivo Event Proxy		Seguridad de la red
Anotar la IP pública y el puerto utilizado para acceder		Seguridad de la red
Instalación de Brivo Event Proxy y módulo para XProtect		Instalación del módulo

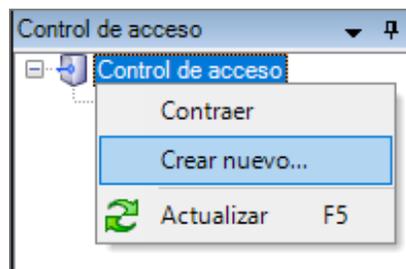
Configuración del Control de Acceso

Esta integración permite que XProtect Access conecte su sistema de control de acceso directamente con el VMS XProtect de Milestone. Está diseñado para encajar perfectamente con cualquier producto XProtect. No importa el tamaño de su instalación; con XProtect Access, podrá controlar sus cámaras de video y acceder a su sistema de control desde una interfaz central.

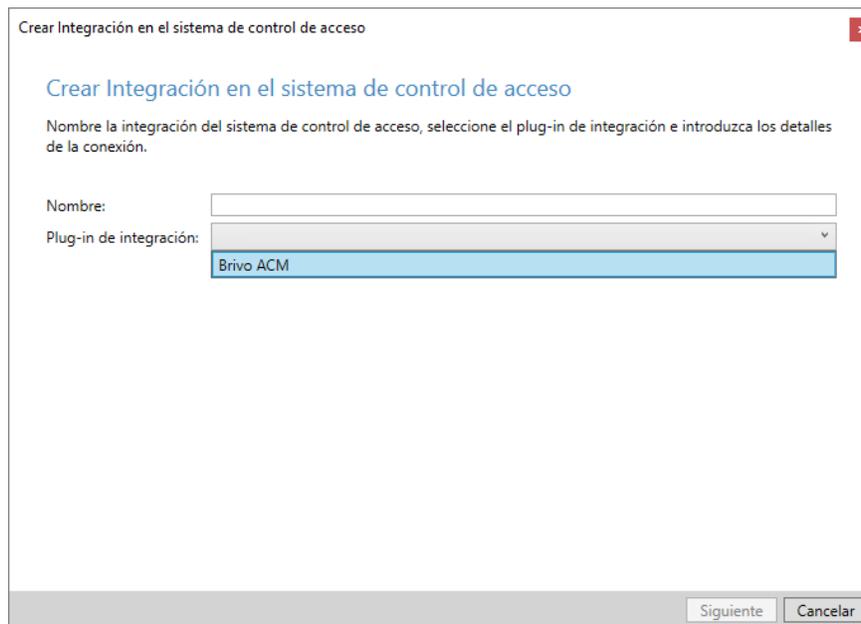
Seleccione la entrada **Control de acceso** en el diagrama de Gestión del Cliente de Milestone.



Haga clic con el botón derecho en **Control de acceso** y seleccione **Crear nuevo....**



Defina un **Nombre** para su sistema de control de acceso. Seleccione Brivo ACM V2 en el menú desplegable.



Esto mostrará la página de configuración predeterminada para este módulo de integración de acceso.

Crear Integración en el sistema de control de acceso

Crear Integración en el sistema de control de acceso

Nombre la integración del sistema de control de acceso, seleccione el plug-in de integración e introduzca los detalles de la conexión.

Nombre:

Plug-in de integración:

Brivo Authentication URL:

Brivo API URL:

Brivo Event Callback URL:

Error E-mail:

Event Proxy Address:

User:

Password:

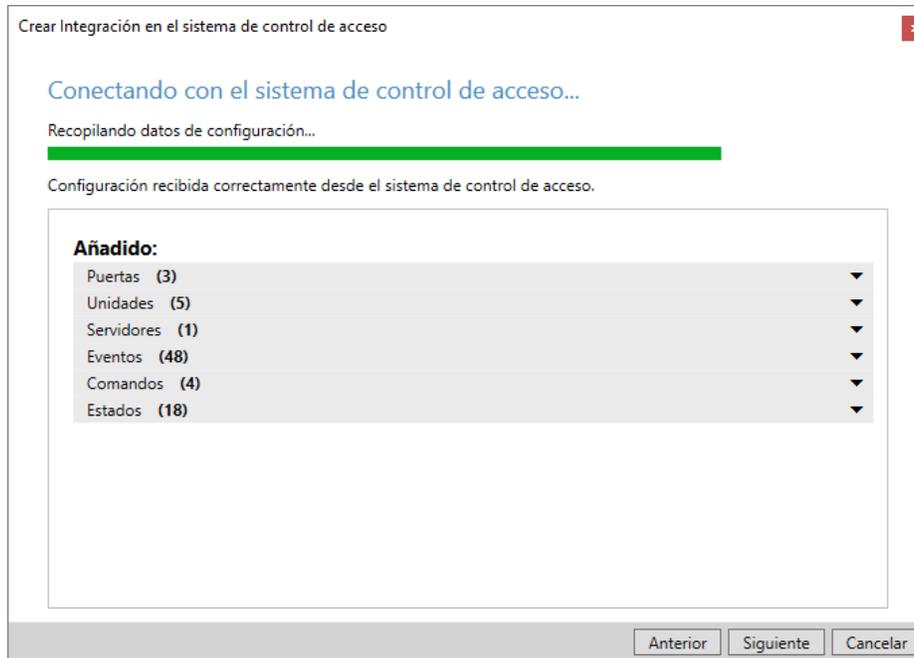
API Key:

API Client ID:

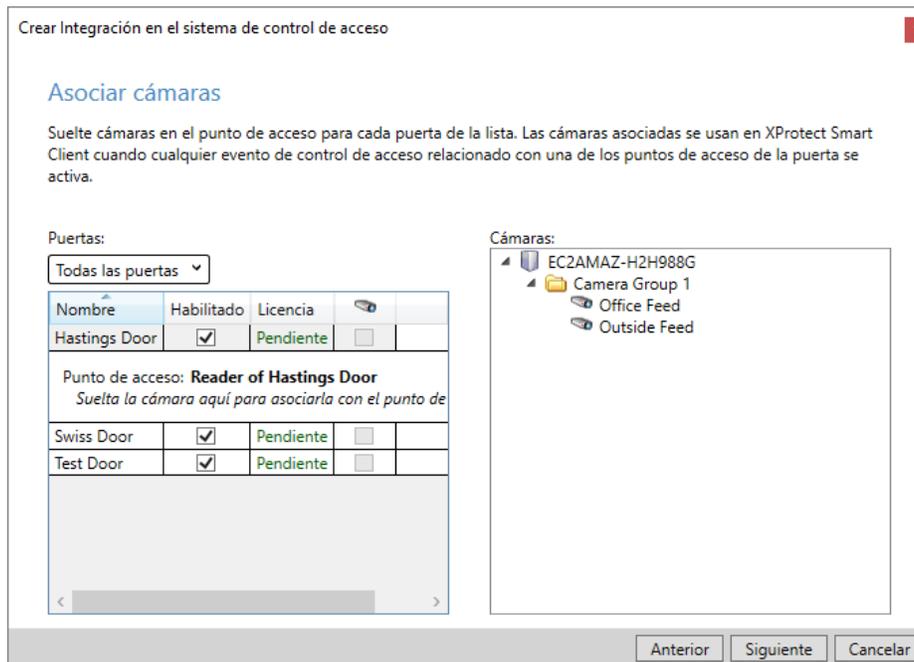
API Client Secret:

- URL de autenticación de Brivo: <https://auth.brivo.com/>. No es necesario cambiarla
- URL de la API de Brivo: <https://api.brivo.com/v1/api/>. No es necesario cambiarla
- URL de Brivo Event Callback: Actualizar con la IP externa/pública y el puerto utilizado para este servicio
- Correo electrónico relacionado con errores: Correos electrónicos enviados desde el servicio en la nube de Brivo relacionados con errores
- Dirección proxy de eventos: Dirección IP local, puerto utilizado para el proxy de eventos (Event Callback)
- Usuario: ID de la cuenta de usuario de Brivo Access (no la dirección de correo electrónico)
- Contraseña: Contraseña del usuario de Brivo Access (utilizada para iniciar sesión con la dirección de correo electrónico)
- Clave API: De la cuenta de desarrollador de Brivo o solicitada (24 caracteres)
- ID de cliente de la API: De la aplicación API creada en la cuenta de Onair
- Secreto del cliente de la API: De la aplicación API creada en la cuenta de Onair

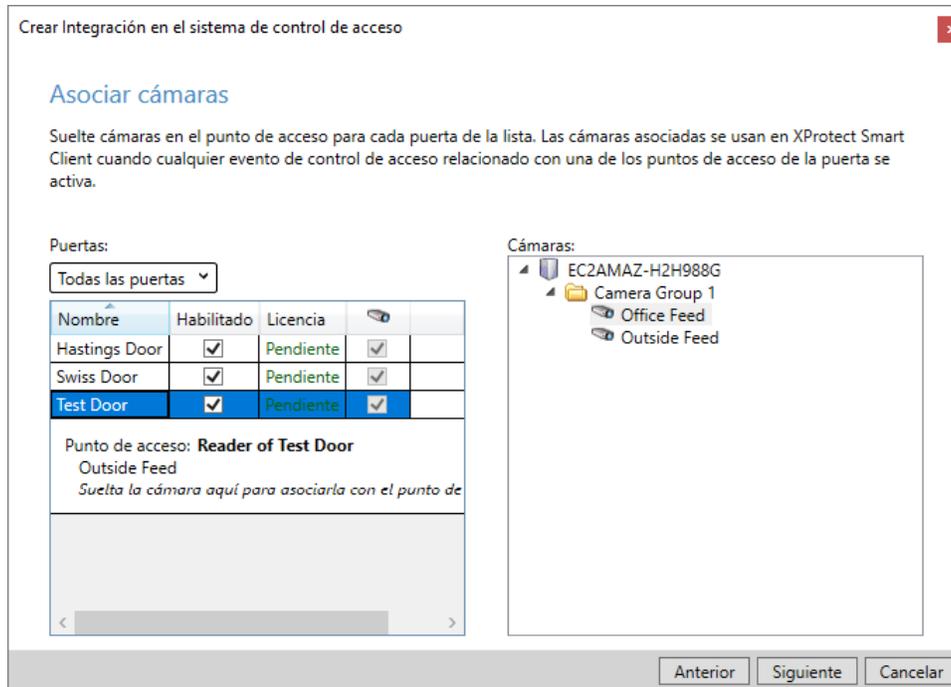
Ahora se completará la conexión con el sistema y se recibirá la configuración permitida.



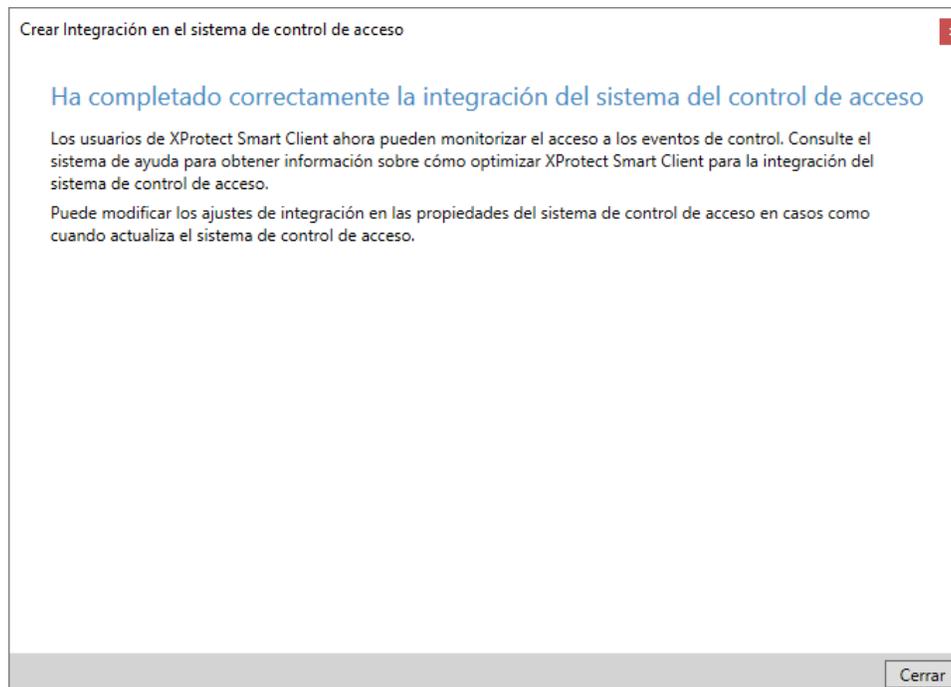
Despliegue las cámaras de Milestone disponibles y arrastre y suelte la cámara asociada a las puertas de acceso.



Una vez añadida, haga clic en **Siguiente**.



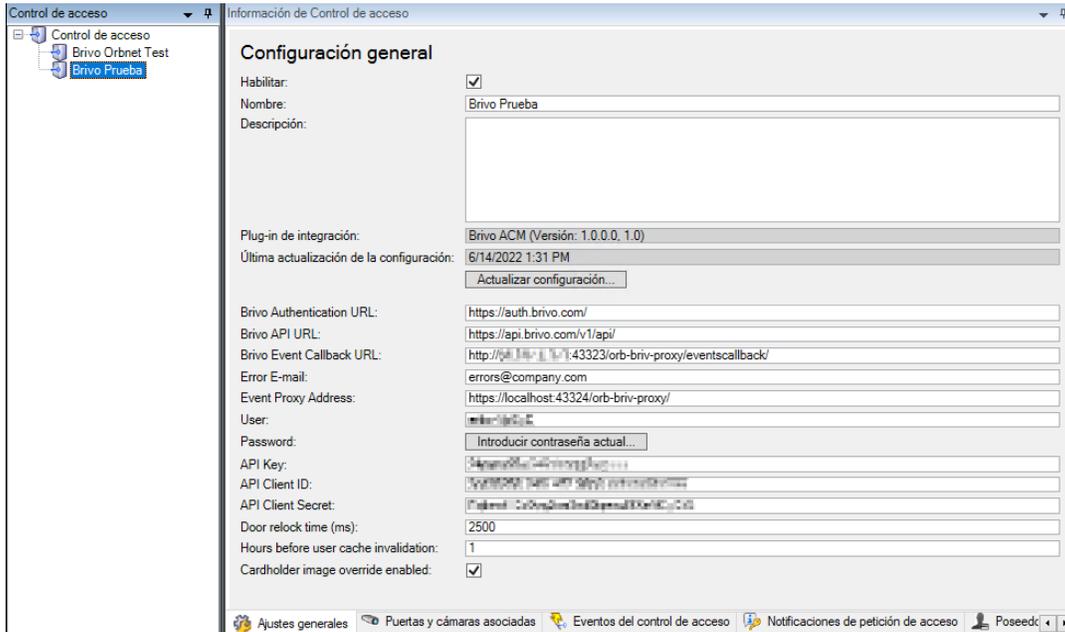
Listo, la configuración inicial ha sido completada. Una configuración adicional puede cambiarse a través del **Gestión del Cliente de Milestone**.



Información sobre el control de acceso/Otros ajustes

Esta integración proporciona las siguientes pestañas de configuración.

Configuración general



Actualizar la configuración:

Para remover o agregar una nueva puerta en el sistema Brivo Access, actualice la configuración a través de Milestone.

Ingrese la contraseña actual:

Si la contraseña de la cuenta ha sido cambiada use la tecla Contraseña para actualizarla. Si hay problemas de conexión, también se utiliza para introducir la contraseña antes de actualizar la configuración.

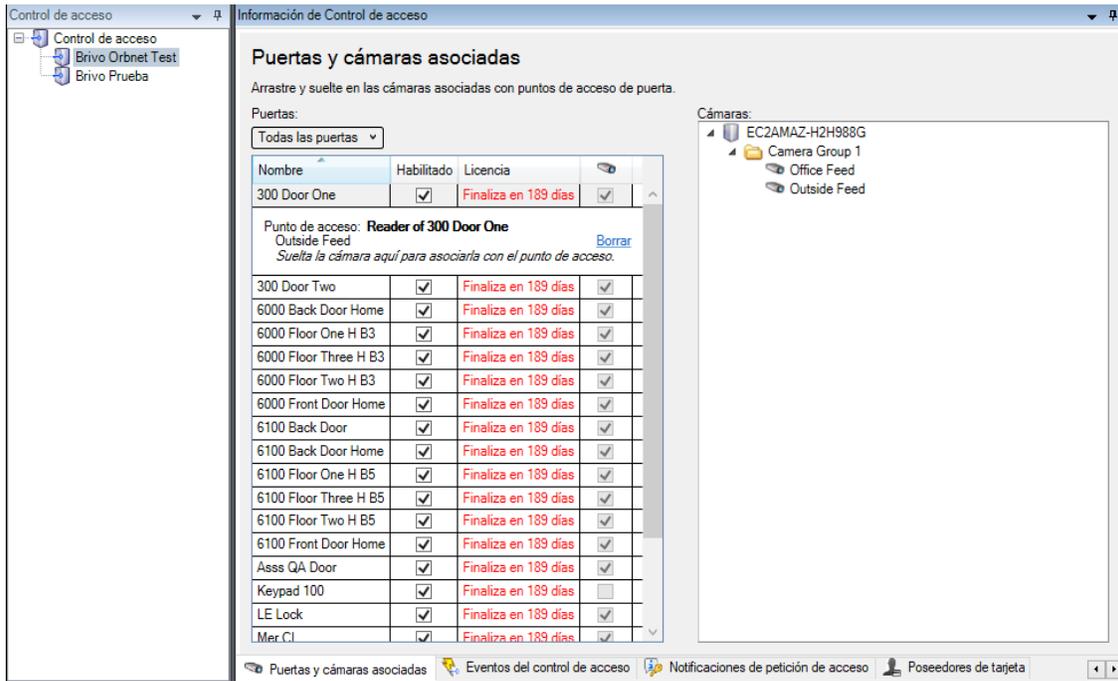
Tiempo de rebloqueo de puerta (ms):

Cuando se envían comandos de abrir puertas desde Milestone, el tiempo predeterminado antes de volver a bloquear la puerta es de (2500ms).

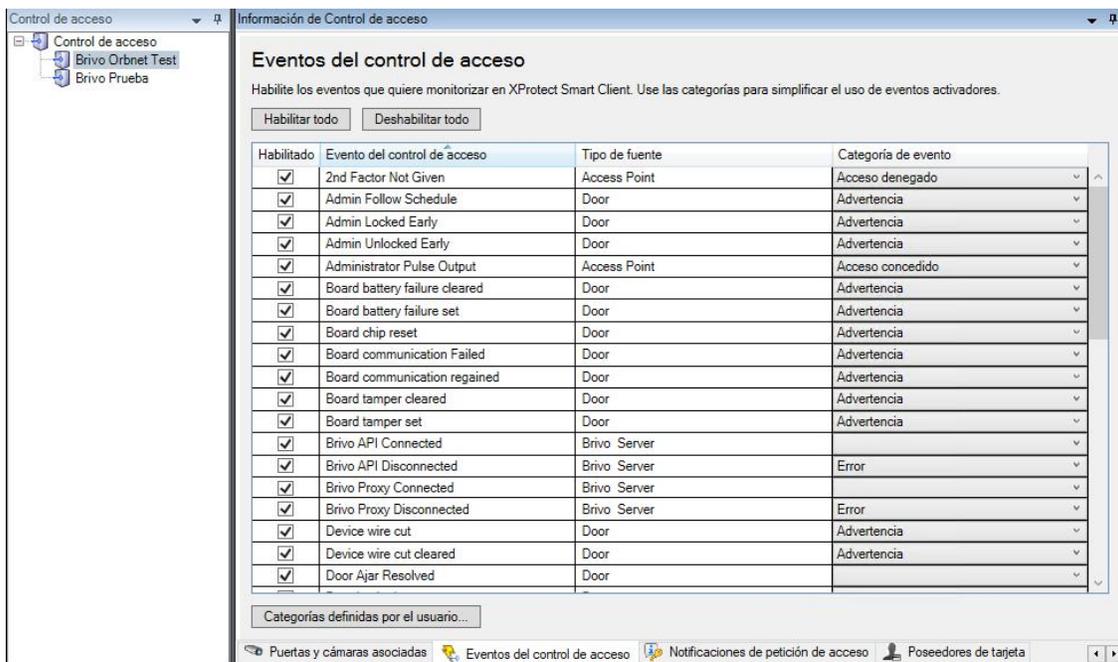
Horas antes de invalidación de caché usuario:

Este es el periodo de tiempo utilizado para actualizar la información del usuario en Milestone, (por ejemplo, nombres, imágenes). Si se realiza un cambio de la información del usuario en Brivo, esto podría demorar el tiempo especificado para aparecer en los eventos de Milestone. Predeterminado (1h), mínimo 1h, máximo 24h

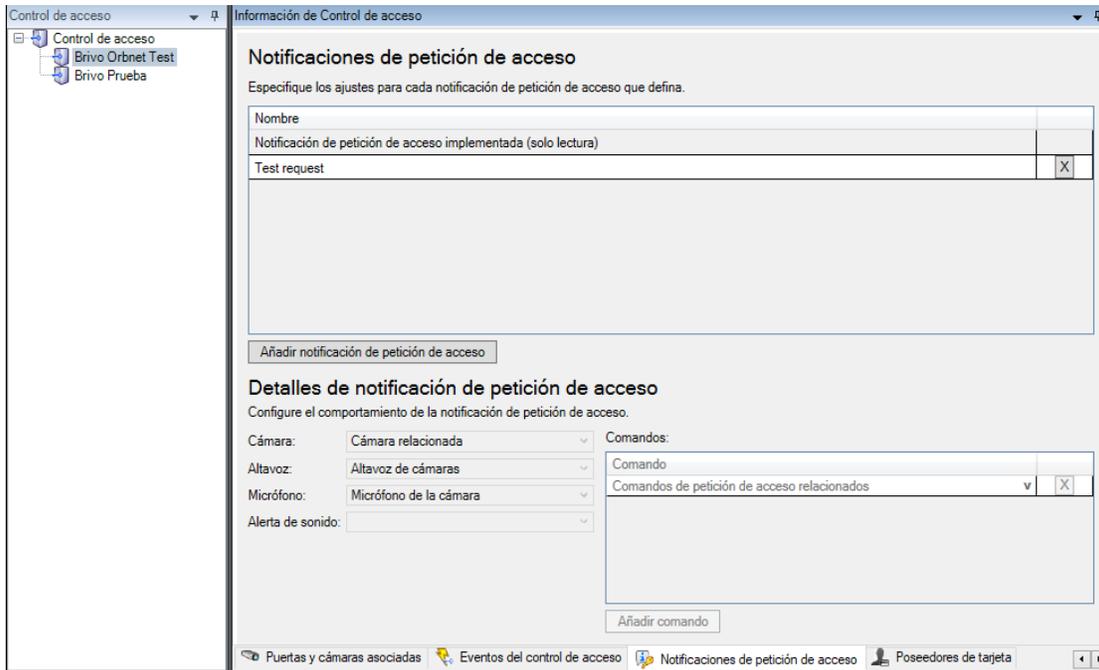
Vinculación de cámaras y puertas



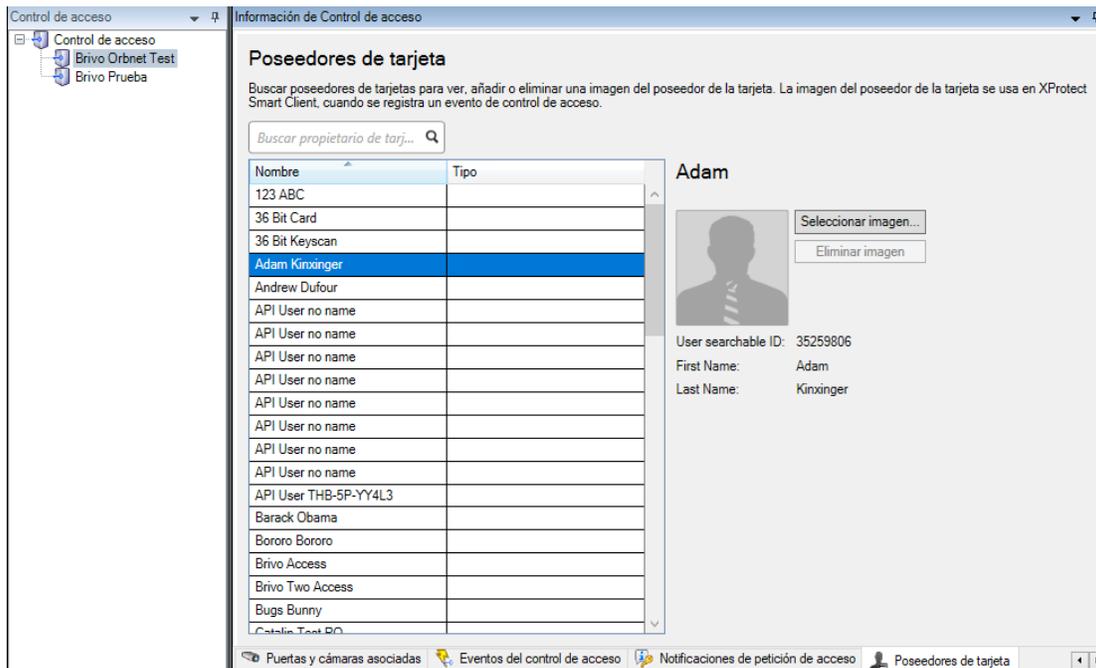
Eventos de control de acceso



Notificaciones de solicitud de acceso (no compatibles actualmente con Brivo Access)



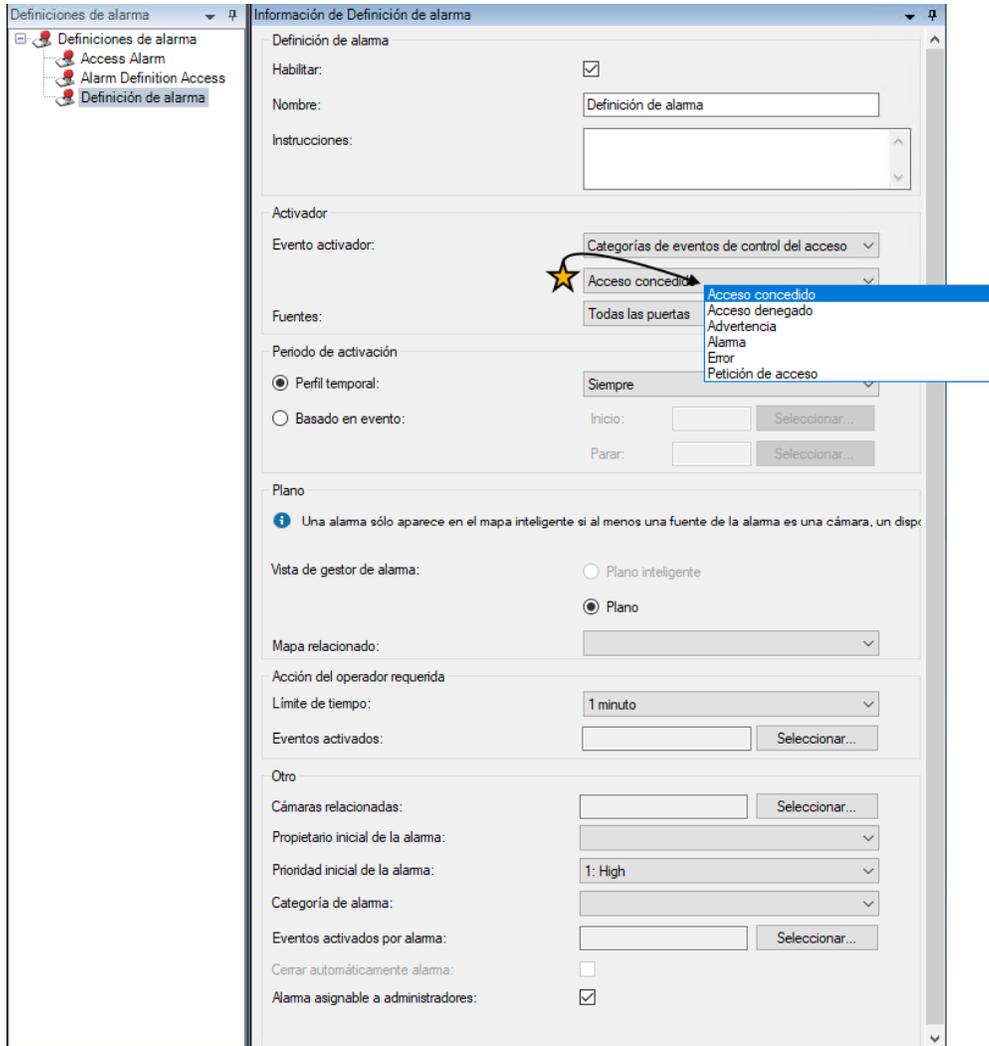
Titulares autorizados de tarjetas electrónicas de acceso (Cardholders)



Configuración de las alarmas

En Gestión de Milestone, se pueden crear alarmas a través de Access Control Events (Eventos de control de acceso).

El siguiente ejemplo de alarma muestra un método sencillo para crear un evento de acceso denegado en todas las puertas del sistema, y luego hacer que ese evento muestre automáticamente una alarma en el Milestone Smart Client mostrando un mapa con una vista especificada.



A continuación se muestra la **Alarma** que se activa en el Smart Client. Aparecerá un anillo rojo intermitente alrededor de la puerta que activó el evento.

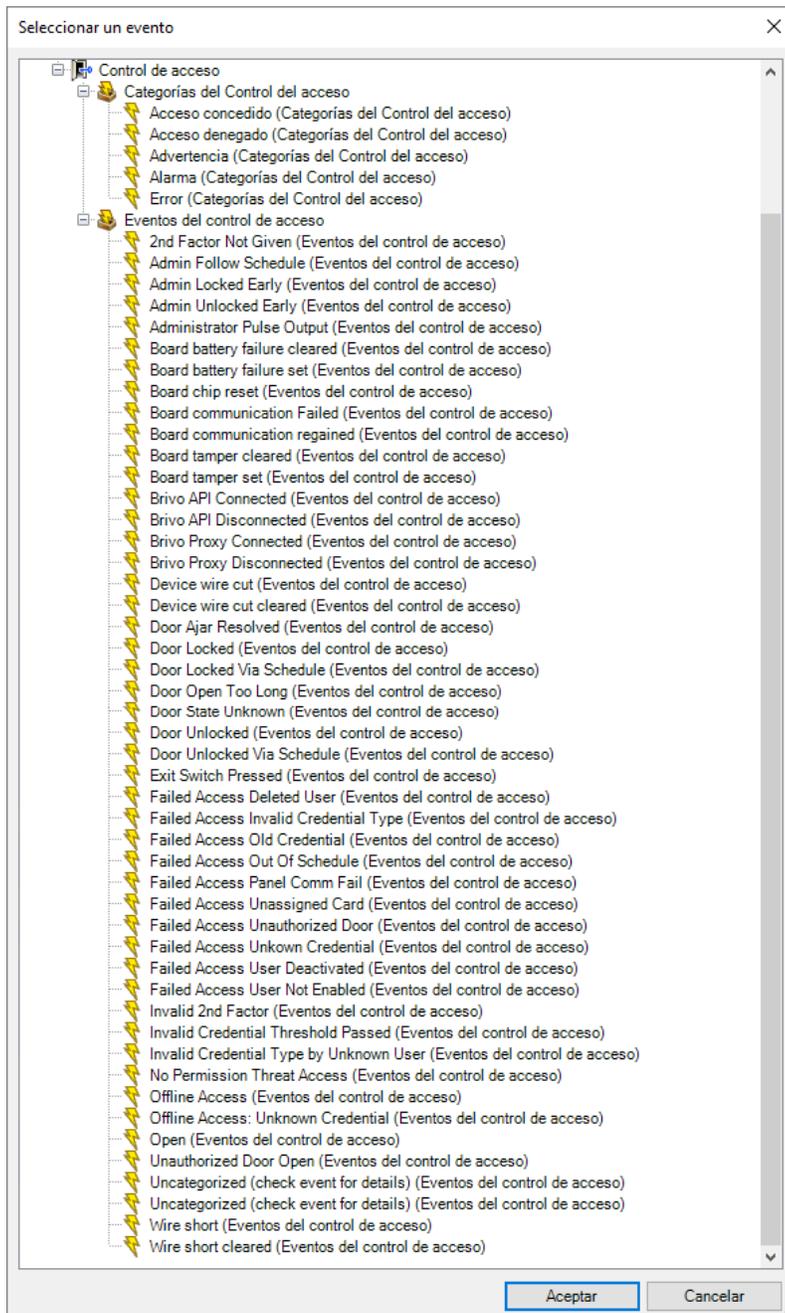
The screenshot displays the Brivo Smart Client interface. At the top, the title bar reads 'Milestone XProtect Smart Client' with the date and time '6/14/2022 1:43:41 PM'. Below the title bar are navigation tabs: 'Directo', 'Reproducción', 'Buscar', 'Gestor de alarma', 'Control del acceso', and 'Monitor de sistema'. The main area is split into two panels. The left panel shows a floor plan of the '01_Ground Floor' with a red circle highlighting '300 Door Two'. The right panel shows a video feed titled 'Office Feed - 6/13/2022 5:07:39.643 PM' showing two people walking through a doorway. Below the video panels is a table of alarm events.

Alarma	Horas	Nivel de prioridad	Nivel de estado	Nombre de estado	Mensaje	Fuente	Propietario	ID
	6:05:03 PM 6/2/2022	1	1	Nuevo	Door Open Tr.	Asss GA Door		161
	2:35:26 PM 5/2/2022	1	1	Nuevo	Door Open Tr.	300 Door Two		160
	2:30:58 PM 5/2/2022	1	1	Nuevo	Unauthorized	300 Door Two		159
	3:18:46 PM 5/30/2022	1	1	Nuevo	Door Open Tr.	300 Door Two		158
	3:18:23 PM 5/30/2022	1	1	Nuevo	Unauthorized	300 Door Two		157
	5:45:47 PM 5/24/2022	1	1	Nuevo	Unauthorized	300 Door One		156
	5:44:18 PM 5/24/2022	1	1	Nuevo	Door Open Tr.	300 Door One		155
	5:44:12 PM 5/24/2022	1	1	Nuevo	Video short	300 Door One		154
	5:43:47 PM 5/24/2022	1	1	Nuevo	Unauthorized	300 Door One		153
	5:37:59 PM 5/24/2022	1	1	Nuevo	Failed Access	Reader of 300 Door Two		152
	5:37:44 PM 5/24/2022	1	1	Nuevo	Door Open Tr.	300 Door One		151
	5:37:07 PM 5/24/2022	1	1	Nuevo	Unauthorized	300 Door One		150
	5:36:42 PM 5/24/2022	1	1	Nuevo	Failed Access	Reader of 300 Door Two		149
	5:35:46 PM 5/24/2022	1	1	Nuevo	Door Open Tr.	Asss GA Door		148
	4:28:26 PM 5/24/2022	1	1	Nuevo	Door Open Tr.	LE Lock		147
	4:27:59 PM 5/24/2022	1	1	Nuevo	Door Open Tr.	300 Door One		146

Configuración de las reglas y los eventos

Para acceder a los eventos de control de acceso en Milestone, seleccione la sección **Reglas y Eventos > Reglas** en el Cliente de Gestión y luego haga clic con el botón derecho en la columna central para añadir una nueva orden.

- Realice una acción en un **Evento**



A través de **Reglas y eventos** en Milestone, es posible habilitar un evento del sistema de control de acceso para activar un evento o acción adicional en XProtect. La siguiente regla es un ejemplo sencillo de cómo registrar una cámara específica cuando se recibe un evento de **Acceso denegado**.

Gestionar regla
— □ ×

Nombre:

Descripción:

Activo:

Paso 3: acciones

Seleccionar las acciones que deben realizarse

- Recuperar y almacenar grabaciones a distancia entre <hora de inicio y fin> desde <dispositivos>.
- Guardar imágenes adjuntas
- Activar archivo en <archivos>
- En el <sitio>, active el <evento definido por el usuario>
- Open <DoorAccess Point>
- Mostrar <access request notification>
- Override Lock <DoorAccess Point>
- Override Unlock <DoorAccess Point>
- Override Cancel <DoorAccess Point>**

Editar la descripción de la regla (haga clic en un elemento subrayado)

Realizar una acción en Acceso ilegal
 de Todas las cámaras
 Open DoorAccess Point
 y Override Lock DoorAccess Point
 y Override Unlock DoorAccess Point
 y Override Cancel DoorAccess Point

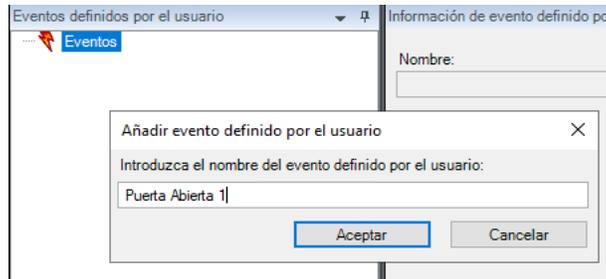
Ayuda
Cancelar
< Anterior
Siguiente >
Finalizar

Configuración de eventos definidos por el usuario

Generalmente, se pasa por alto que la opción **Evento definido por el usuario** permite un fácil acceso al control de una acción de salida a través de Milestone y Smart Client. La configuración inicial del evento definido por el usuario es como un marcador de posición para una orden.

En **Reglas y eventos**, seleccione **Eventos definidos por el usuario**, haga clic con el botón derecho y seleccione **(Añadir evento definido por el usuario)**.

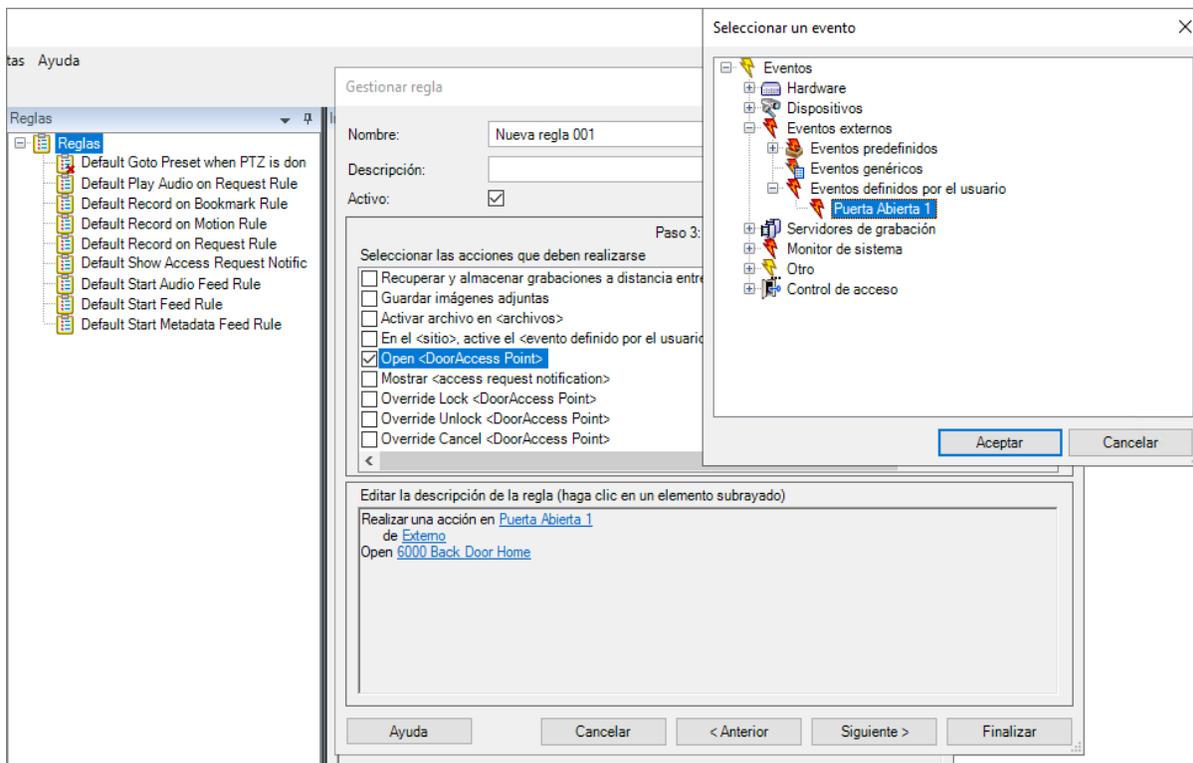
Esto solo proporciona un campo de nombre. Complételo con un nombre relevante para la acción que pretende agregar. Recuerde que este es el nombre del evento que se muestra en el Smart Client.



Vuelva a **Reglas** para crear una nueva regla y seleccione el **Evento definido por el usuario** que fue creado.

Realice una acción en un **Evento**

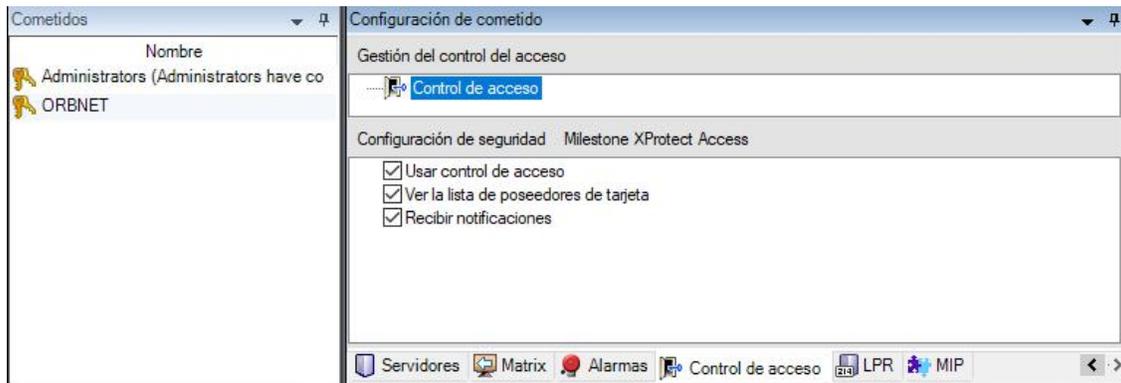
- **Eventos > Eventos externos > Eventos definidos por el usuario**
- Haga clic en **Siguiente** y seleccione la acción pertinente que debe realizarse en el panel de Brivo seleccionando la(s) casilla(s).



Configuración de acceso de los usuarios en Smart Client

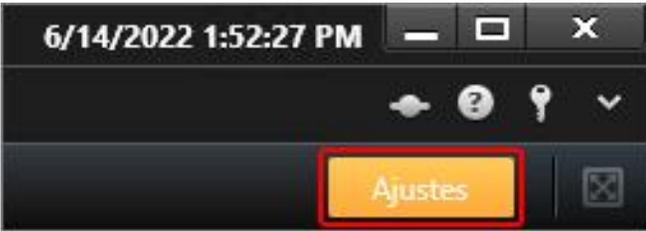
Existen muchas opciones para la visualización y gestión de los datos de control de acceso en el Milestone Smart Client. El objetivo de la integración de los sistemas ORBNET con Brivo es habilitar muchas de ellas.

Para comenzar, inicie sesión en el Smart Client con un usuario miembro que este autorizado para la configuración de control de acceso activada en el Gestión del Cliente de Milestone.



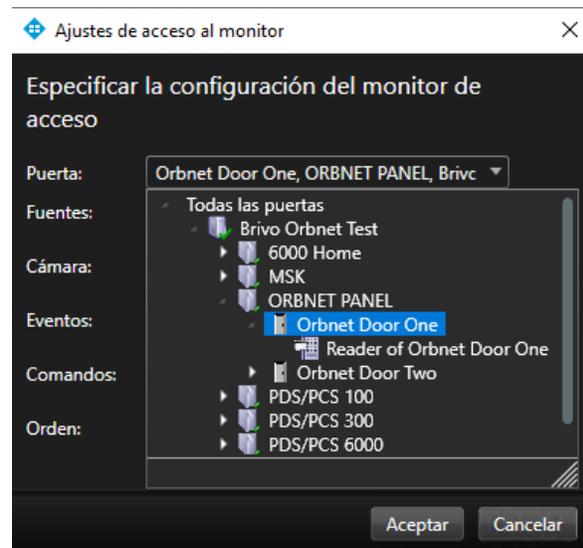
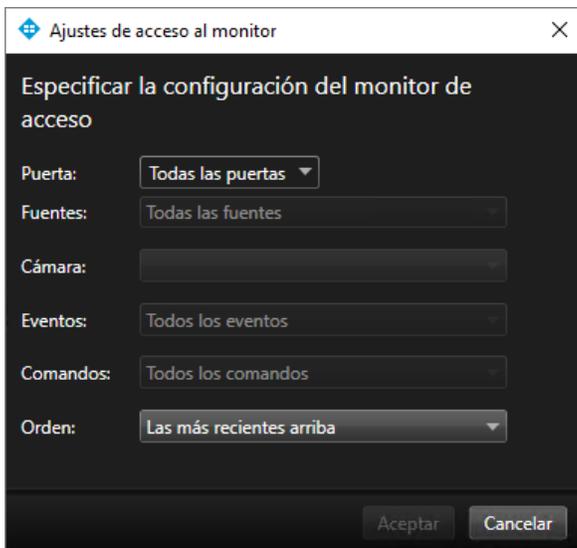
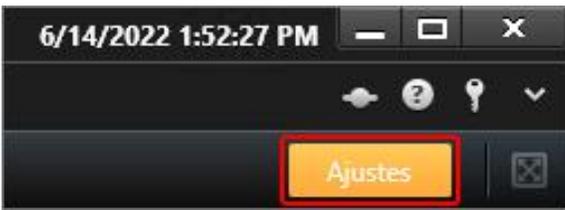
Configuración de funciones y configuración de Smart Client

Una vez que inicie sesión en el Smart Client, ingrese en el modo **Configuración** a través del menú del sitio a la derecha. Esto permite acceder a la configuración de las funciones que se indican a continuación. Las barras de menú se mostrarán en naranja para indicar que la configuración está activada.



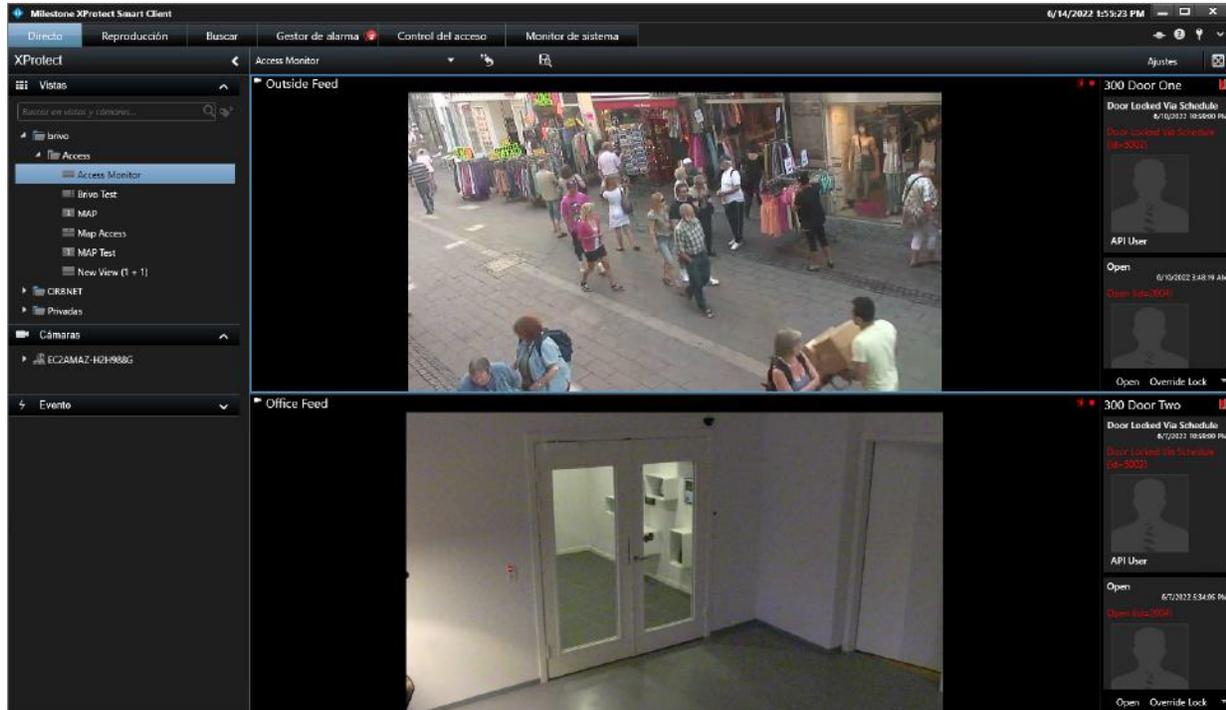
Configuración de monitor de acceso

Arrastre el **Monitor de acceso** al mosaico de la ventana y seleccione la puerta de origen. Ahora elija los eventos que desea recibir de una puerta específica. Se recomienda seleccionar una puerta para el **Monitor de acceso** en lugar del lector, ya que proporcionará más eventos.



El siguiente ejemplo es de una puerta con un lector. Aquí hay una puerta, 2 lectores y 2 cámaras. La misma puerta está asociada a ambas ventanas en el Smart Client y a lectores individuales por cada puerta.

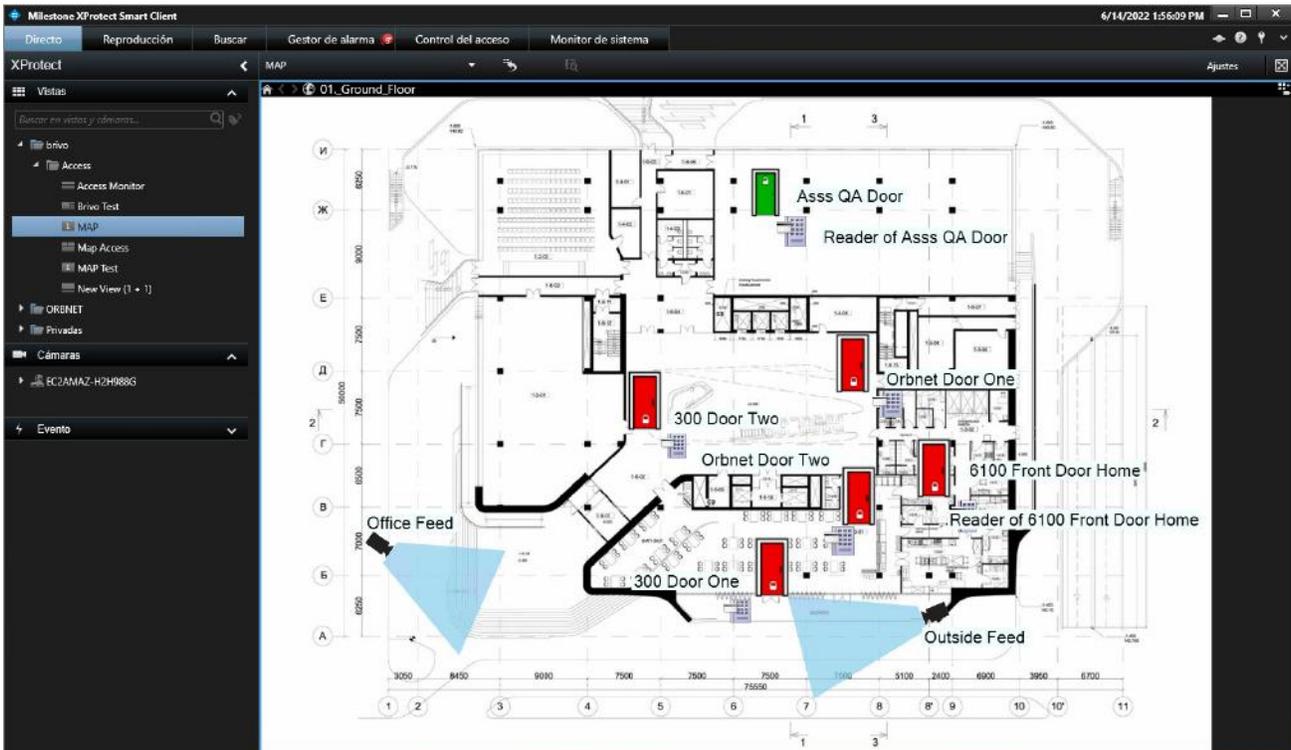
Aquí se puede apreciar una vista de Smart Client donde se muestra la transmisión de la cámara relacionada o seleccionada con los eventos de la puerta a la derecha del recuadro. Cuando se hace clic en un evento, se regresa a la reproducción dentro del recuadro que muestra la hora en que se produjo el evento.



Configuración de las mapas de Smart Client

Todos los componentes de Brivo se pueden añadir a un mapa creado en el Milestone Smart Client.

En los mapas de Milestone se pueden añadir íconos para las **Puertas** y los **Lectores**. Observe que en la captura de pantalla que aparece abajo, el icono del lector cambiará de color según sea la credencial de la persona involucrada en el evento.



Las puertas se mostrarán en rojo cuando estén bloqueadas, y aparecerá una puerta abierta cuando estén desbloqueadas. Respecto a los estados de anulación, estos se muestran con barras en la puerta para indicar un estado fijo de bloqueo (rojo) o desbloqueo (verde). Los lectores parpadearán en verde o en rojo dependiendo de la credencial presentada y estarán en estado normal en caso contrario.

Cuando un dispositivo está sin conexión o hay un problema de conexión, se mostrará el ícono del dispositivo con una cruz.

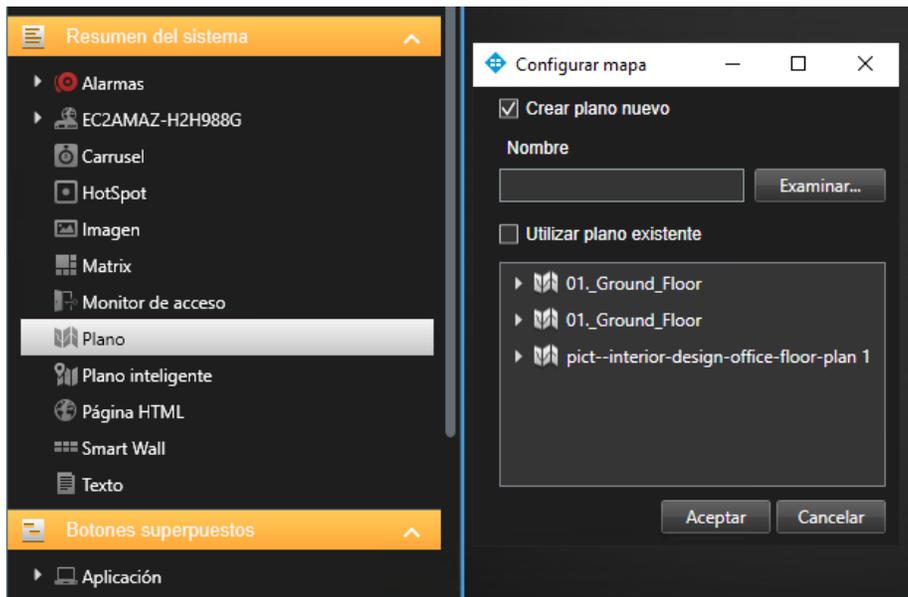
Estados de las puertas



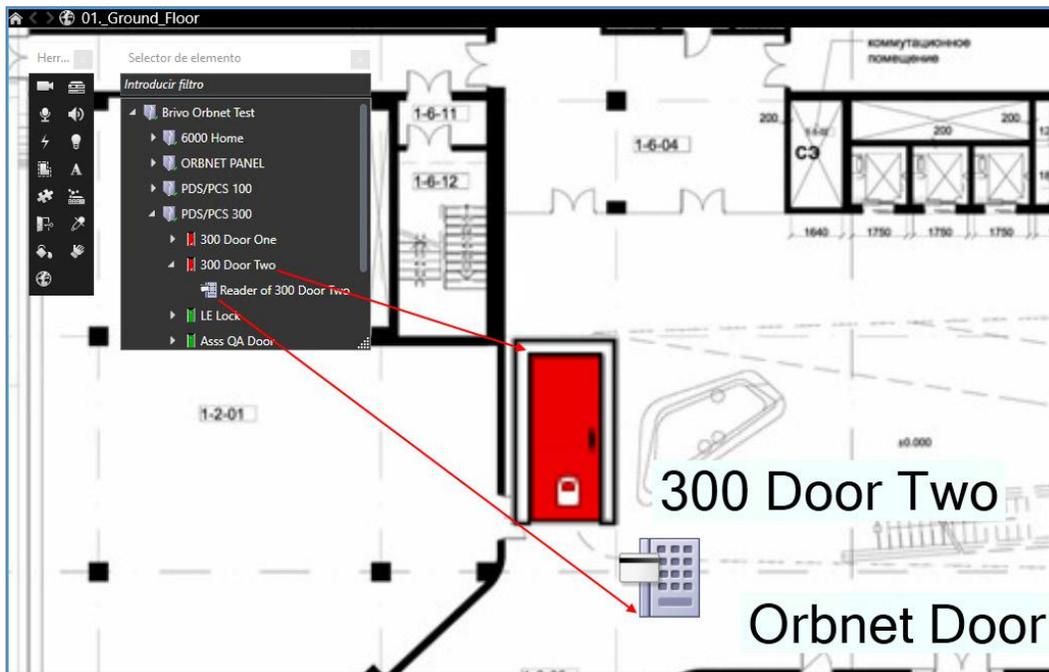
Estados de los lectores



En el modo **Configuración**, cree un nuevo diseño de vista (recomendado 1x1), y arrastre el componente del mapa al mosaico en blanco. Seleccione una imagen del plano de la planta que represente la disposición de su sitio.



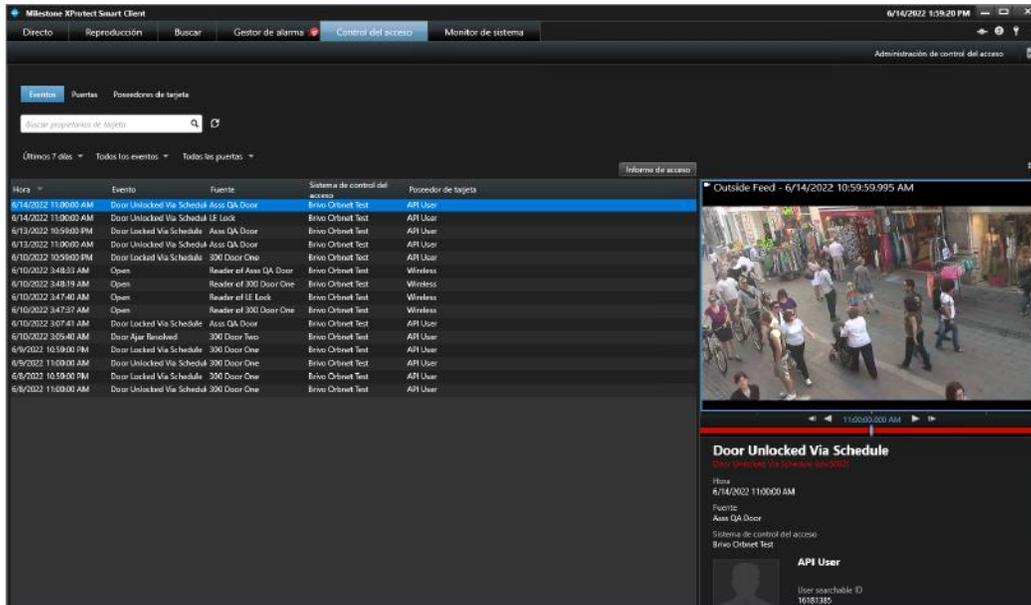
En el menú **Herramientas**, seleccione **Control de acceso**. En la lista desplegable, ahora verá los dispositivos Brivo que se han habilitado en Milestone.



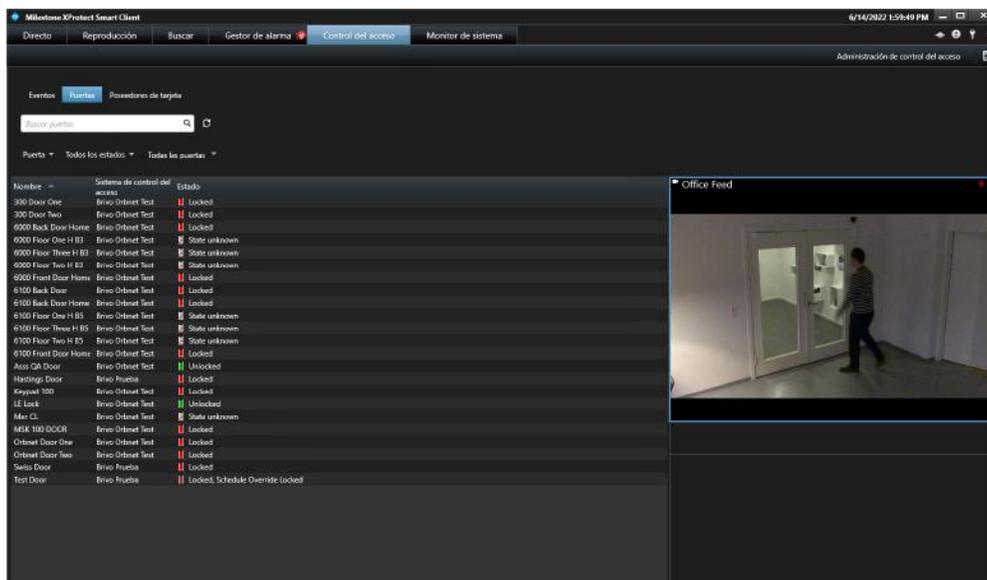
Configuración de la pestaña de control de acceso

La pestaña **Control de acceso** del Milestone Smart Client puede ser utilizada como la interfaz central de monitoreo para el sistema de control de acceso. Los eventos pueden buscarse por tipo de evento, puertas específicas y/o titulares de tarjetas. También hay una opción para que la lista se actualice en directo.

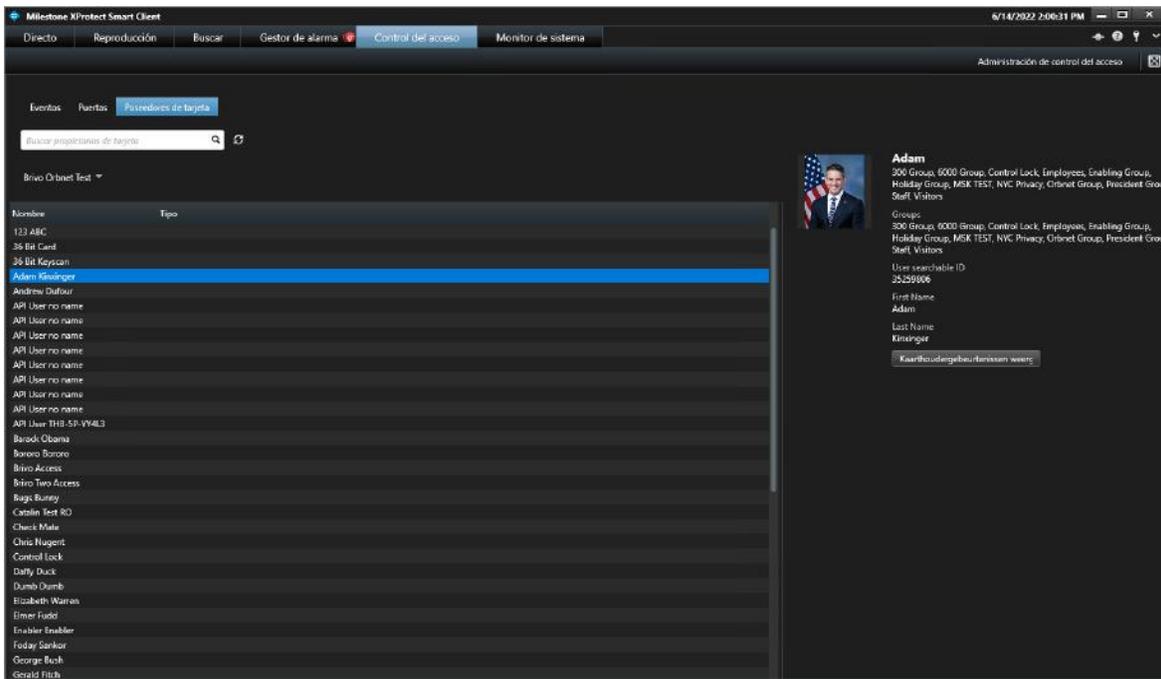
Una vez que se selecciona un evento, como se muestra en la siguiente captura de pantalla, se mostrará información adicional de la puerta, el titular de la tarjeta o el tipo de evento.



La pestaña **Puertas** muestra la lista de puertas del sistema y permite controlar la puerta a través de Milestone. Los controles mostrados son **Abrir**, **Anular bloqueo**, **Anular desbloqueo**, y **Anular cancelación**.



La pestaña **Titulares de tarjetas** permite la búsqueda de prueba de usuarios y la búsqueda con un solo clic de todos los eventos de un usuario específico, lo cual permite crear un informe completo con una captura de pantalla en miniatura para cada evento del titular de la tarjeta, tal y como se muestra a continuación.

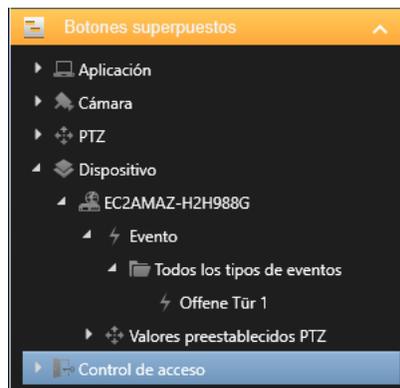


Configuración de eventos definidos por el usuario

Desde un diagrama que ya haya sido creado, busque **Botones de superposición > Dispositivo > {Nombre del servidor} > Eventos > Todos los tipos de eventos > {Evento definido por el usuario}**.

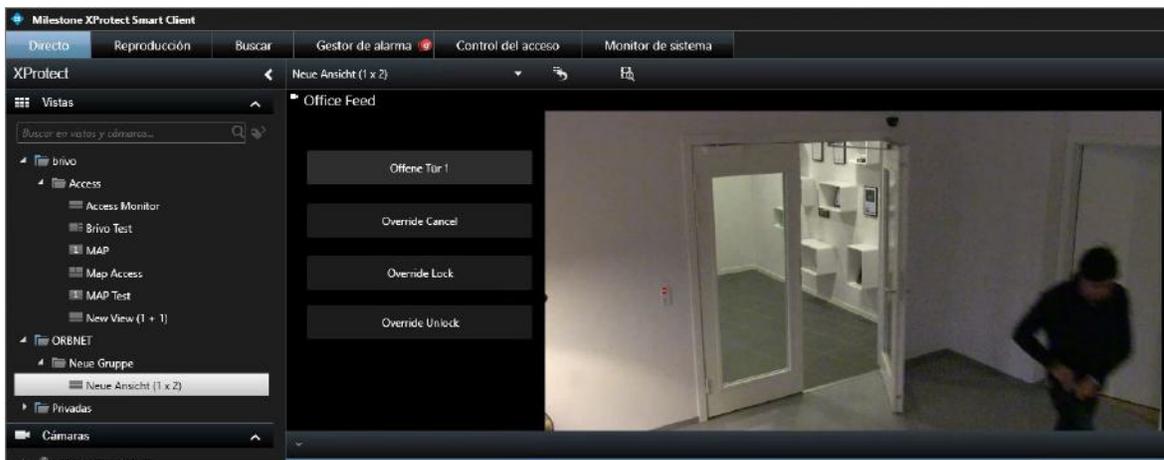
NOTA: Consulte la sección **Eventos definidos por el usuario** en Reglas y alarmas de Milestone de este documento para obtener más información.

Arrastre y suelte esto en un mosaico; esto aparecerá como un botón pulsador sobre el mosaico de la cámara.



Cuando esté fuera de la configuración en el modo En vivo, verá el **Botón de superposición** solo cuando el mouse se sitúe sobre el mosaico de la cámara. Solo se pueden utilizar en un mosaico de la cámara, como se muestra a continuación.

Como se muestra a continuación, **Abrir puerta 1** y **Activar la salida**.



Solución de problemas

Instalación del servidor de eventos

Si Milestone se instaló a través de una instalación personalizada, es posible que el servicio de eventos no se haya incluido, ya que no siempre es necesario.

Desde el servidor/máquina con el servicio de Gestión de Milestone, ingrese a <http://localhost/installation/admin/>

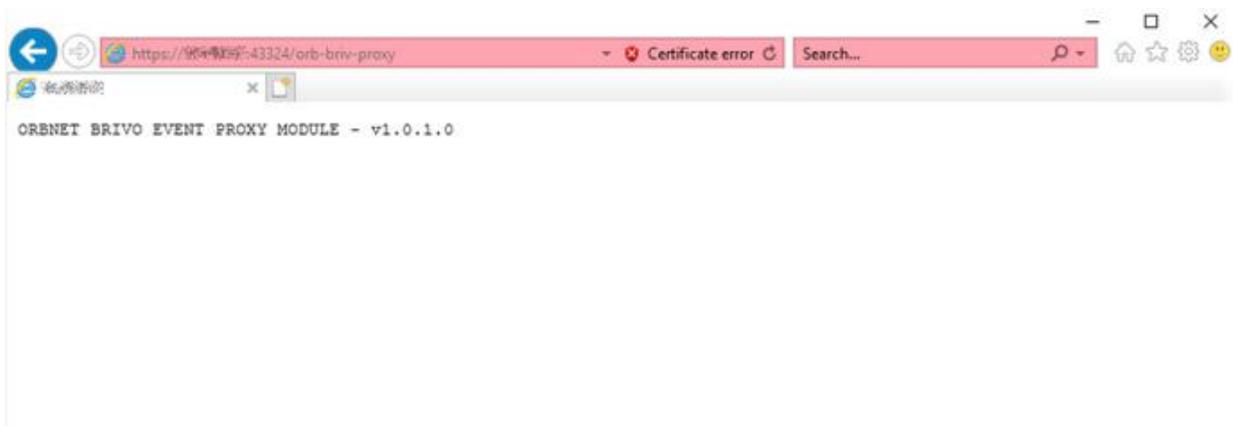
Con esto se abrirá una página de instalación de Milestone en la que podrá ejecutar el instalador del Event Server. Este debe instalarse para que el plugin ORBNET pueda comunicarse con Milestone.

Error al recibir la configuración del sistema de control de acceso

Si Milestone no puede comunicarse con Brivo, compruebe si puede acceder al sitio que figura a continuación. Será necesario implementar una orden de cortafuegos para permitir esta conexión.

<https://<ipOrHostname>:<port>/orb-briv-proxy/eventscallback/>

Utilice su IP externa y el puerto utilizado para este servicio y elimine **eventscallback/** del final de esta URL. Debería poder acceder a la siguiente página web con su IP externa y el puerto **43323** [puerto interno predeterminado].



Cambio del puerto proxy por defecto

Para actualizar el puerto predeterminado, se necesita un cambio manual en el archivo de configuración. Primero, detenga el servicio proxy antes de cambiar y guardar esta configuración. Asegúrese de que esto se actualice en la configuración general de la aplicación de Gestión de Milestone para la conexión de Brivo.

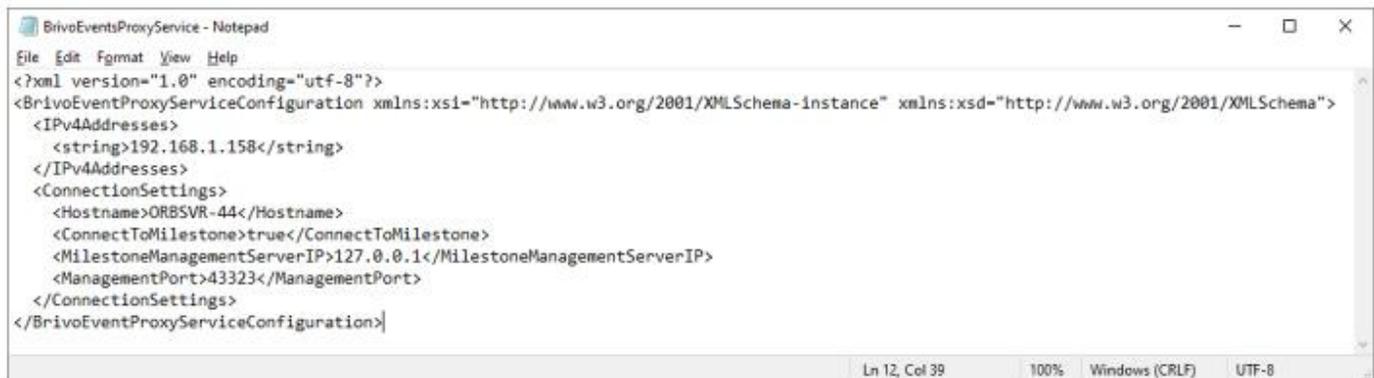
En el caso de las cuentas de servicio;

C:\Users\\AppData\Local\Brivo Events Proxy\Brivo Events Proxy

En el caso de las cuentas de servicios de red;

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Brivo Events Proxy\Brivo Events Proxy

BrivoEventsProxyService.xml



Lista de revisiones

Fecha	Versión	Autor	Descripción
10 de marzo de 2022	1.0	LMW	Borrador inicial
23 de marzo de 2022	1.1	LMW	Precios actualizados de EUR a USD