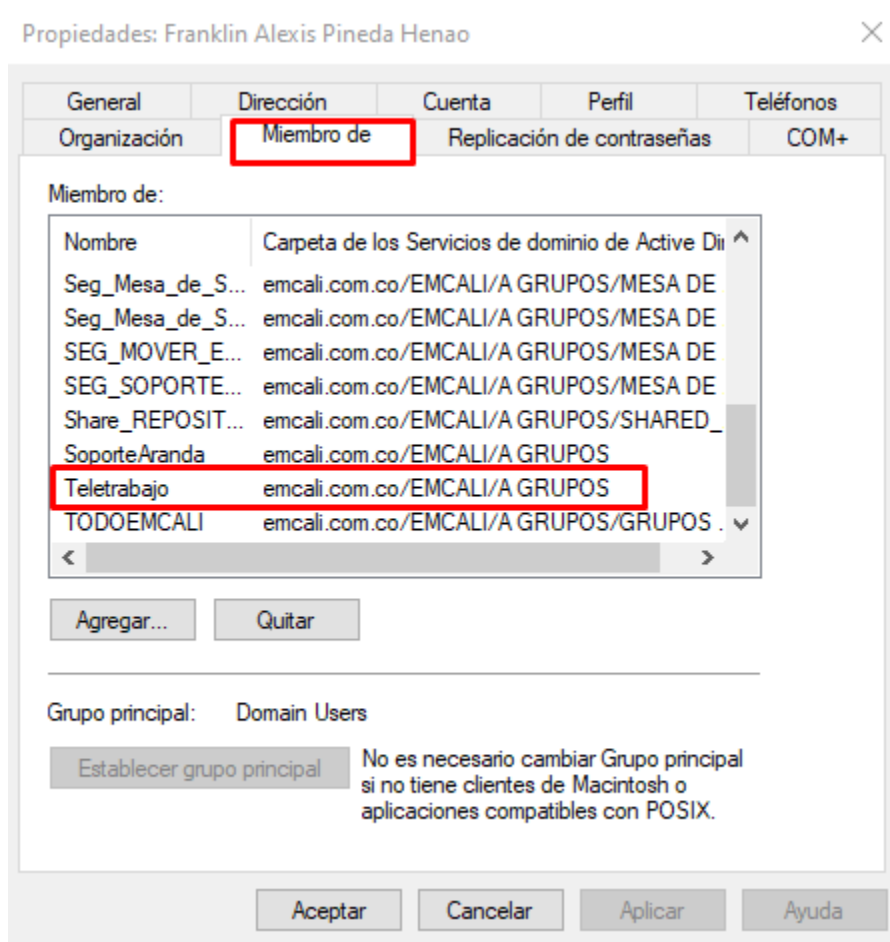
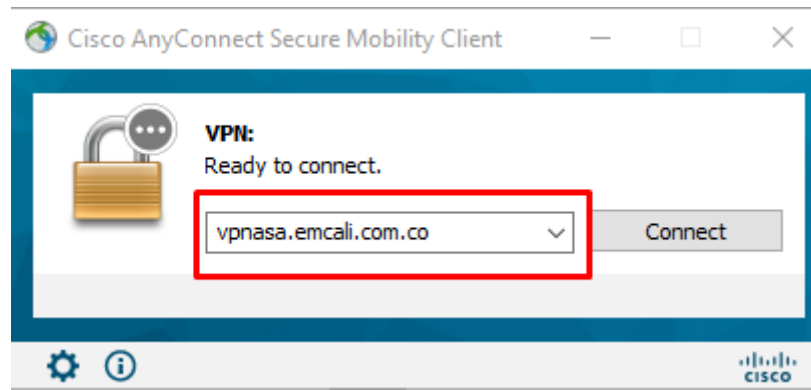


CHECK LIST - VPN ANYCONNECT

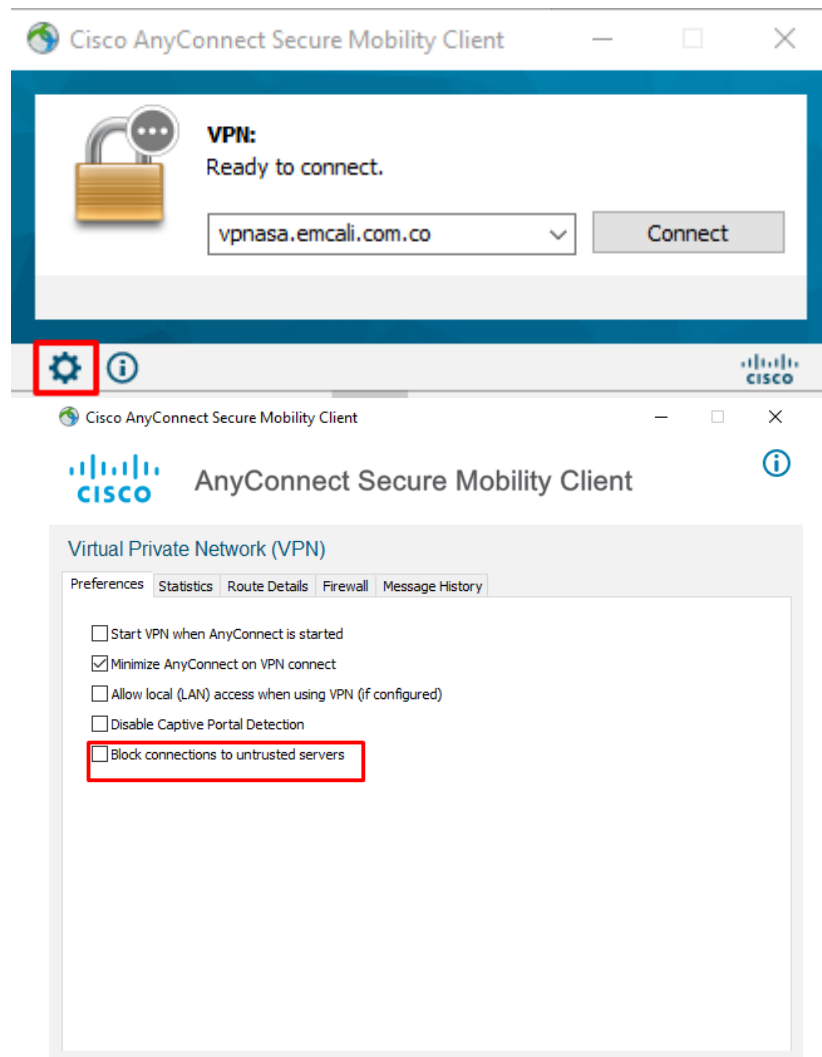
1. Validar en el directorio activo si el usuari@ tiene permisos de teletrabajo.



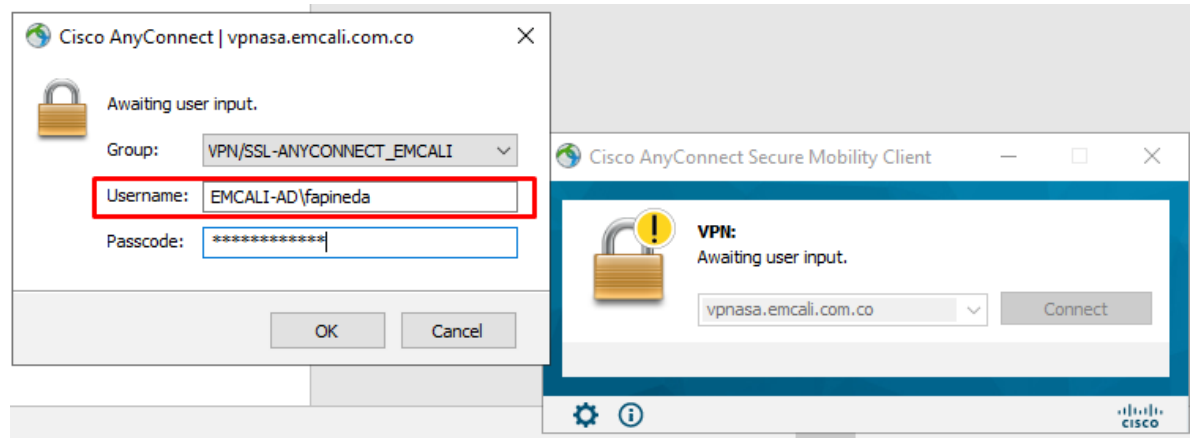
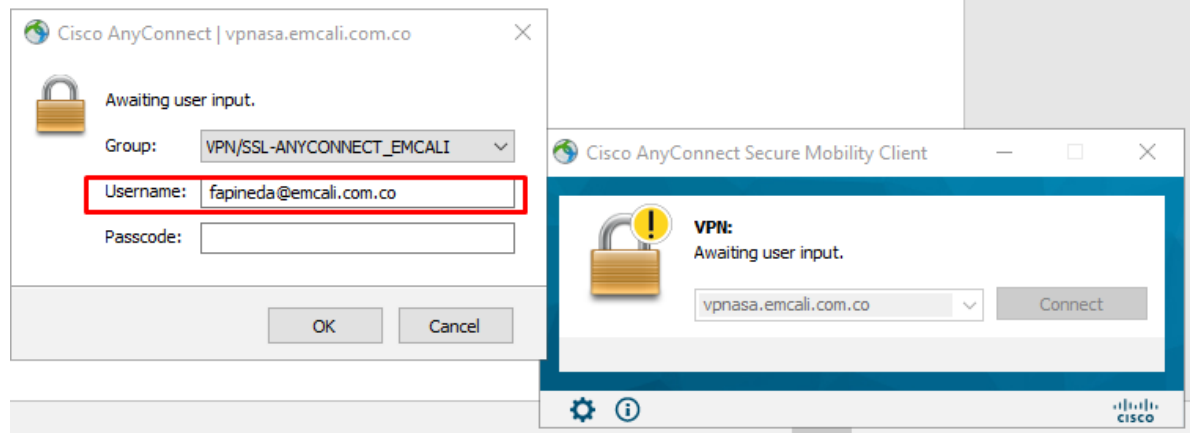
2. Verificar que en el recuadro de la VPN este digitado correctamente “vpnasa.emcali.com.co” si no es posible conectarse de esta manera validar de las siguientes formas: “vpnasa.emcali.net.co” – “200.14.113.162”



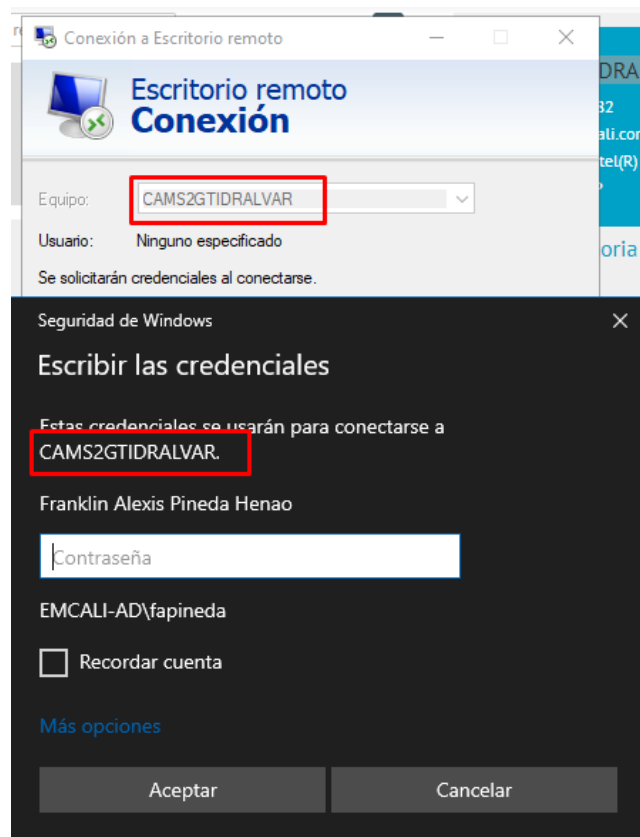
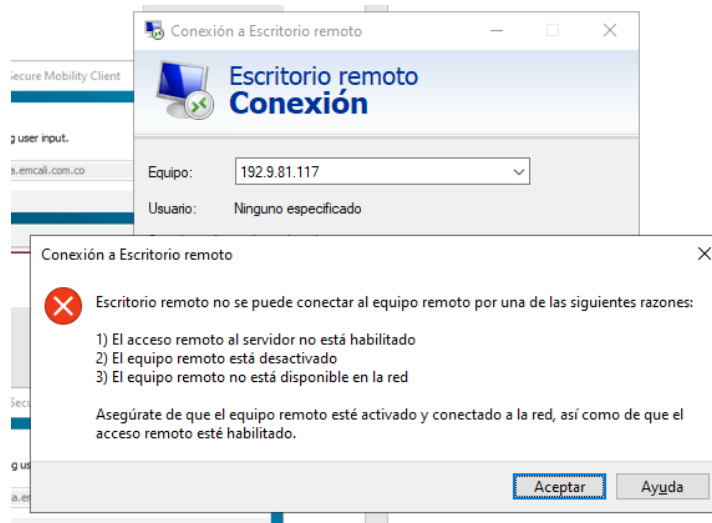
3. Validar que, en las opciones de la VPN, pestaña “preferences” el ultimo recuadro “block connections to untrusted servers” este deshabilitado, es decir no tenga un chulo como se indica en las imágenes.



4. Si al momento de que el funcionari@ digite el usuario de red ejemplo “fapineda” y contraseña y no es posible la conexión, indicarle al usuario digitar en username: de la siguiente manera, ejemplo: “fapineda@emcali.com.co” o “EMCALI-AD\fapineda”



5. Si el usuari@ intenta conectarse por conexión remota y no es posible por medio de la dirección IP del equipo de cómputo (ya que esta en ocasiones cambia), se deben conectar por el nombre del equipo.



6. En caso que no sea posible la conexión por VPN validar con el usuario si la versión es la correcta debe ser “**cisco AnyConnect Secure Mobility Client 4.10**”, caso contrario si es una versión anterior, proceder a enviar por correo electrónico el instalador con el manual al usuario y guiarlo en el proceso, si no es posible la instalación porque el usuario no tiene permisos de instalación, indicarle que debe traer el equipo de cómputo en la sede CAM o su respectiva sede, para que un técnico realice la instalación de la nueva versión de la VPN, dicha instalación debe tener creado su respectiva solicitud (requerimiento y/o incidente).

