Aviso legal

Descargo de responsabilidad legal

Esta guía y su contenido (la «Guía») son proporcionados por NXGEN. Todos los derechos sobre la Guía y sobre la propiedad intelectual incorporada en ella — incluidos, entre otros, marcas, nombres comerciales, logotipos y signos similares que figuren en la Guía — están protegidos por la ley. Todos los derechos, títulos e intereses sobre la Guía y sobre los derechos de propiedad intelectual relacionados pertenecen y permanecen con NXGEN y sus licenciantes.

La Guía se proporciona de forma gratuita, «tal cual» y únicamente con fines informativos, sin garantía de ningún tipo. No está destinada ni es adecuada para establecer relación jurídica alguna entre el lector y NXGEN o sus filiales, incluidas, entre otras, obligaciones de NXGEN o de sus filiales frente al lector.

Las obligaciones de NXGEN y de sus filiales respecto de los productos o servicios de NXGEN adquiridos por un cliente se rigen exclusivamente por los términos del contrato en virtud del cual se adquirieron dichos productos o servicios.

Para mayor claridad

El lector asume todo el riesgo en cuanto al uso, los resultados y el rendimiento de la Guía. En la máxima medida permitida por la ley aplicable, NXGEN rechaza y excluye todas las garantías, ya sean legales, expresas o implícitas — incluidas, entre otras, las garantías implícitas de comerciabilidad, idoneidad para un fin determinado, titularidad y no infracción de derechos de terceros — así como cualquier responsabilidad o garantía derivada de sugerencias, especificaciones o muestras relacionadas con la Guía.

Formación administrativa

Updated 14 August 2026

Qué abarca la formación administrativa

La Formación Administrativa guía a los nuevos administradores por todo lo necesario para desplegar, configurar y mantener GCXONE — desde el primer inicio de sesión hasta las rutinas operativas diarias. Esta guía cubre los requisitos de red, la configuración de la arquitectura del sistema, las tareas previas al lanzamiento y las cadencias de monitorización continuas.

Por qué importa

Un despliegue mal configurado — roles ausentes, sitios no mapeados o estado de salud de la cámara no revisado — genera fallos operativos difíciles de rastrear a posteriori. Seguir la ruta de formación estructurada garantiza que cada administrador parte de una base sólida y validada.

Cómo funciona

Pre-despliegue: Requisitos de navegador y red

Requisitos del navegador:

NAVEGADOR	NIVEL DE APOYO
Google Chrome v90+	Óptima (recomendada)
Mozilla Firefox v88+	Apoyado
Microsoft Edge v90+ (Chromium)	Apoyado
Apple Safari v14+	Limitada
Internet Explorer (cualquier versión)	Bloqueado. No soportado

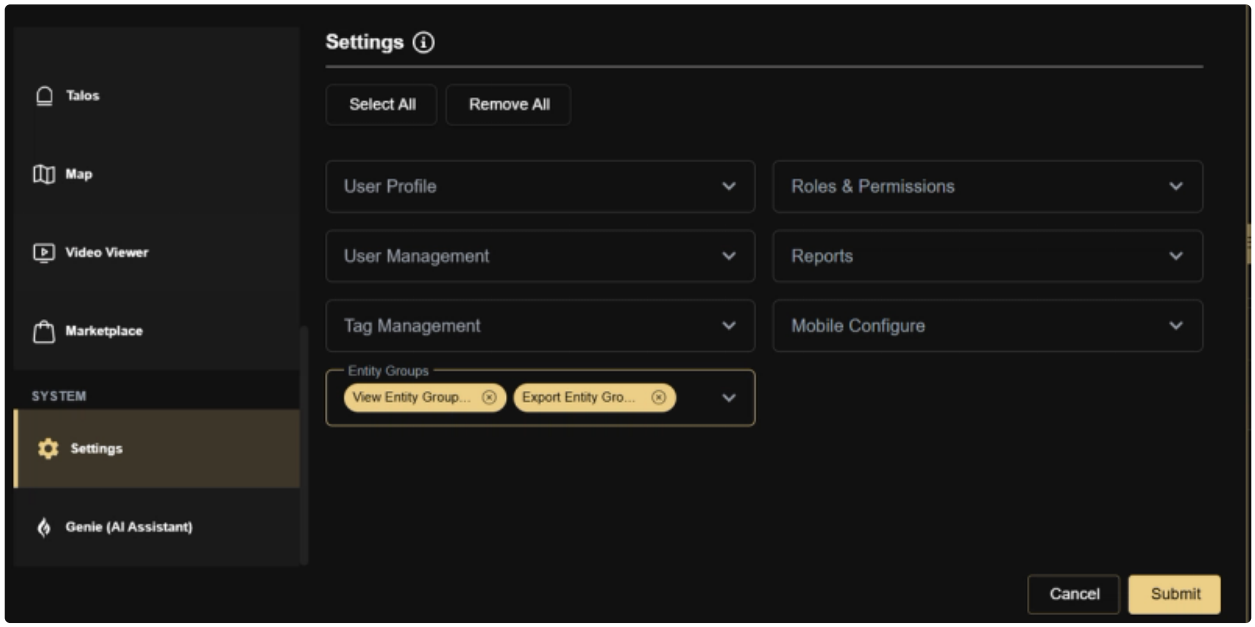
Requisitos de cortafuegos y puertos:

PUERTO	DIRECCIÓN	PROPÓSITO
443 (HTTPS)	Cliente → Nube	Interfaz básica
554 (RTSP) / 443	Bidireccional	Flujos RTSP o negociación de WebRTC
8000 / 80	Dispositivo → Nube	Nodos de eventos HTTP Hikvision/ISAPI
Protocolo DC09	GCXONE → CMS	Reenvío de receptores de alarma externos

> Note
>
> i INFO — Lista blanca de IP: Para redes corporativas seguras, GCXONE proporciona rangos de bloques CIDR. Estos rangos son críticos para hardware de puente de borde y deben ser incluidos en la lista blanca antes de la puesta en funcionamiento.

Ruta de Incorporación de Super Admin

1. Recibir correo de invitación — El despacho de NXGEN envía una invitación de bienvenida al correo de negocios del Super Admin desde `no-reply@nxgen.cloud`.
2. Confirmar dirección de correo electrónico — Haz clic en Confirmar correo electrónico para validar el dominio. Esto mitiga errores de enrutamiento y bloquea el esquema de usuario contra la suplantación.
3. Establecer contraseña criptográfica — Haz clic en el token de Configuración de Contraseña. Esta carga útil expira exactamente 24 horas después de su emisión.
4. Autenticar — Regresar a la URL de tu inquilino. Inicia sesión con credenciales establecidas. Los operadores multi-inquilino verán un selector de organización.



cfb5864a6a30a9e5e507a125b016e562beae6576-1435x711

Establecimiento de la arquitectura del sistema

1. Definir la información del proveedor de servicios — Establecer la marca raíz de la organización, la ubicación regional, las zonas horarias operativas y las variables de contacto SOC. Navegación: Configuración → proveedor de servicios
2. Crear entidades de cliente — Mapea a tus clientes o divisiones internas. Para 100+ entidades, utiliza el framework CSV de BulkImport. Navegación: Configuración → clientes
3. Sitios de despliegue — Definir restricciones geográficas únicas y vincular cada sitio con su cliente correcto. Navegación: Configuración → Sitios
4. Dispositivos de registro — Añadir puentes, NVRs o nodos directos a la nube con definiciones y credenciales correctas de endpoint. Navegación: Configuración → Dispositivos

Cuatro tareas críticas previas al lanzamiento

Note

⚠ ADVERTENCIA — Configurar roles antes de invitar a usuarios: Un usuario invitado sin un rol asignado aparece en una pantalla bloqueada en el momento en que inicia sesión y permanece bloqueado hasta que un administrador le asigna manualmente un rol. Diseña la estructura de tu rol, crea los roles y luego invita a los usuarios.

1. Configurar roles antes de invitar a usuarios — Crea toda la estructura de tu rol antes de enviar cualquier invitación de usuario.

- Super Admin — acceso completo, solo interno.
- Operador — cola de alarma, visor de vídeo, mapa.
- Instalador — configuración del dispositivo, limitada a los sitios asignados.
- Usuario final / Visor de clientes — solo panel de control y vista en vivo.

1. Configurar el sistema de gestión de alarmas — Configura tu integración con el CMS antes de que cualquier sitio se active en monitorización. Las alarmas generadas por sitios no cartografiados no tienen destino y se descartan silenciosamente. Mínimo: conexión DC-09 verificada (verde), todos los sitios activos asignados a un ID de cuenta CMS y al menos una alarma de prueba confirmada en CMS.
2. Habilitar HealthCheck en todos los sitios — HealthCheck debe estar suscrito antes de que las cámaras se activen — no puede capturar eventos retroactivamente. Recomendado: Suscribirse a nivel de cliente con Incluir hijos activado. Navegación: Configuración → [Cliente] → pestaña de análisis → Revisión de estado de la cámara
3. Crear al menos un informe programado — Los informes mensuales de HealthCheck SLA sirven como evidencia verificable de tiempo de actividad para los clientes. Configura el calendario antes de la puesta en marcha para que el primer ciclo capture los datos de referencia. Navegación: Configuración → informes → + Crear nuevo horario

Capacidades clave

Lista de verificación de validación de despliegue

PUNTO	ÁREA
Reglas de firewalls	enrutamiento y NAT verificadas
Inicio de sesión Super Admin operativo	Control de acceso
Topología mínima de cliente/sitio mapeada	Topología
Primer nodo de hardware conectado y en streaming	Ingestión
Alarma de prueba recibida en Talos/DC09	Entrega
Motor HealthCheck activo en el nodo 1	Diagnóstico

Flujos de trabajo orientados a eventos

El nuevo sitio se pone en marcha:

1. Crea la entidad del sitio bajo el Cliente correcto.
2. Registra los dispositivos y confirma que aparecen en línea.
3. Mapea el sitio en AMS (establece el ID de cuenta DC09 o la sincronización de Talos).
4. Activa HealthCheck a nivel de sitio o dispositivo.
5. Envía una alarma de prueba y confirma la recepción en CMS.
6. Asigna cualquier acceso de usuario específico del sitio mediante selección de entidad de rol.

La cámara se desconecta:

1. Consulta el código diagnóstico en el tablero de HealthCheck.
2. Si es tiempo de espera de red: verifica las reglas de conexión física y del cortafuegos.
3. Si se detecta sabotaje: técnico de despacho.
4. Si Calidad de imagen — Iluminación: comprueba IR/iluminación en el sitio.

5. Registra el incidente en tu sistema de tickets con una captura de pantalla de HealthCheck como prueba.

Alarma que no llega al CMS:

1. Abierto Marketplace → Sistema de Gestión de Alarmas.
2. Confirma que la tarjeta AMS muestra el estado verde.
3. Abre la tabla de mapeo AMS — busca filas rojas (sitios no mapeados).
4. Para filas rojas: haz clic en Editar, verifica que el ID de cuenta DC09 coincida exactamente con CMS (distinto de mayúsculas y minúsculas).
5. Ejecuta una alarma de prueba desde el lugar afectado.
6. Si sigue fallando: revisa las reglas del firewall para la IP y el puerto del receptor DC09.

Problema de acceso a los informes de usuarios:

1. Navegar a Configuración → usuarios → [Usuario].
2. Revisa su puesto asignado.
3. El rol de verificación tiene activado el módulo requerido (por ejemplo, Visor de vídeo).
4. Comprobar el acceso de la entidad — confirmar que el Cliente/Sitio relevante está incluido.
5. Utiliza Editar Acceso a la Entidad en el registro de usuario para ajustes por usuario sin cambiar el rol compartido.

Casos de uso en el mundo real

- Un nuevo administrador completa la incorporación completa — inicio de sesión de Super Admin, arquitectura del sistema y la primera alarma de prueba — en un solo día utilizando esta ruta de formación.

- Un administrador completa la Lista de Verificación de Validación de Despliegue y detecta una suscripción faltante a HealthCheck antes de que el sitio se active.
- Un administrador sigue el flujo de trabajo Cámara Se Desconecta e identifica un código de Sabotaje Detectado — envía a un técnico antes del turno de la mañana.
- Un nuevo operador inicia sesión y ve una pantalla bloqueada: el administrador lo rastrea inmediatamente hasta una asignación de rol faltante y lo resuelve en minutos.

Mejores prácticas

- Configura siempre los roles antes de invitar a cualquier usuario: un usuario sin rol es bloqueado inmediatamente al iniciar sesión.
- Completa la Lista de Verificación de Validación de Despliegue antes de que cualquier sitio se active en monitorización.
- Activa HealthCheck a nivel de cliente con Incluir a los niños — esto prepara la incorporación automática de nuevos sitios para el futuro.
- Ejecuta una alarma de prueba después de que cada nuevo sitio esté en funcionamiento — nunca des por hecho que la entrega está funcionando.
- Sigue las cadencias Diaria y Semanal de forma constante: la mayoría de los fallos operativos se detectan durante las revisiones rutinarias, no en la respuesta a incidentes.

Detalles adicionales

Cadencia diaria de monitorización

- KPIs del salpicadero — Pico inusual en el total de alarmas; recuento elevado de cámaras poco saludables.
- Ratio real vs. falsa alarma — Una fuerte caída en el porcentaje real de alarma puede indicar que la IA está sobrebloqueando.

- HealthCheck Board — Cualquier cámara nueva Crítica Offline o Detectada por Sabotaje.
- Estado de la conexión AMS — Verde = reenvío; rojo = alarmas que no llegan al CMS.
- Cola de alarma obsoleta — Las alarmas no reconocidas que tienen más antigüedad que la ventana de turno necesitan seguimiento.

Cadencia Operativa Semanal

- Revisa la lista de cámaras offline — Escala las cámaras fuera de línea > 48 horas al contacto del sitio.
- Auditar las invitaciones de nuevos usuarios — Confirmar que todas las invitaciones pendientes han sido aceptadas.
- Revisa los registros de entrega de informes — Las entregas fallidas indican problemas de enrutamiento de correos.
- Revisa el registro de auditoría para detectar anomalías — Busca cambios inesperados en los roles o ediciones masivas de configuración.
- Validar mapeos de sitios DC-09 — Cualquier fila roja en el mapeo AMS = alarmas no enrutadas.