Cisco ISE integration with Microsoft SCCM Server

Author: Imran Bashir

Table of Contents

Introduction

What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into whom and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

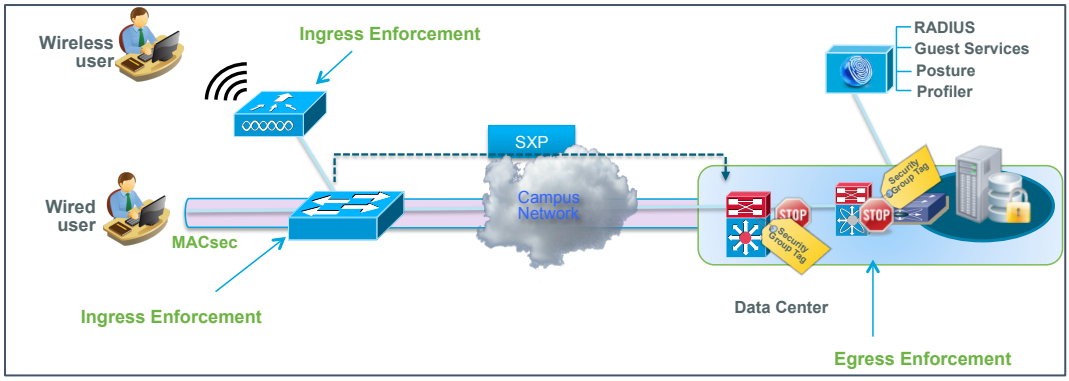


Figure 1.

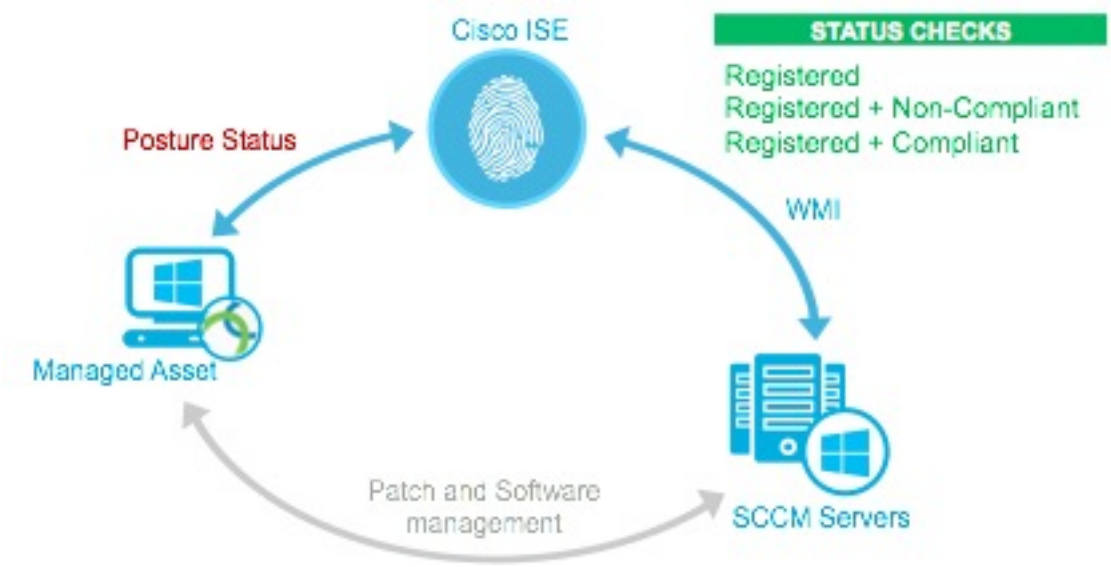
About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy, or simply pick the single use-case that meets your specific need.

Overview

ISE can perform a policy check with SCCM by following methods

- Using AnyConnect for posture (leveraging OPSWAT libraries)
- ISE checking status with SCCM as an MDM Server using WMI



SCCM Policies

There could be various policies configured in SCCM, but you typically start with a baseline policy config, there could be more policies configured by admin

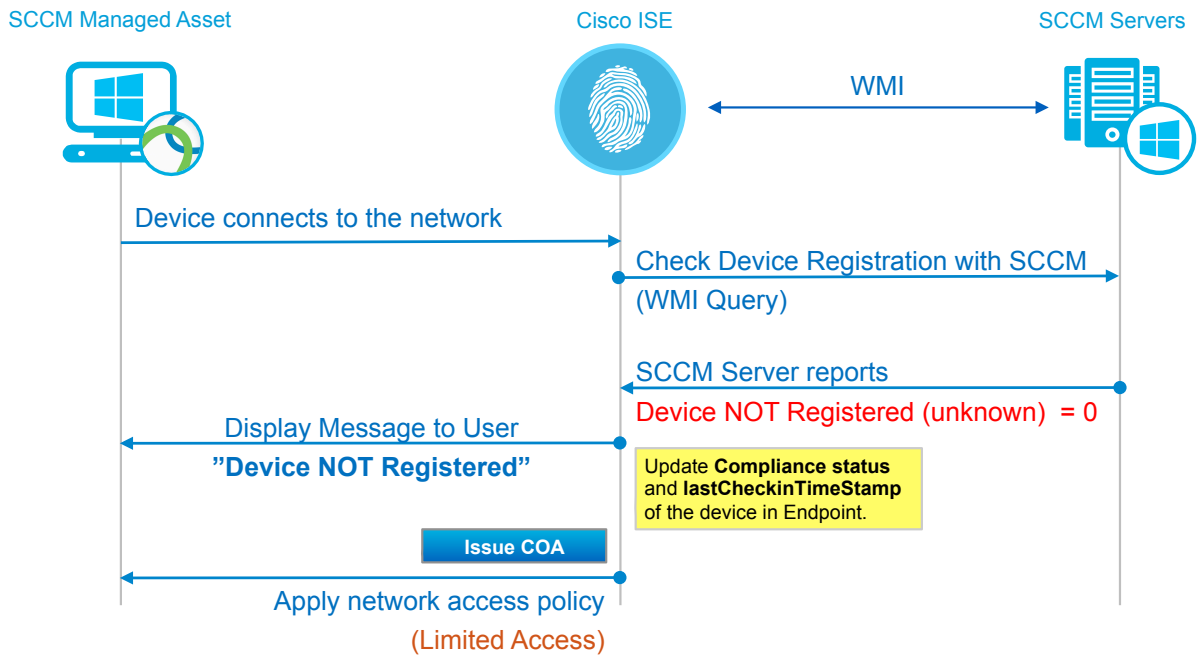
Every policy configured in SCCM generates a policy ID in SCCM, in our findings the Baseline Policy ID does not change even with a new SCCM install.

E.g. Sample Baseline Policy from an SCCM Server CAS
SMS_G_System_CI_ComplianceState.CI_UniqueID='ScopeId_5E0BA349-421B-

4663-8E5F-3D2C408A3FA5/Baseline_28ff969f-cc82-4246-a15d-214d1489b076'

ISE Communication with SCCM Server

ISE leverages WMI to send a Query to SCCM Server, here is an example flow of a managed device, which is NOT registered with SCCM.



SCCM server responds with number of policies configured and the compliance status of those policies e.g. If we have a baseline policy configured with other 2 optional policy checks, ISE will get policy results for all the configured policies in SCCM.

Issue

Once ISE gets results for all the configured policies, it performs and AND function for the final results, i.e to an Endpoint to be compliant, all the configured policies on SCCM must be compliant.
This is why, in current implementation of ISE, you cannot select the

policies to be used for compliance, it's an AND condition.
Sample Query sent from ISE to SCCM Server

select SMS_R_System.Name, SMS_G_System_CI_ComplianceState.CI_UniqueID, SMS_G_System_CI_ComplianceState.ComplianceState, SMS_G_System_CI_ComplianceState.LocalizedDisplayName, SMS_G_System_CH_ClientSummary.LastPolicyRequest from SMS_R_System left join SMS_G_System_CI_ComplianceState on SMS_G_System_CI_ComplianceState.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_CH_ClientSummary on SMS_G_System_CH_ClientSummary.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_NETWORK_ADAPTER on SMS_G_System_NETWORK_ADAPTER.ResourceId = SMS_R_System.ResourceId where (SMS_R_System.MacAddresses like '%MAC_ADDRESS%' OR SMS_G_System_NETWORK_ADAPTER.MACAddress like '%MAC_ADDRESS%') AND SMS_G_System_CI_ComplianceState.CI_UniqueID='ScopeId_5E0BA349-421B-4663-8E5F-3D2C408A3FA5/Baseline_28ff969f-cc82-4246-a15d-214d1489b076'

Workaround (Tested and Verified)

Once we get results for all the configured policies, create a filter in ISE and only look at the Baseline Policy, this ignores the results for any other policy that is configured on SCCM Server, FYR, the filter is marked as red color and is bold.

As mentioned earlier, we haven't seen the baseline policy ID changed across multiple SCCM installs.

mdm.heartbeat.pollintervalMins=5
mdm.constants.httpconnectiontimeout=5000
mdm.constants.readtimeout=30000
mdm.microsoft.intune.discovery.service.relativeurl=/servicePrincipalsByAppId/0000000a-0000-0000-c000-000000000000/serviceEndpoints?api-version=1.6&client-request-id=GENERATE-UUID-PER-REQUEST
mdm.microsoft.intune.service.endpoint.name=NACAPIService
mdm.sccm.namespace.prefix=root\\sms\\site_
mdm.sccm.device.query=select SMS_R_System.Name, SMS_G_System_CI_ComplianceState.CI_UniqueID, \
SMS_G_System_CI_ComplianceState.ComplianceState, SMS_G_System_CI_ComplianceState.LocalizedDisplayName, \
SMS_G_System_CH_ClientSummary.LastPolicyRequest from SMS_R_System left join SMS_G_System_CI_ComplianceState \
on SMS_G_System_CI_ComplianceState.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_CH_ClientSummary \
on SMS_G_System_CH_ClientSummary.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_NETWORK_ADAPTER on \
SMS_G_System_NETWORK_ADAPTER.ResourceId = SMS_R_System.ResourceId where (SMS_R_System.MacAddresses like '%MAC_ADDRESS_VALUE%' \

OR SMS_G_System_NETWORK_ADAPTER.MACAddress like '%MAC_ADDRESS_VALUE%') AND \
SMS_G_System_CI_ComplianceState.CI_UniqueID='ScopeId_5E0BA349-421B-4663-8E5F-3D2C408A3FA5/Baseline_28ff969f-cc82-4246-a15d-214d1489b076'
mdm.sccm.device.query.column.name=SMS_R_System.Name
mdm.sccm.device.query.column.uniqueid=SMS_G_System_CI_ComplianceState.CI_UniqueID
mdm.sccm.device.query.column.compliancestate=SMS_G_System_CI_ComplianceState.ComplianceState
mdm.sccm.device.query.column.policyname=SMS_G_System_CI_ComplianceState.LocalizedDisplayName
mdm.sccm.device.query.column.lastpolicyrequest=SMS_G_System_CH_ClientSummary.LastPolicyRequest
mdm.sccm.device.query.column.key=SMS_G_System_CI_ComplianceState.CI_UniqueID

Workaround (Proposed, Not Tested or Verified)

ISE does not have advance information about the number of policies configured on SCCM server, hence we are not aware of the policy ID's in advance.

If you know the policy ID's and the policy ID does not change (other than Baseline), then you could try adding those policy ID's in to the filter
E.g out of my 10 SCCM policies, I'm only interested in 5 of them, create a filter and include only 5 policy ID's

Again, this is not tested or verified as of now.

Things to change in ISE

Install a Root Patch on ISE and Copy the attached properties file (mdm.properties.gz) and unzip on respective PSN and run tests.

It should query only the baseline policy since we have added the policy ID for baseline policy ONLY.

Recommended to run that query on the SCCM server with MAC Address of on-boarding device. Please check if the PolicyID hardcoded in the

mdm.properties file is ok from Microsoft personnel (we haven't see that change so far).

Copy zip file to the following folder in ISE install
(/opt/CSCOcpm/config directory)

Backup old mdm.properties file
>mv mdm.properties /tmp

Unzip attached zipped file
>gunzip mdm.properties.gz

Make sure unzipped mdm.properties file has proper permissions, if it is read only please change the permissions.
>chmod 755 mdm.properties

A sample successful log is attached FYR (ISESCCMPolicyFixLog)

2017-07-12 15:54:06,518 DEBUG [admin-http-pool6][] cisco.cpm.mdm.api.MdmServerInfoApi -:admin::::- inside the method : callDeviceAttributesApiOnMdmServer with input params - mdmServerId : f4f9a180-674e-11e7-9ac4-000c293a254f, and macAddr : 70:F1:A1:E5:C2:15
2017-07-12 15:54:06,519 DEBUG [admin-http-pool6][] cisco.cpm.mdm.api.MdmServerInfoApi -:admin::::- returning from the method : callDeviceAttributesApiOnMdmServer
2017-07-12 15:54:06,715 TRACE [admin-http-pool6][] cpm.mdm.sccm.util.WmiUtil -:admin::::- WMI Client executeQuery - start query: select SMS_R_System.Name, SMS_G_System_CI_ComplianceState.CI_UniqueID, SMS_G_System_CI_ComplianceState.ComplianceState, SMS_G_System_CI_ComplianceState.LocalizedDisplayName, SMS_G_System_CH_ClientSummary.LastPolicyRequest from SMS_R_System left join SMS_G_System_CI_ComplianceState on SMS_G_System_CI_ComplianceState.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_CH_ClientSummary on SMS_G_System_CH_ClientSummary.ResourceID = SMS_R_System.ResourceId left join SMS_G_System_NETWORK_ADAPTER on SMS_G_System_NETWORK_ADAPTER.ResourceId = SMS_R_System.ResourceId where (SMS_R_System.MacAddresses like '%70:F1:A1:E5:C2:15%' OR SMS_G_System_NETWORK_ADAPTER.MACAddress like '%70:F1:A1:E5:C2:15%') AND SMS_G_System_CI_ComplianceState.CI_UniqueID='ScopeId_5E0BA349-421B-4663-8E5F-3D2C408A3FA5/Baseline_28ff969f-cc82-4246-a15d-214d1489b076', keyproperty: SMS_G_System_CI_ComplianceState@CI_UniqueID
2017-07-12 15:54:06,802 INFO [admin-http-pool6][] cpm.mdm.sccm.util.WmiUtil -:admin::::- Since Unique ID is empty generating Random key to update data.
2017-07-12 15:54:06,816 TRACE [admin-http-pool6][] cpm.mdm.sccm.util.WmiUtil -:admin::::- WMI query returned - key: 1499900046802, values: {LastPolicyRequest=20170712224213.000000+000, LocalizedDisplayName=Himak_file_chk, ComplianceState=1, Name=HK-PC-WIN7}
2017-07-12 15:54:06,817 TRACE [admin-http-pool6][] cpm.mdm.sccm.util.WmiUtil -:admin::::- WmiUtil - executeQuery - last element - Incorrect function. [0x00000001]

```
2017-07-12 15:54:06,817 TRACE  [admin-http-pool6][] cpm.mdm.sccm.util.WmiUtil -:admin:::- WMI Client
executeQuery - end
2017-07-12 15:54:06,817 TRACE  [admin-http-pool6][] cpm.mdm.sccm.api.SccmClient -:admin:::- SCCM returned
device with compliance state: true, checkinTime: 1484289733000, failureReason:
2017-07-12 15:54:06,817 DEBUG  [admin-http-pool6][] cpm.mdm.sccm.api.SccmClient -:admin:::- Found device with
mac: 70:F1:A1:E5:C2:15  formatted mac 70:F1:A1:E5:C2:15 in SCCM server: SCCM1
2017-07-12 15:54:06,883 DEBUG  [admin-http-pool6][] cisco.cpm.mdm.util.MDMUtil -:admin:::- updating device mdm
attributes - mdmServer id: f4f9a180-674e-11e7-9ac4-000c293a254f in endpoint
2017-07-12 15:54:06,883 DEBUG  [admin-http-pool6][] cisco.cpm.mdm.util.MDMUtil -:admin:::- updating device mdm
attributes - mdmServer name: SCCM1 in endpoint
2017-07-12 15:54:07,195 DEBUG  [admin-http-pool6][] cisco.cpm.mdm.util.MDMUtil -:admin:::- updated device mdm
attributes with macaddress: 70:f1:a1:e5:c2:15
2017-07-12 15:54:07,195 DEBUG  [admin-http-pool6][] cisco.cpm.mdm.api.MdmEndpointData -:admin:::-
MdmEndpointData ==> com.cisco.cpm.mdm.api.MdmEndpointData
 Object {
  macaddress: null
  OperatingSystem:
  isRegistered: true
  isCompliant: true
  registrationFailureReason: null
  compliancefailureReason: null
  complianceFailureRemediation: null
  isDiskEncryptionOn: false:
  isPinlockOn: false
  isJailbroken: false
  manufacturer:
  model:
  imei:
  serialNumber:
  phoneNumber:
  meid:
  udid:
  vendorAssignedMdmServerName: SCCM1
  errorMsg: null
  errorOccurred: false
}
```

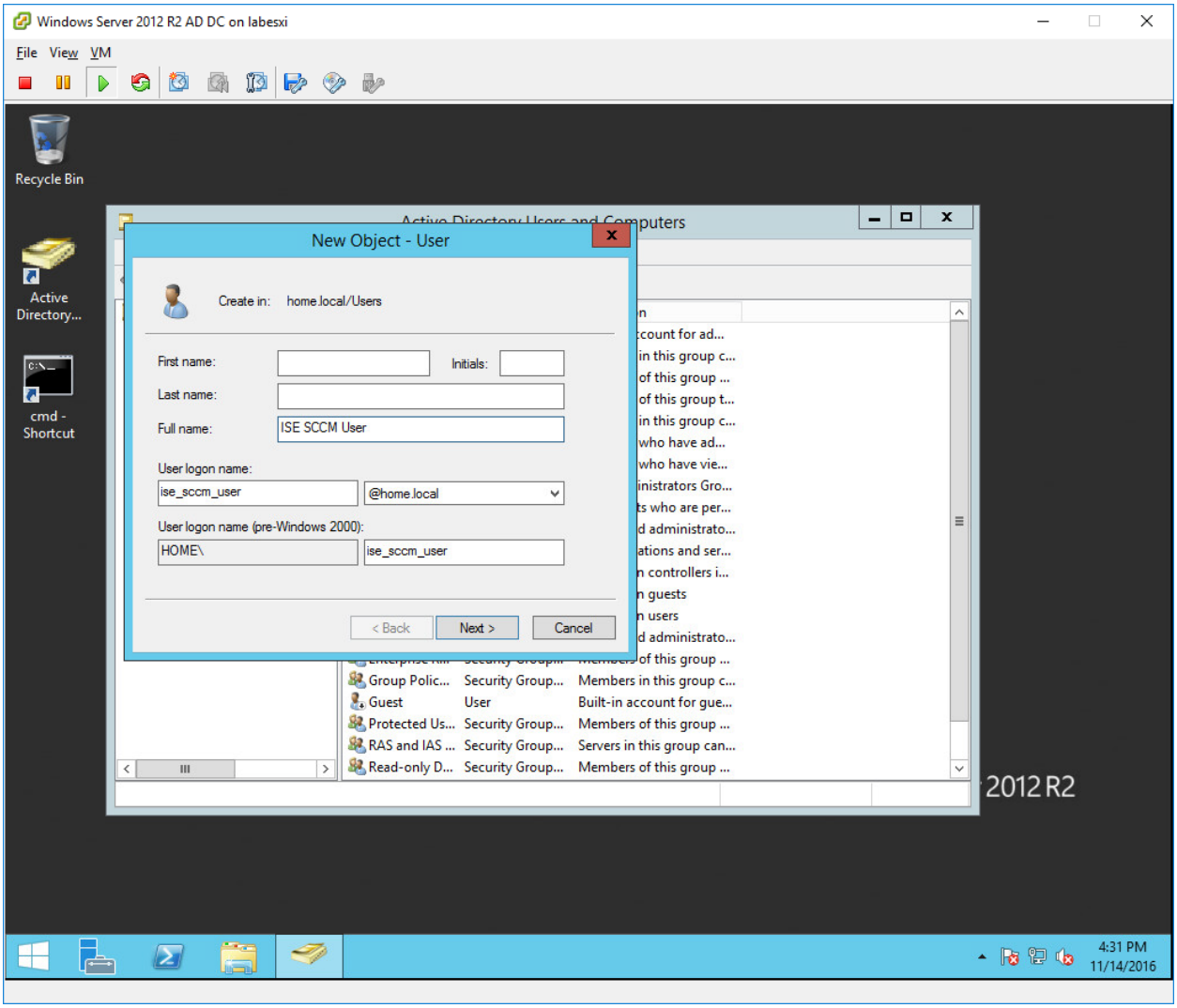
Changes on Microsoft SCCM Server

Central Administration Server (CAS)

Step 1 – Create a user within the Active Directory domain that will be used by ISE to communicate with SCCM and issue queries about the status of authenticating machines.

a. Open Active Directory Users and Computers administrative tool.

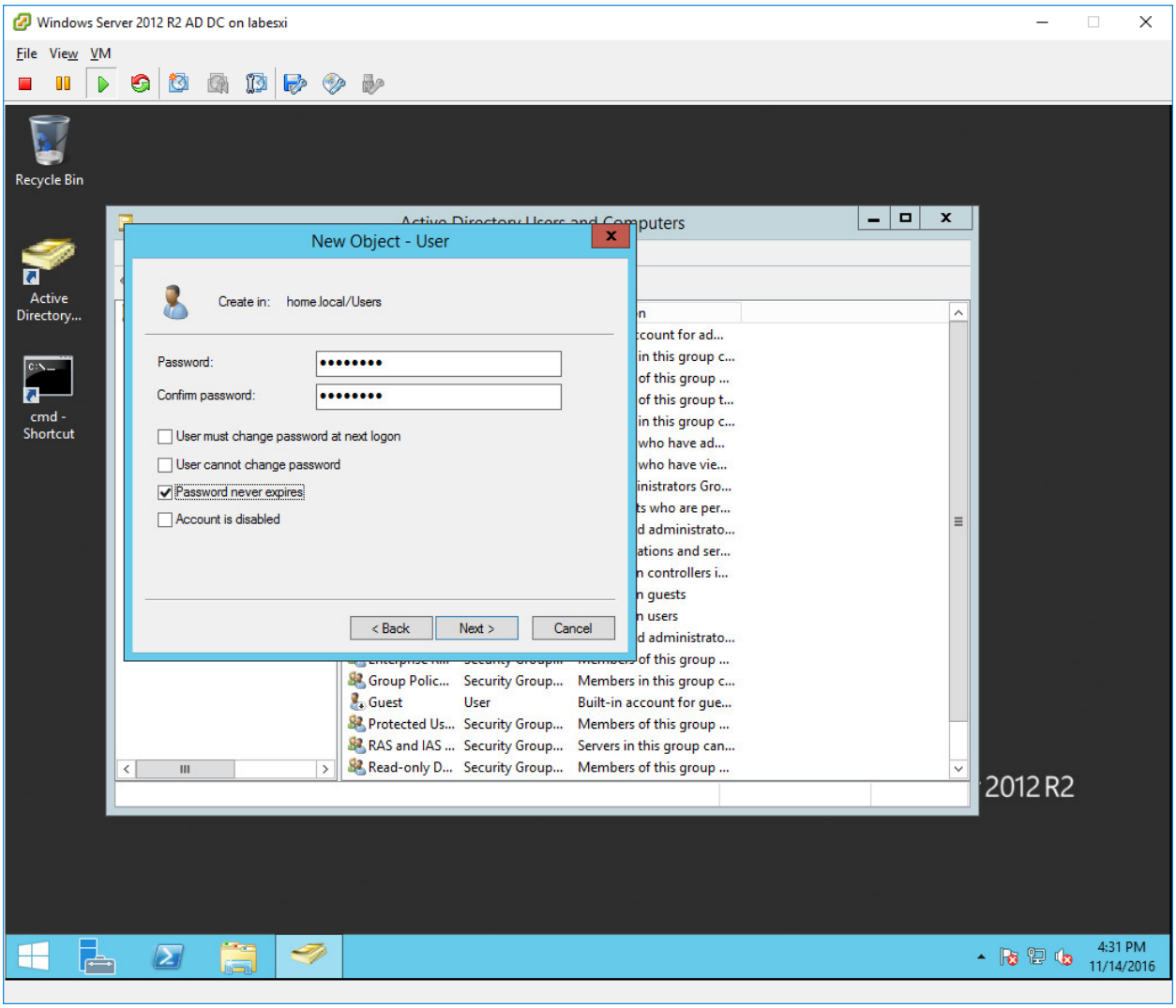
b. Right-click on the OU container where you want to create the new user and select the option to create a new user. You should see the following dialog box.



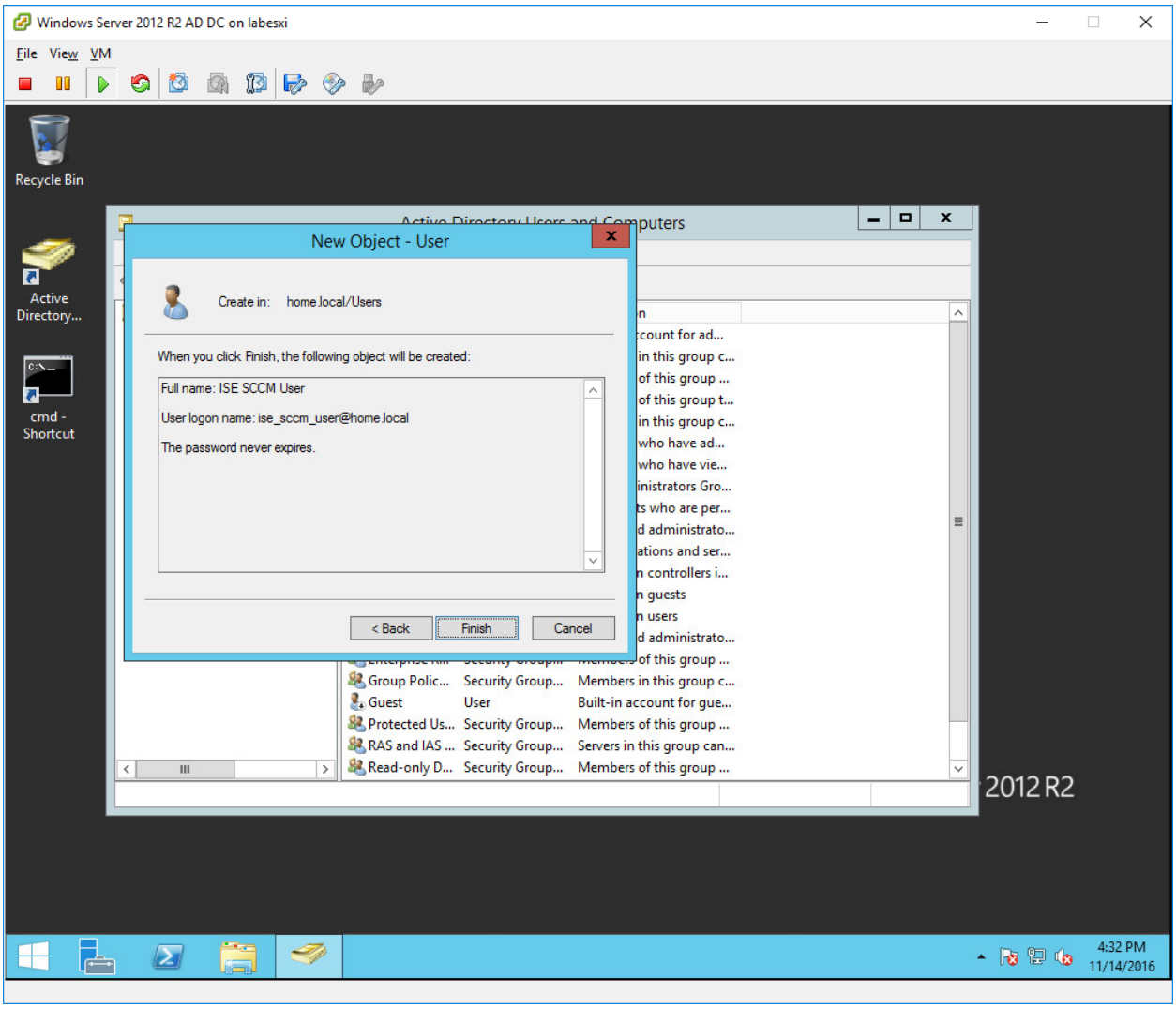
c. Fill in the information as necessary. Select Next. In this example, we are using the “ise_sccm_user” logon name.

d. Create a password that adheres to your organization’s security policy.

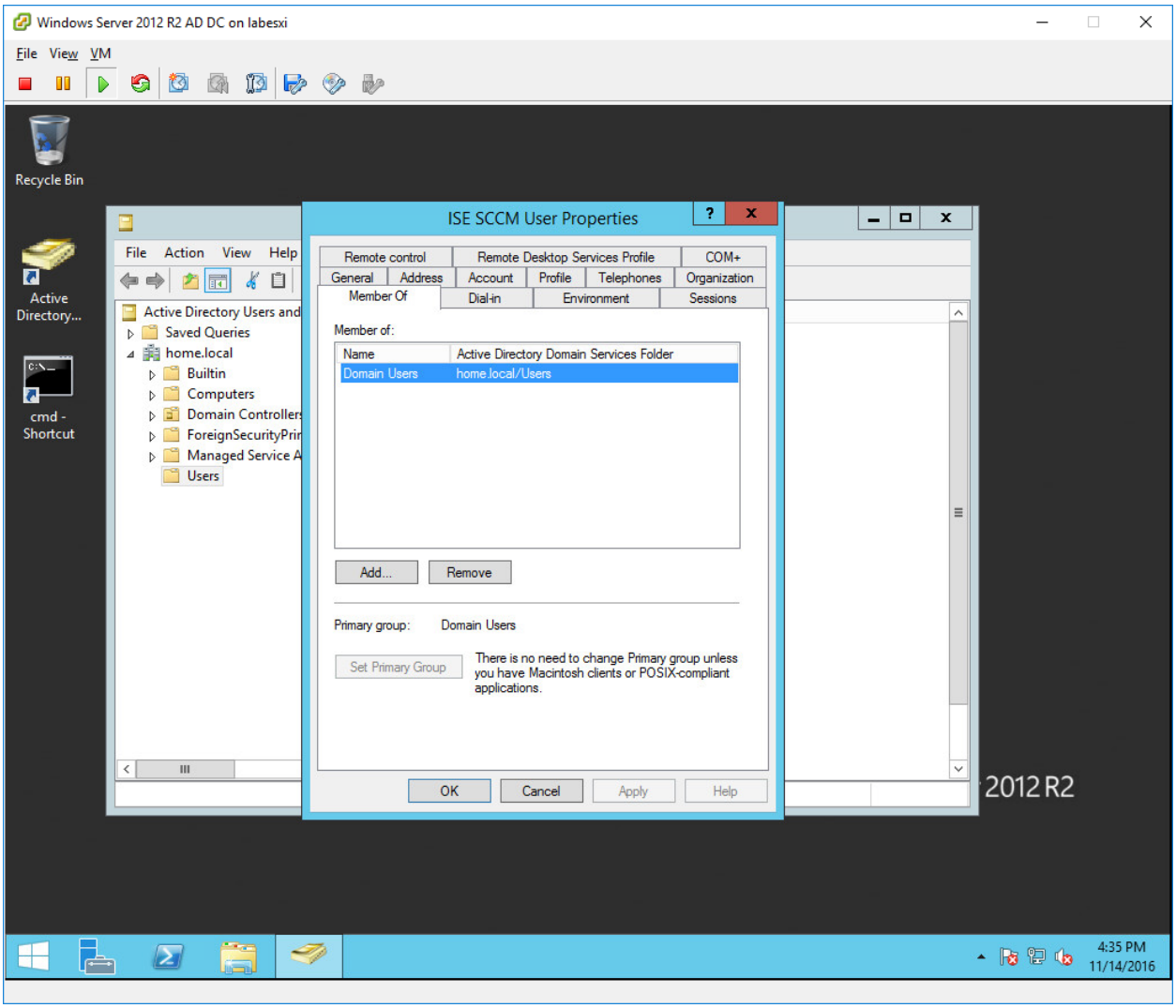
e. Uncheck the option “User must change password at next logon”.



f. Click Next. You should see the following.

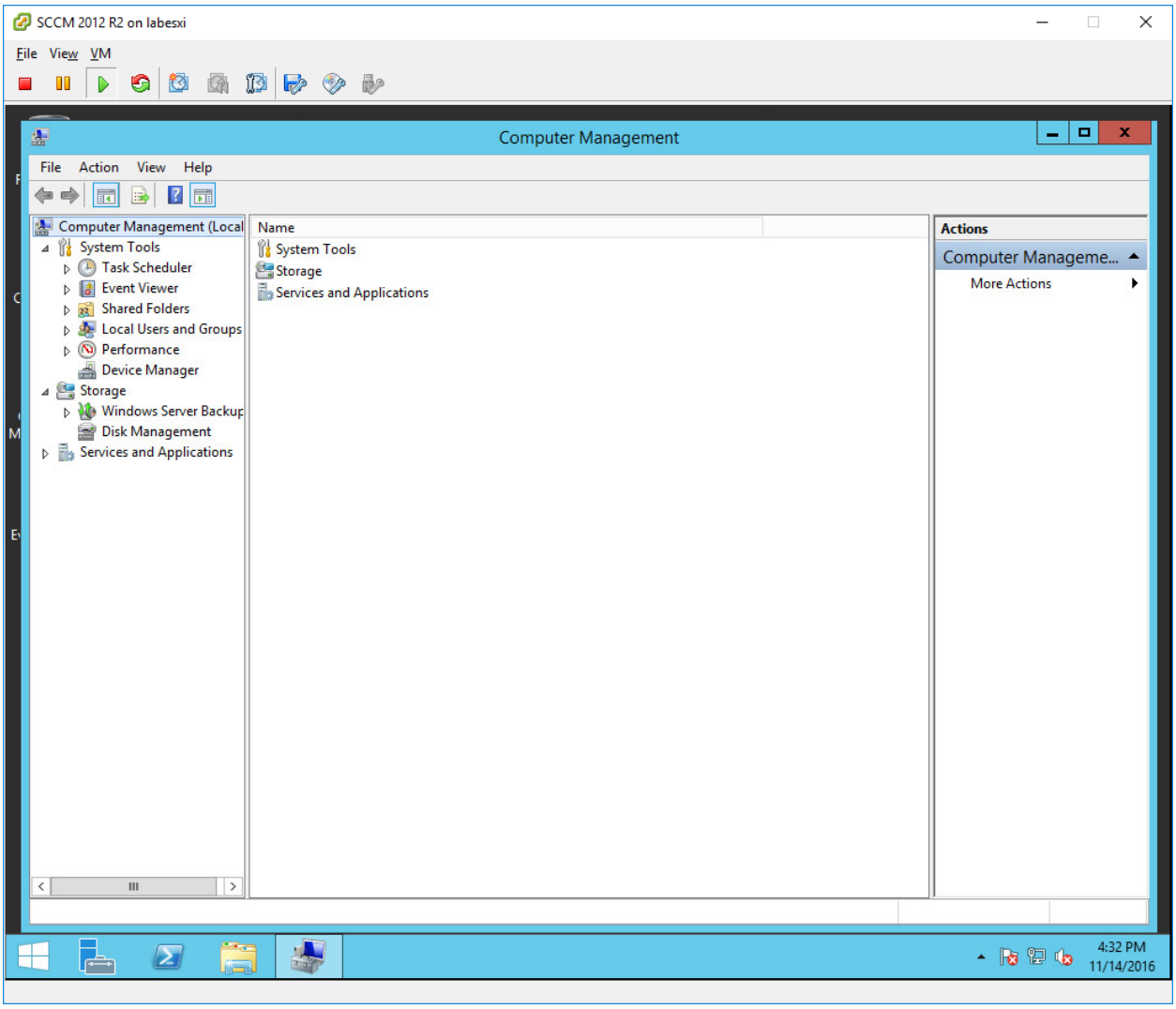


g. The new user is now created. If you check the properties of the user, you will see that the user is only a member of the Domain Users security group in AD.

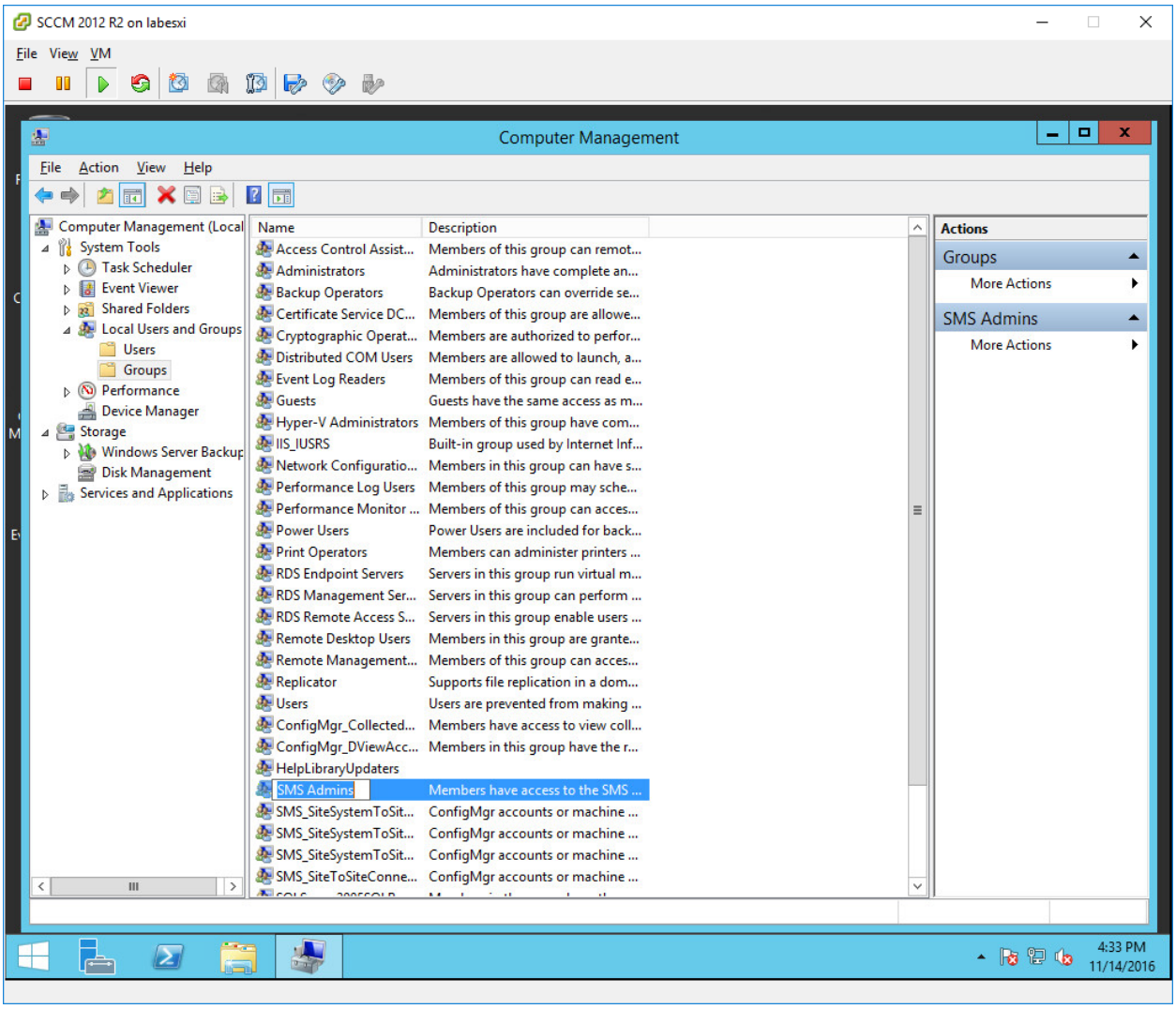


Step 2 – Add the new user created in Step 1 to the “SMS Admins” security group on the Microsoft SCCM Server.

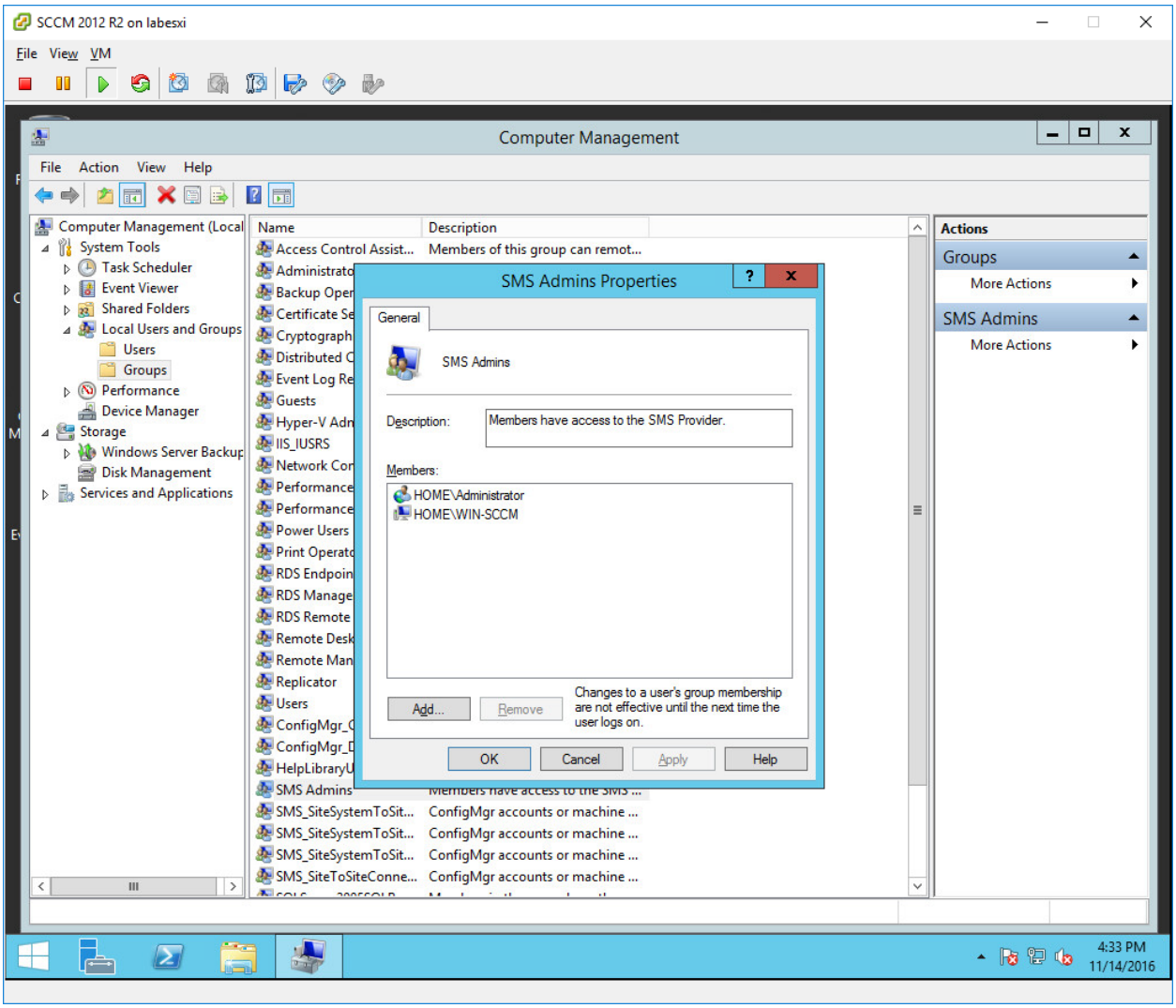
a. On the SCCM Server, open the Computer Management administrative tool.



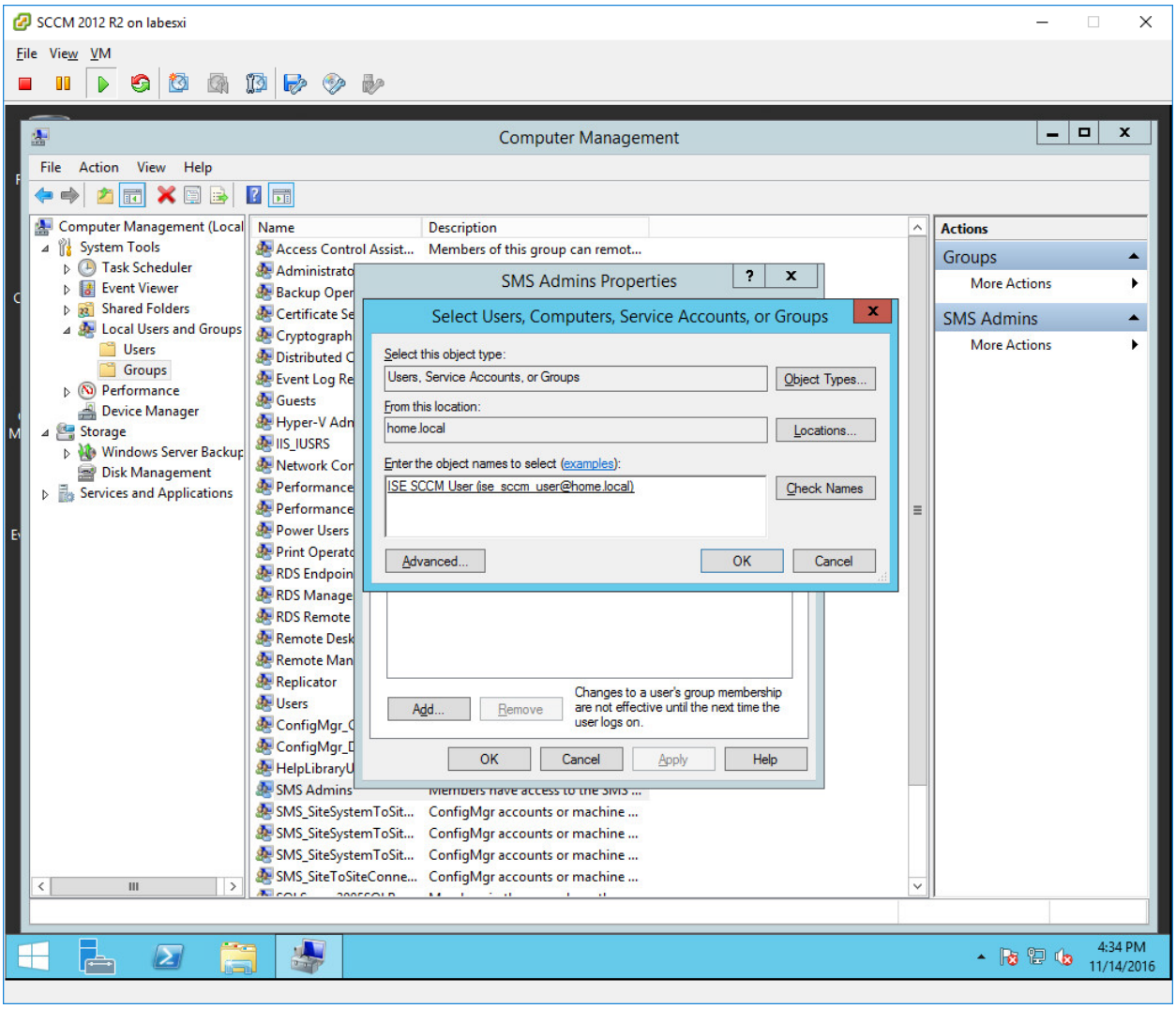
b. Select Local Users and Groups.
c. Select Groups.
d. Locate the “SMS Admins” security group.



e. Double click on the “SMS Admins” security group. This will open up the dialog box showing which users and groups are a member of this local security group.



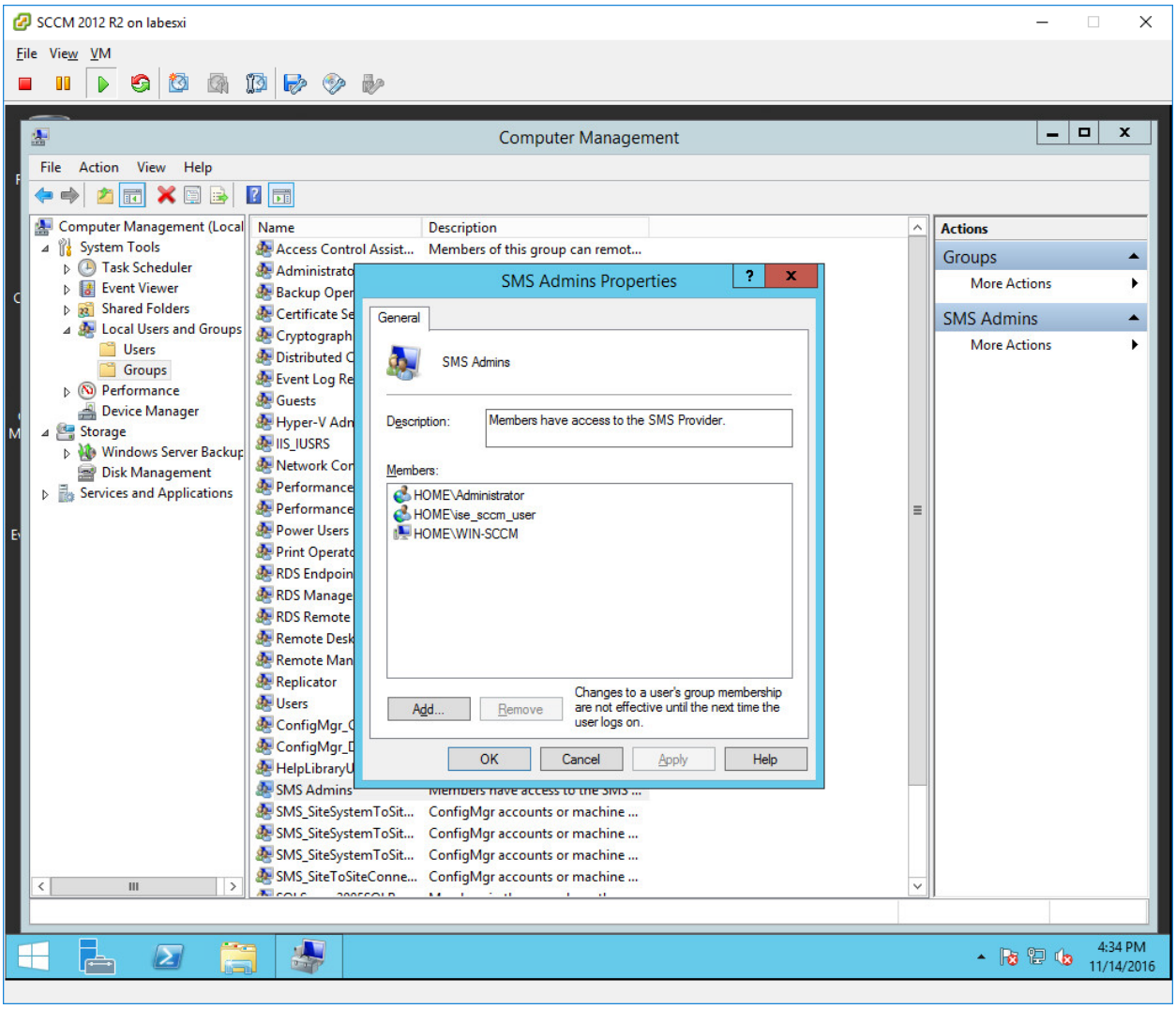
f. We need to add the user created for ISE to this group. Select the “Add…” button.



g. Ensure the location selected is the Active Directory domain. In this example, the domain name is “home.local”.

h. Enter the logon name of the account created in Step 1 and then select the “Check Names” button. The user name should now be underlined, indicating that the server was able to locate the object in the AD domain.

i. Select “OK”.



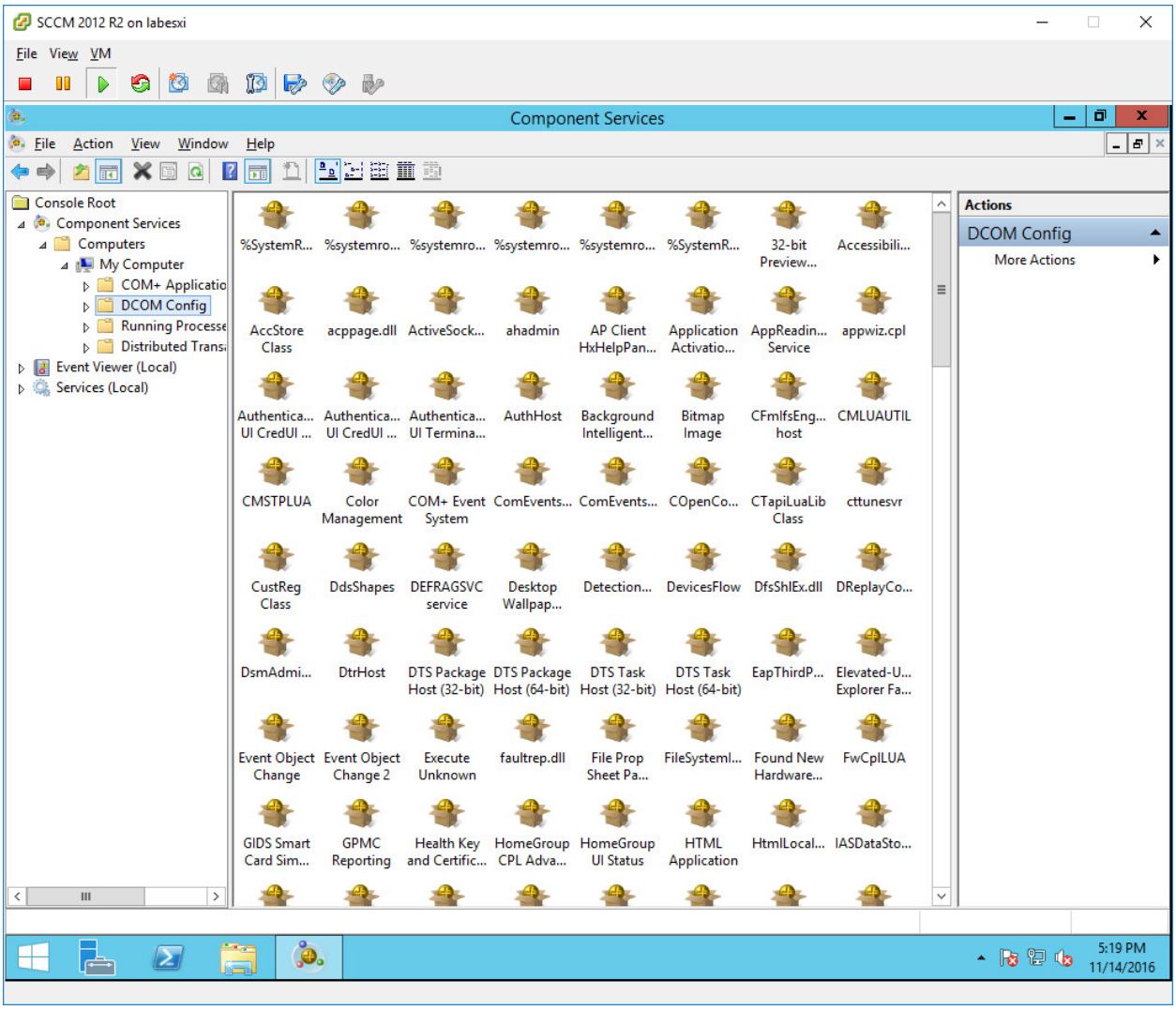
j. You should now see that the new user is a member of the “SMS Admins” local security group.

k. Click “Apply” and “OK” to save the settings and close the dialog box.

Step 3 – Configure the Distributed Component Object Model (DCOM) to allow the new user to access, launch, and activate the objects remotely.

a. On the SCCM Server, open Component Services administrative tool.

b. In the left pane, expand “Component Services” and “My Computer”. You should see something similar to the screenshot below.



c. Expand the “DCOM Config” section and there will be a long list of objects.

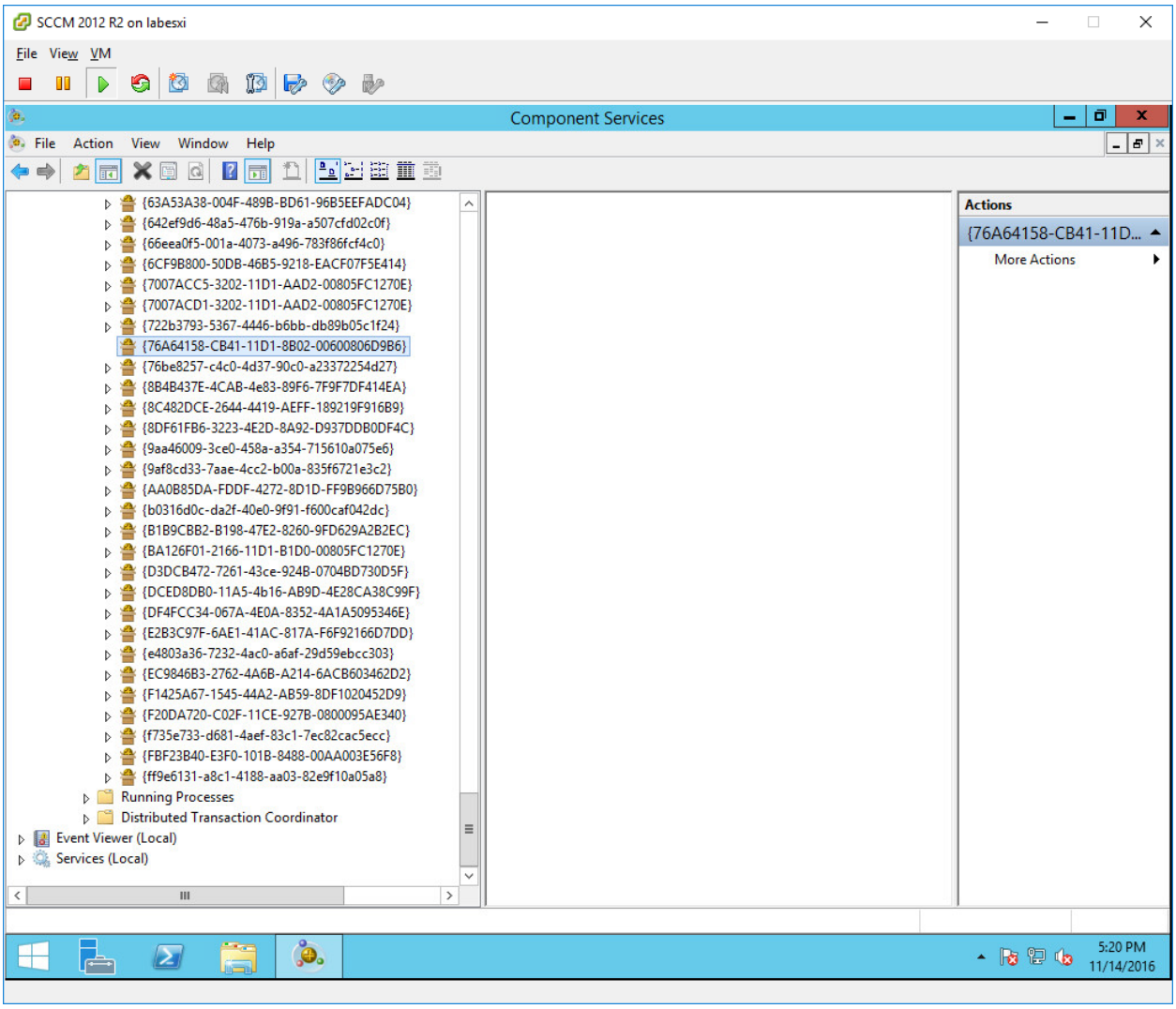
d. You will need to do the following to make the registry keys to appear. These steps need to be done on the SCCM CAS/Primary server in which ISE is trying to connect to.

i. The original owner of the registry keys is TrustedInstaller which will not allow you to make modifications to those keys. You will need to take ownership and grant yourself full control full access you can then modify the keys. These were the registry keys that had to be add/modified in order for the DCOM
to appear.

ii. The information that I used to import into the registry is:
Windows Registry Editor Version 5.00

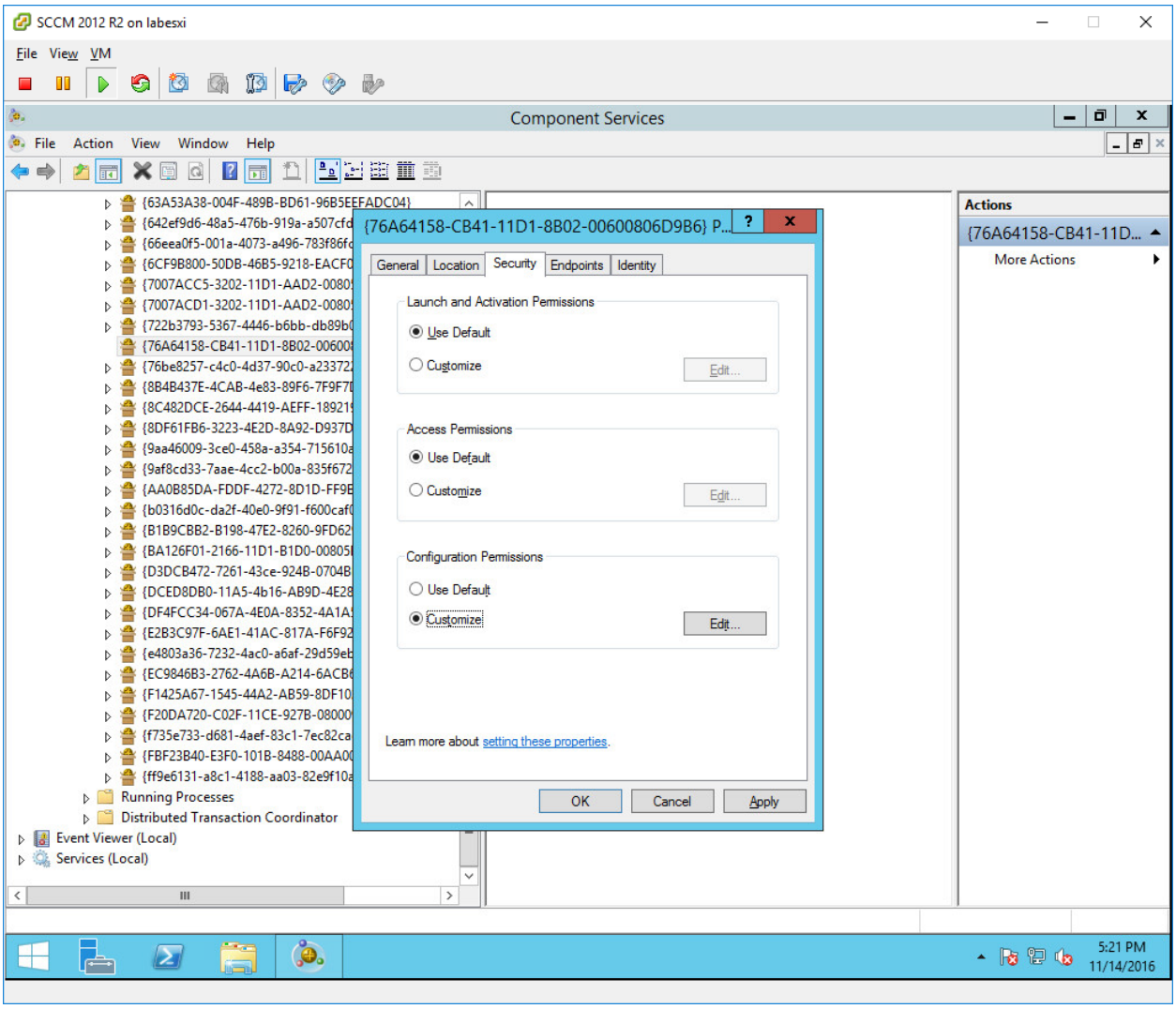
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "

e. Locate the object named “{76A64158-CB41-11D1-8B02-00600806D9B6}” as shown below.



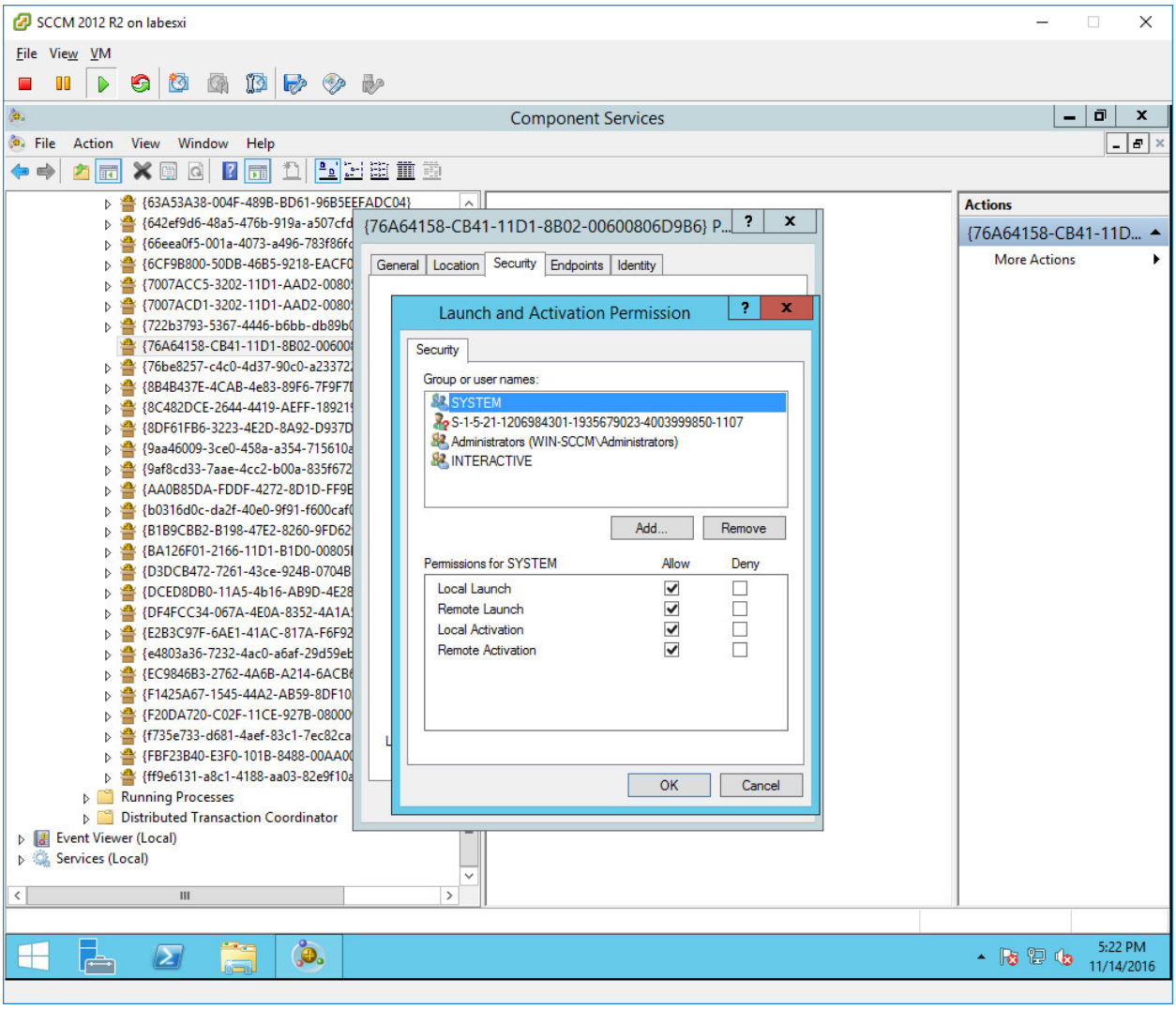
f. Right-click on the object and select “Properties”. A dialog box will open.

g. Select the “Security” tab.



h. In the “Launch and Activation Permissions” section, select the “Customize” radio button.

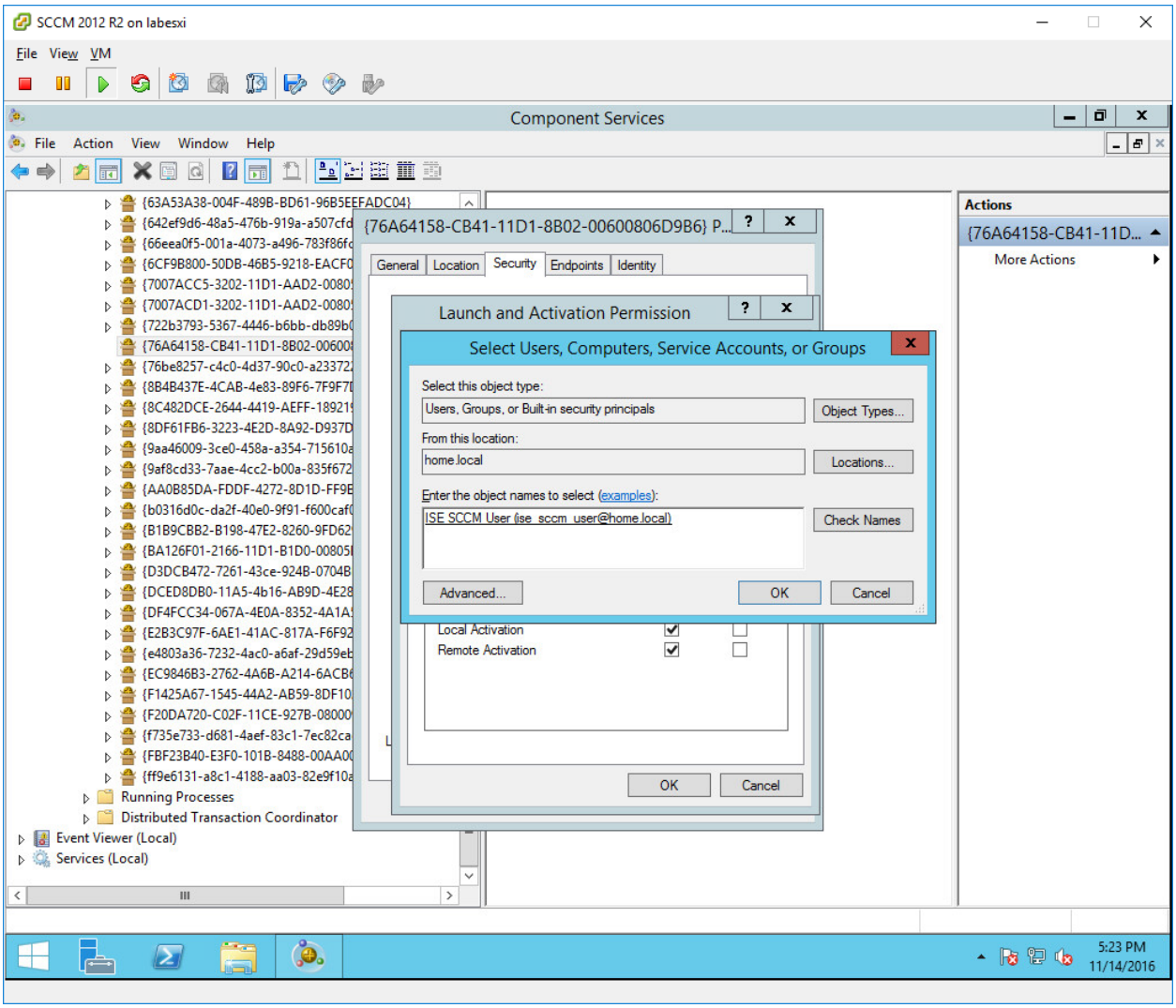
i. Now click on the “Edit…” button in that same section. Another dialog box will open showing the permissions.

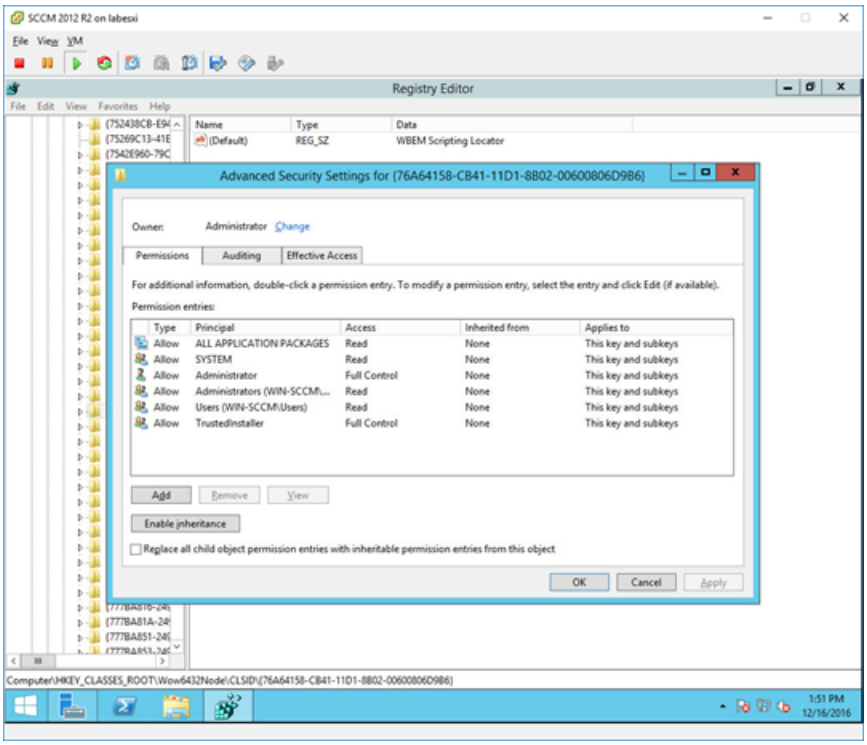


j. Click the “Add…” button to add the new user for ISE.

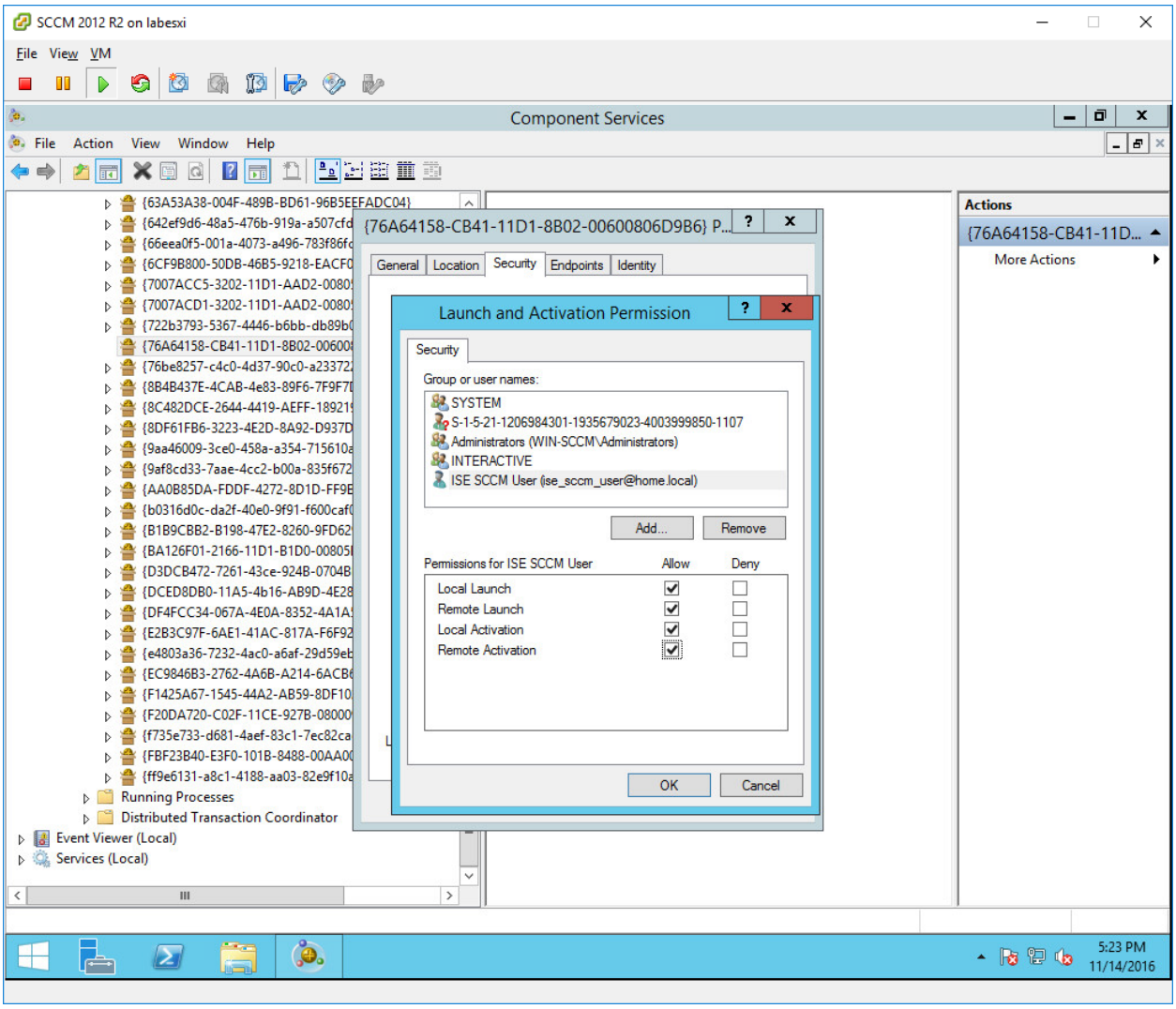
k. In the new dialog box, ensure that the location is set to the AD domain.

l. Enter the new username created in Step 1 and select “Check Names”.


SCCM 2012 R2 on labesxi
File View VM
Component Services
File Action View Window Help
{76A64158-CB41-11D1-8B02-00600806D9B6} P...
General Location Security Endpoints Identity
Launch and Activation Permission
Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
home.local
Locations...
Enter the object names to select (examples):
ISE SCCM User (ise_sccm_user@home.local)
Check Names
Advanced...
OK
Cancel
Local Activation
Remote Activation
OK
Cancel
Actions
{76A64158-CB41-11D...
More Actions
Running Processes
Distributed Transaction Coordinator
Event Viewer (Local)
Services (Local)
5:23 PM
11/14/2016



m. Ensure that the username is found and is now underlined, indicating that the account is valid.
n. Click “OK”.
o. Now select “Allow” for all permissions while the new account is selected. The end result should look similar to the following screenshot.

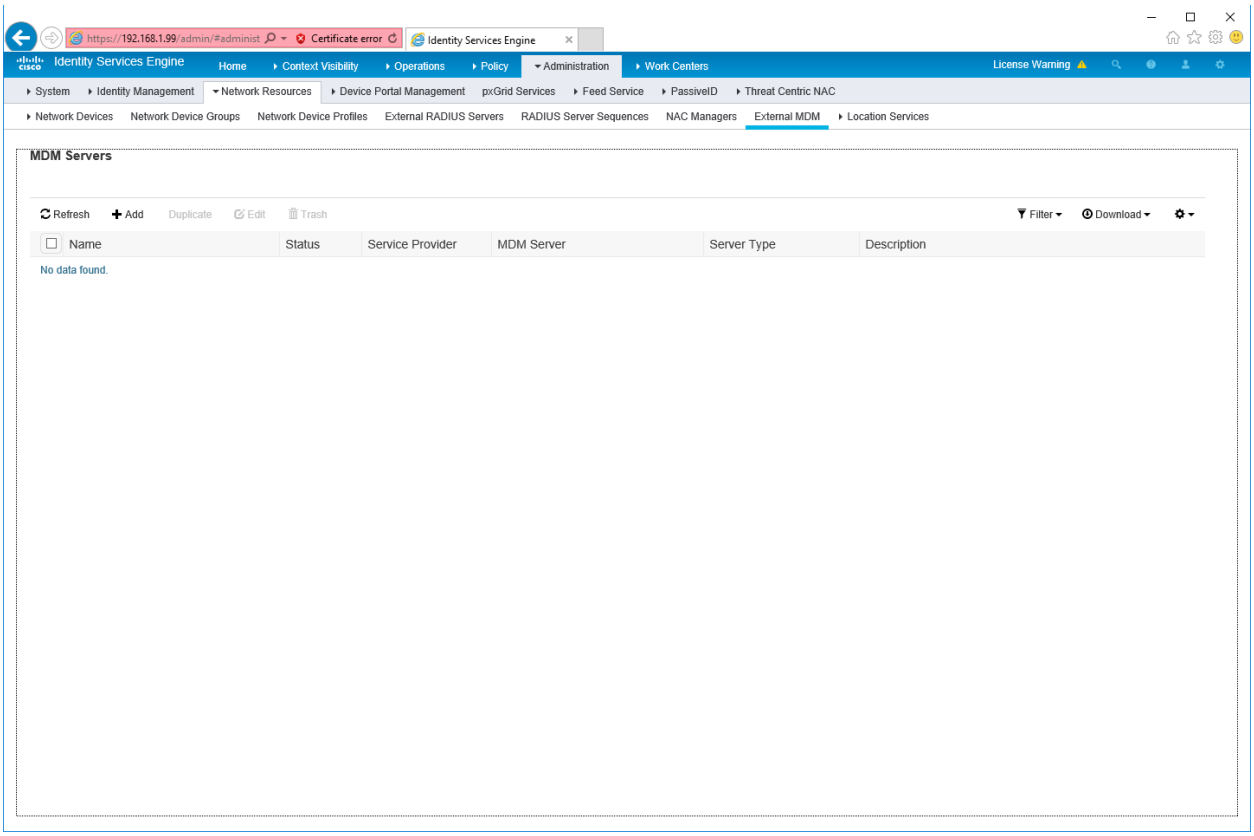


p. Select “OK” on all dialog boxes.

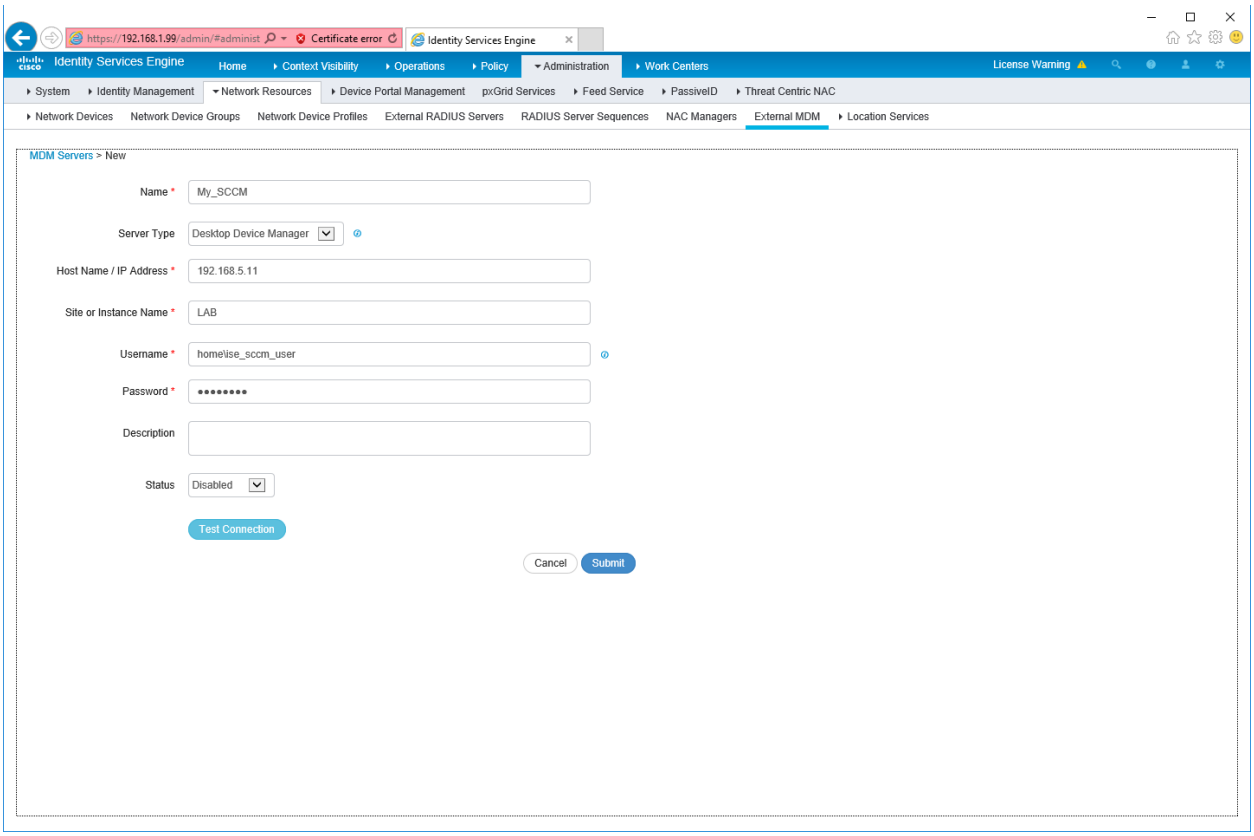
Step 4 – Configure ISE to connect to the SCCM server, test the connection, and add the SCCM server as an available MDM server in the ISE system.

a. Login to the ISE Primary Admin node web interface.

b. Select Administration -> Network Resources -> External MDM.

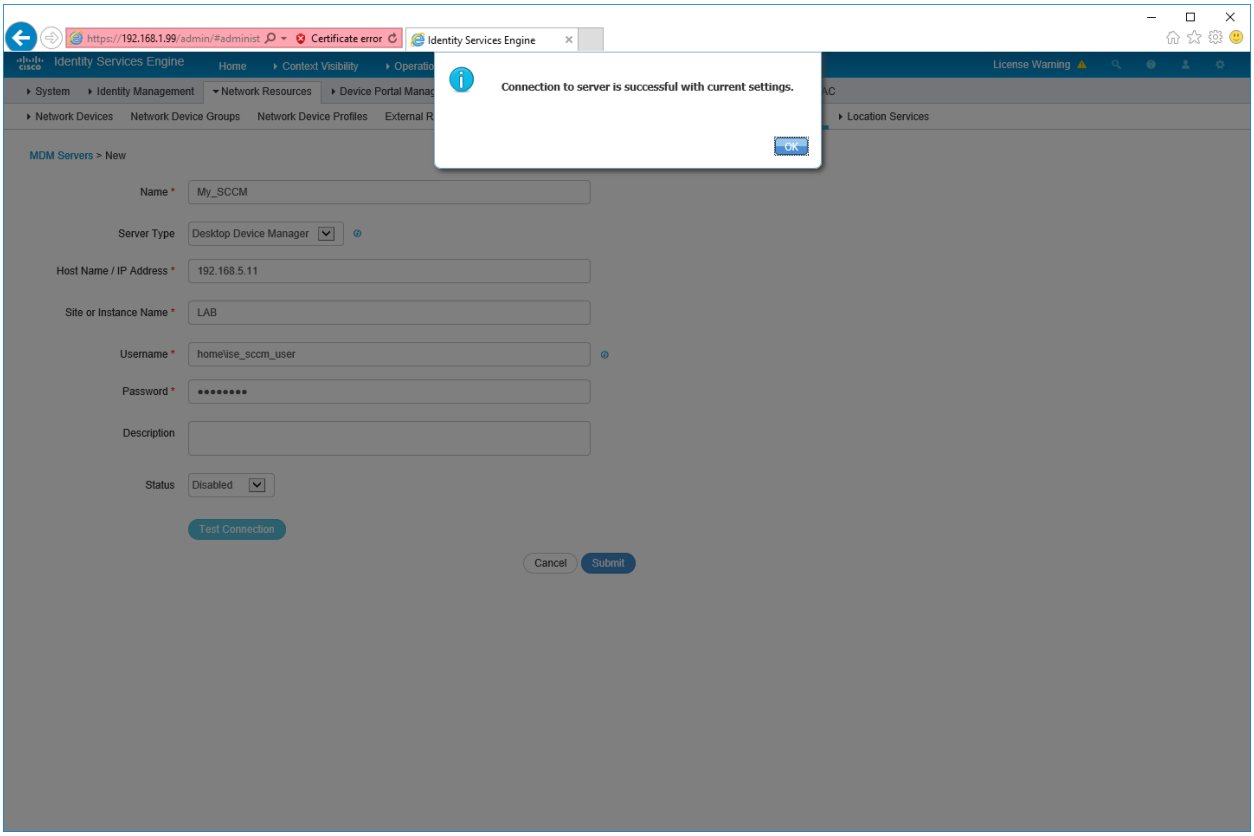


c. Click on the “Add” button to add a new MDM server.

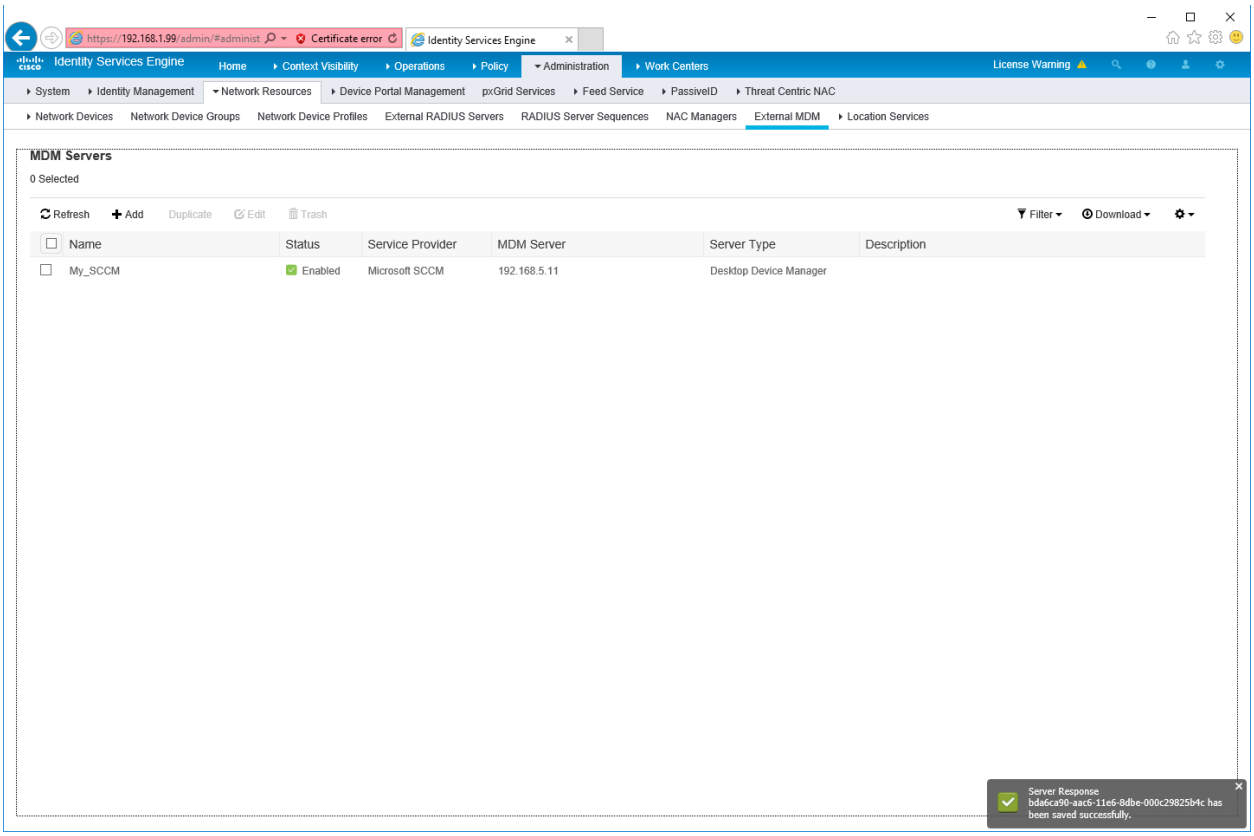


d. The “Name” field can be any name you want to reference the MDM as when creating policies within ISE. The name cannot contain any spaces. In this example, we are using “My_SCCM”.
e. The “Server Type” must be set to “Desktop Device Manager” for SCCM.
f. Enter the Fully Qualified Domain Name (FQDN) of the SCCM server or the IP address that is reachable from the ISE Admin node.
g. For the “Site or Instance Name”, please use the SCCM Site Name.
h. The username will be the user account that was created in Step 1. It is important to preface the username with the domain name. For example, “home\ise_sccm_user” where “home” is the AD domain name.

i. Enter the password for the user account created in Step 1.
j. Select the “Test Connection” button at the bottom to test the connection to the SCCM server. If the connection is successful, you should see a dialog box stating it was successful as shown below.



k. Click the “OK” button on the success dialog.
l. Change the “Status” to “Enabled”.
m. Click “Submit” to add the new SCCM server to ISE as an MDM.


https://192.168.1.99/admin/#administ
Certificate error
Identity Services Engine
Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
License Warning
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
PassiveID
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
MDM Servers
0 Selected
Refresh
Add
Duplicate
Edit
Trash
Filter
Download
Name
Status
Service Provider
MDM Server
Server Type
Description
My_SCCM
Enabled
Microsoft SCCM
192.168.5.11
Desktop Device Manager
Server Response
bda6ca90-aac6-11e6-8dbe-000c29825b4c has been saved successfully.

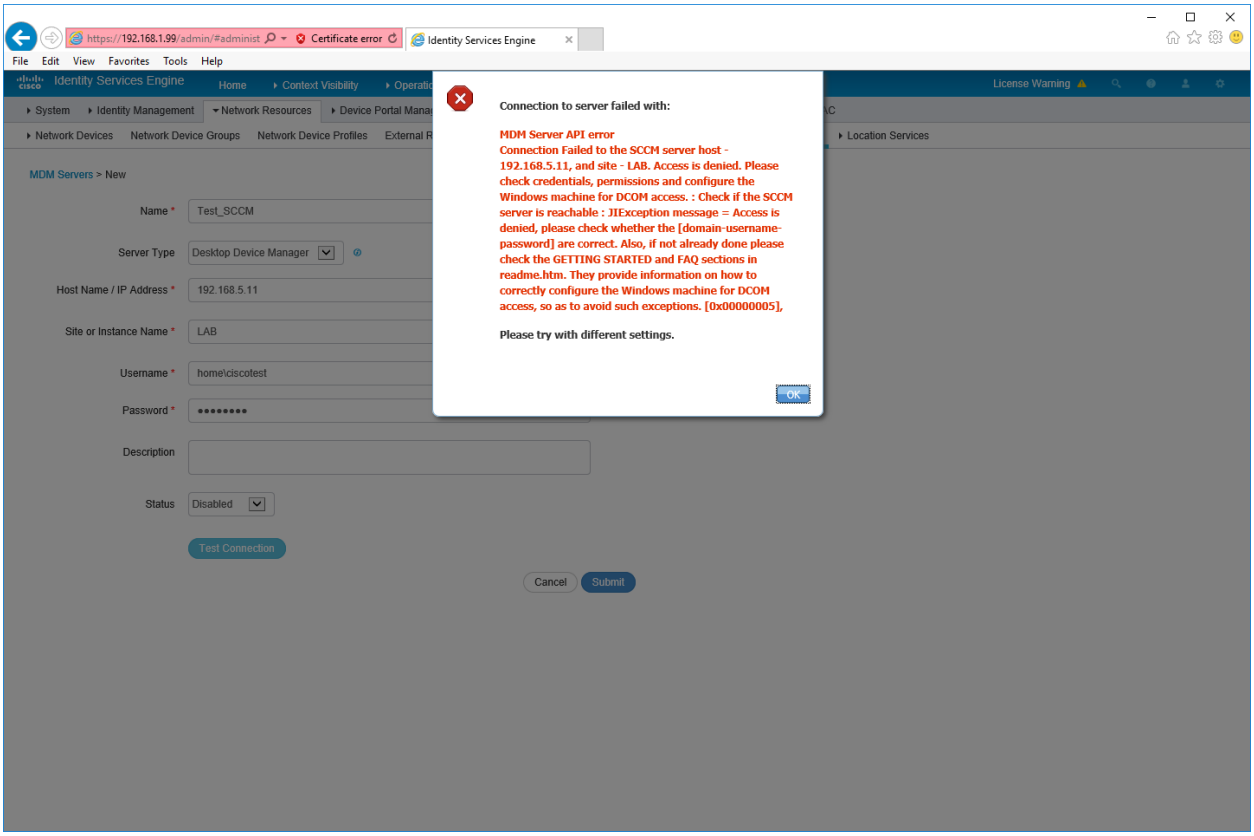
Troubleshooting ISE Integration with SCCM

During the initial configuration of ISE to connect to the SCCM server, you may encounter problems with testing the connection. The connection may fail and various errors will be presented. Unfortunately, the error messages may not be clear enough to isolate the issue.

Considering that there really are only two configurations required on the SCCM server to allow ISE to connect, we can investigate what the errors look like in each of those situations.

Situation 1 – Problem with User Account or Security Group Membership

ISE Error Message:

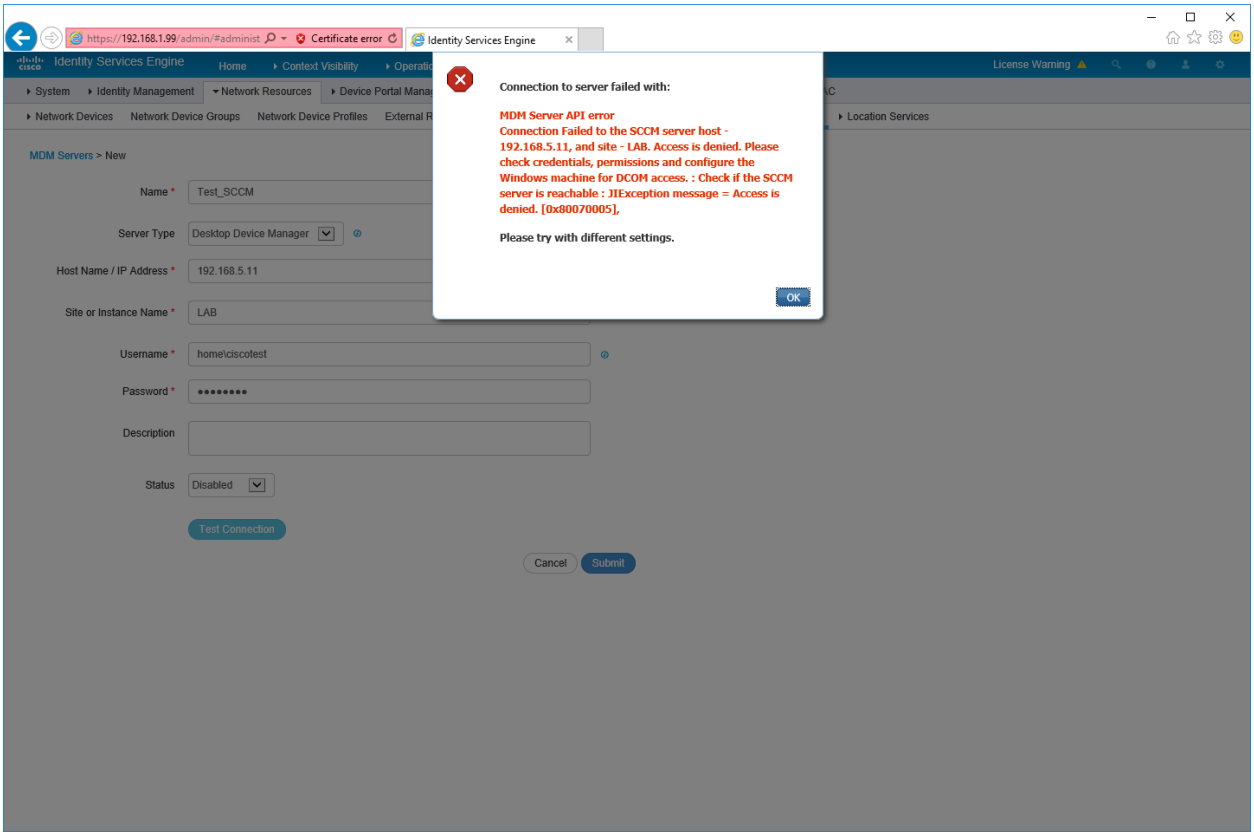


SCCM Server Error Message: None

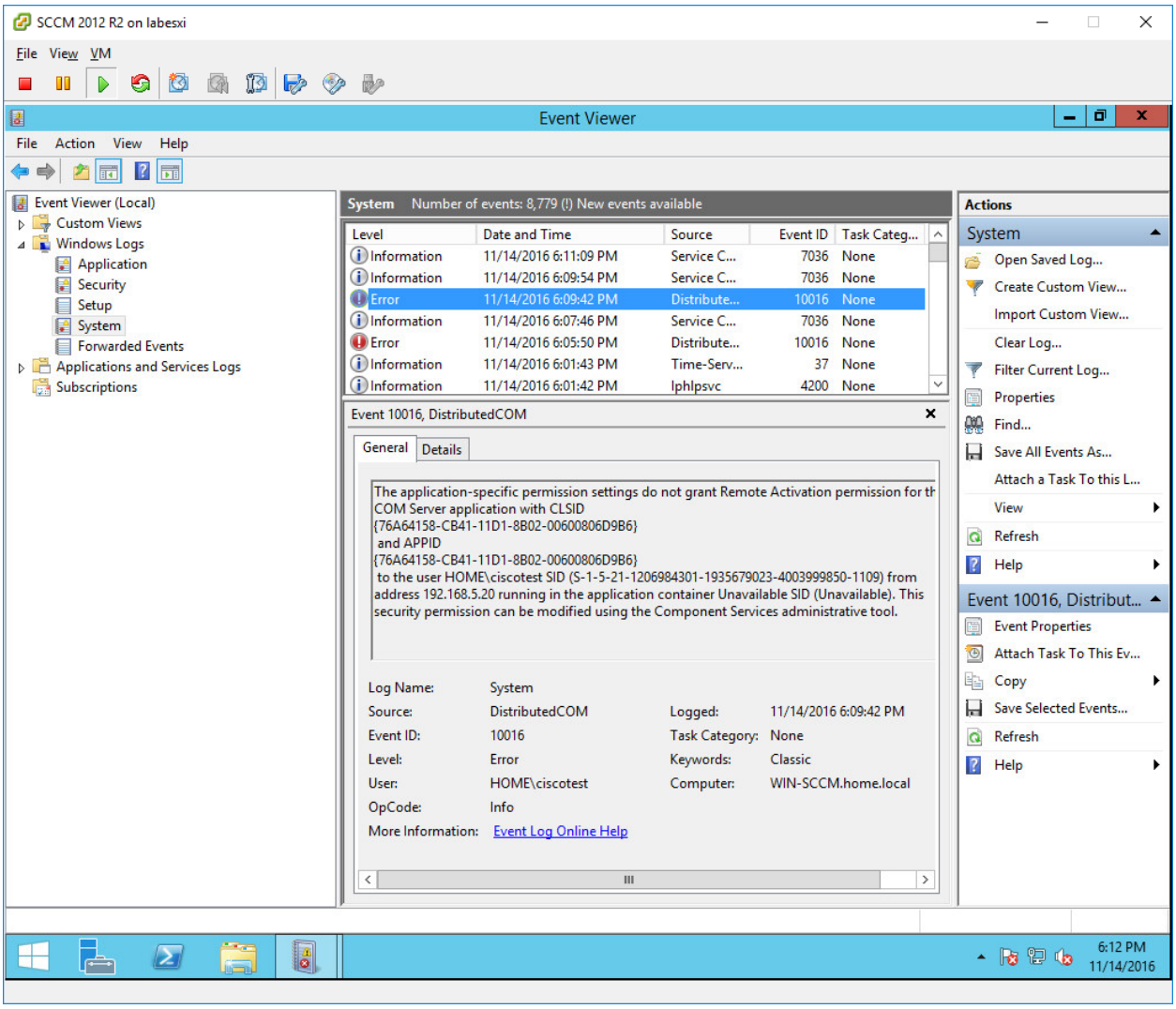
Resolution – Ensure that the account is valid, not locked out, and that the password works. This can be accomplished by attempting to login to the AD domain using the account. If the login works, verify that the user account is a member of the “SMS Admins” local security group on the SCCM Server. Any of these issues will result in the error message shown above.

Situation 2 – Problem with DCOM Permissions

ISE Error Message:



SCCM Server Error Message:



Resolution – Follow the procedures in Step 3 to ensure that the DCOM object has been configured to allow the ISE user account the ability to access, launch, and activate the objects remotely.