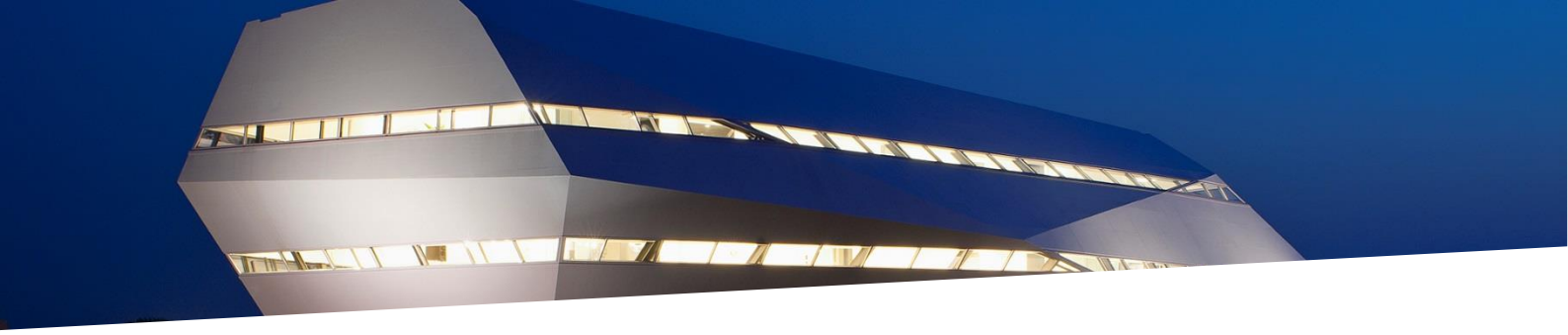

BEVEILIGINGSRICHTLIJNEN

JOIN ZAAK & DOCUMENT CONFIGURATIE

Introductie

Dit document beschrijft kort welke configuratie in JOIN Zaak & Document leidt tot een optimaal beveiligde omgeving. Wij adviseren om al deze punten door te lopen en de aanbevelingen op te volgen, tenzij in het verleden bewust anders is gekozen.

1. Gebruik parameterised database statements

De applicatie maakt standaard gebruik van zgn. parameterised statements bij het benaderen van de database. Het gebruik van deze statements maakt het benaderen van de database veiliger (en sneller). Het is sterk aan te bevelen deze functionaliteit niet uit te schakelen.

Instellingen in JOIN Config Editor:

- Miscellaneous Settings: Disable SQL parameter parsing (zet op False)

2. Gebruik geen RSS

De RSS-functionaliteit van JOIN Zaak & Document kent een lager niveau van authenticatie en wordt zelden of nooit gebruikt. Zet de RSS-functionaliteit uit.

Instellingen in de JOIN Config Editor:

- RSS Server Settings: RSS Server Enabled (zet op False)
- RSS Server Settings: RSS Allow anonymous access (zet op False)

3. Beperk overzichtenfuncties voor gebruikers

De overzichten-functie van het systeem controleert bij het genereren van de overzichten geen autorisaties meer. Bijvoorbeeld omdat managementinformatie anders onvolledig zou zijn, of omdat bij het verzenden van mails de ontvangers onbekend zijn. Deze autorisatie moet dus vooraf goed ingeregeld zijn.

Het is mogelijk om per overzicht te bepalen wie de overzichten mag bekijken of ontvangen. Voor eindgebruikers is het belangrijk om bewust om te gaan met het toekennen van het privilege om rapportages over gerelateerde items te maken.

Instellingen in JOIN Zaak & Document - Beheer:

- Overzichten: Gebruikersprofielrechten/Gebruikersrechten (controleer)
- Exceloverzichten: Gebruikersprofielrechten/Gebruikersrechten (controleer)

- Overzichten: Layout: Emailontvangers (controleer)
- Gebruikers/Gebruikersprofielen: Opties: Rapportages op gerelateerde items maken (vink Uit)

4. Controleer rechten voor raadpleeg-gebruikers

Raadplegers (viewclients) zijn niet altijd correct geautoriseerd, omdat de naam van deze gebruikersgroep impliceert dat zij alleen gegevens raadplegen. Dat is niet correct, omdat deze gebruikers ook individuele stukken kunnen toevoegen. Specifieke uitzonderingen voor deze groep gebruikers moeten goed staan om ervan verzekerd te zijn dat ook voor deze gebruikers de autorisatiematrix goed wordt toegepast.

Instellingen in JOIN Config Editor:

- Miscellaneous Settings: Viewclients Edit own files (zet op True)
- Miscellaneous Settings: Use rights for answer books (zet op True)

5. Controleer de standaardrechten

Als gebruikers helemaal geen autorisaties toegekend hebben gekregen past de applicatie een standaardrecht toe. Zorg ervoor dat dit standaardrecht op “Geen toegang” staat om niet ongemerkt toegang te verschaffen tot gegevens. Er is een afzonderlijk standaardrecht voor gebruikers, beheerders en voor de toegang tot tabellen.

Instellingen in de JOIN Config Editor:

- Default Rights: Default Admin Right (zet op N)
- Default Rights: Default Right (Zet op N)
- Default Rights: Default Table Right (Zet op N)

6. Pas de laagst toegekende autorisatie toe

Als gebruikers een actie toegekend krijgen, dan verkrijgen zij toegang tot het stuk waar de actie toe behoort. Dit kan het gewenste gedrag zijn, maar indien acties handmatig worden toegekend kan een foutieve handeling bij invoer ertoe leiden dat gebruikers stukken te zien krijgen waar ze eigenlijk niet toe gemachtigd zijn.
Indien een gebruiker vanuit zijn profielen meerdere conflicterende autorisaties heeft, is het instelbaar welke autorisatie wordt toegepast.

Instellingen in de JOIN Config Editor:

- Miscellaneous Settings: Do not elevate pending item rights (zet op True)

Instellingen in JOIN Zaak & Document - Beheer:

- Opties: Instellingen: “Geen toegang” krijgt voorrang bij rechten op meerdere gebruikersprofielen (vink Aan)

7. Gebruik de auditfunctie

De audit-functionaliteit van de applicatie is een krachtige bron van informatie om inzicht te krijgen in het gedrag van eindgebruikers. Het is mogelijk om te zien welke wijzigingen er zijn gemaakt, welke bestanden er zijn geopend en welke zoekopdrachten zijn gedaan. Dit is essentieel voor het maken van een reconstructie nadat er mogelijk misbruik is gemaakt van een account.

Instellingen in JOIN Zaak & Document - Beheer:

- Auditgegevens: Alle records (vink Aan)

8. Gebruik een beveiligde HTTPS verbinding

Als de applicatie benaderd wordt zonder adequaat beveiligde verbinding, is het mogelijk om vertrouwelijke informatie te onderscheppen als het netwerkverkeer tussen het werkstation en de server wordt onderschept.

Gebruik een SSL certificaat om een beveiligde HTTPS verbinding op te zetten in plaats van een HTTP verbinding. Zorg ervoor dat het SSL certificaat geen gebruik maakt van verouderde encryptiemethoden, maar tenminste TLS 1.0 én veilige cipher suites (geen MD5, IDEA or RC4). Zie hier voor meer informatie.

Dit betreft de infrastructuur van de applicatie. Deze wijziging kan niet door applicatiebeheer gedaan worden.

9. Beperk de toegang tot de applicatieserver

Kies bewust voor de mate van toegang tot de applicatie voor de eindgebruikers. Voorkom publieke internettoegang door (via VPN) de applicatie alleen voor het interne netwerk beschikbaar te maken.

Dit betreft de infrastructuur van de applicatie. Deze wijziging kan niet door applicatiebeheer gedaan worden.

10. Hergebruik het netwerkwachtwoord

Door wachtwoorden te koppelen aan het netwerkwachtwoord wordt automatisch het wachtwoordbeleid van de organisatie overgenomen. Hiermee wordt verzekerd dat wachtwoorden periodiek wijzigen en aan gestelde criteria voldoen. Ook hebben medewerkers die verwijderd worden uit de centrale directory van de organisatie direct geen toegang meer, zonder dat actie van de applicatiebeheerder noodzakelijk is. Het koppelen van wachtwoorden kan op basis van LDAP of ADFS.

Mocht het niet het mogelijk of wenselijk zijn om wachtwoorden te koppelen aan het netwerk, activeer dan een wachtwoordpolicy in de applicatie zelf.

Instellingen in de JOIN Config Editor:

- Authentication: LDAP Domain
- Authtentication: Use LDAP authentication
- Authentication: Enforce strong password
- ADFS Server: ADFS Server URL

Pas deze instellingen zorgvuldig aan; foutieve configuratie kan ertoe leiden dat niemand meer kan inloggen. Voor activatie van ADFS zijn aanvullende handelingen nodig.

11. Voorkom auto-aanvullen in het loginscherm

Uw browser kan de logingegevens van de applicatie onthouden en automatisch invullen als u de applicatie de volgende keer start. Dit kan betekenen dat iedereen die toegang heeft tot de werkplek vanzelf ingelogd kan worden. Het is mogelijk om de browser te instrueren om geen auto-aanvulfunctionaliteit te gebruiken in het loginscherm, zodat dit wordt voorkomen.

Instellingen in de JOIN Config Editor:

- Authentication: Enable Login Autocomplete (zet op False)

12. Voorkom ongewenst automatisch inloggen

Het is mogelijk om via Single Sign On het inlogproces helemaal over te slaan. De identiteit van de gebruiker die is ingelogd op het werkstation wordt dan hergebruikt. Dit betekent dat iedereen die toegang heeft tot de werkplek vanzelf ingelogd wordt. Het is mogelijk om het automatisch inloggen helemaal uit te schakelen, of uitsluitend te beperken tot werkplekken binnen de organisatie.

Gebruikers die met tablets werken blijven langer ingelogd dan hun sessie. Het is aan te bevelen die periode te beperken tot minder dan een dag.

Instellingen in de JOIN Config Editor:

- Authentication: Use single logon (Zet op False, of op een (lijst van) toegestane IP ranges (bijv. 10.180.*.*))
- Authentication: Valid domain (Zet op de LDAP-domeinnaam van de organisatie)
- Authentication: Login lifetime for tablet application (Zet op 12 uur)

13. Koppel gebruikersbeheer aan de Active Directory

Beheerders van de applicatie kunnen zelf gebruikers aanmaken, autorisaties toekennen en vervolgens namens die gebruiker handelingen uitvoeren. Het is dan niet te herleiden welke persoon die handelingen heeft uitgevoerd.

Het is mogelijk om het gebruikersbeheer te koppelen aan de Active Directory, zodat medewerkers vanzelf worden aangemaakt of gedeactiveerd. Bij de configuratie van deze koppeling kan worden opgegeven dat dit de enige manier moet zijn om gebruikers aan te maken in de applicatie. Ook applicatiebeheerders kunnen dan geen gebruikers meer aanmaken.

Indien de applicatie gebruik maakt van ADFS (zie punt 10), dan is het mogelijk om logins uitsluitend via het ADFS inlogvenster te laten verlopen. Hiermee wordt hetzelfde resultaat bereikt.

Instellingen in de DecosLdapImport.exe.config:

- USERSCREATEDBYLDAP (Zet op 1)

Instellingen in JOIN Config Editor:

- ADFS\Application Preferences: Allow login fallback (zet op False)

14. Beperk sessies

Door gebruikers te beperken tot slechts één sessie valt het eerder op als andere gebruikers hetzelfde account gebruiken om toegang tot het systeem te krijgen.

Instellingen in de JOIN Config Editor:

- Miscellaneous Settings: Limit users to one single web session (zet op True)

15. Beperk bestandstypen

Het is aan te raden om geen bestanden in het systeem te laten plaatsen die uitgevoerd kunnen worden op de server of op de werkstations van eindgebruikers.

Instellingen in de JOIN Config Editor:

- File Transfer: Disallowed file extensions (zet op exe|com|bat|htm|html|js|reg|vbs)

16. Cache geen afbeeldingen van bestanden

De bestandsviewer van JOIN Zaak & Document plaatst afbeeldingen in de tijdelijke internetbestanden van het werkstation, zodat deze afbeeldingen worden hergebruikt op het moment dat het bestand voor een tweede keer bekeken wordt. Ondanks dat de tijdelijke internetbestanden standaard zijn afgeschermd voor andere gebruikers, bestaat hierdoor wel de kans dat er lokaal bestanden achterblijven op de werkplek.

Instellingen in JOIN Config Editor:

- File Viewer Settings: Cache file viewer images in the browser (zet op False)

17. Beperk javascript-transparantie voor eindgebruikers

De applicatie maakt gebruik van javascript voor interactieve onderdelen. Dit script is inzichtelijk als de eindgebruiker de broncode van de webpagina bekijkt. Hierdoor kan extra inzicht worden verkregen in de werking van de applicatie.

Het is mogelijk om de transparantie van deze scripts te beperken, zodat de applicatie moeilijker te doorgronden is.

Instellingen in JOIN Config Editor:

- Logging: Stream Minified javascript (zet op True)
- Logging: Enable javascript console logging (zet op False)