Using CA Identity Manager Bulk Loader Client (BLC) with SiteMinder Authentication & SSL Configuration

Alan Baugher
CA Sr. Principal Architect

Nov 2015

Agenda

- Background / Steps
- Configuration
- Validation
- Troubleshooting Processes
- References

BLC Background

- The CA Identity Manager Bulk Loader Client (BLC) is a pre-built java module to call the CA Identity Manager Task labeled as “ObjectFeeder” with the friendly business name of “Bulk Loader”
- This “Bulk Loader aka ObjectFeeder” task is exposed through the Identity Manager TEWS.
  - When IM TEWS is enabled, this will allow a remote client to communicate via authentication to select Identity Manager Tasks, that have the “checkbox” for Web Service enabled.
- The BLC may be configured in four (4) way(s) for authentication:
  - No authentication, UserID only. {Fine for testing; Not for production environments}
  - UserID/Password via IMCD Userstore (J2EE or via Web Server redirect to J2EE)
  - UserID/Password via SM Authentication (via IMCD Userstore) & SM WebAgent on Web Server
  - UserID with WSS (Web Services Security) {when using other Web Security Solutions}
- The BLC URL should be the protected URI for the IME to avoid security exposure by using an anonymous bind to submit requests/updates to the IME
- Recommend a new userID, for SOD business requirements, be used for the BLC Feed process, e.g. idmfeed.
  - This ID only has access to a single IM Admin Task, e.g. “Bulk Loader aka ObjectFeeder” via a new IM Admin Role “IM Feed”
  - Create the new IM Admin Role “IM Feed” and assign the “Bulk Loader” IM Admin Task & the IM User “idmfeed”
  - Rotate the password for “idmfeed” as needed; update the BLC as needed.
- Use more than one (1) BLC, to speed up processing to multiple J2EE servers (directly) or via a Web Server Farm.
  - Use Pentaho / Spoon to pre-identify the use-cases for new, modify, rename, suspend, terminate, etc. & assign them unique actions.

Process / Methodology

Goal: Validate IM/SM bookshelf notes & TECH Note: TEC560908

For deployment / configuration of IM BLC with Siteminder (SM/SSO) & use of SSL for secure communication.

1) Deploy BLC with no SM auth nor SSL enabled within Web Server (redirected to J2EE tier)
   a. No issues with bookshelf notes.
   b. Clarified steps for password reset after installation {to address business requirements that service account password must rotate on a bi-annual basis}
2) Deploy BLC with no SM auth but with SSL enabled within Web Server (redirected to J2EE tier)
   a. Clarified issue with SSL tokens required to be set for Web Server configuration; to ensure SSL certs were passed correctly.
   b. Used SM bookshelf for clarification with Apache Web Server
3) Deployed BLC with SM auth and no SSL enabled Web Server (redirected to J2EE tier)
   a. Clarified steps on which checkboxes to enable or disable on the IME Advance Settings Page
   b. Use XPSExport to capture pre & post states of SM enabled objects for IM TEWS
   c. Identified gap with re-enablement of SM Auth & how to resolve
4) Deployed BLC with SM auth & SSL enabled Web Server (redirected to J2EE tier)
   a. No issues after resolving the prior test cases

Bulk Loader CheckList - TEC560908

1. Enable Web Services within your environment via IM Management Console for IME/Advance Settings/WebServices/ Enable Web Service checkbox.
2. Enable Web Services for "Bulk Loader" admin task within the IM User Console (IME) / Role&Tasks/AdminTasks/ModifyAdminTasks/ModifyBulkLoaderAdminTask/ Enable Web Service checkbox.
   - Ensure the “Bulk Loader” IM Task is assigned to an IM Admin Role (System Manager or new Role) & the BLC userID (idmfeed or idmadmin) is associated with the new IM Admin Role
3. ~~Enable Web Services for any task which is to be performed (i.e "Bulk Create User", "Bulk Modify User" etc.) within the IM User Console (IME)~~ [Not required for BLC; only ObjectFeeder Task]
4. Ensure fields are identical (case wise) in both CSV and imbulkloadclient.properties -
   If you are using IM 12.5 SP9 or later - ensure you are using Task **tags** in "actionToTaskMapping" field [Older release used Task Names, which had spaces]

   For example: actionToTaskMapping=create.CreateUser;modify.ModifyUser;delete.DeleteUser

5. Make sure actionToTaskMapping contains correct mapping (of existing tasks) for all action types.
   Note: Incorrect task, even if not used in the CSV you are trying to process, will fail the validation and therefore the entire Bulk Load process.

6. Verify the same CSV file can be used with the Bulk Loader Admin Task from Identity Manager
7. Special instructions for using Bulk Loader in a tokenized environment:

   If you are using IM 12.5 SP9 or later with a tokenized environment - you must be using Task **tags** in "actionToTaskMapping" field

   For example: actionToTaskMapping=create.CreateUser;modify.ModifyUser;delete.DeleteUser

8. Special instructions for using Bulk Loader with SiteMinder Authentication:
9. Make sure Identity Manager is functioning correctly with SiteMinder protecting it. Establish a normal login to Identity Manager UI using the browser through the web server port (rather than the usual application server port). If basic integration doesn't work, make sure you fix this before moving forwards with using TEWS and bulk loader client.

   Set the isProtectedBySiteMinder variable in the imbulkloadclient.properties file to true. [This will create IM TEWS6 related objects in SM objectstore]

   Set the serverURL variable in the imbulkloadclient.properties file to reflect the web server port rather than the application server port.

   Make sure that the SiteMinder user being used for the admin_id is valid and not locked out or disabled

10. Update Web Services configuration via the Management console Home / Environments / <YOUR_ENVIRONMENT> / Advanced Settings / Web Services to use the **Basic Authentication** for Site Minder. [Ensure “Admin Password is required” checkbox **NOT** enabled]

11. Verify SiteMinder domain includes: TEWS realm (protected by same agent as Identity Manager), TEWS rule, TEWS policy (ensure that users tab have users that can authenticate and the rules tab has both realm and rule associated).

12. Use SiteMinder Test Tool (from SM SDK) to test the connectivity, protection, authentication and authorization for the /idm/TEWS6/<IMEName> realm.
    1. http://www.ca.com/us/support/ca-support-online/product-content/status/release-notes/using-the-siteminder-test-tool-sm-test.aspx
    2. https://support.ca.com/cadocs/0/CA%20SiteMinder%2012%2052-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?347394.html

How to run BLC on LINUX

1. Install & extract the Windows or Solaris Build of BLC
2. Copy the extracted files and folders (jar files) to a folder on Linux
3. Extract the shell script from Solaris build.
4. Update the shell script to reflect Linux environment, shell, & paths
5. Update the shell script with extra mail.jar file from IAMSuite Tools / Workflow Client / Lib folder
6. Update properties file to current URL, ID, Password, use of SM.
7. Update JDK keystore if SSL is to be used.
8. Create a feed.csv file and validate load.

blc.sh

```
#!/bin/sh
DIRNAME=`dirname $0`
cd "$DIRNAME"
TRUSTSTORE="/opt/CA/blc/bin/imblc.ks"
TRUSTSTORE_PASSWORD=changeit
JAVA_HOME=/opt/CA/jdk/jdk1.7.0_71_x64
PATH=$PATH:$JAVA_HOME/bin

if [ -x ../_uninst/_jvm/bin/java ]; then
  ../_uninst/_jvm/bin/java -mx1024m -Djava.util.logging.config.file=../conf/imbulkloadclient_logging.pro
perties -Djavax.net.ssl.trustStore="$TRUSTSTORE" -
Djavax.net.ssl.trustStorePassword="$TRUSTSTORE_PASSWOR
D" -Dcom.ca.commons.logging.nolog4j=true -cp ".:../conf:../lib/mail.jar:../lib/imbulkloadclient.jar" com
.ca.iam.imbulkloadclient.IMBulkLoadClientApp $*
else
  java -mx1024m -Djava.util.logging.config.file=../conf/imbulkloadclient_logging.properties -Djavax.net.
ssl.trustStore="$TRUSTSTORE" -Djavax.net.ssl.trustStorePassword="$TRUSTSTORE_PASSWORD" -
Dcom.ca.commons.
logging.nolog4j=true -cp ".:../conf:../lib/mail.jar:../lib/imbulkloadclient.jar" com.ca.iam.imbulkloadcl
ient.IMBulkLoadClientApp $*
fi
```

blc_example.sh

```
#!/bin/bash
/opt/CA/blc/bin/blc.sh -v -f CSV -i /opt/CA/blc/bin/feed.csv
```

blc_change_password.sh

```
#!/bin/bash
/opt/CA/blc/bin/blc.sh --storeEndpointInfo --endpointInfoFile imblc_pwd_reset_input_file.txt
```

imblc_pwd_reset_input_file.txt

```
# Select the Inputs to be convert or copied to the properties file
# User and serverURL may be skipped for updates
# Password is clear text; and will be hashed (Crypt)
#
#user=idmadmin
password=Password01
#serverUrl=https://imwa001.im.dom/iam/im/TEWS6/cam
```

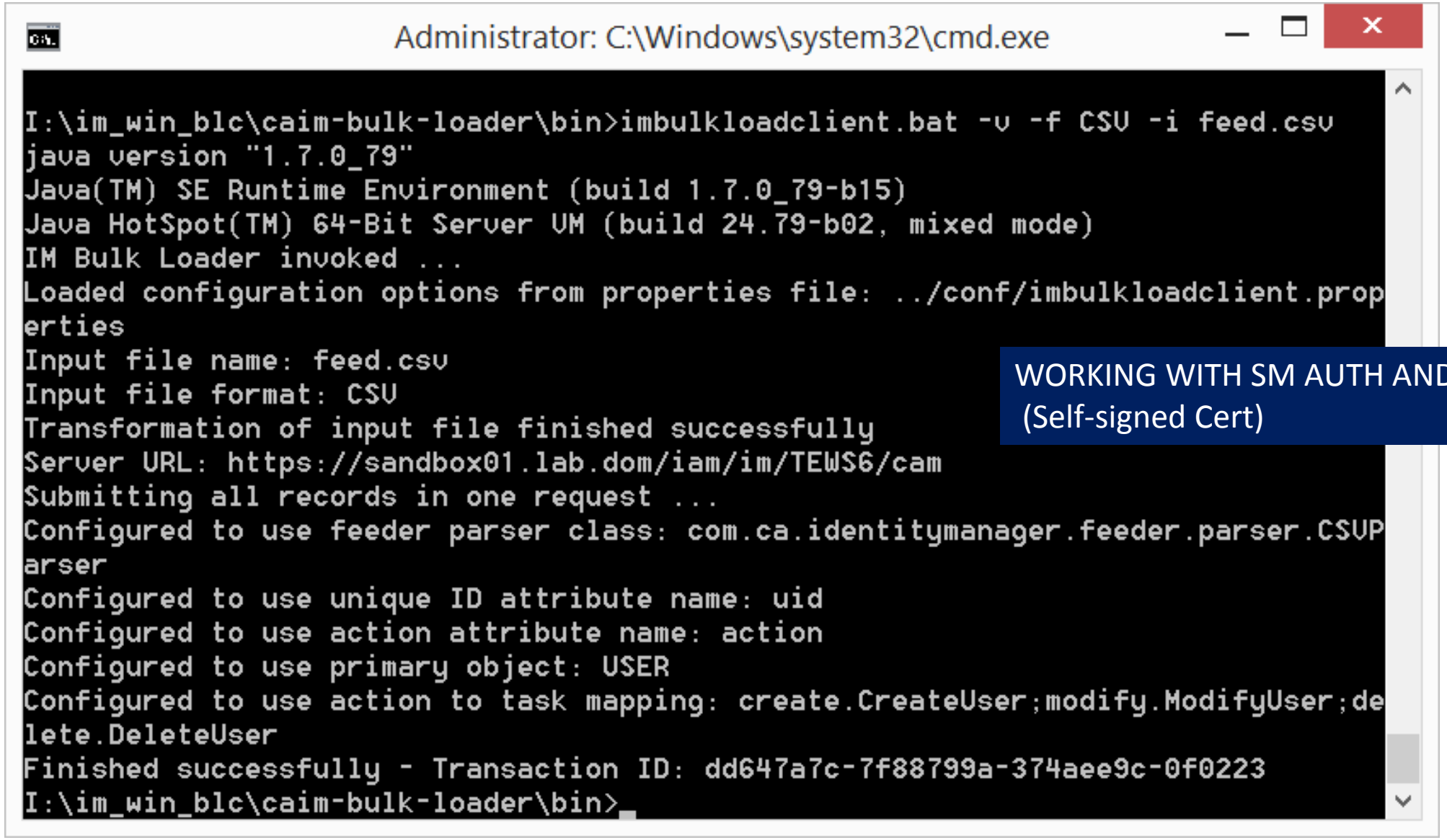
feed.csv

```
action, uid, %FIRST_NAME%, %LAST_NAME%,%FULL_NAME%,%ORG_MEMBERSHIP%
create, bob02, bob, bob01, bob01 bob01,"ou=people,ou=cam,o=ca"
```

imbulkloadclient.properties

```
#serverUrl=https\://sandbox01.lab.dom/iam/im/TEWS6/cam?wsdl
serverUrl=http\://sandbox01.lab.dom:48080/iam/im/TEWS6/cam?wsdl
uniqueIdentifierAttrName=uid
actionToTaskMapping=create.CreateUser;modify.ModifyUser;delete.DeleteUser
primaryObject=USER
user=idmadmin
feederParserClass=com.ca.identitymanager.feeder.parser.CSVParser
actionAttrName=action
isProtectedBySiteMinder=true
password=devrhQ2YEm5RE0IGa3tyoPkiTOe0uYNpgjS1Zlsz9B8\=
```

Test IM BLC with SM + SSL

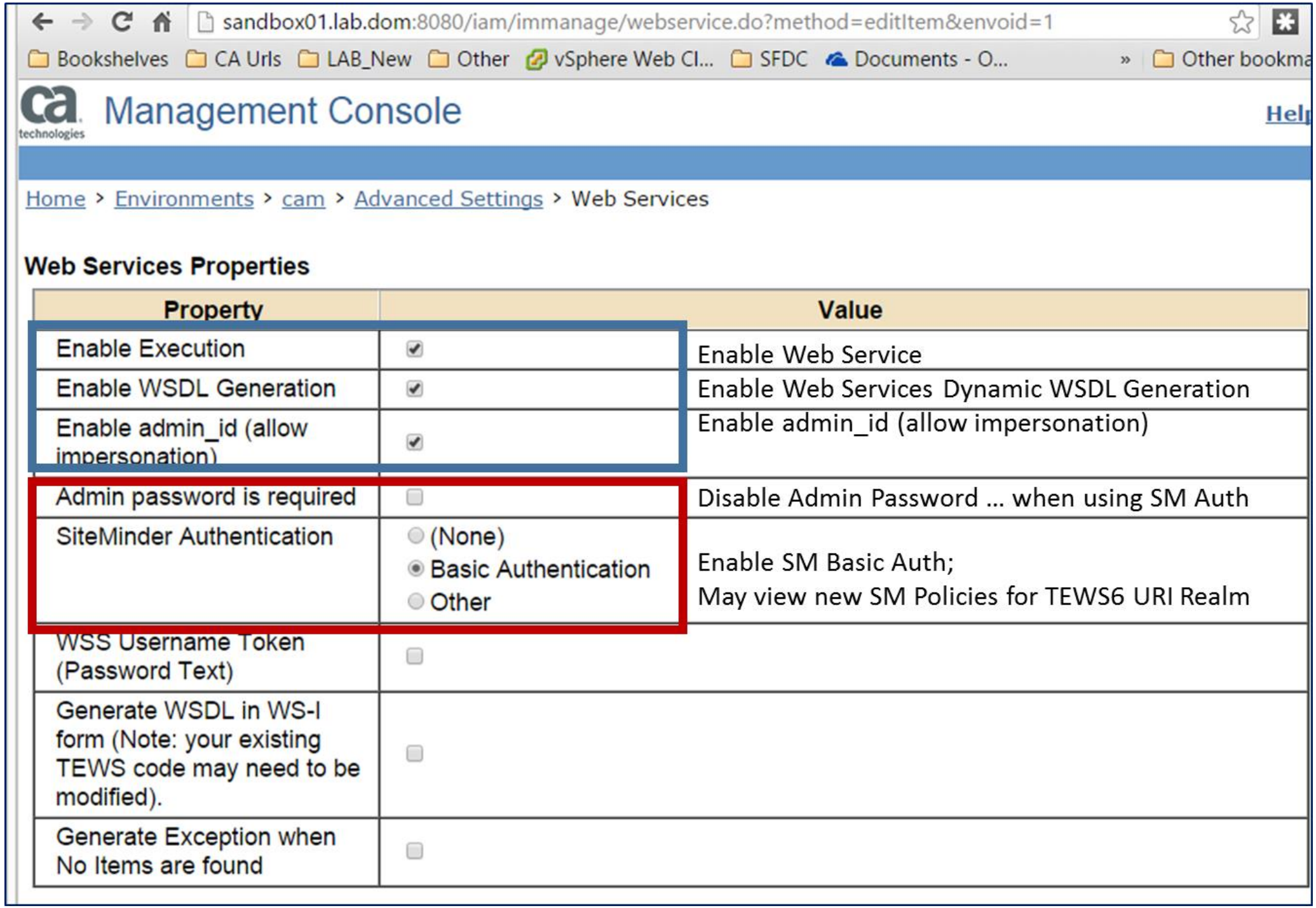


WORKING WITH SM AUTH AND SSL
(Self-signed Cert)

Additional and Supporting Notes

The below slides may be considered as support notes, with regards to capture of error messages, troubleshooting steps, and ssl configurations.

Enable SiteMinder Basic Authentication For IM TEWS


sandbox01.lab.dom:8080/iam/immanage/webservice.do?method=editItem&envoid=1
Bookshelves
CA Urls
LAB_New
Other
vSphere Web Cl...
SFDC
Documents - O...
Other bookma
Management Console
Help
Home > Environments > cam > Advanced Settings > Web Services
Web Services Properties
Property
Value
Enable Execution
Enable Web Service
Enable WSDL Generation
Enable Web Services Dynamic WSDL Generation
Enable admin_id (allow impersonation)
Enable admin_id (allow impersonation)
Admin password is required
Disable Admin Password ... when using SM Auth
SiteMinder Authentication
(None)
Basic Authentication
Other
Enable SM Basic Auth;
May view new SM Policies for TEWS6 URI Realm
WSS Username Token (Password Text)
Generate WSDL in WS-I form (Note: your existing TEWS code may need to be modified).
Generate Exception when No Items are found

Enable admin_id (allow impersonation)

Specifies whether TEWS supports impersonation.

When this option is selected, TEWS uses the admin ID found in the SOAP message sent to the web service to authenticate the request.

When this option is not selected, the ID of the user who generated the request is used to authenticate the request.

This option is ignored when using WSS authentication.

Admin password is required [Needs to be disabled for SM AUTH]

Specifies that CA Identity Manager obtains the admin ID from the session information to determine whether the administrator is authorized to perform the task.

This field is ignored when using WSS authentication.

SiteMinder Authentication

When CA Identity Manager integrates with SiteMinder, you can configure SiteMinder to secure the URL for web services.

- **None (default)**

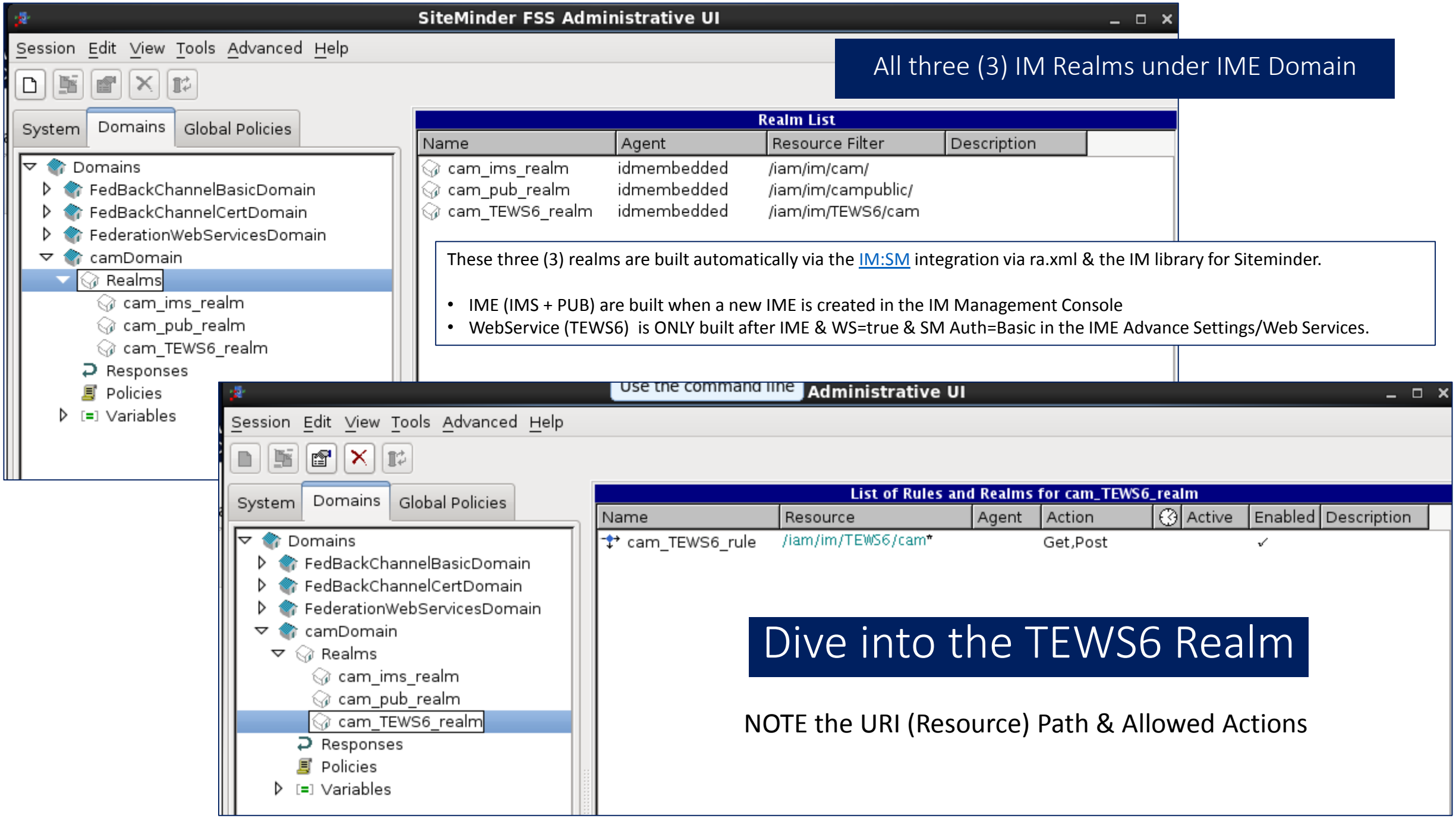
  SiteMinder does not secure the web services URL. In this case, use an external method to secure the web services URL.

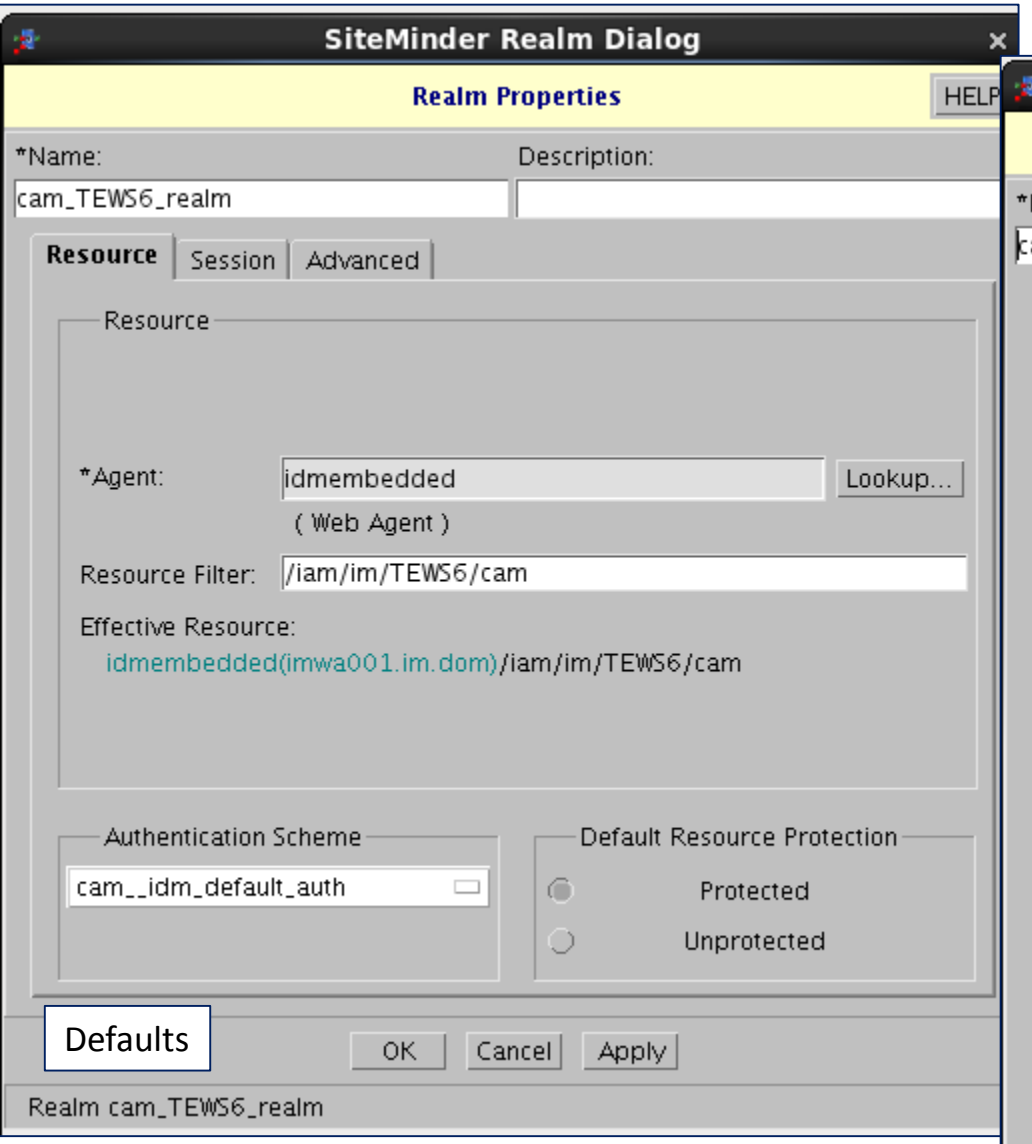
- **Basic Authentication**

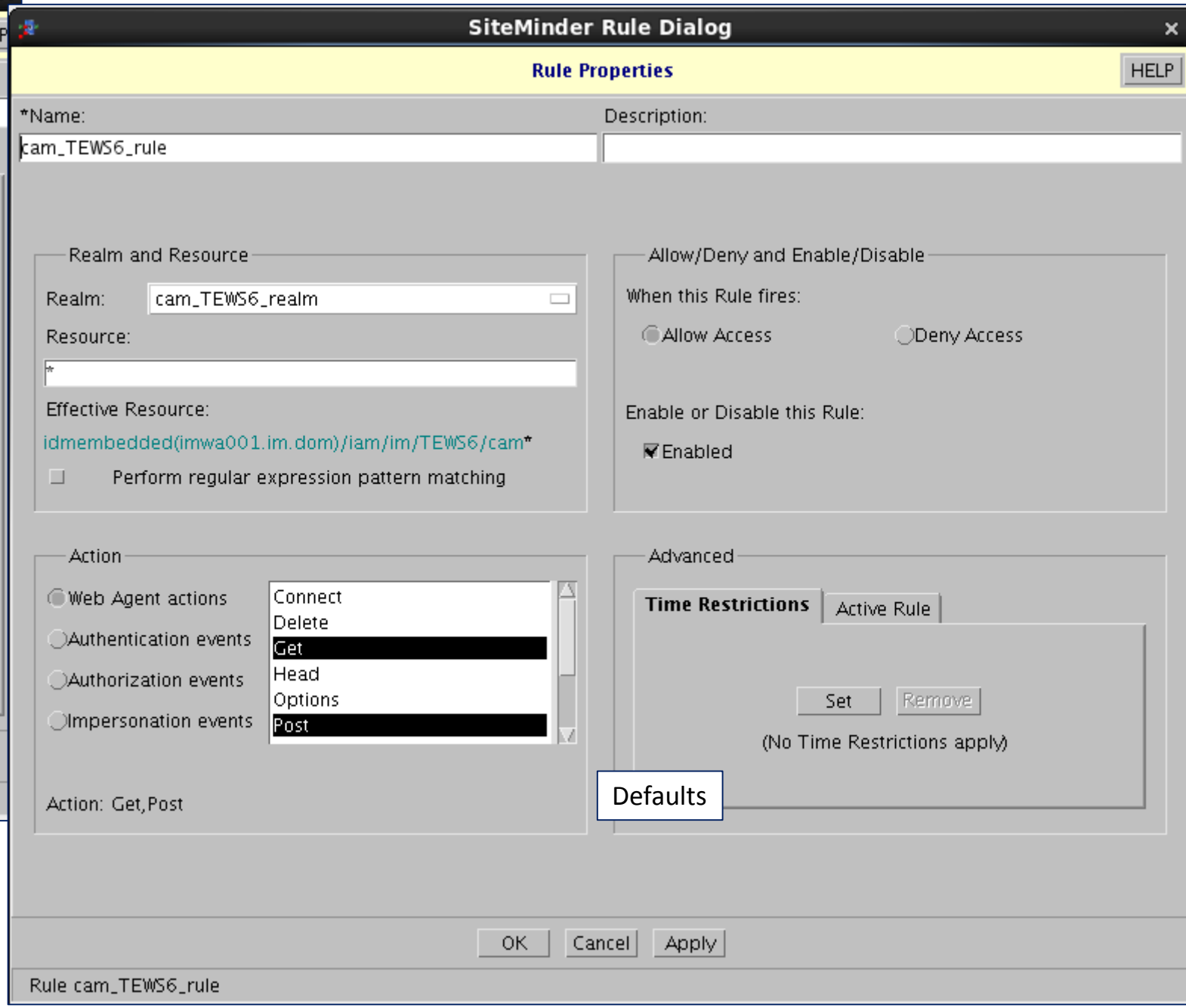
  SiteMinder basic authentication secures access to the web services URL.

  When selected, CA Identity Manager automatically creates the authentication schemes, domain, realm, rule, and policies that are required to secure the URL for web services. You can modify these configuration settings in the SiteMinder Policy Server user interface.

A View of SiteMinder Objects Added when TEWS is enabled for SM Basic Authentication

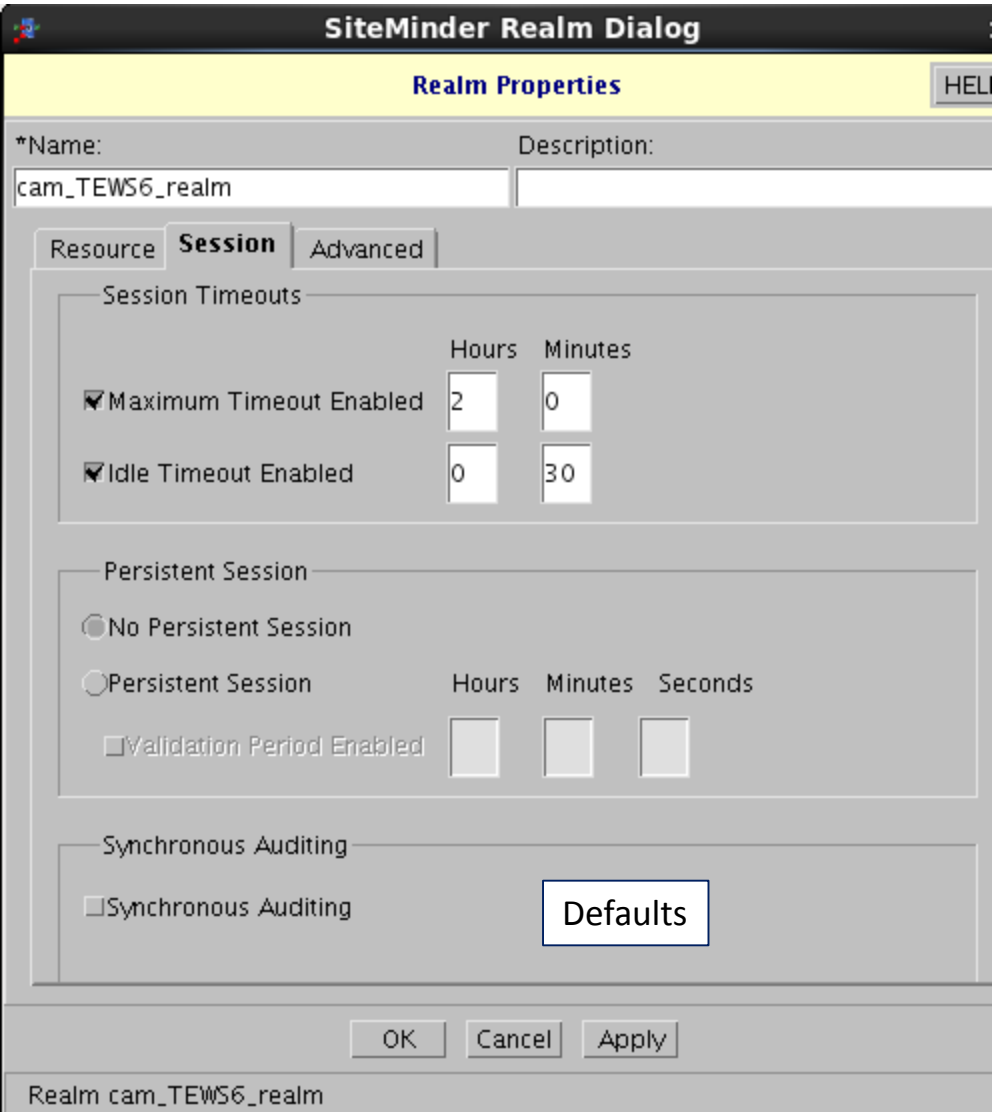

SiteMinder FSS Administrative UI
Session Edit View Tools Advanced Help
System Domains Global Policies
Domains
FedBackChannelBasicDomain
FedBackChannelCertDomain
FederationWebServicesDomain
camDomain
Realms
cam_ims_realm
cam_pub_realm
cam_TEWS6_realm
Responses
Policies
Variables
All three (3) IM Realms under IME Domain
Realm List
Name Agent Resource Filter Description
cam_ims_realm idmembedded /iam/im/cam/
cam_pub_realm idmembedded /iam/im/campublic/
cam_TEWS6_realm idmembedded /iam/im/TEWS6/cam
These three (3) realms are built automatically via the IM:SM integration via ra.xml & the IM library for Siteminder.
• IME (IMS + PUB) are built when a new IME is created in the IM Management Console
• WebService (TEWS6) is ONLY built after IME & WS=true & SM Auth=Basic in the IME Advance Settings/Web Services.
Use the command line
Administrative UI
Session Edit View Tools Advanced Help
System Domains Global Policies
Domains
FedBackChannelBasicDomain
FedBackChannelCertDomain
FederationWebServicesDomain
camDomain
Realms
cam_ims_realm
cam_pub_realm
cam_TEWS6_realm
Responses
Policies
Variables
List of Rules and Realms for cam_TEWS6_realm
Name Resource Agent Action Active Enabled Description
cam_TEWS6_rule /iam/im/TEWS6/cam* Get,Post ✓
Dive into the TEWS6 Realm
NOTE the URI (Resource) Path & Allowed Actions

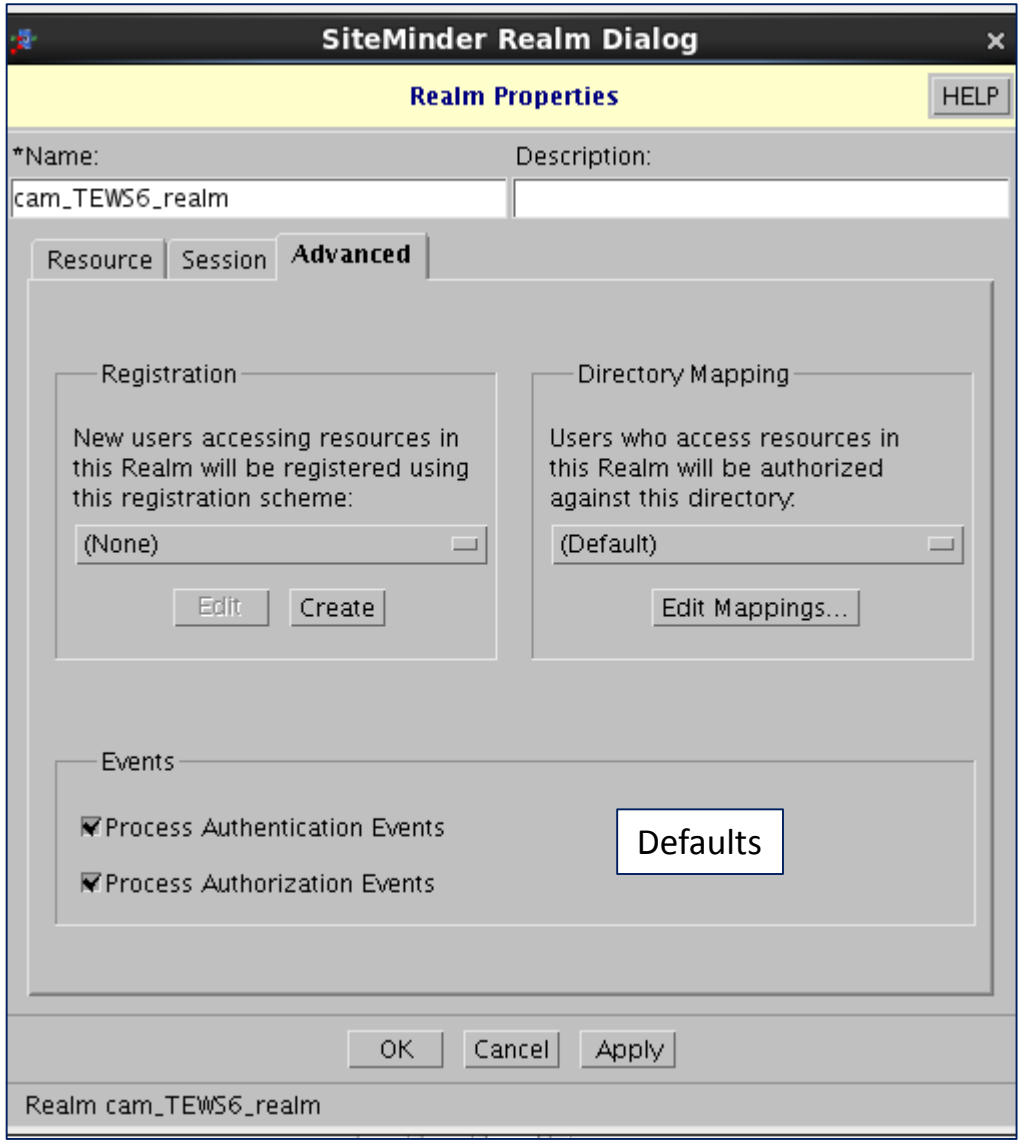




Primary Agent used by IM
(defined with a SM ACO object)

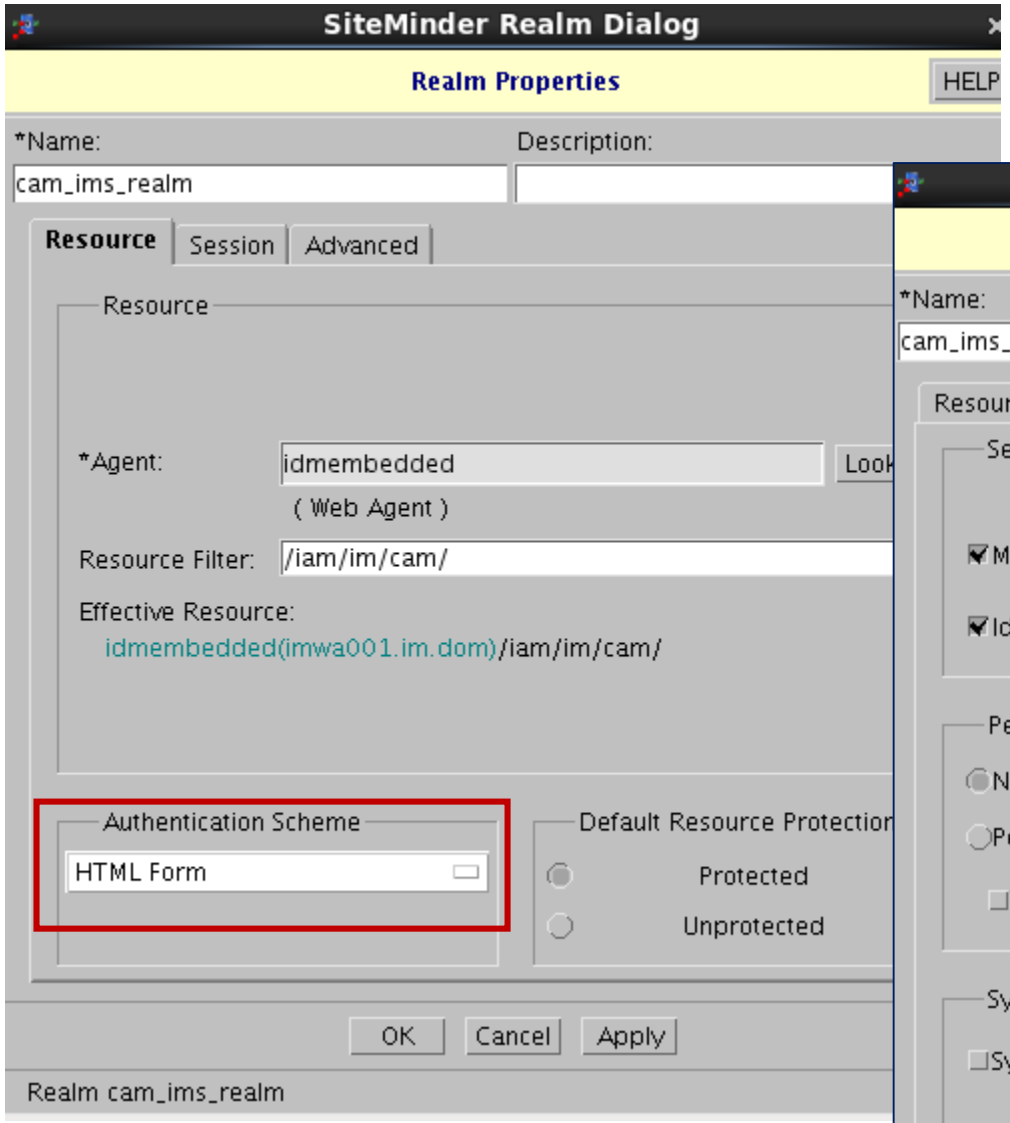
Note: Auth Schema may be default or BASIC
(default includes BASIC Auth)


SiteMinder Realm Dialog
Realm Properties
HELP
*Name:
Description:
cam_TEWS6_realm
Resource
Session
Advanced
Session Timeouts
Hours
Minutes
Maximum Timeout Enabled
2
0
Idle Timeout Enabled
0
30
Persistent Session
No Persistent Session
Persistent Session
Hours
Minutes
Seconds
Validation Period Enabled
Synchronous Auditing
Synchronous Auditing
Defaults
OK
Cancel
Apply
Realm cam_TEWS6_realm

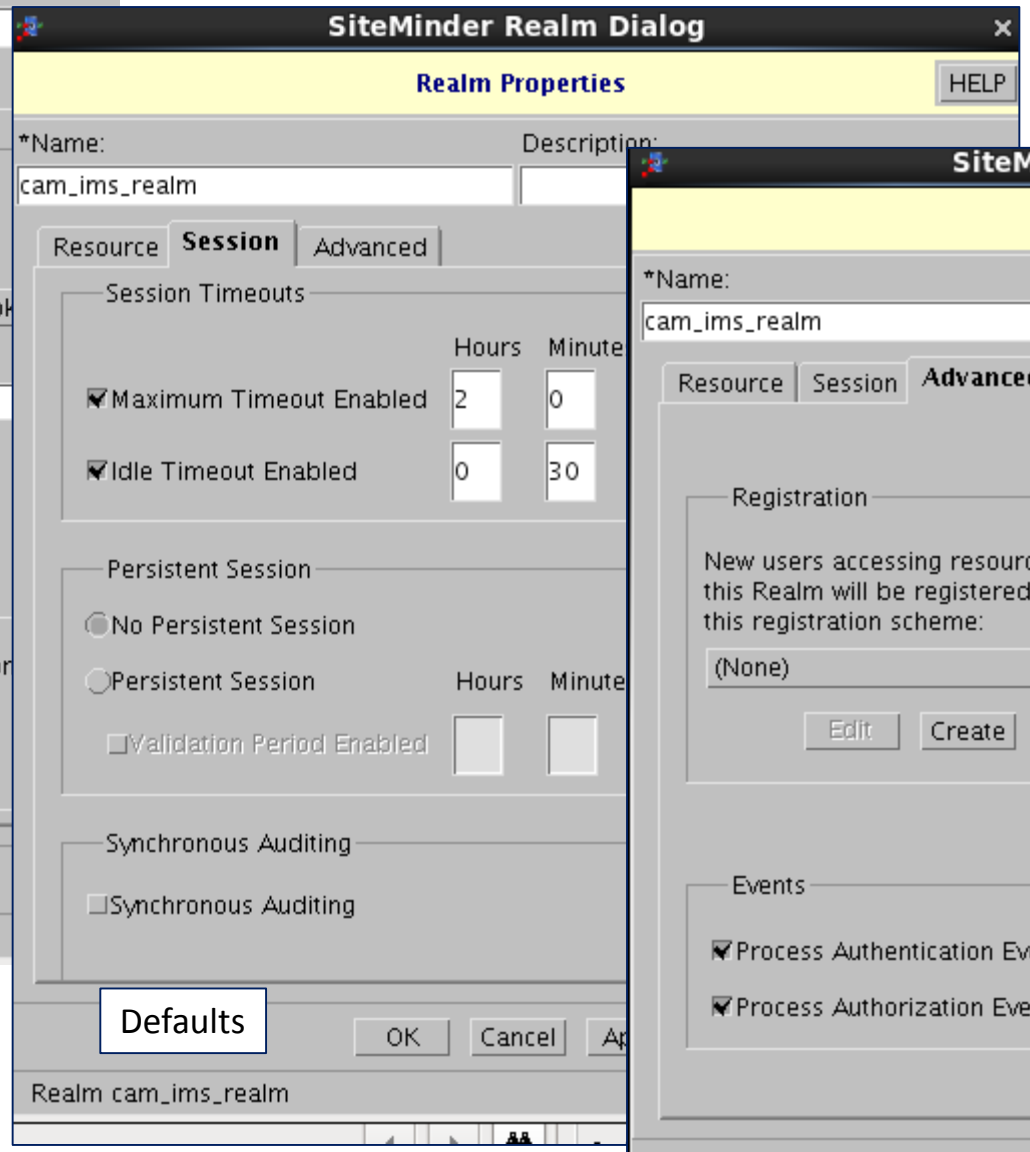

SiteMinder Realm Dialog
Realm Properties
HELP
*Name:
Description:
cam_TEWS6_realm
Resource
Session
Advanced
Registration
New users accessing resources in this Realm will be registered using this registration scheme:
(None)
Edit
Create
Directory Mapping
Users who access resources in this Realm will be authorized against this directory:
(Default)
Edit Mappings...
Events
Process Authentication Events
Process Authorization Events
Defaults
OK
Cancel
Apply
Realm cam_TEWS6_realm

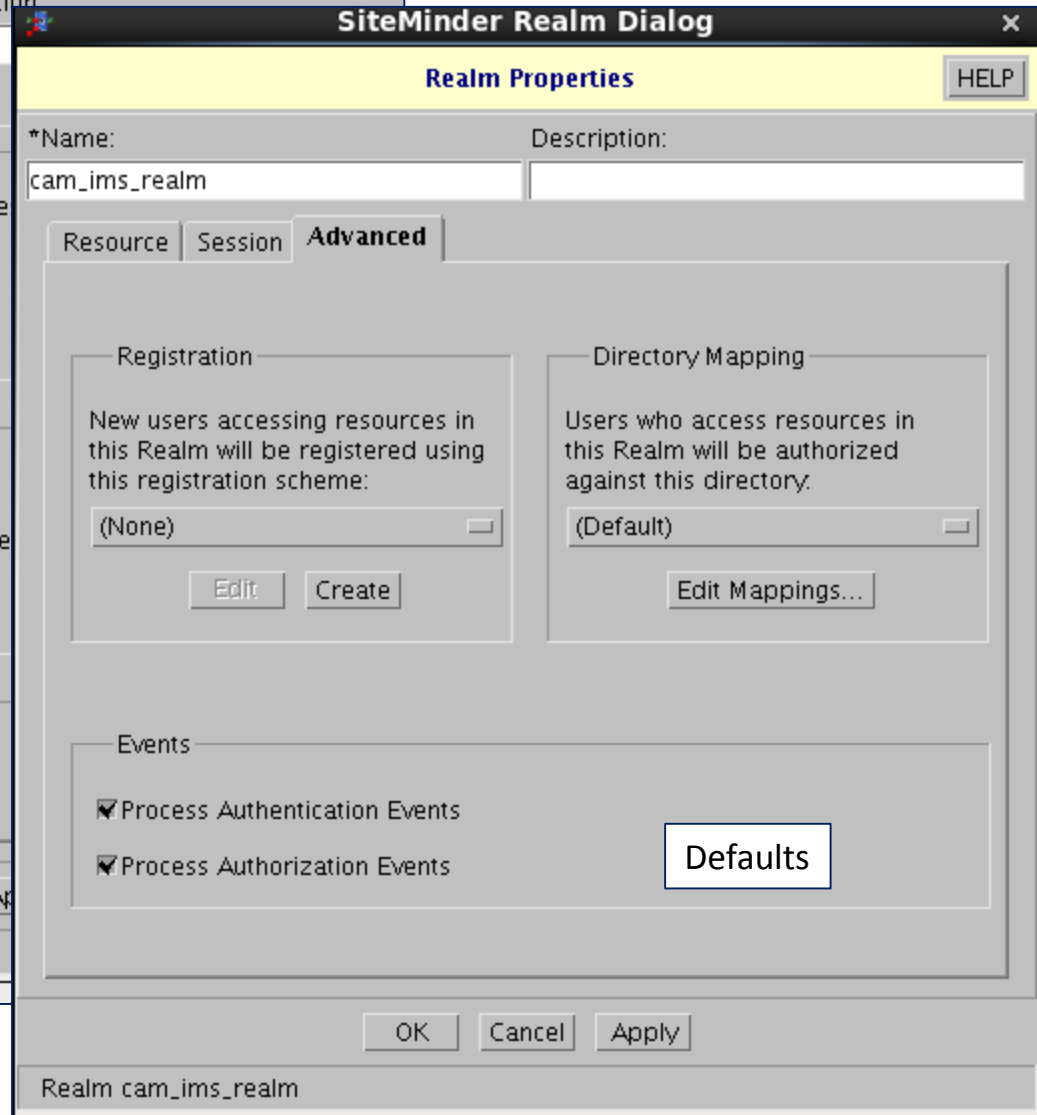
Compare SiteMinder Objects for Protected (cam) and Public (campublic) URI

Protected ENV (cam)

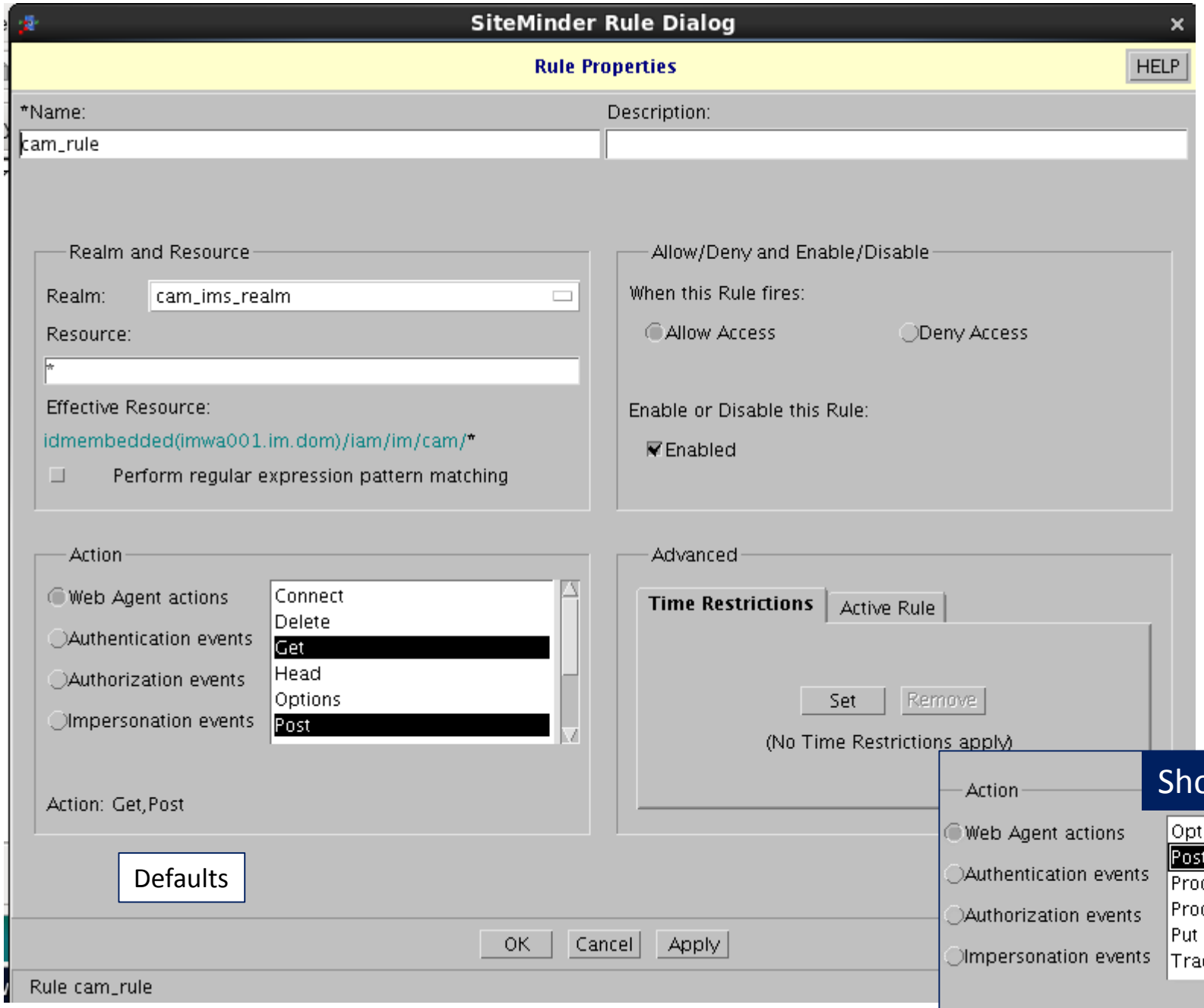


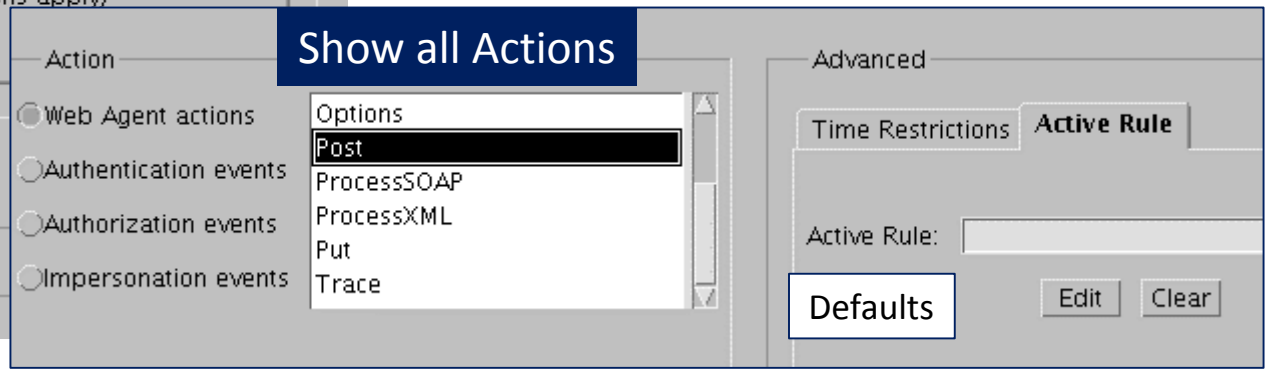
NOT Default. Changed from Basic to HTML
For better look and integration



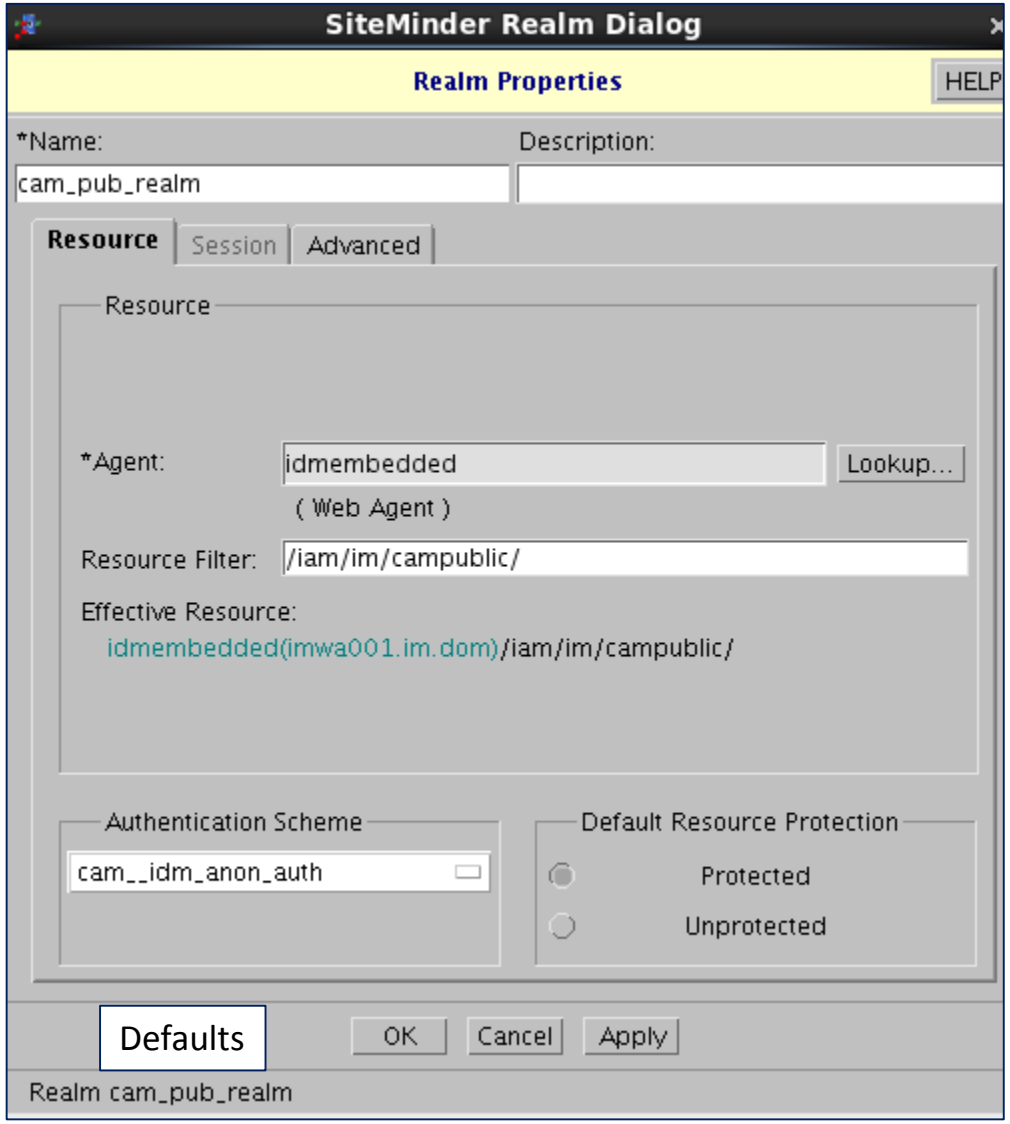


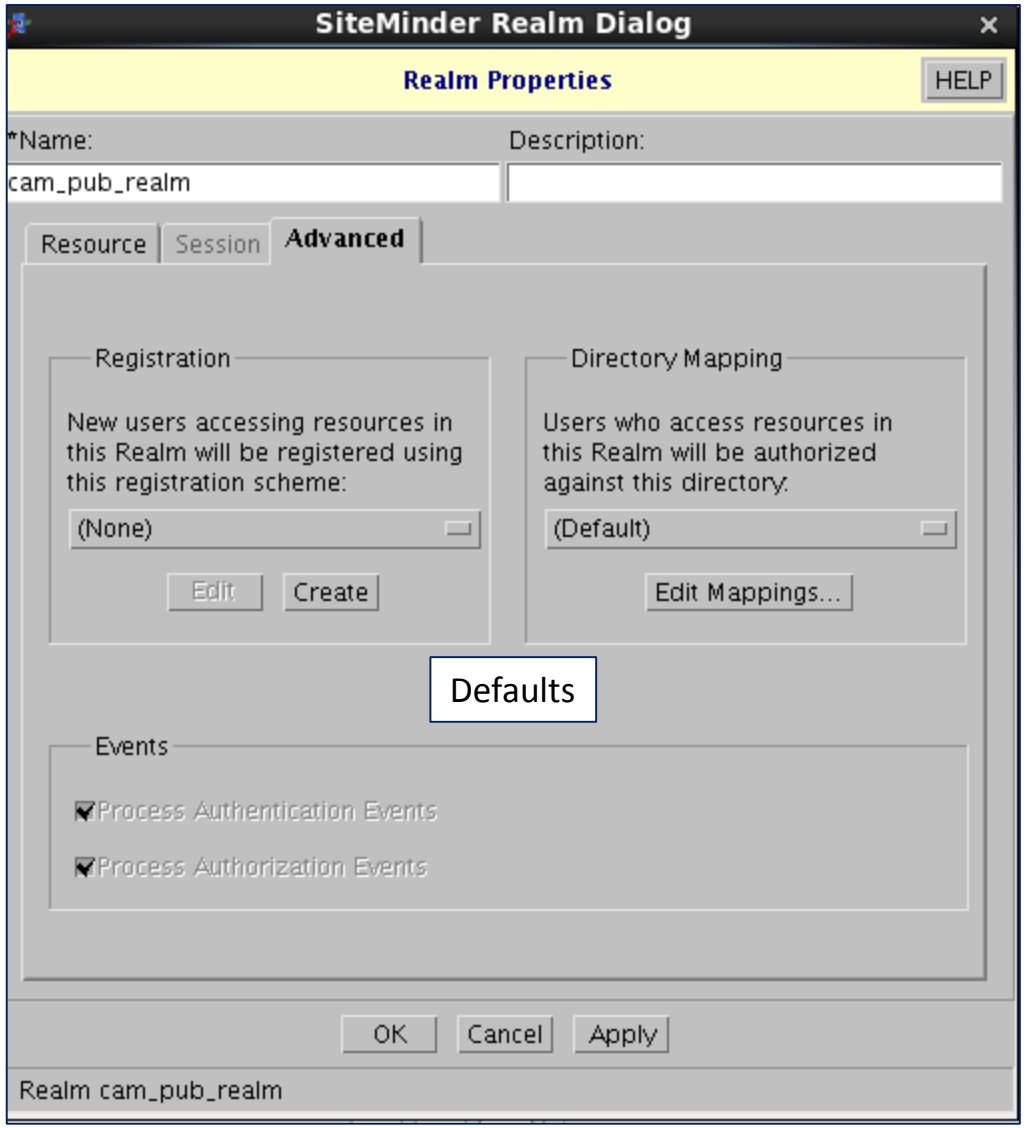
Protected ENV (cam)



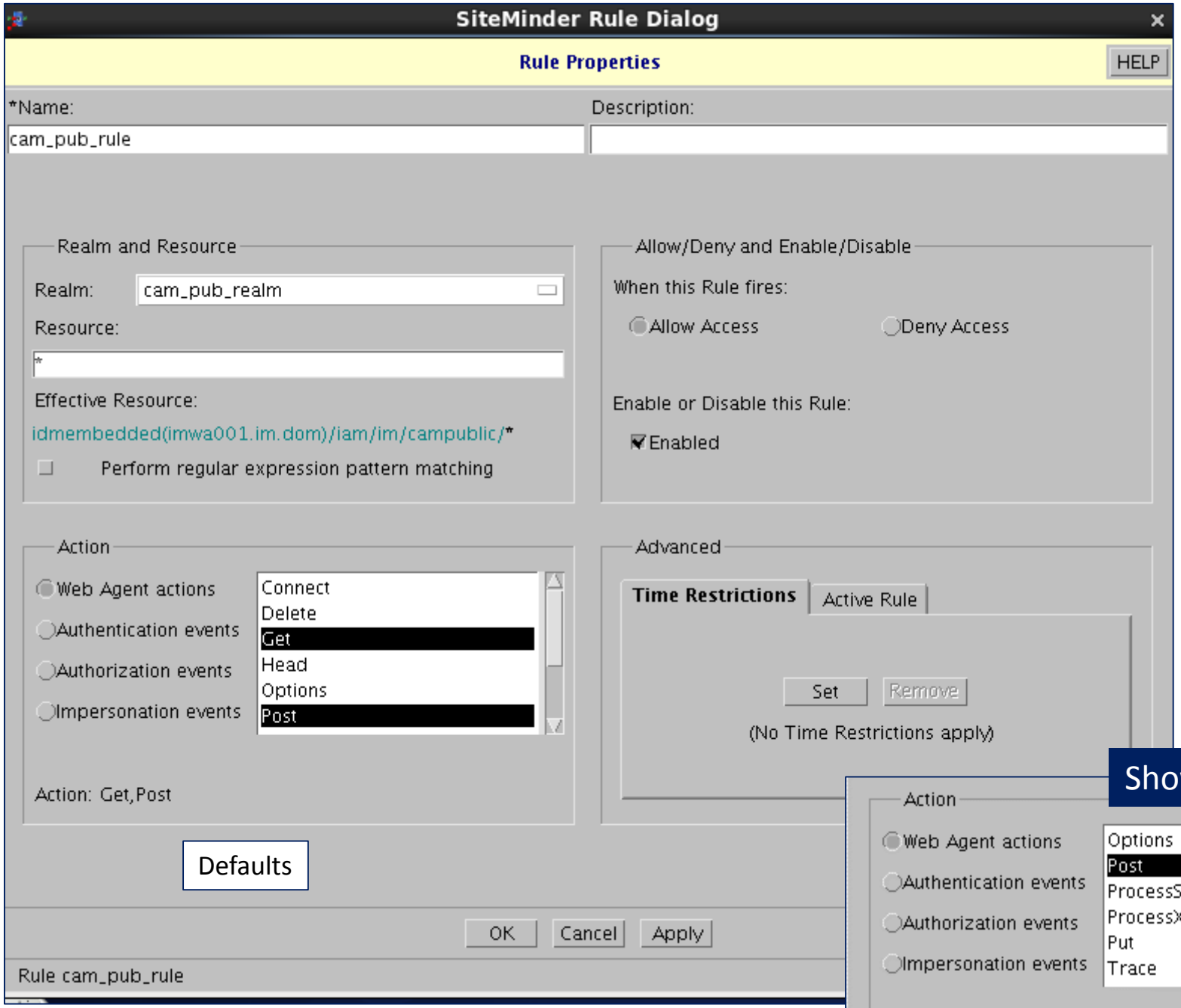


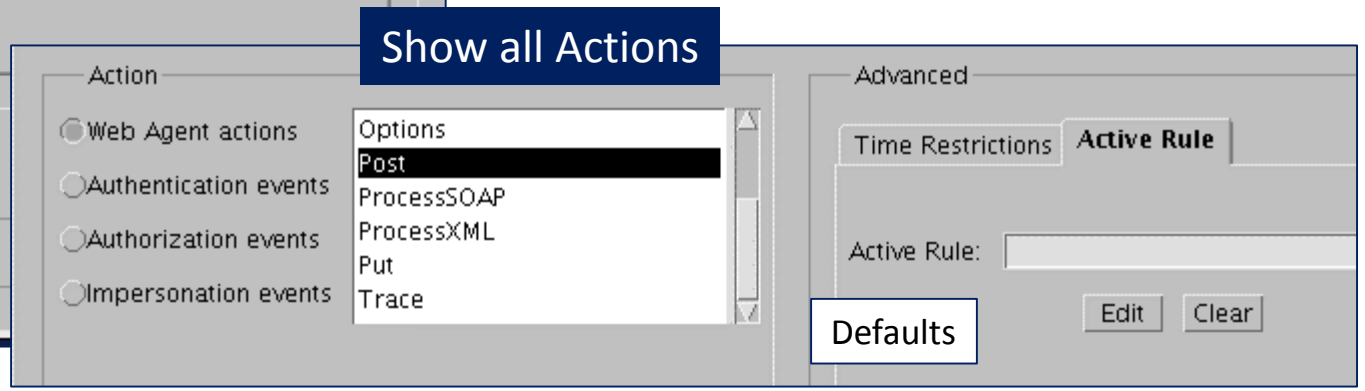
Public ENV (campublic)

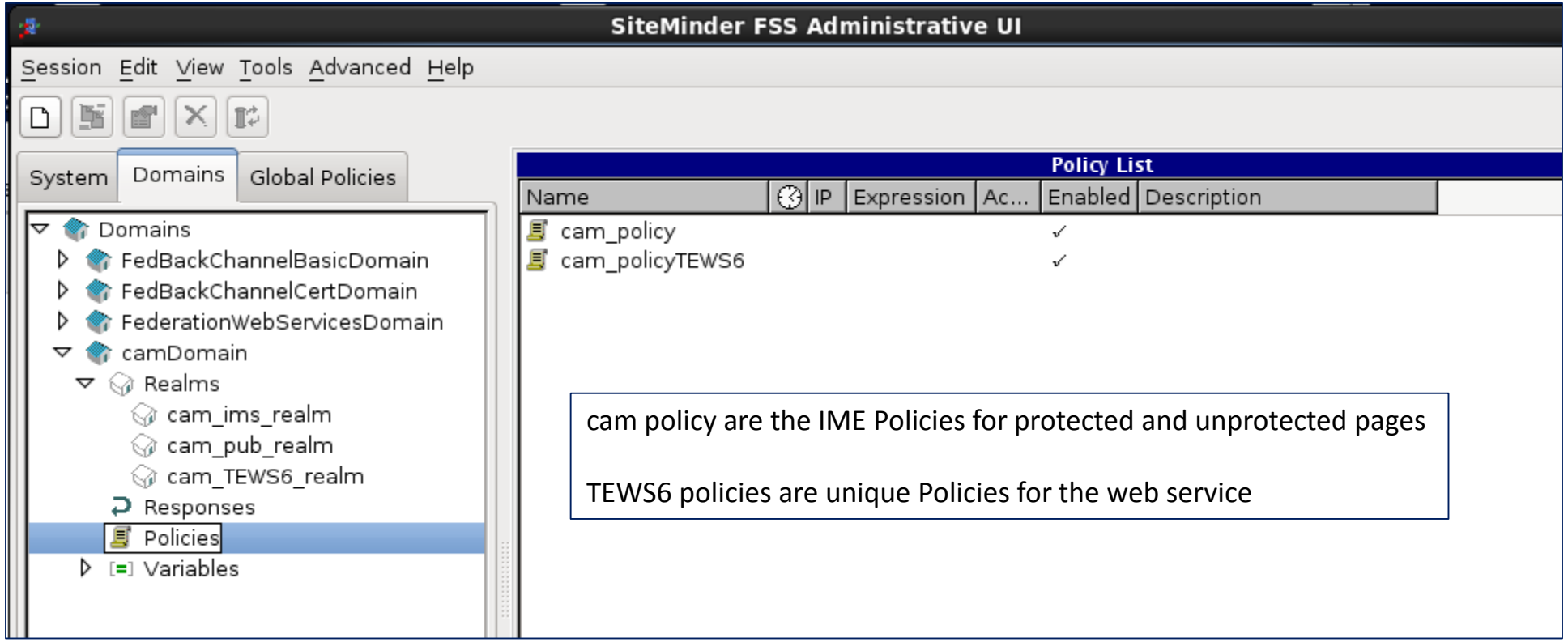


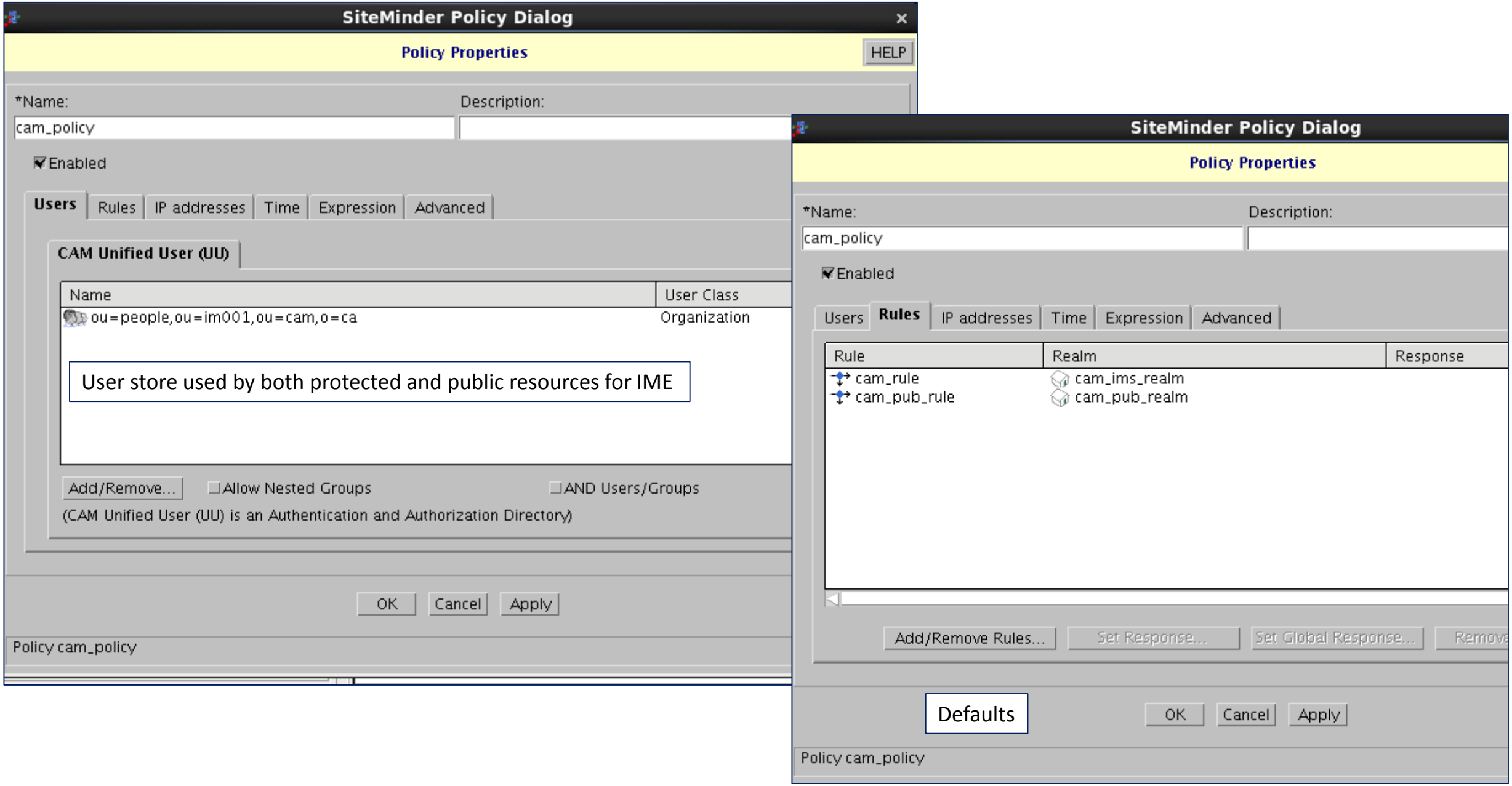


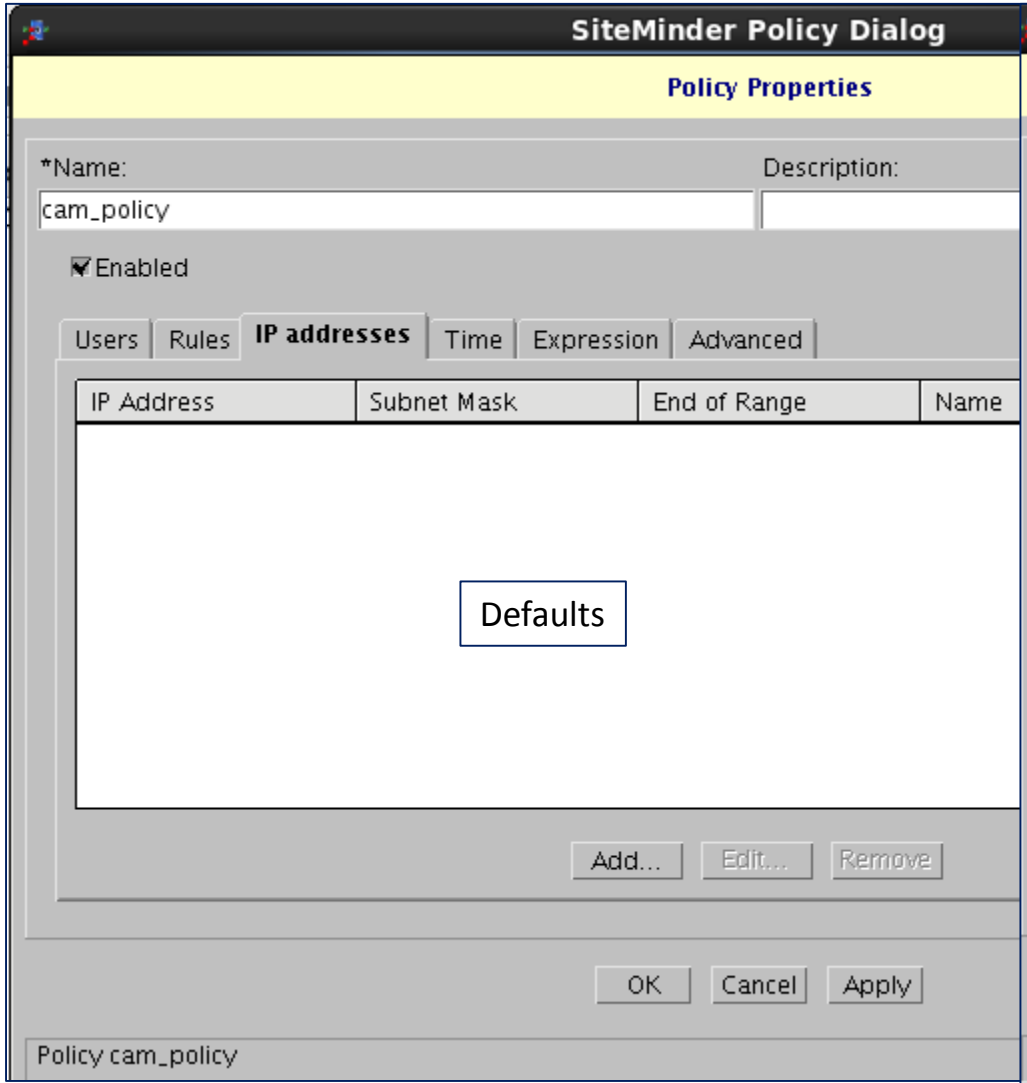
Public ENV (campublic)

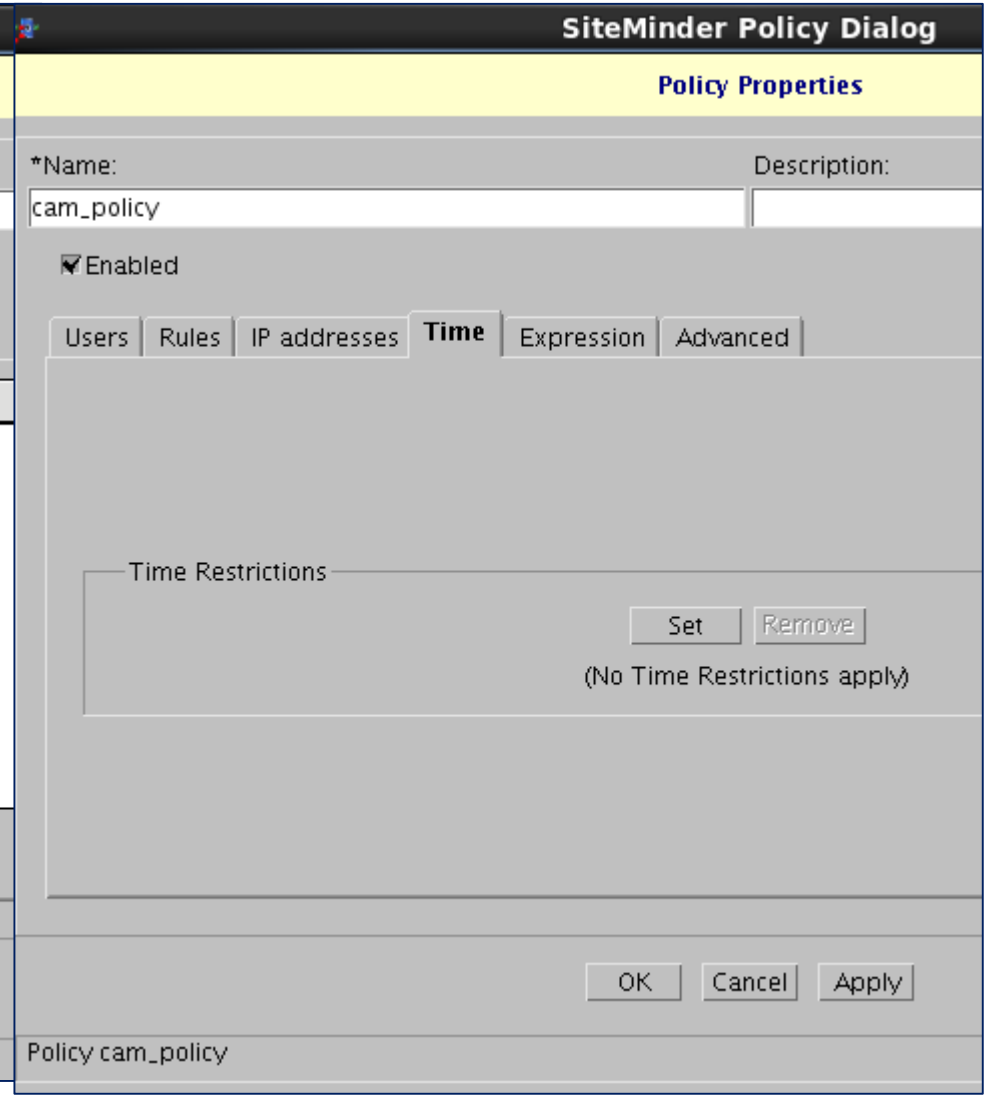


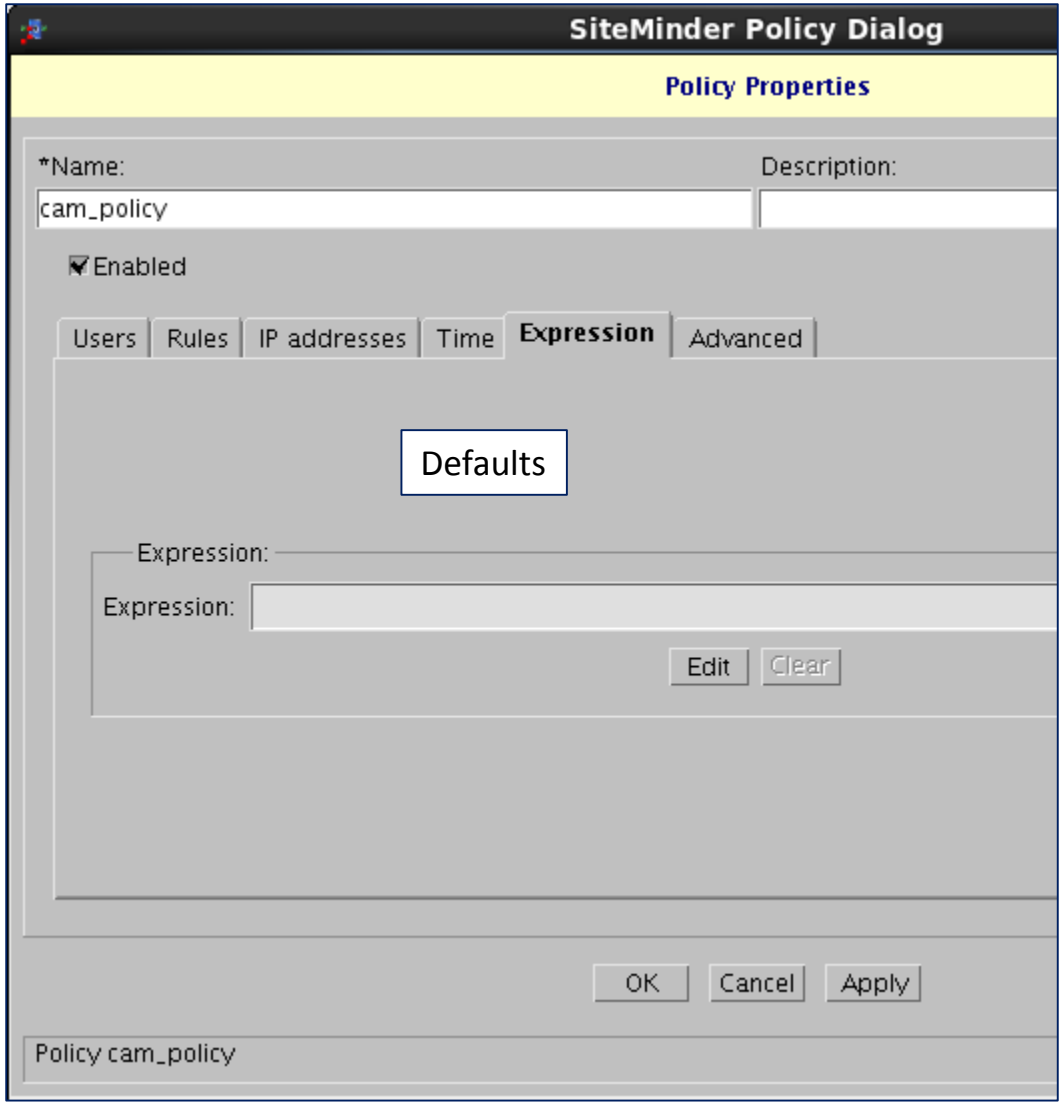


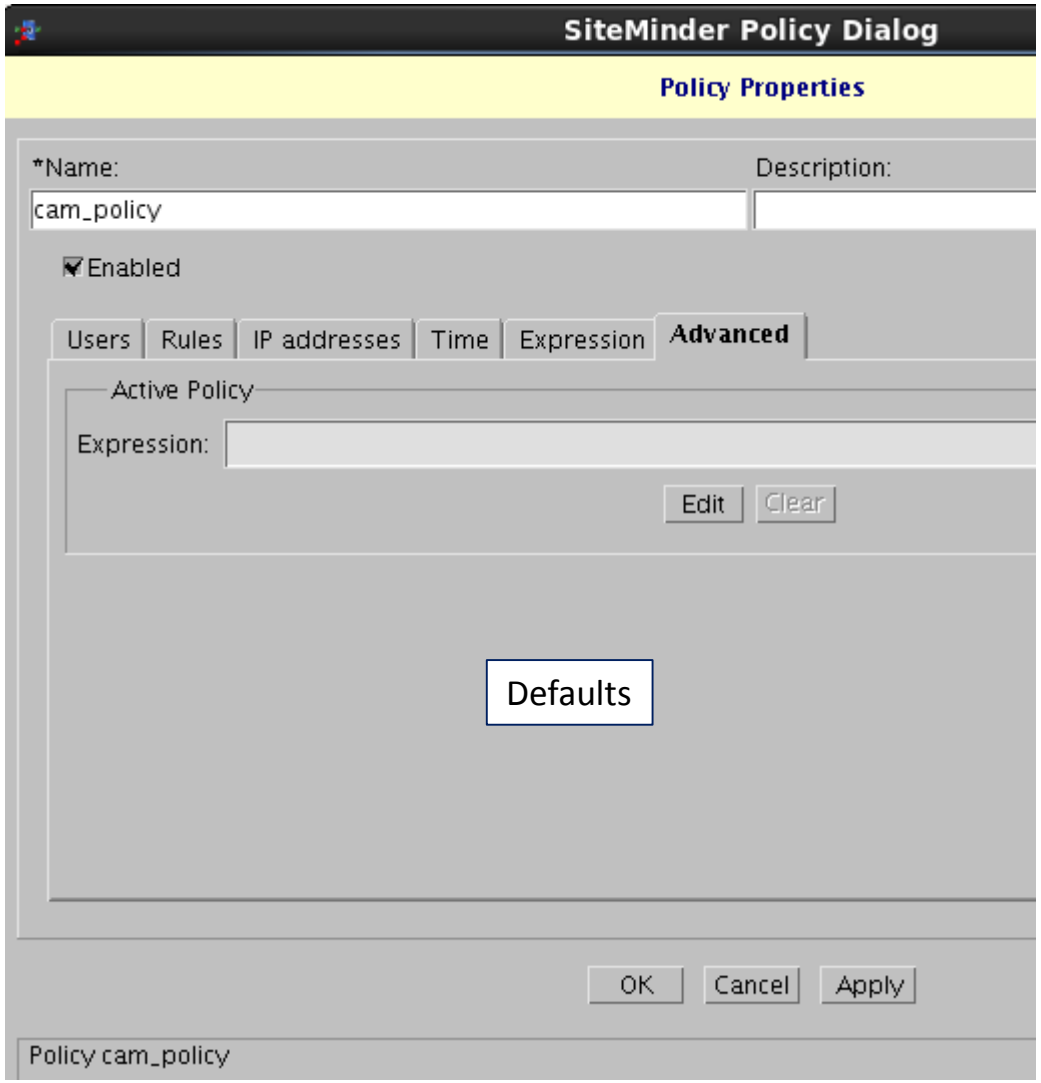

SiteMinder FSS Administrative UI
Session Edit View Tools Advanced Help
System
Domains
Global Policies
Domains
FedBackChannelBasicDomain
FedBackChannelCertDomain
FederationWebServicesDomain
camDomain
Realms
cam_ims_realm
cam_pub_realm
cam_TEWS6_realm
Responses
Policies
Variables
Policy List
Name
IP
Expression
Ac...
Enabled
Description
cam_policy
cam_policyTEWS6
cam policy are the IME Policies for protected and unprotected pages
TEWS6 policies are unique Policies for the web service

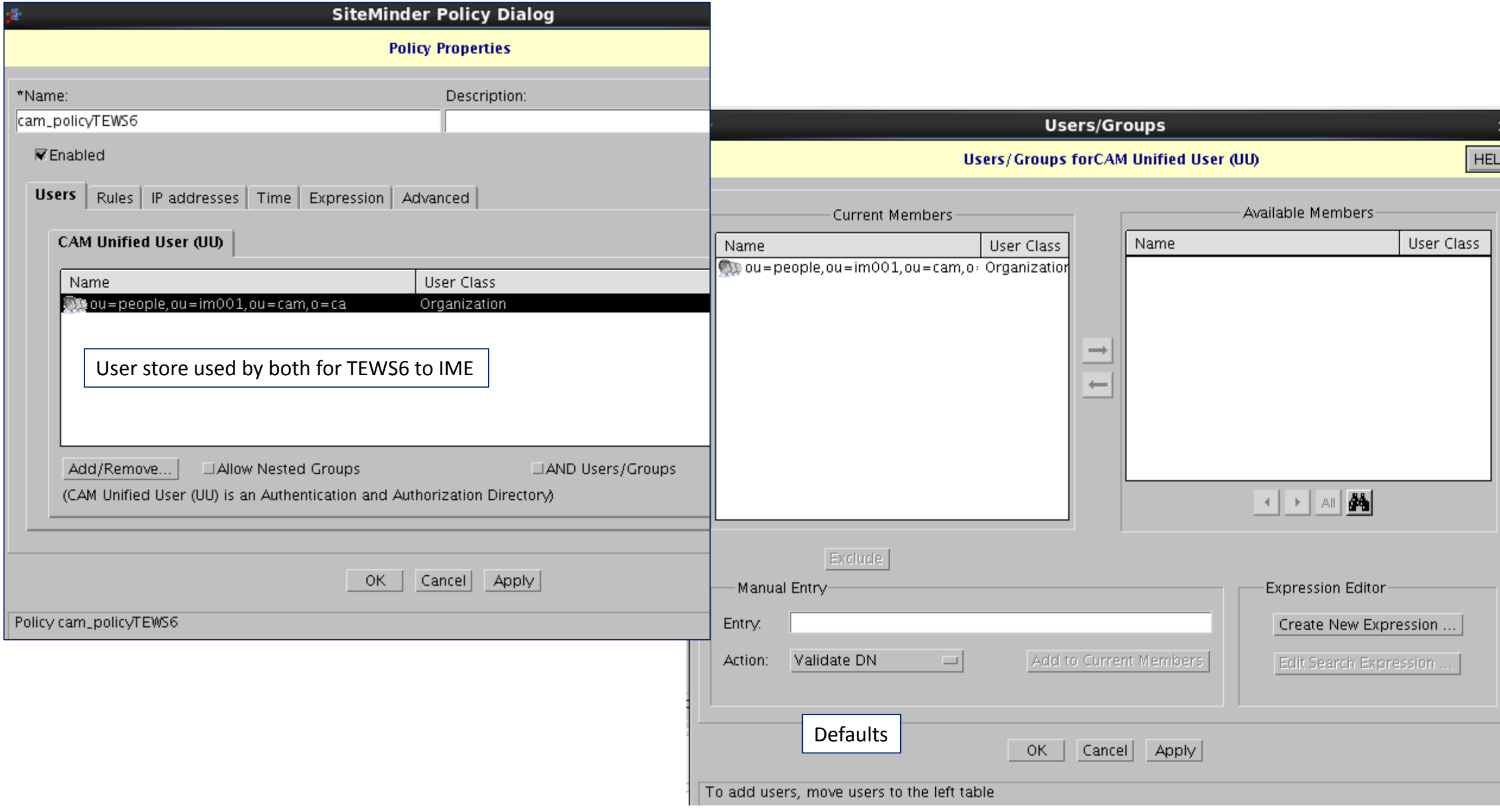

SiteMinder Policy Dialog
Policy Properties
HELP
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
CAM Unified User (UU)
Name
User Class
ou=people,ou=im001,ou=cam,o=ca
Organization
User store used by both protected and public resources for IME
Add/Remove...
Allow Nested Groups
AND Users/Groups
(CAM Unified User (UU) is an Authentication and Authorization Directory)
OK
Cancel
Apply
Policy cam_policy
SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Rule
Realm
Response
cam_rule
cam_ims_realm
cam_pub_rule
cam_pub_realm
Add/Remove Rules...
Set Response...
Set Global Response...
Remove
Defaults
OK
Cancel
Apply
Policy cam_policy

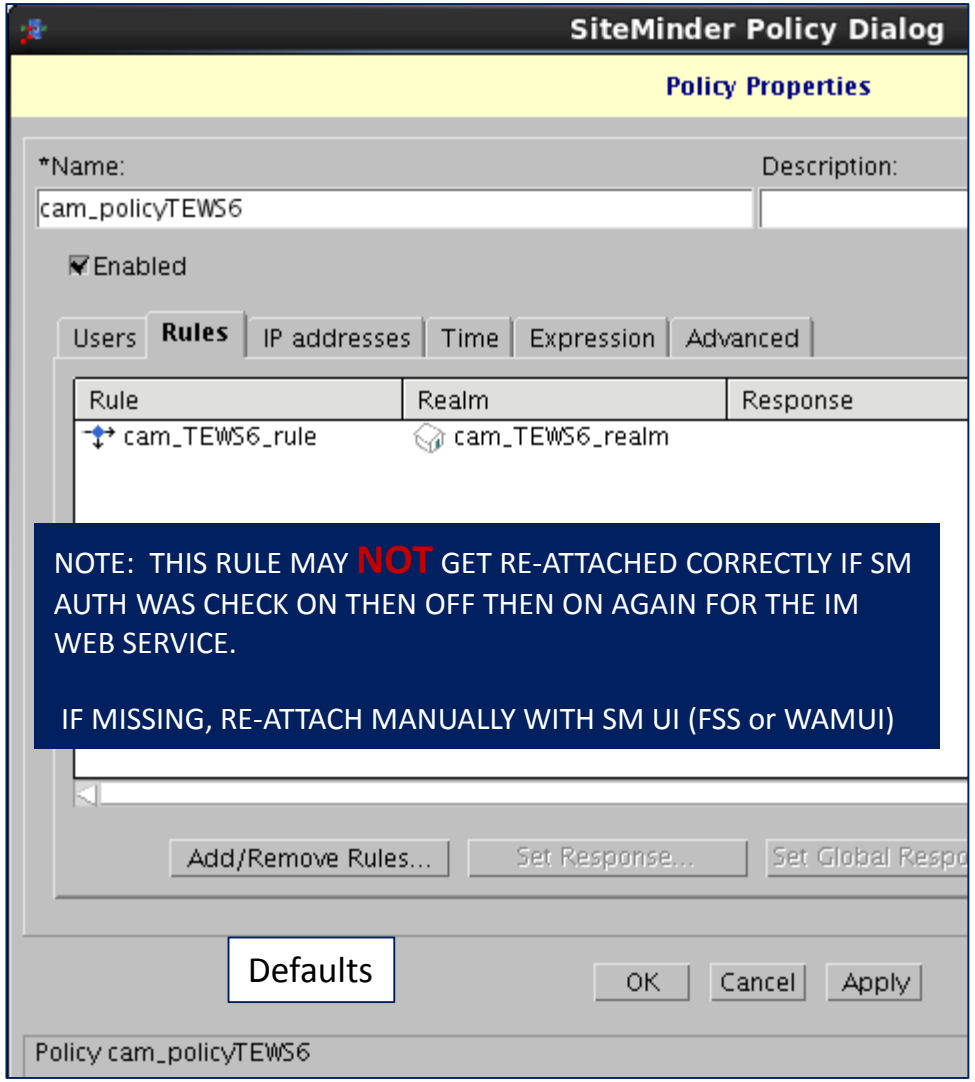

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
IP Address
Subnet Mask
End of Range
Name
Defaults
Add...
Edit...
Remove
OK
Cancel
Apply
Policy cam_policy

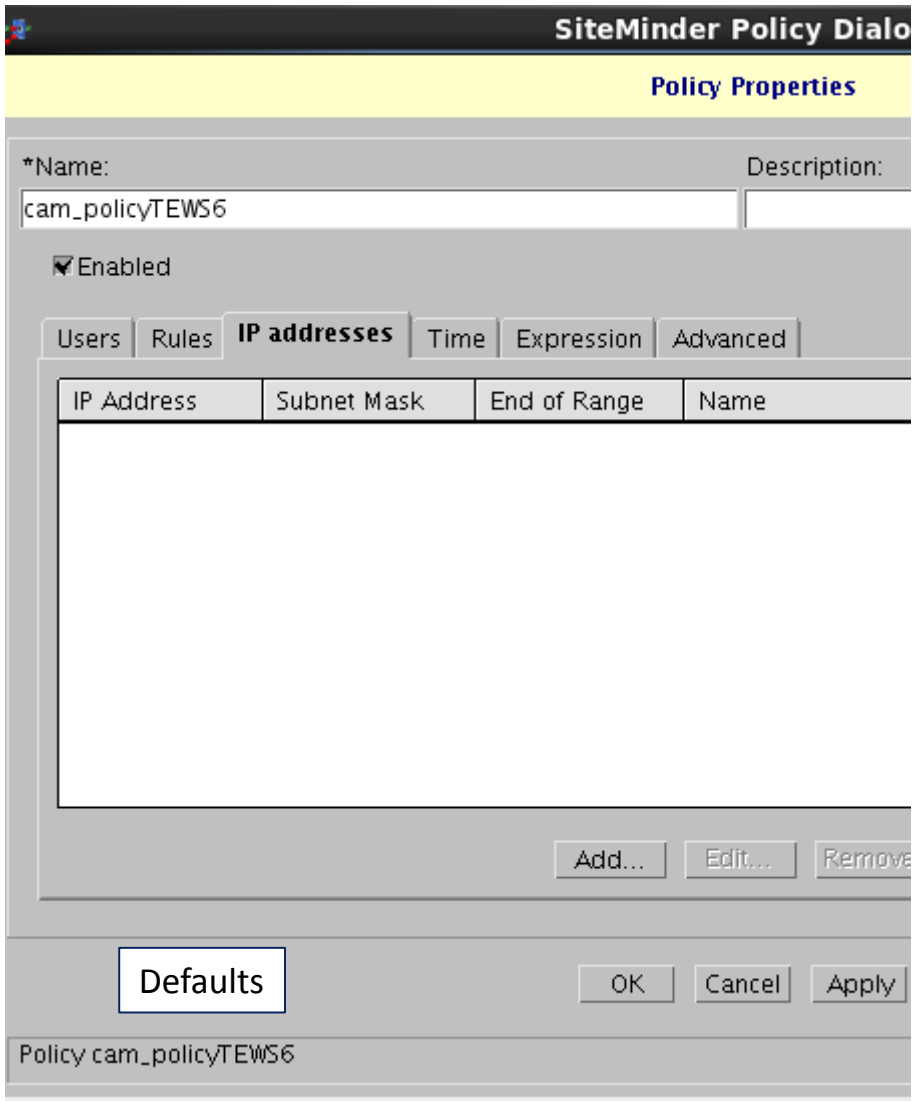

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Time Restrictions
Set
Remove
(No Time Restrictions apply)
OK
Cancel
Apply
Policy cam_policy

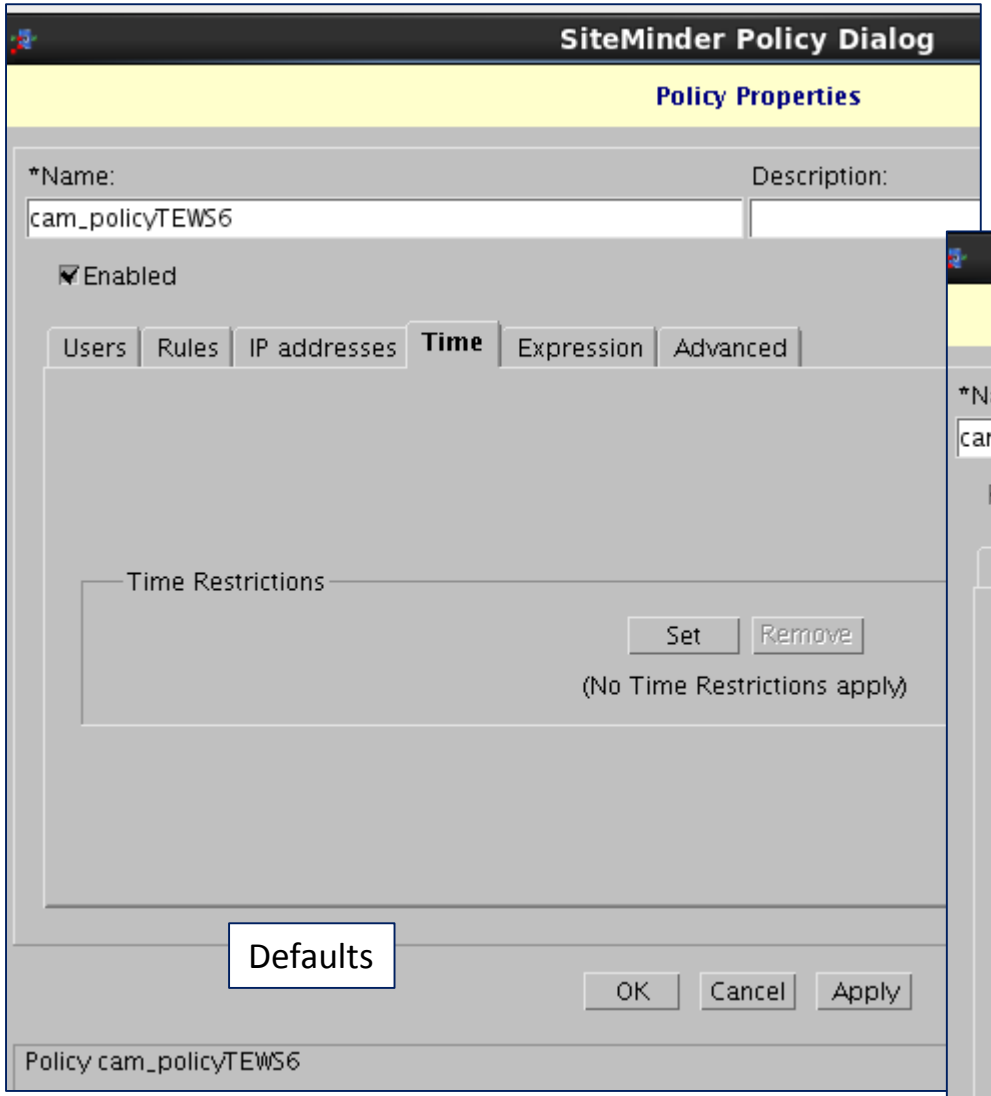

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Defaults
Expression:
Expression:
Edit
Clear
OK
Cancel
Apply
Policy cam_policy

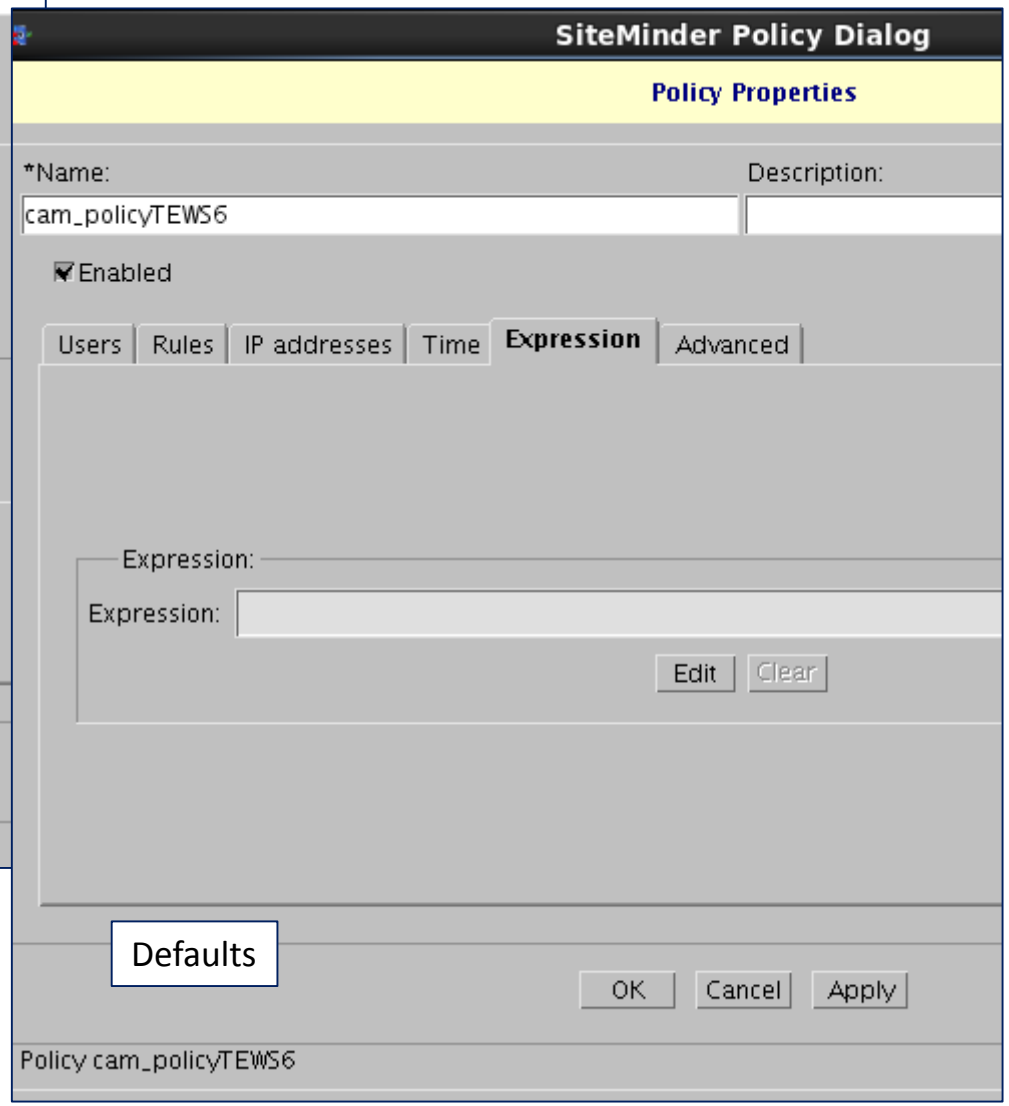

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policy
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Active Policy
Expression:
Edit
Clear
Defaults
OK
Cancel
Apply
Policy cam_policy

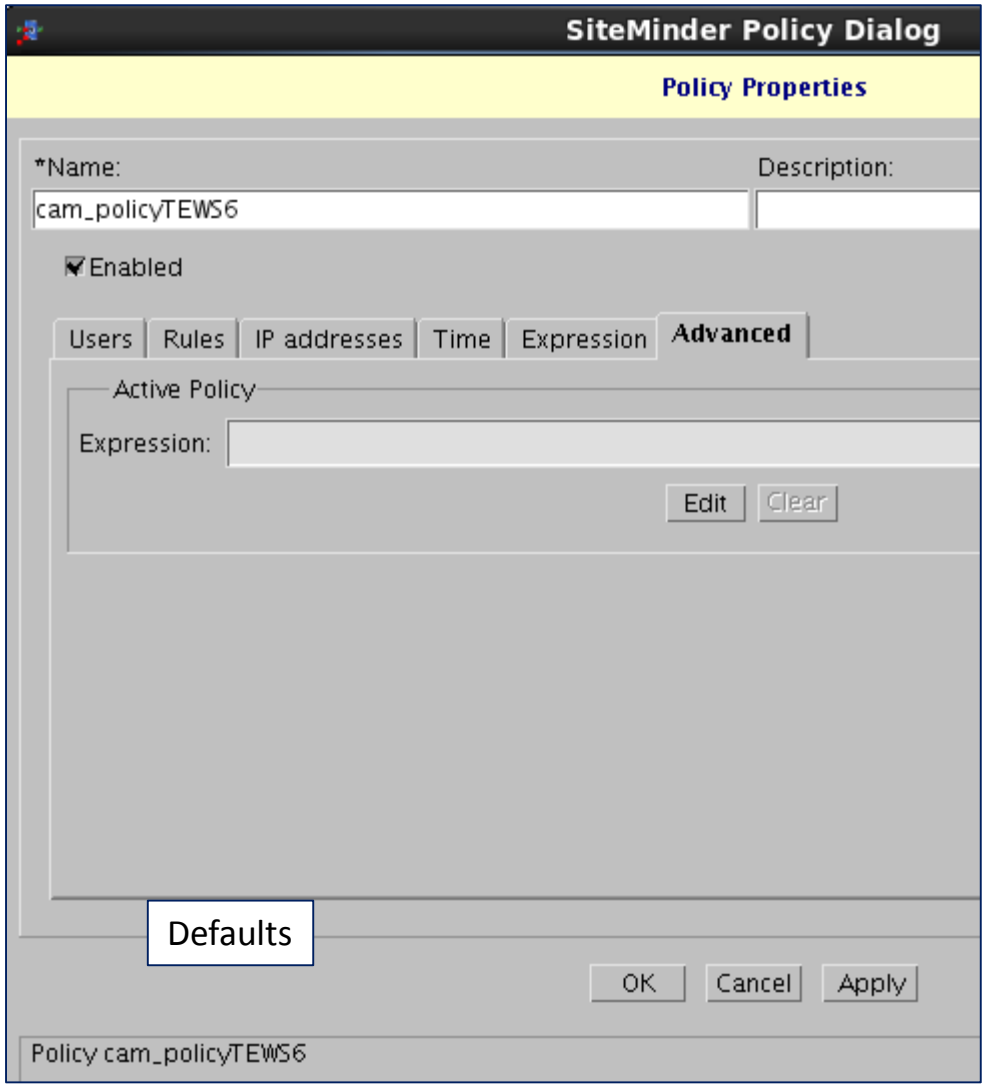

SiteMinder Policy Dialog
Policy Properties
*Name:
cam_policyTEWS6
Description:
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
CAM Unified User (UU)
Name
User Class
ou=people,ou=im001,ou=cam,o=ca
Organization
User store used by both for TEWS6 to IME
Add/Remove...
Allow Nested Groups
AND Users/Groups
(CAM Unified User (UU) is an Authentication and Authorization Directory)
OK
Cancel
Apply
Policy cam_policyTEWS6
Users/Groups
Users/Groups forCAM Unified User (UU)
HEL
Current Members
Name
User Class
ou=people,ou=im001,ou=cam,o
Organizatior
Available Members
Name
User Class
All
Exclude
Manual Entry
Entry:
Action:
Validate DN
Add to Current Members
Expression Editor
Create New Expression ...
Edit Search Expression ...
Defaults
OK
Cancel
Apply
To add users, move users to the left table


SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policyTEWS6
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Rule
Realm
Response
cam_TEWS6_rule
cam_TEWS6_realm
NOTE: THIS RULE MAY NOT GET RE-ATTACHED CORRECTLY IF SM AUTH WAS CHECK ON THEN OFF THEN ON AGAIN FOR THE IM WEB SERVICE.
IF MISSING, RE-ATTACH MANUALLY WITH SM UI (FSS or WAMUI)
Add/Remove Rules...
Set Response...
Defaults
OK
Cancel
Apply
Policy cam_policyTEWS6


SiteMinder Policy Dialo
Policy Properties
*Name:
Description:
cam_policyTEWS6
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
IP Address
Subnet Mask
End of Range
Name
Add...
Edit...
Defaults
OK
Cancel
Apply
Policy cam_policyTEWS6

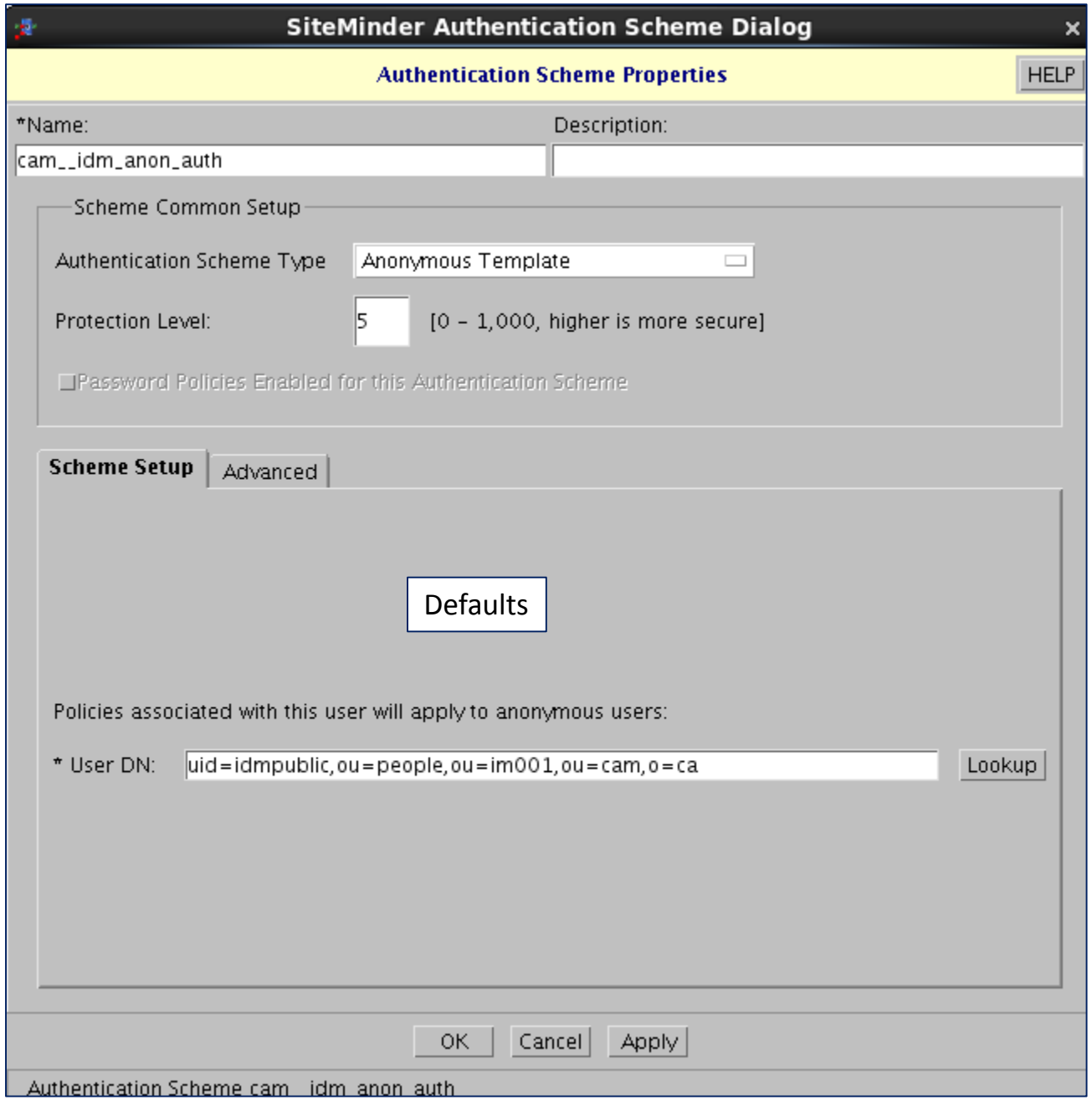

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policyTEWS6
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Time Restrictions
Set
Remove
(No Time Restrictions apply)
Defaults
OK
Cancel
Apply
Policy cam_policyTEWS6

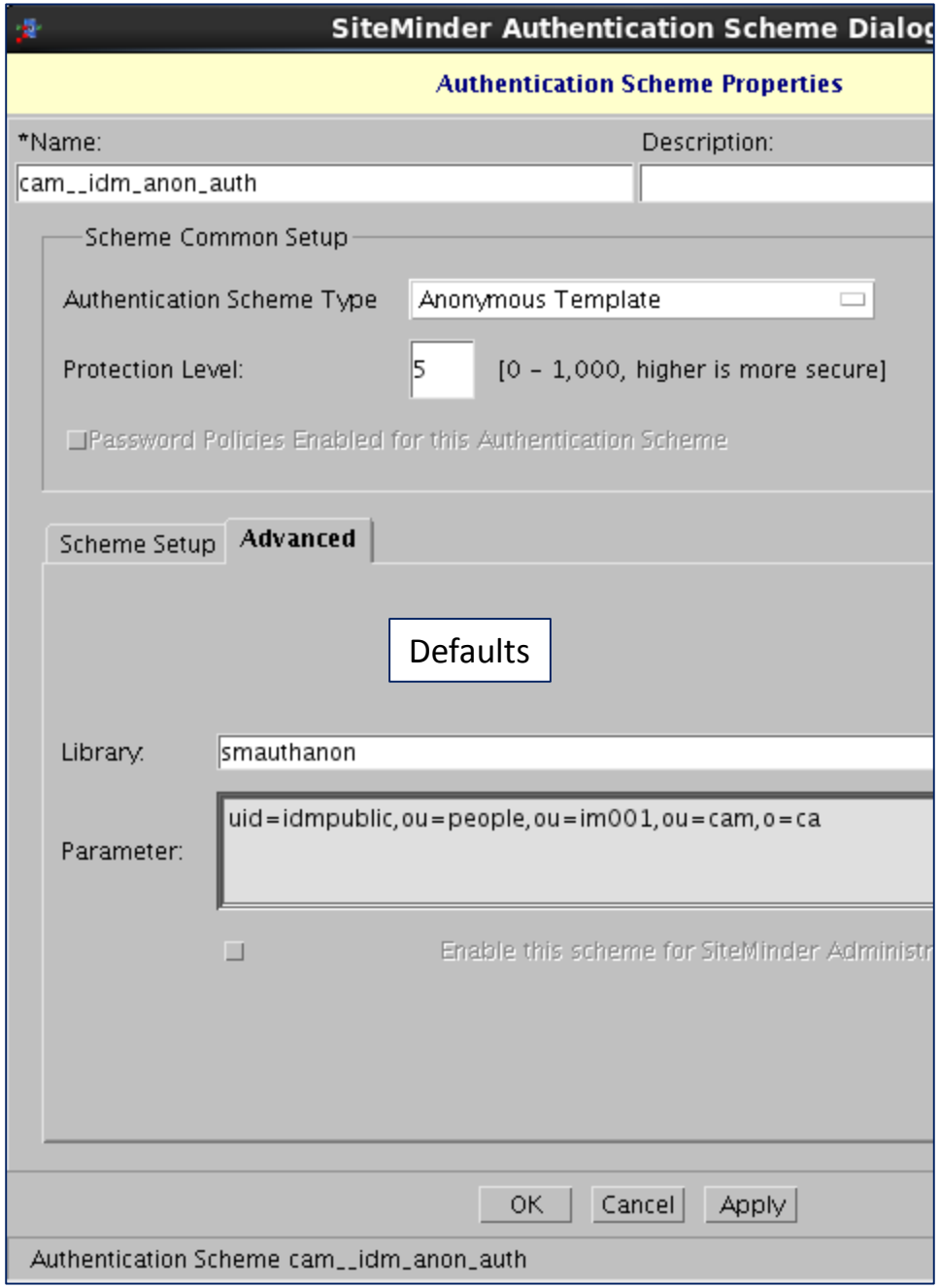

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policyTEWS6
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Expression:
Expression:
Edit
Clear
Defaults
OK
Cancel
Apply
Policy cam_policyTEWS6

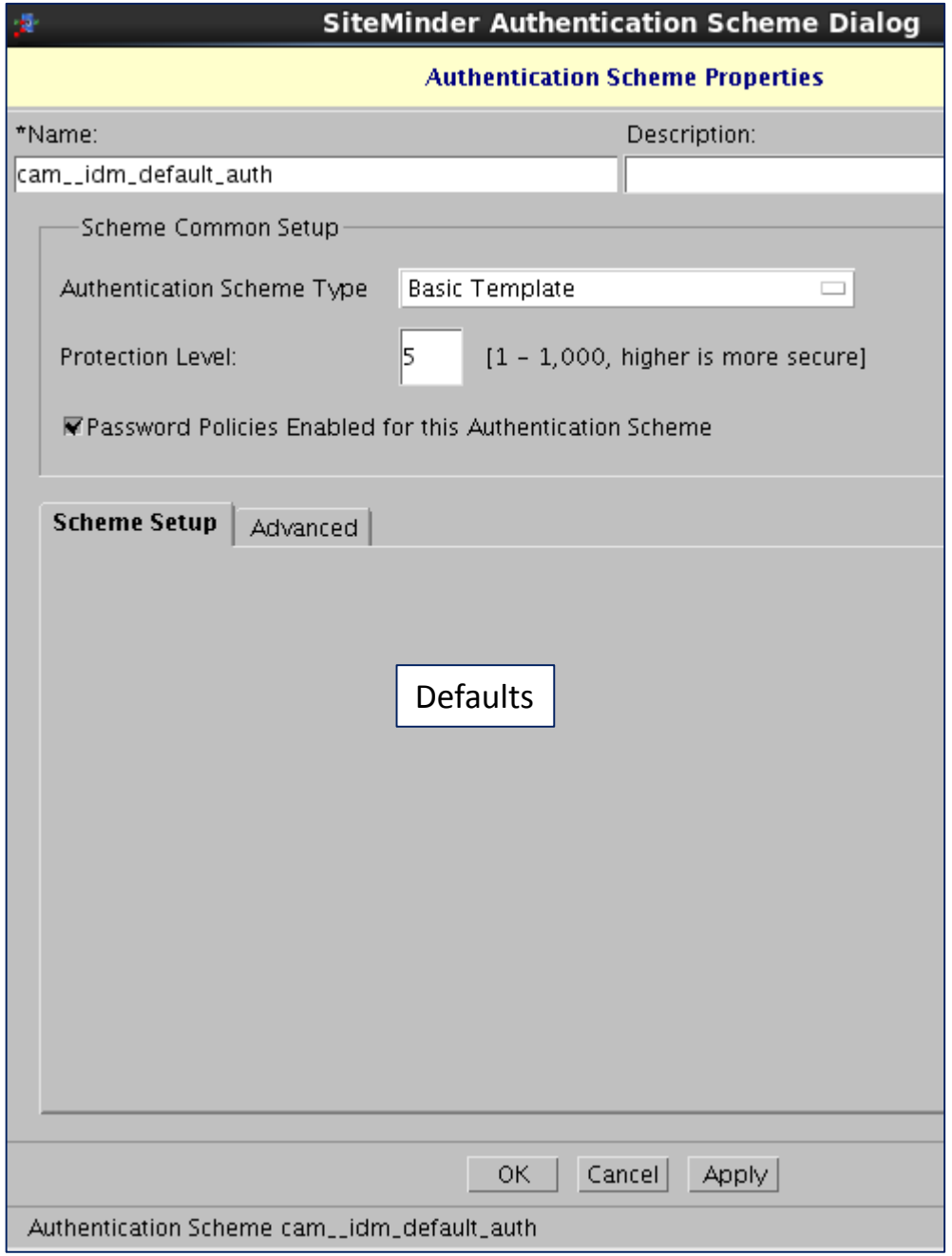

SiteMinder Policy Dialog
Policy Properties
*Name:
Description:
cam_policyTEWS6
Enabled
Users
Rules
IP addresses
Time
Expression
Advanced
Active Policy
Expression:
Edit
Clear
Defaults
OK
Cancel
Apply
Policy cam_policyTEWS6

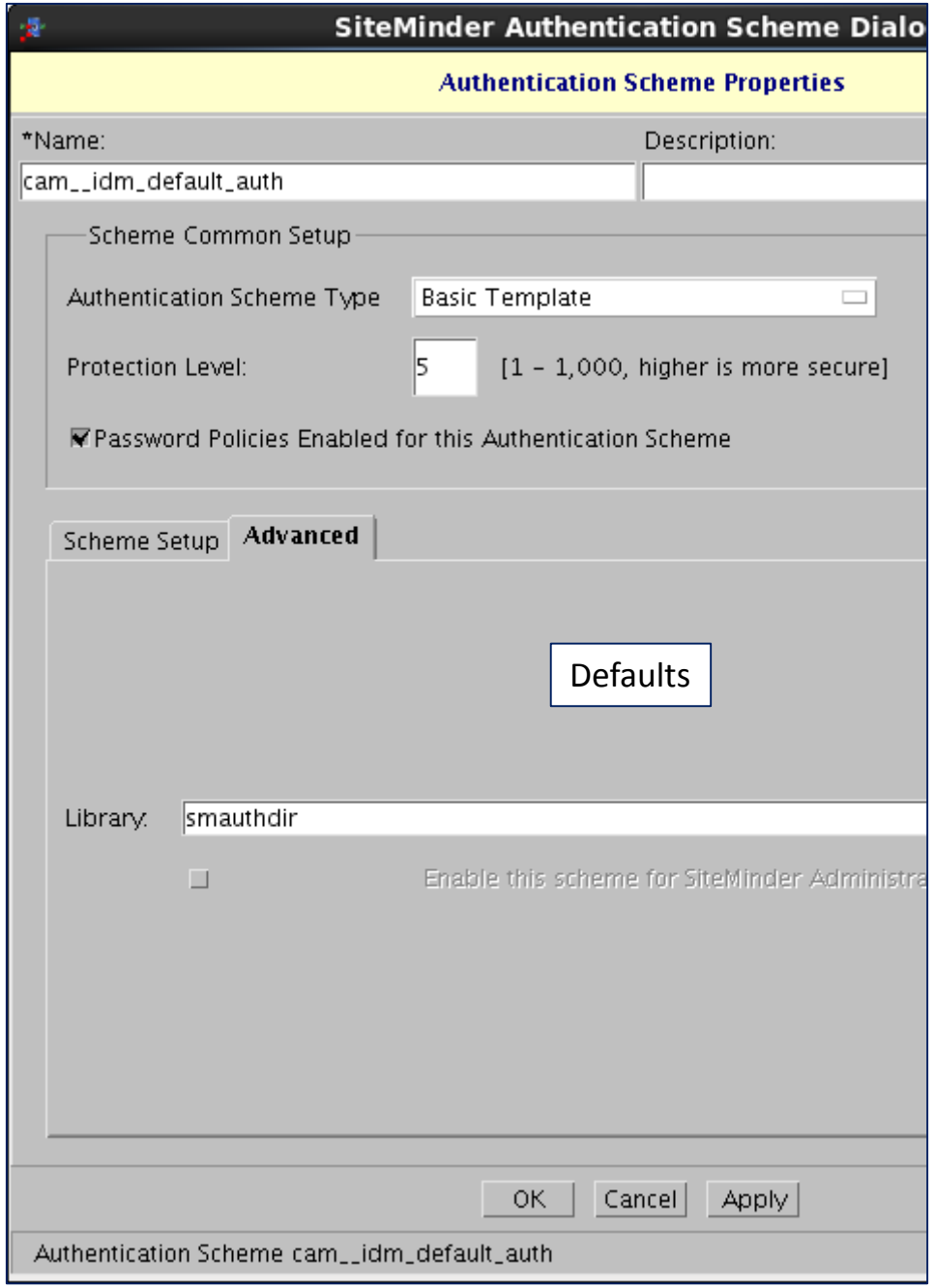
SiteMinder Authentication Objects

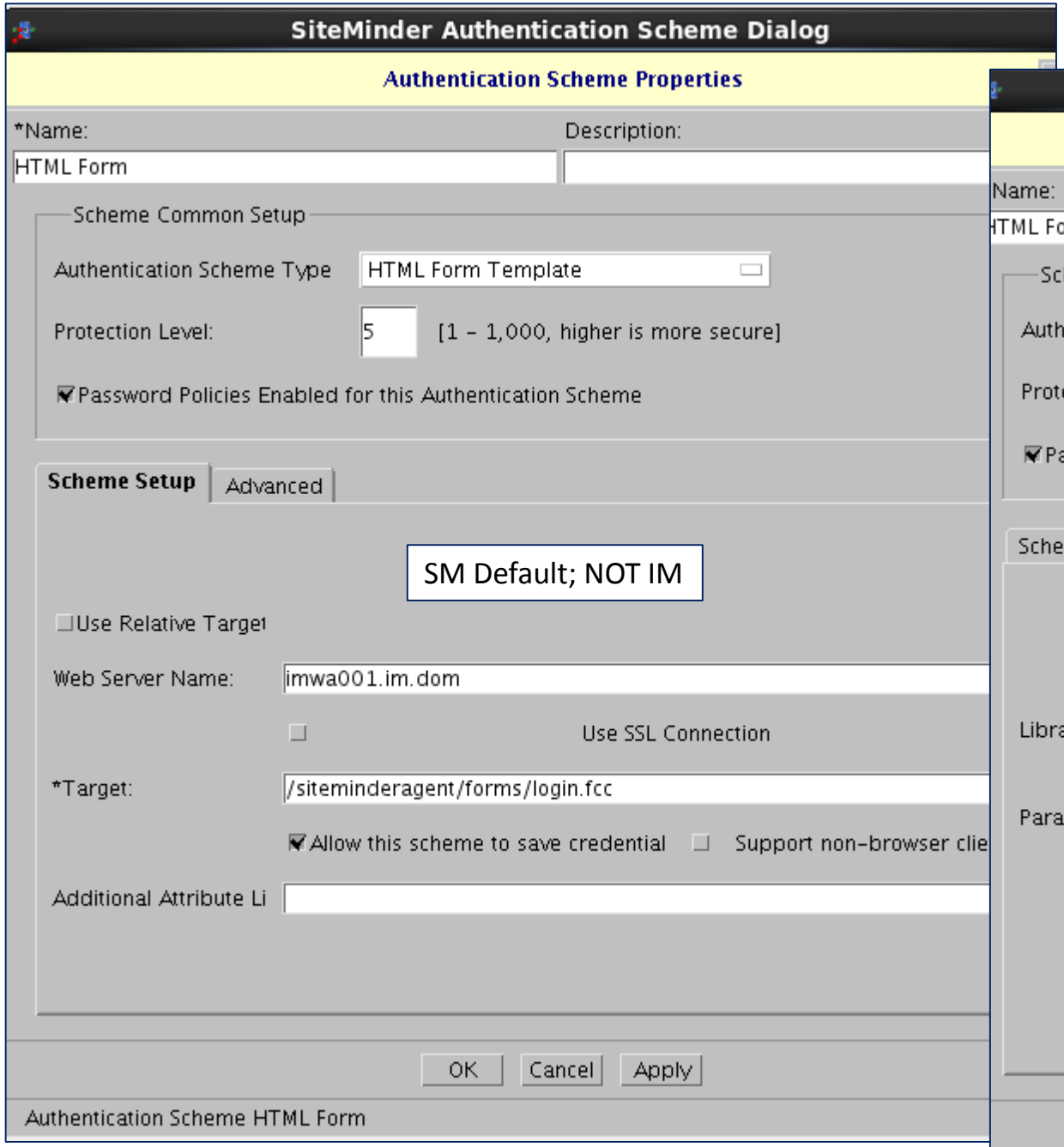
The IM:SM integration will make unique copies of the SM OOTB Authentication Objects and add in the IM IME as a pre-appended test to the usual SM authentication template objects.

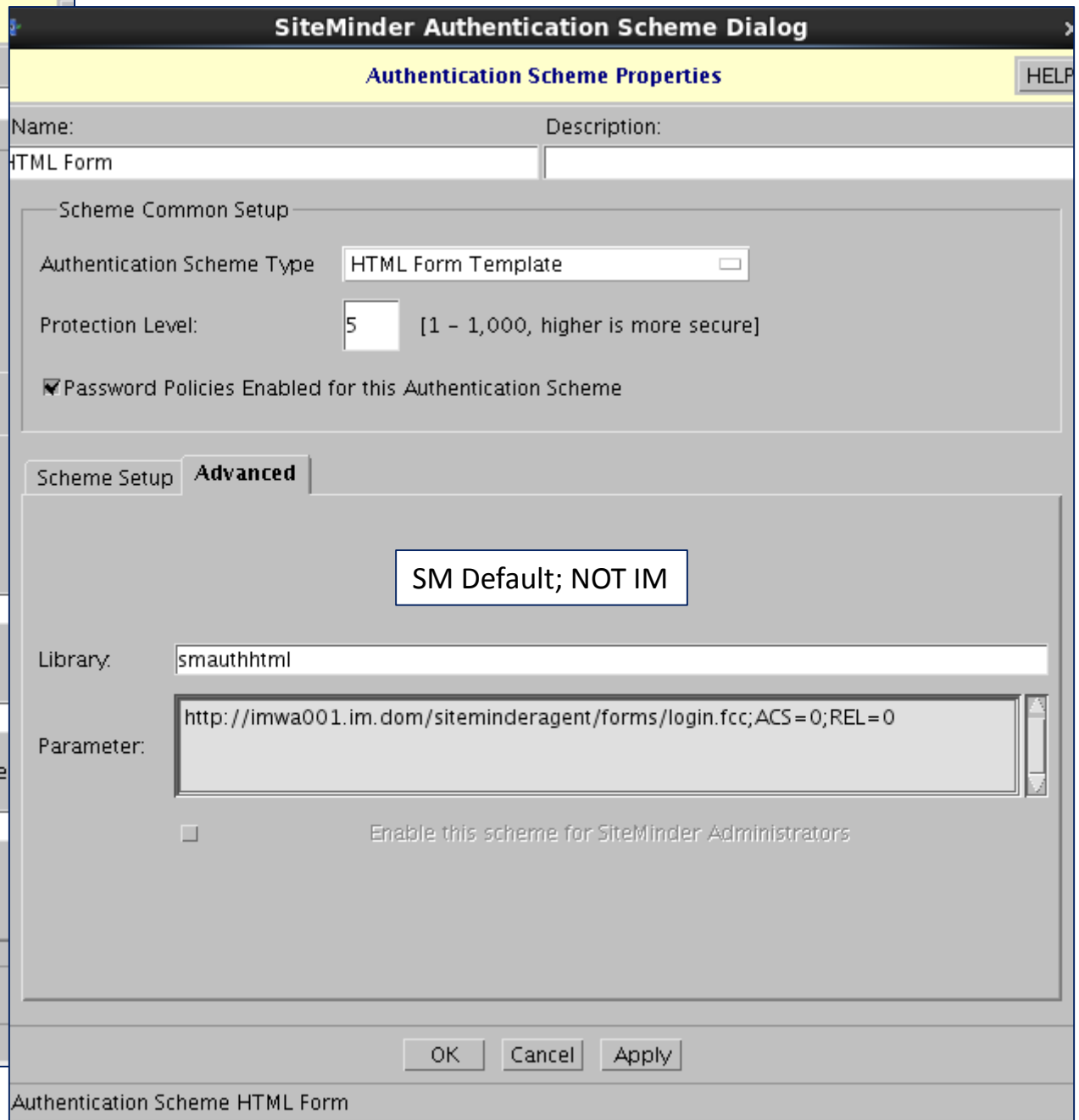

SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
HELP
*Name:
Description:
cam__idm_anon_auth
Scheme Common Setup
Authentication Scheme Type
Anonymous Template
Protection Level:
5
[0 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
Policies associated with this user will apply to anonymous users:
* User DN:
uid=idmpublic,ou=people,ou=im001,ou=cam,o=ca
Lookup
OK
Cancel
Apply
Authentication Scheme cam__idm_anon_auth

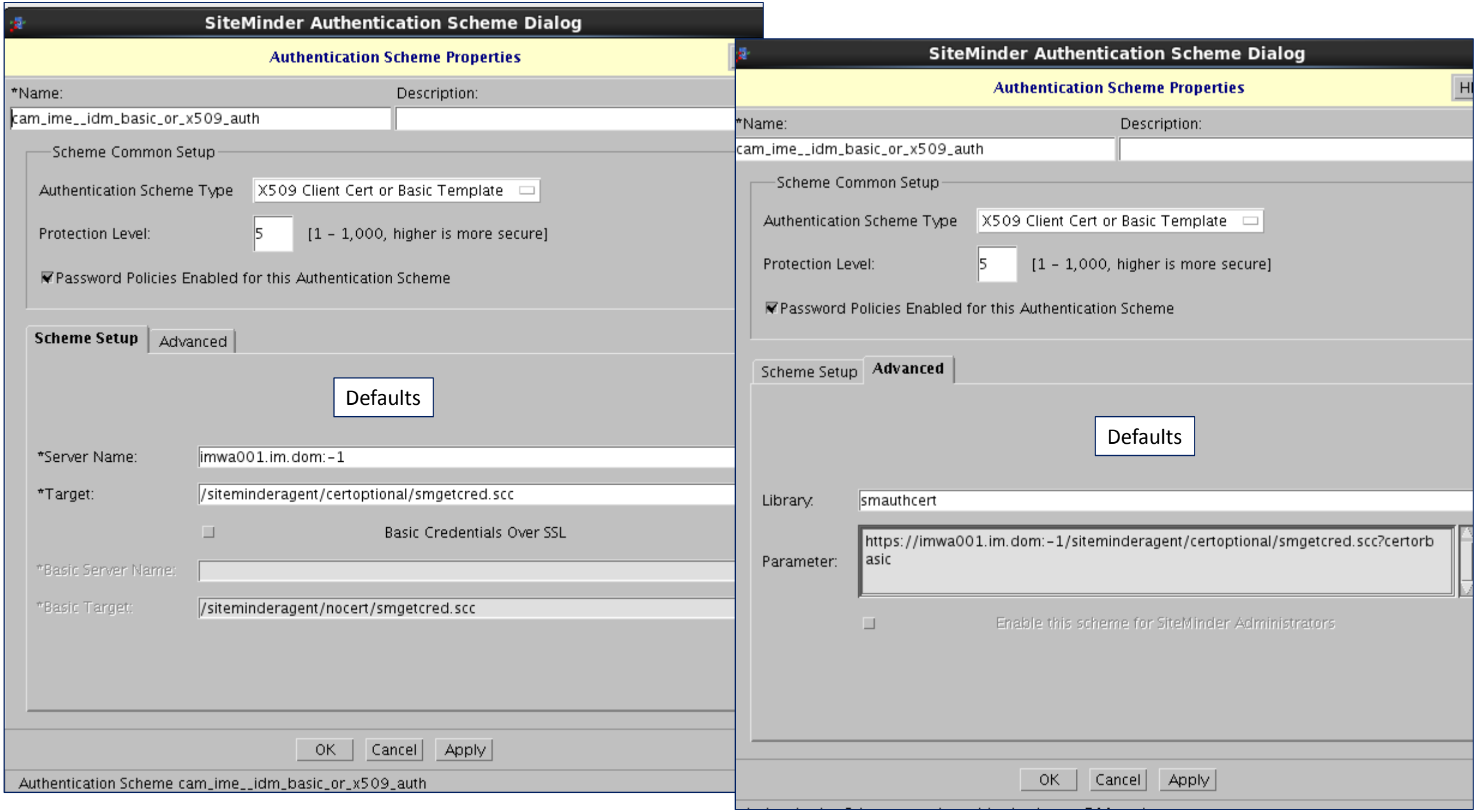

SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Description:
cam__idm_anon_auth
Scheme Common Setup
Authentication Scheme Type
Anonymous Template
Protection Level:
5
[0 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
Library:
smauthanon
Parameter:
uid=idmpublic,ou=people,ou=im001,ou=cam,o=ca
Enable this scheme for SiteMinder Administr
OK
Cancel
Apply
Authentication Scheme cam__idm_anon_auth

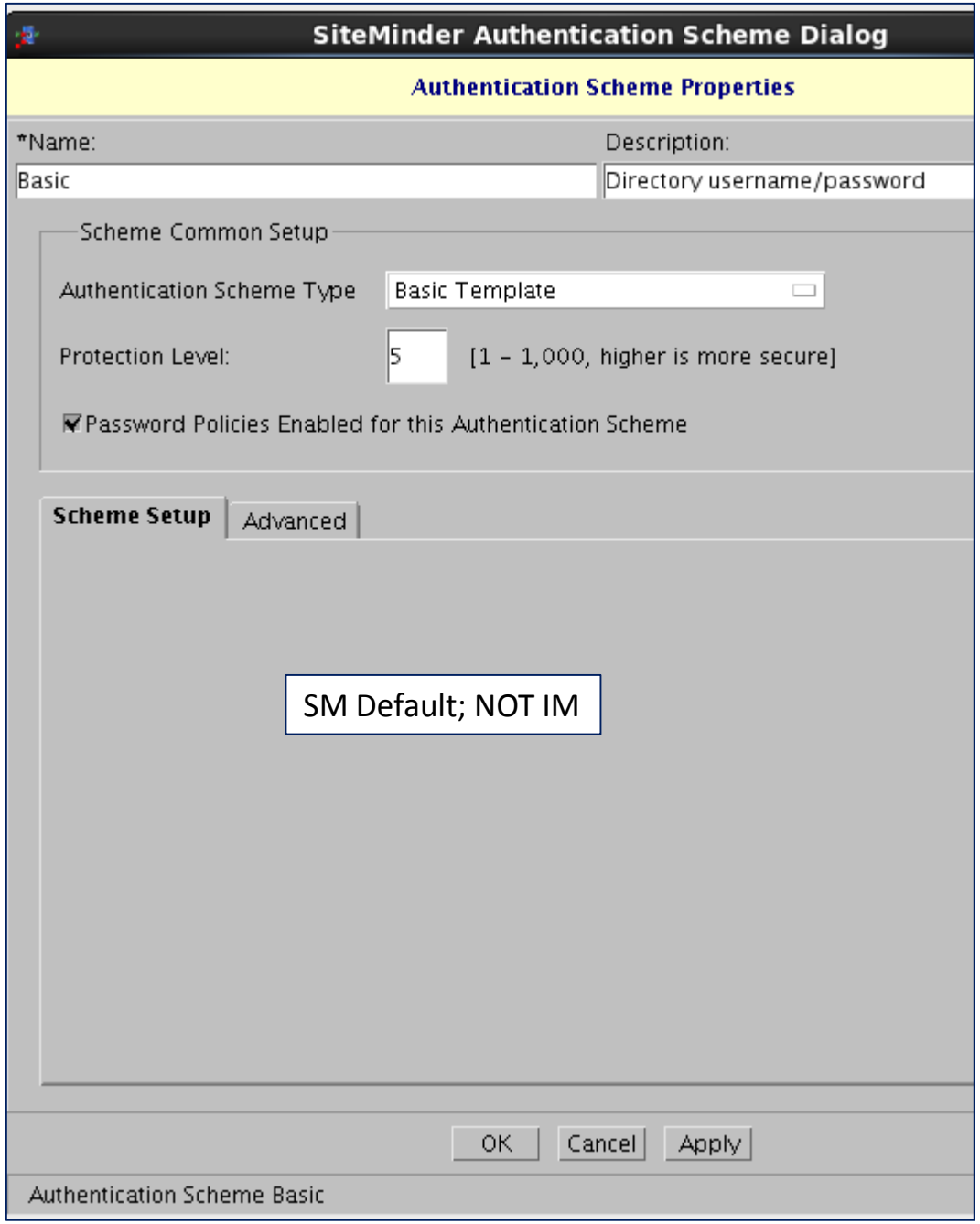

SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Description:
cam__idm_default_auth
Scheme Common Setup
Authentication Scheme Type
Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
OK
Cancel
Apply
Authentication Scheme cam__idm_default_auth

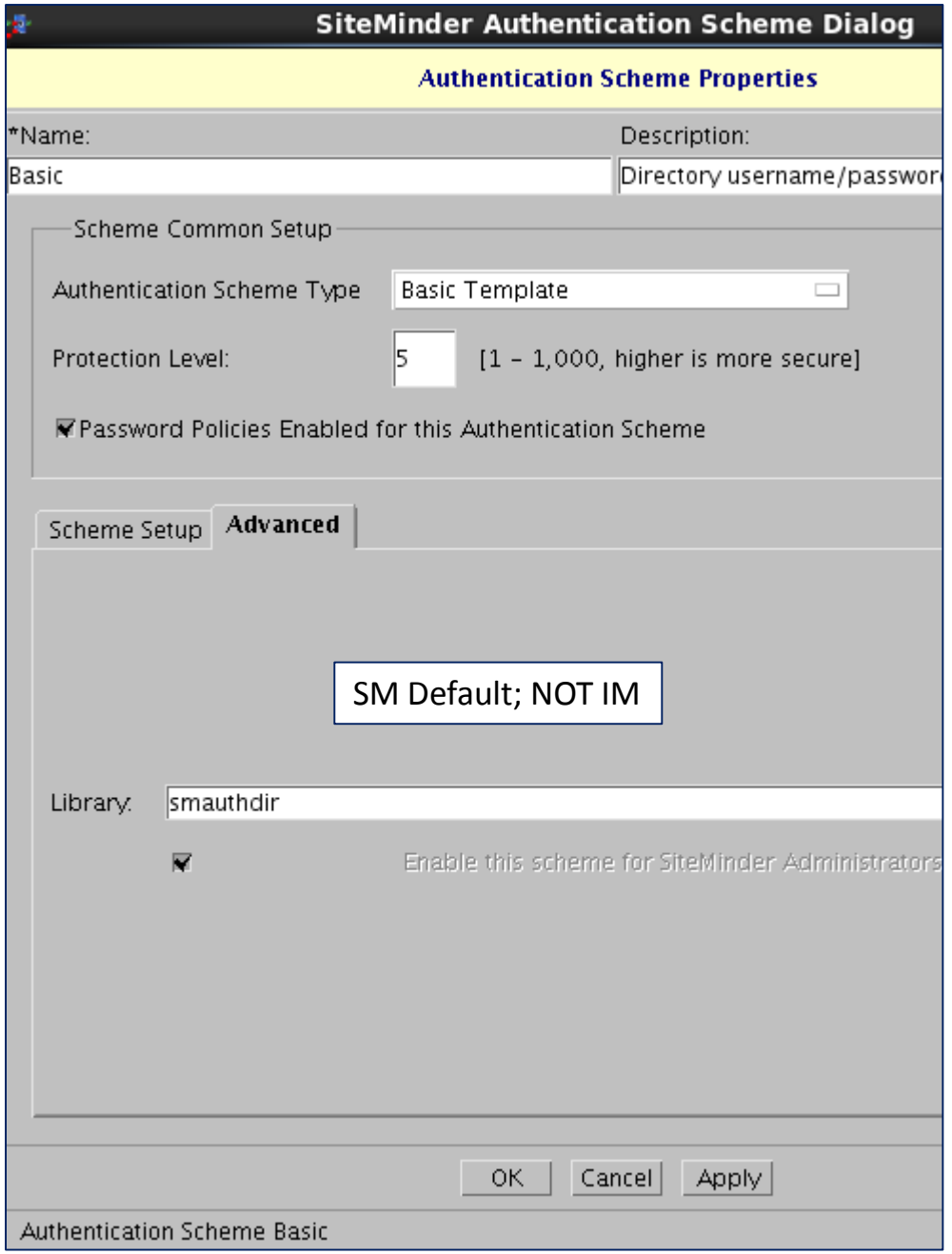

SiteMinder Authentication Scheme Dialo
Authentication Scheme Properties
*Name:
Description:
cam__idm_default_auth
Scheme Common Setup
Authentication Scheme Type
Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
Library:
smauthdir
Enable this scheme for SiteMinder Administra
OK
Cancel
Apply
Authentication Scheme cam__idm_default_auth


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Description:
HTML Form
Scheme Common Setup
Authentication Scheme Type
HTML Form Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
SM Default; NOT IM
Use Relative Target
Web Server Name:
imwa001.im.dom
Use SSL Connection
*Target:
/siteminderagent/forms/login.fcc
Allow this scheme to save credential
Support non-browser clie
Additional Attribute Li
OK
Cancel
Apply
Authentication Scheme HTML Form


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
HELP
Name:
Description:
HTML Form
Scheme Common Setup
Authentication Scheme Type
HTML Form Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
SM Default; NOT IM
Library:
smauthhtml
Parameter:
http://imwa001.im.dom/siteminderagent/forms/login.fcc;ACS=0;REL=0
Enable this scheme for SiteMinder Administrators
OK
Cancel
Apply
Authentication Scheme HTML Form


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Description:
cam_ime__idm_basic_or_x509_auth
Scheme Common Setup
Authentication Scheme Type
X509 Client Cert or Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
*Server Name:
imwa001.im.dom:-1
*Target:
/siteminderagent/certoptional/smgetcred.scc
Basic Credentials Over SSL
*Basic Server Name:
*Basic Target:
/siteminderagent/nocert/smgetcred.scc
OK
Cancel
Apply
Authentication Scheme cam_ime__idm_basic_or_x509_auth
SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Description:
cam_ime__idm_basic_or_x509_auth
Scheme Common Setup
Authentication Scheme Type
X509 Client Cert or Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
Defaults
Library:
smauthcert
Parameter:
https://imwa001.im.dom:-1/siteminderagent/certoptional/smgetcred.scc?certorbasic
Enable this scheme for SiteMinder Administrators
OK
Cancel
Apply


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Basic
Description:
Directory username/password
Scheme Common Setup
Authentication Scheme Type
Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
SM Default; NOT IM
OK
Cancel
Apply
Authentication Scheme Basic


SiteMinder Authentication Scheme Dialog
Authentication Scheme Properties
*Name:
Basic
Description:
Directory username/passwor
Scheme Common Setup
Authentication Scheme Type
Basic Template
Protection Level:
5
[1 - 1,000, higher is more secure]
Password Policies Enabled for this Authentication Scheme
Scheme Setup
Advanced
SM Default; NOT IM
Library:
smauthdir
Enable this scheme for SiteMinder Administrators
OK
Cancel
Apply
Authentication Scheme Basic

SiteMinder Domain Objects

The IM:SM integration will make a new unique SM domain for the IME.

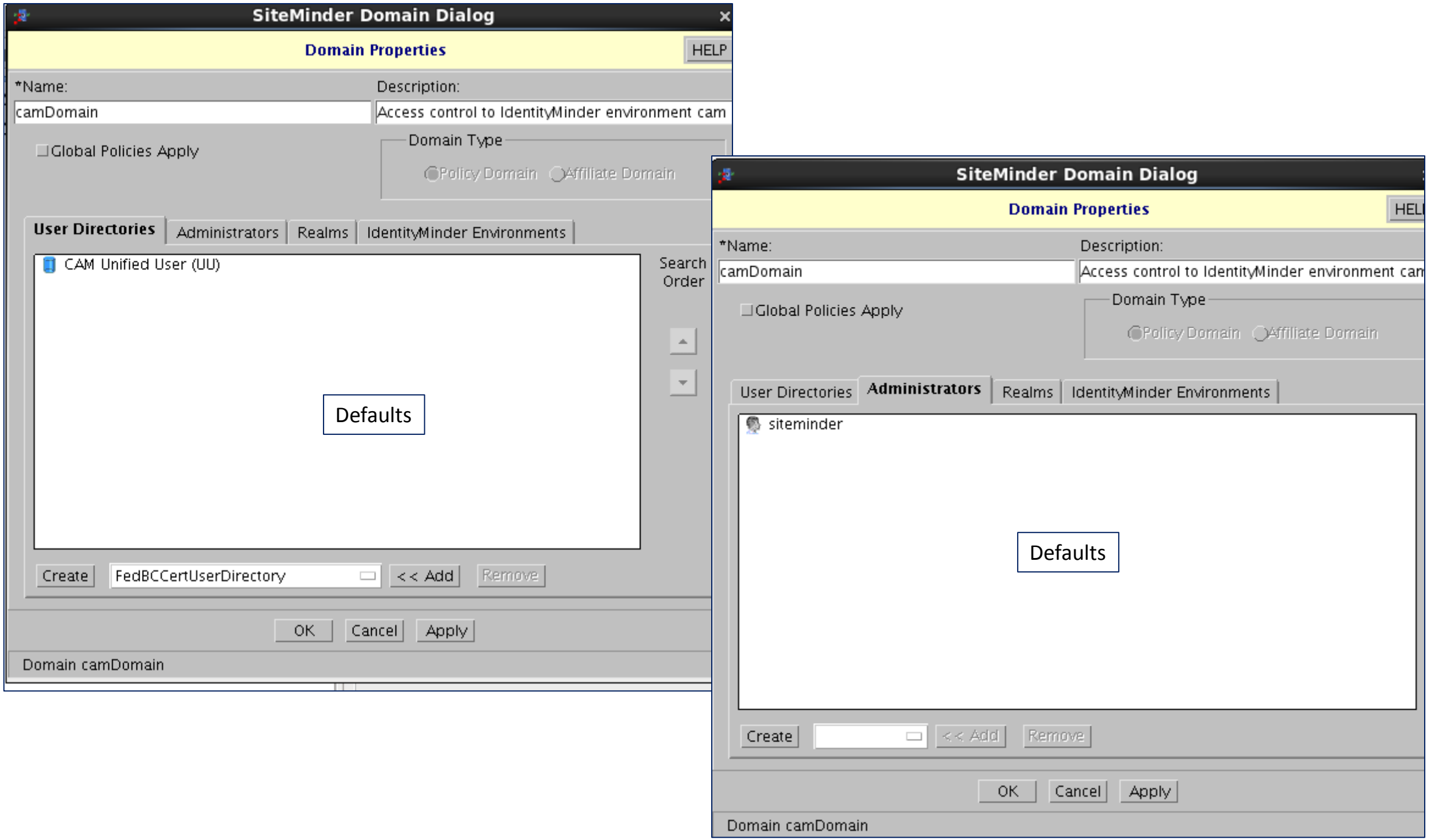
This new SM domain will be labeled after the IME and create two (2) Realms (protected/public)

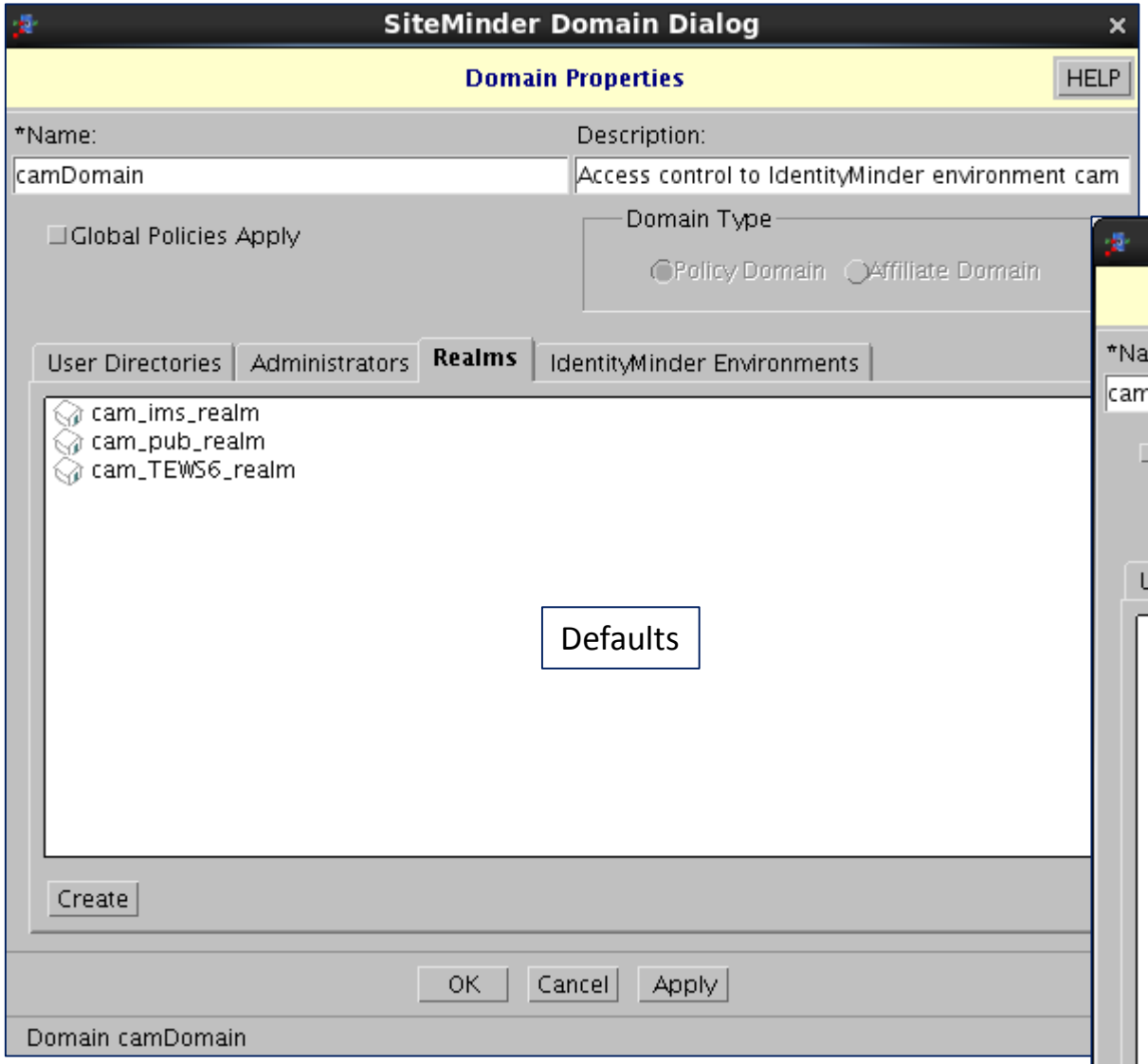
The protected realm will be labeled IME_ims_realm
The public realm will be labeled IME_pub_realm

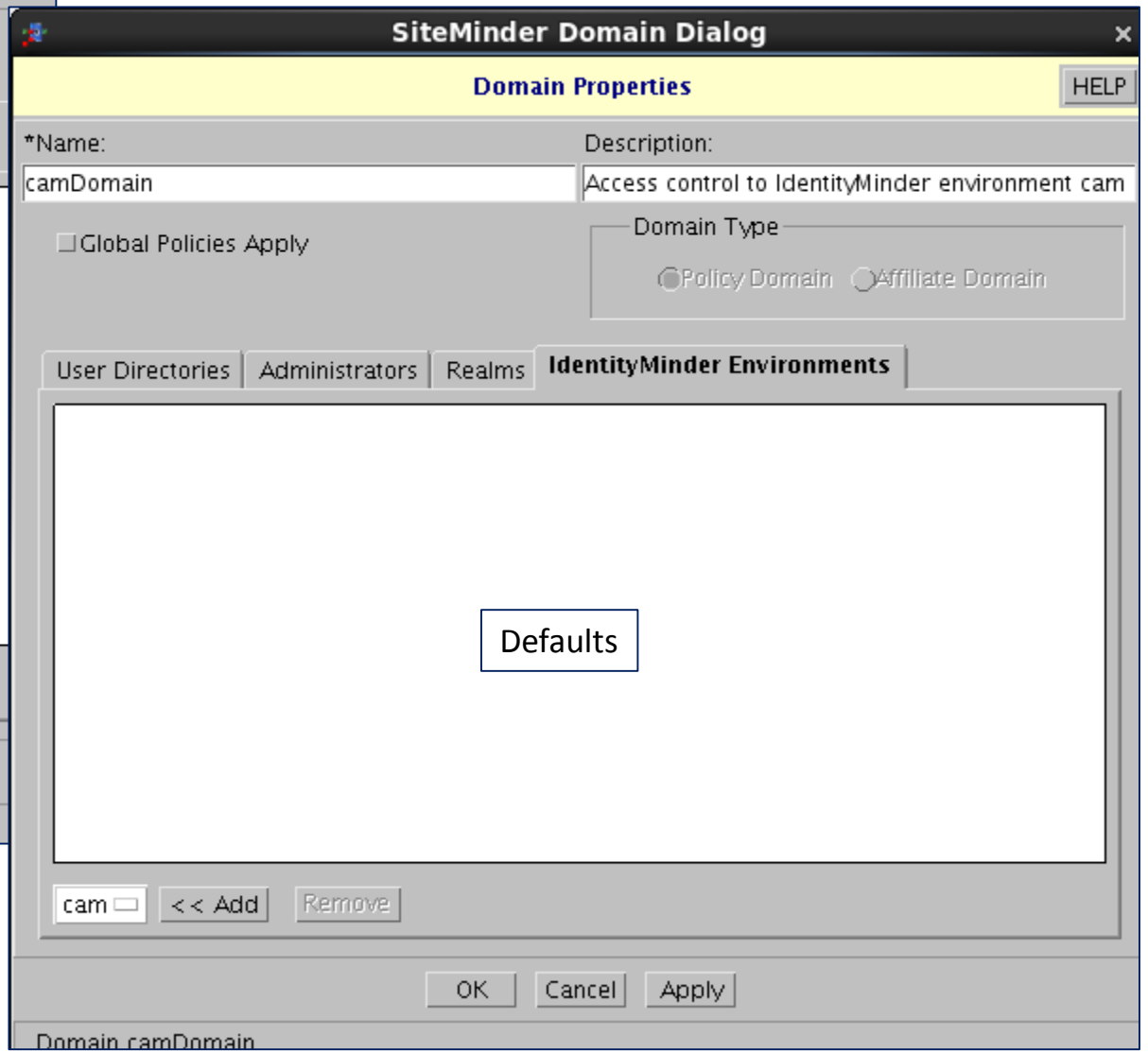
The TEWS6 realm will ONLY be created when the IME Advanced Settings for Web Services is enabled for SM Basic Auth. Validated with XPSExport before & after updating this setting.

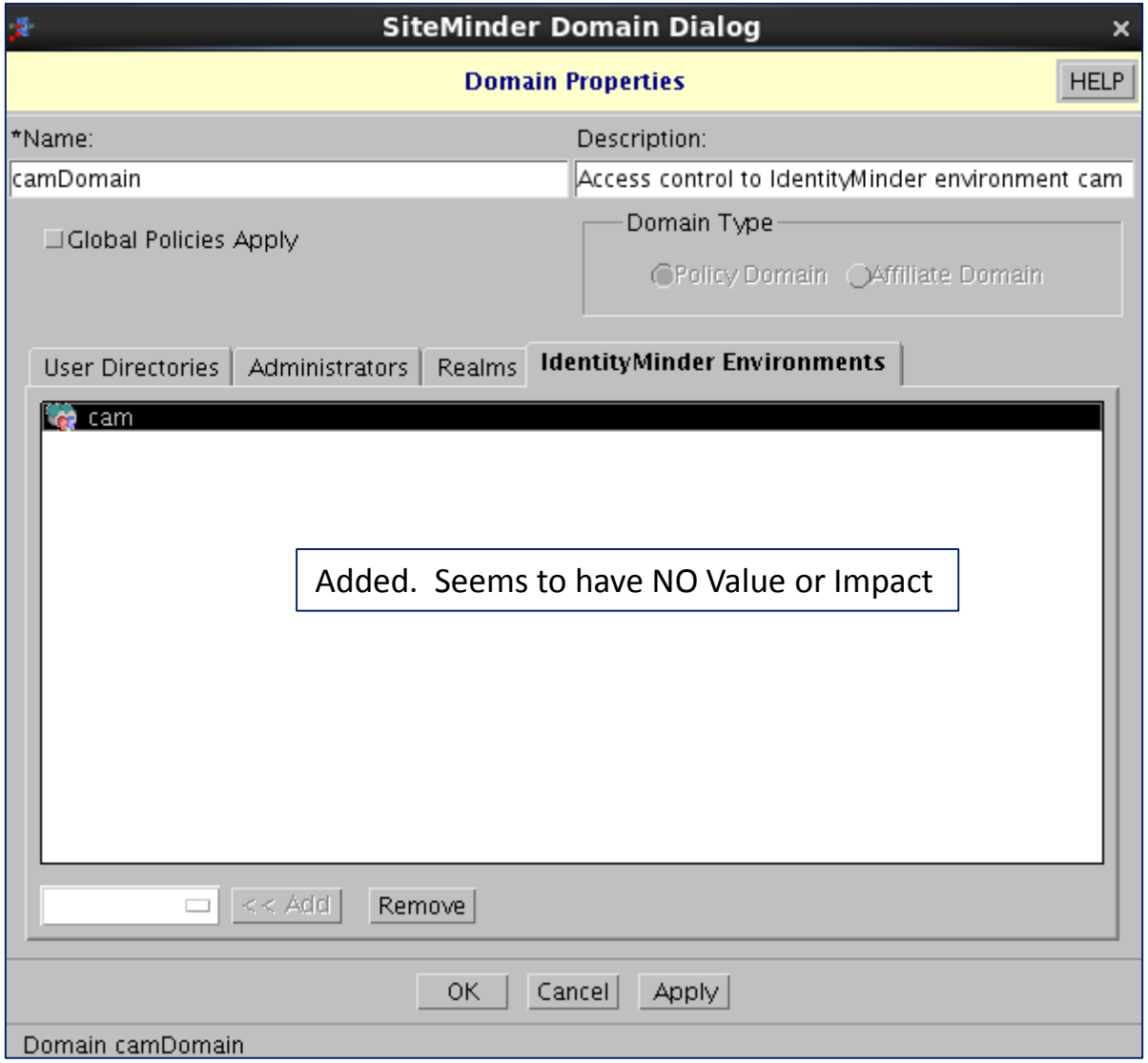
The TEWS6 realm will be labeled IME_TEWS6_realm

Where IME = the real “ime” name


SiteMinder Domain Dialog
Domain Properties
HELP
*Name:
camDomain
Description:
Access control to IdentityMinder environment cam
Global Policies Apply
Domain Type
Policy Domain
Affiliate Domain
User Directories
Administrators
Realms
IdentityMinder Environments
CAM Unified User (UU)
Search Order
Defaults
Create
FedBCCertUserDirectory
<< Add
Remove
OK
Cancel
Apply
Domain camDomain
SiteMinder Domain Dialog
Domain Properties
HELP
*Name:
camDomain
Description:
Access control to IdentityMinder environment cam
Global Policies Apply
Domain Type
Policy Domain
Affiliate Domain
User Directories
Administrators
Realms
IdentityMinder Environments
siteminder
Defaults
Create
<< Add
Remove
OK
Cancel
Apply
Domain camDomain


SiteMinder Domain Dialog
Domain Properties
HELP
*Name:
camDomain
Description:
Access control to IdentityMinder environment cam
Global Policies Apply
Domain Type
Policy Domain
Affiliate Domain
User Directories
Administrators
Realms
IdentityMinder Environments
cam_ims_realm
cam_pub_realm
cam_TEWS6_realm
Defaults
Create
OK
Cancel
Apply
Domain camDomain


SiteMinder Domain Dialog
Domain Properties
HELP
*Name:
camDomain
Description:
Access control to IdentityMinder environment cam
Global Policies Apply
Domain Type
Policy Domain
Affiliate Domain
User Directories
Administrators
Realms
IdentityMinder Environments
Defaults
cam
<< Add
Remove
OK
Cancel
Apply
Domain camDomain

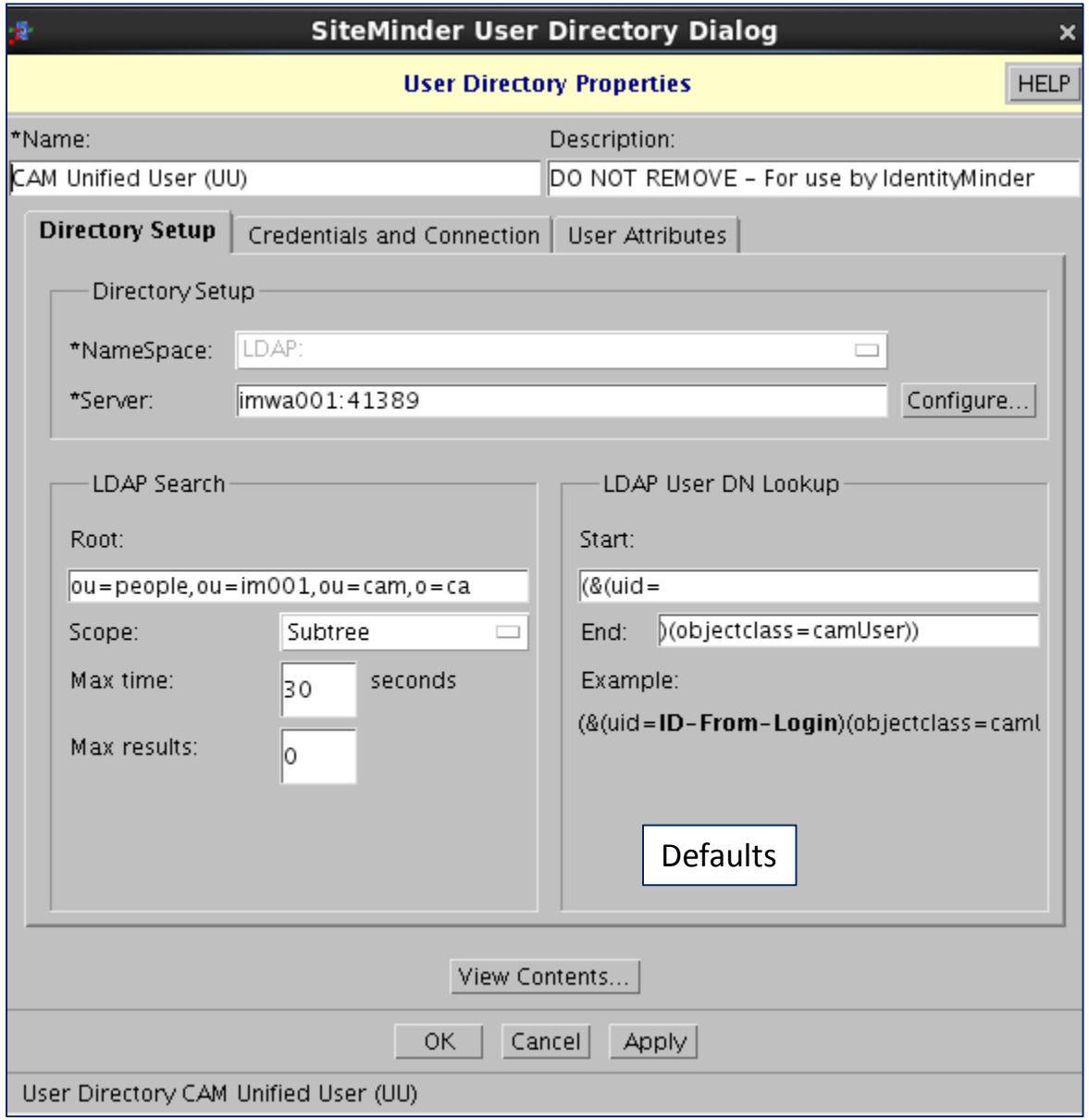

SiteMinder Domain Dialog
Domain Properties
HELP
*Name:
camDomain
Description:
Access control to IdentityMinder environment cam
Global Policies Apply
Domain Type
Policy Domain
Affiliate Domain
User Directories
Administrators
Realms
IdentityMinder Environments
cam
Added. Seems to have NO Value or Impact
<< Add
Remove
OK
Cancel
Apply
Domain camDomain

SiteMinder UserStore Objects

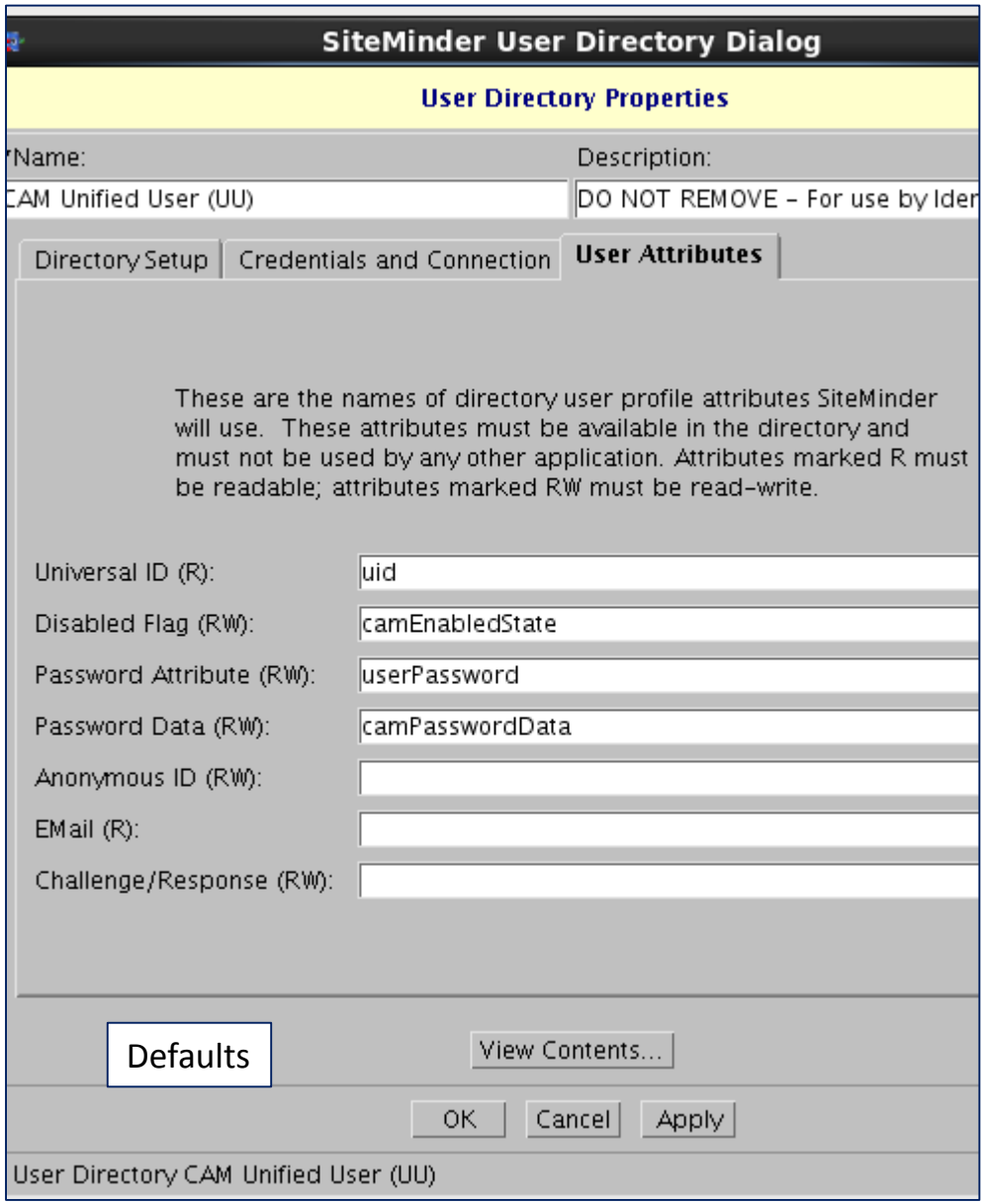
The IM:SM integration will create a userstore object in Siteminder when a new Directory object is created in the IM Management Console via a directory.xml

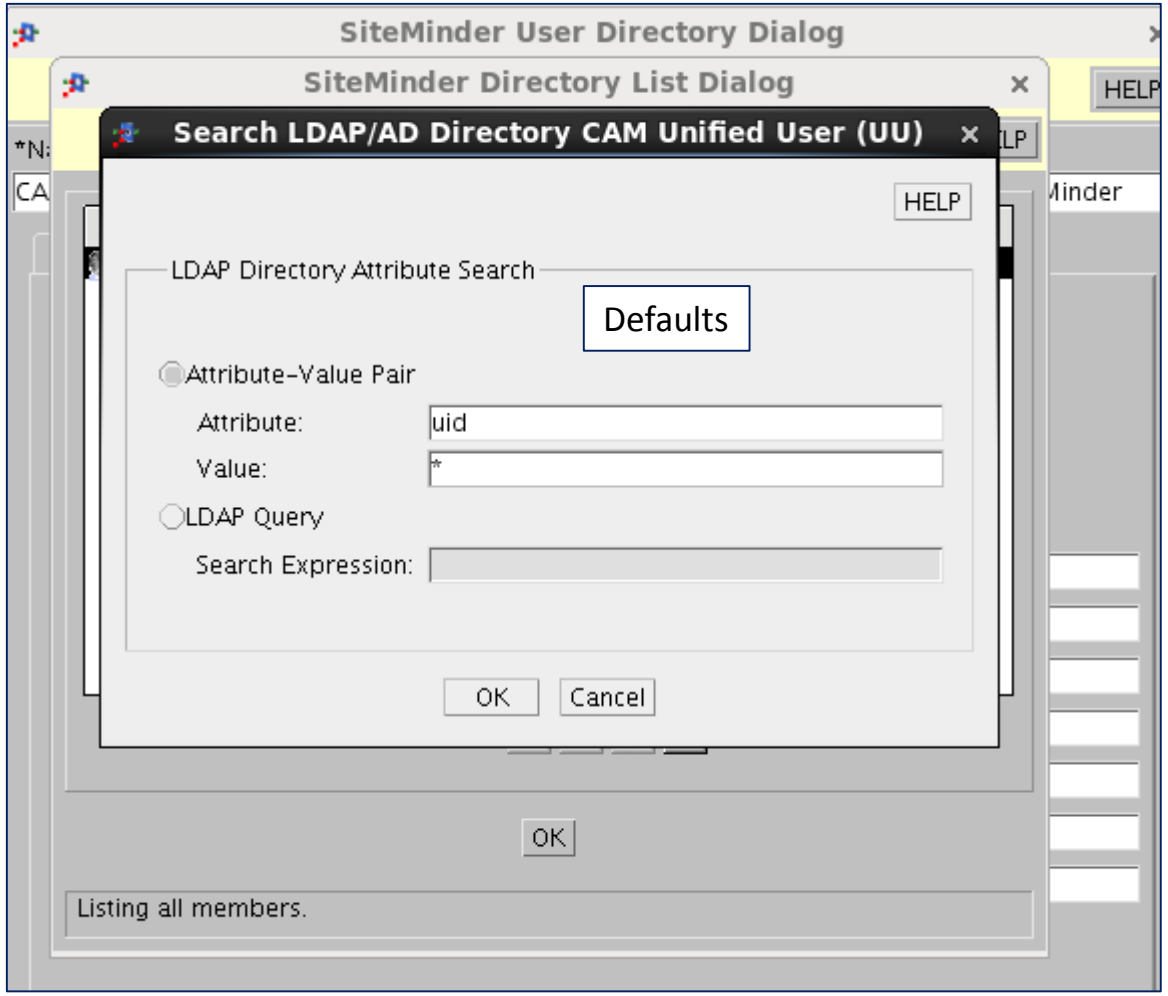
Create the IMCD / IMPS objects first without SSL for LDAPS, to confirm the objects are created.

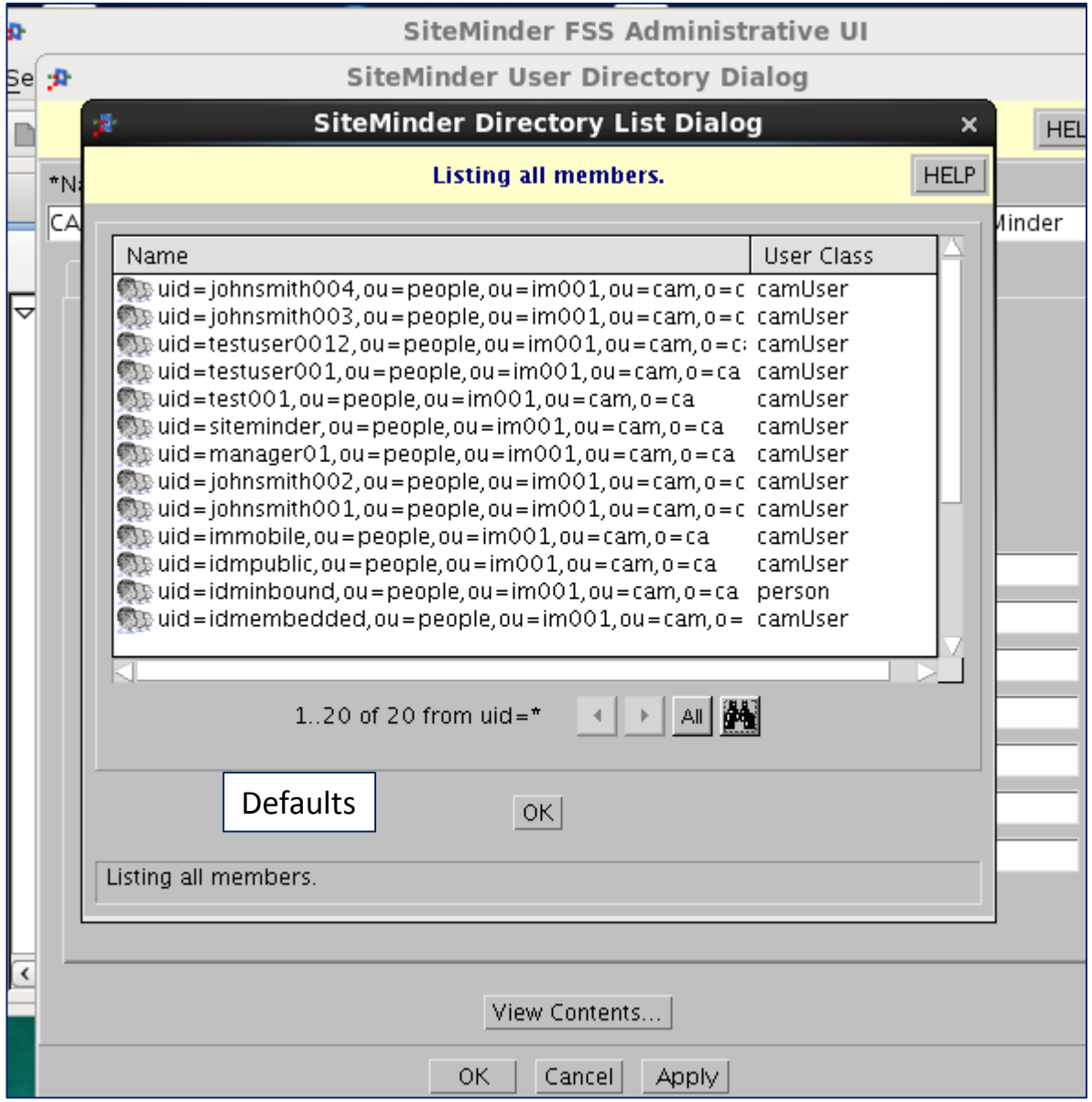
To enable SSL for LDAPS, there are several pre-steps that need to be done.


SiteMinder User Directory Dialog
User Directory Properties
HELP
*Name:
CAM Unified User (UU)
Description:
DO NOT REMOVE – For use by IdentityMinder
Directory Setup
Credentials and Connection
User Attributes
Directory Setup
*NameSpace:
LDAP:
*Server:
imwa001:41389
Configure...
LDAP Search
Root:
ou=people,ou=im001,ou=cam,o=ca
Scope:
Subtree
Max time:
30
seconds
Max results:
0
LDAP User DN Lookup
Start:
(&(uid=
End:
)(objectclass=camUser))
Example:
(&(uid=ID-From-Login)(objectclass=caml
Defaults
View Contents...
OK
Cancel
Apply
User Directory CAM Unified User (UU)


SiteMinder User Directory Dialog
User Directory Properties
HELP
*Name:
CAM Unified User (UU)
Description:
DO NOT REMOVE – For use by IdentityMinder
Directory Setup
Credentials and Connection
User Attributes
Administrator Credentials
Require Credentials
*Username:
uid=idmadmin,ou=people,ou=imC
*Password:
****
*Confirm Password:
****
Run in Authenticated User's Security Context
Secure Connection
Defaults
View Contents...
OK
Cancel
Apply
User Directory CAM Unified User (UU)

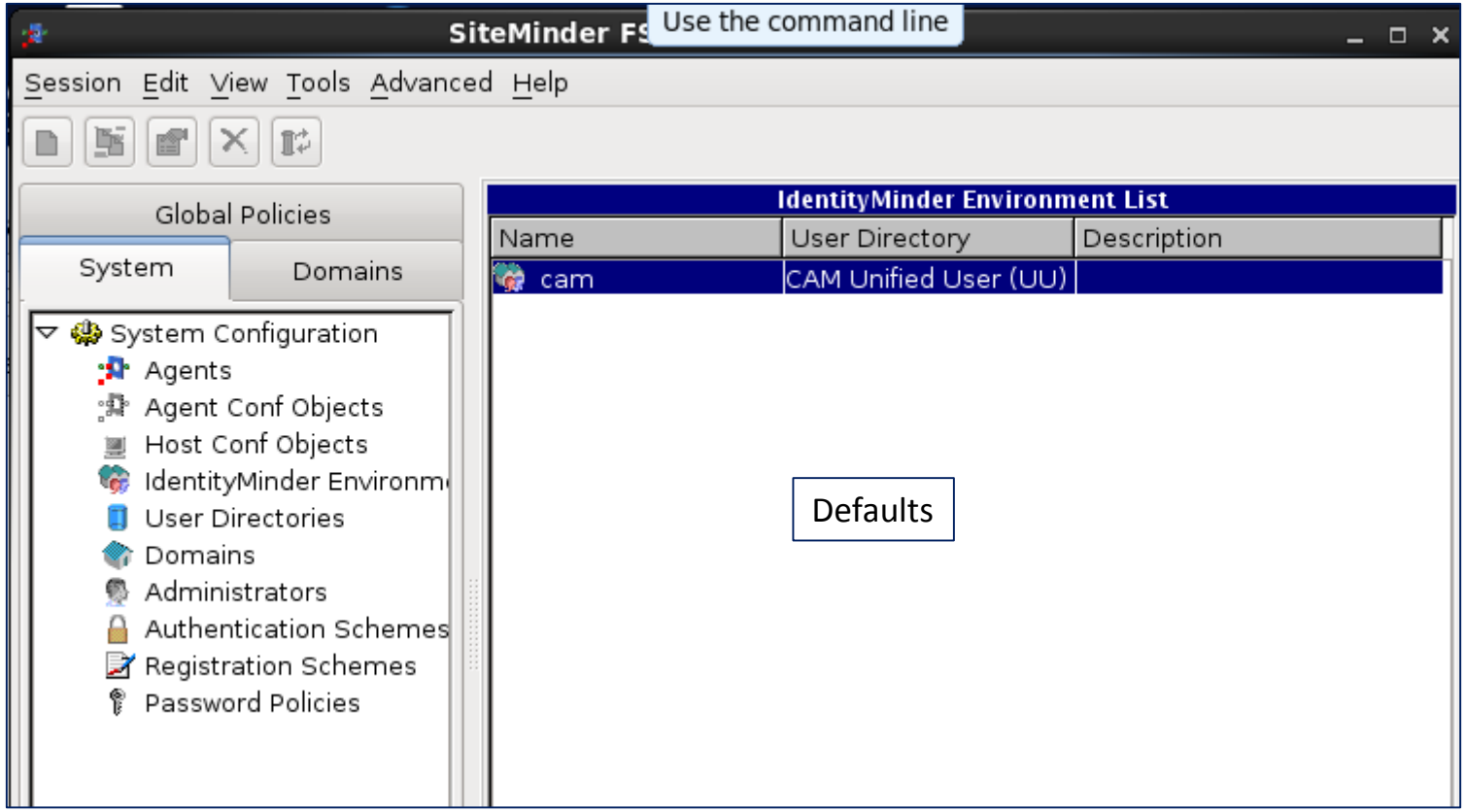

SiteMinder User Directory Dialog
User Directory Properties
Name:
Description:
CAM Unified User (UU)
DO NOT REMOVE - For use by Ider
Directory Setup
Credentials and Connection
User Attributes
These are the names of directory user profile attributes SiteMinder will use. These attributes must be available in the directory and must not be used by any other application. Attributes marked R must be readable; attributes marked RW must be read-write.
Universal ID (R):
uid
Disabled Flag (RW):
camEnabledState
Password Attribute (RW):
userPassword
Password Data (RW):
camPasswordData
Anonymous ID (RW):
EMail (R):
Challenge/Response (RW):
Defaults
View Contents...
OK
Cancel
Apply
User Directory CAM Unified User (UU)


SiteMinder User Directory Dialog
SiteMinder Directory List Dialog
Search LDAP/AD Directory CAM Unified User (UU)
HELP
LDAP Directory Attribute Search
Defaults
Attribute-Value Pair
Attribute:
uid
Value:
*
LDAP Query
Search Expression:
OK
Cancel
OK
Listing all members.


SiteMinder FSS Administrative UI
SiteMinder User Directory Dialog
SiteMinder Directory List Dialog
Listing all members.
HELP
Name
User Class
uid=johnsmith004,ou=people,ou=im001,ou=cam,o=c camUser
uid=johnsmith003,ou=people,ou=im001,ou=cam,o=c camUser
uid=testuser0012,ou=people,ou=im001,ou=cam,o=c: camUser
uid=testuser001,ou=people,ou=im001,ou=cam,o=ca camUser
uid=test001,ou=people,ou=im001,ou=cam,o=ca camUser
uid=siteminder,ou=people,ou=im001,ou=cam,o=ca camUser
uid=manager01,ou=people,ou=im001,ou=cam,o=ca camUser
uid=johnsmith002,ou=people,ou=im001,ou=cam,o=c camUser
uid=johnsmith001,ou=people,ou=im001,ou=cam,o=c camUser
uid=immobile,ou=people,ou=im001,ou=cam,o=ca camUser
uid=idmpublic,ou=people,ou=im001,ou=cam,o=ca camUser
uid=idminbound,ou=people,ou=im001,ou=cam,o=ca person
uid=idmembedded,ou=people,ou=im001,ou=cam,o= camUser
1..20 of 20 from uid=*
All
Defaults
OK
Listing all members.
View Contents...
OK
Cancel
Apply

SiteMinder IM Environment Object

The IM:SM integration will create an IM environment object, but this seems to have little use or function

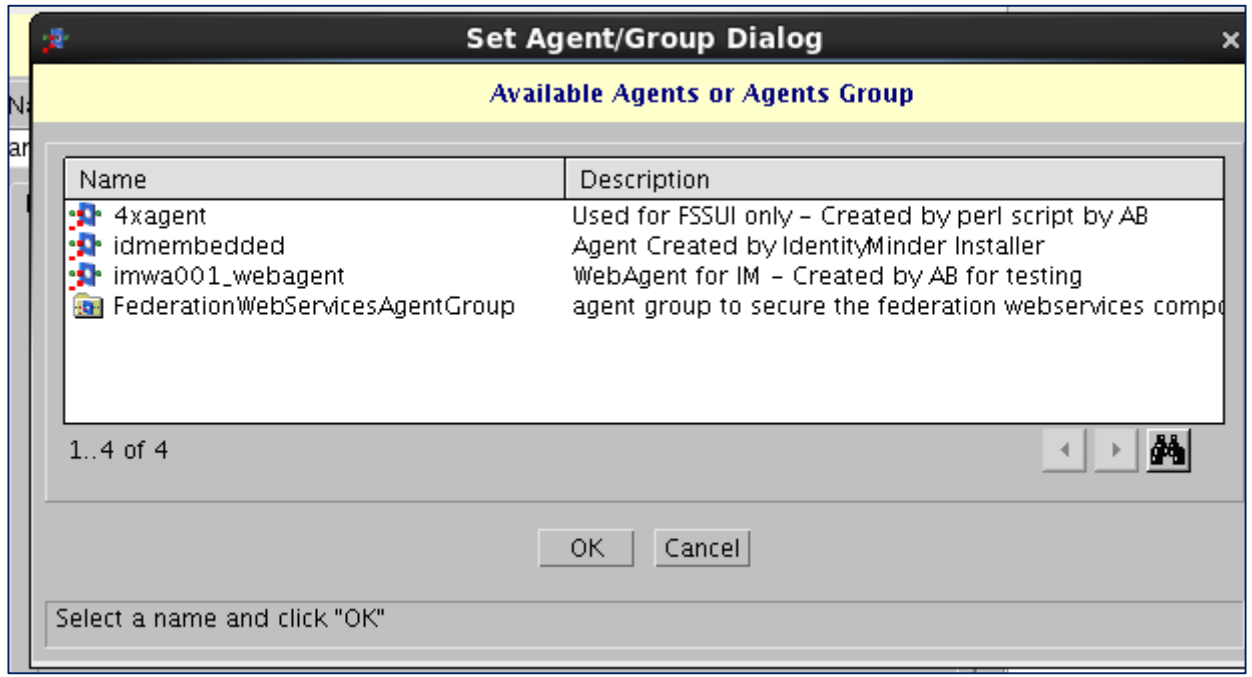

SiteMinder FS
Use the command line
Session Edit View Tools Advanced Help
Global Policies
System
Domains
System Configuration
Agents
Agent Conf Objects
Host Conf Objects
IdentityMinder Environm
User Directories
Domains
Administrators
Authentication Schemes
Registration Schemes
Password Policies
IdentityMinder Environment List
Name
User Directory
Description
cam
CAM Unified User (UU)
Defaults

SiteMinder Web Agent Object

The IM:SM integration will ask for an web agent information & require that a HCO/ACO object exist prior.

Upon IM:SM integration, the web agent will be created for primary IM:SM tunnel agent functionality.

This agent will be used, with the IM's ra.xml & IM library on SM Policy Server to communicate to SiteMinder.


Set Agent/Group Dialog
Available Agents or Agents Group
Name
Description
4xagent
Used for FSSUI only - Created by perl script by AB
idmembedded
Agent Created by IdentityMinder Installer
imwa001_webagent
WebAgent for IM - Created by AB for testing
FederationWebServicesAgentGroup
agent group to secure the federation webservices compo
1..4 of 4
OK
Cancel
Select a name and click "OK"

HOW TO CHANGE THE PASSWORD FOR BLC

Create an INPUT FILE with three tokens and values

The password will be clear text in the input file and then converted to CRYPT format

NOTE: serverUrl does NOT need to have WSDL defined at the end, but it can be useful to have for reference
No impact if ?wsdl is added.

user=idmadmin

password=Password01

serverUrl=https://imwa001.im.dom/iam/im/TEWS6/cam?wsdl

Execute the following line:

#imbulkloadclient.bat --storeEndpointInfo --endpointInfoFile I:\im_win_blc\caim-bulk-loader\conf\imblc_input_file.txt

#IM Bulk Loader invoked ...

#Loaded configuration options from properties file: I:\im_win_blc\caim-bulk-loader\conf\imblc_input_file.txt

#Storing server URL: https://imwa001.im.dom/iam/im/TEWS6/cam

#Storing user name: idmadmin

#Storing obfuscated password: devrhQ2YEm5RE0IGa3tyoPkiTOe0uYNpgjS1Zlsz9B8=

#End point information stored in configuration file: ../conf/imbulkloadclient.properties

https://support.ca.com/cadocs/0/CA%20Identity%20Manager%2012%206%204-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?676576.html?intcmp=searchresultclick&resultnum=1227

Test with SOAP-UI to BLC IM ObjectFeeder Task

The BLC functionality may be emulated with the SOAP-UI tool, http://www.soapui.org/

The IM TEWS6 protocol uses SOAP for requests & submissions.

This was confirmed with Wireshark monitoring the BLC to J2EE server.

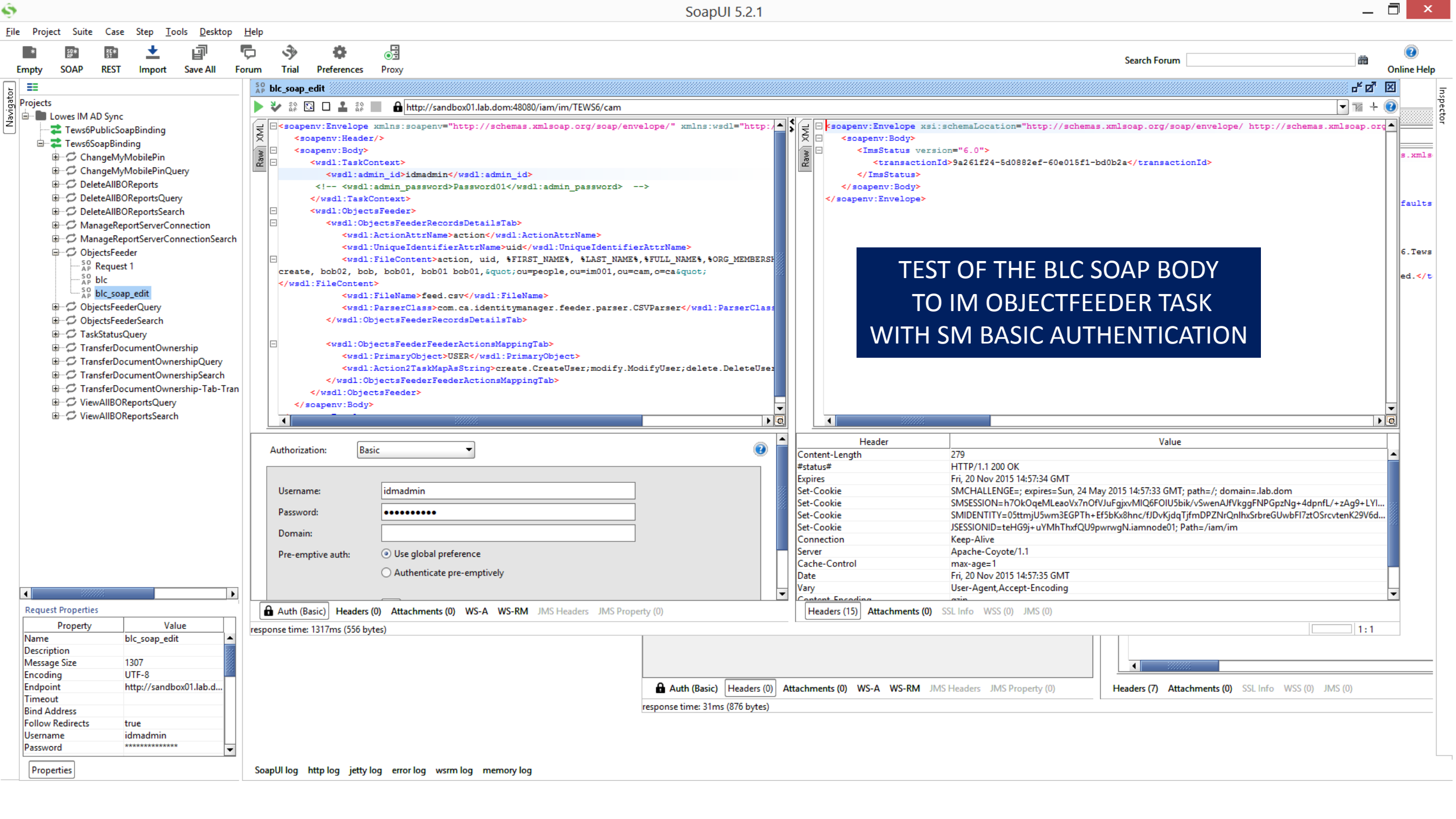
SOAP UI “BLC” BODY FORMAT

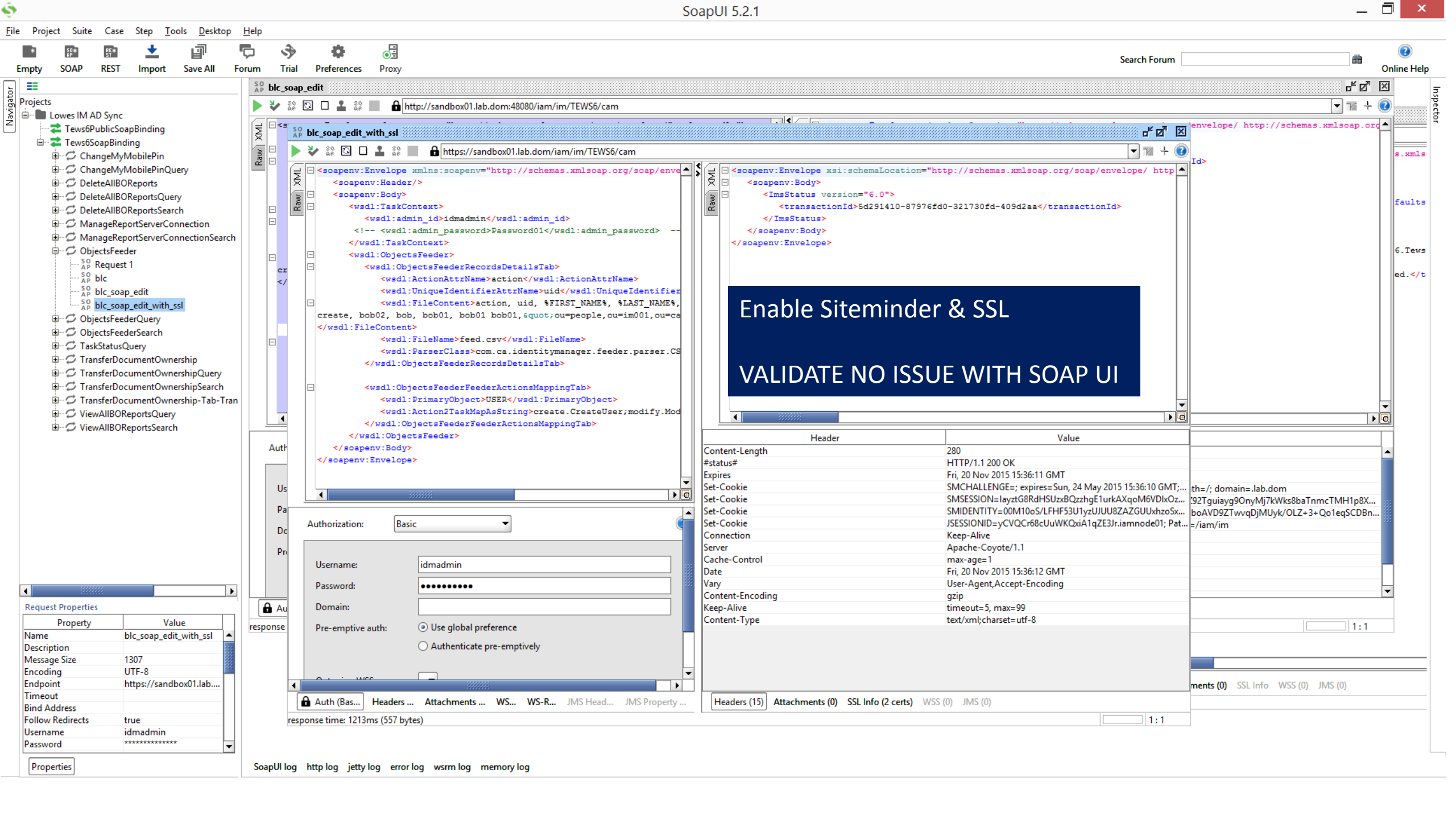
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsdl="http://tews6/wsdl">
  <soapenv:Header/>

  <soapenv:Body>
    <wsdl:TaskContext>
      <wsdl:admin_id>idmadmin</wsdl:admin_id>
     <!-- <wsdl:admin_password>Password01</wsdl:admin_password>     -->
    </wsdl:TaskContext>

    <wsdl:ObjectsFeeder>
      <wsdl:ObjectsFeederRecordsDetailsTab>
        <wsdl:ActionAttrName>action</wsdl:ActionAttrName>
        <wsdl:UniqueIdentifierAttrName>uid</wsdl:UniqueIdentifierAttrName>
        <wsdl:FileContent>action, uid, %FIRST_NAME%,
%LAST_NAME%,%FULL_NAME%,%ORG_MEMBERSHIP%
create, bob02, bob, bob01, bob01
bob01,&amp;quot;ou=people,ou=im001,ou=cam,o=ca&amp;quot;
</wsdl:FileContent>
        <wsdl:FileName>feed.csv</wsdl:FileName>

<wsdl:ParserClass>com.ca.identitymanager.feeder.parser.CSVParser</wsdl:ParserClass
>
      </wsdl:ObjectsFeederRecordsDetailsTab>
      <wsdl:ObjectsFeederFeederActionsMappingTab>
        <wsdl:PrimaryObject>USER</wsdl:PrimaryObject>

<wsdl:Action2TaskMapAsString>create.CreateUser;modify.ModifyUser;delete.Delete
User</wsdl:Action2TaskMapAsString>
      </wsdl:ObjectsFeederFeederActionsMappingTab>
    </wsdl:ObjectsFeeder>
  </soapenv:Body>
</soapenv:Envelope>
```

BLC SOAP BODY FORMAT

Captured with WireShark

```
<soapenv:Body>
<TaskContext xmlns="http://tews6/wsdl">
<admin_id>idmadmin</admin_id>
</TaskContext>

<ObjectsFeeder xmlns="http://tews6/wsdl">
<ObjectsFeederRecordsDetailsTab>
<ActionAttrName>action</ActionAttrName>
<UniqueIdentifierAttrName>uid</UniqueIdentifierAttrName>
<FileContent>action, uid, %FIRST_NAME%,
%LAST_NAME%,%FULL_NAME%,%ORG_MEMBERSHIP%
create, bob02, bob, bob01, bob01
bob01,&amp;quot;ou=people,ou=im001,ou=cam,o=ca&amp;quot;
</FileContent>
<FileName>b.csv</FileName>

<ParserClass>com.ca.identitymanager.feeder.parser.CSVParser</ParserClass>

</ObjectsFeederRecordsDetailsTab>
<ObjectsFeederFeederActionsMappingTab>
<PrimaryObject>USER</PrimaryObject>

<Action2TaskMapAsString>create.CreateUser;modify.ModifyUser;delete.Delete
User</Action2TaskMapAsString>
</ObjectsFeederFeederActionsMappingTab>
</ObjectsFeeder>
</soapenv:Body>
```


SoapUI 5.2.1
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Projects
Lowes IM AD Sync
Tews6PublicSoapBinding
Tews6SoapBinding
ChangeMyMobilePin
ChangeMyMobilePinQuery
DeleteAllBOReports
DeleteAllBOReportsQuery
DeleteAllBOReportsSearch
ManageReportServerConnection
ManageReportServerConnectionSearch
ObjectsFeeder
Request 1
blc
blc_soap_edit
ObjectsFeederQuery
ObjectsFeederSearch
TaskStatusQuery
TransferDocumentOwnership
TransferDocumentOwnershipQuery
TransferDocumentOwnershipSearch
TransferDocumentOwnership-Tab-Tran
ViewAllBOReportsQuery
ViewAllBOReportsSearch
blc_soap_edit
http://sandbox01.lab.dom:48080/iam/im/TEWS6/cam
XML
Raw
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsdl="http:/
<soapenv:Header/>
<soapenv:Body>
<wsdl:TaskContext>
<wsdl:admin_id>idmadmin</wsdl:admin_id>
<!-- <wsdl:admin_password>Password01</wsdl:admin_password> -->
</wsdl:TaskContext>
<wsdl:ObjectsFeeder>
<wsdl:ObjectsFeederRecordsDetailsTab>
<wsdl:ActionAttrName>action</wsdl:ActionAttrName>
<wsdl:UniqueIdentifierAttrName>uid</wsdl:UniqueIdentifierAttrName>
<wsdl:FileContent>action, uid, %FIRST_NAME%, %LAST_NAME%,%FULL_NAME%,%ORG_MEMBERSH
create, bob02, bob, bob01, bob01 bob01,"ou=people,ou=im001,ou=cam,o=ca"
</wsdl:FileContent>
<wsdl:FileName>feed.csv</wsdl:FileName>
<wsdl:ParserClass>com.ca.identitymanager.feeder.parser.CSVParser</wsdl:ParserClass
</wsdl:ObjectsFeederRecordsDetailsTab>
<wsdl:ObjectsFeederFeederActionsMappingTab>
<wsdl:PrimaryObject>USER</wsdl:PrimaryObject>
<wsdl:Action2TaskMapAsString>create.CreateUser;modify.ModifyUser;delete.DeleteUse
</wsdl:ObjectsFeederFeederActionsMappingTab>
</wsdl:ObjectsFeeder>
</soapenv:Body>
<soapenv:Envelope xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http://schemas.xmlsoap.org
<soapenv:Body>
<ImsStatus version="6.0">
<transactionId>9a261f24-5d0882ef-60e015f1-bd0b2a</transactionId>
</ImsStatus>
</soapenv:Body>
</soapenv:Envelope>
TEST OF THE BLC SOAP BODY
TO IM OBJECTFEEDER TASK
WITH SM BASIC AUTHENTICATION
Authorization: Basic
Username: idmadmin
Password: ••••••••••
Domain:
Pre-emptive auth: Use global preference
Authenticate pre-emptively
Auth (Basic) Headers (0) Attachments (0) WS-A WS-RM JMS Headers JMS Property (0)
response time: 1317ms (556 bytes)
Header Value
Content-Length 279
#status# HTTP/1.1 200 OK
Expires Fri, 20 Nov 2015 14:57:34 GMT
Set-Cookie SMCHALLENGE=; expires=Sun, 24 May 2015 14:57:33 GMT; path=/; domain=.lab.dom
Set-Cookie SMSESSION=h7OkOqeMLeaoVx7nOfVJuFgjxvMIQ6FOIU5bik/vSwenAJfVkggFNPGpzNg+4dpnfL/+zAg9+LYl...
Set-Cookie SMIDENTITY=05tttmjU5wm3EGPTh+Ef5bKx8hnc/fJDvKjdqTjfmDPZNrQnlhxSrbreGUwbFI7ztOSrcvtenK29V6d...
Set-Cookie JSESSIONID=teHG9j+uYMhThxfQU9pwrwgN.iamnode01; Path=/iam/im
Connection Keep-Alive
Server Apache-Coyote/1.1
Cache-Control max-age=1
Date Fri, 20 Nov 2015 14:57:35 GMT
Vary User-Agent,Accept-Encoding
Headers (15) Attachments (0) SSL Info WSS (0) JMS (0)
1 : 1
Request Properties
Property Value
Name blc_soap_edit
Description
Message Size 1307
Encoding UTF-8
Endpoint http://sandbox01.lab.d...
Timeout
Bind Address
Follow Redirects true
Username idmadmin
Password **********
Properties
Auth (Basic) Headers (0) Attachments (0) WS-A WS-RM JMS Headers JMS Property (0)
response time: 31ms (876 bytes)
Headers (7) Attachments (0) SSL Info WSS (0) JMS (0)
SoapUI log http log jetty log error log wsrm log memory log
Inspector


SoapUI 5.2.1
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Projects
Lowes IM AD Sync
Tews6PublicSoapBinding
Tews6SoapBinding
ChangeMyMobilePin
ChangeMyMobilePinQuery
DeleteAllBOReports
DeleteAllBOReportsQuery
DeleteAllBOReportsSearch
ManageReportServerConnection
ManageReportServerConnectionSearch
ObjectsFeeder
Request 1
blc
blc_soap_edit
blc_soap_edit_with_ssl
ObjectsFeederQuery
ObjectsFeederSearch
TaskStatusQuery
TransferDocumentOwnership
TransferDocumentOwnershipQuery
TransferDocumentOwnershipSearch
TransferDocumentOwnership-Tab-Tran
ViewAllBOReportsQuery
ViewAllBOReportsSearch
blc_soap_edit
http://sandbox01.lab.dom:48080/iam/im/TEWS6/cam
blc_soap_edit_with_ssl
https://sandbox01.lab.dom/iam/im/TEWS6/cam
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/enve
<soapenv:Header/>
<soapenv:Body>
<wsdl:TaskContext>
<wsdl:admin_id>idmadmin</wsdl:admin_id>
<!-- <wsdl:admin_password>Password01</wsdl:admin_password> --
</wsdl:TaskContext>
<wsdl:ObjectsFeeder>
<wsdl:ObjectsFeederRecordsDetailsTab>
<wsdl:ActionAttrName>action</wsdl:ActionAttrName>
<wsdl:UniqueIdentifierAttrName>uid</wsdl:UniqueIdentifier
<wsdl:FileContent>action, uid, %FIRST_NAME%, %LAST_NAME%,
create, bob02, bob, bob01, bob01 bob01,"ou=people,ou=im001,ou=ca
</wsdl:FileContent>
<wsdl:FileName>feed.csv</wsdl:FileName>
<wsdl:ParserClass>com.ca.identitymanager.feeder.parser.CS
</wsdl:ObjectsFeederRecordsDetailsTab>
<wsdl:ObjectsFeederFeederActionsMappingTab>
<wsdl:PrimaryObject>USER</wsdl:PrimaryObject>
<wsdl:Action2TaskMapAsString>create.CreateUser;modify.Mod
</wsdl:ObjectsFeederFeederActionsMappingTab>
</wsdl:ObjectsFeeder>
</soapenv:Body>
</soapenv:Envelope>
<soapenv:Envelope xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http
<soapenv:Body>
<ImsStatus version="6.0">
<transactionId>5d291410-87976fd0-321730fd-409d2aa</transactionId>
</ImsStatus>
</soapenv:Body>
</soapenv:Envelope>
Enable Siteminder & SSL
VALIDATE NO ISSUE WITH SOAP UI
Authorization: Basic
Username: idmadmin
Password: ••••••••••
Domain:
Pre-emptive auth: Use global preference
Authenticate pre-emptively
Header Value
Content-Length 280
#status# HTTP/1.1 200 OK
Expires Fri, 20 Nov 2015 15:36:11 GMT
Set-Cookie SMCHALLENGE=; expires=Sun, 24 May 2015 15:36:10 GMT;...
Set-Cookie SMSESSION=layztG8RdHSUzxBQzzhgE1urkAXqoM6VDlxOz...
Set-Cookie SMIDENTITY=00M10oS/LFHF53U1yzUJUU8ZAZGUUxhzoSx...
Set-Cookie JSESSIONID=yCVQCr68cUuWKQxiA1qZE3Jr.iamnode01; Pat...
Connection Keep-Alive
Server Apache-Coyote/1.1
Cache-Control max-age=1
Date Fri, 20 Nov 2015 15:36:12 GMT
Vary User-Agent,Accept-Encoding
Content-Encoding gzip
Keep-Alive timeout=5, max=99
Content-Type text/xml;charset=utf-8
Auth (Bas... Headers ... Attachments ... WS... WS-R... JMS Head... JMS Property ...
Headers (15) Attachments (0) SSL Info (2 certs) WSS (0) JMS (0)
response time: 1213ms (557 bytes)
Request Properties
Property Value
Name blc_soap_edit_with_ssl
Description
Message Size 1307
Encoding UTF-8
Endpoint https://sandbox01.lab....
Timeout
Bind Address
Follow Redirects true
Username idmadmin
Password **********
Properties
SoapUI log http log jetty log error log wsrm log memory log
Inspector

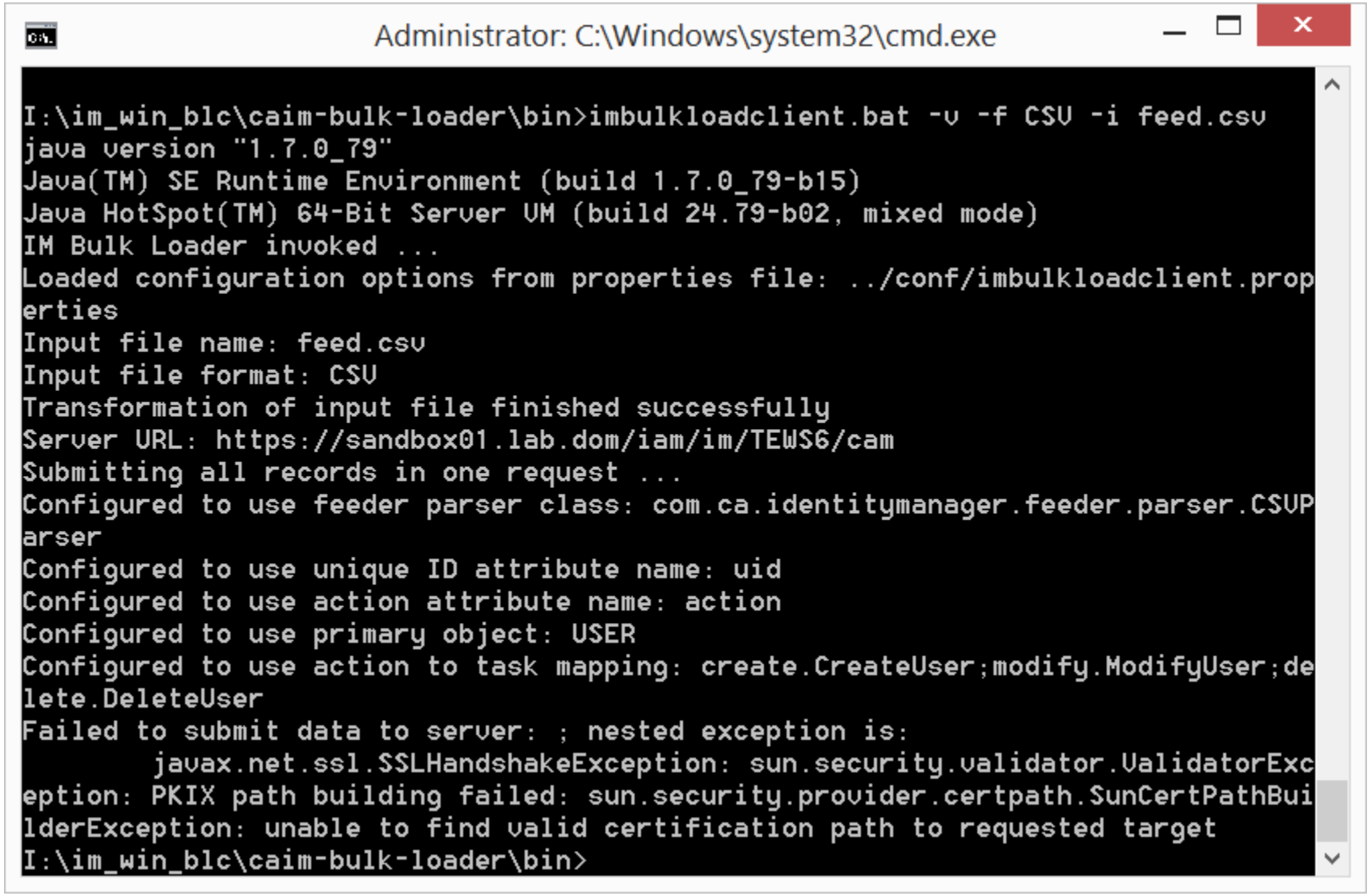
Troubleshoot: BLC Error Message(s): Not Authenticated

- SM Auth enabled (BLC =true & WS SMAuth=true)
  - If WS “Admin ID impersonation” = true & “Admin Password is required” = true
  - BLC will attempt to authenticate just once, but WS will require two (2) logins.

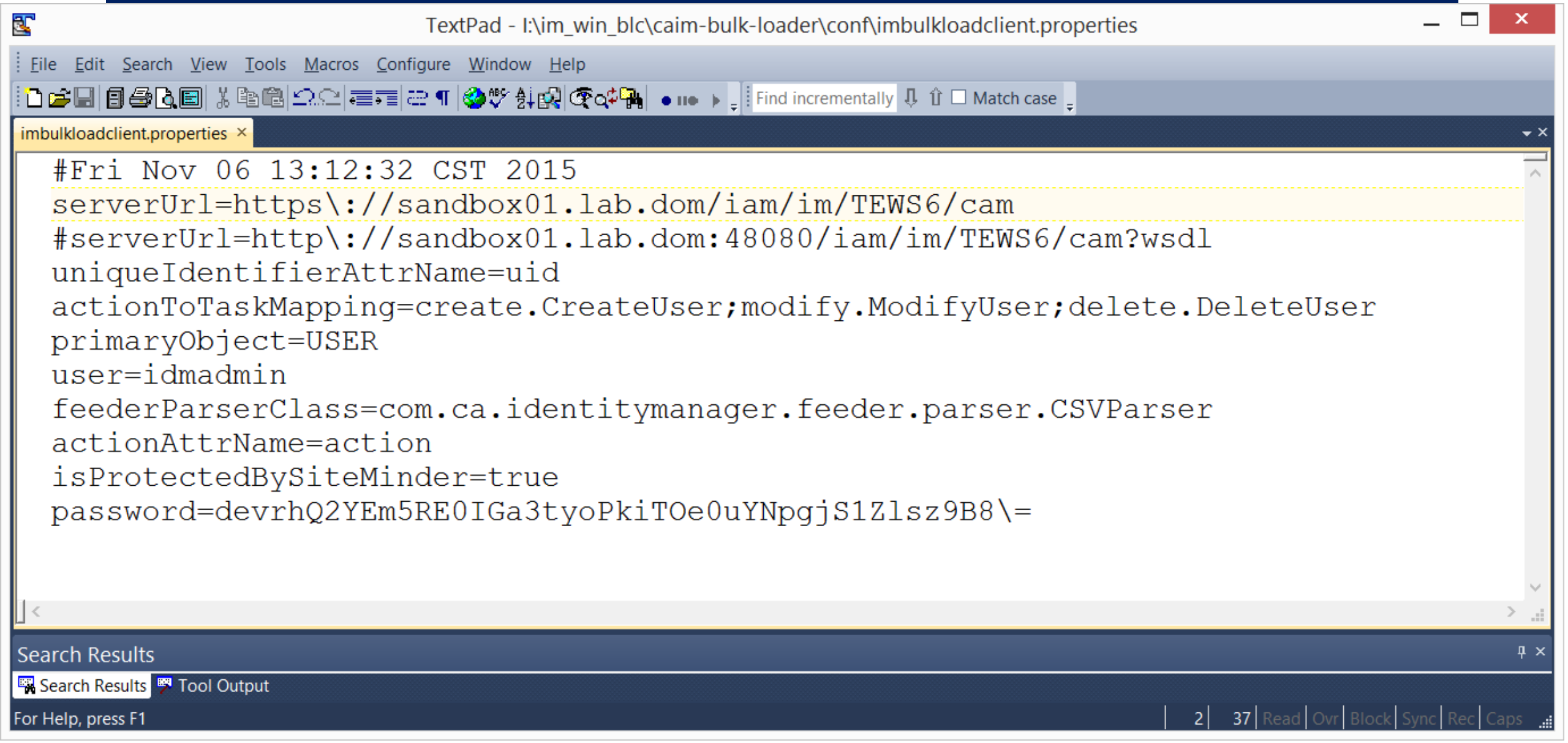
  - Observations:
    - Error from BLC Client & Error from **JBOSS** server.log / No error message from SM Web Agent Trace logs.

```
Failed to submit data to server
ImsException caught:
  Fault Code: Client
  Fault String: Not authorized for service.
    Exceptions:
      Name: com.netegrity.ims.tews6.Tews6Exception
      Code: 400
      Description: Not Authenticated.
```

Troubleshoot: BLC is missing the CA Public Cert



Update BLC Properties File to use SSL URL



Create BLC with SSL CA Certificate & Keystore

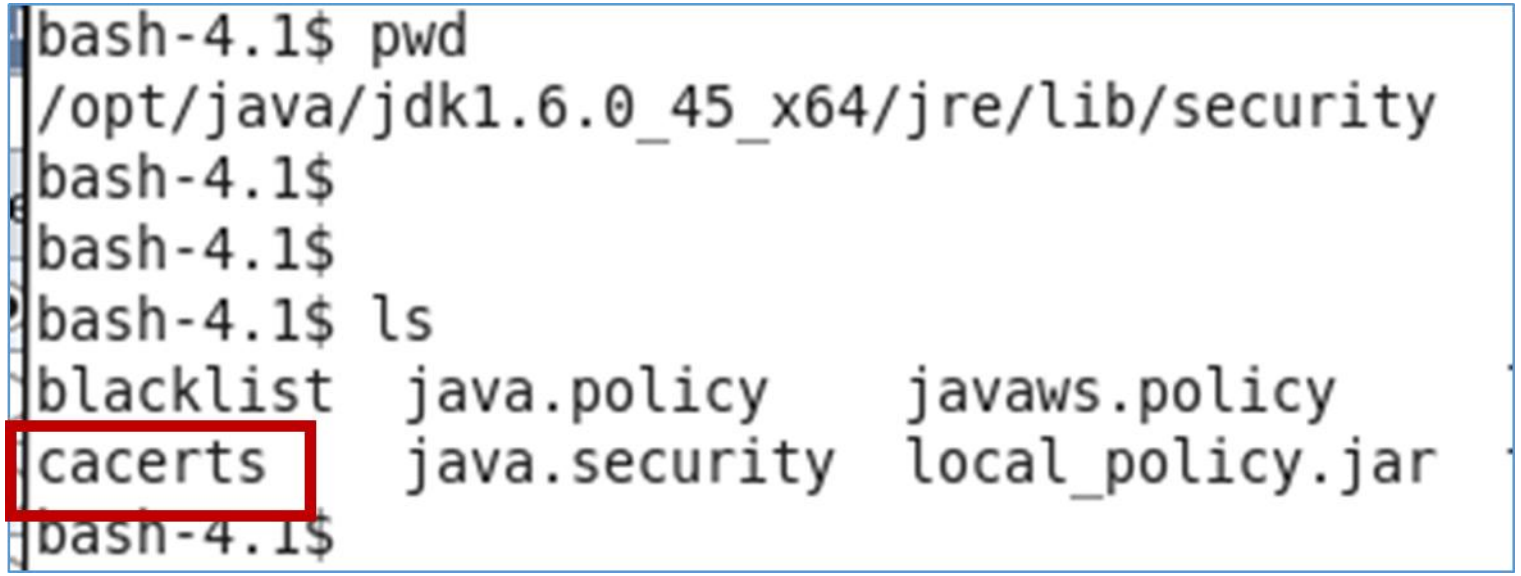
The below process demonstrates a process to remotely query the CA Public Certificate used by the Web Server; and allow the admin user to save this information to a file; using openssl CLI process.

This file can then be imported to a custom BLC keystore, using Java tools / CLI processes.

Ref: https%3A%2F%2Fcommunities.ca.com%2Fdocs%2FDOC-231159591%3Fsr%3Dstream%26ru%3D1654155&usg=AFQjCNEyW14Mqwvw2XUlCrhv9HUi-rm5MQ

Step 1: Identify the CA Certificate from J2EE Server

- Navigate to the JAVA_HOME folder used by the Web Server or J2EE Server.
  - Example: JBOSS
    - JBOSS_HOME/bin/standalone.sh or standalone.bat will have JAVA_HOME defined.
    - Use the command “set” for either Win or Linux/Unix to view environmental variables.
- Change to JAVA_HOME/jre/lib/security (Must be JDK; need keytool)
- Identify keystore
  - Default: **cacerts**



Step 2a: Export the CA Certificate from J2EE Server

- Use the JAVA tool, keytool, to extract the CA Certificate
  - keytool -list -V -keystore <your keystore name>
  - keytool -list -V -keystore cacerts
- If the CA cert does not show, OR you are using a self-signed certificate, then use openssl to validate.
  - **openssl s_client –connect hostname:port -showcerts**

```
C:\Program Files (x86)\VMware\VMware Workstation>openssl s_client -connect imwa0
01.im.dom:443 -showcerts
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
CONNECTED(00000160)
depth=0 C = us, L = Default City, O = Default Company Ltd, CN = imwa001.im.dom
verify error:num=18:self signed certificate
verify return:1
depth=0 C = us, L = Default City, O = Default Company Ltd, CN = imwa001.im.dom
verify return:1
---
Certificate chain
 0 s:/C=us/L=Default City/O=Default Company Ltd/CN=imwa001.im.dom
   i:/C=us/L=Default City/O=Default Company Ltd/CN=imwa001.im.dom
-----BEGIN CERTIFICATE-----
MIICLTCCAZYCCQD1L/ZBGreC9jANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJ1
czEUMBMGA1UEBwwMRGUmYXUsdCBDaXR5MRwwGgYDVQQKDBNEZWZhdWx0IENvbXBh
```

Step 2b: Export the Self-Signed Certificate

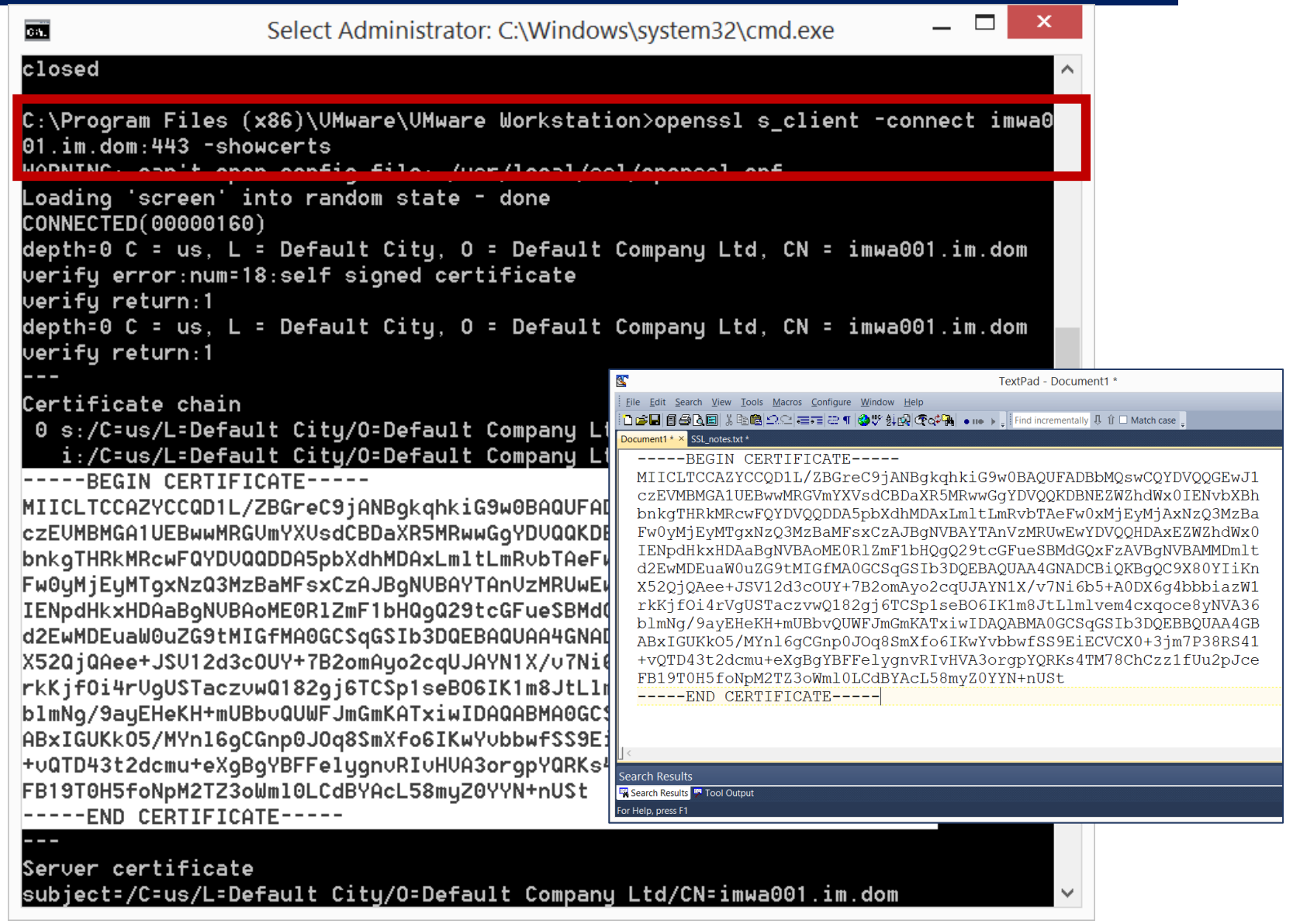
- If you are using a self-signed certificate, then use openssl to validate & then copy from the screen.
  - openssl s_client –connect hostname:port –showcerts

- Select the body between the **FIRST** two markers, including the markers.

----BEGIN CERTIFICATE----

----END CERTIFICATE-----

- Save to a new file.

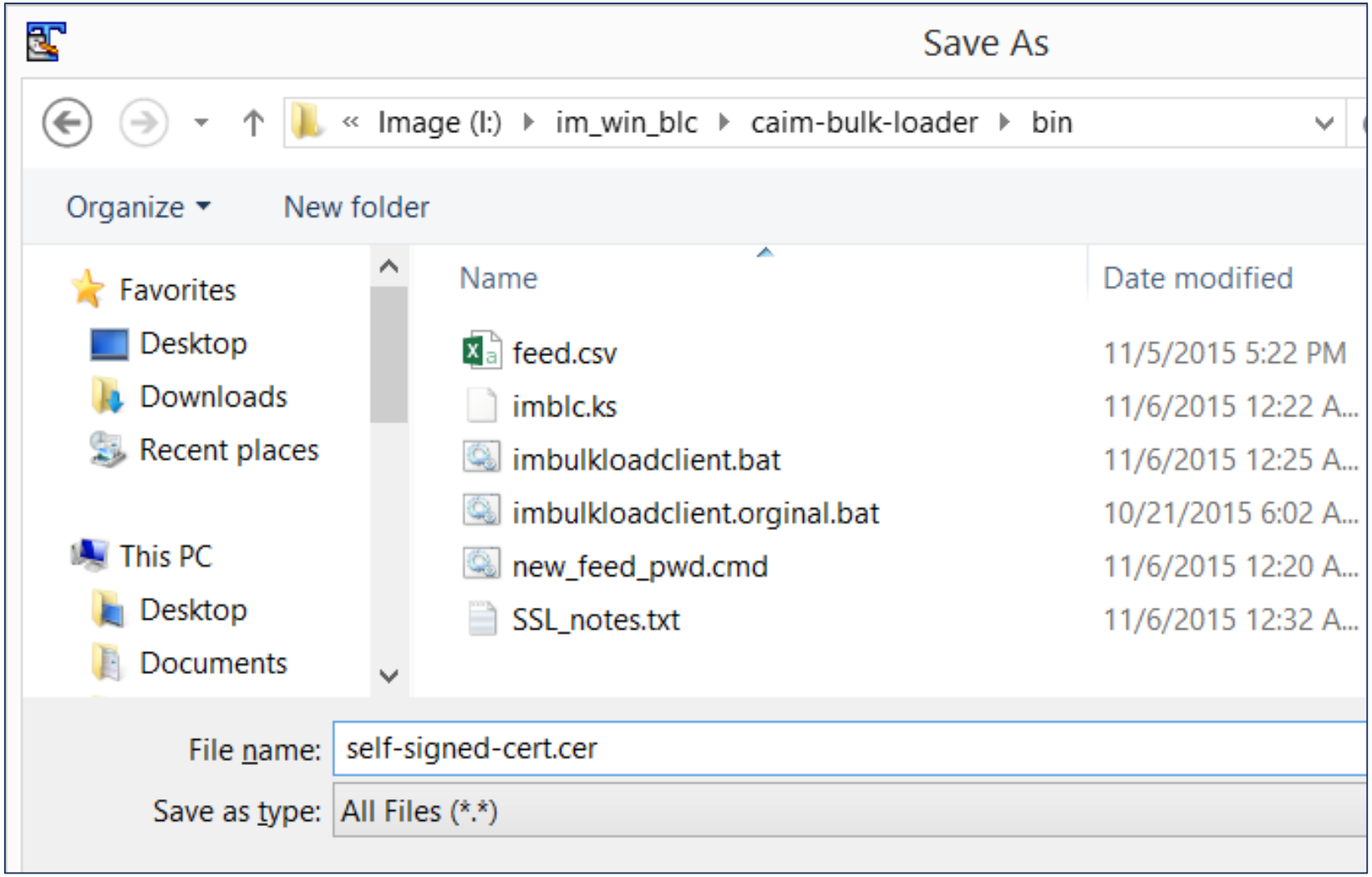


Step 3a: Copy the CA Certificate to BLC Client

- If you are using a CA Public Signed certificate, then use openssl to validate & then copy from the screen.
  - **openssl s_client   -connect hostname:port -showcerts**

- Select the body between the **SECOND** two markers, including the markers.

Step 3b: Copy the Self-Signed Cert to BLC Client



Step 4b: Import the Self-Signed Cert to BLC Client

```
i:\im_win_blc\caim-bulk-loader\bin>"C:\Program Files\Java\jdk1.8.0_31\jre\bin\keytool.exe" -import -alias iam_web_agent
-file self-signed-cert.cer -keystore imblc.ks
keytool error: java.lang.Exception: Keystore file exists, but is empty: imblc.ks

i:\im_win_blc\caim-bulk-loader\bin>del *.ks

i:\im_win_blc\caim-bulk-loader\bin>"C:\Program Files\Java\jdk1.8.0_31\jre\bin\keytool.exe" -import -alias iam_web_agent
-file self-signed-cert.cer -keystore imblc.ks
Enter keystore password:
Re-enter new password:
Owner: CN=imwa001.im.dom, O=Default Company Ltd, L=Default City, C=us
Issuer: CN=imwa001.im.dom, O=Default Company Ltd, L=Default City, C=us
Serial number: f52ff6411ab782f6
Valid from: Thu Dec 20 11:47:30 CST 2012 until: Sun Dec 18 11:47:30 CST 2022
Certificate fingerprints:
         MD5:  FA:9A:BB:7A:22:4D:1D:D7:D5:29:8B:EA:56:69:F5:E9
         SHA1: BA:70:CB:B5:BC:4D:53:EF:D0:24:4E:45:05:14:2E:B5:B6:82:92:76
         SHA256: 69:C0:6E:C0:EE:AA:C8:F2:62:A9:9A:D8:93:19:52:29:E6:FA:44:80:B7:1F:6A:5A:22:FC:45:E1:36:39:1B:06
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore

i:\im_win_blc\caim-bulk-loader\bin>
```

Delete prior keystore if it exists

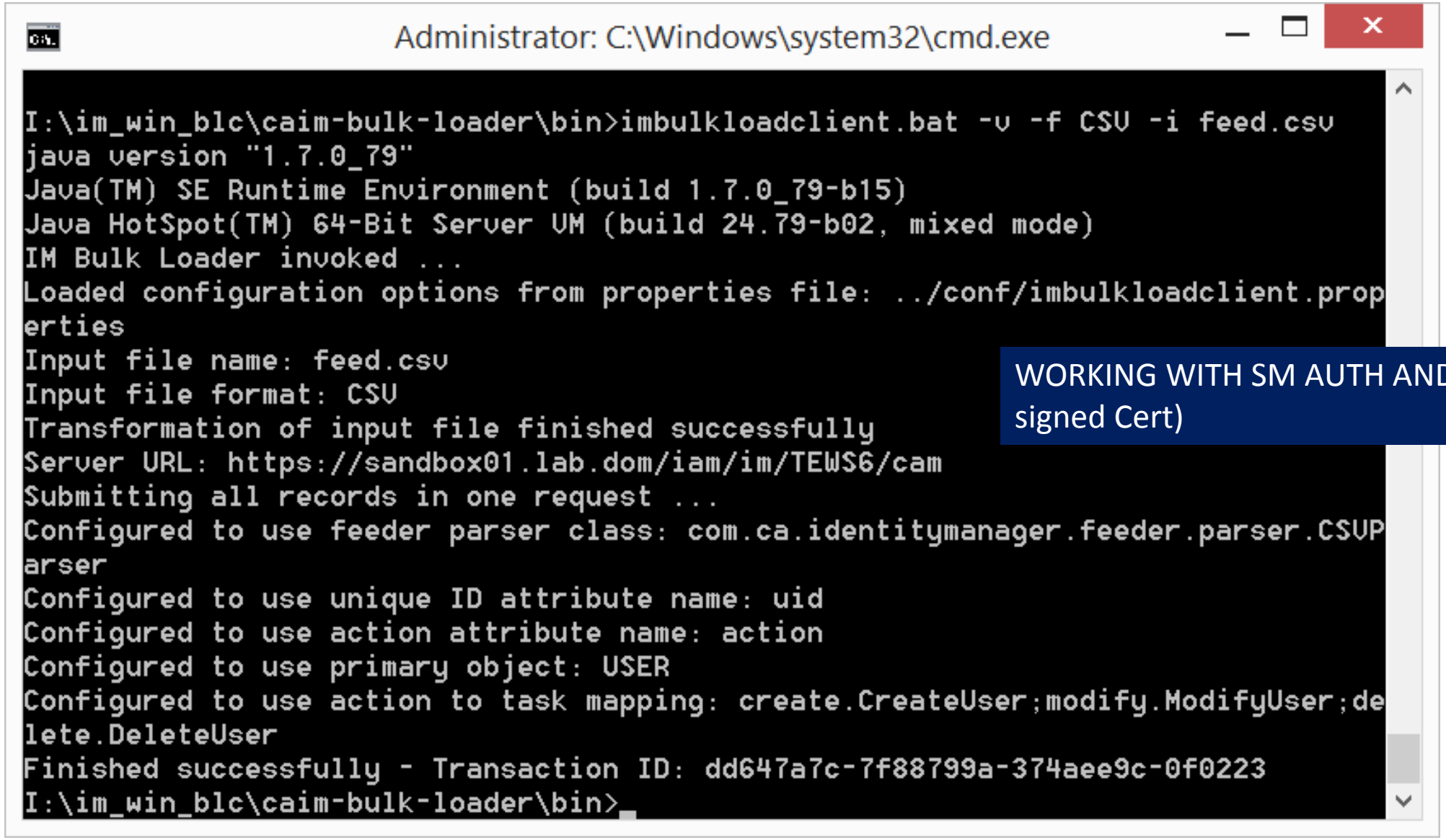
- Import file and create CA keystore for BLC
- keytool -import -alias iam_web_agent -file self-signed-cert.cer -keystore imblc.ks
  - Keytool must be in path, or use full PATH to executable

Step 5b: Validate the Self-Signed Cert in Keystore

```
i:\im_win_blc\caim-bulk-loader\bin>
i:\im_win_blc\caim-bulk-loader\bin>"C:\Program Files\Java\jdk1.8.0_31\jre\bin\keytool.exe" -list -V -keystore imblc.ks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: iam_web_agent
Creation date: Nov 6, 2015
Entry type: trustedCertEntry

Owner: CN=imwa001.im.dom, O=Default Company Ltd, L=Default City, C=us
Issuer: CN=imwa001.im.dom, O=Default Company Ltd, L=Default City, C=us
Serial number: f52ff6411ab782f6
Valid from: Thu Dec 20 11:47:30 CST 2012 until: Sun Dec 18 11:47:30 CST 2022
Certificate fingerprints:
         MD5:  FA:9A:BB:7A:22:4D:1D:D7:D5:29:8B:EA:56:69:F5:E9
         SHA1: BA:70:CB:B5:BC:4D:53:EF:D0:24:4E:45:05:14:2E:B5:B6:82:92:76
         SHA256: 69:C0:6E:C0:EE:AA:C8:F2:62:A9:9A:D8:93:19:52:29:E6:FA:44:80:B7:1F:6A:5A:22:FC:45:E1:36:39:1B:06
         Signature algorithm name: SHA1withRSA
         Version: 1


*******************************************
*******************************************
```

keytool -list -V -keystore imblc.ks

Retest with IM BLC with SM + SSL



WORKING WITH SM AUTH AND SSL (Self-signed Cert)

How to Use Kettle Pentaho with the IM Bulk Load Client

You can use the Bulk Load Client to also run a Kettle job before the bulk load process using the Bulk Load Client command line options.

The sample uses the following options:

imbulkloadclient.bat -f Kettle -t C:/MyKettleJob.kjb -o C:/MyOutput.csv -x 60

The following sections explain each option:

Select the Kettle Job Option
Specify the Kettle Job File
Specify the Output File to Bulk Load
Specify a Timeout for the Kettle Job
Example of Executing a Bulk Load Client with Kettle

Select the Kettle Job option **-f Kettle**

This option specifies that a Kettle job is going to be run. The base option, -f / --format <value>, determines the format of the input file / transform.

Specify the Kettle Job file **-t C:/MyKettleJob.kjb**

This option specifies C:/MyKettleJob.kjb as the file (and its location) used as the template for the input file transformation.

Note: This command string does NOT use the existing -i / --inputFile option for a Kettle Job. Loading the input file should be part of your Kettle Job/Transform

Specify the output File to Bulk Load

There are two ways to specify the output for the Kettle Job that will be bulk loaded.

When outputting the Kettle to a single file, you would use an option similar to the following: **-o C:/MyOutput.csv**

The -o / --outputFile <value> option determines the file of transformation process.

When outputting the Kettle to several files, you would use options similar to the following:

-d C:/MyOutputDir -O MyOutput1.csv,MyOutput2.csv

This uses the following command line options:

-d / --outputDirectory <value> : the directory that contains files output from the transformation process. Note that this is a Kettle-only option.
-O / --outputFileList <value> : A comma-delimited list of files located in the outputDirectory. Note that this is a Kettle-only option

Specify a Timeout for the Kettle Job **-x 60**

This is the Timeout for Kettle transformation, in seconds.

This command is based on the following format: **-x / --transformTimeout <value>**

Note: This command is optional.

Example of Executing a Bulk Load Client with Kettle

For a single output file:

imbulkloadclient.bat -f Kettle -t C:/MyKettleJob.kjb -o C:/MyOutput.csv -x 60

For multiple output files:

imbulkloadclient.bat -f Kettle -t C:/MyKettleJob.kjb -d C:/MyOutputDir -O MyOutput1.csv,MyOutput2.csv -x 60

Troubleshoot: Eliminate the “attachment related” error message when running Bulk Loader Client

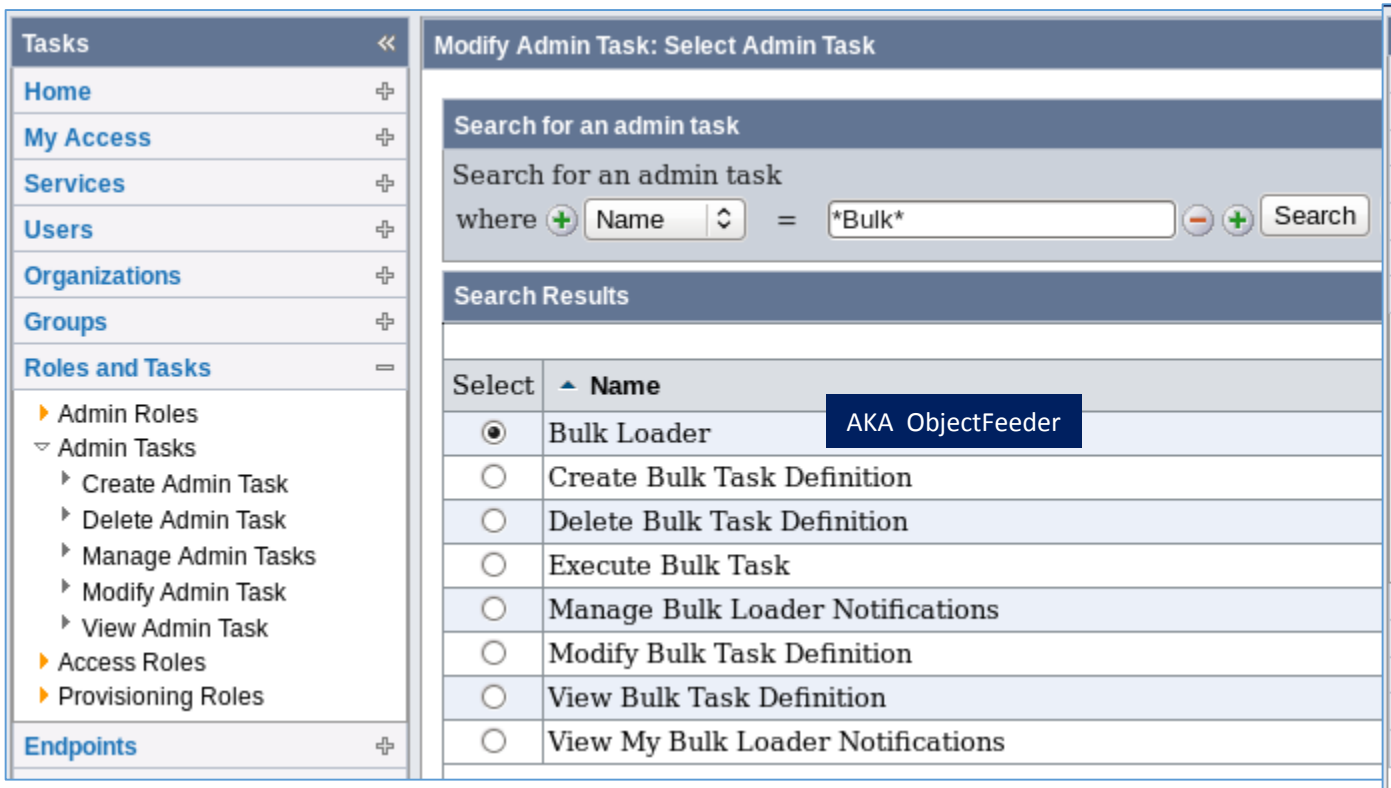
- Tech Note:

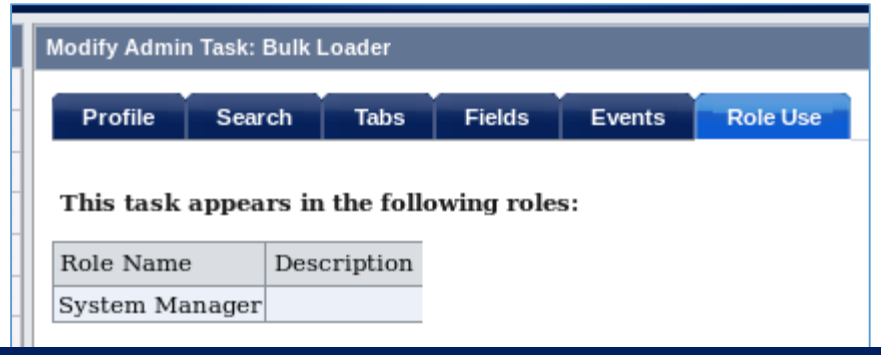
http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec615198.aspx

- Summary:
  - Update missing jar file by coping a version of the mail.jar to BLC lib folder
    - Use the IAMSuite tool workpoint lib folder (mail.jar)
  - Update bat (sh) file to reference jar file in both location (where imbulkloadclient.jar exists).
  - Done

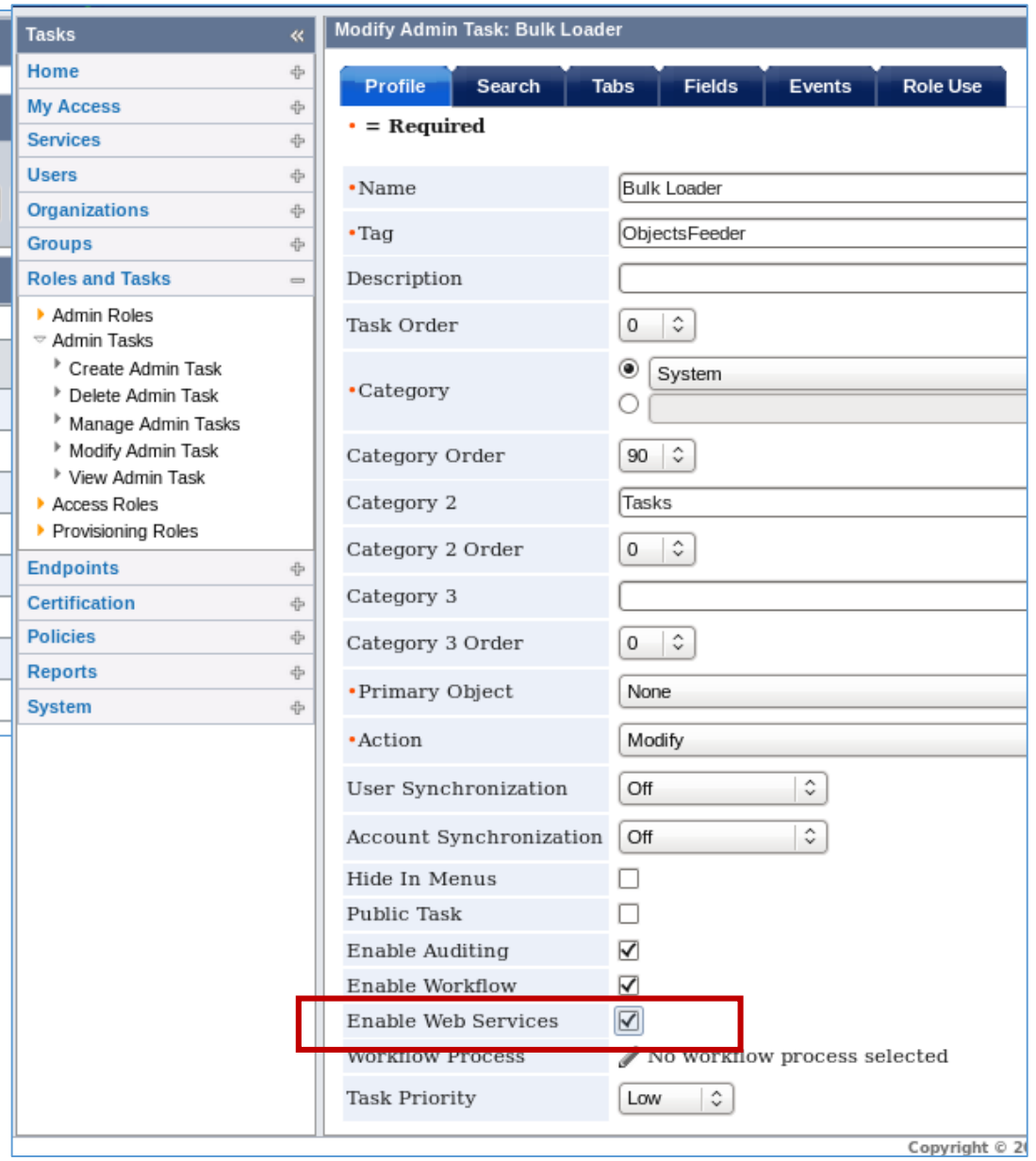
```
-Dcom.ca.commons.logging.nolog4j=true -cp ".:../conf:../lib/mail.jar:../lib/imbulkloadclient.jar"
-Dcom.ca.commons.logging.nolog4j=true -cp ".:../conf:../lib/mail.jar:../lib/imbulkloadclient.jar"
```

Enable Web Services for IM Admin Task “Bulk Loader” & Ensure the BLC userID (idmfeed) is associated to an IM Admin Role

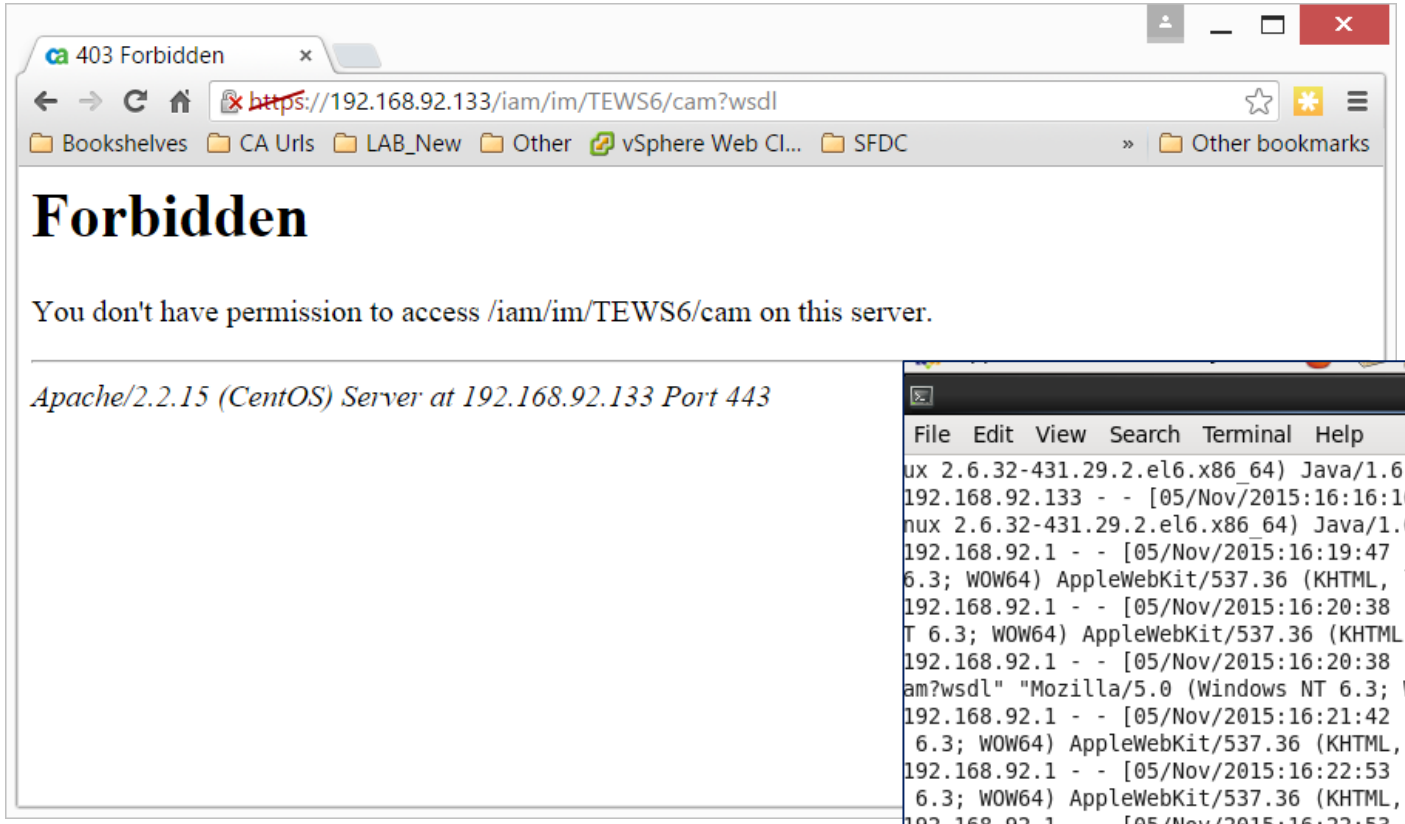


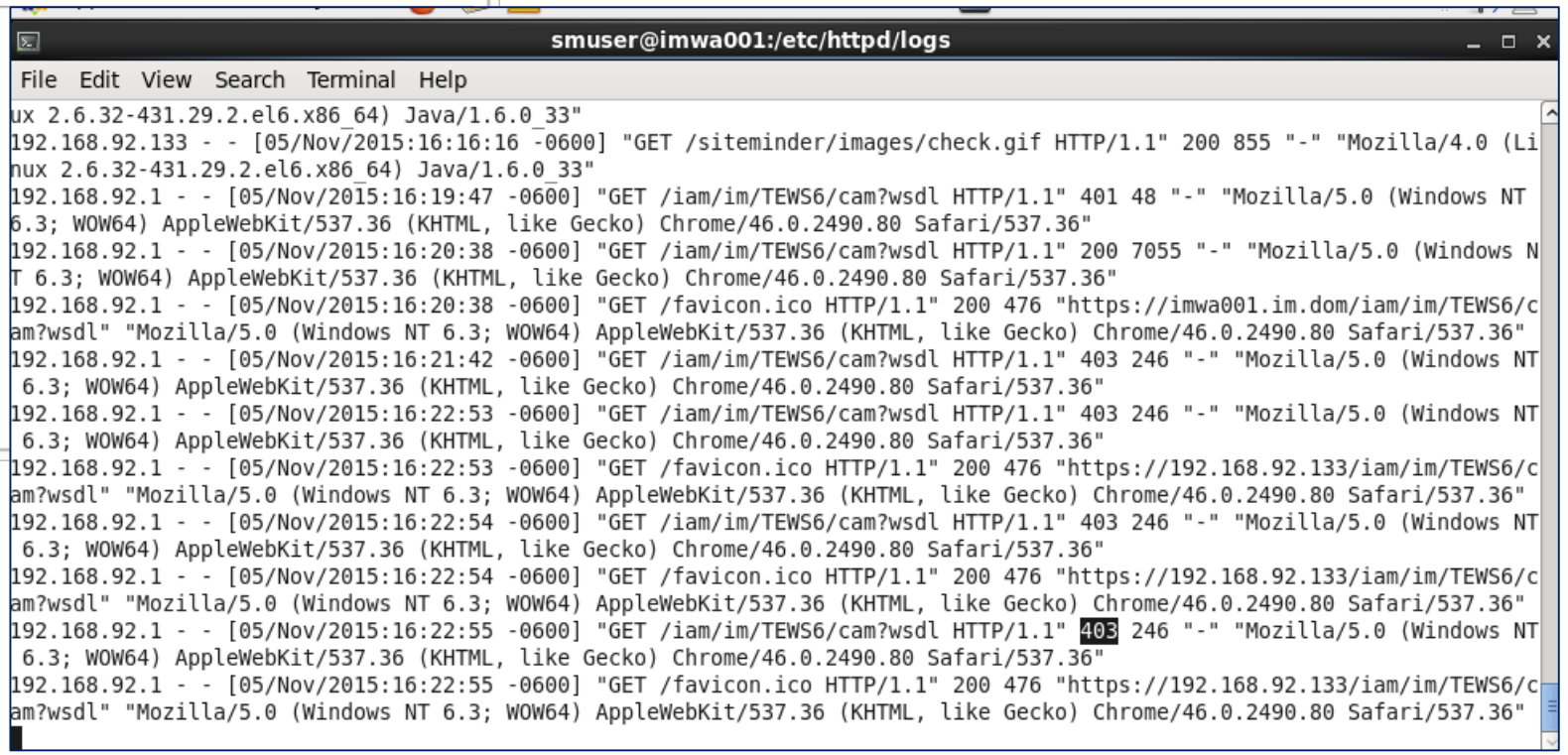


Use System Manager Admin Role
Or Create a NEW SOD Role and add the “Bulk Loader” IM Admin Task to the new Role



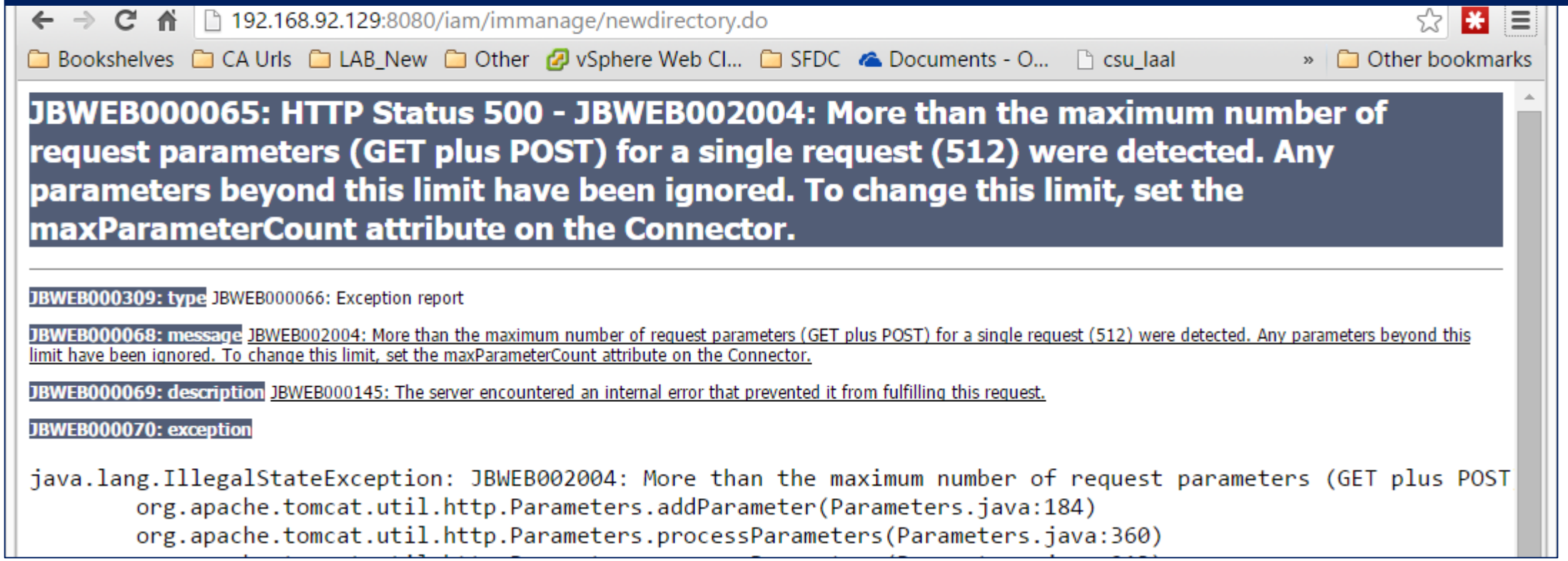
Troubleshoot: Possible Error Seen if HTTPS (SSL) Enabled and using IP Address Instead of FQDN





- 403 error due to use of IP instead of FQDN

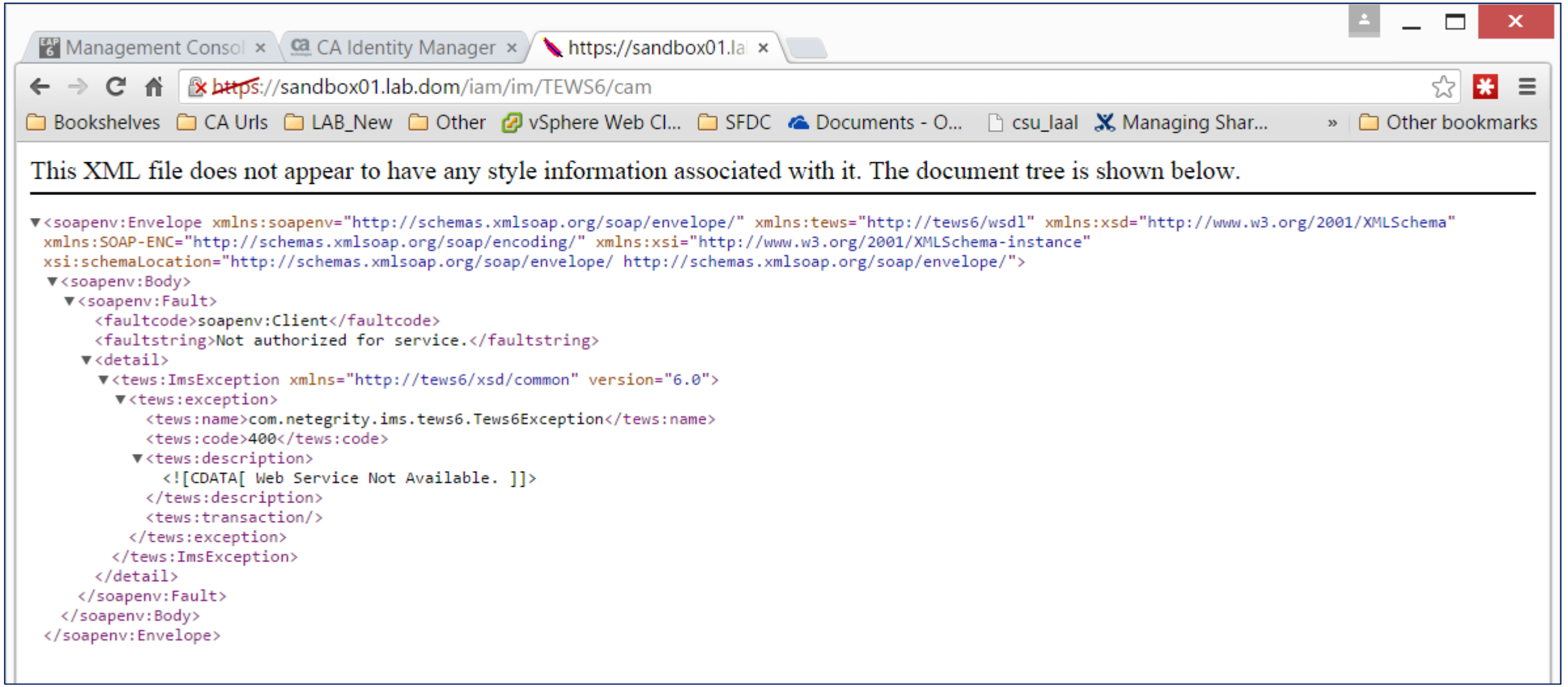
Troubleshoot: JBOSS Error Message may occur if too many entries are defined in a directory.xml (during onboarding of Directory in IM Management Console)



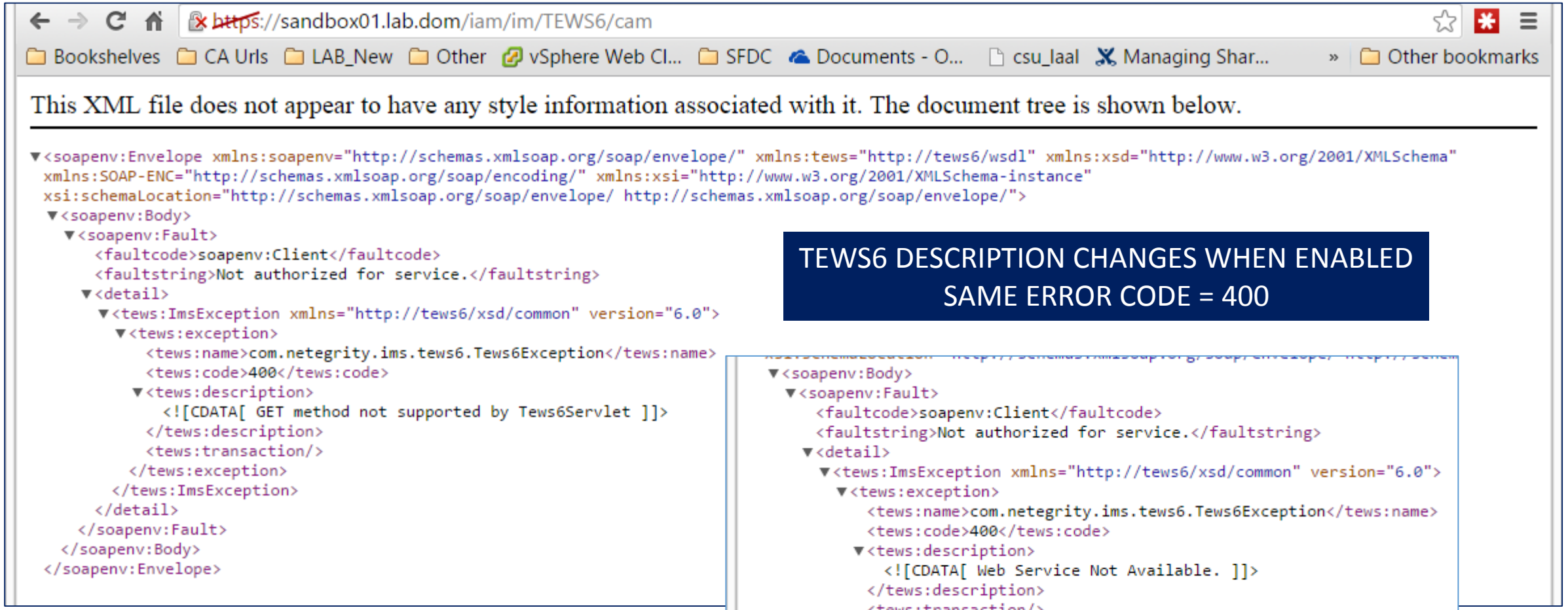
Update JBOSS_HOME/standalone/configuration/standalone-full-ha.xml

```
<!– IM CONFIGURATION CHANGE MARKER #2-->
<!-- Added to address possible max parameters limit on loading IMCD parameters with the default MAX_COUNT=5000 -->
<!-- Add immediately after /extensions> section -->
    <system-properties>
      <property  name="org.apache.tomcat.util.http.Parameters.MAX_COUNT"  value="10000"/>
    </system-properties>
<!-- Added to address possible max parameters limit on loading IMCD parameters with the default MAX_COUNT=5000 -->
```

NOTE: MESSAGE RETURNED WHEN VIEWING TEWS6 BEFORE ENABLING THE WEB SERVICES
"WEB SERVICES NOT AVAILABLE "



NOTE: MESSAGE RETURNED WHEN VIEWING TEWS6 AFTER ENABLING THE WEB SERVICES
"GET METHOD NOT SUPPORTED BY TEWS6SERVELET"

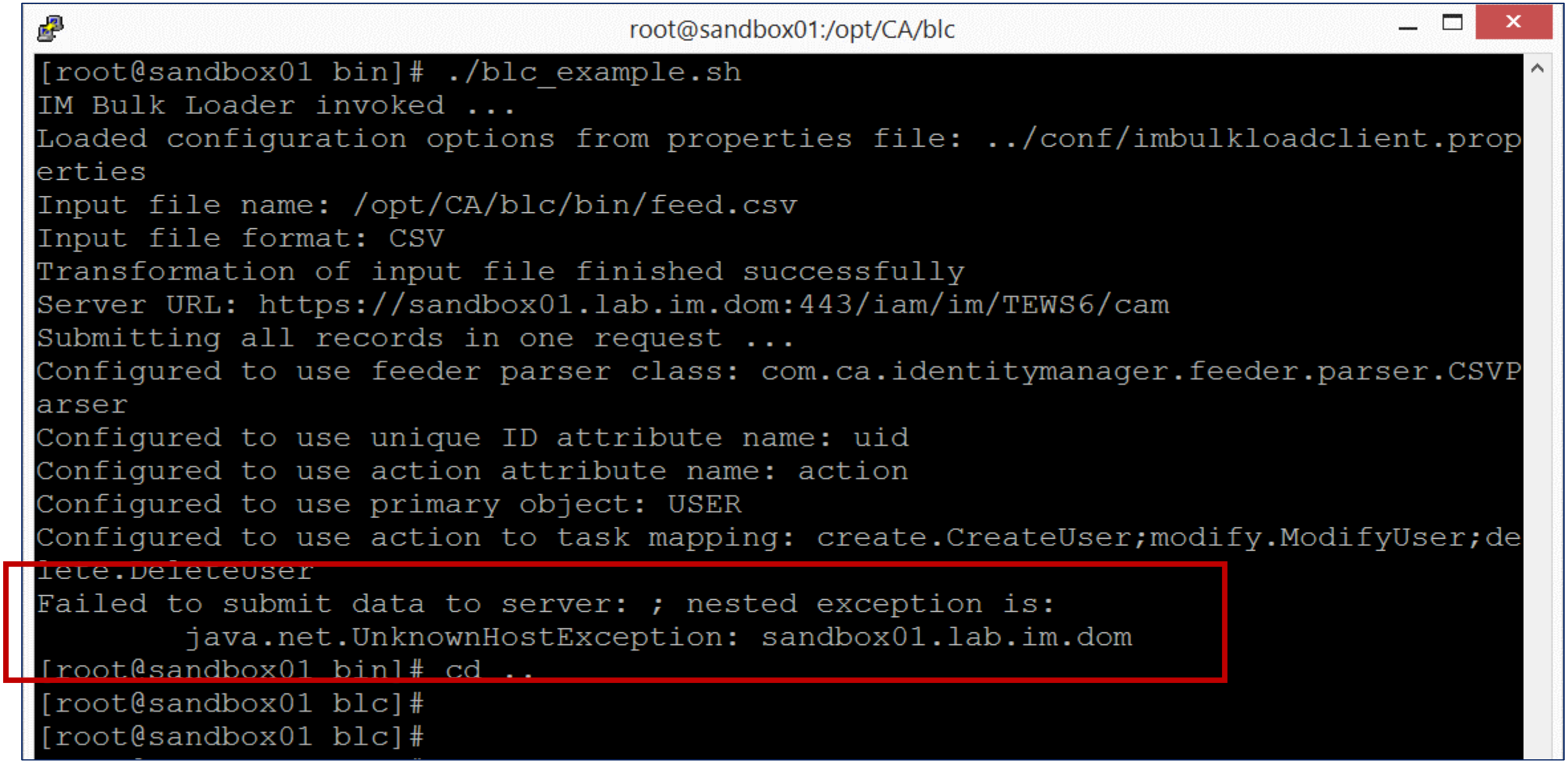


NOTE: IM WSDL WILL DISPLAY BEFORE & AFTER WEB SERVICES ARE ENABLED FOR USE
VALIDATE TEWS6 WSDL RESPONSE BEFORE ENABLING TO CONFIRM

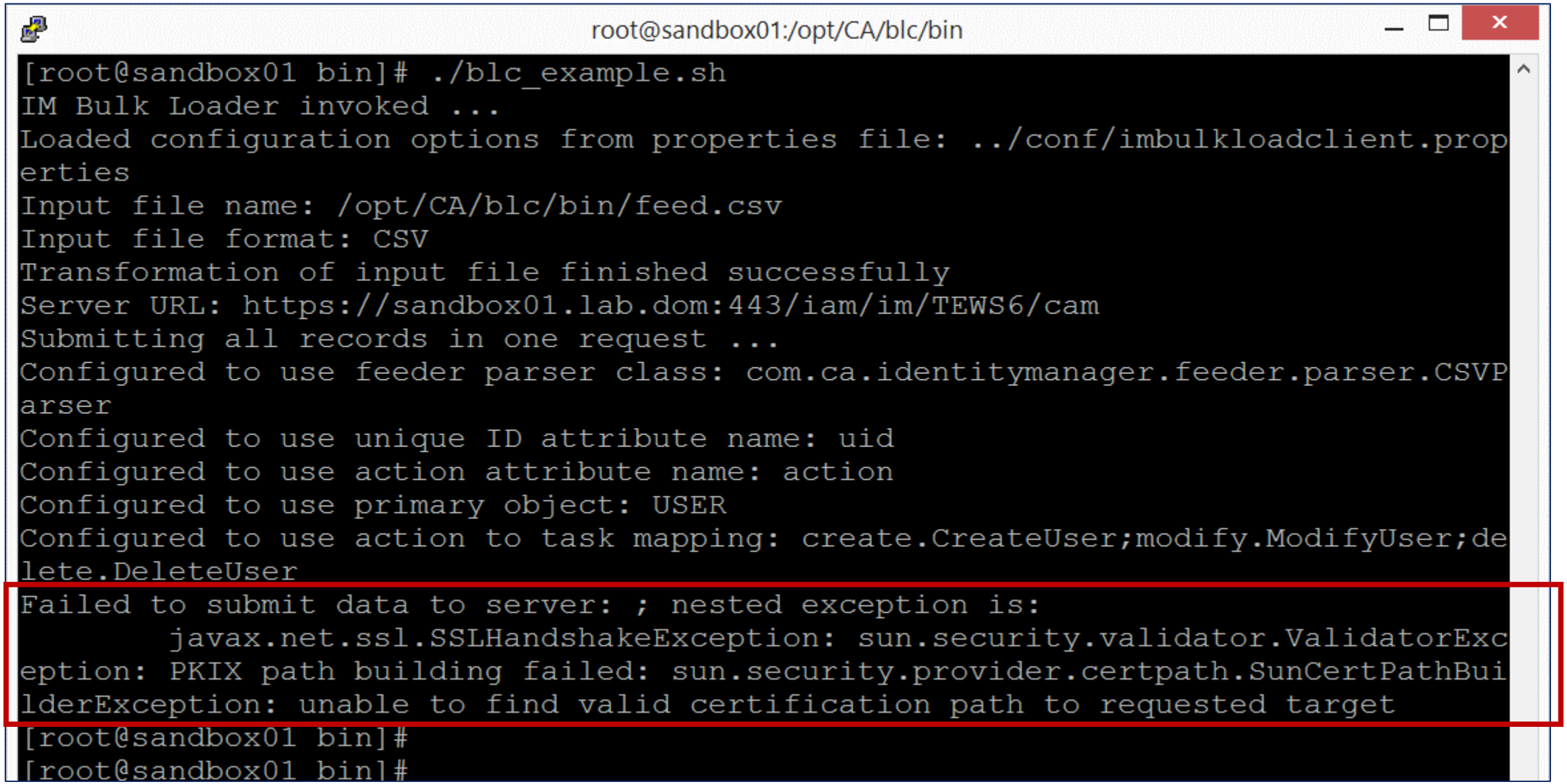
This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<definitions xmlns:tns="http://tews6/wsdl" xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
 xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xs="http://www.w3.org/2001/XMLSchema" name="cam" targetNamespace="http://tews6/wsdl">
 ▼<types>
  ▼<xs:schema xmlns:tns="http://tews6/wsdl" xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://tews6/wsdl" elementFormDefault="qualified"
   attributeFormDefault="unqualified">
   ▼<xs:element name="Search">
    ▼<xs:complexType>
     ▼<xs:sequence>
        <xs:element name="CreateCopy" type="xs:boolean" minOccurs="0"/>
      ▼<xs:element name="Organization" minOccurs="0">
       ▼<xs:complexType>
        ▼<xs:sequence>
           <xs:element name="UniqueName" type="xs:string"/>
           <xs:element name="AndLower" type="xs:boolean"/>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
      ▼<xs:element name="Subject" minOccurs="0" maxOccurs="unbounded">
       ▼<xs:complexType>
        ▼<xs:sequence>
         ▼<xs:choice>
            <xs:element name="UID" type="xs:string"/>
            <xs:element name="UniqueName" type="xs:string"/>
            <xs:element name="FriendlyName" type="xs:string"/>
            <xs:element name="Name" type="xs:string"/>
            <xs:element name="Tag" type="xs:string"/>
            <xs:element name="OID" type="xs:string"/>
          </xs:choice>
          <xs:element name="Check" type="xs:boolean" minOccurs="0"/>
         </xs:sequence>
         <xs:attribute name="index" type="xs:integer" use="required"/>
```

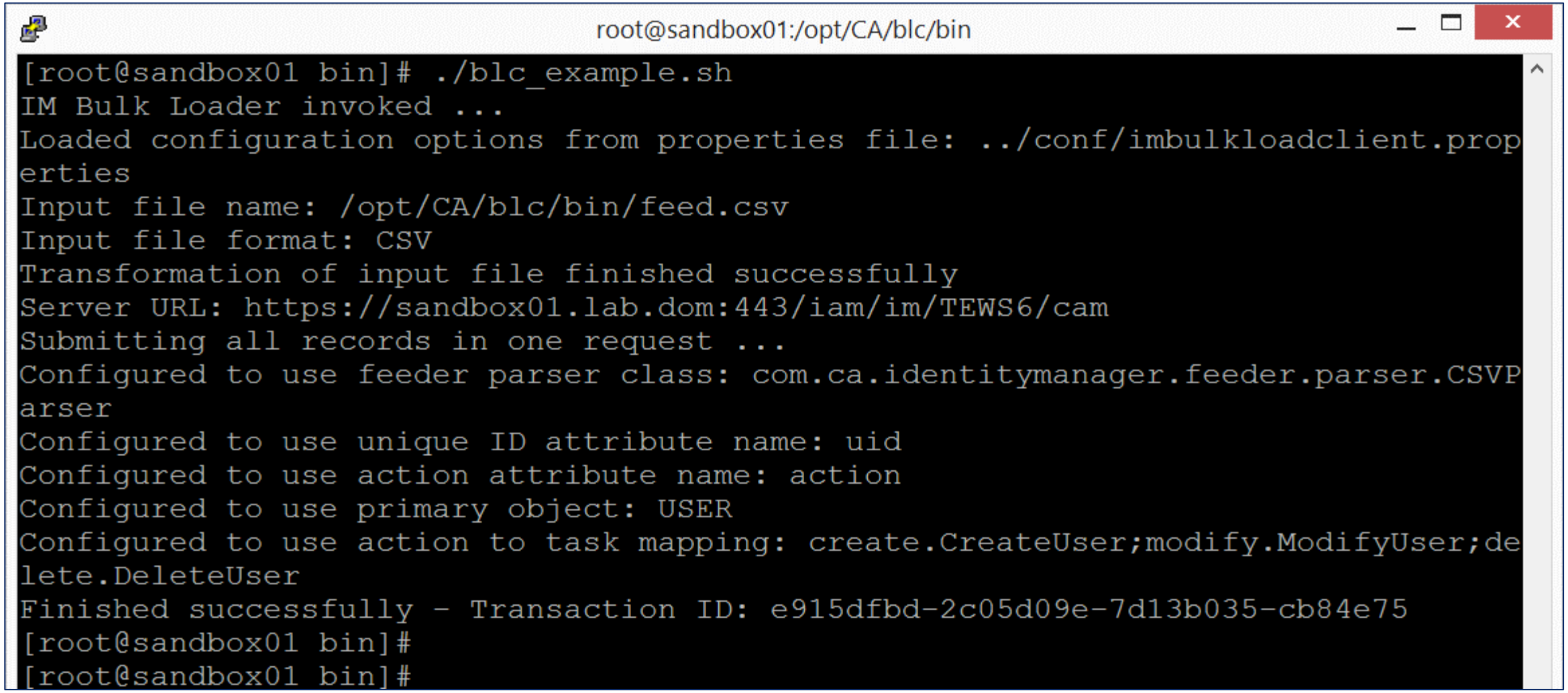
TROUBLESHOOT: ERROR MESSAGE EXAMPLE: INCORRECT HOSTNAME



TROUBLESHOOT: ERROR MESSAGE EXAMPLE: MISSING CA TLS CERT IN BLC KEYSTORE



SUCCESSFUL MESSAGE EXAMPLE: TRANSACTION ID RETURNED FOR CREATE USER RECORD



BLC EXAMPLE: IM VST OF SUCCESSFUL SUBMITED TASK FOR CREATE USER

View Submitted Tasks

	Description	Status	Priority	Initiated by	Submitted	Last Updated	Last Operation
✎	Bulk Loader task	Completed	Low	idmadmin	11/3/2015 2:53 PM	11/3/2015 2:53 PM	All feeder records were submitted for execution. Total number of records submitted is 1
✎	Create User task, User bob02	Completed	Medium	idmadmin	11/3/2015 2:53 PM	11/3/2015 2:53 PM	

View Submitted Tasks

Create User Task Details: bob02

Subject name	bob02 (bob01 bob01)
Task performed by	idmadmin (idmadmin)
Task creation time	Tuesday, November 3, 2015 2:53:02 PM EST
Task status	Completed

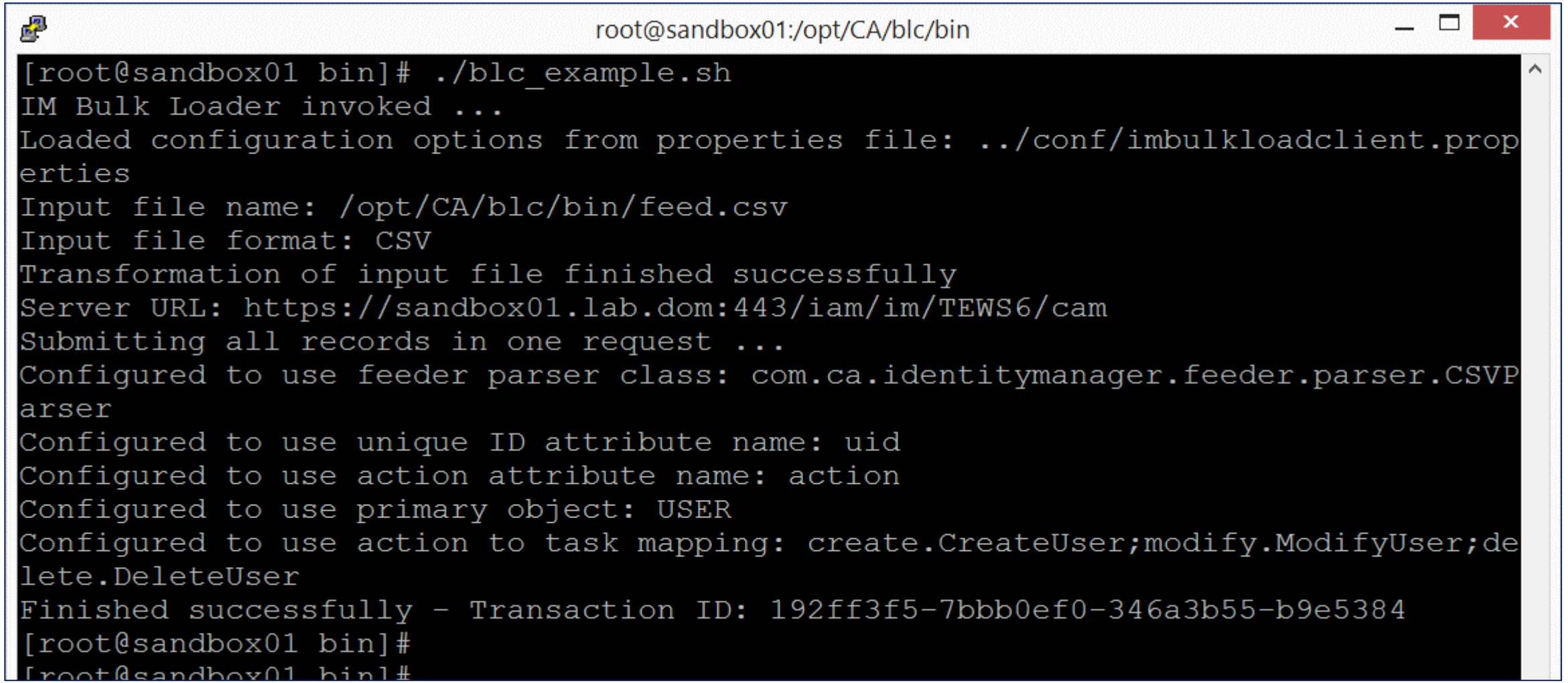
Identity Policy Violations

Identity Policy Name	Type	Workflow Status	Message
No results.			

Included Events

	Event Name	Description	Status	Submitted	Last Updated	Last Activity
✎	Create user	Create user "bob01 bob01 (bob02)" in organization "people"	Completed	11/3/2015 2:53 PM	11/3/2015 2:53 PM	
✎	Synchronize user	Synchronize user "bob01 bob01 (bob02)"	Completed	11/3/2015 2:53 PM	11/3/2015 2:53 PM	

SUCCESSFUL MESSAGE EXAMPLE: TRANSACTION ID RETURNED FOR DUPLICATE OF SAME USER RECORD



SUCCESS ON LOAD FOR BLC AND IM CORRECTLY IDENTIFIED DUPLICATE WITH RE-SUBMISSION OF SAME RECORD

Bulk Loader Task Details

Subject name	NONE
Task performed by	idmadmin (idmadmin)
Task creation time	Tuesday, November 3, 2015 2:55:36 PM EST
Task status	Completed

Identity Policy Violations

Identity Policy Name	Type	Workflow Status	Message
No results.			

Included Events

	Event Name	Description	Status	Submitted	Last Updated	Last Activity
✎	Feed Objects	Bulk Loader Event	Completed	11/3/2015 2:55 PM	11/3/2015 2:55 PM	

Initiated Tasks

These tasks were created as part of initiating this task, and began executing immediately.

	Description	Status	Priority	Initiated by	Submitted	Last Updated	Last Operation
✎	Create User	Audited	Medium	idmadmin	11/3/2015 2:55 PM	11/3/2015 2:55 PM	An error object was posted to the task with text: User id bob02 is a duplicate.

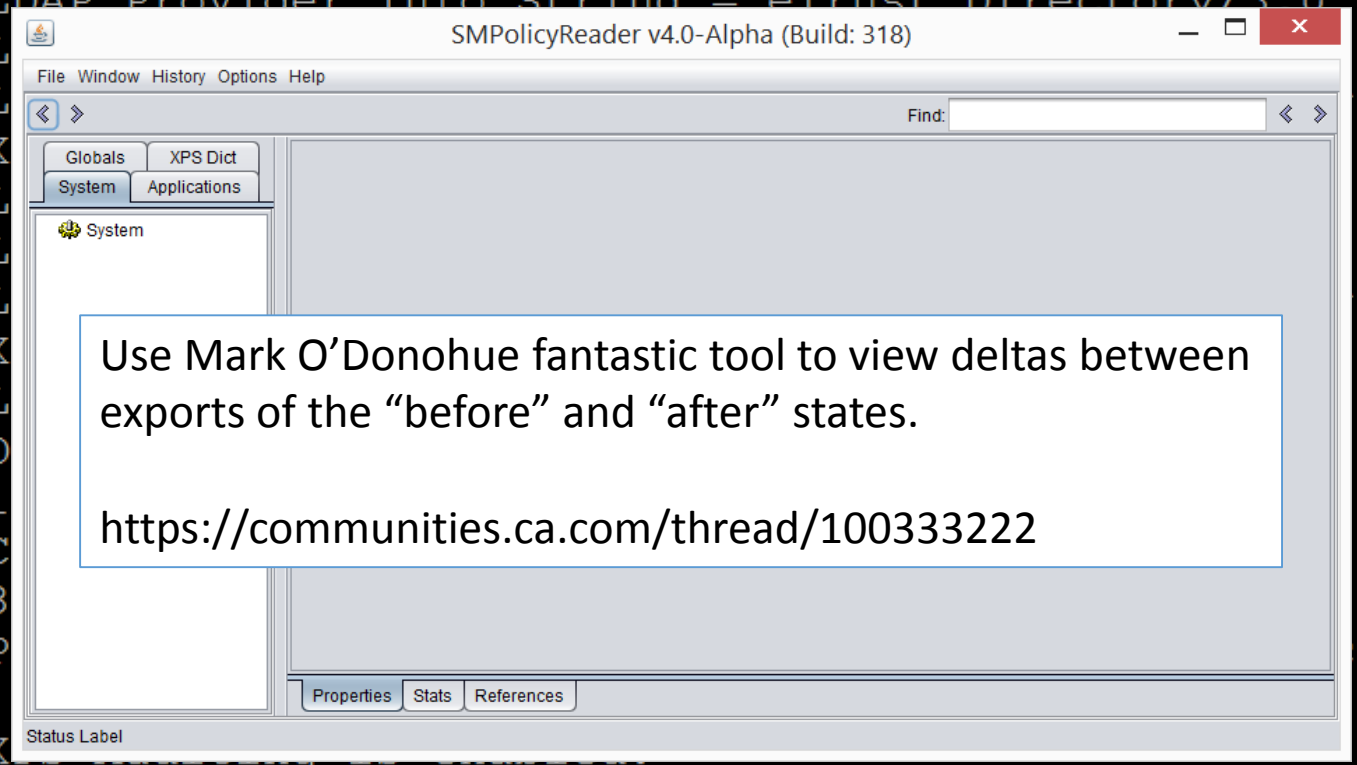
Task History

Source	Description	Time
TASKSESSION	An error object was posted to the task with text: User id bob02 is a duplicate.	2015-11-03 14:55:37.0

PERFORM SM EXPORT TO VIEW CHANGED IN SM POLICY STORE BEFORE & AFTER ENABLING SM AUTH IN IM

root@sandbox01:/opt/CA/jboss/im_01/jboss-eap-6.2/standalone/deployments

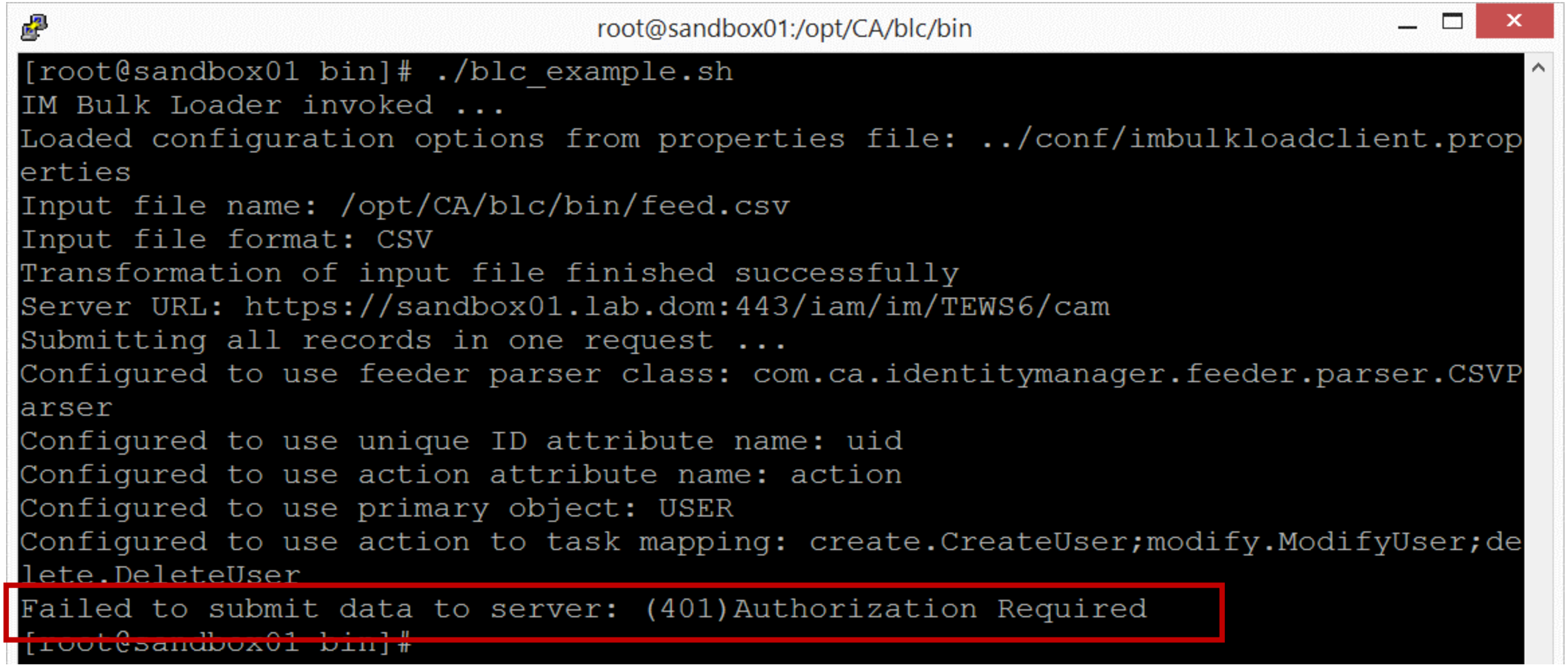
```
bash-4.2$ XPSExport -xb -npass -vT 03_XPSExport_IM_and_SM_integrated_via_ra-xml_
IMCD_and_IME__WS_BulkTask_working__no_IMPS_no_SM_Auth_for_WS.xml
[XPSExport - XPS Version 12.52.0001.154]
Log output: XPSExport.2015-11-03_145713.log
Initializing XPS, please wait...
(INFO) : [sm-xpsxps-00120] Initializing XPS Version 12.52.0001.154
(INFO) : [sm-xpsxps-01160] LDAP Provider Info String = eTrust Directory/3.0
(INFO) : [sm-xpsxps-01120] L
(INFO) : [sm-xpsxps-01120] L                                              r12
.0.16 (build 11032) Linux/DX
(INFO) : [sm-xpsxps-01160] L
(INFO) : [sm-xpsxps-01120] L
(INFO) : [sm-xpsxps-01120] L                                              r12
.0.16 (build 11032) Linux/DX
(INFO) : [sm-xpsxps-01160] L
(INFO) : [sm-xpsxps-00560] D
(INFO) : [sm-xpsxps-00300] 1
(INFO) : [sm-xpsxps-00330] C
(INFO) : [sm-xpsxps-00310] 3
(INFO) : [sm-xpsxps-00430] P                                              0a86
0bf".
(INFO) : [sm-xpsxps-06870] X
(INFO) : [sm-xpsxps-03460] No validation warnings will be logged (controlled by
CA.XPS::$LogValidationWarnings).
```



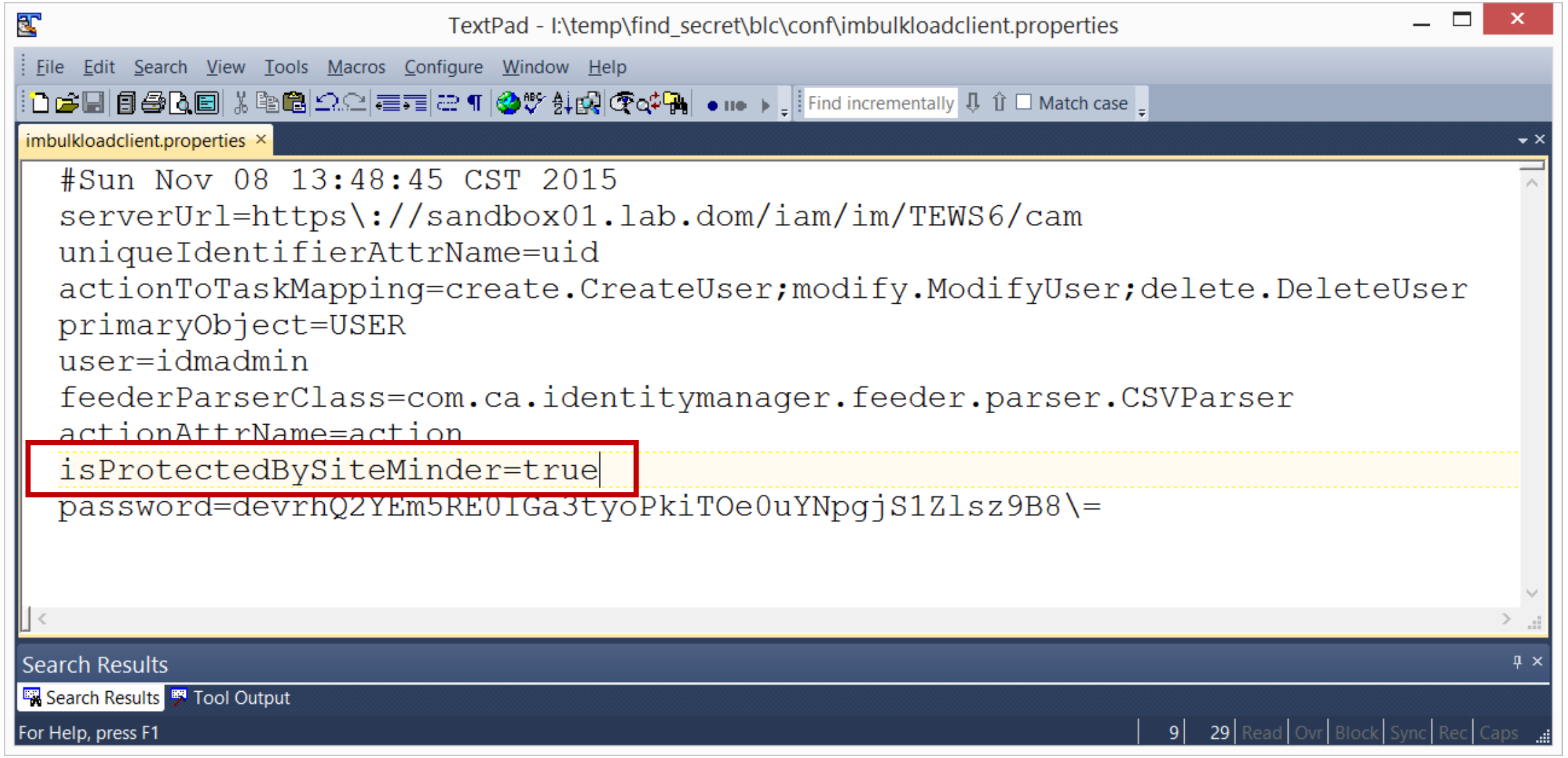
Use Mark O'Donohue fantastic tool to view deltas between exports of the "before" and "after" states.

https://communities.ca.com/thread/100333222

Example Error Message: Validate with BLC submission before changing BLC configuration to use SM Basic Auth



Enable SM Auth in BLC: Change Boolean value from false to true for SM Auth



Review APACHE Web Server with SSL: Tokens Required

Listen Port Defines the port number that Apache uses for the SSL communication.
SSL Engine Specifies the status of the SSLEngine.
SSL Certificate File Path Defines the location of the SSL certificates.
Default: *installation_path*/httpd/conf/SSL/certs/server.crt
SSL Key File Path Defines the location of the key to the SSL certificates.
Default: *installation_path*/secure-proxy/SSL/keys/server.key
SSL Certificate Chain File Path Defines the location of the CA certificates which form the certificate chain.
SSL CA Certificate File Path Defines the location of the CA certificates that are used for client authentication.
Default: *installation_path*/secure-proxy/SSL/certs/ca-bundle.cert
SSL CA Revocation File Path Defines the location of the CA certificate revocation lists that are used for client authentication.
SSL Verify Client Specifies the certification verification level for the SSL client authentication.
SSL Verify Depth Defines the number the levels in the certificate chain that must be searched for the certificate.

https://wiki.ca.com/display/sm1252sp1/Configuring+SSL+on+Apache+Web+Server+Using+Administrative+UI

https://wiki.ca.com/display/sm1252sp1/Configuring+SSL+on+Apache+Web+Server+Manually

https://wiki.ca.com/display/sm1252sp1/SSL+Troubleshooting

Apache httpd ssl configurations (w/wo SM Agent)

LoadModule ssl_module modules/mod_ssl.so

Listen 443

Listen 8443

AddType application/x-x509-ca-cert .crt

AddType application/x-pkcs7-crl .crl

SSLPassPhraseDialog builtin

SSLSessionCache shmcb:/var/cache/mod_ssl/scache(512000)

SSLSessionCacheTimeout 300

SSLMutex default

SSLRandomSeed startup file:/dev/urandom 512

SSLRandomSeed connect builtin

SSLCryptoDevice builtin

ServerName ssl.domain.com

DocumentRoot /opt/CA/httpd/htdocs

ScriptAlias /cgi-bin /home/site/cgi-bin

SSLEngine on

SSLProtocol all -SSLv2

SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW

SSLCertificateFile /opt/CA/httpd/conf/ssl/ssl.domain.com.server.crt

#SSLCertificateKeyFile /opt/CA/httpd/conf/ssl/ssl.domain.com.server.key

Replace the below key with a password protected key for production environments

SSLCertificateKeyFile
/opt/CA/httpd/conf/ssl/ssl.domain.com.server.nopassword.key

Replace the below CertChain from SSL Public Vendor

#SSLCertificateChainFile
/opt/CA/httpd/conf/ssl/parent_root_or__intermediate_bundle.crt

Needed for SM and IM BLC

#https://support.ca.com/cadocs/0/CA%20SiteMinder%2012%2052%20SP1-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?346046.html?intcmp=searchresultclick&resultnum=730

SSLVerifyClient optional **{Needed for IM BLC to function correctly with SSL Certs}**

SSLVerifyDepth 10 **{Needed for IM BLC to function correctly with SSL Certs}**