Configure PCCE Local Authorization

Contents

Introduction

This document describes the steps needed to remove the dependency of Microsoft Active Directory (AD) in order to manage authorization locally in Package Contact Center Enterprise (PCCE) components.

Contributed by Meenakshi Sundaram, Ramiro Amaya, and Anuj Bhatia, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Package Contact Center Enterprise
- Microsoft Active Directory

Components Used

The information used in the document is based on PCCE 12.5(1) version.

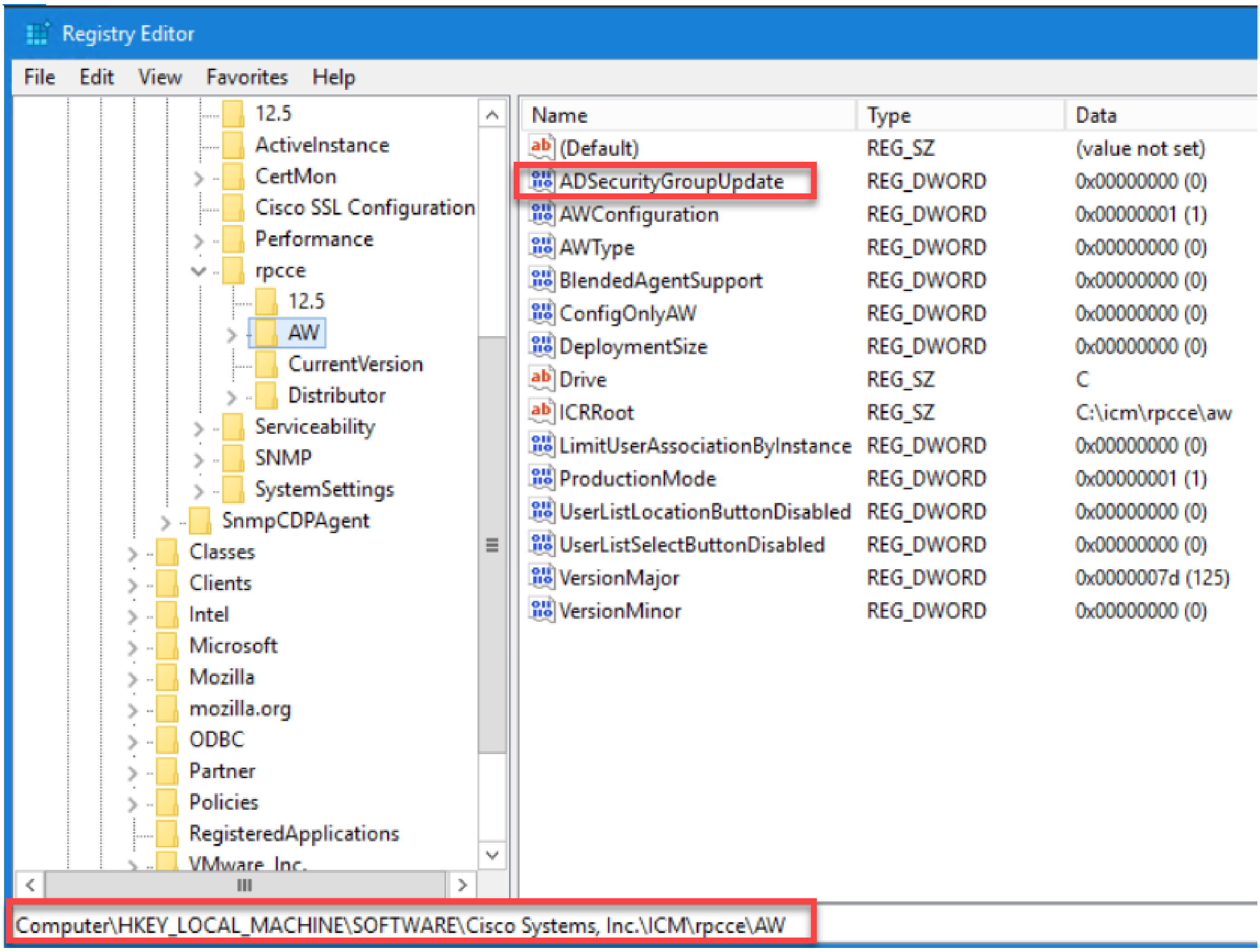
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any step.

Background Information

The PCCE 12.5 release provides user privileges to local user groups on the Administration

Servers (AW), which allows users to move authorization out of Active Directory (AD). This is controlled by the registry **ADSecurityGroupUpdate** which by default is enabled and avoids the use of Microsoft AD Security Groups to control user access rights to perform setup and configuration tasks.

> **Note**: The support for Local Authorization started in Unified Contact Center Enterprise (UCCE) 12.0 and it is now supported in PCCE 12.5.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ADSecurityGroupUpdate	REG_DWORD	0x00000000 (0)
AWConfiguration	REG_DWORD	0x00000001 (1)
AWType	REG_DWORD	0x00000000 (0)
BlendedAgentSupport	REG_DWORD	0x00000000 (0)
ConfigOnlyAW	REG_DWORD	0x00000000 (0)
DeploymentSize	REG_DWORD	0x00000000 (0)
Drive	REG_SZ	C
ICRRoot	REG_SZ	C:\icm\rpcce\aw
LimitUserAssociationByInstance	REG_DWORD	0x00000000 (0)
ProductionMode	REG_DWORD	0x00000001 (1)
UserListLocationButtonDisabled	REG_DWORD	0x00000000 (0)
UserListSelectButtonDisabled	REG_DWORD	0x00000000 (0)
VersionMajor	REG_DWORD	0x0000007d (125)
VersionMinor	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\rpcce\AW

> **Note**: If business needs to have the prior behaviour implemented (AD authorization), the ADSecurityGroupUpdate flag can be changed to 1.

Configure

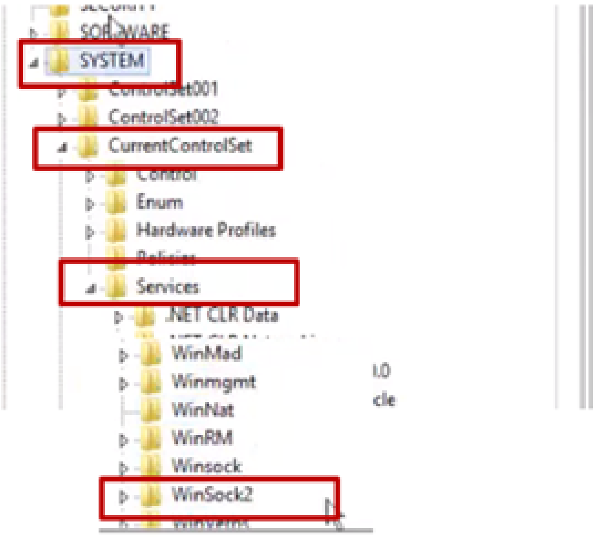
To Grant UcceConfig group permissions in a local AW server, first, permissions need to be provided at the registry level, and second, to the folder level.

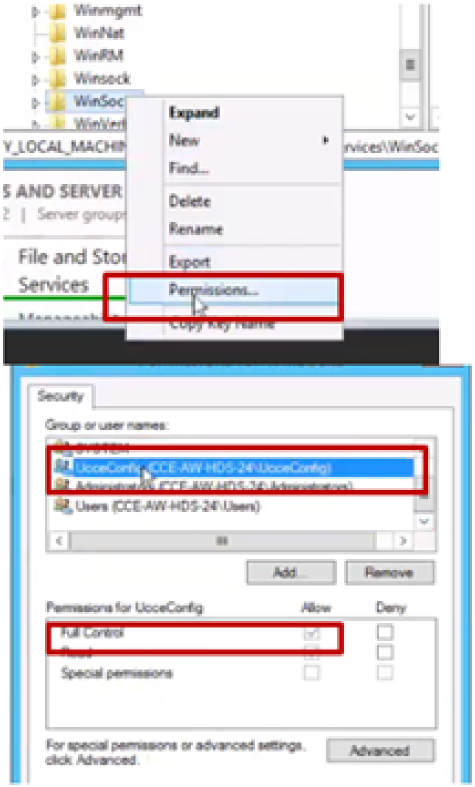
Step 1. Configure Registry Permissions.

1. Run the regedit.exe utility.

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

3. In Permissions under security tab Select **UcceConfig** group and check **Allow for the Full Control** option.




Winmgmt
WinNat
WinRM
Winsock
WinSoc
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Security
Group or user names:
UcceConfig (CCE-AW-HDS-24\UcceConfig)
Administrators (CCE-AW-HDS-24\Administrators)
Users (CCE-AW-HDS-24\Users)
Add...
Remove
Permissions for UcceConfig
Allow
Deny
Full Control ☑ □
Read ☑ □
Special permissions □ □
For special permissions or advanced settings, click Advanced.
Advanced

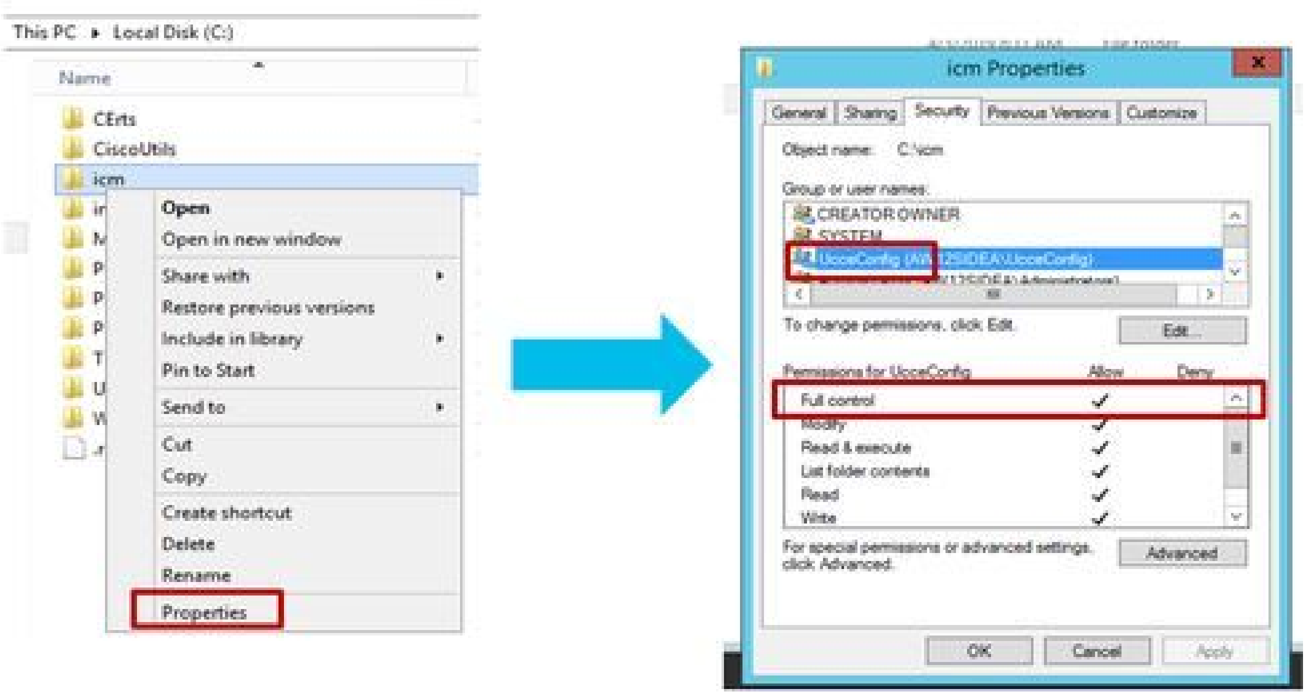
4. Repeat the previous steps to grant full control to the UcceConfig group for these registries.

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

Step 2. Configure Folder Permissions.

1. In Windows Explorer, navigate to `<ICM Installed Directory>:\icm` and select Properties.

2. In Security tab, select **UcceConfig** and check **Allow for the Full Control** option.



3. Select OK to save the changes.

4. Repeat the previous steps to grant full control to the **UcceConfig** group for C:\Temp folder.

5. In SQL Management Studio, do this:

a) Navigate to Security > Logins.

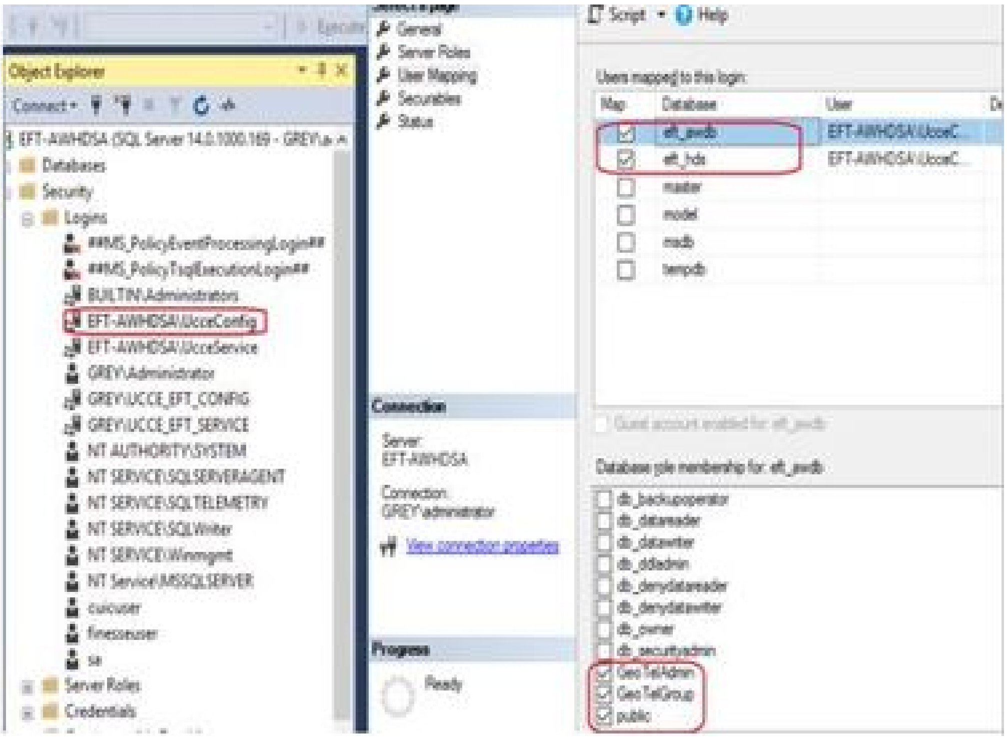
b) Locate <Machine name>\UcceConfig.

c) Right-click and select properties.

d) Navigate User Mappings and select the AWDB database.

e) Tick the GeoTelAdmin, GeoTelGroup and public check boxes.

f) Repeat step d) for the Historical Data (HDS) database.



Server:
EFT-AWHDSA

Connection:
GREY\administrator

Users mapped to this login:

Map	Database	User
☑	eft_awdb	EFT-AWHDSA\UcceC...
☑	eft_hds	EFT-AWHDSA\UcceC...
□	master	
□	model	
□	msdb	
□	tempdb	

□ Guest account enabled for: eft_awdb

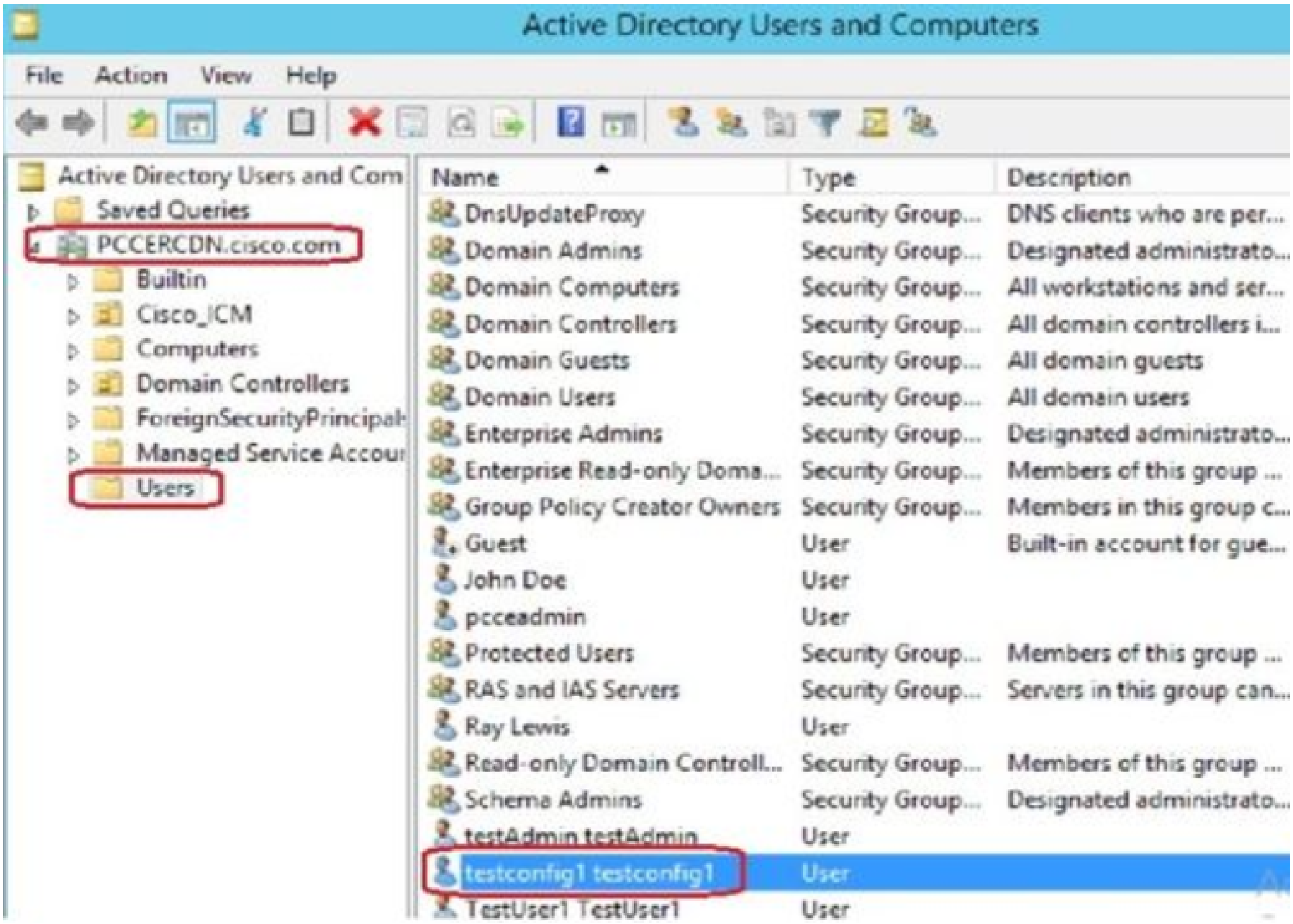
Database role membership for: eft_awdb

□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
□ db_owner
□ db_securityadmin
☑ GeoTelAdmin
☑ GeoTelGroup
☑ public

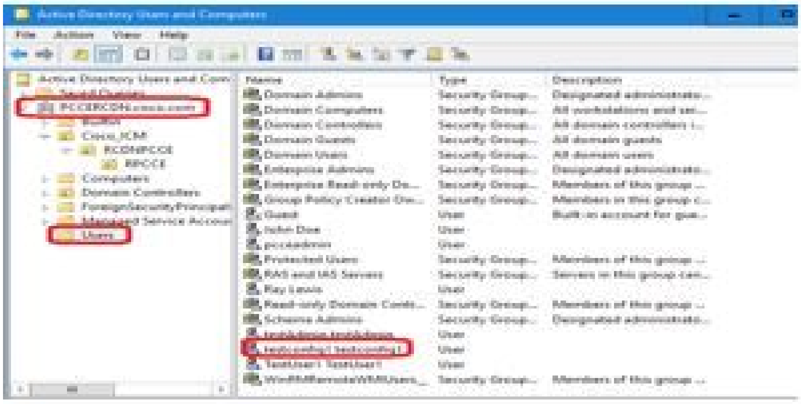
As preliminary configuration has been achieved, follow the steps of how you can promote a domain user in order to have configuration and setup rights.

Step 3. Domain User Configuration.

1. Create a domain user in AD. For this excercise testconfig1 user was created.



Name	Type	Description
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Read-only Doma...	Security Group...	Members of this group ...
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
John Doe	User	
pcceadmin	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Ray Lewis	User	
Read-only Domain Controll...	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
testAdmin testAdmin	User	
testconfig1 testconfig1	User	
TestUser1 TestUser1	User	

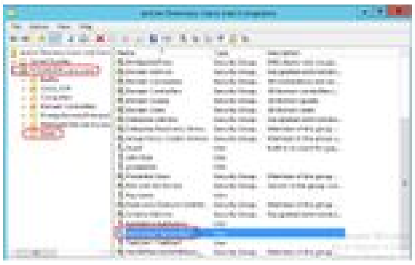


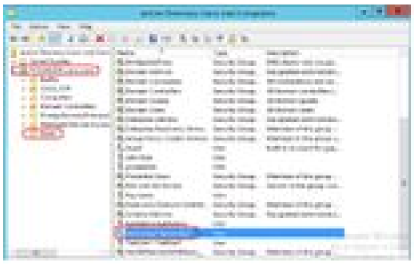
Active Directory Users and Computers

File Action View Help

- Active Directory Users and Com
  - Saved Queries
  - PCCERCDN.cisco.com
    - Builtin
    - Cisco_ICM
      - PCCNPCCE
        - RPCCE
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal
    - Managed Service Accoun
    - Users

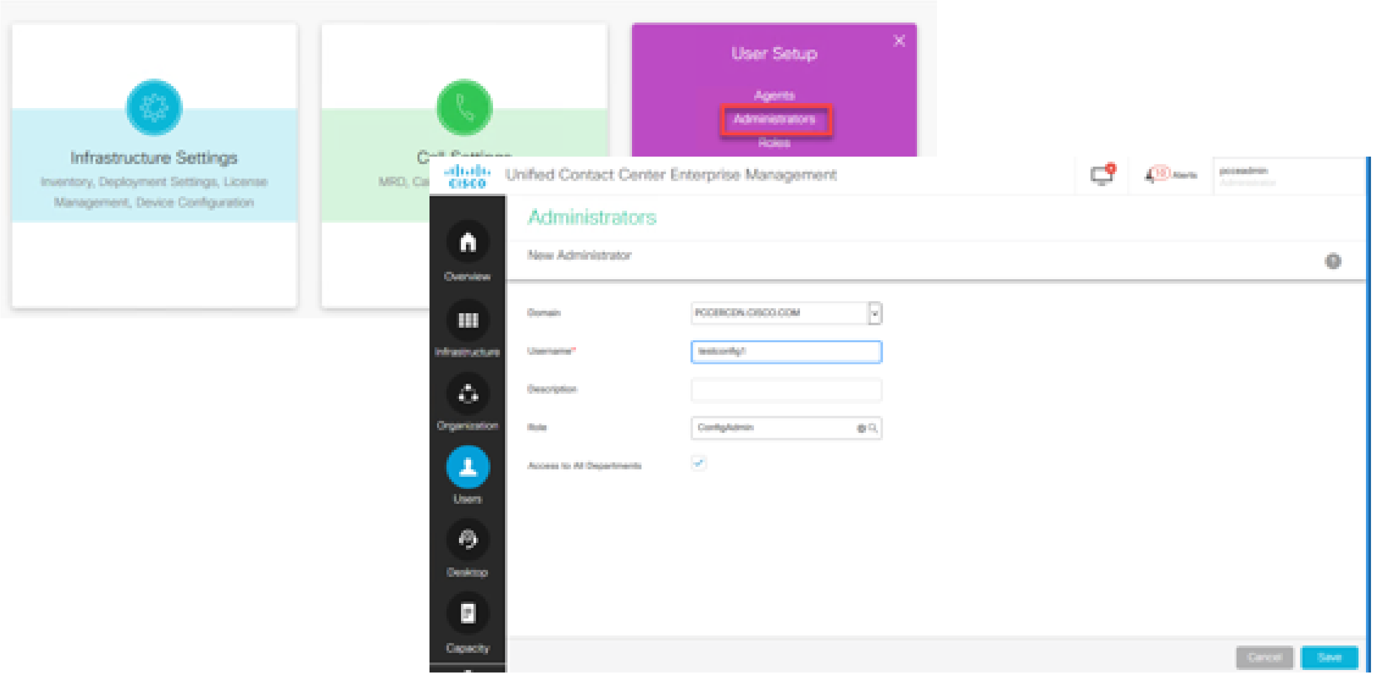
Name	Type	Description
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Read-only Do...	Security Group...	Members of this group ...
Group Policy Creator Ow...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
John Doe	User	
pcceadmin	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Ray Lewis	User	
Read-only Domain Contr...	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
testadmin testadmin	User	
testconfig1 testconfig1	User	
TestUser1 TestUser1	User	
WinRMRemoteWMIUsers_	Security Group...	Members of this group ...





2. Log in to the AW server with a domain admin or local admin account.

3. Open the CCE Admin on the AW. Navigate to the User Setup card, and select Administrators. Add the user and select the role **ConfigAdmin**.



Administrators

New Administrator

Domain: PCCERCDN.CISCO.COM

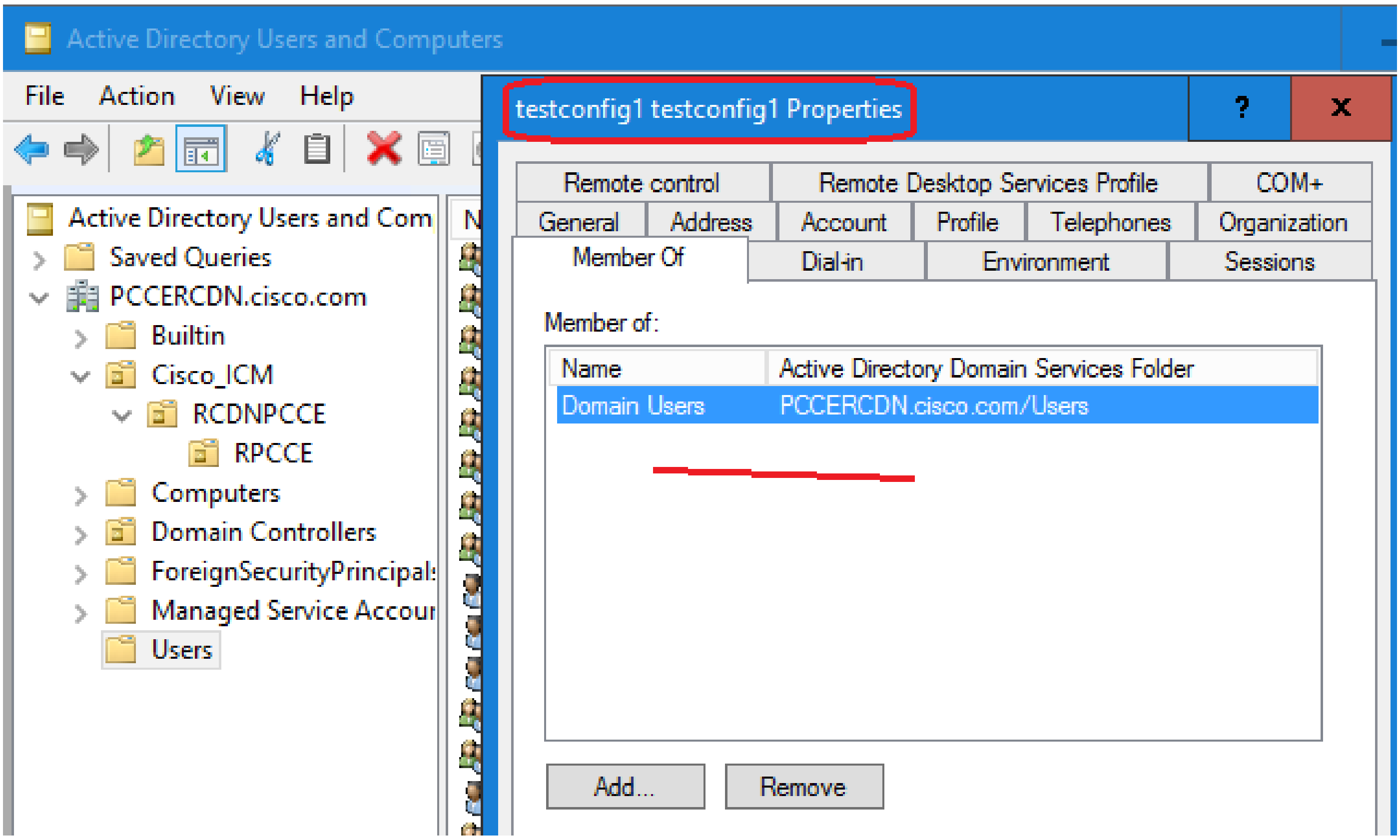
Username*: testconfig1

Description:

Role: ConfigAdmin

Access to All Departments: ☑

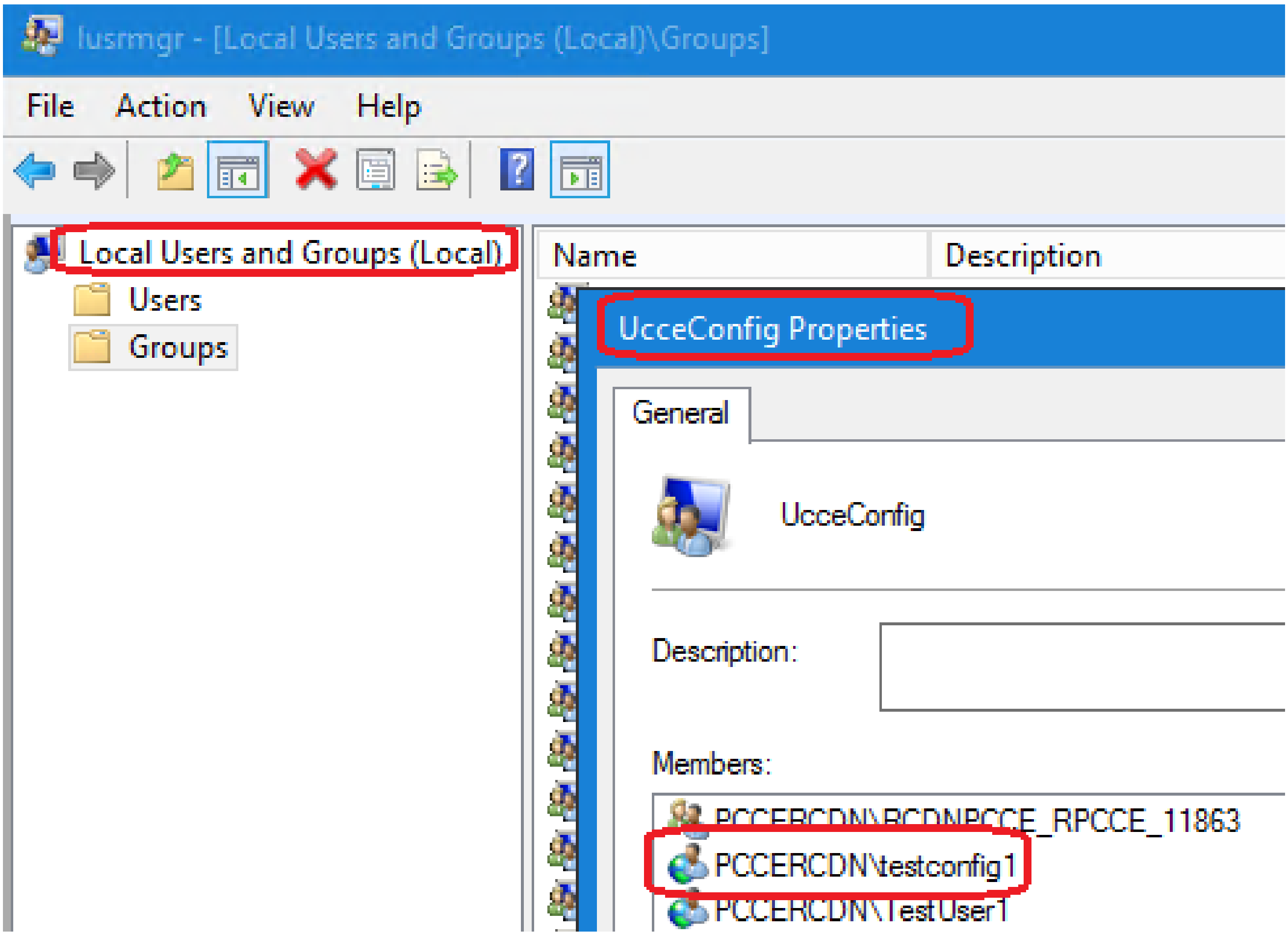
Prior to 12.5 version of PCCE this change would have updated the Config security groups in the domain under an instance Organizational Unit (OU), but with 12.5 the default behaviour is no to add that user to the AD group. As shown in the image, there is no update of this user in the domain ICM Config security group.



Member of:

Name	Active Directory Domain Services Folder
Domain Users	PCCERCDN.cisco.com/Users

4. In the AW Server under **computer management > Local Users and Groups > Groups** select UcceConfig and add testconfig1 user into it.


lusrmgr - [Local Users and Groups (Local)\Groups]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Description
UcceConfig Properties
General

UcceConfig

Description:

Members:

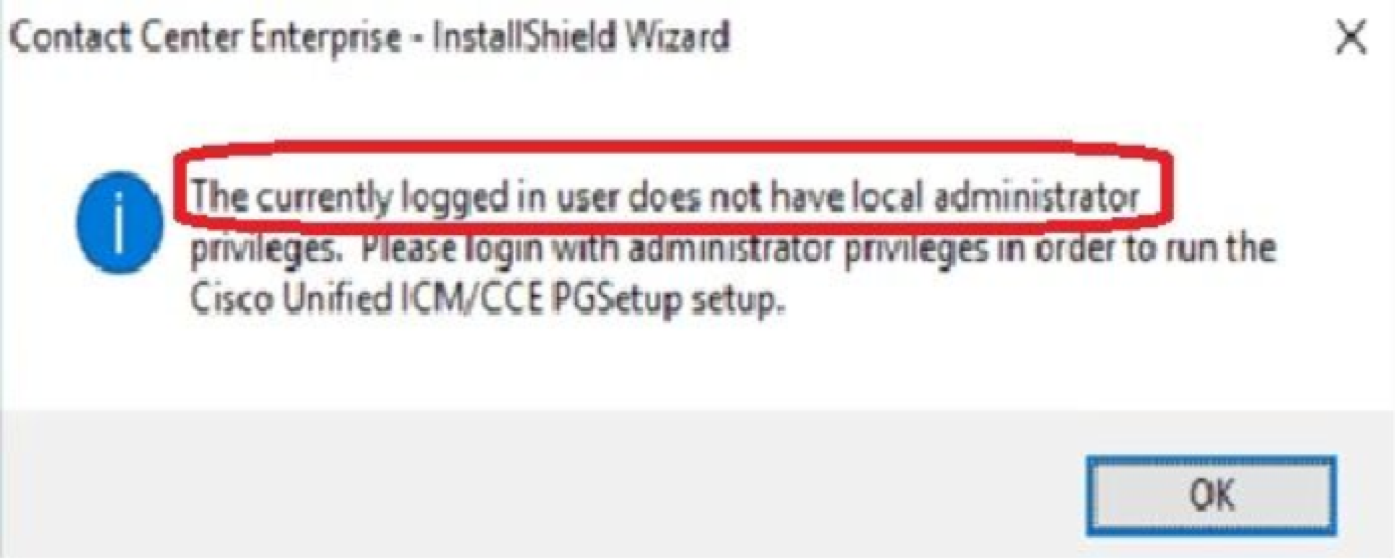
PCCERCDN\RCDNPCCE_RPCCE_11863
PCCERCDN\testconfig1
PCCERCDN\TestUser1

5. Log out from the machine and log in with the credentials of testconfig1 user. As this user has configuration rights, he is able to run CCE configuration tools such as the CCE Admin, Script or

Internet Script Editor.

6. However, If the user tries to run any task which require setup rights, it fails. This user does not have access to all the CCE Admin resources or setup tools.

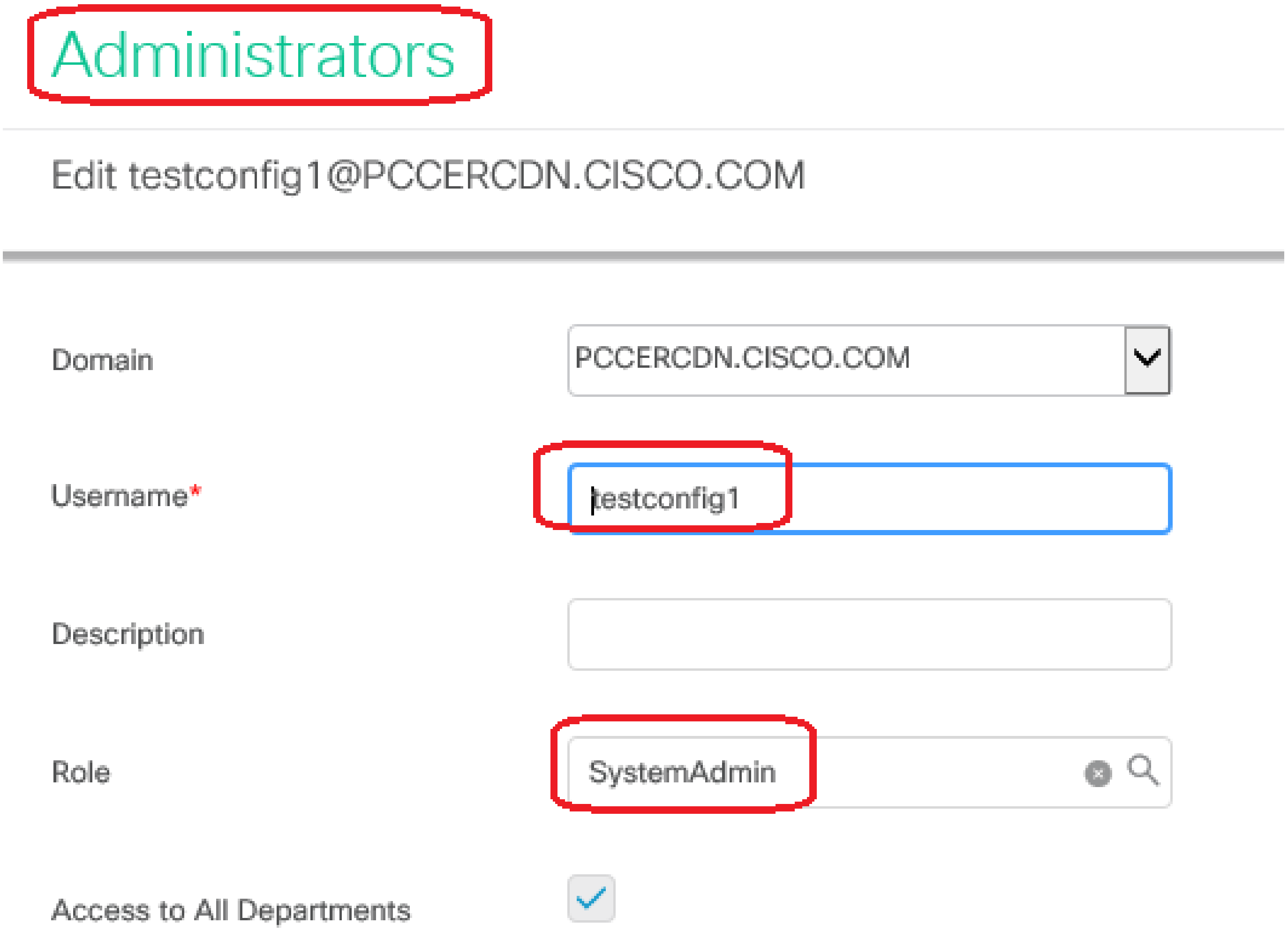
As show in the image, testconfig1 user in PCCE 4K deployment attempts to run the Peripheral Gateway (PG) configuration and the system restricts the change with a warning message.



Contact Center Enterprise - InstallShield Wizard

The currently logged in user does not have local administrator privileges. Please login with administrator privileges in order to run the Cisco Unified ICM/CCE PGSetup setup.

7. If business requires this user to have setup rights along with config, then you have to ensure the user role is changed to SystemAdmin in CCEAdmin.

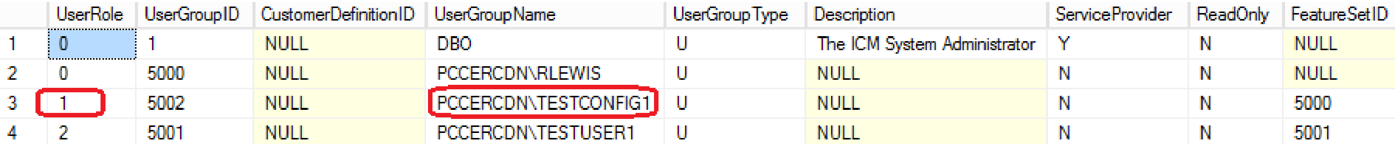


Administrators

Edit testconfig1@PCCERCDN.CISCO.COM

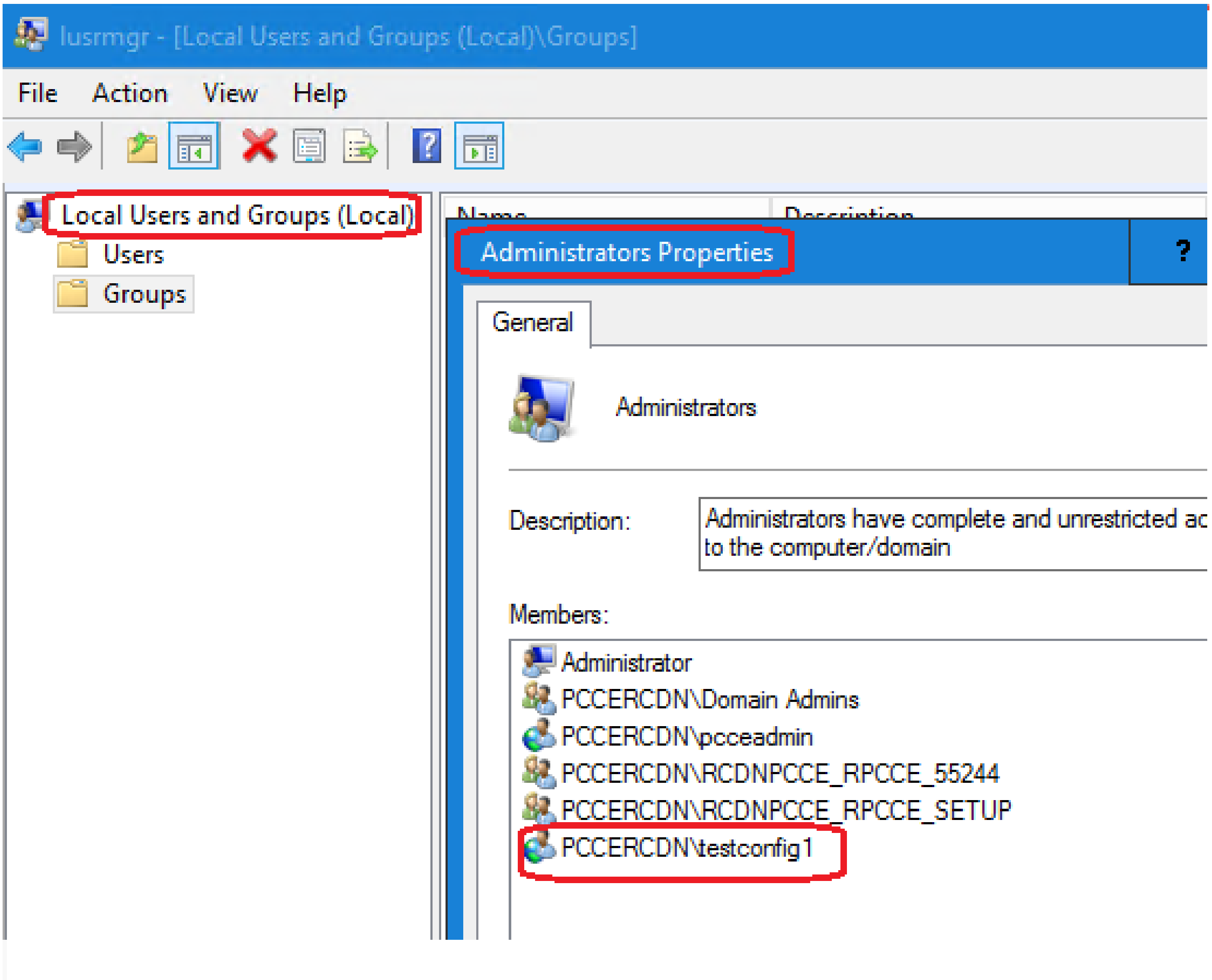
Domain	PCCERCDN.CISCO.COM
Username*	testconfig1
Description	
Role	SystemAdmin
Access to All Departments	✓

User role has been updated as 1 (SystemAdmin) in the database:



	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. Log in to the AW server with the domain or local admin rights account and via **computer management > Local Users and Groups > groups** select Groups and in Administrators add the user to the user.


lusrmgr - [Local Users and Groups (Local)\Groups]

Administrators Properties

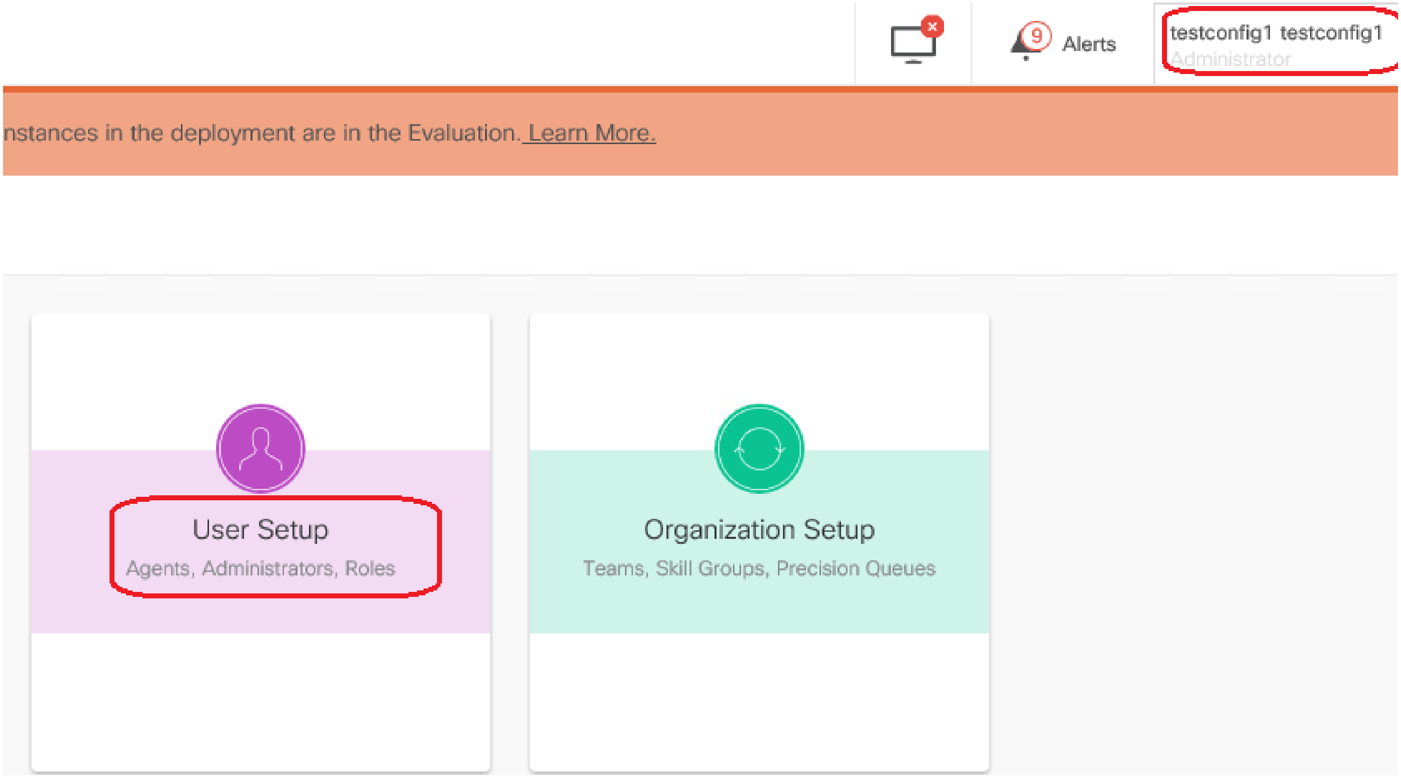
Administrators

Description: Administrators have complete and unrestricted ac to the computer/domain

Members:

- Administrator
- PCCERCDN\Domain Admins
- PCCERCDN\pcceadmin
- PCCERCDN\RCDNPCCE_RPCCE_55244
- PCCERCDN\RCDNPCCE_RPCCE_SETUP
- PCCERCDN\testconfig1

10. The user is now able to access all the resources of CCE application in that AW server and make desired changes.



nstances in the deployment are in the Evaluation. Learn More.

User Setup
Agents, Administrators, Roles
Organization Setup
Teams, Skill Groups, Precision Queues

Verify

The verification procedure is actually part of the configuration process.

Troubleshoot

There is currently no specific steps available to troubleshoot this configuration.

Related Information

PCCE Administration guide

Technical Support & Documentation - Cisco Systems