Inloggen

Alle inloghandelingen worden apart gelogd op de webserver. Het wegschrijven van deze log kan een probleem op zichzelf zijn (schijf vol, server uit de lucht). Indien dit het geval is dan verschijnt de mededeling: Foutcode: Log aanmaken mislukt.

Hieronder de programmaflow van de inlogprocedure en de instellingen die daarop van invloed zijn.

N.B.

De hieronder beschreven programmaflow geldt NIET voor het inloggen middels Single Sign On. Zie pagina Single Sign On voor **de inlogvereisten Single Sign On en benodigde instellingen**.

1. Kloppen login en wachtwoord?

De login (niet case sensitive) wordt vergeleken met tbmedewerkers dvloginnaam. Het wachtwoord (case sensitive) wordt omgezet in bcrypt met het aantal costs van het opgeslagen gecrypte password in medewerkerskolom *pass* (tbmedewerkers.dvpasswcrypt) en hiermee vergeleken. Geen match dan wordt er opnieuw om gevraagd met een tussenpozen van de instelling *Getal1* bij *Sectie: Logon* en *Item: WachtAantalMilliseconden* (default 3000).

2. Mag de inlogger gebruik maken van de browser-versie

De medewerkerskolom *1=desktop, 2=browser, 3=beide* (Tbmedewerkers.dnmaginapp) moet de waarde 2 of 3 hebben: zo niet dan zijn er onvoldoende rechten. De medewerker moet ook verbonden zijn aan een rechtengroep die op minimaal één van de modules (bouw/sloop, horeca, handhavingen, APV/overig/ milieu/gebruik/ info, omgeving of inrichtingen) kijkrechten heeft.

3. Is de medewerker nog in dienst?

Wanneer tbmedewerkers.ddvervaldatum < = vandaag dan is deze vervallen en mag niet inloggen.

4. Is het wachtwoord tijdelijk uitgegeven en is die datum verstreken?

Dit is het geval indien op de medewerkerskaart de kolom *(tijdelijk) geldig tot* (tbmedewerkers.ddlockedfrom) is gevuld met een datum die kleiner is dan de systeemdatum. Er volgt een mededeling *Geldigheid tijdelijke inlog verstreken; neem contact op met de beheerder*.

5 Is het wachtwoord verlopen?

Dit is het geval indien:

- de kolom *Password verloopt nooit* NIET aangevinkt is (tbmedewerkers.dlpassneverexpires = 'F')
- EN minimaal één van onderstaande items is waar:
    - (dddatumpassword is null)
    - (dddatumpassword + aantal dagen van instelling *Getal1* van *Sectie: Logon* en *Item: Password_MaxDagenSindsCreatie* (defaultwaarde 365 < = vandaag).

Zo ja dan wordt om nieuw wachtwoord gevraagd. Dit wordt gecontroleerd op de volgende elementen:

- alleen karakters asci 32 t/m 126 dat zijn a-z A-Z 0-9 en een spatie en de tekens: !“#$%&'()*+,-./:;⇔?@[\]^_`{|}~ (33stuks)
- moet ongelijk zijn aan inlognaam
- moet ongelijk zijn aan oude wachtwoord
- lengte moet groter of gelijk zijn dan de instelling *Getal1* van *Sectie: Logon* en *Item: Pass_MinLength* (default 9)
- het moet aan een bepaalde complexiteit voldoen zoals ingesteld in *Getal1* van *Sectie: Logon* en *Item: Minimumwachtwoordcomplexiteit*. Defaultwaarde = 3. Alleen 0,1,2,3 of 4:
    - 0 = too guessable: risky password (guesses < duizend)
    - 1 = very guessable: protection from throttled online attacks (guesses < 1 miljoen)
    - 2 = somewhat guessable: protection from unthrottled online attacks (guesses < 100 miljoen)
    - 3 = safely unguessable: moderate protection from offline slow-hash scenario (guesses < 10 miljard)
    - 4 = very unguessable: strong protection from offline slow-hash scenario (guesses >= 10 miljard).

Indien mogelijk geeft het programma een hint wanneer een nieuw wachtwoord wordt afgekeurd. Bij niet voldoende complexiteit is dat:*Password te voorspelbaar* mogelijk gevold door één van onderstaande teksten:

- toetsenbordrijtjes zijn makkelijk te raden.
- Korte toetsenbordpatronen zijn makkelijk te raden.
- herhalingen als aaa zijn makkelijk te raden.
- herhalingen zijn makkelijk te raden.
- reeksen als abc or 6543 zijn makkelijk te raden.
- recente jaartallen zijn makkelijk te raden.
- deze staat in de top 10 van meest gebruikte passwords.
- deze staat in de top 100 van meest gebruikte passwords.
- dit is een heel gebruikelijk password.
- dit is vergelijkbaar met een veelgebruikt password.
- een woord op zichzelf is gemakkelijk te raden.
- namen en achternamen op zichzelf zijn gemakkelijk te raden.

Het nieuwe valide password wordt omgezet in bcrypt met het aantal costs van instelling *Getal1* van *Sectie: Logon* en *Item: bcrypt_costs* (default 10).

6. Tijdelijkheid wachtwoord opheffen?

Indien:

- op de medewerkerskaart de kolom *tijdelijke geldigheid opheffen na succesvol inloggen*

(tbmedewerkers.dlopheffenlock) is aangevinkt
- EN de inlogger heeft met succes een nieuw password aangemaakt (vanwege verlopen van de oude)

dan zal op de medewerkerskaart de kolom *(tijdelijk) geldig tot* (tbmedewerkers.ddlockedfrom) worden leeggemaakt.

7. Is 2 factor ingesteld?

2-factor is ingesteld indien:

- de instelling bij *Sectie: Logon* en *Item: 2-factor* is aangevinkt
- EN op de medewerkerskaart de kolom *2-factor type* is ingevuld met de waarde 1 (email) of 2 (sms)
- EN op de medewerkerskaart de kolom *2-factor auth. opheffen* NIET aangevinkt is (tbmedewerkers.dldeviceunlockdisabled = 'F')
- EN het IP-adres waarvan wordt ingelogd voldoet aan geen enkel masker gedefinieerd in de kolom dviprange van de tabel tbipranges (beheerportaal-Nieuw) waarvoor geldt dat de kolom dlskip2factor de waarde 'T' heeft (aangevinkt is) en vervaldatum leeg.

Is dit het geval dan wordt de device van de inlogger als cookie gecontroleerd met tbmedewdevices.dvunlockcookie.

Is de device niet bekend of verlopen (waarbij timestamp wordt vergeleken met tbmedewdevices.ddeunlockcookie + het aantal dagen van instelling *Getal1* van *Sectie: Device* en *Item: Unlock_Cookie_MaxDagenSindsCreatie* (default 365) dan wordt om een unlock pincode gevraagd.

Deze unlockcode wordt tijdelijk opgeslagen in tbmedewekers.dvdeviceunlockcode en de timestamp waarop dat is gebeurd wordt vastgelegd in tbmedewerkers.ddpinunlockcode.

Bovendien wordt de unlockcode:

- ofwel per mail gestuurd naar de inlogger (indien gevulde tbmedewerkers.dvemail). Dit is het geval indien op de medewerkerskaart de kolom *2-factor type* is ingevuld met waarde 1 (tevens defaultwaarde)
- dan wel per sms gestuurd naar de inlogger (indien gevulde tbmedewerkers.dvmobiel). Dit is het geval indien op de medewerkerskaart de kolom *2-factor type* is ingevuld met waarde 2. Het bericht naar de web service van de telecomprovider waarmee hiertoe een contract is afgesloten (die het bericht omzet in een sms) wordt ook gelogd in tbmessagelog (beheertegel *Messagelog*).

Voor e-mailinstellingen zie het hoofdstuk: E-mail SMTP instellingen. Standaard wordt de inhoud van de kolom *Tekst* van de instelling *Sectie: Logon en Item: AfzenderAdres* als afzender genomen voor het verzenden van de unlockcode. Bestaat deze instelling niet (of is *Tekst* leeg) dan zal als afzender de default waarde worden gezet: noreply@openwave.nl.

Voor sms-instellingen zie het hoofdstuk: SMS.

Voor medewerkers zie het hoofdstuk: Medewerkers. Voor vrijstellen 2-factor op basis van IP-adres zie IP-ranges.

De inlogger heeft dan tbmedewerkers.ddpinunlockcode + het aantal uur van de instelling *Getal1* van *Sectie: Device* en *Item: Unlock_Pin_MaxUurSindsCreatie* (default 1) de tijd om de unlockcode door te voeren.

Bij succes EN indien het attribuut op de medewerkerskaart van de inlogger *Verboden om device op te slaan* NIET is aangevinkt, dan wordt de device toegevoegd of vernieuwd in de tabel tbmedewdevices met een nieuwe tbmedewdevices.ddeunlockcookie. Als het programma deze unlockcookie niet kan of mag opslaan dan zal bij 2-factor authenticatie altijd om een nieuwe unlockcode worden gevraagd.

Indien OpenWave wordt gebruikt op dezelfde device vanuit twee verschillende browsers, dan ziet het programma dit als twee verschillende apparaten (cookies worden per browser opgeslagen).

8. Afvinken inlogverklaringen

Indien een inlogverklaring is klaargezet (zie: Loginverklaringen) waarvan:

- de vervaldatum leeg is of in de toekomst ligt
- EN waarvan de ingangsdatum leeg is OF kleiner of gelijk is dan de systeemdatum

dan zal deze verklaring aan de betrokken medewerker die inlogt getoond worden, mits

- de eigenschap op de medewerkerskaart (beheerportaal-Nieuw) *deze medewerker hoeft geen loginverklaringen af te vinken* uit staat (tbmedewerkers.dlskiploginverkl = 'F')
- EN de betreffende verklaring is nog niet eerder afgevinkt of is verlopen. Dat wil zeggen:
  - in tbmwloginverklaringen is geen regel aanwezig bij de medewerker met de betreffende verklaring
  - OF die regel is wel aanwezig maar de afvinkdatum (dddatumgelezen) is langer gelezen dan het aantal herhaaldagen dat is opgegeven bij de verklaring.

De medewerker zal in dat geval de verklaring moeten aanvinken alvorens de toegang tot het openingsportaal wordt verleend. Er wordt een regel aangemaakt in tbmwloginverklaringen met als afvinkdatum de systeemdatum. Indien de regel al bestond in tbmwloginverklaringen en de verklaring was getoond vanwege het verlopen van de afvinkdatum (datumgelezen) op die regel, dan zal enkel die datum worden aangepast.

Na het afvinken zal het programma opnieuw kijken of er (nog) een verklaring klaar staat en deze tonen.

9. Maak sessie

Bij succesvol inloggen wordt voor de inlogger een nieuwe sessie aangemaakt die een instelbare periode geldig blijft. Is die periode afgelopen dan moet de inlogger opnieuw inloggen. Het gaat om twee instellingen in tbinitialisatie:

- *Getal1* van *Sectie: Sessie* en *Item: MaxUurSindsCreatie* (default 144) de sessie blijft zolang bestaan vanaf de creatie
- *Getal1* van *Sectie: Sessie* en *Item: MaxUurSindsAanroep* (default 12).

In de beheertabel tbsession wordt bij het inloggen per medewerker een kaart gemaakt met de

uitgetrokken sessie-id en het tijdstip dat de kaart gecreëerd is (ddcreated). Elke keer dat de medewerker een API-aanroep in OpenWave doet, wordt de kolom ddinvoked overschreven met het tijdstip van dat moment (om nodeloze schrijfacties te vermijden gebeurt dit slechts wanneer het oude tijdstip 10 minuten of langer geleden is). Deze 10 minuten zijn niet instelbaar.

De instelling MaxUurSindsAanroep wordt dus vergeleken met tbsession.ddinvoked.

De instelling MaxUurSindsCreatie wordt vergeleken met ddcreated.

Waarschuwing

Wanneer Single Sign-On ingesteld staat dan dient men de geldigheidsduur van een sessie van een gebruiker in te stellen op de Single Sign-On server zelf. De instellingen op de Single Sign-On server overrulen deze instellingen.

Huidige inlogmethode: getAccess

Eerdere versies dan 1.30 van OpenWave ondersteunde nog, indien zo ingesteld, een oude manier van inloggen. Huidig is dit niet meer mogelijk en wordt altijd de inlogmethode: *getAccess* toegepast. Dit is een vervanger van de oude inlogmethode met het oog op toekomstige uitbreidingen van OpenWave. De beschreven programmalogica op deze pagina is van toepassing op de getAccess methode.

Voor de werking van de inlogmethode moeten de volgende instellingen van toepassing zijn:

- instelling *Sectie: PreInlog* en *Item: ProductNaam* moet bestaan en aan staan en *Tekst* heeft waarde *OpenWave*
- instelling *Sectie: PreInlog* en *Item: GebruikersnaamVergeten* (optioneel). Als bestaat en aan staat dan kan men gebruikmaken van gebruikersnaam vergeten functionaliteit
- instelling *Sectie: PreInlog* en *Item: WachtwoordVergeten* (optioneel). Als bestaat en aan staat dan kan men gebruikmaken van wachtwoord vergeten functionaliteit.

Een overige instelling voornamelijk voor de esthetiek:

- instelling *Sectie: Logon* en *Item: Logo* moet aan staan en *Tekst* = left.

De volgende instellingen zijn benodigd voor het vullen van de gebruikersnaam en wachtwoord vergeten mails aan de gebruiker:

- instelling *Sectie: Inloggegevens* en *Item: WachtwoordEmailTekstBody*. In kolom *Info* staat de tekst van de body van de wachtwoord vergeten mail
- instelling *Sectie: Inloggegevens* en *Item: WachtwoordEmailTekstOnderwerp*. In kolom *Tekst* wordt het onderwerp opgegeven van de wachtwoord vergeten mail
- instelling *Sectie: Inloggegevens* en *Item: GebruikersnaamEmailTekstBody*. In kolom *Info* staat de tekst van de body van de wachtwoord vergeten mail
- instelling *Sectie: Inloggegevens* en *Item: GebruikersnaamEmailTekstOnderwerp*. In kolom *Tekst* wordt het onderwerp opgegeven van de wachtwoord vergeten mail.

inloggen