

Update the CA Identity Manager IMCD UserStore (with CA Directory) to use SSL/TLS & Integrate with SiteMinder Policy Server

Alan Baugher
CA Sr. Principal Architect
Dec 2015

Agenda

- Pre-steps
- Configuration
- Validation
- Troubleshooting Processes
- References

Pre-Steps: openssl cert check

CA SiteMinder uses SSLv3 protocol for non-FIPS communication & TLSv1.x for FIPS communication

- Ensure the IMCD userstore is configured for SSL/TLS communication prior to configuration in Siteminder.
- Use openssl to validate remote connection is available with a public CA root cert & SSLv3 protocol is available. IMCD_HOSTNAME=user store hostname
 - `openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -showcerts`
 - `openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -ssl3`
- Only the IMCD's CA Public Certificate is required for [IM:SM](#) integration for IMCD over SSL
 - Servers / Personalities Certificates are not required for standard userid/password authentication.
 - If authenticate is to be changed from standard userid/password to SSL client authentication; then copy ONLY the public section of the personalities PEM files to siteminder. Do not copy the personalities AS-IS.

Pre-Steps: CA Directory dxsearch check

LDAP tools; including CA Directory search tool (dxsearch), requires the CN of a server SSL certificate to MATCH the hostname.

1. Update the local host file entry with a host alias that matches the DSA name. This is a temporary test; and the host alias does **NOT** need to be retained for SiteMinder.
2. CA Directory CLI commands use the DXHOME/config/ssld/dxldap.conf file for pathing to its keystore. Ensure this file is pointing to trusted.pem or other file used by IMCD DSA, to ensure the CA Public Cert is available to validate SSL communication.

```
dsa@sandbox01 personalities]$ pwd
/opt/CA/Directory/dxserver/config/ssld/personalities
[dsa@sandbox01 personalities]$ cat sandbox01-imcd.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=AU, O=DXCertGenPKI, CN=DXCertGenCA
        Validity
            Not Before: Oct  3 03:53:55 2015 GMT
            Not After : Sep 30 03:53:55 2025 GMT
        Subject: O=ca, CN=sandbox01-imcd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
```

```
root@sandbox01:/opt/CA/media/steps
#192.168.92.129 sandbox01.lab.dom sandbox01 sandbox02
192.168.92.129 sandbox01.lab.dom sandbox01 sandbox02 sandbox01-imcd
"/etc/hosts" 4L, 286C
```

NON-SSL QUERY:

```
dxsearch -L -H ldaps://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca' 'uid=diradmin' sn uid"
```

SSL QUERY

```
dxsearch -Z -L -H ldaps://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca' 'uid=diradmin' sn uid"
```

Note: Only -H ldaps is required, but the -Z switch ensure a viewable message that SSL is enabled and used. Ignore ERROR MESSAGE: ldap_start_tls: Operations error (1)

```
[dsa@sandbox01 ~:/logs]$ tail -f sandbox01-imcd warn 20151212.log
[3] 20151212.180957.446 WARN : TLS/SSL handshake failed for call from 192.168.92.129:29439
[6] 20151212.181027.459 WARN : ERROR IN HANDSHAKE
[6] 20151212.181027.459 WARN : 7fd9480a5738- 80370103 01001e00 00001000 000400fe .7.....
[6] 20151212.181027.459 WARN : 7fd9480a5748- ff00000a 00fefe00 00090000 64000062 .....d..b
[6] 20151212.181027.459 WARN : 7fd9480a5758- 00000300 00060000 ff8a9e86 3e3f5b3e .....>? [>
[6] 20151212.181027.459 WARN : 7fd9480a5768- 3339c996 0ff729be 09 39....).
[6] 20151212.181027.459 WARN : 6:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number:s3_pkt.c:372:
```

Monitor the WARN log of the IMCD DSA. If SSLv3 protocol or the hostname does NOT match the CN of the certificate

```
ldap_start_tls: Can't contact LDAP server (-1)
# additional info: TLS: hostname does not match CN in peer certificate
```

Revised Steps to Create SM NSS cert8.db files with IMCD Public CA Cert

Step 1. Validate that IMCD is available to be access over SSL. (Presteps)

- Use either openssl, dxsearch, Jxplorer, Apache Directory Studio, SoftTerra LDAPBrowser, etc.

Step 2: Copy the IMCD's CA Public Certificate from the CA Directory Server to the CA SiteMinder Policy Server

- May use **openssl s_client -connect hostname:port -showcerts** & copy the 2nd cert from BEGIN to END markers
- Or copy the trusted.pem file from DXHOME/config/ssld/trusted.pem {validate this file is reference in the DXI file for IMCD for SSL via default.dxc or custom DSANAME.dxc}

Step 3: Update or check DXHOME/config/ssld/default.dxc {or custom DSANAME.dxc} [Assumes CA Directory is used]

- Ensure this file allows for SSLv3 protocol to be used for SiteMinder with the update of: protocol=ssl
- Validate with **openssl s_client -connect hostname:port -ssl3**

Step 4: Create the NSS Certificate Keystore files to be used by SiteMinder

- Make a new folder under siteminder, e.g. /opt/CA/siteminder/ldap_tls (or certs, etc.)
- Under that folder issue the following command, as smuser: **certutil -N -d /opt/CA/siteminder/ldap_tls**
- Enter a password twice

Step 5: Add the IMCD's CA Public Certificate to the NSS keystore

- Execute: **certutil -A -n "IMCD_TRUSTED_CA_PUBLIC_CERT" -t "C,," -i trusted.pem -d /opt/CA/siteminder/ldap_tls**

Step 6: Validate the IMCD's CA Public Certificate is loaded fine in the NSS keystore

- Execute: **certutil -L -d /opt/CA/siteminder/ldap_tls** or **certutil -L -a -n IMCD_TRUSTED_CA_PUBLIC_CERT -d /opt/CA/siteminder/ldap_tls**

Step 7: Update SiteMinder to use the new NSS keystore file of cert8.db

- Use either SMCONSOLE GUI & Update Data Tab for Netscape Certificate Database File Entry
- Alternative: Use SM CLI XPSConfig, select SM, and # for LdapObjCertDbPath OR directly edit/sed of the sm.registry file for CertDbPath under HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore

Step 8: Bounce SiteMinder for the smpolicy service: stop-ps & start-ps

Step9: Validate SiteMinder is able to communicate with IMCD userstore over Secure Connection (SSL)

- Open SM User Interface of SMWAMUI or SMFSSUI and select the user store & update the connection to use Secure Connection; ensure that Contents are returned.
- Open CA Directory IMCD warn log; and monitor for any failed SSL connections.

Step 10: Done. Will be able to update the CA Identity Manager IMCD entry from non-SSL to SSL communications.

- Perform similar steps for the **IME's IMPS/IMPD** using the impd_trusted.pem as the IMPD's CA Public Certificate to be added to the NSS keystore.
- IMPS service uses the same CA Public Cert as IMPD. This CA Public cert may be changed via the IMPS\data\tls folder & batch processes.

Revised Steps used in a shell script

```
bash-4.2$ cat step001_~smuser_~create_ssl_certs_db.sh
#!/bin/bash
#####
# Add IMCD SSL CERT to SiteMinder to enable TLS
# Only need CA Public Cert
# No need to copy the Server Certs (personalities)
# SM will use userid/password for authentication
#####
IMCD_HOSTNAME=sandbox01
IMCD_PORT=41389
SMHOME=/opt/CA/siteminder
LDAP_TLS=$SMHOME/ldap_tls
DXHOME=/opt/CA/Directory/dxserver/config/ssld
PATH=$SMHOME/bin:$PATH
PASSWORD=Password01
USER=smuser
GROUP=smuser

echo ""
echo "# Step00: Clean up Prior NSS DB files under $LDAP_TLS"
mkdir -p $LDAP_TLS
cd $LDAP_TLS
rm -rf *.db
rm -rf trusted-root-ca-public-for-imcd.*
# Note: pem format may includes cer (public format) + ascii + optional (private key)

echo ""
echo "# Step01: Check if the CA Public Cert exists AND that SSLv3 protocol is available"
echo "# Siteminder uses SSLv3 protocol for non-FIPS encryption & TLS for FIPS encryption"
echo ""
echo "# The CA Public Cert should display as the 2nd cert in this list with -showcerts"
echo "openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -showcerts"
echo "# The communication will report failure, if SSLv3 protocol is not enabled."
echo "openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -ssl3"
echo "# Run the above lines as a prestep, they are commented out to avoid impacting readability of the other lines"
echo "#openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -showcerts"
echo "#openssl s_client -connect $IMCD_HOSTNAME:$IMCD_PORT -ssl3"
echo ""

echo ""
echo "# Step02: Copy IMCD CA Public Cert Only [Not DSA Server Certs (Personalities)]"
echo "# Ensure that the user of this script has access to the CA Directory SSLD folder"
cd $LDAP_TLS
echo "cp -r -p $DXHOME/trusted.pem $LDAP_TLS/trusted.pem"
cp -r -p $DXHOME/trusted.pem $LDAP_TLS/trusted.pem
echo "# Strip any extra commentary from CA Directory PEM Format. Keep BEGIN CERTIFICATE / END CERTIFICATE markers"
echo ""
echo "openssl x509 -outform der -in trusted.pem -out trusted-root-ca-public-for-imcd.der"
openssl x509 -outform der -in trusted.pem -out trusted-root-ca-public-for-imcd.der
echo "# Strip any extra commentary from CA Directory PEM Format. Keep BEING / END"
echo "openssl x509 -inform der -in trusted-root-ca-public-for-imcd.der -out trusted-root-ca-public-for-imcd.cer"
openssl x509 -inform der -in trusted-root-ca-public-for-imcd.der -out trusted-root-ca-public-for-imcd.cer

echo ""
echo "# Step03: Create a NSS keystore for Siteminder with CertUtil (cert8.db, key3.db, secmod.db)"
echo "# NSS = Netscape Network Security Services & ensure SM version of certutil is being used in the path"
echo ""
echo "( echo $PASSWORD ) > $LDAP_TLS/pwdfilename.txt"
( echo $PASSWORD ) > $LDAP_TLS/pwdfilename.txt
echo "( echo \"$PASSWORD\"; echo \"$PASSWORD\" ) | $SMHOME/bin/certutil -N -d $LDAP_TLS -f $LDAP_TLS/pwdfilename.txt"
( echo \"$PASSWORD\"; echo \"$PASSWORD\" ) | $SMHOME/bin/certutil -N -d $LDAP_TLS -f $LDAP_TLS/pwdfilename.txt
```

```
echo ""
echo "# Step04: Store the IMCD ROOT CA Certificate from CA Directory 'clean version' of IMCD trusted-root-ca-public-for-imcd.pem"
echo "$SMHOME/bin/certutil -A -n "IMCD_TRUSTED_CA_PUBLIC_CERT" -t "C,," -i $LDAP_TLS/trusted-root-ca-public-for-imcd.cer -d $LDAP_TLS"
$SMHOME/bin/certutil -A -n "IMCD_TRUSTED_CA_PUBLIC_CERT" -t "C,," -i $LDAP_TLS/trusted-root-ca-public-for-imcd.cer -d $LDAP_TLS

echo ""
echo "# Step05: Store IMCD DSA Server Public Cert from IMCD personalities IMCD_DSA_HOSTNAME.pem"
echo "$SMHOME/bin/certutil -A -n "IMCD_DSA_HOSTNAME_PUBLIC_CERT" -t "P,," -i $LDAP_TLS/$IMCD_HOSTNAME-imcd-public.cer -d $LDAP_TLS"
echo "### Confirmed this step from bookshelf is NOT required for standard userid/password authentication over SSL/TLS"
echo "### Confirmed this step from bookshelf is NOT required for standard userid/password authentication over SSL/TLS"
echo "### Confirmed this step from bookshelf is NOT required for standard userid/password authentication over SSL/TLS"
echo ""

echo ""
echo "# Step06: List all CA and Server Public Certs in NLS Keystore"
echo "$SMHOME/bin/certutil -L -d $LDAP_TLS"
$SMHOME/bin/certutil -L -d $LDAP_TLS

echo ""
echo "# Step06b: Update ownership of the DB files of $LDAP_TLS/cert8.db"
chown -R $USER:$GROUP $LDAP_TLS
chmod -R 640 $LDAP_TLS/*.db

echo ""
echo "# Step07: Use XPSConfig to update the SM:LdapObjCertDbPath to $LDAP_TLS/cert8.db"
echo "# su - smuser ; XPSConfig ; Select SM ; Select # for LdapObjCertDbPath Likely #83"
echo ""
echo "# Alternatives: Use SMCONSOLE on the Data Tab for Netscape certificate file or"
echo "# edit the SMHOME/registry/smregistry.xml file & update CertDbPath under "
echo "# HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore"
echo ""

echo ""
echo "# Step08: Start / Stop SM Policy Server"
echo "# Shown below for manual step AFTER the above update is done"
echo "$SMHOME/stop-ps"
echo "$SMHOME/start-ps"

echo ""
echo "#####"
echo ""
echo "# Validate NON-SSL/TLS to directory"
echo "# if running this script as root, it will have access to run dxsearch as dsa"
echo "# if running this script as smuser, you will need to type the password for dsa account"
echo ""
echo "dxsearch -Z -L -H ldap://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca' 'uid=diradmin' 'sn uid'"
echo "ou=cam,o=ca" 'uid=diradmin' 'sn uid'"
echo ""
su - dsa -c "dxsearch -L -H ldap://sandbox01:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w $PASSWORD -b 'ou=cam,o=ca' 'uid=diradmin' 'sn uid'"
```

```
echo ""
echo "# Validate SSL/TLS to directory"
echo "# Update /etc/hosts to have alias where DSA_NAME = HOSTNAME"
echo "# Example: 192.168.92.129 sandbox01 sandbox01.im.dom sandbox01-imcd"
echo "# Note: CA Directory CLI commands use DXHOME\config\ssld\dxldap.conf file"
echo ""
echo "# if running this script as root, it will have access to run dxsearch as dsa"
echo "# if running this script as smuser, you will need to type the password for dsa account"
echo ""
echo "dxsearch -Z -L -H ldaps://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca' 'uid=diradmin' 'sn uid'"
echo ""
#su - dsa -c "dxsearch -d 1 -Z -L -H ldaps://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca' 'uid=diradmin' 'sn uid'"
su - dsa -c "dxsearch -Z -L -H ldaps://sandbox01-imcd:41389 -c -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w $PASSWORD -b 'ou=cam,o=ca' 'uid=diradmin' 'sn uid'"

# Ignore ERROR MESSAGE: ldap_start_tls: Operations error (1)
# This message occurs when using both the -Z switch & -H ldaps://hostname:port URI
# This script uses both to confirm that SSL/TLS is being used; and can be seen visually without the need of debug switches.

# Note: If error returned is:

#dxsearch -Z -H ldaps://sandbox01:41389 -c -x -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca'
#ldap_start_tls: Can't contact LDAP server (-1)
# additional info: TLS: hostname does not match CN in peer certificate

# Add the DSA_HOSTNAME as an alias to the local host file to ensure the CN matches the HOSTNAME=DSA_NAME
#dxsearch -Z -H ldaps://sandbox01-imcd:41389 -c -x -D 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca' -w Password01 -b 'ou=cam,o=ca'

echo ""
echo "# View certs in cert8.db file for CA PUBLIC CERT"
echo ""
echo "$SMHOME/bin/certutil -L -a -n IMCD_TRUSTED_CA_PUBLIC_CERT -d $LDAP_TLS"
echo ""
$SMHOME/bin/certutil -L -a -n IMCD_TRUSTED_CA_PUBLIC_CERT -d $LDAP_TLS
echo ""

# As a test to ensure the CA cert was added correctly
$SMHOME/bin/certutil -L -a -n IMCD_TRUSTED_CA_PUBLIC_CERT -d $LDAP_TLS > test_ca.cer
echo ""
# diff test_ca.cer trusted-root-ca-public-for-imcd.cer
```



H:\

smuser_~create_ssl

Option 1: Update SM Policy Server to use certificate database via smconsole GUI; Data Tab; Netscape Certificate Database File Checkbox

The screenshot shows the 'Policy Server Management Console' window with the 'Data' tab selected. The 'Database' is set to 'Policy Store' and 'Storage' is set to 'LDAP'. Under the 'LDAP Policy Store' section, the 'LDAP IP Address' is 'localhost:22389', 'Root DN' is 'o=smps', 'Admin Username' is 'cn=diradmin,c', and 'Password' and 'Confirm Password' are masked. There is a 'Test LDAP Connection' button. At the bottom, the 'Netscape Certificate Database File' is set to '/opt/CA/siteminder/ldap_tls/cert8.db' with a 'Browse ...' button.

The image shows two configuration windows. The 'Additional parameters' window for Xming has the 'No Access Control' checkbox checked, which is highlighted with a red box. The 'PuTTY Configuration' window has the 'X11 forwarding' checkbox checked, also highlighted with a red box.

For remote use of the SM smconsole GUI

1. Download & use open Source Xming on workstation & No Access Control is checked.
2. Ensure smuser has DISPLAY variable populated with workstation's IP address
DISPLAY=192.168.92.1:0.0
3. Ensure putty profile for connection uses X11 Forwarding Feature (checked)

Option 2: Update SM Policy Server to use certificate database via use SM CLI Process: /opt/CA/siteminder/XPSConfig

```
$ XPSConfig
[XPSConfig - XPS Version 12.52.0001.154]
Log output: XPSConfig.2015-12-13_070918.log
```

```
PRODUCTS MENU*****CA
```

```
CDS - CertificateDataStore      12 Parameters
EPM - Enterprise Policy Management 3 Parameters
FED - Federation                3 Parameters
SM - SiteMinder                 162 Parameters
XPS - Extensible Policy Store    25 Parameters
```

```
-----
X - xTrace
```

```
-----
Q - Quit
```

```
-----
Enter Option (id or X or Q):SM
```

```
Enter Option (D, V, F, # or Q): 83
```

```
PARAMETER MENU*****CA.SM::$LdapObjCertDbPath
```

```
Name:      LdapObjCertDbPath [CA.SM::$LdapObjCertDbPath]
Type:      String
Scope:     Managed
Export?    yes
Report?    no
Remote Access:  None
Description:  The certificate used by the LDAP stores' SSL connections.
License Type:  None
Default Value: (not set)
```

```
Current Value:  "/opt/CA/siteminder/ldap_tls/cert8.db"
```

```
-----
C - Change value
Q - Quit
```

```
-----
Enter Option (C, or Q):C
```

```
Enter Option (id or X or Q): SM
```

```
PARAMETERS MENU*****CA.SM
```

```
1-AccTcpPort      Type: Numeric Scope: Managed
                  Desc: The TCP port used by the SiteMinder Policy Server's Accounting service.
                  Current Value:"0"
```

```
<REMOVED SECTION FOR CLARITY>
```

```
83-LdapObjCertDbPath      Type: String Scope: Managed
                          Desc: The certificate used by the LDAP stores' SSL connections.
                          Current Value:"/opt/CA/siteminder/ldap_tls/cert8.db"
```

```
<REMOVED SECTION FOR CLARITY>
```

```
162-WorkerThreadPriorityRatio      Type: Numeric Scope: Managed
                                   Desc: The worker thread priority ratio, from -100 to 100.
                                   Current Value:"0"
```

```
-----
D - Hide Descriptions
V - Hide Values
F - Filter (currently none)
Q - Quit
```

```
-----
Enter Option (D, V, F, # or Q):83
```


Option 3: Update SM Policy Server to use certificate database via directly update SMHOME/registry/sm.registry file

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore=857188358

AdminDN= cn=diradmin,ou=serviceaccount,ou=SiteMinder,ou=Netegrity,o=smps; REG_SZ

AdminPW= {RC2}BZJN06X8IKUFFuAMKQCyhOmBXACyAmIS; REG_SZ

AppSdk= 0; REG_DWORD

CertDbPath= /opt/CA/siteminder/ldap_tls/cert8.db; REG_SZ

Enabled= 0x1; REG_DWORD

PSRootDN= o=smps; REG_SZ

Server= localhost:22389; REG_SZ

Use SSL= 0; REG_DWORD

Version= 5.0; REG_SZ

Option 4: Update SM Policy Server to use certificate database via Unix/Linux sed command to update SMHOME/registry/sm.registry file

Update the string that manages the connection path to the NSS cert8.db file

FROM:

CertDbPath= ; REG_SZ

TO:

CertDbPath= /opt/CA/siteminder/ldap_tls/cert8.db; REG_SZ

grep "^CertDbPath= " sm.registry [Check search criteria for sed. Eleven spaces?]

grep '^CertDbPath=.*REG_SZ\$' sm.registry

grep '^CertDbPath=.*.;.*REG_SZ\$' sm.registry [If entry is not populated, this will display the line; assumes a space prior to ;]

```
sed -i 's|^CertDbPath=.*.;.*REG_SZ$|CertDbPath= /opt/CA/siteminder/ldap_tls/cert8.db; REG_SZ|g' sm.registry
```

Note: The path of the cert8.db file has no space that separates the semi-colon (;) from the file name.
& number of spaces has no impact prior to path.

A view of IMCD's CA Public Certificate (SMPS certutil versus DSA trusted.pem)

IMCD CA Public Cert pulled via certutil from cert8.db file

Note: Only the BEGIN CERTIFICATE / END CERTIFICATE section is retained/stored.

```
bash-4.2$ pwd
/opt/CA/siteminder/ldap_tls
bash-4.2$ certutil -L -a -n IMCD_TRUSTED_CA_PUBLIC_CERT -d .
-----BEGIN CERTIFICATE-----
MIIDEjCCAfqgAwIBAgIBATANBgkqhkiG9w0BAQUFADA6MQswCQYDVQQGEwJBVTEV
MBMGA1UECgwMRfhdZXJ0R2VuUETJMRQwEgYDVQQDDAtEWENlcnRHZW5DQTAeFw0x
NTEwMDMwMzUzNTRaFw0yNTA5MzAwMzUzNTRaMDoxCzAJBgNVBAYTAkFVMRUwEwYD
VQKDAxEWENlcnRHZW5QS0kxFDASBgNVBAMMC0RYQ2VydEdlbkNBMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhdcYA8HaiAg7GWZ5aapLzF8Zsp8HkPbO
pA+NEQEzu+YhquhQwXR9lqhHYSOY01P/na3C7+U0VAve0x2+Qm1gRgnc62xvCL8H
XW8q2q8wOnGYW6wFEuDQV2sk847jmPf5zN3SAelixqjn9pUxNBTKjfxClSa0R3Kc
DHcvV5MAwniP639HPjwy8Wx08H3pEGPvOmCNqDACj1l1rAiKcfJHJVUaC6RBV/oF
FQ4cAjMRVOF9tGPpOwe0/gS0Y4idojvnq+I5lAhjDpX0MBISNQ2J4TEv103iviL+
zi3QTZ4ETLc87CS08KDjJrbFo3gACDHj0CB29TeOaeDoFd8eoB0BewIDAQABoyMw
ITAObgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUF
AAOCAQEAVld+SREdFlBGjzY0EKZgYM20CbzMLvOb6VYYido+MI3Bt10/+P0jyueX
Zf420a0y2iO5kJ65XgXjYArfyD/48jeB9VbRs4xdSXfvq6yU4JCeHX3zsHet4fNT
zylBYvM9reD/R9QXZuZuGheAFH3u2ThrGlpCxaSa02/6lj6BC9eAdh3HoV5xtyaSH
uxinhbY7tdGe8iwj3ggW02BbFa/fejLICHfRlJl3wbMAOk9IMjIB7LL7S21g/Bz2
Tkwnm5c+w9P1pt8H7IEiALekk6aqtDWKuR7Qb+W699NJqHhHJZ9n78NLYYx1Ly7
E5/Y3Pbn/talVpUdXGOAcHeVBX/eYw==
-----END CERTIFICATE-----
bash-4.2$
```

IMCD CA Public Cert from DXHOME/ssld/trusted.pem

The PEM file contains the ASCII text header, as well as the BEGIN CERTIFICATE / END CERTIFICATE section.

```
-----BEGIN CERTIFICATE-----
MIIDEjCCAfqgAwIBAgIBATANBgkqhkiG9w0BAQUFADA6MQswCQYDVQQGEwJBVTEV
MBMGA1UECgwMRfhdZXJ0R2VuUETJMRQwEgYDVQQDDAtEWENlcnRHZW5DQTAeFw0x
NTEwMDMwMzUzNTRaFw0yNTA5MzAwMzUzNTRaMDoxCzAJBgNVBAYTAkFVMRUwEwYD
VQKDAxEWENlcnRHZW5QS0kxFDASBgNVBAMMC0RYQ2VydEdlbkNBMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhdcYA8HaiAg7GWZ5aapLzF8Zsp8HkPbO
pA+NEQEzu+YhquhQwXR9lqhHYSOY01P/na3C7+U0VAve0x2+Qm1gRgnc62xvCL8H
XW8q2q8wOnGYW6wFEuDQV2sk847jmPf5zN3SAelixqjn9pUxNBTKjfxClSa0R3Kc
DHcvV5MAwniP639HPjwy8Wx08H3pEGPvOmCNqDACj1l1rAiKcfJHJVUaC6RBV/oF
FQ4cAjMRVOF9tGPpOwe0/gS0Y4idojvnq+I5lAhjDpX0MBISNQ2J4TEv103iviL+
zi3QTZ4ETLc87CS08KDjJrbFo3gACDHj0CB29TeOaeDoFd8eoB0BewIDAQABoyMw
ITAObgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUF
AAOCAQEAVld+SREdFlBGjzY0EKZgYM20CbzMLvOb6VYYido+MI3Bt10/+P0jyueX
Zf420a0y2iO5kJ65XgXjYArfyD/48jeB9VbRs4xdSXfvq6yU4JCeHX3zsHet4fNT
zylBYvM9reD/R9QXZuZuGheAFH3u2ThrGlpCxaSa02/6lj6BC9eAdh3HoV5xtyaSH
uxinhbY7tdGe8iwj3ggW02BbFa/fejLICHfRlJl3wbMAOk9IMjIB7LL7S21g/Bz2
Tkwnm5c+w9P1pt8H7IEiALekk6aqtDWKuR7Qb+W699NJqHhHJZ9n78NLYYx1Ly7
E5/Y3Pbn/talVpUdXGOAcHeVBX/eYw==
-----END CERTIFICATE-----
[dsa@sandbox01 ssl]$ pwd
/opt/CA/Directory/dxserver/config/ssl
[dsa@sandbox01 ssl]$ cat trusted.pem
```


A view of the CA IMCD DSA Use of SSLv3 Protocol & SM able to communicate to IMCD

The image displays a SiteMinder ESS Administrative UI interface and two terminal windows. The UI shows the 'User Directory Properties' dialog with 'CAM Unified User (UU)' selected, and the 'SiteMinder Directory List Dialog' listing members. The terminal windows show the configuration of the CA Directory - DXserver/config/ssld file, including SSL options and HSM settings.

SiteMinder ESS Administrative UI

SiteMinder User Directory Dialog

User Directory Properties

Name: CAM Unified User (UU)

Directory Setup: ☒ Require Credentials

Run in Authenticated User's Security Context: ☐ Run in Authenticated User's Security Context

Secure Connection: ☒ Secure Connection

SiteMinder Directory List Dialog

Listing all members.

Name	User Class
ou=cam,o=ca	organizationalUnit
ou=people,ou=cam,o=ca	organizationalUnit
ou=serviceaccount,ou=cam,o=ca	organizationalUnit

1.3 of 3

OK Cancel Apply

Terminal 1 (Left):

```
CA Directory - DXserver/config/ssld
# This is a read-only default configuration file. If you need to make changes,
# copy this file and reference the new file from servers/<dsa>.dxi
#
# default CA Directory ssl configuration
# - 'dxcertgen certs' can be used to create a basic set of certificates

set ssl = {
  # folder containing DSA personality certs
  cert-dir = "config/ssld/personalities"

  # trusted root CA that signed DSA certificates
  ca-file = "config/ssld/trusted.pem"

  # SSL options
  cipher = "ALL:!EXPORT40:!ADH:!SSLv2:!EXP:!LOW" # default ciphers - syntax on OpenSSL website

  protocol=ssl
  # protocol = tls
  # fips = true

  # HSM options
  # pin = "<str>"
  # lib = "<str>"
  # slot = <num>
};

"default.dxc" [readonly] 28L, 989C
```

Terminal 2 (Right):

```
CA Directory - DXserver/config/ssld
# This is a read-only default configuration file. If you need to make changes,
# copy this file and reference the new file from servers/<dsa>.dxi
#
# default CA Directory ssl configuration
# - 'dxcertgen certs' can be used to create a basic set of certificates

set ssl = {
  # folder containing DSA personality certs
  cert-dir = "config/ssld/personalities"

  # trusted root CA that signed DSA certificates
  ca-file = "config/ssld/trusted.pem"

  # SSL options
  cipher = "ALL:!EXPORT40:!ADH:!SSLv2:!EXP:!LOW" # default ciphers - syntax on OpenSSL website

  protocol=ssl
  # protocol = tls
  # fips = true

  # HSM options
  # pin = "<str>"
  # lib = "<str>"
  # slot = <num>
};

"default.dxc" [readonly] 28L, 989C
```

Policy Server Management Console

File Help

Status Settings Data Super User Keys Logs **Profiler** Advanced

Configuration Settings

☒ Enable Profiling

Configuration File:
/opt/CA/siteminder/config/smtracedefault.txt

Output

☐ Output to Console

☒ Output to File:
/opt/CA/siteminder/log/smtracedefault.log

Trace Logfile Rollover:

☒ When the server is restarted

☒ When Trace logfile reaches: 10 MB

☐ Time Based

☐ Hourly Every 1 Hours (Start time taken from 0:00 (12:00AM))

☐ Every 0 Days At (24 hour clock)

Retain up to: 10 old Trace Logfile(s)

Select output format:

☐ SiteMinder Default[] (Required by Customer Support) ☐ Fixed Width Fields

☐ XML Tags ☐ Field Delimiter:

OK Cancel Apply

If there is a need to trace communication or view details on the error message from SiteMinder, enable the LDAP component for the SM "profiler", then monitor the SMHOME/log/smtracedefault.log

Troubleshoot Processes: SM Trace Log for LDAP

Policy Server Profiler - eTrust SiteMinder by CA

File

Components Data Filters

Available Components

- AgentFunc
- Server
- Login_Logout
- Directory_Access
- ODBC
- IdentityMinder
- TXM
- Fed_Server
- DLP

Selected Components

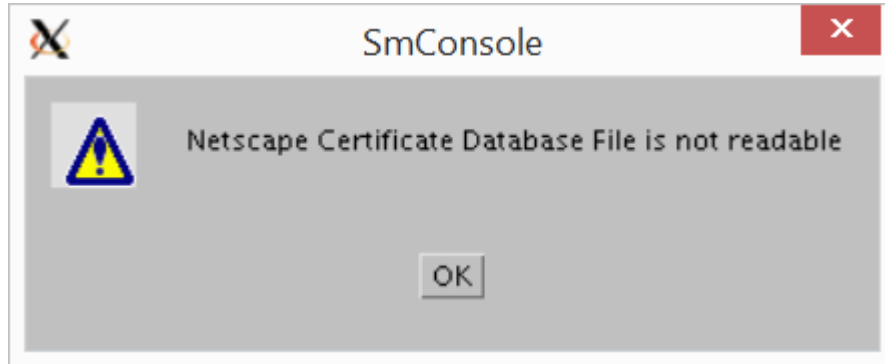
- Send_Response
- Receive_Request
- IsAuthorized
- Tunnel_Service
- JavaAPI
- ODBC
 - Sql_Statement_Begin_End
 - Connection_Management
 - Sql_Errors
 - Connection_Monitor
- LDAP**
 - Ldap_Call_Begin_End
 - Internal_Operation
 - Connection_Management
 - Performance_Measurement
 - Ldap_Error_Messages

Template:

OK Cancel Apply

Profiler Configuration File "/opt/CA/siteminder/config/smtracedefault.txt"

Troubleshoot Processes: Ensure File Permission & Ownership for Certs db files are correct for smuser



```
chmod -R 644 *.db  
chown -R smuser:smuser *.db
```

```
-rw-----. 1 644 smuser 16384 Dec 11 18:29 secmod.db  
drwxrwxr-x. 2 smuser smuser 4096 Dec 11 18:29 .  
-rw-----. 1 644 smuser 16384 Dec 11 18:29 key3.db  
-rw-----. 1 644 smuser 65536 Dec 11 18:29 cert8.db  
drwxr-xr-x. 31 smuser smuser 4096 Dec 12 16:02 ..  
[root@sandbox01 ldap_tls]# chown -R smuser:smuser *.db
```

References

NSS Info (Netscape Network Security Services)

<http://firstyear.id.au/entry/15>

https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil

Various SSL/TLS Certificate File Types/Extensions (pem,der,cer)

<http://blogs.msdn.com/b/kaushal/archive/2010/11/05/ssl-certificates.aspx>

CA SM Documentation (LDAP over SSL with NSS cert8.db)

<https://docops.ca.com/ca-single-sign-on-1251sp1/en/administrating/configuring-policy-server-data-storage-options/how-to-configure-ssl-support>

<https://docops.ca.com/ca-siteminder-federation-standalone/en/configuring/user-directory-connections-for-authentication/how-to-connect-to-an-ldap-user-directory-over-ssl>

CA SM Tech Tips

<https://ca-tech.jiveon.com/thread/241734151>

CA Directory r12sp14 Note about SSLv3 versus TLS (default settings)

<https://communities.ca.com/thread/241739401>