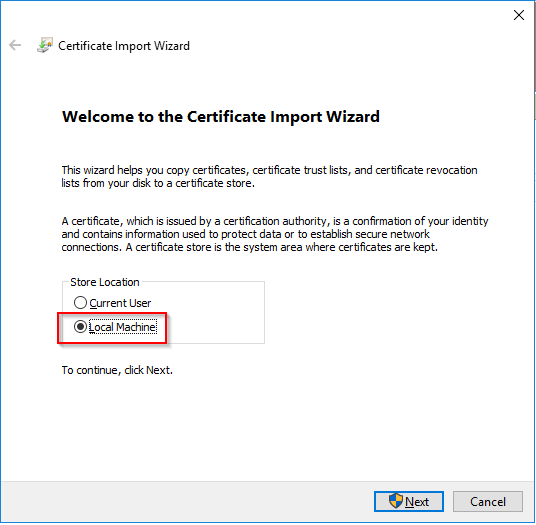
DotNetDynDnsSvc Setup Notes

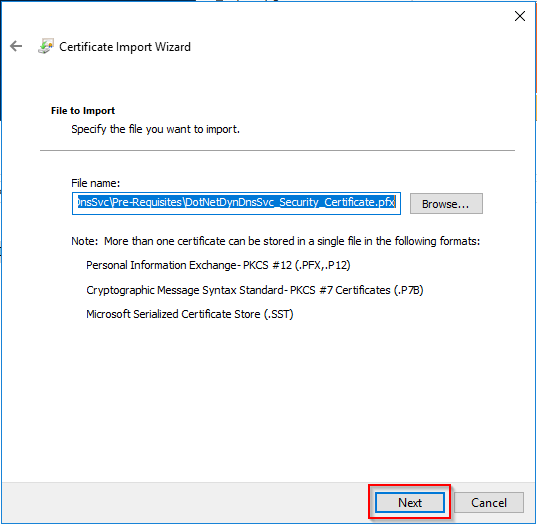
* OS: 2016+
* OS Roles:
  + Web Server (IIS)
* OS Features:
  + Under web server:
    - IIS Management Console
    - ASP.Net 4.6
  + Under Remote Server Administration Tools
    - Under Role Administration Tool
      * DNS Server Tools
* Web Server Role Services:
  + ASP.Net 4.6 (and dependencies)

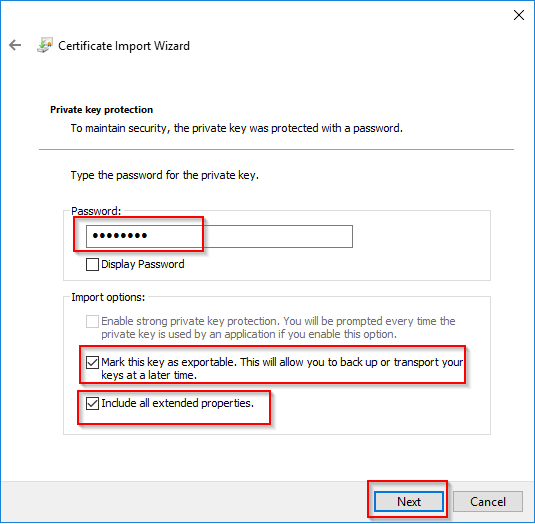
Upgrade .net to 4.7.2. runtime.

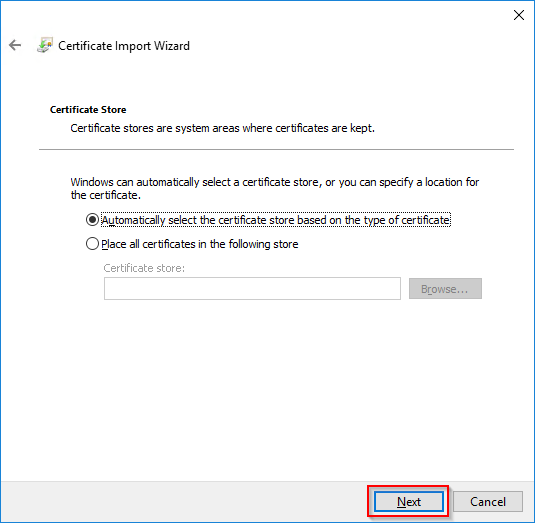
Import the Security Certificate into the Local Machine Store:

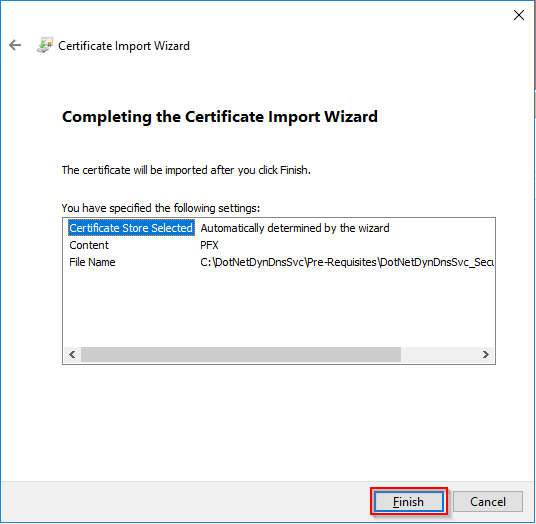
Right click the PFX archive, and choose install PFX and then:



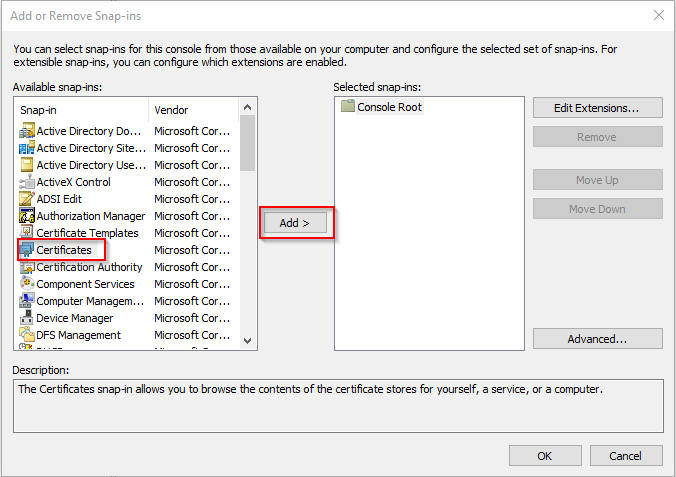


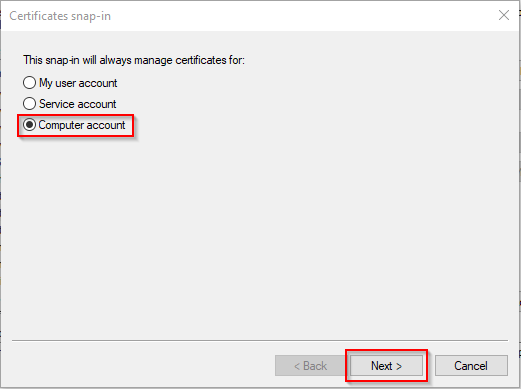


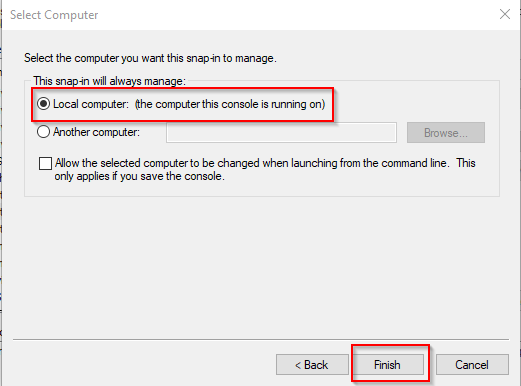




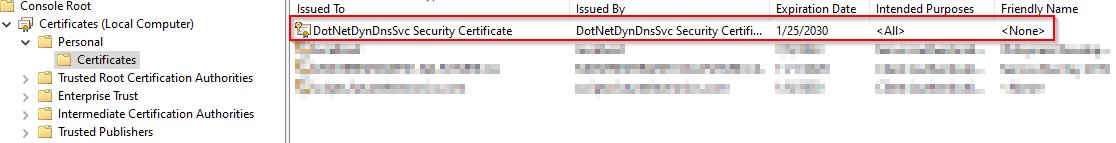
Open a new ‘mmc.exe’ window. Add the certificates snap-in (File -> Add Remove Snap-In, Certificates, click on “Add”), and configure it for the Local Machine:







Navigate to Personal -> Certificates, and find the certificate that was just imported:



Right click it, All tasks -> Manage Private Keys. In the security window that pops-up, add the IIS\_USERS group, and select “Read-Only”. This will allow IIS to have read access on this private key, which the application requires.

Create a folder that will contain the web site and required dependencies. The folder can exist anywhere on the server. The folder structure required is:

* <some folder somewhere – called whatever you want>
  + DB
    - Used to contain the SQLite Database
    - Local IUSR account read only
  + Logs
    - All custom application logs will be written here
    - Local IUSR account read/write
  + wwwroot
    - the folder containing the web site
    - Local IUSR account read only

Create a new web site, name it accordingly (dnsupdates.mydomain.com). physical path should be the wwwroot directory that was created above. Set the host headers and port accordingly. Web site should have anonymous user authentication using the IUSR account. No other authentication methods should be selected (ASP.Net, Forms, Basic, all disabled).