

Microsoft Internet Information Services 7 / 7.5

Följande guide beskriver hur man administrerar certifikat på Microsoft IIS 7 & 7,5.

För support och hjälp till användandet av denna guide kan du kontakta blueSSL på email info@bluessl.com eller telefon +46 (0)10-10 10 334 eller telefon +45 77 345 678. För beställning av certifikat, jämförelse av certifikat och fler guider titta på vår hemsida www.bluessl.com.



Inledning:

För installation av nytt SSL certifikat eller förnyelse av befintligt SSL certifikat på IIS 7.0 och 7.5, kan den samma tekniska guide användas. Vid beställning av certifikatet på vår hemsida www.bluessl.com väljes om certifikat är nytt eller förnyelse.

Det sista kapitel [Avancerat](#) gäller för er som skall importera certifikat från en PFX fil och/eller aktivering av installerat certifikat som är installerat på servern till ett webbsite.

Vi rekommenderar alltid att testa installationen när färdig på www.bluessl.com/sv/ssltest/

VIKTIG INFORMATION – LÄS MIG!

Omstart av tjänster eller server kan vara nödvändigt för att konfigurations ändringar man gjort via denna guide skall synas från Er klient.

Innehållsförteckning

Inledning:	1
Nytt Certifikat	3
Generering av CSR för beställning av certifikat	3
Import av mellanliggande certifikat ("Intermediate Certificate Authority")	4
Installering av certifikat från en certifikats request	7
Aktivering av certifikat på en webbsida	9
Avancerat.....	10
Import af certifikat fra certifikat backupfil (.PFX).....	10
Aktivering av installerat certifikat på en webbsida	14

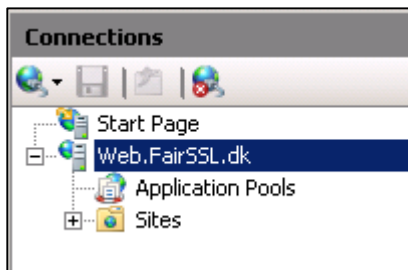
Nytt Certifikat

Detta kapitel täcker hur Ni generar och beställer ett helt nytt certifikat till en ny server, installerar intermediate certifikatet och tillslut installerar certifikatet.

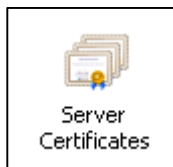
Generering av CSR för beställning av certifikat

Följande guide beskriver hur man genererar en certificate signing request (CSR) på en Microsoft IIS 7.

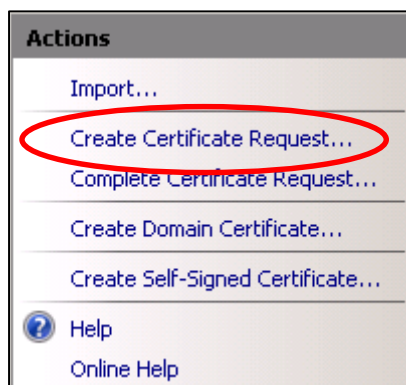
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startar Ni "Internet Information Services (IIS) Manager".
3. Välj Er webserver.



4. Välj "Server Certificates".



5. Under "Actions" väljer Ni "Create Certificate Request".



- Fyll i Era upplysningar för certifikatet som skall skickas till utställaren. All data som är ifylld här under är för FairSSL och skall rättas så det passar er organisation. För att vara säker på att certifikatet utfärdas utan problem bör man undvika "ÅÄÖ" och andra specialtecken.

- Namn på certifikatet och verksamhets information.

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="www.FairSSL.dk"/>
Organization:	<input type="text" value="FairSSL ApS"/>
Organizational unit:	<input type="text" value="IT Afdelingen"/>
City/locality	<input type="text" value="Oerum"/>
State/province:	<input type="text" value="Djurs"/>
Country/region:	<input type="text" value="DK"/>

- Välj kryptering, **minst 2048 Bit**.

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

- Välj vart Ni vill spara CSR filen.

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

...

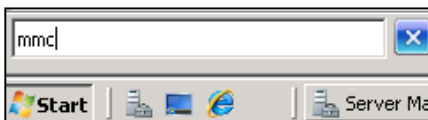
- Nu har Ni skapat en CSR som Ni kan använda till er beställning.

Import av mellanliggande certifikat ("Intermediate Certificate Authority")

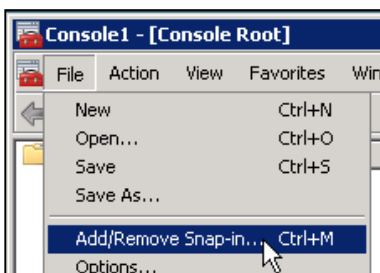
Följande beskriver hur man installerar ett mellanliggande certifikat på en Microsoft Windows server och även en SBS 2003 server. För att säkra upp så att klienter godkänner det mellanliggande certifikatet, måste

detta installeras på SBS 2003 servern. När Ni får ett GlobalSign certifikat får Ni också de offentliga mellanliggande certifikaten.

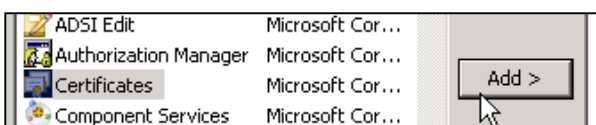
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Kopiera texten från det mellanliggande certifikatet ("Intermediate certificate"), från e-posten med ditt nya certifikat, till en enkel text editor (t.ex. Notepad). Spara filen på skrivbordet med filnamnet "mellanliggandecertifikat.cer".
3. Skriv följande kommando i "mmc.exe".



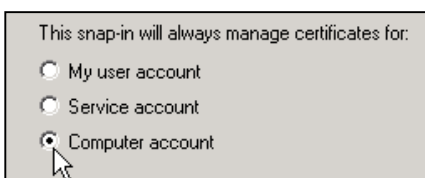
4. Välj "Add/Remove Snap In".



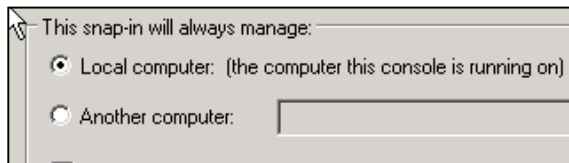
5. Välj "Certificates" och tryck "Add"



6. Välj "Computer account"

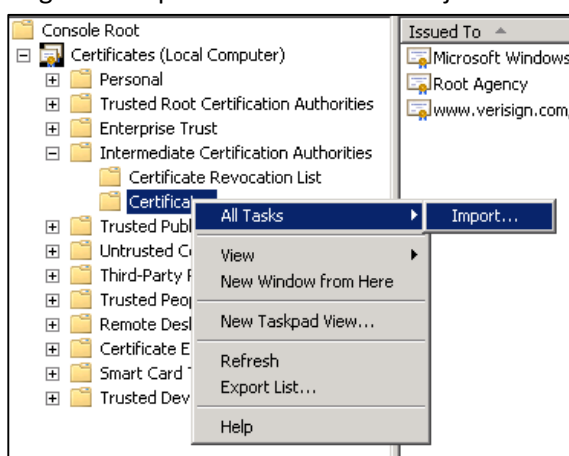


7. Välj "Local computer"

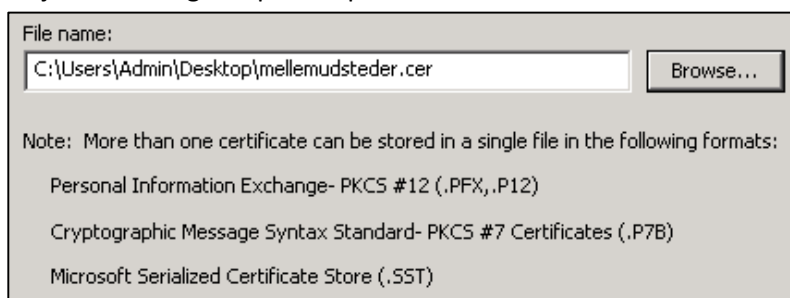


8. Under "Certificates (Local Computer)" expandera "Intermediate Certification Authorities" och "Certificates".

9. Höger klicka på "Certificates" och välj "All-Tasks" och "Import".



10. Välj filen Ni tidigare sparade på skrivbordet.



11. Kontrollera att certifikatet sparas i "Intermediate Certification Authorities"

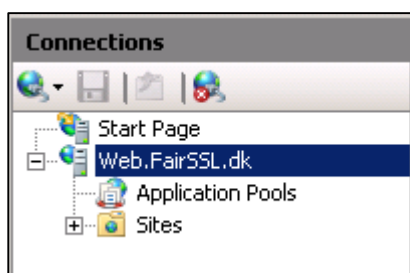


Det mellanliggande certifikatet är nu importerat.

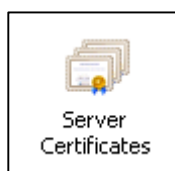
Installering av certifikat från en certifikats request

Följande guide beskriver hur Ni installerar certifikatet efter att det är utställt från den CSR Ni tidigare skapade på samma server.

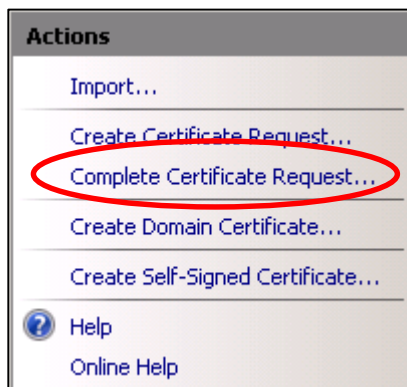
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Kopiera texten från certifikatet, från e-posten med ditt nya certifikat, till en enkel text editor (t.ex. Notepad). Spara filen på skrivbordet med ett passande namn, och en ändelse på ".cer eller .pem" I exemplet här är filnamnet "www.FairSSL.dk.cer"
3. Under "Administrative Tools" startar Ni "Internet Information Services (IIS) Manager"
4. Välj webbservern.



5. Välj "Server Certificates".



6. Under "Actions" väljer Ni "Complete Certificate Request".



7. Välj filen som Ni tidigare sparade på skrivbordet, och välj ett källnamn för certifikatet.

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

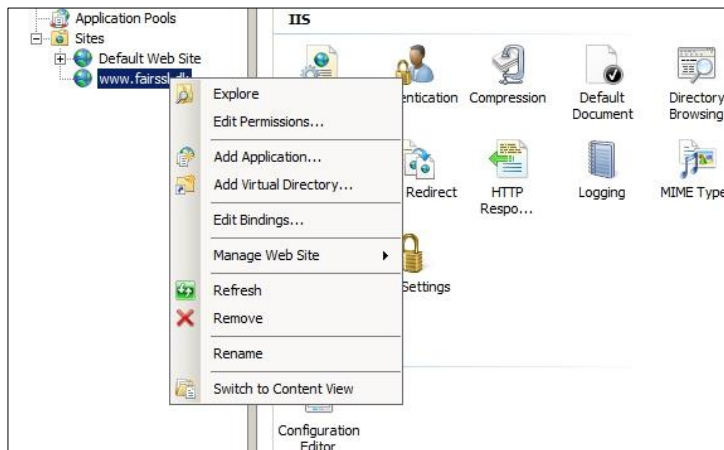
Friendly name:

8. Certifikatet är nu installerat på servern, men det är ännu inte aktiverat på någon webbsida.

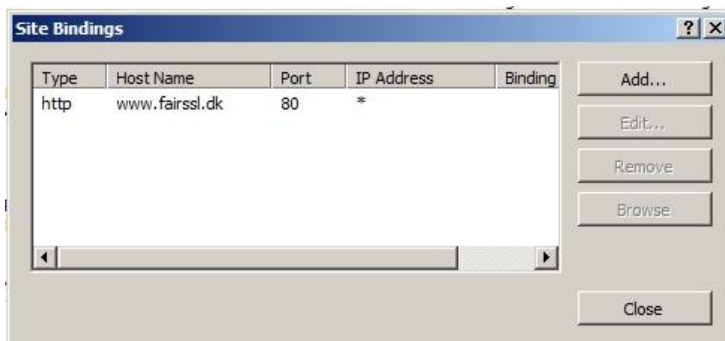
Aktivering av certifikat på en webbsida

Följande guide beskriver hur det nyligen installerade SSL certifikatet aktiveras på en given webbsida. Skall certifikatet brukas på flera olika webbsiter så skall detta kapitel repeteras ett för varje webbsida.

1. Högerklicka på webbsidan och välj "Edit Bindings..."



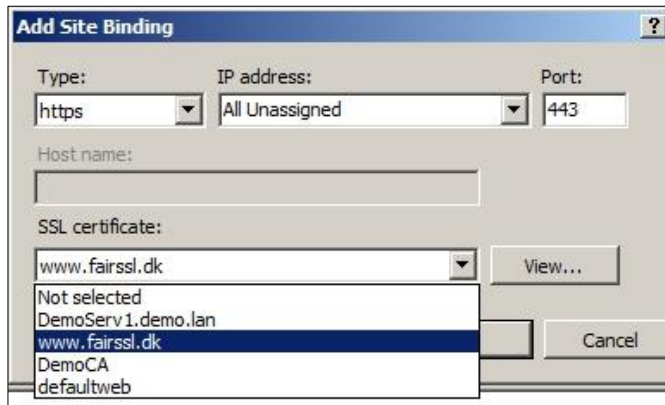
2. På "Site Bindings", Klicka på knappen "Add..."



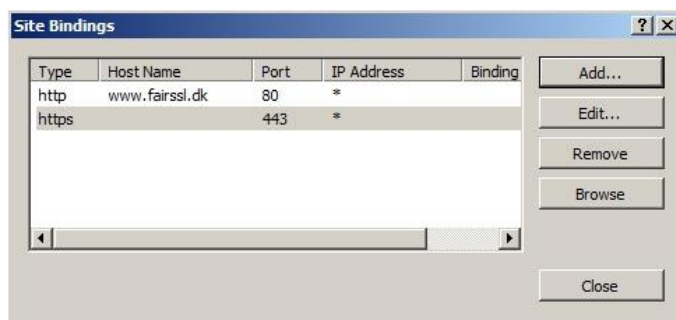
3. Välj "https" som typ



4. Välj det önskade certifikatet och klicka på "OK"



5. Klicka på "Close" för att stänga fönstret



6. Certifikatet är nu aktiverat för det för den valda webbsidan.

Avancerat

Under denna punkt guidar vi Er igenom processen att importera ett certifikat med filändelsen .PFX, hur man aktiverar ett certifikat på sin server och hur man aktiverar ett nytt certifikat utan att störa den befintliga sidan som är i produktion.

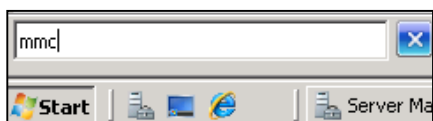
Import af certifikat fra certifikat backupfil (.PFX)

Följande guide beskriver hur man installerar ett certifikat från en .pfx fil.

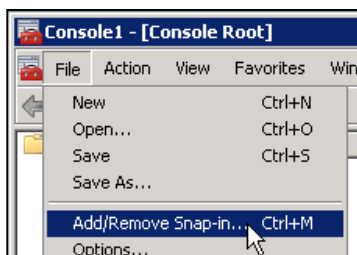
Vid beställning av domäner med FairCSR levereras certifikatet som en backup fil, skyddad med en unik kod.

1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Spara den mottagna filen på ditt skrivbord.

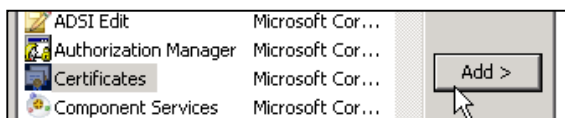
3. Skriv följande kommando "mmc.exe".



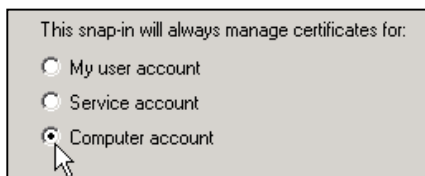
4. Välj "Add/Remove Snap In".



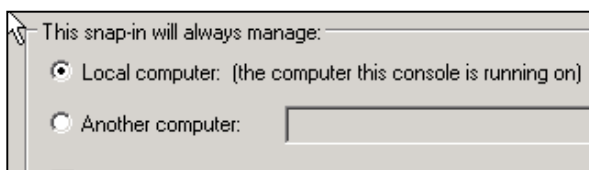
5. Välj "Certificates" och tryck "Add"



6. Välj "Computer account"

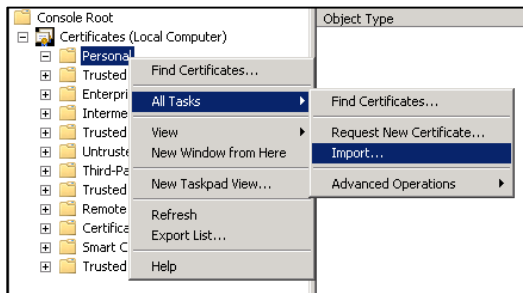


7. Välj "Local computer"

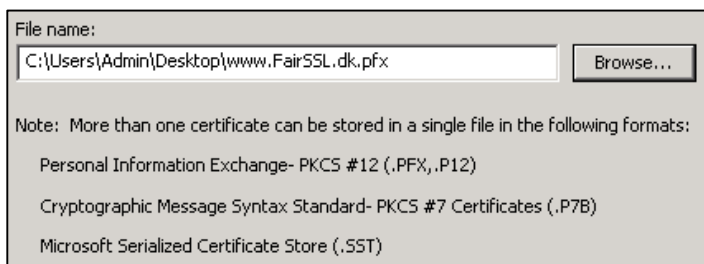


8. Under "Certificates (Local Computer)" expandera "Personal"

9. Höger klicka "Personal" och välj "All-Tasks" och "Import".



10. Välj den fil som Ni tidigare sparade på skrivbordet.

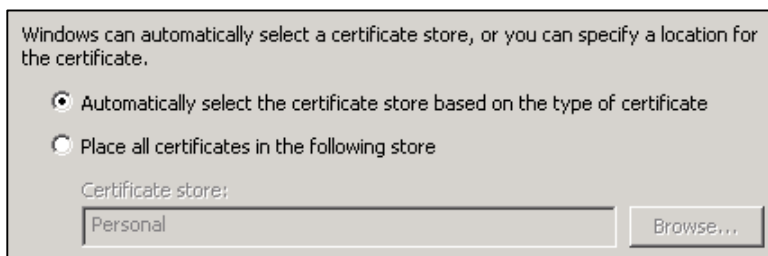


11. Fyll i den kod som certifikatet är krypterat med. Denna kod skall Ni ha fått på SMS.



Observera!!! Om du senare vill kunna exportera detta certifikat till en ny backup fil, skall "Mark this key as exportable" vara markerad.

12. Välj "Automatically select the certificate store based on the type of certificate".

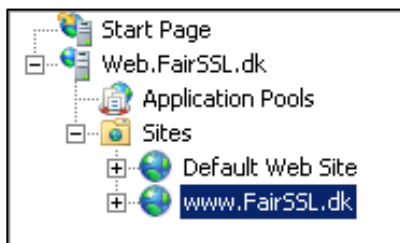


13. Certifikatet är nu importerat på servern.

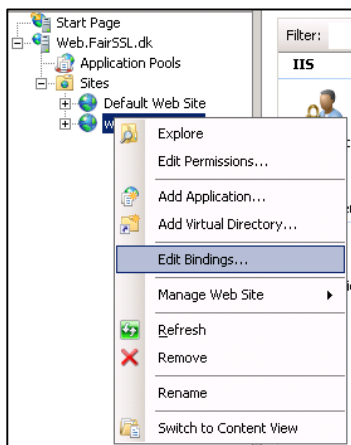
Aktivering av installerat certifikat på en webbsida

Följande guide beskriver hur ett redan installerat certifikat knyts till en webbsida.

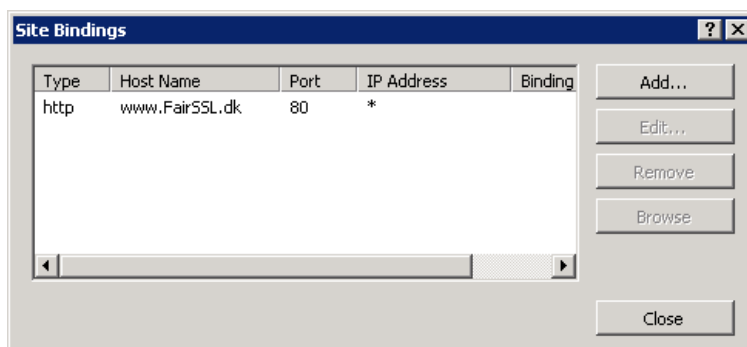
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager"
3. Expandera "Sites".



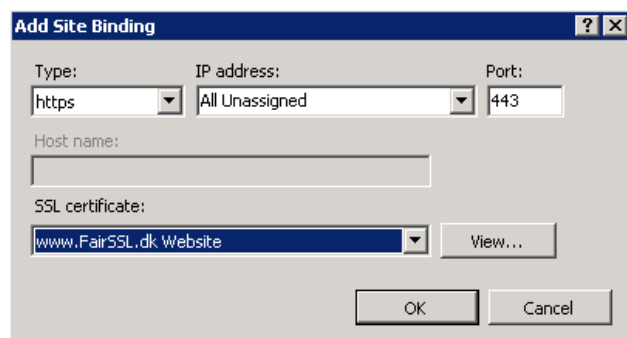
4. Högerklicka på den önskade webbsidan, och välj egenskaper ("Edit Bindings").



5. Välj "Add".



6. Välj "https" som typ, IP adressen, port och certifikat.



The screenshot shows a dialog box titled "Add Site Binding". It has three dropdown menus at the top: "Type" set to "https", "IP address" set to "All Unassigned", and "Port" set to "443". Below these is a text box for "Host name" which is empty. Underneath is another dropdown menu for "SSL certificate" set to "www.FairSSL.dk Website", with a "View..." button to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

7. Certifikatet är nu aktiverat på webbsidan.