

Configuración de la Autorización Local de PCCE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1. Configurar permisos de registro.](#)

[Paso 2. Configurar permisos de carpeta.](#)

[Paso 3. Configuración de usuario de dominio.](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos necesarios para eliminar la dependencia de Microsoft Active Directory (AD) para administrar la autorización localmente en los componentes de Package Contact Center Enterprise (PCCE).

Colaboración de Meenakshi Sundaram, Ramiro Amaya y Anuj Bhatia, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Package Contact Center Enterprise
- Microsoft Active Directory

Componentes Utilizados

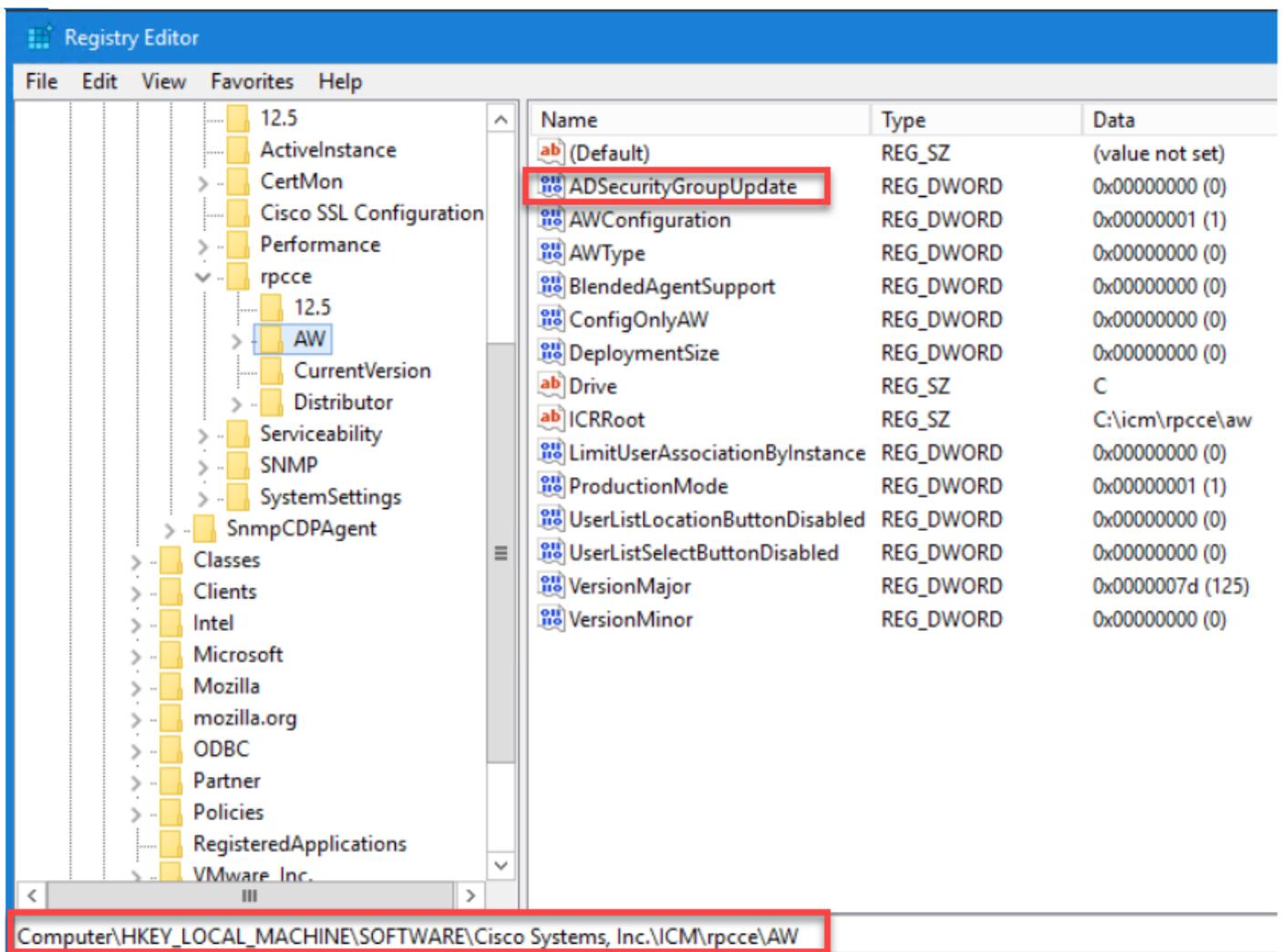
La información utilizada en el documento se basa en la versión 12.5(1) de PCCE.

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 de PCCE 12.5 proporciona privilegios de usuario a los grupos de usuarios locales en Administration Servers (AW), lo que permite a los usuarios sacar la autorización de Active Directory (AD). Esto es controlado por el registro **ADSecsecurityGroupUpdate** que de forma predeterminada está habilitado 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: La compatibilidad con la autorización local se inició en Unified Contact Center Enterprise (UCCE) 12.0 y ahora se admite en PCCE 12.5.



Nota: Si la empresa necesita implementar el comportamiento anterior (autorización de AD), el indicador ADSecsecurityGroupUpdate se puede cambiar a 1.

Configurar

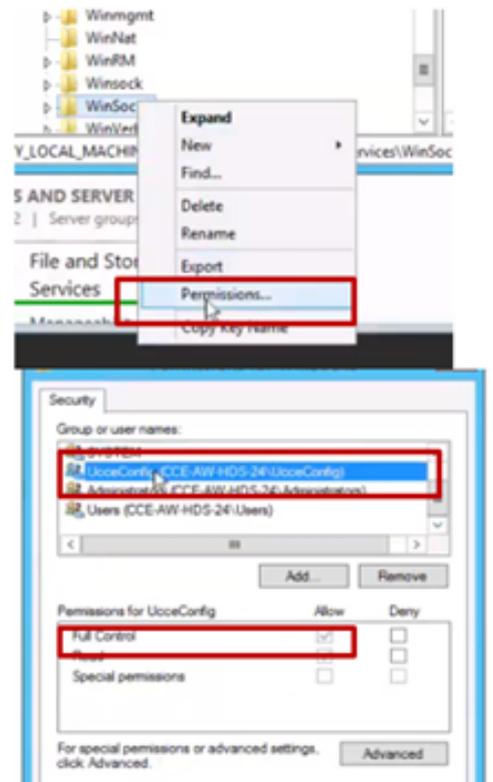
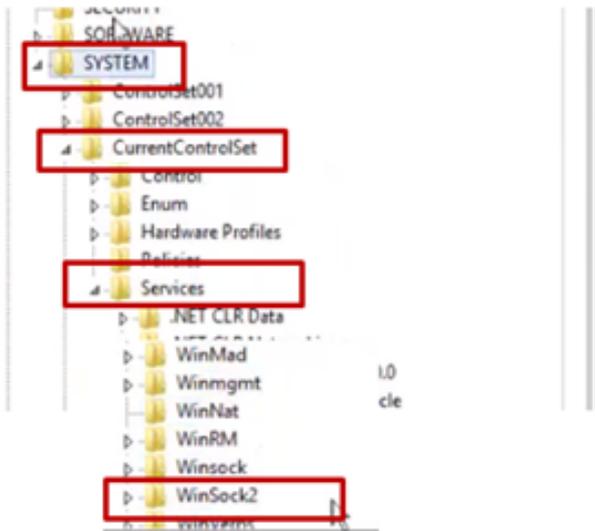
Para otorgar permisos de grupo de UcceConfig en un servidor AW local, primero, se deben proporcionar permisos en el nivel de registro y, segundo, en el nivel de carpeta.

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.



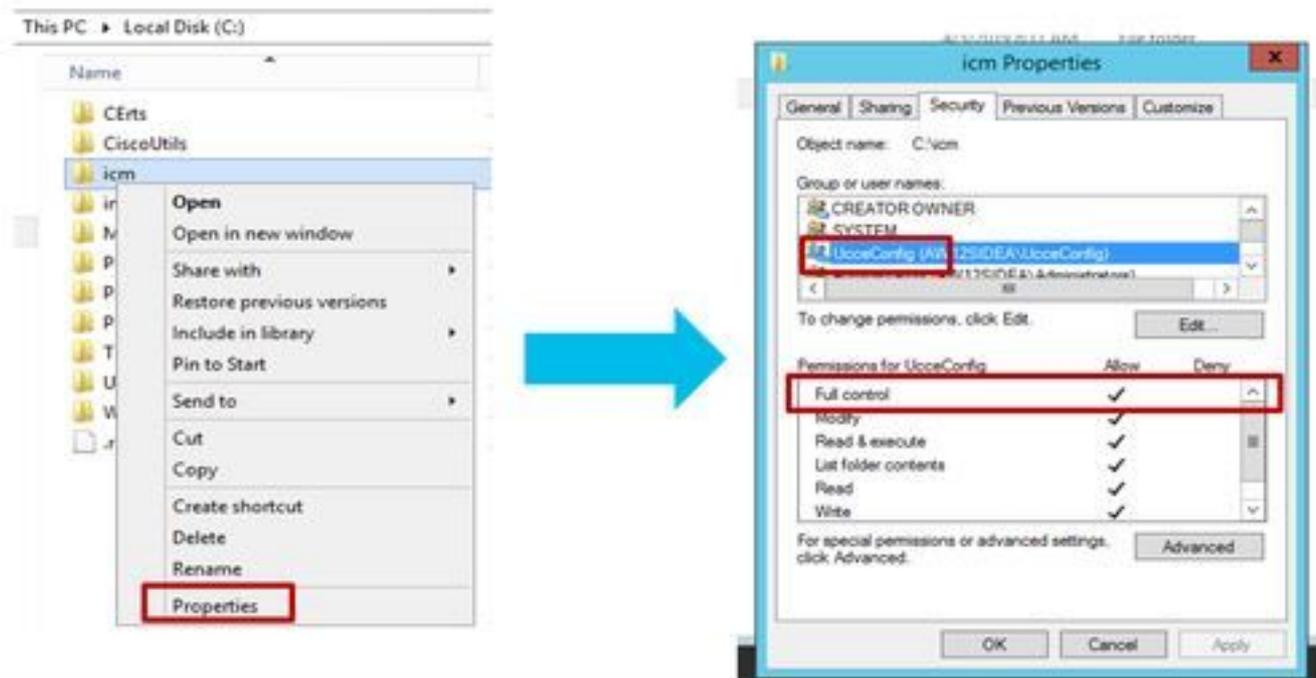
4. Repita los pasos anteriores para conceder el control completo al grupo UcceConfig para estos registros.

- 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, navegue hasta <ICM Installed Directory>:\icm y seleccione Properties .

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



3. Seleccione Aceptar para guardar los cambios.

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

5. En SQL Management Studio, realice lo siguiente:

a) Vaya a Security > Logins.

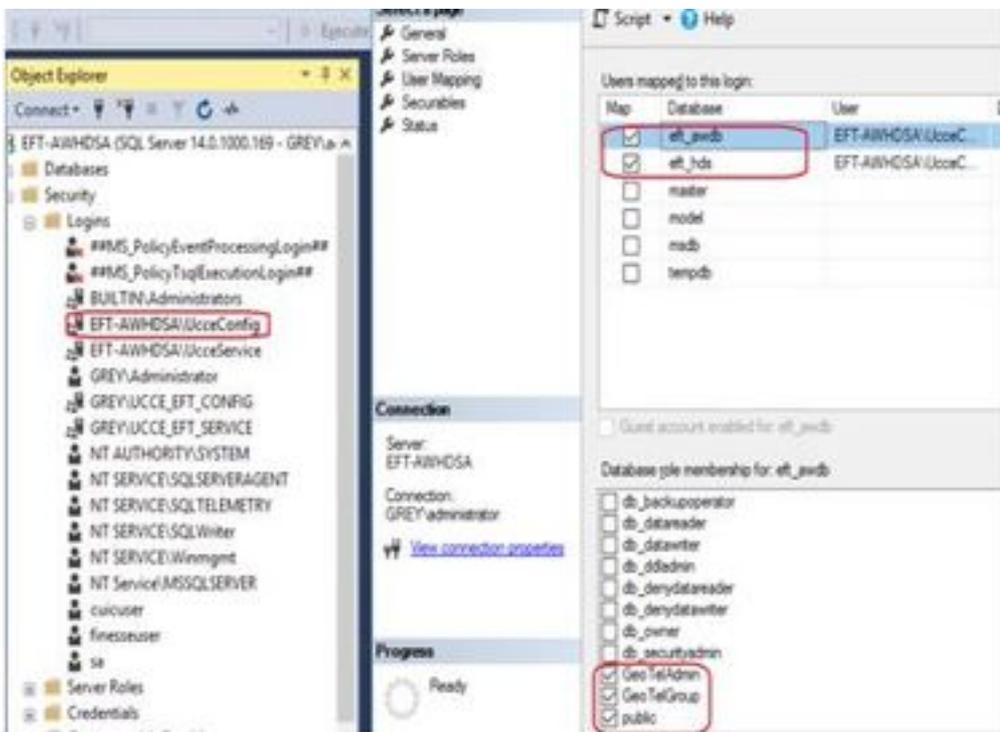
b) Busque <Machine name>\UcceConfig.

c) Haga clic con el botón derecho del ratón y seleccione propiedades.

d) Navegar por las asignaciones de usuario y seleccionar la base de datos AWDB.

e) Marque las casillas de verificación GeoTelAdmin, GeoTelGroup y public.

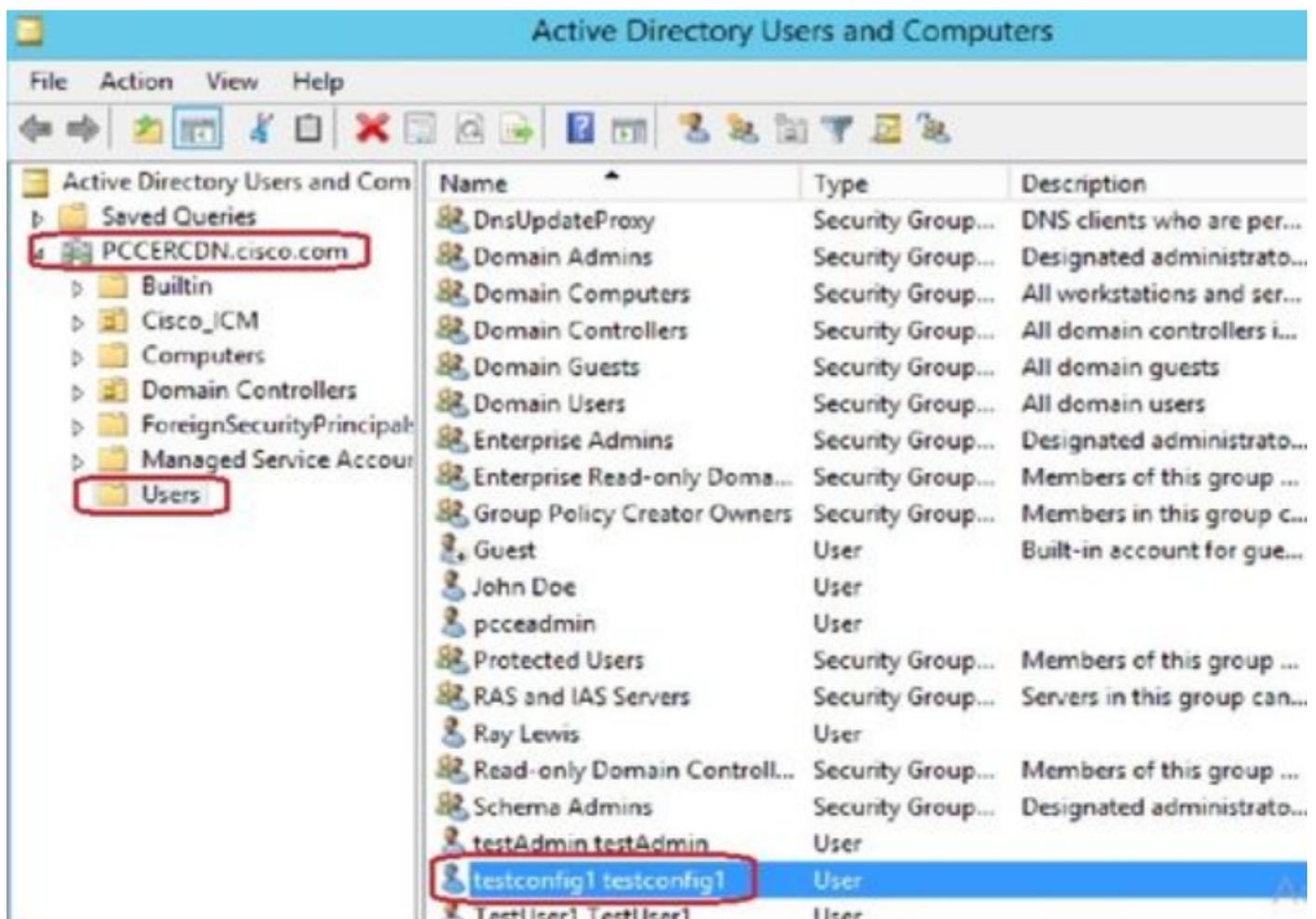
f) Repita el paso d) para la base de datos de datos históricos (HDS).

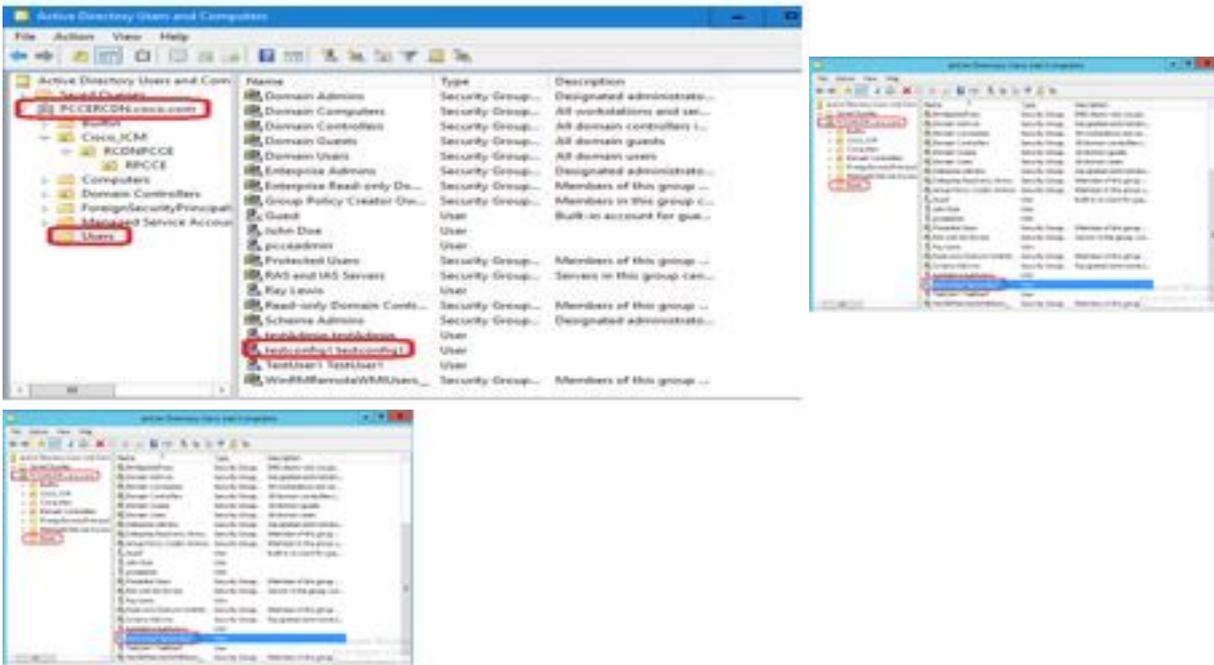


Como se ha alcanzado la configuración preliminar, siga los pasos de cómo puede promocionar a un usuario de dominio para tener derechos de configuración y configuración.

Paso 3. Configuración de usuario de dominio.

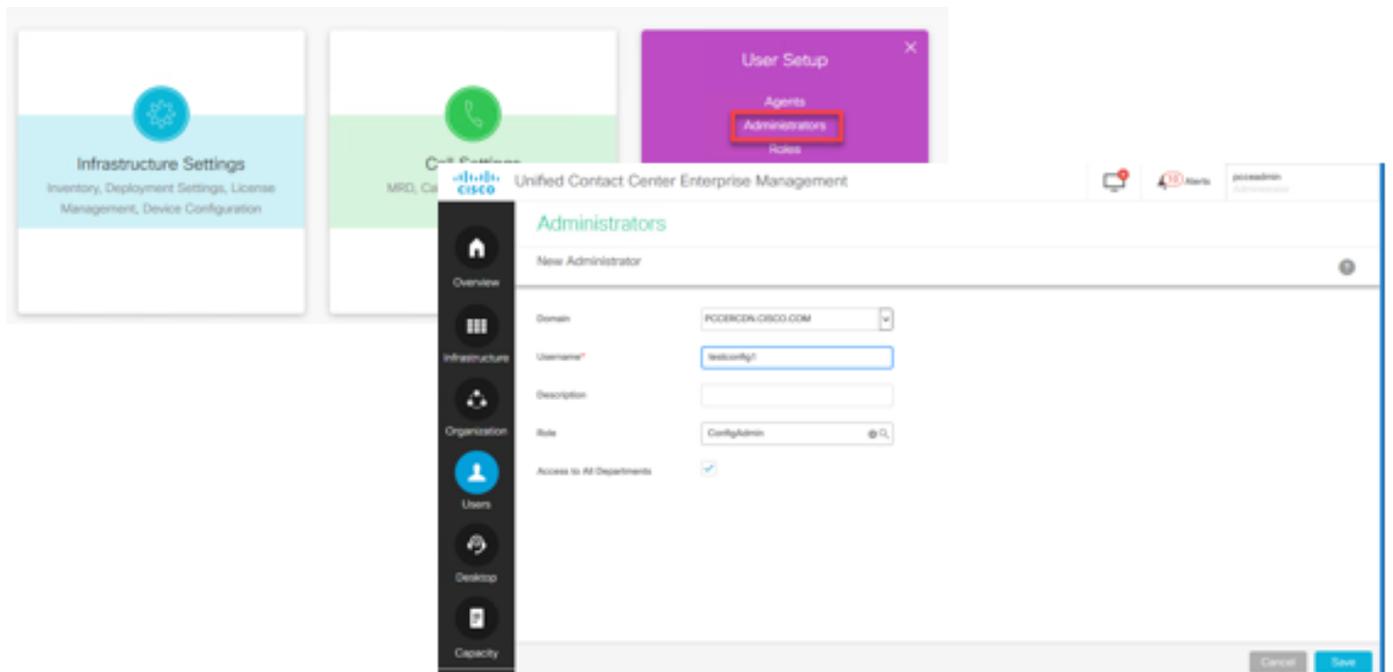
1. Cree un usuario de dominio en AD. Para este ejercicio se creó el usuario testconfig1.



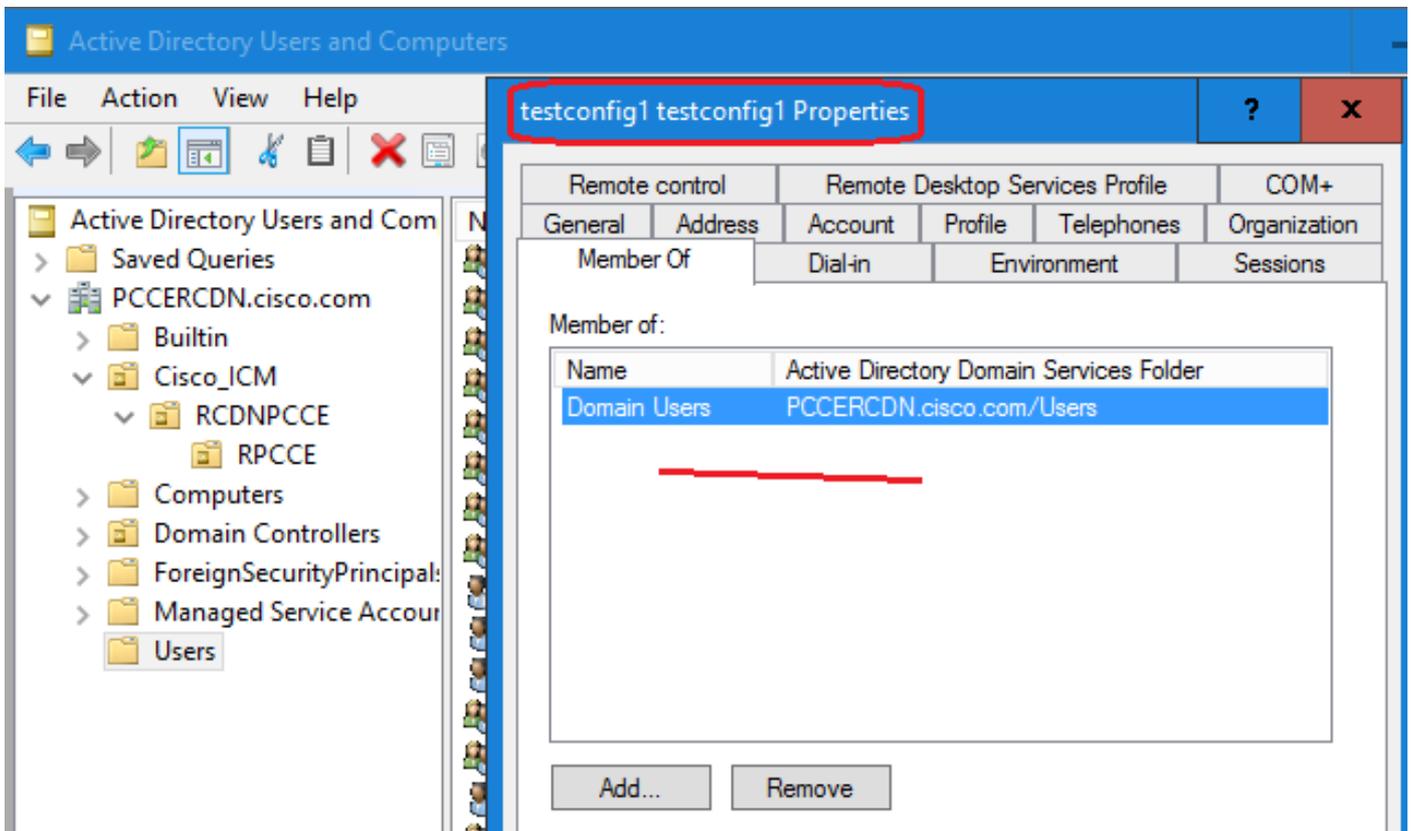


2. Inicie sesión en el servidor AW con una cuenta de administrador de dominio o una cuenta de administrador local.

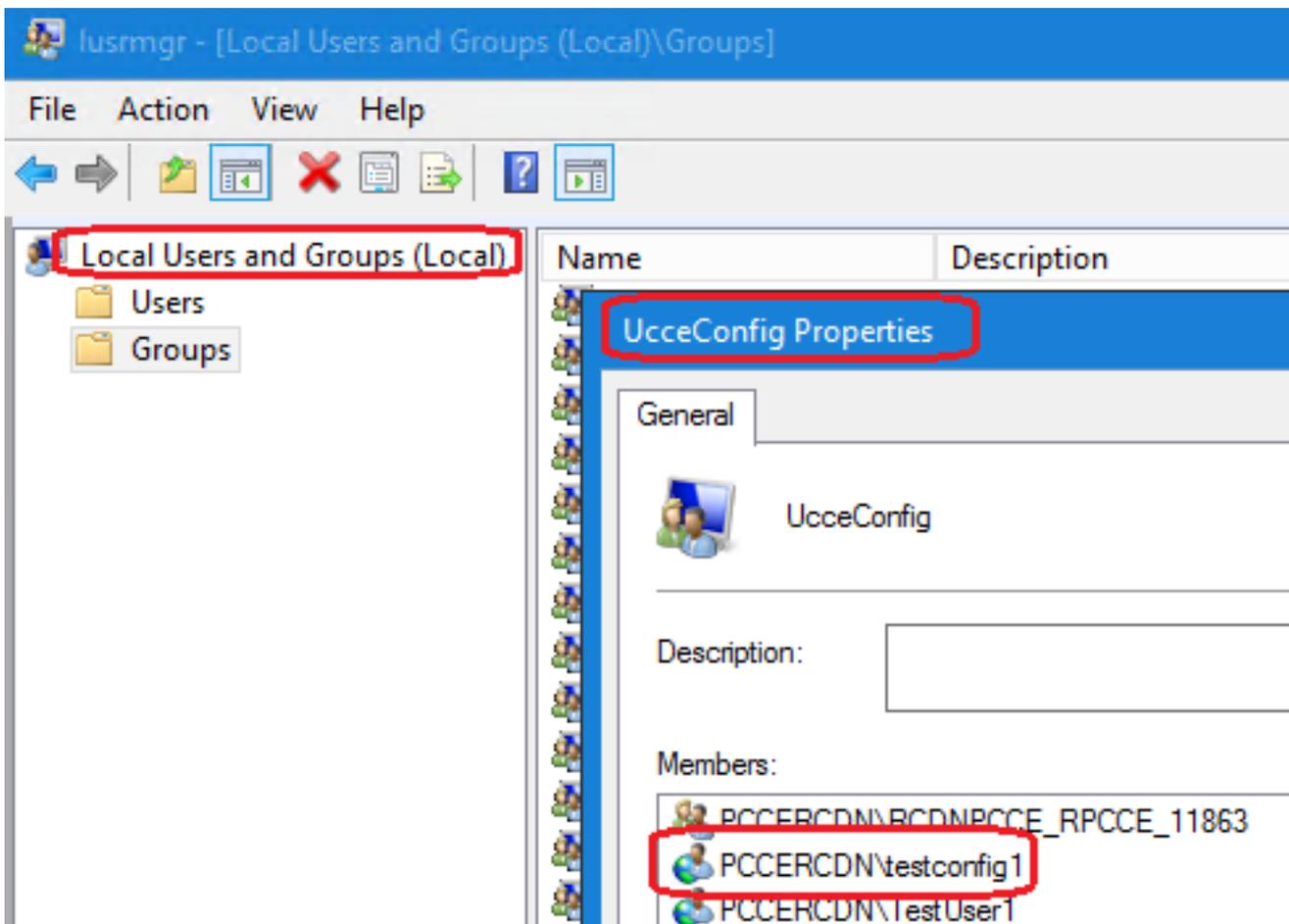
3. Abra CCE Admin en AW. Desplácese a la tarjeta User Setup (Configuración de usuario) y seleccione Administradores. Agregue el usuario y seleccione la función **ConfigAdmin**.



Antes de la versión 12.5 de PCCE, este cambio habría actualizado los grupos de seguridad de configuración en el dominio bajo una unidad organizativa (OU) de instancia, pero con 12.5 el comportamiento predeterminado es no agregar 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.

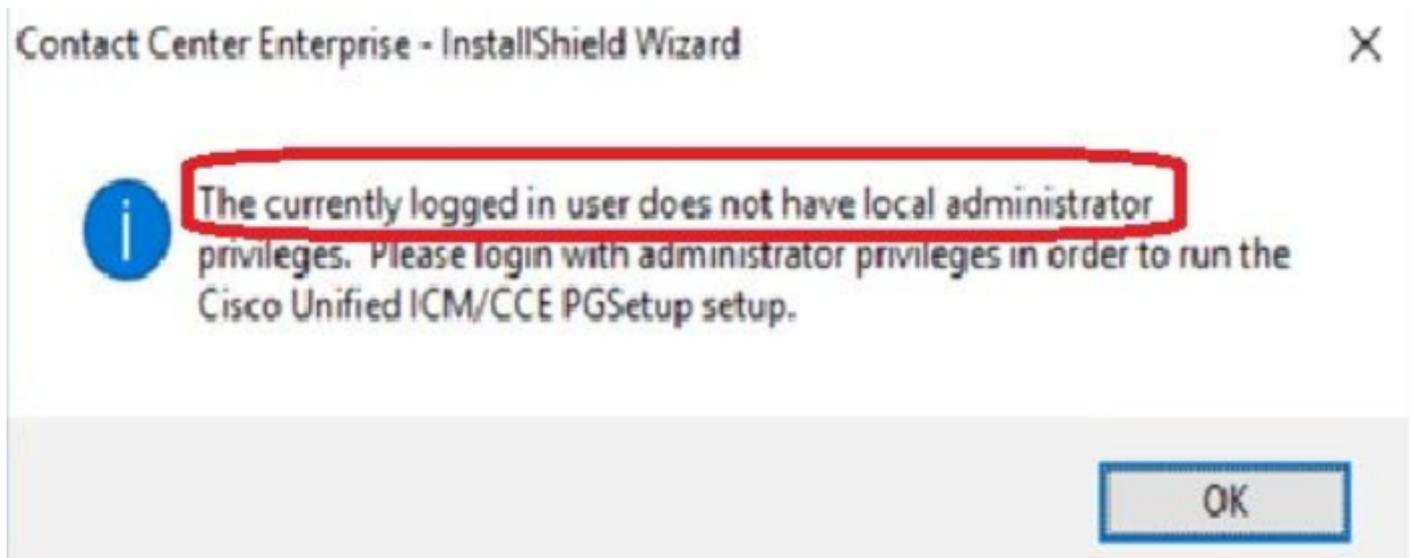


5. Cierre la sesión de la máquina e inicie sesión con las credenciales del usuario testconfig1. Como este usuario tiene derechos de configuración, puede ejecutar herramientas de

configuración de CCE como CCE Admin, Script o Internet Script Editor.

6. Sin embargo, si el usuario intenta ejecutar cualquier tarea que requiera derechos de configuración, se produce un error. Este usuario no tiene acceso a todos los recursos de administración de CCE ni a las herramientas de configuración.

Como se muestra en la imagen, el usuario testconfig1 en la implementación PCCE 4K intenta ejecutar la configuración de la puerta de enlace periférica (PG) 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 la función de usuario se cambie a SystemAdmin en CCEAdmin.

Administrators

Edit testconfig1@PCCERCDN.CISCO.COM

Domain

PCCERCDN.CISCO.COM



Username*

testconfig1

Description

Role

SystemAdmin



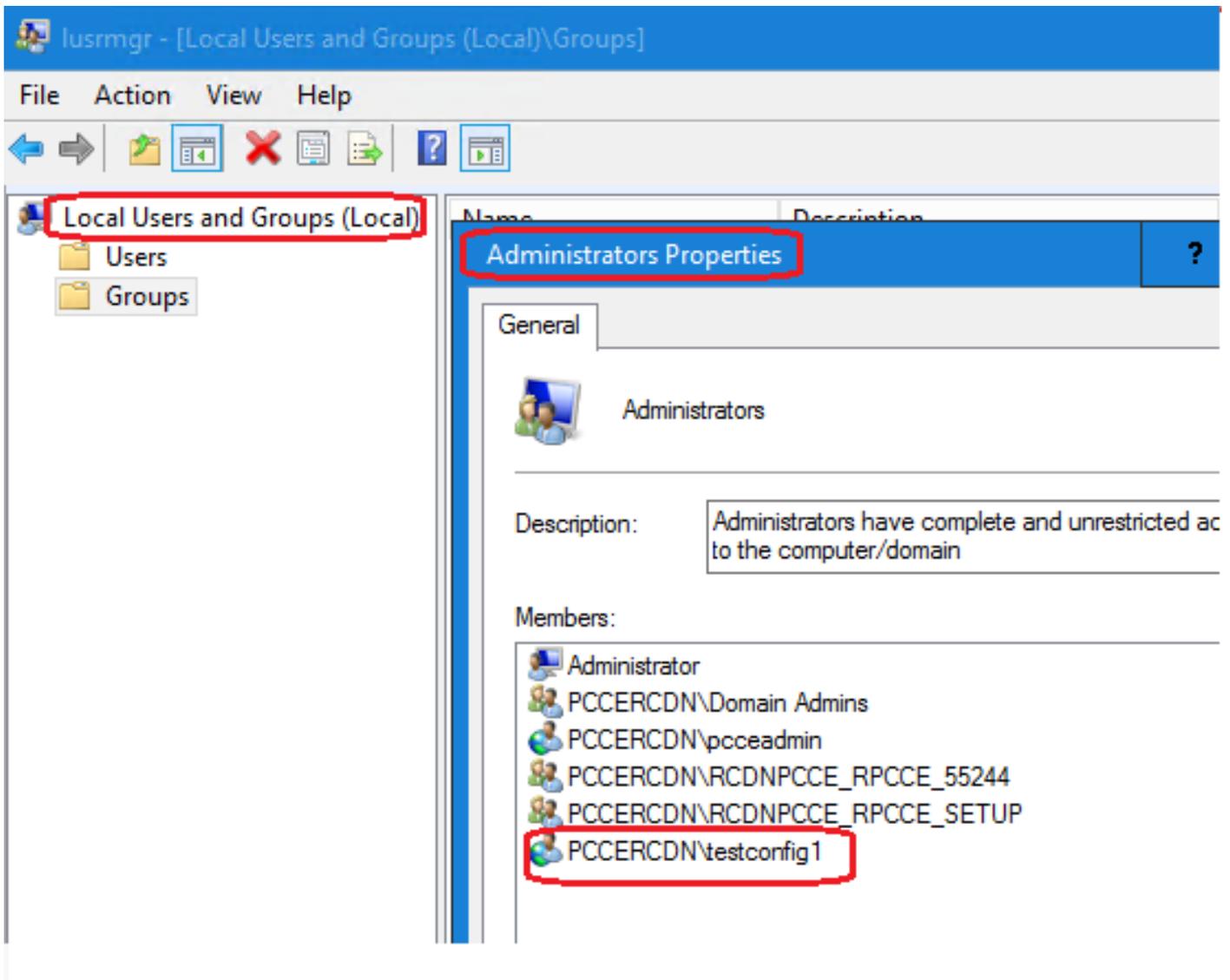
Access to All Departments



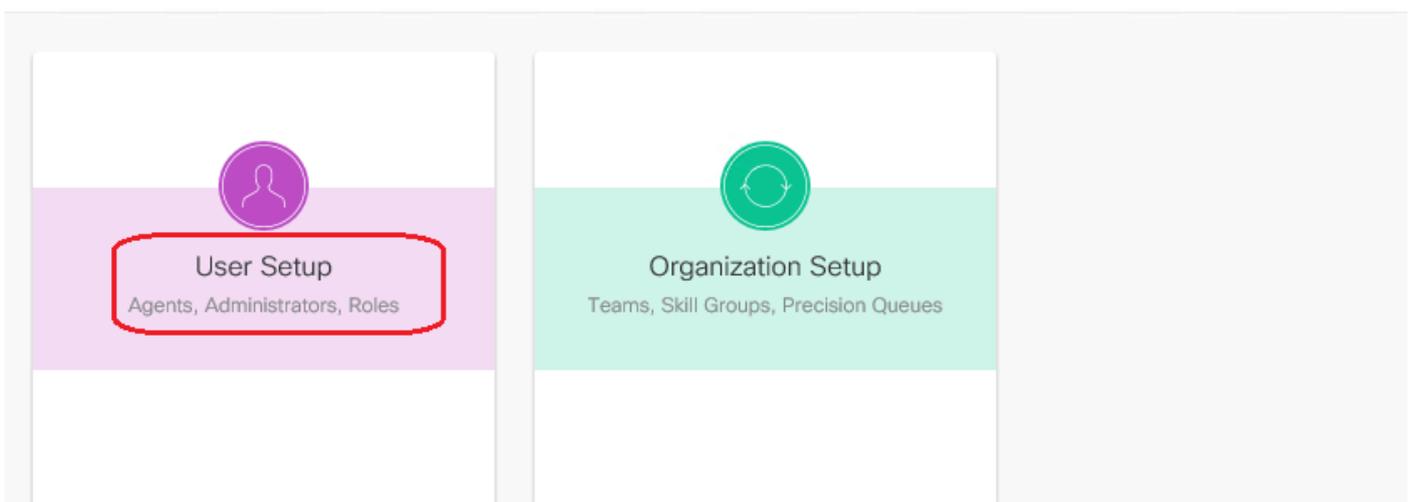
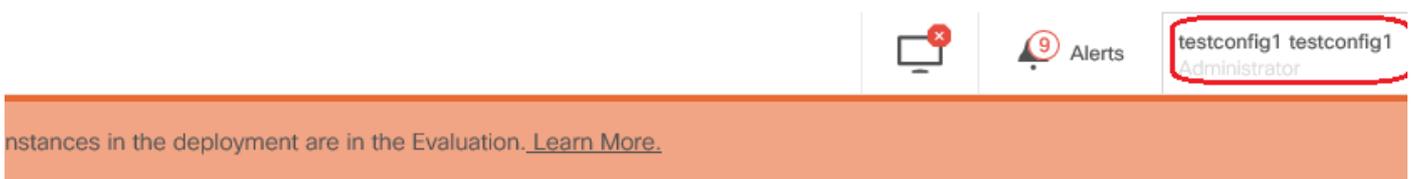
La función de usuario se ha actualizado como 1 (SystemAdmin) en la base de datos:

	UserRole	UserGroupID	CustomerDefinitionID	UserGroupName	UserGroupType	Description	ServiceProvider	ReadOnly	FeatureSetID
1	0	1	NULL	DBO	U	The ICM System Administrator	Y	N	NULL
2	0	5000	NULL	PCCERCDN\RLEWIS	U	NULL	N	N	NULL
3	1	5002	NULL	PCCERCDN\TESTCONFIG1	U	NULL	N	N	5000
4	2	5001	NULL	PCCERCDN\TESTUSER1	U	NULL	N	N	5001

8. 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.



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 pasos específicos disponibles para solucionar este problema de configuración.

Información Relacionada

[Guía de administración de PCCE](#)

[Soporte Técnico y Documentación - Cisco Systems](#)