



Belastingdienst

Aansluitvoorwaarden x86 OS-en voor externe leveranciers

Inschrijver dient voor de op de door de Belastingdienst beschikbaar te stellen Servers en Werkplekken van de belastingdienst te installeren Programmatuur aan te geven in welke mate aan de volgende punten wordt voldaan.

Authenticatie

1. De Programmatuur is alleen toegankelijk voor gebruikers van wie de identiteit is geverifieerd (authenticatie)
2. De Programmatuur sluit aan op de authenticatievoorziening (Microsoft Active Directory Server) van de Belastingdienst
3. De Programmatuur leidt niet tot gebruikersbeheer buiten Microsoft Active Directory.

Single Sign On

De Programmatuur ontvangt middels een koppeling met Microsoft Active Directory Server de informatie van een geauthentiseerde gebruiker, zodat gebruikers niet apart hoeven in te loggen in de programmatuur.

Authenticatie protocol

Geef aan in hoeverre en op welke wijze de Programmatuur protocollen ondersteunt voor de koppeling met Microsoft Active Directory.

In uw beschrijving dient u in ieder geval de volgende aspecten uit te werken:

1. SAMLv2, OpenID Connect (Oauth 2)*.
2. Kerberos
3. Secure LDAP bind naar Active Directory

Er mag alleen gebruik gemaakt worden van door Microsoft ondersteunde en actuele protocollen. Dit betekent bijvoorbeeld dat SBM v1 (en binnenkort SMB v2), LM/NTLM non-secure LDAP, SSLv3 en WINS niet zijn toegestaan.

De Programmatuur mag niet met Domain Admin of local Administrator in het geval van Windows of root rechten in het geval van Linux draaien.

*Ping Federate is de standard federation service van de Belastingdienst en heeft de voorkeur boven ADFS.

Versleuteling van credentials

De communicatie over het netwerk van de credentials van gebruikers (wachtwoorden) is versleuteld.

Foutafhandeling

1. De Programmatuur zal in geval van blokkerende applicatieve fouten tijdens gebruik een foutmelding loggen.
2. Een foutmelding bevat voldoende informatie zodat beheerders van opdrachtgever zelf fouten kunnen herstellen (bijvoorbeeld aanleiding, tijdstip, aard van de fout en context waarbinnen de fout is opgetreden).
3. De Programmatuur biedt de mogelijkheid voor functioneel beheerders om gegevens te herstellen na een foutsituatie zodat de gebruiker zijn werk kan hervatten.

Logging

1. De Programmatuur kan direct of indirect aangesloten worden op het Event Management Framework van Opdrachtgever, zodat events (alarmen en waarschuwingen) van de Programmatuur centraal verzameld en gepresenteerd kunnen worden met als doel inzichtelijk maken waar zich eventuele problemen (gaan) voordoen in de infrastructuur.

Op Windows Server maakt Opdrachtgever gebruik van SCOM 2016, op Linux Server van IBM ITM en logmonitoring.

2. Het gebruik van de Programmatuur kan worden gelogd. Minimaal vereist: system event logging

Installeerbaarheid Server

1. De Programmatuur moet worden geïnstalleerd in het datacenter van de Belastingdienst (on premise) en is geen cloud Programmatuur en vereist tijdens installatie, starten en gebruik geen actieve internet verbinding(en) (Bijvoorbeeld om licenties te checken)
2. De Programmatuur wordt door de Inschrijver ondersteund en moet zonder aanpassing geïnstalleerd kunnen worden op minimaal één van de volgende combinaties van platformen de Belastingdienst. Waarbij de software gecertificeerd moet zijn op de ondersteunde versies van de overige gebruikte producten (.NET, SQL-Server, DB2 enz.)
 - a. Microsoft Windows Server 2016 Core (of bij uitzondering Server 2016 Full GUI).
 - b. Red Hat Enterprise Linux versie 7.
3. Opdrachtgever moet de Programmatuur, conform handleiding, zelf op het genoemde platform kunnen installeren.
4. De installatie van de Programmatuur moet zonder tussenkomst van handmatige handelingen uitgevoerd kunnen worden. Dit door gebruik te maken van het packageformaat behorend bij het platform O.S.
5. Het installeren en updaten van de Programmatuur kan vanaf lokale media zonder (directe) internettoegang. Op de productieomgeving in het datacenter is geen rechtstreekse internet toegang.
6. Het installeren en activeren van eventueel benodigde licenties op de Server kan vanaf lokale media zonder internettoegang.

7. De Programmatuur die de Inschrijver aanbiedt mag niet afhankelijk zijn van externe hardware zoals bijvoorbeeld een Dongle.
8. De programmatuur is geschikt om op een gevirtualiseerd OS te draaien en is onafhankelijk van de onderliggende hardware. En kan dus naar andere hardware gemigreerd worden.

Toelichting: Opdrachtgever wil gebruik maken van standaard infrastructuur zodat de Programmatuur snel inzetbaar is en beheerd kan worden. Op de Productieomgeving is geen internet toegang.

Firewall en integratie

De Programmatuur kan omgaan met de restrictie dat het netwerk wordt beveiligd met een firewall.

De Programmatuur kan omgaan met de restrictie dat een hostbased firewall verplicht en actief is, op zowel Windows als Linux. De Programmatuur mag niet vereisen dat de hostbased firewall op Windows/Linux moet worden uitgezet om te kunnen functioneren. De Programmatuur moet kunnen functioneren met een actieve hostbased firewall.

Indien de Programmatuur zelf netwerkconnectiviteit nodig heeft, is beschreven welke poorten en protocollen hiervoor nodig zijn. Dit geldt zowel voor de firewall in het netwerk als de hostbased firewall.

Virusscanner

De Programmatuur mag niet vereisen dat de virusscanner op Windows Server wordt uitgezet en Opdrachtgever daarmee haar beveiligingsniveau naar beneden moet aanpassen.

De Programmatuur functioneert in de omgeving waar op Windows Server een virusscanner verplicht en actief is, zonder deze virusscanner te hoeven herconfigureren (momenteel is dit de Symantec virusscanner). Indien de actieve virusscanner een negatieve invloed heeft op de performance van de Programmatuur, dan is het toegestaan om beschreven bestanden en/of mappen van de Programmatuur uit te sluiten van de virusscanning met als doel het voorkomen van performance verlies.

Licentiemanagement

De Programmatuur mag niet vereisen dat de licentie management agent wordt uitgezet en Opdrachtgever daarmee haar niveau van compliancy naar beneden moet aanpassen.

De Programmatuur functioneert in de omgeving waar op een Windows of Linux Server een licentie management agent verplicht en actief is (momenteel is dit de IBM Big Fix agent).

Linux security

De Programmatuur functioneert normaal, indien geïnstalleerd op een Linux Server, ook als selinux in die omgeving actief is en staat op 'enforcing'. Het is niet noodzakelijk eigen selinux policies mee te leveren. De Programmatuur zelf mag in de unconfined selinux context draaien.

Admin rechten

De Programmatuur mag geen services of daemons met netwerkconnectiviteit onder een high privileged account (root, local admin of domain admin) draaien.

In het geval van Windows worden in principe alleen (group) Managed Service Accounts toegestaan voor het draaien van IIS (application pools), achtergrond processen (services), batch jobs (scheduled task) en SQL. Standaard service accounts alleen wanneer wachtwoord regelmatig gewijzigd kan worden..

Platform upgrades

1. Platformversies blijven ondersteund worden door Inschrijver, totdat deze vanuit de leverancier van dat platform end-of-support zijn.
2. De Programmatuur wordt door Inschrijver ondersteund op de meest recente security patches van het operating system. Met andere woorden: de Programmatuur mag niet verhinderen dat altijd de laatste security patches worden geïnstalleerd.
3. Bij het beschikbaar komen van een nieuwe versie van een platform levert de Inschrijver binnen 3 maanden na beschikbaar komen daarvan, een werkende versie van haar Programmatuur voor dat platform.
4. Nieuwe functionaliteiten in de Programmatuur (of nieuwe versies van de gehele Programmatuur) van Inschrijver komen beschikbaar voor alle op dat moment door Inschrijver ondersteunde platformen.

Met “ondersteunen” wordt bedoeld dat alle bestaande features van de Programmatuur op dat betreffende platform probleemloos werken en dat de Inschrijver op dat platform ondersteuning verleent.

Toelichting: De Belastingdienst wil beschikken over actuele platformversies, maar Opdrachtgever wil geen gedwongen upgrades naar hogere platformversies om bij te blijven in de life cycle van het product van Inschrijver zolang het platform niet end-of-support is.

Releases

Releases van de Programmatuur kunnen worden geïnstalleerd zonder handmatige migratieacties op Servers of Werkplekken.

Toelichting: Opdrachtgever wil kunnen beschikken over actuele versies van de Programmatuur, zonder dat dit tot een omvangrijke migratie-inspanning leidt.

End of Support

End of Support van de Programmatuur ligt na de laatst mogelijke einddatum van de Overeenkomst

Gebruik virtuele hardware

De servercomponent (zie “Installeerbaarheid Server”) van de Programmatuur kan gebruikt worden gebaseerd op virtuele hardware VMware.