MAKE THE
WORLD SEE

Milestone Systems

Servidor XProtect® Mobile 2025 R1

Manual del administrador

milestone

Contenido

Copyright, marcas comerciales y exención de responsabilidad

Marcas comerciales

XProtect es una marca comercial registrada de Milestone Systems A/S.

Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation. App Store es una marca de servicios de Apple Inc. Android es una marca registrada de Google Inc.

Todas las demás marcas comerciales de este documento pertenecen a sus respectivos propietarios.

Limitación de responsabilidad

Este documento está únicamente concebido como información general, y se ha elaborado con la debida diligencia.

Cualquier daño que pueda derivarse del uso de esta información será responsabilidad del destinatario, y nada de lo aquí escrito podrá ser considerado como ningún tipo de garantía.

Milestone Systems A/S se reserva el derecho de hacer modificaciones sin notificación previa.

Todos los nombres de personas y organizaciones utilizados en los ejemplos de este documento son ficticios. Todo parecido con cualquier persona física, en vida o fallecida, o jurídica real es pura coincidencia y carece de intencionalidad alguna.

Este producto podrá hacer uso de software de terceros, para el que pueden aplicarse términos y condiciones específicos. En tal caso, encontrará más información en el archivo `3rd_party_software_terms_and_conditions.txt`, que se encuentra en la carpeta de instalación de su sistema Milestone.

Generalidades

Novedades

En servidor XProtect Mobile 2023 R3

Información de la conexión:

- Compruebe si el servidor móvil es accesible desde Internet. Consulte Información de la conexión en la página 14.

Alarmas:

- Agregue alarmas de alerta de emergencia para permitir que los usuarios reciban notificaciones de alarma del nivel de gravedad más alto en el cliente XProtect Mobile. Consulte Añadir alarmas de alerta de emergencia en la página 53.

En XProtect Mobile servidor 2023 R2

Marcadores y vídeos en directo compartidos:

- Para compartir marcadores y vídeo en directo en el cliente XProtect Mobile, deberá habilitar el cifrado en el servidor de gestión. Consulte Requisitos para usar Compartir en la página 10.

Notificaciones:

- Puede eliminar los datos de registro de dispositivos de la base de datos de VMS. Consulte Eliminado uno o todos los dispositivos registrados de la lista Dispositivos registrados en la página 40.

En XProtect Mobile Server 2022 R3

IDP externo:

- Ahora puede iniciar sesión en XProtect Web Client y el cliente de XProtect Mobile con un IDP externo. Consulte IDP externo y XProtect Mobile en la página 52

Gestión de dispositivos móviles (MDM):

- El cliente de XProtect Mobile ahora es compatible con gestión de dispositivos móviles (MDM). Con MDM, puede gestionar y proteger dispositivos, aplicaciones y datos desde una consola unificada. Para obtener más información, consulte Gestión de dispositivos móviles (MDM) en la página 50

Notificaciones push:

- Al habilitar esta característica, una advertencia le informa de que su sistema no puede cumplir con el RGPD.

En XProtect Mobile Server 2022 R2

Notificaciones:

- Las notificaciones están deshabilitadas de forma predeterminada

Instalación:

- Cuando instaleMobile Server, puede conectarse al servicio de vigilancia con un usuario básico

XProtect Mobile

XProtect Mobile consta de cinco componentes:

Cliente de XProtect Mobile

El cliente de XProtect Mobile es una aplicación de vigilancia móvil que puede instalar y utilizar en su dispositivo Android o Apple. Puede utilizar tantas instalaciones del cliente de XProtect Mobile según lo necesite.

XProtect Web Client

XProtect Web Client le permite ver vídeo en directo en su navegador web y le permite descargar grabaciones. XProtect Web Client se instala automáticamente junto con la instalación del servidor de XProtect Mobile.

Servidor XProtect Mobile

El servidor de XProtect Mobile maneja inicios de sesión en el sistema desde el cliente de XProtect Mobile o desde XProtect Web Client.

Un servidor de XProtect Mobile distribuye flujos de vídeo desde servidores de grabación al cliente XProtect Mobile o XProtect Web Client. Esto ofrece una configuración segura en la que los servidores de grabación nunca están conectados a Internet. Cuando un servidor de XProtect Mobile recibe flujos de vídeo de servidores de grabación, también maneja la conversión completa de códecs y formatos, lo que permite la transmisión de vídeo en el dispositivo móvil.

XProtect Mobile plug-in

El plug-in XProtect Mobile es parte del componente XProtectMobile Server. El plug-in XProtect Mobile le permite ver y administrar los servidores móviles en su sistema VMS desde el nodo **Servidores** en XProtect Management Client.

Instale el plug-in XProtect Mobileen cualquier ordenador con XProtect Management Client del que quiera gestionar los servidores móviles.

Mobile Server Manager

Utilice el Mobile Server Manager para obtener información sobre el servicio, compruebe el estado del Mobile Server servicio, ver registros o mensajes de estado, e iniciar y detener el servicio.

Este manual cubre el servidor de XProtect Mobile, el plug-in XProtect Mobile y Mobile Server Manager.

Requisitos y consideraciones

Antes de instalar el servidor XProtect Mobile

Para obtener información acerca de los requisitos de sistema para las distintas aplicaciones del VMS y componentes del sistema, vaya al sitio web de Milestone (https://www.milestonesys.com/systemrequirements/).

Milestone recomienda instalar el servidor de XProtect Mobile en un ordenador distinto. Antes de instalar y comenzar a usar el componente XProtect Mobile Server, asegúrese de lo siguiente:

- Ha configurado cámaras y vistas en XProtect Management Client.
- El ordenador servidor móvil resuelve los nombres de host de los equipos que ejecutan los otros componentes de servidor VMS.
- El ordenador del servidor de gestión resuelve el nombre de host del ordenador servidor móvil
- Tiene un VMS en ejecución instalado.
- Ha configurado al menos un usuario de VMS. Para conectarse al sistema de vigilancia, el cometido al que se añade este usuario requiere permisos para el servidor de gestión:
  - **Conectar**
  - **Leer**
  - **Editar**
- Si está actualizando su sistema, asegúrese de que la versión del plug-in XProtect Mobile coincida con la versión del servidor móvil. Es posible que su sistema no funcione correctamente si las versiones del plug-in y los servidores móviles no son idénticas.

Requisitos para configuración de notificaciones

Notificar a los usuarios cuando se produce un evento:

- Debe asociar una o más alarmas a uno o más eventos y reglas. Esto no es obligatorio para las notificaciones del sistema
- Tiene un acuerdo actualizado de Milestone Care™ con Milestone Systems
- Su sistema debe tener acceso a Internet

Para obtener más información, consulte:

Configurar notificaciones push en el servidor XProtect Mobile en la página 39

Pestaña Notificaciones en la página 27

Requisitos para configuración de Smart Connect

Para utilizar Smart Connect y verificar que ha configurado XProtect Mobile correctamente, debe tener:

- Una dirección IP para su servidor XProtect Mobile. La dirección puede ser estática o dinámica, pero normalmente es una buena idea utilizar direcciones IP estáticas
- Una licencia válida para Smart Connect
- Un acuerdo actualizado de Milestone Care™ con Milestone Systems

Requisitos para la configuración de la verificación en dos pasos del usuario

Para configurar los usuarios para la verificación en dos pasos por correo electrónico

- Ha instalado un servidor SMTP
- Ha añadido usuarios y grupos a su sistema XProtect en el Management Client en el nodo **Cometidos** del panel de **Navegación del sitio**. En el cometido correspondiente, seleccione la pestaña **Usuarios y grupos**.
- Si ha actualizado su sistema desde una versión anterior de XProtect, debe reiniciar el servicio para habilitar la función de verificación en dos pasosMobile Server

Para obtener más información, consulte:

Configurar usuarios para la doble verificación de acceso por correo electrónico en la página 48

Pestaña Doble verificación de acceso en la página 28

Requisitos para la configuración de la transmisión push de vídeo

Para transmitir vídeo de una cámara de dispositivo móvil al sistema de vigilancia XProtect, debe tener:

- Una licencia de dispositivo para cada canal que utilice.

Requisitos para transmisión en directo

XProtect Mobile admite la transmisión directa en directo. Para utilizar la transmisión en directo en XProtect Web Client y el cliente de XProtect Mobile, debe tener la siguiente configuración de cámara:

- Las cámaras deben admitir el códec H.264 o el códec H.265.

  XProtect Web Client solo es compatible con H.264.

- Es recomendable que establezca el valor del **tamaño de GOP** en **1 segundo**, y el ajuste de **FPS** debe tener un valor que sea superior a **10** FPS.

Requisitos para usar Compartir

Los usuarios pueden compartir marcadores y vídeos en directo mientras utilizan la aplicación cliente XProtect Mobile. Estas funcionalidades estarán disponibles una vez que haya:

- Ha habilitado el cifrado en el servidor de gestión.

Instalación

Instalar el servidor XProtect Mobile

Una vez instalado el servidor de XProtect Mobile, puede usar el cliente XProtect Mobile y XProtect Web Client con su sistema. Para recudir el uso global de los recursos del sistema en el ordenador en el que se ejecuta el servidor de gestión, instale el servidor de XProtect Mobile en un ordenador separado.

El servidor de gestión tiene una página web de instalación pública integrada. Desde esta página web, los administradores y los usuarios finales pueden descargar e instalar los componentes requeridos del sistema XProtect desde el servidor de gestión o cualquier otro ordenador en el sistema.

> XProtect Mobile el servidor se instala automáticamente al instalar la opción "un solo ordenador".

Descargue el instalador de servidor XProtect Mobile

1. Introduzca la siguiente URL en su navegador: *http://[dirección del servidor de gestión]/instalación/administrador* donde la [dirección del servidor de gestión] es la dirección IP o el nombre host del servidor de gestión.
2. Seleccione **Todos los idiomas** para el XProtect Mobile instalador del servidor.

Instalar el servidor XProtect Mobile

1. Ejecute el archivo descargado. A continuación, seleccione **Sí** para ver todas las advertencias.
2. Seleccione un idioma para el instalador. A continuación, seleccione **Continuar**.
3. Lea y acepte los términos del acuerdo de licencia. A continuación, seleccione **Continuar**.
4. Seleccione el tipo de instalación:
   - Haga clic en **Típica** para instalar el servidor de XProtect Mobile y el plug-in
   - Seleccione **Personalizado** para instalar solo el servidor o solo el plug-in. Por ejemplo, instalar únicamente el plug-in resulta útil si quiere utilizar Management Client para gestionar servidores de XProtect Mobile, pero no necesita un servidor de XProtect Mobile en ese ordenador

     > XProtect Mobile el plug-in se necesita en el ordenador en el que se ejecuta Management Client para gestionar servidores de XProtect Mobile en Management Client.

5. Solo para instalación personalizada: Seleccione los componentes que quiere que estén instalados. A continuación, seleccione **Continuar**.
6. Seleccione la cuenta de servicio para el servidor móvil. A continuación, seleccione **Continuar**.

   Para cambiar o editar las credenciales de la cuenta de servicio posteriormente, debe volver a instalar el servidor móvil.

7. Solo para instalación personalizada: Inicie sesión con una cuenta de usuario de VMS existente cuando se conecte al sistema de vigilancia:
   - **Cuenta de servicio** es la cuenta que seleccionó en el paso 8. Para conectarse utilizando esta cuenta, asegúrese de que la cuenta de servicio es un miembro del dominio al que tiene acceso el servidor de gestión
   - **Usuario básico.** Utilice un usuario básico cuando la cuenta de servicio no es miembro de un dominio al que tiene acceso el servidor de gestión.

   Para cambiar o editar las credenciales de la cuenta de servicio o del usuario básico posteriormente, deberá volver a instalar el servidor móvil.

   Seleccione **Continuar**.
8. En el campo **URL del servidor**, rellene la dirección del servidor de gestión principal.

   Solo para instalación personalizada: Especifique los puertos de conexión para la comunicación con el servidor móvil. A continuación, seleccione **Continuar**. En una instalación típica, los puertos de conexión obtienen los números de puerto predeterminados (8081 para el puerto HTTP y 8082 para el puerto HTTPS).
9. En la página **Asignar una contraseña de protección de datos del servidor móvil**, introduzca una contraseña para cifrar sus investigaciones. Como administrador del sistema, tendrá que introducir esta contraseña para acceder a los datos del servidor móvil en caso de recuperación del sistema o cuando amplíe su sistema con servidores móviles adicionales.

   Debe guardar esta contraseña y mantenerla a salvo. No hacerlo puede comprometer su habilidad para recuperar datos del servidor móvil.

   Si no desea que sus investigaciones estén protegidas por una contraseña, seleccione **Elijo no utilizar una contraseña de protección de datos del servidor móvil y entiendo que las investigaciones no estarán cifradas**.

   Haga clic en **Continuar**.
10. Especifique el cifrado del servidor móvil. A continuación, seleccione **Continuar**.

En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

- Entre los servidores móviles y los servidores de grabación, los colectores de datos y el servidor de gestión. Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado
- Entre los servidores móviles y los clientes. Para habilitar el cifrado entre el servidor móvil y los clientes que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión**, seleccione un certificado

> Si no habilita el cifrado, algunas funciones de algunos clientes no estarán disponibles. Si desea más información, consulte Requisitos de cifrado del servidor móvil para clientes.

Para obtener más información sobre cómo establecer una comunicación segura en su sistema, consulte:

- Cifrado de datos del servidor móvil (explicación)
- La guía Milestone sobre certificados

También puede activar el cifrado una vez completada la instalación desde el icono de la bandeja Mobile Server Manager en la barra de tareas de su sistema operativo. (consulte Habilitar cifrado en el servidor móvil en la página 34).

11. Seleccione la ubicación del archivo y el idioma del producto, y, a continuación, seleccione **Instalar**.

    Cuando la instalación finaliza, aparece una lista de componentes instalados correctamente.

Configuración

Ajustes del servidor móvil

En Management Client, puede configurar y editar una lista de ajustes del servidor de XProtect Mobile. Puede acceder a estos ajustes en la barra de tareas inferior de la sección **Propiedades** del servidor móvil. Desde aquí, puede:

- Habilitar o deshabilitar configuración general de características del servidor (consulte Pestaña general en la página 15)
- Configurar ajustes de conectividad del servidor (consulte Pestaña Conectividad en la página 18)
- Configure la función Smart Connect (consulte Pestaña Conectividad en la página 18)
- Consulte el estado actual del servidor y la lista de usuarios activos (consulte Pestaña Estado del servidor en la página 20)
- Configurar los parámetros de rendimiento para habilitar la transmisión directa y la transmisión adaptativa, o para establecer limitaciones al flujo de vídeo transcodificado (consulte Pestaña Rendimiento en la página 21)
- Configurar ajustes de investigaciones (consulte Pestaña Investigaciones en la página 24)
- Configurar los ajustes de transmisión push de vídeo (consulte Pestaña Transmisión push de vídeo en la página 26)
- Configurar, activar y desactivar notificaciones del sistema, así como notificaciones push (consulte Pestaña Notificaciones en la página 27)
- Habilitar y configurar un paso adicional de inicio de sesión para usuarios (consulte Pestaña Doble verificación de acceso en la página 28)

Información de la conexión

Las siguientes tablas describen los estados y mensajes del servidor móvil que están visibles en todas las pestañas.

El servidor es accesible por internet

Color	Estado	Descripción
Naranja	N/D	El servidor móvil no se ha configurado para ser accesible desde fuera de la red local.

Color	Estado	Descripción
Rojo	No	Los usuarios del cliente XProtect Web Client y XProtect Mobile no pueden conectarse al servidor móvil desde Internet.
Verde	Sí	Los usuarios del cliente XProtect Web Client y XProtect Mobile pueden conectarse al servidor móvil desde Internet.

Conexión al servidor

Color	Mensaje	Descripción
Naranja	**Certificado HTTPS no válido**	El plug-in XProtect Mobile no reconoce el certificado del servidor móvil.
Naranja	**HTTP/HTTPS inalcanzable**	XProtect Management Client no puede acceder al servidor móvil.
Rojo	**HTTP/HTTPS no conectado**	XProtect Management Client ha detectado el servidor móvil, pero no puede conectarse a él.
Verde	**HTTP/HTTPS**	XProtect Management Client ha establecido una conexión con el servidor móvil.

Pestaña general

La siguiente tabla describe los ajustes en esta pestaña.

General

Nombre	Descripción
Nombre del servidor	Introduzca el nombre del servidor de XProtect Mobile.

Nombre	Descripción
Descripción	Introduzca una descripción opcional del servidor de XProtect Mobile.
Servidor móvil	Consulte el nombre del servidor de XProtect Mobile seleccionado actualmente.

Funciones

La tabla siguiente describe cómo controlar la disponibilidad de características de XProtect Mobile.

Nombre	Descripción
Habilitar XProtect Web Client	Habilite el acceso a XProtect Web Client. Esta característica está habilitada de forma predeterminada.
Habilita la vista Todas las cámaras para el XProtect Mobilecliente	Esta vista muestra todas las cámaras que un usuario tiene permiso para ver en un servidor de grabación. Esta característica está habilitada de forma predeterminada.
Habilitar marcadores	Habilite la característica de marcadores para localizar rápidamente secuencias de vídeo en el cliente de XProtect Mobile y en XProtect Web Client. Esta característica está habilitada de forma predeterminada.
Activar acciones (salidas y eventos)	Habilite el acceso a acciones en el cliente de XProtect Mobile y en XProtect Web Client. Esta característica está habilitada de forma predeterminada. Si deshabilita esta característica, los usuarios clientes no son capaces de ver salidas y eventos, incluso en el caso de que estén configurados correctamente.
Habilitar audio entrante	Habilite la característica de audio entrante en XProtect Web Client y en el cliente de XProtect Mobile. Esta característica está habilitada de forma predeterminada.
Habilitar pulsar para hablar	Habilite la función pulsar para hablar (push-to-talk, PTT) en XProtect Web Client y en e cliente de XProtect Mobile. Esta característica está habilitada

Nombre	Descripción
	de forma predeterminada.
Denegar al rol de administrador integrado acceso al servidor de XProtect Mobile	Habilite esto para impedir que los usuarios asignados al rol integrado de administradores accedan al vídeo en el cliente de XProtect Mobile o en XProtect Web Client.

Configuración de registro

Puede utilizar la información de los ajustes del registro.

Nombre	Descripción
Ubicación del archivo de registro	Consulte dónde guardar los archivos de registro el sistema.
Mantener registros durante	Consulte el número de días que se deben conservar los registros. El valor predeterminado es tres días.

Copia de seguridad de configuración

Si su sistema tiene múltiples servidores de XProtect Mobile, puede utilizar la función de copia de seguridad para exportar los ajustes actuales e importarlos a otros servidores de XProtect Mobile.

Nombre	Descripción
Importar	Importe un archivo XML con una configuración del servidor de XProtect Mobile.
Exportar	Exporte su configuración del servidor de XProtect Mobile. Su sistema almacena la configuración en un archivo XML.

Pestaña Conectividad

Los ajustes en la pestaña **Conectividad** se usan en las siguientes tareas:

- Configurar ajustes de conexión en la página 37
- Enviar un mensaje de correo electrónico a los usuarios en la página 38
- Habilite conexiones en redes complejas en la página 37
- Habilite la detección Universal Plug and Play en su router en la página 37

Si desea más información, consulte Smart Connect en la página 36.

> Puede configurar cómo el cliente de XProtect Mobile y los usuarios de XProtect Web Client deben conectarse con el servidor de XProtect Mobile cuando se abre el **Server Configurator** durante la instalación haciendo clic en el icono de la bandeja de Mobile Server Manager después de la instalación. El tipo de conexión puede ser HTTPS o HTTP. Si desea más información, consulte Habilitar cifrado en el servidor móvil en la página 34.

General

Nombre	Descripción
Tiempo de espera del cliente	Establezca un intervalo de tiempo para la frecuencia con la que el cliente de XProtect Mobile y XProtect Web Client deben indicar al servidor de XProtect Mobile que están activos y en funcionamiento. El valor predeterminado es 30 segundos. Milestone recomienda que no aumente el intervalo de tiempo.
Activar detección de UPnP	Esto hace que el servidor de XProtect Mobile sea detectable en la red mediante los protocolos UPnP. El cliente de XProtect Mobile tiene una funcionalidad de escaneado para encontrar servidores de XProtect Mobile basados en UPnP.
Activar el mapeo de puertos automático	Cuando el servidor de XProtect Mobile se instala detrás del cortafuegos, se requiere una asignación de puertos en el router, de modo que los clientes aún pueden acceder al servidor desde Internet. La opción **Habilitar asignación automática de puertos** habilita el servidor de XProtect Mobile para que haga esta asignación de puertos por sí mismo, siempre que el router esté configurado para ello.

Nombre	Descripción
Habilitar conexión inteligente	La conexión inteligente le habilita para verificar que ha configurado el servidor XProtect Mobile correctamente sin iniciar sesión con un dispositivo móvil o una tableta para hacer la verificación. También simplifica el proceso de conexión para los usuarios clientes.

Acceso a Internet

Nombre	Descripción
Configurar el acceso a Internet personalizado	Proporcione la **dirección IP o el nombre de host** y el número de puerto que usar para la conexión. Por ejemplo, podría hacer esto si su router no es compatible con UPnP o si tiene una cadena de routers.
• **HTTP** • **HTTPS**	Seleccione el tipo de conexión.
Seleccione para recuperar la dirección IP dinámicamente	Seleccione la casilla de verificación si sus direcciones IP cambian con frecuencia.
Utilizar solo la dirección URL configurada	Seleccione la casilla de verificación para conectar con el servidor móvil con una dirección IP especificada de forma personalizada o solo con el nombre de host.
Direcciones del servidor	Enumera todas las direcciones URL que están conectadas al servidor móvil.

Notificación de Smart Connect

Nombre	Descripción
Invitación por correo electrónico a	Introduzca la dirección de correo electrónico para el destinatario de la notificación de Smart Connect.
Idioma del correo electrónico	Especifique el idioma utilizado en el correo electrónico.
Token de Smart Connect	Un identificador único que pueden usar los dispositivos móviles para conectarse al servidor XProtect Mobile.
Enlace a Smart Connect	Un vínculo que pueden usar los usuarios de dispositivos móviles para conectarse al servidor de XProtect Mobile.

Pestaña Estado del servidor

Consulte los detalles del estado para el servidor de XProtect Mobile. Los detalles son de solo lectura:

Nombre	Descripción
Servidor activo desde	Muestra la fecha y la hora a la que se inició por última vez el servidor de XProtect Mobile.
% uso de CPU	Muestra el uso actual de la CPU en el servidor móvil.
Ancho de banda externo:	Muestra el ancho de banda actual en uso entre el cliente de XProtect Mobile o XProtect Web Client y el servidor móvil.

Usuarios activos

Consulte los detalles del estado del cliente de XProtect Mobile o XProtect Web Client actualmente conectado al servidor de XProtect Mobile.

Nombre	Descripción
Nombre de usuario	Muestra el nombre de usuario para cada cliente de XProtect Mobile o usuario de XProtect Web Client conectado al servidor móvil.
Estado	Muestra la relación actual entre el servido de XProtect Mobile y el cliente de XProtect Mobile o el usuario de XProtect Web Client en cuestión. Los estados posibles son: • **Conectado**: Un estado inicial en el que los clientes y el servidor intercambian claves y credenciales de cifrado • **Sesión iniciada**: El cliente de XProtect Mobile o el usuario de XProtect Web Client han iniciado sesión en el sistema XProtect
Uso de ancho de banda del vídeo (kB/s)	Muestra el ancho de banda total de los flujos de vídeo que están actualmente abiertos para cada cliente de XProtect Mobile o usuario de XProtect Web Client.
Uso de ancho de banda del audio (kB/s)	Muestra el ancho de banda total de los flujos de audio que están actualmente abiertos para cada usuario de XProtect Web Client.
Flujos de vídeo transcodificados	Muestra el número total de flujos de vídeo transcodificados que están actualmente abiertos para cada cliente de XProtect Mobile o usuario de XProtect Web Client.
Transmisiones de vídeo directo	Muestra el número total de flujos de vídeo directo que están actualmente abiertos para cada cliente de XProtect Mobile o usuario de XProtect Web Client (únicamente para XProtect Expert y XProtect Corporate).
Flujos de audio transcodificados	Muestra el número total de flujos de audio transcodificados que están actualmente abiertos para cada usuario de XProtect Web Client.

Pestaña Rendimiento

En la pestaña **Rendimiento**, puede establecer los siguientes y limitaciones en el rendimiento del servidor de XProtect Mobile:

Ajustes de transmisión de vídeo (únicamente XProtect Expert y XProtect Corporate)

Nombre	Descripción
Activar la transmisión directa	Habilite las transmisión directa en XProtect Web Client y el cliente de XProtect Mobile (para XProtect Expert y XProtect Corporate solamente). Esta característica está habilitada de forma predeterminada.
Activar streaming adaptable	Habilite la transmisión adaptativa en XProtect Web Client y en el cliente de XProtect Mobile (para XProtect Expert y XProtect Corporate únicamente). Esta característica está habilitada de forma predeterminada.
Modos de transmisión	Después de habilitar la función de transmisión adaptativa, puede seleccionar el tipo de modo de transmisión de la lista: • **Optimizar calidad de vídeo (predeterminado)**: selecciona el flujo con la resolución más baja disponible que es igual o superior a la resolución solicitada • **Optimizar rendimiento del servidor** - reduce la resolución solicitada y, a continuación, selecciona el flujo con la resolución más baja disponible que sea igual o superior a la solicitud reducida • **Optimizar resolución para ancho de banda bajo** - selecciona el flujo con la resolución más baja disponible (recomendado si utiliza 3G o una red inestable)

Limitaciones de flujos de vídeo transcodificados

Nivel 1

Nivel 1 es la limitación predeterminada colocada en el servidor de XProtect Mobile. Cualquier limitación que establezca aquí siempre se aplicará a los flujos de vídeo transcodificados de XProtect Mobile.

Nombre	Descripción
Nivel 1	Seleccione la casilla de verificación para habilitar el primer nivel de limitaciones al rendimiento del servidor de XProtect Mobile.

Nombre	Descripción
FPS máx.	Establezca un límite para el número máximo de imágenes por segundo (FPS) para enviar desde el servidor XProtect Mobile a los clientes.
Resolución de imagen máx.	Establezca un límite para la resolución de imagen para enviar desde el servidor de XProtect Mobile a los clientes.

Nivel 2

Si quiere forzar un nivel distinto de limitaciones que el predeterminado en **Nivel 1**, seleccione la casilla de verificación **Nivel 2**. No puede establecer ningún ajuste en un valor por encima del valor en el que los ha establecido ya en el primer nivel. Si, por ejemplo, quiere establecer FPS máx. en 45 en **Nivel 1**, puede establecer FPS máx. en **Nivel 2** solo en 44 o por debajo.

Nombre	Descripción
Nivel 2	Seleccione la casilla de verificación para habilitar el segundo nivel de limitaciones al rendimiento del servidor de XProtect Mobile.
Límite del CPU	Establezca un umbral para la carga de la CPU en el servidor de XProtect Mobile antes de que el sistema fuerce limitaciones en el flujo de vídeo.
Límite de ancho de banda	Establezca un umbral para la carga del ancho de banda en el servidor de XProtect Mobile antes de que el sistema fuerce limitaciones en el flujo de vídeo.
FPS máx.	Establezca un límite para el número máximo de imágenes por segundo (FPS) para enviar desde el servidor XProtect Mobile a los clientes.
Resolución de imagen máx.	Establezca un límite para la resolución de imagen para enviar desde el servidor de XProtect Mobile a los clientes.

Nivel 3

También puede seleccionar una casilla de verificación de **Nivel 3** para crear un tercer nivel para limitaciones. No puede establecer ningún ajuste en un valor por encima del valor en el que los ha establecido ya en **Nivel 1** y **Nivel 2**. Si, por ejemplo, establece el valor de **FPS máx.** en 45 en **Nivel 1** y en Nivel 32 en **Nivel 2**, puede establecer el valor de **FPS máx.** en **Nivel 3** solo en 31 o menos.

Nombre	Descripción
Nivel 3	Seleccione la casilla de verificación para habilitar el tercer nivel de limitaciones al rendimiento del servidor de XProtect Mobile.
Límite del CPU	Establezca un umbral para la carga de la CPU en el servidor de XProtect Mobile antes de que el sistema fuerce limitaciones en el flujo de vídeo.
Límite de ancho de banda	Establezca un umbral para la carga del ancho de banda en el servidor de XProtect Mobile antes de que el sistema fuerce limitaciones en el flujo de vídeo.
FPS máx.	Establezca un límite para los fotogramas por segundo (FPS) para enviar desde el servidor de XProtect Mobile a los clientes.
Resolución de imagen máx.	Establezca un límite para la resolución de imagen para enviar desde el servidor de XProtect Mobile a los clientes.

El sistema no cambia instantáneamente de un nivel a otro. Si su umbral de CPU o de ancho se marcha a menos del cinco por ciento por encima o por debajo de los niveles indicados, el nivel actual permanece en uso.

Pestaña Investigaciones

Configuración de notificación

Puede habilitar investigaciones para que las personas puedan utilizar el cliente de XProtect Mobile o XProtect Web Client para:

- Acceder al vídeo grabado
- Investigar incidentes
- Preparar y descargar evidencia de vídeo

Nombre	Descripción
Habilitar	Seleccione esta casilla de verificación para permitir a los usuarios crear

Nombre	Descripción
investigaciones	investigaciones.
Carpeta de investigaciones	Muestra dónde se guardan sus exportaciones de vídeo en su disco duro.
Ver investigaciones realizadas por otros usuarios	Seleccione esta casilla de verificación para permitir que los usuarios accedan a investigaciones que no crearon.
Habilitar el límite de tamaño de la carpeta de investigaciones	Seleccione esta casilla de verificación para establecer un límite de tamaño en la carpeta de investigaciones e introduzca el número máximo de megabytes que puede contener la carpeta de investigaciones. El tamaño predeterminado es 2000 MB.
Habilitar el periodo de retención de investigación	Seleccione esta casilla de verificación para establecer un tiempo de retención para las investigaciones. De forma predeterminada, el tiempo de retención es de siete días.
Formatos de exportación	Seleccione la casilla de verificación del formato de exportación que quiera usar. Los formatos de exportación disponibles son: • **Formato AVI** • **XProtect formato** • **Formato MKV** De forma predeterminada, las casillas de verificación están desmarcadas.
Incluir marcas de tiempo para exportaciones AVI	Seleccione esta casilla de verificación para incluir la fecha y la hora a las que descargó el archivo AVI.
Códec utilizado para exportaciones de AVI	Seleccione el formato de compresión que usar al preparar paquetes AVI para descargar. Los códecs entre los que puede elegir pueden diferir dependiendo de su sistema operativo. Si no ve el códec que quiere, puede añadirlo a la lista instalándolo en el

Nombre	Descripción
	ordenador en el que se está ejecutando el XProtect Mobile.
Bit de audio utilizado para exportaciones de AVI	Seleccione de la lista la velocidad de bits de audio apropiada cuando el audio se incluya en la exportación de vídeo. El valor predeterminado es 160000 Hz.

Investigaciones

Nombre	Descripción
Investigaciones	Enumera las investigaciones que se han configurado hasta ahora en el sistema. Utilice los botones **Eliminar** o **Eliminar todo** si ya no quiere conservar una investigación. Esto puede resultar útil si, por ejemplo, quiere hacer que haya más espacio disponible en el servidor.
Detalles de la investigación	Para eliminar archivos de vídeo individuales que se exportaron para una investigación, pero conservar la investigación, seleccione la investigación en la lista. En el grupo **Detalles de las investigaciones**, seleccionar el icono eliminar a la derecha de los campos **XProtect**, **AVI** o **MKV** para exportaciones.

Pestaña Transmisión push de vídeo

Puede especificar los siguientes ajustes si habilita la transmisión push de vídeo:

Nombre	Descripción
Vídeo push	Habilite la transmisión push de vídeo en el servidor móvil.
Número de canales	Muestra el número de canales de transmisión push de vídeo en su sistema XProtect.

Nombre	Descripción
Canal	Muestra el número de canal para el canal relevante. No editable.
Puerto	Número de puerto para el canal de transmisión push de vídeo relevante.
Dirección MAC	Dirección MAC para el canal relevante de envío push de vídeo.
Nombre de usuario	Introduzca el nombre de usuario asociado al canal de transmisión push de vídeo relevante.
Nombre de cámara	Muestra el nombre de la cámara, si la cámara se ha identificado.

Una vez completados todos los pasos necesarios (consulte Configurar vídeo transmisión push de vídeo para transmitir vídeo en la página 43), seleccione **Buscar cámaras** para buscar la cámara relevante.

Pestaña Notificaciones

Utilice la pestaña **Notificaciones** para activar o desactivar las notificaciones del sistema y las notificaciones push.

De forma predeterminada, las notificaciones están deshabilitadas.

Si activa las notificaciones y ha configurado una o más alarmas y eventos, XProtect Mobile notifica a los usuarios cuándo se produce un evento. Cuando se abre la aplicación, las notificaciones se entregan en XProtect Mobile en el dispositivo móvil. Las notificaciones push notifican a los usuarios que no tienen el XProtect Mobile abierto. Estas notificaciones se entregan en el dispositivo móvil.

Para obtener más información, consulte: Habilitar el envío de notificaciones push a dispositivos específicos o móviles a todos los dispositivos móviles en la página 40

En la siguiente tabla se describen los ajustes en esta pestaña.

Nombre	Descripción
Notificaciones	Seleccione esta casilla de verificación para activar las notificaciones.
Mantener el	Seleccione esta casilla de verificación para almacenar información sobre los

Nombre	Descripción
registro del dispositivo	dispositivos y usuarios que se conectan a este servidor. El sistema envía notificaciones a estos dispositivos. Si desactiva esta casilla de verificación, también borra la lista de dispositivos. Para usuarios que quieren empezar a recibir notificaciones de nuevo, debe seleccionar la casilla de verificación, y los usuarios deben volver a conectar sus dispositivos al servidor.

Dispositivos registrados

Nombre	Descripción
Habilitado	Seleccione esta casilla de verificación para empezar a enviar notificaciones al dispositivo.
Nombre de dispositivo	Una lista de los dispositivos móviles que se han conectado a este servidor. Puede iniciar o detener el envío de notificaciones para dispositivos específicos seleccionando o desactivando la casilla de verificación **Habilitado**.
Usuario	Nombre del usuario que recibirá notificaciones.

Pestaña Doble verificación de acceso

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Utilice la pestaña **Verificación en dos pasos** para habilitar y especificar un paso de inicio de sesión adicional en los usuarios de:

- XProtect Mobile aplicación en sus dispositivos móviles iOS o Android
- XProtect Web Client

El primer tipo de verificación es una contraseña. El segundo tipo es un código de verificación, que puede configurar para que se envíe al usuario por correo electrónico.

Si desea más información, consulte Configurar usuarios para la doble verificación de acceso por correo electrónico en la página 48.

Las tablas siguientes describen los ajustes para esta pestaña.

Ajustes del proveedor > **Correo electrónico**

Nombre	Descripción
Servidor SMTP	Introduzca la dirección IP o el nombre de host del servidor del protocolo simple de transferencia de correo simple (simple mail transfer protocol, SMTP) para correos electrónicos con verificación de dos pasos.
Puerto del servidor SMTP	Especifique el puerto del servidor SMTP para el envío de correos electrónicos. El puerto predeterminado es 25 sin SSL y 465 con SSL.
Usar SSL	Seleccione la casilla de verificación si su servidor SMTP admite el cifrado SSL.
Nombre de usuario	Especifique el nombre de usuario para iniciar sesión en el servidor SMTP.
Contraseña	Especifique la contraseña para iniciar sesión en el servidor SMTP.
Usar la autenticación de contraseña segura (SPA)	Seleccione esta casilla de verificación si su servidor SMTP admite SPA.
Dirección de correo electrónico del remitente	Especifique la dirección de correo electrónico para el envío de códigos de verificación.
Asunto del correo electrónico	Especifique el título del asunto para el correo electrónico. Ejemplo: Su código de verificación en dos pasos.
Texto del correo electrónico	Introduzca el mensaje que quiere enviar. Ejemplo: Su código es {0}. Si olvida incluir la variable {0}, el código se añade al final del texto de forma predeterminada.

Configuración del código de verificación

Nombre	Descripción
Tiempo de espera de reconexión (0-30 minutos)	Especifique el periodo dentro del que los usuarios clientes de XProtect Mobile no tienen que volver a verificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El periodo por defecto es de tres minutos. Estos ajustes no se aplican a XProtect Web Client.
El código caduca tras (1-10 minutos)	Especifica el periodo en el que el usuario puede utilizar el código de verificación recibido. Después de este periodo, el código no es válido y el usuario tiene que solicitar un nuevo código. El periodo por defecto es de cinco minutos.
Intentos de entrada de código (1-10 intentos)	Especifique el número máximo de intentos de entrada de código antes de que el código proporcionado deje de ser válido. El número por defecto es tres.
Longitud del código (4-6 caracteres)	Especifica el número de caracteres del código. La longitud por defecto es seis.
Composición de código	Especifique la complejidad del código que quiere que genere el sistema. Puede seleccionar entre: • **Caracteres latinos en mayúscula (A-Z)** • **Minúscula latina(a-z)** • **Dígitos (0-9)** • **Caracteres especiales (!@#...)**

Configuración del usuario

Nombre	Descripción
Usuarios y	Enumera los usuarios y los grupos añadidos al sistema XProtect.

Nombre	Descripción
grupos	Si se configura un grupo en Active Directory, el servidor móvil utiliza detalles, como la dirección de corre electrónico, de Active Directory.  Los grupos de Windows no admiten la doble verificación de acceso.
Método de verificación	Seleccione un ajuste de verificación para cada usuario o grupo. Puede seleccionar entre: • **Sin inicio de sesión**: el usuario no puede iniciar sesión • **Sin verificación en dos pasos**: el usuario debe introducir el nombre de usuario y la contraseña • **Correo electrónico**: el usuario debe introducir un código de verificación además del nombre de usuario y la contraseña
Detalles del usuario	Introduzca la dirección de correo electrónico en la que cada usuario recibirá códigos.

Transmisión en directo

XProtect Mobile admite la transmisión directa en directo.

La transmisión en directo es una tecnología de transmisión de vídeo que transfiere vídeo desde un sistema XProtect a los clientes directamente en códec H.264, que es compatible con la mayoría de cámaras IP modernas. Los clientes de XProtect® Mobile también admiten el uso del códec H.265. La transmisión en directo no requiere ninguna transcodificación y, por tanto, elimina parte del estrés en el sistema XProtect.

La tecnología de transmisión en directo es en contraste al ajuste de transcodificación en XProtect, donde un sistema de XProtect decodifica vídeo desde el códec que se utiliza en la cámara en archivos JPEG. Habilitar la característica provoca un menor uso de la CPU para la misma configuración de cámaras y flujos de vídeo. La transmisión en directo también aumenta el rendimiento de la transmisión para el mismo hardware: hasta cinco veces más transmisiones de vídeo simultáneas comparado con la transcodificación.

También puede utilizar la función de transmisión en directo para transferir vídeo desde cámaras compatibles con el códec H.265 directamente al cliente XProtect Mobile.

En Management Client, puede habilitar o deshabilitar flujos directos para clientes (consulte Ajustes del servidor móvil en la página 14).

El flujo de vídeo pasa de transmisión en directo a transcodificación si:

- La función de transmisión en directo se ha deshabilitado en Management Client, o los requisitos no se han cumplido (consulte Requisitos para transmisión en directo en la página 9)
- El códec de la cámara de transmisión es distinto de H.264 (para todos los clientes) o H.265 (únicamente para el cliente de XProtect Mobile)
- El vídeo no puede reproducirse durante más de diez segundos
- La velocidad de fotogramas de la cámara que transmite se establece en un fotograma por segundo (1 FPS)
- Se ha perdido la conexión con el servidor o con la cámara
- La función de enmascaramiento de la privacidad se emplea durante el vídeo en directo

Streaming adaptativo

XProtect Mobile admite la transmisión adaptativa en modo en directo.

Las transmisiones adaptativas son útiles cuando se ven varios flujos de vídeo en directo en la misma vista de cámaras. La característica optimiza el rendimiento del servidor de XProtect Mobile y mejora la capacidad de decodificación y el rendimiento de los dispositivos que están ejecutando el cliente de XProtect Mobile y XProtect Web Client.

Para aprovecharse de la transmisión adaptativa, sus cámaras deben tener múltiples flujos definidos con distintas resoluciones. En este caso, la característica le permite:

- Optimizar calidad de vídeo: selecciona el flujo con la resolución más baja disponible que es igual o superior a la resolución solicitada.
- Optimizar rendimiento del servidor: reduce la resolución solicitada y, a continuación, selecciona el flujo con la resolución más baja disponible que sea igual o superior a la solicitud reducida.
- Optimizar resolución para ancho de banda bajo: seleccione el flujo con la resolución más baja disponible (recomendado si utiliza 3G o una red inestable).

Al aplicar el zoom, el flujo de vídeo seleccionado siempre es uno con la máxima resolución disponible.

El uso de ancho de banda a menudo se reduce cuando se reduce la resolución de los flujos requeridos. El uso del ancho de banda también depende de otros ajustes en las configuraciones de los flujos definidos.

Puede habilitar o deshabilitar la transmisión adaptativa y establecer el modo de transmisión preferido de la característica en la **pestaña Rendimiento** de los ajustes del servidor móvil en Management Client (consulte Ajustes del servidor móvil en la página 14).

Cifrado de datos del servidor móvil (explicación)

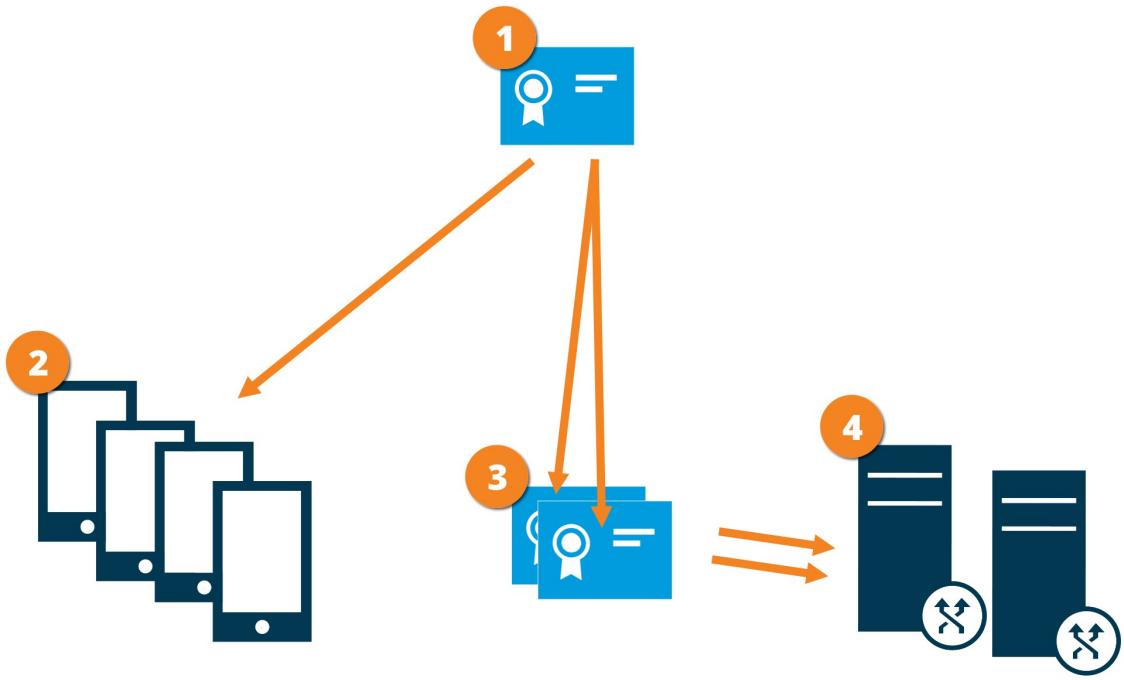
Por motivos de seguridad, Milestone recomienda utilizar una comunicación segura entre el servidor móvil y los clientes al gestionar la configuración de las cuentas de usuario.

Si no habilita el cifrado y utiliza una conexión HTTP, la función pulsar para hablar en XProtect Web Client no estará disponible.

En el VMS XProtect, el cifrado se habilita o deshabilita por servidor móvil. Al activar el cifrado en un servidor móvil, tendrá la opción de utilizar la comunicación cifrada con todos los clientes, servicios e integraciones que recuperen flujos de datos.

Distribución de certificados para servidores móviles

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuye los certificados en el VMS XProtect para asegurar la comunicación con el servidor móvil.



❶ Un certificado CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor móvil) como la parte que verifica el certificado (todos los clientes)

❷ El certificado CA debe ser de confianza en todos los clientes. De este modo, los clientes pueden verificar la validez de los certificados emitidos por la CA

❸ El certificado CA se utiliza para establecer una conexión segura entre el servidor móvil y los clientes y servicios

❹ El certificado CA debe estar instalado en el ordenador en el que se está ejecutando el servidor móvil

Requisitos para el certificado CA:

- El nombre de host del servidor móvil debe estar incluido en el certificado, ya sea como sujeto/propietario o en la lista de nombres DNS a los que se emite el certificado
- El certificado debe ser de confianza en todos los dispositivos que ejecuten servicios que recuperen flujos de datos del servidor móvil
- La cuenta de servicio que ejecuta el servidor móvil debe tener acceso a la clave privada del certificado CA

Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones de XProtect VMS.

Habilitar cifrado en el servidor móvil

Para usar un protocolo HTTPS con el fin de establecer una conexión segura entre el servidor móvil y los clientes y servicios, debe aplicar un certificado válido en el servidor. El certificado confirma que el titular del certificado está autorizado a establecer conexiones seguras.

Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones de XProtect VMS.

Al configurar el cifrado para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si el cifrado está deshabilitado, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Los certificados emitidos por la AC (Autoridad Certificadora) tienen una cadena de certificados y en la raíz de esa cadena está el certificado raíz de la AC. Cuando un dispositivo o navegador ve este certificado, compara su certificado raíz con los preinstalados en el SO (Android, iOS, Windows, etc.). Si el certificado raíz está recogido en la lista de certificados preinstalados, entonces el SO garantiza al usuario que la conexión con el servidor es lo bastante segura. Estos certificados se emiten para un nombre de dominio y no son gratuitos.

Pasos:

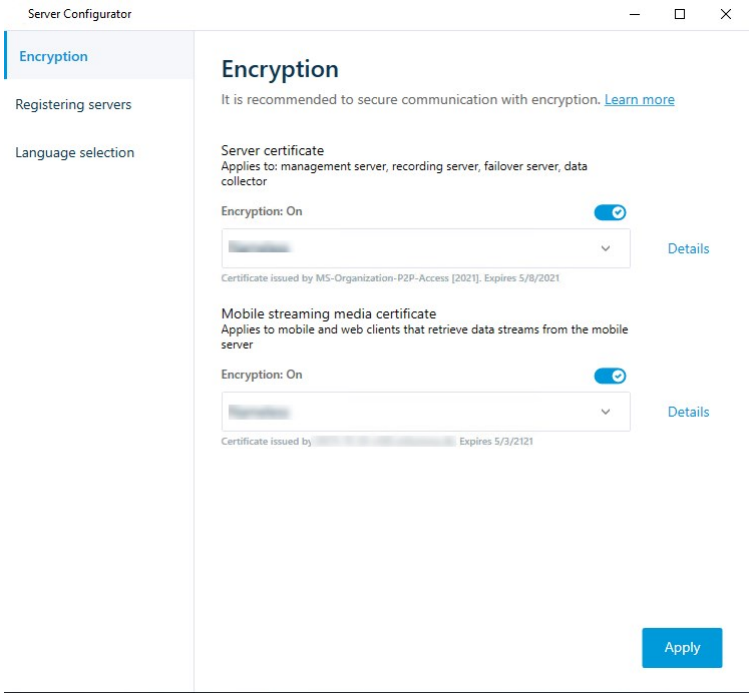
1. En un ordenador con un servidor móvil instalado, abra el **Server Configurator** desde:
   - El menú Inicio de Windows

   o

   - El Mobile Server Manager haciendo clic con el botón derecho en el icono Mobile Server Manager de la barra de tareas del ordenador
2. En el **Server Configurator**, bajo **Certificado de medios de transmisión móvil**, active **Encriptación**.
3. Haga clic en **Seleccionar certificado** para abrir una lista de nombres de sujeto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacenamiento de certificados de Windows.
4. Seleccione un certificado para encriptar la comunicación del cliente de XProtect Mobile y XProtect Web Client con el servidor móvil.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el certificado seleccionado.

   El usuario del servicio Mobile Server ha recibido acceso a la clave privada. Es necesario que este certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.

> Al aplicar certificados, el servidor de Mobile Server se reinicia.

Milestone Federated Architecture y sitios principales/secundarios

Milestone Federated Architecture vincula varios sistemas individuales en una jerarquía de sitios federados de sitios principales/secundarios.

Para acceder a todos los sitios con su XProtect Mobile o XProtect Web Client, instale el servidor XProtect Mobile solo en el sitio principal.

Los usuarios del cliente XProtect Mobile o de XProtect Web Client deben conectarse al servidor de gestión en el sitio principal.

Smart Connect

Smart Connect le habilita para verificar que ha configurado el XProtect Mobile correctamente sin iniciar sesión con un dispositivo móvil o una tableta para hacer la verificación. También simplifica el proceso de conexión para el cliente de XProtect Mobile y los usuarios de XProtect Web Client.

Esta característica requiere que su servidor de XProtect Mobile utilice una dirección IP pública y que su sistema tenga licencia con un paquete de suscripción de Milestone Care Plus.

El sistema le proporciona información instantánea en el Management Client si la configuración de conectividad remota se ha configurado correctamente y confirma que el servidor de XProtect Mobile es accesible desde Internet.

Smart Connect habilita al servidor de XProtect Mobile para cambiar sin problemas entre direcciones IP internas y externas y conectarse al XProtect Mobile desde cualquier ubicación.

Para que sea más fácil configurar el cliente móviles de clientes, puede enviar un correo electrónico directamente desde dentro del Management Client al usuario final. El correo electrónico incluye el vínculo que añade el servidor directamente a XProtect Mobile. Esto completa la configuración sin necesidad de introducir direcciones de red ni puertos.

Configurar Smart Connect

Para configurar la función Smart Connect, haga lo siguiente:

1. En Management Client, en el panel de navegación, expanda **Servidores**, y seleccione **Servidores móviles**.
2. Seleccione el servidor móvil y haga clic en la pestaña **Conectividad**.
3. Habilite la detección Universal Plug and Play en su router.
4. Configure los ajustes de conexión.
5. Envíe un mensaje de correo electrónico a los usuarios.
6. Habilite las conexiones en la red compleja.

Habilite la detección Universal Plug and Play en su router

Para que sea más fácil conectar dispositivos móviles a servidores de XProtect Mobile, puede habilitar Universal Plug and Play (UPnP) en su router. UPnP habilita al servidor XProtect Mobile para que continúe con el reenvío de puertos automáticamente. Sin embargo, también puede configurar manualmente el reenvío de puertos en su router utilizando su interfaz web. Dependiendo del router, el proceso para configurar la asignación de puertos puede variar. Si no está seguro de cómo configurar el reenvío de puertos en su router, consulte la documentación para ese dispositivo.

Cada cinco minutos, el servicio XProtect Mobile Server verifica que el servidor está disponible para los usuarios en Internet. El estado se muestra en la esquina superior izquierda del panel **Propiedades**: 

.

Habilite conexiones en redes complejas

Si tiene una red compleja en la que tiene ajustes personalizados, puede proporcionar la información que necesitan los usuarios para conectarse.

En la pestaña **Conectividad**, en el grupo **Acceso a Internet**, especifique lo siguiente:

- Si utiliza la asignación de puertos UPnP, para dirigir conexiones a una conexión específica, seleccione la casilla de verificación **Configurar acceso personalizado a Internet**. A continuación, proporcione la **dirección IP o el nombre de host** y el puerto que usar para la conexión. Por ejemplo, podría hacer esto si su router no es compatible con UPnP o si tiene una cadena de routers
- Si su dirección IP cambia con frecuencia, seleccione la casilla de verificación **Comprobar para recuperar dirección IP dinámicamente**

Configurar ajustes de conexión

1. En Management Client, en el panel de navegación, expanda **Servidores**, y seleccione **Servidores móviles**.
2. Seleccione el servidor y haga clic en la pestaña **Conectividad**.

3. Utilice las opciones en el grupo **General** para especificar lo siguiente:
    - Para que sea más fácil para el cliente de XProtect Mobile y para los usuarios de XProtect Web Client conectarse a los servidores de XProtect Mobile, seleccione la casilla de verificación **Habilitar Smart Connect**
    - Establecer un intervalo de tiempo para la frecuencia con la que el cliente de XProtect Mobile y XProtect Web Client deben indicar al servidor móvil que están activos y en funcionamiento
    - Para que el servidor de XProtect Mobile sea detectable en la red por medio de los protocolos UPnP, seleccione la casilla de verificación **Habilitar capacidad de detección de UPnP**
    - Para habilitar el servidor de XProtect Mobile, haga la asignación de puertos automáticamente si el router está configurado para ello, seleccione la casilla de verificación **Habilitar asignación automática de puertos**

Enviar un mensaje de correo electrónico a los usuarios

Para que sea más fácil configurar el cliente de XProtect Mobile y XProtect Web Client, puede enviar un correo electrónico directamente desde dentro del Management Client al usuario final. El correo electrónico incluye el vínculo que añade el servidor directamente a XProtect Mobile. Esto completa la configuración sin necesidad de introducir direcciones de red ni puertos.

1. En el campo **Enviar invitación por correo electrónico a**, introduzca la dirección de correcto electrónico para el destinatario de la notificación de Smart Connect y, a continuación, especifique un idioma.
2. A continuación, elija una de las siguientes opciones :
    - Para enviar el mensaje, haga clic en **Enviar**
    - Copiar la información en el programa de mensajería que utilice

Para obtener más información, consulte:

Requisitos para configuración de Smart Connect en la página 8

Pestaña Conectividad en la página 18

Notificaciones

Puede habilitar XProtect Mobile para notificar a los usuarios cuando se produce un evento, como cuando se desencadena una alarma o cuando algo va mal con un dispositivo o servidor.

Las notificaciones siempre se entregan, independientemente de si la aplicación se está ejecutando o no. Cuando XProtect Mobile se abre en el dispositivo móvil, la aplicación entrega la notificación. Las notificaciones del sistema también se entregan aún cuando la aplicación no se esté ejecutando. Los usuarios pueden especificar los tipos de notificaciones que quieren recibir. Por ejemplo, un usuario puede elegir recibir notificaciones para lo siguiente:

- Todas las alarmas
- Solo alarmas asignadas a ellos
- Solo alarmas relacionadas con el sistema

  Estos pueden ser cuando un servidor se desconecta o vuelve a conectarse.

También puede utilizar notificaciones push para notificar a los usuarios que no tienen XProtect Mobile abierto. A esto se le denomina notificaciones push. Las notificaciones push se entregan al dispositivo móvil y son una manera fantástica de mantener informados a los usuarios mientras están sobre la marcha.

De forma predeterminada, las notificaciones están deshabilitadas.

Uso de notificaciones push

Para usar notificaciones push, el sistema debe tener acceso a Internet.

Las notificaciones push utilizan servicios en la nube de Apple, Microsoft y Google:

- Servicio de notificación push de Apple (APN)
- Azure Notification Hub de Microsoft
- Servicio de notificaciones push de mensajería de Google Cloud

Hay un límite en el número de notificaciones que el sistema está autorizado a enviar durante un periodo de tiempo. Si su sistema excede el límite, solo puede enviar una notificación cada 15 minutos durante el siguiente periodo. La notificación contiene un resumen de los eventos que se produjeron durante los 15 minutos. Después del siguiente periodo, se quita la limitación.

Consulte también Requisitos para configuración de notificaciones en la página 8 y Pestaña Notificaciones en la página 27.

Configurar notificaciones push en el servidor XProtect Mobile

Para configurar notificaciones push, siga estos pasos:

1. En Management Client, seleccione el servidor móvil y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Para enviar notificaciones a todos los dispositivos móviles que se conectan con el servidor, seleccione la casilla de verificación **Notificaciones**. Lea la advertencia sobre sus datos personales y seleccione **Sí** si desea continuar.
3. Para almacenar información sobre los usuarios y los dispositivos móviles que se conectan al servidor, seleccione la casilla de verificación **Mantener registro de dispositivos**.

El servidor envía notificaciones solo a los dispositivos móviles de esta lista. Si desactiva la casilla de verificación **Mantener registro del dispositivo** y guarda el cambio, el sistema borra la lista. Para recibir notificaciones push de nuevo, los usuarios deben reconectar su dispositivo.

Habilitar el envío de notificaciones push a dispositivos específicos o móviles a todos los dispositivos móviles

Para habilitar XProtect Mobile, notifique a los usuarios cuando se produzca un evento enviando notificaciones push a dispositivos móviles concretos o a todos los dispositivos móviles:

1. En Management Client, seleccione el servidor móvil y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Puede seguir estos pasos:
   - Para dispositivos individuales, seleccione la casilla de verificación **Habilitado** para cada dispositivo móvil recogido en la tabla **Dispositivos registrados**
   - Para todos los dispositivos móviles, seleccionar la casilla de verificación **Notificaciones**. Lea la advertencia sobre sus datos personales y seleccione **Sí** si desea continuar

Detener el envío de notificaciones push a dispositivos móviles concretos o a todos ellos

Hay varias formas de detener el envío de notificaciones push a dispositivos móviles específicos o a todos ellos.

1. En Management Client, seleccione el servidor móvil y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Puede seguir estos pasos:
   - Para dispositivos individuales, desactive la casilla de verificación **Habilitado** para cada dispositivo móvil. El usuario puede utilizar otro dispositivo para conectarse al servidor de XProtect Mobile
   - Para todos los dispositivos, desactivare la casilla de verificación **Notificaciones**

Para detener temporalmente todos los dispositivos, desactive la casilla de verificación **Mantener registro de dispositivos** y, a continuación, guarde su cambio. El sistema vuelve a enviar notificaciones después de que los usuarios se reconecten.

Eliminado uno o todos los dispositivos registrados de la lista Dispositivos registrados

Al desinstalar la aplicación XProtect Mobile o deshabilitar el dispositivo, es posible que los datos del dispositivo sigan guardados en la base de datos de VMS.

El VMS elimina los datos de registro del dispositivo cuando:

- Elimina a un usuario del sistema:
- Milestone Care Plus no se ha renovado en más de 180 días.

No obstante, hay situaciones en las que los datos de registro del dispositivo no se eliminan automáticamente.

Debe eliminar manualmente uno o todos los dispositivos registrados cuando:

- Un usuario ha perdido su teléfono.
- Quiere desinstalar el servidor móvil completamente y eliminar sus datos.
- Un usuario ha dejado de utilizar la aplicación cliente de XProtect Mobile o las notificaciones.
- Ha añadido un grupo de Active Directory (AD) a un cometido de VMS y los permisos para un usuario han cambiado. Cuando añada un grupo AD, el VMS no verá los usuarios en ese cometido. Si elimina un usuario de un grupo de AD o restringe al usuario el uso del servidor móvil, también deberá eliminar manualmente el dispositivo del usuario de la lista.

Para eliminar un dispositivo registrado:

1. En Management Client, seleccione el servidor móvil y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Puede seguir estos pasos:
    - Para dispositivos individuales, seleccione el dispositivo y, a continuación, seleccione **Eliminar**.
    - Para todos los dispositivos, seleccione **Eliminar todos**.

Configurar investigaciones

Configure investigaciones de modo que las personas puedan utilizar XProtect Web Client o XProtect Mobile para acceder a vídeo grabado e investigar incidentes, así como y preparar y descargar evidencias de vídeo.

Para configurar investigaciones, siga estos pasos:

1. En Management Client, haga clic en el servidor móvil y, continuación, haga clic en la pestaña **Investigaciones**.
2. Seleccione la casilla de verificación **Habilitar investigaciones**. De forma predeterminada, la casilla de verificación está seleccionada.
3. En el campo **Carpeta de investigaciones**, especifique si almacenar vídeo para investigaciones.
4. Opcional: Para permitir a los usuarios acceder a investigaciones que creen otros usuarios, seleccione la casilla de verificación **Ver investigaciones hechas por otros usuarios**. Si no selecciona esta casilla de verificación, los usuarios puede ver solo sus propias investigaciones.
5. Seleccione la casilla de verificación **Habilitar el límite de tamaño de la carpeta de investigaciones** para establecer el número máximo de megabytes que puede contener la carpeta de investigaciones.

6. Seleccione la casilla de verificación **Habilitar el tiempo de retención de investigaciones** para establecer un tiempo de retención para las investigaciones. De forma predeterminada, el periodo de retención se establece en siete días.
7. En **Formatos de exportación**, seleccione la casilla de verificación del formato de exportación que quiera usar. Los formatos de exportación disponibles son:
   - **Formato AVI**
   - **XProtect formato**
   - **Formato MKV**

   De forma predeterminada, las casillas de verificación están desmarcadas.

8. (Opcional) Para incluir la fecha y la hora a las que se descargó un vídeo, seleccione la casilla de verificación **Incluir marcas de tiempo para exportaciones de AVI**.
9. En el campo **Códec utilizado para exportaciones de AVI**, seleccione el formato de compresión que se debe utilizar al preparar paquetes AVI para descargar.

   Los códecs de la lista pueden diferir, dependiendo de su sistema operativo. Si no ve el códec que quiere usar, puede instalarlo en el ordenador en el que se está ejecutando Management Client y se mostrará en esta lista.

   Adicionalmente, los códecs puede usar distintas tasas de compresión, lo que puede afectar a la calidad del vídeo. Tasas de compresión elevadas reducen los requisitos de almacenamiento, pero también pueden reducir la calidad. Tasas de compresión más bajas requieren más capacidad de almacenamiento y de red, pero puede aumentar la calidad. Es buena idea investigar los códecs antes de seleccionar uno.

10. Desde la lista **Velocidad de bits de audio usada para exportaciones AVI**, seleccione la velocidad de bits de audio apropiada cuando el audio se incluye en su exportación de vídeo. El valor predeterminado es 160000 Hz.

    Para habilitar que los usuarios guarden investigaciones, debe conceder el permiso **Exportar** al rol de seguridad asignado a los usuarios.

Limpiar investigaciones

Si tiene exportaciones de vídeos o investigaciones que ya no necesita conservar, puede eliminarlos. Por ejemplo, esto puede resultar útil si quiere hacer que haya más espacio libre del disco disponible en el servidor.

- Para eliminar una investigación y todas las exportaciones de vídeo que se crearon para ella. seleccione la investigación en la lista y después haga clic en **Eliminar**
- Para eliminar archivos de vídeo individuales que se exportaron para una investigación, pero conservar la investigación, seleccione la investigación en la lista. En el grupo **Detalles de la investigación**, haga clic en el icono **Eliminar** a la derecha de los campos **XProtect**, **AVI** o **MKV** para exportaciones

Uso de vídeo push para transmitir vídeo (explicación)

Puede configurar la transmisión push de vídeo de modo que los usuarios puedan mantener a otros informados sobre una situación o grabar un vídeo para investigarlo más tarde transmitiendo vídeo desde la cámara de sus dispositivos móviles a su sistema de vigilancia de XProtect. El flujo de vídeo también puede tener audio.

Consulte también Pestaña Transmisión push de vídeo en la página 26 y Requisitos para la configuración de la transmisión push de vídeo en la página 9.

Configurar vídeo transmisión push de vídeo para transmitir vídeo

Para permitir a los usuarios transmitir vídeo desde sus dispositivos móviles al sistema de XProtect, configure la transmisión push de vídeo en el servidor de XProtect Mobile.

En Management Client, realice estos pasos en el siguiente orden:

1. En la pestaña **Transmisión push de vídeo**, seleccione la casilla de verificación **Transmisión push de vídeo** para habilitar la función.
2. Añada un canal de transmisión push de vídeo para la transmisión de vídeo.
3. Añada el controlador de transmisión push de vídeo como dispositivo de hardware en el Recording Server. El controlador simula un dispositivo de cámara, para que pueda transmitir vídeo al Recording Server.
4. Añada el dispositivo del controlador de transmisión push de vídeo al canal para la transmisión push de vídeo.

Añadir un canal de transmisión push de vídeo para la transmisión de vídeo

Para añadir un canal, siga estos pasos:

1. En el panel de navegación, seleccione **Servidores móviles** y, a continuación seleccione el servidor móvil.
2. En la pestaña **Transmisión push de vídeo**, seleccione la casilla de verificación **Transmisión push de vídeo**.
3. En **Asignación de canales**, en la esquina inferior izquierda, haga clic en **Añadir** para añadir un canal de transmisión push de vídeo.

4. En el cuadro de diálogo que aparece, introduzca el nombre de usuario de la cuenta del usuario (añadida en **Roles**) que utilizará el canal. Esta cuenta de usuario debe poder acceder al servidor de XProtect Mobile y al servidor de grabación (en la pestaña **Seguridad global**).

   Para utilizar la transmisión push de vídeo, los usuarios deben iniciar sesión en XProtect Mobile en su dispositivo móvil utilizando el nombre de usuario y la contraseña para esta cuenta.

   Cuando añade un nuevo canal de transmisión puso de vídeo en el servidor móvil, el sistema genera el número de puerto y la dirección MAC del canal que se usan cuando el canal se añade como dispositivo de hardware en el servidor de grabación. El sistema también genera la contraseña que se usó para conectar el Recording Server con el Mobile Server. La contraseña predeterminada es **Milestone**.

5. Crear una nota en el número de puerto. Lo necesitará cuando añada el controlador de transmisión push de vídeo como dispositivo de hardware en el servidor de grabación.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo del canal de transmisión push de vídeo.
7. Para guardar el canal, haga clic en **Guardar** en la esquina superior izquierda del panel de navegación.

Editar un canal de notificación de push de vídeo

Puede editar los detalles de configuración de un canal de transmisión push de vídeo que ha añadido:

1. En **Asignación de canales**, seleccione el canal para editar y, a continuación, haga clic en **Editar**.
2. Cuando haya terminado con la edición, haga clic en **Aceptar** para cerrar el cuadro de diálogo del canal de transmisión push de vídeo.
3. Para guardar las ediciones haga clic en **Guardar** en la esquina superior izquierda del panel de navegación.

Cuando edite el número de puerto y la dirección MAC de un canal de transmisión push de vídeo, asegúrese de también sustituir los detalles de configuración de transmisión push del vídeo que añadió previamente en el servidor de grabación con la información nueva. De lo contrario, la conexión entre el Recording Server y el Mobile Server se romperá.

Quitar un canal de transmisión push de vídeo

Puede quitar canales que ya no utiliza:

1. En **Asignación de canales**, seleccione el canal que eliminar y, a continuación, haga clic en **Quitar**.
2. Para guardar el cambio, haga clic en **Guardar** en la esquina superior izquierda del panel de navegación.

Cambiar contraseña

Puede cambiar la contraseña generada automáticamente que se utiliza para conectar el Recording Server con el Mobile Server:

1. En **Asignación de canales**, en la esquina inferior derecha, haga clic en **Cambiar contraseña**.
2. En el cuadro de diálogo **Cambiar contraseña de transmisión push de vídeo**, introduzca la nueva contraseña en el primer campo, a continuación repita la nueva contraseña en el segundo campo y, después, haga clic en **Aceptar**.
3. Para guardar el cambio, haga clic en **Guardar** en la esquina superior izquierda del panel de navegación.

Al cambiar la contraseña del canal de transmisión push de vídeo, el cambio se aplicará a todos los canales de transmisión push de vídeo que ya existen en la lista o que se añadirán en el futuro. Incluso si elimina todos los canales de transmisión push de vídeo existente de la lista, la contraseña nueva permanece activa y se aplicará a canales futuros.

Después de guardar el cambio, todos los canales de transmisión push de vídeo existentes dejan de funcionar porque la conexión entre Recording Server y Mobile Server está rota. Para restablecer esta conexión, en el panel de navegación, al hacer clic con el botón derecho en la pestaña **Servidores de grabación**, debe ejecutar el asistente **Sustituir hardware** e introducir la contraseña nueva para el controlador de transmisión push de vídeo que añadió como dispositivo de hardware en el Recording Server.

Añadir el driver de vídeo push como dispositivo de hardware en el servidor de grabación

1. En el panel de navegación, haga clic en **Servidores de grabación**.
2. Haga clic con el botón derecho en el servidor al que quiere transmitir vídeo y haga clic en **Añadir hardware** para abrir el asistente **Añadir hardware**.
3. Seleccione **Manual** como método de detección de hardware y haga clic en **Siguiente**.

4. Introduzca las credenciales de inicio de sesión para el Vídeo Push Driver:
   - Nombre de usuario: Deje el campo en blanco para utilizar el nombre de usuario predeterminado.
   - Contraseña: Introduzca **Milestone**: la contraseña generada por el sistema. Si la ha cambiado al añadir el canal de vídeo push en el servidor móvil, introduzca la contraseña que prefiera usar. A continuación, haga clic en **Siguiente**

   Estas credenciales son para el hardware, no para los usuarios. Las credenciales no están relacionadas con la cuenta de usuario que se utiliza para acceder al canal de transmisión push de vídeo.

5. En la lista de controladores, expanda **Milestone**, seleccione la casilla de verificación **Controlador de transmisión push de vídeo** y haga clic en **Siguiente**.
6. En el campo **Dirección**, introduzca la dirección IP del ordenador en el que está instalado el servidor de XProtect Mobile.

   Es recomendable que utilice la dirección MAC generada por el sistema. Cámbielo solo si experimenta problemas con el dispositivo del controlador de transmisión push de vídeo o, por ejemplo, si ha editado el puerto y la dirección MAC del canal de transmisión push de vídeo en el servidor móvil.

7. En el campo **Puerto**, introduzca el número de puerto para el canal que creó para la transmisión de vídeo. El número de puerto se asignó al crear el canal.
8. En la columna **Modelo de hardware**, seleccione **Controlador de transmisión push de vídeo** y, a continuación, haga clic en **Siguiente**.
9. Cuando el sistema detecta el hardware nuevo, haga clic en **Siguiente**.
10. En el campo **Plantilla de nombre de hardware**, especifique si mostrar el modelo del hardware y la dirección IP o solo el modelo.

11. Especifique si habilitar dispositivos relacionados seleccionando la casilla de verificación **Habilitado**. Puede añadir dispositivos relacionados a la lista para **Controlador de transmisión push de vídeo**, aunque no estén habilitados. Puede habilitarlos más tarde.

    > Si quiere utilizar información sobre la ubicación al transmitir vídeo, debe habilitar el puerto **Metadatos**.

    > Si quiere reproducir audio cuando transmite vídeo, debe habilitar el micrófono relacionado con la cámara que usa para la transmisión de vídeo.

12. Seleccione los grupos predeterminados para los dispositivos relacionados en el lado izquierdo o seleccione un grupo concreto en el campo **Añadir a grupo**. La adición de dispositivos a un grupo puede hacer que sea más fácil aplicar ajustes a todos los dispositivos al mismo tiempo o sustituir dispositivos.

Añadir el dispositivo del controlador de transmisión push de vídeo al canal para la transmisión push de vídeo

Para añadir el dispositivo de controlador de transmisión push de vídeo al canal para transmisión de vídeo push, siga estos pasos:

1. En el panel **Navegación del centro**, haga clic en **Servidores móviles** y, a continuación, haga clic en la pestaña **Transmisión push de vídeo**.
2. Haga clic en **Buscar cámaras**. Si se realiza con éxito, el nombre de la cámara del controlador de transmisión push de vídeo se muestra en el campo **Nombre de cámara**.
3. Guarde su configuración.

Habilitar audio para canal de transmisión push de vídeo existente

Después de haber cumplido los requisitos para habilitar el audio en la transmisión push de vídeo (consulte Requisitos para la configuración de la transmisión push de vídeo en la página 9), en Management Client:

1. En el panel **Navegación del sitio**, expanda el nodo **Servidores** y haga clic en **Servidores de grabación**.
2. En el panel de descripción general, seleccione la carpeta del servidor de grabación relevante, a continuación expanda la carpeta **Controlador de transmisión push de vídeo** y haga clic con el botón derecho en el micrófono relacionado con la transmisión push de vídeo.
3. Seleccione **Habilitado** para habilitar el micrófono.
4. En la misma carpeta, seleccione la cámara relacionada con la transmisión push de vídeo.
5. En el panel **Propiedades**, haga clic en la pestaña **Cliente**.
   Si desea más información, consulte la pestaña Cliente (dispositivos).

6. En el lado derecho del campo **Micrófono relacionado**, haga clic en . Se abre el cuadro de diálogo **Dispositivo seleccionado**.
7. En la pestaña **Servidores de grabación**, expanda la carpeta del servidor de grabación y seleccione el micrófono relacionado con la transmisión push de vídeo.
8. Haga clic en **Aceptar**.

Configurar usuarios para la doble verificación de acceso por correo electrónico

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Para imponer un paso adicional de inicio de sesión a los usuarios del cliente XProtect Mobile o XProtect Web Client, configure la verificación en dos pasos en el servidor XProtect Mobile. Además del nombre de usuario y la contraseña estándar, el usuario debe introducir un código de verificación recibido por correo electrónico.

La verificación en dos pasos aumenta el nivel de protección de su sistema de vigilancia.

En Management Client, lleve a cabo estos pasos:

1. Introducir información sobre su servidor SMTP en la página 48.
2. Especificar el código de verificación que se enviará a los usuarios en la página 49.
3. Asignar el método de verificación a usuarios y Active Directorygrupos en la página 49.

Consulte también Requisitos para la configuración de la verificación en dos pasos del usuario en la página 9 y Pestaña Doble verificación de acceso en la página 28.

Introducir información sobre su servidor SMTP

El proveedor utiliza la información sobre el servidor SMTP:

1. En el panel de navegación, seleccione **Servidores móviles** y seleccione el servidor móvil correspondiente.
2. En la pestaña **Verificación en dos pasos**, seleccione la casilla **Habilitar verificación en dos pasos**.
3. A continuación de los **Ajustes del proveedor**, en la pestaña de **Correo electrónico**, introduzca la información sobre su servidor SMTP y especifique el correo electrónico que el sistema enviará a los usuarios clientes cuando se conecten y estén configurados para un inicio de sesión secundario.

Si desea más información, consulte Pestaña Doble verificación de acceso en la página 28.

Especificar el código de verificación que se enviará a los usuarios

Para especificar la complejidad del código de verificación:

1. En la pestaña **Verificación en dos pasos**, en la sección **Ajustes del código de verificación** , especifique el período en el que los usuarios clientes de XProtect Mobile no tienen que volver a verificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El periodo por defecto es de tres minutos.
2. Especifica el periodo en el que el usuario puede utilizar el código de verificación recibido. Después de este periodo, el código no es válido y el usuario debe solicitar un nuevo código. El periodo por defecto es de cinco minutos.
3. Especifique el número máximo de intentos de entrada de código antes de que el código proporcionado deje de ser válido. El número por defecto es tres.
4. Especifica el número de caracteres del código. La longitud por defecto es seis.
5. Especifique la complejidad del código que desea que el sistema genere.

Si desea más información, consulte Pestaña Doble verificación de acceso en la página 28.

Asignar el método de verificación a usuarios y Active Directorygrupos

En la pestaña **Verificación en dos pasos**, en la sección **Ajustes de usuario** , aparece la lista de usuarios y grupos añadidos a su sistema XProtect.

1. En la columna **Método de verificación**, seleccione un método de verificación para cada usuario o grupo.
2. En el campo **Detalles de usuario**, añada los detalles de la entrega, como las direcciones de correo electrónico de los usuarios individuales. La próxima vez que el usuario inicie sesión en XProtect Web Client o la aplicación XProtect Mobile, se le pedirá un inicio de sesión secundario.
3. Si un grupo está configurado en Active Directory, el servidor XProtect Mobile utiliza detalles, como las direcciones de correo electrónico, de Active Directory.

   Los grupos de Windows no admiten la doble verificación de acceso.

4. Guarde su configuración.

Ha completado los pasos para configurar sus usuarios para la verificación en dos pasos por correo electrónico.

Si desea más información, consulte Pestaña Doble verificación de acceso en la página 28.

Acciones

Puede gestionar la disponibilidad de la pestaña **Acciones** en el cliente de XProtect Mobile o XProtect Web Client habilitando o deshabilitando acciones en la pestaña **General**. Las **acciones** están habilitadas de forma predeterminada, y todas las acciones disponibles para los dispositivos conectados se muestran aquí.

Si desea más información, consulte Pestaña general en la página 15.

Gestión de dispositivos móviles (MDM)

Gestión de dispositivos móviles (Mobile device management, MDM) es un software que asegura, supervisa, gestiona y asiste a los dispositivos móviles implementados por operadores móviles, proveedores de servicios y empresas.

Normalmente, las soluciones MDM incluyen un componente servidor, que envía los comandos de gestión a los dispositivos móviles, y un componente cliente, que se ejecuta en el dispositivo gestionado y recibe e implementa los comandos de gestión.

Puede distribuir el cliente de XProtect Mobile y añadir políticas personalizadas a los dispositivos de su organización.

Para utilizar la funcionalidad MDM en un dispositivo móvil, debe configurar los detalles del servidor móvil en la plataforma de software MDM. Los detalles del servidor móvil incluyen el nombre del servidor, la dirección del servidor, el puerto del servidor y el protocolo de tipo de conexión.

Si ha actualizado los detalles de un servidor móvil ya añadido, el operador debe eliminar manualmente este servidor de la lista **Servidores** y reiniciar la aplicación XProtect Mobile.

Configurar los detalles del servidor móvil en la plataforma MDM (administradores)

Para distribuir y gestionar el cliente de XProtect Mobile a los dispositivos móviles desde una plataforma MDM, es necesario añadir los detalles del servidor. Para obtener más información sobre la configuración, consulte la documentación sobre su software MDM.

Si no ha introducido ninguno de los datos obligatorios del servidor o ha proporcionado datos incorrectos, el servidor móvil no se añadirá a la aplicación XProtect Mobile.

Para usuarios de Android.

Puede especificar los detalles del servidor en la interfaz de usuario de su plataforma MDM. Tiene la opción de cargar un archivo de configuración gestionado con los detalles del servidor.

Detalles del servidor:

- **Nombre del servidor**: (Obligatorio) Escriba el nombre del servidor
- **Dirección del servidor**: (Obligatorio) Escriba la dirección del servidor
- **Puerto del servidor**: (Obligatorio) Escriba el número de puerto del servidor

- **Tipo de protocolo de conexión**: Habilite si utiliza una conexión HTTPS. Deshabilite cuando use una conexión HTTP. De forma predeterminada, la conexión HTTPS está habilitada

Para cargar el archivo en su plataforma MDM:

1. Al final de este manual, en el Apéndice A, encontrará la plantilla de configuración gestionada para los dispositivos Android. Copie el contenido.
2. Abra el editor de texto que prefiera y pegue el contenido.
3. Especifique los detalles del servidor en los campos **android:description**.
4. Guarde el archivo como .XML.
5. Abra su plataforma MDM y cargue el archivo de configuración gestionado.

Para usuarios de iOS.

Para gestionar dispositivos iOS desde una plataforma MDM, es necesario especificar los detalles de conexión en el archivo de configuración gestionado.

1. Al final de este manual, en el Apéndice B, encontrará la plantilla de configuración gestionada para dispositivos iOS. Copie el contenido.
2. Abra el editor de texto que prefiera y pegue el contenido.
3. Especifique los detalles del servidor:
    - **versionConfig** - (Obligatorio) Escriba la versión por defecto de la configuración de la aplicación **1.0.0**
    - **serverNameConfig** - (Obligatorio) Escriba el nombre del servidor
    - **serverAddressConfig** - (Obligatorio) Escriba la dirección del servidor
    - **serverPortConfig** - (Obligatorio) Escriba el número de puerto del servidor
    - **serverConnectionProtocolTypeConfig** - El tipo de conexión predeterminado es **HTTPS**, para usar una conexión no segura, escriba **HTTP**
4. Guarde el archivo como .XML.
5. Abra su plataforma MDM y cargue el archivo de configuración gestionado.

Denominación de una salida para usar el cliente de XProtect Mobile y XProtect Web Client (explicación)

Para conseguir que las acciones se muestren correctamente con una cámara actual, debe crear un grupo de salida que tenga el mismo nombre que la cámara.

Ejemplo:

Cuando se crea un grupo de salida con salidas conectadas a una cámara llamada "AXIS P3301 - 10.100.50.110 - Cámara 1", debe introducir el mismo nombre en el campo **Nombre** (en **Información del grupo de dispositivos**).

En el campo **Descripción**, puede añadir una descripción adicional, por ejemplo, "AXIS P3301 - 10.100.50.110 - Cámara 1 - Cambio ligero".

> Si no sigue estas convenciones de nomenclatura, las acciones no están disponibles en la lista de acciones para la vista de la cámara asociada. En su lugar, las acciones aparecen en la lista de otras acciones en la pestaña **Acciones**.

Si desea más información, consulte Salidas.

IDP externo y XProtect Mobile

IDP es un acrónimo para Identity Provider. Un IDP externo es una aplicación y un servicio externo donde puede almacenar y gestionar la información de la identidad del usuario y proporcionar servicios de autenticación de usuarios a otros sistemas. Puede asociar un IDP externo con el VMS de XProtect.

Puede iniciar sesión en XProtect Web Client o en el cliente de XProtect Mobile mediante un IDP externo con XProtect 2022 R3 y posteriores.

> Para iniciar sesión con un IDP externo en XProtect Web Client o en el cliente de XProtect Mobile, debe utilizar una conexión HTTPS.

Antes de configurar un inicio de sesión con IDP externo para XProtect Web Client y el cliente de XProtect Mobile, asegúrese de que tiene:

- Configurar un IDP externo
- Reclamaciones registradas
- Reclamaciones asignadas a cometidos

Para obtener más información, consulte el manual de administrator para XProtect VMS.

Para iniciar sesión en XProtect Web Client mediante un IDP externo, necesita una configuración adicional. Consulte Configurar el inicio de sesión con IDP externo para XProtect Web Client en la página 52.

Configurar el inicio de sesión con IDP externo para XProtect Web Client

La opción de iniciar sesión mediante un IDP externo para XProtect Web Client está disponible solo para conexiones HTTPS.

1. En Management Client, seleccione **Herramientas** > **Opciones** y abra la pestaña **IDP externo**.
2. En la sección **URI de redireccionamiento para clientes web**, seleccione **Añadir**.
3. Introduzca las direcciones de XProtect Web Client en el formato `https://[dirección]:[número de puerto]/index.html`:
    - Para la dirección, introduzca el nombre de host o la dirección IP del ordenador en el que se ejecuta el servidor móvil
    - Para el número de puerto, introduzca el puerto que XProtect Web Client utiliza para comunicarse con el servidor móvil. Para conexiones HTTPS, el número de puerto predeterminado es 8082

Añadir alarmas de alerta de emergencia

Cuando se detecta una amenaza potencial, la Alerta de emergencia habilita al cliente XProtect Mobile para recibir notificaciones de alarma del nivel de gravedad más alto, ver los detalles de la alarma y actuar inmediatamente. La Alerta de emergencia es un tipo de alarma que define en XProtect Management Client.

Para que esta funcionalidad se ponga en marcha, requiere notificaciones push. Las notificaciones push están disponibles solo si ha comprado una licencia Milestone Care Plus.

Esta función solo está disponible en determinados XProtect productos de VMS. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Para añadir una alarma de este tipo, debe:

1. Añadir una nueva categoría de alarma con nivel 99 en **Alarmas** > **Ajustes de datos de alarma**. Puede crear tantas categorías con nivel 99 como necesite.
2. Añada una definición de alarma con esta categoría.

Mantenimiento

Mobile Server Manager

El Mobile Server Manager es una característica controlada por la bandeja conectada al servidor móvil. Al hacer clic con el botón derecho en el icono de la bandeja Mobile Server Manager en el área de notificación se abre un menú desde el que puede acceder a las funcionalidades del servidor móvil.

Puede:

- Acceso a XProtect Web Client en la página 54
- Inicio, parada y reinicio del servicio de Mobile Server en la página 55
- Cambiar contraseña de protección de datos del servidor móvil en la página 55
- Mostrar/Editar números de puerto en la página 56
- Habilitar cifrado en el servidor móvil en la página 34 utilizando **Server Configurator**
- Abra el archivo de registro de hoy (consulte Registros de acceso e investigaciones (explicación) en la página 56)
- Abrir carpeta Registro (consulte Registros de acceso e investigaciones (explicación) en la página 56)
- Abrir carpeta de investigaciones (consulte Registros de acceso e investigaciones (explicación) en la página 56)
- Cambiar carpeta de investigaciones en la página 57
- Consulte el estado de XProtect Mobile Server (consulte Mostrar estado en la página 58)

Acceso a XProtect Web Client

Si tiene un servidor de XProtect Mobile instalado en su ordenador, puede utilizar el XProtect Web Client para acceder a sus cámaras y vistas. Debido a que no necesita instalar XProtect Web Client, puede acceder a él desde el ordenador en el que instaló el servidor de XProtect Mobile o desde cualquier otro ordenador que quiera utilizar para este fin.

1. Configure el servidor de XProtect Mobile en el Management Client.
2. Si está utilizando el ordenador en el que hay instalado un servidor de XProtect Mobile, puede hacer clic con el botón derecho en el icono de bandeja Mobile Server Manager del área de notificación y seleccionar **Abrir XProtect Web Client**.
3. Si no está utilizando el ordenador en el que hay instalado un servidor de XProtect Mobile, puede acceder a él desde un navegador. Continúe con el paso 4 en este proceso.
4. Abra un navegador de Internet (Microsoft Edge, Mozilla Firefox, Google Chrome o Safari).

5. Introduzca la dirección IP externa, es decir, la dirección externa y el puerto del servidor en el que se está ejecutando el servidor XProtect Mobile.

   Ejemplo: El servidor de XProtect Mobile se instala en un servidor con la dirección IP 127.2.3.4 y se configura para aceptar conexiones HTTP en el puerto 8081 y conexiones HTTPS en el puerto 8082 (ajustes predeterminados del instalador).

   En la barra de direcciones del navegador, introduzca **http://127.2.3.4:8081** si quiere utilizar una conexión HTTP estándar o **https://127.2.3.4:8082** para utilizar una conexión HTTPS segura. Ahora puede empezar a utilizar XProtect Web Client.

6. Añada la dirección como un marcador en su navegador para poder acceder fácilmente en el futuro a XProtect Web Client. Si utiliza XProtect Web Client en el ordenador local en el que instaló el servidor de XProtect Mobile, también puede usar el acceso directo que el instalador crea en el escritorio. Haga clic en el acceso directo para iniciar el navegador predeterminado y abra XProtect Web Client.

Debe borrar la caché de los navegadores de Internet que se ejecutan en el XProtect Web Client antes de poder usar la nueva versión del XProtect Web Client. Los administradores del sistema deben pedir a sus usuarios de XProtect Web Client que borren la caché de su navegador después de actualizar o forzar esta acción de manera remota (puede hacer esta acción solo en Internet Explorer en un dominio).

Inicio, parada y reinicio del servicio de Mobile Server

En caso necesario, puede iniciar, parar y reiniciar el servicio de Mobile Server desde el Mobile Server Manager.

- Para realizar cualquiera de estas tareas, haga clic con el botón derecho en el icono de Mobile Server Manager y seleccione **Iniciar servicio de Mobile Server**, **Detener servicio de Mobile Server** o **Reiniciar servicio de Mobile Server**, respectivamente

Cambiar contraseña de protección de datos del servidor móvil

La contraseña de protección de los datos del servidor móvil se usa para encriptar algoritmos. Como administrador del sistema, tendrá que introducir esta contraseña para acceder a los datos del servidor móvil en caso de recuperación del sistema o cuando amplíe su sistema con servidores móviles adicionales.

Para cambiar la contraseña de protección de los datos del servidor móvil:

1. Haga clic con el botón derecho en el icono Mobile Server Manager y seleccione **Cambiar ajustes de contraseña de protección de datos**. Aparece un cuadro de diálogo.
2. En el campo **Contraseña nueva**, introduzca su contraseña nueva.
3. Vuelva a introducir la contraseña en el campo **Confirmar contraseña nueva**.

4. (Opcional) Si no quiere que sus investigaciones estén protegidas con contraseña, seleccione **Elijo no utilizar una contraseña de protección de datos del servidor móvil y comprendo que las investigaciones no estarán cifradas**.
5. Haga clic en **Aceptar**.

> Debe guardar esta contraseña y mantenerla a salvo. No hacerlo puede comprometer su habilidad para recuperar datos del servidor móvil.

Mostrar/Editar números de puerto

1. Haga clic con el botón derecho en el icono Mobile Server Manager y seleccione **Mostrar/editar números de puerto**.
2. Para editar los números de puerto, introduzca el número de puerto relevante. Puede indicar un número de puerto estándar para conexiones HTTP o un número de puerto seguro para conexiones HTTPS, o ambos.
3. Haga clic en **Aceptar**.

Registros de acceso e investigaciones (explicación)

El Mobile Server Manager le permite acceder rápidamente al archivo de registro del día, abrir la carpeta en la que se guardan los archivos de registro y abrir la carpeta en la que se guardan las investigaciones.

Para abrir cualquiera de estos, haga clic con el botón derecho en el icono de Mobile Server Manager y seleccione:

- **Abrir el archivo de registro de hoy**
- **Abrir carpeta de registro**
- **Abrir carpeta de investigación**

Se crean registros de auditoría para cada acción que no haya registrado el Management Server o el Recording Server.

Las siguientes acciones siempre se registran (incluso cuando el registro de auditoría ampliado no está habilitado):

- Toda la administración (estos mensajes de registro de auditoría contienen el valor antiguo y el valor nuevo)
- Todas las acciones relativas a la creación, edición o eliminación de investigaciones, así como a la preparación y la descarga de material exportado, el cambio de partes relevantes de la configuración. El registro de auditoría contiene detalles sobre lo que se ha hecho.

La transmisión push de vídeo ´se registra solo cuando al registro de auditoría extendido está habilitado.

Si desinstala el servidor de XProtect Mobile de su sistema, los archivos de registro no se eliminan. Los administradores con permisos de usuario apropiados pueden acceder a estos archivos de registro más adelante o decidir eliminarlo si ya no los son necesarios. La ubicación predeterminada de los archivos de registro es en la carpeta **ProgramData**. Si cambia la ubicación predeterminada de los archivos de registro, los registros existentes no se copian en la nueva ubicación, ni se eliminan.

Cambiar carpeta de investigaciones

La ubicación predeterminada de las investigaciones es en la carpeta **ProgramData**. Si cambia la ubicación predeterminada de la carpeta de investigaciones, las investigaciones existentes no se copian automáticamente en la nueva ubicación, ni se eliminan. Para cambiar la ubicación en la que guarda las exportaciones de investigaciones en su disco duro:

1. Haga clic con el botón derecho en el icono Mobile Server Manager y seleccione **Cambiar carpetas de investigaciones**.

   Se abre la ventana **Ubicación de las investigaciones**.

2. Junto al campo **Carpeta** que muestra la ubicación actual, haga clic en el icono de la carpeta para ir a una carpeta existente o crear una carpeta nueva > Haga clic en **Aceptar**.

3. Desde la lista **Investigaciones antiguas**, seleccione la acción que quiere aplicar a las investigaciones existentes que están almacenadas en la ubicación actual. Las opciones son:

   - **Mover**: Mueve las investigaciones existentes a la nueva carpeta

     Si no puede las investigaciones existentes a la nueva carpeta, ya no podrá verlos.

   - **Eliminar**: Elimina las investigaciones existentes
   - **No hacer nada**: Las investigaciones existentes permanecen en la ubicación de la carpeta actual. Ya no podrá verlos después de haber cambiado la ubicación predeterminada en la carpeta de investigaciones

4. Haga clic en **Aplicar** > Haga clic en **Aceptar**.

Mostrar estado

Haga clic con el botón derecho en el icono Mobile Server Manager y seleccione **Mostrar estado** o haga doble clic en el icono Mobile Server Manager para abrir una ventana que muestra el estado del servidor XProtect Mobile. Puede ver la siguiente información:

Nombre	Descripción
Servidor en ejecución desde	Hora y fecha del momento en que el servidor de XProtect Mobile se inició por última vez.
Usuarios conectados	Número de usuarios conectados actualmente al servidor de XProtect Mobile.
Decodificación de hardware	Indica su la decodificación acelerada por hardware está en acción en el servidor de XProtect Mobile.
% uso de CPU	Qué porcentaje de la CPU está utilizando actualmente el servidor de XProtect Mobile.
Historial de uso de CPU	Un gráfico que detalla la historia del uso de la CPU por el servidor de XProtect Mobile.

Usar un equilibrador de carga para el servidor móvil

Como paso de seguridad adicional, XProtect Mobile usa los ID en la comunicación entre el servidor y la aplicación móvil. Cuando un usuario se conecta por primera vez a un servidor móvil desde la aplicación XProtect Mobile, el ID del servidor móvil se copia al dispositivo del usuario. Cada vez que se intenta conectar a un servidor móvil, los ID del servidor se comparan con los que se obtuvieron inicialmente.

De forma predeterminada, cada servidor tiene un ID de servidor único. Para añadir un servidor móvil a un grupo de equilibrio de carga, debe asegurarse de que el ID del servidor móvil coincide con el ID que utilizan los otros servidores móviles del grupo.

En un host del grupo de equilibrio de carga

Para copiar los ID de servidor desde un host:

1. Vaya a `C:\ProgramFiles\Milestone\Milestone Mobile Server` y copie el archivo **VideoOS.MobileServer.Service.exe.config**.
2. Pegue el archivo en el ordenador y ábralo con el editor de texto que desee.

3. Busque en el archivo la etiqueta `ServerSettings`. Deberá tener este aspecto:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

4. Copie los valores **ServiceID** y **ReportedServiceID**.

En los otros hosts que forman parte del grupo

En un host que forma parte del grupo de equilibrio de carga:

1. Vaya a `C:\ProgramFiles\Milestone\Milestone Mobile Server` y abra el archivo **VideoOS.MobileServer.Service.exe.config** con el editor de texto que desee.
2. Busque en el archivo la etiqueta `ServerSettings` y sustituya los valores **ServiceID** y **ReportedServiceID** por los del archivo de configuración original.
3. Para aplicar los cambios, reinicie el servicio Mobile Server.
4. Pida a los usuarios clientes de XProtect Mobile que vuelvan a añadir el servidor móvil.

Repita los pasos en todos los hosts que formen parte del grupo de equilibrio de carga.

Migrar un servidor móvil a otro host

Como paso de seguridad adicional, XProtect Mobile usa los ID en la comunicación entre el servidor y la aplicación móvil. Cuando un usuario se conecta por primera vez a un servidor móvil desde la aplicación XProtect Mobile, el ID del servidor móvil se copia al dispositivo del usuario. Cada vez que la aplicación intenta conectarse a un servidor móvil, compara los ID de servidor con los que recibió inicialmente. Si los ID de servidor no coinciden, no se podrá establecer la conexión.

Al migrar el servidor móvil a otro host y mantener la dirección original, debe mantener el ID del antiguo servidor.

En el antiguo host

Antes de migrar el servidor móvil, debe:

1. Vaya a `C:\ProgramFiles\Milestone\Milestone Mobile Server`, copie el archivo **VideoOS.MobileServer.Service.exe.config** y ábralo con el editor de texto que desee.
2. Busque en el archivo la etiqueta `ServerSettings`. Deberá tener este aspecto:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

3. Copie los valores **ServiceID** y **ReportedServiceID**.

Ya podrá migrar el servidor móvil.

En el nuevo host

Después de haber instalado y configurado el servidor móvil en el nuevo host:

1. Vaya a `C:\ProgramFiles\Milestone\Milestone Mobile Server` y abra el archivo **VideoOS.MobileServer.Service.exe.config** con el editor de texto que desee.
2. Busque en el archivo la etiqueta `ServerSettings` y sustituya los valores **ServiceID** y **ReportedServiceID** por los del archivo de configuración original.
3. Para aplicar los cambios, reinicie el servicio Mobile Server.
4. Pida a los usuarios clientes de XProtect Mobile que vuelvan a añadir el servidor móvil.

Solución de problemas

Solución de problemas de XProtect Mobile

Conexiones

¿Por qué no puedo conectar desde mi cliente de XProtect Mobile con mis grabaciones/servidor de XProtect Mobile?

Para conectar con sus grabaciones, e servidor de XProtect Mobile debe estar instalado en el servidor que ejecuta su sistema XProtect o, como alternativa, en un servidor dedicado. Los ajustes relevantes de XProtect Mobile también son necesarios en su configuración de gestión de vídeo de XProtect. Estos se instalan como plug-in o como parte de la instalación o la actualización de un producto. Para ver los detalles sobre cómo conseguir el servidor de XProtect Mobile y cómo integrar los ajustes de XProtect Mobile relacionados con el cliente en su sistema XProtect, consulte la sección de configuración (consulte Ajustes del servidor móvil en la página 14).

El campo de dirección del servidor debe contener un nombre de host válido cuando se aplica en el dispositivo iOS. Los nombres de host válidos pueden contener las letras ASCII 'a' a 'z' (no distingue entre mayúsculas y minúsculas), los dígitos '0' a '9', el punto y el guion ('-').

Acabo de encender mi cortafuegos y ahora no puedo conectar un dispositivo móvil a mi servidor. ¿Por qué no?

Si se desactivó el cortafuegos mientras instalaba el servidor XProtect Mobile, debe habilitar manualmente las comunicaciones TCP y UDP.

¿Cómo evito la advertencia de seguridad cuando ejecuto XProtect Web Client mediante una conexión HTTPS?

La advertencia parece porque la información de la dirección del servidor en el certificado no es correcta. La conexión seguirá estando cifrada.
El certificado autofirmado en el servidor de XProtect Mobile debe sustituirse por su propio certificado que coincida con la dirección del servidor utilizada para conectar con el servidor de XProtect Mobile. Estos certificados se obtienen por medio de autoridades oficiales de firma de certificados, como Verisign. Consulte a la autoridad de firma elegida para obtener más detalles.
El servidor de XProtect Mobile no utiliza Microsoft IIS. Esto significa que las instrucciones proporcionadas para generar archivos de solicitud de firmas de certificados (CSR) firmando la autoridad de firma utilizando el IIS no son aplicables para el servidor de XProtect Mobile. Debe crear manualmente un archivo CSR utilizando herramientas de certificado de la línea de comandos o cualquier otra aplicación similar de terceros. Este proceso deben realizarlo únicamente administradores del sistema y usuarios avanzados.

No he modificado la dirección del servidor móvil, pero los usuarios clientes de XProtect Mobile ya no se pueden conectar a él. ¿Por qué?

Los clientes de XProtect Mobile se conectan al servidor móvil usando un ID de servicio único. Aunque el nombre de host y la dirección IP del ordenador del servidor móvil sigan siendo los mismos, el ID de servicio puede no coincidir con el almacenado en los clientes, por ejemplo, cuando:

- Ha restablecido el ordenador y vuelto a instalar el servidor móvil.
- Ha transferido el servidor móvil a otro ordenador, pero ha mantenido la configuración original.

Para volver a establecer la conexión, puede:

- Actualice el ID de servicio en el nuevo servidor móvil para que coincida con el ID de servicio de la anterior configuración. Consulte https://developer.milestonesys.com/s/article/unable-to-establish-connection-to-XProtect-Mobile-Server-using-Android-iOS-client.
- Pida a los usuarios clientes de XProtect Mobile que vuelvan a conectarse al servidor móvil.

Calidad de imagen

¿Por qué la calidad de la imagen es a veces mala cuando veo vídeo en el cliente de XProtect Mobile?

El servidor de XProtect Mobile ajusta automáticamente la calidad de la imagen de acuerdo con en ancho de banda disponible entre el servidor y el cliente. Si experimenta una menor calidad de imagen que en el XProtect® Smart Client, podría tener demasiado poco ancho de banda para obtener imágenes de resolución completa mediante el cliente XProtect Mobile. La razón de esto puede ser muy poco ancho de banda ascendente desde el servidor o muy poco ancho de banda descendente en el cliente. Si desea más información, consulte el manual del usuario para XProtect Smart Client.

Si está en un área con ancho de bando inalámbrico mixto, puede observar que la calidad de la imagen mejora cuando entra en un área con mejor ancho de banda.

¿Por qué la calidad de la imagen es mala cuando conecto con mi sistema de gestión de vídeo de XProtect en casa a través del Wi-Fi en mi oficina?

Compruebe el ancho de banda de Internet de su hogar. Muchas conexiones privadas a Internet tienen distintos anchos de banda de descarga y de carga, a menudos descritas como, por ejemplo, 20 Mbit/2 Mbit. Esto es porque los usuarios particulares raras veces tienen que cargar grandes cantidades de datos en Internet, pero, por contra, consumen una gran cantidad de datos. El sistema de gestión de vídeo XProtect necesita enviar vídeo al cliente de XProtect Mobile y está limitado por la velocidad de carga de su conexión. Si la baja calidad de imagen es constante en varias ubicaciones en las que la velocidad de descarga de la red del cliente de XProtect Mobile es buena, el problema podría solucionarse actualizando la velocidad de carga de su conexión a Internet doméstica.

Decodificación acelerada por hardware

¿Admite mi procesador la decodificación acelerada por hardware?

Solo los procesadores más novedosos de Intel son compatibles con la codificación acelerada de hardware. Compruebe en el sitio web de Intel (https://www.intel.com/content/www/us/en/ark/featurefilter.html?productType=873&0_QuickSyncVideo=True) si su procesador es compatible.

En el menú, asegúrese de que **Tecnologías** > **Intel Quick Sync Video** está establecido en **Sí**.

Si su procesador es compatible, la decodificación acelerada por hardware está habilitada de forma predeterminada. Puede ver el estado actual en **Mostrar estado** en el Mobile Server Manager (consulte Mostrar estado en la página 58).

¿Admite mi sistema operativo la decodificación acelerada por hardware?

Todos los sistemas operativos que admite XProtect también admiten la aceleración de hardware.

Asegúrese de instalar los controladores gráficos más recientes en su sistema. Estos controladores no están disponibles en Windows Update.

¿Cómo deshabilito la decodificación acelerada por hardware en el servidor móvil? (Avanzado)

- Si el procesador del servidor móvil es compatible con la decodificación acelerada por hardware, esto está habilitado de forma predeterminada. Para desactivar la decodificación acelerada por hardware, haga lo siguiente:

  1. Localice el archivo VideoOS.MobileServer.Service.exe.config. Normalmente la ruta es: `C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config`.
  2. Abra el archivo en el bloc de notas o en un editor de texto similar. En caso necesario, asocie el tipo de archivo .config con Bloc de notas.
  3. Localice el campo `<add key="HardwareDecodingMode" value="Auto" />`.
  4. Sustituya el valor "Auto" por "Off".
  5. Guarde y cierre el archivo.

Notificaciones

No he realizado ningún cambio en la configuración de las notificaciones, pero los dispositivos registrados han dejado de recibir notificaciones. ¿Por qué?

Si ha actualizado su licencia o renovado su suscripción Milestone Care, debe reiniciar el servicio Mobile Server.

Apéndices

Anexo A

Plantilla de configuración gestionada para Android

```
<?xml version="1.0" encoding="utf-8"?>

<restrictions xmlns:android="http://schemas.android.com/apk/res/android">

    <restriction
        android:defaultValue="1.0.0"
        android:description="The current version of the app configuration"
        android:key="version_config"
        android:restrictionType="hidden"
        android:title="Version" />

    <restriction
```

```
        android:description="(Mandatory) Enter the server name."
        android:key="server_name_config"
        android:restrictionType="string"
        android:title="Server name" />

    <restriction
        android:description="(Mandatory) Enter the server address."
        android:key="server_address_config"
        android:restrictionType="string"
        android:title="Server address" />

    <restriction
        android:description="(Mandatory) Enter the server port."
```

```
        android:key="server_port_config"

        android:restrictionType="integer"

        android:title="Server port" />


    <restriction

        android:description="Enable when you use an HTTPS connection. Disable
when you use an HTTP connection."

        android:key="server_secure_connection_config"

        android:restrictionType="bool"

        android:title="Connection protocol type"

        android:defaultValue="true"/>


</restrictions>
```

Anexo B

Plantilla de configuración gestionada para iOS

```
<managedAppConfiguration>
    <version>1</version>
    <bundleId>com.milestonesys.XProtect</bundleId>
    <dict>
        <string keyName="versionConfig">
            <defaultValue>
                <value>1.0.0</value>
            </defaultValue>
        </string>
        <string keyName="serverNameConfig">
        </string>
        <string keyName="serverAddressConfig">
        </string>
```

```
        <string keyName="serverPortConfig">
        </string>
        <string keyName="serverConnectionProtocolTypeConfig">
            <defaultValue>
                <value>HTTPS</value>
            </defaultValue>
        </string>
    </dict>
    <presentation defaultLocale="en-US">
        <field keyName="versionConfig" type="input">
            <label>
                <language value="en-US">Version</language>
            </label>
            <description>
```

```
                <language value="en-US">The current version of the app
configuration</language>

            </description>

        </field>

    <fieldGroup>

        <name>

            <language value="en-US">Mobile server</language>

        </name>

        <field keyName="serverNameConfig" type="input">

            <label>

                <language value="en-US">Server name</language>

            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
name.</language>
```

```
            </description>
        </field>
        <field keyName="serverAddressConfig" type="input">
            <label>
                <language value="en-US">Server address</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
address.</language>
            </description>
        </field>
        <field keyName="serverPortConfig" type="input">
            <label>
                <language value="en-US">Server port</language>
```

```
            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
port.</language>

            </description>

        </field>

        <field keyName="serverConnectionProtocolTypeConfig" type="input">

            <label>

                <language value="en-US">Connection protocol type</language>

            </label>

            <description>

                <language value="en-US">To specify the connection protocol
type, enter HTTPS or HTTP.</language>

            </description>

        </field>
```

```
    </fieldGroup>

    </presentation>

</managedAppConfiguration>
```

helpfeedback@milestone.dk

Acerca de Milestone

Milestone Systems figura entre los proveedores más destacados de software de gestión de vídeo de plataforma abierta, tecnología que ayuda a determinar cómo garantizar la seguridad, proteger activos y aumentar la eficiencia empresarial. Milestone Systems da soporte a una comunidad de plataforma abierta que fomenta la colaboración y la innovación en el desarrollo y uso de tecnologías de vídeo en red, gracias a soluciones fiables y escalables de eficacia probada en más de 150 000 instalaciones de todo el mundo. Milestone Systems se fundó en 1998 y es una empresa independiente dentro del Canon Group. Para obtener más información, visite https://www.milestonesys.com/.