HDN PROXYSERVER WINDOWS

INSTALLATIE HANDLEIDING

HDN Helpdesk – **T**: 0182 – 750 585 **F**: 0182 – 750 589 **M**: helpdesk@hdn.nl

Inhoudsopgave

1. Inleiding

De HDN Proxyserver is ontwikkeld om HDN communicatie met andere systemen middels een proxyfunctie te realiseren.

Het primaire doel van de HDN proxyserver is het filteren, en doorsturen van HDN communicatie. Daarbij wordt meestal de HDN proxyserver in een DMZ geplaatst en de HDN Enterprise in het interne netwerk. De HDN Proxyserver zorgt ervoor dat gescheiden sessies tussen de remote HDN systemen en de interne HDN Enterprise server ontstaan, waarbij bovendien gewaarborgd is dat er in de DMZ geen ont sleutelde data wordt opgeslagen.
De HDN Proxyserver is bovendien in staat om vanaf het Internet binnenkomende HDN berichten naar een specifieke interne HDN Enterprise server door te sturen. Dit gebeurt op basis van het HDN aansluitnummer van de ontvanger, zoals dit in de SOAP header van het bericht is opgenomen.

Het initiatief voor het opzetten van de verbinding kan hierbij intern bij de organisatie liggen, of van een via het Internet binnenkomende verbinding afkomstig zijn.

De HDN Proxyserver controleert of de data die bij de Proxyserver binnenkomt, voldoet aan de gestelde eisen. Dit betekent dat verkeer door de HDN Proxyserver beperkt wordt tot datgene wat expliciet met het HDN berichtenverkeer te maken heeft.

Ook voorziet de HDN Proxyserver in een logfunctie, waarbij zowel het toegestane verkeer, als de geweigerde verbindingen gelogd worden.

De HDN Proxyserver is geschikt voor het afhandelen van zowel de asynchrone- als de synchrone HDN communicatie.

Deze handleiding behandelt de installatie en configuratie van een HDN Proxyserver.

1.1 Het doel van dit document

Dit document heeft tot doel het beschrijven van de installatie alsmede de functionaliteit van de HDN Proxyserver voor Windows. De HDN proxyserver is een front-end proxyserver dat enkel kan worden gebruikt voor communicatie met HDN nodes en de benodigde HDN diensten.

1.2 Doelgroep van dit document

De doelgroep van dit document is een ieder die gebruik wil maken van de HDN proxyserver ten behoeve van de communicatie via het HDN netwerk.

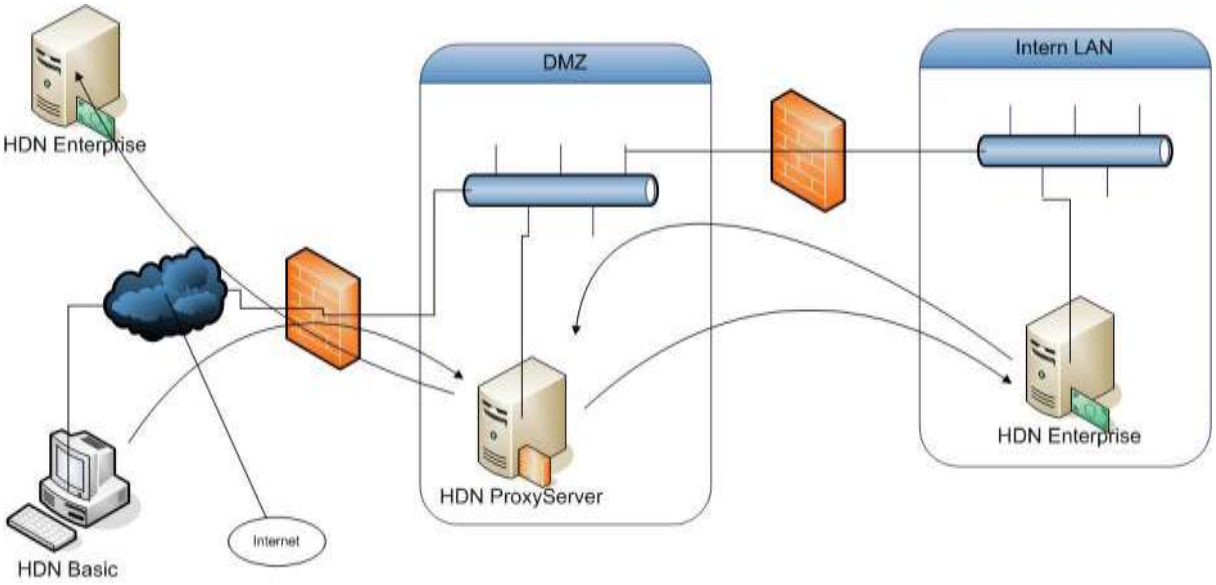
1.3 Reikwijdte

Dit document is beschrijft de installatie en functionaliteit van de HDN Proxy server voor Windows.

Eventuele wijzigingen aan het systeem die noodzakelijk zijn om binnen een beveiligingsbeleid te passen zijn in dit document niet meegenomen.

1.4 Plaats van de HDN Proxyserver

Het doel van de HDN Proxyserver is tweeledig. Ten eerste is deze bedoeld om HDN communicatie mogelijk te maken zonder dat de HDN Enterprise direct aan het internet is gekoppeld. Daarnaast wordt verkeer van een HDN cliënt, komend vanaf het Internet via de HDN proxyserver doorgeleid naar de juiste HDN Enterprise installatie. De HDN proxyserver zal daarom voornamelijk in een DMZ omgeving worden gebruikt zodat de HDN Enterprise niet direct via het internet bereikbaar is. Figuur 1 geeft dit schematisch weer:



Figuur 1 Plaats van de HDN Proxyserver

Uit Figuur 1 blijkt duidelijk dat de HDN Enterprise server nooit een directe verbinding met systemen op het Internet hoeft te hebben. De HDN Proxyserver handelt al het verkeer richting Internet af en zorgt er bovendien voor dat interne IP-adressen voor applicaties op het Internet verborgen blijven.

2. Installatie HDN proxyserver

De HDN Proxyserver kan worden gedownload van de website http://www.hdn.nl onder de Enterprise software.

2.1 Minimale systeem eisen

Om de HDN Proxyserver te kunnen gebruiken dient uw systeem te voldoen aan enkele eisen. Deze vind u hieronder terug.

Het systeem moet draaien op hardware met een i386 of amd64 gebaseerde architectuur.

Daarnaast moet uw systeem aan het volgende voldoen:

2.1.1 Intern geheugen

De HDNProxy software gebruikt als Service 1MB aan intern geheugen. Per simultane verbinding komt hier ca. 1.5 MB aan intern geheugen bij. Voor een systeem dat gedimensioneerd is voor maximaal 30 gelijktijdige sessies, moet dus op een benodigde hoeveelheid intern geheugen van ca. 50 MB gerekend worden.

2.1.2 Vrije schijfruimte

Voor opslag van de HDNProxy software is ca. 6MB vrije schijfruimte benodigd. Daarnaast is ruimte nodig voor opslag van de logbestanden. Het aantal logbestanden is gemaximeerd tot 31. Oude logbestanden worden automatisch overschreven. De benodigde ruimte voor logbestanden is afhankelijk van het niveau waarop gelogd wordt en het aantal sessies dat per dag verwerkt wordt.

2.1.3 Processor capaciteit

De HDNProxy software verricht weinig reken intensieve taken. Voor elke actieve sessie wordt een apart sub-proces gestart. Dit impliceert dat de software goed schaalbaar is, ingeval het systeem over meerdere processorkernen beschikt. De processorcapaciteit zal in de praktijk zelden een bottleneck vormen.

2.1.4 Netwerkadapters

Het verdient de voorkeur om de HDNProxy server met minimaal twee netwerkadapters uit te rusten. Hierdoor is het mogelijk het externe- en interne verkeer over fysiek gescheiden interfaces te laten lopen. Of dit realiseerbaar is, is afhankelijk van de netwerktopologie bij de organisatie waar de HDNProxy server wordt geïnstalleerd.

2.1.5 Netwerksnelheid

Voor een probleemloze werking van de infrastructuur is met name de snelheid van de Internet verbinding en de capaciteit van de interne netwerkinfrastructuur tussen Proxyserver en interne HDN Enterprise server van belang. De benodigde capaciteit is vrijwel uitsluitend afhankelijk van de aantallen berichten en de omvang per bericht van het geen via het HDN netwerk wordt uitgewisseld.

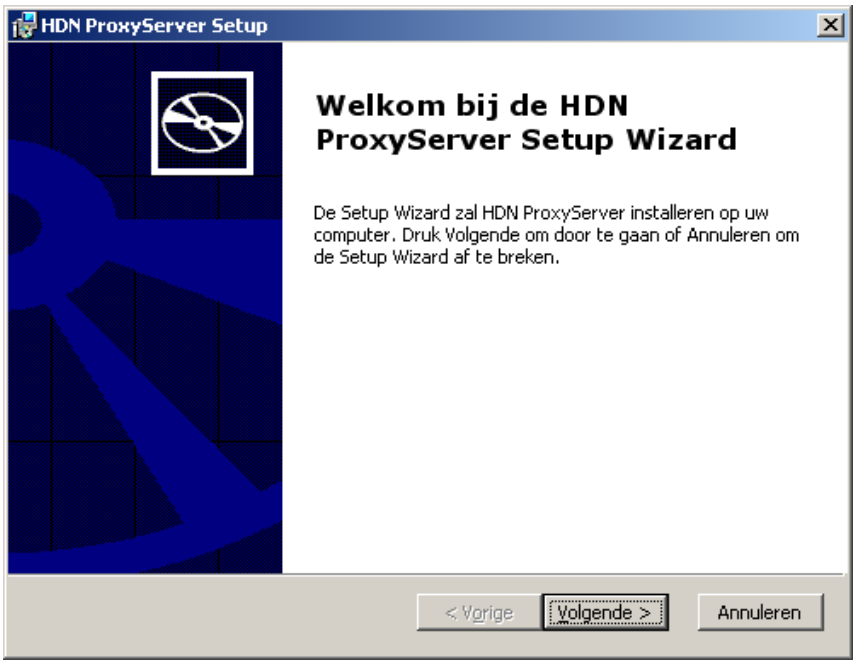
2.1.6 Windows installer 3.0

Om de HDN ProxyServer te kunnen installeren dient minimaal de Windows installer 3.0 geïnstalleerd te zijn op uw systeem.

2.2 Installatie

De HDN ProxyServer software wordt geleverd in de vorm van een installatieprogramma met als naam HDNProxyServer.exe of HDNProxyServer-x64.exe. Door dit programma te starten, zal met de installatie begonnen worden.

De installatieprocedure is zodanig opgezet, dat volstaan kan worden met de default instellingen. Onderstaande schermen geven het verloop van de installatie weer.

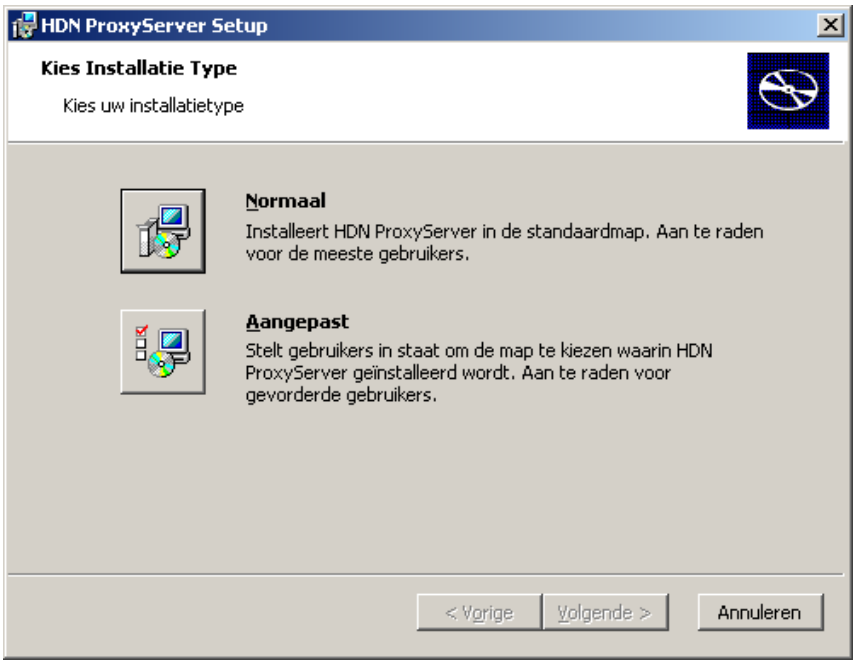


Bij een standaard installatie, zullen de software en configuratiebestanden op locaties geplaatst worden, volgens de richtlijnen van Microsoft.

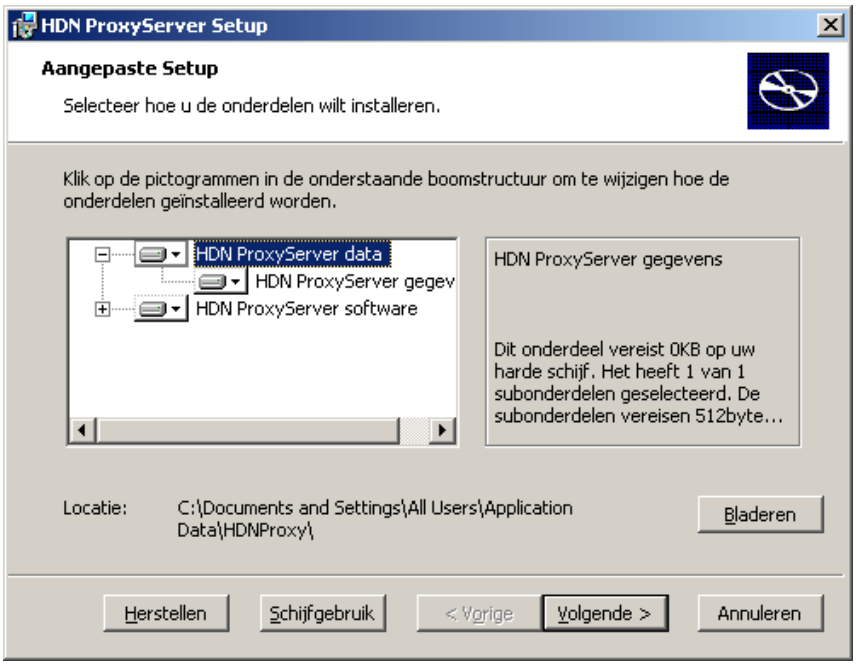
Dit betekent voor de software dat de default installatie directory C:\Program Files\HDNProxy zal zijn.

Voor de configuratie- en logbestanden is dit afhankelijk van het platform waarop de software geïnstalleerd wordt. Onder Windows 7 is dit bijvoorbeeld C:\ProgramData\HDNProxy.

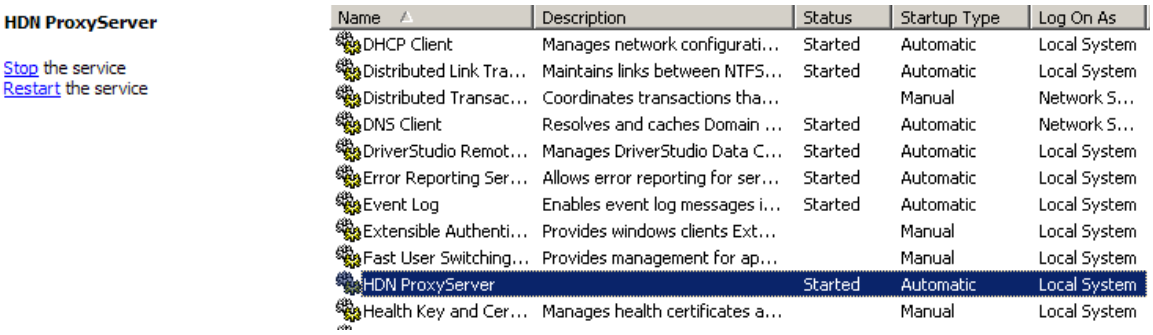
Als u van deze locaties wilt afwijken kunt u, zodra onderstaand scherm getoond wordt, voor "Aangepast" kiezen.



Als u voor het Aangepaste installatietype gekozen heeft, wordt onderstaand scherm getoond, waarbij u de mogelijkheid heeft om voor zowel de programmatuur als de configuratie- en logbestanden een door u gewenste locatie in te stellen.



Zodra de installatie voltooid is, zal de HDN ProxyServer direct als service gestart worden. Onderstaand scherm geeft deze service weer, zoals deze onder de Windows services getoond wordt.



Om te voorkomen dat hierdoor onbedoeld verkeer mogelijk is, worden in de default configuratie uitsluitend verbindingen vanaf de lokale machine geaccepteerd.

2.3 Standaard locaties HDN proxyserver bestanden

Hieronder staan de standaard locaties aangegeven voor de HDN proxyserver bestanden.

[PROGRAMDIR]

Map	Bestand	Beschrijving
asu/		
	ns.wsdl	Service voor Automatische Software Update
certserver/		
	ns.wsdl	CRL distributie/certificaat vernieuwing
hdn/		
	hdnloco.wsdl	Wsdl voor het valideren van HDN loco berichten
	hdnsdn.wsdl	Wsdl voor het valideren van HDN dienst berichten
	hdnws.wsdl	HDN berichtenverkeer waaronder rapportages
README		Document met installatie en configuratie instructies
swpclient/		
	swpublisher.wsdl	Service voor schema updates
bin/		
	hdnproxy.exe	Dit is de HDN proxyserver executable.
	libparms.dll	Leest configuratiedata
	libparms.prm	Gebruikt voor installatie
	libeay32.dll	SSL library
	ssleay32.dll	SSL library
	proxyhelper.dll	Gebruikt voor installatie
	cs2pem.exe	Dit programma converteert de certificaten uit de Windows certstore naar een pem bestand. Wordt automatisch uitgevoerd.
	Openssl.exe	

[DATADIR]

Map	Bestand	Beschrijving
etc/		
	hdnproxy.prm	Dit is het configuratiebestand voor de HDN proxyserver.
	logd.prm	Dit is het configuratiebestand voor de logdeamon
	Cacerts.pem	Bestand met certificaten uit Windows certificaat store.
log/		
	*.log	Logbestand voor de HDN proxyserver.

3. HDN proxyserver configureren

Nadat de HDN proxyserver is geïnstalleerd dienen aanpassingen gemaakt te worden in de hdnproxy.prm. Het betreft hier dan het instellen van poorten, ip adressen en eventueel het loglevel.

De hdnproxy.prm is standaard te vinden in [DATADIR]\etc. Na het aanpassen van de parameters dient de hdn proxy opnieuw gestart te worden.

3.1 Loglevel

Het is mogelijk binnen de HDN proxyserver het loglevel aan te passen. In Tabel 1 zijn de waarden weergegeven die kunnen worden toegekend aan het loglevel

Parameter	Beschrijving	Default
Loglevel		3
	0 Alleen fatale fouten 1 Ook foutmeldingen 2 Ook waarschuwingen 3 Ook info meldingen 4 Ook debug meldingen	

Tabel 1 Loglevel hdnproxy.prm

3.2 Time-outs

Om te voorkomen dat verbinding open blijven staan kent de HDN proxyserver diverse time-outs. In Tabel 2 worden de standaard time-outs weergegeven.

Parameter	Beschrijving	Default
AcceptTimeout	Dit is de intervaltijd, opgegeven in seconden waarmee de Service zal wachten op binnenkomende verbindingen. Deze tijd is ook de maximale tijd die er kan verstrijken als de gebruiker de service probeert te stoppen.	10
MaxConcurrent	Het maximaal aantal gelijktijdige sessies dat de service ondersteunt. Default staat deze parameter ingesteld op een maximum van 10 gelijktijdige sessies. Het is ook mogelijk deze limitering uit te schakelen, door deze parameter een waarde 0 te geven.	50
ReceiveTimeout	Hier wordt de timeout, uitgedrukt in seconden, opgegeven dat de Service wacht op data van hetzij de client die de verbinding heeft opgezet danwel de server waarmee een verbinding gemaakt is.	300

Tabel 2 Time-outs hdnproxy.prm

3.3 Uitgaande verbindingen

In Tabel 3 zijn de parameters weergegeven voor uitgaande verbindingen. Het betreft hier de outbound communicatie tussen de HDN Enterprise en de HDN proxyserver.

Parameter	Beschrijving	Default
ListenPort	Dit is het TCP poortnummer waarop de Service wacht op binnenkomende verbindingen. Poortnummer waarop uitgaande verbindingen binnenkomen	8888
ListenAddress	Hier kan een lijst van IP-adressen worden opgegeven waarop de Service zal luisteren naar binnenkomende verbindingen vanaf het interne LAN. Default staat hier localhost ingevuld. Deze parameter herkent zowel hostnamen, als IP-adressen. Wel moeten de opgegeven adressen c.q. hostnamen lokaal op de machine waar de HDN proxyserver gestart wordt beschikbaar zijn. Als meer dan één adres wordt opgegeven, moeten de verschillende adressen door een komma gescheiden zijn. Bijvoorbeeld: ListenAddress=localhost,192.168.1.34	127.0.0.1

Tabel 3 Uitgaande verbinding hdnproxy.prm

3.4 Inkomende verbindingen

In Tabel 4 zijn de parameters weergegeven voor inkomende verbindingen. Het betreft hier de inbound communicatie tussen de HDN nodes op de WAN interface en de HDN proxyserver.

Parameter	Beschrijving	Default
ExternalAddress	Het externe IP adres van de HDN proxyserver waarop verbindingen vanaf het Internet geaccepteerd mogen worden.	0.0.0.0
AsyncListenPort	Het TCP poortnummer waarop de HDN proxyserver asynchrone HDN berichten vanaf het Internet binnenkrijgt. Wanneer deze poort de waarde 0 heeft, zal er geen listener voor asynchrone berichten gestart worden.	0
SyncListenPort	Het TCP poortnummer waarop de HDN proxyserver synchrone HDN berichten vanaf het Internet binnenkrijgt. Wanneer deze poort de waarde 0 heeft, zal er geen listener voor synchrone berichten gestart worden.	0
AsyncForwardHost	De hostnaam, of het IP-adres van de interne HDN Enterprise server waar de HDN proxyserver binnenkomende asynchrone berichten naar moet doorsturen.	
SyncForwardHost	De hostnaam, of het IP-adres van de interne HDN Enterprise server waar de HDN proxyserver binnenkomende synchrone berichten naar moet doorsturen.	
SyncForwardPort	Het TCP poortnummer op de interne HDN Enterprise server waar binnenkomende synchrone HDN berichten naar doorgestuurd moeten worden.	0

Tabel 4 Inkomende verbindingen hdnproxy.prm

Het is mogelijk om de asynchrone en synchrone berichten naar één interne HDN Enterprise server door te sturen, of naar twee verschillende machines. Ingeval beide berichtsoorten naar één machine doorgestuurd worden, is het van belang dat de parameters SyncForwardPort en AsyncForwardPort niet dezelfde waarde hebben.

3.5 TLS instellingen

HDN maakt gebruik van end-to-end encryptie. Vanaf HDN 7.0 is het mogelijk om naast deze end-to-end encryptie ook transport encryptie te gebruiken (TLS). Uitgangspunt voor de TLS verbinding is het realiseren van 'Perfect Forward Secrecy'.

De HDN software accepteert alleen TLSv1.2. Verder wordt gebruik gemaakt van ECDH key exchange. Indien via de HDN Enterprise geconfigureerd is dat een aansluitnummer/endpoint gebruik maakt van HTTPS en een HDN proxy server geconfigureerd is dan moet de HDN proxy voor HTTPS geconfigureerd worden. Voor gebruik van HTTPS zijn geen andere poorten benodigd. De HDN proxy server detecteert zelf of een inkomende verbinding http of HTTPS is.

Parameter	Beschrijving	Default
CertKeyFile	Het externe IP adres van de HDN proxyserver waarop verbindingen vanaf het Internet geaccepteerd mogen worden.	
CertKeyPassword	Het TCP poortnummer waarop de HDN proxyserver asynchrone HDN berichten vanaf het Internet binnenkrijgt. Wanneer deze poort de waarde 0 heeft, zal er geen listener voor asynchrone berichten gestart worden.	

Tabel 5 TLS instellingen hdnproxy.prm

Het certificaat waarnaar gerefereerd wordt in CertKeyFile dient in PEM format te zijn en dient zowel het server certificaat, uitgever certificaat als de private key te bevatten. De volgorde van de certificaten moet zoals onderstaand zijn:

```
-----BEGIN CERTIFICATE-----
[server certificaat]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[optioneel - intermediate CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[CA certificate]
-----END CERTIFICATE-----
-----BEGIN EC PRIVATE KEY-----
[private key]
-----END EC PRIVATE KEY-----
```

De private key mag een RSA of EC key zijn.

3.6 Beveiliging instellingen

Het is mogelijk beveiliging instellingen aan te passen waaronder het level waarop validatie moet plaatsvinden. In Tabel 6 zijn de diverse parameters weergegeven.

Parameter	Beschrijving	Default
SecurityLevel	0 - Geen controle. Accepteer elke verbinding 1 - Berichten moeten een HTTP header bevatten en een correcte gSOAP user-agent string hebben.	3

	2 - Het bericht moet een geldige SOAP Envelope hebben 3 - De SOAP Body moet overeenkomen met een bericht waarvan de WSDL is toegestaan in deze configuratie.	
SupportCerts	Hier wordt aangegeven of de Service sessies naar de certificaatserver moet toestaan. Default heeft deze parameter de waarde 1. Toegang naar de certificaat kan uitgeschakeld worden door deze parameter de waarde 0 te geven. Deze parameter heeft uitsluitend een functie, als het SecurityLevel minimaal op niveau 2 staat ingesteld.	1
SupportSchemas	Hier wordt aangegeven of de Service sessies naar de Schema update server moet toestaan. Default heeft deze parameter de waarde 1. Schema updates kunnen uitgeschakeld worden door deze parameter de waarde 0 te geven. Deze parameter heeft uitsluitend een functie, als het SecurityLevel minimaal op niveau 2 staat ingesteld.	1
SupportAsu	Hier wordt aangegeven of de Service sessies naar de ASU server moet toestaan. Default heeft deze parameter de waarde 1. ASU kan uitgeschakeld worden door deze parameter de waarde 0 te geven. Deze parameter heeft uitsluitend een functie, als het SecurityLevel minimaal op niveau 2 staat ingesteld	1
SupportHDN	Hier wordt aangegeven of de Service uitgaande HDN berichten moet toestaan. Default heeft deze parameter de waarde 1. HDN berichten kunnen uitgeschakeld worden door deze parameter de waarde 0 te geven. Deze parameter heeft uitsluitend een functie, als het SecurityLevel minimaal op niveau 2 staat ingesteld.	1

Tabel 6 Beveliging instellingen hdnproxy.prm

3.7 Meer dan één Enterprise server

Het is mogelijk op het interne netwerk meer dan één HDN Enterprise server te configureren. Binnenkomende berichten worden in dat geval verdeeld over de geconfigureerde Enterprise servers aan de hand van het ontvanger HDN aansluitnummer, zoals dit in de SOAP Header van het bericht is opgenomen. Om deze functie te kunnen gebruiken, is het noodzakelijk de HDN Proxyserver op Security niveau 3 in te stellen. Dit is tevens het hoogste niveau. De reden hiervoor is dat het afzender- en ontvanger nummer deel uitmaken van de SOAP Header. Deze Header wordt pas op niveau 3 geïnspecteerd. Op lagere niveaus is het doel aansluitnummer dus niet beschikbaar. Voor elke Enterprise server moet een configuratiebestand gemaakt worden en in de nodes directory worden geplaatst. De naam van dit bestand is niet relevant. De extensie is wel verplicht en moet .prm zijn. In onderstaand voorbeeld is een configuratie voor een Enterprise server met aansluitnummer 200000 gemaakt.

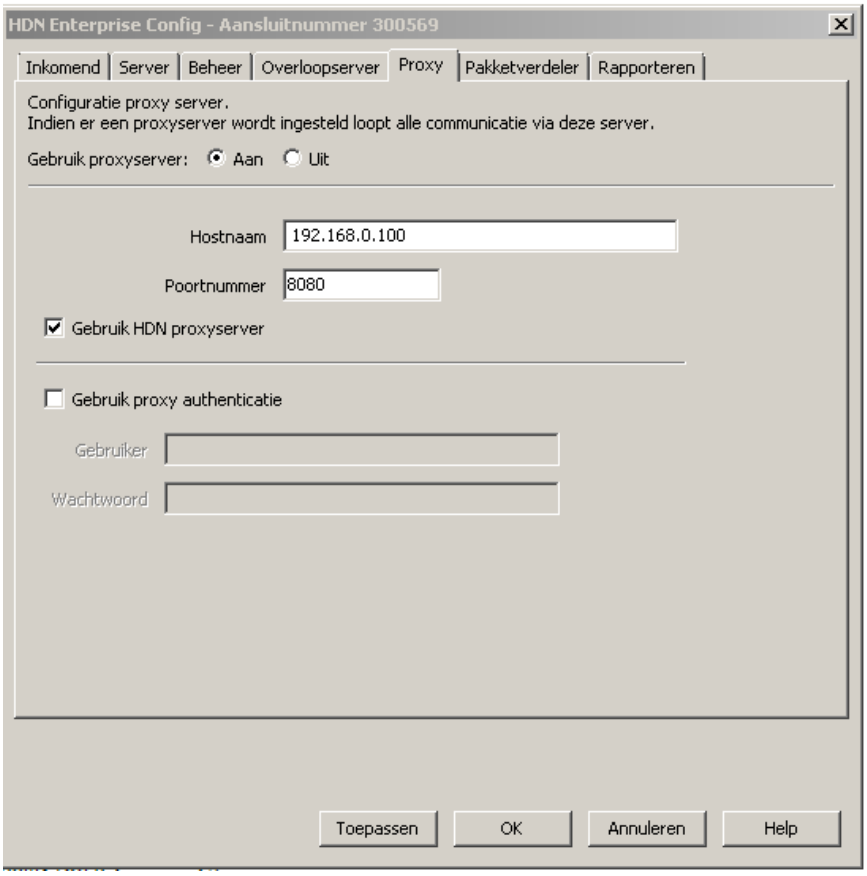
aansluitNummer=200000
AsyncForwardHost=192.168.1.3
AsyncForwardPort=8888

Berichten die ontvangen worden en bestemd zijn voor aansluitNummer 200000, zullen naar de opgegeven locatie worden doorgestuurd. In dit geval is dit 192.168.1.3:8888. Berichten die voor een ander aansluit nummer bedoeld zijn, worden doorgestuurd naar de AsyncForwardHost op de AsyncForwardPort, zoals in het basis configuratiebestand [DATADIR]\ etc\hdnproxy.prm is

opgegeven. De instellingen in het basis configuratiebestand fungeren in dit geval dus als default route naar een interne HDN Enterprise server. In de [DATADIR]\etc\nodes\ directory kunnen net zoveel configuratiebestanden voor specifieke HDN Enterprise server worden geplaatst, als gewenst is.

4. Instellen proxyserver op een HDN Enterprise of HDN Basic

Het is mogelijk om via de HDN configuratie een proxyserver op te geven. De HDN configuratie kan worden gevonden in de bin map van de HDN programma directory. In Figuur 2 is de HDN configuratie zichtbaar voor zowel de Windows als Linux variant.



Figuur 2 HDN Configuratie - Windows en Linux

Om de Proxyserver in te stellen dient u "Gebruik proxyserver" op aan te zetten. Hierdoor komen de invoer velden beschikbaar.

Parameter	Omschrijving
Hostnaam	Bij Hostnaam vult u de FQDN (Fully qualified domain name) of het IP adres van de proxyserver in.
Poortnummer	Hier geeft u het poortnummer op dat u hebt ingesteld bij de parameter listenport in de hdnproxy.prm .
Gebruik HDN proxyserver	Hiermee kunt u aangeven of de proxyserver een HDN proxyserver is. Dit is van belang omdat de HDN proxyserver dient als SSL endpoint.
Gebruik authenticatie	Wanneer u deze inschakelt kunt u een gebruikersnaam en wachtwoord opgeven voor proxy authenticatie. Deze optie kan niet worden gebruikt in combinatie met een HDN proxyserver.

Gebruiker	Hier geeft u de gebruikersnaam in van het account dat dient te worden geauthentiseerd voor communicatie via de proxyserver.
Wachtwoord	Hier geeft u het wachtwoord op dat is benodigd voor de eerder opgegeven gebruikersnaam.

4.1 Configureren ASU software

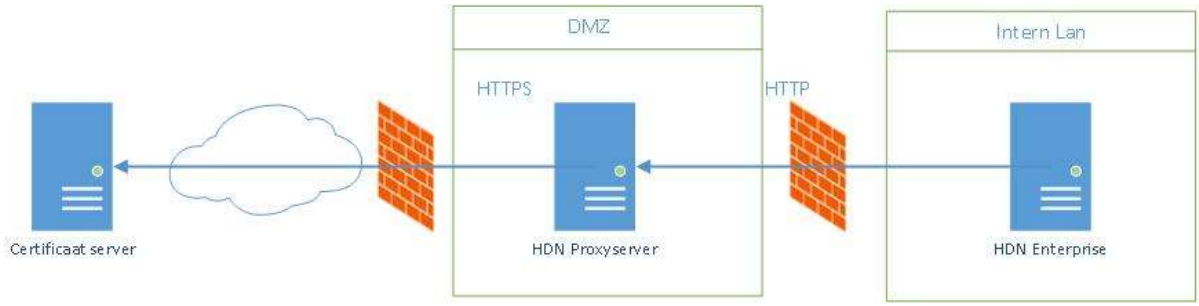
De ASU software werkt onafhankelijk van de HDN communicatiesoftware. Als het gewenst is de ASU software ook via de HDN proxyserver te laten communiceren, moet aan de ASU configuratie ook een proxy.prm bestand worden toegevoegd. Dit bestand moet geplaatst worden in de directory [DATADIR]/CS Engineering/ASU/. Hiervoor kunt u het bestand gebruiken dat via de HDN configuratie is verkregen. Deze is te vinden op de volgende locatie [DATADIR]/etc/hdn/proxy.prm.

5. SSL

Sinds HDN 5.1.1.2 wordt voor communicatie met de certificaatserver gebruik gemaakt van SSL. In het geval van de HDN proxyserver zal deze fungeren als SSL endpoint. Dit betekent dat de communicatie tussen de HDN proxyserver en HDN Enterprise via het normale http protocol verloopt. De HDN proxyserver zet vervolgens een SSL connectie op naar de server.

Om te bepalen of een SSL certificaat geldig is wordt gebruik gemaakt van het bestand cacerts.pem. Via het programma cs2pem.exe worden de certificaten uit de Windows certificaten store omgezet naar het eerder genoemde pem bestand.

In Figuur 3 is weergegeven hoe de communicatie via de HDN proxyserver naar de certificaat server verloopt.



Figuur 3 SSL communicatie

De HDN Enterprise zet een http verbinding op de HDN proxyserver. Deze proxyserver zet vervolgens een https verbinding op met de certificaat server. Hierdoor zijn bijvoorbeeld gegevens die worden opgegeven voor een certificaat aanvraag na de HDN proxyserver versleuteld.

6. Logging

De HDN proxyserver schrijft logmeldingen in een logbestand dat in de [DATADIR]/log directory geplaatst wordt. Hierbij is [DATADIR] de naam van de directory die tijdens installatie van de software is opgegeven als locatie waar configuratie- en logbestanden geplaatst moeten worden.

De naam van het logbestand is LGFILExx.TXT. Hierbij is xx het nummer van de huidige dag. De logdata wordt dus elke dag in een ander bestand geschreven. Als bij het wisselen van dag naar een ander logbestand overgegaan wordt, zal een eventueel al aanwezig bestand gewist worden.

Hiermee wordt bereikt dat de maximale omvang van historische logdata beperkt blijft tot maximaal de laatste 31 dagen.

6.1 Logmeldingen

De HDN proxyserver kent diverse logmeldingen. Deze zijn

Level	Melding	Oorzaak
Fatal	Unable to open WSDL file	
Fatal	No IP ListenAddress specified in hdnproxy.prm	De Service kan niet gestart worden, doordat niet tenminste 1 IP-adres is opgegeven. Pas het configuratiebestand hdnproxy.prm aan.
Fatal	HDN ProxyServer stopped due to fatal error	Deze foutmelding wordt gegeven als er een interne fout geconstateerd wordt, waardoor verdere werking niet mogelijk is. Bij deze melding kan een foutcode gelogd worden.
Fatal	Cse exception: e=%s	
Fatal	Unable to reuse socket for listening	
Fatal	Unable to create synchronisation event	
Fatal	Unable to listen for connection	
Fatal	Unable to bind socket to listener port	Deze foutmelding wordt gegeven als de HDN proxyserver zich niet aan de ingestelde TCP poort kan koppelen. Mogelijk is de opgegeven poort als door een ander proces in gebruik. Ook kan het zijn dat in het configuratiebestand HDNProxy.prm een verkeerd poortnummer is opgegeven.
Fatal	Unable to listen for connection	
Fatal	Invalid configuration	Er is bij het starten van de Service een fout in het configuratiebestand gedetecteerd. Als gevolg daarvan kan de software niet gestart worden. De regel vlak voor deze melding, geeft informatie omtrent het gedetecteerde conflict.
Error	Unable to open WSDL file. filename=%s	Een WSDL bestand kon niet gelezen worden. Controleer of het opgegeven bestand bestaat en door de Service gelezen mag worden.
Error	Unable to create target socket	Er kan geen verbinding met het doelsysteem gemaakt worden. De oorzaak is een fout waardoor op het systeem geen nieuwe TCP sockets gemaakt kunnen worden. Een mogelijke oorzaak is een tekort aan Windows resources.
Error	Unable to resolve target host. host=%s	In het hdnproxy.prm bestand is bij de parameter ListenAddress een hostnaam opgegeven, waar geen IP-adres bij gevonden kan worden.

		Controleer of in de ingevoerde hostnaam geen typefout zit. Ook is het mogelijk dat de HDN proxyserver geen verbinding kan maken met de DNS server waar deze hostnaam in opgegeven is.
Error	Unable to resolve target system	
Error	Select failed	
Error	Client request Is invalid	
Error	Unable to send data to target host	
Error	Unable to read data from target	
Error	Unable to send data to client	
Error	Unhandled exception. file=%s line=%d	
Error	Error initializing winsock	Er kan geen nieuwe sessie gestart worden, doordat de communicatie met de socket component niet geïnitialiseerd kon worden.
Error	Error duplicating socket	Er kan geen nieuwe sessie gestart worden. Een mogelijke oorzaak is een te kort aan Windows resources.
Error	Could not obtain handle to synchronisation event	
Error	Unable to initialize winsock. Error=%d	
Error	Unable to resolve hostname. name=%s	
Error	Accept failed. errnum=%d	
Error	Wait failed. Error=0x%x	
Error	Insufficient memory to allocate %d bytes	
Error	Specific forwarding requires SecurityLevel 3	Er zijn één of meer parameterbestanden in de nodes/ directory gevonden. Het SecurityLevel in hdnproxy.prm staat echter op een lager niveau dan 3 ingesteld.
Warning	Header validation failed at level %d	Er is een sessie gestart naar de HDN ProxyServer met andere software als de HDN communicatieserver, of de HDN ProxyServer staat geblokkeerd voor het protocol dat gebruikt wordt. ASU staat bijvoorbeeld geblokkeerd en de ASU software is toch aktief en probeert verbinding met de ASU server te maken.
Warning	Session dropped. Not enough memory available. active=%d freemem=%d	Deze melding wordt gegeven als de MaxConcurrent parameter in het hdnproxy.prm bestand staat ingesteld op een minimaal benodigde hoeveelheid vrij intern geheugen en er is op dat moment minder dan het opgegeven minimum beschikbaar.
Warning	Unknown event 0x%x	
Warning	Session dropped. Session limit reached. limit=%d	Als de MaxConcurrent parameter in het hdnproxy.prm bestand staat ingesteld op een maximum aantal gelijktijdige sessies en dit aantal is bereikt, dan wordt deze melding gegeven.
Warning	Trying to connect to target %s:%d	Het tot stand brengen van een verbinding met het doelsysteem is mislukt.

		Mogelijke oorzaken zijn bijvoorbeeld een doelsysteem dat tijdelijk niet bereikbaar is of een probleem met netwerkinstellingen. Aanvullend wordt een extra foutmelding gelogd met daarin de Windows foutcode. Deze foutcode kan extra informatie over de oorzaak van deze foutsituatie geven.
Warning	Unable to connect to target %d:%d	
Warning	No target tag in message	
Info	Forwarding to %d specific Enterprise systems	Informatief met het weergegeven getal wordt het aantal .prm bestanden getoond, dat in de nodes/ directory aangetroffen is.
Info	Bind to %s:%d	
Info	Connected to target %s:%d	Er is verbinding met het doelsysteem tot stand gebracht. Het IP-adres en remote poortnummer wordt gelogd.
Info	Found %d SOAP Services	
Info	Start HDN ProxyServer at security level %d	Informatief. Gelogd wordt het niveau waarop de service gestart is.
Info	Connection closed. fromClient=%d fromTarget=%d	De sessie tussen cliënt en het doelsysteem is beëindigd. Deze melding geeft het aantal bytes weer dat verstuurd en ontvangen is.
Info	Stop service on request	
Info	Incoming connect. ip=%s type=%d active=%d	Er is een verbindingsverzoek binnengekomen. Het remote IP-adres wordt gelogd. Het type van de verbinding geeft aan om wat voor soort verbinding het gaat: 0 – Verbinding vanaf het Internet op de asynchrone poort 1 – Verbinding vanaf het Internet op de synchrone poort 2 en hoger – Verbinding vanaf één van de interfaces naar het interne LAN. Ook wordt gelogd hoeveel gelijktijdige sessies er op dat moment zijn.
Info	Entering Run Service	
Debug	Trying to connect to target %s:%d	
Debug	CheckHeaders %s	
Debug	CheckEnvelope %s	
Debug	ChecksoapService %s	
Debug	Waiting %d seconds on socket %d	
Debug	Randomized table of IP-addresses. Size=%d	
Debug	Trying random endpoint %s	
Debug	Message for target %s	
Debug	Forwarding to specific host %d:%d	
Debug	Received from socket bytes=%d inFrame=%d	
Debug	Partial data still in buffer. remainder=%d	
Debug	Sent to target %d bytes	
Debug	Found %s	Melding van een geconfigureerde service naam.

Debug	Sent to client %d bytes	
Debug	Signal parent process	
Debug	Accepting call on socket	
Debug	Waiting for clients. timeout=%d sec	
Debug	Starting child. Active=%d clientsock=%d	
Debug	Socket and type inherited from parent. sock=%d type=%d	
Debug	Handle service event	

7. Index