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

Zzz

Zzz

Guide de configuration de Pro Santé Connect à destination des établissements de santé

Version 0.3 - Février 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](#_Toc159333251)

[1.1 Présentation succincte de Pro Santé Connect (PSC) 5](#_Toc159333252)

[1.2 Objectif du guide 5](#_Toc159333253)

[1.3 Non-objectifs du guide 6](#_Toc159333254)

[2 Raccordement de PSC avec Microsoft Entra ID 7](#_Toc159333255)

[2.1 Inscription auprès de l’ANS 7](#_Toc159333256)

[2.2 Déclaration dans Microsoft Entra ID 8](#_Toc159333257)

[3 Gestion de l’application PSC dans Microsoft Entra ID 13](#_Toc159333258)

[3.1 Gestion des accès à l’application PSC dans Microsoft Entra ID 13](#_Toc159333259)

[3.2 Bonnes pratiques de sécurité concernant l’application PSC 13](#_Toc159333260)

[3.3 Autres opérations 14](#_Toc159333261)

[A. Annexe - Mode de fonctionnement résultant 15](#_Toc159333262)

# 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.

Ces derniers peuvent implémenter gratuitement ce service socle basé sur des technologies standardisées. PSC leur permet :

* Une sécurisation de l’identification électronique des professionnels, protégeant les données de santé éventuellement traitées, et leur garantissant une conformité réglementaire sur le niveau de garantie de l’identification électronique de leurs usagers professionnels.

A date la carte CPS et la e-CPS sont les seuls moyens d’identification électroniques (MIE) aujourd’hui pris en charge par PSC ;

* Un engagement de leurs utilisateurs, familiers de ce mode d’identification électronique commun à de nombreux services ;
* De récupérer les attributs de l’identité sectorielle (profession, savoir-faire, situation d’exercice, …) pour en faire la vérification et éventuellement automatiser leur contrôle d’accès sur cette base.

Pour plus d’informations, nous invitons le lectorat à consulter la page suivante sur le site de l’ANS : [Pro Santé Connect | Agence du Numérique en Santé (esante.gouv.fr)](https://esante.gouv.fr/produits-services/pro-sante-connect).

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 guide « Mise en œuvre Pro Santé Connect - Guide d’intégration de PSC pour le mode sans couture à destination des établissements de santé » disponible sur le site de l’ANS : TBD.

## Objectif du guide

L’objectif de ce guide est d’expliciter la mise en œuvre 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).

Ce guide précise plus particulièrement les éléments de configuration nécessaires pour instaurer une fédération d’identité avec Pro Santé Connect (PSC) avec un locataire Microsoft Entra ID d’un établissement de santé (ES) respectant les exigences de sécurité du référentiel d’exigence PSC sans couture.

Il couvre à ce titre plus précisément l'intégration de l'application Pro Santé Connect (PSC) à destination de Microsoft Entra ID, une application développée pour la circonstance, en mettant en évidence les exigences préalables, les concepts clés et les étapes essentielles. Il comporte ainsi les points spécifiques liés au FI Microsoft Entra ID qui joue le rôle de pilote pour une première fédération d’identité entre PSC et un FI tiers.

Microsoft Entra ID propose une expérience d’authentification unique ou SSO (Single Sign-On) entre toutes les ressources intégrées d’un même locataire d’un ES. Au-delà de l’application PSC, celles-ci peuvent inclure de façon non exhaustive Microsoft 365, Microsoft Dynamics 365, le portail et les services Microsoft Azure et des milliers d’autres applications de type logiciels sous la forme de services (SaaS).

## Non-objectifs du guide

La délégation de l’authentification PSC auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID suppose par ailleurs d’avoir déployé et configuré un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS. La mise en œuvre de ces MIE pour les appareils Windows 10 est couverte dans le Guide de configuration des MIE et de la navigation sans couture 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.

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.

Enfin, l’accès à PSC depuis une session Entra ID ouverte avec un MIE conforme, est permis au travers d’un accès conditionnel afin d’assurer le respect d’un ensemble d’exigences comme la force d’authentification requise. Un tel accès conditionnel est indépendant de la configuration de la navigation sans couture.

La mise en œuvre des politiques d’accès conditionnel attendues est couverte dans le Guide de configuration de l’accès conditionnel à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

# Raccordement de PSC avec Microsoft Entra ID

Comme abordé en introduction de ce guide, Pro Santé Connect (PSC) reconnait dans le cadre du POC Microsoft Entra ID comme solution compatible avec la fédération d'identité.

L’accès non (encore) authentifié à un service numérique connecté à PSC redirige le PS automatiquement vers PSC. Dans le cadre l’intégration proposée avec Microsoft Entra ID comme FI tiers de confiance, le fédérateur PSC redirige alors le PS vers Microsoft Entra ID.

Les modalités pour un ES d’une redirection transparente depuis un service connecté de PSC vers Microsoft Entra ID sont décrites sur le site de l’ANS. Pour plus d’informations, nous invitons le lectorat à consulter le guide « Mise en œuvre Pro Santé Connect - Guide d’intégration de PSC pour le mode sans couture à destination des établissements de santé » disponible sur le site de l’ANS : TBD.

Afin qu’un PS puisse utiliser un compte déclaré dans un locataire Entra ID de l’ES pour accéder en retour au travers de PSC au service numérique souhaité suppose à la fois :

1. Un enregistrement et une contractualisation auprès de l’ANS ;
2. Une configuration au niveau dudit locataire de l’ES suivants.

C’est l’objet des sections suivantes.

## Inscription auprès de l’ANS

Le raccordement du locataire Microsoft Entra ID de l’établissement de santé (ES) suppose l’inscription préalable par l’ANS de l’ID du locataire ou « tenant ID ». Cet ID du locataire est nécessaire pour activer le service Entra ID et doit être communiqué à l’ANS dans le dossier d’inscription.

L’identifiant d’un locataire se présente comme suit dans Microsoft Entra ID :

ID de locataire : 6f5faa16-41fa-4f1f-82ae-3bc3d55811f9

### Obtention de l’identifiant du locataire de l’ES

Procéder comme suit :

1. Depuis un navigateur, se connecter sur le Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com> en tant qu'administrateur du locataire Entra ID à enregistrer auprès de PSC.
2. Aller sur la vue d’ensemble Identité à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
3. Noter la valeur du « tenant ID ».

Note importante : Il convient de s'assurer que dans le cas d’un ES disposant de plusieurs locataires, l'identifiant retenu correspond au locataire qui sera couvert dans le cadre des exigences de raccordement avec l’ANS.

### Communication de l’identifiant du locataire de l’ES à l ’ANS

La communication de l’identifiant du locataire de l’ES s’effectue dans le cadre de l’inscription à effectuer auprès de l’ANS.

Une fois celle-ci effectuée, l’ID de ce locataire est inscrit dans une liste blanche des ID des locataires autorisés à fédérer leurs identités avec PSC. Il doit être ultérieurement confirmé lors de la déclaration dans Microsoft Entra ID pour être entériné et actif dans cette liste blanche.

Seuls les locataires des ES validés par l’ANS suite à une demande d’inscription ont la possibilité de déléguer l’authentification PSC à leur instance Microsoft Entra ID.

## Déclaration dans Microsoft Entra ID

Microsoft Entra ID fournit un système d’identité unique pour les applications cloud et locales, y compris des milliers d’applications pré-intégrées, afin de simplifier la gestion, de renforcer le contrôle et de combler les failles de sécurité critiques.

L’intégration de PSC avec Microsoft Entra ID repose sur ce système. A ce titre, PSC met à disposition une application PSC multilocataire déclarée au sein du locataire de l’ANS, afin d’être accessible depuis des comptes d’autres locataires appartenant aux différents ES.

Il s’agit dans le cadre du POC technique de raccordement et de sécurisation de l’application PSC bac à sable (PSC\_BAS), c.à.d. le portail de gestion utilisateur Bac à sable. Cette application est mise à disposition à l’adresse Internet <https://wallet.bas.psc.esante.gouv.fr/login-page>.

Il est à noter que cette application sert en même temps d’application de test dans le cadre de l’expérimentation.

Le raccordement de PSC avec Microsoft Entra ID suppose pour cette application :

1. La déclaration préalable faite dans le locataire ANS ;
2. La déclaration dans un locataire propre à chaque ES.

### Déclaration préalable faite dans le locataire ANS

Dans une architecture multilocataire, l’inscription initiale de l’application réside dans le locataire utilisé par le développeur de l’application en tant que personne physique ou morale, ici l’ANS. Une première instance de cette application PSC se trouve donc d’ores et déjà déclarée dans un locataire Microsoft Entra ID propre aux environnements Bac à Sable et Production de l’ANS.  Il s’agit de l’application PSC\_BAS pour l’environnement Bac à sable.

Lors de cette déclaration dans chacun de ces environnements, cette application PSC se voit attribuer :

1. Un nom d’application, également appelé URI de l'ID de l'application, par l’ANS. Ce nom de l'application est non seulement globalement unique au locataire de l’ANS considéré (environnement Bac à Sable vs. environnement Production) mais doit également l’être pour tous les locataires Microsoft Entra ID; ce qui garantit que Microsoft Entra ID puisse trouver ladite application PSC dans tous les locataires.
2. Un identifiant d’application ou ID d’application (client) à l’issue de l’expérience Inscriptions d’applications du centre d’administration Microsoft Entra.

A date, les applications PSC disponibles pour les locataires Entra ID de l’ANS sont les suivantes :

|  |  |  |
| --- | --- | --- |
| Environnement | Nom de l'application | ID d’application (client) |
| Bac à Sable | PSC\_BAS | 99383c77-0bb9-41f0-96e1-b72ad6eca607 |
| Production | TBD | TBD |

### Déclaration dans un locataire propre à chaque ES

Ladite application PSC\_BAS doit également être déclarée à son tour dans le locataire de l’ES ayant fait l’objet d’une inscription auprès de l’ANS, Cf. section 2.1 Inscription auprès de l’ANS.

Une telle déclaration s’effectue au travers d’une action d’administration dans ce locataire de l’ES.

Cette application requiert en effet le consentement d’un administrateur pour pouvoir accordées certaines permissions au sein du locataire de l’ES. Si un simple utilisateur ou un PS tente de se connecter à l’application PSC avant que ce consentement ne soit donnée et cette déclaration effectué, un message d’erreur indiquant que l’utilisateur n’est pas en mesure de donner son consentement s’affiche et demande de se connecter avec un compte disposant de privilèges d’administration.

Consentement préalable de l’administrateur

Les autorisations de l’application multilocataire PSC requièrent le consentement d’un administrateur pour pouvoir être accordées au sein d’un locataire. Ces autorisations s’inscrivent plus largement dans le cadre de l’inscription avec l’ANS, Cf. section 2.1 Inscription auprès de l’ANS.

L’administrateur de l’ES doit se connecter une première fois à l’application PSC afin de pouvoir donner son consentement pour les autorisations demandées par l’application.

Procéder comme suit :

1. Depuis un navigateur, accéder à l'URL *adminconsent* de l'application multilocataire PSC en fonction de l’environnement Bac à Sable vs. Production :

https://login.microsoftonline.com/{TenantId}/adminconsent?client\_id={ClientId}

Avec :

|  |  |  |
| --- | --- | --- |
| Paramètre | Condition | Description |
| TenantId | Requis | L’ID de locataire de l’ES pour lequel l’application doit être déclarée et vis-à-vis duquel sont demandées les autorisations. Il s’agit du l’ID obtenu à la section 2.1.1 Obtention de l’identifiant du locataire de l’ES. |
| ClientId | Requis | L’ID d’application que l’expérience Inscriptions d’applications du centre d’administration Microsoft Entra a attribué à l’application PSC lors de son inscription initiale dans le locataire de l’ANS selon l’environnement considéré : Bac à sable vs. Production. |

Par exemple pour l’environnement Bac à Sable si l’ES ne dispose que d’un seul locataire Entra ID :

<https://login.microsoftonline.com/organizations/adminconsent?client_id=99383c77-0bb9-41f0-96e1-b72ad6eca607>

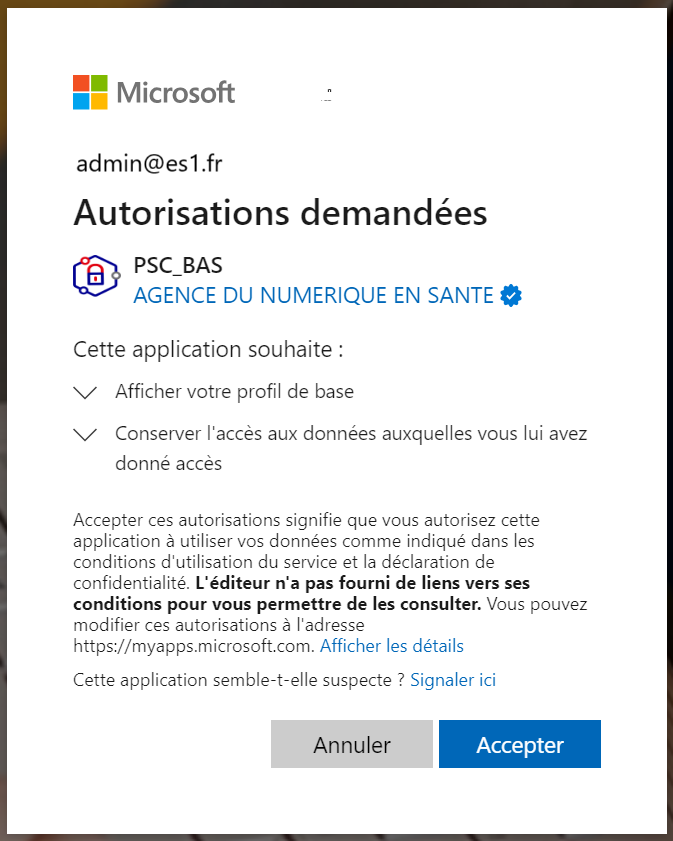
L’accès à ce lien suppose une connexion préalable à Entra ID de façon à identifier le locataire et ainsi l’ES auquel l’administrateur appartient/est rattaché, avant la demande d’approbation des autorisations nécessaires.

1. S'authentifier avec un compte disposant de privilèges d’administration sur le locataire de l’ES inscrit auprès de l’ANS.

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

Description générée automatiquement

Ceci entraine une redirection vers le point de terminaison de consentement administrateur *adminconsent* de la plateforme d’identités Microsoft pour accorder des autorisations au locataire considéré. Il en résulte une demande d'octroi de code OAuth2 qui déclenche le flux de consentement de l'administrateur et crée le principal de service dans le locataire de l'ES.



1. S’assurer de l’authenticité de l’application à laquelle les autorisations demandées seront accordées. Des acteurs malveillants pourraient tenter d’usurper l’identité de l’application portée par l’ANS pour récupérer des autorisations sur l’environnement de l’ES.
   1. Vérifier le nom de l’application PSC. L’application PSC\_BAS est utilisée dans le cadre du POC pour l’environnement Bac à sable.
   2. Vérifier qu’un badge vérifié bleu s’affiche dans l’[invite de consentement](https://learn.microsoft.com/fr-fr/entra/identity-platform/application-consent-experience) de l’application PSC au côté du nom de l’éditeur de l’application AGENCE DU NUMERIQUE EN SANTE.

L’ANS, a vérifié son identité à l’aide d’un compte l’utilisation d’un compte Microsoft Cloud Partner Program (CPP), anciennement appelé Microsoft Partner Network (MPN), qui a été [vérifié](https://learn.microsoft.com/fr-fr/partner-center/verification-responses), et a terminé le processus de vérification avec l’association du PartnerID vérifié à cette inscription d’application.

Documentation Microsoft : Vérification de l’éditeur - Vue d’ensemble – Plateforme d’identité Microsoft : <https://learn.microsoft.com/fr-fr/entra/identity-platform/publisher-verification-overview>.

1. Vérifier la nature des autorisations demandées pour :
   1. Autoriser l’authentification de l’utilisateur.
   2. Récupérer des informations sur l’identité de l’utilisateur (nom, prénom, adresse électronique, nom d’affichage, notamment)
2. Après avoir pris connaissance des autorisations demandées par l’ANS pour l’application PSC :
   1. Sélectionner Consentement pour le compte de votre organisation.
   2. Cliquer sur Accepter.

A l’issue de cette opération :

1. Une délégation est créée dans le locataire qui enregistre le consentement de l’administrateur pour l’application PSC\_BAS, à destination des utilisateurs PS de l’ES.
2. L’application multilocataire PSC\_BAS est également enregistrée au sein du locataire de l’ES.

Documentation Microsoft :

* Application multilocataire sur Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity-platform/howto-convert-app-to-be-multi-tenant> ;
* Consentement administrateur sur la plateforme d’identités Microsoft : <https://learn.microsoft.com/fr-fr/entra/identity-platform/v2-admin-consent>.

Vérification de l’enregistrement

Une fois l’autorisation effectuée par un utilisateur disposant des privilèges d’administration, l’application PSC doit apparaitre dans le menu Applications d’entreprisedu locataire de l‘ES. Ceci correspond à la représentation de l’application appelée principal du service qui a été ainsi créée à cet effet dans le locataire de 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. Aller sur Applications > Applications d’entreprise et cliquer sur l’application PSC\_BAS.

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

Description générée automatiquement

A ce stade, la configuration en place, et l’intégration désormais effective, doivent permette à PSC d’assurer une redirection transparente et automatique vers Microsoft Entra ID lorsqu’un PS souhaite accéder à un service numérique connecté à PSC.

Le mode de fonctionnement complet avec les différentes redirections est décrit en annexe de ce guide, Cf section A. Annexe - Mode de fonctionnement résultant.

# Gestion de l’application PSC dans Microsoft Entra ID

Dans le cadre du POC, il s’agit de l’application PSC\_BAS pour l’environnement Bac à sable.

## Gestion des accès à l’application PSC dans Microsoft Entra ID

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. Aller sur Applications > Applications d’entreprise et cliquer sur l’application PSC.
3. Sous Gérer > Utilisateurs et groupes, ajouter les utilisateurs et/ou groupes ciblés.

Au-delà de la mise en œuvre de ce contrôle d’accès, une politique d’accès conditionnel conforme aux attentes de l’ANS doit être configurée, Cf. Guide de configuration de l’accès conditionnel à destination des établissements de santé.

## Bonnes pratiques de sécurité concernant l’application PSC

### Protection de l’application PSC

La protection de l'application PSC nécessite la mise en place de mesures techniques de sécurité et de procédures opérationnelles. Cela inclut l'implémentation de contrôles d'accès basés sur les rôles, l'utilisation de l'authentification à deux facteurs, l’authentification sans mot de passe, la surveillance continue de l'activité de l'application pour détecter les comportements suspects, et la documentation de procédures de réponse aux incidents de sécurité.

### Défense contre les applications OAuth malveillantes

La défense contre les applications OAuth malveillantes nécessite une approche multidimensionnelle (prévention et détection) qui comprend la surveillance continue des activités suspectes, l'audit des niveaux de privilège de toutes les identités et applications, et la mise en œuvre de politiques de contrôle d'accès strictes.

Les applications malveillantes tentent souvent d'exploiter les permissions OAuth, il est donc essentiel de surveiller de près toutes les applications avec des permissions de type « app-only ». Il est important de rester vigilant envers les applications qui ne possèdent que des permissions au niveau de l'application, car elles pourraient avoir un accès trop privilégié. L’article Investigation des applications compromises et malveillantes, Cf. ci-après, contient des bonnes pratiques dont certaines se basent Microsoft Defender for Cloud Apps afin d’identifier les attaques malveillantes sur des applications OAuth.

L'utilisation de politiques de gouvernance des applications peut aider à identifier et à atténuer les applications OAuth malveillantes. Il est recommandé de mettre en place un contrôle d'accès conditionnel pour les utilisateurs se connectant à partir d'appareils non gérés.

Documentation Microsoft :

* Investigation des applications compromises et malveillantes : <https://learn.microsoft.com/fr-fr/security/operations/incident-response-playbook-compromised-malicious-app> ;
* Guidance for responders on nation-state attack : <https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/>

## Autres opérations

Les autres opérations inclut la formation afin de tenir compte des recommandations les plus récentes en matière de sécurité. Enfin, il est important de former utilisateurs et notamment les administrateurs à reconnaître des applications OAuth suspectes. Pour cela, il faut leur encourager à ne pas autoriser aveuglément toutes les applications OAuth, mais à être conscients des risques et à prendre le temps de vérifier les informations présentées avant d’autoriser une nouvelle application.

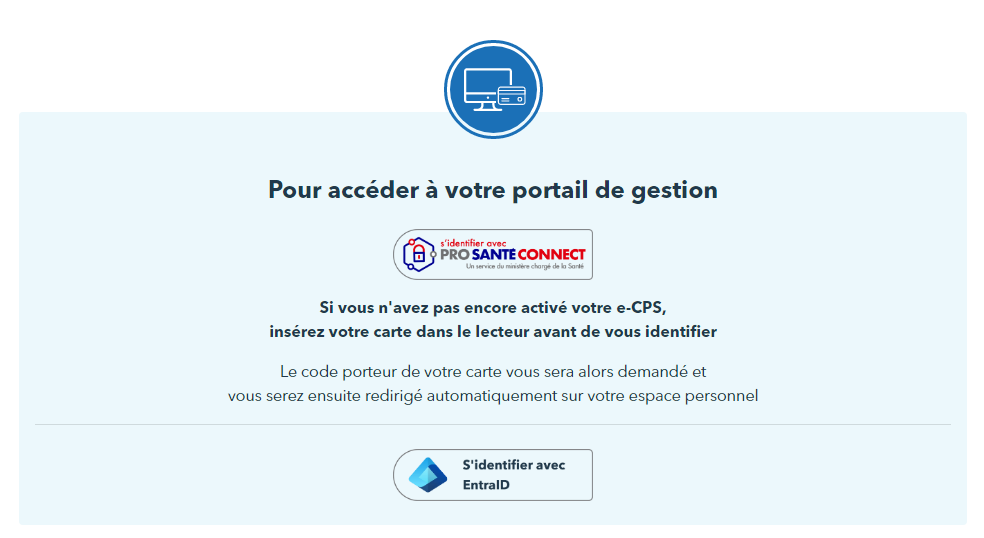
La vérification de l'éditeur de l'application est une étape importante pour éviter les applications suspectes. De plus, les administrateurs et utilisateurs doivent être formés à être vigilants et toujours vérifier les permissions demandées par l'application. Par exemple, il faut commencer par vérifier le nom de l'application, car certaines applications peuvent essayer de se faire passer pour des applications connues en utilisant des noms similaires. Il faut également regarder attentivement les permissions que l'application demande et se méfier si elles sont excessives ou incohérentes avec le service proposé. Enfin, une étape crucial est de vérifier est l'éditeur de l'application, qui doit être reconnu.

Ceci conclut le présent guide.

1. Annexe - Mode de fonctionnement résultant

A ce stade, la configuration en place, et l’intégration désormais effective de l’application PSC\_BAS dans le locataire de l’ES, doivent permette à PSC d’assurer une redirection transparente et automatique vers Microsoft Entra ID lorsqu’un PS souhaite accéder à un service numérique connecté à PSC.

Le lancement de la cinématique avec Microsoft Entra ID peut être effectuée en cliquant sur le bouton S’Identifier avec EntraID.



Dans la pratique, PSC ne redirige pas directement un PS vers son locataire d’origine pour authentification (car il n’en a pas la capacité).

PSC redirige ainsi chaque PS vers un point de redirection Microsoft Entra ID mutualisé à tous les locataires, à savoir le point de terminaison */organizations* de la plateforme d’identités Microsoft utilisé pour connecter un utilisateur à partir de n'importe quel locataire Entra ID.

Point de terminaison de redirection : <https://login.microsoftonline.com/organizations>

Pour cela, une grande partie des informations nécessaires au raccordement de PSC avec Microsoft Entra ID sont téléchargées sur PSC via le document de configuration du fournisseur OpenID Connect (OpenID Connect Discovery 1.0 incorporating errata set 1, <https://openid.net/specs/openid-connect-discovery-1_0.html>) fourni par Microsoft Entra ID comme fournisseur OpenID contenant les URL à utiliser pour l’authentification et la déconnexion (*logout*), les clés de signature publiques du service d’authentification et d’autres métadonnées comme les revendications (*claims*) prises en charge.

Ce document est exposé par le point de terminaison de découverte public exposé à l’adresse Internet : <https://login.microsoftonline.com/organizations/v2.0/.well-known/openid-configuration>

|  |  |
| --- | --- |
| Champ | Valeur |
| Authorization URL | <https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize> |
| Token URL | <https://login.microsoftonline.com/organizations/oauth2/v2.0/token> |
| Logout URL | <https://login.microsoftonline.com/organizations/oauth2/v2.0/logout> |
| User Info URL | <https://graph.microsoft.com/oidc/userinfo> |
| Issuer | [https://login.microsoftonline.com/{tenantid}/v2.0](https://login.microsoftonline.com/%7btenantid%7d/v2.0) |
| JWKS URL | <https://login.microsoftonline.com/organizations/discovery/v2.0/keys> |

Lors de la redirection, quand la plateforme d’identités Microsoft reçoit une demande sur le point de terminaison /*organizations*, cette dernière connecte le PS et découvre ainsi de quel locataire il provient. Ce point de terminaison fonctionne avec tous les protocoles d’authentification pris en charge par Microsoft Entra ID et ici le standard de l’industrie OpenID Connect (OIDC) utilisé par PSC.

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

Description générée automatiquement

La réponse de connexion envoyée à l’application PSC\_BAS contient un jeton d’ID représentant l’utilisateur. La valeur *issuer* du jeton indique à une application de quel client provient l’utilisateur. Quand le point de terminaison /*organizations* retourne une réponse, la valeur *issuer* dans le jeton d’ID correspond au locataire Microsoft Entra ID de l’utilisateur, par exemple https://login.microsoftonline.com/6f5faa16-41fa-4f1f-82ae-3bc3d55811f9/v2.0, en plus de la vérification habituelle que la valeur *tid* (tenant ID), par exemple 6f5faa16-41fa-4f1f-82ae-3bc3d55811f9.

L’application PSC peut ainsi vérifier l’ID de locataire reçu avec sa liste blanche à jour des identifiants des locataires autorisés.

Au-delà de cette information, l’application PSC\_BAS peut également connaître l’heure d’authentification explicite de l’utilisateur, la force d’authentification et le type de moyens d’authentification utilisés pour l’accès à PSC via le locataire Microsoft Entra ID de l’ES.

Le contrôle du moyen d’authentification est de la responsabilité de l’ES et à mettre en place au sein du locataire utilisé pour le raccordement. Microsoft Entra ID ne communique que le type de moyen d’authentification utilisé aux applications accédées, sans communiquer plus de détails sur le modèle ou le type de certificat utilisé par exemple.

Note importante :Les données de chaque locataire sont isolées et invisibles des autres locataires qui partagent l'instance d'application PSC.