impero
education pro

Impero Education Pro

Cloud Hosted Server Active Directory Setup Guide

May 2019

impero

© 2019 Impero Solutions Ltd

Table of Contents

© 2019 Impero Solutions Ltd

Introduction

This document details the steps required to configure Active Directory for use with a cloud hosted Impero Education Pro Server. Impero Education Pro will communicate to the customers domain controller using the Lightweight Directory Access Protocol over Secure Socket Layer (LDAPS). This ensures that any data transmitted between the Domain Controller and Impero Education Pro is encrypted using SSL. This will allow some of the features within Impero to interact with customers active directory such as change password.

Pre Requisites

The below will be needed to get the LDAP's configuration working;

- The following firewall configuration is required only for the Domain Controller that Impero will be contacting over LDAPS.** The Domain controller will need to be publicly accessible either via a DMZ or by Port Forwarding.

Protocol	Port	Traffic Direction	Rule
TCP	636	Inbound & Outbound	Allow
TCP	389	Inbound & Outbound	Block*

**blocking 389 is not a requirement but advised so that there will be no attempt to transmit information across this port.*
*** This is in addition to the usual Impero Exclusions.*

- We advise if you are not already using LDAP's for other reasons that you restrict the communication to our servers.

- Please take note of your Domain Controllers FQDN (Fully Qualified Domain Name) and your Public IP address as this will be required later.

- We advise creating a service account in an active directory such as Impero-Admin who has the permission to be able to change password etc... (Account Operators) as we will need the username and password

© 2019 Impero Solutions Ltd

for authentication purposes but is not essential, this will be described and set up later in this guide.

- You will need to be able to create/generate certificates on the domain controller.

Certificate Setup

In the next following steps, we are going to be setting up the Certificates so that the Impero Services and your domain controller can communicate with each over SSL.

Install Active Directory Certificate Services (AD CS)

1. Open the **'Start'** screen - this can be accessed from the bottom left of the desktop or by pressing the Windows key.
2. Search for **'Server Manager'** and click to open it.
3. Click 'Manage' in the top left of the Server Manager.
4. Click 'Add Roles and Features' (Image 1).

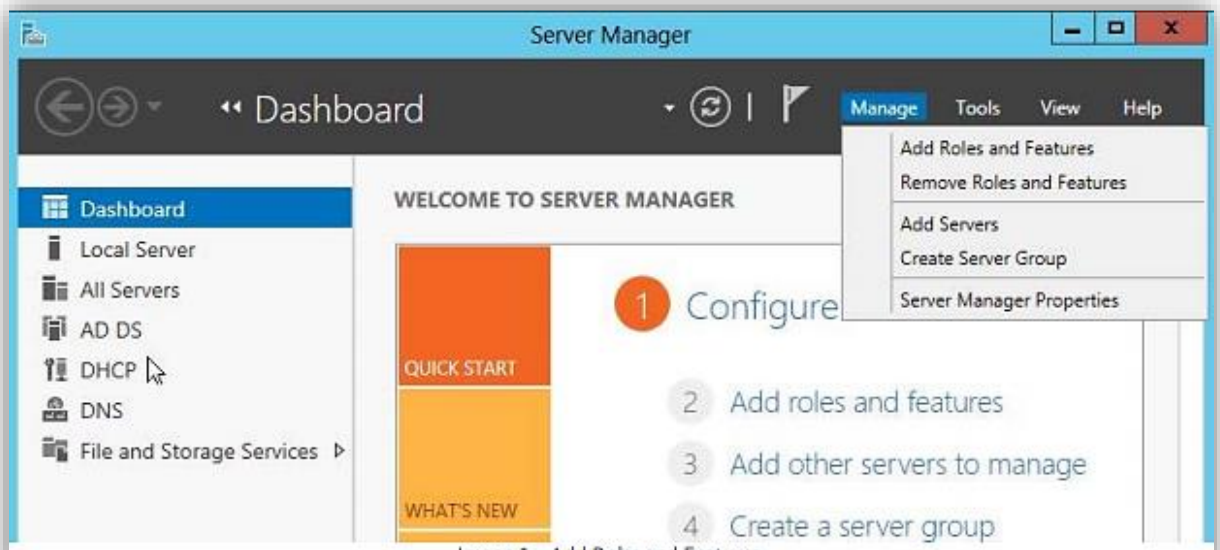
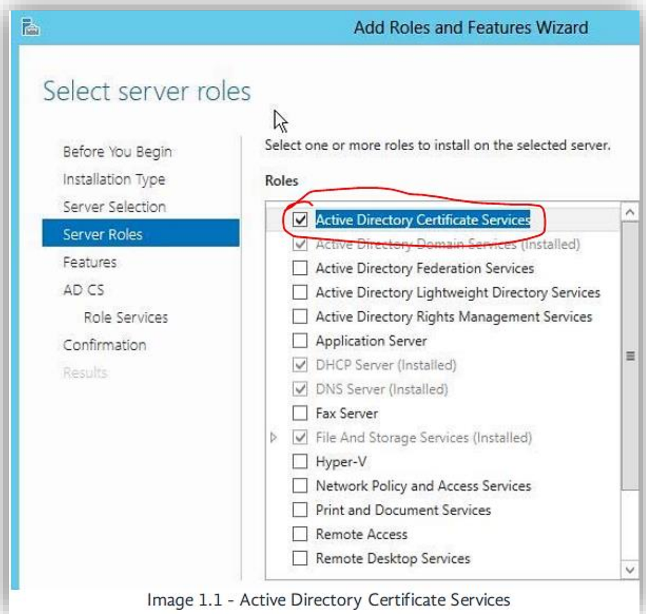


Image 1 - Add Roles and Features

5. The 'Add Roles and Features Wizard' should open.
6. Click 'Next' on the 'Before you Begin' screen.

© 2019 Impero Solutions Ltd

7. Click 'Next' on the 'Installation Type' screen.
8. Click 'Next' on the 'Server Selection' screen.
9. Tick 'Active Directory Certificate Services' and an additional window should appear (Image 1.1).



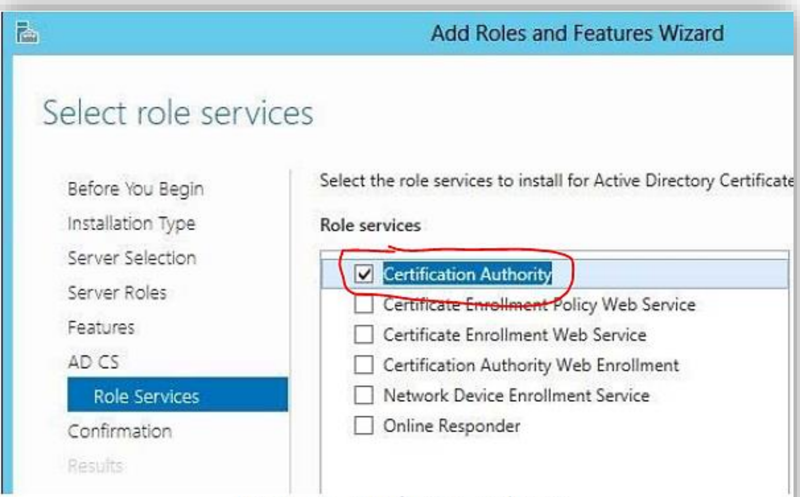
Select one or more roles to install on the selected server.

Roles

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
□ Fax Server
☑ File And Storage Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services

Image 1.1 - Active Directory Certificate Services

10. Click 'Add Features'.
11. Click 'Next' on the 'Server Roles' screen.
12. Click 'Next' on the 'Features' screen.
13. Click 'Next' on the 'AD CS' screen.
14. Ensure that 'Certification Authority' is ticked (Image 1.2).



Select the role services to install for Active Directory Certificate

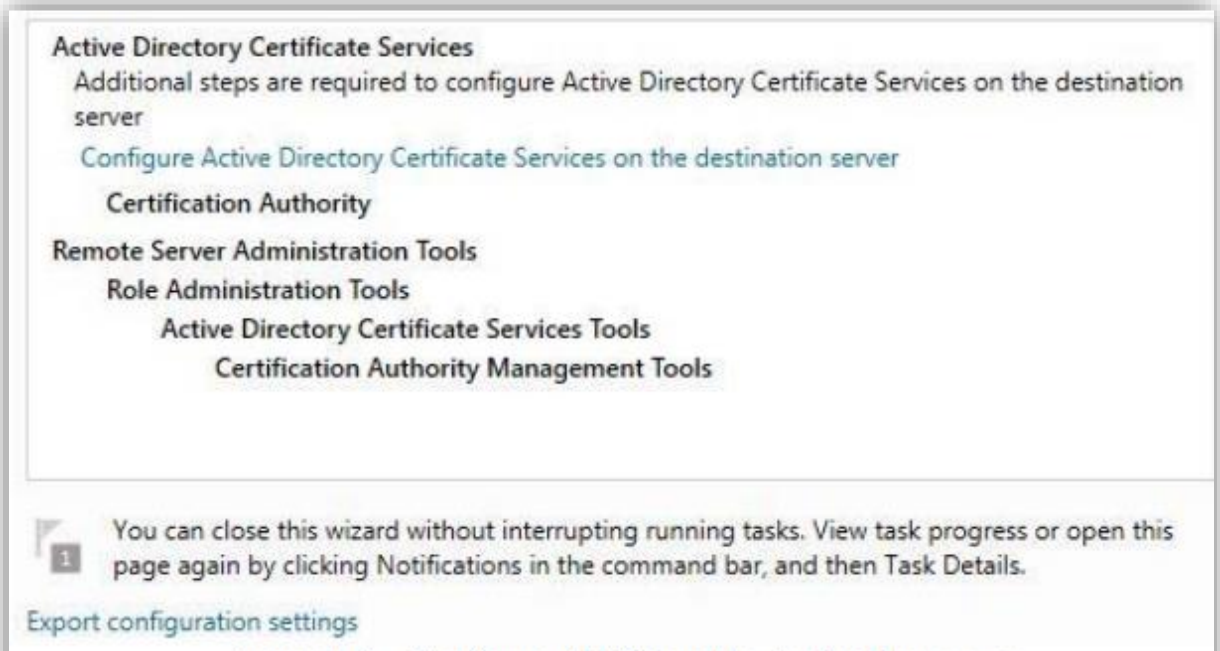
Role services

☑ Certification Authority
□ Certificate Enrollment Policy Web Service
□ Certificate Enrollment Web Service
□ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

Image 1.2 - Certification Authority

© 2019 Impero Solutions Ltd

15. Click 'Next'.
16. Click 'Install' on the 'Confirmation' screen.
17. Wait for the installation to complete.
18. Click 'Configure Active Directory Certificate Services on the destination server' on the 'Results' screen (Image 1.3).



Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on the destination server

Configure Active Directory Certificate Services on the destination server

Certification Authority

Remote Server Administration Tools

Role Administration Tools

Active Directory Certificate Services Tools

Certification Authority Management Tools

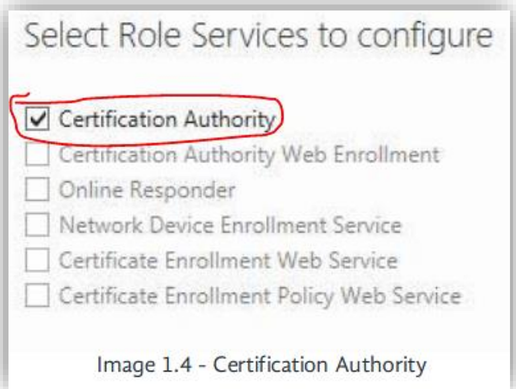
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Image 1.3 - Configure AD CS on the destination server

19. The 'AD CS Configuration' window should open.
20. Confirm that you are using an administrator account which is a member of the Enterprise Admins group. If not, please select 'Change...' and enter the credentials of an account with membership to the Enterprise Admins group.
21. Click 'Next' on the 'Credentials' screen.
22. Tick 'Certification Authority' (Image 1.4).

© 2019 Impero Solutions Ltd

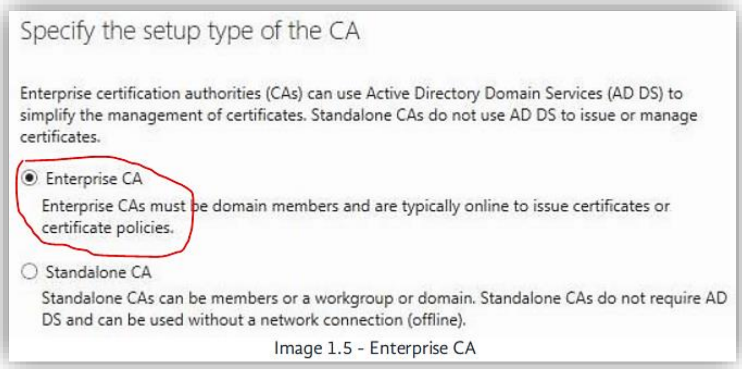


Select Role Services to configure

☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Image 1.4 - Certification Authority

23.Click 'Next' on the 'Role Services' screen.
24.Confirm that 'Enterprise CA' is selected (Image 1.5).



Specify the setup type of the CA

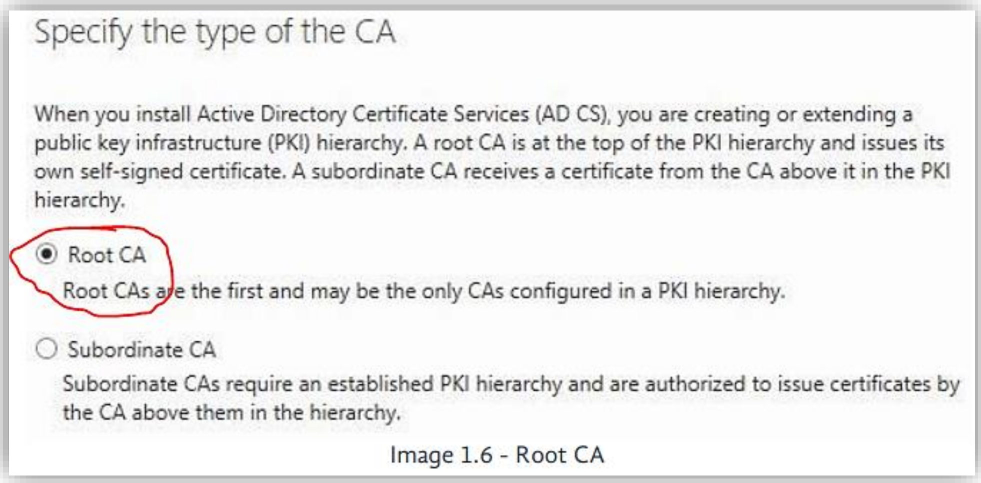
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

Image 1.5 - Enterprise CA

25.Click 'Next' on the 'Setup Type' screen.
26.Confirm that 'Root CA' is selected (Image 1.6).



Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

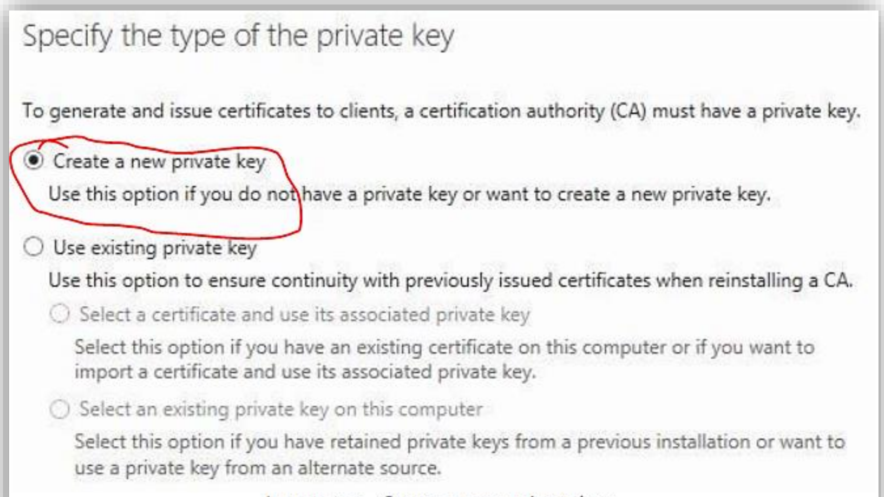
● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Image 1.6 - Root CA

© 2019 Impero Solutions Ltd

27. Click 'Next' on the 'CA Type' screen.
28. Confirm that 'Create a new private key' is selected (Image 1.7).



Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

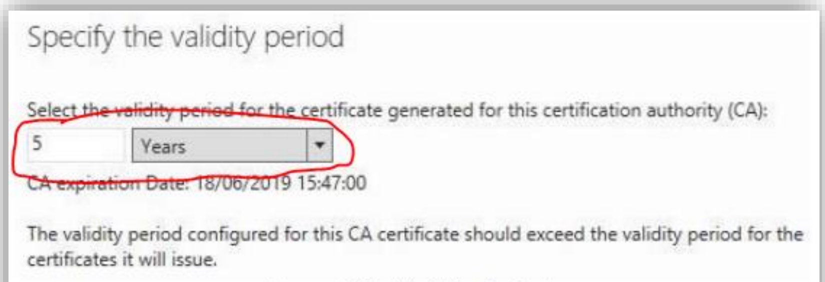
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Image 1.7 - Create a new private key

29. Click 'Next' on the 'Private Key' screen.
30. Click 'Next' on the 'Cryptography' screen.
31. Click 'Next' on the 'CA Name' screen.
32. Confirm that the validity period is set to '5 years' *this is custom and will require this step to be redone on expiry (Image 1.8).



Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years ▾

CA expiration Date: 18/06/2019 15:47:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

Image 1.8 - Validity Period

33. Click 'Next' on the 'Validity Period' screen.
34. Click 'Next' on the 'Certificate Database' screen.
35. Click 'Configure' on the 'Confirmation' screen.
36. Wait for the configuration process to complete.
37. Click 'Close' on the 'Results' screen.
38. Click 'Close' on the 'Add Roles and Features Wizard'.

The Domain Controller CA Certificate has now been created.

Create an Impero LDAPS Certificate Template

1. Open the 'Start' screen/menu.
2. Search for 'certsrv.msc' and click to open it.
3. Expand the entry containing the server name under 'Certification Authority (Local)'.
4. Right-click on 'Certificate Templates'.
5. Click 'Manage' (Image 2).

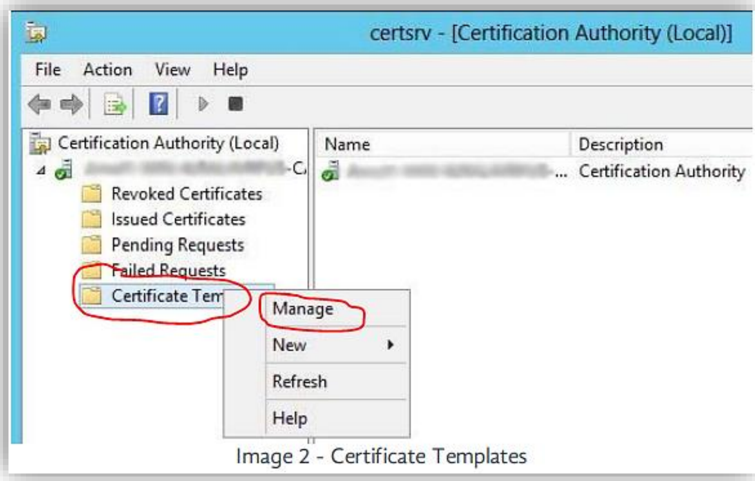
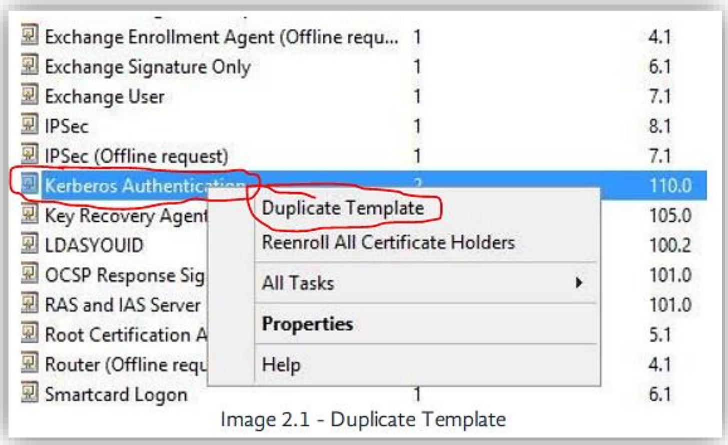


Image 2 - Certificate Templates

6. The 'Certificate Templates Console' should open.
7. Right-click 'Kerberos Authentication' from the list.
8. Click 'Duplicate Template' (Image 2.1).



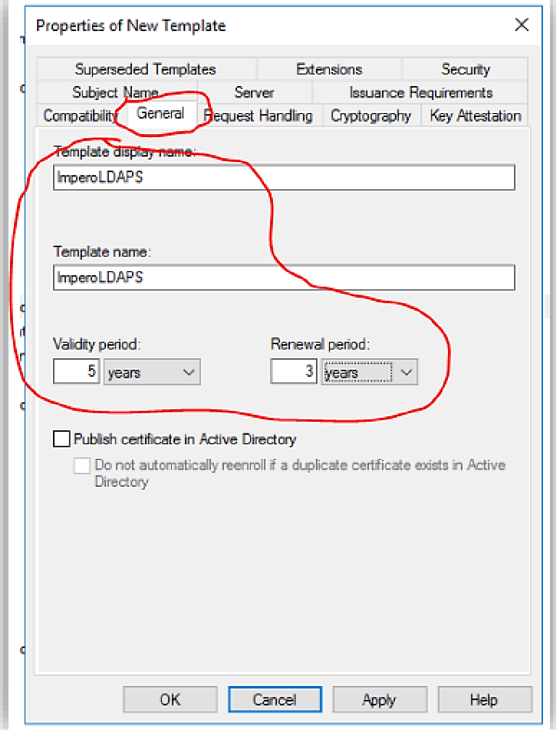
Exchange Enrollment Agent (Offline requ...	1	4.1
Exchange Signature Only	1	6.1
Exchange User	1	7.1
IPSec	1	8.1
IPSec (Offline request)	1	7.1
Kerberos Authentication	2	110.0
Key Recovery Agent		105.0
LDASYOUID		100.2
OCSP Response Sig		101.0
RAS and IAS Server		101.0
Root Certification A		5.1
Router (Offline requ		4.1
Smartcard Logon	1	6.1

Image 2.1 - Duplicate Template

The Kerberos Authentication is a protocol this is used for authenticating the requests between the Impero Service and your Domain Controller across the untrusted network.

© 2019 Impero Solutions Ltd

9. The 'Properties of New Template' window should open
10. Click on the 'General' tab
11. Change the 'Template display name' to 'Impero-LDAPS'
12. Change the 'Validity period' to '5 years' (Image 2.2)
13. Change the 'Renewal period' to '3 years' (Image 2.2)



Template display name:
ImperoLDAPS

Template name:
ImperoLDAPS

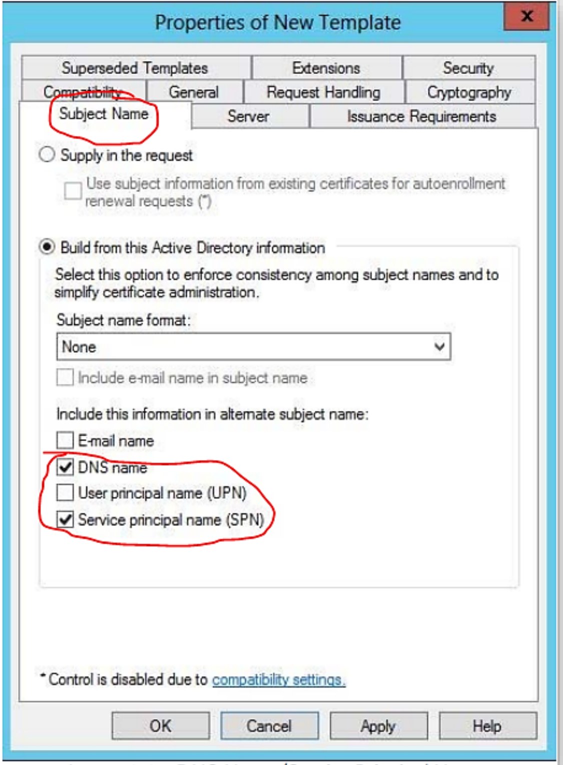
Validity period:
5 years

Renewal period:
3 years

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

14. Click on the 'Subject Name' tab
15. Tick 'DNS name' and 'Service Principal Name (SPN)' (Image 2.3)



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name
☑ DNS name
□ User principal name (UPN)
☑ Service principal name (SPN)

* Control is disabled due to compatibility settings.

Image 2.3 - DNS Name/Service Principal Name

16.Click 'Apply'.
17.Click 'OK'.
18.Close the 'Certificate Templates Console' and return to 'certsrv'.
19.Right-click 'Certificate Templates'.
20.Click 'New -> Certificate Template to Issue' (Image 2.4);

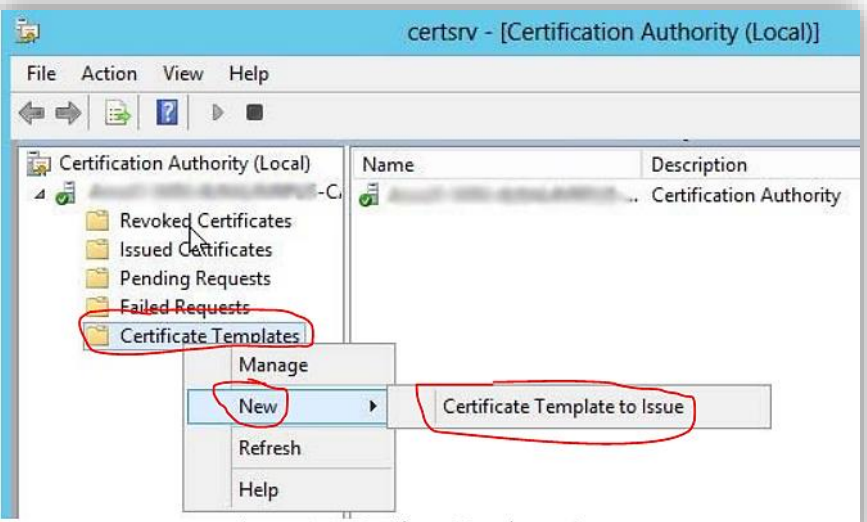
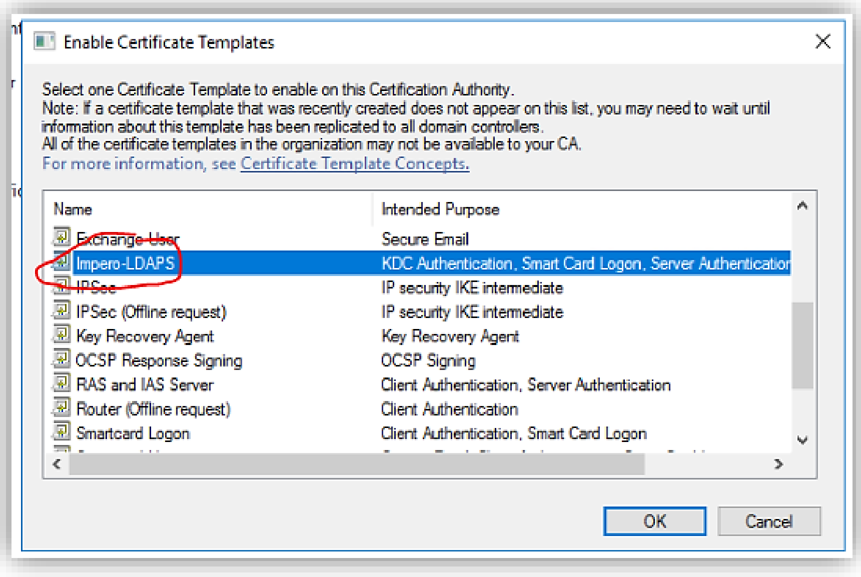


Image 2.4 - Certificate Template to Issue

21.The 'Enable Certificate Templates' window should open.

22.Select 'Impero-LDAPS' from the list (Image 2.5).



Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Exchange User	Secure Email
Impero-LDAPS	KDC Authentication, Smart Card Logon, Server Authenticatior
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon

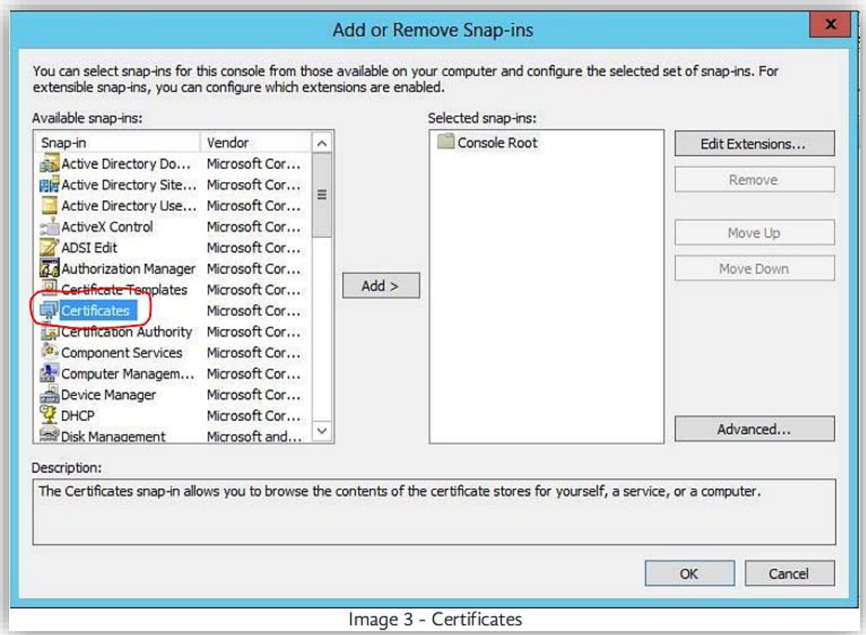
Impero 2.5 - Certificate Templates 1

23.Click 'OK'.

24.Close the 'Certsrv' window.

Request Certificate for Server Authentication

1. Open the 'Start' screen.
2. Search for 'MMC.exe' and click to open it.
3. Click on the 'File' menu in the top left.
4. Click 'Add/Remove Snap-in...'.
5. The 'Add or Remove Snap-ins' window should open.
6. Select 'Certificates' from the left pane (Image 3);



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Image 3 - Certificates

7. Click 'Add >'.
8. The 'Certificates snap-in' window should open.
9. Tick 'Computer account'.
10. Click 'Next'.
11. Click 'Next'.
12. Click 'OK'.
13. Expand 'Certificates (Local Computer)'.
14. Right-click 'Personal'.
15. Click 'All Tasks -> Request New Certificate...' (Image 3.1).

© 2019 Impero Solutions Ltd

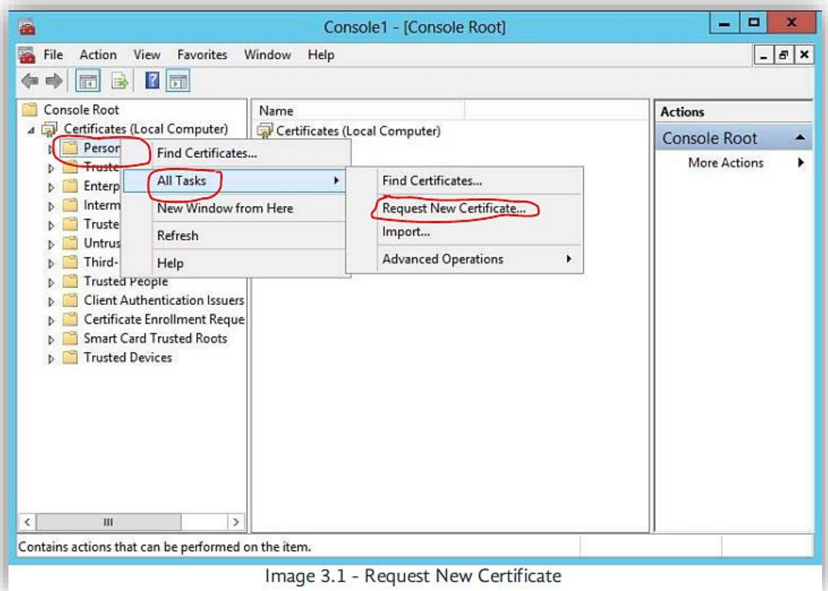
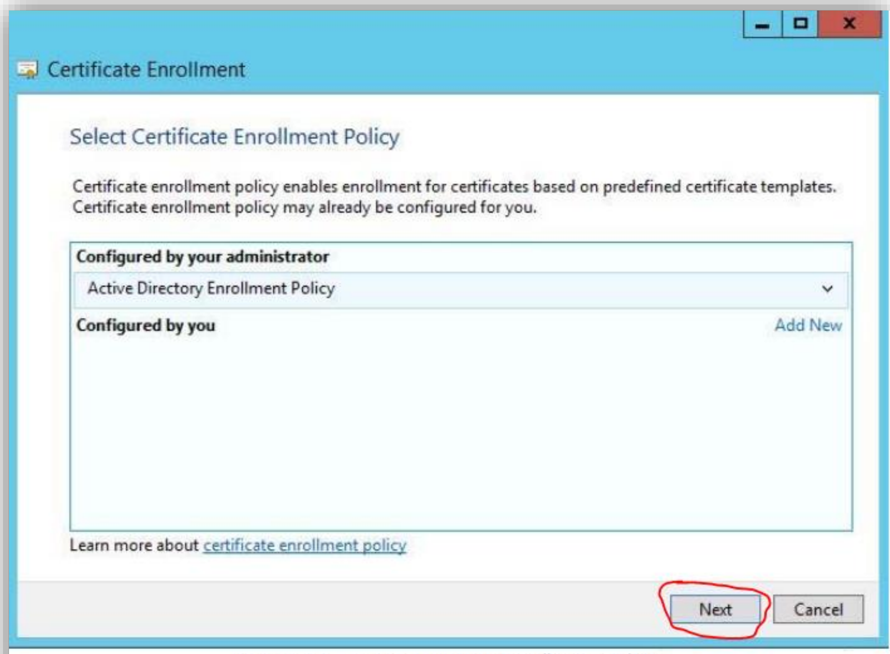

Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Person
Truste
Enterp
Interm
Truste
Untrus
Third-
Trusted People
Client Authentication Issuers
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Find Certificates...
All Tasks
New Window from Here
Refresh
Help
Find Certificates...
Request New Certificate...
Import...
Advanced Operations
Name
Certificates (Local Computer)
Actions
Console Root
More Actions
Contains actions that can be performed on the item.

Image 3.1 - Request New Certificate

16. The 'Certificate Enrollment' window should open.
17. Click 'Next'.
18. Confirm that the 'Active Directory Enrollment Policy' is selected (Image 3.2).


Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

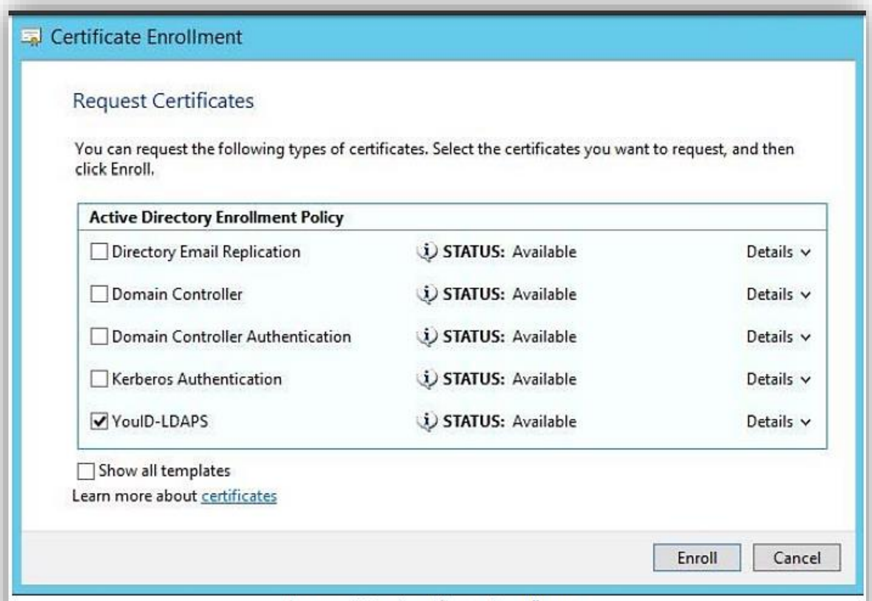
Configured by you

Learn more about certificate enrollment policy

Image 3.2 - Active Directory Enrollment Policy

19. Click 'Next'.
20. Tick 'Impero-LDAPS' (Image 3.3);

© 2019 Impero Solutions Ltd



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Directory Email Replication	**STATUS:** Available	Details
□ Domain Controller	**STATUS:** Available	Details
□ Domain Controller Authentication	**STATUS:** Available	Details
□ Kerberos Authentication	**STATUS:** Available	Details
☑ YouID-LDAPS	**STATUS:** Available	Details

□ Show all templates

Learn more about certificates

Image 3.3 - Certificate Enrollment

21.Click 'Enroll'.

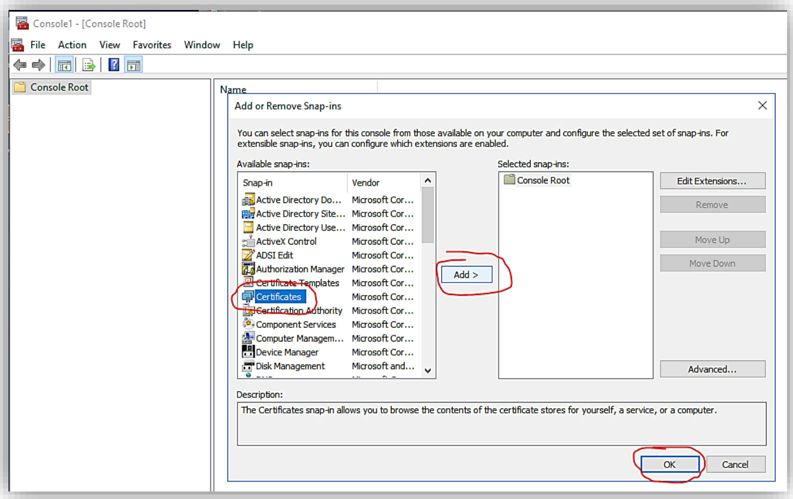
22.Wait for the enrolment to complete.

23.Click 'Finish'.

© 2019 Impero Solutions Ltd

Export Certificates for LDAPS

1. Open the 'Start' screen
2. Search for 'MMC.exe' and click to open it
3. Click on the 'File' menu in the top left
4. Click 'Add/Remove Snap-in...'
5. The 'Add or Remove Snap-ins' window should open
6. Select 'Certificates' from the left pane
7. Click 'Add >'



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

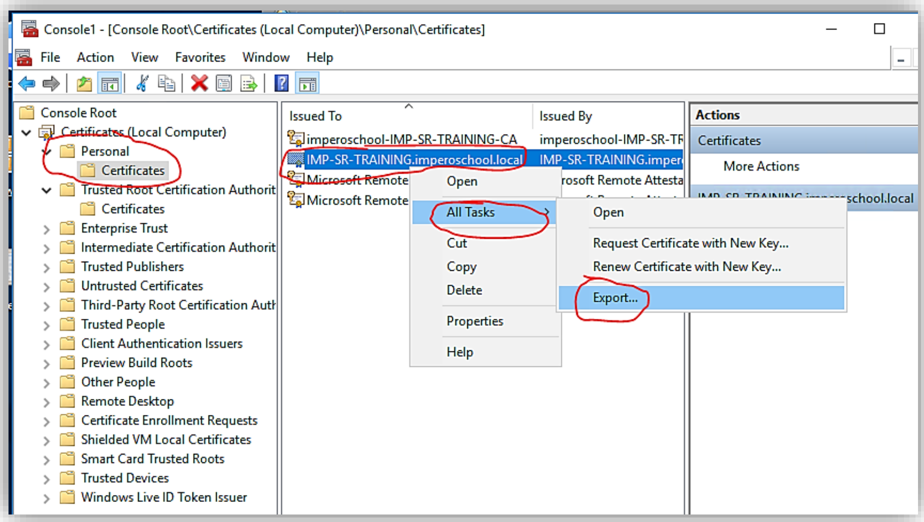
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

8. The 'Certificates snap-in' window should open
9. Tick 'Computer account'
10. Click 'Next'
11. Click 'Next'
12. Click 'OK'
13. Expand 'Certificates (Local Computer)'
14. Expand 'Personal'
15. Select 'Certificates' from the left-hand tree view
16. Locate the certificate with the FQDN of the Domain Controller under 'Issued To' and 'Impero-LDAPS' under 'Certificate Template'
17. Right-click on the certificate
18. Click 'All Tasks -> Export'

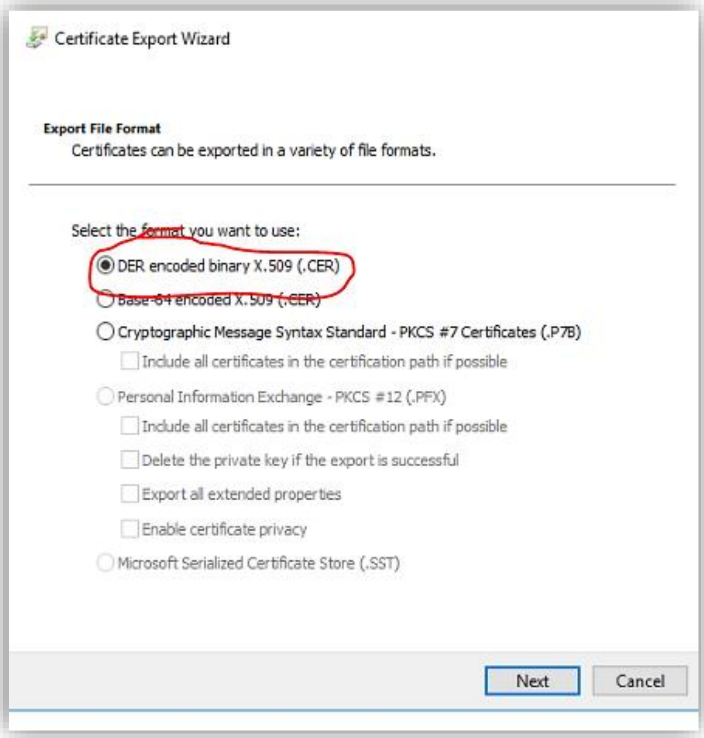

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorit
Certificates
Enterprise Trust
Intermediate Certification Authorit
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Auth
Trusted People
Client Authentication Issuers
Preview Build Roots
Other People
Remote Desktop
Certificate Enrollment Requests
Shielded VM Local Certificates
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
Issued To
Issued By
imperoschool-IMP-SR-TRAINING-CA
imperoschool-IMP-SR-TR
IMP-SR-TRAINING.imperoschool.local
IMP-SR-TRAINING.imper
Microsoft Remote
Microsoft Remote
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Export...
rosoft Remote Attesta
Actions
Certificates
More Actions
IMP-SR-TRAINING.imperoschool.local

19.The 'Certificate Export Wizard' should open

20.Click 'Next'

21.Click 'Next'

22.Confirm that 'DER encoded binary X.509(.CER)' is selected



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

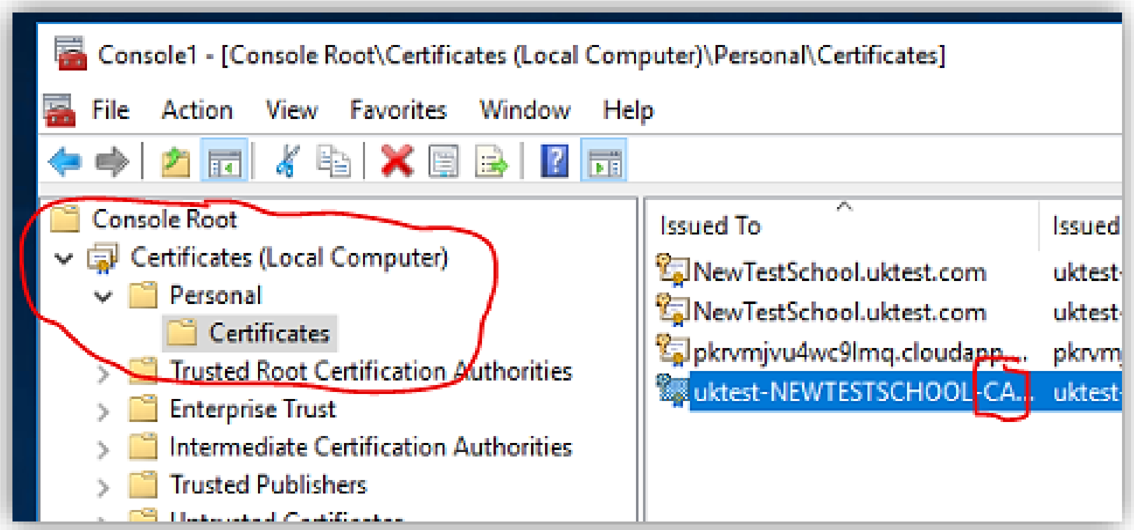
○ Microsoft Serialized Certificate Store (.SST)

23.Click 'Next'

24.Click 'Browse...'

25.Select a location to export the certificate to and enter the server name as the file name e.g. IMPDC01 on C:\Certs

26. Click 'Save'
27. Click 'Next'
28. Click 'Finish'
29. A window should appear confirming the export was successful
30. Click 'OK'
31. Within the MMC 'Certificates' view, locate the certificate with '-CA' at the end under 'Issued To'

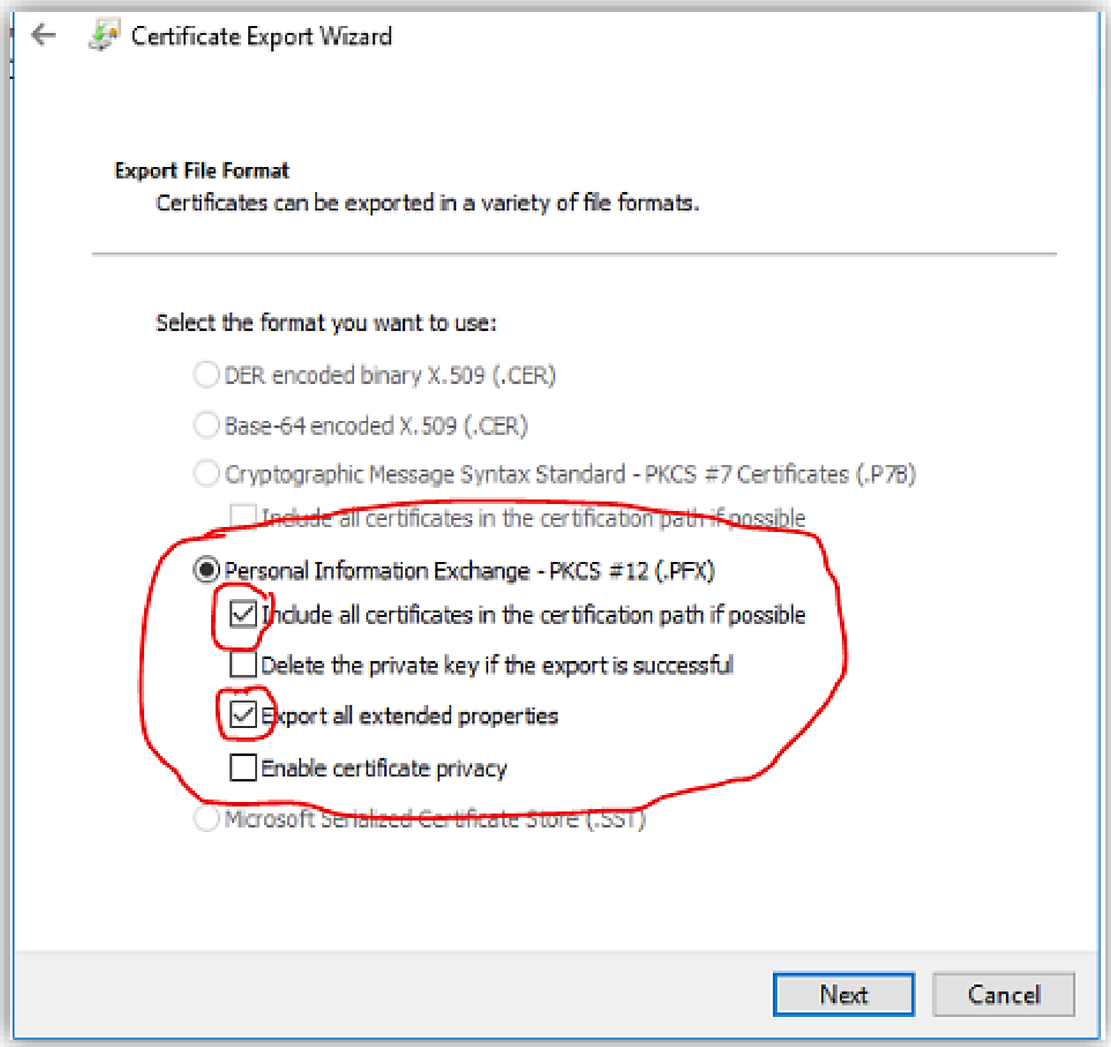


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued
NewTestSchool.uktest.com	uktest-
NewTestSchool.uktest.com	uktest-
pkrvmjvu4wc9lmq.cloudapp...	pkrvm
uktest-NEWTESTSCHOOL-CA...	uktest-

© 2019 Impero Solutions Ltd

32. Right-click on the certificate
33. Click 'All Tasks -> Export'
34. The 'Certificate Export Wizard' should open
35. Click 'Next'
36. Select 'Yes, export the private key'
37. Click 'Next'
38. Tick 'Export all extended properties' and 'Include all certificates in the certification path if possible'.



Certificate Export Wizard

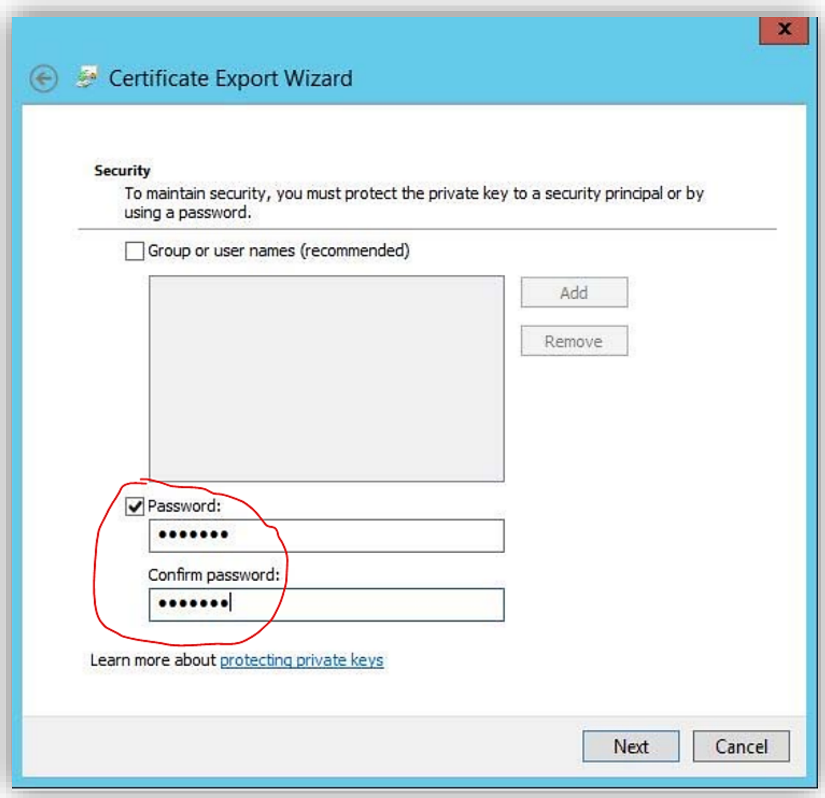
Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
  ☑ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  ☑ Export all extended properties
  □ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

39. Click 'Next'
40. Tick 'Password:
41. Enter a strong password **(Please take note of this as it will be required later);**



Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

☑ Password:
•••••••

Confirm password:
•••••••

Learn more about protecting private keys

42. Click 'Next'
43. Click 'Browse...'
44. Navigate to the same folder you saved the server certificate to
45. Enter the server name with '-CA' at the end as the file name e.g. IMPDC01-CA
46. Click 'Save'
47. Click 'Next'
48. Click 'Finish'
49. A window should appear confirming the export was successful
50. Click 'OK'
51. Close the 'MMC.exe' window

© 2019 Impero Solutions Ltd

Create User Account for authenticating with LDAPS

1. Open the 'Start' screen
2. Search for 'dsa.msc' and click to open it
3. 'Active Directory Users and Computer' should open
4. Navigate to the root Organisational Unit containing all of your users e.g. All Users

For example (You can create this user at the domain root level if you wish: Teaching Staff user accounts are located in a 'Teaching Staff' OU, which is a child of the 'All Users' OU

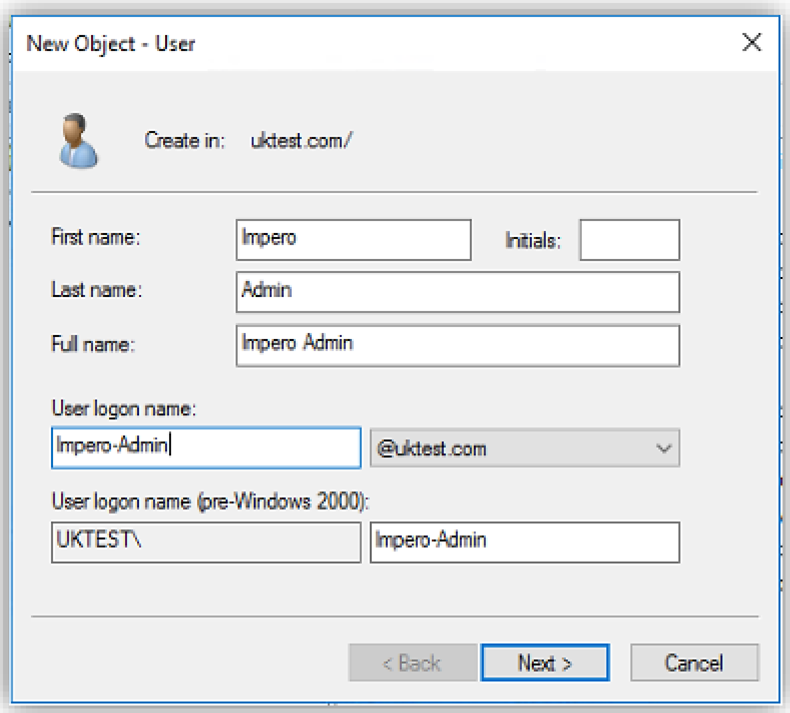
All Users -> Teaching Staff

Student user accounts are located in an OU related to their year group, which in turn is located within a 'Students' OU, which is a child of the 'All Users' OU

All Users -> Students -> Year 12

In this example, the 'All Users' OU would be identified as the root OU.

5. Right-click on the root OU identified above
6. Click 'New -> User'
7. The 'New Object' window should appear
8. In 'First name:' enter 'Impero'
9. In 'Last name:' enter 'Admin'
10. In 'User logon name:' enter 'Impero-Admin';



Create in: uktest.com/

First name: Impero

Initials:

Last name: Admin

Full name: Impero Admin

User logon name: Impero-Admin @uktest.com

User logon name (pre-Windows 2000): UKTEST\ Impero-Admin

11.Click 'Next'

12.Enter a strong password without any ASCII special characters Note : These are the ASCII special characters that should NOT be used when creating the Impero-Admin password;

, . / < > ? ; ' : " [ ] { } \ | ! @ # $ % ^ & * (- = _ +

This is due to incompatibility with specific services. Use uppercase characters, lowercase characters and numbers only.

13.Untick 'User must change password at next logon'

14.Tick 'User cannot change password'

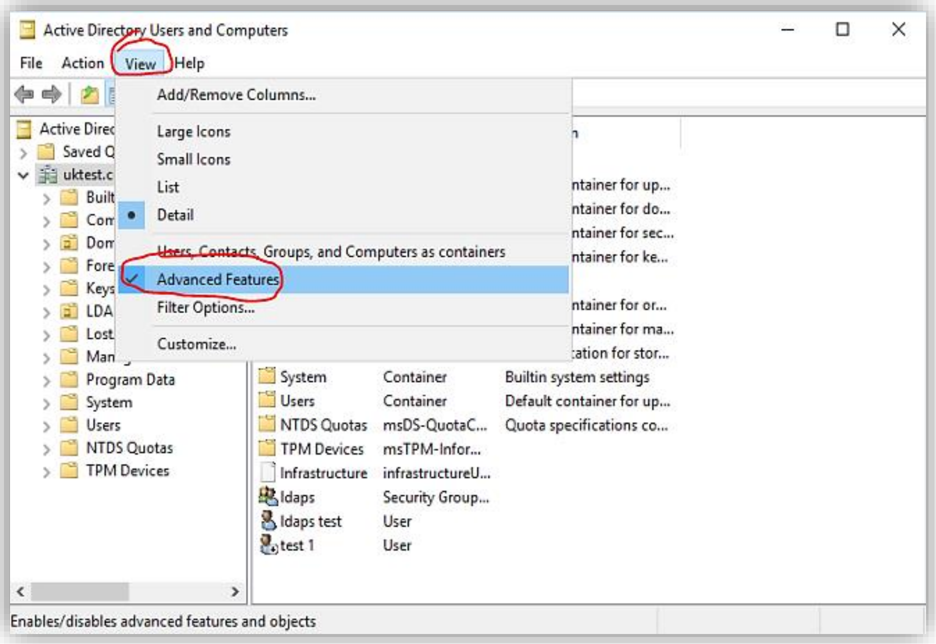
15.Click 'Next'

16.Click 'Finish'

17.Click on the 'View' menu within Active Directory Users and Computers

18.Click 'Advanced Features' to enable the option;

© 2019 Impero Solutions Ltd



Enables/disables advanced features and objects

19. Right-click the 'Impero-Admin' user
20. Click 'Properties'
21. In the 'Email:' field enter a unique email address e.g. imperoadmin@imperosoftware.com (This does not need to be a real account)
22. Click 'Apply'
23. Click on the 'Attribute Editor' tab
24. Click 'Filter'
25. Confirm that 'Show only attributes that have values' is ticked Impero-Admin
26. Take note of the following attribute values as these will be required later;

Attribute	Example
distinguishedName	CN=ldaps test,DC=uktest,DC=com
mail	ldapstest@imperosoftware.com
userPrincipalName	ldapstest@uktest.com

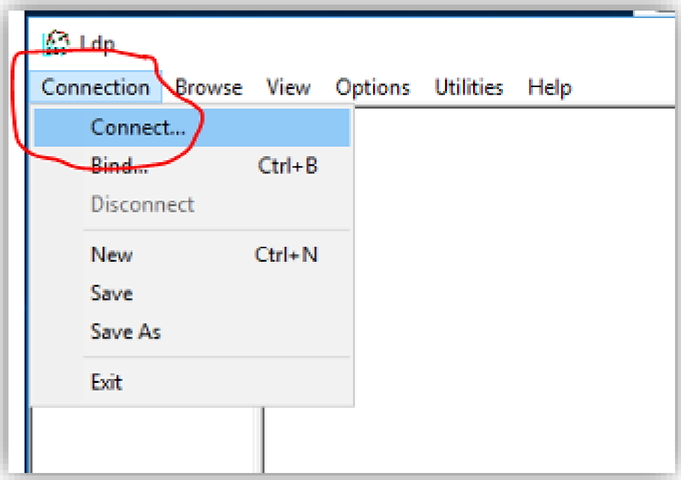
27. Click on the 'Member Of' tab
28. Click 'Add...'
29. In the 'Enter the object names to select' field type 'Domain Admins & Account Operators'
30. Click 'OK'
31. Click 'Apply

The user will now have Domain and Account Control privileges required for some features in Impero such as change password.

Verify local LDAPS connectivity

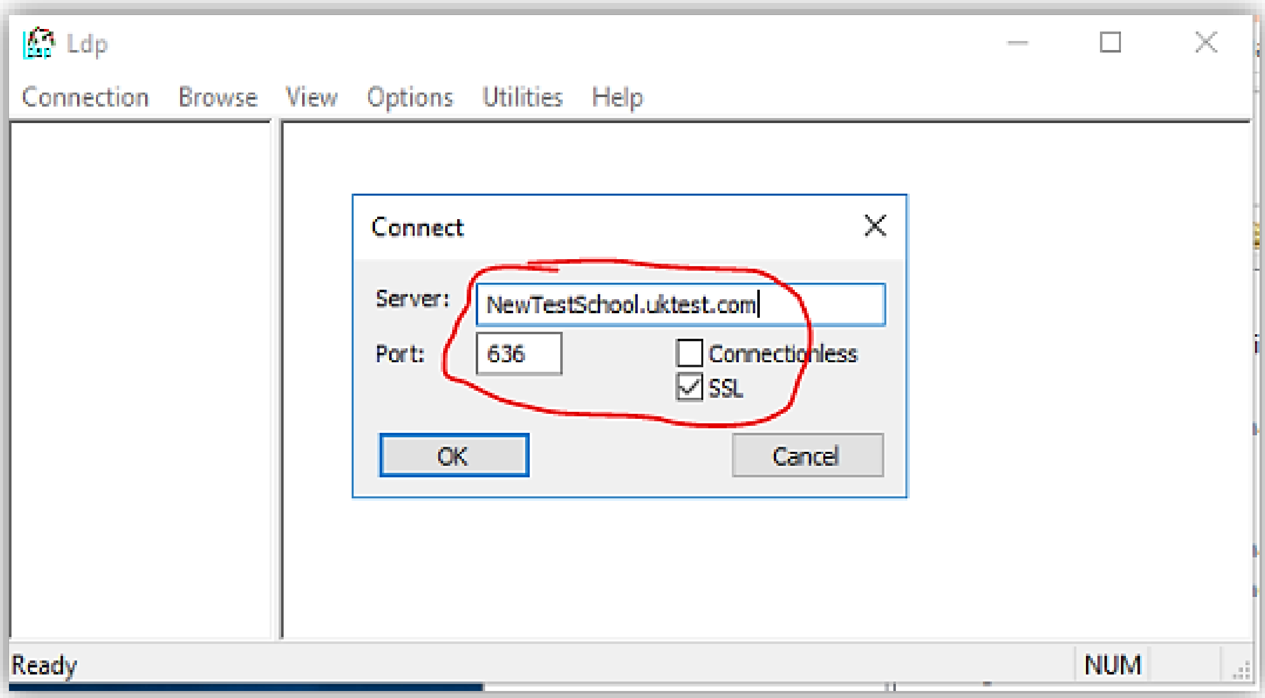
We need to verify that we can connect to the domain controller locally to make sure this is now all working correctly.

1. Open the 'Start' screen
2. Search for 'LDP.exe' and click to open it
3. Click on the 'Connection' menu in the top-left
4. Click 'Connect...'



5. Under 'Server:' type the FQDN of the Domain Controller e.g. IMPDC01.IMPEROSOFTWARE.COM
6. Under 'Port:' type '636'
7. Tick 'SSL'

© 2019 Impero Solutions Ltd



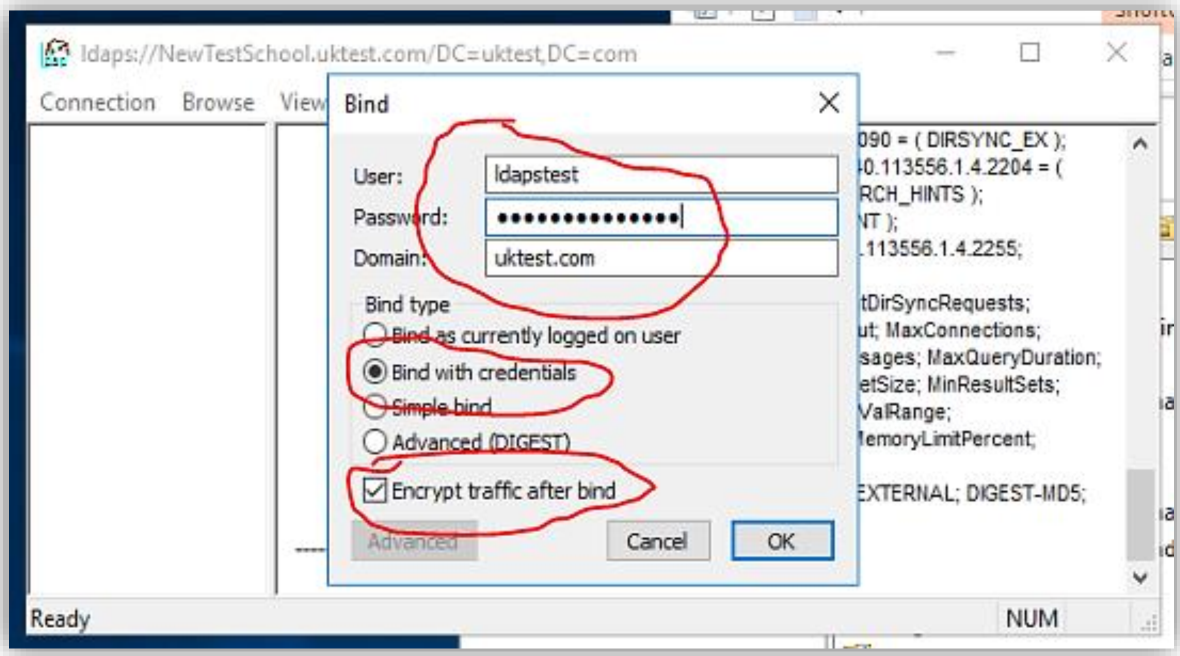
Server: NewTestSchool.uktest.com

Port: 636

□ Connectionless

☑ SSL

8. Click 'OK'
9. Click on the 'Connection' menu
10. Click 'Bind...'
11. Under 'Bind type' select 'Bind with credentials'
12. Under 'User:' enter 'Impero-Admin' (The user created earlier)
13. Under 'Password:' enter the strong password you assigned the user
14. Under 'Domain:' enter your full domain name e.g. imperosoftware.com;



ldaps://NewTestSchool.uktest.com/DC=uktest,DC=com

Bind

User: ldapstest

Password: •••••••••••••••

Domain: uktest.com

Bind type

○ Bind as currently logged on user

● Bind with credentials

○ Simple bind

○ Advanced (DIGEST)

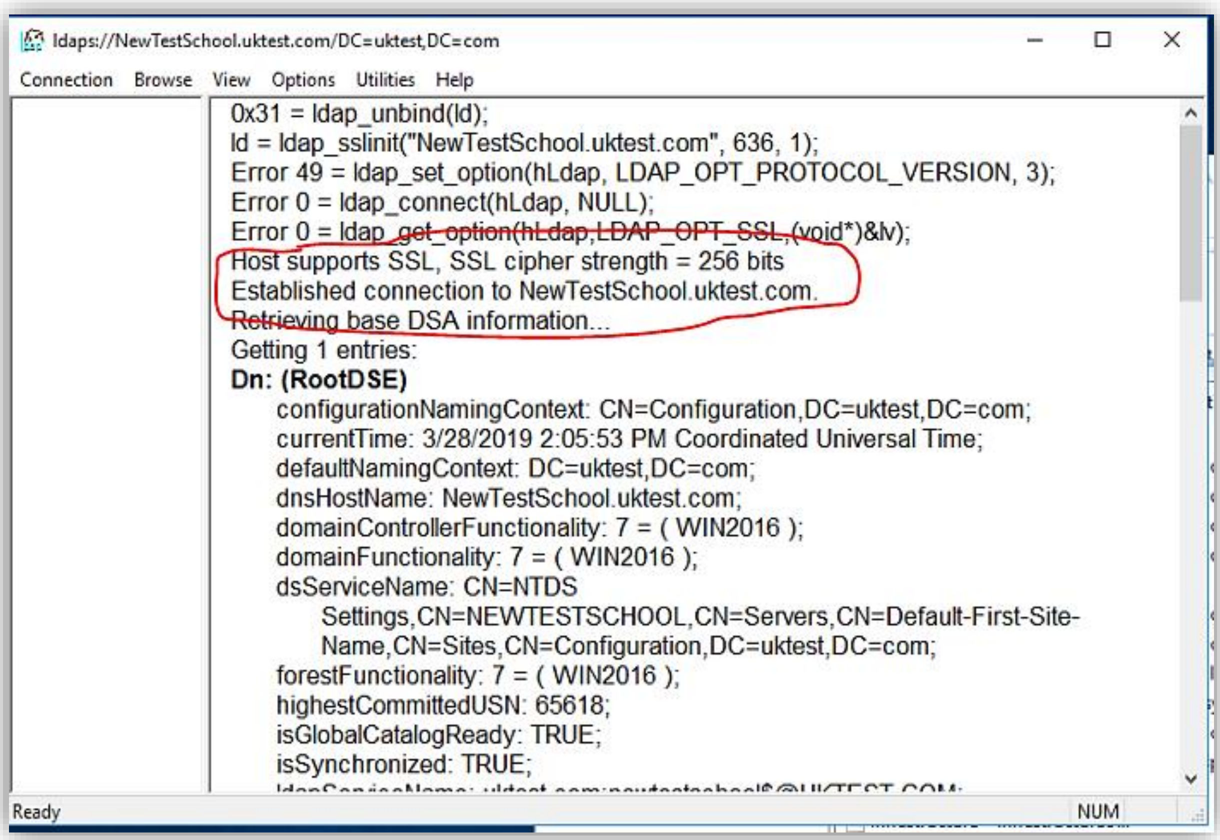
☑ Encrypt traffic after bind

```
090 = ( DIRSYNC_EX );
0.113556.1.4.2204 = (
RCH_HINTS );
NT );
.113556.1.4.2255;

tDirSyncRequests;
ut; MaxConnections;
sages; MaxQueryDuration;
etSize; MinResultSets;
ValRange;
lemoryLimitPercent;

EXTERNAL; DIGEST-MD5;
```

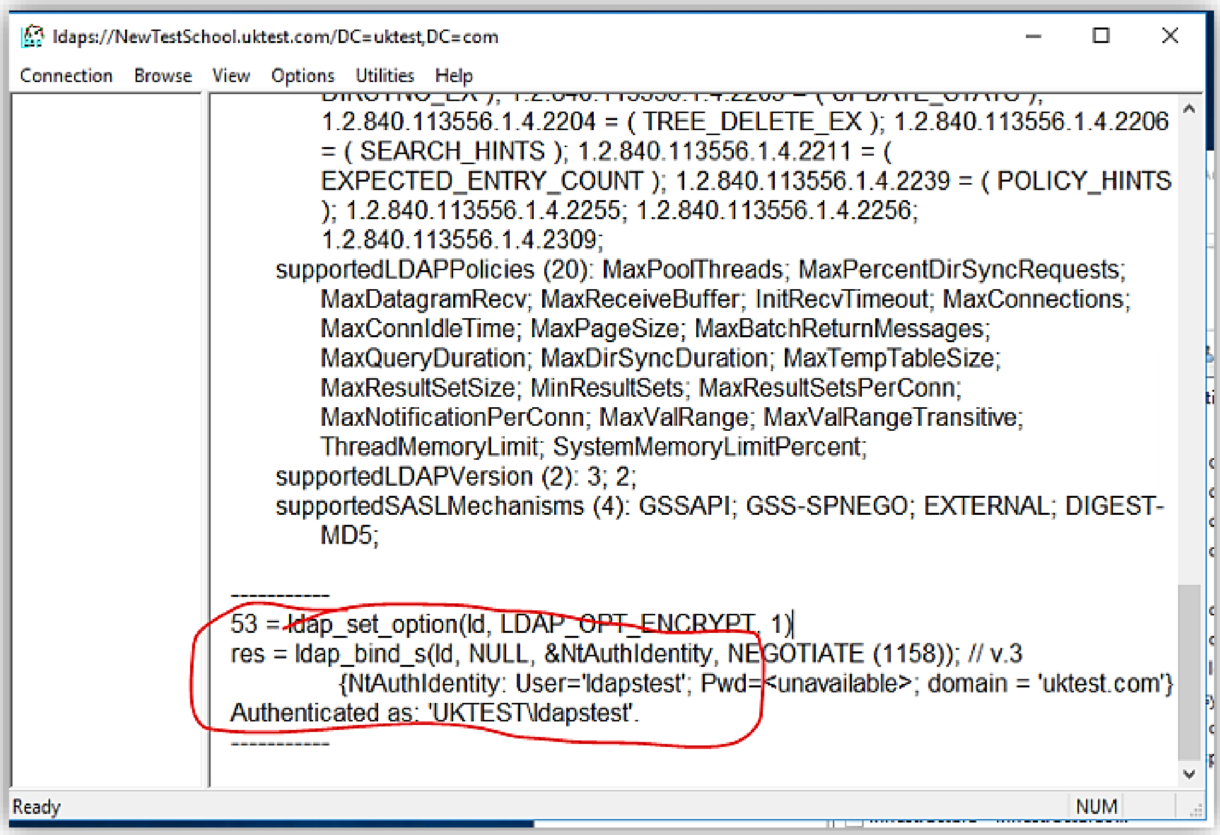
15.Click 'OK'

16.Observe the output in the ldp.exe tool

To confirm we can communicate via SSL and via the Authenticated User you should see the following lines highlighted;



```
0x31 = ldap_unbind(ld);
ld = ldap_sslinit("NewTestSchool.uktest.com", 636, 1);
Error 49 = 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 NewTestSchool.uktest.com.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
    configurationNamingContext: CN=Configuration,DC=uktest,DC=com;
    currentTime: 3/28/2019 2:05:53 PM Coordinated Universal Time;
    defaultNamingContext: DC=uktest,DC=com;
    dnsHostName: NewTestSchool.uktest.com;
    domainControllerFunctionality: 7 = ( WIN2016 );
    domainFunctionality: 7 = ( WIN2016 );
    dsServiceName: CN=NTDS
        Settings,CN=NEWTESTSCHOOL,CN=Servers,CN=Default-First-Site-
        Name,CN=Sites,CN=Configuration,DC=uktest,DC=com;
    forestFunctionality: 7 = ( WIN2016 );
    highestCommittedUSN: 65618;
    isGlobalCatalogReady: TRUE;
    isSynchronized: TRUE;
    ldapServiceName: uktest.com:newtestschool$@UKTEST.COM;
```


ldaps://NewTestSchool.uktest.com/DC=uktest,DC=com
Connection Browse View Options Utilities Help
Ready
NUM

```
          1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206
          = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = (
          EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS
          ); 1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256;
          1.2.840.113556.1.4.2309;
     supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests;
          MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections;
          MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages;
          MaxQueryDuration; MaxDirSyncDuration; MaxTempTableSize;
          MaxResultSetSize; MinResultSets; MaxResultSetsPerConn;
          MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive;
          ThreadMemoryLimit; SystemMemoryLimitPercent;
     supportedLDAPVersion (2): 3; 2;
     supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-
          MD5;

-----------
53 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
          {NtAuthIdentity: User='ldapstest'; Pwd=<unavailable>; domain = 'uktest.com'}
Authenticated as: 'UKTEST\ldapstest'.
-----------
```

Contact Impero

Now this is all setup and confirmed that we can communicate locally you need to contact Impero so they can do their side of the setup.

The following information will be needed, which advise to send in separate emails directly to the Agents email address who your dealing with, if you don't have these details you can call Impero support.

© 2019 Impero Solutions Ltd

If you prefer to not email the details below you could put all this in a shared location and share a Link such as Google Drive, OneDrive etc…

Email	Subject	Contents	Attachments
1	ImperoLdaps-YourSchoolName-S1	Your Domain Controllers Public IP Addresses'	None
2	ImperoLdaps-YourSchoolName-S2	Domain Controller CA Certificate Password (Page 15 of this guide)	Domain Controller server (.cer) certificate. Which Needs to be .zip to get around mail filters
3	ImperoLdaps-YourSchoolName-S3	Impero-Admin user details: distinguishedName mail userPrincipalName	Domain Controller CA (.pfx) certificate. Which Needs to be .zip to get around mail filters
4	ImperoLdaps-YourSchoolName-S3	ImperoAdmin user password	None

© 2019 Impero Solutions Ltd

info@imperosoftware.com

www.imperosoftware.co.uk

www.imperosoftware.com

+44 (0) 1509 611341 UK

877-883-4370 USA

© 2019 Impero Solutions Ltd