

# Configuring SSL on LDAP Server and Client

# 1. Index

1.	Index	1
1.1	. Map of revision	1
2.	Overview	2
3.	Configure LDAP server to have SSL enabled	2
3.1	. Install Active Directory Certificate Services	2
3.2	2. Export Certificate	3
3.3	Change policy password	10
4.	Configure LDAP client computer to connect using SSL	11
4.1	. Import LDAP Server Certificate	11
4.2	2. Edit Your Hosts File	16

# 1.1. Map of revision

Revision	Date Issued	Description	Author	Approval
А	1/9/2017	First version	Leandro Gioria	Gary Wyatt



## 2. Overview

The purpose of this document is to guide configure the LDAP Server to enable Active Directory Certificate Services (ADCS), exports the certificates and import on LDAP Client to have Secure Socket Layer (SSL) enabled to be able to connect using SSL and change the user's password being on same domain and different domains.

Lightweight Directory Access Protocol (LDAP) is used by InduSoft for managing users and groups across many different applications on a network. When this mode is selected, the project gets its users and groups from an LDAP-compliant domain server, such as Microsoft Active Directory for Windows or OpenLDAP for Linux.

### 3. Configure LDAP server to have SSL enabled

### 3.1. Install Active Directory Certificate Services

The certificate service is necessary to be able to connect the client to the server using Secure Socket Layer (SSL).

- 1. Log in to your Active Directory server as an administrator
- 2. Click Start, point to Administrative Tools, and then click Server Manager.
- 3. In the Roles Summary section, click Add Roles.
- 4. On the Select Server Roles page, select the Active Directory Certificate Services check box. Click Next twice.
- 5. On the **Select Server Roles** page, select the **Certification Authority** check box, and then click **Next**.
- 6. On the Specify Setup Type page, click Enterprise, and then click Next.
- 7. On the Specify CA Type page, click Root CA, and then click Next.
- 8. On the Set Up Private Key page, select create a new private key. Click Next.
- 9. On the **Set Up Private Key Cryptography** page, you can configure optional configuration settings. However, the default values should be fine. Click **Next**.
- 10. On the Set Up Private Key CA name page, in the Common name for this CA box, type the common name of the CA, and then click Next.
- 11. On the **Set Up Private Key Validity Period** page, you can set the validity period for the certificate generate for this CA, and then click **Next**.
- 12. On the **Set Up Certificate Period** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click **Next**.



- 13. After verifying the information on the Confirm Installation Selections page, click Install.
- 14. Review the information on the results screen to verify that the installation was successful.
- 15. Start > Run > **gpupdate** /**Force**

### 3.2. Export Certificate

You need to export the certificates files from LDAP Server to import on LDAP client to be able to connect using Secure Socket Layer (SSL).

#### Note: If LDAP server and client are on same domain this step is not necessary.

- 1. Click on the Start menu and click Run.
- 2. Type in **mmc** and click **OK**.



3. Click on the File menu and click Add/Remove Snap-in...

👼 Console1 - [Console Root]		
File Action View Favorites Window	Help	_ 8 ×
New Ctrl+N		
Open Ctrl+O		Actions
Save Curts	There are no items to show in this view.	Console Root
Add/Remove Snap-in Ctrl+M		More Actions
Options	-	
1 C:\Windows\\servermanager	_	
Exit		
Enables you to add spaping to or remove them from	the shan in console	
induces you to dod shap its to or remove them from	are shap in consoler	



4. If you are using Windows Server 2003, click on Add button. Double-Click on Certificates.

crosoft Cor crosoft Cor crosoft Cor			Remove
crosoft Cor crosoft Cor			Remove
crosoft Cor			
rosoft Cor		1	
absorccom			Movello
rosoft Cor —	J		
crosoft Cor	1		Move Down
crosoft and	Add >		
crosoft Cor			
crosoft Cor			
crosoft Cor			
crosoft Cor			
crosoft Cor			a discount of the
rosoft Cor 🗵		J	Advanced
	rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor	rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor	rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor rosoft Cor

5. Click on **Computer Account** and click **Next**.

Certificates snap-in			×
This snap-in will always manage certificates for:			
O My user account			
C Service account			
Computer account			
	< Back	Next >	Cancel

# Configuring SSL on LDAP Server and Client

# ©Copyright InduSoft Systems LLC. 2017



6. Leave Local Computer selected and click Finish.

ect Computer	
Select the computer you want this snap	Hin to manage.
This snap in will always manage:	
Local computer: (the computer till)	his console is running on)
C Another computer:	Browse,
Allow the selected computer to b	be changed when launching from the command line. This
only applies if you save the cons	
	< Back Finish Cancel
	Codicer Finish

7. If you are using Windows Server 2003, click the **Close** button. Click **OK**.

ActiveX Control       Microsoft Cor         Authorization Manager       Microsoft Cor         Authorization Manager       Microsoft Cor         Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Manager       Microsoft Cor         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         Internet Information       Microsoft Cor         IP Security Monitor       Microsoft Cor         Internet Information       Microsoft Cor		vendor	<b>A</b>	Console Root	Edit Extensions
Authorization Manager       Microsoft Cor         Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Manager       Microsoft Cor         Device Manager       Microsoft Cor         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         Internet Information       Internet Information         IP Security Policy Mai       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	ActiveX Control	Microsoft Cor		Certificates (Local Computer)	
Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Managem       Microsoft Cor         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       IP Security Monitor         Microsoft Cor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Authorization Manager	Microsoft Cor			Remove
Component Services       Microsoft Cor         Computer Managem       Microsoft Cor         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       IP Security Monitor         Microsoft Cor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Certificates	Microsoft Cor			
Computer Managem       Microsoft Cor         Device Manager       Microsoft Cor         Disk Management       Microsoft and         Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       IP Security Monitor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Component Services	Microsoft Cor			Move Up
Device Manager       Microsoft Cor         Disk Management       Microsoft and         Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Computer Managem	Microsoft Cor			
Disk Management       Microsoft and       Add >         Event Viewer       Microsoft Cor       Folder         Folder       Microsoft Cor       Folder         Group Policy Object       Microsoft Cor       Folder         Internet Information       Microsoft Cor       Add >         IP Security Monitor       Microsoft Cor       Add >         IP Security Policy Ma       Microsoft Cor       Advanced         Link to Web Address       Microsoft Cor       Advanced	Device Manager	Microsoft Cor			Move Down
Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Internet Information       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Disk Management	Microsoft and	Add >		
Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         Internet Information       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Event Viewer	Microsoft Cor			
Group Policy Object Microsoft Cor  Thernet Information  D IP Security Monitor Microsoft Cor  D IP Security Policy Ma Microsoft Cor  Link to Web Address Microsoft Cor  Advanced	Folder	Microsoft Cor			
Internet Information IP Security Monitor Microsoft Cor IP Security Policy Ma Microsoft Cor Link to Web Address Microsoft Cor Advanced	Group Policy Object	Microsoft Cor			
IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Link to Web Address       Microsoft Cor	Internet Information				
IP Security Policy Ma Microsoft Cor     Advanced	IP Security Monitor	Microsoft Cor			
Link to Web Address Microsoft Cor	IP Security Policy Ma	Microsoft Cor			Advanced
	Link to Web Address	Microsoft Cor	<u> </u>	1	



8. Click the plus sign next to **Certificates** in the left pane.



- 9. Click the plus sign next to the **Trusted Root Certification Authorities** folder and click on the Certificates folder.
- 10. For **Each** certificate with the domain-machine name Right-click on the certificate with domainmachine name and select **All Tasks** and then **Export...**

🧱 Console1 - [Console Root\Certificates - Current L	Jser\Trusted Root Certification Autho	orities\Certificates]	
🚘 File Action View Favorites Window Help			
🗢 🔿 🖄 📰 📋 🙆 🗟 📘			
Console Root	Issued To 🔺	Issued By	Expiration Date
<ul> <li>Certificates - Current User</li> <li>Personal</li> <li>Trusted Root Certification Authorities</li> <li>Certificates</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification Authorities</li> <li>Trusted People</li> <li>Smart Card Trusted Roots</li> </ul>	Peter of Cyte Tristeness  Clast 2 Public Primary Coll Reads  Clast 2 Public Primary Coll Reads  Conversition 1927 Microsoft Corp.  Peter Reads  Pet	<ul> <li>T. Stora, - C. Skir Taint Bont</li> <li>Clerk B Public Privativ Costification A</li> <li>Convergiti (c) 1995 Second Costification A</li> <li>C growt Cub. Temporale EV Poet CA</li> <li>Equitar Secure Carolitate Authority</li> <li>Second Ghoel CA</li> <li>EvoTrast Primery Carolitate Authority</li> <li>GobelSign Road CA</li> <li>Statust Road Automatic</li> <li>Record Cost Road (co) Next Automatic</li> <li>GobelSign Road CA</li> <li>Statust Road Automatic</li> <li>Statust Road Automatic</li></ul>	5/12/2025 8/1/2028 12/30/1999 11/9/2031 8/22/2018 5/20/2022 7/16/2036 1/28/2028 8/13/2018 12/31/2020 5/9/2021 1/7/2004 10/7/2021 10/7/2021 10/7/2021 10/7/2021 12/31/2020 7/16/2036 1/29/2022



11. In the Certificate Export Wizard click **Next**.

Certificate Export Wizard	and the second	×
	Welcome to the Certificate Export Wizard           This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.           A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where	
	certificates are kept.	
	< Back Next > Cancel	

12. Choose "No, do not export the private key" and click Next.

tificate Export Wizard	
Export Private Key	with the certificate
Tou can choose to export the private key	with the certificate.
Private keys are password protected. If y certificate, you must type a password on	rou want to export the private key with the a later page.
Do you want to export the private key wil	th the certificate?
O Yes, export the private key	
No, do not export the private key	,
, , , , , , , . , . , . , . , . , . , . , . , . , . , . , . , . , . , . , . , . , . ,	
Learn more about <u>exporting private keys</u>	
	< Back Next > Cancel

# Configuring SSL on LDAP Server and Client

# ©Copyright InduSoft Systems LLC. 2017



13. Select **DER encoded binary X.509(.CER)** and click **Next**.

Export Fil Certifi	e Format icates can be exported in a variety of file formats.
Select	the format you want to use:
•	DER encoded binary X.509 (.CER)
C	Base-64 encoded X.509 (.CER)
C	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
C	Personal Information Exchange - PKC5 #12 (.PFX)  Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
C	) Microsoft Serialized Certificate Store (.SST)
.earn more	about <u>certificate file formats</u>
	< Back Next > Cancel



14. Click **Browse** and find a location to save the .cer file to. Type in a name such as "mydomain.cer" and then click **Next**.

tificate Export Wizard				×
File to Export Specify the name of the file you want to e	export			Jed By Drave Cylor Town Mark
File name:		Bro	wse	<ul> <li>Support of the American Street Street</li></ul>
Save As			- <b>7</b>	-h Dadhar
Eile name: mydomain.cer				
Save as type: DER Encoded B	inary X.509 (*.ce	r)		
Browse Folders				Save Cancel
				-D. B. CT WE CALCE -D. B. CT WE CALC -D. B. CN WE CALC -D. B. CALVER -D. B. CALVER -D. B. CALVER -D. B. CALVER -D. B. COMMANNER -D. S. C.
	< Back	Next >	Cancel	Who Time the rains CA ISIN Leads & Caller Preserved



15. Click Finish. The .cer file containing the certificate is now saved to the location you specified.

Certificate Export Wizard		×
	Completing the Certificate Export Wizard         You have successfully completed the Certificate Export wizard.         You have specified the following settings:         You have specified the following settings:         File Name       C:\Use         Export Keys       No         Include all certificates in the certification path       No         File Format       DER En	
	< Back Finish Cancel	

- 16. Repeat steps 10-15 For **Each** certificate with the domain-machine name.
- 17. Copy the .cer files saved to the location you specified to LDAP client's machine.

#### 3.3. Change policy password

You can change the policy password as you prefer. The security setting **Minimum password age** is an important attribute because this determines the period of time (in days) that a password must be used before the user can change it. This attribute is very important to test the functionality of change password because the default value is 1 this means that you can change the password once a day.

- 1. Start > Run > **gpmc.msc**
- 2. Domains > Domain > Group Policy Objects > Default Domain Policy > Edit
- Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
- 4. You will see the password policies.

- 5. Double click on one of them and change to your need.
- 6. You may need to run gpupdate for a fast group policy update
- 7. Start > Run > **gpupdate** /**Force**

### 4. Configure LDAP client computer to connect using SSL

### 4.1. Import LDAP Server Certificate

If LDAP server and client are on different domain you need to import the certificates files from LDAP server (see "3.2 Export Certificate") to connect client to server using Secure Socket Layer (SSL).

#### Note: If LDAP server and client are on same domain this step is not necessary.

- 1. Click on the Start menu and click Run.
- 2. Type in mmc and click OK.

🖅 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	mmc	
	🕐 This task will be created with administrative privileges.	
	OK Cancel Browse	





3. Click on the File menu and click Add/Remove Snap-in...

	Ctrl+N				
	Ctrl+0				Actions
	Ctrl+S	There are no	items to show in this view.		Console Root
o-in	Ctrl+M				More Actions
servermanage	r				
	p-in	p-in Ctrl+M \servermanager	yervermanager	There are no items to show in this view.	p+n       Ctrl+M         \servermanager

4. If you are using Windows Server 2003, click on Add button. Double-Click on Certificates.

p-in	Vendor		Console Root	Edit Extensions
ActiveX Control Authorization Manager	Microsoft Cor Microsoft Cor			Remove
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			Move Up
Device Manager	Microsoft Cor			Move Down
Disk Management	Microsoft and	Add >		
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object Internet Information	Microsoft Cor			
P Security Monitor	Microsoft Cor			
P Security Policy Ma	Microsoft Cor			the second se
ink to Web Address	Microsoft Cor	<b>_</b>		Advanced
intion:				
intion:				



5. Click on **Computer Account** and click **Next**.

Certificates snap-in			×
This snap-in will always manage certificates for: My user account Service account Computer account			
	< Back	Next >	Cancel

6. Leave Local Computer selected and click Finish.

Select Computer		×
Select the computer you want This snap-in will always man	t this snap-in to manage. hage:	]
C Another computer:	Browse	
Allow the selected com only applies if you save	uputer to be changed when launching from the command line. This e the console.	
-		
	< Back Finish Cancel	



7. If you are using Windows Server 2003, click the **Close** button. Click **OK**.

nap-in	Vendor			Console Root		Edit Extensions
ActiveX Control	Microsoft Cor			Gertificates (	Local Computer)	
Authorization Manager	Microsoft Cor					Remove
Certificates	Microsoft Cor					
Component Services	Microsoft Cor					Move Up
Computer Managem	Microsoft Cor					
Device Manager	Microsoft Cor	Г				Move Down
Disk Management	Microsoft and		Add >			
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
Internet Information						
IP Security Monitor	Microsoft Cor					
IP Security Policy Ma	Microsoft Cor					Advanced
Link to Web Address	Microsoft Cor	-				Auvanceu
cription:						
alpaon						

8. Right-click on the **Trusted Root Certification Authorities** folder and select **All Tasks** and then **Import...** 

🚟 Console1 - [Console Root\Certificates (Lo	ocal Computer)\Trusted Ro	ot Certification Authorit
🚟 File Action View Favorites Window	Help	
🗢 🔿 🖄 🖬 📋 🔍 🗟 🚺		
<ul> <li>Console Root</li> <li>Certificates (Local Computer)</li> <li>Personal</li> <li>Trusted Root Certification Authorities</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification Authori</li> <li>Trusted People</li> <li>Remote Desktop</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> <li>Trusted Devices</li> </ul>	Object Type         Certificates         Find Certificates         All Tasks         View         New Window from Here         New Taskpad View         Refresh         Export List	Find Certificates Import
	Help	

9. In the Certificate Import Wizard click Next.



ertificate Import Wizard	X
	Welcome to the Certificate Import Wizard         This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.         A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.         To continue, click Next.
	< Back Next > Cancel

- 10. Click the **Browse** button and find the .cer file that you copied over and click **Open** and then **Next**.
- 11. Click "Place all certificates in the following store" and click Next.

ertificate Import Wizard		×
Certificate Store		
Certificate stores are system areas where	e certificates are kept.	
Windows can automatically select a certifi the certificate.	cate store, or you can spe	ecify a location for
C Automatically select the certificate	store based on the type o	of certificate
Place all certificates in the following	; store	
Certificate store:		
Trusted Root Certification Author	ities	Browse
Learn more about <u>certificate stores</u>		
	< Back Nev	t Cancel
	- DOCK NOX	



- 12. Click **Finish** to complete the wizard.
- 13. Repeat steps 8-12 for each of the certificates copied from the server.
- 14. You can now click the **Refresh** button in the toolbar to refresh and find your certificate in the Certificates folder under Trusted Root Certification Authorities.
- 15. Close the MMC console. You do not need to save any changes.

### 4.2. Edit Your Hosts File

You can't use IP address to connect client to server using Secure Socket Layer (SSL), you must use machine's name of LDAP server because the certificate exported from LDAP server is based on server's name.

#### Windows:

- 1. Click on the Start menu and click **Run.**
- 2. Type in notepad c:\Windows\system32\drivers\etc\hosts and press ctrl+shift+enter.



3. Once notepad is open you can edit the file and redirect LDAP Server IP.

# Configuring SSL on LDAP Server and Client



## ©Copyright InduSoft Systems LLC. 2017

	hosts
File Edit Format View Help	
#For NC, no new entry above, between this and next comments	
#end of NC entry	
# copyright (c) 1993-2009 microsoft corp.	
] #	
# this is a sample hosts file used by microsoft tcp/ip for windows.	
#	
# this file contains the mappings of ip addresses to host names. each	
# entry should be kept on an individual line. the ip address should	
# be placed in the first column followed by the corresponding host nam	e.
# the ip address and the host name should be separated by at least on	e
# space.	
#	
# additionally, comments (such as these) may be inserted on individual	
# lines or following the machine name denoted by a #' symbol.	
#	
# for example:	
#	
# 102.54.94.97 rhino.acme.com # source server	
# 38.25.63.10 x.acme.com # x client host	

4. Make sure to **save** it.

#### Linux:

- 1. Open the **terminal**.
- 2. Type in sudo vim /etc/hosts





3. Now that it is open we can edit it to redirect LDAP Server IP.

😣 🛇 🔕 🖉	@ubuntu: ~
File Edit View	Terminal Help
127.0.0.1	localhost
127.0.1.1	ubuntu <- For exemple

4. Make sure to **save** it.

## 5. Appendix

If you encounter the error: Error to connect LDAP server (ldap\_connect) (0x51)

- 1. Confirm network settings by trying connecting without using SSL.
- 2. Verify you have imported all of the certificates from the server. See Section 3.2, steps 10-15 and section 4.1, steps 8-12.