Citrix Secure Private Access

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Citrix Secure Private Access

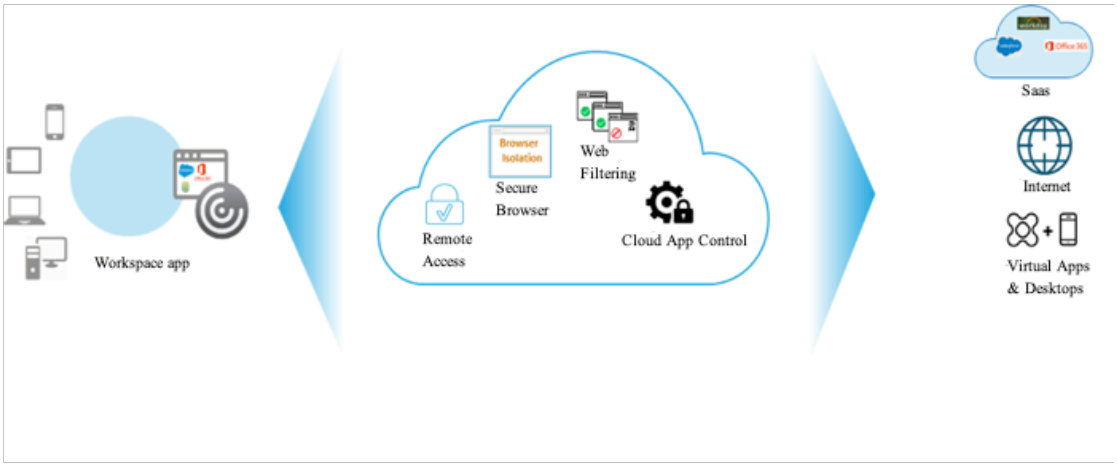
October 21, 2024

Le service Citrix Secure Private Access permet aux administrateurs de fournir une expérience cohérente intégrant l'authentification unique, l'accès à distance et l'inspection du contenu dans une solution unique pour un contrôle d'accès de bout en bout. Les administrateurs informatiques peuvent gérer l'accès aux applications SaaS approuvées avec une expérience d'authentification unique simplifiée. Avec le service Citrix Secure Private Access, les administrateurs peuvent également protéger le réseau de l'organisation et les appareils des utilisateurs finaux contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et à des catégories de sites Web spécifiques. Les administrateurs peuvent appliquer des politiques de sécurité d'accès améliorées pour un accès sécurisé aux applications SaaS. Une fois authentifiés, les employés ont accès à toutes les applications professionnelles critiques à partir de n'importe quel appareil, qu'ils se trouvent dans les locaux du bureau, à la maison ou en déplacement.

Les administrateurs peuvent surveiller les activités des utilisateurs, telles que les sites Web malveillants, dangereux ou inconnus visités, la bande passante consommée et les comportements de téléchargement et de chargement risqués. En utilisant les analyses autour des sites Web et des catégories de sites Web consultés, les administrateurs peuvent prendre des mesures correctives pour protéger le réseau de l'entreprise. Dans le même temps, le service offre aux utilisateurs finaux un accès transparent et sécurisé à toutes leurs applications hébergées.

Les administrateurs peuvent également restreindre les actions, telles que l'impression restreinte, les téléchargements et l'accès au presse-papiers (copier-coller).

Le diagramme suivant est une représentation visuelle du service Secure Private Access.



Principales fonctionnalités de Citrix Secure Private Access

Voici quelques-unes des tâches clés que vous pouvez effectuer avec le service Citrix Secure Private Access :

- **Publiez des applications SaaS avec un accès à authentification unique** - Une fois que l'utilisateur est authentifié sur Citrix Workspace avec une identité principale, les défis d'authentification ultérieurs pour les applications SaaS et Web sont automatiquement satisfaits par la fonctionnalité d'authentification unique dans Citrix Cloud à l'aide d'assertions SAML.

Par défaut, l'assertion SAML utilise l'adresse e-mail associée au compte Active Directory de l'utilisateur (fournisseur d'identité) avec l'adresse e-mail associée au compte SaaS ou d'application Web de l'utilisateur (fournisseur de services).

- **Définissez des politiques de sécurité améliorées pour les applications SaaS. (Par exemple, filigrane, restriction de copier-coller et empêchement des téléchargements.)** - Pour protéger le contenu, les organisations intègrent des politiques de sécurité renforcées au sein des applications SaaS. Chaque politique applique une restriction sur le navigateur Citrix Enterprise lors de l'utilisation de l'application Workspace pour ordinateur de bureau ou sur Secure Browser lors de l'utilisation de l'application Workspace Web ou mobile.
  - Navigateur préféré : désactive l'utilisation du navigateur local et s'appuie sur le moteur de navigateur Citrix Enterprise (application Workspace - bureau) ou sur le navigateur sécurisé (application Workspace - mobile et Web).

  - Restreindre l'accès au presse-papiers : désactive les opérations couper/copier/coller entre l'application et le presse-papiers du point de terminaison.
  - Restreindre l'impression : désactive la possibilité d'imprimer à partir du navigateur de l'application.
  - Restreindre les téléchargements : désactive la capacité de l'utilisateur à télécharger depuis l'application SaaS.
  - Afficher le filigrane : superpose un filigrane sur l'écran indiquant le nom d'utilisateur et l'adresse IP du point de terminaison. Si un utilisateur essaie d'imprimer ou de prendre une capture d'écran, le filigrane apparaît tel qu'affiché à l'écran.

- **Fournir un accès contextuel** - Bien qu'une application SaaS autorisée soit considérée comme sûre, le contenu de l'application SaaS peut en réalité être dangereux, constituant ainsi un risque de sécurité. Lorsqu'un utilisateur clique sur un lien hypertexte dans une application SaaS, le trafic est acheminé via la fonction de filtrage Web, qui fournit une évaluation des risques pour le lien hypertexte. En fonction de l'évaluation des risques du lien hypertexte et de la liste personnalisée des catégories d'URL, la fonction de filtrage Web autorise, refuse ou redirige la demande d'hyperlien de l'utilisateur comme suit :

  - Approuvé : le lien hypertexte est considéré comme sécurisé et le navigateur Citrix Enterprise accède au sein de l'application Workspace et accède au lien hypertexte.
  - Refusé : L'hyperlien est considéré comme dangereux et l'accès est refusé.
  - Redirigé : la demande d'hyperlien est redirigée vers le service Secure Browser, où les activités de navigation Internet de l'utilisateur sont isolées du périphérique terminal, du réseau d'entreprise et de l'application SaaS.

- **Analyse de la sécurité et des performances** - Les utilisateurs accèdent invariablement à des applications SaaS dotées d'une sécurité renforcée inhérente. L'application Workspace, le service Secure Private Access et le service Secure Browser fournissent au service d'analyse de sécurité des informations sur les comportements des utilisateurs et des applications suivants. Ces analyses ont un impact sur le score de risque global de l'utilisateur :

  - Heure de lancement de l'application
  - Heure de fin de l'application
  - Action d'impression
  - Accès au presse-papiers
  - Accès URL
  - Téléchargement de données
  - Téléchargement de données

- **Filtrage Web :** La fonctionnalité de filtrage Web évalue le risque de chaque lien hypertexte sélectionné dans l'application SaaS. L'accès à ces sites et la surveillance des changements de comportement des utilisateurs augmentent le score de risque global de l'utilisateur, car cela signale

que le périphérique terminal est compromis et a commencé à infecter ou à crypter des données ou que l'utilisateur et l'appareil volent la propriété intellectuelle.

- **Intégration avec la gestion des informations et des événements de sécurité (SIEM)** - Les journaux d'accès privé sécurisé peuvent être exportés via Kafka vers SIEM tels que Splunk, Sentinel et Elastic. L'exportation des journaux vers SIEM améliore les capacités de sécurité et améliore l'efficacité de la réponse aux incidents. Pour plus de détails, voir Événements d'accès privé sécurisé.

Nouveautés

October 21, 2024

23 septembre 2024

- **Prise en charge du routage des applications basé sur le contexte et de la sélection des emplacements des ressources**

  La configuration du routage de domaine dynamique dans la politique d'accès permet désormais aux administrateurs de modifier le type de routage interne par URL en fonction du contexte de l'utilisateur. Les administrateurs peuvent modifier les emplacements des ressources afin que les demandes des utilisateurs soient acheminées vers le centre de données optimal, garantissant ainsi que les demandes des utilisateurs sont traitées efficacement et que les performances sont optimisées. Pour plus de détails, voir Routage d'application basé sur le contexte et sélection des emplacements des ressources.

15 août 2024

- **Option permettant de configurer une durée de purge des entrées dans la liste des utilisateurs bloqués**

  Les administrateurs peuvent désormais définir une durée spécifique (1 à 99 jours) pour purger les entrées de la liste des utilisateurs bloqués. Pour plus de détails, voir Mettre fin aux sessions utilisateur actives et ajouter des utilisateurs à la liste de blocage des utilisateurs.

- **Contrôles de sécurité supplémentaires**

  Les contrôles de sécurité supplémentaires suivants sont désormais disponibles pour restreindre l'accès aux applications.

  - Microphone

  - Webcam
  - Notifications
  - Pop-ups
  - Contenu non sécurisé

  Pour plus de détails, voir Options de restriction d'accès.

- **Améliorations apportées à la fonctionnalité de filtrage des sites Web non autorisés**

  La fonctionnalité de sites Web non autorisés (filtrage Web) permet aux administrateurs de bloquer l'accès à tout trafic non autorisé par défaut ou de l'autoriser par défaut via Citrix Enterprise Browser. Pour plus de détails, voir Sites Web non autorisés.

16 juillet 2024

- **Contrôles de sécurité supplémentaires**

  Les contrôles de sécurité supplémentaires suivants sont disponibles pour restreindre l'accès aux applications.

  - Restriction de téléchargement par type de fichier
  - Restriction de téléchargement par type de fichier
  - Masquage des données personnelles
  - Gestion des imprimantes
  - Restriction du presse-papiers pour les groupes de sécurité

  Pour plus de détails, voir Options de restriction d'accès.

- **Affichage des domaines intégrés dans la page de découverte d'applications**

  La fonctionnalité de découverte d'applications permet aux administrateurs de créer de nouvelles applications ou d'ajouter ces domaines à une application existante si un domaine principal ou un domaine intégré (HTTP/HTTPS) ou l'adresse IP de destination (TCP/UDP) n'est pas associé à une application. La page **Découverte d'applications** affiche à la fois le domaine principal et ses domaines intégrés sous-jacents dans une structure arborescente. Pour plus de détails, voir Découvrir les domaines ou les adresses IP auxquels accèdent les utilisateurs finaux.

11 juin 2024

- **Outil de modélisation des politiques**

  L'outil de modélisation des politiques (**Politiques d'accès > Modélisation des politiques**) aide les administrateurs à analyser et à résoudre les problèmes de configuration depuis la console d'administration. Pour plus de détails, voir Outil de modélisation des politiques.

- **Prise en charge des filtres dans le graphique des journaux de diagnostic**

  L'option de filtre dans le graphique **Journaux de diagnostic** aide les administrateurs à affiner la recherche en fonction de différents critères tels que le type d'application, la catégorie et la description pour une analyse et un dépannage plus faciles des journaux. Pour plus de détails, voir Journaux de diagnostic.

13 mars 2024

- **Prise en charge de la fin des sessions utilisateur actives et de l'ajout d'utilisateurs à la liste des utilisateurs désactivés**

  Les administrateurs peuvent désormais mettre fin immédiatement à toutes les sessions d'utilisateurs finaux actifs et ajouter les utilisateurs à la liste des utilisateurs désactivés. L'ajout d'un utilisateur à cette liste d'utilisateurs désactivés met fin à toutes les sessions d'application Secure Private Access actives et bloque l'accès futur à l'application. Pour plus de détails, voir Mettre fin aux sessions utilisateur actives et ajouter des utilisateurs à la liste des utilisateurs désactivés.

12 février 2024

- **Disponibilité générale du navigateur et des analyses antivirus**

  Les analyses de navigateur et d'antivirus prises en charge par le service Device Posture sont désormais généralement disponibles. Pour plus de détails, voir Analyses prises en charge par la posture de l'appareil.

23 janvier 2024

- **Disponibilité générale de la vérification du certificat de l'appareil avec le service Device Posture**

  La vérification du certificat de l'appareil avec le service Device Posture est désormais généralement disponible. Pour plus de détails, voir Vérification du certificat de l'appareil avec le service Device Posture.

20 décembre 2023

- **Disponibilité générale de Secure Private Access sur site**

  Citrix Secure Private Access pour les locaux est désormais disponible en version générale. Pour plus de détails, voir Quoi de neuf.

16 octobre 2023

- **Aperçu des fonctionnalités de la solution sur site Secure Private Access**

  La solution sur site Secure Private Access offre désormais les fonctionnalités suivantes :

  - Interface utilisateur d'administration pour la première configuration.
  - Interface d'administration pour la configuration des applications et des politiques d'accès.
  - Tableau de bord des journaux.

  Pour plus de détails, voir Accès privé sécurisé pour les locaux.

- **Aperçu des fonctionnalités du service Device Posture**

  Le service Device Posture prend désormais en charge les vérifications suivantes :

  - Le service Device Posture est désormais pris en charge sur les plates-formes IGEL.
  - Le service Device Posture prend désormais en charge les vérifications de géolocalisation et de localisation réseau.

  Pour plus de détails, consultez la section Posture de l'appareil.

11 septembre 2023

- **Disponibilité générale de l'intégration de Device Posture avec Microsoft Intune**

  L'intégration de la posture de l'appareil avec Microsoft Intune est désormais disponible au grand public. Pour plus de détails, voir Intégration de Microsoft Intune avec Device Posture.

30 août 2023

- **Gérer le client Citrix Endpoint Analysis pour le service Device Posture**

  Le client EPA peut être utilisé avec NetScaler et Device Posture. Certaines modifications de configuration sont nécessaires pour gérer le client EPA lorsqu'il est utilisé avec NetScaler et Device Posture. Pour plus de détails, voir Gérer le client Citrix Endpoint Analysis pour le service Device Posture.

28 août 2023

- **Prise en charge du service Device Posture sur les plateformes iOS**

  Le service Device Posture est désormais pris en charge sur les plateformes iOS. Pour plus de détails, consultez la section Posture de l'appareil.

Cette fonctionnalité est disponible dans la Tech Preview.

22 août 2023

- **Vérification du certificat de l'appareil avec le service Citrix Device Posture**

  Le service Citrix Device Posture peut désormais activer l'accès contextuel (Smart Access) aux ressources Citrix DaaS et Secure Private Access en vérifiant le certificat du périphérique final par rapport à une autorité de certification d'entreprise pour déterminer si le périphérique final est fiable. Pour plus de détails, voir Vérification du certificat de l'appareil avec le service Device Posture.

  Cette fonctionnalité est disponible dans la Tech Preview.

17 août 2023

- **Événements de posture de l'appareil sur Citrix DaaS Monitor**

  Les événements du service Device Posture et les journaux de surveillance sont désormais consultables sur DaaS Monitor. Pour plus de détails, consultez Événements de posture de l'appareil sur Citrix DaaS Monitor.

07 juin 2023

- **Outil de configuration de l'accès privé sécurisé sur site**

  Une interface utilisateur simplifiée est désormais disponible pour configurer la solution Secure Private Access sur site. L'outil de configuration peut être exécuté sur un contrôleur de distribution Citrix Virtual Apps and Desktops pour créer rapidement une application SaaS ou Web. En outre, vous pouvez utiliser cet outil pour définir des restrictions d'application, le routage du trafic et les paramètres de NetScaler Gateway. Pour plus de détails, voir /en-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html.

29 May 2023

- **Disponibilité générale de la création de politiques d'accès avec plusieurs règles**

  Vous pouvez créer plusieurs règles d'accès et configurer différentes conditions d'accès pour différents utilisateurs ou groupes d'utilisateurs au sein d'une même politique. Ces règles peuvent être appliquées séparément pour les applications HTTP/HTTPS et TCP/UDP, le tout au sein d'une seule politique. Pour plus de détails, voir Configurer une politique d'accès avec plusieurs règles.

[SPA-746]

10 avril 2023

- **Découverte d'applications**

  La fonctionnalité de découverte d'applications aide un administrateur à obtenir une visibilité sur les applications privées internes telles que les applications Web et les applications client-serveur (applications basées sur TCP et UDP) dans son organisation et les utilisateurs accédant à ces applications. Les administrateurs peuvent découvrir les applications en spécifiant la portée des domaines (domaines génériques) ou des sous-réseaux IP. Pour plus de détails, voir Découverte d'applications.

  [ACS-2325]

29 mars 2023

- **Solution d'accès privé sécurisé pour les déploiements sur site**

  En tant que client Citrix StoreFront et NetScaler Gateway, vous pouvez désormais accéder de manière transparente aux applications Web et SaaS ainsi qu'aux applications virtuelles Citrix et aux postes de travail virtuels à l'aide de la solution Citrix Secure Private Access pour les déploiements sur site. Pour plus de détails, voir Accès privé sécurisé pour les locaux.

  [SPAOP-1]

07 mars 2023

- **Configurer les suffixes DNS**

  La fonctionnalité de suffixe DNS du service Citrix Secure Private Access peut être utilisée pour les cas d'utilisation suivants :

  - Permettez au client Citrix Secure Access de résoudre un nom de domaine non entièrement qualifié (nom d'hôte) en un nom de domaine complet (FQDN) en ajoutant le suffixe DNS du domaine pour les serveurs principaux.
  - Permettre aux administrateurs de configurer des applications à l'aide d'adresses IP (IP CIDR/plage IP), afin que les utilisateurs finaux puissent accéder aux applications à l'aide du FQDN correspondant sous le domaine de suffixe DNS.

  Pour plus de détails, voir Suffixes DNS pour résoudre les FQDN en adresses IP.

  [ACS-2490]

23 janvier 2023

- **Service de maintien de l'appareil**

  Le service Citrix Device Posture est une solution basée sur le cloud qui aide les administrateurs à appliquer certaines exigences auxquelles les appareils finaux doivent répondre pour accéder aux ressources Citrix DaaS (applications et postes de travail virtuels) ou Citrix Secure Private Access (applications SaaS, Web, TCP et UDP). Pour plus de détails, consultez la section Posture de l'appareil.

  [AAUTH-90]

- **Intégration de Microsoft Endpoint Manager avec Device Posture**

  En plus des analyses natives proposées par le service Device Posture, le service Device Posture peut également être intégré à d'autres solutions tierces. Device Posture est intégré à Microsoft Endpoint Manager (MEM) sur Windows et macOS. Pour plus de détails, voir Intégration de Microsoft Endpoint Manager avec Device Posture.

  [ACS-1399]

22 décembre 2022

- **Prise en charge de l'authentification unique pour l'URL de l'espace de travail pour les utilisateurs connectés via l'application Citrix Workspace**

  Le client Citrix Secure Access prend désormais en charge l'authentification unique pour l'URL de l'espace de travail lorsqu'il est déjà connecté via l'application Citrix Workspace. Cette fonctionnalité SSO améliore l'expérience utilisateur en évitant les authentifications multiples. Pour plus de détails, voir Prise en charge de l'authentification unique pour l'URL de l'espace de travail.

  [ACS-1888]

- **Activer l'accès aux applications à l'aide de politiques d'accès**

  Pour accorder l'accès aux applications aux utilisateurs, les administrateurs doivent désormais créer des politiques d'accès avec une liste d'abonnements utilisateurs correspondante pour que les applications soient disponibles pour les utilisateurs finaux. Auparavant, les administrateurs devaient ajouter des utilisateurs en tant qu'abonnés pour permettre l'accès. Pour plus de détails, voir Créer des politiques d'accès.

  [ACS-3018]

03 octobre 2022

- **Politiques d'accès pour accorder l'accès aux applications**

  L'option de configuration des abonnés à l'application est supprimée de la section Applications de l'assistant de configuration. Pour accorder l'accès aux applications aux utilisateurs, les administrateurs doivent créer des politiques d'accès. Dans les politiques d'accès, les administrateurs ajoutent des abonnés aux applications et configurent les contrôles de sécurité. Pour plus de détails, voir Créer des politiques d'accès.

  [ACS-3018]

- **Prise en charge des applications UDP**

  Le service Secure Private Access prend désormais en charge l'accès aux applications UDP. Pour plus de détails, voir Fonctionnalités d'aperçu.

  [ACS-1430]

09 septembre 2022

- **Accès adaptatif basé sur le score de risque de l'utilisateur**

  Les administrateurs peuvent désormais configurer une politique d'accès adaptative avec le score de risque utilisateur fourni par Citrix Analytics for Security (CAS). Pour plus de détails, voir Accès adaptatif basé sur le score de risque de l'utilisateur.

  [ACS-877]

- **Accès adaptatif en fonction de l'emplacement réseau de l'utilisateur**

  Les administrateurs peuvent désormais configurer la politique d'accès adaptative en fonction de l'emplacement à partir duquel l'utilisateur accède à l'application. L'emplacement peut être le pays à partir duquel l'utilisateur accède à l'application ou l'emplacement réseau de l'utilisateur. Pour plus de détails, voir Accès adaptatif basé sur l'emplacement.

  [ACS-99]

- **Générateur de politiques d'accès adaptatif amélioré**

  L'accès aux applications est désormais activé uniquement une fois les conditions configurées remplies. L'abonnement aux applications seul ne donne pas à vos clients l'accès aux applications. Les administrateurs doivent ajouter des politiques d'accès pour fournir l'accès aux applications en plus de l'abonnement à l'application. De plus, les utilisateurs ou les groupes sont une condition obligatoire dans les politiques d'accès qui doivent être respectées pour accéder aux applications. Pour plus de détails, voir Créer des politiques d'accès.

  [ACS-1850]

- **Limiter les téléchargements de fichiers dans les applications SaaS/Web**

  Cette fonctionnalité permet aux administrateurs clients de contrôler (autoriser ou restreindre) qui peut télécharger des fichiers dans leurs applications stratégiques. Grâce à cela, seuls les utilisateurs autorisés peuvent télécharger des fichiers dans les applications. Pour plus de détails, voir Créer des politiques d'accès.

  [ACS-655]

- **Tableau de bord amélioré**

  Le tableau de bord Secure Private Access offre désormais une visibilité détaillée sur plusieurs mesures utilisateur telles que l'utilisation des applications, les principaux utilisateurs d'applications, les principales applications consultées, les journaux de diagnostic, etc. Pour plus de détails, voir Tableau de bord.

  [ACS-2480]

- **Abandon de la bibliothèque**

  Les applications Secure Private Access ne sont désormais plus visibles dans la bibliothèque Citrix Cloud. Toutes les applications configurées pour Secure Private Access se trouvent dans la section des applications de la mosaïque du service Secure Private Access. Cela aide les administrateurs à naviguer, modifier et configurer facilement les applications.

  [ACS-1546]

- **Journaux d'audit pour l'accès privé sécurisé**

  Les événements liés au service Citrix Secure Private Access sont désormais capturés dans le journal système **Citrix Cloud > .** Pour plus de détails, voir Journaux d'audit.

  [ACS-876]

- **Journaux de diagnostic pour l'accès aux applications Web et SaaS d'entreprise**

  Les événements Citrix Secure Private Access sont désormais intégrés à Citrix Analytics. Citrix Analytics fournit un point de terminaison public qui permet aux administrateurs d'accéder aux événements et de les télécharger. Ces événements sont accessibles via un script PowerShell. Pour plus de détails, voir Journaux de diagnostic pour l'accès aux applications Web et SaaS d'entreprise.

  [ACS-805]

- **Guide de dépannage**

  Les administrateurs peuvent utiliser le guide de dépannage pour résoudre les problèmes liés à la configuration. Pour plus de détails, consultez Résoudre les problèmes liés aux applications.

  [ACS-2719]

15 juillet 2022

- **Activer l'accès à une application uniquement si une politique d'accès est configurée**

  L'accès aux applications est désormais activé uniquement après que l'administrateur a ajouté une politique d'accès en plus de l'abonnement à l'application. L'abonnement à l'application seul ne permet pas d'accéder aux applications. Avec ce changement, les administrateurs peuvent appliquer une sécurité adaptative en fonction du contexte, comme les utilisateurs, l'emplacement, l'appareil et le risque. Les administrateurs doivent migrer les contrôles de sécurité des applications et les politiques d'accès existants vers le nouveau cadre de politique d'accès. Pour plus de détails, voir Migration des contrôles de sécurité des applications et des politiques d'accès.

  [ACS-1850]

01 juin 2022

- **Service d'authentification adaptative**

  L'authentification adaptative est désormais généralement disponible (GA). Pour des informations détaillées sur l'authentification adaptative, consultez Service d'authentification adaptative.

  [CGS-6510]

04 avril 2022

- **Changements liés au rebranding**

  Le service Citrix Secure Workspace Access est désormais renommé service Citrix Secure Private Access.

  [ACS-2322]

- **Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles**

  Secure Private Access dispose désormais d'une nouvelle expérience d'administration simplifiée avec un processus étape par étape pour configurer l'accès réseau Zero Trust aux applications SaaS, aux applications Web internes et aux applications TCP. Il comprend la configuration de l'authentification adaptative, des applications incluant l'abonnement utilisateur, les politiques d'accès adaptatif et d'autres au sein d'une seule console d'administration. Pour plus de détails, consultez Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles.

  Cette fonctionnalité est désormais généralement disponible (GA).

[ACS-1102]

- **Tableau de bord d'accès privé sécurisé**

  Le tableau de bord Secure Private Access offre aux administrateurs une visibilité complète sur leurs principales applications, leurs principaux utilisateurs, l'état de santé des connecteurs, l'utilisation de la bande passante et un seul endroit pour la consommation. Ces données sont extraites de Citrix Analytics. Pour plus de détails, voir Tableau de bord Secure Private Access.

  Cette fonctionnalité est désormais généralement disponible (GA).

  [ACS-1169]

- **Accès direct aux applications Web d'entreprise**

  Les clients peuvent désormais activer l'accès réseau Zero Trust (ZTNA) pour les applications Web internes, directement à partir de navigateurs Web natifs tels que Chrome, Firefox, Safari et Microsoft Edge. Pour plus de détails, voir Accès direct aux applications Web d'entreprise.

  Cette fonctionnalité est désormais généralement disponible (GA).

- **Accès basé sur un agent ZTNA aux applications TCP/HTTPS**

  Les clients Citrix peuvent désormais activer l'accès réseau Zero Trust (ZTNA) pour toutes les applications client-serveur et les ressources basées sur IP/port, en plus des applications Web internes. Pour plus de détails, voir Prise en charge des applications client-serveur.

  Cette fonctionnalité est désormais généralement disponible (GA).

  [ACS-970]

- **Contrôles d'accès et de sécurité adaptatifs pour les applications Web, TCP et SaaS d'entreprise**

  La fonctionnalité d'accès adaptatif du service Citrix Secure Private Access offre une approche complète d'accès au réseau Zero Trust (ZTNA) qui offre un accès sécurisé aux applications. L'accès adaptatif permet aux administrateurs de fournir un accès granulaire aux applications auxquelles les utilisateurs peuvent accéder en fonction du contexte. Le terme « contexte » fait ici référence à :

  - Utilisateurs et groupes (utilisateurs et groupes d'utilisateurs)
  - Appareils (ordinateurs de bureau ou appareils mobiles)
  - Localisation (géolocalisation ou emplacement réseau)
  - Posture de l'appareil (vérification de la posture de l'appareil)
  - Risque (indice de risque utilisateur)

  Pour plus de détails, voir Contrôles d'accès et de sécurité adaptatifs pour les applications Web d'entreprise, TCP et SaaS.

  Cette fonctionnalité est désormais généralement disponible (GA).

[ACS-878, ACS-879, ACS-882]

- **Journaux d'audit pour l'accès privé sécurisé**

  Les événements liés au service Citrix Secure Private Access sont désormais capturés dans le journal système **Citrix Cloud > .** Pour plus de détails, voir Journaux d'audit.

  Cette fonctionnalité est désormais généralement disponible (GA).

  [ACS-876]

- **Journaux de diagnostic pour l'accès aux applications Web et SaaS d'entreprise**

  Les événements Citrix Secure Private Access sont désormais intégrés à Citrix Analytics. Citrix Analytics fournit un point de terminaison public qui permet aux administrateurs d'accéder aux événements et de les télécharger. Ces événements sont accessibles via un script PowerShell. Pour plus de détails, voir Journaux de diagnostic pour l'accès aux applications Web et SaaS d'entreprise.

  Cette fonctionnalité est désormais généralement disponible (GA).

  [ACS-805]

- **Service d'authentification adaptatif**

  Les clients Citrix Cloud peuvent désormais utiliser Citrix Workspace pour fournir une authentification adaptative aux applications et postes de travail virtuels Citrix. Authentification adaptative est un service Citrix Cloud qui permet une authentification avancée pour les clients et les utilisateurs qui se connectent à Citrix Workspace. Le service d'authentification adaptative est un ADC géré par Citrix et hébergé par Citrix Cloud. Pour plus de détails, voir Service d'authentification adaptative.

  Cette fonctionnalité est disponible dans la Tech Preview.

  [CGS-6510]

16 février 2022

- **Prise en charge des applications client-serveur** Avec la prise en charge des applications client-serveur dans Citrix Secure Private Access, vous pouvez désormais éliminer la dépendance à une solution VPN traditionnelle pour fournir l'accès à toutes les applications privées aux utilisateurs distants.

  Pour plus de détails, voir Prise en charge des applications client-serveur - Aperçu

  [ACS-870]

11 octobre 2021

- **Fusion de la mosaïque de service Citrix Gateway en un seul accès privé sécurisé dans Citrix Cloud**

  La mosaïque du service Citrix Gateway est désormais fusionnée en un seul accès privé sécurisé dans Citrix Cloud.

  - Tous les clients Secure Private Access, y compris Citrix Workspace Essentials et Citrix Workspace Standard, peuvent désormais utiliser une seule mosaïque Secure Private Access pour configurer les applications Web SaaS et Enterprise, les contrôles de sécurité améliorés, les politiques contextuelles, en plus des politiques de filtrage Web.
  - Tous les clients Citrix DaaS peuvent toujours activer le service Citrix Gateway comme proxy HDX à partir de la configuration de l'espace de travail. Cependant, le raccourci permettant d'activer le service Citrix Gateway à partir de la vignette du service de passerelle est supprimé. Vous pouvez activer le service Citrix Gateway depuis **Configuration de l'espace de travail > Accès > Connectivité externe**. Pour plus de détails, voir Connectivité externe. Sinon, aucune autre modification n'a été apportée à la fonctionnalité.

  [NGSWS-16761]

30 juillet 2021

- **Accès contextuel et contrôles de sécurité pour les applications Web et SaaS d'entreprise en fonction de la situation géographique de l'utilisateur**

  Le service Citrix Secure Private Access prend désormais en charge l'accès contextuel aux applications Web et SaaS d'entreprise en fonction de l'emplacement géographique de l'utilisateur.

  [ACS-833]

- **Option permettant de masquer une application Web ou SaaS spécifique à partir du portail Citrix Workspace**

  Les administrateurs peuvent désormais masquer une application Web ou SaaS spécifique du portail Citrix Workspace. Lorsqu'une application est masquée dans le portail Citrix Workspace, le service Citrix Gateway ne renvoie pas cette application lors de l'énumération. Cependant, les utilisateurs peuvent toujours accéder à l'application cachée.

  [ACS-944]

09 juin 2021

- **Tableau de routage pour définir les règles d'acheminement du trafic de l'application**

Les administrateurs peuvent désormais utiliser la table de routage pour définir les règles permettant d'acheminer le trafic de l'application directement vers Internet ou via Citrix Gateway Connector. Les administrateurs peuvent définir le type d'itinéraire pour les applications comme externe, interne, proxy de contournement interne ou externe via le connecteur de passerelle en fonction de la manière dont ils souhaitent définir le flux de trafic.

[ACS-243]

22 May 2021

- **Accès contextuel aux applications Web et SaaS d'entreprise**

  La fonctionnalité d'accès contextuel du service Citrix Secure Private Access offre une approche d'accès zéro confiance complète qui offre un accès sécurisé aux applications. L'accès contextuel permet aux administrateurs de fournir un accès de niveau granulaire aux applications auxquelles les utilisateurs peuvent accéder en fonction du contexte. Le terme « contexte » fait ici référence aux utilisateurs, aux groupes d'utilisateurs et à la plateforme (appareil mobile ou ordinateur de bureau) à partir de laquelle l'utilisateur accède à l'application.

  [ACS-222]

- **Rebranding de l'interface utilisateur de Citrix Gateway Connector**

  L'interface utilisateur de Citrix Cloud Gateway Connector est renommée conformément aux directives de marque Citrix.

  [NGSWS-17100]

01 May 2021

- **Suppression des données client de la banque de données du service Citrix Secure Private Access**

  Les données client, y compris les sauvegardes, sont supprimées de la banque de données du service Citrix Secure Private Access après 90 jours d'expiration du droit de service.

  [ACS-388]

- **Étapes simplifiées pour fédérer un domaine d'Azure AD vers Citrix Workspace**

  Les étapes de fédération d'un domaine d'Azure AD vers l'application Citrix Workspace sont désormais simplifiées pour une intégration plus rapide dans Citrix Workspace. La fédération de domaines peut désormais être effectuée dans l'interface utilisateur du service Citrix Gateway, à partir de la page d'authentification unique.

  [ACS-351]

- **Amélioration de l'outil de test de connectivité**

  L'outil de test de connectivité dans Citrix Gateway Connector a été amélioré pour gérer les erreurs de délai d'expiration et générer les journaux nécessaires.

  [NGSWS-17212]

15 mars 2021

- **Améliorations de la plateforme**

  Diverses améliorations de la plateforme sont apportées pour augmenter la fiabilité de la propagation des configurations d'administration du client vers les connecteurs Citrix Gateway.

  [ACS-85]

- **Amélioration des performances des applications Web**

  Les performances des applications Web lorsque les applications Web sont accessibles à partir du navigateur système à l'aide d'un VPN sans client ont été améliorées.

  [NGSWS-16469]

- **Activation de Citrix Gateway Connector pour utiliser les suites de chiffrement TLS1.2 Grade A ou supérieures**

  Citrix Gateway Connector utilise désormais TLS1.2 avec des suites de chiffrement de niveau A ou supérieur pour se connecter au service Citrix Cloud et à d'autres serveurs principaux.

  [NGSWS-16068]

11 novembre 2020

- **Renommer le service Citrix Access Control**

  Le service de contrôle d'accès est désormais renommé Accès privé sécurisé.

  [NGSWS-14934]

15 octobre 2020

- **Option de sécurité améliorée pour lancer des applications SaaS et Web d'entreprise dans le service d'isolation du navigateur à distance**

  Les administrateurs peuvent désormais utiliser l'option de sécurité améliorée, **Sélectionnez Toujours lancer l'application dans le service Citrix Remote Browser Isolation** pour toujours

lancer une application dans le service Remote Browser Isolation, quels que soient les autres paramètres de sécurité améliorés.

[ACS-123]

08 octobre 2020

- **Configurer les délais d'expiration de session pour l'extension de navigateur Citrix Secure Private Access**

  Les administrateurs peuvent désormais configurer les délais d'expiration de session pour l'extension de navigateur Citrix Secure Private Access. Les administrateurs peuvent configurer ce paramètre à partir de l'onglet **Gérer** dans l'interface utilisateur du service Citrix Gateway.

  [NGSWS-13754]

- **Contrôle RBAC sur les paramètres d'administration de l'extension de navigateur Citrix Secure Private Access**

  Le contrôle RBAC est désormais appliqué aux paramètres d'administration de l'extension de navigateur Citrix Secure Private Access.

  [NGSWS-14427]

24 septembre 2020

- **Activer l'accès sans VPN aux applications Web d'entreprise via un navigateur local**

  Vous pouvez désormais utiliser l'extension de navigateur **Citrix Secure Private Access** pour activer l'accès sans VPN aux applications Web d'entreprise via un navigateur local. L'extension de navigateur **Citrix Secure Private Access** est prise en charge sur les navigateurs Google Chrome et Microsoft Edge.

  [ACS-286]

07 juillet 2020

- **Valider la configuration Kerberos sur Citrix Gateway Connector**

  Vous pouvez maintenant utiliser le bouton **Test** dans la section **Authentification unique** pour valider la configuration Kerberos.

  [NGSWS-8581]

19 juin 2020

- **Accès en lecture seule aux administrateurs du service Citrix Gateway et du service Citrix Secure Private Access**

  Les équipes d'administrateurs de sécurité utilisant le service Citrix Gateway peuvent désormais fournir des contrôles granulaires, tels que l'accès en lecture seule aux administrateurs du service Citrix Gateway et du service Citrix Secure Private Access.

  - Les administrateurs disposant d'un accès en lecture seule au service Citrix Gateway ont uniquement accès à l'affichage des détails de l'application.
  - Les administrateurs disposant d'un accès en lecture seule au service Citrix Secure Private Access peuvent uniquement afficher les paramètres d'accès au contenu.

  [ACS-205]

08 May 2020

- **Nouveaux outils de dépannage dans Citrix Gateway Connector 13.0**

  - **Traçage réseau :** Vous pouvez désormais utiliser la fonctionnalité **Trace** pour résoudre les problèmes d'enregistrement de Citrix Gateway Connector. Vous pouvez télécharger le fichier de trace et le partager avec les administrateurs pour le dépannage. Pour plus de détails, consultez Résoudre les problèmes d'enregistrement de Citrix Gateway Connector.

    [NGSWS-10799]

  - **Tests de connectivité :** Vous pouvez maintenant utiliser la fonctionnalité **Test de connectivité** pour confirmer qu'il n'y a aucune erreur dans la configuration du connecteur de passerelle et que le connecteur de passerelle est capable de se connecter aux URL. Pour plus de détails, voir Connectez-vous et configurez Citrix Gateway Connector.

    [NGSWS-8580]

V2019.04.02

- **Prise en charge de l'authentification Kerberos pour Citrix Gateway Connector vers le proxy sortant** [NGSWS-6410]

  L'authentification Kerberos est désormais prise en charge pour le trafic du connecteur Citrix Gateway vers le proxy sortant. Gateway Connector utilise les informations d'identification du proxy configurées pour s'authentifier auprès du proxy sortant.

V2019.04.01

- **Le trafic des applications Web/SaaS peut désormais être acheminé via un connecteur de passerelle hébergé sur le réseau de l'entreprise, évitant ainsi l'authentification à deux facteurs.** Si un client a publié une application SaaS hébergée en dehors du réseau d'entreprise, une prise en charge est désormais ajoutée pour authentifier le trafic de cette application afin qu'il passe par un connecteur de passerelle sur site.

  Par exemple, imaginons qu'un client dispose d'une application SaaS protégée par Okta (comme Workday). Le client peut souhaiter que même si le trafic de données Workday réel n'est pas acheminé via le service Citrix Gateway, le trafic d'authentification vers le serveur Okta soit acheminé via le service Citrix Gateway via un connecteur de passerelle local. Cela permet au client d'éviter une authentification à deux facteurs à partir du serveur Okta, car l'utilisateur se connecte au serveur Okta depuis le réseau de l'entreprise.

  [NGSWS-6445]

- **Désactivation du filtrage des listes de sites Web et de la catégorisation des sites Web**. Le filtrage des listes de sites Web et la catégorisation des sites Web peuvent être désactivés si l'administrateur choisit de ne pas appliquer ces fonctionnalités à un client spécifique.

  [NGSWS-6532]

- **Routage géographique automatique pour les redirections du service d'isolation du navigateur à distance.** Le routage géographique automatique est désormais activé pour les redirections du service d'isolation du navigateur à distance.

  [NGSWS-6926]

V2019.03.01

- **Le bouton « Détecter » est ajouté à la page « Ajouter un connecteur de passerelle ».** Le bouton **Détecter** est utilisé pour actualiser la liste des connecteurs, permettant au connecteur nouvellement ajouté de se refléter dans la section de connectivité de l'application Web.

  [CGOP-6358]

- **Une nouvelle catégorie « Malveillant et dangereux » est ajoutée dans les catégories « Contrôle d'accès et filtrage Web ».** Une nouvelle catégorie nommée **Malveillant et dangereux** dans les catégories **Contrôle d'accès Filtrage Web** est ajoutée sous le groupe **Logiciels malveillants et spam** .

  [CGOP-6205]

Démarrer avec Citrix Secure Private Access

December 27, 2023

Ce document vous explique comment démarrer l'intégration et la configuration de la diffusion des applications SaaS pour la première fois. Ce document est destiné aux administrateurs d'applications.

Configuration système requise

Prise en charge des systèmes d'exploitation : l'application Citrix Workspace est prise en charge sur Windows 7, 8, 10 et Mac 10.11 et versions ultérieures.

Prise en charge des navigateurs : accédez aux espaces de travail à l'aide des dernières versions d' Edge, Chrome, Firefox ou Safari.

Prise en charge de Citrix Workspace : accédez aux espaces de travail à l'aide de Citrix Workspace pour n'importe quelle plate-forme de bureau (Windows, Mac).

Fonctionnement

Citrix Secure Private Access aide les administrateurs informatiques et de sécurité à gérer l'accès autorisé des utilisateurs finaux aux applications Web SaaS et hébergées par l'entreprise. Les identités et les attributs utilisateur sont utilisés pour déterminer les privilèges d'accès et les stratégies de contrôle d'accès déterminent les privilèges requis pour effectuer des opérations. Une fois qu'un utilisateur est authentifié, le contrôle d'accès autorise le niveau d'accès approprié et les actions autorisées associées aux informations d'identification de cet utilisateur.

Citrix Secure Private Access combine des éléments de plusieurs services Citrix Cloud pour offrir une expérience intégrée aux utilisateurs finaux et aux administrateurs.

Fonctionnalité	Service/Composant fournissant la fonctionnalité
Interface utilisateur cohérente pour accéder aux applications	Workspace Experience/Application Workspace
SSO vers SaaS et applications Web	Norme de service Citrix Gateway
Filtrage Web et catégorisation	Service de filtrage Web
Stratégies de sécurité améliorées pour le SaaS	Contrôle des applications cloud
Navigation sécurisée	Service Remote Browser Isolation

Fonctionnalité	Service/Composant fournissant la fonctionnalité
Visibilité de l'accès au site Web et des comportements à risque	Citrix Analytics

Premiers pas avec le service Citrix Secure Private Access

1. Inscrivez-vous à Citrix Cloud.
2. Demande de droit au service Secure Private Access.
3. Après l'autorisation, Secure Private Access Service est fourni sous **Mes services**.
4. Accédez à l'interface utilisateur du service Secure Private Access.

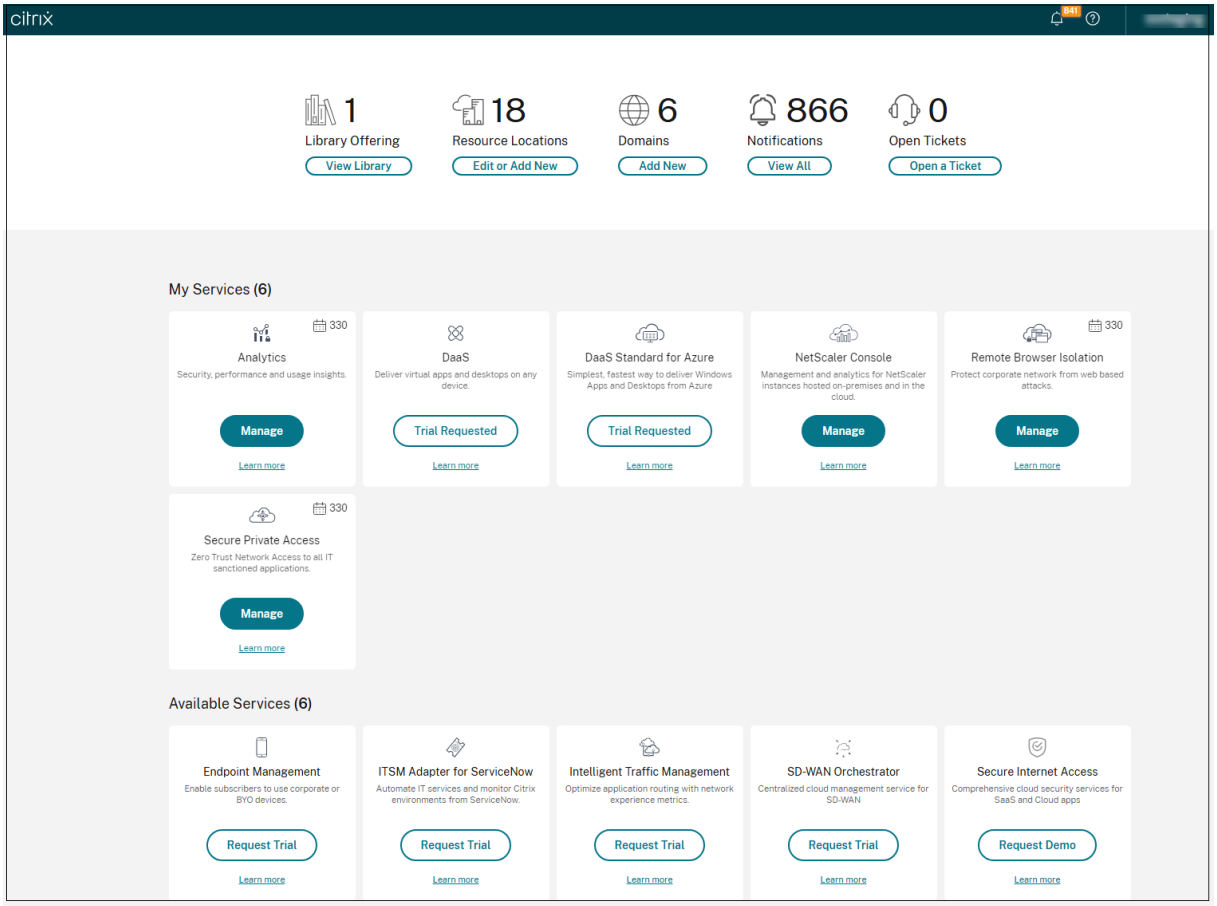
Étape 1 : **Inscrivez-vous à Citrix Cloud**

Pour commencer à utiliser le service Secure Private Access, vous devez d'abord créer un compte Citrix Cloud ou rejoindre un compte existant créé par un autre membre de votre entreprise. Pour des procédures détaillées et des instructions sur la marche à suivre, consultez la section Inscription à Citrix Cloud .

Étape 2 : **Demande de droit au service Secure Private Access**

Pour demander le droit d'accès au service Secure Private Access, sur l'écran **Citrix Cloud**, sous la section **Services disponibles**, cliquez sur l'onglet **Request Trial** présent dans la vignette du service Secure Private Access.

Pour plus de détails sur la licence, consultez https://www.citrix.com/buy/licensing/product.html.



Étape 3 : **Après l'autorisation, Secure Private Access Service est fourni sous Mes services**

Une fois que vous avez reçu le droit de service Secure Private Access, la vignette du service Secure Private Access passe à la section **Mes services** .

Étape 4 : **accéder à l'interface utilisateur du service Secure Private Access**

Cliquez sur l'onglet **Gérer** de la vignette pour accéder à l'interface utilisateur du service Secure Private Access.

Remarque :

- Pour que vos utilisateurs puissent utiliser l'espace de travail et accéder aux applications, ils doivent télécharger et utiliser l'application Citrix Workspace ou utiliser l'URL de l'espace de travail. Vous devez avoir publié quelques applications SaaS dans votre espace de travail pour tester la solution Citrix Secure Private Access. L'application Workspace peut être téléchargée depuis https://www.citrix.com/downloads. Dans la liste **Rechercher des téléchargements**, sélectionnez l'**application Citrix Workspace**.
- Si un pare-feu sortant est configuré, assurez-vous que l'accès aux domaines suivants est autorisé.

- *.cloud.com
- *.nssvc.net
- *.netscalergateway.net

Vous trouverez plus de détails dans Configuration du pare-feu et du proxy d'un Cloud Connector et Exigences en terme de connexion Internet.

- Vous ne pouvez ajouter qu'un seul compte Workspace.

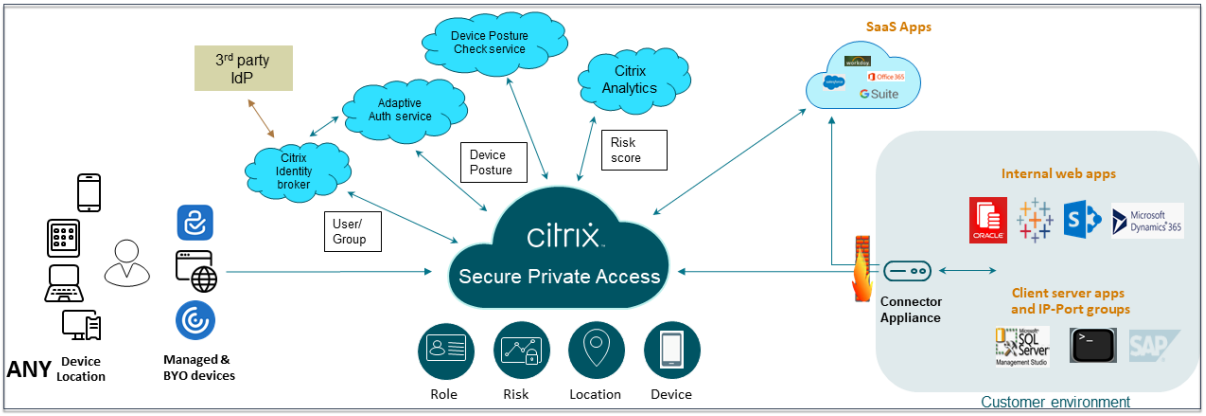
Présentation du service Secure Private Access

October 21, 2024

Présentation de la solution

Les solutions VPN traditionnelles nécessitent que les appareils des utilisateurs finaux soient gérés, fournissent un accès au niveau du réseau et appliquent des politiques de contrôle d'accès statiques. Citrix Secure Private Access offre au service informatique un ensemble de contrôles de sécurité pour se protéger contre les menaces provenant des appareils BYO, offrant aux utilisateurs le choix d'accéder à leurs applications approuvées par le service informatique à partir de n'importe quel appareil, qu'il soit géré ou BYO.

Citrix Secure Private Access offre une authentification adaptative, une prise en charge de l'authentification unique et des contrôles de sécurité améliorés pour les applications. Secure Private Access offre également la possibilité d'analyser l'appareil de l'utilisateur final avant d'établir une session à l'aide du service Device Posture. En fonction des résultats de l'authentification adaptative ou de la posture de l'appareil, les administrateurs peuvent définir les méthodes d'authentification pour les applications.



Sécurité adaptative

L'authentification adaptative détermine le flux d'authentification approprié pour la demande en cours. L'authentification adaptative peut identifier la posture de l'appareil, l'emplacement géographique, le segment de réseau et l'appartenance à l'organisation/au service de l'utilisateur. Sur la base des informations obtenues, un administrateur peut définir comment il souhaite authentifier les utilisateurs auprès de ses applications approuvées par le service informatique. Cela permet aux organisations de mettre en œuvre le même cadre de politique d'authentification sur toutes les ressources, y compris les applications SaaS publiques, les applications Web privées, les applications client-serveur privées et les postes de travail en tant que service (DaaS). Pour plus de détails, voir Sécurité adaptative.

Accès aux applications

Secure Private Access peut créer une connexion aux applications Web sur site sans recourir à un VPN. Cette connexion sans VPN utilise un dispositif de connecteur déployé sur site. L'appliance Connector crée un canal de contrôle sortant vers l'abonnement Citrix Cloud de l'organisation. À partir de là, Secure Private Access peut établir des tunnels de connexion vers les applications Web internes sans avoir besoin d'un VPN. Pour plus de détails, voir Accès aux applications.

Single Sign-On

Avec l'authentification adaptative, les organisations peuvent fournir des politiques d'authentification fortes pour aider à réduire le risque de comptes d'utilisateurs compromis. Les fonctionnalités d'authentification unique de Secure Private Access utilisent les mêmes politiques d'authentification adaptative pour toutes les applications SaaS, Web privées et client-serveur. Pour plus de détails, voir Authentification unique.

Sécurité du navigateur

Secure Private Access permet aux utilisateurs finaux de naviguer en toute sécurité sur Internet avec un navigateur d'entreprise géré de manière centralisée et sécurisé. Lorsqu'un utilisateur final lance une application SaaS ou Web privée, plusieurs décisions sont prises de manière dynamique pour décider de la meilleure façon de servir cette application. Pour plus de détails, voir Sécurité du navigateur.

Position de l'appareil

Le service de posture des appareils permet à un administrateur de définir des politiques pour vérifier la posture des appareils terminaux essayant d'accéder aux ressources de l'entreprise à distance. En

fonction de l'état de conformité d'un point de terminaison, le service de posture de l'appareil peut refuser l'accès ou fournir un accès restreint/complet aux applications et aux postes de travail de l'entreprise.

Lorsqu'un utilisateur final initie une connexion avec Citrix Workspace, le client Device Posture collecte des informations sur les paramètres du point de terminaison et partage ces informations avec le service Device Posture pour déterminer si la posture du point de terminaison répond aux exigences de la stratégie.

L'intégration du service Device Posture avec Citrix Secure Private Access permet un accès sécurisé aux applications SaaS, Web, TCP et UDP depuis n'importe où, avec la résilience et l'évolutivité de Citrix Cloud. Pour plus de détails, voir Posture de l'appareil.

Prise en charge des applications TCP et UDP

Parfois, les utilisateurs distants ont besoin d'accéder à des applications client-serveur privées dont le front-end se trouve sur le point de terminaison et le back-end dans un centre de données. Les organisations peuvent légitimement appliquer des politiques de sécurité strictes autour de ces applications internes et privées, rendant difficile l'accès des utilisateurs distants à ces applications sans compromettre les protocoles de sécurité.

Le service Secure Private Access répond aux vulnérabilités de sécurité TCP et UDP en permettant à ZTNA de fournir un accès sécurisé à ces applications. Les utilisateurs peuvent désormais accéder à toutes les applications privées, y compris les applications TCP, UDP et HTTPS, soit à l'aide d'un navigateur natif, soit d'une application client native via le client Citrix Secure Access exécuté sur leurs machines.

Les utilisateurs doivent installer le client Citrix Secure Access sur leurs appareils clients.

- Pour Windows, la version client (22.3.1.5 et versions ultérieures) peut être téléchargée à partir de https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
- Pour macOS, la version client (22.02.3 et ultérieure) peut être téléchargée depuis l'App Store.

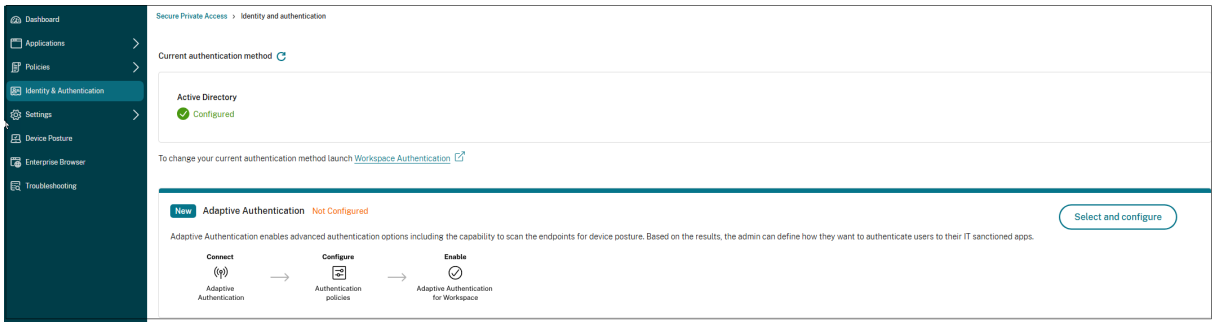
Pour plus de détails, voir Prise en charge des applications client-serveur.

Configurer Citrix Secure Private Access

Activez l'accès réseau Zero Trust aux applications SaaS, aux applications Web internes, aux applications TCP et UDP à l'aide de la console d'administration Secure Private Access. Cette console inclut la configuration de l'authentification adaptative, des applications, notamment l'abonnement utilisateur et les politiques d'accès adaptatif.

Configurer l'identité et l'authentification

Sélectionnez la méthode d'authentification permettant aux abonnés de se connecter à Citrix Workspace. Authentification adaptative est un service Citrix Cloud qui permet une authentification avancée pour les clients et les utilisateurs qui se connectent à Citrix Workspace.



Pour plus de détails, voir Configurer l'identité et l'authentification.

Énumérer et publier des applications

Après avoir sélectionné la méthode d'authentification, configurez les applications Web, SaaS ou TCP et UDP à l'aide de la console d'administration. Pour plus de détails, voir Ajouter et gérer des applications.

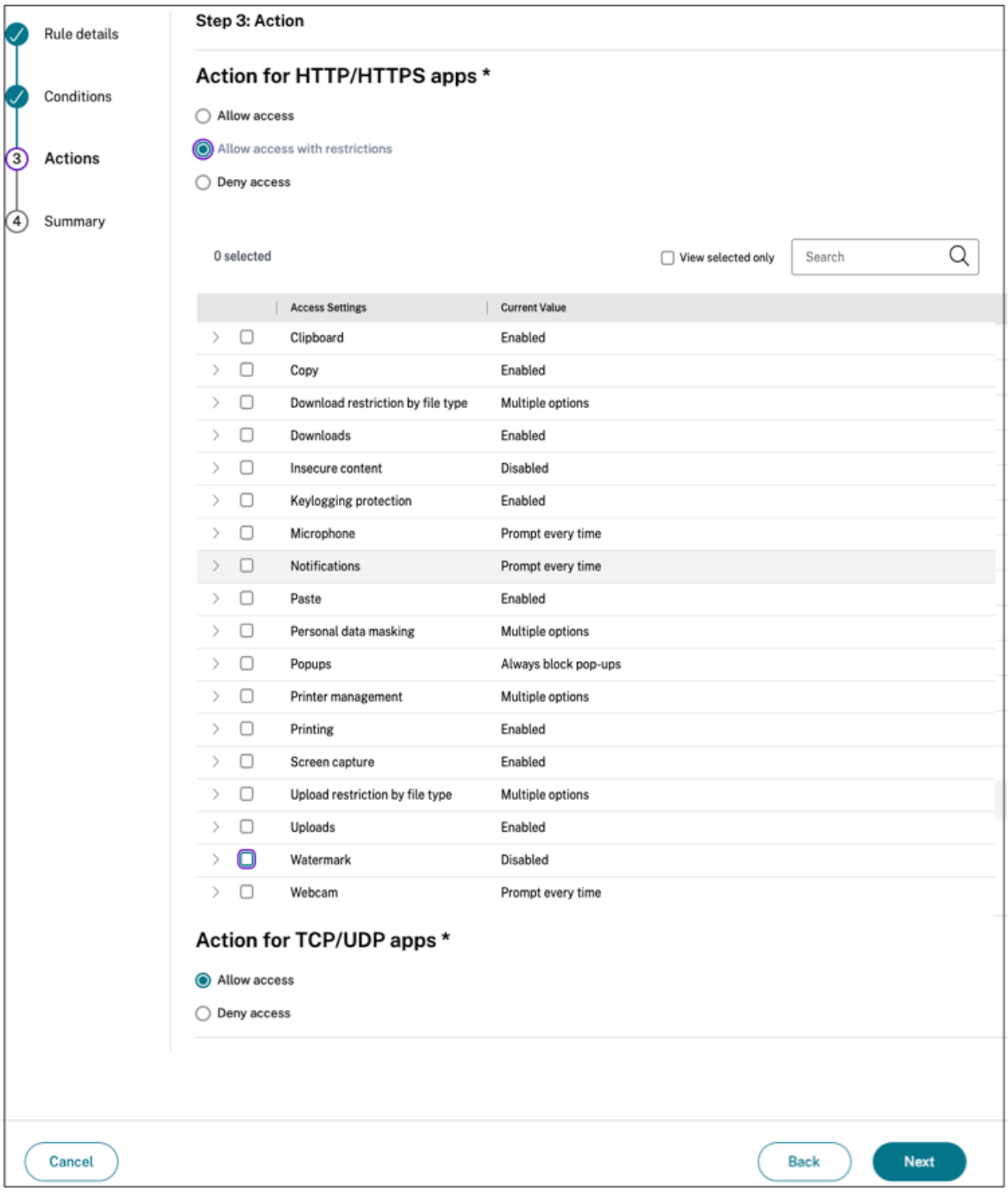
Activer des contrôles de sécurité renforcés

Pour protéger le contenu, les organisations intègrent des politiques de sécurité renforcées au sein des applications SaaS. Chaque politique applique une restriction sur le navigateur Citrix Enterprise lors de l'utilisation de l'application Workspace pour ordinateur de bureau ou sur Secure Browser lors de l'utilisation de l'application Workspace Web ou mobile.

- **Restreindre l'accès au presse-papiers**: Désactive les opérations couper/copier/coller entre l'application et le presse-papiers du système.
- **Restreindre l'impression**: désactive la possibilité d'imprimer à partir du navigateur Citrix Enterprise.
- **Restreindre les téléchargements**: Désactive la capacité de l'utilisateur à télécharger depuis l'application.
- **Restreindre les téléchargements**: Désactive la capacité de l'utilisateur à télécharger dans l'application.
- **Afficher le filigrane**: Affiche un filigrane sur l'écran de l'utilisateur affichant le nom d'utilisateur et l'adresse IP de la machine de l'utilisateur.
- **Restreindre l'enregistrement des frappes.**: Protège contre les enregistreurs de frappe. Lorsqu'un utilisateur tente de se connecter à l'application à l'aide du nom d'utilisateur et du

mot de passe, toutes les clés sont cryptées sur les enregistreurs de frappe. De plus, toutes les activités que l'utilisateur effectue sur l'application sont protégées contre l'enregistrement des frappes. Par exemple, si les stratégies de protection des applications sont activées pour Office 365 et que l'utilisateur modifie un document Word Office 365, toutes les frappes au clavier sont chiffrées sur les enregistreurs de frappe.

- **Restreindre la capture d'écran**: Désactive la possibilité de capturer les écrans à l'aide de l'un des programmes ou applications de capture d'écran. Si un utilisateur tente de capturer l'écran, un écran vide est capturé.



Pour plus de détails, voir Configurer une politique d'accès.

Activer Citrix Enterprise Browser pour les lancements d'applications

Secure Private Access permet aux utilisateurs finaux de lancer leurs applications à l'aide de Citrix Enterprise Browser (CEB). CEB est un navigateur basé sur Chromium intégré à l'application Citrix Work-

space qui permet une expérience d'accès transparente et sécurisée pour accéder aux applications Web et SaaS dans Citrix Enterprise Browser.

CEB peut être configuré comme navigateur préféré ou comme navigateur de travail pour toutes les applications Web hébergées en interne ou les applications SaaS avec des politiques de sécurité. CEB permet aux utilisateurs d'ouvrir tous les domaines d'applications SaaS/Web configurés dans un environnement sécurisé et contrôlé.

Activer le navigateur Citrix Enterprise Les administrateurs peuvent utiliser le service Global App Configuration (GACS) pour configurer Citrix Enterprise Browser comme navigateur par défaut pour lancer des applications Web et SaaS à partir de l'application Citrix Workspace.

Configuration via API:

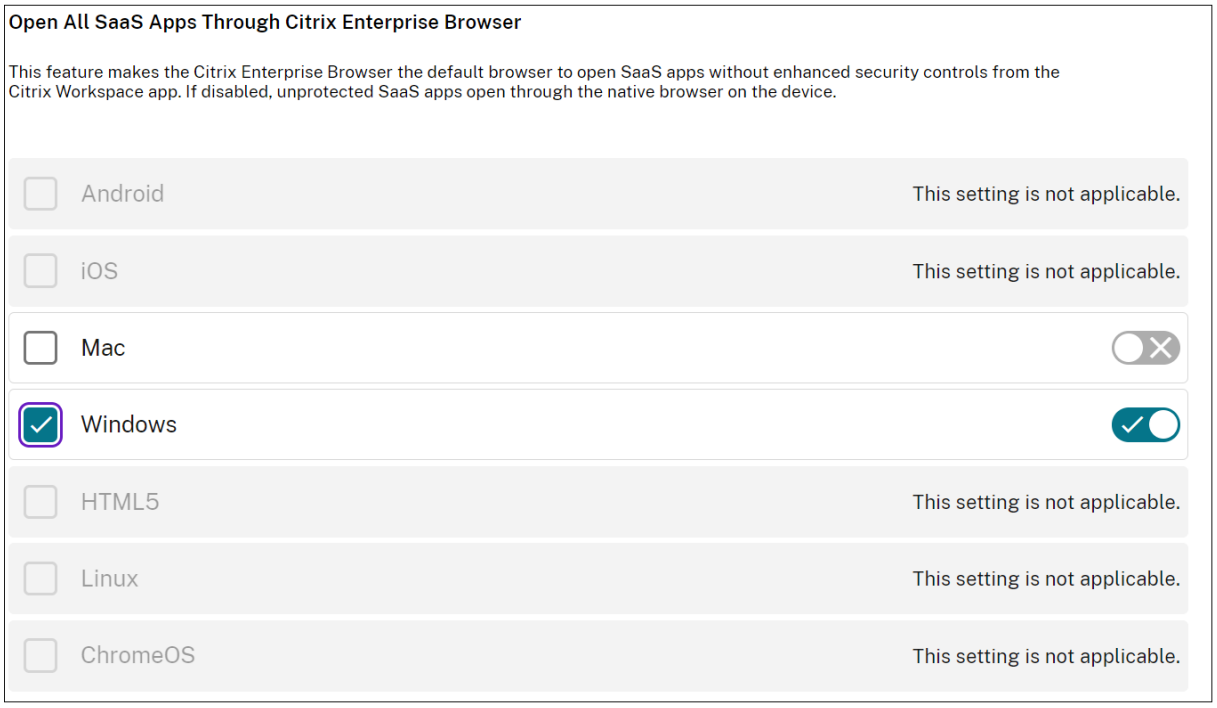
Pour configurer, voici un exemple de fichier JSON pour activer Citrix Enterprise Browser pour toutes les applications, par défaut :

```
"settings": [
                    {

                       "name": "open all apps in ceb",
                       "value": "true"
                     }

                    ]
```

La valeur par défaut est true.

Configuration via l'interface graphique :

Sélectionnez les appareils pour lesquels CEB doit être défini comme navigateur par défaut pour le lancement de l'application.



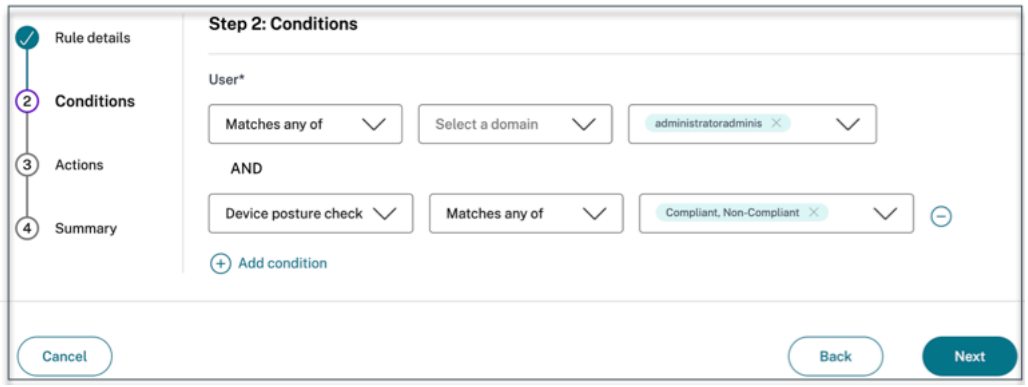
Pour plus de détails, voir Gérer Citrix Enterprise Browser via GACS.

Configurer des balises pour un accès contextuel à l'aide de Device Posture

Après la vérification de la posture de l'appareil, l'appareil est autorisé à se connecter et l'appareil est classé comme conforme ou non conforme. Cette classification est mise à disposition sous forme de balises auprès du service Secure Private Access et est utilisée pour fournir un accès contextuel en fonction de la posture de l'appareil.

1. Connectez-vous à Citrix Cloud.
2. Sur la mosaïque Accès privé sécurisé, cliquez sur **Gérer**.
3. Cliquez sur **Stratégies d'accès** dans la navigation de gauche, puis cliquez sur **Créer une stratégie**.
4. Saisissez le nom de la politique et la description de la politique.
5. Dans **Applications**, sélectionnez l'application ou l'ensemble d'applications sur lesquelles cette politique doit être appliquée.
6. Cliquez sur **Créer une règle** pour créer des règles pour la politique.
7. Saisissez le nom de la règle et une brève description de la règle, puis cliquez sur **Suivant**.
8. Sélectionnez les conditions des utilisateurs. La condition Utilisateurs est une condition obligatoire à respecter pour accorder l'accès aux applications aux utilisateurs.

9. Cliquez sur **+** pour ajouter une condition de posture de l'appareil.
10. Sélectionnez **Vérification de la posture de l'appareil** et l'expression logique dans le menu déroulant.
11. Saisissez l'une des valeurs suivantes dans les balises personnalisées :



- **Conforme** - Pour les appareils conformes
- **Non conforme** - Pour les appareils non conformes

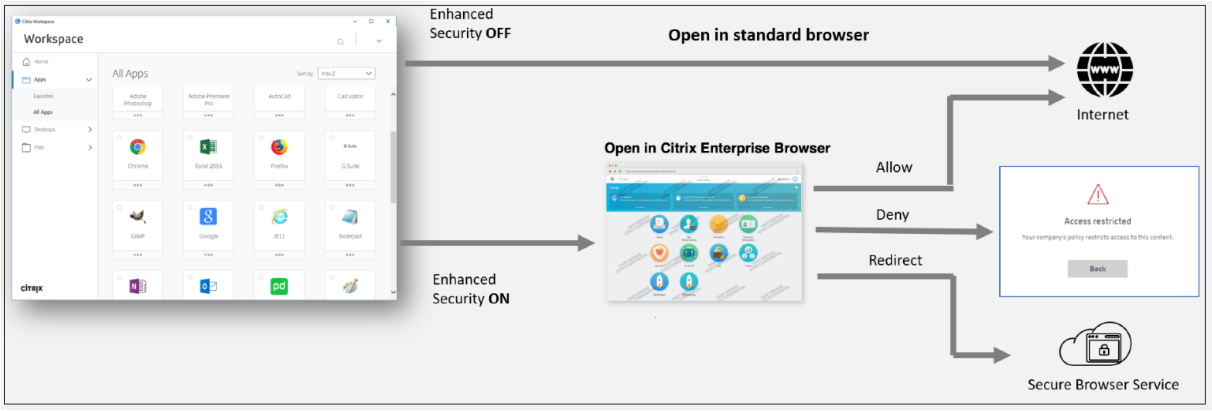
12. Dans **Commandes CLI équivalentes**, passez en revue les commandes et cliquez sur **Suivant**.
13. Sélectionnez les actions qui doivent être appliquées en fonction de l'évaluation de la condition, puis cliquez sur **Suivant**.

    La page Résumé affiche les détails de la politique.
14. Vérifiez les détails et cliquez sur **Terminer**.

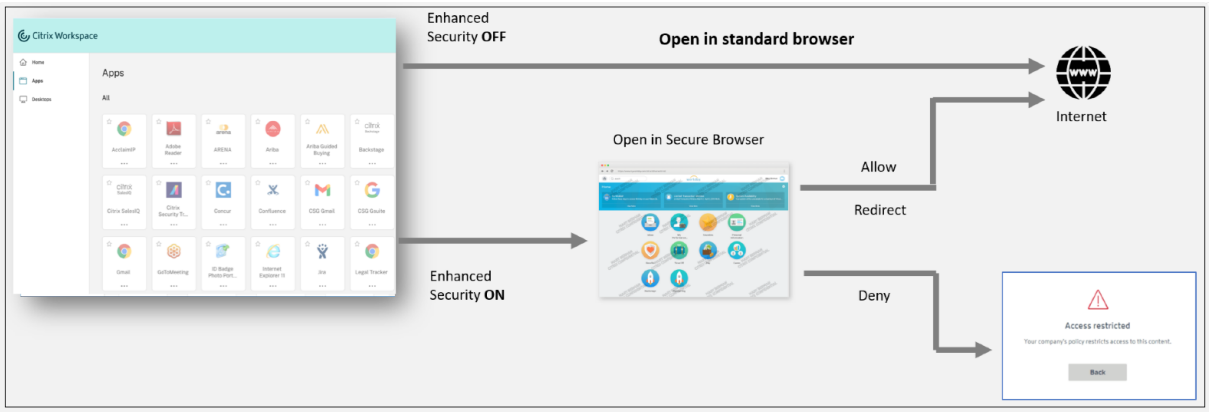
> **Remarque**
>
> Toute application Secure Private Access qui n'est pas marquée comme conforme ou non conforme dans la politique d'accès est traitée comme l'application par défaut et est accessible sur tous les points de terminaison, quelle que soit la position de l'appareil.

Expérience pour l'utilisateur final

L'administrateur Citrix a le pouvoir d'étendre le contrôle de sécurité à l'aide de Citrix Secure Private Access. L'application Citrix Workspace est un point d'entrée pour accéder à toutes les ressources en toute sécurité. Les utilisateurs finaux peuvent accéder aux applications virtuelles, aux postes de travail, aux applications SaaS et aux fichiers via l'application Citrix Workspace. Avec Citrix Secure Private Access, les administrateurs peuvent contrôler la manière dont une application SaaS est accessible par l'utilisateur final via l'interface utilisateur Web Citrix Workspace Experience ou le client d'application Citrix Workspace natif.



Lorsque l'utilisateur lance l'application Workspace sur le point de terminaison, il voit ses applications, ses bureaux, ses fichiers et ses applications SaaS. Si un utilisateur clique sur l'application SaaS alors que la sécurité renforcée est désactivée, l'application s'ouvre dans un navigateur standard installé localement. Si l'administrateur a activé la sécurité renforcée, les applications SaaS s'ouvrent sur le CEB dans l'application Workspace. L'accessibilité aux hyperliens dans les applications SaaS et les applications Web est contrôlée en fonction des politiques des sites Web non autorisés. Pour plus de détails sur les sites Web non autorisés, consultez Sites Web non autorisés.



De même, avec le portail Web Workspace, lorsque la sécurité renforcée est désactivée, les applications SaaS sont ouvertes dans un navigateur standard installé nativement. Lorsque la sécurité renforcée est activée, les applications SaaS sont ouvertes dans le navigateur distant sécurisé. Les utilisateurs peuvent accéder aux sites Web dans les applications SaaS en fonction des politiques relatives aux sites Web non autorisés. Pour plus de détails sur les sites Web non autorisés, consultez Sites Web non autorisés.

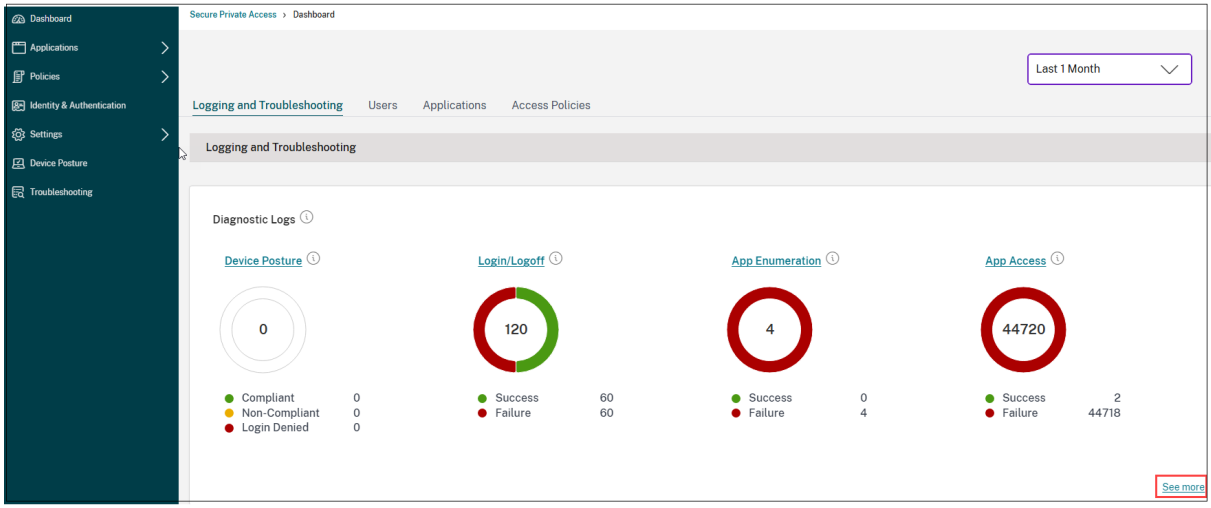
Tableau de bord d'analyse

Le tableau de bord du service Secure Private Access affiche les données de diagnostic et d'utilisation des applications SaaS, Web, TCP et UDP. Le tableau de bord offre aux administrateurs une visibilité complète sur leurs applications, leurs utilisateurs, l'état de santé des connecteurs et l'utilisation de

la bande passante en un seul endroit pour la consommation. Ces données sont extraites de Citrix Analytics. Les mesures sont généralement classées dans les catégories suivantes.

- Journalisation et dépannage
- Utilisateurs
- Applications
- Politiques d'accès

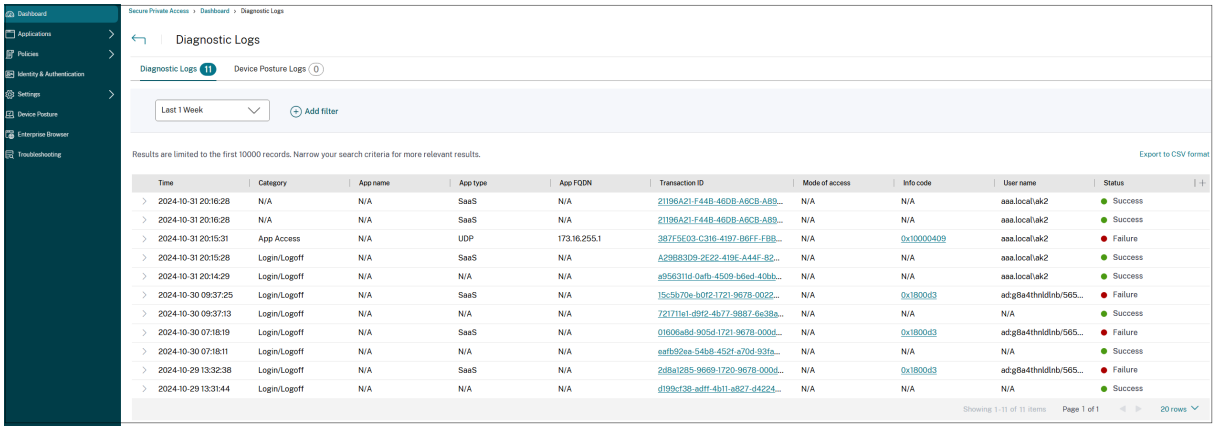
Pour plus de détails, voir Tableau de bord.



Résoudre les problèmes d'application

Le graphique Journaux de diagnostic du tableau de bord Secure Private Access offre une visibilité sur les journaux liés à l'authentification, au lancement d'applications, à l'énumération d'applications et aux journaux de posture de l'appareil.

- **Code d'information**: Certains événements de journal tels que les échecs ont un code d'information associé. Cliquer sur le code d'information redirige les utilisateurs vers les étapes de résolution ou vers plus d'informations sur cet événement.
- **ID de transaction**: Les journaux de diagnostic affichent également un ID de transaction qui met en corrélation tous les journaux Secure Private Access pour une demande d'accès. Une demande d'accès à une application peut générer plusieurs journaux, à commencer par l'authentification, puis l'énumération des applications dans l'application de l'espace de travail, puis l'accès à l'application elle-même. Tous ces événements génèrent leurs propres journaux. L'ID de transaction est utilisé pour corréler tous ces journaux. Vous pouvez filtrer les journaux de diagnostic à l'aide de l'ID de transaction pour rechercher tous les journaux liés à une demande d'accès à une application particulière. Pour plus de détails, voir Résoudre les problèmes d'accès privé sécurisé.



Exemples de cas d'utilisation

- Accédez aux applications internes (Web/TCP/UDP) à l'aide d'une approche Zero-Trust sans ouvrir le trafic entrant sur le pare-feu
- Passez à une approche Zero Trust en découvrant les applications auxquelles les utilisateurs accèdent
- Restreindre l'accès aux applications SaaS à Citrix Enterprise Browser
- Restreindre l'accès aux applications SaaS aux adresses IP publiques appartenant à l'entreprise
- Sécurité renforcée pour les applications SaaS gérées par Azure
- Sécurité renforcée pour Office 365
- Sécurité renforcée pour les applications Okta

Articles de référence

- Introduction à l'accès privé sécurisé
- Fiche technique
- Architecture de référence
- Citrix Enterprise Browser
- Gérer Citrix Enterprise Browser via GACS
- Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles

Vidéos de référence

- Accès réseau Zero Trust (ZTNA) aux applications
- Accès privé aux applications Web avec Citrix Secure Private Access
- Accès aux applications SaaS publiques avec Citrix Secure Private Access
- Accès privé aux applications client-serveur avec Citrix Secure Private Access
- Protection contre les enregistreurs de frappe avec Citrix Secure Private Access

- Protection du partage d'écran avec Citrix Secure Private Access
- Expérience de l'utilisateur final avec Citrix Secure Private Access
- Expérience de connexion ZTNA versus VPN avec Citrix Secure Private Access
- Analyses de ports ZTNA et VPN avec Citrix Secure Private Access

Quoi de neuf dans les produits associés

- Citrix Enterprise Browser : À propos de cette version
- Citrix Workspace : Quoi de neuf
- Citrix DaaS : Quoi de neuf
- Client Citrix Secure Access Clients NetScaler Gateway

Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles

October 21, 2024

Une nouvelle expérience d'administration simplifiée avec un processus étape par étape pour configurer l'accès réseau Zero Trust aux applications SaaS, aux applications Web internes et aux applications TCP est disponible dans le service Secure Private Access. Il comprend la configuration de l'authentification adaptative, des applications incluant l'abonnement utilisateur, les politiques d'accès adaptatif et d'autres au sein d'une seule console d'administration.

Cet assistant aide les administrateurs à obtenir une configuration sans erreur lors de l'intégration ou de l'utilisation récurrente. De plus, un nouveau tableau de bord est disponible avec une visibilité complète sur les mesures d'utilisation globales et d'autres informations clés.

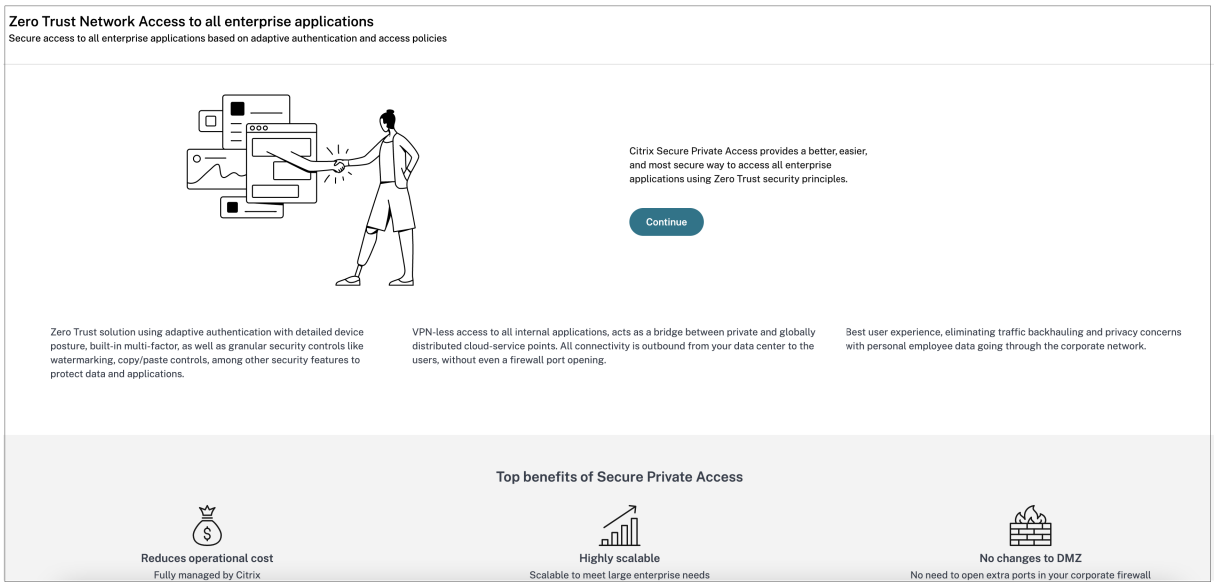
Les étapes de haut niveau comprennent les éléments suivants :

1. Choisissez la méthode d'authentification permettant aux abonnés de se connecter à Citrix Workspace.
2. Ajoutez des applications pour vos utilisateurs.
3. Attribue des autorisations pour l'accès aux applications en créant les politiques d'accès requises.
4. Vérifiez la configuration de l'application.

Accéder à l'assistant de flux de travail guidé par l'administrateur Secure Private Access

Procédez comme suit pour accéder à l'assistant.

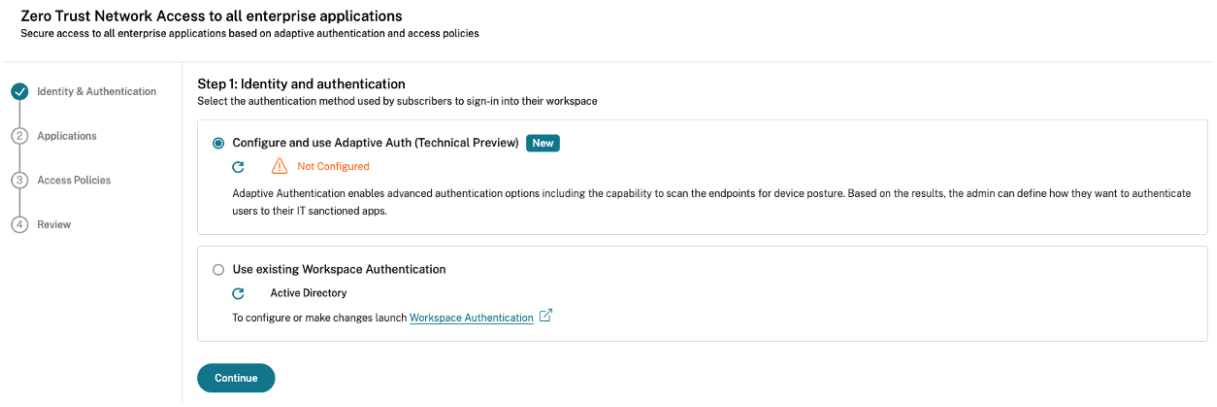
1. Sur la mosaïque de service **Accès privé sécurisé** , cliquez sur **Gérer**.
2. Dans la page Aperçu, cliquez sur **Continuer**.



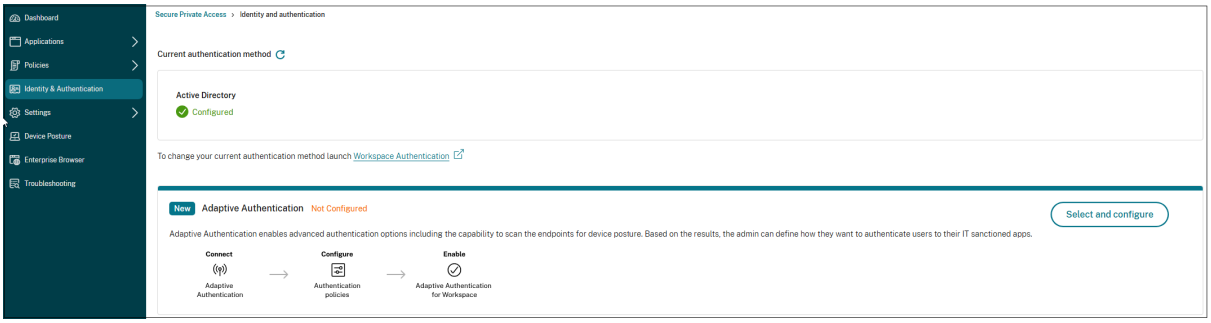
Étape 1 : Configurer l'identité et l'authentification

Sélectionnez la méthode d'authentification permettant aux abonnés de se connecter à Citrix Workspace. Authentification adaptative est un service Citrix Cloud qui permet une authentification avancée pour les clients et les utilisateurs qui se connectent à Citrix Workspace. Le service d'authentification adaptative est un service Citrix ADC hébergé par Citrix, géré par Citrix et hébergé dans le cloud qui fournit toutes les fonctionnalités d'authentification avancées telles que les suivantes.

- Authentification multifacteur
- Scans de posture de l'appareil
- Authentification conditionnelle
- Accès adaptatif aux applications et postes de travail virtuels Citrix
- Pour configurer l'authentification adaptative, sélectionnez **Configurer et utiliser l'authentification adaptative (aperçu technique)** , puis terminez la configuration. Pour plus de détails sur l'authentification adaptative, voir Service d'authentification adaptative. Après avoir configuré l'authentification adaptative, vous pouvez cliquer sur **Gérer** pour modifier la configuration, si nécessaire.



- Si vous avez initialement sélectionné une méthode d'authentification différente et que vous souhaitez passer à l'authentification adaptative, cliquez sur **Sélectionnez et configurez** , puis terminez la configuration.



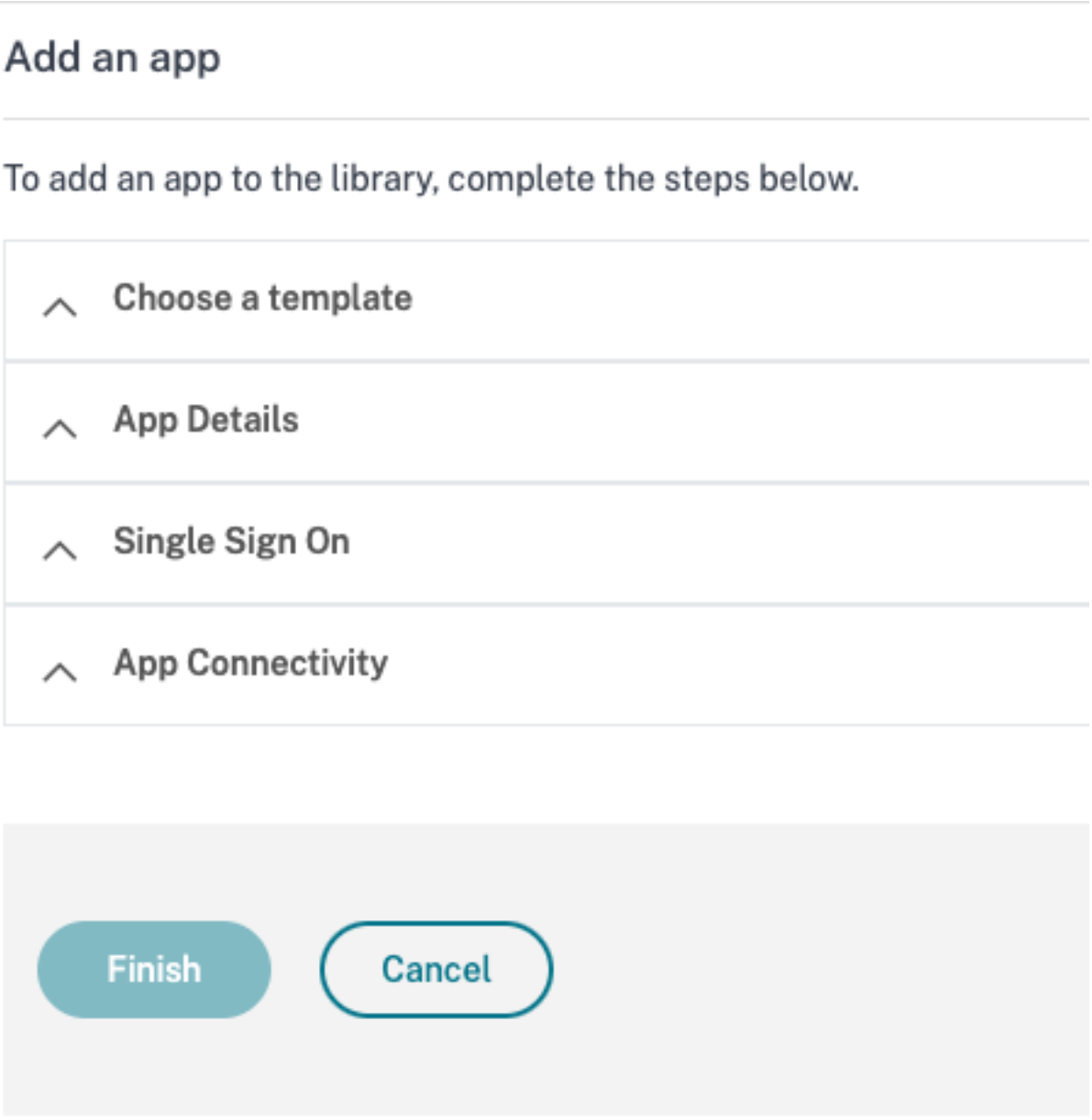
Pour modifier la méthode d'authentification existante ou modifier la méthode d'authentification existante, cliquez sur **Authentification de l'espace de travail**.

Étape 2 : ajouter et gérer des applications

Après avoir sélectionné la méthode d'authentification, configurez les applications. Pour les nouveaux utilisateurs, la page de destination **Applications** n'affiche aucune application. Ajoutez une application en cliquant sur **Ajouter une application**. Vous pouvez ajouter des applications SaaS, des applications Web et des applications TCP/UDP à partir de cette page. Pour ajouter une application, cliquez sur **Ajouter une application**.

Une fois que vous avez ajouté une application, vous pouvez la voir répertoriée ici.

Suivez les étapes affichées dans la figure suivante pour ajouter une application.



- **Ajouter une application Web d'entreprise**
  - Prise en charge des applications Web d'entreprise
  - Configurer l'accès direct aux applications Web
- **Ajouter une application SaaS**
  - Prise en charge de l'application Software as a Service
  - Configuration spécifique au serveur d'applications SaaS
- **Configurer les applications client-serveur**
  - Prise en charge des applications client-serveur

- **Lancer une application**
  - Lancer une application configurée –flux de travail de l'utilisateur final
- **Activer l'accès en lecture seule pour les administrateurs**
  - Accès en lecture seule pour les administrateurs aux applications SaaS et Web

Étape 3 : Configurer une politique d'accès avec plusieurs règles

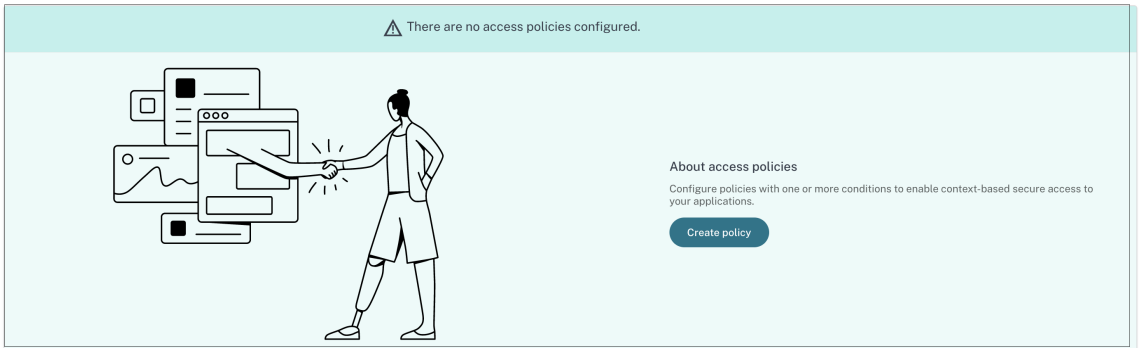
Vous pouvez créer plusieurs règles d'accès et configurer différentes conditions d'accès pour différents utilisateurs ou groupes d'utilisateurs au sein d'une même politique. Ces règles peuvent être appliquées séparément pour les applications HTTP/HTTPS et TCP/UDP, le tout au sein d'une seule politique.

Les politiques d'accès au sein de Secure Private Access vous permettent d'activer ou de désactiver l'accès aux applications en fonction du contexte de l'utilisateur ou de l'appareil de l'utilisateur. De plus, vous pouvez activer l'accès restreint aux applications en ajoutant les restrictions de sécurité suivantes :

- Restreindre l'accès au presse-papiers
- Restreindre l'impression
- Restreindre les téléchargements
- Restreindre les téléchargements
- Afficher le filigrane
- Restreindre l'enregistrement des touches
- Restreindre la capture d'écran

Pour plus d'informations sur ces restrictions, consultez Restrictions d'accès disponibles.

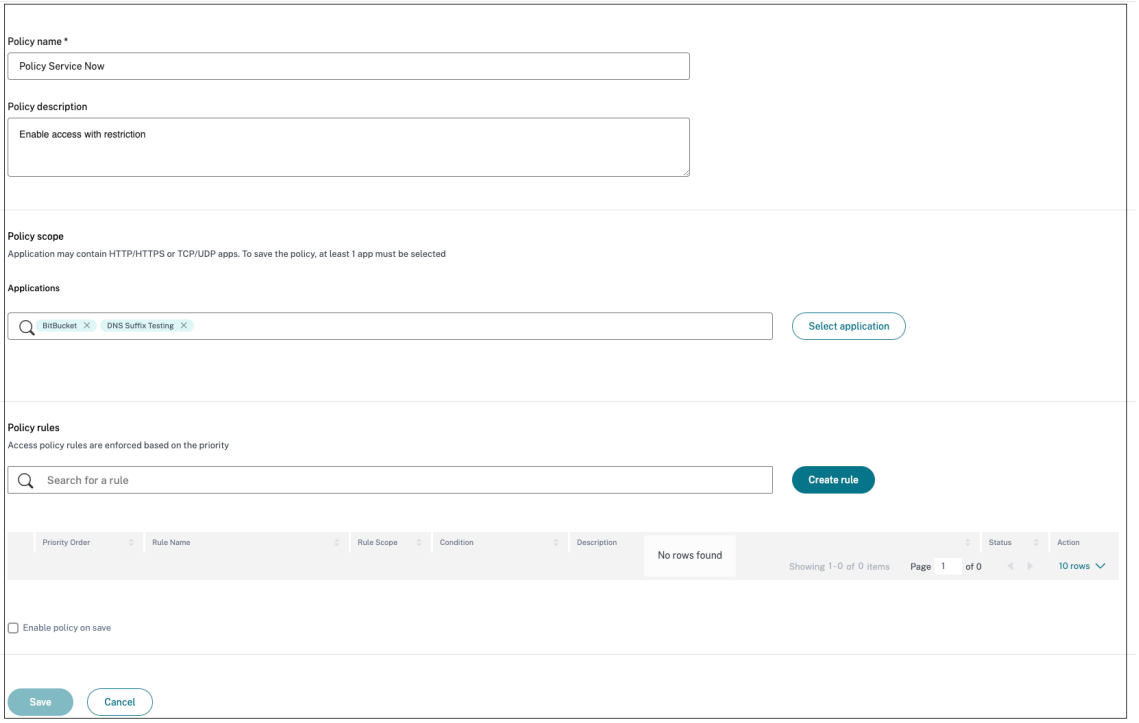
1. Dans le volet de navigation, cliquez sur **Stratégies d'accès** puis sur **Créer une stratégie**.



   Pour les nouveaux utilisateurs, la page de destination **Politiques d'accès** n'affiche aucune politique. Une fois que vous avez créé une politique, vous pouvez la voir répertoriée ici.

2. Saisissez le nom de la politique et la description de la politique.

3. Dans **Applications**, sélectionnez l'application ou l'ensemble d'applications sur lesquelles cette politique doit être appliquée.
4. Cliquez sur **Créer une règle** pour créer des règles pour la politique.



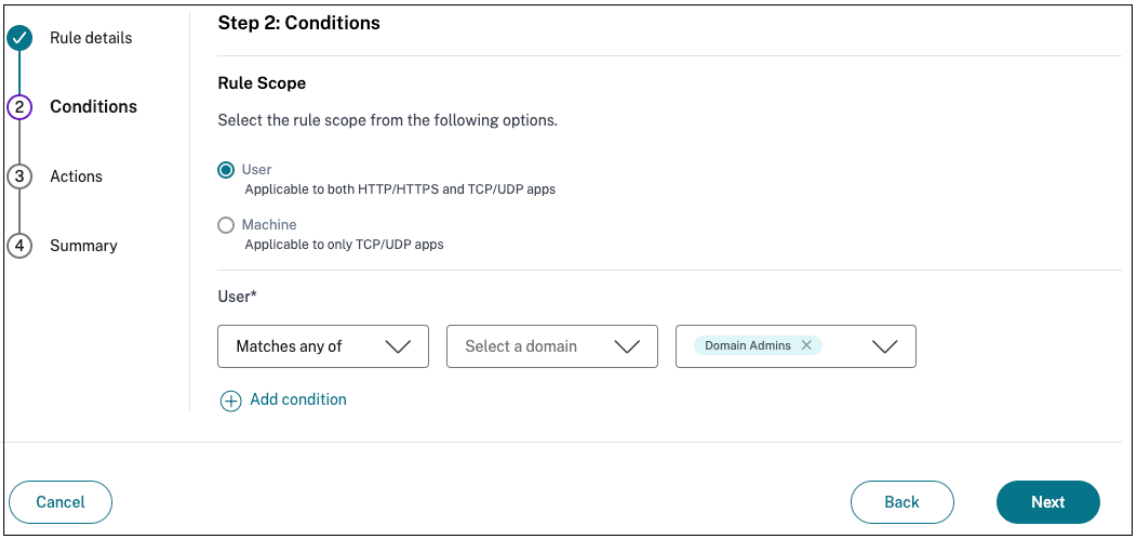
5. Saisissez le nom de la règle et une brève description de la règle, puis cliquez sur **Suivant**.

6. Sélectionnez les conditions des utilisateurs. La condition **Utilisateurs** est une condition obligatoire à respecter pour accorder l'accès aux applications aux utilisateurs. Sélectionnez l'une des options suivantes :

   - **Correspond à l'un des** –Seuls les utilisateurs ou groupes qui correspondent à l'un des

noms répertoriés dans le champ et appartenant au domaine sélectionné sont autorisés à accéder.

- **Ne correspond à aucun** - Tous les utilisateurs ou groupes, à l'exception de ceux répertoriés dans le champ et appartenant au domaine sélectionné, sont autorisés à accéder.



7. (Facultatif) Cliquez sur + pour ajouter plusieurs conditions en fonction du contexte.

   Lorsque vous ajoutez des conditions basées sur un contexte, une opération AND est appliquée aux conditions dans lesquelles la politique est évaluée uniquement si les **Utilisateurs** et les conditions contextuelles facultatives sont remplies. Vous pouvez appliquer les conditions suivantes en fonction du contexte.

   - **Bureau** ou **Appareil mobile** –Sélectionnez l'appareil pour lequel vous souhaitez activer l'accès aux applications.
   - **Géolocalisation** –Sélectionnez la condition et l'emplacement géographique à partir duquel les utilisateurs accèdent aux applications.
     - **Correspond à l'un des éléments suivants :** Seuls les utilisateurs ou les groupes d'utilisateurs accédant aux applications à partir de l'un des emplacements géographiques répertoriés sont autorisés à accéder aux applications.
     - **Ne correspond à aucun :** Tous les utilisateurs ou groupes d'utilisateurs autres que ceux des emplacements géographiques répertoriés ont accès.
   - **Emplacement réseau** –Sélectionnez la condition et le réseau via lesquels les utilisateurs accèdent aux applications.
     - **Correspond à l'un des éléments suivants :** Seuls les utilisateurs ou les groupes d'utilisateurs accédant aux applications à partir de l'un des emplacements réseau répertoriés sont autorisés à accéder aux applications.
     - **Ne correspond à aucun :** Tous les utilisateurs ou groupes d'utilisateurs autres que ceux des emplacements réseau répertoriés ont accès.

- **Vérification de la posture de l'appareil** –Sélectionnez les conditions que l'appareil de l'utilisateur doit respecter pour accéder à l'application.
- **Score de risque utilisateur** –Sélectionnez les catégories de score de risque en fonction desquelles les utilisateurs doivent avoir accès à l'application.
- **URL de l'espace de travail** - Les administrateurs peuvent spécifier des filtres en fonction du nom de domaine complet correspondant à l'espace de travail.
  - **Correspond à l'un des** - Autoriser l'accès uniquement lorsque la connexion utilisateur entrante correspond à l'une des URL d'espace de travail configurées.
  - **Correspond à tout ce qui suit :** - Autorise l'accès uniquement lorsque la connexion utilisateur entrante correspond à toutes les URL d'espace de travail configurées.

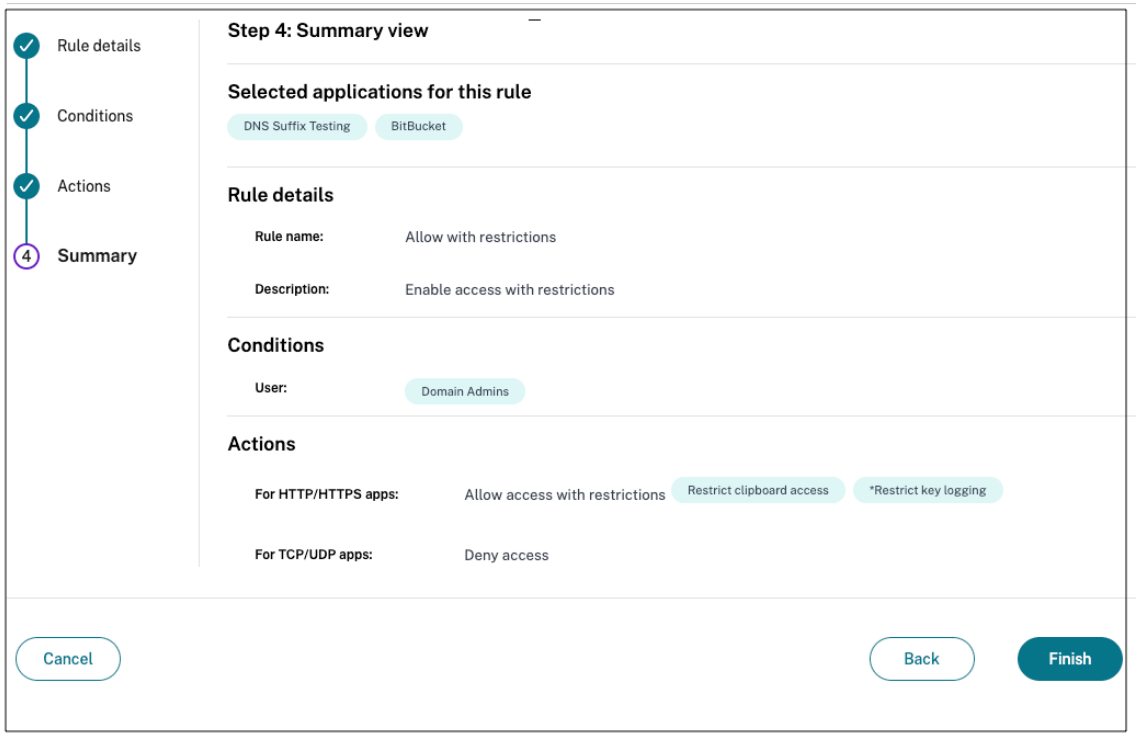
8. Dans **Commandes CLI équivalentes**, passez en revue les commandes et cliquez sur **Suivant**.
9. Sélectionnez les actions qui doivent être appliquées en fonction de l'évaluation de la condition.

   - Pour les applications HTTP/HTTPS, vous pouvez sélectionner les éléments suivants :
     - **Autoriser l'accès**
     - **Autoriser l'accès avec des restrictions**
     - **Refuser l'accès**

> **Remarque**
>
> Si vous sélectionnez **Autoriser l'accès avec des restrictions**, vous devez alors sélectionner les restrictions que vous souhaitez appliquer aux applications. Pour plus de détails sur les restrictions, voir Restrictions d'accès disponibles. Vous pouvez également spécifier si vous souhaitez que l'application s'ouvre dans un navigateur distant ou dans Citrix Secure Browser.

```
- Pour l'accès TCP/UDP, vous pouvez sélectionner les éléments
   suivants :
   - **Autoriser l'accès**
   - **Refuser l'accès**

![Créer une action de règle](/en-us/citrix-secure-private-access/media/
   secure-private-access-policy-rule-actions.png)
```

1. Dans **Commandes CLI équivalentes**, passez en revue les commandes et cliquez sur **Suivant**. La page Résumé affiche les détails de la politique.
2. Vous pouvez vérifier les détails et cliquer sur **Terminer**.



Points à retenir après la création d'une politique

- La politique que vous avez créée apparaît sous la section Règles de politique et est activée par défaut. Vous pouvez désactiver les règles, si nécessaire. Cependant, assurez-vous qu'au moins une règle est activée pour que la politique soit active.
- Un ordre de priorité est attribué à la politique par défaut. La priorité avec une valeur inférieure a la préférence la plus élevée. La règle avec le numéro de priorité le plus bas est évaluée en premier. Si la règle (n) ne correspond pas aux conditions définies, la règle suivante (n+1) est évaluée et ainsi de suite.

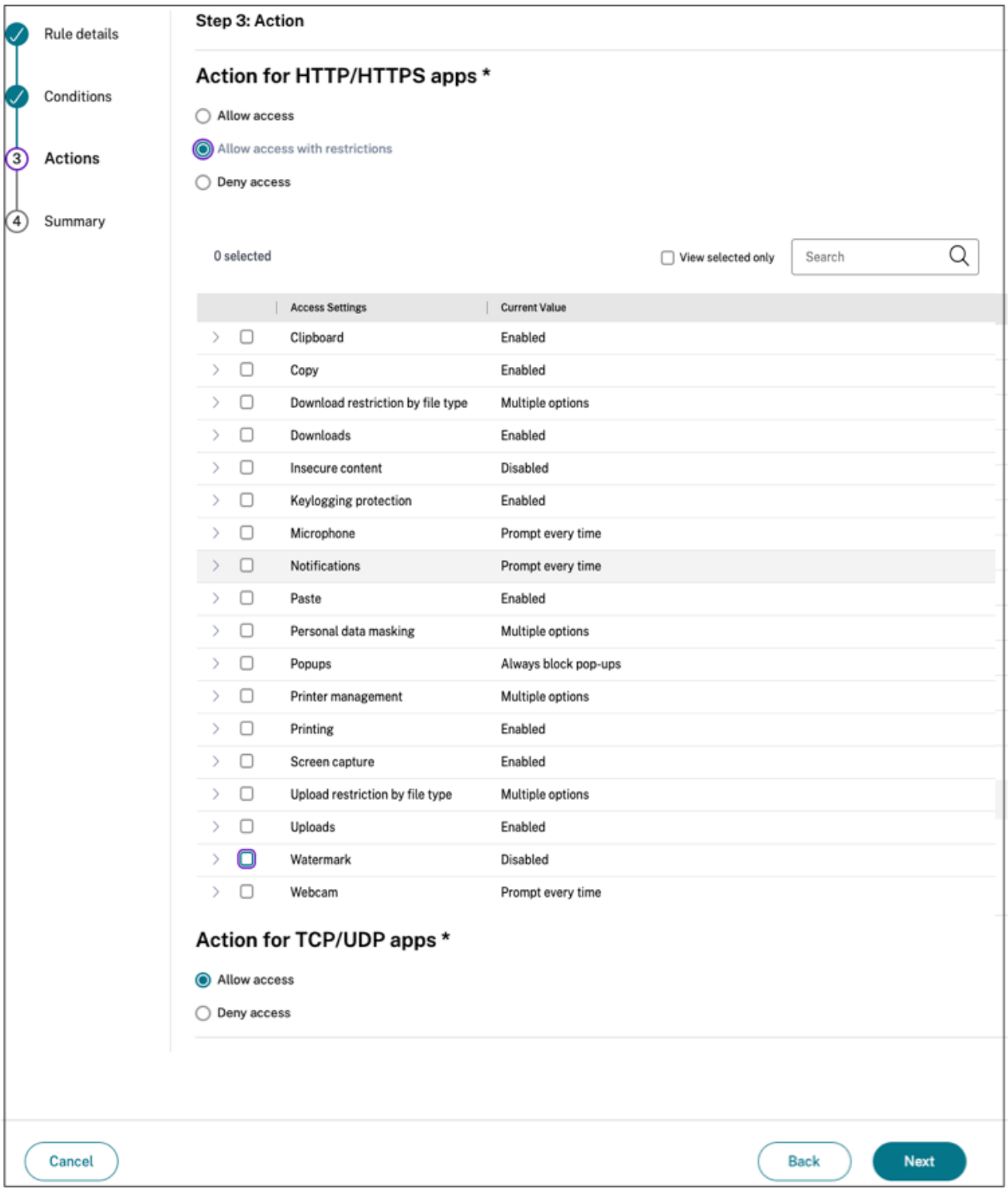
Exemple d'évaluation de règles avec ordre de priorité :

Considérez que vous avez créé deux règles, la règle 1 et la règle 2. La règle 1 est attribuée à l'utilisateur A et la règle 2 est attribuée à l'utilisateur B, puis les deux règles sont évaluées. Considérez que les deux règles Règle 1 et Règle 2 sont attribuées à l'utilisateur A. Dans ce cas, la règle 1 a la priorité la plus élevée. Si la condition de la règle 1 est remplie, alors la règle 1 est appliquée et la règle 2 est ignorée. Sinon, si la condition de la règle 1 n'est pas remplie, la règle 2 est appliquée à l'utilisateur A.

> **Remarque**
>
> Si aucune des règles n'est évaluée, l'application n'est pas répertoriée auprès des utilisateurs.

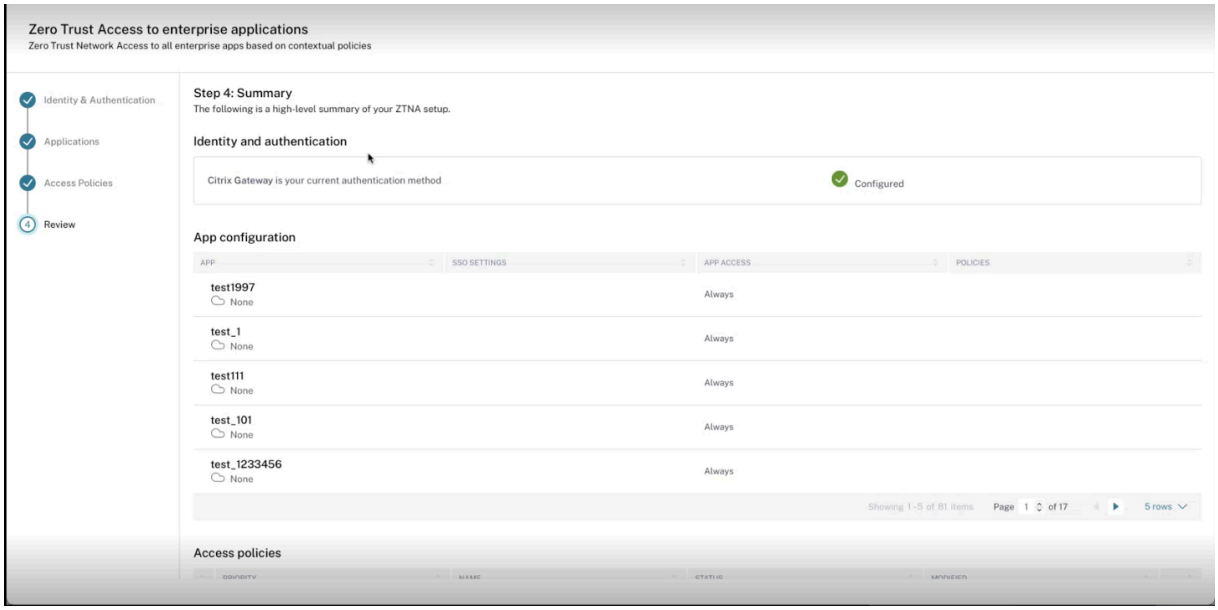
Options de restrictions d'accès disponibles

Lorsque vous sélectionnez l'action **Autoriser l'accès avec des restrictions**, vous devez sélectionner au moins une des restrictions de sécurité. Ces restrictions de sécurité sont prédéfinies dans le système. Les administrateurs ne peuvent pas modifier ou ajouter d'autres combinaisons. Les restrictions de sécurité suivantes peuvent être activées pour l'application. Pour plus de détails, voir Options de restrictions d'accès disponibles.

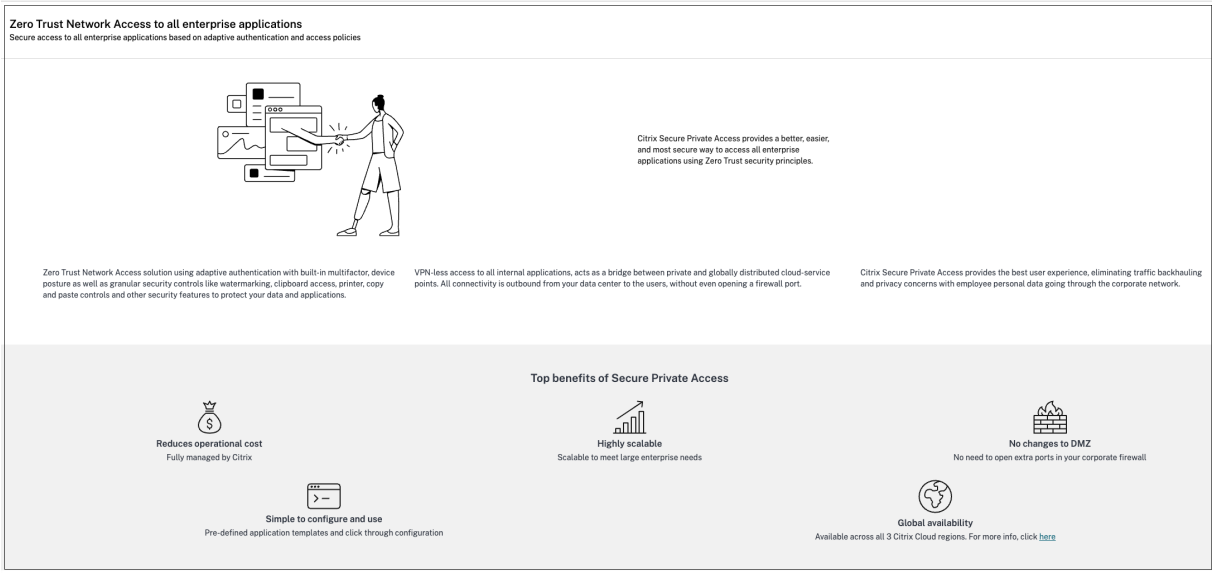


Étape 4 : Examiner le résumé de chaque configuration

Depuis la page d'évaluation, vous pouvez afficher la configuration complète de l'application, puis cliquer sur **Fermer**.

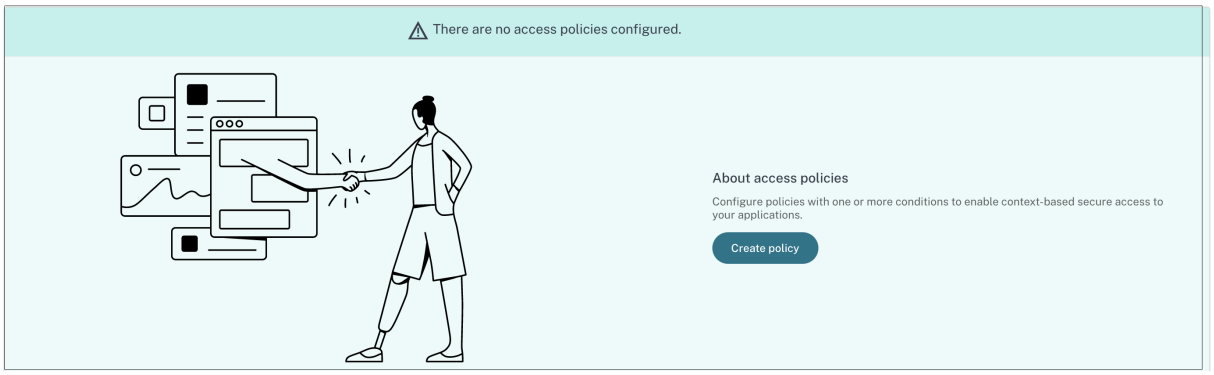


La figure suivante affiche la page une fois la configuration en 4 étapes terminée.



Important :

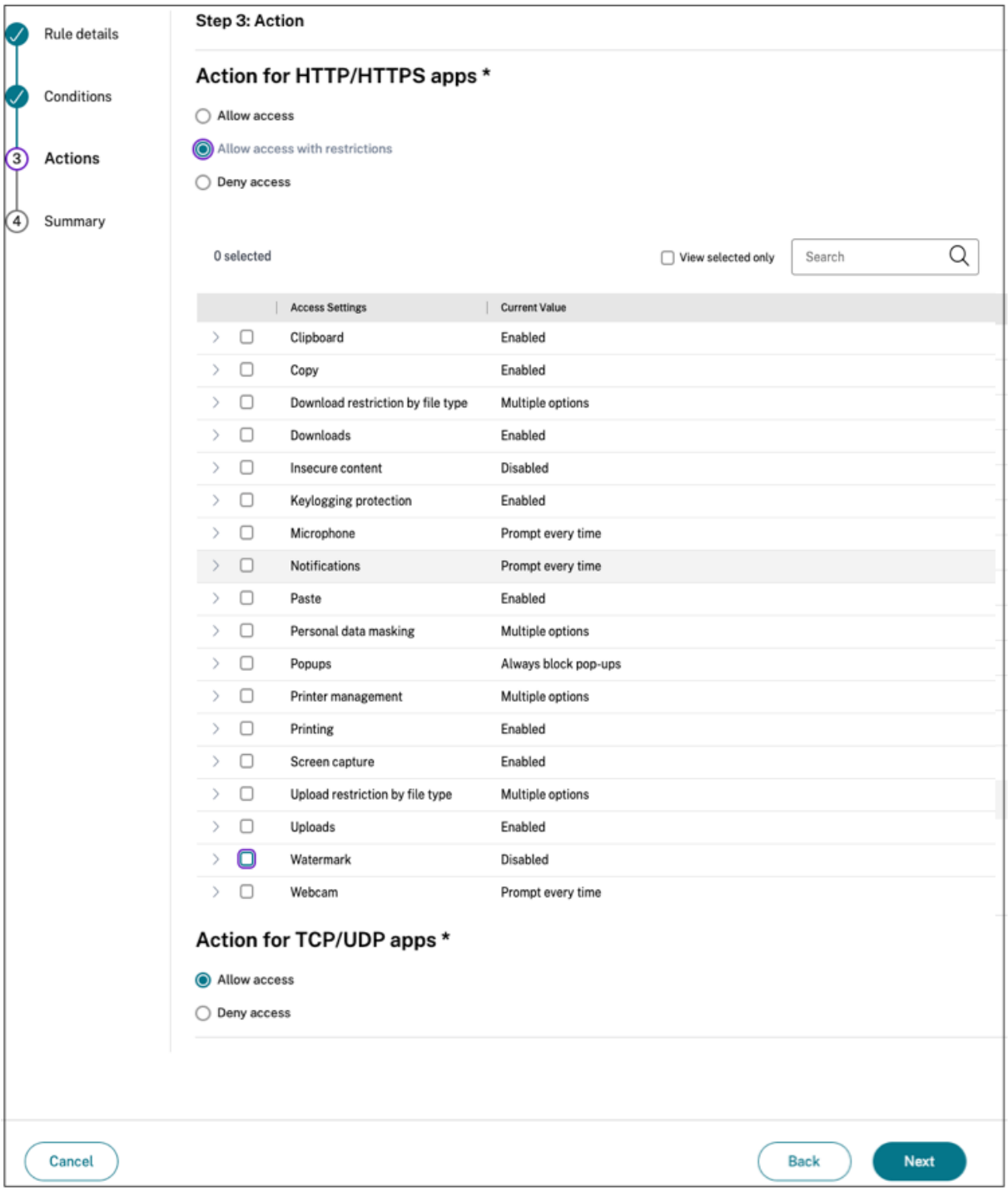
- Après avoir terminé la configuration à l'aide de l'assistant, vous pouvez modifier la configuration d'une section en allant directement dans cette section. Vous n'êtes pas obligé de suivre la séquence.
- Si vous supprimez toutes les applications configurées ou les politiques, vous devez les ajouter à nouveau. Dans ce cas, l'écran suivant apparaît si vous avez supprimé toutes les politiques.



Options de restriction d'accès

October 21, 2024

Lorsque vous sélectionnez l'action **Autoriser l'accès avec des restrictions** lors de la création d'une politique d'accès, vous pouvez sélectionner les restrictions d'accès. Ces restrictions sont prédéfinies dans le système. Les administrateurs ne peuvent pas modifier ou ajouter d'autres combinaisons. Pour plus de détails sur la création d'une politique d'accès et l'activation des restrictions d'accès, voir Configurer une politique d'accès.



Presse-papiers

Activez/désactivez les opérations couper/copier/coller sur une application Web SaaS ou interne avec cette politique d'accès lors de l'accès via Citrix Enterprise Browser. Valeur par défaut : Activé.

Copier

Activez/désactivez la copie des données à partir d'une application SaaS ou Web interne avec cette politique d'accès lors de l'accès via Citrix Enterprise Browser. Valeur par défaut : Activé.

> **Remarque**
>
> - Si les deux restrictions **Presse-papiers** et **Copier** sont activées dans une stratégie, la restriction **Presse-papiers** a priorité sur la restriction **Copier** .
> - Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 2405 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.
> - Pour un contrôle granulaire de l'opération de copie au sein des applications, les administrateurs peuvent utiliser la restriction **Groupes de sécurité** . Pour plus de détails, voir Restriction du presse-papiers pour les groupes de sécurité.

Restriction de téléchargement par type de fichier

Activez/désactivez la capacité de l'utilisateur à télécharger un type MIME (fichier) spécifique à partir de l'application Web SaaS ou interne avec cette politique lors de l'accès via Citrix Enterprise Browser.

> **Remarque**
>
> - La restriction de téléchargement **par type de fichier** est disponible en plus de la restriction de téléchargement ** .
> - Si les deux restrictions **Téléchargements** et **Restriction de téléchargement par type de fichier** sont activées dans une politique, la restriction **Téléchargements** a priorité sur la restriction **Restriction de téléchargement par type de fichier** .
> - Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 2405 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.

Pour activer le téléchargement des types MIME, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Restriction de téléchargement par type de fichier** puis cliquez sur **Modifier**.
4. Dans la page **Paramètres de restriction de téléchargement par type de fichier** , sélectionnez l'une des options suivantes :
    - **Autoriser tous les téléchargements avec des exceptions** –Sélectionnez les types qui doivent être bloqués et autorisez tous les autres types.

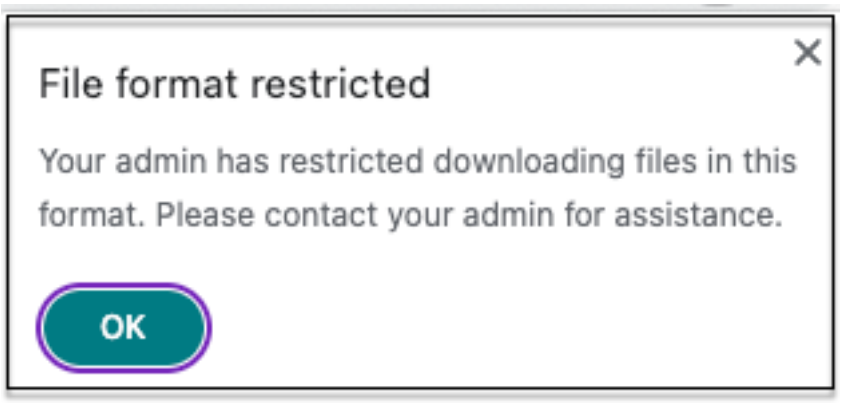
- **Bloquer tous les téléchargements avec des exceptions** –Sélectionnez uniquement les types qui peuvent être téléchargés et bloquez tous les autres types.

5. Si le type de fichier n'existe pas dans la liste, procédez comme suit :

   a) Cliquez sur **Ajouter des types MIME personnalisés**.
   b) Dans **Ajouter les types MIME**, entrez le type MIME au format `catégorie/sous-catégorie<extension>`. Par exemple `image/png`.
   c) Cliquez sur **Terminé**.
   d) Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

   Le type MIME apparaît désormais dans la liste des exceptions.

Lorsqu'un utilisateur final tente de télécharger un type de fichier restreint, Citrix Enterprise Browser affiche le message suivant :



Téléchargements

Activez/désactivez la capacité de l'utilisateur à télécharger depuis l'application SaaS ou Web interne avec cette politique lorsqu'il y accède via le navigateur Citrix Enterprise. Valeur par défaut : Activé.

> **Remarque**
>
> Si les deux restrictions **Téléchargements** et **Restriction de téléchargement par type de fichier** sont activées dans une politique, la restriction **Téléchargements** a priorité sur la restriction **Restriction de téléchargement par type de fichier**.

Contenu non sécurisé

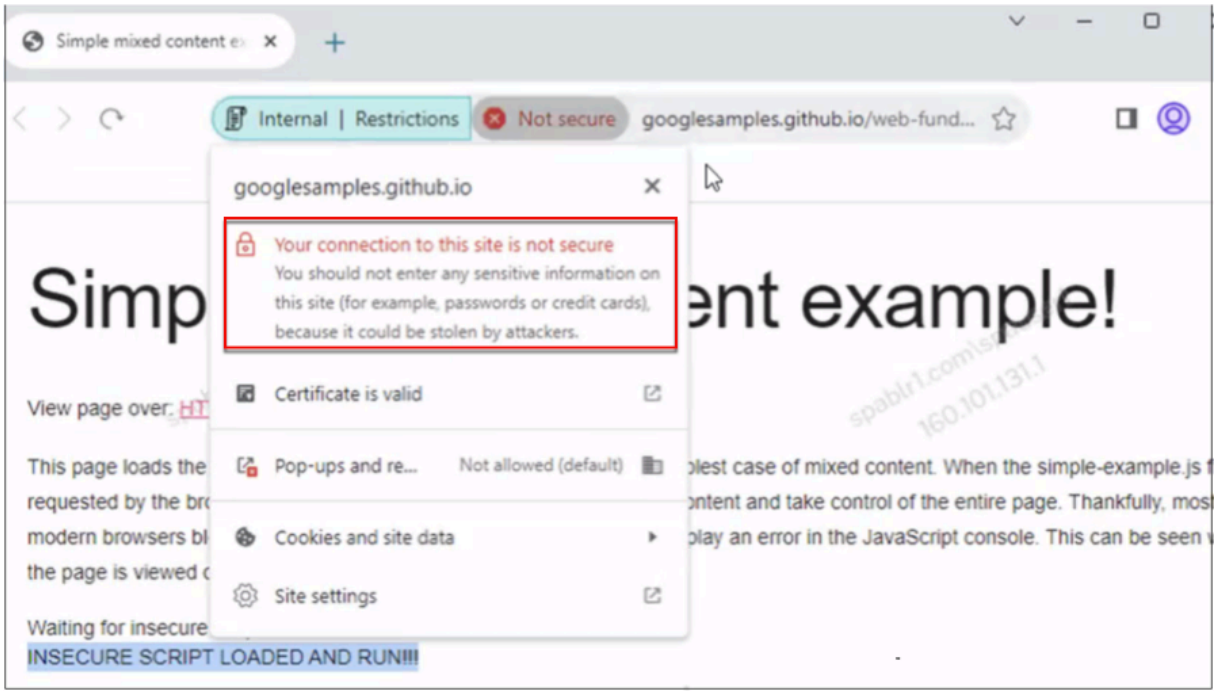
Autorisez/désactivez l'accès des utilisateurs finaux au contenu non sécurisé dans l'application SaaS ou Web interne configurée avec cette politique lorsqu'ils y accèdent via Citrix Enterprise Browser. Le contenu non sécurisé est tout fichier lié à une page Web à l'aide d'un lien HTTP plutôt que d'un lien HTTPS. Valeur par défaut : Désactivé.

Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour désactiver l'accès au contenu non sécurisé.

Pour activer l'accès au contenu non sécurisé, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Sélectionnez **Contenu non sécurisé**.
4. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

La figure suivante affiche un exemple de notification lorsque vous accédez à du contenu non sécurisé.



Protection contre l'enregistrement des frappes

Activez/désactivez les enregistreurs de frappe pour capturer les frappes au clavier à partir de l'application SaaS ou Web interne avec cette politique d'accès lors de l'accès via Citrix Enterprise Browser. Valeur par défaut : Activé.

Microphone

Inviter/ne pas inviter les utilisateurs à chaque fois à accéder au microphone dans l'application SaaS ou Web interne configurée avec cette politique lorsqu'elle est accessible via Citrix Enterprise Browser. Valeur par défaut : demander à chaque fois.

Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour accéder aux applications pour lesquelles la restriction **Microphone** est activée.

Pour activer le microphone à chaque fois sans y être invité, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Microphone** puis sur **Modifier**.
4. Dans la page **Paramètres du microphone** , cliquez sur **Toujours autoriser l'accès**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

> **Remarque**
>
> - Si la restriction **Microphone** est activée dans la stratégie Accès privé sécurisé, Citrix Enterprise Browser affiche les paramètres **Autoriser**.
> - Si l'option **Demander à chaque fois** dans la stratégie d'accès privé sécurisé, le paramètre appliqué sur Citrix Enterprise Browser varie selon que le service de configuration globale des applications (GACS) est utilisé ou non pour gérer Citrix Enterprise Browser.
> - Si GACS est utilisé, le paramètre GACS est appliqué sur Citrix Enterprise Browser.
> - Si GACS n'est pas utilisé, Citrix Enterprise Browser affiche le paramètre **Demander**.

Pour plus d'informations sur GACS, consultez Gérer Citrix Enterprise Browser via le service Global App Configuration.

Notifications

Autoriser/inviter les utilisateurs à chaque fois à afficher les notifications dans l'application SaaS ou Web interne configurée avec cette politique lorsqu'elle est accessible via Citrix Enterprise Browser. Valeur par défaut : demander à chaque fois.

Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée.

Pour bloquer les notifications sans invite, procédez comme suit.

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Notifications** puis sur **Modifier**.
4. Dans la page **Paramètres de notification** , cliquez sur **Toujours bloquer les notifications**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Coller

Activez/désactivez le collage des données copiées dans l'application SaaS ou Web interne avec cette politique d'accès lors de l'accès via Citrix Enterprise Browser. Valeur par défaut : Activé.

> **Remarque**
>
> - Si les deux restrictions **Presse-papiers** et **Coller** sont activées dans une stratégie, la restriction **Presse-papiers** a priorité sur la restriction **Coller** .
> - Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.
> - Pour un contrôle granulaire de l'opération de collage dans les applications, les administrateurs peuvent utiliser la restriction **Groupes de sécurité** . Pour plus de détails, voir Restriction du presse-papiers pour les groupes de sécurité.

Masquage des données personnelles

Activez/désactivez la rédaction ou le masquage des informations personnelles identifiables (PII) sur l'application SaaS ou Web interne avec cette politique lors de l'accès via Citrix Enterprise Browser. Les informations personnelles identifiables peuvent être des numéros de carte de crédit, des numéros de sécurité sociale, des dates, etc. Vous pouvez également définir des règles personnalisées pour détecter des types spécifiques d'informations sensibles et les masquer en conséquence. Les restrictions de masquage des données personnelles offrent également la possibilité de masquer totalement ou partiellement les informations.

> **Remarque**
>
> Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 2405 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.

Pour rédiger ou masquer des informations personnelles identifiables, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Masquage des données personnelles** puis cliquez sur **Modifier**.
4. Sélectionnez le type d'informations que vous souhaitez masquer, puis cliquez sur **Ajouter**.

   Si le type d'informations n'apparaît pas dans la liste prédéfinie, vous pouvez ajouter un type d'informations personnalisé. Pour plus de détails, voir Ajouter un type d'informations personnalisé.

5. Sélectionnez le type de masquage.

    - **Masquage complet** –Couvrez complètement les informations sensibles pour les rendre illisibles.
    - **Masquage partiel** –Couvrir partiellement les informations sensibles. Seules les sections pertinentes sont couvertes, laissant le reste intact.

      Lorsque vous sélectionnez **Marquage partiel**, vous devez sélectionner des caractères à partir du début ou de la fin du document. Vous devez saisir les chiffres dans les champs **Premiers caractères masqués** et **Derniers caractères masqués** .

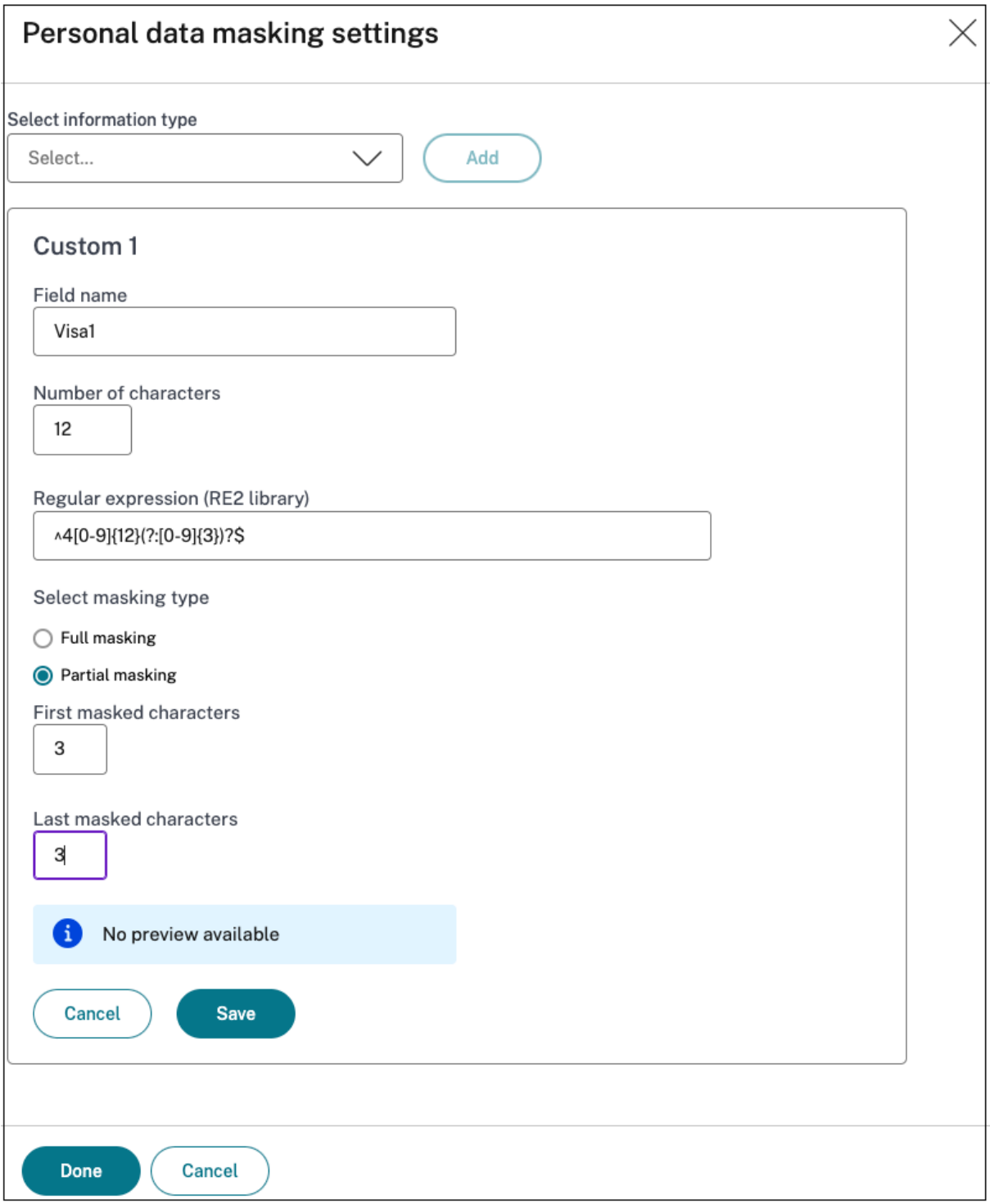
      Le champ **Aperçu** affiche le format de masquage. Cet aperçu n'est pas disponible pour les politiques personnalisées.

6. Cliquez sur **Enregistrer** puis cliquez sur **Terminé**.
7. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

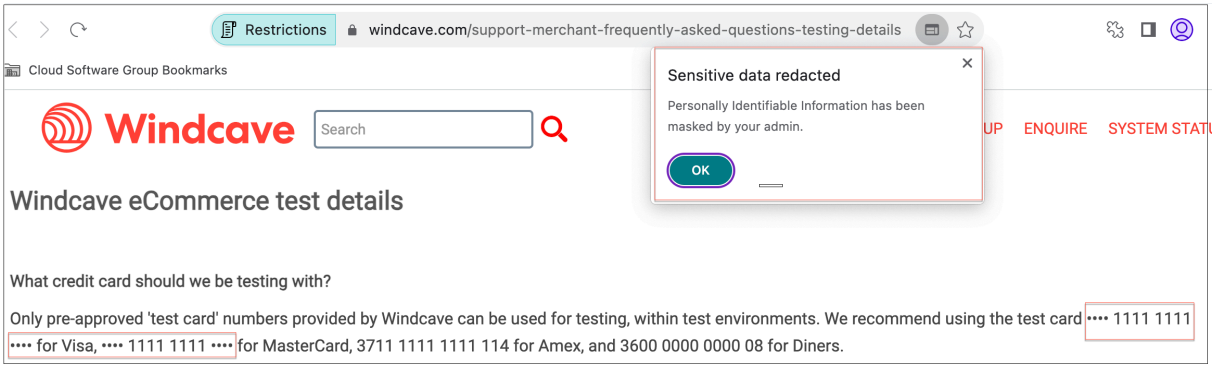
Ajouter un type d'informations personnalisé

Vous pouvez ajouter un type d'informations personnalisé en ajoutant l'expression régulière du type d'informations.

1. Dans **Sélectionnez le type d'informations**, sélectionnez **Personnalisé**, puis cliquez sur **Ajouter**.
2. Dans **Nom du champ**, entrez le nom du type d'informations que vous souhaitez masquer.
3. Dans **Nombre de caractères**, entrez le nombre de caractères du type d'information.
4. Dans **Expression régulière (bibliothèque RE2)**, saisissez l'expression pour le type d'informations personnalisé. Par exemple, `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Sélectionnez le type de masquage, si vous souhaitez masquer les informations complètes ou les premiers ou derniers caractères.
6. Cliquez sur **Enregistrer**, puis cliquez sur **Terminé**.
7. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.



La figure suivante affiche un exemple d'application dans laquelle les informations personnelles identifiables sont masquées. L'image affiche également la notification relative au masquage des informations personnelles identifiables.



Pop-ups

Activez/désactivez l'affichage des fenêtres contextuelles dans l'application Web SaaS ou interne configurée avec cette politique lors de l'accès via Citrix Enterprise Browser. Par défaut, les fenêtres contextuelles sont désactivées dans les pages Web. Valeur par défaut : Toujours bloquer les pop-ups.

Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée.

Pour activer l'affichage des fenêtres contextuelles, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Popups** puis sur **Modifier**.
4. Dans la page **Paramètres des pop-ups** , cliquez sur **Toujours autoriser les pop-ups**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Impression

Activez/désactivez l'impression des données à partir des applications Web SaaS ou internes configurées avec cette politique lors de l'accès via le navigateur Citrix Enterprise. Valeur par défaut : Activé.

Le message suivant s'affiche lorsqu'un utilisateur final tente d'imprimer du contenu à partir de l'application pour laquelle la restriction d'impression est activée.

> **Remarque**
>
> Si les deux restrictions **Impression** et **Gestion des imprimantes** sont activées dans une stratégie, la restriction **Impression** a priorité sur la restriction **Gestion des imprimantes** .

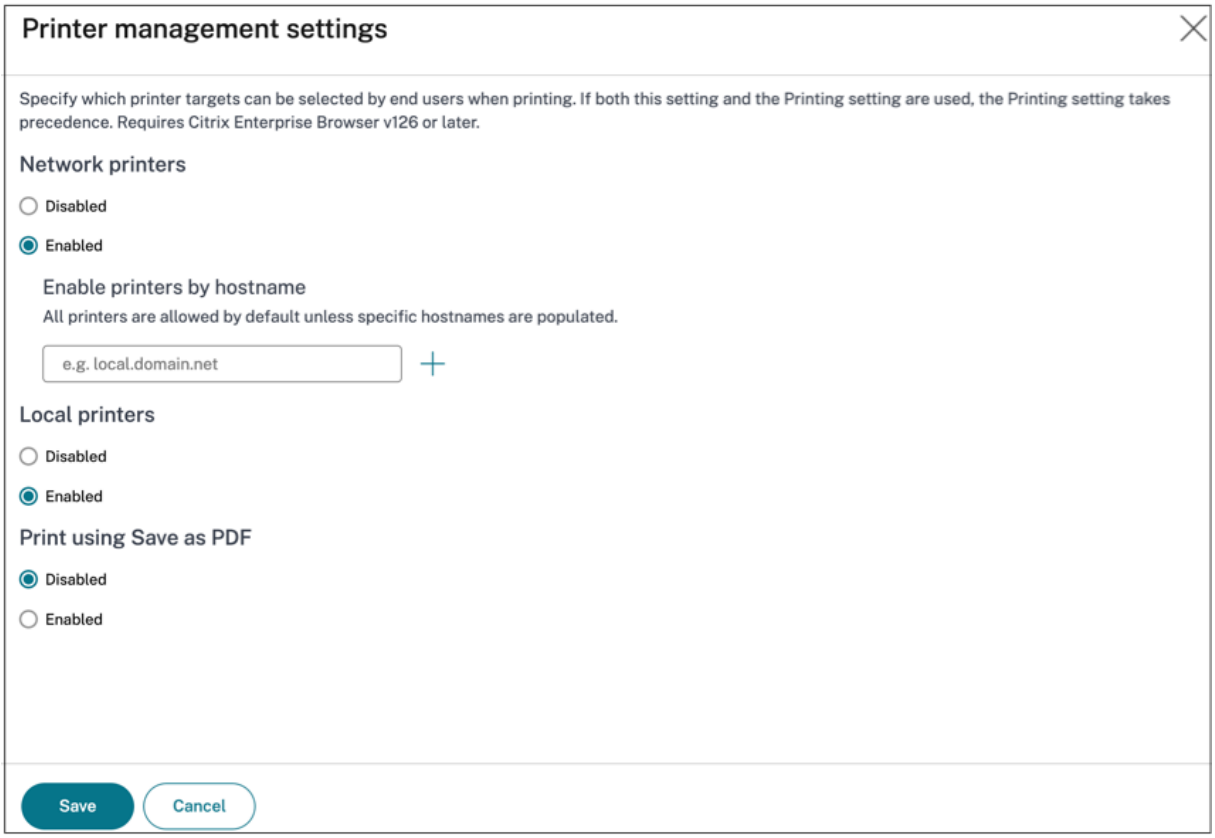
Gestion des imprimantes

Activez/désactivez l'impression des données à l'aide des imprimantes configurées par l'administrateur à partir des applications SaaS ou Web internes configurées avec cette politique lors de l'accès via Citrix Enterprise Browser.

> **Remarque**
>
> - La restriction **Gestion de l'imprimante** est disponible en plus de la restriction **Impression** où l'impression est soit activée, soit désactivée. Si les deux restrictions **Impression** et **Gestion des imprimantes** sont activées dans une politique d'accès, la restriction **Impression** a priorité sur la restriction **Gestion des imprimantes** .
> - Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 2405 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.

Pour activer/désactiver les restrictions d'impression, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Gestion de l'imprimante** puis cliquez sur **Modifier**.



1. Sélectionnez les exceptions selon vos besoins.

   - **Imprimantes réseau** - Une imprimante réseau est une imprimante qui peut être connectée à un réseau et utilisée par plusieurs utilisateurs.

     - **Désactivé :** l'impression à partir de n'importe quelle imprimante du réseau est désactivée.
     - **Activé :** l'impression à partir de toutes les imprimantes réseau est activée. Si des noms d'hôtes d'imprimante sont spécifiés, toutes les autres imprimantes réseau autres que celles spécifiées sont bloquées.

     Remarque : Les imprimantes réseau sont identifiées par leurs noms d'hôte.

   - **Imprimantes locales** - Une imprimante locale est un périphérique directement connecté à un ordinateur individuel via une connexion filaire. Cette connexion est généralement facilitée via USB, des ports parallèles ou d'autres interfaces directes.

     - **Désactivé :** l'impression à partir de toutes les imprimantes locales est désactivée.
     - **Activé :** l'impression à partir de toutes les imprimantes locales est activée.

   - **Imprimer à l'aide de l'option Enregistrer au format PDF**

     - **Désactivé**: L'enregistrement du contenu de l'application au format PDF est désactivé.

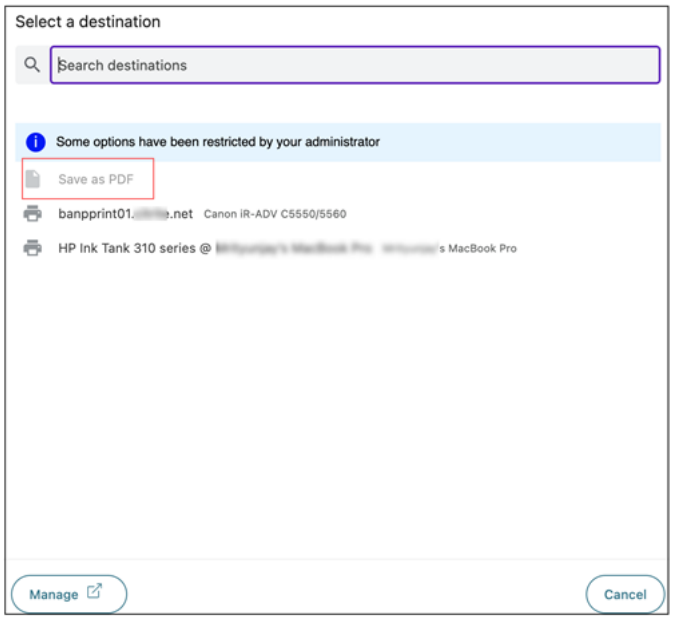
- **Activé :** L'enregistrement du contenu de l'application au format PDF est activé.

2. Cliquez sur **Enregistrer**.
3. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Si une imprimante réseau est désactivée, le nom de l'imprimante spécifique apparaît grisé lorsque les utilisateurs finaux tentent de sélectionner l'imprimante dans le champ **Destination** .

De plus, si **Imprimer en utilisant l'enregistrement au format PDF** est désactivé, alors lorsque vous cliquez sur le lien **Voir plus** dans le champ **Destination** , l'option **Enregistrer au format PDF** apparaît grisée.

Si les utilisateurs finaux renomment les imprimantes réseau, ils ne peuvent pas utiliser l'imprimante réseau.



Capture d'écran

Activez/désactivez la possibilité de capturer les écrans de l'application SaaS ou Web interne avec cette politique lors de l'accès via Citrix Enterprise Browser à l'aide de l'un des programmes ou applications de capture d'écran. Si un utilisateur tente de capturer l'écran, un écran vide est capturé. Valeur par défaut : Activé.

Restriction de téléchargement par type de fichier

Activez/désactivez la capacité de l'utilisateur à télécharger un type MIME (fichier) spécifique à partir de l'application Web SaaS ou interne avec cette politique lors de l'accès via Citrix Enterprise Browser.

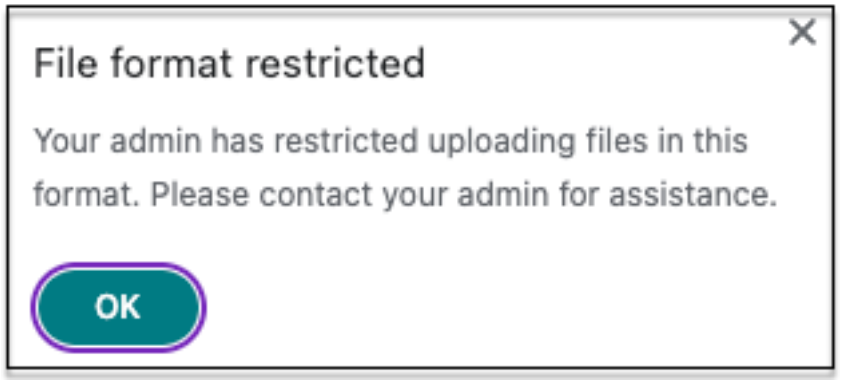
> **Remarque**
>
> - La restriction de téléchargement **par type de fichier** est disponible en plus de la restriction de téléchargement ** .
> - Si les restrictions **Téléchargement** et **Restriction de téléchargement par type de fichier** sont toutes deux activées dans une politique, la restriction **Téléchargements** a priorité sur la restriction **Restriction de téléchargement par type de fichier** .
> - Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 2405 ou ultérieure pour accéder aux applications pour lesquelles cette restriction est activée. Sinon, l'accès à l'application est restreint.

Pour activer/désactiver le téléchargement de types MIME, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Restriction de téléchargement par type de fichier** puis cliquez sur **Modifier**.
4. Dans la page **Paramètres de restriction de téléchargement par type de fichier** , sélectionnez l'une des options suivantes :
   - **Autoriser tous les téléchargements avec des exceptions** –Télécharger tous les fichiers sauf les types sélectionnés.
   - **Bloquer tous les téléchargements avec des exceptions** –Bloque le téléchargement de tous les types de fichiers, à l'exception des types sélectionnés.
5. Si le type de fichier n'existe pas dans la liste, procédez comme suit :
   a) Cliquez sur **Ajouter des types MIME personnalisés**.
   b) Dans **Ajouter les types MIME**, entrez le type MIME au format `catégorie/sous-catégorie<extension>`. Par exemple `image/png`.
   c) Cliquez sur **Terminé**.
   d) Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

   Le type MIME apparaît désormais dans la liste des exceptions.

Lorsqu'un utilisateur final tente de télécharger un type de fichier restreint, Citrix Enterprise Browser affiche un message d'avertissement.



Téléchargements

Activez/désactivez la capacité de l'utilisateur à télécharger dans l'application SaaS ou Web interne configurée avec cette politique lorsqu'il est accessible via le navigateur Citrix Enterprise. Valeur par défaut : Activé.

> **Remarque**
>
> Si les deux restrictions **Téléchargements** et **Restriction de téléchargement par type de fichier** sont activées dans une politique, la restriction **Téléchargements** a priorité sur la restriction **Téléchargement par type de fichier**.

Filigrane

Activer/désactiver le filigrane sur l'écran de l'utilisateur affichant le nom d'utilisateur et l'adresse IP de la machine de l'utilisateur. Valeur par défaut : Désactivé.

Webcam

Inviter/ne pas inviter les utilisateurs à chaque fois à accéder à la webcam dans l'application Web SaaS ou interne configurée avec cette politique lors de l'accès via Citrix Enterprise Browser. Valeur par défaut : demander à chaque fois.

Les utilisateurs finaux doivent utiliser Citrix Enterprise Browser version 126 ou ultérieure pour accéder aux applications pour lesquelles la restriction **Webcam** est activée.

Pour autoriser la webcam à chaque fois sans y être invité, procédez comme suit :

1. Créer ou modifier une politique d'accès. Pour plus de détails, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Cliquez sur **Webcam** puis sur **Modifier**.
4. Dans la page **Paramètres de la webcam** , cliquez sur **Toujours autoriser l'accès**.

5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

> **Remarque**
>
> - Si la restriction **Webcam** est activée dans la stratégie Secure Private Access, Citrix Enterprise Browser affiche les paramètres **Autoriser**.
> - Si l'option **Demander chaque fois** est activée dans la stratégie Accès privé sécurisé, le paramètre appliqué sur Citrix Enterprise Browser varie selon que le service de configuration globale des applications (GACS) est utilisé ou non pour gérer Citrix Enterprise Browser.
> - Si GACS est utilisé, le paramètre GACS est appliqué sur Citrix Enterprise Browser.
> - Si GACS n'est pas utilisé, Citrix Enterprise Browser affiche le paramètre **Demander**.

Pour plus d'informations sur GACS, consultez Gérer Citrix Enterprise Browser via le service Global App Configuration.

Restriction du presse-papiers pour les groupes de sécurité

Vous pouvez restreindre l'accès au presse-papiers à n'importe quel groupe d'applications désigné. Ces groupes d'applications désignés sont créés en tant que groupes de sécurité afin que les utilisateurs finaux soient autorisés à copier et coller du contenu uniquement dans ces groupes de sécurité. Pour activer l'accès au presse-papiers dans les applications d'un groupe de sécurité, vous devez simplement avoir une politique d'accès configurée avec l'action **autoriser** ou **autoriser avec des restrictions** sans sélectionner aucun paramètre d'accès.

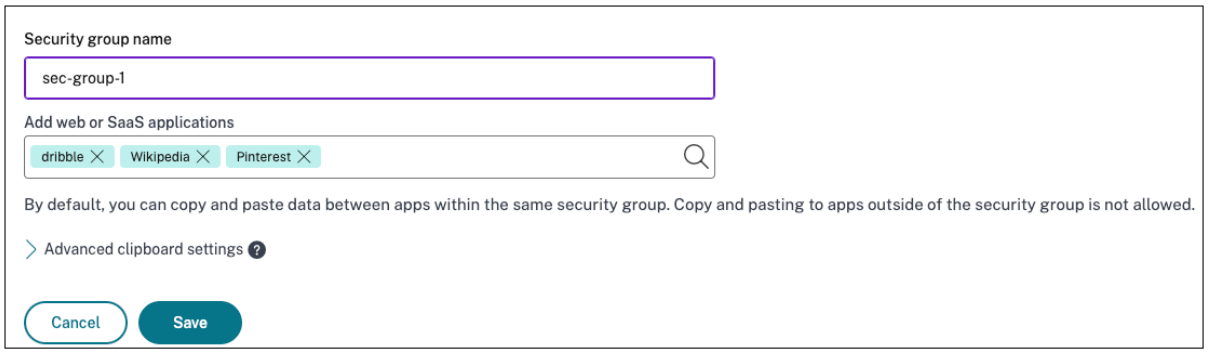
- Lorsque la restriction **Groupes de sécurité** est activée, vous ne pouvez pas copier/coller de données entre des applications dans différents groupes de sécurité. Par exemple, si l'application « ProdDocs » appartient au groupe de sécurité « SG1 » et l'application « Edocs » appartient au groupe de sécurité « SG2 », vous ne pouvez pas copier/coller le contenu de « Edocs » vers « ProdDocs » même si la restriction **Copier** / **Coller** est activée pour les deux groupes.
- Pour les applications ne faisant pas partie d'un groupe de sécurité, vous pouvez créer une politique d'accès avec l'action **autoriser avec des restrictions** et en sélectionnant les restrictions (**Copier**, **Coller**ou **Presse-papiers**). Dans ce cas, l'application ne fait pas partie d'un groupe de sécurité et la restriction **Copier / Coller** peut être appliquée sur cette application.

> **Remarque**
>
> Vous pouvez également restreindre l'accès au presse-papiers pour les applications accessibles via Citrix Enterprise Browser via le service Global App Configuration (GACS). Si vous utilisez GACS pour gérer Citrix Enterprise Browser, utilisez l'option **Presse-papiers sandboxé activé** pour gérer l'accès au presse-papiers. Lorsque vous limitez l'accès au presse-papiers via GACS, cela

> s'applique à toutes les applications accessibles via Citrix Enterprise Browser.

Pour créer un groupe de sécurité, procédez comme suit :

1. Dans la console Secure Private Access, cliquez sur **Applications** puis sur **Groupes de sécurité**.
2. Cliquez sur **Ajouter un nouveau groupe de sécurité**.

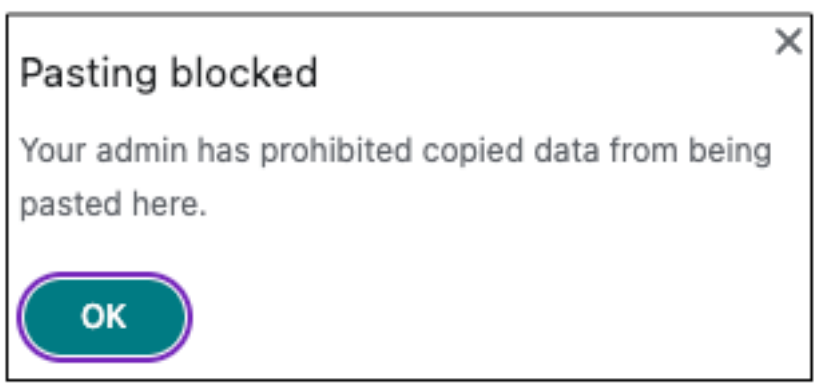


1. Entrez un nom pour le groupe de sécurité.
2. Dans **Ajouter des applications Web ou SaaS**, choisissez les applications que vous souhaitez regrouper pour activer le contrôle copier-coller. Par exemple, Wikipédia, Pinterest et Dribble.
3. Cliquez sur **Enregistrer**.

Pour plus de détails sur les **Paramètres avancés du presse-papiers** , voir Activer les contrôles copier/-coller pour les applications natives et les applications non publiées.

Lorsque les utilisateurs finaux lancent ces applications (Wikipedia, Pinterest et Dribble) depuis Citrix Workspace, ils doivent pouvoir partager des données (copier/coller) d'une application vers les autres applications au sein du groupe de sécurité. Le copier/coller s'effectue indépendamment des autres restrictions de sécurité déjà activées pour les applications.

Cependant, les utilisateurs finaux ne peuvent pas copier et coller le contenu de leurs applications locales sur leurs machines ou des applications non publiées vers ces applications désignées et inversement. La notification suivante apparaît lorsque le contenu est copié de l'application désignée vers une autre application :



> **Remarque**
>
> Vous pouvez copier et coller le contenu entre les applications d'un groupe de sécurité et d'autres applications locales sur les machines ou des applications Web non publiées en utilisant les options de **Paramètres avancés du presse-papiers**. Pour plus de détails, voir Activer les contrôles copier/coller pour les applications natives et les applications non publiées.

Activer l'accès au presse-papiers à un niveau granulaire

Vous pouvez activer l'accès au presse-papiers à un niveau granulaire dans les applications d'un groupe désigné. Vous pouvez le faire en créant des politiques d'accès pour les applications et en activant la restriction **Copier / Coller** selon vos besoins.

> **Remarque**
>
> Assurez-vous que la politique d'accès spécifique que vous avez créée pour l'accès au presse-papiers au niveau granulaire a une priorité plus élevée que la politique que vous avez créée pour les groupes de sécurité.

Exemple :

Considérez que vous avez créé un groupe de sécurité avec trois applications, à savoir Wikipédia, Pinterest et Dribble.

Maintenant, vous souhaitez restreindre le collage de contenu de Wikipédia ou de Dribble dans Pinterest. Pour ce faire, effectuez les opérations suivantes :

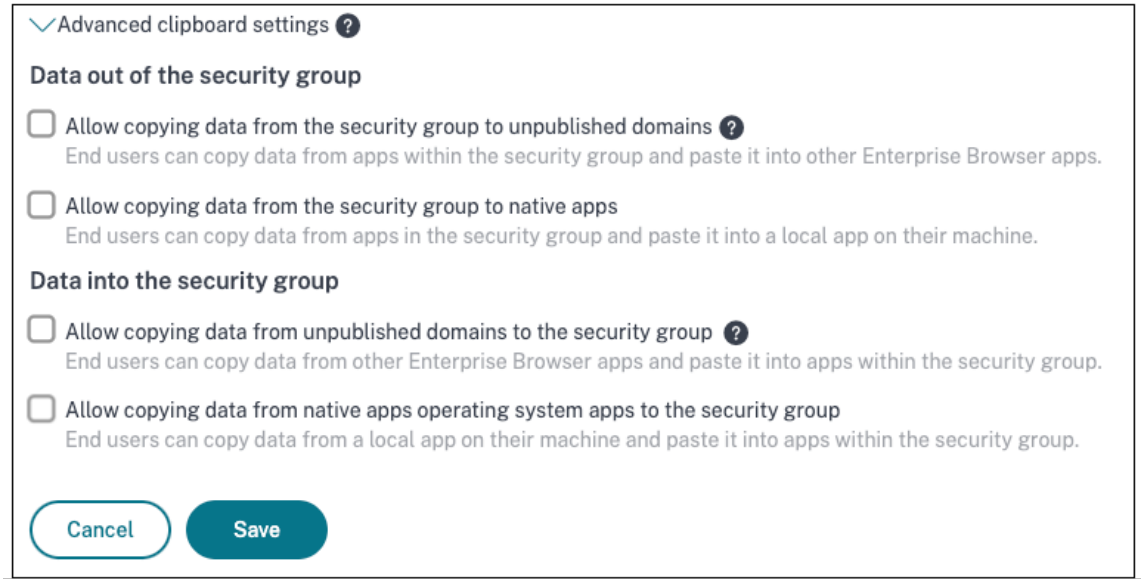
1. Créez ou modifiez une politique d'accès attribuée à l'application `Pinterest`. Pour plus de détails sur la création d'une politique d'accès, voir Créer des politiques d'accès.
2. Dans la page **Étape 3 : Action** , sélectionnez **Autoriser avec restrictions**.
3. Sélectionnez **Coller**.

Bien que Pinterest fasse partie d'un groupe de sécurité qui contient également Wikipédia et Dribble, les utilisateurs ne peuvent pas copier le contenu de Wikipédia ou de Dribble vers Pinterest en raison de la politique d'accès associée à Pinterest dans laquelle la restriction **Coller** est désactivée.

Activer les contrôles copier/coller pour les applications natives et les applications non publiées

Vous pouvez copier et coller le contenu entre les applications d'un groupe de sécurité et d'autres applications locales sur les machines ou des applications Web non publiées en utilisant les options de **Paramètres avancés du presse-papiers**

1. Créer un groupe de sécurité. Pour plus de détails, voir Créer des groupes de sécurité.
2. Développer **Paramètres avancés du presse-papiers**.



3. Sélectionnez l'une des options suivantes selon vos besoins :

   - **Autoriser la copie des données du groupe de sécurité vers des domaines non publiés** – Activer la copie des données des applications des groupes de sécurité vers les applications qui ne sont pas publiées dans Secure Private Access.
   - **Autoriser la copie des données du groupe de sécurité vers les applications natives** - Activer la copie des données des applications des groupes de sécurité vers les applications locales sur vos machines.
   - **Autoriser la copie des données des domaines non publiés vers le groupe de sécurité** –Activer la copie des données des applications non publiées via l'accès privé sécurisé aux applications des groupes de sécurité.
   - **Autoriser la copie des données des applications natives du système d'exploitation du groupe de sécurité** - Activer la copie des données des applications locales sur les machines vers les applications.

Problèmes connus

- La table de routage dans (**Paramètres > Domaine d'application**) conserve les domaines d'une application supprimée. Par conséquent, ces applications sont également considérées comme des applications publiées dans Secure Private Access. Si ces domaines sont accessibles directement depuis Citrix Enterprise Browser, le copier/coller est désactivé à partir de ces applications, quelles que soient les options que vous avez sélectionnées dans **Paramètres avancés du presse-papiers**.

  Par exemple, supposons le scénario suivant :

  - Vous avez supprimé une application nommée Jira2 (`https://test.citrite.net`) qui faisait partie d'un groupe de sécurité.
  - Vous avez activé l'option **Autoriser la copie des données du groupe de sécurité vers des domaines non publiés**.

  Dans ce scénario, si l'utilisateur tente de copier des données de cette application vers une autre application du même groupe de sécurité, le contrôle de collage est désactivé. Une notification à ce sujet est affichée à l'utilisateur.

- Pour une application SaaS, l'accès à l'application peut être refusé si l'application est configurée avec une politique d'accès avec l'action **Refuser l'accès.** Les utilisateurs finaux peuvent toujours accéder à l'application car le trafic de l'application n'est pas acheminé via Secure Private Access. De plus, si l'application fait partie du groupe de sécurité, les paramètres du groupe de sécurité ne sont pas respectés et vous ne pouvez donc pas copier/coller le contenu de l'application.

Outil de modélisation des politiques

October 21, 2024

Le fait d'avoir plusieurs applications et plusieurs politiques d'accès peut rendre difficile pour les administrateurs de comprendre le résultat exact de l'accès à l'application de l'utilisateur final, c'est-à-dire si l'utilisateur final est autorisé ou refusé à accéder à une application en fonction de toutes les configurations.

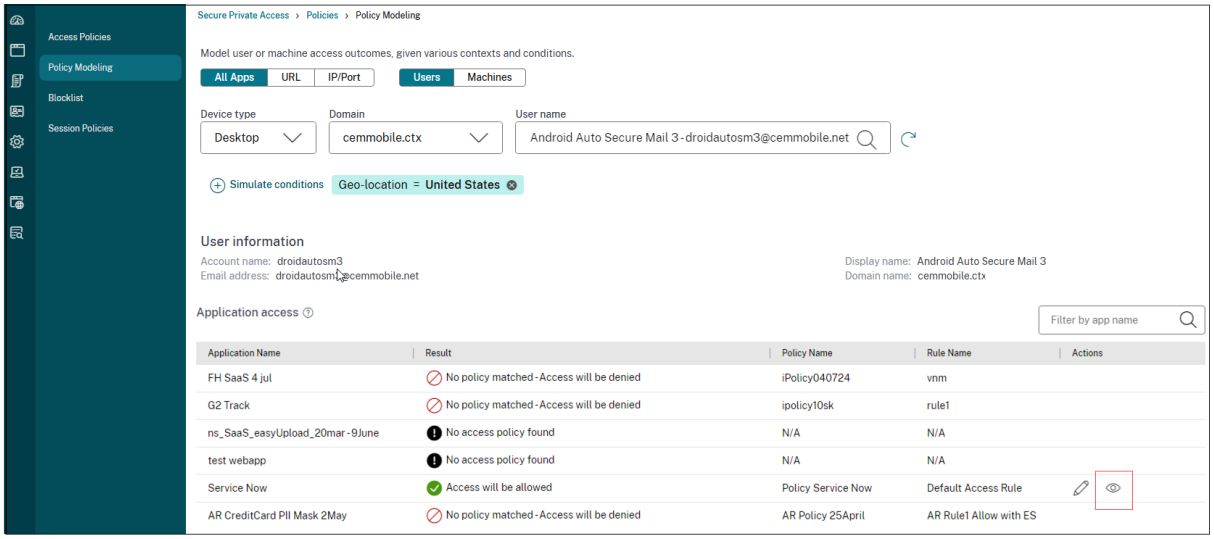
L'outil de modélisation des politiques (A**ccess Policies > Policy Modeling**) résout ce problème en donnant aux administrateurs une visibilité complète sur les résultats d'accès aux applications attendus (autorisés/autorisés avec restriction/refusés) en fonction de leurs configurations existantes. Les administrateurs peuvent vérifier les résultats d'accès de n'importe quel utilisateur en fonction des

conditions de l'utilisateur telles que le type d'appareil, la posture de l'appareil, la géolocalisation, l'emplacement du réseau, le score de risque de l'utilisateur et l'URL de l'espace de travail.

Pour analyser la configuration de la politique d'accès, procédez comme suit.

1. Dans la console Secure Private Access, cliquez sur **Stratégies d'accès** puis cliquez sur l'onglet **Modélisation des stratégies** .
2. Ajoutez les détails suivants :
    - **Type d'appareil**: Sélectionnez le type d'appareil de l'utilisateur final. (**Bureau** est sélectionné par défaut.)
    - **Domaine**: Sélectionnez le domaine associé à l'utilisateur.
    - **Utilisateur**: Sélectionnez le nom d'utilisateur pour lequel vous souhaitez analyser les applications et les politiques associées.
3. Vous pouvez également simuler un ensemble de conditions/contraintes sur l'utilisateur final et ses appareils. >**Remarque :** > >Ajoutez les conditions utilisateur exactes pour obtenir des résultats précis.
4. Cliquez sur **Simuler les conditions**.
5. Sélectionnez la condition (Posture de l'appareil, Géolocalisation, Emplacement du réseau, Score de risque utilisateur et URL de l'espace de travail), puis sélectionnez la valeur associée.
6. Cliquez sur le signe **+** pour ajouter d'autres conditions.
7. Cliquez sur **Appliquer**.

Les applications, les politiques associées et les règles pour l'utilisateur sélectionné sont affichées sous forme de tableau.



Configuration et gestion des applications

December 27, 2023

La mise à disposition d'applications à l'aide du service Citrix Secure Private Access vous fournit une solution simple, sécurisée, robuste et évolutive pour gérer les applications. Les applications livrées sur le cloud présentent les avantages suivants :

- Configuration simple : simplicité d'exploitation, de mise à jour et d'utilisation.
- Authentification unique —Ouverture de session sans tracas grâce à l'authentification unique.
- Modèle standard pour différentes applications SaaS —Configuration basée sur un modèle d'applications populaires. Ces modèles préremplissent une grande partie des informations nécessaires à la configuration des applications. Seules les informations spécifiques au client doivent toujours être fournies.

Prise en charge des applications Web d'entreprise

October 21, 2024

La diffusion d'applications Web à l'aide du service Secure Private Access permet de diffuser à distance des applications spécifiques à l'entreprise sous la forme d'un service Web. Les applications Web couramment utilisées incluent SharePoint, Confluence, OneBug, etc.

Les applications Web sont accessibles via Citrix Workspace à l'aide du service Secure Private Access. Le service Secure Private Access associé à Citrix Workspace offre une expérience utilisateur unifiée pour les applications Web configurées, les applications SaaS, les applications virtuelles configurées ou toute autre ressource d'espace de travail.

L'authentification unique et l'accès à distance aux applications Web sont disponibles dans le cadre des packages de services suivants :

- Norme d'accès privé sécurisé
- Secure Private Access Advanced

Configuration système requise

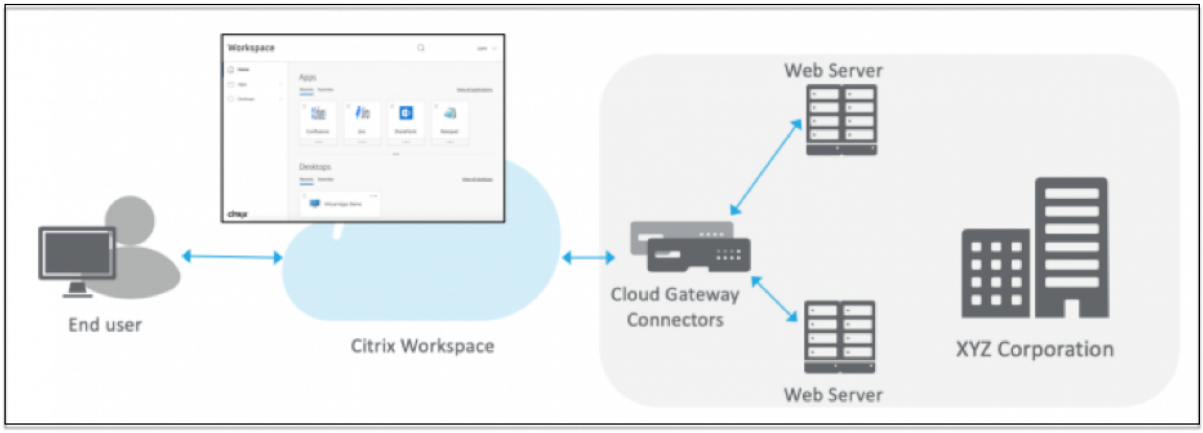
Connector Appliance - Utilisez le Connector Appliance avec le service Citrix Secure Private Access pour prendre en charge l'accès sans VPN aux applications Web d'entreprise dans le centre de données des clients. Pour plus de détails, voir Accès sécurisé à l'espace de travail avec Connector Appliance.

Fonctionnement

Le service Citrix Secure Private Access se connecte en toute sécurité au centre de données local à l'aide du connecteur, qui est déployé sur site. Ce connecteur agit comme un pont entre les applications Web d'entreprise déployées sur site et le service Citrix Secure Private Access. Ces connecteurs peuvent être déployés dans une paire HA et ne nécessitent qu'une connexion sortante.

Une connexion TLS entre le Connector Appliance et le service Citrix Secure Private Access dans le cloud sécurise les applications locales qui sont énumérées dans le service cloud. Les applications Web sont accessibles et diffusées via Workspace à l'aide d'une connexion sans VPN.

La figure suivante illustre l'accès aux applications Web à l'aide de Citrix Workspace.



Configurer une application Web

La configuration d'une application Web implique les étapes de haut niveau suivantes.

1. Configurer les détails de l'application
2. Définir la méthode de connexion préférée
3. Définir le routage des applications

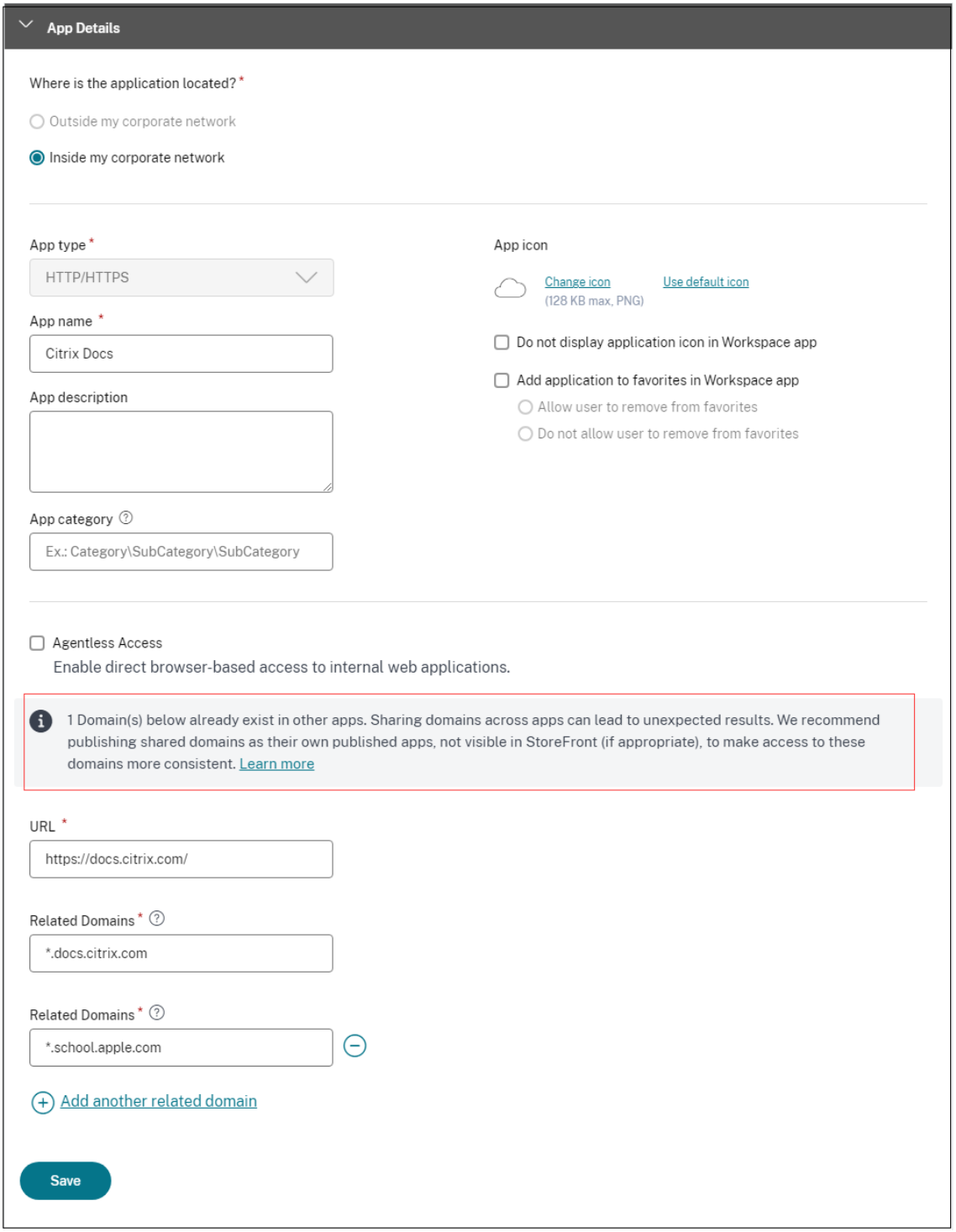
Configurer les détails de l'application

1. Sur la mosaïque **Accès privé sécurisé** , cliquez sur **Gérer.**
2. Sur la page d'accueil de Secure Private Access, cliquez sur **Continuer** puis cliquez sur **Ajouter une application.**

> **Remarque**
>
> Le bouton **Continuer** apparaît uniquement la première fois que vous utilisez l'assistant. Dans les utilisations suivantes, vous pouvez accéder directement à la page **Applications** puis cliquer

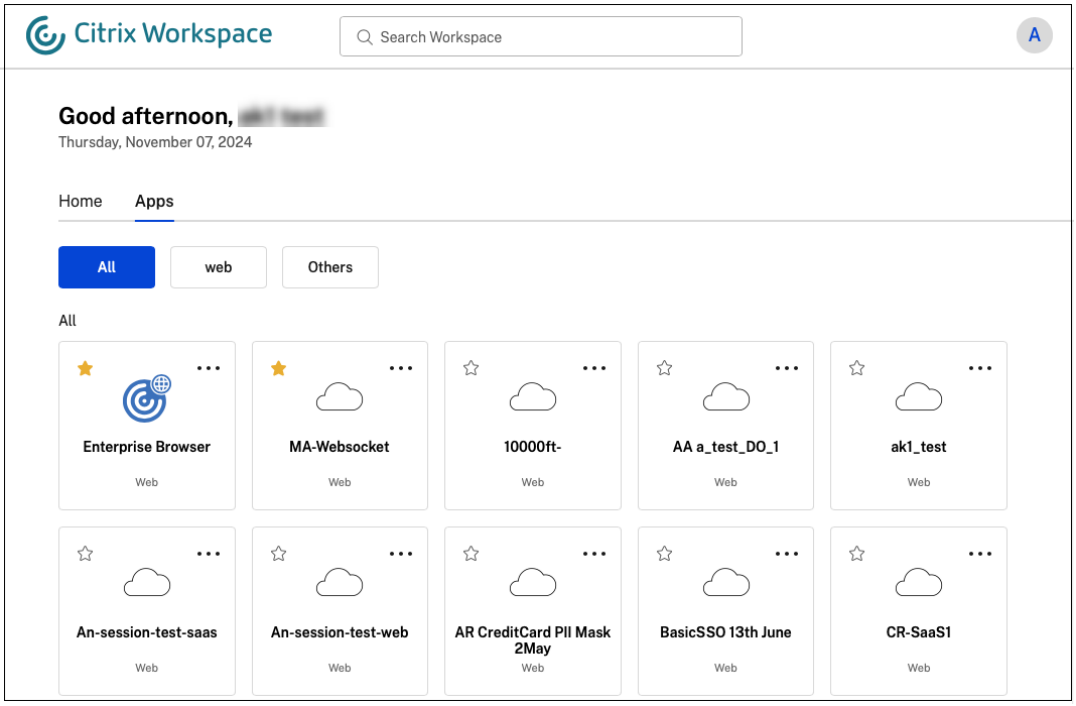
> sur **Ajouter une application.**

1. Sélectionnez l'application que vous souhaitez ajouter et cliquez sur **Ignorer.**
2. Dans **Où se trouve l'emplacement de l'application ?**, sélectionnez l'emplacement.
3. Saisissez les détails suivants dans la section **Détails de l'application** et cliquez sur **Suivant.**



- **Type d'application** –Sélectionnez le type d'application. Vous pouvez sélectionner parmi les applications **HTTP/HTTPS** ou **UDP/TCP** .
- **Nom de l'application** –Nom de l'application.
- **Description de l'application** - Une brève description de l'application. Cette description que vous saisissez ici est affichée à vos utilisateurs dans l'espace de travail.
- **Catégorie d'application** - Ajoutez la catégorie et le nom de la sous-catégorie (le cas échéant) sous lesquels l'application que vous publiez doit apparaître dans l'interface utilisateur de Citrix Workspace. Vous pouvez ajouter une nouvelle catégorie pour chaque application ou utiliser des catégories existantes à partir de l'interface utilisateur de Citrix Workspace. Une fois que vous avez spécifié une catégorie pour une application Web ou SaaS, l'application s'affiche dans l'interface utilisateur de l'espace de travail sous la catégorie spécifique.
  - Les catégories/sous-catégories sont configurables par l'administrateur et les administrateurs peuvent ajouter une nouvelle catégorie pour chaque application.
  - Le champ **Catégorie d'application** s'applique aux applications HTTP/HTTPS et est masqué pour les applications TCP/UDP.
  - Les noms des catégories/sous-catégories doivent être séparés par une barre oblique inverse. Par exemple, **Affaires et productivité\Ingénierie**. De plus, ce champ est sensible à la casse. Les administrateurs doivent s'assurer qu'ils définissent la bonne catégorie. S'il existe une incompatibilité entre le nom dans l'interface utilisateur de Citrix Workspace et le nom de catégorie saisi dans le champ **Catégorie d'application** , la catégorie est répertoriée comme une nouvelle catégorie.

    Par exemple, si vous saisissez incorrectement la catégorie **Entreprise et productivité** comme **Entreprise et productivité** dans le champ **Catégorie d'application** , une nouvelle catégorie nommée **Entreprise et productivité** est répertoriée dans l'interface utilisateur de Citrix Workspace en plus de la catégorie **Entreprise et productivité** .



- **Icône de l'application** –Cliquez sur **Modifier l'icône** pour modifier l'icône de l'application. La taille du fichier d'icône doit être de 128x128 pixels. Si vous ne modifiez pas l'icône, l'icône par défaut s'affiche.

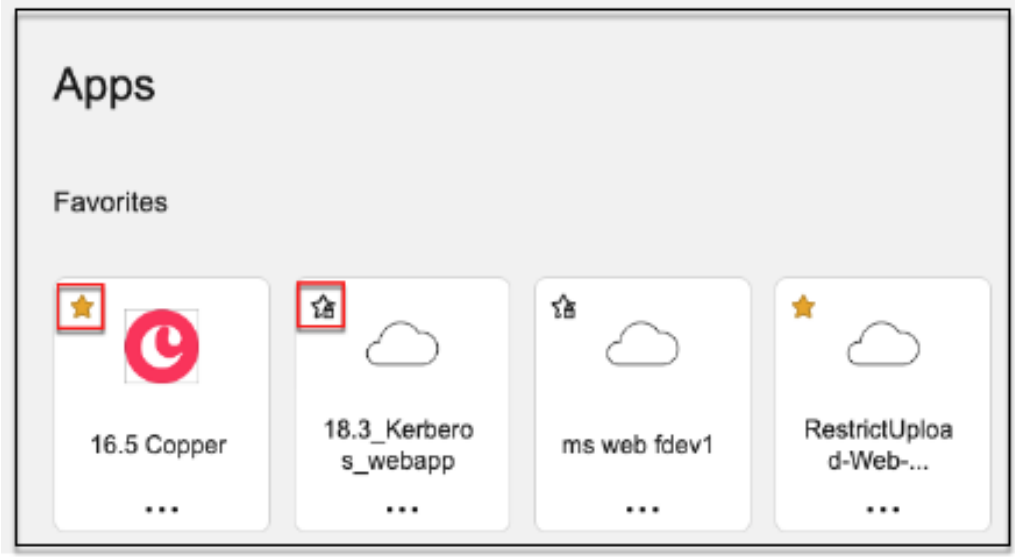
```
If you do not want to display the app icon, select **Do not display application icon to users.**
```

- Sélectionnez **Accès direct** pour permettre aux utilisateurs d'accéder à l'application directement depuis un navigateur client. Pour plus de détails, voir Accès direct aux applications Web d'entreprise.

- **URL** –URL avec votre identifiant client. L'URL doit contenir votre identifiant client (identifiant client Citrix Cloud). Pour obtenir votre identifiant client, consultez S'inscrire à Citrix Cloud. En cas d'échec de SSO ou si vous ne souhaitez pas utiliser SSO, l'utilisateur est redirigé vers cette URL.

```
**Customer domain name** and **Customer domain ID** - Customer domain name and ID are used to create the app URL and other subsequent URLs in the SAML SSO page.

For example, if you're adding a Salesforce app, your domain name is `salesforceformyorg` and ID is 123754, then the app URL is `https://salesforceformyorg.my.salesforce.com/?so=123754.`

Customer domain name and Customer ID fields are specific to certain apps.
```


- **Domaines associés** –Le domaine associé est automatiquement renseigné en fonction de l'URL que vous avez fournie. Le domaine associé aide le service à identifier l'URL dans le cadre de l'application et à acheminer le trafic en conséquence. Vous pouvez ajouter plusieurs domaines associés.
- Cliquez sur **Ajouter automatiquement l'application aux favoris** pour ajouter cette application en tant qu'application favorite dans l'application Citrix Workspace.
  - Cliquez sur **Autoriser l'utilisateur à supprimer des favoris** pour permettre aux abonnés de l'application de supprimer l'application de la liste des applications favorites dans l'application Citrix Workspace. Lorsque vous sélectionnez cette option, une icône en forme d'étoile jaune apparaît dans le coin supérieur gauche de l'application dans l'application Citrix Workspace.
  - Cliquez sur **Ne pas autoriser l'utilisateur à supprimer des favoris** pour empêcher les abonnés de supprimer l'application de la liste des applications favorites dans l'application Citrix Workspace. Lorsque vous sélectionnez cette option, une icône en forme d'étoile avec un cadenas apparaît dans le coin supérieur gauche de l'application dans l'application Citrix Workspace.



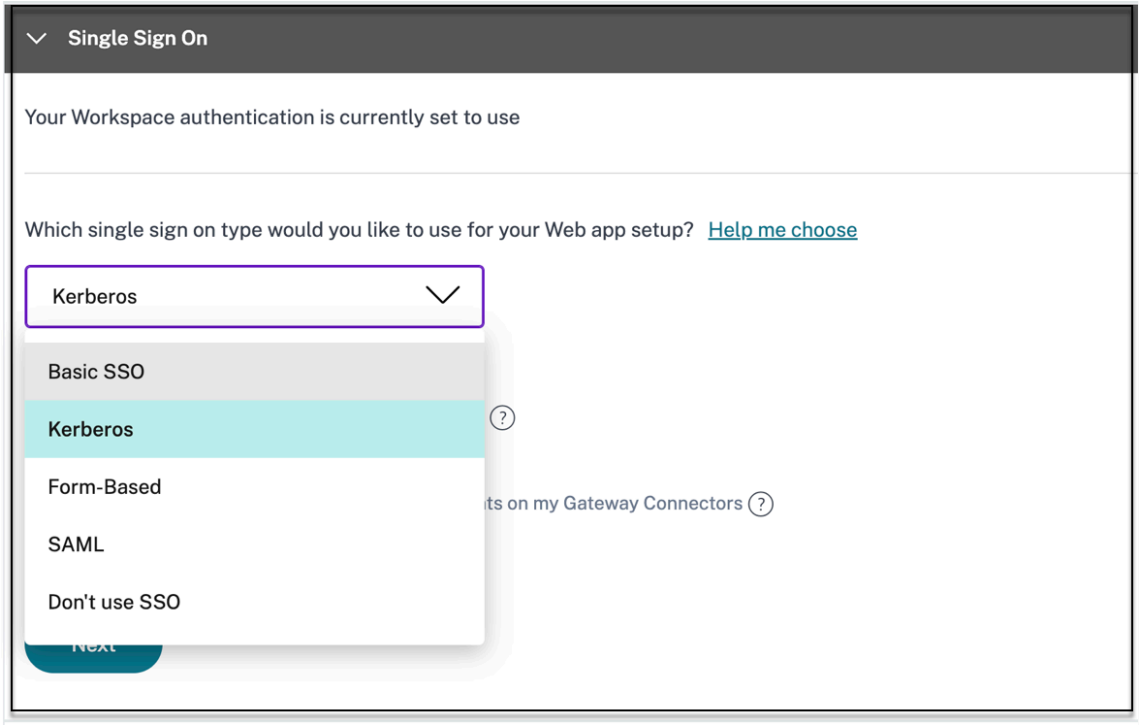
Si vous supprimez les applications marquées comme favorites de la console du service Secure Private Access, ces applications doivent être supprimées manuellement de la liste des favoris dans Citrix Workspace. Les applications ne sont pas automatiquement supprimées de l'application Workspace si elles sont supprimées de la console du service Secure Private Access.

4. Cliquez sur **Suivant.**

> **Important :**
>
> - Pour permettre un accès basé sur la confiance zéro aux applications, l'accès aux applications se voit refuser par défaut. L'accès aux applications est activé uniquement si une politique d'accès est associée à l'application. Pour plus de détails, voir Accès refusé aux applications, par défaut.
> - Si plusieurs applications sont configurées avec le même nom de domaine complet ou une variante du nom de domaine complet générique, cela peut entraîner une configuration conflictuelle. Pour plus de détails, voir Configuration conflictuelle pouvant entraîner des problèmes d'accès aux applications.

Définir la méthode de connexion préférée

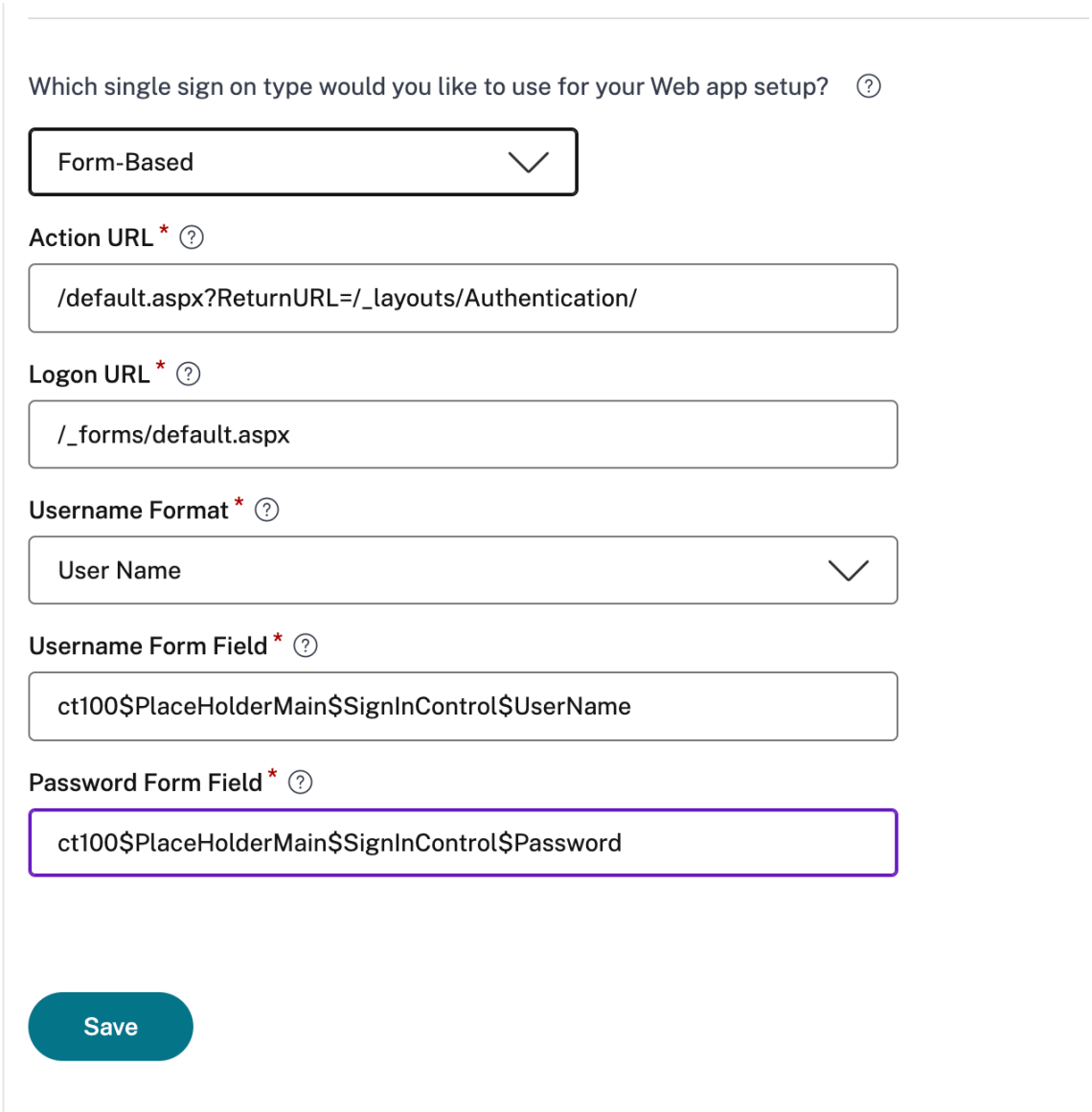
1. Dans la section **Authentification unique** , sélectionnez le type d'authentification unique que vous préférez utiliser pour votre application et cliquez sur **Enregistrer.** Les types d'authentification unique suivants sont disponibles.



   - **Basic** –Si votre serveur back-end vous présente un défi basic-401, choisissez **Basic SSO**. Vous n'avez pas besoin de fournir de détails de configuration pour le type SSO **Basic** .
   - **Kerberos** –Si votre serveur back-end vous présente le défi negotiation-401, choisissez **Kerberos**. Vous n'avez pas besoin de fournir de détails de configuration pour le type SSO **Kerberos** .

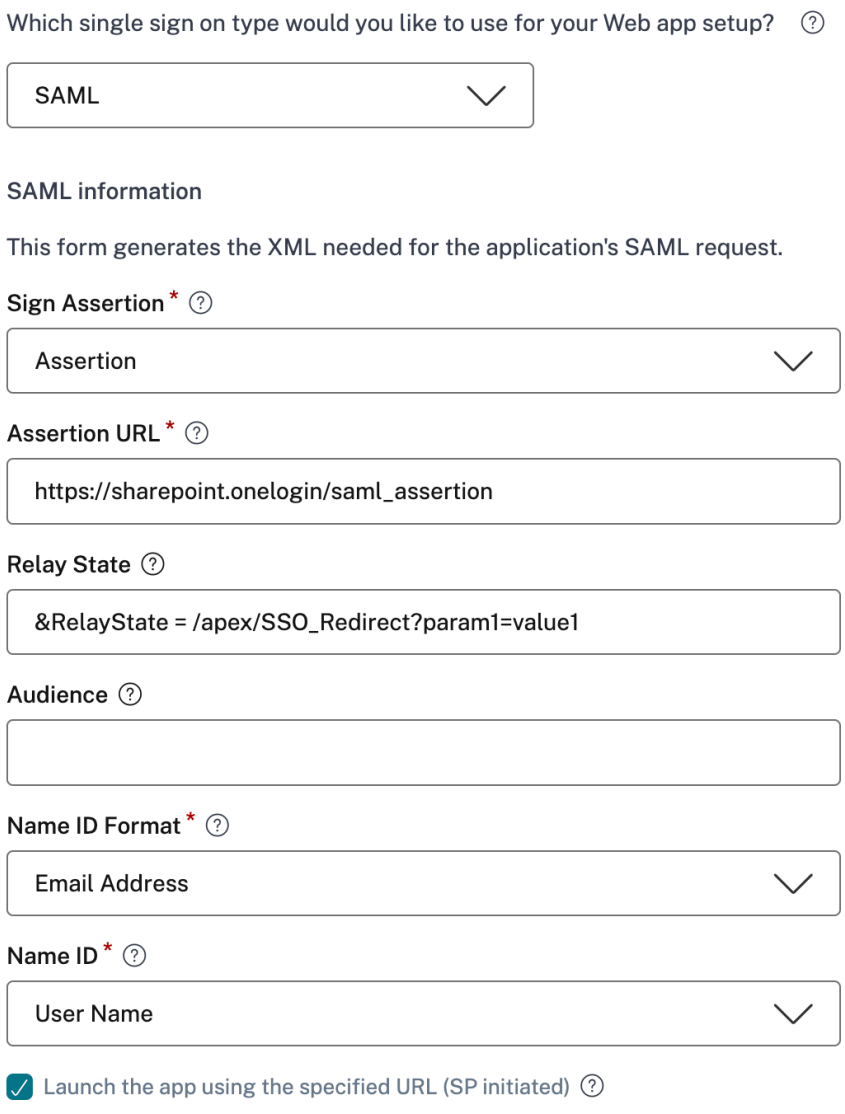
- **Basé sur un formulaire** –Si votre serveur back-end vous présente un formulaire HTML pour l'authentification, choisissez **Basé sur un formulaire**. Saisissez les détails de configuration pour le type SSO **basé sur un formulaire** .
- **SAML** - Choisissez **SAML** pour l'authentification unique basée sur SAML dans les applications Web. Saisissez les détails de configuration pour le type SSO **SAML** .
- **Ne pas utiliser SSO** –Utilisez l'option **Ne pas utiliser SSO** lorsque vous n'avez pas besoin d'authentifier un utilisateur sur le serveur principal. Lorsque l'option **Ne pas utiliser SSO** est sélectionnée, l'utilisateur est redirigé vers l'URL configurée dans la section **Détails de l'application** .

Détails basés sur le formulaire : saisissez les détails de configuration basés sur le formulaire suivants dans la section Authentification unique et cliquez sur Enregistrer.



- **URL d'action** - Tapez l'URL à laquelle le formulaire complété est soumis.
- **URL du formulaire de connexion** –Tapez l'URL sur laquelle le formulaire de connexion est présenté.
- **Format du nom d'utilisateur** - Sélectionnez un format pour le nom d'utilisateur.
- **Champ de formulaire de nom d'utilisateur** –Saisissez un attribut de nom d'utilisateur.
- **Champ de formulaire de mot de passe** –Saisissez un attribut de mot de passe.

SAML : saisissez les informations suivantes dans la section Se connecter et cliquez sur Enregistrer.



- **Assertion de signature** - La signature de l'assertion ou de la réponse garantit l'intégrité du message lorsque la réponse ou l'assertion est remise à la partie de confiance (SP). Vous pouvez sélectionner **Assertion, Réponse, Les deux,** ou **Aucun**.

- **URL d'assertion** –L'URL d'assertion est fournie par le fournisseur de l'application. L'assertion SAML est envoyée à cette URL.
- **État du relais** –Le paramètre État du relais est utilisé pour identifier la ressource spécifique à laquelle les utilisateurs accèdent après s'être connectés et dirigés vers le serveur de fédération de la partie de confiance. Relay State génère une URL unique pour les utilisateurs. Les utilisateurs peuvent cliquer sur cette URL pour se connecter à l'application cible.
- **Audience** –L'audience est fournie par le fournisseur de l'application. Cette valeur confirme que l'assertion SAML est générée pour l'application correcte.
- **Format d'identifiant de nom** –Sélectionnez le format d'identifiant de nom pris en charge.
- **ID de nom** –Sélectionnez l'ID de nom pris en charge.

2. Dans **Attributs avancés (facultatif)** ajoutez des informations supplémentaires sur l'utilisateur qui sont envoyées à l'application pour les décisions de contrôle d'accès.
3. Téléchargez le fichier de métadonnées en cliquant sur le lien sous **Métadonnées SAML.** Utilisez le fichier de métadonnées téléchargé pour configurer SSO sur le serveur d'applications SaaS.

> **Remarque**
>
> - Vous pouvez copier l'URL de connexion SSO sous **URL de connexion** et utiliser cette URL lors de la configuration de SSO sur le serveur d'applications SaaS.
> - Vous pouvez également télécharger le certificat à partir de la liste **Certificat** et utiliser le certificat lors de la configuration de SSO sur le serveur d'applications SaaS.

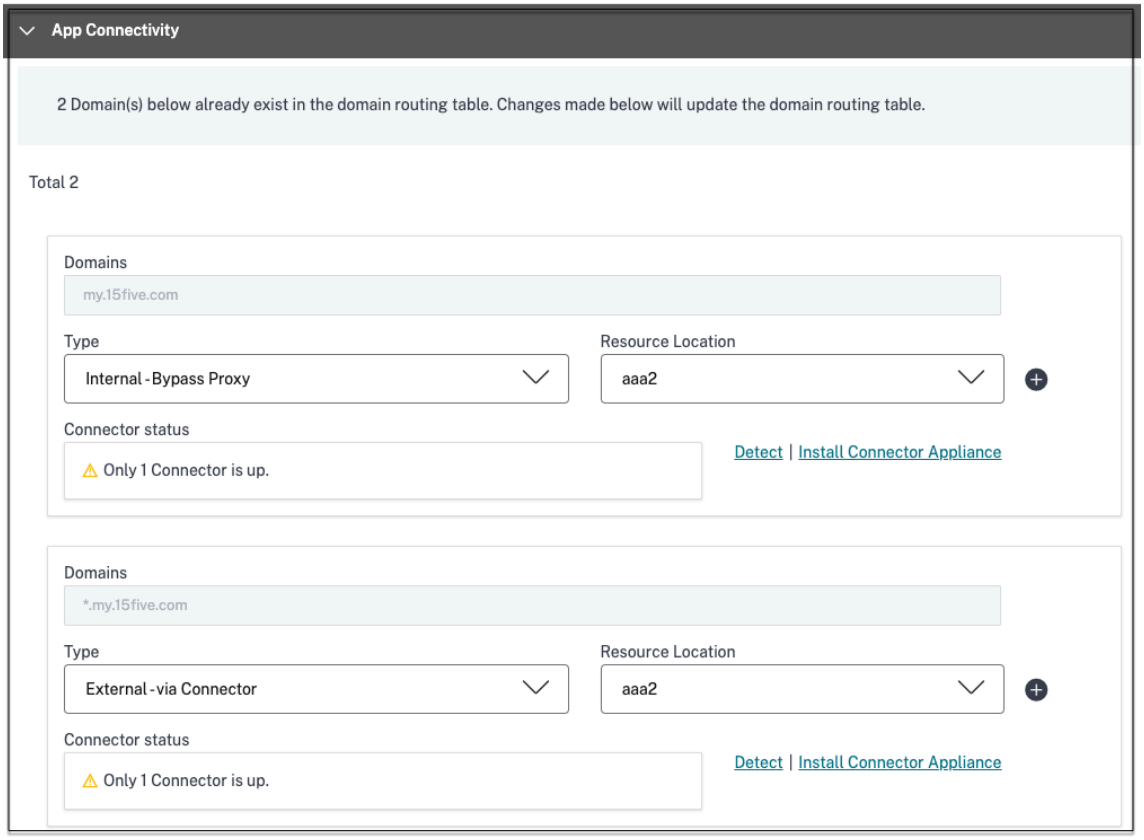
1. Cliquez sur **Suivant.**

Définir le routage des applications

1. Dans la section **App Connectivity** , vous définissez le routage pour les domaines associés des applications, si les domaines doivent être routés en externe ou en interne via Citrix Connector Appliance.

   - **Interne –contourner le proxy** - Le trafic du domaine est acheminé via Citrix Cloud Connector, en contournant le proxy Web du client configuré sur l'appliance Connector.
   - **Interne via le connecteur** - Les applications peuvent être externes mais le trafic doit circuler via l'appliance Connector vers le réseau extérieur.
   - **Externe** –Le trafic circule directement vers Internet.

   Pour plus de détails, consultez Tables de routage pour résoudre les conflits si les domaines associés dans les applications SaaS et Web sont les mêmes.

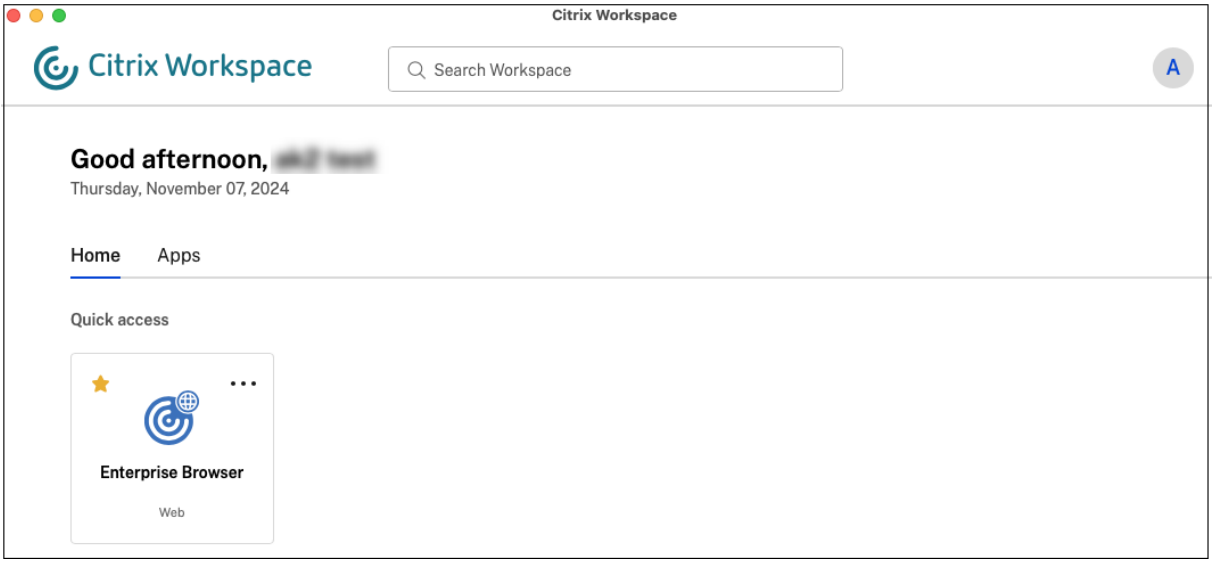


2. Cliquez sur **Terminer.**

   Après avoir cliqué sur **Terminer**, l'application est ajoutée à la page Applications. Vous pouvez modifier ou supprimer une application depuis la page Applications après avoir configuré l'application. Pour ce faire, cliquez sur le bouton points de suspension d'une application et sélectionnez les actions en conséquence.

   - **Modifier l'application**
   - **Supprimer**

Lorsque vous publiez une application Web ou SaaS à partir du service Secure Private Access et si cette application n'est pas masquée, l'application Citrix Enterprise Browser s'affiche automatiquement dans l'interface utilisateur de Citrix Workspace. De plus, le navigateur Citrix Enterprise est également ajouté comme application favorite, par défaut. Les utilisateurs finaux peuvent lancer le navigateur de l'espace de travail sans URL et accéder aux sites Web internes à l'aide des navigateurs de l'espace de travail.



Important :

- Pour accorder l'accès aux applications aux utilisateurs, les administrateurs doivent créer des politiques d'accès. Dans les politiques d'accès, les administrateurs ajoutent des abonnés aux applications et configurent les contrôles de sécurité. Pour plus de détails, voir Créer des politiques d'accès.

Accès direct aux applications Web d'entreprise

October 21, 2024

Les applications Web d'entreprise telles que SharePoint, JIRA, Confluence et autres, hébergées par le client sur site ou sur des clouds publics, sont désormais accessibles directement depuis un navigateur client. Les utilisateurs finaux n'ont plus besoin d'initier l'accès à leurs applications Web d'entreprise à partir de l'expérience Citrix Workspace. Cette fonctionnalité permet également aux utilisateurs finaux d'accéder aux applications Web en cliquant sur des liens depuis leurs e-mails, leurs outils de collaboration ou les signets de leur navigateur. Fournit ainsi une véritable solution à empreinte zéro aux clients.

Fonctionnement

- Ajoutez un nouvel enregistrement DNS ou modifiez un enregistrement DNS existant pour les applications Web d'entreprise configurées.

- L'administrateur informatique ajouterait un nouvel enregistrement DNS public ou modifierait un enregistrement DNS public existant pour le nom de domaine complet de l'application Web d'entreprise configuré afin de rediriger l'utilisateur vers le service Citrix Secure Private Access.
- Lorsque l'utilisateur final initie l'accès à l'application Web d'entreprise configurée, le trafic de l'application est dirigé vers le service Citrix Secure Private Access, qui proxy l'accès à l'application.
- Une fois la demande arrivée sur le service Citrix Secure Private Access, il vérifie l'authentification de l'utilisateur et l'autorisation de l'application, y compris les vérifications des stratégies d'accès contextuelles.
- Une fois la validation réussie, le service Citrix Secure Private Access communique avec les appareils Citrix Cloud Connector, déployés dans l'environnement du client (sur site ou dans le cloud) pour permettre l'accès à l'application Web d'entreprise configurée.

Configurer Citrix Secure Private Access pour un accès direct aux applications Web d'entreprise

Prérequis

Avant de commencer, vous avez besoin des éléments suivants pour configurer l'application.

- Nom de domaine complet de l'application
- Certificat SSL –Certificat public pour l'application à configurer
- Emplacement des ressources –Installer les appareils Citrix Cloud Connector
- Accédez à l'enregistrement DNS public pour le mettre à jour avec le nom canonique (CNAME) fourni par Citrix lors de la configuration de l'application.

Procédure de configuration de l'accès direct aux applications Web d'entreprise :

> **Important :**
>
> Pour une configuration complète de bout en bout d'une application, consultez Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles.

1. Sur la page d'accueil de Secure Private Access, cliquez sur **Continuer.**

> **Remarque**
>
> Le bouton **Continuer** apparaît uniquement la première fois que vous utilisez l'assistant. Dans les utilisations suivantes, vous pouvez accéder directement à la page **Applications** puis cliquer sur **Ajouter une application**.

1. Configurer l'identité et l'authentification. Pour plus de détails, consultez Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles.

2. Procédez à l'ajout d'une application. Pour plus de détails, voir Ajouter et gérer des applications.
3. Sélectionnez l'application que vous souhaitez ajouter et cliquez sur **Ignorer.**
4. Dans **Où se trouve l'emplacement de l'application ?**, sélectionnez l'emplacement.
5. Saisissez les détails suivants dans la section **Détails de l'application** et cliquez sur **Suivant**.

   - **Type d'application** –Sélectionnez le type d'application (HTTP ou HTTPS).
   - **Nom de l'application** –Nom de l'application.
   - **Description de l'application** - Une brève description de l'application. Cette description que vous saisissez ici est affichée à vos utilisateurs dans l'espace de travail.
   - **Icône de l'application** –Cliquez sur **Modifier l'icône** pour modifier l'icône de l'application. La taille du fichier d'icône doit être de 128x128 pixels. Si vous ne modifiez pas l'icône, l'icône par défaut s'affiche.

     Si vous ne souhaitez pas afficher l'icône de l'application, sélectionnez **Ne pas afficher l'icône de l'application aux utilisateurs**.

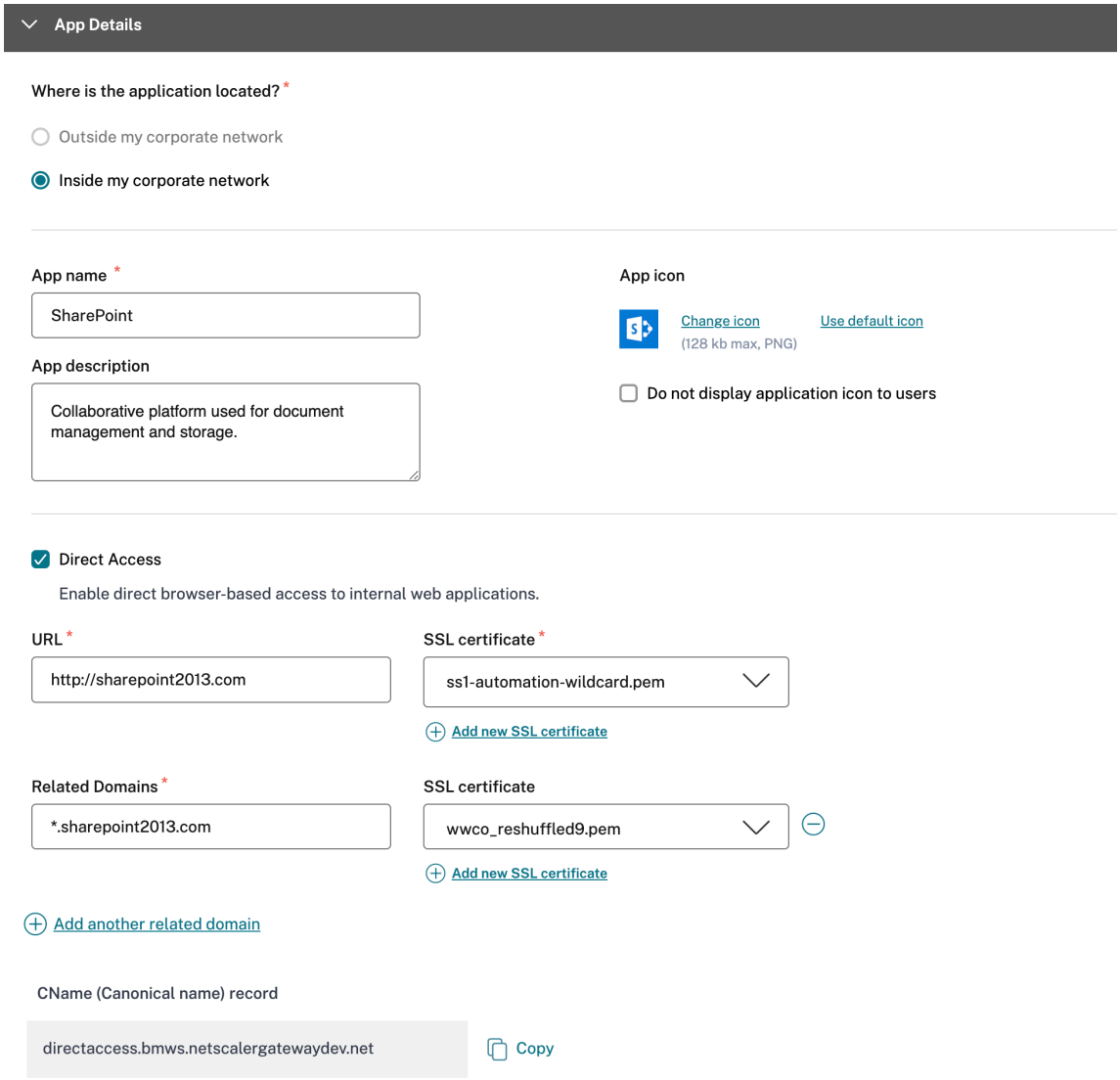
6. Sélectionnez **Accès direct** pour permettre aux utilisateurs d'accéder à l'application directement depuis un navigateur client. Entrez les détails suivants.

   - **URL** –URL de l'application back-end. L'URL doit être au format HTTPS et une entrée DNS correspondante doit être ajoutée par l'administrateur.
   - **Certificat SSL** –Sélectionnez un certificat SSL existant dans le menu déroulant ou ajoutez un nouveau certificat SSL en cliquant sur **Ajouter un nouveau certificat SSL**.

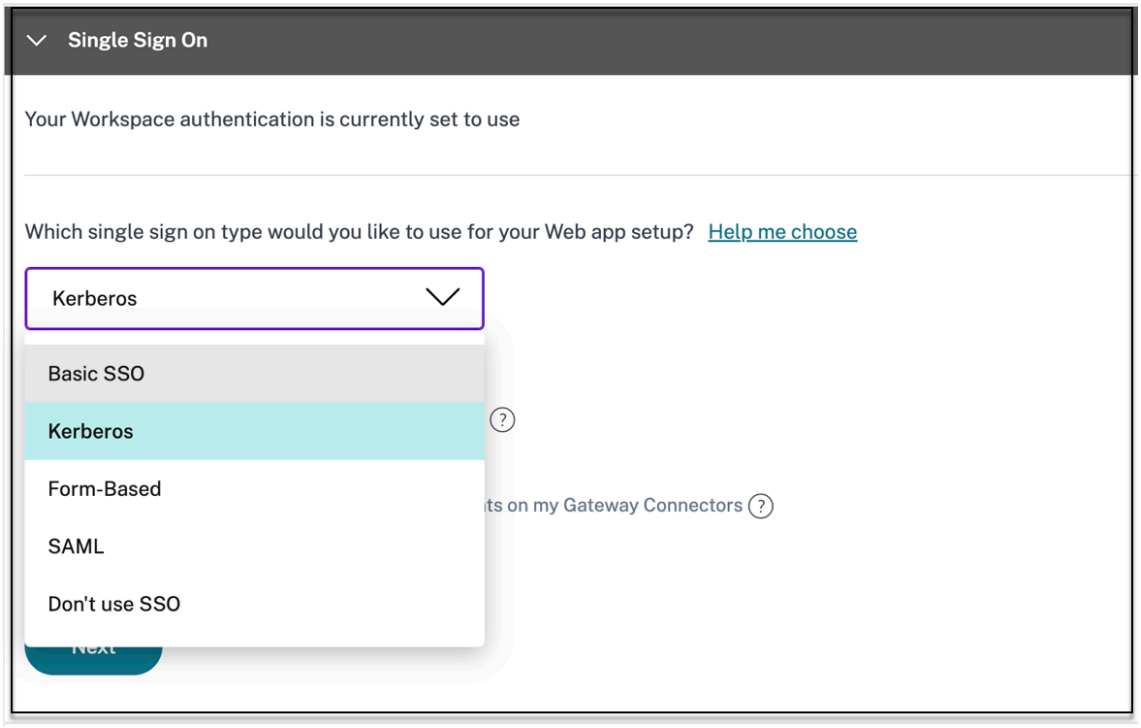
     Points à noter :

     - Seul un certificat d'autorité de certification public ou approuvé est pris en charge. Les certificats auto-signés ne sont pas pris en charge.
     - Une chaîne complète de certificats doit être téléchargée.

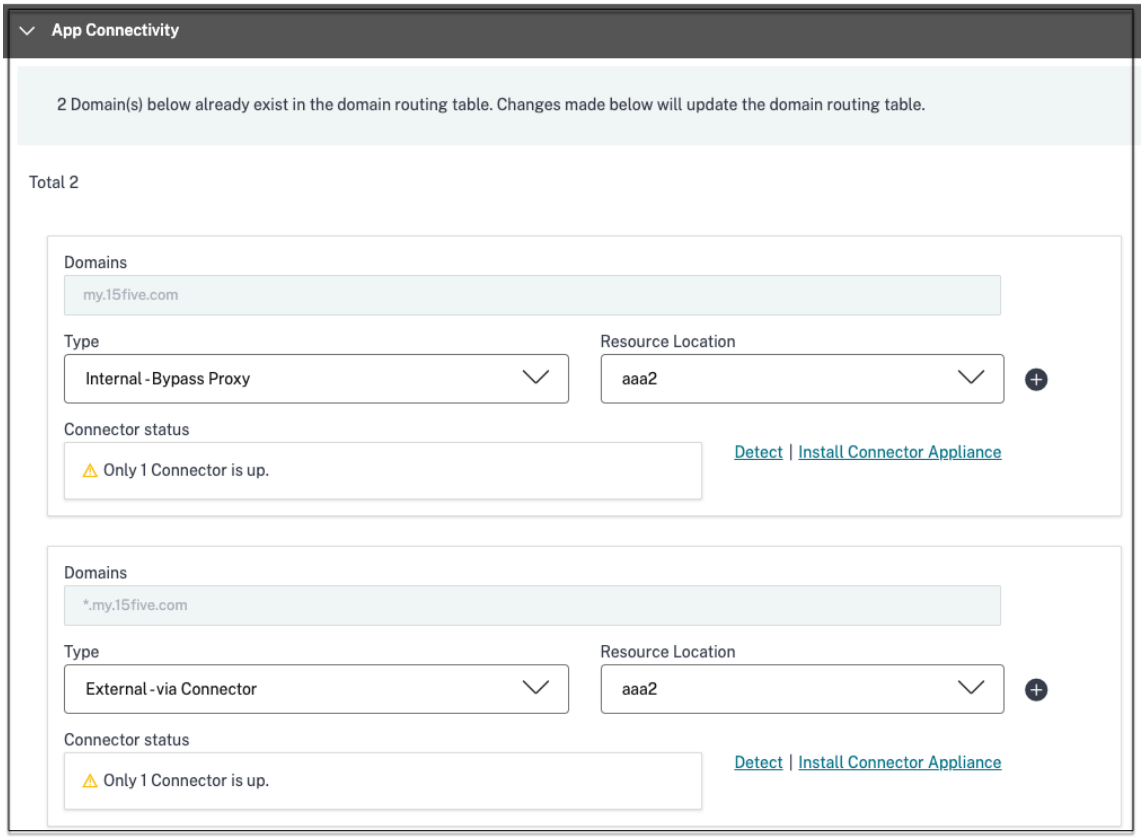
   - **Domaines associés** –Le domaine associé est automatiquement renseigné en fonction de l'URL que vous avez fournie. Le domaine associé aide le service à identifier l'URL dans le cadre de l'application et à acheminer le trafic en conséquence. Vous pouvez ajouter plusieurs domaines associés. Vous pouvez lier un certificat SSL à chaque domaine associé, ceci est facultatif.
   - **Enregistrement CName** –Généré automatiquement par Secure Private Access. Il s'agit de la valeur qui doit être saisie dans le DNS pour permettre l'accès direct à l'application.



7. Cliquez sur **Suivant.**
8. Dans la section **Authentification unique** , sélectionnez votre type d'authentification unique préféré à utiliser pour votre application et cliquez sur**Suivant**.



9. Dans la section **Connectivité des applications** , vous pouvez soit sélectionner un emplacement de ressource existant, soit en créer un et déployer une nouvelle appliance de connecteur. Pour choisir un emplacement de ressource existant, cliquez sur l'un des emplacements de ressource dans la liste des emplacements de ressource, par exemple Mon emplacement de ressource, puis cliquez sur**Suivant**. Pour plus de détails, consultez Tables de routage pour résoudre les conflits si les domaines associés dans les applications SaaS et Web sont les mêmes.



10. Cliquez sur **Terminer**. L'application est ajoutée à la page Applications. Vous pouvez modifier ou supprimer une application depuis la page Applications après l'avoir configurée. Pour ce faire, cliquez sur le bouton points de suspension d'une application et sélectionnez les actions en conséquence.

    - **Modifier l'application**
    - **Supprimer**

> **Important :**
>
> - Pour permettre un accès basé sur la confiance zéro aux applications, l'accès aux applications se voit refuser par défaut. L'accès aux applications est activé uniquement si une politique d'accès est associée à l'application. Pour plus de détails sur la création de politiques d'accès, voir Créer des politiques d'accès.
> - Si plusieurs applications sont configurées avec le même nom de domaine complet ou une variante du nom de domaine complet générique, cela peut entraîner une configuration conflictuelle. Pour éviter les configurations conflictuelles, consultez Bonnes pratiques pour les configurations d'applications Web et SaaS.

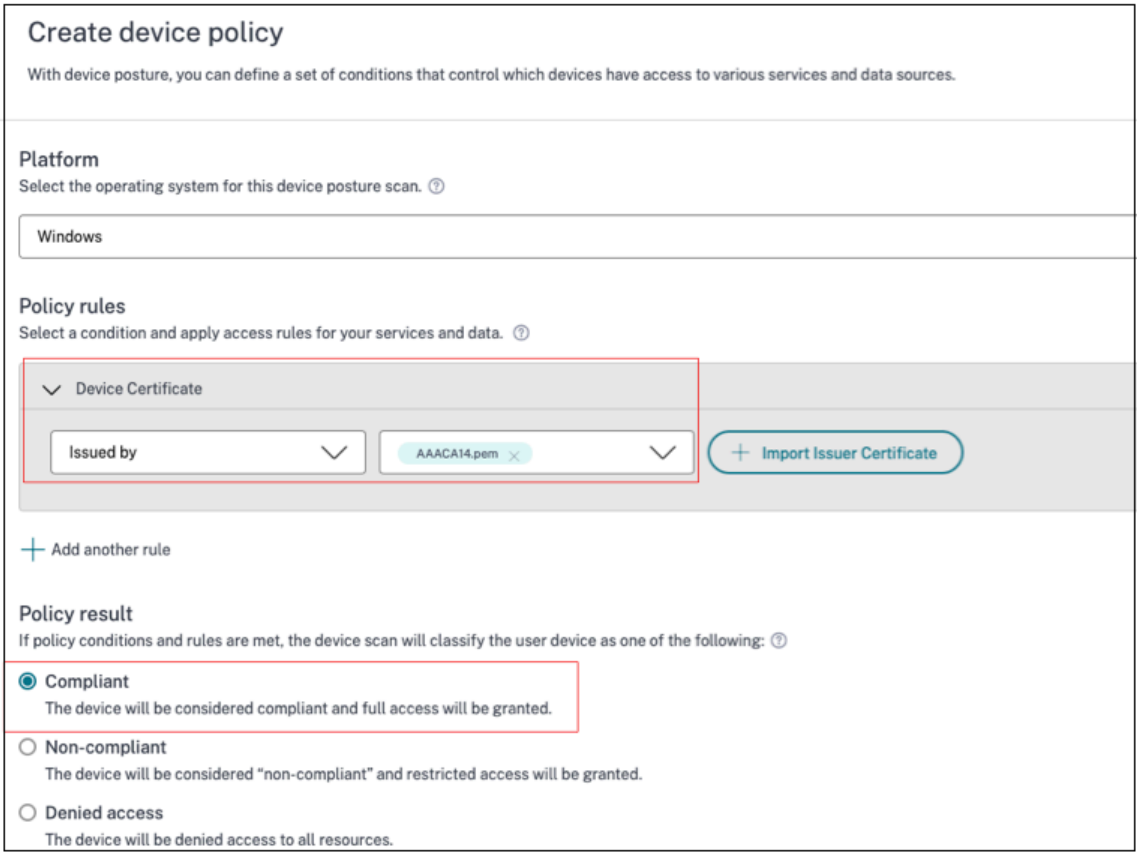
Service Device Posture avec applications à accès direct

Citrix Secure Private Access avec des applications d'accès direct, associé au service Device Posture, peut garantir que seuls les appareils conformes accèdent aux applications sensibles via un accès direct. Les administrateurs peuvent bloquer l'accès aux appareils non conformes ou non gérés en fonction des résultats de l'analyse du service Device Posture.

Étapes à suivre pour activer l'accès direct uniquement pour les appareils conformes

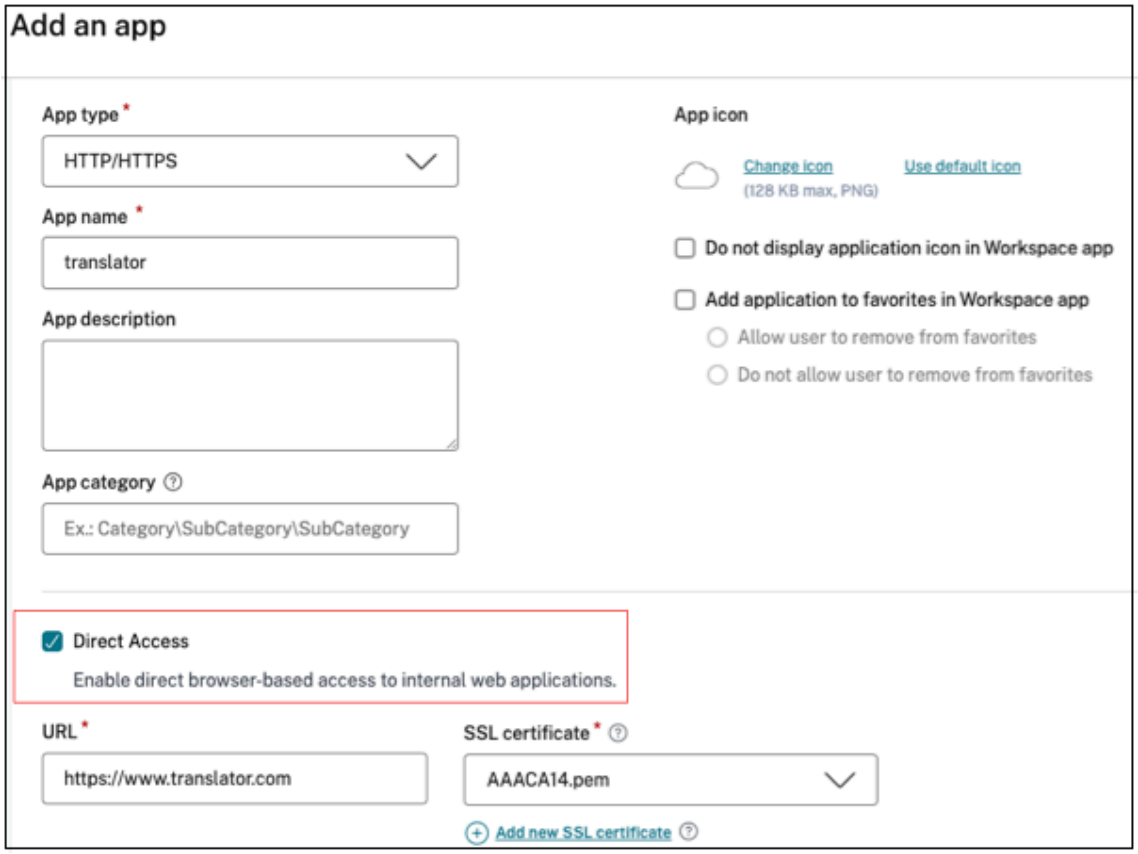
Pour activer l'accès direct uniquement aux appareils conformes, l'administrateur doit effectuer les étapes suivantes :

1. À partir de la console d'administration du service Device Posture, créez une stratégie de posture de l'appareil pour vérifier les conditions d'analyse de posture de l'appareil telles que le certificat de l'appareil, l'antivirus, le navigateur, puis sélectionnez **Conforme** comme action de résultat de stratégie. Pour plus de détails, voir Configurer la posture de l'appareil.



2. Depuis la console d'administration Secure Private Access, procédez comme suit :

    - Créez une application pour laquelle vous souhaitez activer l'accès direct. Pour plus de détails, voir Accès direct aux applications Web d'entreprise.



- Configurez l'accès privé sécurisé avec la posture de l'appareil. Dans **Portée de la règle**, sélectionnez **Vérification de la posture de l'appareil > Correspond à l'un des** et entrez la balise **Conforme**. Cette balise est envoyée depuis le service Device Posture.

> **Remarque**
>
> La balise doit être saisie exactement comme saisie précédemment, en utilisant des majuscules initiales (conforme). Dans le cas contraire, les politiques de posture de l'appareil ne fonctionnent pas comme prévu. Pour plus de détails, voir Configuration de Citrix Secure Private Access avec Device Posture.

```
1 ![Position de l'appareil pour un accès direct3](/en-us/citrix-secure-
    private-access/media/spa-direct-access-device-posture-3.png)
```

Une fois cette configuration effectuée, en fonction des résultats de l'analyse de posture de l'appareil, l'appareil est marqué comme conforme, non conforme ou la connexion est refusée et l'accès à l'application est activé en conséquence.

Exemple :

Considérez que vous avez créé une politique de posture de périphérique pour vérifier la présence d'un certificat de périphérique sur un périphérique de terminaison et déterminer son état de connexion.

Une fois les stratégies de posture de l'appareil définies et la posture de l'appareil activée, les actions suivantes se produisent lorsqu'un utilisateur final se connecte à Citrix Workspace.

1. L'analyse de posture de l'appareil vérifie la présence d'un certificat d'appareil sur le périphérique terminal.
    - Si le certificat de l'appareil est présent sur l'appareil, l'appareil est étiqueté comme **conforme**.
    - Si le certificat de l'appareil n'est pas présent sur l'appareil, l'appareil est marqué comme **non conforme**.
2. Ces informations sont ensuite transmises au service Citrix Secure Private Access sous forme de balises.
3. La politique d'accès est évaluée en fonction de la classification de l'appareil.
    - Si l'appareil est conforme, l'accès direct aux applications est autorisé.
    - Si l'appareil n'est pas conforme, l'accès direct est désactivé pour les applications.

Expérience de l'utilisateur final

L'expérience de l'utilisateur final est basée sur la classification de l'appareil comme conforme ou non conforme.

- **Appareil conforme :**

  L'utilisateur peut lancer l'application d'accès direct depuis Citrix Workspace ou depuis le navigateur à l'aide de l'URL de l'application.

- **Appareil non conforme :**
    - L'application n'est pas répertoriée dans Citrix Workspace.
    - L'utilisateur ne peut pas lancer l'application depuis le navigateur en utilisant l'URL de l'application.
    - Une page d'accès bloqué est affichée à l'utilisateur.

Prise en charge des applications SaaS (Software as a Service)

October 21, 2024

Le logiciel en tant que service (SaaS) est un modèle de distribution de logiciels permettant de fournir des logiciels à distance sous forme de service Web. Les applications SaaS couramment utilisées incluent Salesforce, Workday, Concur, GoToMeeting, etc.

Les applications SaaS sont accessibles via Citrix Workspace à l'aide du service Secure Private Access. Le service Secure Private Access associé à Citrix Workspace offre une expérience utilisateur unifiée pour les applications SaaS configurées, les applications virtuelles configurées ou toute autre ressource d'espace de travail.

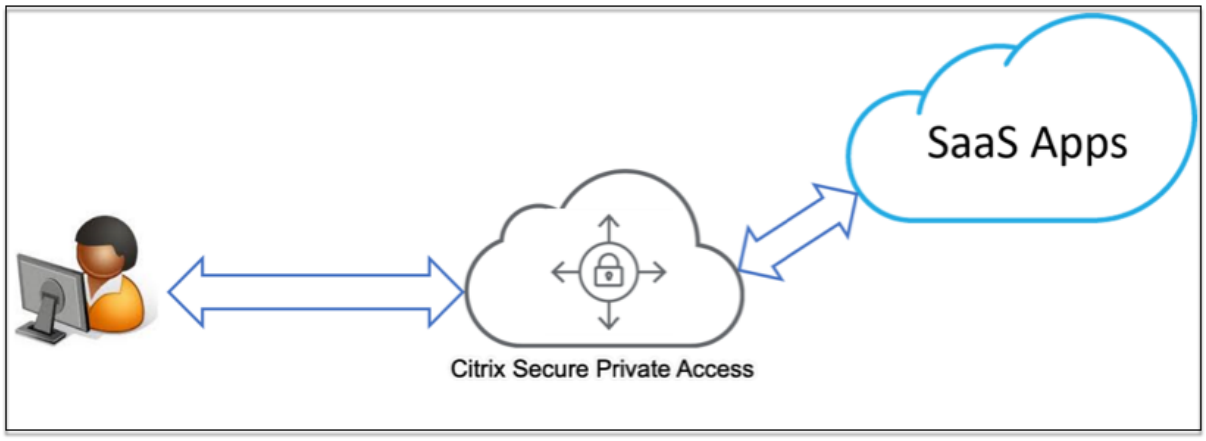
La livraison d'applications SaaS à l'aide du service Secure Private Access vous offre une solution simple, sécurisée, robuste et évolutive pour gérer les applications. Les applications SaaS livrées sur le cloud présentent les avantages suivants :

- **Configuration simple** –Facile à utiliser, à mettre à jour et à consommer.
- **Authentification unique** –Connexion sans tracas avec l'authentification unique.
- **Modèle standard pour différentes applications** –Configuration basée sur un modèle d'applications populaires.

Comment les applications SaaS sont prises en charge avec le service Secure Private Access

1. L'administrateur client configure les applications SaaS à l'aide de l'interface utilisateur du service Secure Private Access.
2. L'administrateur fournit l'URL du service aux utilisateurs pour accéder à Citrix Workspace.
3. Pour lancer l'application, un utilisateur clique sur l'icône de l'application SaaS énumérée.
4. L'application SaaS fait confiance à l'assertion SAML fournie par le service Secure Private Access et l'application est lancée.

> **Remarque**
>
> - Pour accorder l'accès aux applications aux utilisateurs, les administrateurs doivent créer des politiques d'accès. Dans les politiques d'accès, les administrateurs ajoutent des abonnés aux applications et configurent les contrôles de sécurité. Pour plus de détails, voir Créer des politiques d'accès.
> - Les applications SaaS configurées sont agrégées avec les applications virtuelles et d'autres ressources dans Citrix Workspace pour une expérience utilisateur unifiée.



Configurer une application SaaS

La configuration d'une application SaaS implique les étapes de haut niveau suivantes.

1. Configurer les détails de l'application
2. Définir la méthode de connexion préférée
3. Définir le routage des applications

Configurer les détails de l'application

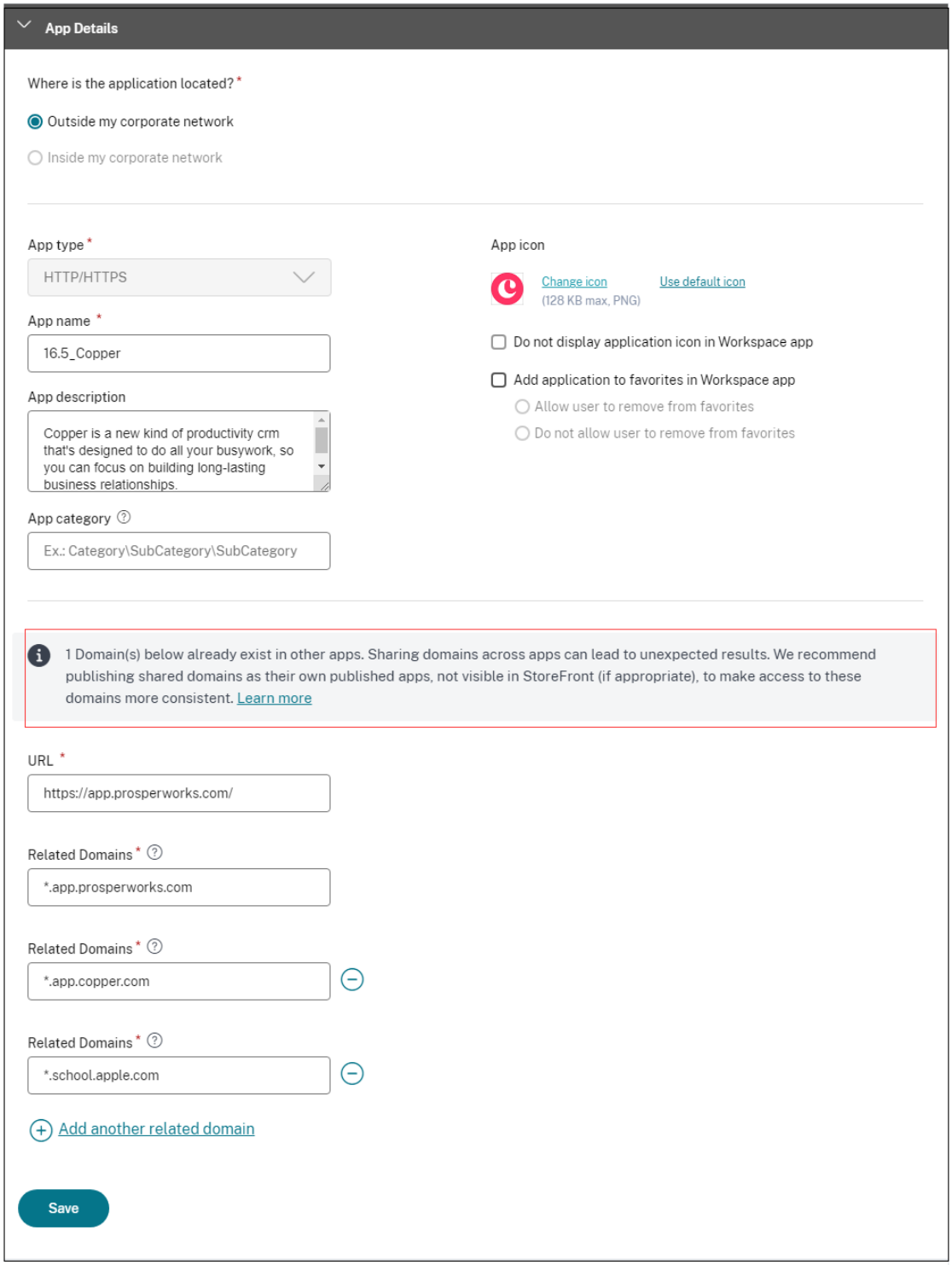
1. Sur la mosaïque **Accès privé sécurisé** , cliquez sur **Gérer.**
2. Cliquez sur **Continuer** puis cliquez sur **Ajouter une application.**

> **Remarque**
>
> - Le bouton **Continuer** apparaît uniquement la première fois que vous utilisez l'assistant. Dans les utilisations suivantes, vous pouvez accéder directement à la page **Applications** puis cliquer sur **Ajouter une application.**
> - Vous pouvez ajouter une application SaaS manuellement en saisissant les détails de l'application ou en sélectionnant un modèle d'application disponible pour une liste d'applications SaaS populaires. Le modèle pré-remplit une grande partie des informations nécessaires à la configuration des applications. Toutefois, les informations spécifiques au client doivent toujours être fournies. Pour plus de détails sur le modèle de configuration d'application SaaS, consultez Configuration spécifique au serveur d'applications SaaS.

1. Configurer l'application.
   - Pour saisir manuellement les détails de l'application, cliquez sur **Ignorer.**
   - Pour configurer l'application à l'aide d'un modèle, cliquez sur **Suivant.**

Le **En dehors de mon réseau d'entreprise** est activé par défaut pour une application SaaS.

2. Saisissez les détails suivants dans la section **Détails de l'application** et cliquez sur **Suivant.**

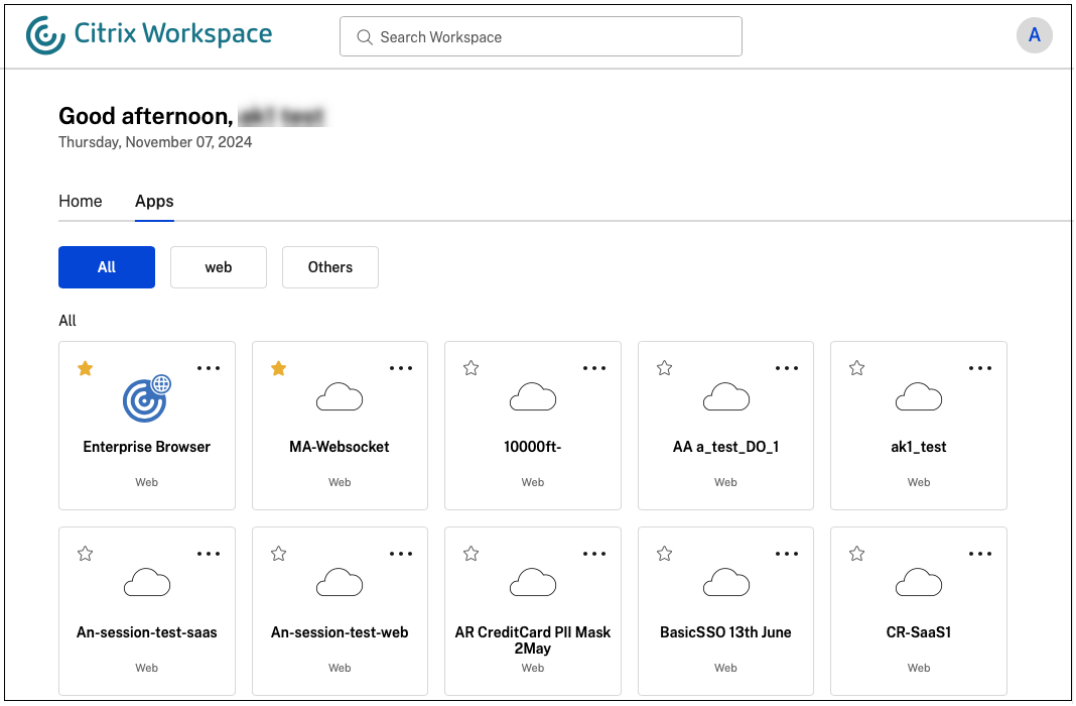


- **Nom de l'application** –Nom de l'application.
- **Description de l'application** - Une brève description de l'application. Cette description

que vous saisissez ici est affichée à vos utilisateurs dans l'espace de travail.

- **Catégorie d'application** - Ajoutez la catégorie et le nom de la sous-catégorie (le cas échéant) sous lesquels l'application que vous publiez doit apparaître dans l'interface utilisateur de Citrix Workspace. Vous pouvez ajouter une nouvelle catégorie pour chaque application ou utiliser des catégories existantes à partir de l'interface utilisateur de Citrix Workspace. Une fois que vous avez spécifié une catégorie pour une application Web ou SaaS, l'application s'affiche dans l'interface utilisateur de l'espace de travail sous la catégorie spécifique.
  - Les catégories/sous-catégories sont configurables par l'administrateur et les administrateurs peuvent ajouter une nouvelle catégorie pour chaque application.
  - Le champ **Catégorie d'application** s'applique aux applications HTTP/HTTPS et est masqué pour les applications TCP/UDP.
  - Les noms des catégories/sous-catégories doivent être séparés par une barre oblique inverse. Par exemple, **Affaires et productivité\Ingénierie**. De plus, ce champ est sensible à la casse. Les administrateurs doivent s'assurer qu'ils définissent la bonne catégorie. S'il existe une incompatibilité entre le nom dans l'interface utilisateur de Citrix Workspace et le nom de catégorie saisi dans le champ **Catégorie d'application** , la catégorie est répertoriée comme une nouvelle catégorie.

    Par exemple, si vous saisissez incorrectement la catégorie **Entreprise et productivité** comme **Entreprise et productivité** dans le champ **Catégorie d'application** , une nouvelle catégorie nommée **Entreprise et productivité** est répertoriée dans l'interface utilisateur de Citrix Workspace en plus de la catégorie **Entreprise et productivité** .



- **Icône de l'application** –Cliquez sur **Modifier l'icône** pour modifier l'icône de l'application. La taille du fichier d'icône doit être de 128x128 pixels. Si vous ne modifiez pas l'icône, l'icône par défaut s'affiche.

```
If you do not want to display the app icon, select **Do not
    display application icon to users**.
```

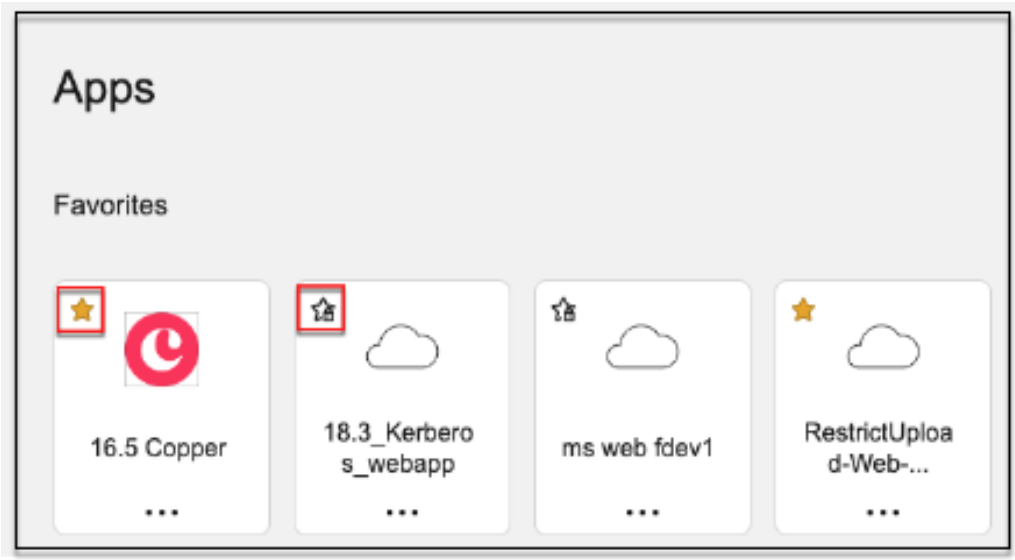
- **URL** –URL avec votre identifiant client. L'URL doit contenir votre identifiant client (identifiant client Citrix Cloud). Pour obtenir votre identifiant client, consultez S'inscrire à Citrix Cloud. En cas d'échec de SSO ou si vous ne souhaitez pas utiliser SSO, l'utilisateur est redirigé vers cette URL.
- **Nom de domaine client** et **ID de domaine client** - Le nom de domaine et l'ID du client sont utilisés pour créer l'URL de l'application et d'autres URL ultérieures dans la page SSO SAML.

```
For example, if you ' re adding a Salesforce app, your domain
    name is `salesforceformyorg` and ID is 123754, then the
    app URL is `https://salesforceformyorg.my.salesforce.com/?
    so=123754.`

Customer domain name and Customer ID fields are specific to
    certain apps.
```

- **Domaines associés** –Le domaine associé est automatiquement renseigné en fonction de l'URL que vous avez fournie. Le domaine associé aide le service à identifier l'URL dans le cadre de l'application et à acheminer le trafic en conséquence. Vous pouvez ajouter

plusieurs domaines associés.

- Cliquez sur **Ajouter automatiquement l'application aux favoris** pour ajouter cette application en tant qu'application favorite dans l'application Citrix Workspace.
  - Cliquez sur **Autoriser l'utilisateur à supprimer des favoris** pour permettre aux abonnés de l'application de supprimer l'application de la liste des applications favorites dans l'application Citrix Workspace. Lorsque vous sélectionnez cette option, une icône en forme d'étoile jaune apparaît dans le coin supérieur gauche de l'application dans l'application Citrix Workspace.
  - Cliquez sur **Ne pas autoriser l'utilisateur à supprimer des favoris** pour empêcher les abonnés de supprimer l'application de la liste des applications favorites dans l'application Citrix Workspace. Lorsque vous sélectionnez cette option, une icône en forme d'étoile avec un cadenas apparaît dans le coin supérieur gauche de l'application dans l'application Citrix Workspace.



Si vous supprimez les applications marquées comme favorites de la console du service Secure Private Access, ces applications doivent être supprimées manuellement de la liste des favoris dans Citrix Workspace. Les applications ne sont pas automatiquement supprimées de l'application Workspace si elles sont supprimées de la console du service Secure Private Access.

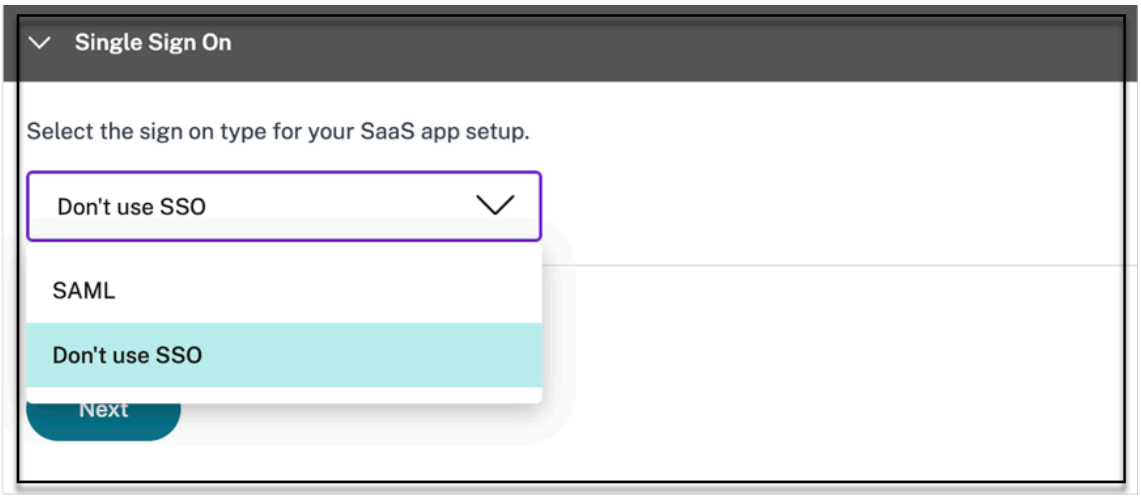
3. Cliquez sur **Suivant.**

> **Important :**
>
> - Pour permettre un accès basé sur la confiance zéro aux applications, l'accès aux applications se voit refuser par défaut. L'accès aux applications est activé uniquement si une poli-

> tique d'accès est associée à l'application. Pour plus de détails, voir Accès refusé aux applications, par défaut.
> - Si plusieurs applications sont configurées avec le même nom de domaine complet ou une variante du nom de domaine complet générique, cela peut entraîner une configuration conflictuelle. Pour plus de détails, voir Configuration conflictuelle pouvant entraîner des problèmes d'accès aux applications.

Définir une méthode de connexion préférée

1. Dans la section **Authentification unique** , sélectionnez le type d'authentification unique que vous préférez utiliser pour votre application et cliquez sur **Enregistrer.** Les types d'authentification unique suivants sont disponibles.



   - **Ne pas utiliser SSO** –Utilisez l'option **Ne pas utiliser SSO** lorsque vous n'avez pas besoin d'authentifier un utilisateur sur le serveur principal. Lorsque l'option **Ne pas utiliser SSO** est sélectionnée, l'utilisateur est redirigé vers l'URL configurée dans la section **Détails de l'application** .
   - **SAML** - Choisissez **SAML** pour l'authentification unique basée sur SAML dans les applications Web. Saisissez les détails de configuration pour le type SSO **SAML** .

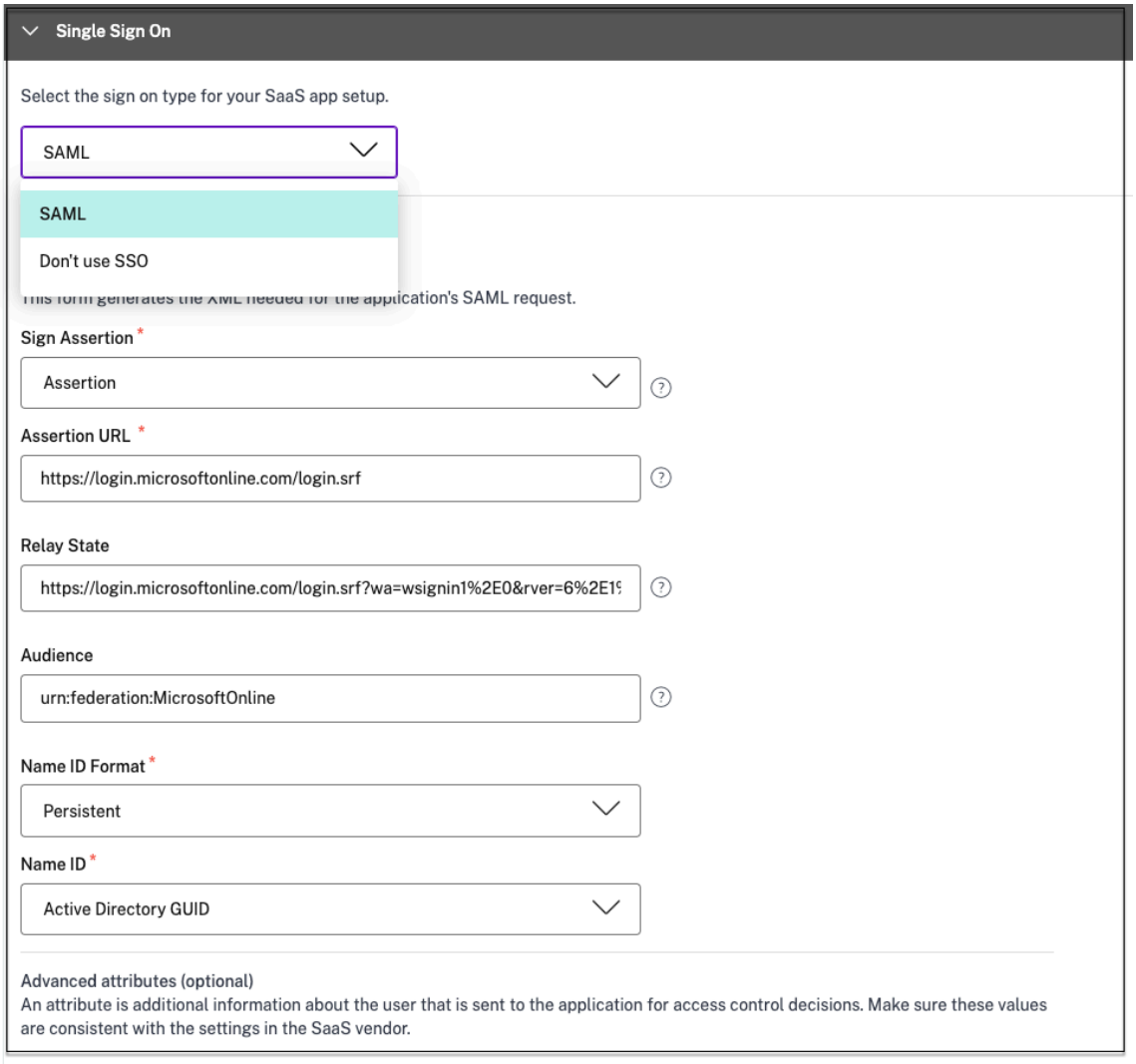
     Saisissez les informations suivantes dans la section Connexion et cliquez sur **Enregistrer**.

     - **Assertion de signature** - La signature de l'assertion ou de la réponse garantit l'intégrité du message lorsque la réponse ou l'assertion est remise à la partie de confiance (SP). Vous pouvez sélectionner **Assertion, Réponse, Les deux,** ou **Aucun**.
     - **URL d'assertion** –L'URL d'assertion est fournie par le fournisseur de l'application. L'assertion SAML est envoyée à cette URL.
     - **État du relais** –Le paramètre État du relais est utilisé pour identifier la ressource spécifique à laquelle les utilisateurs accèdent après s'être connectés et dirigés vers le

serveur de fédération de la partie de confiance. Relay State génère une URL unique pour les utilisateurs. Les utilisateurs peuvent cliquer sur cette URL pour se connecter à l'application cible.

- **Audience** –L'audience est fournie par le fournisseur de l'application. Cette valeur confirme que l'assertion SAML est générée pour l'application correcte.
- **Format d'identifiant de nom** –Sélectionnez le format d'identifiant de nom pris en charge.
- **ID de nom** –Sélectionnez l'ID de nom pris en charge.
- Sélectionnez **Lancez l'application à l'aide de l'URL spécifique (initiée par le fournisseur de services)** pour remplacer le flux initié par le fournisseur d'identité et utiliser uniquement le flux initié par le fournisseur de services.

2. Dans **Attributs avancés (facultatif)**, ajoutez des informations supplémentaires sur l'utilisateur qui sont envoyées à l'application pour les décisions de contrôle d'accès.



3. Téléchargez le fichier de métadonnées en cliquant sur le lien sous **Métadonnées SAML**. Utilisez

le fichier de métadonnées téléchargé pour configurer SSO sur le serveur d'applications SaaS.

> **Remarque**
>
> - Vous pouvez copier l'URL de connexion SSO sous **URL de connexion** et utiliser cette URL lors de la configuration de SSO sur le serveur d'applications SaaS.
> - Vous pouvez également télécharger le certificat à partir de la liste **Certificat** et utiliser le certificat lors de la configuration de SSO sur le serveur d'applications SaaS.

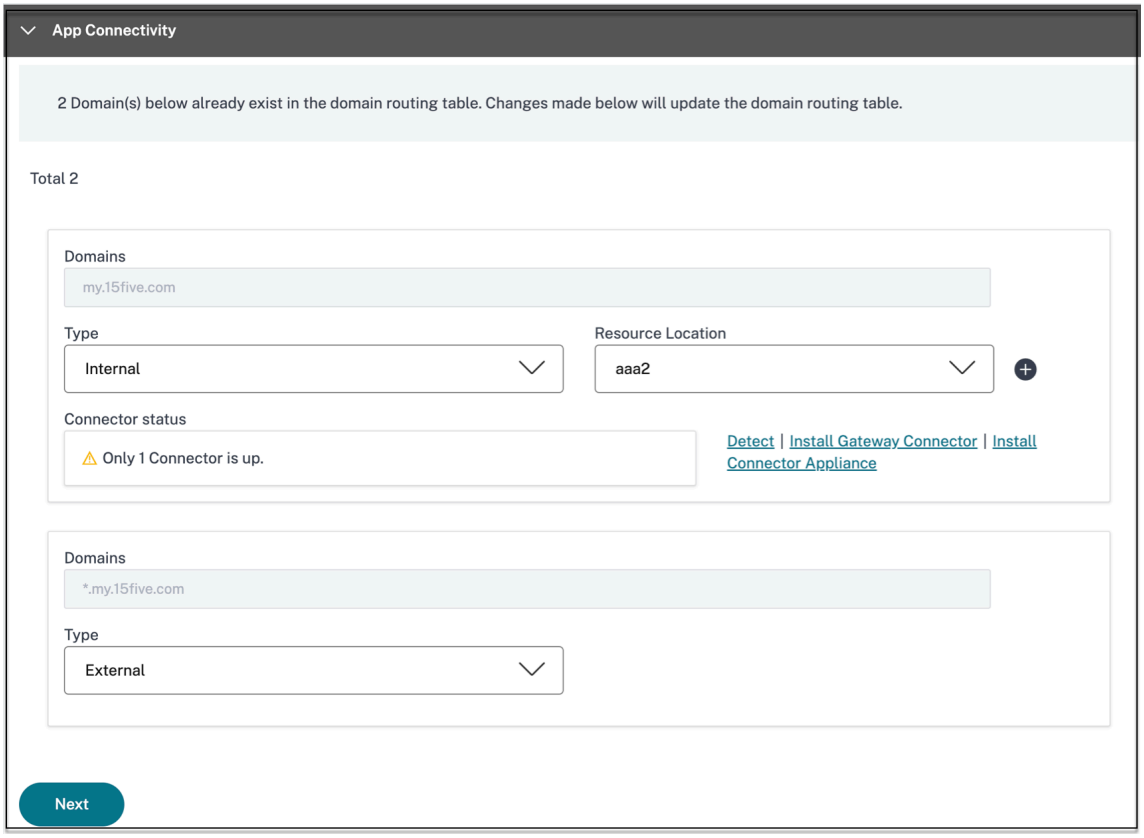
1. Cliquez sur **Suivant.**

Définir le routage des applications

1. Dans la section **App Connectivity** , définissez le routage pour les domaines associés des applications, si les domaines doivent être acheminés en externe ou en interne via les appliances Citrix Connector.

   - **Interne –Contourner le proxy** - Le trafic du domaine est acheminé via Citrix Cloud Connector, en contournant le proxy Web du client configuré sur l'appliance Connector.
   - **Interne via le connecteur** - Les applications peuvent être externes mais le trafic doit circuler via l'appliance Connector vers le réseau extérieur.

   Pour plus de détails, consultez Tables de routage pour résoudre les conflits si les domaines associés dans les applications SaaS et Web sont les mêmes.

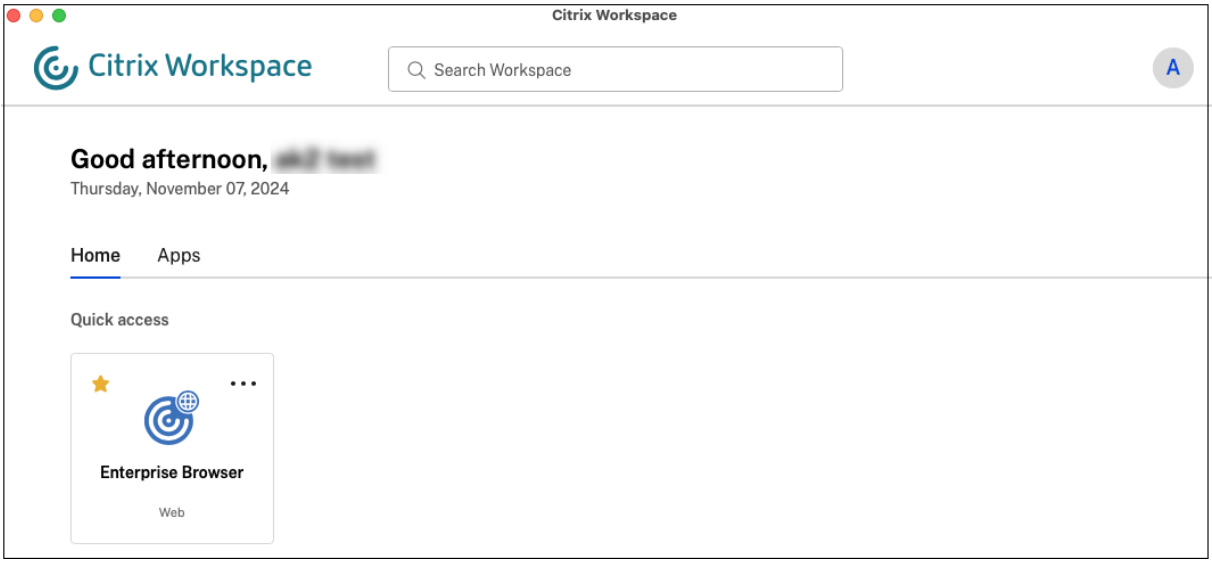


2. Cliquez sur **Terminer.**

   Après avoir cliqué sur **Terminer**, l'application est ajoutée à la page Applications. Vous pouvez modifier ou supprimer une application depuis la page Applications après avoir configuré l'application. Pour ce faire, cliquez sur le bouton points de suspension d'une application et sélectionnez les actions en conséquence.

   - **Modifier l'application**
   - **Supprimer**

Lorsque vous publiez une application Web ou SaaS à partir du service Secure Private Access et si cette application n'est pas masquée, l'application Citrix Enterprise Browser s'affiche automatiquement dans l'interface utilisateur de Citrix Workspace. De plus, le navigateur Citrix Enterprise est également ajouté comme application favorite, par défaut. Les utilisateurs finaux peuvent lancer le navigateur de l'espace de travail sans URL et accéder aux sites Web internes à l'aide des navigateurs de l'espace de travail.



Références

Pour une configuration complète de bout en bout d'une application, consultez Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles.

Configuration des applications à l'aide d'un modèle

December 27, 2023

La configuration des applications SaaS avec authentification unique sur le service Secure Private Access est simplifiée en fournissant une liste de modèles pour les applications SaaS populaires. L'application SaaS à configurer peut être sélectionnée dans la liste.

Le modèle préremplit une grande partie des informations nécessaires à la configuration des applications. Toutefois, les informations spécifiques au client doivent toujours être fournies.

> **Remarque :**
>
> La section suivante décrit les étapes à suivre sur le service Secure Private Access pour configurer et publier une application à l'aide d'un modèle. Les étapes de configuration à effectuer sur le serveur d'applications sont présentées dans la section suivante.

Configuration et publication d'applications à l'aide d'un modèle

Sur la vignette **Secure Private Access**, cliquez sur **Gérer.**

1. Cliquez sur **Continuer**, puis sur **Ajouter une application.**

   > **Remarque :**
   >
   > Le bouton **Continuer** n'apparaît que la première fois que vous utilisez l'assistant. Dans les utilisations suivantes, vous pouvez accéder directement à la page **Applications**, puis cliquer sur **Ajouter une application.**

2. Sélectionnez l'application que vous souhaitez configurer dans la liste **Choisir un modèle** et cliquez sur **Suivant.**

3. Saisissez les informations suivantes dans la section **Détails de l'application**, puis cliquez sur **Enregistrer.**

   Nom de l'application : nom de l'application.

   Description de l'application : brève description de l'application. La description que vous entrez ici est affichée pour vos utilisateurs dans l'espace de travail.

   Icône de l'application : cliquez sur **Modifier l'icône** pour modifier l'icône de l'application. La taille du fichier d'icônes doit être de 128 x 128 pixels. Si vous ne modifiez pas l'icône, l'icône par défaut est affichée.

   Si vous ne souhaitez pas afficher l'icône de l'application, sélectionnez **Ne pas afficher l'icône de l'application aux utilisateurs.**

   URL : URL avec votre ID client. L'utilisateur est redirigé vers cette URL si l'option ;
   - L'authentification unique échoue ou
   - **Ne pas utiliser l'authentification** unique est sélectionnée.

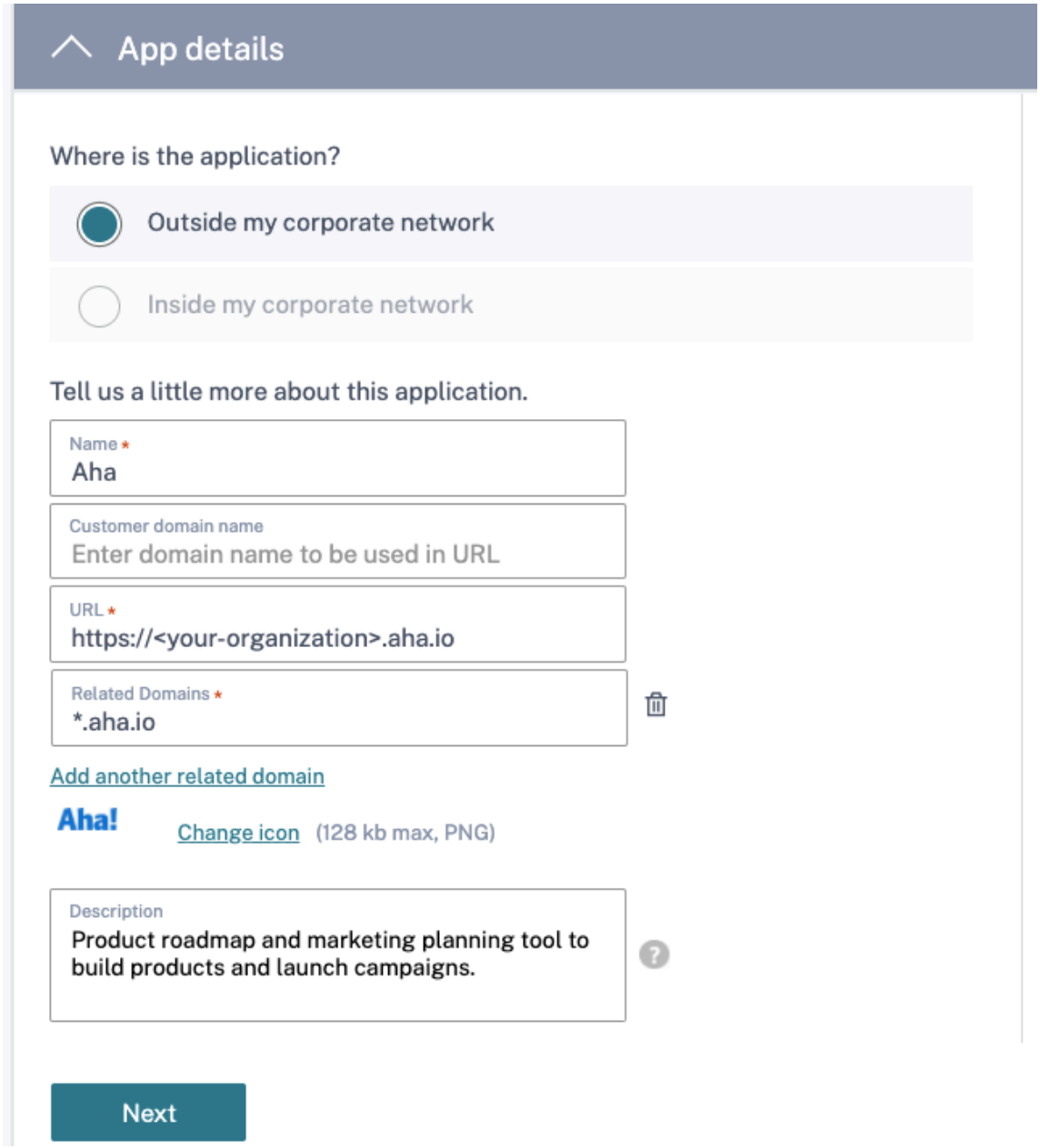
   Nom de domaine clientet ID de domaine client : le nom et l'ID de domaine du client sont utilisés pour créer une URL d'application et d'autres URL suivantes dans la page SSO SAML.

   Par exemple, si vous ajoutez une application Salesforce, votre nom de domaine est `salesforceformyorg` et l'ID est 123754, puis l'URL de l'application est `https://salesforceformyorg.my.salesforce.com/?so=123754.`

   Les champs Nom de domaine du client et ID client sont spécifiques à certaines applications.

   Domaines associés : le domaine associé est automatiquement renseigné en fonction de l'URL que vous avez fournie. Le domaine associé aide le service à identifier l'URL dans le cadre de l'application et à acheminer le trafic en conséquence. Vous pouvez ajouter plusieurs domaines associés.

   Icône : cliquez sur **l'icône Modifier** pour modifier l'icône de l'application. La taille du fichier d'icônes doit être de 128 x 128 pixels. Si vous ne modifiez pas l'icône, l'icône par défaut est affichée.



4. Entrez les détails de configuration SAML suivants dans la section **Single Sign** On et cliquez sur **Enregistrer.**

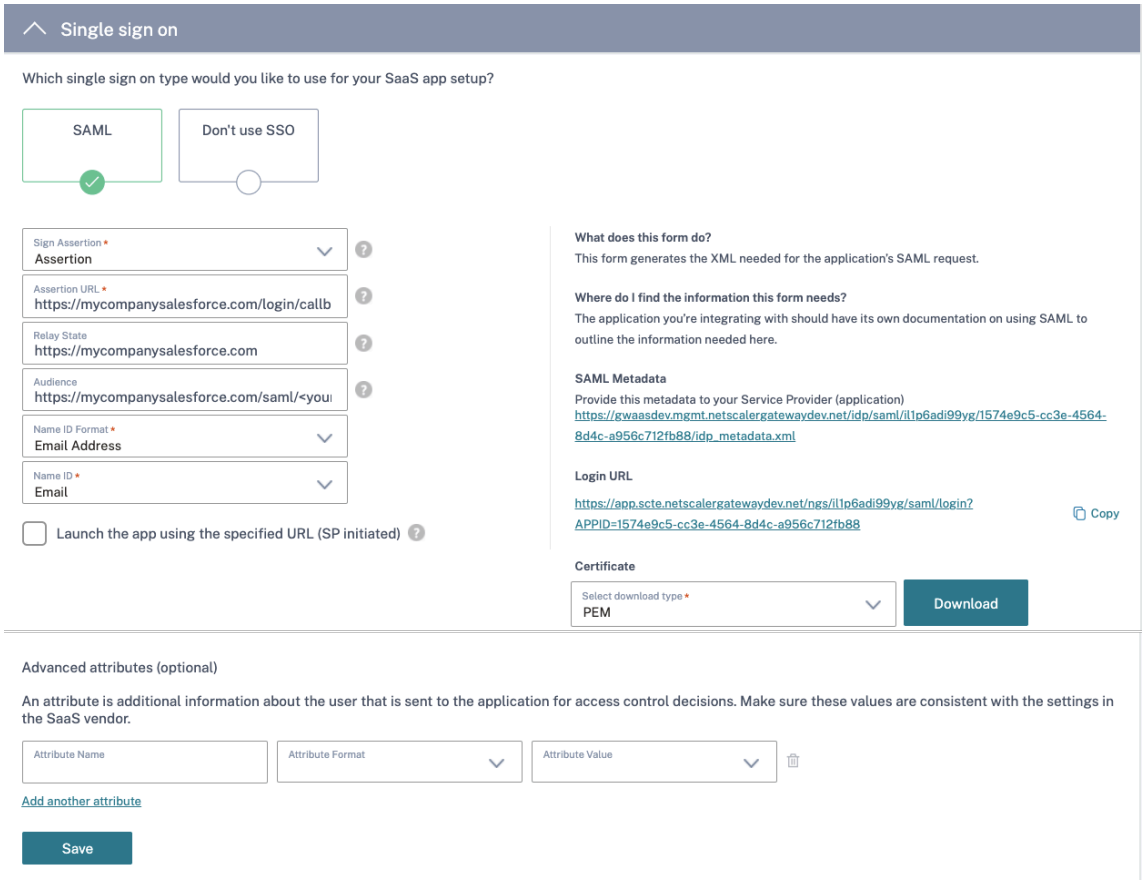
   URL d'assertion : URL d'assertion SAML de l'application SaaS fournie par le fournisseur de l'application. L'assertion SAML est envoyée à cette URL.

   État du relais : le paramètre Relay State est utilisé pour identifier la ressource spécifique à laquelle les utilisateurs accèdent une fois qu'ils sont connectés et dirigés vers le serveur de fédération de la partie de confiance. État de relais génère une URL unique pour les utilisateurs. Les utilisateurs peuvent cliquer sur cette URL pour ouvrir une session sur l'application cible.

   Audience : fournisseur de services auquel l'assertion est destinée.

Format de l'ID de nom : type de format d'utilisateur pris en charge.

ID de nom : nom du type de format de l'utilisateur.



Remarque :

Lorsque l'option **Ne pas utiliser l'authentification** unique est sélectionnée, l'utilisateur est redirigé vers l'URL configurée dans la section **Détails de l'application** .

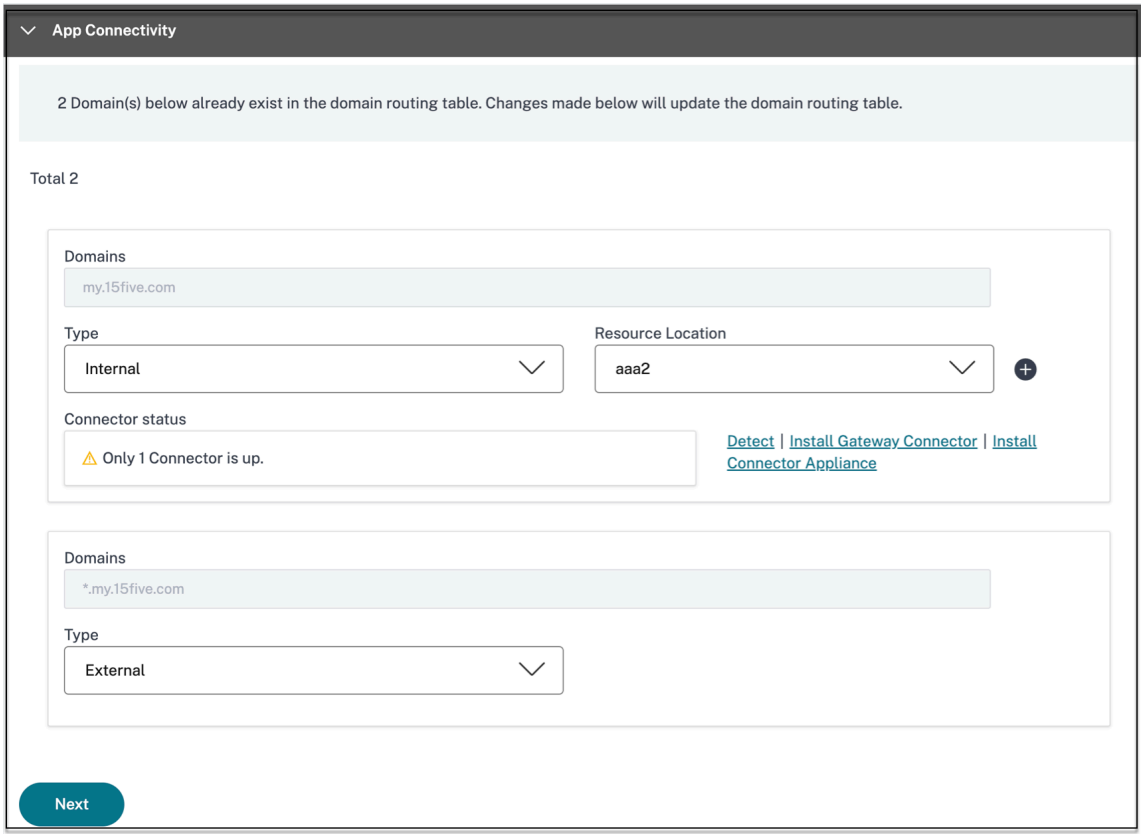
5. Téléchargez le fichier de métadonnées en cliquant sur le lien sous **Métadonnées SAML.** Utilisez le fichier de métadonnées téléchargé pour configurer l'authentification SSO sur le serveur d'applications SaaS.

   Remarque :

   - Vous pouvez copier l'URL de connexion SSO sous URL de **connexion** et utiliser cette URL lors de la configuration de l'authentification unique sur le serveur d'applications SaaS.
   - Vous pouvez également télécharger le certificat à partir de la liste des **certificats** et utiliser le certificat lors de la configuration de l'authentification SSO sur le serveur d'applications SaaS.

6. Cliquez sur **Suivant.**

7. Dans la section **App Connectivity** , définissez le routage pour les domaines d'applications associés, si les domaines doivent être routés en externe ou en interne via une appliance Citrix Connector. Pour plus de détails, consultez la section Tables de routage pour résoudre les conflits si les domaines associés dans les applications SaaS et Web sont identiques.



8. Cliquez sur **Terminer.**

   Après avoir cliqué sur **Terminer**, l'application est ajoutée à la page Applications. Vous pouvez modifier ou supprimer une application depuis la page Applications après avoir configuré l'application. Pour ce faire, cliquez sur le bouton de sélection d'une application et sélectionnez les actions correspondantes.

   - **Modifier l'application**
   - **Supprimer**

> **Remarque :**
>
> Pour accorder l'accès aux applications aux utilisateurs, les administrateurs doivent créer des stratégies d'accès. Dans les stratégies d'accès, les administrateurs ajoutent des abonnés à l'application et configurent des contrôles de sécurité. Pour plus de détails, voir Création de stratégies d'accès.

Configuration spécifique au serveur d'applications SaaS

December 27, 2023

Vous trouverez ci-dessous les liens vers les documents contenant des conseils sur la configuration spécifique du serveur d'applications à l'aide d'un modèle. Citrix prend actuellement en charge les applications SaaS suivantes et ajoute continuellement la prise en charge d'autres applications.

- 15Five - Outil de gestion continue des performances pour coacher les employés.
- 10000 ft - Outil de gestion de projet pour planifier la croissance.
- 4me - Outil de gestion des services pour la collaboration entre les équipes internes, externes et externalisées.
- Abacus - Logiciel de rapport de dépenses en temps réel.
- Absorb - Outil de gestion de l'apprentissage.
- Accompa - Outil de gestion des exigences pour créer des produits.
- Adobe Captivate Prime - Système de gestion de l'apprentissage pour offrir des expériences d'apprentissage personnalisées sur tous les appareils.
- Aha - Feuille de route produit et outil de planification marketing pour créer des produits et lancer des campagnes.
- AlerTops - Outil de réponse aux incidents de collaboration pour gérer les incidents informatiques.
- Allocadia - Outil de gestion des performances marketing pour gérer le processus de planification marketing d'une organisation. ‘
- Anaplan - Outil de planification pour aider les organisations à prendre des décisions en connectant les données, les personnes et les plans.
- &frankly - Un outil d'engagement pour susciter le changement sur le lieu de travail.
- Anodot - Une plateforme d'IA qui surveille les données chronologiques, détecte les anomalies et prévoit les performances de l'entreprise en temps réel.
- App Follow - Outil de gestion des produits pour accélérer la croissance mondiale des applications et augmenter la fidélité des clients.
- Assembla - Outil de contrôle de version et de gestion du code source pour le développement de logiciels.
- Automox - Outil de gestion des correctifs pour suivre, contrôler et gérer le processus d'application des correctifs.

- Azendoo - Outil de collaboration permettant aux équipes de converser et de collaborer.
- BambooHR - Outil de gestion des ressources humaines pour gérer les données des employés.
- Bananatag - Outil de suivi et de planification des e-mails, de suivi des fichiers et de création de modèles d'e-mails
- Base CRM - Outil de gestion des ventes pour gérer les e-mails, les appels téléphoniques et les notes.
- Beekeeper - Outil permettant d'intégrer plusieurs systèmes opérationnels et canaux de communication dans un Secure Hub accessible depuis un ordinateur de bureau et des appareils mobiles.
- BitaBIZ - Outil de planification et de communication des absences et des vacances pour la gestion des congés et des absences.
- BlazeMeter - Suite de test.
- Blissbook - Outil de gestion des stratégies pour créer des manuels d'employés.
- BlueJeans - Solution de visioconférence.
- Bold360 - Outil de chat en direct pour l'engagement client.
- Bonusly - Outil de reconnaissance des employés et de gestion des récompenses pour reconnaître les contributions de l'équipe.
- Box - Outil de gestion de contenu et de partage de fichiers pour gérer, partager et accéder à votre contenu.
- Branch - Une plateforme de liaison mobile alimentant les liens profonds et mobiles.
- Brandfolder - Outil de gestion des actifs numériques pour stocker et partager des actifs numériques.
- Breezy HR - Logiciel de recrutement et système de suivi des candidats.
- Buddy Punch - Outil de gestion du temps pour contrôler la présence des employés.
- Bugsnag - Outil de surveillance pour gérer la stabilité des applications et signaler les erreurs et les données de diagnostic.
- Buildkite - Outil d'infrastructure pour le développement de logiciels d'intégration continue.
- Bullseye Locations - Outil de localisation de magasin pour localiser un magasin ou un revendeur sur un appareil.
- CA Flowdock –Outil de collaboration permettant aux équipes de dialoguer et de collaborer.
- CakeHR - Outil de gestion des ressources humaines pour la gestion des présences et du rendement.

- Cardboard - Outil collaboratif de planification produit pour suivre les informations désorganisées.
- Citrix Cedexis - Outil de gestion du trafic pour les grands sites Web afin de tirer parti du sourcing multifournisseur de centres de données, de fournisseurs de cloud et de réseaux de diffusion de contenu.
- CipherCloud - Plateforme qui fournit une protection des données de bout en bout et une protection avancée contre les menaces, ainsi que des fonctionnalités de conformité complètes pour une entreprise qui adopte des applications basées sur le cloud.
- Celoxis - Outil de gestion de projet pour créer des plans de projet, automatiser le travail et collaborer.
- CircleHD - Outil de formation, d'apprentissage et de collaboration pour partager des vidéos et des diapositives au sein de l'organisation.
- Circonus - Outil d'analyse et de surveillance des données pour fournir des alertes, des graphiques, des tableaux de bord et des informations d'apprentissage automatique.
- Cisco Umbrella - Plateforme de sécurité cloud pour fournir la première ligne de défense contre les menaces sur Internet.
- Citrix RightSignature - Une solution pour obtenir des documents signés électroniquement.
- ClearSlide - Outil d'engagement commercial permettant aux utilisateurs de partager du contenu et du matériel de vente pour l'interaction client.
- Cloudability - Plateforme de gestion des coûts du cloud pour améliorer la visibilité, l'optimisation et la gouvernance dans les environnements cloud.
- CloudAMQP - Outil de file d'attente de messages pour transmettre des messages entre les processus et les autres systèmes.
- CloudCheckr - Outil de gestion des coûts, de sécurité, de création de rapports et d'analyse pour aider les utilisateurs à optimiser leurs déploiements AWS et Azure.
- CloudMonix - Outil de surveillance et d'automatisation des ressources cloud et sur site.
- CloudPassage - Outil de visibilité et de surveillance continue pour réduire les cyberrisques et maintenir la conformité.
- CloudRanger - Outil pour rationaliser vos sauvegardes, la reprise après sinistre et le contrôle des serveurs pour AWS Cloud.
- Clubhouse - Outil de gestion de projet pour le développement de logiciels.
- Coggle - Application Web de Mind Mapping pour créer des documents structurés hiérarchiquement, comme un arbre de branchement.

- Comm100 - Logiciel de service client et outil de communication pour les professionnels du service client.
- Confluence –Outil de collaboration de contenu pour aider les équipes à collaborer et à partager leurs connaissances.
- ConceptShare - Outil de vérification pour diffuser du contenu plus rapidement, plus rapidement et à moindre coût.
- Concur - Outil de gestion des déplacements et des dépenses pour gérer les dépenses en déplacement.
- ConnectWise Control - Outil de gestion d'entreprise pour fournir une assistance et un accès à distance.
- Contactzilla - Outil de gestion des contacts pour accéder à des informations de contact à jour.
- ContractSafe - Outil de gestion des contrats pour suivre, stocker et gérer les contrats.
- Contentful - Logiciel de contenu permettant de créer, gérer et distribuer du contenu sur n'importe quelle plate-forme.
- Convo - Outil de communication et de collaboration d'équipe pour les conversations internes.
- Copper - Outil CRM.
- Cronitor - Outil de surveillance des tâches Cron.
- Crowdin - Solution qui fournit une localisation transparente et continue pour les développeurs.
- Dashlane - Outil de gestion des mots de passe qui gère également les portefeuilles numériques.
- Declaree - Outil de gestion des voyages et des dépenses pour les voyages d'affaires.
- Dell Boomi - Un outil d'intégration pour connecter des applications et des données dans le cloud et sur site.
- Deskpro - Outil d'assistance pour faciliter la gestion des tickets, l'auto-assistance client et les commentaires des clients.
- Deputy - Outil de gestion des effectifs pour planifier et suivre le temps, les tâches et la communication des employés.
- DigiCert - Outil de gestion et de dépannage des certificats SSL pour les sites Web.
- Dmarcian - Outil de surveillance des e-mails pour filtrer le spam, les logiciels malveillants et le phishing.
- DocuSign - Un outil de signature en ligne pour différents documents, tels que les assurances, les soins médicaux et l'immobilier.
- DOME9 ARC –Outil de sécurité et de conformité pour la gestion des environnements de cloud public.

- Dropbox - Outil de stockage dans le cloud pour un partage et un stockage sécurisés des fichiers.
- Duo - Outil de sécurité pour fournir un accès sécurisé à vos applications.
- Dynatrace - Services de laboratoire médical.
- Easy Projects - Outil de gestion de projets.
- EdApp - Outil de gestion de l'apprentissage pour l'apprentissage de l'espace de travail.
- EduBrite - Outil de gestion de l'apprentissage pour créer, diffuser et suivre des programmes de formation.
- Ekarda - Outil de conception de cartes électroniques.
- Envoy - Outil de gestion des visiteurs pour gérer les personnes et les paquets.
- Evernote - Application de prise de notes, d'organisation, de listes de tâches et d'archivage.
- Expensify - Outil de gestion des dépenses pour la gestion des notes de frais, le suivi des reçus et les déplacements professionnels.
- ezeep - Outil de gestion de l'infrastructure d'impression pour imprimer depuis n'importe quel appareil, n'importe quel emplacement vers n'importe quelle imprimante dans le Cloud.
- EZOfficeInventory - Outil de gestion des stocks pour suivre tous vos actifs et équipements.
- EZRentout - Outil de location d'équipement pour suivre la qualité et la disponibilité des équipements.
- Fastly - Plateforme cloud Edge pour servir et sécuriser les applications au plus près des utilisateurs.
- Favro - Outil de planification et de collaboration pour le flux organisationnel.
- Federated Directory - Outil d'annuaire de contacts interentreprises permettant de rechercher dans les carnets d'adresses des différentes entreprises.
- Feeder
- Feedly - Outil d'agrégation de nouvelles pour compiler des flux d'actualités provenant de différentes sources.
- FileCloud - Solution logicielle qui fournit une plateforme d'hébergement et de partage de fichiers robuste et sécurisée pour les organisations.
- Fivetran - Outil pour aider les analystes à répliquer les données dans un entrepôt cloud.
- Flatter Files - Classeur numérique plat pour les dessins et les documents afin de fournir un moyen sûr et simple d'accéder au contenu.
- Float - Outil de planification des ressources pour la planification des projets et la gestion de l'utilisation des équipes.

- Flock - Outil de collaboration.
- Formstack - Un générateur de formulaires en ligne et un outil de collecte de données.
- FOSSA - Outils automatisés d'analyse des licences open source et de gestion des vulnérabilités intégrés en natif dans CI/CD.
- Freshdesk - Outil de support client pour aider à répondre aux besoins des clients.
- Freshservice - outil d'assistance informatique pour simplifier les opérations informatiques.
- FrontApp - Outil de collaboration pour gérer toutes les conversations en un seul endroit.
- Frontify - Plateforme pour faciliter et rationaliser les opérations quotidiennes de marque, de marketing et de développement.
- Fulcrum - Plateforme de collecte de données mobiles qui vous permet de créer facilement des formulaires mobiles et de collecter des données.
- Fusebill - Logiciel de gestion de la facturation et de facturation récurrente.
- G-Suite - Ensemble d'applications intelligentes pour connecter les personnes de votre entreprise.
- GetGuru - Logiciel de gestion des connaissances.
- GitBook - Outil pour créer et gérer votre documentation.
- GitHub - Un service d'hébergement Web pour le contrôle de version utilisant Git pour les référentiels hébergés derrière un pare-feu d'entreprise.
- GitLab - Une plateforme DevOps complète, fournie sous la forme d'une application unique.
- GlassFrog - Logiciel pour la pratique de l'holacratie.
- GoodData - Une plateforme de BI et d'analyse intégrée qui fournit des analyses rapides, fiables et faciles à utiliser
- GoToMeeting - Logiciel de réunion en ligne avec fonctionnalités de visioconférence HD.
- HackerRank - Propose des défis de programmation compétitifs aux consommateurs et aux entreprises.
- HappyFox - Logiciel de service d'assistance en ligne et système de ticket de support Web.
- Helpjuice - Solution de gestion des connaissances pour créer et maintenir des bases de connaissances.
- Help Scout - Logiciel de service client et outil de base de connaissances pour les professionnels du service client.
- Hello sign - Interface de signature électronique pour permettre la signature de n'importe où, à tout moment et sur n'importe quel appareil.

- HelpDocs - un logiciel de base de connaissances pour guider vos utilisateurs lorsqu'ils sont bloqués.
- Honeybadger - Outil de surveillance de l'état des applications.
- Harness - Outil de livraison et d'intégration continues pour les applications Java, .NET dans AWS, GCP, Azure et Bare Metal.
- HelpDocs - Outil pour créer une base de connaissances faisant autorité pour guider vos utilisateurs lorsqu'ils sont bloqués.
- Helpmonks - Une plateforme de messagerie collaborative pour la collaboration en équipe.
- Hoshinplan - Outil pour visualiser vos plans stratégiques et suivre les statuts dans un seul canevas.
- Hosted Graphite - Outil pour surveiller les performances de votre site Web, de votre application, de votre serveur et de votre conteneur.
- Humanity - Logiciel de planification des employés en ligne pour gérer les quarts de travail, les horaires, la paie et l'horloge.
- Igloo - Fournisseur de solutions d'espace de travail numérique et d'intranet pour résoudre les défis informatiques de votre organisation.
- iLobby - Solution de gestion de l'enregistrement des visiteurs basée sur le cloud.
- Illumio - Système de sécurité pour empêcher la propagation des violations dans les environnements de centre de données et de cloud.
- Image Relay - Logiciel de gestion des actifs numériques et de gestion de la marque pour organiser et partager des fichiers numériques en toute sécurité.
- Informatica - Outil d'intégration d'applications SaaS et plateforme de développement et de déploiement de services d'intégration personnalisés.
- Intelligent contract - Logiciel de gestion des contrats.
- iMeet Central - Logiciel de gestion de projet pour les spécialistes du marketing, les agences de création et les entreprises.
- InteractGo - Outil de mesure des données historiques et en temps réel sur les performances du système.
- iQualify One - Outil d'apprentissage et de gestion pour offrir des expériences d'apprentissage authentiques.
- InsideView - Solutions de données et d'intelligence pour résoudre les problèmes de vente, de marketing et d'autres défis commerciaux.

- Insightly - Un outil de gestion de la relation client (CRM) et de gestion de projet basé sur le cloud pour les petites et moyennes entreprises.
- ITGlue - Plateforme de documentation informatique basée sur le cloud pour aider les MSP à normaliser la documentation, à créer des bases de connaissances, à gérer les mots de passe et à suivre les appareils.
- Jitbit - Logiciel de service d'assistance et système de billetterie pour gérer et suivre les e-mails de demande d'assistance entrants et les tickets associés.

JupiterOne - Plateforme logicielle pour créer et gérer l'ensemble de votre processus de sécurité.

- Kanbanize - Un logiciel Kanban de portefeuille en ligne pour la gestion allégée.
- Klipfolio - Une plateforme de tableaux de bord en ligne permettant de créer de puissants tableaux de bord commerciaux en temps réel pour votre équipe ou vos clients.
- Jira - Outil pour planifier, suivre et gérer vos problèmes et projets.
- Kanban Tool - Logiciel de gestion visuelle pour améliorer les performances de votre équipe et augmenter la productivité.
- Keeper Security - Gestionnaire de mots de passe et logiciel de sécurité pour protéger vos mots de passe et vos informations privées.
- Kentik - Outil permettant d'appliquer le Big Data pour la surveillance du réseau et des performances, la protection DDoS et l'analyse des flux réseau ad-hoc en temps réel.
- Kissflow - Outil de flux de travail et logiciel de gestion des flux de travail des processus métier pour automatiser votre processus de flux de travail.
- KnowBe4 - Outil pour fournir une formation de sensibilisation à la sécurité et une simulation d'hameçonnage.
- KnowledgeOwl - Base de connaissances et outil de création.
- Kudos - Systèmes de processus de vente au détail, de travail, de projet et d'exécution.
- LaunchDarkly - Plateforme de gestion des fonctionnalités permettant aux équipes de développement et d'exploitation de contrôler le cycle de vie des fonctionnalités.
- Lifesize - solution de visioconférence.
- Litmos - Système de gestion de l'apprentissage pour la formation des employés, la formation des clients, la formation à la conformité et la formation des partenaires.
- LiquidPlanner - Logiciel de gestion de projets en ligne pour votre entreprise.
- LeanKit - Logiciel de gestion des processus et du travail d'entreprise basé sur Lean pour aider les entreprises à visualiser le travail, à optimiser les processus et à livrer plus rapidement.

- LiveChat - Logiciel de chat en direct et d'assistance pour les entreprises.
- LogDNA - Outil pour collecter, surveiller, analyser et analyser les journaux de toutes les sources dans un seul outil de journalisation centralisé.
- Mango - Logiciel de collaboration en équipe pour consolider et rationaliser les applications cloisonnés en une seule plateforme.
- Manuscrit - Un outil de rédaction pour vous aider à planifier, éditer et partager votre travail.
- Marketo - Logiciel d'automatisation pour aider les équipes marketing à maîtriser l'art et la science du marketing numérique.
- Matomo - Une plateforme d'analyse Web qui évalue l'intégralité du parcours utilisateur de tous ceux qui visitent le site Web.
- Meisterplan - Logiciel qui aide les organisations à créer des portefeuilles de projets.
- Mingle - Un outil de gestion de projet et de collaboration agile pour fournir un espace de travail combiné à l'ensemble de l'équipe.
- MojoHelpDesk - Logiciel de service d'assistance et système de billetterie.
- Monday - Logiciel de gestion d'équipe pour planifier, suivre et collaborer tout votre travail dans un seul outil.
- Mixpanel - Système de suivi des interactions des utilisateurs avec le Web et les appareils mobiles.
- MuleSoft - Logiciel d'intégration pour connecter des applications SaaS et d'entreprise dans le cloud et sur site.
- MyWebTimesheets - Système de suivi du temps en ligne pour suivre le temps passé sur divers projets/emplois/activités.
- New Edge - Service de mise en réseau d'applications sécurisé pour l'informatique hybride.
- NextTravel - Outil logiciel de gestion des voyages d'entreprise.
- N2F - Outil de gestion des notes de frais pour gérer vos dépenses professionnelles et de voyage.
- New Relic - Plateforme d'intelligence numérique pour mesurer et surveiller les performances des applications et de l'infrastructure.
- Nmbrs - Logiciel de gestion des ressources humaines et de paie dans le cloud pour les entreprises.
- Nuclino - Logiciel de collaboration pour collaborer et partager des informations en temps réel.
- Office365 - le service d'abonnement basé sur le cloud de Microsoft.
- OfficeSpace - Plateforme basée sur le cloud qui aide les entreprises à allouer de l'espace de travail.

- OneDesk - Logiciel de gestion de projet et de service d'assistance pour communiquer avec vos clients et les soutenir.
- OpsGenie - Une plateforme de gestion des incidents pour les équipes DevOps et IT Ops afin de rationaliser les processus d'alerte et de résolution des incidents.
- Orginio - Un outil de création d'organigramme en ligne pour visualiser la structure organisationnelle.
- Oomnitza - Solution de plateforme de gestion des actifs informatiques pour suivre et gérer les actifs.
- OpenEye - Application mobile pour visionner des vidéos en direct et enregistrées sur l'enregistreur Apex.
- Oracle ERP Cloud - Suite d'applications logicielles basées sur le cloud pour gérer les fonctions de l'entreprise.
- Pacific Timesheet - Outil Web de feuille de temps pour la paie, les heures de projet et les dépenses.
- PagerDuty - Système de gestion des opérations numériques.
- PandaDoc - Une application mobile permettant aux utilisateurs d'iPhone d'accéder à leurs documents, analyses et tableaux de bord directement sur leur téléphone mobile.
- Panopta - Outil de surveillance de l'infrastructure.
- Panorama9 - Plateforme de gestion informatique basée sur le cloud pour la surveillance du réseau d'entreprise.
- Papyrs - Éditeur pour créer vos propres pages intranet.
- ParkMyCloud - Outil SaaS à usage unique pour se connecter à AWS, Azure Services ou GCP.
- Peakon - Outil pour mesurer et améliorer l'engagement des employés.
- People HR - système logiciel RH pour toutes les fonctions RH clés.
- Pingboard - Outil pour créer des organigrammes pour organiser les équipes et la planification des effectifs.
- Pigeonhole Live - Plateforme interactive de questions-réponses.
- Pipedrive - Logiciel de CRM de vente et de gestion des pipelines.
- PlanMyLeave - Système de gestion des congés pour la gestion et le suivi des congés des employés.
- PlayVox - Outil de surveillance de la qualité du service client.
- Podbean - Fournisseur de services de podcasts.

- Podio - Un outil Web pour organiser la communication d'équipe, les processus métier, les données et le contenu dans les espaces de travail de gestion de projet.
- POPin - Plateforme de résolution de foule et application mobile qui opérationnalise l'engagement de l'équipe pour la résolution de problèmes
- Postman - Environnement de développement d'API.
- Prescreen - Outil de suivi des candidats pour publier les offres d'emploi en ligne et hors ligne.
- ProductBoard - Outil de gestion des produits.
- ProdPad - Logiciel de gestion de produits pour développer des stratégies produits.
- Proto.io - Plateforme de prototypage d'applications pour créer des prototypes haute fidélité entièrement interactifs.
- Proxyclick - Solution de gestion des visiteurs basée sur le cloud pour gérer les visiteurs, développer leur image de marque et assurer la sécurité.
- Pulumi - Plateforme de développement cloud native pour conteneurs, sans serveur, infrastructure et Kubernetes.
- PurelyHR - Outil de gestion des congés pour accéder aux données sur les congés des employés.
- Promapp –Outil de gestion des processus métier (BPM).
- Prescreen - Système de suivi des candidats basé sur le cloud pour publier les offres d'emploi en ligne et hors ligne.
- QAComplete - Outil de gestion des tests logiciels.
- Qualaroo - Outil de rétroaction pour obtenir des informations de la part des clients.
- Quality Built, LLC –Secteur de l'assurance, des finances et de la construction pour fournir des services d'assurance qualité de tiers fiables et innovants.
- Qubole - Plateforme en libre-service pour l'analyse du Big Data basée sur Amazon.
- Questetra BPM Suite - Plateforme de processus métier basée sur le Web pour les flux de travail courants.
- QuestionPro - Logiciel de sondage en ligne pour créer des sondages et des questionnaires.
- Quandora - Solution de gestion des connaissances basée sur les questions et réponses.
- Quip - Suite logicielle de productivité collaborative pour mobile et le Web.
- Rackspace - Services de cloud computing gérés.
- ReadCube - Outil de gestion des références Web, de bureau et mobiles.
- RealtimeBoard - Outil de collaboration sur tableau blanc permettant aux organisations de collaborer au-delà des formats, des outils, des lieux et des fuseaux horaires.

- Receptive - Outil permettant de recueillir les commentaires des clients, des équipes et du marché en un seul endroit.
- Remedyforce - Système de gestion des services informatiques et d'assistance.
- Retrace - Outil de gestion des performances des applications qui fournit le suivi des bogues, l'agrégation des données et des alertes automatiques.
- Robin - Outils d'expérience en milieu de travail pour planifier des salles de conférence et des réservations de bureau.
- Rollbar - Alerte d'erreur en temps réel et outils de débogage pour les développeurs.
- Really Simple Systems - Logiciel CRM basé sur le cloud permettant aux petites entreprises de gérer leurs ventes et leur marketing.
- Reamaze - Logiciel de support client pour soutenir, engager et convertir les clients par chat, réseaux sociaux, SMS, FAQ et e-mail sur une plate-forme unique.
- Resource Guru - Logiciel de gestion des ressources pour planifier le personnel, l'équipement et d'autres ressources.
- Retrace - Gestion des performances des applications pour intégrer le profilage du code, le suivi des erreurs, les journaux des applications et les mesures.
- Roadmunk - Logiciel de feuille de route produit et outil de feuille de route pour créer des feuilles de route de produits.
- Runscope - Outil pour créer, gérer et exécuter des tests et des moniteurs d'API fonctionnels.
- Salesforce - Outil CRM pour gérer les informations de contact des clients, intégrer les médias sociaux et faciliter la collaboration client en temps réel.
- SalesLoft - Plateforme d'engagement commercial pour des ventes efficaces et génératrices de revenus
- Salsify - Plateforme de gestion de l'expérience produit (PXM).
- Samanage - Outil de gestion des services informatiques.
- Samepage - Logiciel de collaboration pour gérer des projets en ligne.
- Screencast-O-Matic —Outil pour capter et éditer des vidéos.
- ScreenSteps —Outils permettant de créer des documents visuels centrés sur des captures d'écran.
- SendSafely —Plateforme de cryptage pour l'échange sécurisé de fichiers et de courriels.
- Sentry - Logiciel de suivi des erreurs open source.
- ServiceDesk Plus - Outil pour le centre de services informatiques.

- ServiceNow - Plateforme Cloud pour créer des flux de travail numériques.
- SharePoint –Plate-forme de collaboration utilisée pour la gestion et le stockage de documents.
- Shufflrr - Outil de gestion des présentations pour créer, mettre à jour, partager et diffuser des présentations.
- Sigma Computing - Un outil d'analyse permettant d'explorer, d'analyser et de visualiser les données.
- Signavio —Un outil de modélisation des processus métier.
- Skeddly - Outil pour automatiser les ressources AWS.
- Skills Base - Outil de gestion des talents pour suivre et documenter les performances et les compétences des employés.
- Skyprep - Système de gestion de l'apprentissage (LMS) pour former les clients et les employés.
- Slack - Outil de collaboration pour communiquer et partager des informations.
- Slemma - Outil d'analyse de données pour créer des rapports de données à partir de plusieurs ensembles de données.
- Sli.do - Outil d'interaction pour les réunions, événements et conférences.
- SmartDraw - Outil de diagramme utilisé pour créer des organigrammes, des organigrammes, des cartes mentales, des diagrammes de projet et d'autres visuels commerciaux.
- SmarterU - Système de gestion de l'apprentissage (LMS) pour former les clients et les employés.
- Smartsheet - Outil de collaboration pour attribuer des tâches, suivre le processus du projet, gérer les calendriers et partager des documents.
- SparkPost - Service de livraison de courrier électronique.
- Split - Application de fractionnement de factures.
- Spoke - Outil de centre de service pour déposer des tickets de service.
- Spotinst - Une plateforme d'optimisation SaaS qui aide les entreprises à acheter et à gérer la capacité de l'infrastructure cloud.
- SproutVideo - Plateforme pour héberger des vidéos professionnelles.
- Stackify - Outil de dépannage qui prend en charge une suite d'outils, notamment Prefix et Retrace.
- StatusCast - Page hébergée pour informer vos employés et vos clients des temps d'arrêt et de la maintenance du site Web.
- StatusDashboard - Plateforme de communication pour héberger des tableaux de bord d'état et diffuser des notifications d'incident aux clients.

- Status Hero - Outil de suivi des mises à jour de statut et des objectifs quotidiens de votre équipe.
- StatusHub - Plateforme pour héberger la page d'état du service.
- Statuspage - Outil de communication de l'état et des incidents.
- SugarCRM - outil CRM pour l'automatisation Salesforce, les campagnes marketing, le support client, la collaboration, le CRM mobile, le CRM social et la création de rapports.
- Sumo Logic - Logiciel d'analyse de données qui se concentre sur la sécurité, les opérations et les cas d'utilisation de la BI.
- Supermood - Plateforme RH pour recueillir les commentaires des employés en temps réel.
- Syncplicity - Outil de partage et de synchronisation de fichiers.
- Tableau - Outil de création de visualisation interactive des données.
- TalentLMS - Système de gestion de l'apprentissage (LMS) pour faciliter les séminaires, cours et autres programmes de formation en ligne.
- Tallie —Outil permettant de capturer et de télécharger des reçus, de générer des notes de frais et de personnaliser les détails des dépenses.
- Targetprocess - Logiciel de gestion de projet Agile pour Scrum, Kanban, SAFe, etc.
- Teamphoria - Logiciel pour fournir des mesures d'engagement des employés en temps réel, des évaluations des employés et une reconnaissance.
- TeamViewer - Application logicielle propriétaire pour le contrôle à distance, le partage de bureau, les réunions en ligne, les conférences Web et le transfert de fichiers entre ordinateurs.
- Tenable.io - Outil qui fournit des données pour identifier, étudier et hiérarchiser la correction des vulnérabilités et des erreurs de configuration dans votre environnement informatique.
- Testable - Outil pour créer des expériences et des enquêtes comportementales.
- TestingBot - Outil permettant de fournir différentes versions de navigateur pour les tests en direct et automatisés.
- TestFairy - Plateforme de test mobile, pour fournir aux entreprises des enregistrements vidéo, des journaux et des rapports de plantage des sessions mobiles.
- TextExpander - Outil de communication permettant d'insérer des extraits de texte provenant d'un référentiel d'e-mails et d'autres contenus, au fur et à mesure de la frappe.
- TextMagic - Service de messagerie pour communiquer avec les clients.
- ThousandEyes - Outil pour surveiller l'infrastructure réseau, résoudre les problèmes de mise à disposition des applications et cartographier les performances Internet.
- Thycotic Secret server - Outil logiciel de gestion de compte pour gérer les mots de passe.

- TimeLive —Outil permettant de fournir des feuilles de temps et de suivre le temps.
- Tinfoil Security - Logiciel de solution de sécurité pour détecter les vulnérabilités.
- Trisotech - Outil qui permet aux clients de découvrir, de modéliser et d'analyser leur entreprise numérique.
- Trumba - Outil pour publier des calendriers d'événements interactifs en ligne.
- TwentyThree - Plateforme de marketing vidéo pour intégrer et ajouter des vidéos à la pile marketing.
- Twilio - Une plateforme de développement pour les communications.
- Ubersmith - Logiciel de gestion d'entreprise pour la facturation basée sur l'utilisation, l'établissement de devis, la gestion des commandes, la gestion de l'infrastructure et les solutions de billetterie du centre d'assistance.
- UniFi - Logiciel de communication et de collaboration avec fonctionnalités vocales, de collaboration Web et de visioconférence.
- UPTRENDS —Solution de surveillance de site Web pour suivre la disponibilité et les performances du site Web.
- UserEcho - outil de forum communautaire qui aide les entreprises à gérer les commentaires des clients.
- UserVoice - Logiciel de gestion des commentaires sur les produits pour permettre aux entreprises de prendre des décisions sur les produits basées sur les données.
- VALIMAIL - Logiciel d'authentification des e-mails pour authentifier les e-mails légitimes et bloquer les attaques par hameçonnage.
- Veracode - L'analyseur de code source et le scanner de code protègent les entreprises contre les cybermenaces et les portes dérobées des applications.
- Velpic - Système de gestion de l'apprentissage (LMS) conçu pour rationaliser la formation en milieu de travail.
- VictorOps - Logiciel de gestion des incidents pour fournir une observabilité DevOps, une collaboration et des alertes en temps réel.
- VIDIZMO - Logiciel de streaming vidéo en direct et à la demande pour les entreprises.
- Visual Paradigm - Plateforme en ligne de modélisation visuelle et de création de diagrammes pour la collaboration en équipe.
- Vtiger - Outil CRM qui permet aux équipes de vente, de support et de marketing de s'organiser et de collaborer.
- WaveMaker - Logiciel pour créer et exécuter des applications personnalisées.

- Weekdone - Outil pour créer un tableau de bord des managers et un service de gestion d'équipe pour les entreprises.
- Wepow - Outil pour connecter les recruteurs, les candidats et les employeurs grâce à une solution d'entretien mobile et vidéo.
- When I Work - Outil de planification des employés et de suivi du temps.
- WhosOnLocation —Outil pour suivre le flux de personnes à travers les sites et les zones.
- Workable - Système de suivi des candidats.
- Workday - Outil de gestion financière, de ressources humaines et de planification.
- Workpath - Outil pour gérer les objectifs et les performances de l'organisation.
- Workplace - Outil de collaboration de Facebook pour aider les employés à communiquer via une interface familière.
- Workstars - Plateforme pour les programmes sociaux et de reconnaissance des employés par les pairs.
- Workteam - Outil de suivi du temps et de la présence des employés.
- Wrike - Logiciel de gestion de projets sociaux et de collaboration.
- XaitPorter - Logiciel de co-création de documents pour les offres et propositions et autres documents commerciaux.
- Ximble - Outil de planification des employés et de suivi du temps.
- XMatters - Plateforme de collaboration avec un logiciel d'alerte qui s'intègre à d'autres outils pour créer un processus transparent et une communication efficace.
- Yodeck - Outil pour gérer les écrans à distance, via le Web ou sur mobile.
- Zendesk - Logiciel permettant de demander le service client et de consigner les tickets de support.
- Ziflow - Outil pour les équipes de production créatives.
- Zillable —Plateforme de collaboration dotée de fonctionnalités de communication.
- Zing tree - Une boîte à outils pour créer des arbres de décision interactifs et des utilitaires de résolution des problèmes.
- ZIVVER - Outil qui permet le transfert sécurisé de courriels et de fichiers depuis votre programme de messagerie familier.
- Zoho - Suite d'applications professionnelles.
- Zoom - Logiciel de communication et de collaboration avec fonctionnalités vocales, de collaboration Web et de visioconférence.

- Zuora - Un logiciel basé sur un abonnement qui permet à une entreprise de lancer, de gérer et de se transformer en entreprise d'abonnement.

Adresses CIDR réservées pour les serveurs TCP et UDP

December 27, 2023

Les administrateurs peuvent configurer des adresses IP CIDR réservées pour les serveurs TCP/UDP. Ces adresses IP sont partagées dans la réponse DNS au lieu de l'adresse IP réelle lors de la résolution DNS.

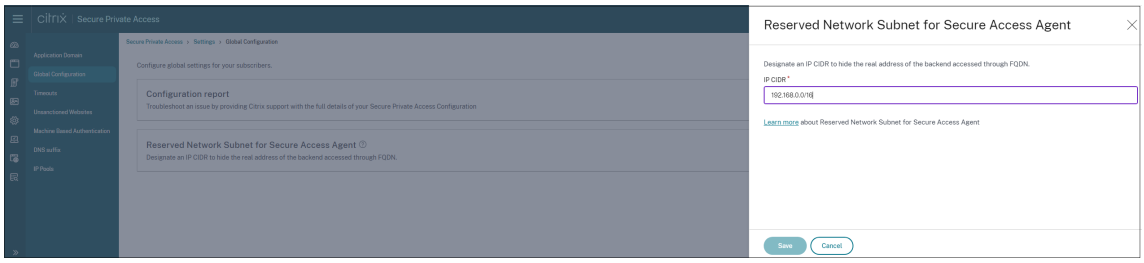
Les plages d'adresses IP CIDR réservées autorisées sont les suivantes :

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> **Remarque :**
>
> Assurez-vous que les adresses IP réservées ne sont pas en conflit avec les adresses suivantes :
>
> - Adresse IP configurée pour les applications TCP/UDP sur le site de ressources du client.
> - Sous-réseau des machines clientes.

Configurer les adresses IP CIDR réservées

1. Cliquez sur **Paramètres**, puis sur **Configuration globale**.



2. Dans le **sous-réseau réservé pour l'agent Secure Access**, cliquez sur **Gérer**.
3. Dans **IP CIDR**, entrez la plage d'adresses IP privées.
4. Cliquez sur **Enregistrer**.

Suffixes DNS pour résoudre les FQDN en adresses IP

December 27, 2023

Le suffixe DNS est une configuration globale qui s'applique à tous les utilisateurs finaux. La fonctionnalité de suffixe DNS du service Citrix Secure Private Access peut être utilisée dans les cas d'utilisation suivants :

- Permettez au client Citrix Secure Access de remplacer un nom de domaine non complet (nom d'hôte) par un nom de domaine complet (FQDN) en ajoutant le domaine de suffixe DNS pour les serveurs principaux.
- Permettez aux administrateurs de configurer des applications à l'aide d'adresses IP (CIDR/plage IP), afin que les utilisateurs finaux puissent accéder aux applications à l'aide du nom de domaine complet correspondant sous le domaine du suffixe DNS.

Par exemple, lors de la résolution d'un nom de domaine « workday » qui n'est pas entièrement qualifié, si le suffixe DNS « citrix.net » est configuré, le système d'exploitation ajoute le suffixe « citrix.net » et le résout en « workday.citrix.net ».

Si plusieurs suffixes DNS sont configurés, les suffixes DNS sont résolus dans une séquence. Supposons, par exemple, que les suffixes suivants soient ajoutés :

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

Lorsqu'un utilisateur final saisit « workday », le système d'exploitation tente de résoudre les FQDN dans l'ordre suivant. S'il réussit avec un suffixe, les suffixes restants sont ignorés.

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> **Important :**
>
> - La configuration du suffixe DNS peut uniquement permettre au client de résoudre un nom de domaine non entièrement qualifié en suffixant le domaine configuré à l'aide de la fonctionnalité de suffixe DNS. Pour qu'un utilisateur final puisse accéder à un FQDN sous le domaine du suffixe DNS, l'administrateur doit configurer une application avec une adresse IP, un FQDN ou un domaine générique. Pour plus de détails, voir le point 4 dans Exemple de cas d'utilisation.
> - Si deux applications différentes sont configurées, l'une avec un nom de domaine complet

> et l'autre avec une adresse IP (toutes deux correspondant au même serveur principal), la stratégie de l'application associée à l'adresse IP a la priorité la plus élevée. Pour plus de détails, voir le point 5 dans Exemple de cas d'utilisation.

Conditions préalables

> - Les clients doivent avoir droit à l'édition Secure Private Access Advanced pour utiliser la fonctionnalité de suffixe DNS.
> - Contactez l'équipe de gestion des produits Citrix pour activer les indicateurs de fonctionnalité de suffixe DNS.

Comment ajouter des suffixes DNS

1. Sur la vignette Secure Private Access, cliquez sur **Gérer**.
2. Sur la page d'accueil de Secure Private Access, cliquez sur **Paramètres,** puis sur **Suffixe DNS**.
3. Dans le champ **Suffixe DNS**, entrez le suffixe qui doit être ajouté lors de la résolution d'un nom non entièrement qualifié.
4. Cliquez sur **Ajouter**.

Les suffixes sont répertoriés en fonction de l'ordre dans lequel ils ont été ajoutés. Les administrateurs peuvent supprimer ou modifier les suffixes.

Exemple de cas d'utilisation

Tenez compte des considérations suivantes :

- Un administrateur a attribué l'adresse IP 192.0.2.1 à une machine du réseau client.
- Les noms de domaine complets de la machine (dont les adresses IP sont 192.0.2.1) se trouvent sous le domaine « citrix.net » (par exemple, workday.citrix.net).

		Suffixe DNS et configuration de l'application	Expérience pour l'utilisateur final
	1	L'administrateur configure le suffixe DNS comme « citrix.net » et crée une application avec l'adresse IP 192.0.2.1 avec une stratégie d'accès définie sur « autoriser » pour l'utilisateur1.	Lorsque user1 essaie de se connecter à « workday », le FQDN est suffixé par « citrix.net » (workday.citrix.net) et l'adresse IP est résolue en 192.0.2.1. Étant donné que la version 192.0.2.1 est autorisée pour l'utilisateur1 avec une application configurée, l'accès est accordé. **Remarque :** l'utilisateur final peut accéder à l'application Workday via 192.0.2.1, workday.citrix.net ou « workday ». Sans configuration du suffixe DNS, l'accès via « workday » et « workday.citrix.net » est refusé.

		Suffixe DNS et configuration de l'application	Expérience pour l'utilisateur final
	2	L'administrateur configure le suffixe DNS comme « citrix.net », crée une application avec le nom de domaine complet (workday.citrix.net) et définit la stratégie d'accès sur « autoriser » pour l'utilisateur1.	Lorsque user1 essaie de se connecter à « workday », « citrix.net » est suffixé à « workday » (workday.citrix.net). L'utilisateur final peut accéder à Workday car une application est configurée avec « workday.citrix.net » et la stratégie d'accès est définie sur « Autoriser » pour l'utilisateur1. **Remarque :** L'utilisateur final peut accéder à l'application Workday via workday.citrix.net ou « workday ». L'accès à 192.0.2.1 est refusé car aucune application n'est configurée avec cette adresse IP.

		Suffixe DNS et configuration de l'application	Expérience pour l'utilisateur final
	3	L'administrateur configure le suffixe DNS comme « citrix.net », crée une application avec le domaine générique « *.citrix.net » et définit la stratégie d'accès sur « autoriser » pour l'utilisateur1.	Lorsque user1 essaie de se connecter à « workday », « citrix.net » est suffixé à « workday » (workday.citrix.net). L'utilisateur final peut accéder à Workday car une application est configurée avec «*.citrix.net » et la stratégie d'accès est définie sur « Autoriser » pour l'utilisateur1. **Remarque :** L'utilisateur final peut accéder à Workday via workday.citrix.net ou « workday ». L'accès à 192.0.2.1 est refusé car aucune application n'est configurée avec cette adresse IP.

		Suffixe DNS et configuration de l'application	Expérience pour l'utilisateur final
	4	L'administrateur configure le suffixe DNS comme « citrix.net ». Aucune application n'est configurée pour user1 avec FQDN (workday.citrix.net) ou 192.0.2.1.	Lorsque user1 essaie de se connecter à « workday », « workday » est suffixé par « citrix.net » par le client et résout « workday.citrix.net » en 192.0.2.1. Toutefois, l'utilisateur 1 ne peut pas se connecter au serveur privé (workday.citrix.net/192.0.2.1) car aucune application n'est configurée avec 192.0.2.1 ou workday.citrix.net ou *.citrix.net pour user1.

	5	L'administrateur configure le suffixe DNS comme « citrix.net ». Ajoute une application dont l'adresse IP est 192.0.2.1 et définit la stratégie d'accès sur « Refuser » pour l'utilisateur1. Ajoute ensuite une autre application avec un nom de domaine complet (workday.citrix.net) qui se résout en 192.0.2.1 et définit la stratégie d'accès sur « autoriser » pour l'utilisateur1.	Lorsque user1 essaie de se connecter à « workday », « citrix.net » est suffixé à Workday (workday.citrix.net) et l'adresse IP est résolue en 192.0.2.1. Toutefois, l'accès à Workday est refusé car la stratégie de l'application configurée avec IP 192.0.2.1 a priorité sur l'application configurée avec le FQDN.

Appliance Connector pour Secure Private Access

June 21, 2024

L'appliance Connector est un composant Citrix hébergé dans votre hyperviseur. Elle sert de canal de communication entre Citrix Cloud et vos emplacements de ressources, ce qui permet d'administrer le cloud sans qu'il soit nécessaire d'effectuer des configurations réseau ou d'infrastructure complexes. L'appliance Connector vous permet de gérer et d'axer la priorité sur les ressources qui apportent de la valeur à vos utilisateurs.

Toutes les connexions sont établies depuis l'appliance Connector vers le cloud à l'aide du port HTTPS standard (443) et du protocole TCP. Aucune connexion entrante n'est acceptée. Le port TCP 443, avec les noms de domaines de compétence FQDN suivants, sont autorisés en sortie :

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net

- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

Configuration de Secure Private Access avec Connector Appliance

1. Installez deux appliances Connector ou plus dans votre emplacement de ressources.

   Pour plus d'informations sur la configuration de vos appliances Connector, consultez Appliance Connector pour Cloud Services.

2. Pour configurer Secure Private Access afin de se connecter aux applications Web locales à l'aide de KCD, configurez KCD en effectuant les étapes suivantes :

   a) Joignez votre appliance Connector à un domaine Active Directory.

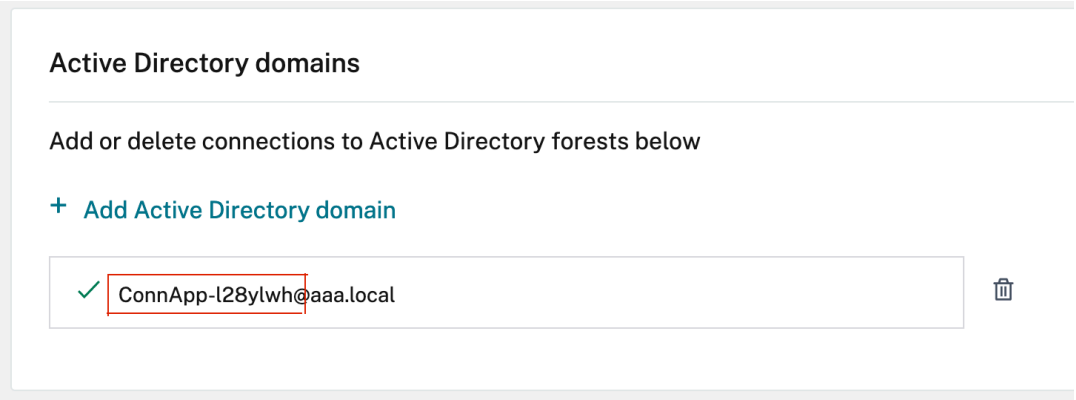
   Rejoindre une forêt Active Directory vous permet d'utiliser la délégation contrainte Kerberos (KCD) lors de la configuration de Secure Private Access, mais cela n'active pas les demandes d'identité ou l'authentification pour utiliser l'appliance Connector.

   - Connectez-vous à la page Web d'administration de Connector Appliance dans votre navigateur à l'aide de l'adresse IP fournie dans la console de Connector Appliance.
   - Dans la section **Domaines Active Directory**, cliquez sur **+ Ajouter un domaine Active Directory** .

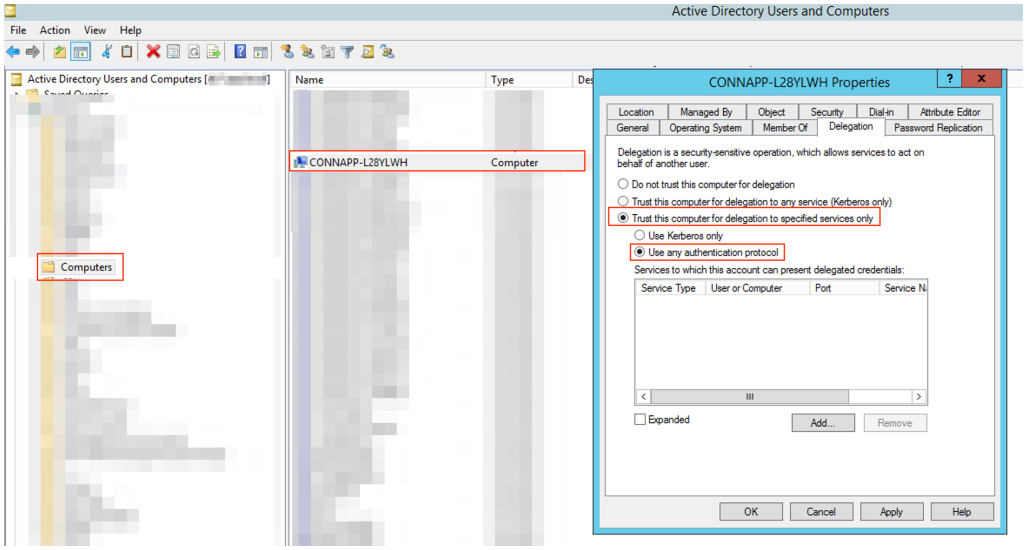
     Si votre page d'administration ne contient pas de section **Domaines Active Directory**, contactez Citrix pour demander votre inscription à l'aperçu.
   - Entrez le nom de domaine dans le champ **Nom de domaine**. Cliquez sur **Ajouter**.
   - Connector Appliance vérifie le domaine. Si la vérification réussit, la boîte de dialogue **Joindre Active Directory** s'ouvre.
   - Entrez le nom d'utilisateur et le mot de passe d'un utilisateur Active Directory qui dispose d'une autorisation de connexion pour ce domaine.
   - Connector Appliance suggère un nom de machine. Vous pouvez choisir de remplacer le nom suggéré et de fournir votre propre nom de machine, d'une longueur maximale de 15 caractères. Notez le nom du compte de la machine.

     Ce nom de machine est créé dans le domaine Active Directory lorsque Connector Appliance le rejoint.
   - Cliquez sur **Joindre**.

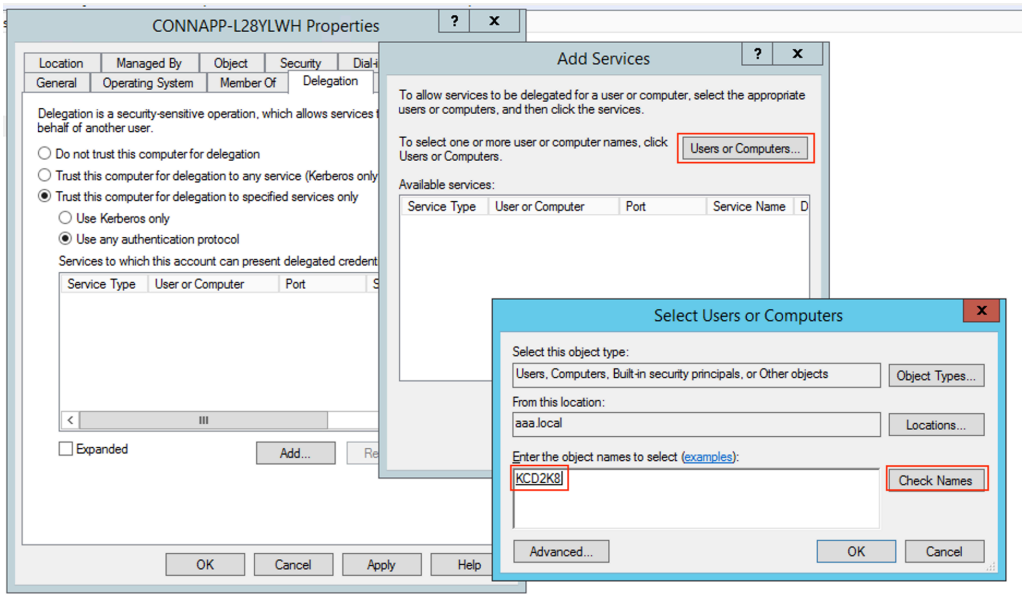
   b) Configurez la délégation de contraintes Kerberos pour un serveur Web sans équilibreur de charge.



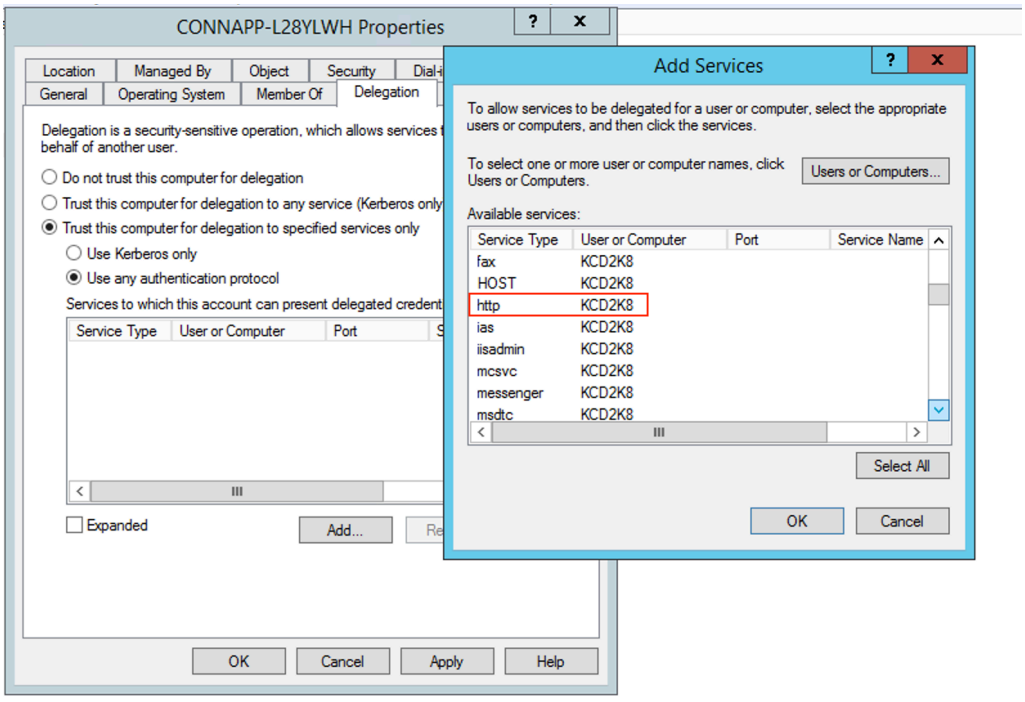
- Identifiez le nom de l'ordinateur du boîtier du connecteur Vous pouvez obtenir ce nom soit à partir de l'endroit où vous avez hébergé votre hébergement, soit simplement à partir de l'interface utilisateur du connecteur.
- Sur votre contrôleur Active Directory, recherchez l'ordinateur de l'appliance du connecteur.
- Accédez aux propriétés du compte d'ordinateur Connector Appliance, puis accédez à l'onglet **Délégation** .
- Choisissez **Faire confiance à l'ordinateur pour la délégation aux services spécifiés uniquement.** puis sélectionnez **Utiliser n'importe quel protocole d'authentification.**



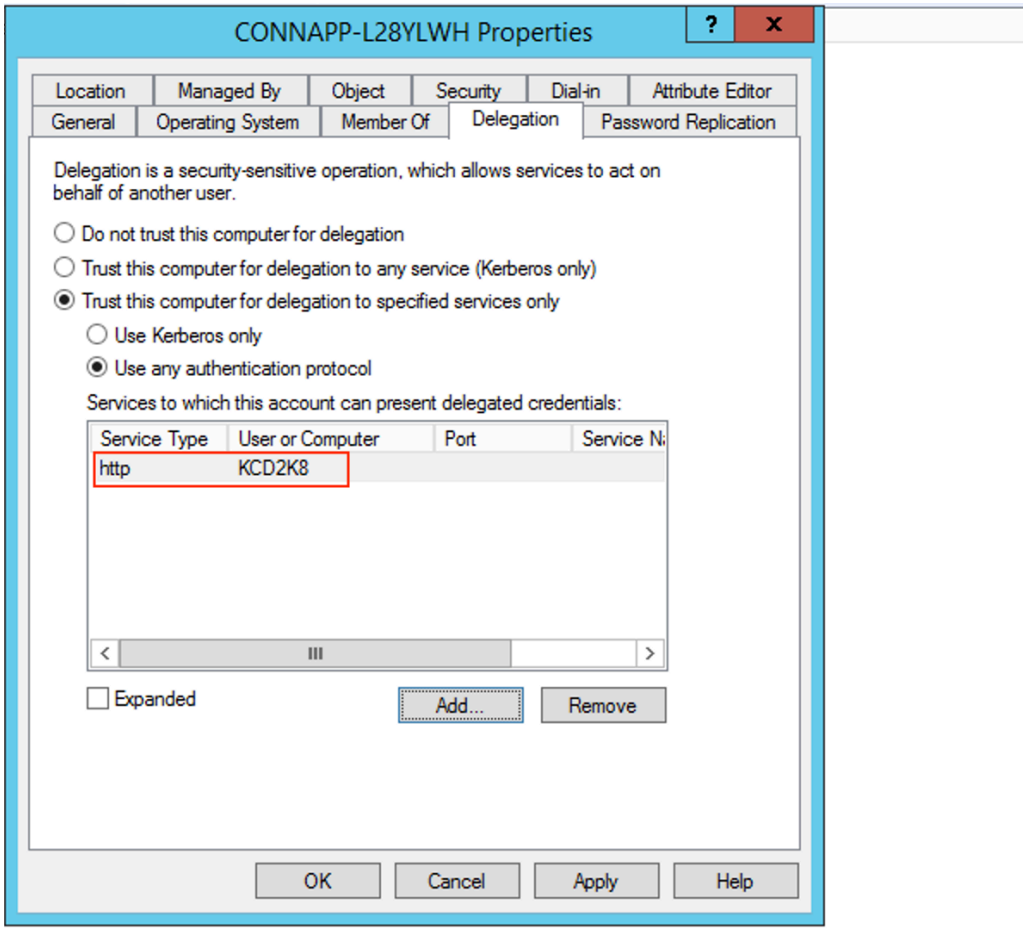
- Cliquez sur **Ajouter.**
- Cliquez sur **Utilisateurs ou Ordinateurs.**
- Entrez le nom de l'ordinateur du serveur Web cible, puis cliquez sur **Vérifier les noms.** Dans l'image précédente, **KCD2K8** est le serveur Web.



- cliquez sur **OK.**
- Sélectionnez le type de service **http.**



- Cliquez sur **OK**.
- Cliquez sur **Appliquer,** puis sur **OK**.



La procédure d'ajout de la délégation pour un serveur Web est ainsi terminée.

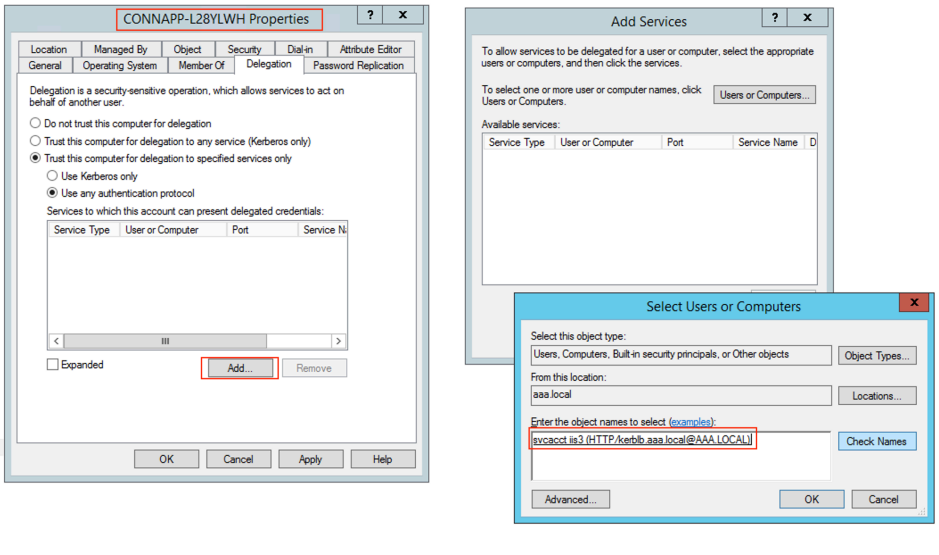
c) Configurez la délégation de contraintes Kerberos (KCD) pour un serveur Web derrière un équilibreur de charge.

- Ajoutez le SPN de l'équilibreur de charge au compte de service à l'aide de la `setspn` commande suivante.
  `setspn -S HTTP/<web_server_fqdn> <service_account>`

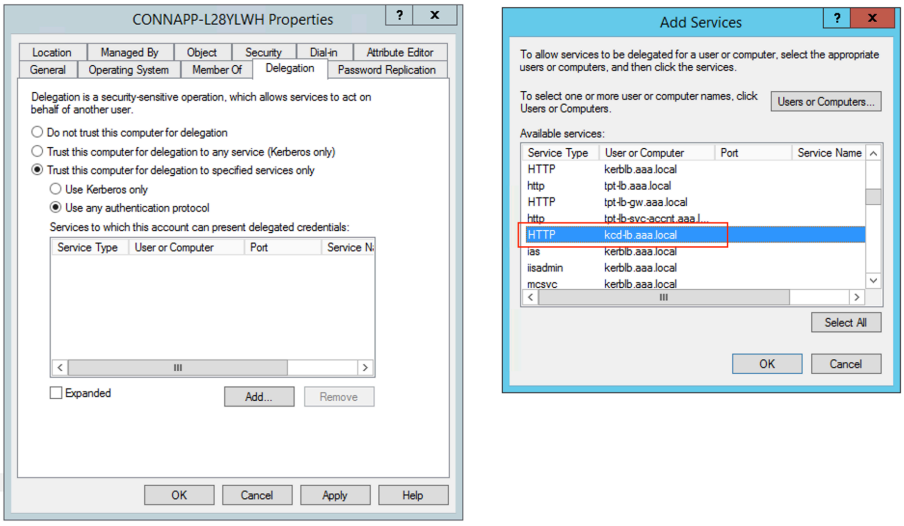
```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local

Registering ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=
local
        HTTP/kcd-lb.aaa.local
Updated object

C:\Windows\system32>_
```

- Confirmez les SPN du compte de service à l'aide de la commande suivante.
  `setspn -l <service_account>`

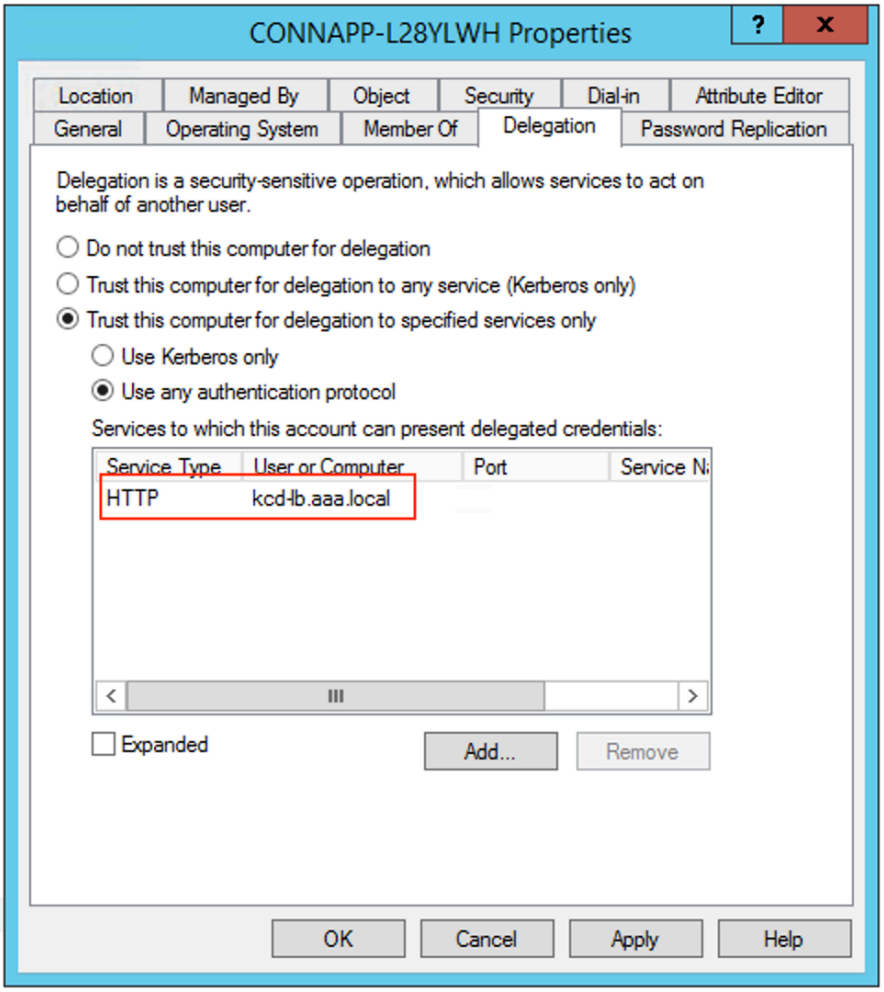
- Créez une délégation pour le compte d'ordinateur de l'appliance Connector.
  - Suivez les étapes pour *configurer la délégation de contraintes Kerberos pour le serveur Web* sans équilibreur de charge afin d'identifier la machine de l'autorité de certification et d'accéder à l'interface utilisateur de délégation.
  - Dans la **section Utilisateurs et ordinateurs**, sélectionnez le compte de service (par exemple, aaa \ svc_iis3).



  - Dans les services, sélectionnez l'entrée **ServiceType : HTTP** et Utilisateur ou Ordinateur : serveur Web (par exemple, `kcd-lb.aaa.local`)



- Cliquez sur **OK**.
- Cliquez sur **Appliquer,** puis sur **OK**.

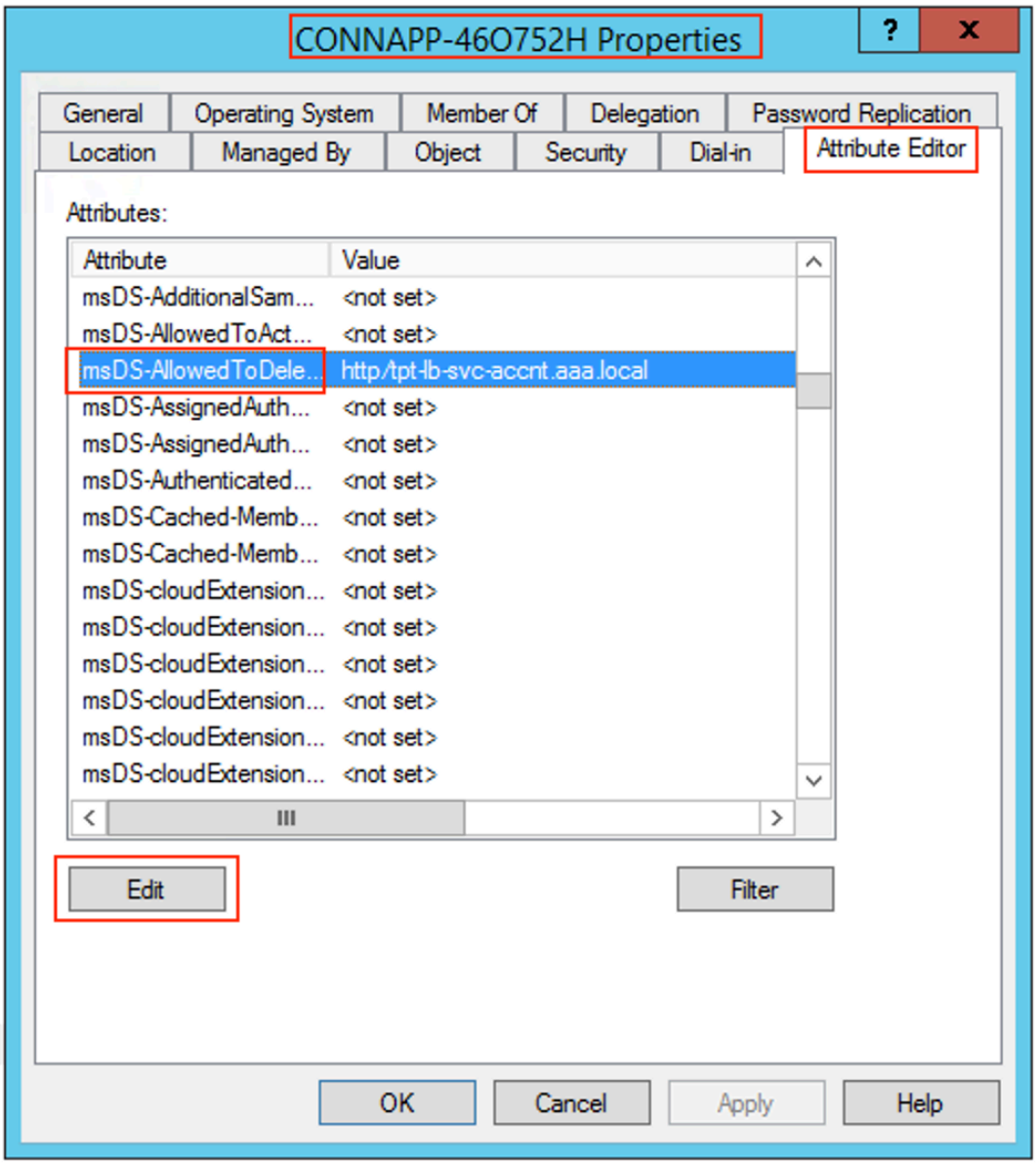


d) Configurez Kerberos Constrained Delegation (KCD) pour un compte de service géré par groupe.

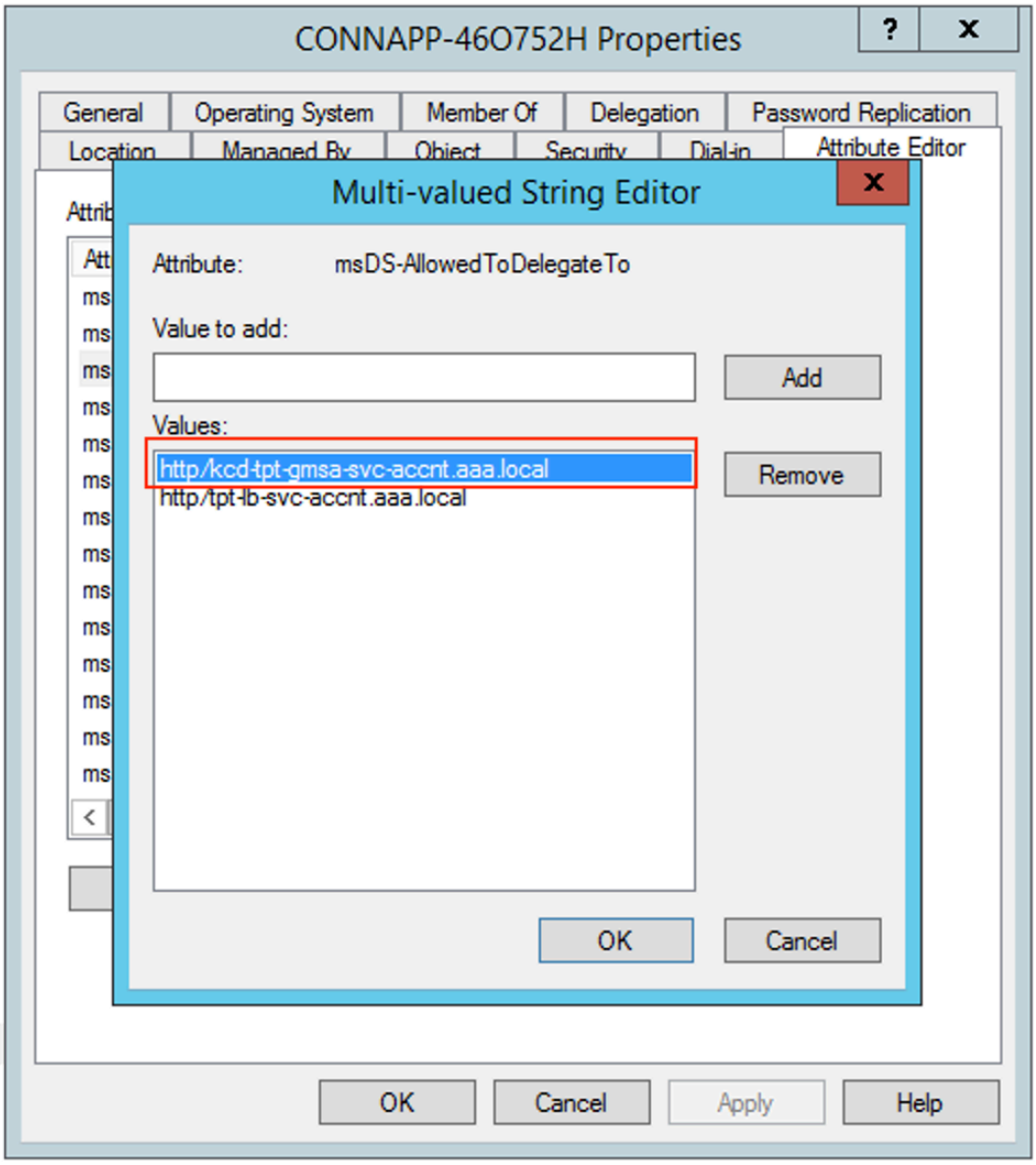
- Ajoutez le SPN au compte de service géré par le groupe si ce n'est pas déjà fait.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Confirmez le SPN à l'aide de la commande suivante.
  `setspn -l <group_manged_service_account>`

Comme le compte de service géré de groupe ne peut pas être affiché dans la `Users and Computers` recherche lors de l'ajout de l'entrée de délégation pour le compte d'ordinateur, vous ne pouvez pas ajouter la délégation pour un compte d'ordinateur en utilisant la méthode habituelle. Par conséquent, vous pouvez ajouter ce SPN en tant qu'entrée déléguée au compte d'ordinateur de l'autorité de certification en passant par l'éditeur d'attributs.

- Dans les propriétés de l'ordinateur Connector Appliance, accédez à l'onglet **Éditeur** d'attributs et recherchez l'`msDA-AllowedToDeleteTo` attribut.
- Modifiez le `msDA-AllowedToDeleteTo attribute`, puis ajoutez le SPN.



)



)

e) Migrez de NetScaler Gateway Connector vers Citrix Connector Appliance.

- Comme les SPN sont déjà définis sur compte de service lors de la configuration du connecteur de passerelle, vous n'avez pas besoin d'ajouter d'autres SPN pour le compte de service si aucune nouvelle application Kerberos n'est configurée. Vous pouvez afficher la liste de tous les SPN attribués au compte de service en suivant la commande et en les affectant en tant qu'entrées déléguées pour le compte d'ordinateur de l'autorité de certification.

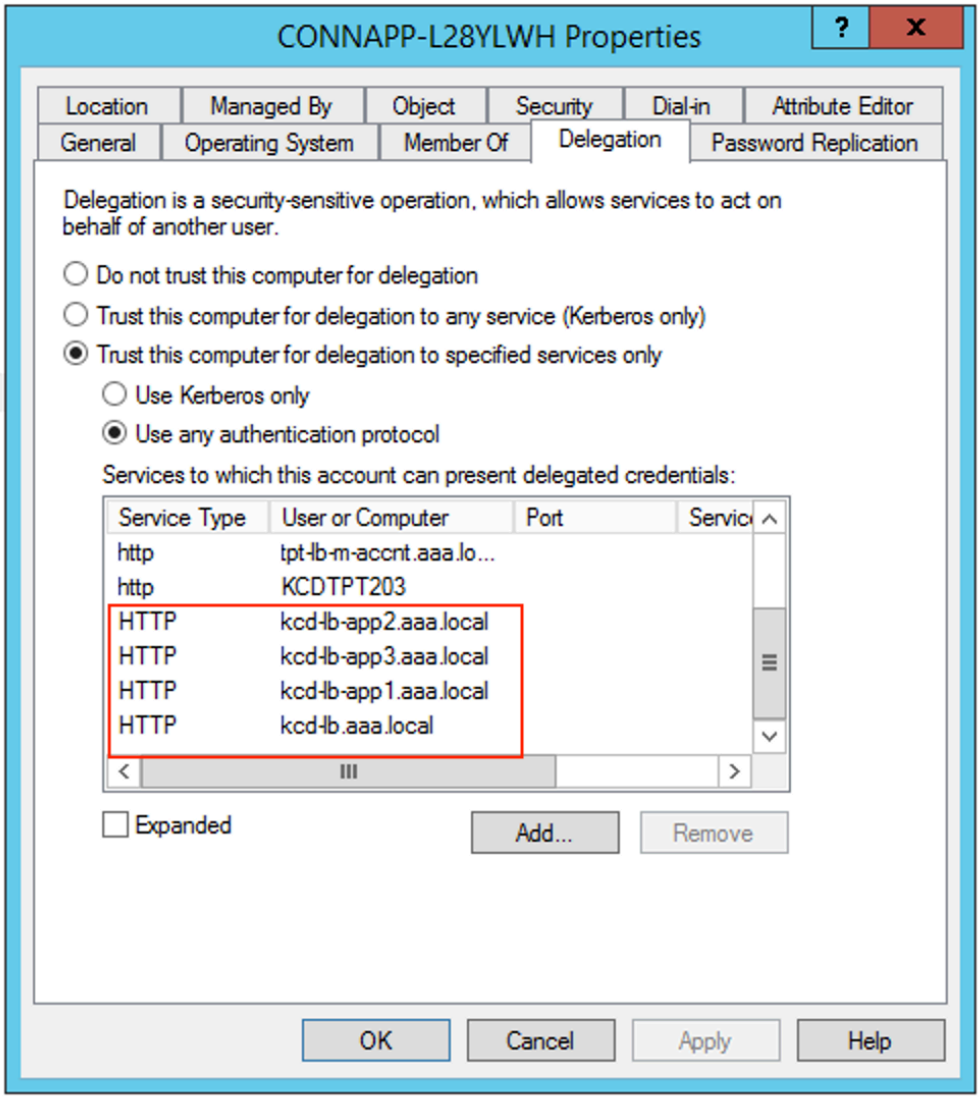
```
setspn -l <service_account>
```



```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

Dans cet exemple, les SPN (`kcd-lb.aaa.local`, `kcd-lb-app1.aaa.local`, `kcd-lb-app2.aaa.local`, `kcd-lb-app3.aaa.local`) sont configurés pour KCD.

- Ajoutez les SPN requis au compte d'ordinateur de l'appliance Connector en tant qu'entrée déléguée. Pour plus de détails, étape *Créer une délégation pour le compte d'ordinateur de l'appliance Connector*.



Dans cet exemple, le SPN requis est ajouté en tant qu'entrées déléguées pour le compte d'ordinateur de l'autorité de certification.

Remarque : Ces SPN ont été ajoutés au compte de service en tant qu'entrées déléguées lors de la configuration du connecteur de passerelle. Au fur et à mesure que vous quittez la délégation de compte de service, ces entrées peuvent être supprimées de l'onglet **Délégation** du compte de service.

f) Consultez la documentation Citrix Secure Private Access pour configurer le service Citrix Secure Private Access. Lors de la configuration, Citrix Cloud reconnaît la présence de vos appliances Connector et les utilise pour se connecter à votre emplacement de ressources.

- Démarrer avec Citrix Secure Private Access
- Configuration de Citrix Secure Private Access
- Appliance Connector pour Cloud Services
- Exigences en termes de connexion Internet
- Prise en charge des applications Web d'entreprise

Validation de votre configuration Kerberos

Si vous utilisez Kerberos pour l'authentification unique, vous pouvez vérifier que la configuration de votre contrôleur Active Directory est correcte sur la **page d'administration de l'Appliance Connector** . La fonctionnalité de **validation Kerberos** vous permet de valider une configuration en mode domaine uniquement Kerberos ou une configuration de délégation Kerberos contrainte (KCD).

1. Accédez à la **page d'administration de l'Appliance Connector** .
   a) À partir de la console de Connector Appliance de votre hyperviseur, copiez l'adresse IP dans la barre d'adresse de votre navigateur.
   b) Entrez le mot de passe que vous avez défini lors de l'enregistrement de votre Connector Appliance.
2. Dans le menu Admin en haut à droite, sélectionnez **Validation Kerberos**.
3. Dans la boîte de dialogue **Validation Kerberos**, choisissez le **mode de validation Kerberos**.
4. Spécifiez ou sélectionnez le **domaine Active Directory**.
   - Si vous validez une configuration en mode domaine uniquement Kerberos, vous pouvez spécifier n'importe quel domaine Active Directory.
   - Si vous validez une configuration de délégation Kerberos contrainte, vous devez sélectionner un domaine dans la liste des domaines de la forêt jointe.
5. Spécifiez le **FQDN du service**. Le nom du service par défaut est supposé être `http`. Si vous spécifiez « ordinateur.exemple.com », il est considéré comme identique à `http/computer.example.com`.

6. Spécifiez le **nom d'utilisateur**.
7. Si vous validez une configuration en mode domaine Kerberos uniquement, spécifiez le **mot de passe** correspondant à ce nom d'utilisateur.
8. Cliquez sur **Tester Kerberos**.

Si la configuration Kerberos est correcte, le message s'affiche `Successfully validated Kerberos setup`. Si la configuration Kerberos n'est pas correcte, un message d'erreur contenant des informations sur l'échec de la validation s'affiche.

Migrer Gateway Connector vers l'appliance Connector

December 27, 2023

NetScaler Gateway Connector est obsolète. Citrix recommande à ses clients d'utiliser les connecteurs NetScaler Gateway dans leur environnement afin de commencer à déployer l'Connector Appliance pour tous les cas d'utilisation de Secure Private Access qui étaient auparavant pris en charge par le connecteur NetScaler Gateway. Cette rubrique fournit des instructions sur la migration de Gateway Connector vers Connector Appliance.

Étapes générales pour migrer Gateway Connector vers Connector Appliance

1. Installez les dispositifs Connector en plus des connecteurs de passerelle dans le même emplacement de ressources.
2. Arrêtez les connecteurs de passerelle et testez la connectivité des applications Web existantes. Vérifiez si l'application Web hébergée sur le même emplacement de ressources est accessible.
3. Supprimez NetScaler Gateway Connector une fois les tests terminés.

Pour installer l'appliance Connector

Procédez comme suit pour installer une appliance Connector.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche de l'écran, sélectionnez **Emplacements des ressources**.
3. Cliquez sur l'icône plus en regard de Connector Appliance pour l'emplacement de ressources auquel vous souhaitez ajouter un dispositif Connector.
4. Sélectionnez l'hyperviseur et cliquez sur **Download Image (Télécharger l'image**).
5. Téléchargez et installez l'appliance Connector sur votre hyperviseur.

6. Connectez-vous à l'interface utilisateur Web (adresse IP fournie sur la console de l'hyperviseur) et configurez un proxy si nécessaire.
7. Cliquez sur le bouton **Enregistrer** et obtenez le code court.
8. Collez le code court dans l'interface utilisateur Citrix Cloud utilisée lors du téléchargement de l'appliance Connector (étape 5).

   L'appliance Connector est enregistrée.

Pour obtenir des instructions détaillées, consultez Appliance Connector pour les services cloud.

FAQ

- Comment télécharger l'appliance Connector ?

  Téléchargez l'appliance Connector.
- Comment installer l'appliance Connector ?

  Installation de l'appliance Connector.
- Comment enregistrer l'appliance Connector ?

  Enregistrement de l'appliance Connector.
- Quelles sont les exigences de connectivité pour l'appliance Connector ?

  Exigences de connectivité Internet de l'appliance Connector.
- Quelle est la configuration système requise pour l'appliance Connector ?

  Configuration système requise pour Connector Appliance
- Comment l'appliance Connector est-elle mise à jour ?

  Mises à jour des appliances

Migration des contrôles de sécurité des applications et des stratégies d'accès vers le nouveau cadre de stratégie d'accès

December 27, 2023

Citrix a apporté des modifications à l'activation de l'accès aux applications dans le produit. Auparavant, les applications devaient être abonnées aux utilisateurs ou aux groupes d'utilisateurs dans la section **Applications > Abonnés aux applications** de l'assistant pour permettre l'accès. À l'avenir,

au moins une stratégie d'accès est requise pour permettre l'accès aux applications. Lors de la création des stratégies, la condition **Utilisateurs ou groupes** est une condition obligatoire à remplir pour accorder l'accès aux applications aux utilisateurs. Pour plus de détails, voir Création de stratégies d'accès.

En outre, la section **Sécurité renforcée** de la configuration de l'application est obsolète. Vous pouvez désormais appliquer des contrôles de sécurité granulaires tels que la restriction du presse-papiers, la restriction de téléchargement, les restrictions d'impression, en plus d'options avancées telles que l'ouverture d'une application dans le navigateur distant à partir des stratégies d'accès Grâce à ce changement, les clients peuvent appliquer une sécurité adaptative basée sur le contexte tel que les utilisateurs, l'emplacement, l'appareil et le risque.

Pour migrer les contrôles de sécurité et les stratégies d'accès de vos applications vers le nouveau cadre de stratégie d'accès et pour éviter tout temps d'arrêt dans l'accès aux applications, Citrix a apporté les modifications requises. Par conséquent, vous remarquerez peut-être certains changements dans votre liste de stratégies, tels que les suivants :

- Nouvelles stratégies créées
- Une seule stratégie divisée en plusieurs stratégies
- Noms de stratégie préfixés par <`System generated policy - App name`>

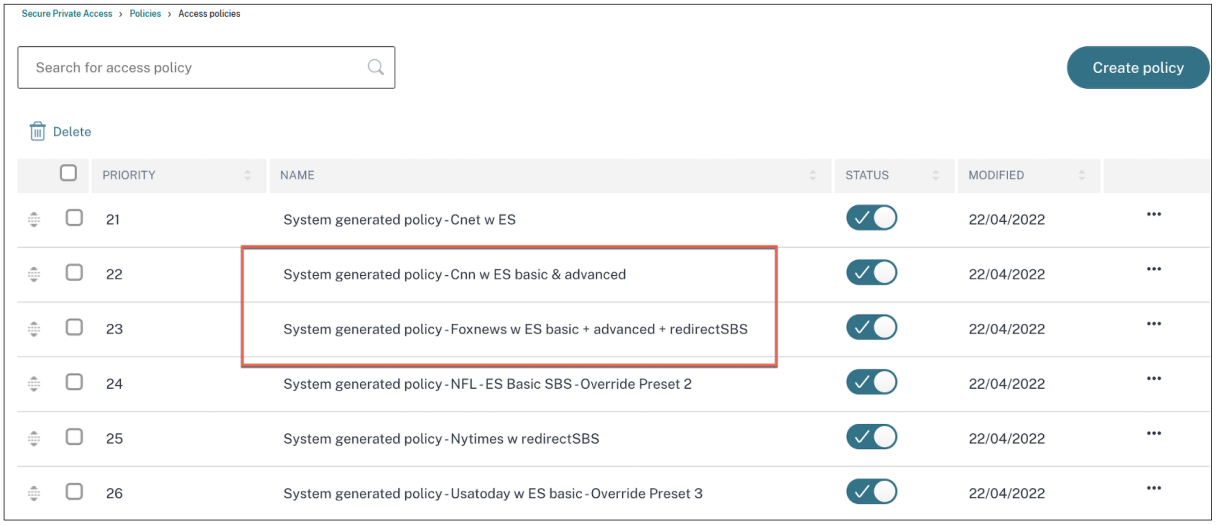
> **Remarque :**
>
> Si aucun utilisateur ou groupe n'a été ajouté aux applications, aucune nouvelle stratégie n'est créée.

Le tableau suivant résume les modifications.

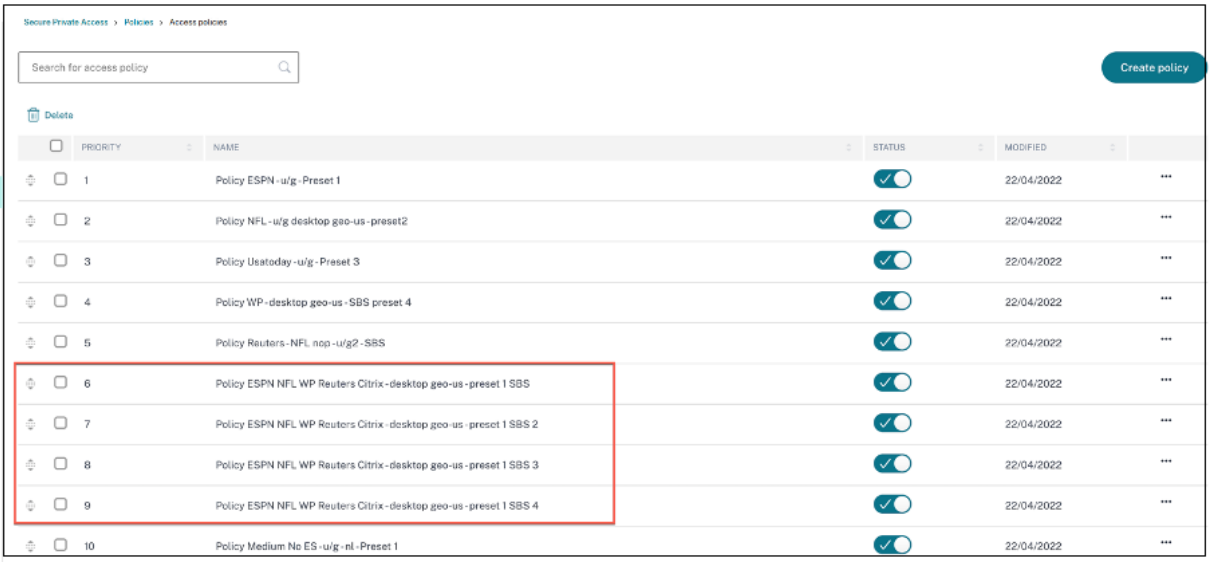
Si vous aviez configuré un…	Alors…
Application sans aucune condition de sécurité renforcée	Une nouvelle stratégie est créée avec des utilisateurs et des groupes comme condition obligatoire. Les utilisateurs ou les groupes sont dérivés des stratégies d'accès. L'action est définie sur **Autoriser l'accès**.

Si vous aviez configuré un…	Alors…
Application avec conditions de sécurité améliorées	Une nouvelle stratégie est créée avec des utilisateurs et des groupes comme condition obligatoire. Les utilisateurs ou les groupes sont dérivés des stratégies d'accès. L'action définie est **Autoriser avec restriction.** Basé sur la condition de sécurité au niveau de l'application configurée précédemment. Les restrictions de sécurité correspondantes sont sélectionnées lors de la création de la stratégie. Les stratégies migrées sont préfixées par <System generated policy - App name>.
Stratégie d'accès avec préréglages	Si une condition de groupe d'utilisateurs est déjà sélectionnée pour la stratégie, une nouvelle stratégie est créée telle quelle et les conditions de sécurité correspondantes sont sélectionnées dans la stratégie d'accès en fonction des préréglages.
Stratégie d'accès sans condition d'utilisateur ou de groupe	Les utilisateurs ou les groupes étant une condition obligatoire pour accéder aux applications, une stratégie unique configurée pour plusieurs applications est désormais divisée en plusieurs stratégies, car chaque application peut avoir un ensemble différent d'utilisateurs ou de groupes. Les utilisateurs ou les groupes sont dérivés des stratégies d'accès. Pour chaque stratégie, les utilisateurs ou les groupes sont définis comme une condition obligatoire.

La figure suivante présente des exemples de noms de stratégie préfixés par <System generated policy - App name>.



La figure suivante montre un exemple de stratégie unique divisée en plusieurs stratégies.



Lancer une application configurée - workflow utilisateur

December 27, 2023

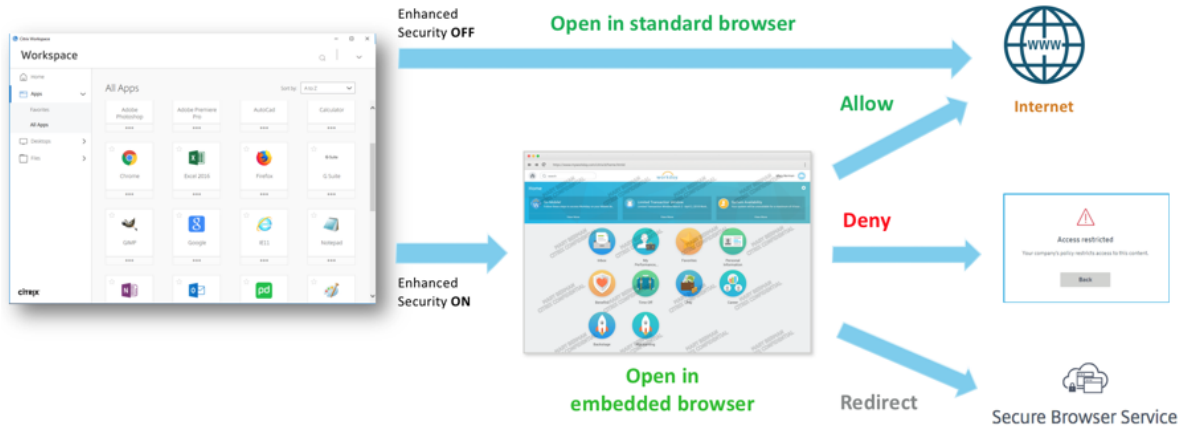
En tant qu'utilisateur, vous devez effectuer les opérations suivantes :

1. Téléchargez l'application Citrix Workspace depuis https://www.citrix.com/downloads. Dans la liste **Find Downloads** (Recherche de téléchargements), sélectionnez **Application Citrix Workspace**.
2. Connectez-vous et recherchez vos applications SaaS. Cliquez sur l'application pour la lancer.

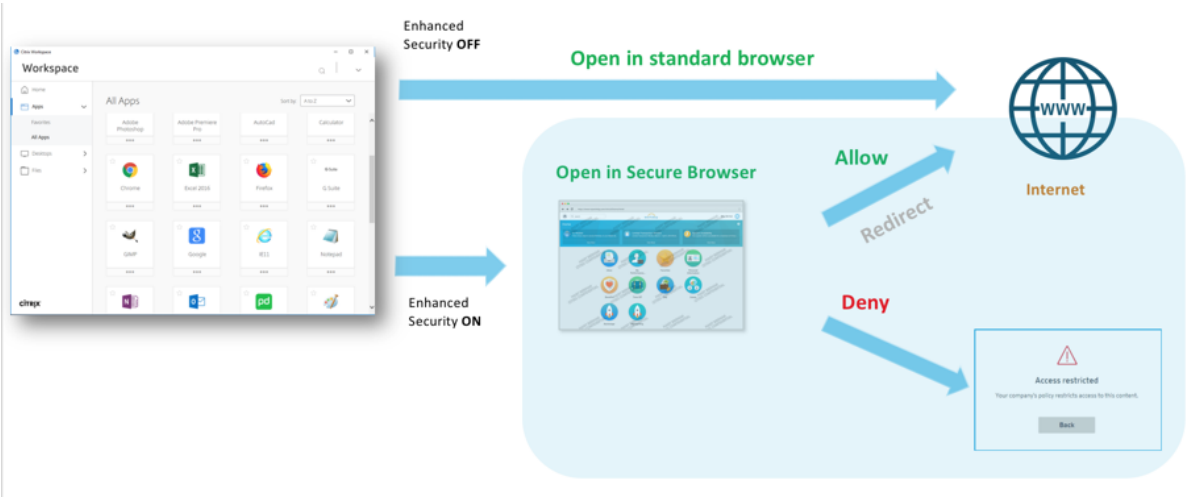
Vous pouvez désormais utiliser l'application SaaS depuis l'application Citrix Workspace ou depuis le portail Web de Citrix Workspace.

Selon les paramètres configurés par l'administrateur, vos applications SaaS s'ouvrent à l'aide du moteur de navigateur de l'application Workspace ou vous êtes redirigé vers un navigateur sécurisé.

Le diagramme suivant montre le flux de haut niveau de l'application Citrix Workspace.



Le diagramme suivant illustre le flux de haut niveau du portail Web de Citrix Workspace.



Découvrir les domaines ou les adresses IP auxquels accèdent les utilisateurs finaux

October 21, 2024

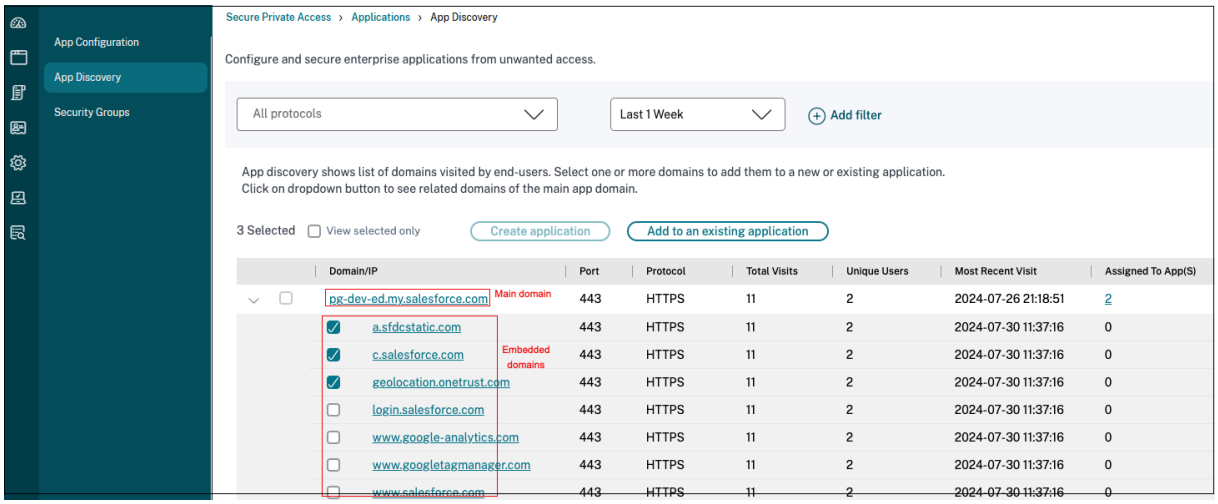
La fonctionnalité de découverte d'applications aide un administrateur à obtenir une visibilité sur les applications externes et internes (applications HTTP/HTTPS et TCP/UDP) auxquelles une organisation

accède. Cette fonctionnalité découvre et répertorie tous les domaines/adresses IP, publiés ou non publiés. Ainsi, les administrateurs peuvent voir quels domaines/adresses IP sont consultés, par qui, et décider s'ils souhaitent les publier en tant qu'applications, en fournissant l'accès à ces utilisateurs.

La fonctionnalité de découverte d'applications fournit les capacités suivantes aux administrateurs :

- Fournit une visibilité sur les domaines/adresses IP internes ou externes auxquels accèdent les utilisateurs finaux.
- Fournit une visibilité complète sur tous les types d'applications accessibles (HTTP, HTTPS, TCP et UDP). Toutes les méthodes d'accès sont prises en charge, c'est-à-dire l'accès via Citrix Enterprise Browser, Secure Access Agent, Direct Access ou Workspace for Web.
- Affiche les domaines/adresses IP publiés ou non publiés auxquels accèdent les utilisateurs finaux.
- Affiche à la fois le domaine principal et ses domaines intégrés sous-jacents qui doivent être configurés en tant que domaines associés lors de la publication des applications pour l'accès via Citrix Enterprise Browser.
- Affiche les domaines intégrés dans une structure arborescente. Les administrateurs peuvent cliquer sur le signe de développement (**>**) en ligne avec le domaine principal pour afficher les domaines intégrés.
- Permet aux administrateurs de créer de nouvelles applications ou d'ajouter ces domaines à une application existante si un domaine principal ou un domaine intégré (HTTP/HTTPS) ou l'adresse IP de destination (TCP/UDP) n'est pas associé à une application.

La figure suivante affiche un exemple de page **de découverte d'application** . La page **Découverte d'application** permet de filtrer les domaines en fonction du protocole (HTTP/HTTPS, TCP/UDP) et de l'adresse de domaine/IP et des numéros de port. Il affiche également les domaines non publiés (non attribués à une application) auxquels accèdent les utilisateurs finaux. Vous pouvez voir un domaine principal avec une liste déroulante de domaines intégrés en dessous. Ces domaines doivent être configurés comme domaines associés lors de la publication de l'application.



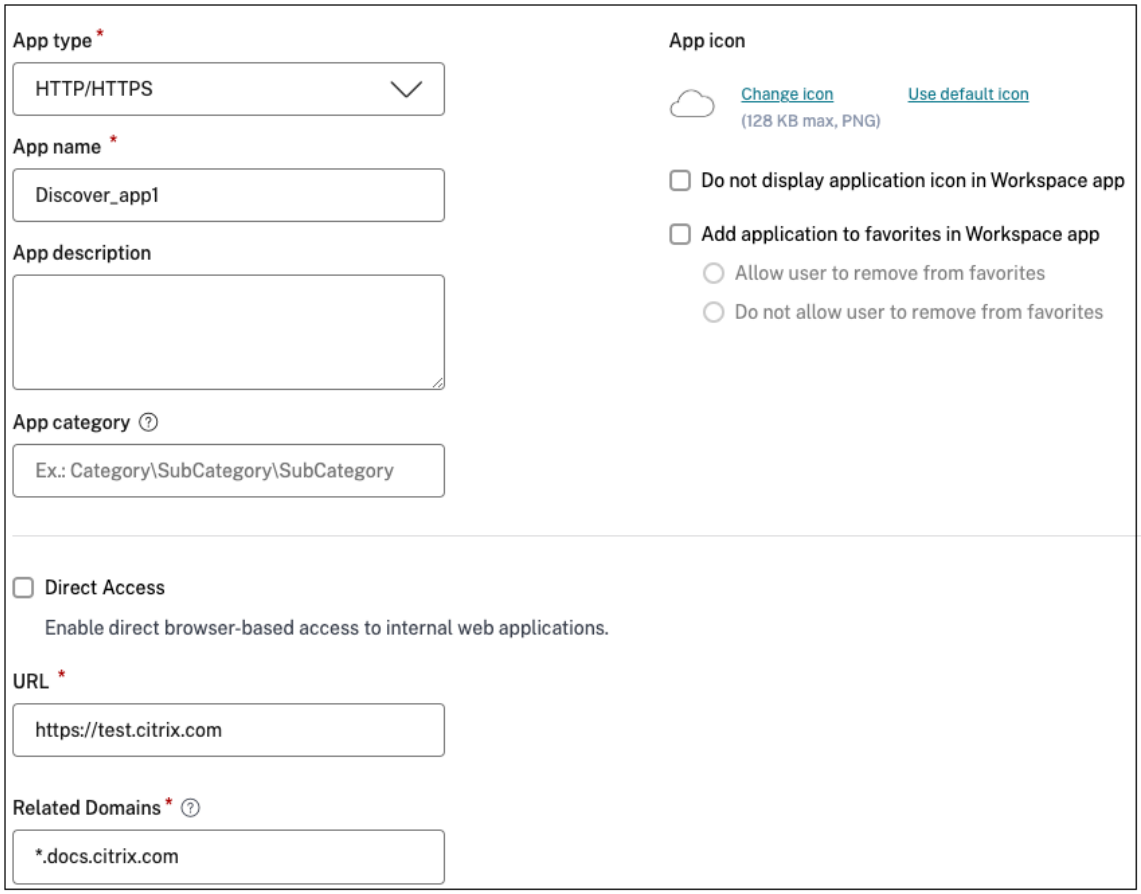
> **Remarque**
>
> - Les domaines intégrés sont regroupés sous le domaine principal uniquement pour les applications HTTP/HTTPS accessibles via Citrix Enterprise Browser. Les domaines TCP/UDP ne sont pas regroupés sous un domaine principal.
> - Le regroupement de domaines intégrés n'est disponible que pour les applications accessibles à partir de Citrix Enterprise Browser (v119 et versions ultérieures).

Découverte d'applications pour les domaines internes dans un nouvel environnement

La fonctionnalité de découverte d'applications peut être utilisée si vous configurez un nouvel environnement d'accès privé sécurisé et souhaitez avoir une visibilité sur les applications à configurer. Cette fonctionnalité détecte et répertorie tous les domaines/adresses IP auxquels vos utilisateurs finaux accèdent afin que vous puissiez les configurer en tant qu'applications. Suivez les étapes suivantes pour activer la fonctionnalité de découverte d'applications lorsque vous configurez votre environnement Secure Private Access :

- Pour découvrir des applications Web internes, configurez une application dans Secure Private Access et spécifiez le domaine associé au caractère générique qui appartient au domaine/sous-domaine des applications que vous souhaitez découvrir.

  Par exemple, si vous souhaitez découvrir toutes les applications avec le domaine citrix.com, créez une application avec un domaine générique associé comme `*.citrix.com`. Pour permettre l'achèvement de la configuration de l'application, ajoutez n'importe quelle URL de test comme section URL principale de l'application Web.

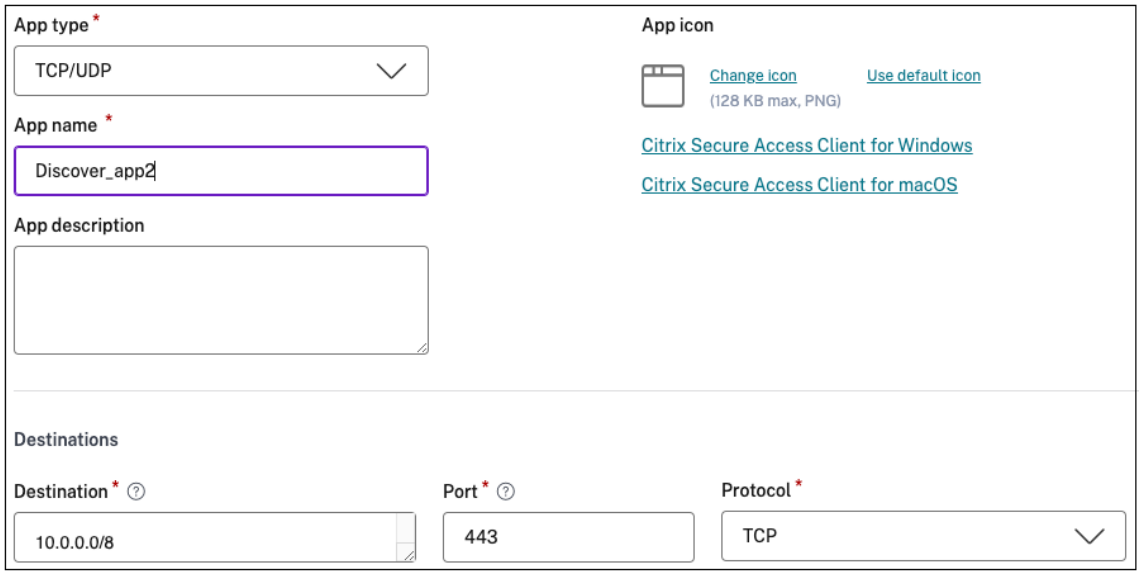


URL de l'application Web : `https://test.citrix.com/` Domaine associé : `*.citrix.com`

- Pour les applications TCP/UDP internes, configurez une application dans Secure Private Access et spécifiez le sous-réseau ainsi que le protocole TCP/UDP et la plage de ports (saisissez * pour inclure la plage entière). Cela permet de découvrir toutes les applications TCP et UDP à partir de l'agent Citrix Secure Access. Par exemple, si vous souhaitez découvrir toutes les applications du sous-réseau 10.0.0.0/8, configurez l'application avec les détails suivants : Exemple : 10.0.0.0/8 :

  Port: (*)

  Protocole : TCP



- Une fois les applications créées, vous devez également définir les utilisateurs autorisés à accéder aux applications avec les domaines et sous-réseaux IP configurés. Créez une politique d'accès et attribuez les utilisateurs auxquels vous souhaitez autoriser l'accès aux noms de domaine complets/adresses IP configurés dans les applications créées. Il peut s'agir d'un ensemble initial d'utilisateurs de test ou d'un nombre limité d'utilisateurs auxquels vous souhaitez donner accès initialement.
- Après avoir créé les applications et les stratégies d'accès correspondantes, les utilisateurs peuvent continuer à accéder aux applications depuis l'application Citrix Workspace et accéder à différents domaines. Toutes les adresses FQDN/IP auxquelles accèdent les utilisateurs finaux commencent à s'afficher sur la page Découverte d'applications.

> **Remarque**
>
> - Une fois que vous avez découvert et identifié la plupart des applications en quelques jours/semaines, nous vous recommandons de supprimer les applications initialement créées afin que l'accès plus large donné via les domaines génériques et les sous-réseaux IP puisse être fermé, et que seules les URL d'application et les adresses IP spécifiques découvertes soient autorisées à accéder via les nouvelles applications.
> - Ajoutez le préfixe `Discover` dans le nom de l'application pour indiquer qu'il s'agit d'une configuration d'application spéciale permettant d'activer la surveillance et la création de rapports de découverte. Cette dénomination vous aide à identifier la suppression des domaines génériques ou des sous-réseaux IP ou des deux afin que vous puissiez réduire la zone d'accès globale de l'application aux seuls noms de domaine complets et combinaisons IP/port spécifiques plus tard dans les semaines ou dans un mois.
> - Pour accéder aux applications TCP/UDP, les utilisateurs doivent utiliser l'agent Citrix Secure Access. L'accès aux applications à partir de différentes méthodes d'accès est surveillé en

> fonction de la configuration des domaines et des sous-réseaux des applications et signalé dans la page **App Discovery** .
> - Même après avoir supprimé les applications découvertes, cette fonctionnalité continue de découvrir les domaines/adresses IP auxquels vos utilisateurs accèdent. Ainsi, à tout moment, vous pouvez revenir à la page **App Discovery** pour voir à quoi vous accédez et si de nouveaux domaines/adresses IP ont été découverts et doivent être configurés en tant qu'applications.

Pour plus de détails sur l'ajout de domaines, de noms de domaine complets ou d'adresses IP, consultez les rubriques suivantes.

- Prise en charge des applications Web d'entreprise
- Prise en charge de l'application Software as a Service
- Prise en charge des applications client-serveur

Créer une application à partir de la page de découverte d'applications

Pour créer une application pour des domaines intégrés ou des domaines non publiés à partir de la page **Découverte d'applications** , procédez comme suit :

1. Accédez à **Applications > Découverte d'applications**.
2. Sélectionnez un domaine dans la liste. Si le domaine contient des domaines intégrés, cliquez sur le signe de développement (**>**) en ligne avec le domaine principal et sélectionnez les domaines intégrés.

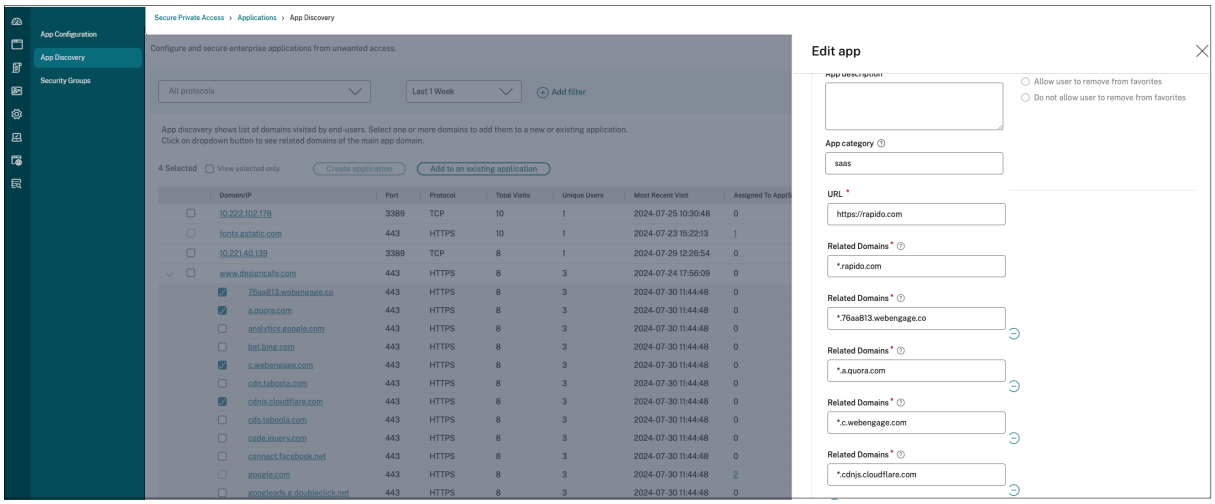
> **Remarque**
>
> - Vous ne pouvez pas sélectionner des domaines appartenant à des protocoles différents pour créer une application. Un message d'erreur s'affiche lorsque vous sélectionnez des domaines appartenant à des protocoles différents.
> - Si un domaine est déjà associé à une application, vous ne pouvez pas sélectionner à nouveau ce domaine pour créer une application. La case à cocher correspondant à ce domaine apparaît grisée et lorsque vous passez la souris sur la case à cocher, une info-bulle apparaît.
> - Vous ne pouvez pas sélectionner et ajouter des domaines intégrés regroupés sous différents domaines principaux à une application. La fonctionnalité de découverte d'applications permet uniquement d'ajouter des domaines intégrés regroupés sous un seul domaine principal à une application. Un message d'erreur s'affiche si des domaines intégrés provenant de différents domaines principaux sont sélectionnés et ajoutés à la même application.

1. Cliquez sur **Créer une application**. Pour plus de détails sur la création d'une application, voir Prise en charge des applications Web d'entreprise, Prise en charge des applications SaaSet Prise en charge des applications client-serveur](/en-us/citrix-secure-private-access/service/spa-support-for-client-server-apps).

Mettre à jour une application existante

Pour ajouter un domaine à une application existante, sélectionnez le domaine dans la liste. Si le domaine contient des domaines intégrés, cliquez sur le signe de développement (**>**) en ligne avec le domaine principal et sélectionnez les domaines intégrés.

1. Sélectionnez le domaine intégré qui doit être ajouté à une application.
2. Cliquez sur **Ajouter à une application existante**.
3. Dans **Applications**, sélectionnez l'application à laquelle vous souhaitez ajouter ces domaines.
4. Cliquez sur **Obtenir les détails de l'application**.
5. Le champ **Domaines associés** affiche tous les domaines intégrés que vous avez sélectionnés précédemment sur des lignes séparées.
6. Cliquez sur **Terminer**.

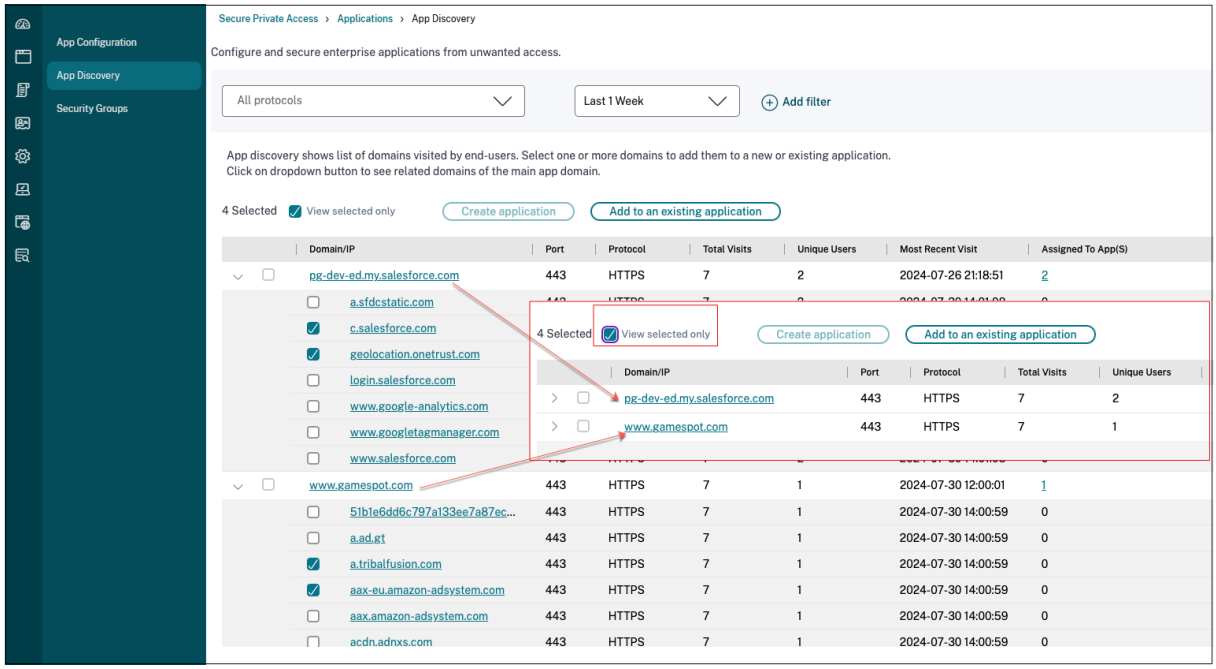


> **Remarque**
>
> - Vous ne pouvez ajouter qu'une adresse IP de destination TCP/UDP à une application TCP/UDP existante. Le champ Applications répertorie uniquement les applications TCP/UDP configurées dans le système.
> - Vous pouvez sélectionner une application HTTP/HTTPS ou TCP/UDP existante pour ajouter des domaines (principaux, à entrée unique ou intégrés) dont le protocole est HTTP/HTTPS.
> - Vous ne pouvez pas sélectionner un domaine déjà associé à une application.

Afficher tous les domaines intégrés sélectionnés

Après avoir sélectionné les domaines, vous pouvez cliquer sur la case à cocher **Afficher uniquement la sélection** et procéder à la création ou à la mise à jour de l'application. De plus, si la liste des noms de domaine complets/adresses IP sur la page de découverte d'applications s'étend sur plusieurs pages,

vous pouvez utiliser la case à cocher **Afficher uniquement la sélection** pour afficher tous les domaines principaux et intégrés que vous avez sélectionnés pour créer ou mettre à jour l'application. Tous les domaines principaux des domaines intégrés sélectionnés sont affichés lorsque cette case à cocher est sélectionnée.



Limitations connues

- Bien que les options **Créer une application** et **Ajouter à une application existante** soient disponibles dans le tableau de bord Secure Private Access (graphique**Principales applications découvertes par nombre total de visites**), il est recommandé de créer ou de mettre à jour une application à partir de l'onglet **Découverte d'applications** (**Applications > Découverte d'applications**). Cela est dû au fait que, lors de l'ajout ou de la mise à jour d'une application depuis le tableau de bord et que vous annulez l'opération, la page est rechargée et par conséquent, tous les paramètres sont réinitialisés.
- Parfois, vous remarquerez peut-être le signe d'extension (>) par rapport à un domaine principal, mais les domaines intégrés ne sont pas récupérés pour ce FQDN spécifique. Ce problème peut survenir dans les cas suivants :
  - Erreur lors du chargement de la page Web principale en raison de certaines restrictions d'accès pour les utilisateurs.
  - Une erreur empêchant le chargement de la page Web.
  - Mise en cache des ressources de domaine intégrées par Citrix Enterprise Browser, ce qui empêche la récupération des domaines intégrés à partir de la source.

Meilleures pratiques de configuration des applications Web et SaaS

June 19, 2024

L'accès aux applications publiées et non publiées dépend des applications et des stratégies d'accès configurées dans le service Secure Private Access.

Accès aux applications publiées et non publiées via Secure Private Access

- **Accès aux applications Web publiées et aux domaines associés :**
  - Lorsqu'un utilisateur accède à un nom de domaine complet associé à une application Web publiée, l'accès n'est autorisé que si une stratégie d'accès est configurée explicitement avec l'action **Autoriser** ou **Autoriseravec restrictions** pour l'utilisateur.

    > **Remarque :**
    >
    > Il est recommandé de faire en sorte que plusieurs applications ne partagent pas le même domaine d'URL d'application ou des domaines associés pour obtenir une correspondance exacte. Si plusieurs applications partagent le même domaine URL d'application ou des domaines associés, l'accès est fourni en fonction de la correspondance exacte du FQDN et de la hiérarchisation des stratégies. Pour plus de détails, consultez la section Correspondance et hiérarchisation des stratégies d'accès.

  - Si aucune stratégie d'accès ne correspond à l'application publiée ou si aucune application n'est associée à une stratégie d'accès, l'accès à l'application est refusé par défaut. Pour plus de détails sur les stratégies d'accès, voir Stratégies d'accès.
- **Accès à des applications Web internes non publiées et à des URL Internet externes :**

  Pour activer la sécurité Zero Trust, Secure Private Access refuse l'accès aux applications Web internes ou aux URL intranet qui ne sont pas associées à une application et pour lesquelles aucune stratégie d'accès n'est configurée pour l'application. Pour autoriser l'accès à des utilisateurs spécifiques, assurez-vous qu'une stratégie d'accès est configurée pour vos applications Web intranet.

  Pour toute URL qui n'est pas configurée en tant qu'application dans Secure Private Access, le trafic est directement dirigé vers Internet.
  - Dans de tels cas, l'accès aux domaines URL des applications Web de l'intranet est acheminé directement et l'accès est donc refusé (sauf si l'utilisateur se trouve déjà dans l'intranet).

- Pour les URL Internet non publiées, l'accès dépend des règles configurées pour les applications non autorisées, si elles sont activées. Par défaut, cet accès est autorisé dans Secure Private Access. Pour plus de détails, voir Configurer les règles pour les sites Web non autorisés.

Correspondance et hiérarchisation des stratégies d'accès

Secure Private Access effectue les opérations suivantes lorsqu'une application correspond à la stratégie d'accès :

1. Fait correspondre le domaine auquel vous accédez au domaine de l'URL de l'application ou à des domaines associés pour obtenir une correspondance exacte.
2. Si une application Secure Private Access configurée avec un FQDN à correspondance exacte est trouvée, Secure Private Access évalue toutes les stratégies configurées pour cette application.
   - Les stratégies sont évaluées par ordre de priorité jusqu'à ce que le contexte utilisateur corresponde. L'action (autoriser/refuser) est appliquée à la première stratégie correspondante dans l'ordre de priorité.
   - Si aucune stratégie ne correspond, l'accès est refusé par défaut.
3. Si aucune correspondance exacte de nom de domaine complet n'est trouvée, Secure Private Access fait correspondre le domaine en fonction de la correspondance la plus longue (telle qu'une correspondance de caractères génériques) pour rechercher les applications et les stratégies correspondantes.

   Exemple 1 : considérez les configurations d'applications et de stratégies suivantes :

Application	URL de l'application	Domaine associé
Intranet	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

Nom de la stratégie	Priorité	Applications utilisateur et associées
Stratégie A	Élevé	Eng-User5 (Intranet)
Stratégie B	Faible	Utilisateur RH 4 (Wiki)

Si `HR-User4` accède à `app.intranet.local`, voici ce qui se passe :

a) Secure Private Access recherche toutes les stratégies présentant une correspondance exacte avec le domaine auquel vous accédez, `app.intranet.local` dans le cas présent.
b) Secure Private Access trouve `PolicyA`et vérifie si les conditions correspondent.
c) Étant donné que les conditions ne correspondent pas, Secure Private Access s'arrête là et ne vérifie pas les correspondances de caractères génériques, même si la stratégie `PolicyB` aurait correspondu (puisque `app.intranet.local` correspond au domaine associé de l'application Wiki `*.intranet.local`) et aurait autorisé l'accès.
d) L'accès à l'application Wiki `HR-User4` est donc refusé.

Exemple 2 : considérez la configuration des applications et des stratégie suivante dans laquelle le même domaine est utilisé dans plusieurs applications :

Application	URL de l'application	Domaine associé
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

Nom de la stratégie	Priorité	Applications utilisateur et associées
Stratégie A	Élevé	Eng-User5 (App1)
Stratégie B	Faible	Utilisateur RH 7 (App 2)

Lorsque l'utilisateur `Eng-User5` accède à `app.intranet.local`, App1 et App2 correspondent en raison de la correspondance exacte du FQDN et, par conséquent, l'accès de l'utilisateur `Eng-User5` via `PolicyA` est autorisé.

Cependant, si le domaine associé d'App1 avait été `*.intranet.local`, l'accès à `Eng-User5` aurait été refusé, car `app.intranet.local` aurait correspondu exactement à la stratégie `PolicyB`, qui interdit l'accès de l'utilisateur `Eng-User5`.

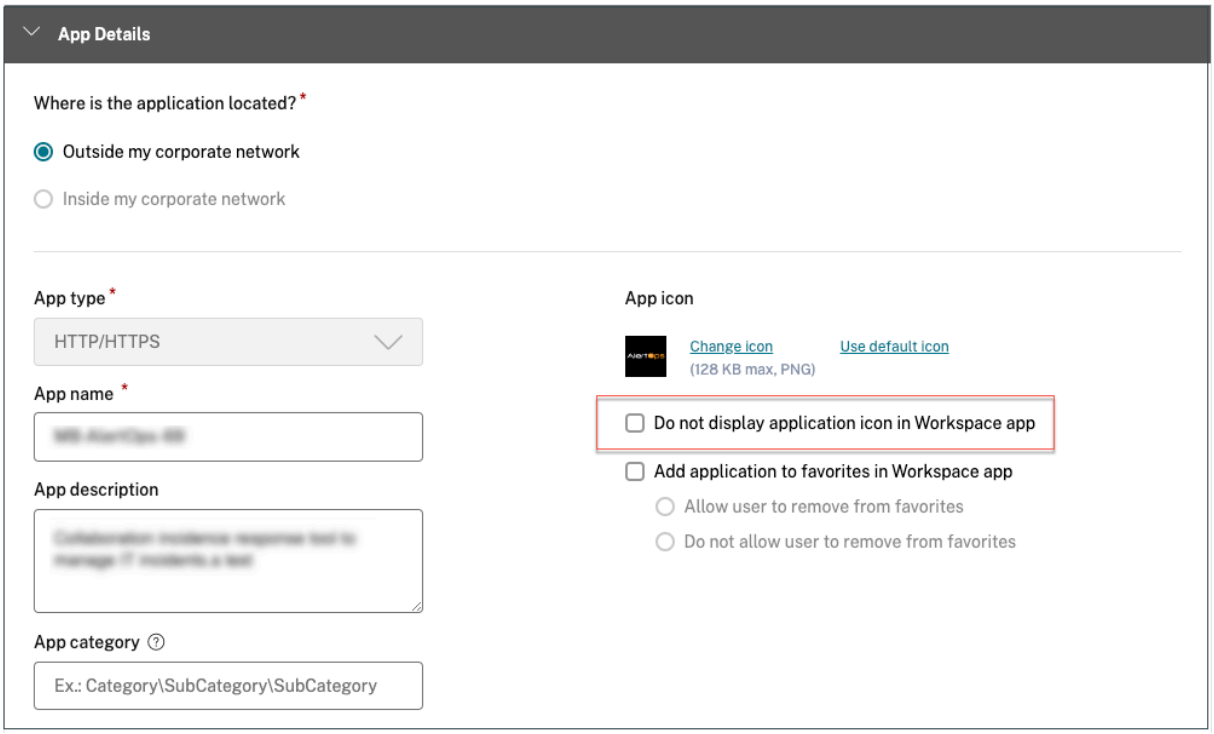
Meilleures pratiques en matière de configuration des applications

Les domaines IDP doivent disposer de leur propre application

Au lieu d'ajouter des domaines IDP en tant que domaines associés dans les configurations de votre application intranet, nous vous recommandons de procéder comme suit :

- Créez des applications distinctes pour tous les domaines IDP.

- Créez une stratégie autorisant tous les utilisateurs qui en ont besoin à accéder à la page d'authentification IDP, puis accordez la priorité absolue à cette stratégie.
- Masquez cette application (en sélectionnant l'option **Ne pas afficher l'icône de l'application aux utilisateurs**) dans la configuration de l'application afin qu'elle ne soit pas énumérée sur l'espace de travail. Pour plus d'informations, voir Configurer les détails de l'application.



> **Remarque :**
>
> cette configuration d'application permet uniquement l'accès à la page d'authentification IDP. L'accès ultérieur à des applications individuelles dépend toujours des configurations individuelles des applications et de leurs stratégies d'accès respectives.

Exemple de configuration :

1. Configurez tous les FQDN courants dans leurs propres applications, en les regroupant le cas échéant.

   Par exemple, si quelques applications utilisent Azure AD comme fournisseur d'identité et que vous devez configurer `login.microsoftonline.com` et d'autres domaines associés (`*.msauth.net`), procédez comme suit :

   - Créez une seule application commune avec `https://login.microsoftonline.com` comme URL de l'application `*.login.microsoftonline.com` et `*.msauth.net` comme domaines associés.

2. Sélectionnez l'option **Ne pas afficher l'icône de l'application aux utilisateurs** lors de la configuration de l'application. Pour plus de détails, voir Configurer les détails de l'application.
3. Créez une stratégie d'accès pour l'application commune et autorisez l'accès à tous les utilisateurs. Pour plus de détails, voir [Configurer une stratégie d'accès](/en-us/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup#step-3-configure-an-access-policy-with-multiple-rules).
4. Attribuez la priorité la plus élevée à la stratégie d'accès. Pour plus de détails, voir Ordre prioritaire.
5. Consultez les journaux de diagnostic pour vérifier que le nom de domaine complet correspond à l'application et que la stratégie est appliquée comme prévu.

Les mêmes domaines associés ne doivent pas faire partie de plusieurs applications

Le domaine associé doit être propre à une application. Des configurations conflictuelles peuvent entraîner des problèmes d'accès aux applications. Si plusieurs applications sont configurées avec le même nom de domaine complet ou une variante du nom de domaine complet générique, vous risquez de rencontrer les problèmes suivants :

- Les sites Web cessent de se charger ou peuvent afficher une page blanche.
- La page **Accès bloqué** peut s'afficher lorsque vous accédez à une URL.
- Il est possible que la page de connexion ne se charge pas.

Nous vous recommandons donc de configurer un domaine associé unique dans une seule application.

Exemples de configuration incorrecte :

- **Exemple : dupliquer des domaines associés dans plusieurs applications**

  Supposons que vous disposiez de deux applications nécessitant toutes deux un accès à Okta (example.okta.com) :

Application	domaine de l'URL de l'application	Domaine associé
App1	`https://code.example.net`	exemple.okta.com
App2	`https://info.example.net`	exemple.okta.com

Nom de la stratégie	Priorité	Applications utilisateur et associées
Refuser App1 à HR	Élevé	Groupe d'utilisateurs HR pour App1
Autoriser tout le monde à accéder à App1	Moyen	Activer l'accès du groupe d'utilisateurs Everyone à App1
Autoriser tout le monde à accéder à App2	Faible	Activer l'accès du groupe d'utilisateurs « Tout le monde » à App2

Problème de configuration : bien que l'intention était d'autoriser tous les utilisateurs à accéder à App2, le groupe d'utilisateurs HR ne peut pas accéder à App2. Le groupe d'utilisateurs HR est redirigé vers Okta, mais est bloqué en raison de la première stratégie qui a refusé l'accès à App1 (qui possède également le même domaine associé `example.okta.com` qu'App2).

Ce scénario est très courant pour les fournisseurs d'identité tels qu'Okta, mais il peut également se produire avec d'autres applications étroitement intégrées ayant des domaines associés communs. Pour plus de détails sur la correspondance et la hiérarchisation des stratégies, voir Correspondance et priorisation des stratégies d'accès.

Recommandation pour la configuration ci-dessus :

1. Supprimez example.okta.com en tant que domaine associé de toutes les applications.
2. Créez une nouvelle application uniquement pour Okta (avec l'URL de l'application `https://example.okta.com` et un domaine associé de `*.okta.com`).
3. Masquez cette application sur l'espace de travail.
4. Attribuez la priorité la plus élevée à la stratégie afin de supprimer tout conflit.

Meilleure pratique :

- Les domaines associés d'une application ne doivent pas chevaucher les domaines associés d'une autre application.
- Dans ce cas, une nouvelle application publiée doit être créée pour couvrir le domaine associé partagé, puis l'accès doit être défini en conséquence.
- Les administrateurs doivent évaluer si ce domaine associé partagé doit apparaître en tant qu'application réelle dans Workspace.
- Si l'application ne doit pas apparaître dans Workspace, lors de la publication de l'application, sélectionnez l'option **Ne pas afficher l'icône de l'application aux utilisateurs** pour la masquer dans Workspace.

URL de lien profond

Pour les URL de lien profond, le domaine de l'URL de l'application intranet doit être ajouté en tant que domaine associé :

Exemple :

L'URL de l'application intranet est configurée avec `https://example.okta.com/deep-link-app-1` comme domaine d'URL principal et le domaine associé est configuré avec le domaine de l'URL de l'application intranet, c'est-à-dire `*.issues.example.net`.

Dans ce cas, créez séparément une application IdP avec une URL `https://example.okta.com` puis un domaine associé tel que `*.example.okta.com`.

Mettre fin aux sessions utilisateur actives et ajouter des utilisateurs à la liste de blocage des utilisateurs

October 21, 2024

Les administrateurs peuvent mettre fin immédiatement à toutes les sessions actives des utilisateurs finaux et ajouter les utilisateurs à la liste de blocage des utilisateurs. L'ajout d'un utilisateur à cette liste de blocage d'utilisateurs met fin à toutes les sessions d'application Secure Private Access actives et bloque l'accès futur à l'application.

Toutes les sessions d'application actives via Citrix Enterprise Browser, l'accès direct, CWA pour HTML5 et l'agent Secure Access sont terminées et bloquées. Toutes les ressources connectées via l'agent Secure Access telles que les partages de fichiers, les sessions RDP et SSH sont également interrompues et bloquées. Les utilisateurs bloqués ne peuvent lancer aucune nouvelle application tant qu'ils ne sont pas supprimés de la liste des utilisateurs bloqués.

> **Remarque**
>
> - L'ajout d'un utilisateur à la liste de blocage des utilisateurs ne modifie pas la politique d'accès Secure Private Access configurée. La résiliation et le blocage de l'accès se produisent quelle que soit la politique d'accès configurée. Une fois l'utilisateur supprimé de la liste, les politiques d'accès Secure Private Access existantes pour l'utilisateur sont rétablies.
> - Seul l'accès aux applications Secure Private Access publiées est bloqué. L'accès à Internet via Citrix Enterprise Browser est autorisé ou refusé même après l'ajout d'un utilisateur à la liste de blocage en fonction de votre configuration de filtrage Web .

Cas d'utilisation

Vous pouvez utiliser cette fonctionnalité dans les scénarios suivants.

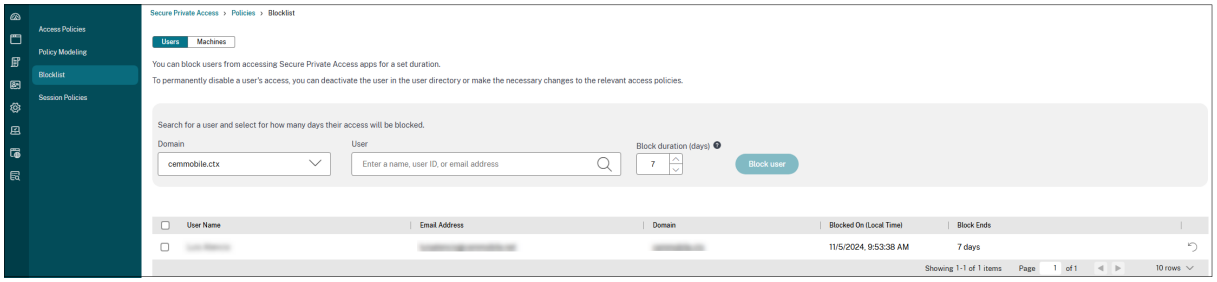
- Un employé quitte l'organisation ou est licencié de l'organisation. Dans ce cas, l'administrateur révoque tous les accès à l'application Secure Private Access en mettant fin aux sessions Secure Private Access actives et en bloquant tout accès futur à l'application.
- Un appareil est perdu ou volé. Dans ce cas, l'accès est bloqué et toutes les sessions en cours sont terminées. L'utilisateur peut être retiré de la liste de blocage des utilisateurs une fois la situation sous contrôle.
- Un utilisateur abuse de l'accès à l'application. Dans ce cas, l'accès de l'utilisateur peut être immédiatement révoqué. L'accès est bloqué jusqu'à ce que l'utilisateur soit ajouté à la liste.

Ajouter des utilisateurs à la liste de blocage des utilisateurs

1. Accédez à **Accès privé sécurisé > Stratégies d'accès** puis cliquez sur l'onglet **Liste de blocage des utilisateurs** .
2. Dans **Domaine**, sélectionnez le domaine pour lequel l'accès doit être désactivé.
3. Dans **Utilisateur**, recherchez le nom d'utilisateur qui doit être ajouté à la liste de blocage des utilisateurs. Tous les noms d'utilisateur correspondant aux critères de recherche sont affichés. Si l'utilisateur est supprimé du service d'annuaire, ce nom d'utilisateur n'apparaît pas dans la liste **Utilisateur** .
4. Dans **Durée du blocage (jours)**, entrez le nombre de jours pendant lesquels cet utilisateur doit être bloqué. Une fois que vous avez ajouté l'utilisateur à la liste bloquée, il est bloqué pendant 7 jours par défaut. Cependant, vous pouvez modifier la durée entre 1 et 99 jours. Une fois la durée terminée, l'accès de l'utilisateur est restauré en fonction de l'annuaire utilisateur et de la configuration de la politique. De plus, cette valeur reste persistante pour l'utilisateur pour les ajouts futurs. Par exemple, si un administrateur définit la durée de blocage pour un utilisateur à 30 jours, ce paramètre est conservé pour l'utilisateur pour les ajouts futurs.
5. Cliquez sur **Bloquer l'utilisateur**.

   L'utilisateur est ajouté à la liste de blocage des utilisateurs. Les actions suivantes se produisent une fois que l'utilisateur est ajouté à la liste de blocage des utilisateurs :

   - Toutes les sessions d'accès privé sécurisé actives sont immédiatement terminées.
   - L'accès futur à toutes les applications publiées Secure Private Access est bloqué.
   - L'accès à Internet via Citrix Enterprise Browser est autorisé même après l'ajout d'un utilisateur à la liste de blocage des utilisateurs. Seul l'accès aux applications Secure Private Access publiées est bloqué.



Vous pouvez restaurer l'accès avant même la fin de la durée du blocage en effectuant l'une des étapes suivantes.

- Sélectionnez l'accès pour lequel vous devez restaurer l'accès puis cliquez sur **Restaurer l'accès**.
- Cliquez sur l'icône de restauration en ligne avec l'utilisateur pour lequel vous souhaitez restaurer l'accès.

Dans les deux cas, une boîte de dialogue de confirmation apparaît.

> **Recommandations :**
>
> - Pour révoquer l'accès d'un utilisateur indéfiniment, supprimez l'utilisateur de votre service d'annuaire respectif, tel qu'Active Directory, puis ajoutez-le à la liste de blocage des utilisateurs. Cela met fin à la session d'accès privé sécurisé active de l'utilisateur, bloque l'accès futur à l'application et, une fois que l'utilisateur est déconnecté de Workspace, il ne peut pas se reconnecter en raison d'informations d'identification d'annuaire inactives.

Délais d'expiration des sessions utilisateur

December 27, 2023

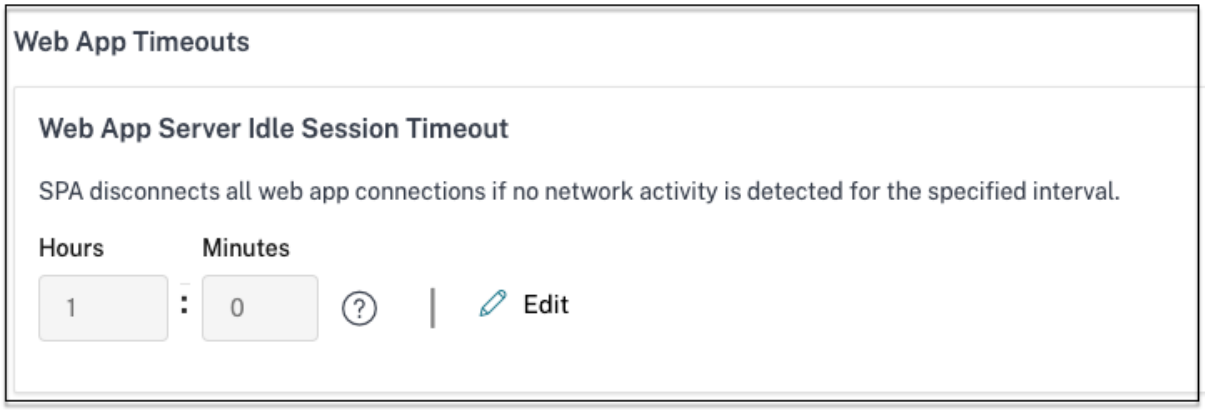
Vous pouvez configurer un délai d'expiration pour les applications Web et le client Citrix Secure Access afin de mettre fin aux sessions des utilisateurs s'il n'y a aucune activité réseau pendant la période spécifiée.
Pour le client Citrix Secure Access, vous pouvez également configurer le client Citrix Secure Access pour mettre fin à une session s'il n'y a aucune activité utilisateur pendant la période spécifiée. Vous pouvez également configurer une déconnexion forcée sur le client Citrix Secure Access indépendamment de l'activité de l'utilisateur et du réseau, une fois la période configurée expirée.

Délai d'expiration pour les serveurs d'applications Web

1. Accédez à **Paramètres > Délais d'expiration.**

2. Dans **Timeout de session d'inactivité du serveur Web App**, sélectionnez la durée, en heures et minutes, pendant laquelle la session d'application Web peut être inactive. Le service Secure Private Access met fin à la session une fois ce délai expiré si la session reste inactive.

   La durée minimale est de 1 heure et la durée maximale peut être de 168 heures. La valeur par défaut est de 2 heures.

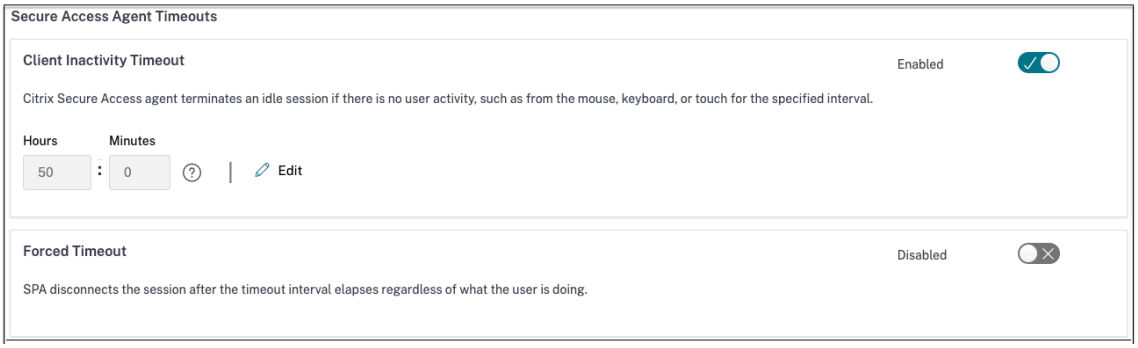


Délais d'expiration pour le client Citrix Secure Access

Vous pouvez configurer les délais d'expiration suivants pour le client Citrix Secure Access :

- Inactivité du client
- Délai d'expiration forcé

1. Accédez à **Paramètres > Délais d'expiration.**



2. Dans **Secure Access Agent Timeout**, sélectionnez la durée, en heures et minutes, du délai d'expiration que vous souhaitez appliquer.

   - **Délai d'inactivité du client** : durée après laquelle le client Citrix Secure Access met fin à une session, s'il n'y a aucune activité utilisateur (souris ou clavier) pendant la période configurée. Cette option est désactivée par défaut. Vous devez activer l'option en utilisant le commutateur à bascule pour appliquer le délai d'expiration configuré. Toutefois,

si vous désactivez le commutateur après l'enregistrement de la configuration, le client ne déclenche pas de délai d'expiration.

La durée minimale est de 5 minutes et la durée maximale peut être de 168 heures. La valeur par défaut est de 8 heures.

- **Délai d'expiration forcé** : durée après laquelle le client Citrix Secure Access met fin à une session, quelle que soit l'activité de l'utilisateur ou du réseau. Cette option est désactivée par défaut. Vous devez activer l'option en utilisant le commutateur à bascule pour appliquer le délai d'expiration configuré. Toutefois, si vous désactivez le commutateur après l'enregistrement de la configuration, le client ne déclenche pas de délai d'expiration.

  Un message de notification apparaît 15 minutes avant la fin de la session.

  La durée minimale est de 1 heure et la durée maximale peut être de 168 heures. La valeur par défaut est de 168 heures.

> **Remarque :**
>
> Si vous activez plusieurs de ces paramètres, le premier délai d'expiration ferme la connexion utilisateur.

Accès en lecture seule pour les administrateurs aux applications SaaS et Web

December 27, 2023

Les organisations comprennent généralement plusieurs administrateurs et les administrateurs doivent disposer de différents niveaux de privilèges d'accès. Les équipes d'administrateurs de sécurité utilisant le service Secure Private Access peuvent fournir des contrôles granulaires, tels qu'un accès en lecture seule aux administrateurs. Les administrateurs qui n'ajoutent ni ne modifient aucune application peuvent bénéficier d'un accès en lecture seule pour afficher les détails de l'application. Les administrateurs du service Secure Private Access disposant d'un accès en lecture seule ne peuvent pas effectuer les tâches suivantes.

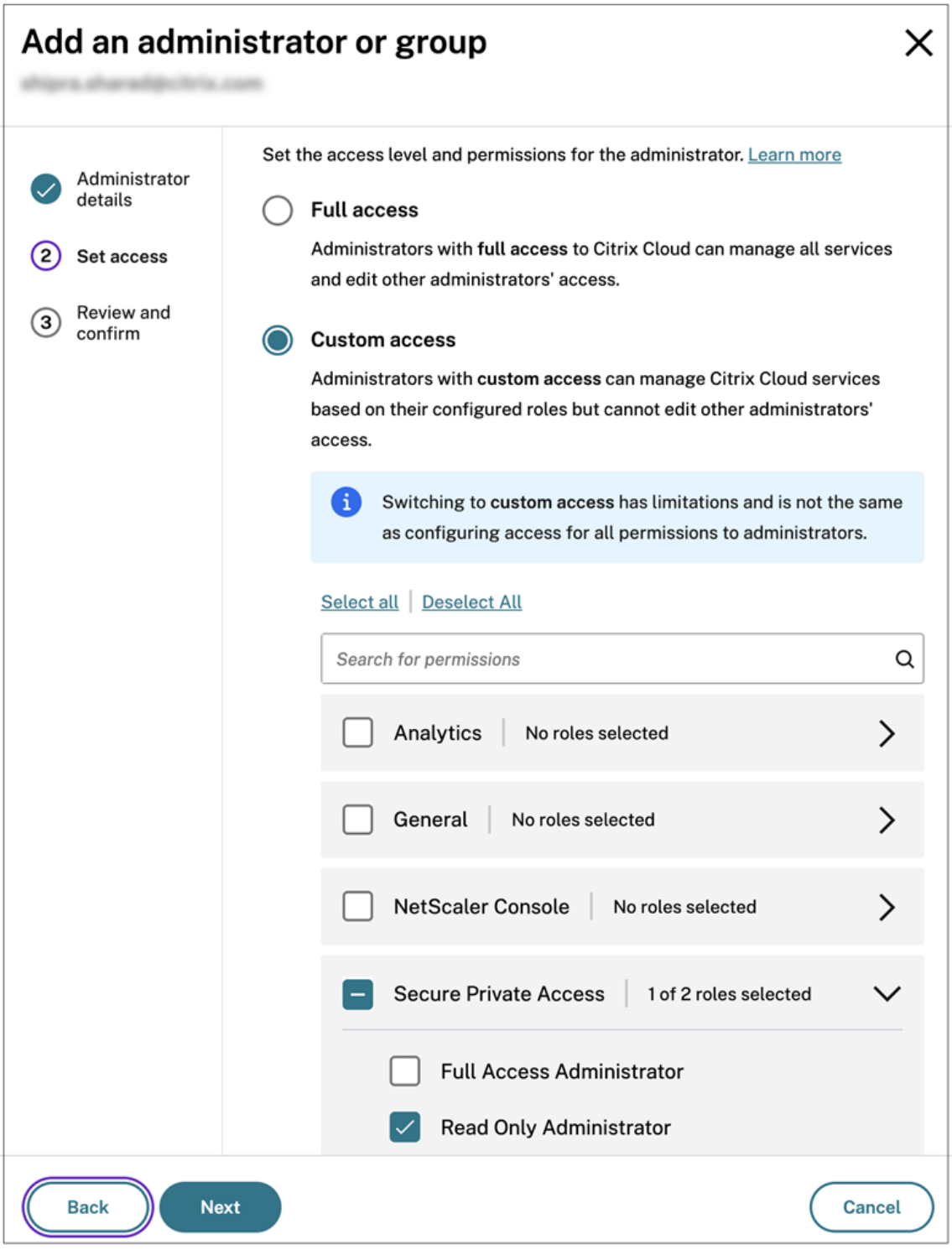
- Ajoutez des applications Web ou SaaS d'entreprise.
- Ajoutez de nouvelles appliances Connector dans des emplacements de ressources existants ou nouveaux.

Comment fournir un accès en lecture seule aux administrateurs

Après vous être connecté à Citrix Cloud, sélectionnez **Gestion des identités et des accès** à partir du menu.
Sur la page Gestion des identités et des accès, cliquez sur **Administrateurs**. La console affiche tous les administrateurs actuels du compte.

Ajouter un administrateur disposant d'un accès en lecture seule

1. Dans **Ajouter des administrateurs**, sélectionnez le fournisseur d'identité à partir duquel vous souhaitez sélectionner l'administrateur. Citrix Cloud peut parfois vous demander de vous connecter d'abord au fournisseur d'identité (par exemple, Azure Active Directory).
2. Si **Citrix Identity** est sélectionné, entrez l'adresse e-mail de l'utilisateur, puis cliquez sur **Inviter**.
3. Si Azure Active Directory est sélectionné, entrez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez sur Inviter.
4. Sélectionnez **Accès personnalisé**. Les options suivantes s'affichent :
   - **Sélectionnez Administrateur à accès complet (Technical Preview)** : fournit un accès complet.
   - **Administrateur en lecture seule (Technical Preview)** : fournit un accès en lecture seule.
5. Sélectionnez **Administrateur en lecture seule (Technical Preview)**.



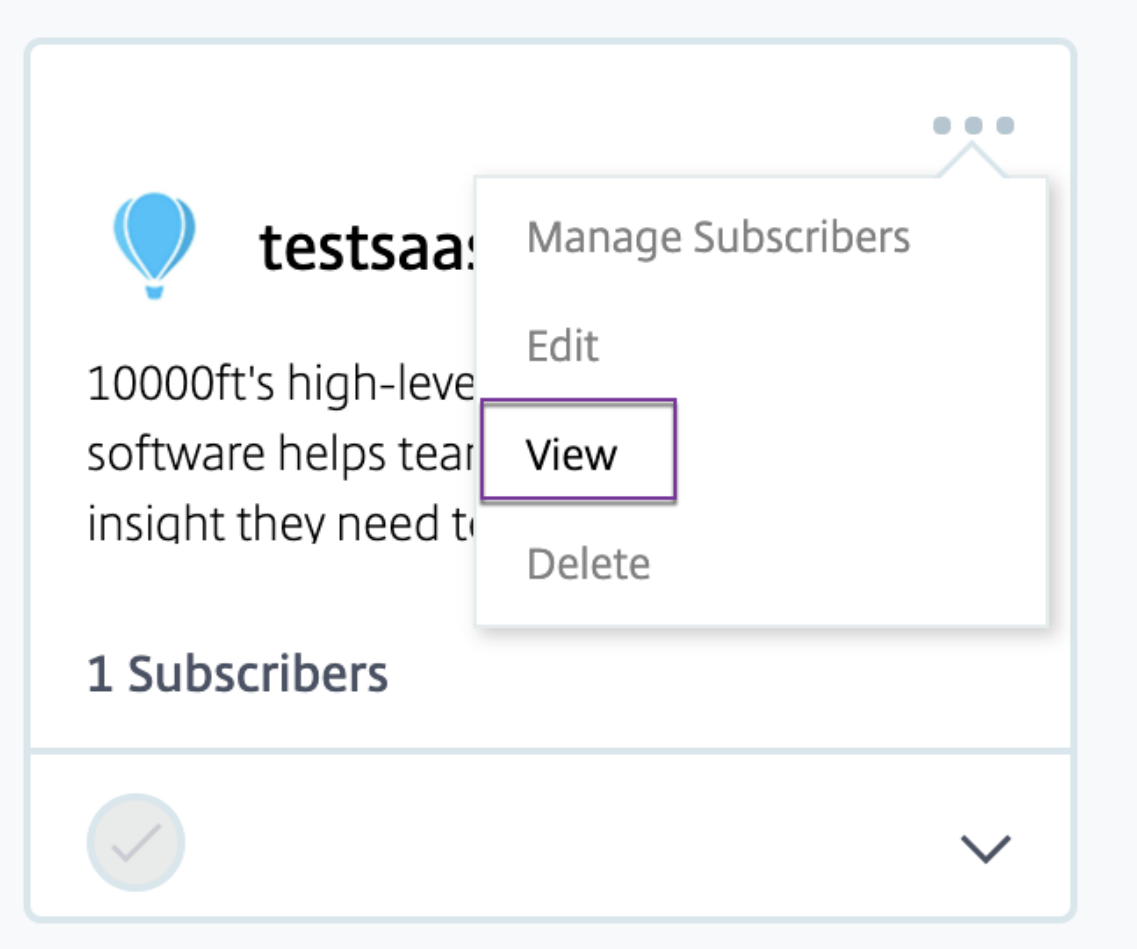
6. Cliquez sur **Envoyer invitation**.

> **Important :**
>
> - Lorsque vous accordez un accès **administrateur en lecture seule** aux administrateurs

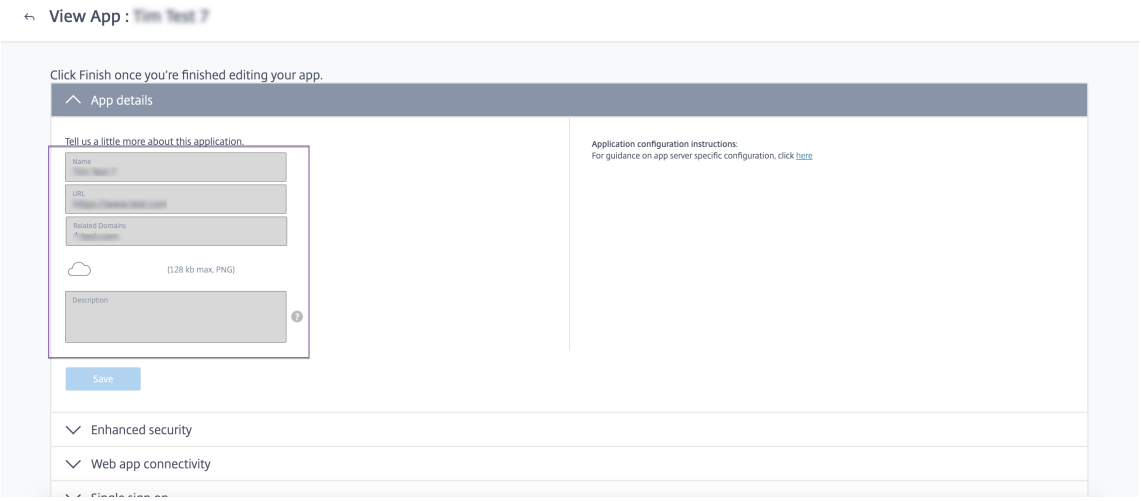
> NetScaler Gateway Service, vous devez également activer la **bibliothèque** à partir de la liste de **gestion générale** pour ces administrateurs. Ce n'est qu'alors que l'option **Afficher** pour les applications est activée pour les administrateurs.
> - Le bouton **Ajouter une application Web/SaaS** est désactivé pour les utilisateurs disposant d'un accès **administrateur en lecture seule** .

Pour afficher les détails de l'application lorsque les administrateurs disposent d'un accès en lecture seule

1. Après vous être connecté à Citrix Cloud, sélectionnez **Bibliothèque** dans le menu.
2. Sélectionnez l'application dont vous souhaitez afficher les détails et cliquez sur les **points de suspension**.
   Seule l'option **Afficher** est activée. Toutes les autres options sont désactivées.



3. Cliquez sur **Afficher**.



Aperçu du tableau de bord

October 21, 2024

Le tableau de bord du service Secure Private Access affiche les données de diagnostic et d'utilisation des applications SaaS, Web, TCP et UDP. Le tableau de bord offre aux administrateurs une visibilité complète sur leurs applications, leurs utilisateurs, l'état de santé des connecteurs et l'utilisation de la bande passante en un seul endroit pour la consommation. Ces données sont extraites de Citrix Analytics. Les données des différentes entités peuvent être visualisées pour une durée prédéfinie ou pour une chronologie personnalisée. Pour certaines entités, vous pouvez effectuer un zoom avant pour afficher plus de détails.

Les mesures sont généralement classées dans les catégories suivantes.

- **Journalisation et dépannage**
  - Journaux de diagnostic : journaux liés à l'authentification, au lancement d'applications, à l'énumération d'applications et aux contrôles de posture de l'appareil.
- **Utilisateurs**
  - Utilisateurs actifs : nombre total d'utilisateurs uniques accédant aux applications (SaaS, Web et TCP) pour l'intervalle de temps sélectionné.
  - Téléchargements : volume total de données téléchargées via le service Secure Private Access pour l'intervalle de temps sélectionné.
  - Téléchargements : Volume total de données téléchargées via le service Secure Private Access pour l'intervalle de temps sélectionné.
- **Applications :**

  - Applications : Nombre total d'applications (indépendamment de l'intervalle de temps) actuellement configurées.
  - Nombre de lancements d'applications : nombre total d'applications (sessions d'application) lancées par chaque utilisateur pour l'intervalle de temps sélectionné.
  - Domaines configurés : nombre total de domaines configurés pour l'intervalle de temps sélectionné.
  - Applications découvertes : nombre total de domaines uniques et individuels auxquels on a accédé mais qui ne sont associés à aucune application

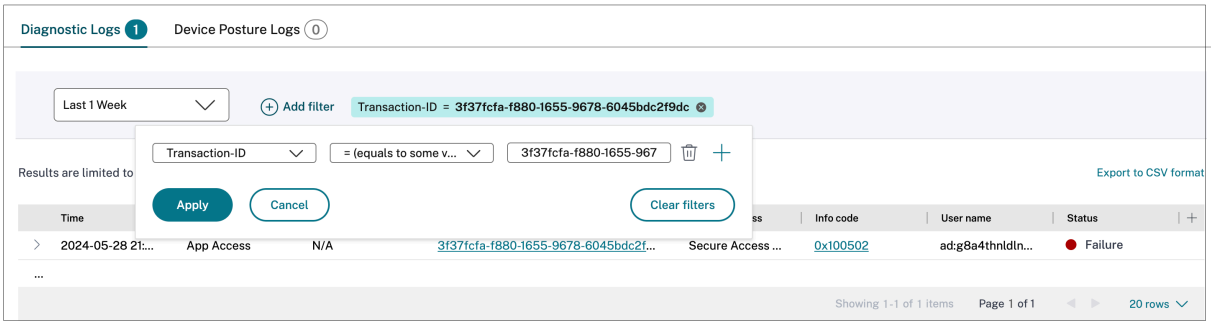
- **Politiques d'accès**

  - Politiques d'accès : Nombre total de politiques d'accès (indépendamment de l'intervalle de temps) actuellement configurées.

Journaux de diagnostic

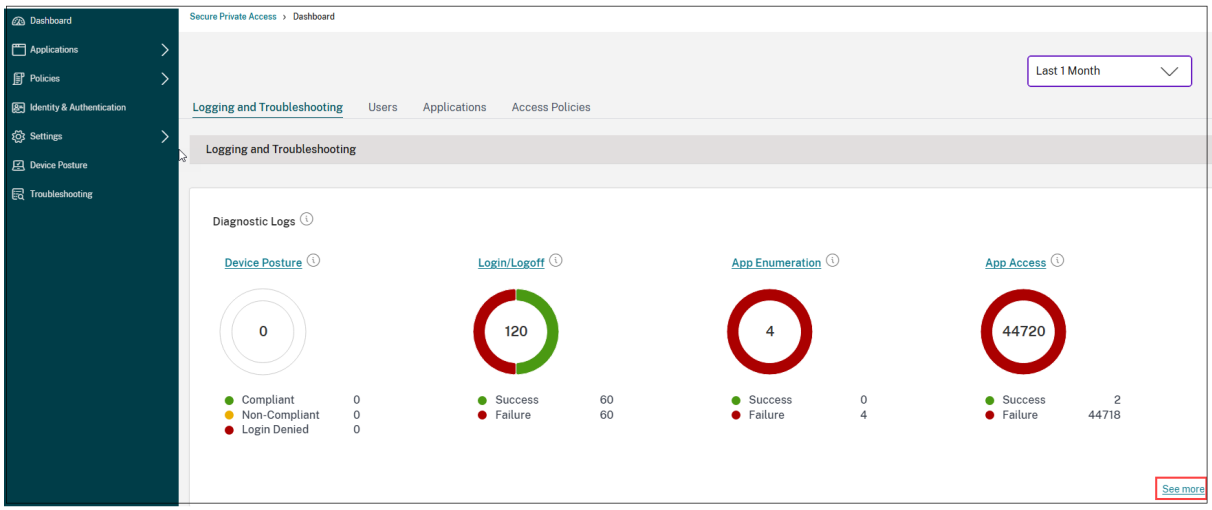
Utilisez le graphique **Journaux de diagnostic** pour afficher les journaux liés à l'authentification, au lancement de l'application, à l'énumération des applications, ainsi que les journaux liés à la posture de l'appareil. Vous pouvez cliquer sur le lien **Voir plus** pour afficher les détails des journaux. Les détails sont présentés sous forme de tableau. Vous pouvez afficher les journaux pour une durée prédéfinie ou pour une chronologie personnalisée. Vous pouvez ajouter des colonnes au graphique en cliquant sur le signe + en fonction des informations que vous souhaitez voir dans le tableau de bord. Vous pouvez exporter les journaux utilisateur au format CSV.

- Vous pouvez utiliser l'option **Ajouter un filtre** pour affiner votre recherche en fonction de différents critères tels que le type d'application, la catégorie, la description. Par exemple, dans les champs de recherche, vous pouvez sélectionner `ID de transaction`, `=` (`égal à` `une valeur`) et saisir `7456c0fb-a60d-4bb9-a2a2-edab8340bb15` dans cette séquence, pour rechercher tous les journaux liés à cet ID de transaction. Pour plus de détails sur les opérateurs de recherche qui peuvent être utilisés avec l'option de filtre, voir Opérateurs de recherche.

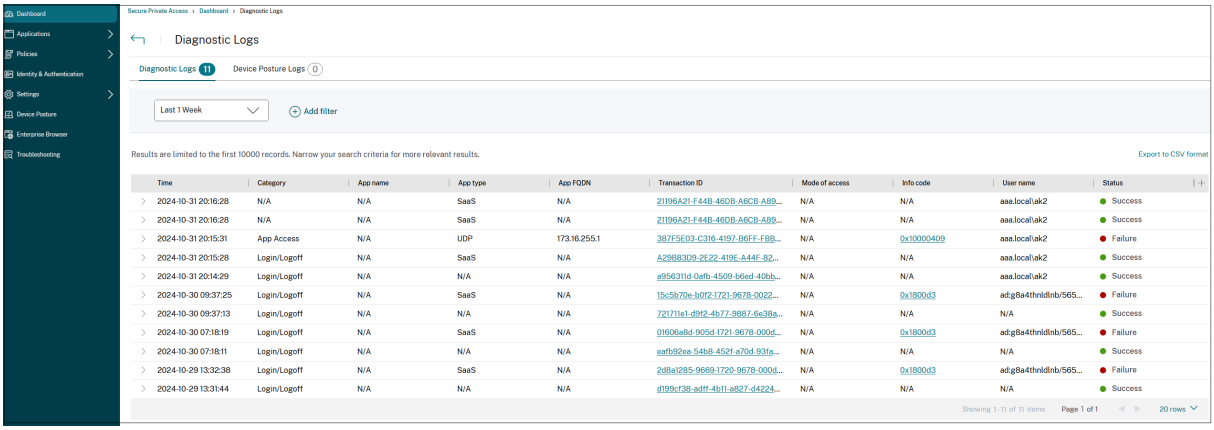


- **Journaux de posture de l'appareil :** Vous pouvez affiner votre recherche en fonction des résultats de la politique (**Conforme, Non conforme et Connexion refusée**). Pour plus de détails sur la posture de l'appareil, voir Posture de l'appareil.

> **Remarque**
>
> - Chaque événement d'échec dans le tableau de bord des journaux de diagnostic Secure Private Access est associé à un code d'information. Pour plus de détails, voir Code d'information.
> - L'ID de transaction met en corrélation tous les journaux d'accès privé sécurisé pour une demande d'accès. Pour plus de détails, voir ID de transaction.



- Vous pouvez cliquer sur l'icône de développement (>) pour afficher les détails complets des journaux.
- La page **Journaux de diagnostic** affiche les domaines intégrés pour chacune des URL principales auxquelles on accède. Les administrateurs peuvent afficher les domaines intégrés en cliquant sur l'icône de développement (>) à partir de l'URL principale. Les administrateurs peuvent utiliser la liste des domaines intégrés pour résoudre les problèmes liés à l'accès aux applications ou au rendu des applications. Par exemple, si un domaine est manquant dans la configuration de l'application, l'application spécifique n'est pas accessible à l'utilisateur final. Dans ce cas, l'administrateur peut afficher la liste des domaines intégrés, identifier le domaine manquant, puis mettre à jour la configuration de l'application avec le domaine manquant.

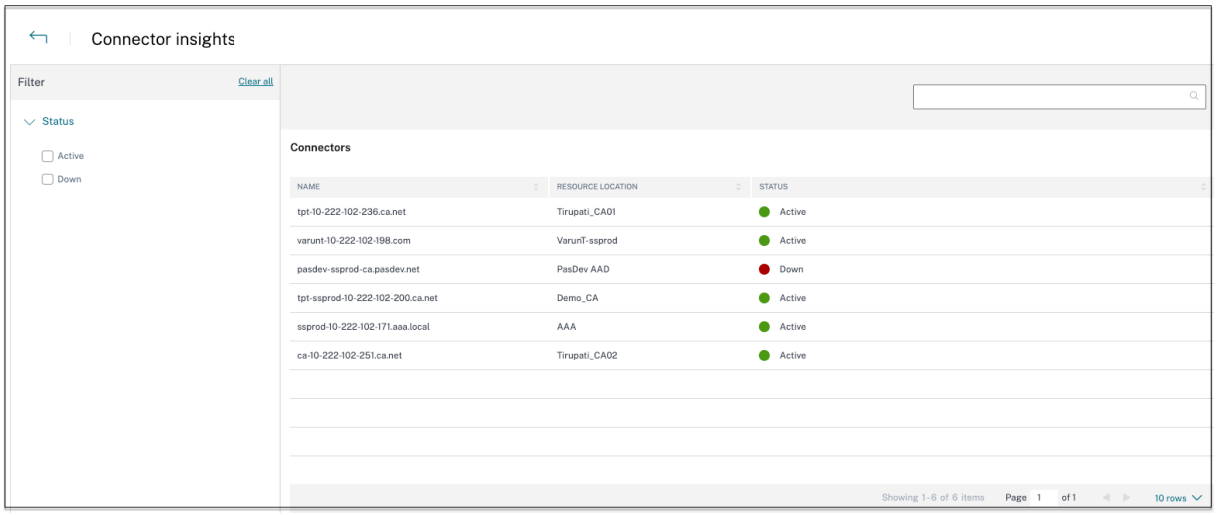


Remarque

- Par défaut, la page **Journaux de diagnostic** affiche les données de la semaine en cours et uniquement les 10 000 enregistrements récents. Utilisez la recherche de date personnalisée et les filtres pour affiner davantage vos résultats de recherche.

État du connecteur

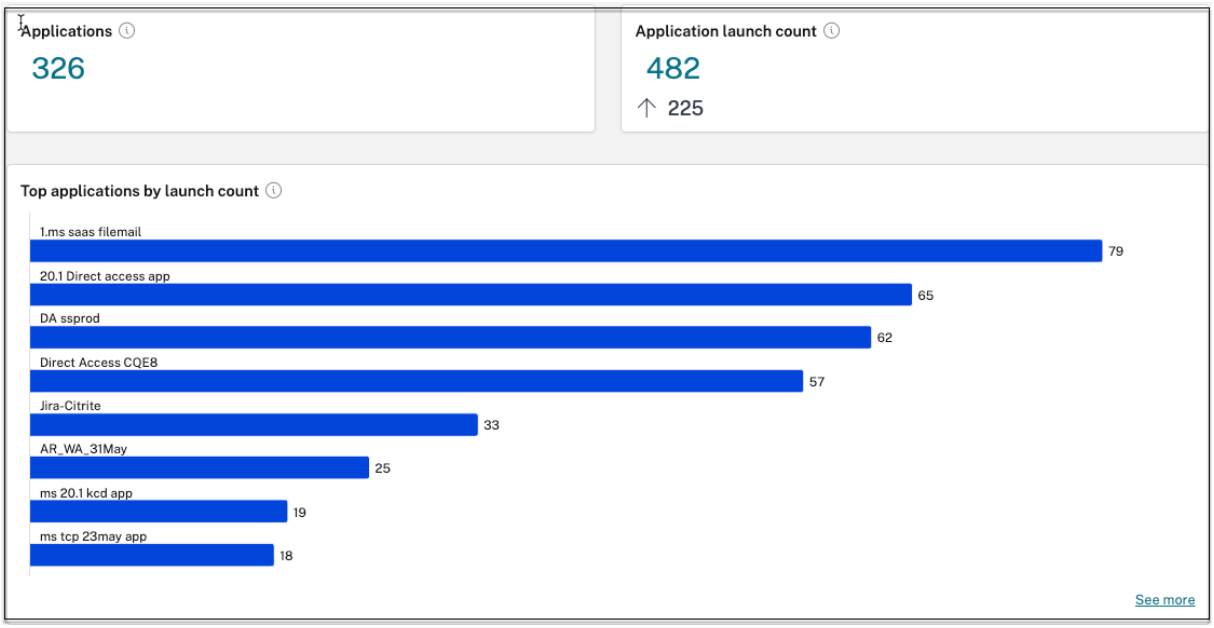
Utilisez le graphique d'état du connecteur ** **pour afficher l'état des connecteurs et les emplacements des ressources où les connecteurs sont déployés. Cliquez sur le lien **Voir plus** pour afficher les détails. Dans la page **Informations sur les connecteurs** , vous pouvez utiliser les filtres **Actif** ou **Inactif** pour filtrer les connecteurs en fonction de leur statut.



Principales applications par nombre de lancements

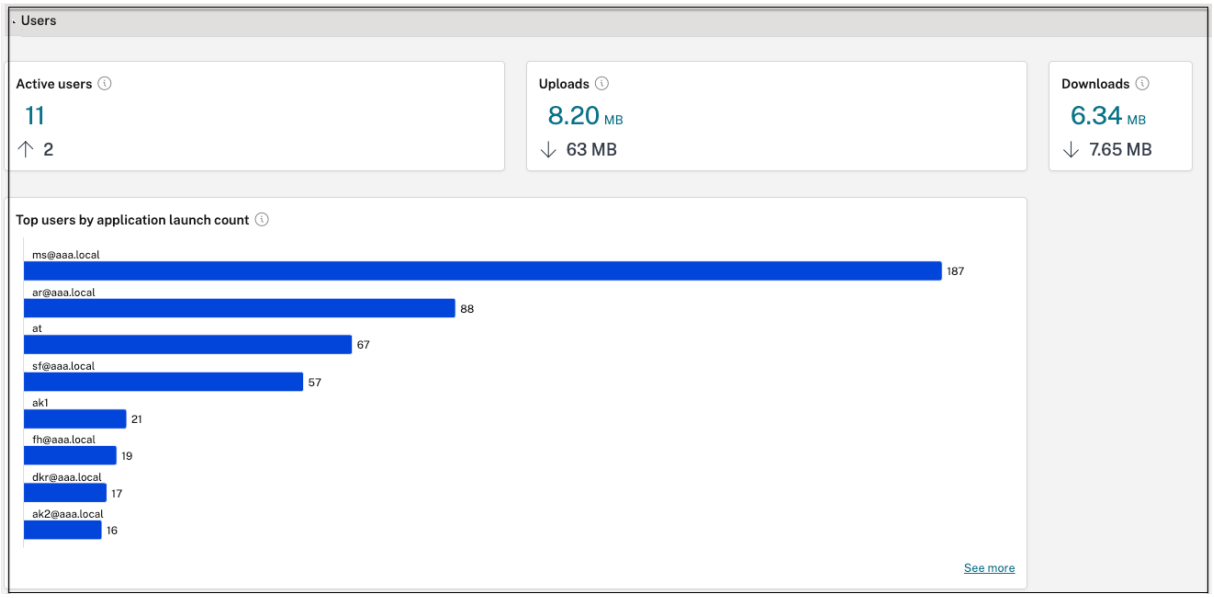
Utilisez le graphique **Principales applications par nombre de lancements** pour afficher la liste des principales applications en fonction du nombre de fois où l'application a été lancée, du volume total

de données téléchargées sur le serveur d'applications et du volume total de données téléchargées depuis le serveur d'applications. Vous pouvez appliquer les filtres **Applications SaaS**, **Applications Web**ou **Applications TCP/UDP** pour affiner votre recherche à des applications spécifiques. Vous pouvez filtrer les données selon une chronologie prédéfinie ou selon une chronologie personnalisée.



Principaux utilisateurs par nombre de lancements d'applications

Utilisez le graphique **Principaux utilisateurs par nombre de lancements d'applications** pour afficher les données par utilisateur. Par exemple, le nombre de fois qu'un utilisateur a lancé l'application TCP, le volume total de données téléchargées sur le serveur d'applications et le volume total de données téléchargées depuis le serveur d'applications. Vous pouvez filtrer les données selon une chronologie prédéfinie ou selon une chronologie personnalisée.

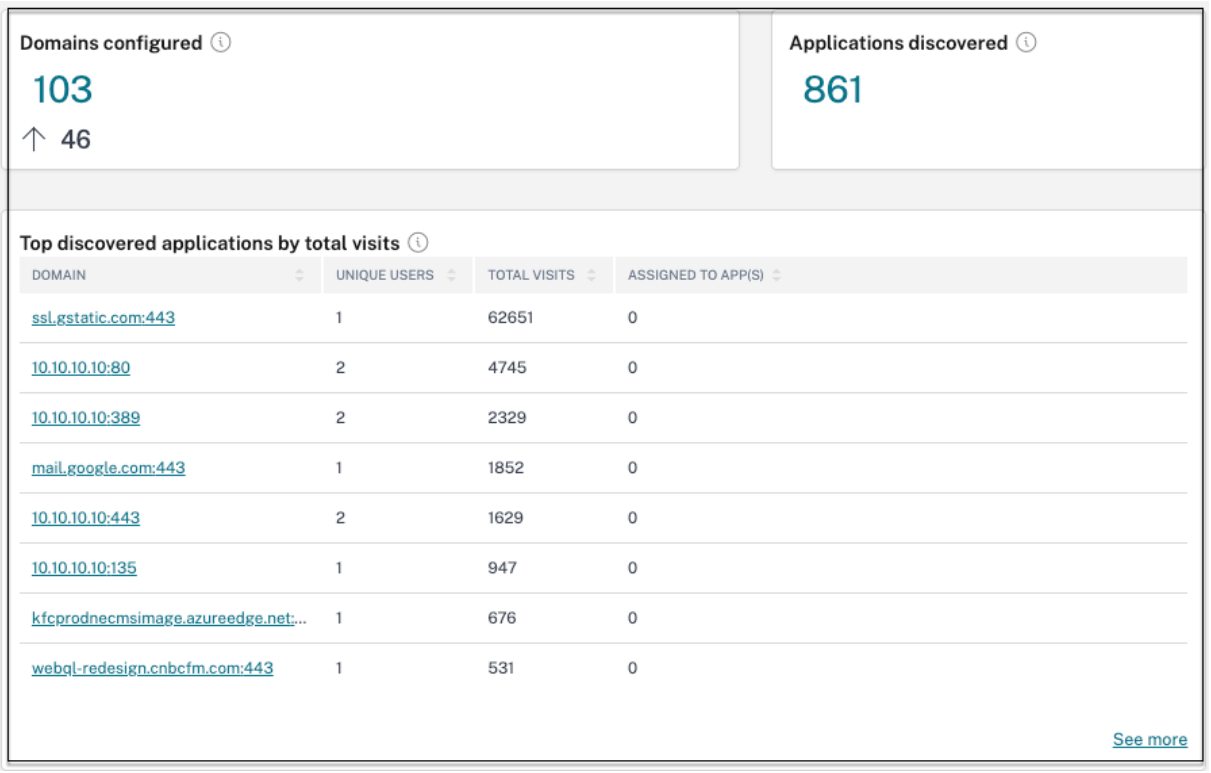


Politiques d'accès les plus importantes par application

Utilisez le graphique **Principales politiques d'accès par application** pour afficher la liste des politiques d'accès appliquées sur les applications. Cliquez sur le lien **Voir plus** pour afficher la liste des politiques associées aux applications et le nombre de fois où les politiques sont appliquées. Vous pouvez également utiliser l'option **Rechercher** dans la page Politiques d'accès pour filtrer les politiques en fonction du nom de la politique. Vous pouvez également rechercher des politiques spécifiques à l'aide des opérateurs de recherche pour affiner davantage votre recherche. Pour plus de détails, voir Opérateurs de recherche.

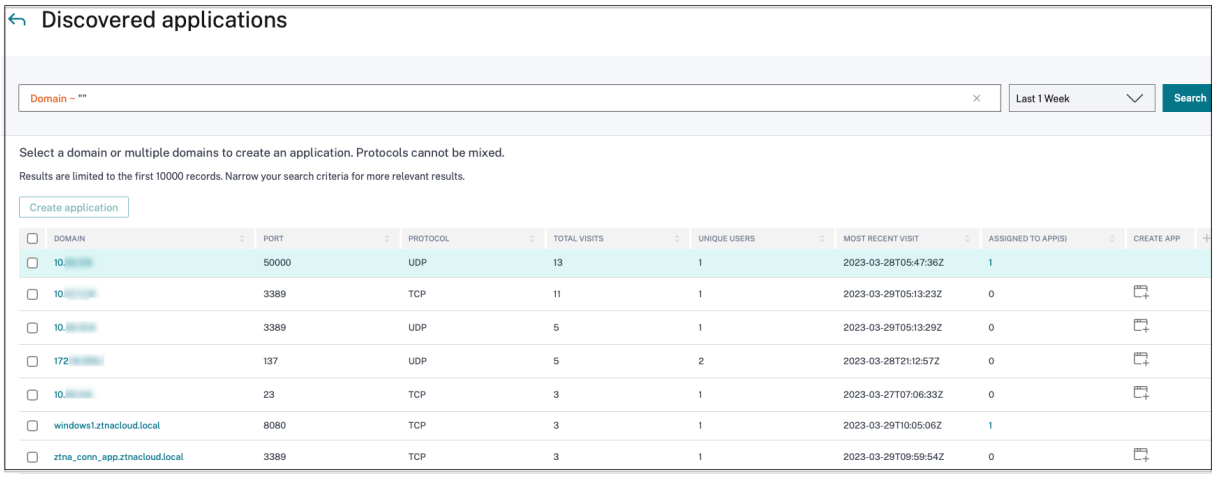
Principales applications découvertes

Utilisez le graphique **Principales applications découvertes par nombre total de visites** pour afficher la liste des domaines uniques et individuels qui ont été consultés à un moment donné mais qui ne sont associés à aucune application. Ces domaines sont répertoriés en fonction du nombre total de visites sur ces domaines. Les administrateurs peuvent utiliser ce graphique pour voir si un domaine présentant un intérêt particulier est consulté par de nombreux utilisateurs. Dans de tels cas, les administrateurs peuvent créer une application avec ce domaine pour un accès facile.



Dans le graphique, la colonne **ASSIGNÉE AUX APPLICATIONS** affiche le nombre total d'applications pour lesquelles ce domaine est configuré dans le cadre de leurs valeurs d'URL associées ou d'URL de destination. Cliquer sur le numéro affiche les applications attribuées à ce domaine.

Vous pouvez cliquer sur le lien **Voir plus** pour afficher plus de détails sur tous les domaines.



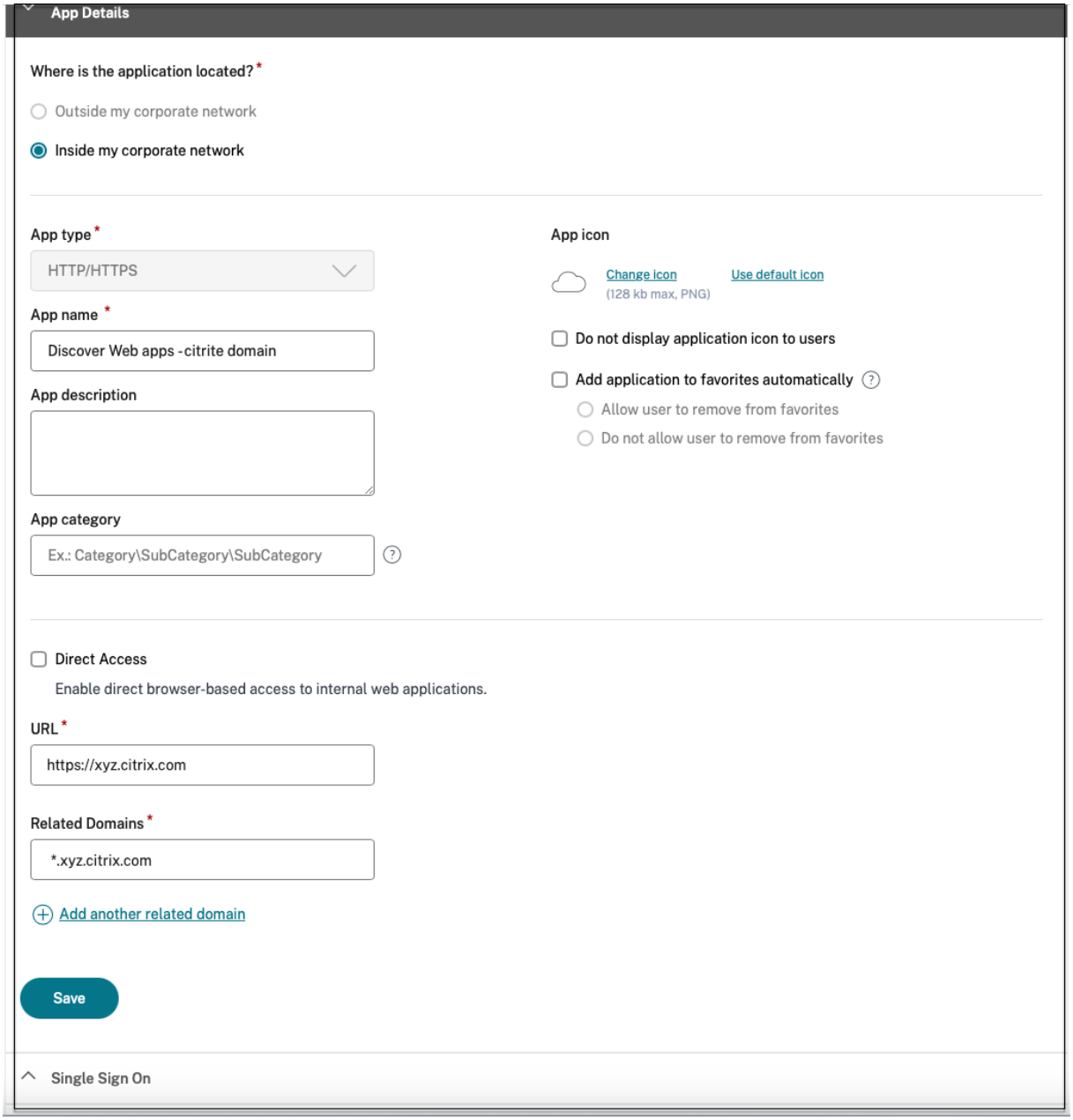
La page **Applications découvertes** affiche les détails des domaines tels que le nom de domaine, le port, le protocole, le nombre total de visites, les utilisateurs uniques et la date de visite la plus récente. Toutes les colonnes du graphique sont triables. Vous pouvez utiliser la barre de recherche pour effectuer une recherche en fonction du domaine.

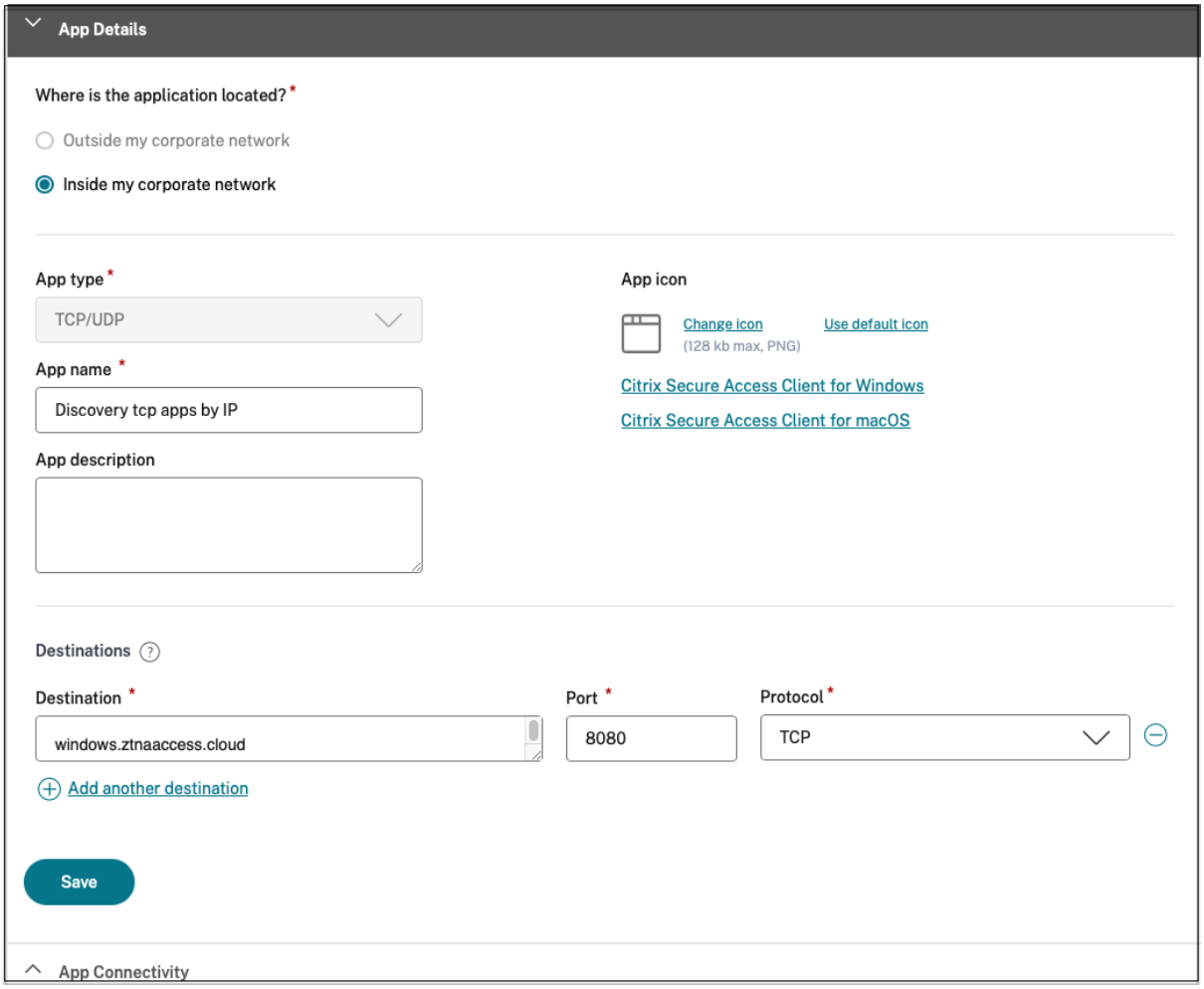
> **Remarque**
>
> - Les protocoles sont dérivés en fonction des ports standard utilisés par les clients.
> - La liste des domaines découverts est limitée à 10 000 enregistrements.

Créer une application à partir du graphique

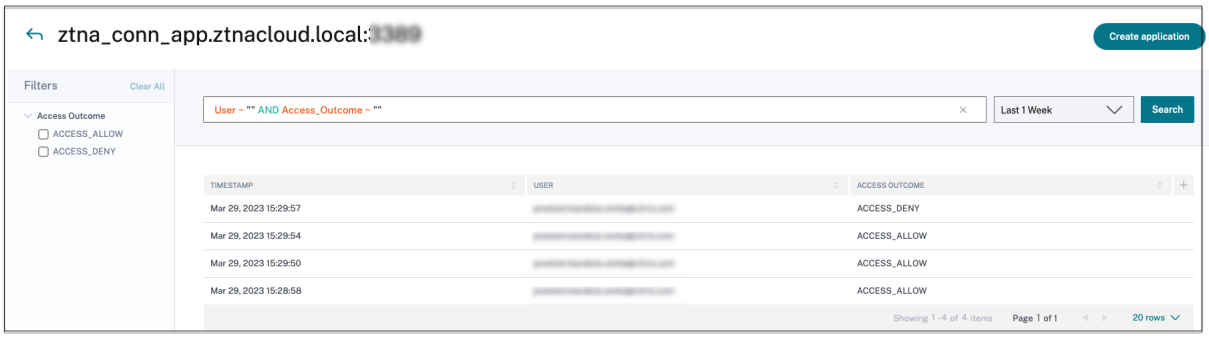
Cliquez sur l'icône **+** en ligne avec le domaine respectif pour créer une application. L'assistant de configuration de l'application apparaît. L'icône de création d'application n'apparaît pas pour les lignes dans lesquelles une application est déjà créée avec la même combinaison de domaine, de port et de protocole, et est dans un état terminé.

- Le type d'application est automatiquement renseigné en fonction du protocole de l'application que vous avez sélectionné. Cependant, vous pouvez modifier le type, si nécessaire.
- Les valeurs dans les champs **URL, Domaines associés, Destination, Port, Protocole** sont toutes renseignées automatiquement. Suivez les étapes pour ajouter une application. Pour plus de détails, consultez Flux de travail guidé par l'administrateur pour une intégration et une configuration faciles.





Vous pouvez également cliquer sur le lien du domaine unique pour voir plus de détails et créer une demande pour ce domaine. Lorsque vous cliquez sur un lien de domaine, les journaux d'authentification utilisateur pour le domaine s'affichent. Cliquez sur le bouton **Créer une application** . Suivez les étapes pour ajouter une application.



Opérateurs de recherche

Voici les opérateurs de recherche que vous pouvez utiliser pour affiner votre recherche :

- **= (égal à une valeur)**: Pour rechercher les journaux/politiques qui correspondent exactement aux critères de recherche.
- **!= (pas égal à une valeur)**: Pour rechercher les journaux/politiques qui ne contiennent pas les critères spécifiés.
- **~ (contient une valeur)**: Pour rechercher les journaux/politiques qui correspondent partiellement aux critères de recherche.
- **!~ (ne contient pas de valeur)**: Pour rechercher les journaux/politiques qui ne contiennent pas certains des critères spécifiés.

Journalisation et dépannage

October 21, 2024

Utilisez cette rubrique pour résoudre certains problèmes liés à la configuration de l'application, à l'authentification et à l'authentification unique, ou à l'accès à l'application. Copiez le code d'information de la colonne « Code d'information » dans les journaux de diagnostic Secure Private Access, puis recherchez ce code sur cette page pour trouver les étapes de dépannage correspondantes. Voici quelques FAQ pour vous aider à mieux utiliser ce sujet.

FAQ?

Que sont les journaux de diagnostic Secure Private Access ?

Où puis-je trouver les journaux d'accès privé sécurisé ?

Quel widget affiche les journaux de diagnostic de Secure Private Access ?

Quels détails puis-je trouver dans les journaux de diagnostic de Secure Private Access ?

Quels événements sont capturés dans les journaux de diagnostic Secure Private Access ?

Comment filtrer les journaux de diagnostic ?

Comment utiliser la rubrique de dépannage de Secure Private Access pour résoudre une panne que j'ai rencontrée ?

Qu'est-ce qu'un code d'information ? Où puis-je les trouver ?

Qu'est-ce qu'un identifiant de transaction ? Comment l'utiliser ?

Quels sont tous les emplacements PoP d'accès privé sécurisé ?

Que dois-je faire si je ne parviens pas à résoudre mon échec à l'aide du code d'information et de la table de recherche d'erreurs ?

Tableau de recherche des codes d'information

Le tableau de recherche d'erreurs suivant fournit un aperçu complet des différentes erreurs que les utilisateurs peuvent éventuellement rencontrer lors de l'utilisation du service Secure Private Access.

Code d'information	Description	Résolution
0x180006, 0x1800B7	Le lancement de l'application a échoué car la longueur du nom de domaine complet de l'application a été dépassée	Le lancement de l'application a échoué car la longueur du nom de domaine complet de l'application a été dépassée
0x180022	Le lancement de l'application a échoué car le service d'authentification est en panne	Le lancement de l'application a échoué car le service d'authentification est en panne
0x180001, 0x18001A, 0x18001B, 0x18008A 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0 0x1800B1, 0x1800B2, 0x1800B3, 0x180048	Erreurs d'authentification unique, échec d'établissement de connexion entre Citrix Cloud et les connecteurs locaux, échec de l'authentification unique SAML, nom de domaine complet d'application non valide	L'accès à l'application est refusé
0x1800EF	Problème de connexion à l'appareil Connector	Problème de connexion à l'appareil Connector
0x18009D	Recherche DNS/Connexion échouée	Service de navigation sécurisé - Erreurs de recherche/connexion DNS
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5 0x1800A6, 0x1800A7	Le lancement de l'application Web a échoué car il est impossible de se connecter à l'application Web principale	Le lancement de l'application Web a échoué car il est impossible de se connecter à l'application Web principale
0x1800BC, 0x1800BF	L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS	L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS
0x1800BD	L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS pour DirectAccess	L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS pour DirectAccess

Code d'information	Description	Résolution
0x1800D0	Le lancement de la session de l'agent Citrix Secure Access a échoué lors de la récupération de la configuration de l'application	Le lancement de la session de l'agent Citrix Secure Access a échoué lors de la récupération de la configuration de l'application
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Le lancement de la session de l'agent Citrix Secure Access a échoué lors de la récupération de la configuration de l'application, le lancement de l'application de l'agent Citrix Secure Access a échoué lors de l'évaluation de la stratégie, le lancement de l'application de l'agent Citrix Secure Access a échoué	Demandes client mal formulées
0x1800DE	Le lancement de l'application de l'agent Citrix Secure Access a échoué lors de l'évaluation de la stratégie	Le lancement de l'application de l'agent Citrix Secure Access a échoué lors de l'évaluation de la stratégie
0x180055, 0x1800DF, 0x1800E3	Applications restreintes par la politique contextuelle, accès refusé en raison de la configuration de la politique	Une ou plusieurs applications non répertoriées dans le tableau de bord de l'utilisateur
0x1800EB	Le lancement de l'application de l'agent Citrix Secure Access a échoué car IPv6 n'est pas pris en charge	Le lancement de l'application de l'agent Citrix Secure Access a échoué car IPv6 n'est pas pris en charge
0x1800EC, 0x1800ED	Le lancement de l'application de l'agent Citrix Secure Access a échoué en raison d'une adresse IP non valide	Le lancement de l'application de l'agent Citrix Secure Access a échoué en raison d'une adresse IP non valide
0x10000001, 0x10000002, 0x10000003, 0x10000004	Échec de la connexion du client Citrix Secure Access en raison d'un problème de réseau	Problème d'accessibilité de la connectivité réseau avec le client Citrix Secure Access

Code d'information	Description	Résolution
0x10000006	Échec de la connexion du client Citrix Secure Access en raison d'un proxy au milieu	Le serveur proxy interfère avec la connectivité du client avec le service
0x10000007	Échec de la connexion du client Citrix Secure Access en raison d'une autorité de certification non approuvée	Un problème de certificat de serveur non approuvé est observé
0x10000008	Échec de la connexion au client Citrix Secure Access en raison d'un certificat non valide	Un problème de certificat de serveur non valide est observé
0x1000000A	Échec de la connexion au client Citrix Secure Access en raison d'un problème de configuration	La connexion a échoué car la configuration est vide pour l'utilisateur
0x1000000B	Échec de la connexion du client Citrix Secure Access en raison d'un échec de connexion	Connexion interrompue par le réseau ou l'utilisateur final
0x10000010	Échec de la connexion au client Citrix Secure Access en raison d'une session expirée	Le téléchargement de la configuration a échoué car la session a expiré
0x10000013	Échec de la connexion au client Citrix Secure Access en raison d'une liste de configuration trop longue	Le client Citrix Secure Access n'a pas pu se connecter
0x11000003	Échec de la connexion du client Citrix Secure Access en raison d'un échec de création du canal de contrôle	L'établissement du canal de contrôle a échoué car la session a expiré
0x11000004	Échec de connexion du client Citrix Secure Access en raison de l'échec de la création du canal de contrôle	Échec de l'établissement du canal de contrôle
0x11000005	Échec de connexion du client Citrix Secure Access en raison de l'échec de la création du canal de contrôle	Échec de l'établissement du canal de contrôle

Code d'information	Description	Résolution
0x11000006	Échec de connexion du client Citrix Secure Access en raison de l'échec de la création du canal de contrôle	L'établissement du canal de contrôle a échoué en raison d'un problème de réseau
0x12000001	Échec de la déconnexion du client Citrix Secure Access car la session a déjà expiré	Impossible de se déconnecter car la session est terminée
0x12000002	Échec de la déconnexion du client Citrix Secure Access car la session a déjà expiré	La session est interrompue de force
0x13000001	L'accès à l'application a échoué car la session a expiré	Le lancement de l'application a échoué car la session a expiré
0x13000002	L'accès à l'application a échoué en raison d'une licence inadéquate	Le lancement de l'application a échoué en raison d'un problème de licence
0x13000003, 0x13000008, 0x001800DF	L'accès à l'application a échoué car l'accès est interdit, le lancement de l'application TCP/UDP est refusé conformément à la politique	Le lancement de l'application a échoué car l'accès est refusé par le service
0x13000004, 0x13000005	L'accès à l'application a échoué car le serveur n'est pas disponible	Le lancement de l'application a échoué car le client ne parvient pas à accéder au service
0x13000007	L'accès à l'application a échoué car la politique d'accès est désactivée ou l'utilisateur n'est pas abonné	Le lancement de l'application a échoué car l'évaluation de la politique et la validation de la configuration ont échoué
0x13000009	L'accès à l'application a échoué car l'entrée de routage est manquante	Le lancement de l'application a échoué en raison de problèmes dans la table des domaines d'application
0x1300000B	Le client a fermé la connexion	Le client a fermé la connexion avec le service Secure Private Access

Code d'information	Description	Résolution
0x1300000C	La résolution FQDN sur ZTNA a échoué	Impossible de résoudre le FQDN par le serveur DNS
0x001800D3	Échec du téléchargement de la configuration des applications lors de la connexion	Échec de la récupération de la liste des destinations d'application configurées
0x001800D9, 0x001800DA	Le lancement de l'application TCP/UDP a échoué lors de l'analyse de la réponse d'évaluation de la politique, le lancement de l'application TCP/UDP a échoué avec un résultat non valide lors de l'évaluation de la politique	Problème de configuration de l'application
0x001800DB	Le lancement de l'application TCP/UDP a échoué avec une configuration d'emplacement de ressource non valide	Problème avec l'emplacement des ressources
0x13000006, 0x001800DC, 0x001800DD	Le lancement de l'application TCP a échoué en raison d'une politique de sécurité renforcée non prise en charge configurée pour l'application. Le lancement de l'application TCP a échoué en raison d'une redirection du service de navigateur sécurisé non prise en charge configurée pour l'application TCP.	La politique de sécurité renforcée est liée à l'application HTTP
0x001800DE	Le lancement de l'application TCP/UDP a échoué car aucune configuration d'application n'a été trouvée pour la destination	Impossible de localiser l'application
0x001800EA	Le lancement de l'application TCP a échoué car le nom de domaine complet de destination est trop long	La longueur du nom d'hôte dépasse 256 caractères

Code d'information	Description	Résolution
0x001800ED	Le lancement de l'application TCP a échoué en raison d'une adresse IP de destination non valide	Adresse IP invalide
0x001800EF	Le lancement de l'application TCP a échoué lors de l'établissement de la connexion au serveur TCP privé	Impossible d'établir une connexion de bout en bout
0x001800F5	Le lancement de l'application UDP a échoué en raison de l'adresse IPV6	IPv6 reçu dans la demande d'application
0x001800F9	Le trafic UDP n'a pas pu être transmis car la connexion client est perdue	Le trafic UDP n'a pas pu être livré
0x001800FF	La livraison du trafic de données UDP a échoué	La livraison du trafic de données UDP a échoué
0x10000401	Échec de la numérotation du serveur de rendez-vous Citrix	Le lancement de l'application a échoué en raison de problèmes de connectivité réseau
0x10000402, 0x1000040C	Impossible d'enregistrer le Connector Appliance, échec d'initialisation de la connexion réseau UDP	L'appareil connecteur n'a pas pu s'enregistrer auprès du service Secure Private Access
0x10000403, 0x10000404, 0x10000407, 0x1000040A 0x1000040B, 0x1000040F, 0x10000410	Erreur de connexion, Échec de transmission du paquet de contrôle, Erreur de lecture du service de passerelle, Échec d'analyse du paquet de contrôle,	Problème de connectivité avec l'appareil Connector
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412	Back-end inaccessible, échec de transmission du paquet UDP, échec de réception du paquet UDP, erreur d'écriture du passerelle	Problèmes de connectivité avec Connector Appliance et les serveurs TCP/UDP privés back-end
0x10000406	La résolution DNS a échoué	L'appareil connecteur ne parvient pas à résoudre le DNS pour les noms de domaine complets
0x10000411	Le service de passerelle a fermé la connexion	Connexion au serveur privé interrompue

Code d'information	Description	Résolution
0x10000413	Erreur dans la détermination de la raison de la suppression de la connexion	Impossible de se connecter ou d'envoyer des données à l'adresse IP ou au nom de domaine complet du service privé
0x100508	Le contexte utilisateur ne correspond pas aux conditions de la règle d'accès	Aucune condition de politique correspondante
0x100509	Politique d'accès non associée à l'application	Aucune politique d'accès associée à l'application
0x10050C	Résultats de l'évaluation des politiques de plusieurs applications auxquelles l'utilisateur pourrait avoir droit	Informations sur l'énumération des applications
0x00180101	Le lancement de l'application TCP/UDP a échoué car l'entrée de routage est manquante dans la table du domaine d'application	Le lancement de l'application TCP/UDP a échoué car l'entrée de routage est manquante dans la table du domaine d'application
0x00180102	Le lancement de l'application TCP/UDP a échoué car les connecteurs ne sont pas sains	Le lancement de l'application TCP/UDP a échoué car les connecteurs ne sont pas sains
0x00180103	La requête UDP/DNS a échoué, car le connecteur est inaccessible	La requête UDP/DNS a échoué, car le connecteur est inaccessible
0x20580001	Impossible de charger la page car le cookie NGS a expiré	Impossible de charger la page car le cookie NGS a expiré
0x20580002	La récupération de la politique d'accès a échoué en raison d'une défaillance du réseau	La récupération de la politique d'accès a échoué en raison d'une défaillance du réseau
0x20580003	La récupération de la politique d'accès a échoué lors de l'analyse du jeton Web JSON	La récupération de la politique d'accès a échoué lors de l'analyse du jeton Web JSON

Code d'information	Description	Résolution
0x20580004	Échec du réseau lors de la récupération des détails de la politique d'accès	Échec du réseau lors de la récupération des détails de la politique d'accès
0x20580005	La récupération de la politique a échoué lors de la récupération du certificat public	La récupération de la politique a échoué lors de la récupération du certificat public
0x20580007	La récupération de la politique a échoué lors de la validation de la signature du JWT	La récupération de la politique a échoué lors de la validation de la signature du JWT
0x20580008	La récupération de la politique a échoué lors de la validation du certificat public	La récupération de la politique a échoué lors de la validation du certificat public
0x2058000A	Impossible de déterminer l'environnement du magasin pour former une URL de politique	Impossible de déterminer l'environnement du magasin pour former une URL de politique
0x2058000B	Impossible d'obtenir la réponse à la demande de récupération de la politique d'accès	Impossible d'obtenir la réponse à la demande de récupération de la politique d'accès
0x2058000C	La récupération de la politique d'accès a échoué en raison d'un jeton d'authentification DS secondaire expiré	La récupération de la politique d'accès a échoué en raison d'un jeton d'authentification DS secondaire expiré
0x10200002	L'appareil connecteur n'est pas enregistré	L'appareil connecteur n'est pas enregistré
0x10200003	Impossible de se connecter à l'appareil connecteur	Impossible de se connecter à l'appareil connecteur
0x10000301	La connexion au service Citrix SPA a échoué	La connexion au service Citrix Secure Private Access a échoué
0x10000303, 0x10000304	Le serveur proxy n'est pas accessible	Le serveur proxy n'est pas accessible

Code d'information	Description	Résolution
0x10000305	L'authentification du serveur proxy a échoué	L'authentification du serveur proxy a échoué
0x10000306	Les serveurs proxy configurés ne sont pas accessibles	Les serveurs proxy configurés ne sont pas accessibles
0x10000307	Réponse d'erreur reçue du serveur principal	Réponse d'erreur reçue du serveur principal
0x10000005	Impossible d'envoyer la requête à l'URL cible	Impossible d'envoyer la requête à l'URL cible
0x10000107	Échec du traitement de l'authentification unique	Échec du traitement de l'authentification unique
0x10000108, 0x1000010B	Échec du traitement de l'authentification unique, impossible de déterminer les paramètres de l'authentification unique	Échec du traitement de l'authentification unique, impossible de déterminer les paramètres de l'authentification unique
0x10000101, 0x10000102, 0x10000103, 0x10000104	Échec de l'authentification unique de FormFill, configuration incorrecte de l'application de formulaire	Échec de l'authentification unique de FormFill, configuration incorrecte de l'application de formulaire
0x1000010A	Échec de l'authentification unique de FormFill, configuration incorrecte de l'application de formulaire	Échec de l'authentification unique de FormFill, configuration incorrecte de l'application de formulaire
0x10000202	Échec de l'authentification unique Kerberos	Échec de l'authentification unique Kerberos
0x10000203	Échec du traitement de l'authentification unique pour le type d'authentification	Échec du traitement de l'authentification unique pour le type d'authentification
0x10000204	Kerberos SSO a échoué mais revient à NTLM	Kerberos SSO a échoué mais revient à NTLM
0x14000001	Plusieurs comptes éligibles ZTNA configurés dans l'application Citrix Workspace	Plusieurs comptes éligibles ZTNA configurés dans l'application Citrix Workspace

Étapes de résolution

Les sections suivantes fournissent des étapes de résolution pour la plupart des codes d'information. Pour les codes dont les étapes de résolution ne sont pas capturées, contactez le support Citrix.

Une ou plusieurs applications non répertoriées dans le tableau de bord de l'utilisateur

Code d'information : 0x180055, 0x1800DF, 0x1800E3

En raison des paramètres de politique contextuels, les applications peuvent ne pas être visibles pour certains utilisateurs ou appareils. Des paramètres tels que les facteurs de confiance (position de l'appareil ou score de risque) peuvent affecter l'accessibilité des applications.

1. Copiez l'ID de transaction de la colonne `raisons` pour le code d'erreur `0x18005C` dans le fichier csv des journaux de diagnostic.
2. Modifiez le filtre de colonne `prod` dans le fichier csv pour afficher les événements du composant appelé `SWA.PSE` ou `SWA.PSE.EVENTS`. Ce filtre affiche uniquement les journaux liés à l'évaluation des politiques.
3. Recherchez la charge utile de la politique évaluée dans la colonne `raison` . Cette charge utile affiche la politique évaluée pour le contexte de l'utilisateur pour toutes les applications auxquelles l'utilisateur est abonné.
4. Si l'évaluation de la politique indique que l'application est refusée pour l'utilisateur, les raisons possibles peuvent être :

    - Conditions de correspondance incorrectes dans la stratégie - vérifiez la configuration de la stratégie d'application dans Citrix Cloud
    - Règles de correspondance incorrectes dans la stratégie - vérifiez la configuration de la stratégie d'application dans Citrix Cloud
    - Règle de correspondance par défaut incorrecte dans la politique : il s'agit d'un cas de défaillance. Ajustez les conditions en conséquence.

L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS

Code d'information : 0x1800BC, 0x1800BF

L'utilisateur a peut-être cliqué sur le lien de l'application pour laquelle il n'a peut-être pas d'abonnement.

Assurez-vous que l'utilisateur dispose d'un abonnement aux applications.

1. Accédez à l'application dans le portail de gestion.
2. Modifiez l'application et accédez à l'onglet **Abonnement** .
3. Assurez-vous que l'utilisateur ciblé dispose d'une entrée dans la liste d'abonnement.

Ralentissement des performances de l'application back-end

Code d'information :0x18000F

Il existe des cas où le réseau client est instable en raison des connecteurs d'un emplacement de ressource qui peuvent être en panne ou du fait que le serveur principal lui-même peut ne pas répondre.

1. Assurez-vous que l'appareil connecteur est positionné géographiquement à proximité du serveur principal pour éliminer les latences du réseau.
2. Vérifiez si le pare-feu du serveur back-end ne bloque pas le dispositif de connexion.
3. Vérifiez si le client se connecte au POP cloud le plus proche.

   Par exemple, `nslookup nssvc.dnsdiag.net` sur le client, le nom canonique dans la réponse indique le serveur géo-spécifique tel que `aws-us-wgnssvc.net`.

Le lancement de l'application a échoué car la longueur du nom de domaine complet de l'application a été dépassée

Code d'information : 0x180006, 0x1800B7

Les noms de domaine complets des applications ne doivent pas dépasser 512 caractères. Vérifiez le FQDN de l'application dans la page de configuration de l'application. Assurez-vous que la longueur ne dépasse pas 512 octets.

1. Accédez à l'onglet **Applications** sur la console de gestion.
2. Recherchez l'application dont le FQDN dépasse 512 caractères.
3. Modifiez l'application et corrigez la longueur du FQDN de l'application.

La longueur des détails de l'application a été dépassée

Code d'information : 0x18000E

Vérifiez les politiques si elles bloquent l'accès à l'application.

1. Accédez à **Politiques d'accès**.
2. Recherchez les politiques auxquelles l'application a droit.
3. Consultez les règles et conditions de la politique pour l'utilisateur final.

L'accès à l'application est refusé

Code d'information : 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

Cela est lié aux politiques contextuelles, où les politiques refusent l'application pour un utilisateur donné.

Vérifiez les politiques si elles bloquent l'accès à l'application

1. Accédez à **Politiques d'accès**.
2. Recherchez les politiques auxquelles l'application a droit.
3. Consultez les règles et conditions de la politique pour l'utilisateur final.

Applications non énumérées

Les applications peuvent être manquantes dans la liste énumérée en raison de refus de politique ou si l'intégration Secure Private Access n'est pas activée.

- Si l'accès doit être activé pour certaines applications mais que vous ne voyez aucune application, essayez d'activer l'intégration Secure Private Access.
  - Connectez-vous à Citrix Cloud.
  - Sélectionnez **Configuration de l'espace de travail** dans le menu hamburger, puis cliquez sur **Intégrations de services**.
  - Cliquez sur le bouton points de suspension dans Secure Private Access, puis cliquez sur **Activer**.
- Si l'intégration Secure Private Access est déjà activée, désactivez-la, puis réactivez-la pour voir si vous avez des applications.

Problème de connexion à l'appareil Connector

Code d'information : 0x1800EF

Le routage des applications échoue en raison de la non-disponibilité des connexions TCP avec les connecteurs sur site.

Examiner les événements du composant du contrôleur

1. Recherchez l'ID de transaction " pour le code d'erreur `0x1800EF` dans le fichier csv des journaux de diagnostic.
2. Filtrer tous les événements correspondant à l'ID de transaction dans le fichier csv.
3. Filtrez également la colonne `prod` dans le fichier csv qui correspond à `SWA.GOCTRL`.

   Si vous voyez des événements avec le message `connectType multiconnect::success`? alors;

- Cela indique que la demande d'établissement du tunnel a été relayée avec succès au contrôleur.
- Vérifiez si l'emplacement de la ressource " dans le message de journal est correct. Si cela est incorrect, corrigez l'emplacement de la ressource dans la section de configuration de l'application sur le portail de gestion Citrix.
- Vérifiez si l'adresse IP VDA `et le port` dans le message de journal sont corrects. L'adresse IP et le port VDA indiquent l'adresse IP et le port de l'application back-end. Si le nom de domaine complet ou l'adresse IP de l'application est incorrect, corrigez-le dans la section de configuration de l'application sur le portail de gestion Citrix.
- Passez à l'examen des événements du connecteur si vous ne trouvez aucun des problèmes mentionnés précédemment.

Si vous voyez des événements avec le message `connectType connect::failure` ou `multiconnect::success`, alors ;

- Vérifiez si le correctif recommandé pour ce message de journal indique - `Vérifiez si le connecteur est toujours connectéau même pop`. Cela indique que le connecteur à l'emplacement de la ressource est peut-être tombé en panne. Procédez à la révision des événements du connecteur .
- Contactez le support client Citrix si les messages mentionnés précédemment ne s'affichent pas.

Si vous voyez des événements avec le message `connectType IntraAll::failure`, contactez le support client Citrix.

Examiner les événements du composant connecteur

1. Recherchez l'ID de transaction " pour le code d'erreur `0x1800EF` dans le fichier csv des journaux de diagnostic.
2. Filtrer tous les événements correspondant à l'ID de transaction dans le fichier csv.
3. Filtrez également la colonne `prod` dans le fichier csv qui correspond à `SWA.ConnectorAppliance.WebApps`.
4. Si vous voyez des événements avec un statut `comme un échec`, alors ;

   - Consultez le message de raison " pour chacun de ces événements d'échec.
   - `UnableToRegister` indique que le connecteur n'a pas pu s'enregistrer correctement sur Citrix Cloud. Contactez le support Citrix.
   - `IsProxyRequiredCheckError` ou `ProxyDialFailed` ou `ProxyConnectionFailed` ou `ProxyAuthenticationFailure` ou `ProxiesUnReachable` indique que le connecteur n'a pas pu résoudre l'URL du back-end via la configuration du proxy. Vérifiez que la configuration du proxy est correcte.
   - Pour un débogage plus approfondi, voir Événements SSO du connecteur.

Erreurs d'authentification unique

Pour l'authentification unique, différents attributs SSO de la configuration de l'application sont extraits et appliqués lors du lancement de l'application. Si cet utilisateur particulier ne dispose pas des attributs ou si les attributs sont incorrects, l'authentification unique peut échouer. Assurez-vous que la configuration semble correcte.

1. Accédez à **Politiques d'accès.**
2. Recherchez les politiques auxquelles l'application a droit.
3. Consultez les règles et conditions de la politique pour l'utilisateur final.

Les méthodes SSO telles que Form SSO, Kerberos et NTLM sont exécutées par le connecteur sur site. Consultez les journaux de diagnostic suivants à partir du connecteur.

Examiner les événements SSO à partir du composant connecteur

1. Filtrez le nom du composant " dans le fichier csv qui correspond à `SWA.ConnectorAppliance.WebApps`.
2. Voyez-vous des événements avec le statut « échec » ?
    - Consultez le message pour chacun de ces événements d'échec.
    - `IsProxyRequiredCheckError` ou `ProxyDialFailed` ou `ProxyConnectionFailed` ou `ProxyAuthenticationFailure` ou `ProxiesUnReachable` indique que le connecteur n'a pas pu résoudre l'URL du back-end via la configuration du proxy. Vérifiez que la configuration du proxy est correcte.
    - `FailedToReadRequest` ou `RequestReceivedForNonSecureBrowse` ou `UnableToRetrieveUserCredentials` ou `CCSPolicyIsNotLoaded` ou `FailedToLoadBaseClient` ou `ProcessConnectionFailure` ou `WebAppUnSupportedAut` indique un échec de tunneling. Contactez le support Citrix.
    - `UnableToConnectTargetServer` indique que le serveur back-end est inaccessible depuis le connecteur. Vérifiez à nouveau la configuration du back-end.
    - `IncorrectFormAppConfiguration` ou `NoLoginFormFound` ou `FailedToConstructForL` ou `FailedToLoginViaFormBasedAuth` indique un échec d'authentification basé sur un formulaire. Consultez la section de configuration SSO du formulaire dans la configuration de l'application dans le portail de gestion Citrix.
    - `NTLMAuthNotFound` indique un échec d'authentification basé sur NTLM. Vérifiez la section de configuration NTLM SSO dans la configuration de l'application dans le portail de gestion Citrix.
    - Pour un débogage plus poussé, voir Événements du connecteur.

Le lancement de l'application a échoué car le service d'authentification est en panne

Code d'information : 0x180022

Secure Private Access permet aux administrateurs de configurer un service d'authentification tiers tel que l'annuaire actif traditionnel, AAD, Okta ou SAML. Les pannes de ces services d'authentification peuvent être à l'origine de ce problème.

Vérifiez si les serveurs tiers sont opérationnels et accessibles.

Échec de l'authentification unique SAML

Code d'information : 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Les utilisateurs sont confrontés à une échec d'authentification lors du lancement de l'application lorsqu'elle est initiée par l'IdP ou peuvent voir des liens inaccessibles lorsqu'elle est initiée par le SP. Vérifiez la configuration de l'application SAML côté service Secure Private Access ainsi que la configuration du fournisseur de services.

Configuration de l'accès privé sécurisé :

1. Accédez à l'onglet **Applications** .
2. Recherchez l'application SAML problématique.
3. Modifiez l'application et accédez à l'onglet **Single Sign On** .
4. Vérifiez les champs suivants.
    - URL d'assertion
    - État du relais
    - Audience
    - Format d'identifiant de nom, identifiant de nom et autres attributs

Configuration du fournisseur de services :

1. Connectez-vous au fournisseur de services.
2. Accédez à **Paramètres SAML.**
3. Vérifiez le certificat IdP, l'audience et l'URL de connexion IdP.

Si la configuration semble correcte, contactez le support Citrix.

Nom de domaine complet de l'application non valide

Code d'information : 0x180048

L'administrateur client a peut-être fourni un nom de domaine complet non valide ou un nom de domaine complet pour lequel la résolution DNS échoue sur le serveur principal.

Dans ce cas, l'utilisateur final voit une erreur sur la page Web. Vérifiez les paramètres de l'application.

Validation d'application SaaS Vérifiez si l'application est accessible depuis le réseau.

Validation d'application Web

1. Accédez à l'onglet **Applications** .
2. Modifiez l'application problématique.
3. Accédez à la page **Détails de l'application** .
4. Vérifiez l'URL. L'URL doit être accessible soit sur intranet soit sur Internet.

Service de navigation sécurisé - Échec de la recherche/connexion DNS

Code d'information : 0x18009D

Expérience de navigation interrompue via le service d'isolation du navigateur à distance. Vérifiez le serveur back-end auquel l'utilisateur final tente de se connecter.

1. Accédez au serveur back-end et vérifiez s'il est opérationnel et s'il est capable de recevoir les demandes.
2. Vérifiez les paramètres proxy s'ils arrêtent la connexion au serveur principal.

> **Remarque**
>
> Le service Citrix Remote Browser Isolation était anciennement connu sous le nom de service Secure Browser.

CWA Web - Erreurs de recherche/connexion DNS pour les applications Web

Code d'information : 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Expérience de navigation interrompue des applications Web exécutées au sein d'un réseau d'entreprise.

1. Filtrez les journaux de diagnostic pour les noms de domaine complets qui ne peuvent pas être résolus.
2. Vérifiez l'accessibilité du serveur back-end depuis l'intérieur du réseau d'entreprise.
3. Vérifiez les paramètres proxy pour voir si le connecteur est bloqué et ne peut pas atteindre le serveur principal.

Accès direct –Mal configuré comme application Web

Étant donné que le trafic des applications Web est toujours acheminé via le connecteur, la configuration de l'accès direct sur ces derniers entraîne une erreur d'accès à l'application.

Vérifiez la configuration conflictuelle entre la table de domaine de routage et la configuration de l'application.

1. Accédez à l'application dans le portail de gestion.
2. Modifiez l'application et vérifiez si l'accès direct est activé.
3. Vérifiez le nom de domaine complet de l'application dans la table des domaines de routage s'il a été marqué comme interne.

L'utilisateur n'est pas autorisé à accéder à l'application Web/SaaS pour DirectAccess

Code d'information : 0x1800BD

La configuration de l'application désactive l'accès direct au trafic provenant de clients basés sur un navigateur.

Assurez-vous que l'utilisateur dispose d'un abonnement aux applications.

1. Accédez à l'application dans le portail de gestion.
2. Modifiez l'application et vérifiez la configuration de l'accès sans agent.

Politiques de sécurité renforcées - Mauvaise configuration du service de navigation sécurisée

Code d'information : 0x1800C3

Comportement incorrect observé par rapport à ce qui était prévu par les règles de politique. Vérifiez les politiques d'accès contextuelles.

1. Accédez à l'onglet **Politiques** .
2. Vérifiez les politiques associées à l'application.
3. Vérifiez les règles de ces politiques.

Politiques de sécurité renforcées –mauvaise configuration des politiques

Comportement incorrect observé par rapport à ce qui était prévu par les règles de politique. Vérifiez les paramètres de sécurité renforcés.

1. Accéder à l'application.
2. Cliquez sur l'onglet **Politiques d'accès** .
3. Vérifiez les paramètres dans la section **Restrictions de sécurité disponibles :** .

Le lancement de la session de l'agent Citrix Secure Access a échoué lors de la récupération de la configuration de l'application

Code d'information : 0x1800D0

L'application Citrix Secure Access ne parvient pas à établir avec succès un tunnel complet vers Citrix Cloud.

1. Vérifiez la configuration du domaine de routage pour les applications TCP/UDP.
2. Assurez-vous que le nombre maximum d'entrées est bien dans la limite de 16 000.

Applications TCP/UDP –Requêtes client mal formées

Code d'information : 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

Soit le tunnel VPN n'est pas établi, soit certains FQDN peuvent ne pas être tunnelés.

1. Assurez-vous que les demandes ne sont pas fabriquées ou reconstruites par des proxys intermédiaires.
2. Suspicion d'attaques de type « man-in-middle ».

Applications TCP/UDP - Mauvaise configuration de la redirection du service de navigation sécurisé

Code d'information : 0x1800DD

Les redirections du service d'isolation du navigateur à distance ne peuvent être appliquées qu'aux applications Web et non aux applications TCP/UDP. Vérifiez la configuration de l'application dans l'interface graphique du service Secure Private Access.

> **Remarque**
>
> Le service Citrix Remote Browser Isolation était anciennement connu sous le nom de service Secure Browser.

Le lancement de l'application de l'agent Citrix Secure Access a échoué lors de l'évaluation de la stratégie

Code d'information : 0x1800DE

Assurez-vous que tous les noms de domaine complets internes qui doivent être tunnelisés par le client Citrix Secure Access ont une entrée correspondante dans la table de domaine de routage.

Le lancement de l'application de l'agent Citrix Secure Access a échoué car IPv6 n'est pas pris en charge

Code d'information : 0x1800EB

Vérifiez les entrées du domaine de routage. Assurez-vous qu'il n'y a pas d'entrées IPV6 dans la table.

Le lancement de l'application de l'agent Citrix Secure Access a échoué en raison d'une adresse IP non valide

Code d'information :0x1800EC, 0x1800ED

Vérifiez les entrées du domaine de routage. Assurez-vous que les adresses IP sont valides et pointent vers le bon back-end.

Problème d'accessibilité de la connectivité réseau avec le client Citrix Secure Access

Code d'information : 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Vérifiez si le réseau de la machine cliente est accessible. Si le réseau est accessible, contactez le support Citrix avec les journaux de débogage du client.
2. Vérifiez si le proxy ou le pare-feu bloque le réseau.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Le serveur proxy interfère avec la connectivité du client avec le service

Code d'information : 0x10000006

1. Vérifiez si le réseau de la machine cliente est accessible.
2. Vérifiez si le proxy est correctement configuré dans le client.
3. S'il n'y a aucun problème avec les deux, contactez le support Citrix avec les journaux de débogage du client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Un problème de certificat de serveur non approuvé est observé

Code d'information : 0x10000007

Contactez le support Citrix pour vérifier si le certificat du serveur est correctement généré par une autorité de certification valide.

Un problème de certificat de serveur non valide est observé

Code d'information : 0x10000008

Contactez le support Citrix pour vérifier si le certificat du serveur est auto-signé, expiré ou provient d'une source non fiable.

La connexion a échoué car la configuration est vide pour l'utilisateur

Code d'information : 0x1000000A

1. Assurez-vous qu'au moins une application TCP/UDP/HTTP est configurée. Pour plus de détails, voir Ajouter et gérer des applications.
2. Assurez-vous que la table Domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**) n'est pas vide ou que toutes les entrées ne sont pas désactivées. Les destinations configurées dans l'application TCP/UDP/HTTP sont automatiquement ajoutées à cette table.

Il est recommandé de ne pas supprimer ou désactiver les destinations ou l'URL d'une application TCP/UDP/HTTP active.

Connexion interrompue par le réseau et/ou l'utilisateur final

Code d'information : 0x1000000B

Vérifiez si le réseau est interrompu ou si l'utilisateur final a annulé la connexion pendant la connexion à la session ZTNA.

Le téléchargement de la configuration a échoué car la session a expiré

Code d'information : 0x10000010

La session VPN a peut-être expiré pendant la demande de téléchargement de la configuration de la session ZTNA. Essayez de vous reconnecter au client Citrix Secure Access.

Le client Citrix Secure Access n'a pas pu se connecter

Code d'information : 0x10000013

Le client Citrix Secure Access n'a pas pu se connecter car la taille de la configuration dépasse la limite de configuration maximale.

1. Vérifiez la configuration du domaine de routage pour les applications TCP/UDP dans **Accès privé sécurisé > Paramètres > Domaine d'application**
2. Assurez-vous que le nombre d'entrées ne soit pas énorme. Si la liste des entrées est énorme, désactivez ou supprimez les destinations inutilisées.

   Si la liste de destination doit contenir plus de 1 000 éléments, essayez d'augmenter la taille maximale de téléchargement de configuration en mettant à jour la clé de registre ConfigSize. Pour plus de détails, consultez Clés de registre du client VPN Citrix Gateway.

L'établissement du canal de contrôle a échoué car la session a expiré

Code d'information : 0x11000003

Le canal de contrôle pour l'établissement de la requête DNS a échoué car la session a expiré.

La session ZTNA a peut-être expiré pendant la configuration du canal de contrôle.

Essayez de vous reconnecter au client Citrix Secure Access.

Échec de l'établissement du canal de contrôle

Code d'information : 0x11000004

Le canal de contrôle pour l'établissement de la requête DNS a échoué.

- **Maintenir l'emplacement des ressources en bon état :**

1. Connectez-vous à Citrix Cloud.
2. Cliquez sur **Emplacement de la ressource** dans le menu hamburger.
3. Exécutez une vérification de l'état des appareils connecteurs sur l'emplacement de ressource correspondant.
4. Si cela ne résout pas le problème, essayez de redémarrer la machine virtuelle du connecteur.

- **Maintenir l'appareil connecteur HA :**

1. Connectez-vous à Citrix Cloud.
2. Cliquez sur **Emplacement de la ressource** dans le menu hamburger.
3. Assurez-vous que l'emplacement de la ressource prévu dispose d'au moins deux appareils de connexion.

Assurez-vous de ce qui suit :

- L'emplacement des ressources LAN est en état de fonctionnement.
- Aucun pare-feu ou proxy ne se trouve au milieu bloquant le Connector Appliance vers le service ou les serveurs back-end.

- Le réseau client est sain.
- Les serveurs privés back-end sont opérationnels.
- Les serveurs DNS sont opérationnels.
- Les FQDN sont résolubles.

Si vous respectez les recommandations précédentes, procédez comme suit.

1. Récupérez l'ID de transaction à partir du journal de diagnostic pour cette erreur.
2. Filtrez tous les événements correspondant à l'ID de transaction dans le tableau de bord Secure Private Access.
3. Vérifiez si une erreur s'est produite dans les journaux de diagnostic du client, de l'appliance connecteur ou du service, correspondant à l'ID de transaction. Prenez ensuite les mesures appropriées en conséquence.
4. Vérifiez si l'emplacement de la ressource est choisi correctement pour la destination dans la table du domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**).
5. Vérifiez si l'application est configurée avec le port, les plages IP et les domaines corrects. Pour plus de détails, voir Ajouter et gérer des applications.

Si vous ne parvenez toujours pas à résoudre le problème, contactez le support Citrix avec le code d'erreur correspondant à l'ID de transaction et aux journaux client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Échec de l'établissement du canal de contrôle

Code d'information : 0x11000005

L'établissement du canal de contrôle (pour la requête DNS) a échoué.

1. Vérifiez les droits de licence du service Secure Private Access.
2. Si vous n'y avez pas droit, contactez le support Citrix pour vérifier la licence.

Pour plus de détails, consultez la section https://www.citrix.com/buy/licensing/product.html.

L'établissement du canal de contrôle a échoué en raison d'un problème de réseau

Code d'information : 0x11000006

L'établissement du canal de contrôle (pour la requête DNS) a échoué en raison d'un problème de réseau.

1. Vérifiez si le service Secure Private Access est accessible.

2. Si vous n'êtes pas joignable, contactez le support Citrix avec le code d'erreur et les journaux du client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

L'établissement du canal de contrôle a échoué en raison d'IIP insuffisants

Code d'information : 0x11000007

L'établissement du canal de contrôle (pour la requête DNS) a échoué en raison d'IIP insuffisantes.

Contactez le support Citrix avec le code d'erreur et les journaux du client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Impossible de se déconnecter car la session est terminée

Ce problème peut s'être produit parce que la machine cliente (clavier ou souris) était inactive pendant une période supérieure au délai d'expiration configuré.

Code d'information : 0x12000001

Essayez de vous reconnecter au client Citrix Secure Access.

La session est interrompue de force

La session est interrompue de force car le délai d'expiration forcé configuré est atteint.

Code d'information : 0x12000002

Essayez de vous reconnecter au client Citrix Secure Access.

Le lancement de l'application a échoué car la session a expiré

Code d'information : 0x13000001

1. La session ZTNA a expiré pendant le lancement de l'application.
2. Essayez de vous reconnecter au client Citrix Secure Access.

Le lancement de l'application a échoué en raison d'un problème de licence

Code d'information : 0x13000002

1. Vérifiez si la licence du service Secure Private Access est valable.

2. Si vous n'y avez pas droit, contactez le support Citrix pour vérifier la licence.

Pour plus de détails, consultez la section https://www.citrix.com/buy/licensing/product.html.

Le lancement de l'application a échoué car l'accès est refusé par le service

Code d'information : 0x13000003, 0x13000008, 0x001800DF

Le lancement de l'application est refusé conformément à la configuration de la politique pour l'utilisateur et l'application.

Assurez-vous de ce qui suit .

- Les mêmes destinations ne sont pas utilisées dans plusieurs applications (HTTP, HTTPS, TCP, UDP)
- Il n'y a pas de destinations qui se chevauchent sur plusieurs applications.
- Les politiques d'accès sont liées aux applications.

Vérifiez également les conditions et les actions des politiques configurées pour l'application refusée. Passez ensuite en revue les conditions et les actions de la politique.

Pour plus de détails, voir Politiques d'accès.

Le lancement de l'application a échoué car le client ne parvient pas à accéder au service

Code d'information : 0x13000004, 0x13000005

1. Vérifiez si le service d'accès privé sécurisé est accessible.
2. Relancez l'application.
3. Si l'application n'est pas accessible pendant une longue période, contactez le support Citrix avec le code d'erreur et les journaux client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Le lancement de l'application a échoué car l'évaluation de la politique et la validation de la configuration ont échoué

Code d'information : 0x13000007

Le lancement de l'application a échoué car l'évaluation de la politique et la validation de la configuration ont échoué par le service Secure Private Access.

Impossible de repérer l'application pour la destination consultée.

Le lancement de l'application a échoué car l'accès est refusé par le service.

Le lancement de l'application a échoué en raison de problèmes dans la table des domaines d'application

Code d'information : 0x13000009

Le lancement de l'application a échoué car la table du domaine d'application ne contient pas d'entrée pour la destination consultée.

Vérifiez que l'entrée d'itinéraire est correctement configurée pour l'application dans **Accès privé sécurisé > Paramètres > Domaine d'application**.

Le client a fermé la connexion avec le service Secure Private Access

Code d'information : 0x1300000B

1. Vérifiez si l'utilisateur final a fermé manuellement la connexion.
2. Dans le cas contraire, contactez le support Citrix avec le code d'erreur et les journaux client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

Impossible de résoudre le FQDN par le serveur DNS

Code d'information : 0x1300000C

Ce problème se produit lorsque l'appliance Connector ne parvient pas à résoudre le DNS pour les noms de domaine complets.

1. Vérifiez l'entrée DNS pour le FQDN de l'application concernée dans le serveur DNS.
2. Assurez-vous qu'un serveur DNS approprié est configuré dans les appareils Connector. Pour plus de détails, voir Configuration des paramètres réseau sur la page d'administration de Connector Appliance.

Impossible de localiser l'application

Code d'information : 0x001800DE

Il se peut que vous ne puissiez pas localiser l'application correspondant à la destination à laquelle l'utilisateur a accédé. Cela peut se produire si le mappage de la destination vers l'emplacement des ressources est manquant dans la table du domaine d'application.

- Assurez-vous que l'application TCP/UDP ou HTTP est configurée pour la destination accessible.
- Assurez-vous que l'utilisateur dispose d'un abonnement à l'application pour la destination consultée.

1. Accédez à l'application dans le portail de gestion.
2. Modifiez l'application et accédez à l'onglet **Abonnement** .
3. Assurez-vous que l'utilisateur ciblé dispose d'une entrée dans la liste d'abonnement.
4. Assurez-vous que la table **Domaine d'application** possède la destination et l'emplacement de ressource approprié.

Échec de la récupération de la liste des destinations d'application configurées

Code d'information : 0x001800D3

- Assurez-vous qu'au moins une application TCP/UDP/HTTP est configurée. Pour plus de détails, voir Ajouter et gérer des applications.
- Assurez-vous que la page du tableau Domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**) n'est pas vide ou que toutes les entrées ne sont pas désactivées. Les destinations configurées dans l'application TCP/UDP/HTTP sont automatiquement ajoutées à cette table. Il est recommandé de ne pas supprimer ou désactiver les destinations ou URL des applications TCP/UDP/HTTP actives dans la table des domaines d'application.

Problème de configuration de l'application

La configuration de l'application contient un caractère spécial ou un problème de configuration de politique.

Code d'information : 0x001800D9, 0x001800DA

Assurez-vous de ce qui suit :

- La configuration de l'application ne contient pas de caractères non pris en charge.
- L'adresse IP de destination ou la plage d'adresses IP ou le CIDR IP sont valides.
- La destination de l'application est activée dans la table Domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**).
- Les politiques sont configurées et liées à l'application respective.
- La configuration de la politique d'accès est correcte.

Problème avec l'emplacement des ressources

Code d'information : 0x001800DB

- Assurez-vous qu'un emplacement de ressource est configuré.

    1. Dans le menu hamburger de Citrix Cloud, sélectionnez **Emplacement des ressources**.

2. Assurez-vous que l'emplacement de la ressource attendu est configuré et que l'emplacement de la ressource est dans un état actif.

- Assurez-vous qu'un emplacement de ressource correct est sélectionné pour la destination dans la table Domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**).

Les destinations configurées dans l'application TCP/UDP/HTTP sont automatiquement ajoutées à cette table. Il est recommandé de ne pas supprimer ou désactiver les destinations ou URL des applications TCP/UDP/HTTP actives dans la table des domaines d'application.

La politique de sécurité renforcée est liée à l'application HTTP

Code d'information : 0x001800DC, 0x001800DD, 0x13000006

L'application HTTP qui dispose d'une politique de sécurité renforcée est accessible via le client Citrix Secure Access.

- Assurez-vous que la même destination n'est pas utilisée pour les applications TCP/UDP et HTTP.
- Si la politique de sécurité renforcée est activée pour l'application HTTP/HTTPS, il est recommandé d'accéder à l'application uniquement via l'application Citrix Workspace ou le service Citrix Remote Browser Isolation.
- Désactivez le contrôle de sécurité amélioré pour les applications HTTP/HTTPS pour accéder à l'application via le client Citrix Secure Access.
  - Accédez au portail d'administration de Secure Private Access.
  - Cliquez sur l'onglet **Applications** et recherchez le nom de la politique pour l'application HTTP/HTTPS de destination consultée.
  - Cliquez sur l'onglet **Stratégies d'accès** et recherchez le nom de la stratégie identifié précédemment.
  - Sélectionnez la politique et cliquez sur **Modifier**.
  - Modifiez l'action de **Autoriser l'accès avec restriction** à **Autoriser l'accès.**

Pour plus de détails sur la configuration, voir Ajouter et gérer des applications.

> **Remarque**
>
> Le service Citrix Remote Browser Isolation était anciennement connu sous le nom de service Secure Browser.

La longueur du nom d'hôte dépasse 256 caractères

Code d'information : 0x001800EA

Le nom d'hôte reçu dans la demande de lancement de l'application dépasse 256 caractères.

Il est recommandé que les caractères FDQN ne dépassent pas 256 caractères.

Adresse IP invalide

Code d'information : 0x001800ED

L'adresse IP reçue dans la demande de lancement de l'application n'est pas valide.

Il est recommandé d'accéder uniquement à une adresse IP privée valide des clients.

Impossible d'établir une connexion de bout en bout

Code d'information : 0x001800EF

Impossible d'établir une connexion de bout en bout entre le client et le serveur configuré dans l'emplacement de la ressource.

- Assurez-vous que l'emplacement de la ressource est dans un état actif.
  - Dans le menu hamburger de Citrix Cloud, sélectionnez **Emplacement des ressources**.
  - Exécutez une vérification de l'état des appareils connecteurs sur l'emplacement de ressource correspondant.
  - Si cela ne résout pas le problème, redémarrez la machine virtuelle du connecteur.
- Maintenir un appareil de connecteur à haute disponibilité
  - Dans le menu hamburger de Citrix Cloud, sélectionnez **Emplacement des ressources**.
  - Assurez-vous que l'emplacement de la ressource dispose d'au moins deux appareils de connexion.
- Assurez-vous de ce qui suit :
  - L'emplacement des ressources LAN est en état de fonctionnement.
  - Aucun pare-feu ni proxy au milieu ne bloque le Connector Appliance vers le service ou les serveurs back-end.
  - Le réseau de clients est sain.
  - Les serveurs privés back-end sont en bonne santé.
  - Les serveurs DNS sont sains.
  - Les FQDN sont résolubles.

S'il n'y a aucun problème avec ceux-ci, procédez comme suit :

1. Récupérez l'ID de transaction à partir des journaux de diagnostic pour cette erreur.

2. Filtrez tous les événements correspondant à l'ID de transaction dans le tableau de bord du service Secure Private Access.
3. Vérifiez les journaux de diagnostic correspondant à l'ID de transaction à partir du tableau de bord du service Secure Private Access, puis prenez les mesures appropriées en conséquence.
4. Vérifiez qu'un emplacement de ressource correct est sélectionné comme destination dans la table Domaine d'application (**Accès privé sécurisé > Paramètres > Domaine d'application**).
5. Vérifiez si l'application est configurée (**Secure Private Access > Applications**) avec l'adresse IP, le port et le FQDN corrects.

Si aucune de ces étapes ne résout le problème, contactez le support Citrix avec le code d'erreur correspondant à l'ID de transaction et collectez les journaux client.

Pour collecter les journaux de débogage client, consultez Comment collecter les journaux client.

IPv6 reçu dans la demande d'application

Code d'information : 0x001800F5

Une adresse IPv6 est reçue dans la demande d'application et n'est pas prise en charge. Actuellement, seul IPv4 est pris en charge.

Modifiez l'application pour résoudre le problème d'adresse IP de l'application.

1. Accédez au portail d'administration de Secure Private Access.
2. Cliquez sur l'onglet **Applications**.
3. Recherchez l'application et cliquez sur **Modifier**.

Pour plus de détails, voir Ajouter et gérer des applications.

Le trafic UDP n'a pas pu être livré

Code d'information : 0x001800F9

Le trafic UDP n'a pas pu être transmis car la connexion client est perdue

1. Vérifiez si la session client est active.
2. Déconnectez-vous puis reconnectez-vous.

La livraison du trafic de données UDP a échoué

Code d'information : 0x001800FF

- Recherchez l'ID de transaction pour le code d'erreur et filtrez tous les événements correspondant à l'ID de transaction dans le tableau de bord du service Secure Private Access.

- Vérifiez si une erreur s'est produite dans l'autre composant correspondant à l'ID de transaction. Si un problème est détecté dans d'autres composants, prenez les mesures appropriées en conséquence.
- Si cela ne résout pas le problème, contactez le support Citrix avec le code d'erreur ainsi que l'ID de transaction correspondant.

Le lancement de l'application a échoué en raison de problèmes de connectivité réseau

Code d'information : 0x10000401

Échec du lancement de l'application en raison de problèmes de connectivité réseau entre l'appliance Connector et le service Secure Private Access

1. Vérifiez la connectivité Internet publique de l'appareil connecteur.
2. Vérifiez si des règles de proxy ou de pare-feu bloquent la connexion.
3. Si un proxy est à l'origine du problème, contournez-le et essayez à nouveau de lancer l'application.
4. Vérifiez l'état de santé de l'appliance Connector (**Citrix Cloud > Emplacement des ressources**).

Pour plus de détails sur les paramètres réseau, consultez Paramètres réseau de votre appareil Connector.

Le connecteur Appliance n'a pas pu s'enregistrer auprès du service Secure Private Access

Code d'information : 0x10000402, 0x1000040C

1. Accédez à la page d'administration des appareils Connector et vérifiez le résumé du connecteur.
2. Si l'état du connecteur n'est pas bon, accédez à l'emplacement de la ressource dans le portail de gestion.
3. Exécutez une vérification de l'état des appareils connecteurs sur l'emplacement de ressource correspondant.
4. Si le contrôle de santé échoue, redémarrez la machine virtuelle du connecteur.
5. Vérifiez le résumé du connecteur et exécutez à nouveau la vérification de l'état.

Pour plus de détails sur les paramètres réseau, consultez Paramètres réseau de votre appareil Connector.

Problème de connectivité avec l'appareil Connector

Code d'information : 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Recherchez l'ID de transaction pour le code d'erreur.
- Filtrez tous les événements correspondant à l'ID de transaction dans le tableau de bord Secure Private Access.
- Vérifiez si une erreur s'est produite dans l'autre composant correspondant à l'ID de transaction s'il est trouvé, effectuez la solution de contournement correspondante correspondant à ce code d'erreur.
- Si aucune erreur n'est détectée dans les autres composants, procédez comme suit :
  - Accédez à la page d'administration des appareils Connector.
  - Téléchargez le rapport de diagnostic. Pour plus de détails, voir Génération d'un rapport de diagnostic.
  - Capturez la trace du paquet. Pour plus de détails, voir Vérifiez votre connexion réseau.
- Contactez le support Citrix avec ce rapport de diagnostic et le suivi des paquets ainsi que le code d'erreur et l'ID de transaction.

Problèmes de connectivité avec Connector Appliance et les serveurs TCP/UDP privés back-end

Code d'information : 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Connector Appliance a un problème de connectivité avec les serveurs TCP/UDP privés principaux.

- Vérifiez si le serveur back-end auquel l'utilisateur final tente de se connecter est opérationnel et est capable de recevoir les demandes.
- Vérifiez l'accessibilité des serveurs back-end depuis l'intérieur du réseau d'entreprise.
- Vérifiez les paramètres proxy pour voir si le connecteur est bloqué et ne peut pas atteindre le serveur principal.
- Si la demande concerne une application basée sur un nom de domaine complet, vérifiez l'entrée DNS de l'application concernée sur le serveur DNS.

Le connecteur Appliance ne parvient pas à résoudre le DNS pour les noms de domaine complets

Code d'information : 0x10000406

- Vérifiez l'entrée DNS pour le FQDN de l'application concernée dans le serveur DNS.
- Assurez-vous qu'un serveur DNS approprié est configuré dans les appareils Connector. Pour plus de détails, voir Configuration des paramètres réseau sur la page d'administration de Connector Appliance.

Connexion au serveur privé interrompue

Code d'information : 0x10000411

La connexion au serveur privé est interrompue par le client ou le service Secure Private Access.

1. Vérifiez si l'utilisateur final a fermé l'application.
2. Vérifiez les autres journaux de diagnostic correspondant à l'ID de transaction de ce journal et prenez les mesures appropriées en conséquence.
3. Relancez l'application.
4. Si cela ne résout pas le problème, contactez le support Citrix avec le code d'erreur et l'ID de transaction.

Impossible de se connecter ou d'envoyer des données à l'adresse IP ou au nom de domaine complet du service privé

Code d'information : 0x10000413

- Connexion au serveur privé interrompue
- [Problèmes de connectivité avec Connector Appliance et les serveurs TCP/UDP privés principaux](/en-us/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#problèmes-de-connectivité-avec-l'appareil-connecteur-et-les-serveurs-tcpudp-privés-backend). Vérifiez les entrées du domaine de routage. Assurez-vous que les adresses IP sont valides et pointent vers le bon back-end.

Aucune condition de politique correspondante

Code d'information : 0x100508

Le contexte utilisateur ne correspond pas aux conditions de règle d'accès définies dans les politiques attribuées à l'application.

Mettez à jour la configuration de la politique pour qu'elle corresponde au contexte de l'utilisateur.

Aucune politique d'accès associée à l'application

Code d'information : 0x100509

1. Dans l'interface graphique du service Citrix Secure Private Access, cliquez sur **Stratégies d'accès** dans la navigation de gauche.
2. Assurez-vous qu'une politique d'accès est associée à l'application concernée.

3. Si aucune politique d'accès n'est associée à l'application, créez une politique d'accès pour l'application. Pour plus de détails, voir Créer des politiques d'accès.
4. Si cela ne résout pas le problème, contactez le support Citrix.

Aucune configuration d'application trouvée pour le FQDN ou l'adresse IP

Code d'information : 0x10050A

Aucune application correspondante n'a été trouvée pour le FQDN entrant ou la demande d'adresse IP. Par conséquent, l'application est classée comme une application non publiée. Si cela n'est pas prévu, procédez comme suit.

1. Accédez au portail d'administration du service Secure Private Access.
2. Cliquez sur **Applications** dans la navigation de gauche.
3. Recherchez l'application et cliquez sur **Modifier**.
4. Ajoutez un FQDN ou l'adresse IP à l'application. Vous pouvez ajouter le domaine exact, l'adresse IP ou un domaine générique.

   Remarque : L'ajout d'un FQDN ou d'une adresse IP dans **Accès privé sécurisé > Paramètres > Domaine d'application** ne résout pas ce problème. Il doit être ajouté dans le cadre de la configuration de l'application.

Informations sur l'énumération des applications

Code d'information : 0x10050C

Ce code capture les résultats de l'évaluation des politiques de plusieurs applications auxquelles l'utilisateur pourrait avoir droit. L'accès à l'application peut être refusé pour les raisons suivantes :

- Le contexte utilisateur ne correspond pas aux conditions de règle d'accès définies dans les politiques attribuées à l'application. Pour plus de détails, voir Aucune condition de politique correspondante.
- Aucune politique d'accès n'est associée à l'application –Pour plus de détails, voir Aucune politique d'accès associée à l'application.
- Une politique associée à l'application est configurée pour refuser l'accès. Dans ce cas, aucune action n'est requise car cela est prévu.
- Erreur interne inattendue lors de l'application de la politique d'accès. Pour plus de détails, contactez le support Citrix.

Le lancement de l'application TCP/UDP a échoué car l'entrée de routage est manquante dans la table du domaine d'application

Code d'information : 0x00180101

Ce problème peut se produire si la configuration de l'application est présente mais que l'entrée de routage est manquante ou a été précédemment supprimée.

Ajoutez une entrée de routage (**Accès privé sécurisé > Paramètres > Domaine d'application**) pour la destination à laquelle vous accédez.

Le lancement de l'application TCP/UDP a échoué car les connecteurs ne sont pas sains

Code d'information : 0x00180102

Ce problème peut se produire si aucun des connecteurs n'est actif/ne répond à la nouvelle connexion.

Exécutez une vérification de l'état des appareils connecteurs sur l'emplacement de ressource correspondant.

La requête UDP/DNS a échoué car le connecteur est inaccessible

Code d'information : 0x00180103

Ce problème peut se produire si le trafic UDP/DNS ne parvient pas à atteindre le connecteur.

Exécutez une vérification de l'état des appareils connecteurs sur l'emplacement de ressource correspondant.

Impossible de charger la page car le cookie NGS a expiré

Code d'information : 0x20580001

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique d'accès a échoué en raison d'une défaillance du réseau

Code d'information : 0x20580002

1. Vérifiez l'URL et la connexion réseau.
2. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
3. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique d'accès a échoué lors de l'analyse du jeton Web JSON

Code d'information :0x20580003

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

Échec du réseau lors de la récupération des détails de la politique d'accès

Code d'information :0x20580004

1. Vérifiez si la politique d'accès est activée.
2. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
3. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique a échoué lors de la récupération du certificat public

Code d'information : 0x20580005

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique a échoué lors de la validation de la signature du jeton Web JSON

Code d'information : 0x20580007

1. Vérifiez si l'heure du réseau et l'heure de l'appareil utilisateur sont synchronisées.
2. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
3. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique a échoué lors de la validation du certificat public

Code d'information : 0x20580008

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

Impossible de déterminer l'environnement du magasin pour former une URL de stratégie

Code d'information : 0x2058000A

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

Impossible d'obtenir une réponse à la demande de récupération de la politique d'accès

Code d'information : 0x2058000B

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

La récupération de la politique d'accès a échoué en raison d'un jeton d'authentification DS secondaire expiré

Code d'information : 0x2058000C

1. Redémarrez le navigateur et essayez à nouveau d'ouvrir l'application.
2. Si cela ne résout pas le problème, contactez le support Citrix.

L'appareil connecteur n'est pas enregistré

Code d'information : 0x10200002

Vérifiez l'enregistrement de l'appareil Connector.

Pour plus de détails, consultez Enregistrez votre appliance Connector auprès de Citrix Cloud.

Impossible de se connecter à l'appliance Connector

Code d'information : 0x10200003

L'appliance Connector ne parvient pas à communiquer entre Citrix Cloud et les emplacements de ressources.

Vérifiez l'enregistrement du connecteur.

Pour plus de détails, consultez Enregistrez votre appliance Connector auprès de Citrix Cloud.

La connexion au service Citrix Secure Private Access a échoué

Code d'information : 0x10000301

Vérifiez les paramètres réseau du Connector Appliance. Pour plus de détails, voir Paramètres réseau de votre appareil Connector.

Le serveur proxy n'est pas accessible

Code d'information : 0x10000303, 0x10000304

Vérifiez les paramètres du serveur proxy et assurez-vous qu'il est accessible au Connector Appliance. Pour plus de détails, consultez Enregistrez votre appliance Connector auprès de Citrix Cloud.

L'authentification du serveur proxy a échoué

Code d'information : 0x10000305

Vérifiez les informations d'identification du serveur proxy et assurez-vous qu'elles sont correctement configurées dans Connector Appliance. Pour plus de détails, voir Après avoir enregistré votre appareil Connector.

Les serveurs proxy configurés ne sont pas accessibles

Code d'information : 0x10000306

Vérifiez les paramètres réseau du Connector Appliance, les paramètres du pare-feu ou les paramètres du serveur proxy. Pour plus de détails, consultez les rubriques suivantes :

- Paramètres réseau de votre Connector Appliance
- Enregistrer votre Connector Appliance avec Citrix Cloud
- Communication de Connector Appliance

Réponse d'erreur reçue du serveur principal

Code d'information : 0x10000307

Vérifiez le code d'état HTTP du serveur Web principal, s'il ne s'agit pas d'un code attendu.

Impossible d'envoyer la requête à l'URL cible

Code d'information : 0x10000005

Vérifiez l'URL cible ou vérifiez les paramètres réseau du Connector Appliance. Pour plus de détails, voir Paramètres réseau de votre appareil Connector.

Échec du traitement de l'authentification unique

Code d'information : 0x10000107

Échec de la récupération des données de configuration de l'application à partir de Citrix Cloud.

Vérifiez les paramètres réseau du Connector Appliance et assurez-vous que le serveur NTP est configuré et qu'il n'y a pas de problèmes de bande horaire. Pour plus de détails, voir Paramètres réseau de votre appareil Connector.

La connexion au service Citrix Secure Private Access a échoué

Code d'information : 0x10000108, 0x1000010B

Vérifiez les paramètres réseau du Connector Appliance. Pour plus de détails, voir Paramètres réseau de votre appareil Connector.

Échec du traitement de l'authentification unique, impossible de déterminer les paramètres de l'authentification unique

Code d'information : 0x1000010A

Vérifiez la configuration SSO et assurez-vous que le serveur est accessible à Connector Appliance.

Échec de l'authentification unique de FormFill, configuration incorrecte de l'application de formulaire

Code d'information : 0x10000101, 0x10000102, 0x10000103, 0x10000104

Vérifiez la configuration de l'application de formulaire SSO et assurez-vous que les champs nom d'utilisateur, mot de passe, action et URL de connexion sont correctement configurés dans les paramètres de l'application.

Échec de l'authentification unique Kerberos

Code d'information : 0x10000202

Vérifiez les paramètres Kerberos SSO sur le serveur principal et le contrôleur de domaine. Vérifiez également les paramètres d'authentification NTLM de secours.

Pour les paramètres SSO Kerberos, voir Validation de votre configuration Kerberos.

Échec du traitement de l'authentification unique pour le type d'authentification

Code d'information : 0x10000203

Vérifiez les paramètres SSO dans le service Secure Private Access et le serveur backend. Pour le service Secure Private Access, voir Définissez la méthode de connexion préférée.

Kerberos SSO a échoué mais revient à NTLM

Code d'information : 0x10000204

La récupération du ticket Kerberos auprès du contrôleur de domaine a échoué. En tant qu'authentification secondaire, Connector Appliance a essayé l'authentification NTLM de secours.

Pour activer l'authentification Kerberos réussie, vérifiez les paramètres Kerberos SSO sur le serveur principal et le contrôleur de domaine.

Pour plus de détails, voir Validation de votre configuration Kerberos.

Plusieurs comptes éligibles ZTNA configurés dans l'application Citrix Workspace

Code d'information : 0x14000001

Configurez un seul compte ZTNA dans l'application Citrix Workspace.

Comment collecter les journaux des clients

- **Client Windows :**
  1. Ouvrez l'application et assurez-vous que la journalisation est activée.
  2. Connectez-vous maintenant au service Secure Private Access et dupliquez le problème auquel vous êtes confronté.
  3. Dans l'application, accédez à **Journalisation** et cliquez sur **Collecter les fichiers journaux**. Ceci génère le fichier journal.
  4. Enregistrez le fichier journal sur le bureau de la machine cliente.
- **Client Mac :**
  1. Ouvrez l'application et accédez à **Journaux > Verbose**.
  2. Effacez les journaux et continuez à reproduire le problème.
  3. Retourner à **Journaux > Exporter les journaux**. Cela crée un fichier zip contenant les fichiers journaux.

Réponses aux questions fréquemment posées

Que sont les journaux de diagnostic Secure Private Access ?

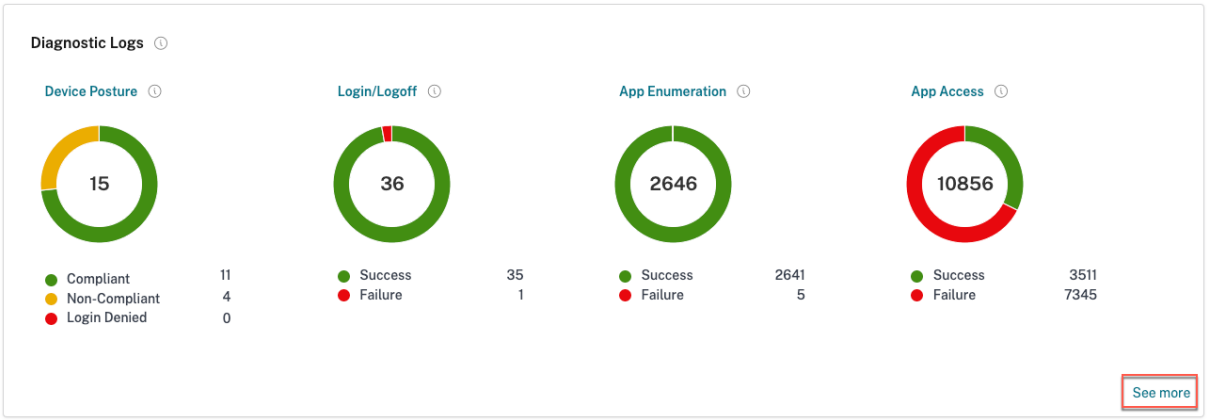
Les journaux de diagnostic Secure Private Access capturent tous les événements qui se produisent lorsqu'un utilisateur accède à n'importe quelle application (Web/SaaS/TCP/UDP). Ces journaux capturent la posture de l'appareil, l'authentification des applications, l'énumération des applications et les journaux d'accès aux applications. Les détails sont présentés sous forme de tableau. Vous pouvez afficher les journaux pour une durée prédéfinie ou pour une chronologie personnalisée. Vous pouvez ajouter des colonnes au graphique en cliquant sur le signe + en fonction des informations que vous souhaitez voir dans le tableau de bord. Vous pouvez exporter les journaux utilisateur au format CSV.

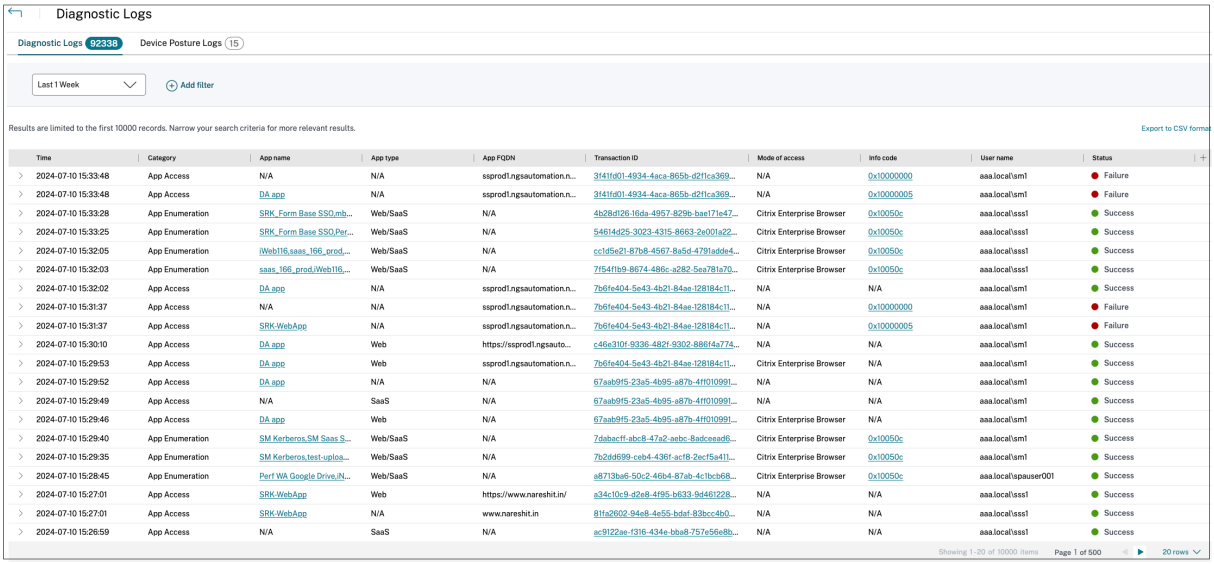
Où puis-je trouver les journaux d'accès privé sécurisé ?

1. Connectez-vous à Citrix Cloud.
2. Sur la mosaïque du service Secure Private Access, cliquez sur **Gérer**.
3. Cliquez sur **Tableau de bord** dans la navigation de gauche dans l'interface utilisateur d'administration.
4. Dans le graphique **Journaux de diagnostic** , cliquez sur le lien **Voir plus** .

Quel widget affiche les journaux de diagnostic de Secure Private Access ?

Les widgets **Journaux de diagnostic** de la section **Journalisation et dépannage** affichent une vue sous forme de graphique à secteurs de tous les événements d'accès privé sécurisé liés à l'authentification, au lancement de l'application, à l'énumération des applications, ainsi qu'aux journaux liés à la posture de l'appareil. Les journaux de diagnostic Secure Private Access récupèrent les événements de plusieurs composants internes, chacun envoyant un événement lorsqu'un utilisateur final accède à une application. Ces événements sont divisés en catégories : **Connexion/Déconnexion**, **Énumération des applications**et **Accès aux applications**. Le graphique à secteurs affiche le ratio global de réussite/échec de chaque catégorie. En cliquant sur le graphique à secteurs coloré de n'importe quel graphique, vous accédez aux journaux de diagnostic où vous pouvez trouver les événements appropriés. Il existe également des journaux de posture de l'appareil si le service de posture de l'appareil est activé. Vous pouvez également cliquer sur le lien **Voir plus** pour afficher les journaux de diagnostic complets.





Quels détails puis-je trouver dans les journaux de diagnostic de Secure Private Access ?

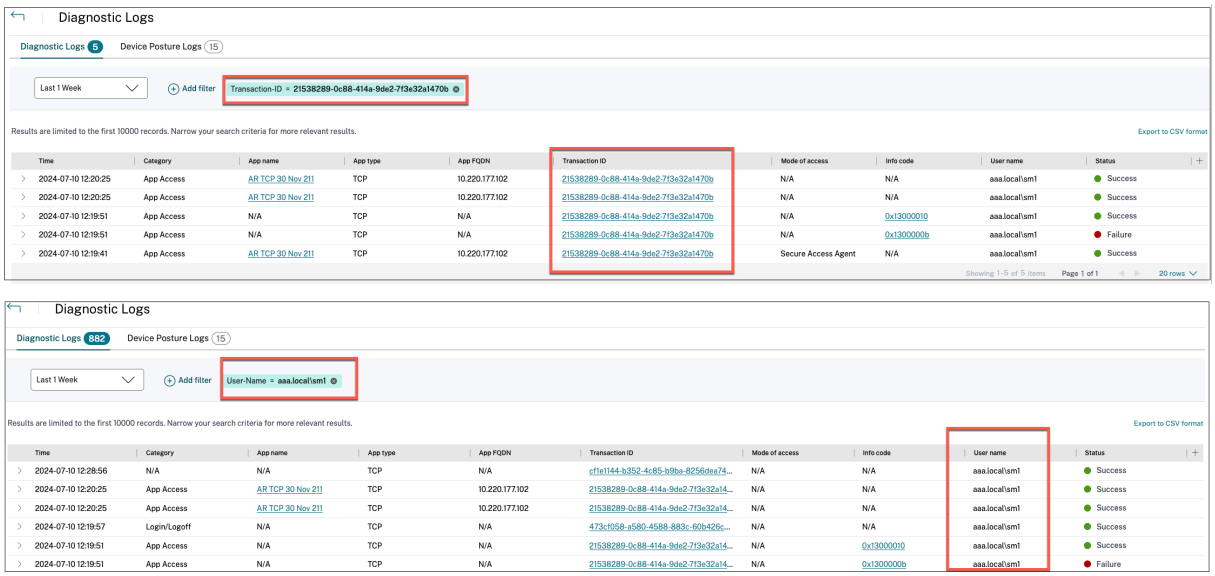
Le tableau de bord des journaux utilisateur de Secure Private Access fournit les détails suivants, par défaut.

- **Horodatage** - Heure de l'événement en UTC.
- **Nom d'utilisateur** - Nom d'utilisateur de l'utilisateur final accédant à l'application.
- **Nom de l'application** - Nom de l'application/des applications auxquelles on a accédé.
- **Informations sur la politique** - Affiche le nom de la ou des politiques d'accès qui ont été déclenchées pendant l'événement.
- **Statut** - Affiche le statut de l'événement, réussite ou échec.
- **Code d'information** - Chaque événement d'échec dans le tableau de bord des journaux de diagnostic Secure Private Access est associé à un code d'information. Voir plus d'informations sur le code info.
- **Description** - Affiche la raison de l'échec ou plus de détails sur l'événement.
- **APP FQDN**: FQDN de l'application consultée

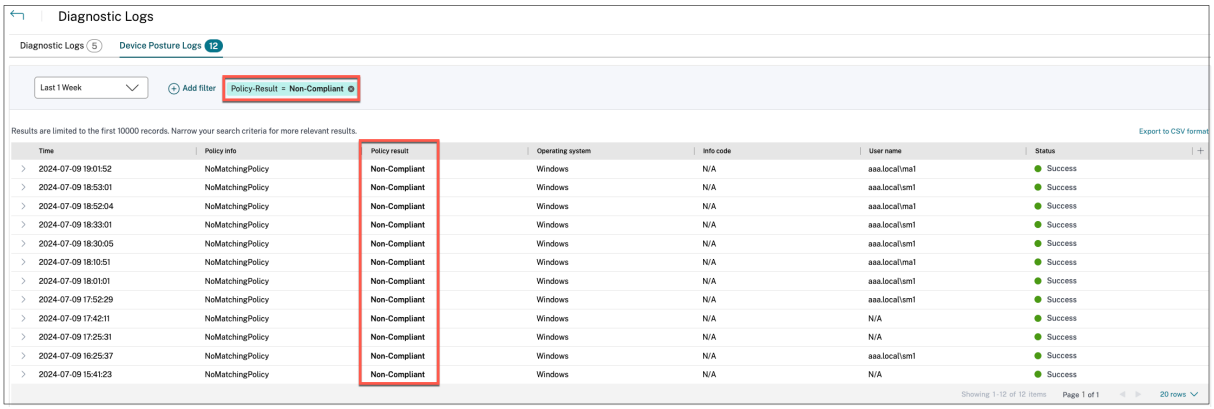
- **Type d'événement** - Affiche le type d'événement associé à l'opération effectuée.
- **Type d'opération** - Affiche l'opération pour laquelle le journal est généré.
- **Catégorie** - Trois catégories sont disponibles selon le type d'événement. Il s'agit de l'authentification d'application, de l'énumération d'applications ou de l'accès aux applications. Ces options sont également disponibles en tant qu'options de filtrage. Vous pouvez utiliser ces options pour filtrer les journaux en fonction du type de problème auquel vous êtes confronté.
- **ID de transaction** - L'ID de transaction met en corrélation tous les journaux d'accès privé sécurisé pour une demande d'accès. Apprenez à utiliser un identifiant de transaction. Les détails suivants peuvent être récupérés en cliquant sur le bouton + à l'extrême droite du tableau de bord :
- **Emplacement PoP SPA** - Affiche le nom/ID de l'emplacement PoP du service Secure Private Access qui a été utilisé lors de l'accès à l'application. Voir Emplacements PoP d'accès privé sécurisé.

Comment filtrer les journaux de diagnostic ?

Vous pouvez utiliser l'option **Ajouter un filtre** pour affiner votre recherche en fonction de différents critères tels que le type d'application, la catégorie, la description. Par exemple, dans le champ de recherche, vous pouvez cliquer sur ID de transaction, = (égal à une valeur) et saisir 21538289-0c88-414a-9de2-7f3e32a1470b pour rechercher tous les journaux liés à cet ID de transaction. Pour plus de détails sur les opérateurs de recherche qui peuvent être utilisés avec l'option de filtre, voir Opérateurs de recherche.



Vous pouvez également utiliser les différentes options de filtrage pour affiner votre recherche dans les journaux de posture de l'appareil.



Quels événements sont capturés dans les journaux de diagnostic Secure Private Access ?

Les journaux de diagnostic Secure Private Access capturent les événements suivants :

- **Posture de l'appareil :** État de l'appareil de l'utilisateur final. Ces journaux capturent des informations sur les résultats de posture de l'appareil. Si l'appareil a été jugé conforme, non conforme ou si l'accès a été refusé en fonction de votre politique de posture de l'appareil.
- **Connexion/Déconnexion**: Événements concernant l'état de connexion ou de déconnexion de l'utilisateur final au client Citrix Secure Access et l'authentification à l'espace de travail (fournisseurs internes ou externes).
- **Énumération des applications**: Dans le service Secure Private Access, les politiques d'accès configurées par les administrateurs décident quel utilisateur peut accéder à quelle application. Les applications refusées ne sont pas visibles (non énumérées) pour les utilisateurs finaux dans Citrix Workspace App. Ces événements vous aident à savoir quelles applications ont été autorisées ou refusées à accéder à un utilisateur en fonction des politiques d'accès configurées dans le service Secure Private Access.
- **Accès à l'application**: Événements d'accès à l'application/au point de terminaison de l'utilisateur final, statut d'autorisation/de refus, statut d'authentification unique et statut de connectivité conformément aux politiques d'accès configurées pour l'intervalle de temps sélectionné.

Comment utiliser la rubrique de dépannage de Secure Private Access pour résoudre une panne que j'ai rencontrée ?

1. Récupérez le code d'information pour l'échec que vous essayez de résoudre.
2. Recherchez le code d'information dans la table de recherche d'erreur .
3. Suivez les étapes de résolution fournies pour ce code d'information.

Qu'est-ce qu'un code d'information ? Où puis-je les trouver ?

Certains événements de journal tels que les échecs ont un code d'information associé. Recherchez ce code d'information dans la table de recherche d'erreurs pour trouver les étapes de résolution ou plus d'informations sur cet événement.

Qu'est-ce qu'un identifiant de transaction ? Comment l'utiliser ?

Les échecs/problèmes d'accès via Citrix Enterprise Browser affichent un ID de transaction à l'utilisateur final. Les administrateurs peuvent récupérer cet ID de transaction auprès des utilisateurs finaux et utiliser cet ID de transaction pour filtrer les journaux exacts qui ont causé le problème, leur permettant ainsi d'identifier le problème exact. Une fois que les administrateurs filtrent les événements avec l'ID de transaction, seuls les événements relatifs au problème en cours sont affichés, fournissant tous les détails aux administrateurs sur la raison pour laquelle l'échec ou le problème s'est produit. Les administrateurs peuvent ensuite utiliser le code d'erreur sur ces journaux pour résoudre davantage les problèmes.

Quels sont tous les emplacements PoP d'accès privé sécurisé ?

Voici la liste des emplacements PoP d'accès privé sécurisé.

Nom du PoP	Zone	Région
az-us-e	Azure estus	Virginie
az-us-w	Azur westus	Californie
az-us-sc	Azure centralus sud	Texas
az-aus-e	Azure Australie-Est	Nouvelle-Galles du Sud
az-eu-n	Azure nordeurope	Irlande
az-eu-w	Azure ouesteurope	Pays-Bas
az-jp-e	Azure Japon-Est	Tokyo, Saitama
az-bz-s	Azure Brésil Sud	État de São Paulo
az-asia-se	Azure Asie du Sud-Est	Singapour
az-uae-n	Azure uaenorth	Dubaï
az-dans-s	Azure Inde du Sud	Chennai
az-asie-hk	Azur estasia	Hong Kong

Que dois-je faire si je ne parviens pas à résoudre mon échec à l'aide du code d'information et de la table de recherche d'erreurs ?

Contactez le support Citrix.

Références

- **Ajouter une application Web**
  - Prise en charge des applications Web d'entreprise
  - Configurer l'accès direct aux applications Web
- **Ajouter une application SaaS**
  - Prise en charge de l'application Software as a Service
  - Configuration spécifique au serveur d'applications SaaS
- **Configurer les applications client-serveur**
  - Prise en charge des applications client-serveur
- **Créer des politiques d'accès**
  - Créer des politiques d'accès
- **Tables de routage**
  - Tables de routage

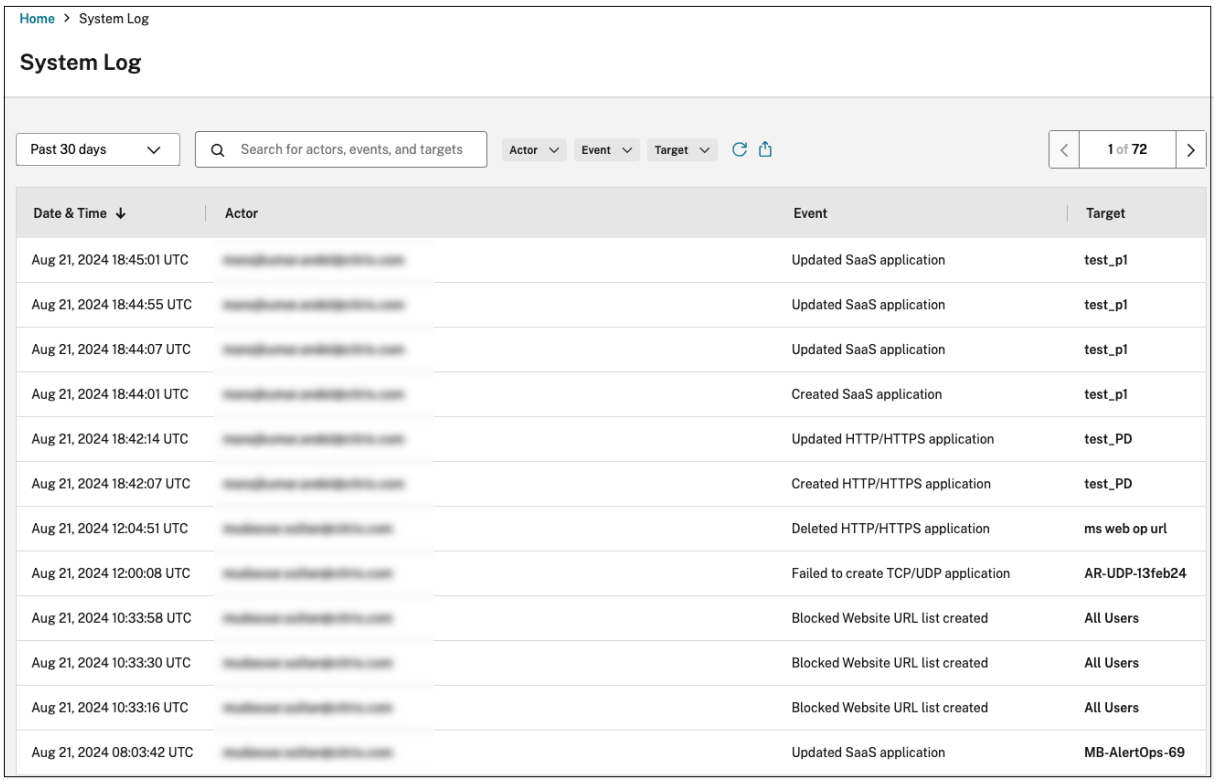
Journaux d'audit

October 21, 2024

Les événements liés au service Secure Private Access sont capturés dans **Citrix Cloud > Journal système**. Tous les événements qu'un administrateur exécute dans le service Citrix Secure Private Access sont envoyés à Citrix Cloud et capturés dans les journaux système. Les événements d'administration peuvent être, sans toutefois s'y limiter, les suivants :

- Créer ou mettre à jour une application
- Supprimer une application
- Configurer ou supprimer une politique d'accès adaptatif
- Mise à niveau du connecteur
- Création de sites Web autorisés ou bloqués

La figure suivante affiche les événements liés à l'accès privé sécurisé dans le journal système **.



Pour plus de détails tels que l'exportation d'événements, la récupération d'événements pour une période spécifique, le transfert d'événements de journal et la conservation des données, voir Journal système.

Contrôles d'accès et de sécurité adaptatifs pour les applications Web, TCP et SaaS d'entreprise

August 26, 2024

Dans les situations en constante évolution d'aujourd'hui, la sécurité des applications est vitale pour toute entreprise. La prise de décisions de sécurité contextuelles, puis l'activation de l'accès aux applications, réduisent les risques associés tout en autorisant l'accès aux utilisateurs.

La fonction d'accès adaptatif du service Citrix Secure Private Access offre une approche d'accès zero-trust complète qui fournit un accès sécurisé aux applications. L'accès adaptatif permet aux administrateurs de fournir un accès de niveau granulaire aux applications auxquelles les utilisateurs peuvent accéder en fonction du contexte. Le terme « contexte » désigne ici :

- Utilisateurs et groupes (utilisateurs et groupes d'utilisateurs)

- Appareils (ordinateurs de bureau ou appareils mobiles)
- Localisation (géolocalisation ou localisation réseau)
- État de sécurité de l'appareil (vérification de l'état de sécurité de l'appareil)
- Risque (indice de risque utilisateur)

La fonction d'accès adaptatif applique des stratégies adaptatives aux applications auxquelles vous accédez. Ces stratégies déterminent les risques en fonction du contexte et prennent des décisions d'accès dynamiques pour accorder ou refuser l'accès aux applications Web d'entreprise, SaaS, TCP et UDP.

Fonctionnement

Pour accorder ou refuser l'accès aux applications, les administrateurs créent des stratégies basées sur les utilisateurs, les groupes d'utilisateurs, les appareils à partir desquels les utilisateurs accèdent aux applications, l'emplacement (pays ou emplacement réseau) depuis lequel l'utilisateur accède à l'application et le score de risque de l'utilisateur.

Les stratégies d'accès adaptatives ont priorité sur les stratégies de sécurité spécifiques à l'application qui sont configurées lors de l'ajout du SaaS ou d'une application Web dans le service Secure Private Access. Les contrôles de sécurité au niveau de l'application sont écrasés par les stratégies d'accès adaptatives.

Les stratégies d'accès adaptatives sont évaluées selon trois scénarios :

- Au cours d'une énumération d'applications Web, TCP ou SaaS à partir du service Secure Private Access : si l'accès à l'application est refusé à cet utilisateur, celui-ci ne peut pas voir cette application dans l'espace de travail.
- Lors du lancement de l'application : après avoir énuméré l'application et si la stratégie adaptative est modifiée pour refuser l'accès, les utilisateurs ne peuvent pas lancer l'application même si l'application a été énumérée précédemment.
- Lorsque l'application est ouverte dans un navigateur Citrix Enterprise ou dans un service Remote Browser Isolation, le navigateur Citrix Enterprise applique certains contrôles de sécurité. Ces contrôles sont appliqués par le client. Lorsque le navigateur Citrix Enterprise est lancé, le serveur évalue les stratégies adaptatives pour l'utilisateur et renvoie ces stratégies au client. Le client applique ensuite les stratégies localement dans Citrix Enterprise Browser.

Création d'une stratégie d'accès adaptative avec plusieurs règles

Vous pouvez créer plusieurs règles d'accès et configurer différentes conditions d'accès pour différents utilisateurs ou groupes d'utilisateurs au sein d'une même stratégie. Ces règles peuvent

être appliquées séparément aux applications HTTP/HTTPS et TCP/UDP, le tout dans le cadre d'une stratégie unique.

Les stratégies d'accès au sein de Secure Private Access vous permettent d'activer ou de désactiver l'accès aux applications en fonction du contexte de l'utilisateur ou de son appareil. En outre, vous pouvez activer l'accès restreint aux applications en ajoutant les restrictions de sécurité suivantes :

- Restreindre l'accès au presse-papiers
- Restreindre l'impression
- Restreindre les téléchargements
- Restreindre les chargements
- Afficher le filigrane
- Restreindre la capture de frappes
- Limiter la capture d'écran

Pour plus d'informations sur ces restrictions, consultez la section Restrictions d'accès disponibles.

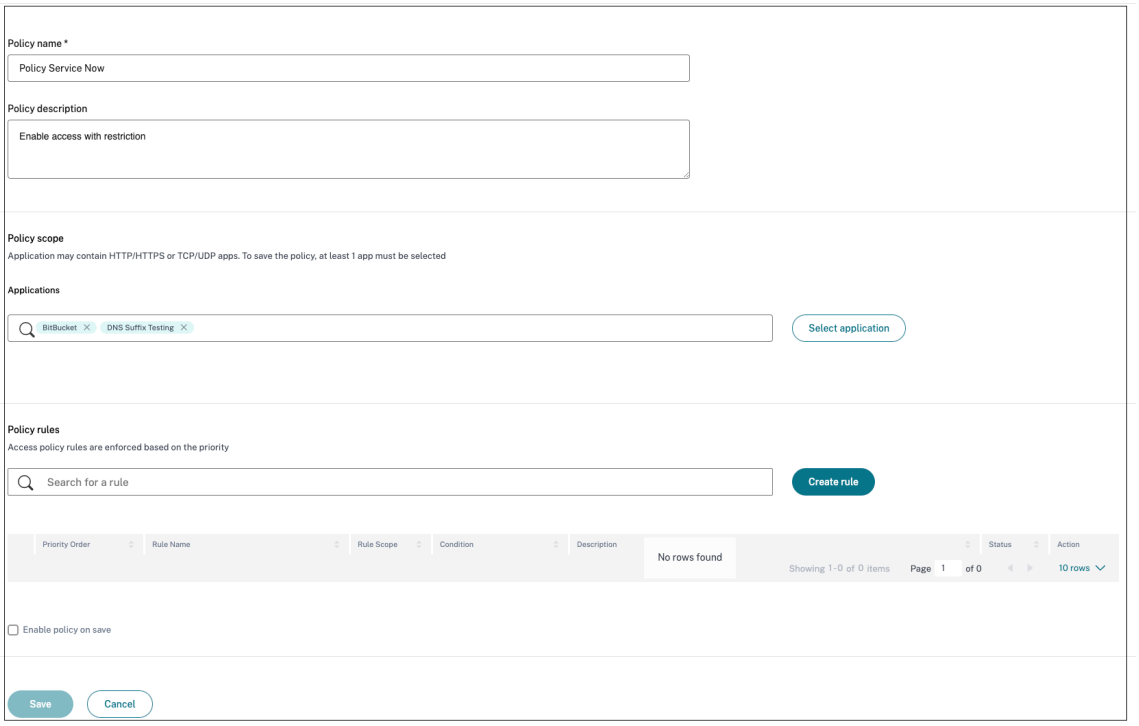
Assurez-vous d'avoir effectué les tâches suivantes avant de configurer une stratégie d'accès.

- Configuration de l'identité et de l'authentification
- Applications configurées

1. Dans le volet de navigation, cliquez sur **Stratégies d'accès**, puis sur **Créer une stratégie**.

   Pour les nouveaux utilisateurs, la page d'accueil **Stratégies d'accès** n'affiche aucune stratégie. Une fois que vous avez créé une stratégie, vous pouvez la voir répertoriée ici.

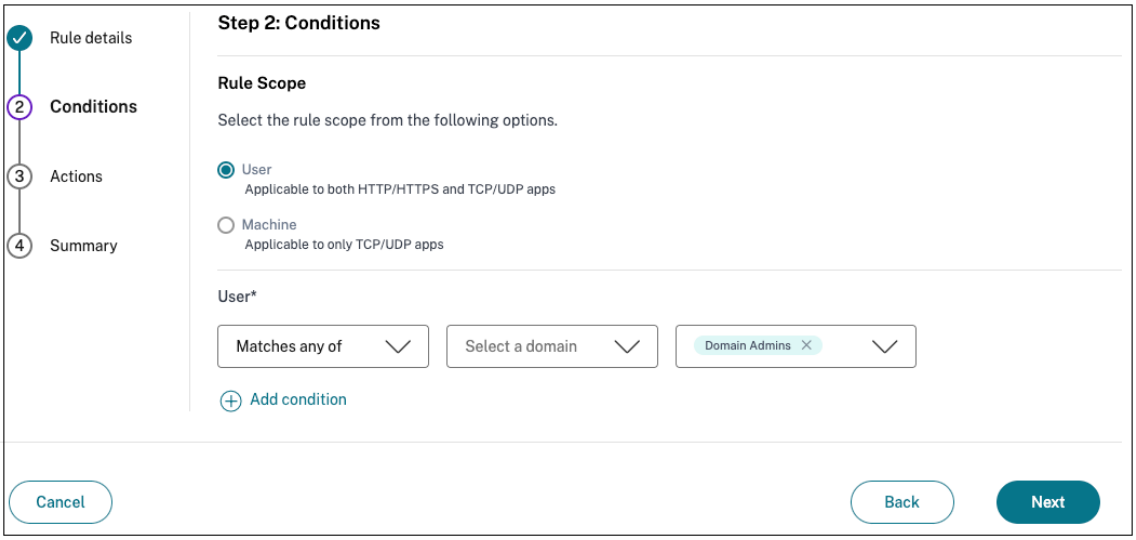
2. Entrez le nom et la description de la stratégie.
3. Dans **Applications**, sélectionnez l'application ou l'ensemble d'applications auxquelles cette stratégie doit être appliquée.
4. Cliquez sur **Créer une règle** pour créer des règles pour la stratégie.



5. Entrez le nom de la règle et une brève description de la règle, puis cliquez sur **Suivant**.

6. Sélectionnez les conditions des utilisateurs. La condition **Utilisateurs** est une condition obligatoire à remplir pour permettre aux utilisateurs d'accéder aux applications. Sélectionnez l'une des options suivantes :

   - **Correspond à l'un des** : seuls les utilisateurs ou groupes correspondant à l'un des noms répertoriés dans le champ et appartenant au domaine sélectionné sont autorisés à accéder.
   - **Ne correspond à aucun** : tous les utilisateurs ou groupes, à l'exception de ceux répertoriés dans le champ et appartenant au domaine sélectionné, sont autorisés à y accéder.



7. (Facultatif) Cliquez sur + pour ajouter plusieurs conditions en fonction du contexte.

   Lorsque vous ajoutez des conditions basées sur un contexte, une opération AND est appliquée aux conditions dans lesquelles la stratégie est évaluée uniquement si les conditions **Users*** et les conditions contextuelles facultatives sont remplies. Vous pouvez appliquer les conditions suivantes en fonction du contexte.

   - **Ordinateur de bureau** ou **appareil mobile** : sélectionnez l'appareil pour lequel vous souhaitez activer l'accès aux applications.
   - **Géolocalisation** : sélectionnez la condition et l'emplacement géographique à partir desquels les utilisateurs accèdent aux applications.
   - **Emplacement réseau** : sélectionnez la condition et le réseau via lesquels les utilisateurs accèdent aux applications.
   - **Contrôle de la posture de l'appareil** : sélectionnez les conditions que la machine utilisateur doit respecter pour accéder à l'application.
   - **Score de risque de l'utilisateur** : sélectionnez les catégories de score de risque en fonction desquelles les utilisateurs doivent avoir accès à l'application.

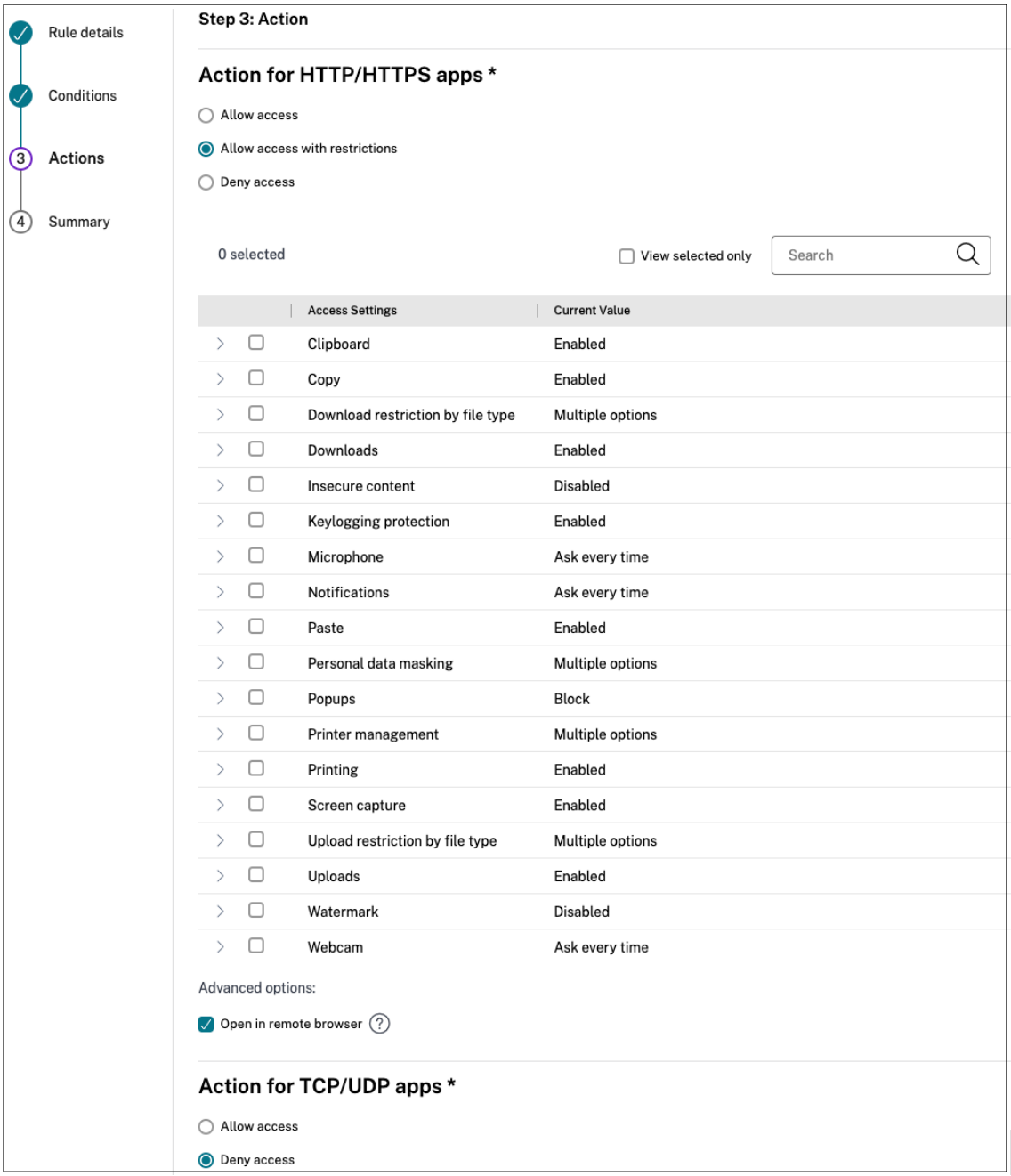
8. Cliquez sur **Suivant**.

9. Sélectionnez les actions qui doivent être appliquées en fonction de l'évaluation des conditions.

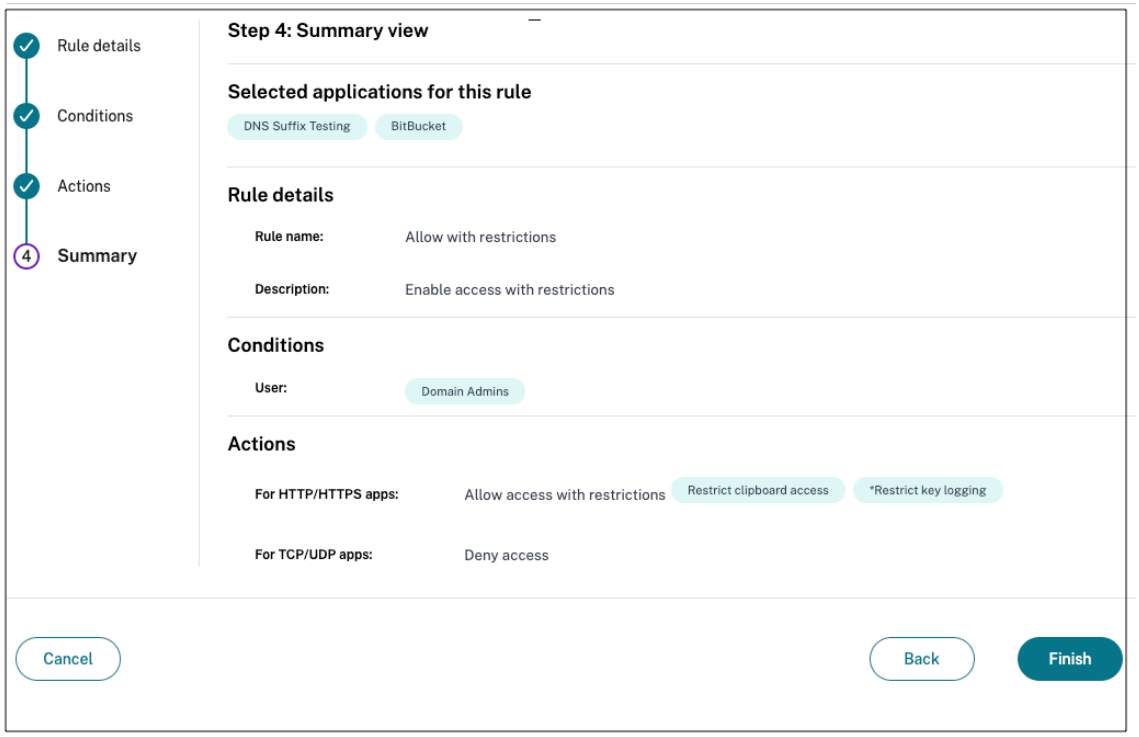
   - Pour les applications HTTP/HTTPS, vous pouvez sélectionner les options suivantes :
     - **Autoriser l'accès**
     - **Autoriser l'accès avec restrictions**
     - **Refuser l'accès**

> **Remarque :**
>
> Si vous sélectionnez **Autoriser l'accès avec restrictions**, vous devez sélectionner les restrictions que vous souhaitez appliquer aux applications. Pour plus de détails sur les restrictions, consultez la section Options de restrictions d'accès disponibles . Vous pouvez également spécifier si vous souhaitez que l'application s'ouvre dans un navigateur distant ou dans Citrix Secure Browser.

- Pour l'accès TCP/UDP, vous pouvez sélectionner les options suivantes :
  - **Autoriser l'accès**
  - **Refuser l'accès**



10. Cliquez sur **Suivant**. La page Résumé affiche les détails de la stratégie.
11. Vous pouvez vérifier les détails et cliquer sur **Terminer**.



Points à retenir après la création d'une stratégie

- La stratégie que vous avez créée apparaît dans la section Règles de stratégie et est activée par défaut. Vous pouvez désactiver les règles, si nécessaire. Assurez-vous toutefois qu'au moins une règle est activée pour que la stratégie soit active.
- Un ordre de priorité est attribué à la stratégie par défaut. La priorité dont la valeur est la plus faible a la préférence la plus élevée. La règle ayant le numéro de priorité le plus faible est évaluée en premier. Si la règle (n) ne correspond pas aux conditions définies, la règle suivante (n+1) est évaluée et ainsi de suite.

Exemple d'évaluation de règles avec ordre de priorité :

Supposons que vous ayez créé deux règles, la Règle 1 et la Règle 2.
La règle 1 est attribuée à l'utilisateur A et la règle 2 à l'utilisateur B, puis les deux règles sont évaluées. Supposons que les règles Règle 1 et Règle 2 soient attribuées à l'utilisateur A. Dans ce cas, la Règle 1 a la priorité la plus élevée. Si la condition de la Règle 1 est remplie, la Règle 1 est appliquée et la Règle 2 est ignorée. Sinon, si la condition de la Règle 1 n'est pas remplie, la Règle 2 est appliquée à l'utilisateur A.

> **Remarque :**
>
> Si aucune des règles n'est évaluée, l'application n'est pas répertoriée pour les utilisateurs.

Options de restrictions d'accès disponibles

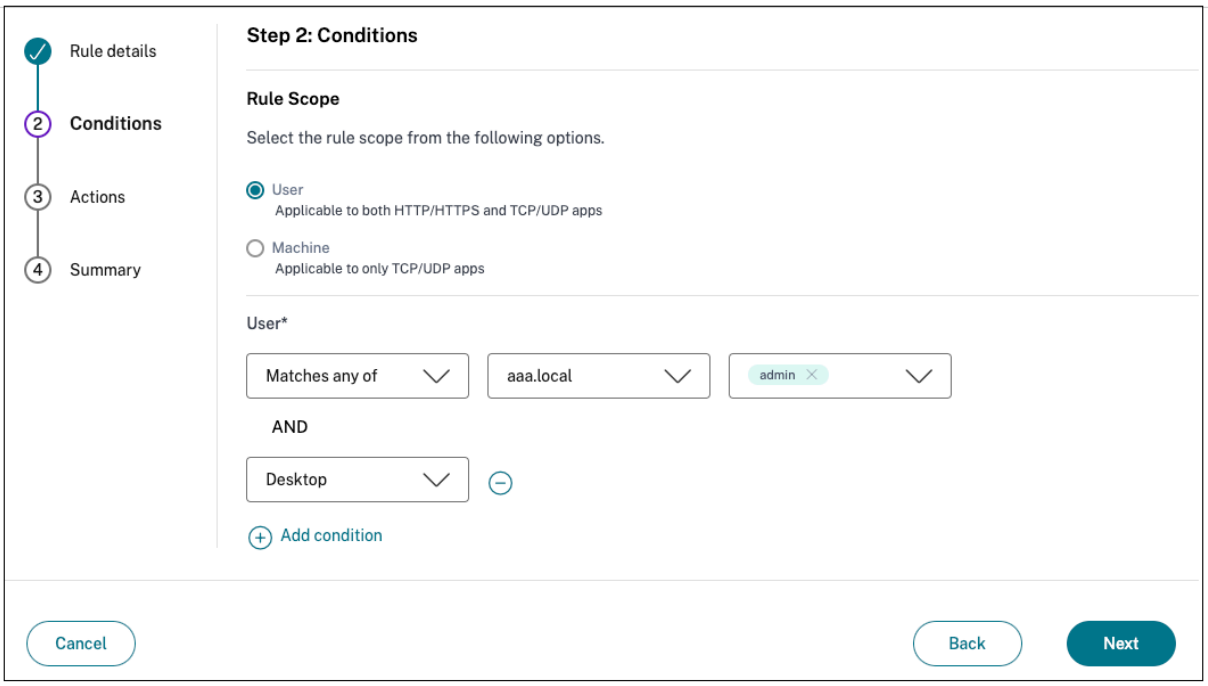
Lorsque vous sélectionnez l'action **Autoriser l'accès avec restrictions**, vous devez sélectionner au moins l'une des restrictions de sécurité. Ces restrictions de sécurité sont prédéfinies dans le système. Les administrateurs ne peuvent pas modifier ou ajouter d'autres combinaisons. Pour plus de détails, voir Options de restrictions d'accès disponibles

Accès adaptatif basé sur les appareils

Pour configurer une stratégie d'accès adaptative basée sur la plate-forme (appareil mobile ou ordinateur de bureau) à partir de laquelle l'utilisateur accède à l'application, utilisez la procédure Créer une stratégie d'accès adaptative avec plusieurs règles avec les modifications suivantes.

- Dans la page **Étape 2 : Conditions**, cliquez sur **Ajouter une condition.**

- Sélectionnez **Ordinateur de bureau** ou **Appareil mobile**.
- Terminez la configuration de la stratégie.



Accès adaptatif en fonction de l'emplacement

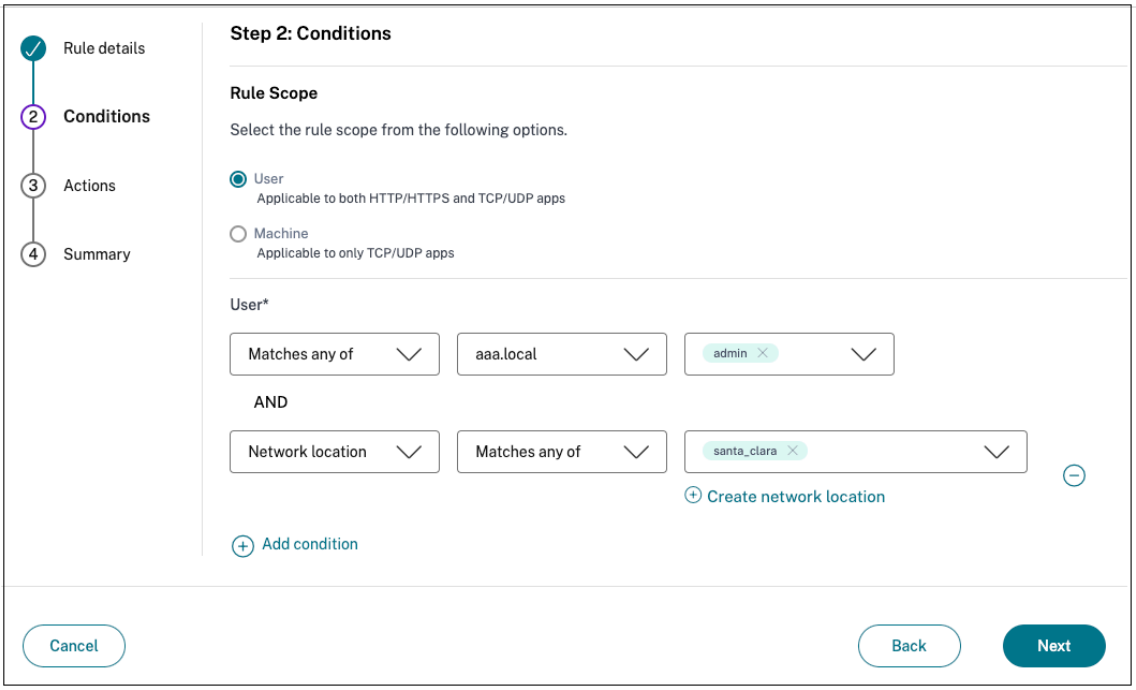
Un administrateur peut configurer la stratégie d'accès adaptative en fonction de l'emplacement depuis lequel l'utilisateur accède à l'application. L'emplacement peut être le pays depuis lequel l'utilisateur accède à l'application ou l'emplacement réseau de l'utilisateur. L'emplacement réseau est défini à l'aide d'une plage d'adresses IP ou d'adresses de sous-réseau.

Pour configurer une stratégie d'accès adaptative en fonction de l'emplacement, utilisez la procédure [Créer une stratégie d'accès adaptative avec plusieurs règles] avec les modifications suivantes.

- Dans la page **Étape 2 : Conditions**, cliquez sur **Ajouter une condition.**
- Sélectionnez **Géolocalisation ou Emplacementréseau.**
- Si vous avez configuré plusieurs géolocalisations ou emplacements réseau, sélectionnez l'une des options suivantes selon vos besoins.
  - **Correspond à l'un des** —Les emplacements géographiques ou les emplacements réseau correspondent à l'un des emplacements géographiques ou des emplacements réseau configurés dans la base de données.
  - **Ne correspond à aucun** —Les emplacements géographiques ou les emplacements réseau ne correspondent pas aux emplacements géographiques ou aux emplacements réseau configurés dans la base de données.

Remarque :

- Si vous sélectionnez **Géolocalisation**, l'adresse IP source de l'utilisateur est évaluée avec l'adresse IP de la base de données du pays. Si l'adresse IP de l'utilisateur correspond au pays indiqué dans la stratégie, la stratégie est appliquée. Si le pays ne correspond pas, cette stratégie adaptative est ignorée et la stratégie adaptative suivante est évaluée.
- Pour **Emplacement réseau**, vous pouvez sélectionner un emplacement réseau existant ou créer un emplacement réseau. Pour créer un nouvel emplacement réseau, cliquez sur **Créer un emplacement réseau**.
- Assurez-vous d'avoir activé Adaptive Access depuis **Citrix Cloud > Citrix Workspace > Access > Adaptive Access**. Dans le cas contraire, vous ne pouvez pas ajouter les balises de localisation. Pour plus de détails, voir Activer l'accès adaptatif.
- Vous pouvez également créer un emplacement réseau à partir de la console Citrix Cloud. Pour plus de détails, consultez la section Configuration de l'emplacement réseau Citrix Cloud.



- Terminez la configuration de la stratégie.

Accès adaptatif en fonction de l'état de sécurité de l'appareil

Vous pouvez configurer Secure Private Access Service pour renforcer le contrôle d'accès à l'aide des balises de posture de l'appareil. Une fois qu'un appareil est autorisé à se connecter après la vérification de sa posture, il peut être classé comme conforme ou non conforme. Ces informations sont

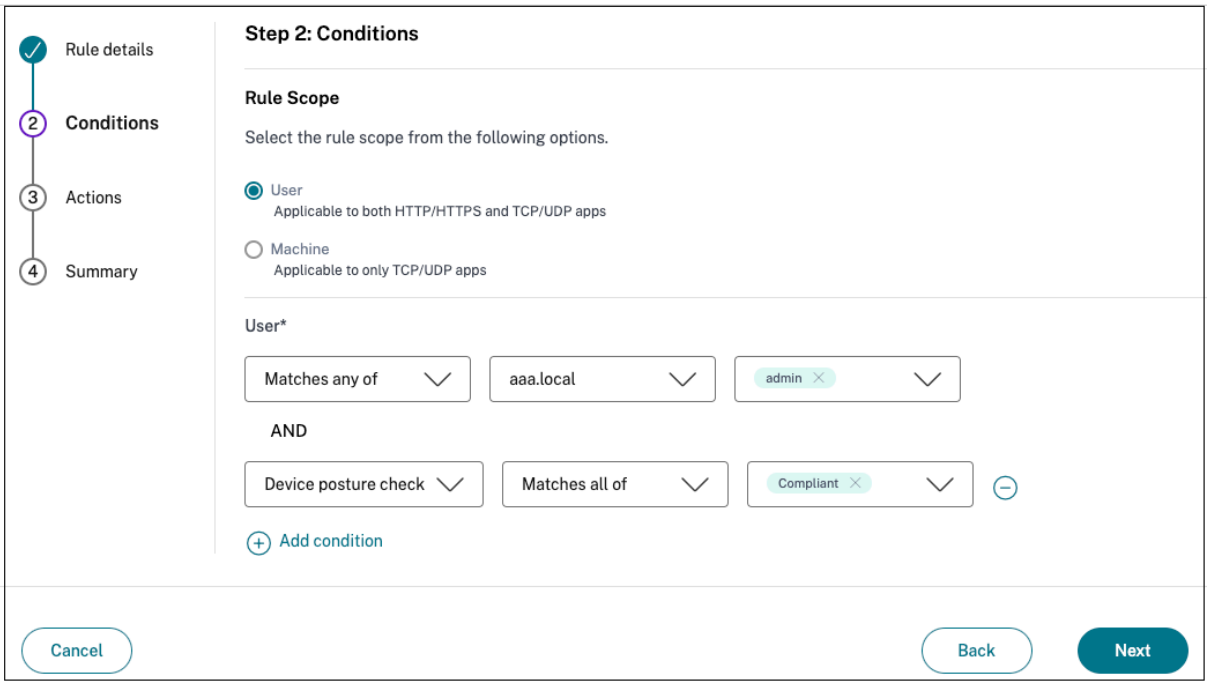
disponibles sous forme de balises pour le service Citrix DaaS et le service Citrix Secure Private Access et sont utilisées pour fournir un accès contextuel en fonction de la posture de l'appareil.

Pour plus de détails sur le service Posture de l'appareil, voir Posture de l'appareil.

Pour configurer une stratégie d'accès adaptative en fonction de la posture de l'appareil, utilisez la procédure Créer une stratégie d'accès adaptative avec plusieurs règles avec les modifications suivantes.

- Dans la page **Étape 2 : Conditions**, cliquez sur **Ajouter une condition.**
- Sélectionnez **Contrôle de la posture de l'appareil** et l'expression logique dans le menu déroulant.
- Entrez l'une des valeurs suivantes dans les balises personnalisées :
  - **Conforme** : pour les appareils conformes
  - **Non conforme** - Pour les appareils non conformes

> **Remarque :**
>
> La syntaxe des étiquettes de classification des appareils doit être saisie de la même manière que celle capturée précédemment, c'est-à-dire en majuscules initiales (conformes et non conformes). Sinon, les stratégies de posture de l'appareil ne fonctionnent pas comme prévu.



Accès adaptatif basé sur le score de risque utilisateur

> **Important :**
>
> Cette fonctionnalité n'est disponible pour les clients que s'ils disposent des droits Security Analytics.

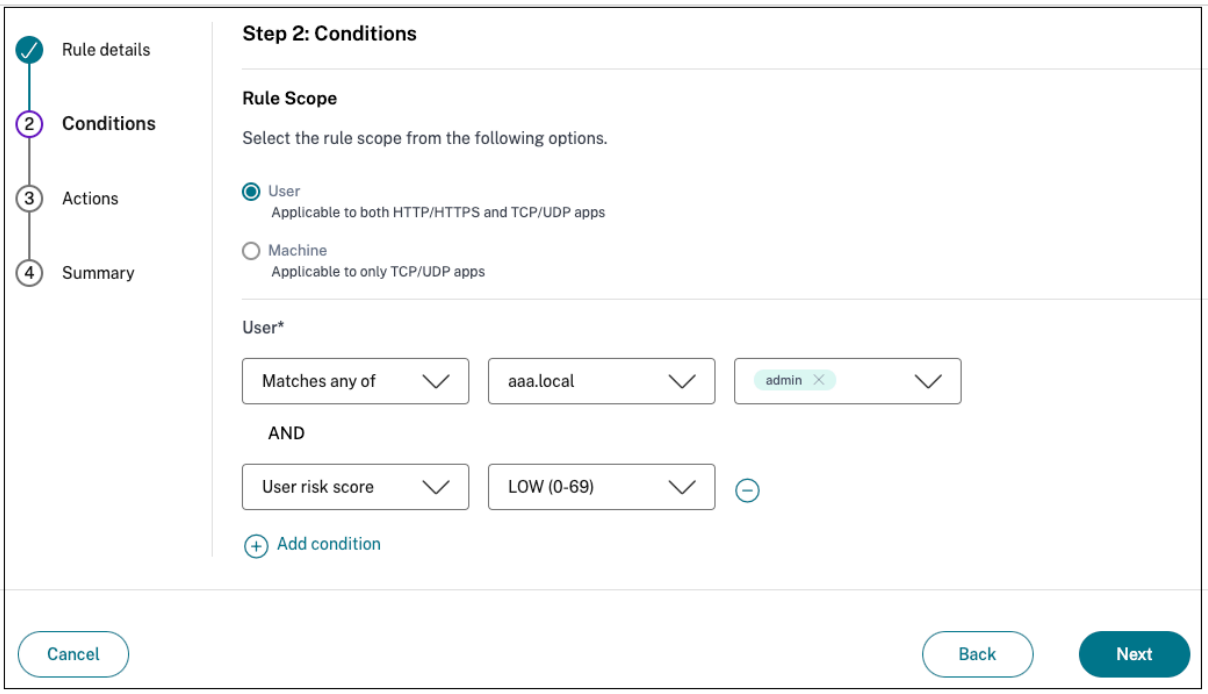
Le score de risque utilisateur est un système de notation permettant de déterminer les risques associés aux activités des utilisateurs dans votre entreprise. Les indicateurs de risque sont attribués aux activités des utilisateurs qui semblent suspectes ou qui peuvent constituer une menace pour la sécurité de votre organisation. Les indicateurs de risque sont déclenchés lorsque le comportement de l'utilisateur s'écarte de la normale. Chaque indicateur de risque peut être associé à un ou plusieurs facteurs de risque. Ces facteurs de risque vous aident à déterminer le type d'anomalies dans les événements utilisateur. Les indicateurs de risque et les facteurs de risque associés déterminent le score de risque d'un utilisateur. Le score de risque est calculé périodiquement et il y a un délai entre l'action et la mise à jour du score de risque. Pour plus de détails, consultez la section Indicateurs de risque utilisateur Citrix

Pour configurer une stratégie d'accès adaptative avec un score de risque, utilisez la procédure Créer une stratégie d'accès adaptative avec plusieurs règles avec les modifications suivantes.

- Dans la page **Étape 2 : Conditions**, cliquez sur **Ajouter une condition.**
- Sélectionnez **Score de risque utilisateur**, puis sélectionnez la condition de risque.
  - Tags prédéfinis récupérés depuis le service CAS
    - **FAIBLE** 1—69
    - **MOYEN** 70—89
    - **HAUT** 90—100

    > **Remarque :**
    >
    > Un score de risque de 0 n'est pas considéré comme ayant un niveau de risque « Faible ».

  - Types de seuil
    - **Supérieur ou égal à**
    - **Inférieur ou égal à**
  - Une plage de numéros
    - **Gamme**



Tables de routage pour résoudre les conflits résultant des mêmes domaines associés

October 21, 2024

La fonctionnalité de domaines d'application du service Citrix Secure Private Access permet aux clients de prendre des décisions de routage qui permettent aux domaines d'application associés d'être acheminés en externe ou en interne via des dispositifs de connecteur.

Considérez que le client a configuré les mêmes domaines associés à la fois dans une application SaaS et dans une application Web interne. Par exemple, si Okta est l'IdP SAML pour Salesforce (application SaaS) et Jira (application Web interne), l'administrateur peut configurer `*.okta.com` comme domaine associé dans la configuration des deux applications. Cela conduit à un conflit et l'utilisateur final subit un comportement incohérent. Dans ce scénario, l'administrateur peut définir des règles pour acheminer ces applications en externe ou en interne via les appareils Connector, selon les besoins.

Comment fonctionne la table de routage

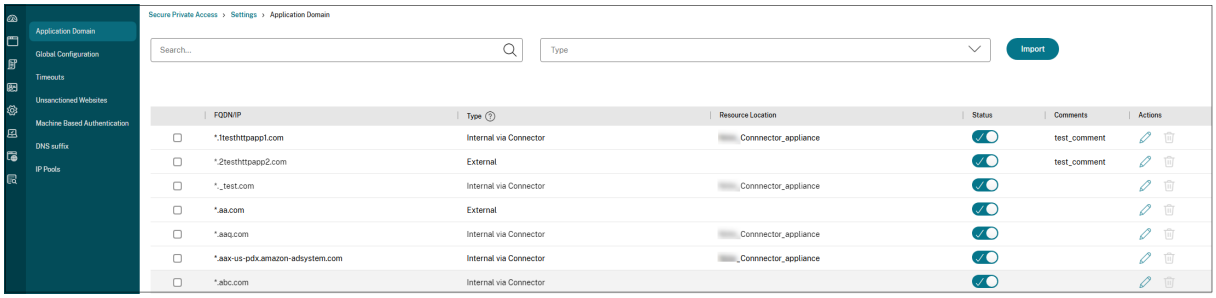
Les administrateurs peuvent définir les types d'itinéraires suivants pour les applications en fonction de la manière dont ils souhaitent définir le flux de trafic.

- **Interne –Contourner le proxy** - Le trafic du domaine est acheminé via Citrix Cloud Connector, en contournant le proxy Web du client configuré sur l'appliance Connector.
- **Interne via le connecteur** - Les applications sont externes mais le trafic doit circuler via l'appliance Connector vers le réseau extérieur.
- **Externe** –Le trafic circule directement vers Internet.

> **Remarque**
>
> - Les entrées d'itinéraire n'ont pas d'impact sur les politiques de sécurité configurées sur les applications.
> - Si les administrateurs n'ont pas l'intention d'utiliser une entrée dans la table de routage ou si les applications correspondantes ne fonctionnent pas comme prévu, les administrateurs peuvent simplement désactiver l'entrée au lieu de la supprimer.
> - Tous les appareils connecteurs d'un client particulier, quel que soit le type d'application, obtiennent les paramètres SSO. Auparavant, le paramètre SSO d'une application particulière était lié à un emplacement de ressource.

Tableau des itinéraires principaux

La table de routage principale de la console Secure Private Access (**Paramètres > Domaines d'application**) est un tableau de bord en lecture seule qui vous donne tous les détails sur les domaines configurés dans toutes les applications. Cela peut être utilisé pour voir les informations suivantes pour n'importe quel domaine :



La table de routage principale peut être utilisée pour voir les informations suivantes pour n'importe quel domaine :

- **FQDN/IP :** FQDN ou adresse IP pour laquelle le type de routage du trafic doit être configuré.
- **Type**: Type d'application. **Interne**, **Interne –Contourner le proxy**, ou **Externe** comme sélectionné lors de l'ajout de l'application.

> **Important :**
>
> S'il y a des conflits, une icône d'alerte s'affiche pour la ligne correspondante dans le tableau. Pour résoudre le conflit, les administrateurs doivent cliquer sur l'icône triangulaire et modifier

> le type d'application à partir du tableau principal.

- **Emplacement de la ressource :** Emplacement de la ressource pour le routage de type **Interne**. Si un emplacement de ressource n'est pas alloué, une icône triangulaire apparaît dans la colonne **Emplacement de ressource** pour l'application concernée. Lorsque vous passez la souris sur l'icône, le message suivant s'affiche.

  Emplacement de la ressource manquant. Assurez-vous qu'un emplacement de ressource est associé à ce nom de domaine complet.

- **Statut :** Le commutateur à bascule dans la colonne **Statut** peut être utilisé pour désactiver l'itinéraire pour une entrée d'itinéraire sans supprimer l'application. Lorsque l'interrupteur à bascule est désactivé, l'entrée d'itinéraire n'a pas d'effet. De plus, si des noms de domaine complets correspondant exactement existent, les administrateurs peuvent sélectionner l'itinéraire à activer ou à désactiver.
- **Commentaires :** Affiche les commentaires, le cas échéant.
- **Actions :** L'icône d'édition est utilisée pour ajouter un emplacement de ressource ou modifier le type d'entrée d'itinéraire. L'icône Supprimer permet de supprimer l'itinéraire.

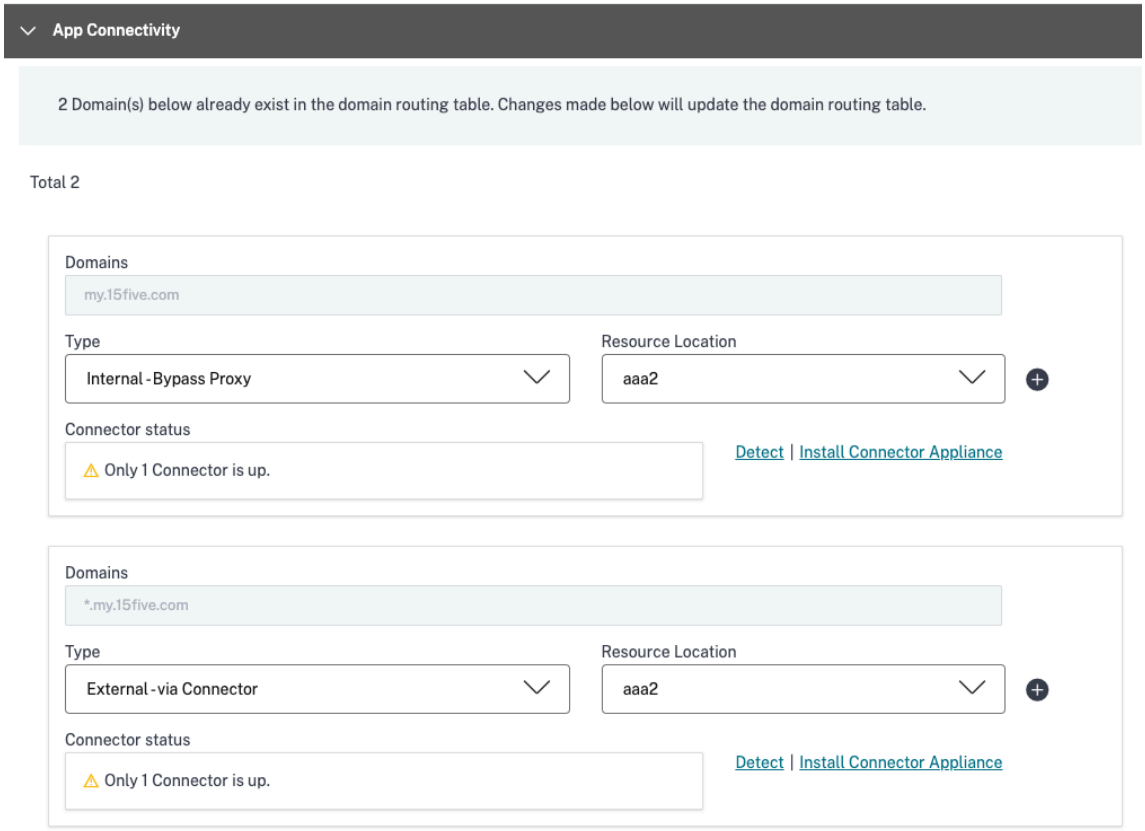
Mini tableau des itinéraires

Une mini version du tableau des domaines d'application est disponible pour prendre les décisions de routage lors de la configuration de l'application. La mini table de routage disponible dans la section **App Connectivity** de l'interface utilisateur du service Citrix Secure Private Access.

Pour ajouter des itinéraires à la mini table d'itinéraires

Les étapes pour ajouter une application dans le service Citrix Secure Private Access restent les mêmes que celles décrites dans les rubriques Prise en charge des applications logicielles en tant que service et Prise en charge des applications Web d'entreprise , à l'exception des deux modifications suivantes :

1. Effectuez les étapes suivantes :
   - Choisissez un modèle.
   - Entrez les détails de l'application.
   - Choisissez des détails de sécurité renforcés, le cas échéant.
   - Sélectionnez la méthode d'authentification unique, le cas échéant.
2. Cliquez sur **Connectivité de l'application**. - Une mini version du tableau des domaines d'application est disponible pour prendre les décisions de routage lors de la configuration de l'application.



- **Domaines :** La colonne Domaines affiche une ou plusieurs lignes pour une application particulière. La première ligne affiche l'URL réelle de l'application que l'administrateur a saisie lors de l'ajout des détails de l'application. Les autres lignes sont tous des domaines associés qui sont saisis lors de l'ajout des détails de l'application. Si l'URL de l'application et les domaines associés sont identiques, ils sont affichés sur une seule ligne.

Une ligne affiche l'URL d'assertion SAML, si SAML SSO est sélectionné.

- **Type :** Sélectionnez l'une des options suivantes.
  - **Interne** –**Contourner le proxy** - Le trafic du domaine est acheminé via Citrix Cloud Connector, en contournant le proxy Web du client configuré sur l'appliance Connector.
  - **Interne via le connecteur** - Les applications sont externes mais le trafic doit circuler via l'appliance Connector vers le réseau extérieur.
  - **Externe** –Le trafic circule directement vers Internet.
- **Emplacement de la ressource :** Rempli automatiquement lorsque vous sélectionnez le type Interne pour une application. Modifiez-le si un emplacement de ressource différent est souhaité.
- **État de l'appliance connecteur :** Rempli automatiquement, avec l'emplacement de la ressource, lorsque vous sélectionnez le type Interne pour une application.

Sites Web non autorisés

October 21, 2024

Les applications (intranet ou Internet) qui ne sont pas configurées dans Secure Private Access sont considérées comme des « sites Web non autorisés ». Par défaut, Secure Private Access refuse l'accès à toutes les applications Web intranet s'il n'existe aucune application ni politique d'accès configurée pour ces applications.

Pour toutes les autres URL Internet ou applications SaaS qui n'ont pas d'application configurée, les administrateurs peuvent utiliser l'onglet **Paramètres > Sites Web non autorisés** de la console d'administration pour autoriser ou refuser l'accès via Citrix Enterprise Browser. Les administrateurs peuvent également rediriger l'accès vers un environnement RBI (Remote Browser Isolé) pour empêcher les attaques basées sur le navigateur. Si un administrateur a configuré la redirection des URL vers RBI, les actions suivantes se produisent.

1. Secure Private Access convertit les domaines.
2. Citrix Enterprise Browser renvoie ensuite ces URL à Secure Private Access.
3. Secure Private Access redirige ces URL vers le service d'isolation du navigateur à distance.

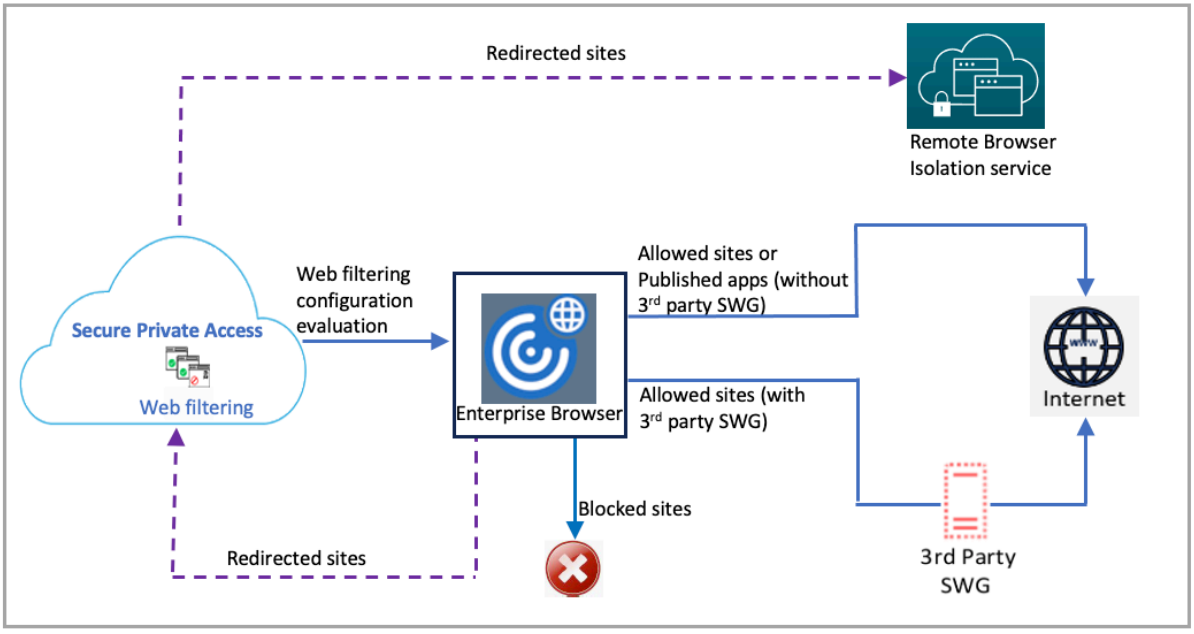
Vous pouvez utiliser des caractères génériques, tels que `*.example.com`, pour contrôler l'accès à tous les domaines de ce site Web et à toutes les pages de ce domaine.

> **Remarque**
>
> Par défaut, les paramètres sont configurés pour AUTORISER l'accès à toutes les URL Internet ou applications SaaS via Citrix Enterprise Browser.

Comment fonctionnent les sites Web non autorisés

1. Une vérification d'analyse d'URL est effectuée pour déterminer si l'URL est une URL de service Citrix.
2. L'URL est ensuite vérifiée pour déterminer s'il s'agit d'une URL d'application Web d'entreprise ou SaaS.
3. L'URL est ensuite vérifiée pour déterminer si elle est identifiée comme une URL bloquée, si elle doit être redirigée vers une session de navigateur sécurisée ou si l'accès à l'URL est autorisé.

L'illustration suivante explique le flux de trafic de l'utilisateur final.

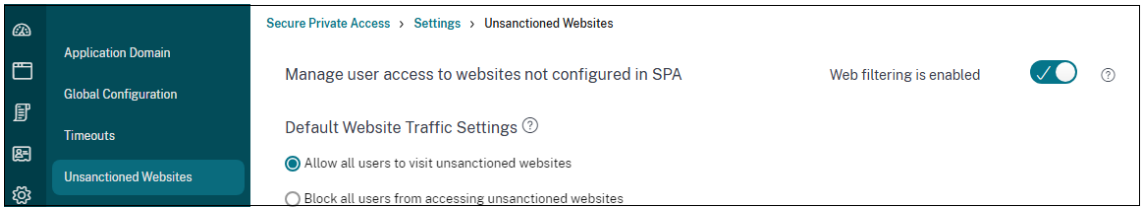


Lorsqu'une demande arrive, les vérifications suivantes sont effectuées et les actions correspondantes sont entreprises :

1. La demande correspond-elle à la liste blanche globale ?
    a) Si cela correspond, l'utilisateur peut accéder au site Web demandé.
    b) Si cela ne correspond pas, les listes de sites Web sont vérifiées.
2. La demande correspond-elle à la liste des sites Web configurés ?
    a) Si cela correspond, la séquence suivante détermine l'action.
        i. Bloquer
        ii. Rediriger
        iii. Allow
    b) Si cela ne correspond pas, l'action par défaut (AUTORISER) est appliquée. L'action par défaut ne peut pas être modifiée.

Configurer des règles pour les sites Web non autorisés

1. Dans la console Secure Private Access, cliquez sur **Paramètres > Sites Web non autorisés**.



Remarque

- La fonction de filtrage Web est activée par défaut et l'accès à toutes les URL Internet non autorisées est autorisé.
- Vous pouvez modifier le paramètre sur **Bloquer l'accès de tous les utilisateurs aux sites Web non autorisés** pour bloquer l'accès à n'importe quelle URL Internet via Citrix Enterprise Browser pour tous les utilisateurs.

```
1  ![Configurer des règles](/en-us/citrix-secure-private-access/media/spa-
       enable-website-list-filtering.png)
2
3  Vous pouvez également modifier les paramètres d'URL spécifiques en les
       ajoutant à des sites Web bloqués, à des sites Web autorisés ou en
       les redirigeant vers la liste d'isolation du navigateur à distance.
4
5  Par exemple, si vous avez bloqué l'accès à toutes les URL non autorisé
       es par défaut et que vous souhaitez autoriser l'accès à quelques URL
        Internet spécifiques uniquement, vous pouvez le faire en procédant
       comme suit :
6
7  1.  Cliquez sur l ' onglet **Sites Web autorisés** , puis cliquez sur **
       Autoriser un site Web**.
8  1.  Ajoutez l'adresse du site Web auquel l'accès doit être autorisé.
       Vous pouvez soit ajouter manuellement l'adresse du site Web, soit
       faire glisser et déposer un fichier CSV contenant l'adresse du site
       Web.
9  1.  Cliquez sur **Ajouter une URL** puis cliquez sur **Enregistrer**.
10
11     L'URL est ajoutée à la liste des sites Web autorisés.
```

Remarque

Un client payant du service Remote Browser Isolation Standard (organisation) bénéficie par défaut de 5 000 heures d'utilisation par an. Pour plus d'heures, ils doivent acheter les packs complémentaires du navigateur sécurisé. Vous pouvez suivre l'utilisation du service d'isolation du navigateur à distance. Pour plus d'informations, consultez les rubriques suivantes :

- Gérer et surveiller les navigateurs isolés distants
- Isolation du navigateur à distance.

Points à noter

Si les utilisateurs n'ont pas accès à une application SaaS, ils ne peuvent pas lancer l'application depuis Citrix Enterprise Browser. Toutefois, ils pourront peut-être toujours accéder à l'application en saisissant l'URL directement dans Citrix Enterprise Browser.

- Si l'accès à une application est refusé par la politique, l'URL de l'application est ajoutée à la liste bloquée si la fonctionnalité **Filtrage Web** est activée. Cela garantit que toute tentative d'accès à l'application, que ce soit via Citrix Enterprise Browser ou directement via URL, est bloquée.
- Pour les applications non publiées, même si le routage est configuré, l'accès à ces applications est refusé. L'URL de l'application non publiée est ajoutée à la liste bloquée si la fonctionnalité **Filtrage Web** est activée, empêchant toute tentative d'accès.

Intégration ADFS avec Secure Private Access

December 27, 2023

Les règles relatives aux réclamations sont nécessaires pour contrôler le flux de réclamations dans le pipeline de réclamations. Les règles de réclamation peuvent également être utilisées pour personnaliser le flux de réclamations pendant le processus d'exécution de la règle de réclamation. Pour plus d'informations sur les revendications, consultez la documentation Microsoft.

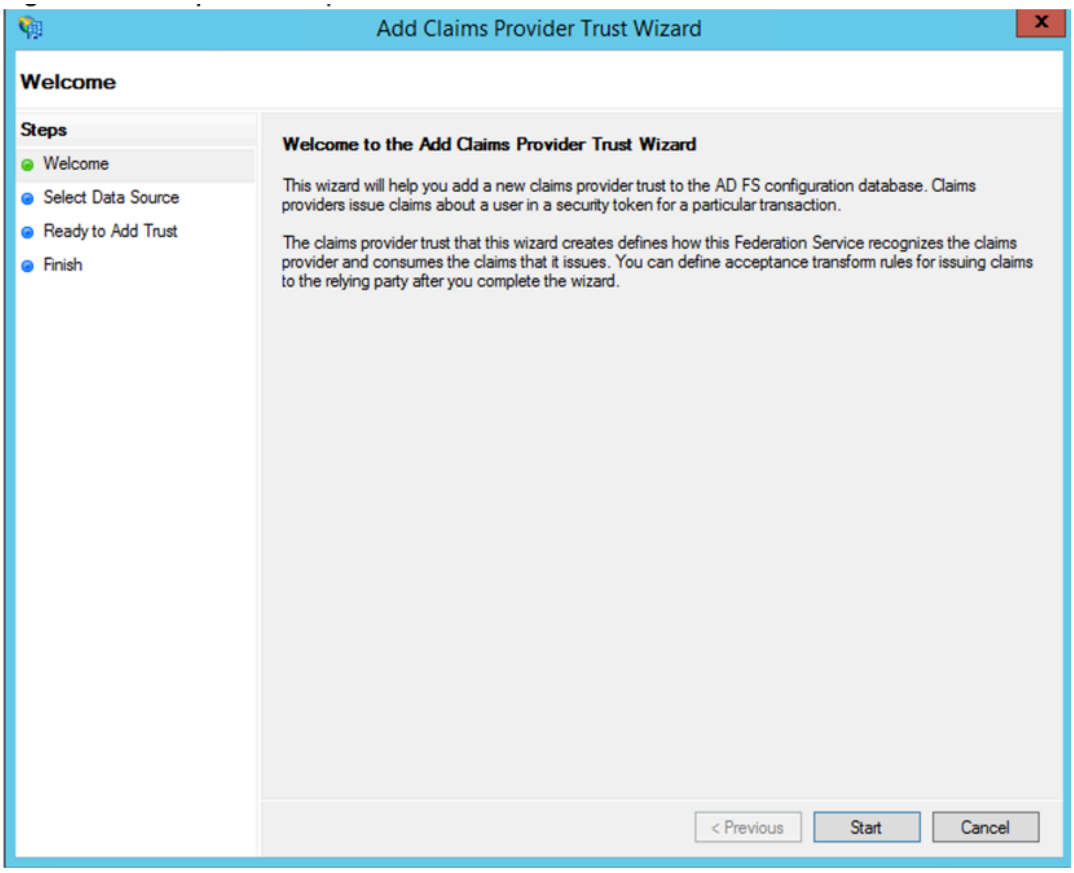
Pour configurer ADFS afin qu'il accepte les réclamations de Citrix Secure Private Access, vous devez effectuer les étapes suivantes :

1. Ajoutez la confiance du fournisseur de réclamation dans ADFS.
2. Terminez la configuration de l'application sur Citrix Secure Private Access.

Ajoutez la confiance du fournisseur de réclamation dans ADFS

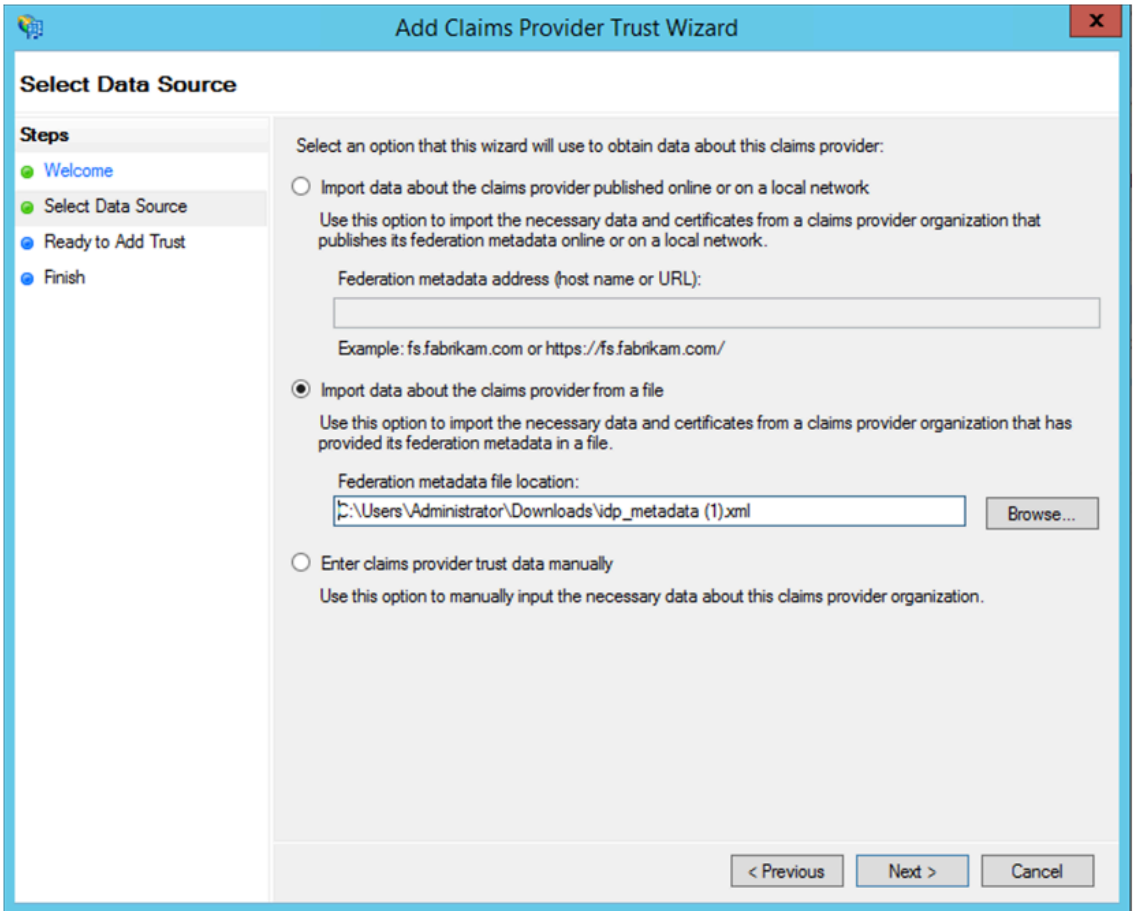
1. Ouvrez la console de gestion ADFS. Accédez à **ADFS > Relation de confiance > Confiance du fournisseur de réclamation**.

    a) Cliquez avec le bouton droit de la souris et sélectionnez **Ajouter une approbation**

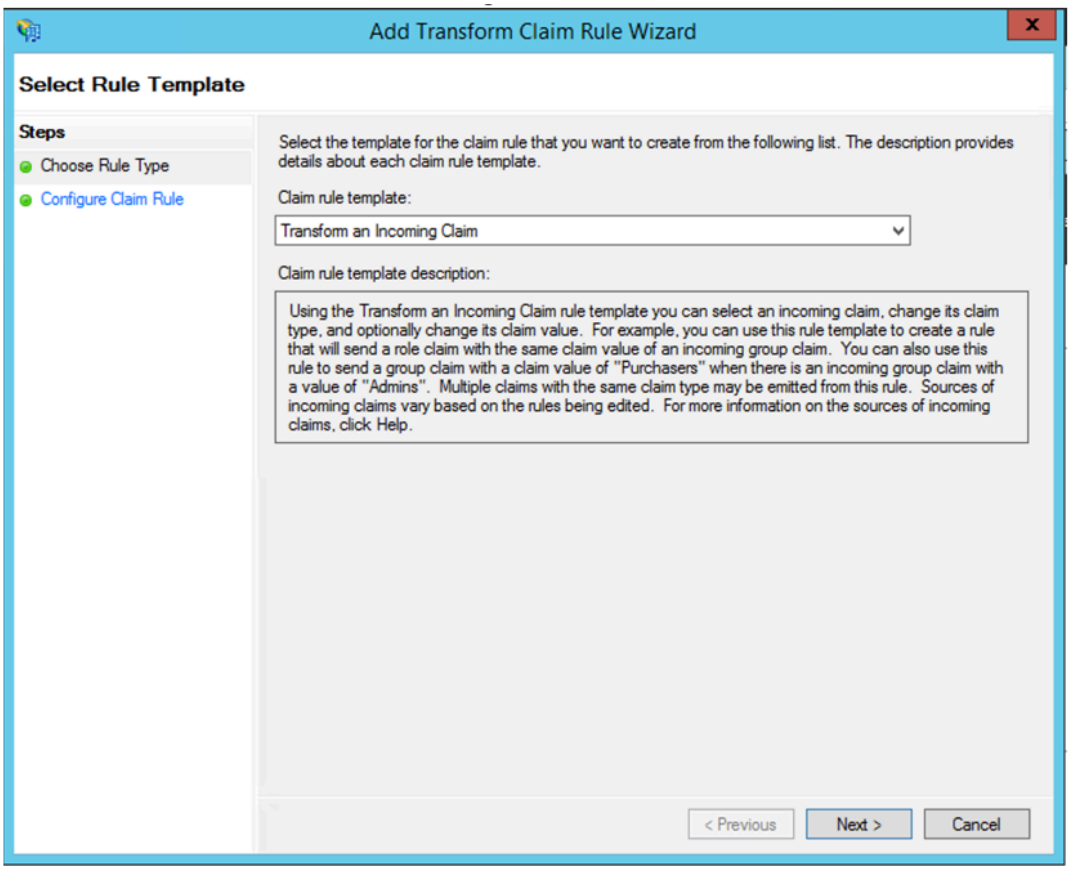


b) Ajoutez une application dans Secure Private Access qui est utilisée pour fédérer vers ADFS. Pour plus de détails, consultez Configuration de l'application sur Citrix Secure Private Access.

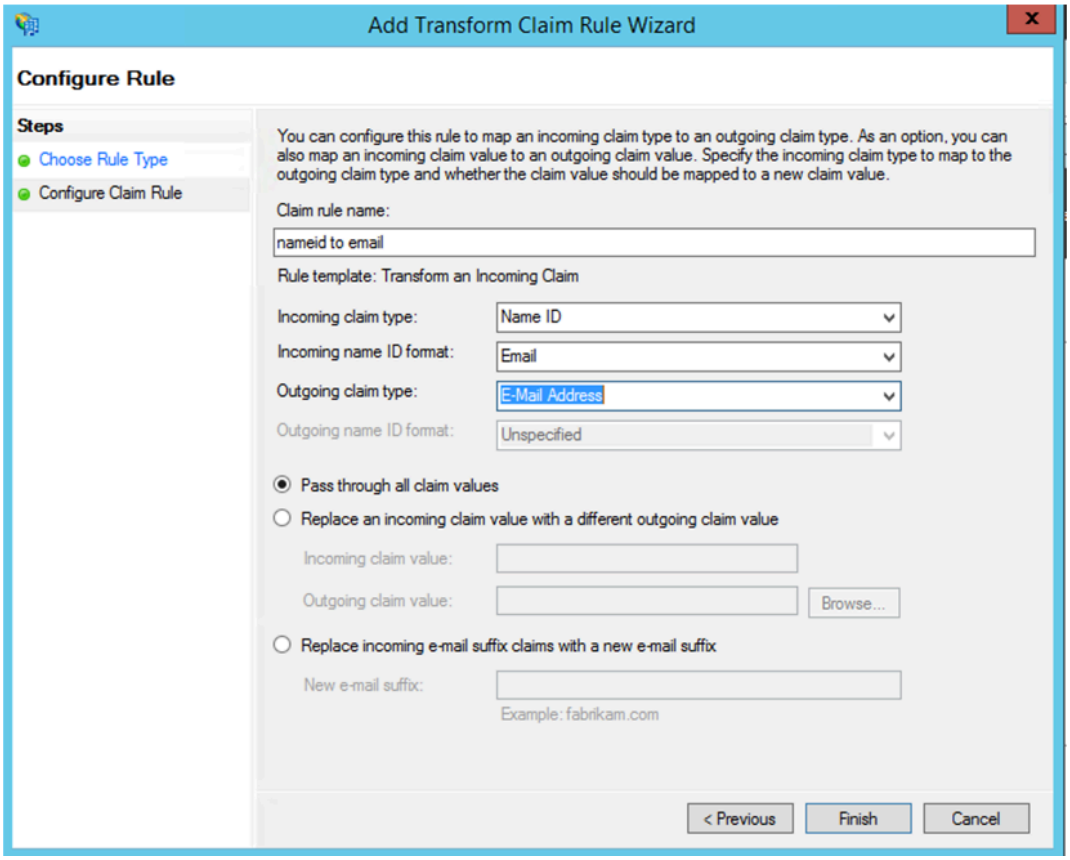
> **Remarque :**
>
> Ajoutez d'abord l'application et, à partir de la section de configuration SSO de l'application, vous pouvez télécharger le fichier de métadonnées SAML, puis importer le fichier de métadonnées dans ADFS.



a) Suivez les étapes pour terminer l'ajout de la confiance du fournisseur de réclamations. Une fois que vous avez terminé d'ajouter la confiance du fournisseur de revendications, une fenêtre permettant de modifier la règle de revendication s'affiche.
b) Ajoutez une règle de réclamation avec **Transformer une réclamation entrante**.



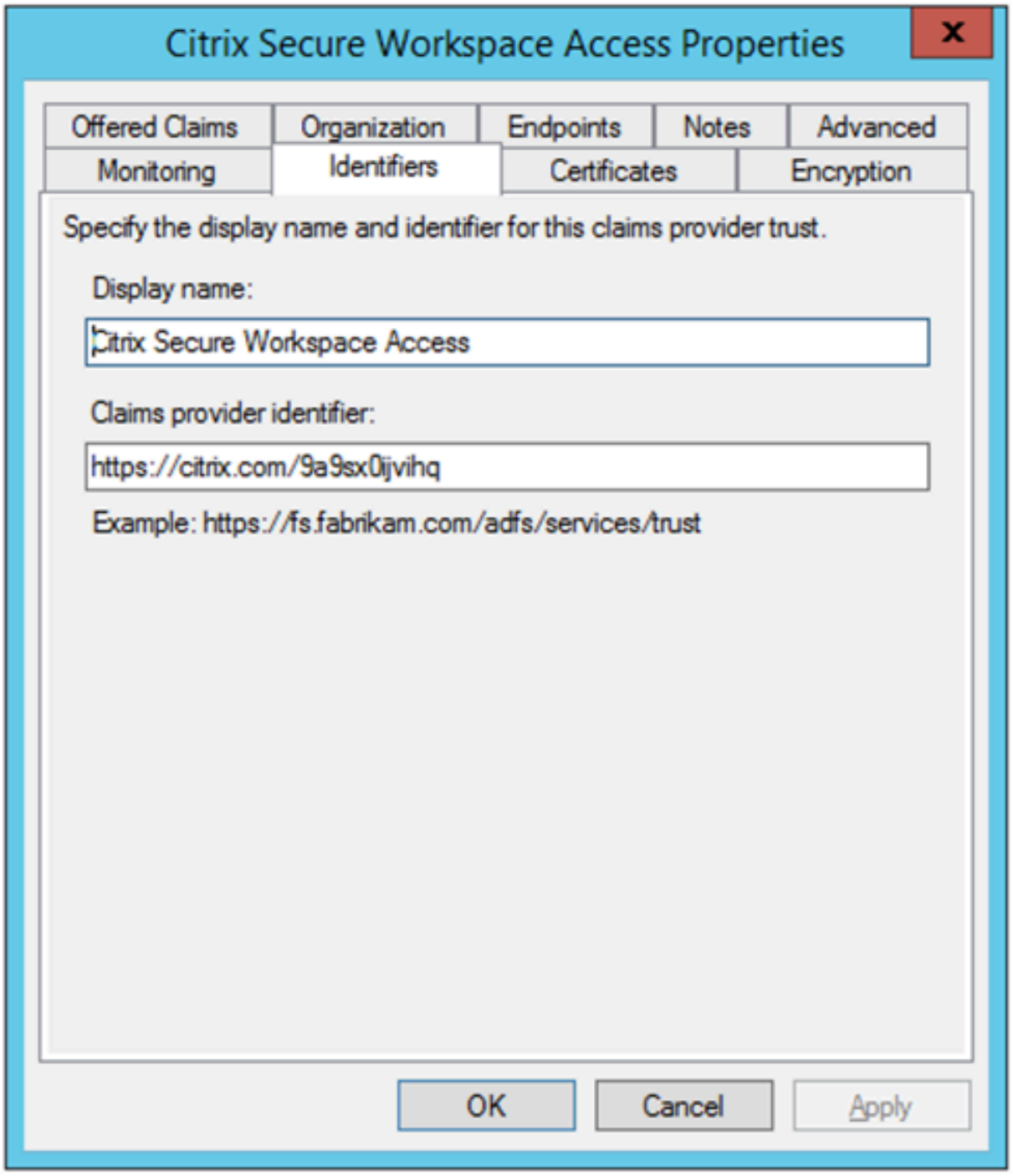
c) Complétez les paramètres comme indiqué dans la figure suivante. Si votre ADFS accepte d'autres revendications, utilisez-les et configurez l'authentification unique dans Secure Private Access également en conséquence.



Vous avez maintenant configuré l'approbation du fournisseur de revendications qui confirme qu' ADFS fait désormais confiance à Citrix Secure Private Access pour SAML.

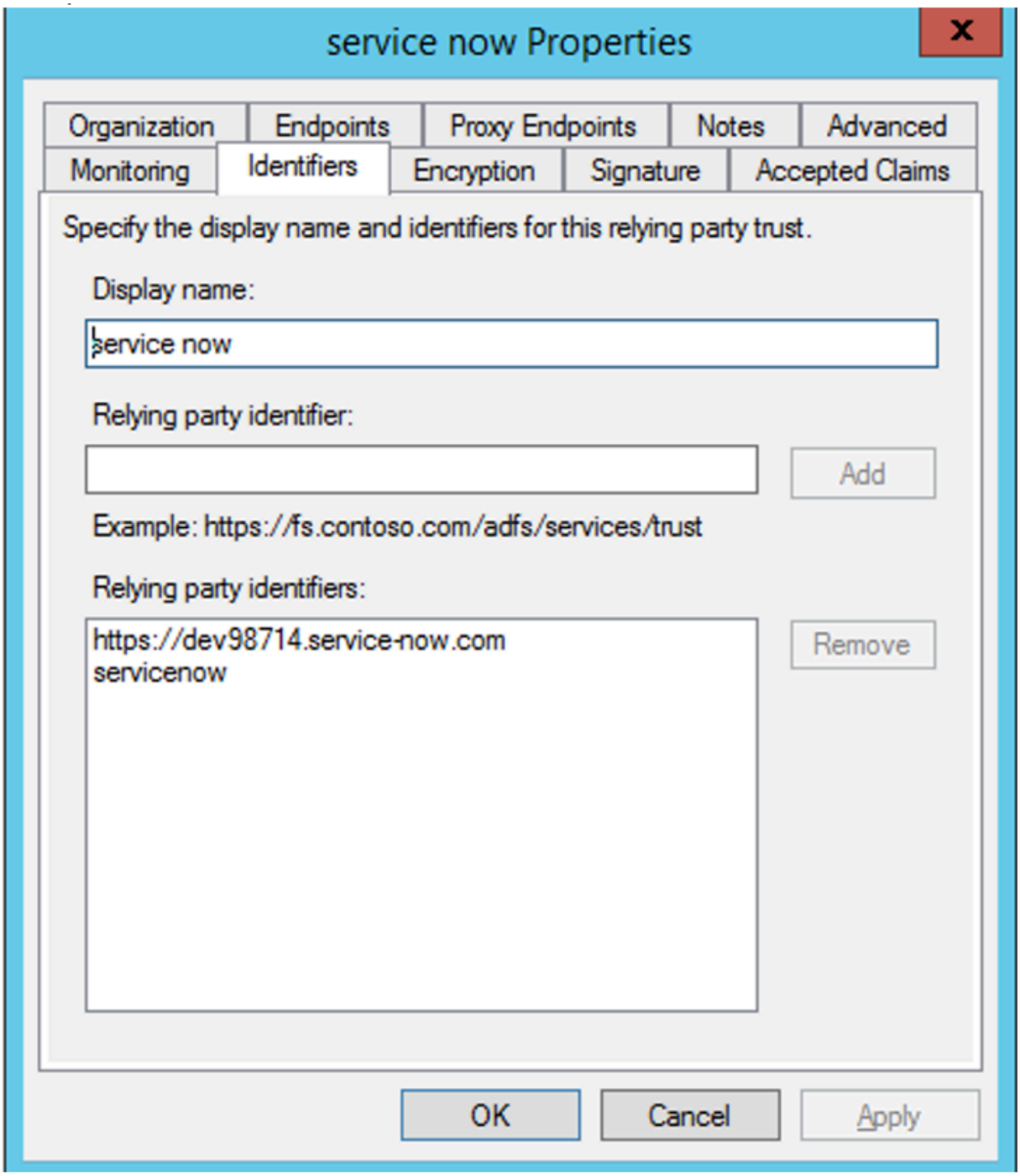
ID de confiance du fournisseur de réclamation

Notez l'identifiant de confiance du fournisseur de réclamation que vous avez ajouté. Vous avez besoin de cet ID lors de la configuration de l'application dans Citrix Secure Private Access.



Identifiant de la partie relais

Si votre application SaaS est déjà authentifiée à l'aide d'ADFS, l'approbation de la partie relais doit déjà être ajoutée pour cette application. Vous avez besoin de cet ID lors de la configuration de l'application dans Citrix Secure Private Access.



Activer l'état du relais dans le flux initié par IdP

RelayState est un paramètre du protocole SAML utilisé pour identifier la ressource spécifique à laquelle les utilisateurs accèdent une fois qu'ils sont connectés et dirigés vers le serveur de fédération de la partie de confiance. Si RelayState n'est pas activé dans ADFS, les utilisateurs voient une erreur après s'être authentifiés auprès des fournisseurs de ressources qui en ont besoin.

Pour ADFS 2.0, vous devez installer la mise à jour KB2681584 (correctif cumulatif 2) ou KB2790338 (correctif cumulatif 3) pour fournir la prise en charge RelayState. ADFS 3.0 intègre la prise en charge RelayState. Dans les deux cas, RelayState doit toujours être activé.

Pour activer le paramètre RelayState sur vos serveurs ADFS

1. Ouvrez le fichier.
   - Pour ADFS 2.0, entrez le fichier suivant dans le bloc-notes : %systemroot%\inetpub\adfs\ls\web.config
   - Pour ADFS 3.0, entrez le fichier suivant dans le bloc-notes : %systemroot%\ADFS\Microsoft.IdentityServ
2. Dans la section Microsoft.IdentityServer.Web, ajoutez une ligne pour UserElyStateForIdpInitiatedSignOn comme suit, et enregistrez la modification :
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - Pour ADFS 2.0, exécutez `IISReset` pour redémarrer IIS.
3. Pour les deux plates-formes, redémarrez les services de fédération Active Directory (`adfssrv`)`service`.
   Remarque : Si vous avez Windows 2016 ou Windows 10, utilisez la commande PowerShell suivante pour l'activer.
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

Lien vers les commandes - https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

Configuration de l'application sur Citrix Secure Private Access

Vous pouvez configurer le flux initié par l'IdP ou le flux initié par le SP. Les étapes de configuration du flux initié par l'IdP ou le SP dans Citrix Secure Private Access sont les mêmes, sauf que pour le flux initié par le SP, vous devez cocher la case **Lancer l'application à l'aide de l'URL spécifiée (initié par le SP)** dans l'interface utilisateur.

Flux initié par l'IdP

1. Lors de la configuration du flux initié par l'IdP, configurez les éléments suivants.
   - **URL de l'application** : utilisez le format suivant pour l'URL de l'application.
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```
   - **FQDN ADFS** : nom de domaine complet de votre configuration ADFS.

- **ID RP** —L'ID RP est l'identifiant que vous pouvez obtenir auprès de votre confiance de partie relais. Il s'agit de la même chose que l'identifiant de la partie relais. S'il s'agit d'une URL, le codage de l'URL se produit.
- **ID du fournisseur d'identité** : l'ID du fournisseur d'identité est le même que l'ID d'approbation du fournisseur de réclamation. S'il s'agit d'une URL, le codage de l'URL se produit.

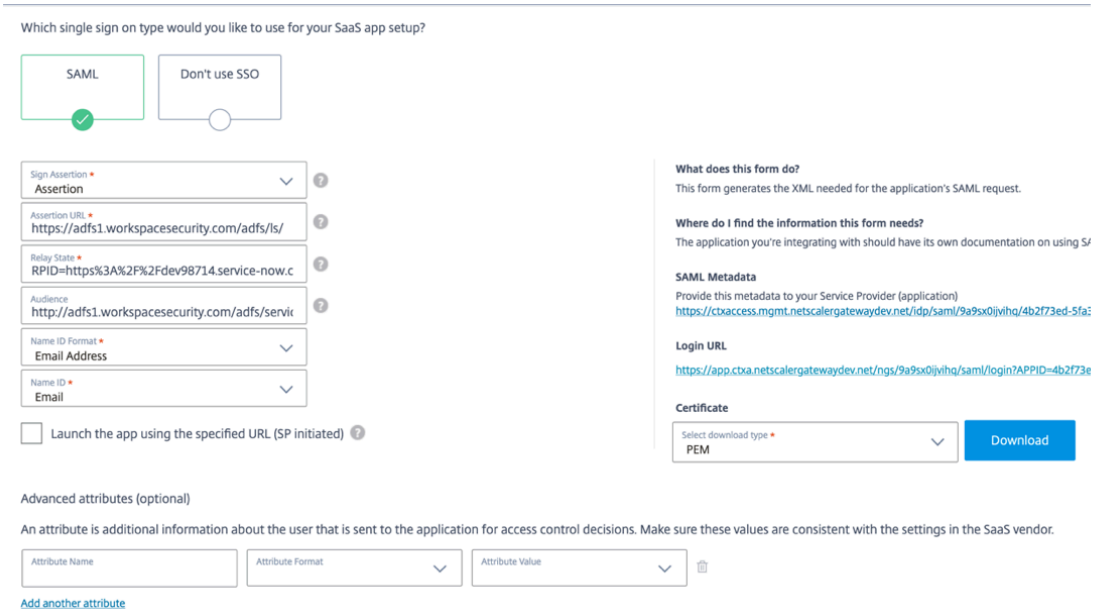
  Exemple : https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. Configuration de l'authentification unique SAML.

   Voici les valeurs par défaut du serveur ADFS. Si l'une des valeurs est modifiée, récupérez les valeurs correctes à partir des métadonnées du serveur ADFS. Les métadonnées de fédération du serveur ADFS peuvent être téléchargées à partir de son point de terminaison des métadonnées de fédération, dont le point de terminaison peut être connu sous **ADFS > Service > Endpoints.**

   - **URL d'assertion** —`https://<adfs fqdn>/adfs/ls/`
   - **État du relais** —L'état du relais est important pour le flux initié par l'IdP. Suivez ce lien pour le construire correctement - `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     Exemple : RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev987
     now.com%2F
   - **Public** —`http://<adfsfqdn>/adfs/services/trust`
   - Pour les autres paramètres de configuration SSO SAML, reportez-vous à l'image suivante. Pour plus de détails, consultez https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html



3. Enregistrez et abonnez l'application à l'utilisateur.

Flux initié par SP

Pour le flux initié par le SP, configurez les paramètres tels qu'ils sont capturés **dans la section Flux initié par le fournisseur**. En outre, activez la case à cocher **Lancer l'application à l'aide de l'URL spécifiée (initiée par le SP)** .

Dépréciations de fonctionnalités

August 26, 2024

Cet article vous informe à l'avance des fonctionnalités du service Secure Private Access qui sont progressivement supprimées, afin que vous puissiez prendre des décisions commerciales en temps opportun. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand retirer les fonctionnalités. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître. Pour plus d'informations sur la prise en charge du cycle de vie des produits, consultez la stratégie de prise en charge du cycle de vie d'un produit.

Le tableau suivant répertorie les fonctionnalités du service Secure Private Access qui sont obsolètes ou dont l'obsolescence est prévue.

Élément	Abandon annoncé	Date d'obsolescence	Solution alternative
Méthode d'accès VPN sans client pour accéder aux applications Web	Janvier 2023	17 octobre 2023	Utilisez le navigateur Citrix Enterprise ou Direct Access selon votre cas d'utilisation. Pour plus de détails, voir À propos de l'obsolescence de l'accès VPN sans client pour l'accès aux applications Web.
Filtrage Web basé sur des catégories	Décembre 2022	31 décembre 2022	La fonctionnalité d'autorisation, de refus ou de redirection RBI par site Web dans Secure Private Access sera conservée afin de fournir un accès sélectif à des sites Web non liés au travail à partir du navigateur Citrix Enterprise.
Restreindre le contrôle de sécurité	Avril 2022	15 juin 2022	S/O
Citrix Gateway Connector	Mai 2022	30 septembre 2022	Appliance Connector. Pour migrer votre Gateway Connector vers Connector Appliance, voir Migrer Gateway Connector vers Connector Appliance.

À propos de l'obsolescence de l'accès VPN sans client pour l'accès aux applications Web

- Qu'est-ce que la méthode d'accès au VPN sans client (VPN sans client) ?

Citrix Secure Private Access utilise la méthode d'accès basée sur le CVVPN lorsqu'une application Web interne, configurée sans aucune restriction de sécurité renforcée, est accessible via Workspace for Web (application Citrix Workspace pour HTML5).

> **Remarque :**
>
> La méthode d'accès VPN sans client n'est utilisée que lorsqu'une application interne est accessible via Workspace for Web (application Citrix Workspace pour HTML5). Seules les applications pour lesquelles des restrictions de sécurité renforcées ne sont pas configurées sont bloquées.

- Pourquoi désapprouvons-nous cette fonctionnalité ?

  La méthode VPN sans client utilise des réécritures d'URL côté client, ce qui présente certaines limites technologiques à l'échelle du secteur. Dans plusieurs cas, cela peut entraîner des échecs d'accès aux applications lorsque certains liens des applications Web sont réécrits. Cela entraîne une mauvaise expérience pour l'utilisateur final. Pour offrir la meilleure expérience d'accès aux applications à nos clients, nous désapprouvons cette fonctionnalité et recommandons de passer à l'une des alternatives mentionnées ci-dessous.

- Quel en sera l'impact sur les utilisateurs finaux qui accèderont aux applications configurées avec Secure Private Access ?

  Si une application Web configurée sans restrictions de sécurité renforcées est accessible via Workspace for Web, l'accès à cette application sera bloqué.
  Cela n'aura aucune incidence sur l'accès des utilisateurs finaux aux applications via l'application Workspace, Direct Access, le service Remote Browser Isolation (RBI) ou l'agent d'accès sécurisé.

- Quelles sont les alternatives et que doivent faire les administrateurs ?

  Navigateur Citrix Enterprise : utilisez l'application Citrix Workspace pour accéder à ces applications via le navigateur Citrix Enterprise. Cette méthode offre la meilleure expérience à l'utilisateur final grâce à des paramètres de sécurité améliorés (tels que la restriction des téléchargements, des restrictions d'impression, le filigrane, la restriction de l'accès au presse-papiers) et à la gestion du navigateur. Secure Private Access pour Citrix Workspace.
  Accès direct : si vous souhaitez une méthode sans client pour accéder aux applications Web, utilisez la méthode Direct Access, qui permet d'accéder directement aux applications depuis n'importe quel navigateur natif tel que Chrome. Cette méthode peut être utilisée dans les cas d'utilisation où l'application Citrix Workspace ne peut pas être installée sur le terminal ou pour les appareils non gérés. Pour plus de détails, voir Accès direct aux applications Web d'entreprise.

- Cela a-t-il un impact sur les applications existantes accessibles via l'application Citrix Workspace ou le Secure Access Agent ?

Non, nous bloquons uniquement l'accès aux applications Web accessibles via Workspace for Web. Cette désapprobation n'aura aucune incidence sur les applications accessibles via l'application Citrix Workspace ou les clients Secure Access installés sur les appareils finaux. Si une application Web configurée avec des restrictions de sécurité renforcées est accessible via Workspace for Web ou la variante HTML5 de l'application Citrix Workspace, l'accès à ces applications sera bloqué.

- Vous avez d'autres questions ?

  Contactez le support Citrix.