

Kerberos Constrained Delegation configuration for Capsule Workspace

Step by Step guide

Kerberos constrained delegation is a Single Sign-on method that uses Kerberos authentication for users to access internal resources without the need to enter a password. It is supported for the Mobile Access portal and Capsule Workspace.

1. Relevant resources

1.1. Mobile Access Blade guide ->

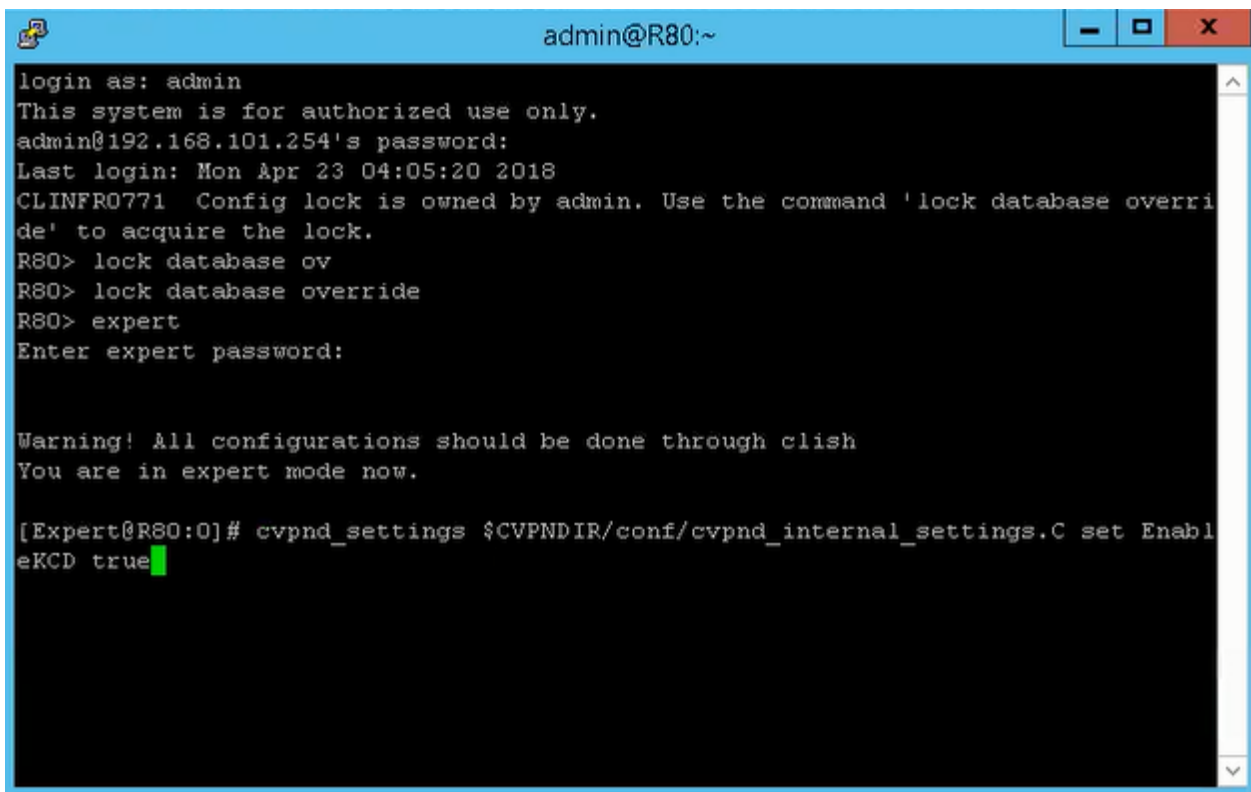
https://sc1.checkpoint.com/documents/R77/CP_R77_Mobile_Access_WebAdmin/84203.htm#o121175

1.2. How to configure EX2016 for Negotiate -> <https://technet.microsoft.com/en-us/library/ff808312%28v=exchg.160%29.aspx?f=255&MSPPErr=2147217396>

2. On the Mobile Access Blade – Enable Kerberos constrained delegation:

2.1. On the Mobile Access gateway, run:

```
cvpnd_settings $CVPNDIR/conf/cvpnd_internal_settings.C set EnableKCD true
```



```
admin@R80:~
login as: admin
This system is for authorized use only.
admin@192.168.101.254's password:
Last login: Mon Apr 23 04:05:20 2018
CLINFRO771 Config lock is owned by admin. Use the command 'lock database override' to acquire the lock.
R80> lock database ov
R80> lock database override
R80> expert
Enter expert password:

Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@R80:0]# cvpnd_settings $CVPNDIR/conf/cvpnd_internal_settings.C set EnableKCD true
```

2.2.Run *cvpnrestart* on the gateway.

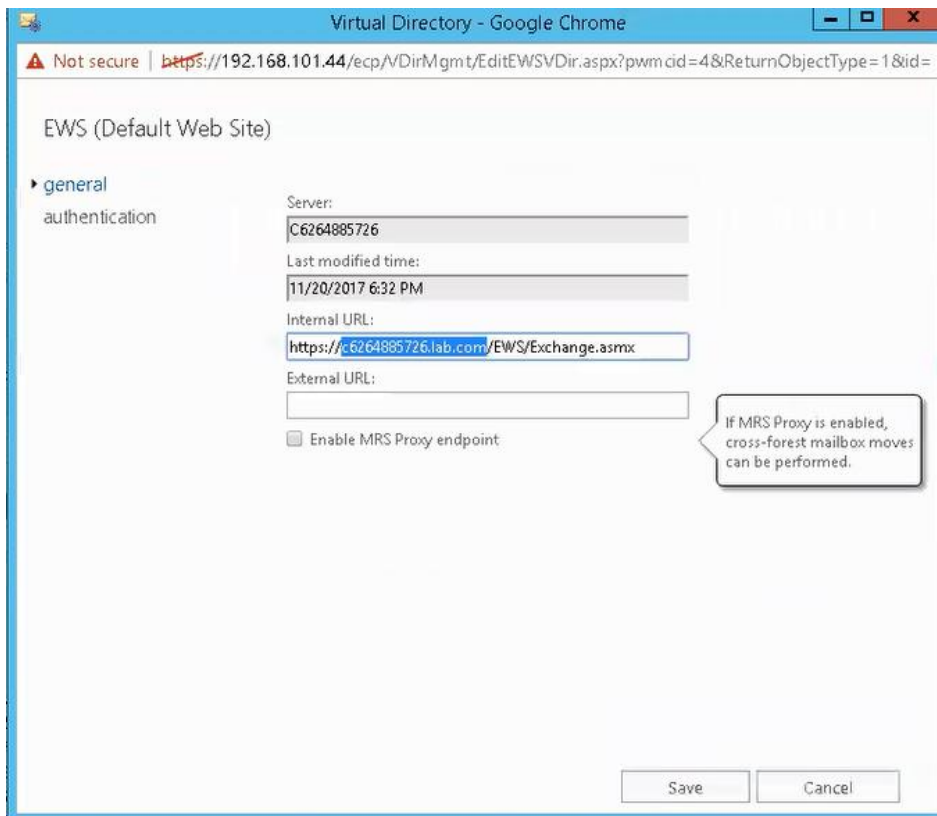
2.3.Validate that the date and time on the gateway and Active Directory server are the same.

2.4.Validate that you use FQDN and not an IP address with your internal server name or Exchange Server. Make sure that the FQDN resolves both on the Security Gateway and on the Kerberos server.

2.4.1. On the MAB -> Putty -> Edit the hosts file on the MAB -> than click i:

```
admin@R80:~  
This file was AUTOMATICALLY GENERATED  
# Generated by /bin/hosts_xlate on Wed Jul 26 20:34:42 2017  
#  
# DO NOT EDIT  
#  
192.168.101.254 R80  
127.0.0.1 localhost  
::1 localhost  
~  
~  
~  
~  
Mobile Access: Starting UserMonitor Service  
Mobile Access: Pinger is already running  
Mobile Access: IdlePinger is already running  
Mobile Access: Starting cvpn service  
Mobile Access: Clearing portal rendering cache in all sessions.  
Mobile Access: Successfully started Mobile Access services.  
[Expert@R80:0]# datetime  
bash: datetime: command not found  
[Expert@R80:0]# date  
Mon Apr 23 04:08:32 PDT 2018  
[Expert@R80:0]# vi /etc/hosts
```

2.4.2. Enter the Web Server \ Exchange address in the file -> This should be the same one that appears in the EWS Server part in the Exchange Server:

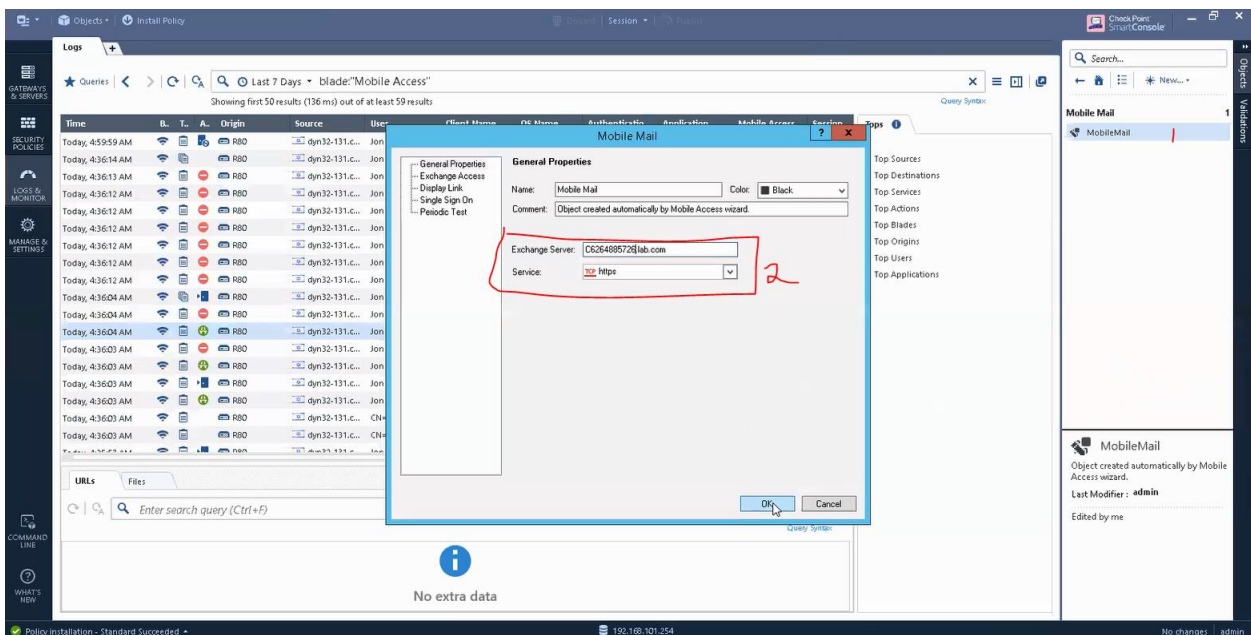


Leads to:

```
admin@R80:~  
# This file was AUTOMATICALLY GENERATED  
# Generated by /bin/hosts_xlate on Wed Jul 26 20:34:42 2017  
#  
# DO NOT EDIT  
#  
192.168.101.254 R80  
127.0.0.1 localhost  
::1 localhost  
192.168.101.44 C6264885726lab.com  
  
-- INSERT --
```

2.4.3. i -> esc -> shift ; -> ;wq

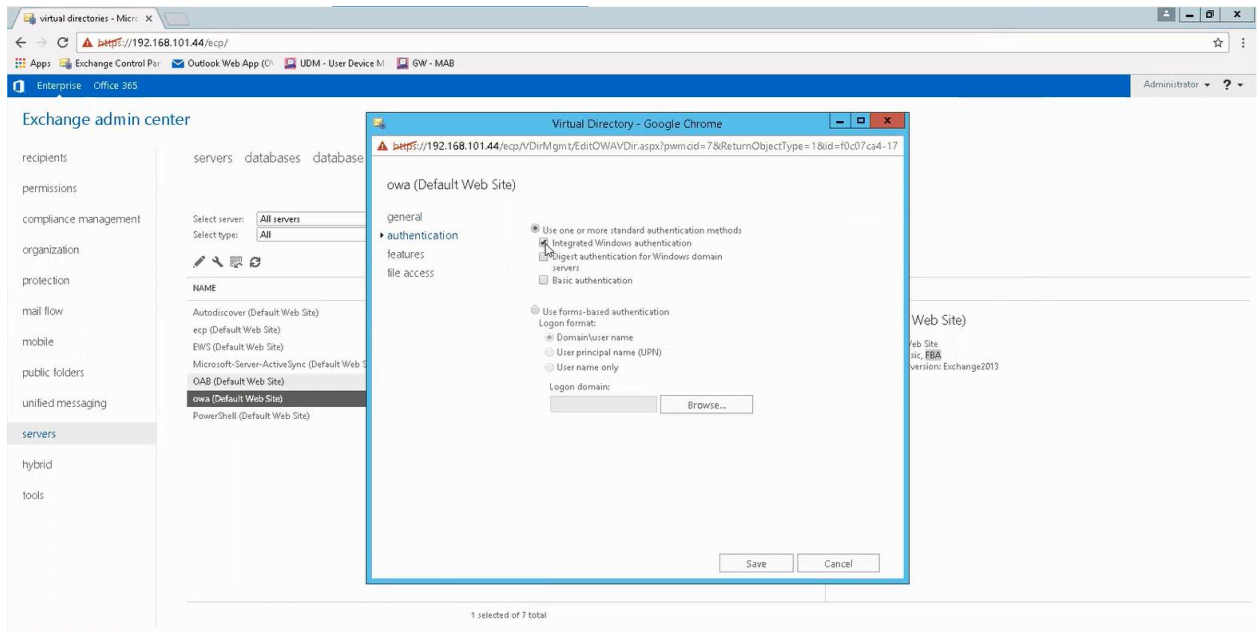
2.4.4. On Smart Dashboard -> Change the Mobile Mail Exchange Server address:



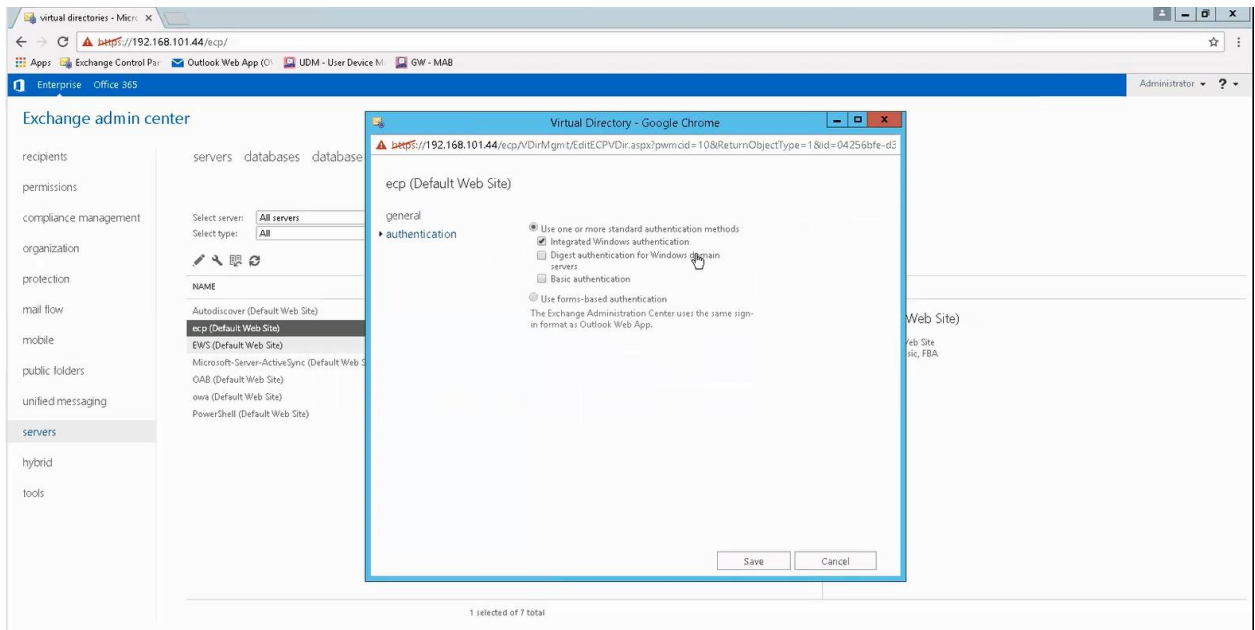
2.5. In a cluster environment, repeat the steps on all cluster members.

3. On the Exchange Machine – validate that the exchange supports Kerberos authentication

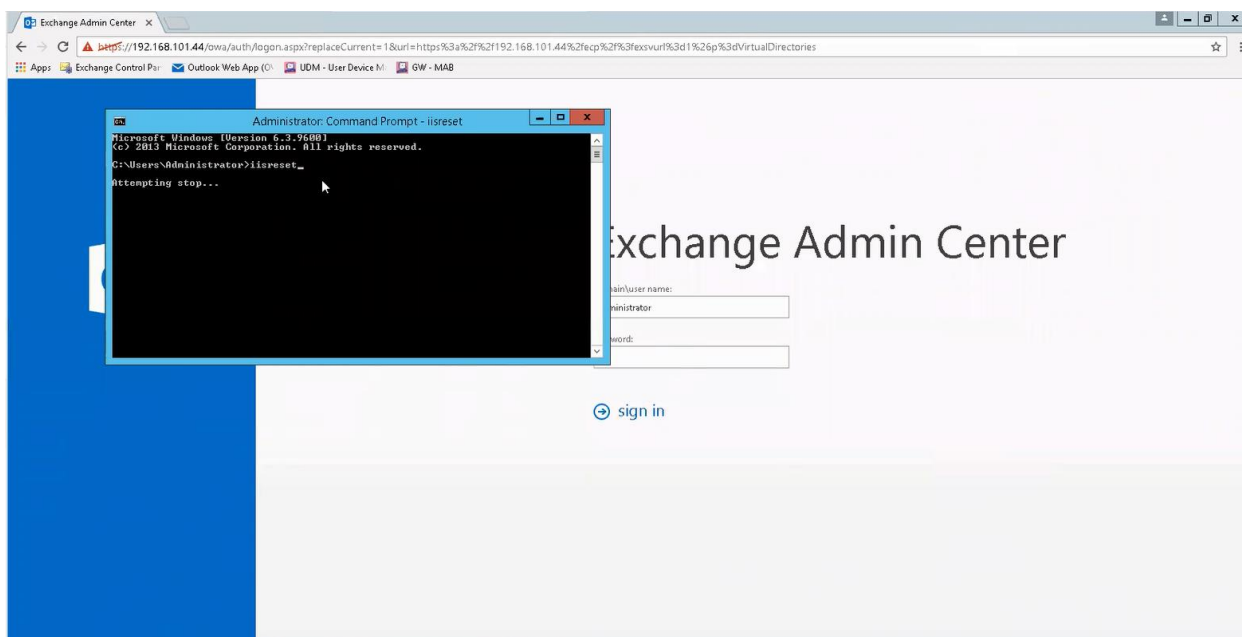
3.1. Go to the Exchange ECP -> Servers -> OWA -> Authentication -> pick integrated Windows authentication:



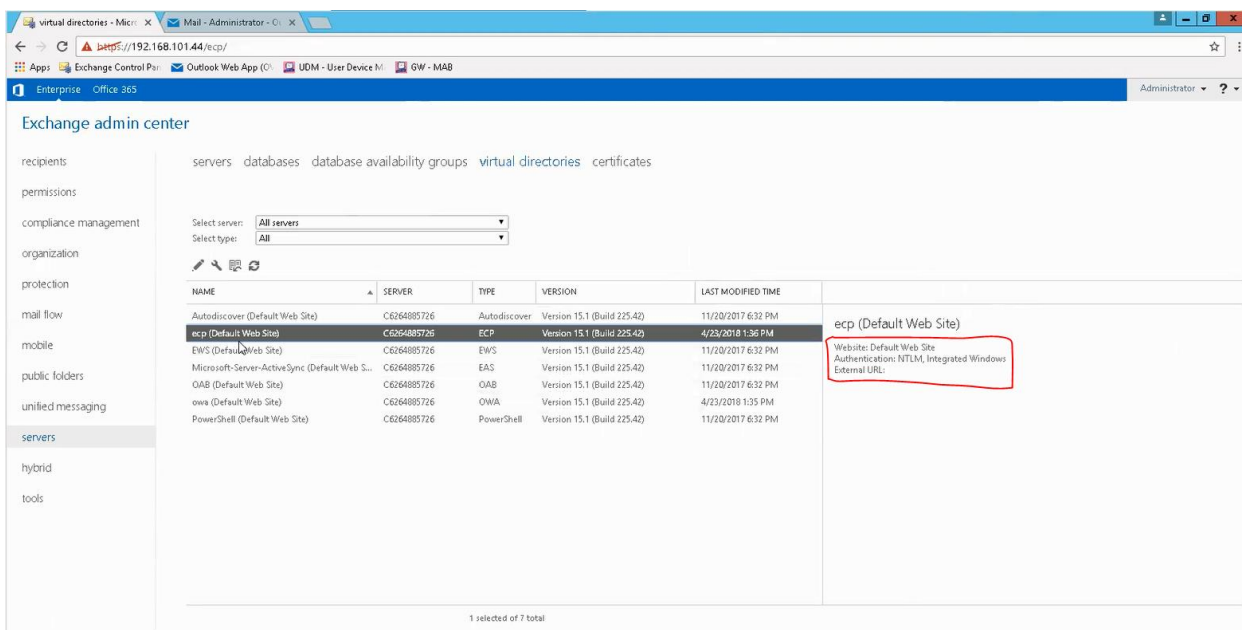
3.2. Go to the Exchange ECP -> Servers -> ecp -> Authentication -> pick integrated Windows authentication:



3.3. On the Exchange Server -> Reset the IIS service -> iisreset



3.4. On the Exchange Server -> Validate that ecp and owa has the same authentication method:



3.5. On the Exchange Server (e.g. C6264885726) -> Enter the Exchange Shell -> enter the following command: **Get-MapiVirtualDirectory -Server C6264885726 | Set-MapiVirtualDirectory -IISAuthenticationMethods Ntlm, Negotiate**

```
Machine: C6264885726.lab.com

[PS] C:\Windows\system32>Get-OVAVirtualDirectory -Server C6264885726
Name                               Server                               OvaVersion
owa (Default Web Site)             C6264885726                         Exchange2013

[PS] C:\Windows\system32>Set-OVAVirtualDirectory -IISAuthenticationMethods Ntlm, Negotiate
A parameter cannot be found that matches parameter name 'IISAuthenticationMethods'.
+ CategoryInfo          : InvalidArgument: (:) [Set-OvaVirtualDirectory], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Set-OvaVirtualDirectory
+ PSComputerName        : c6264885726.lab.com

[PS] C:\Windows\system32>Get-OVAVirtualDirectory -Server C6264885726 ; Set-OVAVirtualDirectory Ntlm, Negotiate
Cannot process argument transformation on parameter 'Identity'. Cannot convert the "System.Collections.ArrayList"
value of type "System.Collections.ArrayList" to type
"Microsoft.Exchange.Configuration.Tasks.VirtualDirectoryIdParameter".
+ CategoryInfo          : InvalidData: (:) [Set-OvaVirtualDirectory], ParameterBindin...ationException
+ FullyQualifiedErrorId : ParameterArgumentTransformationError,Set-OvaVirtualDirectory
+ PSComputerName        : c6264885726.lab.com

[PS] C:\Windows\system32>Get-MapiVirtualDirectory -Server C6264885726 ; Set-MapiVirtualDirectory -IISAuthenticationMetho
ds Ntlm, Negotiate
[PS] C:\Windows\system32>
```

4. **Configuring Kerberos Constrained Delegation**

A delegate user can have specified permissions without being part of a higher privileged group. For Kerberos Constrained Delegation, the delegate user can allow access to other users for specified services.

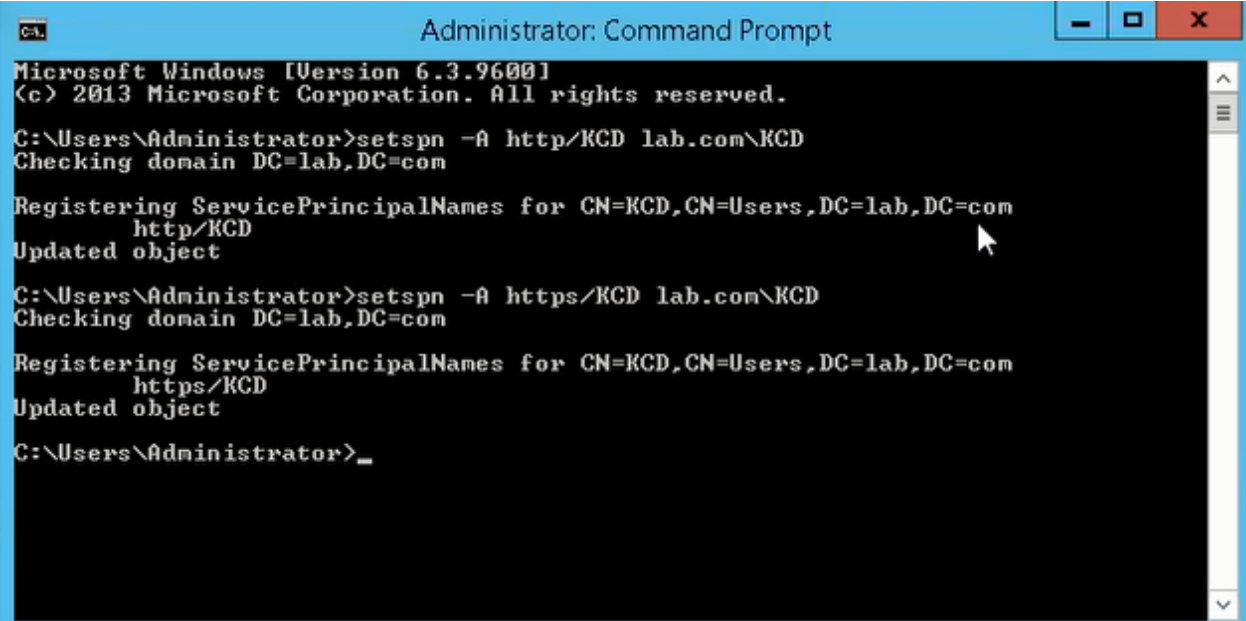
4.1. **Configuring a Delegate User on the AD Server.**

4.1.1. Create Admin user on the AD

4.1.2. On the AD Machine -> Run the following commands on this user:

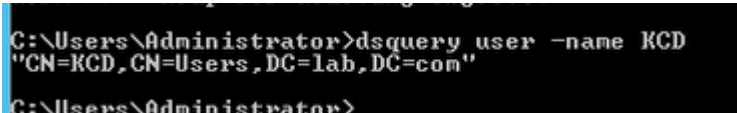
4.1.2.1. `setspn -A http/username domain_name\username` (e.g. `setspn -A http/kcd lab.com\kcd`)

4.1.2.2. `setspn -A https/username domain_name\username` (e.g. `setspn -A https/kcd lab.com\kcd`)



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -A http/KCD lab.com\KCD
Checking domain DC=lab,DC=com
Registering ServicePrincipalNames for CN=KCD,CN=Users,DC=lab,DC=com
http/KCD
Updated object
C:\Users\Administrator>setspn -A https/KCD lab.com\KCD
Checking domain DC=lab,DC=com
Registering ServicePrincipalNames for CN=KCD,CN=Users,DC=lab,DC=com
https/KCD
Updated object
C:\Users\Administrator>_
```

4.1.3. On the AD Machine -> Validate the user's details -> run the following command: `dsquery user -name username`

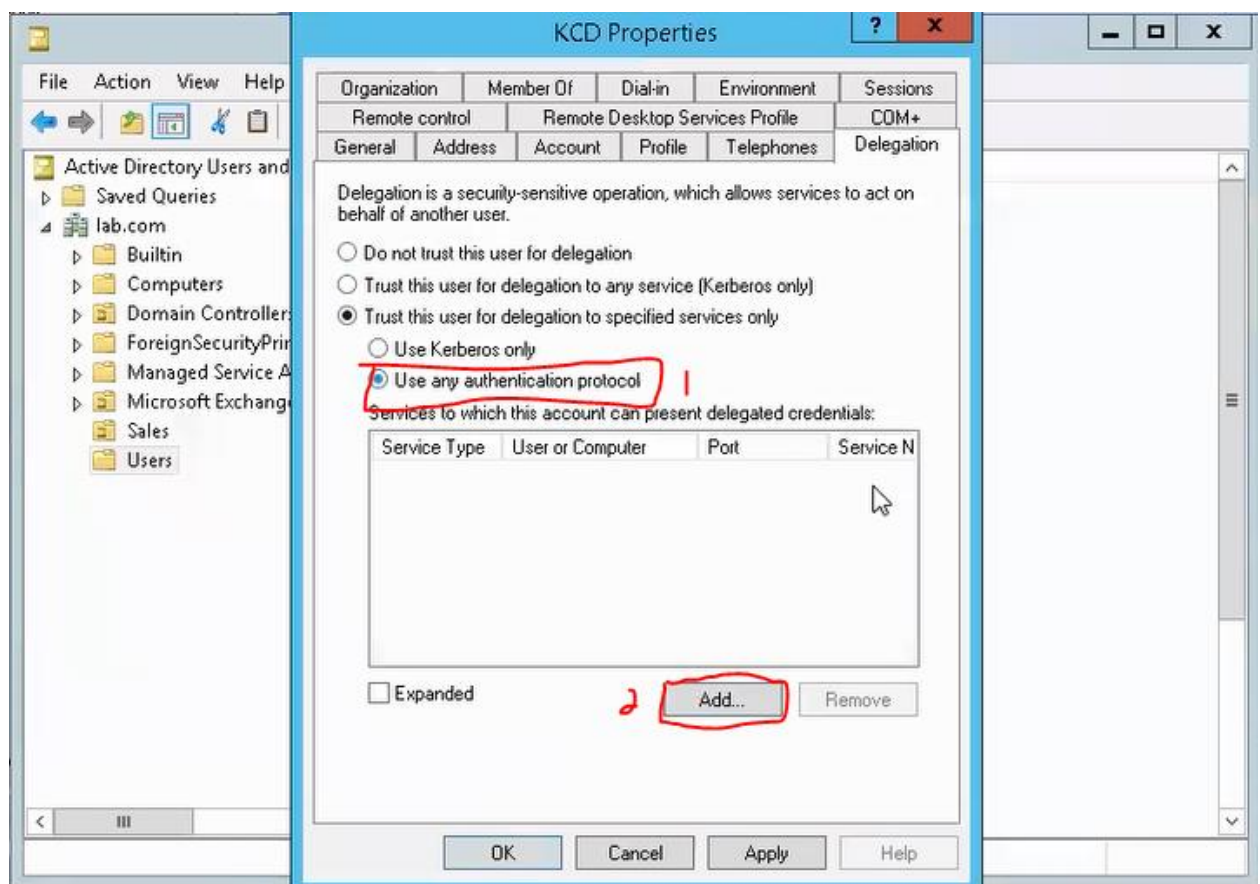


```
C:\Users\Administrator>dsquery user -name KCD
"CN=KCD,CN=Users,DC=lab,DC=com"
C:\Users\Administrator>
```

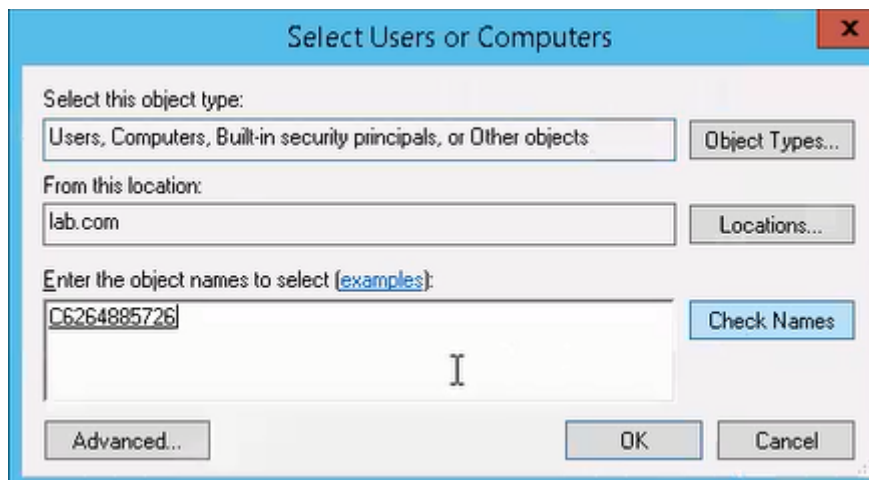
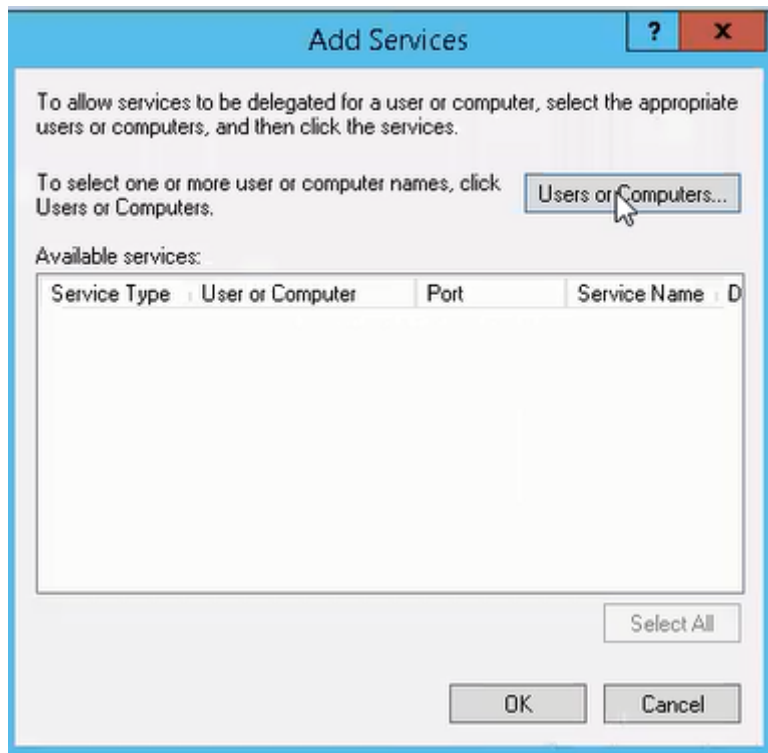

4.1.4. From the Users and Computers tree, right-click the user to open the User Properties of the new user.

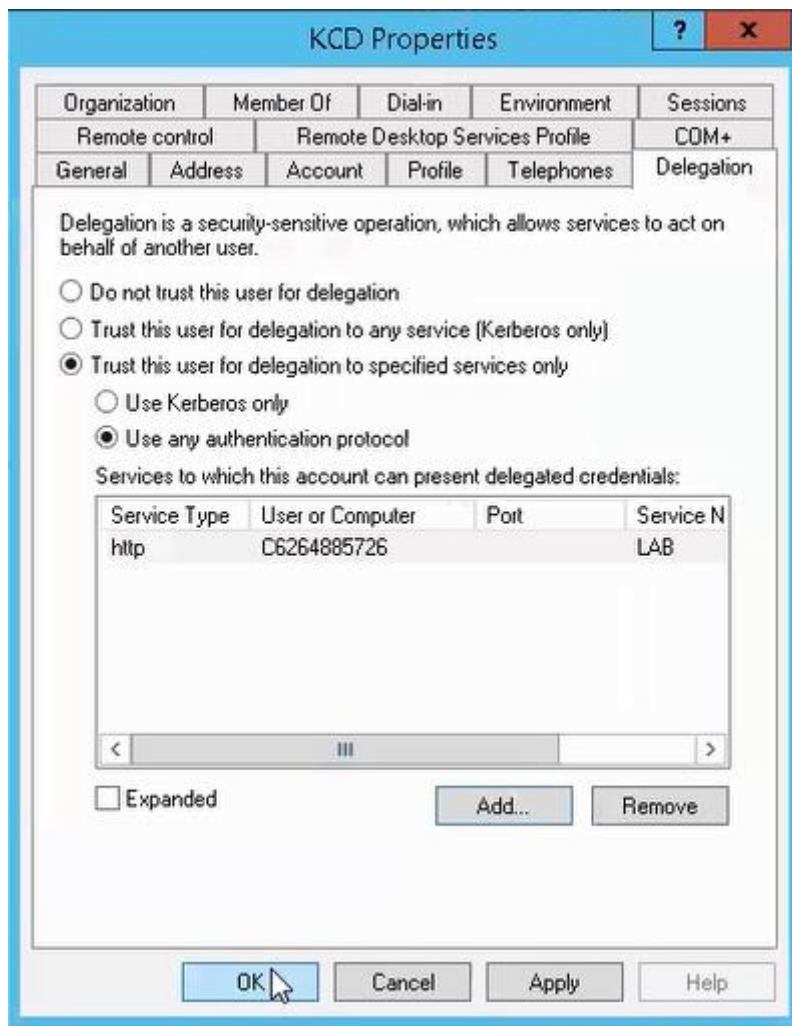
4.1.5. Click the Delegation tab.

4.1.6. In the Services to which this account can present delegated credentials table, click Add to add http on the server that the user is allowed to access -> Click on Trust this user for delegation to specified services only -> Use any authentication protocol -> Click Add:




4.1.7. Pick the relevant users:

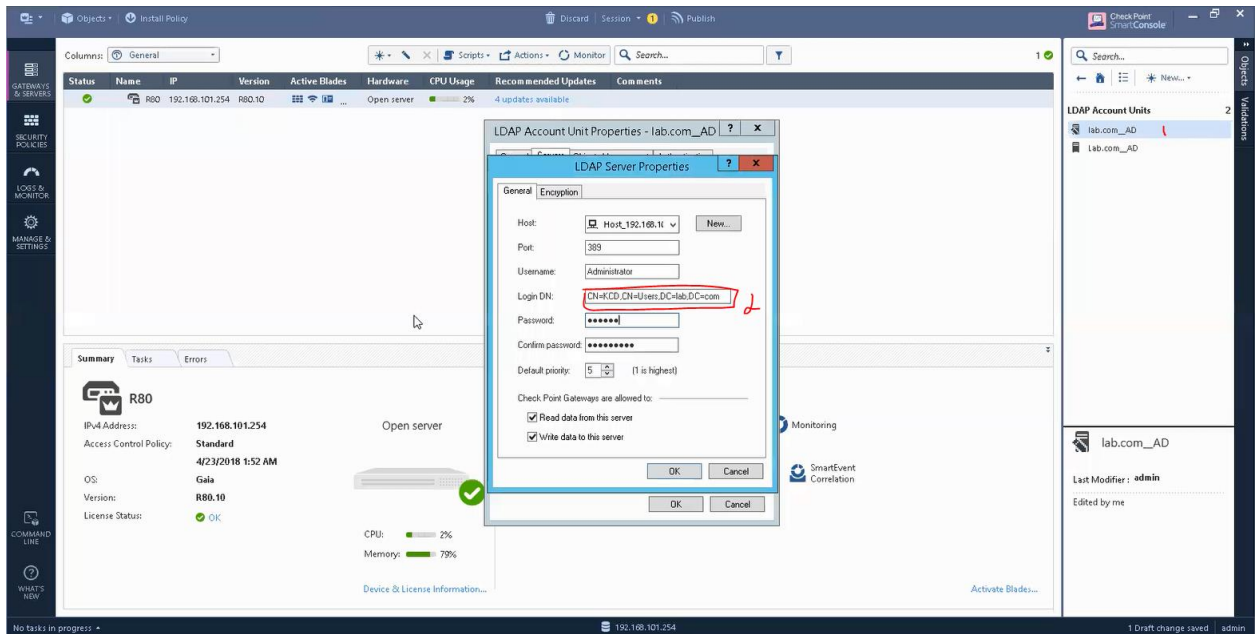




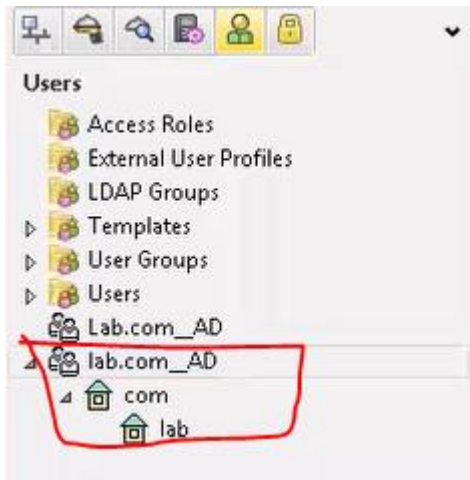
4.1.8. Click OK.

4.2.  Configuring Kerberos Constrained Delegation support on the Mobile Access gateway.

4.2.1. On the MAB Machine -> Pick the relevant LDAP Account Unit -> Change the delegator to be the LDAP Admin:



4.2.2. Validate that you can query the LDAP Account Unit on the old UI:



192.168.101.254 - Check Point SmartDashboard R80.10 - Mobile Access

SmartDashboard

Policy

No.	Users	Applications	Install On	Comment
1	George Jon	<ul style="list-style-type: none"> Google_Browsing Mobile_Mail OWA World_Clock ShareFilesDw youtube_web_app 	R80	

Objects List Identity Awareness

Users

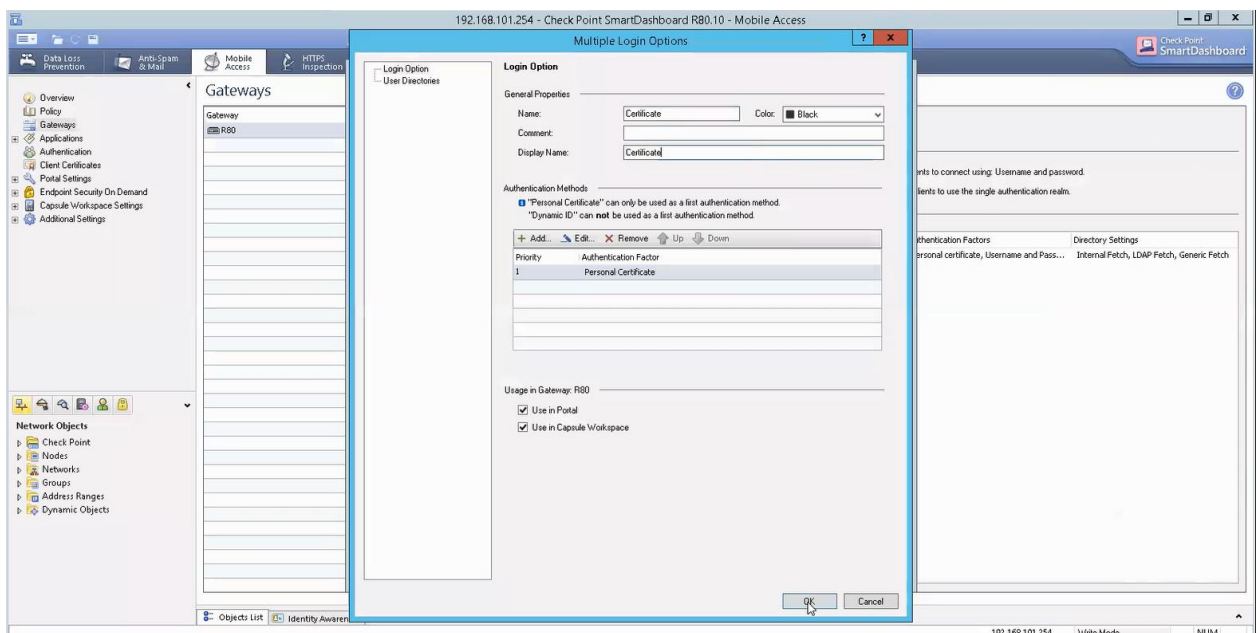
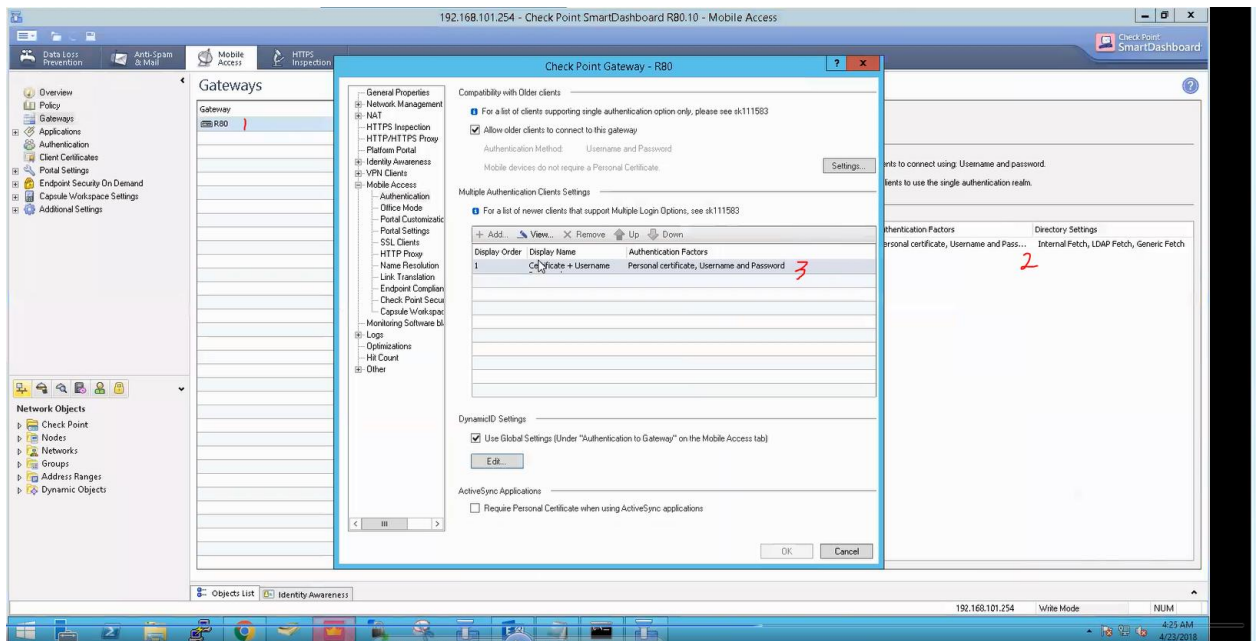
Full Name	Login Name	DN (Distinguished Name)
Protected Users		CN=Protected Users,CN=Users,DC=lab,DC=com
OnsAdmins		CN=OnsAdmins,CN=Users,DC=lab,DC=com
DnsIpdatsProxy		CN=DnsIpdatsProxy,CN=Users,DC=lab,DC=com
Exchange Online - App...	\$731000-08ADA0CME1152	CN=Exchange Online - ApplicationAccount,CN=Users,DC=lab,DC=com
SystemMailbox{f05a...	SM_71c268a51574aecb	CN=SystemMailbox{f05a927-177a-46c9-8e2b-865ef4d0ff41},CN=Users,DC=lab,DC=com
KCD	KCD	CN=KCD,CN=Users,DC=lab,DC=com
SystemMailbox{bb558...	SM_c5a7f927a1f44ddb	CN=SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc9281},CN=Users,DC=lab,DC=com
SystemMailbox{e0dc1...	SM_b7b462a35fe34b379	CN=SystemMailbox{e0dc1c29-89c3-4034-b679-e6c294823e4d9},CN=Users,DC=lab,DC=com
DiscoverySearchMailb...	SM_711f6b9639fa0a78	CN=DiscoverySearchMailbox{D919BA05-46A6-415F-80AD-7E0934B8852},CN=Users,DC=lab,DC=com
Migration_8f2e7716-Z...	SM_c0a6869401b4c36a	CN=Migration_8f2e7716-2011-43a4-96b1-3b4624229136,CN=Users,DC=lab,DC=com
FederatedEmailAc194...	SM_062011b-e413147b0a	CN=FederatedEmailAc194488b-6179-4148-936f-02b859f1c042,CN=Users,DC=lab,DC=com
SystemMailbox{8cc37...	SM_53c2379af7344341b	CN=SystemMailbox{8cc370d3-822a-4ab8-a926-bb94d0641a9},CN=Users,DC=lab,DC=com

Total 31 items in list

192.168.101.254 | Wake Mode | NUM

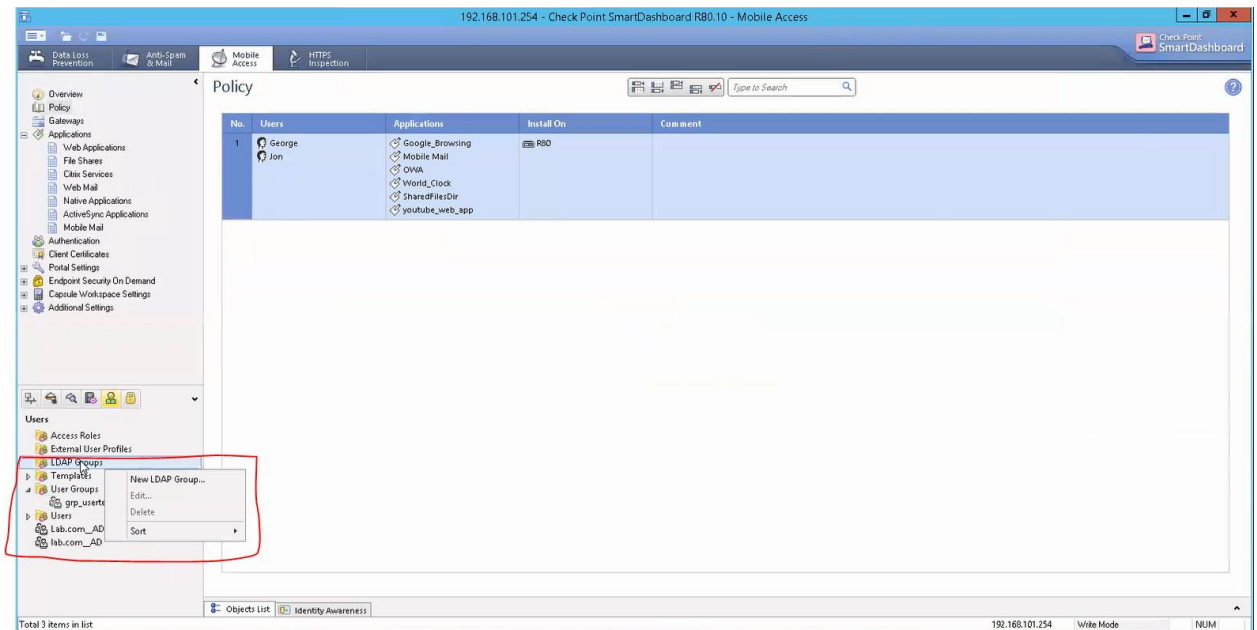
5. Configuring Certificate based authentication

5.1. On the MAB -> Go to Mobile Access Tab -> Click on the R80 Server -> Gateways -> Multiple Login Options for Clients -> Change authentication method to personal certificate

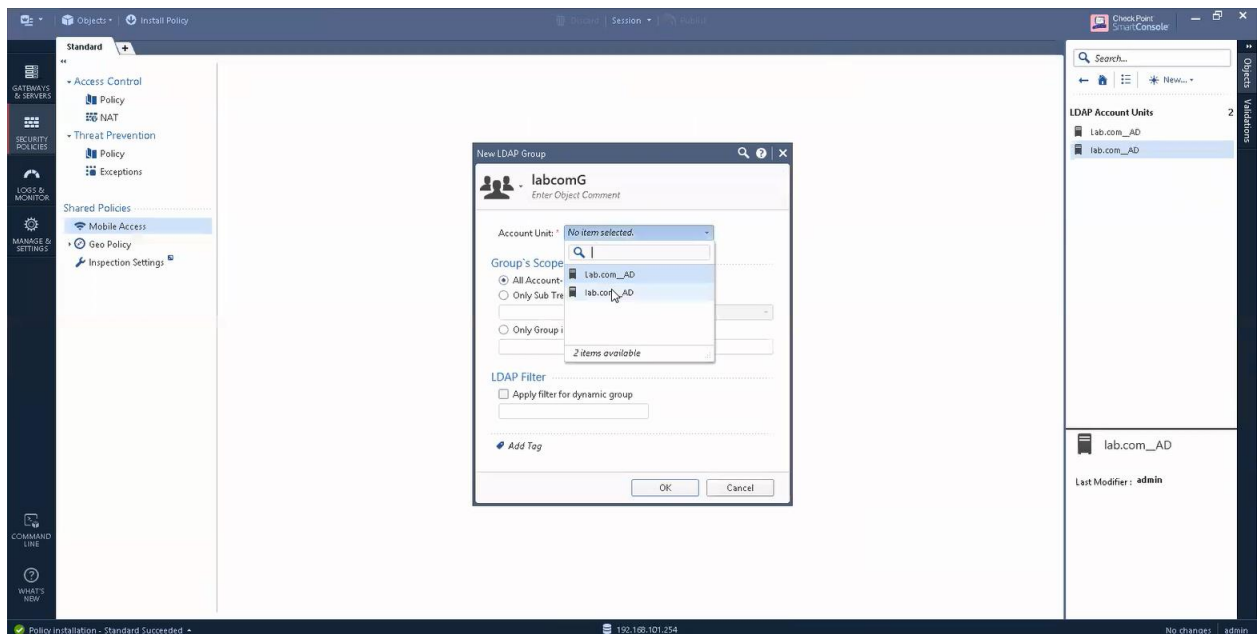


5.2. Install Policy

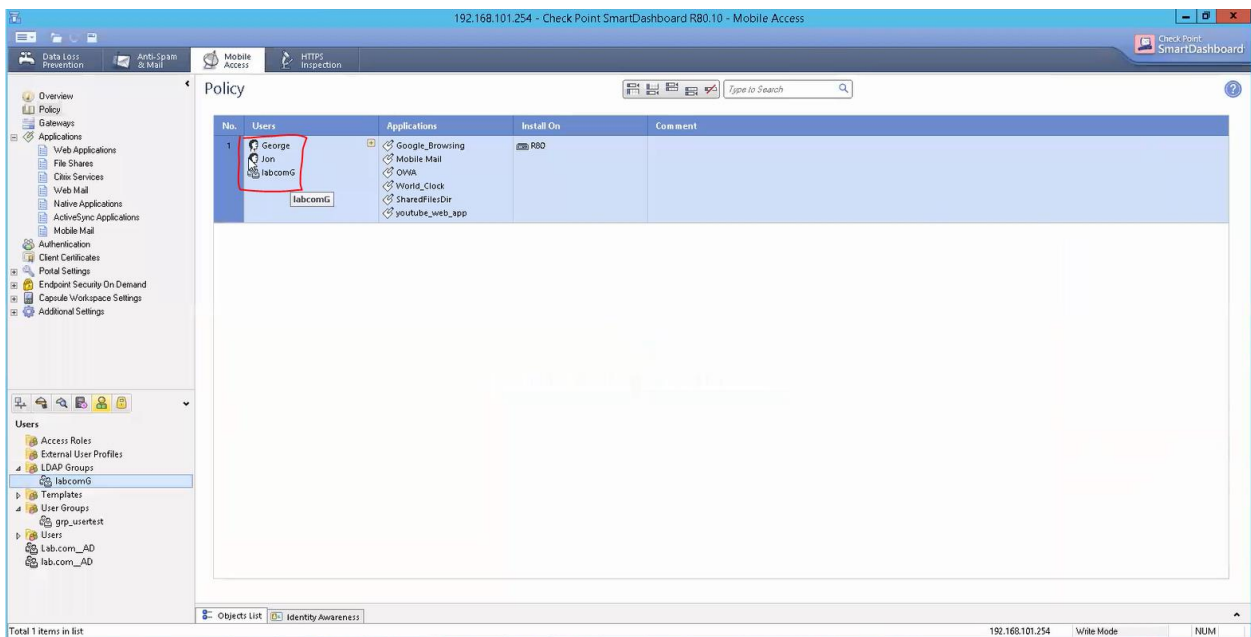
5.3. Create LDAP Group -> New LDAP Group:



5.4. Enter Details:



5.5. Allow group's users to access the Corporate Mail:



5.6. Install Policy

5.7. Create Certificate for the user -> Try to connect

5.8. On the Mobile Access Blade Server -> Putty -> go to tmp/krbcc/ -> ls -> See what tickets are being created:

