# 1. Index



## 1.1. Map of revision

| Revision | Date Issued | Description | Author | Approval |
|---|---|---|---|---|
| A | 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**.

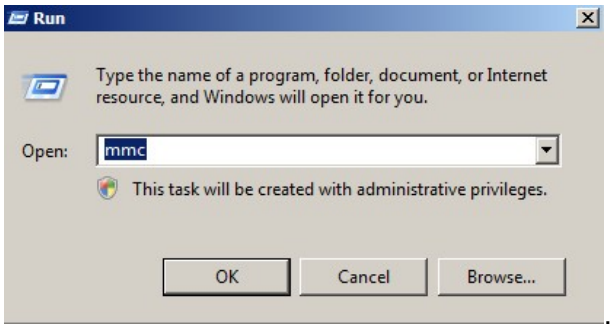
13. After verifying the information on the **Confirm Installation Selections** page, click **Install**.
14. Review the information on the results screen to verify that the installation was successful.
15. Start > Run > **gpupdate /Force**

## 3.2. Export Certificate

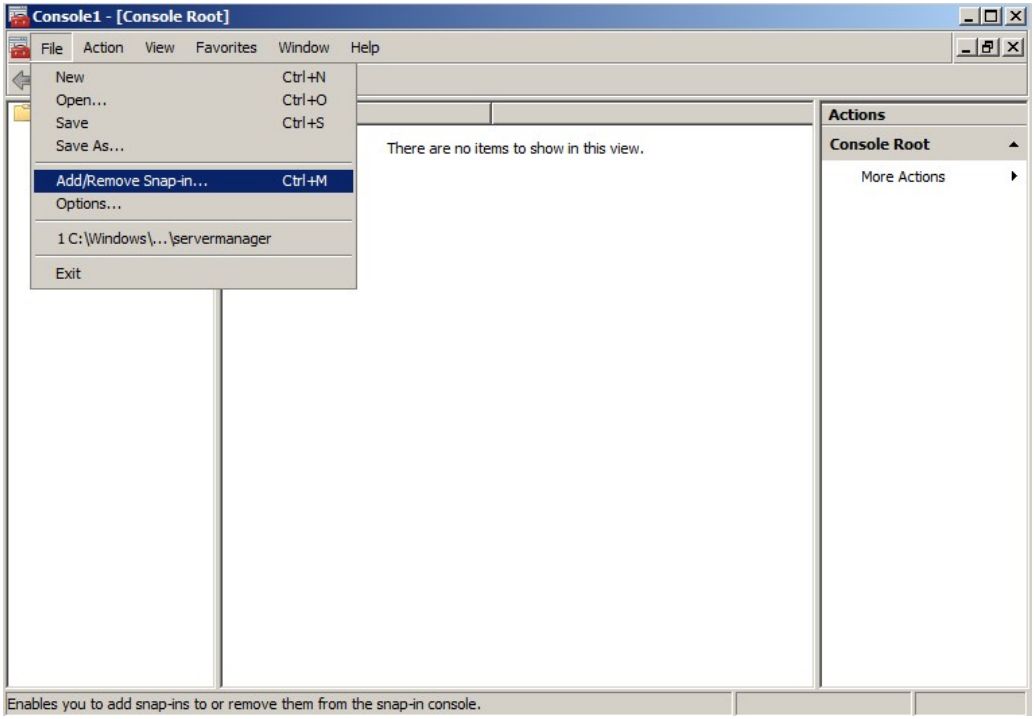
You need to export the certificates files from LDAP Server to import on LDAP client to be able to connect using Secure Socket Layer (SSL).

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

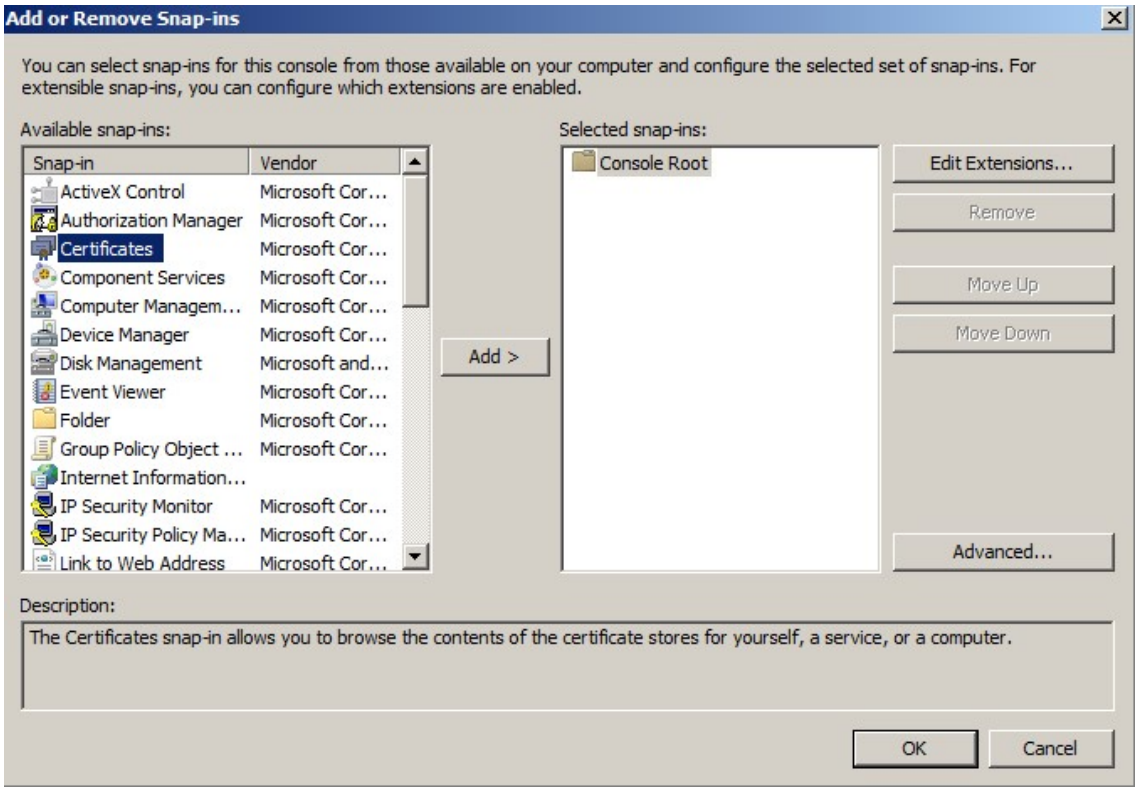
1. Click on the Start menu and click **Run.**
2. Type in **mmc** and click **OK.**



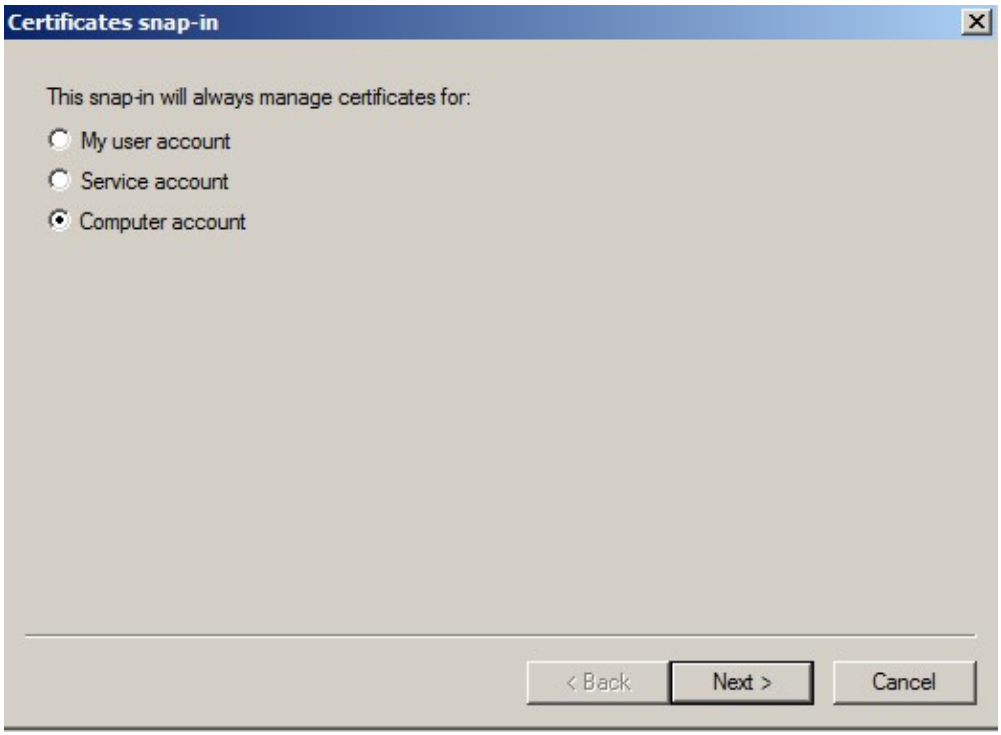

3. Click on the **File** menu and click **Add/Remove Snap-in…**



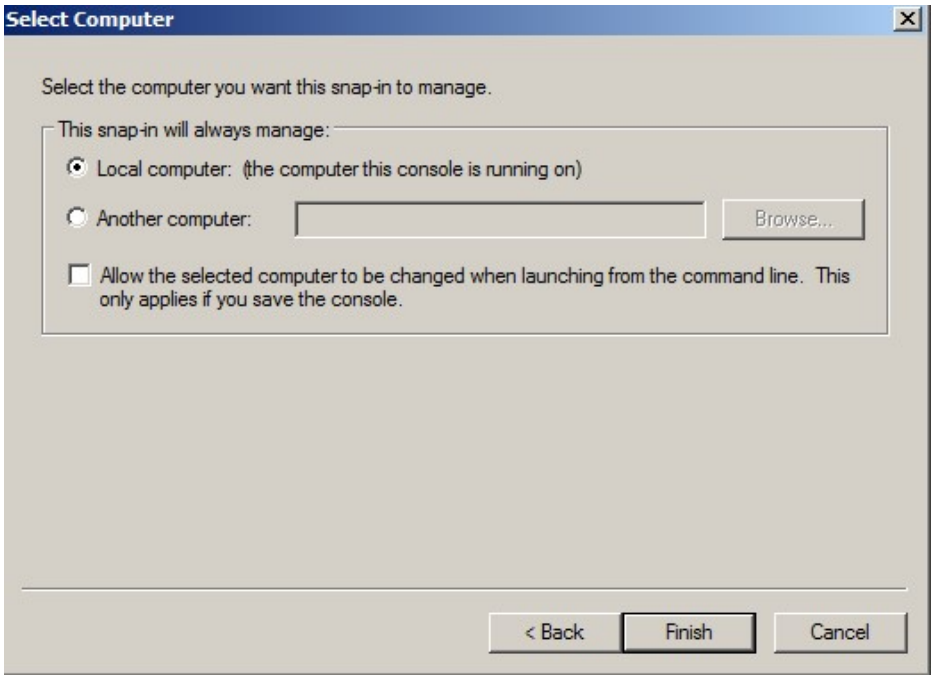
4. If you are using Windows Server 2003, click on **Add** button. Double-Click on **Certificates**.



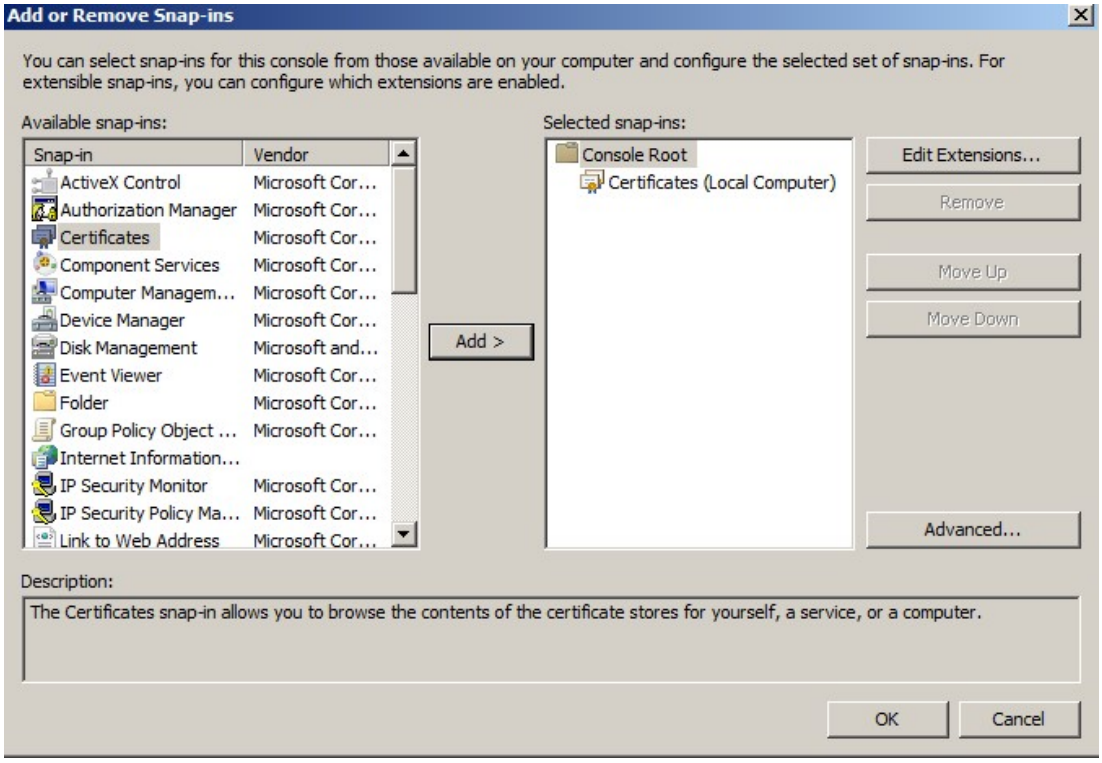

5. Click on **Computer Account** and click **Next**.



6. Leave **Local Computer** selected and click **Finish**.



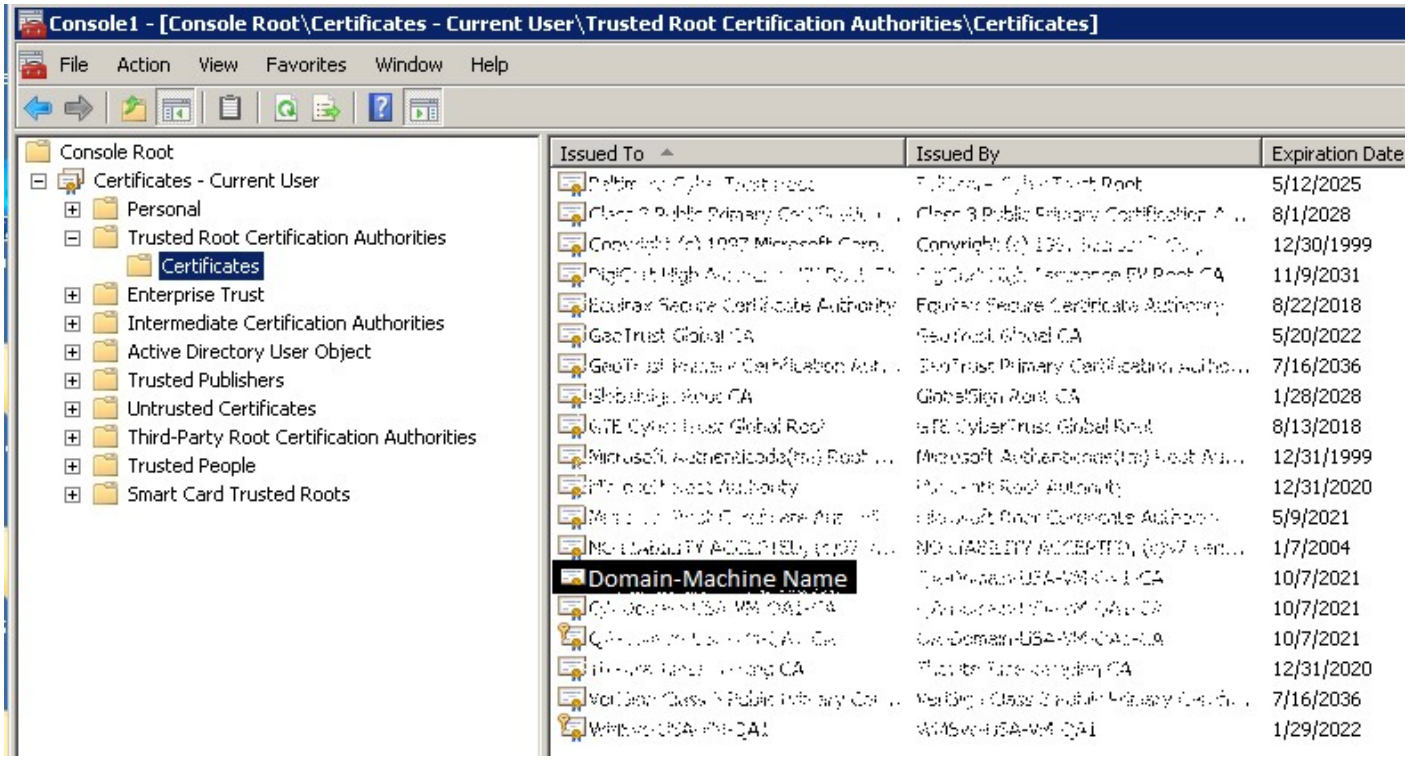

7. If you are using Windows Server 2003, click the **Close** button. Click **OK**.



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

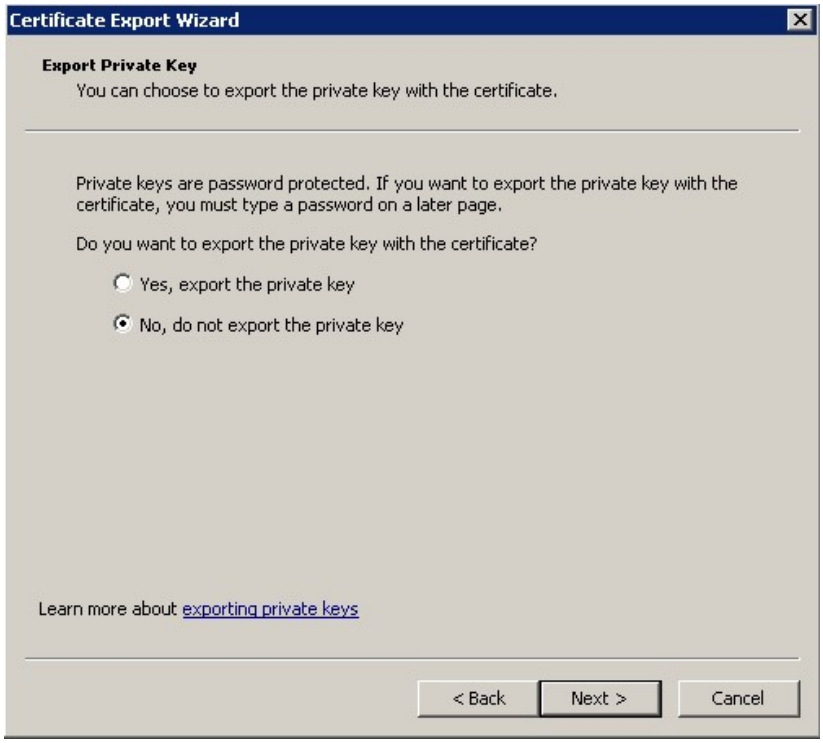

9. Click the plus sign next to the **Trusted Root Certification Authorities** folder and click on the Certificates folder.

10. For **Each** certificate with the domain-machine name Right-click on the certificate with domain-machine name and select **All Tasks** and then **Export...**

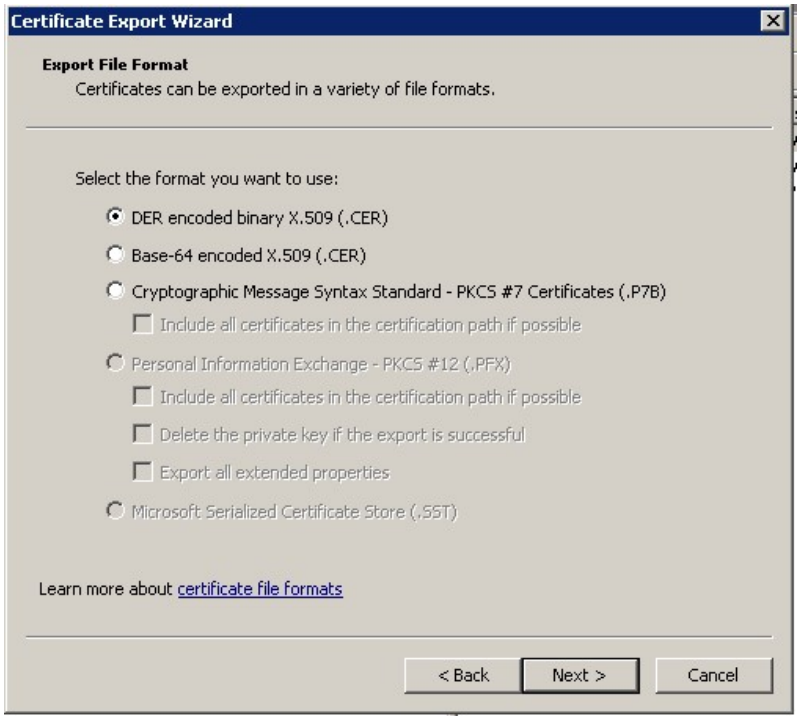


11. In the Certificate Export Wizard click **Next**.

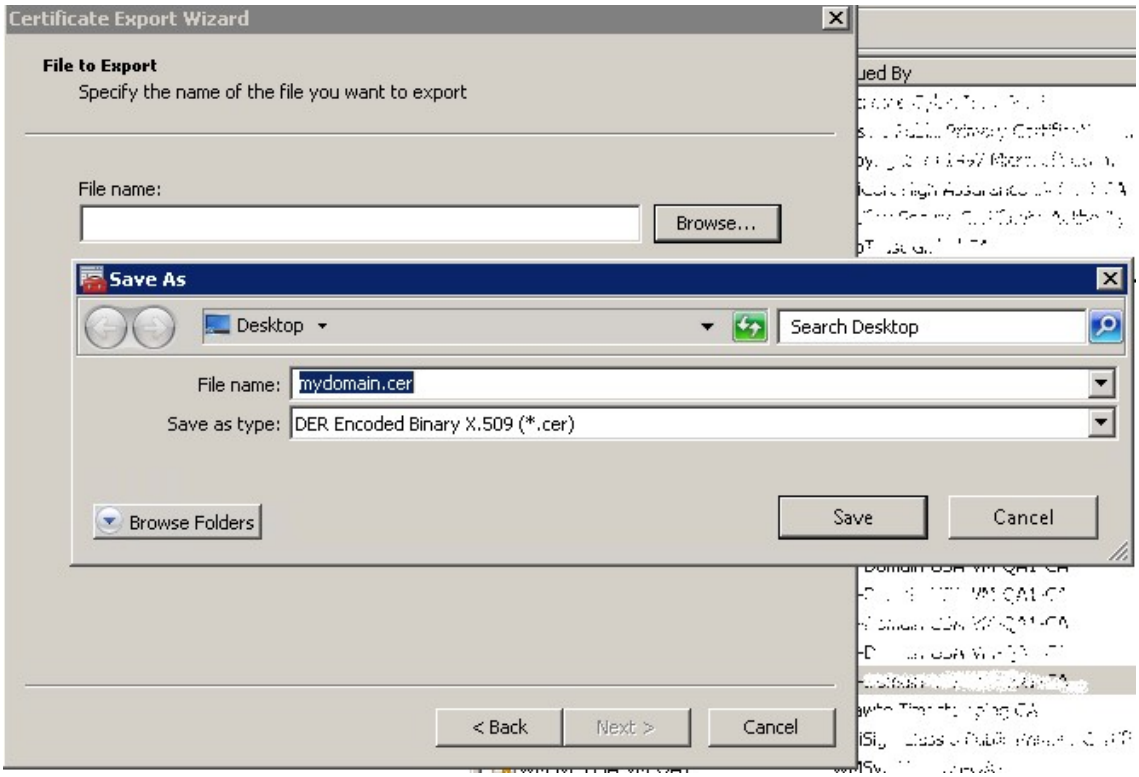

12. Choose "**No, do not export the private key**" and click **Next**.



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



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**.



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


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
3. 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**

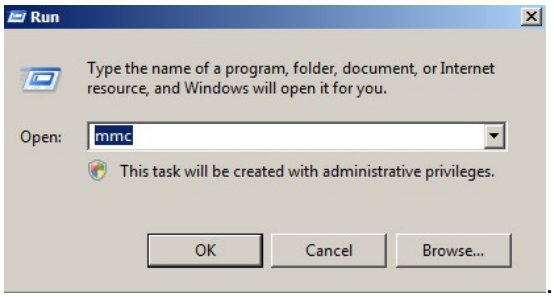
# 4. Configure LDAP client computer to connect using SSL

## 4.1. Import LDAP Server Certificate

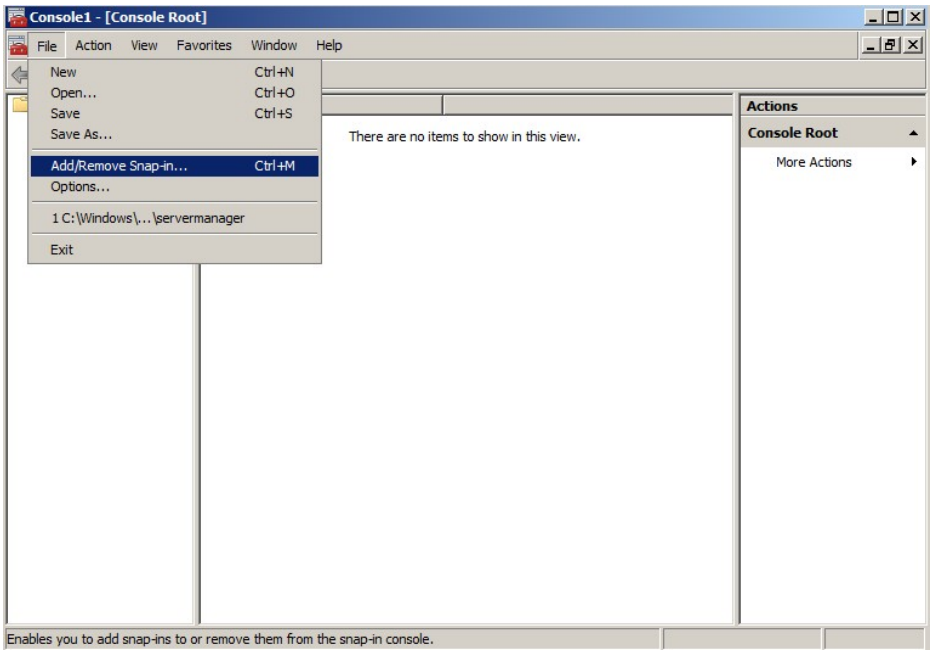
If LDAP server and client are on different domain you need to import the certificates files from LDAP server (see “3.2 Export Certificate”) to connect client to server using Secure Socket Layer (SSL).

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

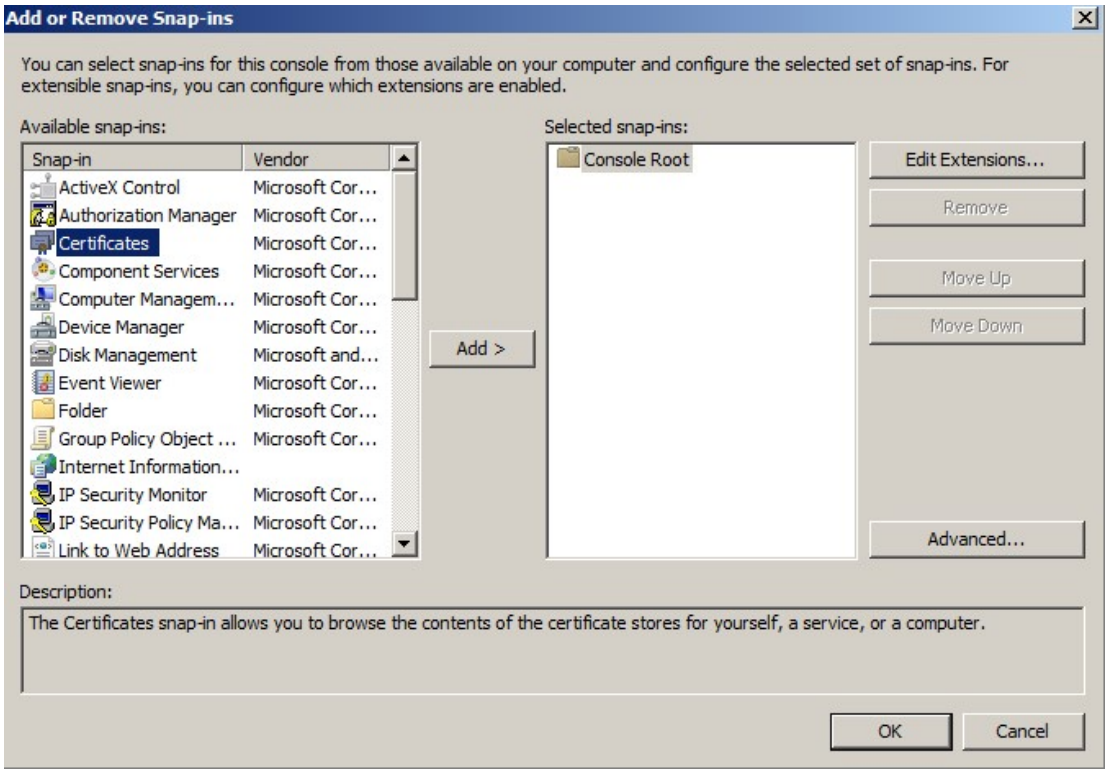
1. Click on the Start menu and click **Run.**
2. Type in **mmc** and click **OK.**



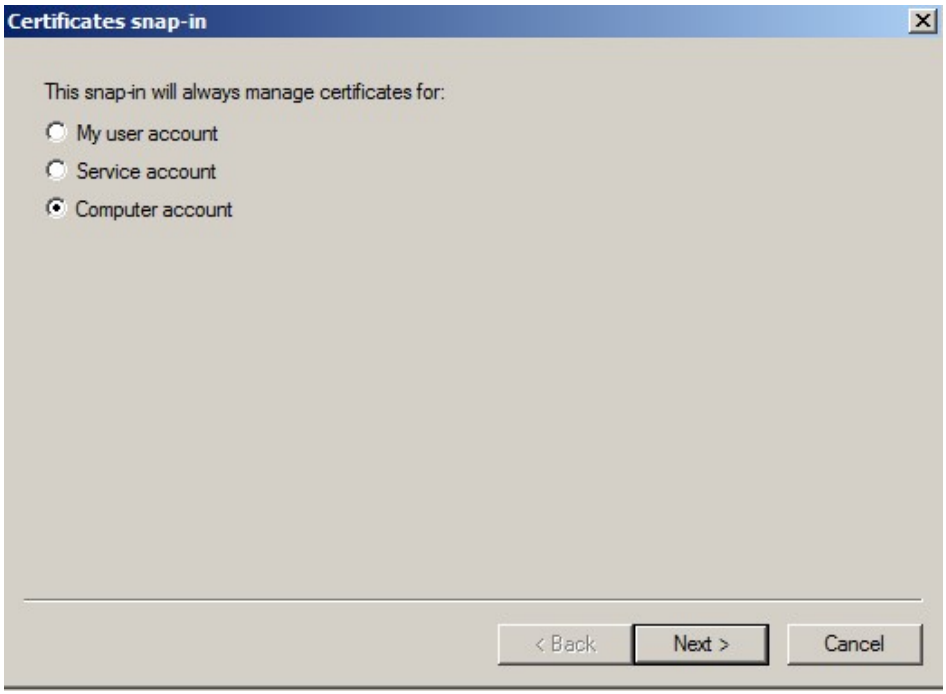
3. Click on the **File** menu and click **Add/Remove Snap-in…**



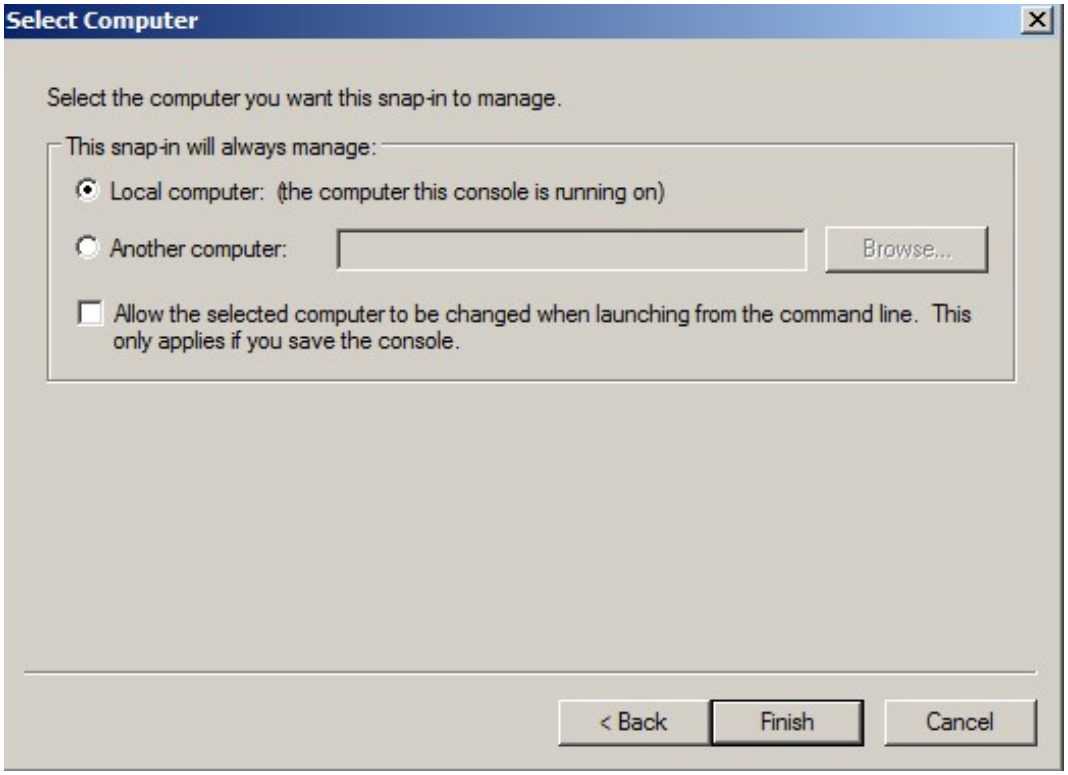

4. If you are using Windows Server 2003, click on **Add** button. Double-Click on **Certificates**.



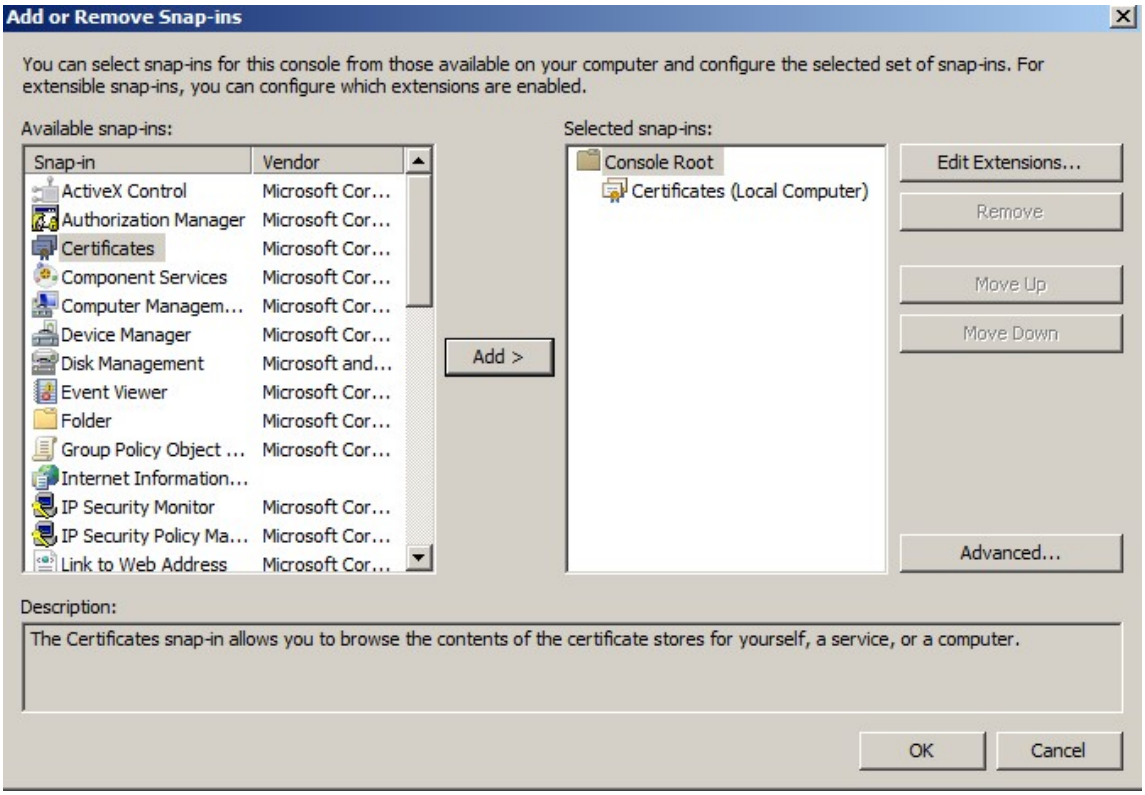
5. Click on **Computer Account** and click **Next**.



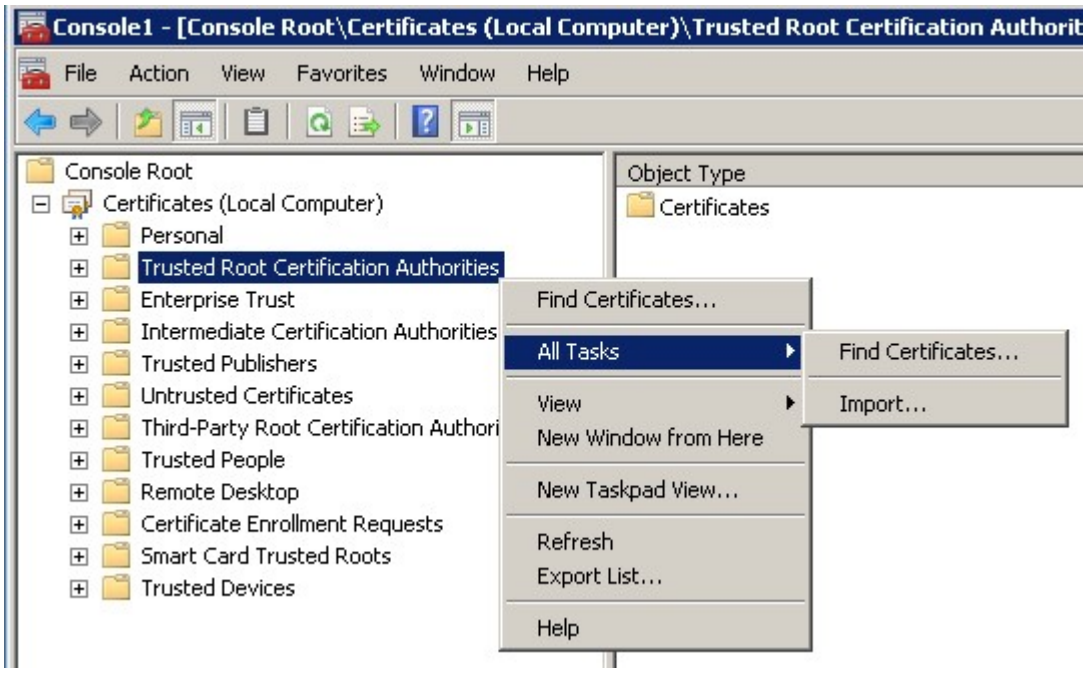

6. Leave **Local Computer** selected and click **Finish**.



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

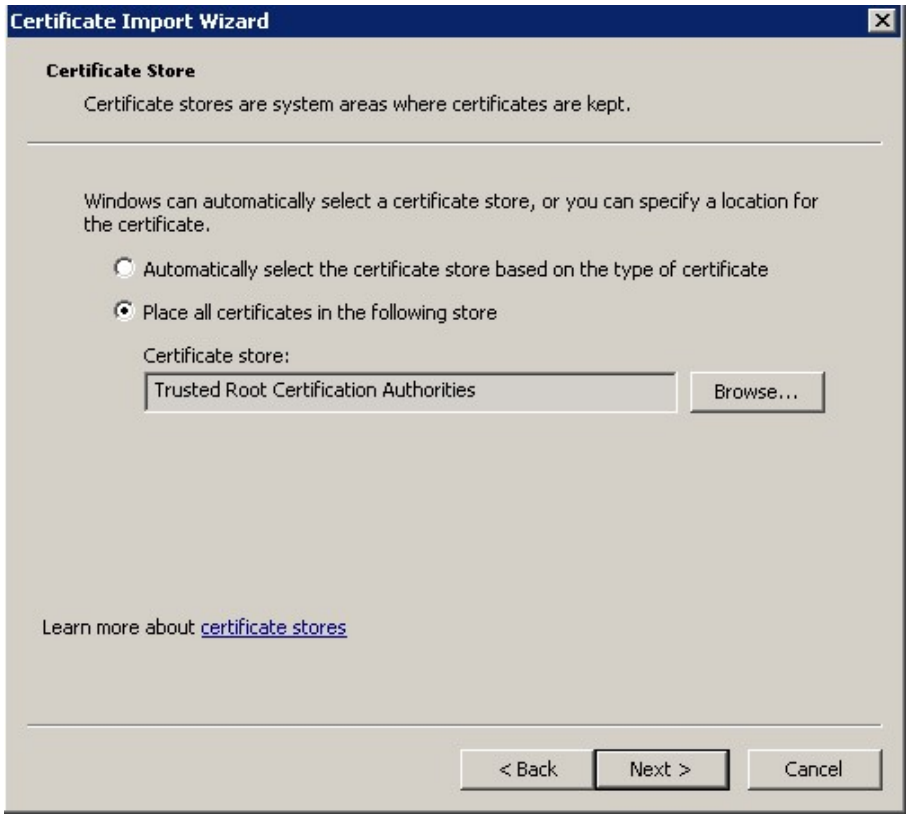



8. Right-click on the **Trusted Root Certification Authorities** folder and select **All Tasks** and then **Import...**




9. In the Certificate Import Wizard click **Next**.


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**.



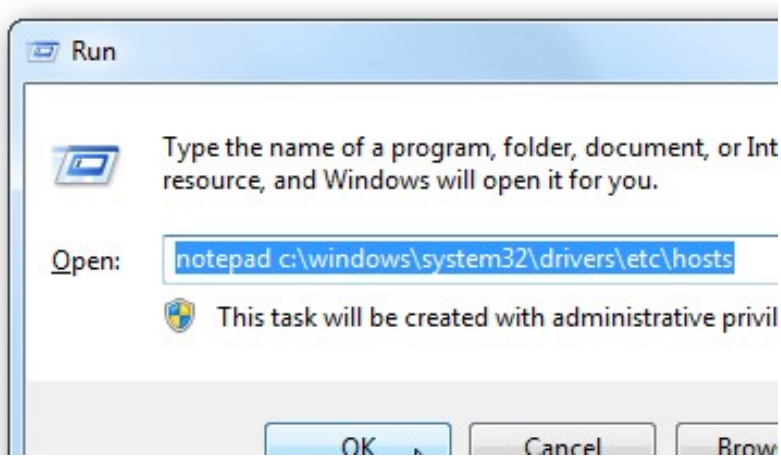
12. Click **Finish** to complete the wizard.
13. Repeat steps 8-12 for each of the certificates copied from the server.
14. You can now click the **Refresh** button in the toolbar to refresh and find your certificate in the Certificates folder under Trusted Root Certification Authorities.
15. Close the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

## 4.2. Edit Your Hosts File

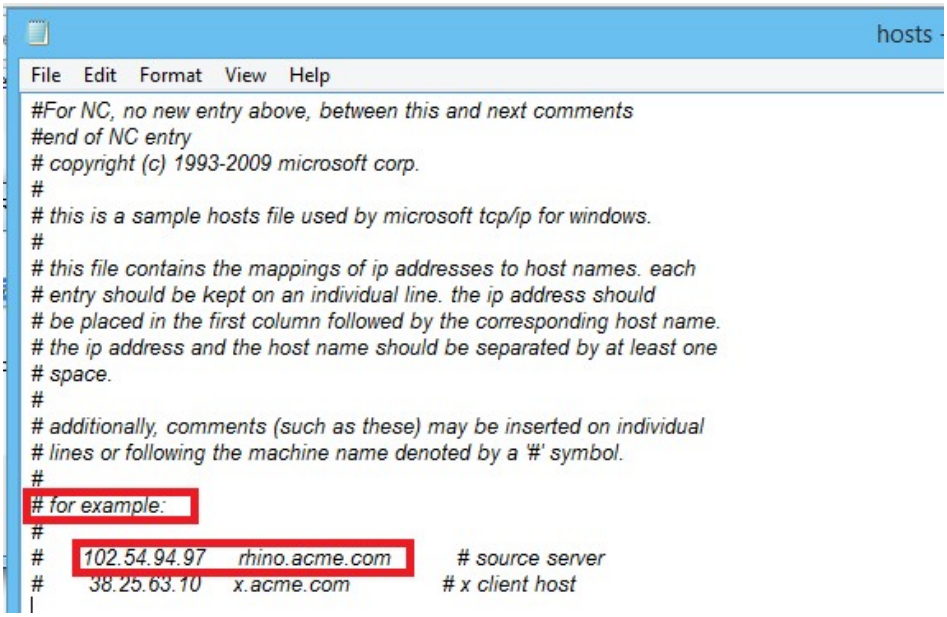
You can't use IP address to connect client to server using Secure Socket Layer (SSL), you must use machine's name of LDAP server because the certificate exported from LDAP server is based on server's name.

**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.**



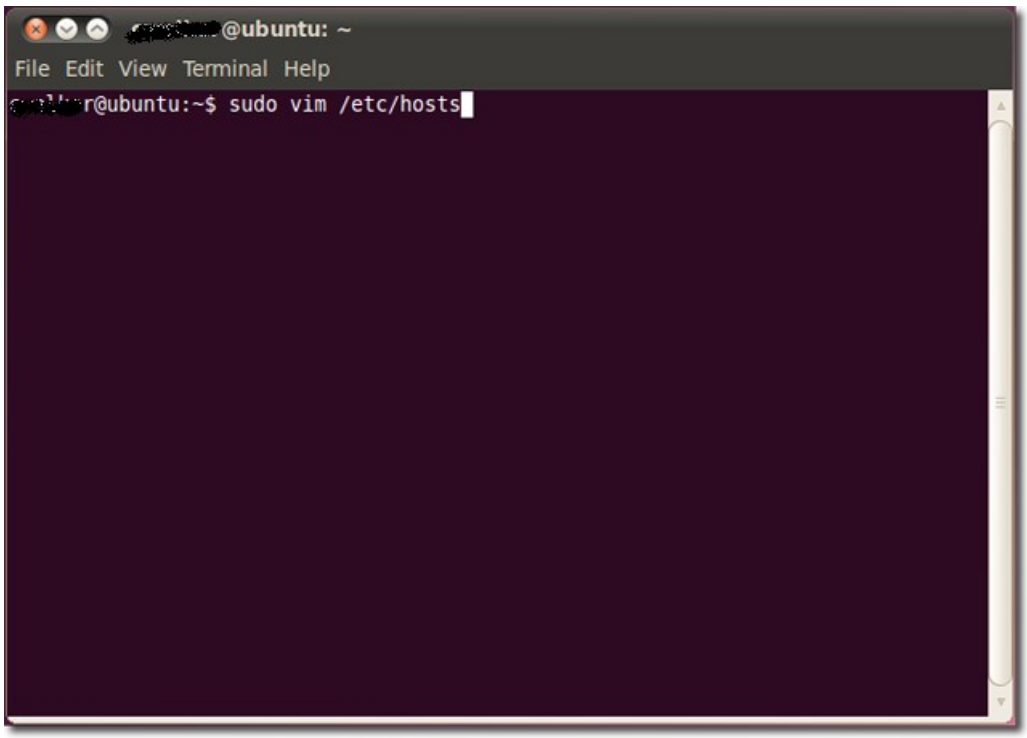

3. Once notepad is open you can edit the file and redirect LDAP Server IP.



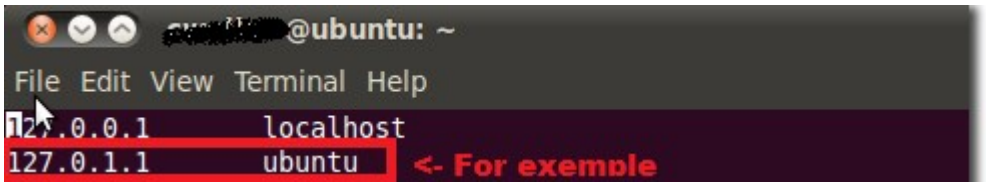

4. Make sure to **save** it.

**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.




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.