CA EEM Backup and Restore Best Practices

This document applies to CA Embedded Entitlements Manager release r12.x. If you are using EEM 8.4 then you should not use this document.

CA Embedded Entitlements Manager (EEM) can be configured for Server failover which automatically routes requests to a secondary EEM Server when the primary EEM server is not available. However, for this configuration to function properly, an initial connection must first be established with the primary EEM server.

Some applications, such as CA Process Automation (formerly CA IT Process Automation Manager or "CA IT PAM"), CA Service Catalog, CA AutoSys and others, allow multiple EEM servers to be listed. This enables those EEM servers to be rotated if the initial connection is not established, however, for the purposes of Disaster Recovery (DR - or if you want to move an EEM Application to a different server - you will need to backup up the existing EEM Application Instance and restore it onto a new server. This document provides procedures and best practices for performing this action.

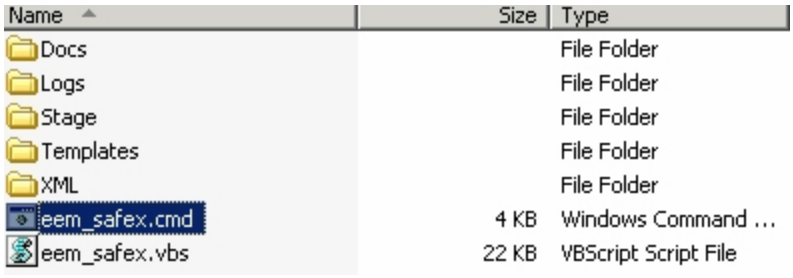
There are several products which do not allow recreating the EEM Application Instance without reconfiguring or in some cases reinstalling it. In addition, you may have carried out extensive EEM changes such as assigning EEM application groups to certain users, updating policies, etc. These would be lost if you recreate application instance. Thus backing up EEM application instances should be included as part of your backup process

Note: The steps outlined in this document only apply to the **backup** and restore of *individual* EEM Application instances. They are **not** designed to handle *multiple* application instances

To backup and restore an EEM Application Instance do the following:

1. Obtain the following information for the EEM Application Instance that is being backed up:
   - Eiam Admin User ID and Password. User defaults to "EiamAdmin" if not specified.
   - EEM Server name. Defaults to your local hostname Application Instance Name.
2. Download the EEM_Export_Import_vx.zip and extract the contents to a folder on your EEM Server.

   Here you can see the contents of the EEM_Export_Import_v4.zip file:



3. Determine if the application instance has a certificate file associated with it.

   CA Process Automation uses a certificate file which is created when the application instance is created. If it does, you must copy that certificate file or generate a new one. For example for CA Process Automation release 4.0, the certificate file is PAM.p12.

   Note: If you are restoring an ITPAM instance to a *different* EEM server, you will have to regenerate this certificate. Please review the "CA Process Automation Certificate" section for details on how to generate this certificate.

4. Execute the eem_safex command to export the EEM instance.

   For example:

   Cd /d <*resourcekit_dir*>

   eem_safex.cmd -mExport -p<*EiamAdmin_password*> -a<*Application_Instance_name*> -e<EEM_servername>

   Here you can see an example of the command results:

```
E:\EEM_Export_Import>eem_safex.cmd -mExport -uEiamAdmin -peiamadminpassword_-aSS
A-SQLVIRTUAL -eDAWYA01C01

%EEMBACK_I_018 Export Started at 12/1/2010 7:54:48 AM

%EEMBACK_I_006 Export completed at 12/1/2010 7:54:56 AM

12/1/2010 7:54:56 AM: Logs\EEM_Export_run.log

Detected EEM Server on host: [DAWYA01C01]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[SSA-SQLVIRTUAL]
OK: action[Export] performed on object[ApplicationInstance] count[1]
OK: action[Export] performed on object[GlobalSettings] count[24]
OK: action[Export] performed on object[Folder] count[5]
OK: action[Export] performed on object[UserGroup] count[5]
OK: action[Export] performed on object[UserGroup] count[0]
OK: action[Export] performed on object[User] count[1]
OK: action[Export] performed on object[Calendar] count[0]
OK: action[Export] performed on object[Policy] count[4]
OK: action[Export] performed on object[AppObject] count[0]
OK: action[Detach] from ApplicationInstance label[SSA-SQLVIRTUAL]
OK: Total objects Added[0]
OK: Total objects Modified[0]
OK: Total objects Removed[0]
OK: Total objects Skipped[0]
OK: Total objects Exported[40]

E:\EEM_Export_Import>_
```

   In this example, the CA Service Operations Insight "SSA-SQLVIRTUAL" will be backed up.

To view the supported syntax for this command execute it using the –h switch. For example:

```
E:\EEM_Export_Import>eem_safex -h
:
: This utility is to Export / Import EEM Application Instance which
: is configured to use External Directory.
:
:
: eem_safex -m(mode) -u(username) -p(password) -a(applicationInstance)
: Required Arguments
:   -m(Export or Import) = Required argument
:   -p(password)  Required parameter
:   -a(ApplicationInstance Name) Required parameter for Export Mode.
:                                Obsolete for Import mode
:
:
:
:   -u(username)       EEM Username - Defaults to EiamAdmin
:   -e(EEM Server) -   Defaults to computername
:   -r(Yes or No)  -   For Import if specified deletes applicaiton instance
:                      prior to import
:   -g(Yes or No)  -   Export Global Settings - External Directory Settings
:                       Defaults to No and only applicable for Export Mode
:   -f(xml fileame) - Optional parameter - If specified overrides the default
:                      xml file name.
:
:
: eem_safex -mExport -uEiamAdmin -pmypassword -aclu-apps10
: eem_safex -mImport -uEiamAdmin -pmypassword -emyDREEMServer
:
E:\EEM_Export_Import>_
```

Important! The specified EEM Application Instance must already exist for the export to work. If it does not, the EEM utility will abend as no validation is performed.

5. To **restore** the Application Instance to a different EEM server, execute the EEM_safex.cmd script using Import mode and point the –e switch to your DR server. For example:

   Cd /d <*resourcekit_dir*>
   eem_safex.cmd -mImport-p<*EiamAdmin_password*> -e<*new_eemservername*> -r<Yes|No>

   Specify –rYes to delete the Application Instance from your new EEM server prior to import. If you specify –rNo or if the –r switch is not specified, the Application Instance will not be deleted prior to import.

```
E:\EEM_Export_Import>eem_safex.cmd -mImport -pdrpassword_-RYes -eDAWYA01SIG

%EEMBACK_I_019 Import Started at 12/1/2010 12:43:52 PM


%EEMBACK_I_020 Removing Application Instance prior to Import at 12/1/2010 12:43:
52 PM


%EEMBACK_I_014 Application instance unregistered.



Setting back end to "DAWYA01SIG"

Setting locale to "en_us"




Detected EEM Server on host: [DAWYA01SIG]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[UnRegister] performed on ApplicationInstance name[SSA-SQLVIRTUAL] wit
h label[SSA-SQLVIRTUAL]
OK: action[Detach] from ApplicationInstance label[]
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]



Setting back end to "DAWYA01SIG"

Setting locale to "en_us"




Detected EEM Server on host: [DAWYA01SIG]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
```

6. If the global settings were also exported (backup), then you need to update the password for the external directory binding as shown in the “Global Settings” section

Global Settings

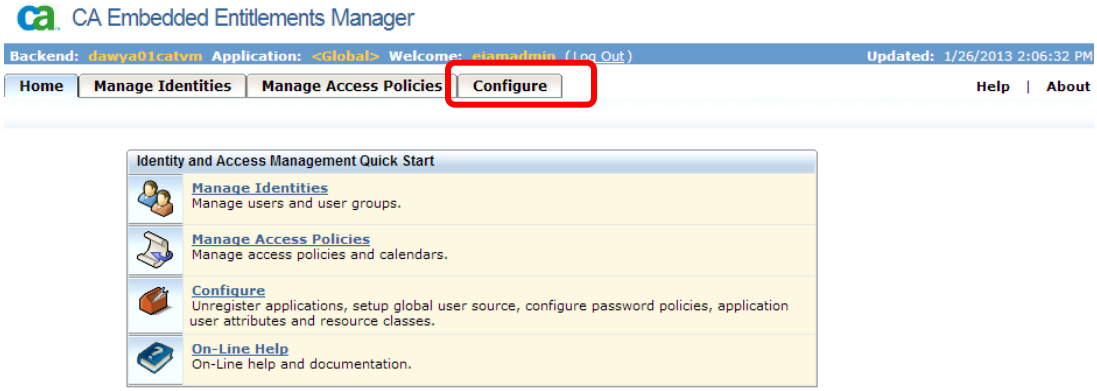
If you wish export your global settings, such as external directory configuration, as well, then set the –g switch to Yes. Note that, for security reasons, the password value will **not** be exported. Therefore, if you set the –g switch to Yes after import (restore) application instance, you must launch the Eiam GUI and set the password for the external directory binding.

To set the password for EEM external directory configuration, do the following:

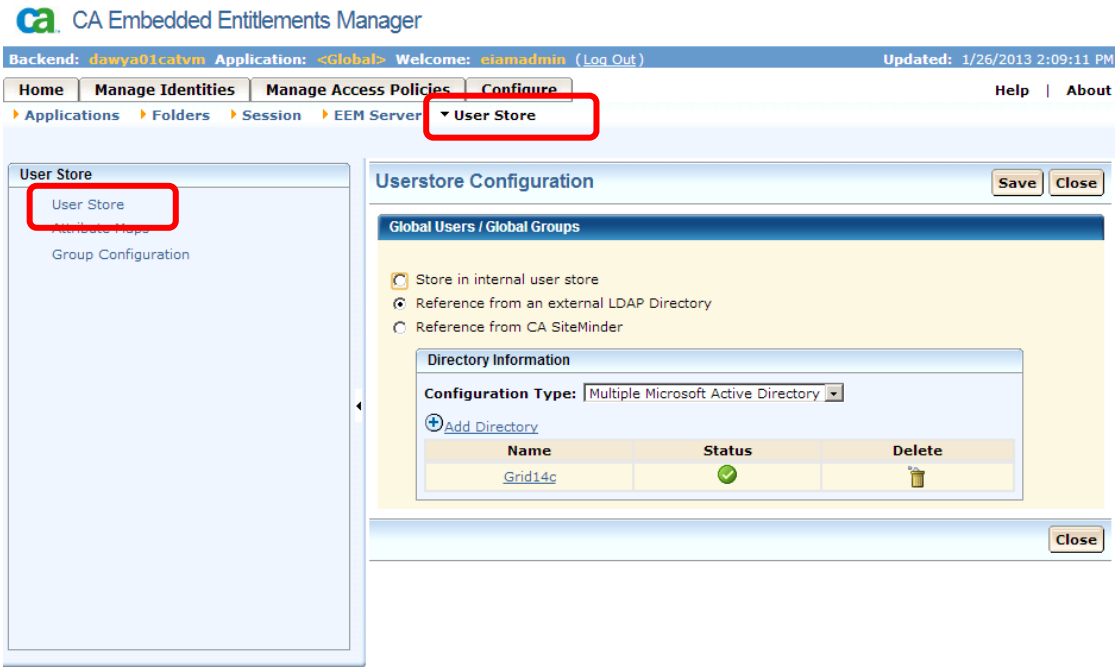
1. Launch the CA EEM UI

   https://localhost:5250/spin/eiam/eiam.csp

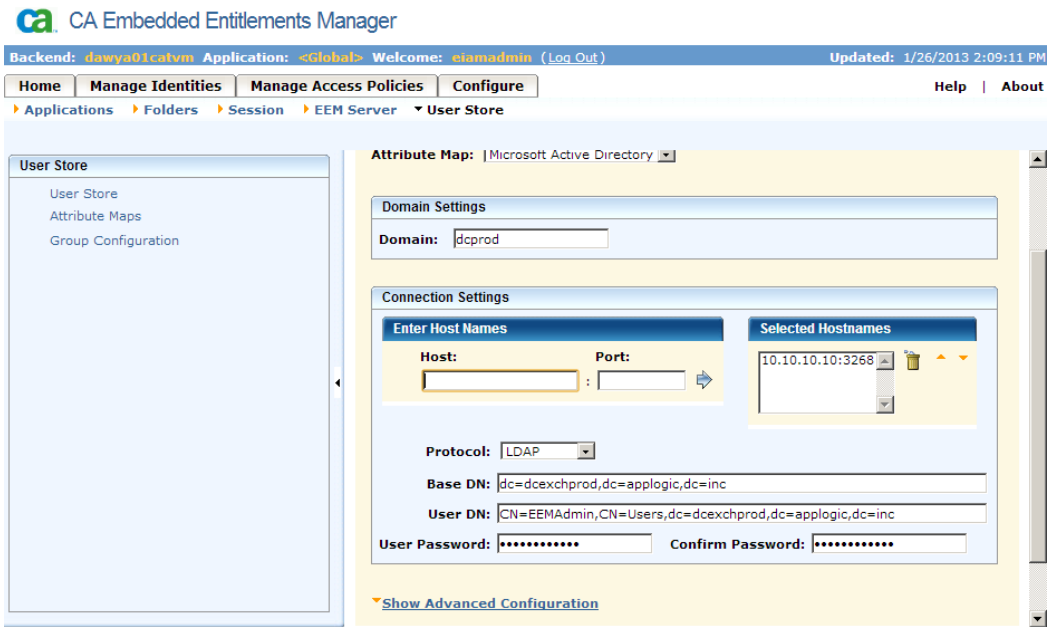
2. Select <Global> application, enter your EiamAdmin password and click **Login**.
3. Select the Configure Tab.



4. Select the “User Store” subtab:
5. Select “User Store” from the right pane.



6. Select “Directory” that had been added. In the above case it is Grid14c



7. Provide the external directory bind password and Click **Save**
8. Verify that the bind was successful

CA Process Automation Certificate

CA Process Automation (formerly, CA IT Process Automation or CA IT PAM) uses certificates for EEM Authentication. The pam.p12 certificate is generated when the "PAM" instance is created and is copied to the EEM ITechnology folder. The CA Process Automation installer also copies file to the following CA Process Automation folder:

```
Program Files\CA\ITPAM\server\c2o\.c2orepository\public\certification
```

If the Application Instance "Process Automation" is being restored to a *different* EEM server, CA Process Automation authentication will fail unless the pam.p12 is regenerated from the new server and copied to the new server's iTechnology folder and the certificate is replaced in the in the CA Process Automation folder (noted above).

Note: The certificate will only be generated when the application instance *is created*. If the "Process Automation" application instance already exists, the certificate it will not be generated.

If you are restoring a "Process Automation" application instance to a different EEM Server you must generate the certificate prior to restoring the "Process Automation" application instance. To generate pam.p12 certificate do the following:

1. Cd to the *EEM_Export_Import* folder
2. Review the Templates\template_itpam_cert.xml file and verify that the certificate file and the password is correct. Since the file lists the dummy password , you must update the password in this template file. The password is what was specified when installing PAM

   Note: The certificate file will be different based on the PAM release. PAM.p12 is for PAM release 4.0
3. Execute the eem_itpam_cert.cmd script. This will display usage information.

```
C:\temp\EEMr12_Export_Import_v4>eem_itpam_cert.cmd -h
:
: This utility is to create IT Pam Certificate file.
: You must run this utility if you intend to restore
: ITPAM application instance to a different EEM Server.
:
: This utility must be run from the EEM server you intend
: to restore the ITPAM applicaiton instance
:
: The certificate file pam.p12 is created in your
:    "C:\temp\EEMr12_Export_Import_v4"
: and should be copied to your iTechnology folder
:
:   "C:\Program Files\CA\SharedComponents\iTechnology\"
:
:
: eem_itapm_cert -u(username) -p(password) -e(EEM ServerName)
:
: Required Arguments
:   -p(password)  Required parameter
:
: Optional Arguments
:
:   -u(username)      EEM Username - Defaults to EiamAdmin
:   -e(EEM Server) -  Defaults to computername
:
: For example
: eem_itpam_cert -uEiamAdmin -pmypassword
:
C:\temp\EEMr12_Export_Import_v4>_
```

Here you can see that the pam/p12 file has been generated by temporarily creating the PAM application instance and then de-registers or deletes it (to allow for clean restore)

```
C:\EEM_Backup_Restore\EEM_Export_Import>eem_itpam_cert -pYD:
Could Not Find C:\EEM_Backup_Restore\EEM_Export_Import\itpamcert.p12
Setting back end to "DAWYA01V64"

Setting locale to "en_us"

Detected EEM Server on host: [DAWYA01V64]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[Register] performed on ApplicationInstance name[ITPAM] with label[ITP
AM]
OK: action[Detach] from ApplicationInstance label[]
OK: action[Attach] with ApplicationInstance label[]
OK: action[UnRegister] performed on ApplicationInstance name[ITPAM] with label[I
TPAM]
OK: action[Detach] from ApplicationInstance label[]
OK: Total objects Added[1]
OK: Total objects Modified[0]
OK: Total objects Removed[1]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]

C:\EEM_Backup_Restore\EEM_Export_Import>_
```

4. Copy the pam.p12 file to your iTechnology folder.
5. Replace your CA Process Automation manager folder pam.p12 file. The default location for this is:

   `C:\Program Files\CA\ITPAM\server\c2o\.c2orepository\public\certification`
6. Restore the PAM application instance

Application Instance Details

Here you can see examples of several Application Instances that were imported from a different EEM Server: