Citrix Workspace

Contents

Vue d'ensemble de Citrix Workspace

November 28, 2023

Citrix Workspace est une solution d'espace de travail numérique qui fournit un accès sécurisé et unifié aux applications, aux bureaux et au contenu (ressources) de n'importe où et sur n'importe quel appareil. Ces ressources peuvent être des instances Citrix DaaS, des applications de contenu, des applications locales et mobiles, des applications SaaS et Web, ainsi que des applications de navigateur.

Fonctionnement de Citrix Workspace

Citrix Workspace agrège et intègre les services Citrix Cloud, permettant un accès unifié à toutes les ressources disponibles pour vos utilisateurs (abonnés) dans un seul emplacement de ressources. Les utilisateurs de Citrix Workspace sont appelés « abonnés » parce que vous « abonnez » les employés aux services que vous mettez à leur disposition par le biais de leurs espaces de travail.

Pour obtenir une vue d'ensemble des services disponibles via Citrix Workspace, consultez Services hébergés dans le cloud via Citrix Workspace.

Les abonnés bénéficient d'une vue complète et unifiée de chaque ressource que vous mettez à leur disposition via ces services dans l'interface utilisateur (UI) de Citrix Workspace. Pour plus d'informations sur l'expérience des abonnés dans l'interface utilisateur de Citrix Workspace, consultez Gérer votre expérience d'espace de travail.

Les abonnés accèdent aux services que vous configurez et activez dans **Configuration de l'espace de travail**, soit via le navigateur avec l'URL de l'espace de travail, soit via l'application Citrix Workspace qui remplace Citrix Receiver. Pour plus d'informations sur la façon dont les utilisateurs accèdent à leurs espaces de travail, consultez Accès à l'espace de travail.

Les abonnés s'authentifient auprès de leurs espaces de travail en utilisant le fournisseur d'identité principal que vous configurez dans **Gestion des identités et des accès**, puis activez dans **Configuration de l'espace de travail**. Les abonnés sont ensuite automatiquement authentifiés auprès de chaque service hébergé dans le cloud acheté pour Citrix Workspace, ce qui contribue à renforcer la sécurité et à réduire les problèmes d'utilisation. Pour plus d'informations sur la configuration de l'authentification auprès de Workspace, consultez Espaces de travail sécurisés

Présentation de la mise en route

Citrix Workspace est configuré via la **console Citrix Cloud**, dans laquelle se trouve un écran d'administration **Gestion des identités et des accès** et une interface de gestion Citrix Workspace appelée **Configuration de l'espace de travail**. La mise en route de Citrix Workspace implique les tâches suivantes.

1. Assurez-vous que votre configuration vous permet de mettre en œuvre Citrix Workspace dans la **console Citrix Cloud** où vous pouvez effectuer les opérations suivantes :
    - Intégrer des services basés sur le cloud
    - Constituer votre équipe de déploiement
    - Configurer votre infrastructure et vos ressources
2. Définissez les fournisseurs d'identité et les comptes dans **Gestion des identités et des accès** pour les groupes suivants :
    - Administrateur Citrix Cloud
    - Abonnés Citrix Workspace
3. Configurez vos espaces de travail dans **Configuration de l'espace de travail**, notamment :
    - Définir l'accès interne et externe
    - Intégrer des services que vous avez configurés dans la console Citrix Cloud dans vos espaces de travail
    - Personnaliser l'apparence de l'espace de travail et l'expérience des abonnés une fois connectés

Au-delà de cette configuration de base, vous avez le choix entre d'autres options de sécurité, de confidentialité et d'optimisation. Les options les plus courantes sont les suivantes :

- Configurer l'authentification unique (SSO) pour DaaS dans Citrix Workspace avec le service d'authentification fédérée Citrix (FAS) FAS est généralement adopté si vous utilisez une méthode d'authentification fédérée, telle qu'Okta ou Azure Active Directory.

Pour obtenir une vue d'ensemble des tâches et des informations nécessaires au fur et à mesure de la progression de votre déploiement, consultez la section Mise en route de Citrix Workspace. Chaque étape vous guide dans la console Citrix Cloud et inclut des instructions pour des tâches telles que la configuration de votre fournisseur d'identité et l'activation des services. La procédure détaillée fournit également un accès rapide aux informations techniques dont vous aurez besoin lorsque vous assemblez votre équipe de déploiement et que vous configurez votre infrastructure et vos ressources.

Services hébergés dans le cloud via Citrix Workspace

Les abonnés utilisent Citrix Workspace pour accéder aux ressources fournies par les services hébergés dans le cloud. Les clients Citrix Cloud existants peuvent passer à l'expérience complète de l'espace de travail numérique en exploitant ces services dans la solution Citrix Workspace.

Cette section décrit les principaux services hébergés dans le cloud qui peuvent être activés pour Citrix Workspace, en fonction de vos droits. Pour plus d'informations sur la façon de configurer et d'activer l'accès aux services que vous avez achetés, consultez la page Mise en route de Citrix Workspace.

Pour obtenir une description complète de chaque édition de Citrix Workspace et des fonctionnalités incluses, consultez le tableau des fonctionnalités de Citrix Workspace.

Citrix DaaS

Citrix Workspace est le point d'accès multi-locataire hébergé dans le cloud de Citrix DaaS. Pour configurer Citrix DaaS, suivez les étapes décrites dans Citrix DaaS.

Si vous êtes un client Virtual Apps and Desktops local, il existe différentes options pour accéder à vos ressources via Citrix Workspace. L'option que vous choisissez dépend si vous souhaitez migrer complètement vers le cloud ou adopter une solution hybride, et si vous prévoyez d'autoriser l'accès externe. Pour plus d'informations sur ces options, consultez la page Mettre à disposition DaaS avec Citrix Workspace.

Applications SaaS et Web, sécurisées avec le service Citrix Secure Private Access

Citrix Secure Private Access (anciennement **Secure Workspace Access** et **Access Control Service**) fournit l'authentification unique (SSO) aux applications Web et SaaS intégrées à Workspace. Le service vous permet également de gérer les privilèges d'accès et les stratégies de contrôle qui sanctionnent les niveaux appropriés d'accès aux applications Web hébergées par l'entreprise en fonction des informations d'identification de l'abonné.

Pour plus d'informations sur les avantages du service **Citrix Secure Private Access**, accédez à la page Tech Brief: Secure Private Access.

Citrix Gateway Service

Citrix Gateway Service (anciennement **NetScaler Gateway Service**) est utilisé avec **Citrix Secure Private Access** pour mettre en œuvre un environnement entièrement hébergé dans le cloud géré par Citrix.

Citrix Gateway Service offre une expérience unifiée aux applications SaaS et aux instances Virtual Apps and Desktops en fournissant une connectivité externe aux espaces de travail sur la base d'une infrastructure de stratégie avancée.

Suivez les étapes pour configurer Citrix Gateway Service, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner un accès à distance. Pour plus d'informations sur la configuration des applications SaaS dans Citrix Gateway Service, consultez Prise en charge des applications SaaS.

Citrix Remote Browser Isolation Service

Intégrez **Citrix Remote Browser Isolation Service** à vos espaces de travail pour isoler la navigation Web et protéger le réseau d'entreprise contre les attaques basées sur les navigateurs. Lorsque des abonnés accèdent à l'URL de l'espace de travail, leurs navigateurs publiés sont affichés, ainsi que d'autres applications et bureaux configurés dans d'autres services Citrix Cloud.

Pour permettre aux abonnés d'accéder à un navigateur isolé distant, configurez Remote Browser Isolation, puis testez et partagez l'URL de l'espace de travail avec vos abonnés.

Citrix Endpoint Management

Citrix Endpoint Management vous permet de gérer les stratégies des appareils et des applications à l'aide d'une sécurité stricte pour l'identité, les appareils, les applications, les données et les réseaux. L'intégration à Citrix Workspace diffère pour les nouveaux clients et les clients existants. Pour plus d'informations sur l'intégration d'Endpoint Management à Citrix Workspace, reportez-vous à la section Intégration à l'expérience Citrix Workspace.

Citrix Analytics

Le service **Citrix Analytics** collecte et fournit des informations sur tous vos abonnés Citrix Workspace. Différentes offres Citrix Analytics sont disponibles en fonction de vos droits. Il s'agit de **Citrix Analytics for Security**, **Citrix Analytics for Performance** et **Citrix Analytics (Usage)**. Pour en savoir plus sur ces services, consultez Citrix Analytics.

Nouveautés

November 28, 2023

L'un des objectifs de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour aux clients de Citrix Workspace lorsqu'elles sont disponibles. Les versions initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients.

Pour plus d'informations sur le contrat de niveau de service dans le cadre de la scalabilité et la disponibilité des services dans le cloud, consultez le Contrat de niveau de service de Citrix Cloud. Pour contrôler les interruptions de service et la maintenance planifiée, consultez le tableau de bord de l'état de service.

Nouveautés dans Citrix Workspace

Recevez les dernières améliorations et mises à jour apportées à Citrix Workspace afin d'exploiter tout le potentiel de notre technologie. Optimisez la productivité de vos utilisateurs et améliorez la qualité de leurs interactions en intégrant des mises à jour en temps opportun de Citrix Workspace.

- Nouveautés dans la plate-forme Workspace
- Nouveautés dans l'interface utilisateur de Workspace
- Nouveautés dans Global App Configuration Service

Application Citrix Workspace sur différentes plates-formes

Pour en savoir plus sur les nouvelles fonctionnalités et améliorations de **l'application Citrix Workspace** pour vos plates-formes préférées, cliquez sur les liens suivants.

- Android
- ChromeOS
- HTML5
- iOS
- Linux
- Mac
- Microsoft Teams
- Windows
- Windows Store

Découvrez également les nouveautés de Citrix Enterprise Browser.

Nouveautés de la plate-forme Workspace

November 28, 2023

L'un des objectifs de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour aux clients de Citrix Workspace lorsqu'elles sont disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible.

Ce processus est transparent pour l'utilisateur. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet de maximiser la qualité et la disponibilité des produits.

Pour plus d'informations sur le contrat de niveau de service dans le cadre de la scalabilité et la disponibilité des services dans le cloud, consultez le Contrat de niveau de service de Citrix Cloud. Pour contrôler les interruptions de service et la maintenance planifiée, consultez le tableau de bord de l'état de service.

Nov 2023

Configurer un domaine personnalisé - Disponibilité générale

La fonctionnalité Domaine personnalisé est désormais disponible pour tous. Vous pouvez configurer un domaine personnalisé pour votre espace de travail, ce qui vous permet d'utiliser le domaine de votre choix pour accéder à votre magasin Citrix Workspace. Vous pouvez ensuite utiliser ce domaine à la place du domaine cloud.com qui vous a été attribué pour y accéder à la fois depuis un navigateur Web et des applications Citrix Workspace. Pour plus d'informations, consultez la section Configurer un domaine personnalisé.

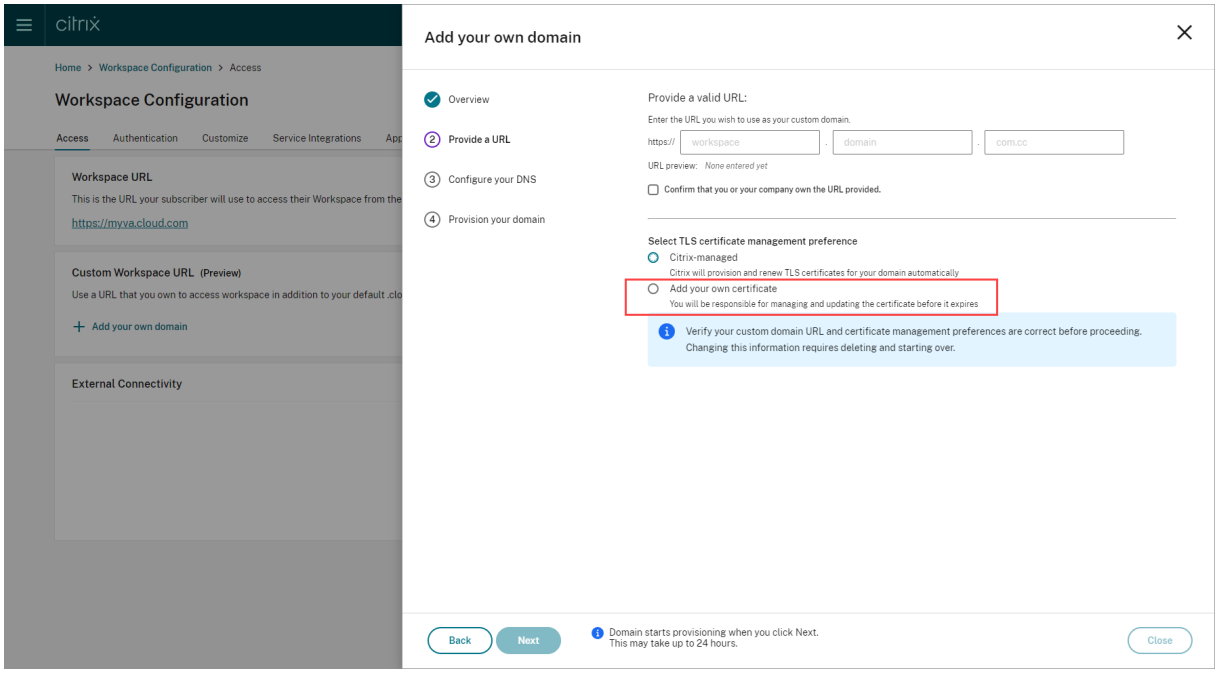
Aug 2023

Ajouter votre propre certificat TLS pour un domaine personnalisé (Technical Preview)

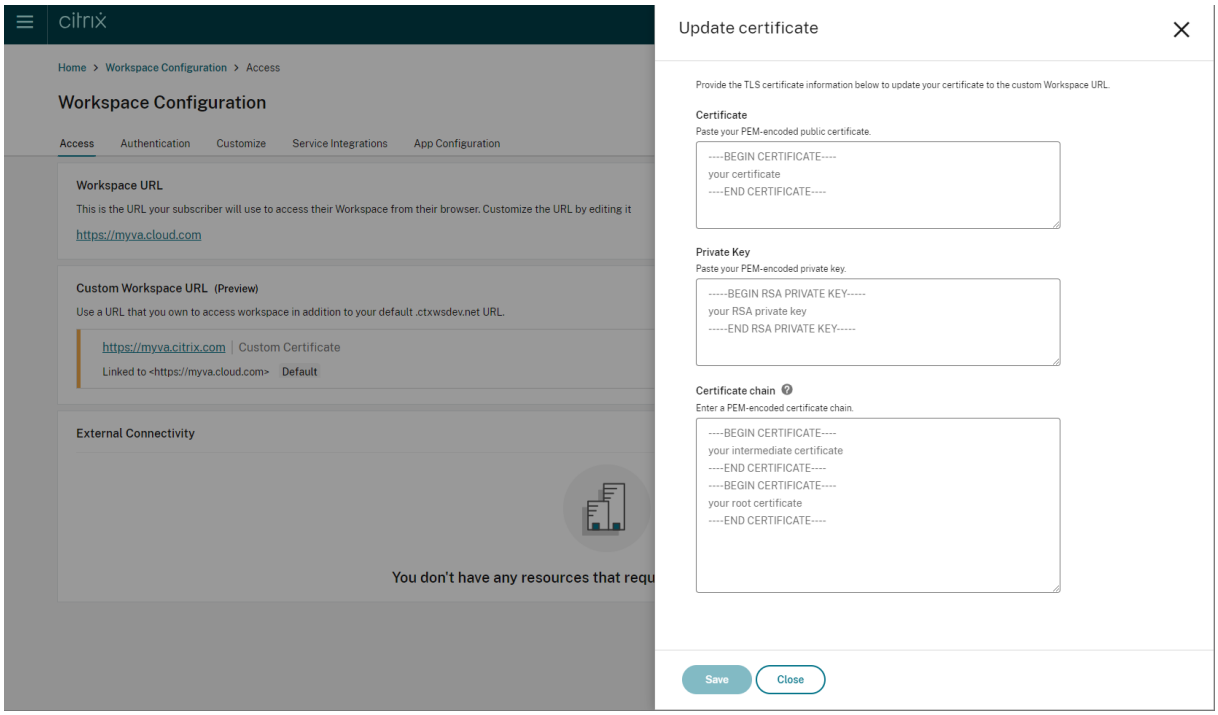
Vous pouvez désormais télécharger votre propre certificat TLS à des fins d'authentification lors de la configuration d'une URL d'espace de travail personnalisée. Avant de télécharger un certificat, assurez-vous qu'il remplit les conditions suivantes.

- Il doit être codé PEM.
- Il devrait rester valide pendant encore au moins 30 jours.
- Il doit être utilisé exclusivement pour l'URL personnalisée de l'espace de travail, les certificats génériques ne sont pas acceptables.
- Le nom courant du certificat doit correspondre au domaine personnalisé.
- Les SAN figurant sur le certificat doivent être destinés au domaine personnalisé. Aucun réseau SAN supplémentaire n'est autorisé.
- La durée de validité du certificat ne doit pas dépasser 10 ans.

Pour ajouter votre certificat, accédez à la page **Fournir une URL** et sélectionnez l'option Ajouter votre propre certificat sous **Sélectionnez votre préférence de gestion des certificats TLS**.



Vous pouvez ensuite ajouter votre certificat sur la page **Ajouter votre propre certificat**.



Pour plus d'informations, consultez Ajout d'un domaine personnalisé.

> **Remarque :**
>
> Vous pouvez nous faire part de vos commentaires concernant cette fonctionnalité Technical Preview à l'aide du formulaire Podio ci-joint.

Mai 2023

Configurer un domaine personnalisé (version préliminaire). Vous pouvez configurer un domaine personnalisé pour votre espace de travail, ce qui vous permet d'utiliser le domaine de votre choix pour accéder à votre magasin Citrix Workspace. Vous pouvez ensuite utiliser ce domaine à la place du domaine cloud.com qui vous a été attribué pour y accéder à la fois depuis un navigateur Web et des applications Citrix Workspace. Pour plus d'informations, consultez Configurer un domaine personnalisé (version préliminaire).

Mars 2023

Paramètres de délai d'inactivité supplémentaires :. Vous pouvez désormais activer des paramètres de délai d'inactivité supplémentaires pour les utilisateurs de l'application Workspace sur bureaux et mobiles. Pour plus d'informations, consultez Personnaliser les stratégies de sécurité et de confidentialité.

Décembre 2022

Option supplémentaire de configuration d'envoi d'une annonce personnalisée :. Vous pouvez désormais définir l'emplacement de la page en haut ou en bas lorsque vous configurez **Envoyer annonce personnalisée**. Pour plus d'informations, consultez Personnaliser les stratégies de sécurité et de confidentialité.

Prise en charge du Chinois traditionnel. Citrix Workspace est désormais disponible en Chinois traditionnel.

Octobre 2022

Prise en charge du coréen. Citrix Workspace est désormais disponible en coréen.

Prise en charge de la personnalisation des paramètres de l'application Citrix Workspace. Les administrateurs peuvent désormais configurer les paramètres de l'application Citrix Workspace pour les plates-formes iOS, Android, HTML5, Mac et Windows à l'aide de Global App Configuration Service.

Août 2022

Amélioration de l'expérience de lancement de Workspace. Lorsqu'un utilisateur lance son espace de travail sur le Web ou un navigateur, une notification indiquant l'état du lancement est affichée. Si l'utilisateur tente de fermer le navigateur alors qu'un lancement est en cours, il est invité à confirmer et est informé qu'une session est en cours de lancement. Pour plus d'informations, consultez la section Découvrez Citrix Workspace.

Juin 2022

Prise en charge de la continuité du service avec Safari. Les extensions Web Citrix Workspace mettent la continuité du service à la disposition des utilisateurs qui accèdent à leurs applications et bureaux via un navigateur. Pour plus d'informations, consultez Continuité du service dans le navigateur.

Mai 2022

Nouvelle option de configuration pour le fournisseur d'identité fédéré : activez ou désactivez votre fournisseur d'identité fédéré pour demander à vos abonnés de s'authentifier lorsqu'ils se connectent à Workspace. Pour plus d'informations, consultez Personnaliser les interactions de l'espace de travail.

Période de réauthentification de l'application Workspace (disponibilité générale) : les périodes de réauthentification permettent aux abonnés de rester connectés à Workspace sans être invités à se connecter chaque fois qu'ils accèdent à leur espace de travail. Lorsque vous vous connectez via l'application Workspace, les abonnés consentent à rester connectés. Les abonnés restent connectés pendant la période de réauthentification tant qu'ils utilisent leurs applications et leurs bureaux. Pour plus d'informations sur cette fonctionnalité, consultez Définir une période de réauthentification pour l'application Citrix Workspace.

Prise en charge de la continuité du service sur iOS : la continuité du service est désormais prise en charge pour l'application Citrix Workspace pour iOS en disponibilité générale. Pour plus d'informations, consultez Continuité du service.

Nouveaux codes d'erreur pour la continuité de service : de nouveaux codes d'erreur sont désormais disponibles pour faciliter le dépannage des échecs de connexion de la continuité du service. Pour plus d'informations, consultez Continuité du service.

Mars 2022

Prise en charge de la continuité du service sur Android et iOS : La continuité du service est désormais prise en charge pour l'application Citrix Workspace pour Android en disponibilité générale et l'application Citrix Workspace pour iOS en version Technical Preview. Pour plus d'informations, consultez Continuité du service.

Février 2022

Prise en charge de la continuité du service avec l'application Citrix Workspace pour Android (disponibilité générale) et l'application Citrix Workspace pour iOS (version Technical Preview) :

la continuité du service permet aux utilisateurs de se connecter à leurs applications et bureaux virtuels, même en cas de panne. Il est désormais prise en charge pour l'application Citrix Workspace pour Android en disponibilité générale et l'application Citrix Workspace pour iOS en version Technical Preview. Pour plus d'informations, consultez Continuité du service.

Envoyer annonce personnalisée et stratégie de connexion personnalisée : deux nouvelles fonctionnalités sont désormais disponibles pour tous les clients. Ces fonctionnalités permettent aux administrateurs de Workspace d'afficher leur propre bannière persistante après la connexion ainsi qu'un message personnalisé de pré-connexion ou un contrat de licence dans l'application Citrix Workspace. Pour plus d'informations, consultez Personnaliser les stratégies de sécurité et de confidentialité.

Décembre 2021

Suppression de l'écran de connexion partagé par défaut pour les employés et les utilisateurs clients de Citrix Content Collaboration : Citrix Workspace vous permet désormais d'activer un flux de connexion unique pour les utilisateurs clients et employés. Pour plus d'informations, consultez Créer un flux de connexion utilisateur unifié.

Prise en charge de la continuité du service du navigateur avec l'application Citrix Workspace pour Mac : les extensions Web Citrix Workspace mettent la continuité du service à la disposition des utilisateurs qui accèdent à leurs applications et bureaux via un navigateur. Cette fonctionnalité est désormais prise en charge sur les appareils exécutant l'application Citrix Workspace pour Mac. Pour plus d'informations, consultez Continuité du service.

Novembre 2021

Thèmes basés sur des stratégies : vous pouvez créer et hiérarchiser les thèmes de l'espace de travail, et ajouter chaque thème à différents groupes d'utilisateurs dans **Configuration de l'espace de travail**. Pour plus d'informations, consultez Personnaliser l'apparence des espaces de travail.

Octobre 2021

Langues prises en charge pour la signature électronique : la fonctionnalité de signature électronique permet désormais de prendre en charge l'italien et le portugais brésilien, en plus des langues suivantes : allemand, français, espagnol, japonais, néerlandais et chinois simplifié. Pour plus d'informations, consultez Prise en charge multilingue de RightSignature.

Prise en charge de FAS pour plusieurs emplacements de ressources (disponibilité générale) : Citrix Workspace prend désormais en charge la fourniture d'authentification unique aux applications et bureaux virtuels sur plusieurs emplacements de ressources. En outre, les serveurs FAS situés dans

un emplacement de ressources peuvent être désignés comme serveurs principaux ou secondaires pour fournir une fonction de basculement aux serveurs FAS situés dans d'autres emplacements de ressources. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Septembre 2021

Compatibilité de l'application Citrix Workspace pour HTML5 avec Citrix Workspace: l'application Citrix Workspace pour HTML5 offre l'expérience Citrix Workspace dans les navigateurs sans aucune installation sur l'appareil. Pour plus d'informations sur l'application Citrix Workspace pour HTML5, y compris les nouvelles fonctionnalités, consultez la documentation produit de l'application Citrix Workspace pour HTML5 .

Prise en charge de la continuité du service du navigateur (disponibilité générale) : les extensions Web Citrix Workspace mettent la continuité du service à la disposition des utilisateurs qui accèdent à leurs applications et bureaux via un navigateur. Cette fonctionnalité est destinée à Google Chrome et Microsoft Edge sur les appareils Windows. Pour plus d'informations, consultez Continuité du service dans le navigateur.

Juillet 2021

Stratégie de contrat de licence d'abonné personnalisée : vous pouvez présenter aux abonnés une stratégie de contrat d'utilisation personnalisée à lire et à accepter avant de se connecter à leur espace de travail. Pour plus d'informations sur cette fonctionnalité, consultez Configurer une stratégie de connexion.

Période de réauthentification de l'application Workspace (version Technical Preview) : les périodes de réauthentification permettent aux abonnés de rester connectés à Workspace sans être invités à se connecter chaque fois qu'ils accèdent à leur espace de travail. Lorsque vous vous connectez via l'application Workspace, les abonnés consentent à rester connectés. Les abonnés restent connectés pendant la période de réauthentification tant qu'ils utilisent leurs applications et leurs bureaux. Pour plus d'informations sur cette fonctionnalité en version Technical Preview, consultez Définir une période de réauthentification pour l'application Citrix Workspace.

Configuration de l'emplacement réseau via Citrix Cloud : vous pouvez désormais configurer des emplacements réseau via la console de gestion Citrix Cloud en plus du script PowerShell fourni par Citrix. Pour plus d'informations sur cette fonctionnalité, consultez Optimiser la connectivité aux espaces de travail avec Direct Workload Connection.

Juin 2021

Prise en charge de FAS pour plusieurs emplacements de ressources (version Technical Preview) : Citrix Workspace prend désormais en charge la fourniture d'authentification unique aux applications et bureaux virtuels sur plusieurs emplacements de ressources. Les serveurs FAS situés dans un emplacement de ressources peuvent être désignés comme serveurs principaux ou secondaires pour fournir une fonction de basculement aux serveurs FAS situés dans d'autres emplacements de ressources. Pour plus d'informations sur cette fonctionnalité en version Technical Preview, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Prise en charge de la continuité du service du navigateur (version Technical Preview) : les extensions Web Citrix Workspace mettent la continuité du service à la disposition des utilisateurs qui accèdent à leurs applications et bureaux via un navigateur. Cette version Technical Preview est destinée à Google Chrome et Microsoft Edge sur les appareils Windows. Pour plus d'informations, consultez Continuité du service dans le navigateur.

Continuité du service (disponibilité générale) : la continuité du service permet aux utilisateurs de se connecter à leurs applications et bureaux virtuels, même en cas de panne dans les composants Citrix Cloud ou dans les clouds publics et privés. Pour plus d'informations, consultez Continuité du service.

Application Citrix RightSignature disponible : profitez de cette application Citrix, une solution de signature électronique fournie avec Workspace Premium et Premium Plus, pour demander des signatures électroniques sur des documents sur n'importe quel appareil via Citrix Workspace. Pour plus d'informations, consultez Configurer l'application Citrix RightSignature.

May 2021

Thèmes personnalisés (version Technical Preview) : la personnalisation de l'apparence de Workspace pour les abonnés prend désormais en charge des thèmes personnalisés que vous pouvez affecter à différents groupes d'utilisateurs. Créez, personnalisez et hiérarchisez des thèmes afin que les abonnés de ces groupes d'utilisateurs voient le thème d'espace de travail approprié lorsqu'ils se connectent. Pour plus d'informations, consultez Personnaliser l'apparence des espaces de travail.

Langues prises en charge pour la signature électronique : la fonctionnalité de signature électronique permet désormais de prendre en charge les langues suivantes : allemand, français, espagnol, japonais, néerlandais et chinois simplifié. Pour plus d'informations, consultez Prise en charge multilingue de RightSignature.

Février 2021

Modifications du mot de passe du compte : les abonnés peuvent modifier leur mot de passe de domaine à partir de Citrix Workspace. Les administrateurs peuvent également fournir des conseils de mot de passe aux abonnés afin de créer des mots de passe complexes valides conformément à la stratégie de mot de passe de leur organisation. Pour plus d'informations, consultez Autoriser les abonnés à modifier le mot de passe de compte.

Décembre 2020

Continuité du service (version Technical Preview) : la continuité du service permet aux utilisateurs de se connecter à DaaS, même en cas de panne dans les composants Citrix Cloud ou dans les clouds publics et privés. Pour plus d'informations, consultez Continuité du service.

Octobre 2020

Conformité FedRAMP : Citrix Workspace est conforme au programme FedRAMP lorsqu'il est déployé dans Citrix Cloud Government. FedRAMP est un programme qui favorise l'adoption de normes de sécurité pour les services cloud utilisés par les organisations gouvernementales américaines. Les organisations gouvernementales américaines qui nécessitent des services cloud FedRAMP Ready peuvent désormais utiliser Citrix Workspace et Citrix DaaS pour fournir des applications et des bureaux DaaS. Pour plus d'informations, consultez Citrix Cloud Government.

Mai 2020

Guide de mise en route de Citrix Workspace : Citrix Workspace inclut désormais une procédure détaillée pour vous aider à fournir rapidement des espaces de travail à vos utilisateurs. La procédure détaillée vous guide dans la console Citrix Cloud afin que vous puissiez configurer un fournisseur d'identité, ajouter des administrateurs et activer l'authentification et les services de l'espace de travail. Pour obtenir une vue d'ensemble des tâches que vous allez effectuer et accéder rapidement aux instructions dont vous avez besoin, consultez la section Mise en route de Citrix Workspace.

Décembre 2019

Service de localisation réseau : vous pouvez désormais vous assurer que les utilisateurs qui lancent des applications et des bureaux dans Workspace à partir du réseau d'entreprise sont acheminés directement vers leurs VDA. Cela permet de contourner la passerelle et d'accélérer les sessions DaaS. Pour plus d'informations sur ce service et les instructions de configuration, consultez Optimiser la connectivité aux espaces de travail avec le service de localisation réseau.

Améliorations apportées aux applications récentes et préférées : les applications récentes et préférées sont chargées en premier dans Workspace afin que les utilisateurs puissent lancer immédiatement leurs applications et bureaux utilisés fréquemment.

Nouveautés dans l'interface utilisateur de Workspace

November 28, 2023

Les sections suivantes répertorient les nouvelles fonctionnalités des versions actuelles et antérieures de l'interface utilisateur de Workspace.

> **Remarque :**
>
> - Pour plus d'informations sur la nouvelle interface, consultez la section Nouvelle interface utilisateur de Workspace.
> - Pour plus d'informations sur le Gestionnaire d'activités, consultez la section Gestionnaire d'activités.

Nouveautés de la version 23.46

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes connus

Il n'y a aucun nouveau problème connu.

Versions précédentes

Cette section fournit des informations sur les nouvelles fonctionnalités et les problèmes résolus dans les versions précédentes que nous prenons en charge.

23.45

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

- L'indexation de Google Search a été supprimée de Citrix Web afin d'empêcher l'affichage des URL internes dans les résultats de recherche de Google. Toutefois, si vos URL ont déjà été indexées par Google, vous devez prendre des mesures pour les supprimer. Pour plus d'informations, consultez Supprimer de Google une page hébergée sur votre site.

23.44

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.43

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.42

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.41

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

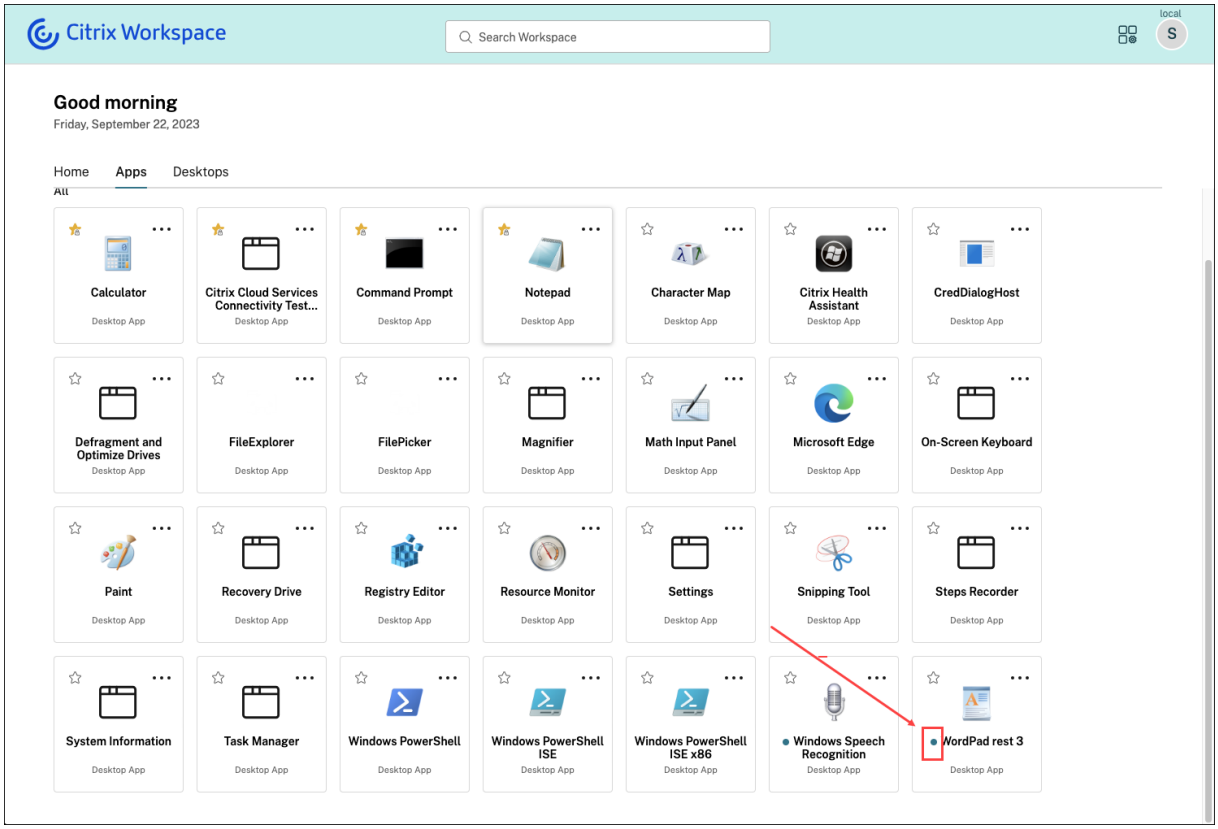
Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.40

Nouveautés

Découverte simplifiée de nouvelles applications Les utilisateurs finaux peuvent désormais repérer facilement les applications récemment ajoutées, ce qui leur permet d'explorer et d'utiliser plus facilement les dernières applications. Lorsqu'un administrateur propose une nouvelle application à un utilisateur final, celle-ci est mise en évidence dans l'espace de travail de l'utilisateur final et un point vert apparaît sur la vignette de l'application pour la première fois.



Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.39

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.38

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.37

Nouveautés

Nouvelle interface utilisateur de Workspace - Disponibilité générale La nouvelle interface utilisateur de Workspace est désormais en disponibilité générale. Elle introduit de nouvelles fonctionnalités d'interface utilisateur avec une apparence moderne pour une vue plus claire. Les améliorations apportées à l'interface utilisateur s'appliquent au Web, aux ordinateurs de bureau et aux appareils mobiles. Les administrateurs peuvent l'activer pour leurs utilisateurs depuis **Configuration de l'espace de travail** > **Personnaliser** > **Fonctionnalités**. Pour plus d'informations, consultez la section Nouvelle interface utilisateur de Workspace.

> **Remarque :**
>
> Par défaut, le nouveau bouton d'interface utilisateur sera désactivé pendant les 6 prochains mois, sauf si les administrateurs l'activent. Après 6 mois, la nouvelle interface utilisateur sera activée par défaut pour tous les utilisateurs et l'expérience utilisateur actuelle sera obsolète. Les administrateurs doivent faire passer leurs utilisateurs à la nouvelle interface utilisateur au cours des 6 prochains mois.

Gestionnaire d'activités - Disponibilité générale La fonctionnalité Gestionnaire d'activités est désormais en disponibilité générale sur la nouvelle interface utilisateur pour le cloud. Le Gestionnaire d'activités est une fonctionnalité simple mais puissante qui permet aux utilisateurs de gérer efficacement leurs ressources. Il améliore la productivité en facilitant les actions rapides sur les applications et les bureaux actifs et déconnectés depuis n'importe quel appareil. Les administrateurs peuvent activer cette fonctionnalité pour leurs utilisateurs en accédant à **Configuration de l'espace de travail** > **Personnaliser** > **Fonctionnalités** > **Gestionnaire d'activités**. Pour plus d'informations, consultez Activer le Gestionnaire d'activités.

Une fois la fonction activée, les applications et les bureaux actifs ou déconnectés s'affichent dans le panneau du Gestionnaire d'activités. Les utilisateurs peuvent cliquer sur l'icône des points de suspension (...) pour effectuer des actions rapides.

Les actions suivantes peuvent être effectuées pour les applications et les bureaux actifs.

- **Déconnecter** : la session à distance est déconnectée, mais les applications et les bureaux sont actifs en arrière-plan.
- **Fermer la session** : ferme la session en cours. Toutes les applications des sessions sont fermées et tous les fichiers non enregistrés sont perdus.
- **Arrêter** : ferme les bureaux déconnectés.
- **Forcer la fermeture** : force la mise hors tension du bureau en cas de problème technique.
- **Redémarrer** : arrête le bureau et le redémarre.

Le Gestionnaire d'activités permet également aux utilisateurs d'interagir avec leurs applications et bureaux déconnectés. Assurez-vous d'avoir effectué la mise à niveau vers la dernière version de DDC (115). Pour plus d'informations, consultez la section Applications et bureaux déconnectés.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

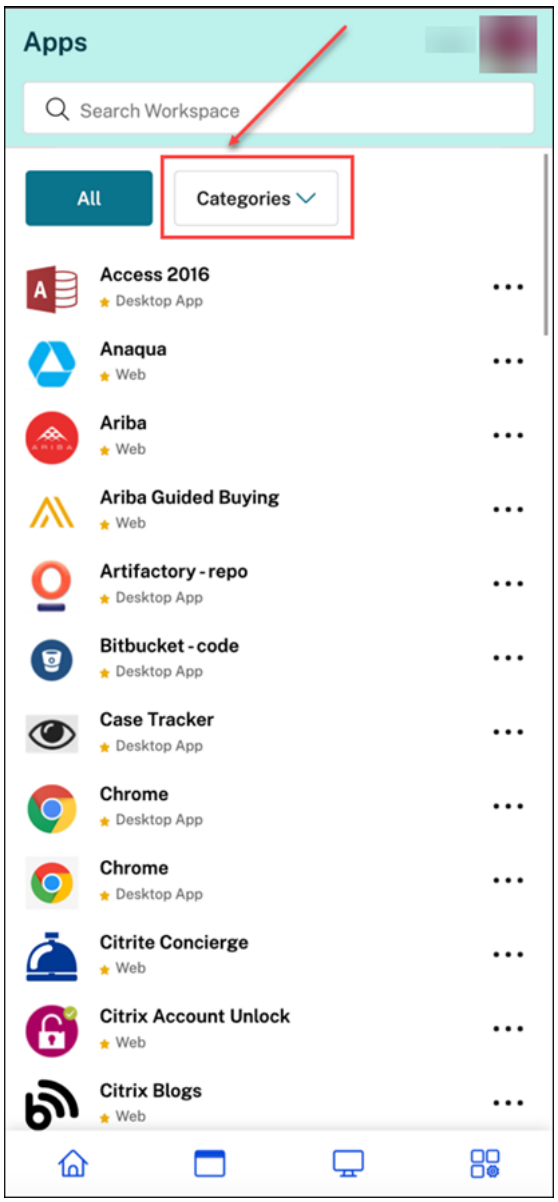
Problèmes connus

- Le panneau du Gestionnaire d'activités affiche les sessions actives dans tous les magasins auxquels l'utilisateur est actuellement connecté.
- Les opérations du Gestionnaire d'activités telles que Fermer la session, Déconnecter, etc. ne sont pas prises en charge pour les applications pour lesquelles la stratégie de protection des applications est activée.

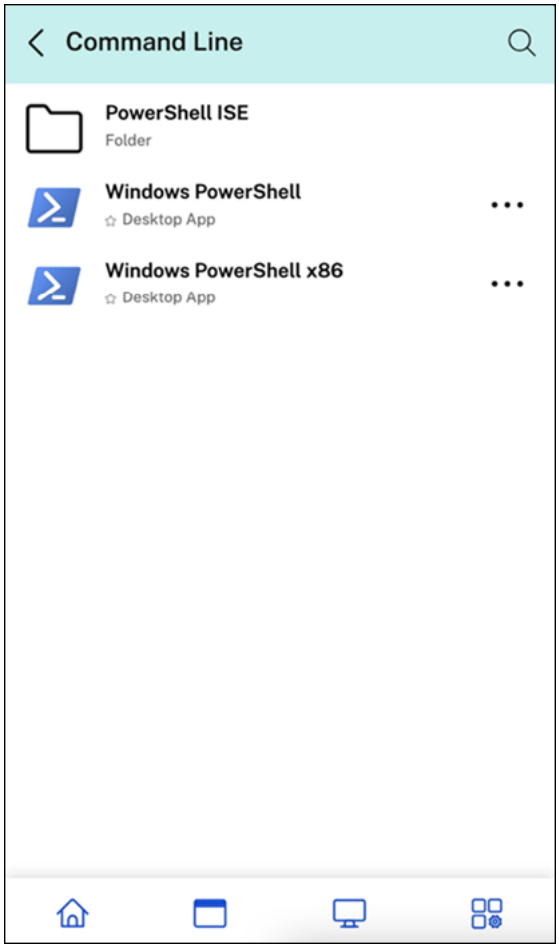
23.36

Nouveautés

Afficher les sous-catégories d'applications sur les plates-formes mobiles Les utilisateurs peuvent désormais afficher leurs applications organisées en catégories et sous-catégories sur les appareils Android et iOS, ce qui leur permet d'y accéder facilement et de bénéficier d'une expérience de navigation intuitive. Pour afficher les catégories, accédez à l'onglet Applications et cliquez sur le menu déroulant Catégories.

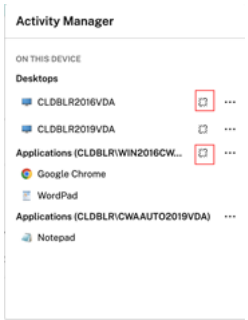


Sélectionnez la catégorie appropriée. Une liste des sous-catégories et d'applications disponibles s'affiche en fonction de la configuration effectuée par l'administrateur. Les sous-catégories sont affichées sous forme de dossiers qui peuvent contenir d'autres sous-dossiers ou applications conformément à la configuration effectuée par l'administrateur. Pour plus d'informations, voir Ajouter un chemin de dossier



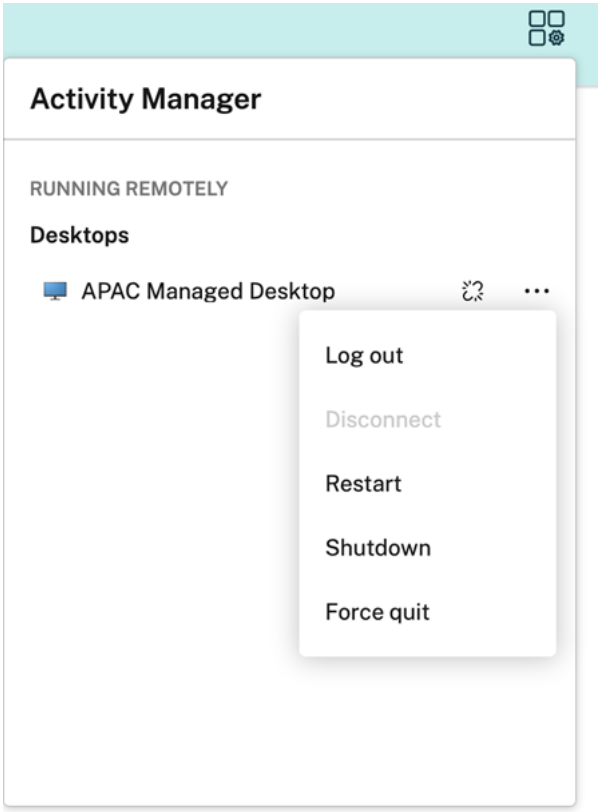
Gérer les sessions déconnectées sur le Gestionnaire d'activités depuis n'importe quel appareil

Le Gestionnaire d'activités permet désormais aux utilisateurs d'afficher les applications et les bureaux qui s'exécutent en mode déconnecté, localement ou à distance, et d'intervenir sur ceux-ci. Les sessions peuvent être gérées à partir d'appareils mobiles ou de bureau, ce qui permet aux utilisateurs d'intervenir lorsqu'ils sont en déplacement. L'intervention sur les sessions déconnectées, telles que la fermeture de session ou l'arrêt, favorise une utilisation optimisée des ressources et réduit la consommation d'énergie.



- Les applications et les bureaux déconnectés sont affichés sur le panneau du Gestionnaire d'

activités et sont marqués d'une icône de déconnexion.
- Les applications déconnectées sont regroupées sous les sessions respectives qui sont marquées d'une icône de déconnexion.



Les utilisateurs peuvent effectuer les actions suivantes sur leurs bureaux déconnectés en cliquant sur le bouton représentant des points de suspension :

- **Fermer la session** : utilisez cette option pour vous déconnecter de votre bureau déconnecté. Toutes les applications de la session sont fermées et tous les fichiers non enregistrés sont perdus.
- **Arrêter** : utilisez cette option pour fermer vos bureaux déconnectés.
- **Forcer la fermeture** : utilisez cette option pour forcer la mise hors tension de vos bureaux déconnectés en cas de problème technique.
- **Redémarrer** : utilisez cette option pour arrêter et redémarrer le bureau déconnecté.

Pour plus d'informations, consultez la section Applications et bureaux déconnectés dans le Gestionnaire d'activités.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.35

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.34

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

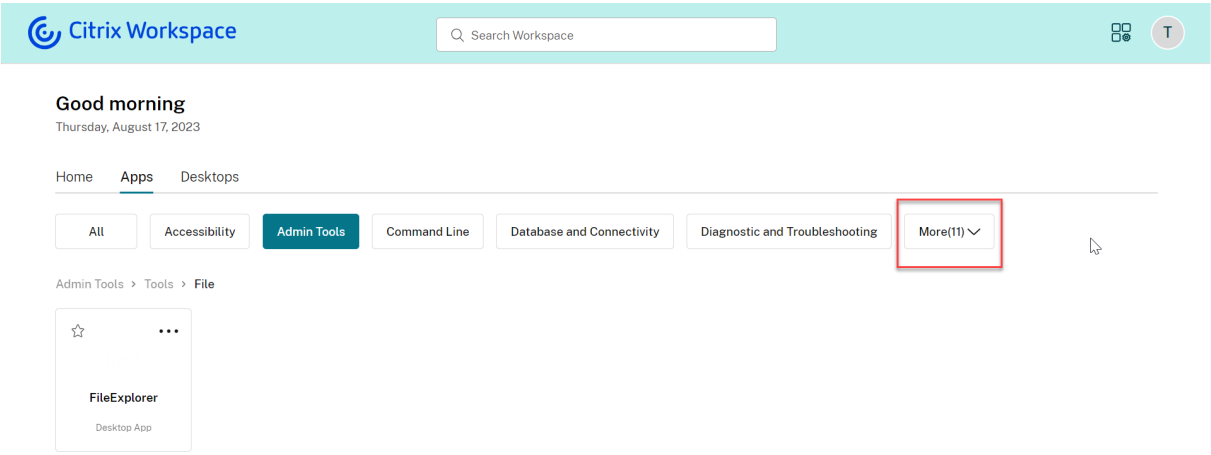
Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.33

Nouveautés

Expérience utilisateur améliorée grâce à la catégorisation des applications Les utilisateurs finaux peuvent consulter leurs applications organisées en catégories et sous-catégories sur l'interface utilisateur de Workspace. Si la catégorisation comporte plus de deux niveaux, les utilisateurs finaux verront leurs applications organisées dans une structure de dossiers. Les fils de navigation sont visibles par les utilisateurs.
Lorsque le nombre de catégories principales créées par les administrateurs dépasse l'espace

disponible sur l'écran de l'utilisateur, l'interface utilisateur s'ajuste en fonction de la taille de l'écran et déplace les catégories de manière dynamique dans le menu déroulant **Plus**.



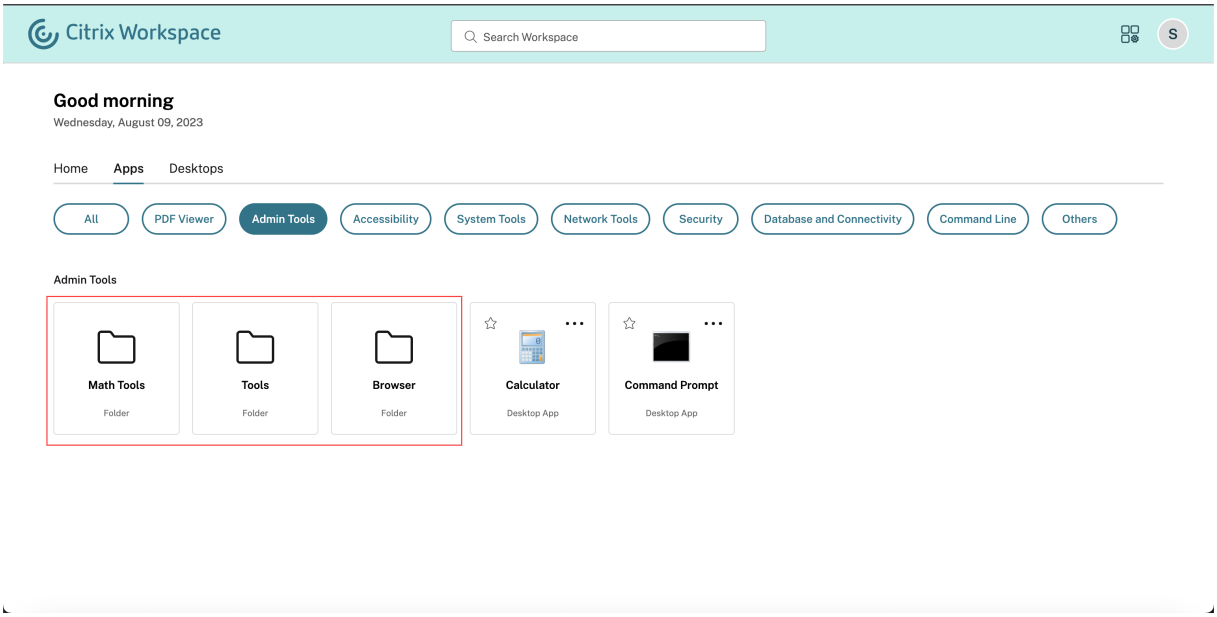
Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.32

Nouveautés

Catégorisation des applications pour un accès facile Les administrateurs peuvent proposer des applications organisées en catégories et sous-catégories, offrant ainsi une expérience de navigation agréable à leurs utilisateurs finaux. À partir du deuxième niveau de catégorisation, les utilisateurs finaux verront une structure de dossiers. La structure organisée en plusieurs niveaux permet une expérience optimisée et sans encombrement qui contribue à améliorer la satisfaction globale des utilisateurs. Pour plus d'informations sur la création de dossiers et de sous-dossiers, voir Créer des groupes de mise à disposition.



Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.31

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.30

Nouveautés

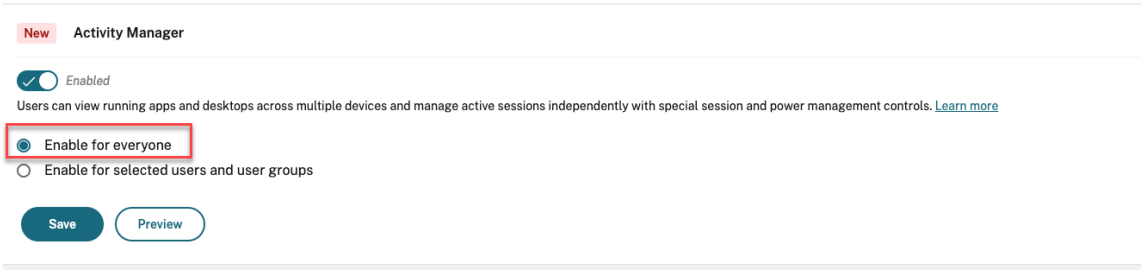
Gérer le Gestionnaire d'activités En tant qu'administrateur, vous pouvez désormais activer ou désactiver la fonctionnalité Gestionnaire d'activités pour vos utilisateurs finaux. Conformément aux stratégies de votre organisation, vous pouvez activer la fonctionnalité pour tout le monde ou uniquement certains utilisateurs et groupes d'utilisateurs. Lorsqu'il est activé, le panneau Gestionnaire d'

activités permet à vos utilisateurs finaux de visualiser et d'interagir avec leurs applications et bureaux actifs. Pour plus d'informations, consultez Gestionnaire d'activités.

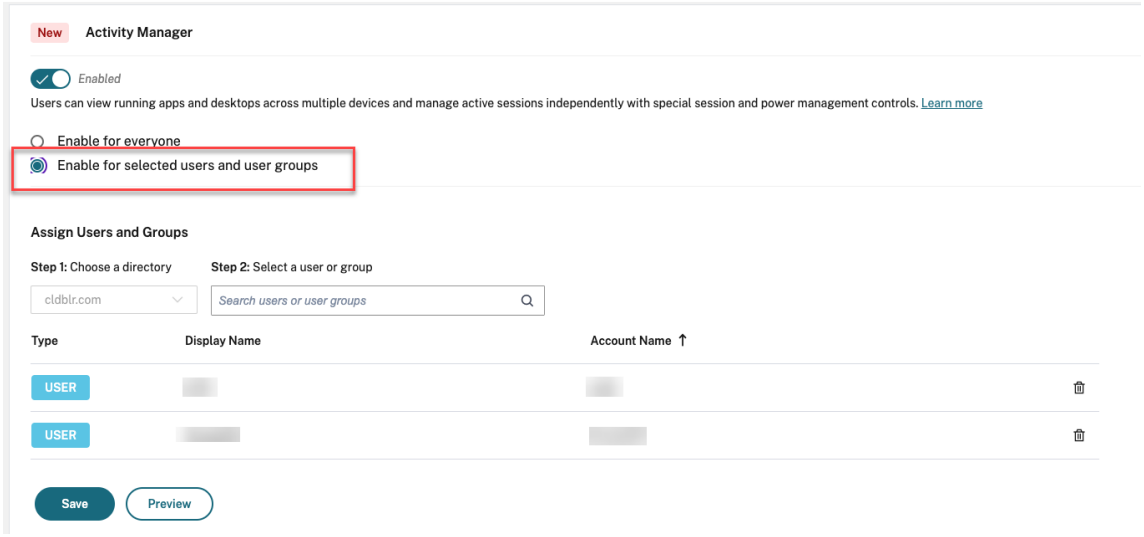
> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que pour les applications et les bureaux virtuels. Elle ne s'applique pas aux applications Web et SaaS.

Pour activer le Gestionnaire d'activités, procédez comme suit :

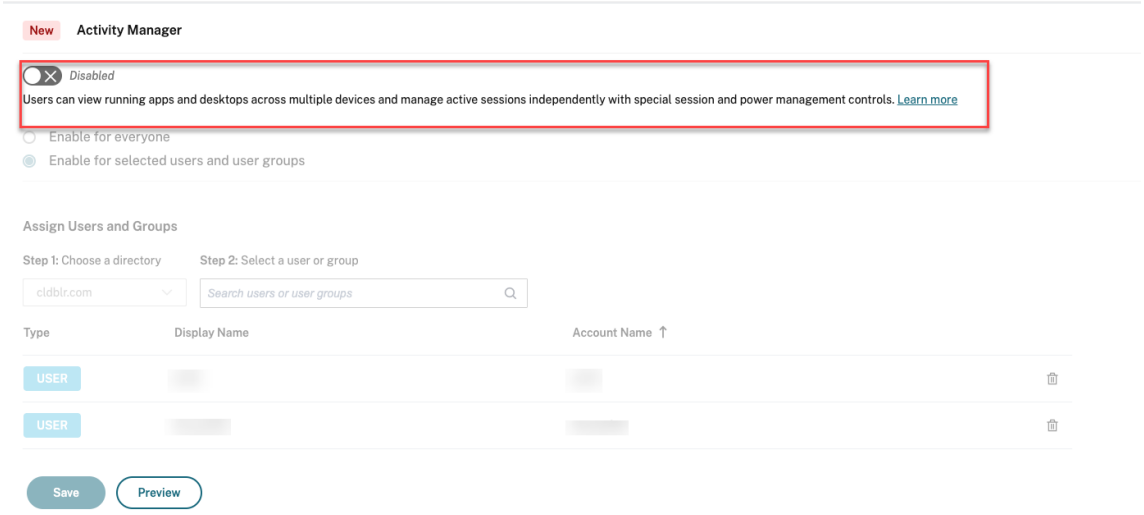
1. Sur la console d'administration, accédez à **Configuration de l'espace de travail** > **Personnaliser** > **Fonctionnalités**.
2. Dans la section Gestionnaire d'activités, activez le bouton bascule pour activer le Gestionnaire d'activités.
3. Vous pouvez ensuite personnaliser les autorisations d'accès comme suit.
    - Pour activer le Gestionnaire d'activités pour tous les utilisateurs finaux, sélectionnez **Activer pour tout le monde**.



    - Pour activer le gestionnaire d'activités pour des utilisateurs et des groupes d'utilisateurs sélectionnés, sélectionnez **Activer pour des utilisateurs et des groupes d'utilisateurs sélectionnés**. Vous pouvez ensuite sélectionner le répertoire auquel les utilisateurs ou les groupes d'utilisateurs appartiennent. Une fois le répertoire approprié sélectionné, vous pouvez voir les utilisateurs et les groupes d'utilisateurs appropriés.



- Pour désactiver le Gestionnaire d'activités pour tout le monde, désactivez ce bouton bascule.



4. Cliquez sur **Save**.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.29

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.28

Nouveautés

Annonce de fin de prise en charge d'Internet Explorer La version 23.26 de l'interface utilisateur de Citrix Workspace est disponible sur Internet Explorer jusqu'à la dernière semaine de 2023. Citrix ne prend pas en charge les nouvelles fonctionnalités, les corrections de bogues ou les correctifs de sécurité postérieurs à la version 23.26. En outre, les administrateurs reçoivent une notification les invitant à effectuer une mise à niveau vers les navigateurs et versions LTSR pris en charge (LTSR2203 ou version ultérieure).

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.27

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

- Avec ce correctif, la gestion des limites d'erreur et des erreurs au niveau des composants a été implémentée. [WSUI-7423]
- La bannière hors ligne est réduite lorsque vous cliquez sur l'icône des points de suspension. [WSUI-7797]

23.26

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

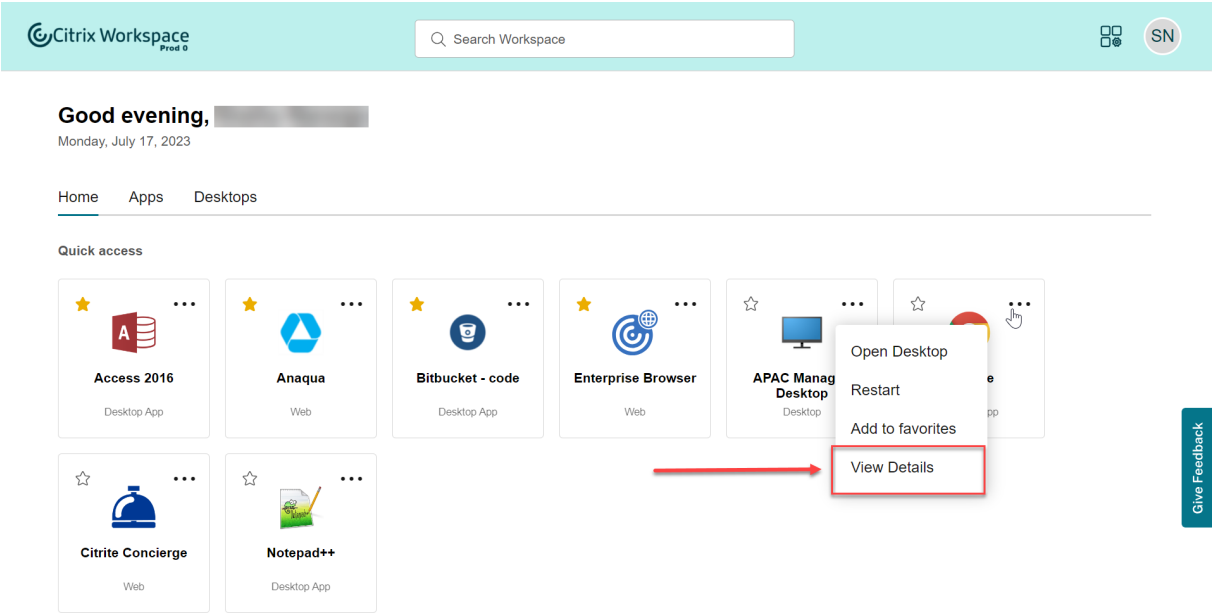
Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.25

Nouveautés

Afficher la description des applications et des bureaux Les utilisateurs peuvent désormais consulter la description des applications et des bureaux fournie par les administrateurs. Ces descriptions aident à comprendre les fonctionnalités prévues d'une application ou d'un bureau. Elles sont particulièrement utiles dans le cas où plusieurs applications portent le même nom mais dont la configuration, l'emplacement, l'environnement, etc. sont différents.
Pour afficher la description d'une application ou d'un bureau, cliquez sur les points de suspension de la vignette correspondante, puis cliquez sur **Afficher les détails**.



Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.24

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.23

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

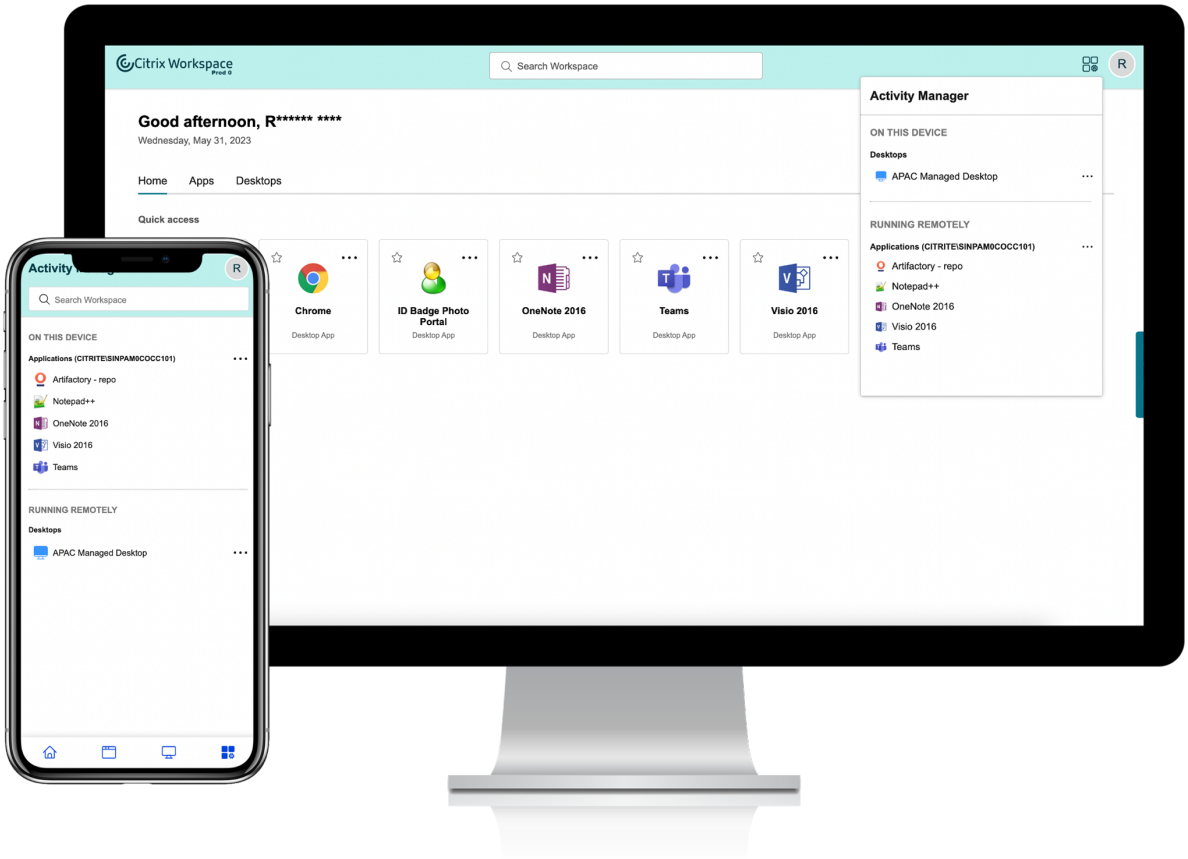
23.22

Nouveautés

Présentation du Gestionnaire d'activités Vous pouvez maintenant gérer et intervenir rapidement sur les applications et les bureaux actifs de n'importe quel appareil à partir d'un seul volet de l'interface utilisateur de Workspace. Toutes les applications et tous les bureaux actifs sont regroupés dans la session que vous utilisez actuellement.

L'icône du Gestionnaire d'activités apparaît dans la fenêtre de l'interface utilisateur de Workspace à gauche de l'icône du profil. Lorsque vous cliquez sur l'icône, les informations suivantes s'affichent :

- Liste des applications et des bureaux démarrés à partir de l'appareil que vous utilisez sous **Sur cet appareil**.
- Liste des applications et des bureaux actifs sur d'autres appareils sous **Exécuté à distance**.



Pour plus d'informations, consultez Gestionnaire d'activités.

> **Remarque :**
>
> Si vous ne parvenez pas à voir clairement l'icône du Gestionnaire d'activités, pensez à modifier la couleur sélectionnée dans le paramètre **Texte de bannière et couleur d'icône**. L'icône peut ne pas être clairement visible en raison du faible contraste entre la bannière et l'icône du Gestionnaire d'activités. Pour plus d'informations, consultez la section Configurer des thèmes personnalisés.

Problèmes connus

- Si une session est déconnectée, les utilisateurs ne pourront pas la fermer. Les sessions déconnectées ne sont pas affichées dans le panneau du Gestionnaire d'activités.
- Sur l'application Citrix Workspace pour Mac, la liste des applications et des bureaux actifs affichée dans le panneau Gestionnaire d'activités répertorie les sessions actives de tous les magasins.

23.15

Nouveautés

Nouvelle interface utilisateur de Workspace L'application Citrix Workspace introduit de nouvelles fonctionnalités d'interface utilisateur avec une apparence moderne pour une vue plus claire. Les améliorations apportées à l'interface utilisateur s'appliquent au Web, aux ordinateurs de bureau et aux appareils mobiles.

Expérience de première utilisation améliorée Lorsque vous lancez l'application Citrix Workspace ou Citrix téléchargée depuis un navigateur pour la première fois, un écran répertoriant les applications pertinentes s'affiche. Ces applications sont choisies par l'administrateur et vous pouvez les ajouter en tant que favoris en un seul clic.

Expérience de recherche améliorée La fonctionnalité de **recherche** améliorée vous permet d'obtenir des résultats plus rapidement dans les moteurs de recherche. L'option **Recherche** vous permet d'effectuer une recherche rapide et intuitive depuis l'application Workspace.

Tâches liées à l'administration

En tant qu'administrateur, vous pouvez personnaliser l'expérience utilisateur de l'application Workspace pour vos abonnés. Pour plus d'informations, consultez les sections suivantes.

- Activer la nouvelle expérience Workspace pour les utilisateurs
- Activer ou désactiver l'écran d'accueil pour les utilisateurs

Nouveautés de Global App Configuration Service

November 28, 2023

Les sections suivantes répertorient les nouvelles fonctionnalités des versions actuelles et antérieures de Global App Configuration Service.

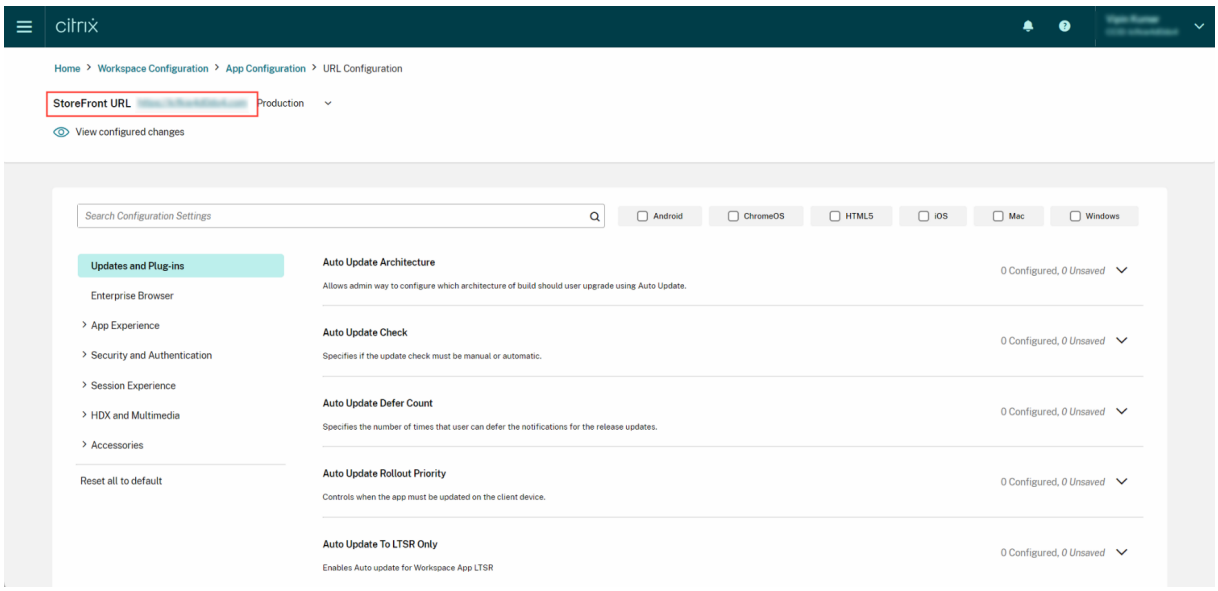
Oct 30, 2023

Configurer les paramètres des magasins locaux

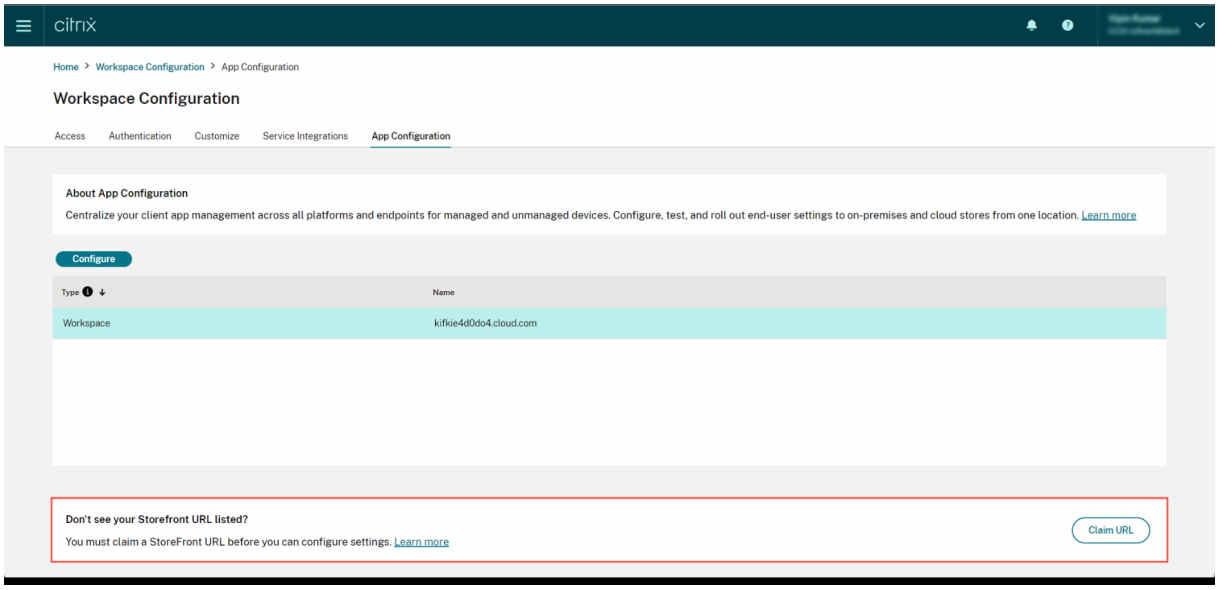
Vous pouvez désormais utiliser l'interface Global App Configuration Service pour configurer les paramètres des magasins sur site. Connectez-vous à votre compte Citrix Cloud et accédez à **Configuration de l'espace de travail > Configuration de l'application**.

> **Remarque :**
>
> Si vous ne possédez pas encore de compte Citrix Cloud, rendez-vous sur la page Citrix Onboarding pour en créer un.

Avant de continuer, vérifiez que vous avez effectué une revendication concernant votre URL StoreFront. Si l'URL a été revendiquée, l'écran suivant s'affiche et vous pouvez commencer à configurer les paramètres de votre magasin sur site.



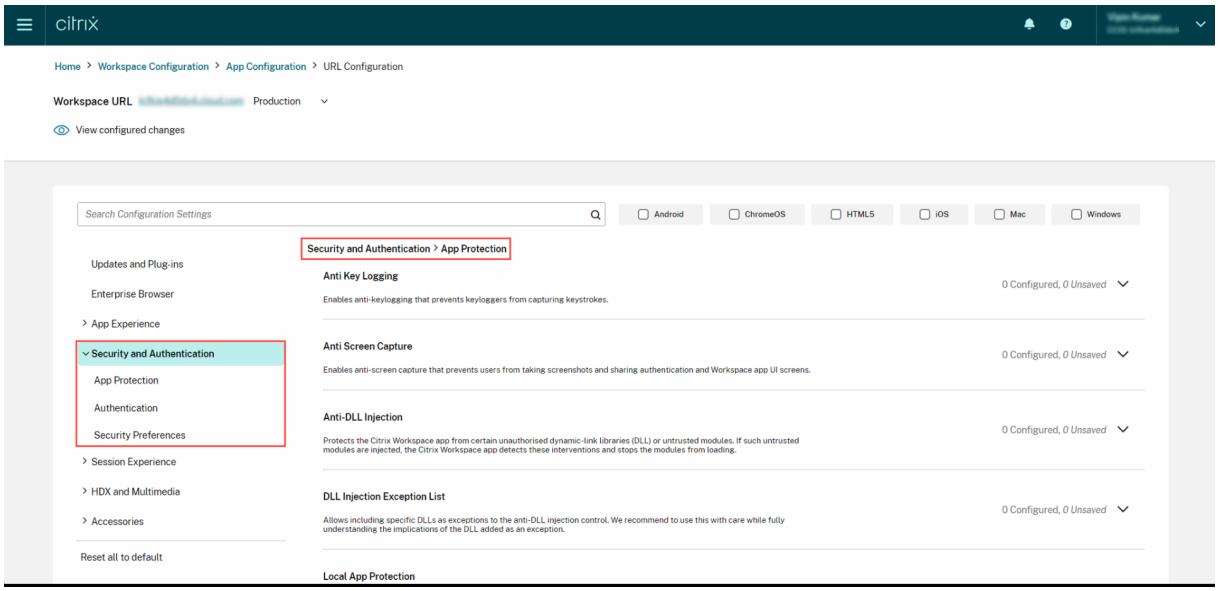
Si vous n'avez pas encore revendiqué votre URL, l'écran suivant s'affiche. Cliquez sur **Démarrer** dans la section **Configurer les paramètres des magasins locaux** pour revendiquer votre URL. Pour plus d'informations, reportez-vous à la section Mise en route.



Sep 28, 2023

Catégorisation des paramètres simplifiée pour faciliter la navigation

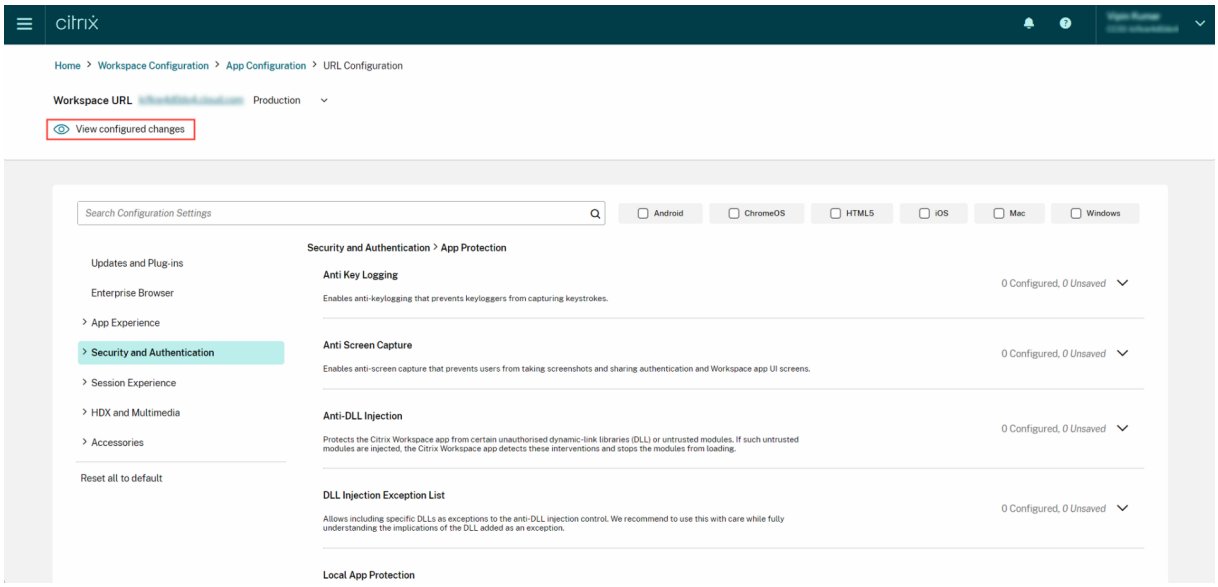
L'interface utilisateur de Global App Configuration Service a été améliorée pour permettre une catégorisation conviviale des paramètres. Les paramètres ont été classés en fonction des workflows et des thèmes des utilisateurs finaux, comprenant sept dossiers principaux et plusieurs sous-dossiers. Cette organisation fluide permet aux administrateurs de naviguer plus facilement parmi plus de 300 paramètres.



Jul 28, 2023

Afficher le résumé des paramètres configurés

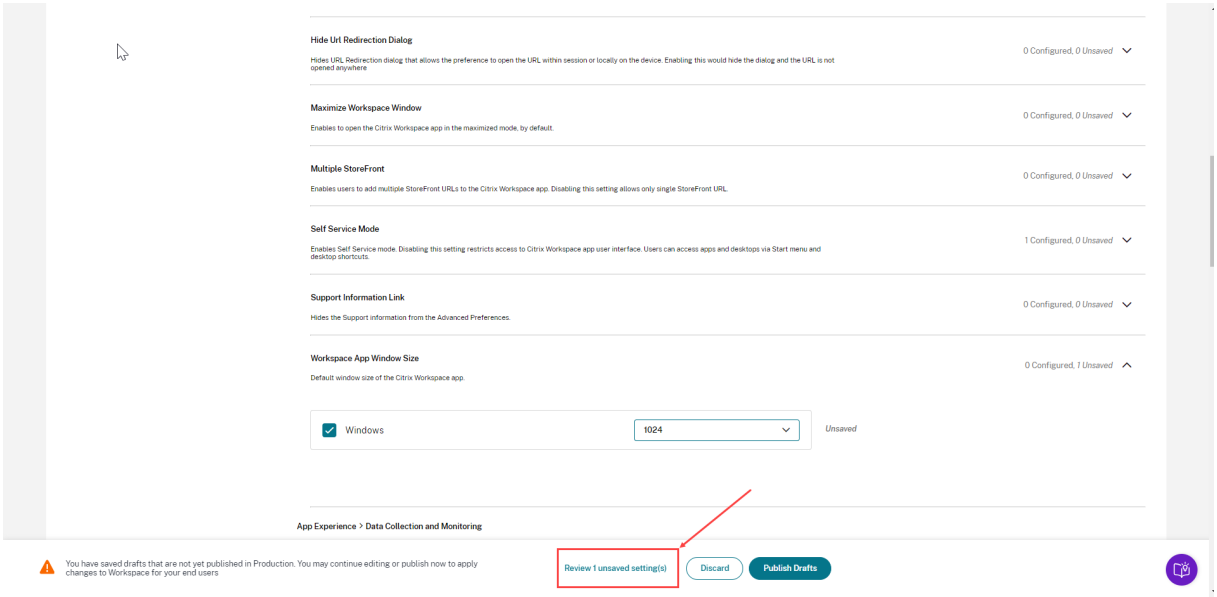
Les administrateurs peuvent désormais consulter un résumé de la configuration actuelle en cliquant sur le bouton **Afficher les paramètres configurés**. Il n'est donc plus nécessaire de développer et de vérifier chaque paramètre séparément. Une liste consolidée de tous les paramètres configurés permet aux administrateurs d'effectuer un examen complet de la configuration actuelle et d'évaluer l'impact sur l'utilisateur.



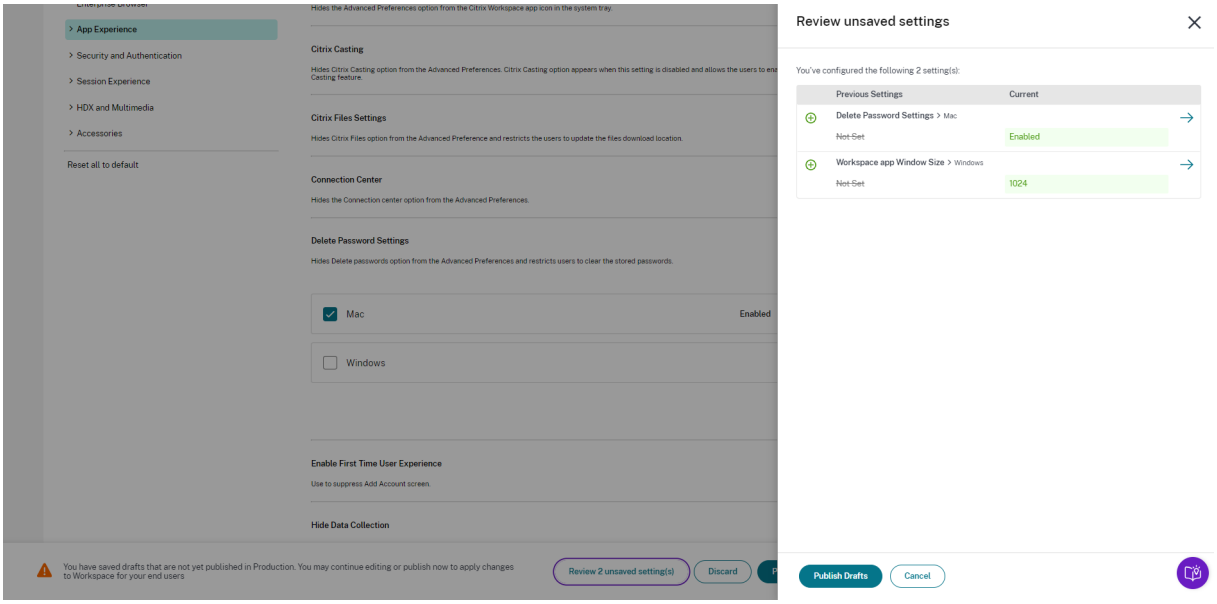
Jun 07, 2023

Vérifier les modifications non enregistrées

Grâce à cette amélioration, les administrateurs peuvent vérifier une dernière fois les modifications non enregistrées avant de publier la configuration. Le nombre de paramètres non enregistrés est affiché dans l'interface utilisateur et les administrateurs peuvent accéder à cette liste en cliquant sur l'option **Vérifier les paramètres non enregistrés**. Cela permet aux administrateurs d'apporter des modifications éclairées et d'assurer l'exactitude des données.



Les administrateurs peuvent également accéder à un paramètre non enregistré en cliquant sur la flèche.

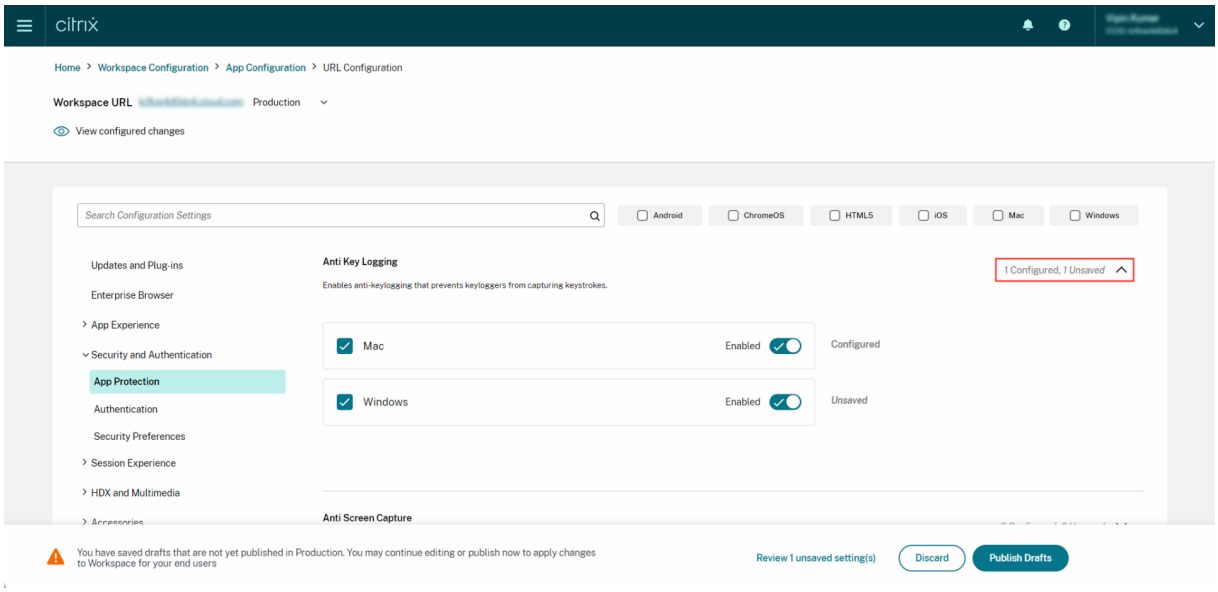


Interface utilisateur améliorée

Les administrateurs peuvent désormais consulter l'état de chaque paramètre sans le développer. Les balises suivantes sont désormais affichées pour faciliter la prise de décision éclairée à chaque étape.

- **Configuré** : affiche le nombre de plateformes (système d'exploitation client) pour lesquelles le paramètre a déjà été configuré.

- **Non enregistré** : affiche le nombre de paramètres configurés mais pas encore enregistrés



May 23, 2023

Fonctions de recherche améliorées

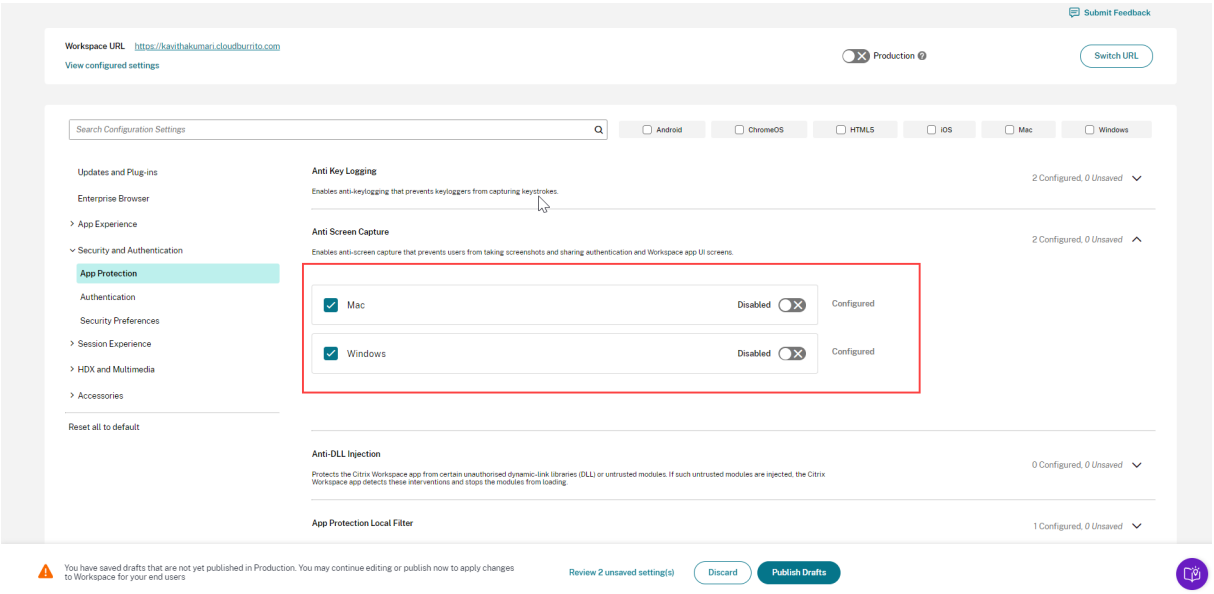
Grâce à cette amélioration, l'expérience de recherche a été améliorée pour offrir une expérience robuste et fluide. Les administrateurs peuvent désormais se connecter au portail cloud et localiser facilement les paramètres requis sur la page Configuration d'application. Ils peuvent utiliser les méthodes de recherche suivantes.

- **Recherche à l'aide de la description des paramètres**
  Les administrateurs peuvent également localiser les paramètres en saisissant les mots clés figurant dans la description du paramètre. Cela permet une approche de recherche plus flexible, en utilisant des termes pertinents associés au paramètre souhaité.
- **Recherche à l'aide du nom du paramètre d'API**
  Les administrateurs ont la possibilité de rechercher des paramètres en saisissant le nom du paramètre d'API correspondant. Cette méthode permet une recherche plus précise et ciblée, permettant aux utilisateurs de trouver rapidement le paramètre spécifique dont ils ont besoin.

Afficher les plateformes applicables à chaque paramètre

Chaque paramètre affiche désormais de manière dynamique uniquement les plateformes pour lesquelles il est pertinent et applicable. Ce filtrage intelligent garantit que les utilisateurs disposent

d'une liste d'options concise et personnalisée, éliminant ainsi tout encombrement et toute confusion inutiles.



Mise en route de Citrix Workspace

October 12, 2023

Cet article décrit les principales étapes de la configuration de Citrix Workspace et des composants associés, du début à la fin. Pour obtenir un résumé des phases impliquées, consultez Présentation du workflow.

Il existe d'autres méthodes pour passer à l'expérience Citrix Workspace complète. Les méthodes les plus courantes sont les suivantes :

- Mise à disposition de Citrix Virtual Apps and Desktops via des espaces de travail
  - Si vous souhaitez accéder aux ressources de votre déploiement Virtual Apps and Desktops local via Workspace, consultez la section Agrégation de sites pour solutions hybrides.
  - Si vous souhaitez migrer vers le cloud, consultez Migration complète vers le cloud.

Présentation du workflow

Si vous configurez Citrix Workspace en tant que nouveau client, il existe cinq étapes principales :

1. Se préparer à Citrix Workspace dans Citrix Cloud
2. Configurer l'accès et l'authentification des abonnés

3. Intégrer les services dans les espaces de travail
4. Personnaliser les espaces de travail en fonction des préférences propres à votre entreprise, telles que les logos et les stratégies de sécurité
5. Déployer Citrix Workspace auprès des abonnés

Le Success Center fournit des conseils supplémentaires basés sur des solutions.

Phase 1 : Se préparer à Citrix Workspace dans Citrix Cloud

Avant de configurer Citrix Workspace, vous devez vous inscrire à Citrix Cloud et vous assurer de répondre aux exigences techniques pour commencer à utiliser Citrix Workspace.

Si vous êtes déjà client Citrix Cloud et que des administrateurs ont été ajoutés via la **Gestion des identités et des accès**, vous pouvez passer à la phase 2 : Configurer l'accès et l'authentification des abonnés.

Les étapes impliquées dans la phase 1 sont les suivantes :

1. S'inscrire à Citrix Cloud
2. Ajouter des administrateurs avec Citrix Identity
3. Configurer l'infrastructure :
    - Créer des emplacements de ressources
    - Déployer des Cloud Connector

La configuration de Citrix Identity implique un mot de passe à usage unique temporaire (TOTP). Outre Citrix Identity, vous pouvez configurer l'authentification Azure AD. Pour plus d'informations sur l'ajout d'administrateurs et la configuration de l'authentification pour les administrateurs, consultez la section Administrateurs dans la documentation du produit Citrix Cloud.

Phase 2 : Configurer l'accès et l'authentification des abonnés

La phase 2 implique la configuration des contrôles d'accès, tels que l'URL de l'espace de travail et la connectivité externe, dans **Configuration de l'espace de travail**.

Vous configurez également un ou plusieurs fournisseurs d'identité dans **Gestion des identités et des accès**, puis activez l'un d'entre eux comme méthode d'authentification principale des abonnés auprès des espaces de travail dans **Configuration de l'espace de travail**.

> **Remarque :**
>
> Vous pouvez accéder à Citrix Workspace de deux manières. La première est l'application Citrix Workspace installée en mode natif, qui remplace Citrix Receiver pour un accès simple et sécurisé aux services et aux espaces de travail Citrix Cloud. L'autre manière d'accéder à Citrix Workspace

> consiste à utiliser un navigateur avec l'URL de l'espace de travail. L'URL de l'espace de travail est activée par défaut, généralement au format : `https://yourcompanyname.cloud.com`.
>
> Pour plus d'informations, consultez Accès à l'espace de travail.

Configurer l'accès aux espaces de travail

Vous pouvez configurer les contrôles d'accès dans **Configuration de l'espace de travail > Accès**. Cela implique généralement les tâches suivantes :

- Configurer et activer l'URL de l'espace de travail
- Configurer la connectivité externe avec Citrix Gateway

Une fois ces deux tâches effectuées, Citrix recommande d'installer, et d'encourager les abonnés à utiliser, l'application Citrix Workspace pour une expérience cohérente des espaces de travail.

Configurer l'authentification des abonnés aux espaces de travail

Vous définissez la manière dont les abonnés s'authentifient pour se connecter à leurs espaces de travail en deux étapes :

1. Dans **Gestion des identités et des accès**, configurez les fournisseurs d'identité.
2. Dans **Configuration de l'espace de travail > Authentification**, choisissez l'une des méthodes d'authentification fournies par les fournisseurs d'identité que vous avez configurés lors de la première étape.

Si vous utilisez un fournisseur d'identité fédéré, vous pouvez également activer l'authentification unique (SSO) à DaaS avec le Service d'authentification fédérée Citrix (FAS).

Pour plus d'informations sur la configuration de l'authentification des abonnés aux espaces de travail, consultez Espaces de travail sécurisés.

Phase 3 : Intégrer les services aux espaces de travail

L'intégration de vos services aux espaces de travail se déroule également en deux étapes :

1. Configurez les services que vous avez achetés dans Citrix Cloud. Pour obtenir la liste des services, consultez Citrix Cloud Services.
2. Activez l'accès à vos services configurés dans **Configuration de l'espace de travail > Intégrations de services**. Pour plus d'informations sur l'intégration des services, consultez Activer et désactiver les services.

Phase 4 : Personnaliser les espaces de travail

Vous pouvez personnaliser l'expérience de l'espace de travail des abonnés pour différents utilisateurs et pour répondre aux exigences organisationnelles spécifiques dans **Configuration de l'espace de travail** en procédant comme suit :

- Personnalisez l'apparence des espaces de travail, y compris les logos et les thèmes personnalisés. Pour savoir comment personnaliser l'apparence de l'espace de travail, consultez Personnaliser l'apparence des espaces de travail.
- Choisissez des options d'interaction, par exemple en autorisant les abonnés à créer des **favoris** et en lançant automatiquement des bureaux. Pour obtenir des instructions sur la personnalisation des interactions des abonnés avec leurs espaces de travail, consultez Personnaliser les interactions de l'espace de travail.
- Personnalisez la confidentialité et la sécurité, y compris la définition d'un délai d'expiration, la création d'une stratégie de connexion et la possibilité de modification du mot de passe des abonnés depuis leur espace de travail. Pour obtenir des instructions sur la façon de personnaliser les stratégies de confidentialité et de sécurité des espaces de travail, consultez Personnaliser les stratégies de sécurité et de confidentialité.

Phase 5 : Déployer Citrix Workspace auprès des abonnés

Citrix vous recommande de vérifier l'intégrité des espaces de travail à l'aide de tests d'acceptation opérationnelle et de contacter notre Success Center pour planifier la manière dont vous intégrez les abonnés. Les principales activités de cette phase sont les suivantes :

1. Tester les espaces de travail
    - Vérifiez que vous pouvez vous connecter via le navigateur et dans l'application Citrix Workspace.
    - Lancez et utilisez toutes les applications et tous les bureaux disponibles.
    - Vérifiez que vous pouvez accéder aux dossiers et fichiers disponibles.
    - Vérifiez que les notifications affichent les actions et les activités attendues.
    - Si cette option est activée, vérifiez que vous pouvez accéder aux ressources des points de terminaison sur les appareils mobiles.
2. Intégrer les abonnés
    - Communiquez les fonctionnalités de Citrix Workspace aux abonnés.
    - Partagez l'URL de l'espace de travail pour un accès via le navigateur.
    - Guidez les utilisateurs pour installer l'application Citrix Workspace.

Pour plus d'informations sur les tests des espaces de travail et l'intégration des abonnés aux espaces de travail, accédez à la page Citrix Workspace end-user adoption resources.

Se préparer à Citrix Workspace

October 12, 2023

Cet article décrit les exigences et les activités administratives nécessaires pour vous aider à préparer la mise en œuvre de Citrix Workspace. Les étapes nécessaires à la préparation de Citrix Workspace sont les suivantes :

1. Assurez-vous de répondre à la configuration requise pour le système et la connectivité pour Citrix Cloud.
2. Planifiez votre déploiement et votre distribution de Citrix Workspace.
3. Connectez-vous ou inscrivez-vous à Citrix Cloud.
4. Ajoutez des administrateurs à Citrix Cloud et Citrix Workspace.
5. Vérifiez vos droits d'utilisation aux services hébergés dans le cloud.
6. Configurez l'infrastructure nécessaire à Citrix Workspace.

Les informations du Citrix Success Center viennent compléter cette documentation. Les articles du Success Center offrent à la fois une perspective globale basée sur les solutions et des détails spécifiques aux services.

La documentation produit Citrix Cloud fournit des conseils plus détaillés aux responsables informatiques et aux développeurs sur les conditions préalables et les activités requises à la préparation de Citrix Workspace dans Citrix Cloud.

Configuration requise pour le système et la connectivité

Citrix Cloud est la console qui vous permet d'afficher et de gérer vos droits de service, et d'accéder à la **configuration de l'espace de travail**.

Si vous avez déjà effectué la configuration pour Citrix Cloud, vous pouvez passer aux étapes décrites dans Planifier votre déploiement et votre distribution.

En résumé, Citrix Cloud nécessite la configuration suivante :

- Un domaine Active Directory pour gérer l'authentification des abonnés aux espaces de travail
- Au moins deux Citrix Cloud Connector par emplacement de ressources
- Une machine dédiée pour chaque Cloud Connector
- Des machines physiques ou virtuelles, appartenant à votre domaine, pour l'hébergement des charges de travail et d'autres composants

Vous avez besoin d'au moins deux machines physiques ou virtuelles, car vous ne pouvez pas installer d'autres composants sur une machine qui héberge un Citrix Cloud Connector.

Pour plus d'informations sur la configuration requise pour Cloud Connector, consultez Détails techniques sur Citrix Cloud Connector. Pour plus d'informations sur l'installation de Cloud Connector, consultez Installation de Cloud Connector.

En outre, les adresses suivantes doivent pouvoir être contactées afin d'utiliser correctement Citrix Workspace :

- `https://*.cloud.com`
- `https://*.citrixdata.com`

Pour obtenir la liste complète des adresses contactables requises pour les services Citrix Cloud, consultez la section Exigences en matière de connectivité des services.

Planifier votre déploiement et votre distribution

Citrix vous recommande de préparer un plan de prise en charge et de gestion Citrix Workspace. Utilisez le Plan du Success Center pour vous aider à établir des objectifs, à définir des cas d'utilisation, à identifier les risques et à créer une stratégie de mise en œuvre, qui inclut les éléments suivants :

- Définissez les résultats commerciaux, les services que vous souhaitez ajouter et les exigences des groupes d'utilisateurs.
- Identifiez les exigences techniques pour configurer l'infrastructure pour Citrix Workspace.
- Constituez votre équipe Workspace. Attribuez des tâches aux équipes de mise à disposition et ajoutez des administrateurs à votre compte Citrix Cloud en donnant l'accès à **Configuration de l'espace de travail**.
- Planifiez l'engagement avec les propriétaires de processus et les abonnés.
  - Préparez une stratégie de changement et un plan de communication.
  - Développez des approches de formation et de renforcement.
  - Réalisez des analyses liées à l'impact et aux intervenants.

Pour plus d'informations sur la planification de votre déploiement et de votre distribution Workspace, consultez la ressource Success Readiness Checklist sur Citrix Success Center.

Se connecter ou s'inscrire à Citrix Cloud

Si vous vous inscrivez en tant que nouveau client, suivez les instructions de la section Inscription à Citrix Cloud.

Si un compte administrateur a déjà été créé pour votre organisation, l'administrateur principal doit vous ajouter au compte d'entreprise. Consultez la section Ajouter des administrateurs pour plus d'informations.

Si vous avez déjà un compte, connectez-vous à Citrix Cloud à l'aide de vos informations d'identification citrix.com, My Citrix ou Citrix Cloud.

Pour plus d'informations sur la connexion ou l'inscription à Citrix Cloud, consultez la ressource Citrix Cloud Services Kickoff Guide.

Ajouter des administrateurs

Le premier compte d'administrateur est créé par le biais du processus d'intégration initial de Citrix Cloud. L'administrateur initial peut ensuite inviter d'autres administrateurs à rejoindre Citrix Cloud. Ces nouveaux administrateurs peuvent utiliser leurs informations d'identification de compte Citrix existantes ou configurer un nouveau compte.

Inviter des administrateurs

Les administrateurs sont ajoutés à votre compte Citrix Cloud via la zone **Gestion des identités et des accès** dans le menu situé sur le côté gauche de la console Citrix Cloud. Entrez l'adresse e-mail de l'administrateur que vous souhaitez ajouter pour lui envoyer une invitation avec les instructions de connexion.

Lorsque vous ajoutez des administrateurs à votre compte Citrix Cloud, vous définissez les autorisations d'administrateur appropriées selon leur rôle dans votre organisation. Les administrateurs disposant d'un **accès complet** peuvent accéder à la **configuration de l'espace de travail** par défaut. Les administrateurs disposant d'un **accès personnalisé** ne peuvent accéder qu'aux fonctions et services que vous sélectionnez. Vous pouvez modifier les autorisations d'accès des administrateurs que vous invitez.

Pour plus d'informations sur l'ajout (et la suppression) d'administrateurs, consultez Administrateurs.

Configurer l'authentification de l'administrateur

Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer votre compte Citrix Cloud. Le fournisseur d'identité Citrix authentifie uniquement les administrateurs Citrix Cloud. Les abonnés doivent s'authentifier auprès de l'un des fournisseurs d'identité répertoriés dans Espaces de travail sécurisés.

Chaque administrateur de votre compte Citrix Cloud doit également configurer l'authentification multifacteur.

L'enregistrement implique le téléchargement et l'installation d'une application d'authentification qui respecte la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO. Pour fa-

ciliter l'enregistrement, Citrix recommande de télécharger et d'installer Citrix SSO *avant* d'effectuer les étapes suivantes.

1. Connectez-vous à votre compte Citrix Cloud.
2. Sélectionnez votre nom et choisissez **Mon profil** dans le menu déroulant.
3. Sélectionnez **Configurer une application d'authentification** sous **Sécurité de connexion** pour recevoir un e-mail contenant le code de vérification nécessaire à l'étape 4.
4. Lorsque vous y êtes invité, saisissez le code de vérification qui vous a été envoyé dans un e-mail de Citrix et le mot de passe de votre compte, puis sélectionnez **Vérifier**.
5. Scannez le code QR ou saisissez la clé dans une application d'authentification qui respecte la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO.
6. Pour confirmer que l'authentification multifacteur a été configurée correctement, entrez le code à 6 chiffres de l'application d'authentification, puis sélectionnez **Vérifier**.
7. Sélectionnez **Ajouter un n° de téléphone de récupération** et saisissez un numéro de téléphone que le support Citrix peut utiliser pour vous joindre pour vérifier votre identité pour les requêtes liées à l'authentification multifacteur.
8. Sélectionnez **Générer des codes de secours** pour créer une liste de codes à usage unique qui peuvent être utilisés si vous perdez l'accès à votre application d'authentification.
9. Sélectionnez **Télécharger les codes** et conservez le fichier texte contenant vos codes de secours dans un emplacement sûr et accessible.
10. Activez la case à cocher, puis sélectionnez **Terminer**.

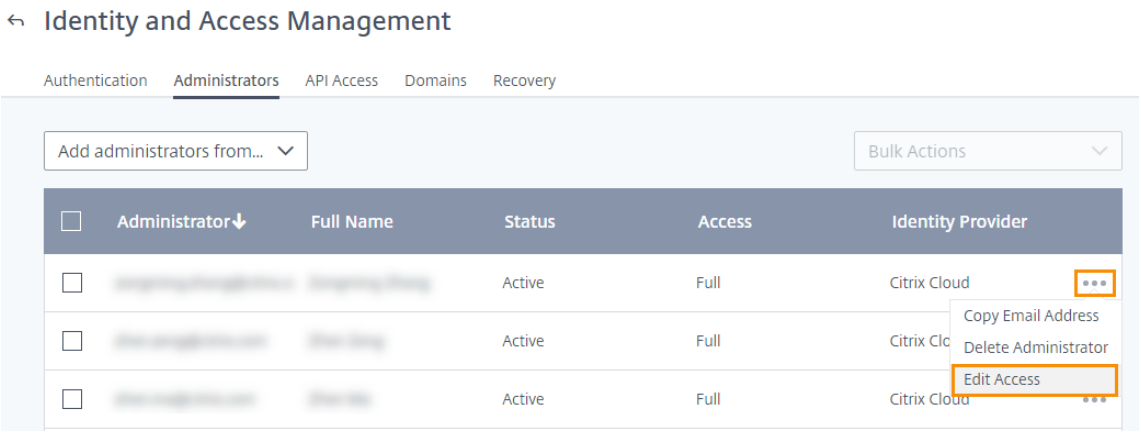
Les instructions relatives à la configuration de l'authentification multifacteur sont également disponibles dans le centre de connaissances et dans la section Configurer l'authentification multifacteur de la documentation produit de Citrix Cloud.

Vous pouvez également configurer Azure Active Directory (AD) pour les administrateurs. Pour plus d'informations sur les fournisseurs d'identité disponibles pour les administrateurs Citrix Cloud et les abonnés Workspace, consultez la section Fournisseurs d'identité.

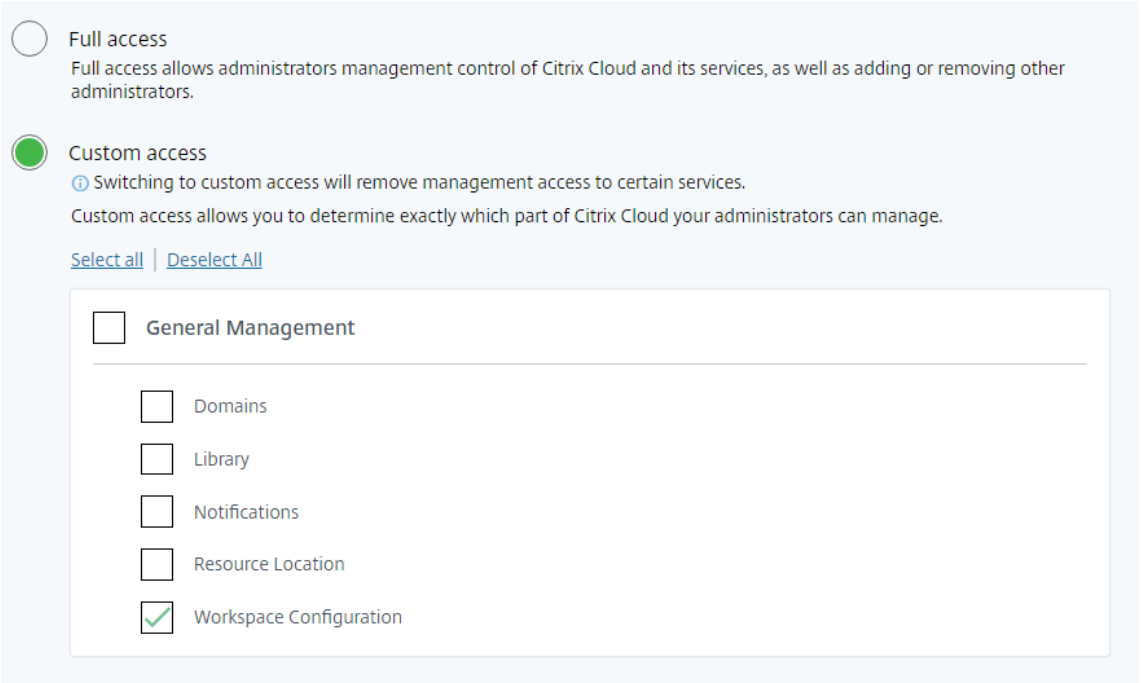
Modifier les autorisations d'administrateur

Pour configurer l'accès personnalisé à la **Configuration de l'espace de travail** :

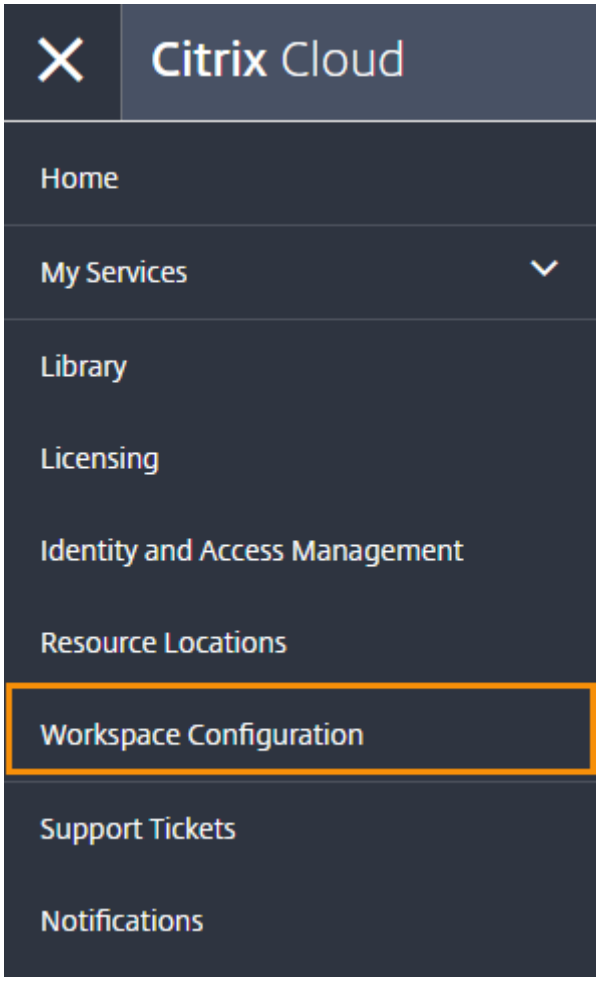
1. Dans le menu **Citrix Cloud**, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Administrateurs**.
2. Recherchez l'administrateur que vous souhaitez gérer, sélectionnez le bouton représentant des points de suspension et sélectionnez **Modifier l'accès**.



3. Vérifiez que le rôle **Accès personnalisé** est activé.
4. Pour activer uniquement l'accès à la **configuration de l'espace de travail**, sélectionnez **Configuration de l'espace de travail** sous **Administration générale**.



Après avoir activé l'accès, les administrateurs se connectent à Citrix Cloud et sélectionnent **Configuration de l'espace de travail** dans le menu **Citrix Cloud**.



> **Remarque :**
>
> Dans Citrix Virtual Apps Essentials, la **configuration de l'espace de travail** est disponible dans le menu Citrix Cloud après la création du premier catalogue.

Vérifier vos droits

Une fois que vous êtes connecté à Citrix Cloud, vous pouvez gérer vos droits, c'est-à-dire les produits et services Citrix que vous avez achetés. Les produits et services Citrix sont affichés sous forme de carte dans le tableau de bord Citrix Cloud et incluent un bouton **Gérer**.

Si vous souhaitez essayer un nouveau service, vous pouvez sélectionner **Demander version d'évaluation** ou **Demander une démo** dans la zone correspondante du tableau de bord Citrix Cloud. Pour plus d'informations sur les évaluations de service, consultez la page Évaluations de services Citrix Cloud.

Si vous souhaitez acheter un nouveau service, vous pouvez convertir un essai en service de production sans reconfiguration ni créer de nouveau compte. Pour acheter un service, notez

l'ID de votre organisation dans le coin supérieur droit de la console Citrix Cloud et accédez à https://www.citrix.com/product/citrix-cloud.

Configurer l'infrastructure

La configuration de l'infrastructure nécessaire à Citrix Workspace implique de connecter vos ressources à Citrix Cloud en effectuant les actions suivantes :

- Déployer les connecteurs dans votre environnement
- Créer des emplacements de ressources

Les emplacements de ressources contiennent les ressources requises pour fournir des services cloud à vos abonnés. Vous pouvez gérer ces ressources à partir de la console Citrix Cloud. Les emplacements de ressources contiennent différentes ressources selon les services que vous utilisez.

Pour créer un emplacement de ressources, vous devez installer au moins deux composants Cloud Connector dans votre domaine.

Citrix Cloud Connector est un composant qui fournit un canal de communication entre Citrix Cloud et vos emplacements de ressources. Le canal établit des connexions au cloud à l'aide du port HTTPS standard (443) et du protocole TCP. Aucune connexion entrante n'est acceptée.

Pour plus d'informations, consultez Citrix Cloud Connector.

> **Remarque :**
>
> Workspace ne prend pas en charge les connexions des clients d'ancienne génération qui utilisent une URL PNAgent pour se connecter aux ressources. Si votre environnement inclut ces clients d'ancienne génération, vous devez plutôt déployer un magasin StoreFront local et activer la prise en charge d'ancienne version. Pour sécuriser ces connexions client, utilisez une instance Citrix Gateway locale au lieu de Citrix Gateway Service.

Étape suivante : Créer votre espace de travail

Maintenant que vous êtes prêt pour Citrix Workspace, effectuez les étapes suivantes :

- Configurez l'accès aux espaces de travail, y compris l'URL de l'espace de travail et la connectivité externe.
- Configurez l'authentification de l'espace de travail, à l'aide des instructions de la section Espaces de travail sécurisés.
- Intégrer les services dans les espaces de travail
- Personnalisez l'expérience des espaces de travail :

- Personnalisez l'apparence des espaces de travail.
- Personnalisez les interactions de l'espace de travail.
- Personnalisez les stratégies de sécurité et de confidentialité.

Nouvelle interface utilisateur de Workspace

November 28, 2023

La nouvelle interface utilisateur de Workspace réduit la complexité visuelle, fournit un accès facile aux fonctionnalités essentielles et améliore l'utilisation et les fonctionnalités de votre application Workspace selon les besoins, ce qui se traduit par une expérience utilisateur optimisée.

Cet article met en évidence certaines des principales fonctionnalités que les abonnés voient lorsqu'ils se connectent à leurs espaces de travail et explique comment accéder à leurs espaces de travail et interagir avec ceux-ci.

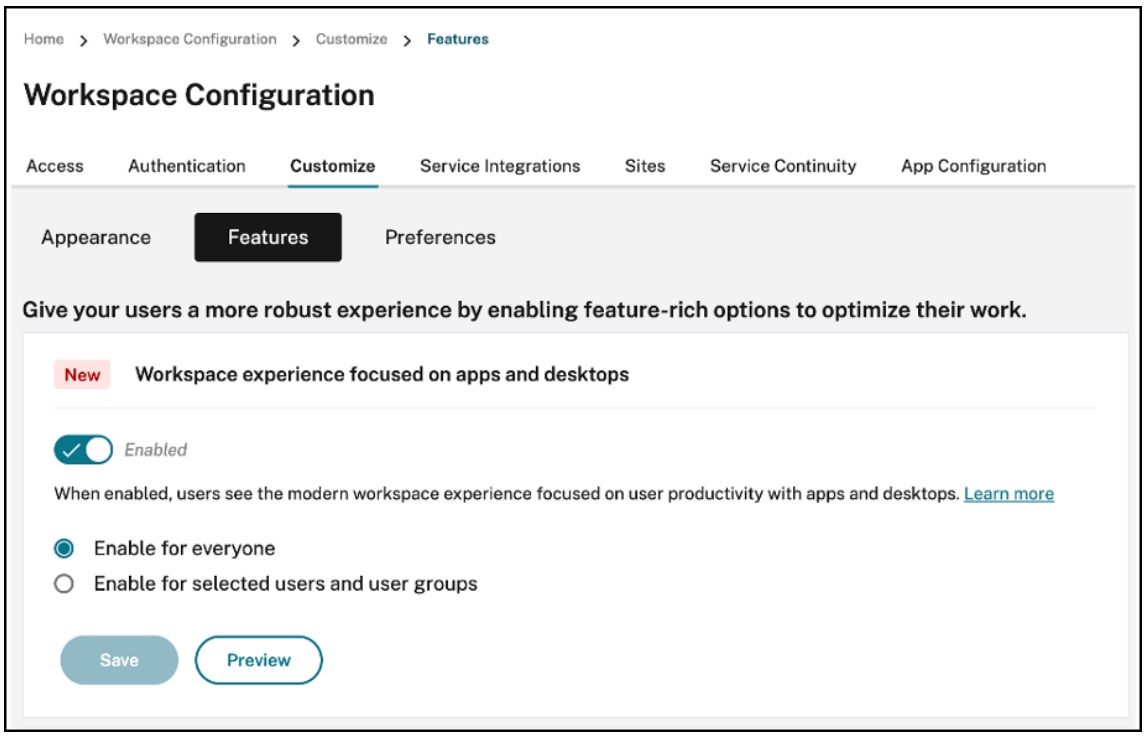
> **Remarque :**
>
> la nouvelle interface utilisateur est compatible avec toutes les versions LTSR de l'application Citrix Workspace. Elle est également compatible avec tous les navigateurs Web à l'exception d'Internet Explorer (pour lequel la version 23.26 de l'interface utilisateur Citrix Workspace est bloquée).

Activer la nouvelle expérience Workspace

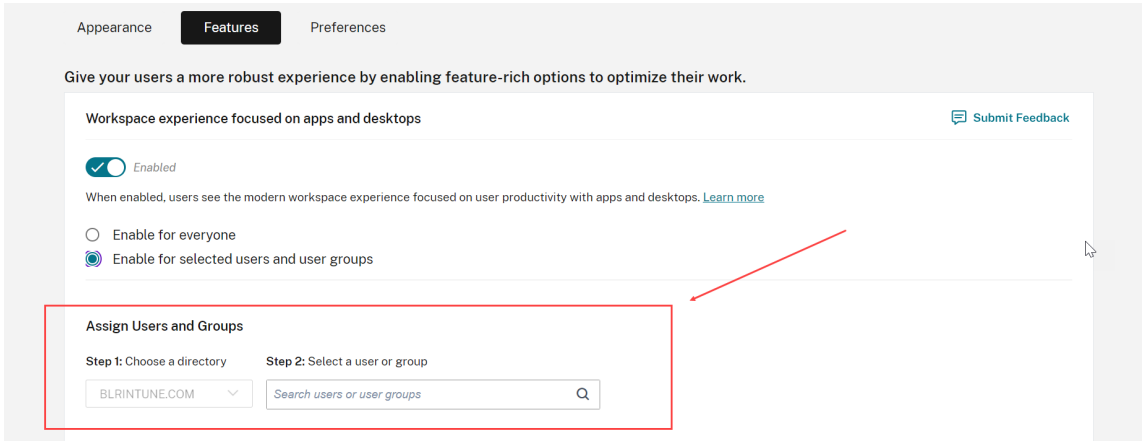
Vous pouvez activer la nouvelle interface utilisateur de Workspace pour les utilisateurs existants. Lorsque cette option est activée, les utilisateurs bénéficient d'un espace de travail moderne axé sur la productivité grâce aux applications et bureaux.

Pour activer la nouvelle interface utilisateur, procédez comme suit :

1. Sur la console d'administration, accédez à **Configuration de l'espace de travail > Personnaliser > Fonctionnalités**.
2. Activez le bouton bascule dans la section **Expérience d'espace de travail centrée sur les applications et les bureaux**. Par défaut, le bouton bascule est désactivé et la fonctionnalité est désactivée.
   Vous avez également la possibilité d'activer cette fonctionnalité pour tous les utilisateurs ou pour certains utilisateurs.



- To enable the new UI for all end users, select **Enable for everyone**.
- To enable the new UI for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



3. Cliquez sur **Save**.
4. Redémarrez l'application Workspace.

> **Remarque :**
>
> La mise à jour de l'interface utilisateur peut prendre environ cinq minutes. Les utilisateurs peu-

> vent voir temporairement une ancienne version de l'interface utilisateur. Si elle est ouverte dans un navigateur, les utilisateurs doivent actualiser la page.

Thèmes, icônes et polices

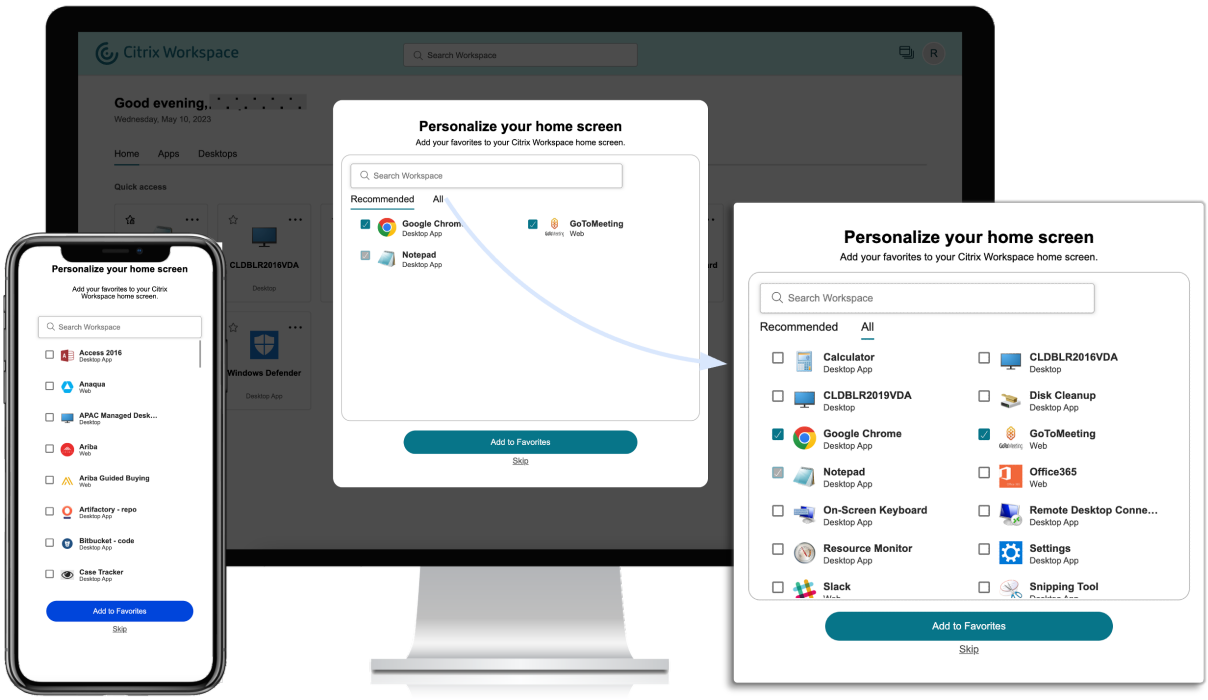
Les nouveaux thèmes de couleurs offrent un contraste amélioré et une palette de couleurs uniforme. La police est utilisée pour l'interface utilisateur sur tous les systèmes d'exploitation pris en charge. Un nouveau jeu d'icônes présente des formes et des couleurs plus reconnaissables, conçues pour plus de lisibilité et de clarté visuelle.

Première expérience utilisateur de l'application Workspace

Lorsqu'ils accèdent à la nouvelle interface utilisateur pour la première fois, les utilisateurs sont invités via une fenêtre contextuelle à ajouter de multiples applications à leurs favoris en une seule étape.

L'expérience de première utilisation est activée lorsque vous possédez plus de 20 applications et que vous n'en avez ajouté aucune à vos favoris. L'expérience est prise en charge sur tous les navigateurs et clients natifs (Mac, Windows, Linux et ChromeOS), ainsi que sur les appareils mobiles (iOS et Android). Vous pouvez la voir la première fois que vous vous connectez.

Les applications recommandées ou obligatoires apparaissent dans l'onglet **Recommandé** de l'écran lors de la première utilisation, tel que défini par les administrateurs sur la console DaaS pour Citrix Virtual Apps and Desktops et sur la console Secure Private Access pour les applications Web et SaaS. Les applications obligatoires sont sélectionnées par défaut et l'option est désactivée. Les applications **recommandées** et mises en favoris automatiquement sont sélectionnées par défaut et l'option est activée pour les utilisateurs. Vous pouvez également sélectionner d'autres applications auxquelles vous abonner ou les ajouter aux favoris depuis tous les onglets. Toutes les applications sélectionnées sont automatiquement ajoutées aux favoris et affichées sur la page d'accueil.



Lorsque vous disposez de cinq applications ou moins, le raccourci bureau d'accès rapide s'affiche dans l'application Citrix Workspace pour Windows.
Les utilisateurs sont abonnés à toutes les applications affichées et les raccourcis de bureau correspondants sont créés.

Limitations

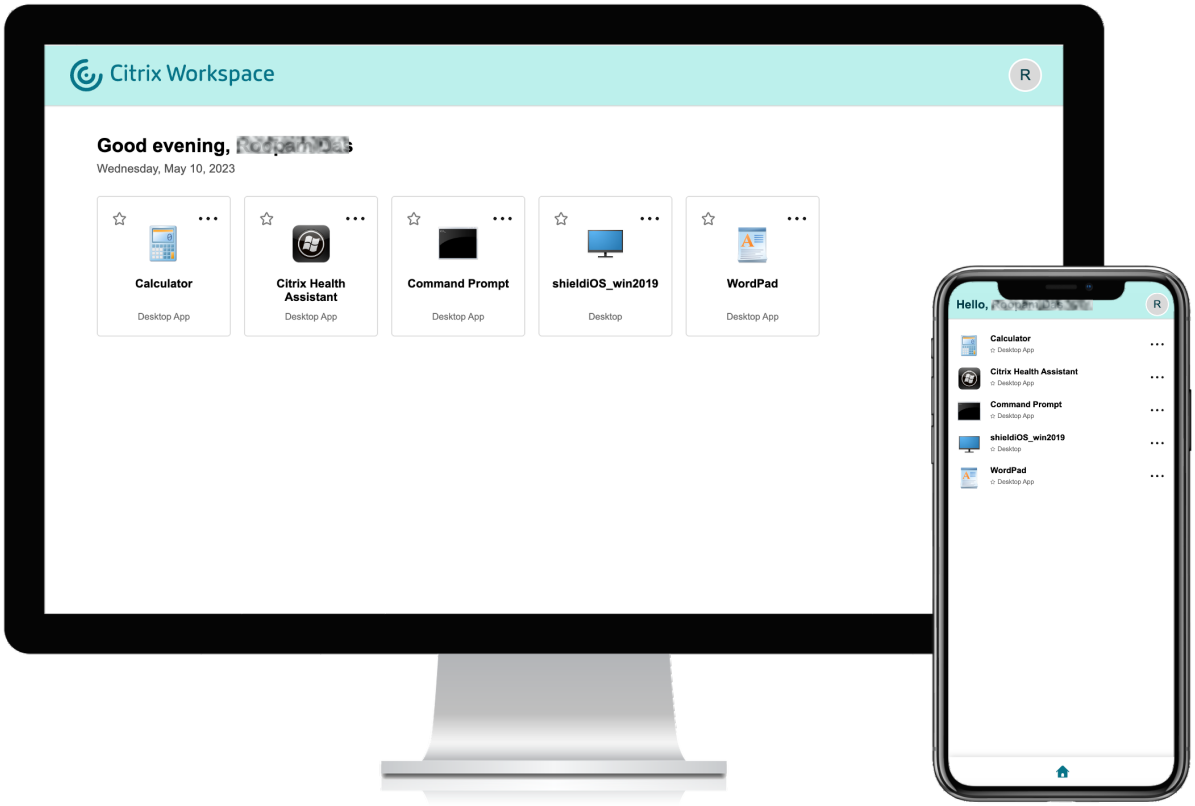
- Tant que le *service de personnalisation de l'utilisateur* n'aura pas été amélioré pour vérifier si l'utilisateur en est à sa première utilisation ou non, l'écran de **personnalisation** s'affichera une fois par appareil et par navigateur, et à chaque fois en mode navigation privée, sauf si les utilisateurs les marquent comme favori.
- Si l'administrateur supprime la balise obligatoire ou recommandée des applications, les applications dans les **favoris** ne sont pas impactées.
- Si l'utilisateur n'a ajouté aucune application à ses **favoris**, l'écran de **personnalisation** s'affiche chaque fois que l'application Workspace est ouverte.
  Pour éviter ce problème :
  - End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.

- Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage** > **Full Configuration** > **Applications**). This prevents the Personalization screen from appearing for all the end-users. For more information, see Customize workspace interactions.

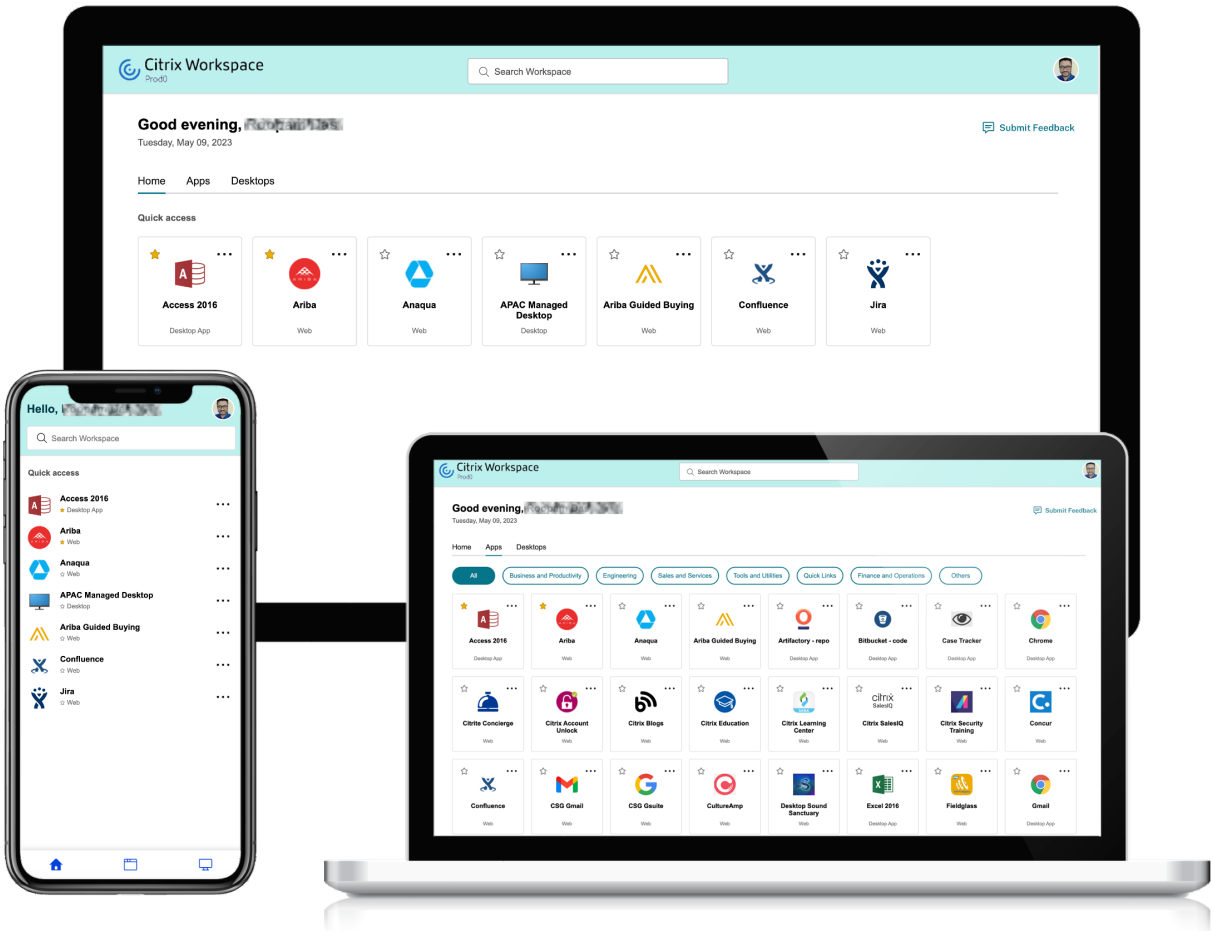
Apparence et disposition de Workspace améliorées

La nouvelle expérience utilisateur est conçue pour mettre l'accent sur la facilité d'utilisation. Vos applications et bureaux virtuels favoris sont organisés en haut de l'interface utilisateur pour en faciliter l'utilisation. Citrix dispose également d'une nouvelle page d'accueil pour améliorer la navigabilité des applications et des bureaux que vous utilisez le plus régulièrement.

Si vous avez moins de 20 applications, vous accédez à l'écran avec une vue simple qui ne comporte aucun onglet ni aucune catégorie. Toutes les applications et tous les bureaux apparaissent sur la même page. Sur cet écran, vos favoris apparaissent en premier, suivis de toutes les autres applications par ordre alphabétique. Toutes les applications ont une icône en forme d'étoile que vous pouvez utiliser pour ajouter des applications à vos favoris ou les supprimer de vos favoris. Vous bénéficiez de cette vue simplifiée de l'application Workspace en fonction du nombre d'applications dont vous disposez, et les applications ne sont pas contrôlées par les administrateurs.



Si vous possédez plus de 20 applications, vous accédez à la page d'accueil lorsque vous vous connectez. Sur cet écran, toutes vos applications favorites apparaissent en premier, suivies des applications les plus récemment utilisées, dans la limite de cinq applications. Les icônes en forme d'étoile des applications **obligatoires** sont verrouillées et vous ne pouvez pas les supprimer des favoris. Si l'administrateur n'a pas activé la page d'accueil, vous accédez à l'écran **Applications**. Sur cet écran, vos favoris apparaissent en premier, suivis de toutes les autres applications par ordre alphabétique. Si l'administrateur a créé des catégories et y a associé des applications, les différentes catégories s'affichent et vous pouvez sélectionner la catégorie d'applications que vous souhaitez consulter.

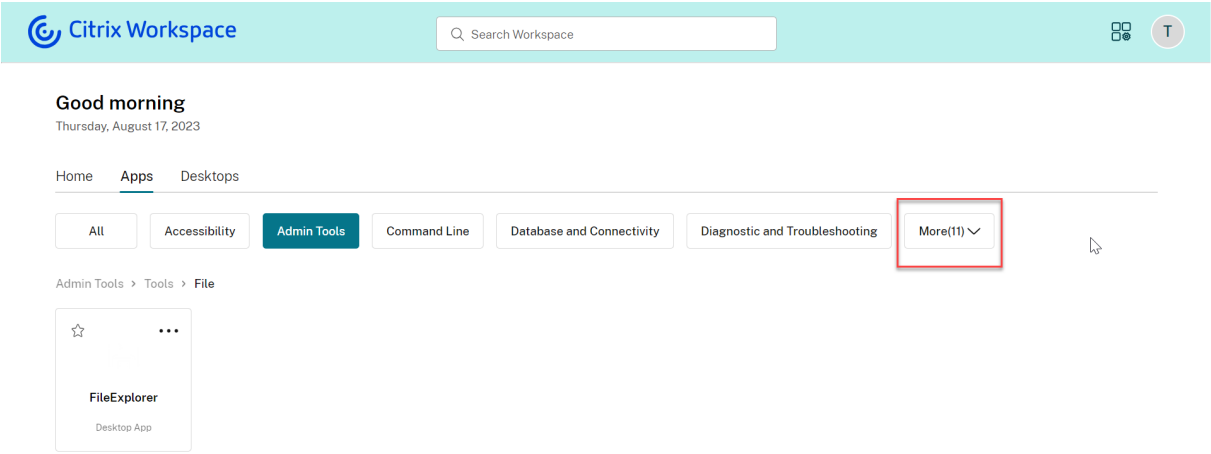


Catégorisation des applications

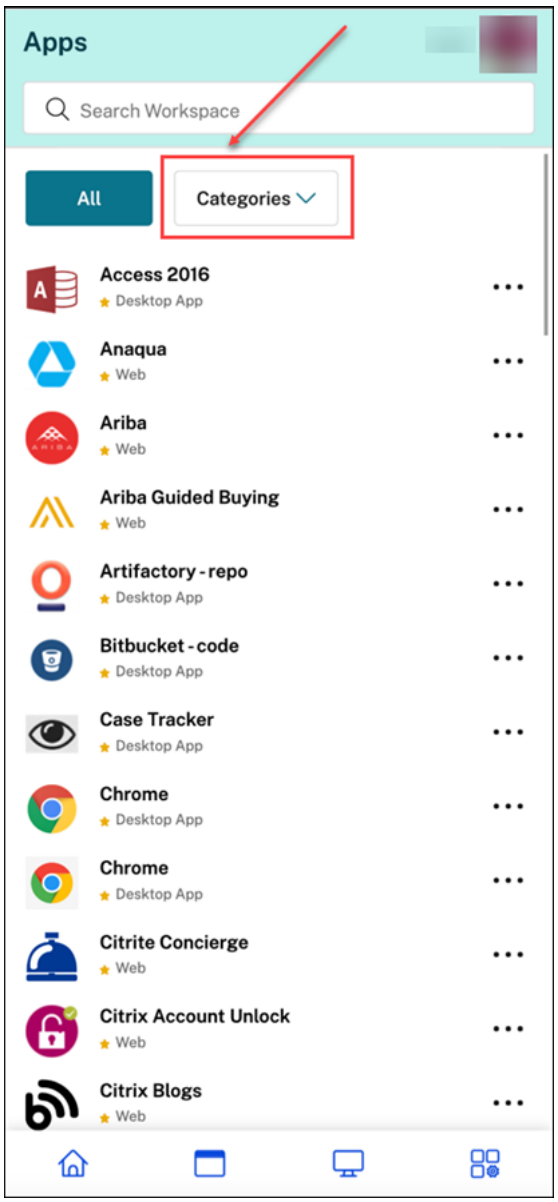
Les utilisateurs finaux peuvent consulter leurs applications organisées en catégories et sous-catégories sur l'interface utilisateur de Workspace. Les sous-catégories sont affichées dans une structure de dossiers. La structure organisée en plusieurs niveaux permet une expérience optimisée et sans encombrement qui contribue à améliorer la satisfaction globale des utilisateurs.

> **Remarque :**
>
> Pour que les applications apparaissent sous une structure de dossiers, les administrateurs doivent ajouter un chemin de dossier. Pour plus d'informations, voir Ajouter un chemin de dossier.

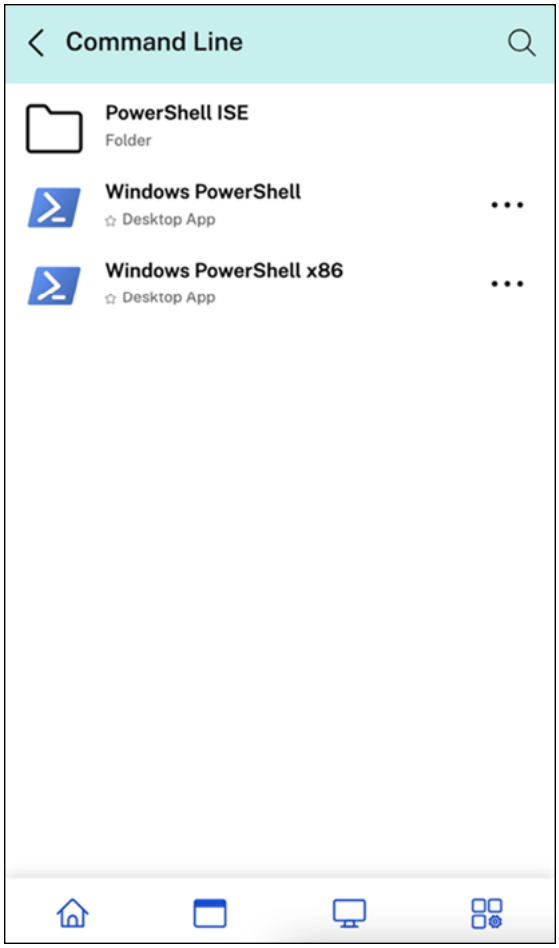
Lorsque le nombre de catégories principales créées par les administrateurs dépasse l'espace disponible sur l'écran de l'utilisateur, l'interface utilisateur s'ajuste en fonction de la taille de l'écran et déplace les catégories de manière dynamique dans le menu déroulant **Plus**.
Les fils de navigation sont également visibles par les utilisateurs.



Sur les plates-formes mobiles, accédez à l'onglet Applications et cliquez sur le menu déroulant **Catégories** pour afficher la liste des catégories disponibles. Les sous-catégories sont affichées sous forme de dossiers qui peuvent contenir d'autres sous-dossiers ou applications conformément à la configuration effectuée par l'administrateur.

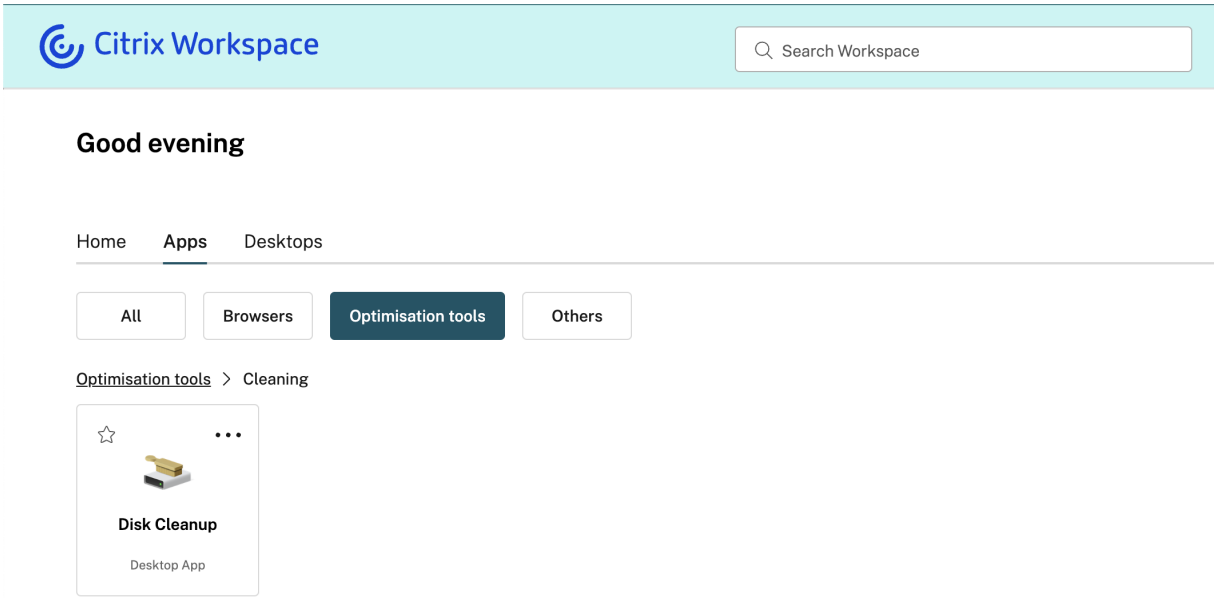


Sélectionnez la catégorie appropriée. Une liste des sous-catégories et d'applications disponibles s'affiche en fonction de la configuration effectuée par l'administrateur.



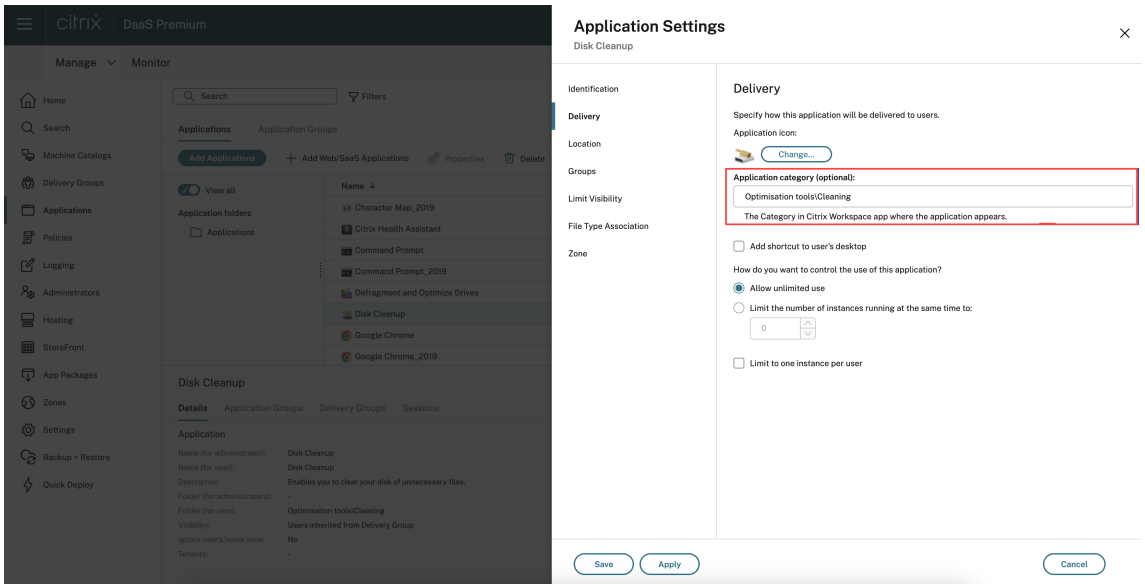
Ajouter un chemin de dossier

Le chemin du dossier vous permet de définir les catégories dans lesquelles une application apparaît. Il représente la structure de dossier qui apparaît à l'écran pour les utilisateurs finaux.
Prenons l'exemple d'une application pour laquelle le dossier est défini comme `Optimisation tools/Cleaning`. Désormais, pour accéder à cette application, les utilisateurs finaux doivent accéder à Outils d'optimisation > Nettoyage, où Outils d'optimisation est une catégorie et Nettoyage est sa sous-catégorie.



Pour définir le chemin du dossier d'une application :

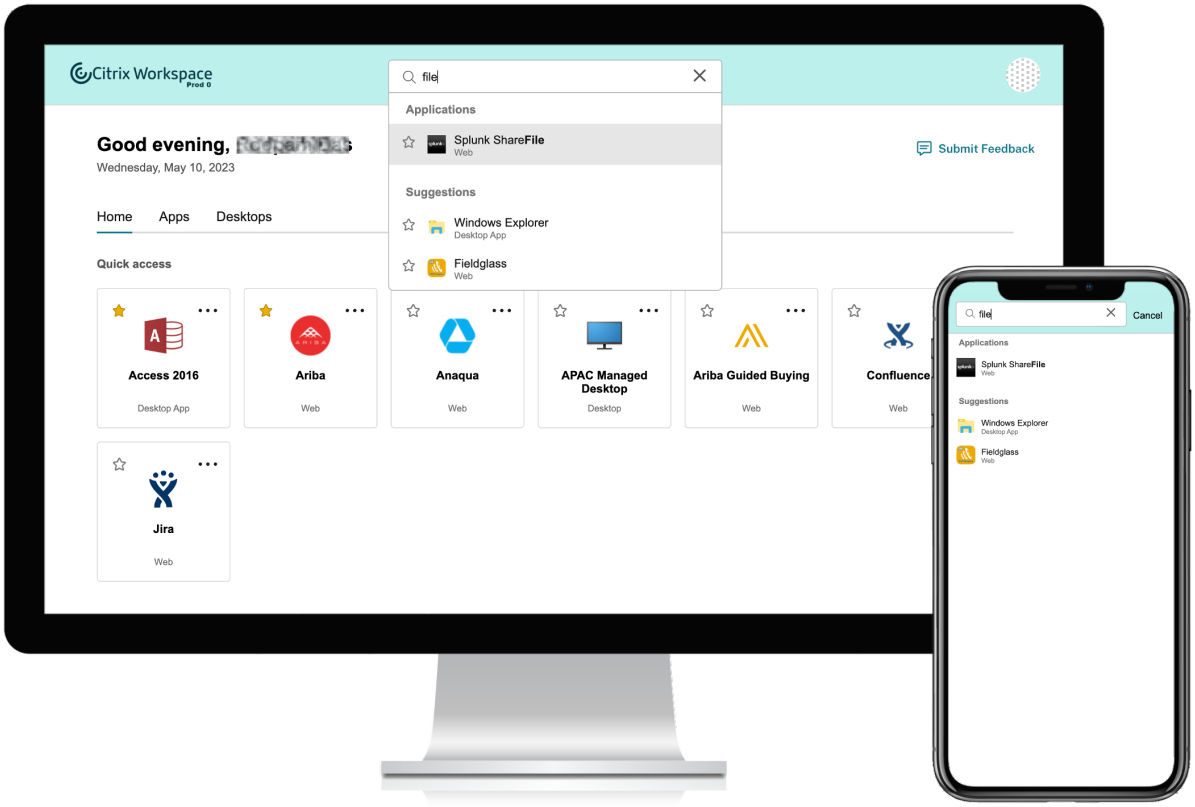
1. Accédez à **Citrix DaaS** sur la console cloud d'administration.
2. Accédez à **Applications** et localisez l'application.
3. Cliquez avec le bouton droit sur l'application et sélectionnez **Propriétés**.
4. Dans le champ **Catégorie d'application**, définissez le chemin du dossier.



5. Cliquez sur **Enregistrer**.

Fonctionnalité de recherche améliorée

La fonctionnalité de **recherche** améliorée vous permet d'obtenir des résultats plus rapidement dans les moteurs de recherche. L'option **Rechercher** apparaît dans la barre d'outils pour faciliter l'utilisation et vous permet d'effectuer une recherche rapide et intuitive depuis l'application Workspace.



Les améliorations suivantes ont été apportées :

- La recherche par défaut affiche les cinq applications ou bureaux les plus récemment utilisés
- La vérification orthographique est activée pour les recherches et les résultats de la saisie automatique sont affichés
- Les résultats de recherche incluent les applications au sein de sessions virtuelles en fonction des applications Web, SaaS et qui ont été consultées récemment.
- Possibilité d'effectuer des recherches par catégories créées par l'administrateur
- Les résultats de recherche affichent les **favoris** en haut de la page

Gestionnaire d'activités

November 28, 2023

Le Gestionnaire d'activités est une fonctionnalité simple mais puissante de Citrix Workspace qui permet aux utilisateurs de gérer efficacement leurs ressources. Il améliore la productivité en facilitant des actions rapides sur les applications et les bureaux actifs depuis n'importe quel appareil. Les utilisateurs peuvent interagir de manière fluide avec leurs sessions, mettre fin ou déconnecter les sessions qui ne sont plus nécessaires, libérant ainsi des ressources et optimisant les performances en déplacement.

Le panneau Gestionnaire d'activités affiche une liste consolidée des applications et des bureaux actifs non seulement sur l'appareil actuel, mais également sur tout appareil distant sur lequel des sessions sont actives. Les utilisateurs peuvent consulter cette liste en cliquant sur l'icône du Gestionnaire d'activités située à côté de l'icône de profil sur le bureau et en bas de leur écran sur les appareils mobiles.

> **Remarque :**
>
> Si vous ne parvenez pas à voir clairement l'icône du Gestionnaire d'activités dans un thème de bannière plus sombre, pensez à modifier et à tester la couleur sélectionnée dans le paramètre **Texte de bannière et couleur d'icône**. L'icône peut ne pas être clairement visible en raison du faible contraste entre la bannière et l'icône du Gestionnaire d'activités. Pour plus d'informations, consultez la section Configurer des thèmes personnalisés.

Activer le Gestionnaire d'activités

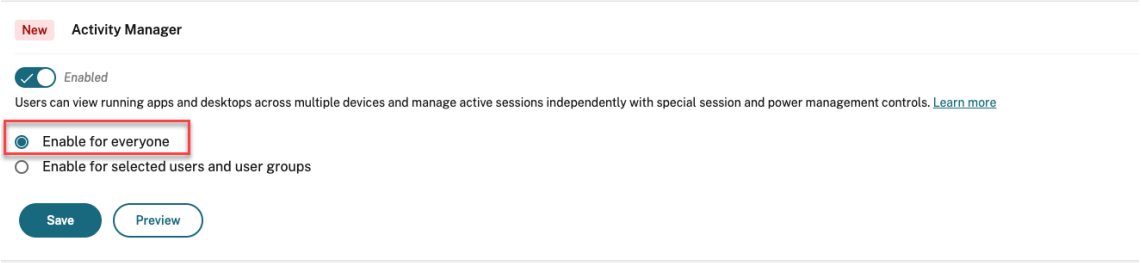
En tant qu'administrateur, vous pouvez désormais activer ou désactiver la fonctionnalité Gestionnaire d'activités pour vos utilisateurs finaux. Conformément aux stratégies de votre organisation, vous pouvez activer la fonctionnalité pour tout le monde ou uniquement certains utilisateurs et groupes d'utilisateurs.

> **Remarque :**
>
> La fonctionnalité Gestionnaire d'activités ne peut être activée que pour la nouvelle interface utilisateur. Pour plus d'informations sur la nouvelle interface utilisateur, consultez Activer la nouvelle expérience Workspace

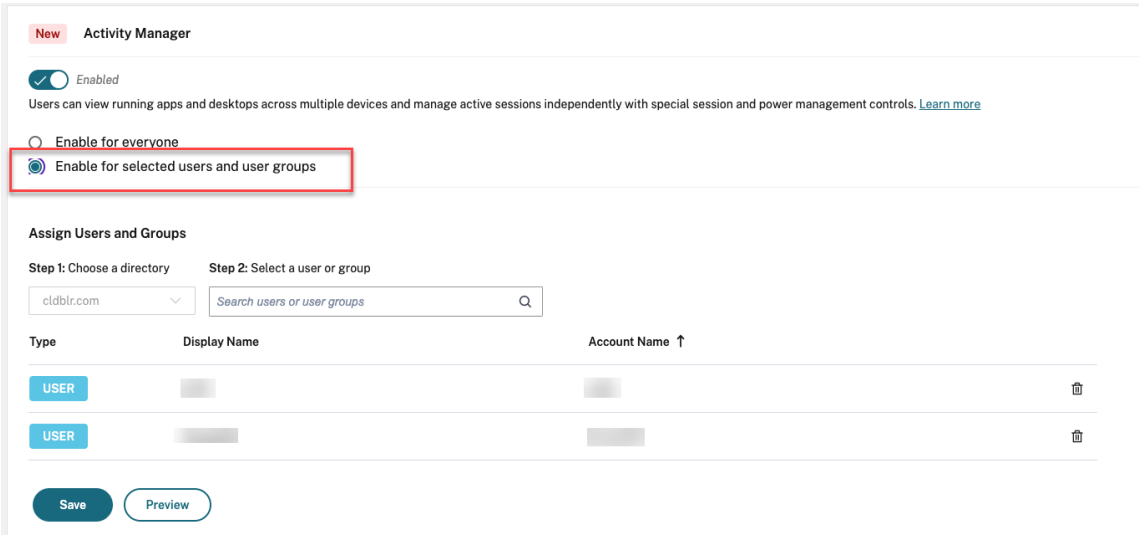
Pour activer le Gestionnaire d'activités, procédez comme suit :

1. Sur la console d'administration, accédez à **Configuration de l'espace de travail** > **Personnaliser** > **Fonctionnalités**.

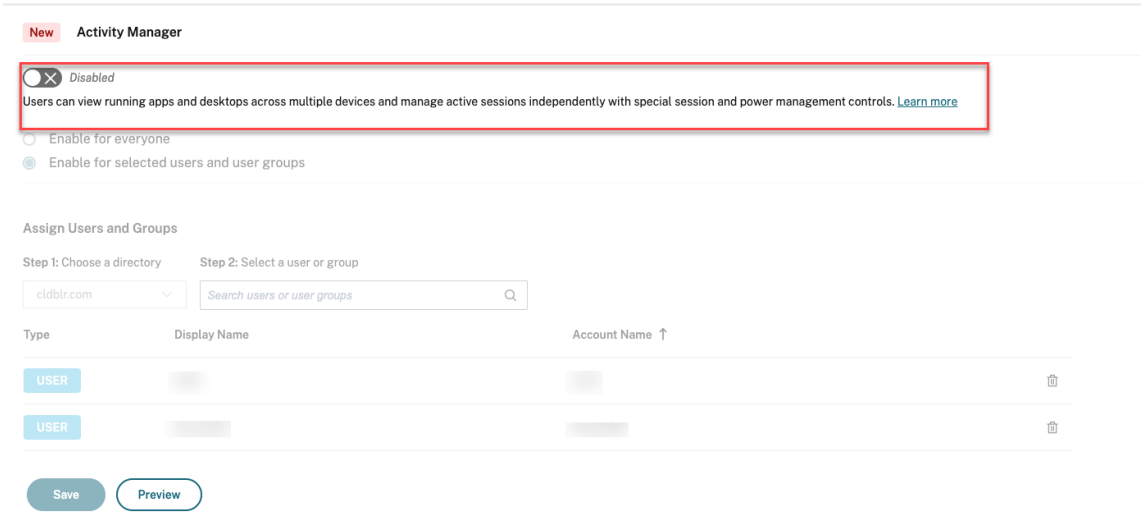
2. Dans la section Gestionnaire d'activités, activez le bouton bascule pour activer le Gestionnaire d'activités.
3. Vous pouvez ensuite personnaliser les autorisations d'accès comme suit.
    - Pour activer le Gestionnaire d'activités pour tous les utilisateurs finaux, sélectionnez **Activer pour tout le monde**.



    - Pour activer le gestionnaire d'activités pour des utilisateurs et des groupes d'utilisateurs sélectionnés, sélectionnez **Activer pour des utilisateurs et des groupes d'utilisateurs sélectionnés**. Vous pouvez ensuite sélectionner le répertoire auquel les utilisateurs ou les groupes d'utilisateurs appartiennent. Une fois le répertoire approprié sélectionné, vous pouvez voir les utilisateurs et les groupes d'utilisateurs appropriés.



    - Pour désactiver le Gestionnaire d'activités pour tout le monde, désactivez ce bouton bascule.



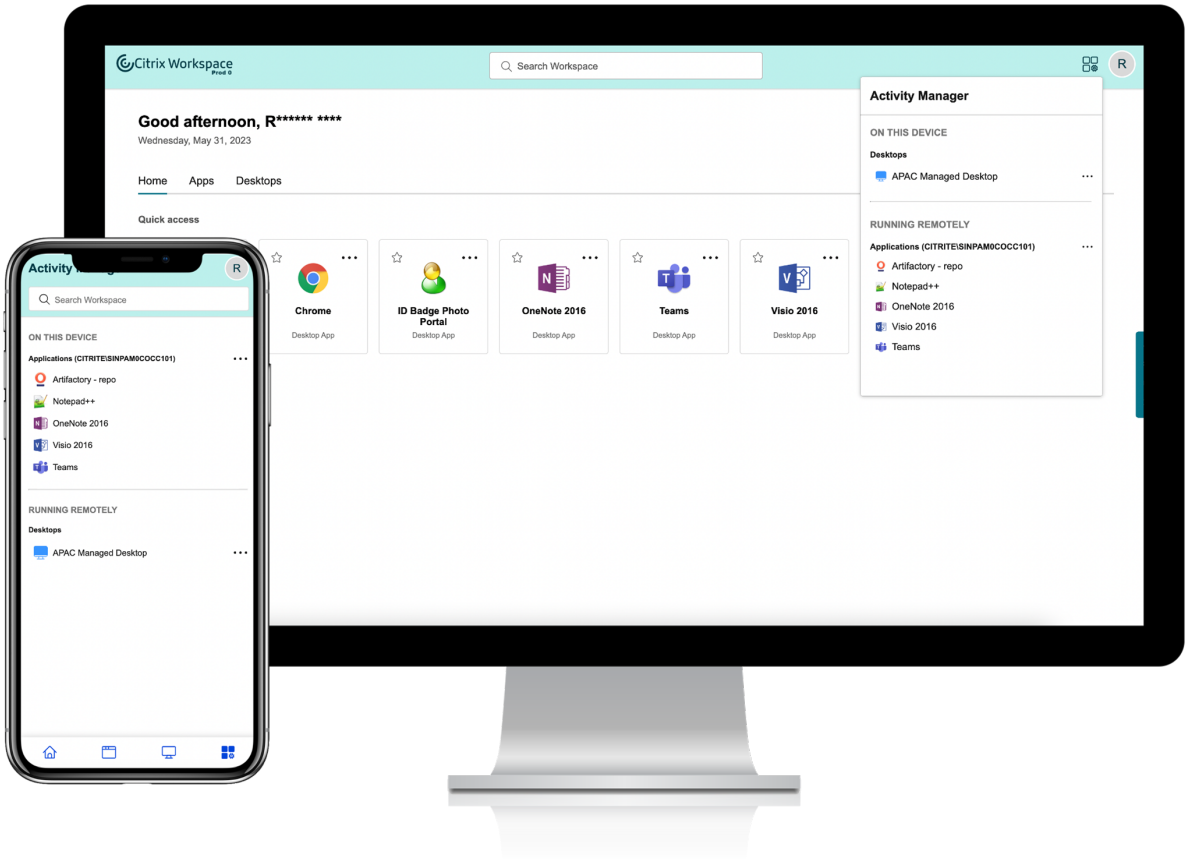
4. Cliquez sur **Save**.

> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que pour les applications et les bureaux virtuels. Elle ne s'applique pas aux applications Web et SaaS.

Utiliser le Gestionnaire d'activités

Les applications et les bureaux actifs sont regroupés comme suit dans le Gestionnaire d'activités.

- La liste des applications et des bureaux actifs sur l'appareil actuel est regroupée sous **Sur cet appareil**.
- La liste des applications et des bureaux actifs sur d'autres appareils est regroupée sous **Exécuté à distance**.



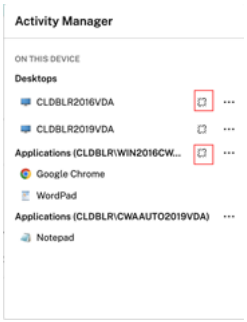
Les utilisateurs peuvent effectuer les actions suivantes sur une application ou un bureau en cliquant sur le bouton des points de suspension (…) correspondant.

- **Déconnecter** : la session à distance est déconnectée, mais les applications et les bureaux sont actifs en arrière-plan.
- **Fermer la session** : ferme la session en cours. Toutes les applications des sessions sont fermées et tous les fichiers non enregistrés sont perdus.
- **Arrêter** : ferme les bureaux déconnectés.
- **Forcer la fermeture** : force la mise hors tension du bureau en cas de problème technique.
- **Redémarrer** : arrête le bureau et le redémarre.

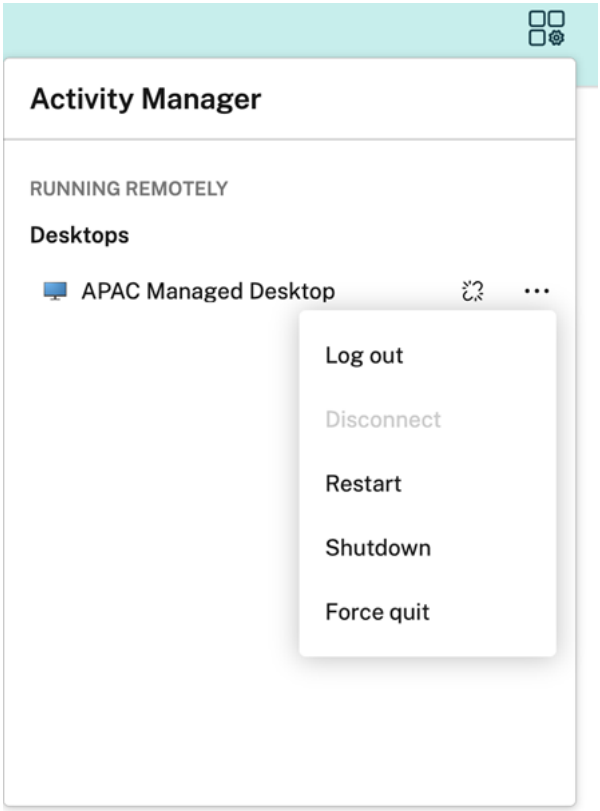
Applications et bureaux déconnectés

Le Gestionnaire d'activités permet désormais aux utilisateurs d'afficher les applications et les bureaux qui s'exécutent en mode déconnecté, localement ou à distance, et d'intervenir sur ceux-ci. Les sessions peuvent être gérées à partir d'appareils mobiles ou de bureau, ce qui permet aux utilisateurs d'intervenir lorsqu'ils sont en déplacement. L'intervention sur les sessions déconnectées, telles que

la fermeture de session ou l'arrêt, favorise une utilisation optimisée des ressources et réduit la consommation d'énergie.



- Les applications et les bureaux déconnectés sont affichés sur le panneau du Gestionnaire d'activités et sont marqués d'une icône de déconnexion.
- Les applications déconnectées sont regroupées sous les sessions respectives qui sont marquées d'une icône de déconnexion.



Les utilisateurs peuvent effectuer les actions suivantes sur leurs bureaux déconnectés en cliquant sur le bouton représentant des points de suspension :

- **Fermer la session** : utilisez cette option pour vous déconnecter de votre bureau déconnecté. Toutes les applications de la session sont fermées et tous les fichiers non enregistrés sont per-

dus.
- **Arrêter** : utilisez cette option pour fermer vos bureaux déconnectés.
- **Forcer la fermeture** : utilisez cette option pour forcer la mise hors tension de vos bureaux déconnectés en cas de problème technique.
- **Redémarrer** : utilisez cette option pour arrêter et redémarrer le bureau déconnecté.

Le comportement des sessions déconnectées sur le Gestionnaire d'activités est différent comme suit.

- Si vous êtes connecté à Citrix Workspace via un navigateur et que vous déconnectez une session locale, la session s'affiche d'abord sous la section Sur cet appareil. Toutefois, une fois que vous fermez et rouvrez le Gestionnaire d'activités, la session déconnectée est déplacée sous la section Exécuté à distance.
- Si vous êtes connecté à l'application Citrix Workspace via un appareil natif et que vous déconnectez une session locale, la session déconnectée disparaît de la liste. Toutefois, une fois que vous fermez et rouvrez à nouveau le Gestionnaire d'activités, la session déconnectée est déplacée sous la section Exécuté à distance.

Mettre à disposition des instances DaaS et Virtual Apps and Desktops avec Citrix Workspace

October 12, 2023

Citrix Workspace est le service cloud multi-locataire qui remplace StoreFront, le magasin d'applications local mono-locataire qui regroupe des applications et des bureaux Citrix DaaS. La plate-forme Citrix Workspace est le composant cloud qui fournit les outils, les services et les fonctionnalités nécessaires au travail à distance, à l'extensibilité et à la personnalisation via Citrix Workspace.

Vous disposez de différentes options pour agréger vos instances DaaS avec Citrix Workspace. L'option que vous choisissez dépend des facteurs suivants :

- Si vous souhaitez migrer complètement vers le cloud ou adopter une solution hybride
- Si vous prévoyez d'autoriser l'accès externe à DaaS.

Migration complète vers le cloud

Vous pouvez migrer votre configuration locale vers le cloud, ce qui permet aux abonnés d'accéder aux instances DaaS via Workspace, en déplaçant votre infrastructure gérée par les services informatiques dans un environnement géré par Citrix. Avec la migration complète, vous gérez moins de composants.

Citrix vous recommande d'utiliser l'outil de configuration automatisée pour simplifier le processus de migration d'un ou plusieurs sites locaux vers un service cloud. Les principales étapes de ce processus sont les suivantes :

1. Assurez-vous de remplir les conditions préalables à la migration de votre configuration.
2. Exportez votre configuration locale. Pour plus d'informations sur ce processus, consultez la section Exportation de votre configuration locale Citrix Virtual Apps and Desktops.
3. Importez votre configuration dans le cloud. Pour plus d'informations sur ce processus, consultez Importation de votre configuration vers Citrix DaaS

Pour plus d'informations sur la configuration automatisée, consultez la section Migrer vers le cloud et le guide de déploiement disponible sur Tech Zone.

Agrégation de sites pour solutions hybrides

Vous pouvez effectuer la transition vers Citrix Workspace avec votre déploiement Virtual Apps and Desktops local existant. Ce processus s'appelle « agrégation de sites » et implique le remplacement de votre infrastructure gérée par les services informatiques par une infrastructure gérée par Citrix.

Vous pouvez choisir l'agrégation de sites pour effectuer une transition lente vers Workspace, ou si vous souhaitez une solution hybride hébergeant certains composants dans le cloud, mais pas tous. Un modèle hybride vous permet de gérer la capacité du cloud parallèlement aux ressources locales tout en offrant une expérience utilisateur unifiée sans migration complète vers le cloud.

Avant de passer de StoreFront à Workspace avec l'agrégation de sites, vous devez disposer d'une configuration Active Directory (AD) et de Cloud Connector installés dans vos emplacements de ressources.

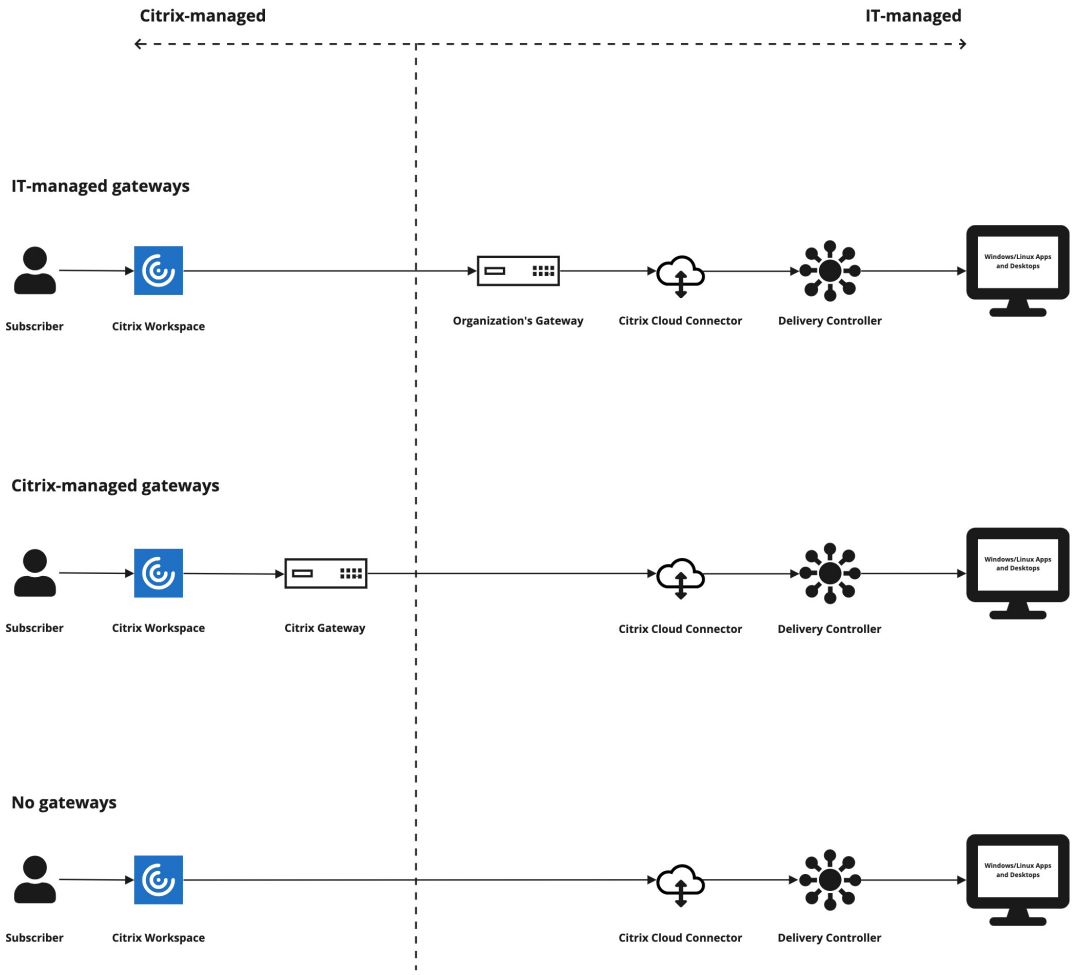
L'agrégation de sites comporte trois grandes étapes :

1. **Identifier le site.** Un site comprend les composants qui constituent un déploiement de production. Vous pouvez disposer de différents sites pour différents emplacements et succursales.
2. **Vérifier la connexion Active Directory (AD).** Les abonnés doivent s'authentifier auprès de Citrix Workspace avec AD. Assurez-vous que les abonnés peuvent s'authentifier en détectant les domaines AD dans lesquels vos Cloud Connector sont installés.
3. **Choisir le type de déploiement.** Il existe trois options de connectivité pour cette étape :
    - Passerelles gérées par les services informatiques
    - Passerelles gérées par Citrix
    - Aucune passerelle

Pour plus d'informations, consultez la section Options de connectivité.

Options de connectivité

Les trois options suivantes permettent d'accéder à DaaS via Citrix Workspace et sont conçues pour répondre à différentes exigences professionnelles.



Option de connectivité	Scénario
Passerelles traditionnelles (gérées par les services informatiques)	Choisissez cette option si vous souhaitez utiliser votre propre passerelle pour la connectivité externe à vos instances DaaS. Cela vous permet de tirer parti de votre investissement actuel dans les passerelles locales.

Option de connectivité	Scénario
Passerelles gérées par Citrix	Choisissez cette option si vous souhaitez utiliser **Citrix Gateway Service** pour une connectivité externe à vos applications et bureaux virtuels. Les connexions HDX entre les clients et les VDA sont transmises par proxy via **Citrix Gateway Service**.
Aucune passerelle (interne uniquement)	Choisissez cette option si vous souhaitez que les abonnés lancent les instances DaaS *uniquement* à l'aide de clients au sein de votre réseau d'entreprise. Les abonnés n'auront pas d'accès externe aux instances DaaS si vous choisissez cette option.

Pour plus d'informations sur le processus d'agrégation de sites et les étapes requises, consultez la page Agréger les applications et les bureaux virtuels locaux dans des espaces de travail.

Configurer la résilience et l'optimisation des espaces de travail

Pour plus d'informations sur l'amélioration de l'efficacité et de la disponibilité de vos instances DaaS via Citrix Workspace, consultez Optimiser DaaS dans Citrix Workspace. Citrix fournit des instructions pour :

- Optimiser la connectivité avec Direct Workload Connection
- Assurer la continuité du service pendant une panne pour une résilience hors ligne.
- Configurer l'authentification unique (SSO) pour les applications et les bureaux virtuels avec le service d'authentification fédérée Citrix (FAS)

Configurer l'accès aux espaces de travail

November 28, 2023

Citrix recommande d'utiliser la dernière version de l'application Citrix Workspace pour accéder aux espaces de travail. L'application Citrix Workspace remplace Citrix Receiver. Vous pouvez également accéder aux espaces de travail via l'URL de Workspace à l'aide de la dernière version de Microsoft Edge, Google Chrome, Mozilla Firefox ou Apple Safari.

Cet article résume les étapes de configuration et d'utilisation :

- URL de Workspace
- Application Citrix Workspace (anciennement Citrix Receiver)
- Instances Citrix Gateway ou Citrix Gateway Service pour la connectivité externe
- Fournisseurs d'identité pour l'authentification aux espaces de travail.

Vue d'ensemble

Les abonnés peuvent accéder à Citrix Workspace via un navigateur avec l'URL Workspace ou via l'application Citrix Workspace installée sur leurs appareils.

L'URL de l'espace de travail est personnalisable et est activée par défaut. Pour obtenir des instructions sur la modification de l'URL de l'espace de travail, consultez URL de l'espace de travail dans cet article.

L'application Citrix Workspace remplace Citrix Receiver en tant qu'application installée en mode natif fournissant l'accès à l'interface utilisateur (UI) Workspace. Pour plus d'informations sur l'application Citrix Workspace et la transition depuis Citrix Receiver, consultez la section Application Citrix Workspace (anciennement Citrix Receiver) dans cet article.

Les abonnés distants peuvent obtenir un accès externe à leurs espaces de travail si vous configurez la connectivité externe avec Citrix Gateway ou Citrix Gateway Service. Pour plus d'informations sur l'activation de l'accès à distance aux espaces de travail, consultez Connectivité externe dans cet article.

Sinon, pour la connectivité interne uniquement, vous pouvez utiliser Citrix Workspace ou héberger un environnement StoreFront local. Pour la connectivité interne, le point de terminaison doit se connecter directement à l'adresse IP du Virtual Delivery Agent (VDA).

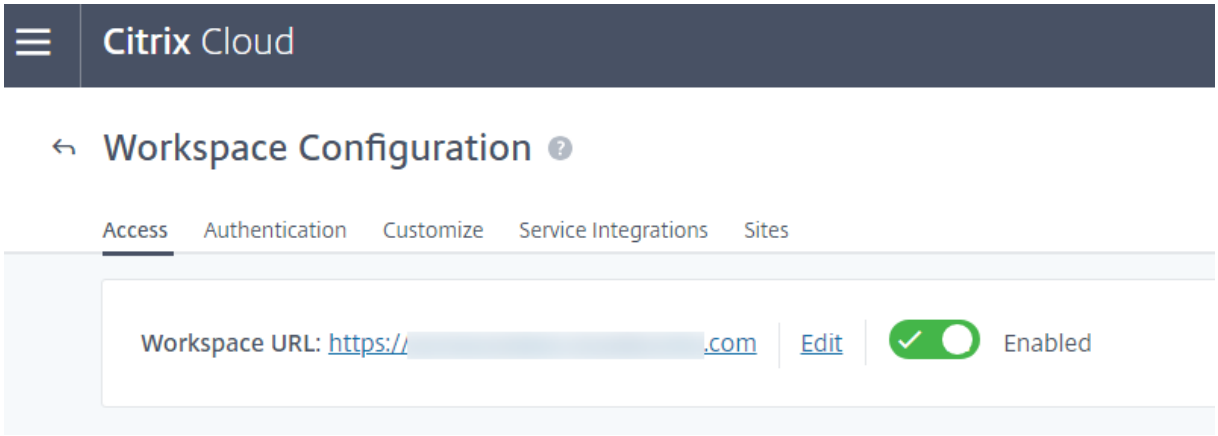
Citrix Workspace prend en charge une liste croissante de fournisseurs d'identité que vous connectez à Citrix Cloud, puis activez dans **Configuration de l'espace de travail** pour authentifier les abonnés à leurs espaces de travail. Pour plus d'informations sur la configuration de l'authentification pour les abonnés Workspace, consultez Authentification aux espaces de travail dans cet article

Citrix Workspace prend également en charge les options d'authentification suivantes :

- Utilisation de jetons comme deuxième facteur d'authentification pour la connexion à des espaces de travail avec Active Directory. Pour plus d'informations sur la configuration de l'authentification multifacteur (MFA) pour les espaces de travail, consultez Authentification à deux facteurs.
- Service d'authentification fédérée (FAS) de Citrix pour fournir une authentification unique auprès de DaaS dans Citrix Workspace. Pour plus d'informations sur la configuration SSO avec FAS, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

URL Workspace

L'URL de l'espace de travail est prête à être utilisée et se trouve dans **Citrix Cloud > Configuration de l'espace de travail > Accès**, où vous pouvez activer, modifier et désactiver l'URL de votre espace de travail.



Personnaliser l'URL de l'espace de travail

La première partie de l'URL de l'espace de travail est personnalisable. Vous pouvez modifier l'URL, par exemple, de `https://example.cloud.com` à `https://newexample.cloud.com`.

Vous ne pouvez modifier l'URL de l'espace de travail que lorsqu'elle est activée. Si l'URL est désactivée, vous devez d'abord la réactiver.

Pour activer l'URL de l'espace de travail, accédez à **Configuration de l'espace de travail > Accès** et sélectionnez l'option pour l'activer. La réactivation de l'URL de l'espace de travail peut prendre jusqu'à 10 minutes pour prendre effet.

La première partie de l'URL de l'espace de travail représente l'organisation qui utilise le compte Citrix Cloud et doit respecter le Contrat d'utilisateur final de Cloud Software Group. L'utilisation abusive des droits de propriété intellectuelle d'un tiers, y compris les marques, peut entraîner la révocation et la réaffectation de l'URL de l'espace de travail ou la suspension du compte Citrix Cloud.

Pour personnaliser votre URL, accédez à **Configuration de l'espace de travail > Accès** et sélectionnez **Modifier**. La partie personnalisable de l'URL doit répondre aux exigences suivantes :

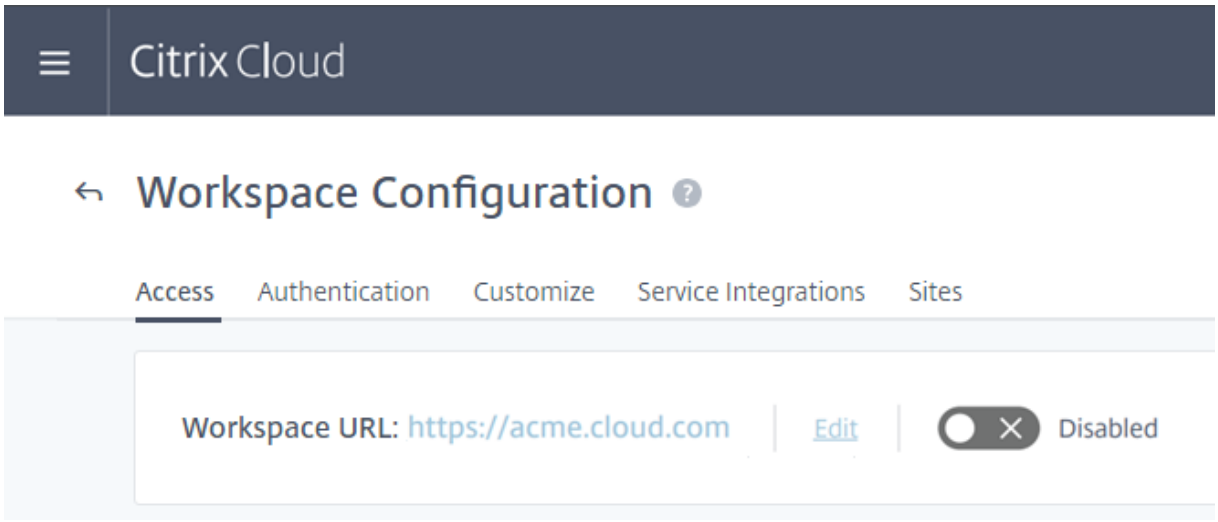
- La longueur doit être comprise entre 6 et 63 caractères. Si vous souhaitez modifier la partie personnalisable de l'URL en utilisant moins de 6 caractères, ouvrez un ticket dans Citrix Cloud.
- Elle doit être composée uniquement de lettres et de chiffres.
- Elle ne peut pas contenir de caractères Unicode.

Lorsque vous renommez une URL, l'ancienne URL est immédiatement supprimée et n'est plus

disponible. Vous devrez également leur communiquer la nouvelle URL et mettre à jour manuellement toutes les applications Citrix Workspace locales pour utiliser la nouvelle URL.

Désactiver l'URL de l'espace de travail

Vous pouvez désactiver l'URL de l'espace de travail pour empêcher les utilisateurs de s'authentifier via Citrix Workspace. Par exemple, vous pouvez préférer que les abonnés utilisent une URL Store-Front locale pour accéder aux ressources ou vous souhaitez empêcher l'accès pendant les périodes de maintenance.



La désactivation de l'URL de l'espace de travail peut prendre jusqu'à 10 minutes pour prendre effet.

La désactivation de l'URL de l'espace de travail a les effets suivants :

- Toutes les intégrations de services sont désactivées. Les abonnés n'ont pas accès aux données et applications de tous les services dans Citrix Workspace.
- Vous ne pouvez pas personnaliser l'URL de l'espace de travail. Vous devez réactiver l'URL avant de pouvoir la modifier.
- Toute personne accédant à l'URL reçoit un message dans son navigateur indiquant que l'espace de travail est introuvable ou que les ressources ne peuvent pas être chargées.

Application Citrix Workspace (anciennement Citrix Receiver)

> **Important :**
>
> Citrix Receiver est arrivé en fin de vie et n'est plus pris en charge. Si vous continuez à utiliser Citrix Receiver, le support technique est limité aux options décrites dans l'article Définitions des étapes du cycle de vie. Pour plus d'informations sur les étapes clés de fin de vie pour Citrix Receiver par plate-forme, reportez-vous à la section Étapes clés du cycle de vie de l'application

> Citrix Workspace et de Citrix Receiver

L'application Citrix Workspace est une application installée en mode natif qui remplace Citrix Receiver pour fournir l'accès aux espaces de travail.

Méthodes d'authentification prises en charge pour l'application Citrix Workspace

Le tableau suivant présente les méthodes d'authentification prises en charge par l'application Citrix Workspace. Le tableau inclut les méthodes d'authentification pertinentes pour des versions spécifiques de Citrix Receiver que l'application Citrix Workspace remplace.

Application Citrix Workspace	Authentification Active Directory	Authentification Active Directory + jeton	Authentification Azure Active Directory
Citrix Workspace pour Windows	Oui	Oui	Oui (application Workspace ; Receiver 4.9 LTSR CU2 et versions ultérieures uniquement ; Receiver 4.11 CR et versions ultérieures uniquement)
Citrix Workspace pour Linux	Oui	Oui	Oui (application Workspace ; Receiver 13.8 et versions ultérieures uniquement)
Citrix Workspace pour Mac	Oui	Oui	Oui
Citrix Workspace pour iOS	Oui	Oui	Oui
Citrix Workspace pour Android	Oui	Oui	Oui (application Workspace ; Receiver 3.13 et versions ultérieures uniquement)

Pour plus d'informations sur les fonctionnalités prises en charge dans l'application Citrix Workspace par plate-forme, reportez-vous au tableau des fonctionnalités de l'application Citrix Workspace.

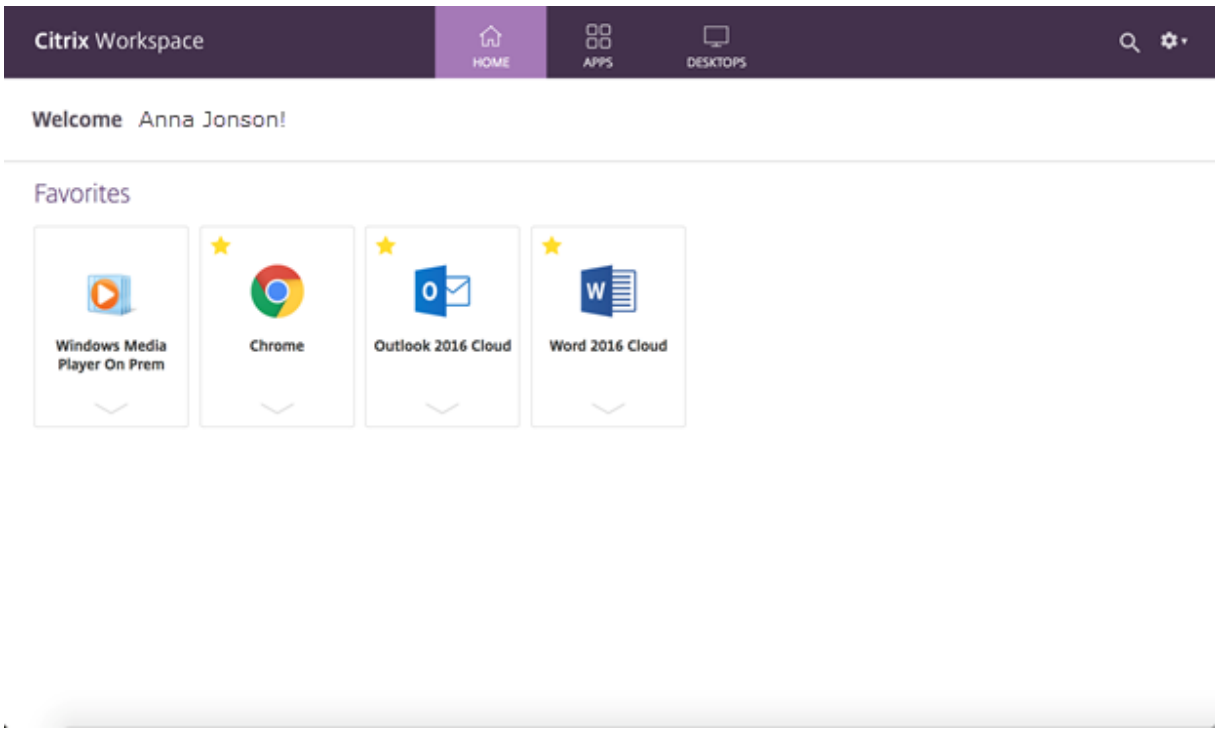
Pour obtenir une vue d'ensemble de la prise en charge de TLS et SHA2 avec les Citrix Receiver, consultez l'article d'assistance CTX23226.

Transition de l'application Citrix Receiver vers l'application Citrix Workspace

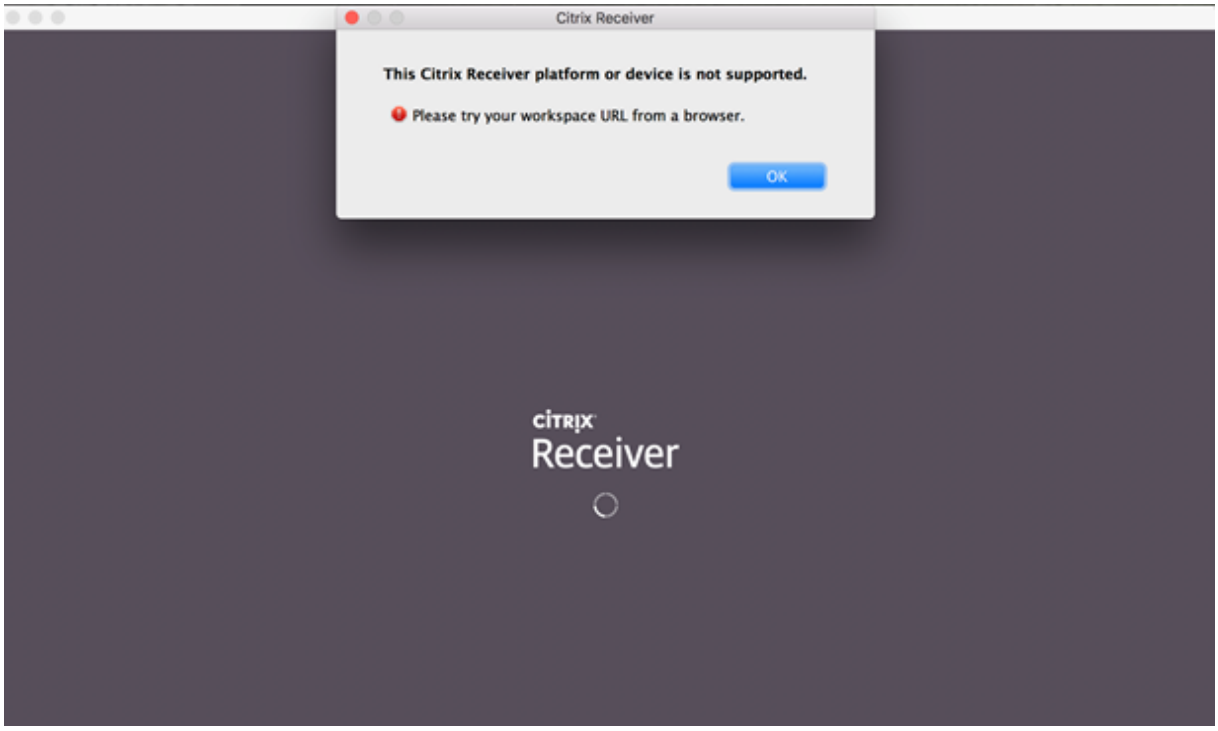
L'application Citrix Workspace remplace et étend les fonctionnalités de Citrix Receiver.

L'application Citrix Workspace offre aux abonnés un accès aux applications SaaS, Web et virtuelles avec une expérience d'authentification unique (SSO). Pour plus d'informations sur l'authentification unique (Single Sign-On) pour les abonnés à l'espace de travail, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

La fonctionnalité de contrôle d'accès n'est pas prise en charge dans Citrix Receiver. Ainsi, avec les mêmes services et le contrôle d'accès activés, les utilisateurs de Citrix Receiver voient toujours l'interface utilisateur de couleur mauve, mais sans applications Web et SaaS. En outre, le service **Files** n'est pas pris en charge dans Citrix Receiver et les abonnés ne peuvent pas y accéder de cette manière.



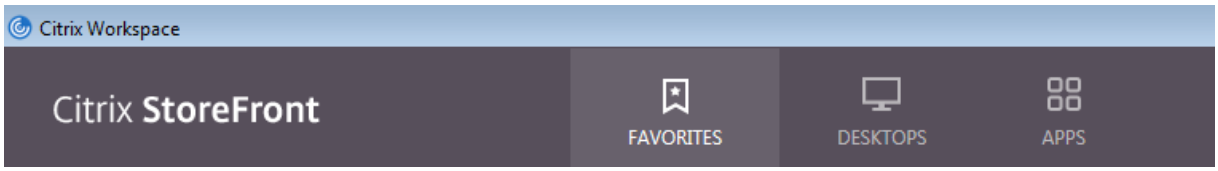
Azure Active Directory (AAD) n'est pas non plus compatible avec Citrix Receiver. Si les abonnés tentent d'accéder à Workspace avec Citrix Receiver alors qu'AAD est activé comme méthode d'authentification, ils voient un message indiquant que l'appareil n'est pas pris en charge. Une fois qu'ils effectuent une mise à niveau vers l'application Citrix Workspace, ils peuvent accéder à leurs espaces de travail.



Les clients qui effectuent une mise à niveau vers l'application Citrix Workspace (ou utilisent un navigateur Web) voient la nouvelle interface utilisateur. Pour plus d'informations sur l'expérience des abonnés avec cette interface utilisateur, consultez Gérer votre expérience d'espace de travail.

Outre une nouvelle interface utilisateur, l'application Citrix Workspace permet aux abonnés d'utiliser toutes les nouvelles fonctionnalités que vous avez activées. Les abonnés peuvent accéder à **Files**, afficher DaaS et accéder aux applications Web et SaaS via Citrix Gateway Service.

Si vous disposez d'un environnement local de StoreFront, la mise à niveau de Citrix Receiver vers l'application Citrix Workspace modifie uniquement l'icône permettant d'ouvrir l'application Citrix Workspace.



> **Remarque :**
>
> Les utilisateurs de Citrix Cloud Government continuent de voir l'interface utilisateur de couleur « mauve » lorsqu'ils utilisent l'application Workspace ou lors de l'accès à Workspace à partir d'un navigateur Web.

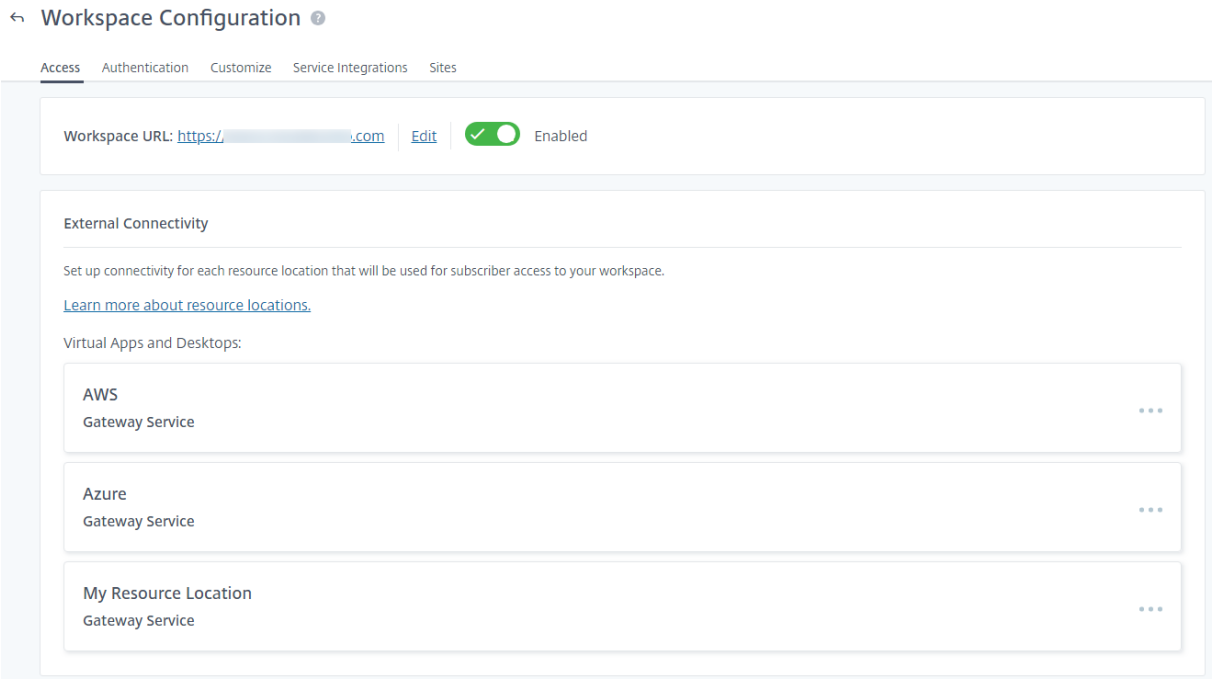
Connectivité externe

Fournissez un accès sécurisé aux abonnés distants en ajoutant des instances Citrix Gateway ou Citrix Gateway Service aux emplacements de ressources.

Citrix prend en charge les options de connectivité externe suivantes :

- Citrix héberge Citrix Gateway et Citrix ADC.
- Vous hébergez Citrix Gateway et Citrix ADC sur site.

Vous pouvez ajouter des Citrix Gateway à partir de **Configuration de l'espace de travail > Accès > Connectivité externe** ou à partir de **Citrix Cloud > Emplacements des ressources**.



> **Remarque :**
>
> La partie Connectivité externe de la page **Configuration de l'espace de travail > Accès** n'est pas disponible dans Citrix Virtual Apps Essentials. Citrix Virtual Apps Essentials Service utilise Citrix Gateway Service, qui ne nécessite aucune configuration supplémentaire.

Authentification aux espaces de travail

La configuration de l'authentification de l'espace de travail pour les abonnés comprend deux étapes :

1. Définissez un ou plusieurs fournisseurs d'identité dans **Gestion des identités et des accès**. Pour obtenir des instructions, consultez Gestion des identités et des accès.

2. Choisissez un de vos fournisseurs d'identité comme méthode d'authentification utilisée par les abonnés pour se connecter à leurs espaces de travail dans **Configuration de l'espace de travail**. Pour obtenir des instructions, consultez Choisir ou modifier les méthodes d'authentification.

La configuration d'autres fournisseurs d'identité dans **Gestion des identités et des accès** vous donne accès à davantage d'options dans **Configuration de l'espace de travail** pour déterminer comment les abonnés se connectent à leurs espaces de travail

Fournisseurs d'identité pris en charge pour l'authentification des abonnés

Les abonnés peuvent s'authentifier auprès de leurs espaces de travail à l'aide de l'une des méthodes suivantes :

- Active Directory
- Active Directory + jeton
- Azure Active Directory
- Citrix Gateway
- Okta
- SAML 2.0
- Google

Pour plus d'informations sur les méthodes prises en charge pour l'authentification des abonnés aux espaces de travail, consultez Espaces de travail sécurisés.

Pour utiliser Active Directory (AD), vous devez disposer d'au moins deux Citrix Cloud Connector installés dans le domaine AD local. Pour plus d'informations sur Citrix Cloud Connector, consultez Citrix Cloud Connector.

AD + Jeton est le fournisseur d'identité par défaut utilisé pour authentifier les abonnés aux espaces de travail. Les abonnés génèrent des jetons en tant que deuxième facteur d'authentification à l'aide de toute application qui respecte la norme TOTP (Time-Based One-Time Password), telle que Citrix SSO. Pour plus d'informations sur la configuration de l'authentification à deux facteurs basée sur des jetons, consultez Authentification à deux facteurs.

Changer de fournisseur d'identité

Vous devez choisir un fournisseur d'identité comme méthode d'authentification principale pour Citrix Workspace dans **Configuration de l'espace de travail**. Le fournisseur d'identité que vous choisissez doit d'abord être configuré dans **Gestion des identités et des accès**. La modification du fournisseur d'identité dans **Configuration de l'espace de travail** n'affecte pas les fournisseurs d'identité que vous avez configurés dans **Gestion des identités et des accès**.

La configuration des fournisseurs d'identité dans **Gestion des identités et des accès** ne modifie pas la méthode d'authentification principale pour la connexion à Citrix Workspace. Pour *modifier* la méthode d'authentification principale pour vous connecter à Citrix Workspace, vous devez :

1. Configurez le nouveau fournisseur d'identité dans **Gestion des identités et des accès**.
2. Modifiez le fournisseur d'identité dans **Configuration de l'espace de travail**.

Vous pouvez configurer et modifier votre méthode d'authentification principale pour Citrix Workspace sans perturber votre environnement de production. Si vous souhaitez tester le nouveau fournisseur d'identité, vous pouvez créer une organisation Citrix Cloud test ou prévoir de modifier la méthode d'authentification dans **Configuration de l'espace de travail** lorsque les abonnés n'utilisent pas leur espace de travail.

Authentification unique (SSO) pour les applications SaaS et Web

Citrix Workspace offre une expérience fluide permettant une authentification unique (SSO) pour les ressources secondaires une fois que l'abonné s'est connecté à son espace de travail. Associé à Citrix Gateway Service, Citrix Secure Private Access fournit une authentification unique pour les applications SaaS et Web en tant que partie intégrante de Citrix Workspace.

Outre les fonctionnalités d'authentification unique, Citrix Secure Private Access vous permet de définir des stratégies de sécurité améliorées, de configurer un accès contextuel et de collecter des analyses. Pour plus d'informations sur Citrix Secure Private Access, visitez Citrix Secure Private Access.

Authentification unique (SSO) vers DaaS

Outre les applications SaaS et Web, Active Directory (AD) et AD+Jeton fournissent déjà une authentification unique pour les applications et bureaux DaaS une fois que les abonnés se sont connectés à leur espace de travail.

Si vous sélectionnez un autre fournisseur d'identité pour l'authentification initiale de l'abonné auprès de Citrix Workspace, vous pouvez également installer et configurer le service d'authentification fédérée Citrix (FAS). Avec FAS, les abonnés saisissent leurs informations d'identification une seule fois pour accéder à leur DaaS, tout comme ils le font avec les applications SaaS et Web.

FAS est généralement l'option adoptée si l'un des fournisseurs d'identité suivants est utilisé pour l'authentification Workspace :

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

> **Remarque :**
>
> Selon la façon dont vous configurez Citrix Gateway, vous n'aurez peut-être pas besoin de FAS pour l'authentification unique avec DaaS. Pour plus d'informations sur la configuration de Citrix Gateway, consultez Créer une stratégie IdP OAuth sur Citrix Gateway local.

Pour plus d'informations sur FAS, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Informations supplémentaires

- Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix
- Architecture de référence : Service d'authentification fédérée
- Tech Insight : Service d'authentification fédérée

Configuration d'un domaine personnalisé

November 28, 2023

La configuration d'un domaine personnalisé pour votre espace de travail vous permet d'utiliser le domaine de votre choix pour accéder à votre magasin Citrix Workspace. Vous pouvez ensuite utiliser ce domaine à la place du domaine cloud.com qui vous a été attribué pour y accéder à la fois depuis un navigateur Web et des applications Citrix Workspace.

Un domaine personnalisé ne peut pas être partagé avec d'autres clients Citrix Workspace. Chaque domaine personnalisé doit être unique à ce client. Assurez-vous de choisir le domaine personnalisé que vous ne souhaitez pas attribuer à un autre client, à moins que vous ne souhaitiez le supprimer ultérieurement.

La désactivation de l'URL de Workspace dans Citrix Cloud ne désactive pas l'accès à Citrix Workspace via le domaine personnalisé. Pour désactiver l'accès à Citrix Workspace lors de l'utilisation d'un domaine personnalisé, désactivez également le domaine personnalisé.

Scénarios pris en charge

Scénarios	Pris en charge	Non pris en charge
Fournisseurs d'identité	AD (+ jeton), Azure AD, Citrix Gateway, Okta et SAML	Google
Types de ressources	Virtual Apps and Desktops	Applications SaaS
Méthodes d'accès	Navigateur (à l'exception d'Internet Explorer), application Citrix Workspace pour Windows, Mac, Linux et iOS	-
Utilisation	Workspace	Cloud Connector et console d'administration Cloud

En quoi est-elle différente de l'URL Workspace personnalisée actuelle ?

Si une URL Workspace personnalisée est déjà activée pour votre client, la vue suivante s'affiche.

Vous pouvez utiliser cette URL pour le moment et poursuivre les étapes décrites dans ce document pour intégrer une autre URL Workspace personnalisée. Elle sera dépréciée à l'avenir.

Si vous souhaitez utiliser la même URL, supprimez l'URL Workspace personnalisée précédente et supprimez tous les enregistrements DNS pour continuer.

Conditions préalables

- Vous pouvez choisir un domaine récemment enregistré ou un domaine que vous possédez déjà. Le domaine doit être au format sous-domaine (your.company.com). Citrix ne prend pas en charge l'utilisation d'un domaine racine uniquement (company.com).
- Citrix vous recommande d'utiliser un domaine dédié en tant que domaine personnalisé pour l'accès à Citrix Workspace, afin de pouvoir le modifier facilement si nécessaire.
- Les domaines personnalisés ne peuvent pas contenir de marques déposées Citrix. Vous trouverez la liste complète des marques déposées Citrix ici.
- Le domaine que vous choisissez doit être configuré dans le DNS public. Tous les noms et valeurs d'enregistrement CNAME inclus dans la configuration de votre domaine doivent pouvoir être résolus par Citrix.

> **Remarque :**
>
> Les configurations DNS privées ne sont pas prises en charge.

- La longueur du nom de domaine ne doit pas dépasser 64 caractères.

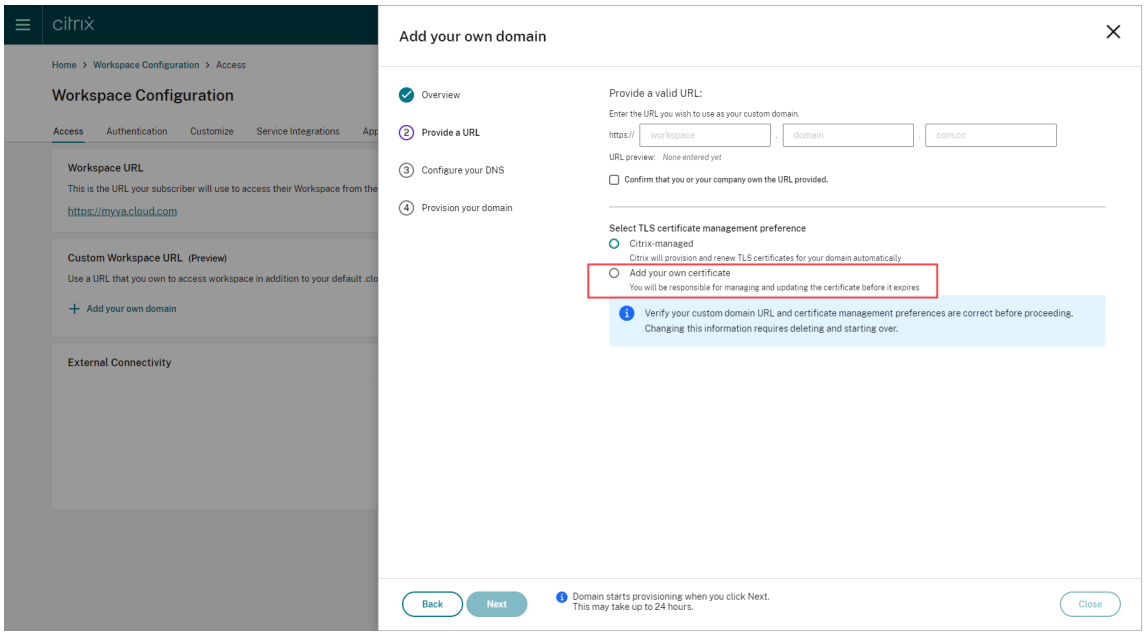
Configuration de votre domaine personnalisé

Une fois qu'un domaine personnalisé est défini, vous ne pouvez pas modifier l'URL ou le type de certificat. Vous pouvez uniquement le supprimer. Assurez-vous que le domaine que vous choisissez n'est pas déjà configuré dans le DNS. Supprimez tous les enregistrements **CNAME** existants avant de tenter de configurer votre domaine personnalisé.

Si vous utilisez le protocole SAML pour vous connecter à votre fournisseur d'identité, vous devez effectuer une étape supplémentaire pour terminer la configuration SAML. Pour plus d'informations, consultez SAML.

Ajouter un domaine personnalisé

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**, puis sélectionnez **Accès**.
3. Dans l'onglet **Accès**, sous **URL d'espace de travail personnalisée**, sélectionnez **+ Ajouter votre propre domaine**.



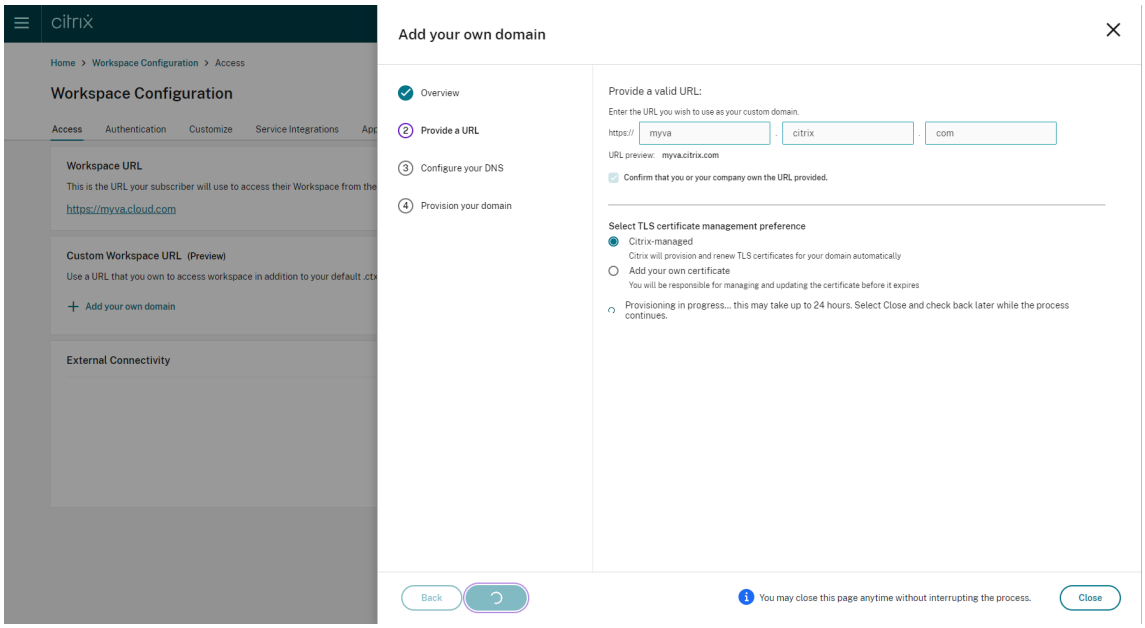
4. Lisez les informations affichées sur la page **Aperçu**, puis sélectionnez **Suivant**.
5. Entrez le domaine que vous avez choisi sur la page **Fournissez une URL**. Confirmez que vous êtes propriétaire du domaine spécifié en sélectionnant **Confirmez que vous ou votre entreprise êtes propriétaire de l'URL fournie**, puis choisissez vos préférences en matière de gestion des certificats TLS. Citrix recommande la méthode gérée, car les renouvellements de certificats

sont gérés pour vous. Pour plus d'informations, consultez la section Fournir un certificat renouvelé. Cliquez sur **Suivant**.

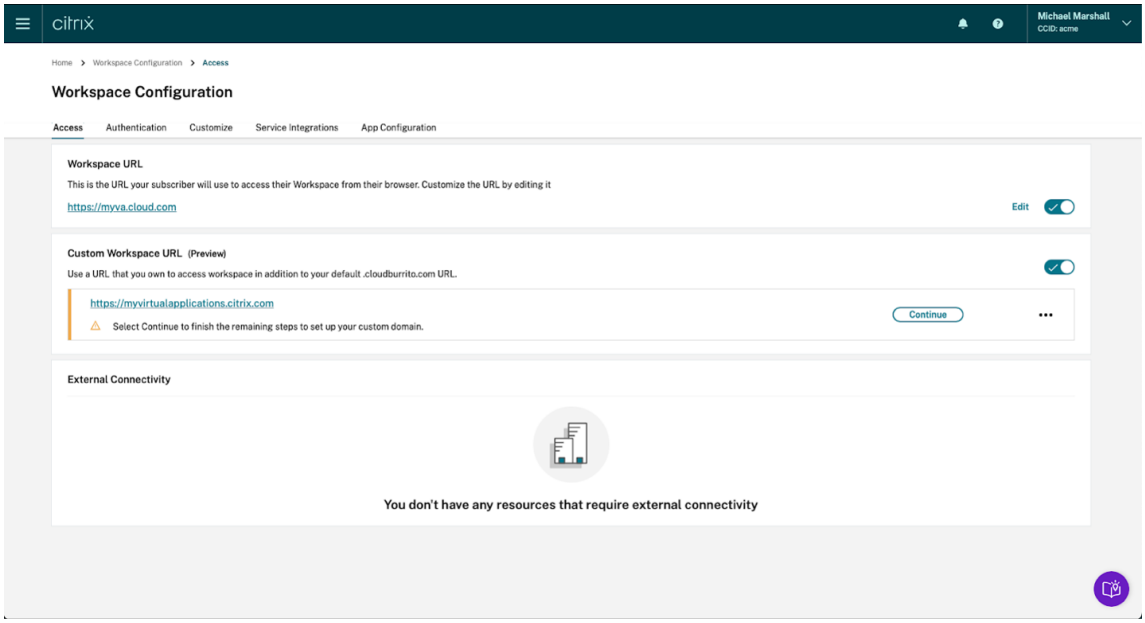
Si des avertissements apparaissent sur cette page, corrigez le problème surligné pour continuer.

Si vous avez choisi de fournir votre propre certificat, vous devez suivre une étape supplémentaire dans les instructions.

Le provisioning du domaine que vous avez choisi prend un certain temps. Vous pouvez attendre et rester sur la page ou la fermer pendant que le provisioning est en cours.



6. Si la page **Fournissez une URL** est ouverte alors que le provisioning se termine, la page **Configurez votre DNS** s'ouvre automatiquement. Si vous avez fermé la page, sélectionnez le bouton **Continuer** correspondant à votre domaine personnalisé dans l'onglet **Accès**.

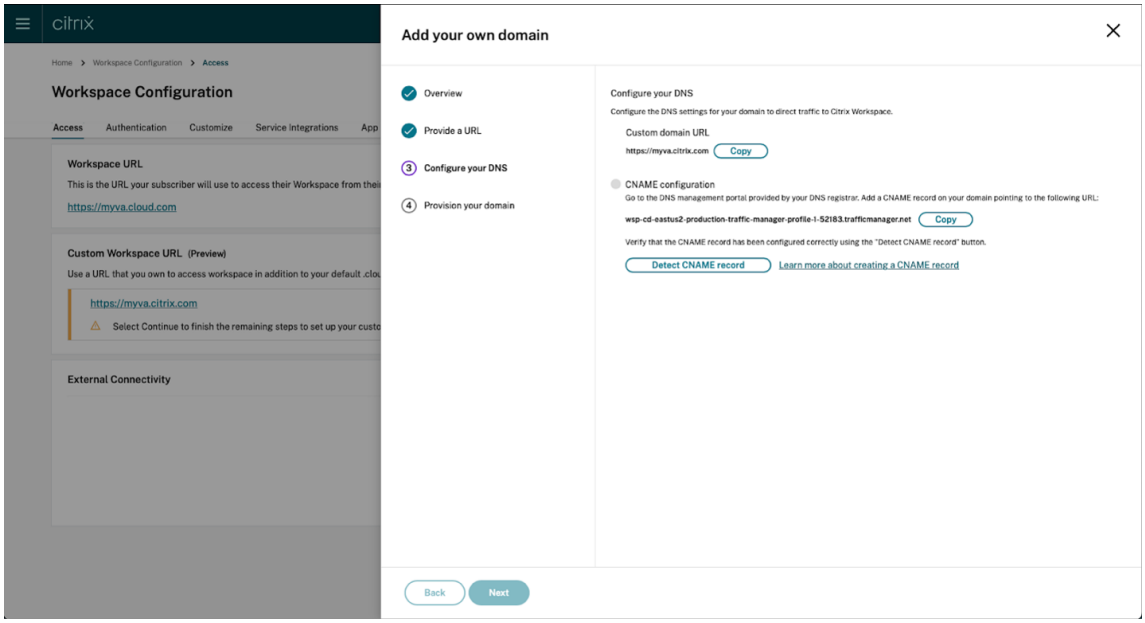


7. Effectuez cette étape sur le portail de gestion fourni par votre bureau d'enregistrement DNS. Ajoutez un enregistrement **CNAME** pour le domaine personnalisé de votre choix qui pointe vers le Azure Traffic Manager qui vous a été attribué.

   Copiez l'adresse du gestionnaire de trafic depuis la page **Configurez votre DNS**. Dans l'exemple, l'adresse est la suivante :

   wsp-cd-eastus2-production-traffic-manager-profile-1-52183.trafficmanager.net

   Si des enregistrements d'autorisation de l'autorité de certification (CAA) sont configurés dans votre DNS, ajoutez-en un qui permet à *Let's Encrypt* de générer des certificats pour votre domaine. *Let's Encrypt* est l'autorité de certification (CA) que Citrix utilise pour générer un certificat pour votre domaine personnalisé. La valeur de l'enregistrement CAA doit être la suivante : *0 issue "letsencrypt.org"*

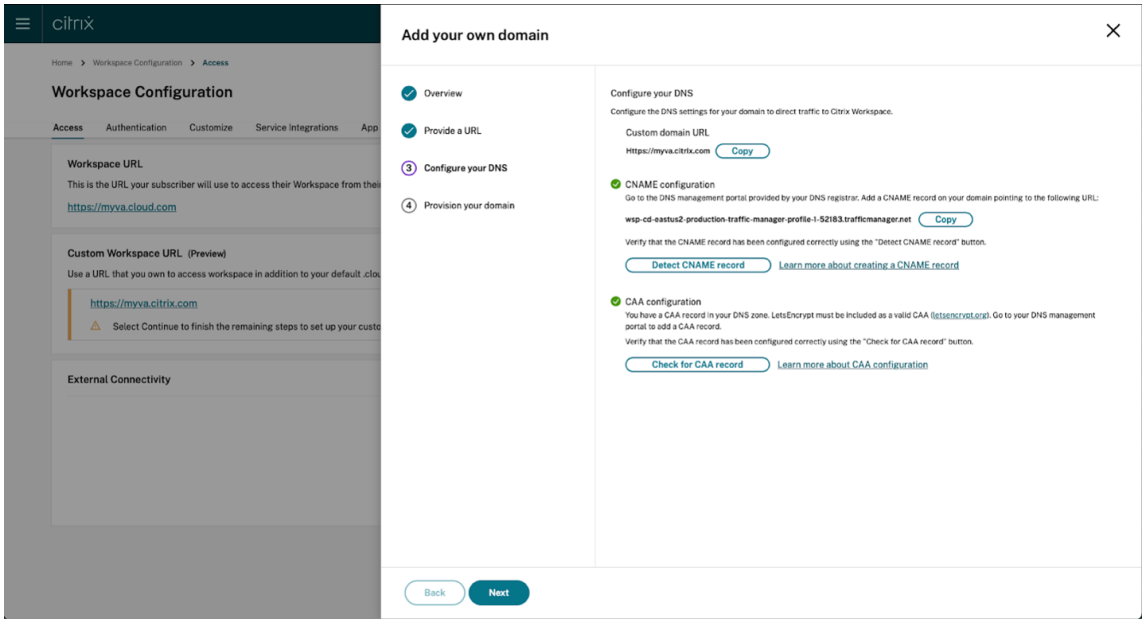


8. Une fois que vous avez configuré l'enregistrement CNAME avec votre fournisseur DNS, sélectionnez **Détecter enregistrement CNAME** pour vérifier que votre configuration DNS est correcte. Si l'enregistrement CNAME a été correctement configuré, une coche verte apparaît à côté de la section **Configuration de CNAME**.

   Si des avertissements apparaissent sur cette page, corrigez le problème pour continuer.

   Si vous avez configuré des enregistrements CAA avec votre fournisseur DNS, une **configuration CAA** distincte s'affiche. Sélectionnez **Détecter enregistrement CAA** pour vérifier que votre configuration DNS est correcte. Si la configuration de votre enregistrement CAA est correcte, une coche verte apparaît à côté de la section **Configuration de CAA**.

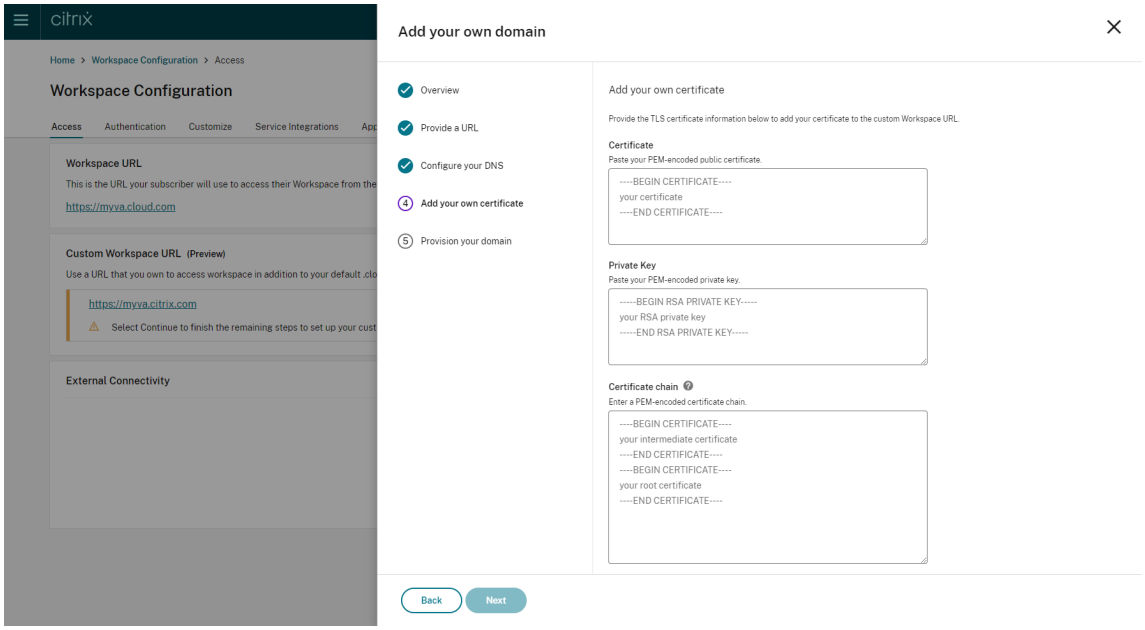
   Une fois votre configuration DNS vérifiée, cliquez sur **Suivant**.



9. **Il s'agit d'une étape facultative**. Si vous avez choisi d'ajouter votre propre certificat, complétez les informations requises sur la page **Ajouter votre propre certificat**.

   Si des avertissements apparaissent sur cette page, corrigez le problème surligné pour continuer. Assurez-vous que le certificat remplit les conditions suivantes.

   - Il doit être codé PEM.
   - Il devrait rester valide pendant encore au moins 30 jours.
   - Il doit être utilisé exclusivement pour l'URL personnalisée de l'espace de travail, les certificats génériques ne sont pas acceptables.
   - Le nom courant du certificat doit correspondre au domaine personnalisé.
   - Les SAN figurant sur le certificat doivent être destinés au domaine personnalisé. Aucun réseau SAN supplémentaire n'est autorisé.
   - La durée de validité du certificat ne doit pas dépasser 10 ans.



> **Remarque :**
>
> Citrix vous recommande d'utiliser un certificat utilisant une fonction de hachage cryptographique sécurisée (SHA 256 ou supérieur). Vous êtes responsable du renouvellement du certificat. Si votre certificat a expiré ou est sur le point d'expirer, consultez la section Fournir un certificat renouvelé.

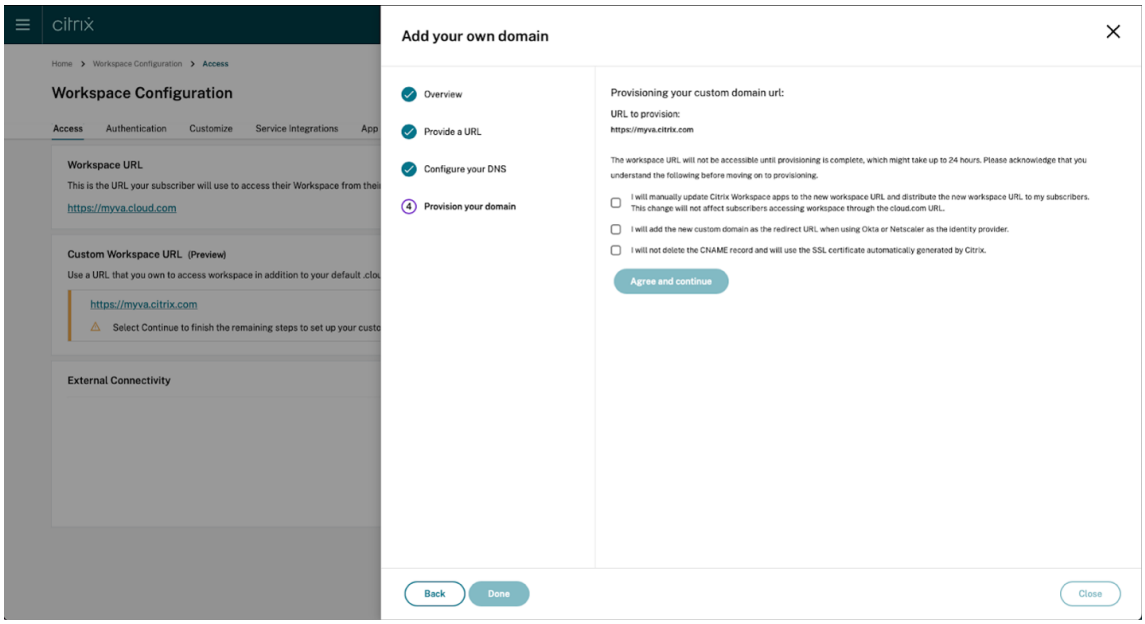
10. **Il s'agit d'une étape facultative.** Si vous utilisez SAML comme fournisseur d'identité, fournissez la configuration associée. Renseignez les informations requises sur la page **Configurer pour SAML**.

    Utilisez les informations suivantes lors de la configuration de l'application dans votre fournisseur d'identité :

Propriété	Valeur
Audience	`https://saml.cloud.com`
Destinataire	`https://<your custom domain>/saml/acs`
Validateur des URL ACS	`https://<your custom domain>/saml/acs`
URL des consommateurs ACS	`https://<your custom domain>/saml/acs`
URL de déconnexion unique	`https://<your custom domain>/saml/logout/callback`

11. Lisez les informations affichées sur la page **Provisionnez votre domaine** et confirmez avoir lu les instructions. Lorsque vous êtes prêt à continuer, sélectionnez **Accepter et continuer**.

    Cette dernière étape de provisioning peut prendre un certain temps. Vous pouvez attendre et rester sur la page jusqu'à la fin de l'opération ou fermer la page.



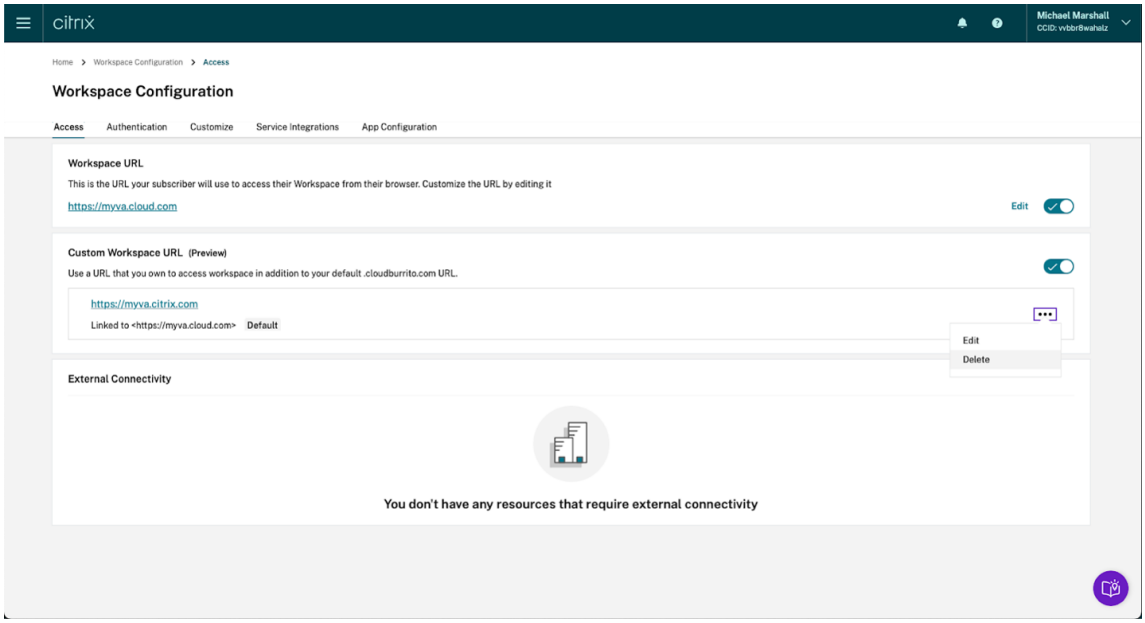
Supprimer un domaine personnalisé

La suppression d'un domaine personnalisé pour votre client supprime la possibilité d'accéder à Citrix Workspace à l'aide d'un domaine personnalisé. Après avoir supprimé le domaine personnalisé, vous ne pouvez accéder à Citrix Workspace qu'à l'aide de l'adresse cloud.com.

Lorsque vous supprimez un domaine personnalisé, assurez-vous que l'enregistrement CNAME est supprimé de votre fournisseur DNS.

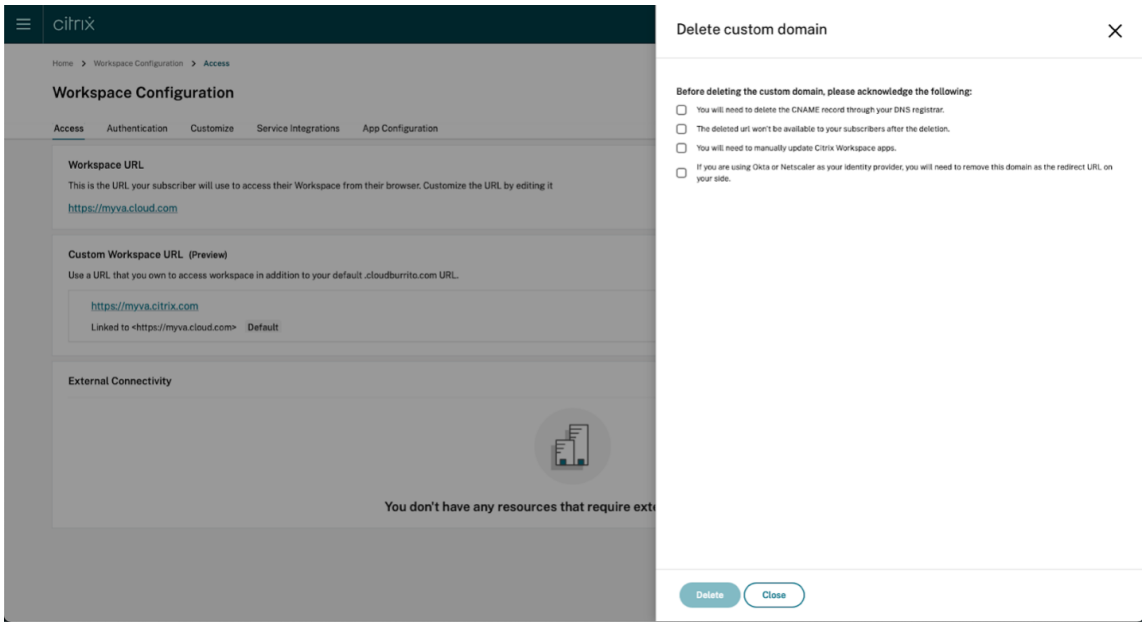
Pour supprimer un domaine personnalisé,

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail > Accès**.
3. Développez le menu contextuel **(...)** pour le domaine personnalisé dans l'onglet **Accès**, puis sélectionnez **Supprimer**.



4. Lisez les informations affichées sur la page **Supprimer domaine personnalisé** et confirmez avoir lu les instructions. Lorsque vous êtes prêt à continuer, sélectionnez **Supprimer**.

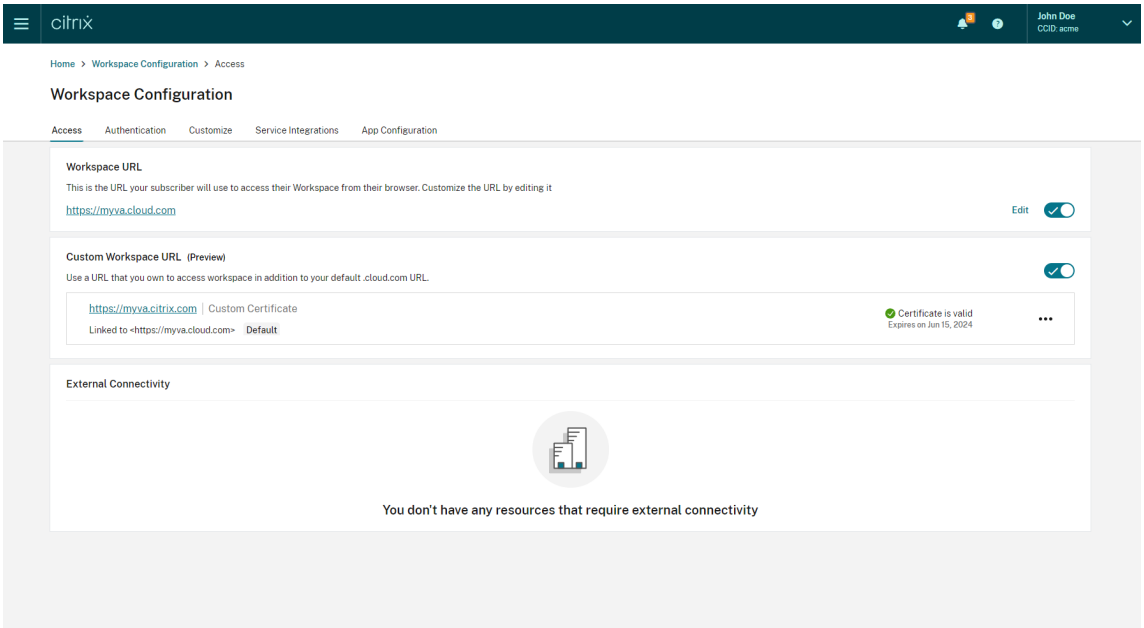
   La suppression d'un domaine personnalisé prend un certain temps. Vous pouvez attendre et rester sur la page jusqu'à la fin de l'opération ou fermer la page.



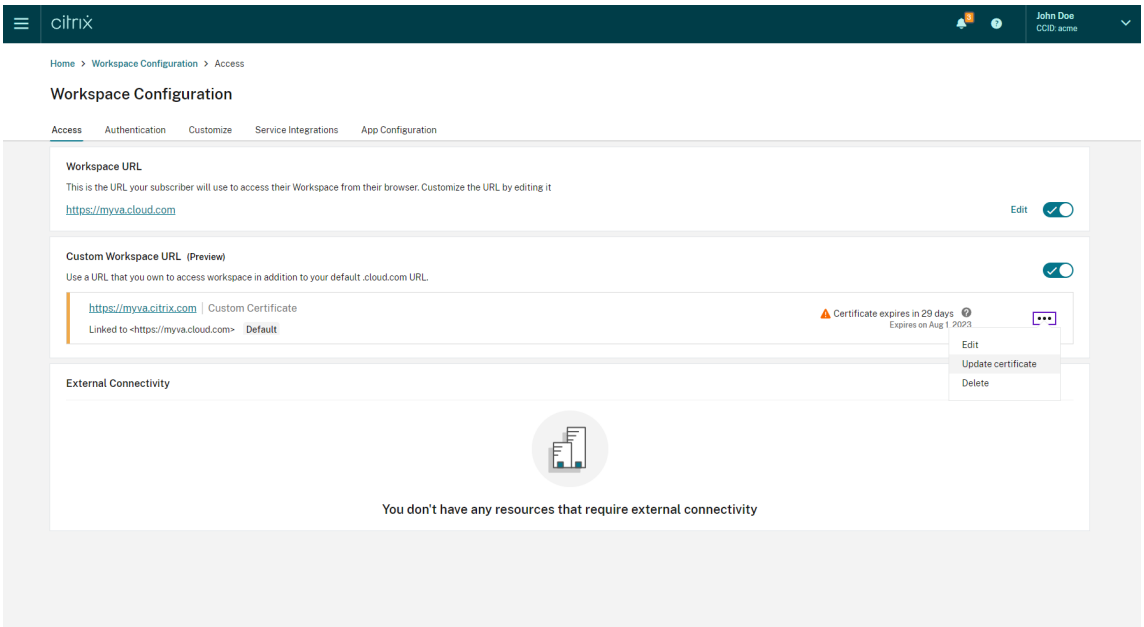
Fournir un certificat renouvelé

1. Connectez-vous à Citrix Cloud.
2. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail** > **Accès**.

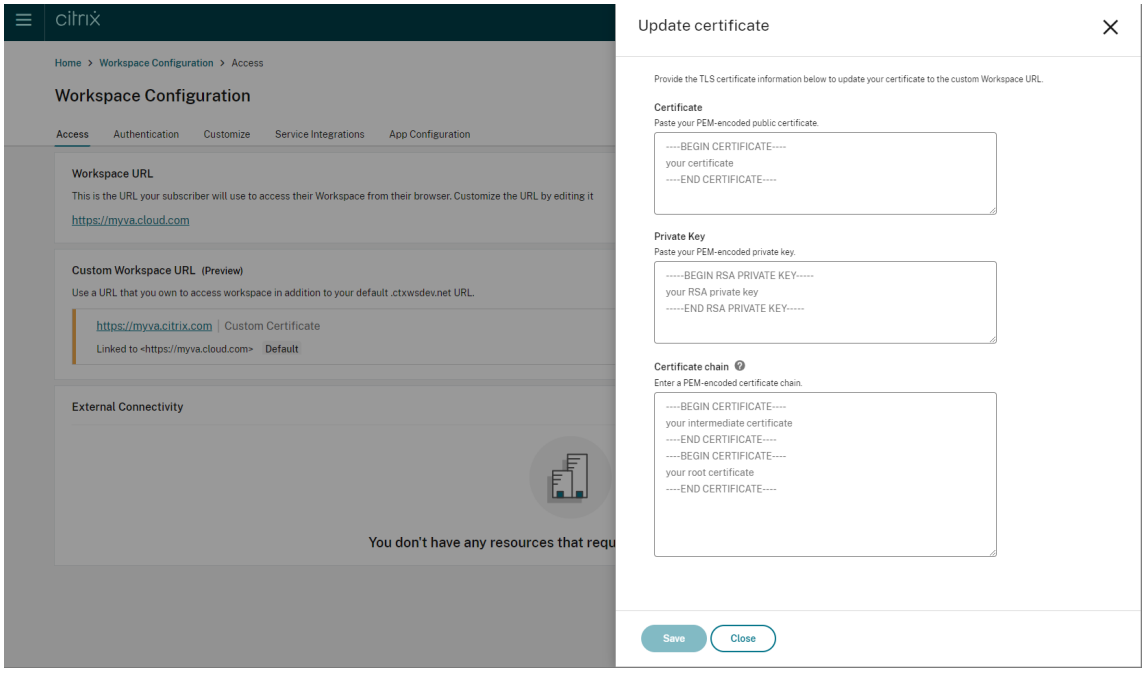
3. La date d'expiration du certificat sera affichée à côté du domaine personnalisé auquel il est attribué.



Lorsque votre certificat doit expirer dans un délai de 30 jours ou moins, votre domaine personnalisé affiche un avertissement.



4. Développez le menu contextuel **(...)** pour le domaine personnalisé dans l'onglet **Accès**. Sélectionnez **Mettre à jour le certificat**.



5. Entrez les informations requises sur la page **Mettre à jour le certificat**, puis sélectionnez **Enregistrer**.

Si des avertissements apparaissent sur cette page, corrigez le problème surligné pour continuer.

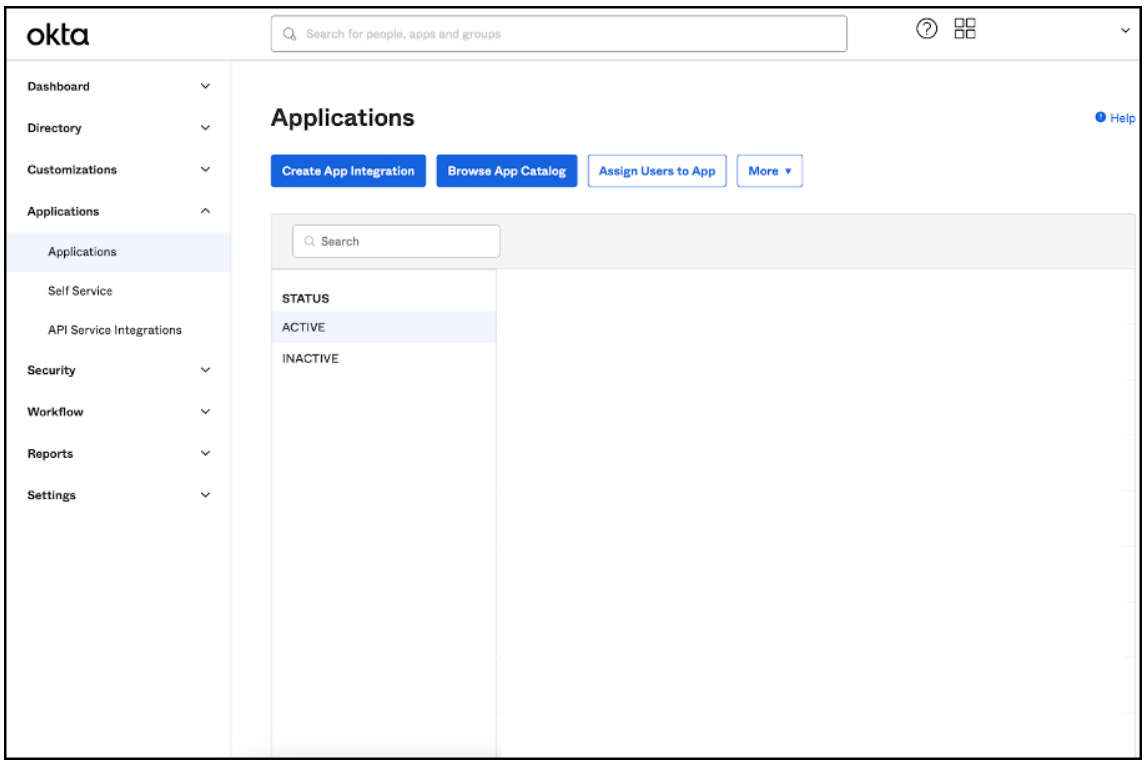
Le certificat doit répondre aux mêmes exigences que lors de la création du domaine personnalisé. Vous pouvez les vérifier dans Ajouter un domaine personnalisé.

Configuration de votre fournisseur d'identité

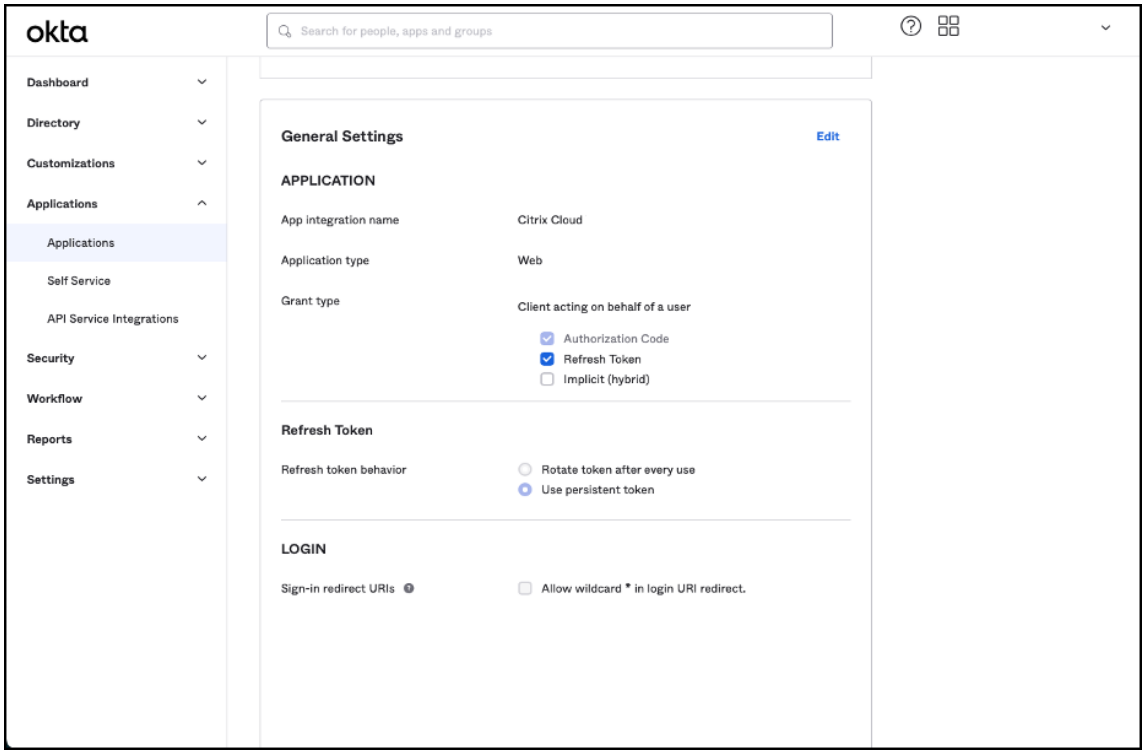
Configuration d'Okta

Procédez comme suit si vous utilisez Okta comme fournisseur d'identité pour l'accès à Citrix Workspace.

1. Connectez-vous au portail administrateur de votre instance Okta. Cette instance contient l'application utilisée par Citrix Cloud.
2. Développez **Applications**, puis sélectionnez **Applications** dans le menu.



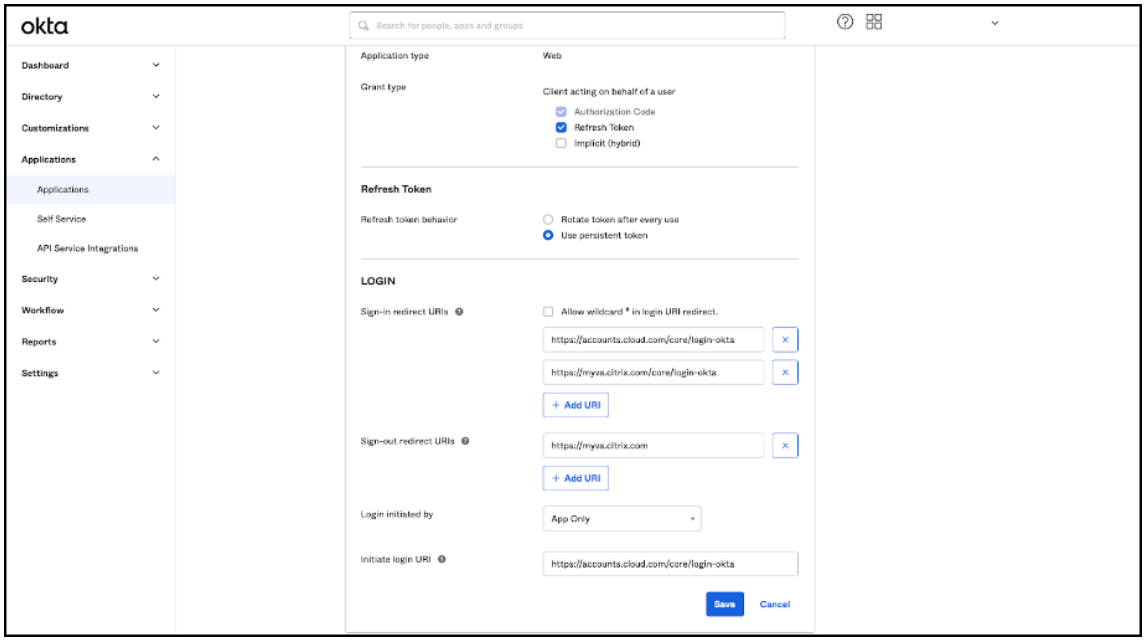
3. Ouvrez l'application liée à Citrix Cloud.
4. Sélectionnez **Edit** dans la section **General Settings**.



5. Dans la section **LOGIN** de **General Settings**, ajoutez une nouvelle valeur pour **Sign-in redirect**

URIs. Ajoutez la nouvelle valeur aux valeurs existantes et ne les remplacez pas. La nouvelle valeur doit être au format suivant : https://your.company.com/core/login-okta

6. Dans la même section, ajoutez une nouvelle valeur pour **Sign-out redirect URIs**. Ajoutez la nouvelle valeur aux valeurs existantes et ne les remplacez pas. La nouvelle valeur doit être au format suivant : https://your.company.com



7. Cliquez sur **Save** pour enregistrer la nouvelle configuration.

Configuration de stratégies et de profils OAuth

> **Important**
>
> La stratégie et le profil OAuth existants qui relient Citrix Cloud à Citrix Gateway ou à votre paire d'authentification adaptative HA ne doivent être mis à jour qu'en cas de perte des informations d'identification OAuth. La modification de cette stratégie risque de rompre le lien entre Citrix Cloud et des Workspace et d'affecter votre capacité à vous connecter à des Workspace.

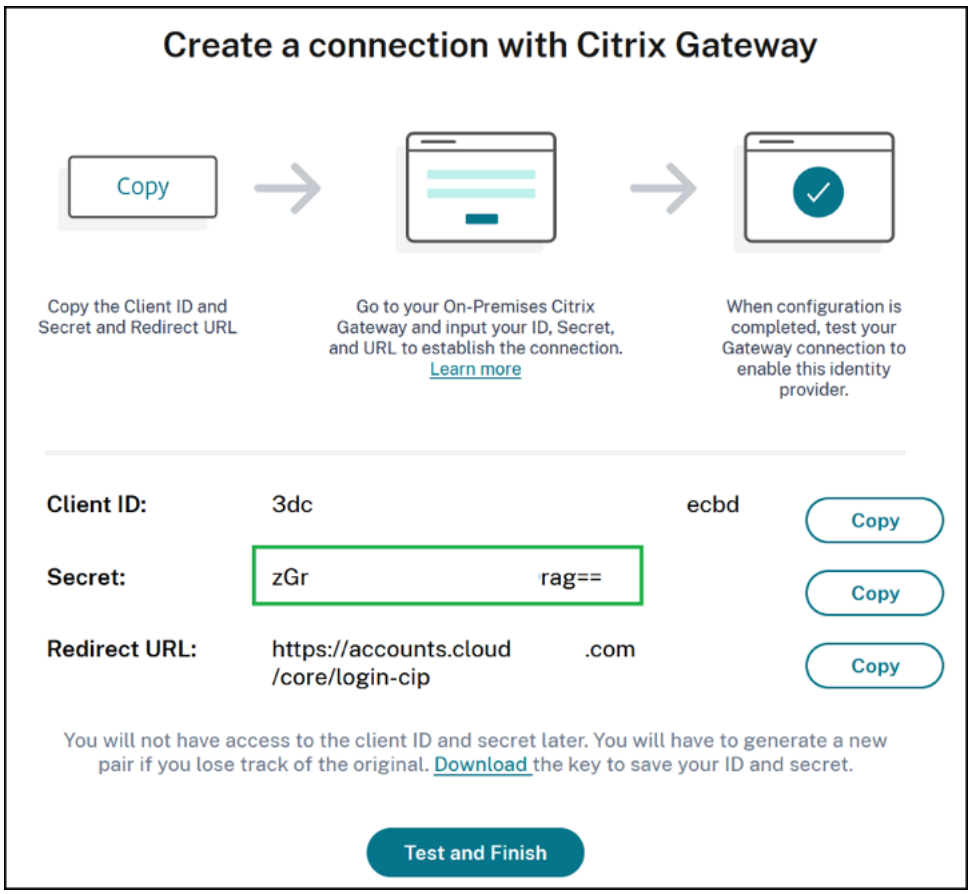
Configurer Citrix Gateway

L'administrateur de Citrix Cloud a accès à la clé secrète client non chiffrée. Ces informations d'identification sont fournies par Citrix Cloud lors du processus de liaison avec Citrix Gateway dans **Gestion des identités et des accès > Authentification**. Le profil et la stratégie OAuth ont été créés manuellement par l'administrateur Citrix sur Citrix Gateway au cours du processus de connexion.

Vous avez besoin de l'ID client et de la clé secrète client non chiffrée qui ont été fournis lors du processus de connexion à Citrix Gateway. Ces informations d'identification sont fournies par Citrix Cloud et

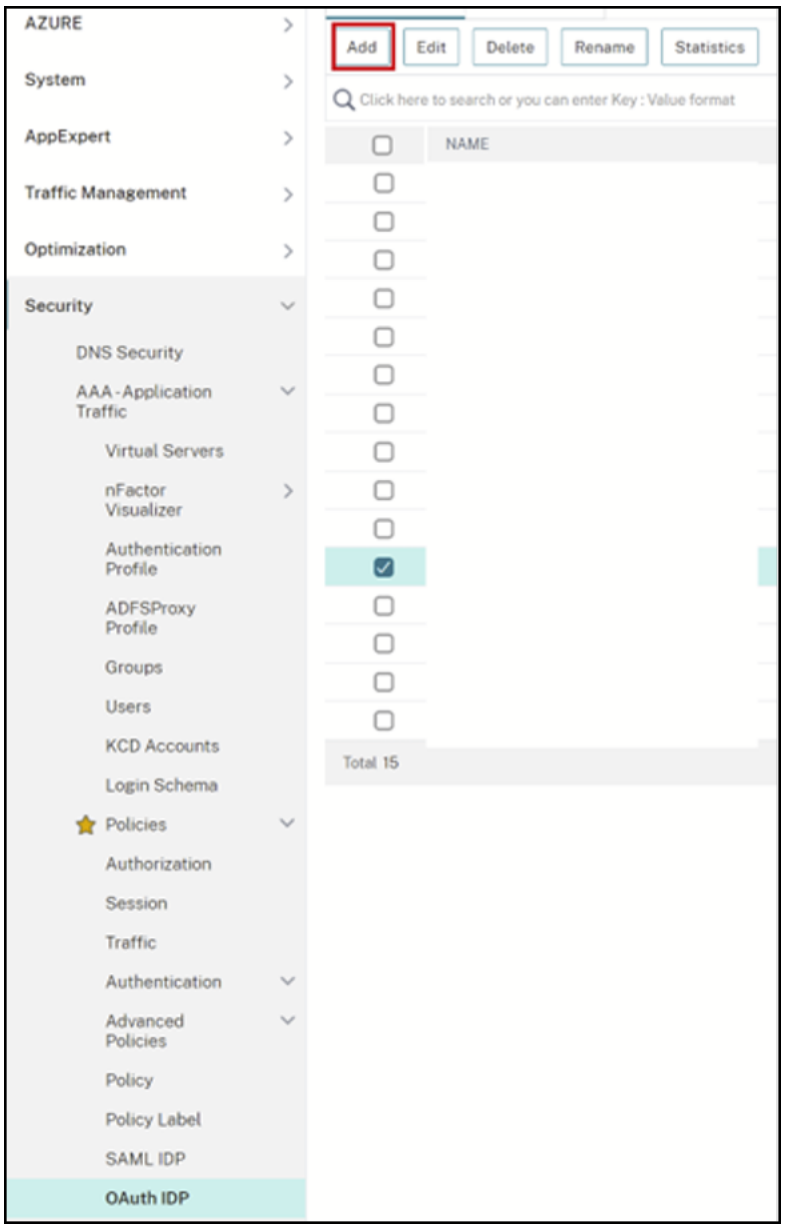
ont été enregistrées de manière sécurisée.
La clé secrète non chiffrée est nécessaire pour utiliser à la fois l'interface de Citrix ADC ou l'interface de ligne de commande (CLI) afin de créer une stratégie et un profil OAuth.

Voici un exemple d'interface utilisateur lorsque l'ID client et le secret sont fournis à l'administrateur Citrix. Si l'administrateur Citrix ne parvient pas à enregistrer les informations d'identification pendant le processus de connexion, il ne pourra pas obtenir une copie du secret non chiffré après la connexion de Citrix Gateway.

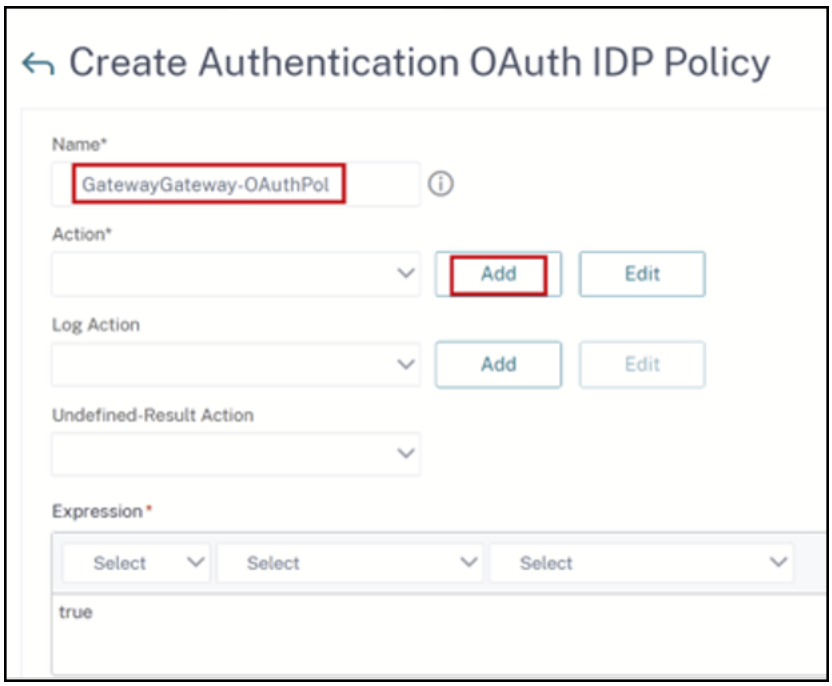


Utilisation de Citrix Cloud Procédez comme suit pour ajouter un profil et une stratégie OAuth supplémentaires à l'aide de l'interface de Citrix Gateway :

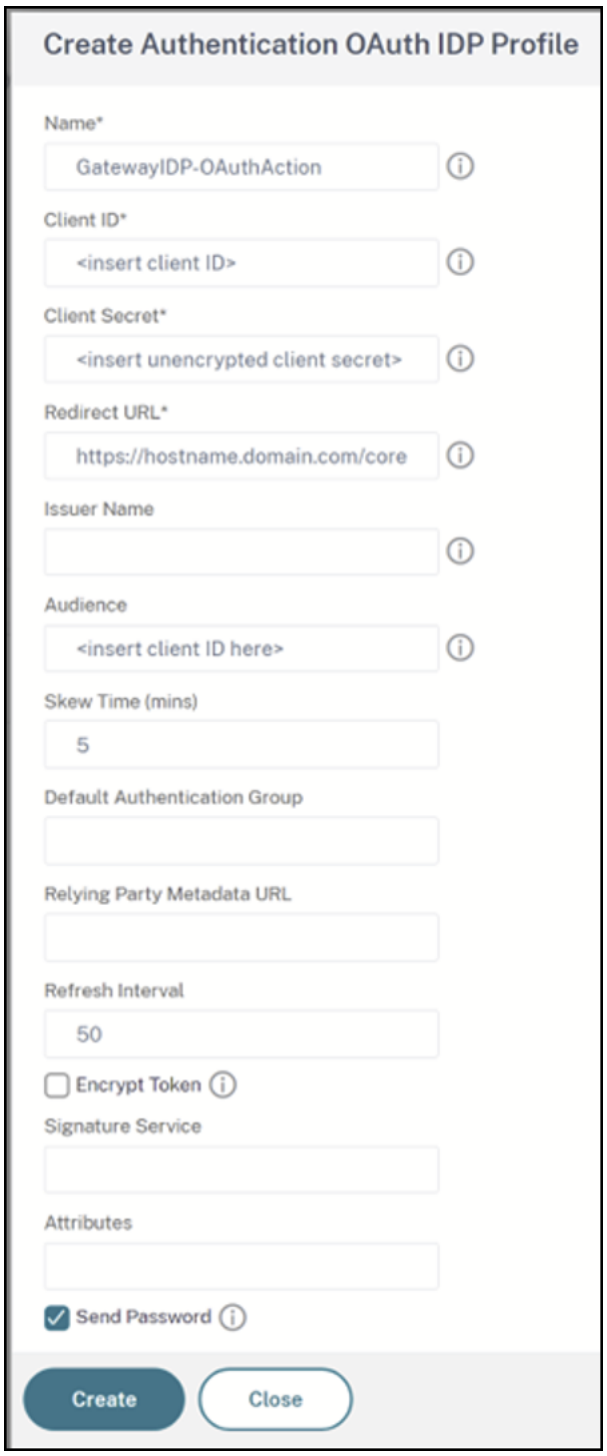
1. Dans le menu, sélectionnez **Security > AAA - Application Traffic > OAuth IDP.** Sélectionnez la stratégie OAuth existante et cliquez sur **Add**.



2. Lorsque vous y êtes invité, modifiez le nom de la nouvelle stratégie OAuth pour la différencier de la stratégie existante sélectionnée à l'étape précédente. Citrix suggère d'ajouter une *URL personnalisée* à son nom.



3. Sur l'interface graphique de Citrix Gateway, créez votre profil OAuth existant.
4. Dans le même menu de l'interface graphique, à côté de **Action**, cliquez sur **Add**.



5. Sur l'interface graphique de Citrix Gateway, liez la nouvelle stratégie OAuth à votre serveur virtuel d'authentification, d'autorisation et d'audit existant.
6. Accédez à **Security > Virtual Servers > Edit**.

À l'aide de l'interface de ligne de commande (CLI)

> **Important**
>
> Si aucune copie des informations d'identification OAuth n'est enregistrée de manière sécurisée, vous devez déconnecter puis reconnecter votre Citrix Gateway et mettre à jour votre profil OAuth existant avec les nouvelles informations d'identification OAuth fournies par la Gestion des identités et des accès de Citrix Cloud. Ne mettez à jour votre profil OAuth existant avec de nouvelles informations d'identification que si les anciennes informations d'identification sont irrécupérables. Ceci n'est pas recommandé sauf si vous n'avez pas d'autre choix.

1. Utilisez un outil SSH tel que PuTTY pour vous connecter à votre instance Citrix Gateway.
2. Créez OAuthProfile et OAuthPolicy. Ajoutez l'authentification OAuthIDPProfile.

   ```
   "CustomDomain-OAuthProfile"-clientID "<clientID>"-clientSecret "<unencrypted client secret>"-redirectURL "https://hostname.domain.com/core/login-cip"-audience "<clientID>"-sendPassword ON

   add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule true -action "CustomDomain-OAuthProfile"
   ```

3. Liez la OAuthPolicy au serveur virtuel d'authentification, d'autorisation et d'audit approprié avec une priorité inférieure à celle de la stratégie existante. Cette instance suppose que la stratégie existante a une priorité de 10, donc 20 est utilisé pour la nouvelle stratégie. Liez le serveur virtuel d'authentification.

   ```
   "CitrixGatewayAAAvServer"-policy "CustomDomain-OAuthPol"-priority 20
   ```

Configuration de l'authentification adaptative

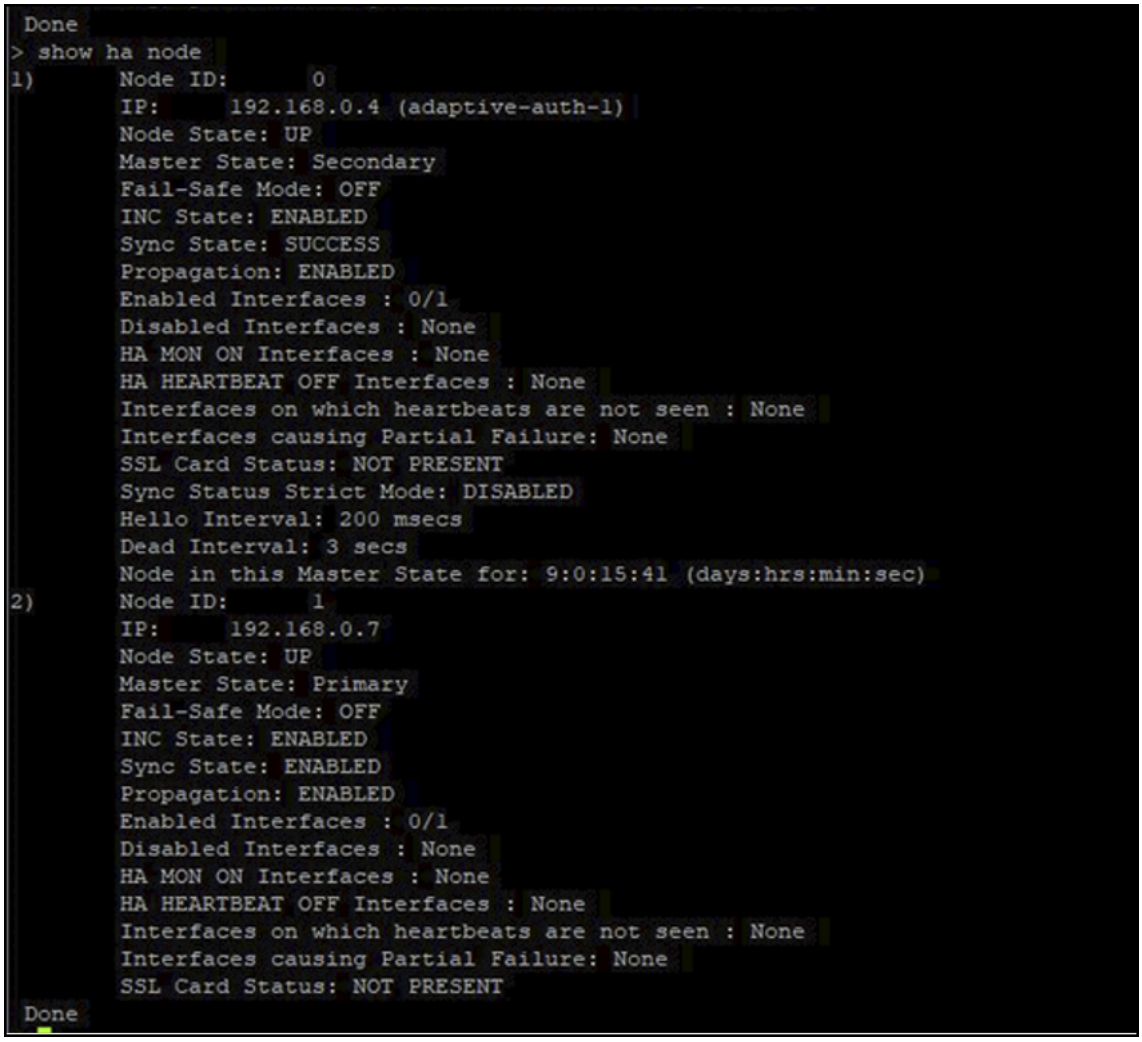
> **Important**
>
> La clé secrète chiffrée et les paramètres de chiffrement du profil OAuth sont différents sur les passerelles HA principales et secondaires d'authentification adaptative. Assurez-vous d'obtenir la clé secrète chiffrée auprès de la passerelle HA principale et exécutez également ces commandes sur la passerelle HA principale.

L'administrateur de Citrix Cloud n'a pas accès à la clé secrète client non chiffrée. La stratégie et le profil OAuth sont créés par le Citrix Adaptive Authentication Service pendant la phase de provisioning.

Il est nécessaire d'utiliser la clé secrète chiffrée et les commandes CLI obtenues à partir du fichier ns.conf pour créer des profils OAuth. Cela ne peut pas être effectué à l'aide de l'interface utilisateur de Citrix ADC. Liez la nouvelle URL personnalisée OAuthPolicy à votre serveur virtuel d'authentification, d'autorisation et d'audit existant en utilisant un niveau de priorité supérieur à celui de la stratégie existante liée à votre serveur virtuel d'authentification, d'autorisation et d'audit existant. Notez que les niveaux de priorité les moins élevés sont évalués en premier. Définissez la stratégie existante sur la priorité 10 et la nouvelle stratégie sur la priorité 20 pour vous assurer qu'elles sont évaluées dans le bon ordre.

1. Connectez-vous à votre nœud principal d'authentification adaptative à l'aide d'un outil SSH tel que PuTTY.

   ```
   show ha node
   ```

2. Localisez la ligne dans la configuration en cours de la passerelle HA principale contenant votre profil OAuth existant.

   ```
   sh runn | grep oauth
   ```


3. Copiez le résultat depuis l'interface de ligne de commande de Citrix ADC, y compris tous les paramètres de chiffrement.

4. Modifiez la ligne que vous avez copiée à l'étape précédente et utilisez-la pour créer une nouvelle commande CLI qui vous permettra de créer un profil OAuth à l'aide de la version chiffrée de l'ID client. Cela nécessite l'inclusion de tous les paramètres de chiffrement.

   - Mettez à jour le nom du profil OAuth sur *CustomDomain-OAuthProfile*
   - Mettez à jour -redirectURL sur https://hostname.domain.com/core/login-cip

   Voici un exemple après les deux mises à jour.

   ```
   add authentication OAuthIDPProfile "CustomDomain-OAuthProfile"-
   clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret <long
    encrypted client Secret> -encrypted -encryptmethod ENCMTHD_3
   -kek -suffix 2023_04_19_09_12_25 -redirectURL "https://hostname
   .domain.com/core/login-cip"-audience b1656835-20d1-4f6b-addd-1
   a531fd253f6 -sendPassword ON
   ```

   ```
   add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule
   true -action "CustomDomain-OAuthProfile"
   ```

5. Liez la OAuthPolicy au serveur virtuel d'authentification, d'autorisation et d'audit approprié avec une priorité inférieure à celle de la stratégie existante. Le nom du serveur virtuel d'authentification, d'autorisation et d'audit pour tous les déploiements de l'authentification adaptative est *auth_vs*. Cette instance suppose que la stratégie existante a une priorité de 10, donc 20 est utilisé pour la nouvelle stratégie.

   ```
   bind authentication vserver "auth_vs"-policy "CustomDomain-
   OAuthPol"-priority 20
   ```

Limitations connues

Les limites connues de la solution de domaine personnalisé sont les suivantes :

Plate-forme Workspace

- Ne prend actuellement en charge qu'un seul domaine personnalisé par client.
- Un domaine personnalisé ne peut être lié qu'à l'URL par défaut de Workspace. Les autres URL de Workspace ajoutées via la fonctionnalité multi-URL ne peuvent pas avoir de domaine personnalisé. La fonctionnalité multi-URL est actuellement disponible dans la version Private Tech Preview et n'est peut-être pas disponible pour tous les clients.

- Si vous avez configuré un domaine personnalisé sur la solution précédente et que vous utilisez SAML ou Azure AD pour authentifier l'accès à Citrix Workspace, vous **ne pouvez pas** configurer un domaine personnalisé sur la nouvelle solution sans **supprimer d'abord votre domaine personnalisé existant**.

SAML

La prise en charge de SAML est limitée à l'un des cas d'utilisation suivants :

- SAML peut être utilisé exclusivement pour les domaines cloud.com. Dans ce cas, l'utilisation de SAML couvrirait l'accès à Citrix Workspace et l'accès administrateur à Citrix Cloud.
- SAML peut être utilisé exclusivement pour un domaine personnalisé.

Application Citrix Workspace pour Windows

- Cette fonctionnalité n'est pas prise en charge dans les versions 2305 et 2307 de l'application Citrix Workspace pour Windows. Effectuez la mise à jour vers la dernière version prise en charge.

Espaces de travail sécurisés

October 12, 2023

En tant qu'administrateur, vous pouvez exiger que vos abonnés s'authentifient auprès de leurs espaces de travail à l'aide de l'une des méthodes d'authentification suivantes :

- Active Directory (AD)
- Active Directory + jeton
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

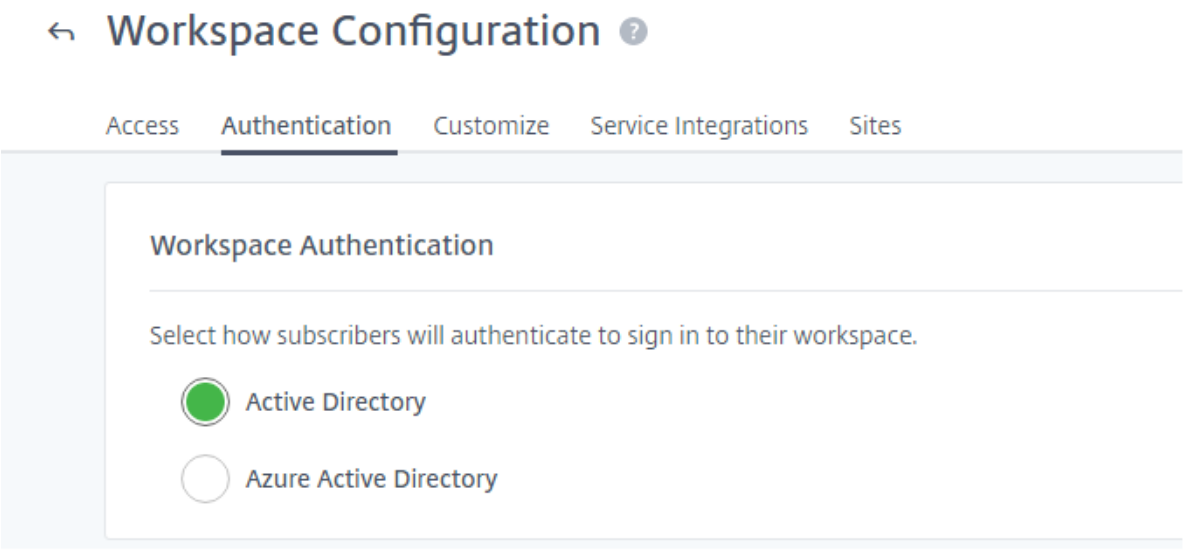
Ces options d'authentification sont disponibles pour tous les services Citrix Cloud. Pour plus d'informations, consultez Fiche technique : Identité Workspace.

Citrix Workspace prend aussi en charge l'utilisation du Service d'authentification fédérée Citrix (FAS) pour fournir l'authentification unique (SSO) à DaaS. Lorsque l'authentification unique est utilisée avec FAS, les abonnés n'ont plus besoin de s'authentifier auprès de DaaS une fois qu'ils sont connectés à leurs espaces de travail à l'aide d'une méthode d'authentification fédérée. Pour plus d'

informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Choisir ou modifier les méthodes d'authentification

Après avoir configuré vos fournisseurs d'identité, vous pouvez choisir ou modifier le mode d'authentification des abonnés auprès de leur espace de travail dans **Configuration de l'espace de travail > Authentification > Authentification de l'espace de travail**.



> **Important :**
>
> Le changement de mode d'authentification peut prendre jusqu'à cinq minutes et entraîne une interruption pour vos abonnés pendant cette période. Citrix recommande d'effectuer ces modifications uniquement pendant les périodes de faible utilisation. Si vous avez des abonnés connectés à Citrix Workspace à l'aide d'un navigateur ou d'une application Citrix Workspace, veuillez leur indiquer de fermer le navigateur ou de quitter l'application. Après avoir attendu environ cinq minutes, ils peuvent se reconnecter à l'aide de la nouvelle méthode d'authentification.

Active Directory (AD)

Par défaut, Citrix Cloud utilise Active Directory (AD) pour gérer l'authentification des abonnés aux espaces de travail.

Pour utiliser AD, vous devez disposer d'au moins deux Citrix Cloud Connector installés dans le domaine AD local. Pour plus d'informations sur l'installation de Cloud Connector, consultez Installation de Cloud Connector.

Active Directory (AD) + jeton

Pour plus de sécurité, Citrix Workspace prend en charge un jeton temporel en tant que deuxième facteur d'authentification pour la connexion AD.

Pour chaque connexion, Workspace invite les abonnés à entrer un jeton provenant d'une application d'authentification sur leur appareil inscrit. Avant de se connecter, les abonnés doivent inscrire leur appareil auprès d'une application d'authentification qui respecte la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO. Actuellement, les abonnés ne peuvent inscrire qu'un seul appareil à la fois.

Pour plus d'informations, consultez Tech Insight : Authentification - TOTP et Tech Insight : Authentification - Push.

Configuration requise pour AD + jeton

L'authentification Active Directory + jeton répond aux exigences suivantes :

- Une connexion entre Active Directory et Citrix Cloud, avec au moins deux Cloud Connector installés dans votre environnement local. Pour connaître les exigences et les instructions, consultez Connecter Active Directory à Citrix Cloud.
- Authentification **Active Directory + jeton** activée sur la page **Gestion des identités et des accès**. Pour plus d'informations, consultez Activer l'authentification Active Directory + jeton.
- Accès des abonnés à la messagerie électronique pour inscrire des appareils.
- Appareil sur lequel télécharger l'application d'authentification.

Première inscription

Les abonnés peuvent inscrire leurs appareils en utilisant le processus d'inscription décrit à la section Enregistrer les appareils pour l'authentification à deux facteurs.

Lors de la première connexion à Workspace, les abonnés suivent les invites pour télécharger l'application Citrix SSO. L'application Citrix SSO génère un mot de passe unique sur un appareil inscrit toutes les 30 secondes.

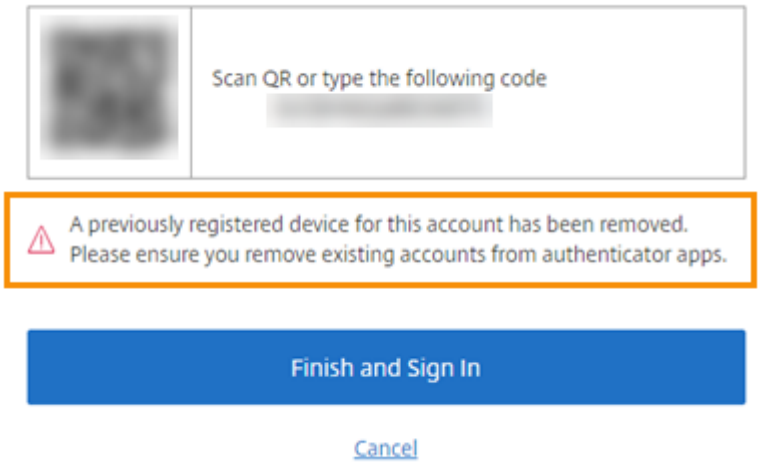
> **Important :**
>
> Pendant le processus d'inscription de l'appareil, les abonnés reçoivent un e-mail contenant un code de vérification temporaire. Ce code temporaire est utilisé uniquement pour inscrire l'appareil de l'abonné. L'utilisation de ce code temporaire comme jeton pour se connecter à Citrix Workspace avec l'authentification à deux facteurs n'est pas prise en charge. Seuls les codes de

> vérification générés à partir d'une application d'authentification sur un appareil inscrit sont pris en charge pour l'authentification à deux facteurs.

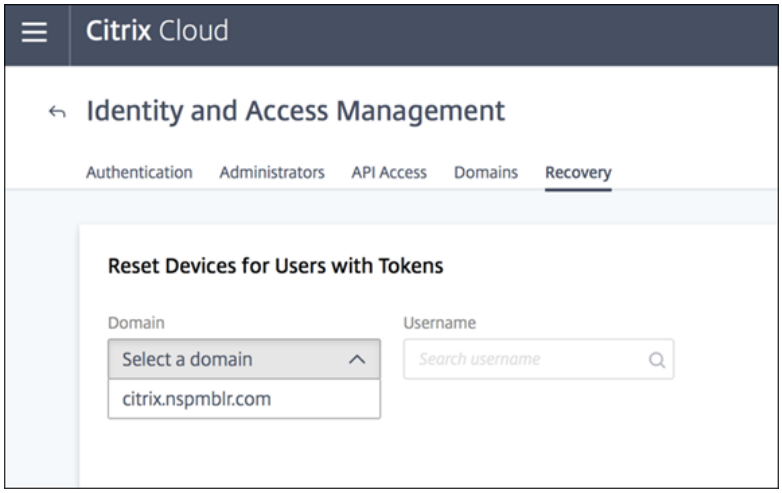
Réinscrire un appareil

Si un abonné n'a plus son appareil inscrit ou doit le réinscrire (par exemple, après avoir effacé le contenu de l'appareil), Workspace propose les options suivantes :

- Les abonnés peuvent réinscrire leurs appareils en utilisant le même processus d'inscription décrit à la section Enregistrer les appareils pour l'authentification à deux facteurs. Étant donné que les abonnés ne peuvent inscrire qu'un seul appareil à la fois, l'inscription d'un nouvel appareil ou la réinscription d'un appareil existant supprime l'enregistrement précédent de l'appareil.



- Les administrateurs peuvent rechercher des abonnés par nom Active Directory et réinitialiser leur appareil. Pour ce faire, accédez à **Gestion des identités et des accès > Récupération**. Lors de la prochaine connexion à Workspace, l'abonné suit les étapes effectuées lors de la première inscription.



Azure Active Directory

L'utilisation d'Azure Active Directory (AD) pour gérer l'authentification des abonnés aux espaces de travail satisfait aux exigences suivantes :

- Azure AD avec un utilisateur disposant d'autorisations d'administrateur général. Pour plus d'informations sur les applications Azure AD et les autorisations utilisées par Citrix Cloud, consultez Autorisations Azure Active Directory pour Citrix Cloud.
- Un Citrix Cloud Connector installé dans le domaine Active Directory local. La machine doit également être jointe au domaine qui se synchronise avec Azure AD.
- VDA version 7.15.2000 LTSR CU VDA ou version actuelle 7.18 ou supérieure.
- Une connexion entre Azure AD et Citrix Cloud. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud.

Lors de la synchronisation de votre Active Directory avec Azure AD, les entrées UPN et SID doivent être incluses dans la synchronisation. Si ces entrées ne sont pas synchronisées, certains workflows échoueront dans Citrix Workspace.

> **Avertissement :**
>
> - Si vous utilisez Azure AD, ne modifiez pas le Registre comme décrit dans l'article CTX225819. Cette modification peut entraîner l'échec du lancement de sessions pour les utilisateurs Azure AD.
> - L'ajout d'un groupe en tant que membre d'un autre groupe (imbrication) est prise en charge lorsque la fonctionnalité `DSAuthAzureAdNestedGroups` est activée. Vous pouvez activer `DSAuthAzureAdNestedGroups` en soumettant une demande auprès du support Citrix.

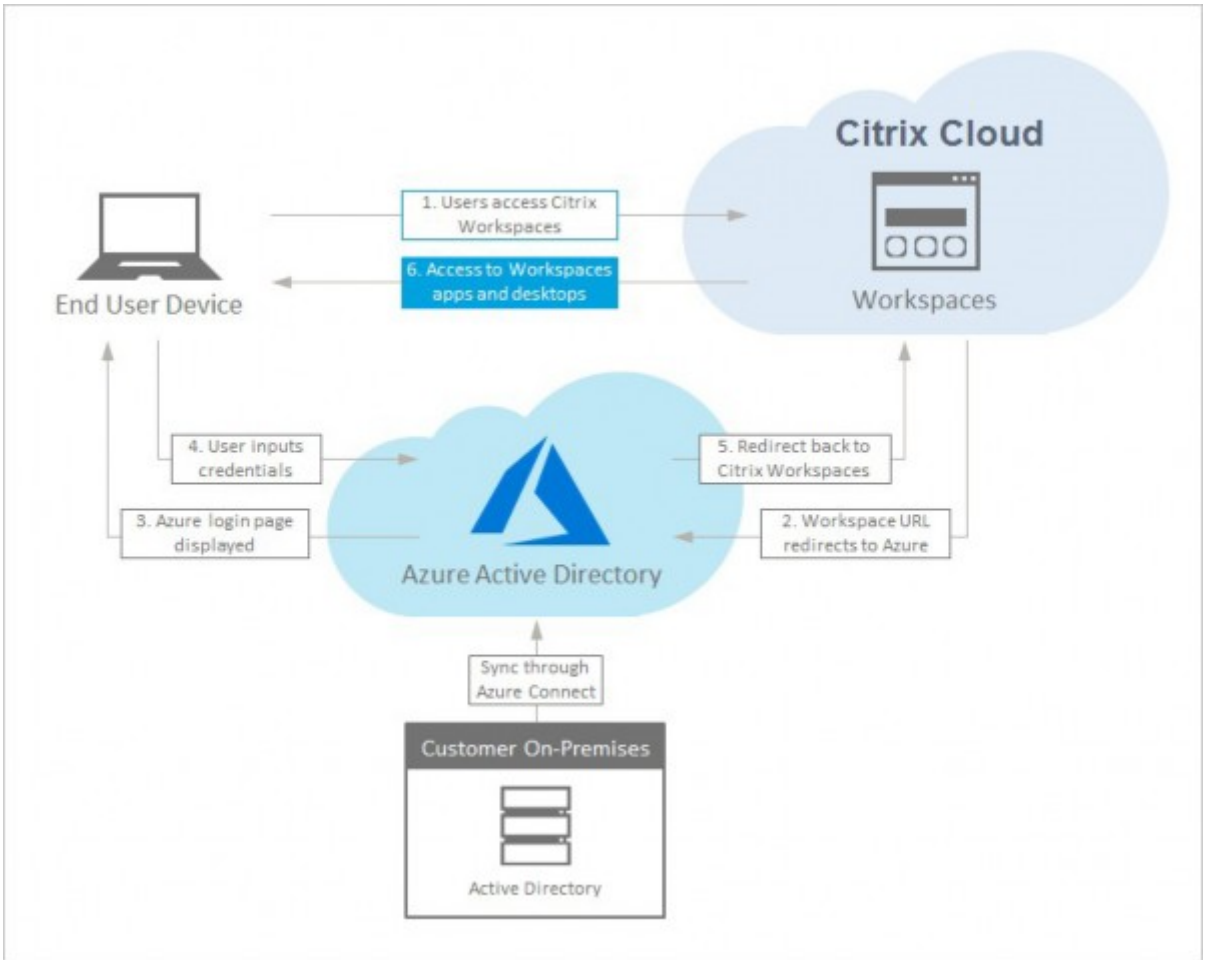
Après l'activation de l'authentification Azure AD :

- **Sécurité accrue :** pour plus de sécurité, les utilisateurs sont invités à se reconnecter lorsqu'ils lancent une application ou un bureau. Les informations de mot de passe circulent directement de l'appareil de l'utilisateur vers le VDA qui héberge la session.
- **Expérience de connexion :** l'authentification Azure AD fournit une connexion fédérée, et non une authentification unique (SSO). Les abonnés se connectent à partir d'une page de connexion Azure et devront peut-être s'authentifier à nouveau lors de l'ouverture de Citrix DaaS.

Pour l'authentification unique (SSO), activez le Service d'authentification fédérée Citrix dans Citrix Cloud. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Vous pouvez personnaliser l'expérience de connexion pour Azure AD. Pour de plus amples informations, veuillez consulter la documentation Microsoft. Les personnalisations de connexion (logo) effectuées dans la configuration de Workspace n'affectent pas l'expérience de connexion d'Azure AD.

Le diagramme suivant montre la séquence de l'authentification Azure AD.



Citrix Gateway

Citrix Workspace prend en charge l'utilisation d'une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour gérer l'authentification des abonnés sur les espaces de travail. Pour plus d'informations, consultez Tech Insight : Authentification - Citrix Gateway.

Configuration requise pour Citrix Gateway

L'authentification Citrix Gateway a les conditions requises suivantes :

- Une connexion entre votre Active Directory et Citrix Cloud. Pour connaître les exigences et les instructions, consultez Connecter Active Directory à Citrix Cloud.
- Les abonnés doivent être des utilisateurs Active Directory pour pouvoir se connecter à leurs espaces de travail.
- Si vous configurez une fédération, vos utilisateurs AD doivent être synchronisés avec le fournisseur de fédération. Citrix Cloud requiert les attributs AD pour permettre aux utilisateurs de se connecter correctement.
- une passerelle Citrix Gateway locale :
  - Citrix Gateway 12.1 54.13 Édition Advanced ou ultérieure
  - Citrix Gateway 13.0 41.20 Édition Advanced ou ultérieure
- L'authentification **Citrix Gateway** est activée sur la page **Gestion des identités et des accès**. Cette action génère l'ID client, le secret et l'URL de redirection nécessaires pour créer la connexion entre Citrix Cloud et votre passerelle Gateway locale.
- Sur Gateway, une stratégie d'authentification de fournisseur d'identité OAuth est configurée à l'aide de l'ID client, du secret et de l'URL de redirection générés.

Pour plus d'informations, consultez Connecter une passerelle Citrix Gateway locale en tant que fournisseur d'identité à Citrix Cloud.

Expérience de l'abonné avec Citrix Gateway

Lorsque l'authentification avec Citrix Gateway est activée, le flux de travail est le suivant pour les abonnés :

1. L'abonné accède à l'URL de Workspace dans son navigateur ou lance l'application Workspace.
2. L'abonné est redirigé vers la page d'ouverture de session Citrix Gateway et est authentifié à l'aide de toute méthode configurée sur Gateway, par exemple, MFA, fédération, stratégies d'accès conditionnel, etc. Vous pouvez personnaliser la page d'ouverture de session Gateway afin qu'elle ressemble à la page de connexion Workspace à l'aide des étapes décrites à la section CTX258331.

3. Une fois que l'authentification a réussi, l'espace de travail de l'abonné apparaît.

Google

Citrix Workspace prend en charge l'utilisation de Google en tant que fournisseur d'identité pour gérer l'authentification des abonnés sur les espaces de travail.

Configuration requise pour Google

- Une connexion entre votre Active Directory local et Google Cloud.
- Un compte développeur avec accès à la console Google Cloud Platform. Ce compte est requis pour créer un compte de service et une clé, et pour activer Admin SDK API.
- Un compte administrateur avec accès à la console d'administration de Google Workspace. Ce compte est requis pour configurer la délégation au niveau du domaine et un compte utilisateur d'API en lecture seule.
- Une connexion entre votre domaine Active Directory local et Citrix Cloud, avec l'authentification **Google** activée sur la page **Gestion des identités et des accès**. Pour créer cette connexion, au moins deux Cloud Connector sont nécessaires dans votre emplacement de ressources.

Pour plus d'informations, consultez Connecter Google en tant que fournisseur d'identité à Citrix Cloud.

Expérience des abonnés avec Google

Lorsque l'authentification avec Google est activée, le flux de travail est le suivant pour les abonnés :

1. L'abonné accède à l'URL de Workspace dans son navigateur ou lance l'application Workspace.
2. L'abonné est redirigé vers la page de connexion Google et est authentifié à l'aide de la méthode configurée dans Google Cloud (par exemple, authentification multifacteur, stratégies d'accès conditionnel, etc.).
3. Une fois que l'authentification a réussi, l'espace de travail de l'abonné apparaît.

Okta

Citrix Workspace prend en charge l'utilisation d'Okta en tant que fournisseur d'identité pour gérer l'authentification des abonnés sur les espaces de travail. Pour plus d'informations, consultez Tech Insight : Authentification - Okta.

Configuration requise pour Okta

L'authentification Okta a les exigences suivantes :

- Une connexion entre votre Active Directory local et votre organisation Okta.
- Une application Web Okta OIDC configurée pour une utilisation avec Citrix Cloud. Pour connecter Citrix Cloud à votre organisation Okta, vous devez fournir l'ID client et la clé secrète client associés à cette application.
- Une connexion entre votre domaine Active Directory local et Citrix Cloud, avec l'authentification **Okta** activée sur la page **Gestion des identités et des accès**.

Pour plus d'informations, consultez Connecter Okta en tant que fournisseur d'identité à Citrix Cloud.

Expérience de l'abonné avec Okta

Lorsque l'authentification avec Okta est activée, le flux de travail est le suivant pour les abonnés :

1. L'abonné accède à l'URL de Workspace dans son navigateur ou lance l'application Workspace.
2. L'abonné est redirigé vers la page de connexion Okta et est authentifié à l'aide de la méthode configurée dans Okta (par exemple, authentification multifacteur, stratégies d'accès conditionnel, etc.).
3. Une fois que l'authentification a réussi, l'espace de travail de l'abonné apparaît.

L'authentification Okta fournit une connexion fédérée, et non une authentification unique (SSO). Les abonnés se connectent à l'espace de travail à partir d'une page de connexion Okta et devront peut-être s'authentifier à nouveau lors de l'ouverture de Citrix DaaS. Pour l'authentification unique (SSO), activez le Service d'authentification fédérée Citrix dans Citrix Cloud. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

SAML 2.0

Citrix Workspace prend en charge l'utilisation de SAML 2.0 pour gérer l'irtual Apps and Desktoauthentification des abonnés sur les espaces de travail. Vous pouvez utiliser le fournisseur SAML de votre choix, à condition qu'il prenne en charge SAML 2.0.

Configuration requise pour SAML 2.0

L'utilisation de l'authentification SAML exige les conditions suivantes :

- Fournisseur SAML prenant en charge SAML 2.0
- Domaine Active Directory local
- Deux Cloud Connector déployés sur un emplacement de ressources et associés à votre domaine AD local
- Intégration AD avec votre fournisseur SAML

Pour plus d'informations sur la configuration de l'authentification SAML pour les espaces de travail, consultez la section Connecter SAML en tant que fournisseur d'identité à Citrix Cloud.

Expérience de l'abonné avec SAML 2.0

1. L'abonné accède à l'URL de Workspace dans son navigateur ou lance l'application Citrix Workspace.
2. L'abonné est redirigé vers la page de connexion du fournisseur d'identité SAML pour son organisation. L'abonné s'authentifie avec le mécanisme configuré pour le fournisseur d'identité SAML, tel que l'authentification multifacteur ou les stratégies d'accès conditionnel.
3. Une fois que l'authentification a réussi, l'espace de travail de l'abonné apparaît.

Service d'authentification fédérée (FAS) de Citrix

Citrix Workspace prend en charge l'utilisation du Service d'authentification fédérée Citrix (FAS) pour fournir l'authentification unique (SSO) à DaaS. Sans FAS, les abonnés utilisant un fournisseur d'identité fédéré sont invités à entrer leurs informations d'identification plusieurs fois pour accéder à DaaS.

Pour plus d'informations, consultez la section Service d'authentification fédérée Citrix (FAS).

Expérience de déconnexion de l'abonné

Utilisez **Paramètres > Déconnexion** pour terminer le processus de déconnexion depuis Workspace et Azure AD. Si les abonnés ferment le navigateur au lieu d'utiliser l'option **Déconnexion**, ils peuvent rester connectés à Azure AD.

> **Important :**
>
> Si Citrix Workspace expire dans le navigateur en raison d'une inactivité, les abonnés restent connectés à Azure AD. Cela empêche l'expiration d'une application Citrix Workspace ce qui entraînerait la fermeture d'autres applications Azure AD.

Informations supplémentaires

- Fiche technique : Authentification unique pour Workspace
- Tech Insights - Citrix Workspace
- Guides de preuve de concept - Citrix Workspace

Intégrer les services aux espaces de travail

November 28, 2023

Cet article décrit les deux étapes à suivre pour ajouter des services à Citrix Workspace :

1. Configurez des services individuels dans Citrix Cloud. Vous trouverez une liste des services Citrix Cloud contenant des liens vers des instructions pour chacun d'entre eux dans Citrix Cloud Services.
2. Activez (et désactivez) l'accès à vos services configurés dans **Configuration de l'espace de travail** > **Intégrations de services**.

Configurer les services

Les services que vous avez achetés sont affichés sous forme de carte dans le tableau de bord Citrix Cloud et incluent un bouton **Gérer**.

Pour configurer les services achetés :

1. Connectez-vous à Citrix Cloud.
2. Sélectionnez **Gérer** dans la vignette du service que vous souhaitez configurer.
3. Suivez les instructions pour configurer ce service.

Pour obtenir une brève description des services hébergés dans le cloud, consultez Services hébergés dans le cloud via Citrix Workspace.

Si vous souhaitez essayer un nouveau service, vous pouvez demander une évaluation ou une démonstration. Pour plus d'informations sur les évaluations de service, consultez la page Évaluations de services Citrix Cloud.

Activer les services

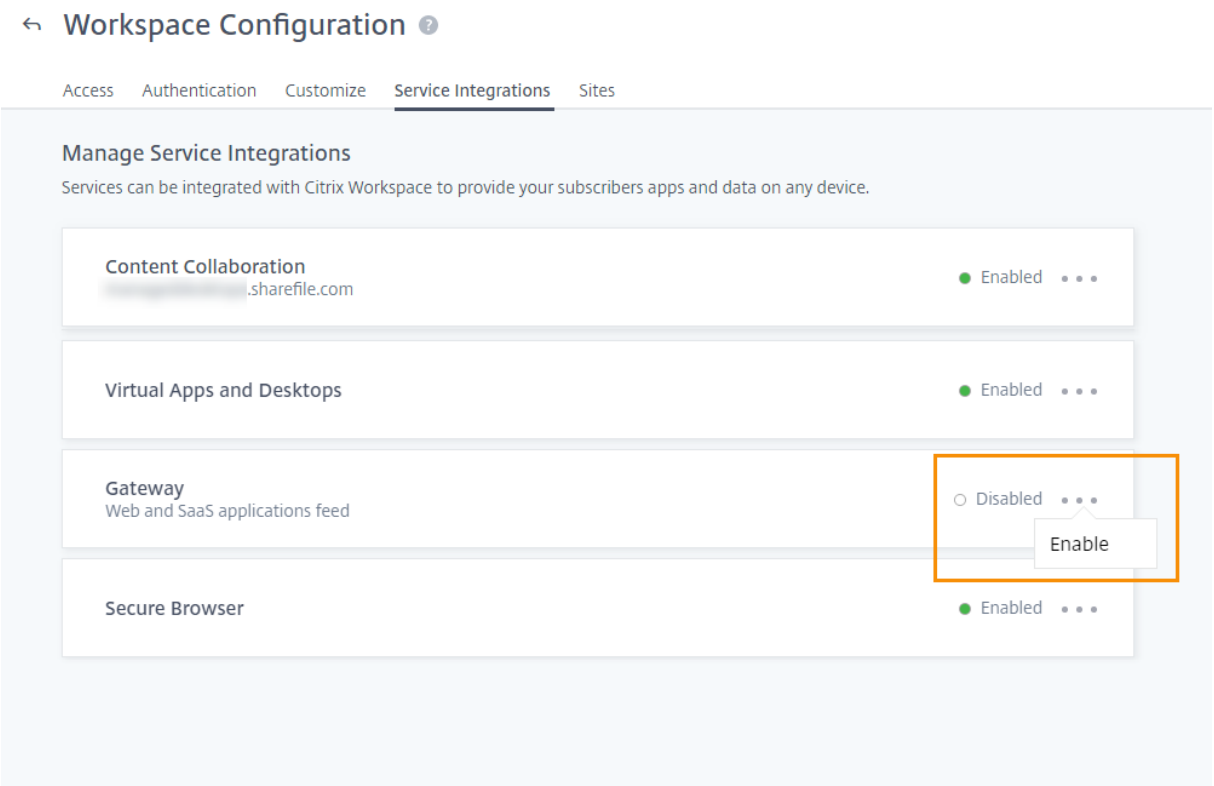
Une fois que vous avez configuré vos services, vous pouvez les intégrer dans Citrix Workspace.

Par défaut, **DaaS** et **Remote Browser Isolation Service** sont activés une fois que vous y êtes abonné. Tous les autres nouveaux services auxquels votre organisation est abonnée sont désactivés par défaut.

> **Remarque :**
>
> **Citrix Apps Essentials Service** et **Citrix DaaS** s'affichent en tant que « Citrix DaaS » dans l'onglet **Intégrations de services** sous **Configuration de l'espace de travail**.

Pour activer l'intégration de l'espace de travail pour un service :

1. Accédez à **Configuration de l'espace de travail** > **Intégrations de services**.
2. Sélectionnez le bouton représentant des points de suspension à côté du service, puis sélectionnez **Activer**.



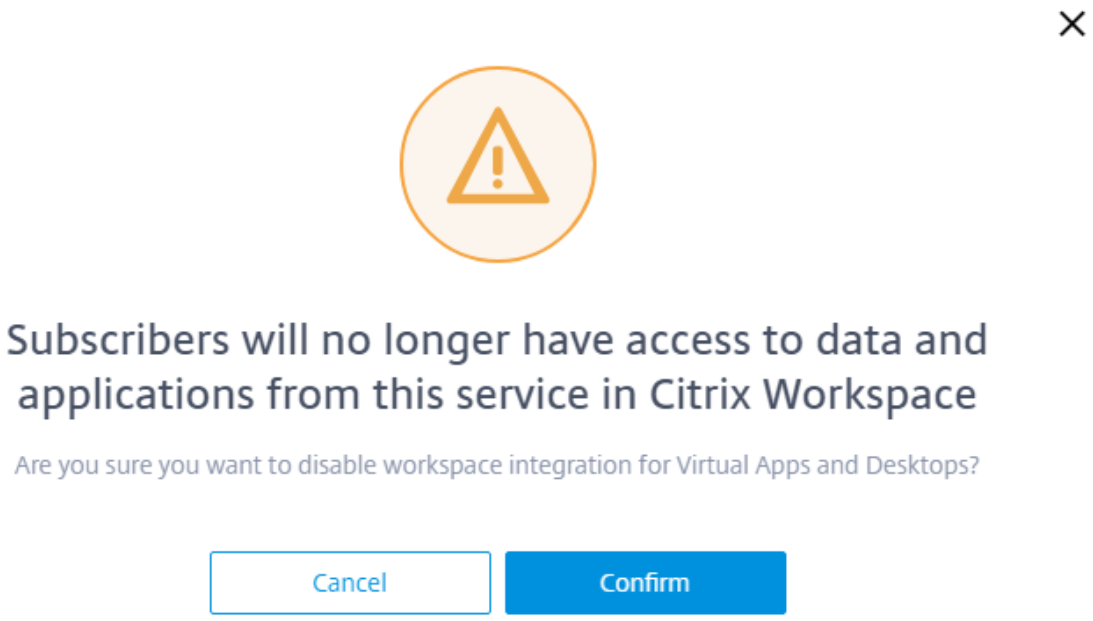
Désactiver les services

La désactivation de l'intégration de l'espace de travail bloque l'accès des abonnés à ce service. Cela ne désactive pas l'URL de l'espace de travail, mais les abonnés n'auront plus accès aux données et applications de ce service dans Citrix Workspace.

Pour désactiver l'intégration de l'espace de travail pour un service :

1. Accédez à **Configuration de l'espace de travail** > **Intégrations de services**.

2. Sélectionnez le bouton représentant des points de suspension à côté du service, puis sélectionnez **Désactiver**.
3. Lorsque vous y êtes invité, sélectionnez **Confirmer** pour confirmer que les abonnés n'auront plus accès aux données ou aux applications depuis le service.



Configurer l'application Citrix Workspace

November 28, 2023

Vous pouvez configurer l'application Citrix Workspace à l'aide de Global App Configuration Service (GACS). Ce service vous aide à gérer les paramètres de l'application pour les utilisateurs sur les appareils gérés et non gérés.
Les paramètres peuvent être configurés pour les environnements cloud (Citrix Workspace) et locaux (Citrix StoreFront) à l'aide de l'une des méthodes suivantes :

- Interface utilisateur (UI) de Global App Configuration Service :
  - Configurer les paramètres des magasins cloud
  - Configurer les paramètres des magasins locaux
- API : pour configurer les paramètres à l'aide d'API, consultez Citrix Developer.

Ce service est compatible avec les plateformes Windows, Mac, Android, iOS, HTML5 et ChromeOS.

Principaux avantages

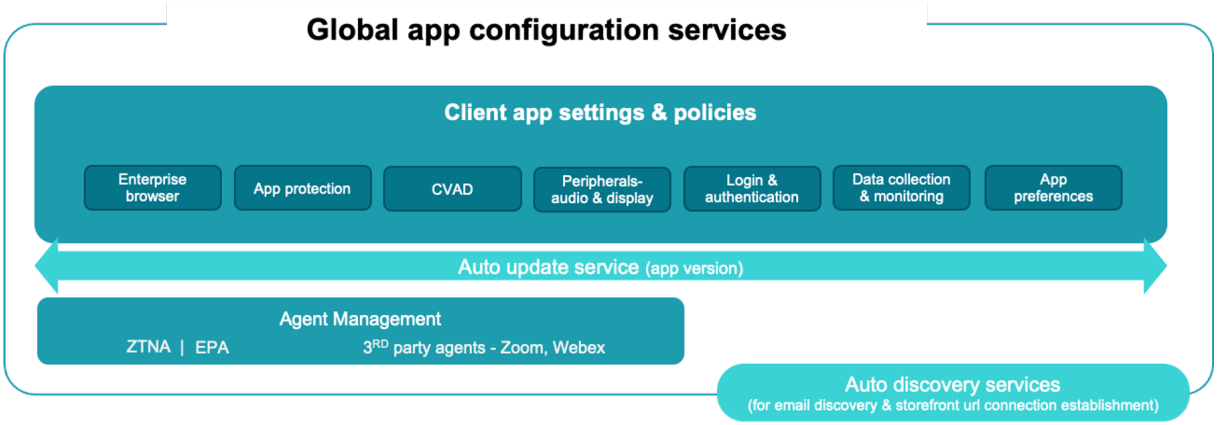
Global App Configuration Service vous permet d'exécuter les fonctions suivantes à partir d'une interface centralisée :

- Configurer les paramètres des appareils gérés et non gérés (Apportez votre propre appareil)
- Configurer les paramètres de plusieurs magasins
- Mettre à jour et gérer les agents des applications clientes (par exemple, Endpoint Analysis, ZTNA) et les agents tiers (par exemple, Zoom, Webex)
- Mettre à jour et gérer automatiquement la version de l'application Citrix Workspace pour les utilisateurs
- Tester la configuration avant de la déployer auprès de vos utilisateurs

Comment fonctionne Global App Configuration Service ?

Global App Configuration Service est une solution IP Citrix utilisée pour configurer et gérer les paramètres des applications clientes. Ce service utilise les services et paramètres suivants pour offrir une expérience fluide à vos utilisateurs.

- **Services de découverte automatique** : mappent des domaines pour stocker des URL, ce qui permet à vos utilisateurs de se connecter à l'aide de leur adresse e-mail. Les utilisateurs ne sont pas tenus de fournir l'URL de leur magasin au moment de la connexion.
- **Service de mise à jour automatique et gestion des agents** : met automatiquement à jour l'application Citrix Workspace vers la version spécifiée pour vos utilisateurs. Vous avez la possibilité de configurer différentes versions d'applications pour différentes plateformes.
- **Paramètres et stratégies de l'application cliente** : tous les paramètres utilisateur de l'application Citrix Workspace peuvent être configurés et définis de manière centralisée. Cela inclut des paramètres tels que l'expérience de connexion, la sécurité, les options d'authentification et les paramètres d'applications et de bureaux virtuels.



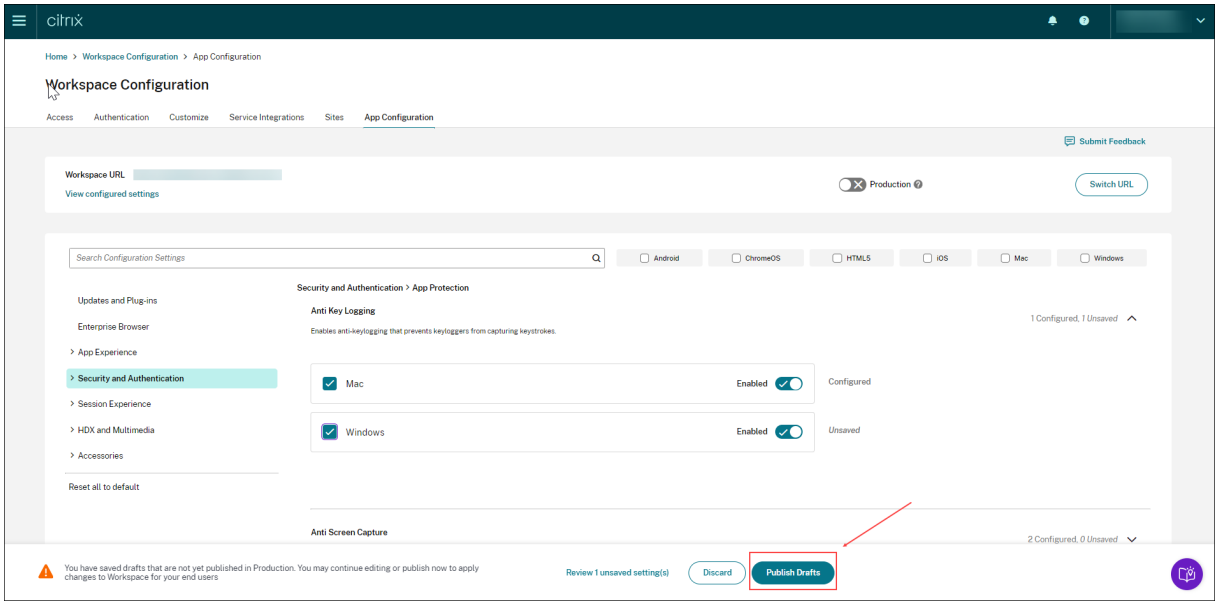
Conditions préalables

Avant de configurer les paramètres de l'application, assurez-vous que la version de l'application Citrix Workspace est égale ou supérieure aux versions spécifiées. Pour plus d'informations, consultez le tableau suivant.

Plate-forme d'application Citrix Workspace	Version minimale prise en charge
Windows	Version actuelle - 2106, LTSR - 2203.1
Mac	2203.1
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

Comment utiliser Global App Configuration Service ?

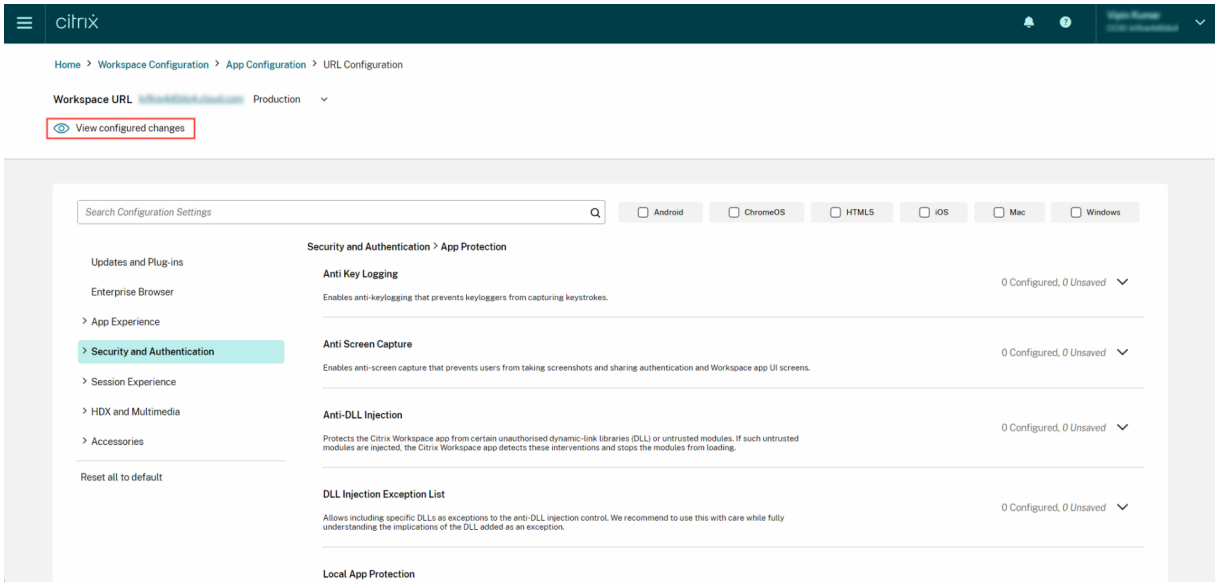
Pour configurer les paramètres, connectez-vous au portail Citrix Cloud et accédez à **Configuration de l'espace de travail** > **Configuration d'applications**. Modifiez les paramètres des applications conformément aux stratégies de votre organisation. Vous pouvez ensuite cliquer sur **Publier brouillons** pour enregistrer et publier vos paramètres.



L'interface utilisateur propose également les options suivantes pour une expérience utilisateur simplifiée.

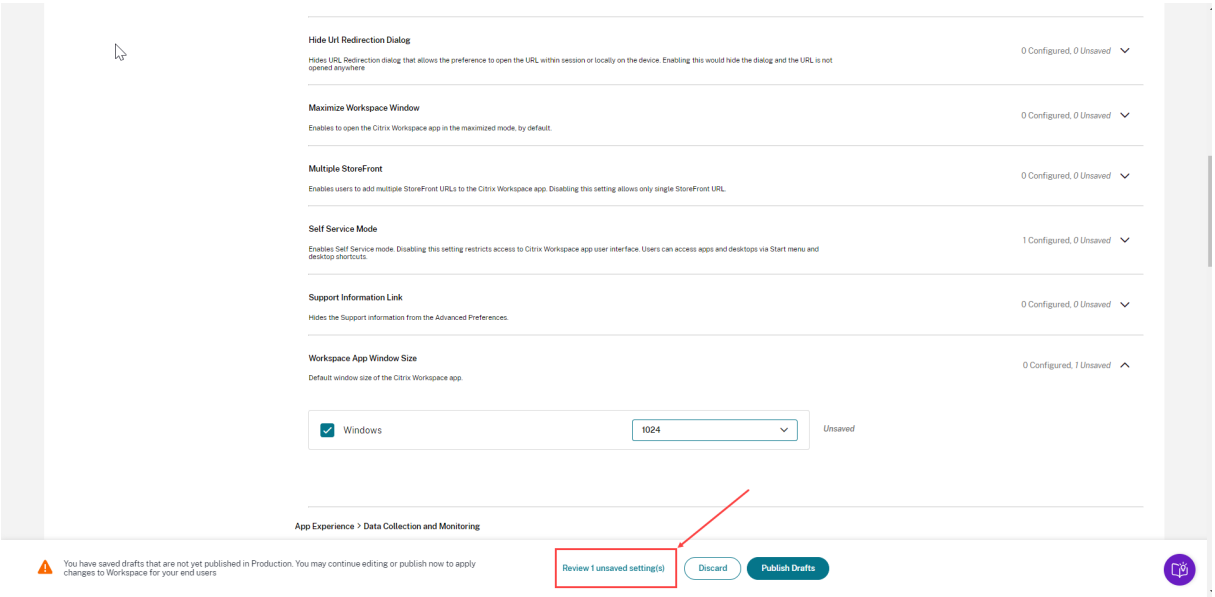
Afficher un résumé des paramètres configurés

Vous pouvez consulter un résumé de la configuration actuelle en cliquant sur le bouton **Afficher les paramètres configurés**. Il n'est donc plus nécessaire de développer et de vérifier chaque paramètre séparément. Une liste consolidée de tous les paramètres configurés vous permet d'effectuer un examen complet de la configuration actuelle et d'évaluer l'impact sur l'utilisateur.

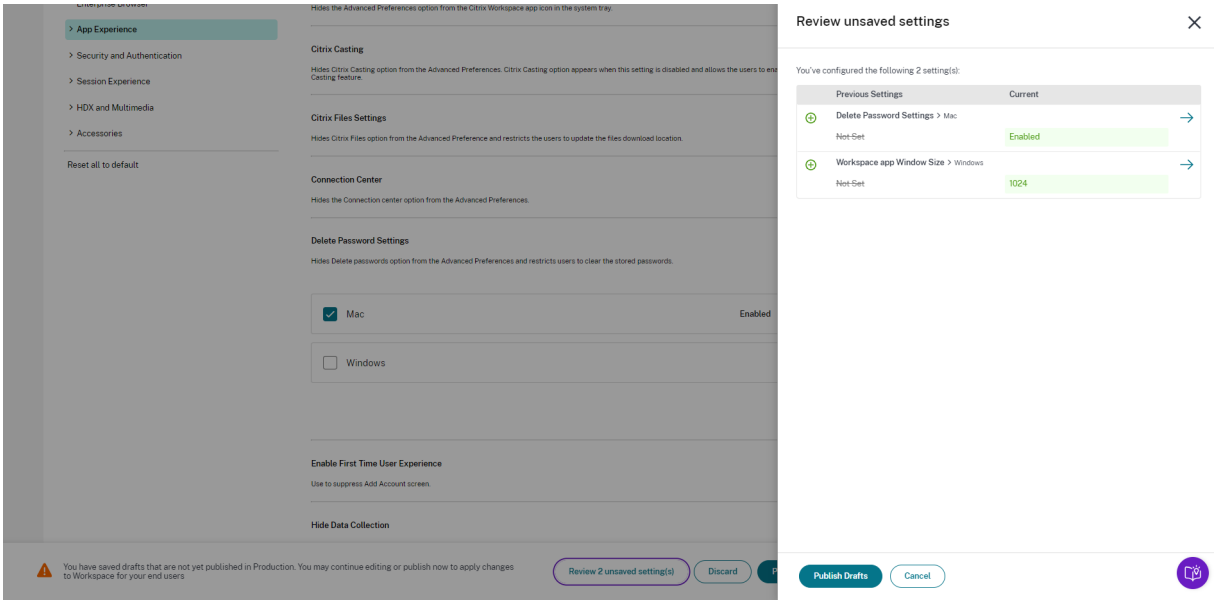


Vérifier les modifications non enregistrées

Vérifiez une dernière fois les modifications non enregistrées avant de publier la configuration. Le nombre de paramètres non enregistrés est affiché dans l'interface utilisateur et vous pouvez accéder à cette liste en cliquant sur l'option **Vérifier les paramètres non enregistrés**. Cela vous permet d'apporter des modifications éclairées et d'assurer l'exactitude des données.



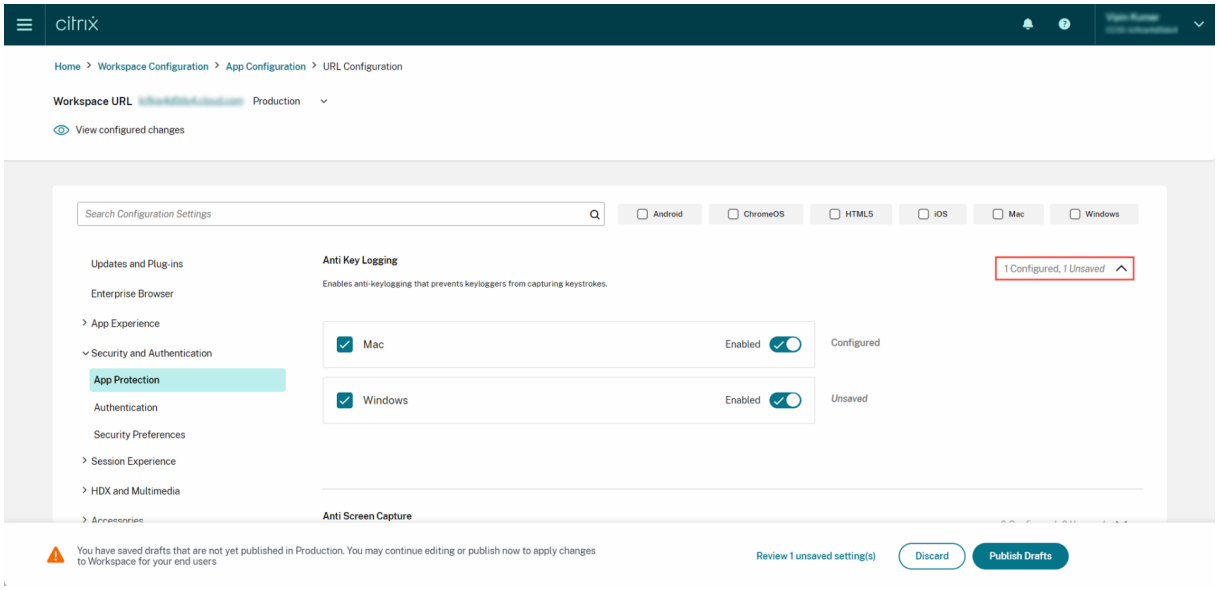
Vous pouvez également accéder à un paramètre non enregistré en cliquant sur la flèche.



Interface utilisateur améliorée

Consultez l'état de chaque paramètre sans le développer. Les balises suivantes sont désormais affichées pour faciliter la prise de décisions éclairées à chaque étape.

- **Configuré** : affiche le nombre de plateformes (système d'exploitation client) pour lesquelles le paramètre a déjà été configuré.
- **Non enregistré** : affiche le nombre de paramètres configurés mais pas encore enregistrés



Option de recherche améliorée

L'expérience de recherche a été améliorée pour offrir une expérience robuste et fluide. Les administrateurs peuvent désormais se connecter au portail cloud et localiser facilement les paramètres requis sur la page Configuration d'application. Ils peuvent utiliser les méthodes de recherche suivantes.

- **Recherche à l'aide de la description du paramètre**

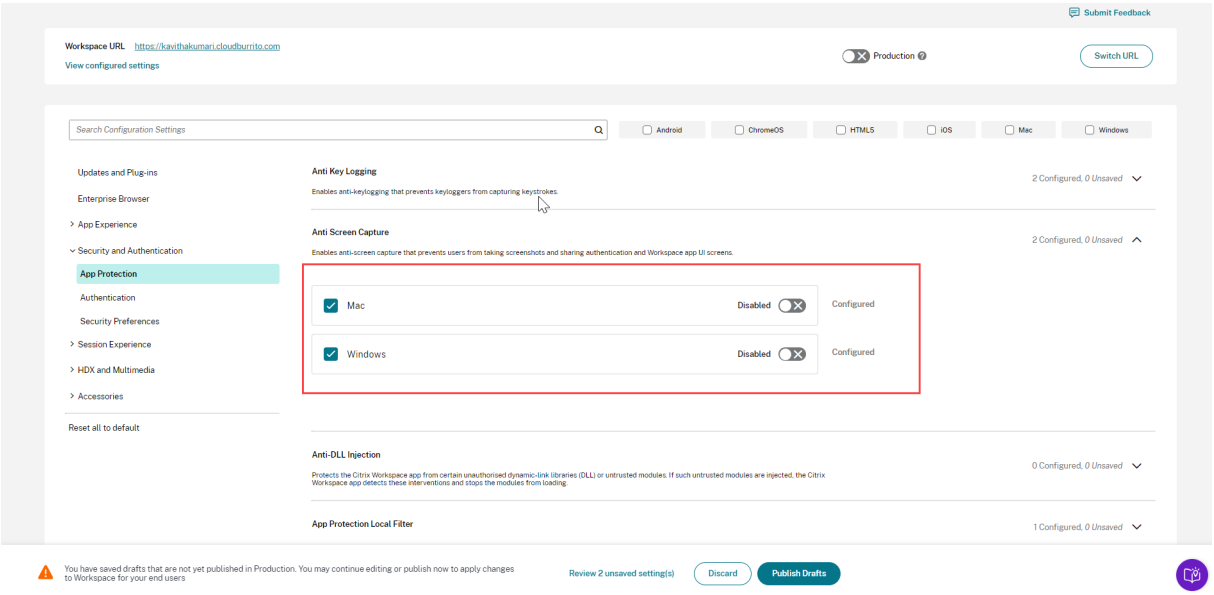
Vous pouvez localiser les paramètres en saisissant les mots clés figurant dans la description du paramètre. Cela permet une approche de recherche plus flexible, en utilisant des termes pertinents associés au paramètre souhaité.

- **Recherche à l'aide du nom du paramètre d'API**

Vous pouvez rechercher des paramètres en saisissant le nom du paramètre d'API correspondant. Cette méthode permet une recherche plus précise et ciblée, permettant aux utilisateurs de trouver rapidement le paramètre spécifique dont ils ont besoin.

Afficher les plateformes applicables à chaque paramètre

Chaque paramètre affiche désormais de manière dynamique uniquement les plateformes pour lesquelles il est pertinent et applicable. Cette approche garantit que les utilisateurs disposent d'une liste d'options concise et personnalisée.



Fréquence de récupération des paramètres mis à jour

Une fois la configuration publiée, la mise à jour des paramètres côté client peut prendre quelques heures.

- Au cours de la même session, les paramètres sont mis à jour comme suit.

Plateforme	Durée maximale requise pour mettre à jour les paramètres
Application Citrix Workspace pour Windows	jusqu'à 6 heures
Application Citrix Workspace pour macOS	jusqu'à 6 heures
Application Citrix Workspace pour HTML5	jusqu'à 3 heures
Application Citrix Workspace pour ChromeOS	jusqu'à 3 heures
Application Citrix Workspace pour iOS	jusqu'à 6 heures
Application Citrix Workspace pour Android	jusqu'à 6 heures

- Pour Windows et macOS, les paramètres peuvent être mis à jour immédiatement si les utilisateurs quittent et redémarrent leur application Citrix Workspace.
- Lorsqu'un utilisateur ajoute un magasin à son application Citrix Workspace, les paramètres de ce magasin sont automatiquement mis à jour.

Ordre de priorité pour l'application des paramètres

Outre Global App Configuration Service, il existe des outils spécifiques à la plate-forme, tels que GPO pour Windows, qui peuvent être utilisés pour configurer les paramètres des utilisateurs.
En cas de conflit entre les paramètres configurés via Global App Configuration Service et d'autres outils de la plateforme, les paramètres sont appliqués dans l'ordre suivant.

Plateforme	Type de magasin	Ordre de priorité
Application Citrix Workspace pour Windows	StoreFront et Cloud	**Objet de stratégie de groupe (GPO) > Global App Configuration Service > Registre**
Application Citrix Workspace pour Mac	StoreFront et Cloud	**MDM > Global App Configuration Service > UserDefaults**
Application Citrix Workspace pour HTML5	StoreFront	Global App Configuration Service > Configuration.js
	Cloud	Global App Configuration Service
Application Citrix Workspace pour ChromeOS	StoreFront	**Stratégie d'administration Google > Global App Configuration Service >** Configuration.js
	Cloud	**Stratégie d'administration Google > Global App Configuration Service**
Application Citrix Workspace pour iOS	StoreFront et Cloud	Global App Configuration Service
Application Citrix Workspace pour Android	StoreFront et Cloud	Global App Configuration Service

Limitations

- Global App Configuration Service n'est pas pris en charge pour Linux.
- Vous ne pouvez pas ajouter plus d'un magasin compatible avec Global App Configuration Service sous Windows et Mac.

Ressources supplémentaires

- Dossier technique sur Global App Configuration Service
- FAQ : Paramètres et comportements de Global App Configuration Service
- Enregistrement du webinaire : How to use Global App Configuration service
- Présentation des fonctionnalités de Citrix : Global App Configuration Service

Configurer les paramètres des magasins cloud

November 28, 2023

Vue d'ensemble

Vous pouvez configurer les paramètres de l'application Citrix Workspace pour les magasins cloud à l'aide du service GACS (Global App Configuration Service). Cela aide les administrateurs à configurer et à gérer l'application Citrix Workspace pour les utilisateurs sur les appareils gérés et non gérés. Ce service est compatible avec les plateformes Windows, Mac, Android, iOS, HTML5 et ChromeOS.

Conditions préalables

- L'adresse https://discovery.cem.cloud.us doit être accessible. Elle est nécessaire au fonctionnement des services de découverte par e-mail et de Global App Configuration Service.
- Vérifiez que vous avez accès à un compte Citrix Cloud. Si ce n'est pas le cas, vous pouvez créer un compte depuis https://onboarding.cloud.com/. Pour plus d'informations, consultez la section S'inscrire à Citrix Cloud.
- Vérifiez que vous disposez d'un abonnement Workspace.

Mise en route

Vous pouvez vous connecter à votre compte Citrix Cloud et configurer les paramètres depuis **Configuration de l'espace de travail** > **Configuration de l'application**.
Avant de continuer, vérifiez si vous disposez des autorisations suivantes.

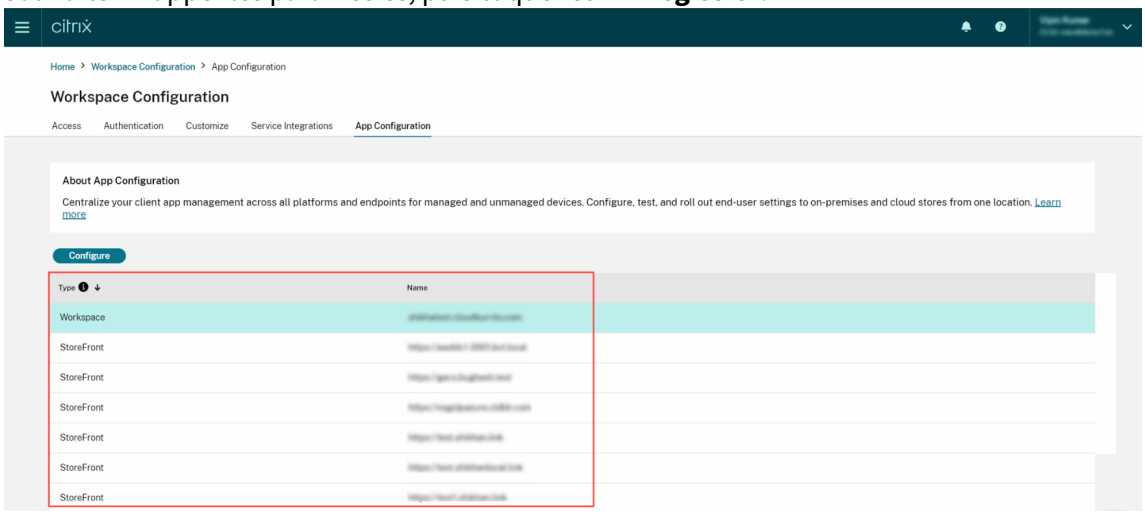
- **Abonnement Workspace :** l'abonnement Workspace est requis pour créer une URL d'espace de travail. Si vous n'avez pas d'abonnement, vous ne pourrez pas ajouter ni configurer de magasins cloud.
  Vous ne serez invité qu'à configurer des magasins sur site.

- **URL de l'espace de travail :** si vous êtes abonné à Workspace mais que vous n'avez pas encore ajouté votre URL, l'écran suivant s'affiche. Vous pouvez cliquer sur **Démarrer** sous **Configurer les paramètres des magasins cloud** pour créer votre URL.

Configurer les paramètres

Vous pouvez configurer les paramètres de l'application Citrix Workspace depuis le portail Citrix Cloud. Si plusieurs magasins ont été configurés pour votre organisation, vous pouvez configurer chacun d'eux séparément.

1. Accédez à Citrix Cloud et connectez-vous avec vos informations d'identification Citrix Cloud.
2. Accédez à **Configuration de l'espace de travail** > **Configuration d'applications**.
3. Cliquez sur **Changer d'URL** pour sélectionner le magasin pour lequel vous souhaitez configurer les paramètres.
4. Dans la liste des URL de magasins configurés, sélectionnez le magasin pour lequel vous souhaitez mapper les paramètres, puis cliquez sur **Enregistrer**.



5. Modifiez les paramètres de vos plateformes préférées selon vos besoins.
6. Cliquez sur **Publier brouillons** pour enregistrer les paramètres.

> **Remarque :**
>
> La mise à jour des paramètres sur les clients de l'application Citrix Workspace peut prendre quelques heures. Pour plus d'informations, consultez la section Fréquence de récupération des paramètres mis à jour.

Configurer la découverte basée sur une adresse e-mail

Le service de découverte basée sur une adresse e-mail permet aux utilisateurs de se connecter automatiquement à l'aide de leur adresse e-mail. Ils ne sont pas tenus de fournir les URL de leur magasin.
Pour activer ce service pour les magasins dans le cloud, vous devez suivre les étapes suivantes.

1. Revendiquer un domaine
2. Créer un mappage entre un domaine et une URL

Revendiquer un domaine

Pour revendiquer un domaine :

1. Accédez à https://adsui.cloud.com.
2. Accédez à **Revendications** > **Domaines** > **Ajouter un domaine**.
3. Entrez le domaine que vous souhaitez revendiquer (par exemple, ace.example.com).
4. Cliquez sur **Confirmer**.
5. Copiez le jeton DNS affiché à l'écran.
6. Pour créer un enregistrement TXT DNS, accédez au portail du fournisseur de services et ajoutez le jeton DNS.
7. Pour démarrer le processus de vérification :
    a) Accédez à **Réclamations** > **Domaines**.
    b) Accédez au domaine que vous avez ajouté et cliquez sur le menu représentant des points de suspension.
    c) Sélectionnez **Vérifier le domaine**.
    d) Cliquez sur **Démarrer vérification de DNS**.

Une fois la vérification terminée, le statut de votre domaine passe de *En attente* à *vérifié*.

Créer un mappage entre un domaine et une URL

1. Accédez à **Réclamations** > **Domaines**.
2. Accédez au domaine que vous avez ajouté et cliquez sur le menu représentant des points de suspension.

3. Cliquez sur **Ajouter une autre URL de serveur**.
4. Entrez l'URL du magasin que vous souhaitez associer à ce domaine.
5. Cliquez sur **Save**.

Configurer les paramètres des magasins locaux

November 28, 2023

Vue d'ensemble

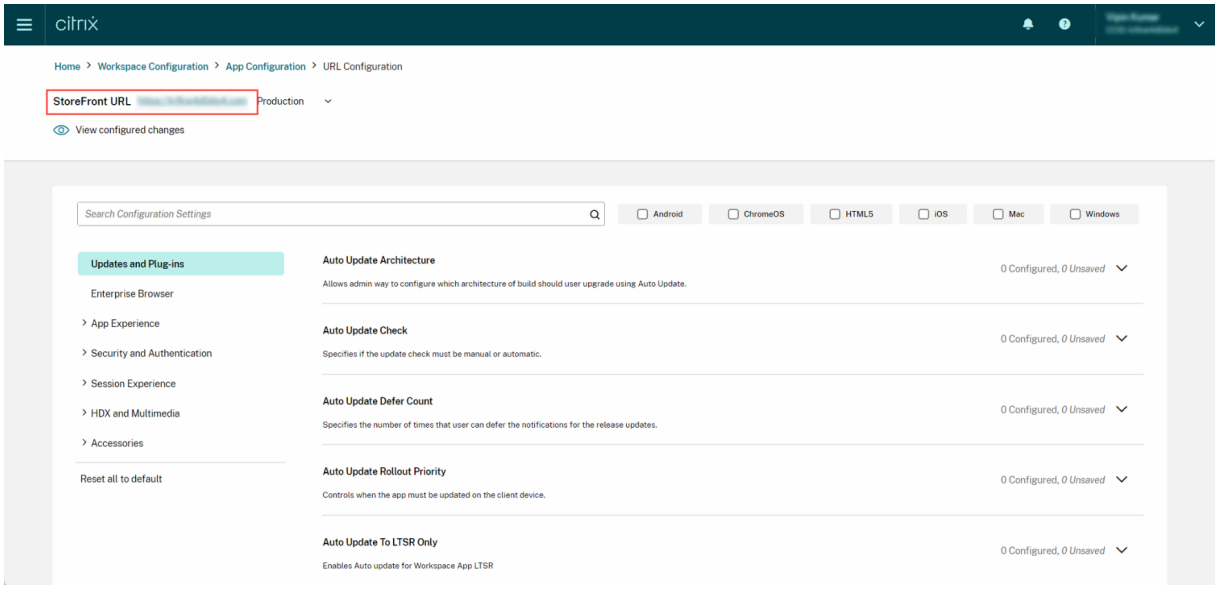
Vous pouvez configurer les paramètres de l'application Citrix Workspace pour les magasins locaux à l'aide de Global App Configuration Service (GACS). Ce service vous aide à configurer et à gérer l'application Citrix Workspace pour les utilisateurs sur les appareils gérés et non gérés. Global App Configuration Service est pris en charge sur les plateformes Windows, Mac, Android, iOS, HTML5 et ChromeOS.

Conditions préalables

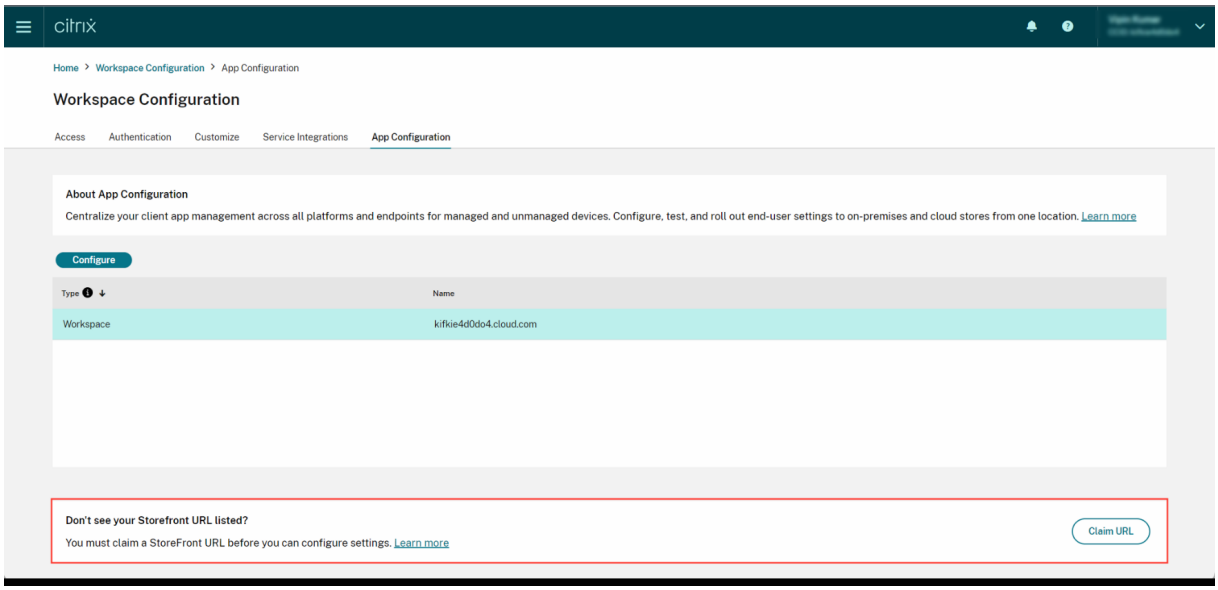
- L'adresse https://discovery.cem.cloud.us doit être accessible. Elle est nécessaire au fonctionnement des services de découverte par e-mail et de Global App Configuration Service.
- Vérifiez que vous avez accès à un compte Citrix Cloud. Si vous n'avez pas encore de compte, vous pouvez en créer un à partir de https://onboarding.cloud.com/. Pour plus d'informations, consultez la section S'inscrire à Citrix Cloud.
- Dans un environnement local, vous devez revendiquer une URL avant de pouvoir configurer les paramètres. Pour plus d'informations, consultez la section Revendiquer une URL.

Mise en route

Pour configurer les paramètres d'un magasin sur site, connectez-vous à votre compte Citrix Cloud et accédez à **Configuration de l'espace de travail** > **Configuration de l'application**.
Si vous avez revendiqué la propriété de votre URL StoreFront, l'écran suivant s'affiche dans lequel vous pouvez commencer à configurer les paramètres. Pour plus d'informations, consultez la section Configurer les paramètres.



Si vous n'avez pas encore revendiqué la propriété de votre URL StoreFront, l'écran suivant vous invite à revendiquer votre URL avant de continuer. Pour plus d'informations, consultez la section Revendiquer une URL pour les magasins locaux.



Revendiquer une URL pour les magasins locaux

Il est obligatoire de revendiquer votre URL avant de commencer à configurer ses paramètres.

Pour revendiquer une URL :

1. Accédez à https://adsui.cloud.com/url et connectez-vous avec vos informations d'identification Citrix Cloud.

2. Accédez à **Revendications** > **URL** > **Ajouter une URL**.
3. Entrez l'URL que vous souhaitez revendiquer.
4. Cliquez sur **Confirmer**. La fenêtre contextuelle de vérification s'affiche.

   > **Remarque :**
   >
   > Si NetScaler Gateway n'est pas installé dans l'environnement sur site, vous ne pourrez pas effectuer le processus de vérification (à partir de l'étape 5). Dans ce cas, effectuez les étapes 1 à 4 comme décrit dans la procédure précédente et contactez notre équipe d'assistance en indiquant votre ID client et l'URL que vous souhaitez revendiquer.

5. Si NetScaler Gateway est installé dans votre configuration sur site, vous pouvez vérifier votre URL en procédant comme suit.

   a) **Copiez** le jeton qui apparaît dans la fenêtre contextuelle.
   b) Créez et configurez une action de réponse et une stratégie de réponse au sein de votre Citrix ADC.
   c) Liez votre stratégie de réponse globalement.
   d) Accédez à `https://<customergatewayurl>/vpn/CitrixClaims` pour vérifier si votre stratégie de réponse est correctement configurée.
   e) Revenez à **Revendications** > **URL**, puis recherchez l'URL que vous avez ajoutée.
   f) Cliquez sur l'icône représentant des points de suspension dans le menu correspondant à l'URL ajoutée.
   g) Sélectionnez **Vérifier l'URL**.
   h) Cliquez sur **Démarrer vérification de la revendication** pour démarrer le processus de vérification.

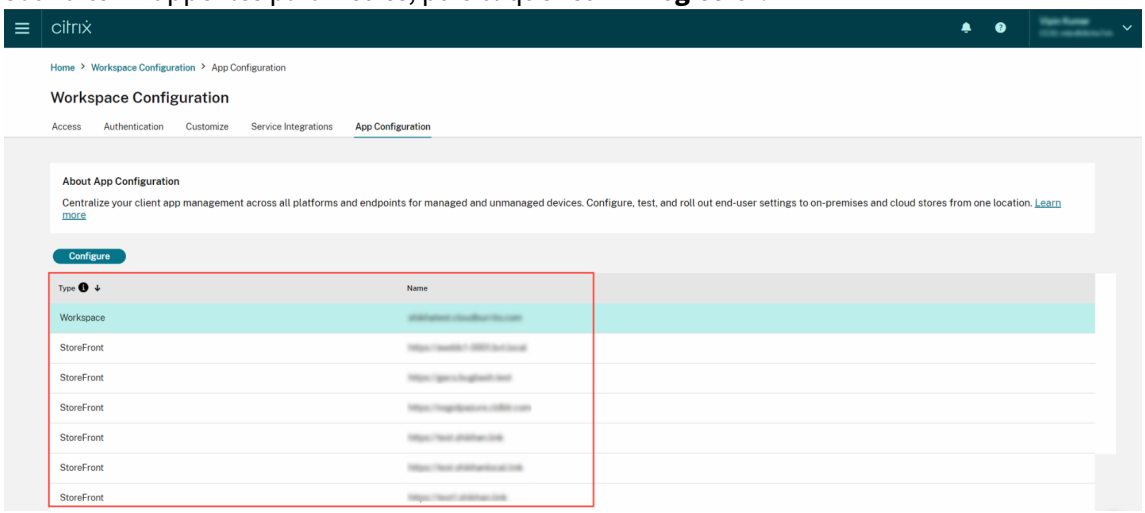
   Une fois la configuration terminée, le statut de votre domaine passe de *En attente* à *vérifié*.

Configurer les paramètres

Vous pouvez configurer les paramètres de l'application Citrix Workspace une fois que vous avez revendiqué l'URL. Si plusieurs magasins ont été configurés pour votre entreprise, vous pouvez configurer les paramètres de chacun d'eux séparément.

1. Accédez au portail Citrix Cloud et connectez-vous à l'aide de vos informations d'identification.
2. Accédez à **Configuration de l'espace de travail** > **Configuration d'applications**.
3. Cliquez sur **Changer d'URL** pour sélectionner le magasin pour lequel vous souhaitez configurer les paramètres.

4. Dans la liste des URL de magasins configurés, sélectionnez le magasin pour lequel vous souhaitez mapper les paramètres, puis cliquez sur **Enregistrer**.



5. Modifiez les paramètres de vos plateformes préférées selon vos besoins.
6. Cliquez sur **Publier brouillons** pour enregistrer les paramètres.

> **Remarque :**
>
> La mise à jour des paramètres sur les clients de l'application Citrix Workspace peut prendre quelques heures. Pour plus d'informations, consultez la section Fréquence de récupération des paramètres mis à jour.

Configurer la découverte basée sur les e-mails

Le service de découverte basée sur une adresse e-mail permet aux utilisateurs de se connecter automatiquement à l'aide de leur adresse e-mail. Ils ne sont pas tenus de fournir les URL de leur magasin.
Pour activer ce service pour les magasins dans le cloud, vous devez suivre les étapes suivantes.

1. Revendiquer un domaine
2. Créer un mappage entre un domaine et une URL

Revendiquer un domaine

Pour revendiquer un domaine :

1. Accédez au service AutoDiscovery.
2. Accédez à **Revendications** > **Domaines** > **Ajouter un domaine**.

3. Entrez le domaine que vous souhaitez revendiquer (par exemple, ace.example.com).
4. Cliquez sur **Confirmer**.
5. Copiez le jeton DNS qui apparaît à l'écran dans le presse-papiers.
6. Pour créer un enregistrement TXT DNS, accédez au portail du fournisseur de services et ajoutez le jeton DNS.
7. Pour démarrer le processus de vérification :

    a) Accédez à **Réclamations** > **Domaines**.
    b) Accédez au domaine que vous avez ajouté et cliquez sur le menu représentant des points de suspension.
    c) Sélectionnez **Vérifier le domaine**.
    d) Cliquez sur **Démarrer vérification de DNS**.

Une fois la vérification terminée, le statut de votre domaine passe de *En attente* à *vérifié*.

> **Remarque :**
>
> Vous pouvez revendiquer un maximum de 10 domaines. Si vous souhaitez revendiquer plus de 10 domaines, contactez le support Citrix et fournissez votre ID client et votre URL.

Créer un mappage entre un domaine et une URL

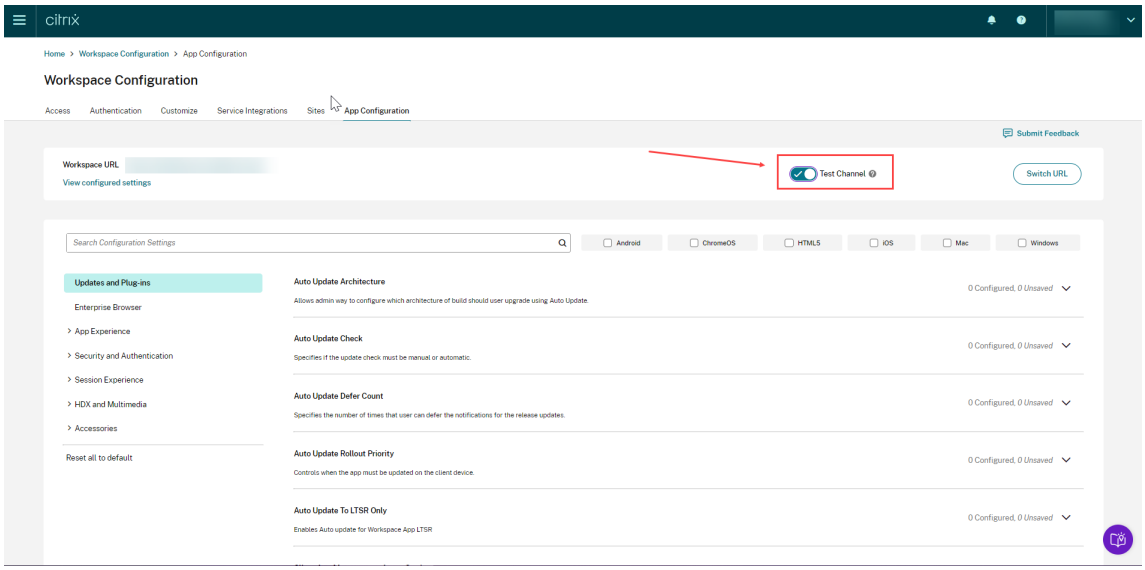
1. Accédez à **Réclamations** > **Domaines**.
2. Accédez au domaine que vous avez ajouté et cliquez sur le menu représentant des points de suspension.
3. Cliquez sur **Ajouter une autre URL de serveur**.
4. Entrez l'URL du magasin que vous souhaitez associer à ce domaine et enregistrez.

Configuration du canal de test

November 28, 2023

Vous pouvez tester votre configuration avant de l'activer pour les utilisateurs. Il vous aide à détecter et à résoudre les problèmes qui peuvent survenir après le déploiement.
La fonctionnalité de test réduit considérablement la probabilité de perturbations ou d'erreurs pendant le processus de déploiement et augmente la satisfaction globale des utilisateurs.
Pour tester votre configuration :

1. Accédez au portail cloud et connectez-vous à l'aide de vos informations d'identification Citrix Cloud.
2. Accédez à **Configuration de l'espace de travail** > **Configuration d'applications**.
3. Basculez le commutateur sur **Canal de test**. Il est réglé sur **Production** par défaut.



4. Modifiez les paramètres de vos plateformes préférées selon vos besoins.
5. Vous pouvez ensuite cliquer sur **Publier brouillons** pour publier vos paramètres sur le canal de test.

> **Remarque :**
>
> Global App Configuration Service ne prend en charge que deux canaux par magasin, un canal de production (par défaut) et un canal de test.

Configurer la prise en charge des canaux sur les appareils des utilisateurs

Windows

Pour tester la configuration définie par les administrateurs sur un appareil Windows, les utilisateurs doivent créer le registre suivant.

```
    Path- HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
    Name- AppConfigChannelName
    Type- REG_SZ
    Value- testrolloutchannel1

<!--NeedCopy-->
```


Mac

Pour tester la configuration définie par l'administrateur sur un appareil Mac, les utilisateurs doivent suivre les étapes suivantes.

1. Définissez le nom du canal de test de Global App Configuration Service à l'aide de la commande suivante :

```
defaults write com.citrix.receiver.nomas GACSChannelName
    testrolloutchannel1

<!--NeedCopy-->
```

2. Redémarrez Citrix Workspace Helper à l'aide des commandes suivantes :

```
launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.
    plist

launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.
    plist

<!--NeedCopy-->
```

Une fois que l'appareil redémarre, la configuration du canal de test est récupérée automatiquement.

iOS

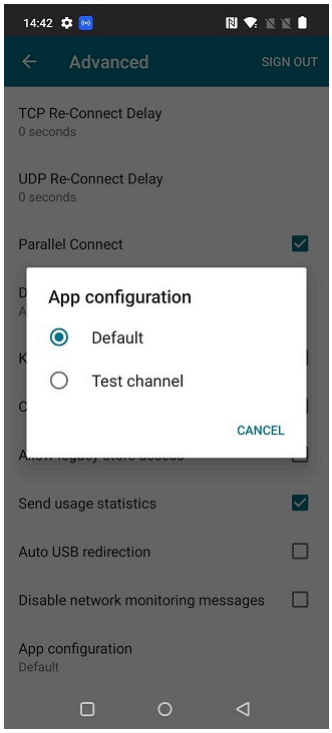
Pour tester la configuration définie par l'administrateur sur un appareil iOS, procédez comme suit.

1. Connectez-vous à l'application Citrix Workspace.
2. Accédez à **Paramètres** > **Avancé** > **Configuration d'applications**.
3. Sélectionnez le canal de test.
4. Vous pouvez maintenant tester la configuration définie par l'administrateur.

Android

Pour tester la configuration définie par l'administrateur sur un appareil Android, procédez comme suit.

1. Connectez-vous à l'application Citrix Workspace.
2. Accédez à **Paramètres** > **Avancé** > **Configuration d'applications**.
3. Sélectionnez le canal de test.
4. Vous pouvez maintenant tester la configuration définie par l'administrateur.



Gérer votre expérience d'espace de travail

November 28, 2023

Cet article fournit une vue d'ensemble de la manière dont les abonnés peuvent accéder à leurs espaces de travail et interagir avec eux. Il décrit les options de personnalisation permettant d'améliorer l'expérience de l'espace de travail et fournit des solutions aux problèmes courants.

Accès à l'espace de travail

Les abonnés peuvent accéder à Citrix Workspace de deux manières :

- Via un navigateur avec l'URL de l'espace de travail
- Avec l'application Citrix Workspace, installée sur les appareils des abonnés

Accès au navigateur

Les abonnés doivent utiliser la dernière version d'Edge, de Chrome, Firefox ou Safari lorsqu'ils se connectent via le navigateur. Les utilisateurs peuvent saisir l'URL de leur espace de travail pour y accéder. Pour plus d'informations, consultez l'article Workspace Browser Compatibility.

L'URL de l'espace de travail est activée par défaut, généralement au format : `https://yourcompanyname.cloud.com`. Pour plus d'informations sur la configuration de l'URL de l'espace de travail, consultez URL de l'espace de travail.

Accès à l'application Citrix Workspace

Citrix recommande d'utiliser la dernière version de l'application Citrix Workspace pour accéder aux espaces de travail.

L'application Citrix Workspace est une application installée en mode natif qui remplace Citrix Receiver et fournit une expérience utilisateur cohérente de l'interface utilisateur (UI) Workspace sur toutes les plates-formes. L'application Citrix Workspace est disponible pour différents systèmes d'exploitation. Pour plus de détails, consultez la documentation produit de l'application Citrix Workspace.

Si vous utilisez Citrix Receiver, guidez les utilisateurs à effectuer une mise à niveau vers l'application Citrix Workspace afin de tirer parti de toutes les fonctionnalités de l'interace Workspace. Pour plus d'informations sur les fonctionnalités prises en charge dans l'application Citrix Workspace par plate-forme, reportez-vous au tableau des fonctionnalités de l'application Workspace.

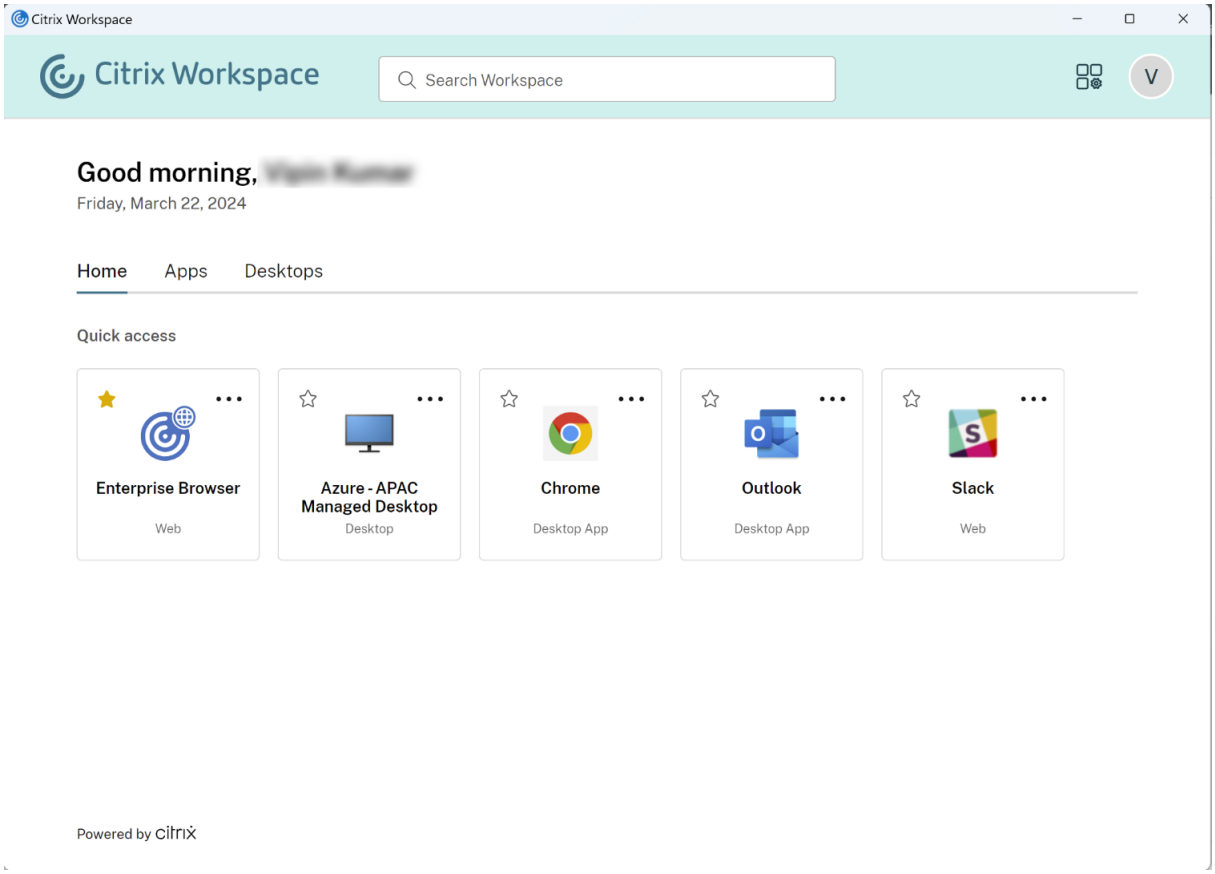
Pour plus d'informations sur l'installation de l'application Citrix Workspace, consultez la page Télécharger l'application Citrix Workspace.

Pour les périphériques qui ne peuvent pas installer le logiciel de l'application Citrix Workspace, l'application Citrix Workspace pour HTML5 offre une connexion via un navigateur Web compatible HTML5.

Interface utilisateur et fonctionnalités de Workspace

Nouveaux clients. Si c'est la première fois que vous utilisez un espace de travail, vous obtiendrez la dernière version de l'interface utilisateur dès qu'elle est disponible.

Clients existants. Si vous avez utilisé une version antérieure de Citrix Workspace, l'interface utilisateur mise à jour peut prendre environ cinq minutes à s'afficher. Vous pouvez voir temporairement une ancienne version de l'interface utilisateur.



L'interface utilisateur de Citrix Workspace comprend les fonctionnalités suivantes :

Authentification unique (SSO)

Grâce à l'authentification unique (SSO), Citrix Workspace offre une expérience fluide aux ressources secondaires qui nécessiteraient autrement une autre forme d'authentification.

Disposition des cartes

Les **applications**, les **bureaux**, les **fichiers**, les **actions** et le **flux d'activités** sont présentés sous forme de « carte ». Une fenêtre contextuelle affiche plus de détails et d'actions.

Paramètres

Les abonnés accèdent aux **paramètres** à partir d'un menu qui s'affiche lorsqu'ils sélectionnent l'icône de leur profil dans le coin supérieur droit de l'interface utilisateur de Workspace.

Icône Profil

Les abonnés peuvent télécharger une photo sur leur profil. Si aucune image de profil n'est définie, l'image par défaut est une icône basée sur le nom complet Active Directory de l'abonné.

Recherche

L'outil de recherche situé en haut de l'interface utilisateur recherche toutes les ressources de l'espace de travail et permet aux abonnés d'ouvrir des applications directement à partir des résultats de recherche. La recherche nécessite au moins trois caractères.

Vue Récents et Favoris

Les abonnés peuvent choisir entre une vue **Récents** et **Favoris** de leurs applications, de leurs bureaux et de leurs fichiers.

Vous pouvez configurer les **Favoris** pour rendre cette fonctionnalité disponible ou non disponible pour les abonnés dans **Configuration de l'espace de travail**. Pour plus d'informations sur l'activation et la désactivation de la fonctionnalité **Favoris** dans Citrix Workspace, consultez Autoriser les favoris.

Authentification à deux facteurs (facultatif)

Avant que les abonnés Workspace puissent utiliser l'authentification à deux facteurs avec Citrix Workspace, ils doivent d'abord enregistrer leur appareil. Lors de l'inscription, Workspace présente un code QR que l'abonné peut scanner avec une application d'authentification. L'application d'authentification doit être conforme à la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO.

> **Remarque :**
>
> Pour faciliter le processus d'enregistrement, Citrix recommande de télécharger et d'installer Citrix SSO sur l'appareil cible au préalable.

Pour s'inscrire à l'authentification à deux facteurs, procédez comme suit :

1. Ouvrez un navigateur, accédez à la page de connexion de Workspace et sélectionnez **Pas de jeton ?**
2. Entrez votre nom d'utilisateur au format `domain\username` ou l'adresse e-mail de votre entreprise, puis sélectionnez **Suivant**. Citrix Cloud envoie ensuite à l'abonné un e-mail contenant un code de vérification temporaire.

3. Entrez le code de vérification et le mot de passe du compte Active Directory lorsque vous y êtes invité et sélectionnez **Suivant**.

   > **IMPORTANT :**
   >
   > Le code de vérification est un jeton temporaire avec une période de validité de 24 heures et n'est utilisé que pour enregistrer l'appareil de l'abonné. L'abonné ne doit pas utiliser ce code pour se connecter à son espace de travail via l'authentification à deux facteurs.

4. À partir de l'application d'authentification, scannez le code QR ou saisissez le code de vérification manuellement.
5. Sélectionnez **Terminer** et **Se connecter** pour terminer l'enregistrement.

Une fois l'enregistrement terminé, les abonnés peuvent revenir à la page de connexion de Workspace et entrer leurs informations d'identification Active Directory, ainsi que le jeton affiché dans leur application d'authentification.

Seuls les codes de vérification générés à partir d'une application d'authentification sur un appareil inscrit sont pris en charge pour l'authentification à deux facteurs. Les abonnés ne doivent pas utiliser le jeton temporaire reçu par e-mail lors du processus d'enregistrement.

Personnaliser les espaces de travail

Vous pouvez personnaliser l'expérience de l'espace de travail des abonnés pour différents utilisateurs et pour répondre aux exigences organisationnelles spécifiques dans **Configuration de l'espace de travail**.

- Pour configurer les notifications ciblées dans le **flux d'activité** et la carte **Actions** des espaces de travail, consultez Personnaliser les notifications de l'espace de travail.
- Pour personnaliser l'apparence des espaces de travail, y compris les logos et les thèmes personnalisés, consultez Personnaliser l'apparence des espaces de travail.
- Pour choisir la façon dont les abonnés interagissent avec leurs espaces de travail, par exemple pour permettre aux abonnés de créer des **favoris** et lancer automatiquement des bureaux, consultez Personnaliser les interactions de l'espace de travail.
- Pour personnaliser les stratégies de confidentialité et de sécurité, consultez Personnaliser les stratégies de sécurité et de confidentialité. Les stratégies de confidentialité et de sécurité incluent des paramètres tels que le délai d'expiration, la stratégie de connexion et la gestion des mots de passe pour les utilisateurs finaux.

Dépannage

Déconnection et reconnexion après la modification de la méthode d'authentification

Après avoir modifié la méthode d'authentification, les abonnés connectés peuvent voir un message d'erreur s'afficher. Les abonnés doivent se déconnecter de Citrix Workspace et fermer le navigateur ou l'application Citrix Workspace, et attendre environ 5 minutes pour se reconnecter. Les abonnés peuvent ensuite se connecter à l'aide de la nouvelle méthode d'authentification.

Pour plus d'informations, consultez l'article Choisir ou modifier les méthodes d'authentification.

Actualisation après la modification de l'abonnement au service

Si vous avez modifié votre abonnement au service, les abonnés devront peut-être actualiser manuellement l'application Citrix Workspace locale. Pour actualiser l'application Citrix Workspace pour Windows, procédez comme suit :

1. Cliquez avec le bouton droit sur l'icône de Citrix Workspace dans la barre d'état système Windows et sélectionnez **Préférences avancées > Réinitialiser Citrix Workspace**.
2. Ouvrez l'application Citrix Workspace pour Windows et sélectionnez **Comptes > Ajouter**.
3. Entrez l'URL de l'espace de travail, puis sélectionnez **Ajouter**.

Vous pouvez également actualiser l'application Citrix Workspace à partir du navigateur. En cas d'actualisation à partir du navigateur, procédez comme suit :

1. Cliquez avec le bouton droit sur l'icône de Citrix Workspace dans la barre d'état système Windows et sélectionnez **Préférences avancées > Réinitialiser Citrix Workspace**.
2. Entrez l'URL de l'espace de travail dans le navigateur et connectez-vous.
3. Téléchargez le fichier de configuration dans **Paramètres > Paramètres du compte > Avancé > Télécharger configuration de Workspace**.

Cela permet de télécharger un fichier avec une extension **.cr** qui ajoute l'espace de travail à votre application Citrix Workspace locale.

Personnaliser l'apparence des espaces de travail

October 12, 2023

Personnaliser l'interface utilisateur de Workspace

Cette section décrit comment personnaliser l'apparence des espaces de travail en mettant à jour les thèmes dans **Configuration > Personnaliser > Apparence**.

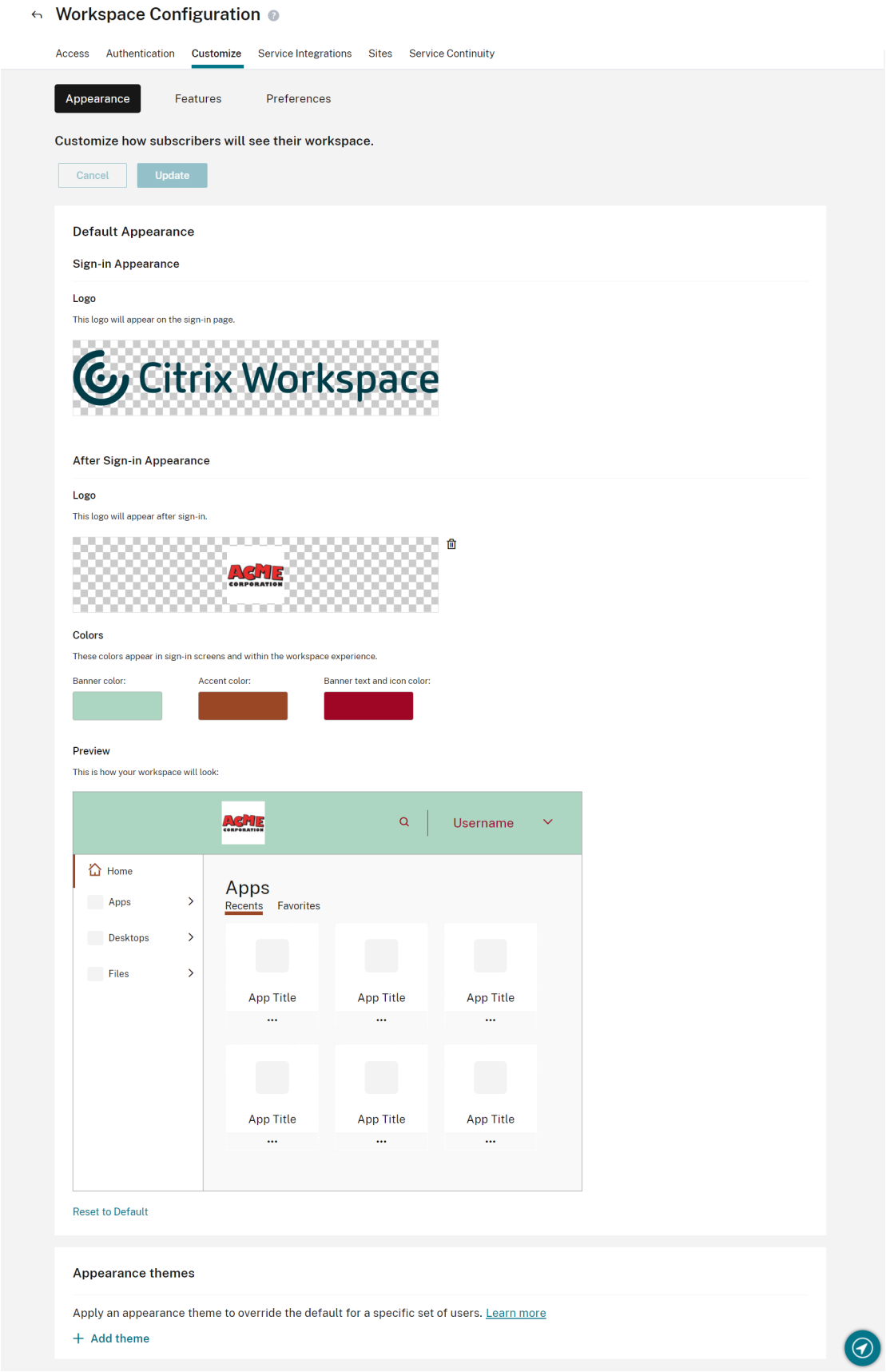
Les thèmes vous permettent de configurer les couleurs et les logos de votre espace de travail. Les logos doivent correspondre aux dimensions requises pour éviter d'apparaître déformés ou d'entraîner un message d'erreur.

Logo	Dimensions requises	Taille maximale	Formats pris en charge
Logo de connexion	480 x 120 pixels	2 Mo	JPEG, JPG ou PNG
Logo après la connexion	340 x 80 pixels	2 Mo	JPEG, JPG ou PNG

Les modifications apportées à l'apparence de l'espace de travail prennent effet immédiatement après la sélection du bouton **Enregistrer**.

Personnaliser votre thème par défaut

Le thème par défaut inclut le logo de connexion, le logo et les couleurs de l'espace de travail que les abonnés voient après leur connexion. Vous pouvez modifier un de ces éléments, certains ou tous pour le thème par défaut.



Personnaliser l'apparence de connexion

Pour la page de connexion, vous ne pouvez remplacer que le logo. Le reste de la page de connexion, y compris les couleurs, n'est pas affecté.

Les modifications apportées à l'apparence de l'espace de travail prennent effet immédiatement. Il faut environ cinq minutes pour que l'interface utilisateur mise à jour s'affiche dans les applications Citrix Receiver locales.

> **Remarque :**
>
> Les modifications apportées au logo de connexion n'affectent pas les utilisateurs qui s'authentifient sur leur espace de travail à l'aide de fournisseurs d'identité tiers, tels que Azure AD et Okta.
>
> Pour plus d'informations sur la personnalisation d'une page de connexion Azure AD, consultez la documentation Microsoft. Pour plus d'informations sur la personnalisation de la page de connexion hébergée par Okta, consultez la documentation du développeur Okta.

Vous pouvez également personnaliser la page de connexion de l'instance Citrix Gateway locale, configurée dans l'appliance Citrix ADC plutôt que dans le menu **Configuration de l'espace de travail**. Pour plus d'informations, consultez l'article du centre de connaissances.

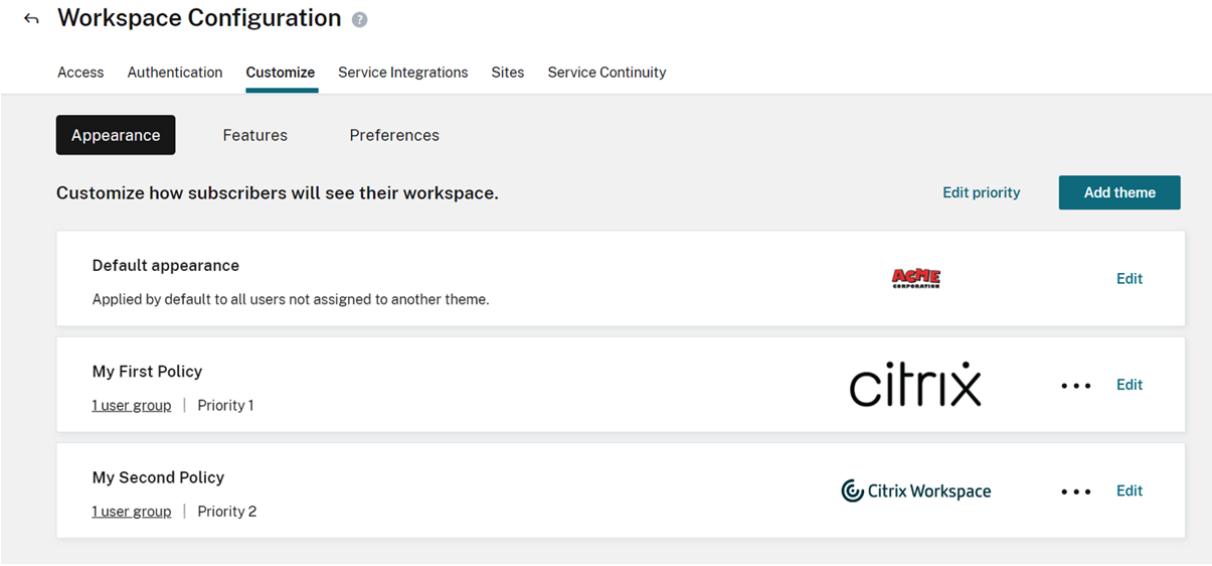
Personnaliser l'apparence des espaces de travail

Le logo de connexion ne doit pas nécessairement être le même que celui qui apparaît en haut à gauche de l'espace de travail après la connexion d'un abonné. En plus de remplacer le logo de l'espace de travail, vous pouvez définir les couleurs de bannière, d'accentuation, de texte et d'icône de l'espace de travail.

Créer plusieurs thèmes personnalisés

> **Important :**
>
> Il s'agit d'une **fonction mono-locataire**. Si votre client est un locataire Citrix Service Provider, il doit avoir son propre emplacement de ressources, ses propres Cloud Connector et un domaine Active Directory dédié. Les locataires Citrix Service Provider qui partagent un emplacement de ressources, des Cloud Connector et un domaine Active Directory dédié (clients multi-locataires) ne sont actuellement pas pris en charge.

Vous pouvez configurer et hiérarchiser plusieurs thèmes Citrix Workspace pour des groupes d'utilisateurs spécifiques. Ces thèmes personnalisés sont répertoriés dans des fiches individuelles sous le thème par défaut. Si vous ne configurez pas plusieurs thèmes, le thème existant (par défaut) est appliqué à tous les utilisateurs.



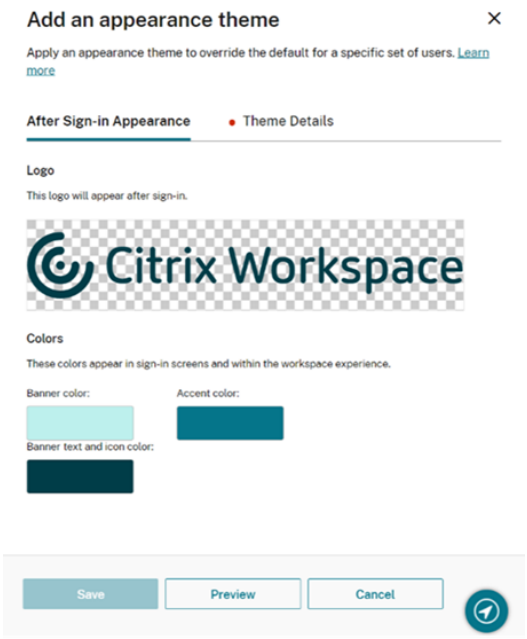
Configurer des thèmes personnalisés

Pour ajouter votre premier thème personnalisé sous votre thème par défaut, sélectionnez **Ajouter un thème** en bas à gauche de la fiche sous la section **Apparence par défaut**.

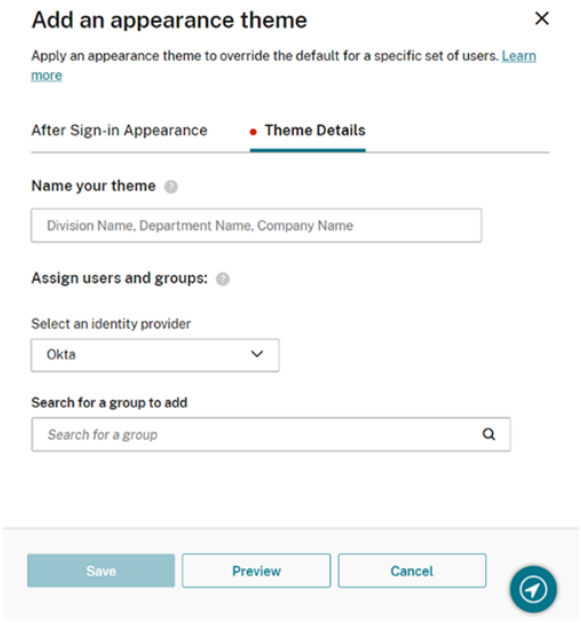
Si vous avez déjà au moins un thème personnalisé sous le thème par défaut, sélectionnez **Ajouter un thème** en haut à droite de la liste des thèmes existants.

1. Configurez votre thème personnalisé :

   a) Téléchargez votre **logo** (facultatif).
   b) Définissez les **couleurs** de la bannière, de l'accentuation, du texte et de l'icône (facultatif).

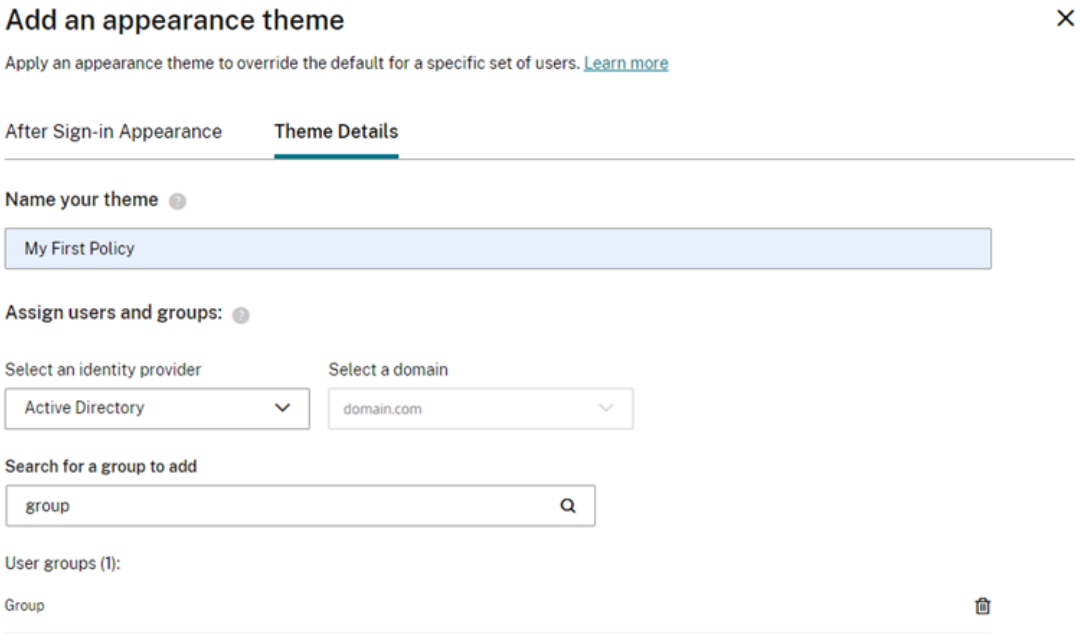


2. Sélectionnez **Détails du thème** et saisissez un nom significatif pour le thème.



3. Affectez des groupes d'utilisateurs au thème :

a) Sélectionnez un fournisseur d'identité et son domaine si vous y êtes invité.
b) Recherchez le groupe d'utilisateurs que vous souhaitez ajouter au thème personnalisé.
c) Sélectionnez le bouton avec le signe plus (**+**) en regard de ce groupe.
d) Répétez cette procédure pour chaque groupe que vous souhaitez ajouter à votre thème.



4. Sélectionnez **Aperçu** pour voir à quoi ressemblera votre espace de travail pour les abonnés. Enregistrez votre thème lorsque vous avez terminé.

> **Remarque :**
>
> L'**aperçu de l'espace de travail** n'affiche pas d'aperçu si vous travaillez actuellement avec l'ancienne interface utilisateur de couleur mauve.

5. Répétez les étapes 1 à 4 pour continuer à ajouter de nouveaux thèmes personnalisés.

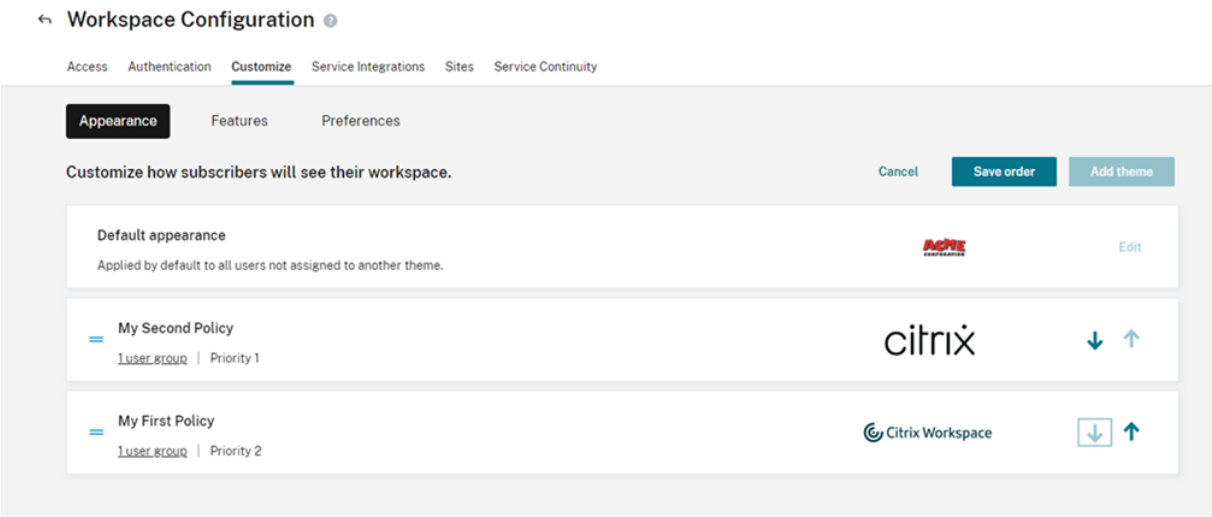
Hiérarchiser les thèmes personnalisés

Un utilisateur peut appartenir à plusieurs groupes d'utilisateurs, chacun pouvant correspondre à un thème différent. Vous pouvez définir le thème qu'un abonné voit s'il en a plusieurs en définissant la priorité des thèmes personnalisés.

> **Important**
>
> Pour que la hiérarchisation relative des thèmes personnalisés fonctionne, vous devez configurer deux thèmes personnalisés ou plus sous le thème par défaut.

1. Sélectionnez **Modifier la priorité** en haut à droite de la liste des thèmes, en regard de **Ajouter un thème**.

2. Vous pouvez réorganiser la priorité des thèmes de l'une des deux manières suivantes :
    - Utilisez les flèches sur le côté droit de chaque thème.
    - Faites glisser les thèmes individuels vers le haut et le bas de la liste à l'aide de la poignée située à gauche de la fiche.
3. Une fois que vous avez réorganisé les éléments, sélectionnez **Enregistrer l'ordre**.



Personnaliser les interactions de l'espace de travail

November 28, 2023

Personnalisez la manière dont les abonnés interagissent avec leurs espaces de travail dans **Configuration de l'espace de travail > Personnaliser > Préférences**.

Si vous souhaitez personnaliser les préférences de l'espace de travail qui affectent l'expérience de connexion afin de répondre aux exigences de votre entreprise, consultez Personnaliser les stratégies de sécurité et de confidentialité de l'espace de travail.

Si vous souhaitez personnaliser l'apparence de l'espace de travail avant et après la connexion, consultez Personnaliser l'apparence des espaces de travail

Autoriser la mise en cache

Le paramètre **Autoriser la mise en cache** améliore les performances des abonnés qui accèdent à Citrix Workspace via un navigateur Web. La mise en cache est prise en charge lors de l'accès à Citrix Workspace à l'aide d'un navigateur Web compatible. La mise en cache n'est pas disponible lors de l'utilisation d'une application Citrix Workspace installée localement.

Lorsque cette option est activée, certaines données sensibles peuvent être stockées localement sur les appareils des abonnés. Ces données sont constituées de métadonnées de fichier et sont chiffrées avec une clé unique à l'identité authentifiée de l'abonné. Les données chiffrées sont stockées dans la propriété `localStorage` du navigateur Web sur l'appareil de l'abonné.

Si vous désactivez la mise en cache, les données chiffrées sont purgées la prochaine fois que l'abonné se connecte à Citrix Workspace via son navigateur Web. En outre, l'abonné peut purger ces données manuellement en effaçant les données de navigation de son navigateur Web.

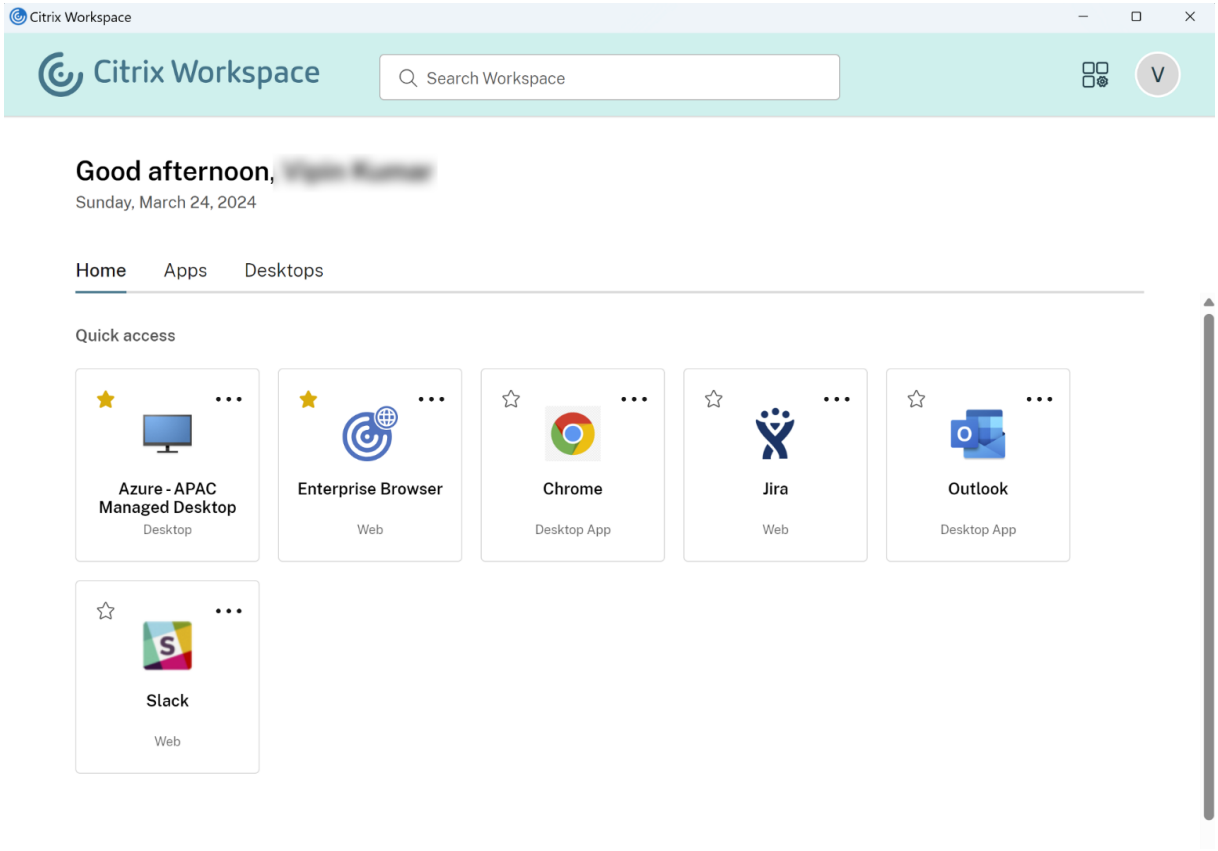
Autoriser les favoris

Les clients qui ont accès à **Configuration de l'espace de travail** et à la nouvelle expérience d'espace de travail peuvent permettre aux abonnés d'ajouter des ressources d'application et de bureau aux favoris ou de les en retirer. La fonctionnalité **Autoriser les favoris** est activée par défaut.

> **Remarque :**
>
> - Pour certains clients existants (nouveaux utilisateurs de Workspace entre décembre 2017 et avril 2018), l'option **Autoriser les favoris** est définie sur **Désactivé** par défaut. L'administrateur peut décider quand activer cette fonctionnalité pour ses abonnés.

Expérience des abonnés avec l'option Autoriser les favoris

Lorsque cette option est activée (par défaut), les abonnés peuvent ajouter jusqu'à 250 **favoris** à l'aide de l'icône étoile située dans le coin supérieur gauche de chaque fiche d'application (non obligatoire) et de bureau. L'étoile se remplit de jaune lors de l'ajout aux favoris.



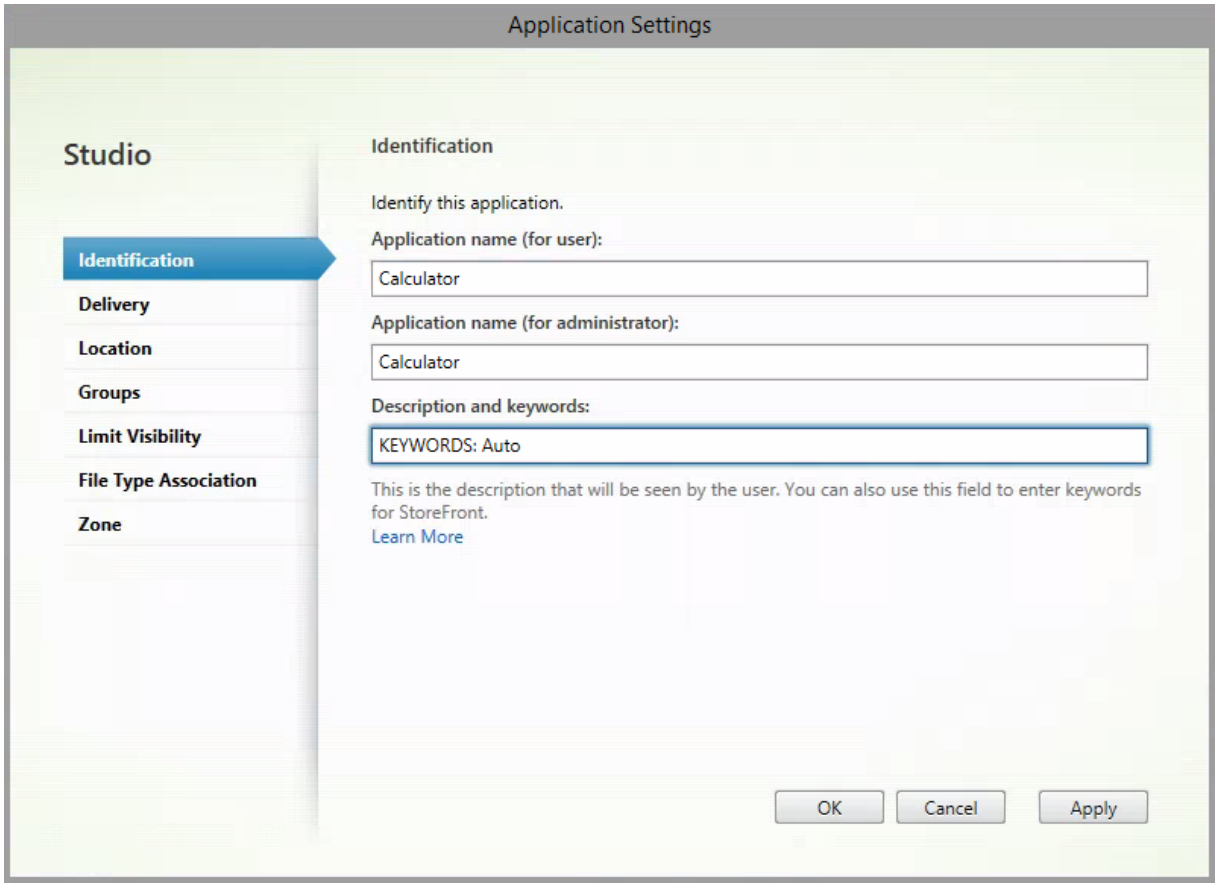
Si un abonné ajoute plus de 250 ressources en tant que favoris, la « préférée la plus ancienne » est supprimée (ou la plus proche pour conserver les **favoris** les plus récents).

Lorsque cette option est désactivée, les abonnés à l'espace de travail ne voient pas d'étoiles sur les fiches d'application et de bureau, ni les sous-menus **Toutes les applications** et **Favoris** de ces ressources dans la barre de navigation. Les applications et bureaux ajoutés aux **favoris** ne sont pas supprimés et peuvent être récupérés si vous réactivez les **favoris**.

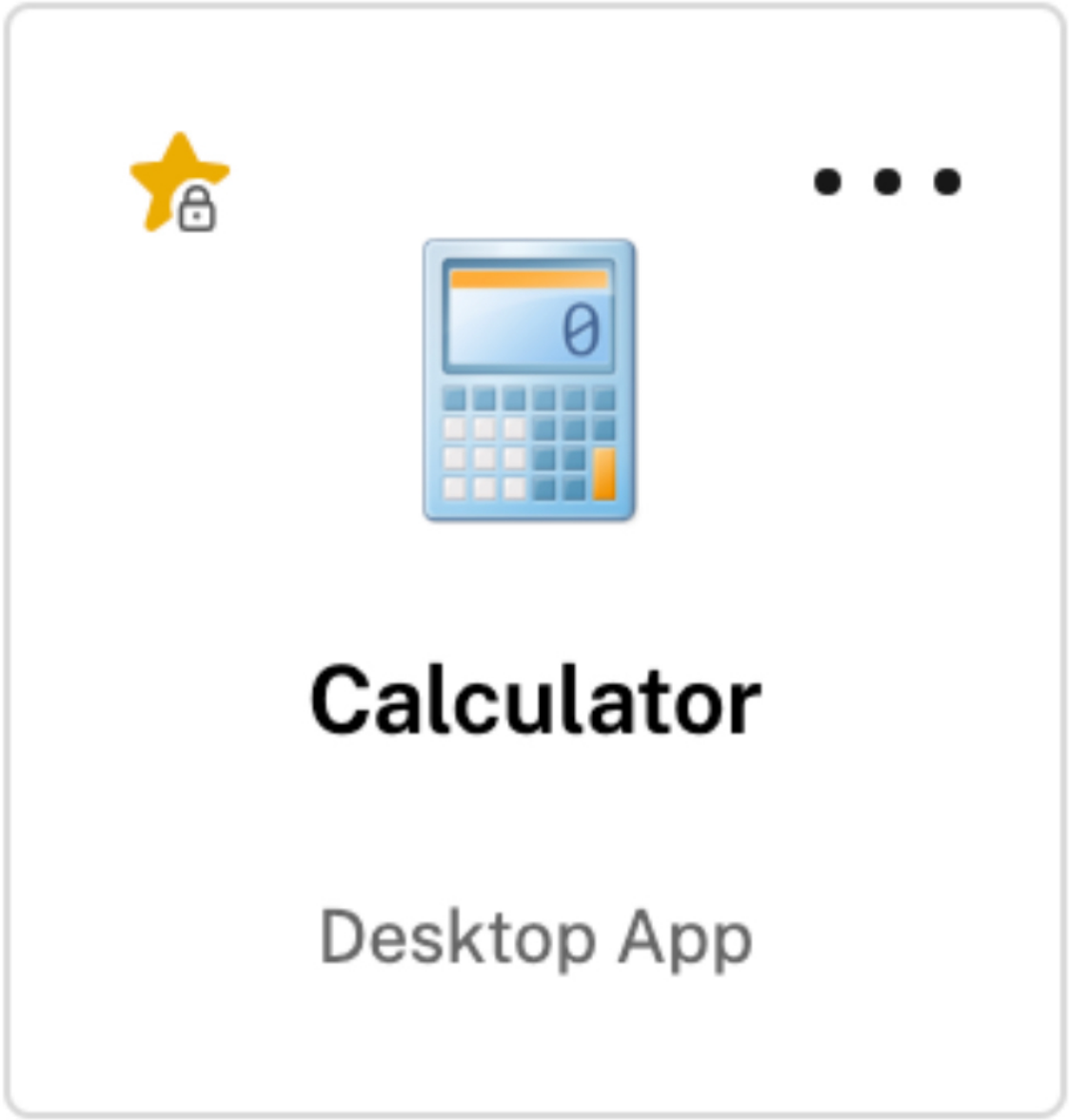
> **Remarque :**
>
> Si vos abonnés n'ont pas accès aux bureaux configurés, la sélection de bureaux dans la barre latérale ne s'affiche pas.

Mots clés pour applications et bureaux

Les administrateurs peuvent ajouter automatiquement des **applications préférées** pour les abonnés en utilisant les paramètres `KEYWORDS:Auto` et `KEYWORDS:Mandatory` dans Citrix DaaS (**Gérer** > **Configuration complète** > **Applications**).



- **KEYWORDS:Auto**. L'application ou le bureau est ajouté en tant que **favori**, et les abonnés peuvent supprimer le **favori**.
- **KEYWORDS:Mandatory**. L'application ou le bureau est ajouté en tant que **favori**, et les abonnés ne peuvent pas supprimer le **favori**. Les applications et bureaux obligatoires affichent une icône étoile avec un cadenas pour indiquer qu'ils ne peuvent pas être retirés des favoris.



> **Remarque :**
>
> Si vous utilisez les mots-clés **Mandatory** et **Auto** pour une application, le mot-clé **Mandatory** remplace le mot-clé **Auto**, et l'application ou le bureau ne peut pas être supprimé des favoris.

Pour un abonné ayant accès uniquement aux applications et aux bureaux dont le mot-clé est **Mandatory** :

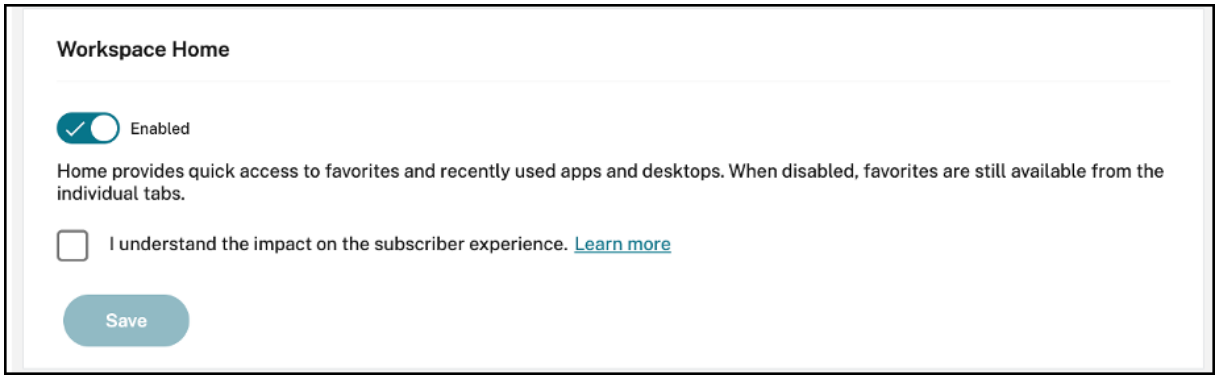
- L'abonné ne voit que la page **Applications** dans le panneau de navigation de gauche de Workspace. La page **Favoris** n'apparaît pas dans le panneau gauche : il n'y a aucune différence entre les applications qui apparaissent sur la page **Applications** ou sur la page **Favoris**.
- L'abonné ne voit pas l'onglet **Favoris** sur la page d'accueil. Seul l'onglet **Récents** s'affiche.

Activer ou désactiver l'écran d'accueil pour les utilisateurs (Tech Preview)

Vous pouvez activer ou désactiver la page d'**accueil** de vos utilisateurs afin d'améliorer l'organisation de leurs applications.

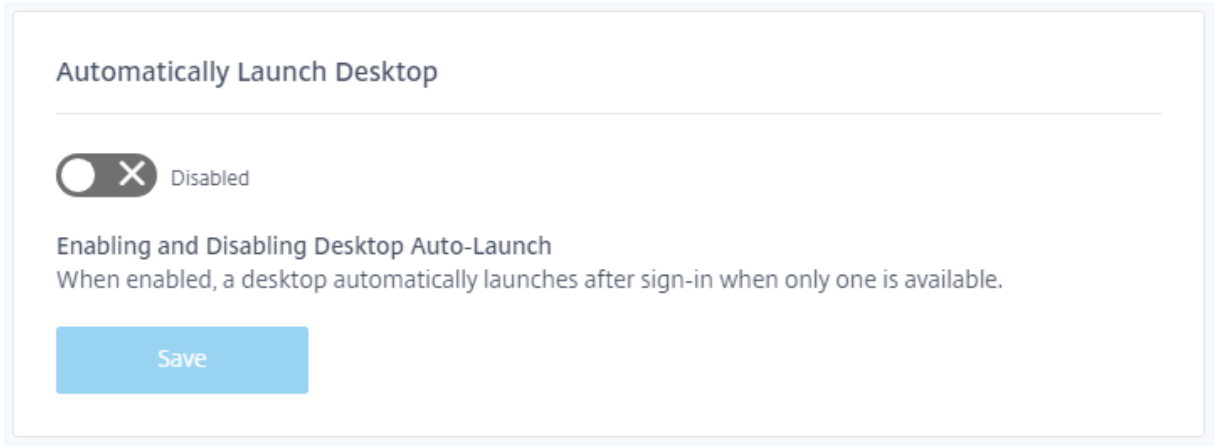
Cette fonctionnalité s'applique lorsque les utilisateurs disposent de plus de 20 applications sur leur bureau. Si les utilisateurs disposent de 20 applications ou moins, ils ne verront qu'une seule vue sans options de navigation ni de recherche.

Pour configurer les paramètres, accédez à **Configuration de l'espace de travail > Personnaliser > Apparence**. Lorsque le bouton bascule est activé, les utilisateurs sont redirigés vers la page d'**accueil**. Si vous désactivez le bouton bascule, les utilisateurs accèdent directement à la page **Applications**. Par défaut, le bouton bascule est activé et la fonctionnalité est activée.



Lancer bureau automatiquement

L'option **Lancer bureau automatiquement** est disponible pour les clients qui ont accès à la **configuration de l'espace de travail** et à la nouvelle expérience de l'espace de travail. La préférence s'applique uniquement à l'accès à l'espace de travail à partir d'un navigateur.



Lorsqu'il est désactivé (par défaut), le paramètre empêche Citrix Workspace de démarrer automatiquement un bureau lorsqu'un abonné se connecte. Les abonnés doivent lancer manuellement leur

bureau après la connexion.

Lorsque que le paramètre est activé, si un abonné ne dispose que d'un bureau disponible, le bureau se lance automatiquement lorsque l'abonné se connecte à son espace de travail.

Les applications de l'abonné ne sont pas reconnectées, quelle que soit la configuration du contrôle de l'espace de travail.

> **Remarque :**
>
> Pour permettre à Citrix Workspace de lancer automatiquement des postes, les abonnés qui accèdent au site via Internet Explorer doivent ajouter l'URL de l'espace de travail à la zone Intranet local ou Sites de confiance.

Sessions de fournisseur d'identité fédéré

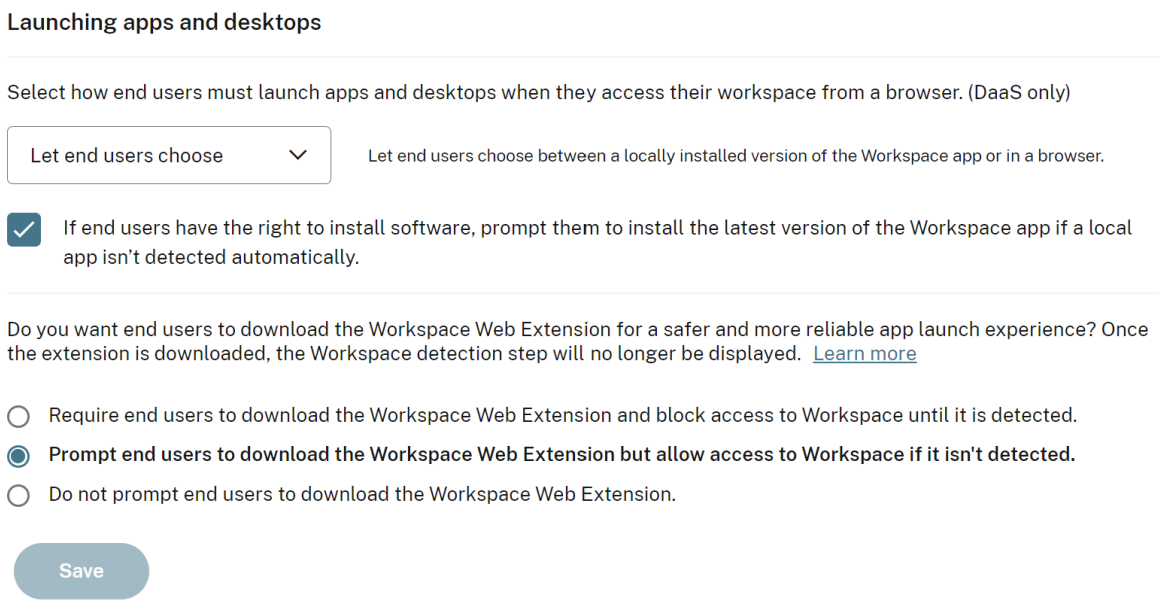
Lorsque Workspace est configuré pour utiliser un fournisseur d'identité fédéré, la session d'authentification et sa durée de vie sont généralement contrôlées par le fournisseur d'identité. Le paramètre **Sessions de fournisseur d'identité fédéré** permet de transférer le contrôle au fournisseur de services. Lorsqu'il est activé (par défaut), Workspace impose que les utilisateurs s'authentifient auprès du fournisseur d'identité lorsqu'une nouvelle session Workspace est nécessaire. Lorsqu'il est désactivé, un abonné n'est pas invité à s'authentifier auprès du fournisseur d'identité s'il accède à Workspace avec une session valide.

Si ce paramètre est activé et que vous utilisez Azure AD pour l'authentification auprès de Workspace, les abonnés peuvent être invités à se reconnecter même si un jeton d'authentification Microsoft valide est présent pour leur session. Pour plus d'informations sur ce scénario, consultez l'article CTX253779.

Lancement d'applications et de bureaux

L'option **Lancement d'applications et de bureaux** est disponible pour les clients qui ont accès à **Configuration de l'espace de travail** et à la nouvelle expérience Espace de travail. La préférence est disponible pour les nouveaux clients et les clients existants. Toutefois, l'introduction de cette fonctionnalité ne modifie aucun paramètre pour les clients existants.

La préférence s'applique à la façon dont les utilisateurs ouvrent les applications et les bureaux fournis par **Citrix DaaS** uniquement. Il peut s'agir du service ou de l'application locale **Citrix DaaS** accédé(e) à partir de la fonctionnalité Agrégation de sites. L'option **Lancement d'applications et de bureaux** ne s'applique pas, par exemple, aux applications SaaS mises à disposition par Citrix Gateway Service.



Choisissez l'un des paramètres suivants :

- **Dans une application native** (par défaut) : les utilisateurs finaux doivent utiliser une version installée localement de l'application Workspace.
- **Dans un navigateur :** les utilisateurs finaux doivent utiliser une version de navigateur de l'application Workspace pour HTML5.
- **Laissez les utilisateurs choisir :** les utilisateurs finaux peuvent choisir entre une version installée localement de l'application Workspace ou lancer des applications et des bureaux dans un navigateur.

Une option supplémentaire pour les paramètres **Dans une application native** et **Laisser les utilisateurs choisir** invite les utilisateurs à installer la dernière version de l'application Citrix Workspace si une application locale ne peut pas être détectée automatiquement. Supprimez cette sélection si vos abonnés ne disposent pas des droits nécessaires pour installer le logiciel.

Intégrer Microsoft Teams à Workspace

Grâce à l'intégration de Microsoft Teams, les abonnés peuvent partager des fiches depuis le **flux d'activités** de leur espace de travail avec d'autres abonnés via des canaux dans Microsoft Teams.

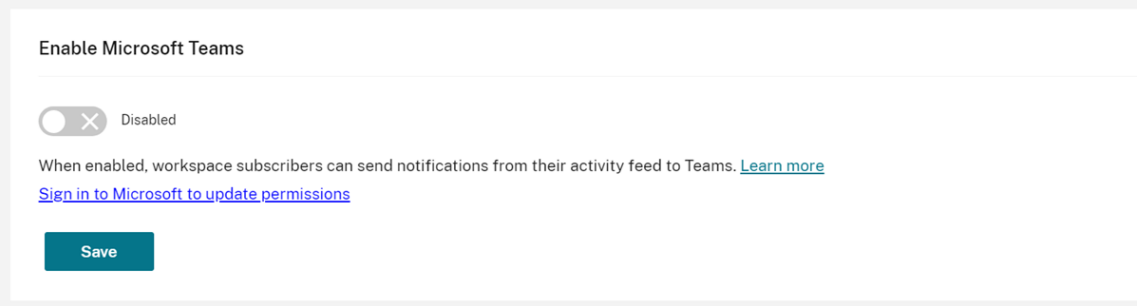
Exigences

- Vous devez être un administrateur avec **accès complet** dans Citrix Cloud pour activer l'intégration de Microsoft Teams. Les administrateurs disposant d'un **accès personnalisé** ne disposent pas des autorisations requises pour activer l'intégration de Microsoft Teams.

- Vous devez configurer l'authentification Azure AD dans **Gestion des identités et des accès**. Pour plus d'informations sur la configuration de l'authentification Azure AD, consultez la section Connecter Azure Active Directory à Citrix Cloud.
- Vous ne pouvez utiliser qu'une seule instance Azure AD avec Microsoft Teams. Si l'instance Azure AD que vous configurez a activé Microsoft Teams via un autre compte Citrix Cloud, vous ne pouvez pas activer l'intégration Microsoft Teams pour votre compte Citrix Cloud.
- La fonction **IwsMicrosoftTeams** doit être activée.
- Les fonctions **Actions et flux d'activités** doivent être activées pour les espaces de travail.
- Les abonnés à l'espace de travail doivent installer le client de bureau Microsoft Teams.

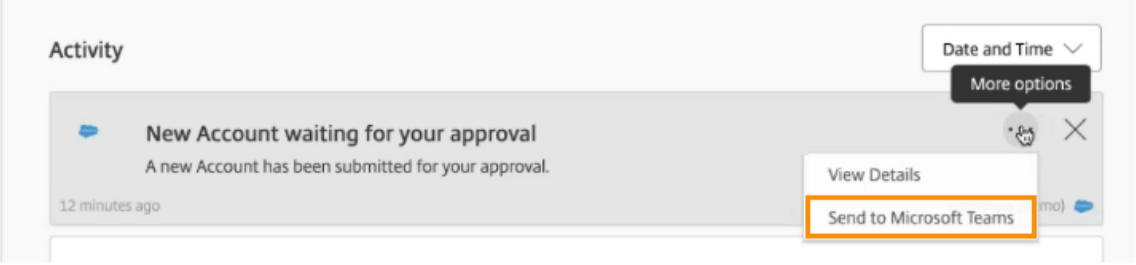
Activer l'intégration de Microsoft Teams

1. Après vous être connecté à Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.
2. Sélectionnez **Personnaliser**, puis l'onglet **Préférences**.
3. Sous **Activer Microsoft Teams**, sélectionnez le bouton Activer/désactiver.



4. Sélectionnez **Enregistrer**.

   Les utilisateurs Workspace peuvent désormais afficher l'option **Envoyer à Microsoft Teams** et partager des fiches à partir de Workspace. Les utilisateurs peuvent avoir besoin d'actualiser leurs écrans (Ctrl+F5).

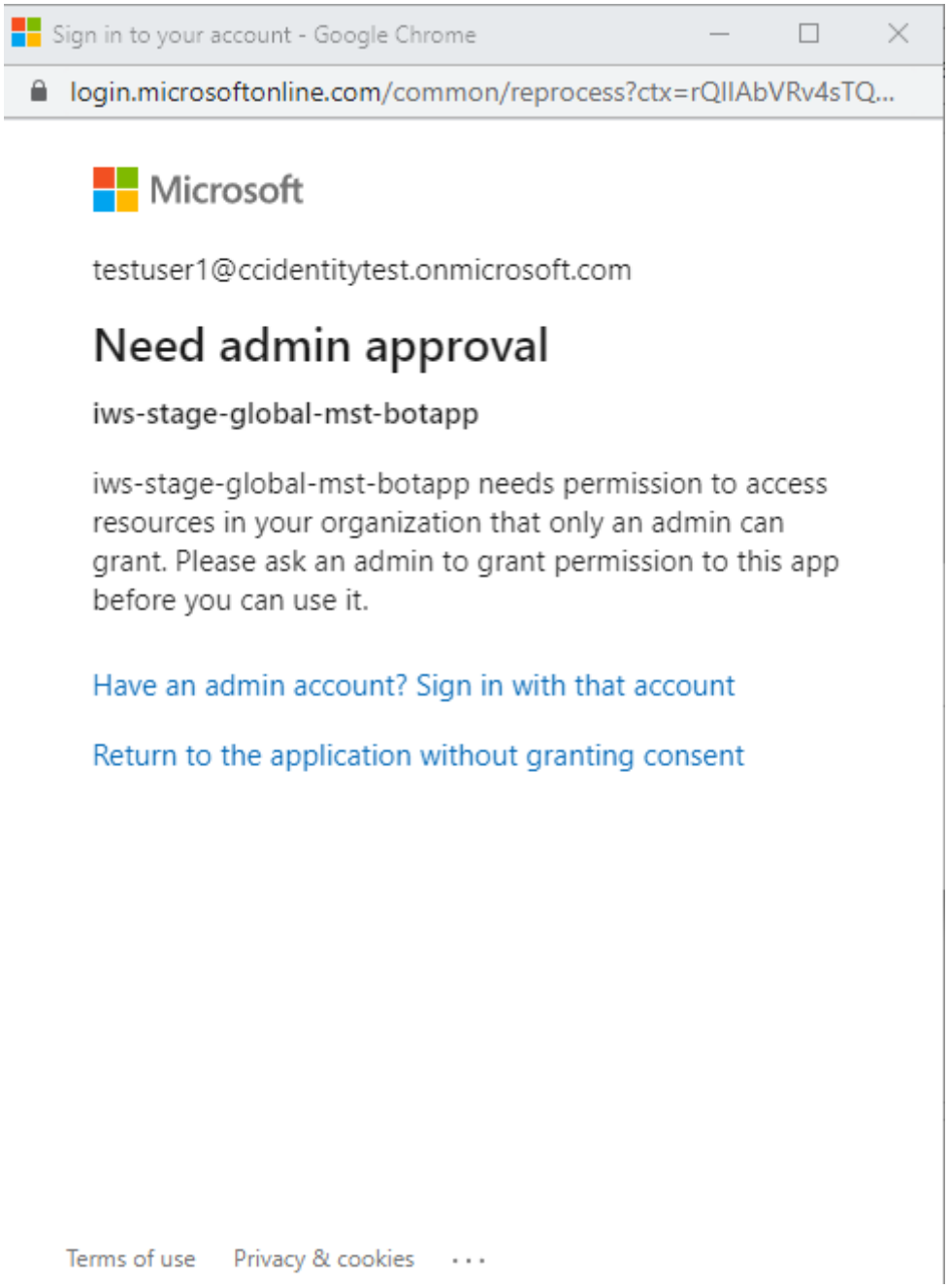


Accepter les autorisations Workspace

D'autres étapes de configuration sont nécessaires pour activer cette intégration. Le compte **Administrateur Microsoft** doit accepter les autorisations de l'intégration dans l'interface utilisateur

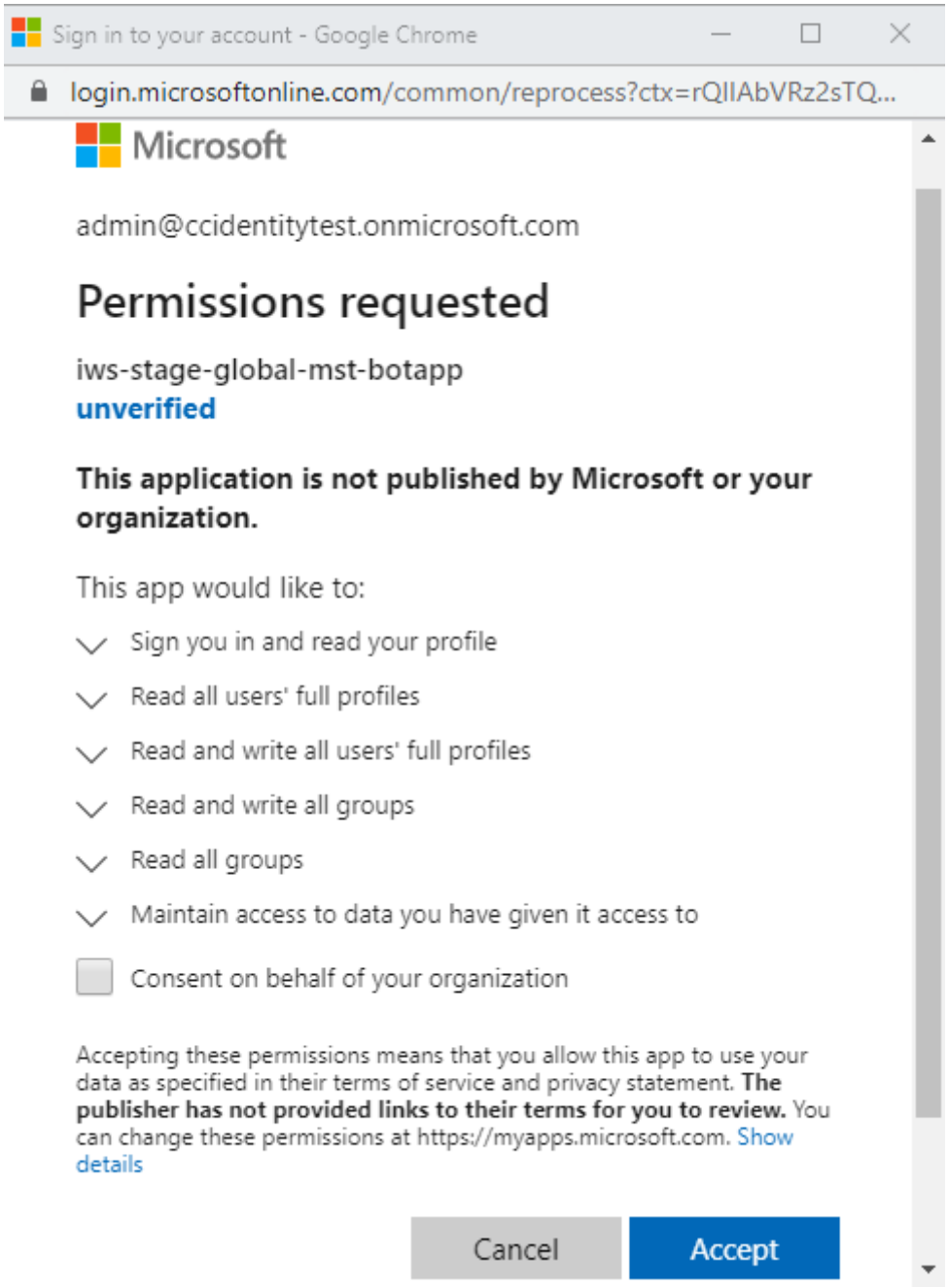
Workspace afin que les utilisateurs de votre organisation puissent partager des fiches avec Microsoft Teams.

1. Connectez-vous à n'importe quel compte d'espace de travail et essayez de partager une fiche.
2. Si le compte **Administrateur Microsoft** n'a pas encore accepté les autorisations de l'intégration à Microsoft Teams et que vous essayez de vous connecter avec un compte non administrateur, le message suivant s'affiche :



3. Pour accepter les autorisations, connectez-vous à votre compte administrateur en sélection-

nant **Vous possédez un compte administrateur ? Connectez-vous avec ce compte**. Les autorisations suivantes pour accéder aux données sont requises pour activer l'intégration de Microsoft Teams avec Citrix Workspace :



4. Lorsque la boîte de dialogue **Autorisations acceptées** s'ouvre, vérifiez les options. L'option **Consentement pour le compte de votre organisation** accorde des autorisations à tous les abonnés Workspace associés à cet administrateur. Sinon, les autorisations sont accordées uniquement pour le compte administrateur.
5. Sélectionnez **Accepter**.

Personnaliser les stratégies de sécurité et de confidentialité

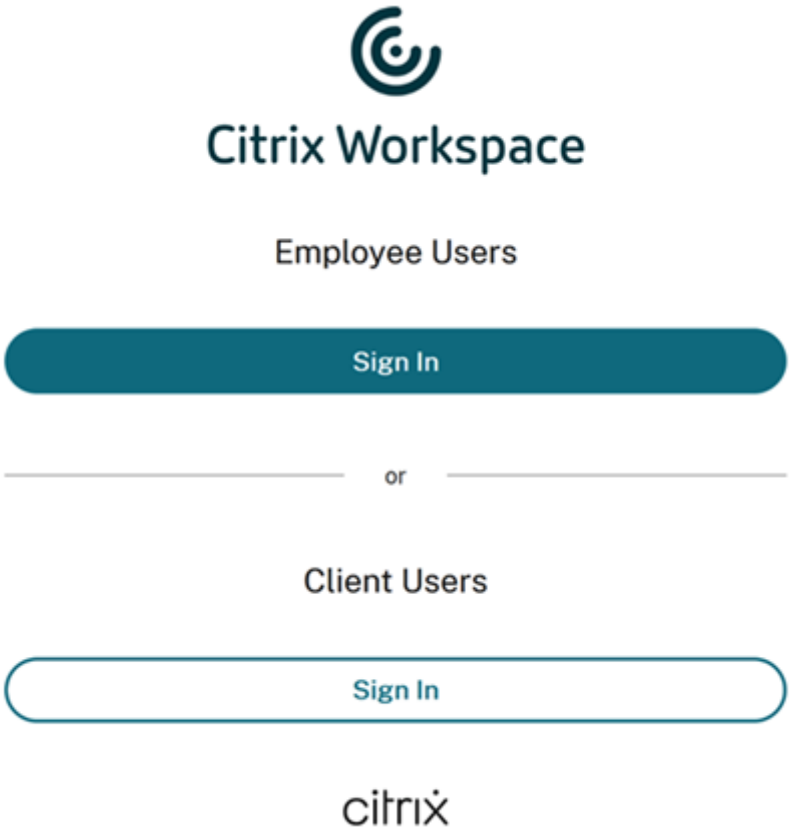
November 28, 2023

Cet article fournit des conseils sur la façon de personnaliser l'expérience de connexion une fois que vous avez déjà configuré l'accès et l'authentification à l'espace de travail.

Pour obtenir une vue d'ensemble des étapes de configuration de l'accès et de l'authentification à l'espace de travail, consultez Configurer l'accès. Pour plus d'informations sur la façon de configurer l'authentification des abonnés aux espaces de travail, consultez Espaces de travail sécurisés.

Créer un flux de connexion utilisateur unifié

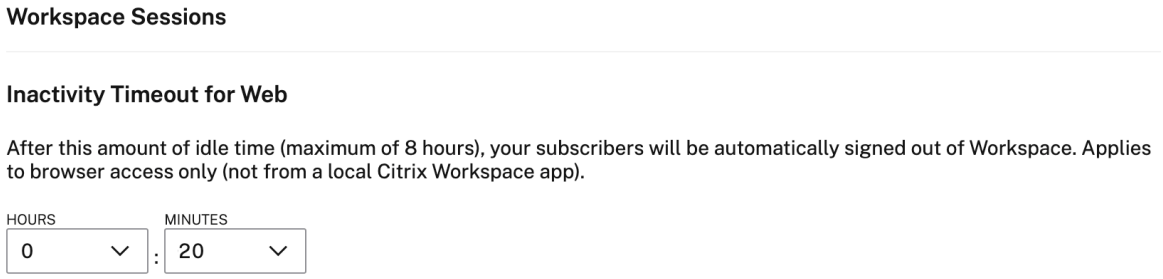
L'expérience de connexion par défaut est un écran partagé pour les utilisateurs employés et les utilisateurs clients (externes).



Pour supprimer l'écran partagé, accédez à **Configuration de l'espace de travail > Authentification > Flux de connexion utilisateur unifié** et sélectionnez **Activer**. L'activation de cette fonctionnalité permet à tous les utilisateurs de bénéficier de la même option de connexion.

Définir le délai d'inactivité pour l'application Workspace et Web sur les bureaux et appareils mobiles

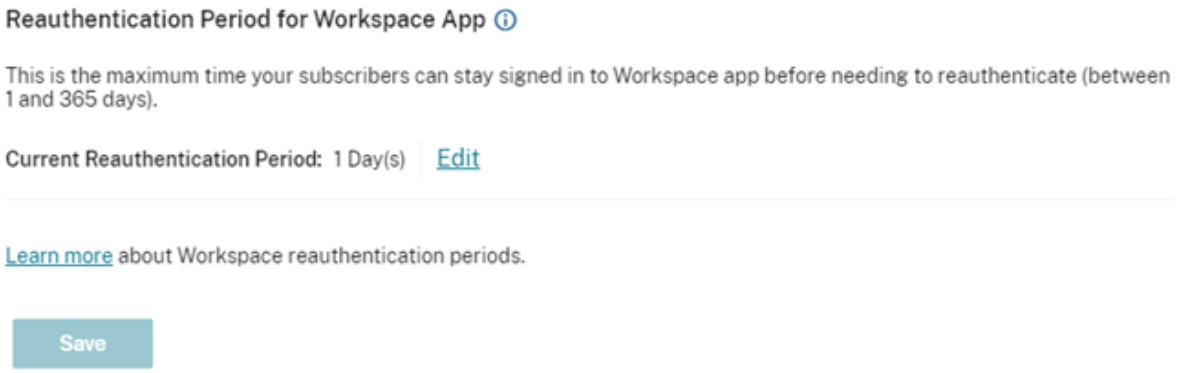
Utilisez le paramètre **Délai d'inactivité du Web** dans **Configuration de l'espace de travail > Personnaliser > Préférences** pour spécifier la durée d'inactivité autorisée (8 heures maximum) avant que les abonnés ne soient automatiquement déconnectés de Citrix Workspace. Vous pouvez également activer le délai d'inactivité pour l'application Workspace sur les bureaux et appareils mobiles en sélectionnant la case de configuration correspondante.



Contrairement à la déconnexion manuelle, qui déconnecte les sessions DaaS, les abonnés restent connectés à leurs sessions DaaS après l'expiration du délai d'inactivité.

Définir une période de réauthentification pour l'application Citrix Workspace

Utilisez le paramètre **Période de réauthentification de l'application Workspace** dans **Configuration de l'espace de travail > Personnaliser > Préférences** pour spécifier la durée pendant laquelle les abonnés peuvent rester connectés à l'application Citrix Workspace avant de devoir se connecter à nouveau.



Par défaut, ce paramètre exige que les abonnés se connectent toutes les 24 heures (un jour). Vous pouvez spécifier une période de réauthentification plus longue pouvant aller jusqu'à 365 jours. Les périodes de réauthentification plus longues nécessitent le consentement des abonnés pour rester connectés. Pour les utilisateurs provisionnés après le 27 septembre 2021, une période de 30 jours est requise pour que les abonnés puissent se reconnecter.

Pendant la période de réauthentification que vous avez définie, les abonnés restent connectés, sauf s'ils sont inactifs pendant 14 jours ou plus à la fois. Si un abonné est inactif pendant 14 jours ou plus, il est invité à se réauthentifier la prochaine fois qu'il tente d'accéder à son espace de travail.

Vous pouvez invalider la session pour vos abonnés en téléchargeant ce script PowerShell et en suivant les instructions incluses dans le téléchargement. Une fois les sessions invalidées, les abonnés doivent se réauthentifier auprès de leurs espaces de travail dans les 24 heures qui suivent.

Si vous devez définir la période de réauthentification pour l'application Citrix Workspace sur moins de 24 heures, vous pouvez le faire via PowerShell.
Pour plus d'informations, consultez l'article Steps to configure InactivityTimeoutInMinutes.

Clients de l'application Workspace pris en charge

Les versions suivantes de l'application Citrix Workspace prennent en charge cette fonctionnalité :

- Application Workspace pour Windows 2106 ou version ultérieure
- Application Workspace pour Mac 2106 ou version ultérieure
- Application Workspace pour iOS 21.6.5 ou version ultérieure
- Application Workspace pour Android 21.6.0 ou version ultérieure

Méthodes d'authentification prises en charge

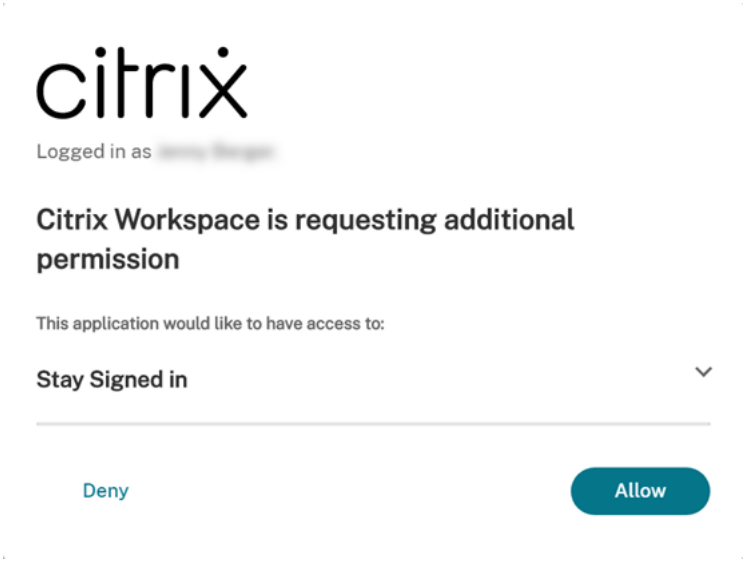
Le maintien de la connexion à l'application Citrix Workspace est pris en charge pour les méthodes d'authentification suivantes :

- Active Directory
- Active Directory + jeton
- Azure Active Directory
- Citrix Gateway
- Okta

> **Remarque :**
>
> Pour bénéficier de la même expérience qu'un client Citrix DaaS utilisant Okta ou Azure Active Directory, configurez le service d'authentification fédérée Citrix (FAS). Pour plus d'informations sur FAS, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Expérience d'abonné pour rester connecté

Lorsque les abonnés se connectent à Workspace sur leur appareil, Workspace les invite à consentir à rester connectés.



Lorsque l'abonné sélectionne **Autoriser**, il reste connecté pendant la période de réauthentification. Si aucune activité n'est détectée sur l'appareil d'un abonné pendant quatre jours, l'abonné est automatiquement invité à se réauthentifier. Une fois qu'il s'est connecté à l'application Citrix Workspace, la période de réauthentification reste en vigueur tant qu'il utilise ses applications et ses bureaux sur l'appareil.

Si l'abonné sélectionne **Refuser**, Workspace l'invite à se reconnecter. Par la suite, Workspace invite l'abonné à se connecter à nouveau après 24 heures.

Si le mot de passe de l'abonné change, il doit se déconnecter et se reconnecter via l'application Citrix Workspace pour que la période de réauthentification continue de fonctionner.

Autoriser les abonnés à modifier le mot de passe de compte

> **Remarque :**
>
> Cette fonctionnalité est en cours de déploiement auprès des clients de manière incrémentielle. Il se peut que cette fonctionnalité ne s'affiche pas tant que le processus de déploiement n'est pas terminé.
>
> L'un des objectifs de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour de produits aux clients de Citrix Workspace lorsqu'elles sont disponibles. Ce processus est transparent pour l'utilisateur. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet de garantir la qualité des produits et de maximiser la disponibilité.

Le paramètre **Autoriser la modification du mot de passe du compte** dans **Configuration de l'espace de travail > Personnaliser > Préférences** contrôle si les abonnés peuvent modifier leur mot de passe de domaine à partir de Citrix Workspace. Vous pouvez également fournir des conseils aux abonnés afin de créer des mots de passe valides conformément à la stratégie de mot de passe de votre organisation.

Lorsque cette option est activée (par défaut), les abonnés peuvent modifier leur mot de passe à tout moment, en fonction des paramètres Active Directory de votre organisation. Si cette option est désactivée, Workspace invite les abonnés à modifier leur mot de passe lorsqu'il expire, mais ils ne peuvent pas modifier leur mot de passe non expiré dans Workspace.

Méthodes d'authentification prises en charge

- Active Directory
- Active Directory + jeton

Clients de l'application Workspace pris en charge

Les versions suivantes de l'application Citrix Workspace prennent en charge cette fonctionnalité :

- Application Workspace pour Windows 2101 ou version ultérieure

- Application Workspace pour Mac 2012 ou version ultérieure
- Application Workspace pour Chrome 2010 ou version ultérieure
- Application Workspace pour HTML5 2101 ou version ultérieure
- Application Workspace pour Android 21.1.0 ou version ultérieure

Les abonnés peuvent également utiliser cette fonctionnalité lorsqu'ils accèdent à des espaces de travail avec la dernière version des navigateurs Web Edge, Chrome, Firefox ou Safari.

Cette fonctionnalité n'est pas prise en charge sur les anciennes versions de l'application Citrix Workspace et de l'application Citrix Workspace pour Linux.

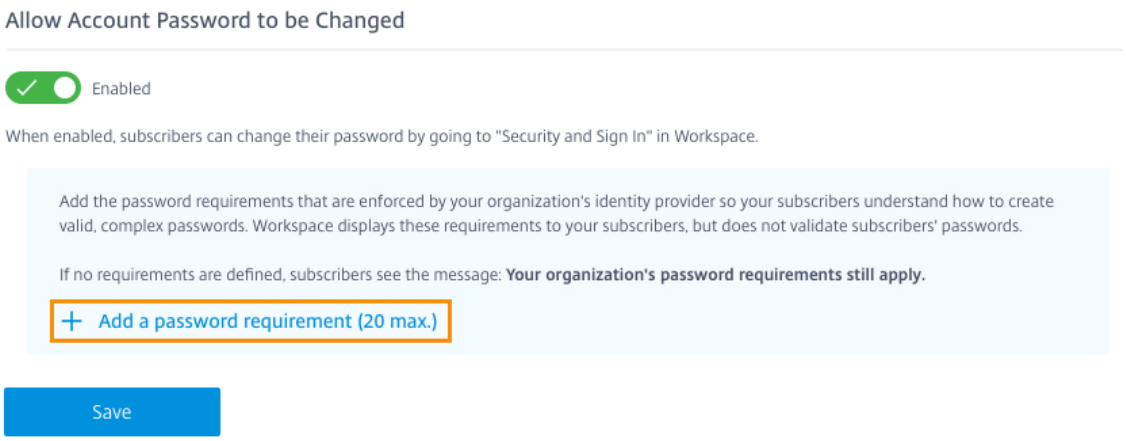
Conseils sur les mots de passe

Vous pouvez ajouter jusqu'à 20 exigences de mot de passe qui répondent à la stratégie de sécurité de votre organisation et que votre fournisseur d'identité applique. Workspace affiche ces exigences en tant que guide lorsque les abonnés modifient leur mot de passe à partir de la page **Paramètres du compte** dans Workspace. Si vous n'ajoutez aucune exigence de mot de passe, Workspace affiche le message « Les exigences de mot de passe de votre organisation s'appliquent toujours. »

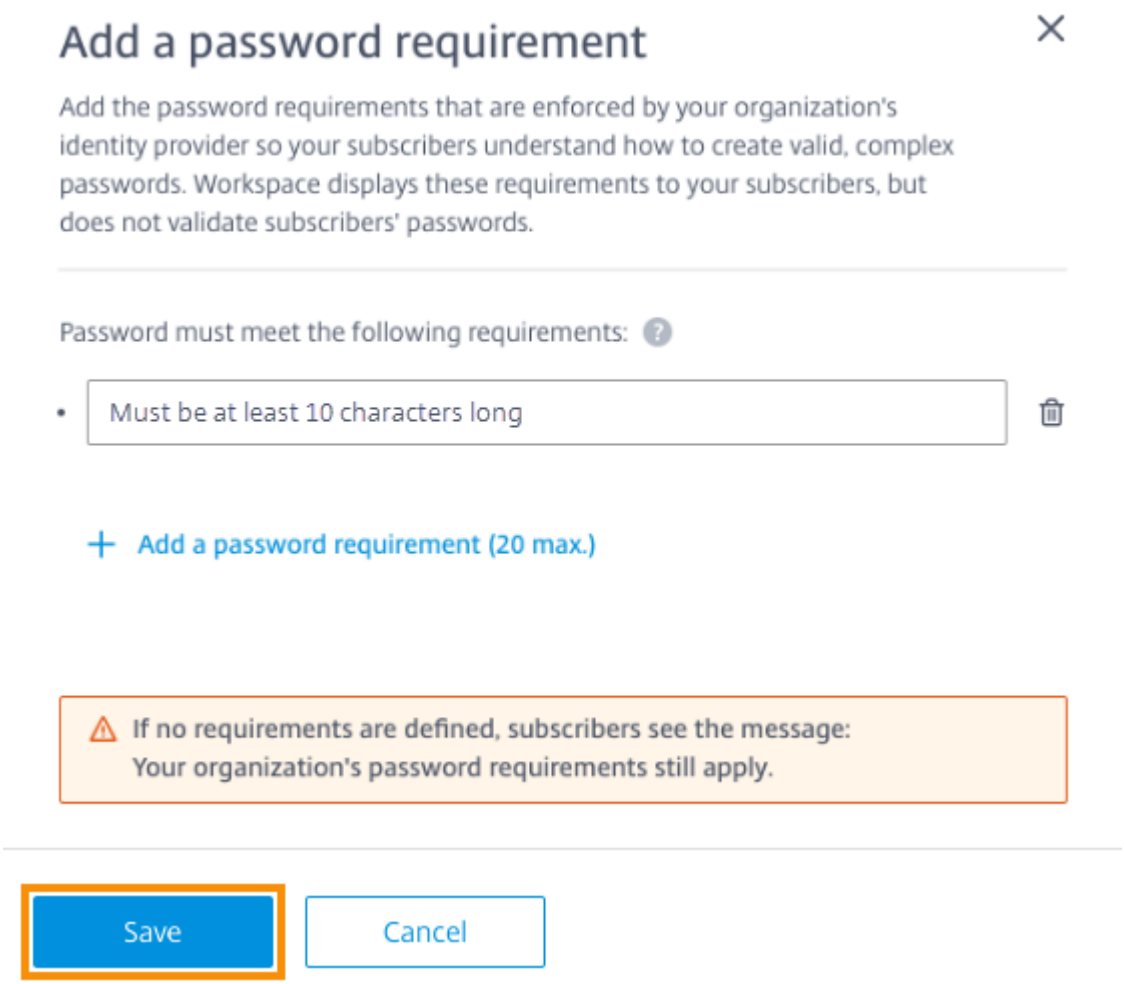
> **Important :**
>
> Citrix Workspace ne valide pas les nouveaux mots de passe saisis par vos abonnés. Si un abonné tente de changer son mot de passe valide par un mot de passe non valide via Workspace, votre fournisseur d'identité rejette le nouveau mot de passe. Le mot de passe existant n'est pas modifié.

Pour ajouter des exigences de mot de passe :

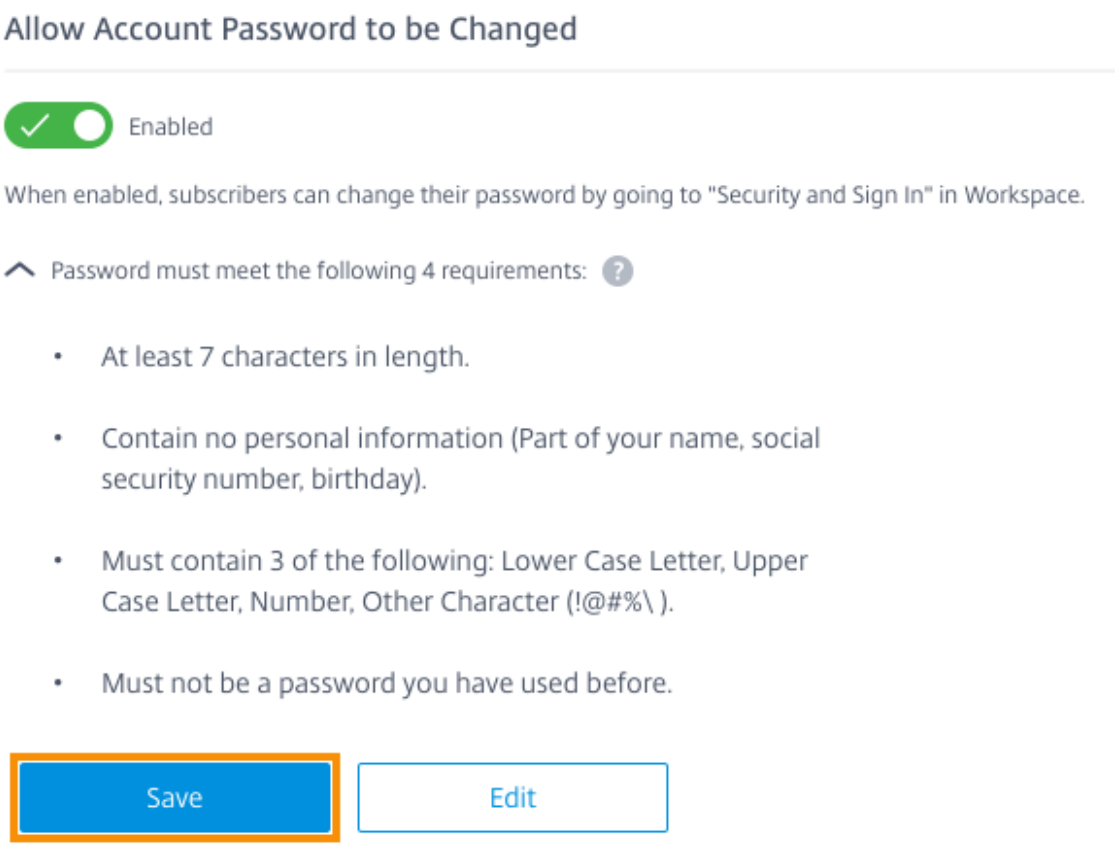
1. Accédez à **Configuration de l'espace de travail > Personnaliser > Préférences**.
2. Sous **Autoriser la modification du mot de passe du compte**, vérifiez que le paramètre est activé. Si cette option est désactivée, activez le paramètre.
3. Sélectionnez **Ajouter une exigence de mot de passe**.



4. Entrez une exigence qui correspond à chacune des exigences de sécurité existantes de votre organisation pour les mots de passe valides. Par exemple, vous pouvez spécifier qu'un mot de passe doit avoir une certaine longueur de caractère. Sélectionnez **Ajouter une exigence de mot de passe** pour ajouter d'autres éléments que vous souhaitez afficher aux abonnés lorsqu'ils modifient leur mot de passe.



5. Lorsque vous avez terminé d'ajouter des exigences, sélectionnez **Enregistrer**.
6. Sélectionnez à nouveau **Enregistrer** pour enregistrer toutes les modifications apportées aux paramètres.

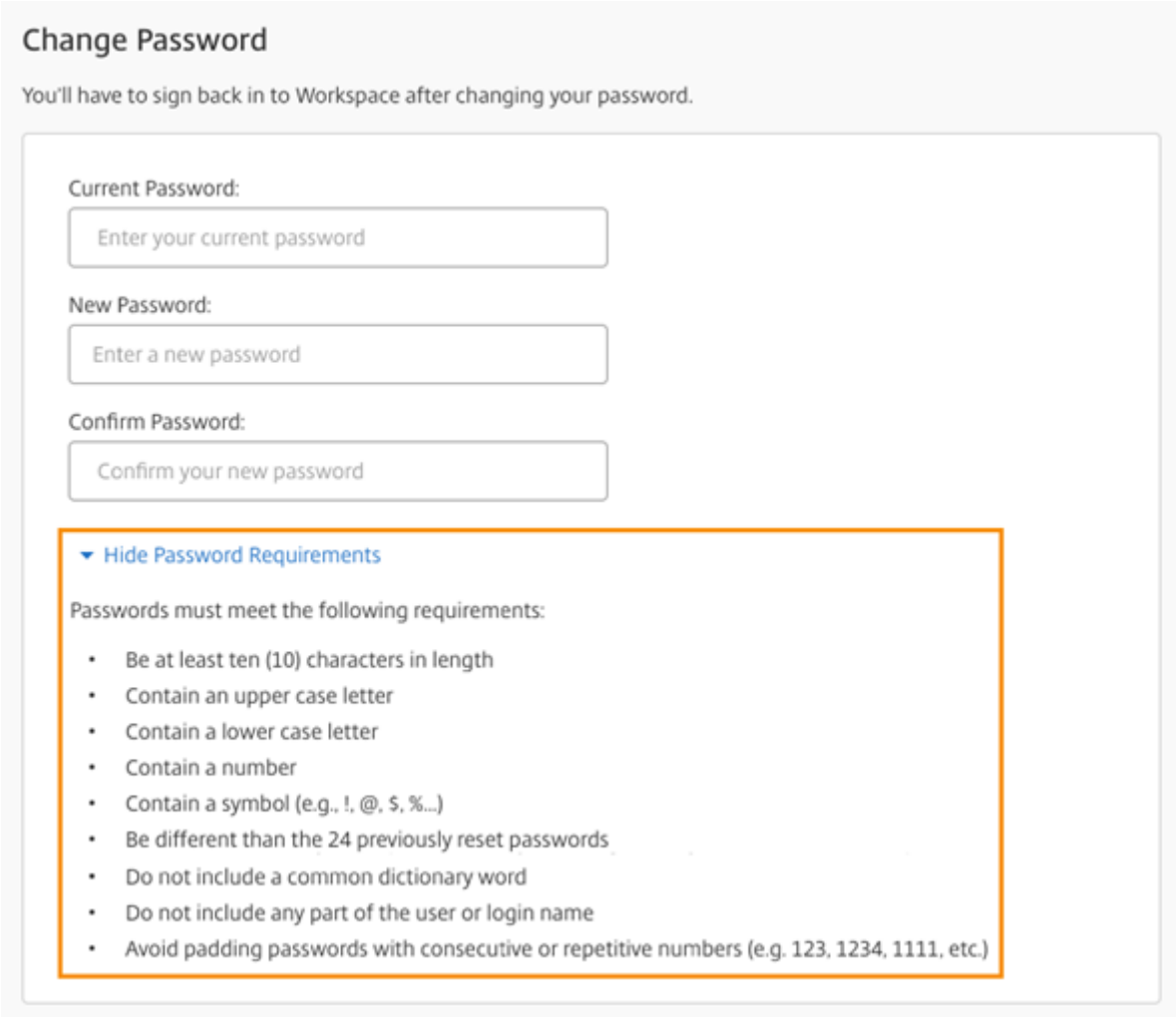


Expérience de l'abonné lors de la modification des mots de passe

> **Conseil :**
>
> Pour mieux faire connaître cette fonctionnalité auprès de vos abonnés, envisagez d'inclure une recommandation dans votre base de connaissances interne pour que les abonnés changent leurs mots de passe de domaine via Workspace. Téléchargez ce fichier PDF pour obtenir des instructions que vous pouvez inclure dans vos propres articles de communication et de base de connaissances.

Lorsque l'option **Autoriser la modification du mot de passe du compte** est activée, les abonnés peuvent modifier leur mot de passe dans Workspace en accédant à **Paramètres du compte > Sécurité et connexion**.

Sélectionnez **Afficher les exigences de mot de passe** pour afficher toutes les exigences saisies dans **Configuration de l'espace de travail**.



Après avoir modifié leur mot de passe, les abonnés sont automatiquement déconnectés de Workspace et doivent se connecter à nouveau avec leur nouveau mot de passe.

Envoyer des annonces personnalisées

Envoyez une annonce personnalisée pour afficher un message à durée limitée de votre choix, tel qu'une fenêtre de maintenance à venir.

L'annonce personnalisée est affichée pour tous les abonnés dans tous les clients, y compris les appareils Web et mobiles. Les abonnés voient le message après s'être connectés. Les abonnés ne peuvent pas ignorer ce message, mais ils peuvent le réduire sur leur appareil mobile.

1. Dans le menu **Citrix Cloud**, sélectionnez **Configuration de l'espace de travail > Personnaliser > Préférences > Envoyer annonce personnalisée > Configurer**.
2. Entrez le titre et le texte du message que vous souhaitez afficher, puis sélectionnez les dates, les heures et l'emplacement (haut ou bas) d'affichage du message aux abonnés.

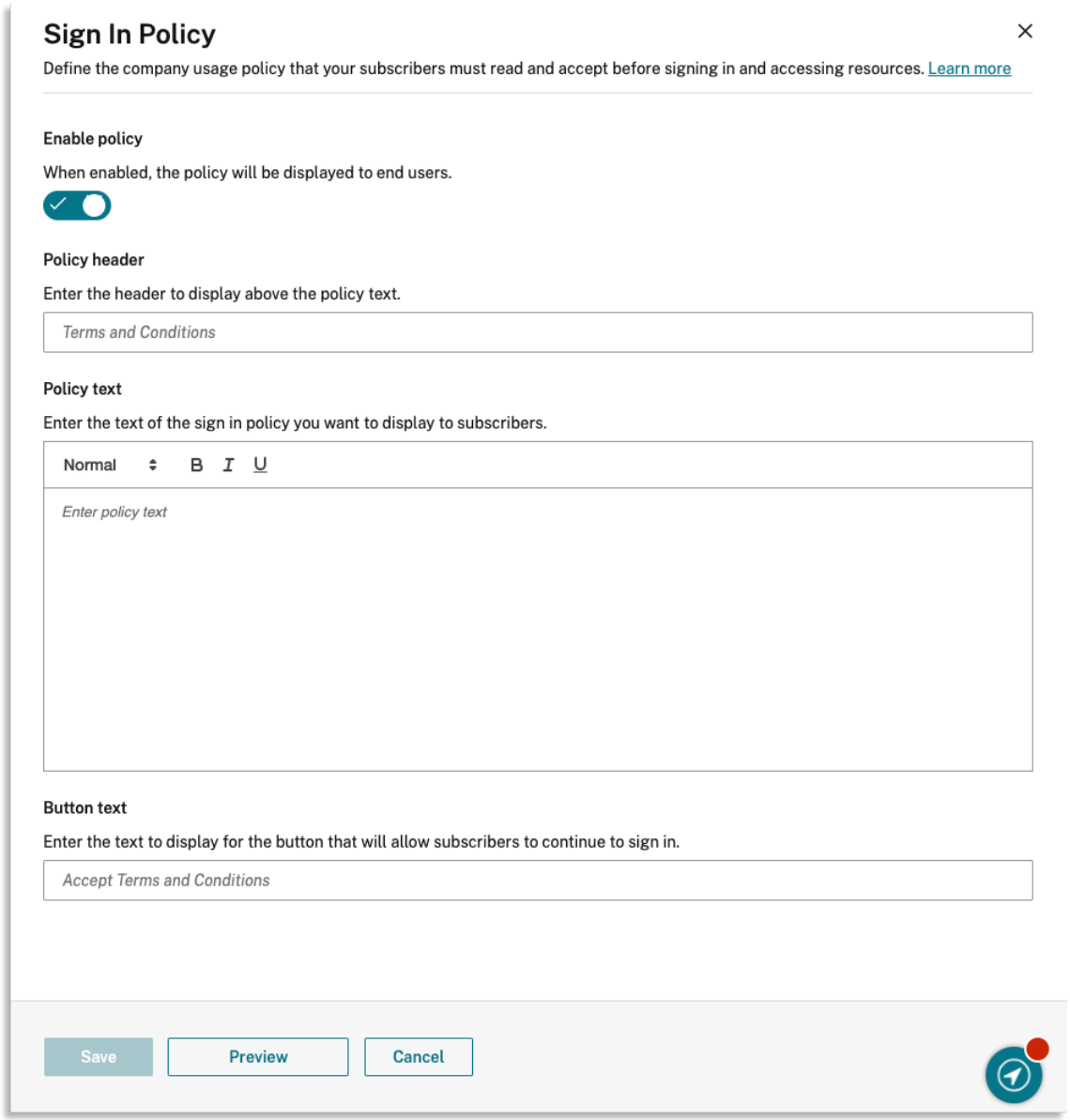
3. Pour voir comment votre message apparaîtra aux abonnés, sélectionnez **Aperçu**.
4. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Configurer une stratégie de connexion

Créez une stratégie de connexion personnalisée pour informer les abonnés du contrat de licence d'utilisateur final (CLUF) de votre organisation lorsqu'ils se connectent à leur espace de travail.

Lorsqu'elle est activée et configurée, la stratégie de connexion s'affiche dans tous les clients, y compris sur le Web et les appareils mobiles. Les abonnés peuvent consulter la stratégie de connexion lorsqu'ils se connectent. Les abonnés ne peuvent pas contourner la stratégie et doivent l'accepter pour se connecter à leur espace de travail.

1. Dans le menu **Citrix Cloud**, sélectionnez **Configuration de l'espace de travail > Personnaliser > Préférences**.
2. Dans la section **Stratégie de connexion**, sélectionnez **Configurer**. Si une stratégie existe, le bouton indique **Modifier**.
3. Activez la fonctionnalité à l'aide de l'option **Activer la stratégie**.
4. Dans **En-tête de la stratégie**, saisissez un titre pour la stratégie.
5. Entrez le texte de stratégie que les abonnés doivent accepter avant de se connecter. Si nécessaire, ajoutez du texte traduit pour d'autres langues dans la même zone de texte.
6. Entrez le nom du bouton que les abonnés doivent sélectionner pour accepter la stratégie.



7. Sélectionnez **Aperçu** pour voir à quoi ressemblera la stratégie pour les abonnés.
8. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

> **Remarque**
>
> Si Citrix Gateway est configuré en tant que fournisseur d'identité Workspace, vous disposez peut-être déjà d'une stratégie de connexion dans le cadre de votre flux d'authentification multifacteur (nFactor). Citrix recommande de configurer une seule stratégie de connexion, soit dans le cadre de votre flux d'authentification nFactor existant, soit en dehors du flux à l'aide de la console d'administration Citrix Cloud.

Optimiser DaaS dans Citrix Workspace

October 12, 2023

Vous pouvez améliorer l'efficacité et la disponibilité de vos applications et bureaux DaaS grâce aux options suivantes :

- Mettre votre déploiement d'applications et de bureaux virtuels locaux existant à la disposition des abonnés Workspace grâce à l'agrégation de sites
- Optimiser la connectivité avec Direct Workload Connection, qui implique la configuration des emplacements réseau dans Citrix Cloud
- Assurer la continuité du service pendant une panne pour une résilience hors ligne.
- Configurer l'authentification unique (SSO) à DaaS avec le service d'authentification fédérée Citrix (FAS).

Agrégation de sites

L'agrégation de sites vous permet d'ajouter votre déploiement d'applications et de bureaux virtuels local à votre espace de travail afin que les abonnés puissent accéder à ces ressources en même temps que les ressources gérées dans le cloud.

Pour plus d'informations sur l'agrégation de sites, consultez l'article Agréger les applications et les bureaux virtuels locaux dans des espaces de travail.

Pour plus d'informations sur les limites de scalabilité, consultez la section Limites de scalabilité de la plate-forme Workspace.

Direct Workload Connection

La fonction Direct Workload Connection utilise les emplacements réseau pour basculer entre les itinéraires internes et externes vers les machines virtuelles qui hébergent vos applications et bureaux virtuels.

Avec Direct Workload Connection, vous autorisez les clients de votre réseau d'entreprise à passer aux lancements directs de Citrix DaaS. Les lancements directs ne nécessitent pas que les connexions HDX entre les clients et les VDA soient transmises par proxy via une passerelle. Direct Workload Connection nécessite au moins un emplacement réseau interne.

Pour plus d'informations, consultez Optimiser la connectivité avec Direct Workload Connection.

Continuité du service

La continuité du service garantit que les abonnés conservent l'accès aux applications et aux bureaux critiques via l'application Citrix Workspace en cas de panne de Citrix Cloud.

La continuité du service stocke les locations de connexion sur les disques clients sur lesquels l'application Citrix Workspace est installée. Les locations de connexion sont actualisées régulièrement lorsque les clients accèdent au magasin Workspace. Les clients peuvent ensuite lancer les instances Citrix DaaS auxquelles ils pouvaient accéder avant la panne. Pour plus d'informations, consultez Continuité du service.

Service d'authentification fédérée (FAS) de Citrix

Citrix Workspace prend en charge l'utilisation du Service d'authentification fédérée Citrix (FAS) pour fournir l'authentification unique (SSO) à DaaS. FAS permet aux abonnés qui utilisent un fournisseur d'identité fédéré, tel qu'Azure AD ou Okta, de saisir leurs informations d'identification une seule fois, lorsqu'ils se connectent à leurs espaces de travail. Sans FAS, les abonnés utilisant un fournisseur d'identité fédéré sont invités à entrer leurs informations d'identification plusieurs fois pour accéder à leurs applications et bureaux virtuels.

L'utilisation de FAS avec Workspace présente les conditions suivantes :

- Un serveur FAS configuré comme décrit dans la section Exigences de la documentation du produit FAS.
- Une connexion entre votre serveur FAS et Citrix Cloud, créée via l'option **Connect to Citrix Cloud** dans le programme d'installation FAS.
- Une connexion entre votre domaine Active Directory local et Citrix Cloud, avec FAS activé dans **Configuration de l'espace de travail**.

Pour plus d'informations sur l'implémentation de FAS, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Agréger les applications et les bureaux virtuels locaux dans des espaces de travail

November 28, 2023

Vous pouvez ajouter votre site (déploiement Virtual Apps and Desktops) à Citrix Workspace pour mettre vos applications et bureaux existants à la disposition des abonnés. Une fois votre site ajouté, les

abonnés peuvent accéder à toutes leurs applications et bureaux virtuels, ainsi qu'à leurs fichiers et autres ressources, lorsqu'ils se connectent à leur espace de travail. Ce processus est appelé *Agrégation de sites*.

L'agrégation de sites est disponible dans toutes les éditions de Citrix Workspace. Pour plus d'informations sur les fonctionnalités incluses dans chaque édition Workspace, consultez le tableau des fonctionnalités de Citrix Workspace.

Environnements pris en charge

L'agrégation de sites est prise en charge sur les déploiements sur site des produits Citrix suivants :

- Virtual Apps and Desktops 7 1808 ou version ultérieure
- XenApp et XenDesktop 7.0 à 7.18

Les sites locaux exécutant des versions antérieures de XenApp ou XenApp et XenDesktop ne sont pas pris en charge avec Citrix Workspace.

> **Important :**
>
> XenApp et XenDesktop 7.x inclut des versions en fin de vie. Les versions XenApp et XenDesktop antérieures à la version 7.14 ont atteint la fin de vie le 30 juin 2018. La prise en charge de l'agrégation de sites avec des versions en fin de vie de XenApp et XenDesktop 7.x dépend de l'énumération et du lancement réussis de ressources avec votre déploiement StoreFront.

Pour utiliser l'agrégation de sites avec un déploiement local qui inclut le Service d'authentification fédérée de Citrix (FAS), votre site doit utiliser l'une des versions de produit Citrix suivantes :

- Virtual Apps and Desktops 7 1808 ou version ultérieure
- XenApp et XenDesktop 7.16 jusqu'à 7.18

La connexion à Citrix Cloud est requise pour utiliser FAS avec Citrix Workspace. Mettez à jour vos serveurs FAS vers la dernière version du logiciel FAS afin de pouvoir vous connecter à Citrix Cloud. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Limites de scalabilité de la plate-forme Workspace

Les limites de scalabilité suivantes s'appliquent à la plate-forme Workspace :

Type de limite	Mesures de SLI	Limite de seuil SLO
Limites d'utilisation	Utilisateurs finaux simultanés pour tous les sites Citrix Virtual Apps and Desktops agrégés locaux	500
Limites supplémentaires d'intégration backend/frontend	Nombre de sites Citrix Virtual Apps and Desktops locaux	4

> **Remarque :**
>
> si le nombre de sites d'intégration backend/frontend dépasse quatre, les sites peuvent observer des temps de réponse lents. La continuité du service ou la prise en charge du LHC ne sont pas non plus présentes pour les sites locaux.

Vue d'ensemble des tâches

Lorsque vous ajoutez votre site local à Citrix Workspace, l'assistant **Ajouter un site** vous guide à travers les tâches suivantes :

1. Découverte de votre site et sélection de l'emplacement de ressources que vous souhaitez utiliser
2. Détection des domaines Active Directory sur lesquels vos Cloud Connector sont installés
3. Spécification de la connectivité à utiliser entre Citrix Cloud et votre site

L'emplacement de ressources spécifie le domaine et la méthode de connectivité pour tous les utilisateurs qui accèdent à votre site. Au cours de ce processus, Citrix Cloud teste la connectivité pour vérifier que votre site est accessible depuis les Cloud Connector. Citrix Cloud affiche ensuite une liste de vos emplacements de ressources. Si vous disposez d'emplacements de ressources sans Cloud Connector, téléchargez et installez le logiciel requis.

Pour une connectivité externe, vous pouvez utiliser votre propre Citrix Gateway ou Citrix Gateway Service. Pour vous assurer que seuls les utilisateurs sur le même réseau que votre site peuvent accéder aux applications, vous pouvez spécifier un accès uniquement en interne.

Conditions préalables

Cloud Connector

Les Cloud Connector permettent à Citrix Cloud de localiser et de communiquer avec votre site. Pour une interruption minimale, Citrix recommande d'installer les Cloud Connector avant d'ajouter votre site à Citrix Workspace.

Pour une haute disponibilité, Citrix recommande de disposer au moins de deux (2) serveurs sur lesquels installer le logiciel Citrix Cloud Connector. Ces serveurs doivent remplir les critères suivants :

- Répondre aux exigences système décrites dans Détails techniques sur Cloud Connector.
- N'avoir aucun autre composant Citrix installé.
- Ne pas être un contrôleur de domaine Active Directory.
- Ne pas être une machine essentielle à votre infrastructure d'emplacement de ressources.
- Être joints au domaine de votre site. Si les utilisateurs accèdent aux applications de votre site dans plusieurs domaines, installez au moins deux Cloud Connector dans chaque domaine.
- Être connectés à un réseau pouvant contacter votre site.
- Être connectés à Internet. Pour plus d'informations, consultez la section Configuration requise pour le système et la connectivité.

Pour plus d'informations sur l'installation des composants Cloud Connector, consultez la section Installation de Cloud Connector.

Configuration du proxy Web

Si vous avez un proxy Web dans votre environnement, assurez-vous que les Cloud Connector peuvent valider la connectivité au service XML dans votre site. Ajoutez chaque serveur XML du site à la liste de contournement proxy sur chaque Cloud Connector. N'utilisez pas de caractères génériques ou d'adresses IP ; le Cloud Connector prend uniquement en charge la gestion des noms de domaine complets.

1. Ajoutez les serveurs XML à la liste de contournement proxy :
    a) Sur le Cloud Connector, sélectionnez **Start**, puis tapez **Internet Options**.
    b) Sélectionnez l'onglet **Connections**, puis **LAN Settings**.
    c) Sous **Proxy server**, sélectionnez **Advanced**.
    d) Sous **Exceptions**, ajoutez le nom de domaine complet de chaque serveur XML dans votre site à l'aide de lettres minuscules. Si ces entrées utilisent des majuscules ou des majuscules, l'agrégation du site peut échouer. Pour plus d'informations, veuillez consulter CTX272160 dans le Centre de connaissances Citrix.
2. Importez la liste afin que les services Cloud Connector puissent les consommer. À l'invite de commandes, tapez `netsh winhttp import proxy source=ie`.
3. À partir de la console **Services**, redémarrez tous les services Citrix Cloud sur chaque machine hébergeant le Cloud Connector.

Active Directory

L'agrégation de sites prend en charge les sites qui utilisent un répertoire Active Directory local.

Configuration de Azure Active Directory Pour ajouter des sites utilisant Azure Active Directory à Citrix Workspace, configurez votre site pour faire confiance aux demandes de service XML. Pour des instructions détaillées, consultez les articles suivants :

Pour XenApp et XenDesktop 7.x et Virtual Apps and Desktops 7 1808, consultez l'article CTX236929.

> **Important :**
>
> Si vous utilisez Azure Active Directory, Okta, SAML ou un autre fournisseur d'identité fédérée avec des espaces de travail et une agrégation de sites, les utilisateurs sont invités à s'authentifier auprès de chaque application qu'ils lancent.
>
> FAS fournit une expérience d'authentification unique (SSO) pour le lancement de ressources à l'aide de l'authentification fédérée. Pour activer l'authentification unique (SSO) pour les abonnés, inscrivez un ou plusieurs serveurs FAS avec le même emplacement de ressources que celui que vous avez configuré pour ajouter votre site.

Approbations Active Directory Si vous disposez de forêts d'utilisateurs et de ressources distinctes dans Active Directory, des Cloud Connector doivent être installés dans chaque forêt avant d'ajouter votre site local. Citrix Cloud détecte ces forêts au cours du processus de détection du site via les Cloud Connector. Vous pouvez ensuite utiliser les utilisateurs et les ressources des forêts pour créer des espaces de travail pour vos utilisateurs.

Limitations :

Lorsque vous ajoutez votre site, vous ne pouvez pas utiliser des forêts d'utilisateurs et de ressources distinctes lorsque vous définissez l'emplacement des ressources. Étant donné que les Cloud Connector ne participent pas aux approbations inter-forêts qui pourraient être établies, Citrix Cloud ne peut pas détecter votre site via les Cloud Connector dans ces forêts. Vous pouvez utiliser ces forêts lorsque vous définissez un emplacement de ressources secondaire afin d'offrir une option de connectivité différente à vos utilisateurs. Pour de plus amples informations, consultez Ajouter des plages d'adresses IP pour différentes options de connectivité.

Les forêts non approuvées ne sont pas prises en charge pour l'agrégation de sites. Bien que Citrix Cloud et Citrix Workspace prennent en charge les utilisateurs issus de forêts non approuvées, ces utilisateurs ne peuvent pas utiliser Citrix Workspace après l'ajout d'un site local via l'agrégation de sites. Seuls les utilisateurs situés dans des forêts approuvées par le site peuvent se connecter et utiliser Citrix Workspace. Si les utilisateurs d'une forêt non approuvée tentent de se connecter à Citrix Workspace, ils reçoivent le message d'erreur « Votre ouverture de session a expiré. Rouvrez une session pour continuer. »

Connectivité interne et externe aux ressources d'un espace de travail

Au cours du processus d'ajout de votre site à Citrix Workspace, vous pouvez spécifier si vous souhaitez fournir un accès interne ou externe aux ressources que vous mettez à la disposition des utilisateurs via Workspace. Si vous avez l'intention d'autoriser uniquement les utilisateurs internes à accéder à votre site via Citrix Workspace, les utilisateurs doivent être sur le même réseau que le site pour accéder à leurs applications.

Si vous avez l'intention d'autoriser des utilisateurs externes à accéder à ces ressources, vous disposez des options suivantes :

- Utiliser votre instance Citrix Gateway existante pour gérer le trafic entre votre site local et Citrix Cloud. Votre instance Citrix Gateway doit être configurée pour utiliser des Cloud Connector en tant que serveurs STA (Secure Ticket Authority) **avant** d'ajouter votre site à Citrix Workspace. Pour obtenir des instructions, veuillez consulter l'article CTX232640.
- Utiliser Citrix Gateway Service si vous préférez autoriser Citrix à gérer le trafic entre votre site et Citrix Cloud. Vous pouvez activer une évaluation du service et configurer le service lorsque vous ajoutez votre site. Si vous êtes déjà inscrit à Citrix Gateway Service, Citrix Cloud détecte votre abonnement lorsque vous sélectionnez cette option.

> **Remarque :**
>
> Pour que Citrix Cloud détecte votre abonnement à Citrix Gateway Service, vous devez utiliser le même OrgID que celui que vous avez utilisé lors de votre inscription à Citrix Gateway Service. Pour plus d'informations sur les OrgID dans Citrix Cloud, consultez la section [Qu'est-ce qu'un OrgID ?](/en-us/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html#what-is-an-orgid)

Informations d'identification et ports pour la détection du site

Au cours du processus d'ajout de votre site à Citrix Workspace, Citrix Cloud détecte votre site et s'assure que le Controller que vous spécifiez est disponible. Avant d'ajouter votre site local, vérifiez les éléments suivants :

- Vous disposez d'informations d'identification d'administrateur Citrix avec au minimum des autorisations **Lecture seule**. Au cours du processus de détection de sites, Citrix Cloud vous invite à fournir ces informations d'identification. Citrix Cloud ne stocke pas ces informations d'identification et ne les utilise pas pour apporter des modifications à votre site.

Pour activer la détection de site sans les informations d'identification de site XenApp et XenDesktop 7.x et Virtual Apps and Desktops 7 1808 uniquement : si vous ne souhaitez pas fournir les informations d'identification de votre site pour des raisons de sécurité, vous pouvez autoriser Citrix

Cloud à détecter votre site sans demander les informations d'identification du site. Effectuez cette tâche **avant** d'ajouter votre site à Citrix Workspace.

1. Installez au moins deux Cloud Connector dans le domaine de votre site.
2. Créez un groupe de sécurité Active Directory et ajoutez-y les Cloud Connector de votre domaine.
3. Redémarrez les Cloud Connector.
4. Dans Studio, accordez au minimum les autorisations **Lecture seule** au groupe de sécurité.

Tâche 1 : Détecter votre site

Dans cette étape, vous fournissez les informations dont Citrix Cloud a besoin pour localiser votre site et vous sélectionnez votre emplacement de ressources. L'emplacement de ressources spécifie le domaine et la connectivité pour tous les utilisateurs qui accèdent à votre site. Si vous devez installer des Cloud Connector dans le domaine de votre site, vous pouvez le faire maintenant. Si vous avez déjà installé des Cloud Connector, vous pouvez les sélectionner lorsque vous y êtes invité.

1. Dans le menu Citrix Cloud, accédez à **Configuration de l'espace de travail > Sites > Ajouter un site**.
2. Sélectionnez le type de site local que vous souhaitez ajouter et continuez.

   Citrix Cloud tente de détecter tous les emplacements de ressources et les Cloud Connector de votre domaine et affiche une liste parmi laquelle vous pouvez sélectionner.
3. Effectuez l'une des actions suivantes :

   - Si vous n'avez installé aucun Cloud Connector dans le domaine de votre site, cliquez sur **Installer connecteur**. Citrix Cloud vous invite à télécharger le logiciel Cloud Connector et à compléter l'assistant d'installation.
   - Si vous avez installé des Cloud Connector, Citrix Cloud affiche les connecteurs dans les domaines dans lesquels ils ont été détectés. Sélectionnez l'emplacement de ressources que vous souhaitez ajouter à Citrix Workspace. Cet emplacement de ressources devient l'emplacement de ressources par défaut.
   - Si vous avez installé des Cloud Connector mais qu'ils ne sont pas affichés, sélectionnez **Détecter**.
4. Sélectionnez l'emplacement des ressources et le Cloud Connector que vous souhaitez utiliser pour détecter votre site.
5. Dans **Entrez l'adresse du serveur**, ajoutez l'adresse IP ou le nom de domaine complet d'un Controller dans le site, puis sélectionnez **Découvrir**.

> **Remarque :**
>
> Si vous utilisez un nom de domaine complet, vous devez disposer d'un enregistrement DNS qui pointe vers le Delivery Controller que vous souhaitez détecter.
>
> Pour les sites XenApp et XenDesktop 7.x, Citrix Cloud détecte automatiquement le port du serveur XML.

6. Si vous y êtes invité, entrez les informations d'identification de l'administrateur Citrix pour le site.

   Citrix Cloud effectue un test de connectivité pour vérifier que votre site est accessible. La détection peut prendre quelques minutes, selon le type et la taille du site.

7. Si un message de réussite s'affiche indiquant que le site a été détecté, sélectionnez **Continuer**.

Tâche 2 : Vérifier la connexion Active Directory

Dans **Vérifier la connexion Active Directory**, Citrix Cloud affiche les domaines utilisés avec votre site et indique si des Cloud Connector sont installés dans ces domaines.

S'il n'y a pas de Cloud Connector dans un domaine, les utilisateurs dans ce domaine ne peuvent pas utiliser Citrix Workspace pour accéder aux applications publiées dans ce domaine. Si vous n'avez qu'un seul Cloud Connector dans votre domaine, deux options s'offrent à vous :

- Installez d'autres Cloud Connector en sélectionnant **Installer connecteur**.
- Continuez sans installer d'autres Cloud Connector en sélectionnant **Je comprends que la haute disponibilité nécessite l'installation de deux connecteurs dans chaque domaine**.

Si des utilisateurs locaux sont attribués à des applications de votre site, sélectionnez **Télécharger la liste des utilisateurs (.csv)**.

Après avoir vérifié votre connexion Active Directory, sélectionnez **Continuer**.

Tâche 3 : Configurer la connectivité

Au cours de cette étape, vous indiquez si vous souhaitez autoriser uniquement les utilisateurs internes à accéder à votre site via Citrix Workspace ou les utilisateurs externes. La connectivité interne nécessite que vos utilisateurs se trouvent sur le même réseau que votre site et les VDA qui hébergent vos ressources publiées. Pour une connectivité externe, vous pouvez utiliser votre instance Citrix Gateway locale existante ou le service hébergé dans le cloud Citrix Gateway Service.

Sélectionnez l'une des options suivantes dans **Sélectionner le type de connectivité > Configurer la connectivité** :

- **Ajouter Gateway existant :** sélectionnez cette option pour utiliser votre Citrix Gateway existant pour fournir un accès externe.
- **Citrix Gateway Service :** sélectionnez cette option pour activer une évaluation du service ou utiliser votre abonnement existant avec votre site.
- **Interne uniquement :** sélectionnez cette option si aucune autre configuration n'est requise.

Si **Ajouter Gateway existant** est sélectionné, effectuez les actions suivantes :

1. Sélectionnez **Modifier** et saisissez l'URL publique de Citrix Gateway.
2. Vérifiez que Citrix Gateway est configuré pour utiliser vos Cloud Connector en tant que serveurs STA comme décrit dans l'article CTX232640.
3. Sélectionnez **Tester STA**, puis, lorsque le test est réussi, sélectionnez **Continuer**. Si le test échoue, reportez-vous à l'article CTX232517 pour les étapes de dépannage.

Si **Citrix Gateway Service** est sélectionné, mais que le service n'est pas activé pour votre compte Citrix Cloud en tant qu'évaluation ou en tant qu'achat, vous pouvez sélectionner **Commencer une version d'évaluation de 60 jours**. Citrix Cloud active le service en tant que version d'évaluation. Si le service a été activé plus tôt, Citrix Cloud détecte le service et affiche le nombre de jours restants.

Après avoir terminé les tâches précédentes, sélectionnez **Continuer**.

Tâche 4 : Confirmer l'agrégation de sites

Dans cette étape, vous confirmez l'agrégation de sites, c'est-à-dire vous vérifiez le port XML, les serveurs XML, les domaines Active Directory et le type de connectivité que vous avez choisis précédemment.

Citrix Cloud affiche jusqu'à cinq des serveurs XML auxquels il peut se connecter. Si vous avez plusieurs serveurs XML sur votre site mais qu'un seul s'affiche, Citrix Cloud affiche une alerte. Pour résoudre ce problème, reportez-vous à l'article CTX232516.

1. Dans **Confirmer l'agrégation de sites**, vérifiez le port XML, les serveurs XML, les domaines Active Directory et le type de connectivité que vous avez choisis précédemment.
2. Sélectionnez **Enregistrer et terminer**. La page **Sites** affiche le site que vous venez d'ajouter.

Si vous souhaitez spécifier différents serveurs XML, vous pouvez ensuite modifier votre site pour modifier ces valeurs après avoir sélectionné **Enregistrer et terminer**.

Tâche 5 : Gérer les intégrations de services

Après avoir ajouté votre premier site, vous devez activer l'option **Intégrations de services** pour les sites locaux Virtual Apps and Desktops, qui est désactivée par défaut. Les abonnés ne peuvent pas afficher les ressources du site tant que vous n'avez pas activé cette option.

1. Accédez à **Configuration de l'espace de travail > Intégrations de services > Sites Virtual Apps and Desktops locaux** et sélectionnez les points de suspension pour ouvrir le menu des actions du site.
2. Activez l'intégration du service afin que les abonnés puissent se connecter à leurs espaces de travail et consulter les ressources du site.

Modifier la configuration de votre site

Redétecter votre site

Si vous ajoutez des Delivery Controller à votre site ou si vous modifiez les ports XML, vous pouvez initier une nouvelle détection pour vérifier que votre site est toujours accessible dans Citrix Workspace.

1. Accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez mettre à jour, puis sélectionnez **Modifier site**.
2. Dans **Adresse du serveur**, tapez l'adresse IP ou le nom de domaine complet d'un Delivery Controller dans le site et sélectionnez **Redétecter**.

Ajouter ou modifier des serveurs XML

Lorsque vous ajoutez un nouveau site à Citrix Workspace, Citrix Cloud détecte automatiquement les serveurs XML de votre site et affiche jusqu'à cinq serveurs XML dans votre configuration. Vous pouvez ajouter et supprimer des serveurs XML selon les besoins de configuration de site, jusqu'à la limite d'affichage de cinq serveurs XML.

Pour ajouter un serveur XML

1. Accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez mettre à jour, puis sélectionnez **Modifier site**.
2. Dans la section **Serveurs XML**, tapez le port du serveur XML et sélectionnez **Utiliser SSL** si nécessaire.
3. Sélectionnez une méthode de connectivité :
    - **Équilibrage de charge :** cette option permet à Citrix Cloud de sélectionner un serveur XML aléatoire dans la liste.
    - **Basculement :** cette option permet à Citrix Cloud d'utiliser les serveurs XML répertoriés dans l'ordre dans lequel ils apparaissent dans la liste. Seul le premier service XML de la liste est utilisé pour le lancement, sauf s'il devient indisponible, puis le deuxième serveur est utilisé. Vous pouvez réorganiser la liste en faisant glisser et en déposant chaque serveur.

4. Sélectionnez **Enregistrer les modifications**.

Si vous rencontrez une erreur lors de l'ajout d'un serveur XML, reportez-vous à l'article CTX232516 pour les étapes de dépannage.

Ajouter des plages d'adresses IP pour différentes options de connectivité

Si vous avez des VDA ou des hôtes de session dans différents sous-réseaux, vous pouvez spécifier des plages d'adresses IP avec un type de connectivité différent pour chacun. Chaque plage d'adresses IP peut également être associée à un emplacement de ressources différent. Par exemple, vous pouvez avoir une plage d'adresses IP pour les machines situées en Europe où les utilisateurs se connectent en interne, une plage d'adresse IP pour les machines en Europe où les utilisateurs se connectent via votre instance Citrix Gateway et une plage d'adresses IP pour les machines aux États-Unis où les utilisateurs se connectent via le Citrix Gateway Service.

1. Accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez mettre à jour, puis sélectionnez **Modifier site**.
2. Dans la section **Connectivité**, sélectionnez **Ajoutez une plage d'adresses IP avec une option de connectivité différente** et entrez une plage d'adresses IP au format CIDR.

Pour créer un emplacement de ressources pour votre plage d'adresses IP :

1. Sélectionnez **Ajouter un nouvel emplacement de ressources** et entrez un nom convivial.
2. Dans **Sélectionner votre connectivité**, indiquez si vous souhaitez fournir un accès interne uniquement ou autoriser un accès externe à l'aide de votre instance Citrix Gateway ou de Citrix Gateway Service.

Pour attribuer un emplacement de ressources existant à la plage d'adresses IP :

1. Choisissez **Sélectionner un emplacement de ressources existant**.
2. Sélectionnez l'emplacement de ressources que vous souhaitez utiliser.
3. Si vous choisissez un emplacement de ressources avec un seul Cloud Connector installé, sélectionnez **Je comprends que la haute disponibilité nécessite l'installation de deux connecteurs dans un emplacement de ressources**.
4. Sélectionnez **Add**.

Ajouter des domaines Active Directory supplémentaires

Si vous installez des Cloud Connector dans des domaines supplémentaires avec des utilisateurs Active Directory sur votre site, vous pouvez vous assurer qu'ils sont ajoutés à la configuration de votre site dans Citrix Workspace.

1. Accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez mettre à jour, puis sélectionnez **Modifier site**.
2. Sous Active Directory, sélectionnez **Actualiser**.

Désactiver les sites

Si vous ne souhaitez plus rendre votre site local disponible aux utilisateurs dans Citrix Workspace, vous pouvez le désactiver. Vous pouvez désactiver un site local individuel ou tous les sites locaux que vous avez ajoutés à Citrix Workspace.

Lorsque les sites sont désactivés, les utilisateurs ne peuvent pas accéder aux applications locales de ces sites via Citrix Workspace. Toutefois, la configuration de ces sites est préservée. Lorsque vous réactivez un site ultérieurement, les paramètres par défaut d'emplacement, de domaine, de serveur XML et de connectivité du site sont conservés.

Pour désactiver un site local

1. Accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez désactiver, puis sélectionnez **Désactiver**.
2. Un message de confirmation s'affiche. Sélectionnez à nouveau **Désactiver**.

Pour désactiver tous les sites locaux

Pour désactiver tous les sites sur la page **Sites**, vous devez désactiver l'intégration de service de l'espace de travail pour tous les sites Virtual Apps and Desktops locaux. Pour obtenir des instructions, consultez Désactiver l'intégration de l'espace de travail pour un service.

Pour réactiver un site local ou pour ajouter un autre site ultérieurement, vous devez d'abord réactiver l'intégration de l'espace de travail pour tous les sites sur la page **Intégrations de services**.

Supprimer un site de Citrix Workspace

Si vous n'avez plus besoin de la configuration de votre site local dans Citrix Workspace, vous pouvez supprimer le site. Lorsque vous supprimez un site, seule la configuration du site dans Citrix Workspace est supprimée. Citrix Cloud ne modifie pas votre site.

Pour supprimer un site, accédez à **Configuration de l'espace de travail > Sites**, sélectionnez les points de suspension en regard du site que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

Optimiser la connectivité aux espaces de travail avec Direct Workload Connection

November 28, 2023

Avec la fonction Direct Workload Connection de Citrix Cloud, vous pouvez optimiser le trafic interne vers les applications et les bureaux des espaces de travail des abonnés afin de rendre les sessions HDX plus rapides. Normalement, les utilisateurs des réseaux internes et externes se connectent à des VDA via une passerelle externe. Cette passerelle peut se trouver localement dans votre organisation ou fournie en tant que service par Citrix et ajoutée à l'emplacement des ressources dans Citrix Cloud. Direct Workload Connection permet aux utilisateurs internes de contourner la passerelle et de se connecter directement aux VDA, réduisant ainsi la latence du trafic réseau interne.

Pour configurer Direct Workload Connection, vous avez besoin d'emplacements réseau correspondant à l'endroit où les clients lancent des applications et des bureaux dans votre environnement. Ajoutez une adresse publique pour chaque adresse de bureau où résident ces clients à l'aide du service de localisation réseau (NLS). Vous disposez de deux options pour configurer les emplacements réseau :

- Utilisation de l'option de menu **Emplacements réseau** dans Citrix Cloud
- Utilisation d'un module PowerShell fourni par Citrix

Les emplacements réseau correspondent aux plages IP publiques des réseaux depuis lesquels vos utilisateurs internes se connectent, tels que les emplacements de votre bureau ou de votre succursale. Citrix Cloud utilise des adresses IP publiques pour déterminer si les réseaux à partir desquels des applications ou des bureaux virtuels sont lancés sont internes ou externes au réseau de l'entreprise. Si un abonné se connecte à partir du réseau interne, Citrix Cloud achemine la connexion directement vers le VDA, en contournant NetScaler Gateway. Si un abonné se connecte en externe, Citrix Cloud achemine l'abonné via NetScaler Gateway, puis dirige le trafic de session via Citrix Cloud Connector vers le VDA dans le réseau interne. Si Citrix Gateway Service est utilisé et que le protocole Rendezvous est activé, Citrix Cloud achemine les utilisateurs externes via Gateway Service vers le VDA du réseau interne. Les clients itinérants tels que les ordinateurs portables peuvent utiliser l'une ou l'autre de ces itinéraires réseau, selon que le client se trouve à l'intérieur ou à l'extérieur du réseau de l'entreprise au moment du lancement.

> **Important :**
>
> Si votre environnement inclut Citrix DaaS Standard pour Azure avec des VDA locaux, la configuration de Direct Workload Connection entraîne l'échec des lancements à partir du réseau interne.

Les lancements de ressources Remote Browser Isolation, Citrix Virtual Apps Essentials et Citrix Virtual Desktops Essentials sont toujours acheminés via la passerelle. Ces lancements ne permettent pas d'

améliorer les performances de la configuration de Direct Workload Connection.

Exigences

Configuration réseau requise

- Le réseau d'entreprise et les réseaux Wi-Fi invités doivent comporter des adresses IP publiques distinctes. Si vos réseaux d'entreprise et d'invité utilisent les mêmes adresses IP publiques, les utilisateurs du réseau invité ne peuvent pas lancer les sessions DaaS.
- Utilisez les plages d'adresses IP publiques des réseaux à partir desquels vos utilisateurs internes se connectent. Les utilisateurs internes de ces réseaux doivent disposer d'une connexion directe aux VDA. Si ce n'est pas le cas, les lancements de ressources virtuelles échouent car Workspace tente d'acheminer les utilisateurs internes directement vers les VDA, ce qui n'est pas possible.
- Bien que les VDA soient généralement situés au sein de votre réseau local, vous pouvez également utiliser des VDA hébergés dans un cloud public tel que Microsoft Azure. Les lancements de clients doivent disposer d'un itinéraire réseau pour contacter les VDA sans être bloqués par un pare-feu. Cela nécessite un tunnel VPN entre votre réseau local et un réseau virtuel sur lequel résident les VDA.

Exigences TLS

TLS 1.2 doit être activé dans PowerShell lors de la configuration de vos emplacements réseau. Pour forcer PowerShell à utiliser TLS 1.2, utilisez la commande suivante avant d'utiliser le module PowerShell :

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
]::Tls12
```

Exigences relatives à l'espace de travail

- Vous avez un espace de travail configuré dans Citrix Cloud.
- Citrix DaaS est activé dans **Configuration de l'espace de travail > Intégrations de services**.

Activer TLS pour l'application Workspace pour les connexions HTML5

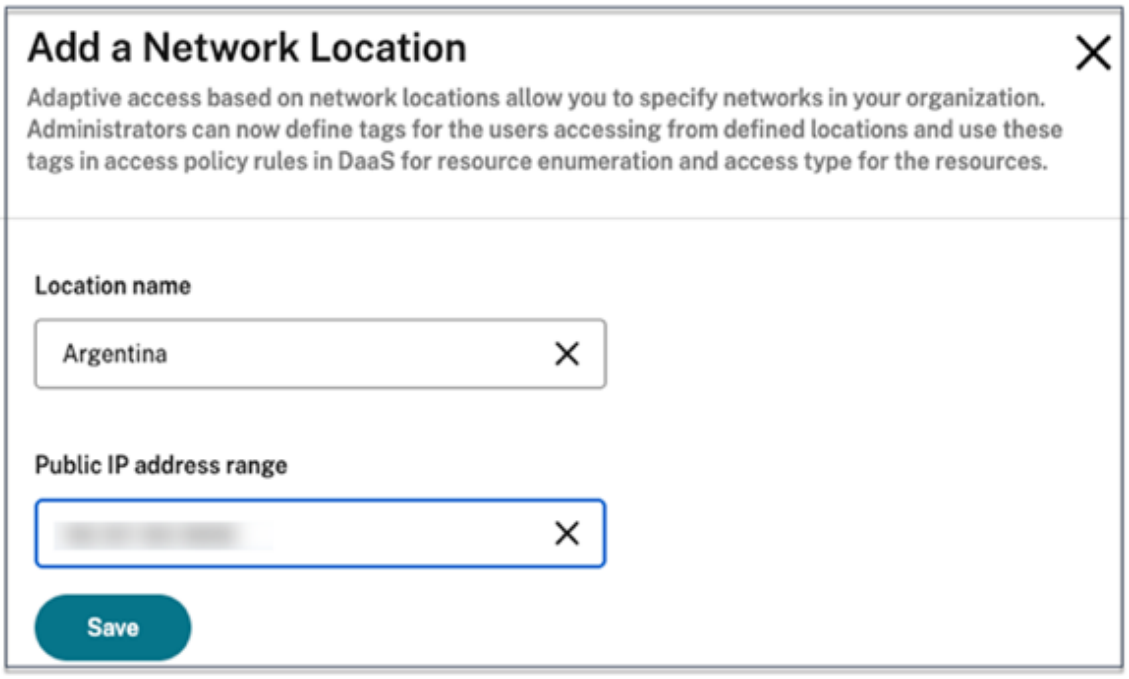
Si vos abonnés utilisent l'application Citrix Workspace pour HTML5 pour lancer des applications et des bureaux, Citrix recommande de configurer TLS sur les VDA de votre réseau interne. La configuration de vos VDA pour utiliser des connexions TLS garantit la possibilité de pouvoir lancer directement

des applications et bureaux depuis des VDA. Si TLS n'est pas activé sur les VDA, les lancements d'applications et de bureaux doivent être acheminés via une passerelle lorsque les abonnés utilisent l'application Citrix Workspace pour HTML5. Les lancements à l'aide de Desktop Viewer ne sont pas affectés. Pour plus d'informations sur la sécurisation des connexions VDA directes avec TLS, consultez l'article CTX134123 dans le Centre de connaissances Citrix.

Ajouter des emplacements réseau via l'interface graphique

La configuration Direct Workload Connection via Citrix Cloud implique la création d'emplacements réseau à l'aide des plages d'adresses IP publiques de chaque emplacement de succursale à partir de laquelle vos utilisateurs internes se connectent.

1. Dans la console Citrix Cloud, accédez à **Emplacements réseau**.
2. Cliquez sur **Ajouter un emplacement réseau**.
3. Entrez un nom d'emplacement réseau et une plage d'adresses IP publiques pour l'emplacement.



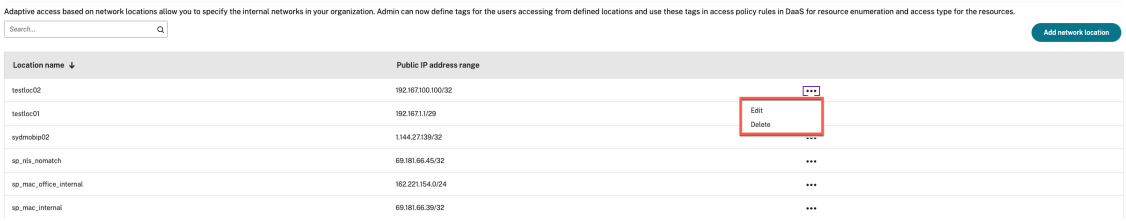
4. Cliquez sur **Save**.
5. Répétez ces étapes pour chaque nouvel emplacement réseau que vous souhaitez ajouter.

> **Remarque :**
>
> Les balises d'emplacement ne sont pas requises pour Direct Workload Connection car le type de connectivité est toujours **interne**. Le champ **Balises d'emplacement** de la page **Ajouter un em-**

> **placement réseau** (**Citrix Cloud > Emplacements réseau > Ajouter un emplacement réseau > Balises d'emplacement**) n'est visible que si la fonctionnalité Accès adaptatif est activée. Pour plus de détails, voir Activer la fonctionnalité Accès adaptatif.

Modifier ou supprimer des emplacements réseau

1. Dans la console Citrix Cloud, accédez à **Emplacements réseau** dans le menu principal.
2. Localisez l'emplacement réseau que vous souhaitez gérer et cliquez sur le bouton représentant des points de suspension.



3. Sélectionnez l'une des commandes suivantes :
   - Sélectionnez **Modifier** pour modifier l'emplacement réseau. Après avoir apporté des modifications, cliquez sur **Enregistrer**.
   - Sélectionnez **Supprimer** pour supprimer l'emplacement réseau. Sélectionnez **Oui, supprimer** pour confirmer la suppression. Vous ne pouvez pas annuler cette opération.

Ajouter et modifier des emplacements réseau avec PowerShell

Au lieu d'utiliser l'interface de la console de gestion Citrix Cloud, vous pouvez utiliser un script PowerShell pour configurer Direct Workload Connection. La configuration de Direct Workload Connection avec PowerShell implique les tâches suivantes :

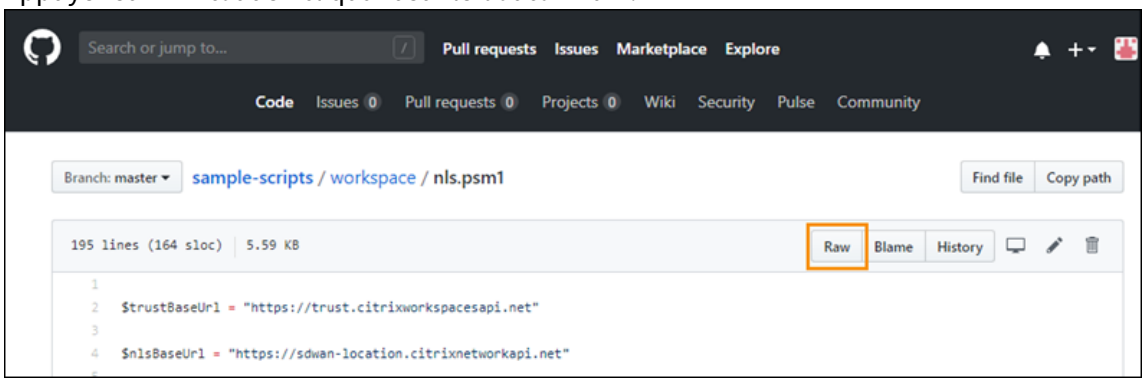
1. Déterminez les plages d'adresses IP publiques de chaque emplacement de succursale à partir de laquelle vos utilisateurs internes se connectent.
2. Téléchargez le module PowerShell.
3. Créez un client API sécurisé dans Citrix Cloud et notez l'ID client et le secret.
4. Importez le module PowerShell et connectez-vous au service de localisation réseau avec les détails de votre client API.
5. Créez des sites de service de localisation réseau pour chacun de vos emplacements de succursales avec les plages d'adresses IP publiques que vous avez précédemment déterminées. Direct Workload Connection est automatiquement activé pour tous les lancements provenant des emplacements réseau internes que vous avez spécifiés.

6. Lancez une application ou un bureau à partir d'un appareil de votre réseau interne et vérifiez que la connexion va directement au VDA, en contournant la passerelle. Pour plus d'informations, consultez la section Journalisation des fichiers ICA dans cet article.

Télécharger le module PowerShell

Avant de configurer vos emplacements réseau, téléchargez le module PowerShell fourni par Citrix (nls.psm1) à partir du référentiel Citrix GitHub. À l'aide de ce module, vous pouvez configurer autant d'emplacements réseau que nécessaire pour vos VDA.

1. Dans un navigateur Web, accédez à https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1.
2. Appuyez sur **ALT** tout en cliquant sur le bouton **Raw**.



3. Sélectionnez un emplacement sur votre ordinateur et cliquez sur **Enregistrer**.

Détails de configuration requis

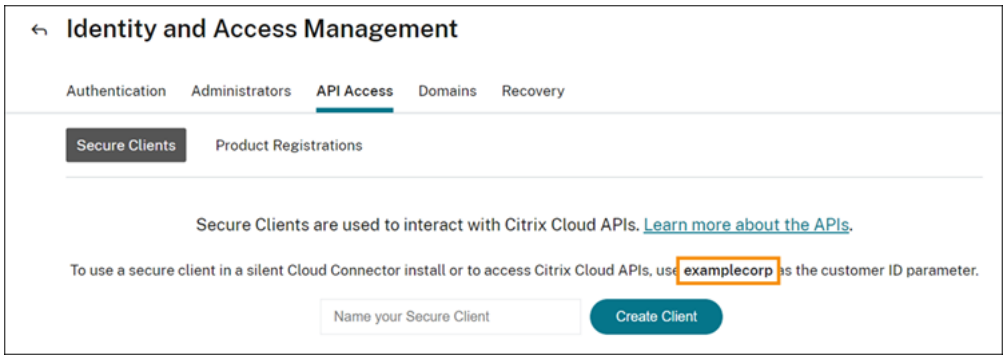
Pour configurer vos emplacements réseau, vous avez besoin des informations suivantes :

- ID client sécurité Citrix Cloud, ID client et secret client. Pour obtenir ces valeurs, consultez la section Créer un client sécurisé dans cet article.
- Plages d'adresses IP publiques des réseaux à partir desquels vos utilisateurs internes se connectent. Pour plus d'informations sur ces plages d'adresses IP publiques, consultez la section Exigences dans cet article.

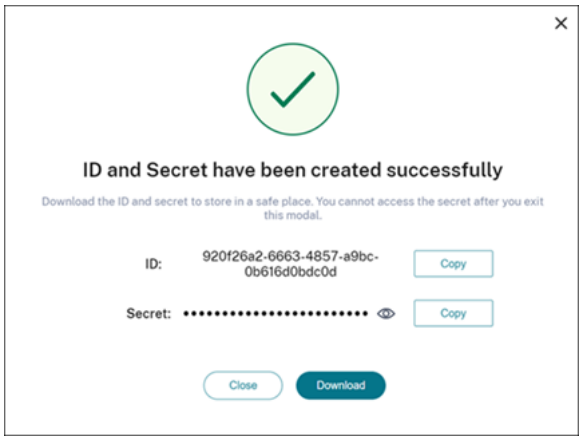
Créer un client sécurisé

1. Connectez-vous à Citrix Cloud sur `https://citrix.cloud.com`.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Accès aux API**.

3. Dans l'onglet **Clients sécurisés**, notez votre ID client.



4. Entrez un nom pour le client, puis sélectionnez **Créer un client**.
5. Copiez l'ID client et le secret client.



Configurer les emplacements réseau

1. Ouvrez une fenêtre de commande PowerShell et accédez au répertoire où vous avez enregistré le module PowerShell.
2. Importez le module : `Import-Module .\nls.psm1 -Force`
3. Définissez les variables requises avec les informations de votre client sécurisé dans Créer un client sécurisé :
   - `$clientId = "YourSecureClientID"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourSecureClientSecret"`
4. Connectez-vous au service de localisation réseau à l'aide de vos informations d'identification de client sécurisé :

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -
    customer $customer
```


5. Créez un emplacement réseau en remplaçant les valeurs des paramètres par les valeurs correspondant au réseau interne à partir duquel vos utilisateurs internes se connectent directement :

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

Pour spécifier une seule adresse IP au lieu d'une plage, ajoutez **/32** à la fin de l'adresse IP. Par exemple :

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

> **Important :**
>
> Lorsque vous utilisez la commande `New-NLSSite`, incluez au moins une valeur pour chaque paramètre. Si vous exécutez cette commande sans argument de ligne de commande, PowerShell vous invite à entrer les valeurs appropriées pour chaque paramètre, une par une. La propriété `internal` est une propriété booléenne obligatoire avec les valeurs possibles `$True` ou `$False` qui correspond à l'interface utilisateur via PowerShell. Par exemple, `(UI)Network Internal -> (PowerShell)-internal=$True`.

Lorsque l'emplacement réseau est créé, la fenêtre de commande affiche les détails de l'emplacement réseau.

6. Répétez l'étape 5 pour tous les emplacements réseau à partir desquels les utilisateurs se connectent.
7. Exécutez la commande `Get-NLSSite` pour renvoyer une liste de tous les sites que vous avez configurés avec le service de localisation réseau et vérifiez que leurs détails sont corrects.

Modifier les emplacements réseau

Pour modifier un emplacement réseau existant, procédez comme suit :

1. Dans une fenêtre de commande PowerShell, listez tous les emplacements réseau existants : `Get-NLSSite`
2. Pour modifier la plage d'adresses IP d'un emplacement réseau spécifique, tapez

```
(Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","
4.3.2.1/32")
```


où [N] est le nombre correspondant à l'emplacement dans la liste (qui commence par un zéro) et "1.2.3.4/32","4.3.2.1/32" sont les plages d'adresses IP séparées par des virgules que vous souhaitez utiliser. Par exemple, pour modifier le premier emplacement répertorié, tapez la commande suivante :

```
(Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32","
141.43.0.0/24")
```

Supprimer des emplacements réseau

Pour supprimer des emplacements réseau que vous ne souhaitez plus utiliser, procédez comme suit :

1. Dans une fenêtre de commande PowerShell, listez tous les emplacements réseau existants : `Get-NLSSite`
2. Pour supprimer tous les emplacements réseau, tapez `Get-NLSSite | Remove-NLSSite`
3. Pour supprimer des emplacements réseau spécifiques, tapez `(Get-NLSSite)[N] | Remove-NLSSite`, où [N] est le numéro correspondant à l'emplacement dans la liste. Par exemple, pour supprimer le premier emplacement répertorié, tapez `(Get-NLSSite)[0] | Remove-NLSSite`.

Vérifier que les lancements internes sont acheminés correctement

Pour vérifier que les lancements internes accèdent directement aux VDA, utilisez l'une des méthodes suivantes :

- Affichez les connexions VDA via la console DaaS.
- Utilisez la journalisation des fichiers ICA pour vérifier l'adresse correcte de la connexion client.

Console Citrix DaaS

Sélectionnez **Gérer > Moniteur**, puis recherchez un utilisateur dont la session est active. Dans la section **Détails de la session** de la console, les connexions VDA directes s'affichent sous forme de connexions UDP tandis que les connexions par passerelle s'affichent sous forme de connexions TCP.

Si UDP n'apparaît pas sur la console DaaS, vous devez activer la stratégie HDX Adaptive Transport pour les VDA.

Journalisation des fichiers ICA

Activez la journalisation des fichiers ICA sur l'ordinateur client comme décrit à la section Pour autoriser la journalisation du fichier launch.ica. Après le lancement des sessions, examinez les entrées **Address** et **SSLProxyHost** dans le fichier journal.

Connexions VDA directes Pour les connexions VDA directes, la propriété **Address** contient l'adresse IP et le port du VDA.

Voici un exemple de fichier ICA lorsqu'un client lance une application à l'aide de NLS :

```
[Notepad++ Cloud]
Address=;10.0.1.54:1494
SSLEnable=Off
<!--NeedCopy-->
```

La propriété **SSLProxyHost** n'est pas présente dans ce fichier. Cette propriété est incluse uniquement pour les lancements via une passerelle.

Connexions de passerelle Pour les connexions de passerelle, la propriété **Address** contient le ticket STA Citrix Cloud, la propriété **SSLEnable** est définie sur **On**et la propriété **SSLProxyHost** contient le nom de domaine complet et le port de la passerelle.

Voici un exemple de fichier ICA lorsqu'un client dispose d'une connexion via Citrix Gateway Service et lance une application :

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
SSLEnable=On
SSLProxyHost=global.g.nssvcstaging.net:443
<!--NeedCopy-->
```

Voici un exemple de fichier ICA lorsqu'un client dispose d'une connexion via une passerelle locale et lance une application à l'aide d'une passerelle locale configurée dans l'emplacement de ressources :

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
SSLEnable=On
SSLProxyHost=onpremgateway.domain.com:443
<!--NeedCopy-->
```

> **Remarque :**
>
> Les serveurs virtuels de passerelle locale utilisés pour lancer des applications et des bureaux virtuels doivent être des serveurs virtuels VPN, et non des serveurs virtuels d'authentification

> nFactor. Les serveurs virtuels d'authentification nFactor servent uniquement à l'authentification des utilisateurs et ne fournissent pas de proxy pour le trafic de lancement ICA et des ressources HDX.

Exemple de script

L'exemple de script inclut toutes les commandes dont vous pourriez avoir besoin pour ajouter, modifier et supprimer les plages d'adresses IP publiques de vos succursales. Cependant, vous n'avez pas besoin d'exécuter toutes les commandes pour exécuter une fonction unique. Pour que le script s'exécute, incluez toujours les 10 premières lignes, de **Import-Module** jusqu'à **Connect-NLS**. Par la suite, vous pouvez inclure uniquement les commandes pour les fonctions que vous souhaitez effectuer.

```
Import-Module .\nls.psm1 -Force

$clientId = "XXXX" #Replace with your clientId
$clientSecret = "YYY"    #Replace with your clientSecret
$customer = "CCCCCC"  #Replace with your customerid

# Connect to Network Location Service
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer $customer

# Create a new Network Location Service Site (Replace with details corresponding to your branch locations)
New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True

# Get the existing Network Location Service Sites (optional)
Get-NLSSite

# Update the IP Address ranges of your first Network Location Service Site (optional)
$s = (Get-NLSSite)[0]
$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
\$s | Set-NLSSite

# Remove all Network Location Service Sites (optional)
Get-NLSSite | Remove-NLSSite

# Remove your third site (optional)
\(Get-NLSSite)\[2] | Remove-NLSSite
```


Dépannage

Échecs de lancement du VDA

Si les sessions VDA ne parviennent pas à démarrer, vérifiez que vous utilisez des plages d'adresses IP publiques à partir du réseau approprié. Lors de la configuration de vos emplacements réseau, vous devez utiliser les plages d'adresses IP publiques sur le réseau à partir duquel vos utilisateurs se connectent pour accéder à Internet. Pour plus d'informations, consultez la section Exigences dans cet article.

Les lancements de VDA internes sont toujours acheminés par la passerelle

Si les sessions VDA lancées en interne sont toujours acheminées via la passerelle comme s'il s'agissait de sessions externes, vérifiez que vous utilisez l'adresse IP publique correcte à partir de laquelle vos utilisateurs internes se connectent pour accéder à leur espace de travail. L'adresse IP publique répertoriée sur le site NLS doit correspondre à l'adresse que le client qui lance les ressources utilise pour accéder à Internet. Pour obtenir l'adresse IP publique correcte pour le client, connectez-vous à l'ordinateur client, visitez un moteur de recherche et saisissez « what is my ip » dans la barre de recherche.

Tous les clients qui lancent des ressources à partir du même emplacement de bureau accèdent généralement à Internet en utilisant la même adresse IP publique de sortie réseau. Ces clients doivent disposer d'un itinéraire réseau Internet vers les sous-réseaux où résident les VDA, qui n'est pas bloqué par un pare-feu. Pour plus d'informations, consultez la section Exigences dans cet article.

Erreurs lors de l'exécution des applets de commande PowerShell sur des plates-formes non Windows

Si vous rencontrez des erreurs lors de l'exécution des applets de commande avec les paramètres corrects sur PowerShell Core, vérifiez que l'opération a bien été effectuée. Par exemple, si vous rencontrez des erreurs lors de l'exécution de l'applet de commande New-NLSSite, exécutez `Get-NLSSite` pour vérifier que le site a été créé. L'exécution de ces applets de commande sur des plates-formes macOS ou Linux à l'aide de PowerShell Core peut entraîner une erreur même si l'opération a été exécutée avec succès.

Si vous rencontrez ce problème lors de l'exécution d'applets de commande avec les paramètres corrects sur une plate-forme Windows à l'aide de PowerShell, assurez-vous d'utiliser la dernière version du module PowerShell. Avec la dernière version du module PowerShell, ce problème ne se produit pas sur les plates-formes Windows.

Aide et support supplémentaires

Pour obtenir de l'aide ou des questions sur la résolution des problèmes, contactez votre représentant commercial Citrix ou le support Citrix.

Continuité du service

November 28, 2023

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Les utilisateurs peuvent lancer leurs applications et bureaux Citrix DaaS quel que soit l'état d'intégrité des services cloud.

La continuité du service permet aux utilisateurs de se connecter à leurs applications et bureaux DaaS pendant les pannes, tant que la machine utilisateur maintient une connexion réseau à un emplacement de ressources. Les utilisateurs peuvent se connecter à leurs applications et bureaux DaaS pendant les pannes dans les composants Citrix Cloud ou dans les clouds publics et privés. Les utilisateurs peuvent se connecter directement à l'emplacement des ressources ou via Citrix Gateway Service.

La continuité du service améliore la représentation visuelle des ressources publiées pendant les pannes en utilisant la technologie Progressive Web Apps Service Worker pour mettre en cache les ressources dans l'interface utilisateur.

La continuité du service utilise les locations de connexion Workspace pour permettre aux utilisateurs d'accéder aux applications et aux bureaux en cas de panne. Les locations de connexion Workspace sont des jetons d'autorisation de longue durée. Les fichiers de location de connexion Workspace sont mis en cache en toute sécurité sur la machine utilisateur. Lorsqu'un utilisateur se connecte à Citrix Workspace, les fichiers de location de connexion Workspace sont enregistrés dans le profil utilisateur pour chaque ressource publiée pour l'utilisateur. La continuité du service permet aux utilisateurs d'accéder aux applications et aux bureaux pendant une panne, même si l'utilisateur n'a jamais lancé d'application ou de bureau auparavant. Les fichiers de location de connexion Workspace sont signés et cryptés, et sont associés à l'utilisateur et à la machine utilisateur. Lorsque la continuité du service est activée, une location de connexion Workspace permet aux utilisateurs d'accéder aux applications et aux bureaux pendant sept jours par défaut. Vous pouvez configurer les locations de connexion Workspace pour autoriser l'accès jusqu'à 30 jours.

Lorsque les utilisateurs quittent l'application Citrix Workspace, l'application Citrix Workspace se ferme, mais les locations de connexion Workspace sont conservées. Les utilisateurs quittent l'application Citrix Workspace en cliquant avec le bouton droit sur son icône dans la barre d'état système ou en redémarrant la machine utilisateur. Vous pouvez configurer la continuité du service

pour supprimer ou conserver les locations de connexion Workspace lorsque les utilisateurs se déconnectent de Citrix Workspace pendant une panne. Par défaut, les locations de connexion Workspace sont supprimées des machines utilisateur lorsque les utilisateurs se déconnectent pendant une panne.

La continuité du service est prise en charge pour les scénarios de double saut lorsque l'application Citrix Workspace est installée sur un bureau virtuel.

Pour obtenir un article technique détaillé sur les fonctionnalités de résilience Citrix Cloud, y compris la continuité du service, consultez la page Citrix Cloud Resiliency.

> **Remarque :**
>
> La fonctionnalité obsolète Citrix DaaS appelée « location de connexion » ressemble aux locations de connexion Workspace car elle permettait d'améliorer la résilience de connexion pendant les pannes. À part cela, cette fonctionnalité obsolète n'est pas liée à la continuité du service.

Configuration de l'appareil utilisateur

Pour accéder aux ressources pendant une panne, les utilisateurs doivent se connecter à Citrix Workspace avant la panne. Lorsque vous activez la continuité du service, les utilisateurs doivent effectuer les opérations suivantes sur leurs appareils :

1. Téléchargez et installez une version prise en charge de l'application Citrix Workspace.
2. Ajouter l'URL Workspace de votre organisation à l'application Citrix Workspace (par exemple, `https://example.cloud.com`)
3. Se connecter avec Citrix Workspace

Lorsqu'un utilisateur se connecte à Citrix Workspace pour la première fois, la continuité du service télécharge les locations de connexion Workspace sur la machine utilisateur.

Le téléchargement de locations de connexion Workspace peut prendre jusqu'à 15 minutes pour la première connexion. Les utilisateurs peuvent continuer à lancer des ressources publiées pendant la période de téléchargement.

Expérience utilisateur lors d'une panne

Lorsque la continuité du service est activée, l'expérience utilisateur pendant une panne varie en fonction des éléments suivants :

- Type de panne
- Configuration (ou non) de l'application Citrix Workspace avec l'authentification pass-through au domaine

- Activation (ou non) du partage de session pour le bureau ou l'application auquel l'utilisateur se connecte

En cas de panne, les utilisateurs continuent d'accéder à leurs applications et bureaux DaaS sans que leur expérience utilisateur ne change. Pour d'autres pannes, l'utilisateur peut constater un changement dans la façon dont Workspace apparaît ou être invité à prendre des mesures.

Ce tableau résume comment la continuité du service aide les utilisateurs à accéder aux applications et aux bureaux lors de différents types de pannes.

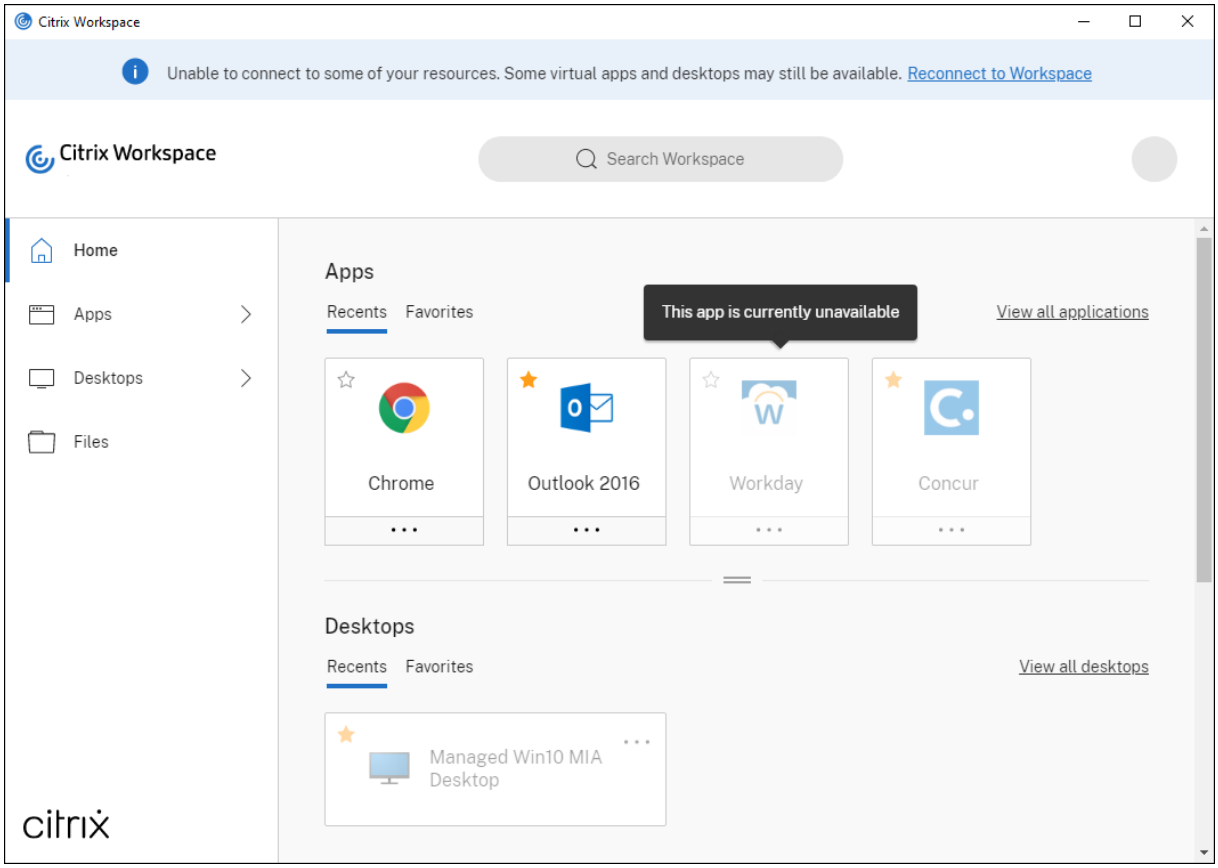
Emplacement de la panne	Comment la continuité du service maintient l'accès des utilisateurs	Expérience utilisateur lors d'une panne
Service Citrix Workspace	L'application Citrix Workspace énumère les applications et les bureaux en fonction du cache local sur la machine utilisateur.	Les icônes des applications et des bureaux non disponibles sont assombries. Les utilisateurs peuvent toujours accéder aux applications et aux bureaux dont les icônes ne sont pas assombries. Après avoir cliqué sur une icône non grisée, les utilisateurs peuvent être invités à entrer à nouveau leurs informations d'identification sur le VDA. Pour accéder de nouveau à toutes leurs applications et bureaux, les utilisateurs peuvent essayer d'établir leur connexion à Workspace en cliquant sur le lien « Se reconnecter à Workspace ».

Emplacement de la panne	Comment la continuité du service maintient l'accès des utilisateurs	Expérience utilisateur lors d'une panne
Fournisseur d'identité	L'application Citrix Workspace énumère les applications et les bureaux en fonction du cache local sur la machine utilisateur.	Les utilisateurs peuvent ne pas être en mesure de se connecter à Workspace. Les utilisateurs cliquent sur le lien « Utiliser Workspace hors ligne » pour accéder à certaines applications et bureaux dans une expérience identique à une panne de service Workspace.
Citrix Cloud Broker Service	Le service High Availability Service du Cloud Connector reprend la négociation des connexions. Tous les VDA enregistrés auprès de Cloud Broker Service s'ont inscrits auprès de High Availability Service.	Certains utilisateurs peuvent ne pas être en mesure d'accéder aux ressources virtuelles lorsque les VDA s'inscrivent auprès de High Availability Service. Les sessions existantes ne sont pas affectées. Aucune action utilisateur n'est requise.
Secure Ticket Authority	Les locations de connexion Workspace fournissent un accès aux ressources virtuelles lorsque les fichiers ICA ne le peuvent pas.	Les lancements de sessions peuvent prendre quelques secondes de plus. Aucune action utilisateur n'est requise.
Citrix Gateway Service	Le trafic réseau bascule vers l'emplacement POP (Point of Presence) Citrix Gateway opérationnel le plus proche.	La reconnexion des sessions existantes peut prendre quelques secondes. Aucune action utilisateur n'est requise.

Emplacement de la panne	Comment la continuité du service maintient l'accès des utilisateurs	Expérience utilisateur lors d'une panne
Connexion Internet sur le réseau local	L'application Citrix Workspace énumère les applications et les bureaux en fonction du cache local sur la machine utilisateur. Si un utilisateur dispose d'une connexion réseau directe à l'emplacement des ressources, l'application Citrix Workspace contourne Citrix Gateway Service lorsque l'utilisateur clique sur des icônes non grisées. L'application Citrix Workspace contacte le Cloud Connector via TCP 2598 et contacte les VDA via TCP 2598 ou UDP 2598.	Les icônes des applications et des bureaux non disponibles sont assombries. Les utilisateurs peuvent toujours accéder aux applications et aux bureaux dont les icônes ne sont pas assombries. Après avoir cliqué sur une icône non grisée, les utilisateurs peuvent être invités à entrer à nouveau leurs informations d'identification sur le VDA. Pour accéder de nouveau à toutes leurs applications et bureaux, les utilisateurs peuvent essayer d'établir leur connexion à Workspace en cliquant sur le lien « Se reconnecter à Workspace ».

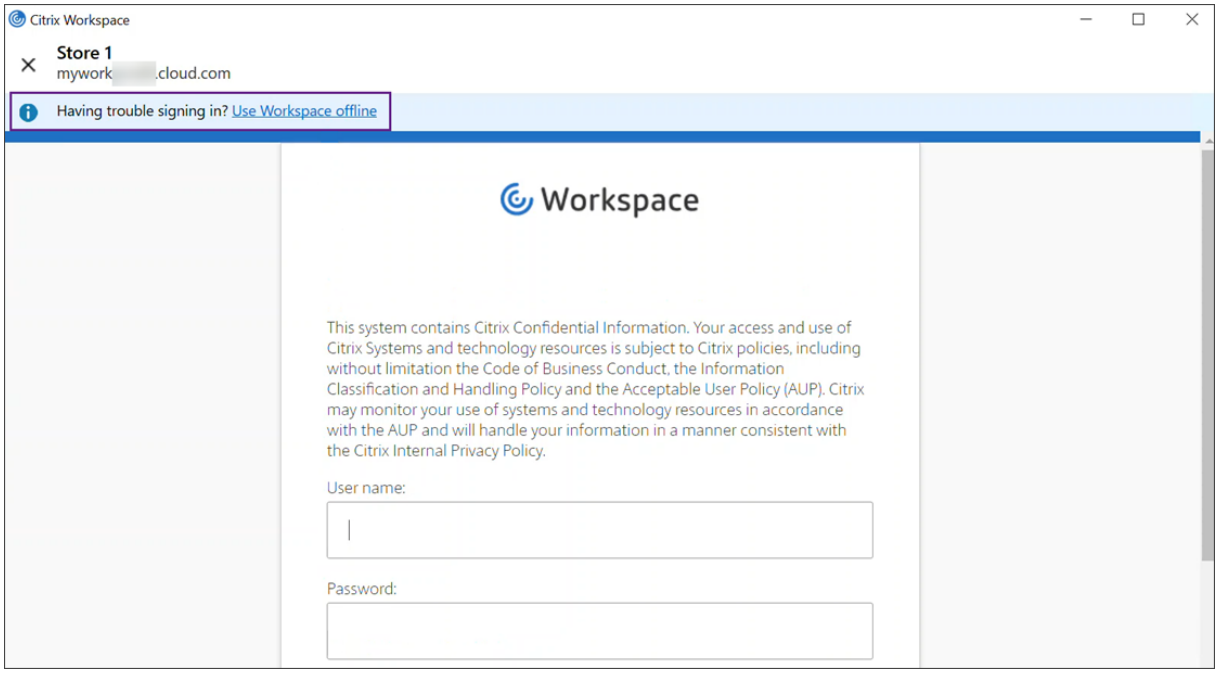
> **Remarque :**
>
> Pour plus d'informations sur la validation des scénarios de panne dans un environnement hors production, consultez le Service Continuity Companion Guide.

Lors d'une panne Citrix Workspace, les utilisateurs voient ce message en haut de la page d'accueil de Citrix Workspace : « Impossible de se connecter à certaines de vos ressources. Certaines applications et certains bureaux virtuels peuvent toujours être disponibles. » Les utilisateurs voient les applications et les bureaux auxquels ils peuvent se connecter pendant la panne. Si l'application ou le bureau n'est pas disponible, l'icône apparaît grisée.



Pour accéder aux ressources disponibles pendant une panne, les utilisateurs sélectionnent une icône de ressources qui n'est pas grisée. Si vous y êtes invité, l'utilisateur saisit de nouveau ses informations d'identification AD sur le VDA avant d'accéder aux ressources.

Lors d'une panne avec le fournisseur d'identité pour l'authentification de l'espace de travail, les utilisateurs peuvent ne pas être en mesure de se connecter à Citrix Workspace via la page de connexion Workspace. Au bout de 40 secondes, ce message s'affiche en haut de la page d'accueil de Citrix Workspace.



La page d'accueil Citrix Workspace s'affiche ensuite. Les utilisateurs accèdent alors aux ressources comme lors d'une panne de Citrix Workspace.

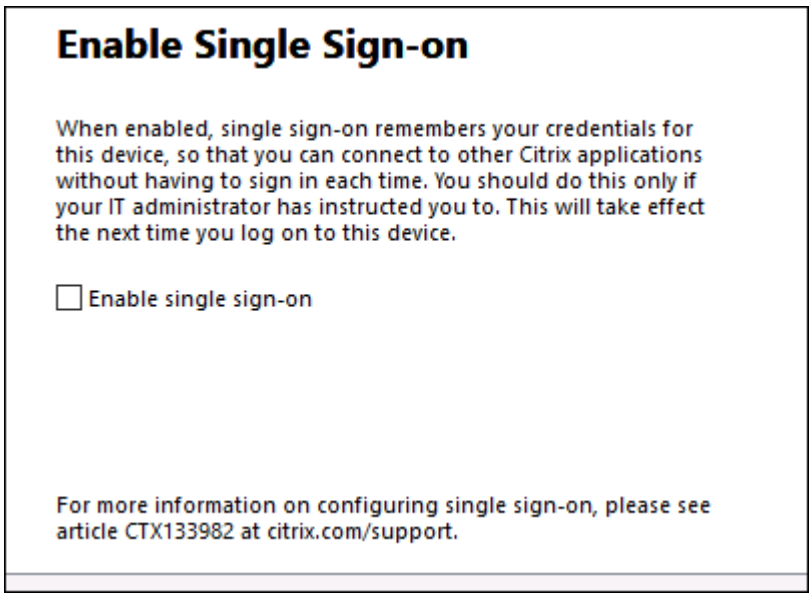
Quel que soit le type de panne, les utilisateurs peuvent continuer à accéder aux ressources s'ils quittent et relancent l'application Citrix Workspace. Les utilisateurs peuvent redémarrer leurs machines utilisateur sans perdre l'accès aux ressources.

Dans la configuration par défaut de la continuité du service, les utilisateurs perdent l'accès à leurs ressources s'ils se déconnectent de Citrix Workspace. Si vous souhaitez que les utilisateurs conservent l'accès à leurs ressources après leur déconnexion, spécifiez que les locations de connexion Workspace doivent être conservées lorsque les utilisateurs se déconnectent. Consultez Configurer la continuité du service.

Selon la façon dont l'application Citrix Workspace et les VDA sont configurés, pendant une panne, le VDA peut inviter les utilisateurs à entrer leurs informations d'identification dans l'interface utilisateur d'ouverture de session Windows. Si cette invite s'affiche, les utilisateurs saisissent leurs informations d'identification Active Directory (AD) ou le code PIN de leur carte à puce pour accéder à l'application ou au bureau. Cette étape est requise lorsque les informations d'identification de l'utilisateur ne sont pas transmises pendant les pannes. Avant d'accéder à une application ou à un bureau, les utilisateurs doivent s'authentifier à nouveau auprès du VDA.

Les utilisateurs peuvent accéder aux ressources sans entrer leurs informations d'identification AD dans les cas suivants :

- Citrix Workspace est configuré pour l'authentification unique (Single Sign-On) pendant l'installation lorsque la case à cocher Single Sign-On est sélectionnée.



- L'application Citrix Workspace est configurée avec l'authentification pass-through au domaine. Les utilisateurs peuvent accéder à n'importe quelle ressource disponible pendant une panne de Citrix Workspace sans entrer leurs informations d'identification. Pour plus d'informations sur la configuration de l'authentification pass-through au domaine pour l'application Citrix Workspace pour Windows, consultez Configurer Single Sign-On à l'aide de l'interface utilisateur graphique, disponible dans la section **Authentification**.

  > **Remarque**
  >
  > StoreFront n'est pas requis pour autoriser Single Sign-On à votre VDA en cas de panne.

- Le partage de session est activé. Les utilisateurs peuvent accéder aux applications ou aux bureaux hébergés sur le même VDA après avoir fourni leurs informations d'identification pour une ressource sur ce VDA. Le partage de session est configuré pour le groupe d'applications contenant la ressource sur le VDA. Pour plus d'informations sur la configuration des groupes d'applications, consultez la section Créer des groupes d'applications.

Dans toutes les autres configurations, les utilisateurs sont invités à entrer de nouveau leurs informations d'identification AD sur le VDA avant d'accéder aux ressources.

Configuration requise et limitations

Configuration requise liée au site

- Prise en charge dans toutes les éditions de Citrix DaaS et de Citrix DaaS Standard pour Azure lorsque vous utilisez l'expérience d'espace de travail.

- Non prise en charge pour Citrix Workspace avec l'agrégation de sites vers des sites Virtual Apps and Desktops locaux
- Non pris en charge lorsque l'instance Citrix Gateway locale est utilisée comme proxy ICA. (L'utilisation de Citrix Gateway comme méthode d'authentification Workspace est prise en charge.)

Configuration requise pour la machine utilisateur

Versions minimales de l'application Citrix Workspace prises en charge :

- Application Citrix Workspace pour Windows 2106
- Application Citrix Workspace pour Linux 2106
- Application Citrix Workspace pour Mac 2106
- Application Citrix Workspace pour Android 22.2.0
- Application Citrix Workspace pour iOS 22.4.5
- Application Citrix Workspace pour ChromeOS 2301

> **Remarque :**
>
> Pour plus d'informations sur l'installation de l'application Citrix Workspace pour Linux, y compris sur l'installation de l'application pour une utilisation avec la continuité du service, consultez Application Citrix Workspace pour Linux.

- Pour les utilisateurs qui accèdent à leurs applications et bureaux à l'aide d'un navigateur :
  - Google Chrome ou Microsoft Edge.
  - Application Citrix Workspace 2109 pour Windows, au minimum. Pris en charge avec Google Chrome et Microsoft Edge.
  - Application Citrix Workspace pour Mac version 2112 au minimum pour une utilisation avec Google Chrome.
  - Application Citrix Workspace pour Mac version 2206 au minimum pour une utilisation avec le navigateur Safari.

  Consultez Continuité du service dans le navigateur.
- Un seul utilisateur par appareil est pris en charge. Les machines utilisateur de type kiosque ou « hot desk » ne sont pas prises en charge.

Méthodes d'authentification de l'espace de travail

- Active Directory
- Active Directory + jeton
- Azure Active Directory

- Okta
- Citrix Gateway (la revendication de l'utilisateur principal doit provenir d'AD)
- SAML 2.0

Limites d'authentification

- L'authentification unique avec le Service d'authentification fédérée de Citrix (FAS) n'est pas prise en charge. Les utilisateurs saisissent leurs informations d'identification AD dans l'interface utilisateur de connexion Windows sur le VDA.
- L'authentification unique au VDA n'est pas prise en charge.
- Les comptes mappés locaux ne sont pas pris en charge.
- Les VDA appartenant à Azure AD ne sont pas pris en charge. Tous les VDA doivent appartenir à un domaine AD.

Dimensionnement et scalabilité de Citrix Cloud Connector

- 4 processeurs virtuels ou plus
- 4 Go de mémoire ou plus

Sécurité du Powershell de Citrix Cloud Connector

Assurez-vous que l'exécution du script est activée en définissant la stratégie d'exécution sur la valeur **remotedSigned** adaptée à votre environnement.
D'autres privilèges d'exécution de scripts peuvent également fonctionner, tels que **Default** ou **AllSigned**.

Connectivité Citrix Cloud Connector

Citrix Cloud Connector doit pouvoir accéder à `https://rootoftrust.apps.cloud.com`. Configurez votre pare-feu pour autoriser cette connexion. Pour plus d'informations sur le pare-feu Cloud Connector, consultez Configuration du pare-feu et du proxy d'un Cloud Connector.

Connexion réseau de l'application Workspace

Si vous configurez la connexion à votre emplacement de ressources depuis l'extérieur de votre réseau local, l'application Workspace sur les machines utilisateur doit être en mesure d'atteindre le nom de domaine complet de Citrix Gateway Service, `https://*.g.nssvc.net`. Assurez-vous que votre

pare-feu est configuré pour autoriser le trafic sortant vers `https://global-s.g.nssvc.net:433`, afin que les machines utilisateur puissent se connecter à Citrix Gateway Service à tout moment.

Limitations d'optimisation de la connectivité

L'analyse EPA (Advanced Endpoint Analysis) n'est pas prise en charge.

La fonction Enlightened Data Transport (EDT) n'est pas pris en charge pendant les pannes.

Configuration requise et limitations du VDA

- Les VDA 7.15 LTSR ou toute version actuelle qui n'a pas atteint sa fin de vie sont pris en charge.
- Les VDA appartenant à Azure AD ne sont pas pris en charge. Tous les VDA doivent appartenir à un domaine AD.
- Les VDA doivent être en ligne pour que les utilisateurs puissent accéder aux ressources VDA pendant une panne. Les ressources VDA ne sont pas disponibles lorsque le VDA est affecté par des pannes dans les services suivants :
  - AWS
  - Azure
  - Cloud Delivery Controller, sauf si la fonctionnalité Autoscale est activée pour le groupe de mise à disposition fournissant la ressource.
- Les charges de travail VDA sont prises en charge pendant les pannes :
  - Applications et bureaux partagés hébergés
  - Bureaux aléatoires non persistants (bureau VDI regroupé) avec gestion de l'alimentation
  - Bureaux statiques non persistants
  - Bureaux statiques persistants, y compris Remote PC Access

> **Remarque :**
>
> L'attribution lors de la première utilisation n'est pas prise en charge pendant les pannes. Les bureaux non persistants aléatoires avec gestion de l'alimentation ne sont pas disponibles par défaut si les Cloud Connector perdent la connectivité avec Citrix Cloud, sauf si `ReuseMachinesWithoutShutdownInOutage` est configuré pour le groupe de mise à disposition. Pour plus d'informations, consultez Prise en charge des applications et des bureaux.

Pour plus d'informations sur les fonctions VDA disponibles pendant les pannes, consultez la section Gestion du VDA pendant les pannes.

Exigences et limitations du mappage du clavier local

L'interface utilisateur d'ouverture de session Windows qui invite les utilisateurs à se réauthentifier sur le VDA ne prend pas en charge le mappage de la langue du clavier local. Pour permettre aux utilisateurs de s'authentifier de nouveau lors d'une panne s'ils disposent d'un mappage de la langue du clavier local sur leurs appareils, préchargez les dispositions de clavier dont ces utilisateurs ont besoin.

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Modifiez cette clé de registre dans l'image VDA :

```
HKEY_USERS\.DEFAULT\Keyboard Layout\Preload
```

Le pack de langue correspondant dans l'image du bureau virtuel doit être installé.

Pour obtenir la liste des identificateurs de clavier associés aux langues du clavier, consultez Identificateurs de clavier et éditeurs de méthode d'entrée pour Windows.

Configurer la connectivité réseau d'emplacement des ressources pour assurer la continuité

Vous pouvez configurer votre emplacement de ressources pour accepter les connexions provenant de l'extérieur ou de l'intérieur de votre réseau local (ou des deux).

Configurer les connexions provenant de l'intérieur de votre réseau local

1. Dans le menu Citrix Cloud, accédez à **Configuration de l'espace de travail > Accès**.
2. Sélectionnez **Configurer la connectivité**.
3. Sélectionnez **Interne uniquement** comme type de connectivité.
4. Cliquez sur **Save**.

Configurez vos pare-feu Citrix Cloud Connector et VDA pour accepter les connexions via le port TCP 2598 de Common Gateway Protocol (CGP). Cette configuration est le paramètre par défaut.

Configurer les connexions provenant de l'extérieur de votre réseau local

1. Dans le menu Citrix Cloud, accédez à **Configuration de l'espace de travail > Accès**.
2. Sélectionnez **Configurer la connectivité**.
3. Sélectionnez **Gateway Service** comme type de connectivité.
4. Cliquez sur **Save**.

Configurer les connexions provenant de l'extérieur et de l'intérieur de votre réseau local

Exécutez cette commande PowerShell :

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocationE
)-EnableHybridConnectivityForResourceLeases $true
```

Remplacez `YourResourceLocationExternalUid` par l'UID externe de l'emplacement de ressources.

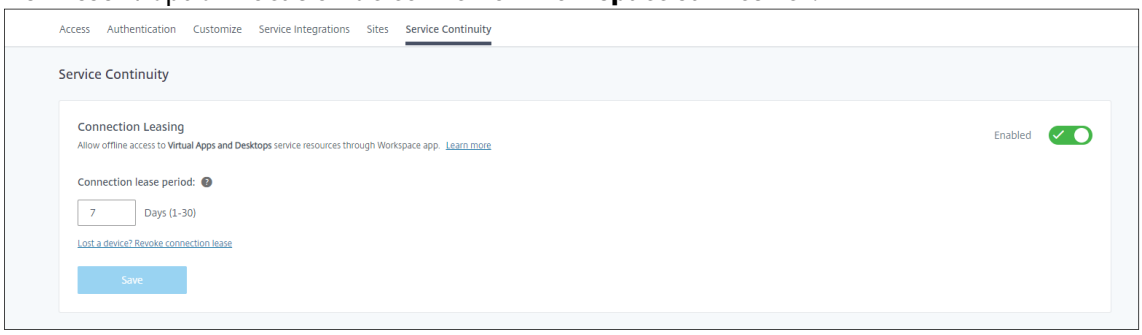
Cette commande permet des connexions directes au nom de domaine complet Citrix Cloud Connector via TCP 2598 pendant les pannes. Si cette connexion échoue, Gateway Service est utilisé comme connexion de secours. Autorisez les utilisateurs internes à contourner la passerelle et à se connecter directement à l'emplacement des ressources afin de réduire la latence du trafic réseau interne.

> **Remarque :**
>
> Cette commande PowerShell est similaire à Direct Workload Connection. En effet, elle optimise la connectivité aux espaces de travail en permettant aux utilisateurs internes de contourner la passerelle et de se connecter directement aux VDA. Lorsque la continuité du service est activée, Direct Workload Connection n'est pas disponible pendant les pannes.

Configurer la continuité du service

Pour activer la continuité du service pour votre site :

1. Dans le menu Citrix Cloud, accédez à **Configuration de l'espace de travail > Continuité du service**.
2. Définissez l'option **Location de connexion Workspace** sur **Activer**.



3. Définissez l'option **Période de location de connexion** sur le nombre de jours pendant lesquels une location de connexion Workspace peut être utilisée pour maintenir une connexion. La période de location de connexion Workspace s'applique à toutes les locations de connexion Workspace via votre site. La période de location de connexion Workspace commence la première fois qu'un utilisateur se connecte au magasin Citrix Cloud Workspace. Les locations de connexion Workspace sont actualisées chaque fois que l'utilisateur se connecte, jusqu'à une fois par jour. La période de location de connexion Workspace peut aller d'un jour à 30 jours. La valeur par défaut est de sept jours.
4. Cliquez sur **Save**.

Lorsque vous activez la continuité du service, cette fonction est activée pour tous les groupes de mise à disposition de votre site. Pour désactiver la continuité du service pour un groupe de mise à disposition, utilisez la commande PowerShell suivante :

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

Remplacez `deliverygroup` par le nom du groupe de mise à disposition.

Par défaut, les locations de connexion Workspace sont supprimées de la machine utilisateur si l'utilisateur se déconnecte de Citrix Workspace pendant une panne. Si vous souhaitez que les locations de connexion Workspace restent sur les machines utilisateur après que les utilisateurs se déconnectent, utilisez la commande PowerShell suivante :

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

> **Remarque :**
>
> Les locations de connexion Workspace ne peuvent pas être configurées pour rester sur les machines utilisateur une fois que les utilisateurs se sont déconnectés pour des utilisateurs se connectant à l'application Citrix Workspace pour Mac. Citrix Workspace pour Mac ne peut pas lire la valeur de la propriété `DeleteResourceLeaseOnLogOff`.

Fonctionnement de la continuité du service

S'il n'y a pas de panne, les utilisateurs accèdent aux applications et aux bureaux virtuels à l'aide de fichiers ICA. Citrix Workspace génère un fichier ICA unique chaque fois qu'un utilisateur sélectionne une icône d'application ou de bureau virtuel. Chaque fichier ICA contient un ticket STA (Secure Ticket Authority) et un ticket d'ouverture de session qui ne peuvent être échangés qu'une seule fois pour obtenir un accès autorisé aux ressources virtuelles. Les tickets dans chaque fichier ICA expirent après environ 90 secondes. Une fois le ticket d'un fichier ICA utilisé ou expiré, l'utilisateur a besoin d'un autre fichier ICA de Citrix Workspace pour accéder aux ressources. Lorsque la continuité du service n'est pas activée, les pannes peuvent empêcher les utilisateurs d'accéder aux ressources si Citrix Workspace ne peut pas générer de fichier ICA.

Citrix Workspace génère des fichiers ICA lorsque les utilisateurs lancent des applications et des bureaux virtuels, que la continuité du service soit activée ou non. Lorsque la continuité du service est activée, Citrix Workspace génère également l'ensemble unique de fichiers qui composent une location de connexion Workspace. Contrairement aux fichiers ICA, les fichiers de location de connexion Workspace sont générés lorsque l'utilisateur se connecte à Citrix Workspace, et non lorsque l'utilisateur lance la ressource. Lorsqu'un utilisateur se connecte à Citrix Workspace, des fichiers de location de connexion sont générés pour chaque ressource publiée pour cet utilisateur. Les locations de connexion Workspace contiennent des informations qui donnent à l'utilisateur l'accès aux ressources virtuelles. Si une panne empêche un utilisateur de se connecter à Citrix Workspace ou d'accéder aux ressources à l'aide d'un fichier ICA, la location de connexion fournit un accès autorisé à la ressource.

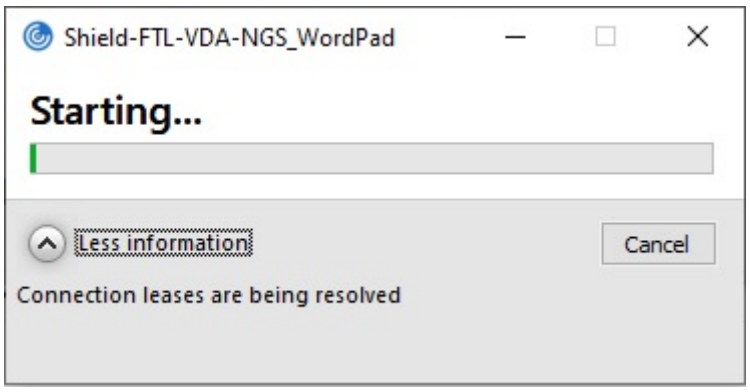
Lancement des sessions pendant les pannes

Lorsque les utilisateurs cliquent sur une icône pour une application ou un bureau pendant une panne, l'application Citrix Workspace trouve la location de connexion Workspace correspondante sur la machine utilisateur. L'application Citrix Workspace ouvre ensuite une connexion. Si la connectivité à l'emplacement de ressources qui héberge l'application ou le bureau est configurée pour accepter des connexions provenant de l'extérieur de votre réseau local, une connexion à Citrix Gateway Service s'ouvre. Si la connectivité à l'emplacement de ressources qui héberge l'application ou le bureau est configurée pour accepter des connexions à partir de votre réseau local uniquement, une connexion au Cloud Connector s'ouvre.

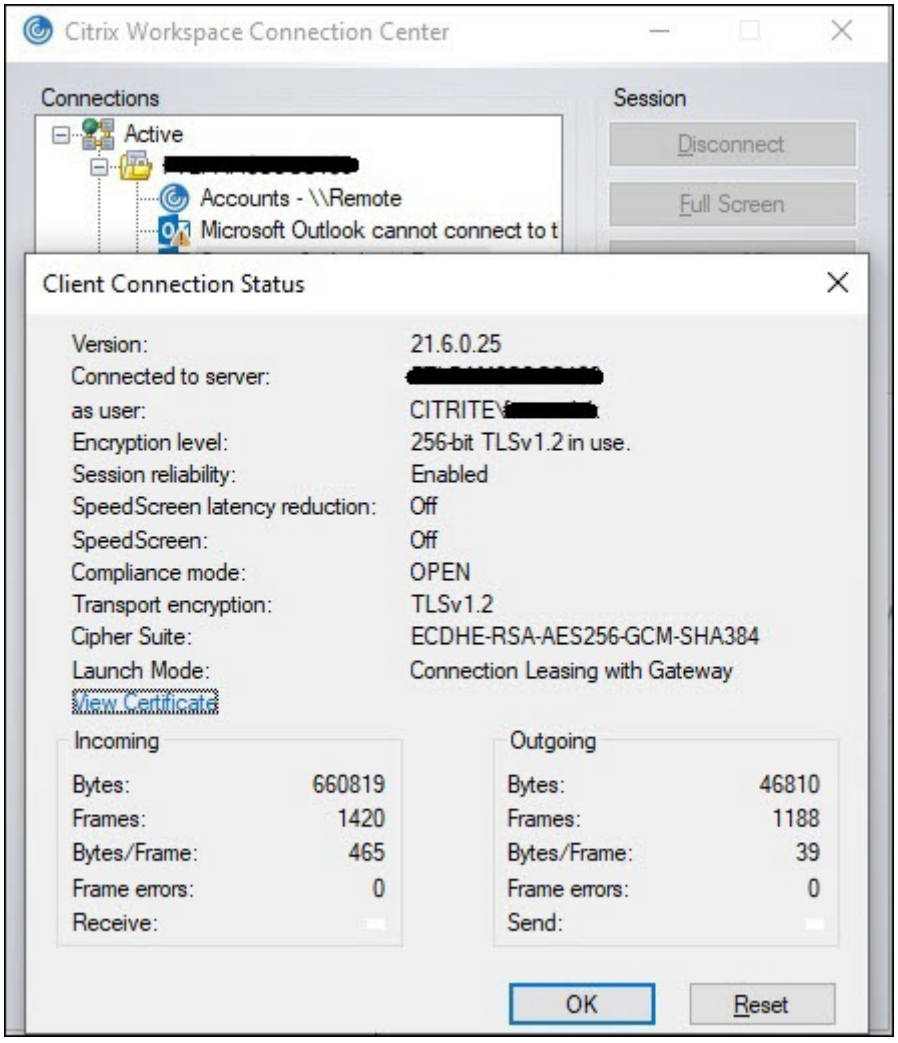
Lorsque le broker Citrix Cloud est en ligne, Cloud Connector utilise le broker Citrix Cloud pour résoudre le VDA disponible. Lorsque le broker Citrix Cloud est hors ligne, le broker secondaire pour Cloud Connector (également connu sous le nom de High Availability Service) écoute et traite les demandes de connexion.

Les utilisateurs qui sont connectés lorsqu'une panne se produit peuvent continuer à travailler sans interruption. Les délais des nouvelles connexions et des reconnexions sont réduits. Cette fonctionnalité est similaire à celle du cache d'hôte local, mais elle ne nécessite pas d'instance StoreFront locale.

Lorsqu'un utilisateur lance une session pendant une panne, cette fenêtre apparaît indiquant que les locations de connexion Workspace ont été utilisées pour le lancement de la session :



Une fois que l'utilisateur a fini de se connecter à la session, ces propriétés apparaissent dans le Centre de connexion Workspace :



La propriété Mode de lancement fournit des informations sur les locations de connexion Workspace utilisées pour lancer la session.

Sur les appareils exécutant l'application Citrix Workspace pour Mac, Citrix Viewer affiche des informa-

tions indiquant que des locations de connexion Workspace ont été utilisées pour le lancement de la session :

Sécurité de la fonction

Toutes les informations sensibles contenues dans les fichiers de location de connexion Workspace sont cryptées avec le chiffrement AES-256. Les locations de connexion Workspace sont liées à une paire de clés publique/privée uniquement associée à la machine client spécifique et ne peuvent pas être utilisées sur un autre appareil. Un mécanisme cryptographique intégré applique l'utilisation de la paire de clés unique sur chaque appareil.

Les locations de connexion Workspace sont stockées sur la machine utilisateur dans AppData\Local\Citrix\SelfService\ConnectionLeases.

L'architecture de sécurité de la continuité du service repose sur la cryptographie de clé publique, tout comme une infrastructure de clé publique (PKI), mais sans chaîne de certificats ni d'autorité de certification. Au lieu de cela, tous les composants établissent une approbation transitive en s'appuyant sur un nouveau service Citrix Cloud appelé racine de confiance qui agit comme une autorité de certification.

Bloquer les locations de connexion

Si une machine utilisateur est perdue ou volée, ou si un compte d'utilisateur est fermé ou compromis, vous pouvez bloquer les locations de connexion Workspace. Lorsque vous bloquez les locations de connexion Workspace associées à un utilisateur, l'utilisateur ne peut pas se connecter aux ressources. Citrix Cloud ne génère plus ni ne synchronise les locations de connexion Workspace pour l'utilisateur.

Lorsque vous bloquez les locations de connexion Workspace associées à un compte d'utilisateur, vous bloquez les connexions à ce compte sur tous les appareils associés à ce compte. Vous pouvez bloquer

les locations de connexion Workspace pour un utilisateur ou pour tous les utilisateurs d'un groupe d'utilisateurs.

Pour révoquer les locations de connexion Workspace pour un seul utilisateur ou groupe d'utilisateurs, utilisez la commande PowerShell suivante :

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays
 Days
```

Remplacez `username` par l'utilisateur associé au compte auquel vous souhaitez bloquer la connexion. Remplacer `username` par un groupe d'utilisateurs pour bloquer la connexion de tous les comptes du groupe d'utilisateurs. Remplacer `Days` par le nombre de jours pendant lesquels les connexions seront bloquées.

Par exemple, pour bloquer les connexions pour xd.local/user1 pendant les 7 prochains jours, entrez :

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
     LeaseRevocationDays 7
```

Pour afficher la période pendant laquelle les locations de connexion Workspace sont révoquées, utilisez la commande PowerShell suivante :

```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

Remplacez `username` par l'utilisateur ou le groupe d'utilisateurs pour lequel vous souhaitez afficher la période.

Par exemple, pour afficher la période pendant laquelle les locations de connexion Workspace sont révoquées pour xd.local/user1, entrez :

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

Cette information apparaît :

```
1 FullName                          :
2 Name                              : XD\user2
3 UPN                               :
4 Sid                               : S-1-5-21-nnnnnn
5 LeaseRevocationDays               : 2
6 LeaseRevocationDateTimeInUtc      : 2020-12-17T17:34:25Z
7 LastUpdateDateTimeInUtc           : 2020-12-19T17:34:25Z
```

Cette sortie indique que l'utilisateur xd.local/user2 dispose de locations de connexion Workspace révoquées pendant deux jours, du 17 décembre 2020 au 19 décembre 2020, à 17:34:25 UTC chaque jour.

Pour autoriser un compte d'utilisateur dont les locations de connexion Workspace sont révoquées à recevoir une nouvelle connexion, supprimez le bloc à l'aide de cette commande PowerShell :


```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

Remplacez `username` par l'utilisateur ou le groupe d'utilisateurs bloqué que vous souhaitez autoriser à recevoir la connexion. Pour autoriser tous les comptes d'utilisateur bloqués à recevoir des connexions, omettez l'option `Name`.

Scénarios double saut

La continuité du service peut permettre aux utilisateurs d'accéder aux ressources virtuelles lors de pannes dans le scénario de double saut s'ils sont connectés à Citrix Workspace avant que la panne ne se produise. Dans un scénario de double saut, une machine utilisateur physique se connecte à un bureau virtuel sur lequel l'application Citrix Workspace est installée. Le bureau virtuel se connecte ensuite à une autre ressource virtuelle.

Dans le scénario de double saut, la continuité du service peut permettre aux utilisateurs d'accéder aux ressources virtuelles pendant une panne, quel que soit le type de bureau virtuel. Si le bureau virtuel conserve les modifications apportées par l'utilisateur, la continuité du service peut également fournir un accès aux ressources virtuelles lors des pannes qui se produisent alors que l'utilisateur n'est pas connecté.

La continuité du service traite la machine utilisateur physique et le bureau virtuel dans un scénario de double saut comme des points de terminaison client individuels. Chaque appareil possède son propre ensemble de locations de connexion Workspace. Lorsqu'un utilisateur se connecte à Citrix Workspace sur une machine physique, les fichiers de location de connexion Workspace sont téléchargés et enregistrés dans le profil utilisateur sur la machine physique. L'utilisateur accède ensuite à un bureau virtuel et se connecte à Citrix Workspace sur le bureau virtuel. À ce stade, un ensemble différent de locations de connexion Workspace est téléchargé et enregistré dans le profil utilisateur sur le bureau virtuel. Les fichiers de location de connexion Workspace sont associés à l'appareil sur lequel ils sont téléchargés. Les fichiers de location de connexion Workspace ne peuvent pas être copiés sur un autre appareil et réutilisés, même par le même utilisateur. Ainsi, la continuité du service ne peut pas fournir d'accès aux ressources lors des pannes qui se produisent après la fin de la session si le bureau virtuel supprime les modifications apportées au cours d'une session utilisateur. Pour ce type de bureau virtuel, les locations de connexion Workspace font partie des modifications supprimées.

Voici comment fonctionne la continuité du service dans les scénarios de double saut avec chaque type de bureau virtuel pris en charge.

Pour les doubles sauts qui comprennent…	La continuité du service permet d'accéder aux ressources virtuelles pendant les pannes…
Bureaux partagés hébergés	si la panne se produit alors que l'utilisateur est connecté au bureau virtuel.

Pour les doubles sauts qui comprennent…	La continuité du service permet d'accéder aux ressources virtuelles pendant les pannes…
Bureaux non persistants aléatoires (bureau VDI groupé)	si la panne se produit alors que l'utilisateur est connecté au bureau virtuel.
Bureaux statiques non persistants	si le bureau virtuel n'a pas redémarré depuis la dernière connexion de l'utilisateur.
Bureaux statiques persistants	chaque fois qu'une panne survient.

Gestion du VDA pendant les pannes

La continuité du service utilise la fonction Cache d'hôte local dans Citrix Cloud Connector. Le cache d'hôte local permet de continuer les connexions négociées par broker sur un site lorsque la connexion entre Cloud Delivery Controller et Cloud Connector échoue. Étant donné que la continuité du service repose sur le cache d'hôte local, elle partage certaines limitations avec cette fonctionnalité.

> **Remarque :**
>
> Bien que la continuité du service utilise le cache d'hôte local dans Cloud Connector, contrairement au cache d'hôte local, la continuité du service n'est pas prise en charge avec StoreFront local.

Gestion de l'alimentation des VDA pendant les pannes

Si les Cloud Connector perdent leur connectivité à Citrix Cloud, ils ne peuvent pas recevoir les informations d'identification de l'hyperviseur de la part de Citrix Cloud. Cela signifie :

- Durant une panne, toutes les machines se trouvent dans un état d'alimentation inconnu et aucune opération d'alimentation ne peut être émise. Toutefois, les VM de l'hôte qui sont sous tension peuvent être utilisées pour les demandes de connexion.

Par défaut, les VDA de bureau avec alimentation gérée appartenant à des groupes de mise à disposition regroupés dont la propriété **ShutdownDesktopsAfterUse** est activée ne sont pas disponibles pour de nouvelles connexions si les Cloud Connector perdent leur connectivité avec Citrix Cloud. Vous pouvez modifier ce paramètre pour autoriser l'utilisation de ces bureaux si les Cloud Connector perdent leur connectivité avec Citrix Cloud en configurant l'indicateur `ReuseMachinesWithoutShutdownInOutage` sur vos groupes de mise à disposition. La définition du paramètre `ReuseMachinesWithoutShutdownInOutage` sur $true peut entraîner la présence des données des sessions utilisateur précédentes sur le VDA jusqu'à son redémarrage.

La gestion de l'alimentation reprend lorsque les opérations normales reprennent après une panne.

Attribution de machines et inscription automatique

Une machine attribuée peut uniquement être utilisée si l'attribution s'est produite lors d'un fonctionnement normal. De nouvelles attributions ne peuvent pas être effectuées lors d'une panne.

L'inscription et la configuration automatiques de machines Remote PC Access ne sont pas possibles. Toutefois, les machines qui ont été inscrites et configurées lors du fonctionnement normal peuvent être utilisées.

Ressources VDA dans différentes zones

Les utilisateurs d'applications et de bureaux hébergés sur le serveur peuvent utiliser plus de sessions que leurs limites de session configurées, si les ressources se trouvent dans des zones différentes.

Contrairement au cache hôte local, la continuité du service peut lancer des applications et des bureaux à partir de VDA enregistrés dans différentes zones, à condition que la ressource soit publiée dans plusieurs zones. L'application Citrix Workspace peut prendre plus de temps pour trouver une zone saine car elle passe successivement à travers toutes les zones de la location de connexion Workspace.

Surveillance et dépannage

La continuité du service effectue deux actions principales :

- Télécharge les locations de connexion Workspace sur la machine utilisateur. Les locations de connexion Workspace sont générées et synchronisées avec l'application Citrix Workspace.
- Lancez les applications et bureaux virtuels à l'aide des locations de connexion Workspace.

Dépannage du téléchargement des locations de connexion Workspace

Vous pouvez afficher les locations de connexion Workspace à cet emplacement sur la machine utilisateur.

Sur les appareils Windows :

`C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\Store GUID\User GUID\leases`

`Username` est le nom d'utilisateur.

`Store GUID` est l'identificateur unique global du magasin Workspace.

`User GUID` est l'identificateur unique global de l'utilisateur.

Sur les appareils Mac :

`$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot`

Par exemple, ouvrez `/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot`

Sur Linux :

`$HOME/.ICAClient/cache/ConnectionLease`

Par exemple, ouvrez `/home/user1/.ICAClient/cache/ConnectionLease`

Les locations de connexion Workspace sont générées lorsque l'application Citrix Workspace se connecte au magasin Workspace. Affichez les valeurs de clé de registre sur la machine utilisateur pour déterminer si l'application Citrix Workspace a correctement contacté le service de location de connexion Workspace dans Citrix Cloud.

Ouvrez regedit sur la machine utilisateur et affichez cette clé :

`HKCU\Software\Citrix\Dazzle\Sites\store-xxxx`

Si ces valeurs apparaissent dans la clé de registre, l'application Citrix Workspace a contacté ou tenté de contacter le service de location de connexion Workspace :

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

Si l'application Citrix Workspace n'a pas réussi à contacter le service de location de connexion Workspace, `leaseLastCallHomeTime` affiche une erreur avec un horodatage non valide :

```
leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM
```

Si `leaseLastCallHomeTime` n'est pas initialisé, cela signifie que l'application Citrix Workspace n'a jamais tenté de contacter le service de location de connexion Workspace. Pour résoudre ce problème, supprimez le compte de l'application Citrix Workspace et ajoutez-le à nouveau.

Codes d'erreur de l'application Citrix Workspace pour les locations de connexion Workspace

Lorsqu'une erreur de continuité de service se produit sur la machine utilisateur, un code d'erreur apparaît dans le message d'erreur. Les erreurs courantes sont les suivantes :

Code d'erreur	Description
3000	Aucun fichier de location de connexion présent
3002	Impossible de lire ou de trouver la location de connexion
3003	Aucun emplacement de ressource trouvé

Code d'erreur	Description
3004	Détails de connexion manquants dans les locations
3005	Fichier ICA vide
3006	Expiration de la location de connexion. Reconnectez-vous à Workspace.
3007	Location de connexion non valide
3008	Résultat de validation de la location de connexion : vide
3009	Résultat de validation de la location de connexion : non valide
3010	Paramètre manquant
3020	Échec de validation de la location de connexion
3021	Aucun emplacement de ressources trouvé où l'application est publiée
3022	Résultat de validation de la location de connexion : refus
3023	Expiration de l'application Citrix Workspace
3024	L'utilisateur a annulé le lancement basé sur la location alors qu'il était en cours
3025	Dépassement du nombre de nouvelles tentatives de lancement
3026	La ressource négociée (application ou bureau) ne peut pas être lancée

Accéder à selfservice.txt

Pour accéder au fichier `selfservice.txt` pour effectuer le dépannage en libre-service, effectuez les opérations suivantes :

1. Créez un fichier texte vide et nommez-le `enableshieldandlogging.reg`.
2. Copiez le texte suivant dans le fichier et enregistrez-le :

   Éditeur de registre Windows version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle]
   "Tracing"="True"
   "AuxTracing"="True"

"DefaultTracingConfiguration"="global all -detail"
"ConnectionLeasingEnabled"="True"

[HKEY_CURRENT_USER\Software\Citrix\Dazzle]
"RemoteDebuggingPort"="8088"

3. Placez votre fichier enregistré sur le point de terminaison de votre client.
4. Le fichier `selfservice.txt` est désormais détectable sur le chemin suivant : `%LocalAppData%\Citrix\SelfService`.

Continuité du service dans le navigateur

Les extensions pour Google Chrome et Microsoft Edge mettent la continuité du service à la disposition des utilisateurs Windows qui accèdent à leurs applications et bureaux à l'aide de ces navigateurs. Les extensions sont appelées extension Web Citrix Workspace et sont disponibles sur le Chrome Web Store et le site Web du module complémentaire Microsoft Edge.

Ces extensions de navigateur nécessitent une application Citrix Workspace native sur la machine utilisateur pour prendre en charge la continuité du service. Ces versions sont prises en charge :

- Application Citrix Workspace 2109 pour Windows, au minimum. Pris en charge avec Google Chrome et Microsoft Edge.
- Application Citrix Workspace pour Mac version 2112 au minimum. Pris en charge avec Google Chrome.
- Application Citrix Workspace pour Mac version 2206 au minimum pour une utilisation avec le navigateur Safari.

L'application Citrix Workspace pour Windows (Store) n'est pas prise en charge.

L'application Workspace native communique avec l'extension Web Citrix Workspace à l'aide du protocole hôte de messagerie natif pour les extensions de navigateur. Ensemble, l'application Workspace native et l'extension Web Workspace utilisent des locations de connexion Workspace pour permettre aux utilisateurs du navigateur d'accéder à leurs applications et bureaux pendant les pannes.

Cette vidéo montre comment installer et utiliser la continuité de service dans un navigateur.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Configuration de la machine utilisateur pour les utilisateurs du navigateur

Pour utiliser la continuité du service, les utilisateurs doivent effectuer les opérations suivantes sur leurs appareils :

1. Téléchargez et installez une version de l'application Citrix Workspace prise en charge pour les utilisateurs de navigateurs.
2. Téléchargez et installez l'extension Web Citrix Workspace pour Chrome ou Edge.

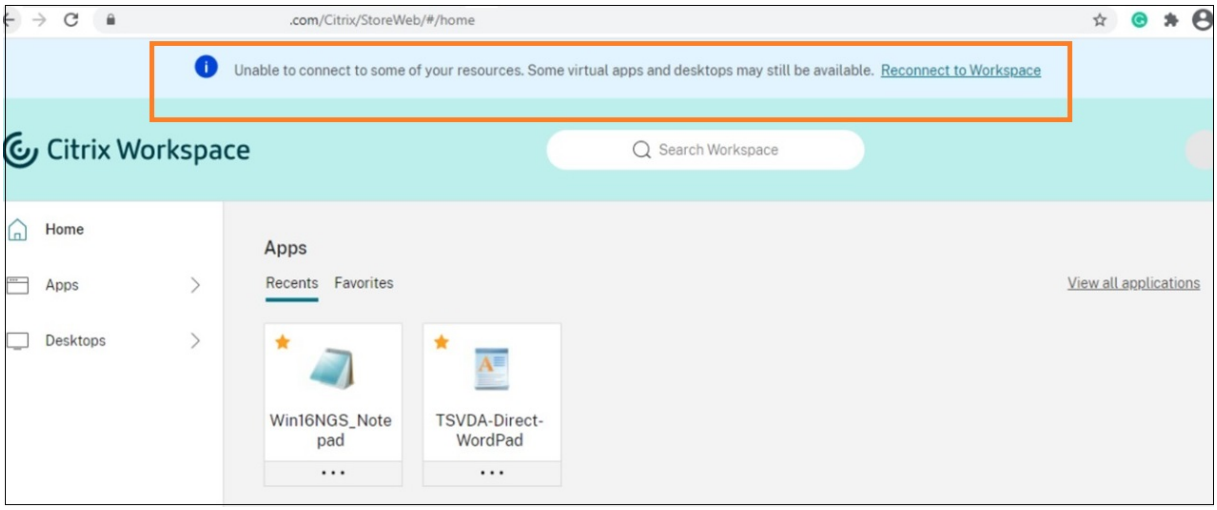
Expérience utilisateur du navigateur

Lorsque les utilisateurs cliquent sur leurs applications ou leurs bureaux, l'application ou le bureau s'ouvre sans que les utilisateurs ne soient invités à ouvrir **Citrix Workspace Launcher**.

Expérience utilisateur du navigateur pendant les pannes

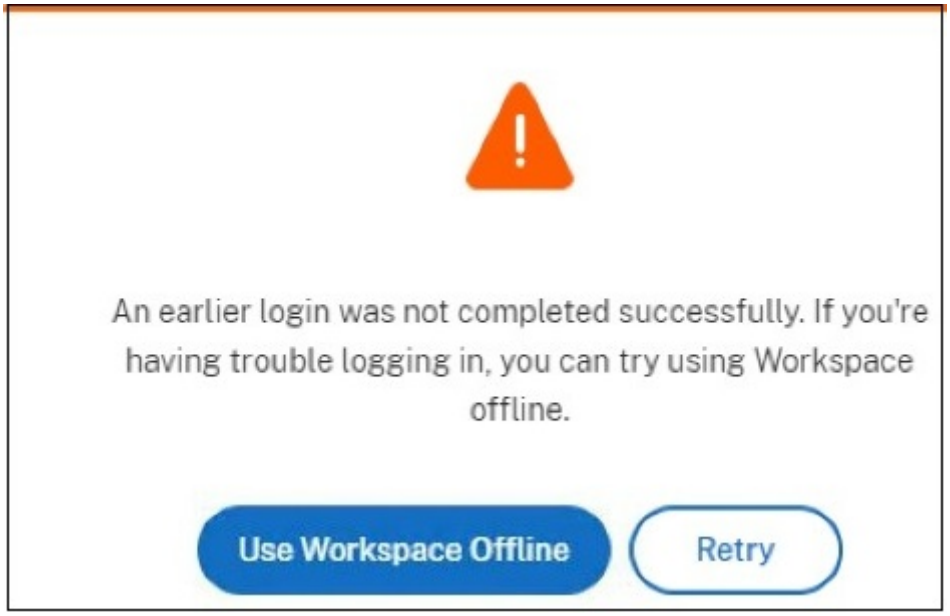
Les utilisateurs peuvent accéder à leurs applications et bureaux à partir d'un navigateur lors de pannes, à condition que la machine utilisateur maintienne une connexion réseau à un emplacement de ressources.

Si une panne survient alors que l'utilisateur est connecté à Workspace via un navigateur, ce message apparaît en haut de la fenêtre du navigateur :



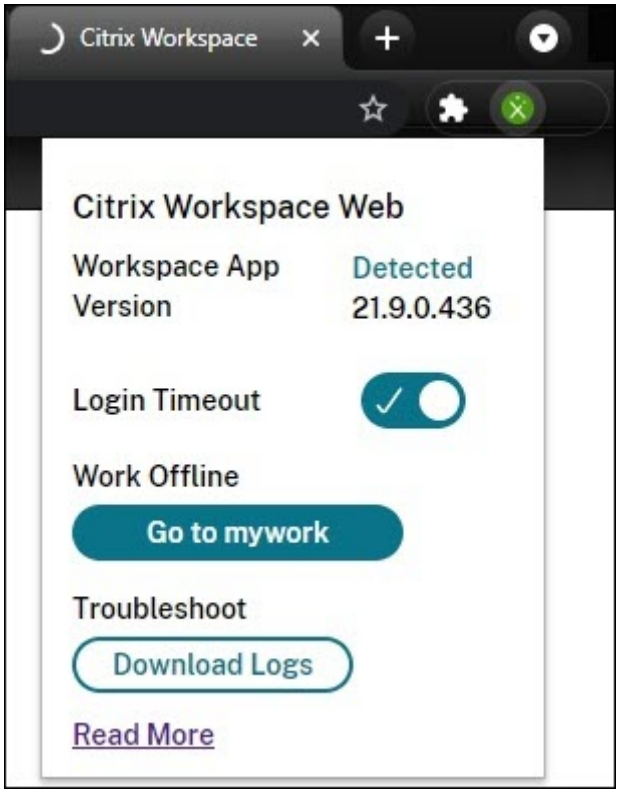
Les utilisateurs peuvent accéder aux applications et aux bureaux disponibles hors connexion en cliquant sur n'importe quelle icône non grisée. Les utilisateurs peuvent également essayer de se remettre en ligne en cliquant sur **Se reconnecter à Workspace**.

Lorsqu'une panne empêche les utilisateurs de se connecter à Workspace via un navigateur, l'utilisateur est invité à travailler hors connexion ou à réessayer de se connecter. Pour accéder aux applications et bureaux disponibles hors connexion, les utilisateurs cliquent sur **Utiliser Workspace hors ligne**.



Si une panne empêche les utilisateurs de se connecter à Workspace après avoir accédé à l'URL de Workspace, la fenêtre apparaît après un intervalle de délai spécifié. Par défaut, la fenêtre apparaît 30 secondes après que l'utilisateur ait accédé à l'URL de Workspace. Vous pouvez définir cette valeur sur 15, 30, 45 ou 60 secondes. Vous pouvez également désactiver le délai d'expiration de la connexion. Si le délai d'expiration de la connexion est désactivé, la fenêtre invitant les utilisateurs à travailler hors connexion apparaît lorsque l'utilisateur accède à l'URL de Workspace.

Pour configurer le paramètre de délai d'expiration de la connexion, cliquez sur l'icône de l'extension dans le navigateur de la machine utilisateur. Utilisez la fenêtre qui apparaît pour activer ou désactiver le délai d'expiration de la connexion et définir la durée du délai d'expiration :



Une panne peut empêcher l'utilisateur de se connecter si le navigateur a été redirigé vers un site d'authentification de fournisseur d'identité tiers. Dans ce cas, l'utilisateur peut saisir l'URL de Workspace dans le navigateur, ce qui provoque l'apparition de la fenêtre invitant les utilisateurs à travailler hors connexion. L'utilisateur n'a pas besoin d'attendre le délai d'expiration de la connexion avant que la fenêtre apparaisse.

Les utilisateurs peuvent également accéder aux applications et aux bureaux disponibles lors d'une panne de cette façon :

1. Cliquez sur l'icône de l'extension dans le navigateur.
2. Dans la fenêtre qui apparaît, cliquez sur le bouton sous **Travailler hors connexion**. Ce bouton indique **Aller à**, puis le nom de votre magasin Workspace.
3. Dans la fenêtre qui apparaît, cliquez sur **Utiliser Workspace hors ligne**.

Lors de certaines pannes, la fenêtre d'avertissement invitant les utilisateurs à travailler hors connexion s'affiche automatiquement lorsque l'extension détecte des problèmes du côté Workspace. L'utilisateur n'a pas besoin de prendre des mesures ou d'attendre le délai d'expiration de la connexion.

Limitations du navigateur

Si les utilisateurs effacent les cookies et autres données de site dans leur navigateur lors d'une panne, la continuité du service ne fonctionne pas tant qu'ils ne s'authentifient pas à nouveau auprès de Work-

space.

À moins que l'utilisateur n'autorise l'extension à fonctionner en mode de navigation privée, la continuité du service n'est pas prise en charge en mode de navigation privée.

Dépannage pour les utilisateurs du navigateur

Dans le menu **Avancé** des paramètres du navigateur associé à l'application Citrix Workspace, assurez-vous que la méthode actuelle de préférence de lancement de l'application et du bureau est définie sur **Utiliser l'application Citrix Workspace**. Si cette option est définie sur **Utiliser navigateur Web**, la continuité du service n'est pas prise en charge dans le navigateur.

Assurez-vous que l'icône de l'extension dans le navigateur apparaît en vert une fois que le navigateur charge l'URL de l'espace de travail.

Pour télécharger les journaux, cliquez sur l'icône de l'extension dans le navigateur. Cliquez ensuite sur **Télécharger les journaux**.

Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix

October 12, 2023

Service d'authentification fédérée (FAS) de Citrix pour permettre l'authentification unique auprès de DaaS dans Citrix Workspace. FAS est généralement l'option adoptée si l'un des fournisseurs d'identité suivants est utilisé pour l'authentification Citrix Workspace :

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

Avec FAS, les abonnés saisissent leurs informations d'identification une seule fois pour accéder à leurs applications et bureaux DaaS.

FAS n'est pas nécessaire pour l'authentification unique à DaaS si vous utilisez Active Directory (AD), AD + jeton ou des configurations spécifiques de Citrix Gateway. Pour plus d'informations sur la configuration de Citrix Gateway, consultez Créer une stratégie IdP OAuth sur Citrix Gateway local.

Serveurs FAS

Dans chaque emplacement de ressources, vous pouvez connecter plusieurs serveurs FAS à Citrix Cloud à des fins d'équilibrage de charge et de basculement.

Citrix Cloud prend en charge l'utilisation de serveurs FAS dans les scénarios suivants.

Dans les deux scénarios, les abonnés se connectant à leurs espaces de travail via un fournisseur d'identité fédéré ne saisissent leurs informations d'identification qu'une seule fois pour accéder aux applications et bureaux.

Serveurs FAS connectés à un seul emplacement de ressources

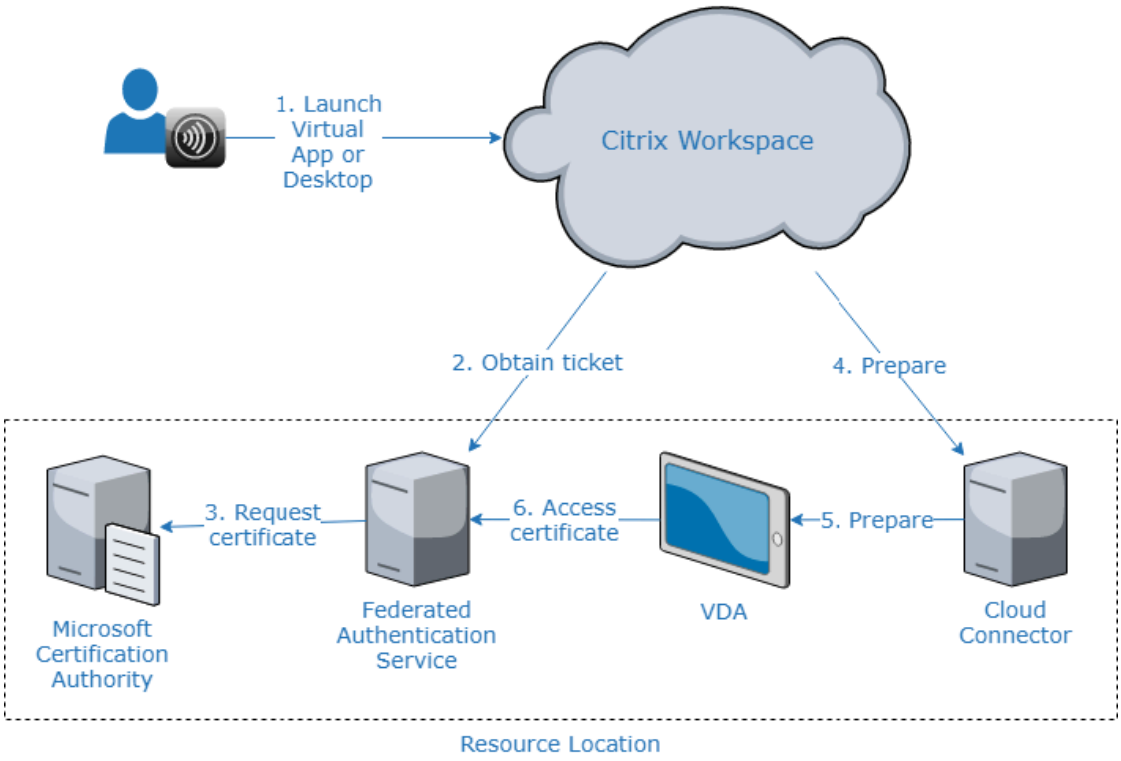
Si vos emplacements de ressources contiennent une infrastructure variée (par exemple, différents emplacements de ressources contiennent différentes forêts Active Directory), vous déployez des serveurs FAS vers l'emplacement de ressources où se trouvent vos VDA. L'authentification unique est active uniquement dans les emplacements de ressources où un ou plusieurs serveurs FAS sont connectés.

Serveurs FAS connectés à plusieurs emplacements de ressources

Si vous disposez d'une connectivité réseau entre vos emplacements de ressources et qu'ils contiennent une infrastructure similaire, vous pouvez connecter vos serveurs FAS à plusieurs emplacements de ressources. L'authentification unique est active pour les abonnés de l'espace de travail qui se connectent à des applications et des bureaux situés dans ces emplacements de ressources. Dans ce scénario, il n'est pas nécessaire de connecter des serveurs FAS distincts à chaque emplacement de ressources.

Lorsque les abonnés lancent une application ou un bureau virtuel, Citrix Cloud sélectionne un serveur FAS dans le même emplacement de ressources que l'application ou le bureau en cours de lancement. Citrix Cloud contacte le serveur FAS sélectionné pour obtenir un ticket qui accorde l'accès à un certificat utilisateur stocké sur le serveur FAS. Pour authentifier l'abonné, le VDA se connecte au serveur FAS et présente le ticket.

Vous pouvez utiliser le même serveur FAS pour l'authentification locale et Citrix Cloud à l'aide d'une configuration de règle appropriée.



Priorité de basculement pour plusieurs emplacements de ressources

Lors de l'utilisation de serveurs FAS avec plusieurs emplacements de ressources, les serveurs FAS d'un emplacement de ressources peuvent fournir un basculement vers des serveurs FAS situés dans d'autres emplacements de ressources. Lorsque vous ajoutez des serveurs FAS à d'autres emplacements de ressources, vous désignez chaque serveur comme serveur principal ou secondaire. Lorsque les abonnés lancent une application ou un bureau virtuel, Citrix Cloud utilise cette désignation de la manière suivante pour sélectionner un serveur FAS :

- Les serveurs FAS désignés comme serveurs principaux dans l'emplacement de ressources donné sont pris en compte en premier lieu.
- Si aucun serveur principal n'est disponible, les serveurs FAS désignés comme serveurs secondaires sont pris en compte.
- Si aucun serveur secondaire n'est disponible, le lancement se poursuit, mais l'authentification unique ne se produit pas.

Présentation vidéo

Pour obtenir une vue d'ensemble du Service d'authentification fédérée pour Citrix Workspace, visionnez la vidéo Tech Insight :

Exigences

Exigences en matière de connectivité

Utilisez la console d'administration FAS pour connecter un serveur FAS à Citrix Cloud. Vous pouvez utiliser cette console pour configurer un serveur FAS local ou distant. Pour activer l'authentification unique pour les espaces de travail avec FAS, la console d'administration FAS et le service FAS accèdent aux adresses suivantes à l'aide du compte de compte de l'utilisateur de la console et du compte de service réseau, respectivement.

- Console d'administration FAS avec utilisation du compte de l'utilisateur de la console :
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Adresses requises par un fournisseur d'identité tiers, si elles sont utilisées dans votre environnement
- Service FAS avec utilisation du compte de service réseau :
  - `*.citrixworkspacesapi.net`


```
- https://*.citrixnetworkapi.net/
```

Si votre environnement inclut des serveurs proxy, configurez le proxy utilisateur avec les adresses de la console d'administration FAS. Assurez-vous également que l'adresse du compte de service réseau est configurée en fonction de votre environnement.

Configuration système requise pour FAS

La configuration système décrite dans cette section s'appliquent à tous les serveurs FAS que vous prévoyez de connecter à Citrix Cloud.

Pour connaître la configuration système complète requise pour le serveur FAS, consultez la section Configuration système requise dans la documentation produit de FAS.

Le Service d'authentification fédérée 2003 (version 10.1) ou version ultérieure doit être installé sur les serveurs FAS de votre environnement Citrix Virtual Apps and Desktops local.

Si votre serveur FAS existant est plus ancien que la version 10, vous pouvez télécharger le dernier logiciel FAS à partir de Citrix et mettre à niveau le serveur avant de créer cette connexion. Lorsque vous créez la connexion, vous sélectionnez l'emplacement de ressources dans lequel vous souhaitez que votre serveur FAS réside. L'authentification unique est active pour les abonnés uniquement dans les emplacements de ressources où les serveurs FAS sont présents.

Pour plus d'informations sur la mise à niveau d'un serveur FAS existant, consultez Installer et configurer dans la documentation produit de FAS. Le même serveur FAS peut être utilisé pour les déploiements Workspace et locaux.

Citrix Workspace

Vous devez avoir provisionné et activé Citrix DaaS dans Workspace. Par défaut, DaaS est activé dans Configuration de l'espace de travail une fois que vous êtes abonné au service. Toutefois, le service nécessite que vous déployiez des Citrix Cloud Connector pour permettre à Citrix Cloud de communiquer avec votre environnement local.

Cloud Connector

Citrix Cloud Connector permet la communication entre votre emplacement de ressources (où résident les VDA) et Citrix Cloud. Déployez au moins deux Cloud Connector pour garantir une haute disponibilité. Les serveurs sur lesquels vous installez le logiciel Cloud Connector doivent répondre aux exigences suivantes :

- Exigences système décrites dans Détails techniques sur Cloud Connector.

- Aucun autre composant Citrix ne doit être installé sur ces serveurs ; ils ne doivent pas être un contrôleur de domaine Active Directory ou une machine critique à votre infrastructure d'emplacement de ressources.
- Les serveurs doivent être associés au domaine sur lequel résident vos VDA.

Pour plus d'informations sur le déploiement de Cloud Connector, reportez-vous aux articles suivants :

- Configuration du pare-feu et du proxy d'un Cloud Connector
- Installation de Cloud Connector

Présentation de la configuration

1. Si vous déployez de nouveaux serveurs FAS, consultez la section Exigences et suivez les instructions décrites dans la section Installer et configurer FAS de cet article.
2. Connectez votre serveur FAS à Citrix Cloud comme décrit dans la section Connecter un serveur FAS à Citrix Cloud dans cet article. L'exécution de cette tâche permet de connecter votre serveur FAS à un seul emplacement de ressources.
3. Si vous envisagez de connecter votre serveur FAS à plusieurs emplacements de ressources, suivez les instructions de la section Ajouter un serveur FAS à plusieurs emplacements de ressources dans cet article.

Installer et configurer FAS

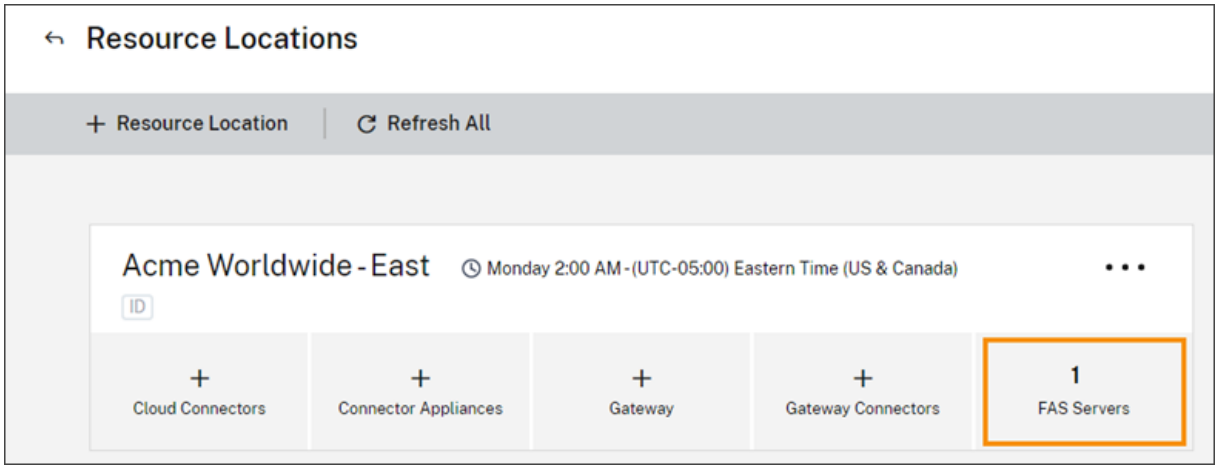
Suivez le processus d'installation et de configuration FAS décrit dans la documentation du produit FAS. Les étapes de configuration pour StoreFront ou le Delivery Controller ne sont pas requises.

> **Conseil :**
>
> Vous pouvez également télécharger le programme d'installation du Service d'authentification fédérée à partir de la console Citrix Cloud :
>
> 1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
> 2. Sélectionnez la vignette **Serveurs FAS**, puis cliquez sur **Télécharger**.

Connecter les serveurs FAS à Citrix Cloud

Utilisez la console d'administration FAS pour connecter votre serveur FAS à Citrix Cloud, comme décrit dans la section Installer et configurer de la documentation du produit FAS.

Une fois l'étape de configuration **Se connecter à Citrix Cloud** effectuée, Citrix Cloud enregistre le serveur FAS et l'affiche sur la page Emplacements des ressources de votre compte Citrix Cloud.



Si la page Emplacements des ressources est déjà chargée dans votre navigateur, actualisez-la pour afficher le serveur FAS enregistré.

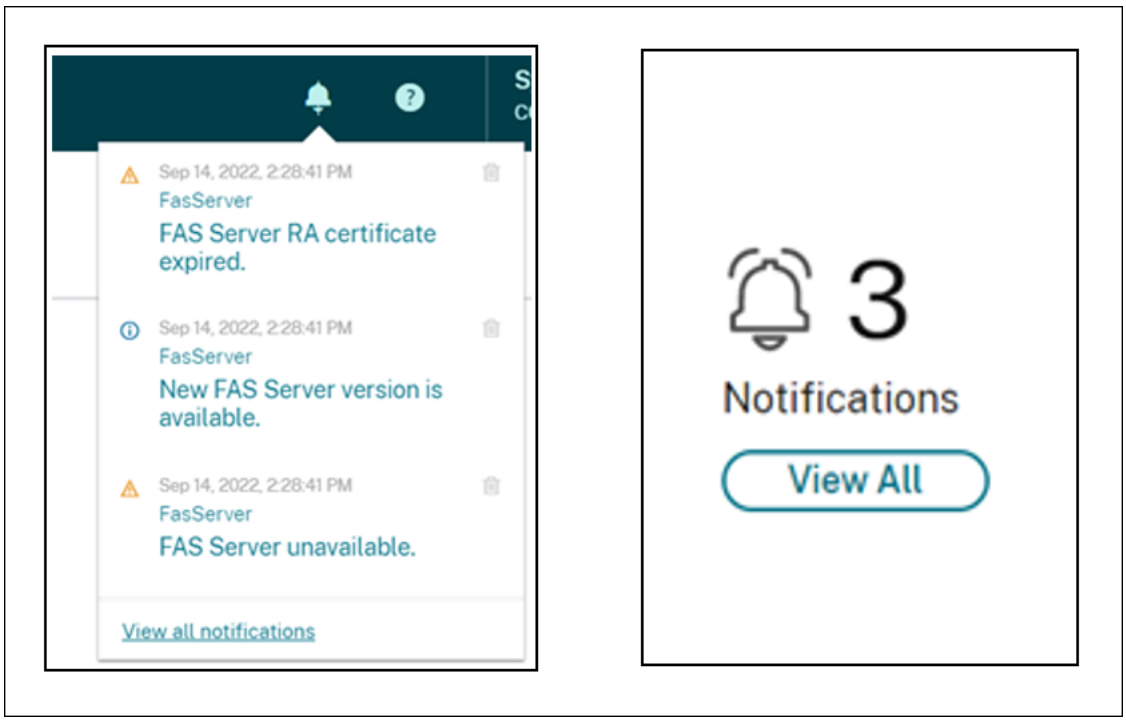
Prise en charge des notifications du cloud

FAS prend désormais en charge les notifications cloud. Avec les nouvelles notifications cloud pour les serveurs FAS, vous recevez des notifications dans les cas suivants :

- Un serveur FAS est en panne ou n'est pas disponible.
- Le certificat d'autorité d'inscription (RA) d'un serveur FAS a expiré ou est sur le point d'expirer.
- Une nouvelle version de FAS est disponible en téléchargement.

Déclenchement de notifications

Une vérification périodique des nouvelles notifications est effectuée et déclenchée dans la console de gestion Citrix Cloud. Les notifications apparaissent sous l'icône en forme de cloche dans le coin supérieur droit de la console de gestion Citrix Cloud. Sélectionnez **Tout afficher** sur l'icône de notification pour afficher toutes les notifications. Pour de plus amples informations, consultez la section Notifications.

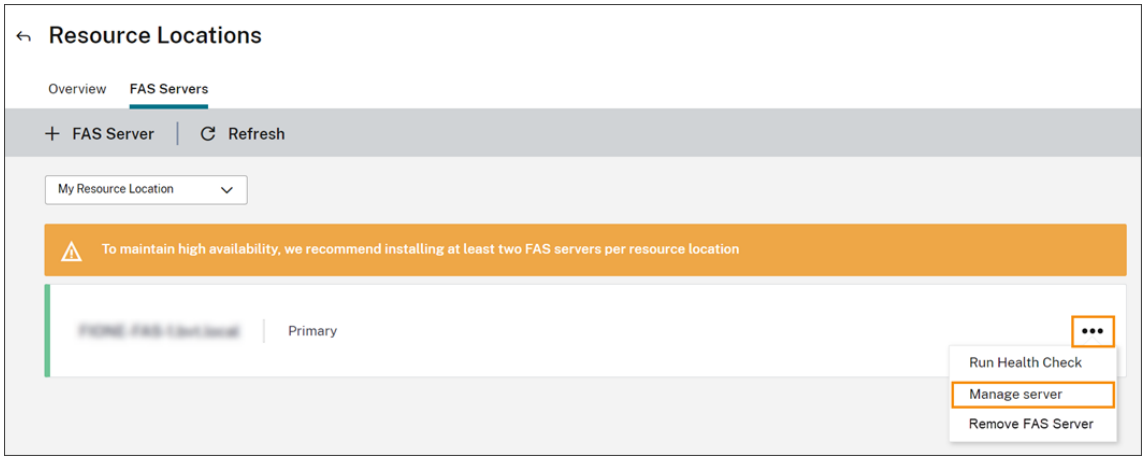


> **Remarque :**
>
> Lorsqu'une notification est émise, elle sera à nouveau émise périodiquement uniquement si le problème n'est pas résolu.

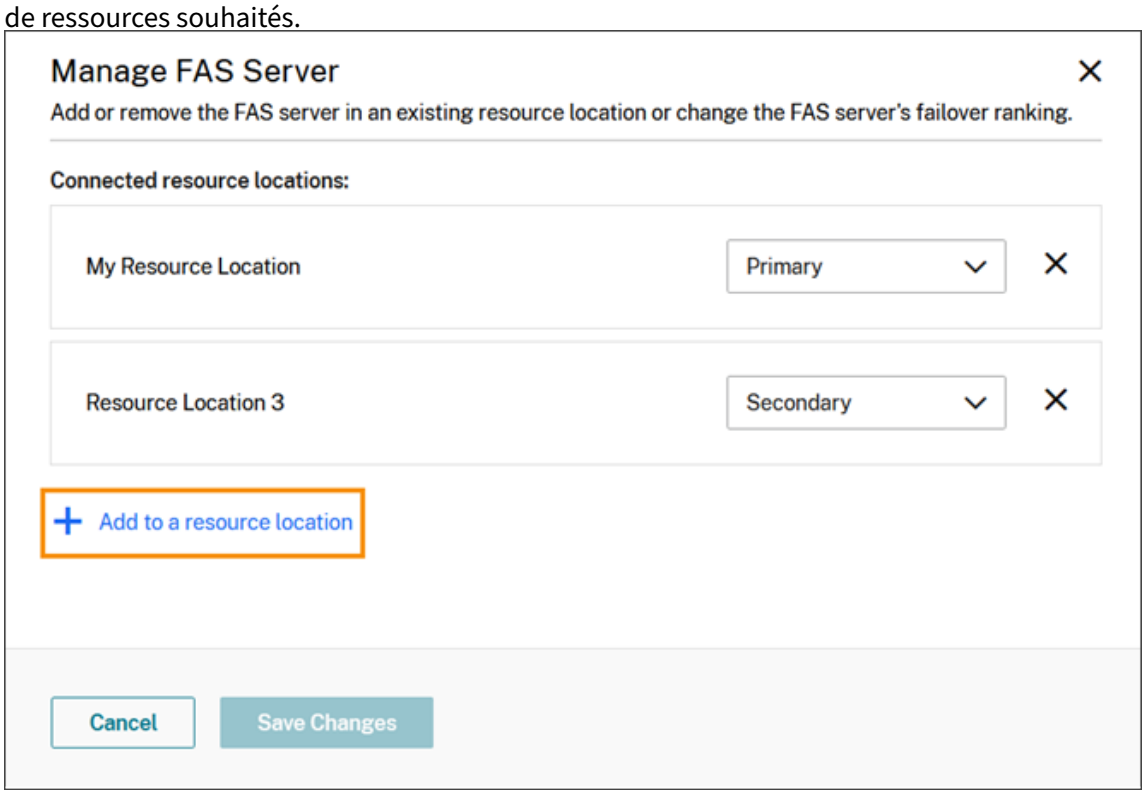
Toutes les notifications contiennent le nom de domaine complet du serveur FAS impacté. La notification d'expiration du certificat RA s'affiche uniquement pour les serveurs FAS dotés de la version 10.10.0.14 ou d'une version ultérieure.

Ajouter un serveur FAS à plusieurs emplacements de ressources

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**, puis l'onglet **Serveurs FAS**.
2. Localisez le serveur FAS que vous souhaitez gérer, cliquez sur les points de suspension (…) situés à droite de l'entrée, puis sélectionnez **Gérer le serveur**.



3. Sélectionnez **Ajouter à un emplacement de ressources**, puis sélectionnez les emplacements de ressources souhaités.

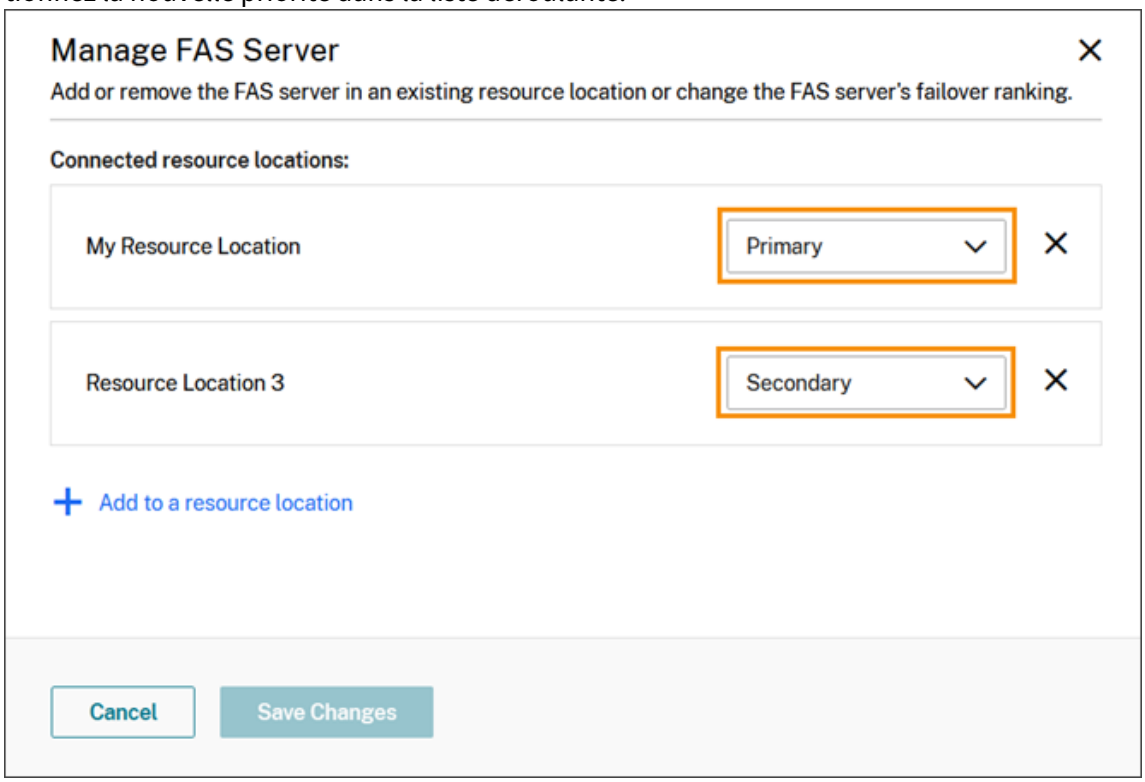


4. Sélectionnez **Principal** ou **Secondaire** pour spécifier la priorité de basculement du serveur FAS dans chaque emplacement de ressources sélectionné.
5. Sélectionnez **Enregistrer les modifications**.

Pour afficher le serveur FAS ajouté, sélectionnez **Emplacements des ressources** dans le menu **Citrix Cloud**, puis sélectionnez l'onglet **Serveurs FAS**. La liste de tous les serveurs FAS pour tous les emplacements de ressources connectés s'affiche. Pour afficher les serveurs FAS associés à un emplacement de ressources spécifique, sélectionnez l'emplacement de ressources dans la liste déroulante.

Modifier la priorité de basculement d'un serveur FAS

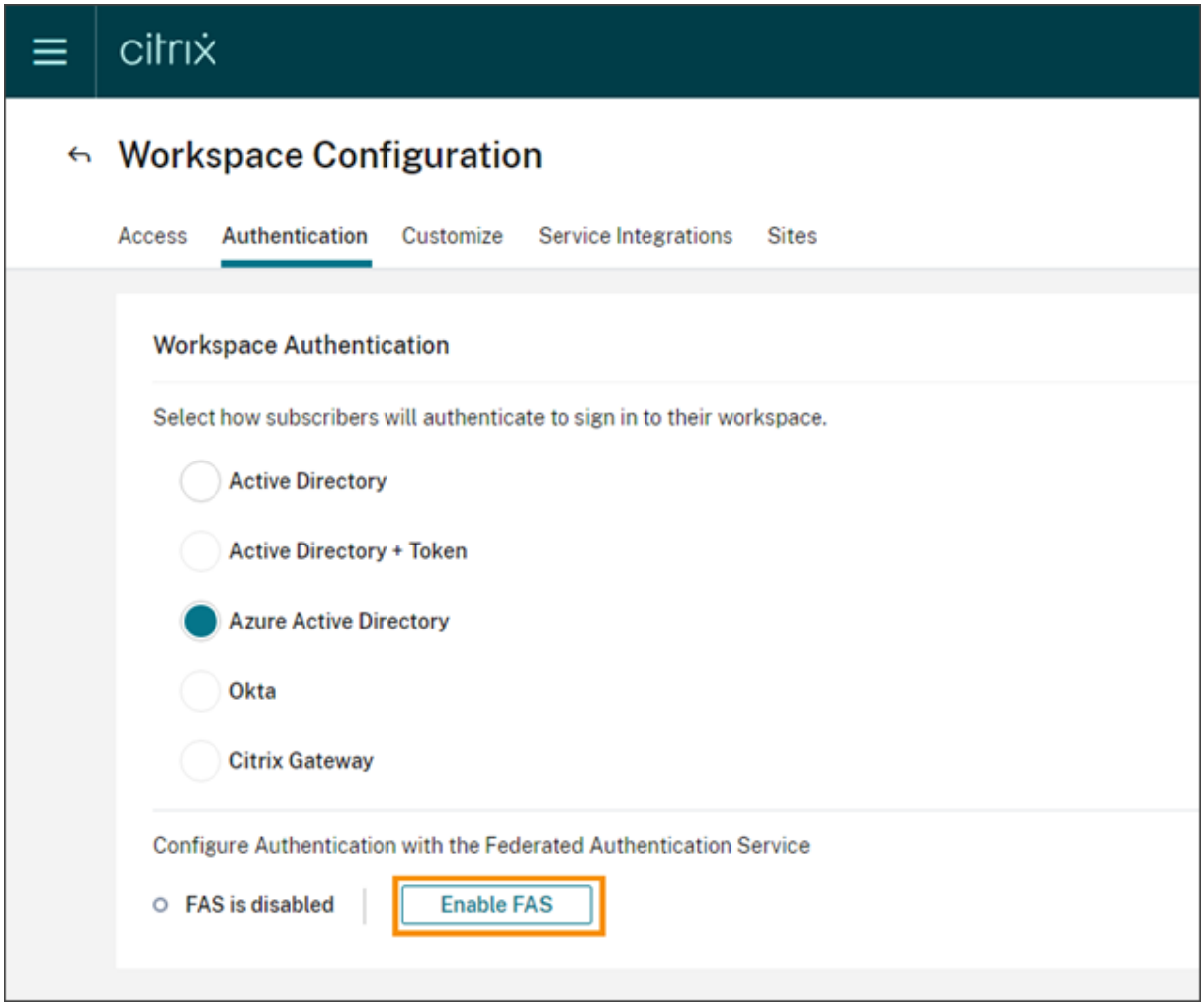
1. Sur la page **Emplacements des ressources**, sélectionnez la vignette **Serveurs FAS** pour l'emplacement de ressources que vous souhaitez gérer.
2. Sélectionnez l'onglet **Serveurs FAS** .
3. Localisez le serveur FAS que vous souhaitez gérer, cliquez sur les points de suspension situés à droite de l'entrée, puis sélectionnez **Gérer le serveur**.
4. Localisez l'emplacement de ressources avec la priorité que vous souhaitez modifier et sélectionnez la nouvelle priorité dans la liste déroulante.



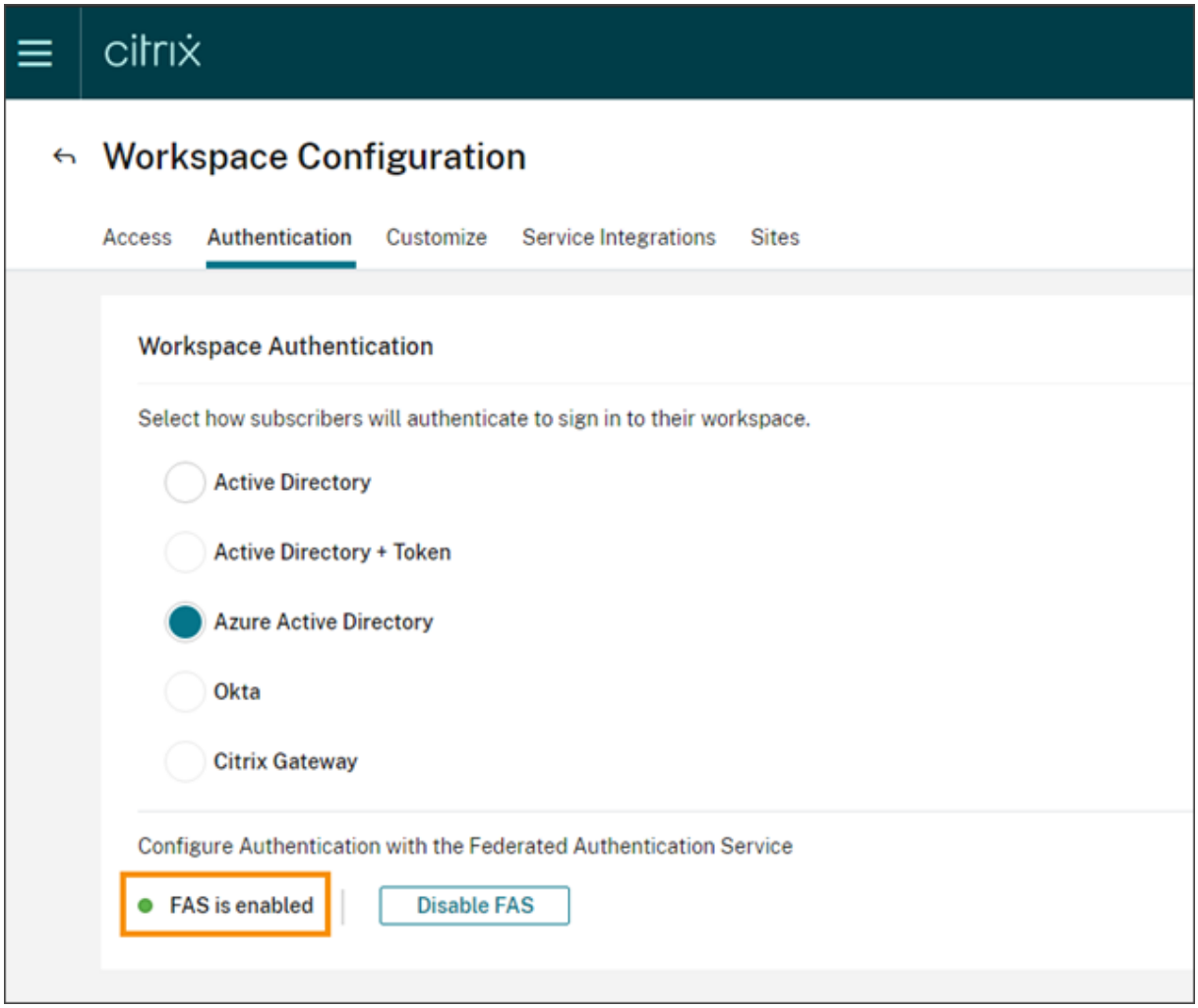
5. Sélectionnez **Enregistrer les modifications**.

Activer l'authentification fédérée pour les espaces de travail

1. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**, puis sélectionnez **Authentification**.
2. Cliquez sur **Activer FAS**. Cette modification peut prendre jusqu'à cinq minutes pour être appliquée aux sessions des abonnés.



Ensuite, le Service d'authentification fédérée est actif pour tous les lancements d'applications et de bureaux virtuels à partir de Citrix Workspace.



Lorsque les abonnés se connectent à leur espace de travail et lancent une application ou un bureau virtuel dans le même emplacement de ressources que le serveur FAS, l'application ou le bureau démarre sans demander d'informations d'identification.

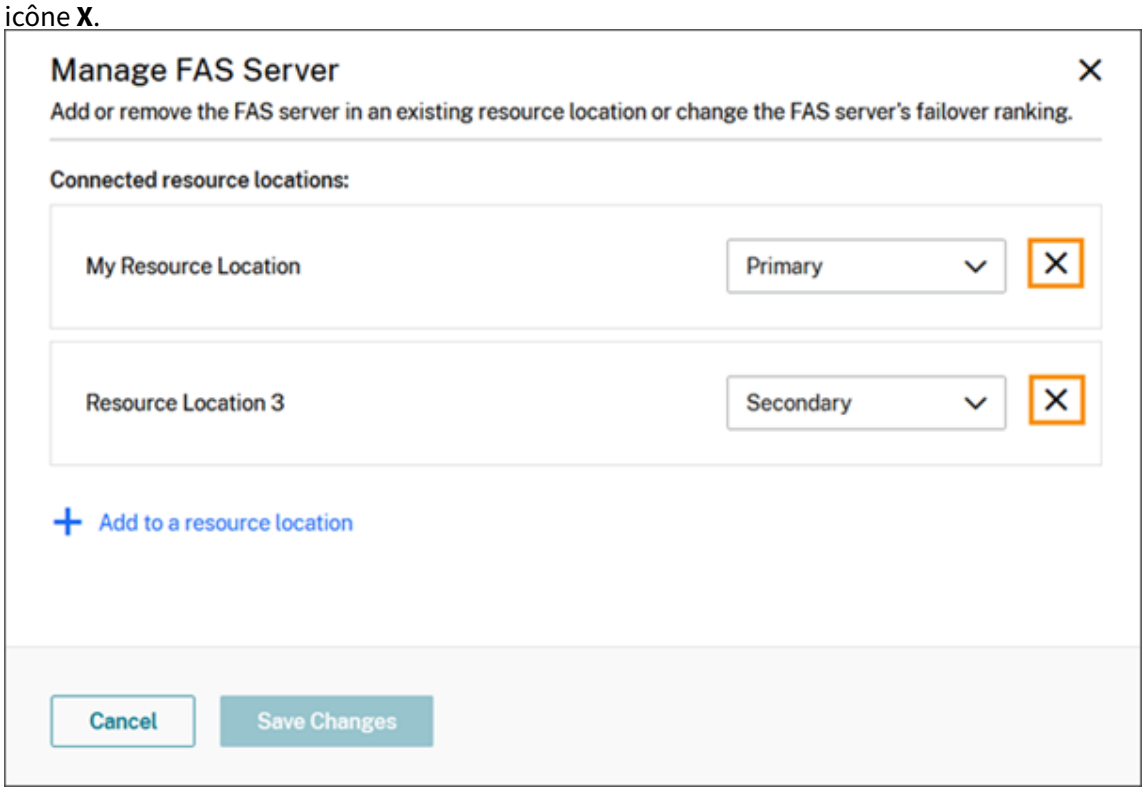
> **Remarque :**
>
> Si tous les serveurs FAS d'un emplacement de ressources sont en panne ou en mode de maintenance, le lancement de l'application réussit, mais l'authentification unique n'est pas active. Les abonnés sont invités à fournir leurs informations d'identification AD pour accéder à chaque application ou bureau.

Supprimer un serveur FAS

Pour supprimer un serveur FAS d'un emplacement de ressources unique :

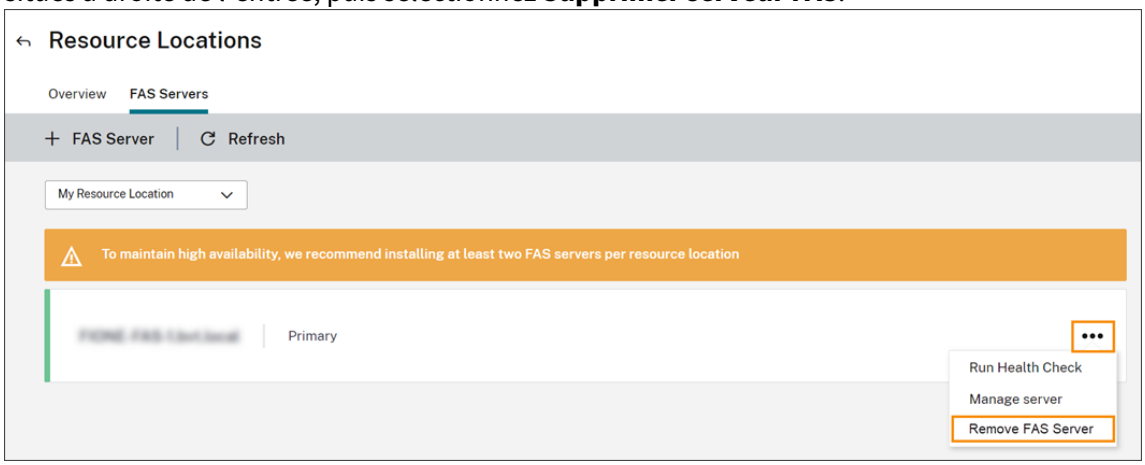
1. Sur la page **Emplacements des ressources**, sélectionnez la vignette **Serveurs FAS** pour l'emplacement de ressources que vous souhaitez gérer.

2. Sélectionnez l'onglet **Serveurs FAS** .
3. Localisez le serveur FAS que vous souhaitez gérer, cliquez sur les points de suspension situés à droite de l'entrée, puis sélectionnez **Gérer le serveur**.
4. Recherchez l'emplacement de ressources que vous souhaitez supprimer, puis cliquez sur l'icône **X**.

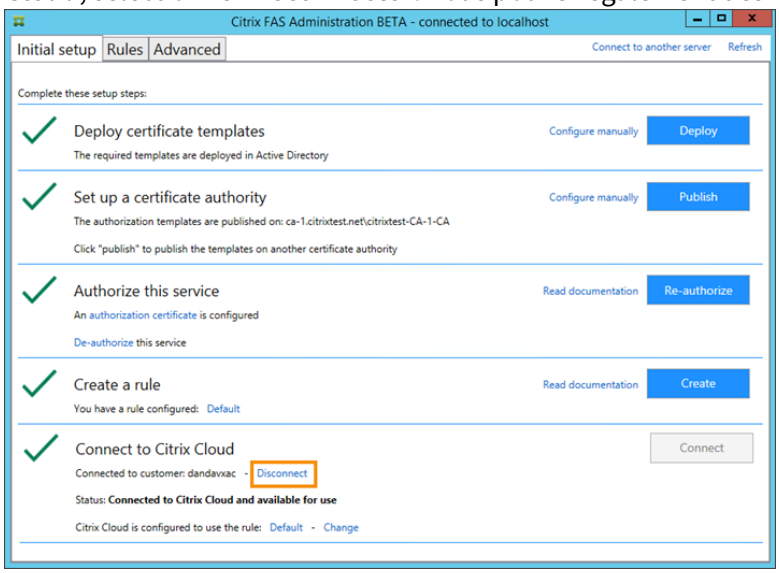


Pour supprimer un serveur FAS de tous les emplacements de ressources connectés :

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
2. Recherchez l'emplacement des ressources à gérer, puis sélectionnez la vignette **Serveurs FAS**.
3. Localisez le serveur FAS que vous souhaitez supprimer, cliquez sur les points de suspension situés à droite de l'entrée, puis sélectionnez **Supprimer serveur FAS**.

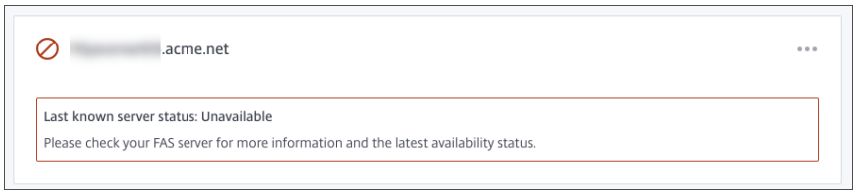


4. Sur la console d'administration FAS (sur votre serveur FAS local), dans **Se connecter à Citrix Cloud**, sélectionnez **Déconnecter**. Vous pouvez également désinstaller FAS.

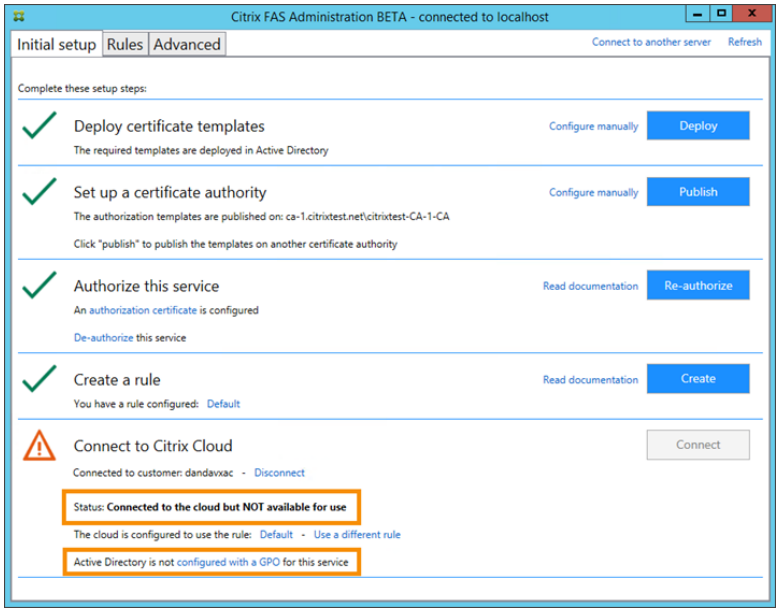


Dépannage

Si le serveur FAS n'est pas disponible, un message d'avertissement s'affiche sur la page Serveurs FAS.



Pour établir un diagnostic du problème, ouvrez la console d'administration FAS sur votre serveur FAS local et inspectez l'état. Par exemple, ici, le serveur FAS n'est pas présent dans l'objet de stratégie de groupe du serveur FAS :



Si la console d'administration FAS indique que le serveur fonctionne correctement, mais qu'il existe toujours des problèmes d'ouverture de session VDA, consultez le guide de dépannage FAS.

Informations supplémentaires

Configuration de Single Sign-On sur l'application Workspace