UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide des administrateurs M365

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Table des matières

INTRODUCTION

1.1 CONTEXTE

De nos jours, les établissements font face à plusieurs défis dans la manière de gérer les accès privilégiés et cela s'est accentué avec l'avènement de l'infonuagique. Le déploiement de Microsoft 365 (M365) vient avec plusieurs rôles d'administrateurs que l'on peut créer. Cependant, il est important de créer ces rôles basés sur les bonnes pratiques de sécurité. Le contrôle d'accès basé sur les rôles est essentiel pour améliorer le niveau de sécurité de l'établissement, ceci permet au service informatique d'agir de manière ciblée en se concentrant sur les autorisations.

Le CESI a décidé de créer un guide M365 pour les administrateurs afin que les établissements puissent s'en inspirer lors du déploiement de M365 ou après le déploiement afin de s'assurer que les bons rôles d'administrateurs ont été attribués.

1.2 OBJECTIF

Le présent document vise à préciser quelques bonnes pratiques à suivre avant d'attribuer des rôles d'administrateurs dans M365.

1.3 PORTÉE

Ce document s'adresse à tous les établissements d'enseignement supérieur, aux détenteurs de l'information, aux professionnels de la sécurité de l'information et à toutes les ressources qui seront sollicitées lors du déploiement de M365 dans l'établissement.

2 ADMINISTRATEUR MICROSOFT M365

Un rôle d'administrateur est utilisé afin de gérer les accès qui accordent des privilèges pour permettre d'effectuer certaines tâches. Chaque rôle d'administrateur correspond à des fonctions qui donnent, aux personnes concernées dans votre établissement, des autorisations pour effectuer des tâches spécifiques.

Le contrat de service Microsoft 365 (M365) est fourni avec un ensemble de rôles d'administrateur que vous pouvez attribuer aux utilisateurs de votre établissement.

L'attribution des rôles administrateurs se fait à partir du Centre d'administration Microsoft 365.

3 QUELQUES BONNES PRATIQUES À SUIVRE AVANT D'ATTRIBUER LES RÔLES D'ADMINISTRATEUR

3.1 ADMINISTRATEURS DANS MICROSOFT (M365)

Le rôle d'un administrateur M365 est très complexe et exige non seulement une expertise technique, mais aussi un éventail de compétences professionnelles telles que des capacités interpersonnelles, une gestion efficace du temps, une forte orientation vers le service à la clientèle et une habileté dans la gestion du personnel.

Un administrateur M365 joue un rôle crucial dans la supervision des abonnements M365, la gestion des utilisateurs et la configuration pour maintenir l'ordre et l'efficacité. Pour rationaliser les tâches et déléguer efficacement les responsabilités, il existe différents rôles d'administrateur. Ces rôles peuvent être attribués en fonction de l'expertise d'une personne, et il est possible d'avoir plusieurs administrateurs avec le même rôle.

3.2 ATTRIBUER LE RÔLE LE MOINS PERMISSIF

Microsoft recommande d'attribuer aux utilisateurs de M365 le niveau d'accès et de permission minimum requis pour leur permettre d'effectuer leur travail. Même s'il peut être tentant de désigner plusieurs administrateurs généraux pour venir à bout de la charge de travail, cela constitue un risque pour la sécurité et cela pourrait causer des problèmes si l'établissement fait l'objet d'un audit dans le cadre d'une certification de sécurité ou d'une réglementation relative aux données. Il est aussi plus facile de surveiller deux administrateurs que d'en surveiller une dizaine.

L'attribution du rôle le moins permissif est aussi un requis des bonnes pratiques générales et de la gestion des identités et des accès (GIA). La GIA est basée sur les principes du droit d'accès minimal et de séparation des tâches.

Si vous souhaitez par exemple que quelqu'un réinitialise les mots de passe des employés, vous ne devez pas attribuer le rôle d'administrateur global illimité, vous devez attribuer un rôle d'administrateur limité, comme administrateur de mot de passe ou administrateur du service d'assistance. Cela aidera à protéger vos données. Il est important d'attribuer le rôle d'administrateur le moins permissif aux utilisateurs afin qu'ils aient accès seulement à ce dont ils ont besoin pour effectuer leur travail.

3.3 AUTHENTIFICATION MULTIFACTEUR

Les comptes auxquels sont affectés les droits d'administration sont les plus ciblés par les attaquants, car ils vous donnent accès à des privilèges que les utilisateurs réguliers n'ont pas. L'authentification multifactorielle permet aux utilisateurs d'utiliser une deuxième méthode d'identification pour vérifier leur identité. Si vous avez recours à l'authentification multifactorielle, même si le mot de passe de l'administrateur est compromis, le mot de passe devient inutile sans la deuxième méthode d'identification. Exiger l'authentification multi facteur (MFA) sur ces comptes administrateurs est un moyen simple de réduire le risque de compromission de ces comptes. Microsoft recommande d'exiger l'authentification multifactorielle (MFA) pour tous les utilisateurs, et les administrateurs devraient utiliser l'authentification multifactorie lle pour se connecter.

4 LES RÔLES ADMINISTRATEURS PAR APPLICATION

4.1 ADMINISTRATEUR GLOBAL

Les administrateurs globaux sont les seuls administrateurs qui ont un accès quasi illimité aux paramètres de votre établissement et à la plupart de ses données. Un administrateur global peut verrouiller son compte par inadvertance et demander une réinitialisation de son mot de passe. Un autre administrateur global ou un administrateur d'authentification privilégiée peut réinitialiser le mot de passe d'un administrateur global. Par conséquent, Microsoft recommande d'avoir au moins un autre administrateur global ou un administrateur d'authentification privilégié au cas où un administrateur global verrouillerait son compte. Microsoft recommande d'avoir au moins 2 à 4 administrateurs généraux.
Seuls les administrateurs généraux peuvent :

- Réinitialiser les mots de passe pour l'ensemble des utilisateurs;
- Ajouter et gérer des domaines;
- Débloquer un autre administrateur général.

4.2 ADMINISTRATEUR EXCHANGE

Un administrateur de serveur Exchange met en place et gère un serveur Microsoft Exchange. Il aide à configurer les comptes d'utilisateurs et les boites aux lettres, à sauvegarder, sécuriser et restaurer les fichiers. Il effectue la maintenance de routine du serveur, configure les nouveaux utilisateurs et est le premier point de contact en cas de problèmes liés à Microsoft Exchange.
Les administrateurs Exchange peuvent :

- Récupérer des éléments supprimés dans une boite aux lettres utilisateur;

- Configurez une stratégie d'archivage et de suppression pour les boites aux lettres de votre établissement;
- Configurez les fonctionnalités de boite aux lettres telles que la stratégie de partage de boites aux lettres;
- Configurez les délégués « Envoyer en tant que » et « Envoyer de la part » pour la boite aux lettres d'une personne;
- Créez une boite aux lettres partagée afin qu'un groupe de personnes puisse surveiller et envoyer des courriels à partir d'une adresse commune;
- Configurer la protection antipourriel dans Exchange Online Protection (EOP);
- Gestion des groupes Microsoft 365.

4.3 ADMINISTRATEUR SHAREPOINT

Les administrateurs SharePoint sont responsables de la gestion des sites SharePoint, de l'accès des utilisateurs et des autorisations. Ils configurent et entretiennent les serveurs SharePoint, résolvent les problèmes, surveillent les performances du système et fournissent une assistance technique. Ils collaborent avec les parties prenantes pour assurer le bon fonctionnement, la sécurité et l'optimisation des environnements SharePoint au sein de l'établissement.

Les administrateurs globaux de Microsoft 365 sont responsables d'attribuer à des utilisateurs le rôle d'administrateur SharePoint. Il est à noter que le rôle d'administrateur global dispose déjà de toutes les autorisations du rôle d'administrateur SharePoint.

Les administrateurs SharePoint ont accès au centre d'administration SharePoint et peuvent :

- Créer et gérer des sites
- Désigner des administrateurs de sites
- Gérer les paramètres de partage
- Gérer les groupes Microsoft 365 (création, suppression, restauration de groupes et modification des propriétaires de groupes)

4.4 ADMINISTRATEUR TEAMS

À l'aide de Microsoft Entra ID, vous pouvez désigner des administrateurs qui ont besoin de différents niveaux d'accès pour gérer Microsoft Teams. Les administrateurs peuvent gérer l'intégralité de la charge de travail Teams ou disposer d'autorisations déléguées pour résoudre les problèmes de qualité des appels ou gérer les besoins de téléphonie de votre établissement.

Il existe plusieurs rôles d'administrateur dans Teams :

a) **Administrateur Teams** : parfois appelé administrateur du service Teams, il est votre administrateur principal pour Teams. Il a accès à votre centre d'administration Teams et le gère dans son intégralité, notamment ses paramètres, stratégies et mises à niveau.

b) **Administrateur des communications Teams** : ce rôle a pour but de gérer les fonctionnalités d'appel et de réunion au sein du service Teams. (Gérer les réunions, la voix, résoudre des problèmes de qualité et la fiabilité des appels.)

c) **Administrateur d'appareil Teams** : est un rôle qui permet de surveiller l'intégrité des appareils installés avec Microsoft Teams et de gérer la configuration et les mises à jour de ces appareils. Ce rôle est très important si vous utilisez des appareils de salle de réunion connectés à Teams.

d) **L'ingénieur de support des communications Teams** est essentiellement chargé de surveiller et résoudre les problèmes d'appel. Ce rôle d'administrateur a accès à l'analyse des appels, qui comprend les profils des utilisateurs, l'historique des appels et les statistiques, ainsi qu'à des outils avancés conçus pour faciliter la résolution des problèmes concernant la qualité des appels.

e) **Le spécialiste du support des communications Teams** est lui aussi chargé de la surveillance et de la résolution des problèmes liés aux appels, mais, à la différence de l'ingénieur de support des communications, il n'a pas accès aux outils avancés. Le spécialiste du support des communications peut consulter le profil des utilisateurs en effectuant une recherche, des données anonymes ainsi que des statistiques limitées.

4.5 ADMINISTRATEUR DE LICENCES

Auparavant, les autorisations requises pour gérer les attributions de licences n'étaient accordées qu'aux rôles d'administrateur global et d'administrateur de compte d'utilisateur, ce qui a entraîné des problèmes pour respecter le principe du moindre privilège.

Le rôle d'administrateur de licences permet de gérer les licences des utilisateurs, sans accorder d'autorisations supplémentaires. En dehors de la gestion des attributions de licences, les seules autres actions que les membres du rôle d'administrateur de licences peuvent effectuer sont de définir la propriété "UsageLocation" pour les utilisateurs, ce qui est une condition préalable à l'attribution d'une licence, et d'accéder à la partie Tableau de bord de l'état des services du portail. En outre, les utilisateurs auxquels le rôle d'administrateur de licences a été attribué peuvent gérer l'octroi de licences par groupe. Ils ne peuvent cependant pas acheter de nouveaux abonnements, gérer des utilisateurs ou des groupes, ou effectuer toute autre action.

4.6 ADMINISTRATEUR D'APPLICATIONS OFFICE

Un établissement disposant d'un environnement M365 bien administré est forcément bien plus productif qu'un établissement dont l'environnement M365 est mal géré.

Une bonne administration implique que les utilisateurs puissent gérer l'accès à leurs sites en fonction de leurs stratégies de gouvernance et partager les documents de la façon la plus fluide possible.

Pour ce faire, les administrateurs d'applications Office sont nécessaires pour prendre en charge la gestion :

- Des paramètres d'audit;
- Des types de contenus et des stratégies relatives aux documents d'archives;
- De l'encadrement du partage de l'information;
- D'utiliser le service de stratégie infonuagique pour Microsoft 365 pour créer et gérer des stratégies basées sur le nuage;
- De la création et gestion des demandes de service;
- Du contenu Nouveautés que les utilisateurs voient dans leurs applications Microsoft 365;
- De la surveillance de l'état d'intégrité des services.

4.7 ADMINISTRATEUR DE MOTS DE PASSE

L'administrateur de mot de passe gère la réinitialisation des mots de passe des utilisateurs. Il peut gérer les demandes de service et surveiller l'intégrité des services.

Votre établissement peut aussi décider de configurer la réinitialisation de mot de passe en libre-service. Cela permettra aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe Azure AD.

5 GESTION DES COMPTES À HAUTS PRIVILÈGES DANS MICROSOFT ENTRA (PIM)

La gestion des comptes à hauts privilèges (PIM) est un service de Microsoft Entra ID qui vous permet de gérer, de contrôler et de surveiller l'accès aux ressources importantes de votre organisation. Elle assure aussi une activation de rôle basée sur l'heure et l'approbation pour atténuer les risques d'autorisations d'accès excessives, injustifiées ou malveillantes sur les ressources qui vous intéressent.
PIM nous donne accès à un moyen sécurisé pour accorder l'accès aux ressources de votre organisation.
Le processus ci-dessous décrit les étapes à compléter pour l'attribution des rôles aux membres :

1. **Assigner**

Le processus d'attribution comprend :

- Éligibles exigent des membres qu'ils effectuent une action pour utiliser ce rôle.
- Actives n'exigent pas des membres qu'ils effectuent une action pour utiliser ce rôle.
- La durée de l'attribution (dates de début et de fin).

2. Activer

Seuls les utilisateurs qui sont éligibles pour un rôle peuvent activer l'attribution de rôle avant d'utiliser le rôle.

Pour activer le rôle :

- Sélectionner une durée d'activation précise comprise dans les limites configurées par les administrateurs.
- Donner la raison de la demande d'activation.

3. Approuver ou rejeter

- Les approbateurs délégués reçoivent des notifications par courriel lorsqu'une demande de rôle est en attente de leur approbation.
- Les approbateurs peuvent afficher, approuver ou rejeter ces demandes en attente dans PIM.
- Une fois la demande approuvée, le membre peut commencer à utiliser le rôle

4. Étendre et renouveler

- **Étendre** : Lorsqu'une attribution de rôle est sur le point d'expirer, l'utilisateur peut demander son extension à travers PIM.
- **Renouveler** : quand une attribution de rôle a expiré, l'utilisateur peut demander son renouvellement à travers PIM.

6 COMPARAISON DE QUELQUES RÔLES ADMINISTRATEURS

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Consulter les propriétés de base sur toutes les ressources dans le Centre d'administration Microsoft 365	*	*	*	*	*	*	*
Lire les rapports d'utilisation dans le Centre d'administration Microsoft 365	*				*	*	*
Créer et gérer des demandes de service dans le Centre d'administration Microsoft 365	*		*		*	*	*
Consulter et configurer l'état du service dans le Centre d'administration Microsoft 365	*		*	*	*	*	*
Lire toutes les propriétés des performances réseau dans le Centre d'administration Microsoft 365	*				*	*	*
Créer et gérer des tickets de support dans le Centre d'administration Microsoft Entra.	*		*		*	*	*
Gérer tous les aspects de Skype Entreprise Online	*						

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Réinitialiser les mots de passe de tous les utilisateurs		*					
Lire et configurer l'état du service dans Centre d'administration Microsoft Entra.			*	*	*	*	*
Créer et supprimer toutes les ressources, puis lire et mettre à jour les propriétés standard dans SharePoint						*	*
microsoft.office365.migrations/allEntities/allProperties/allTasks						*	*
Gérer tous les aspects d'Exchange Online					*	*	
Mettre à jour la propriété des Groupes Microsoft 365					*		*
Mettre à jour l'appartenance aux Groupes Microsoft 365					*		*
Mettre à jour les propriétés de base des Groupes Microsoft 365					*		*
Restaurer les groupes Microsoft 365 supprimés					*		*
Supprimer des Groupes Microsoft 365					*		*
Créer des Groupes Microsoft 365					*		*
Consulter les membres masqués d'un groupe					*		*
Lire et configurer tous les aspects du service Windows Update						*	
Gérer tous les aspects de Microsoft Defender - Protection avancée contre les menaces						*	
microsoft.viva.pulse/allEntities/allProperties/allTasks						*	
microsoft.viva.goals/allEntities/allProperties/allTasks						*	
Gérer tous les aspects des consultations virtuelles						*	
Gérer tous les aspects de Microsoft Teams						*	
Gérer tous les aspects de Power BI						*	
Gérer tous les aspects de Power Apps						*	
Gérer tous les aspects d'Entra Permissions Management						*	
Gérer tous les aspects de Yammer						*	
Gérer tous les aspects de communication des utilisateurs finaux			*			*	
Gérer tous les aspects de Skype Entreprise Online						*	
Créer et supprimer toutes les ressources, et lire et mettre à jour les propriétés standard dans le Centre de sécurité et conformité						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Gérer tous les aspects du contenu dans Recherche Microsoft						*	
Gérer tous les aspects de Microsoft 365 et du centre de sécurité et de conformité						*	
Gérer tous les aspects de création des messages Microsoft 365 organisationnels						*	
Lire les messages de sécurité dans le Centre de messages du Centre d'administration Microsoft 365						*	
Lire les messages dans le Centre de messages dans le Centre d'administration Microsoft 365, à l'exception des messages de sécurité			*			*	
Gérer tous les aspects de Customer Lockbox						*	
Gérer les sources d'apprentissage et toutes leurs propriétés dans l'application d'apprentissage						*	
Gérer la visibilité des sujets sur le réseau de connaissances dans le Centre d'administration Microsoft 365						*	
Lire et mettre à jour toutes les propriétés du réseau de connaissances dans Centre d'administration Microsoft 365						*	
Consulter les rapports d'analyse sur la compréhension du contenu dans le centre d'administration Microsoft 365						*	
Lire et mettre à jour toutes les propriétés de la compréhension de contenu dans le Centre d'administration Microsoft 365						*	
Gérer tous les aspects d'analyses du bureau						*	
Gérer tous les aspects du gestionnaire de conformité Microsoft Purview						*	
Gérer tous les aspects de Microsoft Intune						*	
Gérer tous les aspects de Viva Insights						*	
Créer et gérer tous les aspects des revendications de garantie matérielle Microsoft						*	
Lire les statuts d'expédition pour les réclamations ouvertes concernant la garantie du matériel Microsoft						*	
Créer, lire, mettre à jour et supprimer les adresses d'expédition pour les revendications de garantie matérielle Microsoft, y compris les adresses d'expédition créées par d'autres personnes						*	
Gérer tous les aspects de Microsoft Power Automate						*	
microsoft.networkAccess/allEntities/allProperties/allTasks						*	
Gérer tous les aspects de Microsoft Edge						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Gérer tous les aspects de Dynamics 365						*	
Lire les services d'achat dans le centre Administration M365.						*	
Gérer tous les aspects de la facturation Office 365						*	
Gérer tous les aspects de Windows 365						*	
Gérer tous les aspects d'Azure Information Protection						*	
Gérer tous les aspects de Protection avancée contre les menaces Azure						*	
microsoft.directory/externalUserProfiles/delete						*	
microsoft.directory/externalUserProfiles/basic/update						*	
microsoft.directory/externalUserProfiles/standard/read						*	
microsoft.directory/pendingExternalUserProfiles/delete						*	
microsoft.directory/pendingExternalUserProfiles/basic/update						*	
microsoft.directory/pendingExternalUserProfiles/standard/read						*	
microsoft.directory/pendingExternalUserProfiles/create						*	
Gérer tous les aspects des flux de travail et des tâches de cycle de vie dans Microsoft Entra ID						*	
Configuration de mise à jour requise pour créer et gérer des informations d'identification vérifiables						*	
Configuration de lecture requise pour créer et gérer des informations d'identification vérifiables						*	
Supprimer la configuration requise pour créer et gérer les informations d'identification vérifiables et supprimer toutes les informations d'identification vérifiables						*	
Créer une configuration requise pour la création et la gestion des informations d'identification vérifiables						*	
Mettre à jour un contrat d'information d'identification vérifiable						*	
Lire un contrat d'information d'identification vérifiable						*	
Créer un contrat d'information d'identification vérifiable						*	
Révoquer une carte d'information d'identification vérifiable						*	

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Lire une carte d'information d'identification vérifiable						*	
Créer des locataires dans Microsoft Entra						*	
Mettre à jour des propriétés de base des stratégies de création d'un principal du service						*	
Lire les propriétés standard des stratégies de création d'un principal du service						*	
Supprimer des stratégies de création d'un principal du service						*	
Créer des stratégies de création du principal du service						*	
Mettre à jour des propriétés de base des stratégies d'octroi d'autorisation						*	
Lire les propriétés standard pour les stratégies d'octroi d'autorisation						*	
Supprimer des stratégies d'octrois d'autorisations						*	
Créer des stratégies pour les octrois d'autorisations						*	
microsoft.directory/users/convertExternalToInternalMemberUser						*	
Créer et supprimer des utilisateurs, et lire et mettre à jour toutes les propriétés						*	
L'achat et la gestion d'abonnement incluent les autorisations pour supprimer un abonnement						*	
Lire toutes les propriétés sur les rapports de connexion, y compris les propriétés privilégiées						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/schema/manage						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/jobs/manage						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/credentials/manage						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage						*	
microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage						*	
Lire les paramètres d'approvisionnement associés aux principaux de service						*	
Attribuer des autorisations pour tous les administrateurs globaux						*	
Créer et supprimer des principaux de service, et lire et mettre à jour toutes les propriétés						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Effectuer l'action de service « récupérer les propriétés d'extension disponibles »						*	
Exécuter l'action de service « activer la fonctionnalité d'annuaire »						*	
Exécuter l'action de service « désactiver la fonctionnalité d'annuaire »						*	
Effectuer l'action « activer le service » pour un service						*	
Créer et supprimer des appartenances aux rôles étendues, puis lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des définitions de rôles, et lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des affectations de rôle, et lire et mettre à jour toutes les propriétés						*	
Mettre à jour du contexte d'authentification de l'accès conditionnel des actions de ressources de contrôle d'accès basé sur les rôles (RBAC) de Microsoft 365.						*	
Lire toutes les propriétés des journaux d'approvisionnement						*	
Lire toutes les ressources dans Privileged Identity Management						*	
microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/standard/read						*	
microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/basic/update						*	
microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/create						*	
Mettre à jour les restrictions de client de la stratégie d'accès interclient pour les partenaires						*	
Mettre à jour les paramètres de réunion Teams infonuagique de la stratégie d'accès interclient pour les partenaires						*	
Mettre à jour les paramètres de connexion directe Microsoft Entra B2B de la stratégie d'accès interclient pour les partenaires						*	
Mettre à jour les paramètres de collaboration Microsoft Entra B2B de la stratégie d'accès interclient pour les partenaires						*	
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/standard/read						*	
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/resetToDefaultSettings						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/basic/update						*	
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/standard/read						*	
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/resetToDefaultSettings						*	
microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/basic/update						*	
Lire les propriétés de base de la stratégie d'accès interclient pour les partenaires						*	
Créer la stratégie d'accès interclient pour les partenaires						*	
Créer une stratégie d'accès interclient pour les partenaires						*	
Mettre à jour les restrictions de client de la stratégie d'accès interclient par défaut						*	
Mettre à jour les paramètres de réunion Teams infonuagique de la stratégie d'accès interclient par défaut						*	
Mettre à jour les paramètres de connexion directe Microsoft Entra B2B de la stratégie d'accès interclient par défaut						*	
Mettre à jour les paramètres de collaboration Microsoft Entra B2B de la stratégie d'accès interclient par défaut						*	
Lire les propriétés de base de la stratégie d'accès interlocataires par défaut						*	
Mettre à jour les paramètres de base de la stratégie d'accès interclient						*	
Mettre à jour les points de terminaison infonuagiques autorisés de la stratégie d'accès interclient						*	
Lire les propriétés de base de la stratégie d'accès interclient						*	
Gérer tous les aspects des stratégies d'accès conditionnel						*	
Créer et supprimer des stratégies, et lire et mettre à jour toutes les propriétés						*	
Gérer tous les aspects de la synchronisation du hachage de mot de passe pour Microsoft Entra Connect						*	
Créer et supprimer des organisations, et lire et mettre à jour toutes les propriétés						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Créer et supprimer des autorisations accordées pour OAuth 2.0, puis lire et mettre à jour toutes les propriétés						*	
Gérer tous les aspects liés à la personnalisation de l'organisation des pages de connexion						*	
Créer et supprimer toutes les ressources, puis lire et mettre à jour les propriétés standards dans Protection Microsoft Entra ID						*	
Gérer la stratégie d'authentification hybride dans Microsoft Entra ID						*	
Créer et supprimer des modèles de paramètres de groupe et lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des paramètres de groupe, et lire et mettre à jour toutes les propriétés						*	
Mettre à jour des groupes à affecter à un rôle administratif						*	
Restaurer des groupes avec attribution de rôles						*	
Supprimer des groupes avec attribution de rôles						*	
Créer des groupes avec attribution de rôles						*	
Créer et supprimer des groupes, et lire et mettre à jour toutes les propriétés						*	
Créer, puis supprimer des ressources; lire, puis mettre à jour toutes les propriétés de gestion des habilitations Microsoft Entra ID						*	
Supprimer la configuration de fédération de base pour les domaines						*	
Créer la configuration de fédération de base pour les domaines						*	
Mettre à jour la configuration de fédération de base pour les domaines						*	
Lire les propriétés standard de la configuration de fédération pour les domaines						*	
Créer et supprimer des domaines, et lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des modèles de rôle d'annuaire et lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des rôles d'annuaire, et lire et mettre à jour toutes les propriétés						*	
Mettre à jour les propriétés de base sur les stratégies d'inscription des appareils						*	
Lire les propriétés standard sur les stratégies d'inscription des appareils						*	
Mettre à jour les propriétés de base des stratégies d'une application de gestion des appareils						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Lire les propriétés standard des stratégies d'une application de gestion des appareils						*	
Lire toutes les propriétés des informations d'identification du compte d'administrateur local sauvegardé pour Microsoft Entra ID appareils joints, à l'exception du mot de passe.						*	
Mettre à jour les propriétés de base des règles personnalisées qui définissent les emplacements réseau						*	
Lire les propriétés de base des règles personnalisées qui définissent les emplacements réseau						*	
Supprimer des règles personnalisées qui définissent les emplacements réseau						*	
Créer des règles personnalisées qui définissent les emplacements réseau						*	
microsoft.directory/multiTenantOrganization/tenants/standard/read						*	
microsoft.directory/multiTenantOrganization/tenants/organizationDetails/read						*	
microsoft.directory/multiTenantOrganization/tenants/delete						*	
microsoft.directory/multiTenantOrganization/tenants/create						*	
microsoft.directory/multiTenantOrganization/tenants/organizationDetails/update						*	
microsoft.directory/multiTenantOrganization/standard/read						*	
microsoft.directory/multiTenantOrganization/joinRequest/standard/read						*	
microsoft.directory/multiTenantOrganization/joinRequest/organizationDetails/update						*	
microsoft.directory/multiTenantOrganization/create						*	
microsoft.directory/multiTenantOrganization/basic/update						*	
microsoft.directory/groupsAssignableToRoles/reprocessLicenseAssignment						*	
microsoft.directory/groupsAssignableToRoles/assignLicense						*	
Créer et supprimer des appareils, et lire et mettre à jour toutes les propriétés						*	
Restaurer l'état d'origine des objets supprimés						*	
Supprimer définitivement les objets qui ne peuvent plus être restaurés						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Créer et gérer des extensions d'authentification personnalisées						*	
Créer et supprimer des contrats de partenariat, et lire et mettre à jour toutes les propriétés						*	
Créer et supprimer des contacts, et lire et mettre à jour toutes les propriétés						*	
Mettre à jour les paramètres des groupes de connecteurs						*	
Consulter toutes les propriétés des groupes de connecteurs						*	
Supprimer des groupes de connecteurs						*	
Créer des groupes de connecteurs						*	
Consulter des propriétés du connecteur d'application du proxy d'application						*	
Créer des connecteurs						*	
Créer et supprimer toutes les ressources, et lire et mettre à jour les propriétés standard dans Microsoft Cloud App Security						*	
Lire les touches BitLocker						*	
Gérer tous les aspects des méthodes d'autorisation						*	
Mettre à jour les propriétés de base des méthodes d'authentification pour les utilisateurs						*	
Mettre à jour les propriétés standard des méthodes d'authentification pour les utilisateurs						*	
Supprimer les méthodes d'authentification pour les utilisateurs						*	
Créer des méthodes d'authentification pour les utilisateurs						*	
Consulter toutes les propriétés sur les journaux d'audit, y compris les propriétés privilégiées						*	
Instancier des applications de galerie à partir de modèles d'application						*	
Lire les paramètres d'approvisionnement associés aux ressources de l'application						*	
Créer et supprimer des applications, et lire et mettre à jour toutes les propriétés						*	
Lire toutes les propriétés des demandes de consentement pour les applications inscrites auprès de Microsoft Entra ID						*	
Créer, supprimer et mettre à jour des unités administratives						*	
Gérer les stratégies de demande de consentement de l'administrateur dans Azure AD						*	

Autorisations	Admin. Skype Entreprise	Admin. de mots de passe	Admin. applications Office	Admin. licence	Admin. exchange	Admin. général	Admin. SharePoint
Gérer les révisions d'accès de toutes les ressources pouvant faire l'objet d'une révision dans Microsoft Entra ID						*	
Créer, puis supprimer les révisions d'accès; lire, puis mettre à jour toutes les propriétés des révisions d'accès dans Microsoft Entra ID						*	
Mettre à jour l'emplacement d'utilisation des utilisateurs				*			
Retraiter les attributions des licences aux utilisateurs				*			
Gérer les licences des utilisateurs				*			
Retraiter les attributions de licence pour les licences basées sur les groupes				*			
Attribuer des licences de produit à des groupes pour les licences basées sur les groupes				*			
Lire les propriétés standard sur les stratégies d'autorisation				*			

7 SOURCES

https://www.nucleustechnologies.com/blog/different-admin-roles-in-office-365/
https://learn.microsoft.com/fr-fr/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide
https://learn.microsoft.com/fr-ca/microsoftteams/using-admin-roles
https://www.avepoint.com/blog/fr/microsoft-teams-fr/roles-administrateur-dans-teams#:~:text=Ces%20administrateurs%20s'occupent%20d%C3%A9j%C3%A0,de%20travail%20et%20applications%20M365.
https://practical365.com/license-admin-role-and-other-improvements-in-azure-ad-administration/
https://config.office.com/officeSettings/unAuthorized
https://learn.microsoft.com/fr-ca/entra/id-governance/privileged-identity-management/pim-configure

8 RÉVISIONS

Date	Action	Auteur	Ver.
2024-02-09	Version courante	CESI de l'UQ	1.0