Microsoft logo white text versionMicrosoft logo white text versionMise en œuvre Pro Santé Connect avec Microsoft Entra ID

Zzz

Zzz

Guide de configuration de l’accès conditionnel à destination des établissements de santé

Version 0.4b - Septembre 2024

Cette page est intentionnellement laissée vide.

Avertissement

Les informations contenues dans le présent document, y compris les URL et autres références à des sites Internet, sont susceptibles d'être modifiées sans préavis. Sauf indication contraire, les exemples de sociétés, d'organisations, de produits, de noms de domaine, d'adresses électroniques, de logos, de personnes, de lieux et d'événements décrits dans le présent document sont fictifs et aucune association avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel n'est voulue ou ne doit être déduite. Il incombe à l'utilisateur de se conformer à toutes les lois applicables en matière de droits d'auteur.

A drawing of a face

Description automatically generated

Attribution 4.0 International (CC BY 4.0)

Microsoft et tous les contributeurs vous accordent une licence pour ce document sous la licence [Creative Commons Attribution 4.0 International Public License](https://creativecommons.org/licenses/by/4.0/legalcode), Cf. fichier [LICENSE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE), et vous accordent une licence pour tout code dans le référentiel sous la licence MIT, Cf. fichier [LICENSE-CODE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE).

Microsoft, Windows, Microsoft Azure et/ou d'autres produits et services Microsoft référencés dans le document peuvent être des marques commerciales ou des marques déposées de Microsoft aux États-Unis et/ou dans d'autres pays. La licence de ce document ne vous donne pas le droit d'utiliser les noms, logos ou marques de Microsoft. Les directives générales de Microsoft en matière de marques sont disponibles à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkID=254653>.

Des informations sur la protection de la vie privée sont disponibles à l'adresse suivante : <https://privacy.microsoft.com/fr-fr/>

Microsoft et tous les contributeurs se réservent tous les autres droits, que ce soit au titre de leurs droits d'auteur, de leurs brevets ou de leurs marques respectives, que ce soit de manière implicite, par préclusion ou de toute autre manière.

Contenu

[1 Introduction 5](#_Toc178077073)

[1.1 Présentation succincte de Pro Santé Connect (PSC) 5](#_Toc178077074)

[1.2 Accès conditionnel dans Microsoft Entra ID 5](#_Toc178077075)

[1.3 Objectif du guide 6](#_Toc178077076)

[1.4 Non-objectifs du guide 6](#_Toc178077077)

[1.5 Atelier compagnon du guide 7](#_Toc178077078)

[2 Planification des stratégies d’accès conditionnel Microsoft Entra ID 8](#_Toc178077079)

[2.1 Prise en compte des prérequis pour les stratégies d’accès conditionnel 8](#_Toc178077080)

[2.2 Recommandations d’ordre général 11](#_Toc178077081)

[2.3 Mise en œuvre d’une fondation sécurisée 12](#_Toc178077082)

[2.4 Adoption d’une convention de nommage des stratégies 13](#_Toc178077083)

[2.5 Considérations liées à la maintenance des stratégies 14](#_Toc178077084)

[3 Définition des stratégies d’accès conditionnel Microsoft Entra ID 15](#_Toc178077085)

[3.1 Considérations importantes relatives à la définition des stratégies d’accès conditionnel 15](#_Toc178077086)

[3.2 Documentation des stratégies d’accès conditionnel 19](#_Toc178077087)

[4 Configuration, test et déploiement des stratégies d’accès conditionnel Microsoft Entra ID 21](#_Toc178077088)

[4.1 Déploiement progressif des stratégies d’accès conditionnel 21](#_Toc178077089)

[4.2 Stratégies de modèles d’accès conditionnel pour une fondation sécurisée 23](#_Toc178077090)

[4.3 Stratégie d’accès conditionnel pour les conditions générales d’utilisation (CGU) de l’ES - Optionnel 24](#_Toc178077091)

[4.4 Stratégie d’accès conditionnel pour l’accès à PSC sans couture 28](#_Toc178077092)

[4.5 Autres stratégies 31](#_Toc178077093)

[4.6 Lister les stratégies d’accès conditionnel 31](#_Toc178077094)

[5 Pratiques recommandées 37](#_Toc178077095)

[5.1 Surveillance des journaux Microsoft Entra ID 37](#_Toc178077096)

[5.2 Validation régulière des comptes d’accès d’urgence 41](#_Toc178077097)

# Introduction

## Présentation succincte de Pro Santé Connect (PSC)

Pro Santé Connect (PSC) est le fédérateur d’identités des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS). Ce service socle est proposé par l’Agence du Numérique en Santé (ANS) en sa qualité d’autorité compétente.

Il leur offre une manière simple, sécurisée et unifiée de se connecter à tous leurs services numériques en santé, en pouvant passer de l’un à l’autre de manière particulièrement fluide.

Dans le cadre de cette expérimentation, le fédérateur d’identités PSC permet la délégation de l’authentification auprès de fournisseurs d’identités (FI) tiers. Une telle mise en œuvre et les capacités nouvelles ainsi proposées constituent un premier niveau de livrable du projet Pro Santé Connect sans couture.

Pour plus d’informations, nous invitons le lectorat à consulter le Portail Industriels de l’ANS :

* Délégation à un fournisseur d'identité local : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/delegation-un-fournisseur-d-identite-local> ;
* Liste des fournisseurs d’identités déjà supportés par Pro Santé Connect : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique-idp-externe>.

Dans le cadre de l’expérimentation avec Microsoft Entra ID, nous supposons dans ce document la configuration effective :

1. D’un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS.
2. D’une délégation de l’authentification Pro Santé Connect (PSC) auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID (anciennement connu sous le nom d’Azure AD).

Ces deux volets de la mise en œuvre constituent un prérequis au présent document.

Nous invitons le lectorat à se repoter si besoin au Guide de configuration des MIE et de la navigation sans couture à destination des établissements de santé respectivement au Guide d’intégration de Pro Santé Connect à destination des établissements de santé pour les éléments de configuration associés.

## Accès conditionnel dans Microsoft Entra ID

La délégation de l’authentification auprès de fournisseurs d’identités (FI) tiers, comme ici avec Microsoft Entra ID, impose le respect d’un ensemble d’exigences comme une force d’authentification requise pour accéder à PSC ou encore une durée d’activité maximale d’une session autorisée sur PSC.

L’accès conditionnel permet d’apporter une réponse pertinente pour assurer le respect de telles exigences. L’accès conditionnel dans Microsoft Entra ID est un moteur de stratégie intelligent qui aide les organisations à mieux contrôler les modalités d’accès des utilisateurs aux ressources d’une entreprise en :

* Appliquant des contrôles d’accès avec des stratégies adaptatives. Il s’agit de regrouper divers signaux en temps réel (contexte d’utilisateur, appareil, emplacement et niveau de risque de la session) afin de déterminer quand il convient d’autoriser l’accès, le bloquer ou le limiter, ou d’exiger des étapes de vérification supplémentaire ;
* Protégeant les données dans les applications et les services numériques. Il s’agit de surveiller et de contrôler les sessions, l’accès aux applications, aux services numériques et les données sensibles dans l’ensemble de l’organisation en temps réel sur la base du comportement des utilisateurs dans les applications et les services numériques, en local et dans le cloud ;
* Limitant l’accès des appareils vulnérables ou compromis. Il s’agit d’utiliser des stratégies d’accès conditionnel pour vérifier l’intégrité et la posture de sécurité des appareils inscrits et réserver l’accès aux ressources de votre entreprise aux seuls appareils intègres et approuvés. Les appareils Windows 10 ou ultérieur avec une jointure (hybride) à Microsoft Entra peuvent ainsi voir leur posture de sécurité vérifier.

Ces différentes modalités sont exprimées au travers de la définition de stratégies d’accès conditionnel.

## Objectif du guide

L’objectif de ce guide est d’expliciter la mise en œuvre des stratégies d’accès conditionnel attendues en termes de prérequis, de planification, de conception et de déploiement.

Dans le cadre de la conduite du POC Microsoft Entra ID dans un environnement de test, nous invitons le lectorat à se reporter directement aux sections suivantes pour répondre aux exigences de mise en œuvre exprimées par l’ANS :

* Section 4.2 Stratégie d’accès conditionnel pour les conditions générales d’utilisation de PSC ;
* Section 4.3 Stratégie d’accès conditionnel pour l’accès à PSC sans couture.

Dans les autres situations, ce guide aborde différentes considérations qu’il est important d’avoir à l’esprit ou de revoir en fonction du degré de maîtrise de l’accès conditionnel dans Microsoft Entra ID.

## Non-objectifs du guide

Comme indiqué ci-avant, la délégation de l’authentification PSC auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID est couverte dans le Guide d’intégration de Pro Santé Connect à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

De même, les MIE conformes pour les appareils Windows 10 (et ultérieur) sont couverts dans les guides suivants :

* Guide de configuration des cartes CPx à destination des établissements de santé ;
* Guide de configuration des clés de sécurité FIDO2 à destination des établissements de santé ;
* Guide de configuration des Microsoft Authenticator à destination des établissements de santé ;
* Guide de configuration de Windows Hello Entreprise à destination des établissements de santé.

Nous invitons le lectorat à s’y reporter.

Microsoft Entra ID propose par ailleurs des mécanismes permettant une navigation sans couture dès l’ouverture de session sur un appareil Windows pour l’accès à une application ou un service numérique déléguant l’authentification à PSC. Si les prérequis pour la mise en place de ces éléments pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS, ceux-ci sont néanmoins couverts dans ce même guide. Nous invitons le lectorat à s’y reporter le cas échéant.

Enfin, la mise en œuvre des MIE conformes avec les exigences établies par l’ANS ainsi que cette expérience navigation sans couture peuvent être étendues à d’autres types de dispositifs comme les services de terminaux Windows. Ceci requiert la mise en œuvre additionnelle de Microsoft Entra Private Access, un produit de type ZTNA (Zero Trust Network Access) centré sur l'identité. Cette dernière est couverte dans le Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

## Atelier compagnon du guide

Le présent guide est accompagné d’un support de présentation modulaire destiné à aider l’ES le cas échéant à conduire des ateliers afin de préciser la configuration de l’accès conditionnel dans le contexte spécifique de l’ES.

Ce support de présentation Atelier de configuration de l’accès conditionnel à destination des établissements de santé est disponible via le lien raccourci : <https://aka.ms/psc_ca2_entraid>.

Ce support propose un parcours complet pour :

* L’accès conditionnel « dans le détail » :

Une image contenant texte, Police, nombre, diagramme

Description générée automatiquement

* Les stratégies d’accès conditionnel pour une fondation sécurisée :

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

Nous invitons le lectorat à s’y reporter si besoin.

# Planification des stratégies d’accès conditionnel Microsoft Entra ID

Les sections suivantes vise à préciser et détailler autant que faire se peut le plan de haut niveau pour leur mise en œuvre de l’accès conditionnel dans le cadre de la délégation de l’authentification à Microsoft Entra ID pour Pro Santé Connect sans couture.

Si deux stratégies sont proposées pour la délégation de l’authentification à Microsoft Entra ID, nous recommandons d’inscrire ces dernières dans une réflexion plus large si telle n’est pas déjà la cas sur la sécurisation des applications et des ressources raccordées à Microsoft Entra ID et la mise en œuvre d’un accès conditionnel dans ce contexte.

La planification de tout déploiement d’accès conditionnel joue un rôle capital dans la réussite de la stratégie d’accès à mettre en œuvre que ce soit pour l’application PSC afin de respecter les exigences énoncées par l’ANS pour bénéficier de la fonction sans couture pour les PS ou plus largement pour l’ensemble des applications et des ressources de l’ES accessibles d’une session Entra ID.

Si les stratégies d’accès conditionnel offrent une grande flexibilité pour la configuration, cette flexibilité exige toutefois une planification minutieuse de la part de l’ES afin d’éviter des résultats indésirables.

Documentation Microsoft :

* Planifier un déploiement d’accès conditionnel: <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/plan-conditional-access>.

## Prise en compte des prérequis pour les stratégies d’accès conditionnel

### Eléments de configuration pour l’intégration de Pro Santé Connect (PSC)

Comme indiqué en introduction, i) la délégation de l’authentification Pro Santé Connect (PSC) auprès de Microsoft Entra ID ainsi que ii) le déploiement et à la configuration d’un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS, constituent des prérequis pour le présent guide.

### Licences Entra ID

Le locataire de l’ES doit disposer à minima de la licence Microsoft Entra ID P1 pour utiliser les fonctionnalités d’accès conditionnel et la force d’authentification.

L’abonnements Microsoft Entra ID P2 permet de bénéficier de Microsoft Entra Identity Protection pour détecter des risques basés sur l’identité et prendre des décisions en matière d’accès.

Remarque importante : Lorsque des licences requises pour l’accès conditionnel expirent, les stratégies ne sont pas automatiquement désactivées ou supprimées. Cela permet à l’ES de migrer en dehors des stratégies d’accès conditionnel sans changer soudainement leur posture de sécurité. Les stratégies restantes peuvent être consultées et supprimées, mais elles ne sont plus mises à jour.

Les paramètres de sécurité par défaut dans Microsoft Entra ID aident à protéger contre les attaques liées à l’identité et sont disponibles pour tous les clients, Cf. section 2.2 Mise en œuvre d’une fondation sécurisée.

Documentation Microsoft :

* Qu’est-ce que la protection de l'ID Microsoft Entra ? : <https://learn.microsoft.com/fr-fr/entra/id-protection/overview-identity-protection> ;
* Paramètres de sécurité par défaut dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults>.

### Privilèges d’administration

Par ailleurs, en termes de privilèges nécessaires pour procéder à la configuration, les administrateurs interagissant avec l’accès conditionnel doivent avoir une ou plusieurs des attributions de rôles suivantes en fonction des tâches qu’ils effectuent :

* Lire les stratégies et configurations d’accès conditionnel :
  + Lecteur de sécurité : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#security-reader> ;
  + Lecteur général : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#global-reader>.
* Créer ou modifier des stratégies d’accès conditionnel :
  + Administrateur de l’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#conditional-access-administrator> ;
  + Administrateur de la sécurité : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#security-administrator>.

Pour suivre le principe du moindre privilège de la Confiance Zéro (Zero Trust), nous recommandons d’utiliser Microsoft Entra Privileged Identity Management (PIM) pour activer juste-à-temps les attributions de rôles privilégiés.

Documentation Microsoft :

* Qu’est-ce que Privileged Identity Management ? : <https://learn.microsoft.com/fr-fr/entra/id-governance/privileged-identity-management/pim-configure>.

### Comptes d’accès d’urgence ou de secours

Il est important d’éviter de bloquer par inadvertance le locataire Entra ID de l’ES, sans pouvoir se connecter ou activer un autre compte d’utilisateur avec des privilèges d’administration.

Pour pallier à l’impact d’un défaut d’accès administratif, un minimum de deux comptes d’accès d’urgence doivent être crées dans le locataire Entra ID.

Les comptes d’accès d’urgence sont hautement privilégiés et ne sont pas affectés à des personnes spécifiques. Les comptes d’accès d’urgence sont limités à des cas d’urgence ou à des scénarios « de secours » où il est impossible d’utiliser des comptes d’administration normaux. Nous recommandons de fixer pour objectif la limitation de l’utilisation du compte d’urgence uniquement lorsque cela est strictement nécessaire.

Pour créer un compte d’accès d’urgence, procéder comme suit :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter en tant qu’Administrateur général.
3. Accéder à Utilisateurs > Tous les utilisateurs.
4. Sélectionner Nouvel utilisateur.
5. Sélectionner Créer un utilisateur.
   1. Donner un Nom d’utilisateur à votre compte, par exemple « *caurgence* ».
   2. Donner un Nom à votre compte, par exemple « Compte d’accès d’urgence ».
   3. Créer un mot de passe long et complexe pour le compte.
   4. Sous Rôles, attribuez le rôle Administrateur général.
   5. Dans Lieu d’utilisation, sélectionnez l’endroit souhaité.
6. Cliquer sur Créer.
7. Stocker les informations d’identification de compte en toute sécurité. Dans la liste des MIE conformes, une clés de sécurité FIDO2 pourra par exemple être utilisée pour Microsoft Entra ID.
8. Surveiller les journaux de connexion et d’audit, Cf. section 5.1 Gestion des journaux Microsoft Entra ID.
9. Valider régulièrement les comptes, Cf. section 5.1.4 Surveiller les comptes d’accès d’urgence.

Lors de la configuration de ces comptes d’accès d’urgence, les conditions suivantes doivent être remplies :

* Les comptes d’accès d’urgence ne doivent être associés à aucun utilisateur au sein de l’ES. Il convient de veiller à ce que de tels comptes d’accès d’urgence ne soient pas connectés à un matériel fourni par l’ES à un administrateur comme un appareil, un module de sécurité matériel, ou d’autres informations d’identification propres à cet administrateur. Cette précaution de sécurité couvre les cas où un administrateur n’est pas joignable alors que les informations d’identification doivent être fournies. Il est important de s’assurer que tous les appareils inscrits sont conservés dans un endroit sûr et connu, disposant de plusieurs moyens de communication avec Microsoft Entra ID.
* L’authentification forte doit être utilisée pour les comptes d’accès d’urgence mais il convient de s’assurer qu’elle n’utilise pas les mêmes méthodes d’authentification que les autres comptes d’administration. Par exemple quant aux MIE conformes, si un compte d’administrateur normal utilise l’application Microsoft Authenticator pour une authentification forte, une clé de sécurité FIDO2 peut être utilisée pour vos comptes d’urgence. Il est de plus nécessaire de tenir compte des dépendances entre les différentes méthodes d’authentification afin d’éviter d’ajouter des exigences externes dans le processus d’authentification.
* L’appareil ou les informations d’identification ne doivent pas expirer ou faire potentiellement l’objet d’un nettoyage automatisé en raison d’une utilisation insuffisante.
* Si l’ES utilise Microsoft Entra Privileged Identity Management (PIM), l’attribution de rôle d’administrateur général doit être permanente (et non éligible) pour les comptes d’accès d’urgence.

Documentation Microsoft :

* Gérer des comptes administrateur d’accès en cas d’urgence : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/security-emergency-access> ;
* Rôles intégrés Microsoft Entra – Administrateur général : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#global-administrator> ;
* Renforcer la résilience avec la gestion des informations d’identification dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/architecture/resilience-in-credentials>.

### Comptes de test

Des comptes de test sont par ailleurs nécessaires comme indiqué quant au socle technique minimal pour la mise en œuvre de PSC avec Microsoft Entra ID :

* Un utilisateur test (non administrateur) permet de vérifier que les stratégies envisagées fonctionnent comme prévu avant le déploiement vers des utilisateurs réels de l’ES comme des PS.
* Groupe auquel appartient l’utilisateur test. Si vous devez créer un groupe, consultez Créer un groupe et ajouter des membres dans Microsoft Entra ID.

Si un utilisateur et/ou un groupe de test doivent être créés, consulter le socle minimal : <https://github.com/microsoft/prosanteconnect/blob/main/PREREQUISITES.md>.

Cette même approche peut par la suite être étendue à des groupes d’utilisateurs pilotes en vue d’un déploiement progressif des stratégies d’accès conditionnel, Cf. section 4.1 Déploiement progressif des stratégies d’accès conditionnel.

## Recommandations d’ordre général

Sur la base de ce que nous savons sur l’utilisation de l’accès conditionnel et sur la prise en charge d’autres clients, voici quelques recommandations.

### Attribution de stratégies d’accès conditionnel à chaque application

Si c’est précisément l’un des objectifs de mise en œuvre pour l’application PSC et l’accès à Pro Santé Connect sans couture, il convient de s’assurer qu’au moins une stratégie d’accès conditionnel est appliquée à chaque application pour le locataire Microsoft Entra ID considéré.

Du point de vue de la sécurité, il est préférable de créer une stratégie qui englobe toutes les applications cloud, puis d’exclure les applications auxquelles il n’est pas souhaitable d’appliquer cette stratégie. Cette pratique vous évite d’avoir à mettre à jour les stratégies d’accès conditionnel chaque fois qu’une nouvelle application est intégrée.

L’application PSC constitue typiquement une exclusion dans la mesure où des stratégies d’accès conditionnel propre lui sont appliqués pour répondre aux exigences de l’ANS quant à la délégation de l’authentification à Microsoft Entra ID pour Pro Santé Connect sans couture.

### Réduction du nombre de stratégies d’accès conditionnel

En dehors des exigences propres qui s’appliquent à l’application PSC, créer une stratégie pour chaque application n’est pas efficace et entraîne une administration compliquée. L’accès conditionnel a une limite de 195 stratégies par locataire. Nous recommandons d’analyser les applications et de les regrouper par applications qui présentent les mêmes besoins en ressources pour les mêmes utilisateurs. Une stratégie unique peut alors être créer pour inclure toutes les applications auxquelles elle s’applique.

Les stratégies d’accès conditionnel sont contenues dans un fichier JSON et ce fichier est lié par une limite de taille que nous ne nous attendons pas à ce qu’une seule stratégie dépasse. Si une longue liste de GUID est utilisée dans une stratégie, cette limite peut être atteinte. Si tels est le cas, nous vous recommandons d’utiliser les alternatives suivantes :

* Utiliser des groupes ou des rôles pour inclure ou exclure des utilisateurs au lieu de répertorier chaque utilisateur individuellement ;
* Utiliser un filtre pour que les applications incluent ou excluent des applications au lieu de les spécifier individuellement.

Documentation Microsoft :

* Accès conditionnel : identités d’utilisateurs, de groupes et de charge de travail : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-users-groups> ;
* Accès conditionnel : filtre pour applications : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-filter-for-applications>.

## Mise en œuvre d’une fondation sécurisée

Pour faciliter et guider la mise en place de stratégies adaptées, Microsoft met à disposition un ensemble de modèles d’accès conditionnel conçus pour fournir une protection maximale alignée sur des stratégies couramment utilisées pour différents types de clients et d’emplacements.

Les 16 modèles de stratégie d’accès conditionnel ainsi proposés et organisés en 5 catégories (Fondation sécurisée, Confiance Zéro, travail à distance, Protection de l'administrateur et Menaces émergentes) fournissent une méthode pratique de déploiement de nouvelles stratégies alignées sur les recommandations de Microsoft.

Nous recommandons à un ES de considérer la mise en œuvre au minimum de tous les modèles de stratégies de Fondation sécurisée et recommandons un déploiement groupé.

Microsoft recommande en effet l’utilisation de ces 6 stratégies comme base pour toutes les organisations :

1. Exiger l’authentification multifacteur pour les administrateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa> ;
2. Sécurisation de l’inscription des informations de sécurité : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-registration> ;
3. Bloquer l’authentification héritée : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy> ;
4. Exiger l’authentification multifacteur pour tous les utilisateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-all-users-mfa> ;
5. Exiger une authentification multifacteur pour la gestion Azure : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-azure-management> ;
6. Exiger un appareil compatible ou avec jonction hybride à Microsoft Entra, ou l’authentification multifacteur pour tous les utilisateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-compliant-device> ;

Nous recommandons d’appliquer ces modèles pour le locataire Entra ID de l’ES sélectionné pour l’intégration avec PSC et destiner à être configuré pour respecter les exigences de sécurité du référentiel d’exigence PSC sans couture.

Cela autorise également d'améliorer ensuite graduellement la sécurité avec les principes de Confiance Zéro (Zero Trust) en tirant parti de stratégies supplémentaires telles que les stratégies basées sur les risques, les conditions de localisation, etc. qui contribuent à renforcer une posture de sécurité dans l'ensemble de l’ES.

Pour ces mêmes raisons, nous recommandons également d’appliquer ces modèles aux éventuels autres locataires de production de l’ES.

Comme indiqué dans la section 2.1.2 Licences Entra ID, ces locataires « principaux » doivent, au minimum, disposer d'une licence Entra ID P1 pour tous les utilisateurs afin que ces 6 stratégies de modèles d’accès conditionnel de fondation sécurisées ou des stratégies personnalisées » équivalentes puissent être mises en œuvre.

Nous recommandons également d’appliquer l'accès conditionnel pour des locataires « secondaires » (par exemple pour des environnements de test), mais compte tenu de l’exigence de licences Entra ID P1 pour chaque utilisateur au sein du locataire, ces locataires « secondaires » devraient, au minimum, activer les paramètres de sécurité par défaut pour tous les locataires.

Les paramètres de sécurité par défaut aident à protéger une organisation des attaques liées à l’identité, telles que la pulvérisation de mot de passe, le rejeu et le hameçonnage courants dans les environnements actuels. Ils correspondent dans la pratique aux 5 contrôles suivants :

1. Exiger que tous les utilisateurs s’inscrivent pour l’authentification multifacteur : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults#require-all-users-to-register-for-azure-ad-multifactor-authentication> ;
2. Exiger que les administrateurs effectuent l’authentification multifacteur : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults#require-administrators-to-do-multifactor-authentication> ;
3. Exiger que les utilisateurs effectuent l’authentification multifacteur si nécessaire : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults#require-users-to-do-multifactor-authentication-when-necessary> ;
4. Bloquer les protocoles d’authentification hérités : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults#block-legacy-authentication-protocols> ;
5. Protéger des activités privilégiées, telles que l’accès au Portail Azure : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults#protect-privileged-activities-like-access-to-the-azure-portal>.

Microsoft rend les paramètres de sécurité préconfigurés accessibles à tous, car nous savons que la gestion de la sécurité peut être difficile. Selon nos connaissances, plus de 99,9% de ces attaques liées à l’identité sont stoppées en utilisant l’authentification multifacteur et en bloquant l’authentification héritée. Notre but est de nous assurer que toutes les organisations ont activé au moins un niveau de sécurité de base, sans coût supplémentaire.

Ainsi, si le locataire a été créé le 22 octobre 2019 ou à une date ultérieure, il est possible que les paramètres de sécurité par défaut soient activés dans votre locataire. Pour protéger tous les utilisateurs, les paramètres de sécurité par défaut sont déployés sur tous les nouveaux locataires créés, de sorte qu'une telle activation ne serait nécessaire que pour les anciens locataires (créés avant le 22 octobre 2019) ou les locataires où le paramètre a été désactivé manuellement par l'administrateur dudit locataire pour des raisons autres que la mise en œuvre de l'accès conditionnel.

Documentation Microsoft :

* Sécuriser vos ressources avec des modèles de stratégie d’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation> ;
* Paramètres de sécurité par défaut dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/fundamentals/security-defaults>.

## Adoption d’une convention de nommage des stratégies

Une convention de nommage permet de rechercher des stratégies particulières et de comprendre leurs objectifs sans les ouvrir dans le Centre d’administration Microsoft Entra .

Nous recommandons de nommer les stratégies pour faire ressortir notamment :

* Un numéro de séquence ;
* L’application ou les applications cloud auxquelles elle s’applique ;
* La réponse ;
* Les groupes ou utilisateurs auxquels elle s’applique (qui) ;
* Le ou les types d’appareil auxquels elle s’applique ;
* Avec une description (le cas échéant).

Si l’ES ne dispose pas à date d’une convention en la matière, nous suggérons d’adopter le cas échéant une convention de ce type :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| <ACsn>- | <App>- | <Réponse>- | <Utilisateurs>- | <Appareils>- | <DescriptionOptionnelle> |

Par exemple, une stratégie qui exige une authentification multifacteur pour les PS accédant à l’application PSC depuis n’importe quel type d’appareils pour répondre aux exigences de l’ANS peut être formulée de la façon suivante :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC02- | ProSantéConnect- | Session4hAvecMFA- | Global- | ToutePlateforme- | PourANS |

Un nom descriptif contribue à conserver une vue globale de l’implémentation par l’ES de l’accès conditionnel dans Microsoft Entra ID. Le numéro de séquence est utile si une référence à une stratégie donnée doit être faite dans le cadre d’un échange. Par exemple, il est possible de faire référence à cette stratégie AC02-ProSantéConnect pour résoudre un problème.

Dans la définition du POC envisagé, et indépendamment de toute convention de nommage en place au niveau de l’ES, les préfixes AC01-ProSantéConnect et AC02-ProSantéConnect devront être utilisés par l’ES pour nommer les deux stratégies d’accès conditionnel demandées dans le cadre de la délégation de l’authentification à Microsoft Entra ID. Ces préfixes permettront de s’assurer simplement si ces deux stratégies existent, si elles sont activées, si elles sont conformes dans la définition de leurs différentes composantes, si elles couvrent bien à ce titre l’application PSC, etc.

## Considérations liées à la maintenance des stratégies

Si l’accès conditionnel dans Microsoft Entra ID permet une large personnalisation au contexte spécifique de l’ES, la gestion et la maintenance de stratégies d’accès conditionnel complexes peut nécessiter du temps supplémentaire et des ressources dédiées.

Des règles mal configurées peuvent par exemple déclencher des restrictions ou accorder un accès dans des situations inappropriées d’où la nécessité de notamment surveiller les activités de connexion et les stratégies d’accès conditionnel appliquées dans ce contexte, Cf. sections 5.1.3 Afficher les stratégies d’accès conditionnel appliquées, 5.1.4 Surveiller les autres activités et 5.1.5 Surveiller les comptes d’accès d’urgence.

# Définition des stratégies d’accès conditionnel Microsoft Entra ID

Les sections suivantes décrivent la configuration des stratégies d'accès conditionnel à appliquer dans le cadre de la délégation de l’authentification à Microsoft Entra ID par Pro Santé Connect (PSC).

Remarque préliminaire importante : Les risques qui pèsent sur les systèmes et les données informatiques sont en constante évolution, et les contre-mesures pour y faire face continueront d'évoluer au fil du temps. Cela a deux conséquences. La première est qu’il est impératif de réévaluer régulièrement la catégorie de risque pour l’application PSC et l’accès à Pro Santé Connect sans couture afin de s’assurer que l'application est protégée de manière adéquate. Cette considération s'applique également à toute autre application ou ressources intégrées au locataire Entra ID considéré. Deuxièmement, les conditions et les contrôles que les stratégies d'accès conditionnel appliquent doivent faire régulièrement l’objet d’une à jour afin de bénéficier des évolutions apportés à Microsoft Entra ID au fur et à mesure que de nouvelles fonctionnalités sont introduites.

## Considérations importantes relatives à la définition des stratégies d’accès conditionnel

### Exclusion de comptes utilisateurs

Exclure au moins un compte de l’authentification multifacteur

Afin de réduire le risque d’attaques résultant d’un mot de passe compromis, Microsoft Entra recommande de généraliser l’authentification multifacteur pour tous les utilisateurs au-delà des exigences propres qui s’appliquent dans le contexte de ce document aux personnes devant accéder à la plateforme PSC. Ceci comprend les administrateurs et tous les autres utilisateurs en dehors des PS dont un compte compromis aurait un impact important.

Cependant, au moins un des comptes d’accès d’urgence ne doit pas avoir le même mécanisme d’authentification multifacteur (MFA) que les autres comptes non dédiés à l’accès d’urgence. Cela inclut les solutions relatives aux différents MIE conformes.

Si une stratégie d’accès conditionnel impose l’authentification multifacteur à chaque administrateur pour Microsoft Entra ID et d’autres applications connectées comme nous le recommandons pour une fondation de sécurité, Cf. section 2.2 Mise en œuvre d’une fondation sécurisée, il est nécessaire de soustraire les comptes d’accès d’urgence de cette exigence et configurer un autre mécanisme à la place. Il est en outre nécessaire de s’assurer que les comptes ne font pas l’objet d’une stratégie d’authentification multifacteur par utilisateur.

Exclure au moins un compte des stratégies d’accès conditionnel

En cas d’urgence, une stratégie ne doit pas risquer d’empêcher un accès pour résoudre un problème. De fait, au moins un compte d’accès d’urgence doit être exclu de TOUTES les stratégies d’accès conditionnel.

### Définition des emplacements nommés

Une stratégie d’accès conditionnel est à la base constituée d’une instruction de type « if-then » combinant des signaux, qui permet de prendre des décisions et d’appliquer les stratégies de l’ES. L’un de ces signaux est la localisation.

Lors de la définition des emplacements à utiliser dans les stratégies d'accès conditionnel, nous recommandons de définir des emplacements nommés.

Ces derniers peuvent inclure les plages réseau du ou des sites de l’ES ou du VPN, ou les plages qu’il est souhaitable de bloquer pour des raisons qui appartiennent à l’ES. Par exemple, les sous-réseaux internes (et adresses IP de confiance) de l’ES représentent des lieux et des réseaux qui peuvent déjà faire l'objet de restrictions d'accès physiques et/ou d'autres contrôles, tels que la gestion des systèmes informatiques, l'authentification au niveau du réseau et la détection des intrusions. Ces emplacements sont plus sûrs et l'application de conditions d'accès peut être le cas échéant assouplie.

Les emplacements nommés sont définis par des plages d’adresses IPv4 et IPv6 ou par pays/région.

Le tableau suivant peut aider à définir de tels emplacements :

|  |  |  |
| --- | --- | --- |
| Emplacements nommées | Plage IP | De confiance |
|  |  |  |
|  |  |  |
|  |  |  |

Documentation Microsoft :

* Utilisation de la condition d’emplacement dans une stratégie d’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/location-condition>.

### Exigence d’une force d’authentification donnée pour PSC sans couture

La force d'authentification est un contrôle d'accès conditionnel qui permet aux administrateurs de spécifier quelle combinaison de méthodes d'authentification peut être utilisée pour accéder à une ressource. Cela peut varier en fonction du niveau de sensibilité de la ressource et du risque d'utilisateur, de l'emplacement, etc.

Pour spécifier une force d'authentification afin d'accéder à une ressource ou à une application, les administrateurs doivent créer une stratégie d'accès conditionnel avec le contrôle Exiger une force d'authentification.

Ils peuvent choisir parmi trois forces d'authentification intégrées ou créer une force d'authentification personnalisée.

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter.
3. Aller sur Protection > Méthodes d’authentifications > Points forts d’authentification. 3 forces d’authentification sont configurées par défaut :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Afin de créer des forces d’authentification personnalisées :

1. Cliquer sur Nouvelle force d’authentification.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

1. Donner le nom FA01-ProSantéConnect pour la nouvelle force d’authentification.

Au même titre que l’utilisation de préfixes est imposé pour les stratégies d’accès conditionnel relative à Pro Santé Connect sont imposés indépendamment d’une convention de nommage en place, il est demandé ici à l’ES de respecter ce nom pour les mêmes raisons évoquées.

1. Fournir une description si souhaité.
2. Sélectionner les méthodes disponibles autorisées suivantes :
   1. Sous MFA anti-hameçonnage, cocher les méthodes Windows Hello Entreprise, Clé de sécurité FIDO2 et Authentification basée sur un certificat (multifacteur).
   2. Sous Authentification multifacteur sans mot de passe, cocher la méthode Microsoft Authenticator (connexion par téléphone).

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

La prise en charge des moyens d’identification électronique (MIE) conformes est décrite dans les guides suivants :

* + Guide de configuration des cartes CPx à destination des établissements de santé ;
  + Guide de configuration des clés de sécurité FIDO2 à destination des établissements de santé ;
  + Guide de configuration des Microsoft Authenticator à destination des établissements de santé ;
  + Guide de configuration de Windows Hello Entreprise à destination des établissements de santé..

Nous invitons le lectorat à s’y reporter.

1. Cliquer sur Suivant et passez en revue la configuration.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Cliquer sur Créer.

Une image contenant texte, Police, ligne, nombre

Description générée automatiquement

Une fois la force d'authentification ainsi créée, une stratégie d'accès conditionnel doit être créer pour exiger cette force d'authentification lors de l’accès à PSC sans couture, Cf. section 4.3 Stratégie d’accès conditionnel pour l’accès à PSC sans couture.

Remarque : Les stratégies d'accès conditionnel sont uniquement évaluées après l'authentification initiale. Par conséquent, la force d'authentification ne restreint pas la méthode d’authentification utilisée lors de la connexion d'un utilisateur à son locataire Entra ID.

Documentation Microsoft :

* Force d’authentification de l’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-authentication-strengths>.

### Fréquence de connexion pour PSC sans couture

La fréquence de connexion, aussi connu sous le nom de réauthentification périodique, des utilisateurs définit la période avant qu'un utilisateur ne soit invité à se reconnecter lorsqu'il tente d'accéder à une ressource. Par défaut, Microsoft Entra ID demande une réauthentification tous les 90 jours.

Cette fréquence doit donc être ajustée pour répondre aux exigences spécifiques de l’ANS. La période de temps maximum pour PSC est de 4 heures.

Documentation Microsoft :

* Configurer la gestion de session d’authentification avec l’accès conditionnel :  
  <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency>

## Documentation des stratégies d’accès conditionnel

Le tableau suivant peut aider à la documentation des différentes stratégies d’accès conditionnel à mettre en œuvre dans le cadre de la délégation de l’authentification à Microsoft Entra ID pour PSC sans couture ou plus largement pour la sécurisation des différentes applications et ressources du ou des locataires de l’ES :

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Accès conditionnel : Utilisateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-users-groups> ;
* Accès conditionnel : Ressources cibles : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-cloud-apps> ;
* Accès conditionnel : Conditions : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-conditions> ;
* Accès conditionnel : Octroyer : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-grant> ;
* Accès conditionnel : Session : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-session>.

# Configuration, test et déploiement des stratégies d’accès conditionnel Microsoft Entra ID

Sur la base de la définition précédente, les sections suivantes décrivent les modalités opérationnelles de configuration, de test et de déploiement des stratégies d'accès conditionnel à appliquer dans le cadre de la délégation de l’authentification à Microsoft Entra ID par Pro Santé Connect (PSC).

## Déploiement progressif des stratégies d’accès conditionnel

L'implémentation de stratégies d'accès conditionnel peut perturber les activités de l'ES. Il est nécessaire de faire preuve de prudence lors de la configuration, du test et du déploiement de chaque stratégie dans un locataire Entra ID de production, comme cela peut avoir une incidence négative sur l'accès aux applications de production.

Il est en particulier important que les stratégies appliquées soient testées de manière approfondie et que les PS et autres utilisateurs finaux soient informés des modifications à venir avant que les stratégies ne soient activées.

Le test des stratégies d'accès conditionnel nécessite deux activités principales :

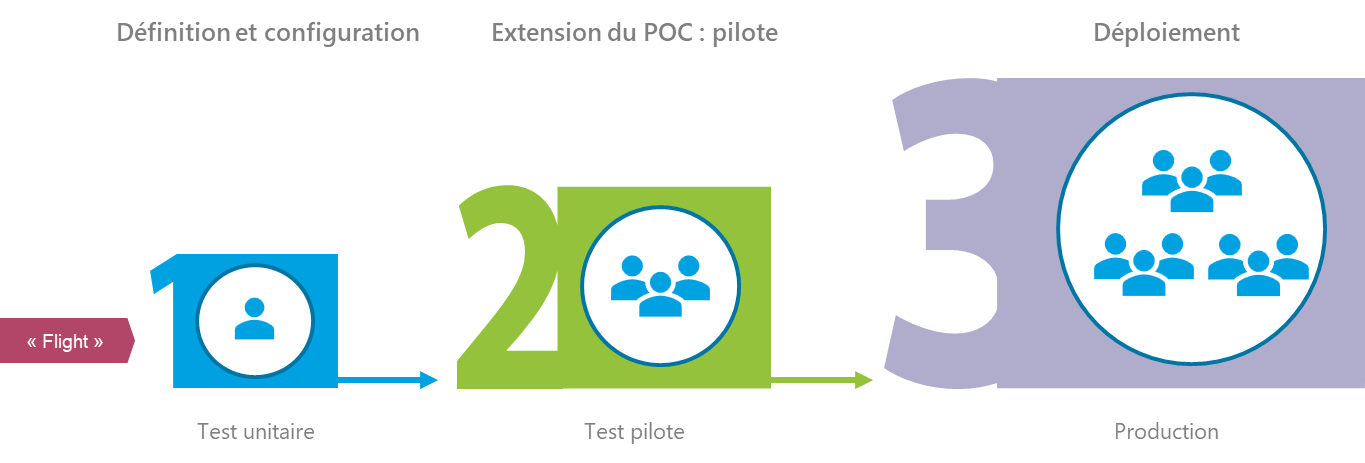
1. Des tests unitaires, pour déterminer si des conditions ou des contrôles spécifiques sont déclenchés, appliqués et validés. Le mode rapport uniquement peut s’avérer utile à ce titre dans un premier temps avant de passer à l’activation effective des stratégies considérées ;
2. La validation de l'expérience utilisateur finale, pour s'assurer de l’utilisabilité des applications comme en particulier ici l’application PSC.

De même, pour faciliter ces tests et la mise en œuvre de stratégies d’accès conditionnel, il est recommandé de limiter la portée des stratégies d’abord à des utilisateurs de test spécifiques pour effectuer des tests unitaires, puis à un groupe d’utilisateurs pilote pour effectuer des tests fonctionnels, Cf. section 2.1.5 Comptes de test.

Une fois ces tests concluants, vous pouvez alors supprimer cette restriction.

À cette fin, il est recommandé d'utiliser une approche de mise en œuvre progressive qui utilise l'ensemble d'activités suivantes pour les stratégies envisagées qu’il s’agisse des deux stratégies ciblant l’application PSC\_BAS ou celles recommandées quant à la mise en œuvre d’une fondation sécurisée :

1. Configurer les stratégies envisagés en mode rapport uniquement pour l'évaluation du risque ;
2. Attribuer ces stratégies à une application de test et effectuer des tests unitaires. Ceci est de facto le cas pour les deux stratégies propres à l’application PSC\_BAS et à définir pour les stratégies de modèles d’accès conditionnel suggérées, Cf. section 2.3 Mise en œuvre d’une fondation sécurisée, pour lesquelles pour mémoire l’applications PSC\_BAS doit être spécifiquement exclue ;
3. Attribuer ces stratégies à des utilisateurs de test, puis à un groupe d’utilisateurs de test pour passer enfin à un groupe pilote plus large d'utilisateurs ;
4. Déployer ensuite par étapes en augmentant le nombre d'utilisateurs ciblés par les stratégies.



Le configuration et le déploiement de stratégies d'accès conditionnel implique l'utilisation du Centre d’administration Microsoft Entra  pour définir une stratégie, puis limiter la portée de la stratégie à des utilisateurs de test spécifiques et à une ou plusieurs applications dédiées comme l’application PSC\_BAS afin que les conditions puissent être testées et vérifiées.

L’accès conditionnel se trouve sous Protection > Accès conditionnel et permet de configurer les stratégies attendues et de les tester unitairement pour vérifier que les différents contrôles et conditions ainsi que les filtres éventuels sont correctement structurés pour atteindre la cible de déploiement souhaitée.

Une image contenant texte, logiciel, nombre, Police

Description générée automatiquement

* La page Vue d’ensemble fournit un résumé de l’état de la stratégie, des utilisateurs, des appareils et des applications, ainsi que des alertes générales et de sécurité accompagnées de suggestions.
* La page Couverture  offre un résumé des applications avec et sans couverture de stratégie d’accès conditionnel au cours des sept derniers jours.
* La page Surveillance permet aux administrateurs d’afficher un graphique des connexions qui peuvent être filtrées afin de voir les lacunes potentielles dans la couverture de la stratégie.

Les stratégies d’accès conditionnel dans la page Stratégies peuvent être filtrées par les administrateurs en fonction d’éléments tels que la ressource cible comme ici l’application PSC pour l’accès à Pro Santé Connect Sans couture, l’acteur, la condition, le contrôle appliqué, l’état ou la date. Cette capacité de filtrage permet de rechercher rapidement des stratégies spécifiques en fonction de leur configuration.

## Stratégies de modèles d’accès conditionnel pour une fondation sécurisée

Comme abordé à la section 2.3 Mise en œuvre d’une fondation sécurisée, nous recommandons l’utilisation des 6 stratégies proposés par les modèles d’accès conditionnel pour la catégorie Fondation sécurisée.

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/> et se connecter en tant qu’Administrateur général.
2. Obtenir ces modèles depuis Protection > Accès conditionnel > Créer une nouvelle stratégie à partir de modèles.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Sélectionner le modèle d’accès conditionnel à instancier pour créer la stratégie et cliquer sur Vérifier + créer.
   1. Sous Informations de base, sélectionner l’Etat de la stratégie souhaité.

Par défaut, la stratégie est créée en mode Rapport uniquement. Nous recommandons à l’ES de tester et de superviser l’utilisation, pour s’assurer du résultat escompté, avant d’activer la stratégie.

* 1. Sous Affectations, la stratégie de modèle d’accès conditionnel exclu uniquement l’utilisateur qui crée la stratégie à partir du modèle. Si l’ES doit exclure d’autres comptes, modifier la stratégie une fois créée.

1. Cliquer sur Créer.

Pour modifier les exclusions, procéder comme suit :

1. Aller sur la vue Protection > Accès conditionnel > Stratégies.
2. Sélectionner la stratégie nouvellement créée pour ouvrir l’éditeur.
3. Modifier les utilisateurs et groupes exclus afin de sélectionner les comptes à exclure.
4. Exclure l’application PSC\_BAS de la cible applicative.

L’ES peuvent sélectionner des modèles de stratégie individuels et :

* Afficher un résumé des paramètres de la stratégie.
* Les modifier pour les personnaliser en fonction des besoins de l’ES.
* Exporter le cas échéant la définition JSON pour une utilisation dans des workflows programmatiques. Ces définitions JSON peuvent être modifiées, puis importées dans la page principale des stratégies d’accès conditionnel à l’aide de l’option Télécharger un fichier de stratégie.

Documentation Microsoft :

* Sécuriser vos ressources avec des modèles de stratégie d’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation> ;
* Qu’est-ce que le mode rapport uniquement de l’accès conditionnel ? : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/concept-conditional-access-report-only>.

## Stratégie d’accès conditionnel pour les conditions générales d’utilisation (CGU) de l’ES - Optionnel

L’ES peut de façon optionnelle exprimer des conditions générales d’utilisation (CGU) propres à l’utilisation de PSC sans couture. De telles conditions devront être préalablement accepter par les utilisateurs concernés de l’ES avant de pouvoir bénéficier de PSC sans couture.

La mise en place de ces CGU dans ce contexte suppose la configuration d’une stratégie d’accès conditionnel. Ceci implique dans un premier temps de créer dans le locataire Entra ID lesdites conditions d’utilisation à prendre en compte puis de les intégrer à une stratégie d’accès conditionnel.

C’est l’objet des deux sections suivantes.

### Expression de conditions générales d’utilisation (CGU) de l’ES

Une fois les conditions générales d’utilisation (CGU) définies par l’ES, procéder comme suit :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Dans Protections > Accès conditionnel, cliquer sur Conditions d’utilisation.
3. Dans le menu supérieur, cliquer sur Nouvelles conditions.
4. Sous Nom, saisir par exemple « CGU-ProSantéConnect ».
5. Sous Document Conditions d’utilisation :
   1. Charger les conditions générales d’utilisation (CGU) ainsi définies sous forme de fichier PDF, par exemple pour les besoins de cette illustration CGU Pro Santé Connect sans cuture.pdf.
   2. Pour Sélectionner la langue par défaut, choisir Français dans la liste déroulante.
   3. Sous Nom d’affichage, spécifier par exemple « *Conditions générales d’utilisation Pro Santé Connect sans couture*».
6. Sous Demander aux utilisateurs d’étendre les conditions d’utilisation, sélectionner Activé.
7. Sous Accès conditionnel, pour l’option Appliquer avec des modèles de stratégie d’accès conditionnel, sélectionner Créer une stratégie d’accès conditionnel plus tard.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

1. Cliquer sur Créer.

Une image contenant texte, Police, ligne, capture d’écran

Description générée automatiquement

### Création de la stratégie d’accès conditionnel pour les CGU

Sur la base de la convention de nommage, Cf. section 2.4 Adoption d’une convention de nommage des stratégies, nous suggérons de nommer de cette stratégie AC01-ProSantéConnect-AcceptationCGU-Global-ToutePlateforme-PourANS.

Ce nom est à aligner le cas échéant avec une convention de nommage de l’ES au préfixe près AC02-ProSantéConnect qui est imposé par l’ANS afin de simplifier une vérification du respect des exigences exprimées pour l’accès conditionnel. Les CGU constituent une fonctionnelle optionnelle rentrant dans ce cadre.

Procéder comme suit :

1. Dans le panneau à droite du Centre d’administration Microsoft Entra
2. Aller sur Applications > Applications d’entreprise et cliquer sur l’application PSC. Par exemple, PSC\_BAS pour l’environnement Bac à sable.
3. Dans Sécurité > Accès conditionnel, cliquer sur Nouvelle stratégie dans le menu supérieur.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

1. Indiquer comme nom par exemple « *AC01-ProSantéConnect-AcceptationCGU-Global-ToutePlateforme-PourANS* ».
2. Spécifier les différentes composantes de la stratégie d’accès conformément à sa définition pour l'environnement cible.
   1. Sous Utilisateurs, cliquer sur 0 utilisateurs et groupes sélectionnés et sélectionner Inclure.
      * Dans le cadre du POC, indiquer Sélectionner des utilisateurs et des groupes, puis cocher Utilisateurs et groupes. Sélectionner le groupe de test et/ou les utilisateurs de tests concernés dans le cadre du déploiement progressif de la stratégie, Cf. section 2.1.5 Comptes de test. Cliquer enfin sur Sélectionner pour valider.
      * A termes, indiquer Tous les utilisateurs.
   2. Sous Contrôles d’accès > Octroyer, cliquer sur 0 contrôles sélectionnés, sélectionner Accorder l’accès et sélectionnez les conditions d’utilisation précédemment créées : CGU-ProSantéConnect.

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

* 1. Cliquer sur Sélectionner.

1. Sous Activer une stratégie, sélectionner Activé.

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

1. Cliquer sur Créer.

## Stratégie d’accès conditionnel pour l’accès à PSC sans couture

Sur la base de la convention de nommage, Cf. section 2.4 Adoption d’une convention de nommage des stratégies, nous suggérons de nommer de cette stratégie AC02-ProSantéConnect-Session4hAvecMFA-Global-ToutePlateforme-PourANS.

Ce nom est à aligner le cas échéant avec une convention de nommage de l’ES au préfixe près AC02-ProSantéConnect qui est imposé par l’ANS afin de simplifier une vérification du respect des exigences exprimées pour l’accès conditionnel.

Pour définir cette stratégie d’accès conditionnel, procéder comme suit :

1. Depuis la vue précédente Accès conditionnel relative à l’application PSC dans le Centre d’administration Microsoft Entra, cliquer à nouveau sur Nouvelle stratégie.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Indiquer comme nom par exemple « *AC02-ProSantéConnect-Session4hAvecMFA-Global-ToutePlateforme-PourANS* ».
2. Spécifier les différentes composantes de la stratégie d’accès conformément à sa définition pour l'environnement cible.
3. Sous Utilisateurs, cliquer sur 0 utilisateurs et groupes sélectionnés et sélectionner Inclure.
   * + Dans le cadre du POC, indiquer Sélectionner des utilisateurs et des groupes, puis cocher Utilisateurs et groupes. Sélectionner le groupe de test et/ou les utilisateurs de tests concernés dans le cadre du déploiement progressif de la stratégie, Cf. section 2.1.5 Comptes de test. Cliquer enfin sur Sélectionner pour valider.
     + A termes, indiquer Tous les utilisateurs.
4. Sous Contrôles d'accès > Octroyer, cliquer sur 0 contrôles sélectionnés, sélectionner Accorder l’accès :
   * 1. Sélectionner Exiger la force d’authentification. Dans la liste déroulante, sélectionner FA-ProSantéConnect, Cf. section 3.1.3 Exigence d’une force d’authentification donnée pour PSC sans couture.

Une image contenant texte, capture d’écran, Police, Site web

Description générée automatiquement

Remarque : Si la force d’authentification n’apparaît pas, il faut attendre quelques minutes que l’actualisation.

* + 1. Cliquer sur Sélectionner.

1. Sous Contrôles d'accès > Session, cliquer sur 0 contrôles sélectionnés et sélectionner Fréquence de connexion et sélectionner Réauthentification périodique. PSC sans couture impose une réauthentification périodique – Le maximum est de 4 heures.
2. Indiquer 4 dans le premier champ.
3. Dans Sélectionner les unités, choisir Heures.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Cliquer sur Sélectionner.
2. Sous Activer une stratégie, sélectionner Activé.

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

1. Cliquer sur Créer.

A ce stade, les deux stratégies d’accès conditionnel attendues pour Pro Santé Connect sans couture sont en place dans le locataire Entra ID.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

## Autres stratégies

Des stratégies additionnelles sont susceptibles de s’ajouter à l’exigence précédente à l’avenir.

## Lister les stratégies d’accès conditionnel

Compte tenu des différentes stratégies d’accès conditionnelles à définir qui s’appliquent à l’application PSC de façon à répondre aux attendus de l’ANS, il peut s’avérer intéressant de pouvoir en lister les éléments de configuration et d’en exporter les détails sous la forme d’un fichier au format JSON.

Le script PowerShell *ListerStrategiesAccesPSC.ps1* suivant permet d’offrir un premier niveau de réponse. A cette fin, et à titre d’illustration, ce dernier repose sur le module Microsoft Graph PowerShell (Microsoft.Graph.Identity.SignIns). Il utilise pour cela l’usage du cmdlet [Get-MgIdentityConditionalAccessPolicy](https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/get-mgidentityconditionalaccesspolicy?view=graph-powershell-1.0) qui fait partie de ce module.

Remarque importante : Les modules Azure AD, Azure AD Preview et MS Online PowerShell sont obsolètes depuis le 30 mars 2024 dernier. Une assistance n’est offerte depuis que pour les correctifs de sécurité critiques. Ces modules continueront à fonctionner jusqu'au 30 mars 2025. En conséquence, il convient de ne plus utiliser [Get-AzureADMSConditionalAccessPolicy](https://learn.microsoft.com/fr-fr/powershell/module/azuread/migrate/get-azureadmsconditionalaccesspolicy?view=azureadps-2.0).

Documentation Microsoft :

* New Blog | Important update: Deprecation of Azure AD PowerShell and MSOnline PowerShell modules - Microsoft Community Hub : <https://techcommunity.microsoft.com/t5/microsoft-entra/new-blog-important-update-deprecation-of-azure-ad-powershell-and/m-p/4102339>;
* Important update: Deprecation of Azure AD PowerShell and MSOnline PowerShell modules - Microsoft Community Hub : <https://techcommunity.microsoft.com/t5/microsoft-entra-blog/important-update-deprecation-of-azure-ad-powershell-and-msonline/ba-p/4094536>.

# Description: List all the policies that both apply to the PSC application and are active, and

# optionnaly export them as a JSON output to a file

# Param Chemin: The export filepath

Param (

[string][Parameter(Mandatory=$true)]$Nom,

[string]$Chemin

)

# Get the PSC application name

if (-not $Nom) {

Write-Output 'Le paramètre Nom est obligatoire'

exit

}

# Connect to Microsoft Graph

Connect-MgGraph -Scopes "Application.Read.All,Policy.Read.All"

# Get the service principal for the PSC application

$servicePrincipal = Get-MgServicePrincipal -Filter "DisplayName eq '$Nom'"

# Get the application ID

$appId = $servicePrincipal.appId

# Get all conditional access policies

$policies = Get-MgIdentityConditionalAccessPolicy

# Filter policies that apply to the specified application and are active

$appPolicies = $policies | Where-Object {

$\_.Conditions.Applications.IncludeApplications -contains $appId -and $\_.State -eq "enabled"

}

# Create an array to store policy details

$policyDetails = @()

# Loop through each policy and extract details

foreach ($policy in $appPolicies) {

$details = [PSCustomObject]@{

PolicyName = $policy.DisplayName

State = $policy.State

CreatedDateTime = $policy.CreatedDateTime

ModifiedDateTime = $policy.ModifiedDateTime

Description = $policy.Description

Conditions = $policy.Conditions

GrantControls = $policy.GrantControls

SessionControls = $policy.SessionControls

}

$policyDetails += $details

}

# Display the policy details in a table format

$policyDetails | Format-Table -AutoSize

# Retrieve the output file path

if (-not $Chemin) {

exit

}

$outputFilePath = $Chemin

# Convert the policy details to JSON

$jsonOutput = $policyDetails | ConvertTo-Json -Depth 3

# Export the JSON output to a file

$jsonOutput | Out-File -FilePath $outputFilePath -Encoding utf8

# Display a message indicating the export is complete

Write-Output "Le détails des stratégies d'accès conditionnel a été exporté vers $outputFilePath"

Pour exécuter ce script et vérifier les stratégies d’accès conditionnel de l’application PSC, procéder comme suit :

1. Ouvrir un invite de commande PowerShell. Rechercher “*PowerShell*” dans le menu Démarrer et ouvrir Windows PowerShell ou Windows PowerShell ISE avec des privilèges d’administration, c.à.d. en tant qu’administrateur. Confirmer dans le dialogue qui s’ouvre en cliquant sur Oui.
2. Installer le module Microsoft Graph PowerShell si ce n’est pas déjà fait avec la commande :

PS C:\> Install-Module -Name Microsoft.Graph

Lorsque le message suivant s’affiche :

Vous installez les modules à partir d'un référentiel non approuvé. Si vous approuvez ce référentiel, modifiez sa valeur InstallationPolicy en exécutant l'applet de commande Set-PSRepository. Voulez-vous vraiment installer les modules à partir de PSGallery ?

[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « N ») :

Taper T.

1. Depuis l’invite de commande, naviguer jusqu’au répertoire où se trouve le script *ListerStrategiesAccesPSC.ps1* avec la commande cd.
2. Comme ce script n’est pas signé, il est nécessaire de modifier la stratégie d’exécution de script en place qui permet de se prémunir contre les scripts jugés non fiables.
3. Exécuter la commande :

PS C:\> Set-ExecutionPolicy -ExecutionPolicy Unrestricted

Pour plus d’information, nous invitons le lectorat à consulter l’article suivant : A propos des stratégies d’exécution - PowerShell (<https://learn.microsoft.com/fr-fr/powershell/module/microsoft.powershell.core/about/about_execution_policies>).

1. Le dialogue Modification de la stratégie d’exécution s’ouvre  Cliquer sur Oui pour confirmer l’opération.
2. Exécuter le script en passant en argument :
   * Le nom donné à l’application PSC dans le locataire de l’ES. Par exemple, PSC\_BAS pour l’environnement Bac à sable dans notre illustration ;
   * Le chemin de sortie approprié pour le fichier JSON.

PS C:\> .\ListerStrategiesAccesPSC.ps1 -Nom "PSC\_BAS" -Chemin "C:\Temp\PSC\_CA.json"

1. Lors de la connexion à Microsoft Graph avec le cmdlet Connect-MgGraph, une fenêtre de connexion s’ouvre dans le navigateur par défaut afin de préciser les informations d’identification pour le locataire Entra ID de l’ES.

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

1. Si le module Microsoft Graph PowerShell ne dispose pas (encore) des permissions nécessaire, un dialogue additionnel pour recueillir le consentement s’ouvre :

Une image contenant texte, capture d’écran, Page web, logiciel

Description générée automatiquement

Cliquer sur Accept. Le message suivant s’affiche alors dans le navigateur :

Authentication complete. You can return to the application. Feel free to close this browser tab.

1. L’onglet du navigateur peut être fermé à ce stade comme indiqué.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

PS C:>.\ListerStrategiesAccesPSC.ps1 -Nom "PSC\_BAS" -Chemin "C:\Temp\PSC\_CA.json"

Welcome to Microsoft Graph!

PolicyName State CreatedDateTime ModifiedDateTime Description Conditions

---------- ----- --------------- ---------------- ----------- ----------

AC02-ProSantéConnect-Session4hAvecMFA-Global-ToutePlateforme-PourANS enabled 23/09/2024 08:57:01 Microsoft.Graph.PowerShell....

Le détails des stratégies d'accès conditionnel a été exporté vers C:\Temp\PSC\_CA.json

A ce stade, les détails des stratégies d’accès conditionnel définies pour l’application PSC sont exportés dans un fichier JSON à l’emplacement spécifié.

Par défaut, le script inclut les propriétés suivantes dans l’export JSON :

1. DisplayName : Le nom affiché de la stratégie.
2. State : L’état de la stratégie (enabled, disabled).
3. CreatedDateTime : La date et l’heure de création de la stratégie.
4. ModifiedDateTime : La date et l’heure de la dernière modification de la stratégie.
5. Description : Une description de la stratégie.
6. Conditions : Les conditions de la stratégie, telles que les utilisateurs, les emplacements, les plateformes, etc.
7. GrantControls : Les contrôles de concession, comme dans le contexte présent l’exigence de MFA (authentification multifacteur).
8. SessionControls : Les contrôles de session, comme les restrictions de session.

Comme suit :

{

"PolicyName": "AC02-ProSantéConnect-Session4hAvecMFA-Global-ToutePlateforme-PourANS",

   "State": "enabled",

   "CreatedDateTime": "\/Date(1727081821827)\/",

   "ModifiedDateTime": null,

   "Description": null,

   "Conditions": {

"Applications": {

      "ExcludeApplications": [],

"IncludeApplications": ["99383c77-0bb9-41f0-96e1-b72ad6eca607"],

         "IncludeAuthenticationContextClassReferences": [],

         "IncludeUserActions": [],

      },

      "ClientAppTypes": ["all"],

      "ClientApplications": {

      "ExcludeServicePrincipals": null,

         "IncludeServicePrincipals": null

},

      "Devices": {

      "DeviceFilter": {

          "Mode": null,

            "Rule": null

         }

      },

      "Locations": {

      "ExcludeLocations": null,

        "IncludeLocations": null

      },

      "Platforms": {

      "ExcludePlatforms": null,

         "IncludePlatforms":  null

      },

      "ServicePrincipalRiskLevels": [],

      "SignInRiskLevels": [],

      "UserRiskLevels": [],

      "Users": {

      "ExcludeGroups": [],

         "ExcludeRoles": [],

         "ExcludeUsers": [],

         "IncludeGroups": ["2bf25bf6-6d83-4eac-9afc-5ac968de09e4"],

"IncludeRoles": [],

         "IncludeUsers": []

}

  },

   "GrantControls": {

    "BuiltInControls": [],

      "CustomAuthenticationFactors": [],

      "Operator": "OR",

      "TermsOfUse": []

   },

   "SessionControls": {

    "ApplicationEnforcedRestrictions": {

"IsEnabled": null

},

    "CloudAppSecurity": {

"CloudAppSecurityType":  null,

      "IsEnabled":  null

},

    "DisableResilienceDefaults":  null,

    "PersistentBrowser":  {

    "IsEnabled":  null,

      "Mode":  null

    },

    "SignInFrequency": {

"AuthenticationType": "primaryAndSecondaryAuthentication",

"FrequencyInterval":  "timeBased",

                            "IsEnabled":  true,

                            "Type":  "hours",

                            "Value":  4

    }

  }

}

# Pratiques recommandées

## Surveillance des journaux Microsoft Entra ID

Cette section aidera à comprendre comment utiliser et gérer les journaux Microsoft Entra ID.

### Compréhension des journaux

Le suivi et l'audit des activités et événements de votre annuaire est essentiel pour détecter les menaces, identifier les anomalies, résoudre les problèmes et répondre tout simplement aux demandes d'audit.   
Microsoft Entra ID fournit deux types de journaux d'activité : les journaux de connexion et les journaux d'audit.

1. Journaux de connexion : ces journaux contiennent des informations sur les tentatives de connexion réussies et échouées des utilisateurs et des applications à votre annuaire Entra ID ;
2. Journaux d’audit : ces journaux contiennent des informations sur les opérations effectuées dans votre annuaire Entra ID, telles que la création, la modification ou la suppression d'utilisateurs, de groupes, d'applications ou de règles.

### Rôles pour accéder aux journaux

Pour accéder aux journaux d’activité, il est nécessaire de disposer d'un rôle approprié.

Les rôles Microsoft Entra ID permettent de définir des niveaux d'accès appropriés pour les utilisateurs et les groupes d’utilisateurs. Ces rôles comprennent notamment l'administrateur global, le lecteur global, l'administrateur de sécurité et l'administrateur du support utilisateur.

Il existe différents types de rôles qui donnent des niveaux de permissions variables:

* Le rôle Administrateur global vous donne le niveau de permission le plus élevé. Vous pouvez accéder à tous les journaux de connexion et d'audit, ainsi qu'à toutes les autres fonctionnalités de Microsoft Entra ID ;
* Le rôle Lecteur global vous donne le niveau de permission le plus bas. Vous pouvez accéder aux journaux de connexion et d'audit en lecture seule, mais vous ne pouvez pas effectuer d'autres opérations dans Microsoft Entra ID ;
* Le rôle Administrateur de sécuritévous donne un niveau de permission intermédiaire. Vous pouvez accéder aux journaux de connexion et d'audit en lecture-écriture, ainsi qu'à certaines fonctionnalités liées à la sécurité, telles que la gestion des alertes, des rapports et des stratégies ;
* Le rôle Administrateur du support utilisateurvous donne un niveau de permission similaire à celui de l'administrateur de sécurité, mais limité aux utilisateurs dont vous êtes le responsable hiérarchique. Vous pouvez accéder aux journaux de connexion et d'audit en lecture-écriture pour ces utilisateurs, ainsi qu'à certaines fonctionnalités liées au support utilisateur, telles que la réinitialisation des mots de passe ou la gestion des appareils.

Documentation Microsoft :

* Rôles intégrés dans Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference>.

### Affichage des stratégies d’accès conditionnel appliquées

Les stratégies d’accès conditionnel permettent de contrôler la façon dont vos utilisateurs accèdent aux ressources du ou des locataires Entra ID de l’ES. En tant qu’administrateur de locataire, il est convient d’être en mesure de déterminer l’effet des stratégies d’accès conditionnel sur les connexions du ou des locataires afin de pouvoir prendre des mesures si nécessaire.

Dans Microsoft Entra ID, les journaux de connexion fournissent les informations nécessaires pour évaluer l’effet des stratégies.

Procéder comme suit :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter en tant que Lecteur global.
3. Accéder à Surveillance et intégrité > Journaux d’activité de connexion.
4. Sélectionner un élément de connexion dans le tableau pour afficher le volet des détails de l'inscription.
5. Les détails d’activité des journaux de connexion contiennent plusieurs onglets. Sélectionner l’onglet Accès conditionnel.
6. Considérer la liste de stratégies d’accès conditionnel appliquées à l’événement de connexion. Si aucune stratégie d’accès conditionnel n’est listée, vérifier que le rôle utilisé confère bien l’accès aux journaux de connexion et aux stratégies d’accès conditionnel, Cf. section précédente.

Documentation Microsoft :

* Afficher les stratégies d’accès conditionnel appliquées dans les journaux de connexion Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/monitoring-health/how-to-view-applied-conditional-access-policies>.

### Surveillance des autres activités

Pour identifier la compromission potentielle d'une application, ici en particulier l’application PSC, il est essentiel de surveiller les événements suivants :

1. Modifications en dehors des horaires normaux ;
2. Modifications des identifiants d'application ;
3. Modifications des autorisations des applications ;
4. Attribution de principaux services à des rôles Microsoft Entra ID ou à des rôles de contrôle d'accès basé sur les rôles Azure (RBAC) ;
5. Autorisations très privilégiées accordées aux applications – en particulier celles relatives à l’application PSC - ;
6. Modifications sur Azure Key Vault (si applicable) ;
7. Consentement de l'utilisateur final pour les applications ;
8. Modifications de la configuration de l'application, y compris les modifications d'URI.

Procéder comme suit :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter en tant que Lecteur global.
3. Accéder à Surveillance et intégrité > Journaux d’activité de connexion.
4. Sélectionner un élément de connexion dans le tableau pour afficher le volet des détails de l'inscription.

### Surveillance des comptes d’accès d’urgence

L’ES doit surveiller l’activité de connexion et le journal d’audit à partir des comptes d’urgence et déclencher des notifications à d’autres administrateurs.

Lorsque l’activité sur des comptes d’urgence est surveillée, nous invitons à vérifier que ces comptes ne sont utilisés uniquement pour les tests ou les urgences réelles. Azure Log Analytics peut être utilisé pour surveiller les journaux de connexion et déclencher des alertes par e-mail et SMS aux administrateurs de l’ES à chaque fois que des comptes d’urgence se connectent, Cf. section 5.1.7 Aller plus loin avec les classeurs.

### Durée de rétention des journaux

Les journaux d'activité sont conservés pendant une durée limitée dans le centre d’administration de Microsoft Entra. La durée de rétention dépend du type de journal et du niveau de licence Microsoft Entra ID dont dispose l’ES.

Les journaux de connexion sont conservés pendant 7 jours pour les licences gratuites, 30 jours pour les licences Microsoft Entra ID P1 et P2. Les journaux d'audit sont conservés pendant 7 jours pour les licences gratuites et 30 jours pour les licences Microsoft Entra ID P1 et P2. Pour une conservation plus longue, il est possible d’exporter et de sauvegarder les journaux.

### Exportation et sauvegarde des journaux

Pour conserver les journaux d'activité au-delà de la durée de rétention du portail Azure, il est nécessaire de les exporter vers un autre emplacement.

Il est possible :

* D’afficher les journaux d’activité et les rapports dans le Portail Azure ;
* D’accéder aux journaux d’activité via l’API Microsoft Graph ;
* De diffuser en continu les journaux d’activité vers un Event Hub ;
* D’intégrer les journaux d’activité aux journaux d’activité Azure Monitor ;
* De superviser l’activité en temps réel avec Microsoft Sentinel.

S’assurer que les procédures de sauvegarde sont bien documentées.

Consulter les ressources suivantes pour en savoir plus sur la récupération des journaux d'activité.

Documentation Microsoft :

* Comment accéder aux journaux d'activité dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/monitoring-health/howto-access-activity-logs>.

### Aller plus loin avec les classeurs

À l’aide des paramètres de diagnostic dans Microsoft Entra ID, il est possible d’intégrer les journaux à Azure Monitor afin que l’activité de connexion et la piste d’audit des modifications au sein du locataire de l’ES puissent être analysées avec d’autres données Azure.

Ainsi, les classeur d’Azure Log Analytics permettent de surveiller les activités de consentement et de permissions dans Microsoft Entra ID. Le classeur « Consent Insights » offre une vue des applications en fonction du nombre de demandes de consentement échouées.

Prérequis en complément de ceux exprimés à la section 2.1 Prise en compte des prérequis pour les stratégies d’accès conditionnel :

* Un abonnement Azure. Si besoin, un essai gratuit peut être demandé : <https://azure.microsoft.com/free/>.
* Un espace de travail Log Analytics dans un abonnement Azure. Se référer à Créer un espace de travail Log Analytics : <https://learn.microsoft.com/fr-fr/azure/azure-monitor/logs/quick-create-workspace?tabs=azure-portal> ;
* Autorisations d’accès aux données dans l’espace de travail Log Analytics. Se référer à Gestion de l’accès des espaces Log Analytics : <https://learn.microsoft.com/fr-fr/azure/azure-monitor/logs/manage-access?tabs=portal>.

Accès aux classeur de Log Analytics

Pour accéder aux classeurs

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter.
3. Aller à Surveillance et intégrité > Classeurs.
4. Chercher le rapport "Sensitive Operations Report".

Types de classeurs à considérer

 Les classeurs les plus importants sont :

* Rapport sur les modifications des méthodes d'authentification des applications et des principaux de services :
  + Surveille les nouvelles informations d'identification ajoutées, les modifications d'informations d'identification, etc.
  + Contexte : les attaquants cherchent à établir une persistance dans votre environnement en créant des accès malveillants sur des applications et des principaux de services existants. Ils utilisent ensuite ces informations d'identification pour s'authentifier en tant qu'application cible ou principal de service, leur accordant ainsi l'accès à toutes les ressources pour lesquelles ils disposent de permissions.

Eléments importants à surveiller :

* + - Toutes les nouvelles informations d'identification ajoutées aux applications et principaux de services, y compris le type d'informations d'identification ;
    - Principaux acteurs et nombre de modifications d'informations d'identification qu'ils ont effectuées ;
    - Chronologie de toutes les modifications d'informations d'identification.
* Rapport sur les nouvelles autorisations accordées aux principaux de services :
  + Liste les autorisations accordées et enquête sur toute autorisation excessive.
  + Contexte : les attaquants cherchent à obtenir un principal de service ou une application disposant d'un ensemble d'autorisations à haut privilège pour accéder à votre environnement. S'ils n'y parviennent pas, ils essaient d'ajouter des autorisations à d'autres principaux de service ou applications pour obtenir cet accès.

Eléments importants à surveiller :

* + - Liste des autorisations accordées aux principaux de services existants ;
    - Enquêter sur toute autorisation excessive accordée à des services tels que Microsoft Graph, etc.
* Rapport sur les mises à jour des rôles et des membres de groupe :
  + Surveille les modifications apportées aux adhésions, les additions aux rôles et groupes à haut privilège, etc.
  + Contexte : parfois, Les attaquants ne peuvent pas ou ne veulent pas ajouter de nouvelles autorisations aux principaux de services ou aux applications existantes. Dans ce cas, ils ajoutent de nouvelles autorisations aux rôles ou aux groupes de répertoire existants.

Eléments importants à surveiller :

* + - Liste de toutes les modifications apportées aux adhésions des principaux de services ;
    - Liste de toutes les additions aux rôles et aux groupes à haut privilège ;
    - Surveillance des principaux de services en tant que membres de rôles de répertoire (rôles d'administration) ou de groupes.

## Validation régulière des comptes d’accès d’urgence

Cette section aide à définir des procédures adaptées lorsque l’ES forme les membres du personnel à l’utilisation et à la validation des comptes d’accès d’urgence.

Nous recommandons de suivre au moins les procédures suivantes à intervalles réguliers :

* S’assurer que les personnels en charge de la surveillance et de la sécurité sont informés que l’activité de vérification du compte est permanente ;
* S’assurer que le processus de secours permettant d’utiliser ces comptes est documenté et à jour ;
* S’assurer que les administrateurs et les responsables de la sécurité susceptibles de devoir suivre ces étapes en cas d’urgence sont formés au processus ;
* Mettre à jour les informations d’identification de compte, en particulier les mots de passe, pour les comptes d’accès d’urgence, puis confirmer que ceux-ci peuvent se connecter et effectuer des tâches administratives ;
* S’assurer-vous que les utilisateurs n’ont pas enregistré d’authentification multifacteur (MFA) ou de réinitialisation de mot de passe en libre-service (SSPR) sur un appareil individuel ou dans un MIE personnel ;
* Si les comptes sont inscrits pour une authentification multifacteur sur un appareil, en vue de servir pendant la connexion ou l’activation de rôle, vérifier que tous les administrateurs susceptibles d’utiliser l’appareil en cas d’urgence ont accès à celui-ci. Vérifier également que l’appareil peut communiquer via au moins deux chemins d’accès réseau qui ne partagent pas un mode d’échec commun. Par exemple, l’appareil doit être capable de communiquer sur internet via le réseau sans fil d’une installation et le réseau d’un fournisseur de données cellulaires.

Ces étapes doivent être effectuées à intervalles réguliers et pour les principaux changements :

* Au moins tous les 90 jours ;
* En cas de remaniement récent de l’équipe informatique (IT), par exemple suite à un changement de poste, à un départ ou à l’arrivée d’un nouvel employé ;
* Lorsque les abonnements Microsoft Entra de l’ES changent.

Ceci conclut le présent guide.

1. Annexe – Eléments de définition des stratégies

Emplacements nommés

Les emplacement nommés suivants ont été définis pour l’ES :

|  |  |  |
| --- | --- | --- |
| Emplacements nommées | Plage IP | De confiance |
|  |  |  |
|  |  |  |
|  |  |  |

Stratégies de modèles d’accès conditionnel

Exiger l’authentification multifacteur pour les administrateurs

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Exiger l’authentification multifacteur pour les administrateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa>.

Sécurisation de l’inscription des informations de sécurité

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Sécurisation de l’inscription des informations de sécurité : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-registration>.

Bloquer l’authentification héritée

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Bloquer l’authentification héritée : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>.

Exiger l’authentification multifacteur pour tous les utilisateurs

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Exiger l’authentification multifacteur pour tous les utilisateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-all-users-mfa>.

Exiger une authentification multifacteur pour la gestion Azure

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Exiger une authentification multifacteur pour la gestion Azure : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-azure-management>.

Exiger un appareil compatible ou avec jonction hybride à Microsoft Entra, ou l’authentification multifacteur pour tous les utilisateurs

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Documentation Microsoft :

* Exiger un appareil compatible ou avec jonction hybride à Microsoft Entra, ou l’authentification multifacteur pour tous les utilisateurs : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-policy-compliant-device>.

Stratégie d’accès conditionnel pour les conditions générales d’utilisation de PSC

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |

Stratégie d’accès conditionnel pour l’accès à PSC sans couture

|  |  |
| --- | --- |
| Nom |  |
| Affectations | |
| Utilisateurs | Inclure  Aucun  Tous les utilisateurs  Sélectionner des utilisateurs et des groupes  Exclure  Sélectionner les utilisateurs et groupes à exclure de la stratégie :  Utilisateurs invites ou externes  Rôles d’annuaire  Utilisateurs et groupes |
| Ressources cibles | Applications cloud  Actions de l’utilisateur  Contexte d’authentification |
| Conditions | Risque de l’utilisateur  Risque de connexion  Plateformes d’appareils  Emplacements  Applications clientes  Filtres pour les appareils |
| Contrôles d’accès | |
| Octroyer | Bloquer l’accès  Accorder l’accès  Exiger une authentification multifacteur  Exiger la force de l’authentification  Exiger que l’appareil soit marqué comme conforme  Exiger un appareil avec jointure Microsoft Entra hybride  Demander une application cliente approuvée  Exiger une stratégie de protection des applications  Nécessite une modification du mot de passe  Pour plusieurs contrôles  Demander tous les contrôles sélectionnés  Demander un des contrôles sélectionnés |
| Session | Utiliser les restrictions appliquées par l’application  Utiliser le contrôle d’accès par accès conditionnel  Fréquence de connexion  Session de navigateur persistante  Personnaliser l’évaluation de l’accès en continu  Désactiver les valeurs par défaut de la résilience  Exiger une protection par jeton pour les sessions de connexion (préversion)  Utiliser le profil d’accès sécurisé global |
| Activer une stratégie | Rapport uniquement  Activé  Désactivé |