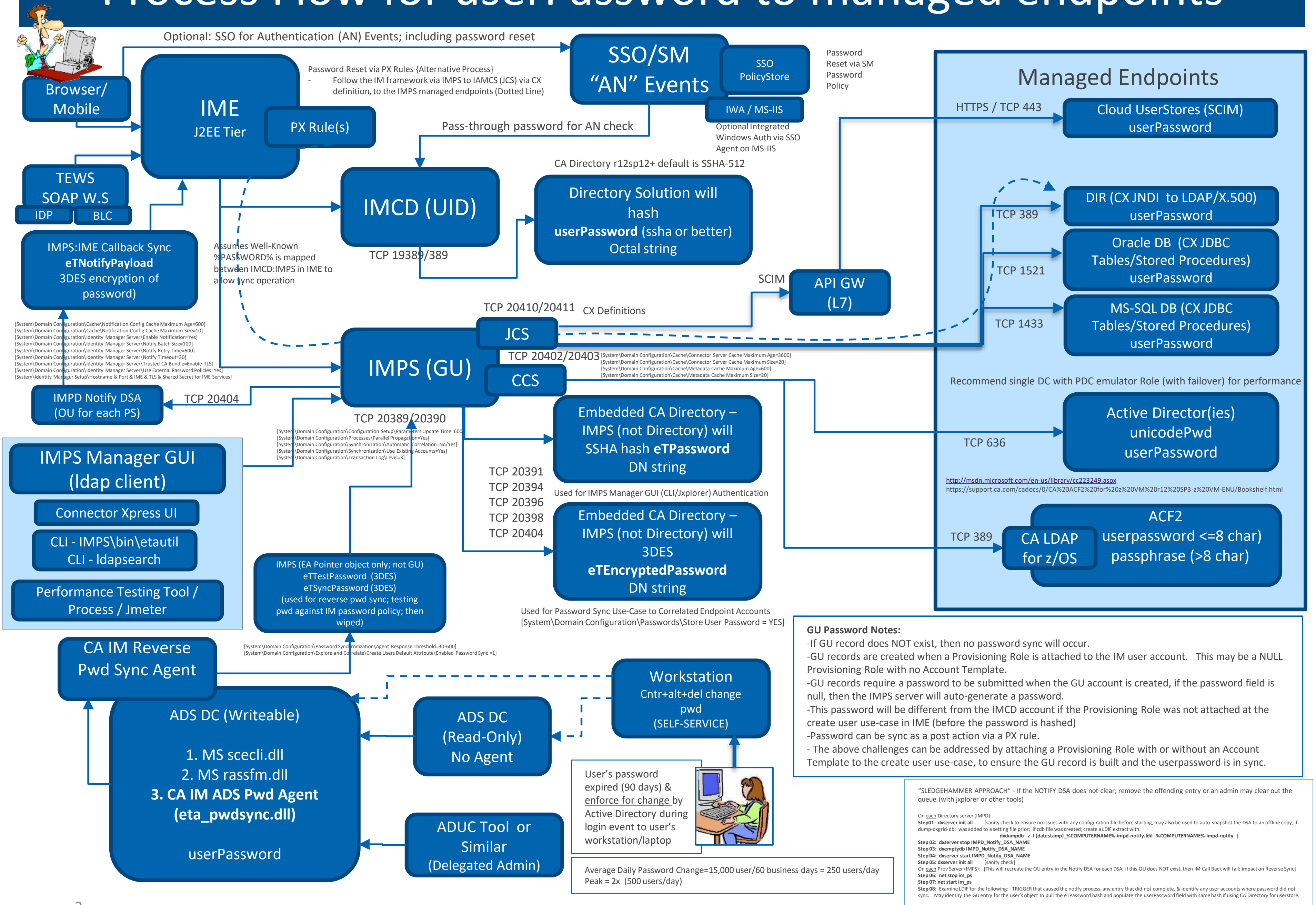
LIFECYCLE of the Password in the CA Identity Management Solution

IME/IMCD/IMPS/Endpoints(userstores) &
Active Directory (Reverse Sync Agent)

Alan Baugher
Sr. Principal Architect
Aug, 2016

Process Flow for userPassword to managed endpoints



Optional: SSO for Authentication (AN) Events; including password reset

Browser/ Mobile

IME
J2EE Tier

PX Rule(s)

Password Reset via PX Rules {Alternative Process}
- Follow the IM framework via IMPS to IAMCS (JCS) via CX definition, to the IMPS managed endpoints (Dotted Line)

SSO/SM "AN" Events

SSO PolicyStore

IWA / MS-IIS

Optional Integrated Windows Auth via SSO Agent on MS-IIS

Password Reset via SM Password Policy

Pass-through password for AN check

TEWS SOAP W.S

IDP

BLC

IMCD (UID)

TCP 19389/389

CA Directory r12sp12+ default is SSHA-512

Directory Solution will hash **userPassword** (ssha or better) Octal string

IMPS:IME Callback Sync **eTNotifyPayload** 3DES encryption of password)

Assumes Well-Known %PASSWORD% is mapped between IMCD:IMPS in IME to allow sync operation

```
[System\Domain Configuration\Cache\Notification Config Cache Maximum Age=600]
[System\Domain Configuration\Cache\Notification Config Cache Maximum Size=10]
[System\Domain Configuration\Identity Manager Server\Enable Notification=Yes]
[System\Domain Configuration\Identity Manager Server\Notify Batch Size=100]
[System\Domain Configuration\Identity Manager Server\Notify Retry Time=600]
[System\Domain Configuration\Identity Manager Server\Notify Timeout=30]
[System\Domain Configuration\Identity Manager Server\Trusted CA Bundle=Enable TLS]
[System\Domain Configuration\Identity Manager Server\Use External Password Policies=Yes]
[System\Identity Manager Setup\Hostname & Port & IME & TLS & Shared Secret for IME Services]
```

IMPD Notify DSA (OU for each PS)

TCP 20404

TCP 20410/20411

CX Definitions

SCIM

API GW (L7)

JCS

IMPS (GU)

TCP 20402/20403

```
[System\Domain Configuration\Cache\Connector Server Cache Maximum Age=3600]
[System\Domain Configuration\Cache\Connector Server Cache Maximum Size=20]
[System\Domain Configuration\Cache\Metadata Cache Maximum Age=600]
[System\Domain Configuration\Cache\Metadata Cache Maximum Size=20]
```

CCS

TCP 20389/20390

```
[System\Domain Configuration\Configuration Setup\Parameters Update Time=600]
[System\Domain Configuration\Processes\Parallel Propagation=Yes]
[System\Domain Configuration\Synchronization\Automatic Correlation=No/Yes]
[System\Domain Configuration\Synchronization\Use Existing Accounts=Yes]
[System\Domain Configuration\Transaction Log\Level=3]
```

Managed Endpoints

HTTPS / TCP 443

Cloud UserStores (SCIM) userPassword

TCP 389

DIR (CX JNDI to LDAP/X.500) userPassword

TCP 1521

Oracle DB (CX JDBC Tables/Stored Procedures) userPassword

TCP 1433

MS-SQL DB (CX JDBC Tables/Stored Procedures) userPassword

Recommend single DC with PDC emulator Role (with failover) for performance

TCP 636

Active Director(ies) unicodePwd userPassword

http://msdn.microsoft.com/en-us/library/cc223249.aspx
https://support.ca.com/cadocs/0/CA%20ACF2%20for%20z%20VM%20r12%20SP3-z%20VM-ENU/Bookshelf.html

TCP 389

CA LDAP for z/OS

ACF2 userpassword <=8 char) passphrase (>8 char)

Embedded CA Directory – IMPS (not Directory) will SSHA hash **eTPassword** DN string

Used for IMPS Manager GUI (CLI/Jxplorer) Authentication

TCP 20391
TCP 20394
TCP 20396
TCP 20398
TCP 20404

Embedded CA Directory – IMPS (not Directory) will 3DES **eTEncryptedPassword** DN string

Used for Password Sync Use-Case to Correlated Endpoint Accounts
[System\Domain Configuration\Passwords\Store User Password = YES]

IMPS Manager GUI (ldap client)

Connector Xpress UI

CLI - IMPS\bin\etautil
CLI - ldapsearch

Performance Testing Tool / Process / Jmeter

IMPS (EA Pointer object only; not GU) eTTestPassword (3DES) eTSyncPassword (3DES) (used for reverse pwd sync; testing pwd against IM password policy; then wiped)

```
[System\Domain Configuration\Password Synchronization\Agent Response Threshold=30-600]
[System\Domain Configuration\Explore and Correlate\Create Users Default Attribute\Enabled Password Sync =1]
```

CA IM Reverse Pwd Sync Agent

ADS DC (Writeable)

1. MS scecli.dll
2. MS rassfm.dll
3. CA IM ADS Pwd Agent (eta_pwdsync.dll)

userPassword

ADS DC (Read-Only) No Agent

ADUC Tool or Similar (Delegated Admin)

Workstation
Cntr+alt+del change pwd
(SELF-SERVICE)

User's password expired (90 days) & enforce for change by Active Directory during login event to user's workstation/laptop

Average Daily Password Change=15,000 user/60 business days = 250 users/day
Peak = 2x (500 users/day)

GU Password Notes:

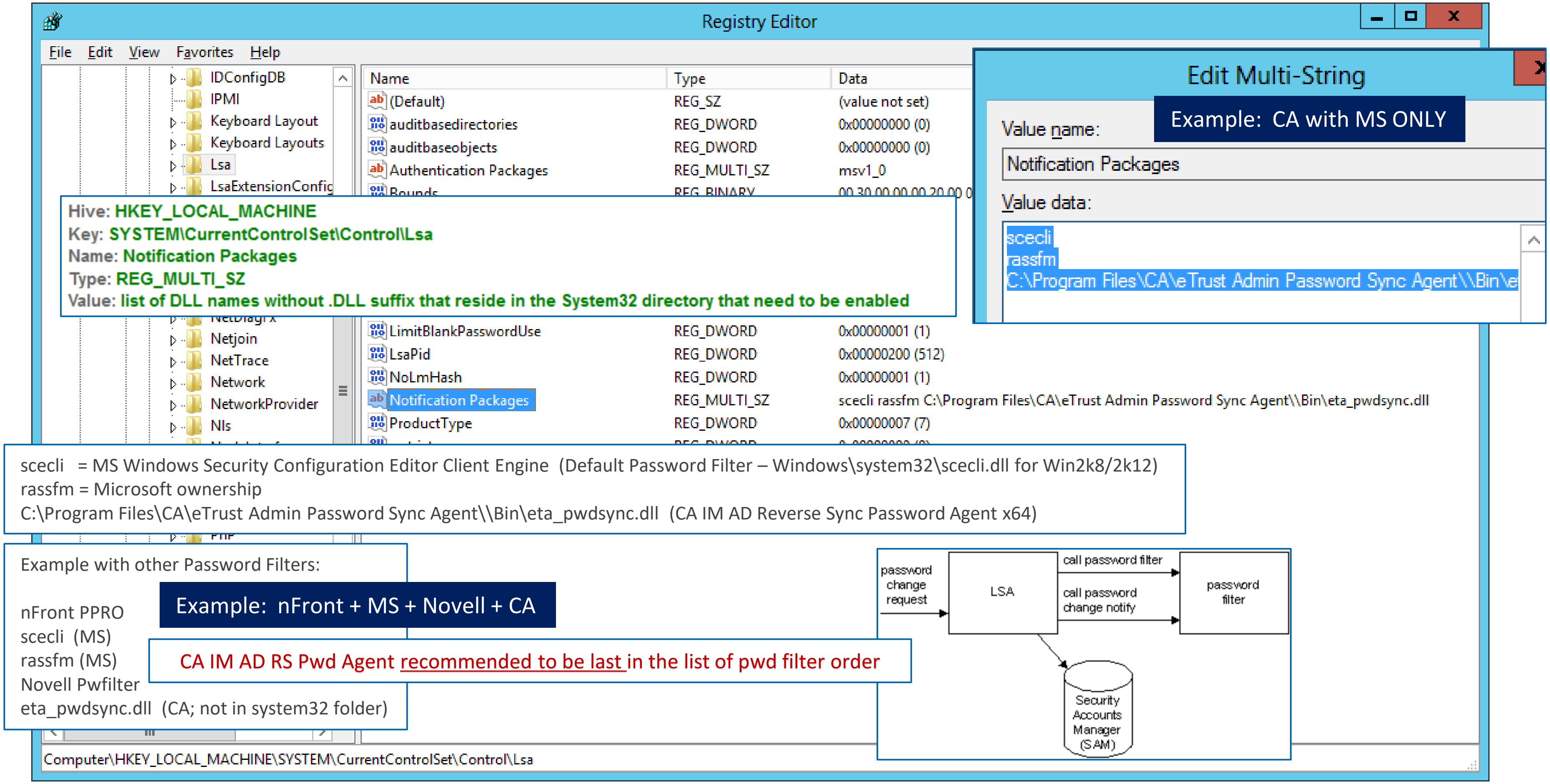
-If GU record does NOT exist, then no password sync will occur.
-GU records are created when a Provisioning Role is attached to the IM user account. This may be a NULL Provisioning Role with no Account Template.
-GU records require a password to be submitted when the GU account is created, if the password field is null, then the IMPS server will auto-generate a password.
-This password will be different from the IMCD account if the Provisioning Role was not attached at the create user use-case in IME (before the password is hashed)
-Password can be sync as a post action via a PX rule.
- The above challenges can be addressed by attaching a Provisioning Role with or without an Account Template to the create user use-case, to ensure the GU record is built and the userpassword is in sync.

"SLEDGEHAMMER APPROACH" - If the NOTIFY DSA does not clear; remove the offending entry or an admin may clear out the queue (with jxplorer or other tools)

On each Directory server (IMPD):
Step01: dxserver init all [sanity check to ensure no issues with any configuration file before starting, may also be used to auto-snapshot the DSA to an offline copy, if dump-dxgrid-db; was added to a setting file prior; if zdb file was created; create a LDIF extract with:
dxdumpdb -z -f {datestamp}_%COMPUTERNAME%-impd-notify.ldif %COMPUTERNAME%-impd-notify]
Step 02: dxserver stop IMPD_Notify_DSA_NAME
Step 03: dxemptydb IMPD_Notify_DSA_NAME
Step 04: dxserver start IMPD_Notify_DSA_NAME
Step 05: dxserver init all [sanity check]
On each Prov Server (IMPS): [This will recreate the OU entry in the Notify DSA for each DSA; if this OU does NOT exist, then IM Call Back will fail; impact on Reverse Sync]
Step 06: net stop im_ps
Step 07: net start im_ps
Step 08: Examine LDIF for the following: TRIGGER that caused the notify process, any entry that did not complete, & identify any user accounts where password did not sync. May identity the GU entry for the user's object to pull the eTPassword hash and populate the userPassword field with same hash if using CA Directory for userstore.

Customer may validate hash/encryptions with Jxplorer to Directory Solutions' ports

MS Password Filter DLL Section (CA IM AD RS Pwd Agent)



Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbasedirectories	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 0
LimitBlankPasswordUse	REG_DWORD	0x00000001 (1)
LsaPid	REG_DWORD	0x00000200 (512)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Packages	REG_MULTI_SZ	scecli rassfm C:\Program Files\CA\eTrust Admin Password Sync Agent\\Bin\eta_pwdsync.dll
ProductType	REG_DWORD	0x00000007 (7)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Edit Multi-String — Example: CA with MS ONLY

Value name: Notification Packages

Value data:

```
scecli
rassfm
C:\Program Files\CA\eTrust Admin Password Sync Agent\\Bin\e
```

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\Lsa
Name: Notification Packages
Type: REG_MULTI_SZ
Value: list of DLL names without .DLL suffix that reside in the System32 directory that need to be enabled

scecli = MS Windows Security Configuration Editor Client Engine (Default Password Filter – Windows\system32\scecli.dll for Win2k8/2k12)
rassfm = Microsoft ownership
C:\Program Files\CA\eTrust Admin Password Sync Agent\\Bin\eta_pwdsync.dll (CA IM AD Reverse Sync Password Agent x64)

Example with other Password Filters:

Example: nFront + MS + Novell + CA

nFront PPRO
scecli (MS)
rassfm (MS)
Novell Pwfilter
eta_pwdsync.dll (CA; not in system32 folder)

CA IM AD RS Pwd Agent recommended to be last in the list of pwd filter order

nFront Password Filter may not be installed on this DC.
Start + Run + winmsd. Expand Software Environment + Loaded Modules. Look for ppro.dll (or pprompe.dll or passfilt.dll). If ppro.dll is not found the DLL was not loaded by the operating system at boot. Perhaps the installation failed. Check the registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages to see if it shows an entry for PPRO (or PPROMPE or PASSFILT for older versions). If so the DLL failed to load on the last boot cycle. Verify the c:\winnt\system32 directory contains a pprompe.dll. Try rebooting the DC to see if it will load. If not, please call or email our technical support.

NOVELL- Password change is picked up at a domain controller and pwfilter.dll is notified. (This is done by the fact that pwfilter is running and is a notification package in HKLM/SYSTEM/CurrentControlSet/Control/Lsa)
- PWFILTER places the password change in a new registry key under HKLM/SOFTWARE/Novell/PwFilter/Data/<username> for that user example: Password change for BOB1 would be in HKLM/SOFTWARE/Novell/PwFilter/Data/BOB1.

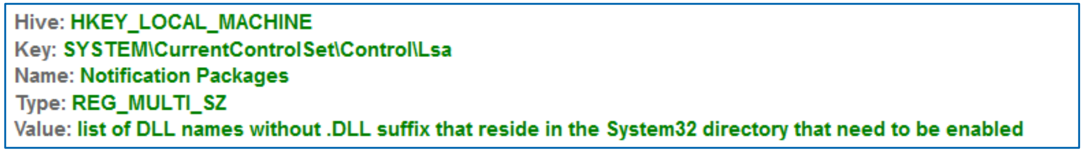
The **PasswordFilter** function is implemented by a *password filter* DLL. The value returned by this function determines whether the new password is accepted by the system. All of the password filters installed on a system must return **TRUE** for the password change to take effect.

TRUE	Return **TRUE** if the new password is valid with respect to the password policy implemented in the password filter DLL. When **TRUE** is returned, the *Local Security Authority* (LSA) continues to evaluate the password by calling any other password filters installed on the system.
FALSE	Return **FALSE** if the new password is not valid with respect to the password policy implemented in the password filter DLL. When **FALSE** is returned, the LSA returns the ERROR_ILL_FORMED_PASSWORD (1324) status code to the source of the password change request.

https://msdn.microsoft.com/en-us/library/windows/desktop/ms721882%28v=vs.85%29.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms721766%28v=vs.85%29.aspx
https://technet.microsoft.com/en-us/library/cc963221.aspx
https://msdn.microsoft.com/en-us/library/ms813420.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms721878%28v=vs.85%29.aspx
http://nfrontsecurity.com/downloads/nFront-Password-Filter-Documentation.pdf.
https://www.novell.com/support/kb/doc.php?id=3976631

Troubleshooting ADS Password Filter Logs:
nFront, Novell, Microsoft & CA

1. Check Order of Password Filter on DC (writable)
2. Execute Password Change on DC (ADUC)
3. View Logs



Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\Lsa
Name: Notification Packages
Type: REG_MULTI_SZ
Value: list of DLL names without .DLL suffix that reside in the System32 directory that need to be enabled

Order	Vendor	Filter Name	Log Location (Server – Path)	Log Names
1	nFront	ppro.dll	AD DC – c:\windows\system32\logfiles\	nFront-expired-pw.log nFront-expiring-soon.log
2	Microsoft	scecli.dll	AD DC – MS Event Service	MS Event Viewer
3	Microsoft	rassfm.dll	AD DC – MS Event Service	MS Event Viewer
4	Novell	pwfilter.dll	AD DC – MS Event Service	MS Event Viewer
5	CA	Eta_pwdsync.dll	AD DC - C:\Program Files\CA\Identity Manager\Provisioning Password Sync Agent for Windows\Logs\ [C:\Program Files\CA\eTrust Admin Password Sync Agent\Logs]	eta_pwdsync.log
6	CA	n/a	IMPS- IMPS_HOME\logs\	etatrans*.log + others
7	CA	n/a	IMPS – Notify – IMPS_HOME\logs\	etanotify*.log
8	CA	n/a	IMPS – CCS – IMPS_HOME\logs\	satrans*.log + others
9	CA	n/a	IAMCS – JCS – IAMCS_HOME\jcs\logs\	jcs_daily + \endpoint\endpoint.log
10	Endpoints	n/a	Endpoint / Userstores / Applications	*
11	CA	n/a	IMWA – IME VST (View Submitted Task)	n/a (database/audit/tp)

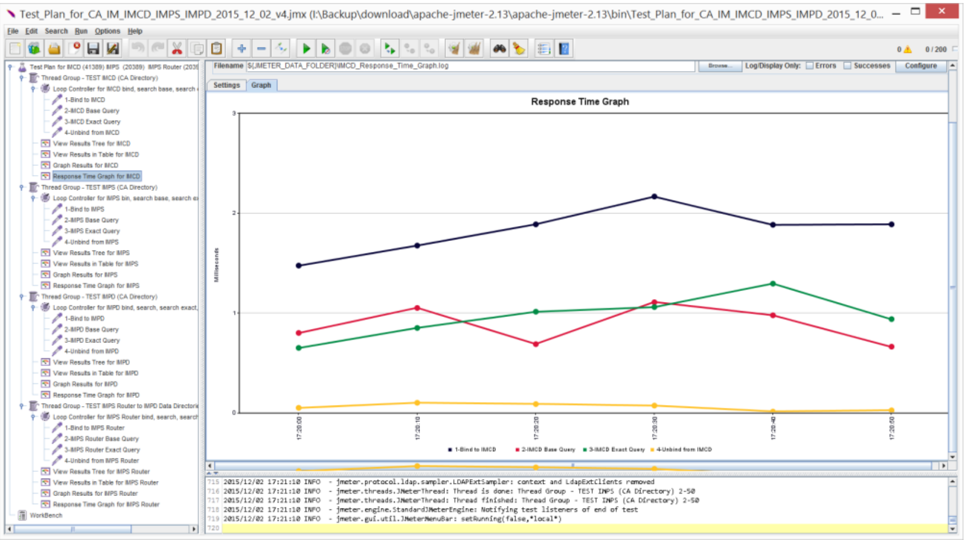
IM AD Password Reverse Sync Configuration File

[C:\Program Files\CA\Identity Manager\Provisioning Password Sync Agent for Windows\data\eta_pwdsync.conf]
[C:\Program Files\CA\eTrust Admin Password Sync Agent\data\eta_pwdsync.conf]

```
[Main]
out_of_sync=yes                  [Allow ADS User's password change to complete, even if EVERY IMPS server is down;  recommend leaving this value enabled]
pwd_sync_enable=yes              [yes/no values.     Deploy to all "writable" DCs with value = no , as a pre-step prior to any go-live; since DCs need to be rebooted to apply the password filter]
;; serialize-requests=no         [parallel or serial.    Leave with default of parallel; allow the DC to open as many connections as needed]
[Timeout]                                  [Default timeouts; leave as is, unless slow network impact password changes]
search_acct_dn=20
password_update_timeout=1
connection_request_timeout=20
password_quality_check_timeout=20
password_quality_check_connection_request_timeout=5
password_quality_check_search_acct_dn=10
[Logs]                                     [Ignore the Log Levels.    Keep Logging_enabled = yes,   ldap_logging_enabled = no  (unless there is a need to debug)]
logging_enabled=yes
ldap_logging_enabled=no
log_file=C:\Program Files\CA\Identity Manager\Provisioning Password Sync Agent for Windows\Logs\eta_pwdsync.log     [Older Path:  C:\Program Files\CA\eTrust Admin Password Sync Agent\Logs\eta_pwdsync.log]
[PasswordProfile]
profile_enabled=no                         [Default = yes;   Not required if using IME to validate password.   Has no impact if IMPS eTPasswordProfile is not enabled in IMPS]
profile_dn=eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=im
[EtaDomain]
etrust_suffix="dc=eta"
directory_dn=eTADSDirectoryName=adsserver-01.exchange.exc,eTNamespaceName=ActiveDirectory,dc=im,dc=eta
acct_attribute_name=eTADSsAMAccountName
domain=im
domain_suffix=dc=im
namespace=ActiveDirectory
directory=adsserver-01.exchange.exc
container_dn=eTADSAccountContainerName=Accounts,eTADSDirectoryName=adsserver-01.exchange.exc,eTNamespaceName=ActiveDirectory,dc=im
acct_object_class=eTADSAccount
[Server]                                   [Recommendation:  Use the Password Sync Agent Configuration Wizard (under the bin folder) to make changes to the below lines]
admin=idmadsync                            [Create a new IMPS GU "Admin" account, for SOD requirements; and add clarity to the IMPS logs which service ID changed what value]
admin_suffix=dc=im
servers=ldaps://IMPS-001:20390,ldaps://IMPS-002:20390     [Ensure multiple servers are available for failover]
machine_account=no
remote_server=no                           [Not required for on-prem installations; used for Cloud Minder (over TLS to exposed internet connection / MAN)]
host=IMPS-001,IMPS-002                     [Ensure multiple servers are available for failover]
password={3DES}hP+RqF2Nqkja5o6JGSe7Dw==                   [Use Password Sync Agent Configuration Wizard (under the bin folder) to change password 3DES hash]
```

Scalability Validation: Use Jmeter for testing Password Resets

1. Install Apache Jmeter & Jxplorer on the IMPS (Provisioning Server)
2. Use Jxplorer to connect to the IMPS 20389 and select the DN attribute of an "Explored" Endpoint Account (EA)
    a. This "pointer object" will ONLY be created after an initial Explore operation to the endpoint. When this object is select (via IMPS 20389), the IMPS services will query the CCS/JCS connector for the endpoint; and pull back or update the endpoint account.
3. Open Apache Jmeter & Create a Test Plan with two (2) sections
    a. SECTION ONE: Password Reset via IMPS & Connectors to managed endpoints
        a. Step 01: Bind to IMPS Service (IMPS Host + 20389/20390) with Admin Account (etaadmin/idmadmin)
        b. Step 02: Exact LDAP query : Query EA [Copy from Jxplorer]
            i. eTADSAccountName=BugsBunny,eTADSContainerName=Users,eTADSDirectoryName=TEST,eTNamespaceName=ActiveDirectory,dc=im,dc=eta
                a) Format: eTXXXAccountName where XXX = ADS, ACC, AS4, DB2, DBZ, ETC, FND, KRB, LND, N16, NIS, ORA, PLS, RAC, RSA, SAP Exceptions: EIAM and DYN (all CX connectors)
                b) Other exceptions: eTACFLid=BugsBunny,eTLIDContainerName= [alternative format: eTACFLid, eTTSSAcid, eTSBLUser, eTSQLLogin, eTPPSUser]
            ii. eTDYNAccount=BugsBunny,eTDYNContainerName= {all CX connectors}
        c. Step 03: Exact Account LDAP update: Update userPassword [Copy from Jxplorer]
        d. Step 04: Unbind from IMPS Service
    b. SECTION TWO: Password Reset directly to userstores
4. Ramp up testing from 1-50 users over 60 seconds.
5. Monitor Output
    a. Create four (4) reports


Test_Plan_for_CA_IM_IMCD_IMPS_IMPD_2015_12_02_v4.jmx (I:\Backup\download\apache-jmeter-2.13\apache-jmeter-2.13\bin\Test_Plan_for_CA_IM_IMCD_IMPS_IMPD_2015_12_0...
File Edit Search Run Options Help
0
0 / 200
Test Plan for IMCD (41389) IMPS (20389) IMPS Router (2039
Thread Group - TEST IMCD (CA Directory)
Loop Controller for IMCD bind, search base, search
1-Bind to IMCD
2-IMCD Base Query
3-IMCD Exact Query
4-Unbind from IMCD
View Results Tree for IMCD
View Results in Table for IMCD
Graph Results for IMCD
Response Time Graph for IMCD
Thread Group - TEST IMPS (CA Directory)
Loop Controller for IMPS bin, search base, search ex
1-Bind to IMPS
2-IMPS Base Query
3-IMPS Exact Query
4-Unbind from IMPS
View Results Tree for IMPS
View Results in Table for IMPS
Graph Results for IMPS
Response Time Graph for IMPS
Thread Group - TEST IMPD (CA Directory)
Loop Controller for IMPD bind, search, search exact,
1-Bind to IMPD
2-IMPD Base Query
3-IMPD Exact Query
4-Unbind from IMPD
View Results Tree for IMPD
View Results in Table for IMPD
Graph Results for IMPD
Response Time Graph for IMPD
Thread Group - TEST IMPS Router to IMPD Data Directorie
Loop Controller for IMPS Router bind, search, search
1-Bind to IMPS Router
2-IMPS Router Base Query
3-IMPS Router Exact Query
4-Unbind from IMPS Router
View Results Tree for IMPS Router
View Results in Table for IMPS Router
Graph Results for IMPS Router
Response Time Graph for IMPS Router
WorkBench
Browse...
Log/Display Only: □ Errors □ Successes
Configure
Settings
Graph
Response Time Graph
Milliseconds
3
2
1
0
17:20:00
17:20:10
17:20:20
17:20:30
17:20:40
17:20:50
■ 1-Bind to IMCD
■ 2-IMCD Base Query
■ 3-IMCD Exact Query
■ 4-Unbind from IMCD

Filename ${JMETER_DATA_FOLDER}\IMCD_Response_Time_Graph.log

```
715 2015/12/02 17:21:10 INFO  - jmeter.protocol.ldap.sampler.LDAPExtSampler: context and LdapExtClients removed
716 2015/12/02 17:21:10 INFO  - jmeter.threads.JMeterThread: Thread is done: Thread Group - TEST IMPS (CA Directory) 2-50
717 2015/12/02 17:21:10 INFO  - jmeter.threads.JMeterThread: Thread finished: Thread Group - TEST IMPS (CA Directory) 2-50
718 2015/12/02 17:21:10 INFO  - jmeter.engine.StandardJMeterEngine: Notifying test listeners of end of test
719 2015/12/02 17:21:10 INFO  - jmeter.gui.util.JMeterMenuBar: setRunning(false,"local")
720
```

May also use other tools, e.g. HP Load Runner, for same performance/ scalability validation

To view all endpoint objects Names/Classes without installing or using Jxplorer: **IMPS_HOME\bin\dumpptt.exe –f –of c:\temp\imps-dumppt.txt**