

Handleidingen 1.0

Beheerpaneel



Handleidingen 1.0 Beheerpaneel

In dit document vind je de handleidingen voor het Beheerpaneel van ECM2.

I. Handleiding ECM2 Beheerpaneel	1
1. Inleiding	3
2. Inloggen op het beheerpaneel	5
3. Functionaliteiten	7
3.1. Het Dashboard	7
3.1.1. Gegevens	8
3.1.2. CRM	9
3.1.3. Kopano	10
4. Wachtwoorden beheren	15
4.1. Wachtwoord resetten	15
4.2. Wachtwoord zelf aanpassen	15
4.2.1. Kies zelf een wachtwoord	15
4.2.2. Genereer zelf een wachtwoord	16
5. Extra beveiligingsopties	19
5.1. Twee-factor authenticatie inschakelen (beheerder)	19
5.1.1. Schakel twee-factor authenticatie in	19
5.1.2. Vereis twee-factor authenticatie	19
5.2. Ophalen van je persoonlijke tweede factor (gebruiker)	19
5.3. Hoe gaat inloggen als alles is ingesteld?	20
5.4. Wat is een 'trusted device'?	20
6. Groepen	23
6.1. Instellen van een groep	23
6.2. Kopano	24
6.2.1. Permissies op gedeelde Agenda's en mappen	24
6.3. Alfresco	28
6.3.1. Werken met permissies op groepsniveau	28
6.4. NLCloudopslag	28
6.4.1. Mappen delen met groepen	28
Register	31

Deel I. Handleiding ECM2 Beheerpaneel

Inleiding

Het beheerpaneel is bedoeld om onze klanten zoveel mogelijk zelf de kans te geven om gebruikers te beheren en gegevens aan te passen. Daarmee zijn wijzigingen 24/7 mogelijk en dus kan je wijzigingen zelf doorvoeren wanneer jij dat wilt.



Opmerking

Het beheerpaneel is in ontwikkeling en wordt uitgebreid. Momenteel kan je alleen gebruikers laten verwijderen of aanmaken via de helpdesk. Houd rekening mee dat zo'n verandering kosten met zich mee brengt.

Binnen het beheerpaneel kennen wij twee types gebruiker: '**beheerders**' en '**normale gebruikers**'. De beheerder kan alle accountgegevens van de organisatie beheren en een normale gebruiker alleen een deel van zijn / haar persoonlijke gegevens..

Standaard is alleen de persoon die de dienst(en) bij ECM2 heeft aangevraagd 'beheerder', maar die rol kan ook worden overgedragen aan één of meer andere gebruikers. Dat kan je als beheerder via het beheerpaneel zelf doen. Deze rol als 'beheerder' staat overigens los van wie bijvoorbeeld de beheerder is in de diensten / applicaties zelf. Een beheerder kan deze beheerder die functie ook bij normale gebruikers beleggen.

Inloggen op het beheerpaneel

Iedere gebruiker met een account kan inloggen op het beheerpaneel van ECM2. Je logt in met de gebruikelijke gegevens waarmee je ook op andere diensten van ECM2 inlogt.

Het adres van het Beheerpaneel is: <https://beheer.ecm2.nl>. Na het inloggen kom je terecht op het zogenaamde Dashboard.

Functionaliteiten

3.1. Het Dashboard

Direct na het inloggen, kom je terecht op het gebruikersdashboard. Dit geeft een overzicht van alle gebruikers en diensten binnen jouw organisatie. Op het Dashboard is er direct een verschil tussen de twee type gebruikers: *Beheerders* en *normale gebruikers*:

- Als je een **beheerder** bent van jouw organisatie, dan zie je hier alle gebruikers staan met hun naam, e-mailadres en tot welke diensten zij toegang hebben.
- Ben je een **normale gebruiker** dan zie je alleen jezelf staan. Je hebt dan ook geen toegang tot de tabs 'Groepen', 'Domeinen' en 'Bedrijven'.

The screenshot shows the ECM2 dashboard interface. At the top, there is a blue header with the ECM2 logo. Below the header, there are four tabs: 'Gebruikers' (highlighted with a red box), 'Groepen', 'Domeinen', and 'Bedrijven'. The 'Gebruikers' tab displays a table with the following data:

Naam	E-mail	Alfresco	CRM	Kopan
Henk Jansen	user2@testco1.nl	Aan	Aan	Aan
John Smith	user1@testco1.nl	Aan	Aan	Aan

At the bottom right of the table, there are navigation controls including a page number '1' and arrows for navigation.

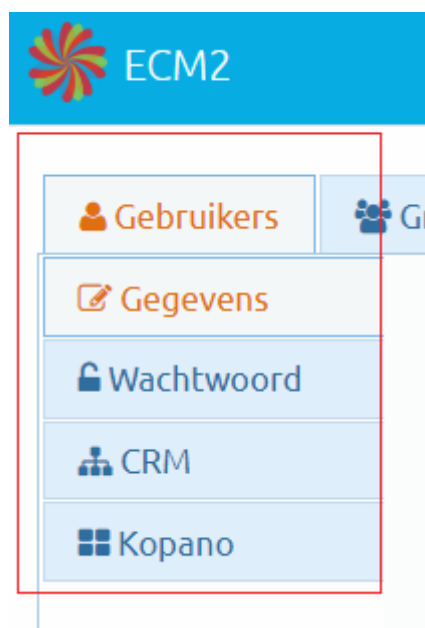
Naast de gebruikers staat een aantal rode en/of groene vierkanten. Staat in de kolom onder een dienst een groen vierkanten met de tekst "Aan", dan heeft die gebruiker toegang tot deze dienst. Bij een rood vierkanten met de tekst "Uit" heeft een gebruiker geen toegang tot deze dienst. Staat er een groen vierkant onder 'Beheeraccount', dan die de gegevens van alle gebruikers aanpassen. Staat er een rood voerkant, dan heeft die gebruiker een 'normaal' account en kan die alleen zichzelf aanpassen.

Opmerking

Let op dat **de vierkanten** die je hier ziet staan, alleen aangeven of iemand toegang heeft tot de betreffende diensten, niet welke rechten deze gebruiker heeft binnen die diensten. Die rechten bepaal je gewoonlijk binnen de dienst zelf.

Om de gegevens van een gebruiker te wijzigen, dubbelklik je op de naam van de gebruiker of klik je op de blauwe 'Bewerk' knop in de regel van de gebruiker. Je komt dan terecht op de 'Gegevenspagina' van deze gebruiker. Ook zie je dat in de linker balk één of meer opties verschijnen. In die linker kolom zie je altijd de tab 'Gegevens' staan, maar afhankelijk van de voor deze gebruiker

ingeschakelde diensten zijn er ook andere opties beschikbaar. Klik op een van deze opties om naar de instelling te gaan van z'n dienst.



3.1.1. Gegevens

De eerste optie van het submenu is 'Gegevens'. Je komt hier bij het bewerken van een gebruiker standaard als eerste op terecht. In dit menu staan de basisgegevens van de geselecteerde gebruiker. Je kunt de gegevens in de velden met een witte achtergrond aanpassen. Ben je een beheerder, dan kan je bij andere gebruikers de schakelaar voor "Beheeraccount" omzetten, waarmee je aangeeft dat die gebruiker ook andere gebruikers kan beheren.

Je kunt die schakelaar bij jezelf niet aanpassen, dat kan alleen een andere beheerder bij jou doen. Na het omzetten van een schakelaar of het wijzigen van de waarde in een veld, worden de wijzigingen automatisch opgeslagen en krijg je een pop-up te zien dat er een aanpassing heeft plaatsgevonden. Zijn er ongeldige gegevens ingevuld, dan krijg je daar een notificatie van met aanwijzingen en wordt de aanpassing niet doorgevoerd totdat je de gegevens verder juist aanpast. Hierna zie jij jouw aanpassing terug in het grafische overzicht.



Gebruikers	Groepen	Domeinen	Bedrijven
Gegevens		Beheerder in CRM	
Wachtwoord		Uit ▼	
CRM		Taal CRM	
Kopano		Nederlands ▼	

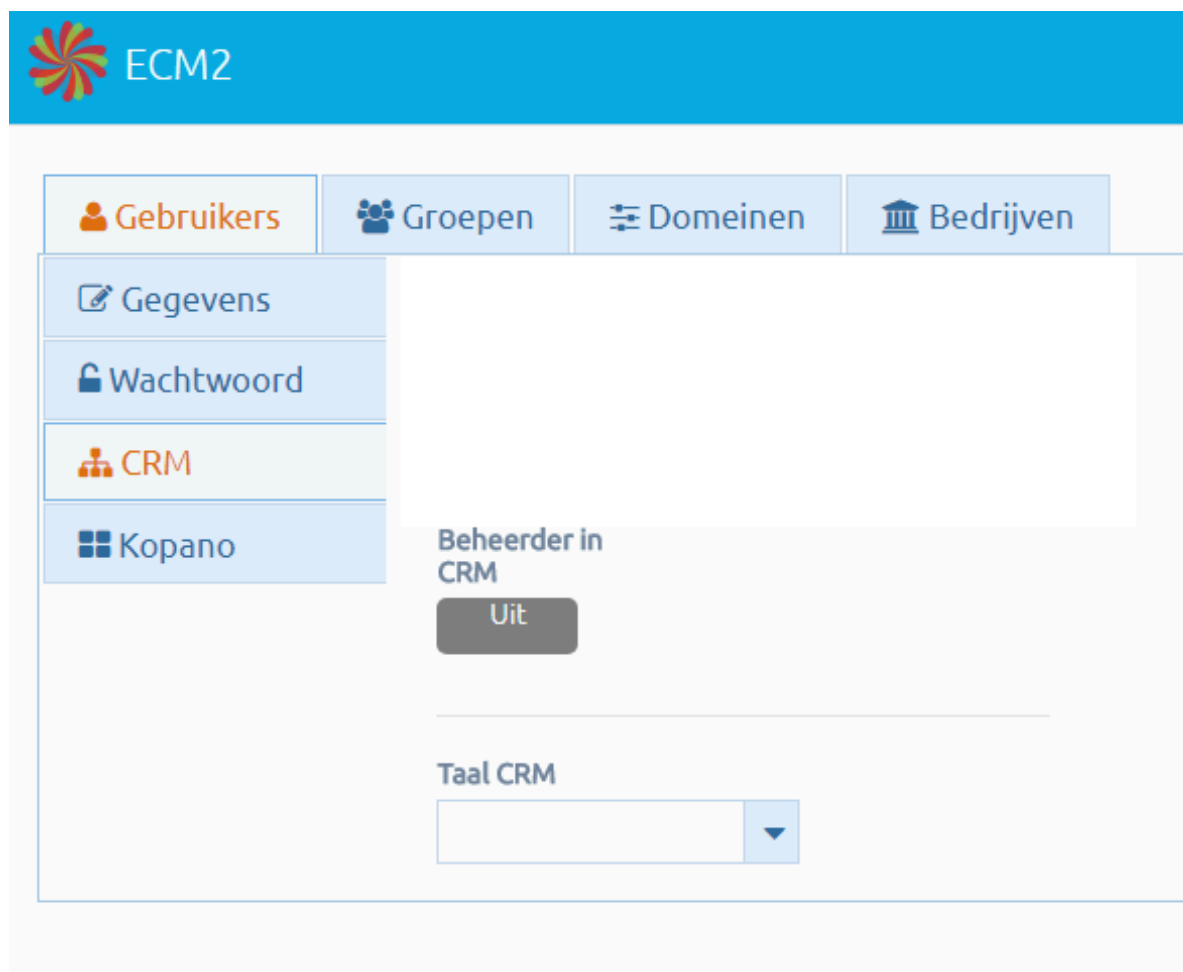
3.1.2. CRM

De optie 'CRM' geeft toegang tot de instellingen die specifiek en alleen voor de dienst 'CRM' gelden. Klik op deze optie en je komt op de pagina voor 'CRM'.

Hier kan je de volgende instellingen aanpassen voor jouw CRM:

- Je kunt een gebruiker **Beheerder** maken binnen dat CRM. Let op dat deze gebruiker dan altijd toegang heeft tot alle gegevens in het CRM en dat deze gebruiker ook aanpassingen kan doen binnen dat CRM.
- Bij '**Taal CRM**' pas je de gewenste taal aan waarin je het CRM wilt gebruiken. Wanneer je de volgende keer weer inlogt op SuiteCRM zal deze taal standaard ingesteld zijn. Is '*Geen voorkeur*' geselecteerd, dan wordt voor de gebruiker in het CRM een standaardtaal ingesteld die geldt voor dat CRM. In de meeste gevallen is dat Nederlands.

Wijzigingen worden automatisch opgeslagen na dat de gebruiker een aanpassing heeft gedaan.




The screenshot shows the ECM2 user interface. At the top, there is a blue header with the ECM2 logo and name. Below the header, there are four tabs: 'Gebruikers', 'Groepen', 'Domeinen', and 'Bedrijven'. The 'Gebruikers' tab is selected. On the left side, there is a vertical menu with four items: 'Gegevens', 'Wachtwoord', 'CRM', and 'Kopano'. The 'Kopano' item is selected. The main content area shows the 'Beheerder in CRM' section with a 'Uit' button. Below this is a 'Taal CRM' section with a dropdown menu.

3.1.3. Kopano

De optie '**Kopano**' geeft toegang tot de instellingen van de verschillende 'mailboxes' van het bedrijf als jij Kopano bij ECM2 afneemt. Hier kan je de volgende instellingen aanpassen voor jouw mailboxen:


- Je kunt iemand '**Beheerder**' maken door voor 'Aan' te kiezen bij de dropdown "Beheeraccount". Let op dat deze gebruiker toegang heeft tot alle mailboxen. Standaard staat deze op 'Nee'.
- Met '**Verberg gebruiker**' kan je voorkomen dat de geselecteerde gebruiker zichtbaar is in het gemeenschappelijke adresboek in Kopano. Standaard staat deze op 'Nee'.
- Met '**Gedeelde mailbox**' bepaal je of dit een mailbox betreft waarop je rechtstreeks mag inloggen. Als dat niet de bedoeling is (denk aan info@ of administratie@), dan zet je de optie '*Gedeelde mailbox*' aan en is deze alleen toe te voegen als extra mailbox aan jouw account in WebApp of Outlook, mits je voldoende rechten hebt op die mailbox. Standaard staat deze op 'Nee'.
- Wanneer je één of meer gebruikers aanvinkt bij '**Mag versturen namens deze gebruiker**' dan kunnen deze gebruikers e-mail versturen namens de geselecteerde gebruiker, dus met het bij e-mail getoonde adres als afzender.
- Bij '**Aliassen**' kan je meerdere e-mailadressen koppelen aan deze mailbox. Op al deze adressen kan deze gebruiker e-mail ontvangen. Selecteer de juiste domeinnaam en geef in het veld daarvoor een geldige waarde op voor het stuk voor het '@'-teken van het e-mailadres. Om de alias toe te voegen, druk op de groene knop '*Toevoegen*'. Wijzigingen worden na invoeren automatisch opgeslagen.

 ECM2

[Gebruikers](#) [Groepen](#) [Domeinen](#) [Bedrijven](#)

Naam ▾	Kopano ▾	Kopano server ▾
testco1.nl	<input type="button" value="Aan"/>	vpt009.ecm2.nl

◀ ◁ 1 ▷ ▶

 ECM2 testco1.

[Gebruikers](#) [Groepen](#) [Domeinen](#) [Bedrijven](#)

[Gegevens](#)

Kopano

Domeinnaam

Hoofdstuk 3. Functionaliteiten

- Als je een e-mailadres invult bij **Uitgaande e-mails altijd BCC-en naar dit e-mail adres**, wordt alle uitgaande mail van deze mailbox standaard ook naar het opgegeven adres gestuurd. De ontvanger ziet dit adres niet in de CC staan.



Opmerking

De domeinnamen waarop je e-mail kunt ontvangen dien je van tevoren bij ECM2 aan te geven. Heb je dat gedaan, dan vind je die terug in de lijst onder '*Domeinen*' en verschijnt de domeinnaam als optie verschijnt bij het aanmaken van een alias.



Gebruikers

Groepen

Domeinen

Bedrijven

Gegevens

Wachtwoord

CRM

Kopano

Beheerder

Aan ▼

Verberg gebruiker

Aan ▼

Gedeelde mailbox

Uit

E-mail adres

user1@testco1.nl

Uitgaande e-mails altijd BCC-en naar dit e-mail adres

user1BCC@example.com

Aliassen

E-mail

@

testco1.nl

Toevoegen

#	Aliassen ↕	
#1	s1@testco1.nl	Ver
#2	us1@testco1.nl	Ver
#3	u1@testco1.nl	Ver

⏪ ⏩ 1 ⏪ ⏩ 10 ▼

Wachtwoorden beheren

4.1. Wachtwoord resetten

Wanneer je jouw wachtwoord kwijt bent, dan is er een snelle manier om **zelf een nieuw wachtwoord te krijgen**. Ga naar de inlogpagina van het Beheerpaneel en klik op de tekst '**Wachtwoord vergeten?**'. Op de volgende pagina vul je in het e-mail veld het e-mailadres in dat aan jouw ECM2-account is gekoppeld. Op dat e-mailadres krijg je de informatie toegestuurd om een nieuw wachtwoord te krijgen.



Opmerking

Let op dat het wachtwoord pas wordt aangepast, nadat de stappen in de e-mail zijn doorlopen. Heb je ook geen toegang meer tot het e-mailadres dat bij ECM2 bekend is? Dan kan je aan jouw Beheerder vragen of deze inlogt op het Beheerpaneel.

Als beheerder ga je naar de betreffende gebruiker toe en kies je op de tab "*Wachtwoord*". Het beste is om dan opties "*Genereer een wachtwoord*" te kiezen en die automatisch te laten versturen. Heeft de ontvangende partij geen toegang meer tot de betreffende mailbox, vink dan eerst de checkbox "*Stuur de e-mail met het wachtwoord naar een ander e-mail adres*" aan. Vul een alternatief e-mailadres in in het veld "*E-mail adres*" en klik dan op de groene knop "*Genereer en stuur e-mail*". De nieuwe inloggegevens voor deze gebruiker gaan dan naar dat adres.

4.2. Wachtwoord zelf aanpassen

Wil je het wachtwoord veranderen van een gebruiker? Ga dan naar de tab '*Gegevens*' van de gebruiker en klik links op de tab '*Wachtwoord*'. Je kan op twee manieren het wachtwoord wijzigen via het Beheerpaneel: Kies zelf een wachtwoord of laat een wachtwoord genereren.



Opmerking

1. Let op dat wanneer je het wachtwoord wijzigt, dat nieuwe wachtwoord direct actief is voor alle ECM2-diensten van jouw account. Dat kan betekenen dat je op verschillende plekken gevraagd wordt het het wachtwoord opnieuw in te voeren.
2. Denk bijvoorbeeld aan de mobiele Apps en aan Outlook of andere e-mail clients op jouw apparatuur.
3. Bij bepaalde applicaties kan het wat langer duren voordat je de melding krijgt: je hebt dan nog een geldige sessie, waardoor je niet direct nogmaals hoeft in te loggen.

4.2.1. Kies zelf een wachtwoord

Wanneer je zelf een sterk wachtwoord hebt kies je voor de optie "*Kies zelf een wachtwoord*". Voer tweemaal dat wachtwoord in de twee wachtwoordvelden. Als het wachtwoord voldoende sterk is en je

hebt tweemaal hetzelfde ingegeven, dan klik je op 'Wijzig' om dit wachtwoord actief te maken. Is dat niet het geval, dan krijg je een melding om opnieuw een sterk wachtwoord in te voeren.

The screenshot shows the ECM2 user management interface. At the top, there is a blue header with the ECM2 logo. Below the header, there are four tabs: 'Gebruikers', 'Groepen', 'Domeinen', and 'Bedrijven'. The 'Gebruikers' tab is selected. On the left side, there is a vertical menu with options: 'Gegevens', 'Wachtwoord', 'CRM', and 'Kopano'. The 'Wachtwoord' option is highlighted. The main content area shows the password change form for a user with the email address 'user1@testco1.nl'. The form includes a text input field for the current password, a 'Kies zelf een wachtwoord' section with a 'Generereer een wachtwoord' button, and two required password fields: 'Nieuw wachtwoord *' and 'Herhaal wachtwoord *'. At the bottom right, there are two buttons: 'wijzig' (highlighted) and 'An'.

4.2.2. Genereer zelf een wachtwoord

Je kunt ook een wachtwoord laten genereren. Wanneer je op de 'Wachtwoord' pagina staat, kies dan voor de tab 'Generereer wachtwoord'. Kies dan of je dit nieuwe wachtwoord naar het e-mailadres laat mailen dat hoort bij de gebruiker, of dat je kiest voor een willekeurig ander e-mailadres. Je doet dat met de schuif bij "Stuur de e-mail met het wachtwoord naar een ander e-mail adres?". Klik daarna op 'Generereer en stuur wachtwoord'. Er wordt een nieuw wachtwoord opgestuurd via de e-mail. Let op dat dit wachtwoord direct actief is voor deze gebruiker en het oude wachtwoord dus niet meer functioneert.



Gebruikers	Groepen	Domeinen	Bedrijven
-------------------	----------------	-----------------	------------------

Gegevens	E-mail adres
Wachtwoord	user1@testco1.nl
CRM	<div style="border: 1px solid red; padding: 5px;"> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid gray; padding: 5px;">Kies zelf een wachtwoord</div> <div style="border: 1px solid gray; padding: 5px;">Genereer een wachtwoord</div> </div> <p>Laat een wachtwoord genereren en mail deze naar het adres van de gebruiker. Stuur de e-mail met het wachtwoord naar een ander e-mail adres.</p> <p>E-mail adres *</p> <div style="border: 1px solid gray; padding: 5px;"> Alternatief e-mail adres</div> </div>
Kopano	

Genereer en stuur e-mail

Annuleer

Extra beveiligingsopties

5.1. Twee-factor authenticatie inschakelen (beheerder)

Twee-factor authenticatie (ook wel afgekort als 2fa), biedt een extra veiligheidslaag aan voor iedereen. Op het terrein van twee-factor authenticatie bieden wij drie niveaus aan. De beheerders kan als enige binnen de omgeving bepalen óf en op welke manier twee-factor authenticatie wordt toegepast. In het beheerportaal onder **tab Bedrijven** kan je als beheerder kiezen voor "Schakel twee-factor authenticatie in" of "Vereis twee-factor authenticatie".



Opmerking

Let op: het is aan te raden om van te voren te zorgen voor goede communicatie met de gebruiker door af te spreken hoe en wanneer deze functie in gebruik genomen gaat worden. Spreek bijvoorbeeld af dat twee-factor authenticatie een eerste periode alleen wordt inschakeld, zodat de gebruikers het daarna voor zichzelf kunnen instellen. Na deze periode kan de beheerder het gebruik ervan verplicht stellen.

5.1.1. Schakel twee-factor authenticatie in

Bij optie "Schakel twee-factor authenticatie in" is het gebruik van twee-factor authenticatie vrijblijvend. Staat deze aan? Dan kan een gebruiker, wanneer twee-factor authenticatie gewenst is, deze alleen voor zichzelf inschakelen in het beheerportaal bij zijn eigen account. Deze gebruiker is daarna verplicht om de tweede factor in te voeren bij het inloggen.

5.1.2. Vereis twee-factor authenticatie

Wil je afdwingen dat iedereen verplicht een tweede factor instelt, dan kan dat met de optie "Vereis twee-factor authenticatie". Als deze "Aan" staat moet iedereen gebruik maken van twee-factor authenticatie. Gebruikers moeten deze twee-factor authenticatie wel zelf nog persoonlijk inschakelen bij hun eigen account in het beheerportaal. Hierna is deze functionaliteit operationeel en kan iedereen alleen op deze manier inloggen. Heeft een gebruiker de tweede factor niet ingesteld, dan kan die niet inloggen op de applicatie(s).

Wanneer is het verstandig om voor verplicht te kiezen? Als je veel met gevoelige informatie werkt en/of on niet-persoonsgebonden apparatuur werkt, kan het een aanrader zijn om het verplicht te stellen en technisch af te dwingen dat gebruikers werken met twee-factor authenticatie. Ook is het gebruik van een tweede factor noodzakelijk als je als organisatie aan bepaalde standaarden moet voldoen, bijvoorbeeld bij NEN 7510.

5.2. Ophalen van je persoonlijke tweede factor (gebruiker)

Wat moet je doen om dit in te stellen? Eerst moet je een "tweede factor app" installeren op de mobiele telefoon. Deze moet "TOTP" ondersteunen (daar kan je in de app winkels op zoeken). Wij raden de volgende Apps aan: "andOTP" voor Android en "Authenticator" voor iOS, uiteraard zijn er ook ander app aanwezig maar kijk goed of je een betrouwbare gaat gebruiken. Als je deze hebt geïnstalleerd ben je klaar voor onderstaande stappen.

1. Log in op beheer.ecm2.nl.
2. Dubbelklik op je eigen naam.

3. Ga naar de sub-tab "Wachtwoorden".
4. Zet de optie met de naam "Schakel twee-factor authenticatie in" op "Aan".
5. Je krijgt dan een pop-up met een specifieke melding. Lees dit bericht en volg de aanwijzingen op wanneer je nog niet een tweede factor app had geïnstalleerd.
6. Klik op "Bevestig".
7. Er wordt een code in de vorm van een Quick Respons of QR-code gegenereerd. Dat is een code in de vorm van een specifieke grafische afbeelding die informatie bevat.
8. Pak nu jouw mobiele telefoon en open jouw tweede factor app en klik op de knop om de QR-code te scannen, bij tweede factor app "andOTP" is dat de knop QR-code scannen.
9. Houd de camera recht voor de QR-code. Het programma zal bij een scherp beeld meteen de QR-code scannen en slaat deze apart op. Deze code is alleen geschikt om in te loggen op de ECM2-omgeving.
10. Het is handig om dit bestand een onderscheidende naam te geven via de bewerk knop rechts van deze code.
11. Klik op etiket bewerken om jouw specifieke naam toe te voegen voor snel herkennen.

5.3. Hoe gaat inloggen als alles is ingesteld?

1. Log zoals normaal gesproken via login.ecm2.nl in op jouw account.
2. Hierna krijg je het centrale overzicht met alle app's.
3. Klik op jouw actieve app (kleur blauw) om deze te openen.
4. Nu opent een aparte "Second factor required" pagina. Daarop dien je jouw zescijferige code in te voeren.
5. Pak je telefoon erbij met in jouw "tweede factor app" de juiste record voor onze omgeving. Je hebt maximaal 30 seconden de tijd om deze in dat veld in te voeren. Daarna wordt er weer een nieuwe code gegenereerd en dien je die in te vullen.
6. Klik na invoeren op de bevestig knop en je gaat hierna meteen naar jouw applicatie bij ECM2.
7. Je hebt nu gebruik gemaakt van Twee-factor authenticatie

Vergeet dus niet om altijd jouw mobiele telefoon bij je te hebben om in te loggen. Wat te doen als je jouw code kwijt bent, bijvoorbeeld doordat jouw telefoon kapot is, of je de App hebt verwijderd? Log zelf in op beheer.ecm2.nl en ga dan naar sub-tab "Wachtwoorden". Schakel hier deze functionaliteit eerst uit en dan weer in. Na inschakelen zal het systeem een nieuwe QR-code aanmaken en tonen. Scan deze nieuwe code in en je hebt weer de mogelijkheid om gebruikt te maken van Twee-factor authenticatie bij ECM2.

5.4. Wat is een 'trusted device'?

Dit is de applicatie op een computer, tablet of smartphone waarvan jij of jouw organisatie vindt dat je die kunt vertrouwen.

- De "**applicatie**" in deze zin refereert dan vaak aan de browser op een PC die je gebruikt om mee in te loggen, of de Nextcloud applicatie op een tablet of smartphone. Elke van deze applicaties krijgt tijdens het inloggen een specifiek kenmerk, waarmee die geïdentificeerd kan worden. Als je

op een PC meerdere browsers gebruikt betreft dat allemaal aparte applicaties die je wel/niet kunt vertrouwen.

- Zo'n applicatie die je **vertrouwt** betreft vaak alleen jouw eigen PC/Mac of die op kantoor en natuurlijk de apparatuur die je altijd bij je hebt, zoals een tablet of smartphone..

Omdat je na inloggen met je ECM2-account direct alle applicaties kunt openen, biedt het verplicht invullen van de code bij het openen van een nieuwe applicatie extra veiligheid. Dat is de standaardinstelling. Als je de checkbox "Trusted Device" leeg laat, moet je dus elke keer bij het openen van een applicatie via login.ecm2.nl jouw Tweede Factor code opnieuw invoeren. Heb je de applicatie al een keer geopend, wel afgesloten, maar je browser actief gehouden, dan is de code voor die applicatie nog onthouden.

Vink je tijdens het inloggen de checkbox "Trusted Device" wel aan, dan hoeft je slechts eenmaal deze Tweede Factor code in te voeren en kan je daarna de andere applicaties openen zonder nogmaals een code te hoeven invoeren. Dit vergroot het gebruiksgemak, maar verlaagt de beveiliging iets enigszins. Doe dit daarom alleen op een computer of apparaat dat jij vertrouwt, vandaar ook de naam "Trusted Device".

Groepen

6.1. Instellen van een groep

Je hebt een van de volgende diensten bij ons afgenomen, Alfresco, Kopano of NLCloudOpslag en je wilt daarna goed gaan regelen wie wat mag doen en zien binnen deze software. Dat kan bereikt worden door voor individuele gebruikers rechten in te stellen of door zo'n gebruiker onder een groep te plaatsen en voor deze groep alles te regelen voor jouw omgeving.

Wat is een groep? Een groep is verzameling van een zelfde type gebruiker met overeenkomende rechten. Dit is een manier om meerdere gebruikers te bundelen onder een naam en aan deze groep kermerken toe te wijzen. Als zo een kenmerkt overeenkomst met een kenmerk bij een map of Site dan kan zo groep deze pas zien en mogelijk er iets mee doen. Wat zijn rechten? Met een recht wordt bedoelt met iets wat je mag binnen een omgeving. Dus mag je iets zien, kan je iets bewerken of verwijderen. Je gebruik deze onder meer voor **autorisatiedoelinden** of om **e-mails naar meerdere personen** te kunnen sturen.

Het apart per gebruiker instellen kost veel tijd en het werken met groepen vereenvoudigt en versnelt dat instelproces. Je stelt groepen in via het Beheerportaal. Dat is bereikbaar via "**beheer.ecm2.nl**". Elke gebruiker uit onze omgeving kan daarop inloggen met zijn inloggegevens. Beheerders mogen groepen aanmaken en instellen, standaard gebruikers kunnen dat niet. Wanneer het Beheerportaal is geopend, klik dan op de subtab "*Groepen*". Hier zie je een lijst staan met al aangemaakt groepen.

Hoe maak je een groep aan? De generieke instructies vind je hier direct onder; specifieke instellingen in de paragrafen daarna.

1. Klik op de tab "*Groepen*" om een nieuwe groep toe te voegen of bestaande te wijzigen
2. Via "*Toevoegen*" kan jezelf een nieuwe aanmaken
3. Voer eerst een naam in voor deze groep
4. Voeg via "*Lid van deze groep*" de gebruikers toe die onder deze dienst moeten gaan vallen.
5. Je kan geen groepen aanmaken zonder lid.
6. Kies hierna welke dienst gekoppeld moet worden aan deze groep.

Binnen deze diensten kan een groep gebruikt worden voor specifieke functionaliteit. Denk hierbij aan **het delen van een agenda in Kopano** of **het delen van mappen in NLCloudOpslag** met collega's van specifieke afdelingen.

Naam	E-mail	Alfresco
testco1.nl	em1@testco1.nl	Aan

6.2. Kopano

6.2.1. Permissies op gedeelde Agenda's en mappen

Om snel groepen van medewerkers toegang te geven tot gedeelde mappen en agenda's, is het aan te raden om te gaan werken met autorisatiegroepen. Je geeft zo'n groep permissies op een gedeelde agenda of map, waarna direct alle leden van die groep over die permissies beschikken. Dat scheelt een hoop werk bij het beheren van toegang.

Aanmaken van de groep en permissies toewijzen;

1. Maak in Kopano een groep aan en geef die een goede naam, bijvoorbeeld "Secretariaat" en koppel daar dan alle secretaresse's aan.
2. Zet de knop "Autorisatiegroep" aan.
3. Ga naar de Kopano WebApp of DeskApp.
4. Open de gedeelde Agenda en klik daar met de rechtermuisknop op en selecteer "Eigenschappen".
5. In de pop-up klik op "Machtigingen" en dan op "Voeg Toe".
6. Selecteer uit het "Adresboek" de juiste Groep.
7. Bepaal bij "Profiel" wat de leden van deze groep mogen doen met deze agenda.
8. Sla de wijzigingen op.
9. Vanaf nu kunnen de medewerkers uit deze groep deze gedeelde agenda toevoegen aan hun eigen account.

6.2.1.1. Mailgroep

Om ervoor te zorgen dat je één mail kunt sturen aan meerdere gebruikers, maak je een mailgroep aan.

Aanmaken van deze mailgroep;

1. Klik op de knop "Toevoegen", geef een passende naam op en vink alle gebruikers aan die onder deze nieuwe groep moeten vallen.
2. Klik op de knop "Kopano" en zet deze "Aan".
3. Klik dan op de "subtab Kopano" onder "Groepen" en voeg een e-mailadres toe voor deze groep.
4. Als je wilt kan je hierna ook "Aliassen" toevoegen voor dit e-mailadres.
5. Je kan een "Groep" ook verbergen, wat wil zeggen dat deze niet zichtbaar is in het adresboek van Kopano.

Na het aanmaken van deze groep krijgen alle gebruikers die onder deze groep horen een e-mail als je naar het adres van de mailgroep een e-mail verstuurt.

6.2.1.2. Behouden van afzender voor een e-mail alias

Wanneer je werkt met e-mail aliassen kan je zijn opgevallen dat bij alle e-mails in jouw inbox nooit jouw specifieke alias staat vermeld. Standaard worden de aliassen namelijk 'herschreven' naar het primaire adres. Als je het alias-adres graag wilt behouden, dan kan je een mailgroep (zie paragraaf hiervoor) gebruiken, met maar een lid: jij zelf.

Instelling voor Behoud van afzender;

1. Verwijder de alias bij jouw gebruiker: je kunt een e-mail adres maar één keer gebruiken en we gaan die aan de groep toewijzen.
2. Klik bij Groepen op de knop "Toevoegen", geef een passende naam op en vink alleen jezelf aan.
3. Klik op de knop "Kopano" en zet deze "Aan".
4. Klik dan op de "subtab Kopano" onder "Groepen" en voeg de alias toe voor deze groep.

Wil je ook nog kunnen versturen namens die alias? Dan dien je jezelf die permissies te geven.

Hoe verstuur ik namens een groep;

1. Vink jezelf aan bij de Groep onder **namens de groep versturen**.
2. Ga naar de Kopano WebApp, en maak een nieuwe e-mail aan.
3. Controleer in dat scherm of onder de groene verzend-knop het veld "**Afzender**" actief is.
4. Als dat niet zo is doe het volgende, klik op het icoon "**Toon afzender**" (persoon in poszegel) in de menubalk om dat veld zichtbaar te maken.
5. Klik dan op de knop "**Afzender**" om pop-up "**Adresboek**" zichtbaar te maken.
6. Selecteer hieruit *jouw groep*.
7. Nu is de afzender *jouw groep* en zal de ontvanger dat ook gaan zien.

ECM2 testco1.nl

Gebruikers | **Groepen** | Domeinen | Bedrijven

Gegevens | Kopano


Alfresco	Kopano	NLCloudOpslag
Aan	Aan	Aan





Groepsnaam


testco1.nl


Lid van deze groep

- John Smith
- Henk Jansen

 ECM2
testco1.n

 Gebruikers
 Groepen
 Domeinen
 Bedrijven


 Gegevens

 Kopano


Verberg groep
Autorisatiegroep

Uit
Aan

Groepsnaam


 testco1.nl

E-mail adres

 em1@testco1.nl

Wijzigen

Aliassen

 E-mail


@ testco1.nl

▼

Toevoegen

#	Aliases	
#1	elm@testco1.nl	Verwijder
#2	asd@testco1.nl	Verwijder

⏪ ⏩ 1 ⏪ ⏩ 10 ▼

 **Opmerking**

Let op dat er een vertraging kan zitten bij het inschakelen van deze optie: bepaalde gegevens synchroniseren periodiek van de centrale authenticatie naar Alfresco.

6.3. Alfresco

6.3.1. Werken met permissies op groepsniveau

Je wilt werken met permissies binnen Alfresco, omdat niet iedere gebruiker alles mag doen en zien. Je wilt een Site maken voor de financiële afdeling waar alleen medewerkers toegang tot mogen krijgen die bij deze afdeling horen. Andere medewerkers hebben er niets te zoeken.

Dat kan goed bij Alfresco, maar houd rekening met het volgende;

- Door het instellen van specifieke rollen binnen Alfresco met wat gebruikers en leden van groepen wel en niet mogen doen reguleert men toegang tot bepaalde Sites en de daarbij horende inhoud.
- Een gebruiker of groep kan in elke Site een andere rol en dus andere rechten hebben.
- Het is handig om met groepen te werken omdat je hierdoor snel meerdere gebruikers onder kan hangen en zo een groep snel koppelt aan een specifieke rol bij een Site.

Zo maak je jouw Site toegankelijk voor een groep;

1. Maak in het Beheerpaneel een groep aan via de knop **Toevoegen** onder de tab "Groepen".
2. Geef deze een passende naam en vink alle gebruikers aan die hier onder moeten vallen.
3. Zet onder Gegevens de knop **Alfresco** op "Aan" om deze "Groep" te gaan gebruiken voor jouw Alfresco.
4. Als je deze groep hebt aangemaakt wordt deze *gesynchroniseerd* met de leden naar Alfresco.
5. Deze groep wordt gebruikt voor **autorisatiedoelinden** binnen Alfresco.
6. Zorg in Alfresco dat je Site manager bent, zodat je de permissies van een Site kunt aanpassen.
7. Klik op **Uitnodigen voor Site** in het Site Members gedeelte, dan op **Groepen**, dan op **Toevoegen Groepen**.
8. Via **Search** kan je jouw groep op naam zoeken. Voer minimaal één karakter in om op te Zoeken.
9. Klik op **Toevoegen** om een nieuwe groep toe te voegen.
10. Stel **de Site rol** in voor deze groep.
11. Klik op **Toevoegen Groepen** om de weergegeven Groepen te selecteren

Hierna kan iedereen die lid is van die groep de Site gebruiken met de ingestelde permissies.

6.4. NLCloudopslag

6.4.1. Mappen delen met groepen

Omdat je met een aantal personen in NLCloudOpslag werkt, wil je gaan werken met groepen. Dat maakt het beheer van gedeelde mappen een stuk eenvoudiger en sneller.

Houd rekening met het volgende;

- Door het instellen van specifieke rollen bij NLCloudOpslag met wat gebruikers en leden van groepen wel en niet mogen doen reguleer je de toegang tot bepaalde mappen en de daaronder vallende inhoud.
- Dus per map en wat er onder valt koppelt je een groep, waaraan je de permissies toewijst.
- Een gebruiker of groep kan bij elke map andere rechten hebben.

Zo stel jij dat in bij NLCloudopslag

1. In het Beheerportaal maak je een een "Groep" aan. Geef deze een passende naam en vink alle gebruikers aan die hier onder moeten vallen.
2. Zet onder "Gegevens" de knop "NLCloudopslag" op "Aan" om deze groep bruikbaar te maken voor NLCloudopslag.
3. Open "NLCloudopslag" in de browser.
4. Ga naar *de map* die je wilt delen en klik aan de rechterkant van het scherm op de *drie zwarte horizontale puntjes*.
5. klik in de pop-up op *Details* en kies rechts in het scherm op *Delen*.
6. Type onder delen in *het zoekveld* de naam van jouw groep en klik op de naam voor toevoegen.
7. Stel via "**Kan bewerken**" en **rechts de drie zwarte bolletjes** in wat de groep mag doen.

Je hebt nu deze groep permissies gegeven op deze map alleen en alles daaronder. Je kunt deze permissies altijd aanpassen.

Register

