Protocolo de Configuración y Enrolamiento: Equipos Samsung (Android 16)

Manual Unificado de Verificación FENRIR / Workspace ONE

Uso Exclusivo Técnico

Arquitectura del Protocolo

Pre-Configuración en Plataforma MDM

- Control de Equipos de Reposición
- Gestión de Etiquetas (Sin perfiles)

Las 6 Fases Operativas (Dispositivo)

1. **Fase 1:** Actualización y Enrolamiento
2. **Fase 2:** Permisos de Misión Crítica
3. **Fase 3:** Optimización de Sistema
4. **Fase 4:** Hardware e Interfaz
5. **Fase 5:** Conectividad y Red
6. **Fase 6:** Verificación Final (POC)

ALERTA DE PROTOCOLO: Equipos de Reposición (Stock)

Antes de manipular cualquier permiso de forma manual en el teléfono, es de carácter OBLIGATORIO ejecutar los siguientes dos pasos:

Paso 1

1. Sincronizar el dispositivo físicamente con el MDM.

Paso 2

2. Verificar la fecha de la última actualización directamente desde la consola de la plataforma.

Gestión Serie L: Ciclo de Vida de la Etiqueta “Sin perfiles”

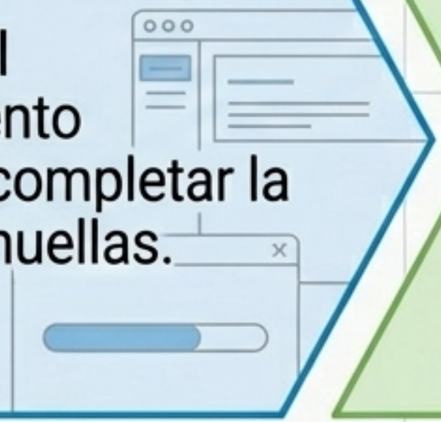
Aplica a Equipos L (Est L, Comunas, Samsung, Motorola).
Objetivo: Evitar que los perfiles se reinstalen automáticamente al apagar o reiniciar lequipos.

Fase A: ANTES

Colocar la etiqueta “Sin perfiles” en el MDM **antes de cualquier** configuración.

Fase B: DURANTE

Realizar el enrolamiento normal y completar la carga de huellas.



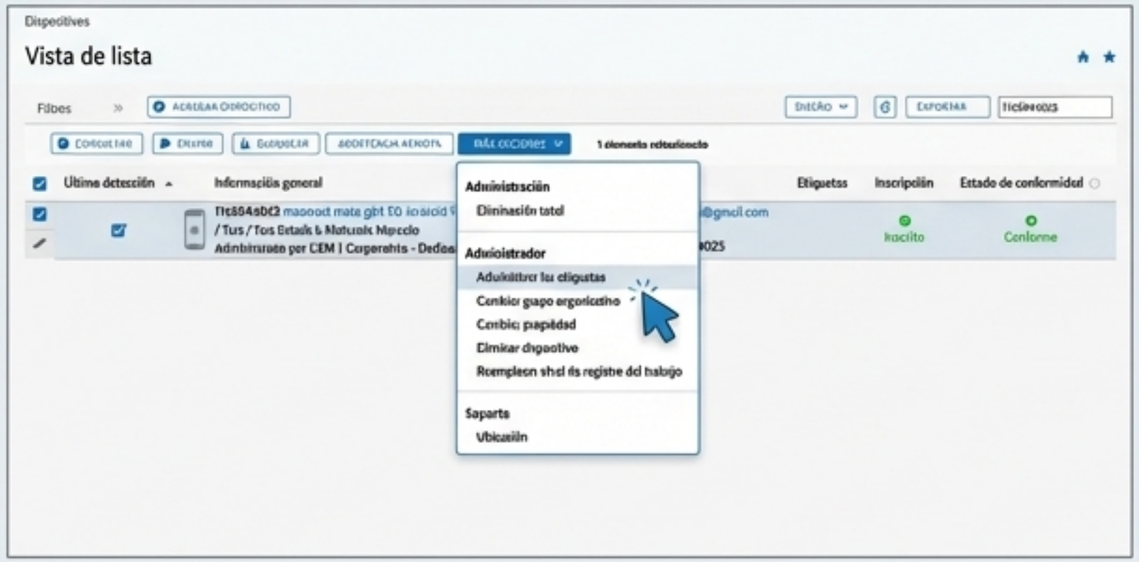
Fase C: AL FINALIZAR

Quitar la etiqueta del MDM para reactivar los perfiles automáticamente.

¡Atención! Al finalizar, se debe cotejar obligatoriamente que los perfiles figuren activos tanto en la plataforma como en el equipo.

Rutas en Consola MDM: Administrar las etiquetas

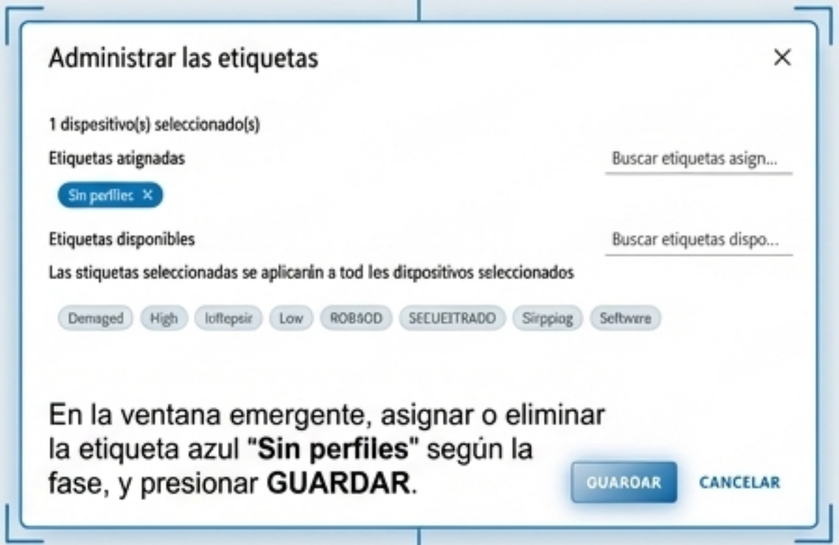
Ruta A: Desde Vista de Lista



1. Navegar a **Vista de lista**.
2. Seleccionar el dispositivo objetivo.
3. Desplegar menú superior **MÁS ACCIONES**.
4. Bajo **Administrador**, seleccionar **Administrar las etiquetas**.

Ruta B: Desde el Dispositivo

1. Entrar al detalle específico del dispositivo.
2. Clic en menú superior derecho **MÁS ACCIONES**.
3. Bajo **Administrador**, seleccionar **Administrar las etiquetas**.



Fase 1: Actualización y Enrolamiento

Formateo por **FENRIR** al último software.

¡NO usar HOME! El teléfono quedará bloqueado.

Escanear QR de carpeta PROV 5, inscribir y reiniciar **UNA SOLA VEZ.**

Limpieza MDM: Sacar Ajustes XML y Restricciones.

NUNCA desde el teléfono, siempre desde MDM.

Ingresar a Hub, dar “Entendido” y Sincronizar Dispositivo (acelera la salida de perfiles).

Conectar Wi-Fi e ingresar a PlayStore.

⚠ Cancelar TODAS las actualizaciones automáticas en curso primero. Luego actualizar/instalar.

Fase 2: Matriz de Permisos de Misión Crítica

Aplicación	Aparecer encima	Instalar apps desconocidas	Imagen en imagen	Cambiar ajustes de sistema
ASSIST (Dar Entendido primero)	✓	✓	✓	✓
HUB	✓	✓	✓	✓
SISEP	✓	✓	✓	✓
LAUNCHER	✓	✓	✓	✓

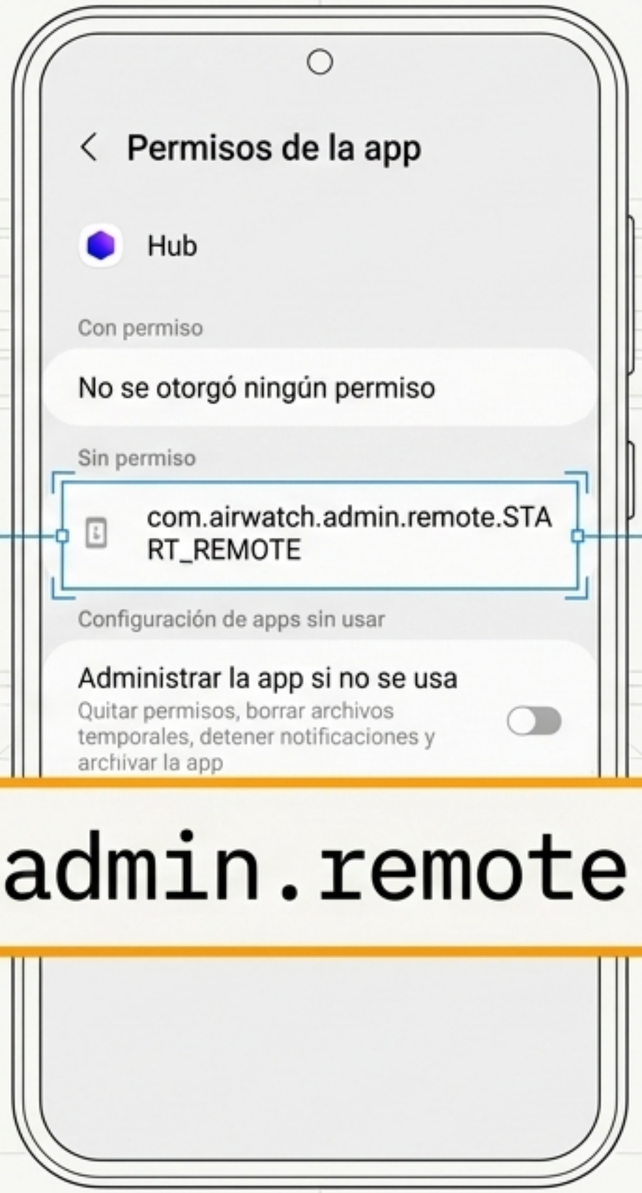
Configuración Launcher

En notificaciones, habilitar SOLO Launcher y desactivar el resto.

Configuración Maps / Ubicación

Seleccionar “Permitir todo el tiempo” para Hub, Launcher, Maps, y Sisep Mobile. Activar “Precisión de la ubicación” + Búsqueda por Wi-Fi y Bluetooth.

Fase 2 (Profundidad): El Permiso Exclusivo



- **Exclusividad:** Este permiso a nivel de código pertenece ÚNICA Y EXCLUSIVAMENTE a la aplicación Hub.

- **Función:** Garantiza la capacidad operativa para la asistencia y administración remota del dispositivo.

`com.airwatch.admin.remote.START_REMOTE`

- **Exclusividad:** Este permiso a nivel de código pertenece ÚNICA Y EXCLUSIVAMENTE a la aplicación Hub.

- **Acción Requerida:** Asegurar su validación manual en la sección de permisos de la app Hub para evitar puntos ciegos en el soporte.

Fase 3: Optimización (Bypass de Batería y Memoria)

El Bypass de Batería (Secuencia Exacta)

Paso 1: ACTIVAR temporalmente "Ahorro de energía".

Paso 2: DESACTIVAR todas las sub-opciones bloqueadas (Limitar CPU al 70%, Disminuir Brillo, etc.).

Paso 3: DESACTIVAR el "Ahorro de energía" general.

Blindaje de Memoria (Evitar Cierres)

Acción A: Desactivar "Suspender aplicaciones sin uso".

Acción B: En "Apps sin autosuspensión", agregar TODAS las apps con el botón "+".

Acción C: En "Memoria > **Aplicaciones excluidas**", agregar TODAS las apps con el botón "+".

Fase 4: Estandarización de Interfaz y Hardware

Sonido

Volumen

Configurado al Máximo (todas las barras).

Pantalla

Configuración Visual

- Desactivar "Brillo adaptable".
- Setear brillo fijo al 80/90%.
- App Brillo: Destildar Auto Close, Auto Rotate y Show Popup.

Bloqueo

Seguridad

Tipo: PIN. Código estandarizado:

0000

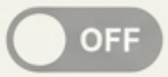
Botón Lateral

Funciones Avanzadas

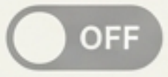
Pulsación larga configurada obligatoriamente para activar el “Menú Apagado”.

Fase 5: Conectividad y Verificación de Enrutamiento

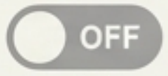
Desactivación de Redes



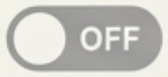
- **Apagar Wi-Fi** (y olvidar la red de enrolamiento).



- **Apagar** “Llamada Wi-Fi” y “Pagos NFC”.



- Redes Móviles: Apagar Roaming de Datos.



- Forzar Modo de red en 4G preferida.

Matriz de IP Crítica

Verificar Nombre de Punto de Acceso (APN): “Personal Datos” o “Movistar Internet”. Navegar a: **Acerca del teléfono > Información de Estado.**

Segmento IP	Red APN Asignada
10.86	APN TECO (Personal)
10.87	APN MOVISTAR
10.75	APN RESTRINGIDO

Fase 6: Proof of Concept (Verificación Final Operativa)

☐ **Validación de Línea** 	Realizar llamada saliente: Verificar número correcto y confirmar que la SIM no contenga contactos de equipos anteriores.
☐ **Disponibilidad SISEP** 	Permitir pop-ups solicitados. Realizar ciclo de prueba: Cambiar estado a "En Servicio" y retornar a "Franco".
☐ **Despliegue y Geolocalización** 	Verificar que la ubicación figure correctamente en el mapa. Seleccionar “Enviar Posición”. **(Nota: Si no carga o figura en la 9 de Julio, salir y reintentar).**
☐ **Identificación Criptográfica** 	Verificar que en el apartado ‘Identificación’, el Código GPS coincida exactamente con el IMEI físico del equipo.

Cierre de Protocolo: Certificación de Despliegue

El Último Reinicio

Reiniciar el equipo por última vez para asegurar que todas las políticas de MDM y configuraciones locales impacten correctamente a nivel kernel.

Verificado: MDM con permisos/perfiles gestionados (Serie L sin perfiles temporales).

Verificado: Equipo enrolado y reportando bi-direccionalmente en plataforma SISEP.

El dispositivo cumple con los estándares FENRIR y se encuentra 100% Operativo para su asignación.