

Notice explicative: processus d'attribution de rôle dans le système IAM pour utilisateurs avancés (Power-User) et application

Table des matières

Introduction	2
1 Condition préalable	2
2 Processus d'enregistrement	2
3 Attribution de rôle pour un nouvel utilisateur	2
4 Description des rôles	7
4.1 Rôles pour le Registre central des conventions «RCCo»	8
4.2 Rôles pour le registre des codes-créanciers «RCC»	8
5 Information à l'utilisateur	8
6 Processus d'accès de l'utilisateur après l'attribution de rôle	8
7 Messages d'erreurs possibles	9
7.1 401 Bad Backend Request	9

Introduction

Cette notice explicative décrit le processus d'attribution de rôle par l'utilisateur avancé (Power-User) aux utilisateurs d'une organisation dans le système de gestion d'identité et d'accès IAM (Identity and Access Management). Dès qu'un utilisateur s'est enregistré sur une application de SASIS, l'utilisateur avancé reçoit un message électronique qui contient l'information d'enregistrement. L'utilisateur avancé doit alors attribuer les rôles dont l'utilisateur a besoin, c'est-à-dire les autorisations d'accès à l'application.

L'utilisateur avancé est le premier interlocuteur compétent pour les questions concernant les autorisations d'accès aux applications de SASIS pour les utilisateurs de son organisation. Il est autorisé en tout temps à faire appel à l'assistance du service Support de SASIS SA (support@sasis.ch).

Vous pouvez accéder au système IAM du groupe santésuisse en cliquant sur le lien suivant: <https://access.santesuisse.ch>

1 Condition préalable

L'utilisateur avancé est déjà enregistré et a demandé auprès de SASIS SA l'autorisation d'accès, puis s'est vu attribuer le rôle correspondant. Les rôles nécessaires et les rôles à attribuer sont à la disposition de l'utilisateur avancé dans le système IAM.

2 Processus d'enregistrement

Le processus d'enregistrement est décrit dans un [document séparé](#).

3 Attribution de rôle pour un nouvel utilisateur

1. Dès qu'un utilisateur de votre organisation s'est enregistré sur une application de SASIS, vous recevez en tant qu'utilisateur avancé un message électronique d'information, dont le contenu est le suivant:

Attribution de rôle pour nouveaux utilisateurs

Bonjour Monsieur XXX

Hans Muster (hans.muster@sasis.ch) s'est enregistré pour un nouvel accès à des applications de SASIS via la plateforme Single Sign-On. Veuillez attribuer à ce compte utilisateur les rôles nécessaires en suivant le lien:

<https://access.santesuisse.ch/m/IdentityManagement/CoreIdentity/GetById/4702>

Lors de son enregistrement via RCC/RCCo, Hans Muster a soumis la demande d'accès suivante:

Je demande l'accès à la version intégrale du RCC et au RCCo avec droits d'écriture!

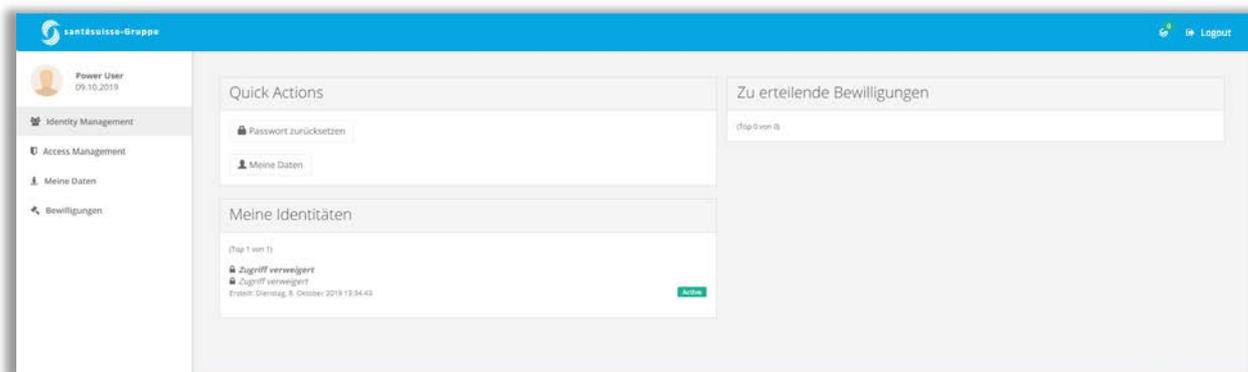
Pour toute question, nous sommes à votre disposition à l'adresse support@sasis.ch.
Vous remerciant, nous vous adressons nos salutations les meilleures
SASIS SA

2. Lorsque vous cliquez sur le lien indiqué dans le message électronique, le masque d'identification suivant apparaît:

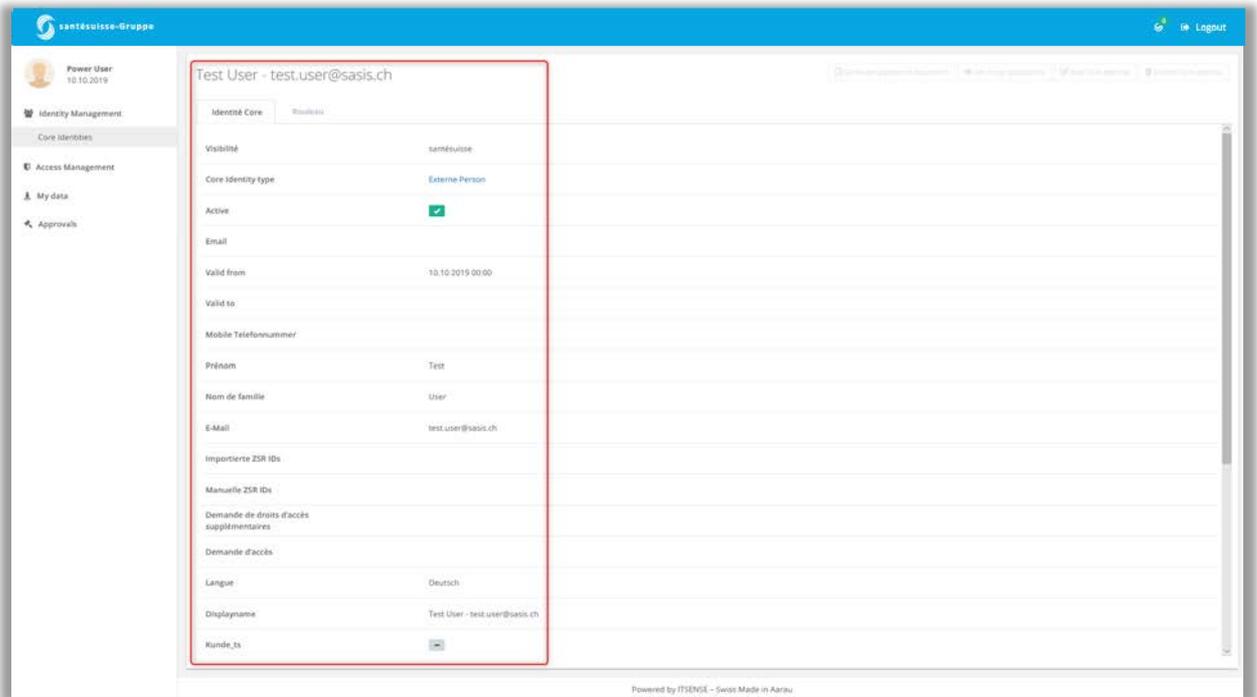


The screenshot shows a login form for 'santésuisse-Gruppe'. At the top left is the logo. Below it, the text 'E-Mail' is followed by the input field containing 'monemail@sasis.ch'. Underneath is the 'Mot de passe' field, which is masked with seven dots. To the left of the password field is a checked checkbox labeled 'Souviens-toi de moi', and to the right is a link labeled 'Nouveau mot de passe'. At the bottom of the form are two buttons: a prominent green button labeled 'Suivant' and a white button with a green border labeled 'Enregistrer'.

3. Après avoir saisi vos données d'accès, cliquez sur «Suivant». Vous serez automatiquement redirigé(e) vers la console de gestion du système IAM pour l'attribution des rôles:

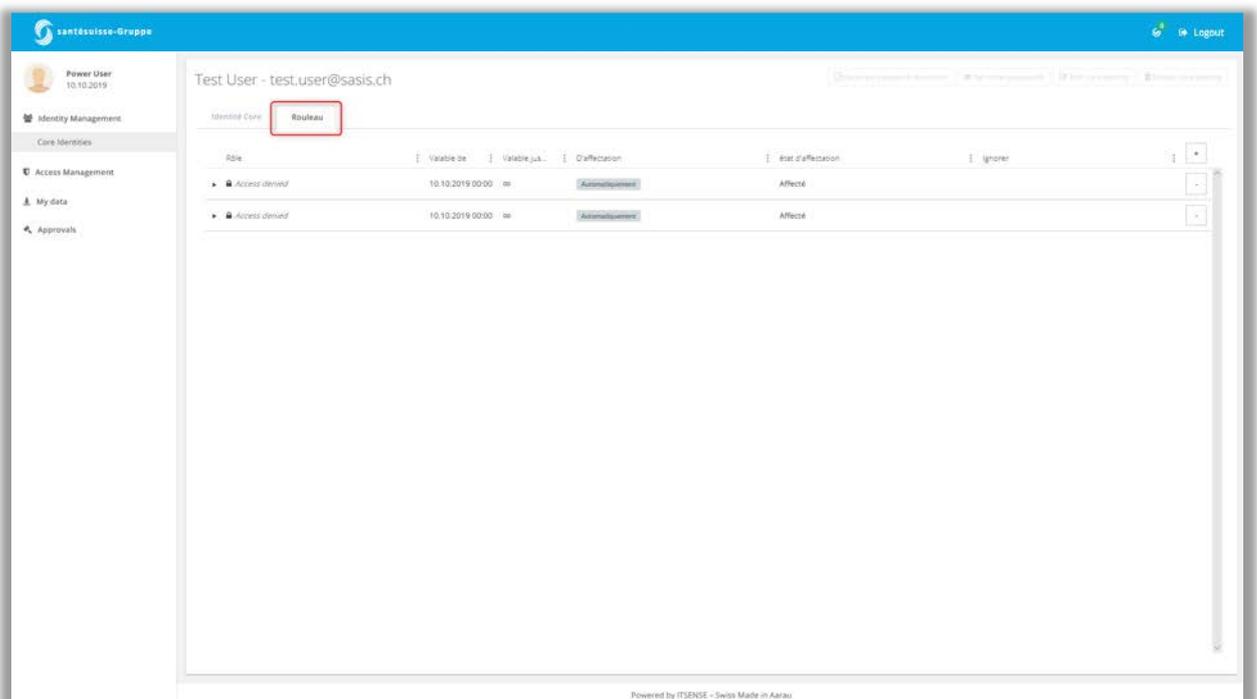


- Après avoir cliqué sur le lien indiqué dans le courriel et vous être connecté(e), la page contenant l'identité Core (informations utilisateur) de l'utilisateur auquel l'autorisation doit être attribuée s'ouvre automatiquement:

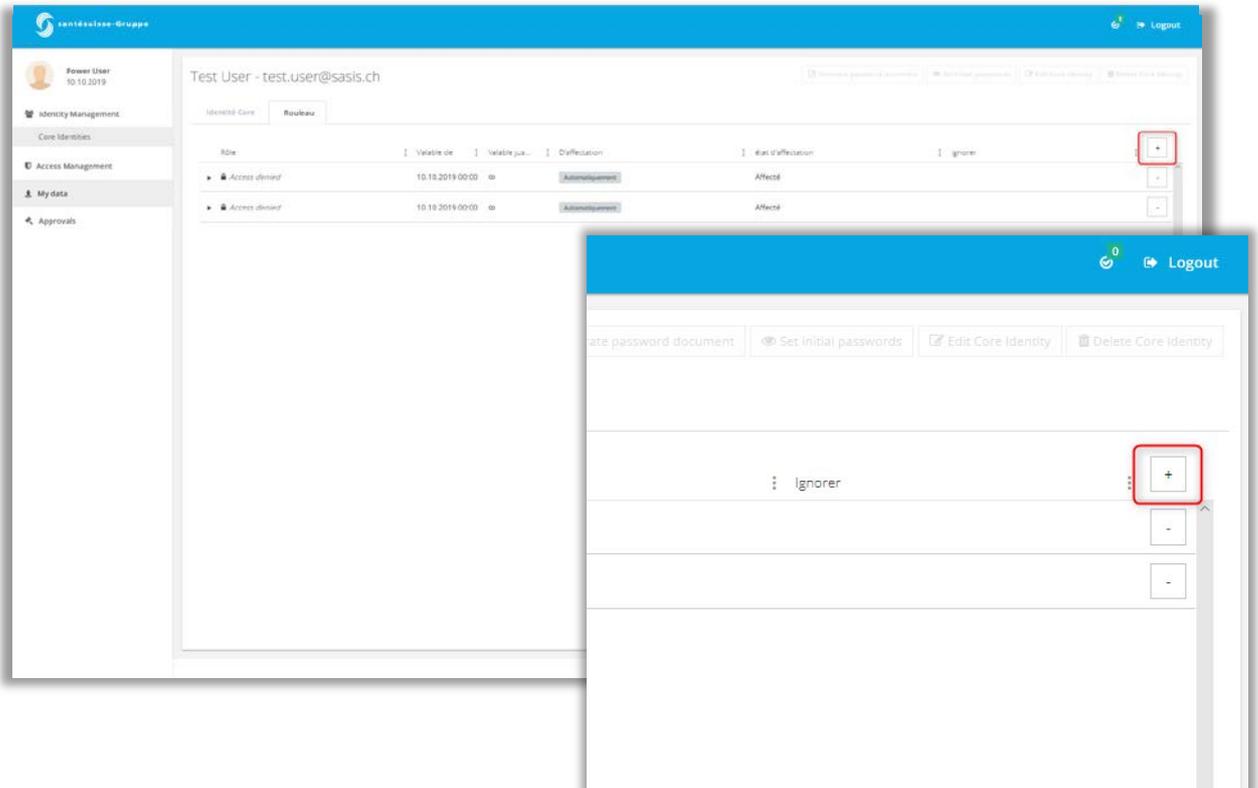


P.S.: en cliquant sur le point de menu Identités Core, vous pouvez rechercher d'autres utilisateurs.

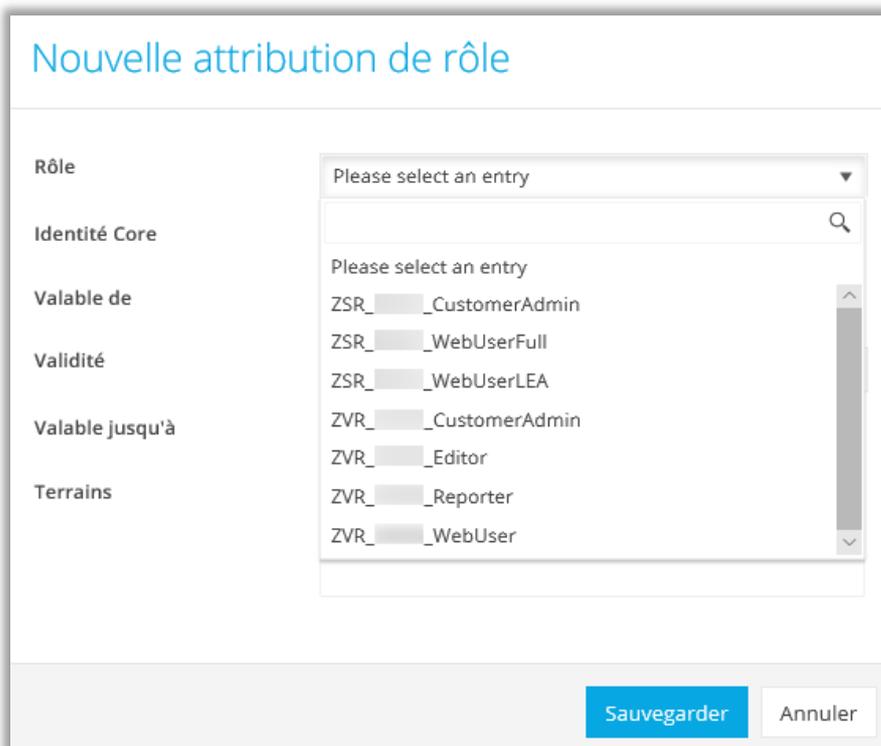
- Cliquez sur l'onglet «Rôle»:



6. Cliquez sur le signe plus (+) dans le coin supérieur droit du masque pour l'attribution des rôles:



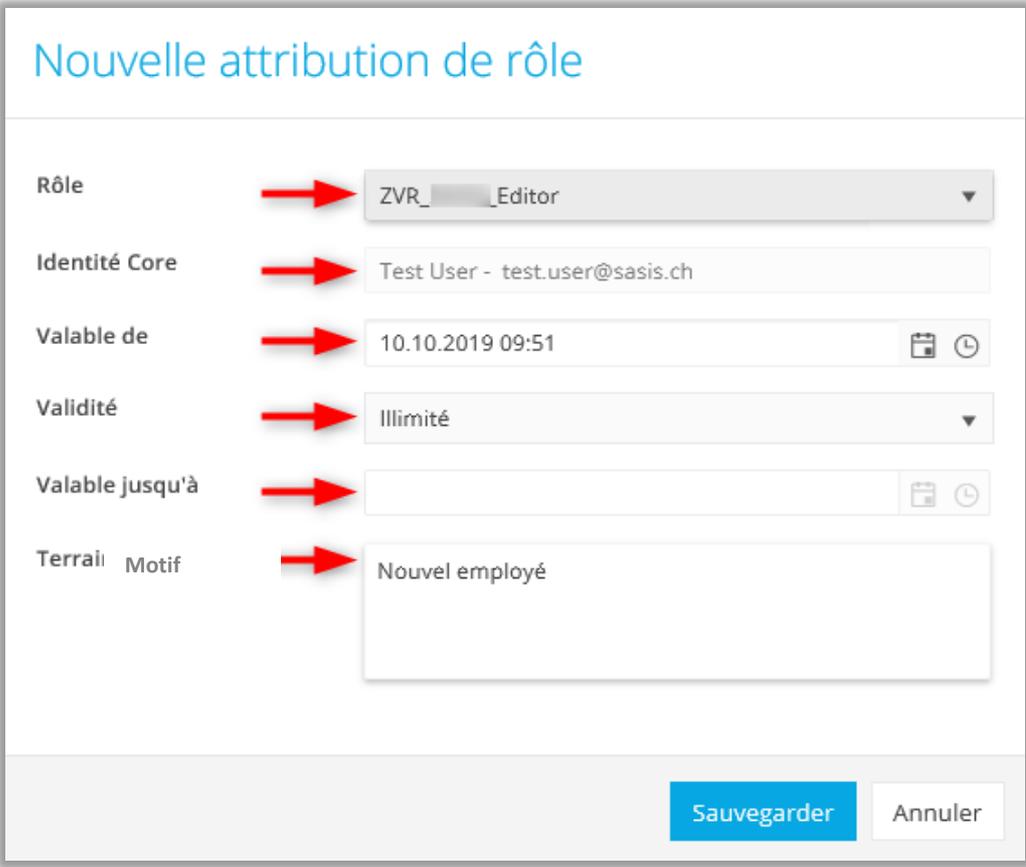
7. Dès que vous cliquez sur le champ «Rôle», vous voyez s'afficher tous les rôles de votre organisation qui sont à votre disposition et que vous pouvez attribuer:



8. Dans la boîte de dialogue «Nouvelle attribution de rôle» qui s'affiche, vous pouvez attribuer le rôle souhaité à l'utilisateur concerné. Si vous ne modifiez pas le champ «Valable de», la date et l'heure actuelle sont automatiquement reprises par le système. Si vous sélectionnez le champ «Validité limitée», vous devez taper une date «Valable jusqu'à». Après avoir indiqué un motif, cliquez sur «Sauvegarder». Pour ajouter d'autres rôles, vous pouvez répéter cette procédure autant de fois que nécessaire:

Exemple:

Il est possible d'attribuer à un utilisateur le rôle «ZVR_Organisation_Editor» afin qu'il ait accès à l'outil d'administration RCCo ainsi que le rôle «ZVR_Organisation_WebUser» pour qu'il puisse accéder au Web RCCo.



Nouvelle attribution de rôle

Rôle → ZVR_..._Editor

Identité Core → Test User - test.user@sasis.ch

Valable de → 10.10.2019 09:51

Validité → Illimité

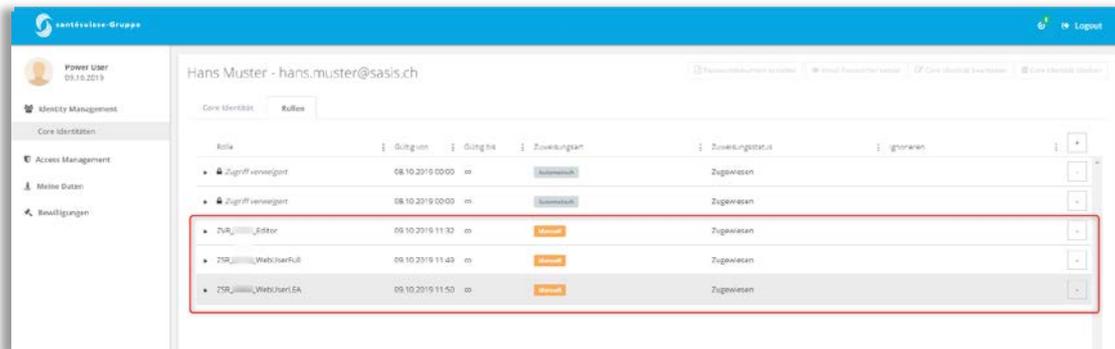
Valable jusqu'à →

Terrain Motif → Nouvel employé

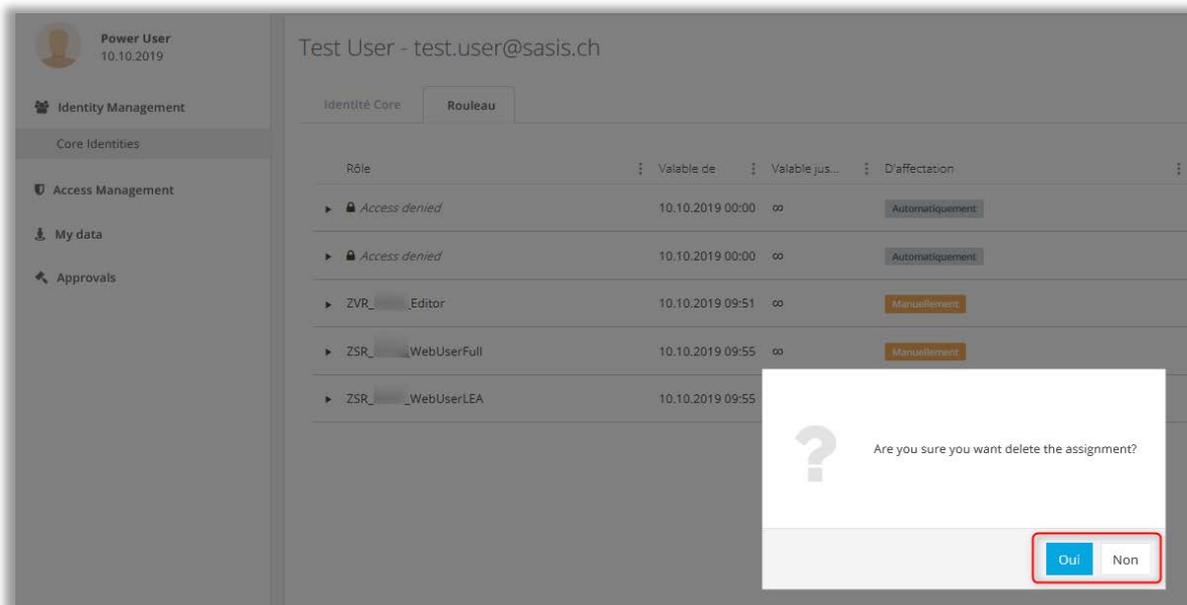
Sauvegarder Annuler

9. La capture d'écran ci-dessus présente les rôles qui sont attribués à l'utilisateur:

A noter: Les entrées présentées avec la mention «Accès refusé» sont des rôles généraux de l'utilisateur qui n'ont pas de lien avec votre organisation et, par conséquent, ne peuvent pas être édités par vous.



10. Pour supprimer un rôle pour l'utilisateur, cliquez pour le rôle en question sur le signe moins (-) situé à droite de l'écran, puis dans le champ de dialogue sélectionnez «Oui» pour confirmer ou «Non» pour annuler l'opération.



4 Description des rôles

Ce paragraphe récapitule tous les rôles et décrit les fonctions qui peuvent être mises à votre disposition pour procéder à l'attribution du rôle.

4.1 Rôles pour le Registre central des conventions «RCCo»

ZVR_ORGANISATION_CustomerAdmin

- Rôle d'utilisateur avancé pour l'attribution des rôles dans le système IAM ainsi que pour la gestion des utilisateurs dans l'outil d'administration RCCo

ZVR_ORGANISATION_Editor

- Rôle d'éditeur permettant de saisir et de traiter des données dans l'outil d'administration RCCo

ZVR_ORGANISATION_Reporter

- Rôle disposant uniquement de droits de lecture dans l'outil d'administration RCCo.

ZVR_ORGANISATION_WebUser

- Rôle d'utilisateur, uniquement autorisé à utiliser l'outil d'administration RCCo

4.2 Rôles pour le registre des codes-créanciers «RCC»

ZSR_ORGANISATION_CustomerAdmin

- Rôle d'utilisateur avancé pour l'autorisation à l'attribution des rôles dans le système IAM

ZSR_ORGANISATION_WebUserFull

- Rôle disposant de l'accès à la version intégrale du RCC

ZSR_ORGANISATION_WebUserLea

- Rôle disposant de l'accès aux informations de la liste des hôpitaux

5 Information à l'utilisateur

Une fois qu'il a achevé l'attribution des rôles, l'utilisateur avancé doit informer l'utilisateur que de nouveaux droits d'accès viennent de lui être attribués.

L'attribution des rôles par le système IAM peut durer quelques minutes. Si l'utilisateur ne parvient pas à accéder immédiatement à l'application, demandez-lui de faire une nouvelle tentative de connexion au bout de 15 minutes. Ce délai s'applique également en cas de suppression d'un rôle.

6 Processus d'accès de l'utilisateur après l'attribution de rôle

1. Une fois les rôles attribués, les utilisateurs peuvent se connecter aux applications SASIS correspondantes à l'aide du nouveau mot de passe créé et de leur adresse e-mail:

Liens

Site Internet SASIS: www.sasis.ch

Site Internet RCCo: www.zentralesvertragsregister.ch

Site Internet RCC: www.sasis.ch/zsr/de/Vollversion

E-Mail
monemail@sasis.ch

Mot de passe
.....

Souviens-toi de moi Nouveau mot de passe

Suivant

Enregistrer

Deutsch English Français Italiano

7 Messages d'erreurs possibles

7.1 401 Bad Backend Request

Si le message d'erreur «401 Bad Backend Request» s'affiche lors de l'authentification, veuillez refermer votre navigateur et accéder à l'application en l'ouvrant à nouveau. Merci de noter que la fenêtre d'identification ne doit pas être ouverte dans plusieurs onglets du navigateur. Cela provoque l'affichage de ce message d'erreur.

Exemple:

