FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Synology Diskstation 4.0

Synology producerer en lang række af netværksharddiske (NAS) rettet mod både privat og firma. Fælles for alle deres produkter er operativsystemet DSM.

Følgende vejledning beskriver hvordan man administrere certifikater på en Synology netværksharddisk (NAS) med DSM 4.0 eller nyere som operativsystem.

For support og hjælp til anvendelsen af denne vejledning kan du kontakte FairSSL på e-mail info@fairssl.dk eller telefon +45 77 345 678. For certifikat bestilling, certifikat sammenligning og flere vejledninger se websitet på www.fairssl.dk.

For generel support af Synology produkter, se www.synology.com

Hvis serveren er tilgængelig fra internettet bør installationen efterfølgende testes gratis på www.fairssl.dk/ssltest/

Indholdsfortegnelse

Version 1.0 – Maj 2012

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

SSL Begrænsninger i DSM <4.0

DSM versioner før 4.0 understøtter ikke Intermediate certifikater. Det er muligt at installere et eksisterende certifikat, men ikke certifikatets tilhørende mellemudsteder certifikat. Det vil derfor kun være nogle browsere (fx IE) og klienter som automatisk kan rette denne fejl der vil virke. Vi anbefaler at opgradere til DSM 4.0+ inden installation af SSL certifikat på en Synology Diskstation.

SSL Begrænsninger i DSM 4.0+

Synology DiskStation 4.0 understøtter installation af et eksisterende SSL certifikater inkl. intermediate (mellemudsteder) certifikater direkte via den grafiske brugerflade.

Det er dog ikke muligt at oprette et certifikat forespørgsel fra Synology Diskstation. Privat nøgle og CSR skal derfor laves separat på en anden maskine eller via vores websites værktøjer på www.fairssl.dk.

Valg af SSL certifikat til Synology NAS

Hvis synology boksen kun anvendes med dens fulde servernavn (FQDN) fx synology.fairssl.dk, både internt og eksternt med SSL/HTTPS, vil ethvert servercertifikat kunne anvendes. Dette er normalt, da websitet vil anvendes eksternt og internt anvendes normal windows fildeling eller lignende.

Der er dog situationer hvor Synology boksen tilgås med forskellige navne via websitet og her kræves at alle disse navne er i certifikatet for at undgå certifikatfejl. Dette kan løses med et SAN SSL certifikat eller wildcard SSL certifikat hvis navnene er under samme hoveddomæne.

Hvis minimal support er krævet (e-mail + chat), anbefaler vi som det biligste produkt et AlphaSSL certifikat. Ved større behov for support eller behov for flere servernavne anbefaler vi et GlobalSign DV/OV SAN certifikat. Alternativt et wildcard SSL certifikat, hvis det også skal anvendes til andre servere.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

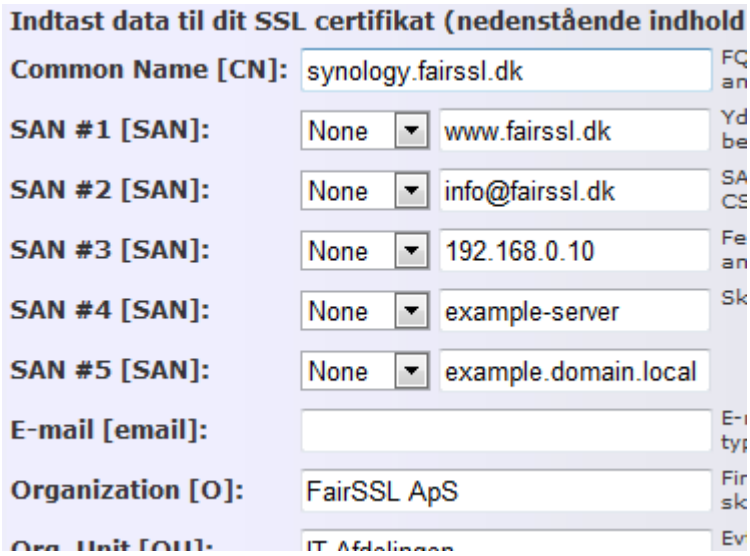
Trin 1: Lav privat nøgle og bestil SSL certifikat

Du skal oprette en privat nøgle og med denne lave en CSR certifikat forespørgsel. Det letteste for efterfølgende installation er at lave dette på vores website https://www.fairssl.dk/sslgenerator/ eller en via en lokal installation af OpenSSL værktøjet.

Hvis du allerede har et udstedt SSL certifikat, skal du skippe dette trin. Hvis certifikatet ikke er i et BASE64 kodet PEM format (fx PFX/PKCS#12), skal du først konvertere certifikatet med et værktøj som OpenSSL.

1. Gå til https://www.fairssl.dk/sslgenerator/

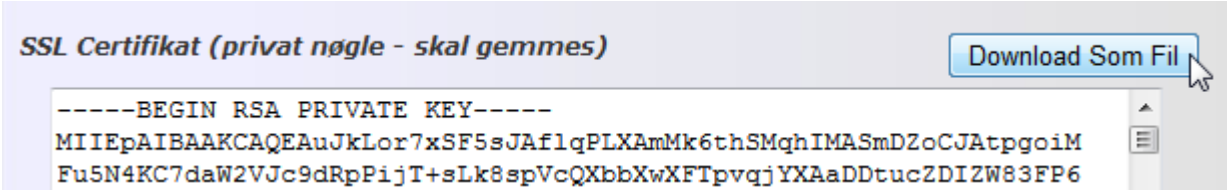
2. Ret Common Name [CN] til din synology's servernavn, eks. synology.fairssl.dk.



3. Ret firmanavn [O], By [L] og Stat [ST].

4. Klik på "Opret Certifikat"

5. Klik på "SSL Certifikat (privat nøgle – skal gemmes) Download Som Fil" knappen.



6. Vælg Gem/Save i din browser, evt. Gem Som og vælg placering og filnavn.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Kopier teksten fra ”Certificate Signing Request (CSR)” tekst feltet, som begynder med -----BEGIN NEW CERTIFICATE REQUEST-----” og indsæt den i din SSL certifikat bestilling.

Når dit certifikat bliver udstedt vil du modtage en tekst eller fil med dit servercertifikat og tilhørende intermediate certifikat (nogle udstedere giver blot et link til hvor man kan hente denne).

Du bør derfør nu have 3 filer (filnavne kan variere) som skal anvendes ved installationen i et PEM BASE64 kodet format.

- Private.key
  Privat certifikat nøgle. Tekst der starter med ”-----BEGIN RSA PRIVATE KEY-----”.

- Server.Certificate.cer
  Indeholde den offentlige del af din servers unikke SSL certifikat. T ekst der starter med ”-----BEGIN CERTIFICATE-----”.

- Intermediate.cer
  Inderholder dit certifikats intermediate (mellemudsteder) certifikat. Tekst der starter med ”----- BEGIN CERTIFICATE-----”.

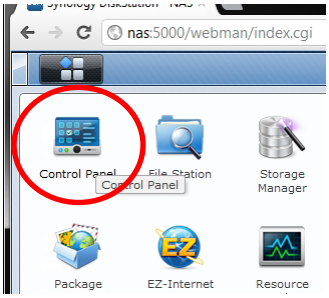
Når du har de 3 filer, er du parat til at installere certifikatet på Synology enheden.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

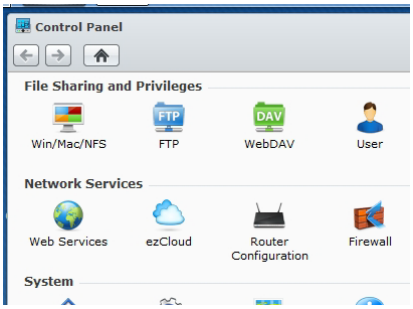
Trin 2: Installation af SSL certifikatet

1. Log ind på Synology Diskstation administrationssiden med en administrator konto

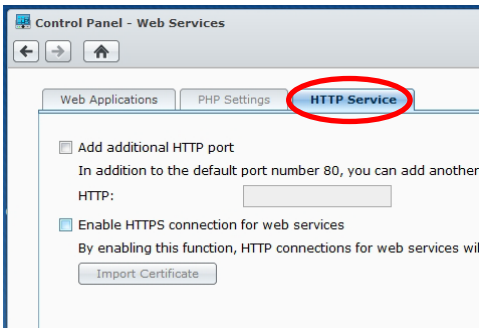
2. Gå ind i ”Control Panel”



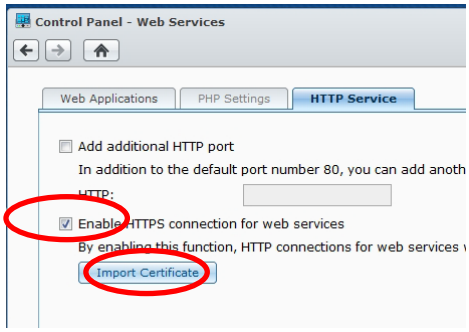
3. I Control Panel, gå ind i ”Web Services”.



4. I Web Services, klik på fanebladet ”HTTP Service”

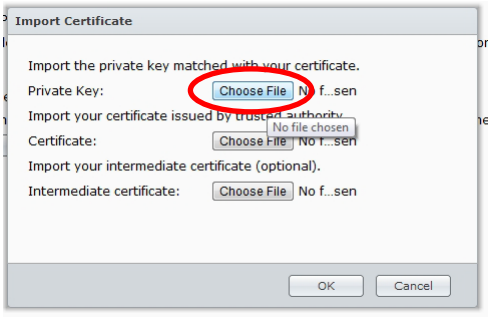


5. Sæt hak i ”Enable HTTPS connection for web services” og klik på knappen “Import Certificate”

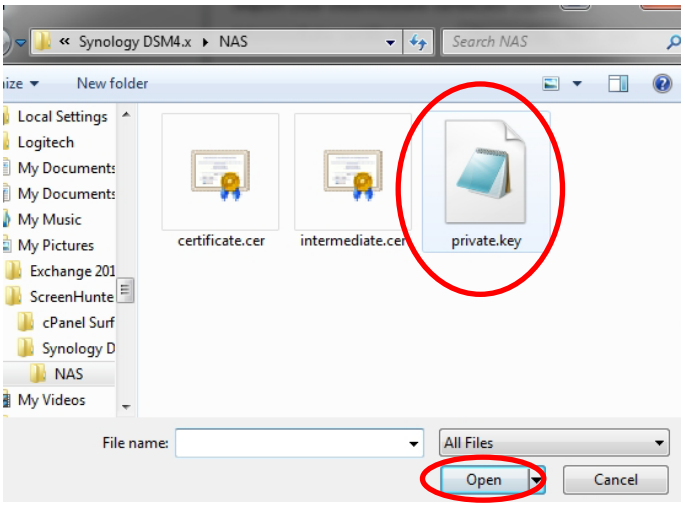


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

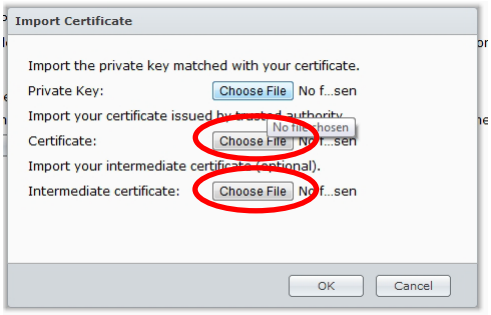
6. I det nye vindue "Import Certificate", klik på "Choose File" knappen ud for "Private Key".



7. I den filmanager som vises, marker den private nøglefil og klik "Open"



8. Gentag trin 6+7 for hhv. "Certificate" og "Intermediate Certificate"



9. Klik "OK" for at lukke vinduet og derefter "Apply" i Control Panel for at gemme instillingerne. Certifikatet er nu installeret og kan testes.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Trin 3: Test certifikatet

1. Gå til www.ssltest.dk og indtast servernavn, kolon og en fra internettet åben port på din Synology boks. Eks. ”ds209.fairssl.dk:5001”

2. Klik på ”Check SSL”.

3. Tilgå din Synology boks direkte via websitet på https://ditservernavn.dk:5001 i en browser