Instellen en gebruik beheer-ID en token

Maak je gebruik van een app als token? Dan dien je deze eerst te installeren op jouw mobiele telefoon. Gebruik de app FreeOTP, verkrijgbaar in de App stores:

- FreeOTP voor Android
- FreeOTP voor Apple

FreeOTP is gratis, open source, en werkt eenvoudig en betrouwbaar. Andere OTP-apps werken ook, bijvoorbeeld Google Authenticator of Microsoft Authenticator.

1. Activeren beheer-ID en instellen token

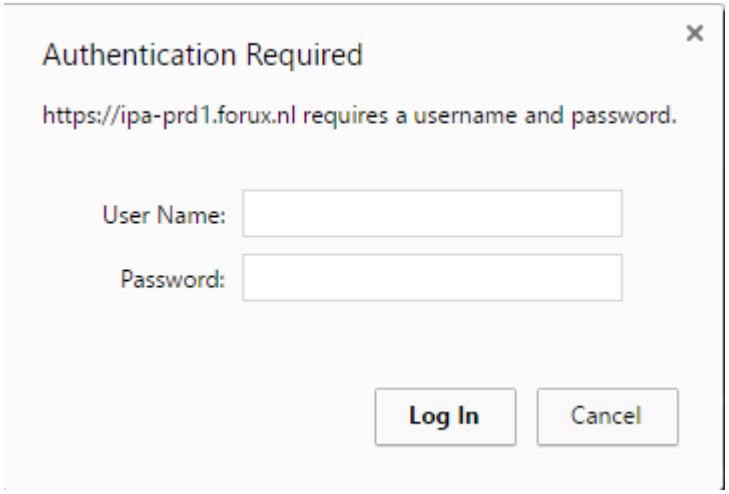
Controleer of je de volgende gegevens hebt:

- Jouw nieuwe beheer-ID (username). Dit is jouw HvA-ID met voorvoegsel ‘b-‘.
- Een tijdelijk wachtwoord.
- Een YubiKey (usb-stick) òf de mededeling dat je een app nodig hebt.

Stap 1 – Inloggen op de beheer-ID zelfbediening

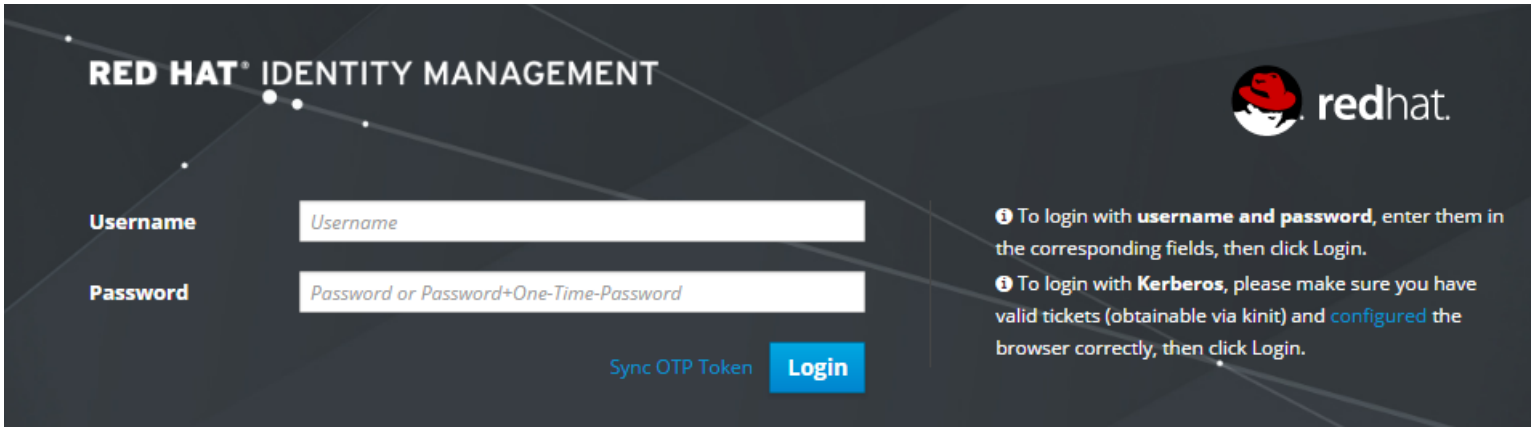
Voor het instellen van beheer-ID’s is er een speciale zelfbediening: https://beheerid.hva.nl.
Toegang tot deze website is alleen mogelijk vanuit het HvA-netwerk; zie hoofdstuk 5 wat je moet doen als je nooit op een HvA-locatie komt.

Ga met jouw browser naar https://beheerid.hva.nl.
In **sommige** browsers (Google Chrome) krijg je nu een pop-up:



Klik op Cancel als je dit krijgt (het is een bug).

Je krijgt nu het volgende inlogscherm:



Vul jouw beheer-ID (b-xxx) bij *Username* in en jouw tijdelijke wachtwoord bij *Password*.

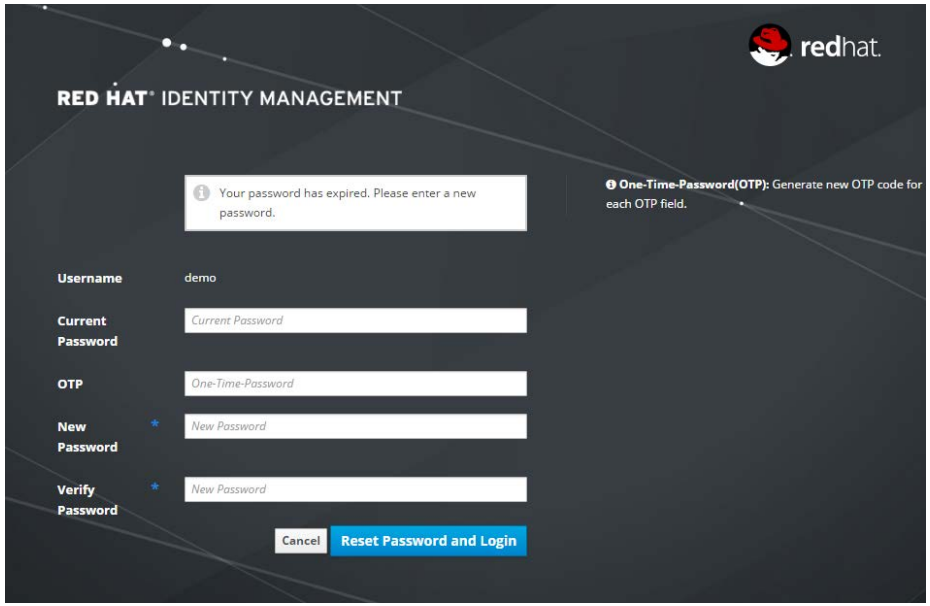
Als je al een YubiKey (usb-stick) hebt gekregen, laat de cursor dan direct achter jouw wachtwoord staan, stop de YubiKey in een usb-poort, en druk ~1 sec op de knop van de YubiKey (er moeten 8 sterretjes verschijnen). Klik daarna op ‘Login’.

Stap 2 – Instellen wachtwoord

Er verschijnt nu een scherm waarop je jouw definitieve wachtwoord moet kiezen:

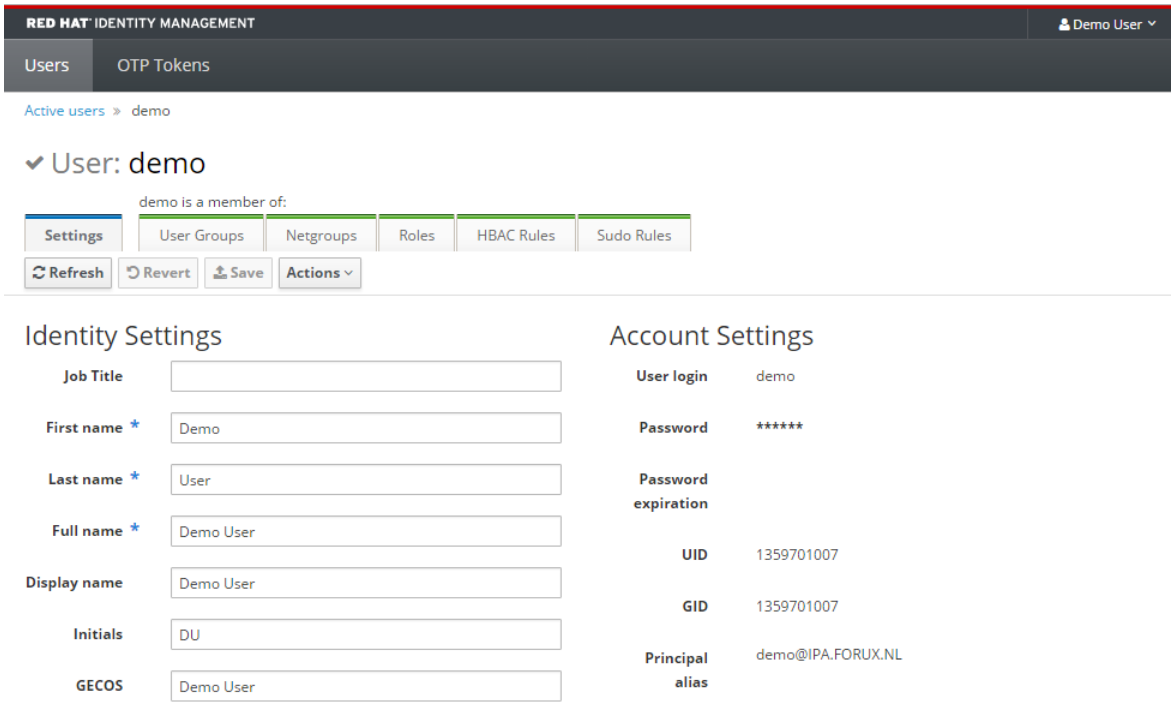
Vul in:

- *Current password*: jouw tijdelijke wachtwoord
- *OTP*: *<alleen invullen als je al een YubiKey of app hebt>*
  YubiKey: Klik in dit veld en druk op de knop van jouw YubiKey. Er moeten 8 sterretjes verschijnen.
  App: typ de unieke code over.
- *New password*: vul jouw definitieve wachtwoord in. Dit moet voldoen aan de volgende eisen:
  - Moet èn een kleine letter èn een hoofletter èn een cijfer èn een leesteken bevatten.
  - Totale lengte minstens 10 tekens.
- Klik vervolgens op ‘Reset Password and Login’.



Je krijgt nu de melding dat jouw wachtwoord-update gelukt is.
Alleen als je al een token hebt moet je vervolgens opnieuw inloggen (met het nieuwe wachtwoord en de unieke code), anders gaat dat vanzelf.

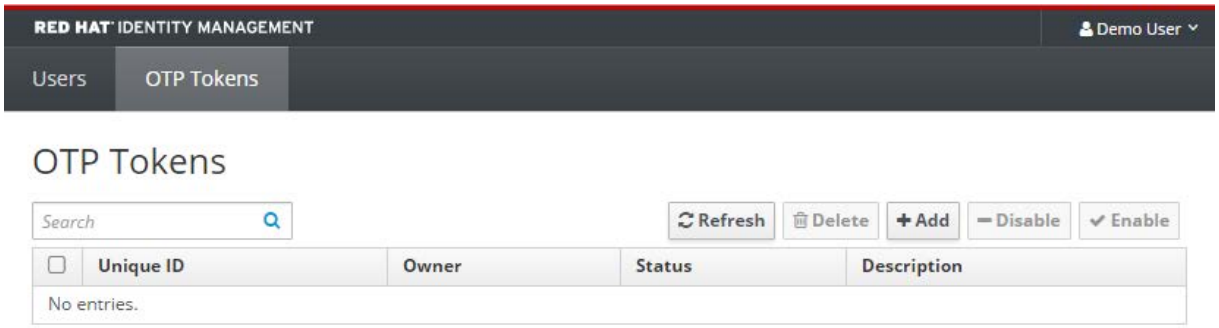
Na een paar seconden (even geduld!) verschijnt het volgende scherm:



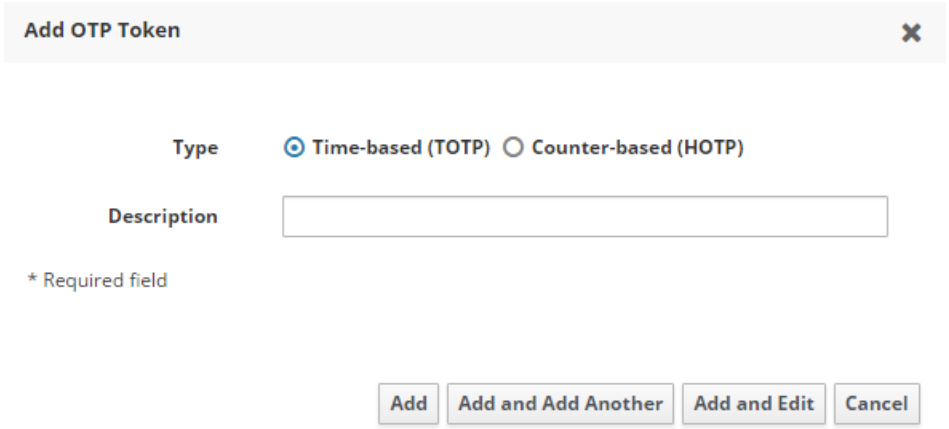
Je bent succesvol ingelogd met jouw nieuwe wachtwoord.

Stap 3 – Instellen app

Als je een YubiKey krijgt of hebt kun je deze stap overslaan en naar 'Stap 4: Uitloggen' gaan.
Klik in de grijze balk bovenaan op 'OTP Tokens'. Je krijgt het volgende scherm:

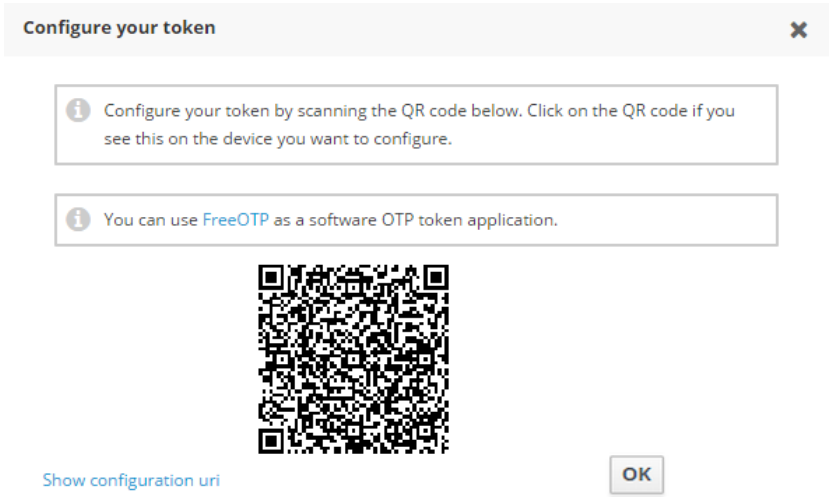


Klik rechts op de knop ‘+Add’. Je krijgt de volgende pop-up:



Kies voor *Counter-based (HOTP)*. [Time-based mag ook, maar is lastiger in gebruik].
Vul bij *Description* jouw beheer-ID in. Klik op ‘Add’.

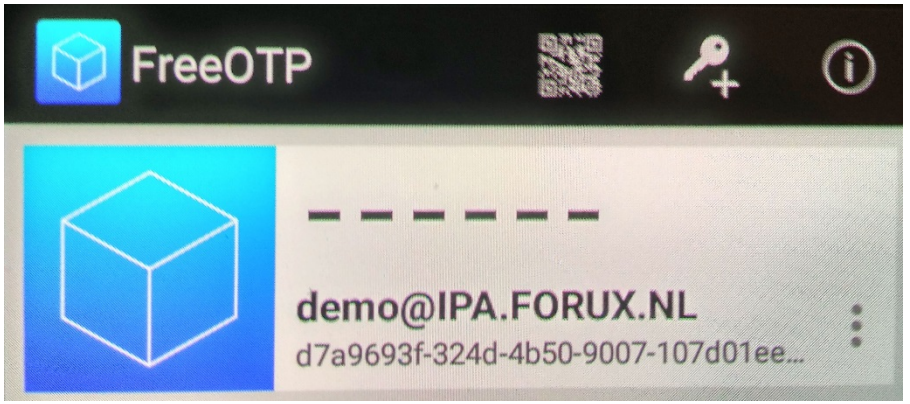
Je krijgt nu een QR-code op het scherm:



Open de app op jouw mobiele telefoon. Dit voorbeeld gaat uit van de app FreeOTP.
Scan de QR-code van het scherm m.b.v. jouw camera door op het QR-symbooltje te klikken:

De app zal nu jouw camera gebruiken. Richt de camera zodat de QR-code precies in beeld komt.
Zodra de app de code herkent wordt deze ingelezen.

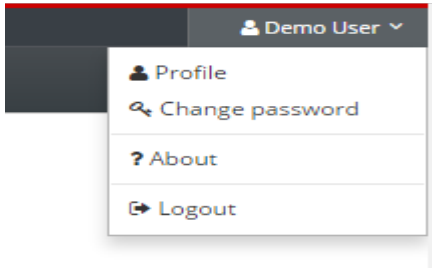
De token wordt nu ingesteld, met als naam <beheer-id>@IPA.FORUX.NL.



Klik in jouw browser op ‘OK’.

Stap 4 – Uitloggen

Klik in de browser rechtsboven op jouw naam en selecteer ‘Logout’:



Je bent nu klaar om jouw beheer-ID te gebruiken.

2. Gebruik beheer-ID en token

Als je op de beheer-VPN inlogt vul je jouw beheer-ID in als *username*.
Als *password* moet je jouw wachtwoord invoeren, ***direct gevolgd door de unieke code.***

Hoe je dit doet is afhankelijk van het type token dat je hebt:

- Bij gebruik van de app op jouw telefoon, start je deze op en klik je op jouw beheer-ID.
  De zes (of acht) cijfers die je dan te zien krijgt zijn jouw unieke code.
  Als password vul je in: MijnPassword123456
- Bij gebruik van een YubiKey stop je jouw usb-stick in een usb-poort van je computer.
  Als password vul je in: MijnPassword
  Direct daarna druk je ~1 sec op de knop van jouw YubiKey; de unieke code wordt automatisch achter jouw eigen wachtwoord gezet.

Zorg dat je jouw token altijd bij de hand hebt. ***Zonder token kun je geen gebruik maken van de beheer-VPN en heb je geen beheertoegang.***

Verlies van een token dien je altijd ***direct te melden*** bij de servicedesk ICTS.

3. Meer over de beheer-ID zelfbediening

De zelfbediening voor beheer-ID's zal je ook later nodig kunnen hebben:

- Als je jouw wachtwoord vergeten bent krijg je een nieuw tijdelijk wachtwoord. Je moet dan weer een definitief wachtwoord instellen zoals hierboven beschreven in stap 1 en 2.
  Let op: Bij stap 2 moet je nu ook de unieke code opgeven van jouw token.
- Als je jouw token kwijt bent wordt het (na een melding!) uit het systeem verwijderd. Je dient een nieuwe token in te stellen als in stap 3. Je logt op de zelfbediening in met alleen jouw wachtwoord.
- Als je jouw wachtwoord èn token kwijt bent worden beide verwijderd en krijg je een nieuw tijdelijk wachtwoord. Je doorloopt dan weer stap 1 tot 3.

Het beheer-ID systeem wordt in de toekomst ook gebruikt voor toegang tot Linux-servers. Je gebruikt de beheer-ID zelfbediening dan óók om Linux-specifieke zaken, zoals SSH public keys, te beheren.

4. Meer over YubiKeys

YubiKeys zijn usb-sticks, die zich gedragen als een toetsenbord. Door op een knop te drukken wordt een unieke code verstuurd, alsof je het zelf intypt.

De Yubikey 4 wordt gebruikt. Omdat deze een USB-A aansluiting heeft kan dit lastig zijn in sommige (nieuwere) laptops die alleen USB-C aansluiting hebben. Op verzoek kan een Yubikey 4 Nano met USB-C adapter geleverd worden. In alle andere gevallen dien je zelf voor een geschikte adapter te zorgen.

YubiKeys zijn hardware-devices en daarom veiliger dan tokens zoals een app. Voor toegang tot de meest kritische systemen stelt de HvA de YubiKey verplicht. Voor de meeste systemen is een app voldoende; op speciaal verzoek (bijvoorbeeld wegens slechtziendheid) kan een YubiKey gebruikt worden.

5. Toegang vanuit internet tot beheer-ID zelfbediening

De beheer-ID zelfbediening is, in tegenstelling tot de beheer-VPN, niet toegankelijk van buiten het HvA-netwerk. Dat kan een probleem zijn voor wie nooit op HvA-locaties werkt.

Er zijn verschillende oplossingen mogelijk.

a. Gebruik reguliere VPN

De eenvoudigste oplossing is dat je (eenmalig) gebruik maakt van de ***reguliere*** VPN-service die HvA aan haar gebruikers biedt via https://vpn.hva.nl.
Je gebruikt jouw reguliere HvA-ID + wachtwoord om in te loggen. Je gebruikt dezelfde PulseSecure VPN-client om verbinding te maken.

Nadat je de VPN-verbinding hebt gemaakt kun je inloggen op de beheer-ID zelfbediening. Als je jouw wachtwoord en eventueel token hebt ingesteld moet je deze VPN-verbinding verbreken voordat je probeert in te loggen op de beheer-VPN.

b. Maatwerk

Op verzoek kun je een YubiKey aanvragen, ook als de app voldoende is. Deze YubiKey kan naar een door jouw opgegeven postadres gestuurd worden. Je kunt dan met jouw beheer-ID, tijdelijke wachtwoord en YubiKey inloggen op de beheer-VPN. Uiteraard moet je dan direct inloggen op de beheer-ID zelfbediening om jouw wachtwoord in te stellen.

In overleg zijn ook andere oplossingen, via een betrouwbare tussenpersoon, mogelijk.