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

Zzz

Guide de configuration Microsoft Entra Private Access à destination des établissements de santé

Version 1.0 - Décembre 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.

Content

[1 Introduction 5](#_Toc189647761)

[1.1 Objectifs du guide 6](#_Toc189647762)

[1.2 Non-objectifs du guide 6](#_Toc189647763)

[2 Vue d’ensemble de Microsoft Entra Private Access 8](#_Toc189647764)

[2.1 Appliquer l'accès conditionnel à toutes les ressources privées 9](#_Toc189647765)

[2.2 Offrir un accès transparent aux applications et ressources privées 10](#_Toc189647766)

[2.3 Moderniser l’accès aux applications privées 10](#_Toc189647767)

[2.4 Mettre en œuvre un accès juste-à-temps aux ressources sensibles 11](#_Toc189647768)

[3 Configuration de Microsoft Entra Private Access 12](#_Toc189647769)

[3.1 Prise en compte des prérequis 13](#_Toc189647770)

[3.2 Prise en compte des limitations connues 14](#_Toc189647771)

[3.3 Activation de l’Accès global sécurisé 14](#_Toc189647772)

[3.4 Configuration de l’Accès rapide 15](#_Toc189647773)

[3.5 Configuration de l’Accès par application 22](#_Toc189647774)

[4 Configuration des appareils Windows 26](#_Toc189647775)

[4.1 Mise en œuvre du client d’Accès global sécurisé 26](#_Toc189647776)

[4.2 Considérations relatives à l’utilisation de Kerberos pour l’authentification unique (SSO) 30](#_Toc189647777)

[4.3 Résolution de problèmes 31](#_Toc189647778)

[5 Accès privé aux ressources RDP 33](#_Toc189647779)

[5.1 Etapes de mise en œuvre 33](#_Toc189647780)

[5.2 Problèmes courants et solutions pour les connexions RDP 34](#_Toc189647781)

[6 Accès privé aux ressources SMB 36](#_Toc189647782)

[7 Conclusion 38](#_Toc189647783)

# Introduction

Les modèles traditionnels de sécurité réseau deviennent de plus en plus inefficaces dans un monde où l’accès à distance, l’utilisation de services cloud ou encore le recours à des prestataires externes deviennent de plus en plus la norme. Les établissements de Santé (ES) n’échappent pas à cette situation et se trouvent de facto en première ligne. Ils doivent adapter leur architecture et leurs mesures de sécurité pour répondre aux défis actuels de cybersécurité. L’identité avec la sécurité réseau devient la première ligne de défense et le fondement de toute stratégie « Confiance Zéro » ou Zero Trust, Cf. Modèle Confiance Zéro - Architecture de sécurité moderne : <https://www.microsoft.com/fr-fr/security/business/zero-trust>.

Dans un paysage où les frontières s’estompent, les technologies héritées (*legacy*) peuvent augmenter les risques en matière de cybersécurité avec :

* Des contrôles d'accès au réseau inadéquats et incohérents. Des technologies conventionnelles comme les VPN hérités, bien que populaires, offrent une protection limitée, accordant généralement aux utilisateurs un accès excessif au réseau et étendent la surface d’attaque. S’ils sont compromis, ceux-ci peuvent entraîner un accès non autorisé et potentiellement des mouvements latéraux au sein des réseaux d’un ES, exposant ainsi des données et des ressources sensibles.
* Une complexité opérationnelle accrue. La gestion de plusieurs solutions de différents fournisseurs en matière d'identité, d'accès au réseau et de mise en réseau augmente les risques de sécurité, les coûts et la complexité.
* Une expérience utilisateur faible. La lenteur et l'incohérence de l'accès en terme d’ergonomie ont un impact sur les professionnels de Santé (PS) et plus généralement l’ensemble des utilisateurs.

Sécuriser l’accès à toutes les applications et ressources privées pour l’ensemble des utilisateurs, où qu’ils se trouvent devient un enjeu crucial pour les ES.

Le ZTNA (Zero Trust Network Access) ou l’accès réseau Zero Trust constitue un modèle pertinent centré sur l’identité de l’utilisateur et le contexte de la demande, plutôt que sur le réseau depuis lequel l’accès est demandé.

La vérification systématique au cas par cas – aucune confiance n’est accordée par défaut - des tentatives d’accès à ces applications et ressources privées, s’effectue ainsi généralement via une authentification multifacteur (MFA) résistante à l’hameçonnage (*phishing*) de même nature que celle mise en œuvre dans le cadre de la délégation de Pro Santé Connect (PSC) à un fournisseur d’identité (FI) local, et plus spécifiquement dans le cadre de ce guide à Microsoft Entra ID pour le locataire d’un ES.

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

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> ;
* Travaux en cours : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/travaux-en-cours>.

Une telle mise en œuvre et les capacités nouvelles ainsi proposées constituent un premier niveau de livrable du projet Pro Santé Connect sans couture.

## Objectifs du guide

La mise en œuvre pour un ES du modèle ZTNA constitue en soi une prolongation naturelle du projet Pro Santé Connect sans couture.

L’accès à une application ou à une ressource privée de l’ES n’est accordé que si la demande est conforme à la politique de sécurité de l’ES et que l’utilisateur parvient à s’authentifier selon les modalités et les moyens d’identification électroniques (MIE) validés.

L’objectif de ce guide est d’expliciter la mise en œuvre de ce modèle ZTNA avec Microsoft Entra Private Access, de préciser la configuration permettant une telle expérience ainsi que les prérequis éventuels associés. Cette mise en œuvre repose sur Microsoft Entra ID et le locataire de l’ES mis en œuvre dans le cadre de ma configuration de la délégation de l’authentification PSC.

Ce guide se présente comme un complément des guides de déploiement Microsoft disponibles sur Microsoft Learn :

* Guide de déploiement de Microsoft Global Secure Access : <https://learn.microsoft.com/fr-fr/entra/architecture/gsa-deployment-guide-intro> ;
* Guide de déploiement de Microsoft Global Secure Access pour Microsoft Entra Private Access : <https://learn.microsoft.com/fr-fr/entra/architecture/gsa-deployment-guide-private-access>.

Le premier guide fournit des conseils pour lancer, planifier, exécuter, surveiller et clôturer un projet de déploiement d’Accès global sécurisé (Global Secure Access ou GSA) et le second aide à tester et déployer Microsoft Entra Private Access dans l’environnement de production lors de la phase d’exécution du déploiement. Nous invitons le lectorat à s’y reporter.

## Non-objectifs du guide

La configuration de la délégation de l’authentification PSC auprès du FI tiers Microsoft Entra ID n’est pas couverte dans ce guide. Cette dernière fait l’objet du Guide de configuration de Pro Santé Connect à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Cela 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 (et ultérieur) est couverte 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 de Microsoft Authenticator et des clés d’accès 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.

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.

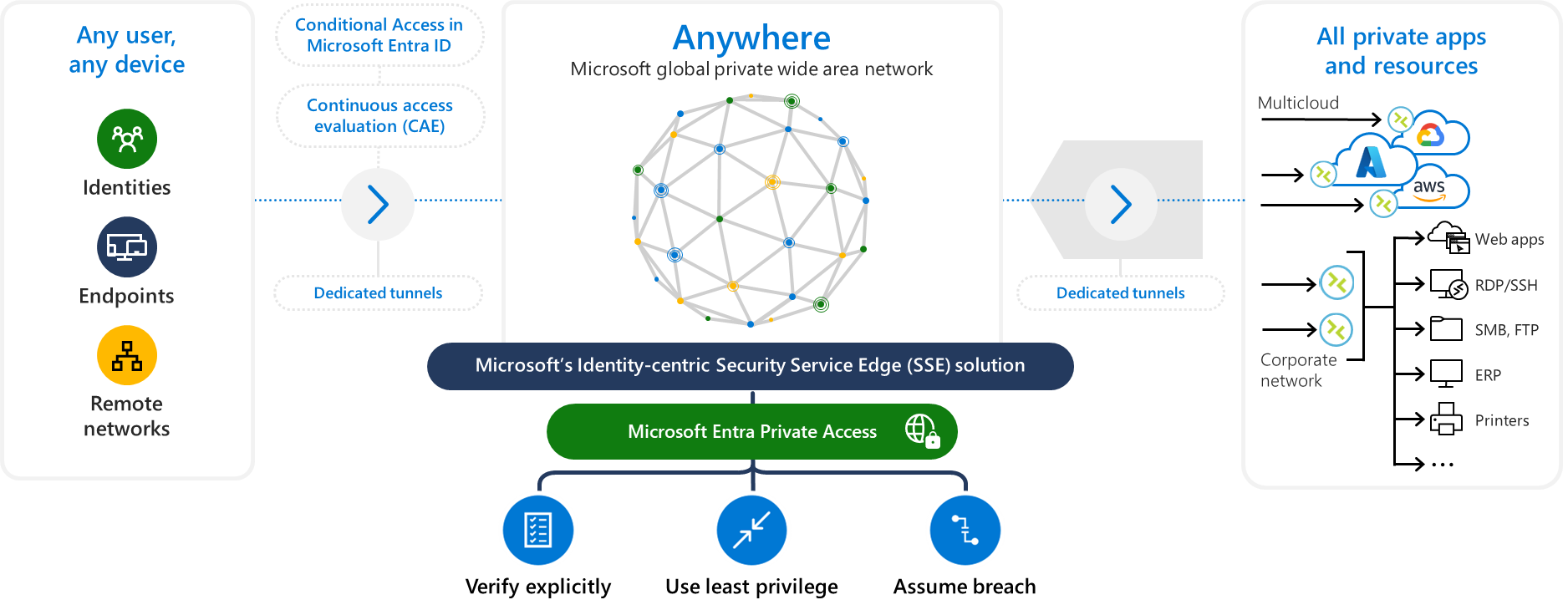
La mise en œuvre des politiques d’accès conditionnel attendues dans le cadre de la délégation est couverte dans le Guide de configuration de l’accès conditionnel à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

# Vue d’ensemble de Microsoft Entra Private Access

Basé sur les principes Zero Trust, [Microsoft Entra Private Access](https://www.microsoft.com/fr-fr/security/business/identity-access/microsoft-entra-private-access) permet à un ES de se protéger contre les cybermenaces et d’atténuer les mouvements latéraux.

Il fournit aux utilisateurs de l’ES, qu’ils soient sur site ou à distance, un accès sécurisé aux applications et ressources privées en s’appuyant sur les fonctionnalités du proxy d’application de Microsoft Entra ID et étendant l’accès à n’importe quelle ressource privée, port et protocole.

Sans apporter de modifications à ses applications et ressources en place, l’ES peut ainsi étendre les stratégies d’accès conditionnel déjà mises en œuvre dans le cadre de la délégation précédente, Cf. Guide de configuration de l’accès conditionnel à destination des établissements de santé, à son réseau à l’aide de contrôles d’accès centrés sur l’identité et activer l’authentification unique (SSO) et l’authentification multifacteur (MFA) vis-à-vis de n’importe quelle application et ressource privées sans exposer un accès réseau complet à l’ensemble du patrimoine numérique.



Le réseau privé (mondial) de Microsoft permet d’offrir le cas échéant aux utilisateurs une expérience d’accès rapide et transparente à l’échelle qui allie sécurité et productivité. Les utilisateurs (distants) se connectent à ces applications et ressources privées dans des environnements hybrides et multicloud, des réseaux privés et des centres de données à partir de n’importe quel appareil et réseau sans avoir besoin d’un VPN avec un accès adaptatif pour une sécurité plus granulaire qu’un VPN.

Microsoft Entra Private Access est un composant central de la solution SASE (Secure Access Service Edge) de Microsoft, elle-même intégrée à [Microsoft Entra Suite](https://learn.microsoft.com/fr-fr/entra/fundamentals/try-microsoft-entra-suite), qui rassemble plus globalement les contrôles d’identité et d’accès au réseau pour sécuriser l’accès à n’importe quelle application ou ressource cloud ou locale, depuis n’importe quel emplacement. Ces solution et suite ont été annoncées en disponibilité générale en juillet 2024.

Documentation Microsoft :

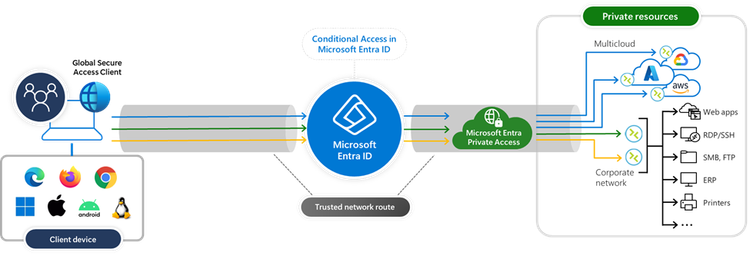
* Qu’est-ce que Global Secure Access ? : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/overview-what-is-global-secure-access>.
* Microsoft Security Service Edge now generally available : <https://techcommunity.microsoft.com/blog/identity/microsoft-security-service-edge-now-generally-available/3847828>.
* La sécurité Zero Trust simplifiée avec la suite Microsoft Entra et la plateforme d'opérations de sécurité unifiée, maintenant disponible de manière générale : <https://www.microsoft.com/en-us/security/blog/2024/07/11/simplified-zero-trust-security-with-the-microsoft-entra-suite-and-unified-security-operations-platform-now-generally-available/>.

## Appliquer l'accès conditionnel à toutes les ressources privées

Pour améliorer la posture de sécurité de l’ES et minimiser la surface d’attaque du système d’information hospitalier (SIH), il est essentiel de pouvoir appliquer un accès conditionnel à l’ensemble des applications et ressources privées de l’ES.

Il s’agit ainsi plus particulièrement :

* D’étendre les contrôles d’accès conditionnel robustes comme ceux suggérés dans le cadre de la délégation d’identité à Microsoft Entra ID, Cf. Guide de configuration de l’accès conditionnel à destination des établissements de santé, à l’ensemble des applications locales, y compris les applications héritées (*legacy*) ou propriétaires qui peuvent ne pas prendre en charge l’identité moderne et les ressources non Web, telles que RDP, SSH, SMB, SAP, l’impression ou toute autre application, ressource ou point de terminaison réseau privé basé sur TCP ou UDP.
* D’appliquer l’authentification multifacteur (MFA) sans hameçonnage (*phishing*) avec les MIE déjà validés dans le cadre de la délégation aux applications et ressources sur site lorsqu’elles sont accessibles à partir d’un environnement en local.
* Bénéficier d’une visibilité granulaire et simplifier la segmentation des applications et des ressources privées.

****

L’accès conditionnel est appliqué à chaque flux réseau ; ce qui garantit une couverture de sécurité complète pour l’ensemble des applications et ressources privées, avec i) une authentification multifacteur, ii) une sécurité fondée sur la localisation, iii) une segmentation avancée et iv) des stratégies d’accès adaptatives de moindre privilège, sans apporter de modifications aux dites applications ou ressources.

Documentation Microsoft :

* Qu’est-ce que l’accès conditionnel ? : <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/overview>.
* Appliquer des stratégies d’accès conditionnel aux applications Accès privé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-target-resource-private-access-apps>.

## Offrir un accès transparent aux applications et ressources privées

L’authentification unique (SSO) permise par le locataire Entra ID de l’ES simplifie l’expérience utilisateur en éliminant la nécessité de se connecter individuellement à chaque application privée.

Avec l’authentification unique, les PS et les autres utilisateurs bénéficient d’un accès transparent à l’ensemble des applications (privées) nécessaires à leur activité, qu’elles soient situées sur site ou dans différents clouds (via la plateforme PSC), sans avoir besoin d’une authentification répétée ou de modifications des applications existantes.

Microsoft Entra Private Access simplifie encore ce processus en fournissant l’authentification unique pour les ressources locales, à l’aide de Kerberos pour une authentification sécurisée basée sur les tickets.

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

Description générée automatiquement

Pour une expérience encore plus intégrée, Il est possible d’utiliser l’approbation Kerberos cloud de Windows Hello Entreprise pour autoriser l’authentification unique pour les utilisateurs, offrant ainsi une option d’authentification moderne et sans mot de passe pour les utilisateurs. Cette approche cohérente de l’authentification unique, prise en charge par Microsoft Entra Private Access, garantit un système de gestion des accès sécurisé et efficace pour les ressources privées dans l’ensemble de l’entreprise.

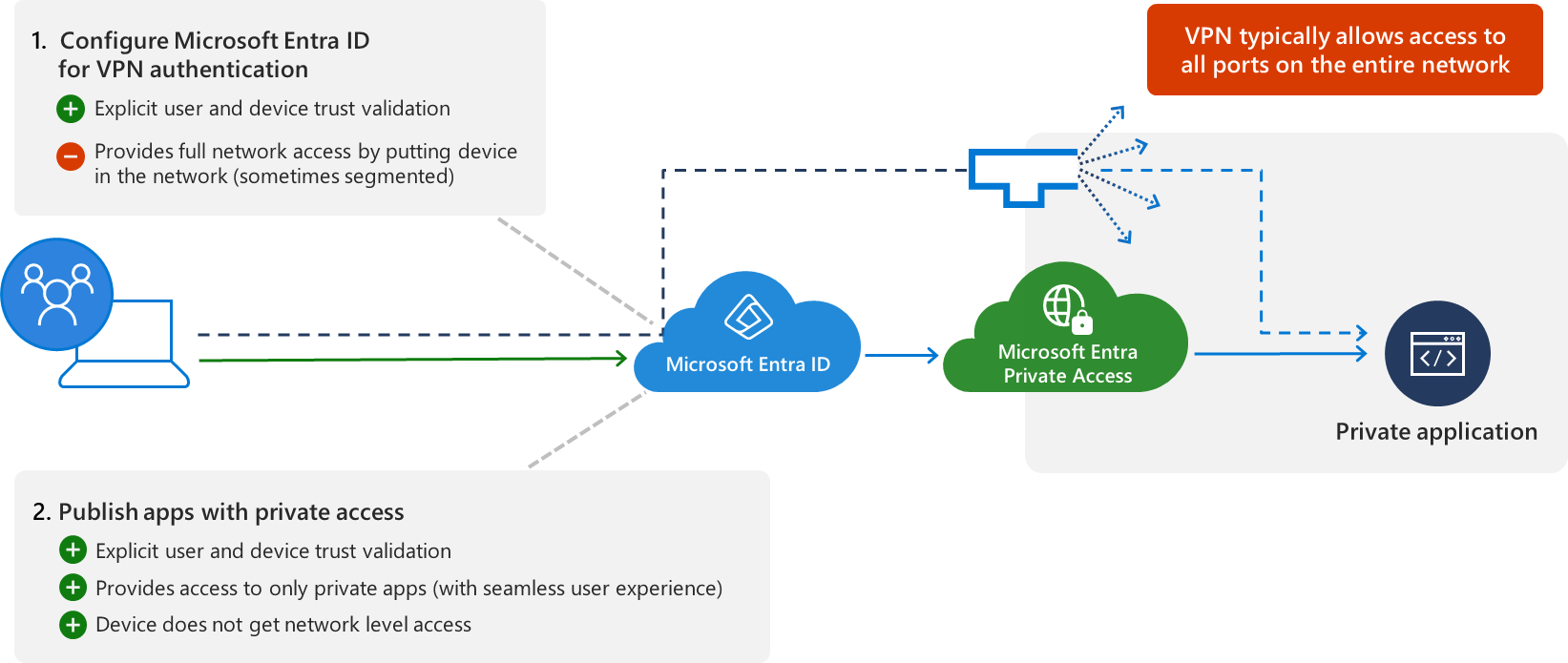
Documentation Microsoft :

* Utiliser Kerberos pour l’authentification unique (SSO) sur vos ressources avec l’Accès privé Microsoft Entra Private Access : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-kerberos-sso>.

## Moderniser l’accès aux applications privées

Au-delà de l’accès – en particulier au travers la plateforme Pro Santé Connect (PSC) dans le cadre de la délégation de l’authentification à Microsoft Entra ID -, à un ensemble de services présent dans le cloud, et de l’accès à aux applications et ressources privées au niveau de son infrastructure sur site, un ES utilise le cas échéant des VPN hérités pour permettre certains accès à distance à ces mêmes applications et ressources. Les VPN hérités accordent généralement un accès excessif à l’ensemble du réseau en intégrant l’appareil de l’utilisateur distant au réseau de l’ES.

Dans ce contexte, Microsoft Entra Private Access aide à décommissionner facilement un VPN hérité et à passer à une solution ZTNA centrée sur l’identité qui permet de réduire la surface d’attaque, d’atténuer les mouvements de menaces latéraux et de supprimer la complexité opérationnelle inutile pour les équipes informatiques de l’ES. Contrairement aux VPN traditionnels, Microsoft Entra Private Access protège l’accès au réseau de l’ES pour tous ses utilisateurs (externes), qu’ils soient distants ou locaux, et qu’ils accèdent à toutes les applications héritées, personnalisées, modernes ou privées qui se trouvent sur site ou sur n’importe quel cloud (via la plateforme PSC).



Microsoft Entra Private Access renforce la sécurité des sessions RDP (Remote Desktop Protocol) en permettant l’accès sans connectivité réseau directe. Il s’appuie sur des politiques d’accès conditionnel pour valider les identités des utilisateurs et des appareils ; ces dernières intégrant à ce titre l’authentification multifacteur (MFA).

Cela garantit que seuls les utilisateurs authentifiés disposant d’appareils conformes peuvent établir une session RDP sur le réseau de l’ES, offrant ainsi une expérience d’accès à distance sécurisée et transparente. En s’intégrant à Microsoft Entra ID, Microsoft Entra Private Access valide les jetons d’accès et connecte les utilisateurs au serveur privé approprié, renforçant ainsi la posture de sécurité (sans avoir besoin de solutions VPN traditionnelles).

## Mettre en œuvre un accès juste-à-temps aux ressources sensibles

Avec une intégration étroite avec Microsoft Entra Privileged Identity Management (PIM), le service de gouvernance de la famille de produits Microsoft Entra, Microsoft Entra Private Access permet de sécuriser l’accès juste-à-temps (just-in-time) aux applications et ressources privées de l’ES pour les utilisateurs privilégiés. Cette intégration garantit que l’accès privilégié n’est accordé qu’en cas de nécessité, conformément au principe Zero Trust de l’accès au moindre privilège.

Il permet d’appliquer des contrôles d’accès conditionnel robustes, tels que l’authentification multifacteur (MFA), afin de garantir que seuls les utilisateurs éligibles et validés peuvent accéder aux ressources sensibles.

Une telle approche améliore non seulement la sécurité, mais prend également en charge les exigences de conformité et d’audit en fournissant un suivi et une journalisation détaillés des demandes d’accès privilégiés.

Documentation Microsoft :

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

Fort de cette vue d’ensemble de Microsoft Entra Private Access, il est temps de passer à la mise en œuvre et à la configuration. C‘est l’objet du prochain chapitre.

# Configuration de Microsoft Entra Private Access

Microsoft Entra Private Access permet de spécifier les noms de domaine complets (FQDN) et les adresses IP considérées comme privés ou internes, afin de pouvoir gérer la façon dont les utilisateurs de l’ES y accèdent. Avec le client d’Accès sécurisé global (Global Secure Access ou GSA) installé sur leurs appareils (Windows 10 ou ultérieur), les utilisateurs à distance n’ont pas besoin d’utiliser un VPN hérité pour accéder à ces applications et ressources : le client les connecte silencieusement et en toute transparence aux ressources dont ils ont besoin.

A cette fin, Microsoft Entra Private Access offre deux façons de configurer les applications et ressources privées à « tunneliser » via le service, à savoir avec :

1. L’Accès rapide dans un premier temps pour définir une liste d’applications et de ressources privées à toujours « tunneliser » via le service. Ce groupe principal de noms de domaine complets, d’adresses IP et de plages d’adresses IP est ce que vous ajoutez à Accès rapide un groupe principal de noms de domaine complets (FQDN) et d’adresses IP à sécuriser.

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

Description générée automatiquement

Au fil du temps, la fonctionnalité de Découverte de l’application en préversion permet de découvrir toutes les applications privées, et de les intégrer pour permettre un accès segmenté par application.

1. L’Accès par application pour une approche granulaire de la sécurisation ; ce qui permet de spécifier différents sous-ensembles d’applications et/ou de ressources privées à sécuriser et de simplifier la création et l’association de politiques d'accès conditionnel pour des groupes d'applications et/ou de ressources en fonction de leur niveau d'impact sur l’ES et de renforcer ainsi sa posture de sécurité.

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

Description générée automatiquement

Qu’il s’agisse de l’Accès rapide ou de l’Accès par application, une application d’entreprise Entra ID est créée ; celle-ci agit en tant que conteneur pour les applications et ressources privées à sécuriser.

Chaque application d’entreprise ainsi créée dispose de son propre connecteur de réseau privé Microsoft Entra pour répartir la connexion entre le service et les applications et ressources privées considérées.

Il convient d’affecter des utilisateurs et des groupes à ladite application, puis d’utiliser des stratégies d’accès conditionnel pour contrôler l’accès à cette dernière.

## Prise en compte des prérequis

### Licences Entra ID

Le locataire de l’ES doit disposer à minima :

1. De la licence Microsoft Entra ID P1 pour utiliser les fonctionnalités de Microsoft Entra Private Access.
2. D’une licence pour Microsoft Entra Private Access.

Cette dernière est disponible dans le cadre de Microsoft Entra Suite. Pour en savoir plus sur les coûts de licence et Microsoft Entra Suite, consulter les offres et prix de Microsoft Entra : <https://www.microsoft.com/fr-fr/security/business/microsoft-entra-pricing>. L’onglet des produits autonomes de la Suite Microsoft Entra de la page de gestion des licences précise l’achat d’une licence individuelle.

Pour commencer une version d’essai afin d’explorer la disponibilité générale de Microsoft Entra Private Access, se rendre sur <https://aka.ms/PrivateAccessTrial>.

Il est également possible de s’inscrire à une [version d’essai de Microsoft Entra Suite](https://aka.ms/EntraSuiteTrial), qui inclut Microsoft Entra Private Access. Se rendre pour cela sur <https://aka.ms/EntraSuiteTrial>.

**Documentation Microsoft :**

* Guide de l’utilisateur de la version d’essai Microsoft Entra Suite : <https://learn.microsoft.com/fr-fr/entra/fundamentals/try-microsoft-entra-suite>.

### Privilèges d’administration

Par ailleurs, en termes de privilèges nécessaires pour procéder à la configuration, les administrateurs interagissant avec Microsoft Entra Private Access doivent avoir une ou plusieurs des attributions de rôles suivantes dans Microsoft Entra ID en fonction des tâches qu’ils effectuent :

* Rôle Administrateur d’accès global sécurisé pour créer et gérer tous les aspects Microsoft Entra Private Access.
* Rôles Administrateur d’application pour configurer les accès aux applications et ressources privées et pour gérer des groupes de connecteurs de réseau privé utilisés pour ces accès.
* Rôle Administrateur d’accès conditionnel pour créer et gérer tous les aspects des stratégies d’accès conditionnels.

**Documentation Microsoft :**

* Administrateur d’accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#global-secure-access-administrator>.
* Administrateur d’application : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#application-administrator>.
* Administrateur de l’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#conditional-access-administrator>.

## **Prise en compte des limitations connues**

Les noms de domaine complets, adresses IP et plages IP entre l’Accès rapide et l’Accès par application ne doivent pas se chevaucher.

Le tunneling du trafic vers des destinations Accès privé par adresse IP est pris en charge uniquement pour les plages IP en dehors du sous-réseau local de l’appareil de l’utilisateur final.

À l’heure actuelle, le trafic Accès privé ne peut être acquis qu’avec le client Accès global sécurisé. Les réseaux distants ne peuvent pas être attribués au profil de transfert de trafic Accès privé.

## **Activation de l’Accès global sécurisé**

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet [https://entra.microsoft.com/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView).
2. Se connecter en tant qu’administrateur d’application du répertoire de l’ES qui utilise le proxy d’application. P. ex., si le domaine de l’ES est *esfoo.fr*, l'administrateur doit être *admin@esfoo.fr* ou tout autre alias administratif sur ce domaine. Sélectionner le nom d’utilisateur en haut à droite et vérifier qu’il s’agit bien du répertoire qui utilise le service Proxy d’application. Pour changer de répertoire, sélectionner Changer de répertoire et choisir un répertoire qui utilise le service Proxy d’application.
3. Accéder à Accès global sécurisé > Tableau de bord.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Cliquer sur Activer. Cette opération prend quelques minutes.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Cliquer sur Prise en main. Visionner la vidéo Welcome to the Global Secure Access Dashboard et cliquer sur Close.

## **Configuration de l’Accès rapide**

La configuration des paramètres de l’Accès rapide est une composante majeure de l’utilisation de Microsoft Entra Private Access. Comme indiqué ci-dessus, la configuration initiale crée une application d’entreprise dans le locataire Entra ID de l’ES et les propriétés de cette nouvelle application sont automatiquement configurées pour fonctionner avec Entra Private Access.

Pour configurer l’Accès rapide, procéder comme suit :

1. Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif.
2. Configuration de l’Accès rapide.
3. Affectation des utilisateurs et des groupes à l’application.
4. Configuration des stratégies d’accès conditionnel.
5. Activation du profil de transfert de trafic de l’Accès global sécurisé.

Ces différentes étapes sont préciser dans les sections suivantes.

**Documentation Microsoft :**

* Comment configurer l’accès rapide pour l’accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-quick-access>.

### Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif

L’ES doit disposer d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif. Le groupe de connecteurs gère le trafic vers l’application d’entreprise relative à l’Accès rapide, Cf. section suivante.

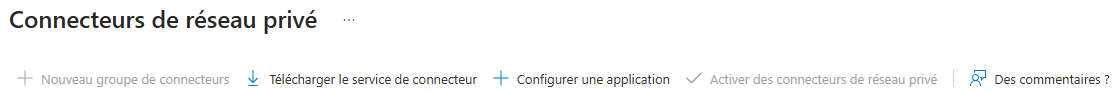
**Création d’un connecteur de réseau privé**

Un connecteur doit être installé sur un ou plusieurs serveur Windows Server au niveau de l’ES. Le connecteur est un agent qui gère la connexion sortante des serveurs d’applications locales vers Global Secure Access. L’ES peut installer un connecteur sur des serveurs sur lesquels d'autres agents d'authentification (comme Microsoft Entra) sont également déjà installés.

Si l’ES dispose déjà d’un connecteur, le réinstaller pour obtenir la dernière version. Lors de la mise à niveau, désinstaller le connecteur existant et supprimer tous les dossiers associés. A la date de rédaction de ce guide, la version minimale du connecteur requise est 1.5.3417.0.

Pour installer un connecteur sur un serveur Windows Server, procéder comme suit :

1. Depuis le Centre d’administration Microsoft Entra, accéder à Accès global sécurisé > Connexion > Connecteurs.



1. Cliquer sur Télécharger le service de connecteur.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Lire les conditions d'utilisation du service, puis cliquer sur Accepter les conditions d’utilisation et télécharger. Le fichier *MicrosoftEntraPrivateNetworkConnectorInstaller.exe* se télécharge.
2. Double-cliquer sur le fichier *MicrosoftEntraPrivateNetworkConnectorInstaller.exe* pour installer le connecteur sur le serveur Windows Server considéré. Un Assistant d'installation s'ouvre.

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

Description générée automatiquement

1. Cocher I agree to the license terms and conditions, cliquer sur Install et suivre les instructions de l’Assistant pour installer le service. Lorsqu’invité à inscrire le connecteur auprès du proxy d’application du locataire Entra ID de l’ES, fournir les informations d’identification d’administrateur d’application.
2. Vérifier l’installation effective du connecteur depuis la page précédente Connecteurs du Centre d’administration Microsoft Entra. Tous les connecteurs et les groupes de connecteurs apparaissent sur cette page.

L’installation du connecteur peut être également vérifiée par le biais du Gestionnaire de services Windows (*services.msc*) sur le serveur Windows Server.

Cette opération doit être effectuée sur les différents server Windows Serveur concernés.

Remarque : Un ES utilisant déjà un proxy d’application Microsoft Entra peut passer en toute transparence et en toute confiance à Microsoft Entra Private Access en sachant que tous les cas d’utilisation existants et l’accès aux applications web privées existantes continueront de fonctionner sans interruption.

**Documentation Microsoft :**

* Documentation sur le proxy d’application : <https://learn.microsoft.com/fr-fr/entra/identity/app-proxy/>.

**Création d’un groupe de connecteurs**

**Les groupes de connecteurs de réseau privé permettent d’affecter des connecteurs spécifiques à des applications spécifiques. Les groupes de connecteurs donnent à l’ES plus de contrôle et permettent d’optimiser les déploiements.**

Pour créer autant de groupes de connecteurs, procéder comme suit :

1. Depuis la page Connecteurs du Centre d’administration Microsoft Entra, cliquer sur Nouveau groupe de connecteurs.
2. Donnez un nom au nouveau groupe de connecteurs, puis utiliser le menu déroulant pour sélectionner le ou les connecteurs qui appartiennent à ce groupe.
3. Sélectionner Enregistrer.

**Documentation Microsoft :**

* Présentation du connecteur de réseau privé Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/concept-connectors>.
* Comment configurer des connecteurs pour Accès privé Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-connectors>.
* Documentation sur le proxy d’application : <https://learn.microsoft.com/fr-fr/entra/identity/app-proxy/>.
* Comprendre les groupes de connecteurs de réseau privé Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/concept-connector-groups>.

### Configuration de l’Accès rapide

La page Accès rapide dans le Centre d’administration Microsoft Entra permet i) de préciser un nom pour l’application d’entreprise relative à l’Accès rapide, ii) de sélectionner un groupe de connecteurs et iii) d’ajouter des segments d’application, notamment des noms de domaine complets (FDQN) et des adresses IP.

Ces trois étapes peuvent être effectuées en même temps ou l’ajout des segments d’application peut être effectué une fois la configuration initiale terminée.

**Définition du nom et d’un groupe de connecteurs**

Pour préciser un nom et un groupe de connecteurs, procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra, accéder à Accès global sécurisé > Applications > Accès rapide.
2. Dans Nom, préciser un nom. Il est recommandé d’utiliser le non « Accès rapide ».
3. Dans Groupe de connecteurs, sélectionner le groupe de connecteur précédemment créé dans le menu déroulant.
4. Sélectionner Enregistrer pour créer l’application, p. ex. Accès rapide, sans noms de domaine complets, adresses IP et suffixes DNS privés.

**Ajout d’un segment d’application Accès rapide**

Des noms de domaine complets, des adresses IP et des plages d’adresses IP peuvent être à présent ajoutés pour l’Accès rapide. Chaque segment d’application ainsi créé permet d’ajouter plusieurs ports et plages de ports.

Pour créer des segment d’application, procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra, accéder à Accès global sécurisé > Applications > Accès rapide.

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

Description générée automatiquement

1. Cliquer sur Ajouter un segment d’application Accès rapide. Un panneau Créer un segment d’application s’ouvre :

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

Description générée automatiquement

* 1. Dans Type de destination, sélectionner le type de destination souhaité :
     + Adresse IP : adresse IPv4 (Internet Protocol version 4), telle que 192.168.2.1, qui identifie un appareil sur le réseau.
     + Nom de domaine complet  : nom de domaine (y compris les noms de domaine complets génériques) qui spécifie l’emplacement exact d’un ordinateur ou d’un hôte dans le système DNS.
     + Plage d’adresses IP (CIDR) : plage d’adresses IP. Une adresse IP est suivie d’un suffixe indiquant le nombre de bits réseau dans le masque de sous-réseau. P. ex., 192.168.2.0/24 indique que les 24 premiers bits de l’adresse IP représentent l’adresse réseau, tandis que les 8 bits restants représentent l’adresse d’hôte.
     + Plage d’adresses IP (IP à IP) : plage d’adresses IP allant de l’IP de début (par exemple, 192.168.2.1) jusqu’à l’IP de fin (par exemple, 192.168.2.10).
  2. Préciser les détails appropriés pour le type sélectionné. Les champs suivants changent en fonction de la sélectionner.
     + Adresse IP : indiquer les ports à inclure.
     + Nom de domaine complet (y compris les noms de domaine complets génériques) : indiquez les noms à inclure. NetBIOS n’est pas pris en charge. P. ex., utiliser *esfoo.local/app1* au lieu de *esfoo/app1*.
     + Plage d’adresses IP (CIDR) : indiquer l’adresse de départ, le masque de réseau et les ports.
     + Plage d’adresses IP (IP à IP) : indiquez le début, la fin et les ports de l’adresse IP.
  3. Entrer les ports et le protocole :
     + Séparer plusieurs ports par une virgule.
     + Spécifier des plages de ports avec un trait d’union.

Le protocole RDP (Remote Desktop Protocol) utilise le port 3389 (Cf. section 4 Accès aux ressources RDP), le partage de fichier SMB (Server Message Block) le port 445 (Cf. section 5 Accès aux ressources SMB).

Pour utiliser Kerberos pour l’authentification unique (SSO pour des applications ou des ressources « Kerbérisées » sur site via Microsoft Entra Private Access, les contrôleurs de domaine doivent être publiés afin que les clients puissent obtenir des tickets Kerberos. Ces tickets sont nécessaires pour l’authentification unique auprès des ressources locales.

Ajouter toutes les adresses IP de contrôleurs de domaine ou noms de domaine complets (FQDN) et ports conformément à la table suivante.

|  |  |  |
| --- | --- | --- |
| Port | Protocole | Objectif |
| 88 | UDP/TCP | Kerberos |
| 389 | UDP | Localisateur du contrôleur de domaine |
| 464 | UDP/TCP | Demande de modification de mot de passe |
| 123 | UDP | Synchronisation de l’heure |

Veiller à ne PAS utiliser de noms de domaine complets génériques pour publier vos contrôleurs de domaine, au lieu de cela, ajouter leurs adresses IP ou noms de domaine complets spécifiques. De plus, SEULS les contrôleurs de domaine du site Active Directory où les connecteurs sont installés doivent être publiés, Cf. section 5.3.1 Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif ci-dessus.

Remarque : ce guide se concentre sur l’activation de l’authentification unique sur des ressources locales et exclut la configuration nécessaire pour les appareils joints à un domaine Active Directory local afin d’effectuer des opérations de domaine (modification de mot de passe, stratégie de groupe, etc.).

* 1. Sélectionner Appliquer**.**

1. **Répéter l’étape 2 autant que nécessaire.** Jusqu’à 500 segments d’application peuvent être ajoutés à l’Accès rapide.

Les noms de domaine complets, adresses IP et plages IP entre l’Accès rapide et l’Accès par application ne doivent pas se chevaucher.

1. **Sélectionner Enregistrer pour terminer.**

**Ajout de suffixes DNS privés**

La prise en charge du DNS privé pour Microsoft Entra Private Access permet à l’ES d’interroger ses propres serveurs DNS internes pour résoudre les adresses IP pour des noms de domaine internes.

Cela permet notamment de :

* De configurer un suffixe DNS correspondant à une plage d’adresse donnée afin que le client d’Accès global sécurisé (Global Secure Access ou GSA) puisse résoudre les noms DNS privés et sache comment router correctement la requête. Le client l’utilise pour accéder aux ressources locales publiées.

Comme souligné précédemment, il est possible d’utiliser Kerberos pour l’authentification unique (SSO) pour des applications ou des ressources « Kerbérisées » sur site. Les noms DNS privé sont nécessaires dans cette configuration.

* D’accélérer considérablement les temps de résolution DNS à la périphérie SASE de Microsoft et d’améliorer les performances avec la mise en cache des réponses DNS ;
* De simplifier l’accès Zero Trust aux applications et ressources privées à l’aide de noms de domaine complets, rationalisant ainsi le processus de connexion aux ressources internes, tout en utilisant les déploiements DNS existants.

Cela est particulièrement avantageux dans les scénarios où les utilisateurs ont besoin d’accéder de manière transparente à des ressources privées sans avoir besoin de VPN ou d’appareils joints à un domaine, tout en offrant un moyen plus sûr et plus efficace de gérer l’accès.

De plus, l’intégration du DNS privé avec l’accès conditionnel ajoute une couche supplémentaire de contrôles de sécurité centrés sur l’identité, permettant un contrôle plus granulaire de l’accès aux ressources privées.

**Documentation Microsoft :**

* Utiliser Kerberos pour l’authentification unique pour vos ressources avec Microsoft Entra Private Access : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-kerberos-sso>.

Pour ajouter un suffixe DNS à utiliser pour le DNS privé, procéder comme suit :

1. Sélectionner l’onglet DNS privé.

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

Description générée automatiquement

1. Cocher la case pour activer le DNS privé.

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

Description générée automatiquement

1. Sélectionner Ajouter un suffixe DNS.

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

Description générée automatiquement

1. Entrer le suffixe DNS, puis sélectionner Ajouter.

Pour utiliser Kerberos pour l’authentification unique (SSO), ajouter au minimum les suffixes de niveau supérieur de la ou des forêts Active Directory de l’ES hébergeant les utilisateurs synchronisés avec Microsoft Entra ID pour le locataire de l’ES.

A ce stade, avec un groupe de connecteurs de réseau privé et l’application d’entreprise pour l’Accès rapide configurés, il est nécessaire d’accorder l’accès à l’application en attribuant des utilisateurs et/ou des groupes à l’application.

### Affectation des utilisateurs et des groupes à l’application d’entreprise

Les propriétés de l’application d’entreprise précédemment créée peuvent être affichées à partir d’ Accès global sécurisé depuis le Centre d’administration Microsoft Entra soit de la page Accès rapide soit de la page Applications d’entreprise sous Applications via une recherche de ladite application.

Pour rechercher une application sur la page Applications d’entreprise, procéder comme suit :

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

Description générée automatiquement

1. Désactiver tous les filtres afin de ne pas masquer l’application recherchée.
2. Cliquer sur Modifier les paramètres d’application dans Accès rapide.
3. Sélectionner Utilisateurs et groupes dans le menu latéral.
4. Ajouter des utilisateurs et des groupes selon les besoins de l’ES.

Remarque importante :Les utilisateurs doivent être directement attribués à l’application ou au groupe attribué à l’application. Les groupes imbriqués ne sont pas pris en charge.

**Documentation Microsoft :**

* Affecter des utilisateurs et des groupes à une application : <https://learn.microsoft.com/fr-fr/azure/active-directory/manage-apps/assign-user-or-group-access-portal>.

### Configuration des stratégies d’accès conditionnel pour cette application

A ce stade, des stratégies d’accès conditionnel sont à appliquer à l’application d’entreprise pour l’Accès rapide. L’application de stratégies d’accès conditionnel offre davantage d’options pour gérer l’accès aux applications, aux sites et aux services.

Une stratégie d’accès conditionnel pour cette application peut être créer à partir d’Accès global sécurisé depuis le Centre d’administration Microsoft Entra. Le démarrage du processus depuis Accès global sécurisé ajoute automatiquement l’application d’entreprise sélectionnée en tant que Ressource cible pour la stratégie. Il suffit alors de configurer les paramètres de stratégie.

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet [https://entra.microsoft.com/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView).
2. Se connecter en tant qu’administrateur d’accès conditionnel.
3. Accéder à Accès global sécurisé > Applications > Applications d’entreprise.
4. Sélectionner une application dans la liste.
5. Cliquer sur Accès conditionnel à partir du menu latéral. Toutes les stratégies d’accès conditionnel existantes s’affichent dans une liste.
6. Cliquer sur Nouvelle stratégie. L’application sélectionnée s’affiche dans les détails des Ressources cibles.
7. Configurer les conditions, les contrôles d’accès et affectez des utilisateurs et des groupes selon les besoins.

Il est également possible d’appliquer des stratégies d’accès conditionnel à un groupe d’applications basé sur des attributs personnalisés.

**Documentation Microsoft :**

* Comment appliquer des stratégies d’accès conditionnel à des applications Microsoft Entra Private Access : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-target-resource-private-access-apps>.
* Filtre pour applications dans une stratégie d’accès conditionnel : <https://learn.microsoft.com/fr-fr/azure/active-directory/conditional-access/concept-filter-for-applications>.

### Activation du profil de transfert de trafic de l’Accès global sécurisé

Une fois l’application d’entreprise pour l’Accès rapide dûment configurée, les applications et ressources privées ajoutées et les utilisateurs attribués à l’application, le profil Accès privé peut être activé à partir de la page Transfert de trafic d’Accès global sécurisé depuis le Centre d’administration Microsoft Entra.

Ce profil peut être activé avant de configurer l’Accès rapide avec les étapes précédentes, mais sans l’application et le profil configurés, il n’y a aucun trafic à transférer.

Pour activer le profil de transfert de trafic Accès privé, procéder comme suit ;

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet [https://entra.microsoft.com/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView).
2. Se connecter en tant qu’administrateur d’accès global sécurisé.
3. Accéder à Accès global sécurisé > Connexion > Transfert de trafic.
4. Cocher la case Private access profile.

**Documentation Microsoft :**

* Comment gérer le profil d’accès privé de transfert du trafic : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-manage-private-access-profile>.

## **Configuration de l’Accès par application**

L'Accès par application est configuré en créant une nouvelle application Global Secure Access. Vous créez l'application, sélectionnez un groupe de connecteurs et ajoutez des segments d'accès au réseau. Ces paramètres constituent l'application individuelle à laquelle vous pouvez attribuer des utilisateurs et des groupes.

Pour configurer l'accès par application, vous devez disposer d'un groupe de connecteurs avec au moins un connecteur [proxy d'application Microsoft Entra](https://learn.microsoft.com/fr-fr/azure/active-directory/app-proxy/application-proxy) actif. Ce groupe de connecteurs gère le trafic vers cette nouvelle application. Avec les connecteurs, vous pouvez isoler les applications par réseau et par connecteur.

Pour configurer l’Accès par application, procéder comme suit :

1. Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif.
2. Création d’une application Global Secure Access.
3. Affectation des utilisateurs et des groupes à l’application d’entreprise.
4. Attribution des stratégies d’accès conditionnel pour cette application.
5. Activation du profil de transfert de trafic de l’Accès global sécurisé.

Ces différentes étapes sont préciser dans les sections suivantes.

**Documentation Microsoft :**

* Comment configurer l’accès par application en utilisant des applications Global Secure Access : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-quick-access>.

### Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif

Cf. section éponyme 3.3.1 Création d’un groupe de connecteurs avec au moins un connecteur de réseau privé actif ci-dessus.

### Configuration l’Accès par application

La création d’une nouvelle application pour l’Accès par application nécessite de fournir un nom, de sélectionner un groupe de connecteurs, puis d’ajouter des segments d'application. A l’instar de l’Accès rapide, les segments d'application incluent les noms de domaine complets (FQDN) et les adresses IP à acheminer via le service. Ces trois étapes peuvent être effectuée en même temps ou les segments d’application peuvent être ajoutés une fois la configuration initiale terminée.

**Définition du nom et d’un groupe de connecteurs**

Pour préciser un nom et un groupe de connecteurs, procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra avec les rôles appropriés, accéder à Accès global sécurisé > Applications > Applications d’entreprise.
2. Sélectionner Nouvelle application.
3. Préciser un nom pour l’application.
4. Sélectionner un groupe de connecteurs dans le menu déroulant. Il est nécessaire disposer d’au moins un connecteur actif pour créer l’application.
5. Cliquer sur Enregistrer en bas de la page pour créer l’application sans ajouter d’applications ou ressources privées.

**Ajout d’un segment d’application Accès rapide**

A l’instar de l’Accès rapide, des noms de domaine complets, des adresses IP et des plages d’adresses IP pour l’Accès par application. Chaque segment d’application ainsi créé permet d’ajouter plusieurs ports et plages de ports.

Pour créer un segment d’application, procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra, accéder à Accès global sécurisé > Applications > Applications d’entreprise.

Une image contenant texte, Police, ligne, blanc

Description générée automatiquement

1. Sélectionner l’application nouvellement créée puis cliquer sur Ajouter un segment d’application Accès rapide. Dans le panneau Créer un segment d’application qui s’ouvre :

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

Description générée automatiquement

* 1. Sous Type de destination, sélectionner le type de destination souhaité.
  2. Préciser les détails appropriés pour le type sélectionné. Les champs suivants changent en fonction de la sélectionner.
  3. Entrer les ports et le protocole.
  4. Cliquer sur Appliquer**.**

**Cf. section 3.3.2** Configuration de l’Accès rapide **ci-dessus.**

1. **Répéter l’étape 2 autant que nécessaire.** Jusqu’à 500 segments d’application peuvent être ajoutés à l’Accès rapide.

Les noms de domaine complets, adresses IP et plages IP entre l’Accès rapide et l’Accès par application ne doivent pas se chevaucher.

1. **Cliquer sur Enregistrer pour terminer.**

### Affectation des utilisateurs et des groupes à l’application d’entreprise

Cf. section éponyme 3.3.3 Affectation des utilisateurs et des groupes à l’application d’entreprise ci-dessus.

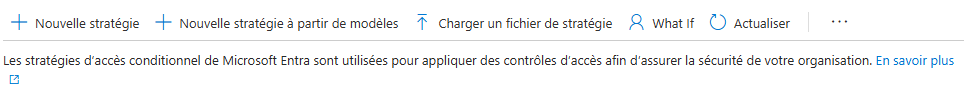
### Attribution des stratégies d’accès conditionnel pour cette application

Les stratégies d’accès conditionnel pour l’Accès par application sont configurées au niveau de l’application d’entreprise pour chaque application. Les stratégies d’accès conditionnel peuvent être créées et appliquées à l’application d’entreprise à partir de deux endroits depuis le Centre d’administration Microsoft Entra :

* Accéder à Accès global sécurisé > Applications > Applications d'entreprise. Sélectionner une application, puis sélectionner Accès conditionnel dans le menu latéral.

- ou -

* Accéder à Protection > Accès conditionnel > Stratégies. Cliquer + Nouvelle stratégie.



Cf. section éponyme 3.3.4 Configuration des stratégies d’accès conditionnel pour cette application ci-dessus.

### Activation du profil de transfert de trafic de l’Accès global sécurisé

Cf. section éponyme 3.3.5 Activation du profil de transfert de trafic de l’Accès global sécurisé ci-dessus.

Il est à présent temps de passer à la configuration des appareils. C’est l’objet du chapitre suivant.

# Configuration des appareils Windows

## Mise en œuvre du client d’Accès global sécurisé

Le client d’Accès global sécurisé (Global Secure Access ou GSA), composant essentiel de l’Accès global sécurisé, aide l’ES à gérer et à sécuriser le trafic réseau sur les appareils Windows (10 ou ultérieurs) des PS et des autres utilisateurs concernés par cette solution.

Le rôle principal du client GSA est d’acheminer le trafic qui doit être sécurisé par l’Accès global sécurisé, vers le service cloud. Tous les autres trafics sont directement acheminés vers le réseau de l’ES. Les profils de transfert Accès privé configurés dans le Centre d’administration Microsoft Entra, Cf. sections 5.3 **Configuration de l’Accès rapide** ci-dessous et 5.4 **Configuration de l’Accès par application** ci-dessous, déterminent le trafic que le client de l’Accès global sécurisé achemine vers le service cloud.

Documentation Microsoft :

* Client Accès global sécurisé pour Microsoft Windows : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-install-windows-client>.
* Profils de transfert de trafic dans l’Accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/concept-traffic-forwarding>.

### Prise en compte des prérequis

Le client d’Accès global sécurisé (GSA) nécessite :

* Un locataire Entra ID intégré à l’Accès global sécurisé comme couvert à la section 3 Configuration de Microsoft Entra Private Access ci-dessus.
* Des licences comme décrit à la section 3.1 Prise en compte des prérequis ci-dessus.
* Un appareil géré joint au locataire intégré. L’appareil doit être joint à Entra ID, de manière hybride ou non. Les appareils inscrits à (ou enregistrés) Entra ID ne sont pas pris en charge pour cette mise en œuvre à la différence de la délégation.

La différence entre un appareil inscrit à Entra ID et un appareil joint à Entra ID réside principalement dans la manière dont l’appareil est intégré et utilisé au sein de l’ES :

1. Appareils inscrits à Entra ID : il s‘agit typiquement des appareils personnels pris en charge dans le cadre d’une politique BYOD (*Bring Your Own Device*) de l’ES.

* Connexion : le PS ou tout autre utilisateur utilise un compte local (comme un compte Microsoft) pour se connecter à l’appareil.
* Gestion : l’appareil peut être géré via des outils de gestion des périphériques mobiles (MDM) comme Microsoft Intune.
* Accès : l’appareil permet l’accès aux ressources de l’ES via des stratégies d’accès conditionnel.

1. Appareils joints à Entra ID : il s’agit d’appareils appartenant à l’ES.

* Connexion : le PS ou tout autre utilisateur se connecte à l’appareil avec un compte Microsoft Entra ID ou Active Directory synchronisé de l’ES.
* Gestion : l’appareil est entièrement intégré dans l’environnement de gestion de l’organisation.
* Accès : L’appareil offre une authentification unique (SSO) et un accès direct aux ressources de l’organisation.

En résumé, les appareils inscrits sont souvent des appareils personnels avec un accès limité et géré, tandis que les appareils joints sont des appareils organisationnels avec une intégration et une gestion complètes.

Documentation Microsoft :

* Que sont les appareils enregistrés Microsoft Entra ? : <https://learn.microsoft.com/fr-fr/entra/identity/devices/concept-device-registration>.
* Qu’est-ce qu’un appareil à jonction hybride Microsoft Entra ? : <https://learn.microsoft.com/fr-fr/entra/identity/devices/concept-hybrid-join>.
* Qu’est-ce qu’un appareil joint Microsoft Entra ? : <https://learn.microsoft.com/fr-fr/entra/identity/devices/concept-directory-join>.

### Prise en compte des limitations connues

Les limitations connues pour la version actuelle du client d’Accès global sécurisé (GSA) sont les suivantes :

* Le DNS sécurisé dans ses différentes versions, telles que DNS sur HTTPS (DoH), DNS sur TLS (DoT) ou les extensions de sécurité DNS (DNSSEC) n’est PAS pris en charge. Le DNS sécurisé doit être le cas échéant désactivé pour que le client GSA puisse acquérir le trafic réseau.

Documentation Microsoft :

* Désactiver le DNS sécurisé dans les navigateurs : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/troubleshoot-global-secure-access-client-diagnostics-health-check#secure-dns-disabled-in-browsers-microsoft-edge-chrome-firefox>.
* Le DNS sur TCP n’est PAS pris en charge. Si le DNS utilise typiquement le port 53 UDP pour la résolution des noms, certains navigateurs ont leur propre client DNS qui prend également en charge le port 53 TCP.

En guise de mesure palliative, désactiver le client DNS du navigateur en définissant les valeurs de Registre suivantes :

* + Pour Microsoft Edge :

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Edge] "BuiltInDnsClientEnabled"=dword:00000000

* + Pour Chrome :

[HKEY\_CURRENT\_USER\Software\Policies\Google\Chrome] "BuiltInDnsClientEnabled"=dword:00000000

Ajouter également l’accès à chrome://flags et désactiver Async DNS resolver.

* IPv6 n’est PAS (encore) pris en charge. Le client « tunnelise » uniquement le trafic IPv4. Le trafic IPv6 n’est pas (encore) acquis par le client GSA et est donc transféré directement vers le réseau de l’ES. Pour permettre à tout trafic pertinent d’être « tunnelisé », nous recommandons de configurer le client de manière à préférer IPv4 à IPv6, si :

1. Le profil de transfert est configuré pour acquérir le trafic par IPv4 (par opposition à un nom de domaine complet).
2. Le nom de domaine complet résolu pour cette adresse IP est également résolu en adresse IPv6.

Pour configurer le client de manière à préférer IPv4 à IPv6, définir la clé de Registre suivante, puis redémarrer ensuite l’appareil :

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters] "DisabledComponents"=dword:00000020

* L’adresse IP source de la connexion comme l’adresse IP de périphérie (et non comme l’adresse IP de l’appareil) est détectée pour le trafic réseau « tunnelisé ». Ce scénario peut impacter les services qui s’appuient sur la géolocalisation. Pour qu’Entra ID détecte la véritable adresse IP source de l’appareil, envisager d’activer la restauration d’adresse IP source.

Documentation Microsoft :

* Restauration de l’adresse IP source : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-source-ip-restoration>.
* Si un proxy est configuré au niveau de l’application (p. ex., un navigateur) ou au niveau du système d’exploitation, configurez un fichier PAC (Proxy Auto Configuration) afin d’exclure tous les noms de domaine complets et les adresses IP que le client GSA va « tunneliser ».

Pour empêcher les requêtes HTTP pour des noms de domaine complets/adresses IP spécifiques de « tunneliser « vers le proxy, ajouter les noms de domaine complets/adresses IP au fichier PAC en tant qu’exceptions. (Ces noms de domaine complets/adresses IP se trouvent dans le profil de transfert de l’Accès global sécurisé pour la tunnelisation), p. ex. :

function FindProxyForURL(url, host) {

        if (isPlainHostName(host) ||

            dnsDomainIs(host, ".microsoft.com") || // tunneled

            dnsDomainIs(host, ".msn.com")) // tunneled

           return "DIRECT";                    // If true, sets "DIRECT" connection

        else                                   // If not true...

           return "PROXY 10.1.0.10:8080";  // forward the connection to the proxy

}

Si une connexion internet directe n’est pas possible, configurer le client GSA pour qu’il se connecte au service d’Accès global sécurisé via un proxy. P. ex., définir la variable système grpc\_proxy pour qu’elle corresponde à la valeur du proxy, p. ex. *http://proxy:8080*.

Pour appliquer les modifications de la configuration, redémarrer les services Windows du client GSA.

### Installation du client d’Accès global sécurisé

La version la plus récente du client d’Accès global sécurisé (GSA) peut être téléchargée à partir du Centre d’administration Microsoft Entra.

Pour installer le client sur un appareil, procéder comme suit ;

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet [https://entra.microsoft.com/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView).
2. Se connecter en tant qu’administrateur d’accès global sécurisé.
3. Accéder à Accès global sécurisé > Connexion > Téléchargement du client.

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

Description générée automatiquement

1. Sous Windows, cliquer sur Télécharger le client. Le fichier d’installation *GlobalSecureAccessClient.exe* se télécharge sur l’appareil.
2. Exécuter le fichier d’installation *GlobalSecureAccessClient.exe*. etaccepter les termes du contrat de licence logicielle.

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

Description générée automatiquement

1. Cocher I agree to the license terms and conditions pour accepter les termes du contrat de licence logicielle et cliquer sur Install.
2. Le client s’installe et se connecte de manière silencieuse à l’aide des informations d’identification Entra ID. Si la connexion silencieuse échoue, le programme d’installation invite à se connecter manuellement.
3. Une fois la connexion établie, l’icône de connexion devient verte. Pointer sur celle-ci pour ouvrir la notification de statut du client GSA, qui doit afficher Connecté.

L’ES peut installer le client GSA de manière silencieuse à l’aide du commutateur /quiet, ou utiliser des solutions de gestion des appareils mobiles (MDM) comme Microsoft Intune pour déployer le client GSA sur ses appareils.

### Collecte de journaux et diagnostics avancés

Le monitoring du trafic pour l’Accès global sécurisé est une activité importante pour veiller à ce que le locataire de l’ES soit configuré correctement et que les PS ainsi que tous les autres utilisateurs visés bénéficient de la meilleure expérience possible.

Le tableau de bord de l’Accès global sécurisé fournit des visualisations du trafic réseau acquis par Microsoft Entra Private Access et compile les données des configurations réseau de l’ES, y compris les appareils, les utilisateurs et les locataires dans plusieurs widgets. Ces visualisation peuvent être complétées avec les classeurs (*workbooks*) Azure qui proposent rapports interactifs complets.

Les actions suivantes permettent de compléter ces premières activités:

1. Collecte de journaux : Utiliser l'option de collecte de journaux dans le client GSA pour collecter des informations sur l’appareil client, les journaux d'événements associés aux services, et les valeurs de registre :
   1. Les journaux du trafic de l’Accès global sécurisé (préversion) fournissent un aperçu sur les personnes qui accèdent aux ressources, l’endroit à partir duquel elles y accèdent et l’action qui a eu lieu.
   2. Les journaux d’audit Microsoft Entra constituent une source précieuse d’informations lors de l’examen ou de la résolution des modifications apportées à votre environnement Microsoft Entra. Les modifications liées à l’Accès global sécurisé sont capturées dans les journaux d’audit dans plusieurs catégories, telles que les profils de transfert de trafic, la gestion réseau à distance, etc.

Partager ces journaux avec le support Microsoft pour une investigation approfondie.

1. Diagnostics avancés : Utiliser l'utilitaire de diagnostics avancés pour accéder à un ensemble d'outils de dépannage. Cela inclut la vérification de la connectivité réseau, l'analyse des journaux de sécurité, et la vérification des configurations de stratégies d'accès conditionnel.

Documentation Microsoft :

* Présentation du tableau de bord de l’Accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/concept-traffic-dashboard>.
* Journaux et supervision de l’Accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/concept-global-secure-access-logs-monitoring>.
* Journaux de trafic de l’Accès global sécurisé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-view-traffic-logs>.
* Procédure pour accéder aux journaux d’audit de l’Accès global sécurisé (préversion)  : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-access-audit-logs>.
* Accéder aux journaux d’activité dans Microsoft Entra ID: <https://learn.microsoft.com/fr-fr/entra/identity/monitoring-health/howto-access-activity-logs>.
* Comment utiliser des classeurs avec l’accès sécurisé global : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-use-workbooks> .

## Considérations relatives à l’utilisation de Kerberos pour l’authentification unique (SSO)

### Appareils joints à Microsoft Entra ID – Authentification unique basée sur mot de passe

Une configuration supplémentaire de ce qui est détaillé dans ce guide n’est pas nécessaire si les utilisateurs utilisent des mots de passe pour se connecter à Windows.

Les appareils joints à Microsoft Entra ID s’appuient sur le domaine Active Directory et les informations utilisateur synchronisées par Microsoft Entra ID Connect. Le localisateur de contrôleurs de domaine Windows trouve les contrôleurs de domaine grâce à la synchronisation. Le nom d’utilisateur principal (UPN) et le mot de passe de l’utilisateur sont utilisés pour demander un Ticket-Granting Ticket (TGT) Kerberos.

Documentation Microsoft :

* Fonctionnement de l’authentification unique auprès de ressources locales sur des appareils joints à Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/devices/device-sso-to-on-premises-resources>.

### Appareils hybrides joints à Microsoft Entra ID et appareils joints à Microsoft Entra ID – Authentification unique Windows Hello Entreprise

Une configuration supplémentaire de ce qui se trouve dans ce guide est nécessaire pour Windows Hello Entreprise.

Le déploiement de l’approbation Kerberos cloud hybride avec Microsoft Entra ID est en effet recommandé. Les appareils utilisant l’approbation Kerberos cloud obtiennent un ticket TGT utilisé pour l’authentification unique. Pour en savoir plus sur l’approbation Kerberos cloud, consultez [Activer la connexion de clé de sécurité sans mot de passe aux ressources locales à l’aide de Microsoft Entra ID](https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises#use-sso-to-sign-in-to-on-premises-resources-by-using-fido2-keys).

Pour déployer l’approbation Kerberos cloud de Windows Hello Entreprise avec un Active Directory local, procéder comme suit :

1. Installer un objet serveur Kerberos, Cf. Installer le module AzureADHybridAuthenticationManagement: <https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises#install-the-azureadhybridauthenticationmanagement-module> ;
2. Configurer l’appareil à l'aide de Microsoft Intune ou via une stratégie de groupe (Group Policy Object ou GPO) pour permettre la connexion avec l'Active Directory en local, Cf. Guide de déploiement de l’approbation Kerberos cloud : <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/deploy/hybrid-cloud-kerberos-trust>.

Cette configuration est couverte dans le Guide de configuration de Windows Hello Entreprise à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

## Résolution de problèmes

Comme souligné à la section 4.1.1 Appareils joints à Microsoft Entra ID – Authentification unique basée sur mot de passe ci-dessus, ces appareils s’appuient sur les attributs synchronisés par Microsoft Entra ID Connect.

Vérifier que les attributs onPremisesDomainName, onPremisesUserPrincipalName et onPremisesSamAccountName ont les bonnes valeurs avec :

* L’explorateur Microsoft Graph : <https://developer.microsoft.com/en-us/graph/graph-explorer>.
* PowerShell : .

Si ces valeurs ne sont pas présentes, vérifier les paramètres de synchronisation Microsoft Entra ID Connect et vérifier que ces attributs sont synchronisés.

Documentation Microsoft :

* Synchronisation Microsoft Entra Connect : attributs synchronisés avec Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized>.

Si Windows Hello Entreprise est utilisé comme MIE pour la connexion, procéder comme suit :

1. Ouvrir un invite de commande sans élévation de privilège est exécuter la commande :

C:\> dsregcmd /status

Vérifier que les attributs ont YES en tant que valeurs.

PRT doit être présente, Cf. Résoudre les problèmes de jeton d’actualisation principaux sur les appareils Windows. : <https://learn.microsoft.com/fr-fr/entra/identity/devices/troubleshoot-primary-refresh-token>.

OnPremTgt : YES indique qu’Entra Kerberos est correctement configuré et que l’utilisateur a reçu une requête TGT partielle pour l’authentification unique sur les ressources locales, Pour la configuration de l’approbation Kerberos cloud, nous invitons le lectorat à consulter Connexion avec clé de sécurité sans mot de passe à des ressources locales. : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises#install-the-azureadhybridauthenticationmanagement-module>.

1. Exécuter la commande :

C:\> klist cloud\_debug

Vérifier que le champ Cloud Primary (Hybrid logon) TGT available: a la valeur 1.

1. Exécuter la commande :

C:\> nltest /dsgetdc:contoso /keylist /kdc

Vérifier que le localisateur de contrôleur de domaine retourne un contrôleur de domaine participant aux opérations d’approbation Kerberos cloud. Le contrôleur de domaine retourné doit avoir l’indicateur klist.

A ce stade, le guide suppose que Microsoft Entra Private Access est configuré pour le locataire Entra ID de l’ES, que le client GSA est déployés sur des appareils (de test).

Les chapitres suivants couvrent plus précisément les protocoles RDP et SMB.

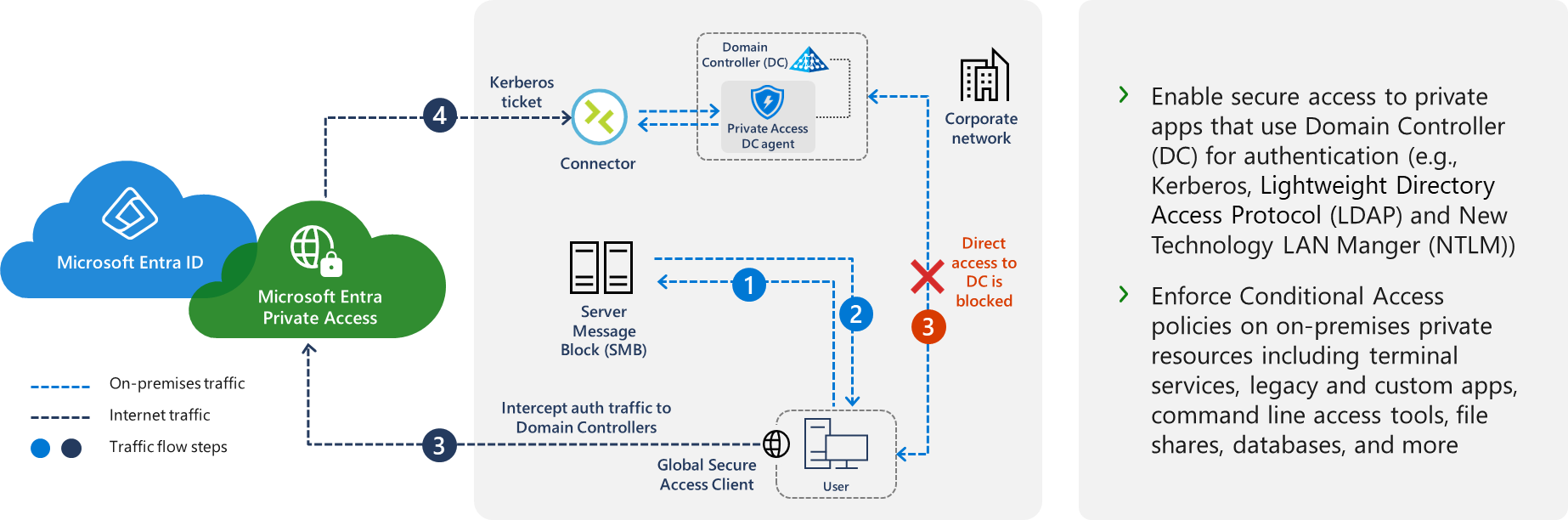
# Accès privé aux ressources RDP

Microsoft Entra Private Access permet un accès sécurisé aux ressources héritées via le protocole RDP (Remote Desktop Protocol).

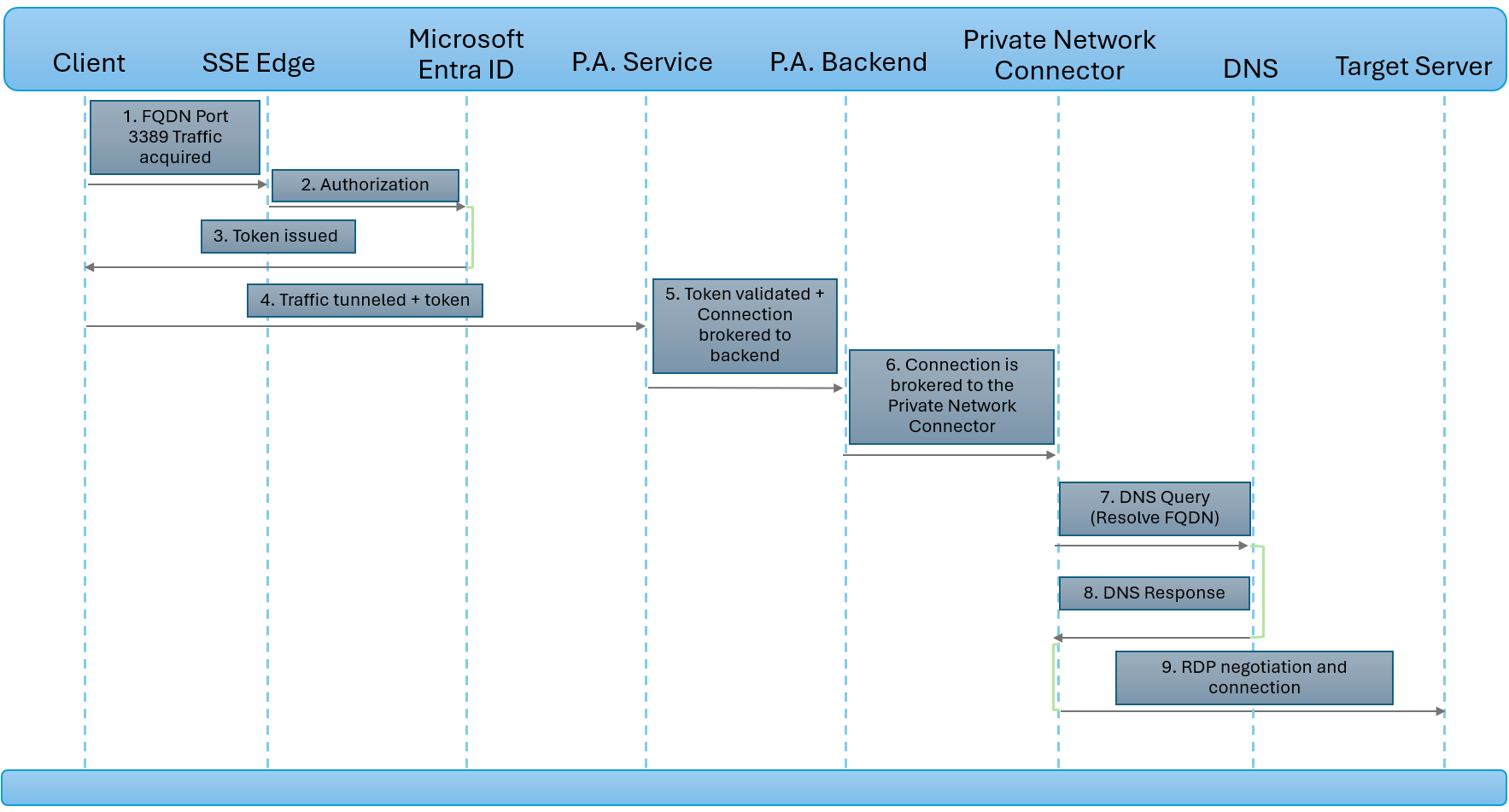
## Etapes de mise en œuvre

La mise en œuvre suppose que les étapes suivantes sont réalisés dans le cadre de la configuration de l’Accès rapide ou de l’Accès par application, Cf. sections 5.3.2 Configuration de l’Accès rapide ci-dessus ou 5.4.2 Configuration l’Accès par application ci-dessus :

1. Déploiement et configuration des connecteurs ainsi que de l’Accès rapide ou de l’Accès par application pour prendre en charge les sessions RDP et les exigences de sécurité.
2. Configuration de stratégies d'accès conditionnel pour les sessions RDP intégrant l’authentification multifacteur (MFA) ainsi que des vérifications de conformité des appareils.
3. Activation de l'authentification unique pour les sessions RDP à l’aide du protocole Kerberos.



Le diagramme montre comment l’accès privé Microsoft Entra fonctionne lors d’une tentative d’utilisation du protocole RDP (Remote Desktop Protocol) pour se connecter à un serveur sur un réseau privé.

[](https://learn.microsoft.com/fr-fr/entra/global-secure-access/media/how-to-configure-per-app-access/private-access-remote-desktop-protocol-network-diagram.png#lightbox)

|  |  |
| --- | --- |
| Etape | Description |
| 1 | L’utilisateur initie une session RDP vers un nom de domaine complet qui correspond au serveur cible. Le client GSA intercepte le trafic et l’achemine vers le SSE Edge. |
| 2 | Le SSE Edge évalue les stratégies stockées dans Microsoft Entra ID, il vérifie par exemple si l’utilisateur est affecté à l’application et aux stratégies d’accès conditionnel. |
| 3 | Une fois l’utilisateur autorisé, Microsoft Entra ID émet un jeton pour l’application d’accès privé. |
| 4 | Le trafic est libéré et continue vers le service d’accès privé avec le jeton d’accès de l’application. |
| 5 | Le service d’accès privé valide le jeton d’accès et la connexion est acheminée vers le service principal d’accès privé. |
| 6 | La connexion est acheminée vers le connecteur de réseau privé. |
| 7 | Le connecteur de réseau privé effectue une requête DNS pour identifier l’adresse IP du serveur cible. |
| 8 | Le service DNS du réseau privé envoie la réponse. |
| 9 | Le connecteur de réseau privé transfère le trafic vers le serveur cible. La session RDP est négociée (notamment l’authentification RDP), puis est établie. |

Documentation Microsoft :

* RDP (Remote Desktop Protocol) pour se connecter à un serveur sur un réseau privé : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-per-app-access#enable-microsoft-entra-private-access>.

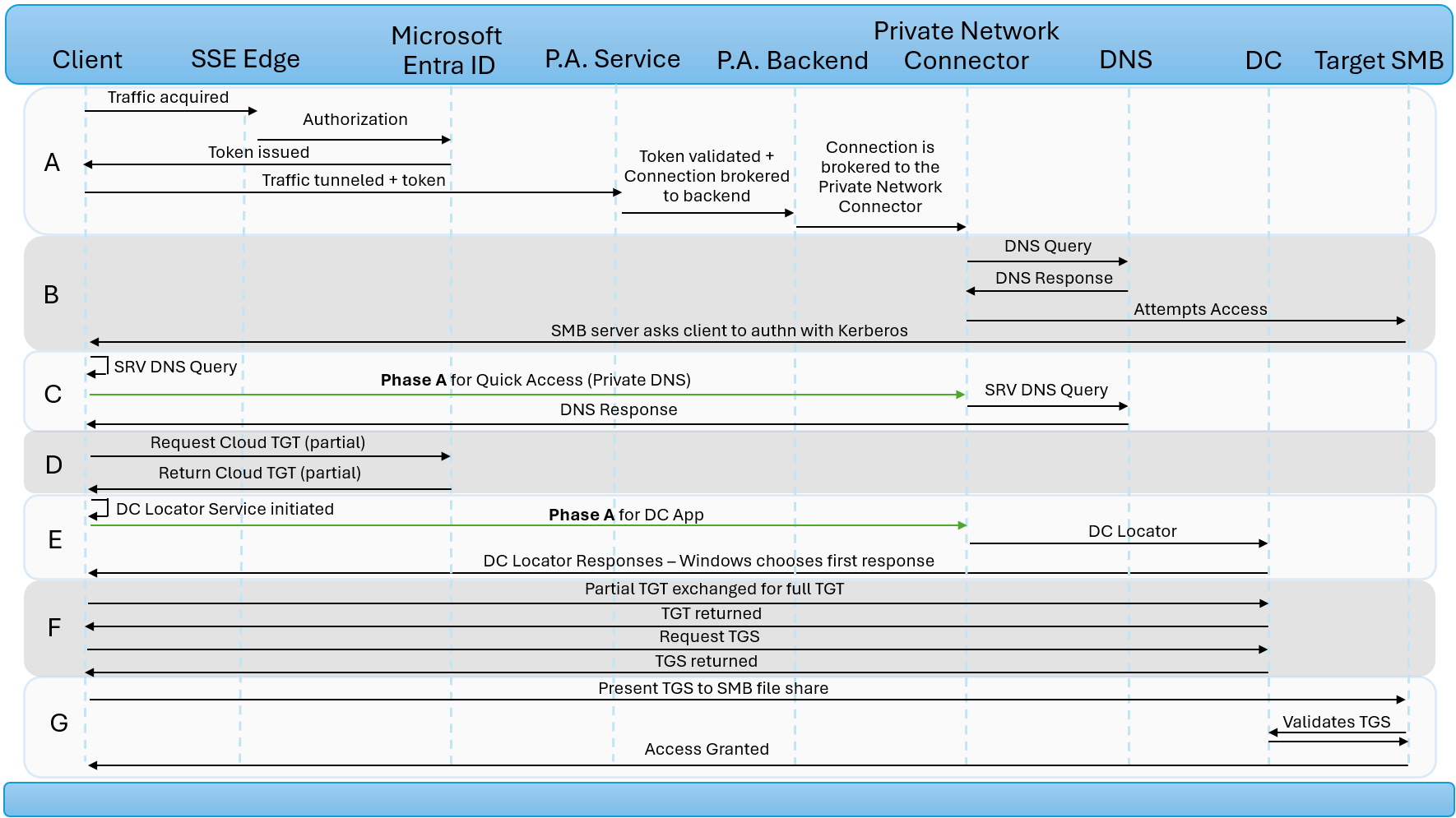
## Problèmes courants et solutions pour les connexions RDP

1. Problème : Échec de la connexion RDP avec un message d'erreur d'authentification.
   1. Solution : Vérifier que les stratégies d'accès conditionnel sont correctement configurées et que les utilisateurs ont activé l’authentification multifacteur (MFA). S’assurer également que les connecteurs sont correctement configurés pour gérer les exigences de sécurité exprimées.
2. Problème : Latence élevée ou connexion RDP lente.
   1. Solution : Vérifier la configuration réseau et s’assurer que les connecteurs sont déployés dans des emplacements optimaux pour minimiser la latence. Utiliser le réseau privé mondial de Microsoft pour améliorer le cas échéant les performances.
3. Problème : Les utilisateurs ne peuvent pas accéder aux ressources RDP après l'activation de la MFA.
   1. Solution : S’assurer que les appareils (Windows) des utilisateurs sont conformes aux stratégies d’accès conditionnel et que l’authentification multifacteur (MFA) est correctement configurée pour les MIE pris en charge et déployés.

# Accès privé aux ressources SMB

L’accès privé aux ressources SMB (Server Message Block) nécessite d’ajouter un nouveau segment d’application pour l’Accès rapide ou l’Accès privé avec l’adresse IP du serveur de fichiers à l’aide du port 445/TCP utilisé par le protocole SMB, Cf. sections 5.3.2 Configuration de l’Accès rapide ci-dessus ou 5.4.2 Configuration l’Accès par application ci-dessus.

Ce diagramme montre comment Accès privé Microsoft Entra fonctionne lorsqu'on essaie d'accéder à un partage de fichiers SMB à partir d'un appareil Windows qui est configuré avec Windows Hello Entreprise + Cloud Trust. Dans cet exemple, l’administrateur a configuré le DNS privé d’accès rapide et deux applications d’entreprise : une pour les contrôleurs de domaine et un pour le partage de fichiers SMB.



|  |  |
| --- | --- |
| Etape | Description |
| A | L’utilisateur tente d’accéder au partage de fichiers SMB à l’aide du nom de domaine complet. Le client GSA intercepte le trafic et l’achemine vers le SSE Edge. Les stratégies d’autorisation dans Microsoft Entra ID sont évaluées et appliquées, par exemple si l’utilisateur est affecté à l’application et à l’accès conditionnel. Une fois l’utilisateur autorisé, Microsoft Entra ID émet un jeton pour l’application d’entreprise SMB. Le trafic est libéré et continue vers le service d’accès privé avec le jeton d’accès de l’application. Le service d’accès privé valide le jeton d’accès et la connexion est acheminée vers le service principal d’accès privé. La connexion est ensuite répartie sur le connecteur de réseau privé. |
| B | Le connecteur de réseau privé effectue une requête DNS pour identifier l’adresse IP du serveur cible. Le service DNS du réseau privé envoie la réponse. Le connecteur de réseau privé tente d’accéder au partage de fichiers SMB cible, qui demande ensuite l’authentification Kerberos. |
| C | Le client génère une requête DNS SRV pour localiser les contrôleurs de domaine. La phase A est répétée, interceptant la requête DNS et autorisant l’utilisateur pour l’application Accès rapide. Le connecteur de réseau privé envoie la requête DNS SRV au réseau privé. Le service DNS envoie la réponse DNS au client via le connecteur de réseau privé. |
| D | L’appareil Windows demande un TGT partiel (également appelé TGT cloud) à partir de Microsoft Entra ID (s’il n’en a pas déjà). Microsoft Entra ID émet un TGT partiel. |
| E | Windows lance une connexion de localisateur DC sur le port UDP 389 avec chaque contrôleur de domaine répertorié dans la réponse DNS de la phase C. La phase A est répétée, interceptant le trafic du localisateur DC et autorisant l’utilisateur pour l’application Entreprise qui publie les contrôleurs de domaine locaux. Le connecteur de réseau privé envoie le trafic du localisateur DC à chaque contrôleur de domaine. Les réponses sont relayées vers le client. Windows sélectionne et met en cache le contrôleur de domaine avec la réponse la plus rapide. |
| F | Le client échange le TGT partiel pour un TGT complet. Le TGT complet est ensuite utilisé pour demander et recevoir un TGS pour le partage de fichiers SMB. |
| G | Le client présente le TGS au partage de fichiers SMB. Le partage de fichiers SMB valide le TGS. L’accès au partage de fichiers est accordé. |

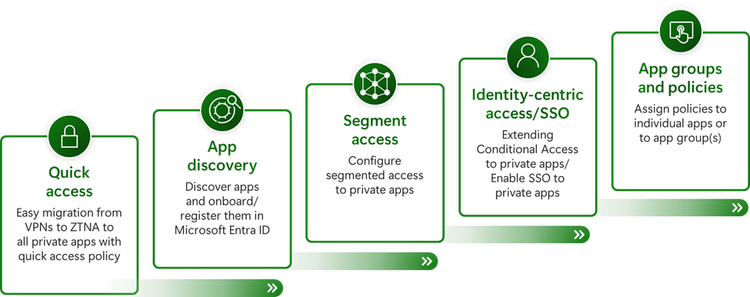
Documentation Microsoft :

* Comment utiliser l’authentification unique Kerberos pour accéder à un partage de fichiers SMB : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/how-to-configure-kerberos-sso#how-to-use-kerberos-sso-to-access-an-smb-file-share>.

# Conclusion

Simplifier et sécuriser l'accès est crucial dans un paysage hybride où les frontières traditionnelles se sont dissoutes. L'application de l'accès au moindre privilège et la réduction de la dépendance à l'égard d'outils hérités sont des étapes essentielles pour réduire les risques et atténuer les cyberattaques sophistiquées.

Microsoft Entra Private Access aide à accélérer la transition de l’ES vers le ZTNA et répond à ce besoin en proposant une approche rationalisée pour aider à appliquer l'accès à moindre privilège aux applications locales ou privées, renforçant ainsi l'importance d'étendre les principes Zero Trust à toutes les applications ou ressources privées, quel que soit leur emplacement, sur site ou dans n'importe quel cloud – via le cas échéant la plateforme Pro Santé Connect (PSC) pour les ressources pertinentes -.

****

Microsoft Entra Private Access permet de sécuriser l’accès à l’ensemble des applications et ressources privées de l’ES pour les PS, le personnel administratif et de direction, et les autres personnels de l’ES, où qu’ils soient, grâce à une solution ZTNA centrée sur l’identité et le contexte de la demande, plutôt que sur le réseau depuis lequel l’accès est demandé.

L’approche unifiée de l’identité et de l’accès au réseau au sein de la solution SASE (Secure Access Service Edge) de Microsoft marque le début d’une nouvelle ère de la sécurité réseau. Cette approche garantit que seuls les utilisateurs autorisés sont authentifiés et que leurs appareils (Windows 10 ou ultérieur) sont conformes avant d’accéder aux ressources privées sans exposer un accès réseau complet à l’ensemble du patrimoine numérique de l’ES.

A ce propos, l’une des caractéristiques distinctives de cette solution SASE est sa compatibilité intégrée avec les solutions d’accès réseau tierces, où elle permet d’acquérir uniquement le trafic dont l’ES a besoin pour envoyer aux périphéries SASE de Microsoft.

L’écosystème de partenaires SASE de Microsoft est conçu pour fournir une infrastructure de sécurité flexible et robuste à l’ES. Microsoft collabore avec les grands fournisseurs de sécurité pour veiller à ce que sa solution SASE puisse s’intégrer en toute transparence à divers produits non fournis par Microsoft.

Documentation Microsoft :

* Vue d’ensemble de l’écosystème de partenaires : <https://learn.microsoft.com/fr-fr/entra/global-secure-access/partner-ecosystems-overview>.

Il est ainsi possible de tirer parti des solutions d’accès au réseau de Microsoft et de tierces parties dans un environnement unifié pour exploiter un ensemble robuste de fonctionnalités des deux solutions afin d’accélérer la transition de l’ES vers la « Confiance Zéro » ou Zero Trust.

Les options de déploiement flexibles de cette solution SASE de Microsoft offrent ainsi à l’ES une sécurité renforcée et une connectivité transparente pour une expérience utilisateur optimale.

Ceci conclut le présent guide.