

Instalación y operaciones

Edición en español · 26 de septiembre de 2026

UIC Home 3.9.14-dev · xTMSAgent · .NET 8 · SQL Server

Contenido

1. Alcance y preparación / 2
2. Instalar el servidor Windows / 3
3. Puertos, TLS y secretos protegidos / 4
4. Registrar terminal e instalar UIC Home / 5
5. Inscripción de desarrollo por USB / 6
6. Permisos Android y aceptación / 7
7. Panel, flota y operaciones remotas / 8
8. Rotar el secreto del dispositivo / 9
9. Certificados IoT: aprovisionar, rotar, revocar / 10
10. Biblioteca y distribución de aplicaciones / 11
11. Esquemas, catálogos y parámetros / 12
12. Mantenimiento y solución de problemas / 13
13. Cuenta, recuperación de contraseña y MFA / 14
14. Manuales de integración y ubicaciones históricas / 15

1. Alcance y preparación

Esta guía describe el sistema implementado con UIC Home 3.9.14-dev (código de versión 27) y xTMSAgent. NEWPOS NEW9810, NEXGO N82 y UIC A10-T se han probado contra el portal; cada firmware de producción todavía requiere calificación formal. Los APK y claves de desarrollo no son credenciales de producción.

El banco es el cliente. SuperAdmin crea clientes, registra modelos y dispositivos y rota credenciales. Los administradores de cliente operan dentro de su banco. Seleccione el cliente correcto antes de modificar datos.

Prepare Windows x64, entornos .NET 8 y ASP.NET Core 8, una base SQL existente, DNS accesible, certificados TLS y respaldos protegidos. No se requiere IIS, SDK de .NET ni Windows Desktop runtime. Mantenga los parches aprobados. El paquete del servidor no compila, configura ni instala aplicaciones Android.

La inspección de APK está incluida y se ejecuta dentro del proceso .NET. No requiere instalar Android SDK ni Java. La inscripción de agentes en producción, el análisis de malware y la validación de cada firmware siguen siendo requisitos previos al despliegue.

Registre nombres, puertos, rutas, vencimientos y responsables. Guarde secretos en una bóveda autorizada, nunca en capturas ni en esta guía.

2. Instalar el servidor Windows

1. Ejecute `dotnet --list-runtimes`. Confirme `Microsoft.NETCore.App 8.x` y `Microsoft.AspNetCore.App 8.x`.
2. Cree por separado la base SQL y el usuario. Valores predeterminados: `UICConnectTMS` y `app_uic_tms`. La instalación necesita permisos de migración; los servicios, permisos de aplicación. El instalador no crea base ni usuario SQL.
3. Compare `Get-FileHash <paquete.zip> -Algorithm SHA256` con la suma suministrada. Extraiga el paquete completo en una carpeta temporal.
4. Ejecute `Configure.cmd` como administrador. Mantenga juntas las carpetas `setup` y `payload`. Configuración: `C:\ProgramData\UICConnectTMS`; instalación: `C:\Program Files\UICConnectTMS`.
5. Ingrese servidor SQL, base, autenticación y contraseña. Cifrado SQL es `true` por defecto; Confiar en el certificado es `false`. Prefiera un certificado SQL confiable.
6. Configure conexiones, certificados y almacenamiento. Las bibliotecas de inspección APK están incluidas; no configure rutas Java ni SDK.
7. Cree el administrador inicial solo para una base nueva, con contraseña de al menos 12 caracteres. Se conservan usuarios existentes. Seleccione `instalar/iniciar servicios`.
8. Abra los puertos HTTPS/MQTT necesarios en el firewall; el instalador no crea reglas. Ingrese a `https://<servidor>:5102` o al puerto configurado.

Con `Get-Service` confirme `Running` en `UICConnectTMS.DataService`, `UICConnectTMS.Mqtt` y `UICConnectTMS.Portal`. Iniciar servicios no demuestra por sí solo conectividad con terminales.

`Enter` conserva valores y contraseñas existentes. Las contraseñas se ocultan y nunca se muestran como valores predeterminados. Al actualizar, seleccione el mismo directorio de configuración.

3. Puertos, TLS y secretos protegidos

Componente	Valor de producción
HTTPS del portal y escritorio remoto	5102, TLS externo
MQTT	5883, TLS mutuo
HTTP del portal	15100, solo local
gRPC HTTP/2 interno	15101, solo local
Sesión remota / admisión / concurrencia	10 minutos / 120 segundos / 100

El relay remoto se ejecuta dentro del portal. No se instala el proxy antiguo por separado. Los límites de sesión son configurables, no garantías de capacidad medida.

Seleccione `pfx`, `machine` o `user` para el certificado del servidor. PFX requiere ruta y contraseña. Machine/User busca en Personal (My) por CN exacto o nombre descriptivo. Seleccione la coincidencia numerada y revise vigencia, clave privada y SAN del servidor. User corresponde a la cuenta que ejecuta el instalador elevado.

La selección desde almacén requiere clave privada exportable y crea una copia PFX cifrada para LocalService. La renovación no es automática: ejecute nuevamente la configuración. Un certificado autofirmado requiere confianza explícita. No desactive validación para resolver errores de nombre o confianza.

El certificado TLS del servidor, la CA IoT y la firma APK cumplen funciones distintas. El instalador crea una CA IoT independiente. Ingrese su clave común de 64 caracteres hexadecimales en el campo oculto y entréguela solo mediante inscripción protegida.

Las credenciales SQL y otros secretos se cifran en `runtime.secrets.dpapi`, con DPAPI vinculado al equipo y permisos restringidos. Copiar solo ese archivo a otro servidor no funciona: configure de nuevo e ingrese secretos. Respalde juntos base, archivos, TLS y CA IoT. No distribuya archivos `.local` de desarrollo.

4. Registrar terminal e instalar UIC Home

1. Como SuperAdmin, abra Administración. Cree/seleccione el banco y su administrador inicial.
2. Agregue modelo con Marca, Modelo y SO (Android o Linux). Registre el terminal bajo ese cliente y modelo.
3. Use la serie de la etiqueta del fabricante, no la serie interna Android. Son diferentes en el NEW9810 verificado.
4. Guarde la inscripción mostrada una sola vez: ID, secreto del dispositivo, cliente, época de asignación y prefijo MQTT. La pantalla aún puede llamar Contraseña/Password al secreto. El servidor solo conserva su hash.
5. Complete la configuración con servidor MQTT accesible, puerto TLS, URL HTTPS, certificado confiable y clave común IoT. Sincronice la hora; el aprovisionamiento tolera dos minutos de diferencia.
6. Instale el APK UIC Home aprobado para la marca. Conserve su firma para actualizar. El paquete NEWPOS de desarrollo es `com.uic.tms.home.uic.newpos.debug`; producción y otras variantes pueden diferir.

Límite actual: la importación privada por archivo Android es exclusiva de debug. Instalar un APK release no configura el terminal. Producción necesita un canal aprobado de aprovisionamiento. Siga el manual de integración Android para instalar desde memoria interna o USB/OTG, inscribir, revisar restricciones y ejecutar la aceptación.

Para instalación USB de desarrollo, autorice la estación, ejecute `adb devices -l`, seleccione la serie exacta y use `adb -s <serie> install -r <UIC-Home.apk>`. La opción `-r` conserva datos. No desinstale ni borre almacenamiento en actualizaciones normales.

5. Inscripción de desarrollo por USB

Este procedimiento es para terminales de desarrollo autorizados, no para inscribir versiones de producción. ADB se utiliza en la estación de aprovisionamiento, no en el servidor TMS.

Prepare un JSON protegido con `deviceId`, `password` (secreto), `customerId`, `serial`, `assignmentEpoch`, `topicPrefix`, `host`, `port`, `packageBaseUrl`, `serverCertificate` (PEM) e `iotBootstrapKey`. Use valores reales del administrador. El nombre técnico sigue siendo `password`.

Transfiera el JSON por ADB run-as a `files/tms-enrollment.json` dentro del espacio privado de la app. Envíe bytes por entrada estándar, no secretos como argumentos ni mediante almacenamiento compartido. El comando receptor se muestra abajo; un script debe suministrar el JSON protegido por su entrada estándar.

```
adb -s <serie> shell run-as <paquete> sh -c 'cat > files/tms-enrollment.json'
```

Reinicie UIC Home. El importador debug cifra la inscripción mediante `AndroidKeyStore` y elimina la entrada sin cifrar. Confirme que existe `tms-enrollment.enc` y desapareció el JSON. Inicie `com.uic.home.LauncherActivity` en el paquete instalado y revise la conexión.

Solo para el laboratorio USB actual, se utiliza `localhost`, MQTT 18883 y HTTPS `https://localhost:15102`. Se necesitan ambos mapeos:

```
adb -s <serie> reverse tcp:18883 tcp:18883
adb -s <serie> reverse tcp:15102 tcp:15102
```

Los mapeos desaparecen al desconectar USB. Producción usa un servidor realmente accesible y sus puertos, normalmente 5883/5102. Una prueba USB no demuestra conectividad independiente.

Desinstalar, Borrar almacenamiento y ciertas limpiezas de pruebas Gradle eliminan inscripción y claves privadas. Evite ese ejecutor en terminales inscritos; la instrumentación directa puede conservar la app. Perder claves requiere reinscripción y rotación IoT.

6. Permisos Android y aceptación

Seleccione UIC Home como aplicación de inicio y pulse Inicio. Wi-Fi y Celular no requieren código. Ajustes Android utiliza un código UIC Home de seis dígitos; el predeterminado de desarrollo es 896345. Cámbielo antes de entregar el terminal. No es el secreto del dispositivo.

Seleccione Permitir conexión con pantalla apagada y acepte Permitir en Android. El agente ya usa servicio persistente en primer plano, reconexión y bloqueo parcial limitado de CPU. La exención adicional permite mantener la red durante Doze. Valide políticas del fabricante.

El aprovisionamiento USB autorizado puede aplicar y verificar la exención:

```
adb -s <serie> shell dumpsys deviceidle whitelist +<paquete>
adb -s <serie> shell dumpsys deviceidle whitelist
```

Habilite UIC remote input en Accesibilidad y acepte Android para permitir toques/deslizamientos remotos. La captura sigue requiriendo aprobación en cada sesión. Conceda permisos de ubicación si se necesita; soportar GPS no garantiza señal en interiores.

Lista de aceptación:

- Certificado IoT Aprovisionado, dispositivo En línea, telemetría reciente y serie/modelo correctos.
- Apague la pantalla, espere más que el intervalo de estado del portal, envíe un mensaje de prueba y verifique encendido y Correcto. Significa mostrado, no leído.
- Solicite estado y confirme un reporte nuevo. Pruebe Inicio, Wi-Fi y Celular.
- Solicite asistencia remota, apruebe localmente, verifique un toque real y finalice la sesión.
- Después de configurar una conexión real, desconecte USB y verifique funcionamiento independiente.

7. Panel, flota y operaciones remotas

Panel es la página inicial con contadores y Comandos recientes. Dispositivos combina filtros por serie, grupo/subgrupo, etiquetas, modelo y estado. Los grupos incluyen descendientes. Use Grupos y etiquetas para jerarquías/asignaciones y Administración para modelos.

Resumen presenta identificadores del terminal/red, organización, almacenamiento libre y total, memoria disponible y total, y ubicación. La falta de IMEI, ICCID, MAC o coordenadas puede obedecer a hardware o restricciones del SO. Las coordenadas reportadas crean un punto histórico solo después de un movimiento mínimo de 100 metros. Si el dispositivo nunca reportó una posición válida, un operador autorizado puede fijarla por dirección, pin o coordenadas; un reporte posterior del dispositivo reemplaza esa ubicación manual. Diagnóstico muestra telemetría técnica.

Operaciones incluye Enviar mensaje, Reiniciar, Solicitar estado y Asistencia remota. Los botones dependen de En línea y capacidades. Enviar mensaje abre un diálogo; Reiniciar pide confirmación. Revise Comandos recientes: En cola o Enviado no significa completado. Fallido o Caducado requiere investigación, no envíos repetidos.

Los mensajes encienden la pantalla sin evitar un bloqueo seguro Android. Reiniciar necesita firmware compatible. El visor requiere consentimiento local. Solo lectura indica que falta entrada remota: habilite UIC remote input. Use maximizar/pantalla completa y Finalizar sesión. No se graba; reiniciar el portal finaliza sesiones y exige una solicitud nueva.

8. Rotar el secreto del dispositivo

Es la credencial exclusiva del terminal, distinta del código Home, cuenta del portal, contraseña SQL y certificado IoT.

1. Prepare cómo actualizar la inscripción antes de rotar. El secreto nuevo no se entrega automáticamente por la conexión anterior.
2. Como SuperAdmin, abra Dispositivos > terminal > Operaciones > Administración de credenciales. Expanda Rotar secreto del dispositivo y lea el aviso.
3. Seleccione Rotar secreto del dispositivo. Cambia la credencial y cancela comandos pendientes. No lo use como prueba inocua de conexión.
4. Guarde la inscripción nueva mostrada una sola vez. Puede aparecer como Contraseña/Password. Salir sin guardarla puede exigir otra rotación.
5. Actualice la inscripción privada con secreto y vinculación devueltos, conservando conexiones, confianza y clave común. Reinicie/reconecte mediante el proceso autorizado.
6. Confirme En línea y telemetría reciente. Revise trabajo cancelado y recree solo tareas necesarias.

Cambiar únicamente el portal deja al terminal con una credencial inválida. Si también perdió su clave privada IoT, rote el certificado. No es posible recuperar el secreto desde su hash.

9. Certificados IoT: aprovisionar, rotar, revocar

UIC Home genera la clave privada en AndroidKeyStore. Envía solo la pública por HTTPS autenticado, descarga un certificado firmado y demuestra posesión. La confirmación cambia a Aprovisionado y bloquea nuevas descargas. MQTT exige certificado y credencial correcta.

Abra Dispositivos > terminal > Operaciones > Administración de credenciales > Certificados IoT. El cliente limita visibilidad; SuperAdmin rota/revoca. Emitido significa confirmación pendiente. Aprovisionado permite MQTT. Revocado permanece en historial y no puede reconectar.

Para rotar, seleccione Rotar certificado y confirme. Se revoca el anterior y se habilita emisión nueva. Un agente bien inscrito reintentará, genera clave/certificado y confirma. Verifique huella Aprovisionada nueva, anterior Revocada, En línea y telemetría. Si se borraron datos, restaure también la inscripción.

Para revocar, seleccione Revocar certificado y confirme. Invalida certificados existentes y bloquea descargas futuras. Úselo para terminales perdidos/retirados. No hay recuperación automática: una rotación explícita reabre emisión. El broker consulta el registro de revocación para conexiones nuevas y activas.

Controle vencimientos y rote antes de caducar. No se implementaron renovación automática, rotación de CA ni publicación CRL/OCSP. Respalde juntos clave privada CA, configuración y base de datos. Restaurar revocaciones antiguas puede recuperar autorizaciones obsoletas.

10. Biblioteca y distribución de aplicaciones

Seleccione primero el archivo. El portal muestra progreso y extrae paquete, nombre, versión e icono disponible. APK admite modelos Android solamente. Asocie todos los modelos compatibles con ese binario. Otro APK puede cubrir modelos distintos de la misma aplicación.

Guarde la compilación validada, revise versiones/integridad y libérela antes de distribuir. Compare SHA-256 de firma con versiones anteriores; el hash del archivo cambia, la firma debe ser compatible. Verificar firma no analiza malware. Producción requiere análisis/aprobación.

Cree la distribución eligiendo compilación liberada y terminales. Fecha UTC vacía inicia ahora; para programar, indique fecha futura. Defina ventana, revise destinos elegibles/excluidos y confirme. Terminales desconectados pueden recibir dentro de la ventana. Cancelar afecta cola, no una instalación enviada.

Progreso de entrega muestra cada distribución en una fila con aplicación, fecha de creación, estado general, cantidad de destinos, correctos, fallidos y pendientes. Seleccione Detalles para revisar dispositivos individuales y buscar por número de serie o modelo. Actualizar renueva los estados y contadores sin recargar la página.

En Aplicaciones del terminal, Enviar aplicación selecciona app/versión y opcionalmente Iniciar después de instalar. Inventario muestra apps de usuario y nombres/paquetes, excluyendo sistema. Desinstalar pide confirmación y no está disponible para UIC Home. Después de confirmar una instalación o eliminación, la página muestra el estado de la tarea, solicita un reporte nuevo al terminal cuando finaliza correctamente y actualiza el inventario automáticamente.

Enviado no significa instalado. El agente descarga por HTTPS autenticado y verifica antes de confirmar. xTMSAgent instala y elimina paquetes nativos A10 aprobados, reporta el inventario desde `user app l` y reinicia después de una instalación o eliminación confirmada. UIC Home instala APK Android solamente. Consulte el manual de integración Linux; las instrucciones formales de instalación en campo para A10-T se agregarán en una versión posterior.

11. Esquemas, catálogos y parámetros

Abra Parámetros, seleccione banco y cree/importe un esquema con nombre. Defina tablas/campos con una sola Etiqueta en el idioma del banco. Los controles tienen inglés/español; las etiquetas propias no se traducen. Use Terminal > Adquirente > Emisor y catálogos compartidos para hosts, rangos y EMV.

Guarde esquema y catálogos. Hay una configuración actual guardada, sin Publicar. Paquete y SHA-256 de firma son restricciones opcionales del consumidor; cada campo vacío omite solo esa restricción. Autenticación y aislamiento siguen activos. Los campos no son una bóveda; no se admiten claves de pago ni valores secretos/cifrados no vacíos.

Desde Parámetros del dispositivo, elija esquema, cree datos vacíos o desde plantilla, edite y Guarde. Seleccione referencias válidas. Filas de solo referencia tienen selector/eliminar; las ordinarias admiten duplicar. Eliminar requiere confirmación. Resuelva campos obligatorios y referencias desconocidas.

Guardar como plantilla y Copiar a dispositivo usan valores guardados. Las plantillas quedan independientes. Guarde primero y revise identificadores de terminal/comercio antes de copiar a un reemplazo, confirmando sobrescritura.

Cuando la app de pagos solicita un esquema mediante el proveedor de solo lectura de Home, se compilan esquema, catálogos y filas actuales al momento. Guardar habilita descarga; no prueba aplicación por la app. No hay envío programado de parámetros, alternativa sin conexión ni confirmación de aplicación.

12. Mantenimiento y solución de problemas

Antes de actualizar, respalde juntos SQL, archivos, configuración, TLS y CA IoT. Detenga los tres servicios, extraiga el paquete nuevo por separado, ejecute Configure.cmd con rutas existentes y conserve certificados. Verifique portal, conexión y una operación. No hay reversión automática; las migraciones pueden exigir restauración coordinada.

Síntoma	Revisión y recuperación
Sin conexión con pantalla apagada	Red, servicio, exención de batería, política del fabricante; mapeos USB reverse en laboratorio
Falla de aprovisionamiento IoT	Hora, confianza/nombre HTTPS, secreto, serie, época y clave común; rotar si se perdió la clave privada
Certificado revocado	Rotar explícitamente después de aprobar regreso a servicio
Remoto solo lectura / sin imagen	Accesibilidad para entrada; aprobación de captura y WebSocket seguro para imagen
Falla APK	Conservar bibliotecas incluidas; revisar firma, modelo/SO y firmware
No guarda parámetros	Obligatorios, padres, referencias actuales y ediciones concurrentes

No desactive TLS ni amplíe tiempos En línea para ocultar fallas. Para soporte registre IDs de dispositivo/comando, hora, versión y error; excluya secretos/claves. Pruebe restauraciones en un entorno separado.

Referencias técnicas: capítulos 02, 17, 27, 28 y 29 del conjunto de arquitectura. Comportamiento Android: <https://developer.android.com/training/monitoring-device-state/doze-standby>

13. Cuenta, recuperación de contraseña y MFA

El enlace Ayuda en el encabezado del portal abre este manual antes o después de iniciar sesión. Seleccione el nombre de su cuenta para abrir Mi perfil, actualizar su nombre o nombre visible, cambiar la contraseña y administrar la autenticación multifactor (MFA).

1. En la pantalla de acceso seleccione **¿Olvidó su contraseña?**, ingrese el correo de acceso y envíe la solicitud.
2. El portal siempre muestra la misma respuesta para no revelar si la cuenta existe. Cuando la recuperación por correo está habilitada y la cuenta está activa, se envía un mensaje bilingüe.
3. Abra el enlace HTTPS de un solo uso dentro de 30 minutos y establezca una contraseña de 14–128 caracteres. El restablecimiento revoca las sesiones existentes. El enlace no se puede reutilizar.

Si no llega el mensaje, revise correo no deseado y consulte si el administrador habilitó la recuperación por correo. Los administradores de cliente pueden asignar una contraseña nueva a los usuarios de su cliente; los SuperAdmin administran los usuarios de plataforma. Los administradores no pueden leer una contraseña existente.

1. Abra **Mi perfil > Autenticación multifactor > Configurar MFA**.
2. Agregue la clave mostrada a un autenticador TOTP compatible. El código cambia cada 30 segundos.
3. Ingrese el código actual de seis dígitos y su contraseña del portal. La configuración vence después de 10 minutos.
4. Guarde los diez códigos de recuperación en un gestor de contraseñas aprobado. Se muestran una sola vez y cada uno funciona una vez.

Los accesos siguientes requieren la contraseña y luego un código del autenticador o uno de recuperación sin usar. Cinco códigos fallidos o una espera de cinco minutos invalidan el desafío. Para deshabilitar MFA, ingrese la contraseña actual y un factor válido en Mi perfil. Recuperar la contraseña no deshabilita MFA.

La configuración de Windows registra la URL HTTPS pública y admite SMTP estándar o la API nativa AWS SES v2. SMTP requiere servidor, puerto, selección TLS, remitente y credenciales opcionales. AWS SES requiere una identidad de remitente verificada y una región; luego usa la cadena de credenciales predeterminada de AWS, como un rol de instancia EC2, o una clave de acceso dedicada con permiso `ses:SendEmail`. Las cuentas SES en modo sandbox solo pueden enviar a destinatarios verificados.

Las contraseñas SMTP, las credenciales AWS SES configuradas explícitamente y la clave de cifrado MFA se guardan únicamente en el archivo de secretos DPAPI vinculado al equipo. Conserve la misma configuración protegida durante actualizaciones. La auditoría registra solicitudes de recuperación, restablecimientos, habilitación y deshabilitación de MFA sin guardar contraseñas, tokens, claves de configuración ni códigos de recuperación.

14. Manuales de integración y ubicaciones históricas

Use el manual de integración Android para seleccionar el paquete UIC Home, instalar el APK desde USB/OTG o memoria del dispositivo, inscribir, entender la comunicación MQTT/HTTPS, permisos, restricciones y aceptación. Use el manual de integración Linux para alta de xTMSAgent, comunicaciones, inscripción, telemetría, inventario y paquetes nativos A10. El manual Linux no prescribe todavía el procedimiento futuro de instalación en campo del A10-T.

Ambos agentes exigen que el SuperAdmin cree la serie exacta bajo un modelo compatible antes de inscribir. El terminal no puede crear su propio registro. La primera conexión MQTT autenticada cierra la descarga de credenciales y marca el dispositivo aprovisionado para IoT. Una nueva inscripción requiere rotación o restablecimiento administrativo explícito.

El historial guarda cambios reportados o manuales solo cuando la distancia desde el último punto almacenado es de al menos 100 metros. La ubicación manual solo está disponible antes de una posición válida reportada por el equipo. Todo cambio manual queda auditado; la telemetría del dispositivo mantiene prioridad.