

Generate SSL Cert “Server Auth” for ADS Domain Controller with MS Cert Authority Solution

With Open SSL from CA IMPS\bin folder or new install of openssl
& MS Cert tools certreq.exe & certlm.msc

Ref: <https://support.microsoft.com/en-us/kb/321051>

Alan Baugher, CA Sr. Principal Architect
Aug 2016

Method 01: Generate a root CA key and a Server Auth Key for ADS DC

GOAL: Create a SSL Server auth cert for MS Active Directory to avoid installing MS CA Enterprise Auth for LAB & use TCP 636 for CA IM

On the CA IMPS server

- Ensure IMPS\bin is in the PATH or Install OpenSSL on a window server and update PATH to use that install folder

Step 01: Redirect the OpenSSL configuration to an sample configuration file. {Not necessary but it may be customized.}

set OPENSSL_CONF=C:\Users\Administrator\Desktop\openssl_DC\openssl_config_sample.cfg.txt

Step 02: Make a folder to hold these new files c:\temp\ssl

Step 03: Generate a private CA key using OpenSSL <Enter a password twice>

openssl genrsa -des3 -out 01.rootCA.key 1024

openssl rsa -in 01.rootCA.key -out 02.rootCA_nopassword.key <To remove password for later phases>

Step 04: Create a self-signed x509 CA certificate. The CA certificate will be valid for 20 years (-days 7300).

openssl req -out 03.rootCA.crt -key 02.rootCA_nopassword.key -new -x509 -days 7300 -subj "/CN=#####_LAB_Root_Certificate_Authority_#####"

Switch Servers: Execute the following ONLY the Active Directory Server (DC)

Step 05: Edit the input CSR file; ensure CN = FQDN {see the box to the side}

Step 06: Create the CSR using MS command line tool: certutil

certreq -new request.inf <FQDN>.csr {IMPORTANT: If CA is removed from ADS DC, this step must be re-done}

Switch Server: Copy the CSR to the IMPS server.

Step 07: Sign the CSR with the private CA key

openssl x509 -req -days 3650 -in <FQDN>.csr -CA 03.rootCA.crt -CAkey 02.rootCA_nopassword.key -set_serial 01 -out <FQDN>.crt

Step 08: On BOTH the IMPS & the ADS DC; and import the CA root file into the following:

certlm.msc (The root CA cert into (Local Computer \ Trusted Root Cert Auth \ Certificates)

03.rootCA.crt

Step 09: ONLY the ADS Server: Accept the signed cert <This will validate against the Trusted Root Cert Auth>

certreq -accept <FQDN>.crt {This file will be copied to Local Computer \ Personal \ Certificates **IMPORTANT – MUST PASS THIS TEST/PROCESS TO SUCCEED** }

Step 10: Validate TCP 636 is available with a SSL Cert using MS LDP w/SSL enabled or other tool. DC may not need to be rebooted/bounced.



openssl_configuration_example.cfg.txt

```
C:\Users\Administrator\Desktop\openssl\new>certreq -new directoryserver.voonair.local.inf ad2.csr
CertReq: Request Created
C:\Users\Administrator\Desktop\openssl\new>certreq -accept ad2.crt
C:\Users\Administrator\Desktop\openssl\new>
```

```
----- request.inf -----
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=directoryserver.voonair.local"
;
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1; this is for Server Authentication
```

```

@echo on
:: Create a CA root Certificate using OpenSSL-Win64 (or Win32)
:: Set an initial openssl configuration file
set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg
set FQDN=dc001.exchange.lab
set PASSWORD=P$ssword01

:: Make a output folder
mkdir c:\temp\openssl

:: Clean up Certs from prior executions / stores
certutil -delstore "Root" ###_LAB_ROOT_CA_Cert_Auth_For_Active_Directory_###
certutil -delstore "My" %FQDN%

:: Update inf file with the latest FQDN name
copy ADS_server_cert_request.inf c:\temp\openssl\ADS_server_cert_request.inf

:: Generate a private CA key
cd /d C:\OpenSSL-Win64\bin
openssl genrsa -des3 -passout pass:%PASSWORD% -out c:\temp\openssl\01.rootCA.key 1024
openssl rsa -in c:\temp\openssl\01.rootCA.key -passin pass:%PASSWORD% -out c:\temp\openssl\02.rootCA_nopassword.key

:: Create a self-signed x509 cert
openssl req -out c:\temp\openssl\03.rootCA.crt -key c:\temp\openssl\02.rootCA_nopassword.key -new -x509 -days 7300 -subj
"/CN=###_LAB_ROOT_CA_Cert_Auth_For_Active_Directory_###"

:: Execute on the Active Directory Server (DC) only
certreq -f -new c:\temp\openssl\ADS_server_cert_request.inf c:\temp\openssl\%FQDN%.csr

:: Sign the CSR with the private CA key
openssl x509 -req -days 3650 -in c:\temp\openssl\%FQDN%.csr -CA c:\temp\openssl\03.rootCA.crt -CAkey c:\temp\openssl\02.rootCA_nopassword.key -set_serial 01 -out
c:\temp\openssl\%FQDN%.crt

:: On both the AD & IMPS Servers, import the CA root file into (Local Computer \ Trusted Root Cert Auth \ Certificates)
::certlm.msc
certutil -addstore "Root" c:\temp\openssl\03.rootCA.crt

:: Only on the AD server, accept the signed cert. This MUST PASS to SUCCEED
:: Cert will then be auto-copied to (Local Computer \ Personal \ Certificates )
certreq -accept c:\temp\openssl\%FQDN%.crt
pause
:: Validate TCP 636 is available with a SSL Cert; may use MS LDP. Note: DC may not need to be rebooted/bounced.
ldp.exe

```

```

;----- request.inf -----
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=dc001.exchange.lab"
;
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1; this is for Server Authentication

```

VALIDATE FROM MS ACTIVE DIRECTORY DOMAIN CONTROLLER

certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authentication	The U...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authentication	DigiC...

certlm - [Certificates - Local Computer\Personal\Certificates]

There are no items to show in this view.

BEFORE STATE on MS Active Directory Domain Controller

certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
#####_LAB_Root_Certificate_Authority_#####	#####_LAB_Root_Certificate_Authority_#####	6/7/2036	<All>	
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authentication	

certlm - [Certificates - Local Computer\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
directoryserver.voonair.local	#####_LAB_Root_Certificate_Authority_#####	6/10/2026	<All>	<None>

AFTER STATE on MS Active Directory Domain Controller

VALIDATE FROM MS ACTIVE DIRECTORY DOMAIN CONTROLLER

ldp.exe MS ADS LDAP Tool

Connect

Server:

Port: ☐ Connectionless ☒ SSL

OK Cancel

```
ldaps://directoryserver.voonair.local/DC=voonair,DC=local
Connection Browse View Options Utilities Help

ld = ldap_sslinit("directoryserver.voonair.local", 636, 1);
Error 0 = ldap_set_option(hLdap,
LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
Host supports SSL, SSL cipher strength = 256 bits
Established connection to directoryserver.voonair.local.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
  configurationNamingContext:
    CN=Configuration,DC=voonair,DC=local;
  currentTime: 6/12/2016 10:20:40 PM Eastern Daylight Time;
  defaultNamingContext: DC=voonair,DC=local;
  dnsHostName: directoryserver.voonair.local;
  domainControllerFunctionality: 6 = ( WIN2012R2 );
  domainFunctionality: 3 = ( WIN2008 );
  dsServiceName: CN=NTDS
    Settings,CN=DIRECTORYSERVER,CN=Servers,CN=Def
    au't First Site
    Mo
```

WORKING CERTS EXAMPLE

```
ld = ldap_sslinit("directoryserver.voonair.local", 636, 1);
Error 81 = ldap_set_option(hLdap,
LDAP_OPT_PROTOCOL_VERSION, 3);
Error 81 = ldap_connect(hLdap, NULL);
Server error: <empty>
Error <0x51>: Fail to connect to directoryserver.voonair.local.
```

NO CERTS EXAMPLE



Validate from CA IMPS Server: adsldapdiag.exe

```
Administrator: Command Prompt

E:\Programs\CA\Identity Manager\Provisioning Server\bin>adsldapdiag directoryserver.voonair.local

***** 06/12/16 - 22:39:00 *****
***** Connect to:
        Server: directoryserver.voonair.local
        Port:   636
        SSL :   YES

ldap_sslinit() ..... Done
ldap_connect() ..... Done
ldap_get_option() ..... Done
        Cipher Strength: 256
        Hash   Strength: 384

ldap_get_option() ..... Done
        Size Limit: 0
ldap_set_option() ..... Done
ldap_get_option() ..... Done
        Keep Alive: 120
ldap_get_option() ..... Done
        Reconnect: 1
ldap_search_s() ..... Done
        Default Naming Context:
        DC=voonair,DC=local
        Root Naming Context:
        DC=voonair,DC=local
        Bind DN: CN=Administrator,CN=Users,DC=voonair,DC=local

ldap_simple_bind_s() ..... ERROR: 49
        LdapGetLastError(): 49
        Error msg: Invalid Credentials

Attempting manual connection to server:
```

VALIDATE FROM CA IMPS SERVER

```
E:\Programs\CA\Identity Manager\Provisioning Server\bin>adsldapdiag -v -u administrator directoryserver.voonair.local  
caeducation
```

```
***** 06/12/16 - 22:51:07 *****
```

```
***** Connect to:
```

```
Server: directoryserver.voonair.local
```

```
Port: 636
```

```
SSL : YES
```

```
ldap_sslinit() ..... Done
```

```
ldap_connect() ..... Done
```

```
ldap_get_option() ..... Done
```

```
Cipher Strength: 256
```

```
Hash Strength: 384
```

```
ldap_get_option() ..... Done
```

```
Size Limit: 0
```

```
ldap_set_option() ..... Done
```

```
ldap_get_option() ..... Done
```

```
Keep Alive: 120
```

```
ldap_get_option() ..... Done
```

```
Reconnect: 1
```

```
ldap_search_s() ..... Done
```

```
Default Naming Context:
```

```
DC=voonair,DC=local
```

```
Root Naming Context:
```

```
DC=voonair,DC=local
```

```
Bind DN: CN=adminiator,CN=Users,DC=voonair,DC=local
```

```
ldap_simple_bind_s() ..... Done
```

```
***** Connection Established: 22:51:07
```

```
Attempting manual connection to server:
```

VALIDATE FROM CA IMPS SERVER


```
openssl s_client -connect HOST:636 -showcerts
```



```
E:\Programs\CA\Identity Manager\Provisioning Server\bin>openssl s_client -connect directoryserver:636 -showcerts -CAfile
C:\Users\Administrator\Desktop\openssl_DC\new\03.rootCA.crt
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
CONNECTED(0000015C)
depth=1 CN = "#####_LAB_Root_Certificate_Authority_#####"
verify return:1
depth=0 CN = directoryserver.voonair.local
verify return:1
---
Certificate chain
 0 s:/CN=directoryserver.voonair.local
  i:/CN=#####_LAB_Root_Certificate_Authority_#####
  -----BEGIN CERTIFICATE-----
MIIBZjCCATcCAQEDQYJKoZIhvcNAQEFBQAwwNzE1MDMGA1UEAwwsIyMjIyMjX0xB
Q19Sb290X0NlcnRyZmljYXRlX0F1dGhvcml0eU8jIyMjIyMwHhcNMTYwNjEzMDIz
NDAzWhcNMjYwNjEzMDIzNDAzWjA0MSYwJAYDUQDDDB1kaXJlY3RvcnlsZXJ2ZXIu
dm9ubmFpcis5sb2NhbnDCBnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAu4nw9XAT
SXc0sUxQGxaiHAR81Jx7qijGDPO85aFbWw19cbAaYvF6ClUprMplqbizD2ZZJz00
c0ZiLgxiG3sSJDQweT07QQRfNyLbgUygyRyak3a92M0tZi0m7g659b7imnhDBtbKR
DhyWCLH2j12JQwUvai664+3a72Ngj+qPJCsCAwEAATANBgkqhkiG9w0BAQUFAAOB
gQAQ0QFLlmPcUeiztYmnjb72/yC+91WaF7eRGRJk7uBg0RJ7ACz5gyJNUe3loETC
bpkIEBbzEUW40ihyeQeTY+hNkisNERH1fKwEMf qW/vpTpEfmb13+LAZP5EPg4xcL
SUBem+eb77R08XiGNEJaaNTUWCY5NqnRAn8/6Ui8xHKGrw==
-----END CERTIFICATE-----
---
Server certificate
subject=/CN=directoryserver.voonair.local
issuer=/CN=#####_LAB_Root_Certificate_Authority_#####
---
No client certificate CA names sent
---
SSL handshake has read 1165 bytes and written 359 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : DHE-RSA-AES256-GCM-SHA384
    Session-ID: 9123000056FF9654BA2BEC1B148844E7449C656838C1555BDD34F5C87CEAE6BE
    Session-ID-ctx:
    Master-Key: 7B39DE01C437C58349CA3D42C4A85BD09A4BD5D62615156538A373639522BB67DEFBACCDD86C33FA29F7A792FA373839
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1465793699
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

VALIDATE FROM CA IMPS SERVER

USING

openssl s_client -connect HOST:636 -showcerts -CAfile rootCA.crt

Program Exits Reference Attribute Mapping Logging

* ADS Server Security Configuration Endpoint Settings

* Name:

Description:

Server

Use the fully qualified name of the server.

* Host Name:

* User ID:

* Password:

☐ Enable Failover

Account Template

Domain Account Template

Default:

VALIDATE FROM CA IMPS SERVER

Program Exits Reference Attribute Mapping Logging

* ADS Server Security Configuration Endpoint Settings

The IM Provisioning server can communicate with Active Directory in one of three ways:

- * Use LDAP via an SSL secure encryption link (Drawback: Additional setup required.)
- * Use LDAP without SSL; use ADSI for passwords only (Drawback: Less security; ADSI does not work in all environments) (For demo purposes only.) (NOTE: For ADSI only, the login id must be provided in the format <domain>\<id> for proper operations.)
- * Use LDAP without SSL; ignore all password requests (Drawback: Not for production environments)

☒ Use LDAP - SSL Encryption (Recommended)

☐ Use LDAP without SSL; use ADSI to set passwords only (for demo only)

☐ Do not use SSL (Useful for demo purposes only.)

By choosing this option, I understand that IM Provisioning will not be able to manage passwords on this endpoint, and will silently ignore all password set/change requests.

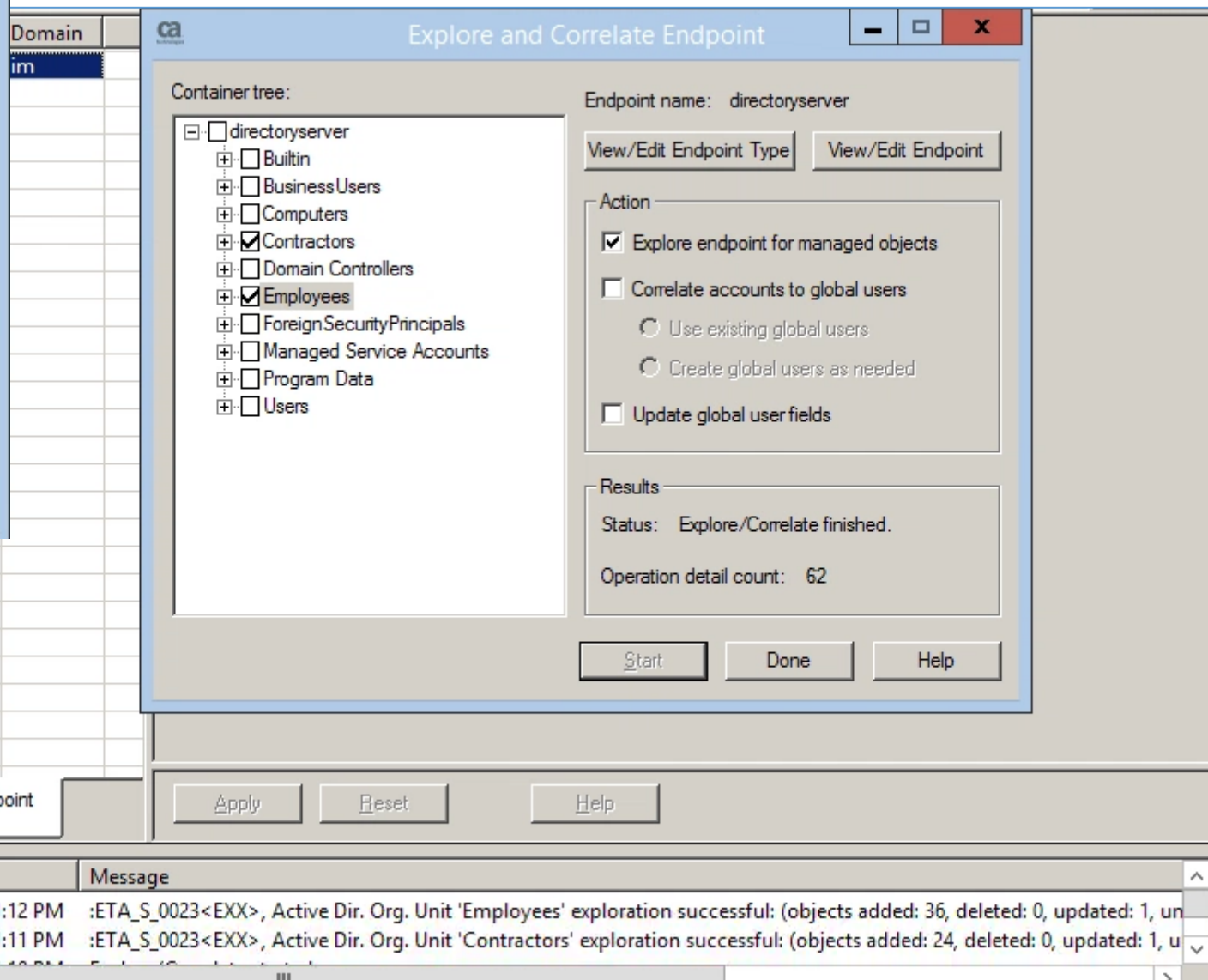
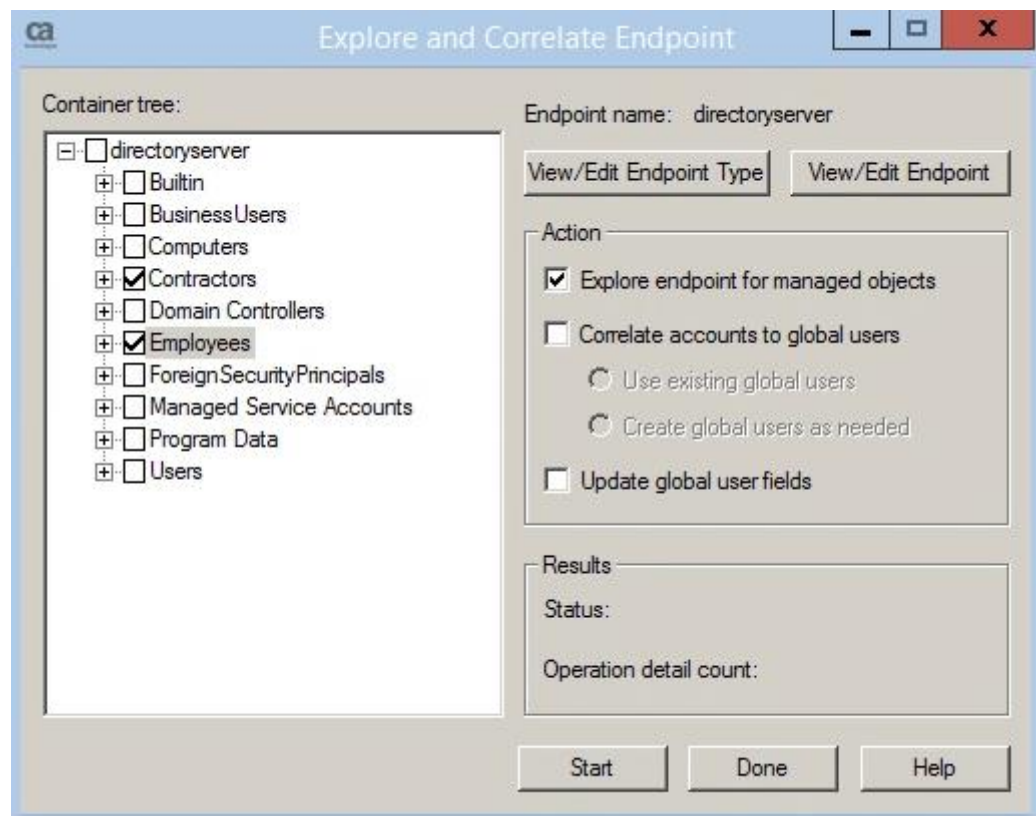
Active Directory Endpoint

Time	Message
6/12/2016 10:58:05 PM	:ETA_S_0001<ADI>, Active Directory Endpoint 'directoryserver' created successfully
6/12/2016 10:56:06 PM	Welcome to Provisioning Manager.

For Help, press F1

Server: imserver

Object Count: 1



VALIDATE FROM CA IMPS SERVER

Object Domains: im Domains Object type Object Domain

Simple attribute: EndpointName Advanced V Simple attribute

ADSAccount ▼

Alice Dubois
Anita Hirsch
Anne Garrett
Art Katect
Bai Chin
Brian Mendoza
Bruce Adams
Carlos Pena
Cat Taylor
Cathy Dimitri
Charlie Boyd
Colter Ames
Dave Abraham
Debbie Patrick
Dylan Davies
Heather Marley
Jason Sauer
Jeff Hardy
Joe Smith
Joy Suthe

Endpoint Content

Object type: Active Dir. Account

Create new content

Container tree

- directoryserver
 - Contractors
 - Employees

Search for content

Attribute: ADSAccount

Value: *

Advanced Search

Container type: ADSOrgUnit

☐ Search only one container level

Active Directory Account

User Certificates | Object | Account Templates | Security Identity Mapping | Statistics

Telephones | Organization | Groups (Member Of) | Dial-in | Custom | Terminal Services

* General | Common Account Settings | Address | * Account | Password | Profile

First name: Anne Initials:

Last name: Garrett

* Display name: Anne Garrett

Active Directory Account

User Certificates | Object | Account Templates | Security Identity Mapping | Statistics

Telephones | Organization | Groups (Member Of) | Dial-in | Custom | Terminal Services

* General | Common Account Settings | Address | * Account | Password | Profile

Container: Employees/Information Technology

First name: Anne Initials:

Last name: Garrett

* Display name: Anne Garrett

Active Directory Account

User Certificates | Object | Account Templates | Security Identity Mapping | Statistics

Telephones | Organization | Groups (Member Of) | Dial-in | Custom | Terminal Services

* General | Common Account Settings | Address | * Account | Password | Profile

Password: *

Confirm password: *

* User login name:

* User login name (pre Windows 2000):

Mandatory Attribute was missing
Will impact password reset

Time	Message
6/12/2016 11:05:56 PM	:ETA_S_0006<MAC>, Active Dir. Account 'Anne Garrett' on 'directoryserver' modified successfully
6/12/2016 11:01:12 PM	:ETA_S_0023<EXX>, Active Dir. Org. Unit 'Employees' exploration successful: (objects added: 36, deleted: 0, updated: 1, un

File Edit Format View Help

```

20160612:230555:TID=001f5c:Modify :E531:-----S: =====
20160612:230555:TID=001f5c:Modify :E531:-----S: External Modify (eTADSAccountName=Anne Garrett) Requested by User idmadmin - Tena
20160612:230555:TID=001f5c:Modify :E531:-----S: +ntNotSet
20160612:230555:TID=001f5c:Modify :E531:-----P: dn: eTADSAccountName=Anne Garrett,eTADSOrgUnitName=Information Technology,eTA
20160612:230555:TID=001f5c:Modify :E531:-----P: + DSOrgUnitName=Employees,eTADSDirectoryName=directoryserver,eTNamespaceName=Ac
20160612:230555:TID=001f5c:Modify :E531:-----P: + tiveDirectory,dc=im
20160612:230555:TID=001f5c:Modify :E531:-----P: eTADSuserPrincipalName: agarrett@voonair.local [REPLACE]
20160612:230555:TID=001f5c:Modify :E531:-----P: eTPassword: ** NOT SHOWN ** [REPLACE]
20160612:230555:TID=001f5c:Modify :E531:-----P: eTUseOperationID: 735e2941-31a2-44bd-a293-0afa2917eab4 [REPLACE]
20160612:230555:TID=001f5c:Modify :E531:-----P: eTUpdateNode: IMSERVER [REPLACE]
20160612:230555:TID=001f5c:Modify :E531:-----P: modifiersName: ETGLOBALUSERNAME=IDMADMIN,ETGLOBALUSERCONTAINERNAME=GLOBAL US
20160612:230555:TID=001f5c:Modify :E531:-----P: + ERS,ETNAMESPACENAME=COMMONOBJECTS,DC=IM,DC=ETA [REPLACE]
20160612:230555:TID=001f5c:Modify :E531:-----P: modifyTimestamp: 20160613030555Z [REPLACE]
20160612:230556:TID=001f5c:Add :Y544:E531:S: Notify Add (eTNotifyOpID=3fde4051-c8b8-40b9-8940-a175afb7e2d4) Requested by User
20160612:230556:TID=001f5c:Add :Y544:E531:S: +idmadmin - TenantNotSet
20160612:230556:TID=001f5c:Add :Y544:E531:P: URL: ldaps://imserver:20391
20160612:230556:TID=001f5c:Add :Y544:E531:P: dn: eTNotifyOpID=3fde4051-c8b8-40b9-8940-a175afb7e2d4
20160612:230556:TID=001f5c:Add :Y544:E531:P: objectClass: eTNotifyOp
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyOpID: 3fde4051-c8b8-40b9-8940-a175afb7e2d4
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyEncrypted: yes
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyPayload: {3DES}F0U70eVUYVpad+5N/kuKxXftkFHnq7PJJaGHhb2qJEFgb8fkCwwoZ7
20160612:230556:TID=001f5c:Add :Y544:E531:P: + kfIHdZGienMSRchgh5m5f2x91aJwXGcWUq41FQDox6Wyph52qvB4F+47Ew3z8EqBNHr01ZXqQU5gJ
20160612:230556:TID=001f5c:Add :Y544:E531:P: + WT7kHPzzI+PwACwc5EB080GPPzFshdny5f84DALfx0Di17C55vcXTxw+i14ITuDTmWC+bDpazZ91m
20160612:230556:TID=001f5c:Add :Y544:E531:P: + a5oE0nV5PDjjMRL0vAN/fiHY0d12Q+uOp9j17H3kdFFsqCuTMmBFP5cmK3JUx551SnOxHmE41kppx
20160612:230556:TID=001f5c:Add :Y544:E531:P: + E+3sAN/fiHY0d12Q+uOp9j17H3kdFFsqCuTM3vDPkjztPh9pBohjBouhRgNB7YFIBX6qTKEPmt5jk
20160612:230556:TID=001f5c:Add :Y544:E531:P: + us/JtRdGrjyfOukcD/jl23MKYqlyzhPzV4f2kCa402Igd8GHojVABB1CNN30jhFAklxsdJTXnUp7
20160612:230556:TID=001f5c:Add :Y544:E531:P: + 9gG/T/u6z3oSl+HkSmdc12eElKvzoHTQ5oKb8yzTz8kgEMriTaj0XRC2...
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyState: Complete
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyCreateTimet: 1465787156
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifySequenceNo: 0000000073
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyProvOpDN: eTADSAccountName=Anne Garrett,eTADSOrgUnitName=Information
20160612:230556:TID=001f5c:Add :Y544:E531:P: + Technology,eTADSOrgUnitName=Employees,eTADSDirectoryName=directoryserver,eTN
20160612:230556:TID=001f5c:Add :Y544:E531:P: + amespaceName=ActiveDirectory,dc=im
20160612:230556:TID=001f5c:Add :Y544:E531:P: eTNotifyProvOp: Modify_Account_Password
20160612:230556:TID=001f5c:Add :Y544:E531:F: SUCCESS: Notify Add (eTNotifyOpID=3fde4051-c8b8-40b9-8940-a175afb7e2d4)

```


File Edit Format View Help

```
20160612:230153:TID=000c14:I: SeqNo: 0000000072
20160612:230153:TID=000c14:I: Try sending payload to http://imserver.voonair.local:8080/iam/im/ETACALLBACK/?env=identityEnv
20160612:230154:TID=000c14:I: SUCCESS: Payload sent successfully
20160612:230154:TID=000c14:I: DONE: Notifications Processed: 20/20+
20160612:230154:TID=000c14:I: =====
20160612:230154:TID=000c14:I: START: Notify Batch Processing
20160612:230154:TID=000c14:I: DONE: Notifications Processed: 0/0
20160612:230556:TID=000c14:I: =====
20160612:230556:TID=000c14:I: START: Notify Batch Processing
20160612:230556:TID=000c14:I: Sending Notification: eTNotifyOpID=3fde4051-c8b8-40b9-8940-a175afb7e2d4
20160612:230556:TID=000c14:I: Event: Modify_Account_Password (eTADSAccountName=Anne Garrett)
20160612:230556:TID=000c14:I: SeqNo: 0000000073
20160612:230556:TID=000c14:I: Try sending payload to http://imserver.voonair.local:8080/iam/im/ETACALLBACK/?env=identityEnv
20160612:230557:TID=000c14:I: SUCCESS: Payload sent successfully
20160612:230557:TID=000c14:I: DONE: Notifications Processed: 1/1+
20160612:230557:TID=000c14:I: =====
20160612:230557:TID=000c14:I: START: Notify Batch Processing
20160612:230557:TID=000c14:I: DONE: Notifications Processed: 0/0
```

```

-----
-> eTADSDirectoryName=directoryserver,eTNamespaceName=ActiveDirectory,dc=im,dc=etasa <-
-----

Config ExpirePwd: 0
Config HomeDirInheritPermission: 0

***** 06/12/16 - 22:58:03 *****
***** Connect to:
Server: directoryserver.voonair.local
Port: 636
SSL : YES

ldap_sslinit() ..... Done
ldap_connect() ..... Done
ldap_get_option() ..... Done
    Cipher Strength: 256
    Hash Strength: 384

ldap_set_option() size limit..... Done
    New Size Limit: 1000
ldap_get_option() size limit..... Done
    Current Size Limit : 1000
ldap_set_option() time limit..... Done
    New Time Limit: 150
ldap_get_option() time limit..... Done
    Current Time Limit: 150
ldap_set_option() Protocol Version..... Done
ldap_set_option() Referrals..... Done
ldap_get_option() Referrals..... Done
    Current Referral Value : 0
ldap_get_option() Keep Alive..... Done
    Current Keep Alive value: 120
ldap_get_option() Auto Reconnect..... Done
    Current Reconnect value: 1














```

```

-----
TID=0x25e0: init object: CN=Users,DC=voonair,DC=local, rc=0x0
TID=0x25e0: adopted DN: CN=Users,DC=voonair,DC=local, rc=0x0
TID=0x25e0: skip special DN: DC=ForestDnsZones,DC=voonair,DC=local, name: ForestDnsZones
TID=0x25e0: skip special DN: DC=DomainDnsZones,DC=voonair,DC=local, name: DomainDnsZones
Search for attribute uPNSuffixes didn't return any value, err=80
Search for attribute uPNSuffixes didn't return any value, err=80
Search for attribute uPNSuffixes didn't return any value, err=80
23:03:37 - TID:0x25e0 GetPrimaryGroup of CN=Anne Garrett,OU=Information Technology,OU=Employees,DC=voonair,DC=local succeeded
getSamAcctName: value from LDAPsearch: DIRECTORYSERVER
TID=0x25e0: 2016.06.12 - 23:03:37.456 : Get TS
TID=0x25e0: 2016.06.12 - 23:03:38.519 : Done Get TS: rc=0
23:05:56 - TID:0x10f0 GetPrimaryGroup of CN=Anne Garrett,OU=Information Technology,OU=Employees,DC=voonair,DC=local succeeded
Search for attribute objectClass didn't return any value, err=80
23:05:56 - TID:0x10f0 GetPrimaryGroup of CN=Anne Garrett,OU=Information Technology,OU=Employees,DC=voonair,DC=local succeeded
TID=0x10f0: 2016.06.12 - 23:05:56.361 : Get TS
TID=0x10f0: 2016.06.12 - 23:05:57.438 : Done Get TS: rc=0

```


Tasks	«
Home	⊕
My Access	⊕
Services	⊕
Users	⊕
Organizations	⊕
Groups	⊕
Roles and Tasks	⊕
Endpoints	⊕
Policies	⊕
Reports	⊕
Environment Administration	⊕
System	—
» Bulk Tasks	
» Email	
» JDBC Connection Management	
» Logical Attributes	
» Select Box Data	
» Web Services	
» Bulk Loader	
» Cleanup Submitted Tasks	
» Configure Global Policy Based Workflows	
» Delete Recurring Tasks	
» Secret Keys	
» View Submitted Tasks	
» Provisioning Configuration	
» Reporting	

View Submitted Tasks							
▼ Description	▼ Status	▼ Priority	▼ Initiated by	▼ Submitted	▼ Last Updated	▼ Last Operation	
 Add Managed Object to Provisioning Directory: Charlie Boyd task, Provisioning Non Managed Object Charlie Boyd	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Carlos Pena task, Provisioning Non Managed Object Carlos Pena	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Joy Sutherland task, Provisioning Non Managed Object Joy Sutherland	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Dylan Davies task, Provisioning Non Managed Object Dylan Davies	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Dave Abraham task, Provisioning Non Managed Object Dave Abraham	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Bai Chin task, Provisioning Non Managed Object Bai Chin	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Brian Mendoza task, Provisioning Non Managed Object Brian Mendoza	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Anne Garrett task, Provisioning Non Managed Object Anne Garrett	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Anita Hirsch task, Provisioning Non Managed Object Anita Hirsch	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Wes Seacrest task, Provisioning Non Managed Object Wes Seacrest	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Rod Waterhouse task, Provisioning Non Managed Object Rod Waterhouse	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Alice Dubois task, Provisioning Non Managed Object Alice Dubois	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	
 Add Managed Object to Provisioning Directory: Markus Eckhard task, Provisioning Non Managed Object Markus Eckhard	Completed	Medium	imadmin	6/12/2016 11:01 PM	6/12/2016 11:01 PM	There was no workflow process mapped to this task.	

Provisioning Manager - by CA (imidnadmin@im) - [System Task/2]

File Edit View Frame Object Window Help

Wizards Users Roles Endpoints System

Global Properties

Domain

im

Domains

Domain Configuration

Password Profile

Program Exits

Identity Manager Setup

IdentityMinder Setup

IdentityMinder Server and Environment

Host Name

Port

Environment

Secured Connection ☐

Add

http://imserver:8080/iam/im/ETACALLBACK/?env=cam
http://imserver.voonair.local:8080/iam/im/ETACALLBACK/?env=cam

Modify

Delete

Move Up

Move Down

Shared secret

Confirm shared secret

Log Level

Info

☐ Suspend sending notifications

Apply Reset Help

Time	Message
6/12/2016 11:19:14 PM	:ETA_S_0005<MCF>, Configuration Object 'BLS Connectivity Configuration' modified successfully
6/12/2016 11:05:56 PM	:ETA_S_0006<MAC>, Active Dir. Account 'Anne Garrett' on 'directoryserver' modified successfully
6/12/2016 11:04:13 PM	:ETA_S_0003<ENV>, Active Dir. Group 'Mainframe' modified successfully

For Help, press F1

Server: imserver

[Version]
Signature="\$Windows NT\$"

[NewRequest]

Subject = "CN=www01.fabrikam.com"; Remove to use an empty Subject name.

;Because SSL/TLS does not require a Subject name when a SAN extension is included, the certificate Subject name can be empty. If you are using another protocol, verify the certificate requirements.

EncipherOnly = FALSE ; Only for Windows Server 2003 and Windows XP. Remove for all other client operating system versions.

Exportable = FALSE ; TRUE = Private key is exportable

KeyLength = 2048 ; Valid key sizes: 1024, 2048, 4096, 8192, 16384

KeySpec = 1 ; Key Exchange – Required for encryption

KeyUsage = 0xA0 ; Digital Signature, Key Encipherment

MachineKeySet = True

ProviderName = "Microsoft RSA SChannel Cryptographic Provider"

RequestType = PKCS10 ; or CMC.

[EnhancedKeyUsageExtension]

; If you are using an enterprise CA the EnhancedKeyUsageExtension section can be omitted

OID=1.3.6.1.5.5.7.3.1 ; Server Authentication

OID=1.3.6.1.5.5.7.3.2 ; Client Authentication

[Extensions]

; If your client operating system is Windows Server 2008, Windows Server 2008 R2, Windows Vista, or Windows 7

; SANs can be included in the Extensions section by using the following text format. Note 2.5.29.17 is the OID for a SAN extension.

2.5.29.17 = "{text}"

continue = "dns=www01.fabrikam.com&"

continue = "dn=CN=www01,OU=Web Servers,DC=fabrikam,DC=com&"

continue = "url=http://www.fabrikam.com&"

continue = "ipaddress=172.31.10.134&"

continue = "email=hazem@fabrikam.com&"

continue = "upn=hazem@fabrikam.com&"

continue = "guid=f7c3ac41-b8ce-4fb4-aa58-3d1dc0e36b39&"

; If your client operating system is Windows Server 2003, Windows Server 2003 R2, or Windows XP

; SANs can be included in the Extensions section only by adding Base64-encoded text containing the alternative names in ASN.1 format.

; Use the provided script MakeSanExt.vbs to generate a SAN extension in this format.

2.5.29.17=MCaCEnd3dzAxLmZhYnJpa2FtLmNvbYlQd3d3LmZhYnJpa2FtLmNvbQ==

[RequestAttributes]

; If your client operating system is Windows Server 2003, Windows Server 2003 R2, or Windows XP

; and you are using a standalone CA, SANs can be included in the RequestAttributes section by using the following text format.

SAN="dns=www01.fabrikam.com&dns=www.fabrikam.com&ipaddress=172.31.10.130"

; Multiple alternative names must be separated by an ampersand (&).

CertificateTemplate = WebServer ; Modify for your environment by using the LDAP common name of the template.

;Required only for enterprise CAs.

[https://technet.microsoft.com/en-us/library/dn296456\(v=ws.11\).aspx#BKMK_accept](https://technet.microsoft.com/en-us/library/dn296456(v=ws.11).aspx#BKMK_accept)

<https://technet.microsoft.com/library/ff625722.aspx>