

# Guide de l'utilisateur BPA Autorisations RBAC v5.1

- [Introduction](#)
- [Nouvelles autorisations](#)
  - [Définir les autorisations statiques](#)
- [Inscription des autorisations dans BPA](#)
- [Autorisations de mappage](#)
  - [Définition du mappage des autorisations](#)
  - [Mise à jour du mappage des autorisations](#)

## Introduction

Le contrôle d'accès basé sur les rôles (RBAC) est une méthode de restriction d'accès basée sur les rôles des utilisateurs au sein d'une entreprise. Les rôles par défaut sont disponibles et vous pouvez en créer de nouveaux en sélectionnant les autorisations souhaitées et en mappant ces rôles aux groupes d'utilisateurs. Le mappage des rôles aux groupes d'utilisateurs permet à tous les utilisateurs de ce groupe d'effectuer les opérations associées au rôle.

## Nouvelles autorisations

Cette section décrit comment un microservice peut définir son propre ensemble d'autorisations RBAC.

### Définir les autorisations statiques

Pour définir des autorisations statiques :

1. Créez un fichier JSON répertoriant toutes les autorisations dans le chemin d'accès `microservice/src/config/device-permissions-spec.json`.
2. Exécutez le code JSON suivant pour obtenir une autorisation :

```
{
  "service": "service-name",
  "permissions": [
    {
      "group": "group-name",
      "actions": [
```

```

        {"name":"action-name","displayName":"Display name to be shown in roles page"}
      ]
    }
  ]
}

```

Reportez-vous à l'exemple suivant pour créer, afficher, gérer et supprimer des autorisations au sein d'un groupe d'informations d'identification.

```

{
  "service":"AssetManagerService",
  "permissions": [
    {
      "group": "credential",
      "actions": [
        {"name":"view","displayName":"View Asset Credentials"},
        {"name":"manage","displayName":"Manage Asset Credentials"},
        {"name":"remove","displayName":"Remove Asset Credentials"}
      ]
    }
  ]
}

```

Exemple de création d'autorisations

## Inscription des autorisations dans BPA

Pour enregistrer des autorisations :

1. Importez `rbacSpecProcessorHelper` à partir de `@cisco-bpa-platform/mw-util-common-app`.

```
const { rbacHelper, rbacSpecProcessorHelper } = require('@cisco-bpa-platform/mw-util-common-app');
```

2. Exécutez la commande suivante pour utiliser `rbacSpecProcessorHelper` afin de traiter les autorisations répertoriées dans le fichier JSON.

```

let resources = require('./config/asset-manager-permissions-spec');
let rbacSpecProcessorObj = rbacSpecProcessorHelper.getRbacSpecProcessorUtil();
rbacSpecProcessorObj.setSpec(resources);
await rbacSpecProcessorObj.process();

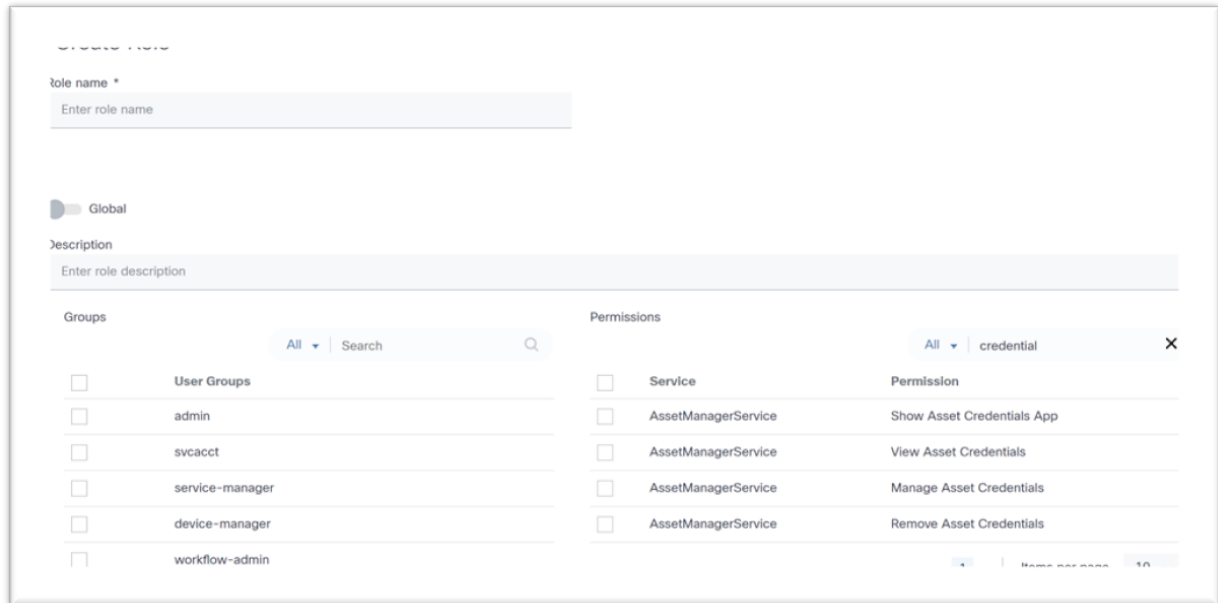
```

---

 Remarque : Les utilisateurs peuvent également se référer aux méthodes partagées dans `@cisco-bpa-platform/mw-util-common-app` pour enregistrer, afficher, gérer et supprimer des

---

Les utilisateurs peuvent afficher les autorisations enregistrées dans les pages Créer un rôle et Modifier le rôle.



**Create Role**

role name \*

Enter role name

☐ Global

Description

Enter role description

**Groups**

All | Search

|                          | User Groups     |
|--------------------------|-----------------|
| <input type="checkbox"/> | admin           |
| <input type="checkbox"/> | svcacct         |
| <input type="checkbox"/> | service-manager |
| <input type="checkbox"/> | device-manager  |
| <input type="checkbox"/> | workflow-admin  |

**Permissions**

All | credential X

|                          | Service             | Permission                 |
|--------------------------|---------------------|----------------------------|
| <input type="checkbox"/> | AssetManagerService | Show Asset Credentials App |
| <input type="checkbox"/> | AssetManagerService | View Asset Credentials     |
| <input type="checkbox"/> | AssetManagerService | Manage Asset Credentials   |
| <input type="checkbox"/> | AssetManagerService | Remove Asset Credentials   |

10

Créer un rôle

## Autorisations de mappage

Les autorisations créées dans la section précédente peuvent être mappées à des rôles par défaut ou en définissant un mappage avec des rôles.

### Définition du mappage des autorisations

Pour mapper les autorisations définies sur les rôles par défaut, créez un fichier JSON dans le chemin d'accès microservice/src/config/device-role-permissions-mapping-spec.json.

Dans l'exemple ci-dessous, trois (3) autorisations sont mappées au rôle BPA Super Admin, deux (2) sont mappées au rôle Admin du service partagé et une (1) est mappée au rôle Opérateur réseau.

---

 Remarque : Le nom du service, le nom du groupe et le nom de l'action doivent être définis de la même manière que dans le fichier JSON.

---

```

{
  "service": "AssetManagerService",
  "roles": [
    {
      "name": "BPA Super Admin",
      "permissions": [
        {"name": "view", "displayName": "View Asset Credentials", "group": "credential"},
        {"name": "remove", "displayName": "Remove Asset Credentials", "group": "credential"},
        {"name": "manage", "displayName": "Manage Asset Credentials Add, Update and Delete Asset C"},
      ]
    },
    {
      "name": "Tenant Admin",
      "permissions": [
        {"name": "view", "displayName": "View Asset Credentials", "group": "credential"},
        {"name": "remove", "displayName": "Remove Asset Credentials", "group": "credential"}
      ]
    },
    {
      "name": "Network Operator",
      "permissions": [
        {"name": "view", "displayName": "View Asset Credentials", "group": "credential"}
      ]
    }
  ]
}

```

## Mise à jour du mappage des autorisations

Pour mettre à jour le mappage des autorisations :

1. Importez `rbacHelper`, `rbacPermissionMappingHelper` depuis `@cisco-bpa-platform/mw-util-common-app`.

```
const { rbacHelper, rbacPermissionMappingHelper } = require('@cisco-bpa-platform/mw-util-common-app');
```

2. Exécutez la commande suivante pour mettre à jour le mappage des autorisations avec les rôles :

```

let rbacUtilObj = rbacHelper.getRbacUtilObj();
let registryDetails = await rbacUtilObj.getRegistryByName({}, 'device-role-permissions-mapping-spec');
if (Array.isArray(registryDetails) && registryDetails.length === 0) {
  let rbacPermissionMappingSpecProcessorObj = rbacPermissionMappingHelper.getRbacSpecProcessorUtil()
  let rolePermissions = require('./config/device-role-permissions-mapping-spec');
  rbacPermissionMappingSpecProcessorObj.setSpec(rolePermissions);
  await rbacPermissionMappingSpecProcessorObj.process();
  let rbacUtilObjRegister = rbacHelper.getRbacUtilObj();
  await rbacUtilObjRegister.addRegistry({}, 'device-role-permissions-mapping-spec');
}

```

3. Exécutez la commande suivante pour traiter les fichiers, créer une liste d'autorisations et mapper les autorisations avec les rôles :

```
async function permissionsSpecProcessor() {
  let resources = require('./config/device-permissions-spec');
  let rbacSpecProcessorObj = rbacSpecProcessorHelper.getRbacSpecProcessorUtil();
  rbacSpecProcessorObj.setSpec(resources);
  await rbacSpecProcessorObj.process();

  let rbacUtilObj = rbacHelper.getRbacUtilObj();
  let registryDetails = await rbacUtilObj.getRegistryByName({} 'device-role-permissions-mapping-spec');
  if (Array.isArray(registryDetails) && registryDetails.length === 0) {
    let rbacPermissionMappingSpecProcessorObj = rbacPermissionMappingHelper.getRbacSpecProcessorUtil();
    let rolePermissions = require('./config/device-role-permissions-mapping-spec');
    rbacPermissionMappingSpecProcessorObj.setSpec(rolePermissions);
    await rbacPermissionMappingSpecProcessorObj.process();
    let rbacUtilObjRegister = rbacHelper.getRbacUtilObj();
    await rbacUtilObjRegister.addRegistry({}, 'device-role-permissions-mapping-spec');
  }
}
```

---

 Remarque : Les utilisateurs peuvent également se référer aux méthodes partagées dans [@cisco-bpa-platform/mw-util-common-app](https://github.com/cisco-bpa-platform/mw-util-common-app) pour mettre à jour le mappage d'autorisations avec des rôles.

---

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.