Configuración de la autorización local de UCCE 12.0(X)

Contenido

Introducción

Este documento describe los pasos necesarios para eliminar la dependencia de microsoft active directory (AD) para administrar la autorización en los componentes de Unified Contact Center Enterprise (CCE).

Colaborado por Anuj Bhatia, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

Componentes Utilizados

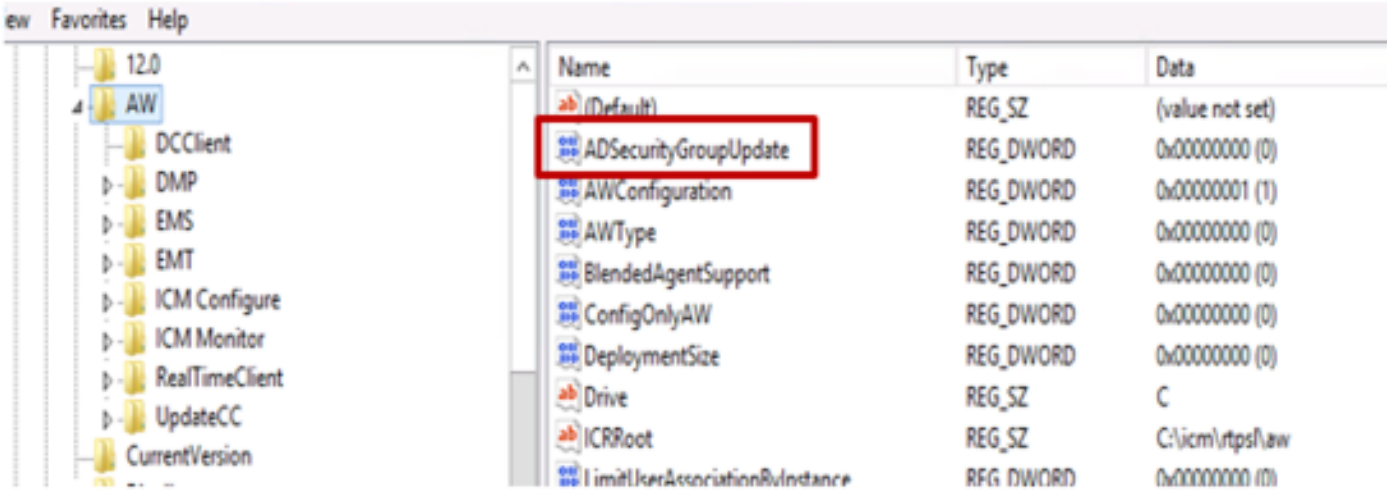
La información utilizada en el documento se basa en la versión 12.0(1) de la solución UCCE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier paso.

Antecedentes

La versión UCCE 12.X proporciona privilegios de pertenencia de usuario a los grupos de usuarios

locales en el servidor de administración local (AW), lo que permite a los usuarios sacar la autorización de Active Directory (AD). Esto es controlado por el registro **ADSecsecurityGroupUpdate** que está habilitado de forma predeterminada y evita el uso de los Grupos de seguridad de Microsoft AD para controlar los derechos de acceso de los usuarios para realizar tareas de configuración y configuración.



> **Nota:** Si la empresa desea elegir el comportamiento anterior, el indicador ADSecsecurityGroupUpdate se puede cambiar a 1, que permite actualizarlo a Active Directory (AD)

Para sacar la autorización de AD, se requiere una tarea única en cada máquina de servidor AW para conceder los permisos necesarios para el grupo UcceConfig y este documento tiene como objetivo mostrar los pasos necesarios para configurar estos permisos junto con un ejemplo de cómo asignar un usuario de dominio como parte del grupo Configuración y Configuración de CCE.

Configurar

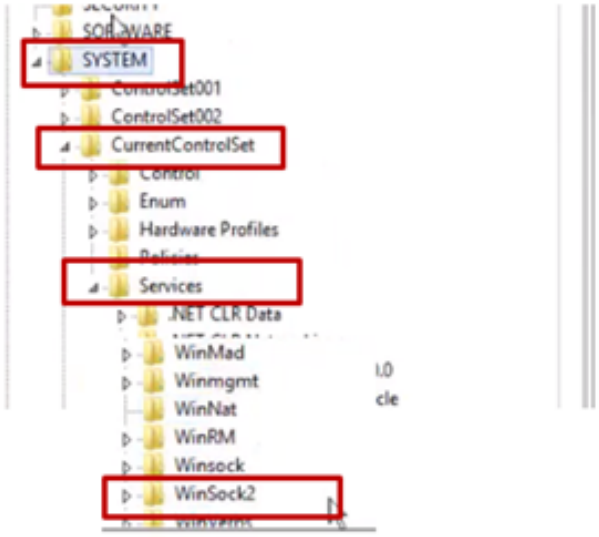
Conceder permisos de grupo de UcceConfig en el servidor AW local es un proceso de dos pasos: en primer lugar, los permisos se proporcionan en el nivel de registro y, en segundo lugar, se pasan al nivel de carpeta.

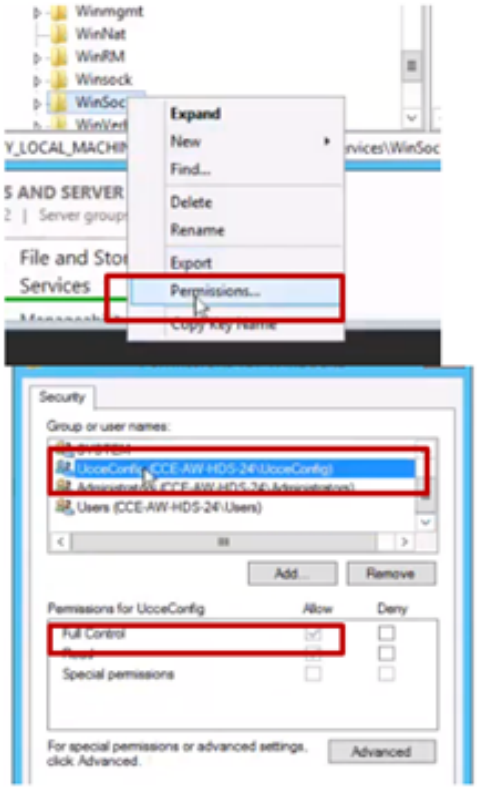
Paso 1. Configurar permisos de registro

1. Ejecute la utilidad regedit.exe.

2. Seleccione **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2**.

3. En Permisos en la ficha Seguridad, seleccione el grupo **UcceConfig y active la opción Permitir el control completo**.





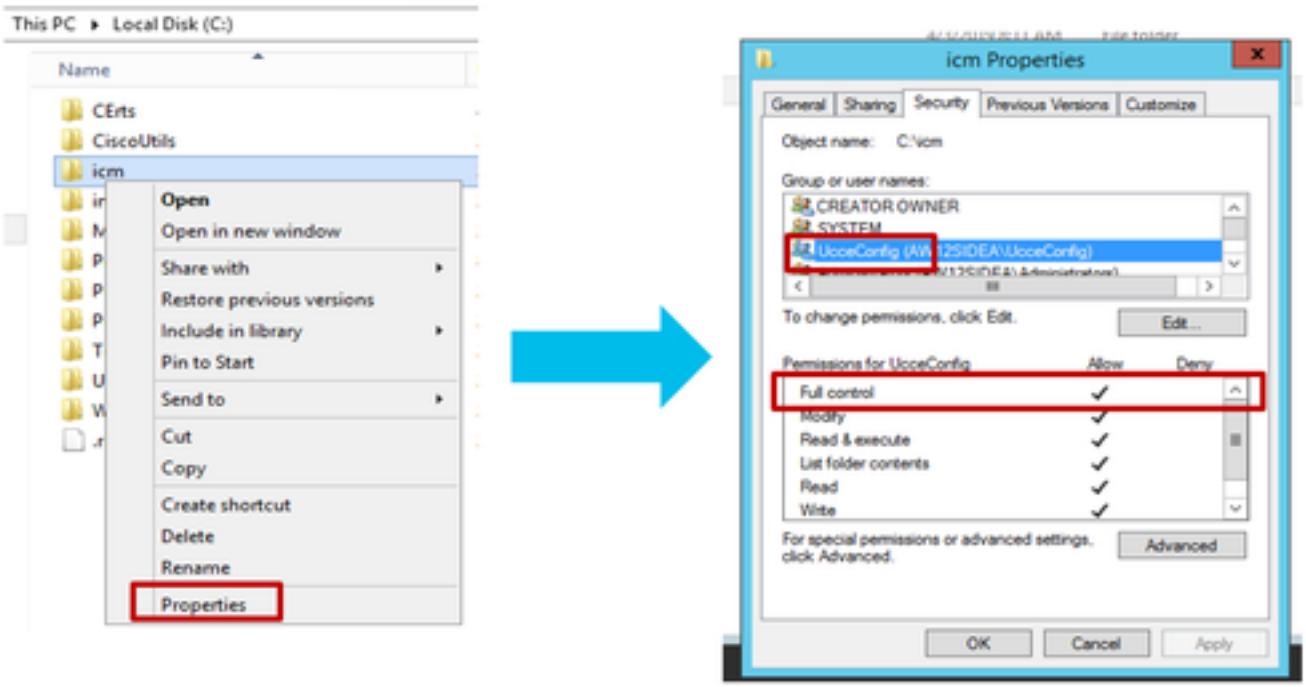
4. Repita los pasos anteriores para conceder el control completo al grupo UcceConfig para los registros

- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, inc.\ICM**
- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, inc.\ICM**

Paso 2. Configurar permisos de carpeta

1. En el Explorador de Windows, seleccione C:\icm and go to Properties.

2. En la ficha Seguridad, seleccione **UcceConfig** y marque **Allow for the Full Control** option.



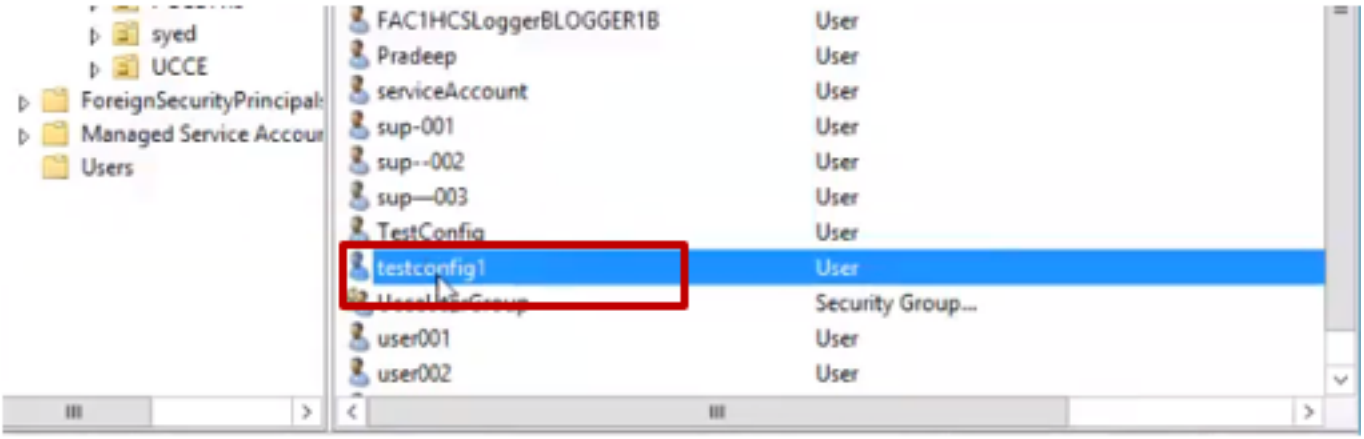
3. Seleccione Aceptar para guardar el cambio.

4. Repita los pasos anteriores para conceder el control completo al grupo **UcceConfig** para C:\Temp folder.

A medida que se ha alcanzado la configuración preliminar del día 0, observe los pasos sobre cómo puede promocionar a un usuario de dominio para que tenga derechos de configuración y configuración.

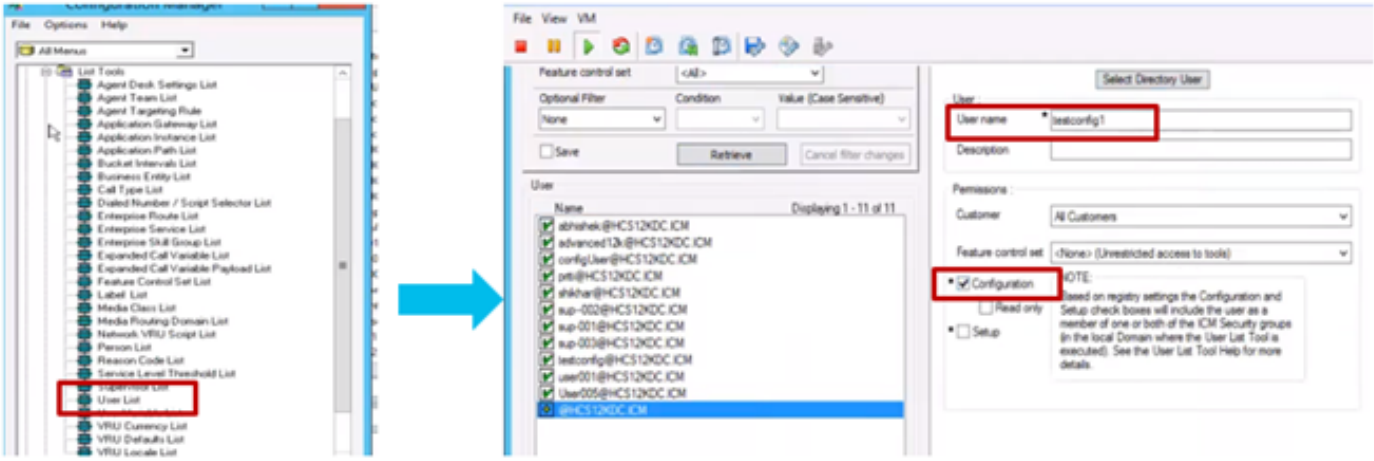
Paso 3: Configuración de usuario de dominio

1. Cree un usuario de dominio en AD, para este ejercicio se ha creado el usuario testconfig1.

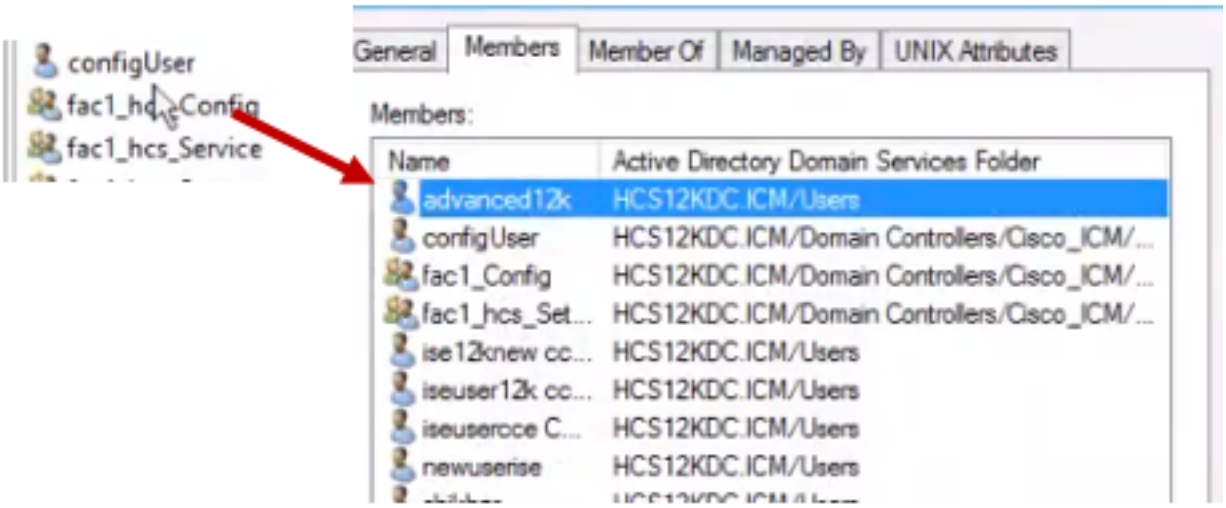


2. Inicie sesión en el servidor AW con un administrador de dominio o una cuenta de administrador local.

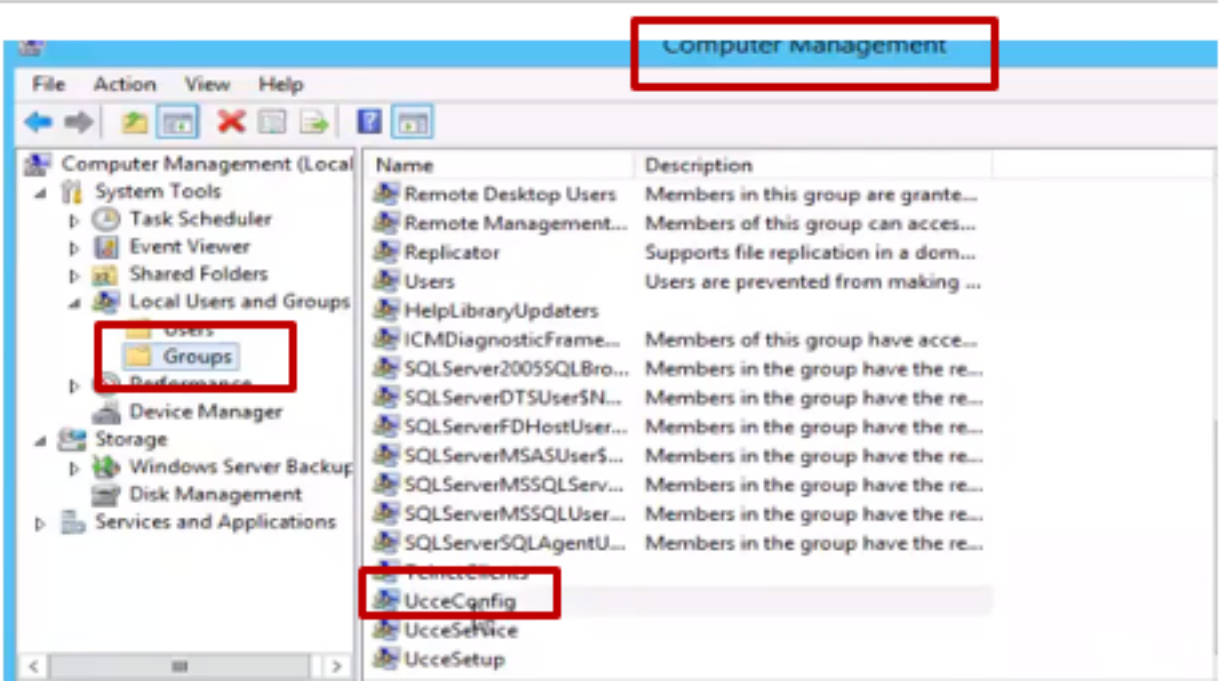
3. En Configuration Manager a través de la herramienta de lista de usuarios, agregue el usuario y verifique la opción **configuration**.



Antes de la versión 12.0, este cambio habría actualizado los grupos de seguridad de configuración en el dominio bajo una unidad organizativa (OU) de instancia, pero con 12.0 el comportamiento predeterminado es que no agrega ese usuario al grupo AD. Como se muestra en la imagen, no hay actualización de este usuario en el grupo de seguridad de configuración de dominio ICM.



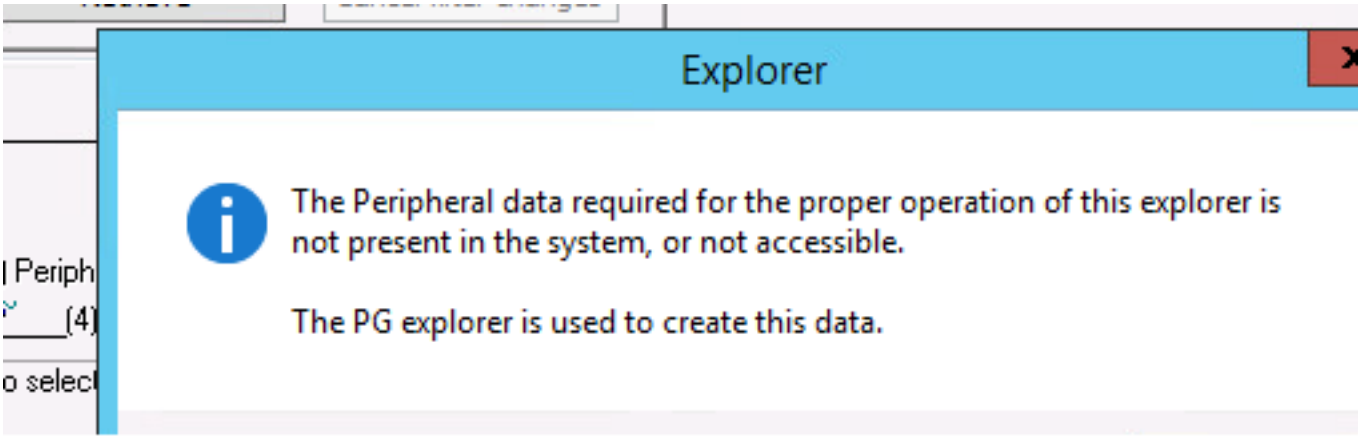
4. En AW Server bajo **computer management > Local Users and Groups > Groups > Groups** seleccione UcceConfig y agregue testconfig1 user en él.



5. Cierre la sesión de la máquina e inicie sesión con las credenciales del usuario testconfig1. Como este usuario tiene derechos de configuración, podrá ejecutar herramientas de configuración de CCE como el Administrador de configuración , Script o el Editor de secuencias de comandos de Internet.

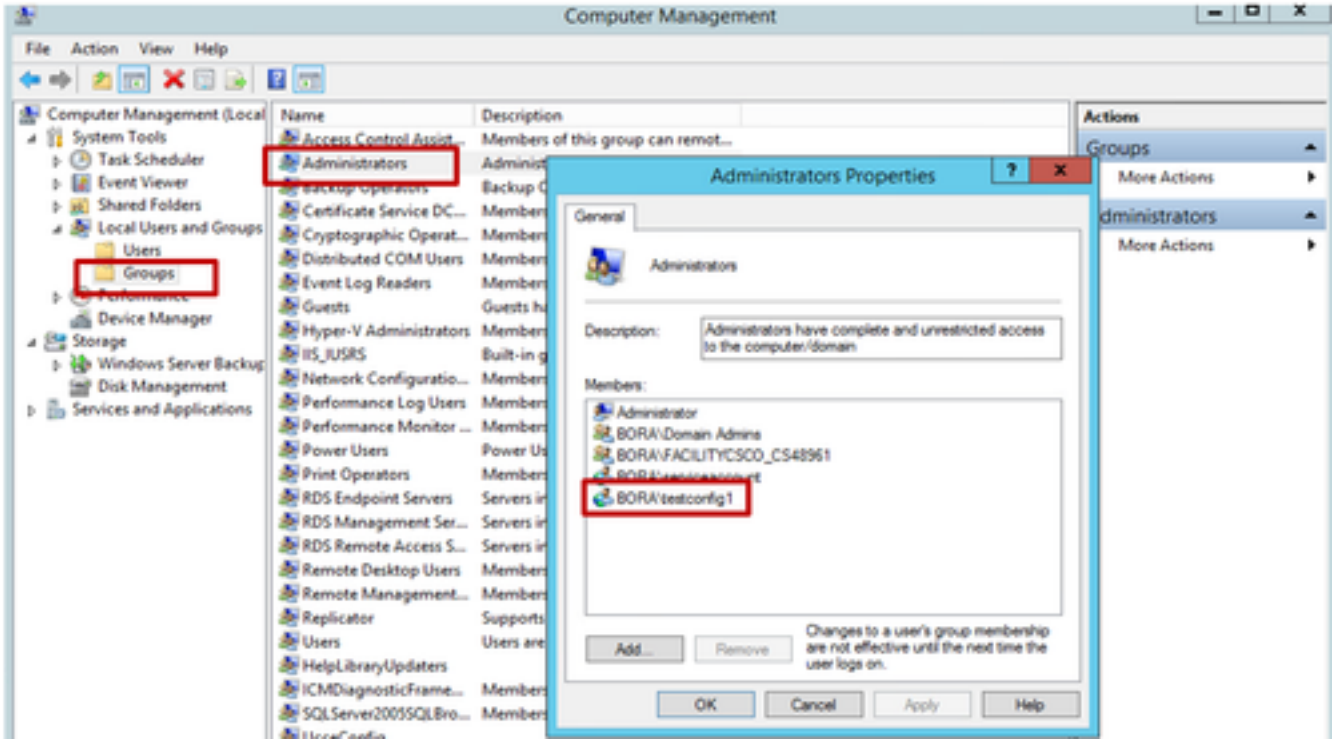
6. Sin embargo, si el usuario intenta ejecutar cualquier tarea que requiera derechos de configuración, se produce un error.

En este ejemplo se muestra testconfig1 user changing pheral gateway (pg) configuration y el sistema restringe el cambio con un mensaje de advertencia.

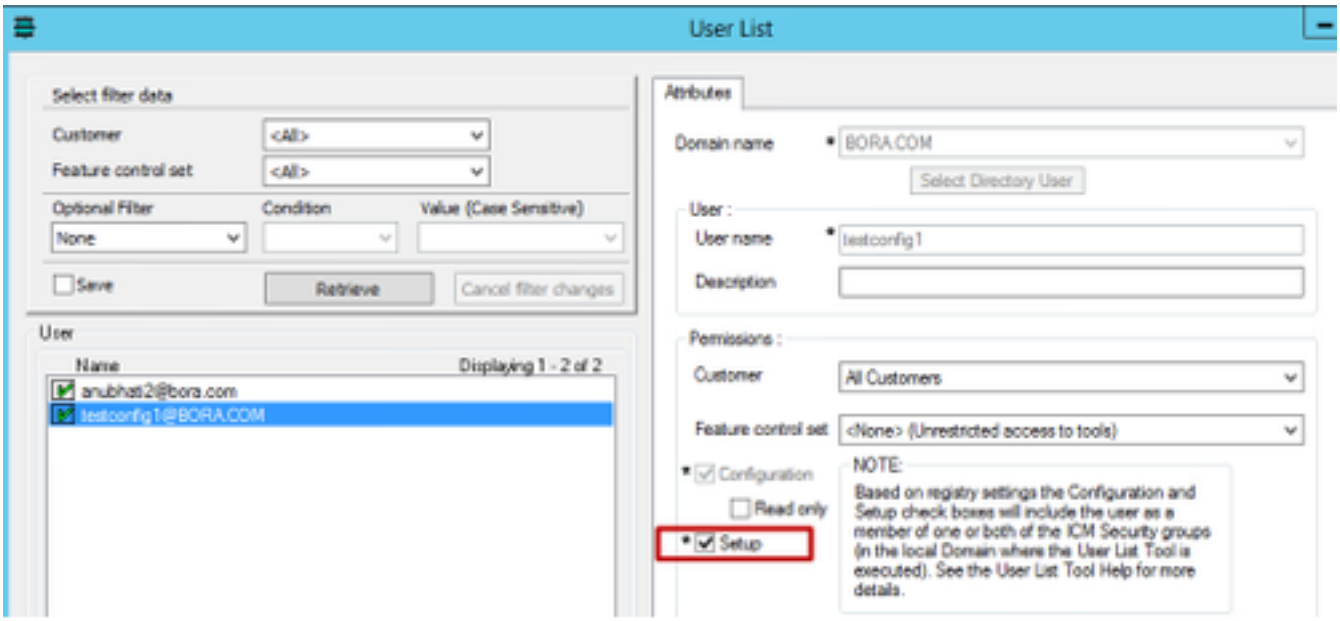


7. Si la empresa requiere que este usuario tenga derechos de configuración junto con la configuración, debe asegurarse de que el usuario se agrega al grupo de administración local del servidor AW.

8. Para lograrlo, inicie sesión en el servidor AW con el dominio o la cuenta de derechos de administrador local y a través de **administración de equipo > Usuarios y grupos locales > grupos** seleccione Grupos y en Administradores agregue el usuario al usuario.



9. En Administrador de configuración a través de la herramienta Lista de usuarios, seleccione el usuario y active la opción de configuración.



10. El usuario ahora puede acceder a todos los recursos de la aplicación CCE en ese servidor AW y realizar los cambios deseados.

Verificación

El procedimiento de verificación es en realidad parte del proceso de configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.