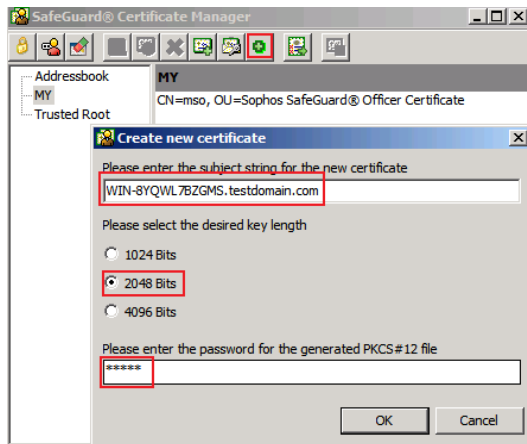


5. Create a new certificate. The name of the certificate must be the same as the name of the machine which was gathered in step 2 having the current domain suffix (FQDN name of the IIS box).

In this case the certificate's name would be "WIN-8YQWL7BZGMS.testdomain.com" since the name of the machine is "WIN-8YQWL7BZGMS" and the name of the domain is "testdomain.com".

The key length of the certificate remains on the default value. The password can be set just as desired.



6. After pressing OK save the cert and the p12 file to a destination that can be reached from the machine which hosts the IIS.

Please read carefully

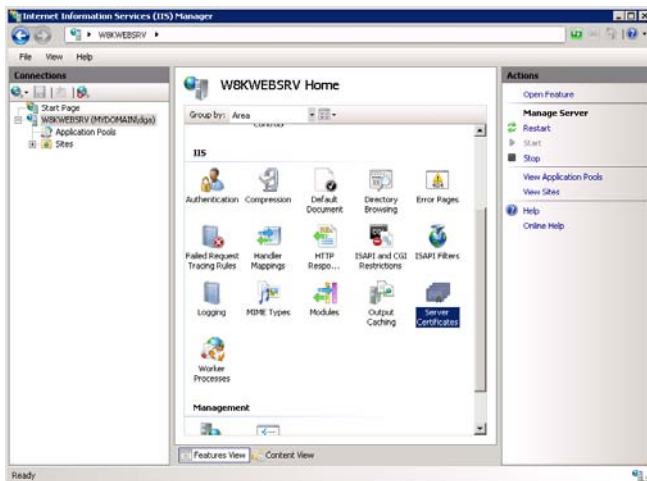
In case of using a PKI please create a certificate for the machine that is running the SafeGuard Enterprise Server. The certificate's name must be identical to the identity that is shown in the Internet Information Service (IIS) Manager top node. Besides this the certificate must be issued to the machine using the FQDN name of this machine.

In case only a certificate is created by a public PKI and no PKI infrastructure is available it is not possible to use this certificate to secure the communication with SSL. Such a scenario would require to set up a PKI infrastructure or to create a self- signed certificate which is described in section 3.1 of this document.

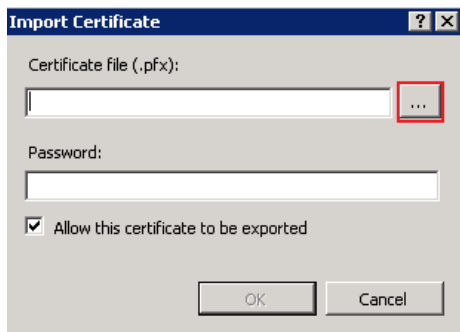
5.3 Configuring the SGNSRV web page to accept certificates

As soon as a valid certificate in order to use SSL is available it is possible to configure the SGNSRV web page to accept a certificate secured connection. The required steps to do so are like this:

1. Open the Internet Information Services (IIS) Manager.
2. Click on the server name.
3. From the center menu, double-click the "Server Certificates" button in the "IIS" section center pane.



4. From the Actions menu (on the right), select **Import**. This will open the **Import Certificate** wizard.



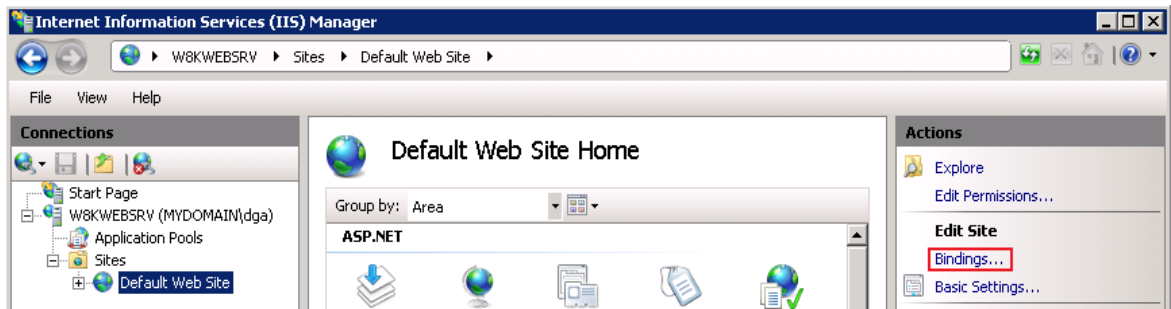
5. In the open dialog change the file extension to *.* and browse to the location where the .p12 and the .cer file are stored. Select the p12 file that was created before. In case that file extensions are disabled please select the file with the description *Personal information Exchange*



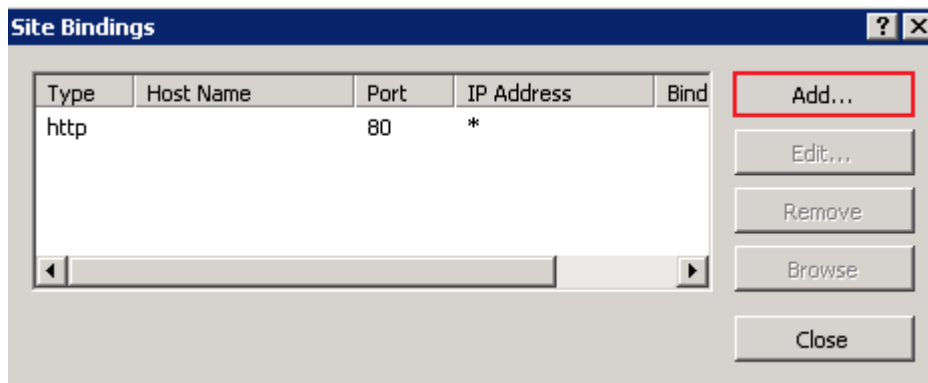
- Once the certificate has been installed successfully on the server, you will need to assign that certificate to the appropriate website using IIS.

From the "Connections" menu left hand side in the main Internet Information Services (IIS) Manager window, select the name of the server on which the certificate was installed.

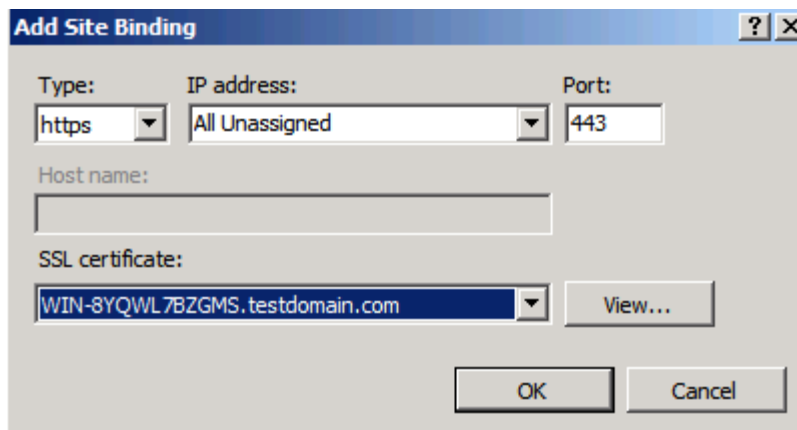
- Under **Sites**, select the site to be secured with SSL.
- From the **Actions** menu (on the right), select **Bindings**. This will open the **Site Bindings** window.



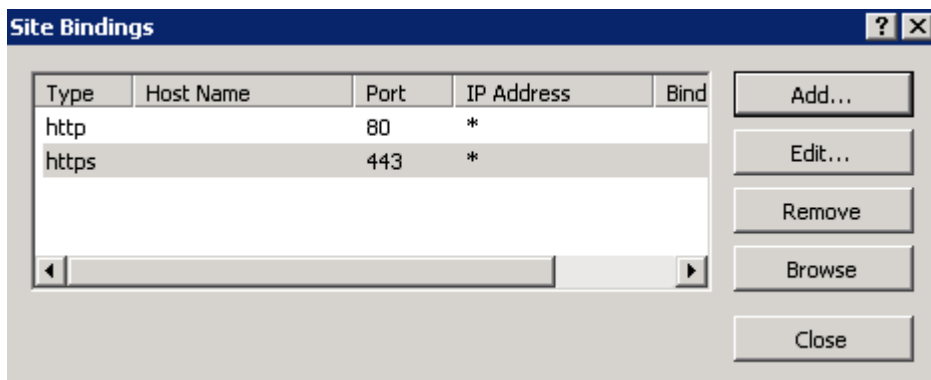
- In the **Site Bindings** window, click **Add...** This will open the **Add Site Binding** window.



- Under **Type** choose **https**. The IP address should be **All Unassigned**, and the **Port** over which traffic will be secured by SSL is **443**. The **SSL certificate** field should specify the certificate that was installed before.



11. Click OK.



The certificate is now installed, and the website configured to accept secure connections.

5.4 Deploying the certificate to the clients

The last step of this section is to deploy the certificate to the client as well since SSL would otherwise not work.

There are multiple ways of assigning a certificate to a client. One way of doing the assignment is using a Microsoft Group Policy. This is the way that will be described here. In case a different way of distribution should be used please ensure that the certificate is stored in the Computer Certificate Store.

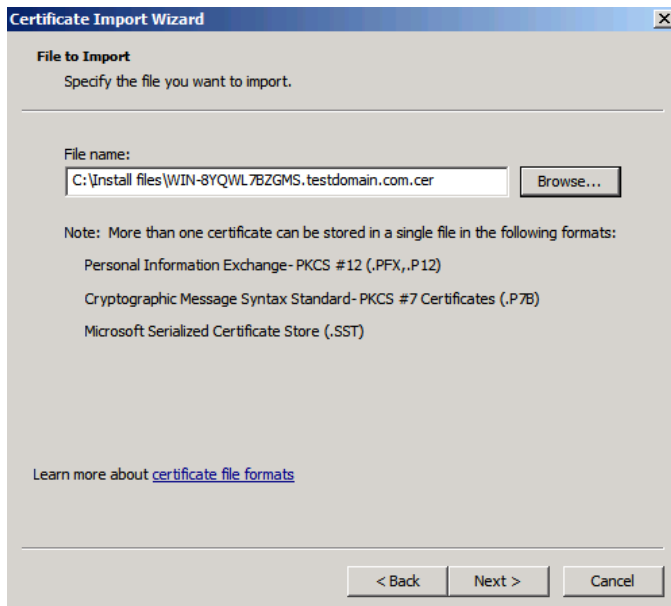
So in order to assign the certificate to the client using the Active Directory group policy mechanism perform the following steps.

Note: Ensure that the policy with the certificate deployment reaches all machines that should be installed with SafeGuard Enterprise especially if these objects are not centrally stored in one single OU.

The detailed steps are:

1. Open the Group Policy Management console (**Start > Run > Gpmc.msc**).
2. Create a new group policy object.
3. Open the new GPO and browse to **Computer Configuration > Windows settings > Security. Settings > Public Key Policies > Trusted Root Certification Authorities**.
4. Right click in the right hand pane window > **Import**

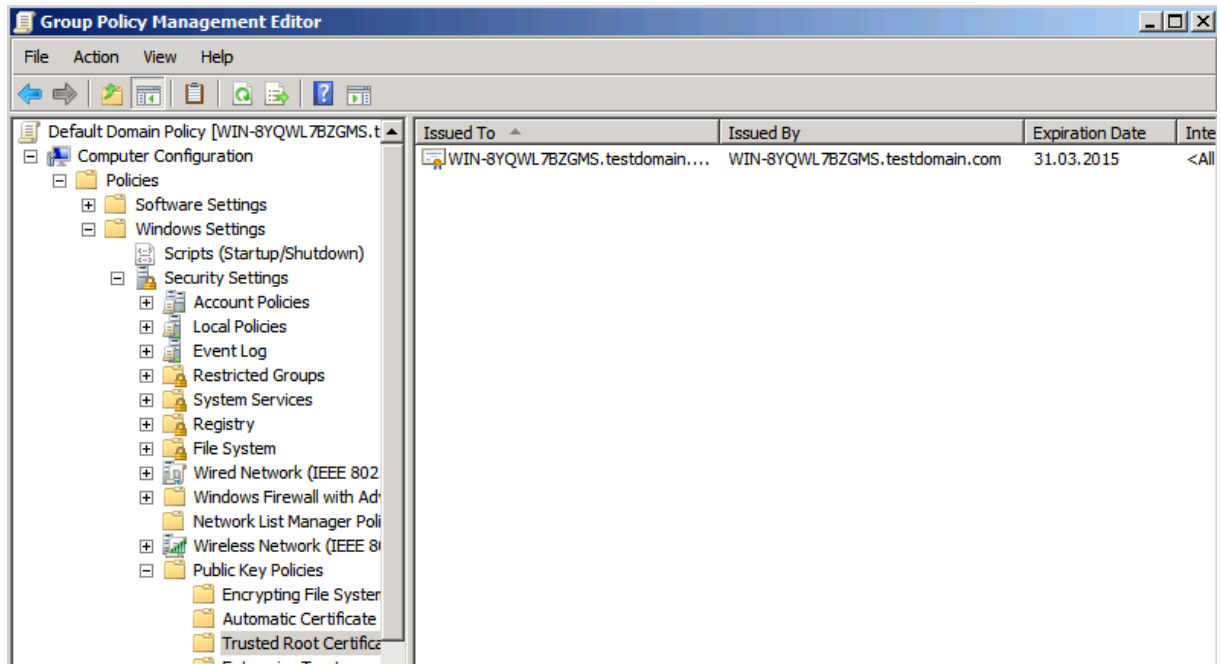
- Browse to the .cer and the p12 which was created to secure the communication > select the .cer file.



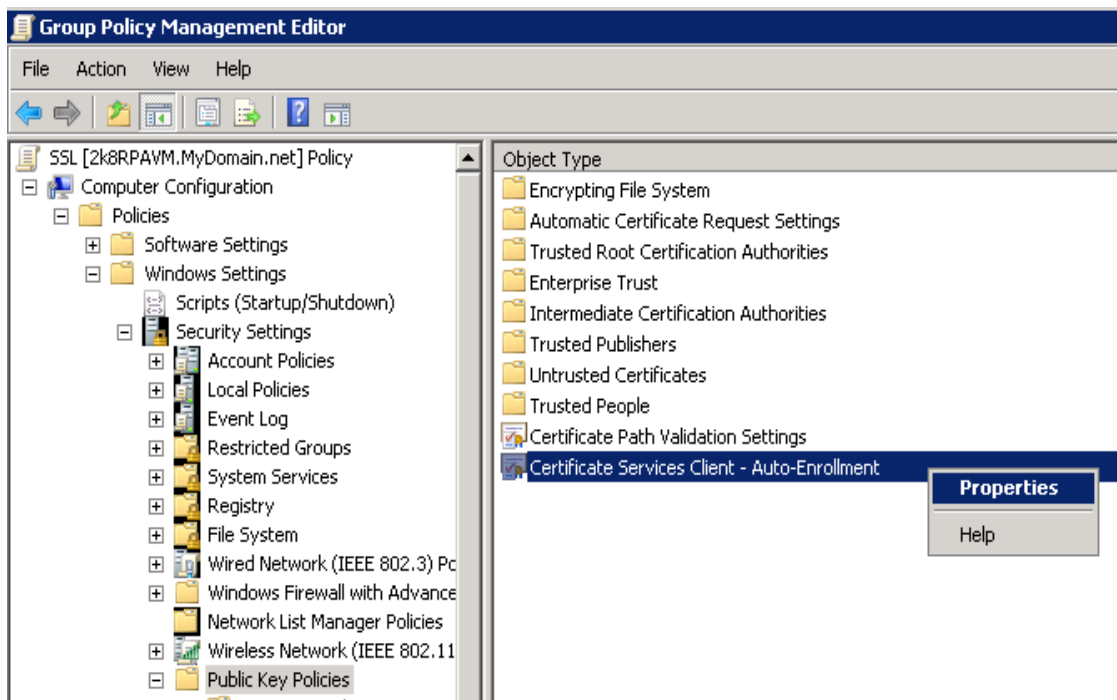
- By default the certificate will be located at the right place on the client.



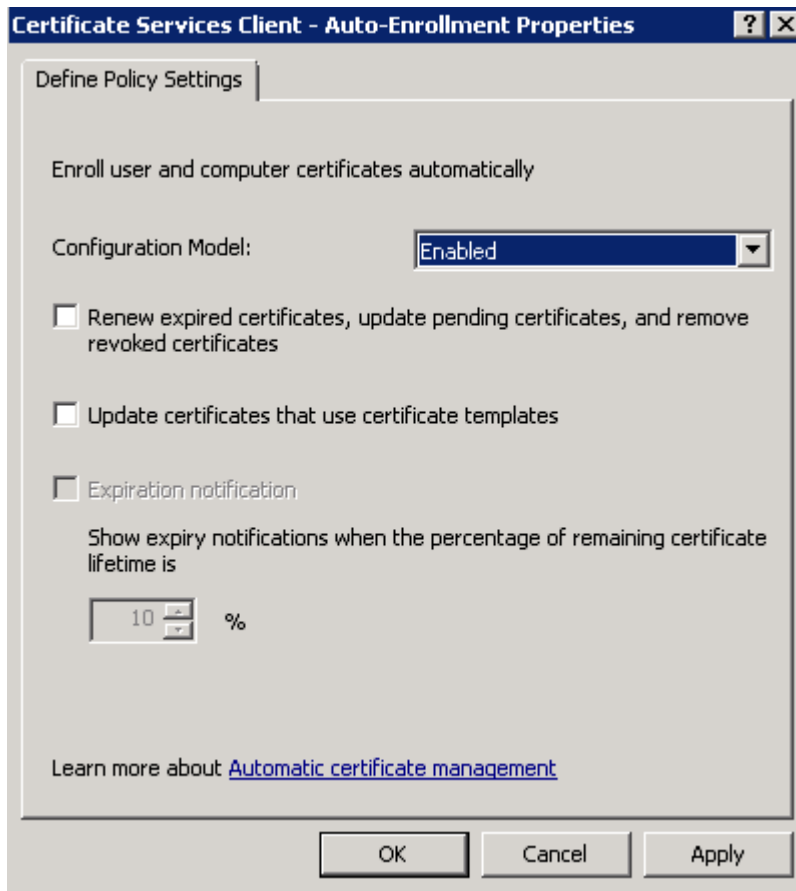
7. Having completed this successfully the GPO will look like this:



8. Browse back to the **Public Key Policies** node > right click on *Certificate Services Client - Auto-Enrollment* in the right hand pane > **Properties**.



9. Activate the automatic enrollment of certificates. This will ensure that every client receives the required policy.



10. Apply the changes and close the snap-in.

The configuration of the SafeGuard Enterprise back end is now completed!

The next step is to proceed with the installation of the client.

6. Installing the SafeGuard Enterprise Client

As soon as the back end is running the deployment and installation of the SafeGuard Enterprise client can begin.

The installation of the SafeGuard Enterprise client is straight forward. However, there are some things that should be considered such as preparation tasks prior to the installation. Although these steps are only optional we highly recommend following these steps to ensure a smooth implementation.

The SafeGuard Enterprise Client can be installed on different kinds of hardware and on different operating systems. A full list of all operating systems supported and the minimum system requirements can be found in the *Release Notes* which is part of the product CD.

Besides this there is a list of hardware which has been tested successfully or which is already known to need a POA hot key to function properly. Further details about SafeGuard Enterprise POA hot keys can be found in our knowledge base under <http://www.sophos.com/support/> > please use *SGN POA hot key* or *SGN hardware* as search expression. Reading these articles is highly recommended before starting the installation of the SafeGuard Enterprise client.

This example will use a Windows 7 (32 bit) machine to demonstrate the installation.

6.1 Quick installation reference

1. Check that the certificate has reached the client.
2. Prepare the operating system using *chkdsk /f/v/x* and *defrag*.
3. Install the SafeGuard Client package including the latest hardware compatibility list.
4. Create a new client configuration package.
5. Install the client configuration package.
6. First reboot and user initialization .

6.2 Checking the certificate arrival on the client

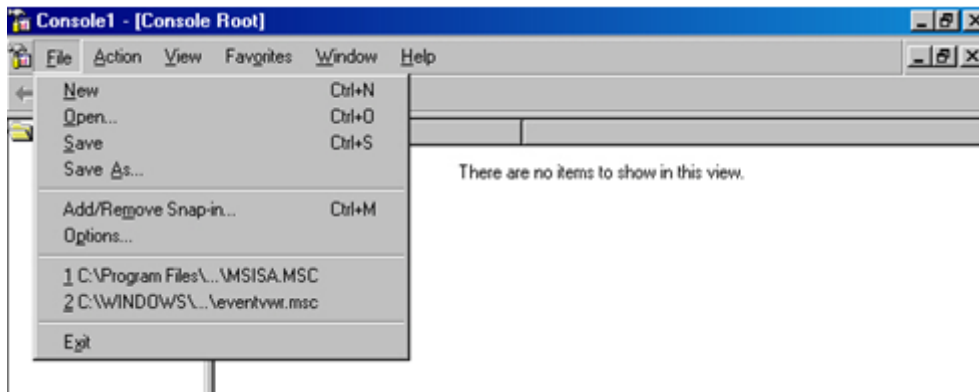
In order to check if the certificate was distributed correctly please take these actions.

The certificate must be assigned to the computer and not to the user. The **certificate file** must be available in the Certificate Store of Microsoft under **Trusted Root Certification Authorities** (in case of having a PKI running this is not required).

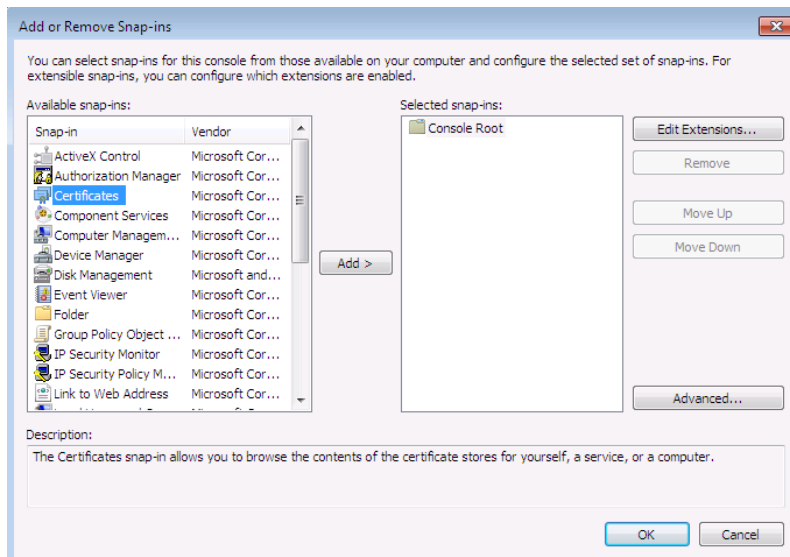
In order to do so please follow these steps on the client:

1. Log on to the machine using an administrative account.
2. Click **Start** > **Run** > *mmc* .

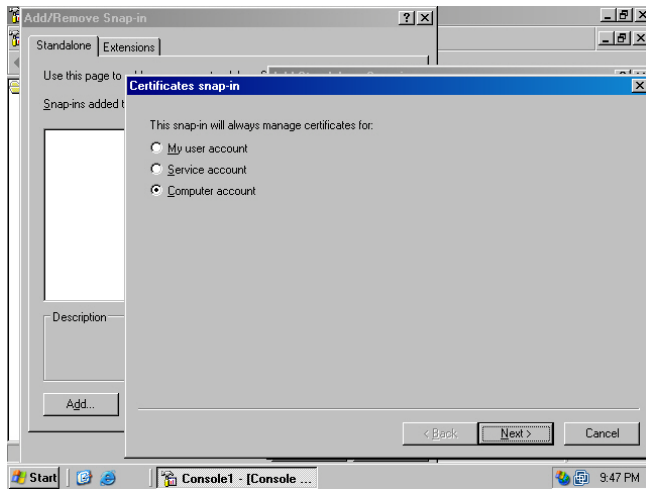
3. In the Console1 window, click the File menu and then click the Add/Remove Snap-in command.



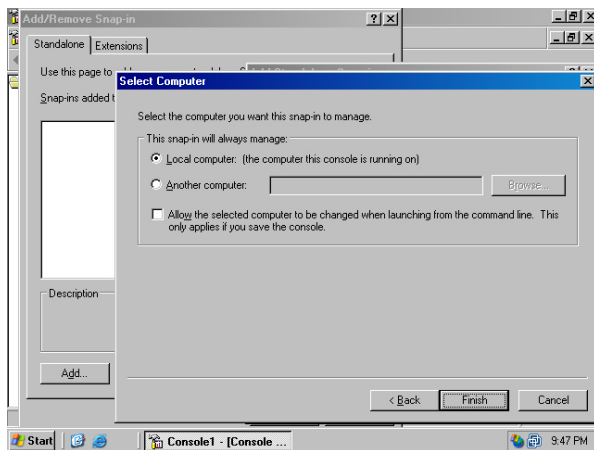
4. In the Add/Remove Snap-in dialog box select Certificates in the left hand pane and click the Add button in the center afterwards.



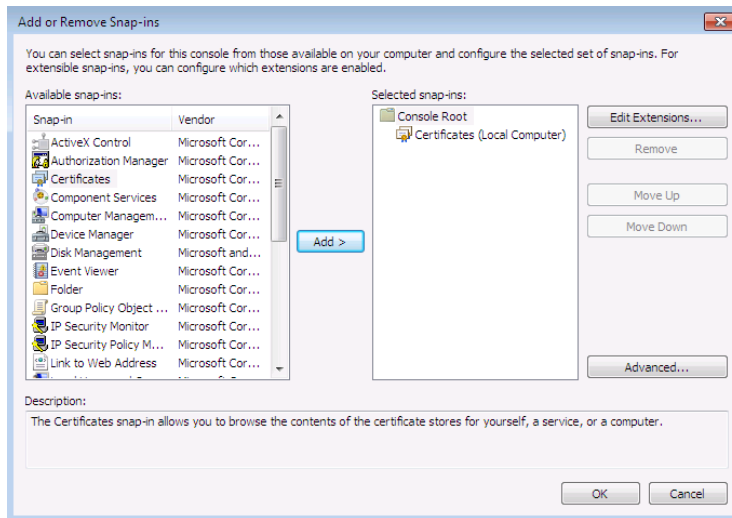
5. Select the **Computer** account option on the **Certificates snap-in** page.



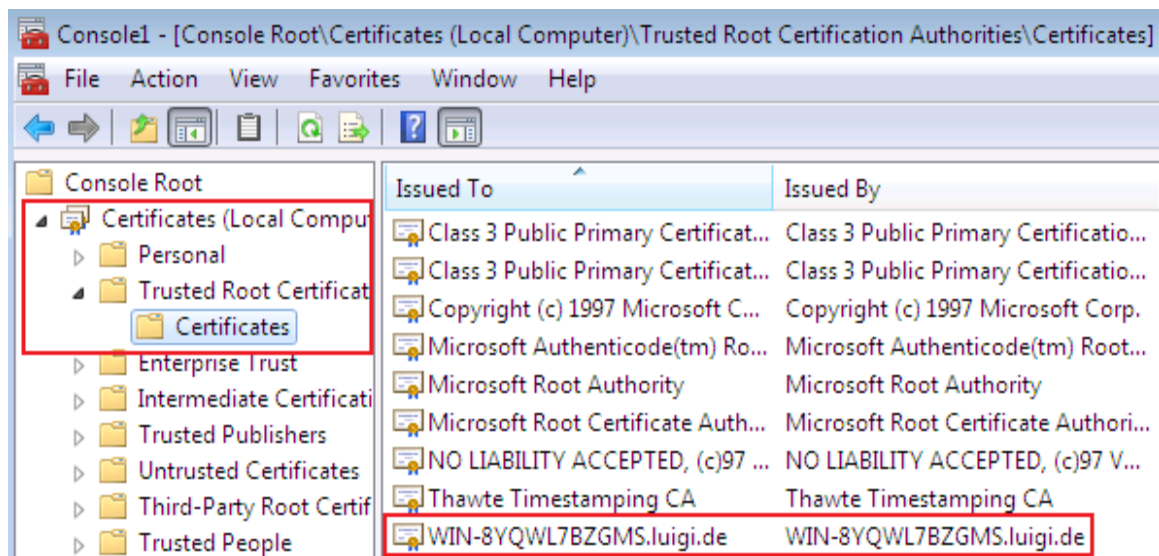
6. Select **Local computer: (the computer this console is running on)** on the **Select Computer** page. Click **Finish**.



7. Click OK in the Add Standalone Snap-in dialog box.



8. In the left pane click **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
9. Check in the right hand pane if the certificate which was created before is showing up.



In case the certificate appears this step is completed.

Note: If the certificate does not appear take these steps:

- Start > run > `gpupdate /force` > a Windows command box will come up.
- Wait until the box has closed and perform the above steps again starting at 1.

8. Legal notices

Copyright © 1996 - 2011 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

Sophos is a registered trademark of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.