# 2-way encryptie van externe wachtwoorden

Op een aantal plekken in de database van OpenWave zijn externe wachtwoorden opgeslagen die het programma gebruikt voor authenticatie bij berichtenverkeer naar webservices van derden of voor toegang tot een fileshare.

Deze wachtwoorden kunnen nu geëncrypt worden opgeslagen, zodat iemand die toegang heeft tot de database niet direct externe wachtwoorden kan uitlezen. De encryptie moet door OpenWave ongedaan gemaakt kunnen worden, omdat de ongecrypte versie (plain) gebruikt wordt voor authenticatie. Vandaar 2-weg encryptie. 2-weg encryptie werkt altijd met een secret-key die per OpenWave installatie op de webserver wordt opgeslagen in de file wave.ini in de wsas.conf map. Om deze key in te zien of te wijzigen zijn dus systeembeheerrechten op die webserver-machine nodig.

## Encryptie methode (DEPRECATED)

Notitie

De instelling voor de encryptie van wachtwoorden is deprecated: Dit betekent dat de Java niet meer kijkt naar de instelling Encryption - Method. Nu is de methode altijd 3 (ontcrypten met AESkey die te vinden is in de ini-file van OpenWave). Het kan zijn dat er in de toekomst weer 1 bij komt, maar voor nu alleen AESkey encryptie.

Er waren drie manieren waarop een wachtwoord geëncrypt kan worden:

De methode die OpenWave gebruikt is instelbaar met de waarde van *GetaI1* van de instelling *Sectie: Encryption* en *Item: Method*.

Deze waarde kan zijn: 1 of 2 of 3.

Indien een andere waarde dan 1, 2, of 3 is ingevuld of wanneer de instelling niet bestaat, dan is de default encryptiemethode 1.

Indien de encryptie methode:

- = 1 dan wordt het ingebrachte wachtwoord **plain** opgeslagen voorafgegaan door '01_'
- = 2 dan wordt het ingebrachte wachtwoord met de interne sleutelfunctie **RemCrypt** opgeslagen voorafgegaan door '02_'
- = 3 dan wordt het ingebrachte wachtwoord **AES256** versleuteld opgeslagen voorafgegaan door '03_'

Doordat het geëncrypte wachtwoord voorafgegaan wordt door de prefix 01_, 02_ of 03_ weet OpenWave hoe het geëncrypte wachtwoord ontsleuteld moet worden. Indien de prefix 01_, 02_ of 03_ ontbreekt dan wordt er uiteraard helemaal niets gedecrypt.

Waarschuwing

Het wijzigen van de encryptiemethode betekent niet dat bestaande versleutelingen automatisch

aangepast worden. De plain-versie van het te crypten wachtwoord zal opnieuw over de bestaande (al of niet gecrypte) versie heen geschreven moeten worden, waarna het programma de ingevoerde waarde encrypt volgens de op dat moment ingestelde methode.

## Welke methode wanneer

- De methode 1 (plain) wordt gebruikt indien er andere programma's zijn die ook van dezelfde OpenWave database gebruik maken om wachtwoorden voor externe authenticatie op te halen, maar die geen toegang of functionaliteit hebben tot de sleutels van RemCrypt en AES256. Deze methode kan ook als veiligheidsklep fungeren indien onverhoopt de andere versleutelingen problemen geven.
- De methode 2 (RemCrypt) wordt gebruikt indien er andere programma's zijn die ook van dezelfde OpenWave database gebruik maken om wachtwoorden voor externe authenticatie op te halen (OpenWave desktop!!!) EN die wel toegang en functionaliteit hebben voor RemCrypt versleuteling, maar niet voor AES256.
- De methode 3 (AES256) wordt gebruikt indien er GEEN andere programma's zijn die van dezelfde OpenWave database gebruik maken om wachtwoorden voor externe authenticatie op te halen.

## Extra restricties

De te encrypten wachtwoorden mogen niet langer zijn dan 158 tekens en alleen karakters mogen gebruikt worden van de ASCII-reeks 32 t/m 126 dat zijn: a-z A-Z 0-9 en een spatie en de tekens: !“#$%&'()*+,-./:;⇔?@[\]^_`{|}~ (33stuks).

## Foutmeldingen

- Wanneer het encrypten mislukt vanwege te lange string dan komt foutcode 201 in beeld.
- Anders, wanneer encrypten mislukt vanwege andere oorzaak dan komt foutcode 696 in beeld.
- Wanneer het decrypten mislukt wordt een lege string gebruikt als authenticatie.

## Voor welke cellen is de 2-way encryptie enabled?

Dit betekent dus, dat wanneer bij onderstaande cellen een nieuwe waarde wordt ingebracht, deze wordt geëncrypt volgens methode 1 of 2 of 3.

- Tabel TbInitalisatie: (de genoemde kolommen zijn zichtbaar als ):
    - *Sectie: Documenten* en *Item: OphalenViaFileserver_Password* (authenticatie voor opslaan/ophalen documenten op fileshare)
    - *Sectie: KOPPELING ZAAK* en *Item: HTTPAuthenticatiePass* (http-authenticatie voor stuf zaak/DMS creëer en update-berichten)
    - *Sectie: KOPPELINGDOCNAARDMS* en *Item: HTTPAuthenticatiePass* (http-authenticatie voor stuf zaak/DMS plaatsen en ophalen-documenten berichten)
    - *Sectie: KOPPELINGDOCNAARDMS* en *Item: Pass_cmis* (Authenticatie voor DMS benadering

via CMIS)
    - *Sectie: KOPPELINGBAG* en *Item: HTTPAuthenticatiePass* (http-authenticatie voor stuf BAG-berichten)
    - *Sectie: KOPPELINGGBA* en *Item: HTTPAuthenticatiePass* (http-authenticatie voor stuf GBA-berichten)
    - *Sectie: KOPPELINGNHR* en *Item: HTTPAuthenticatiePass* (http-authenticatie voor stuf NHR-berichten)
    - *Sectie: Web.sms* en *Item: password* (password voor endpoint telecomprovider sms-berichten bij inloggen met 2-factor)
    - *Sectie: KadasterBAG* en *Item: password* (password voor endpoint ophalen maandmutaties BAG)
    - *Sectie: SingleSignOn* en *Item: clientsecret*
    - *Sectie: Xential* en *Item: password* Opvragen ticketid bij Xential
    - *Sectie: Logon* en *Item: externOLOpass*
    - *Sectie: koppeling OLO* en *Item: ftps-site* Ophalen gemiste OLO-documenten (paswword ftp site)
    - *Sectie: OnlyOffice* en *Item: sleuteldomein*
    - *Sectie: REV* en *Item: client_secret*
- Tabel tb33gemeente: kolom dvBrpSslKeystorePassword
- Tabel tbmedewerkers: kolommen dvdmspass en dvextchklstpass

Verder kan de encryptiemethode worden aangeroepen vanuit een documentsjabloon. De string <%strEncrypt(:columnname)%> in een sjabloon wordt bij het creëren van een document als volgt geïnterpreteerd. Het programma zal columnname interpreteren als een kolomnaam uit de hoofdtabel van het sjabloon. De waarde van die kolom wordt gecrypt volgens de ingestelde methode en deze gecrypte waarde wordt in het document opgenomen op de betreffende plaats. Voorbeeld: <%strEncrypt(:dnkey)%>.