

Identity Governance Rubicon RCMC

Last updated by | Fausto Koeman | Oct 26, 2023 at 11:03 AM GMT+2

Hieronder wordt beschreven hoe de technische inrichting in de Azure tenant van de klant dient te worden uitgevoerd. Hiermee kunnen RCMC en Consulant medewerkers beveiligd toegang krijgen tot een klantomgeving en hier werkzaamheden voor uitvoeren.

Benodigde rechten: Global Administrator

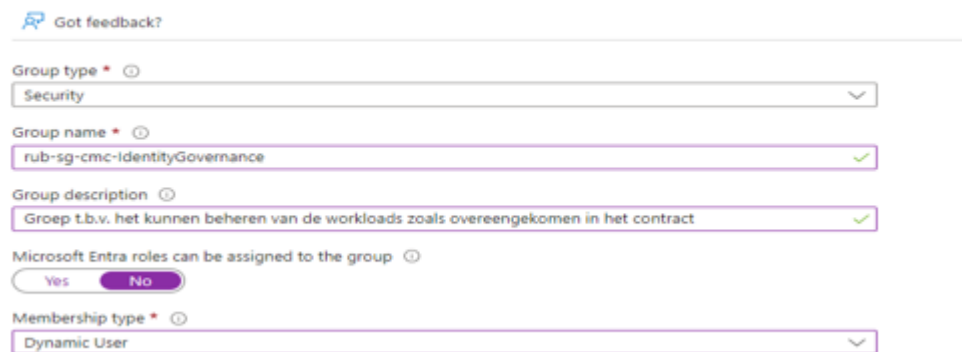
Guest toegang: Moet ingeschakeld staan

Vorbereiding Azure AD Groep

1. Maak de volgende dynamische groep aan in de Azure AD van de klant:

- **Naam:** Rub-sg-cmc-IdentityGovernance
- **Type Groep:** Dynamisch
- **Beschrijving:** Groep t.b.v. het kunnen beheren van de workloads zoals overeengekomen in het contract

New Group



Got feedback?

Group type * ⓘ
Security

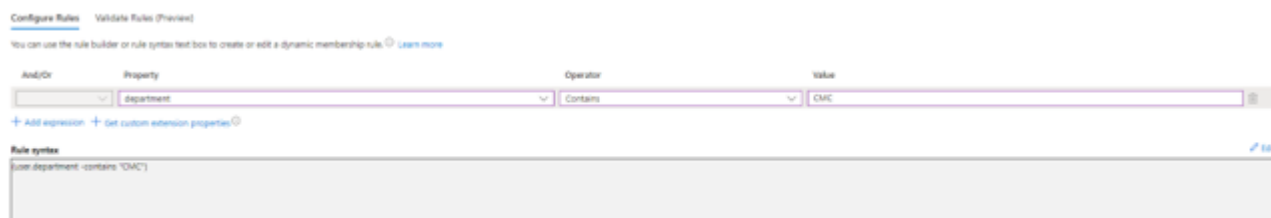
Group name * ⓘ
rub-sg-cmc-IdentityGovernance

Group description ⓘ
Groep t.b.v. het kunnen beheren van de workloads zoals overeengekomen in het contract

Microsoft Entra roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Dynamic User

2. Creëer een dynamic query met de volgende **settings:** (user.department -contains "RCMC")
Deze (**Department** = RCMC) dient ingevuld te worden wanneer een guest invite wordt uitgevoerd.
Hiermee kan er eenvoudig worden gerapporteerd. Klik hierna op create



Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

| And/Or | Property | Operator | Value |
|--------|------------|----------|-------|
| | department | Contains | CMC |

+ Add expression + Get custom extension properties ⓘ






Rule syntax ⓘ

(user.department -contains 'CMC')

Identity Governance Inrichting

1. Ga naar : https://portal.azure.com/#view/Microsoft_AAD_ERM/DashboardBlade/~-/Dashboard
2. Klik aan de linkerkant op Acces review -> Acces review

Access reviews

-  Overview
-  Access reviews
-  Programs
-  Settings
-  Review History

Privileged Identity Management

3. Klik linksboven op + New Access review en stel onder review type de volgende instellingen in: Selecteer hier de groep: **Rub-sg-cmc-IdentityGovernance**

New access review

Review type * Reviews Settings * Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
[Learn more](#)

Select what to review *

Teams + Groups

Review scope *

- ☐ All Microsoft 365 groups with guest users ⓘ
- ☒ Select Teams + groups

Group *

rub-sg-cmc-IdentityGovernance

Scope *

- ☒ Guest users only
- ☐ All users ⓘ

 In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ ☐

Next: Reviews

4. Stel het volgende in en klik daarna op Next

5. Bepaal nu zoals afgesproken met klant het review termijn en wie het moet reviewen (klant of RCMC kernteam)

New access review ...


* Review type

* Reviews

Settings

* Review + Create


Determine review stages, reviewers, and timeline below.

Multi-stage review * 

☐

Specify reviewers

Select reviewers *

 Identities who cannot review their own access. Click here to learn more.

Users review their own access

Group owner(s)

Selected user(s) or group(s)

Users review their own access

Managers of users


Specify recurrence of review

Duration (in days) *

3

Review recurrence *

Start date *

10/05/2023 

6. Bepaal de acties zoals overeengekomen met de klant en naar wie het eindrapport moet worden gestuurd

[* Review type](#) [* Reviews](#) [Settings](#) [* Review + Create](#)

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource ⓘ



If reviewers don't respond ⓘ

Take recommendations



Setting 'If reviewers don't respond' to 'Remove access' or 'Take recommendations' while 'Auto-apply results to resource' is enabled could potentially lead to all access to this resource being revoked if the reviewers fail to respond.

Action to apply on denied guest users ⓘ

Block user from signing-in for 30 ...



At end of review, send notification to

+ Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days ⓘ



User-to-Group Affiliation ⓘ



Advanced settings

Justification required ⓘ



Email notifications ⓘ



Reminders ⓘ



Additional content for reviewer email ⓘ

7. Op het eind zie je een samenvatting van de instellingen, sla deze op en deel het met de klant.

8. Sla de Review op en geef het een duidelijke omschrijving mee

Wanneer je al een Guest policy hebt, kun je onderscheid maken door de volgende regel toe te voegen aan je huidige acces review policy.

(user.userType -eq "Guest") and (user.department -ne "RCMC")

Conditional Acces policy inrichten + Terms Of use

1. ga naar:

https://portal.azure.com/feature.msals=true#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/_/TermsOfUse

2. klik op **(+ New terms)** om een nieuwe terms of use aan te maken

settings

- Name
- Rubicon B.V. Guest Terms of Use (**klantnaam**)
- Require users to expand the terms of use
- On
- Require users to consent on every device
- Off
- Expire consents
- Off
- Expire starting on
- -
- Frequency
- -
- Duration before re-acceptance required (days)
- 90
- Users accepted
- 1
- Users declined
- 0

3. Sla deze op en koppel deze aan een conditional acces policy voor de desbetreffende groep:

Rub-sg-cmc-IdentityGovernance

4. instellingen

GRANT - Terms of Use for Guests ...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *

Assignments

Users
Specific users included

Target resources
All cloud apps

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☒ Guest or external users

6 selected

☒ B2B collaboration guest users

☒ B2B collaboration member users

☒ B2B direct connect users

☒ Local guest users

☒ Service provider users

☒ Other external users

GRANT - Terms of Use for Guests ...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Name *

Assignments

Users
Specific users included

Target resources
All cloud apps

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Select what this policy applies to

Include Exclude

☐ None

☒ All cloud apps

☐ Select apps

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. [Learn more](#)

Control access enforcement to block or grant access. [Learn more](#)

- ☐ Block access
- ☒ Grant access

- ☐ Require multifactor authentication ⓘ
- ☐ Require authentication strength ⓘ
- ☐ Require device to be marked as compliant ⓘ
- ☐ Require Microsoft Entra hybrid joined device ⓘ
- ☐ Require approved client app ⓘ
[See list of approved client apps](#)
- ☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)
- ☐ Require password change ⓘ
- ☒ Rubicon B.V. Guest Terms of Use
- ☐ Rubicon B.V. Internal Terms of Use

For multiple controls

- ☐ Require all the selected controls
- ☒ Require one of the selected controls

Inrichting proces

1. RCMC krijgt akkoord van de klant om de de inrichting te mogen uitvoeren
2. RCMC kernteam wordt gemachtigd om de accounts aan te maken in de klantomgeving
3. RCMC zorgt dat de aangemaakt security groep is voorzien van PIM zodat dit binnen de gemaakte afspraken blijft
4. Manager RCMC bespreek met de manager van professional services de backlog log en schat in welke medewerkers de werkzaamheden op basis van hun expertise kunnen uitvoeren
5. De desbetreffende medewerkers krijgen een uitnodiging om de documentatie van de klant door te nemen en in te schatten of zij de werkzaamheden kunnen uitvoeren
6. Op basis van een Go/No Go krijgt de destreffende medewerker een Guest uitnodiging in de omgeving van de klant.
7. Hierna kan de medewerker starten met het uitvoeren van de werkzaamheden, deze werkt altijd onder de vlag van een RCMC Coördinator.
8. Wanneer de werkzaamheden zijn voltooid kan het account worden gesloten of automatisch worden opgeruimd via het Acces review procedure

e-mail:

Betreft: Nieuwe service van Rubicon

Beste [Naam],

Ik hoop dat dit bericht je in goede gezondheid bereikt. Graag deel ik een nieuwe ontwikkeling binnen

Rubicon met je, met als doel onze dienstverlening nog beter te laten aansluiten op jouw behoeften.

Naast onze vertrouwde IT service management, bieden wij bij Rubicon ook uitgebreide Professional services aan. We zijn altijd op zoek naar manieren om de doorloopsnelheid van klantverzoeken te optimaliseren. Daarom introduceren wij een nieuw initiatief waar ik graag meer over vertel.

Wat houdt het in? Onze toegewijde professionals binnen RCMC hebben nu de mogelijkheid om op een slimme en flexibele wijze hun kennis en vaardigheden in te zetten daar waar het jou het meeste helpt. Hierbij wordt het kennisniveau gewaarborgd en vindt altijd een grondige eindcontrole plaats door het RCMC team.

Ik ben ervan overtuigd dat dit voor jou de volgende voordelen met zich meebrengt:

- Aanzienlijk verkorte doorlooptijd van meldingen
- Verhoogde capaciteit tijdens piekmomenten en bij complexe verzoeken
- Toegang tot een pool van 250 MS professionals
- Onveranderde kwaliteitscontroles door jou bekende RCMC-medewerkers
- De vertrouwde korte communicatielijnen met je huidige contactpersonen

Wat betreft de kosten voor deze aanvullende service, vragen we slechts een bescheiden bedrag van EUR 6,60 per maand voor een Microsoft Entra ID Governance licentie. Voor meer informatie over deze licentie kun je een kijkje nemen op: [\[Link\]](#)

Het is belangrijk om te benadrukken dat er, buiten dit geringe bedrag, geen financiële veranderingen plaatsvinden in onze samenwerking.

Hieronder een beknopt overzicht van de stappen:

- Je geeft aan gebruik te willen maken van deze nieuwe dienst en ontvangt een aangepast contract.
- Als onderdeel van dit contract machtigt je RCMC om hun collega's bij Rubicon uit te nodigen.
- Na beoordeling deel je je akkoord met ons, inclusief de vereiste machtiging.
- Rubicon stelt een dynamische security group op, inclusief PIM voor de RCMC-accounts.
- Vervolgens zetten we een toegangsbeoordelingsprocedure op waarmee accounts binnen de beveiligingsgroep automatisch kunnen worden beheerd.
- Al onze accounts binnen de security group gaan akkoord met de gecombineerde gebruiksvoorwaarden van zowel Rubicon als jouw organisatie.
- Indien een account langer dan 7 dagen inactief is, wordt het automatisch uit de beveiligingsgroep verwijderd.
- Als uitbreiding op de bestaande Healthcheck ontvang je een activiteiten van de leden in de security group.

Ik ben natuurlijk beschikbaar om al je vragen te beantwoorden en verdere toelichting te geven over deze nieuwe dienst. Mag ik je daarom uitnodigen voor een kort gesprek?