

Reset IM's Service Passwords: IM/IMPS/CCS/JCS

Using Pwdmgr, CX, and Jxplorer tools

Alan Baugher, June 2016

CA Sr. Principal Architect



Agenda

Challenge/Requirement:

Clients have SLA to change service account passwords on a scheduled basis (yearly or when concern about comprised is warranted)

Proposal:

This document provide a clear and crisp view to list, and how to change service account passwords using CA tools and/or LDAP administration tools.

A primary and secondary processes are provided for known and unknown passwords.

Processes were checked with MS Sysinternal ProcMon, dxdumpdb of IMPD, and JCS logs with “Before –n- After” snapshots

Password Locations for Service accounts

ID	Component	Password Location (s)	Primary Update Process	Secondary Update Process
idmadmin / etaadmin Idmbatch	Global User Admin Service ID for IMPS & Integration User ID for IME IMPS XML & idmbatch ID in IMPS	1) CA Directory's IMPD CO Branch 2) IME IMCD XML hash.	1) Use IMPM GUI 2) Use IM Management Console to export IMPS XML; update and reimport IMPS XML	1) Use Jxplorer to IMPS 20389/20390 or IMPD 20391. May reset to anon configuration to reset unknown pwd.
cn=root,dc=etasa	IM CCS SA Service ID 20402 (non-TLS; localhost) 20403 (TLS; localhost)	1) All IM CCS Servers: Windows Registry (WinOS) or ZeroG Registry (Linux/Solaris) 2) CA Directory's IMPD CO Branch under Parameters for CCS Connectors	1) Use IMPS PwdMgr Tool. Ensure PwdMgr Tool is executed on each IMPS/IM CCS Server. 2) Use IM ConnectorXpress to update IM CCS Password within IMPS; to allow it to connect to IM CCS.	None.
eTDSAContainerName=D SAs,eTNamespaceName= CommonObjects,dc=etadb (1) eTDSAContainerName=D SAs,eTNamespaceName= CommonObjects,dc=im,d c=etadb (2)	BIND DN for IMPD. Used by IMPS Server via IMPD Router (20391) to IMPS DSAs.	CA Directory's IMPD IM CO Branch CA Directory's IMPD Non-IM CO Branch	1) Use IMPS PwdMgr Tool. Ensure PwdMgr Tool is executed on each IMPS Server.	1) Use Jxplorer to IMPD 20391 (20394/20396/20398/20404). May reset to anon configuration to reset unknown pwd.
cn=root,dc=etasa & uid=admin,ou=system	IAMCS (JCS) SA Service ID & Alias ID 20410 (non-TLS; host) 20411 (TLS; host)	1) All IM JCS Servers: Local JCS embedded flat configuration database. 2) CA Directory's IMPD CO Branch under Parameters for JCS Connectors	1) Use IM ConnectorXpress to update IM CCS Password within IMPS; to allow it to connect to IM JCS. This tool will also connect to JCS to update the IAM CS Password for both the service ID and the alias ID. 2) Use the IAM CS UI Console to reset the alias ID's password.	1) Use Jxplorer to IAMCS 20410/20411 to reset alias ID's password. May reset the IAMCS configuration files to allow anonymous connection to reset unknown pwd.
cn=etaserver,dc=eta	Maintenance Account. Used during initial install. May be disabled.	1) CA Directory IMPD base.	1) Use IMPS PwdMgr Tool.	1) Use Jxplorer to IMPS 20389/20390 or IMPD 20391. May reset to anon configuration to reset unknown pwd.
idmadmin / idmfeed / idminbound / idmpublic	Corporate User Store Accounts used for various use-cases functionality	1) Corporate User Store 2) IM Database for IM Management Console	1) Use IME User Console 2) IM Management Console	2) Use jxplorer to corporate userstore.
idmdba_os_tp_wf_aud Idmdba_tpa_rpt	Database accounts for "active-runtime" databases and "scheduled-as-needed" databases	1) Database Login ID associated with each IM database	1) Update via database tools	None

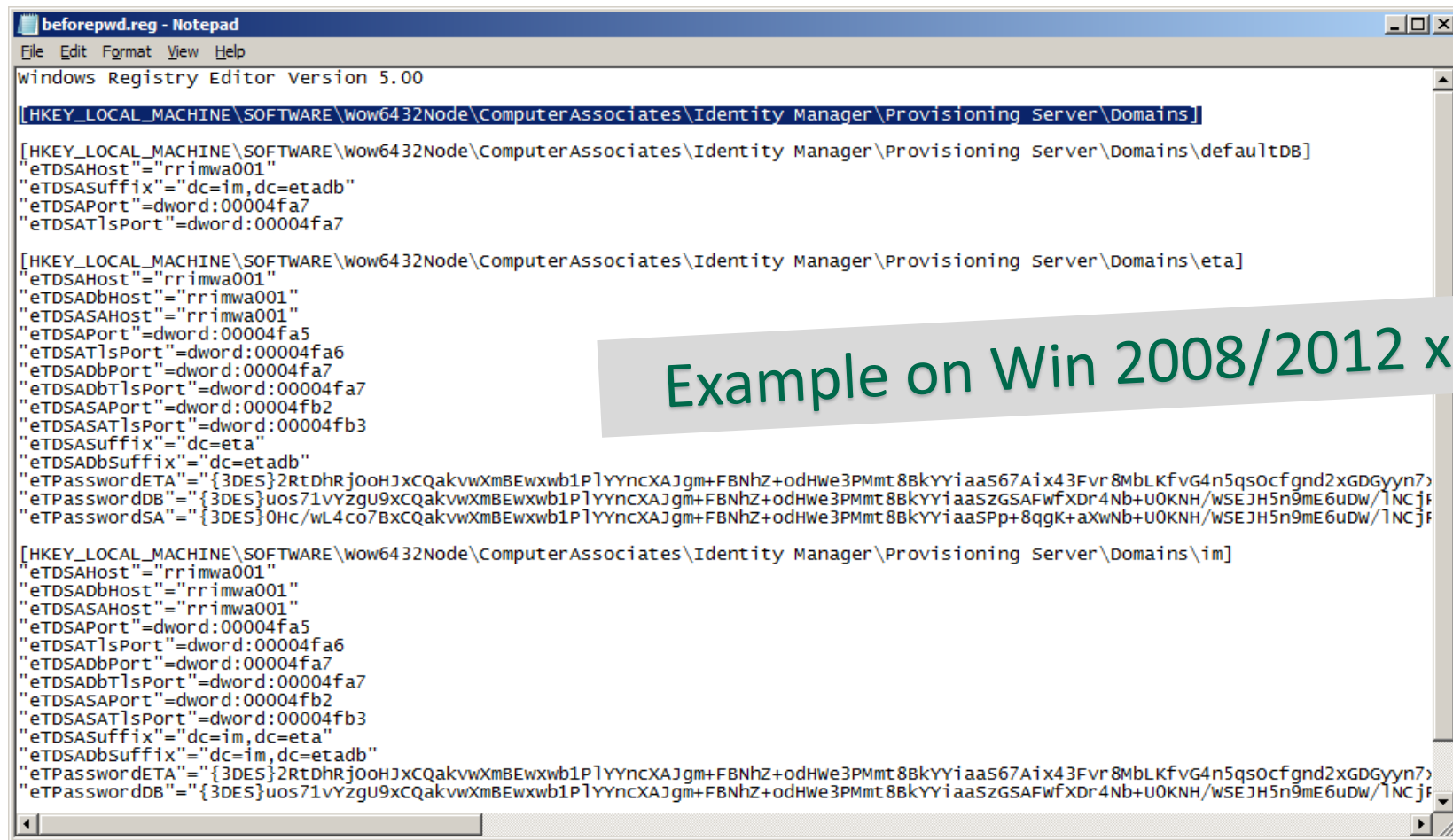
Password Locations for Service accounts

ID	Component	Password Location (s)	Primary Update Process	Secondary Update Process
SiteMinder	SM admin ID	1) ra.xml 2) SM PolicyStore	1) Use Password Encryption Tool in IAMSuite & then update ra.xml with password hash 2) Update SM admin password in SM PolicyStore	None
Idmembedded (or as created during installation)	IIM Management Console Authentication Directory's ID. Bootstrap directory for authentication. May be changed to use IMCD	1) iam/im/jdbc/jdbc/objectstore IM_AUTH_USER	1) Use IM Management Console to export Authentication Directory XML; update and reimport XML 2) Select IMCD and use Update Authentication to move from database to IMCD as authentication source for Management Console.	None.
idmadmin (or as created during installation)	J2EE Admin ID for JBOSS EAP 6.1	1) JBOSS configuration file mgmt.-users.properties This will be different process for other version of JBOSS	1) Use Jboss Admin Console	1) Use add-user.bat/sh to re-create userid entry with new password hash
J2EE Admin (non-JBOSS)	J2EE Admin ID for Oracle WebLogic / IBM WebSphere	1) Embedded within the J2EE solution data source	1) Use Admin Console of either J2EE Tool	None
imdba001, imdba002, etc.	Oracle/SQL Database Source DSN Ids to allow IM to use	1) XML files under EAP 6.1: Jboss_home\standalone\configuration\ Community: jboss_home\server\default\deploy\	1) Use IM Password Encryption Tool in IAMSuite & then update XML files with password hash.	None
gadmin	GovernanceMinder Admin ID to access IdentityMinder (used for SOD requirements to avoid using a single admin id)	1) Corporate User Store 2) GovernanceMinder Console	1) Use IME User Console 2) Use GM User Console	1) Use jxplorer to corporate userstore.

Backup Before Making IMPD Password Change - 1 of 3

- Use MS Windows Registry tool to export the branch below on **ALL** IMPS servers

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains]



```
beforepwd.reg - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\defaultdb]
"eTDSAHost"="rrimwa001"
"eTDSASuffix"="dc=im,dc=etadb"
"eTDSAPort"=dword:00004fa7
"eTDSATlsPort"=dword:00004fa7

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\eta]
"eTDSAHost"="rrimwa001"
"eTDSADbHost"="rrimwa001"
"eTDSASAHost"="rrimwa001"
"eTDSAPort"=dword:00004fa5
"eTDSATlsPort"=dword:00004fa6
"eTDSADbPort"=dword:00004fa7
"eTDSADbTlsPort"=dword:00004fa7
"eTDSASAPort"=dword:00004fb2
"eTDSASATlsPort"=dword:00004fb3
"eTDSASuffix"="dc=eta"
"eTDSADbSuffix"="dc=etadb"
"eTPasswordETA"="{3DES}2RtDhRj0oHjxCQakvwXmBEwxwb1PlyYncXAJgm+FBNhZ+odHwe3PMmt8BkYYiaa567Aix43Fvr8MbLKfVG4n5qsOcfgnd2xGDgyyn7>"
"eTPasswordDB"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PlyYncXAJgm+FBNhZ+odHwe3PMmt8BkYYiaa567Aix43Fvr8MbLKfVG4n5qsOcfgnd2xGDgyyn7>"
"eTPasswordSA"="{3DES}0Hc/wL4co7BxCQakvwXmBEwxwb1PlyYncXAJgm+FBNhZ+odHwe3PMmt8BkYYiaa567Aix43Fvr8MbLKfVG4n5qsOcfgnd2xGDgyyn7>"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im]
"eTDSAHost"="rrimwa001"
"eTDSADbHost"="rrimwa001"
"eTDSASAHost"="rrimwa001"
"eTDSAPort"=dword:00004fa5
"eTDSATlsPort"=dword:00004fa6
"eTDSADbPort"=dword:00004fa7
"eTDSADbTlsPort"=dword:00004fa7
"eTDSASAPort"=dword:00004fb2
"eTDSASATlsPort"=dword:00004fb3
"eTDSASuffix"="dc=im,dc=eta"
"eTDSADbSuffix"="dc=im,dc=etadb"
"eTPasswordETA"="{3DES}2RtDhRj0oHjxCQakvwXmBEwxwb1PlyYncXAJgm+FBNhZ+odHwe3PMmt8BkYYiaa567Aix43Fvr8MbLKfVG4n5qsOcfgnd2xGDgyyn7>"
"eTPasswordDB"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PlyYncXAJgm+FBNhZ+odHwe3PMmt8BkYYiaa567Aix43Fvr8MbLKfVG4n5qsOcfgnd2xGDgyyn7>"
```

Example on Win 2008/2012 x64

Backup Before Making IMPD Password Change - 2 of 3

- Use Jxplorer and DXHOME\dxserver\config\settings\impd_anon.dxc file
 - Replace existing impd.dxc file with impd_anon.dxc ; and perform: dxserver init all
 - Then use Jxplorer to connect anonymously to main DSA on TCP **20394 & no Base DN**
- Export the LDIF branch of 1st DSA Account:
eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb

The image shows two overlapping windows from the Jxplorer application. The 'Open LDAP/DSML Connection' window on the left is configured with Host: rrimwa001, Port: 20394, Protocol: LDAP v3, and Security Level: Anonymous. The User DN is set to s,eTNamespaceName=CommonObjects,dc=etadb. The 'JXplorer - impd_router_20391' window on the right shows a tree view with 'World' > 'etadb' > 'CommonObjects' > 'DSAs' selected. The right pane displays a table of attributes for the selected object.

attribute type	value
eTDSAContainerName	DSAs
objectClass	eTDSAContainer
userPassword	(non string data)
eTAgentOnly	
eTAllowPartialResult	

Backup Before Making IMPD Password Change - 3 of 3

- Use Jxplorer and DXHOME\dxserver\config\settings\impd_anon.dxc file
 - Replace existing impd.dxc file with impd_anon.dxc ; and perform: dxserver init all
 - Then use Jxplorer to connect anonymously to co DSA on TCP **20396 & no Base DN**
- Export the LDIF branch of 2nd DSA Account:
eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,**dc=im**,dc=etadb

The image shows two overlapping windows from the Jxplorer application. The 'Open LDAP/DSML Connection' window on the left is configured with Host: rrimwa001, Port: 20396, Protocol: LDAP v3, and Security Level: Anonymous. The User DN is set to s,eTNamespaceName=CommonObjects,dc=etadb. The 'JXplorer - impd_router_20391' window on the right displays a directory tree with 'etadb' expanded, showing 'im' and 'CommonObjects'. The 'DSAs' folder under 'CommonObjects' is selected. The right pane shows the HTML View of the selected object, displaying attributes like eTDSAContainerName (DSAs), objectClass (eTDSAContainer), and userPassword ((non string data)).

attribute type	value
eTDSAContainerName	DSAs
objectClass	eTDSAContainer
objectClass	top
userPassword	((non string data))
eTAgentOnly	
eTAllowPartialResult	
eTCheckDelete	
eTCheckPermission	
eTComments	
eTCreateDate	
eTCreateNode	
eTCreateTime	
eTCreateUserid	
eTCreateUserName	
eTDBOnly	
eTDeleteEntry	

IMPS PWDMGR Tool: Component=IM Provisioning Server relates to the maintenance account cn=etaserver,dc=eta per IM bookshelf note

Local Domain: im.

Administrator ID: idmadmin

Password for administrator: [masked]

Component: IM Provisioning Server

For Domain: eta

New Password: [masked]

Confirm: [masked]

Password locked down to the following server/port/tls_port:

Host: imps-001

Port: 20389

Tls Port: 20390

Use TLS: Yes

Buttons: Apply, Close, Help

pwdmgr [X]
Successfully set Provisioning Server password.
OK

IMPS Domain Configuration / Authentication/Disable Maintenance User
Values: No (default) or Yes

Description: Set this parameter to yes to disable the ability to authenticate to the Provisioning Server using the built-in user with the Distinguished Name cn=etaserver,dc=eta. This user, whose password is controlled by the pwdmgr utility, is used internally during installation. After installation, this user is only needed for maintenance functions such as resetting an administrator's password. We recommend that you disable this user after installation.

Local Domain: im.

Administrator ID: idmadmin

Password for administrator: [masked]

Component: IM Provisioning Server

For Domain: im

New Password: [masked]

Confirm: [masked]

Password locked down to the following server/port/tls_port:

Host: imps-001

Port: 20389

Tls Port: 20390

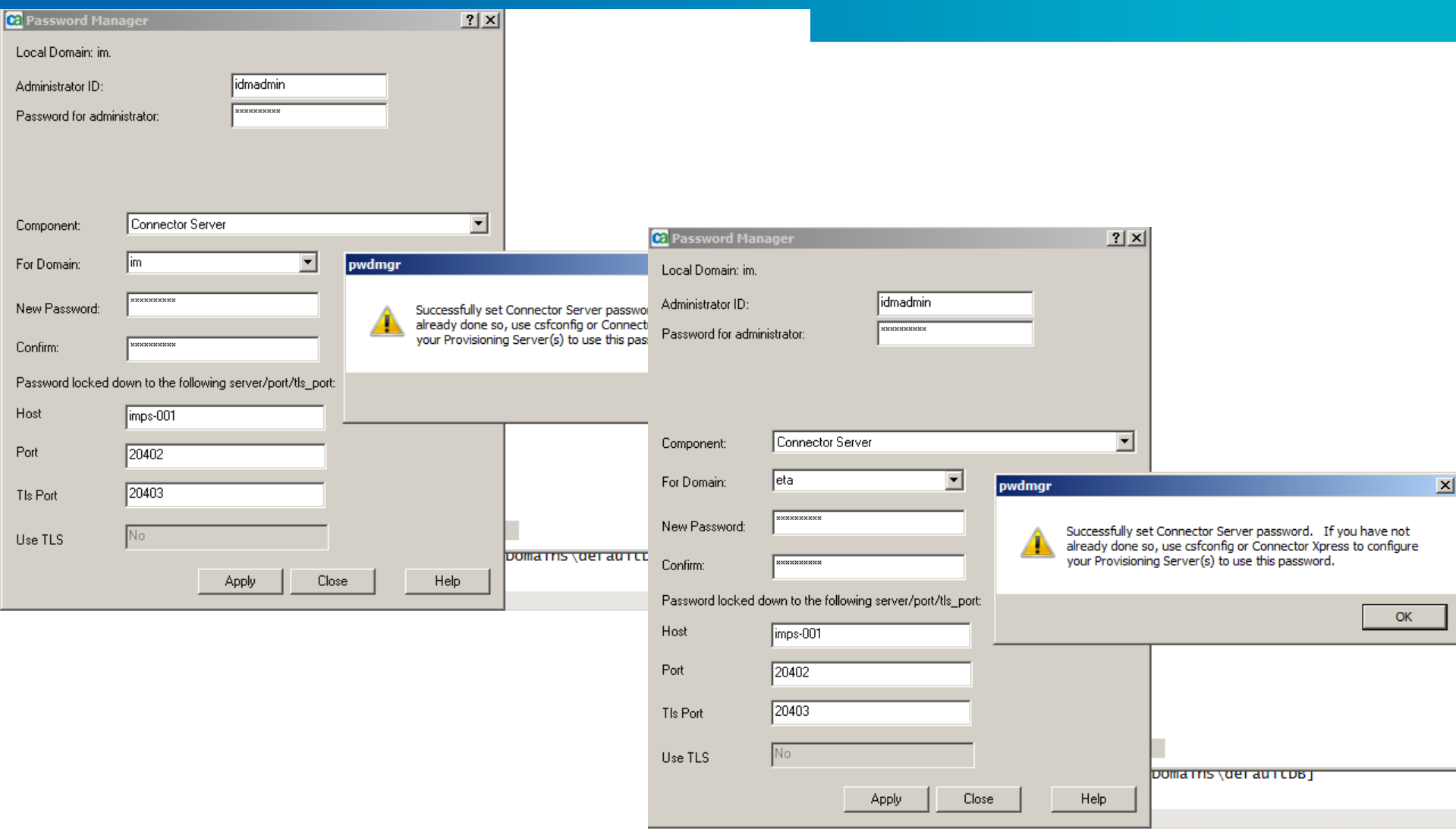
Use TLS: Yes

Buttons: Apply, Close, Help

pwdmgr [X]
Successfully set Provisioning Server password.
OK

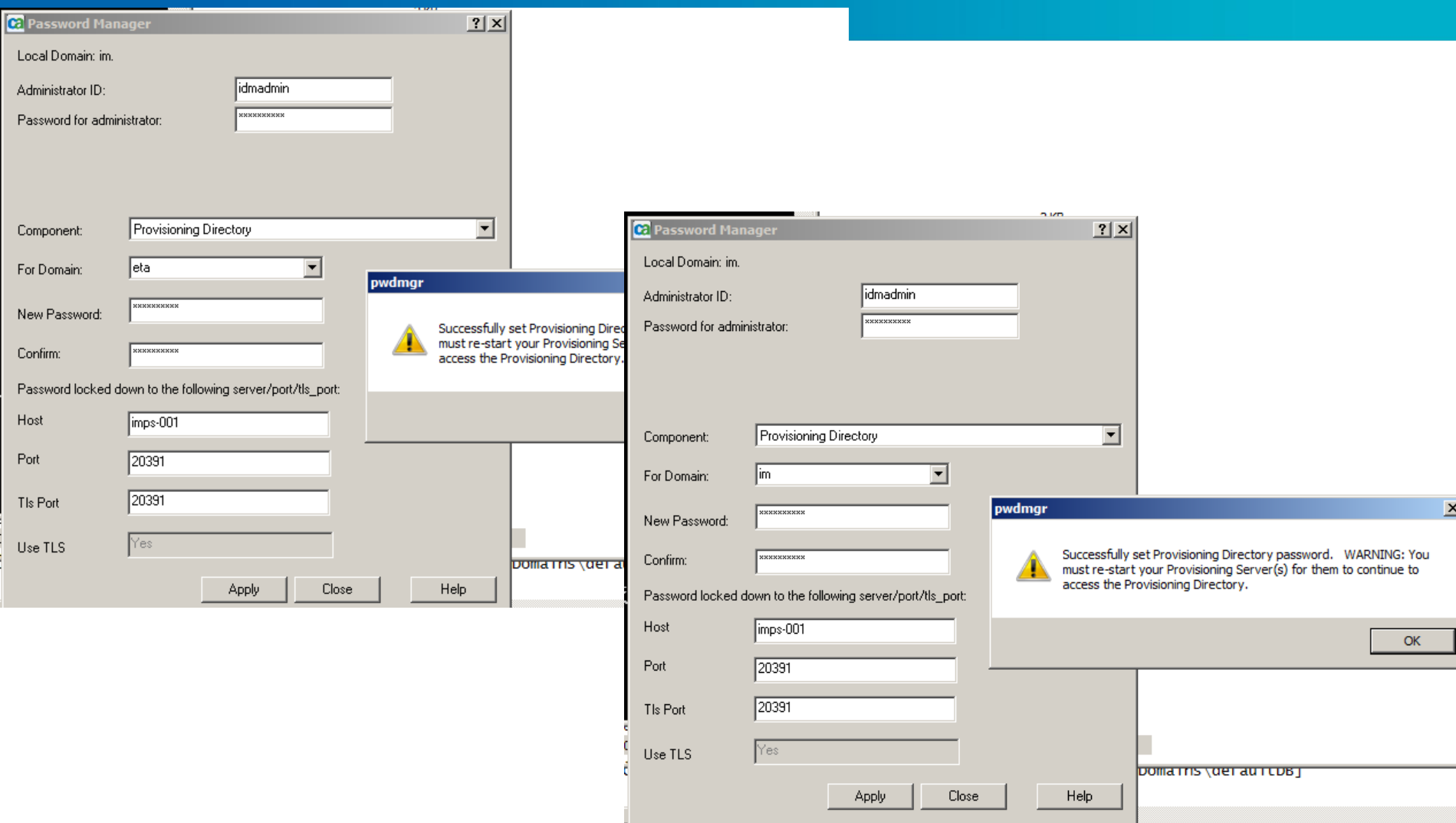
cn=etaserver,dc=eta

IMPS PWDMGR Tool: Component=Connector Server relates to the connection (service account) between IMPS and the CCS components



cn=root,dc=etasa

IMPS PWDMGR Tool: Component=Provisioning Directory relates to the connection (service account) between IMPS and the IMPD DSA Router/Data components



eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb

eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=im,dc=etadb

Verification Example: Registry Strings before and after use of PwdMgr Tool

BEFORE

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\eta]
- "eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYYncXAJgm+FBNhZ+odHWe3PMmt8BkYYiaaS67Aix43Fvr8MbLKfvG4n5qsOcfgnd2xGDGyyn7xuJ+YreqSLBGVqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38kA1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDGk1e0MbLKfvG4n5hQQq30scOPOb5PmuPrTKHqrTHxaOv2MW2gSB6CXSwuaCja0CFpVluU3aOadyhDmypojsbra9UkJzQPhOLd4r2qbJ1WMA2cr6A1v5TQo0f9ZncXX0yEaDw4="

AFTER

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\eta]
- "eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYYncXAJgm+FBNhZ+odHWe3PMmt8BkYYiaaS67Aix43Fvr8MbLKfvG4n5qsOcfgnd2xGDGyyn7xuJ+YreqSLBGVqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38kA1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDGk1e0MbLKfvG4n5hQQq30scOPOHQMx9kLgJYCHDnVUU+BOGd3eOi/nNgg06VGPI0sKPKyrTHxaOv2MW2gSB6CXSwuaCja0CFpVluV0ez7grskBag1v5TQo0f9ZncXX0yEaDw4="

Verification Example: Full View of all Registry Strings before and after

BEFORE

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\etata]

"eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Aix43Fvr8MbLkFvG4n5qsOcfngnd2xGDGyyn7xuJ+YreqSLBGvqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38ka1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDgk1e0MbLkFvG4n5hQqQ30scOPOb5PmuPrTKHqRTHxaOv2MW2gSB6CXswuaCjaOCFpVluU3aOadyhDmpjSbra9UkJzQPhOLd4r2qbj1WMA2c6A1v5TQo0f9ZncXX0yEaDw4="

"eTPasswordDB"="{3DES}0Hc/wL4co7BxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567GSAFWfXDr4Nb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPN96QfN8mXe0wxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT53cs7tm40KTINb+U0KNH/WVLCwIxfRsQEcXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi3TUT0oanhPFoeE8megiYLn+XGURgbaAY5xiXoLR2y+0wxwb1PIYnR/PEwqE+vyU="

"eTPasswordSA"="{3DES}oqNKkskRlnNxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Pp+8qgk+aXwNb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPjEX7JiHplkwxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT50HdmoWUPoH8Nb+U0KNH/WVLCwIxfRsQEcXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi3TUT0oanhPFtCgc/IO8+4K0XbhmIhcWGQGe3XDIYkOeGiSfxxD/cK3"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im]

"eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Aix43Fvr8MbLkFvG4n5qsOcfngnd2xGDGyyn7xuJ+YreqSLBGvqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38ka1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDgk1e0MbLkFvG4n5hQqQ30scOPOb5PmuPrTKHqRTHxaOv2MW2gSB6CXswuaCjaOCFpVluU3aOadyhDmpjSbra9UkJzQPhOLd4r2qbj1WMA2c6A1v5TQo0f9ZncXX0yEaDw4="

"eTPasswordDB"="{3DES}0Hc/wL4co7BxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567GSAFWfXDr4Nb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPN96QfN8mXe0wxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT53cs7tm40KTINb+U0KNH/WVLCwIxfRsQEcXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi3TUT0oanhPFoeE8megiYLn+XGURgbaAY5xiXoLR2y+0wxwb1PIYnR/PEwqE+vyU="

"eTPasswordSA"="{3DES}oqNKkskRlnNxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Pp+8qgk+aXwNb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPjEX7JiHplkwxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT50HdmoWUPoH8Nb+U0KNH/WVLCwIxfRsQEcXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi3TUT0oanhPFtCgc/IO8+4K0XbhmIhcWGQGe3XDIYkOeGiSfxxD/cK3"
```

AFTER

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\etata]

"eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Aix43Fvr8MbLkFvG4n5qsOcfngnd2xGDGyyn7xuJ+YreqSLBGvqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38ka1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDgk1e0MbLkFvG4n5hQqQ30scOPOHQMx9klgJYCHDNVUU+BOGD3eOi/nNgg06VGPI0sKPKyrTHxaOv2MW2gSB6CXswuaCjaOCFpVluV0ez7grskBag1v5TQo0f9ZncXX0yEaDw4="

"eTPasswordDB"="{3DES}0Hc/wL4co7BxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567GSAFWfXDr4Nb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPN96QfN8mXe0wxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT53cs7tm40KTINb+U0KNH/WVLCwIxfRsQEHY1tbUHW22/nJtDjCh5iWfXVWg9wNYVicXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi38M/VFZBvO3Ewxwb1PIYnR/PEwqE+vyU="

"eTPasswordSA"="{3DES}oqNKkskRlnNxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Pp+8qgk+aXwNb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPjEX7JiHplkwxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT50HdmoWUPoH8Nb+U0KNH/WVLCwIxfRsQEHY1tbUHW22+HyY096dKi5HjnxA6zvH9xjG10fSusxkY4hkD/ibYy8uengArm2DGyyn7xuJ+Y59f9Yb/gWjmiSfxxD/cK3"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im]

"eTPasswordETA"="{3DES}uos71vYzgU9xCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Aix43Fvr8MbLkFvG4n5qsOcfngnd2xGDGyyn7xuJ+YreqSLBGvqZRglFIWXdzuk/kOCy1aUTi0h74XICW2OGMYxtJX0rrMkAja/oFZ2i4R3cRsXQ38ka1v5TQo0f9Z1uXIVGHewDoNb+U0KNH/WVLCwIxfRsQEBtWApDgk1e0MbLkFvG4n5hQqQ30scOPOHQMx9klgJYCHDNVUU+BOGD3eOi/nNgg06VGPI0sKPKyrTHxaOv2MW2gSB6CXswuaCjaOCFpVluV0ez7grskBag1v5TQo0f9ZncXX0yEaDw4="

"eTPasswordDB"="{3DES}0Hc/wL4co7BxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567GSAFWfXDr4Nb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPN96QfN8mXe0wxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT53cs7tm40KTINb+U0KNH/WVLCwIxfRsQEHY1tbUHW22/nJtDjCh5iWfXVWg9wNYVicXAJgm+FBNigkTBijcocsn7mz7D9as5z/kOCy1aUTi38M/VFZBvO3Ewxwb1PIYnR/PEwqE+vyU="

"eTPasswordSA"="{3DES}oqNKkskRlnNxCQakvwXmBEwxwb1PIYncXAJgm+FBNhZ+odHWe3PMmt8BkYyiaa567Pp+8qgk+aXwNb+U0KNH/WSEJH5n9mE6uDW/INCjR/1mLJA3ncRj8yl6l7LdjfIBVDGyyn7xuJ+Yb/sIY3Vpw0Axssp+8bifm1qx4lxZ9KpPjEX7JiHplkwxwb1PIYnOfrXGIZ6RtdMMcG9T5WGJ+VHJjCSRLT50HdmoWUPoH8Nb+U0KNH/WVLCwIxfRsQEHY1tbUHW22+HyY096dKi5HjnxA6zvH9xjG10fSusxkY4hkD/ibYy8uengArm2DGyyn7xuJ+Y59f9Yb/gWjmiSfxxD/cK3"
```

Verification Example Using Idifdelta – check before and after

— Main DSA

```
Idifdelta -S IMPS-001-impd-main 20140123_19405742_IMPS-001-impd-main-sorted.Idif 20140123_19132563_IMPS-001-impd-main-sorted.Idif
```

— CO (common objects) DSA

```
Idifdelta -S IMPS-001-impd-co 20140123_19132563_IMPS-001-impd-co-sorted.Idif 20140123_19405742_IMPS-001-impd-co-sorted.Idif
```

— INC (inclusions) DSA

```
Idifdelta -S IMPS-001-impd-inc 20140123_19132563_IMPS-001-impd-inc-sorted.Idif 20140123_19405742_IMPS-001-impd-inc-sorted.Idif
```

Idif files created with CA Directory dxdumpdb process

Verification Example: Delta in IMPD Main DSA

dn: eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb

changetype: modify

replace: eTUpdateDate

eTUpdateDate: 0000112193

-

replace: eTUpdateTime

eTUpdateTime: 0006041000

-

replace: eTUpdateUserName

eTUpdateUserName: idmadmin

-

replace: modifyTimestamp

modifyTimestamp: 20120711214650.572Z

-

replace: userPassword

userPassword: {SHA}xGSvgXKHNDMFy9ZJPfK4hWld9TE=

-

Idifdelta summary:

130665 entries in old file

130665 entries in new file

Produced:

0 add entry records

0 delete entry records

1 modify entry records

Connection credentials used by IMPS to communicate to IMPS DSA Router for IMPD

Verification Example: Delta in IMPD CO DSA

dn: eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=im,dc=etadb

changetype: modify

replace: eTUpdateDate

eTUpdateDate: 0000114023

-

replace: eTUpdateTime

eTUpdateTime: 0006979700

-

replace: eTUpdateUserid

eTUpdateUserid: idmadmin

-

replace: eTUpdateUserName

eTUpdateUserName: DO NOT REMOVE idmadmin

-

replace: modifyTimestamp

modifyTimestamp: 20140124012317.742Z

-

replace: userPassword

userPassword: {SSHA512}CkZfP43j2LRxwv52M7ROWUFZGONY2DY8pggbizJpWyKFjEAuoazFaO

6xQNUboVLcreGZR1ohejMM7kzjenF2T38CPo=

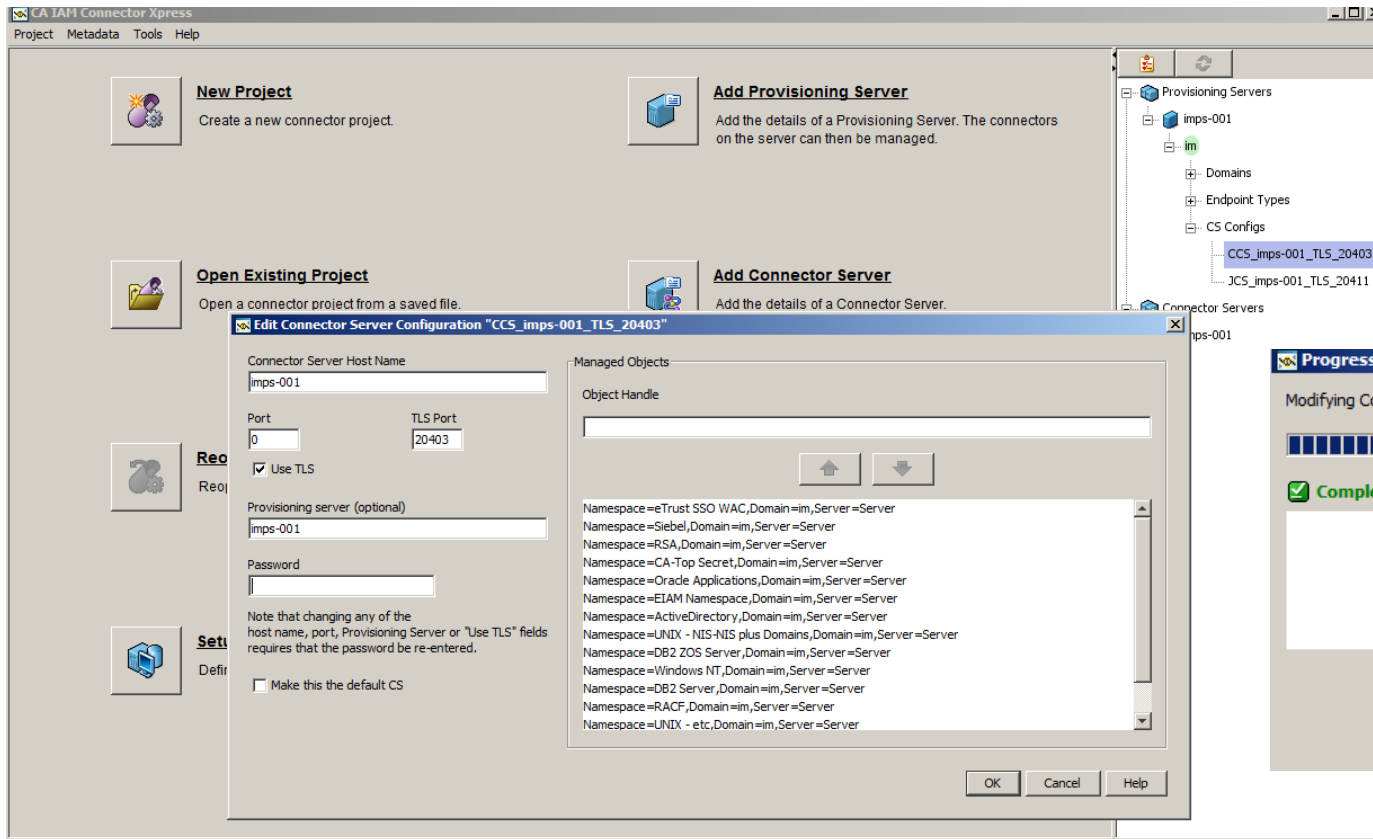
-

- Idifdelta summary:
- 278 entries in old file
- 267 entries in new file
- Produced:
- 0 add entry records
- 11 delete entry records
- 1 modify entry records

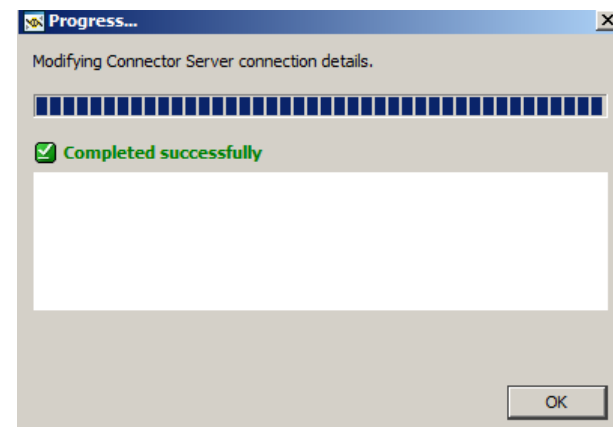
Verification Example: Delta in IMPD INC DSA

- Idifdelta summary:
 - 47 entries in old file
 - 47 entries in new file
- Produced:
 - 0 add entry records
 - 0 delete entry records
 - 0 modify entry records

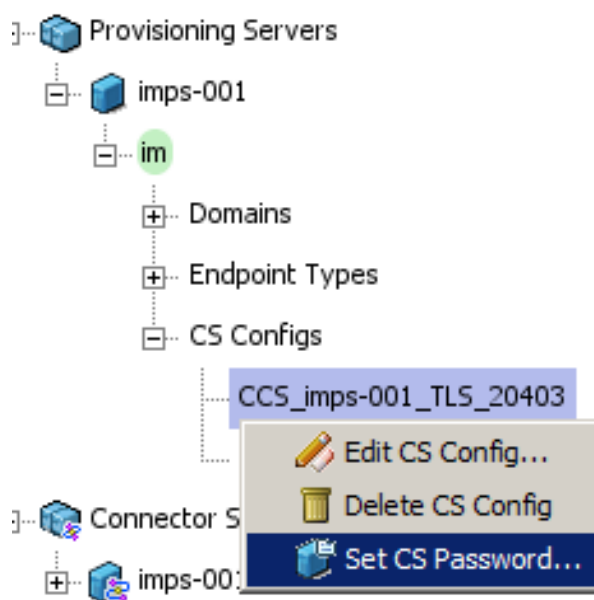
How to Use Connector Xpress to Update CCS Password



Right click and select
Edit CS Config



Do **not** use this selection for CCS Pwd



— **Set CS Password Only** works for JCS

Modify under CO DSA if pwd is different

ldifdelta -S IMPS-001-impd-co 20140123_20113952_IMPS-001-impd-co-sorted.ldif
20140123_20360545_IMPS-001-impd-co-sorted.ldif

dn: eTConfigParamName=Password,eTConfigParamFolderName=CCSimps-001_TLS_20403, eTConfigParamFolderName=Connector
Servers,eTConfigParamContainerName=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=CommonObjects,dc=im, dc=etadb

changetype: modify

replace: eTConfigParamValue

eTConfigParamValue:
{3DES}aKA8VIBCQX1d+L5VsSNIGe1lXmn4xVaw6QaQ2LoTIHX2WAmaZ3+z3g==

-

replace: modifyTimestamp

modifyTimestamp: 20140124023433.896Z

-

- ldifdelta summary:
- 267 entries in old file
- 267 entries in new file
- Produced:
- 0 add entry records
- 0 delete entry records
- 1 modify entry records

Note: No changes under Main, CO or INC DSA if new password is same as current password

Idifdelta -S IMPS-001-impd-inc

20140123_19132563_IMPS-001-impd-inc-sorted.ldif

20140123_20113952_IMPS-001-impd-inc-sorted.ldif

Idifdelta summary:

47 entries in old file

47 entries in new file

Produced:

0 add entry records

0 delete entry records

0 modify entry records

Idifdelta -S IMPS-001-impd-co

20140123_19405742_IMPS-001-impd-co-sorted.ldif

20140123_20113952_IMPS-001-impd-co-sorted.ldif

Idifdelta summary:

267 entries in old file

267 entries in new file

Produced:

0 add entry records

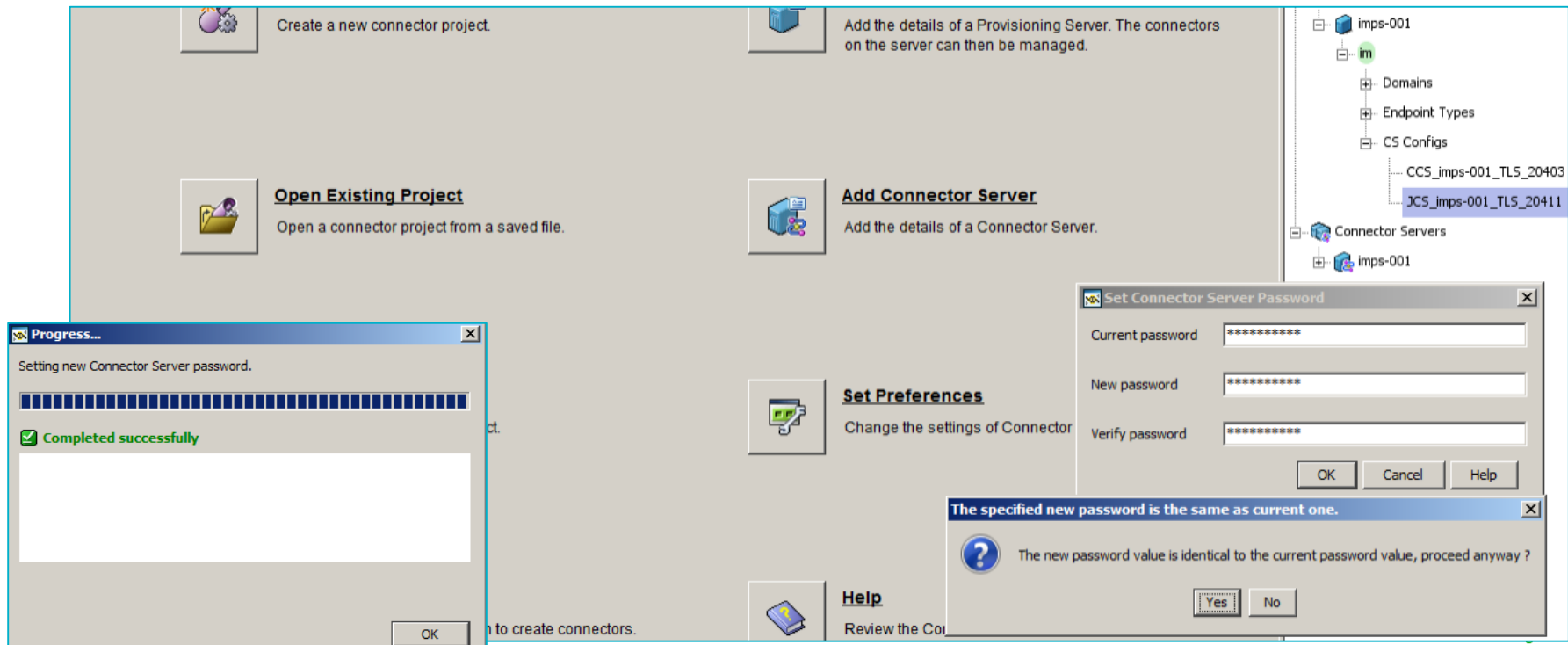
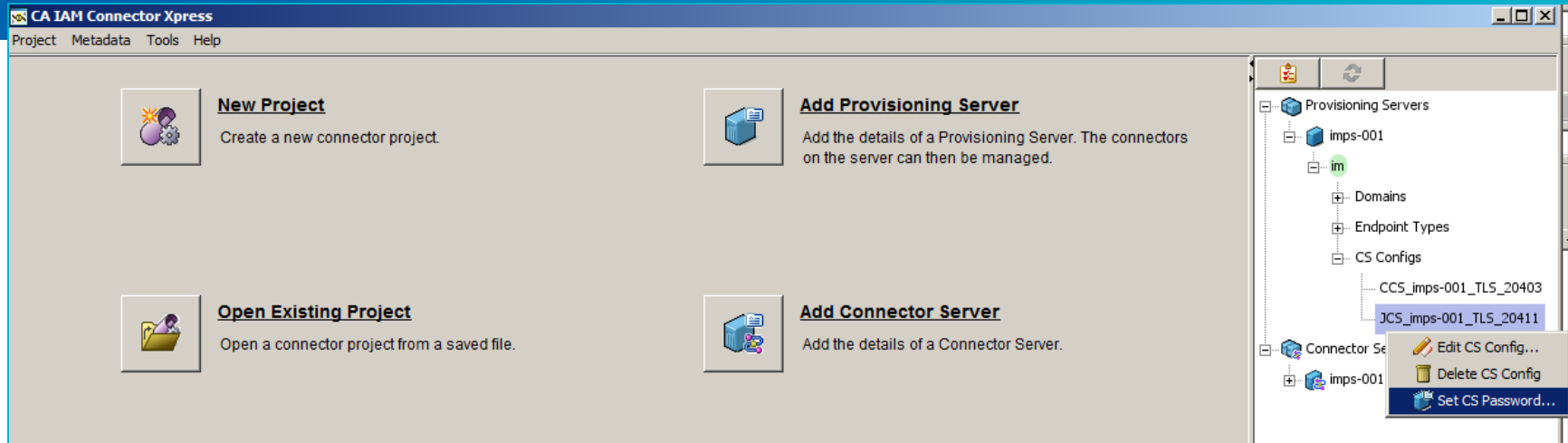
0 delete entry records

0 modify entry records

IAMCS (JCS) Password: uid=admin,ou=system

- Three (3) ways:
 - ConnectorXpress
 - Integrated JCS: Acquire IMPS Server and select JCS; right click to reset password.
 - Standalone JCS: Acquire standalone JCS; right click to reset password.
 - IAMCS Web Console
 - Login with id: admin and current password; reset password in UI
 - Use Jxplorer to reset
 - Login with id: uid=admin,ou=system and current password; reset password in Jxplorer
- https://supportcontent.ca.com/cadocs/O/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/docs/index.htm?toc.htm?1795944.html?zoom_highlight=Change%2Bthe%2BJava%2BCS%2BAdministration%2BStored%2BPassword
- If current password is unknown,
 - Update IAMCS configuration to allow anonymous connection, change token value from false to true, bounce the im_jcs service, then use Jxplorer to set the password for this id: uid=admin,ou=system on port 20410 (wo ssl) ; reset token afterwards.
 - IM r12.6.3 JCS conf folder & file: Connector Server\jcs\conf\server_osgi_ad.xml
 - `<property name="allowAnonymousAccess"><value>false</value></property>`
 - Note: IM r12.5 will likely be a different filename but same token.

Change IAMCS Password with Connector Xpress



Jxplorer Example to IAMCS 20410/20411

Open LDAP/DSML Connection

Host: localhost Port: 20410

Protocol: LDAP v3

Optional Values

Base DN:

Read Only: ☐

Security

Level: User + Password

User DN: uid=admin,ou=system

Password:

Use a Template

Save iamcs_20410 Delete Default

OK Cancel Help

Open LDAP/DSML Connection

Host: localhost Port: 20411

Protocol: LDAP v3

Optional Values

Base DN:

Read Only: ☐

Security

Level: SSL + User + Password

User DN: cn=root,dc=etasa

Password:

Use a Template

Save iamcs_20411_root Delete Default

OK Cancel Help

JXplorer - iamcs_20410

File Edit View Bookmark Search LDIF Options Tools Security Help

cn = Quick Search

Explore Results Schema

HTML View Table Editor

World

- system
 - admin
 - configuration
 - groups
 - sysPrefRoot
 - users

attribute type	value
cn	system administrator
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	inetOrgPerson
sn	administrator
createTimestamp	20140315002041Z
creatorsName	0.9.2342.19200300.100.1.1=admin,2.5.4.11=system
displayName	Directory Superuser
uid	admin
userPassword	(non string data)
audio	
businessCategory	

Submit Reset Change Class Properties

uid=admin,ou=system: (0)

IAMCS Anonymous Connection via Jxplorer

Set anonymous connection in IAMCS configuration files to use

Couldn't Connect: Try Again

Host: localhost Port: 20410

Protocol: LDAP v3

Optional Values

Base DN:

Read Only: ☐

Security

Level: Anonymous

User DN: uid=admin,ou=system

Password:

Use a Template

Save iamcs_20410 Delete Default

OK Cancel Help

Programs\CA\Identity Manager\Connector Server\jcs\conf

Name	Date modified	Type	Size
server_osgi_ad.xml	4/3/2014 10:15 AM	XML Document	20 KB
server_osgi_jcs.xml	3/14/2014 7:20 PM	XML Document	62 KB
server_osgi_shared.xml	3/14/2014 7:20 PM	XML Document	8 KB
ssl.keystore	3/14/2014 7:20 PM	KEYSTORE File	82 KB
server_osgi_common.xml	3/14/2014 7:19 PM	XML Document	8 KB
server_osgi_ad - Copy.xml	3/14/2014 7:19 PM	XML Document	20 KB

server_osgi_ad.xml Date modified: 4/3/2014 10:15 AM Date created: 3/14/2014 7:19 PM
XML Document Size: 19.8 KB

Error Encountered

Unable to perform Extended request Connection Request operation.

error details

javax.naming.NoPermissionException: [LDAP: error code 50 - code 50 (INSUFFICIENT_ACCESS_RIGHTS): failed on search operation: : Anonymous access disabled.]; remaining name ''

Print Stack OK

Administrator: Command Prompt

```
E:\Programs\CA\Identity Manager\Provisioning Server\bin>netstat -an | more
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1882	0.0.0.0:0	LISTENING
TCP	0.0.0.0:4105	0.0.0.0:0	LISTENING
TCP	0.0.0.0:20080	0.0.0.0:0	LISTENING
TCP	0.0.0.0:20410	0.0.0.0:0	LISTENING
TCP	0.0.0.0:20411	0.0.0.0:0	LISTENING
TCP	0.0.0.0:20443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:22001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:22002	0.0.0.0:0	LISTENING
TCP	0.0.0.0:22099	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING

net stop im_jcs

net stop im_ccs

net start im_ccs

net start im_jcs

Open LDAP/DSML Connection

Host: Port:

Protocol:

Optional Values

Base DN:

Read Only: ☐

Security

Level:

User DN:

Password:

Use a Template

Save Delete Default

OK Cancel Help

JXplorer - im_ccs_20403_root

File Edit View Bookmark Search LDIF Options Tools Security Help

cn Quick Search

Explore Results Schema

World

- etasa
 - Configuration
 - Installed Connectors

HTML View Table Editor

attribute type	value
eTConfigParamName	Installed Connectors
eTConfigParamValue	Access Control
eTConfigParamValue	CA-ACF2
eTConfigParamValue	ActiveDirectory
eTConfigParamValue	OS400
eTConfigParamValue	DB2 Server
eTConfigParamValue	DB2 ZOS Server
eTConfigParamValue	EIAM Namespace
eTConfigParamValue	UNIX - etc
eTConfigParamValue	Oracle Applications
eTConfigParamValue	KRB Namespace
eTConfigParamValue	Lotus Domino Server
eTConfigParamValue	Windows NT

Submit Reset Change Class Properties

eTConfigParamName=Installed Connectors,eTConfigContainerName=Configuration,dc=etasa: (0)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path

1:02:4...	im_ccs.exe	1672	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im\TPasswordSA
1:02:4...	im_ccs.exe	1672	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im\TPasswordSA
1:02:4...	im_ccs.exe	1672	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im\TPasswordSA
1:02:4...	im_ccs.exe	1672	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im\TPasswordSA
1:02:4...	im_ccs.exe	1672	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im
1:02:4...	javaw.exe	2352	TCP Receive	c0a8-5c8b::3831:271a:80fa:fff:49192 -> mimps001.r.dom:20403
1:02:4...	javaw.exe	2352	TCP Receive	c0a8-5c8b::3831:271a:80fa:fff:49192 -> mimps001.r.dom:20403
1:02:4...	javaw.exe	2352	TCP Receive	c0a8-5c8b::3831:271a:80fa:fff:49192 -> mimps001.r.dom:20403
1:02:4...	javaw.exe	2352	TCP Receive	c0a8-5c8b::3831:271a:80fa:fff:49192 -> mimps001.r.dom:20403

Showing 1,466 of 71,596 events (2.0%)

Backed by virtual memory

Event Properties

Date:	4/20/2014 1:02:47 PM
Thread:	3520
Class:	Registry
Operation:	RegQueryValue
Result:	SUCCESS
Path:	HKLM\SOFTWARE\Wow6432Node\ComputerAssociates\Identity Manager\Provisioning Server\Domains\im\TPasswordSA
Duration:	0.000094

Type: REG
Length: 4
Data:

Windows Event Viewer

Local Security Authority (LSA)

Source: Local Security Authority (LSA)

Date: 4/9/2014 1:02:47 PM

Thread: 3520

Class: Registry

Operation: Impersonation

Result: SUCCESS

Path: HLM\SOFTWARE\Wow6432node\Computer Associates\Identity Manager\Provisioning Server\Domains\pin\PasswordISA

Duration: 0.000094

Type: REG_SZ

Length: 742

Data: [XES]0h4L4ko7BcQk4vW8BxwbB7f1n043gn4B9h2+ad4t03Pm08B7t0a0Gp+80gK+at0h0+4u000+105E349de

Next highlighted

Copy All Close

AD Password Sync Agent – Debug with Single DC

Force a Secure Channel Session Between a Member and a Specific Domain Controller

Members often establish secure channel sessions with non-local domain controllers. To force a secure channel session between a member and a specific domain controller by using the /server parameter with the reset operation, type the following at the command prompt:

```
netdom reset /d:devgroup.example.com mywksta /Server:mylocalbdc
```

Ref: [http://technet.microsoft.com/en-us/library/cc776879\(d=printer,v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc776879(d=printer,v=ws.10).aspx)

Useful for testing the CA IM AD Reverse Sync Agent process.

Step 01: At the user's workstation; open command line window and execute **set**

Step 02: Record the current **LOGONSERVER** value.

Step 03: Execute the above command, netdom, with the correct AD domain information & selected DC Server for testing

Step 04: Exercise Use-Case for Self-Service Password Change,

e.g. Cntl-Alt-Del to access "Change a Password" task on MS Window Secure Logon Screen