

# How to configure APM Authentication with EEM local authentication

Sergio Morales  
Principal Support Engineer  
CA Technologies  
[Morse06@ca.com](mailto:Morse06@ca.com)

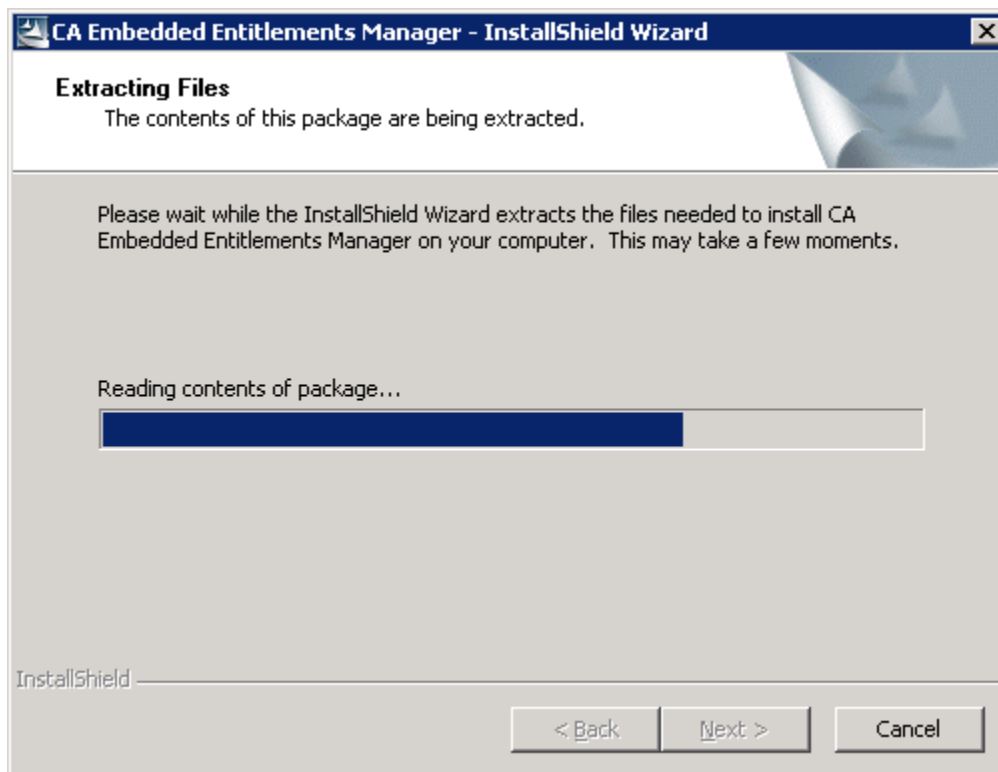
**Last updated: Feb, 2011**

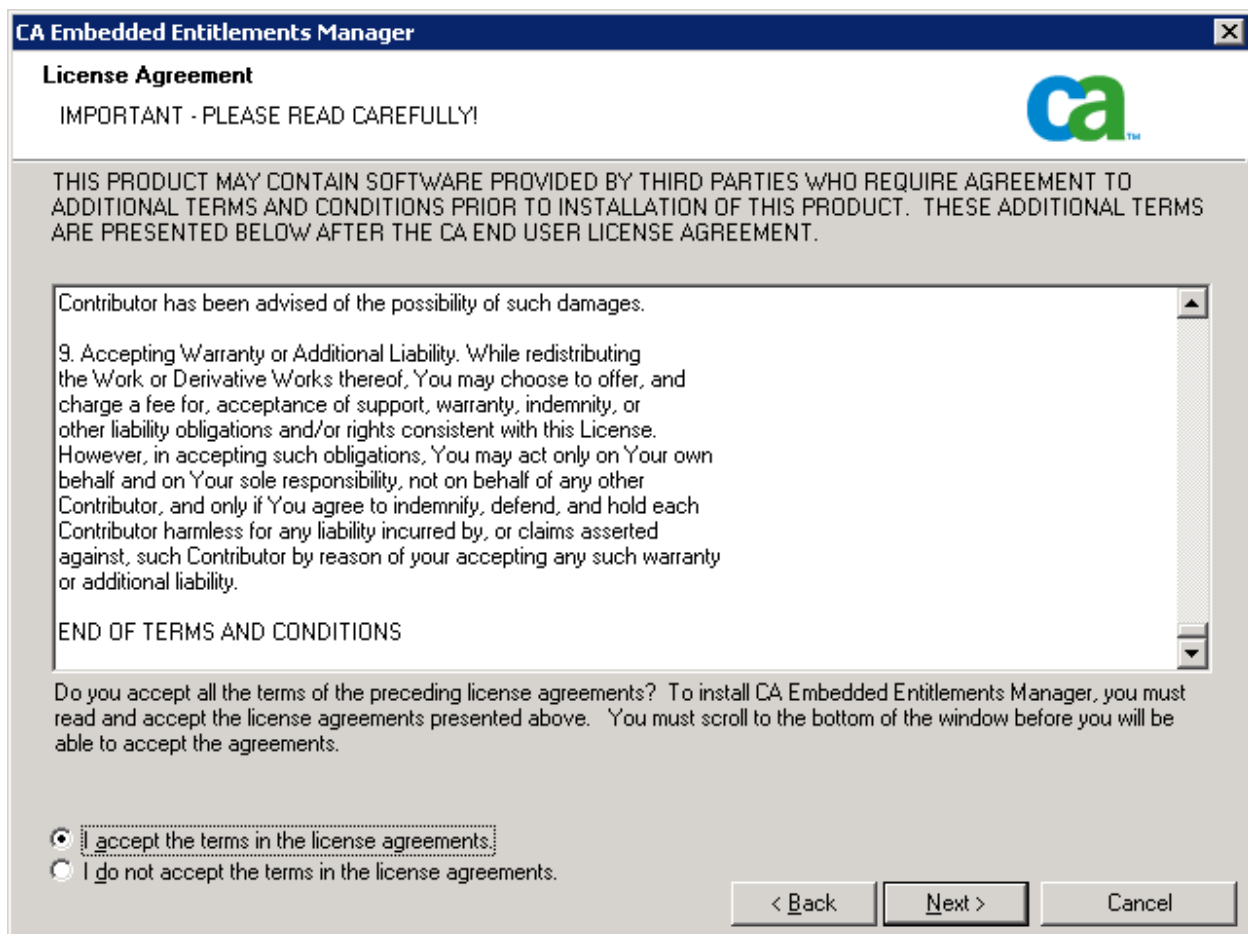
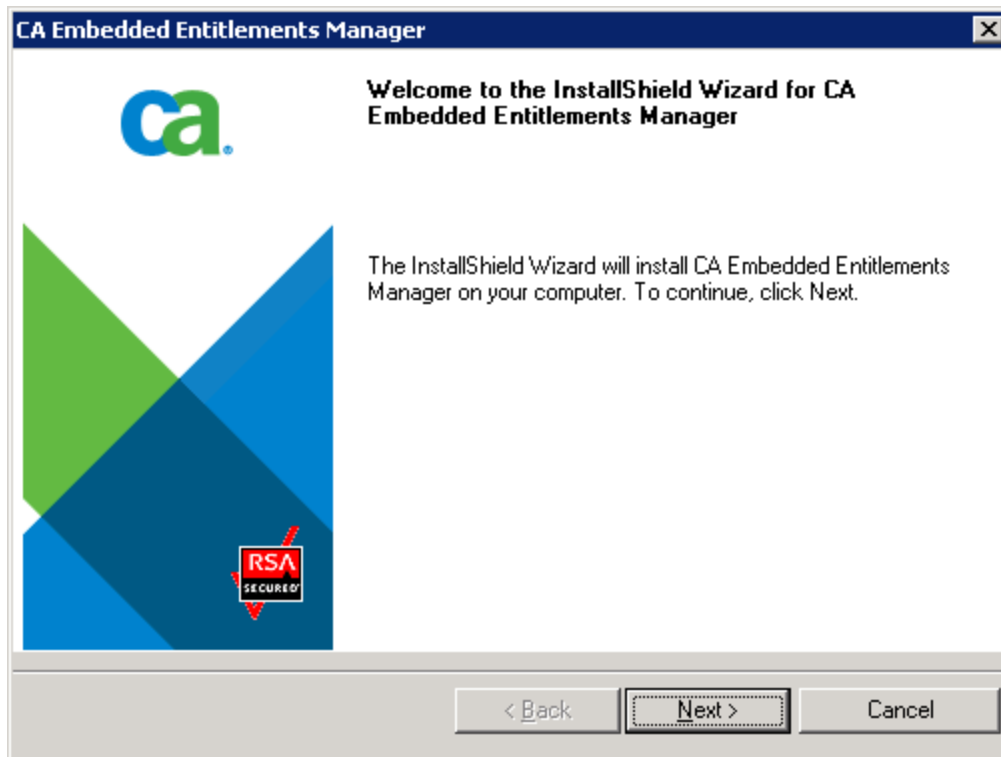
This document covers the following 2 possible case scenarios:

**CASE 1:** Configuring EEM using the default safex xml scripts provided with the EM installer.  
It will only created the default APM user and groups, for example: Admin, see Page 5

**CASE2:** Configuring EEM with Introscope to use your own users, groups and policies for domains  
It covers a basic example where a “test” user belong to a “grouptest” group and has permission to a specific custom domain, see page 11

**Step 1:** Download and install EEM: APM\_EEM\_9060.zip






**CA Embedded Entitlements Manager** ✕

**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 Browse...

InstallShield


< Back Next > Cancel

Enter the EiamAdmin password=@dmin123

**CA Embedded Entitlements Manager** ✕

**Install is now setting up the CA Embedded Entitlements Manager.**

Please specify the Eiam Admin password



EiamAdmin password:

Confirm password:

InstallShield

< Back Next > Cancel

CA Embedded Entitlements Manager

**Choose Java Home**

Select folder where Java is installed.



Please enter the location of the Java Home. You may type a folder name or click the Browse button to locate Java Home.

C:\Program Files\Java\jdk1.6.0\_12

Browse...

InstallShield

Skip

< Back

Next >

Cancel

CA Embedded Entitlements Manager



**CA Embedded Entitlements Manager Installation Complete**

Setup has finished installing CA Embedded Entitlements Manager on your computer.



< Back

Finish

Cancel

**CASE 1:** Configuring EEM using the default safex xml scripts provided with the EM installer.

It will only created the default APM user and groups, for example: Admin

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

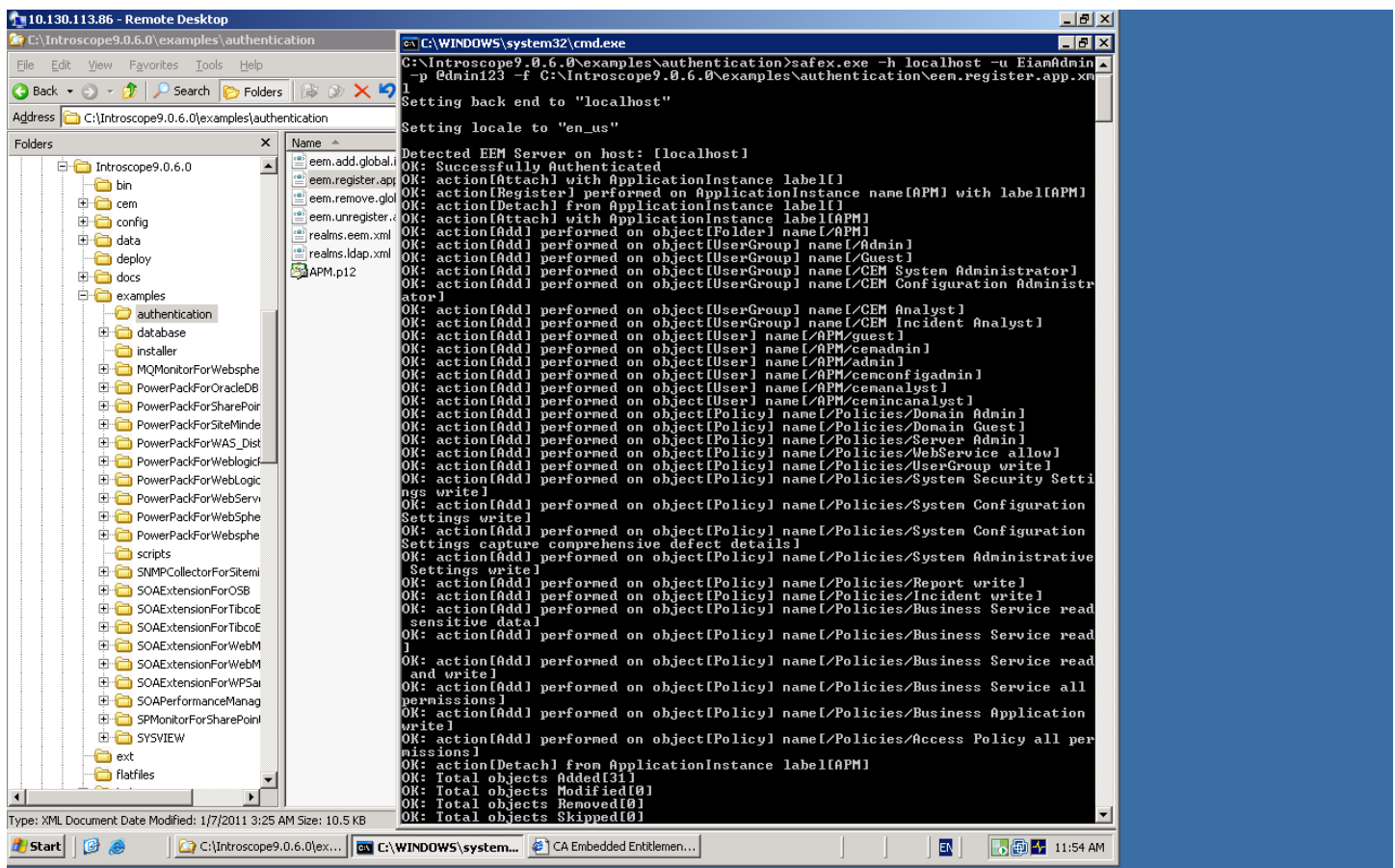
Use an administrator account

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
```

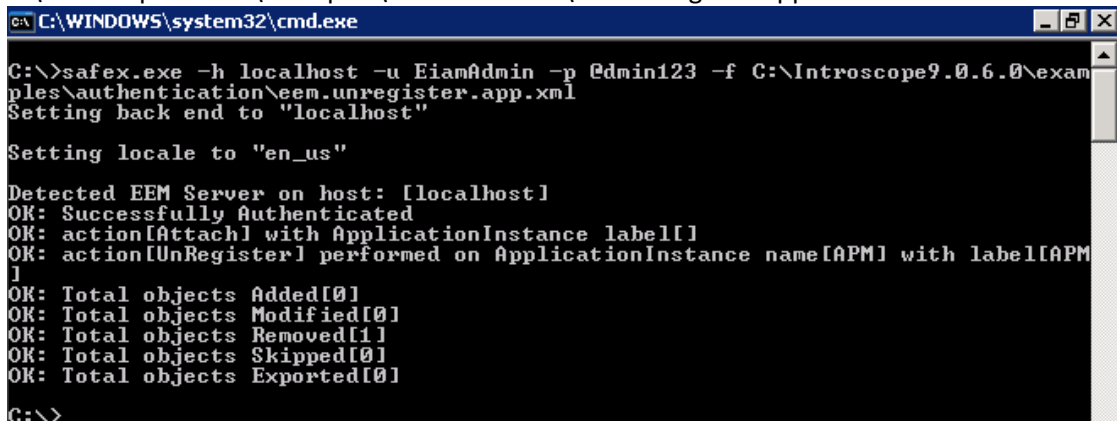


```
C:\Introscope9.0.6.0\examples\authentication>C:\WINDOWS\system32\cmd.exe
C:\Introscope9.0.6.0\examples\authentication>safex.exe -h localhost -u EiamAdmin
-p @dmin123 -f C:\Introscope9.0.6.0\examples\authentication\eem.register.app.xml
Setting back end to "localhost"
Setting locale to "en_us"
Detected EEM Server on host: [localhost]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[Register] performed on ApplicationInstance name[APM] with label[APM]
OK: action[Detach] from ApplicationInstance label[]
OK: action[Attach] with ApplicationInstance label[APM]
OK: action[Add] performed on object[Folder] name[/APM]
OK: action[Add] performed on object[UserGroup] name[/Admin]
OK: action[Add] performed on object[UserGroup] name[/Guest]
OK: action[Add] performed on object[UserGroup] name[/CEM System Administrator]
OK: action[Add] performed on object[UserGroup] name[/CEM Configuration Administrator]
OK: action[Add] performed on object[UserGroup] name[/CEM Analyst]
OK: action[Add] performed on object[UserGroup] name[/CEM Incident Analyst]
OK: action[Add] performed on object[User] name[/APM/guest]
OK: action[Add] performed on object[User] name[/APM/cemadmin]
OK: action[Add] performed on object[User] name[/APM/admin]
OK: action[Add] performed on object[User] name[/APM/cemconfigadmin]
OK: action[Add] performed on object[User] name[/APM/cemanalyst]
OK: action[Add] performed on object[Policy] name[/Policies/Domain Admin]
OK: action[Add] performed on object[Policy] name[/Policies/Domain Guest]
OK: action[Add] performed on object[Policy] name[/Policies/Server Admin]
OK: action[Add] performed on object[Policy] name[/Policies/WebService allow]
OK: action[Add] performed on object[Policy] name[/Policies/UserGroup write]
OK: action[Add] performed on object[Policy] name[/Policies/System Security Settings write]
OK: action[Add] performed on object[Policy] name[/Policies/System Configuration Settings write]
OK: action[Add] performed on object[Policy] name[/Policies/System Configuration Settings capture comprehensive defect details]
OK: action[Add] performed on object[Policy] name[/Policies/System Administrative Settings write]
OK: action[Add] performed on object[Policy] name[/Policies/Report write]
OK: action[Add] performed on object[Policy] name[/Policies/Incident write]
OK: action[Add] performed on object[Policy] name[/Policies/Business Service read sensitive data]
OK: action[Add] performed on object[Policy] name[/Policies/Business Service read and write]
OK: action[Add] performed on object[Policy] name[/Policies/Business Service all permissions]
OK: action[Add] performed on object[Policy] name[/Policies/Business Application write]
OK: action[Add] performed on object[Policy] name[/Policies/Access Policy all permissions]
OK: action[Detach] from ApplicationInstance label[APM]
OK: Total objects Added[31]
OK: Total objects Modified[0]
OK: Total objects Removed[0]
OK: Total objects Skipped[0]
OK: Total objects Skipped[0]
```

**NOTE:** If for some reason you need to remove the default APM users, run:

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

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



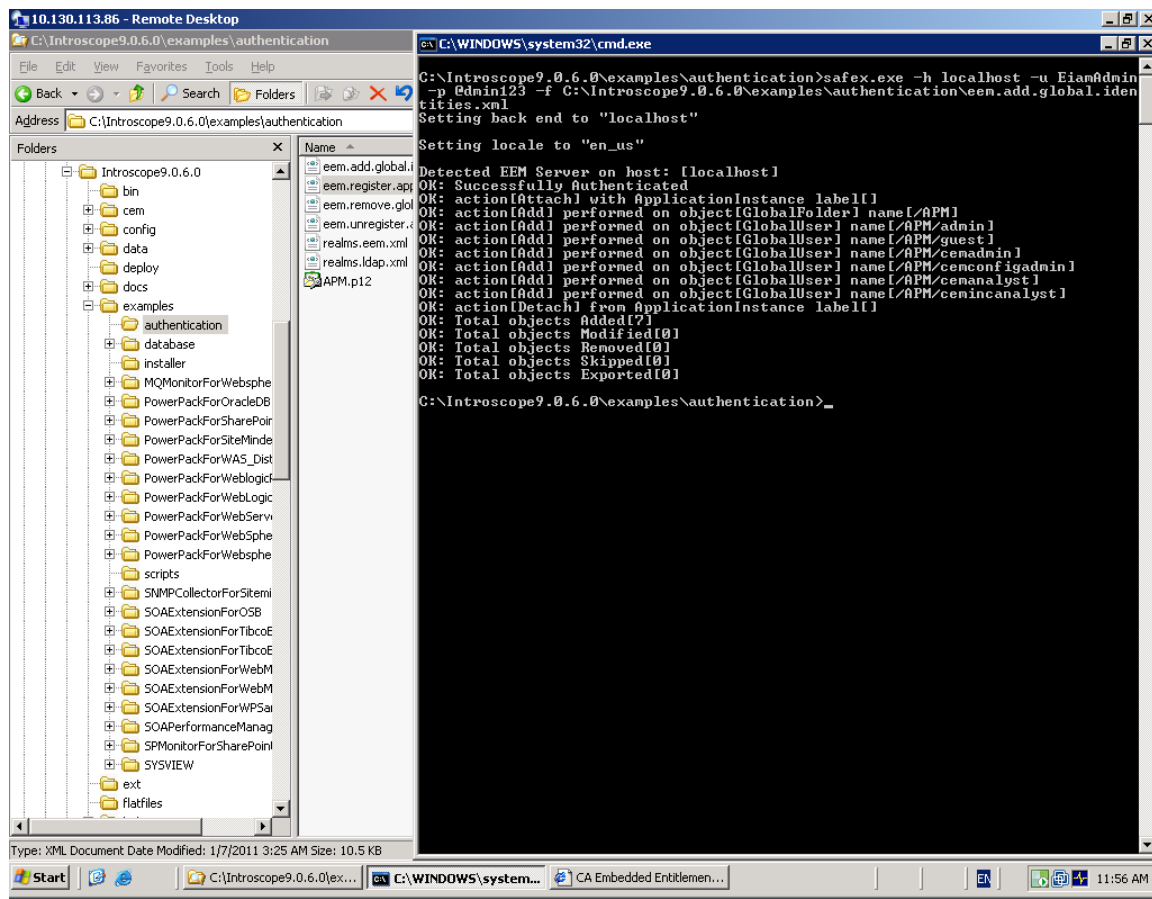
```
C:\WINDOWS\system32\cmd.exe
C:\>safex.exe -h localhost -u EiamAdmin -p @dmin123 -f C:\Introscope9.0.6.0\examples\authentication\eem.unregister.app.xml
Setting back end to "localhost"
Setting locale to "en_us"
Detected EEM Server on host: [localhost]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[UnRegister] performed on ApplicationInstance name[APM] with label[APM]
OK: Total objects Added[0]
OK: Total objects Modified[0]
OK: Total objects Removed[1]
OK: Total objects Skipped[0]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]
C:\>_
```

### Step 3: Creating APM users in CA EEM, page 77

Run the following command:

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

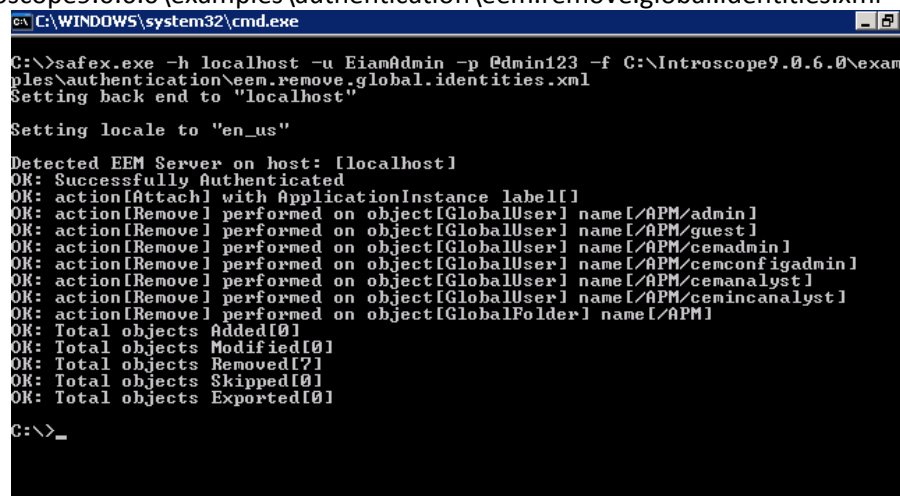
```
C:\Introscope9.0.6.0\examples\authentication\eem.add.global.identities.xml
```



**NOTE:** If for some reason you need remove the default users, run:

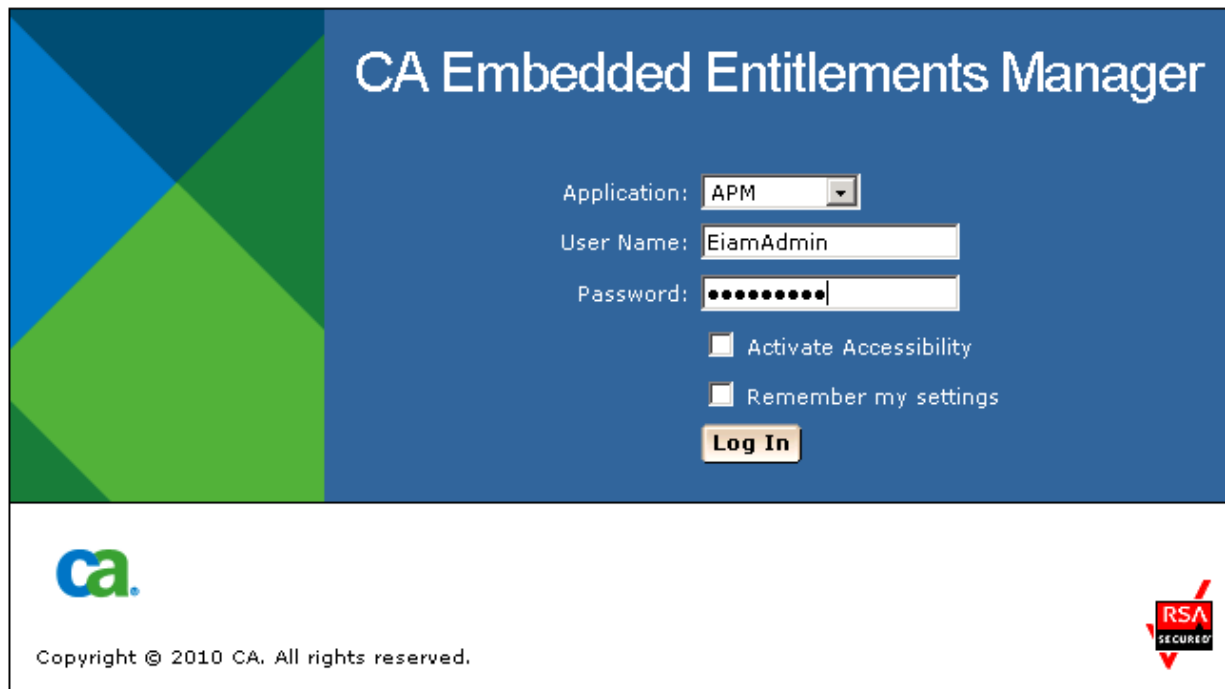
```
safex.exe -h localhost -u EiamAdmin -p @dmin123 -f
```

```
C:\Introscope9.0.6.0\examples\authentication\eem.remove.global.identities.xml
```



#### Step 4: Verify application and created users and groups.

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



The login screen for CA Embedded Entitlements Manager features a blue header with the title 'CA Embedded Entitlements Manager'. On the left is a green and blue geometric logo. The login form includes a dropdown for 'Application' (set to 'APM'), a text field for 'User Name' (containing 'EiamAdmin'), and a password field with masked characters. Below the password field are two checkboxes: 'Activate Accessibility' and 'Remember my settings'. A 'Log In' button is positioned below these options. The footer contains the 'ca.' logo, the copyright notice 'Copyright © 2010 CA. All rights reserved.', and an 'RSA SECURED' logo.

Application: APM

User Name: EiamAdmin

Password: .....

☐ Activate Accessibility

☐ Remember my settings

Log In

ca.

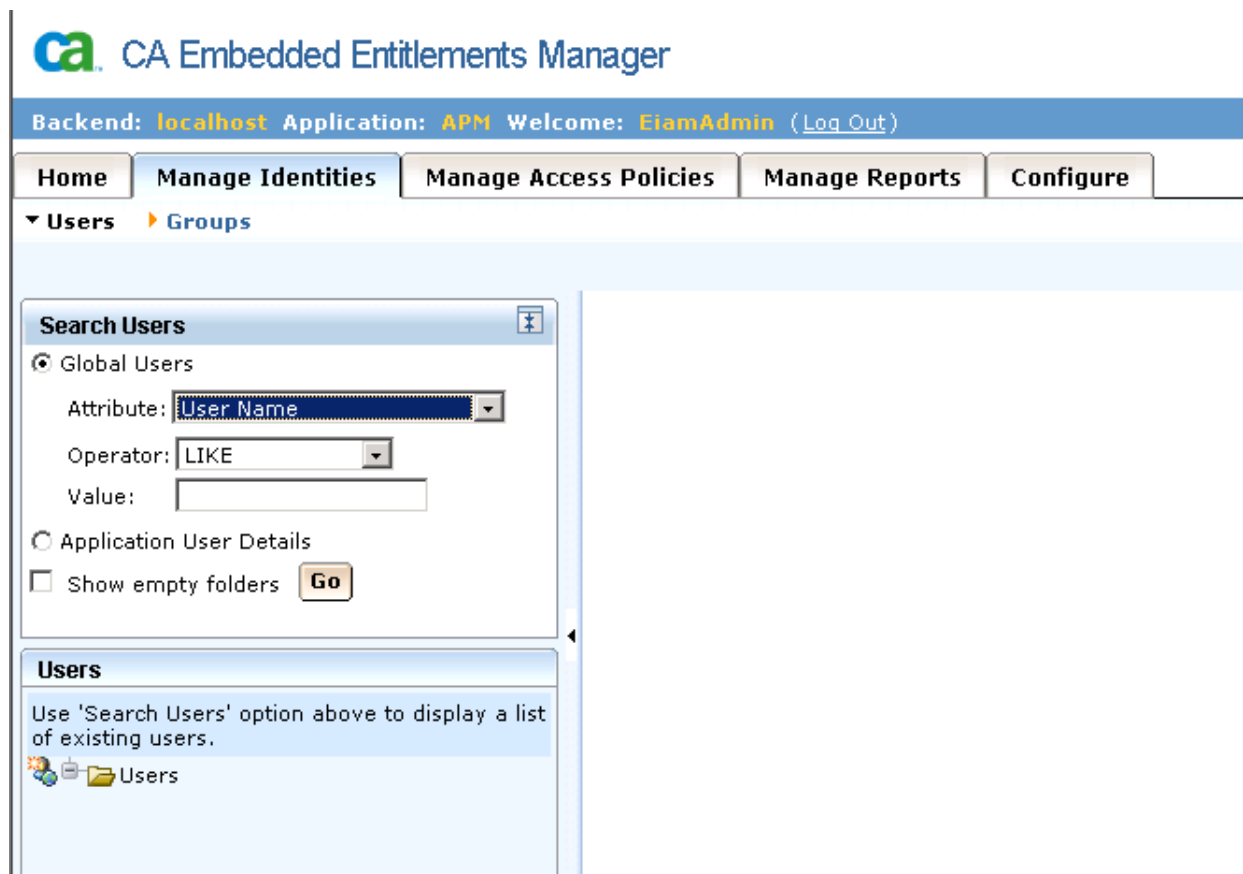
Copyright © 2010 CA. All rights reserved.

RSA SECURED

Application = 'APM'

User Name = 'EiamAdmin'

Password = @dmin123



The main interface of the CA Embedded Entitlements Manager shows a blue header with the title 'CA Embedded Entitlements Manager'. Below the header is a status bar displaying 'Backend: localhost Application: APM Welcome: EiamAdmin (Log Out)'. A navigation bar contains five tabs: 'Home', 'Manage Identities', 'Manage Access Policies', 'Manage Reports', and 'Configure'. The 'Manage Identities' tab is selected, and the 'Users' sub-tab is active. The 'Search Users' panel on the left includes a radio button for 'Global Users' (selected), a dropdown for 'Attribute' (set to 'User Name'), a dropdown for 'Operator' (set to 'LIKE'), and a text field for 'Value'. There are also radio buttons for 'Application User Details' and a checkbox for 'Show empty folders' with a 'Go' button. The 'Users' panel below shows a message: 'Use 'Search Users' option above to display a list of existing users.' and a folder icon labeled 'Users'.

CA Embedded Entitlements Manager

Backend: localhost Application: APM Welcome: EiamAdmin (Log Out)

Home Manage Identities Manage Access Policies Manage Reports Configure

▼ Users ▸ Groups

**Search Users**

☒ Global Users

Attribute: User Name

Operator: LIKE

Value:

☐ Application User Details

☐ Show empty folders Go

**Users**

Use 'Search Users' option above to display a list of existing users.

Users

Click the Manage Identities Tab, click 'Go' in the Search Users box

You will get the list of default users that were added with the sample scripts



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

**Home** **Manage Identities** **Manage Access Policies** **Manage Reports** **Configure**

▼ **Users** ▶ **Groups**

**Search Users**

☒ Global Users

Attribute:

Operator:

Value:

☐ Application User Details

☐ Show empty folders

**Users**

- Users
  - APM
    - Admin
    - cemadmin
    - cemanalyst
    - cemconfigadmin
    - cemincanalyst
    - cemsysadmin
    - Guest

**Step 5:** Configure Introscope Enterprise Manager to connect to EEM

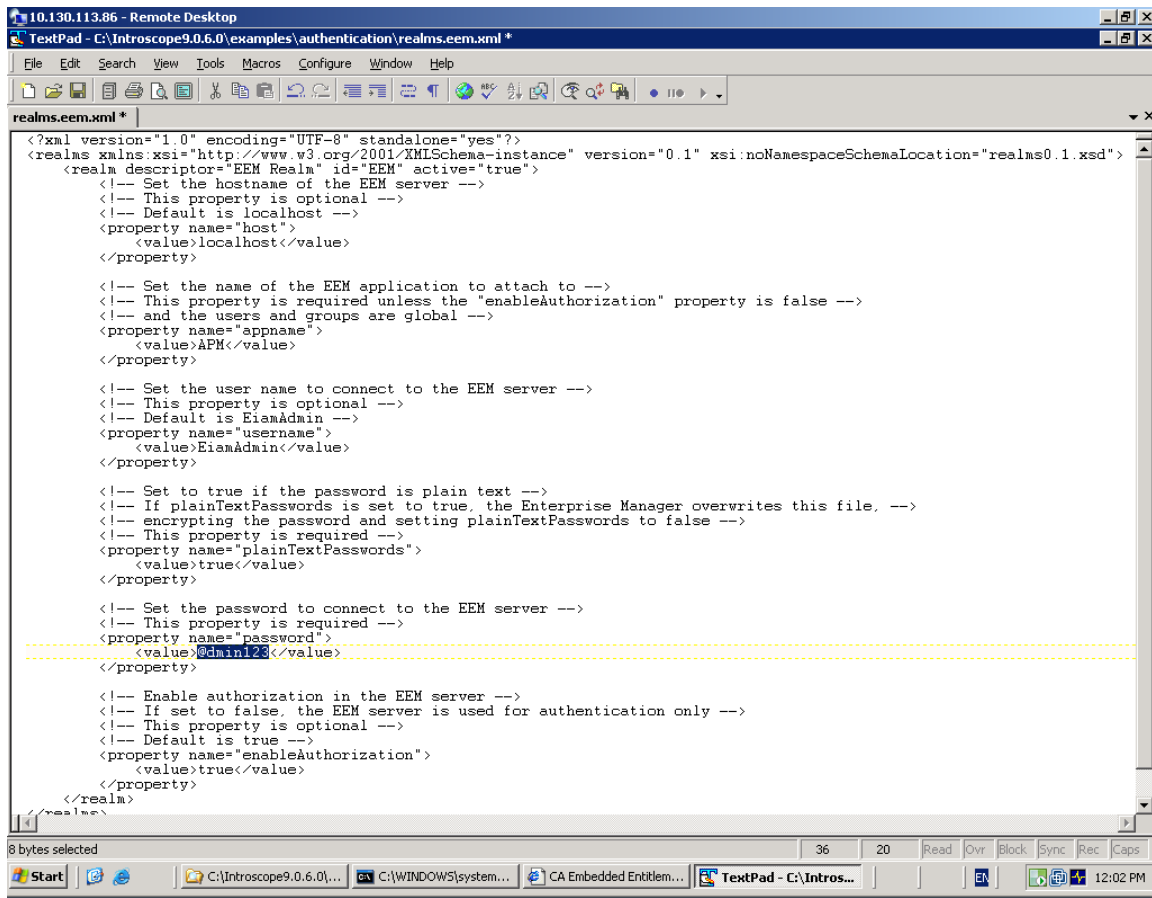
Stop the Enterprise Manager if it is running.

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>

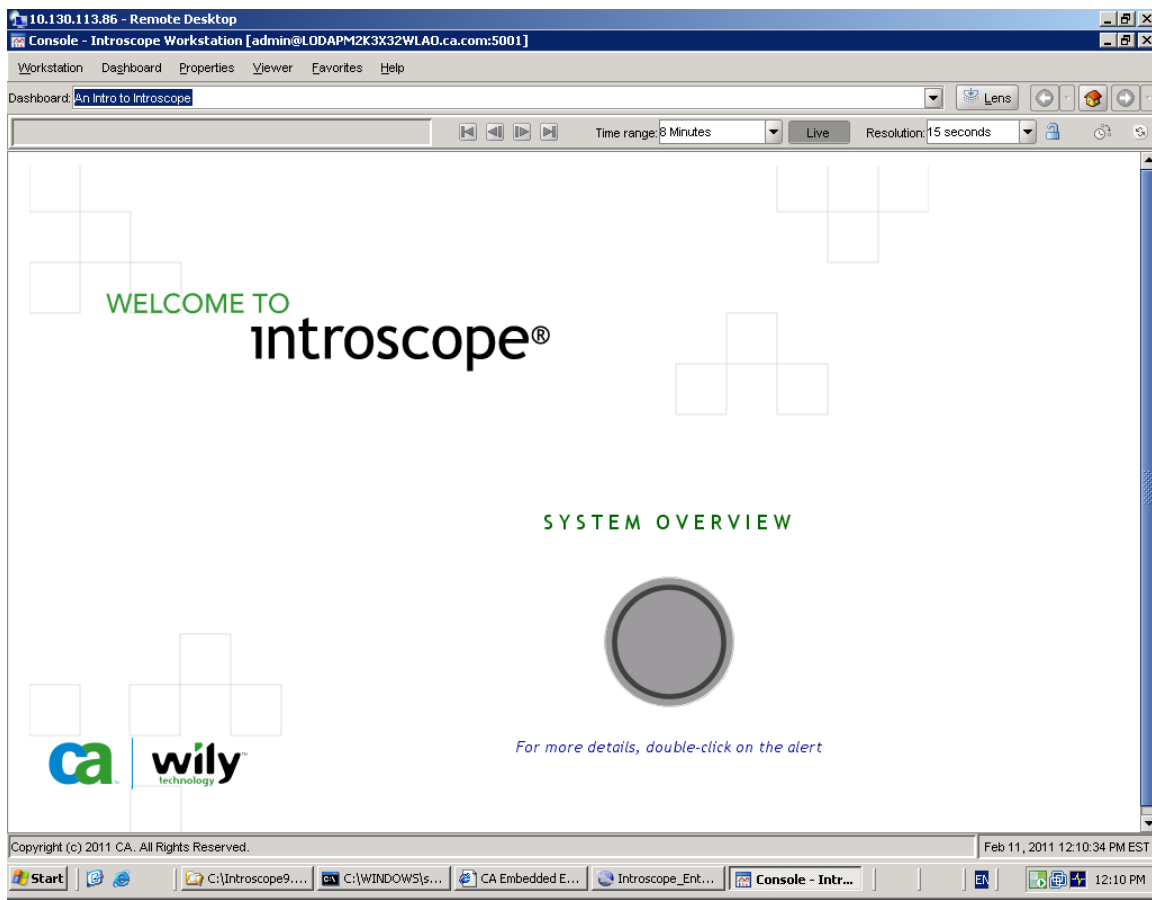
```

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, try to login using admin, password=admin



Connection successful

In the EM log:

2/11/11 12:10:20.498 PM EST [INFO] [PO:main Mailman 6] [Manager] User "admin" logged in successfully from host "Node=Workstation\_0, Address=LODAPM2K3X32WLAO.ca.com/10.130.113.86:1597, Type=socket"

## CASE2: Configuring EEM with Introscope to use your own users, groups and policies for domains

For example:, you have a test user that belong to a "grouptest" group and the "test" user has only access to a specific "DummyAgentDomain" domain:

-In users.xml:

```
users.xml | IntroscopeEnterpriseManager.log |
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<principals xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" pl.
  <users>
    <user password="d66636b253cb346dbb6240e3def3618" name="cemad:
    <user password="" name="Admin"/>
    <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest
    <user password="" name="test"/>
  </users>
  <groups>
    <group description="CEM Configuration Administrator Group" n.
    <group description="CEM System Administrator Group" name="CE
      <user name="cemadmin"/>
      <user name="Admin"/>
    </group>
    <group description="Administrator Group" name="Admin">
      <user name="cemadmin"/>
      <user name="Admin"/>
    </group>
    <group description="CEM Analyst Group" name="CEM Analyst"/>
    <group description="CEM Incident Analyst Group" name="CEM In
    <group description="grouptest" name="grouptest">
      <user name="test"/>
    </group>
  </groups>
</principals>
```

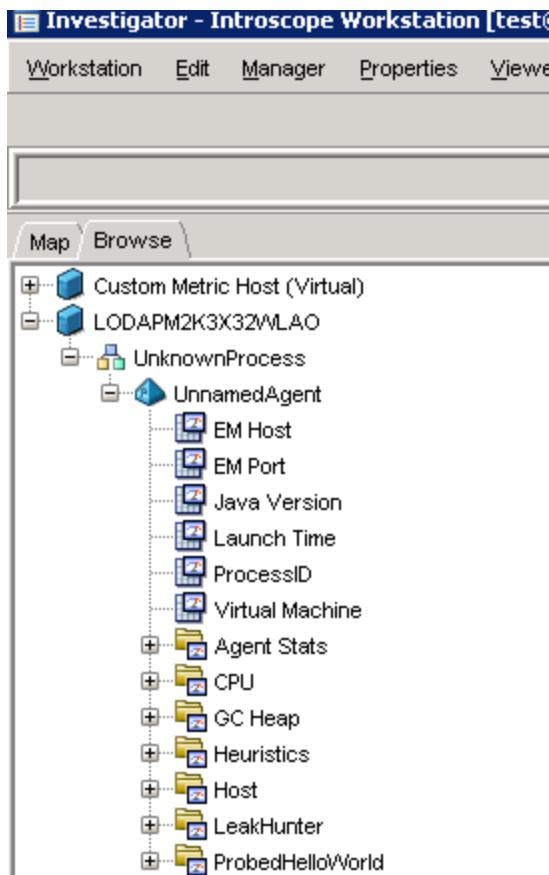
-In server.xml:

```
server.xml * | users.xml | IntroscopeEnterpriseManager.log |
<?xml version="1.0" encoding="UTF-8"?>
<server xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xs
  <grant group="Admin" permission="full"/>
  <grant group="testgroup" permission="full"/>
</server>
```

-In domains.xml:

```
domains.xml * | server.xml | users.xml | IntroscopeEnterpriseManager.log |
<?xml version="1.0" encoding="UTF-8"?>
<domains xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSche
  <domain name="DummyAgentsDomain" description="DummyAgentsDomain">
    <agent mapping="(.*)\|(.*)\|UnnamedAgent"/>
    <grant user="Test" permission="full"/>
  </domain>
  <SuperDomain>
    <agent mapping="(.*)" />
    <grant group="Admin" permission="full"/>
    <grant user="Guest" permission="read"/>
  </SuperDomain>
</domains>
```

Connecting as "test" user, you have only access to dummyagent domain:



How to implement this with EEM?

### Step 1: Registering APM applications in CA EEM, page 75

Make sure to use an administrator account and add C:\Program Files\CA\SharedComponents\iTechnology to your PATH environment variable.

Update the C:\Introscope9.0.6.0\examples\authentication\eem.register.app.xml as below:

Add the group "testgroup" and user "test"

eem.register.app.xml	domains.xml	server.xml	users.xml	IntroscopeEnterpriseManager.log
<pre> &lt;Description&gt;CEM Analyst&lt;/Description&gt; &lt;/UserGroup&gt;  &lt;UserGroup name="CEM Incident Analyst" folder="/"&gt;   &lt;Description&gt;CEM Incident Analyst&lt;/Description&gt; &lt;/UserGroup&gt;  &lt;UserGroup name="testgroup" folder="/"&gt;   &lt;Description&gt;Test Group&lt;/Description&gt; &lt;/UserGroup&gt;  &lt;!-- add users to groups --&gt; &lt;User folder="/APM" name="test"&gt;   &lt;GroupMembership&gt;testgroup&lt;/GroupMembership&gt; &lt;/User&gt; </pre>				

Add the policy for the domain:

eem.register.app.xml \*

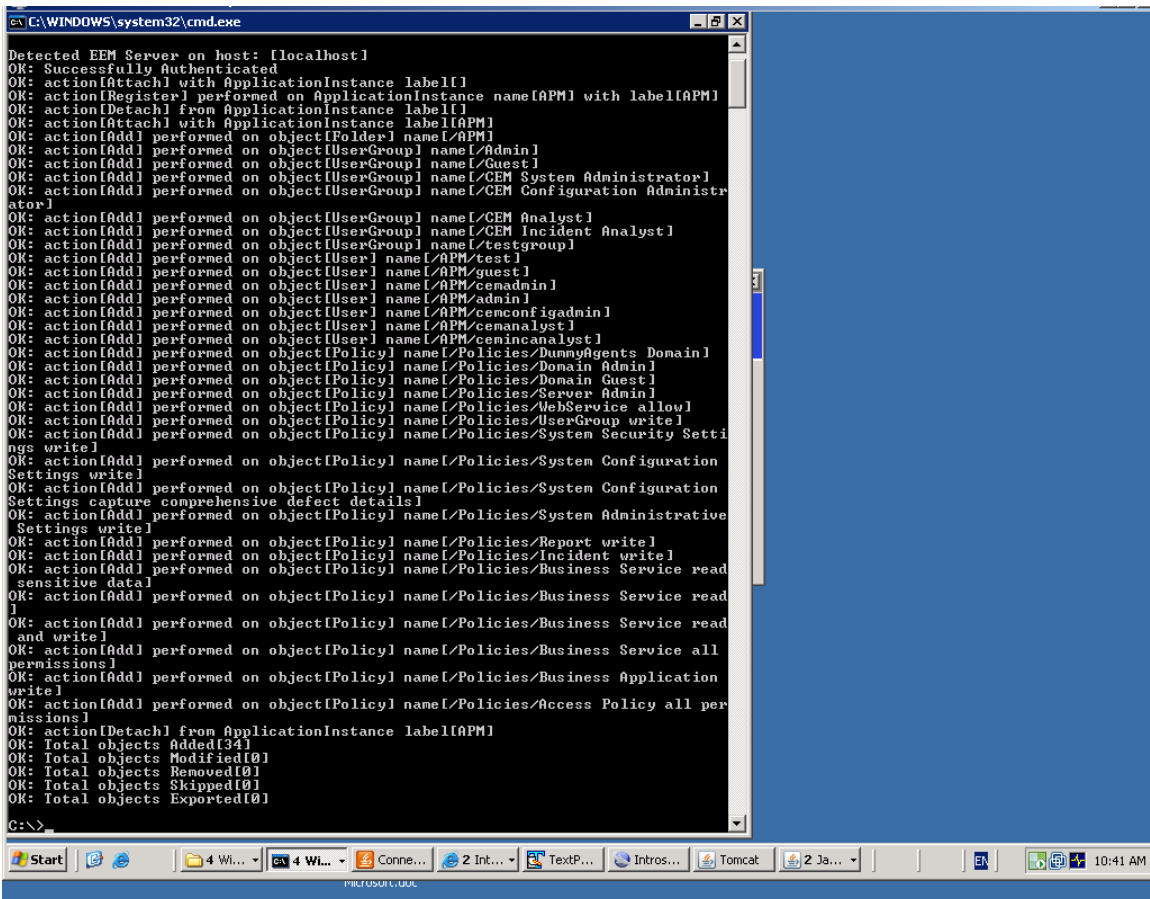
```
<User folder="/APM" name="cemincanalyst">
  <GroupMembership>CEM Incident Analyst</GroupMembership>
</User>

<!-- add policies -->
<Policy name="DummyAgents Domain" folder="/Policies">
  <Description>Test group has full permission for only dummygents Domains</Description>
  <Identity>ug:testgroup</Identity>
  <Action>full</Action>
  <ResourceClassName>Domain</ResourceClassName>
  <Resource>DummyAgentsDomain</Resource>
</Policy>
```

Run the following command:

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

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



**NOTE:** If for some reason you need to remove the default APM users, run:

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

C:\Introscope9.0.6.0\examples\authentication\eem.unregister.app.xml

```
C:\WINDOWS\system32\cmd.exe

C:\>safex.exe -h localhost -u EiamAdmin -p @dmin123 -f C:\Introscope9.0.6.0\exam
ples\authentication\eem.unregister.app.xml
Setting back end to "localhost"

Setting locale to "en_us"

Detected EEM Server on host: [localhost]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[UnRegister] performed on ApplicationInstance name[APM] with label[APM
]
OK: Total objects Added[0]
OK: Total objects Modified[0]
OK: Total objects Removed[1]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]

C:\>_
```

### Step 3: Creating APM users in CA EEM, page 77

Update the C:\Introscope9.0.6.0\examples\authentication\ eem.add.global.identities.xml as below as per our example:

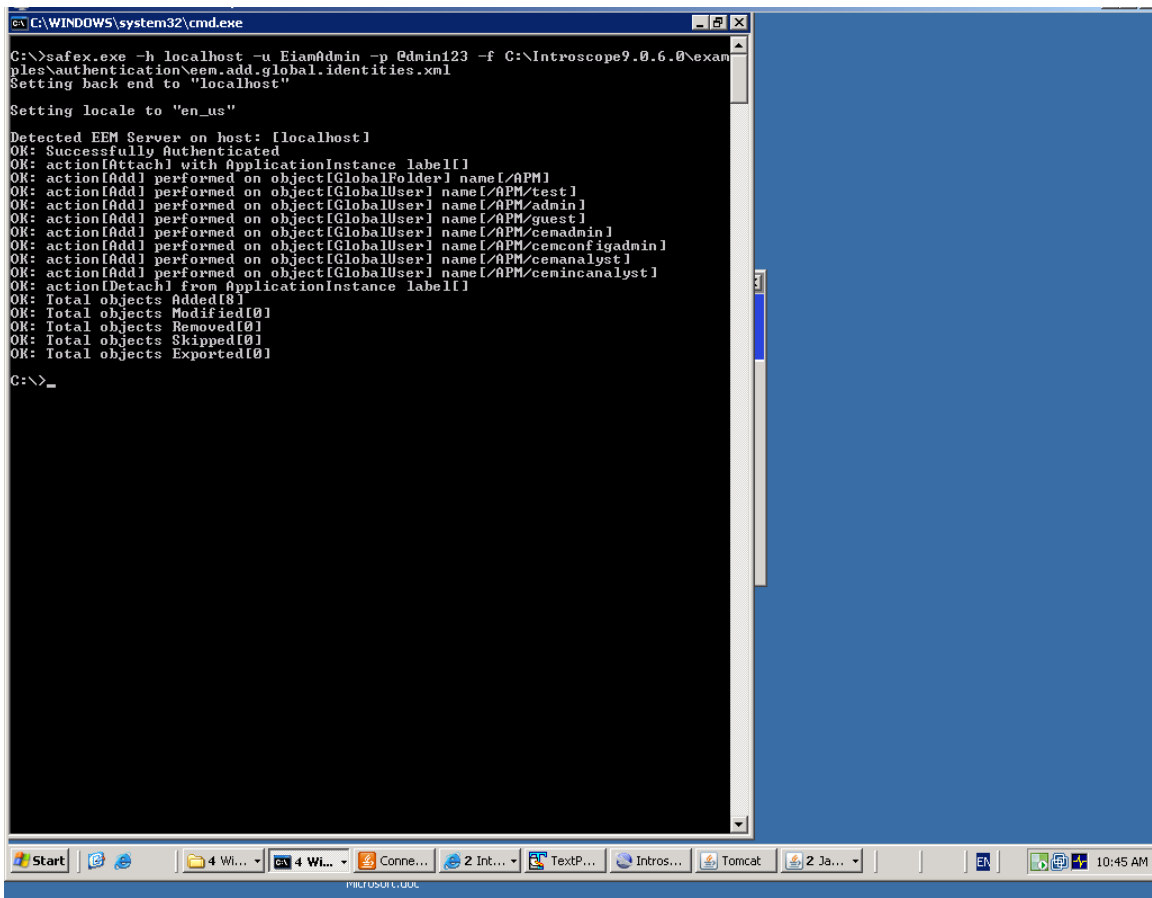
```
eem.add.global.identities.xml * | eem.register.app.xml | domains.xml | server.xml | users.xml | IntroscopeEnterpriseManager.log |

<GlobalFolder name="/APM" />
  <GlobalUser name="test" folder="/APM">
    <UserName>test</UserName>
    <DisplayName>test</DisplayName>
    <Password>test</Password>
    <FirstName>test</FirstName>
    <LastName>test</LastName>
    <WorkPhoneNumber>1 888 GET WILY (1-888-438-9459)</WorkPhoneNumber>
    <EmailAddress>support@wilytech.com</EmailAddress>
  </GlobalUser>
  <GlobalUser name="admin" folder="/APM">
```

Run the following command:

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

```
C:\Introscope9.0.6.0\examples\authentication\ eem.add.global.identities.xml
```

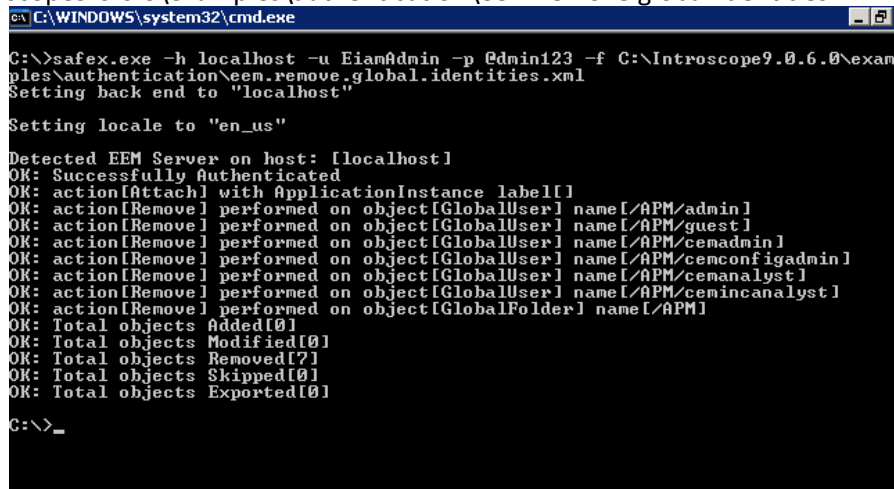


```
C:\WINDOWS\system32\cmd.exe
C:\>safex.exe -h localhost -u EiamAdmin -p @dmin123 -f C:\Introscope9.0.6.0\examples\authentication\eem.add.global.identities.xml
Setting back end to "localhost"
Setting locale to "en_us"
Detected EEM Server on host: [localhost]
OK: Successfully Authenticated
OK: action[attach] with ApplicationInstance label[]
OK: action[add] performed on object[GlobalFolder] name[/APM]
OK: action[add] performed on object[GlobalUser] name[/APM/test]
OK: action[add] performed on object[GlobalUser] name[/APM/admin]
OK: action[add] performed on object[GlobalUser] name[/APM/guest]
OK: action[add] performed on object[GlobalUser] name[/APM/cemadmin]
OK: action[add] performed on object[GlobalUser] name[/APM/cemconfigadmin]
OK: action[add] performed on object[GlobalUser] name[/APM/cemanalyst]
OK: action[add] performed on object[GlobalUser] name[/APM/cemincanalyst]
OK: action[detach] from ApplicationInstance label[]
OK: Total objects Added[8]
OK: Total objects Modified[0]
OK: Total objects Removed[0]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]
C:\>_
```

**NOTE:** If for some reason you need remove the default users, run:

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


C:\Introscope9.0.6.0\examples\authentication\eem.remove.global.identities.xml



```
C:\WINDOWS\system32\cmd.exe
C:\>safex.exe -h localhost -u EiamAdmin -p @dmin123 -f C:\Introscope9.0.6.0\examples\authentication\eem.remove.global.identities.xml
Setting back end to "localhost"
Setting locale to "en_us"
Detected EEM Server on host: [localhost]
OK: Successfully Authenticated
OK: action[attach] with ApplicationInstance label[]
OK: action[Remove] performed on object[GlobalUser] name[/APM/admin]
OK: action[Remove] performed on object[GlobalUser] name[/APM/guest]
OK: action[Remove] performed on object[GlobalUser] name[/APM/cemadmin]
OK: action[Remove] performed on object[GlobalUser] name[/APM/cemconfigadmin]
OK: action[Remove] performed on object[GlobalUser] name[/APM/cemanalyst]
OK: action[Remove] performed on object[GlobalUser] name[/APM/cemincanalyst]
OK: action[Remove] performed on object[GlobalFolder] name[/APM]
OK: Total objects Added[0]
OK: Total objects Modified[0]
OK: Total objects Removed[7]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]
C:\>_
```

**Step 4: Verify application and created users and groups.**

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.



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

 CA Embedded Entitlements Manager

Backend: localhost Application: APM Welcome: EiamAdmin (Log Out)

Home

Manage Identities

Manage Access Policies

Manage Reports

Configure

▼ Users   ► Groups

Search Users

☒ Global Users

Attribute:

Operator:


Value:

☐ Application User Details

☐ Show empty folders

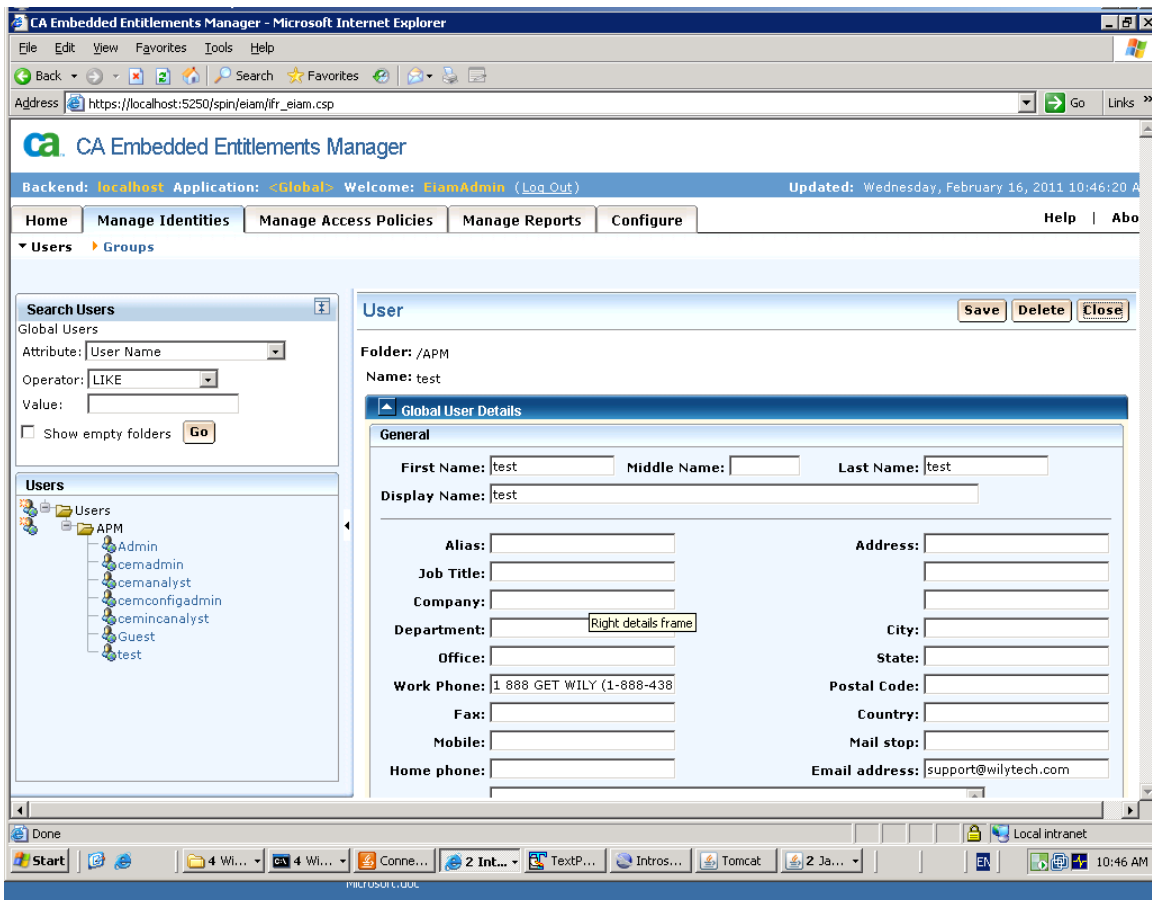
Users

Use 'Search Users' option above to display a list of existing users.

 Users

Click the Manage Identities Tab, click 'Go' in the Search Users box  
You will get the list of default users that were added with the sample scripts





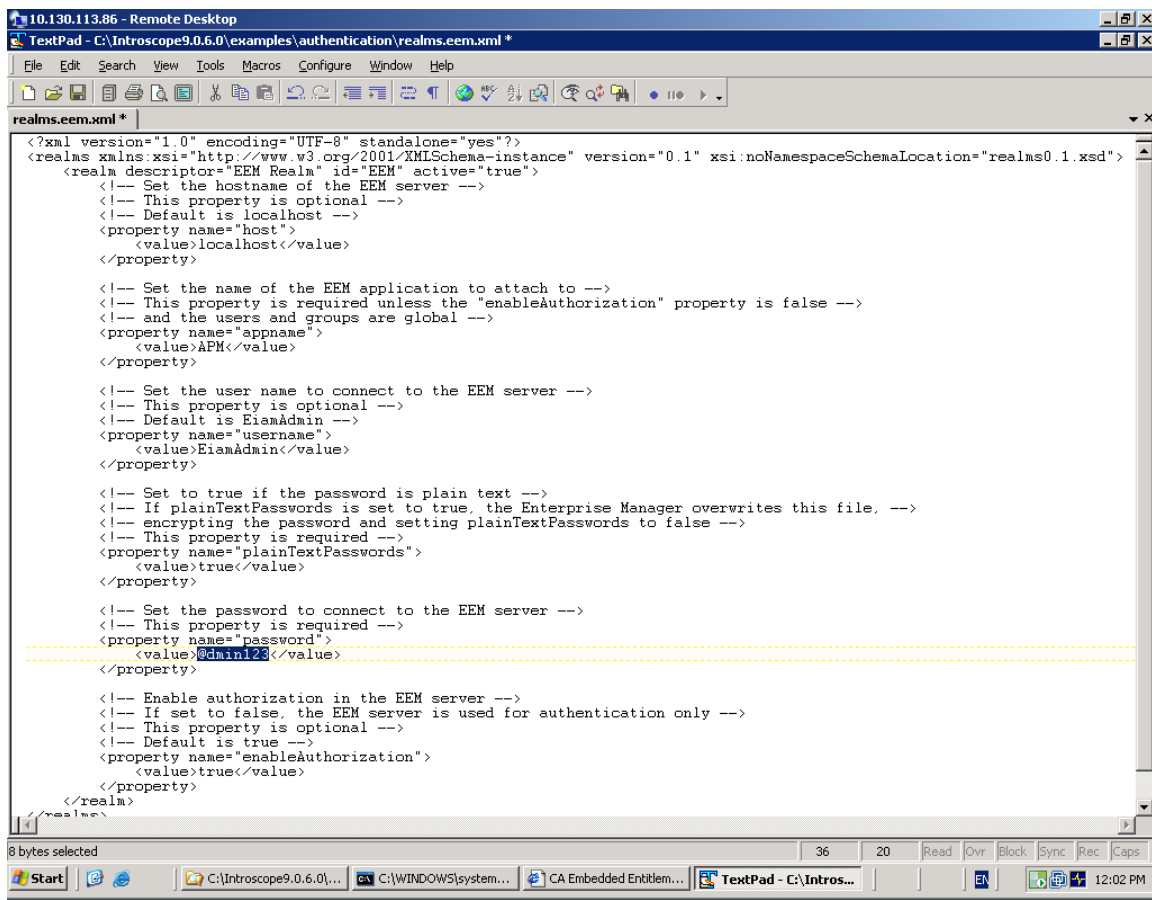
## Step 5: Configure Introscope Enterprise Manager to connect to EEM

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.

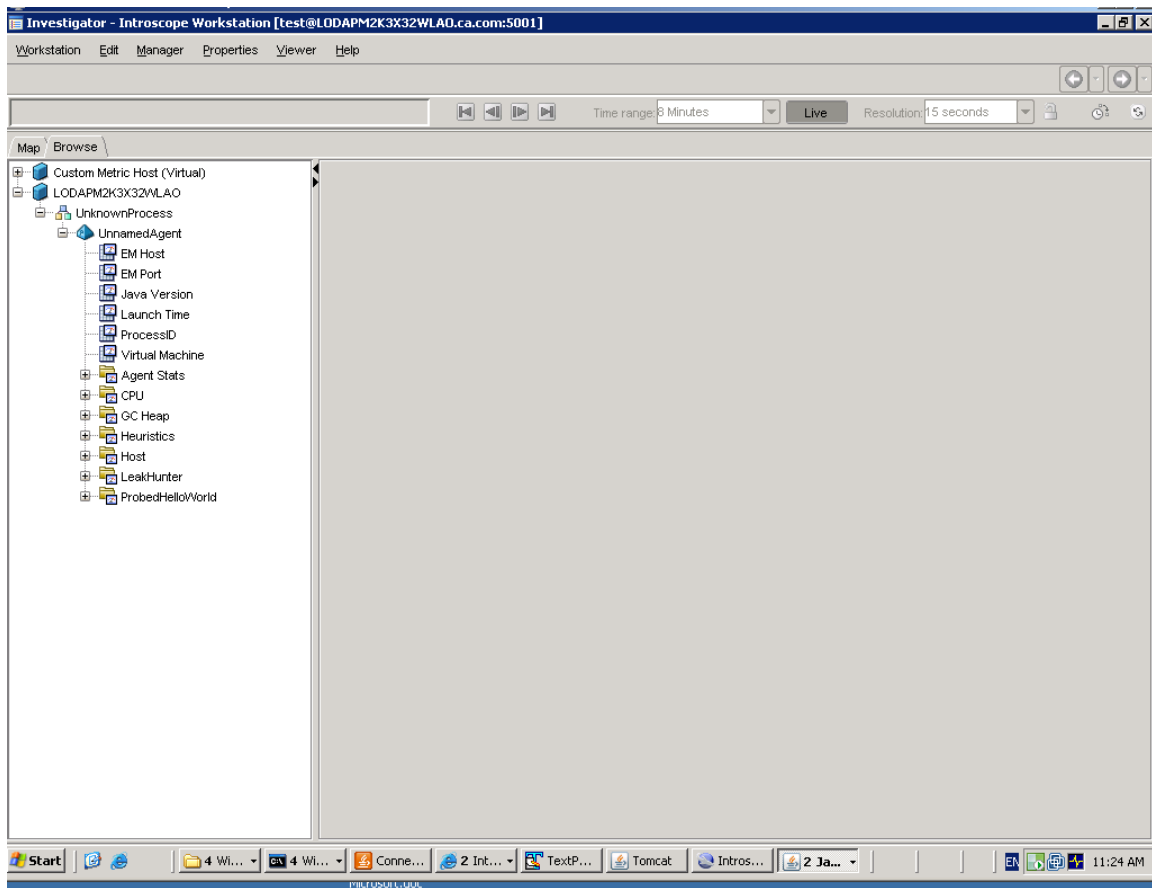
```
<property name="host">
  <value>LODVMEEMSERVER.ca.com</value>
</property>
```

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, login using test user, password=test



Connection successful

In the EM log:

2/16/11 11:21:19.235 AM EST [INFO] [btpool0-2] [Manager.EemRealm] "EEM" realm attached to application "APM" in EEM server at "localhost"

2/16/11 11:21:21.548 AM EST [INFO] [PO:main Mailman 6] [Manager] User "test" logged in successfully from host "Node=Workstation\_0, Address=LODAPM2K3X32WLAO.ca.com/10.130.113.86:2609, Type=socket"