Navision Stat 11.4

BIA/TJO/ANHCH
19.11.2024

Installationsvejledning til eDelivery-integration

Overblik

Formål
Dokumentet beskriver hvorledes hostere opsætter og konfigurerer servere således at eDelivery implementeringen i NS 11.2 kan anvendes, med henblik på at efterkomme ny afsendelsesmetode for elektroniske dokumenter.

Indholdsfortegnelse

Målgruppe
Hostere af Navision Stat databaser

Hvorfor er det vigtigt?
eDelivery er nødvendig for at kunne sende og modtage elektroniske dokumenter.

Copyright

Seneste ændring
Publiceret første gang: 02-10-2023
Seneste ændring: 19-11-2024

Beskrivelse

Roller

Rettighed	Beskrivelse
NS_OPS_INTEGRATION	Rettighedssættet giver rettigheder til at foretage opsætninger i forbindelse med elektronisk fakturering, ØDUP, NAS og XML broer m.m.

Se yderligere **Brugervejledning til Brugeradministration**, for en mere specifik beskrivelse af ovenstående roller.

Opbygning og komponenter

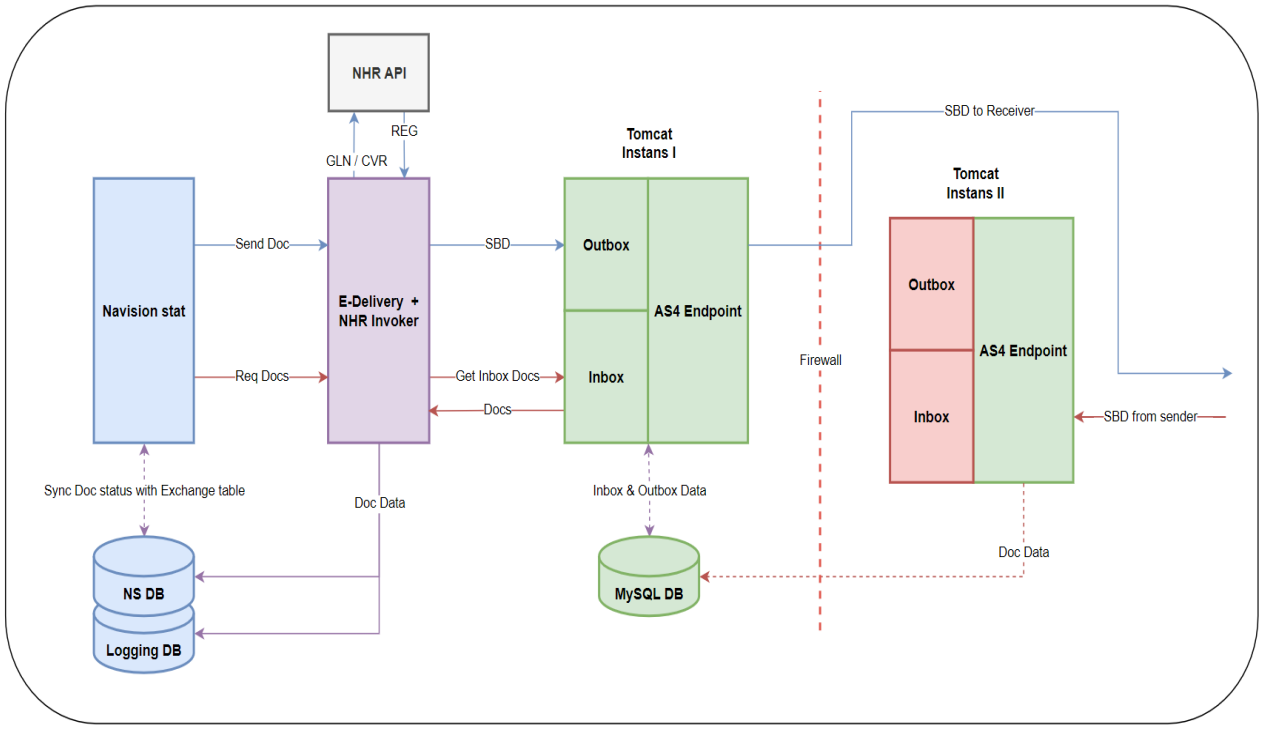
Overgangen til eDelivery indebærer en række ændringer i Navision Stat, samt tilføjelser til løsningens eksterne komponenter. Dette er for at understøtte kommunikationen med den referenceimplementering som Erhvervsstyrelsen har udgivet.

Det er derfor nødvendigt for hostere at opgradere til *minimum* NS 11.2, for at kommunikationen mellem NS og referenceimplementeringen, og altså afsendelse af elektroniske dokumenter via eDelivery, kan understøttes.

Ud over den obligatoriske opgradering, indebærer overgangen ligeledes en opsætning af ikke bare én, men to servere med Tomcat hos hosteren selv. Dette skyldes for det første at referenceimplementeringen er udviklet i Java, og for det andet en nødvendighed for ekstra sikring af kommunikationen mellem endpoints.

Èn af de opsatte servere skal ligeledes have en MySQL databaseserver, som implementeringen anvender under modtagelse, afsendelse og logning af elektroniske dokumenter.

På næste side ses en figur som illustrerer sammenhængen mellem løsningens komponenter.



Figur 1: Oversigt over komponenter i eDelivery-implementering for Navision Stat, samt disses tekniske relationer. Her bemærkes den dobbelte Tomcat instans af forskellig opsætning på hvv. den indre og ydre side af firewall.

Her ses hvordan afsendelse af dokumenter starter i Navision Stat. Det resulterende XML-dokument omformes af den nyudviklede eDelivery invoker, som blandt andet slår op i NHR API for at finde profiler for modtageren.

Derefter dannes en HTML POST request, som indeholder en såkaldt SBD (Standard business dokument) hvilket involverer en header med metadata, samt selve dokumentet som payload. Endpointet er her vores **indre** Tomcat instans' Outbox.
Hvis alt forløber korrekt, vil dokumentet (SBD) blive afsendt via AS4 endpointet til modtageren. Bemærk her hvordan den ydre Tomcat instans ikke er i spil under afsendelse.

Ved modtagelse, derimod, kan der udelukkende sendes til den ydre Tomcat instans' AS4 endpoint. Dette er for at forhindre uvedkommende at kalde vores in – og outbox, som vi af sikkerhedsmæssige årsager har placeret inden for vores firewall.

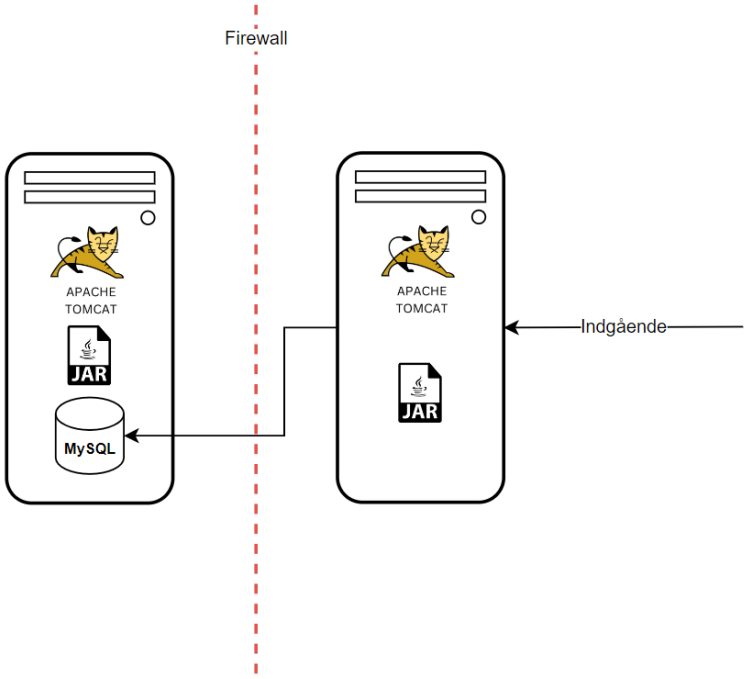
Indgående dokumenters data indsættes i den opsatte MySQL database som befinder sig inden for firewall. Her kan vores indre instans efterfølgende frit tilgå data, når modtagne dokumenter skal indlæses fra inbox. Bemærk her hvordan en

indlæsning af dokumenter starter med et aktivt kald fra Navision Stat til eDelivery-invokeren, og hvordan disses data lægges i 2 forskellige NS databaser. Til installationen er der anvendt Windows Server 2022.

Opsætning

Efter opgradering til NS 11.2, skal der foretages følgende opsætninger fra hosterens side:

1. **Installation af**
   - 1.1. Java 8 JDK
   - 1.2. Apache Tomcat
   - 1.3. MySQL
   - 1.4. Keystore program
   - 1.5. eDelivery invoker
   - 1.6. Program til hashing af password
2. **Oprettelse af**
   - 2.1. MySQL Database
   - 2.2. MySQL Databasebruger
   - 2.3. MySQL Schema til Oxalis
   - 2.4. Oxalis API bruger
3. **Konfiguration af**
   - 3.1. Installationspakker
   - 3.2. Java Keystore til SSL certifikatet
   - 3.3. Java Keystore til MitID erhverv systemcertifikat (OCES-III)
   - 3.4. Tomcat anvendelse af TLS (Transport Layer Security)
   - 3.5. Oxalis Webservice
   - 3.6. Oxalis Webside
   - 3.7. Oxalis Logning
4. **Åbninger af porte i firewall (ekstern og intern webserver)**



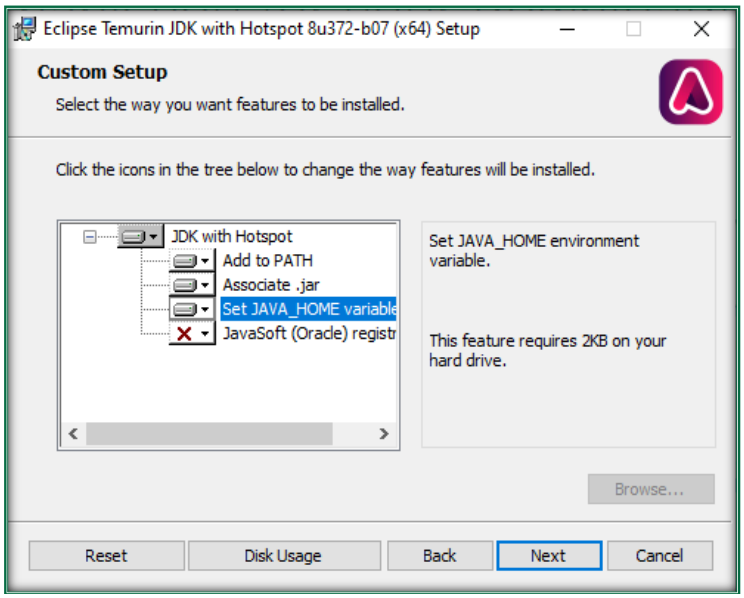
Figur 2: Illustration af den ønskede arkitektoniske opbygning for indgående dokumenter

Installation

Installation af: Java

Vær opmærksom på at Java fra Oracle er et licenseret produkt og dermed koster penge.
Derfor anbefales det at installere en open-source udgave som f.eks. OpenJava, som kan findes her:
https://adoptium.net/temurin/releases/?version=8

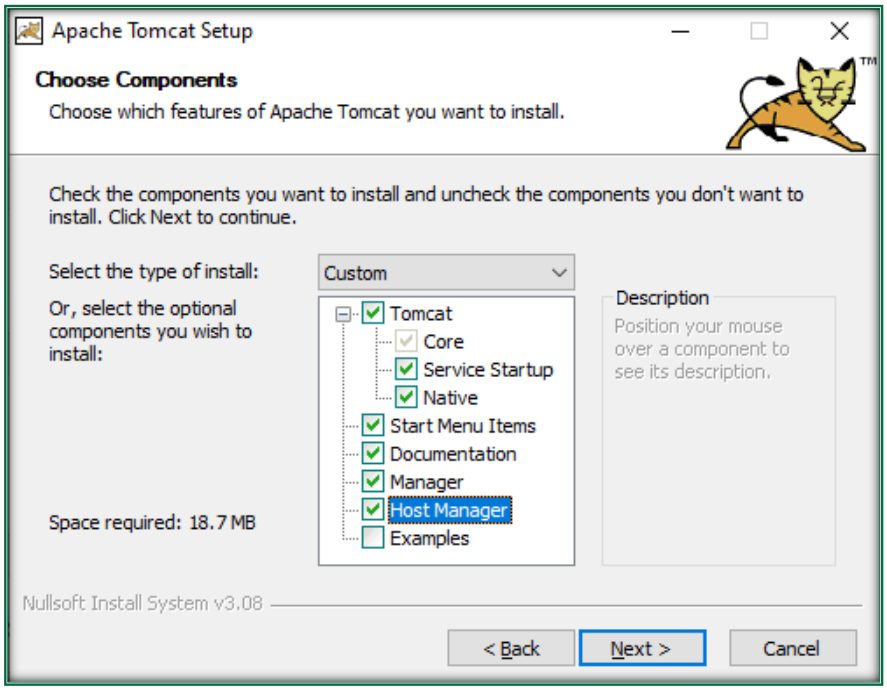
Vælg det rigtige operativsystem og arkitektur, og download .msi filen (buildnummeret kan afvige fra nedenstående, men skal være minimum 252).
Under installationen så vælg at "Set JAVA_HOME" variable skal installeres.



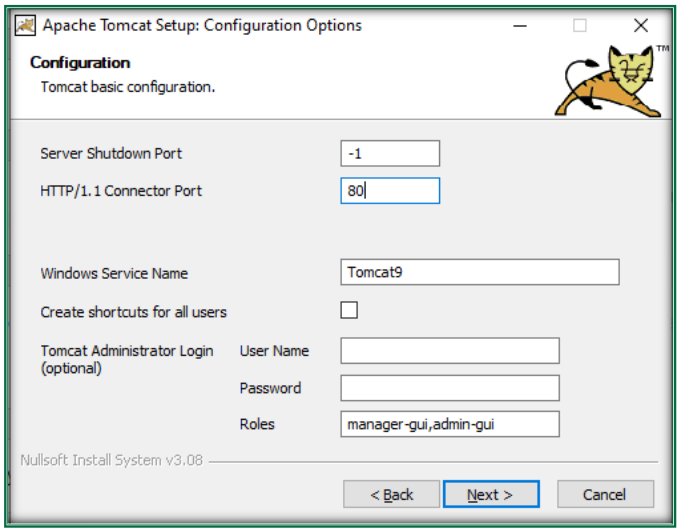
Installation af Apache Tomcat

Til installationen skal anvendes Apache Tomcat som er en Java webserver.
Der skal anvendes version 9 som kan hentes her:
[Apache Tomcat® - Apache Tomcat 9 Software Downloads]

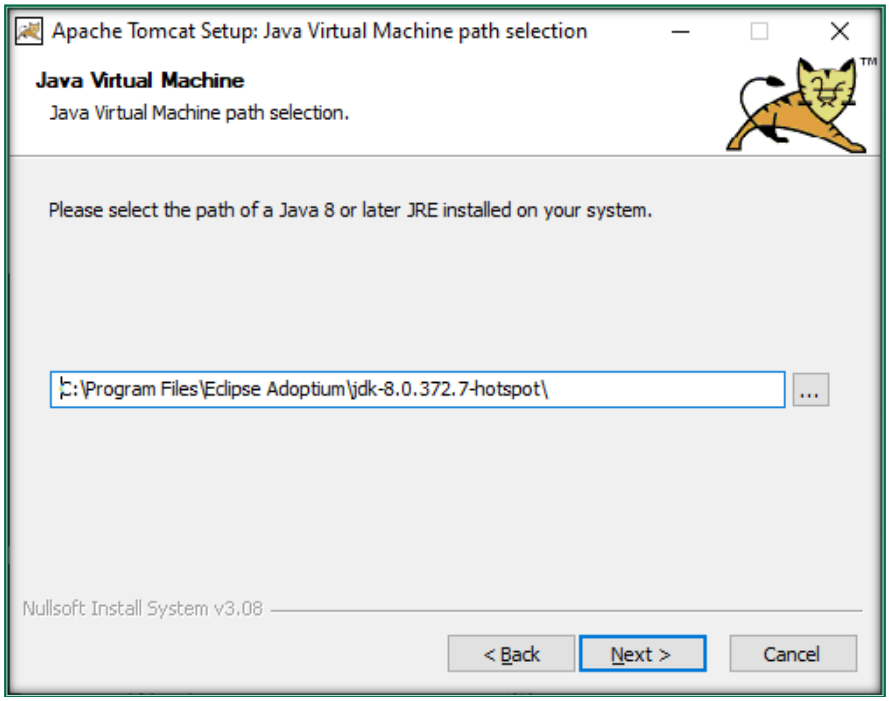
Vælg 32-bit/64-bit Windows Service Installer installationsfilen.
Vælg følgende komponenter:



Ændr http/1.1 Connector Port til 80 og angiv et brugernavn og et stærkt password under Tomcat Administrator Login:



Hvis Java er installeret, vil den selv finde stien, ellers skal du selv angive den:



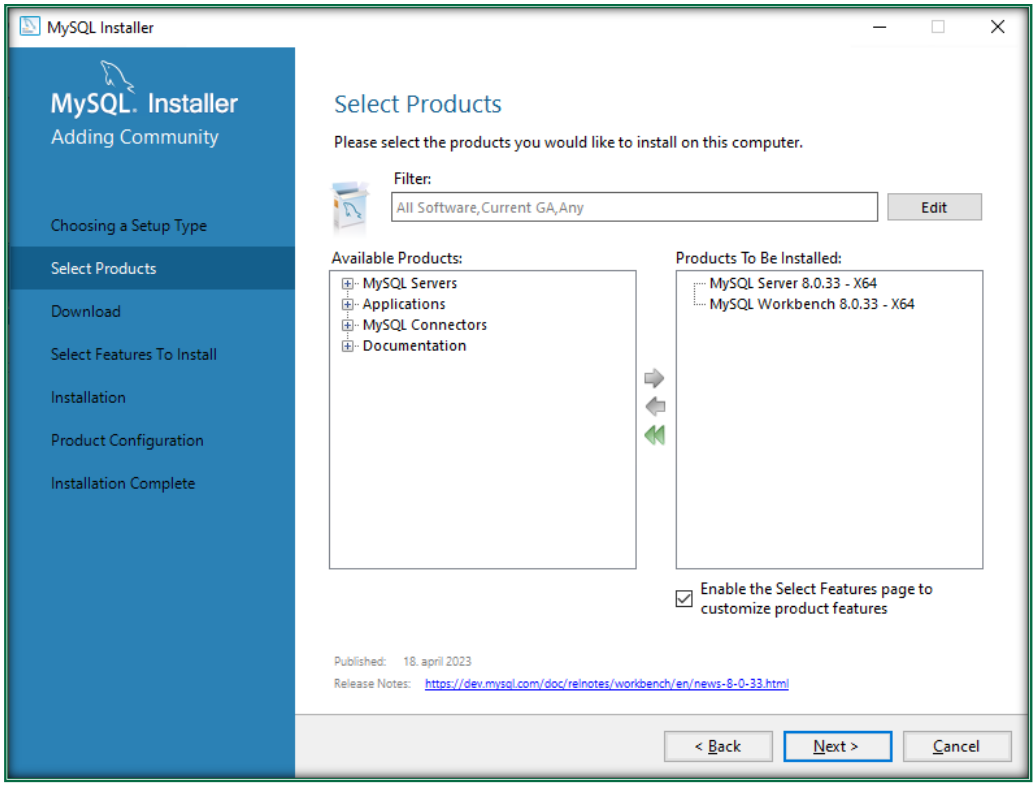
Installation af MySQL

For at gemme eDelivery dokumenter skal der også installeres en MySQL database.

Dette skal gøres på den server, hvor den **interne** Oxalis webservice er installeret.
Programmet kan hentes her:

[MySQL :: Download MySQL Community Server]

Hent "MySQL Installer for Windows" og vælg den første .msi-fil.
Vælg "No thanks, just start my download" på den efterfølgende side.
Kør installationsprogrammet og vælg "Custom Setup Type".
Vælg følgende produkter som minimum (versionsnummeret kan afvige):



Efter programmet er installeret skal det konfigureres.
Vælg først "Server Computer" i "Config Type" under "Type and Networking".
Vælg "Use Strong Password Encryption for Authentication" under "Authentication Method".
Angiv et stærkt password til root brugeren under Accounts and Roles.
Vælg standardindstillingerne under Windows Service.
Vælg "Yes, grant full access…" under "Server File Permissions".

For at kunne sende og modtage store filer, er det nødvendigt at justere på MySQL opsætningen, men det skal gøres ved at rette direkte i konfigurationsfilen.
Stop MySQL servicen.
Rediger filen my.ini som kan findes her: C:\ProgramData\MySQL\MySQL Server 8.0
Søg efter parameteren max_allowed_packet og ændr værdien til 300M.

Installation af program til administration af keystore

Til at administrere certifikater til brug for Java applikationer, kan du vælge at bruge Java kommandoen keytool. Hvis du ikke har erfaring med Java, anbefaler vi at installere et program med en intuitiv brugergrænseflade. I denne vejledning anvendes Keystore Explorer.
Det kan hentes her: KeyStore Explorer - Download (keystore-explorer.org)
Vælg filen som hedder kse-552-setup-no-jre.exe (versionsnummeret kan afvige).

Installation af eDelivery invoker

Installationsprogrammet til eDelivery webservice er en del af eDelivery pakken som kan hentes på Økonomistyrelsens hjemmeside. Naviger til denne side ved at klikke her.

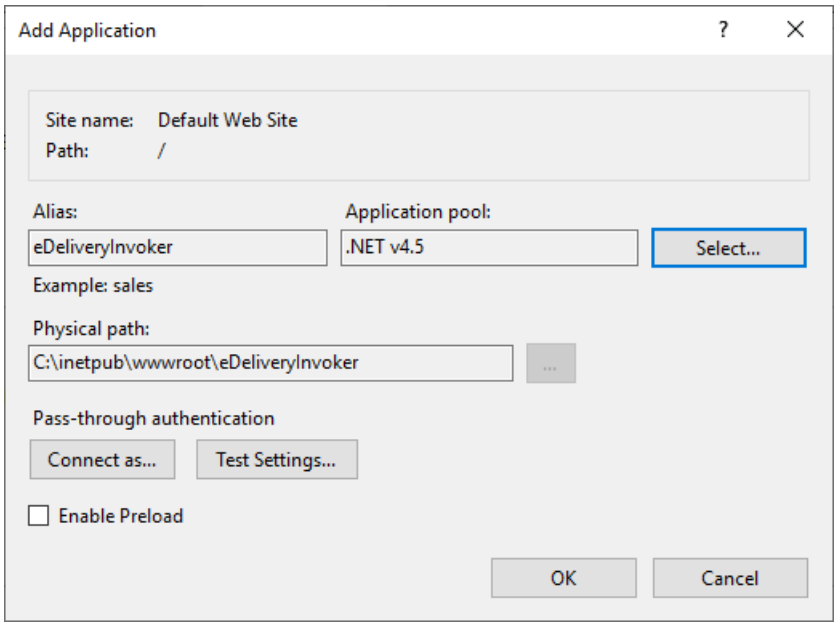
Det anbefales at installere webservicen på den samme server, hvor de øvrige interne komponenter til transportlaget som f.eks. TSIOController ligger. Installationsprogrammet køres. Bemærk at programmet selv vælger at installere installationsmappen på det drev, hvor der er mest plads. Ret evt. stien til C-drevet, fx C:\eDeliveryInvoker 11.2.000.006 Install\.

Denne skabelonmappe indeholder webservicen, som kan anvendes til at lave flere instanser af webservice.

Dette gøres ved at kopiere mappen ' eDeliveryInvoker 11.2.000.006 Install' til placeringen for websites, typisk 'C:\inetpub\wwwroot'.
Omdøb mappen til f.eks. eDeliveryInvoker.

Opret derefter webservicen i IIS Manager.

Højreklik på mappen eDeliveryInvoker i det site, den tilhører.
Vælg 'Convert to Application':



Tryk på Select knappen og vælg den Application pool som hedder .NET v4.5. Tryk derefter OK.

Derefter skal webservicen konfigureres til at køre under en afviklingsbruger opsat som servicebruger.

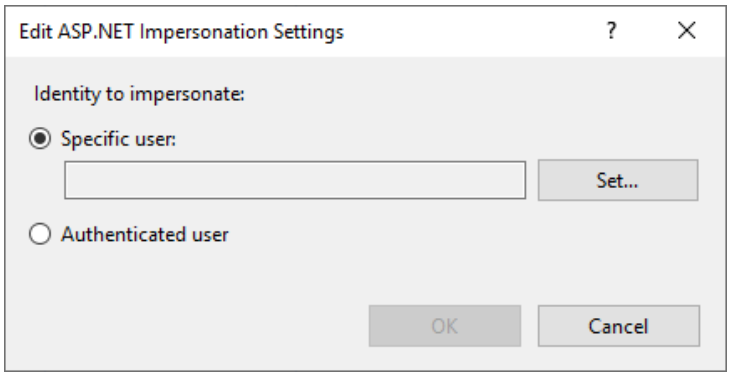
Bemærk at sitets afviklingsbruger skal have modify-rettighed til mappen Temporary ASP.NET Files i den relevante .NET-versions undermappe under C:\Windows\Microsoft.NET\

Man kan med fordel anvende den samme afviklingsbruger som til 'NS transportlaget'.

Hvis en sådan bruger endnu ikke er oprettet, skal brugeren i sikkerhedspolitikken have rettigheder til 'Log on as a batch job' og 'Log on as a service'.

Hvis der ikke anvendes den samme bruger som til transportlaget, skal brugeren have SQL rettighederne db_datareader og db_datawriter til Logging databasen.

Marker den oprettede webservice 'eDeliveryInvoker' og åbn Authentication. Marker 'ASP.NET Impersonation' og vælg 'Edit'.



Tryk på 'Specific user' og vælg 'Set'.

Udfyld med den oprettede servicebruger og password og tryk OK 2 gange.

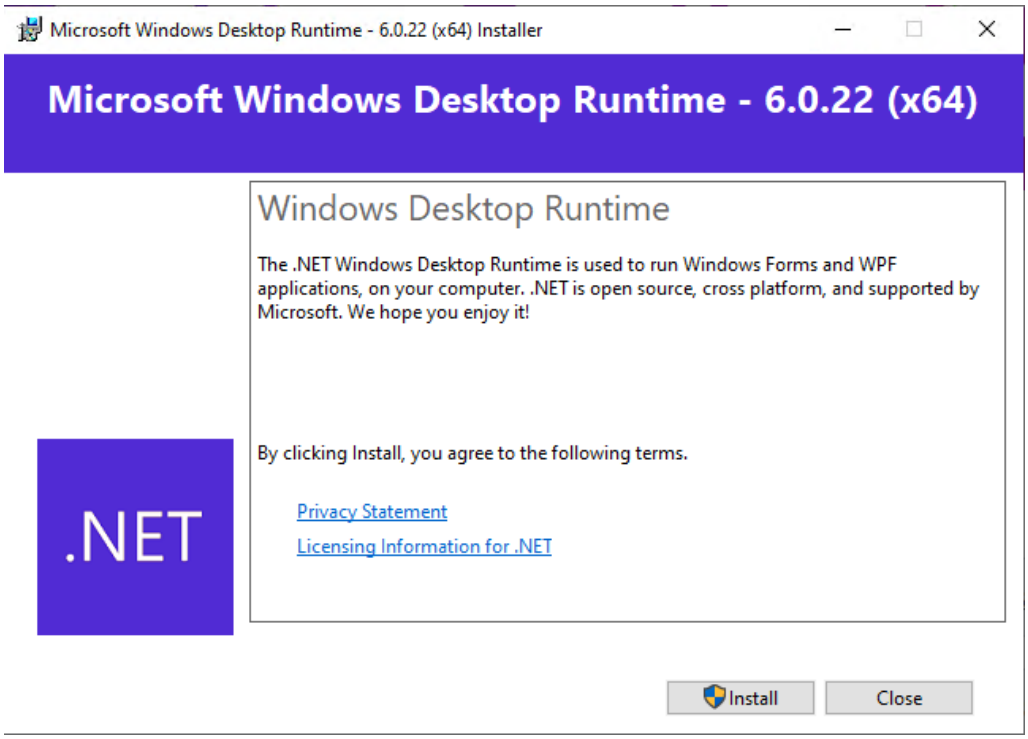
Tjek også at 'ASP.NET Impersonation' er 'Enabled'.

Installation af program til hashing af password

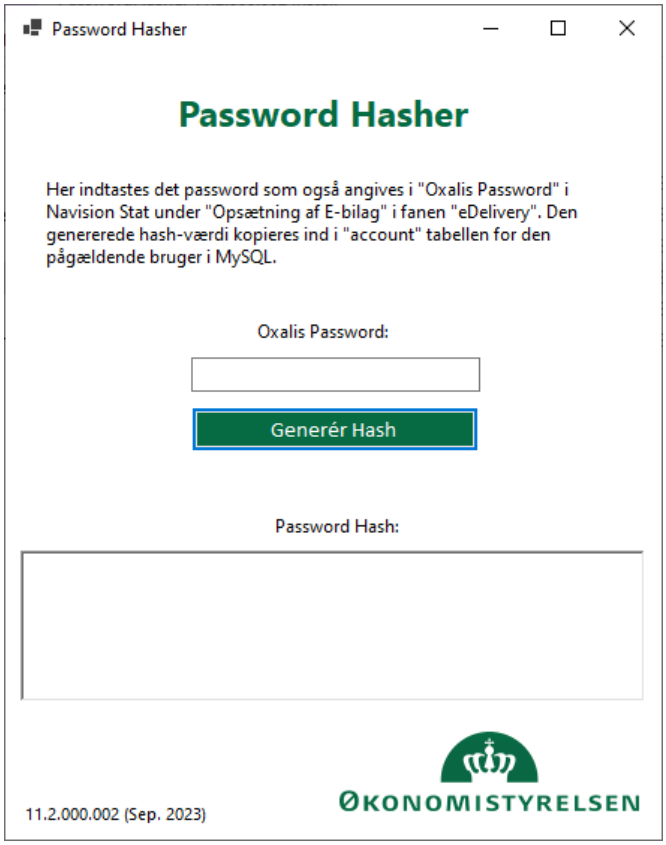
Installationsprogrammet til Password Hasher er en del af eDelivery pakken som kan hentes på Økonomistyrelsens hjemmeside. Naviger til denne side ved at klikke her.
Installer programmet ved at køre programmet PasswordHasher 11.2.000.002 Install.msi.
Hvis nedenstående kommer frem under installationen, skal du først installere .NET Desktop Runtime.

Dette kan hentes her:
[Download .NET 6.0 (Linux, macOS, and Windows) (microsoft.com)]
Vælg x64 versionen som står under punktet .NET Desktop Runtime 6.0.22 (versionsnummeret kan afvige, vælg som udgangspunkt den nyeste version).

Kør installationsprogrammet som bliver downloadet:



Efter Runtime er installeret kan Password Hasher programmet installeres.
Når du kører programmet kommer nedenstående vindue:



Indtast det password som skal anvendes til opsætning af Navision.
Tryk på knappen Generér Hash.
Derefter bliver der genereret en hashværdi som skal anvendes i dette afsnit.

Oprettelse

Opret Java keystore til SSL certifikat på den eksterne Tomcat webserver.

1. Åbn Keystore Explorer.
2. Tryk på Create a new KeyStore.
3. Vælg JKS.
4. Tryk Ctrl-K for at importere Key Pair.
5. Vælg PKCS #12
6. Vælg SSL certifikatfilen og angiv passwordet til filen.
7. Skriv et alias eller behold det foreslåede.
8. Vælg et password til nøglen.

9. Tryk Ctrl-S for at gemme keystore.
10. Skriv et password til keystore, det er vigtigt at det er det samme som til nøglen.
11. Gem filen i C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf og husk at tilføje extension .jks.

Opret Java keystore til MitID Erhverv systemcertifikat (OCES3) på både den interne og eksterne Tomcat webserver

1. Åbn Keystore Explorer.
2. Tryk på Create a new KeyStore.
3. Vælg PKCS #12.
4. Tryk Ctrl-K for at importere Key Pair.
5. Vælg PKCS #12
6. Vælg OCES3 certifikatfilen og angiv passwordet til filen.
7. Skriv et alias eller behold det foreslåede.
8. Vælg et password til nøglen.
9. Tryk Ctrl-S for at gemme keystore.
10. Skriv et password til keystore, det er vigtigt at det er det samme som til nøglen.
11. Gem filen i C:\Program Files\Apache Software Foundation\Tomcat 9.0\oxalis og husk at tilføje extension .p12.

Oprettelse af schema (database) til Oxalis.

1. Åbn MySQL Workbench og log på med "root".
2. Vælg "Schemas" fanen i "Navigator" ruden og vælg "Create schema…"
3. Giv det et passende navn og tryk "Apply".

Hvis opsætningen af Oxalis skal laves for flere institutioner, anbefales det at lave et schema for hver institution, så det følger logikken for den nuværende Logging database, men dog kun hvis hver institution anvender særskilte MitID Erhverv systemcertifikater. Ellers skal de deles om det samme schema.

Oprettelse af databasebruger i MySQL som anvendes af Oxalis til at læse og gemme dokumenter.

1. Vælg "Administration" fanen i "Navigator" ruden og "Users and Privileges".
2. Tryk på "Add Account".
3. Giv brugeren et passende navn.
4. Bibehold Standard under "Authentication Type".
5. I "Limit to Hosts Matching" er det en god ide at skrive et IP-adresseområde som må tilgå serveren, så den ikke kan tilgås fra uvedkommende lokationer.
6. Opret et stærkt password til brugeren og skift til fanen "Schema Privileges".

7. Tryk på ”Add Entry”… og vælg ”Selected schema” og vælg det schema som blev oprettet til Oxalis.
8. Tryk ”Ok” og giv følgende rettigheder til brugeren:
9. ALTER, CREATE, DELETE, DROP, INSERT, REFERENCES, SELECT, UPDATE
10. Tryk til sidst på ”Apply”.

Hvis opsætningen af Oxalis skal laves for flere institutioner, skal der laves en databasebruger i hver institutions schema.

Oprettelse af Oxalis API bruger

Til at kommunikere med Oxalis API, skal der oprettes en MySQL bruger og en modtager for hvert regnskab.
Dette kan dog ikke gøres før Oxalis servicen kører uden fejl og Oxalis schema er blevet populeret med standardtabellerne vha. Liquibase.
Hashing af password kan gøres med programmet Password Hasher som er beskrevet her.

1. Indsæt følgende i **account** tabellen:
2. I ”username” feltet skrives et unikt brugernavn for hvert regnskab.
3. I ”password” feltet skrives det hashede password til brugeren.
4. I ”version” feltet skrives 1.
5. I ”created_date” feltet skrives datoen for oprettelsen i formatet YYYY-MM-DD HH:MM:SS
6. I ”created_by” feltet skrives et id for den bruger der har lavet oprettelsen.

7. Indsæt følgende i **account_receiver** tabellen:
8. I ”account_id” feltet skrives id’et fra det tilhørende regnskab som blev oprettet i account tabellen.
9. I ”participant_id” feltet skrives det modtagende GLN nummer med 0088: foran, f.eks. 0088:5798009811127.
10. I ”version” feltet skrives 1.
11. I ”created_date” feltet skrives datoen for oprettelsen i formatet YYYY-MM-DD HH:MM:SS
12. I ”created_by” feltet skrives et id for den bruger der har lavet oprettelsen.
13. I ”cvr_number” feltet skrives CVR nummeret for det pågældende regnskab.

Hvis opsætningen af Oxalis skal laves for flere institutioner, skal der laves en API bruger for hvert regnskab i institutionens Navision database.

Hvis institutionen har flere GLN numre tilknyttet det samme regnskab, kan de deles om den samme API bruger.

Konfiguration

1. Opret en mappe på serveren hvor Apache Tomcat er installeret og hvor Oxalis programmet skal lægges, f.eks. C:\oxalis
2. Kopier oxalis.war fra installationspakken til mappen som er oprettet i punkt 1
3. Udpak oxalis-as4.zip fra installationspakken til en undermappe som hedder oxalis-as4 under mappen som er oprettet i punkt 1

Konfiguration af logning af Oxalis

1. Opret mappen "oxalis" under "C:\Program Files\Apache Software Foundation\Tomcat 9.0"
2. Kopier filen "logback.xml" fra installationspakken til ovenstående mappe.

   Logningen kan tilpasses efter behov, men hvis Apache Tomcat er installeret på standardplaceringen, er der ikke behov for ændringer.

Konfiguration af Oxalis webservicen

1. Kopier filen "oxalis.conf" og "Nemkonto_Dummy.xsd" fra installationspakken til mappen "C:\Program Files\Apache Software Foundation\Tomcat 9.0\oxalis".
2. Denne sti betegnes som oxalis_home.
3. Filen udfyldes som det står beskrevet i filen.
4. Dog skal værdien i "liquibase.run: true" ændres til "false" på den eksterne webserver.
5. Værdierne i rest.inbox.enabled = true og rest.outbox.enabled = true skal også sættes til false på den eksterne webservice for at lukke for adgangen til inbox og outbox udefra.

Konfiguration af webside til Oxalis

1. Kopier "oxalis.xml" fra installationspakken til mappen "C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\Catalina\localhost".
2. Vær opmærksom på om værdien i "Environment name="OXALIS_HOME" er udfyldt med stien til den rigtige oxalis_home mappe.
3. Ret værdien i Context docBase til den mappe der blev oprettet til oxalis her, f.eks. <Context docBase="C:\oxalis\oxalis.war">
4. Ret værdien i base til undermappen oxalis-as4, f.eks. base="C:\oxalis\oxalis-as4"

Opsætning af Tomcat til at anvende TLS

Dette skal kun gøres på den *eksterne* webserver.

1. Tag en kopi af server.xml og web.xml i **"C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf".**

2. Rediger "server.xml" og find nedenstående sektion:

```
<Connector port="80" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443"
           maxParameterCount="1000"
           />
<!--
   <Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="150" SSLEnabled="true"
           maxParameterCount="1000"
           >
      <SSLHostConfig>
         <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
                  type="RSA" />
      </SSLHostConfig>
   </Connector>
   -->
```

3. Fjern udkommenteringen og ret til nedenstående:

```
<Connector port="80" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="443"
           maxParameterCount="1000"
           />

<Connector port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="150" SSLEnabled="true"
```

```
            maxParameterCount="1000" scheme="https" secure="true"
>
      <SSLHostConfig protocols="TLSv1.2+TLSv1.3"
honorCipherOrder="true"
ciphers="TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TL
S_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDS
A_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_CHACH
A20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
A384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_R
SA_WITH_CHACHA20_POLY1305_SHA256">
            <Certificate certificateKeystoreFile="conf/[Placering af
keystore].jks"
                        certificateKeystorePassword="[password angivet i tidligere
afsnit]"
                        type="RSA" />
      </SSLHostConfig>
   </Connector>
```

---

4. Hvor værdien i certificateKeystoreFile ændres til placeringen af keystore til SSL certifikatet og hvor værdien i certificateKeystorePassword ændres til det password som blev angivet i ovenstående afsnit.
5. Det anbefales at spærre for adgangen til diverse undersider for ikke at udstille informationer som kan misbruges.
   Find nedenstående sektion:
   ```
   <Host name="localhost"  appBase="webapps"
       unpackWARs="true" autoDeploy="true">
   ```
6. Indsæt nedenstående linjer lige efter, det kan dog være nødvendigt at tilpasse værdien i Context path eller tilføje flere linjer, hvis der er anvendt andre navne på url'er:
   ```
   <Context path="/inbox" docBase="" >
   <Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
   deny="*" />
   </Context>
   <Context path="/outbox" docBase="" >
   <Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
   deny="*" />
   </Context>
   <Context path="/status" docBase="" >
   <Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
   deny="*" />
   </Context>
   <Context path="/as4/status" docBase="" >
   <Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
   deny="*" />
   ```

```
</Context>
<Context path="/oxalis/api/inbox" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/oxalis/api/outbox" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/oxalis/status" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/oxalis/as4/status" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/openapi.json" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/openapi-ui" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/oxalis/openapi.json" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
<Context path="/oxalis/openapi-ui" docBase="" >
<Valapp     className="org.apache.catalina.valapps.RemoteAddrValapp"
deny="*" />
</Context>
```

7. For at konfigurere serveren så den understøtter HSTS, rediger derefter web.xml og find </filter-class>
8. Indsæt nedenstående i en ny linje lige efter </filter-class>:

```
<init-param>
  <param-name>hstsMaxAgeSeconds</param-name>
  <param-value>31536000</param-value>
</init-param>”
```

Derefter skal det se sådan ud:

```
<filter>
```

```
        <filter-name>httpHeaderSecurity</filter-name>
        <filter-
class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
                    <init-param>
                      <param-name>hstsMaxAgeSeconds</param-name>
                      <param-value>31536000</param-value>
                    </init-param>
                    <async-supported>true</async-supported>
</filter>
```

9. Find nedenstående sektion og udkommenter den:

```
<!--
   <filter-mapping>
      <filter-name>httpHeaderSecurity</filter-name>
      <url-pattern>/*</url-pattern>
      <dispatcher>REQUEST</dispatcher>
   </filter-mapping>
-->
```

10. For at lave redirect fra http til https, find **"</web-app>"**
11. Indsæt nedenstående lige over **"</web-app>"**:

```
<!-- Force HTTPS, required for HTTP redirect! -->
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>

<!-- auth-constraint goes here if you require authentication -->
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

Singletenancy

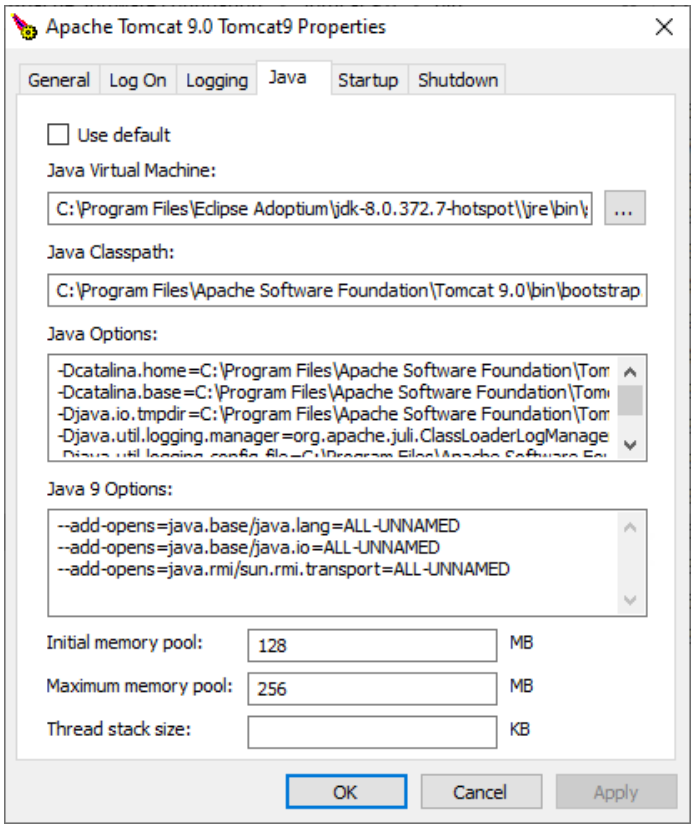
Hvis det er nødvendigt at lave flere instanser af Oxalis fordi man skal lave en opsætning for flere institutioner som anvender hvert sit MitID Erhverv systemcertifikat, så følg nedenstående fremgangsmåde:
Flere instanser af Oxalis webservicen kan laves ved at oprette flere oxalis_home mapper samt flere xml-filer under C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\Catalina\localhost
Ret oxalisinstansnavn.xml filerne så de peger på de respektive oxalis_home mapper.
Ret oxalis.conf så den peger på det rigtige MySQL schema.

Ret også parameteren LOG_FILE_NAME i logback.xml, så der oprettes en separat logfil for hver instans.
Navnet på oxalis_home mappen og oxalis.xml skal stemme overens.
Så f.eks. C:\Program Files\Apache Software Foundation\Tomcat 9.0\oxalis_oes og C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\Catalina\localhost\oxalis_oes.xml.

Tag en kopi af filen catalina.properties i mappen C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf
Rediger derefter catalina.properties og find teksten shared.loader.
Indsæt følgende lige efter shared.loader:
"${catalina.home}/shared/lib","${catalina.home}/shared/lib/*.jar"
For hver xml-fil som ligger i mappen C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\Catalina\localhost skal følgende indsættes lige efter </Resources>:
<Loader delegate="true"/>
Tag filen STjars.zip som ligger i eDelivery installationspakken som kan hentes på Økonomistyrelsens hjemmeside. Naviger til denne side ved at klikke her.
Udpak STjars.zip i mappen C:\Program Files\Apache Software Foundation\Tomcat 9.0
Derefter skal der findes en mappe som hedder shared med en undermappe der hedder lib og i den mappe skal der ligge 2 jar-filer.

Bemærk at dette skal gøres på både den interne- og eksterne webserver.

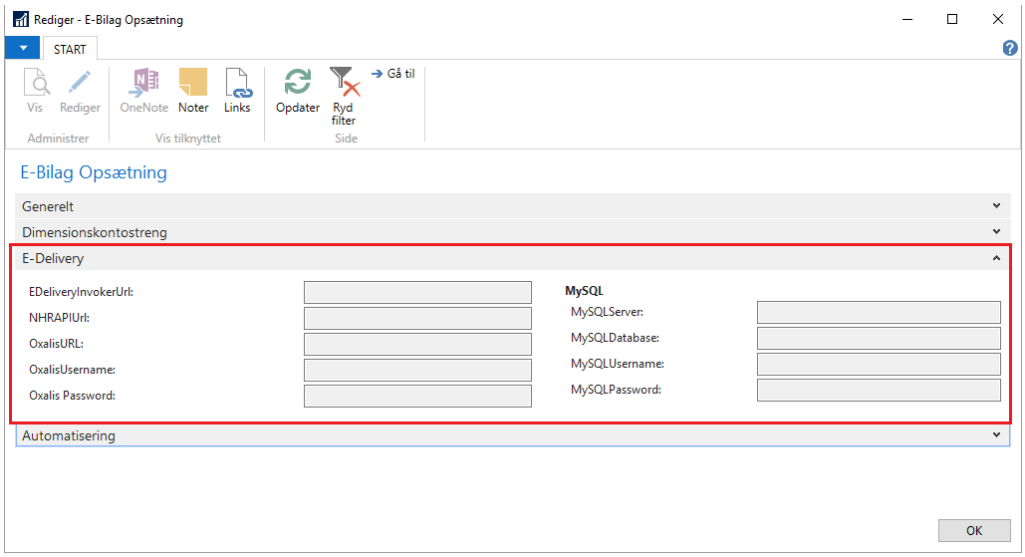
Hvis der laves flere instanser, vil det højst sandsynligt være nødvendigt at justere på den mængde af hukommelse som er dedikeret til Apache Tomcat.
Dette gøres ved at køre programmet Tomcat9w.exe som ligger i C:\Program Files\Apache Software Foundation\Tomcat 9.0\bin
Skift til fanen Java:



Udfyld Maximum memory pool med en større værdi.
Vi anbefaler at sætte værdien til minimum 1024, men afhængig af hvor mange instanser der skal køre, kan det være nødvendigt at sætte værdien højere.

Opsætning i Navision Stat

Opsætning af eDelivery findes via Sti:
Afdelinger/Opsætning/Programopsætning/Generel Integration/NS TS Integration og Opsætning af E-Bilag



Oversigtspanelet E-Delivery indeholder den tekniske opsætning, som er beskrevet nedenfor.

Felt	Beskrivelse
EdeliveryInvokerUrl	Udfyldes med den url der er oprettet til eDeliveryInvoker webservicen
NHRAPIUrl	Udfyldes med url til Nemhandel API webservice. I skrivende stund er det: https://api.nemhandel.dk/v3-nhr-api/
OxalisURL	Udfyldes med url til den interne Tomcat webserver efterfulgt af /oxalisinstansnavn/api
OxalisUsername	Udfyldes med det brugernavn der er oprettet her
Oxalis Password	Udfyldes med det password der er oprettet her
MySQLServer	Udfyldes med serveradressen for MySQL serveren
MySQLDatabase	Udfyldes med det schemanavn der er oprettet her
MySQLUsername	Udfyldes med det brugernavn der er oprettet her
MySQLPassword	Udfyldes med det password der er oprettet her

Åbninger i firewall

På den *eksterne* webserver skal der åbnes for:
Port 443 (HTTPS) indgående fra internettet
Port 3306 (MySQL) udgående mod den *interne* webserver
Port 53 udp og tcp (DNS) udgående mod edelivery.tech.ec.europa.eu og edel.sml.dataudveksling.dk
Port 443 (HTTPS) udgående mod internettet

På den *interne* webserver skal der åbnes for:
Port 80 (HTTP) indgående fra server med eDelivery invoker
Port 3306 (MySQL) indgående fra den *eksterne* webserver
Port 53 udp og tcp (DNS) udgående mod edelivery.tech.ec.europa.eu og edel.sml.dataudveksling.dk
Port 80 (HTTP) udgående mod internettet
Port 443 (HTTPS) udgående mod internettet

På serveren hvor eDelivery invoker er installeret skal der åbnes for:
Port 80 (HTTP) udgående mod den *interne* webserver
Port 443 (HTTPS) udgående mod api.nemhandel.dk
Port 389 (MitID LDAP) udgående mod ldap.ca1.gov.dk (dog ikke hvis eDelivery invokeren ikke er installeret på samme server som TSIOController)

Drift

Man kan lave en hurtig test for at se om oxalis webservicen fungerer.
Hvis man har fulgt standardinstallationen vil man kunne åbne siden servernavn/oxalisinstansnavn/as4 i en browser og så skal der komme en side hvor der står Hello AS4 world.
Man kan også åbne siden servernavn/oxalisinstansnavn/status for at se programversioner og det benyttede certifikat.

Vær opmærksom på at URL'er i Tomcat som standard er case-sensitive.

For at fejlsøge kan man kigge på de logs der ligger i mappen C:\Program Files\Apache Software Foundation\Tomcat 9.0\logs
Loggen som hedder oxalisinstansnavn.log indeholder evt. fejl ved opstart af oxalis webservicen samt kommunikationen med servicen.

Når der er lavet ændringer i konfigurationen, er det bedst at genstarte Apache Tomcat servicen for at genindlæse oxalis programmet.

ISBN nr. 87-7956-795-9