EEM SUPPORTABILITY

Quick Start Reference Guide

This document was created to help provide steps that all Workload Automation AutoSys Edition Scheduler product (WA AE) users and support team members need to know it work with the CA Common Services (CCS) Security application, the CA Embedded Entitlmennts Manager (EEM) facility. The EEM facility is required with the WA AE GUI, called the Workload Control Center (WCC). The WA AE scheduler product itself can also be configured to utilize the same EEM facility used by WCC.

1. Configure EEM to use LDAP, (point to an AD).
   Create a filter to limit AD groups pulled in.
Show use of AS_EEM_AUTHUSER_MODE
3. Creating dynamic user groups
   Adjusting policies using those group
   Setup the env for different levels of access
   Read only user (verses admin)
4. Hide Server from JSC server tab
5. Show certain jobs in JSC
   Use ServerAccess Access Policy
   Create a new policy of type "ServerAccess" and use "Explicit Deny"
   Add users you want to deny access.
6. Manipulate various AUTOSYS and WCC EEM policies.
   Restrict job access via as-job
   Create objectaccess policies to filter jobs

This document assumes that WA AE, WCC and EEM faiclities have been installed and are available.

I. Determine EEM Version

To **confirm** which version of EEM SDK (Safe.jar) the WCC server is using then unzip the <WCC>\CommonLib\Safe.jar and view the META-INF/MANIFEST.MF file and it will indicate which version of EEM SDK is inside, ie:

I. Ex: Specification-Version: 8.3.0.122
II. Ex: Specification-Version: 8.4.406

This information is important to know, and will be referenced below.

II. Import/Export Policies

In order to export EEM policies and settings using safex, you have to create a file with commands that tells safex to export.
Once the export command file is created, you will then use safex and the import function on the export command file.
First Need to verify/modify the "**eiam.xml**" file to indicate to WCC which available version of EEM (if more than one) it should use.

Command to import:
safex -h (EEM SERVER) -u EiamAdmin -p (EiamAdmin Password) -f (Import file or export command file)

A. Safex Export Command File samples:
(All samples are outputted to a folder /tmp on UNIX, and C:\TEMP\ for Windows)
1. UNIX\LINUX – WorkloadAutomationAE 11.3 Sample

```
<Safex>
<Attach label="WorkloadAutomationAE"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you store the global users and global groups in CA's Management Database (CA-MDB) all the objects are exported.
You can override the maximum number of items that are returned by the backend server. The default is 2000. To change the maximum number of items to return, include the maxsearchsize="Value" -->

<Export file="/tmp/WorkloadAutomationAE_EEM_Export.txt" globalfolders="y" globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y" users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

2. UNIX\LINUX – WCC 11.3 Sample

```
<Safex>
<Attach label="WCC0003"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you store the global users and global groups in CA's Management Database (CA-MDB) all the objects are exported.
You can override the maximum number of items that are returned by the backend server. The default is 2000. To change the maximum number of items to return, include the maxsearchsize="Value" -->

<Export file="/tmp/WCC0003_EEM_Export.txt" globalfolders="y" globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y" users="y" calendars="y" policies="y" appobjects="y"/>
```

```
<Detach/>
</Safex>
```

3. UNIX\LINUX – AutoSys 11.0 Sample

```
<Safex>
<Attach label="UnicenterAutoSysJM"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->

<Export file="/tmp/UnicenterAutoSysJM_EEM_Export.txt" globalfolders="y"
globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y"
users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

4. UNIX\LINUX – WCC 11.1 Sample

```
<Safex>
<Attach label="WCC0002"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->

<Export file="/tmp/WCC0002_EEM_Export.txt" globalfolders="y" globalusergroups="y"
globalusers="y" globalsettings="y" folders="y" usergroups="y" users="y" calendars="y"
policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

5. WINDOWS – WorkloadAutomationAE 11.3 Sample

```
<Safex>
<Attach label="WorkloadAutomationAE"/>
```

```
<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->

<Export file="C:\TEMP\WorkloadAutomationAE_EEM_Export.txt" globalfolders="y"
globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y"
users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

6. WINDOWS – WCC 11.3 Sample

```
<Safex>
<Attach label="WCC0003"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->

<Export file=" C:\TEMP\WCC0003_EEM_Export.txt" globalfolders="y"
globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y"
users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

7. WINDOWS – AutoSys 11.0 Sample

```
<Safex>
<Attach label="UnicenterAutoSysJM"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->
```

```
<Export file=" C:\TEMP\UnicenterAutoSysJM_EEM_Export.txt" globalfolders="y"
globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y"
users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

8. WINDOWS – WCC 11.1 Sample

```
<Safex>
<Attach label="WCC0002"/>

<!-- You can control the data to be exported by specifying the Yes(Y) or No(N). If you
store the global users and global groups in CA's Management Database (CA-MDB) all the
objects are exported.
You can override the maximum number of items that are returned by the backend
server. The default is 2000. To change the maximum number of items to return, include
the maxsearchsize="Value" -->

<Export file=" C:\TEMP\WCC0002_EEM_Export.txt" globalfolders="y"
globalusergroups="y" globalusers="y" globalsettings="y" folders="y" usergroups="y"
users="y" calendars="y" policies="y" appobjects="y"/>

<Detach/>
</Safex>
```

B. Safex Import of Exported EEM polices to an EEM server:

Command:
safex -h (EEM SERVER) -u EiamAdmin -p (PASSWORD) -f (filesname)

C. Export WCC policies from EEM

a. Log in to EEM under the WCC0001 application.
b. Go to the Configure tab -> Embedded IAM Server -> Export Application
c. Select all except "Override The Max Search Size"
d. Click Export and save to a file

II. Register WCC with EEM

First Need to verify/modify the "**eiam.xml**" file to indicate to WCC which available version of EEM (if more than one) it should use.

To register CA WCC with CA EEM and to issue the certificate is as follows:

Restart the CA WCC server when the CA WCC installation is complete.

Open a Command Prompt window and change to the following directory:
%CA_WCC_INSTALL_LOCATION%\safex

Run the following command:
safex -h EEM_server_host_name -u EiamAdmin -p EiamAdmin_password -f UWCCRegister.xml

Note: The values of EEM_server_host_name and EiamAdmin_password should be the same values you entered on the EEM Server panel when you installed CA WCC; however, you need to enter only the value for the active CA EEM server if you originally entered a list of CA EEM servers.

CA WCC is registered with CA EEM and the CA EEM policies are uploaded.

Run the following command:
safex -h EEM_server_host_name -u EiamAdmin -p EiamAdmin_password -f IssueCertificate.xml

The certificate for authentication of CA WCC on the CA EEM server is created at %CA_WCC_INSTALL_LOCATION%\safex. The file name is uwcc-cert.p12.

Copy the uwcc-cert.p12 file to the following directory:
%CA_WCC_INSTALL_LOCATION%\ConfigServer\config

Restart the EEM and WCC servers

III. Configure EEM to use LDAP

IV. Create Dynamic User Groups

V. Restrict jobs viewable by a specific user

There are three procedures needed to restrict the set of jobs viewable by a specified user ID on the WCC R11.1 facility. Each procedure is noted below.

A. Steps to display only the jobs (job editor) you want the client to see.

1. Make sure in WCC that the autosys server is defined to UWCC with Filter Object enabled.
2. Logout of UWCC.
3. Login to EEM using WCC000* Application.
4. Go to "Manage Access Policies"
5. Go to "Access Policies" --> "ObjectAccess"
6. Open "ObjectAccessDefault" and save as "EXAMPLE"
7. Open "ObjectAccessDefault" and check off the disable button.
8. Open "Example" and add the user you want to see jobs that start with PopCorn. Ex. PopCorn_isYummy
9. Remove the other identities from the user list.
10. Remove the */Job/* Resource.
11. Add the job you only want this user to see */Job/PopCorn*
12. Click SAVE and perform a Sync Push
13. Login to WCC and this user should only see jobs that start with PopCorn.

B. Steps to create JSC views that only show jobs you want users to see

1- Created a new view to display jobs which were only to be accesses by group TEAM. i.e jobs starting with TEAM*. To create the View performed these steps.
- logged into UWCC
- clicked on JSC
- click on "configuration" from the sublink
- enter a new configuration name i.e TEAM-ONLY
- once created then click on "filter" from the sublink and select "add" button to create a new filter
- entries in the feilds
  name: TEAM-ONLY
  Server: servername
  job: TEAM*(to filter all jobs starting with the letters TEAM)
- click on ok to save
- uncheck the checkbox for the default view and check the box for the new filter created
- then click on "update" to update the view.
- click on "configuration again and resave the "TEAM-ONLY" configuration that was created earlier.

2- Logout and log back into UWCC and access the newly created view and confirm that the view only displays the jobs that this group\user is supposed to view.

C. Create EEM Policy for MonitorControl Access

1- Login to EEM
2- Open "manage access policies"
3- Next open "MonitorViewControl"
4- Define a new policy

5- In identities select the user\group for which the policy needs to be implemented
6- In resource select the options to allow users the capability to perform.
7- for the resource name add "view/TEST-ONLY*"
8- Save the policy
Need to change to:
9. Create New “Deny” policy”
10. Add User\group to deny access
VERSES:
9- Next open "ServerAccess" policy
10- Again, add the user\group
11- in Resource leave the default of "server/*"
12- Next click on "filters"
13- Enter the following in the fields,
logic: NONE
- Named Attribute
- Component
- String
- NOTEQUAL !=
- value
- JobStatusConsole

At this point, the facility has finished needed configurations.
Save the policy, then click on config - >sessions and then click on
Synchronize Cache
Synchronize Push

Now to test the policies logout from UWCC and log in with a userid that is
a member of the TEAM group, once connected you should only see TEAM-ONLY view
in the job status console views. Next open JSC and you should not see any
listed servers. Next click on view and you should only see TEAM-ONLY view
listed and when selected it should only display the jobs for which the
group\user has access to view.

V. Set Read Only Access for a User or Group (for WCC 11.1)

To make a user or group have read only access we need to update eem to block ceratin users/groups from running a sendevents. To do this, perform the following steps:

Open EEM, and login under WCC.
Go to Manage Access Policies.
Select "JobActionAutoSys"
Select "JobActionAutoSysDefault"
Select "Save As" and give it a name.
Now check off "Explicit Deny" and click save.

Click on "Identity Access Control List"
Enter the identity you would like to block.
Search for the user and select it from the box and press the down arrow.
Remove the following users from your current list of identities in your
new Explicit Deny: Commander, ConsoleOperator, Scheduler, Supervisor,
Do this so all you see is your newly added user.
Make sure none of the default boxes are checked off and check the boxes
of the actions you would like to block the user from doing.
Click save and logout and login to WCC and that users actions will be blocked.

Notes:
You can add more users to this new Explicit Deny.
Make sure in WCC you have filters turned on and EEM turned on, under the "Configuration Manager, Servers, then select the server.

Your user/group should now, not be able to run sendevents if you checked the sendevent box.

V. Enabling logging in EEM SDK

Applicable for : EEM 8.4 SR02 onwards.

Note: For C# Sdk, applicable from 8.4 SP03 onwards.

For enabling EEM SDK logging, make sure that the application which is using EEM SDK is installed on the machine on which the logging is to be performed.

For the Windows Platform, here are the steps to enable EEM java\cpp\c# SDK logging in trace mode:

1. Set EIAMCONFIG to absolute path to eiam.config file. (eiam.config , eiam.log4j.config, eiam.log4cxx.config & eiam.log4net.config shipped with EEM SDK)

Eg: set EIAMCONFIG=c:\casupport\eiam.config

2. Verify if the EIAMCONFIG is set correctly by checking the same by opening a new command prompt. In the new command prompt execute - echo % EIAMCONFIG%.

3. Edit eiam.config and put absolute path of eiam.log4j.config file for Java , eiam.log4cxx.config file for CPP & eiam.log4net.config for .Net\C# SDK.

Eg: <LoggerConfiguration file="c:\casupport\eiam.log4j.config"/>

4. Change log level from "error" to "trace" in eiam.log4<SDKType>.config file. Here SDKType = cpp or java or c#

Eg: <root> <priority value="trace" />

5. Restart application which is using EEMJava/cpp/c# SDK.

6. Check if the eiam.(cpp\java\c#)sdk.log is being generated.

7. Once the eiam.< SDKType >sdk.log is being generated, the EEMSDK logging is enabled properly.

8. Replicate the problem and save the eiam.< SDKType >sdk.log file, this file should be send across for further investigation.