Configure UCCE 12.0(X) Local Authorization

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Step 1. Configure Registry Permissions
Step 2. Configure Folder Permissions
Verify
Troubleshoot

Introduction

This document describes the steps needed to remove the dependency of microsoft active directory (AD) to manage authorization in Unified Contact Center Enterprise (CCE) components.

Contributed by Anuj Bhatia, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

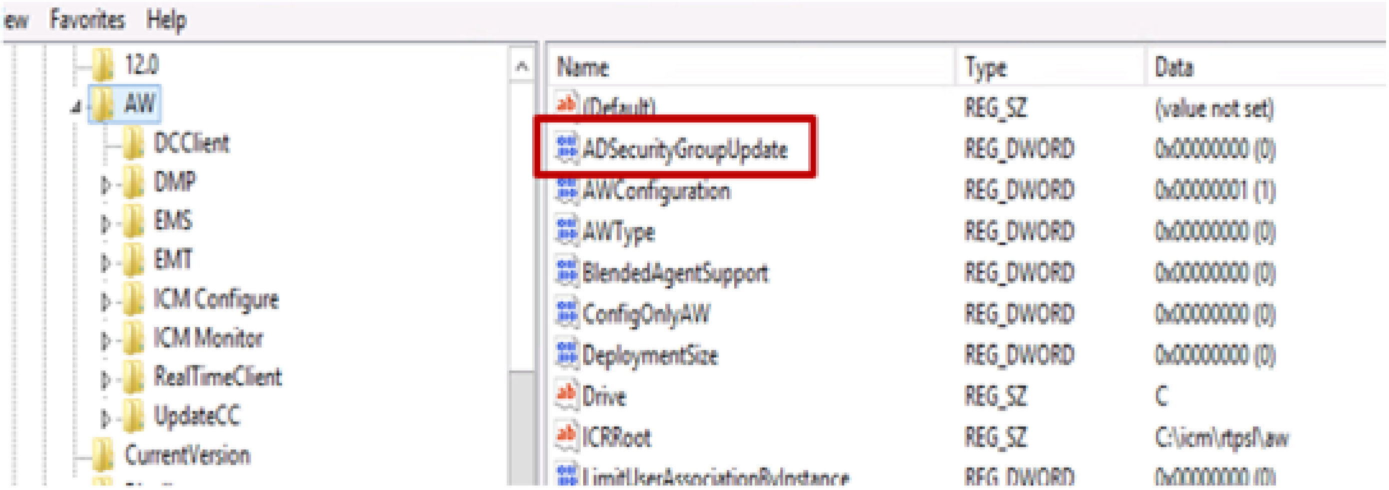
Components Used

The information used in the document is based on UCCE solution 12.0(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 UCCE 12.X release provides user membership privileges to local user groups on the local Administration Server (AW), which allows users to move authorization out of Active Directory (AD). This is controlled by the registry **ADSecurityGroupUpdate** which by defult is enabled and avoids the use of Microsoft AD Security Groups to control user access rights to perform setup and configuration tasks.



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\rtpsl\aw
LimitUserAssociationByInstance	REG_DWORD	0x00000000 (0)

> **Note**: If business wishes to choose the prior behaviour, ADSecurityGroupUpdate flag can be changed to 1 which allows updated to Active Directory (AD)

To move authorization out of AD requires a one-time task on each AW server machine to grant the required permissions for the UcceConfig group and this document aims to showcase the steps needed to configure these permission's along with an example of how to map a domain user as a part of CCE Configuration and Setup group.

Configure

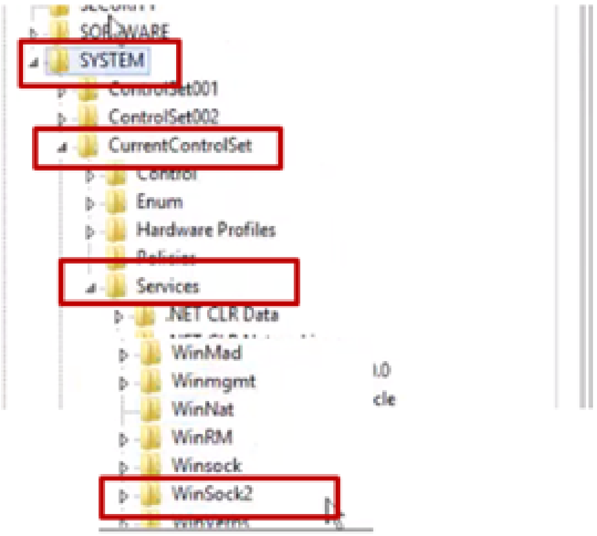
To Grant UcceConfig group permissions in local AW server is a two step process: first, permissions are provided at the registry level, and second, passed on to the folder level.

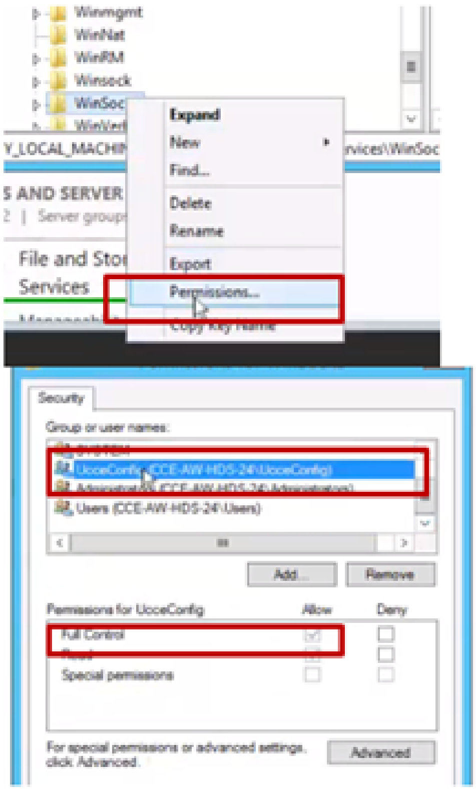
Step 1. Configure Registry Permissions

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

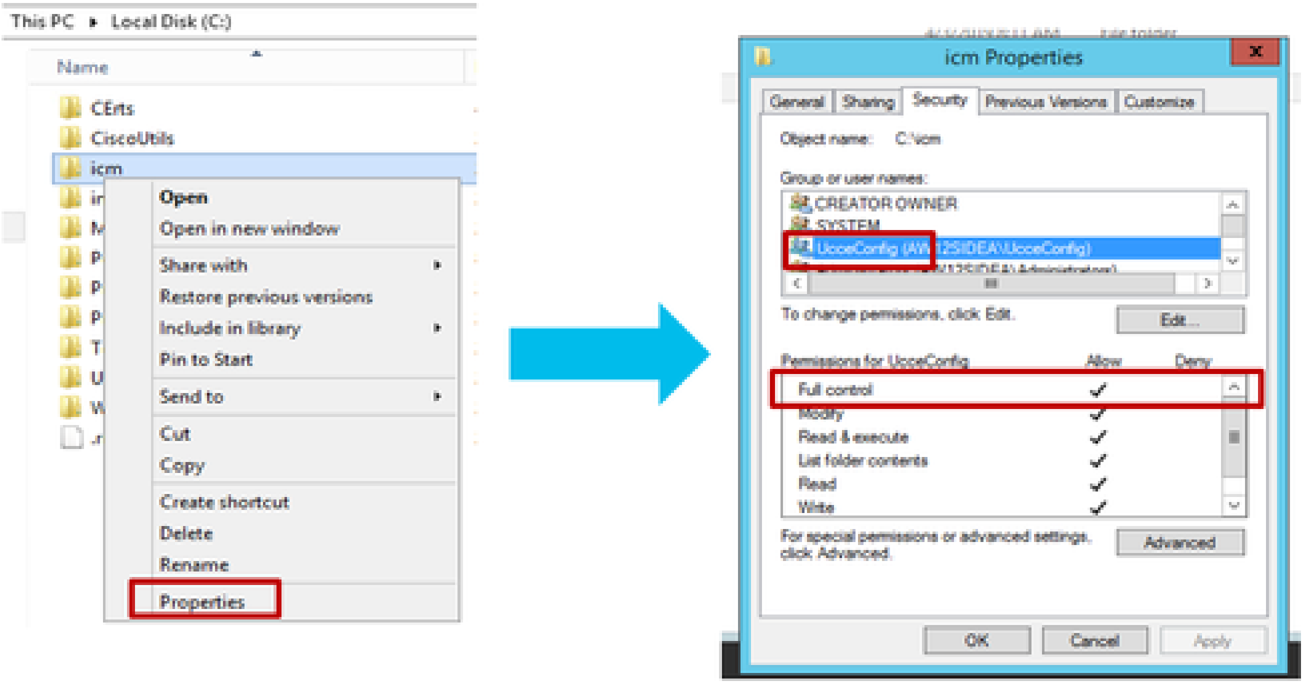
4. Repeat the previous steps to grant Full Control to the UcceConfig group for registries

- **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, select C:\icm and go to Properties.

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



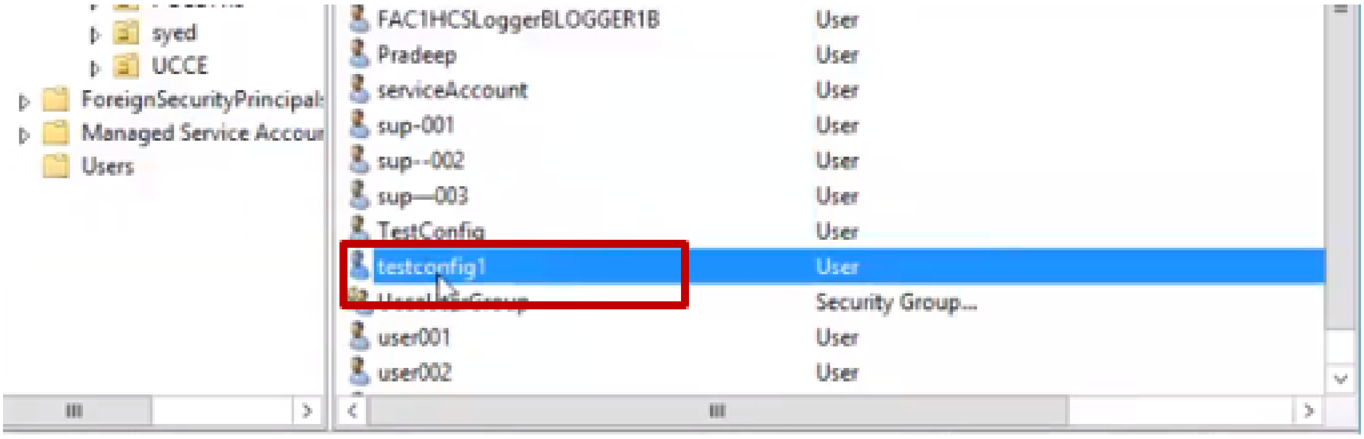
3. Select OK to save the change.

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

As Day 0 preliminary configuration has been acheived, look at the steps on how you can promote a domain user to have configuration and setup rights.

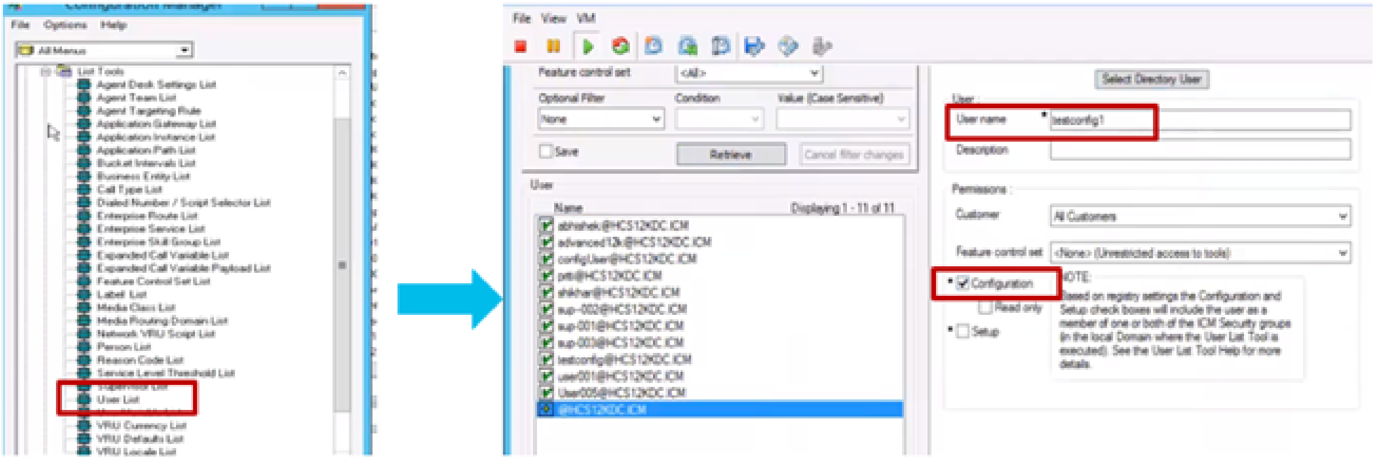
Step 3: Domain User Configuration

1. Create a domain user in AD, for this excercise testconfig1 user had been created.



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

3. In configuration manager through User list tool add the user and check the **configuration** option.



Feature control set <All>

Optional Filter: None; Condition; Value (Case Sensitive)

□ Save

User

Name — Displaying 1 - 11 of 11

- abhishek@HCS12KDC.ICM
- advanced12k@HCS12KDC.ICM
- configUser@HCS12KDC.ICM
- pritl@HCS12KDC.ICM
- shikhar@HCS12KDC.ICM
- sup-002@HCS12KDC.ICM
- sup-001@HCS12KDC.ICM
- sup-003@HCS12KDC.ICM
- testconfig@HCS12KDC.ICM
- user001@HCS12KDC.ICM
- User005@HCS12KDC.ICM
- @HCS12KDC.ICM

User:

User name * testconfig1

Description

Permissions :

Customer: All Customers

Feature control set <None> (Unrestricted access to tools)

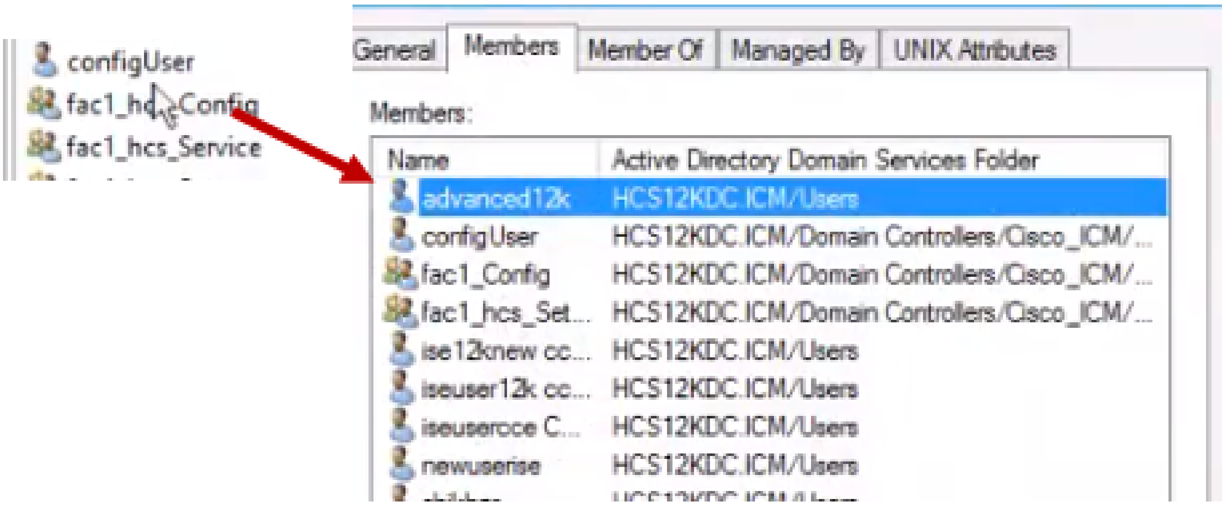
* ☑ Configuration

□ Read only

* □ Setup

NOTE:
Based on registry settings the Configuration and Setup check boxes will include the user as a member of one or both of the ICM Security groups (in the local Domain where the User List Tool is executed). See the User List Tool Help for more details.

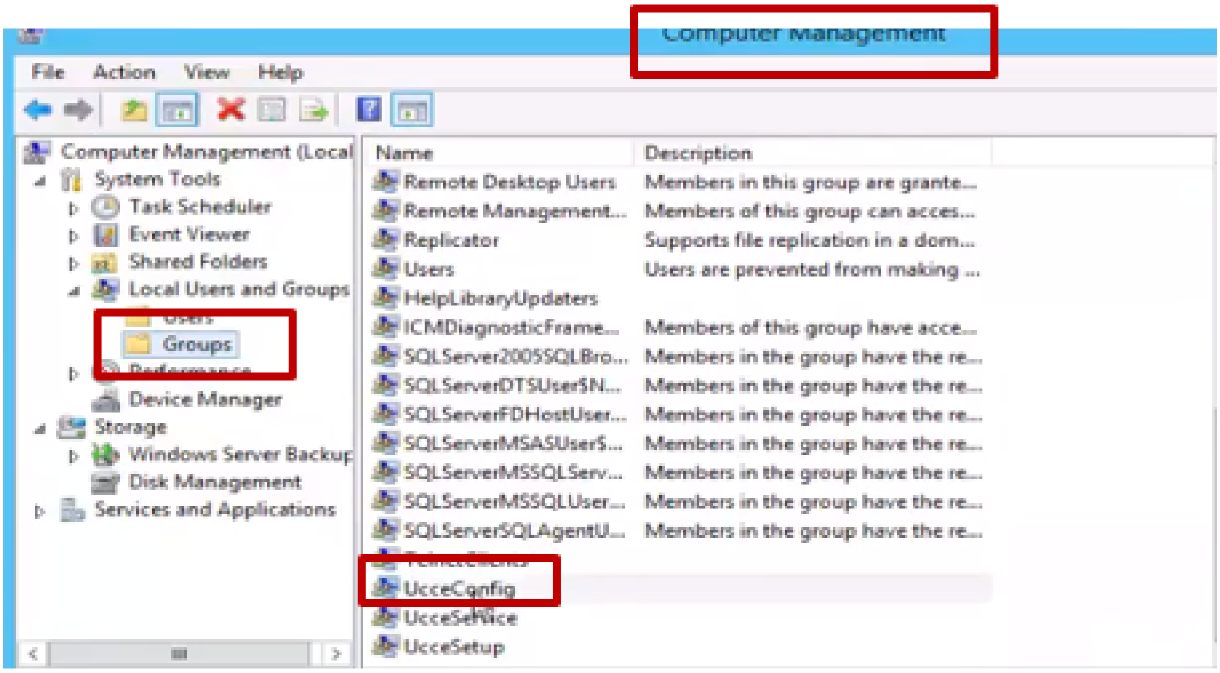
Prior to 12.0 version this change would have updated the Config security groups in the domain under an instance Organizational Unit (OU), but with 12.0 the default behaviour is that it does not add that user to the AD group. As shown in the image, there is no update of this user in the domain ICM Config security group.



Members:

Name	Active Directory Domain Services Folder
advanced12k	HCS12KDC.ICM/Users
configUser	HCS12KDC.ICM/Domain Controllers/Cisco_ICM/...
fac1_Config	HCS12KDC.ICM/Domain Controllers/Cisco_ICM/...
fac1_hcs_Set...	HCS12KDC.ICM/Domain Controllers/Cisco_ICM/...
ise12knew cc...	HCS12KDC.ICM/Users
iseuser12k cc...	HCS12KDC.ICM/Users
iseuserce C...	HCS12KDC.ICM/Users
newuserise	HCS12KDC.ICM/Users

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

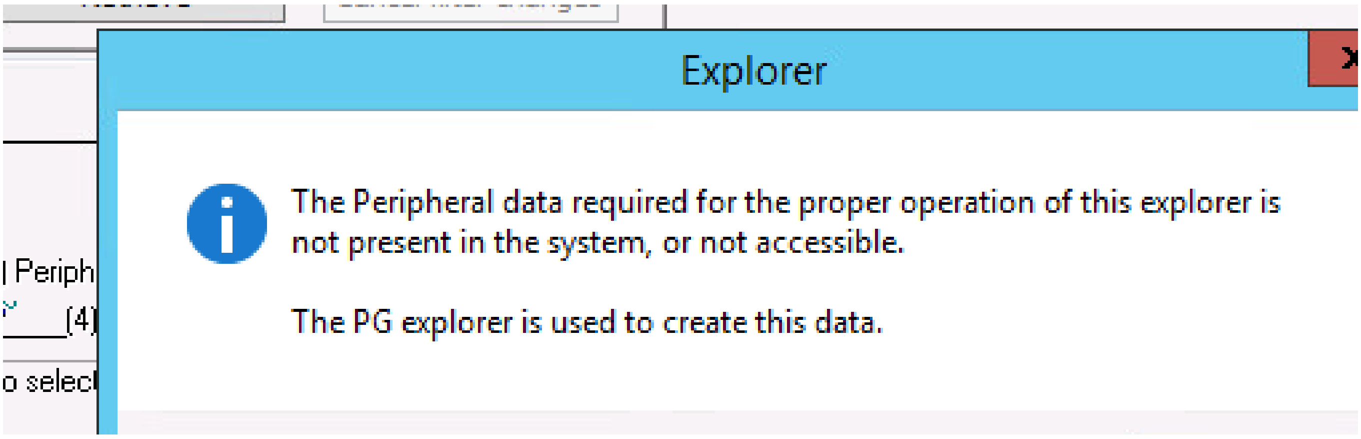


Name	Description
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
HelpLibraryUpdaters	
ICMDiagnosticFrame...	Members of this group have acce...
SQLServer2005SQLBro...	Members in the group have the re...
SQLServerDTSUser$N...	Members in the group have the re...
SQLServerFDHostUser...	Members in the group have the re...
SQLServerMSASUser$...	Members in the group have the re...
SQLServerMSSQLServ...	Members in the group have the re...
SQLServerMSSQLUser...	Members in the group have the re...
SQLServerSQLAgentU...	Members in the group have the re...
TelnetClients	
UcceConfig	
UcceService	
UcceSetup	

5. Log out from the machine and log in with the crendentials of testconfig1 user. As this user has configuration rights it will be able to run CCE configuration tools such as the Configuration Manager , Script or Internet Script Editor.

6. However , If the user tries to execute any task which require setup rights it fails.

This example showcases testconfig1 user changing peripheral gateway (pg) configuration and system restricts the change with a warning message.

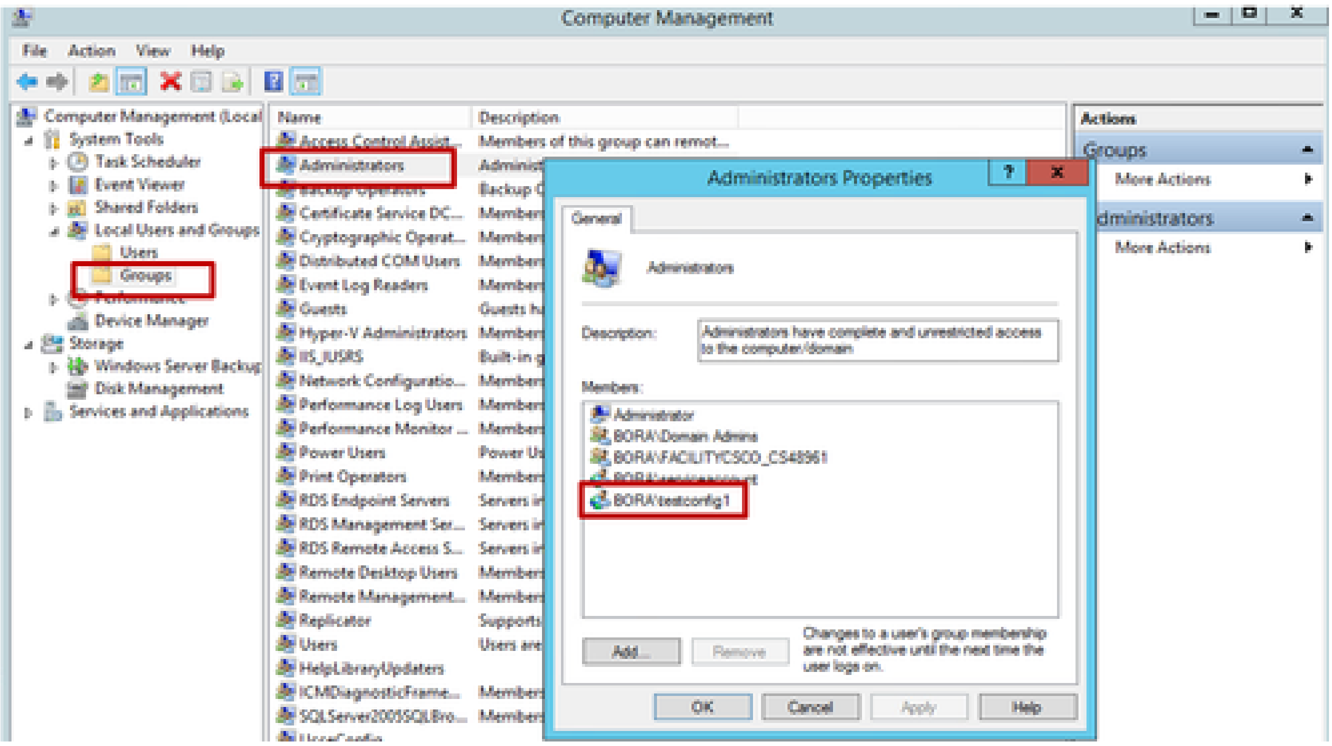


The Peripheral data required for the proper operation of this explorer is not present in the system, or not accessible.

The PG explorer is used to create this data.

7. If business requires this user to have setup rights along with config, then you has to ensure the user is added to the AW server Local Admin group.

8. In order To acheive, 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.



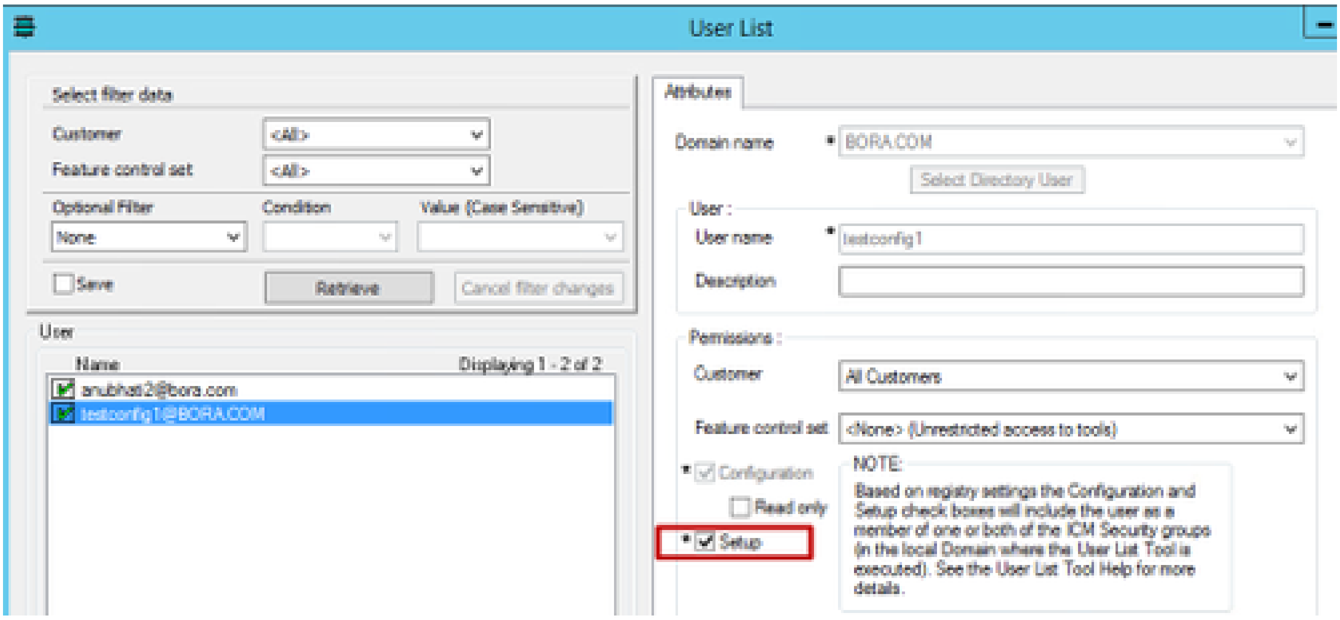
Administrators

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

Members:
- Administrator
- BORA\Domain Admins
- BORA\FACILITYCSCO_CS48961
- BORA\serviceaccount
- BORA\testconfig1

Changes to a user's group membership are not effective until the next time the user logs on.

9. In Configuration manager through User list tool select the user and check the setup option.



Customer: <All>

Feature control set: <All>

Optional Filter: None

☐ Save

Name — Displaying 1 - 2 of 2
- ☑ anubhati2@bora.com
- ☑ testconfig1@BORA.COM

Domain name * BORA.COM

User :

User name * testconfig1

Description

Permissions :

Customer: All Customers

Feature control set: <None> (Unrestricted access to tools)

* ☑ Configuration

☐ Read only

* ☑ Setup

NOTE:
Based on registry settings the Configuration and Setup check boxes will include the user as a member of one or both of the ICM Security groups (in the local Domain where the User List Tool is executed). See the User List Tool Help for more details.

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

Verify

The verification procedure is actually part of the configuration process.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.