

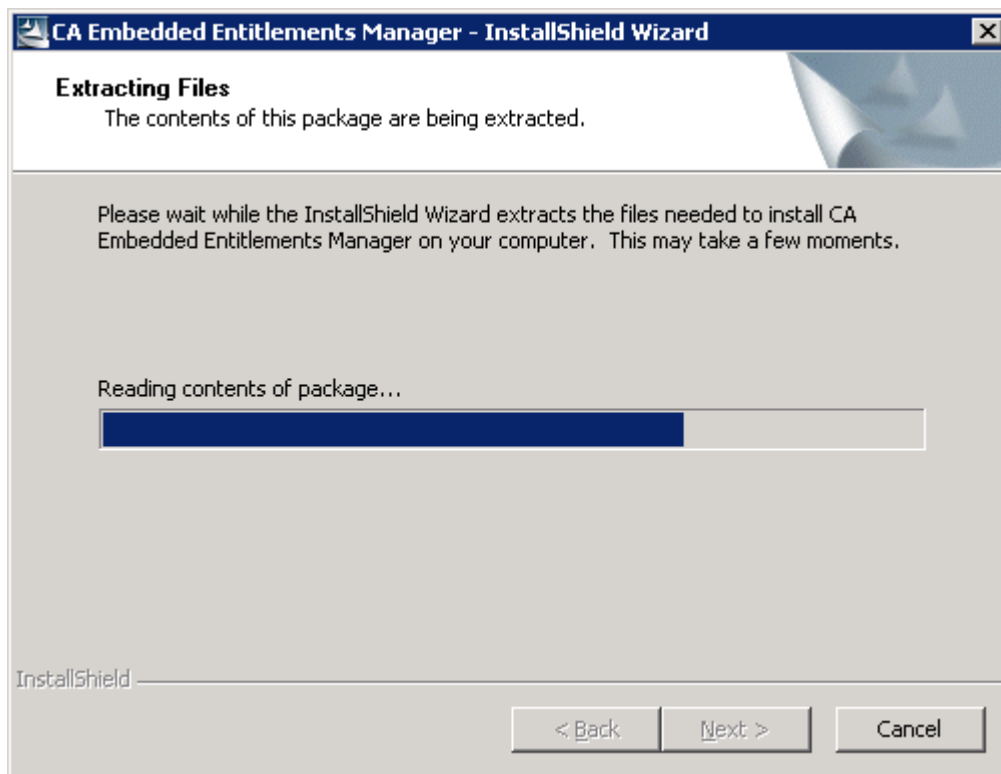
How to configure APM authentication with EEM configured with LDAP?

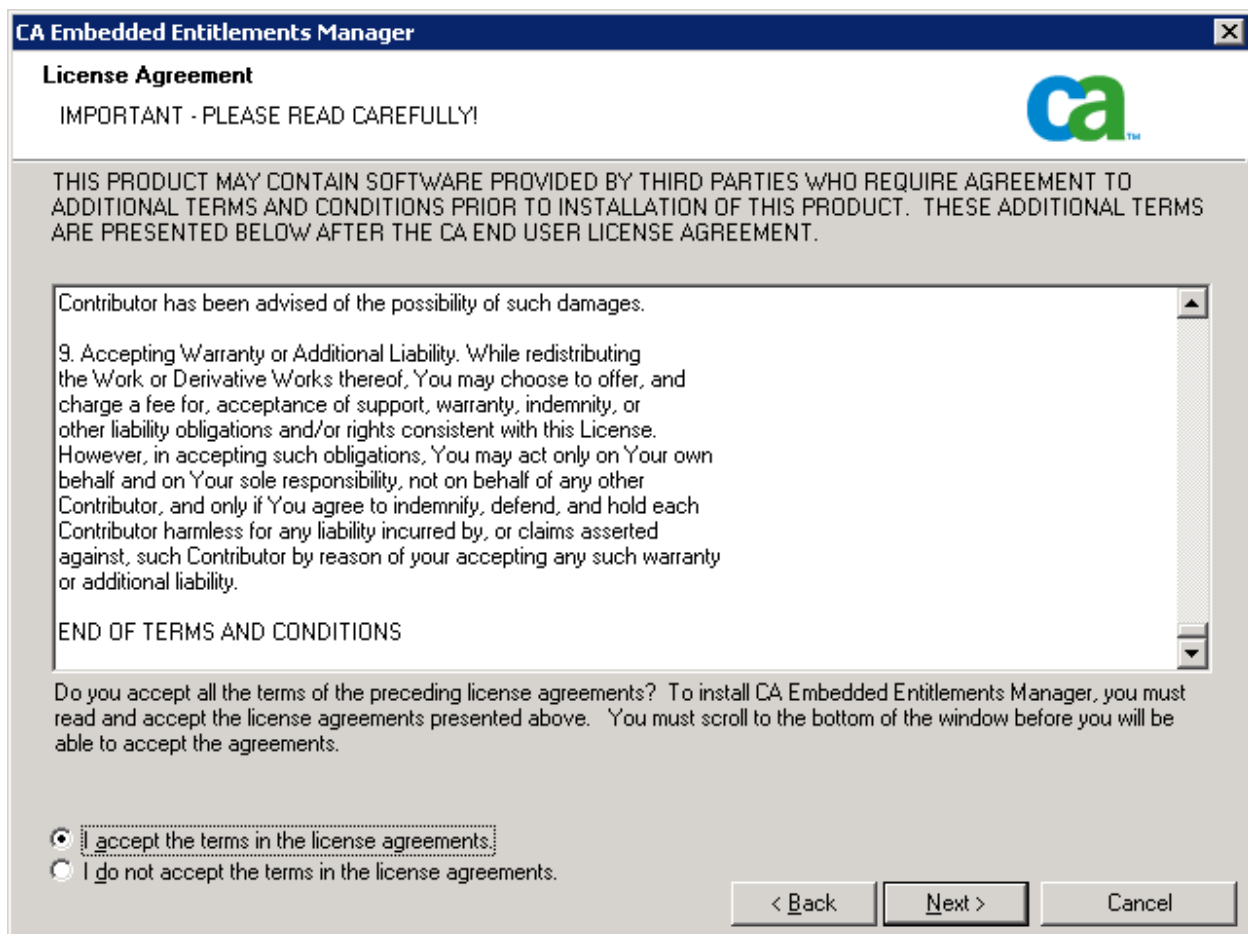
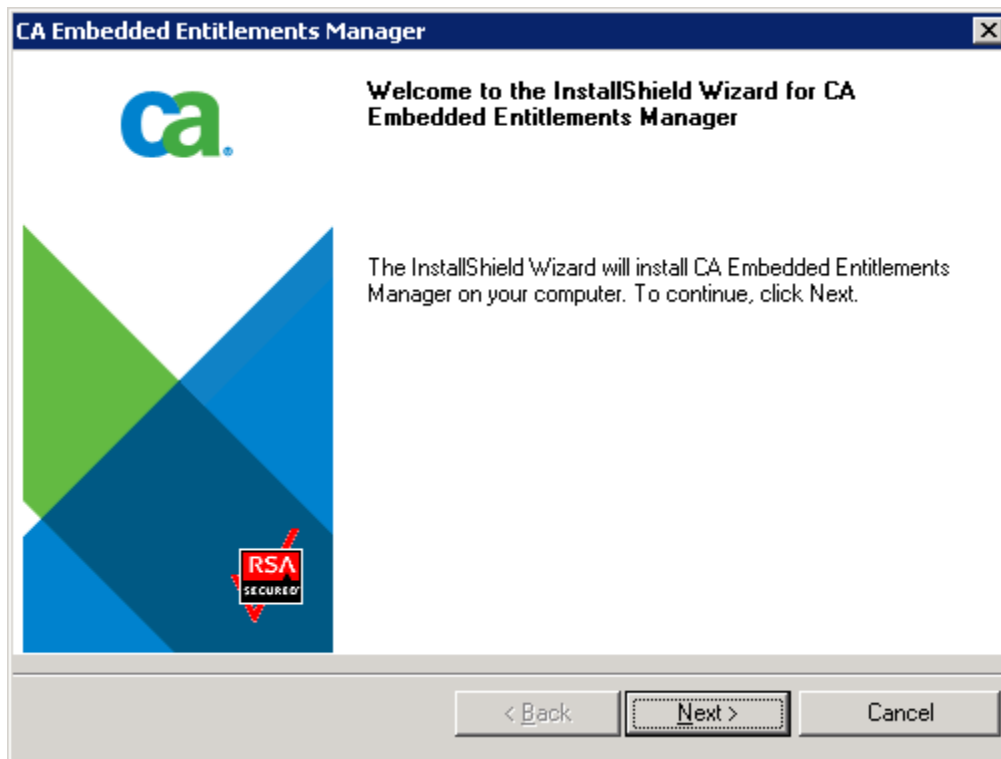
Sergio Morales
Principal Support Engineer
CA Technologies
Morse06@ca.com

Last updated: Feb, 2011

Applies to any 9.x version

Step 1: Download and install EEM: APM_EEM_9060.zip






CA Embedded Entitlements Manager [X]

Choose Destination Location

Select folder where Setup will install files.



Setup will install CA Embedded Entitlements Manager in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\...\CA\SharedComponents\Embedded IAM


InstallShield

Enter the EiamAdmin password=@dmin123

CA Embedded Entitlements Manager [X]

Install is now setting up the CA Embedded Entitlements Manager.

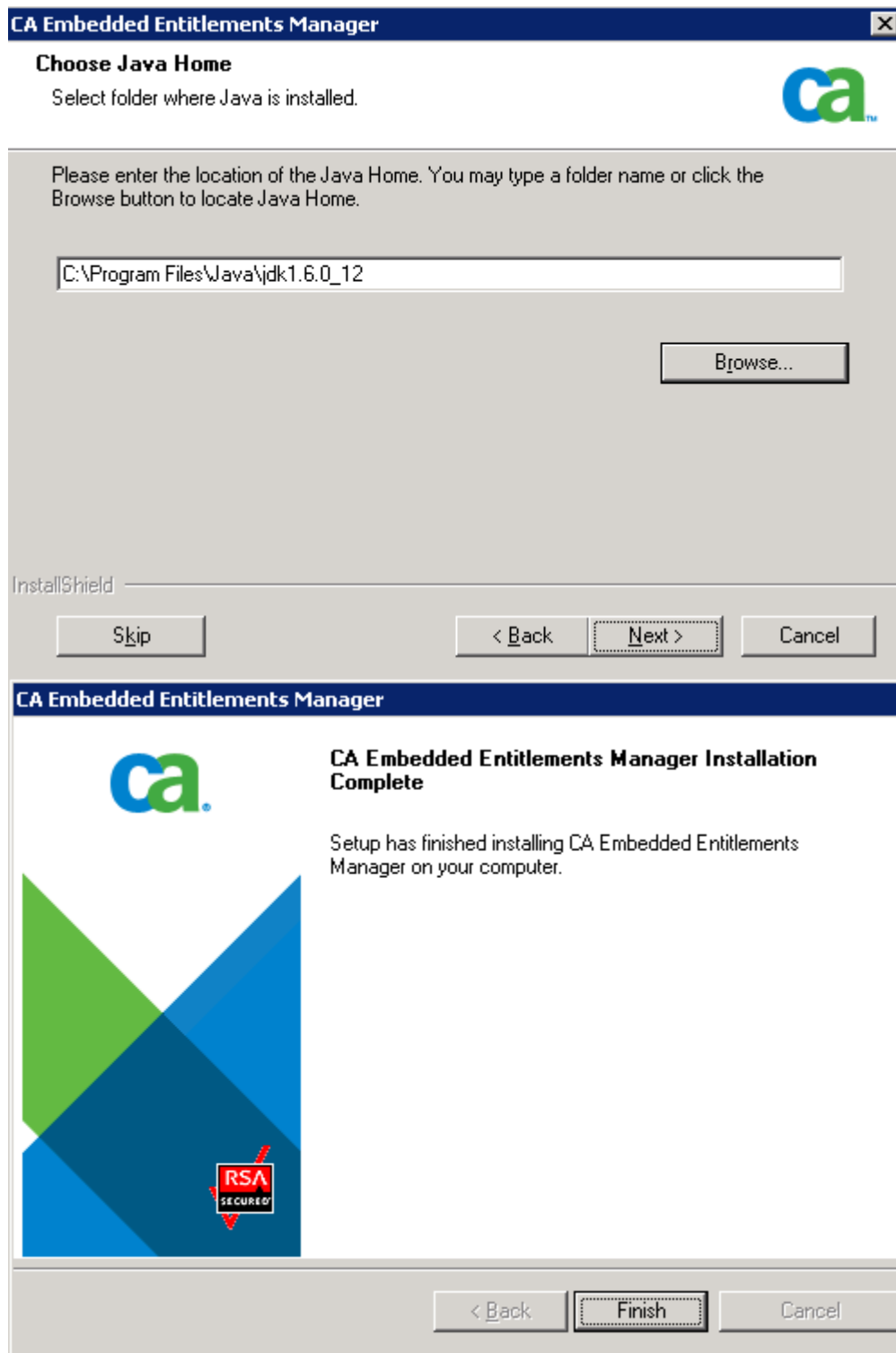
Please specify the Eiam Admin password



EiamAdmin password:

Confirm password:

InstallShield



Step 2: Registering APM applications in CA EEM, page 75

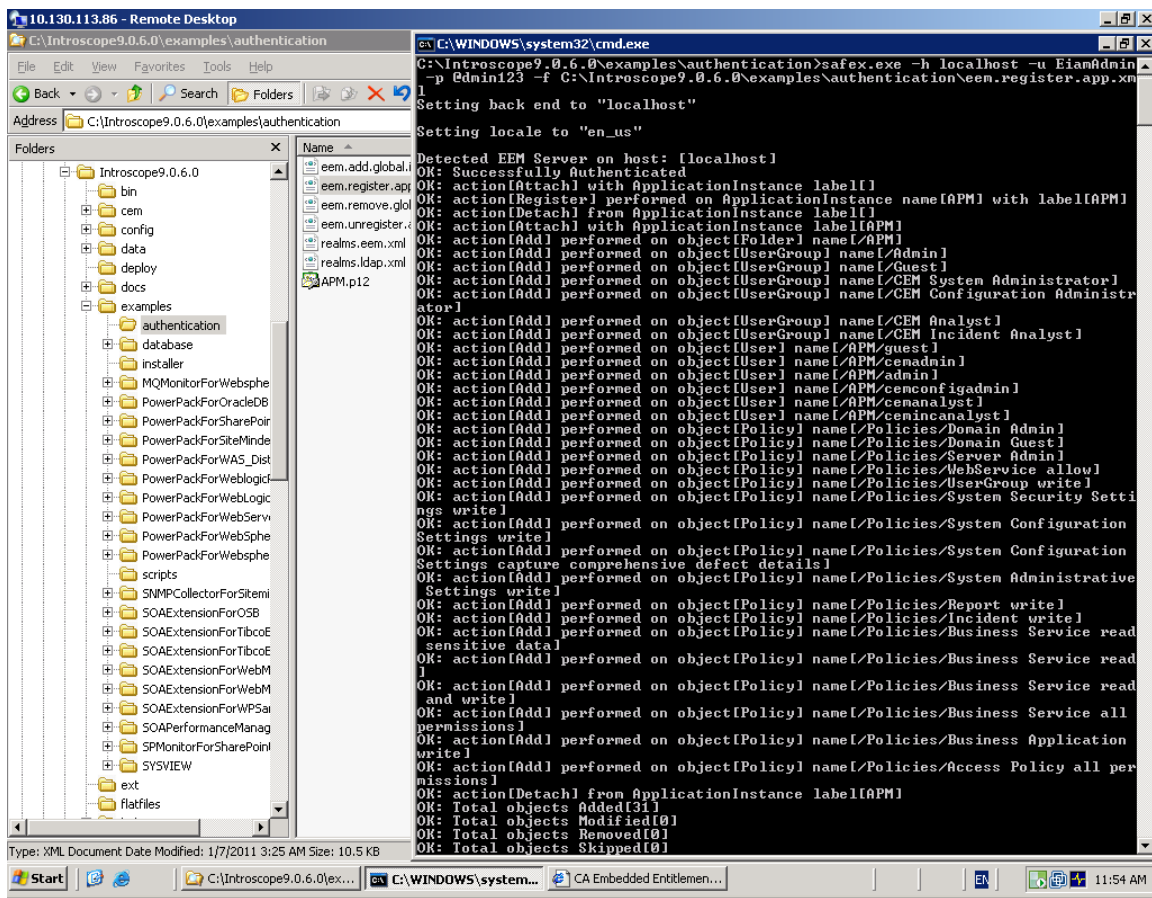
Use an administrator account

Add C:\Program Files\CA\SharedComponents\iTechnology to your PATH environment variable.

Run the following command:

```
safex.exe -h localhost -u EiamAdmin -p @dmin123 -f
```

```
C:\Introscope9.0.6.0\examples\authentication\eem.register.app.xml
```



Step 3: Verify application.

Connect to the EEM UI: <http://<EEM HostName>:5250/spin/eiam/eiam.csp>

CA Embedded Entitlements Manager

Application:

User Name:

Password:

☐ Activate Accessibility

☐ Remember my settings

Copyright © 2010 CA. All rights reserved.

RSA SECURED

Application = 'APM'
 User Name = 'EiamAdmin'
 Password = @dmin123

Click the Manage Access Policies Tab. You will have the default APM policy listed on the left

CA Embedded Entitlements Manager

Backend: **localhost** Application: **APM** Welcome: **EiamAdmin** ([Log Out](#))

Home

Manage Identities

Manage Access Policies

Manage Reports

Configure

▼ **Policies** ▶ **Calendars** ▶ **Permission Check**

Search Policies

Explicit Grants

Explicit Denies

☒ Show policies matching name
Name:

☐ Show policies matching identity

☐ Show policies matching resource

Go

Access Policies

Access Policy

Business Application

Business Service

Domain

Incident

Report

Server

System Administrative Settings

System Configuration Settings

System Security Settings

UserGroup

Step 4: Configure EEM with LDAP.

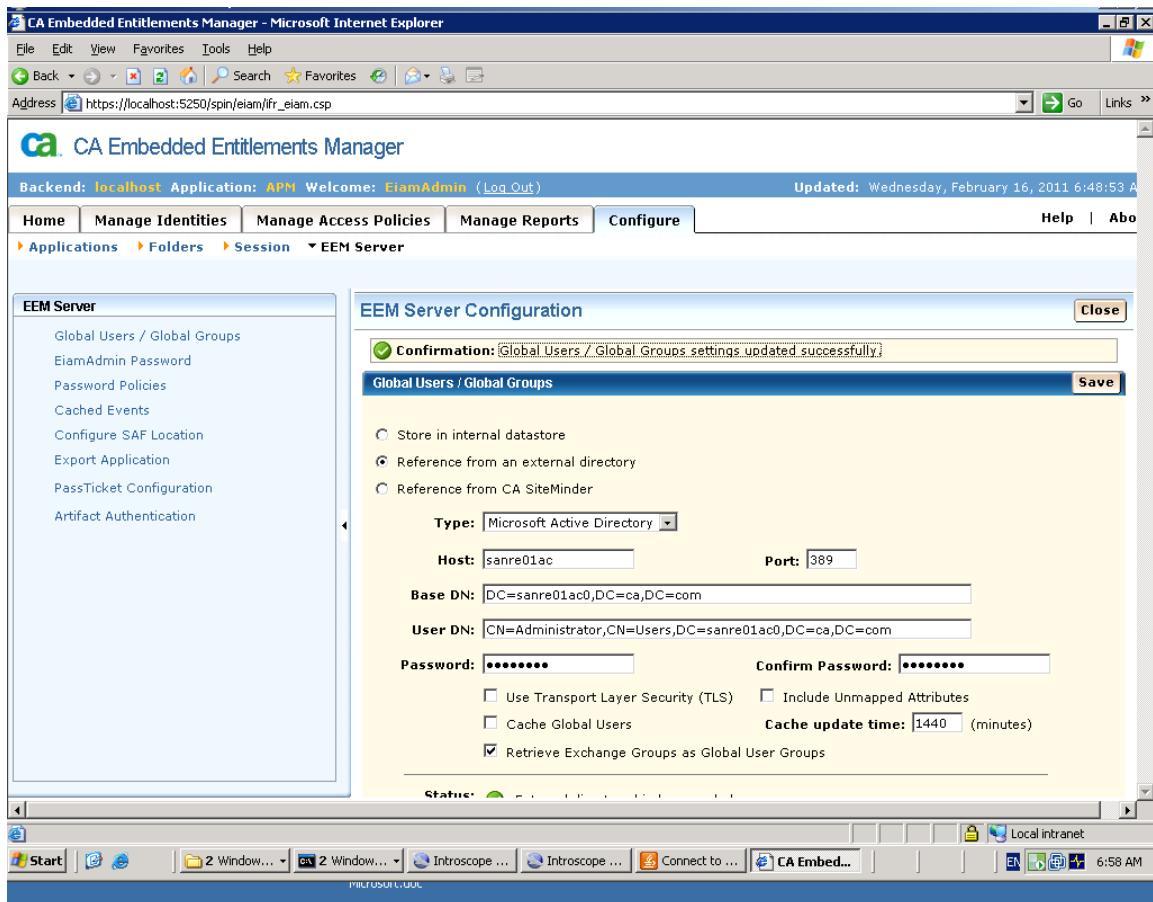
NOTE: For configuring EEM to any external LDAP login as EiamAdmin

Go to Configure > Global Users/ Global Groups

Select "Reference from an external directory"

NOTE: Contact your LDAP administrator to obtain the Base DN and the User DN information.

The below screenshot showing EEM being configured successfully with External LDAP.

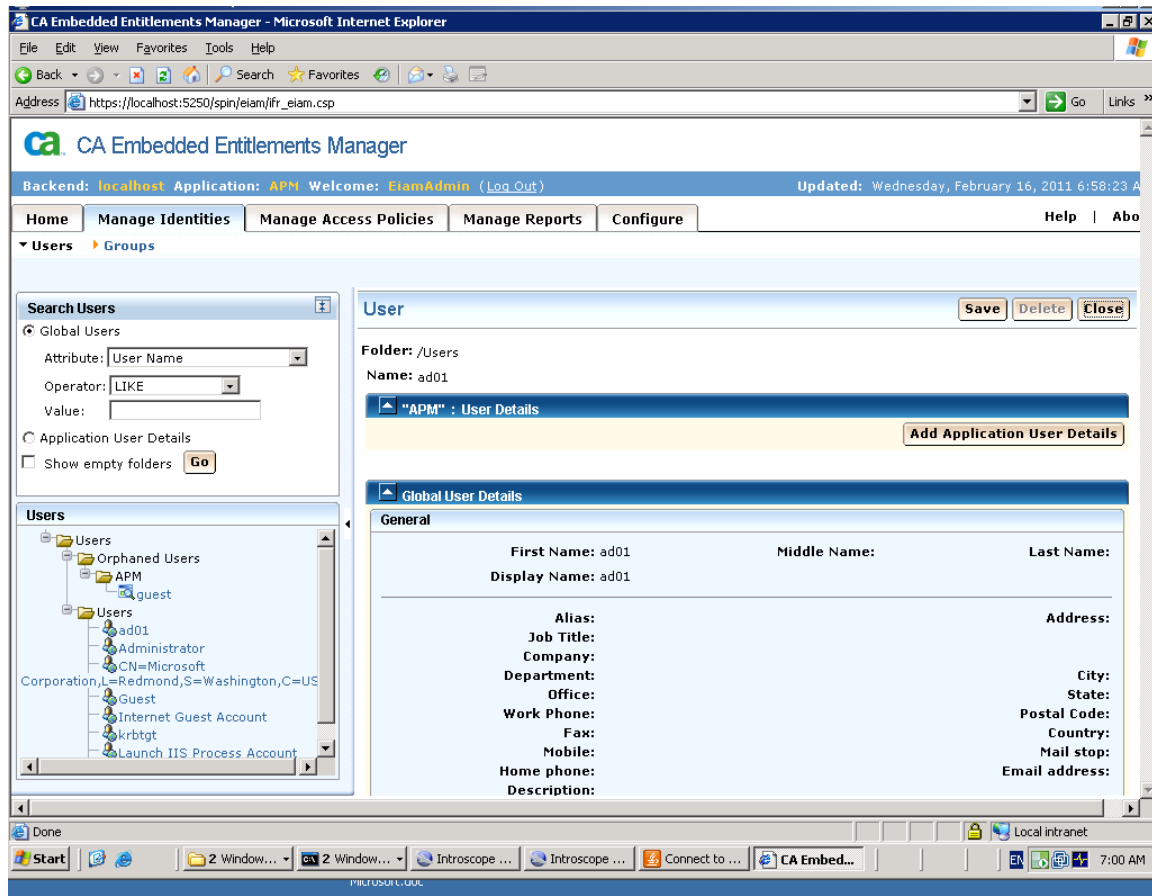


Step 5: Add the users from the LDAP (here the LDAP is Microsoft Active Directory) to the Application Specific Groups that were created while registering the APM application – in step 2 above.

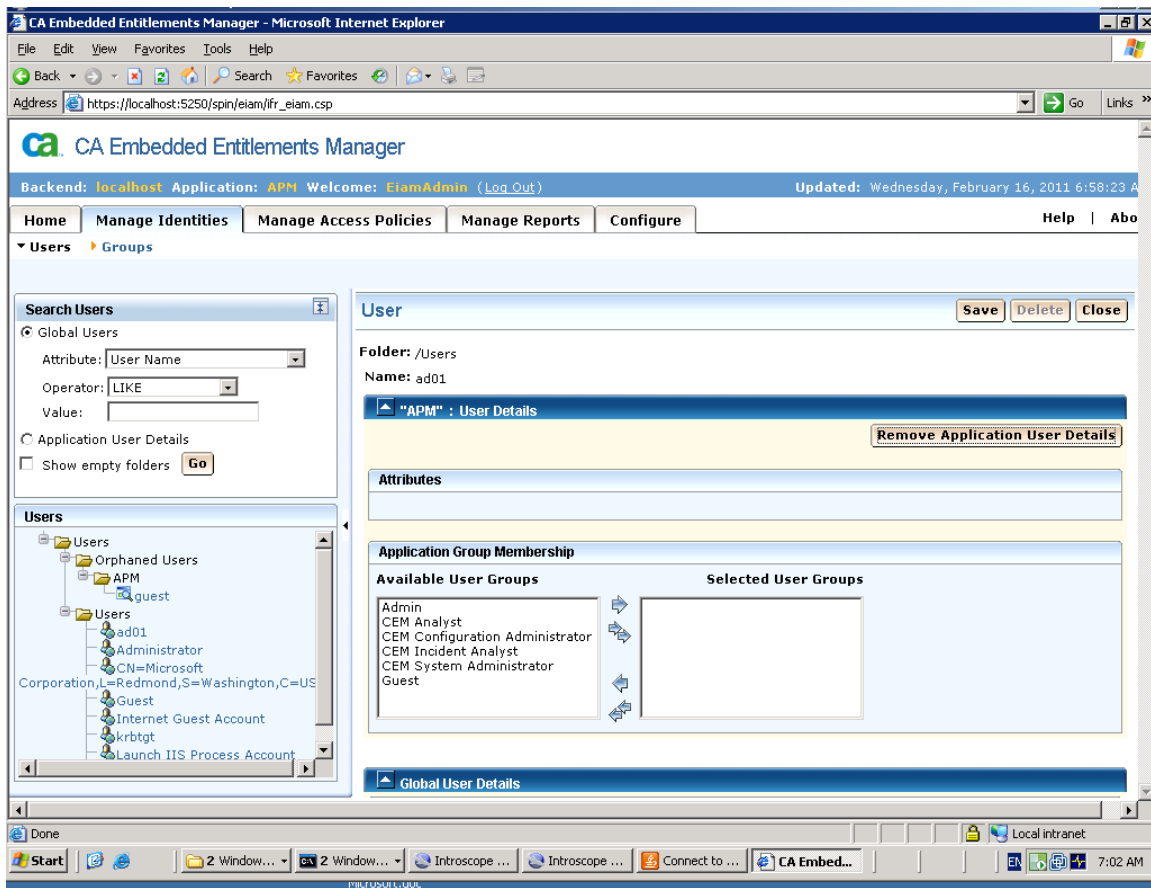
a) Go to Manage Identities Tab > Users

Select the users individually that are required to be part of the application group, for example “ad01”

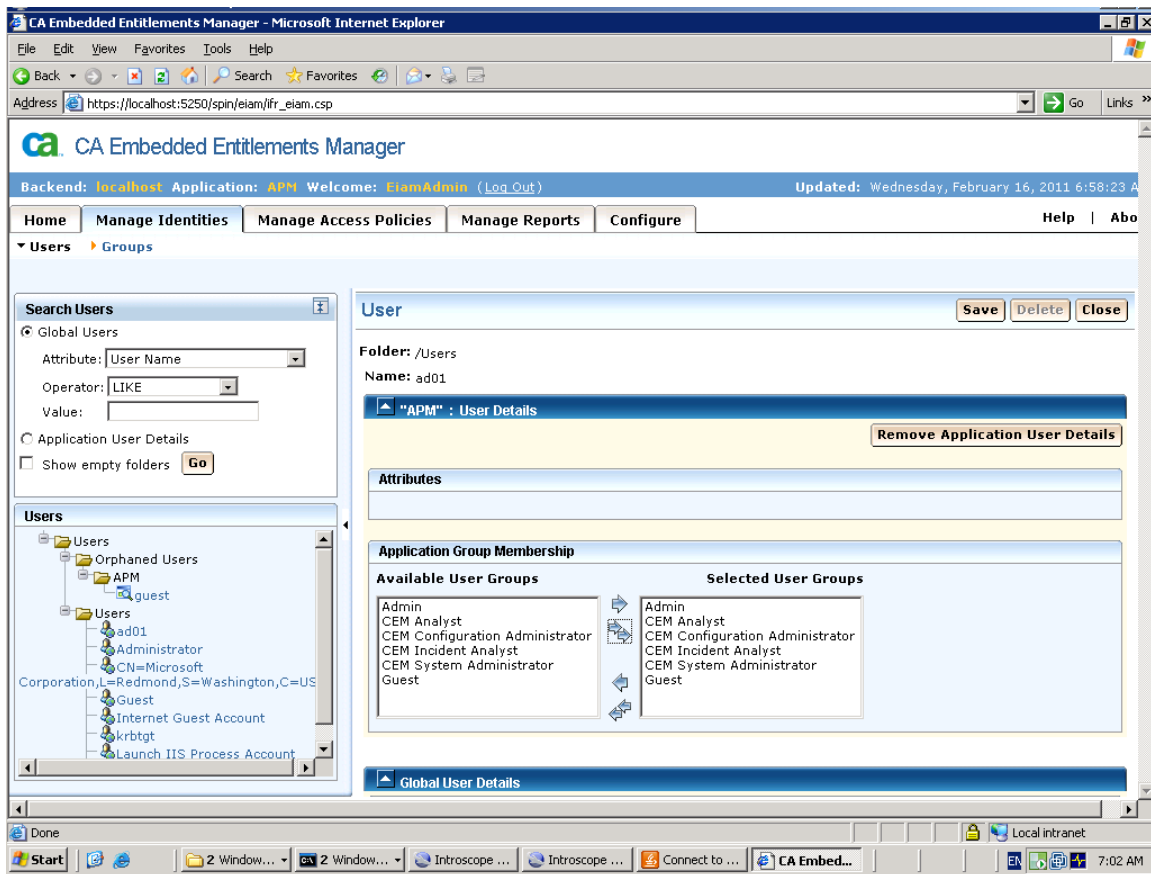
NOTE: Make sure that you are logged in as “EiamAdmin” into the application “APM” while performing the below step.



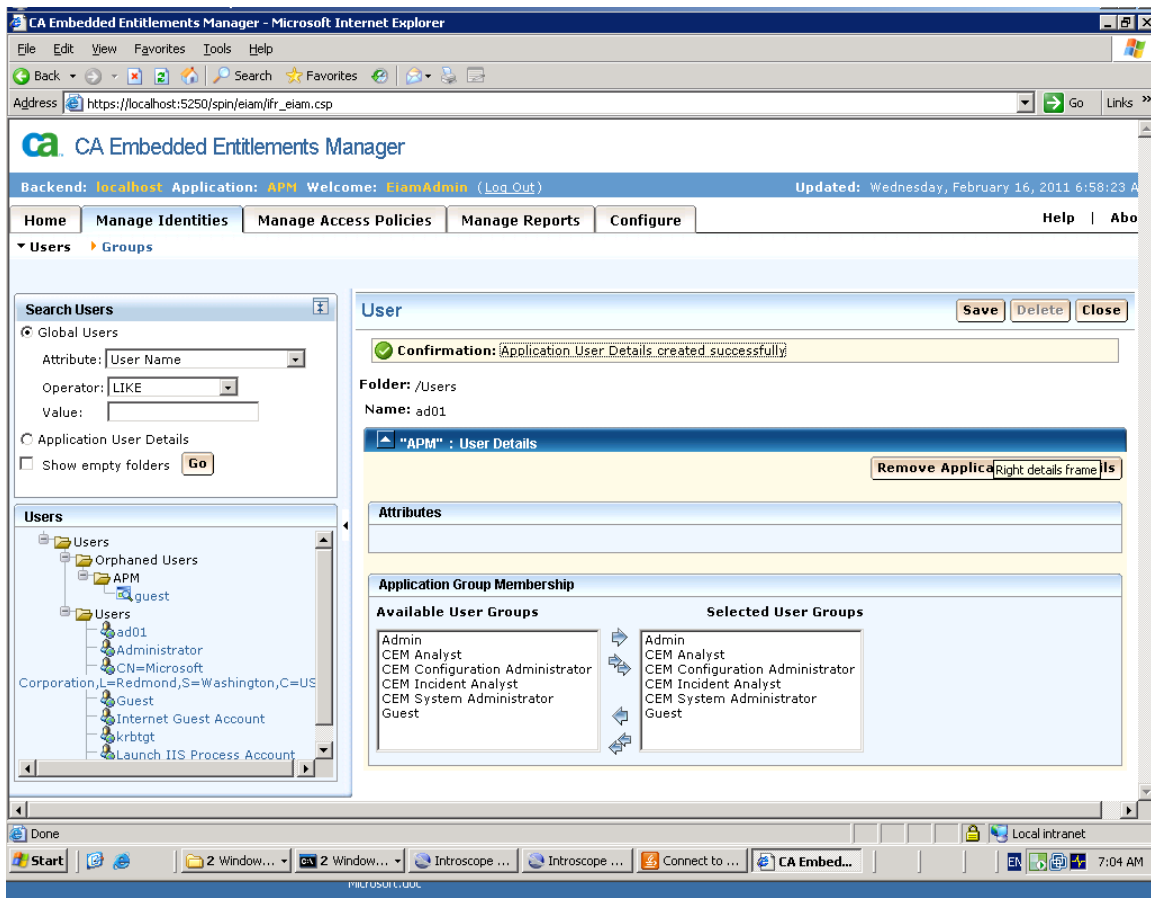
b) Click on the “Add Application User Details” button.



c) Select the Groups the user should be belonging to: for example I selected all groups

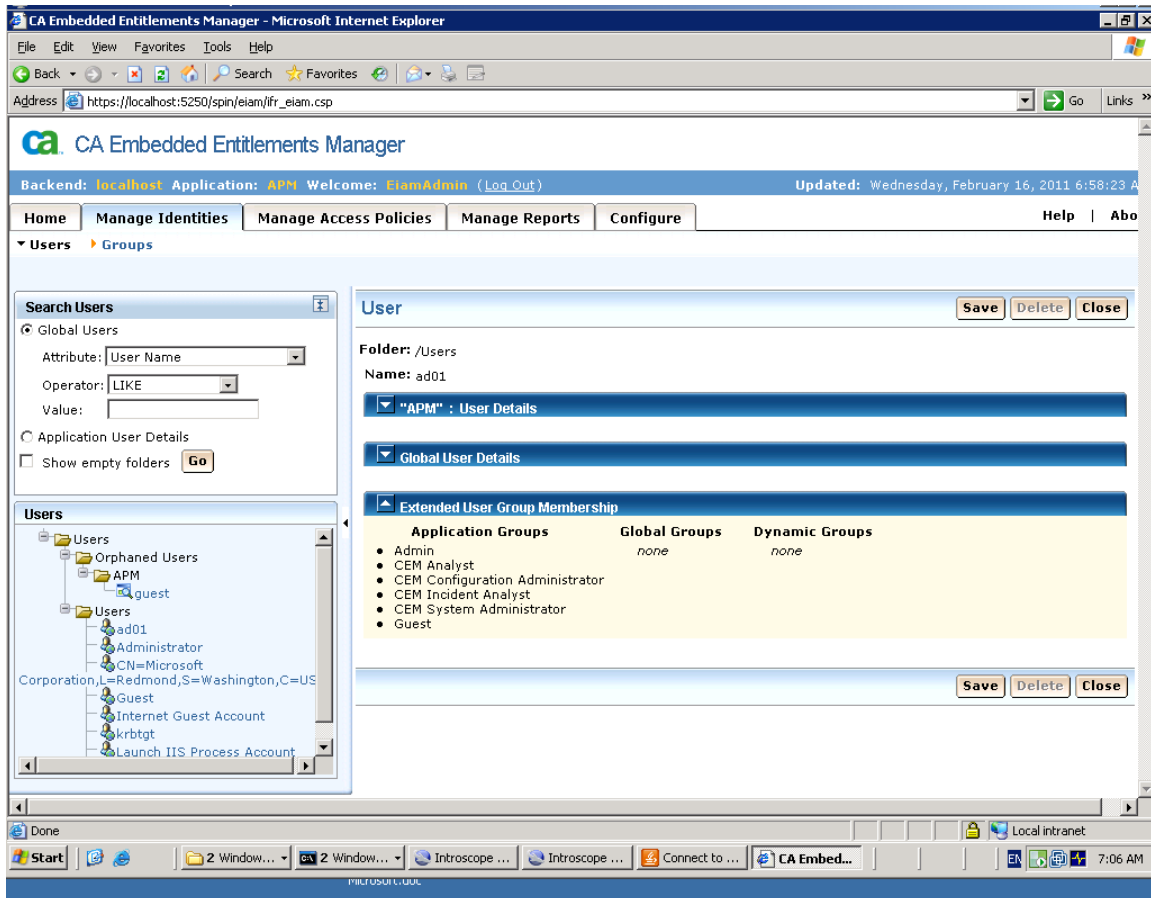


d) Save this information, click on the "Save" button.



You will receive a confirmation on success

e) Collapse the “User Details” and “Global User Details” section:



You can confirm that the user now belong to the appropriate groups

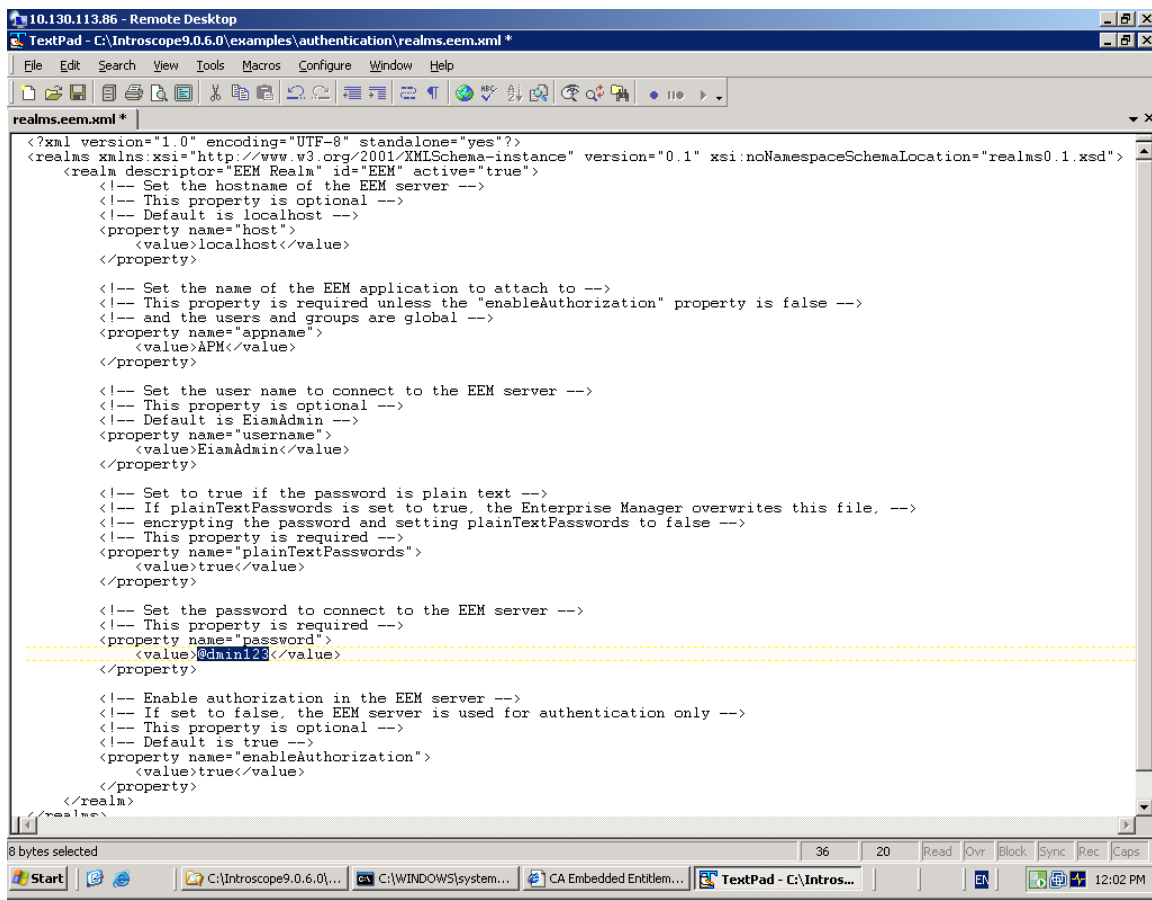
Step 6: Configure Introscope Enterprise Manager to connect to EEM

Stop the Enterprise Manager if it is running.

Locate the example file

<EnterpriseManagerHome>\examples\authentication\realms.eem.xml

Edit the realms.eem.xml file with a text editor and enter the correct password



In case the EEM installation is on a different machine than the Introscope EM, also edit the <host> property above.

```
<property name="host">
  <value>LODVMEEMSERVER.ca.com</value>
</property>
```

Copy the realms.eem.xml file to the <EnterpriseManagerHome>\config directory.

Rename the existing realms.xml to realms.xml.backup

Rename the realms.eem.xml to realms.xml

Restart Enterprise Manager

Step 7: Launch the Introscope Workstation Webstart by connecting to:

http://<Introscope_EM_hostname>:8081/workstation

Provide the credentials of the LDAP user who is part of the application group.



Select a host and port for your
Introscope Enterprise Manager
connection:

Host: LODAPM2K3X32VLAO.ca.com ▼

Port: 5001 ▼

User Name: ad01 ▼

Password: ●●●●●●●●

Connect

Set Defaults

Exit



Connection successful

In the EM_HOME\logs\IntroscopeEnterpriseManager.log:

2/16/11 07:12:43.251 AM EST [INFO] [btpool0-4] [Manager.EemRealm] "EEM" realm attached to application "APM" in EEM server at "localhost" using external directory

Successive logins will have the following in the EM Log:

2/16/11 07:42:30.517 AM EST [INFO] [PO:main Mailman 3] [Manager] User "ad01" logged in successfully from host "Node=Workstation_11, Address=LODAPM2K3X32WLAO.ca.com/10.130.113.86:3216, Type=socket"

Note: The hostname would differ as per your configuration in the EM log.

For more information refer to the [wyapm_security_guide](#)