

Navision Stat 9.2.005 (NS 9.3)

ØSY/NSIR/RASEG
Dato 07.03.2019

Danske Bank Webservice Installationsvejledning

Overblik

Introduktion

Indholdsfortegnelse

Overblik	1
Introduktion	1
Målgruppe	2
Før du går i gang.....	3
Installationskrav	3
Certifikat.....	3
Sådan installeres Danske Bank Webservice.....	4
Installation af Danske Bank WS.....	4
Oprettelse af WS-bruger	4
Installation på Service-Tier	4
Opsætning af Navision Stat databasen	8

Målgruppe

Denne vejledning er rettet mod den relevante IT-funktion, som skal installere Danske Bank Webservice og tilhørende certifikat, samt foretage opsætningen i Navision Stat regnskabet.

Opsætningen i regnskabet kan evt. udføres af regnskabspersonale.

Beskrevet og supporteret for

Windows Server 2012R2.

Copyright

© 2019 Microsoft Corporation and Moderniseringsstyrelsen.

All rights reserved.

Seneste ændring

Publiceret første gang: 28. marts 2019

Seneste ændring: 30. april 2019

Før du går i gang

Installationskrav

Installationen tager udgangspunkt i Windows Server 2012 R2.

Installationen vil sandsynligvis ligeledes virke på nyere versioner af Windows Server, men er ikke testet herpå.

Certifikat

Danske Bank Webservice integrationen afhænger af, at der manuelt installeres et Dansk Bank rod-certifikat, samt installeres et brugercertifikat via programmet 'ContiniaDanskeBankCertificateInstaller.exe'

Sådan installeres Danske Bank Webservice

Installation af Danske Bank WS

I forbindelse med opgradering til NS9.0, og PM2.25 blev mulighed for at udveksle betalingsdata med Danske Bank via DB WS introduceret. Dette fremfor det tidligere API. Som institution kan man selv vælge, hvornår der skiftes metode (API/WS) for det enkelte regnskab, forudsat at Navision Stat installationen er forberedt herfor.

Oprettelse af WS-bruger

1. Såfremt man har en eksisterende API-bruger opsat for regnskabet, kan denne videreføres som WS bruger via bestilling af et webservicemodul. Slutresultatet af denne proces er en fremsendelse af en midlertidig PIN-kode tilhørende det eksisterende brugernummer for API-brugeren
2. Såfremt man ikke allerede har opsat en API-bruger for regnskabet kan der bestilles en ny WS bruger. Slutresultatet af denne proces er en fremsendelse af en midlertidig PIN-kode og et nyt brugernummer.

Bemærk, den midlertidige PIN-kode udløber efter 3 måneder!

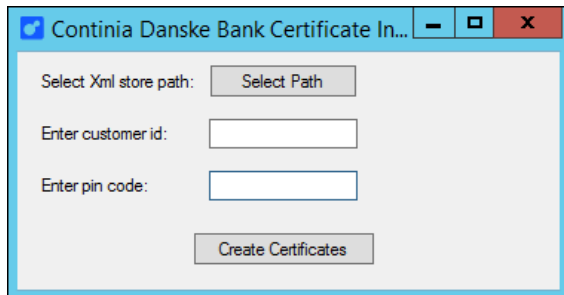
Se vejledning fra Danske Bank på: <http://www.danskebank.dk/da-dk/skbobs/Beskrivelser/Business-Online/Pages/Kom-godt-i-gang-med-Business-Online.aspx>

Afsnittet: 'Etablering af Webservice i Business Online'

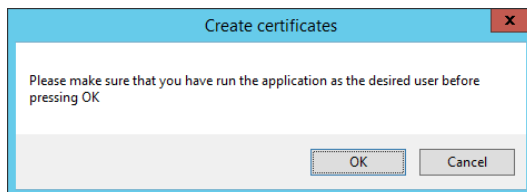
Installation på Service-Tier

3. Tilgå service tier'et med en bruger, der har administratorrettigheder. Download Continia_DB_WS.zip og udpak filerne på et fællesdrev.
4. Find filen Continia.DB.WS.dll, som skal kopieres ind i ADD-INS biblioteket, typisk: c:\Program Files\Microsoft Dynamics NAV\90\service\Add-ins\
Tjek herefter, at filen Continia.DB.WS.dll ikke er 'Blocked', under Properties.
- 4.a Såfremt der er tale om en opdatering af Continia DB WS Integration, skal punkt 4 stadig følges – dvs. at den nye Continia.DB.WS.dll her skal erstatte den gamle i \Add-ins\-mappen.
5. Genstart alle klient services, hvor 'Credential Type' er enten 'Windows' (win) eller 'NavUserPassword' (psw), for en sikring af, at ændringen slår igennem.
6. Inden du afvikler næste trin, dvs. ContiniaDanskeBankCertificateInstaller.exe, skal rodcertifikatet være installeret. Se "Installation af Rod-certifikat".
7. Tilgå nu service tier'et med servicebrugeren, der benyttes til klientservices, og afvikl 'ContiniaDanskeBankCertificateInstaller.exe' for at danne certifikatet.

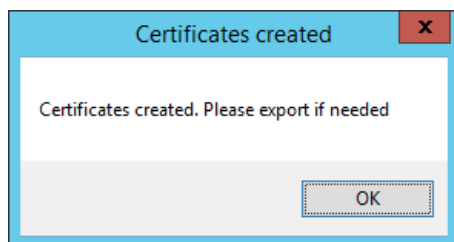
- 'Select XML store patch' og vælg ny folder 'C:\Danske Bank Certifikater\'. Indtast hhv. customer ID (brugernummer) og 4-cifrede pin code (sikkerhedskode), der er erhvervet fra Danske Bank. Klik 'Create Certificates'



- Klik herefter på OK for at bekræfte, at du har foretaget certifikatinstallation med den servicebruger, der benyttes til klientservice'ne.



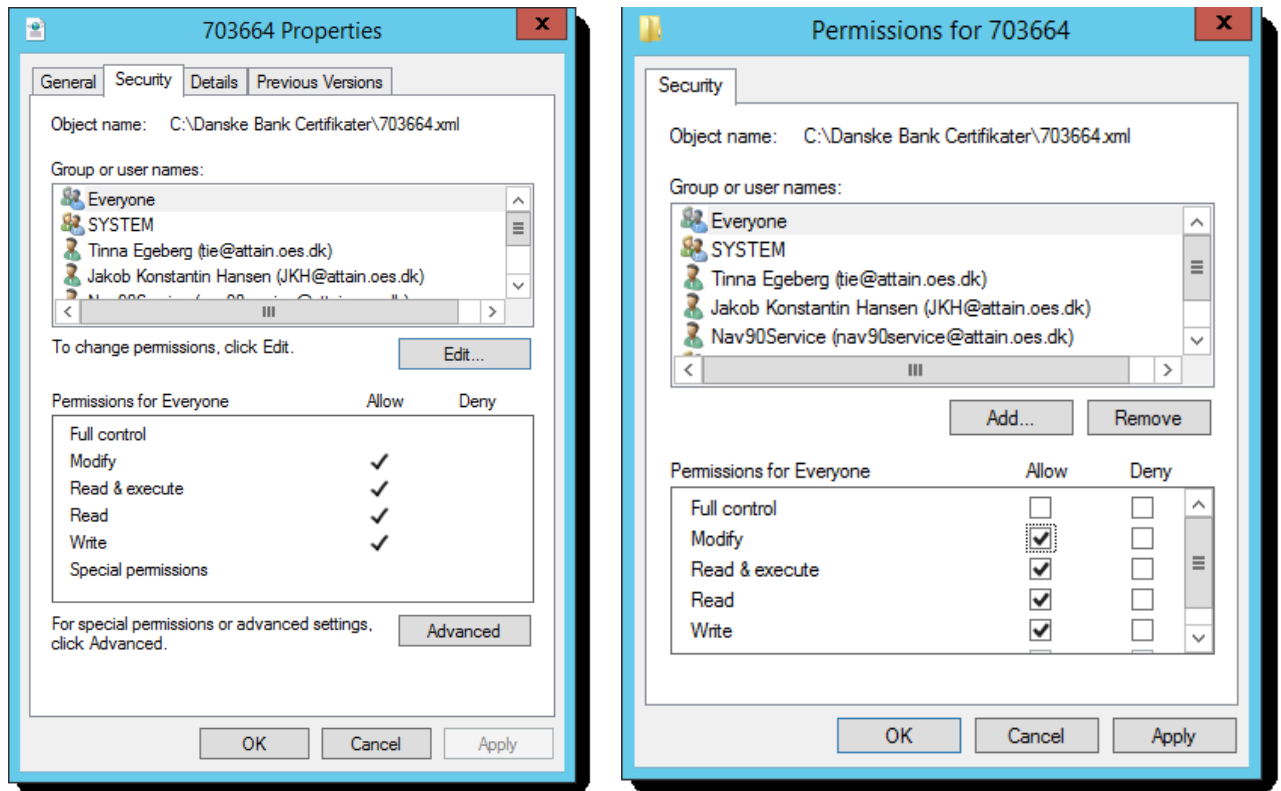
- Klik på Yes for at bekræfte, at navnet på rodcertifikatet er DBGROOT.
- Klik herefter OK til dialogboksen:



Certifikatfilen, '[Brugernummer].xml' skulle nu gerne være dannet og gemt i 'C:\Danske Bank Certifikater\'. Hvis certifikatfilen ikke har navnet i formatet: '[Brugernummer].xml' er det vigtigt at du omdøber filen.

Bemærk at hvis certifikatet skal bruges på flere servere, skal certifikat og xml-fil nu kopieres til eventuelle ekstra servere.

12. NST-Brugeren skal som minimum tildeles MODIFY-rettigheder til XML-Filen.



Stien til xml-filen skal efterfølgende angives i Navision Stat. Dette gøres ved at følge den videre vejledning.

13. Når der udveksles data med Danske Bank via DB Webservice gemmer systemet en logfil. Det gælder både når der sendes betalinger direkte til banken, hvor banken returnerer kvitteringer for modtagelse, eller når der hentes filer til bankkontoafstemning og ved indlæsning af valutakurser. Logfilerne bliver altid prøvet gemt på C-drevet på applikationsserveren under stien 'C:\Data\Test'. Alle brugere der enten sender betalinger eller indlæser filer vil derfor skulle have oprettet en mappe "Test" på deres C-Drev. Systemet kan automatisk oprette denne placering, men så skal man bekræfte oprettelsen via en dialogboks ved første anvendelse af DB Webservice. Det anbefales derfor at mappen oprettes manuelt med MODIFY adgang til servicebrugeren.

Installation af Rod-certifikat

Udover brugercertifikatet skal der installeres et rodcertifikat fra Danske Bank på service-tier. Dette skal bruges for at kunne validere certifikatet, oprettet med 'ContiniaDanskeBankCertificateInstaller.exe' i det tidligere step. Rodcertifikatet findes i pakken "Continia_DB_WS" og hedder 'DBGROOT_1111110003.cer'.

14. For at installere dette på service-tier skal man logge ind med administrator-rettigheder på serveren og dobbeltklikke på certifikatet.
15. Vælg herefter "Installer certifikat".
16. Vælg "Lokal Computer".
17. Vælg "Placer alle certifikater i følgende certifikatlager".
18. Vælg "Gennemse..." og herefter mappen "Trusted Root..".
19. Certifikatet er nu installeret.

Opsætning af Navision Stat databasen

20. Åbn relevant regnskab.

21. Tilgå Bankcentraler under stien

Afdelinger/Opsætning/Programopsætning/Økonomistyring/
Finans/Betalingsformidling/Avanceret/Bankcentraler. Opret ny Bankcentral
med koden 'DBISO20022' jf. nedenstående opsætning:

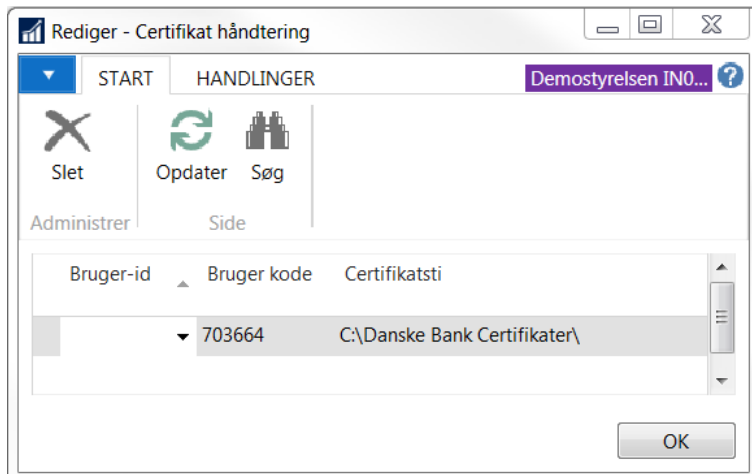
Kode	Navn	Programversion	Bankopsætn...	Send via	PM Dire...	Prok... kræv...	BO aftalenr.	NKS Aftalenumm...	NKS Myndigheds...
DBISO20022	Danske Bank Busine...	1.00	2.30	DB Webservi...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		0	0
NKS	Nem Konto System	1.00	2.15	Webservice	<input type="checkbox"/>	<input checked="" type="checkbox"/>	002782	100029	4528

22. Tilgå Bank under stien

Afdelinger/Økonomistyring/Opsætning/Betalingsformidling/Bank.
Opret nyt bankkort med koden 'DBWS' jf. nedenstående opsætning.
Brugernummeret enten skal enten være det samme brugernummer (Customer ID) som tidligere blev anvendt for API-brugeren eller det nye, der er modtaget for WS-brugeren, fra Danske Bank.

Generelt		Bestil status: Alle	
Kode:	DBWS	Anvendes:	<input checked="" type="checkbox"/>
Navn:	Danske Bank Webservice	Direkte:	<input type="checkbox"/>
Filnavn indland (send):		Brugernummer:	703664
Filnavn udland (send):		Sikkerhedskode:	
Advar ved fil-overskrivning:	<input checked="" type="checkbox"/>	Hoved reg. nr.:	
Bankcentralkode:	DBISO20022	Kreditor nr.:	
Aktiver Log:	<input type="checkbox"/>		

23. I det nyoprettede bankkort 'DBWS' vælges 'Navigér' og 'Certifikater/Brugere'



Feltet Bruger-ID efterlades blankt, mens du skal udfylde 'Bruger kode' med API/WS brugernummeret fra 'Brugernummer' feltet på selve bankkortet. Udfyld ligeledes feltet 'Certifikatsti' med den sti, hvor certifikatfilen er gemt på serveren, og klik OK..

Bemærk! Certifikatet kan kun anvendes for de regnskaber, hvor det opsatte brugernummer på regnskabets bankkort for DBISO20022, er magen til det brugernummer, som certifikatet er dannet med.

Bemærk! Beskrivelsen forudsætter ligeledes at certifikaterne installeres under servicebrugere (CURRENT USER)¹. Der skal derfor installeres et certifikat pr. servicebruger. I tilfælde af, at der anvendes forskellige servicebrugere til forskellige klientservices, skal der således dannes en certifikatpakke pr. servicebruger. Hvis den samme servicebrugere derimod opsættes for flere services, kan man nøjes med et certifikat, så længe det sker indenfor den samme server.

¹ Hvis privatnøglen til det certifikat, der installeres under CURRENT USER er markeret som 'Eksporterbar', kan man i øvrigt normalt blot eksportere det, og lægge det ind i LOCAL MACHINE, hvorefter alle, som man giver rettigheder kan tilgå det. Adgang til certifikatets private nøgle kan styres via funktionen "Manage Private Keys".