Citrix Secure Internet 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 Internet Access

January 26, 2022

Qu'est-ce que Citrix Secure Internet Access ?

Citrix Secure Internet Access (CSIA) est un service fourni dans le cloud qui fournit un accès sécurisé aux applications Web et SaaS, dans le monde entier. Il fournit une pile complète de fonctionnalités de sécurité, telles que la Secure Web Gateway, le courtier de sécurité d'accès au cloud, la protection contre les logiciels malveillants avec bac à sable, les systèmes de prévention et de détection des intrusions et la prévention contre la perte de données.

Avec le SD-WAN et Secure Workspace Access, Citrix Secure Internet Access constitue l'un des piliers de la solution Secure Access Service Edge (SASE) entièrement intégrée fournie par Citrix.

Citrix Secure Internet Access offre un accès sécurisé aux applications Web et SaaS à l'intérieur et à l'extérieur de Citrix Workspace, quel que soit l'emplacement de l'utilisateur. Il ajoute une couche de protection supplémentaire pour les utilisateurs de Citrix Workspace et s'intègre également à Citrix SD-WAN pour une solution de réseau et de sécurité Citrix entièrement convergente.

Caractéristiques et avantages de Citrix Secure Internet Access

Citrix Secure Internet Access permet de fournir une gestion unifiée des services mis à disposition via Citrix Cloud. La liste suivante résume les principales fonctionnalités et avantages de Citrix Secure Internet Access.

- **Gestion unifiée**.
  - Une vue holistique et un contrôle granulaire des fonctionnalités de sécurité complètes. Ces informations sont fournies sur une plateforme unique, ainsi que des analyses pour identifier les incidents de sécurité, les comportements inhabituels, les risques signalés, les pertes de productivité et les violations de politique.
  - Les utilisateurs disposant à la fois de droits SD-WAN et Citrix Secure Internet Access peuvent gérer ces services à partir du même volet. En conséquence, tout le trafic et les utilisateurs sont protégés par une combinaison d'architectures réseau et de sécurité sur une seule plateforme.
- **Efficacité**.
  - Déploiement simple et rapide, avec configuration automatisée entre Citrix SD-WAN et Citrix Secure Internet Access.

  - Architecture hautes performances qui évolue à la vitesse du cloud.
  - Architecture en un seul passage pour des performances optimales : le trafic est déchiffré une fois et tous les contrôles de sécurité sont appliqués avant d'être rechiffré.
  - Latence réduite avec le SD-WAN : sélection automatique du nœud de passerelle Citrix Secure Internet Access le plus proche.

- **Performances fiables**.
  - Mises à jour automatiques pour la dernière protection contre les menaces de sécurité.
  - Liens de secours pour une double résilience.
  - Dépannage plus rapide pour les services informatiques grâce à la vue unique et unifiée.

- **Intimité**. Les données de chaque client sont traitées via des passerelles distinctes et séparées par entreprise dans le service Citrix Secure Internet Access.

- **Meilleure expérience utilisateur de travail à distance**. Le fait de déplacer la sécurité du réseau vers le cloud, où les ressources auxquelles les utilisateurs souhaitent accéder sont déjà actives, rapproche la sécurité des utilisateurs. Le service Citrix Secure Internet Access possède plus de 100 points de présence (PoP) dans le monde entier.

Pour plus d'informations sur les principales fonctionnalités et avantages, consultez le dossier de solution.

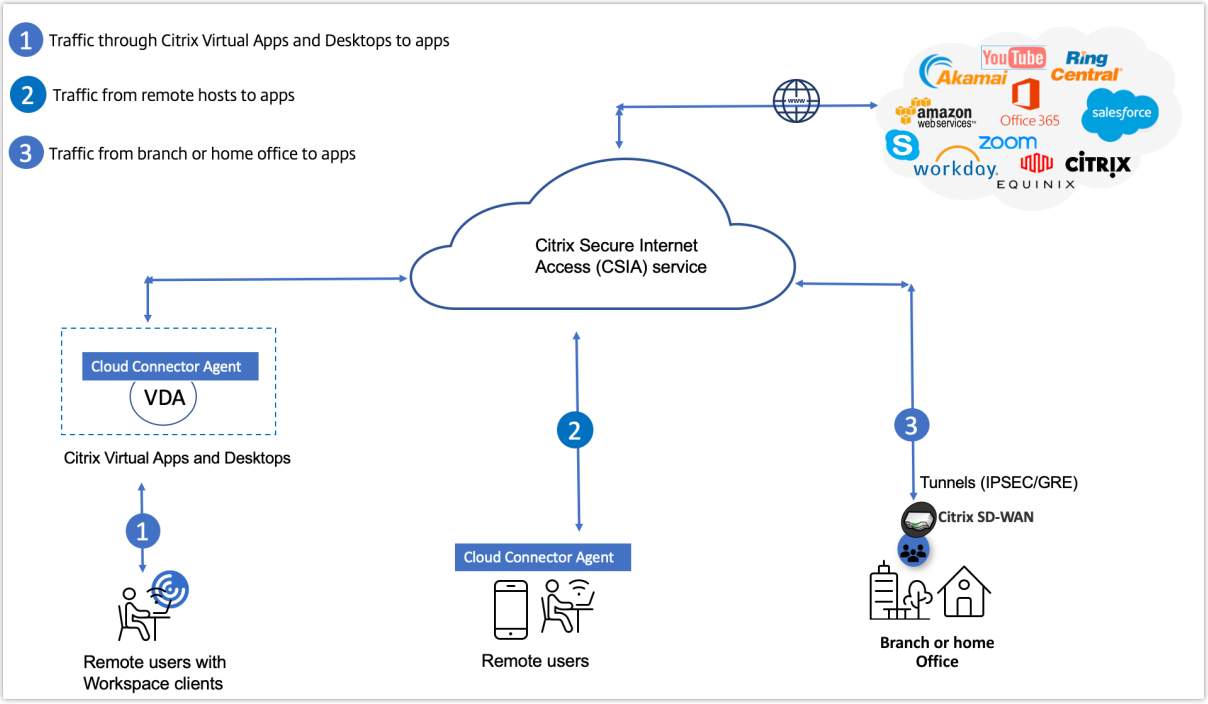
Comment fonctionne Citrix Secure Internet Access

Vos utilisateurs peuvent accéder à des applications Web et SaaS non autorisées en utilisant l'une des méthodes suivantes :

- via des bureaux virtuels à l'aide de Citrix Workspace
- à distance depuis des systèmes hôtes locaux
- depuis une succursale ou un bureau à domicile

Quelle que soit la méthode d'accès direct à Internet adoptée par l'utilisateur, le trafic est redirigé via Citrix Secure Internet Access.

Le schéma suivant est une représentation visuelle des différents cas d'utilisation.



Comme le montre l'image précédente, les trois principaux cas d'utilisation suivants décrivent le fonctionnement du processus.

1. **Citrix Virtual Apps and Desktops**. Les utilisateurs distants disposant d'applications Workspace peuvent accéder en toute sécurité aux applications Web et SaaS non autorisées via Citrix Virtual Apps and Desktops. Installez un agent CSIA Cloud Connector sur le Virtual Delivery Agent (VDA) pour rediriger le trafic Internet vers le service Citrix Secure Internet Access.

2. **Navigateurs natifs sur les systèmes hôtes**. Les utilisateurs distants peuvent accéder en toute sécurité à des applications non autorisées à l'aide de leurs systèmes locaux, tels que des ordinateurs portables et des appareils mobiles (gérés ou non gérés). Pour sécuriser le trafic sur ces appareils, installez les agents CSIA Cloud Connector pour rediriger tout le trafic Internet vers le service Citrix Secure Internet Access.

   L'agent Cloud Connector authentifie également l'utilisateur et installe les certificats appropriés pour le déchiffrement SSL. Les agents Cloud Connector sont disponibles pour les systèmes d'exploitation suivants : iOS, macOS, Android, Windows, Linux.

3. **Les succursales**. Les utilisateurs sur site peuvent accéder en toute sécurité aux applications Web et SaaS via Citrix SD-WAN en redirigeant le trafic vers Citrix Secure Internet Access. Cela se produit par le biais de tunnels IPSEC ou GRE, sans qu'un agent Cloud Connector soit nécessaire.

   Citrix SD-WAN crée automatiquement une connectivité sécurisée au point de présence (PoP) Citrix Secure Internet Access le plus proche. Le trafic passe par des tunnels IPsec ou GRE. La redondance est obtenue à la fois au niveau du tunnel et par le biais de plusieurs liens vers des points de présence Citrix Secure Internet Access principaux et secondaires.

Autres ressources

- Découvrez les éditions de licence disponibles. Voir Licences
- Passez en revue les conditions préalables avant de commencer l'intégration. Voir Exigences
- Commencez le processus d'intégration. Voir Intégration
- Configurez les agents Cloud Connector. Voir Configuration

Notes de publication

January 26, 2022

Les notes de mise à jour du service Citrix Secure Internet Access décrivent les nouvelles fonctionnalités, les problèmes résolus et les problèmes connus d'une version révisée. Les notes de mise à jour comprennent les sections suivantes :

- Nouveautés : les nouvelles fonctionnalités et améliorations de la version.
- Problèmes résolus : problèmes qui ont été corrigés dans la version.
- Problèmes connus : les problèmes existants et leur solution de contournement, le cas échéant.

Nouveautés

January 26, 2022

Cet article fournit une liste des dernières fonctionnalités destinées aux clients pour la version Citrix Secure Internet Access (CSIA) 2021-Q3.

2 décembre 2021

Prise en charge d'Azure Active Directory pour l'authentification unique

Azure Active Directory (AD) est également pris en charge en tant que fournisseur d'identité (IdP) pour l'authentification unique (SSO) avec un compte Citrix Secure Internet Access (CSIA). Par défaut, le compte CSIA est configuré avec les paramètres du fournisseur d'identité Citrix. Si Azure AD est activé pour le locataire Citrix, le compte CSIA est configuré avec l'IdP Azure AD pour la validation SSO. Actuellement, un compte CSIA donné peut être configuré pour avoir des paramètres IdP Azure AD ou Citrix IdP.

Intégration avec le service Citrix Secure Browser

Le service Citrix Secure Browser fournit une **isolation du navigateur à distance** en isolant la navigation Web afin de protéger le réseau d'entreprise contre les attaques basées sur le navigateur. Avec Citrix Secure Internet Access, vous pouvez créer et appliquer des règles de filtrage Web pour rediriger le trafic Web vers une instance de Secure Browser.

28 octobre 2021

Intégration

L'intégration de Citrix Secure Internet Access vous aide à configurer votre compte d'utilisateur une fois que vous avez obtenu l'accès au cloud et que vous avez terminé la configuration initiale. Vous devez effectuer certains paramètres d'intégration de base pour accéder à l'autre configuration CSIA. Vous ne pouvez pas afficher le portail de stratégie de configuration sans avoir terminé le processus d'intégration.

Paramètres du compte

La fonctionnalité **Paramètres du compte** permet de modifier/remplacer le nom du compte d'utilisateur qui apparaît pour votre compte dans le portail de services Citrix Secure Internet Access.

14 octobre 2021

Sauvegarde cloud hors ligne

Les paramètres de **sauvegarde hors ligne dans le cloud** permettent de stocker/enregistrer les paramètres de sauvegarde et les journaux des nœuds de reporting en fonction de la **région, de l'emplacement** et de l'**heure** que vous sélectionnez.

API Citrix Secure Internet Access avec prise en charge Swagger

Un ensemble d'API liées à la configuration est désormais disponible dans les documents Swagger . Les informations de l'API Swagger CSIA-Core sont disponibles dans la section sia-core-controller .

15 septembre 2021

Rôles prédéfinis

Client : le rôle Accès en lecture seule (mode Confidentialité) est introduit en tant que nouveau rôle prédéfini. Vous pouvez ajouter un utilisateur et attribuer ce rôle à partir de **Citrix Identity and Access Management**. Un utilisateur auquel est attribué le rôle **Client : accès en lecture seule (mode Confidentialité)** dispose d'un accès en lecture seule pour afficher toutes les fonctionnalités du service, à l'exception des **licences** et des **paramètres utilisateur**.

Paramètres d'e-mail

La page **Paramètres de messagerie** sous **Configuration > Paramètres du cloud** a été améliorée pour inclure les fonctionnalités suivantes :

- **Paramètres d'e-mail de test** : Vérifiez vos paramètres de messagerie.
- **Définir les paramètres par défaut** : renseignez les paramètres d'e-mail par défaut.
- **Destinataires des e-mails** : ajoutez des destinataires d'e-mail pour recevoir des alertes utilisateur et des demandes d'exception d'URL.

29 juillet 2021

Paramètres du cloud dans l'interface utilisateur Citrix Secure Internet Access

L'interface utilisateur prend désormais en charge les paramètres de configuration Cloud pour le serveur NTP, la maintenance de la plate-forme, les paramètres de mise à jour et la journalisation anonymisée. Pour plus d'informations, consultez Configuration.

Équilibrage de charge dans les tunnels

Citrix Secure Internet Access prend désormais en charge l'équilibrage de charge ECMP du service SD-WAN Orchestrator. Pour plus d'informations, consultez Équilibrage de charge ECMP.

29 avril 2021

Séparation Internet pour le trafic Cloud Connector

Le trafic vers les nœuds de cloud Citrix Secure Internet Access est redirigé via les services Internet au lieu des tunnels IPsec et GRE déployés sur le site. Avec cette cassure directe, vous évitez de créer un tunnel dans le trafic deux fois.

Notifications

Pour vous assurer de ne pas manquer de messages importants concernant l'abonnement iboss et les modifications de configuration, le service Citrix Secure Internet Access affiche des alertes sous forme de notifications dans le tableau de bord.

Réaffectation des utilisateurs

Pour réduire la latence dans certains emplacements, vous pouvez désormais reconfigurer l'emplacement de vos nœuds au sein d'une région géographique. Vous pouvez également modifier le nombre d'utilisateurs affectés à ces nœuds.

Prise en charge de plusieurs liens avec les tunnels IPsec et GRE

Distribuez le trafic réseau sur plusieurs tunnels en parallèle en configurant des tunnels à partir d'un seul emplacement avec plusieurs connexions ISP vers les mêmes points de présence du fournisseur de services (POP).

Carte du réseau des POP sous un nœud

Affichez les points de présence (POP) utilisés par un client et les succursales SD-WAN qui se connectent aux points de présence Citrix Secure Internet Access.

Paramètres du rôle (Technical Preview)

Citrix propose un contrôle d'accès basé sur les rôles (RBAC). Le contrôle d'accès basé sur les autorisations vous permet de personnaliser les rôles basés sur les autorisations et d'ajouter ces rôles à différents utilisateurs.

Problèmes résolus

January 26, 2022

Les problèmes suivants ont été corrigés.

28 octobre 2021

SIAS-27 : Les graphiques Data Loss Prevention (DLP) sont désormais étiquetés avec des noms lors de l'utilisation de modèles de recherche d'analyse de contenu.

SIAS-290 : La section des détails du rapport d'état du cloud n'est plus coupée.

SIAS-394 : Les alertes pour les avis et les incidents incluent les informations du centre de données concerné.

SIAS-451 : Les contrôles d'application personnalisés du Cloud Access Security Broker (CASB) étaient désormais rendus dans l'interface utilisateur.

15 septembre 2021

SIAS-218 : Le provisionnement des SKU d'essai pour la région du Moyen-Orient ne se termine pas correctement.

SIAS-302 : L'activation des rapports et l'envoi de notifications par e-mail d'alerte nécessitaient des modifications des paramètres de messagerie. Le problème est maintenant résolu en renseignant les champs **Configuration > Paramètres de messagerie** avec des valeurs par défaut.

SIAS-306 : La page **Configuration > Paramètres utilisateur** est affichée (au lieu d'être masquée) aux administrateurs qui n'ont pas accès à la page. En cas de tentative d'accès, une erreur s'affiche.

SIAS-307 : Le fait d'avoir des rôles d'utilisateur avec des autorisations en lecture seule peut mettre en cache les données d'un client et les présenter comme les données d'un autre locataire.

SIAS-329 : Le format des alertes et des notifications par e-mail d'état du cloud est modifié pour inclure les statuts de maintenance, d'incident ou de message d'avertissement suivants :

- Nouveau
- Actualisé
- Reprogrammé
- terminé
- Annulé

SIAS-395 : Les notifications de recatégorisation d'URL sont améliorées pour inclure l'état, l'ancienne catégorie et la nouvelle catégorie pour l'URL demandée.

29 juillet 2021

SIAS-1 : Les utilisateurs reçoivent une page de blocage pour l'application write.com

SIAS-161 : Le client 32 bits Win7 ne se connecte pas.

SDW-18408 : Les utilisateurs disposant des mêmes autorisations pour Citrix Secure Internet Access et SD-WAN sont affichés en double dans les paramètres **Modifier le rôle** .

NSSDW-32478 : Les rôles d'utilisateur pour l'étendue du client sont affichés en double pour un utilisateur donné pour un client SIA + SD-WAN

29 avril 2021

NSSDW-33107 : La connectivité du tunnel GRE à partir de Citrix SD-WAN n'est pas prise en charge.

NSSDW-33099 : Frame Breakout pour connecteur Android.

NSSDW-33530 : Les requêtes Postgres ne sont pas chiffrées entre la passerelle/les serveurs de reporting.

NSSDW-34575 : Le **proxy et la mise en cache** ne sont pas en cours de chargement.

Problèmes connus

January 26, 2022

Le service Citrix Secure Internet Access présente les problèmes suivants :

SIAS-13 : Le blocage Ultrasurf nécessite une configuration supplémentaire au-delà des paramètres du protocole d'évasion.

SIAS-22 : Sur le portail de stratégie de configuration, certains paramètres peuvent ne pas s'appliquer aux déploiements Citrix Secure Internet Access.

Mise en route

January 26, 2022

Cet article explique comment démarrer avec Citrix Secure Internet Access (CSIA) pour la première fois.

Avant de commencer la configuration initiale, consultez les informations relatives aux licences et aux conditions préalables .

Conditions préalables

Vérifiez que vous disposez des éléments suivants :

- **Compte Citrix Cloud**. Pour utiliser Citrix Secure Internet Access, vous devez disposer d'un compte Citrix Cloud. Accédez à https://citrix.cloud.com et vérifiez que vous pouvez vous connecter avec votre compte Citrix Cloud existant.

  Si vous n'avez pas de compte Citrix Cloud, créez d'abord un compte Citrix Cloud. Vous pouvez également rejoindre un compte existant créé par un autre membre de votre organisation. Pour obtenir des processus détaillés et des instructions sur la façon de procéder, consultez S'inscrire à Citrix Cloud.

- **Déploiement Citrix Virtual Apps and Desktops** accessible via Citrix Workspace.
- **L'application Workspace** sur vos systèmes hôtes tels que les ordinateurs portables et les appareils mobiles.
- **Déploiements SD-WAN**. Si vous travaillez depuis une succursale, vous devez disposer des déploiements suivants :
  - Citrix SD-WAN 11.1 et versions ultérieures
  - Abonnement au service Citrix SD-WAN Orchestrator. Assurez-vous d'avoir effectué la configuration initiale et configuré les sites sur votre SD-WAN Orchestrator.

Configuration initiale

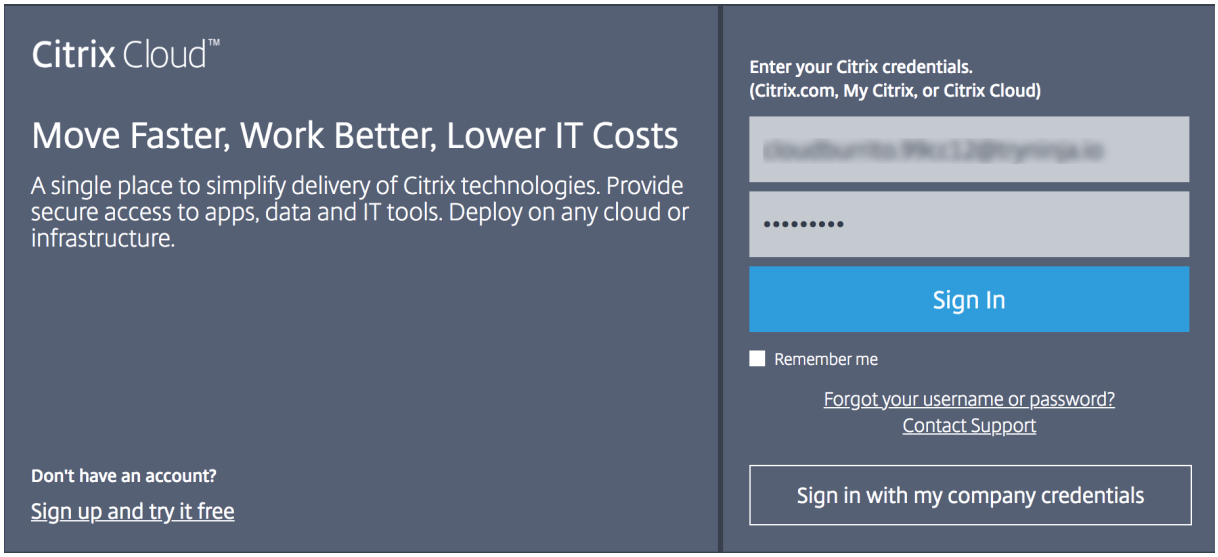
Cette section décrit les tâches requises pour la configuration initiale de Citrix Secure Internet Access.

Étape 1 : Demander l'accès à Citrix Secure Internet Access

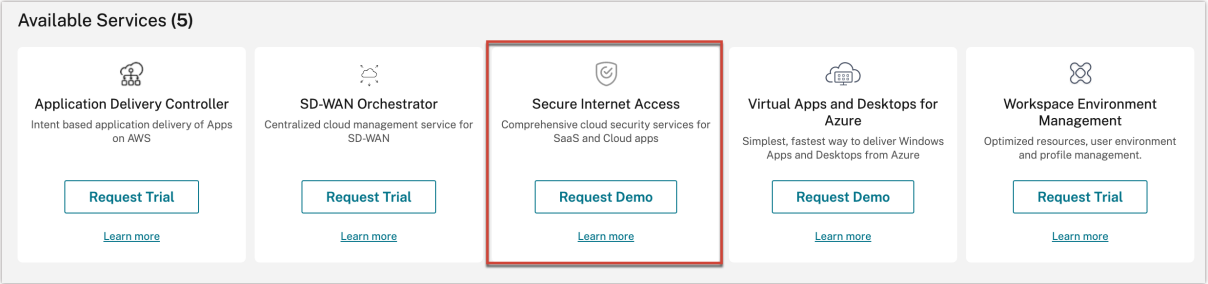
Vous pouvez accéder à Citrix Secure Internet Access en demandant un essai de Citrix Secure Internet Access. Vous pouvez utiliser l'essai pendant une période maximale de 60 jours. Pour plus d'informations sur les essais de service, consultez la section Essais de service Citrix Cloud.

Pour demander un essai,

Connectez-vous à votre compte Citrix Cloud.

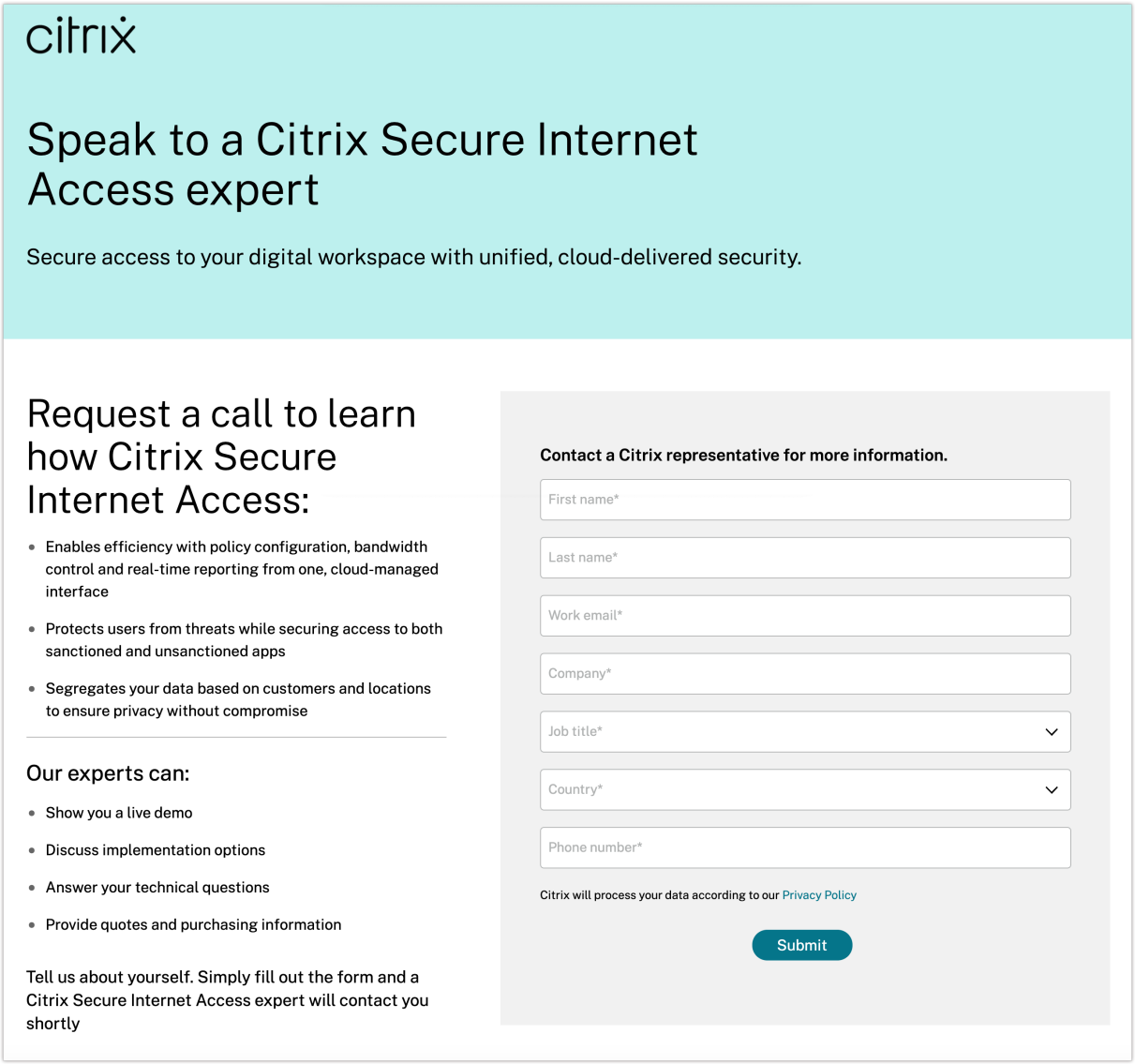


Sur la page d'accueil Citrix Cloud, dans **Services disponibles**, sur la vignette **Secure Internet Access**, cliquez sur **Demander une démo**.



> **Remarque**
>
> Vous pouvez également vous rendre sur https://www.citrix.com/products/citrix-secure-internet-access/form/inquiry/ et contacter un expert Citrix qui pourra vous aider.

Entrez les informations requises et sélectionnez **Soumettre**.



Lorsque votre essai est approuvé, Citrix lance le processus d'évaluation et crée votre package d'habilitation client en fonction du pack de licences sélectionné. Vous recevez également un e-mail de confirmation.

Étape 2 : Afficher l'état de votre compte

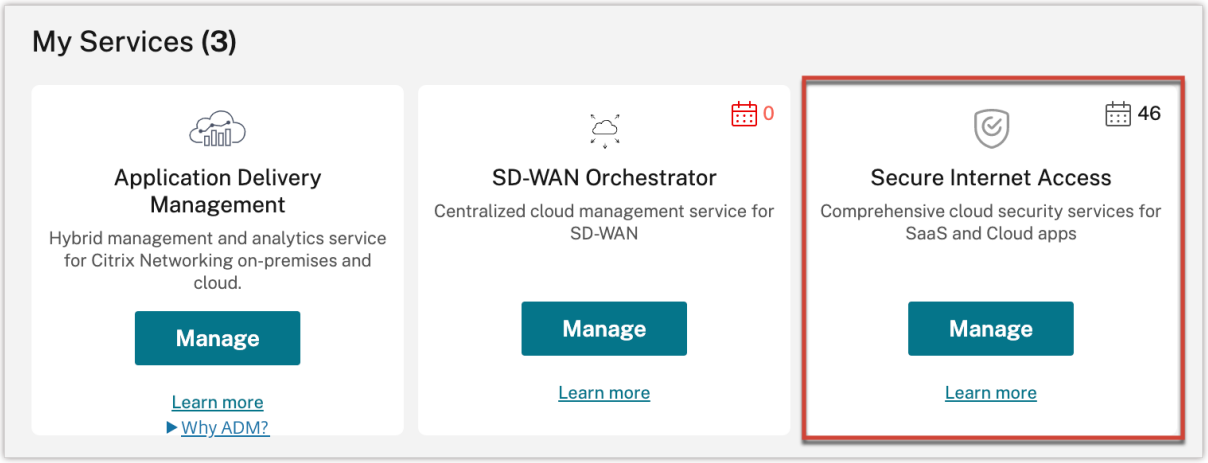
Une fois votre essai approuvé et lancé, vous recevrez un e-mail de confirmation et vous pourrez également consulter l'état de votre compte sur Citrix Cloud.

Pour configurer votre compte, Citrix fournit des nœuds de passerelle pour vous de manière implicite. Ces nœuds sont des nœuds conteneurisés qui analysent les données et le trafic dans le cloud. Les nœuds exécutent également des fonctions de sécurité telles que le filtrage Web, la prévention des logiciels malveillants et la prévention de la perte de données.

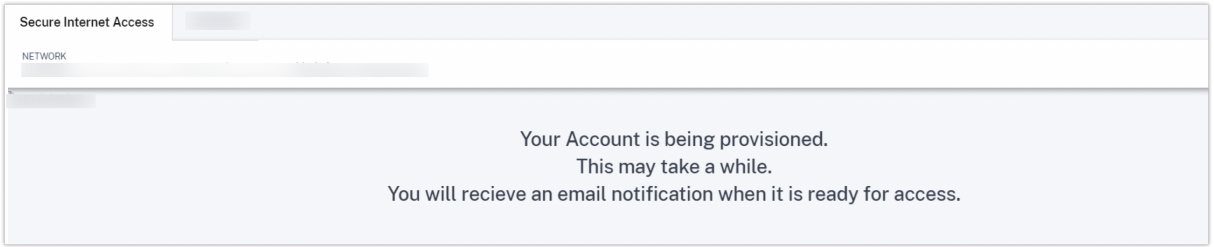
Une fois les nœuds configurés, vous recevez une notification par e-mail indiquant que votre compte est disponible. Le provisionnement des nœuds peut prendre quelques jours.

Pour consulter l'état de votre compte

1. Connectez-vous à votre compte Citrix Cloud.
2. Sur la page d'accueil de **Citrix Cloud**, dans **Mes services**, sur la vignette **Secure Internet Access**, cliquez sur **Gérer**.



Si la mise en service de votre compte est en cours, le message suivant s'affiche :

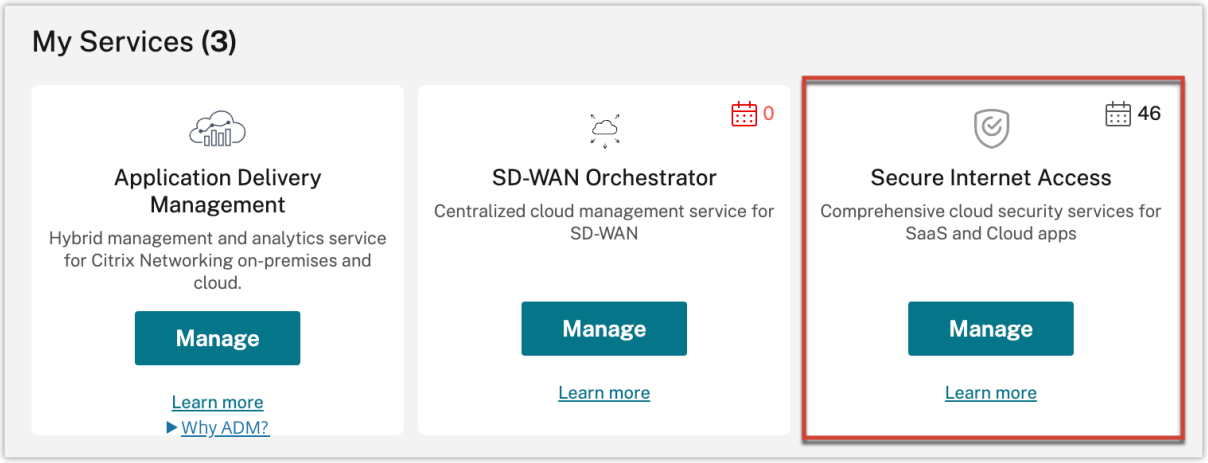


Étape 3 : Gérer Citrix Secure Internet Access

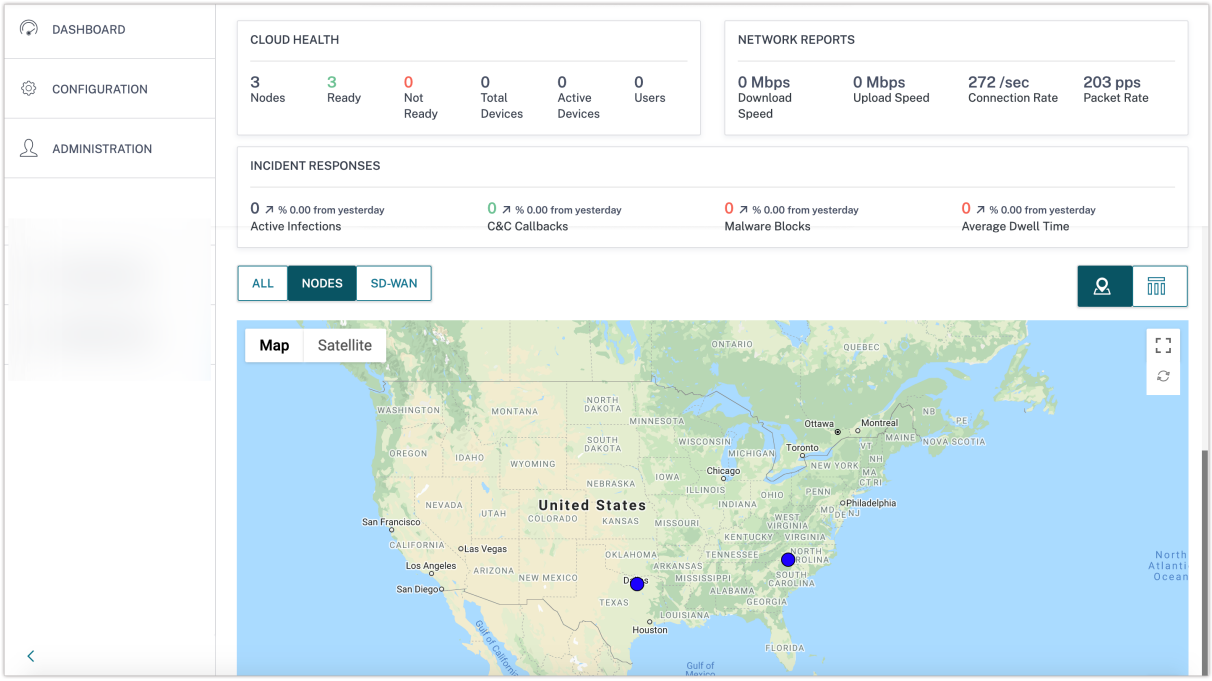
Après avoir reçu l'e-mail de confirmation concernant la configuration de votre compte, connectez-vous à Citrix Cloud et commencez à configurer et à gérer votre déploiement.

Sur la page d'accueil de **Citrix Cloud**, dans **Mes services**, sur la vignette **Secure Internet Access**, cliquez sur **Gérer**.

> **Remarque**
>
> Si vous avez un abonnement Citrix SD-WAN Orchestrator, vous pouvez également cliquer sur **Gérer** dans la vignette **SD-WAN Orchestrator** pour afficher le tableau de bord Citrix Secure Internet Access.



Dans le menu **Tableau de bord**, vous pouvez afficher l'état et une représentation graphique de vos nœuds.



La configuration initiale est maintenant terminée.

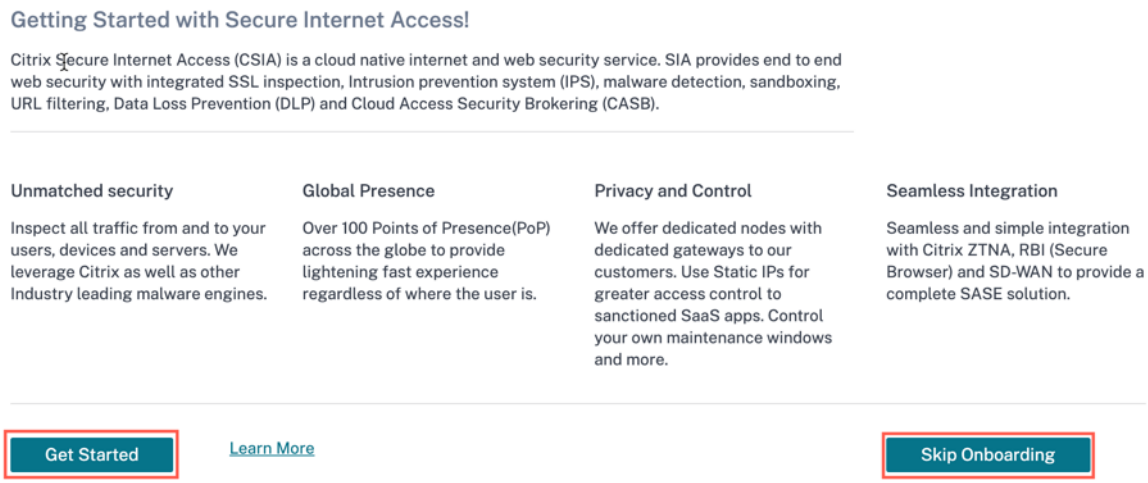
Intégration

L'intégration Citrix Secure Internet Access vous permet de configurer votre compte d'utilisateur une fois votre compte configuré. Vous devez effectuer certains paramètres d'intégration de base pour accéder à l'autre configuration CSIA.

L'option **Ouvrir la configuration Citrix SIA** est disponible sur la page d'**accueil de la configuration réseau** . Vous ne pouvez pas afficher le portail de stratégie de configuration sans avoir terminé le

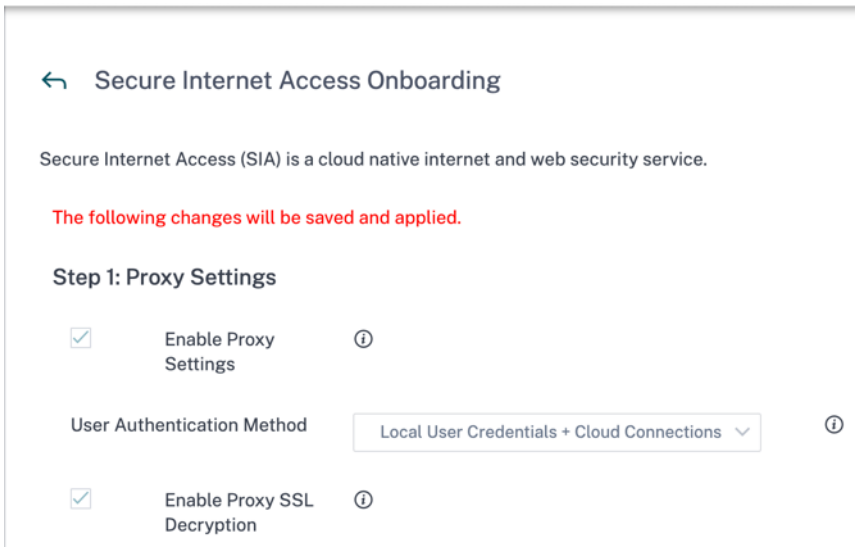
processus d'intégration.

Une fois votre compte configuré, vous accédez par défaut à la page d'intégration de Citrix Secure Internet Access. Cliquez sur **Commencer** pour poursuivre le processus d'intégration ou cliquez sur **Ignorer l'intégration** pour ignorer cette étape et effectuer l'intégration plus tard. Lorsque vous cliquez sur **Ignorer l'intégration**, vous accédez à la page du tableau de bord Citrix Secure Internet Access.



1. Configurer les paramètres du proxy

   Sélectionnez la méthode d'authentification de l'utilisateur dans la liste déroulante. La valeur par défaut est définie sur **Informations d'identification de l'utilisateur local+Connexions cloud**.



   Les quatre méthodes d'authentification sont les suivantes :

   - **Informations d'identification de l'utilisateur local+connexions cloud** : connectez-vous avec un compte d'accès Internet sécurisé local. Cette méthode prend également en charge le mode agent qui permet aux agents/points d'extrémité d'accès Internet

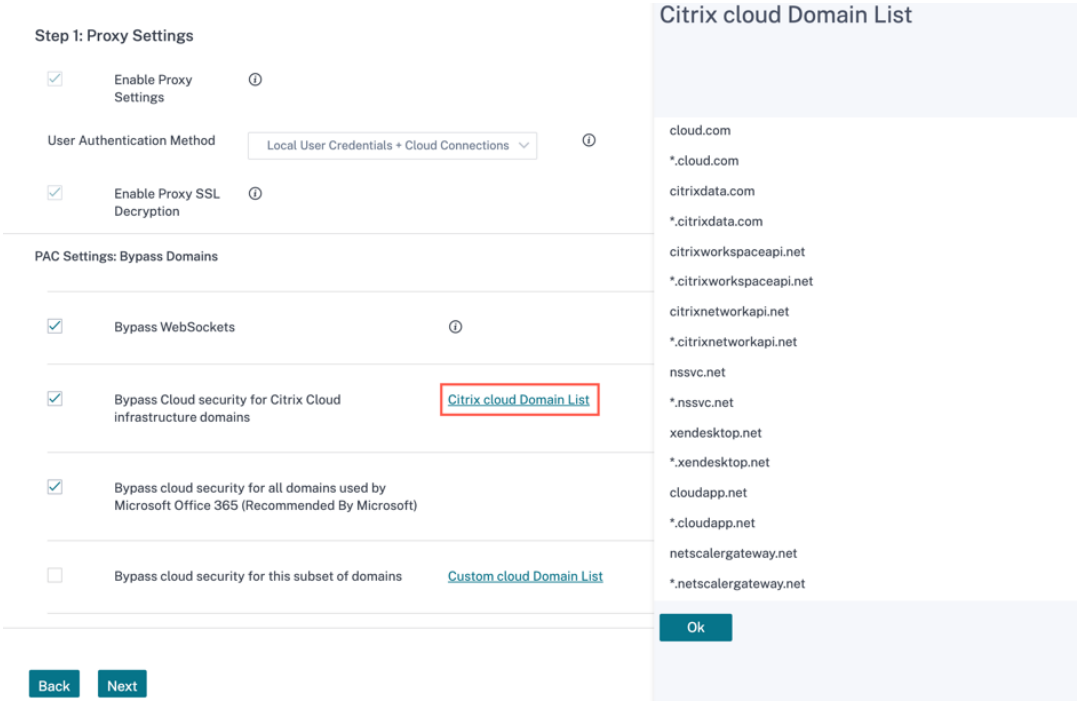
sécurisés de s'enregistrer automatiquement auprès de la passerelle en injectant une authentification proxy dans les demandes.

- **Informations d'identification de l'utilisateur local** : connectez-vous avec un compte d'accès Internet sécurisé local.
- **Cloud Connector uniquement** : utilise le mode agent qui permet aux agents/points de terminaison d'accès Internet sécurisés de s'enregistrer automatiquement auprès de la passerelle en injectant une authentification proxy dans les demandes.
- **SMAL basé sur un navigateur** : Authentification dans le navigateur et idéal pour les utilisateurs de succursales qui proviendraient de la même adresse IP publique.

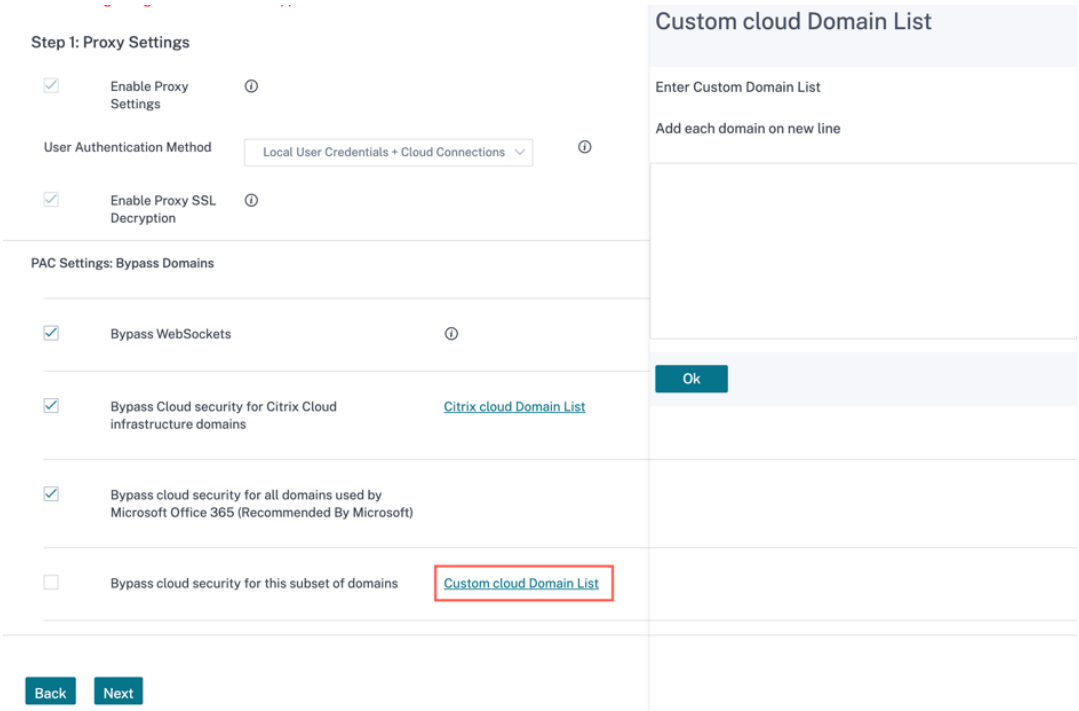
Les paramètres**Activer les paramètres** de **proxy et Activer le déchiffrement SSL** du proxy sont activés par défaut et les cases à cocher ne sont pas modifiables.

Dans les paramètres de configuration automatique du proxy, sous la section **Paramètres PAC : Bypass Domains**, cochez la case suivante selon vos besoins :

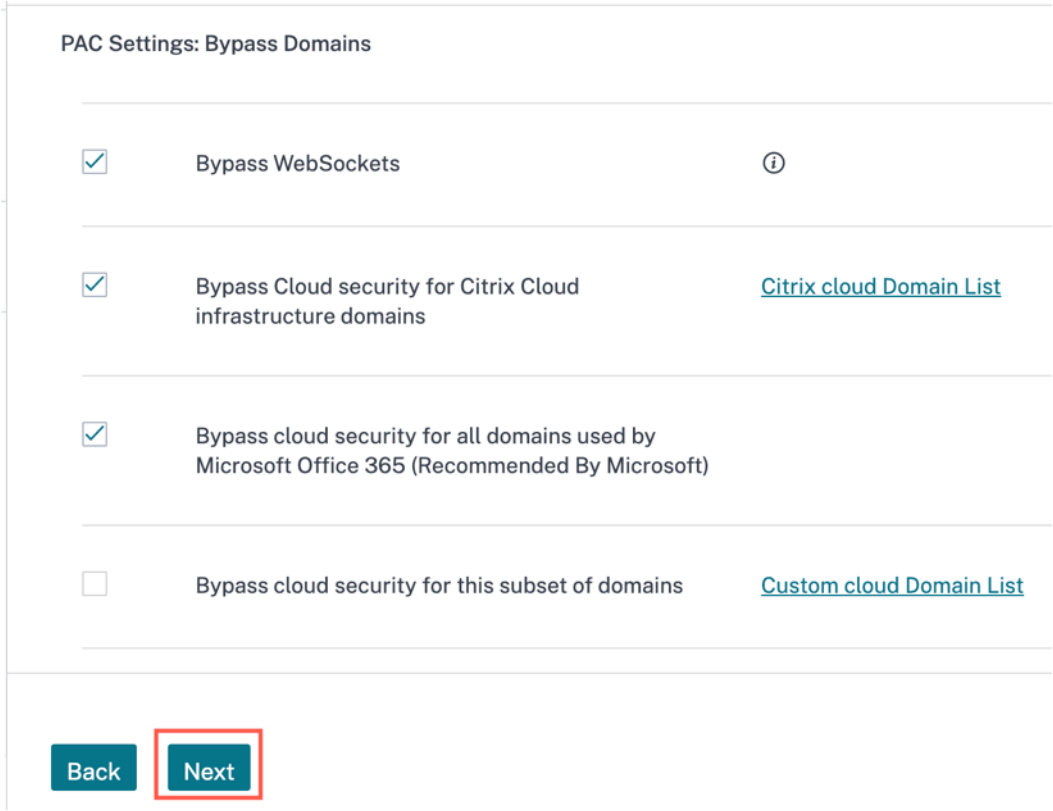
- **Bypass WebSockets** : contournez les domaines pour le trafic WebSockets et le trafic WebSockets sur Secure Sockets Layer (SSL) /Transport Layer Security (TLS). La case à cocher **Ignorer les WebSockets** est activée par défaut.
- **Bypass Cloud Security pour les domaines d'infrastructure Citrix Cloud** : Ignorez les demandes de sites Citrix. Ce paramètre est activé par défaut. La **liste des domaines Citrix Cloud** est une liste non modifiable des domaines d'infrastructure Citrix Cloud qui doivent être ignorés lors de toute inspection.



- **Contourner la sécurité du cloud pour tous les domaines utilisés par Microsoft Office 365 (recommandé par Microsoft)** : Ignorez les domaines utilisés pour Microsoft Office 365. La case à cocher **Contourner la sécurité du cloud pour tous les domaines utilisés par Microsoft Office 365 (recommandé par Microsoft)** est activée par défaut.
- **Ignorer la sécurité du cloud pour ce sous-ensemble de domaines** : Ignorez tous les domaines personnalisés. Vous pouvez créer vos propres domaines à l'aide de l'option **Liste de domaines cloud personnalisée** .

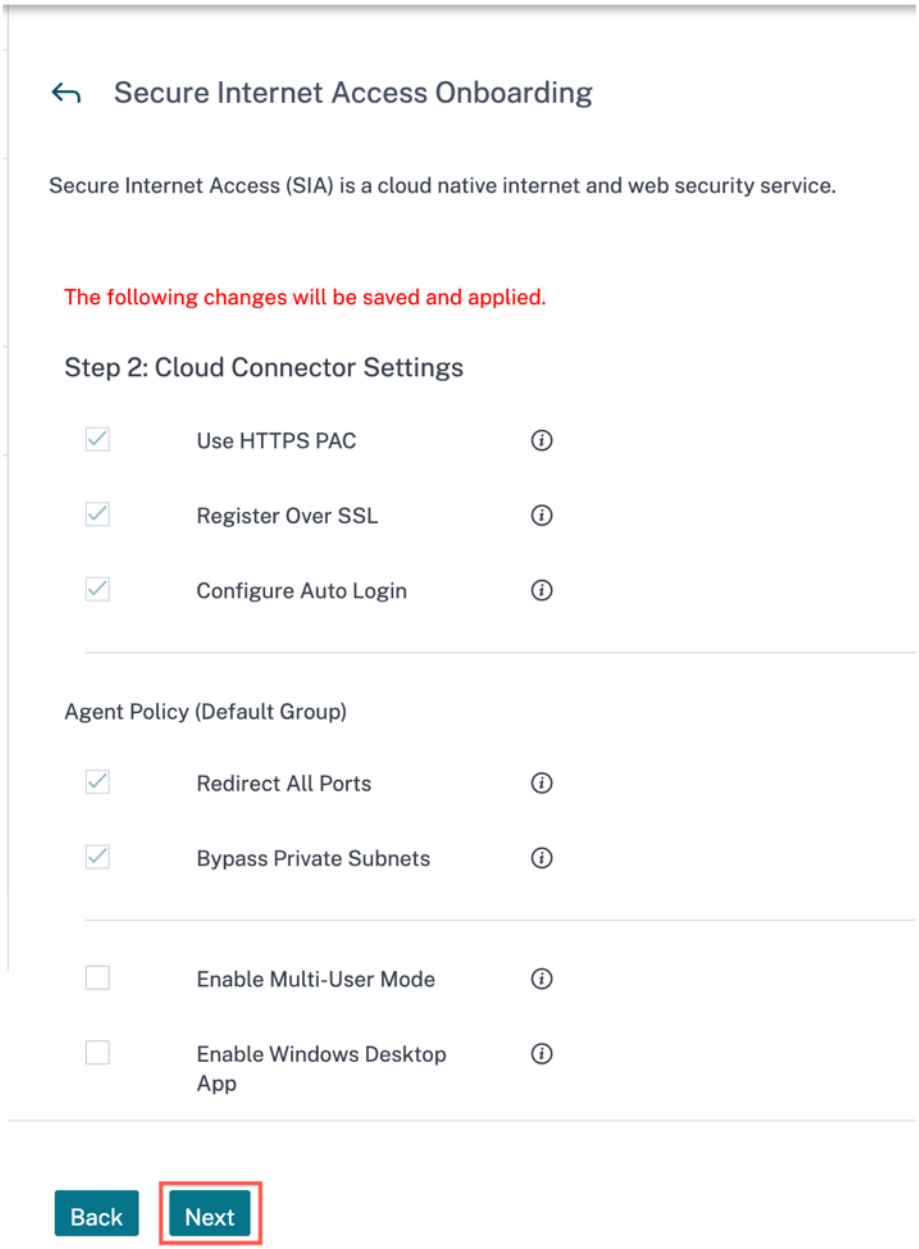


Cliquez sur **Suivant**.



2. Configurer les paramètres Cloud Connector

   Le Cloud Connector est un agent téléchargeable disponible pour divers systèmes d'exploitation tels que Windows, Linux, macOS, etc. Ces paramètres configureront le comportement du Cloud Connector installé sur vos appareils.



Les paramètres Utiliser le **PAC HTTPS, Enregistrer sur SSL, Configurer la connexion automatique, Rediriger tous les ports** et **Ignorer les sous-réseaux privés** sont activés par défaut et ne peuvent pas être modifiés.

- **Activer le mode multi-utilisateurs** : Cochez/décochez la case **Activer le mode multi-utilisateurs** si nécessaire. Vous pouvez sélectionner Activer le**mode multi-utilisateurs** pour prendre en charge plusieurs sessions utilisateur lors de l'exécution d'un bureau virtuel ou d'un serveur Terminal Server.
- **Activer l'application de bureau Windows** : Cochez/décochez la case **Activer l'application de bureau Windows si** nécessaire. L'**option Activer l'application de bureau Win-**

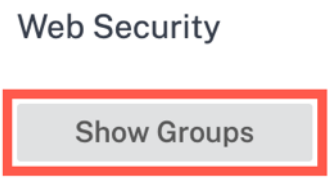
dows installe une application de bureau interactive sur les appareils Windows.

Cliquez sur **Suivant**.

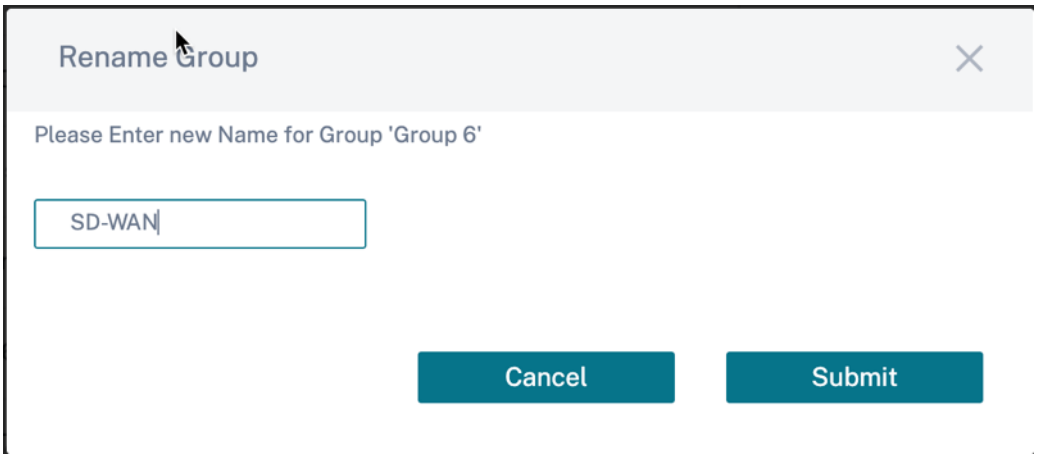
3. Configurer les paramètres de sécurité

   Dans la page Paramètres de sécurité, configurez les paramètres Sécurité Web, Agent de sécurité d'accès au cloud, Protection contre les logiciels malveillants et Prévention des intrusions (disponibles dans les SKU avancés et Premium) et Prévention contre la perte de données (disponible dans les SKU Premium).

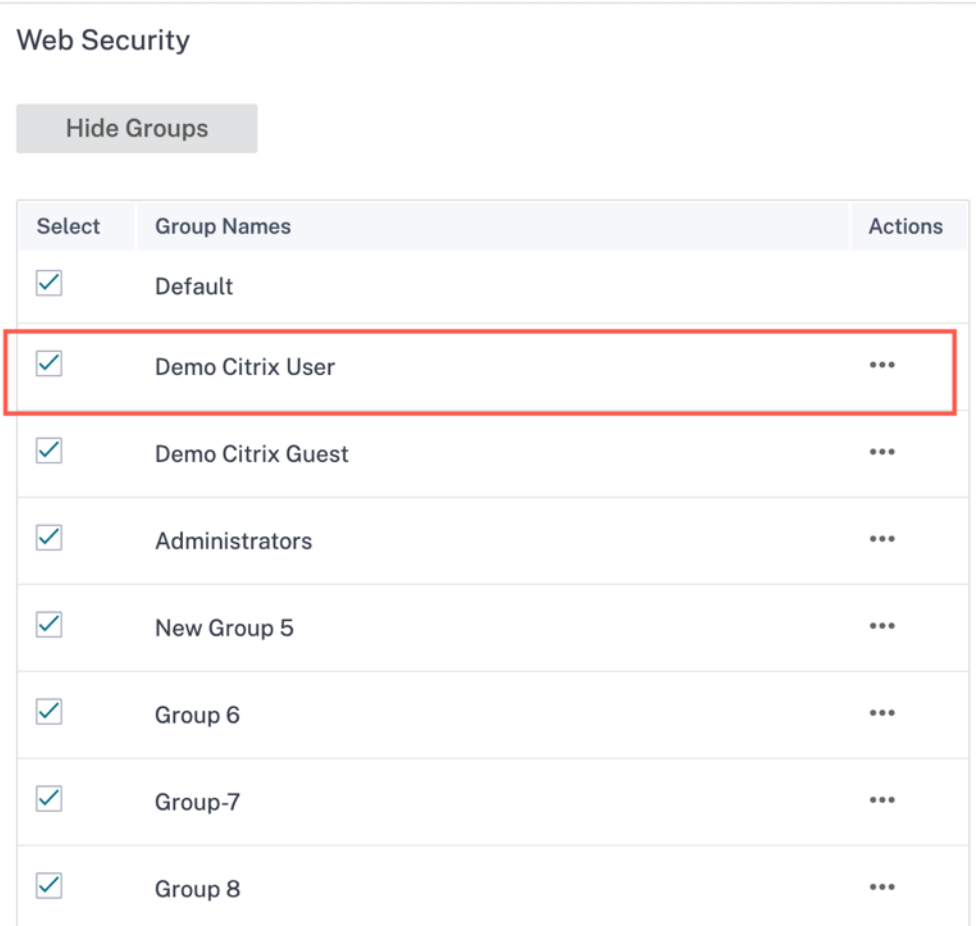
   - **Sécurité Web**
     - **Afficher les groupes** : affichez la liste des 20 premiers groupes.



Vous pouvez modifier les noms du groupe, par exemple département/domaine/produit, etc. Cliquez sur l'option de modification en regard du nom du groupe, saisissez le nom du groupe, puis cliquez sur **Soumettre**.



Lors de la sélection d'un groupe, la stratégie de groupe prédéfinie est appliquée à l'utilisateur. Le groupe **Par défaut** est un groupe non modifiable.

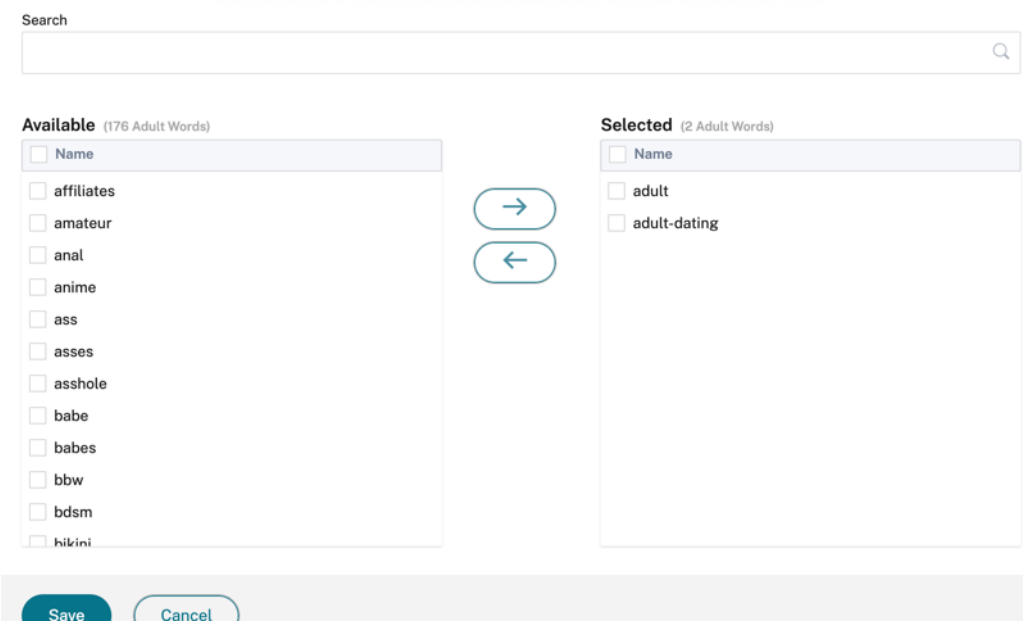


Tous ces 20 groupes sont cochés par défaut. Vous pouvez cocher/décocher les groupes selon vos besoins. Les modifications que vous apportez aux paramètres de sécurité sont appliquées au groupe sélectionné.

- **Bloquer les mots-clés par défaut** : cochez les cases **Adulte** et **Risque élevé** pour bloquer les mots-clés définis. L'option **Modifier** vous permet de configurer l'ensemble de mots-clés que vous souhaitez bloquer.

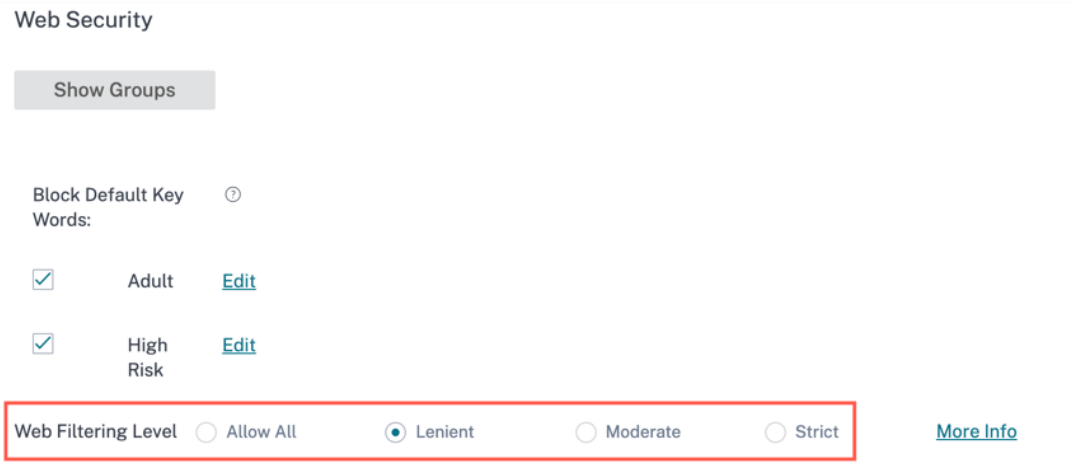
  Cliquez sur **Modifier** Sélectionner des **mots adultes/Sélectionner des mots à haut risque** sélectionnez les mots clés disponibles et déplacez-les dans la section sélectionnée, puis cliquez sur **Enregistrer**.

  La barre de recherche permet de trouver rapidement le mot-clé que vous recherchez.



- **Niveau de filtrage Web** : sélectionnez le **niveau de filtrage Web** pour **autoriser tout, profil indulgent, modéré** ou **strict** . Ces niveaux de filtrage sont définis en fonction de certaines catégories prédéfinies, comme décrit dans le tableau ci-dessous :

Catégorie	Tolérant	Modéré	Strict
Adulte	Bloqué	Bloqué	Bloqué
Informatique et Internet	Certains bloqués	Certains bloqués	Bloqué
Jeux d'argent	Bloqué	Bloqué	Bloqué
Contenus illégaux et préjudiciables	Bloqué	Bloqué	Bloqué
Malwares et Spam	Bloqué	Bloqué	Bloqué
Finance, Commerce et industrie	Autorisé	Bloqué	Bloqué
Courriel, messagerie, chat, téléphonie	Autorisé	Bloqué	Bloqué
Nouvelles, divertissement et société	Autorisé	Certains bloqués	Bloqué
Réseaux sociaux	Autorisé	Bloqué	Bloqué

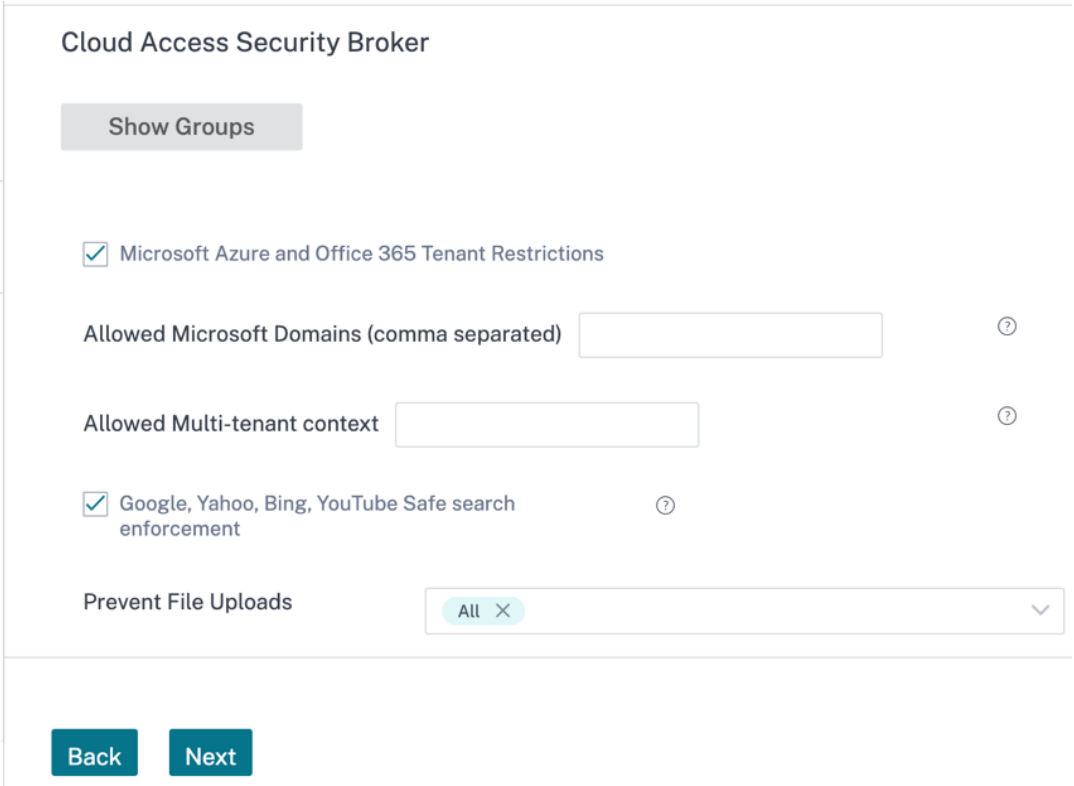


Cliquez sur le lien **Plus d'informations** pour afficher les informations relatives au niveau de filtrage Web.

- **Agent de sécurité d'accès au cloud** : permet de bloquer les téléchargements de fichiers vers divers services, d'appliquer une recherche sécurisée via divers moteurs de recherche tels que Google/Yahoo/Bing, etc.

  Si la case à cocher **Restriction des locataires Microsoft Azure et Office 365** est activée, spécifiez les noms de domaine autorisés et le contexte mutualisé pour appliquer les paramètres de sécurité.

  Sélectionnez l'emplacement (Tous/Dropbox/Box/OneDrive/Google Drive/Chargements de fichiers génériques Aucun) dans la liste déroulante **Empêcher les téléchargements de fichiers** pour empêcher le téléchargement des fichiers. Par défaut, **Tout** est sélectionné.



Dans Citrix Secure Internet Access, trois SKU différents sont disponibles : Standard, Advanced et Premium.

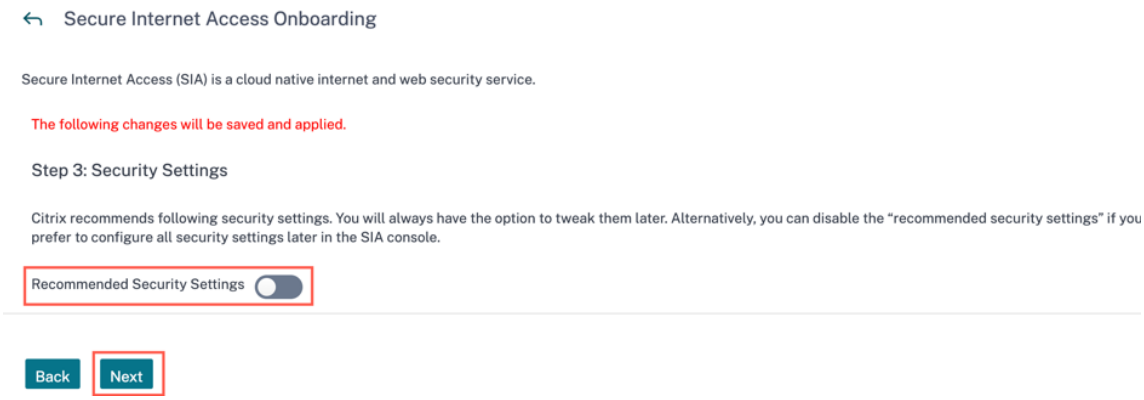
Dans l'interface graphique de Citrix Secure Internet Access :

- L'option **Paramètres de protection contre les logiciels malveillants et de prévention des intrusions** est uniquement disponible pour les clients disposant de SKU Advanced et Premium.
- L'option **de prévention contre la perte de données (DLP)** n'est disponible que pour les clients disposant de SKU Premium.

Pour le plan Standard, les **paramètres de défense contre les programmes malveillants et de prévention des intrusions et les** options de **prévention contre la perte de données (DLP)** ne sont pas disponibles dans l'interface utilisateur Citrix Secure Internet Access

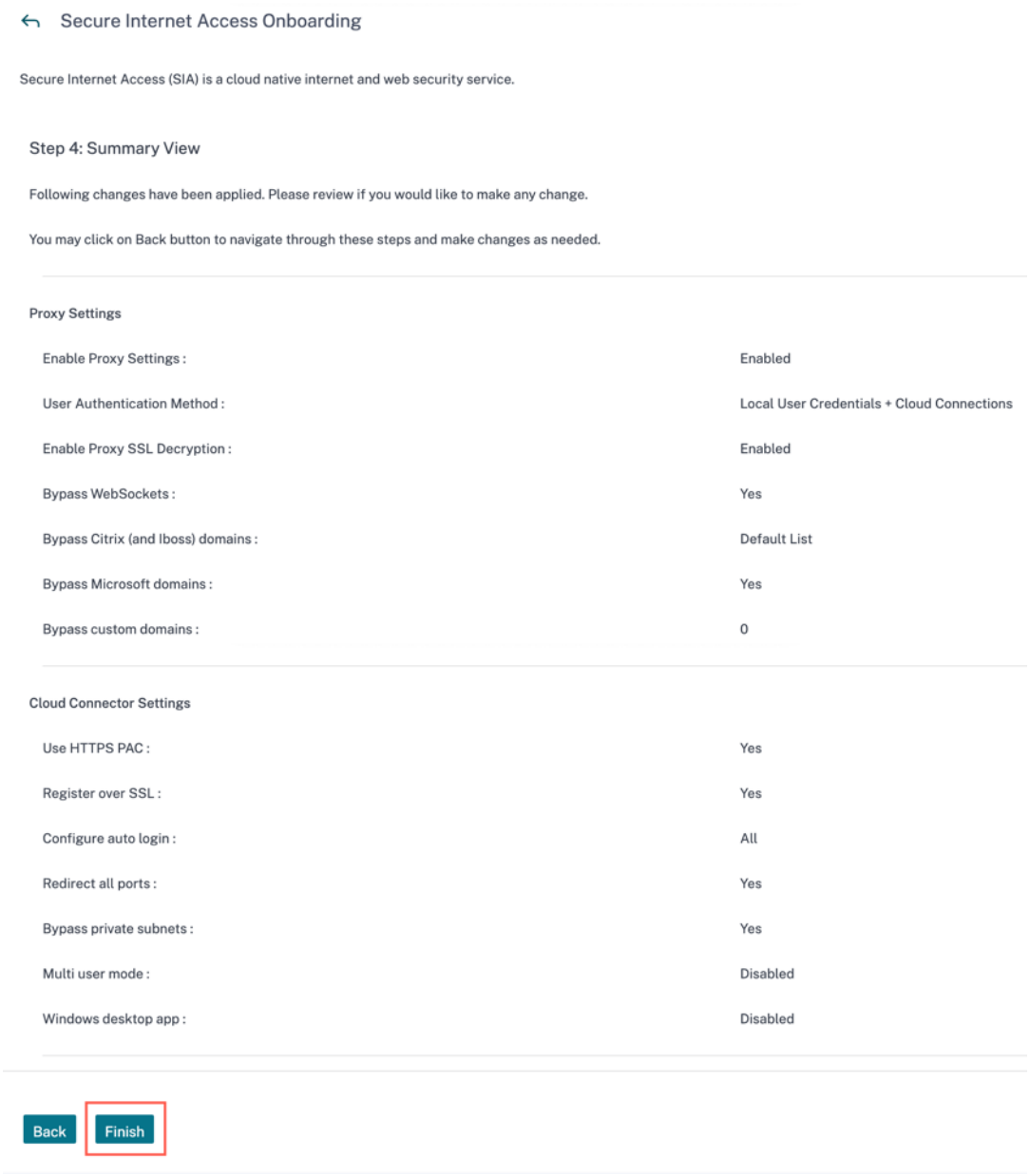
Par défaut, toutes les options sont pré-cochées pour les **paramètres de défense contre les logiciels malveillants et de prévention des intrusions** et **la prévention contre la perte de données (DLP)**. Vous pouvez réinitialiser les paramètres ou sélectionner les options selon vos besoins. Cliquez sur **Suivant**.

Si vous souhaitez ignorer la configuration des **paramètres de sécurité**, vous pouvez également désactiver le bouton **Paramètres de sécurité recommandés** . Vous pouvez configurer les paramètres ultérieurement dans la console CSIA.

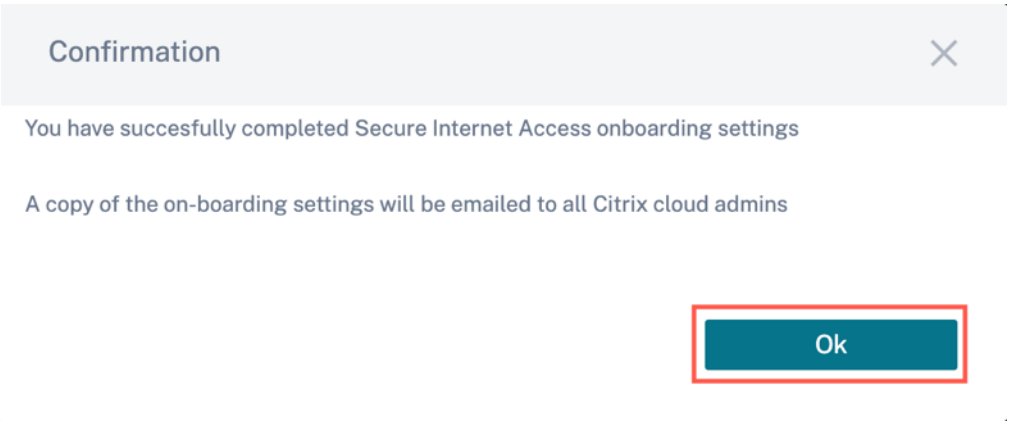


Dans ce scénario, cliquez sur **Suivant** et vérifiez les paramètres que vous avez définis, puis cliquez sur **Terminer** pour enregistrer les modifications.

4. Vous pouvez afficher la page récapitulative avec tous les paramètres que vous avez définis pour terminer le processus d'intégration.



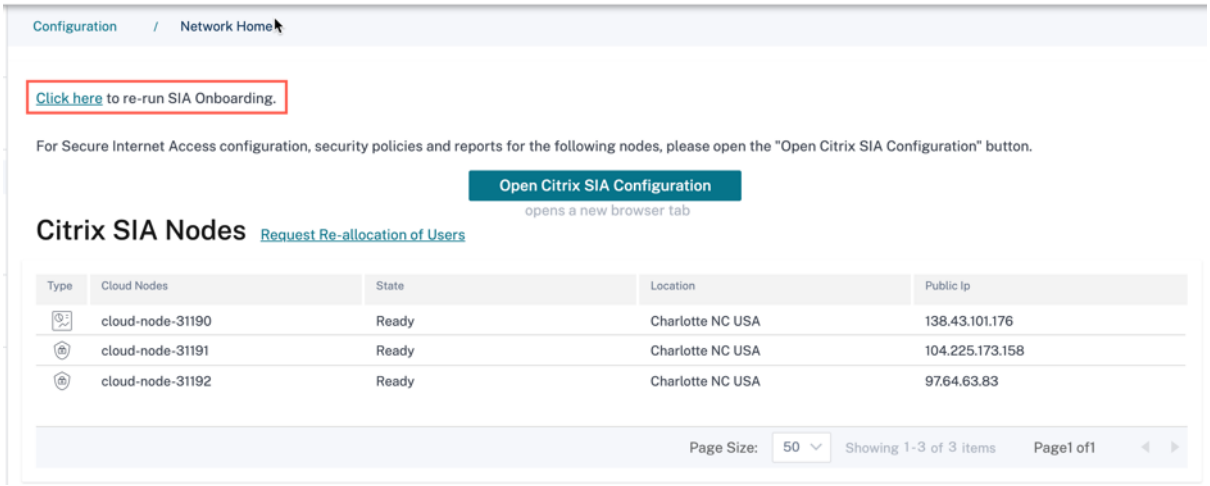
Cliquez sur **Terminer**, une fenêtre contextuelle s'affiche pour confirmer que vous avez correctement défini les paramètres d'intégration. Cliquez sur **OK**.



En outre, un e-mail est envoyé à tous les administrateurs Citrix Cloud qui ont été ajoutés à ce compte client pour le service Citrix Internet Secure Access.

Une fois l'intégration terminée, accédez à **Configuration > Accueil de la configuration réseau > Ouvrir la configuration Citrix SIA** sélectionnez **Connecter l'appareil au cloud**. Sur cette page, vous pouvez suivre les instructions pour télécharger/installer Cloud Connector correspondant au système d'exploitation du terminal.

Vous pouvez réexécuter le processus d'intégration à partir de **la page Configuration > Accueil de la configuration réseau** . Si vous avez oublié des paramètres, vous pouvez toujours revenir en arrière et relancer le processus d'intégration pour rétablir les paramètres par défaut/recommandés.



Quelle est la prochaine étape ?

- Affichez l'état des nœuds de votre réseau. Voir Tableau de bord.
- Consultez les détails concernant les droits de licence auxquels vous avez souscrit. Consultez Afficher les détails de la licence.
- Configurez les agents CSIA Cloud Connector sur les Virtual Delivery Agents (VDA) et les systèmes

hôtes locaux. Reportez-vous à la section Configurer les agents Citrix Secure Internet Access Cloud Connector.
- Configurez des tunnels pour votre succursale si vous disposez également d'un déploiement Citrix SD-WAN. Consultez la section Configurer les tunnels pour les succursales.
- Utilisez le portail de stratégie de configuration Citrix Secure Internet Access pour configurer les connecteurs cloud et les fonctionnalités de sécurité, ainsi que pour surveiller les rapports et les journaux. Consultez la section Configuration.

Gestion des licences

January 26, 2022

Citrix Secure Internet Access (CSIA) est disponible en trois éditions.

- **Standard** : solution de sécurité basée sur le cloud qui fournit une gestion et une administration centralisées dans le cloud. Il comprend des fonctionnalités de sécurité essentielles telles que le filtrage du contenu Web et Internet, la gestion du trafic SSL et le CASB.
- **Avancé** : solution de sécurité complète avec des offres de sécurité supplémentaires telles que la prévention des logiciels malveillants et la détection des violations, la détection des rappels de commande et de contrôle et la réponse aux incidents.
- **Premium** : solution de sécurité complète qui inclut la détection avancée des contenus sensibles et un moteur d'analyse de contenu avancé.

Pour obtenir la liste complète des fonctionnalités disponibles dans une édition, consultez le tableau des fonctionnalités à l'adresse https://www.citrix.com/.

Chacune de ces éditions inclut les éléments suivants :

- 500 Go d'espace de stockage
- Un tunnel IPSEC ou GRE pour 10 utilisateurs d'un compte

Vous pouvez acheter plus d'espace de stockage ou de tunnels.

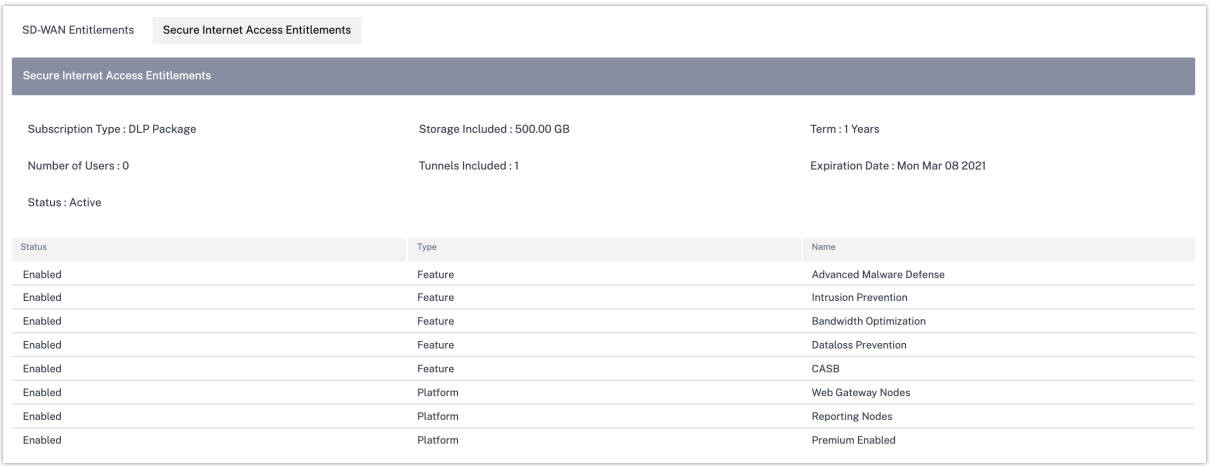
Une fois votre processus d'intégration terminé, vous pouvez obtenir des informations sur la licence que vous avez souscrite et les détails d'utilisation.

Afficher les détails des licences

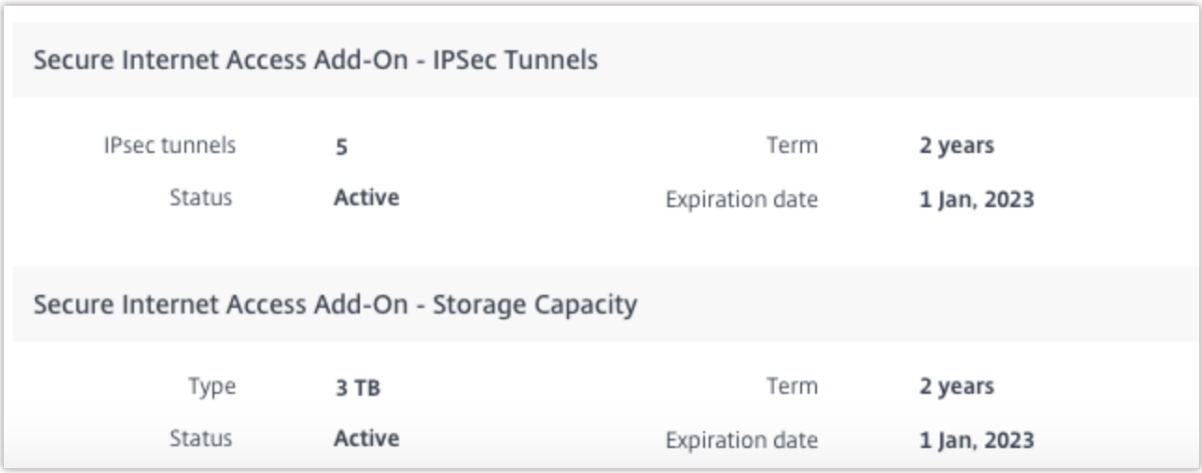
Consultez les détails concernant les droits de licence auxquels vous avez souscrit en accédant à **Administration** > **Licence**.

Vous pouvez afficher les informations suivantes dans l'onglet **Droits d'accès Internet sécurisé** :

- Type d'abonnement et liste des fonctionnalités activées pour votre abonnement.
- Capacité de stockage incluse dans votre forfait d'abonnement. Par défaut, chaque abonnement inclut 500 Go d'espace de stockage.
- Nombre de tunnels inclus dans votre forfait d'abonnement. Par défaut, chaque abonnement inclut un tunnel pour 10 utilisateurs d'un compte.
- Durée de la licence et date d'expiration
- Nombre d'utilisateurs ajoutés à cet abonnement
- État de votre droit



Vous pouvez également afficher des informations sur l'espace de stockage ou les tunnels supplémentaires que vous avez achetés.



> **Remarque**
>
> Si vous disposez également d'un droit Citrix SD-WAN, vous pouvez afficher les détails de la licence SD-WAN dans l'onglet SD-WAN. Pour plus d'informations sur les licences SD-WAN, consultez la section Gestion des licencesSD-WAN Orchestrator.

Insights sur l'utilisation

Vous pouvez obtenir des informations sur l'utilisation des licences en accédant à **Administration** > Informations sur l'**utilisation des licences**.

Affichez le nombre total de licences utilisateur dont vous disposez et le nombre de licences utilisateur actives. Vous pouvez également afficher le nombre de licences totales et actives pour le stockage de données et les tunnels.

Ces informations vous aident à déterminer si vous avez besoin de davantage de licences utilisateur, de capacité de stockage ou de tunnels.

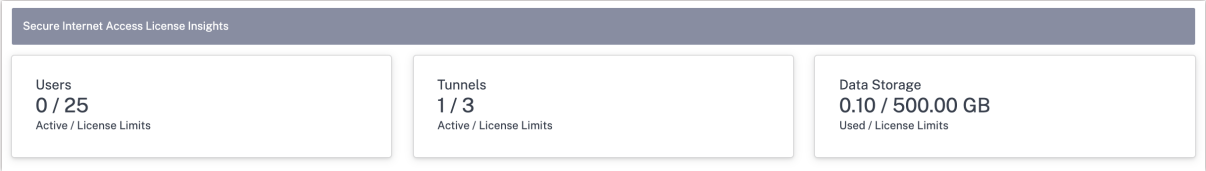
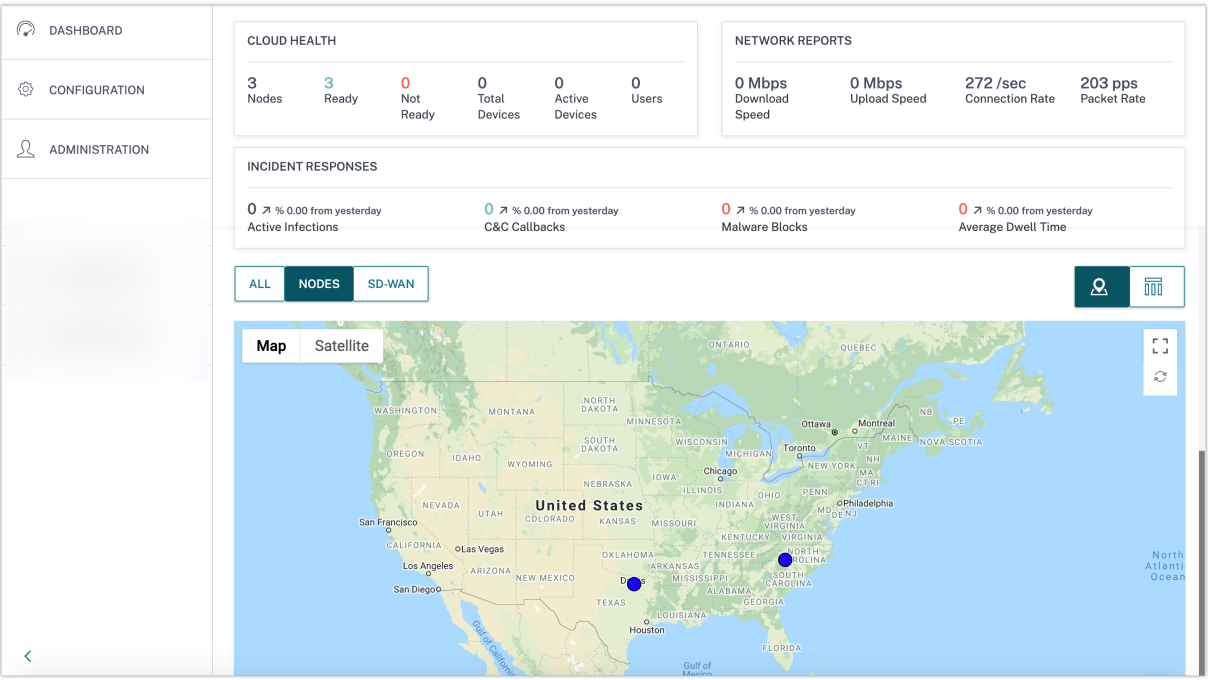


Tableau de bord

January 26, 2022

Le tableau de bord, comme illustré dans l'image suivante, fournit une vue de haut niveau des performances de votre réseau Citrix Secure Internet Access (CSIA).



Le **tableau de bord** comprend quatre sections principales : l'**état du cloud**, **les rapports réseau**, **les réponses aux incidents**et une **vue cartographique** du réseau.

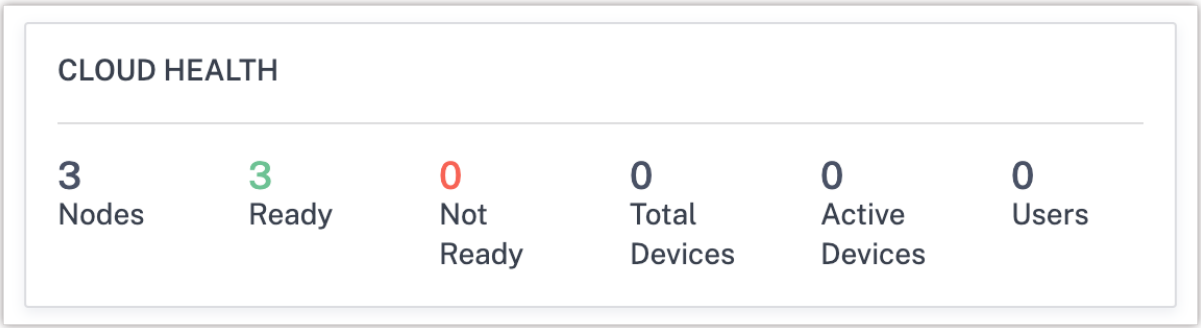
Vous pouvez accéder à des rapports plus détaillés sur la page **Rapports et analyses** . Pour ce faire, accédez à **Configuration** > **Ouvrir la configuration Citrix SIA**.

Santé du cloud

Cette section indique l'état des nœuds de votre réseau. Affichez le nombre total de nœuds qui ont été configurés pour vous. Vérifiez également combien de ces nœuds sont prêts et combien ne le sont pas.

Un nœud qui **n'est pas prêt** ne fonctionne pas ou n'est pas provisionné, ce qui indique un problème que vous devez étudier ou signaler pour pouvoir être résolu.

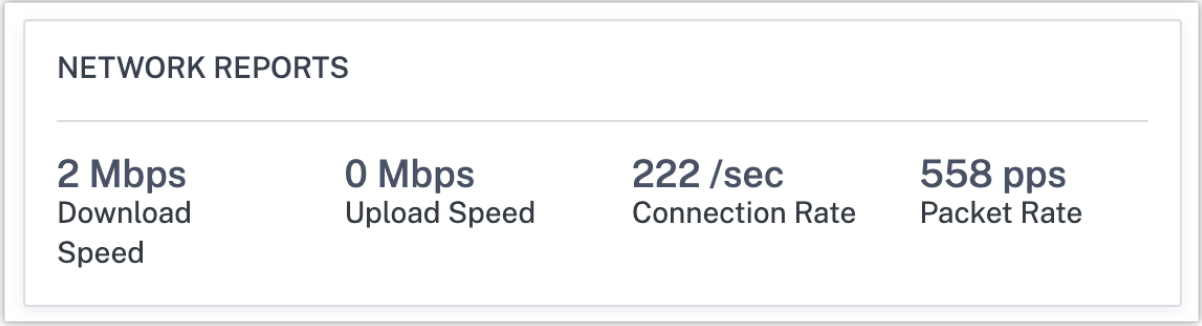
La section sur l'**état du cloud** fournit également des informations sur le nombre total d'appareils connectés aux nœuds et le nombre d'appareils actifs. Il vous permet également de suivre le nombre d'utilisateurs connectés au réseau.



Rapports réseau

Cette section fournit un aperçu de l'activité en temps réel sur votre réseau. Il répertorie l'utilisation de la bande passante, telle que la vitesse de téléchargement et la vitesse de téléchargement pour tous les appareils connectés. Cette section fournit également des informations sur le taux de connexions et de paquets utilisés sur le réseau.

Ensemble, ces informations peuvent vous indiquer s'il existe un problème de réseau qui doit être traité.



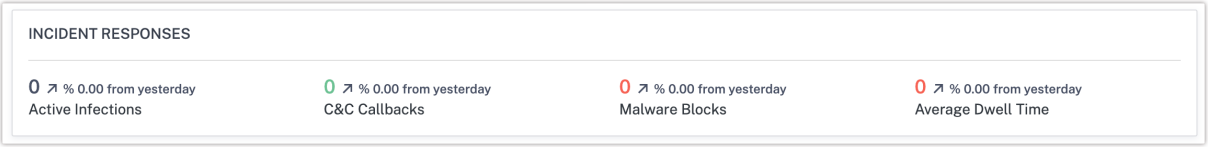
Réponses aux incidents

Cette section fournit une vue de haut niveau des appareils infectés de votre réseau et que vous devez examiner ou signaler.

Cette section répertorie les données de sécurité suivantes :

- le nombre d'infections actuellement actives sur le réseau
- le nombre de rappels de commande et de contrôle (C&C)
- le nombre total de logiciels malveillants dont l'entrée sur le réseau a été bloquée
- le temps de séjour moyen des infections sur l'ensemble du réseau.

Cette section montre également le pourcentage d'augmentation de chacun de ces incidents depuis la veille.



Notifications

Les mises à jour importantes relatives à votre abonnement au service Citrix Secure Internet Access vous sont envoyées sous forme de notifications dans le tableau de bord. Les notifications incluent, mais ne sont pas limitées à :

- Informations sur l'expiration de la licence
- Notes de publication des nouvelles versions
- Demandes de révision d'URL
- Alertes et avis

Citrix vous informe que vous avez reçu des notifications avec un numéro sur l'icône en forme de cloche. Vous pouvez trouver l'icône en forme de cloche en haut à droite du tableau de bord. Vous

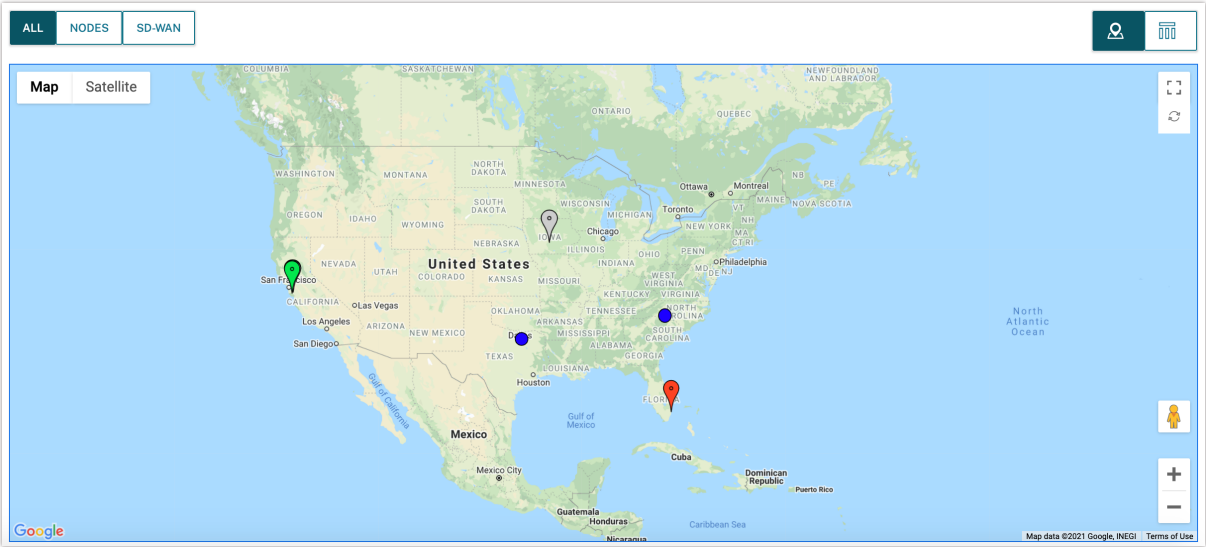
pouvez développer la vue des notifications en sélectionnant l'icône en forme de cloche. Ces notifications s'affichent uniquement dans l'icône en forme de cloche et ne sont pas envoyées par e-mail.

Vue cartographique

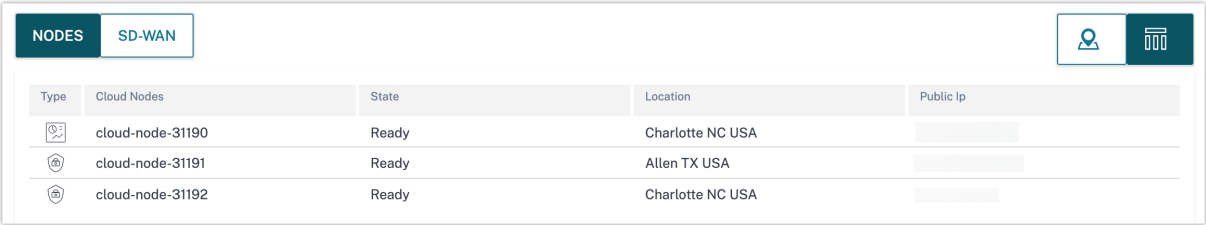
La vue cartographique montre les emplacements géographiques des nœuds de cloud et de passerelle de votre déploiement Citrix Secure Internet Access. Les points bleus représentent les nœuds de la carte.

Si vous disposez d'un droit SD-WAN, vous pouvez voir les emplacements géographiques de vos sites SD-WAN. Les sites sont indiqués en vert, en rouge ou en gris sur la carte.

Vous pouvez limiter cette vue aux nœuds Citrix Secure Internet Access en sélectionnant l'onglet **Noeuds** ou aux sites SD-WAN en sélectionnant l'onglet **SD-WAN** .



Pour afficher ces informations sous forme de tableau, sélectionnez l'icône de la vue tabulaire située à l'extrême droite, juste au-dessus de la carte. Pour revenir à la vue cartographique, sélectionnez l'icône de la vue cartographique située à gauche de l'icône de la vue tabulaire.



Configuration

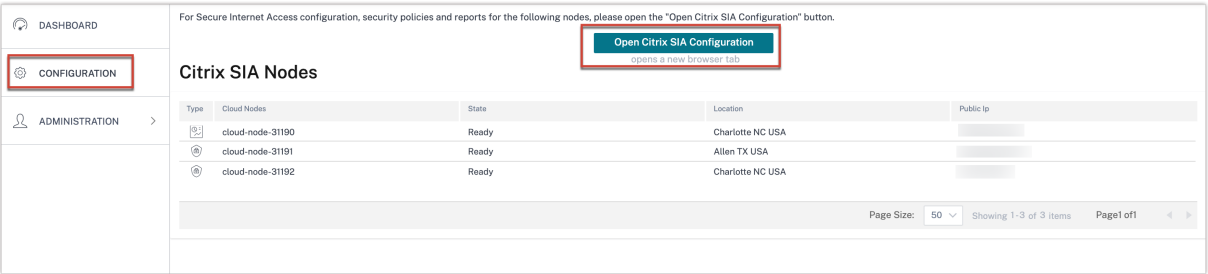
January 26, 2022

Utilisez le portail de stratégie de configuration Citrix Secure Internet Access (CSIA) pour configurer les connecteurs cloud et les stratégies de sécurité, ainsi que pour surveiller les rapports et les journaux.

Pour accéder au portail des stratégies de configuration :

1. Connexion à Citrix Cloud
2. Sur la vignette **Accès Internet sécurisé**, sélectionnez **Gérer**
3. Dans le volet de navigation, sélectionnez **Configuration**

   La page Configuration répertorie également les détails concernant les nœuds de cloud qui ont été configurés pour vous. Toutes les configurations que vous effectuez sont connectées à ces nœuds.
4. Sélectionnez **Ouvrir la configuration Citrix SIA** pour afficher le portail de stratégie de configuration et commencer à configurer les fonctionnalités et les stratégies de sécurité.



Comment obtenir de l'aide sur la configuration

Pour obtenir des instructions sur la configuration ou obtenir de l'aide sur n'importe quelle page de configuration, vous pouvez effectuer l'une des opérations suivantes :

- **Accédez à la documentation d'aide**. Dans le coin supérieur droit du portail de stratégie de configuration, cliquez sur le menu (où votre nom apparaît) et sélectionnez **HelpDocs**. Vous pouvez consulter la documentation d'aide complète.

  > **Remarque**
  >
  > La documentation d'aide inclut des références à la terminologie iboss, aux éléments de l'interface utilisateur iboss, aux fonctionnalités iboss non prises en charge par Citrix et aux informations de support iboss.
  >
  > Consultez l'article suivant avant d'utiliser la documentation d'aide : Citrix Secure Internet

> Access et intégration iboss. Vous pouvez accéder à cet article uniquement après vous être connecté à Citrix Secure Internet Access.

- **Accédez à l'aide contextuelle**. Dans le coin supérieur droit de chaque page de configuration, sélectionnez l'**icône d'aide (?)** pour afficher la documentation d'aide relative à cette page.
- **Contactez l'assistance Citrix**. Connectez-vous avec votre compte Citrix et ouvrez un dossier de support, démarrez un chat en direct ou explorez les autres options disponibles pour recevoir de l'aide.

Configurer les agents Citrix Secure Internet Access Cloud Connector

Les agents CSIA Cloud Connector sont des agents logiciels qui redirigent le trafic Internet via Citrix Secure Internet Access.

Une fois votre processus d'intégration terminé, procédez comme suit :

- **Installer l'agent CSIA Cloud Connector sur Virtual Delivery Agent (VDA)** : pour accéder en toute sécurité aux applications Web et SaaS non autorisées à partir de bureaux virtuels sur Citrix Workspace, configurez les agents CSIA Cloud Connector pour rediriger le trafic via Citrix Secure Internet Access.

  Pour connaître les étapes de configuration détaillées, consultez Citrix Secure Internet Access avec Citrix Virtual Apps and Desktops.

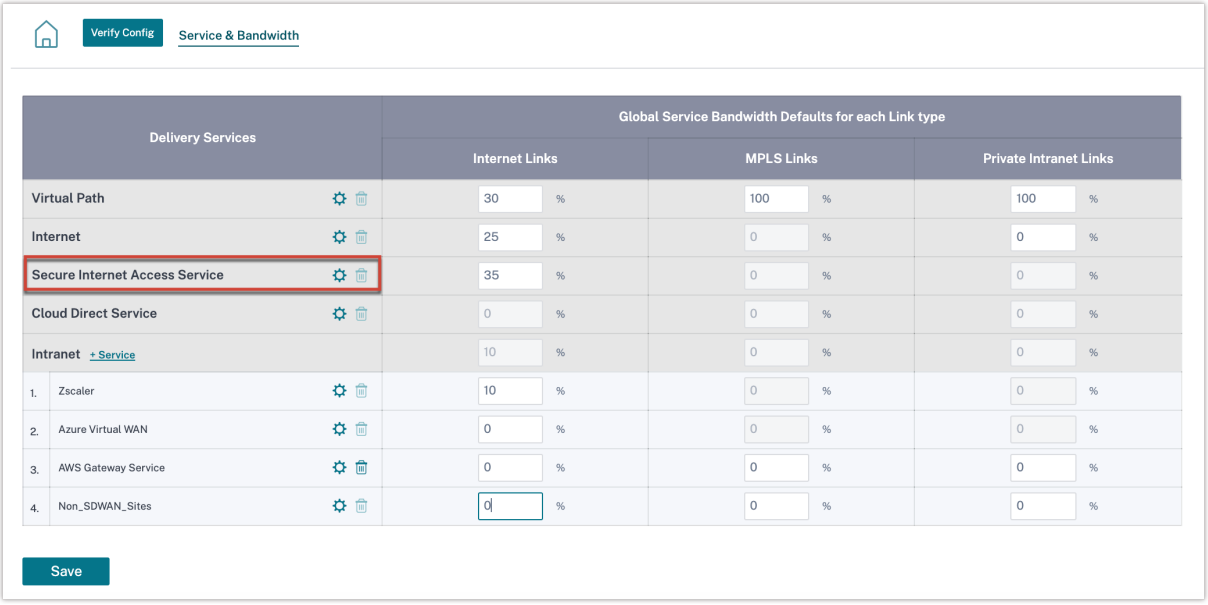
- **Installez l'agent Cloud Connector CSIA sur votre appareil hôte** : pour accéder en toute sécurité au trafic Internet direct de vos systèmes hôtes tels que les ordinateurs portables et les appareils mobiles, installez des agents Cloud Connector sur chaque appareil.

Configurer les tunnels pour les succursales

Si vous avez un déploiement Citrix SD-WAN dans votre succursale, vous devez configurer des tunnels IPSEC ou GRE. Cela redirige le trafic des succursales vers des applications Web et SaaS non autorisées via Citrix Secure Internet Access. Vous utilisez Citrix SD-WAN Orchestrator pour configurer les tunnels.

Sur Citrix SD-WAN Orchestrator, le service Citrix Secure Internet Access est disponible dans **Configuration** > **Services de livraison** > **Service et bande passante**.

> **Remarque**
>
> Le lien de service n'est visible que si vous êtes un client SD-WAN Orchestrator et que vous disposez des droits Citrix Secure Internet Access.



La configuration inclut les étapes de haut niveau suivantes :

1. Créez un service Citrix Secure Internet Access en spécifiant le pourcentage de bande passante et le pourcentage de provisionnement pour les liens Internet.
2. Ajoutez et mappez des sites SD-WAN au service Citrix Secure Internet Access et sélectionnez le tunnel approprié (IPSEC ou GRE). Activez ensuite la configuration pour activer l'établissement d'un tunnel entre Citrix SD-WAN et le PoP Citrix Secure Internet Access.
3. Créez des itinéraires d'application pour orienter le trafic dans les tunnels.

Pour obtenir des instructions détaillées, reportez-vous à la section Services de mise à disposition - Service Citrix Secure Internet Access.

Réaffectation des utilisateurs

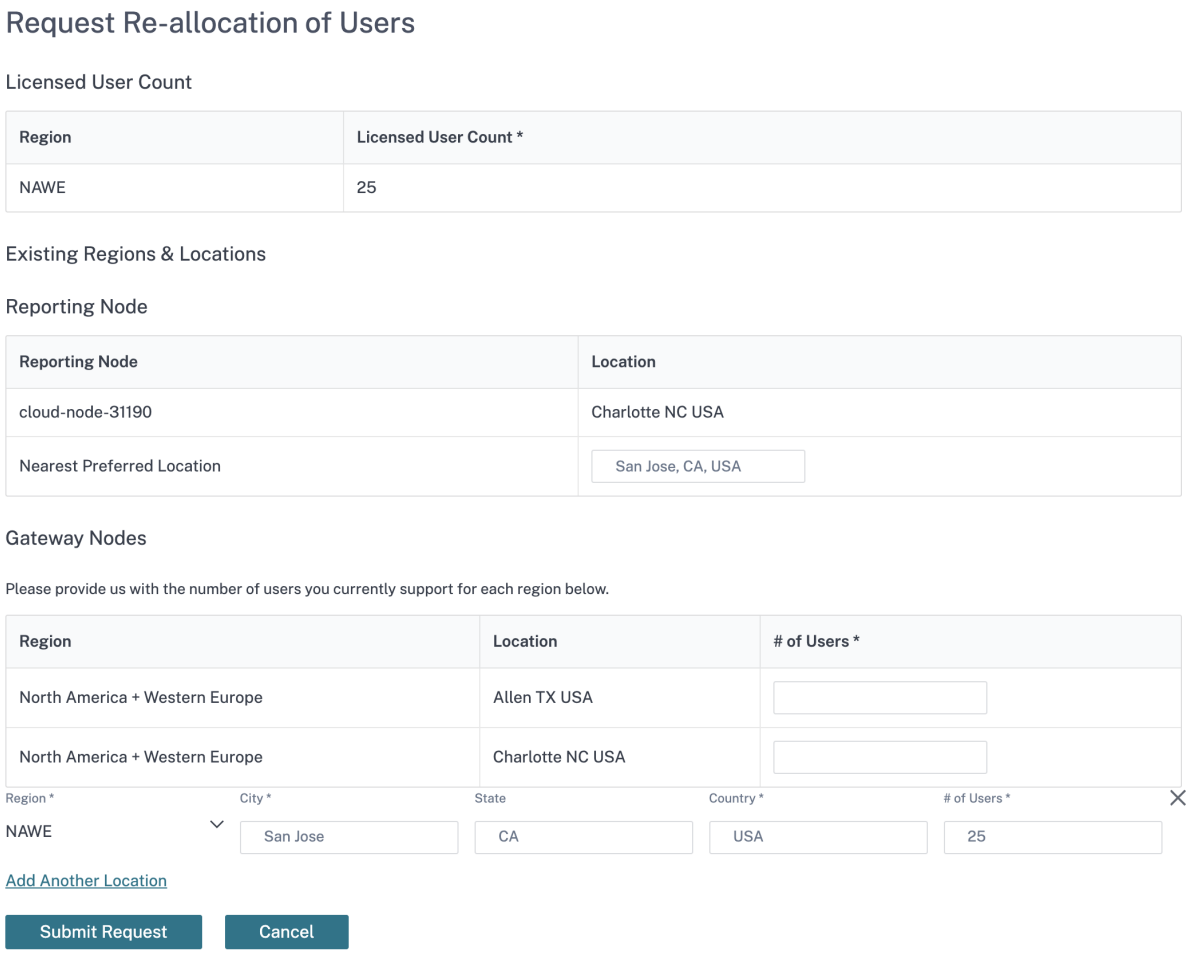
Vous pouvez réduire la latence pour les utilisateurs situés dans des emplacements particuliers en redistribuant les nœuds de cloud au sein d'une région géographique.

Vous pouvez faire une demande de redistribution à la fois des nœuds de rapport qui collectent des données d'utilisation et des nœuds de passerelle qui exécutent des fonctions de sécurité. Citrix vise à fournir les nœuds les plus proches des utilisateurs en fonction de la disponibilité des nœuds.

> **Important**
>
> La réallocation des nœuds entraîne une brève interruption du service. L'opération est généralement effectuée immédiatement après l'activation du compte, avant la configuration et la distribution des connecteurs clients. Citrix vous recommande de demander la réallocation des nœuds

> au début du déploiement afin de réaligner les nœuds les plus proches des utilisateurs et de réallouer les nœuds peu fréquemment.

Vous pouvez également déplacer des utilisateurs entre des nœuds ou les ajouter à un nœud s'ils ne sont pas déjà alloués à un nœud.



Pour afficher, redistribuer et gérer les nœuds, accédez à l'onglet **Configuration** dans le menu de gauche et sélectionnez **Demander la réallocation des utilisateurs** au-dessus du tableau.

> **Remarque**
>
> Vous ne pouvez redistribuer les nœuds que dans la même région géographique.

Paramètres du cloud

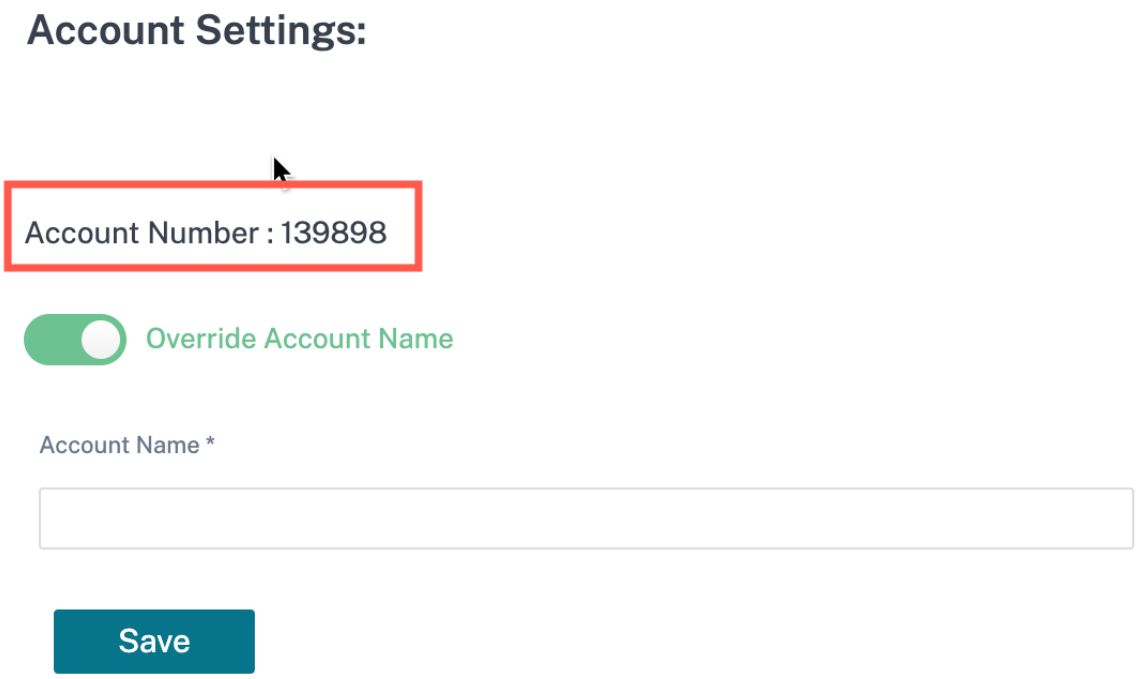
Pour configurer les paramètres de votre serveur NTP (Network Time Protocol), la maintenance de la plateforme et les versions de mise à jour, accédez à l'onglet **Configuration** et sélectionnez **Paramètres du cloud**.

Paramètres du compte

La fonctionnalité **Paramètres du compte** permet de modifier/remplacer le nom du compte d'utilisateur qui apparaît pour votre compte dans le portail de services Citrix Secure Internet Access.

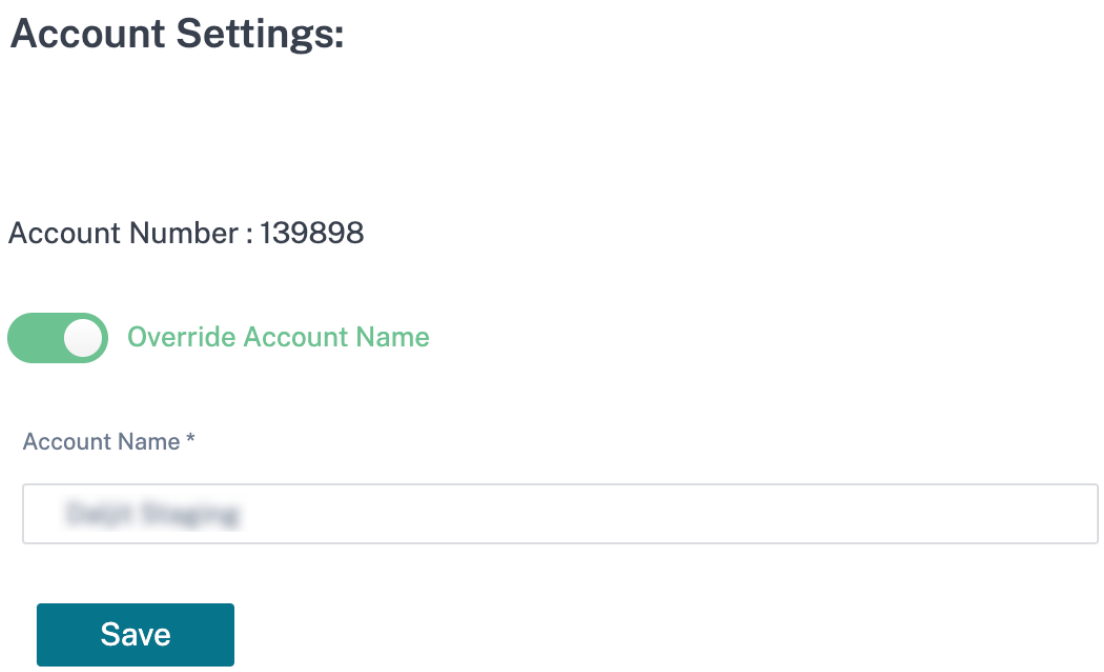
Pour remplacer le nom du compte, accédez à **Configuration > Paramètres du cloud > Paramètres du compte**.

Vous pouvez consulter le numéro de compte Citrix Secure Internet Access.



> **Remarque**
>
> Le nom de compte initialement configuré est toujours présent dans le portail CSIA si vous n'avez créé aucun nom ou si le **nom de compte de remplacement** est désactivé.

1. Activez l'**option Remplacer le nom du compte** et saisissez un nom. Par défaut, le **nom de compte de remplacement** est désactivé.



Attendez un certain temps pour afficher le nom de compte mis à jour sur le portail. Il se peut que vous deviez vous reconnecter une fois le nom du compte modifié.

2. Cliquez sur **Enregistrer**.

Serveur NTP

Pour synchroniser la date et l'heure, accédez au **serveur NTP** sous **Paramètres du cloud**. Entrez le fuseau horaire, le format de date, l'adresse du serveur NTP et les informations d'heure d'été.

Le **fuseau horaire** définit l'heure standard régionale utilisée pour les horodatages. Après avoir modifié le fuseau horaire, les horodatages des événements dans les rapports seront décalés pour s'aligner sur le nouveau fuseau horaire et maintenir la continuité. Les horodatages sont relatifs au nouveau fuseau horaire.

Le **format de date** définit la structure de la date sous forme numérique. Ce paramètre peut être réglé sur **jj/mm/aaaa ou**jj/mm/aaaa**.

Le **serveur NTP** définit l'adresse du serveur NTP.

L'heure d'été définit si le fuseau horaire est conforme à l'heure d'été. Ce paramètre peut être défini sur **États-Unis** ou **Royaume-Uni** selon la région du fuseau horaire.

Maintenance des plateformes

Cette fonctionnalité vous permet de planifier les jours et les heures de maintenance afin de vous assurer que votre réseau est disponible pendant les heures de pointe.

Pour planifier la maintenance automatique effectuée en votre nom, accédez à **Maintenance de la plateforme** sous **Paramètres du cloud**, puis activez **Fenêtre de maintenance préférée**. Sélectionnez ensuite vos dates et heures préférées pour la maintenance automatique.

Paramètres de mise à jour

Pour choisir les types de mises à jour qui sont installées en votre nom, accédez aux paramètres de **mise à jour des versions sous Paramètresdu cloud**, puis sélectionnez l'un des niveaux de version suivants :

- **Obligatoire**, pour les mises à jour critiques de la plate-forme et les correctifs de sécurité, y compris les nouvelles fonctionnalités, les mises à jour des fonctionnalités, les corrections de bugs
- **Facultatif**, pour les versions recommandées mais qui n'incluent pas de correctifs critiques.
- **Accès anticipé**, pour un accès anticipé aux nouvelles fonctionnalités, aux mises à jour, aux corrections de bogues et aux améliorations des performances.

Paramètres de messagerie

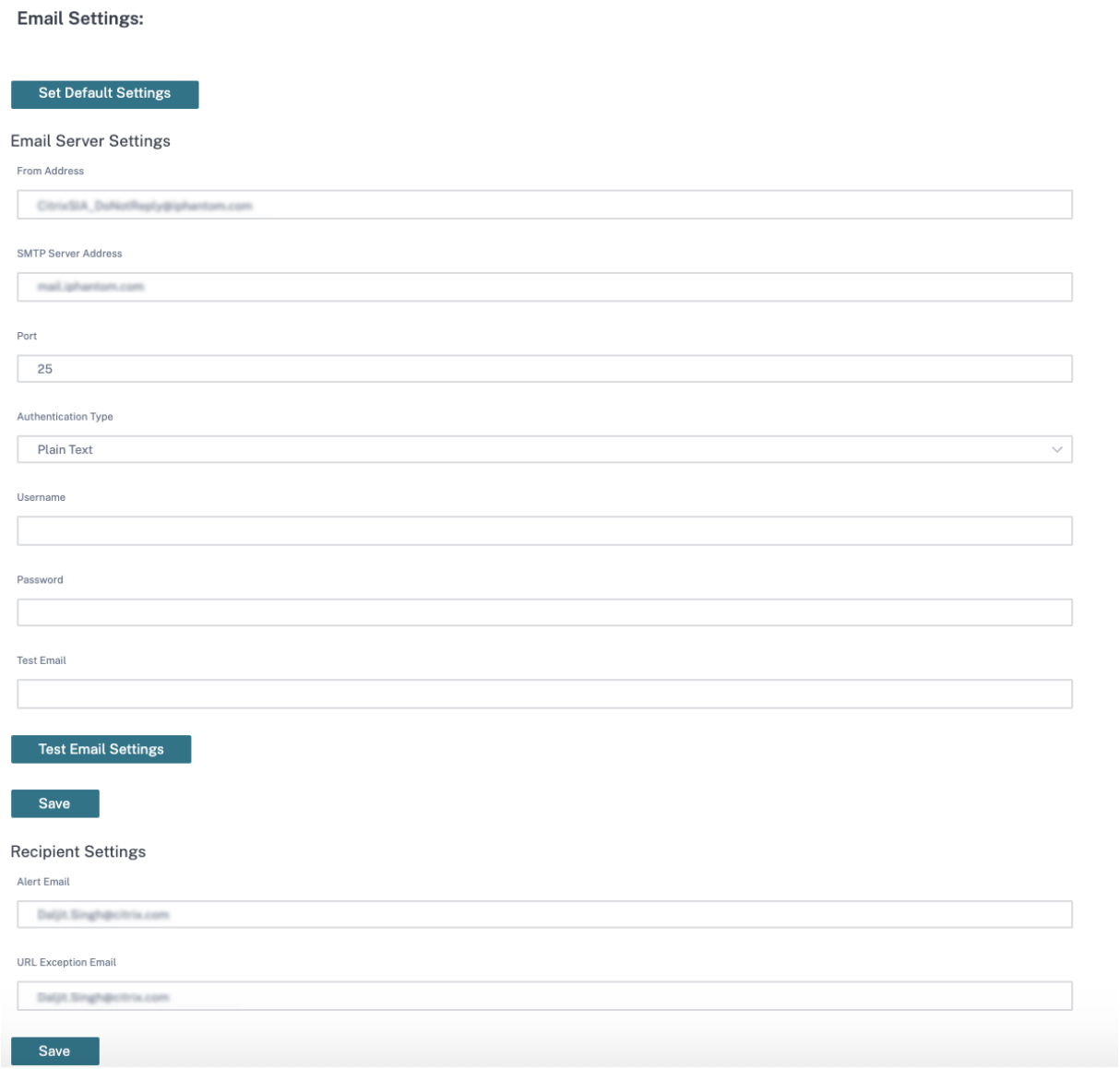
Vous pouvez configurer les paramètres du serveur de messagerie pour relayer les e-mails contenant des alertes, des rapports planifiés et d'autres notifications. Pour autoriser les passerelles Web et les nœuds de création de rapports à envoyer des notifications par e-mail, remplissez le formulaire dans **Paramètres de messagerie** sous **Paramètres du cloud**. Ce processus implique la configuration de l'adresse du serveur SMTP afin que vous puissiez recevoir des notifications par e-mail.

Vous pouvez vérifier les paramètres d'e-mail à l'aide de l'option **Tester les paramètres d'e-mail** . Vous pouvez également renseigner les paramètres de messagerie par défaut à l'aide du bouton **Définir les paramètres par défaut** .

Configurez les adresses e-mail pour recevoir des alertes utilisateur et des demandes d'exception d'URL.

- **E-mail d'alerte** : adresse de destination des alertes déclenchées par des mots clés à haut risque.
- **E-mail d'exception d'URL** : adresse de destination pour les demandes d'exception d'URL envoyées à partir de pages de blocage.

> **Remarque**
>
> Des alertes par e-mail supplémentaires sont disponibles sur la page **Alertes en temps réel** .



> **Remarque :**
>
> En règle générale, les serveurs SMTP sont configurés avec des listes d'autorisation basées sur l'adresse IP pour empêcher le spam. Vous devez donc ajouter les adresses IP de tous les nœuds à la liste d'autorisation du serveur SMTP.
>
> Pour réduire le spam, les serveurs SMTP utilisent parfois d'autres mécanismes, tels que DKIM. Il peut être nécessaire d'exempter les passerelles Web et les nœuds de reporting de ces restrictions sur le serveur SMTP.

Si vous ne disposez pas de votre propre serveur SMTP interne, vous pouvez utiliser l'un des services SMTP de Google. Pour cela, vous devez disposer d'un compte Gmail valide.

Les serveurs SMTP de Google utilisent les ports 25, 465, 587 ou une combinaison de ceux-ci. Le plus populaire est **smtp.gmail.com**, qui utilise les ports 465 (avec SSL) ou 587 (avec TLS).

> **Remarque :**
>
> Les serveurs SMTP écoutent généralement les ports TCP 25, 465 ou 587, mais peuvent écouter n'importe quel port sur lequel ils sont configurés pour fonctionner. Le protocole SMTP sur SSL utilise le port 465 et le protocole SMTP sur TLS utilise le port 587. Les ports 465 et 587 nécessitent des services d'authentification. Le port 25 n'est pas chiffré et ne nécessite aucune authentification.
>
> Lorsque vous travaillez avec des passerelles Web locales ou des nœuds de reporting, assurez-vous que les ports requis ne sont pas restreints.

Les configurations pour chacun des trois serveurs SMTP de Google sont les suivantes :

Nom de domaine complet	Configuration requise	Configuration requise pour l'authentification
smtp-relay.gmail.com	Port 25, 465 ou 587, avec les protocoles Secure Socket Layer (SSL) ou TLS (Transport Layer Security), et une ou plusieurs adresses IP statiques.	Adresse IP.
smtp.gmail.com	Port 465 avec SSL ou port 587 avec TLS. Les adresses IP dynamiques sont autorisées.	Votre adresse e-mail complète Gmail ou G Suite.
aspmx.l.google.com	Le courrier ne peut être envoyé qu'aux utilisateurs de Gmail ou de G Suite. Les adresses IP dynamiques sont autorisées.	Aucune.

smtp-relay.gmail.com est utilisé pour envoyer des messages de votre organisation en s'authentifiant avec les adresses IP associées. Vous pouvez envoyer des messages à toute personne se trouvant à l'intérieur ou à l'extérieur de votre domaine en utilisant les ports 25, 465 ou 587.

smtp.gmail.com est utilisé pour envoyer des e-mails à toute personne se trouvant à l'intérieur ou à l'extérieur de votre domaine. Vous devez vous authentifier à l'aide de votre compte Gmail ou G Suite et de votre mot de passe. Vous pouvez utiliser SMTP sur SSL (port 465) ou TLS (port 587).

aspmx.l.google.com est utilisé pour envoyer des messages aux utilisateurs de Gmail ou de G Suite uniquement. Cette option ne nécessite pas d'authentification. Vous ne pouvez pas utiliser SSL ou TLS avec ce serveur SMTP, et le trafic est donc en texte brut, ce qui n'est pas recommandé.

Journalisation anonymisée

Pour des raisons de conformité réglementaire et de confidentialité, la **journalisation anonymisée** dans **les paramètres du cloud** crypte les informations utilisateur personnelles que les administrateurs délégués utilisent pour surveiller l'utilisation du réseau.

Vous devez créer une clé de chiffrement avant d'activer la **journalisation anonymisée** en sélectionnant le bouton **Ajouter une clé** sous l'option **Activer la journalisation anonymisée** . Entrez une valeur de 64 caractères pour la clé de chiffrement dans le champ **Clé de chiffrement** . Vous pouvez entrer votre propre clé de chiffrement ou utiliser l'option **Générer automatiquement la clé** .

> **Important :**
>
> Citrix vous recommande vivement d'enregistrer la clé de chiffrement dans un emplacement distinct avant de continuer. Vous avez besoin de la clé de chiffrement pour déchiffrer les données qui lui sont associées tant qu'elles sont actives sur la plateforme.

Vous pouvez configurer une clé pour chiffrer les données identifiables d'une catégorie particulière en activant les options suivantes sous **Chiffrer les catégories** :

- **Informations personnelles.** Active et désactive le chiffrement de toutes les informations personnellement identifiables, y compris le nom d'utilisateur, le nom complet et le nom de machine de l'activité utilisateur signalée.
- **Source de données.** Active et désactive le chiffrement de toutes les informations relatives à la source de données de l'activité utilisateur signalée.
- **Noms de groupes.** Active et désactive le chiffrement des noms de groupe associés à l'activité utilisateur signalée.

Vous pouvez également configurer les clés de chiffrement pour qu'elles s'appliquent uniquement à un ensemble particulier de groupes dans l'onglet **Association de groupe** . Lorsque l'**option Sélectionner tout** est activée, la clé de chiffrement actuellement configurée s'applique à tous les groupes de sécurité. Lorsque l'**option Sélectionner tout** est désactivée, vous pouvez sélectionner les groupes de sécurité à chiffrer avec la clé de chiffrement.

Après avoir configuré une clé de chiffrement, activez la **journalisation anonymisée** pour surveiller l' utilisation du réseau en fonction des journaux anonymisés de l'activité en ligne des utilisateurs.

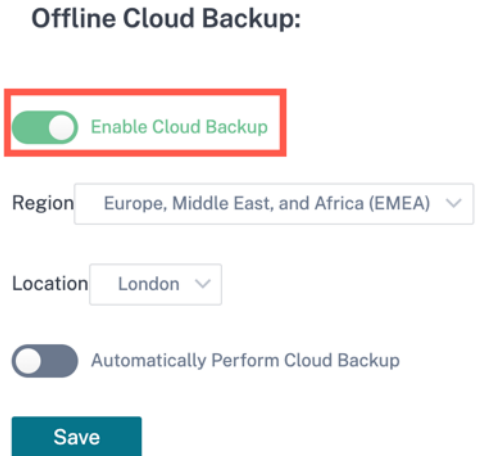
Pour supprimer une clé de chiffrement précédemment définie, sélectionnez les points de suspension en regard de la clé de chiffrement correspondante dans le tableau, puis sélectionnez **Supprimer**.

Sauvegarde dans le cloud

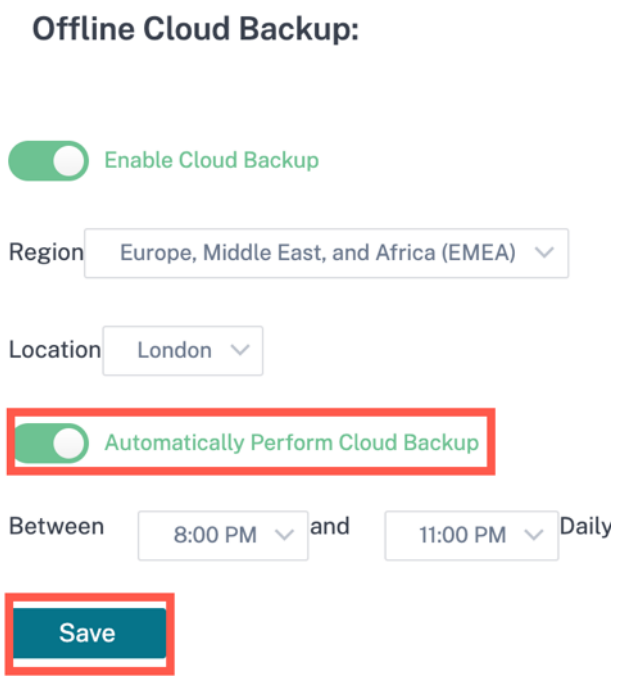
Les paramètres de **sauvegarde hors ligne dans le cloud** permettent de stocker/enregistrer les paramètres de sauvegarde et les journaux des nœuds de reporting en fonction de la **région**, de l' **emplacement**et de l'**heure** que vous sélectionnez. Avec l'option de **sauvegarde cloud hors ligne**, vous pouvez enregistrer les sauvegardes cloud via l'interface CSIA.

Pour activer les paramètres de sauvegarde dans le cloud, accédez à **Configuration** développez **Paramètres du cloud** sélectionnez **Sauvegarde dans le cloud**.

1. Activez le bouton bascule **Activer la sauvegarde dans le cloud** et sélectionnez la **région** et l' **emplacement** dans la liste déroulante.



2. Vous pouvez également activer le bouton bascule **Effectuer automatiquement la sauvegarde dans le cloud** et définir l'intervalle de temps pour l'exécution et la création de la sauvegarde quotidienne. Cliquez sur **Enregistrer**.

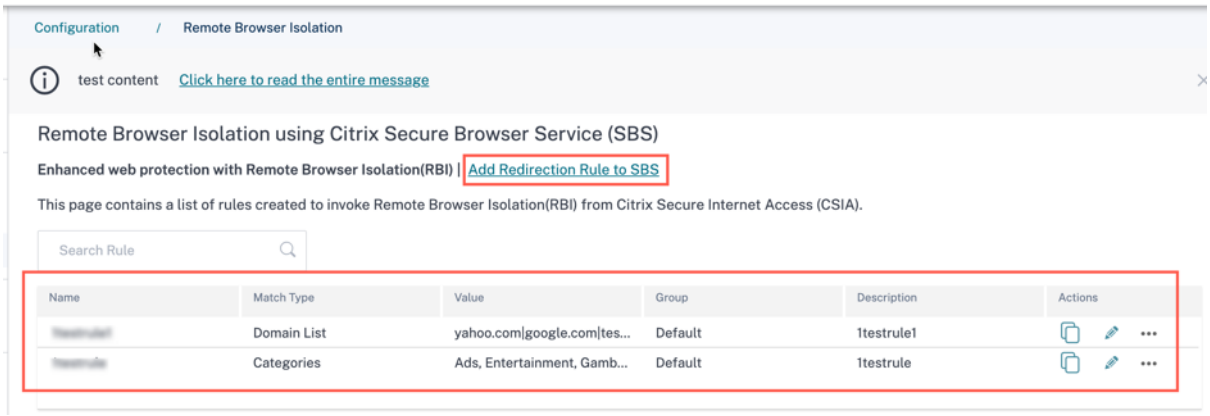


Isolation du navigateur distant

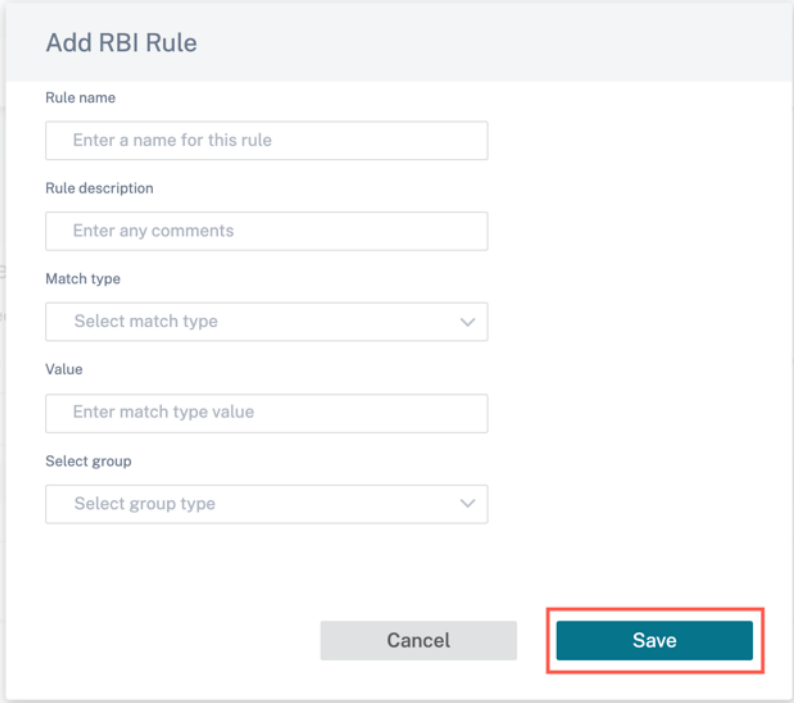
L'isolation du navigateur à distance est une fonction de protection Web avancée qui assure la sécurité contre les logiciels malveillants/menaces malveillantes. Avec l'isolation du navigateur à distance, la fonctionnalité de filtrage Web Citrix Secure Internet Access peut être utilisée avec le service Secure Browser (SBS) pour protéger le réseau d'entreprise contre les attaques basées sur le navigateur. Pour plus d'informations, consultez Secure Browser Service.

Avec la fonctionnalité d'isolation du navigateur à distance, vous pouvez définir des règles pour certains sites Web ciblés qui ne sont pas fiables pour être isolés et lancés uniquement via le service de navigateur sécurisé distant basé sur le cloud. Vous pouvez créer et appliquer la règle à une combinaison de groupes d'utilisateurs et de types de trafic que vous souhaitez isoler.

Vous pouvez afficher la liste des règles créées pour invoquer l'isolation du navigateur distant.



Pour définir les règles de redirection pour le trafic qui doit être appelé, accédez à **Configuration > Isolation du navigateur distant** Cliquez sur **Ajouter une règle de redirection à SBS**.



- **Nom de la règle** : indiquez un nom de règle.
- **Description de la règle** : Fournissez une description de la règle.
- **Type de correspondance** : Sélectionnez un type de correspondance tel que Regex de domaine, Liste de domaines, Adresse IP, URL ou Catégories dans la liste déroulante.
- **Valeur** : Entrez le type de valeur de correspondance.
- **Sélectionner un groupe** : sélectionnez un groupe dans la liste déroulante.

Avec l'option **Ajouter une règle de redirection à SBS**, vous pouvez créer les règles de filtrage Web sur le portail d'accès Internet sécurisé pour rediriger le trafic vers le service de navigateur. Pour chaque règle d'isolation de navigateur distant, une URL de navigateur sécurisée est associée. Cela signifie que lorsque les URL sont lancées via le service d'accès Internet sécurisé, si l'URL correspond à l'une des règles de correspondance d'isolation de navigateur distant définies, la demande est alors redirigée vers le service de navigateur sécurisé associé.

Administration

January 26, 2022

Le rôle d'un administrateur définit les autorisations permettant d'afficher les fonctionnalités et d'effectuer diverses activités dans le service Citrix Secure Internet Access (CSIA).

Les fonctionnalités suivantes sont incluses dans le cadre du service Citrix Secure Internet Access :

- **Tableau de bord**. Accès aux rapports de haut niveau.
- **Passerelle Web**. Accès au service Secure Web Gateway.
- **Rapports et analyses**. Accès à des rapports plus détaillés.
- **Emplacements et géocartographie**. Accès aux emplacements géographiques des nœuds de cloud et de passerelle.
- **Gestion des collections de nœuds**. Accès à la fonctionnalité de gestion des collections de nœuds.
- **Licences**. Possibilité de récupérer les détails de licence pour le service.
- **Gestion des utilisateurs**. Possibilité de créer des rôles personnalisés et d'attribuer des rôles personnalisés à d'autres administrateurs.

Contrôle d'accès basé sur les rôles

Comme pour Citrix SD-WAN Orchestrator, l'accès aux ressources du service Citrix Secure Internet Access est géré en fonction des rôles attribués aux administrateurs individuels. Il existe quatre niveaux d'accès qui peuvent être attribués à un utilisateur administrateur du service Citrix Secure Internet Access : client-maître-administrateur, client-maître-administrateur en lecture seule, client-non-accès et mode de confidentialité client-maître-lecture-administrateur-lecture-seul.

- Le niveau **Client-Maître-Admin** est un rôle d'accès complet qui permet à l'administrateur d' effectuer les opérations suivantes :
  - Gérer toutes les fonctionnalités du service Citrix Secure Internet Access.
  - Ajouter des administrateurs au service.
  - Supprimer les administrateurs du service.
  - Attribuer, modifier et supprimer des rôles au sein du réseau client.
  - Créer des rôles personnalisés.
- Le niveau **Client-Master-ReadOnly-Admin** est un rôle en lecture seule qui permet à l'administrateur d'afficher uniquement les fonctionnalités du service Citrix Secure Internet Access.
- Le niveau **Client sans accès** refuse l'accès à toutes les fonctionnalités du service Citrix Secure Internet Access.
- Le niveau **Customer-Master-ReadOnly-Admin-Privacy-Mode** accorde un accès en lecture seule à toutes les fonctionnalités du service Citrix Secure Internet Access, à l'exception des **licences** et des **paramètres utilisateur**. Les utilisateurs ayant ce rôle ne peuvent pas afficher la liste des autres utilisateurs administrateurs de leur compte, les rôles attribués ou les informations relatives aux licences.

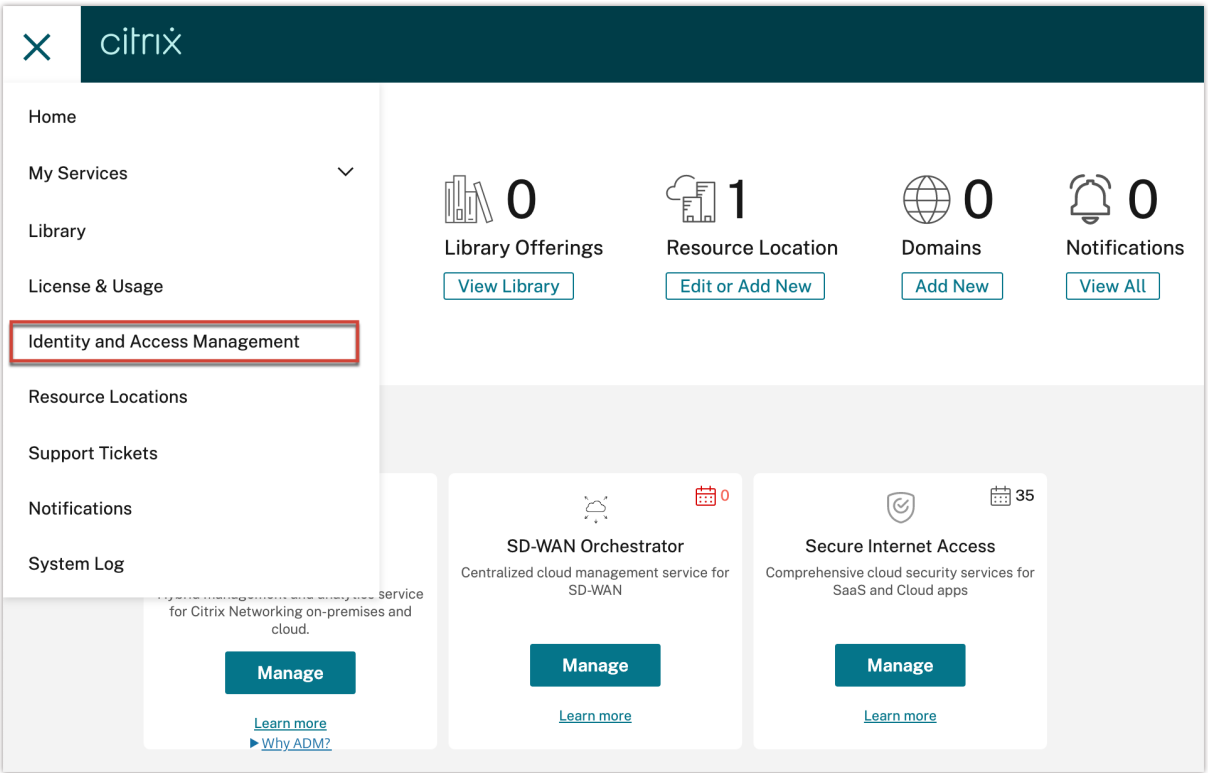
> **Remarque :**
>
> Pour le service Citrix Secure Internet Access, les rôles sont attribués au niveau du **client** . Pour le service Citrix SD-WAN Orchestrator, les rôles sont attribués à la fois au niveau du **client** et au niveau du **fournisseur** . Par conséquent, le service Citrix SD-WAN Orchestrator a à la fois le rôle **Client-maître-administrateur** et le rôle **Fournisseur-maître-administrateur-tous** disponibles.

Pour appliquer le RBAC, vous devez d'abord ajouter des utilisateurs en tant qu'administrateurs aux services Citrix Cloud.

Ajouter de nouveaux utilisateurs aux services Citrix Cloud

Vous pouvez ajouter des administrateurs au service Citrix Secure Internet Access à l'aide de la fonctionnalité **Gestion des identités et des accès** de Citrix Cloud. Les nouveaux administrateurs peuvent utiliser leurs informations d'identification de compte Citrix existantes ou créer un nouveau compte si nécessaire.

Pour ajouter de nouveaux administrateurs, sélectionnez **Gestion des identités et des accès** dans le menu de la page d'accueil Citrix Cloud, puis suivez les instructions de l'interface utilisateur. Pour plus d'informations, consultez Gérer les administrateurs Citrix Cloud.

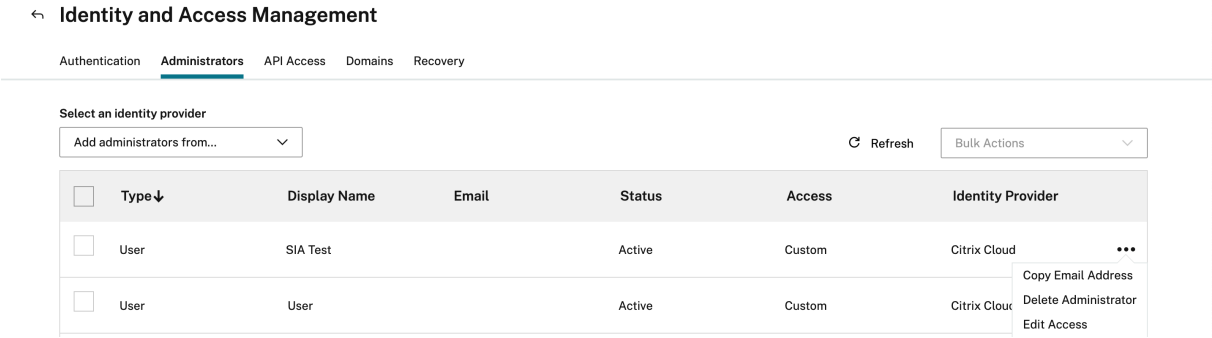


Tout nouvel administrateur que vous ajoutez se voit automatiquement attribuer un accès complet aux services Citrix Cloud. Vous pouvez modifier les parties de Citrix Cloud qu'un administrateur peut afficher et gérer à un niveau plus granulaire.

Accès en édition pour les nouveaux utilisateurs

Une fois que vous avez ajouté un nouvel administrateur via Citrix **Identity and Access Management**, vous pouvez définir le rôle.

Sélectionnez **Modifier l'accès** dans la liste des actions sur le compte que vous avez créé et choisissez « Accès complet » (aux services Citrix Cloud) ou « Accès personnalisé ».



Pour accorder un accès complet au service Citrix Secure Internet Access, sans sélection personnalisée de sous-fonctionnalités (sous **Accès personnalisé** > **Gestion générale**), sélectionnez l'option **Accès complet** de haut niveau.

Sélectionnez **Accès personnalisé si l'** une ou les deux conditions suivantes s'appliquent :

- Vous souhaitez réglementer l'accès aux sous-fonctionnalités répertoriées sous **Gestion générale**.
- Vous souhaitez réguler le niveau d'accès au service Citrix Secure Internet Access, en particulier.

Si vous choisissez **Accès personnalisé**, vous devez spécifier le niveau d'accès pour **Secure Internet Access** séparément de **la gestion générale**. Cet accès peut être : un accès complet, un accès en lecture seule, un accès en lecture seule (mode Confidentialité) ou aucun accès.

Un utilisateur auquel est affecté **Customer Admin : Full Access** a le même accès au service Citrix Secure Internet Access que celui accordé par l'option **Accès complet** de haut niveau (située au-dessus de **Accès personnalisé**). Choisissez **Customer Admin : Full Access** pour accorder un accès complet aux fonctionnalités du service Citrix Secure Internet Access tout en choisissant différents niveaux d'accès aux sous-fonctionnalités sous **Gestion générale**.

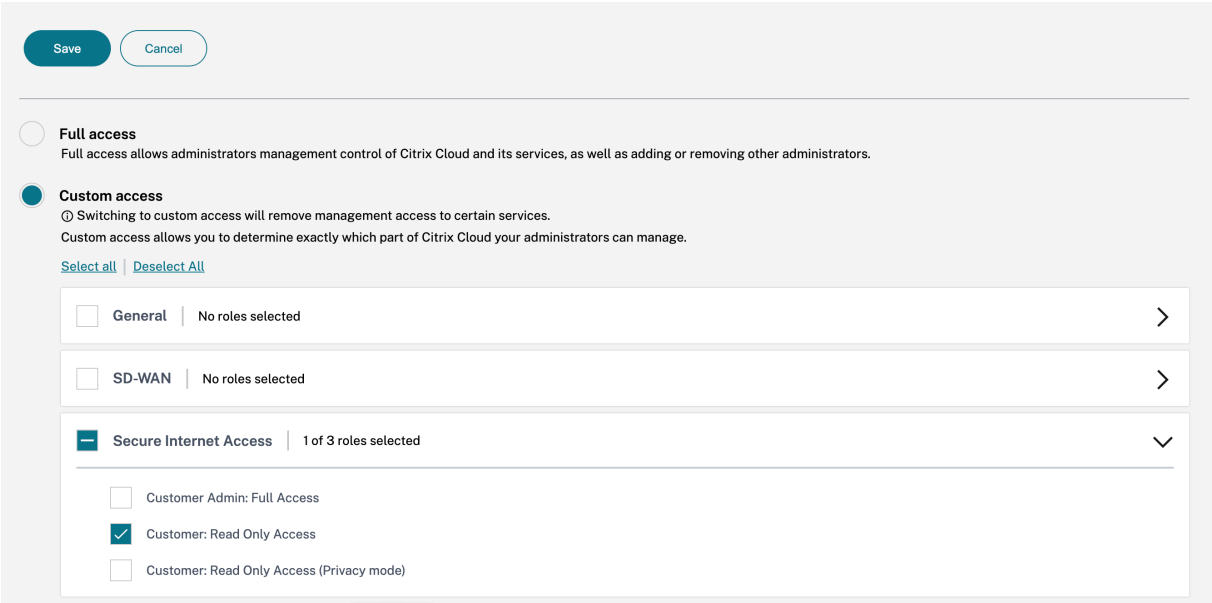
> **IMPORTANT**
>
> **Cochez une** ou **aucune** des cases sous **Accès Internet sécurisé**. Si les deux cases sont cochées,

> le niveau d'autorisation le plus élevé est accordé à l'administrateur, ce qui présente un risque pour la sécurité.

Un utilisateur auquel est affecté **Client : Accès en lecture seule** peut uniquement *afficher* les fonctionnalités du service. Un utilisateur auquel est attribué **Client : Accès en lecture seule (mode Confidentialité)** dispose d'un accès en lecture seule pour afficher toutes les fonctionnalités du service, à l'exception des **licences** et des **paramètres utilisateur**.

Si vous ne sélectionnez aucune des options, l'utilisateur n'a pas accès aux fonctionnalités de Citrix Secure Internet Access.

> **Remarque**
>
> Vous ne pouvez pas modifier le rôle d'un administrateur dans le service Citrix Secure Internet Access si l'accès lui est refusé dans **Gestion des identités et des accès**. Pour afficher et modifier un administrateur dans le service Citrix Secure Internet Access, vous devez lui accorder un accès complet ou en lecture seule lorsque vous l'ajoutez pour la première fois.



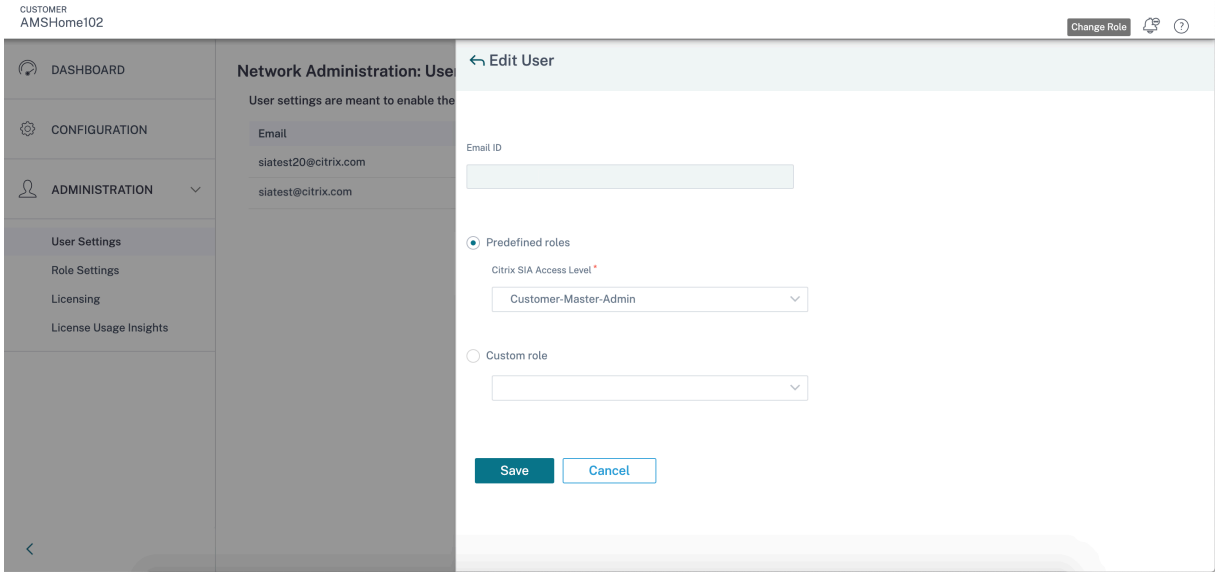
> **IMPORTANT**
>
> Toutes les modifications ultérieures apportées à l'accès d'un utilisateur doivent se produire dans les paramètres utilisateur du service Citrix Secure Internet Access. Les autorisations existantes pour un administrateur qui sont modifiées dans **Gestion des identités et des accès** ne sont pas envoyées au service Citrix Secure Internet Access. Dans certains cas, vous devrez peut-être supprimer et réinviter l'administrateur.

Définition des rôles des utilisateurs

Cette section explique comment vous pouvez définir et gérer davantage l'accès administrateur aux fonctionnalités du service Citrix Secure Internet Access.

> **Remarque :**
>
> Les clients qui disposent à la fois d'un abonnement au service Citrix Secure Internet Access et d'un abonnement au service Citrix SD-WAN Orchestrator partagent **Administration > Paramètres utilisateur**.

Pour modifier le rôle d'un utilisateur existant en tant qu'administrateur pour le service Citrix Secure Internet Access, accédez à **Administration** > **Paramètres utilisateur**. Vous pouvez attribuer des rôles à partir d'une liste de rôles prédéfinis et d'une liste de rôles personnalisés. Choisissez l'accès basé sur les rôles approprié dans l'un des menus, puis enregistrez votre sélection.

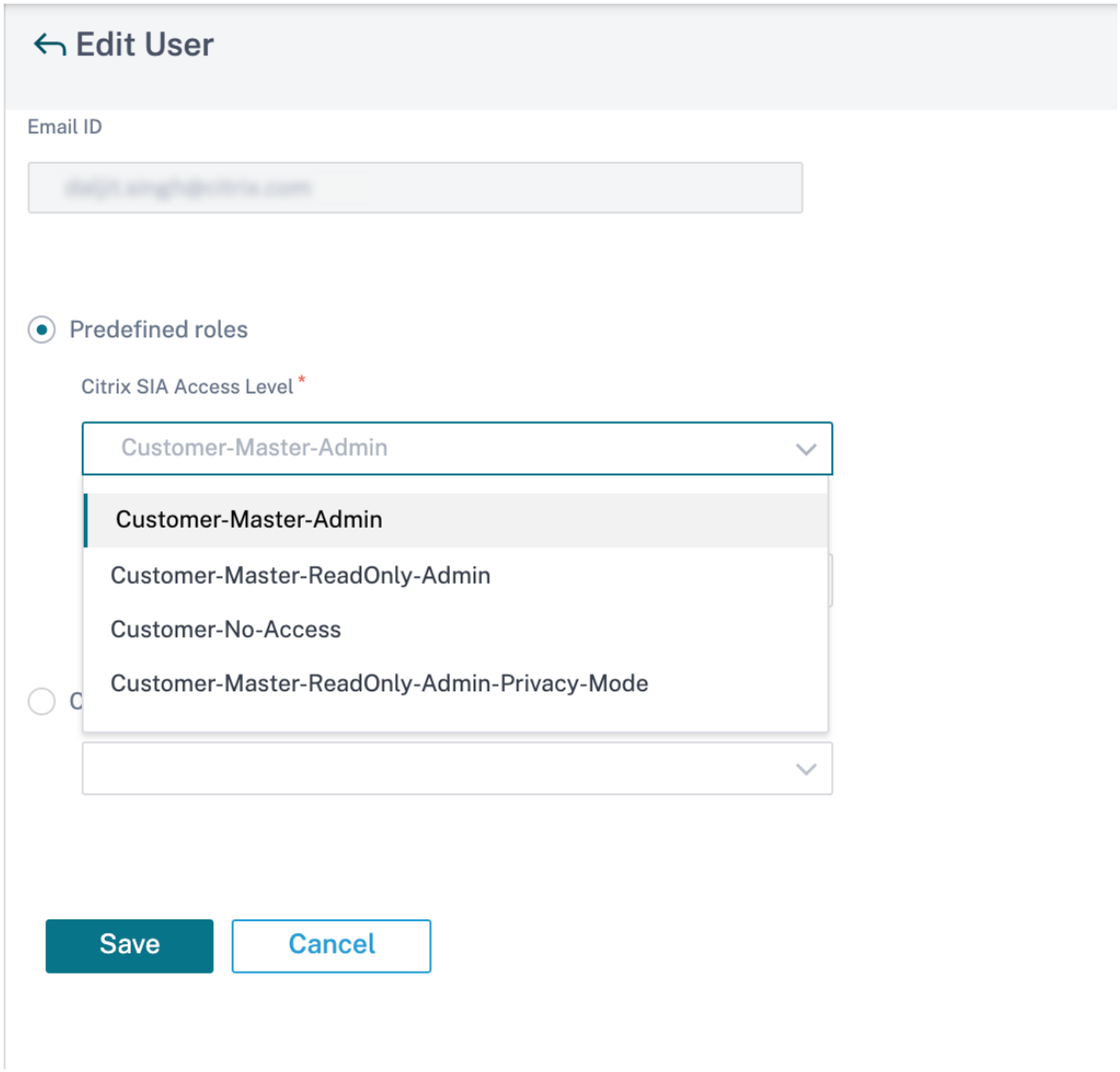


Rôles prédéfinis

Quatre rôles prédéfinis au niveau du **client** sont disponibles pour le service Citrix Secure Internet Access :

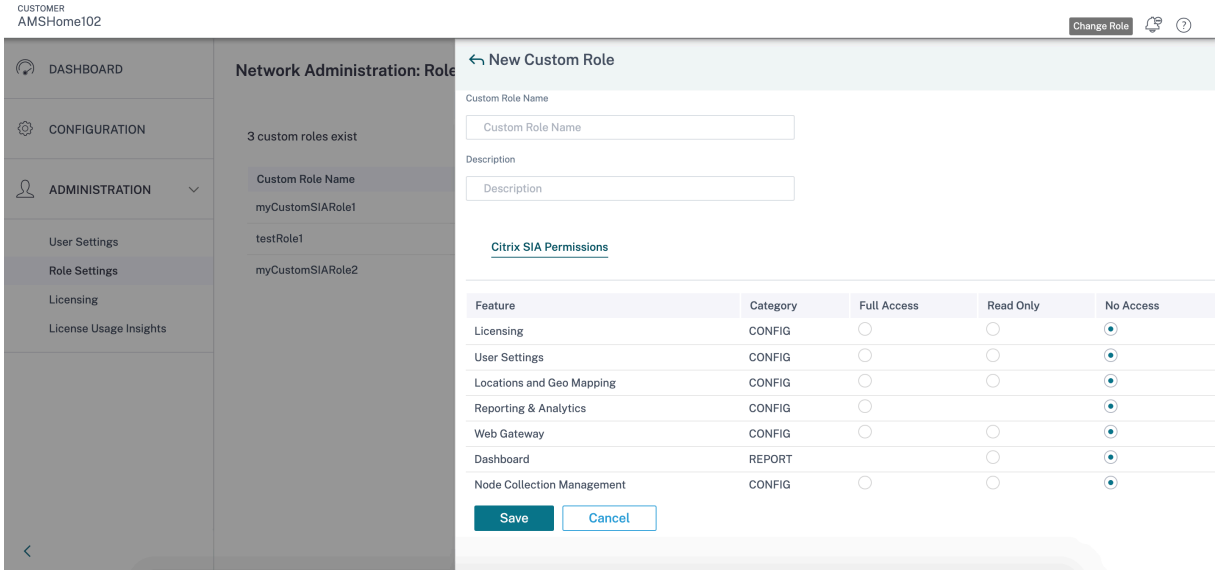
- Le rôle **Client-Master-Admin** (par défaut) permet à l'administrateur d'afficher et de modifier les informations de Citrix Secure Internet Access.
- Le rôle **Customer-Master-ReadOnly-Admin** permet à l'administrateur d'afficher les informations Citrix Secure Internet Access, sans autorisation de modification.
- Le rôle **Client sans accès** refuse à l'administrateur l'accès aux fonctionnalités du service Citrix Secure Internet Access.

- Le niveau **Customer-Master-ReadOnly-Admin-Privacy-Mode** accorde un accès en lecture seule à toutes les fonctionnalités du service Citrix Secure Internet Access, à l'exception des **licences** et des **paramètres utilisateur**. Les utilisateurs ayant ce rôle ne peuvent pas afficher la liste des autres utilisateurs administrateurs de leur compte, les rôles attribués ou les informations relatives aux licences.



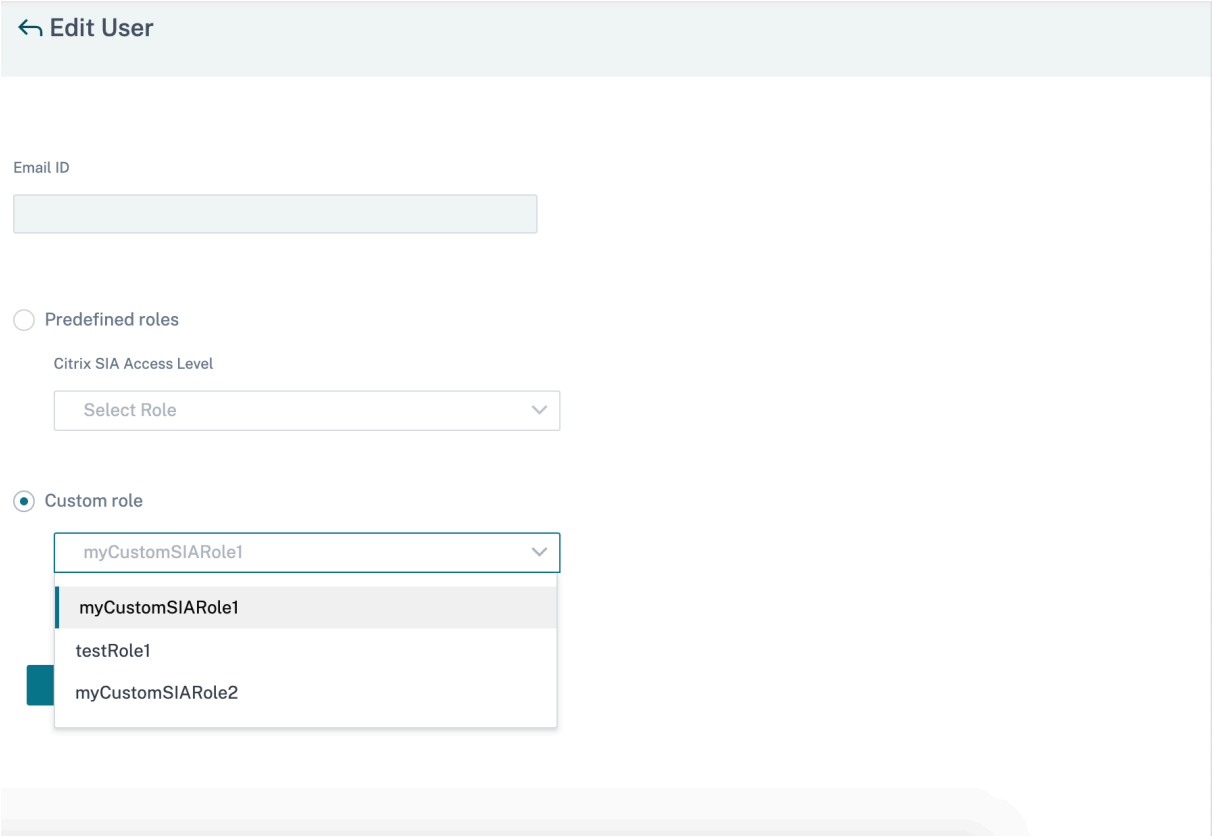
Rôles personnalisés

Vous pouvez créer des rôles personnalisés en fonction de différentes autorisations pour les fonctionnalités individuelles du service Citrix Secure Internet Access.



Pour créer un rôle d'administrateur personnalisé qui peut ensuite être attribué à des administrateurs, accédez à **Administration** > **Paramètres du rôle**. Le formulaire **Nouveau rôle personnalisé** vous permet de sélectionner différents niveaux d'accès pour les fonctionnalités individuelles du service Citrix Secure Internet Access.

Une fois que vous avez créé un rôle personnalisé, il apparaît dans la liste des rôles personnalisés dans **les paramètres utilisateur**.



Rôles multiples

Si un utilisateur est administrateur de plusieurs clients, plusieurs rôles lui sont attribués dans le service Citrix Secure Internet Access et peuvent basculer entre les comptes. Dans de tels scénarios, l'utilisateur peut avoir un rôle différent en fonction de chaque compte.

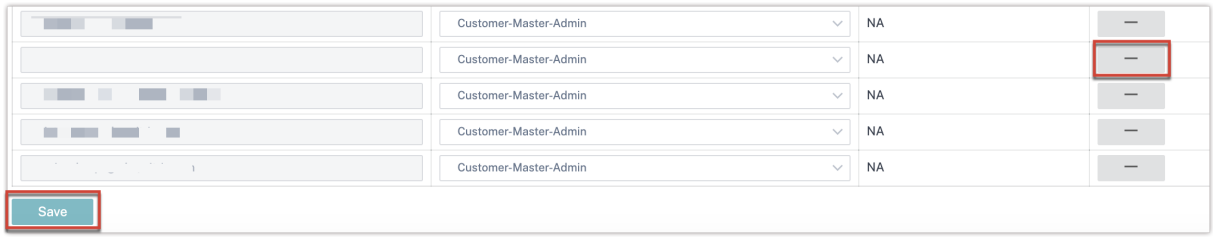
Pour basculer entre les rôles, sélectionnez **Changer de rôle** en haut à droite de l'écran, à côté de l'icône en forme de cloche.

Afficher les informations relatives à

Vous pouvez afficher les rôles et les adresses e-mail de tous les administrateurs. Pour afficher les détails de l'administrateur, accédez à **Administration** > **Administrateurs**.

Supprimer un administrateur

Pour supprimer un administrateur du service Citrix Secure Internet Access, accédez à **Administration** > **Administrateurs**. Cliquez sur le bouton Supprimer en regard du compte que vous souhaitez supprimer, puis sélectionnez **Enregistrer**.



Glossaire

January 26, 2022

Citrix Cloud : Citrix Cloud est une plateforme qui héberge et administre les services Citrix. Il se connecte à vos ressources via des connecteurs sur tout cloud ou toute infrastructure de votre choix (infrastructure locale, cloud public, cloud privé ou cloud hybride). Il vous permet de créer, de gérer et de déployer des espaces de travail contenant des applications et des données pour vos utilisateurs finaux à partir d'une console unique.

Citrix SD-WAN : Citrix SD-WAN simplifie la mise en réseau des succursales grâce à une expérience d'espace de travail fiable et hautes performances qui facilite l'accès aux applications SaaS, aux bureaux virtuels ou aux centres de données traditionnels.

Citrix Secure Workspace Access : le service Citrix Secure Workspace 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 de contrôle d'accès de bout en bout. Avec le service Citrix Secure Workspace Access, les administrateurs peuvent également protéger le réseau et les machines des utilisateurs finaux de l'entreprise 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.

Citrix Workspace : Citrix Workspace est une solution complète d'espace de travail numérique qui vous permet de fournir un accès sécurisé aux informations, applications et autres contenus pertinents pour le rôle d'une personne dans votre organisation. Les utilisateurs s'abonnent aux services que vous mettez à disposition et peuvent y accéder depuis n'importe où, sur n'importe quel appareil. Citrix Workspace vous aide à organiser et à automatiser les détails les plus importants dont vos utilisateurs ont besoin pour collaborer, prendre de meilleures décisions et se concentrer pleinement sur leur travail.

Application**Citrix Workspace : l'**application Citrix Workspace permet aux utilisateurs d'accéder instantanément à toutes leurs applications SaaS et Web, à leurs fichiers et applications mobiles, ainsi qu'à leurs applications et bureaux virtuels à partir d'une interface tout-en-un facile à utiliser. L'application Citrix Workspace constitue un point d'entrée unique pour tous les services d'espace de travail des utilisateurs. Les utilisateurs bénéficient d'un accès transparent et sécurisé à toutes les applications dont ils ont besoin pour rester productifs, y compris des fonctionnalités telles que la navigation intégrée et l'authentification unique.

Virtual Delivery Agent (VDA) : le VDA est un composant clé de Citrix Virtual Apps and Desktops. Le VDA est installé sur chaque machine physique ou virtuelle de votre site que vous mettez à disposition des utilisateurs. Le VDA permet aux machines de s'enregistrer auprès du Controller, qui permet à la machine et aux ressources qu'elle héberge d'être mise à la disposition des utilisateurs. Les VDA établissent et gèrent la connexion entre la machine et l'appareil de l'utilisateur. Les VDA vérifient également qu'une licence Citrix est disponible pour l'utilisateur ou la session et appliquent les stratégies configurées pour la session.