

Bijlage 1.2 Aansluitvoorwaarden ProRail

1 Actueel overzicht toegepaste technologie

Om de voorwaarden overzichtelijker te maken is een aantal specifieke gebieden (categorieën) te onderscheiden waarbinnen deze gelden. Bijvoorbeeld: hardware, beveiliging, netwerk.

1.1 Categorieën

Applicaties hebben te maken met de volgende categorieën ICT componenten:

1. User Workspace
2. Services: Servers (Hardware, OS), Directory, Web, Distributie, Database, E-mail
3. Netwerk
4. Security
5. Systems Management

De omschrijving geeft het product weer. De kolom "Minimaal vereist" geeft de actuele versie weer die nu in gebruik is, de kolom "Maximaal toegestaan" geeft weer welke versie bij uitzondering en/of op relatief korte termijn gepland staat om in gebruik te worden genomen. Indien de kolom "Maximaal toegestaan" leeg is, is "Maximaal toegestaan" gelijk aan "Minimaal vereist".

2 Verkorte lijst van infrastructuur componenten

Hieronder is een niet uitputtende lijst van de belangrijkste generieke infrastructuur componenten opgenomen.

2.1 User Workspace

OS – werkstations			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Microsoft Windows	Windows 10 x64 1809	Windows 10 x64 1809	Semi-Annual Channel release

OS – draagbaar			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Windows tablet	10	10	versie in lijn met werkstation
Android	8.0 Oreo	10	
iPad iOS	12	13	

Client applicaties en platforms			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Office applicaties	MS Office 1803 (O365)	MSOffice O365, 1808 vanaf 2019H ¹)	Compatibiliteit met Office 365 (incl. Office 2016 C2R) is vereist
Internet Explorer	MS IE11	MS Edge (Chromium)	De serverzijde dient aan te geven in welke compatibiliteitsmodus de browser dient te Werken. CIS security adviezen zijn van toepassing
Chrome	Volgt strikt het release beleid van Google		CIS security adviezen zijn van toepassing. Applicaties dienen altijd de laatste versie van Chrome te ondersteunen. Geen uitzondering mogelijk.
.pdf reader	DC2015	DC2015	
Java 32bit	Corretto 8.232	Corretto 11.03.x	Maximaal een half jaar oud. Neem voor specifieke versie contact op. Mogelijk overgang naar AdaptOpenJDK in 2020
Media Player	MS Media Player 2013	MS Media Player 2013	
Flash player	Adobe Flash Player 32.x	Adobe Flash Player 32.x	Ivm naderend EOL/EOS overgang naar HTML5
Silverlight	OS release afhankelijk	Migreer naar HTML5	Ivm End Of Live Silverlight
Terminal Services	Windows remote desktop	Windows remote desktop	²
SBC Client	Citrix Receiver 4.7	Citrix Receiver 4.7	²
SCCM client	5.0.8	5.x	
.NET	.Net Framework 2.0 (uit .Net Framework 3.5 4.8	.Net Framework 4.8	

Opmerking. Office Applicaties worden in het image geplaatst. Om de stabiliteit maximaal te garanderen van de lokale Office applicaties is het voor overige producten niet toegestaan wijzigingen aan te brengen in de Office Applicatie bubble.

Mogelijke invoegtoepassingen die voor Office applicaties zijn bedoeld kunnen niet worden geïnstalleerd. Deze maatregel voorkomt dat er voor elke wijziging, van zowel de betrokken Office invoegcomponent, als vanuit Office365 een recursieve test met alle betrokken componenten moet worden uitgevoerd. Wijzigingen voor Office2016 Click2 Run worden vanuit Microsoft Office365 doorgevoerd. De wijzigingen, met uitzondering van kritische patches, worden bij ProRail op de werkplek ter beschikking gesteld middels het LCM proces in de cyclus van het Windows 10 Semi-Annual Channel en Office update proces.

¹ Bij het extern afnemen van terminal services dienst via een RDP (of variant) protocol dient deze door de leverancier via een HTTPS gateway aangeboden te worden.

In de groep optionele applicaties is het mogelijk om beperkt Microsoft Access ter beschikking te stellen als persoonlijk database programma. Vanwege netwerk technische en performance redenen mag de database niet in multi usermode worden gebruikt. Voor multi usermode databasesystemen dient SQL Server gebruikt te worden.

Het installeren van extensies in browsers is niet mogelijk op de werkplek. Indien een applicatie een browser extensie vereist wordt die extensie als onderdeel van het applicatiepackage opgenomen. Bij incompatibiliteit tussen een browserversie en een extensie heeft de browserversie prioriteit. Dit betekent dat een extensie uitgeschakeld kan worden na een browserupdate bij gebleken incompatibiliteit.

2.2 Auto update

Voor een aantal applicaties is het wenselijk dat nieuwe functionaliteit vaker dan 2x per jaar beschikbaar komt. Voor andere applicaties geldt dat beveiligingsaanpassingen vaker dan 2x per jaar moeten worden doorgevoerd. Applicaties worden nu per werkplek release geüpdatet. Indien applicaties de mogelijkheid biedt voor auto updates dan kan deze functie worden geactiveerd onder de volgende voorwaarden:

- Een applicatie mag een auto update uitvoeren zo lang de impact van de wijziging zich beperkt tot de applicatie zelf.
- Er geen componenten geüpgraded worden afkomstig uit andere packages, zoals bijvoorbeeld Office componenten die door Microsoft geplaatst worden.
- De eigenschappen van de werkplek moeten ongewijzigd blijven met uitzondering van de applicatie zelf.
- De functioneel beheerder van de applicatie stemt met zijn collega's van de applicatieketen af of de auto update functie geactiveerd wordt.

Het besluit wordt aangegeven op het AIF. Bij de omschrijving van de applicatie in de store wordt aangegeven dat de applicatie zichzelf update.

2.3 Netwerk

Hardware - netwerk			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Fabrikant routers, switches	Cisco		
Netwerk Protocollen	TCP/IP V4 (S)FTP, (S)RCP, RDP, NTP, HTTP(S), ICA, 802.1X	TCP/IP V4	IP V6 voorbereid
Services: DHCP, WINS, DNS, DFS	Windows 2019	Windows 2019	
Load Balancers	Citrix NetScaler VPX	Citrix NetScaler VPX	Versie 12

2.4 Security t.a.v. accounts

Naast technische maatregelen zoals genoemd in de tabel hieronder geldt er vanuit security de eis op traceerbaarheid. Dit betekent dat alle niet publiek toegankelijk informatie of handelingen voor het aanmaken en muteren van informatie herleidbaar moet zijn naar een natuurlijke persoon. Om deze reden zijn functionele accounts niet meer toegestaan. De CISO (Chief Information Security Officer), afd. Informatie Beleid, is de enige rol die hiervoor een uitzondering kan toestaan.

2.5 Security gerelateerde producten

preventie			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Virusscan server	McAfee ENS	McAfee ENS	vanaf 2018Q4
Client	Microsoft Endpoint Protection		
Exchange	Microsoft Exchange Online protection		
Encryptie client (inclusief USB storage)	BitLocker		
Reverse proxy / Proxy	NetScaler/ Cisco WSA		
SSL / TLS	Minimaal TLS 1.2		SSL3 en lager is niet toegestaan.
SMB	v2 bij voorkeur v3		
Apparaat netwerktoegangsbeveiliging (van toepassing op apparatuur die in een kantoor omgeving op het netwerk wordt aangesloten)	802.1X		Authenticatie voor device middels PEAP / EAP-TLS / PEAP-MSChapv2