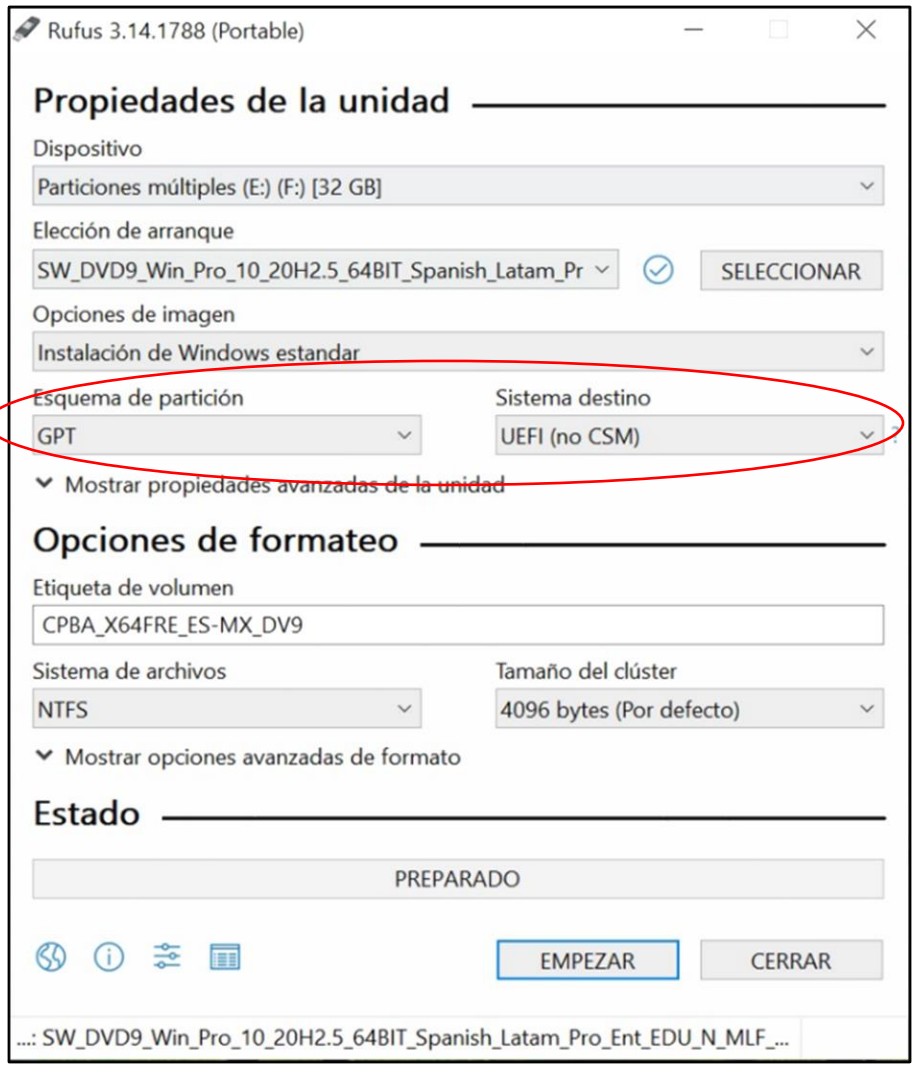
Requisitos previos de la instalación de la imagen de Windows

1. Contar con el archivo .ISO de Windows Enterprise en ingles

Crear USB Booteable (Arranque UEFI) utilizando RUFUS

Se realiza la creación de un usb booteable con los siguientes parámetros:

1. Esquema de partición GPT.
2. Sistema destino: UEFI (no CSM).



Creación de imagen “Máster” a dos capas de Windows 11

Se recomienda utilizar dos capas en el proceso de creación de imagen, constando de la siguiente información:

Capa 0

1. Sistema Operativo.
2. Controladores.
3. Actualizaciones.

Capa 1

1. Aplicaciones Internas.
2. Aplicaciones de Terceros.
3. Personalización y configuración de OS
4. Instalación de Agentes.

Creación de la capa 0

La creación de la capa 0 consta de las siguientes actividades:

1. Instalación del sistema operativo Windows 10 u 11
2. Cuando se reinicie por primera vez (Cuando pide el nombre de quien usara el equipo) presionar **ctrl + shift + f3** para ingresar en **modo audit.**
3. Instalación de controladores.
4. Descarga e instalación de actualizaciones para Windows 10.
5. Limpieza de unidad C:\ (huellas de configuración).
6. Captura de imagen (OPCIONAL).

Creación de la capa 1

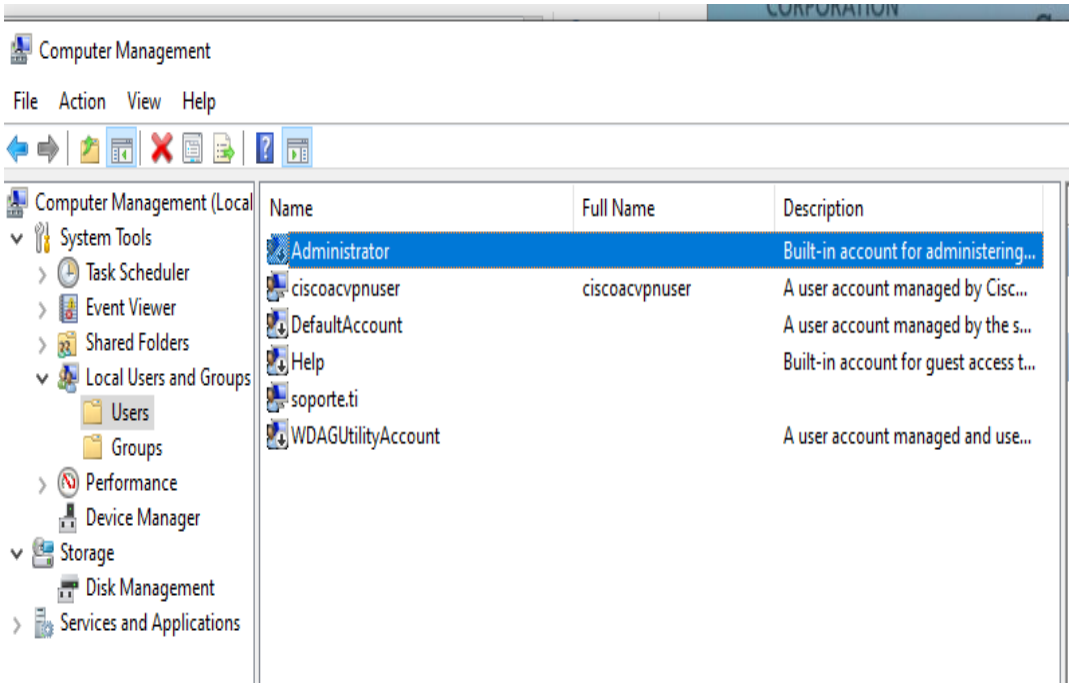
La creación de la capa 1 consta de las siguientes actividades:

1. Instalación de aplicaciones internas.
2. Instalación de aplicaciones de terceros (Office, Cisco, Chrome, webex, etc).
3. Personalización y configuración de OS.
4. Instalación de Agentes y solo copiar carpeta client de SCCm en c:\.
5. Configuraciones para el área de seguridad que consta de lo siguiente:

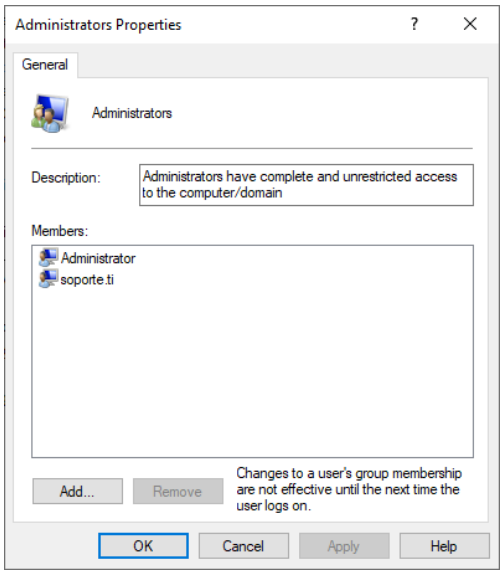
Usuarios dados de alta.

- El usuario **administrator** en el equipo de escritorio no se puede renombrar por problemas de compatibilidad, en las laptops de puso el nombre de **AgentPC**.
- El usuario **guest** se renombra por **Help**.

- Los únicos usuarios habilitados deberán ser **ciscoacvpnuser**, utilizado para la VPN, pero sin privilegios y **soporte.ti** que está asignado para el área de soporte a PC, este con privilegios de administrador.

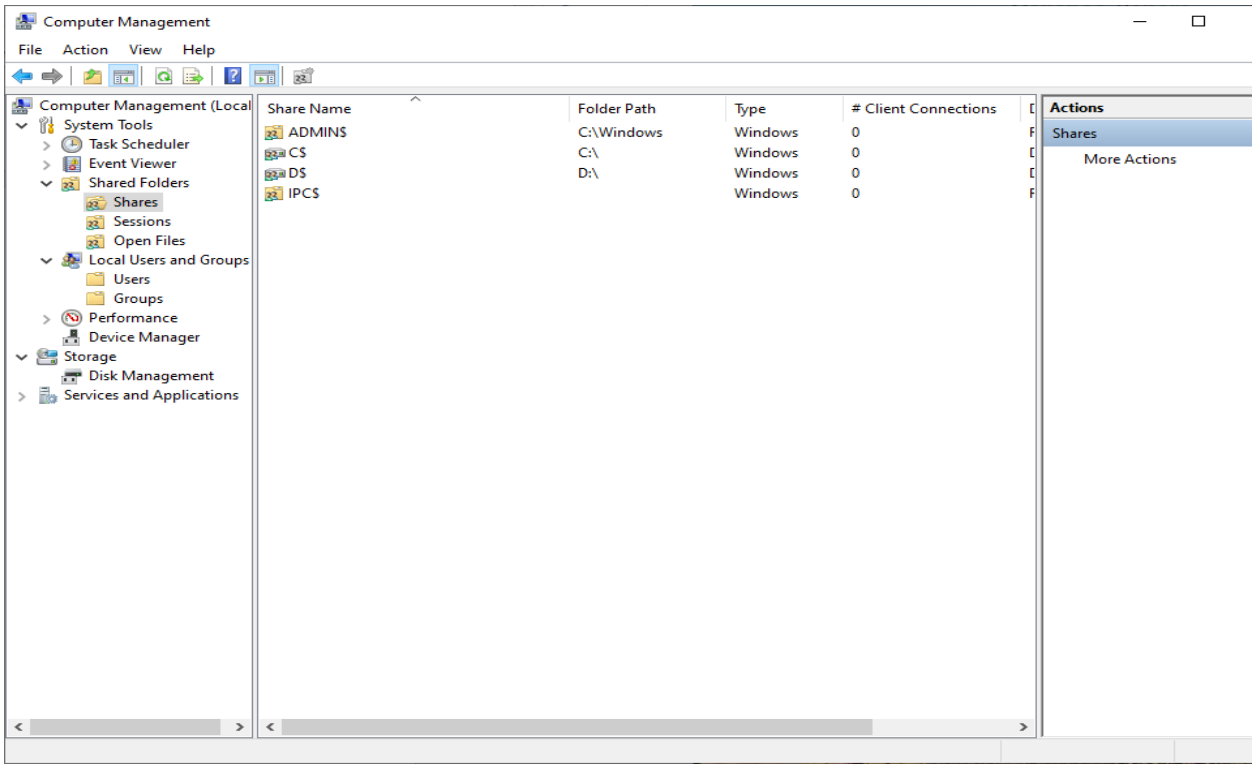


- Los usuarios que pertenecen al grupo de administrador sólo son administrator y soporte.ti.



- Los únicos recursos compartidos son los que trae el equipo por default ya que el deshabilitarlos puede generar un impacto en la operación.

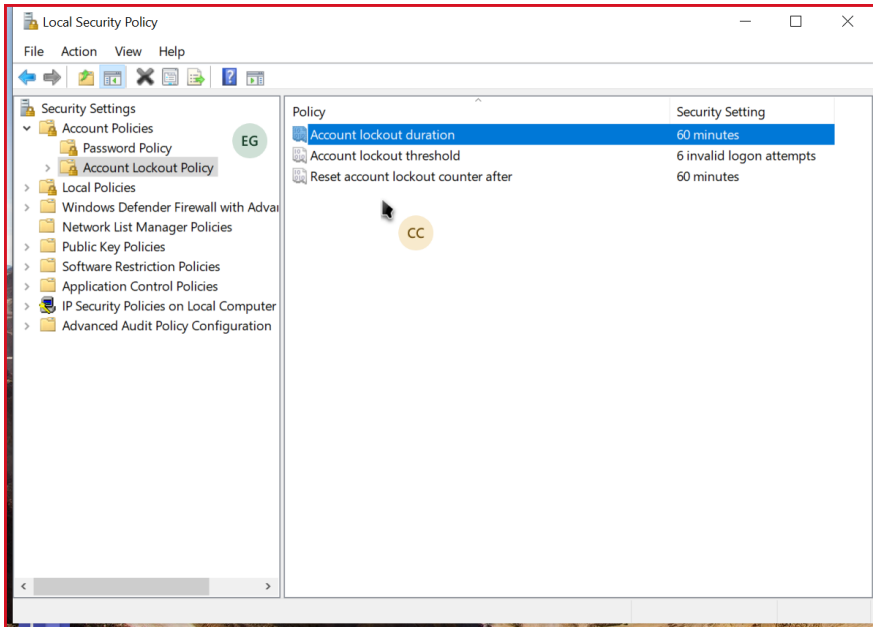
a. ADMIN$: Es un recurso que se utiliza durante la administración remota de un equipo.
b. IPC$: Es un recurso que comparte las canalizaciones con el nombre que debe tener para la comunicación entre programas. Este recurso no puede eliminarse.
c. C$ y D$: Se trata de un volumen o partición raíz compartido. Las particiones raíz compartido y volúmenes se muestran como el nombre de letra de unidad seguido del signo de dólar ($).



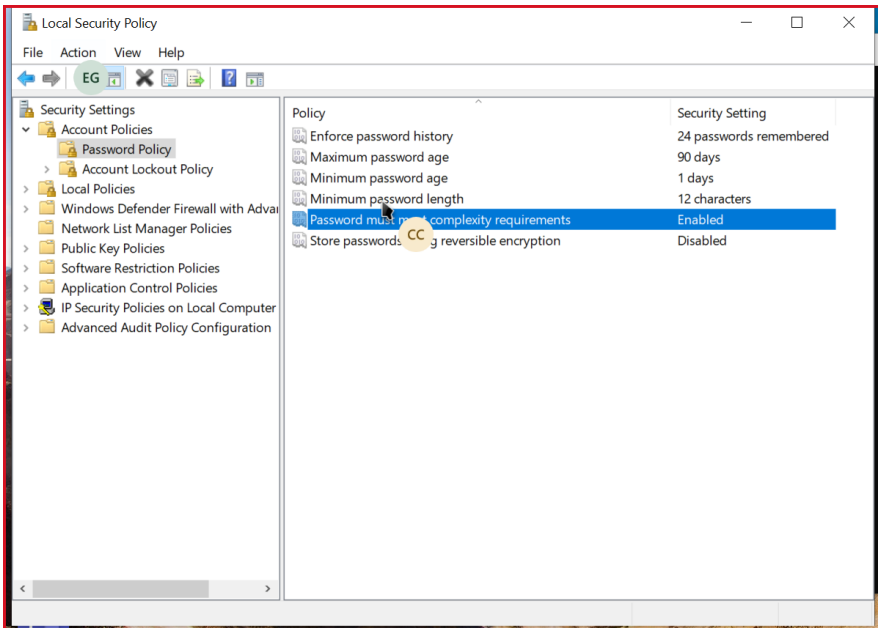
- Los logs de eventos tomarán de las políticas del Directorio Activo.

- Las políticas de contraseña y bloqueo de cuentas quedaran modificadas localmente con los siguientes valores.

POLITICAS DE CONTRASEÑAS:



POLITICAS DE BLOQUEO



6. Desactivar bitlocker.
7. Ejecución de generalización de imagen con Sysprep.

Ejecución de generalización de Imagen con Sysprep

- La generalización de la imagen con Sysprep, permitirá que esta pueda ser duplicada y garantizar que no existirá una duplicidad en los identificadores del equipo de referencia hacia todos los equipos duplicados generados con la imagen.
- La ejecución del comando Sysprep requerirá de la utilización de un archivo de respuestas o “Unattend.xml” el cual, en este momento, solo contiene la instrucción de que los drivers persistan después del Sysprep.
- Después de que el equipo de referencia ha reiniciado en modo Audit, se procede a copiar el archivo unattend.xml a la ruta **C:\Windows\System32\Sysprep\Panther**
- Abrir un cmd en modo administrador y escribir el siguiente comando dentro de la ruta de sysprep:

  C:\Windows\System32\Sysprep>sysprep.exe /generalize /oobe /shutdown /unattend:"C:\Windows\System32\Sysprep\Panther\unattend.xml"

- Después de terminada la ejecución del proceso de sysprep, el equipo se apagará.

Captura de imagen Capa 1

Capturar imagen de capa 1 con Acronis u otro método como DISM, si se elige utilizar DISM seguir los siguientes pasos:

- Cuando el equipo de referencia inicie desde el USB presionar la combinación de teclas Shift + F10. Esta combinación de teclas abre una línea de comandos de CMD.
- Cuando se encuentre en la línea de comandos (CMD) ubique la unidad de Disco donde se encuentra instalado Windows 10 (origen) y donde se capturar la imagen (destino), para este ejemplo fue H:\ el destino y E:\ el origen y ejecute el siguiente comando:

  Dism /Capture-Image /ImageFile:"**H:\ModeloX\CAPA1\CERRADA\install.wim**" /CaptureDir:E:\ /Name:Capa1_C_MM

- Esperamos a que concluya el proceso y marque que la operación fue completada satisfactoriamente.
- Después de haber capturado exitosamente el archivo install.WIM puede desconectar las USB´s (USB de Booteo y USB de almacenamiento), cerrar todas las aplicaciones y reinicie el PC de referencia.

Para poder probar que la captura se realizó correctamente, se utilizará una USB booteable a la cual le será remplazado el archivo install.wim original por el archivo install.wim generado en la captura. Una vez realizado este proceso se utilizará el segundo equipo Modelo X, bootearemos utilizando este nueva USB que contiene el archivo install.wim de la captura y finalizada la instalación, podremos validar la versión de Windows 10 instalado, así como el que los drivers se hayan mantenido

Una vez finalizada la captura de la capa 1 seguir los pasos siguientes:

- Cargar equipo con imagen.
- Cuando lo solicite el sistema agregar el usuario **soporte.ti** con contraseña de administrador
- Ingresar el equipo a dominio con nomenclatura correspondiente.
- Activar sccm con el comando del site que corresponda, los cuales son los siguientes:

SITE CODE TRIARA
ccmsetup.exe smssitecode=TR1 /Source:C:\CMClient smsmp=SCCMAMC.gmexico.com fsp=SCCMAMC.gmexico.com DNSSUFIX=gmexico.com

SITE CODE FUNDICION
ccmsetup.exe smssitecode=FN1 /Source:C:\CMClient smsmp=mx53sccm.gmexico.com fsp=mx53sccm.gmexico.com DNSSUFIX=gmexico.com

SITE CODE SAN LUIS ZINC
ccmsetup.exe smssitecode=SZ1 /Source:C:\CMClient smsmp=dpimmslz1.gmexico.com fsp=dpimmslz1.gmexico.com DNSSUFIX=gmexico.com

SITE CODE SANTA BARBARA
ccmsetup.exe smssitecode=SB1 /Source:C:\CMClient smsmp=mssccmsba01.gmexico.com fsp=mssccmsba01.gmexico.com DNSSUFIX=gmexico.com

SITE CODE SAN MARTIN
ccmsetup.exe smssitecode=SM1 /Source:C:\CMClient smsmp=dpimmsasma01.gmexico.com fsp=dpimmsasma01.gmexico.com DNSSUFIX=gmexico.com

SITE CODE CANANEA
ccmsetup.exe smssitecode=CA1 /Source:C:\CMClient smsmp=dp-cananead.gmexico.com fsp=dp-cananead.gmexico.com DNSSUFIX=gmexico.com

NOTA 1:
Para instalar el agente de SCCM en equipos conectados por VPN utilice la línea de comando del sitio TRIARA