



Citrix Workspace

Contents

Citrix Workspace の概要	3
新機能	6
Workspace プラットフォームの新機能	7
Workspace ユーザーインターフェイス (UI) の新機能	14
Global App Configuration Service の新機能	30
Citrix Workspace の利用を開始する	35
Citrix Workspace を準備する	39
新しいワークスペースユーザーインターフェイス	45
アクティビティマネージャー	55
Citrix Workspace を使用して DaaS と Virtual Apps and Desktops を配信する	60
ワークスペースへのアクセスを構成する	63
カスタムドメインの構成	72
セキュアなワークスペース	91
サービスをワークスペースに統合する	100
Citrix Workspace アプリの構成	102
クラウドストアの設定の構成	109
オンプレミスストアの設定の構成	112
テストチャネルの構成	116
ワークスペース環境の管理	120
ワークスペースの外観をカスタマイズする	125
ワークスペース操作をカスタマイズする	131
セキュリティとプライバシーポリシーをカスタマイズする	141
Citrix Workspace での DaaS の最適化	152

オンプレミスの Virtual Apps and Desktops をワークスペースに集約	153
直接ワークロード接続でワークスペースへの接続を最適化	163
サービス継続性	173
Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化	197

Citrix Workspace の概要

November 28, 2023

Citrix Workspace は、場所とデバイスを選ばず、アプリ、デスクトップ、およびコンテンツ（リソース）へのセキュアで統合されたアクセスを可能にする、デジタルワークスペースソリューションです。これらのリソースには、Citrix DaaS、コンテンツアプリ、ローカルアプリとモバイルアプリ、SaaS アプリと Web アプリ、ブラウザアプリなどがあります。

Citrix Workspace の仕組み

Citrix Workspace は、[Citrix Cloud サービス](#)を集約および統合し、1つの[リソースの場所](#)で、エンドユーザー（利用者）が利用できるすべてのリソースへの統一されたアクセスを可能にします。Citrix Workspace のエンドユーザーは、利用者と呼ばれます。従業員は自分のワークスペースからサービスを「利用」するよう設定されるためです。

Citrix Workspace を介して利用できるサービスの概要については、「[Citrix Workspace を介したクラウドでホストされるサービス](#)」を参照してください。

利用者は、Citrix Workspace ユーザーインターフェイス（UI）内のこれらのサービスで利用できる各リソースを、統一された完全なビューで表示できます。Citrix Workspace UI の利用者エクスペリエンスについて詳しくは、「[ワークスペース環境の管理](#)」を参照してください。

利用者は、管理者が [ワークスペース構成] で構成して有効にしたサービスに、Workspace URL を入力したブラウザ、または Citrix Receiver に代わる[Citrix Workspace アプリ](#)を使用して、アクセスします。ユーザーがワークスペースにアクセスする方法については詳しくは、「[ワークスペースアクセス](#)」を参照してください。

利用者は、プライマリ ID プロバイダーを使用して各自のワークスペースに認証します。ID プロバイダーは [ID およびアクセス管理] で構成してから [ワークスペース構成] で有効にします。利用者は、Citrix Workspace 用に購入したクラウドホストの各サービスに対して自動的に認証されます。これにより、セキュリティが向上し、使いやすくなります。Workspace 認証の構成について詳しくは、「[セキュアなワークスペース](#)」を参照してください。

開始の概要

Citrix Workspace は、**Citrix Cloud** コンソールでセットアップします。このコンソールには、[ID およびアクセス管理] 管理画面と、[ワークスペース構成] という Citrix Workspace 管理インターフェイスがあります。Citrix Workspace の使用を開始するには、次のタスクを実行します。

1. **Citrix Cloud** コンソールで Citrix Workspace を実装する設定にしてあることを確認します。コンソールで以下を実行します：
 - クラウドベースのサービスにオンボードする。
 - 展開チームを編成する。

- インフラストラクチャとリソースを構成する。
2. 以下に対し、[ID およびアクセス管理] で ID プロバイダーとアカウントを設定します：
- Citrix Cloud 管理者。
 - Citrix Workspace 利用者。
3. 以下を含め、[ワークスペース構成] でワークスペースを構成します：
- 外部アクセスと内部アクセス。
 - Citrix Cloud コンソールで構成したサービスをワークスペースに統合する。
 - サインイン後のワークスペースの外観と利用者エクスペリエンスをカスタマイズする。

この基本設定に加えて、その他のセキュリティ、プライバシー、および最適化のオプションを選択できます。最も一般的なものは次のとおりです：

- [Citrix フェデレーション認証サービス \(FAS\)](#) を使用した、Citrix Workspace での DaaS へのシングルサインオン (SSO) を構成する。通常、FAS は、Okta や Azure Active Directory などのフェデレーション認証方法を使用している場合に採用されます。

タスクの概要と、展開を進めるときに必要な情報については、「[Citrix Workspace の利用を開始する](#)」を参照してください。各手順では、Citrix Cloud コンソールを使用した ID プロバイダーの構成やサービスの有効化などのタスクに関する指示を記載しています。このチュートリアルでは、展開チームを編成してインフラストラクチャとリソースを構成するのに必要となる技術情報にすばやくアクセスできるようになっています。

Citrix Workspace を介したクラウドでホストされるサービス

利用者は、Citrix Workspace を使用して、クラウドでホストされるサービスが提供するリソースにアクセスできます。Citrix Cloud の既存顧客は、これらのサービスを Citrix Workspace ソリューションに組み込むことで、完全なデジタルワークスペースエクスペリエンスに移行できます。

このセクションでは、使用権に応じて Citrix Workspace で有効にできる主なクラウドホストサービスについて説明します。購入したサービスへのアクセスを構成および有効化する方法については、「[Citrix Workspace の利用を開始する](#)」を参照してください。Citrix Workspace の各エディションおよびその機能に関する説明については、「[Citrix Workspace の機能マトリックス](#)」を参照してください。

Citrix DaaS

Citrix Workspace は、Citrix DaaS へのマルチテナントのクラウドホストアクセスポイントです。Citrix DaaS をセットアップするには、「[Citrix DaaS](#)」に記載されている手順に従います。

オンプレミスの Virtual Apps and Desktops をご利用の場合、Citrix Workspace を介してリソースにアクセスするためのさまざまなオプションがあります。選択するオプションは、クラウドに完全に移行するか、ハイブリッドソリューションを採用するか、および外部アクセスを許可するかどうかによって異なります。これらのオプションについて詳しくは、「[Citrix Workspace を使用して DaaS を配信する](#)」を参照してください。

SaaS アプリおよび Web アプリ、**Citrix Secure Private Access** サービスで保護

Citrix Secure Private Access (以前の **Secure Workspace Access** および **Access Control Service**) は、Workspace に統合されている Web アプリおよび SaaS アプリへのシングルサインオン (SSO) を提供します。また、このサービスでは、アクセス権限を管理し、利用者の資格情報に基づいてエンタープライズホストの Web アプリに適切なレベルのアクセスを認可するポリシーを制御できます。

Citrix Secure Private Access サービスのメリットについて詳しくは、「[技術概要: Secure Private Access](#)」を参照してください。

Citrix Gateway サービス

Citrix Gateway サービス (以前の **NetScaler Gateway Service**) は、Citrix によって管理される完全にクラウドでホストされる環境用に、**Citrix Secure Private Access** とともに使用されます。

Citrix Gateway サービスは、高度なポリシーインフラストラクチャに基づいてワークスペースへの外部接続を提供することにより、SaaS アプリと Virtual Apps and Desktops に統一されたエクスペリエンスを提供します。

手順に従って [Citrix Gateway サービス](#) をセットアップし、Workspace URL をテストして利用者と共有し、利用者のリモートアクセスを可能にします。Citrix Gateway サービスで SaaS アプリを構成する方法については、「[Support for Software as a Service Apps](#)」を参照してください。

Citrix Remote Browser Isolation サービス

Citrix Remote Browser Isolation サービスをワークスペースに統合し、Web 閲覧アクティビティを分離して、ブラウザーベースの攻撃から企業のネットワークを保護します。利用者が Workspace URL に移動すると、他の Citrix Cloud サービスで構成されているアプリやデスクトップとともに、公開 Web ブラウザーが表示されます。

利用者にリモート分離ブラウザーへのアクセス権を付与するには、[Remote Browser Isolation](#) をセットアップしてから、テストして Workspace URL を利用者と共有します。

Citrix Endpoint Management

Citrix Endpoint Management を使用すると、ID、デバイス、アプリ、データ、およびネットワークに対するセキュリティ保護が厳重な状態で、デバイスとアプリのポリシーを管理できます。Citrix Workspace との統合は、新規顧客か既存顧客かで異なります。Citrix Workspace との Endpoint Management の統合については、「[Citrix Workspace 環境との統合](#)」を参照してください。

Citrix Analytics

Citrix Analytics サービスは、すべての Citrix Workspace 利用者に関する分析情報を収集して提供します。使用権に応じて、さまざまな Citrix Analytics オファリングを利用できます。さまざまなオファリングとは、**Citrix**

Analytics for Security、**Citrix Analytics for Performance**、および **Citrix Analytics (Usage)** のこと
です。これらのサービスについて詳しくは、「[Citrix Analytics](#)」を参照してください。

新機能

November 28, 2023

Citrix は、Citrix Workspace をご使用のお客様に、新機能と更新情報をいち早くお届けするよう取り組んでいます。
最初のリリースは、Citrix 内部サイトのみ適用され、その後徐々に顧客環境に適用されます。

クラウドの規模とサービスの可用性に関するサービスレベルアグリーメントについては、Citrix Cloud の [サー
ビスレベルアグリーメント](#) を参照してください。サービスの中断および定期メンテナンスを監視するには、[Service
Health Dashboard](#) を参照してください。

Citrix Workspace の新機能

Citrix Workspace の機能強化とアップデートに関する最新情報を入手して、テクノロジーの可能性を最大限に活用
してください。Citrix Workspace からのタイムリーなアップデートを組み込むことで、ユーザーの生産性を最大化
し、対話の品質を向上させます。

- [Workspace プラットフォームの新機能](#)
- [Workspace ユーザーインターフェイスの新機能](#)
- [Global App Configuration Service の新機能](#)

さまざまなプラットフォーム上の Citrix Workspace アプリ

次のリンクを使用して、お気に入りのプラットフォームに対する **Citrix Workspace** アプリの新機能と拡張機能の
詳細を確認してください。

- [Android](#)
- [ChromeOS](#)
- [HTML5](#)
- [iOS](#)
- [Linux](#)
- [Mac](#)
- [Microsoft Teams](#)
- [Windows](#)
- [Windows ストア](#)

また、[Citrix Enterprise Browser](#) の新機能もご覧ください。

Workspace プラットフォームの新機能

November 28, 2023

Citrix は、Citrix Workspace をご使用のお客様に、新機能と更新情報をいち早くお届けするよう取り組んでいます。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。

このプロセスは、わかりやすいものになっています。最初の更新は、Citrix 内部サイトのみにも適用され、その後徐々に顧客環境に適用されます。段階的に更新することによって、製品の品質と可用性を最大化しています。

クラウドの規模とサービスの可用性に関するサービスレベルアグリーメントについては、Citrix Cloud の [サービスレベルアグリーメント](#) を参照してください。サービスの中断および定期メンテナンスを監視するには、[Service Health Dashboard](#) を参照してください。

2023 年 11 月

カスタムドメインの構成 - 一般提供

カスタムドメイン機能が一般提供されるようになりました。ワークスペースのカスタムドメインを構成すると、選択したドメインを使用して Citrix Workspace ストアにアクセスできるようになります。これにより、割り当てられた cloud.com ドメインの代わりにこのドメインを使用して、Web ブラウザーと Citrix Workspace アプリケーションの両方からアクセスできるようになります。詳細については、「[カスタムドメインの構成](#)」を参照してください。

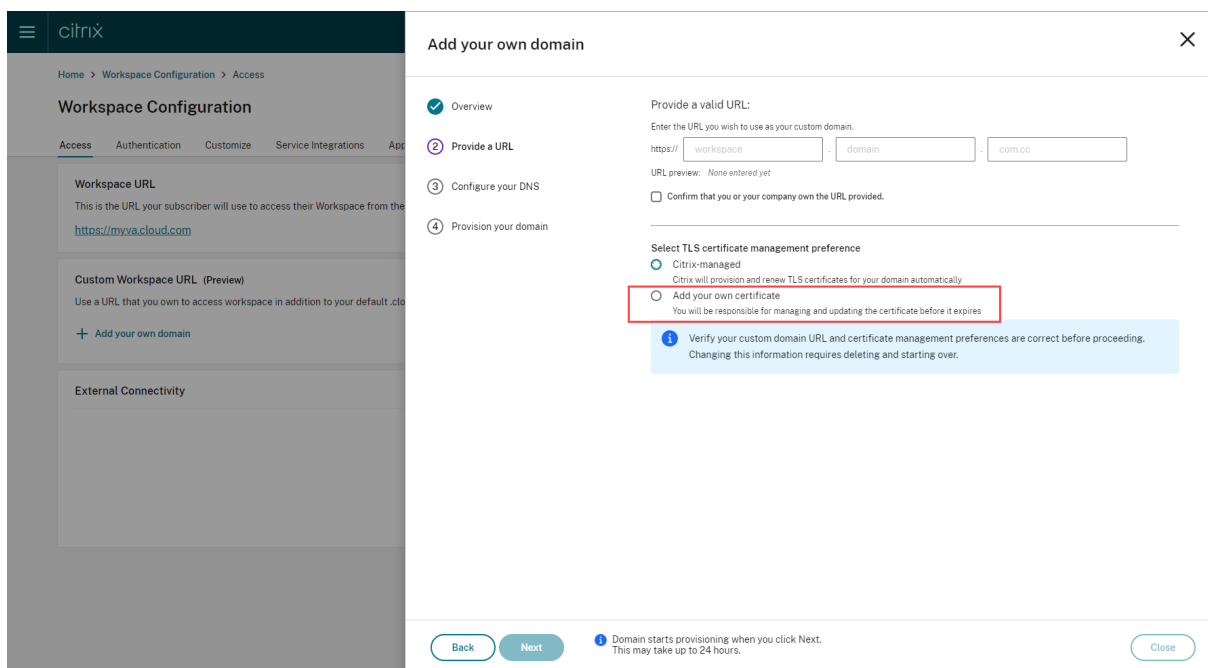
2023 年 8 月

カスタムドメインの独自の TLS 証明書を追加する (プレビュー)

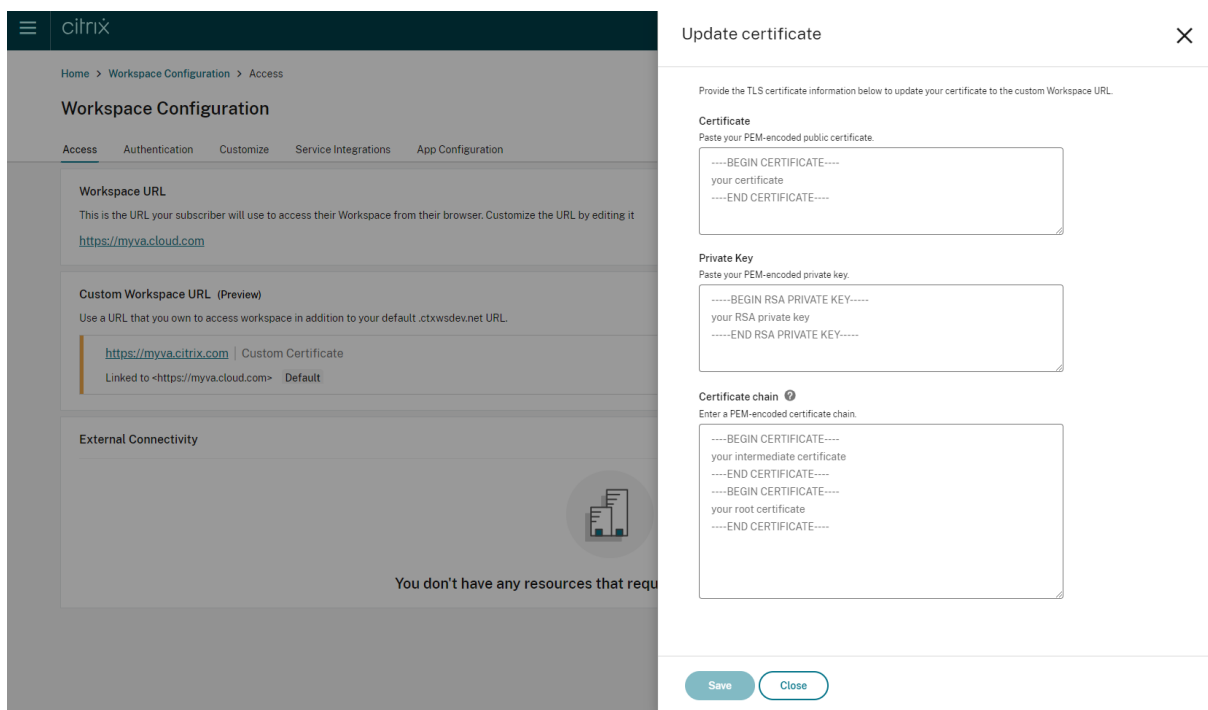
カスタム Workspace URL を構成する際に、認証用に独自の TLS 証明書をアップロードできるようになりました。証明書をアップロードする前に、証明書が次の条件を満たしていることを確認してください。

- PEM でエンコードされている必要があります。
- 少なくとも今後 30 日間有効である必要があります。
- これはカスタム Workspace URL にのみ使用する必要があります、ワイルドカード証明書は受け入れられません。
- 証明書の共通名はカスタムドメインと一致する必要があります。
- 証明書上の SAN はカスタムドメイン用であり、追加の SAN は許可されません。
- 証明書の有効期間は 10 年を超えてはなりません。

証明書を追加するには、[URL を指定する] ページに移動し、[TLS 証明書の管理設定を選択する] の下にある [独自の証明書を追加する] オプションを選択します。



その後、[独自の証明書を追加する] ページで証明書を追加できます。



詳細については、「[カスタムドメインの追加](#)」を参照してください。

注:

添付のPodioフォームを使用して、このプレビュー機能に対するフィードバックを送信できます。

2023 年 5 月

カスタムドメイン（プレビュー）の構成ワークスペースのカスタムドメインを構成すると、選択したドメインを使用して Citrix Workspace ストアにアクセスできるようになります。これにより、割り当てられた cloud.com ドメインの代わりにこのドメインを使用して、Web ブラウザーと Citrix Workspace アプリケーションの両方からアクセスできるようになります。詳細については、「[カスタムドメイン（プレビュー）の構成](#)」を参照してください。

2023 年 3 月

追加の非アクティブタイムアウト設定。Workspace アプリのデスクトップユーザーとモバイルユーザーの両方に対して、追加の非アクティブタイムアウト設定を有効にできるようになりました。詳しくは、「[セキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。

2022 年 12 月

カスタム通知の送信に関する追加の構成オプション:。[**Send custom announcement**] を構成するときに、ページを上部または下部に配置するかを設定できるようになりました。詳しくは、「[セキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。

繁体字中国語のサポート。Citrix Workspace が繁体字中国語で利用できるようになりました。

2022 年 10 月

韓国語のサポート。Citrix Workspace が韓国語で利用できるようになりました。

Citrix Workspace アプリ設定のカスタマイズのサポート。管理者は、Global App Configuration Service を使用して、iOS、Android、HTML5、Mac、Windows プラットフォーム向け Citrix Workspace アプリの設定を構成できるようになりました。

2022 年 8 月

Workspace 起動エクスペリエンスの向上。ユーザーが Web またはブラウザーで自分のワークスペースを起動する場合、起動状態を示す通知がトリガーされます。起動中にユーザーがブラウザーを閉じようとする、確認が求められ、セッション起動が進行中であることが通知されます。詳しくは、「[Citrix Workspace の利用を開始する](#)」を参照してください。

2022 年 6 月

Safari でのサービス継続性のサポート。Citrix Workspace Web 拡張機能は、Web ブラウザーでアプリやデスクトップにアクセスするユーザーにサービス継続性を提供します。詳しくは、「[ブラウザーのサービス継続性](#)」を参照し

てください。

2022年5月

フェデレーション ID プロバイダーの新しい構成オプション：フェデレーション ID プロバイダーを有効または無効にして、Workspace にログインするときに利用者に対して認証を求めるプロンプトを表示できるようにします。詳しくは、「[ワークスペース操作をカスタマイズする](#)」を参照してください。

Workspace アプリの再認証期間（一般提供）：再認証期間により、利用者は Workspace にアクセスするたびにサインインを求められることなく、Workspace にサインインした状態を維持できます。Workspace アプリでサインインする際、利用者はサインインしたままにすることに同意します。利用者は、アプリとデスクトップを使用している限り、再認証期間中はサインインしたままになります。この機能について詳しくは、「[Citrix Workspace アプリの再認証期間を設定する](#)」を参照してください。

iOS のサービス継続性のサポート：一般提供の iOS 向け Citrix Workspace アプリで、サービス継続性がサポートされるようになりました。詳しくは、「[サービス継続性](#)」を参照してください。

サービス継続性の新しいエラーコード：失敗したサービス継続性接続のトラブルシューティングに役立つ新しいエラーコードを使用できるようになりました。詳しくは、「[サービス継続性](#)」を参照してください。

2022年3月

Android および **iOS** でのサービス継続性のサポート：一般提供の Android 向け Citrix Workspace アプリおよび Technical Preview の iOS 向け Citrix Workspace アプリで、サービス継続性がサポートされるようになりました。詳しくは、「[サービス継続性](#)」を参照してください。

2022年2月

Android 向け **Citrix Workspace** アプリ（一般提供）および **iOS** 向け **Citrix Workspace** アプリ（**Technical Preview**）によるサービス継続性のサポート：サービス継続性により、ユーザーは停止中でも仮想アプリやデスクトップに接続できます。一般提供の Android 向け Citrix Workspace アプリおよび Technical Preview の iOS 向け Citrix Workspace アプリで、サービス継続性がサポートされるようになりました。詳しくは、「[サービス継続性](#)」を参照してください。

カスタム通知とカスタムサインインポリシー：すべてのお客様が2つの新機能を利用できるようになりました。これらの機能により、ワークスペース管理者は Citrix Workspace アプリで独自のログイン後の固定バナーや、ログイン前のカスタムメッセージ、またはライセンス契約を表示できます。詳しくは、「[セキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。

2021年12月

Citrix Content Collaboration の従業員とクライアントユーザーのデフォルトの分割サインイン画面を削除します: Citrix Workspace で、クライアントユーザーと従業員ユーザーの両者に対してシングルサインインフローを有効にすることができました。詳しくは、「[統一されたユーザーサインインフローを作成する](#)」を参照してください。

Mac 向け Citrix Workspace アプリを使用したブラウザのサービス継続性のサポート: Citrix Workspace Web 拡張機能は、Web ブラウザーでアプリやデスクトップにアクセスするユーザーにサービス継続性を提供します。この機能は、Mac 向け Citrix Workspace アプリを実行しているデバイスでサポートされるようになりました。詳しくは、「[サービス継続性](#)」を参照してください。

2021年11月

ポリシー駆動型テーマ: Workspace テーマを作成して優先順位を付け、[ワークスペース構成] のさまざまなユーザーグループに各テーマを追加できます。詳しくは、「[ワークスペースの外観をカスタマイズする](#)」を参照してください。

2021年10月

電子署名の言語サポート: 電子署名で、日本語、ドイツ語、フランス語、スペイン語、オランダ語、簡体字中国語に加えて、イタリア語、ブラジルポルトガル語がサポートされるようになりました。詳しくは、「[RightSignature 多言語サポート](#)」を参照してください。

複数のリソースの場所の **FAS** サポート (一般公開): Citrix Workspace では、複数のリソースの場所にまたがる仮想アプリおよび仮想デスクトップへのシングルサインオンの提供がサポートされています。また、1つのリソースの場所にある FAS サーバーをプライマリまたはセカンダリとして指定して、他のリソースの場所にある FAS サーバーにフェイルオーバーを提供できます。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

2021年9月

Citrix Workspace に導入された **HTML5** 向け **Citrix Workspace** アプリ: HTML5 向け Citrix Workspace アプリは、デバイスにインストールしなくても、ブラウザで Citrix Workspace と同じ操作を実行できます。新機能など、HTML5 向け Citrix Workspace アプリについて詳しくは、[HTML5 向け Citrix Workspace アプリ](#)の製品ドキュメントを参照してください。

Web ブラウザーのサービス継続性のサポート (一般公開): Citrix Workspace Web 拡張機能は、Web ブラウザーでアプリやデスクトップにアクセスするユーザーにサービス継続性を提供します。この機能は、Windows デバイスでの Google Chrome および Microsoft Edge 用です。詳しくは、「[ブラウザのサービス継続性](#)」を参照してください。

2021年7月

カスタムの利用者ライセンス契約ポリシー：利用者に対してカスタムの使用契約ポリシーを提示し、Workspace にサインインする前に読んで同意するように求めることができます。この機能について詳しくは、「[サインインポリシーの構成](#)」を参照してください。

Workspace アプリの再認証期間（プレビュー）：再認証期間により、利用者は Workspace にアクセスするたびにサインインを求められることなく、Workspace にサインインした状態を維持できます。Workspace アプリでサインインする際、利用者はサインインしたままにすることに同意します。利用者は、アプリとデスクトップを使用している限り、再認証期間中はサインインしたままになります。このプレビュー段階の機能について詳しくは、「[Citrix Workspace アプリの再認証期間を設定する](#)」を参照してください。

Citrix Cloud を介したネットワークの場所の構成：Citrix が提供する PowerShell スクリプトの使用に加えて、Citrix Cloud 管理コンソールを介してネットワークの場所を構成できるようになりました。この機能について詳しくは、「[直接ワークロード接続を使用したワークスペースへの接続を最適化](#)」を参照してください。

2021年6月

複数のリソースの場所の **FAS** サポート（プレビュー）：Citrix Workspace では、複数のリソースの場所にまたがる仮想アプリおよび仮想デスクトップへのシングルサインオンの提供がサポートされています。1つのリソースの場所にある FAS サーバーをプライマリまたはセカンダリとして指定して、他のリソースの場所にある FAS サーバーにフェイルオーバーを提供できます。このプレビュー段階の機能について詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

Web ブラウザーのサービス継続性のサポート（**Technical Preview**）：Citrix Workspace Web 拡張機能は、Web ブラウザーでアプリやデスクトップにアクセスするユーザーにサービス継続性を提供します。この Technical Preview は、Windows デバイスでの Google Chrome および Microsoft Edge 用です。詳しくは、「[ブラウザーのサービス継続性](#)」を参照してください。

サービス継続性（一般公開）：サービス継続性により、Citrix Cloud コンポーネントまたはパブリッククラウドやプライベートクラウドが停止しているときでも、ユーザーは仮想アプリと仮想デスクトップに接続できます。詳しくは、「[サービス継続性](#)」を参照してください。

Citrix RightSignature アプリが利用可能：Workspace Premium および Premium Plus に付属する電子署名ソリューションの Citrix アプリを使用して、Citrix Workspace を介して任意のデバイス上のドキュメントに電子署名を要求できます。詳しくは、「[Citrix RightSignature アプリの構成](#)」を参照してください。

2021年5月

カスタムテーマ（**Technical Preview**）：利用者向けの Workspace の外観のカスタマイズで、さまざまなユーザーグループに割り当てられるカスタムテーマがサポートされるようになりました。テーマを作成、カスタマイズ、および優先順位付けして、それらのユーザーグループの利用者が、サインインしたときに適切なワークスペーステーマを表示できるようにします。詳しくは、「[ワークスペースの外観をカスタマイズする](#)」を参照してください。

電子署名の言語サポート: 電子署名機能で、日本語、ドイツ語、フランス語、スペイン語、オランダ語、簡体字中国語がサポートされるようになりました。詳しくは、「[RightSignature 多言語サポート](#)」を参照してください。

2021年2月

アカウントパスワードの変更: 利用者は、Citrix Workspace 内からドメインパスワードを変更できます。管理者は、組織のパスワードポリシーに従って有効で複雑なパスワードを作成できるように、利用者にガイダンスを提供することもできます。詳しくは、「[利用者がアカウントのパスワードを変更できるようにする](#)」を参照してください。

2020年12月

サービス継続性 **Technical Preview**: サービス継続性により、Citrix Cloud コンポーネントまたはパブリッククラウドやプライベートクラウドが停止しているときでも、ユーザーは Citrix DaaS に接続できます。詳しくは、「[サービス継続性](#)」を参照してください。

2020年10月

FedRAMP Ready: Citrix Cloud Government に展開する場合、Citrix Workspace は FedRAMP Ready のステータスを取得しています。FedRAMP は、米国政府機関が使用するクラウドサービスのセキュリティ基準を促進するプログラムです。FedRAMP Ready のステータスを取得済みのクラウドサービスを必要とする米国政府機関が、Citrix Workspace および Citrix DaaS サービスを使用して DaaS を配信できるようになりました。詳しくは、「[Citrix Cloud Government](#)」を参照してください。

2020年5月

Citrix Workspace 導入ガイド: Citrix Workspace には、エンドユーザーにワークスペースをすばやく提供するための手順ごとのチュートリアルが含まれています。このチュートリアルでは、Citrix Cloud コンソールを使用して、ID プロバイダーの構成、管理者の追加、ワークスペースの認証とサービスの有効化を行うことができます。タスクの概要と必要な手順にすばやくアクセスするには、「[Citrix Workspace の利用を開始する](#)」を参照してください。

2019年12月

ネットワークの場所サービス: 企業ネットワーク内のワークスペースからアプリやデスクトップを起動するユーザーは、VDA に直接ルーティングされるようになります。これによってゲートウェイを省略できるため、よりすばやく DaaS セッションを起動できます。このサービスとセットアップ手順について詳しくは、「[ネットワークの場所サービスを使用したワークスペースへの接続の最適化](#)」を参照してください。

最近使用したアプリおよびお気に入りのアプリへのアクセスの向上: 最近使用したアプリやお気に入りのアプリは Workspace に最初に読み込まれるため、ユーザーはよく使用するアプリやデスクトップをすぐに起動できます。

Workspace ユーザーインターフェイス (UI) の新機能

November 28, 2023

以下のセクションでは、Workspace UI の新旧リリースの新機能について説明します。

注:

- 詳しくは、「[新しいワークスペースユーザーインターフェイス \(プレビュー\)](#)」を参照してください。
- アクティビティマネージャーについて詳しくは、「[アクティビティマネージャー \(プレビュー\)](#)」を参照してください。

23.46 の新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

既知の問題

新しい既知の問題はありません。

以前のリリース

このセクションでは、サポートされている以前のリリースでの新機能と解決された問題に関する情報を提供します。

23.45

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

- 内部 URL が Google の検索結果に表示されないように、Google 検索のインデックス付けは Citrix Web から削除されました。ただし、URL が既に Google によってインデックス化されている場合は、それらを削除する手順を実行する必要があります。詳しくは「[自身のサイトでホストしているページを Google から削除する](#)」を参照してください。

23.44

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.43

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.42

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.41

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

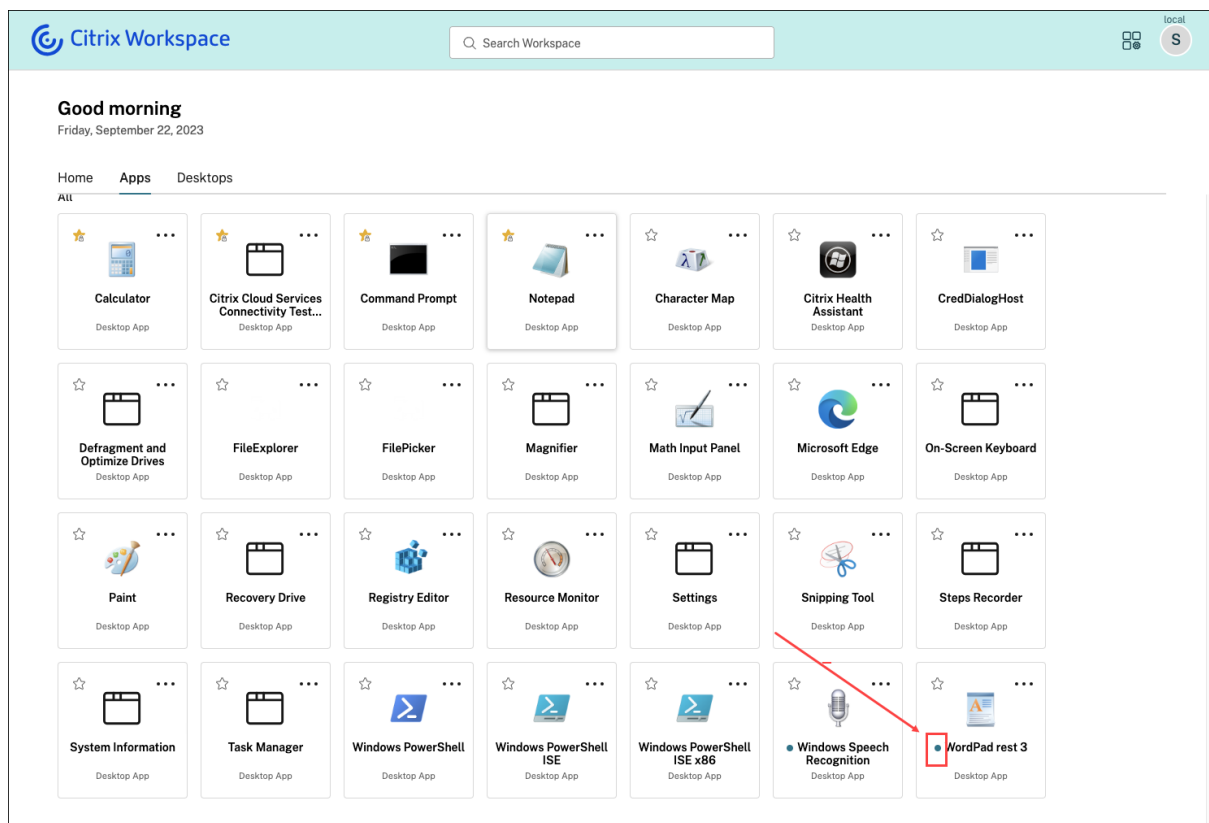
解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.40

新機能

新しいアプリの検出を効率化 エンドユーザーは新しく追加されたアプリを簡単に見つけられるようになり、最新のアプリの探索と利用が容易になります。管理者が新規アプリをエンドユーザーに配信すると、初回はエンドユーザーのワークスペースでそのアプリが強調表示され、アプリタイトルに緑色の点が表示されます。



解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.39

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.38

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.37

新機能

新しいワークスペース UI - 一般提供 新しいワークスペースユーザーインターフェイスの一般提供が開始されました。よりクリーンなビューのための最新の外観を備えた新しいユーザーインターフェイス機能が導入されています。ユーザーインターフェイスの機能強化は、Web、デスクトップ、モバイルに適用できます。管理者は、ワークスペースの [構成] > [カスタマイズ] > [機能] で、エンドユーザーに対してこれを有効にすることができます。詳しくは、「[新しいワークスペースユーザーインターフェイス \(プレビュー\)](#)」を参照してください。

注:

新しい UI トグルは、デフォルトでは今後 6 か月間無効にされた状態です (除く: 管理者が有効にした場合)。6 か月後、現在の UI エクスペリエンスは廃止され、新しい UI がデフォルトですべてのユーザーにとって有効になります。管理者は、今後 6 か月以内にユーザーを新しい UI に移行させる必要があります。

アクティビティマネージャー - 一般提供 クラウドの新しい UI におけるアクティビティマネージャー機能の一般提供が開始されました。アクティビティマネージャーは、ユーザーがリソースを効果的に管理できるようにする、シンプルかつ強力な機能です。この機能により、アクティブおよび切断状態にあるアプリやデスクトップに対するあらゆるデバイスからの迅速なアクションが容易になるので、生産性が向上します。管理者は、ワークスペースの [構成] > [カスタマイズ] > [機能] > [アクティビティマネージャー] で、エンドユーザーに対してこの機能を有効にすることができます。詳しくは、「[アクティビティマネージャーを有効にする](#)」を参照してください。

アクティビティマネージャーを有効にすると、アクティブまたは切断状態にあるアプリとデスクトップが [アクティビティマネージャー] パネルに表示されます。エンドユーザーは、省略記号 (...) アイコンをクリックして迅速なアクションを実行できます。

アクティブなアプリとデスクトップに対して実行できるアクションは、次のとおりです。

- 切断: リモートセッションは切断されますが、アプリとデスクトップはバックグラウンドでアクティブになっています。
- ログアウト: 現在のセッションからログアウトされます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン: 切断されたデスクトップを閉じます。
- 強制終了: 技術的な問題が発生した場合、デスクトップの電源を強制的に切ります。
- 再起動: デスクトップをシャットダウンし、再度起動します。

また、アクティビティマネージャーにより、エンドユーザーが切断されたアプリやデスクトップを操作できるようになります。DDC を必ず最新バージョン (115) にアップグレードしてください。詳しくは、「[切断されたアプリとデスクトップ](#)」を参照してください。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

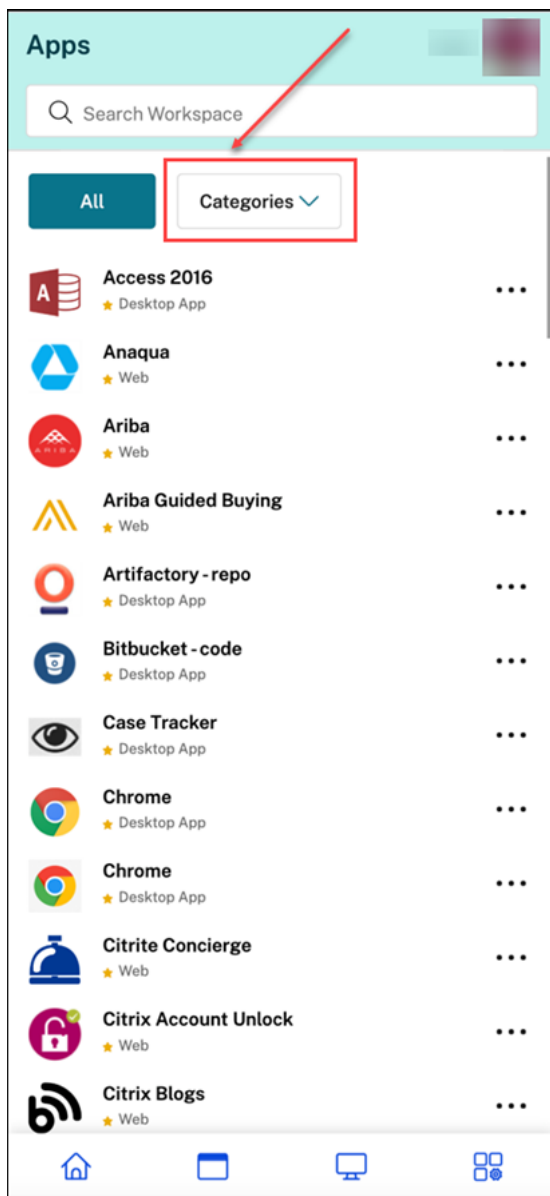
既知の問題

- [アクティビティマネージャー] パネルには、ユーザーが現在サインインしているすべてのストアにおけるアクティブなセッションが表示されます。
- ログアウト、切断などのアクティビティマネージャーの操作は、App Protection ポリシーが有効になっているアプリケーションではサポートされません。

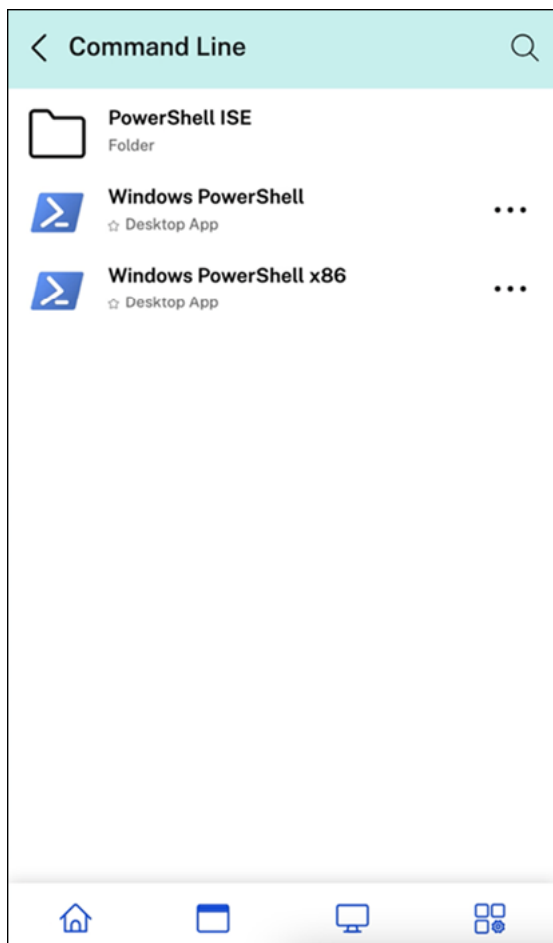
23.36

新機能

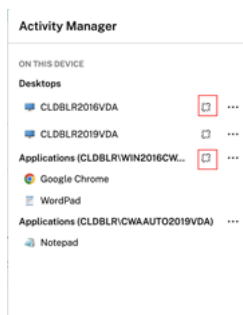
モバイルプラットフォームのアプリケーションのサブカテゴリを表示する エンドユーザーは、Android および iOS デバイス上でアプリをカテゴリやサブカテゴリに分類して表示できるようになるので、アプリに簡単にアクセスできるとともに、アプリを快適にブラウジングできるようになります。カテゴリを表示するには、[アプリ] タブに移動し、[カテゴリ] ボックスをクリックします。



関連するカテゴリを選択すると、管理者が行った構成に基づいて、存在するサブカテゴリとアプリケーションのリストが表示されます。サブカテゴリはフォルダーとして表示され、フォルダーにはさらに管理構成に応じてサブフォルダーまたはアプリケーションが含まれます。詳しくは、「[フォルダーパスの追加](#)」を参照してください

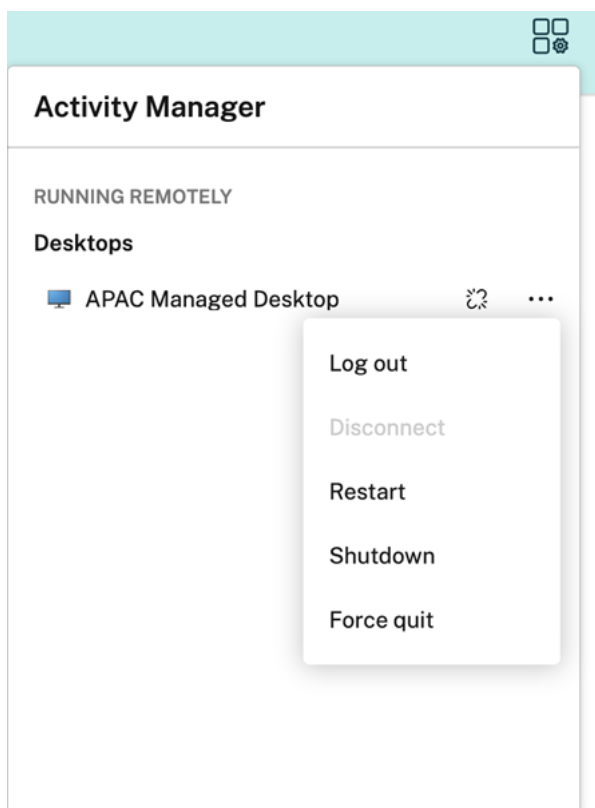


切断されたセッションを任意のデバイスからアクティビティマネージャーで管理する。アクティビティマネージャーにより、エンドユーザーはローカルまたはリモートにおいて切断モードで実行されているアプリとデスクトップを表示し、それらに対するアクションを実行できるようになりました。モバイルまたはデスクトップデバイスからセッションを管理できるため、エンドユーザーは外出先でもアクションを実行できます。切断されたセッションに対してログアウトやシャットダウンなどのアクションを実行すると、リソースの使用が最適化されるので、消費電力が削減されます。



- 切断されたアプリとデスクトップは [アクティビティマネージャー] パネルに表示され、切断状態を示すアイコンで示されます。

- 切断されたアプリはそれぞれのセッションの下にグループ化され、それらのセッションには切断状態を示すアイコンが表示されます。



エンドユーザーは、切断されたデスクトップに対し、[省略記号] をクリックすることで次のアクションを実行できます。

- ログアウト: これを使用すると、切断されたデスクトップからログアウトできます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン: このオプションを使用すると、切断されたデスクトップを閉じることができます。
- 電源オフ: 技術的な問題が発生した場合に、このオプションを使用すると、切断されたデスクトップの電源を強制的に切ることができます。
- 再起動: このオプションを使用すると、切断されたデスクトップをシャットダウンし、再度起動することができます。

詳しくは、「[アクティビティマネージャー \(プレビュー\)](#)」を参照してください。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.35

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.34

新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

解決された問題

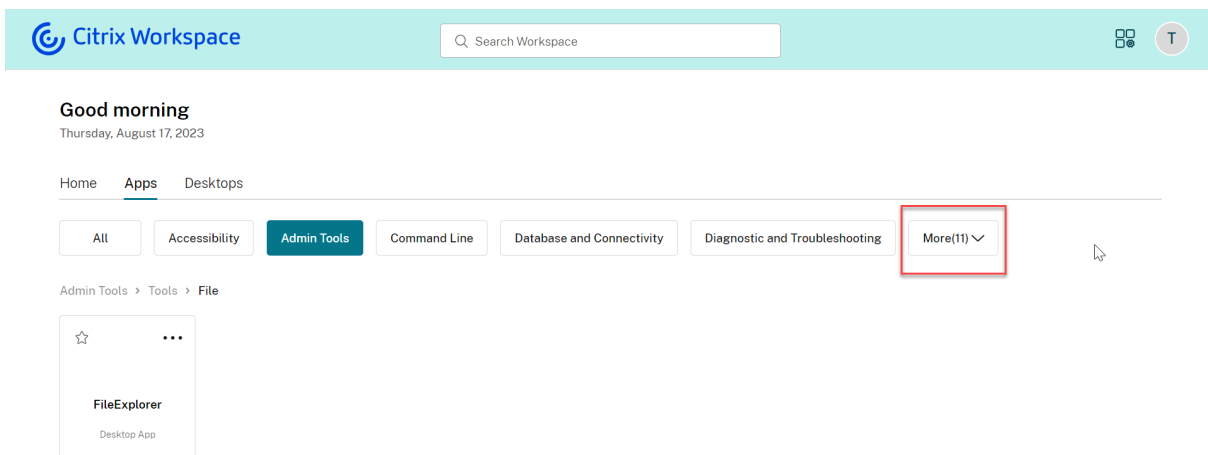
このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.33

新機能

アプリの分類によるユーザーエクスペリエンスの向上 エンドユーザーは、Workspace ユーザーインターフェイスでアプリケーションをカテゴリおよびサブカテゴリに分類して表示できます。分類に 3 つ以上のレベルが含まれる場合、エンドユーザーはアプリケーションがフォルダー構造内に配置されていることを確認できます。ナビゲーションのブレッドクラムがユーザーに表示されます。

管理者が作成したプライマリカテゴリの数がユーザーの画面上で利用可能なスペースを超えると、ユーザーインターフェイスは画面サイズに基づいて調整され、カテゴリを [その他] ドロップダウンの下に動的に移動します。



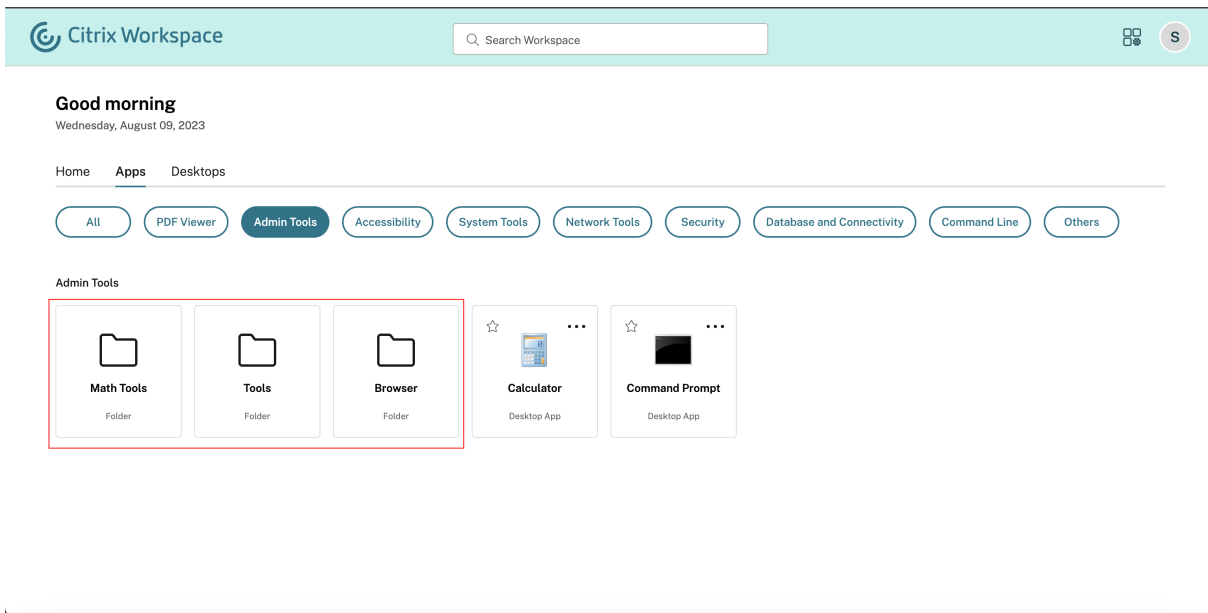
解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.32

新機能

アプリの分類により簡単にアクセス可能 管理者はアプリをカテゴリとサブカテゴリに分類して配信し、エンドユーザーはアプリを快適に閲覧できます。分類の 2 番目のレベルから、エンドユーザーにはフォルダー構造が表示されます。整理されたマルチレベル構造により、混乱のない、最適化されたエクスペリエンスが実現され、全体的なユーザー満足度の向上に役立ちます。フォルダーとサブフォルダーの作成の詳細については、「[デリバリーグループの作成](#)」を参照してください。



解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

23.31

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.30

新機能

アクティビティマネージャーの管理 管理者は、エンドユーザーに対してアクティビティマネージャー機能を有効または無効にできるようになりました。組織のポリシーに従って、全ユーザー、または選択したユーザーおよびユーザーグループに対してこの機能を有効にすることができます。有効にすると、アクティビティ マネージャー パネルを使用して、エンド ユーザーがアクティブなアプリとデスクトップを表示し、操作できるようになります。詳細については、「[アクティビティ マネージャー](#)」を参照してください。

注:

この機能は、仮想アプリとデスクトップでのみサポートされます。Web アプリや SaaS アプリには適用されません。

アクティビティマネージャーを有効にするには、以下の手順に従います:

1. 管理コンソールで、[ワークスペース構成] > [カスタマイズ] > [機能] に移動します。
2. アクティビティマネージャーセクションで、トグルをオンにしてアクティビティマネージャーを有効にします。
3. 次に、以下のようにアクセス権限をカスタマイズできます。
 - すべてのエンドユーザーに対してアクティビティマネージャーを有効にするには、[全ユーザーに対して有効にする] を選択します。

New Activity Manager

Enabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Save **Preview**

- 選択したユーザーおよびユーザーグループに対してアクティビティマネージャーを有効にするには、[選択したユーザーとユーザーグループに対して有効にする] を選択します。次に、ユーザーまたはユーザーグループが属するディレクトリを選択できます。適切なディレクトリを選択すると、関連するユーザーとユーザーグループを表示できます。

New Activity Manager

Enabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory Step 2: Select a user or group

cldblr.com Search users or user groups

Type	Display Name	Account Name ↑	
USER			🗑️
USER			🗑️

Save **Preview**

- すべてのユーザーに対してアクティビティマネージャーを無効にするには、トグルをオフにします。

New Activity Manager

Disabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory Step 2: Select a user or group

cldblr.com Search users or user groups

Type	Display Name	Account Name ↑	
USER			🗑️
USER			🗑️

Save **Preview**

4. [保存] をクリックします。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.29

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.28

新機能

Internet Explorer の廃止に関する情報 Citrix Workspace UI バージョン 23.26 は、2023 年の最終週まで Internet Explorer で利用できます。Citrix は、23.26 リリース以降、新機能、バグ修正、またはセキュリティパッチをサポートしません。さらに、管理者は、サポートされているブラウザおよびサポートされている LTSR (LTSR 2203 以降) にアップグレードするための通知を受け取ります。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.27

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

解決された問題

- この修正により、エラー境界およびコンポーネントレベルのエラー処理が実装されました。[WSUI-7423]
- 省略アイコンをクリックすると、オフラインバナーが最小化されます。[WSUI-7797]

23.26

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

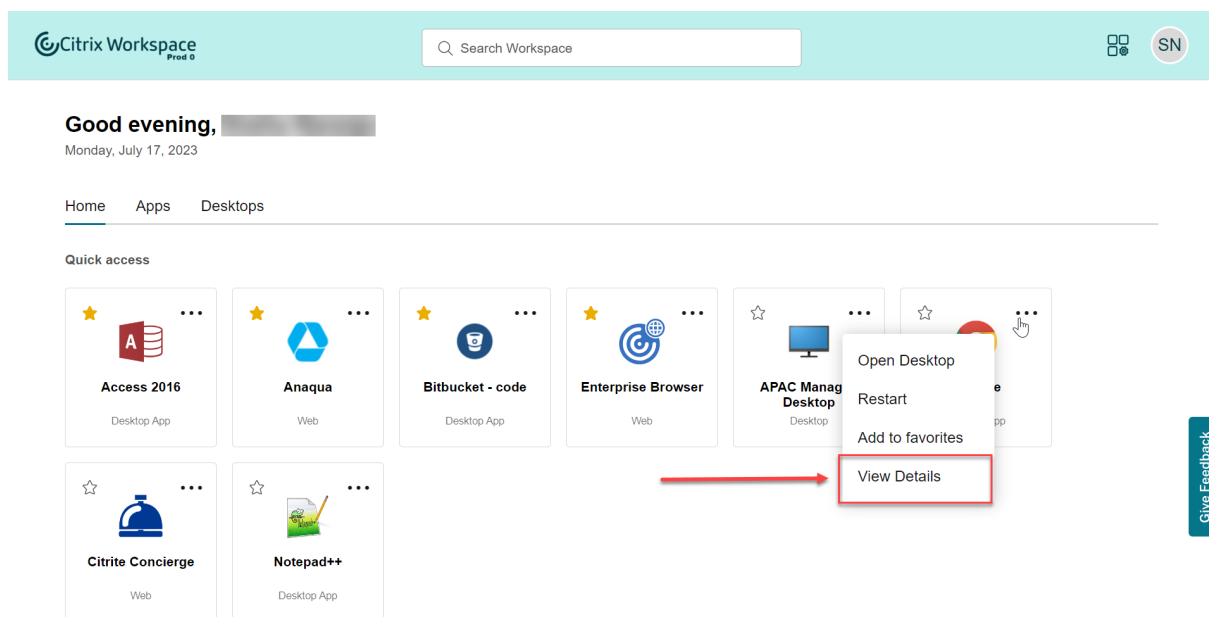
解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.25

新機能

アプリとデスクトップの説明を表示 エンドユーザーは、管理者によるアプリとデスクトップに関する説明を表示できるようになりました。こうした説明は、アプリまたはデスクトップの機能の目的を理解するのに役立ちます。これらは、同じ名前で構成、場所、環境などが異なる複数のアプリが存在する場合に特に便利です。アプリまたはデスクトップの説明を表示するには、それぞれのタイトルの省略記号をクリックし、[詳細の表示] をクリックします。



解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.24

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.23

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

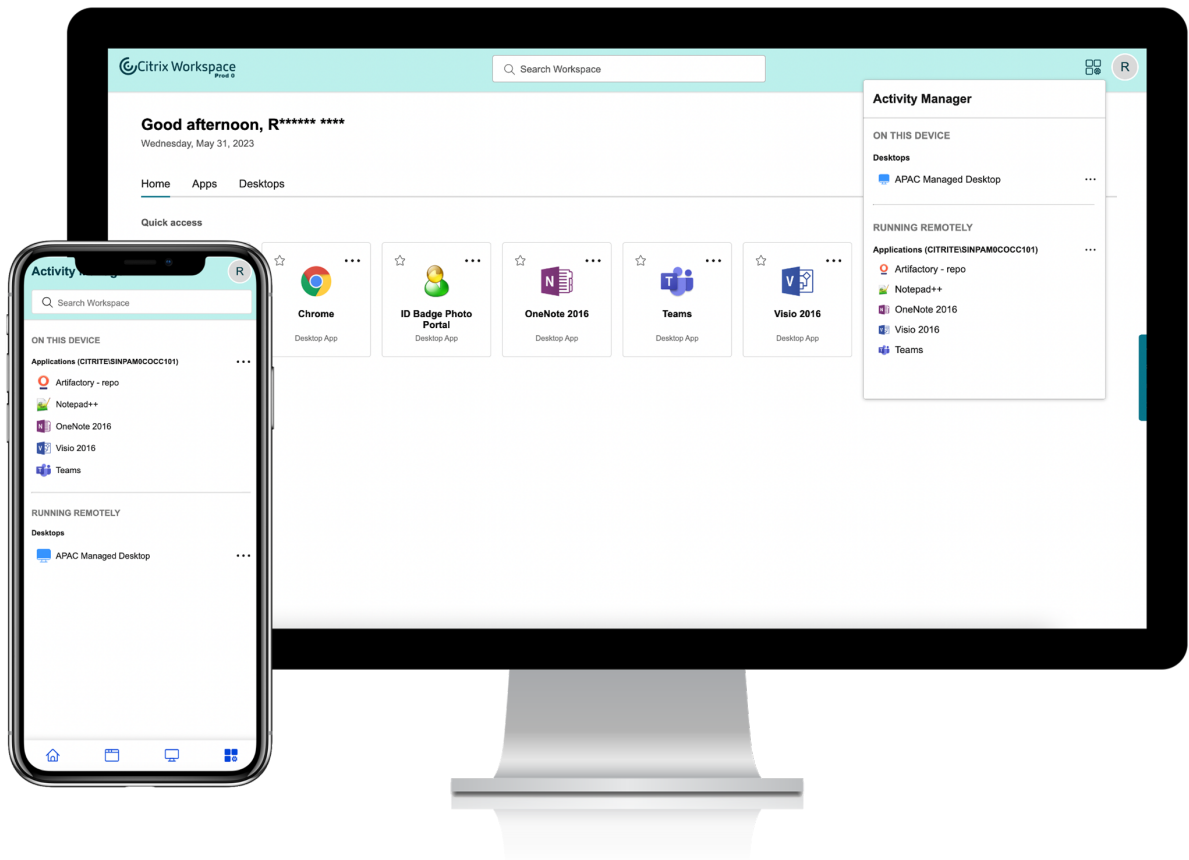
23.22

新機能

アクティビティマネージャーの紹介 ワークスペースユーザーインターフェイス内の 1 つのウィンドウペインから、あらゆるデバイスでアクティブになっているアプリとデスクトップを管理し、迅速なアクションを実行できるようになりました。すべてのアクティブなアプリとデスクトップは、現在使用しているセッションにグループ化されます。

アクティビティマネージャーアイコンは、[ワークスペースユーザーインターフェイス] ウィンドウのプロファイルアイコンの左側に表示されます。アイコンをクリックすると、次の内容が表示されます。

- [このデバイス上] の下に、現在使用しているデバイスから始まるアプリとデスクトップの一覧が表示されます。
- [リモートで実行] に、他のデバイスでアクティブなアプリとデスクトップのリストが表示されます。



詳細については、「[アクティビティ マネージャー](#)」を参照してください。

注:

アクティビティマネージャーアイコンがはっきりと表示されない場合は、[バナーのテキストとアイコンの色]の設定で選択した色を変更することを検討してください。バナーとアクティビティマネージャーアイコンとのコントラストが低いため、アイコンがはっきりと見えない場合があります。詳しくは、「[カスタムテーマを構成する](#)」を参照してください。

既知の問題

- セッションが切断されると、ユーザーはセッションからログアウトできなくなります。切断されたセッションは、[アクティビティマネージャー] パネルには表示されません。
- Mac 向け Citrix Workspace アプリでは、アクティビティマネージャーパネルに表示されるアクティブなアプリとデスクトップの一覧に、すべてのストアのアクティブなセッションが表示されます。

23.15

新機能

新しいワークスペースユーザーインターフェイス Citrix Workspace アプリには、よりクリーンなビューのための最新の外観を備えた新しいユーザーインターフェイス機能が導入されています。ユーザーインターフェイスの機能強化は、Web、デスクトップ、モバイルに適用できます。

強化された最初のユーザーエクスペリエンス ダウンロードした Citrix Workspace アプリまたは Citrix をブラウザから初めて起動すると、関連するアプリの一覧が画面に表示されます。これらのアプリは管理者によって決定され、ワンクリックでこれらのアプリをお気に入りとして追加できます。

強化された検索エクスペリエンス 強化された検索機能により、検索エンジンからより迅速な結果が得られます。[検索] オプションを使用すると、ワークスペースアプリ内から迅速かつ直感的に検索を行うことができます。

管理者関連のタスク

管理者は、サブスクリイバー向けに Workspace アプリのユーザーエクスペリエンスをカスタマイズできます。詳しくは、後のセクションを参照してください。

- [ユーザーの新しいワークスペースエクスペリエンスを有効にする](#)
- [ユーザーのホーム画面を有効または無効にする](#)

Global App Configuration Service の新機能

November 28, 2023

次のセクションでは、Global App Configuration Service の最新リリースおよび以前のリリースの新機能について説明します。

2023 年 10 月 30 日

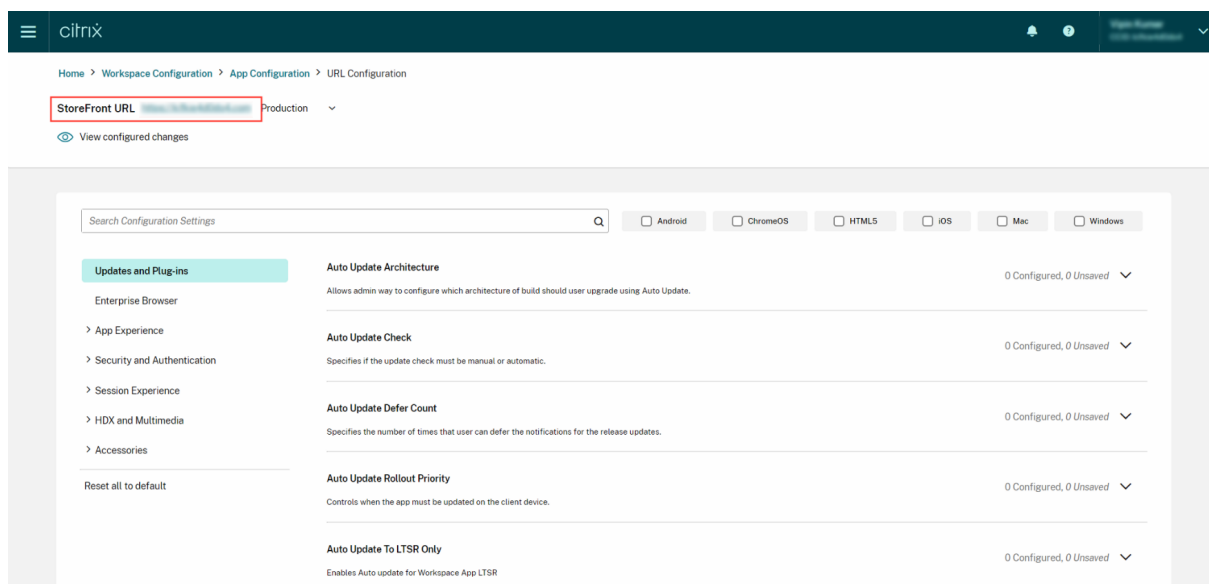
オンプレミスストアの設定の構成

Global App Configuration Service のユーザーインターフェイスを使用して、オンプレミスストアの設定を構成できるようになりました。Citrix Cloud アカウントにサインインし、[ワークスペース構成] > [アプリ構成] に移動して開始します。

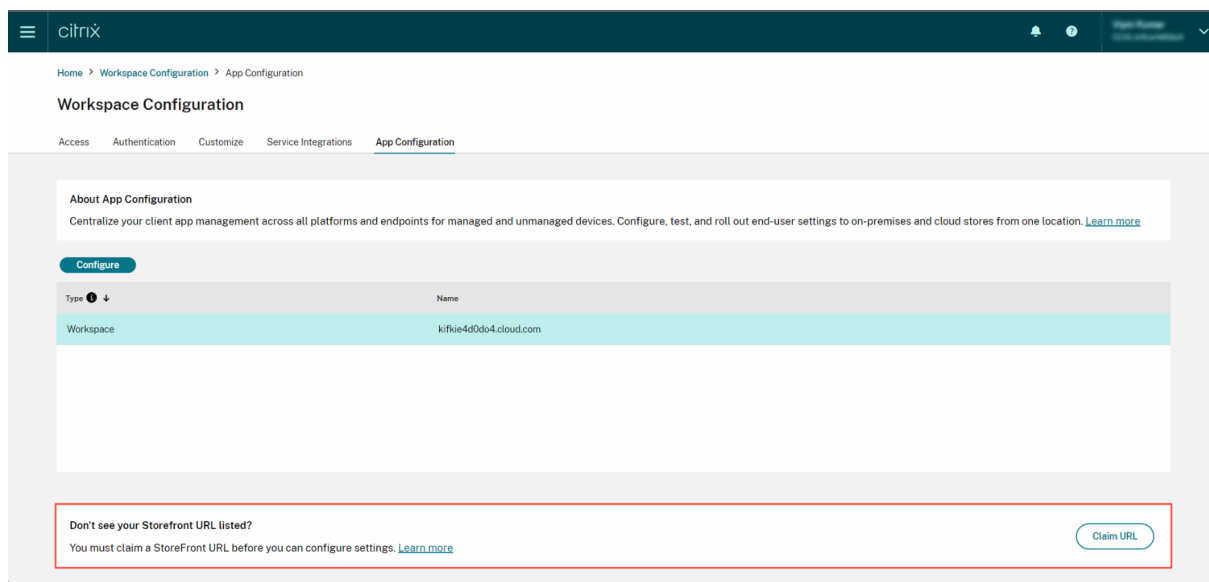
注:

Citrix Cloud アカウントをまだお持ちでない場合は、[サインアップページ](#)に移動してアカウントを作成してください。

続行する前に、StoreFront URL に対する要求が確立されていることを確認してください。URL を要求した場合は、次の画面が表示され、オンプレミスストアの設定の構成を開始できます。



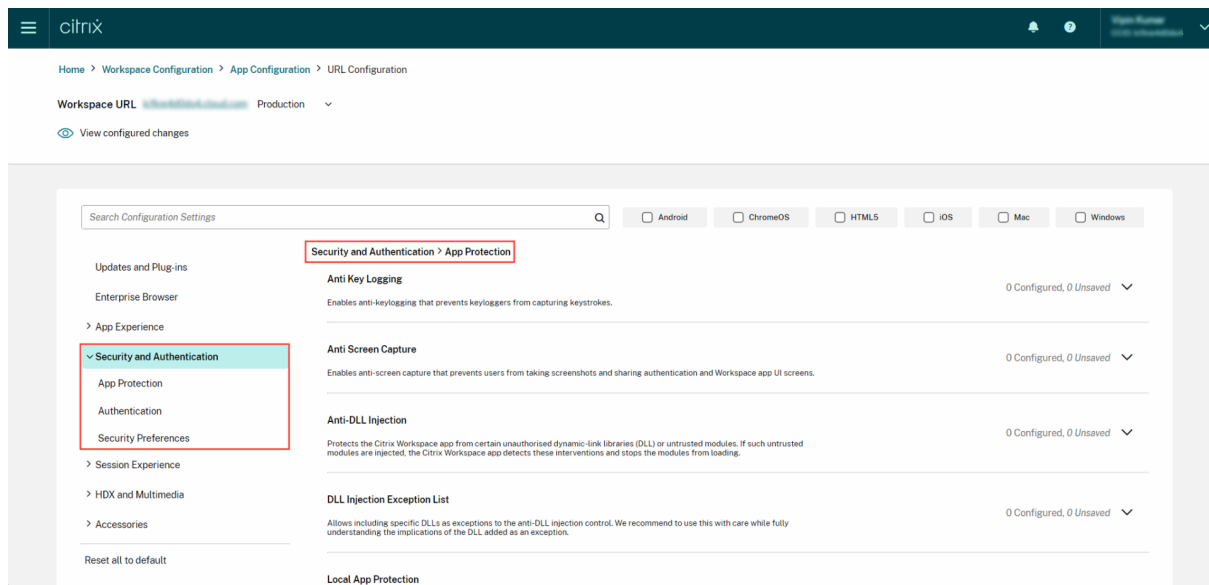
URL をまだ要求していない場合は、次の画面が表示されます。[オンプレミスストアの設定を構成する] セクションで [開始] をクリックして、URL を要求します。詳しくは、「[はじめに](#)」を参照してください。



2023年9月28日

シンプルな設定の分類で移動がスムーズ

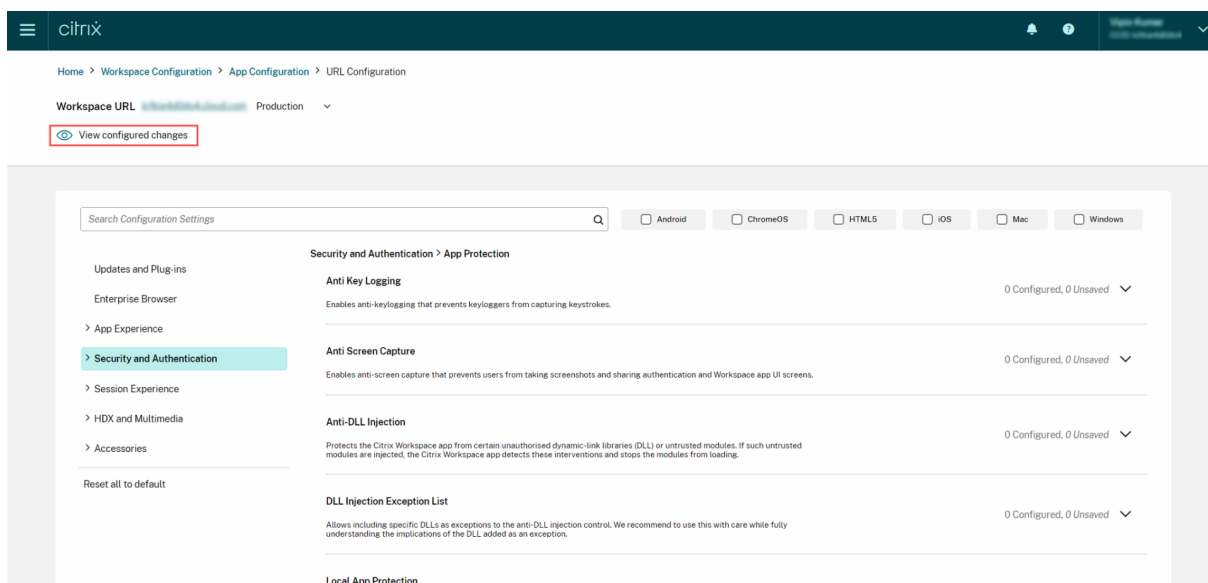
Global App Configuration Service ユーザーインターフェイスが強化され、ユーザーにわかりやすいように設定が分類されるようになりました。設定はエンドユーザーのワークフローとトピックに基づいて分類されており、7つの主なフォルダーと複数のサブフォルダーで構成されています。この整理された構成により、管理者は300以上の設定間を簡単に移動できるようになります。



2023年7月28日

構成された設定の概要を表示する

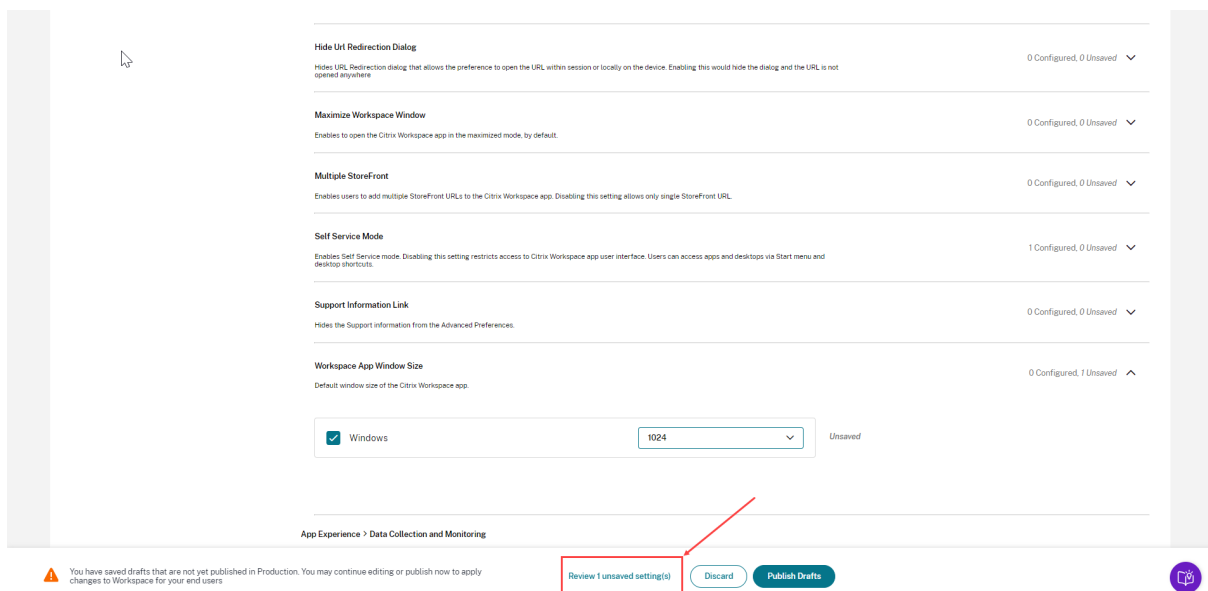
管理者は、[構成された設定を表示] ボタンをクリックして現在の構成の概要を表示できるようになりました。これにより、それぞれの設定を個別に展開して確認する必要がなくなります。構成されたすべての設定の統合リストにより、管理者は、現在の構成を包括的に確認し、ユーザーへの影響を評価することができます。



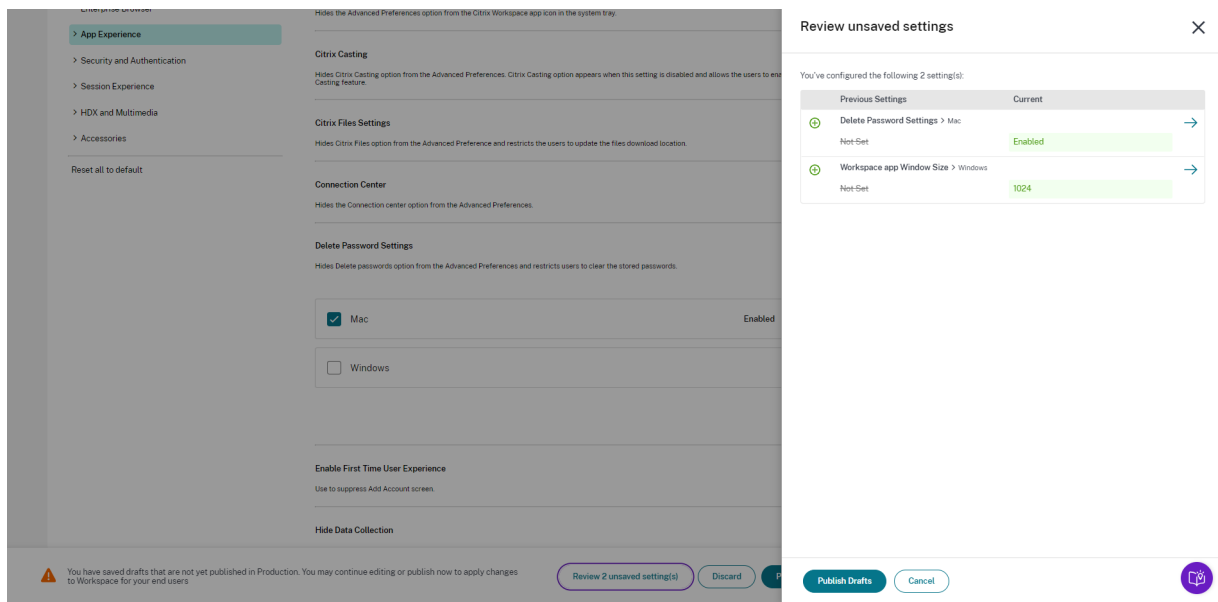
2023年6月7日

未保存の変更を確認する

この機能強化により、管理者は、構成を公開する前に未保存の変更の最終確認を実行できます。未保存の設定の数がUIに表示され、管理者は、[未保存の設定を確認] オプションをクリックしてこのリストにアクセスできます。これにより、管理者は、情報に基づいて変更を加え、データの正確性を維持できます。



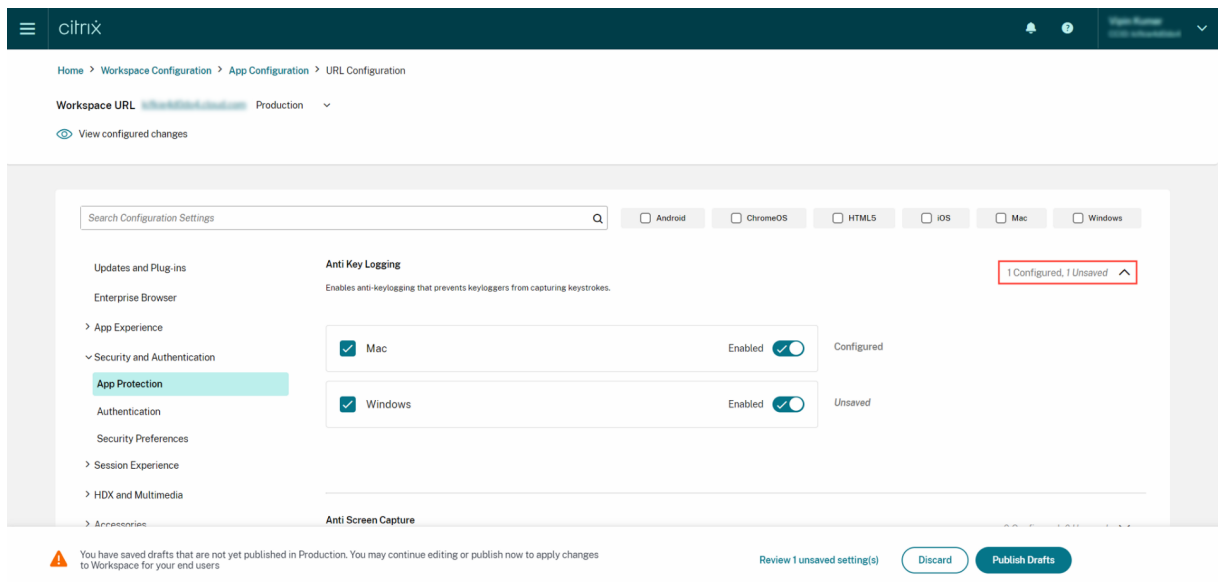
管理者は、矢印をクリックして未保存の設定に移動することもできます。



強化されたユーザーインターフェイス

管理者は、それぞれの設定を展開せずにステータスを表示できるようになりました。各ステップで情報に基づいた決定が簡単にできるように、次のタグが表示されるようになりました。

- 構成済み: 設定がすでに構成されているプラットフォーム（クライアント OS）の数が表示されます。
- 未保存: 構成されているがまだ保存されていない設定の数が表示されます



2023年5月23日

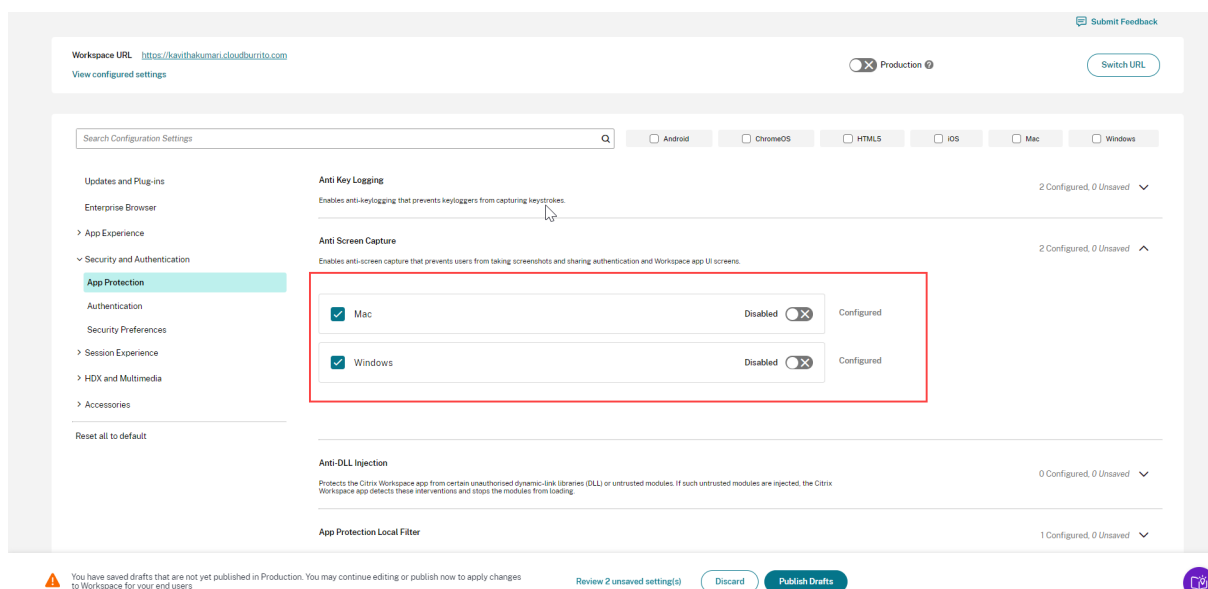
強化された検索機能

この機能強化により、検索エクスペリエンスが強化され、堅牢でシームレスなエクスペリエンスが提供されます。管理者は、クラウドポータルにサインインし、[アプリ構成] ページで必要な設定を簡単に見つけることができるようになりました。次の検索方法を使用できます。

- **設定の説明を使用した検索**
管理者は、設定の説明内にあるキーワードを入力して設定を見つけることもできます。これにより、目的の設定に関連付けられた関連用語を利用して、より柔軟な検索アプローチが可能になります。
- **API 設定名を使用した検索**
管理者は、対応する API 設定名を入力して設定を検索することができます。この方法により、より正確で絞った検索が可能になり、ユーザーは必要な特定の設定をすばやく見つけることができます。

各設定に適用可能なプラットフォームを表示する

各設定には、関連する適用可能なプラットフォームのみが動的に表示されるようになりました。このインテリジェントなフィルタリングにより、ユーザーには簡潔でカスタマイズされたオプションのリストが表示され、不必要な混乱が排除されます。



Citrix Workspace の利用を開始する

October 12, 2023

この記事では、Citrix Workspace および関連コンポーネントのセットアップに関連する主な手順を最初から最後まで概説します。関連するフェーズの概要については、「[ワークフローの概要](#)」を参照してください。

完全な Citrix Workspace 環境に移行する方法は他にもあります。最も一般的な方法は次のとおりです：

- ワークスペースを介した Citrix Virtual Apps and Desktops の配信。
 - Workspace を介してオンプレミスの Virtual Apps and Desktops 展開のリソースにアクセスする場合は、「[ハイブリッドソリューションのサイトアグリゲーション](#)」を参照してください。
 - クラウドに移行する場合は、「[クラウドへの完全な移行](#)」を参照してください。

ワークフローの概要

Citrix Workspace を新規顧客として設定する場合、作業には 5 つの大きなフェーズがあります：

1. [Citrix Cloud](#) で [Citrix Workspace](#) の準備をする。
2. [利用者のアクセスと認証を構成する](#)。
3. [サービスをワークスペースに統合します](#)。
4. ロゴやセキュリティポリシーなど企業固有の設定で、[ワークスペースをカスタマイズする](#)。
5. [Citrix Workspace](#) を利用者にロールアウトする。

[Success Center](#)では、追加のソリューションベースのガイダンスを提供しています。

フェーズ 1: [Citrix Cloud](#) で [Citrix Workspace](#) の準備をする

[Citrix Workspace](#) を構成する前に、[Citrix Cloud](#) にサインアップし、[Citrix Workspace](#) を使用開始するための技術要件を満たしていることを確認する必要があります。

既に [Citrix Cloud](#) をご利用で、[\[ID およびアクセス管理\]](#) を通じて管理者が追加されている場合は、スキップして「[フェーズ 2: 利用者のアクセスと認証を構成する](#)」に進んでいただいてもかまいません。

フェーズ 1 の手順には、次のようなものがあります：

1. [Citrix Cloud](#) にサインアップする。
2. [Citrix ID](#) を持つ管理者を追加する。
3. 次の方法でインフラストラクチャを設定する：
 - リソースの場所の作成
 - [Cloud Connector](#) の展開

[Citrix ID](#) の構成には、時間ベースのワンタイムパスワード (TOTP: time-based one-time password) が含まれます。[Citrix ID](#) に加えて、[Azure AD](#) 認証を構成できます。管理者の追加と管理者の認証の構成について詳しくは、[Citrix Cloud](#) 製品ドキュメントの「[管理者](#)」を参照してください。

フェーズ 2: 利用者のアクセスと認証を構成する

フェーズ 2 では、[ワークスペース構成] で Workspace URL や外部接続などのアクセス制御を構成します。

また、[ID およびアクセス管理] で 1 つまたは複数の ID プロバイダーを構成してから、利用者がワークスペースに認証する際の主な方法として、ID プロバイダーのいずれかを [ワークスペース構成] で有効にします。

注:

Citrix Workspace にアクセスするには 2 つの方法があります。1 つは、ネイティブインストールされた [Citrix Workspace アプリ](#) です。このアプリは Citrix Receiver に代わるサービスで、Citrix Cloud サービスとワークスペースに簡単かつ安全にアクセスできます。Citrix Workspace にアクセスするもう 1 つの方法は、ブラウザで [Workspace URL](#) を使用します。Workspace URL はデフォルトで有効になっており、通常は次の形式です: <https://yourcompanyname.cloud.com>。

詳しくは、「[ワークスペースへのアクセス](#)」を参照してください。

ワークスペースアクセスの構成

[ワークスペース構成] > [アクセス] で、アクセス制御を構成します。これには通常、次のようなタスクがあります:

- [Workspace URL](#) を構成して有効にする。
- [Citrix Gateway](#) との外部接続を構成する。

これらの 2 つのタスクの後、ワークスペースの一貫したエクスペリエンスを実現するために、[Citrix Workspace アプリ](#) をインストールし、利用者に使用を促すことをお勧めします。

ワークスペースへの利用者認証の構成

利用者がワークスペースにサインインするための認証方法を定義することには、2 段階のプロセスがあります:

1. [ID およびアクセス管理] で、ID プロバイダーを構成します。
2. [ワークスペース構成] > [認証] に移動し、最初の手順で構成した ID プロバイダーが提供している認証方法のいずれかを選択します。

フェデレーション ID プロバイダーを使用している場合は、[Citrix フェデレーション認証サービス \(FAS\)](#) を使用して DaaS へのシングルサインオン (SSO) を有効にすることもできます。

ワークスペースへの利用者認証の構成について詳しくは、「[セキュアなワークスペース](#)」を参照してください。

フェーズ 3: サービスをワークスペースに統合する

サービスをワークスペースに統合することには、別の二段階のプロセスがあります:

1. 購入したサービスを Citrix Cloud で構成します。サービスの一覧については、「[Citrix Cloud サービス](#)」を参照してください。
2. [ワークスペース構成] > [サービス統合] で、構成したサービスへのアクセスを有効にします。サービス統合について詳しくは、「[サービスの有効化と無効化](#)」を参照してください。

フェーズ 4: ワークスペースをカスタマイズする

以下を実行することで、[ワークスペース構成] で、各ユーザーのワークスペースの利用者エクスペリエンスをカスタマイズし、組織の特定の要件を満たすことができます:

- ログやカスタムテーマなど、ワークスペースの外観をカスタマイズする。ワークスペースの外観をカスタマイズする手順については、「[ワークスペースの外観をカスタマイズする](#)」を参照してください。
- 利用者が [お気に入り] を作成できるようにしたり、デスクトップを自動起動できるようにしたりするなど、操作オプションを選択する。利用者がワークスペースを操作する方法のカスタマイズ手順については、「[ワークスペース操作をカスタマイズする](#)」を参照してください。
- タイムアウト期間の設定、サインインポリシーの作成、利用者のワークスペース内からのパスワード変更の許可など、プライバシーとセキュリティをカスタマイズする。ワークスペースのプライバシーとセキュリティポリシーをカスタマイズする方法については、「[セキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。

フェーズ 5: Citrix Workspace を利用者にロールアウトする

運用での受け入れテストでワークスペースの整合性を検証し、[Success Center](#)を参照しながら、利用者のオンボード方法を計画することをお勧めします。このフェーズの大きな作業には、次のようなものがあります:

1. ワークスペースをテストする。
 - ブラウザーから Citrix Workspace アプリにサインインできることを確認する。
 - 使用できるすべてのアプリとデスクトップを起動して使用する。
 - 使用できるフォルダーとファイルにアクセスできることを確認する。
 - 通知に予期したとおりの操作とアクティビティが表示されていることを確認する。
 - 有効になっている場合は、モバイルデバイスのエンドポイントリソースにアクセスできることを確認する。
2. 利用者をオンボードする。
 - Citrix Workspace 機能と利用者をつなぐ。
 - ブラウザーの [Workspace URL](#) を共有する。
 - [Citrix Workspace アプリ](#) をインストールするようにユーザーを案内する。

ワークスペースのテストとワークスペースへの利用者のオンボードについて詳しくは、「[Citrix Workspace エンドユーザー採用リソース](#)」を参照してください。

Citrix Workspace を準備する

October 12, 2023

この記事では、Citrix Workspace 実装の準備に役立つ要件と管理者のアクティビティについて説明します。Citrix Workspace の準備に関連する手順には次のようなものがあります：

1. Citrix Cloud の [システムと接続の要件](#) を満たしていることを確認する。
2. Citrix Workspace の [展開とロールアウトを計画](#) する。
3. [Citrix Cloud にサインインまたはサインアップ](#) する。
4. Citrix Cloud および Citrix Workspace に [管理者を追加](#) する。
5. クラウドでホストされるサービスの [使用権を確認](#) する。
6. Citrix Workspace に必要な [インフラストラクチャをセットアップ](#) する。

[Success Center](#) は、このドキュメントに欠かせないパートナーです。Success Center の記事では、ソリューションに基づいた幅広い視点と、サービス固有の詳細な情報を提供しています。

[Citrix Cloud](#) 製品ドキュメントでは、IT マネージャーと開発者向けに、Citrix Cloud での Citrix Workspace の準備に関連する前提条件とアクティビティについて、詳細な情報を提供しています。

システムおよび接続要件

Citrix Cloud は、サービス使用権を表示および管理し、[ワークスペース構成] にアクセスするためのコンソールです。

Citrix Cloud を既にセットアップしている場合は、「[展開とロールアウトを計画](#)する」で説明されている手順をスキップできます。

まとめると、Citrix Cloud には以下の構成が必要です：

- 利用者のワークスペースへの認証を管理するための Active Directory ドメイン。
- リソースの場所ごとに少なくとも 2 つの Citrix Cloud Connector。
- 各 Cloud Connector に専用のマシン。
- ワークロードと他のコンポーネントをホストするためのドメイン参加済みの物理マシンまたは仮想マシン。

Citrix Cloud Connector をホストするマシンに他のコンポーネントをインストールすることはできないため、少なくとも 2 台の物理マシンまたは仮想マシンが必要です。

Cloud Connector の要件については、「[Citrix Cloud Connector の技術詳細](#)」を参照してください。Cloud Connector のインストールについては、「[Cloud Connector のインストール](#)」を参照してください。

また、Citrix Workspace を操作するには、以下のアドレスが利用可能である必要があります：

- https://*.cloud.com

- https://*.citrixdata.com

Citrix Cloud サービスで必須の接続可能アドレスの完全な一覧については、「[サービス接続要件](#)」を参照してください。

展開とロールアウトを計画する

Citrix Workspace のサポートと管理の計画を準備することをお勧めします。[Success Center のプラン](#)を参照して、目標を設定し、ユースケースを定義し、リスクを特定し、以下を含む実装戦略を作成します：

- ビジネスの成果、追加するサービス、およびユーザーグループの要件を確立する。
- Citrix Workspace の「[インフラストラクチャをセットアップする](#)」の技術的な要件を確認する。
- Workspace チームを構築する。配信チームにタスクを割り当て、[ワークスペース構成] にアクセスできる Citrix Cloud アカウントに[管理者を追加](#)します。
- プロセスの所有者と利用者とのかわり方を計画する。
 - 変更戦略とコミュニケーションプランを作成します。
 - トレーニングと強化のアプローチ方法を開発します。
 - 影響と利害関係者の分析を実施します。

ワークスペースの展開とロールアウトの計画について詳しくは、Success Center の「[Success Readiness Checklist](#)」を参照してください。

Citrix Cloud にサインインまたはサインアップする

新規顧客としてサインアップする場合は、「[Citrix Cloud にサインアップする](#)」の手順に従ってください。

組織の管理者アカウントが既に作成されている場合は、プライマリ管理者が会社のアカウントにあなたを追加する必要があります。詳しくは、「[管理者の追加](#)」を参照してください。

既にアカウントがある場合は、[citrix.com](#)、My Citrix、または Citrix Cloud の資格情報を使用して、Citrix Cloud にサインインします。

Citrix Cloud へのサインインまたはサインアップについて詳しくは、「[Citrix Cloud Services Kickoff Guide](#)」を参照してください。

管理者を追加する

最初の管理者アカウントは、最初の Citrix Cloud オンボードプロセスを通じて作成されます。この最初の管理者が、Citrix Cloud に参加する他の管理者を招待できます。これらの新しい管理者は、既存の Citrix アカウント資格情報を使用するか、新しいアカウントをセットアップすることができます。

管理者を招待する

管理者は、Citrix Cloud コンソールの左側にあるメニューの **[ID およびアクセス管理]** から、Citrix Cloud アカウントに追加されます。追加する管理者のメールアドレスを入力して、サインイン手順を記載した招待状を送信します。

Citrix Cloud アカウントに管理者を追加するときは、組織内での役割に適した管理者権限を定義します。フルアクセス権限を持つ管理者は、デフォルトで **[ワークスペース構成]** にアクセスできます。カスタムアクセス権限を持つ管理者は、選択された機能およびサービスのみアクセスできます。招待する管理者のアクセス権限を変更できます。

管理者の追加（および削除）については、「[管理者](#)」を参照してください。

管理者認証をセットアップする

デフォルトでは、Citrix Cloud は Citrix ID プロバイダーを使用して、Citrix Cloud アカウントを管理します。Citrix ID プロバイダーは、Citrix Cloud 管理者のみを認証します。利用者は、「[セキュアなワークスペース](#)」に記載されているいずれかの ID プロバイダーで認証する必要があります。

Citrix Cloud アカウントの各管理者は、多要素認証（MFA）も設定する必要があります。

登録のプロセスでは、Citrix SSO などの [時間ベースのワンタイムパスワード（TOTP: Time-Based One-Time Password）標準](#) に準拠した認証アプリをダウンロードしてインストールします。スムーズに登録するために、以下の手順を完了する前に、[Citrix SSO](#)をダウンロードしてインストールすることをお勧めします。

1. Citrix Cloud アカウントにサインインします。
2. 名前を選択し、ドロップダウンメニューから **[マイプロフィール]** を選択します。
3. 手順 4 で必要な確認コードが記載されたメールを受信するには、**[ログインセキュリティ]** の **[認証アプリのセットアップ]** を選択します。
4. プロンプトが表示されたら、Citrix から送信されたメールに記載された確認コードとアカウントのパスワードを入力し、**[確認]** をクリックします。
5. QR コードをスキャンするか、Citrix SSO などの時間ベースのワンタイムパスワード（TOTP）標準に準拠した認証アプリにキーを入力します。
6. MFA が正しく設定されていることを確認するには、認証アプリから 6 桁のコードを入力し、**[確認]** を選択します。
7. **[復旧用の電話番号を追加する]** を選択し、Citrix サポートが MFA 関連のクエリの ID を確認できる連絡先電話番号を入力します。
8. **[バックアップコードを生成する]** を選択して、認証アプリにアクセスできない場合に使用できる 1 回限りの使用コードの一覧を作成します。
9. **[コードをダウンロードする]** を選択し、バックアップコードを含むテキストファイルを安全でアクセス可能な場所に保管します。
10. チェックボックスをオンにしてから、**[完了]** を選択します。

MFA の設定手順は、[Knowledge Center](#)の記事、および Citrix Cloud 製品ドキュメントの「[多要素認証を設定する](#)」にも記載されています。

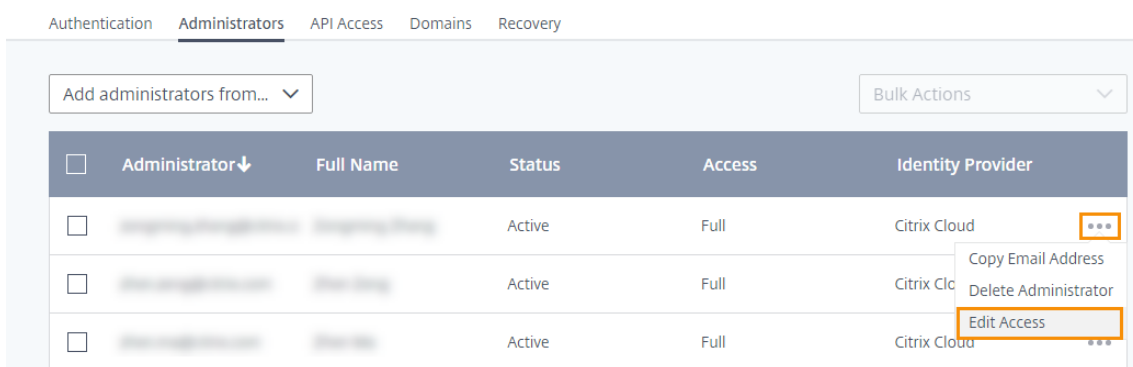
オプションで、管理者用に Azure Active Directory (AD) をセットアップすることもできます。Citrix Cloud の管理者と Workspace の利用者が使用できる ID プロバイダーについて詳しくは、「[ID プロバイダー](#)」を参照してください。

管理者権限を編集する

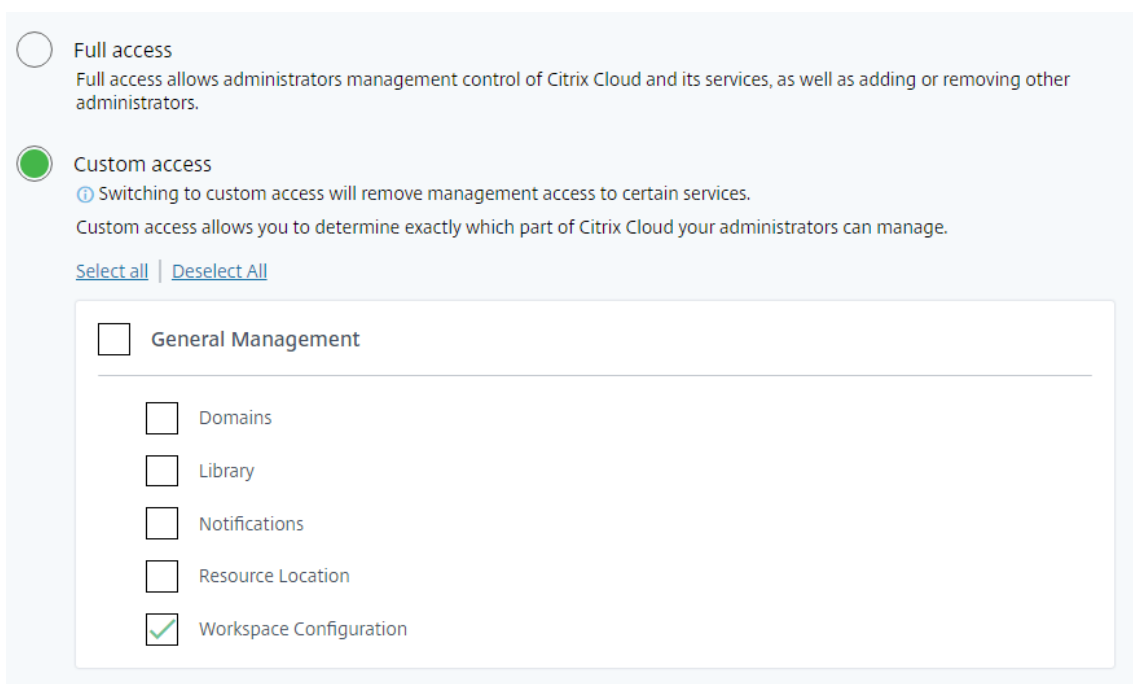
[ワークスペース構成] へのカスタムアクセスを構成するには:

1. **Citrix Cloud** メニューから、[ID およびアクセス管理] を選択し、[管理者] を選択します。
2. 管理する管理者を見つけ、省略記号ボタンをクリックし、[アクセスの編集] を選択します。

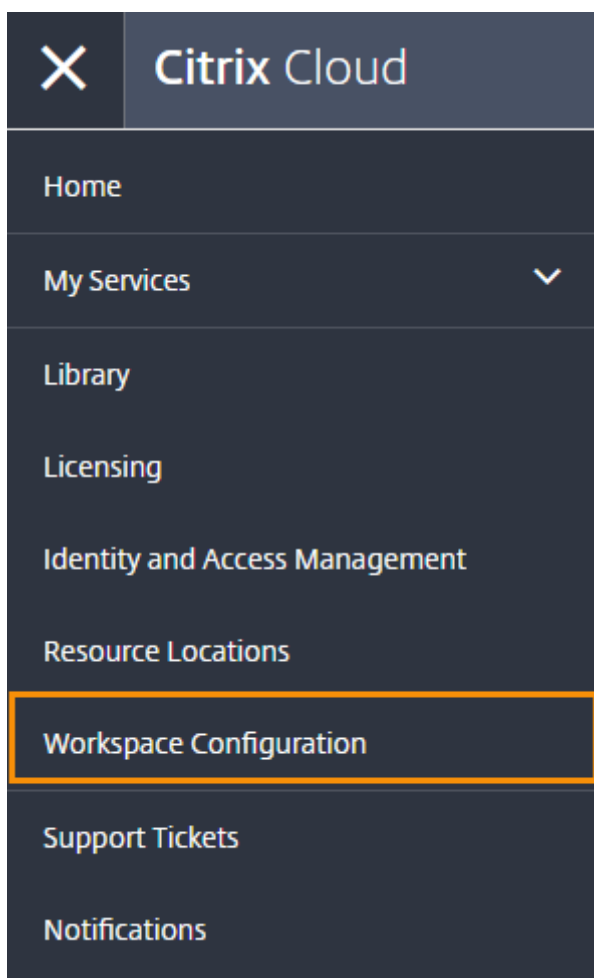
← Identity and Access Management



3. [カスタムアクセス] が有効になっていることを確認します。
4. [ワークスペース構成] のアクセスのみを有効にするには、[一般管理] で [ワークスペース構成] を選択します。



アクセスを有効にした後、管理者は Citrix Cloud にサインインして **[Citrix Cloud]** メニューで **[ワークスペース構成]** を選択できます。



注:

Citrix Virtual Apps Essentials では、最初のカatalogを作成した後に、[Citrix Cloud] メニューで [ワークスペース構成] を選択できるようになります。

使用権を確認する

Citrix Cloud にサインインすると、購入した Citrix の製品とサービスの使用権を管理できます。Citrix の製品とサービスは、Citrix Cloud ダッシュボードにカードレイアウトで表示されます。購入して利用者登録した製品とサービスには、[管理] ボタンが表示されます。

新しいサービスを試す場合は、Citrix Cloud ダッシュボードにある対応するボックスで **[トライアルのリクエスト]** または **[デモをリクエストする]** を選択できます。サービストライアルについて詳しくは、「[Citrix Cloud サービスのトライアル](#)」を参照してください。

新しいサービスを購入する場合は、構成し直したり新しいアカウントを作成したりせずに、トライアルを製品版

サービスに変換できます。サービスを購入するには、Citrix Cloud コンソールの右上隅にある組織 ID をメモして、<https://www.citrix.com/product/citrix-cloud>にアクセスします。

インフラストラクチャをセットアップする

Citrix Workspace に必要なインフラストラクチャをセットアップするには、次の方法でリソースを Citrix Cloud に接続する必要があります：

- ご使用の環境にコネクタを展開します。
- リソースの場所を作成します。

リソースの場所には、利用者にクラウドサービスを提供するために必要なリソースが含まれます。これらのリソースは、Citrix Cloud コンソールで管理します。リソースの場所に含まれるリソースは、使用しているサービスによって異なります。

リソースの場所を作成するには、ドメインに少なくとも 2 つの Cloud Connector をインストールする必要があります。

Citrix Cloud Connector は、Citrix Cloud とリソースの場所との間の通信チャンネルを提供するコンポーネントです。このチャンネルは、標準 HTTPS ポート (443) と TCP プロトコルを使用して、クラウドへの接続を確立します。受信接続は受け入れられません。

詳しくは、「[Citrix Cloud Connector](#)」を参照してください。

注：

ワークスペースは、PNAgent URL を使用してリソースに接続する従来のクライアントからの接続をサポートしていません。そうした従来のクライアントが環境に含まれている場合は、代わりにオンプレミスに StoreFront を展開して、従来のサポートを有効にする必要があります。従来のクライアントの接続を保護するには、Citrix Gateway サービスではなくオンプレミスの Citrix Gateway を使用します。

次の手順：ワークスペースを構築する

Citrix Workspace の準備ができたので、以下のように次の手順に進みます：

- Workspace URL や外部接続など、[ワークスペースへのアクセスを構成](#)します。
- 「[セキュアなワークスペース](#)」の手順に従って、ワークスペース認証を構成します。
- [サービスをワークスペースに統合](#)します。
- ワークスペースのエクスペリエンスをカスタマイズします：
 - [ワークスペースの外観をカスタマイズ](#)します。
 - [ワークスペース操作をカスタマイズ](#)します。
 - [セキュリティとプライバシーポリシーをカスタマイズ](#)します。

新しいワークスペースユーザーインターフェイス

November 28, 2023

新しいワークスペースユーザーインターフェイス (UI) は、視覚的な複雑さを軽減し、重要な機能に簡単にアクセスできるようにし、必要に応じてワークスペースアプリの使用と機能をより詳細に制御することで、ユーザーエクスペリエンスを向上させます。

この記事では、サブスクライバーがワークスペースにサインインするときに表示される主な機能のいくつかに焦点を当て、ワークスペースにアクセスして操作する方法を要約します。

注:

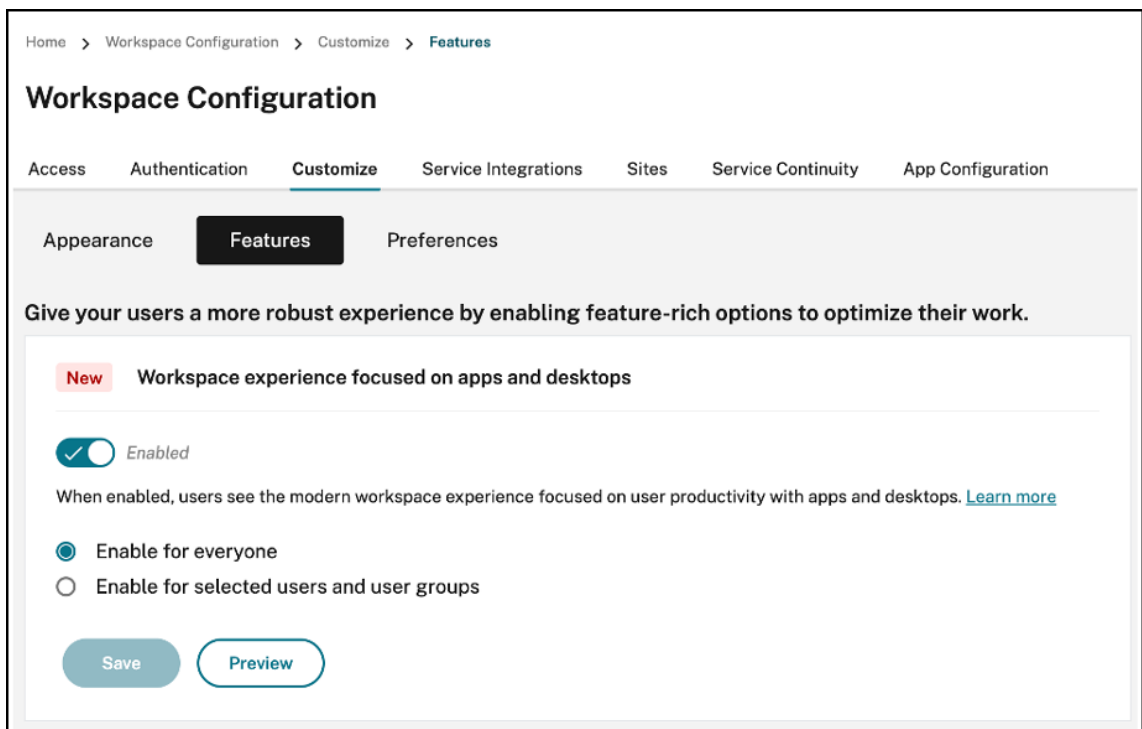
新しいユーザーインターフェイスは、Citrix Workspace アプリのすべての LTSR バージョンでサポートされています。また、Internet Explorer (Citrix Workspace ユーザーインターフェイスバージョン 23.26 はフリーズされています) を除くすべての Web ブラウザーとも互換性があります。

新しいワークスペースエクスペリエンスを有効にする

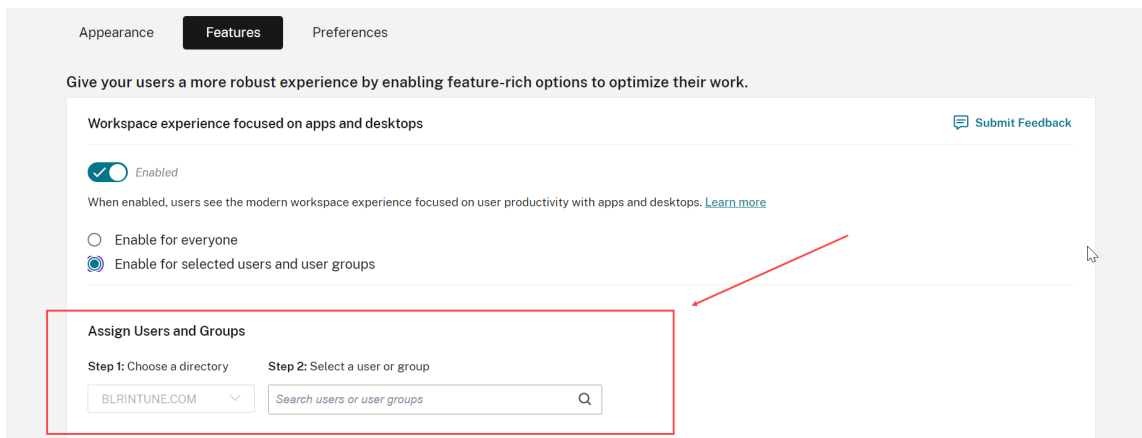
既存のユーザーに対して新しいワークスペースユーザーインターフェイスを有効にすることができます。有効にすると、ユーザーはアプリとデスクトップの生産性を重視した最新のワークスペースを体験できます。

新しいユーザーインターフェイスを有効にするには、次の手順に従います。

1. 管理コンソールで、[ワークスペース構成] > [カスタマイズ] > [機能] に移動します。
2. [アプリとデスクトップに重点を置いたワークスペースエクスペリエンス] セクションでトグルをオンにします。デフォルトではトグルはオフになっており、この機能は無効になっています。この機能をすべてのユーザーに対して有効にするか選択したユーザーに対して有効にするかを選択するオプションもあります。



- 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. [保存] をクリックします。
4. ワークスペースアプリを再起動します。

注:

更新されたユーザーインターフェイスが表示されるまでに約 5 分かかる場合があります。古いバージョンの UI

が一時的に表示されることがあります。ブラウザーで開いた場合、ユーザーはページを更新する必要がある場合があります。

テーマ、アイコン、フォント

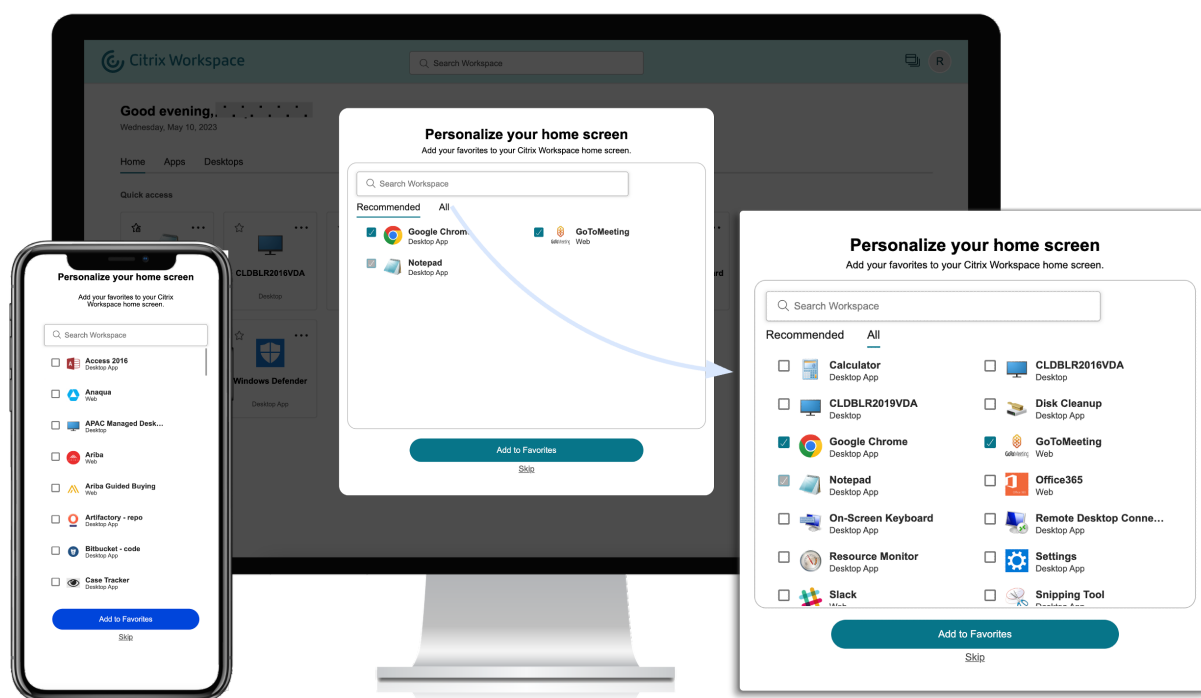
新しいカラーテーマにより、カラーパレットのコントラストと一貫性が向上しました。このフォントは、サポートされているすべてのオペレーティング システムのユーザーインターフェイスに使用されます。新しいアイコンセットには、読みやすさと視覚的な明瞭さのために設計された、より識別しやすい形状と色が使用されています。

ワークスペースアプリの初めてのユーザーエクスペリエンス

新規ユーザーが新しいユーザーインターフェイスにアクセスすると、ポップアップが表示され、簡単な 1 つの手順で複数のアプリをお気に入りに登録できます。

新規ユーザーのエクスペリエンスは、20 個を超えるアプリがあり、それらのアプリをお気に入りに追加していない場合にアクティブになります。このエクスペリエンスは、すべてのブラウザーとネイティブクライアント (Mac、Windows、Linux、ChromeOS)、およびモバイルデバイス (iOS および Android) でサポートされています。初めてサインインすると表示されるようになります。

推奨または必須のアプリは、管理者が設定したとおり、Citrix Virtual Apps and Desktops の DaaS コンソールと、Web および SaaS アプリの Secure Private Access コンソールの新規ユーザー画面の 推奨タブに表示されます。必須アプリはデフォルトで選択されており、チェックマークは無効になっています。推奨アプリと自動お気に入りアプリはデフォルトで選択されており、チェックマークはユーザーに対して有効になっています。他のアプリを選択してサブスクライブしたり、すべてのタブから [お気に入り] に追加したりすることもできます。選択したすべてのアプリが自動的に [お気に入り] に追加され、ホームページに反映されます。



アプリの数が5個以下の場合、Windows向けCitrix Workspaceアプリではクイックアクセスデスクトップショートカットが表示されます。

表示されたすべてのアプリがユーザーにサブスクライブされ、対応するデスクトップショートカットが作成されます。

制限事項

- ユーザー個人設定サービスが拡張されてユーザーが新規ユーザーであるかどうかを追跡するまで、[個人設定]画面はデバイスおよびブラウザーごとに1回表示され、ユーザーがお気に入りのマークを付けられない限りシークレットモードでは毎回表示されます。
- 管理者がアプリから必須タグまたは推奨タグを削除した場合、[お気に入り]内のアプリには影響がありません。
- エンドユーザーが[お気に入り]にアプリを追加していない場合、ワークスペースアプリを開くたびに[個人設定]画面が表示されます。

これを回避するには、以下の操作を行います：

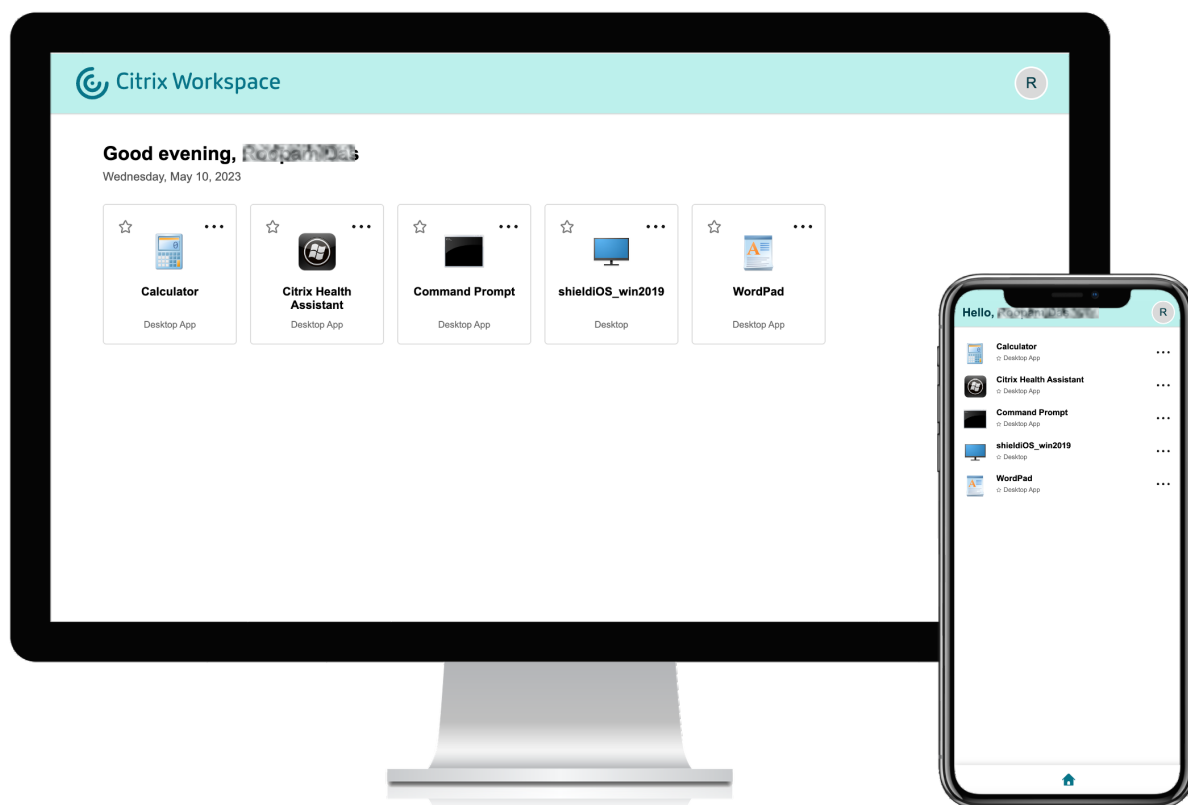
- End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.
- Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage > Full Configuration >**

Applications). This prevents the Personalization screen from appearing for all the end-users. For more information, see [Customize workspace interactions](#).

ワークスペースの視覚表示とレイアウトの改善

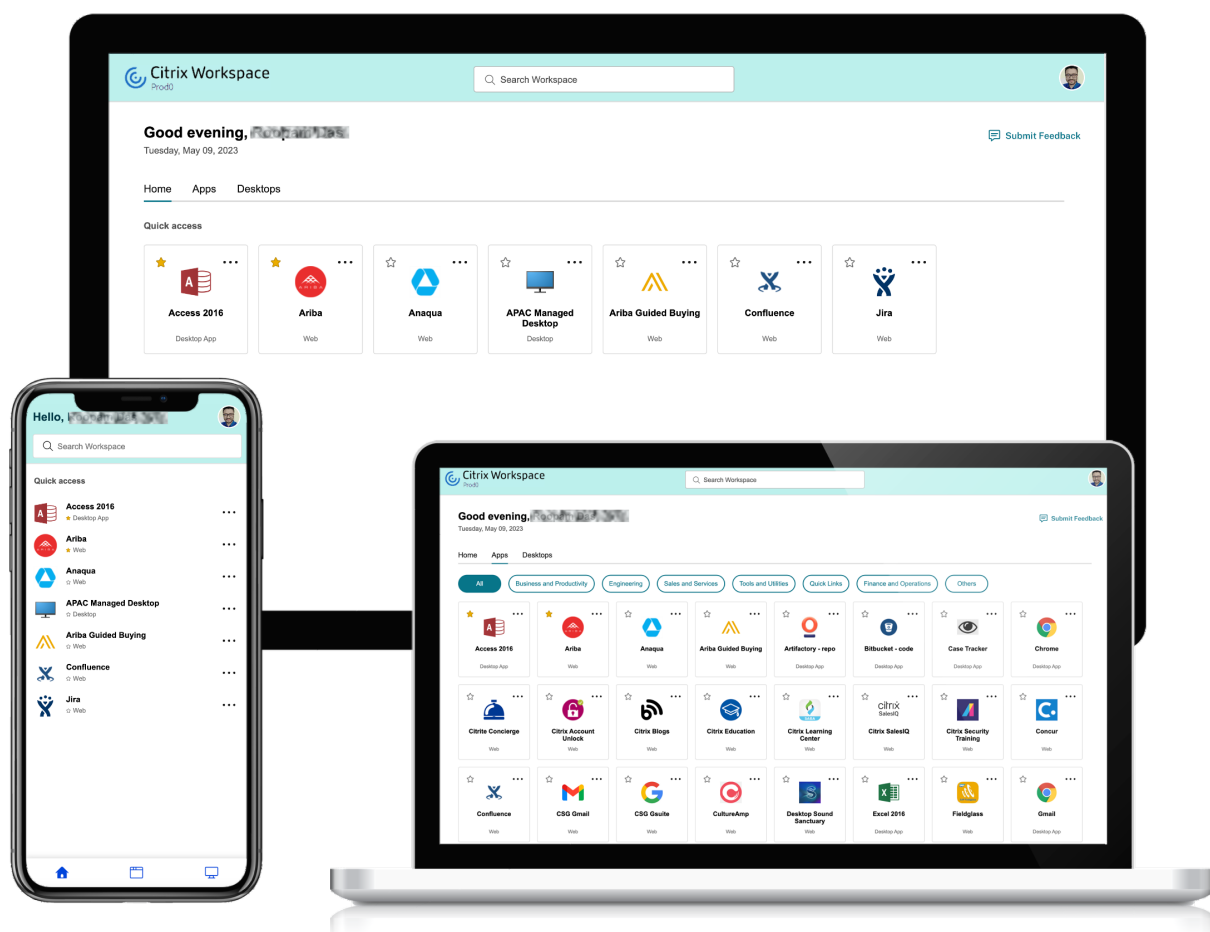
新しいユーザーエクスペリエンスは、直感的なフローと使いやすさに重点を置いて設計されています。アプリや仮想デスクトップのお気に入りには、使いやすいようにユーザーインターフェイスの上部に整理されています。Citrix には、頻繁に使用するアプリやデスクトップ間の移動のしやすさを向上させるための新しいホームページもあります。

アプリの数が 20 未満の場合は、タブやカテゴリのないシンプルビューが画面に表示されます。すべてのアプリとデスクトップが同じページに表示されます。この画面では、お気に入りが最初に表示され、その後他のすべてのアプリがアルファベット順に表示されます。すべてのアプリには星のアイコンがあり、アプリをお気に入りに追加したりお気に入りから外したりできます。所有するアプリの数に応じて、このワークスペースアプリのシンプルビューが表示され、アプリは管理者によって制御されていません。



20 を超えるアプリがある場合は、サインインするとホームページが表示されます。この画面では、すべてのお気に入りアプリが最初に表示され、次に最近使用したアプリが 5 つまで表示されます。必須アプリの星アイコンはロックされており、[お気に入り] から削除できません。管理者がホームページを有効にしていない場合は、[アプリ] 画面が表示されます。この画面では、お気に入りが最初に表示され、その後他のすべてのアプリがアルファベット順に表示

示されます。管理者がカテゴリを作成し、それらにアプリを接続している場合、さまざまなカテゴリが表示され、表示するアプリのカテゴリを選択できます。



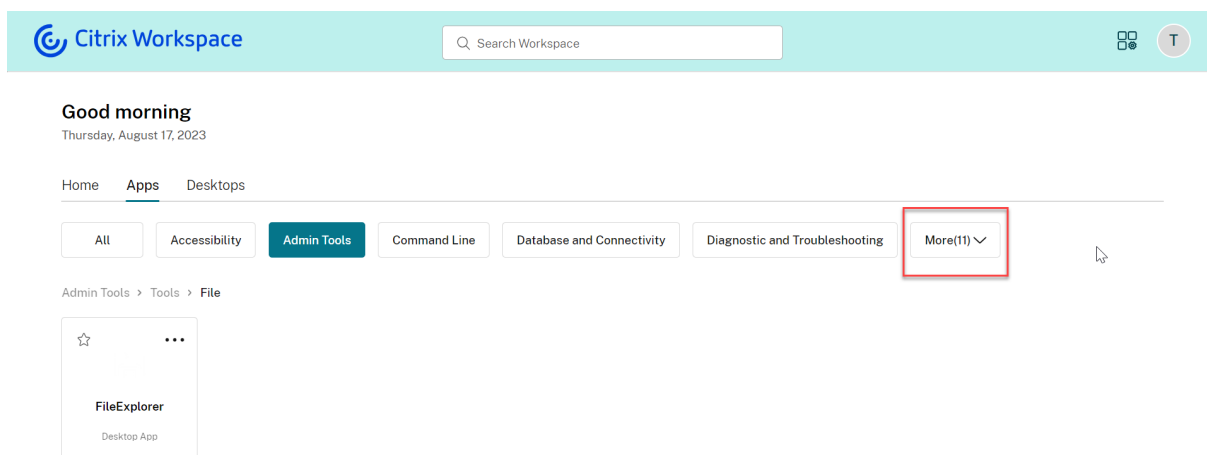
アプリの分類

エンドユーザーは、Workspace ユーザーインターフェイスでアプリケーションをカテゴリおよびサブカテゴリに分類して表示できます。サブカテゴリはフォルダー構造で表示されます。整理されたマルチレベル構造により、混乱のない、最適化されたエクスペリエンスが実現され、全体的なユーザー満足度の向上に役立ちます。

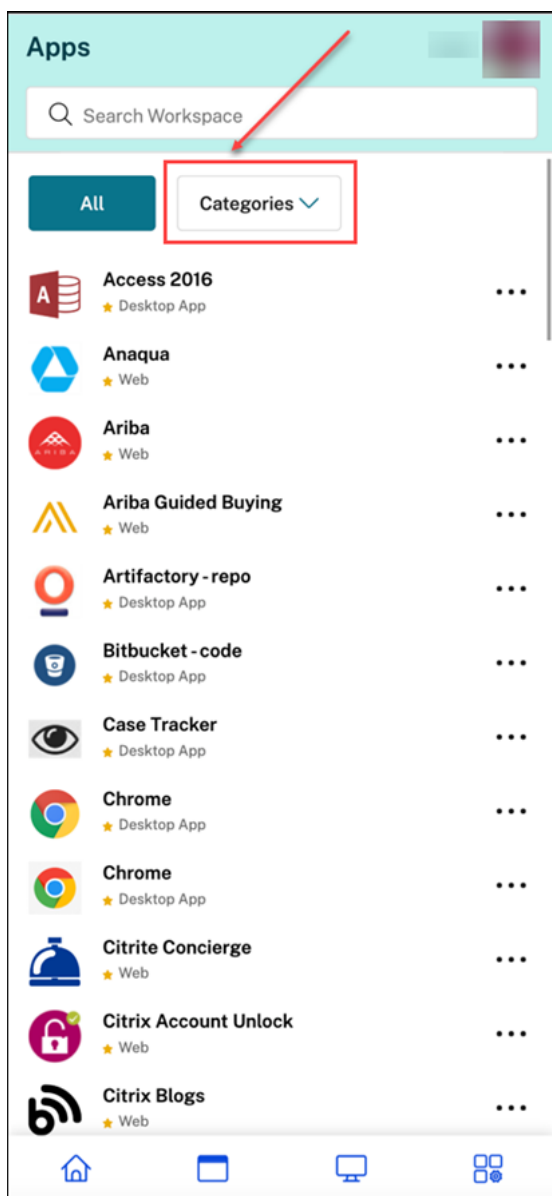
注:

アプリをフォルダー構造の下に表示するには、管理者がフォルダーパスを追加する必要があります。詳しくは、「フォルダーパスの追加」を参照してください。

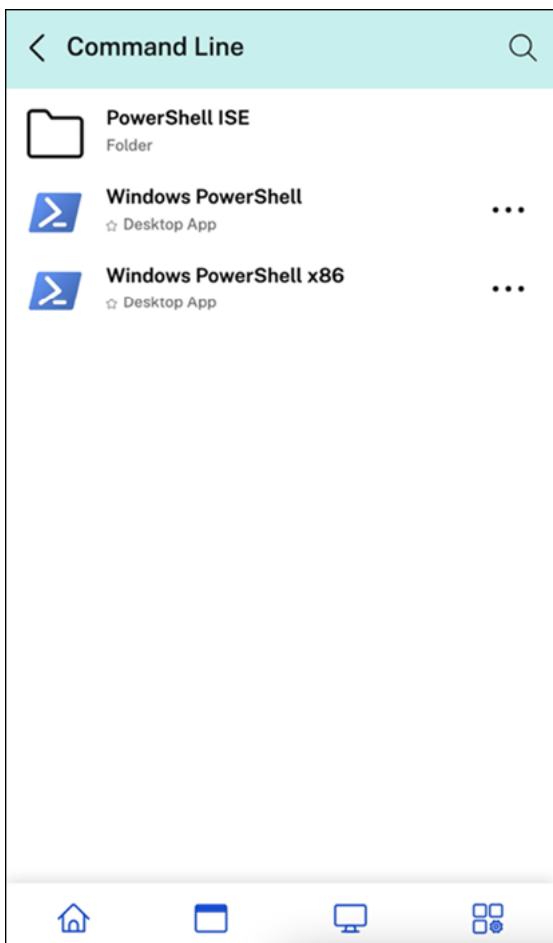
管理者が作成したプライマリカテゴリの数がユーザーの画面上で利用可能なスペースを超えると、ユーザーインターフェイスは画面サイズに基づいて調整され、カテゴリを [その他] ボックスの下に動的に移動します。ナビゲーションのブレッドクラムもユーザーに表示されます。



モバイルプラットフォームでは、[アプリ] タブに移動し、[カテゴリ] ボックスをクリックして、使用可能なカテゴリのリストを表示します。サブカテゴリはフォルダーとして表示され、フォルダーにはさらに管理構成に応じてサブフォルダーまたはアプリケーションが含まれます。



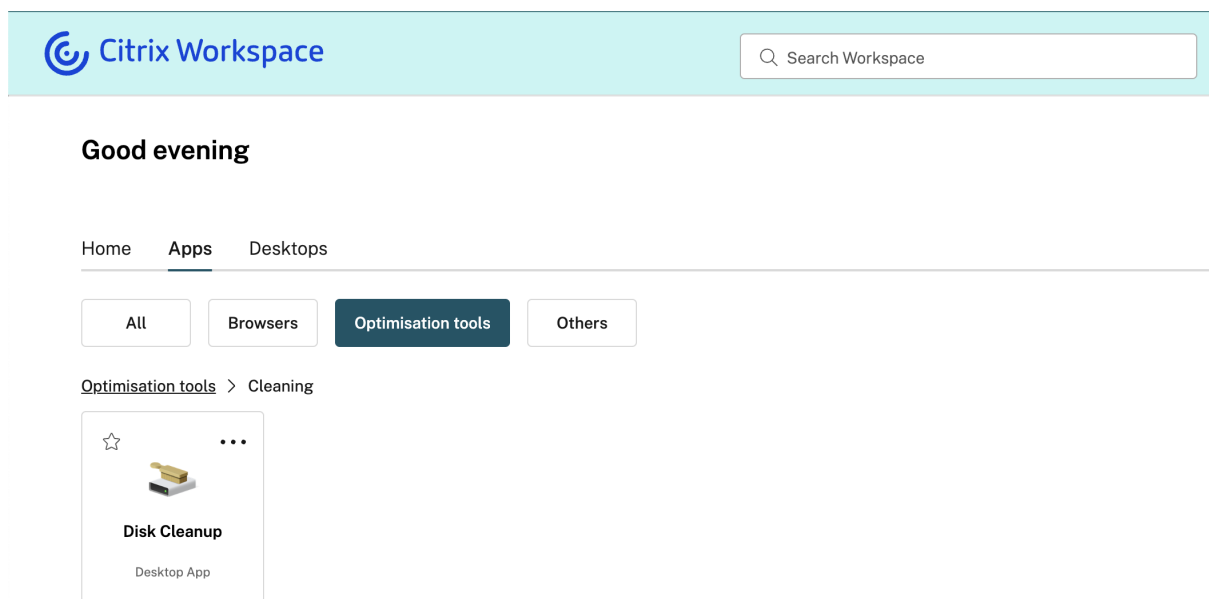
関連するカテゴリを選択すると、管理者が行った構成に基づいて、存在するサブカテゴリとアプリケーションのリストが表示されます。



フォルダーパスの追加

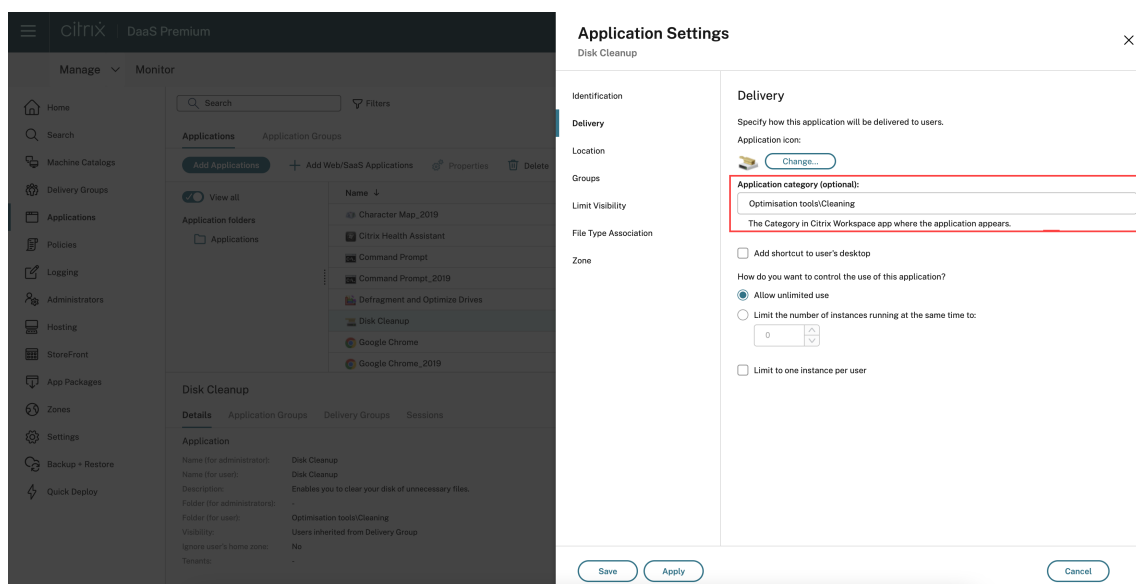
フォルダーパスは、アプリが表示されるカテゴリを定義するのに役立ちます。これは、エンドユーザーの画面に表示されるフォルダー構造を表します。

たとえば、フォルダーが **Optimisation tools/Cleaning** として定義されているアプリについて考えてみましょう。このアプリにアクセスするには、エンドユーザーは [Optimisation tools] > [Cleaning] に移動する必要があります。ここで、[Optimisation tools] はカテゴリであり、[Cleaning] はそのサブカテゴリです。



アプリケーションのフォルダーパスを定義するには、以下の手順を実行します：

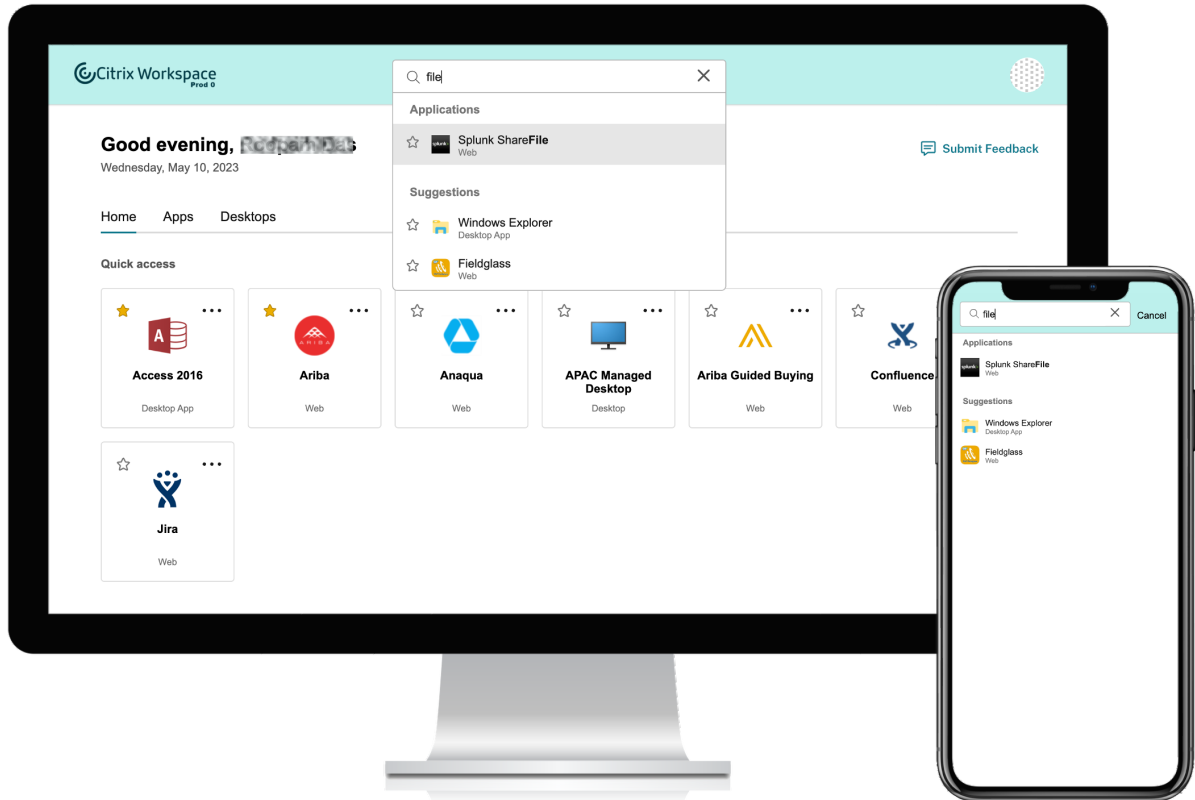
1. 管理クラウドコンソールで [**Citrix DaaS**] に移動します。
2. [アプリケーション] に移動し、アプリを見つけます。
3. アプリを右クリックして [プロパティ] を選択します。
4. [アプリケーションカテゴリ] フィールドで、フォルダーのパスを定義します。



5. [保存] をクリックします

強化された検索機能

強化された検索機能により、検索エンジンからより迅速な結果が得られます。[検索] オプションは使いやすさを考慮してツールバー内に表示され、ワークスペースアプリ内から迅速かつ直感的に検索を行うことができます。



これには次の改善が含まれます。

- デフォルトの検索では、最近使用した 5 つのアプリまたはデスクトップが表示されます
- 検索はスペルチェックで有効になり、オートコンプリート結果が表示されます
- 検索結果には、最近アクセスした仮想セッション内のアプリ、Web アプリ、SaaS アプリが含まれます
- 管理者が作成したカテゴリによる検索を実行する
- 検索結果の上部に [お気に入り] が表示されます

アクティビティマネージャー

October 12, 2023

アクティビティマネージャーは、ユーザーが効果的にリソースを管理するための、Citrix Workspace のシンプルかつ強力な機能です。あらゆるデバイスからアクティブなアプリやデスクトップに対するすばやいアクションを容易にすることで、生産性を向上させます。ユーザーはセッションをシームレスに操作でき、不要になったセッションを終了または切断してリソースを解放し、外出先でもパフォーマンスを最適化できます。

[アクティビティマネージャー] パネルには、現在のデバイスだけでなく、アクティブなセッションがあるリモートデバイス上の、アクティブなアプリとデスクトップの統合された一覧が表示されます。ユーザーは、デスクトップではプロファイルアイコンの横にあり、モバイルデバイスでは画面の下部にあるアクティビティマネージャーアイコンをクリックすると、この一覧を表示できます。

注:

暗いバナーテーマの中ではアクティビティマネージャーアイコンが見えない場合は、[バナーのテキストとアイコンの色] の設定で選択した色を変更してみてください。バナーとアクティビティマネージャーアイコンとのコントラストが低い場合、アイコンがはっきりと見えない場合があります。詳しくは、「[カスタムテーマを構成する](#)」を参照してください。

アクティビティマネージャーを有効にする

管理者は、エンドユーザーに対してアクティビティマネージャー機能を有効または無効にできるようになりました。組織のポリシーに従って、全ユーザー、または選択したユーザーおよびユーザーグループに対してこの機能を有効にすることができます。

注:

アクティビティマネージャー機能は、新しい UI でのみ有効にできます。新しい UI について詳しくは、「[新しいワークスペースユーザーインターフェイス \(プレビュー\)](#)」を参照してください。

アクティビティマネージャーを有効にするには、以下の手順に従います:

1. 管理コンソールで、[ワークスペース構成] > [カスタマイズ] > [機能] に移動します。
2. アクティビティマネージャーセクションで、トグルをオンにしてアクティビティマネージャーを有効にします。
3. 次に、以下のようにアクセス権限をカスタマイズできます。
 - すべてのエンドユーザーに対してアクティビティマネージャーを有効にするには、[全ユーザーに対して有効にする] を選択します。

New Activity Manager

Enabled

Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone

Enable for selected users and user groups

Save Preview

- 選択したユーザーおよびユーザーグループに対してアクティビティマネージャーを有効にするには、[選択したユーザーとユーザーグループに対して有効にする] を選択します。次に、ユーザーまたはユーザーグループが属するディレクトリを選択できます。適切なディレクトリを選択すると、関連するユーザーとユーザーグループを表示できます。

New Activity Manager

Enabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory: cldbl.com
Step 2: Select a user or group: Search users or user groups

Type	Display Name	Account Name ↑	
USER	[Redacted]	[Redacted]	🗑️
USER	[Redacted]	[Redacted]	🗑️

Save **Preview**

- すべてのユーザーに対してアクティビティマネージャーを無効にするには、トグルをオフにします。

New Activity Manager

Disabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory: cldbl.com
Step 2: Select a user or group: Search users or user groups

Type	Display Name	Account Name ↑	
USER	[Redacted]	[Redacted]	🗑️
USER	[Redacted]	[Redacted]	🗑️

Save **Preview**

4. [保存] をクリックします。

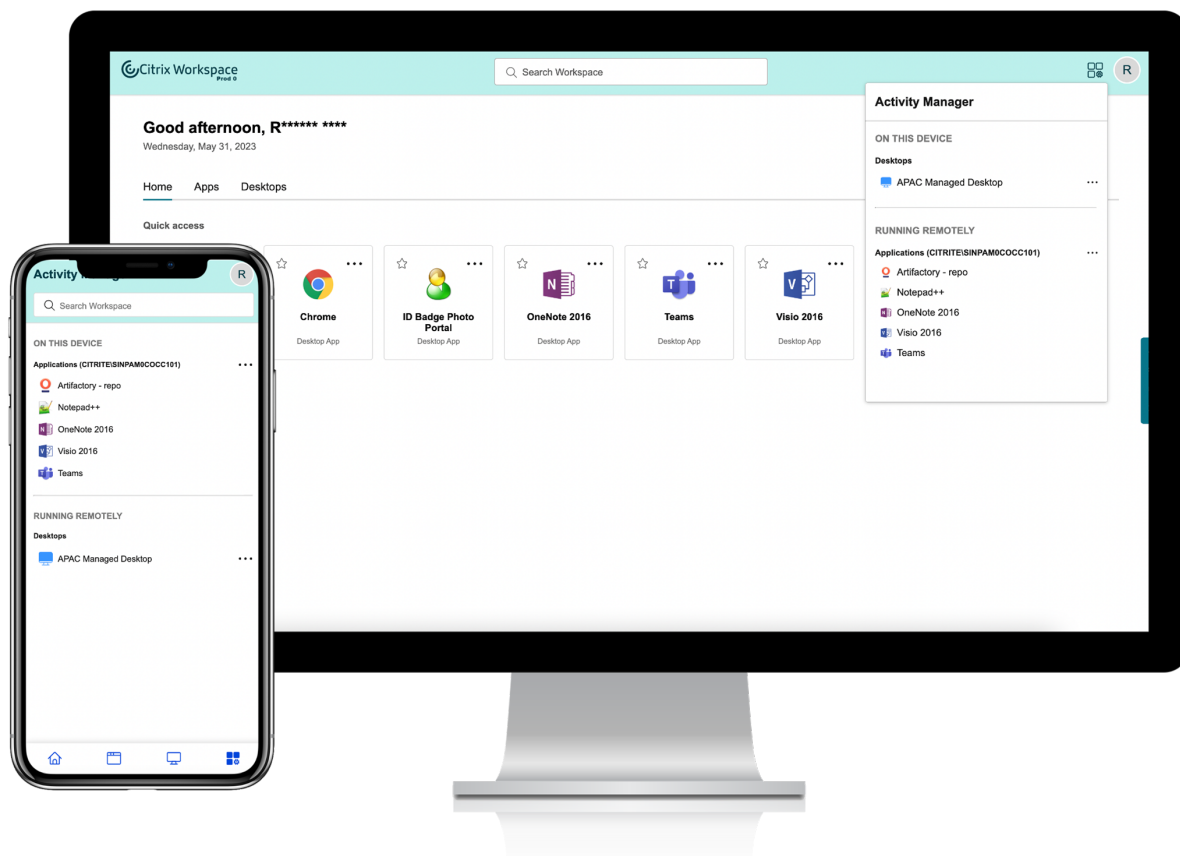
注:

この機能は、仮想アプリとデスクトップでのみサポートされます。Web アプリや SaaS アプリには適用されません。

アクティビティマネージャーの使用

アクティブなアプリとデスクトップは、アクティビティマネージャー上で次のようにグループ化されます。

- このデバイスでアクティブなアプリとデスクトップは、[このデバイス上] に1つのリストとしてグループ化されます。
- 他のデバイスでアクティブなアプリとデスクトップは、[リモートで実行] に1つのリストとしてグループ化されます。

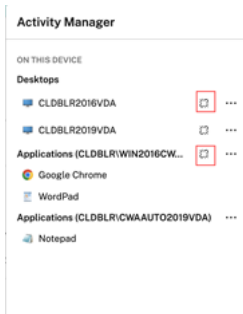


ユーザーは、それぞれの省略記号 (...) ボタンをクリックすることで、アプリまたはデスクトップ上で次のアクションを実行できます。

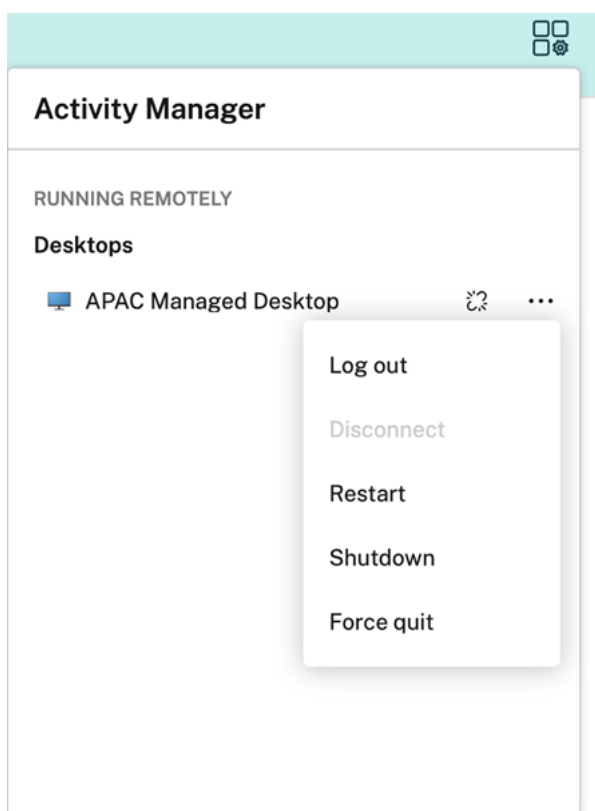
- 切断: リモートセッションは切断されますが、アプリとデスクトップはバックグラウンドでアクティブになっています。
- ログアウト: 現在のセッションからログアウトされます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン: 切断されたデスクトップを閉じます。
- 強制終了: 技術的な問題が発生した場合、デスクトップの電源を強制的に切ります。
- 再起動: デスクトップをシャットダウンし、再度起動します。

切断されたアプリとデスクトップ

アクティビティマネージャーにより、エンドユーザーはローカルまたはリモートにおいて切断モードで実行されているアプリとデスクトップを表示し、それらに対するアクションを実行できるようになりました。モバイルまたはデスクトップデバイスからセッションを管理できるため、エンドユーザーは外出先でもアクションを実行できます。切断されたセッションに対してログアウトやシャットダウンなどのアクションを実行すると、リソースの使用が最適化されるので、消費電力が削減されます。



- 切断されたアプリとデスクトップは [アクティビティマネージャー] パネルに表示され、切断状態を示すアイコンで示されます。
- 切断されたアプリはそれぞれのセッションの下にグループ化され、それらのセッションには切断状態を示すアイコンが表示されます。



エンドユーザーは、切断されたデスクトップに対し、[省略記号] をクリックすることで次のアクションを実行できます。

- ログアウト: これを使用すると、切断されたデスクトップからログアウトできます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン: このオプションを使用すると、切断されたデスクトップを閉じることができます。
- 電源オフ: 技術的な問題が発生した場合に、このオプションを使用すると、切断されたデスクトップの電源を強制的に切ることができます。
- 再起動: このオプションを使用すると、切断されたデスクトップをシャットダウンし、再度起動することができます。

切断されたセッションのアクティビティマネージャーにおける動作は、以下のようにさまざまです。

- ブラウザーを通じて Citrix ワークスペースにサインインし、ローカルセッションを切断すると、切断されたセッションはまず [このデバイス上] に表示されます。ただし、アクティビティマネージャーを閉じて再度開くと、切断されたセッションは [リモートで実行] の下に移動しています。
- ネイティブデバイスを介して Citrix Workspace アプリにサインインし、ローカルセッションを切断すると、切断されたセッションはリストから消えます。ただし、アクティビティマネージャーを閉じて再度開くと、切断されたセッションは [リモートで実行] の下に移動しています。

Citrix Workspace を使用して DaaS と Virtual Apps and Desktops を配信する

October 12, 2023

Citrix Workspace は、Citrix DaaS のアプリとデスクトップを集約するシングルテナントのオンプレミスアプリリストアである [StoreFront](#) に代わる、マルチテナントクラウドサービスです。Citrix Workspace プラットフォームは、Citrix Workspace を介したリモート作業、拡張性、およびカスタマイズに必要なツール、サービス、および機能を提供する、クラウドコンポーネントです。

Citrix Workspace には、DaaS を集約するためのさまざまなオプションがあります。選択するオプションは、以下のことに依存します:

- クラウドに完全に移行するか、ハイブリッドソリューションを採用するか。
- DaaS への外部アクセスを許可する予定があるかどうか。

クラウドへの完全な移行

オンプレミス構成をクラウドに移行することで、IT 管理インフラストラクチャを Citrix 管理環境に移行すれば、利用者が Workspace を介して DaaS にアクセスできるようにすることができます。クラウドへの完全な移行は、管理するコンポーネントが少なくなることを意味します。

自動構成ツールを使用して、1 つまたは複数のオンプレミスサイトからクラウドサービスへの移行プロセスを簡素化することをお勧めします。このプロセスの主な手順は次のとおりです：

1. 「構成を移行するための前提条件」を満たしているかを確認します。
2. オンプレミス構成をエクスポートします。このプロセスについては、「[Citrix Virtual Apps and Desktops オンプレミス構成のエクスポート](#)」を参照してください。
3. 構成をクラウドにインポートします。このプロセスについては、「[Citrix DaaS への構成のインポート](#)」を参照してください。

自動構成について詳しくは、「[クラウドへの移行](#)」と [Tech Zone の展開ガイド](#) を参照してください。

ハイブリッドソリューションのサイトアグリゲーション

既存のオンプレミスの Virtual Apps and Desktops 展開で Citrix Workspace に移行できます。このプロセスはサイトアグリゲーションと呼ばれ、IT 管理のインフラストラクチャを Citrix 管理のインフラストラクチャに置き換えます。

サイトアグリゲーションで Workspace に徐々に移行することを選択するか、あるいはクラウド内のすべてではなく一部のコンポーネントをホストするハイブリッドソリューションが必要な場合があります。ハイブリッドモデルを選択すると、オンプレミスのリソースとともにクラウド容量を管理でき、クラウドに完全に移行することなく、統合されたエンドユーザーエクスペリエンスを提供できます。

サイトアグリゲーションを使用して StoreFront から Workspace に移行する前に、Active Directory (AD) を構成し、Cloud Connector をリソースの場所にインストールする必要があります。

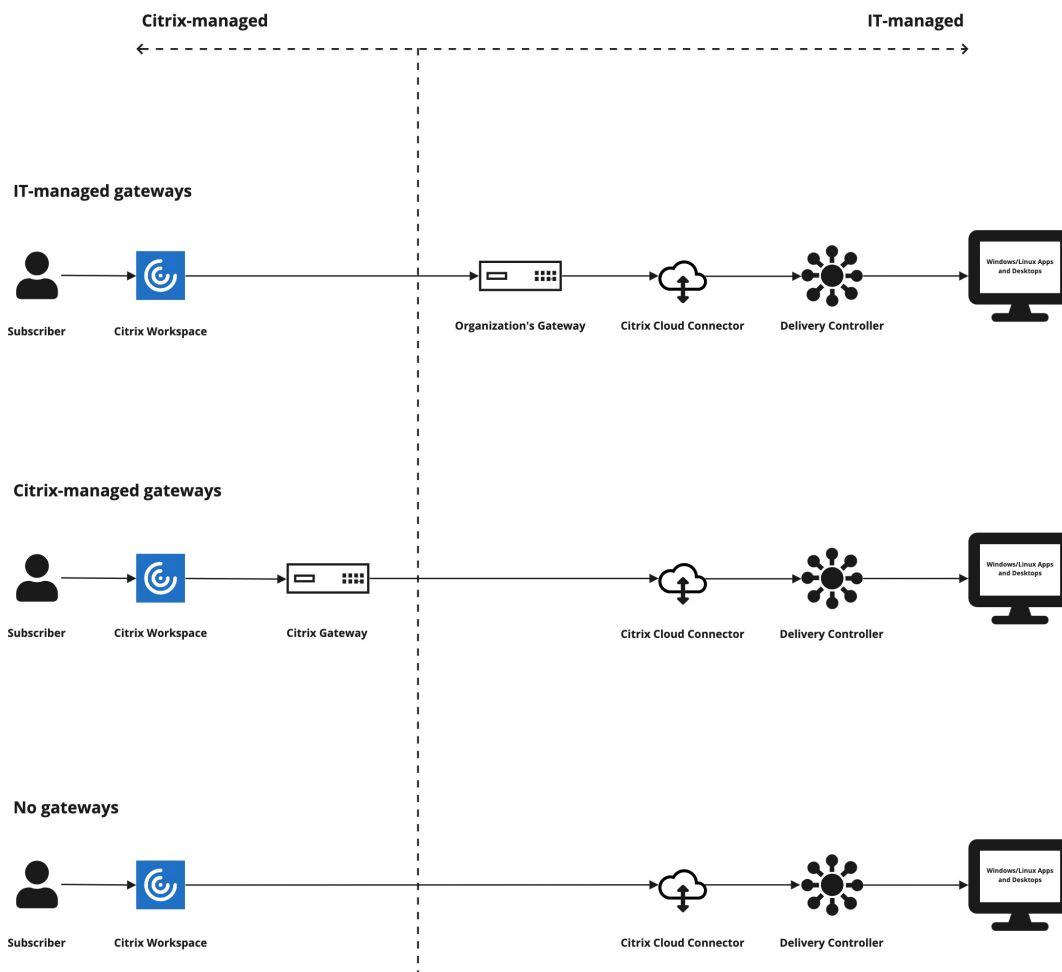
サイトアグリゲーションには、大きく分けて 3 つの手順があります：

1. サイトを見つけます。サイトは、実稼働環境を形作るコンポーネントで構成されます。場所や支店ごとに異なるサイトがある場合があります。
2. **Active Directory (AD)** の接続を確認します。利用者は、AD を使用して Citrix Workspace に認証する必要があります。Cloud Connector がインストールされている AD ドメインを検出して、利用者が認証できることを確認します。
3. 展開の種類を選択します。この手順には、次の 3 つの接続オプションがあります：
 - IT 管理のゲートウェイ
 - Citrix 管理のゲートウェイ
 - ゲートウェイなし

詳しくは、「[接続オプション](#)」を参照してください。

接続オプション

次の 3 つのオプションは、Citrix Workspace を介した DaaS へのアクセスを提供します。これらは、さまざまなビジネス要件に合わせて設計されています。



接続オプション

シナリオ

従来の（IT 管理の）ゲートウェイ

DaaS への外部接続に独自のゲートウェイを使用する場合は、このオプションを選択します。このオプションを使用すれば、オンプレミスのゲートウェイに投資してきた分を活用できます。

Citrix 管理のゲートウェイ

Virtual Apps and Desktops への外部接続に **Citrix Gateway** サービスを使用する場合は、このオプションを選択します。クライアントと VDA との間の HDX 接続は、**Citrix Gateway** サービスによりプロキシされません。

ゲートウェイなし（内部のみ）

利用者が社内ネットワーク内のクライアントのみを使用して DaaS を起動するように設定する場合は、このオプションを選択します。このオプションを選択した場合、利用者は DaaS に外部アクセスできなくなります。

サイトアグリゲーションのプロセスと手順については、「[オンプレミスの Virtual Apps and Desktops をワークスペースに集約](#)」を参照してください。

ワークスペースの回復性と最適化を構成する

Citrix Workspace を使用して、DaaS の効率と可用性を向上させる方法については、「[Citrix Workspace での DaaS の最適化](#)」を参照してください。以下を行う方法についての説明があります：

- 直接ワークロード接続で接続を最適化する。
- オフラインの回復力のために、停止時のサービス継続性を確保する。
- Citrix フェデレーション認証サービス（FAS）を使用した Virtual Apps and Desktops へのシングルサインオン（SSO）を構成する。

ワークスペースへのアクセスを構成する

November 28, 2023

ワークスペースにアクセスするには、最新バージョンの Citrix Workspace アプリを使用することをお勧めします。Citrix Workspace アプリは Citrix Receiver に代わるサービスです。Workspace URL を使用して、最新バージョンの Microsoft Edge、Google Chrome、Mozilla Firefox、または Apple Safari でワークスペースにアクセスすることもできます。

本記事では、構成と使用などの手順を要約しています：

- [Workspace URL](#)
- [Citrix Workspace アプリ（旧称 Citrix Receiver）](#)。
- [外部接続用の Citrix Gateway](#) または [Citrix Gateway サービス](#)。
- [ワークスペースへの認証用の ID プロバイダー](#)。

概要

利用者は、Workspace URL を使用してブラウザーで、またはデバイスにインストールした Citrix Workspace アプリで、Citrix Workspace にアクセスできます。

Workspace URL はカスタマイズでき、デフォルトで有効になっています。Workspace URL の編集手順については、本記事の「[Workspace URL](#)」を参照してください。

Citrix Workspace アプリは、Workspace ユーザーインターフェイス (UI) へのアクセスを提供するネイティブインストールされたアプリであり、Citrix Receiver に代わるサービスです。Citrix Workspace アプリについてと Citrix Receiver からの移行については、本記事の「[Citrix Workspace アプリ \(旧称 Citrix Receiver\)](#)」を参照してください。

Citrix Gateway または Citrix Gateway サービスとの外部接続を構成すると、リモートの利用者はワークスペースへの外部アクセスを取得できます。ワークスペースへのリモートアクセスを有効にする方法については、本記事の「[外部接続](#)」を参照してください。

また、内部接続の場合のみ、顧客が単独で Citrix Workspace を使用する、またはオンプレミス StoreFront をホストすることができます。内部接続の場合、エンドポイントは Virtual Delivery Agent (VDA) の IP アドレスに直接接続する必要があります。

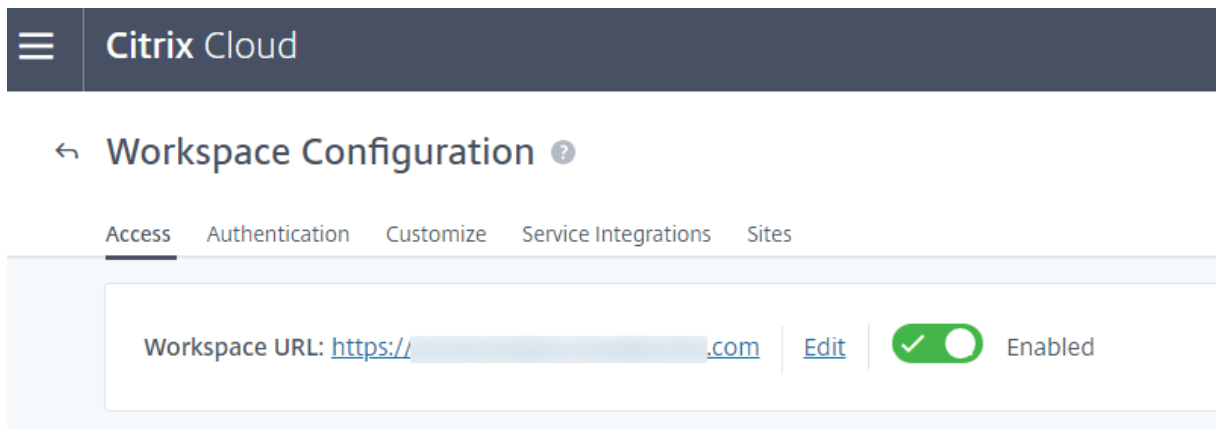
Citrix Workspace でサポートされる ID プロバイダーは増え続け、この ID プロバイダーにより、利用者は Citrix Cloud に接続し、[ワークスペースの構成] を有効にして、ワークスペースに認証できます。ワークスペース利用者の認証の構成については、本記事の「[ワークスペースへの認証](#)」を参照してください。

Citrix Workspace は、次の認証オプションもサポートしています：

- 認証の 2 番目の要素としてのトークン。これにより、Active Directory でワークスペースにサインインできます。ワークスペースへの多要素認証 (MFA) の設定について詳しくは、「[2 要素認証](#)」を参照してください。
- Citrix フェデレーション認証サービス (FAS) は、Citrix Workspace で DaaS へのシングルサインオン (SSO) を提供します。FAS を使用した SSO の設定について詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

ワークスペース URL

Workspace URL を使用する準備ができていたら、[**Citrix Cloud**] > [ワークスペース構成] > [アクセス] で、Workspace URL を有効化、編集、および無効化できます。



ワークスペース URL のカスタマイズ

Workspace URL の最初の部分はカスタマイズできます。たとえば、<https://example.cloud.com>から<https://newexample.cloud.com>に URL を変更することができます。

Workspace URL は、有効になっている場合にのみ変更できます。URL が無効になっている場合は、最初に再度有効にする必要があります。

Workspace URL を有効にするには、[ワークスペース構成] > [アクセス] に移動し、トグルを選択してオンにします。Workspace URL が再度有効になるまでに、最大で 10 分かかる場合があります。

Workspace URL の最初の部分は、Citrix Cloud アカウントを使用している組織を表し、[Cloud Software Group のエンドユーザーサービス契約](#)に準拠している必要があります。商標を含む第三者の知的財産権の不正使用は、URL の取り消しおよび再割り当て、または Citrix Cloud アカウントの停止を招く可能性があります。

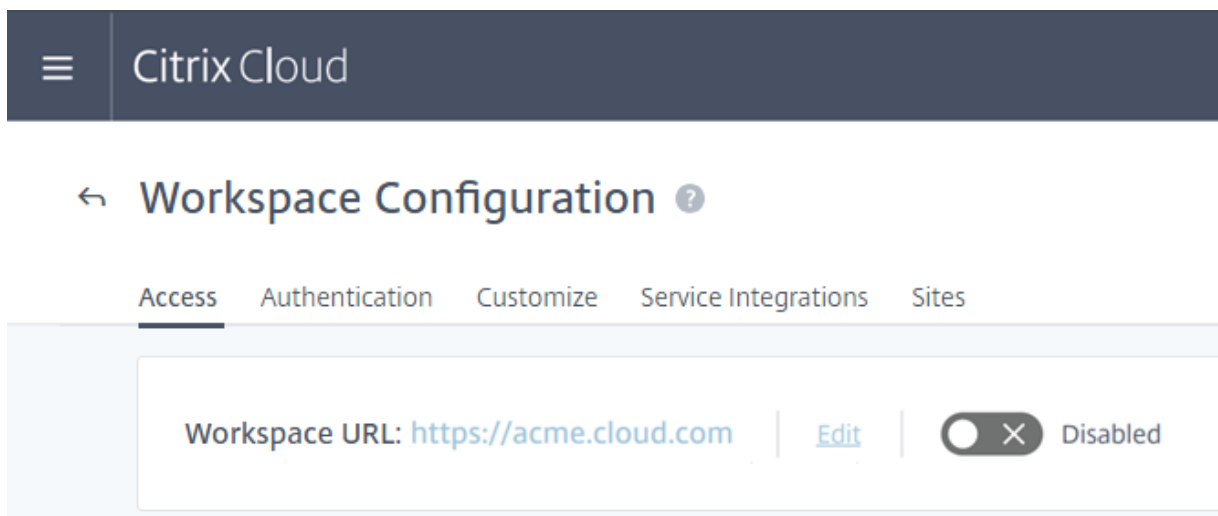
URL をカスタマイズするには、[ワークスペース構成] > [アクセス] に移動し、[編集] を選択します。URL のカスタマイズ可能な部分については以下の制限があります：

- 6～63 文字の長さである必要があります。6 文字未満に変更する場合は、Citrix Cloud でチケットを開きます。
- 文字と数字だけで構成する必要があります。
- Unicode 文字は使用できません。

URL の名前を変更すると、古い URL は直ちに削除され、使用できなくなります。新しい URL を利用者に知らせ、新しい URL を使用できるようにすべてのローカルの Citrix Workspace アプリを手動で更新します。

Workspace URL の無効化

Workspace URL を無効にして、ユーザーが Citrix Workspace を使用して認証できないようにすることができます。たとえば、利用者がオンプレミスの StoreFront URL を使用してリソースにアクセスするようしたり、メンテナンス中にアクセスを禁止したりできます。



Workspace URL が無効になるまでに、最大で 10 分かかる場合があります。

ワークスペース URL を無効にすると、次のようになります：

- すべてのサービス統合が無効になります。利用者は、Citrix Workspace のサービスでデータおよびアプリケーションにアクセスできません。
- Workspace URL はカスタマイズできません。URL を変更する前に、URL を再度有効にする必要があります。
- URL にアクセスすると、ワークスペースが見つからない、またはリソースを読み込めないことを示すメッセージがブラウザーに表示されます。

Citrix Workspace アプリ（旧称 Citrix Receiver）

重要：

Citrix Receiver は製品終了（EoL: End of Life）となり、サポートも終了しました。Citrix Receiver を引き続き使用する場合、テクニカルサポートは「[ライフサイクルマイルストーンと定義](#)」で説明されているオプションに限定されます。プラットフォームごとの Citrix Receiver の EoL マイルストーンについては、「[Citrix Workspace アプリおよび Citrix Receiver のライフサイクルマイルストーン](#)」を参照してください。

Citrix Workspace アプリは、Citrix Receiver に代わるワークスペースにアクセスするためのネイティブインストールされたアプリです。

Citrix Workspace アプリでサポートされている認証方法

次の表に、Citrix Workspace アプリでサポートされている認証方法を示します。この表には、Citrix Workspace アプリが受け継ぐ Citrix Receiver の特定のバージョンに関連する認証方法が記載されています。

Citrix Workspace アプリ	Active Directory 認証	Active Directory+ トークン認証	Azure Active Directory 認証
Windows 向け Citrix Workspace	はい	はい	サポート（Workspace アプリ、Receiver 4.9 LTSR CU2 以降、Receiver 4.11 CR 以降のみ）
Linux 向け Citrix Workspace	はい	はい	サポート（Workspace アプリ、Receiver 13.8 以降のみ）
Mac 向け Citrix Workspace	はい	はい	はい
iOS 向け Citrix Workspace アプリ	はい	はい	はい

Citrix Workspace アプリ	Active Directory 認証	Active Directory+ トークン認証	Azure Active Directory 認証
Android 向け Citrix Workspace	はい	はい	サポート (Workspace アプリ、Receiver3.13 以降のみ)

プラットフォームごとの Citrix Workspace アプリでサポートされている機能については、「[Workspace アプリの機能マトリックス](#)」を参照してください。

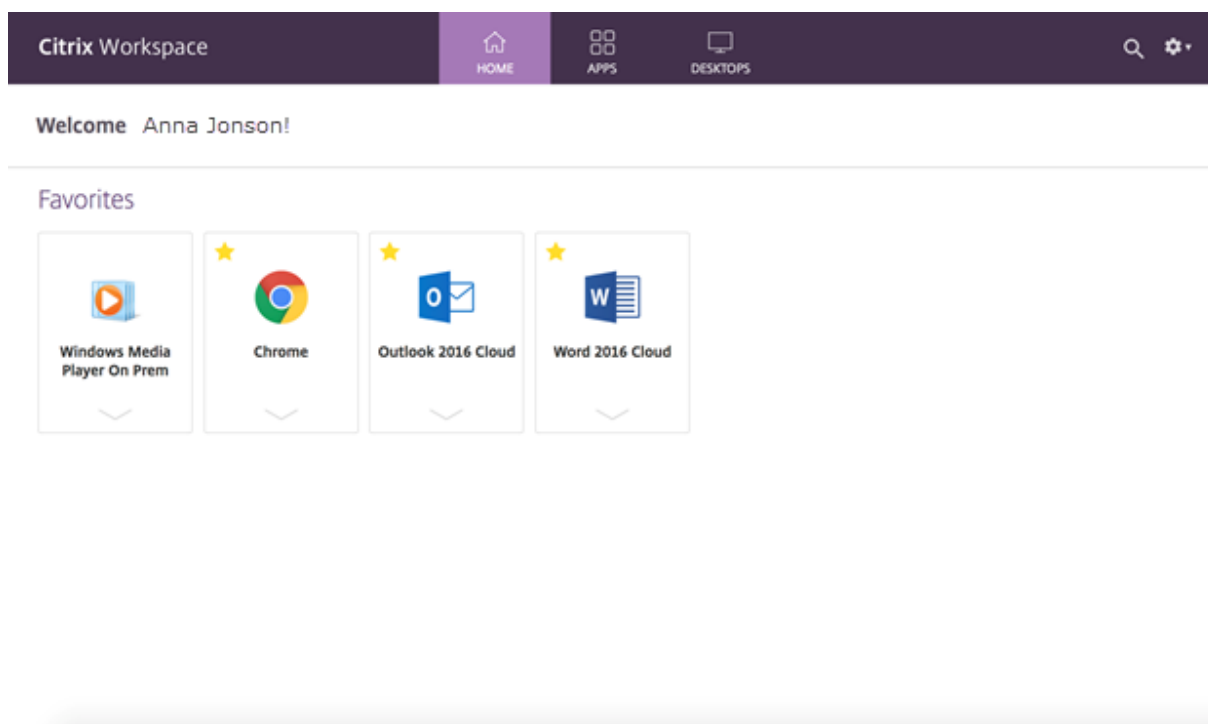
Citrix Receiver での TLS および SHA2 サポートの概要については、[CTX23226](#)のサポート記事を参照してください。

Citrix Receiver から Citrix Workspace アプリへの移行

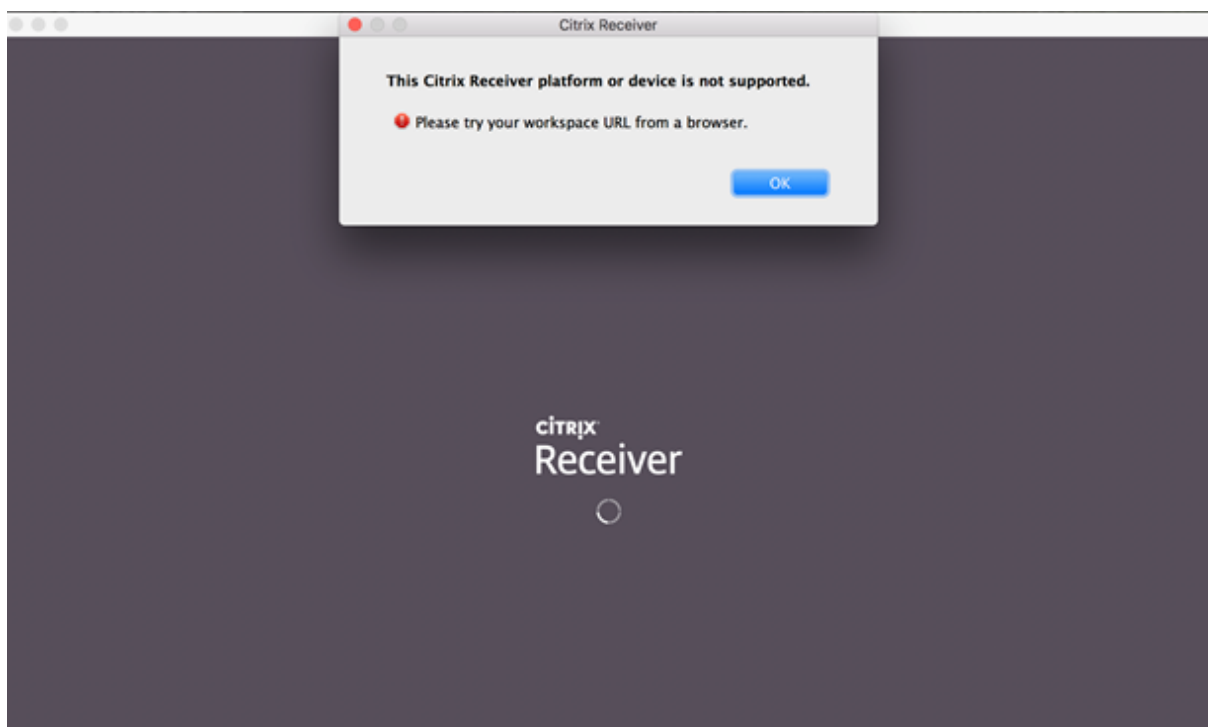
Citrix Workspace アプリは、Citrix Receiver の機能を受け継いで拡張しています。

Citrix Workspace アプリで、利用者は SaaS、Web、および仮想アプリにシングルサインオン (SSO) でアクセスできます。ワークスペース利用者のシングルサインオンについては、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

このアクセス制御機能は、Citrix Receiver ではサポートされていません。したがって、同じサービスとアクセス制御を有効にしても、Citrix Receiver ユーザーには紫色の UI が表示されますが、Web アプリと SaaS アプリは表示されません。また、**Files** は Citrix Receiver でサポートされておらず、利用者はこの方法でアクセスできません。



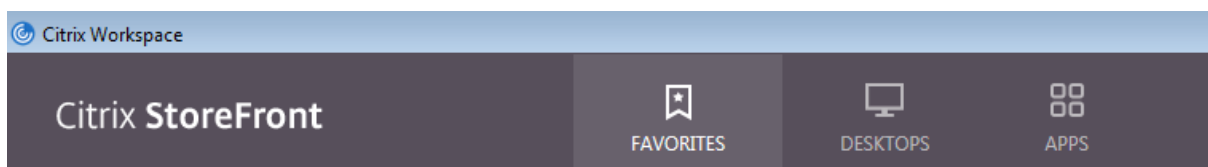
Azure Active Directory (AAD) も Citrix Receiver と互換性がありません。認証方法として AAD が有効になっているときに利用者が Citrix Receiver を使用して Workspace にアクセスしようとすると、デバイスがサポートされていないというメッセージが表示されます。Citrix Workspace アプリにアップグレードすると、利用者が自分のワークスペースにアクセスできるようになります。



Citrix Workspace アプリにアップグレードする（または Web ブラウザーを使用する）顧客には、新しい UI が表示されます。この UI の利用者エクスペリエンスについては、「[ワークスペース環境の管理](#)」を参照してください。

新しい UI を除いて、Citrix Workspace アプリを使用すると、利用者は有効にしたすべての新機能を使用できます。利用者は、Citrix Gateway サービスを介して、**Files** にアクセスしたり、DaaSを確認したり、Web アプリと SaaS アプリにアクセスしたりできます。

StoreFront（オンプレミス）展開の場合、Citrix Receiver から Citrix Workspace アプリにアップグレードすると、アイコンが変更されて Citrix Workspace アプリが開きます。



注:

[Citrix Cloud Government](#) ユーザーには、Citrix Workspace アプリを使用しているとき、または Web ブラウザーから Workspace にアクセスしているときに、引き続き紫色の UI が表示されます。

外部接続

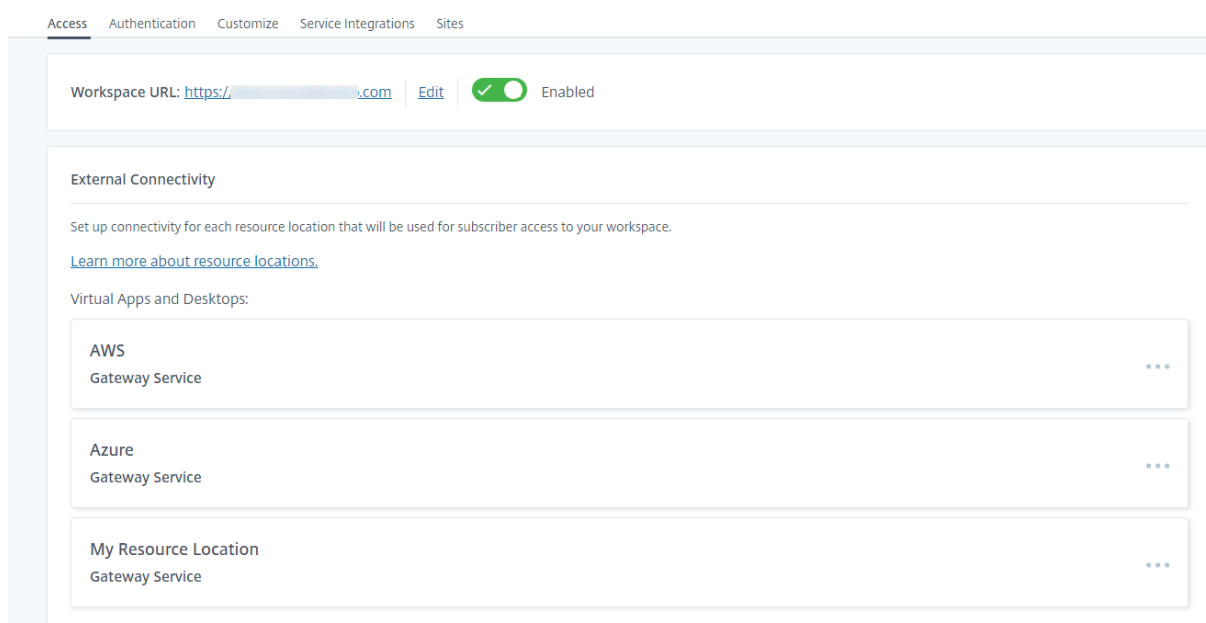
Citrix Gateway または Citrix Gateway サービスをリソースの場所に追加することにより、リモートの利用者にセキュアなアクセスを提供します。

Citrix は、以下の外部接続オプションをサポートしています：

- Citrix が Citrix Gateway および Citrix ADC をホストします
- 顧客が Citrix Gateway およびオンプレミス Citrix ADC をホストします

Citrix Gateway は、[ワークスペース構成] > [アクセス] > [外部接続] または **[Citrix Cloud]** > [リソースの場所] で追加できます。

Workspace Configuration



注：

[ワークスペース構成] > [アクセス] ページの [外部接続] は、Citrix Virtual Apps Essentials では使用できません。Citrix Virtual Apps Essentials サービスは Citrix Gateway サービスを使用しているため、追加の構成は必要ありません。

ワークスペースへの認証

利用者のワークスペース認証の構成は、2 段階のプロセスです：

1. **[ID およびアクセス管理]** で、1 つまたは複数の ID プロバイダーを定義します。手順については、「[ID およびアクセス管理](#)」を参照してください。

2. [ワークスペース構成] で、利用者がワークスペースにサインインするために使用する認証方法として、構成した ID プロバイダーのいずれかを選択します。手順については、「[認証方法の選択または変更](#)」を参照してください。

[ID およびアクセス管理] で複数の ID プロバイダーを構成すると、利用者がワークスペースにサインインする方法について、[ワークスペース構成] で選択できるオプションが増えます。

利用者認証でサポートされている ID プロバイダー

利用者は、次のいずれかの方法で、ワークスペースに対して認証できます：

- [Active Directory](#)
- [Active Directory+ トークン](#)
- [Azure Active Directory](#)
- [Citrix Gateway](#)
- [Okta](#)
- [SAML 2.0](#)
- [Google](#)

ワークスペースへの利用者認証でサポートされている方法について詳しくは、「[セキュアなワークスペース](#)」を参照してください。

Active Directory (AD) では、オンプレミスの AD ドメインに少なくとも 2 つの Citrix Cloud Connector がインストールされている必要があります。Citrix Cloud Connector については、「[Citrix Cloud Connector](#)」を参照してください。

AD+ トークンは、ワークスペースへの利用者認証に使用されるデフォルトの ID プロバイダーです。利用者は、Citrix SSO などの [時間ベースのワンタイムパスワード \(TOTP\) 標準](#) に従うアプリケーションを使用して、認証の第 2 要素としてトークンを生成します。トークンベースの 2 要素認証の設定については、「[2 要素認証](#)」を参照してください。

ID プロバイダーの変更

[ワークスペース構成] で、Citrix Workspace のプライマリ認証方法として ID プロバイダーを選択します。選択する ID プロバイダーは、最初に [ID およびアクセス管理] で構成する必要があります。[ワークスペース構成] で ID プロバイダーを変更しても、[ID およびアクセス管理] で構成した ID プロバイダーには影響しません。

[ID およびアクセス管理] で ID プロバイダーを構成しても、Citrix Workspace にサインインするためのプライマリ認証方法は変更されません。Citrix Workspace にサインインするためのプライマリ認証方法を変更するには、次のことを行う必要があります：

1. [ID およびアクセス管理] で、新しい ID プロバイダーを構成します。
2. [ワークスペース構成] で ID プロバイダーを変更します。

実稼働環境に影響を与えずに、Citrix Workspace のプライマリ認証方法を構成および変更できます。新しい ID プロバイダーをテストする場合は、テスト用の Citrix Cloud 組織を作成するか、利用者がワークスペースを使用していないときに [ワークスペース構成] で認証方法を変更することを検討します。

SaaS および Web アプリへのシングルサインオン (SSO)

Citrix Workspace は、利用者がワークスペースにサインインした後、セカンダリリソースにシングルサインオン (SSO) できるようにすることで、シームレスなエクスペリエンスを提供します。Citrix Gateway サービスと連携して、Citrix Secure Private Access は、Citrix Workspace に統合された一部として SaaS および Web アプリへの SSO を提供します。

SSO 機能のほかに、Citrix Secure Private Access を使用すると、機能強化されたセキュリティポリシーを設定し、コンテキストに基づくアクセスを構成し、分析用データを収集できます。Citrix Secure Private Access について詳しくは、「[Citrix Secure Private Access](#)」を参照してください。

DaaS へのシングルサインオン (SSO)

SaaS と Web アプリのほか、Active Directory (AD) と AD+ トークンでは既に、利用者がワークスペースにサインインした後の DaaS アプリとデスクトップへの SSO を提供しています。

Citrix Workspace への利用者の初期認証に別の ID プロバイダーを選択した場合は、Citrix フェデレーション認証サービス (FAS) をインストールして構成することもできます。FAS を使用すると、SaaS や Web アプリの場合と同様に、利用者は資格情報を 1 回入力するだけで DaaS にアクセスできます。

通常、FAS は、Workspace 認証に以下の ID プロバイダーのいずれかを使用している場合に採用されます：

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

注：

Citrix Gateway の構成方法によっては、DaaS への SSO に FAS が必要ない場合があります。Citrix Gateway の構成について詳しくは、「[オンプレミスの Citrix Gateway での OAuth ID プロバイダーポリシーの作成](#)」を参照してください。

FAS について詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

追加情報

- [Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)

- [リファレンスアーキテクチャ: フェデレーション認証サービス](#)
- [Tech Insight: フェデレーション認証サービス](#)

カスタムドメインの構成

November 28, 2023

ワークスペースのカスタムドメインを構成すると、選択したドメインを使用して Citrix Workspace ストアにアクセスできるようになります。これにより、割り当てられた cloud.com ドメインの代わりにこのドメインを使用して、Web ブラウザーと Citrix Workspace アプリケーションの両方からアクセスできるようになります。

カスタムドメインは、他の Citrix Workspace の顧客と共有することはできません。各カスタムドメインはその顧客に固有である必要があります。後でカスタムドメインを削除する場合を除き、必ず別の顧客に割り当てることがないカスタムドメインを選択してください。

Citrix Cloud 内で Workspace URL を無効にしても、カスタムドメインを介した Citrix Workspace へのアクセスは無効になりません。カスタムドメインの使用時に Citrix Workspace へのアクセスを無効にするには、カスタムドメインも無効にします。

サポートされているシナリオ

シナリオ	サポート対象	未サポート
ID プロバイダー	AD (+Token)、Azure AD、Citrix Gateway、Okta、および SAML	Google
リソースの種類	Virtual Apps and Desktops	SaaS アプリ
アクセス方法	ブラウザ（Internet Explorer を除く）、Windows、Mac、Linux 向け Citrix Workspace アプリ、iOS アプリ	-
使用状況	ワークスペース	Cloud Connector とクラウド管理者コンソール

現在のカスタム **Workspace URL** との違いは何ですか？

顧客に対してカスタム Workspace URL がすでに有効になっている場合は、次のビューが表示されます。

当面はこの URL を使用できますが、このドキュメントの手順に進んで別のカスタム Workspace URL をオンボードすることができます。将来的には廃止される予定です。

同じ URL を使用する場合は、以前のカスタム Workspace URL を削除し、DNS レコードを削除して続行します。

前提条件

- 新しく登録したドメイン、またはすでに所有しているドメインを選択できます。ドメインはサブドメイン形式 (your.company.com) である必要があります。Citrix は、ルートドメイン (company.com) のみの使用をサポートしていません。
- Citrix では、Citrix Workspace アクセス用のカスタムドメインとして専用ドメインを使用し、必要に応じて簡単に変更できるようにすることをお勧めします。
- カスタムドメインには Citrix の商標を含めることはできません。Citrix の商標の完全なリストについては、[こちら](#)をご覧ください。
- 選択するドメインはパブリック DNS で構成されている必要があります。ドメイン構成に含まれる CNAME レコード名と値はすべて、Citrix によって解決可能である必要があります。

注:

プライベート DNS 構成はサポートされていません。

- ドメイン名の長さは 64 文字以内にする必要があります。

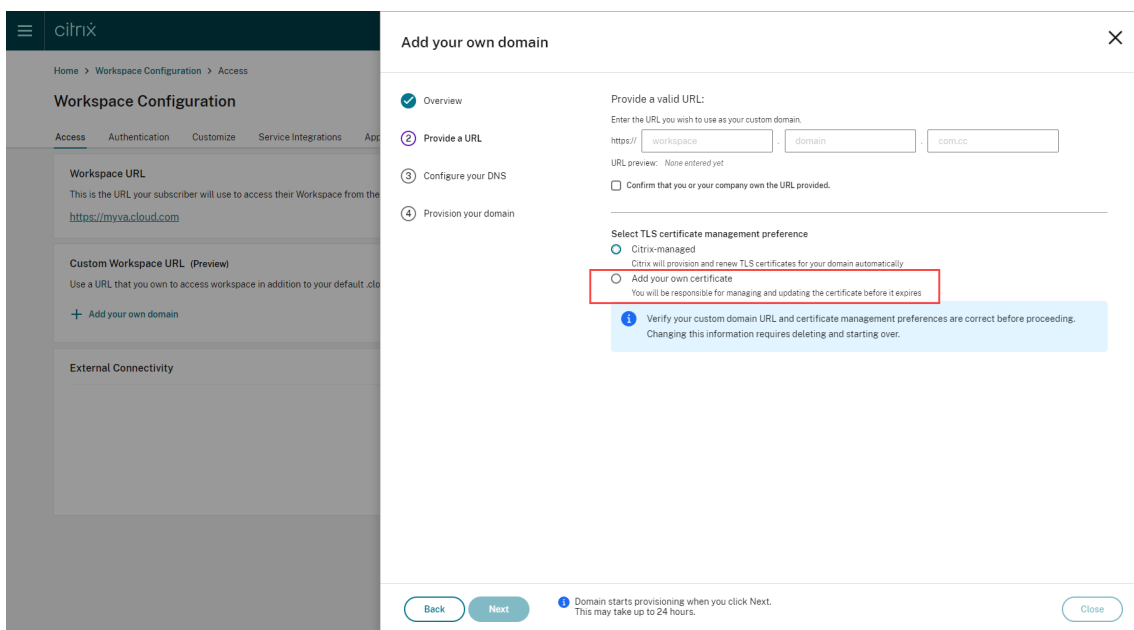
カスタムドメインの構成

カスタムドメインを設定すると、URL や証明書の種類を変更することはできません。削除することしかできません。選択したドメインがまだ DNS で構成されていないことを確認してください。カスタムドメインを構成する前に、既存の **CNAME** レコードをすべて削除してください。

SAML を使用して ID プロバイダーに接続している場合は、SAML 構成を完了するために追加の手順を実行する必要があります。詳細については、「[SAML](#)」を参照してください。

カスタムドメインの追加

1. <https://citrix.cloud.com> で Citrix Cloud にサインインします。
2. Citrix Cloud メニューから [ワークスペース構成] を選択し、[アクセス] を選択します。
3. [アクセス] タブの [カスタム **Workspace URL**] で、[+ 独自のドメインを追加] を選択します。

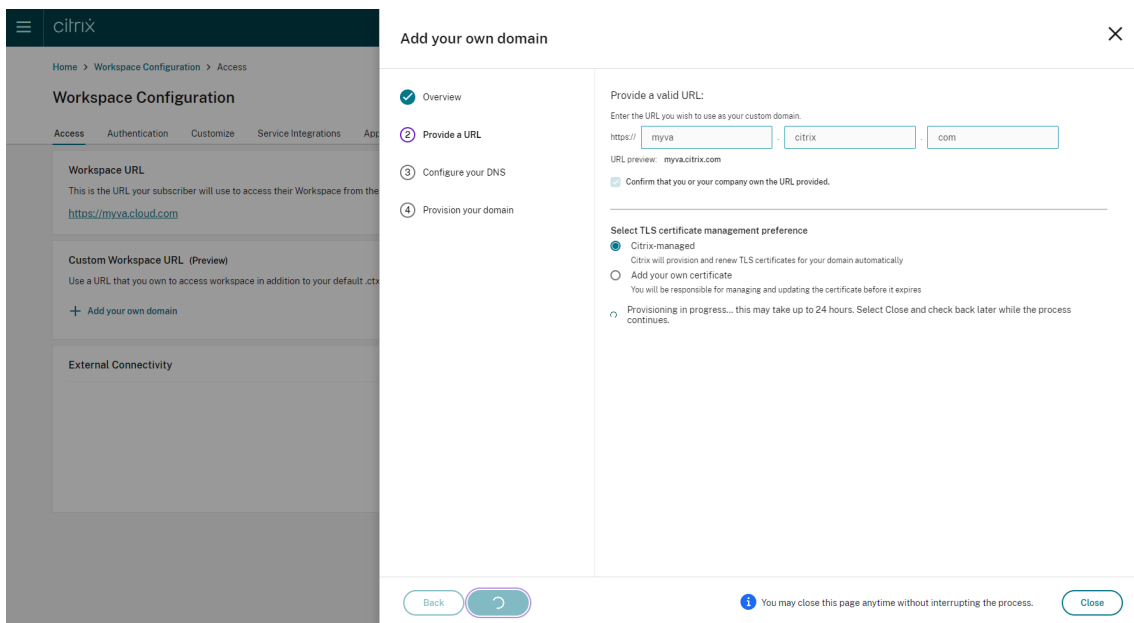


4. [概要] ページに表示される情報を読み、[次へ] を選択します。
5. [URL を指定する] ページに選択したドメインを入力します。[指定された URL を自分または会社が所有していることを確認する] を選択して、指定したドメインを所有していることを確認し、TLS 証明書管理設定を選択します。Citrix は、証明書の更新が自動的に処理される管理型をお勧めします。詳しくは、「更新された証明書の提供」を参照してください。[次へ] をクリックします。

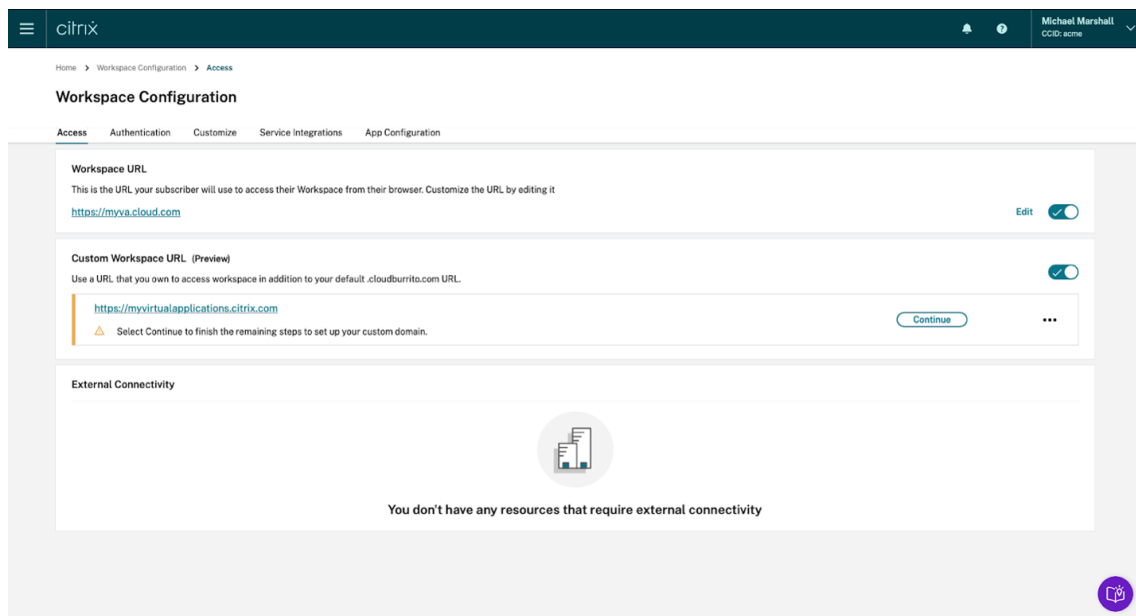
このページに警告が表示された場合は、強調表示された問題を修正して続行します。

独自の証明書を提供することを選択した場合は、手順にある追加の手順を完了する必要があります。

選択したドメインのプロビジョニングには時間がかかります。プロビジョニングの進行中は、ページを開いたまま待つことも、ページを閉じることもできます。



6. プロビジョニングの完了中に [URL を指定する] ページを開いている場合は、[DNS を構成する] ページが自動的に開きます。ページを閉じた場合は、[アクセス] タブからカスタムドメインの [続行] ボタンを選択します。

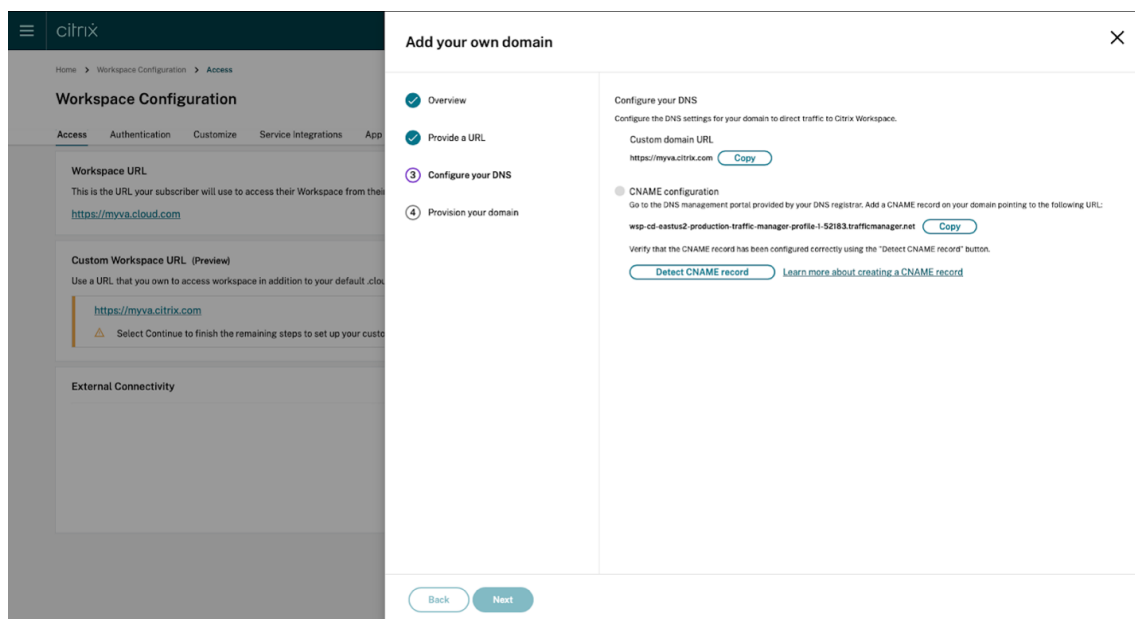


7. この手順は、DNS レジストラが提供する管理ポータルで実行します。自分に割り当てられた Azure Traffic Manager を指す、選択したカスタムドメインの **CNAME** レコードを追加します。

[DNS を構成する] ページからトラフィックマネージャーのアドレスをコピーします。例のアドレスは次のとおりです。

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

DNS に証明機関承認 (CAA) レコードが構成されている場合は、*Let's Encrypt* がドメインの証明書を生成できるようにするレコードを追加します。*Let's Encrypt* は、Citrix がカスタムドメインの証明書を生成するために使用する証明機関 (CA) です。CAA レコードの値は次のようにする必要があります: *0 issue "letsencrypt.org"*

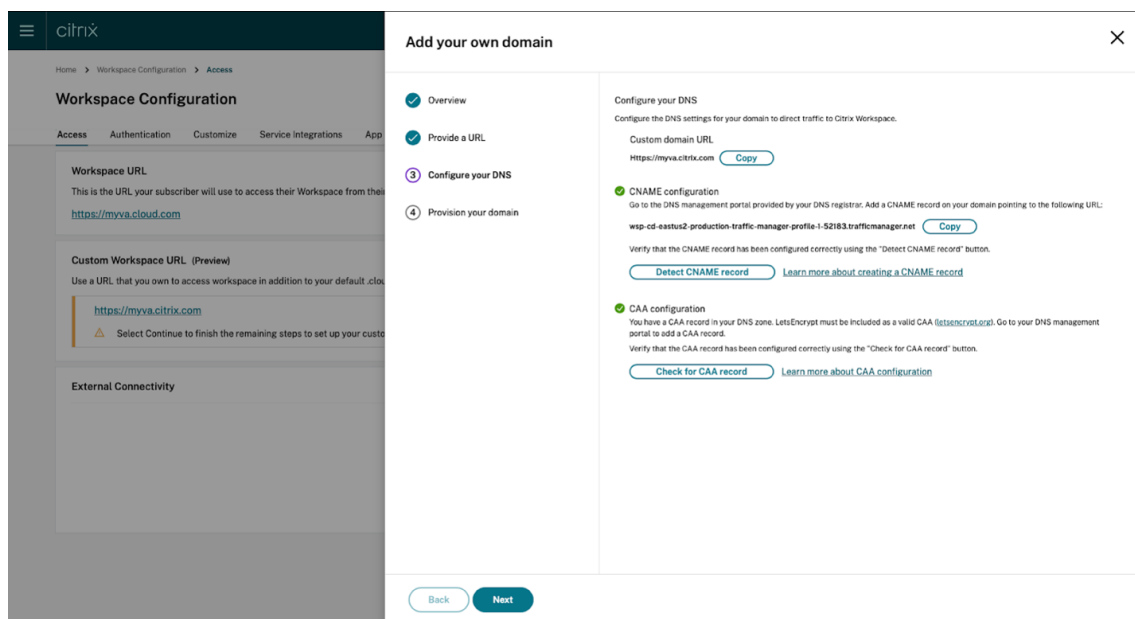


8. DNS プロバイダーで CNAME レコードを構成したら、[**CNAME** レコードの検出] を選択して DNS 構成が正しいことを確認します。CNAME レコードが正しく構成されている場合は、[**CNAME** 構成] セクションの横に緑色のチェックマークが表示されます。

このページに警告が表示された場合は、強調表示された問題を修正して続行してください。

DNS プロバイダーで CAA レコードが構成されている場合は、別の **CAA** 構成が表示されます。[**CAA** レコードの検出] を選択して、DNS 構成が正しいことを確認します。CAA レコードの構成が正しい場合は、[**CAA** の構成] セクションの横に緑色のチェックマークが表示されます。

DNS 構成を確認したら、[次へ] をクリックします。



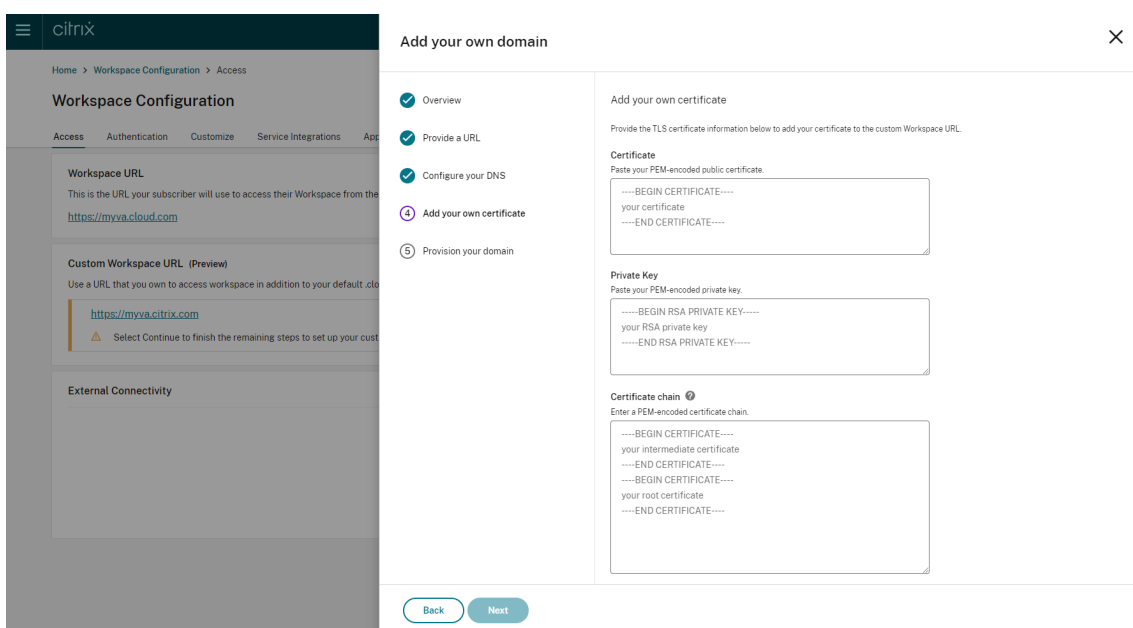
9. これはオプションの手順です。独自の証明書を追加することを選択した場合は、[独自の証明書を追加する] ペ

ページに必要な情報を入力します。

このページに警告が表示された場合は、強調表示された問題を修正して続行します。

証明書が次の条件を満たしていることを確認してください。

- PEM でエンコードされている必要があります。
- 少なくとも今後 30 日間有効である必要があります。
- これはカスタム Workspace URL にのみ使用する必要があり、ワイルドカード証明書は受け入れられません。
- 証明書の共通名はカスタムドメインと一致する必要があります。
- 証明書上の SAN はカスタムドメイン用であり、追加の SAN は許可されません。
- 証明書の有効期間は 10 年を超えてはなりません。



注:

Citrix は安全な暗号化ハッシュ関数 (SHA 256 以上) を使用した証明書を使用することをお勧めします。証明書はユーザーが更新する必要があります。証明書の有効期限が切れているか、もうすぐ期限切れになる場合は、「更新された証明書の提供」セクションを参照してください。

10. これはオプションの手順です。SAML を ID プロバイダーとして使用している場合は、関連する構成を指定します。[SAML の構成] ページに必要な情報を入力します。

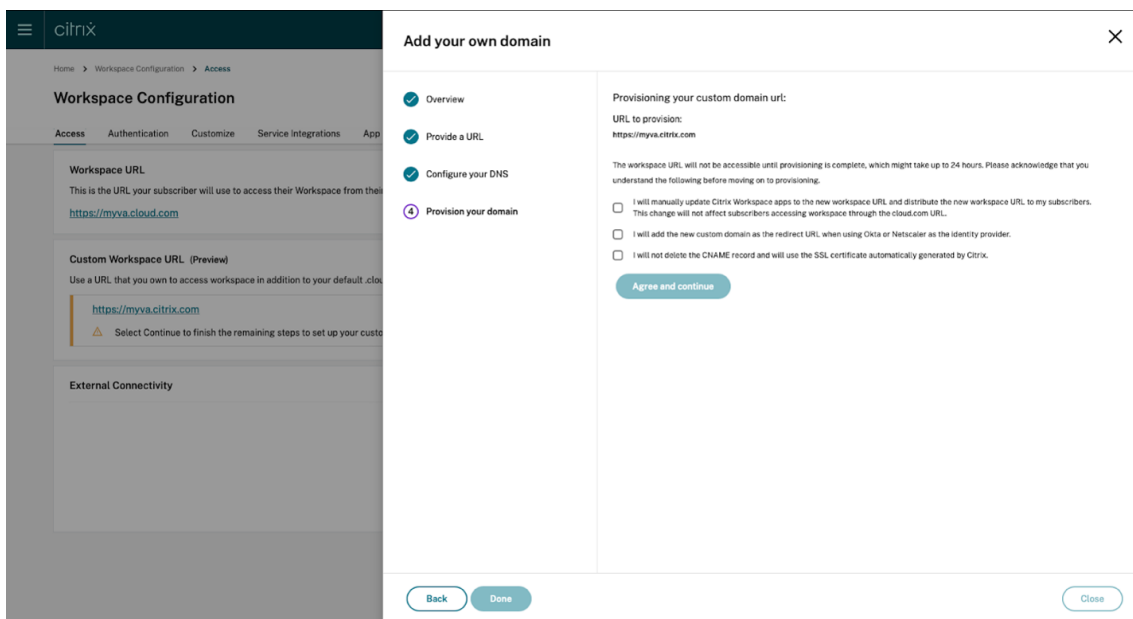
ID プロバイダーでアプリケーションを構成する場合は、次の詳細を使用します。

プロパティ	Value
オーディエンス	https://saml.cloud.com

プロパティ	Value
受信者	<code>https://<your custom domain>/saml/acs</code>
ACS URL バリデーター	<code>https://<your custom domain>/saml/acs</code>
ACS コンシューマー URL	<code>https://<your custom domain>/saml/acs</code>
単一のログアウト URL	<code>https://<your custom domain>/saml/logout/callback</code>

11. [ドメインをプロビジョニングする] ページに表示される情報を読み、指定された指示に同意します。続行する準備ができたなら、[同意して続行する] を選択します。

この最後のプロビジョニング手順が完了するまでに時間がかかる場合があります。操作が完了する間、ページを開いたまま待つことも、ページを閉じることもできます。



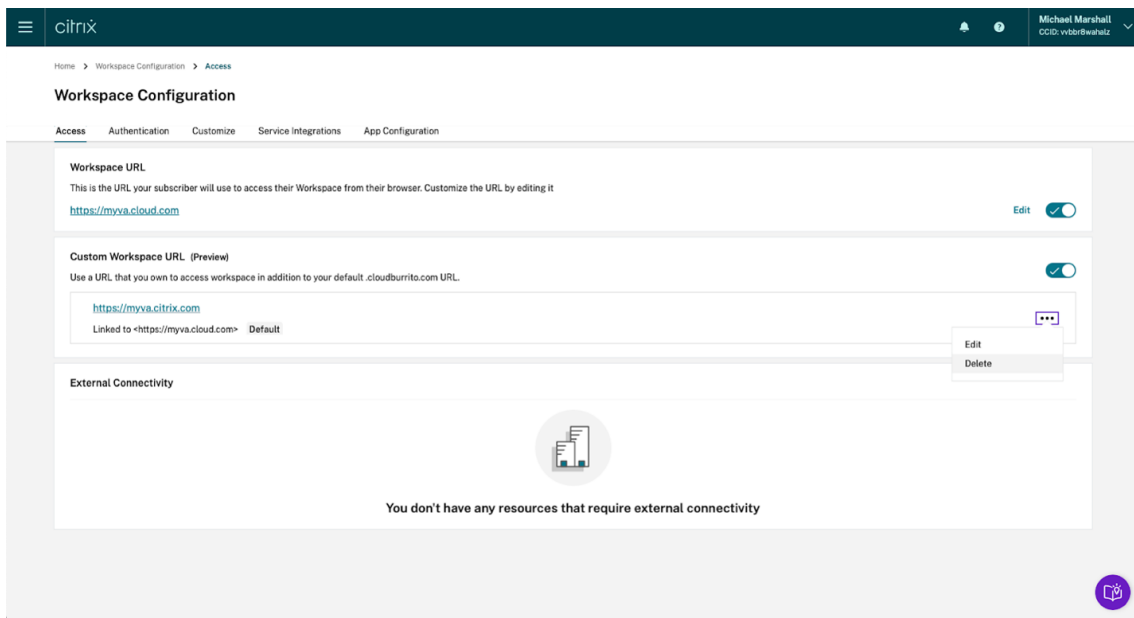
カスタムドメインの削除

顧客からカスタムドメインを削除すると、カスタムドメインを使用して Citrix Workspace にアクセスできなくなります。カスタムドメインを削除した後は、cloud.com アドレスを使用してのみ Citrix Workspace にアクセスできます。

カスタムドメインを削除するときは、CNAME レコードが DNS プロバイダーから削除されていることを確認してください。

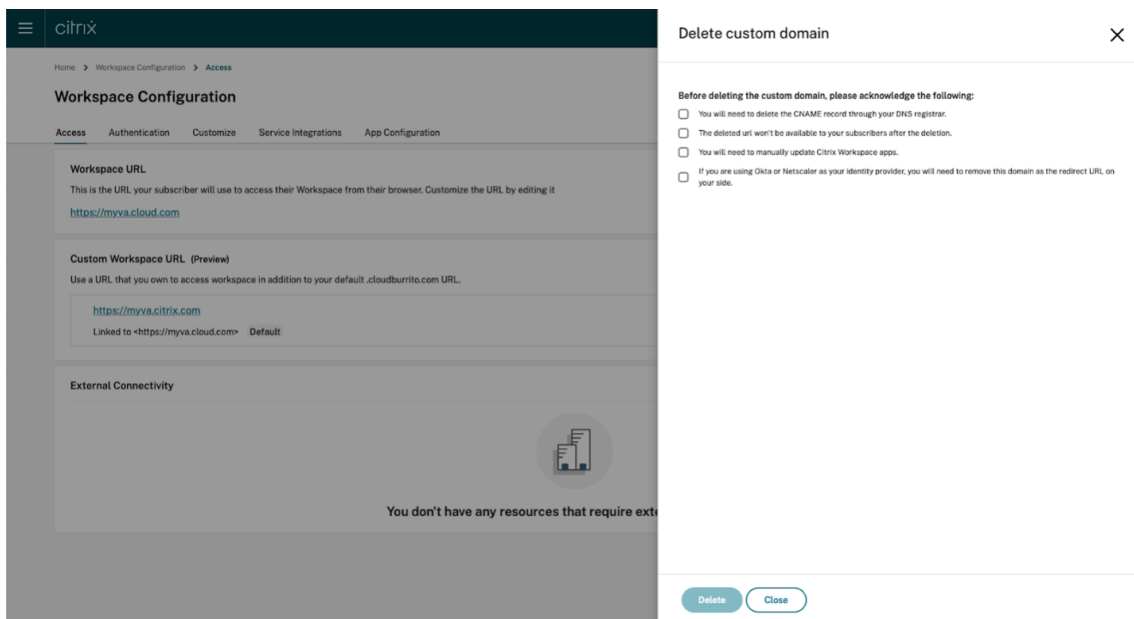
カスタムドメインを削除するには、

1. <https://citrix.cloud.com> で Citrix Cloud にサインインします。
2. Citrix Cloud メニューから、[ワークスペース構成] > [アクセス] を選択します。
3. [アクセス] タブでカスタムドメインのコンテキストメニュー (⋮) を展開し、[削除] を選択します。



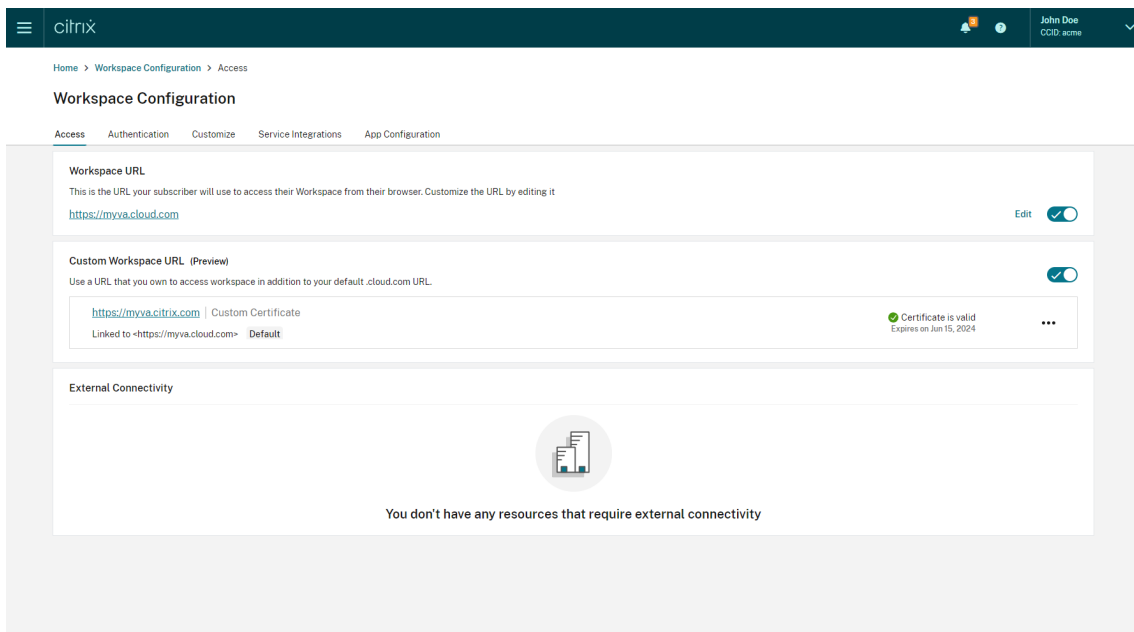
4. [カスタムドメインの削除] ページに表示される情報を読み、指定された指示に同意します。続行する準備ができたなら、[削除] を選択します。

カスタムドメインの削除は、完了するまでに時間がかかります。操作が完了する間、ページを開いたまま待つことも、ページを閉じることもできます。

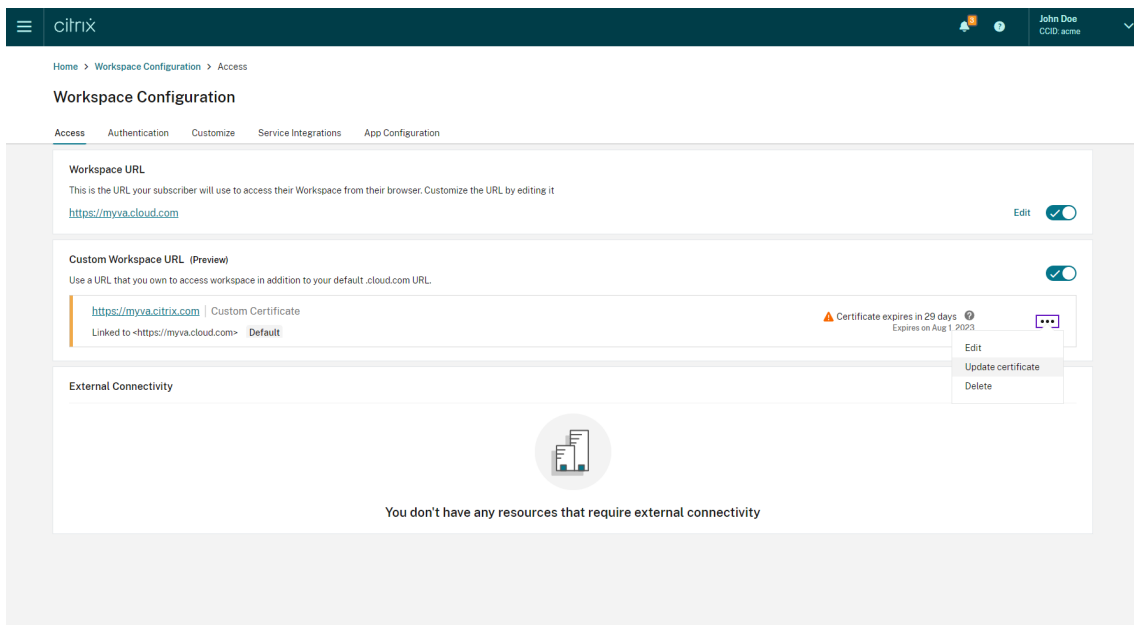


更新された証明書の提供

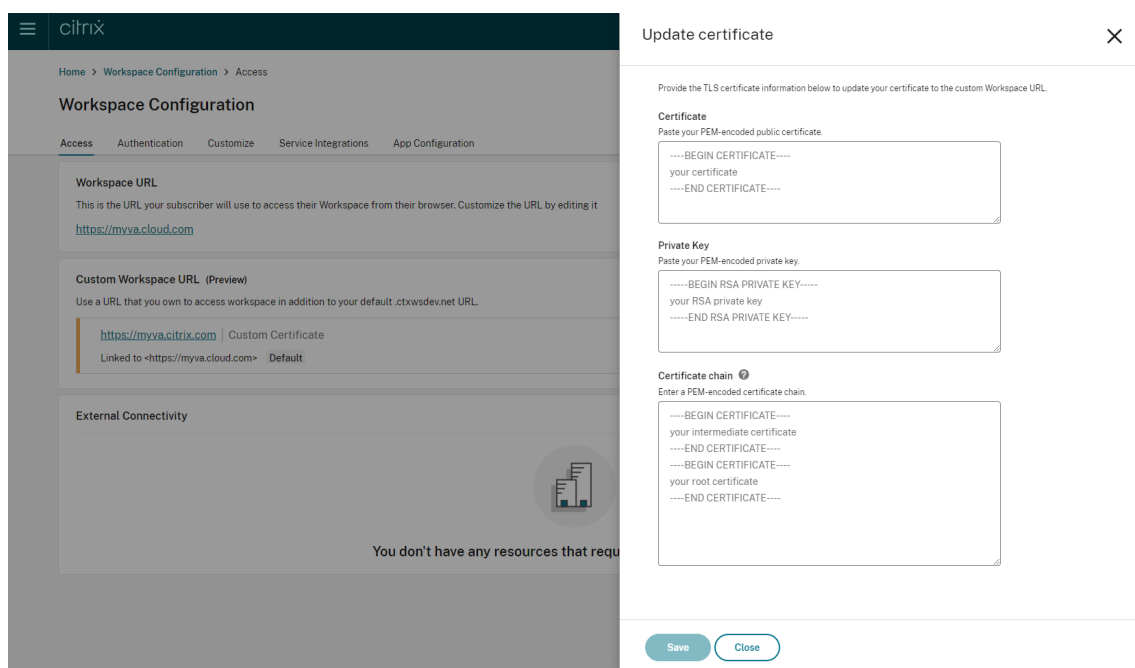
1. Citrix Cloudにサインインします。
2. Citrix Cloud メニューから、[ワークスペース構成] > [アクセス] を選択します。
3. 証明書の有効期限は、証明書が割り当てられているカスタムドメインの横に表示されます。



証明書の有効期限が 30 日以内に切れる場合、カスタムドメインに警告が表示されます。



4. [アクセス] タブでカスタムドメインのコンテキストメニュー (...) を展開します。[証明書を更新] を選択します。



5. [証明書を更新] ページで必要な情報を入力し、[保存] を選択します。

このページに警告が表示された場合は、強調表示された問題を修正して続行します。

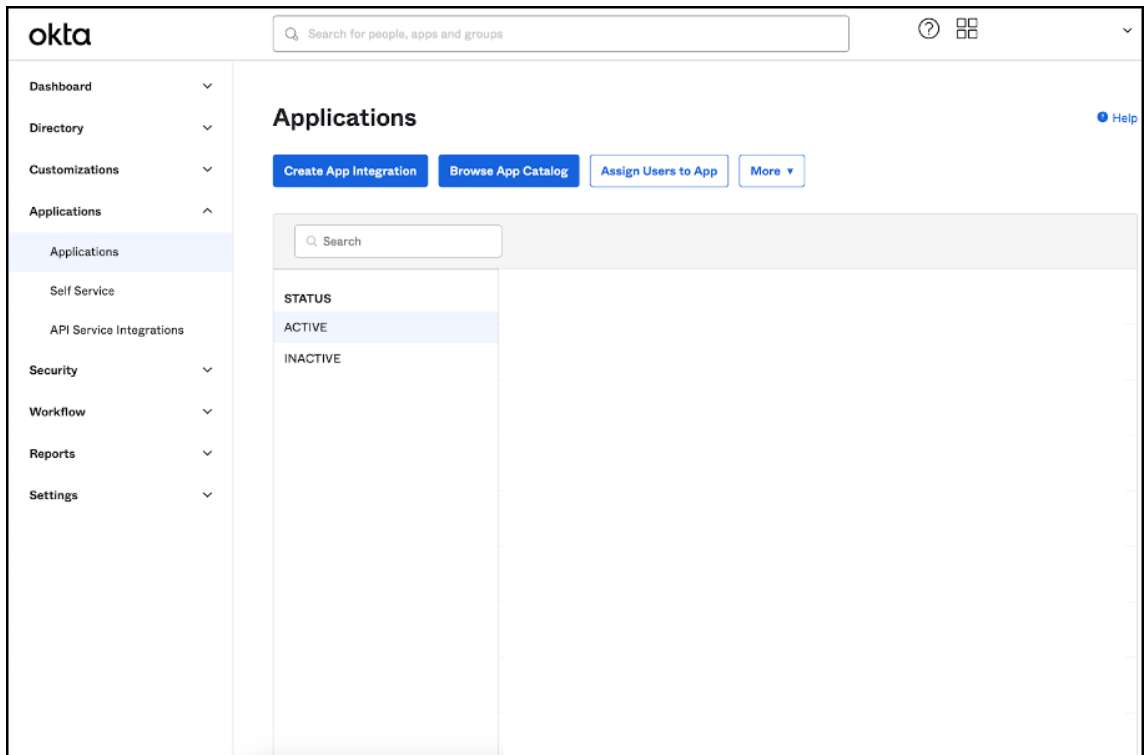
証明書は、カスタムドメインの作成時と同じ要件を満たす必要があります。詳細については、「[カスタムドメインの追加](#)」を参照してください。

ID プロバイダーの構成

Okta の構成

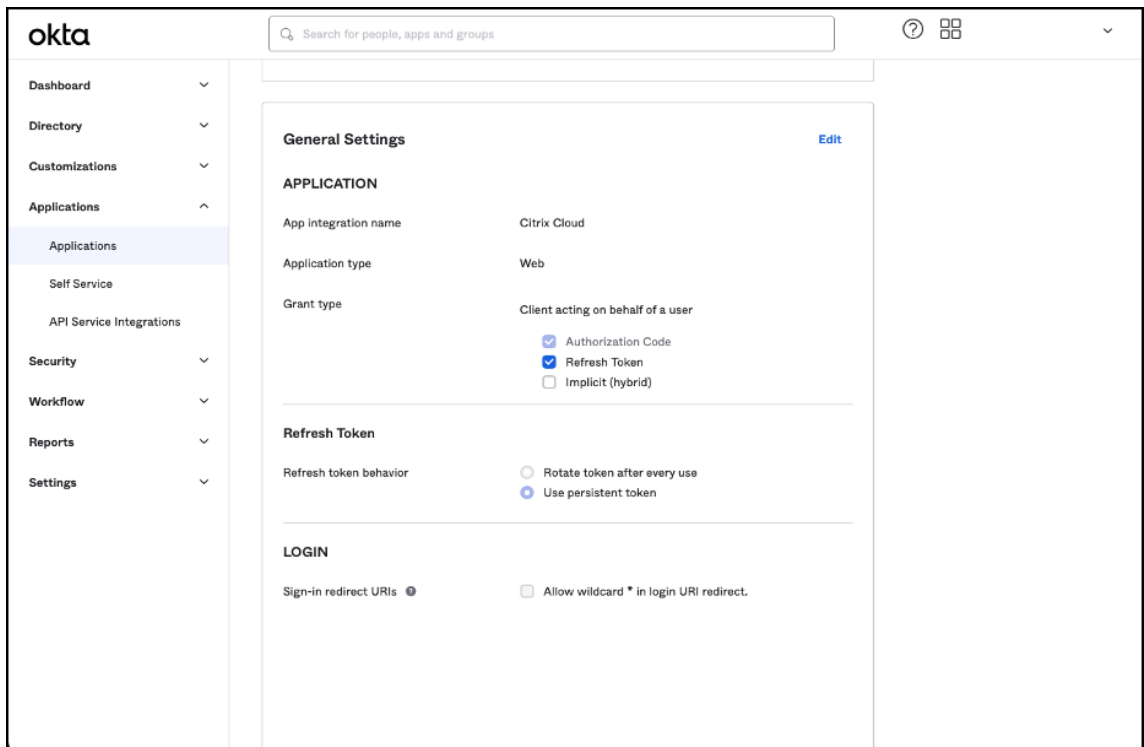
Citrix Workspace アクセスの ID プロバイダーとして Okta を使用している場合は、次の手順を実行します。

1. Okta インスタンスの管理者ポータルにサインインします。このインスタンスには、Citrix Cloud で使用されるアプリケーションが含まれています。
2. [アプリケーション] を展開し、メニューで [アプリケーション] を選択します。



3. Citrix Cloud にリンクされているアプリケーションを開きます。

4. [全般設定] セクションで [編集] を選択します。



5. [全般設定] の [ログイン] セクションで、[Sign-in redirect URIs] の新しい値を追加します。既存

の値を置き換えるのではなく、新しい値を追加します。新しい値は次の形式にする必要があります：
<https://your.company.com/core/login-okta>

6. 同じセクションで、[Sign-out redirect URIs] の新しい値を追加します。既存の値を置き換えるのではなく、新しい値を追加します。新しい値は次の形式にする必要があります：<https://your.company.com>

7. [保存] をクリックして新しい構成を保存します。

OAuth ポリシーとプロファイルの構成

重要

Citrix Cloud と、Citrix Gateway またはアダプティブ認証 HA ペアをリンクする既存の OAuth ポリシーとプロファイルは、OAuth 資格情報が失われた場合にのみ更新する必要があります。このポリシーを変更すると、Citrix Cloud と Workspaces 間のリンクが切断されるリスクがあり、Workspaces へのログイン機能に影響します。

Citrix Gateway の構成

Citrix Cloud 管理者は、暗号化されていないクライアントシークレットにアクセスできます。これらの資格情報は、[ID およびアクセス管理] > [認証] 内の Citrix Gateway リンクプロセス中に Citrix Cloud によって提供されます。OAuth プロファイルとポリシーは、接続プロセス中に Citrix 管理者によって Citrix Gateway 上に手動で作成されました。

Citrix Gateway の接続プロセス中に提供されたクライアント ID と暗号化されていないクライアントシークレットが必要です。これらの資格情報は Citrix Cloud によって提供され、安全に保存されています。

暗号化されていないシークレットは、Citrix ADC インターフェイスまたはコマンドラインインターフェイス (CLI) の両方を使用して OAuth ポリシーとプロファイルを作成するために必要です。

以下は、クライアント ID とシークレットが Citrix 管理者に提供されるときユーザーインターフェイスの例です。Citrix 管理者が接続プロセス中に資格情報の保存に失敗した場合、Citrix Gateway の接続後に暗号化されていないシークレットのコピーを取得できなくなります。

Create a connection with Citrix Gateway



Copy the Client ID and Secret and Redirect URL

Go to your On-Premises Citrix Gateway and input your ID, Secret, and URL to establish the connection. [Learn more](#)

When configuration is completed, test your Gateway connection to enable this identity provider.

Client ID: 3dc ecbd

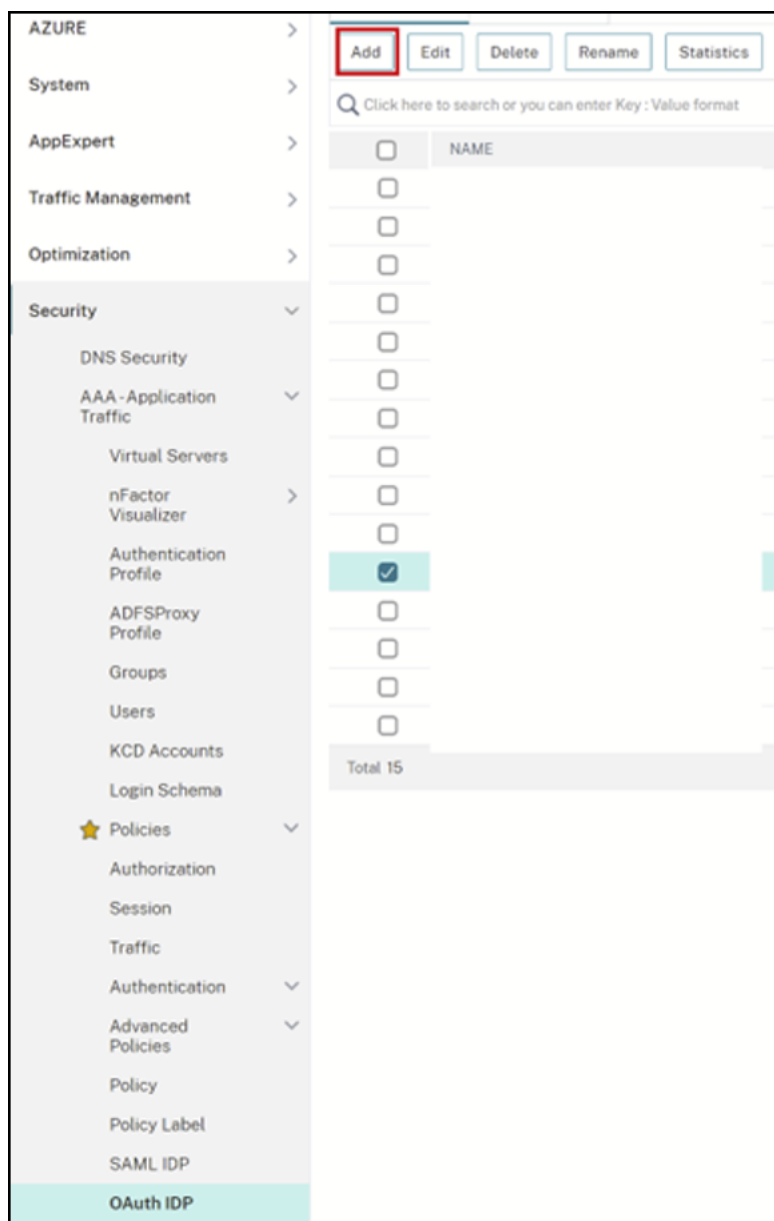
Secret: zGr rag==

Redirect URL: https://accounts.cloud .com /core/login-cip

You will not have access to the client ID and secret later. You will have to generate a new pair if you lose track of the original. [Download](#) the key to save your ID and secret.

Citrix Cloud の使用 Citrix Gateway インターフェイスを使用して追加の OAuth プロファイルとポリシーを追加するには、次の手順を実行します。

1. メニューから、[セキュリティ] > **[AAA - アプリケーショントラフィック]** > **[OAuth IDP]** を選択します。既存の OAuth ポリシーを選択し、[追加] をクリックします。



2. プロンプトが表示されたら、新しい OAuth ポリシーの名前を、前の手順で選択した既存のポリシーとは異なる名前に変更します。Citrix では、名前に *custom-url* を追加することをお勧めします。

← Create Authentication OAuth IDP Policy

Name*
GatewayGateway-OAuthPol ⓘ

Action*
Add Edit

Log Action
Add Edit

Undefined-Result Action

Expression *
Select Select Select
true

3. Citrix Gateway GUI で、既存の OAuth プロファイルを作成します。
4. 同じ GUI メニューで、[アクション] の横にある [追加] をクリックします。

Create Authentication OAuth IDP Profile

Name*
GatewayIDP-OAuthAction ⓘ

Client ID*
<insert client ID> ⓘ

Client Secret*
<insert unencrypted client secret> ⓘ

Redirect URL*
https://hostname.domain.com/core ⓘ

Issuer Name
ⓘ

Audience
<insert client ID here> ⓘ

Skew Time (mins)
5

Default Authentication Group

Relying Party Metadata URL

Refresh Interval
50

Encrypt Token ⓘ

Signature Service

Attributes

Send Password ⓘ

Create Close

5. Citrix Gateway GUI で、新しい OAuth ポリシーを既存の認証、承認、および監査の仮想サーバーにバインドします。
6. [セキュリティ] > [仮想サーバー] > [編集] に移動します。



コマンドラインインターフェイス (CLI) の使用

重要

OAuth 資格情報のコピーが安全に保存されていない場合は、Citrix Gateway を切断して再接続し、Citrix Cloud の ID およびアクセス管理によって提供される新しい OAuth 資格情報で既存の OAuth プロファイルを更新する必要があります。古い資格情報を回復できない場合にのみ、既存の OAuth プロファイルを新しい資格情報で更新してください。他に選択肢がない場合を除き、これはお勧めできません。

1. PuTTY などの SSH ツールを使用して、Citrix Gateway インスタンスに接続します。
2. OAuthProfile と OAuthPolicy を作成します。認証の OAuthIDPProfile を追加します。

```
"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. OAuthPolicy を、既存のポリシーよりも優先順位の低い、正しい認証、承認、および監査の仮想サーバーにバインドします。このインスタンスでは、既存のポリシーの優先度が 10 であると想定しているため、新しいポリシーには 20 が使用されます。認証仮想サーバーをバインドします。

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

アダプティブ認証の構成

重要

OAuth プロファイルの暗号化されたシークレットと暗号化パラメータは、アダプティブ認証のプライマリ HA ゲートウェイとセカンダリ HA ゲートウェイで異なります。必ずプライマリ HA ゲートウェイから暗号化されたシークレットを取得し、これらのコマンドをプライマリ HA ゲートウェイで実行してください。

Citrix Cloud 管理者は暗号化されていないクライアントシークレットにアクセスできません。OAuth ポリシーとプロファイルは、プロビジョニングフェーズ中に Citrix アダプティブ認証サービスによって作成されます。OAuth プロファイルを作成するには、ns.conf ファイルから取得した暗号化されたシークレットと CLI コマンドを使用する必要があります。これは、Citrix ADC ユーザーインターフェイスを使用して実行することはできません。既存の認証、承認、および監査の仮想サーバーにバインドされている既存のポリシーよりも高い優先度番号を使用して、新しいカスタム URL OAuthPolicy を既存の認証、承認、および監査の仮想サーバーにバインドします。優先度の低い番号が

最初に評価されることに注意してください。既存のポリシーの優先度を 10 に設定し、新しいポリシーの優先度を 20 に設定して、それらが正しい順序で評価されるようにします。

1. PuTTY などの SSH ツールを使用して、アダプティブ認証プライマリノードに接続します。

show ha node

```
Done
> show ha node
1) Node ID: 0
   IP: 192.168.0.4 (adaptive-auth-1)
   Node State: UP
   Master State: Secondary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: SUCCESS
   Propagation: ENABLED
   Enabled Interfaces : 0/1
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : None
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
   Sync Status Strict Mode: DISABLED
   Hello Interval: 200 msec
   Dead Interval: 3 secs
   Node in this Master State for: 9:0:15:41 (days:hrs:min:sec)
2) Node ID: 1
   IP: 192.168.0.7
   Node State: UP
   Master State: Primary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: ENABLED
   Propagation: ENABLED
   Enabled Interfaces : 0/1
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : None
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
Done
```

2. プライマリ HA ゲートウェイの実行中の構成内で、既存の OAuth プロファイルを含む行を見つけます。

sh runn | grep oauth

3. すべての暗号化パラメーターを含む、Citrix ADC CLI からの出力をコピーします。

```
> sh runn | grep oauth
add authentication OAuthIDPProfile AAuthAutoConfig oauthIdpProf -clientID b1656835-20d1-4f6b-4ddd-1a531fd253f6 -clientSecret od20
E14a222303d -encrypted -encryptmethod ENCRYPTMD_3 -kek -suffix 2023_04
_09_12_25 -redirectURL "https://accounts.cloudburrito.com/core/login-cip" -audience b1656835-20d1-4f6b-4ddd-1a531fd253f6 -sendPassword ON
```

4. 前の手順でコピーした行を変更し、それを使用して、暗号化されたバージョンのクライアント ID を使用して OAuth プロファイルを作成できる新しい CLI コマンドを作成します。これには、すべての暗号化パラメーターを含める必要があります。

- OAuth プロファイルの名前を *CustomDomain-OAuthProfile* に更新します

- -redirectURL を<https://hostname.domain.com/core/login-cip>に更新します

両方の更新後の例を次に示します。

```
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. OAuthPolicy を、既存のポリシーよりも優先順位の低い、正しい認証、承認、および監査の仮想サーバーにバインドします。すべてのアダプティブ認証展開の認証、承認、および監査の仮想サーバー名は `auth_vs` になります。このインスタンスでは、既存のポリシーの優先度が 10 であると想定しているため、新しいポリシーには 20 が使用されます。

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

既知の制限事項

カスタムドメインソリューションの既知の制限は次のとおりです。

Workspace プラットフォーム

- 現在、顧客ごとに 1 つのカスタムドメインのみをサポートしています。
- カスタムドメインは、デフォルトのワークスペース URL にのみリンクできます。マルチ URL 機能を通じて追加された他のワークスペース URL にはカスタムドメインを含めることはできません。マルチ URL 機能は現在 Private Tech Preview 段階にあり、すべての顧客が利用できるわけではありません。
- 以前のソリューションでカスタムドメインが構成されており、SAML または AzureAD を使用して Citrix Workspace アクセスを認証している場合は、最初に既存のカスタムドメインを削除しないと、新しいソリューションでカスタムドメインを構成できません。

SAML

SAML サポートは次のいずれかのユースケースに限定されます。

- SAML は cloud.com ドメインにのみ使用できます。この例では、SAML の使用により、Citrix Workspace アクセスと Citrix Cloud 管理者アクセスがカバーされます。
- SAML はカスタムドメインにのみ使用できます。

Windows 向け Citrix Workspace アプリ

- この機能は、Windows 向け Citrix Workspace アプリバージョン 2305 および 2307 ではサポートされていません。サポートされている最新バージョンに更新してください。

セキュアなワークスペース

October 12, 2023

管理者は、利用者が次のうちのいずれかの認証方法を使用して、ワークスペースへの認証を実行するよう選択できます:

- Active Directory (AD)
- Active Directory+ トークン
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

これらの認証オプションは、すべての Citrix Cloud サービスで利用できます。詳しくは、「[技術概要: Workspace ID](#)」を参照してください。

Citrix Workspace では、Citrix フェデレーション認証サービス (FAS) を使用した Citrix DaaS へのシングルサインオン (SSO) の提供もサポートされています。FAS を使用した SSO により、利用者は、フェデレーション認証方式でワークスペースに既にサインインしていれば、DaaS に認証する必要がなくなります。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

認証方法の選択または変更

ID プロバイダーを構成した後、[ワークスペース構成] > [認証] > [ワークスペースの認証] で、利用者のワークスペースへの認証方法を選択または変更します。

← Workspace Configuration ?

Access Authentication **Customize** Service Integrations Sites

Workspace Authentication

Select how subscribers will authenticate to sign in to their workspace.

- Active Directory
- Azure Active Directory

重要:

認証モードの切り替えには最大 5 分かかり、その間利用者はアクセスできません。変更は、使用頻度の低い期間に限定することを Citrix ではお勧めします。ブラウザまたは Citrix Workspace アプリを使用して Citrix Workspace にログオンしている利用者がある場合は、ブラウザを終了するか、アプリを終了するよう利用者に指示します。約 5 分間の待機後、利用者は新しい認証方法でまたサインインできます。

Active Directory (AD)

デフォルトでは、Citrix Cloud は Active Directory (AD) を使用して、ワークスペースへの利用者認証を管理します。

AD を使用するには、オンプレミスの AD ドメインに少なくとも 2 つの Citrix Cloud Connector がインストールされている必要があります。Cloud Connector のインストールについて詳しくは、「[Cloud Connector のインストール](#)」を参照してください。

Active Directory (AD) + トークン

セキュリティを強化するために、Citrix Workspace は、AD サインインに対する認証の 2 番目の要素として時間ベースのトークンをサポートしています。

Workspace は、利用者のログインごとに、登録済みデバイスの認証アプリからトークンを入力するように求めます。利用者は、サインインする前に、Citrix SSO などの時間ベースのワンタイムパスワード (TOTP: Time-Based One-Time Password) 標準に準拠した認証アプリに、デバイスを登録する必要があります。現時点では、一度に 1 つのデバイスしか登録できません。

詳しくは、「[Tech Insight: 認証 - TOTP](#)」および「[Tech Insight: 認証 - プッシュ](#)」を参照してください。

AD+ トークンの要件

Active Directory+ トークン認証には次の要件があります：

- Active Directory と Citrix Cloud 間の接続と、オンプレミス環境での少なくとも 2 つの Cloud Connectors のインストール。要件と手順については、「[Active Directory を Citrix Cloud に接続する](#)」を参照してください。
- [ID およびアクセス管理] ページにおける [**Active Directory + トークン**] 認証の有効化。詳しくは、「[Active Directory+ トークン認証を有効にするには](#)」を参照してください。
- 利用者によるメールへのアクセスとデバイスの登録。
- 認証アプリをダウンロードするデバイス。

初めての登録

利用者は、「[2 要素認証に対するデバイスの登録](#)」で説明した登録プロセスにより、デバイスを登録します。

Workspace への最初のサインインの際に、利用者はプロンプトに従って Citrix SSO アプリをダウンロードします。Citrix SSO アプリは、30 秒ごとに登録済みデバイスに一意的ワンタイムパスワードを生成します。

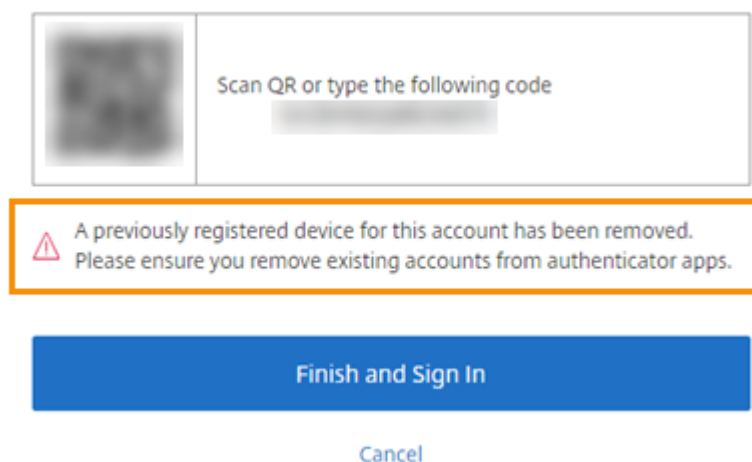
重要：

デバイスの登録処理中に、利用者は一時的な確認コードが記載されたメールを受信します。この一時コードは、利用者のデバイスを登録するためにのみ使用されます。この一時コードを、2 要素認証で Citrix Workspace にサインインするためのトークンとして使用することはサポートされていません。2 要素認証のトークンとしてサポートされているのは、登録済みデバイス上の認証アプリから生成された確認コードのみです。

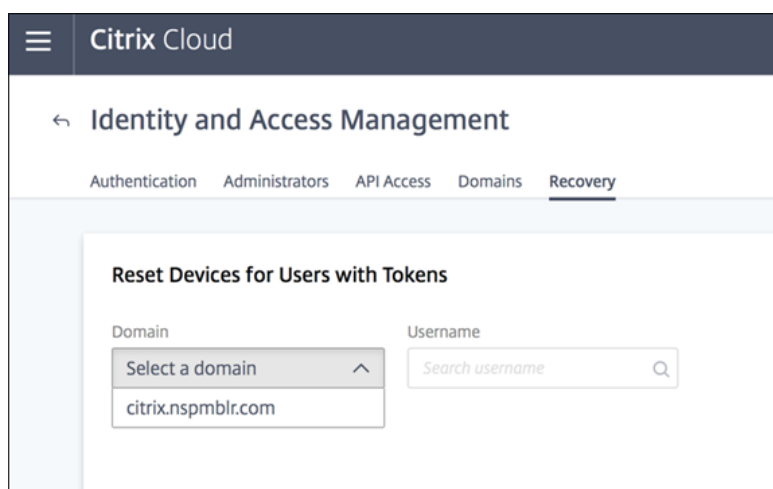
デバイスの再登録

利用者が自分の登録済みデバイスを所有していない、またはそのデバイスを再登録する必要がなくなった場合（たとえば、デバイスからコンテンツを削除したあと）は、Workspace では以下のオプションが提供されます：

- 利用者は、「[2 要素認証に対するデバイスの登録](#)」で説明したのと同じ登録プロセスにより、デバイスを再登録できます。利用者は一度に 1 つのデバイスしか登録できないため、新しいデバイスを登録するか、既存のデバイスを再登録することで、以前のデバイス登録を削除します。



- 管理者は、Active Directory の名前で利用者を検索して自分のデバイスをリセットできます。それを行うには、[ID およびアクセス管理] > [復旧] に移動します。Workspace への次のサインオンの際、利用者は初めての登録の手順に従います。



Azure Active Directory

Azure Active Directory (AD) を使用してワークスペースへの利用者の認証を管理するには、以下の要件があります：

- Azure AD は、グローバル管理者権限を持つユーザーが使用。Citrix Cloud が使用する Azure AD アプリケーションと権限について詳しくは、「[Citrix Cloud 用の Azure Active Directory の権限](#)」を参照してください。
- Citrix Cloud Connector がオンプレミスの AD ドメインにインストールされていること。マシンが Azure AD と同期しているドメインに参加している必要もあります。
- バージョン 7.15.2000 LTSR CU の VDA または 7.18 最新リリース以降の VDA。
- Azure AD と Citrix Cloud 間の接続。詳しくは、「[Azure Active Directory を Citrix Cloud に接続する](#)」を参照してください。

Active Directory を Azure AD に同期させるときは、UPN および SID エントリを同期の対象に含める必要があります。これらのエントリが同期されていないと、Citrix Workspace の特定のワークフローが失敗します。

警告:

- Azure AD を使用している場合、[CTX225819](#)に記載されているようにレジストリに変更を加えないでください。このように変更すると、Azure AD ユーザーがセッションを起動できない可能性があります。
- `DSAuthAzureAdNestedGroups`機能を有効にすると、別のグループのメンバーとしてグループを追加できます（入れ子構造）。`DSAuthAzureAdNestedGroups`を有効にするには、Citrix サポートにリクエストを送信してください。

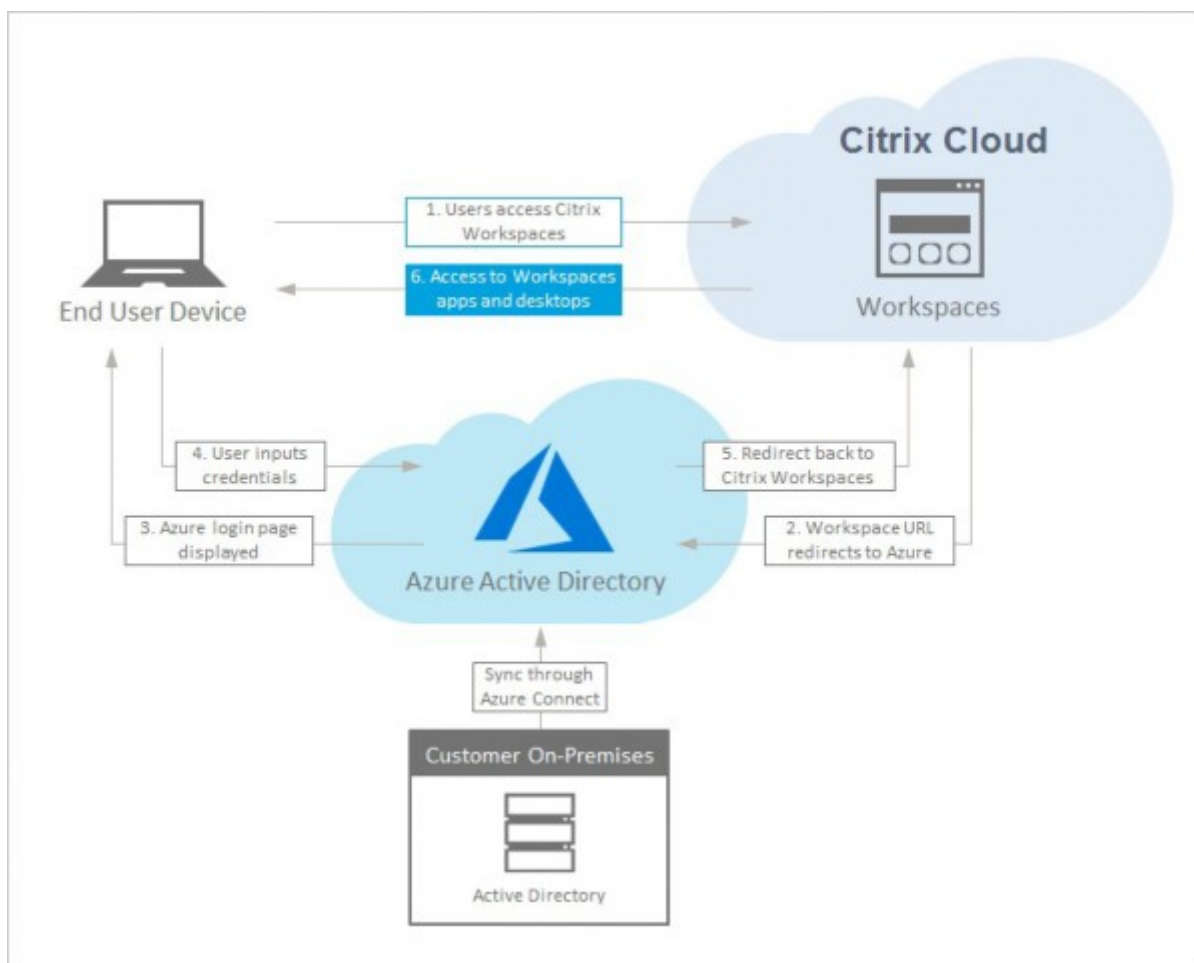
Azure AD 認証を有効にした後:

- セキュリティの強化: セキュリティのために、ユーザーは、アプリやデスクトップの起動時に再度サインインするよう求められます。パスワード情報は、ユーザーのデバイスからセッションをホストしている VDA に直接送信されます。
- サインインエクスペリエンス: Azure AD 認証は、シングルサインオン (SSO) ではなく、フェデレーションサインインを提供します。利用者は Azure サインインページからサインインし、Citrix DaaS を開くときに再度認証する必要がある場合があります。

SSO を使用するには、Citrix Cloud で Citrix フェデレーション認証サービスを有効にします。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

Azure AD のサインイン操作をカスタマイズすることができます。詳しくは、[Microsoft 社のドキュメント](#)を参照してください。[ワークスペース構成] で行われたサインインのカスタマイズ (ロゴ) は、Azure AD のサインイン操作に影響しません。

次の図は、Azure AD 認証のシーケンスを示しています。



Citrix Gateway

Citrix Workspace では、オンプレミスの Citrix Gateway を ID プロバイダーとして使用してワークスペースへの利用者の認証を管理できます。詳しくは、「[Tech Insight: 認証 - Citrix Gateway](#)」を参照してください。

Citrix Gateway の要件

Citrix Gateway 認証には次の要件があります：

- Active Directory と Citrix Cloud 間の接続。要件と手順については、「[Active Directory を Citrix Cloud に接続する](#)」を参照してください。
- 利用者がワークスペースにサインインするには、Active Directory ユーザーである必要があります。
- フェデレーションを実行している場合、AD ユーザーをフェデレーションプロバイダーと同期する必要があります。Citrix Cloud では、ユーザーが正常にサインインできるよう、AD ユーザー属性が必要とされます。
- オンプレミスの Citrix Gateway:
 - Citrix Gateway 12.1 54.13 Advanced Edition 以降

- Citrix Gateway 13.0 41.20 Advanced Edition 以降

- **Citrix Gateway** 認証が **[ID およびアクセス管理]** ページで有効になっています。これにより、Citrix Cloud とオンプレミスの Gateway との接続を作成するために必要なクライアント ID、シークレット、リダイレクト URL を生成します。
- Gateway で、生成されたクライアント ID、シークレット、リダイレクト URL を使用して OAuth ID プロバイダー認証ポリシーが構成されます。

詳しくは、「[オンプレミスの Citrix Gateway を ID プロバイダーとして Citrix Cloud に接続する](#)」を参照してください。

利用者による **Citrix Gateway** の操作

Citrix Gateway での認証が有効になっている場合、利用者は次のワークフローを経験します：

1. ブラウザーでワークスペース URL に移動するか、Workspace アプリを起動します。
2. 利用者は、Citrix Gateway のログオンページにリダイレクトされ、Gateway で構成された方法で認証されます。この方法には、MFA、フェデレーション、条件付きアクセスポリシーなどがあります。[CTX258331](#)に記載されている手順に従い、Workspace のサインインページと見た目が同じになるよう Gateway のログオンページをカスタマイズできます。
3. 認証に成功すると、利用者のワークスペースが表示されます。

Google

Citrix Workspace では、Google を ID プロバイダーとして使用してワークスペースへの利用者の認証を管理できます。

Google の要件

- オンプレミスの Active Directory と Google Cloud 間の接続。
- Google Cloud Platform コンソールにアクセスできる開発者アカウント。このアカウントは、サービスアカウントとキーを作成し、Admin SDK API を有効にするために必要です。
- Google Workspace 管理コンソールにアクセスできる管理者アカウント。このアカウントは、ドメイン全体の委任と読み取り専用の API ユーザーアカウントを構成するために必要です。
- **[ID およびアクセス管理]** ページで有効にした **[Google]** 認証を使用した、オンプレミスの Active Directory と Citrix Cloud 間の接続。この接続を作成するには、リソースの場所に少なくとも 2 つの Cloud Connector が必要です。

詳しくは、「[Google を ID プロバイダーとして Citrix Cloud に接続する](#)」を参照してください。

利用者による **Google** の操作

Google での認証が有効になっている場合、利用者は次のワークフローに従います：

1. 利用者はブラウザでワークスペース URL に移動するか、Workspace アプリを起動します。
2. Google のサインインページにリダイレクトされ、Google Cloud で構成された方法（多要素認証、条件付きアクセスポリシーなど）で認証されます。
3. 認証に成功すると、利用者のワークスペースが表示されます。

Okta

Citrix Workspace では、Okta を ID プロバイダーとして使用してワークスペースへの利用者の認証を管理できません。詳しくは、「[Tech Insight: 認証 - Okta](#)」を参照してください。

Okta の要件

Okta 認証には次の要件があります：

- オンプレミスの Active Directory と Okta 組織の間の接続。
- Citrix Cloud で使用するために構成された Okta OIDC Web アプリケーション。Citrix Cloud を Okta 組織に接続するには、このアプリケーションに関連付けられているクライアント ID とクライアントシークレットを指定する必要があります。
- **[ID およびアクセス管理]** ページで有効にした **[Okta]** 認証を使用した、オンプレミスの Active Directory と Citrix Cloud 間の接続。

詳しくは、「[Okta を ID プロバイダーとして Citrix Cloud に接続する](#)」を参照してください。

利用者による **Okta** の操作

Okta での認証が有効になっている場合、利用者は次のワークフローに従います：

1. 利用者はブラウザでワークスペース URL に移動するか、Workspace アプリを起動します。
2. Okta のサインインページにリダイレクトされ、Okta で構成された方法（多要素認証、条件付きアクセスポリシーなど）で認証されます。
3. 認証に成功すると、利用者のワークスペースが表示されます。

Okta 認証は、シングルサインオン (SSO) ではなく、フェデレーション ID によるサインインを提供します。利用者は Okta サインインページからワークスペースにサインインし、Citrix DaaS を開くときに再度認証する必要がある場合があります。SSO を使用するには、Citrix Cloud で Citrix フェデレーション認証サービスを有効にします。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

SAML 2.0

Citrix Workspace では、SAML 2.0 を使用してワークスペースへの利用者の認証を管理できます。SAML 2.0 をサポートしている場合は、選択した SAML プロバイダーを使用できます。

SAML 2.0 の要件

SAML 認証には次の要件があります：

- SAML 2.0 をサポートする SAML プロバイダー
- オンプレミスの Active Directory ドメイン
- リソースの場所に展開され、オンプレミスの AD ドメインに参加している 2 つの Cloud Connector。
- SAML プロバイダーとの AD 統合

ワークスペースでの SAML 認証の構成について詳しくは、「[SAML を ID プロバイダーとして Citrix Cloud に接続する](#)」を参照してください。

利用者による SAML 2.0 の操作

1. 利用者は、ブラウザで Workspace URL に移動するか、Citrix Workspace アプリを起動します。
2. 組織の SAML ID プロバイダーのサインインページにリダイレクトされます。多要素認証や条件付きアクセスポリシーなど、SAML ID プロバイダー用に構成されたメカニズムを使用して認証します。
3. 認証に成功すると、利用者のワークスペースが表示されます。

Citrix フェデレーション認証サービス (FAS)

Citrix Workspace では、Citrix フェデレーション認証サービス (FAS) を使用した Citrix DaaS へのシングルサインオン (SSO) がサポートされています。FAS がないと、フェデレーション ID プロバイダーを使用している利用者は、DaaS にアクセスするために資格情報を複数回入力するように求められます。

詳しくは、「[Citrix フェデレーション認証サービス \(FAS\)](#)」を参照してください。

利用者のサインアウト操作

[設定] > [ログオフ] をして、Workspace および Azure AD からのサインアウトプロセスを完了します。[ログオフ] オプションを使用せずにブラウザを閉じると、Azure AD にサインインしたままになる可能性があります。

重要：

ブラウザで Citrix Workspace が非アクティブなためにタイムアウトした場合でも、利用者は Azure AD に

サインインしたままになります。これは、Citrix Workspace のタイムアウトによって他の Azure AD アプリケーションを強制的に終了させないようにするためです。

追加情報

- [技術概要: Workspace のシングルサインオン](#)
- [Tech Insight - Citrix Workspace](#)
- [概念実証ガイド - Citrix Workspace](#)

サービスをワークスペースに統合する

October 12, 2023

この記事では、Citrix Workspace にサービスを追加する手順の概要を説明します。これには 2 段階のプロセスがあります:

1. Citrix Cloud で個々のサービスを構成します。「[Citrix Cloud サービス](#)」には Citrix Cloud サービスの一覧があり、各サービスの説明ページへのリンクがあります。
2. [ワークスペース構成] > [サービス統合] で、構成したサービスへのアクセスを有効化（および無効化）します。

サービスを構成する

購入したサービスは、Citrix Cloud ダッシュボードにカードレイアウトで表示されます。購入したサービスには、[管理] ボタンがあります。

購入したサービスを構成するには:

1. Citrix Cloud にサインインします。
2. 構成するサービスのタイルで [管理] を選択します。
3. そのサービスを設定するための手順に従います。

クラウドでホストされるサービスの簡単な説明については、「[Citrix Workspace を介したクラウドでホストされるサービス](#)」を参照してください。

新しいサービスを試してみたい場合は、トライアルまたはデモをリクエストできます。サービストライアルについて詳しくは、「[Citrix Cloud サービスのトライアル](#)」を参照してください。

サービスを有効にする

サービスを構成したら、それらを Citrix Workspace に統合できます。

デフォルトでは、サブスクリプションをすることで、**DaaS** と **Remote Browser Isolation** サービスが使用できるようになります。組織がサブスクリプションするその他のすべての新しいサービスは、デフォルトで無効になっています。

注:

Citrix App Essentials サービスと Citrix DaaS は、[ワークスペース構成] の [サービス統合] タブで「**Citrix DaaS**」として表示されます。

サービスのワークスペース統合を有効にするには:

1. [ワークスペース構成] > [サービス統合] に移動します。
2. サービスの横の省略記号 (⋮) ボタンを選択し、[有効化] を選択します。

← Workspace Configuration ⓘ

The screenshot shows the 'Manage Service Integrations' page in Citrix Workspace. The page has a navigation bar with 'Access', 'Authentication', 'Customize', 'Service Integrations', and 'Sites'. Below the navigation bar, there is a section titled 'Manage Service Integrations' with a subtitle 'Services can be integrated with Citrix Workspace to provide your subscribers apps and data on any device.' The main content area displays a list of services with their status and an 'Enable' button highlighted for the 'Gateway' service.

Service Name	Status	Action
Content Collaboration [redacted].sharefile.com	Enabled	⋮
Virtual Apps and Desktops	Enabled	⋮
Gateway Web and SaaS applications feed	Disabled	Enable
Secure Browser	Enabled	⋮

サービスを無効にする

ワークスペース統合を無効にすると、そのサービスへの利用者のアクセスはブロックされます。これによりワークスペースの URL が無効になるわけではありませんが、利用者は Citrix Workspace のそのサービスから、データおよびアプリケーションにアクセスできなくなります。

サービスのワークスペース統合を無効にするには:

1. [ワークスペース構成] > [サービス統合] に移動します。
2. サービスの横の省略記号 (...) ボタンを選択し、[無効化] を選択します。
3. プロンプトが表示されたら、[確認] を選択し、利用者がサービスからデータまたはアプリケーションにアクセスできなくなることを確認します。



Subscribers will no longer have access to data and applications from this service in Citrix Workspace

Are you sure you want to disable workspace integration for Virtual Apps and Desktops?

Cancel

Confirm

Citrix Workspace アプリの構成

November 28, 2023

Global App Configuration Service を使用して Citrix Workspace アプリを構成できます。これは、管理者が管理対象デバイスと管理対象外デバイスの両方でエンドユーザーのアプリ設定を管理するのに役立ちます。

次のいずれかの方法を使用して、クラウド (Citrix Workspace) 環境とオンプレミス (Citrix StoreFront) 環境の両方に対して設定を構成できます：

- Global App Configuration Service のユーザーインターフェイス (UI)：
 - [クラウドストアの設定の構成](#)
 - [オンプレミスストアの設定の構成](#)
- API: API を使用して設定を構成するには、[Citrix Developer](#)を参照してください。

このサービスは、Windows、Mac、Android、iOS、HTML5、および ChromeOS プラットフォームでサポートされています。

主なメリット

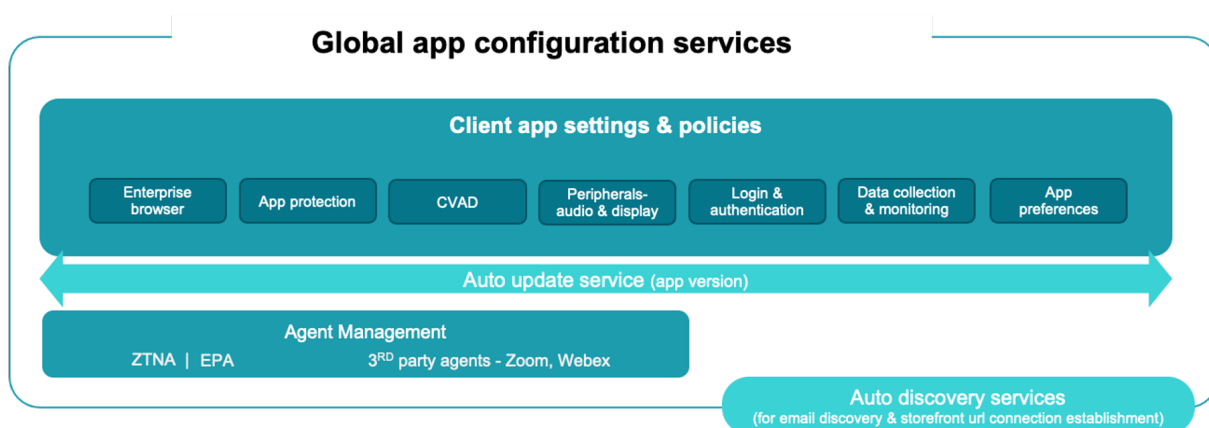
Global App Configuration Service を使用すると、一元化されたインターフェイスから次の機能を実行できます:

- 管理対象デバイスと管理対象外デバイス（個人所有のデバイス）の両方の設定を構成する
- 複数のストアの設定を構成する
- クライアントアプリエージェント（Endpoint Analysis、ZTNA など）およびサードパーティエージェント（Zoom、Webex など）を更新および管理する
- エンドユーザー向けの Citrix Workspace アプリのバージョンを自動的に更新および管理する
- エンドユーザーに展開する前に構成をテストする

Global App Configuration Service の機能?

Global App Configuration Service は、クライアントアプリの設定を構成および管理するために使用される Citrix IP ソリューションです。次のサービスと設定を使用して、エンドユーザーにシームレスなエクスペリエンスを提供します。

- **Autodiscovery** サービス: ドメインをストア URL にマッピングし、エンドユーザーがメールアドレスを使用してサインインできるようにします。エンドユーザーは、サインイン時にストア URL を提供する必要はありません。
- 自動更新サービスとエージェント管理: エンドユーザーが指定された Citrix Workspace アプリのバージョンを使用できるように自動で更新します。さまざまなプラットフォームに対してさまざまなアプリのバージョンを柔軟に構成できます。
- クライアントアプリの設定とポリシー: Citrix Workspace アプリのすべてのエンドユーザー設定は一元的に構成および設定できます。これには、ログイン操作、セキュリティ、認証オプション、仮想アプリ、デスクトップ設定などの設定が含まれます。



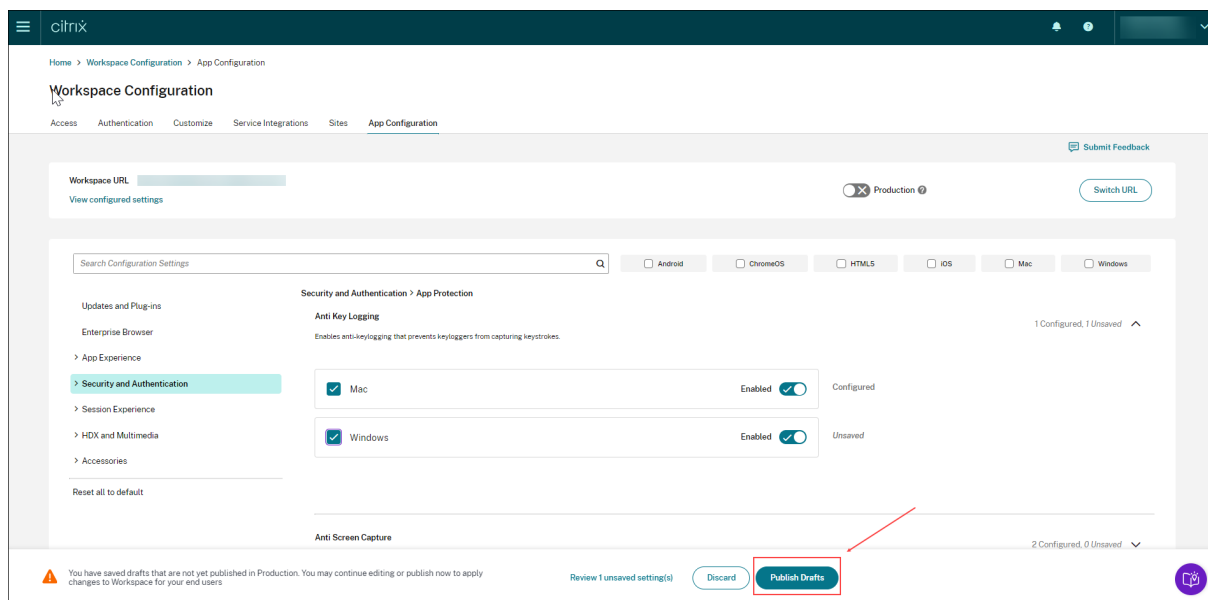
前提条件

アプリ設定を構成する前に、Citrix Workspace アプリのバージョンが指定されたバージョン以上であることを確認してください。詳しくは、次の表を参照してください。

Citrix Workspace アプリプラットフォーム	サポートされている最小バージョン
Windows	最新リリース - 2106、LTSR - 2203.1
Mac	2203.1
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

Global App Configuration Service を使用する方法?

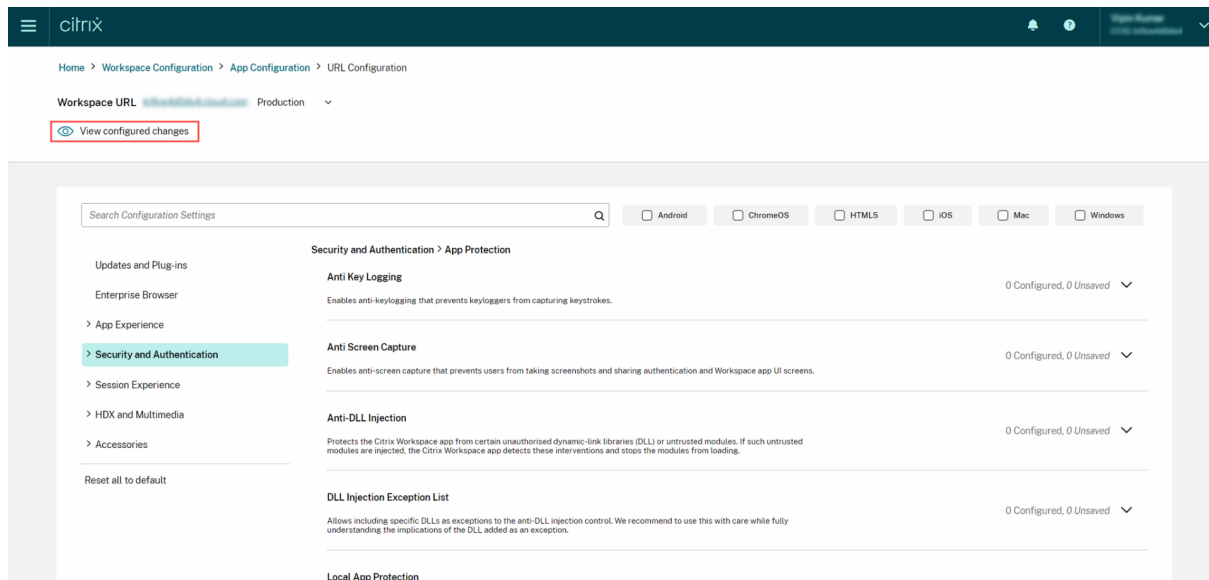
設定を構成するには、Citrix Cloudポータルにサインインし、[ワークスペース構成] > [アプリ構成] に移動します。組織のポリシーに従ってアプリの設定を変更します。次に、[下書きの公開] をクリックして、設定を保存して公開します。



ユーザーインターフェイスには、簡素化されたユーザーエクスペリエンスを実現する次のオプションも用意されています。

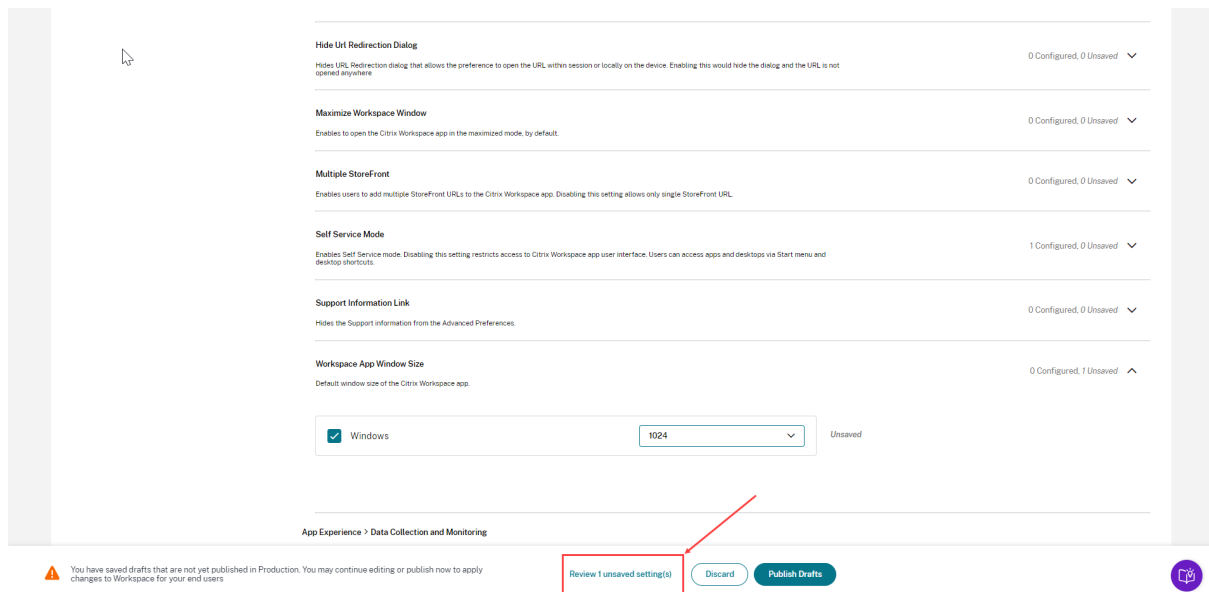
構成された設定の概要を表示する

[構成した設定を表示する] ボタンをクリックすると、現在の構成の概要を表示できます。これにより、それぞれの設定を個別に展開して確認する必要がなくなります。構成されたすべての設定の統合リストにより、現在の構成を包括的に確認し、ユーザーへの影響を評価することができます。

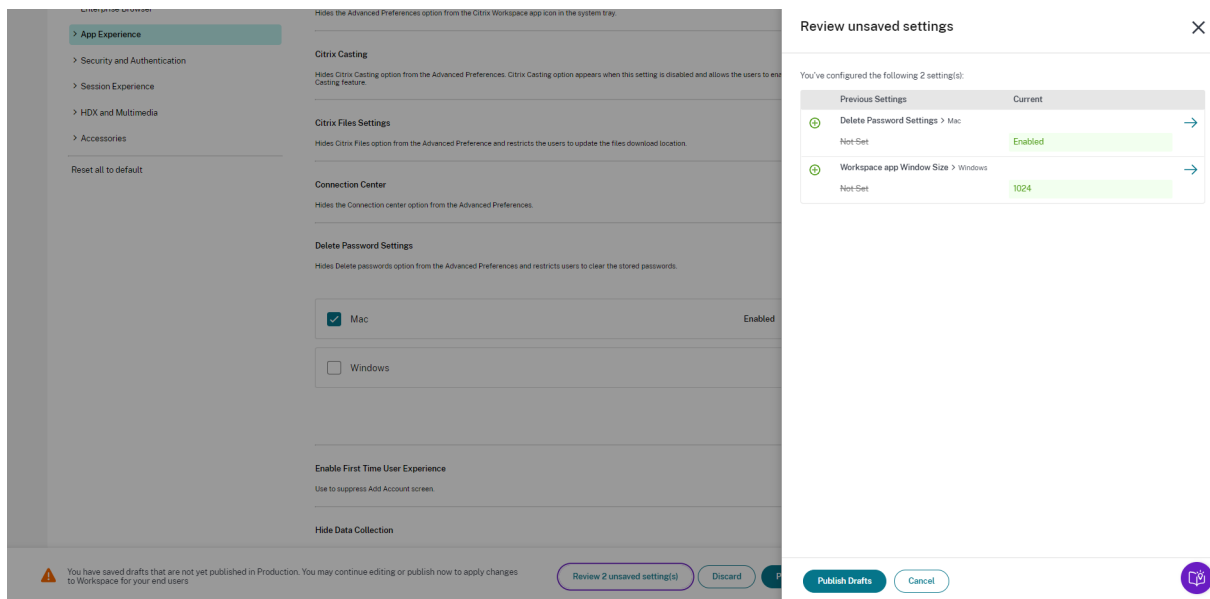


未保存の変更を確認する

構成を公開する前に、未保存の変更の最終確認を実行します。未保存の設定の数が UI に表示され、[未保存の設定を確認] オプションをクリックしてこのリストにアクセスできます。これにより、情報に基づいて変更を加え、データの正確性を維持できます。



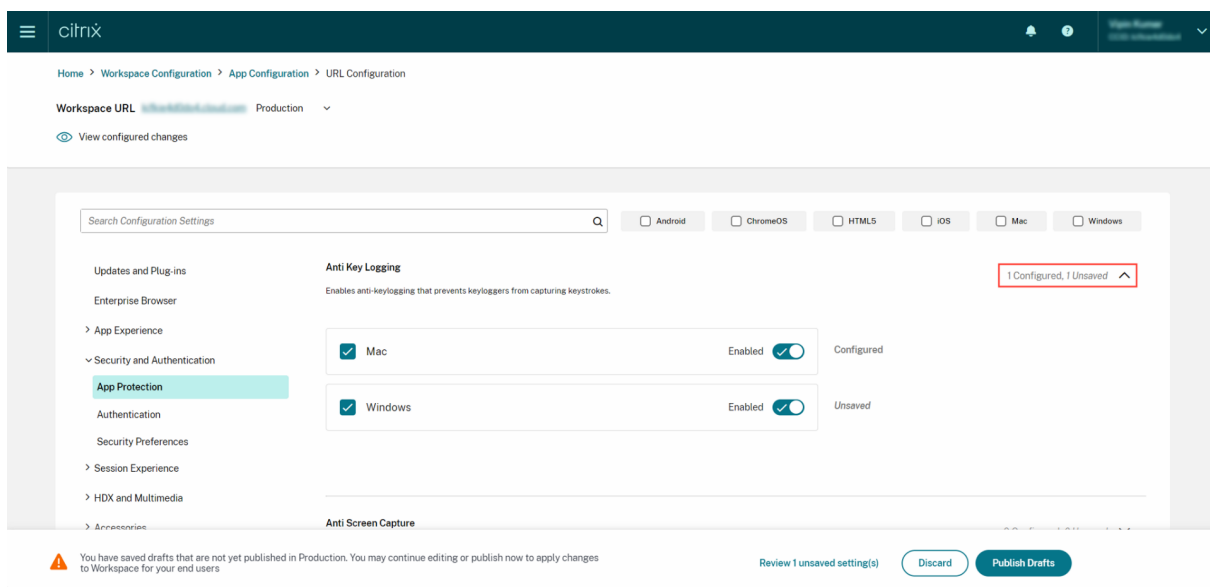
矢印をクリックして未保存の設定に移動することもできます。



強化されたユーザーインターフェイス

それぞれの設定を展開せずにステータスを表示します。各ステップで情報に基づいた決定が簡単にできるように、次のタグが表示されるようになりました。

- 構成済み: 設定がすでに構成されているプラットフォーム (クライアント OS) の数が表示されます。
- 未保存: 構成されているがまだ保存されていない設定の数が表示されます



強化された検索オプション

検索エクスペリエンスが強化され、堅牢でシームレスなエクスペリエンスが提供されます。管理者は、クラウドポータルにサインインし、[アプリ構成] ページで必要な設定を簡単に見つけることができるようになりました。次の検索方法を使用できます。

- 設定の説明を使用した検索

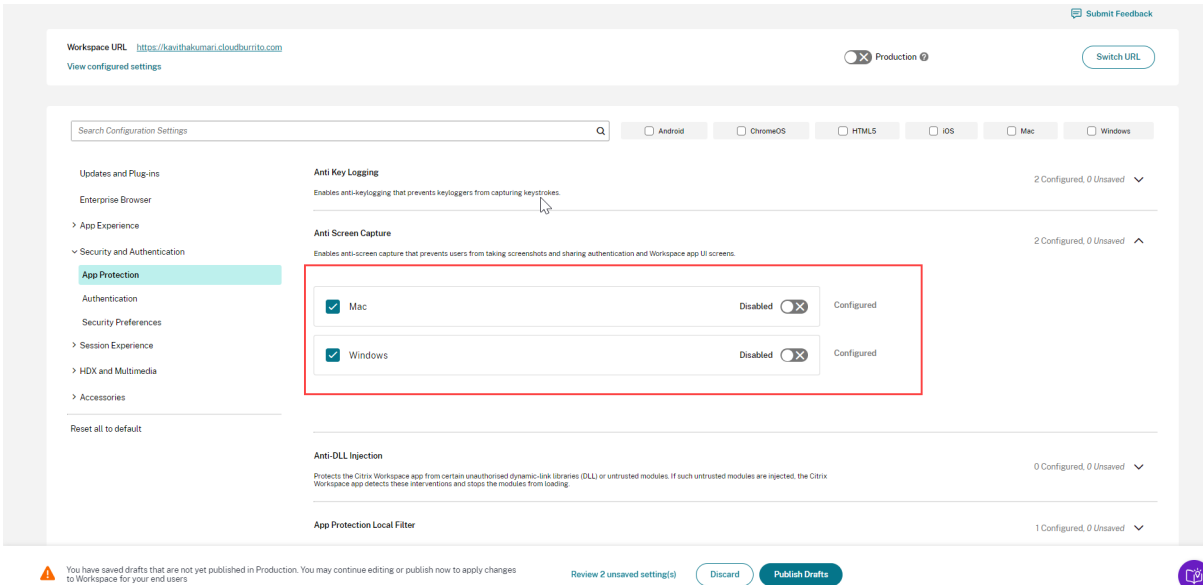
設定の説明内にあるキーワードを入力して設定を見つけることができます。これにより、目的の設定に関連付けられた関連用語を利用した、より柔軟な検索アプローチが可能になります。

- **API** 設定名を使用した検索

対応する API 設定名を入力して設定を検索することができます。この方法により、より正確で的を絞った検索が可能になり、ユーザーは必要な特定の設定をすばやく見つけることができます。

各設定に適用可能なプラットフォームを表示する

各設定には、関連する適用可能なプラットフォームのみが動的に表示されるようになりました。このアプローチにより、簡潔でカスタマイズされたオプションの一覧がユーザーに確実に表示されます。



The screenshot displays the Citrix Workspace configuration page. At the top, the workspace URL is <https://kajihabumari.cloudburst.com>. The environment is set to 'Production'. A search bar is present with the text 'Search Configuration Settings'. Below the search bar, there are filters for platforms: Android, ChromeOS, HTML5, iOS, Mac, and Windows. The 'App Protection' section is expanded, showing settings for 'Anti Key Logging', 'Anti Screen Capture', 'Anti-DLL Injection', and 'App Protection Local Filter'. The 'Anti Screen Capture' section is highlighted with a red box, showing that it is configured for 'Mac' and 'Windows' platforms, both with the 'Disabled' toggle switch turned off. The status for each platform is 'Configured'.

更新された設定を取得する頻度

構成が公開されると、クライアント側で設定が更新されるまでに数時間かかる場合があります。

- 同じセッション内で、次のように設定が更新されます：

プラットフォーム	設定の更新に必要な最大時間
Windows 向け Citrix Workspace アプリ	最大 6 時間
macOS 向け Citrix Workspace アプリ	最大 6 時間
HTML5 向け Citrix Workspace アプリ	最大 3 時間
ChromeOS 向け Citrix Workspace アプリ	最大 3 時間
iOS 向け Citrix Workspace アプリ	最大 6 時間
Android 向け Citrix Workspace アプリ	最大 6 時間

- Windows および macOS の場合、エンドユーザーが Citrix Workspace アプリを終了して再起動すると、設定をすぐに更新できます。
- エンドユーザーが Citrix Workspace アプリにストアを追加すると、そのストアの設定は自動的に更新されま

設定を適用する優先順位

Global App Configuration Service に加えて、Windows の GPO など、エンドユーザー設定の構成に使用できるプラットフォーム固有のツールもあります。

Global App Configuration Service を通じて構成された設定と他のプラットフォームツールの間で競合が発生した場合、設定は次の順序で適用されます。

プラットフォーム	ストアの種類	優先順位
Windows 向け Citrix Workspace アプリ	StoreFront と Cloud	グループポリシーオブジェクト (GPO) > Global App Configuration Service > レジストリ
Mac 向け Citrix Workspace アプリ	StoreFront と Cloud	MDM > Global App Configuration Service > UserDefaults
HTML5 向け Citrix Workspace アプリ	StoreFront	Global App Configuration Service > Configuration.js
	Cloud	Global App Configuration Service

プラットフォーム	ストアの種類	優先順位
ChromeOS 向け Citrix Workspace アプリ	StoreFront	Google 管理ポリシー > Global App Configuration Service > Configuration.js
	Cloud	Google 管理ポリシー > Global App Configuration Service
iOS 向け Citrix Workspace アプリ	StoreFront と Cloud	Global App Configuration Service
Android 向け Citrix Workspace アプリ	StoreFront と Cloud	Global App Configuration Service

制限事項

- Global App Configuration Service は Linux ではサポートされていません。
- Windows と Mac では、Global App Configuration Service を有効にしたストアを複数追加することはできません。

Additional Resources

- [Global App Configuration Service の技術概要](#) (英語)
- [FAQ: Global App Configuration サービスの設定および動作](#) (英語)
- [ウェビナー録画: Global App Configuration サービスの使用方法](#) (英語)
- [Citrix 機能の説明: Global App Configuration サービス](#) (英語)

クラウドストアの設定の構成

November 28, 2023

概要

Global App Configuration Service (GACS) を使用して、クラウドストアの Citrix Workspace アプリ設定を構成できます。これは、管理者が管理対象デバイスと管理対象外デバイスの両方でエンドユーザー向けに Citrix Workspace アプリを構成および管理するのに役立ちます。このサービスは、Windows、Mac、Android、iOS、HTML5、および ChromeOS プラットフォームでサポートされています。

前提条件

- アドレス<https://discovery.cem.cloud.us>に接続できる必要があります。これは、メールアドレスによる検出サービスと Global App Configuration Service が機能するために必要です。
- Citrix Cloud アカウントにアクセスできることを確認します。アクセスできない場合は、<https://onboarding.cloud.com/>からアカウントを作成できます。詳しくは、「[Citrix Cloud への登録](#)」を参照してください。
- Workspace サブスクリプションがあることを確認します。

開始

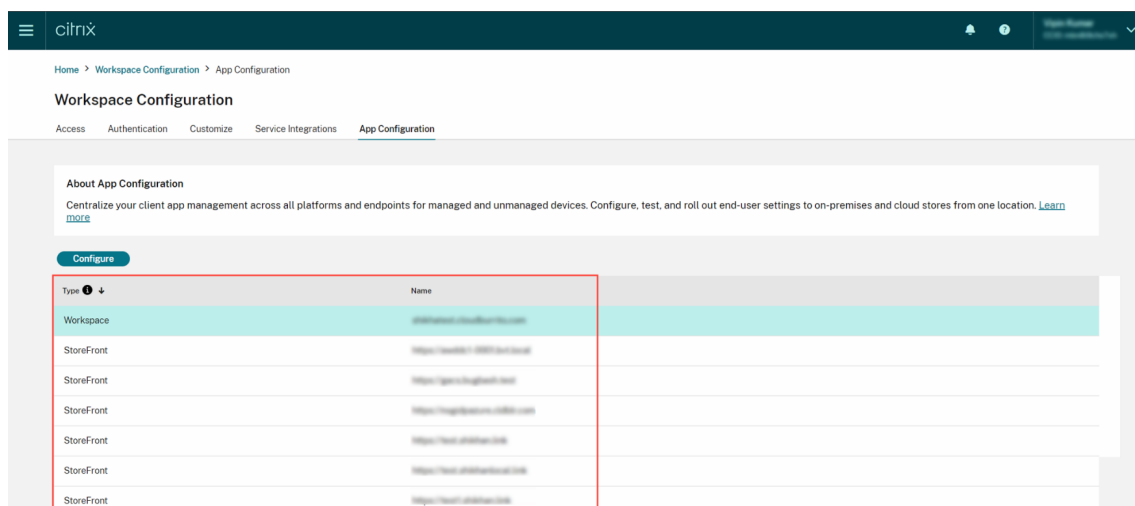
Citrix Cloud アカウントにサインインし、[ワークスペース構成] > [アプリ構成] から設定を構成できます。続行する前に、次の権限があるかどうかを確認してください。

- **Workspace** サブスクリプション: ワークスペース URL を作成するには、Workspace サブスクリプションが必要です。サブスクリプションがない場合、クラウドストアを追加および構成することはできません。オンプレミスストアを構成するオプションのみが表示されます。
- **Workspace URL**: ワークスペースサブスクリプションを持っていて、URL をまだ追加していない場合は、次の画面が表示されます。[クラウドストアの設定を構成する] で [開始] をクリックして、URL を作成できます。

設定を構成する

Citrix Cloud ポータルから Citrix Workspace アプリの設定を構成できます。組織に複数のストアが構成されている場合は、各ストアを個別に構成できます。

1. [Citrix Cloud](#)に移動し、Citrix Cloud 資格情報を使用してサインインします。
2. [ワークスペース構成] > [アプリ構成] に移動します。
3. [**URL** を切り替える] をクリックして、構成を行うストアを選択します。
4. 構成されたストア URL の一覧から、設定をマッピングするストアを選択し、[保存] をクリックします。



5. 要件に応じて、優先するプラットフォームの設定を変更します。

6. [下書きの公開] をクリックして設定を保存します。

注:

設定が Citrix Workspace アプリクライアントに更新されるまでに数時間かかる場合があります。詳しくは、「[更新された設定を取得する頻度](#)」を参照してください。

メールアドレスによる検出をセットアップする

メールアドレスによる検出サービスを使用すると、エンドユーザーがメールアドレスを使用して自動的にサインインできます。ストア URL を提供する必要はありません。

クラウドストアでこのサービスを有効にするには、次の手順を実行する必要があります。

1. [ドメインを要求する](#)
2. [ドメインと URL のマッピングを作成する](#)

ドメインを要求する

ドメインを要求するには、以下の手順に従います:

1. <https://adsui.cloud.com> に移動します。
2. [クレーム] > [ドメイン] > [ドメインの追加] に移動します。
3. 要求するドメインを入力します (例: ace.example.com)。
4. [確認] をクリックします。
5. 画面に表示された DNS トークンをコピーします。

6. DNS TXT レコードを作成するには、サービスプロバイダーポータルに移動し、DNS トークンを追加します。

7. 検証プロセスを開始するには、以下の手順に従います：

- a) [クレーム] > [ドメイン] に移動します。
- b) 追加したドメインに移動し、省略記号メニューをクリックします。
- c) [ドメインの確認] を選択します。
- d) [**DNS** チェックの開始] をクリックします。

確認が完了すると、ドメインの状態が [保留中] から [確認済] に変わります。

ドメインと **URL** のマッピングを作成する

1. [クレーム] > [ドメイン] に移動します。
2. 追加したドメインに移動し、省略記号メニューをクリックします。
3. [別のサーバー **URL** を追加] をクリックします。
4. このドメインにマッピングするストアの URL を入力します。
5. [保存] をクリックします。

オンプレミスストアの設定の構成

November 28, 2023

概要

Global App Configuration Service (GACS) を使用して、オンプレミスストアの Citrix Workspace アプリ設定を構成できます。これは、管理者が管理対象デバイスと管理対象外デバイスの両方でエンドユーザー向けに Citrix Workspace アプリを構成および管理するのに役立ちます。Global App Configuration Service は、Windows、Mac、Android、iOS、HTML5、および ChromeOS プラットフォームでサポートされています。

前提条件

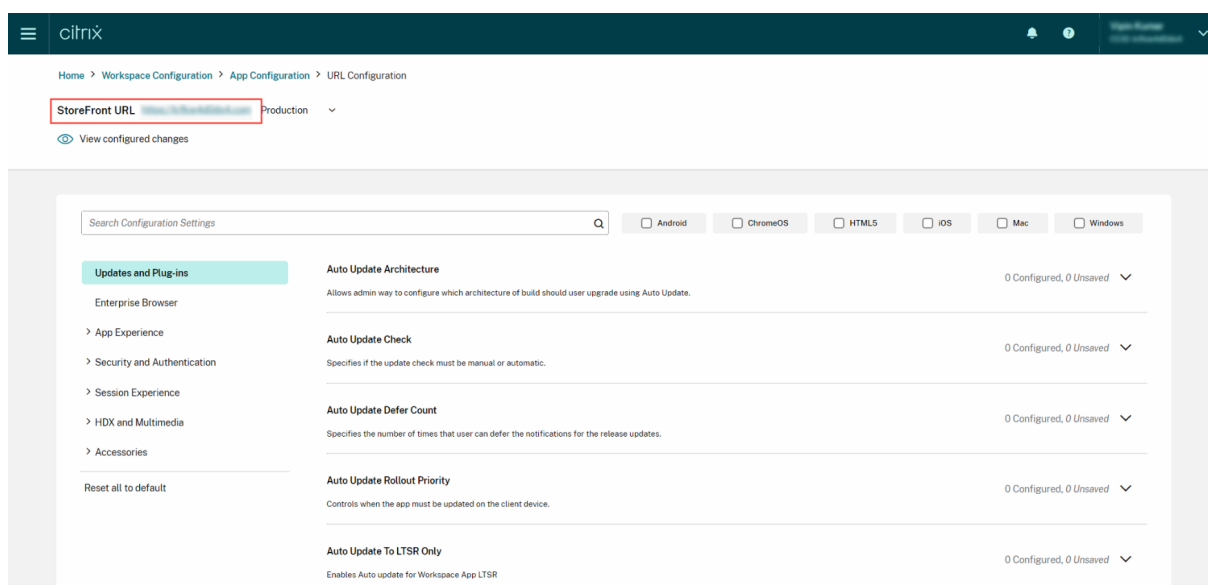
- アドレス <https://discovery.cem.cloud.us> に接続できる必要があります。これは、メールアドレスによる検出サービスと Global App Configuration Service が機能するために必要です。

- Citrix Cloud アカウントにアクセスできることを確認します。まだアカウントをお持ちでない場合は、<https://onboarding.cloud.com/>から作成できます。詳しくは、「[Citrix Cloud への登録](#)」を参照してください。
- オンプレミス環境では、設定を構成する前に URL を要求する必要があります。詳しくは、「[URL の要求](#)」を参照してください。

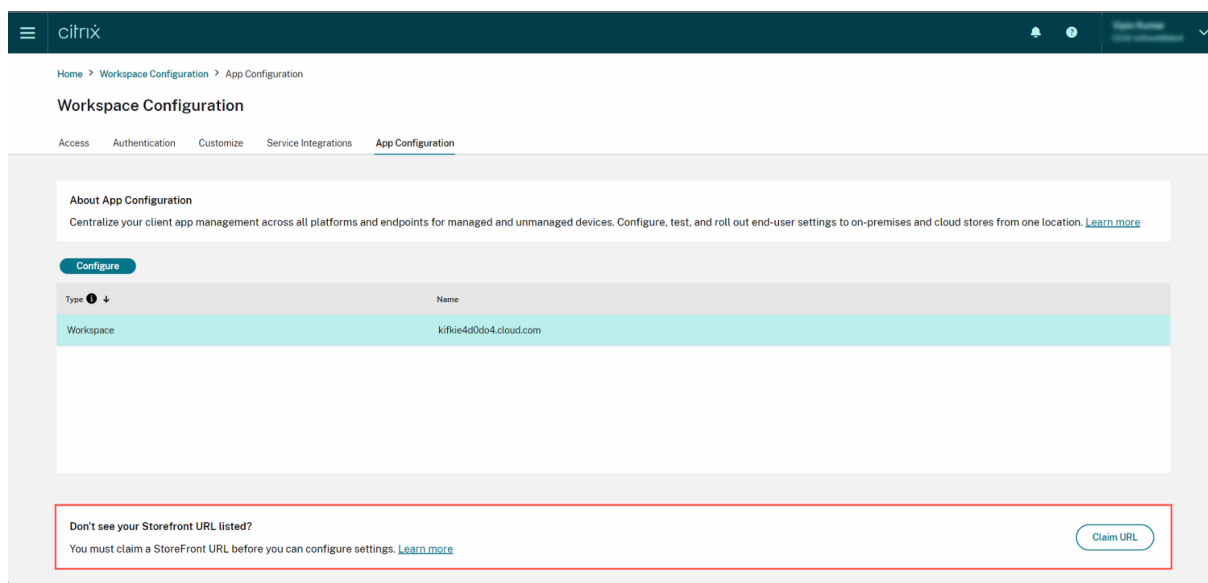
開始

オンプレミスストアの設定を構成するには、Citrix Cloud アカウントにサインインし、[ワークスペース構成] > [アプリ構成] に移動します。

StoreFront URL の所有権を要求した場合は、設定の構成を開始できる次の画面が表示されます。詳しくは、「[設定を構成する](#)」セクションを参照してください。



StoreFront URL の所有権をまだ要求していない場合は、続行する前に URL を保護するように求める次の画面が表示されます。詳しくは、「[オンプレミスストアの URL を要求する](#)」を参照してください。



オンプレミスストアの **URL** を要求する

URL の設定の構成を開始する前に、URL に対する要求を確立することが必須です。

URL を要求するには、以下の手順を実行します。:

1. <https://adsui.cloud.com/url>に移動し、Citrix Cloud 資格情報を使用してサインインします。
2. [クレーム] > [URL] > [URL の追加] に移動します。
3. 要求する URL を入力します。
4. [確認] をクリックします。確認のポップアップが開きます。

注:

オンプレミス環境に NetScaler Gateway がインストールされていない場合、検証プロセス（手順 5 以降）を実行できません。この場合、上記の手順で説明されている手順 1~4 を実行し、[サポートチーム](#)に連絡して、顧客 ID と要求する URL を伝えてください。

5. オンプレミスのセットアップに NetScaler Gateway がインストールされている場合は、次のステップを使用して URL を確認できます。
 - a) ポップアップに表示されるトークンをコピーします。
 - b) Citrix ADC 内でレスポnderアクションとレスポnderポリシーを作成して構成します。
 - c) レスポnderポリシーをグローバルにバインドします。
 - d) <https://<customergatewayurl>/vpn/CitrixClaims> に移動して、レスポnderポリシーが正しく構成されているかどうかを確認します。
 - e) [クレーム] > [URL] に移動し、追加した URL を見つけます。
 - f) 追加された URL の省略記号メニューアイコンをクリックします。

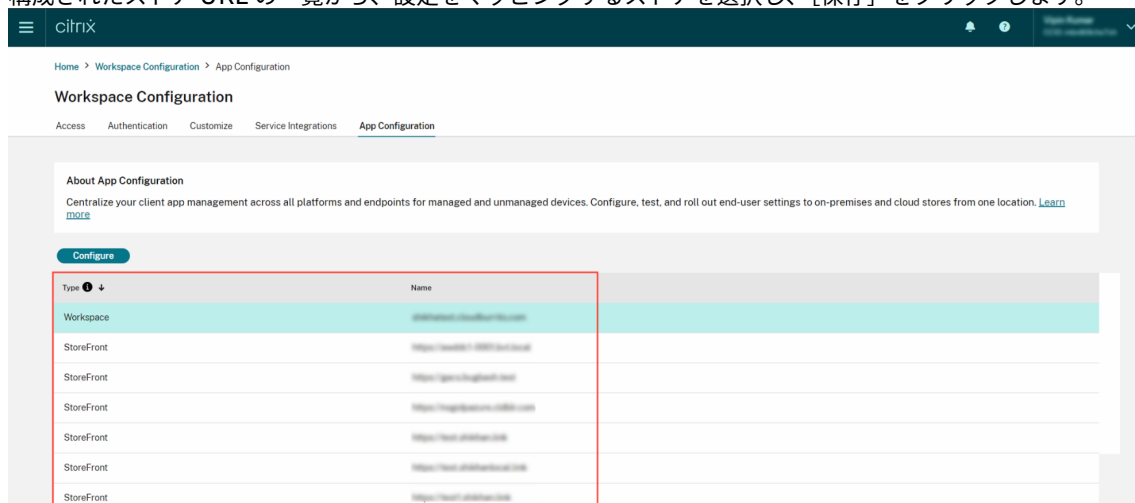
- g) **[URL の確認]** を選択します。
- h) **[要求の確認を開始する]** をクリックして確認プロセスを開始します。

構成が完了すると、ドメインの状態が **[保留中]** から **[確認済]** に変わります。

設定を構成する

URL を要求したら、Citrix Workspace アプリの設定を構成できます。会社に複数のストアが構成されている場合は、それぞれのストアを個別に設定できます。

1. **Citrix Cloud**ポータルに移動し、資格情報を使用してサインインします。
2. **[ワークスペース構成]** > **[アプリ構成]** に移動します。
3. **[URL を切り替える]** をクリックして、構成を行うストアを選択します。
4. 構成されたストア URL の一覧から、設定をマッピングするストアを選択し、**[保存]** をクリックします。



5. 要件に応じて、優先するプラットフォームの設定を変更します。
6. **[下書きの公開]** をクリックして設定を保存します。

注:

設定が Citrix Workspace アプリクライアントに更新されるまでに数時間かかる場合があります。詳しくは、「[更新された設定を取得する頻度](#)」を参照してください。

メールアドレスによる検出をセットアップする

メールアドレスによる検出サービスを使用すると、エンドユーザーがメールアドレスを使用して自動的にサインインできます。ストア URL を提供する必要はありません。

クラウドストアでこのサービスを有効にするには、次の手順を実行する必要があります。

1. [ドメインを要求する](#)
2. [ドメインと URL のマッピングを作成する](#)

ドメインを要求する

ドメインを要求するには、以下の手順に従います：

1. [Autodiscovery サービス](#)に移動します。
2. [クレーム] > [ドメイン] > [ドメインの追加] に移動します。
3. 要求するドメインを入力します（例：ace.example.com）。
4. [確認] をクリックします。
5. 画面に表示された DNS トークンをクリップボードにコピーします。
6. DNS TXT レコードを作成するには、サービスプロバイダーポータルに移動し、DNS トークンを追加します。
7. 検証プロセスを開始するには、以下の手順に従います：
 - a) [クレーム] > [ドメイン] に移動します。
 - b) 追加したドメインに移動し、省略記号メニューをクリックします。
 - c) [ドメインの確認] を選択します。
 - d) [**DNS** チェックの開始] をクリックします。

確認が完了すると、ドメインの状態が [保留中] から [確認済] に変わります。

注：

最大 10 個のドメインを要求できます。10 個を超えるドメインを要求する場合は、[Citrix サポート](#)に連絡し、顧客 ID と URL を伝えてください。

ドメインと **URL** のマッピングを作成する

1. [クレーム] > [ドメイン] に移動します。
2. 追加したドメインに移動し、省略記号メニューをクリックします。
3. [別のサーバー **URL** を追加] をクリックします。
4. このドメインにマッピングするストアの URL を入力します。

テストチャネルの構成

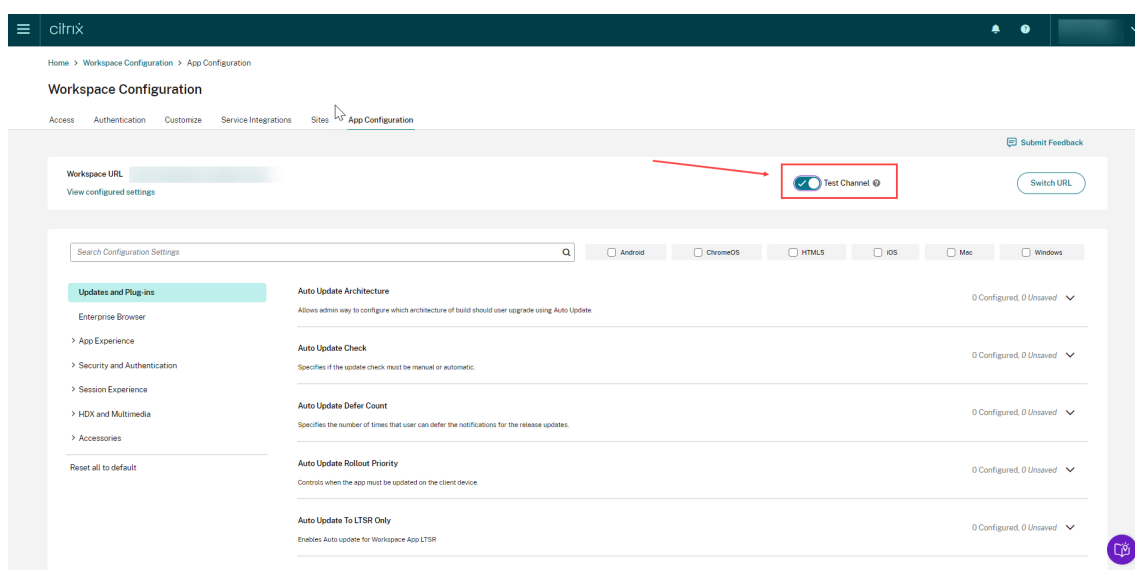
November 28, 2023

エンドユーザーに対して構成を有効にする前に、構成をテストできます。これは、展開後に発生する可能性がある問題を検出して解決するのに役立ちます。

テスト機能により、展開プロセス中の中断やエラーの可能性が大幅に軽減され、全体的なユーザーの満足度が向上します。

構成をテストするには、以下の手順に従います：

1. [Cloud ポータル](#)に移動し、Citrix Cloud 資格情報を使用してサインインします。
2. [ワークスペース構成] > [アプリ構成] に移動します。
3. トグルを [テストチャンネル] に切り替えます。デフォルトでは [製品版] に設定されています。



4. 要件に応じて、優先するプラットフォームの設定を変更します。
5. 次に、[下書きの公開] をクリックして、設定をテストチャンネルに公開します。

注：

Global App Configuration Service は、1つのストアにつき、製品版（デフォルト）チャンネルとテストチャンネルの2つのチャンネルのみをサポートします。

エンドユーザーデバイスでのチャンネルサポートの構成

Windows

Windows デバイス上で管理者が定義した構成をテストするには、ユーザーは次のレジストリを作成する必要があります。

```
1 Path- HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
2 Name- AppConfigChannelName
3 Type- REG_SZ
4 Value- testrolloutchannel1
```

```
5  
6 <!--NeedCopy-->
```

Mac

Mac デバイス上で管理者が定義した構成をテストするには、ユーザーは次の手順を実行する必要があります。

1. 次のコマンドを使用して、Global App Configuration Service のテストチャンネルの名前を設定します：

```
1 defaults write com.citrix.receiver.nomas GACSCChannelName  
   testrolloutchannel1  
2  
3 <!--NeedCopy-->
```

2. 次のコマンドを使用して、Citrix Workspace ヘルパーを再起動します：

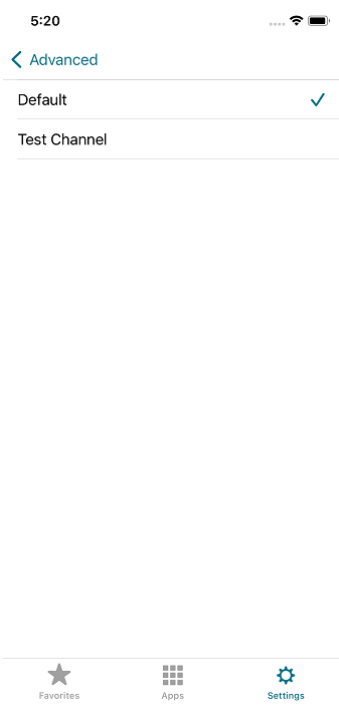
```
1 launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.  
   plist  
2  
3 launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.  
   plist  
4  
5 <!--NeedCopy-->
```

デバイスが再起動すると、テストチャンネルの構成が自動的に取得されます。

iOS

iOS デバイス上で管理者が定義した構成をテストするには、次の手順を実行します：

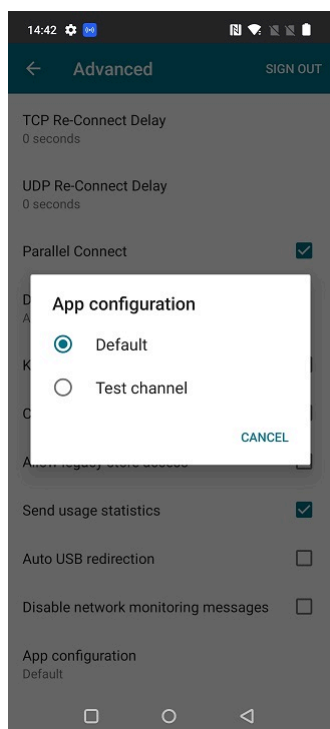
1. Citrix Workspace アプリにサインインします。
2. [設定] > [詳細] > [アプリ構成] に移動します。
3. テストチャンネルを選択します。
4. これで、管理者が定義した構成をテストできるようになりました。



Android

Android デバイス上で管理者が定義した構成をテストするには、次の手順を実行します。

1. Citrix Workspace アプリにサインインします。
2. [設定] > [詳細] > [アプリ構成] に移動します。
3. テストチャンネルを選択します。
4. これで、管理者が定義した構成をテストできるようになりました。



ワークスペース環境の管理

November 28, 2023

この記事では、利用者がワークスペースにアクセスして、ワークスペースを利用する方法の概要を説明します。ワークスペースのエクスペリエンスを向上させるためのカスタマイズオプションについて説明し、一般的な問題の解決策を提供します。

ワークスペースへのアクセス

利用者は、次の 2 つの方法で Citrix Workspace にアクセスできます：

- ブラウザーで Workspace URL を使用して。
- 利用者のデバイスにインストールした Citrix Workspace アプリで。

ブラウザーアクセス

利用者は、ブラウザー経由でサインインする際に、Edge、Chrome、Firefox、または Safari の最新バージョンを使用する必要があります。ユーザーは、ワークスペース URL を入力してワークスペースにアクセスできます。詳しくは、「[Workspace Browser Compatibility](#)」を参照してください。

Workspace URL はデフォルトで有効になっており、通常は次の形式です: <https://yourcompanyname.cloud.com>。Workspace URL を構成する方法については、「[Workspace URL](#)」を参照してください。

Citrix Workspace アプリのアクセス

ワークスペースにアクセスするには、最新バージョンの Citrix Workspace アプリを使用することをお勧めします。

Citrix Workspace アプリは、Citrix Receiver に代わるネイティブインストールされたアプリであり、プラットフォーム間で Workspace ユーザーインターフェイス (UI) の一貫したユーザーエクスペリエンスを提供します。Citrix Workspace アプリは、さまざまなオペレーティングシステム向けに提供されています。詳しくは、[Citrix Workspace アプリ](#)の製品ドキュメントを参照してください。

Citrix Receiver を使用している場合、ユーザーが Workspace UI 機能のすべてを使用できるように、Citrix Workspace アプリへのアップグレード方法をユーザーに説明してください。プラットフォームごとの Citrix Workspace アプリでサポートされている機能について詳しくは、「[Workspace アプリの機能マトリックス](#)」を参照してください。

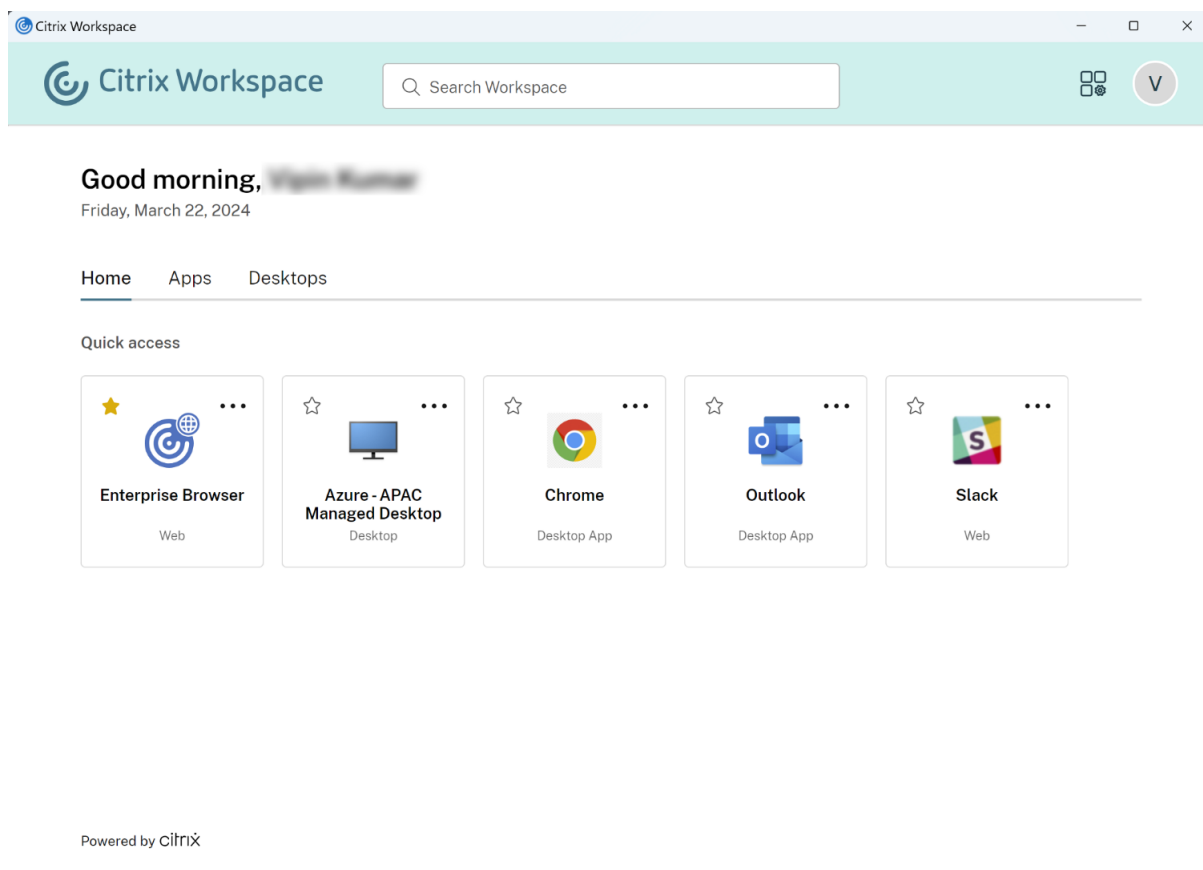
Citrix Workspace アプリをインストールする方法については、「[Citrix Workspace アプリのダウンロード](#)」を参照してください。

Citrix Workspace アプリソフトウェアをインストールできないデバイスでは、HTML5 互換のブラウザから HTML5 向け Citrix Workspace アプリを使用してアクセスすることもできます。

Workspace のユーザーインターフェイスと機能

新規顧客: ワークスペース環境を初めて使用する利用者の場合、最新バージョンの UI を利用できます。

既存顧客: 以前のバージョンの Citrix Workspace アプリを使用している場合、更新された UI が表示されるまでに約 5 分かかることがあります。古いバージョンの UI が一時的に表示されることがあります。



Citrix Workspace UI は、次の機能で構成されています：

シングルサインオン (SSO)

Citrix Workspace は、別の形式の認証を必要とするセカンダリリソースへのシングルサインオン (SSO) により、シームレスなエクスペリエンスを提供します。

カードのレイアウト

アプリ、デスクトップ、ファイル、操作、およびアクティビティフィードは、「カード」レイアウトで表示されます。ポップアップウィンドウに詳細と操作が表示されます。

設定

利用者は、Workspace UI の右上隅にあるプロフィールアイコンを選択したときに表示されるメニューから [設定] にアクセスします。

プロフィールアイコン

利用者は、自分のプロフィールに画像をアップロードできます。プロフィール画像が設定されていない場合、画像はデフォルトで、利用者の Active Directory の表示名に基づいたアイコンになります。

検索

UI の上部にある検索ツールを使用すると、ワークスペース内のすべてのリソースを検索でき、利用者は検索結果から直接アプリを開くことができます。検索には最低 3 文字が必要です。

最近とお気に入りのビュー

利用者はアプリ、デスクトップ、ファイルの [最近] と [お気に入り] ビューを選択できます。

[ワークスペース構成] で、利用者がこの機能を使用できるように、または使用できないように、[お気に入り] を構成できます。Citrix Workspace の [お気に入り] 機能の有効化と無効化について詳しくは、「[お気に入りを許可](#)」を参照してください。

2 要素認証 (オプション)

Citrix Workspace の利用者が 2 要素認証を使用する前に、利用者はデバイスを登録する必要があります。登録時に、Workspace は、利用者が認証アプリでスキャンするための QR コードを提示します。認証アプリは、[Citrix SSO](#) などの [時間ベースのワンタイムパスワード \(TOTP: Time-Based One-Time Password\)](#) 標準に準拠している必要があります。

注:

登録プロセスを円滑にするために、事前にターゲットデバイスに [Citrix SSO](#) をダウンロードしてインストールすることをお勧めします。

2 要素認証に登録するには、利用者に次のように案内します:

1. ブラウザーを開き、Workspace サインインページに移動し、[トークンをお持ちではない場合] を選択します。
2. ユーザー名を `domain\username` 形式で入力するか会社のメールアドレスを入力して、[次へ] を選択します。Citrix Cloud から利用者に、一時的な確認コードが記載されたメールが送信されます。
3. プロンプトが表示されたら、確認コードと Active Directory アカウントのパスワードを入力し、[次へ] を選択します。

重要:

確認コードは、有効期間が 24 時間の一時トークンであり、利用者のデバイスを登録するためにのみ使用されます。利用者は、2 要素認証でこのコードを使用してワークスペースにサインインしてはいけません。

ん。

4. 認証アプリで、QR コードをスキャンするか、確認コードを手動で入力します。
5. [完了] と [サインイン] を選択して登録を完了します。

登録完了後、利用者は Citrix Workspace サインインページに戻り、認証アプリに表示されるトークンを使用して、Active Directory の資格情報を入力できます。

2 要素認証のトークンとしてサポートされているのは、登録済みデバイス上の認証アプリから生成された確認コードのみです。利用者は、登録処理中に送信された一時的なメールトークンを使用してはいけません。

ワークスペースのカスタマイズ

[ワークスペース構成] で、各ユーザーのワークスペースの利用者エクスペリエンスをカスタマイズして、組織の特定の要件を満たすことができます。

- ワークスペースの [アクティビティフィード] と [操作] カード内で、ターゲットを絞った通知を構成する方法については、「[ワークスペース通知のカスタマイズ](#)」を参照してください。
- ロゴやカスタムテーマなど、ワークスペースの外観をカスタマイズするには、「[ワークスペースの外観をカスタマイズする](#)」を参照してください。
- 利用者による [お気に入り] の作成やデスクトップの自動起動を許可するなど、利用者のワークスペース操作方法をカスタマイズする方法については、「[ワークスペース操作をカスタマイズする](#)」を参照してください。
- プライバシーとセキュリティポリシーをカスタマイズするには、「[セキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。プライバシーおよびセキュリティポリシーには、タイムアウト期間、サインインポリシー、エンドユーザーのパスワード管理などの設定が含まれます。

トラブルシューティング

認証方法を変更した後、ログアウトして再度ログインする

認証方法を変更した後、ログインしている利用者にエラーメッセージが表示されることがあります。利用者は Citrix Workspace からログアウトし、ブラウザまたは Citrix Workspace アプリを閉じて、約 5 分間待ってから再度ログインする必要があります。これにより、新しい認証方法を使用してサインインできるようになります。

詳しくは、「[認証方法の選択または変更](#)」を参照してください。

サービスサブスクリプションを変更した後に更新する

サービスサブスクリプションを変更した場合、利用者はローカルの Citrix Workspace アプリを手動で更新する必要があります。Windows 向け Citrix Workspace アプリを更新するには:

1. Windows システムトレイの Citrix Workspace アイコンを右クリックし、[高度な設定] > [Citrix Workspace をリセットする] の順に選択します。
2. Windows 向け Citrix Workspace アプリを開き、[アカウント] > [追加] を選択します。
3. Workspace URL を入力してから [追加] を選択します。

ブラウザから Citrix Workspace アプリを更新することもできます。ブラウザから更新する場合：

1. Windows システムトレイの Citrix Workspace アイコンを右クリックし、[高度な設定] > [Citrix Workspace をリセットする] の順に選択します。
2. ブラウザーに Workspace URL を入力し、サインインします。
3. [設定] > [アカウント設定] > [詳細] > [Workspace 構成のダウンロード] で、構成ファイルをダウンロードします。

これにより、ワークスペースをローカルの Citrix Workspace アプリに追加する、拡張子が **.cr** のファイルがダウンロードされます。

ワークスペースの外観をカスタマイズする

October 12, 2023

ワークスペースのユーザーインターフェイスをカスタマイズする

このセクションでは、[構成] > [カスタマイズ] > [外観] でテーマを更新してワークスペースの外観をカスタマイズする方法について説明します。

テーマを使用すると、ワークスペースの色とロゴを構成できます。ロゴが歪んだりエラーメッセージが表示されたりしないように、ロゴはサイズの要件を満たしている必要があります。

ロゴ	必要なサイズ	最大サイズ	サポートされる形式
サインインロゴ	480 × 120 ピクセル	2MB	JPEG、JPG、PNG
サインイン後のロゴ	340 × 80 ピクセル	2MB	JPEG、JPG、PNG

ワークスペースの外観の変更は、[保存] を選択した直後に有効になります。

デフォルトのテーマをカスタマイズする

デフォルトのテーマには、サインインロゴ、サインイン後に利用者に表示されるワークスペースのロゴと色が含まれます。これらの要素の 1 つ、一部、またはすべてをデフォルトのテーマに変更できます。

Workspace Configuration

- Access
- Authentication
- Customize
- Service Integrations
- Sites
- Service Continuity

- Appearance
- Features
- Preferences

Customize how subscribers will see their workspace.

Cancel Update

Default Appearance

Sign-in Appearance

Logo

This logo will appear on the sign-in page.



After Sign-in Appearance

Logo

This logo will appear after sign-in.



Colors

These colors appear in sign-in screens and within the workspace experience.

Banner color:



Accent color:

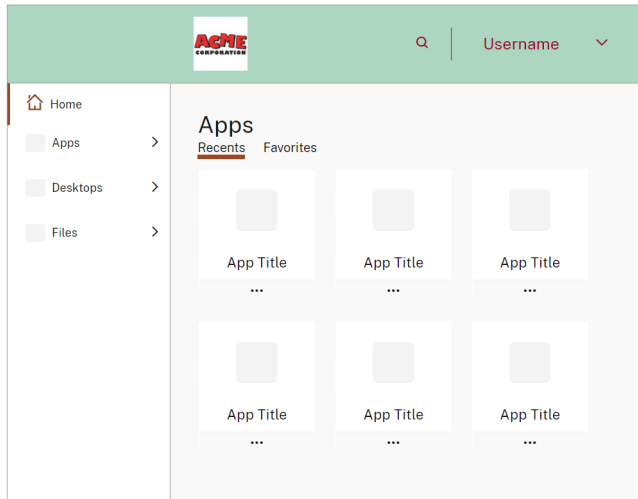


Banner text and icon color:



Preview

This is how your workspace will look:



Reset to Default

Appearance themes

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

+ Add theme



サインインの外観をカスタマイズする

サインインページでは、ロゴのみを置き換えることができます。色を含むサインインページの残りの部分は変更されません。



The image shows a login form for Citrix Workspace. At the top center is the Citrix logo, a stylized 'C' composed of three concentric, curved lines. Below the logo is the text 'Citrix Workspace' in a dark teal font. Underneath is a 'Username' label followed by a text input field containing the placeholder text 'domain\user or user@domain.com'. Below that is a 'Password' label followed by a text input field containing the placeholder text 'Enter password'. At the bottom of the form is a large, rounded teal button with the text 'Sign In' in white.

変更はすぐに反映されます。ローカルの Citrix Receiver アプリで、更新されたユーザーインターフェイスが表示されるまで、5分程度かかる場合があります。

注:

サインインロゴの変更は、Azure AD や Okta などのサードパーティの ID プロバイダーを使用してワークスペースに認証するユーザーには影響しません。

Azure AD サインインページをカスタマイズする方法については、[Microsoft 社のドキュメント](#)を参照してください。Okta がホストするサインインページをカスタマイズする方法については、[Okta 開発者向けドキュメント](#)を参照してください。

[ワークスペース構成] ではなく Citrix ADC アプライアンスで構成された、オンプレミスの Citrix Gateway サインインページをカスタマイズすることもできます。詳しくは、[Support Knowledge Center の記事](#)を参照してください。

ワークスペースの外観をカスタマイズする

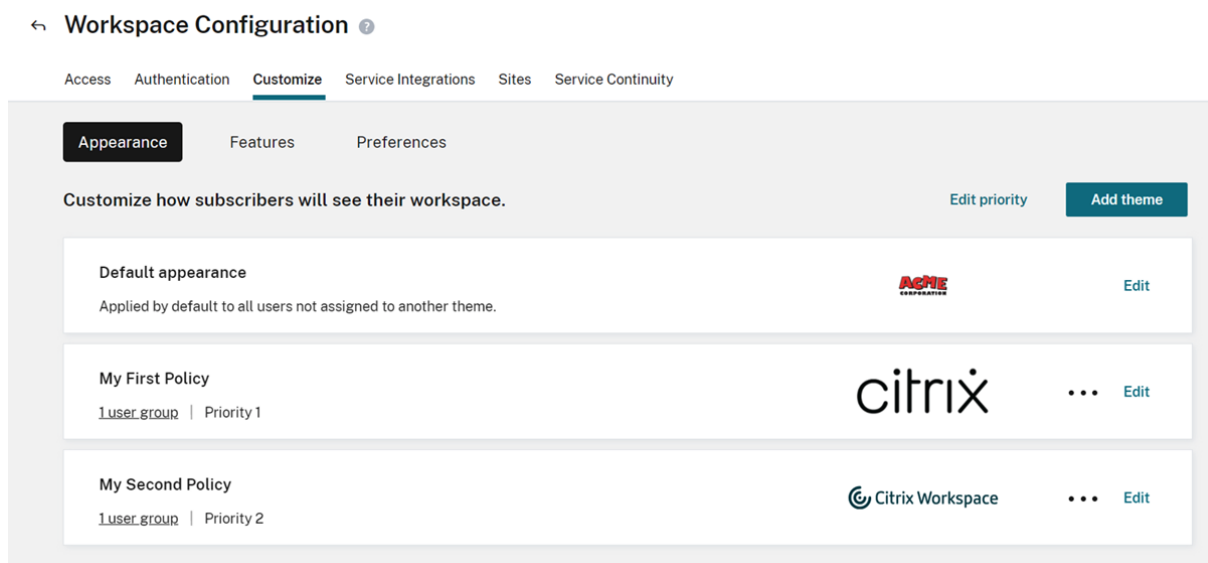
サインインロゴは、利用者がサインインした後にワークスペースの左上に表示されるロゴと同じである必要はありません。ワークスペースのロゴを置き換えるだけでなく、ワークスペースのバナー、アクセント、テキストとアイコンの色を定義できます。

複数のカスタムテーマを作成する

重要:

これはシングルテナント機能です。顧客が Citrix Service Provider テナントである場合は、独自のリソースの場所、Cloud Connector、および専用の Active Directory ドメインが必要です。リソースの場所、Cloud Connector、および Active Directory ドメイン（マルチテナント）を共有する Citrix Service Provider テナントには、現在対応していません。

特定のユーザーグループに対して、複数の Citrix Workspace テーマを構成して優先順位を付けることができます。これらのカスタムテーマは、デフォルトのテーマの下で個別のカードに表示されます。複数のテーマを設定しない場合、既存（デフォルト）のテーマがすべてのユーザーに適用されます。



カスタムテーマを構成する

デフォルトのテーマの下に最初のカスタムテーマを追加するには、[デフォルトの外観] セクションの下にあるカードの左下の **[Add theme]** を選択します。

デフォルトのテーマの下に少なくとも 1 つのカスタムテーマがある場合は、既存のテーマ一覧の右上にある **[Add theme]** を選択します。

1. カスタムテーマを構成します:

- a) ロゴをアップロードします (オプション)。
- b) バナー、アクセント、テキストとアイコンの色を定義します (オプション)。

Add an appearance theme ×

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

After Sign-in Appearance • Theme Details

Logo
This logo will appear after sign-in.



Colors
These colors appear in sign-in screens and within the workspace experience.

Banner color:

Accent color:

Banner text and icon color:



2. **[Theme Details]** を選択し、テーマのわかりやすい名前を入力します。

Add an appearance theme ×

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)


After Sign-in Appearance • **Theme Details**


Name your theme ?

Assign users and groups: ?

Select an identity provider

Search for a group to add



3. テーマにユーザーグループを割り当てます。

- a) ID プロバイダーと、プロンプトが表示された場合はそのドメインを選択します。
- b) カスタムテーマに追加するユーザーグループを検索します。
- c) グループの横にあるプラス記号 (+) ボタンを選択します。
- d) テーマに追加するグループごとに、この手順を繰り返します。

Add an appearance theme ×

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

After Sign-in Appearance

Theme Details

Name your theme ●

My First Policy

Assign users and groups: ●

Select an identity provider

Active Directory

Select a domain

domain.com

Search for a group to add

group

User groups (1):

Group

4. [プレビュー] を選択して、ワークスペースが利用者にどのように表示されるかを確認します。完了後は、テーマを保存します。

注:

以前の紫色のユーザーインターフェイスで作業している場合は、[ワークスペースのプレビュー] でプレビューが表示されません。

5. 新しいカスタムテーマの追加を続行するには、手順 1 から 4 を繰り返します。

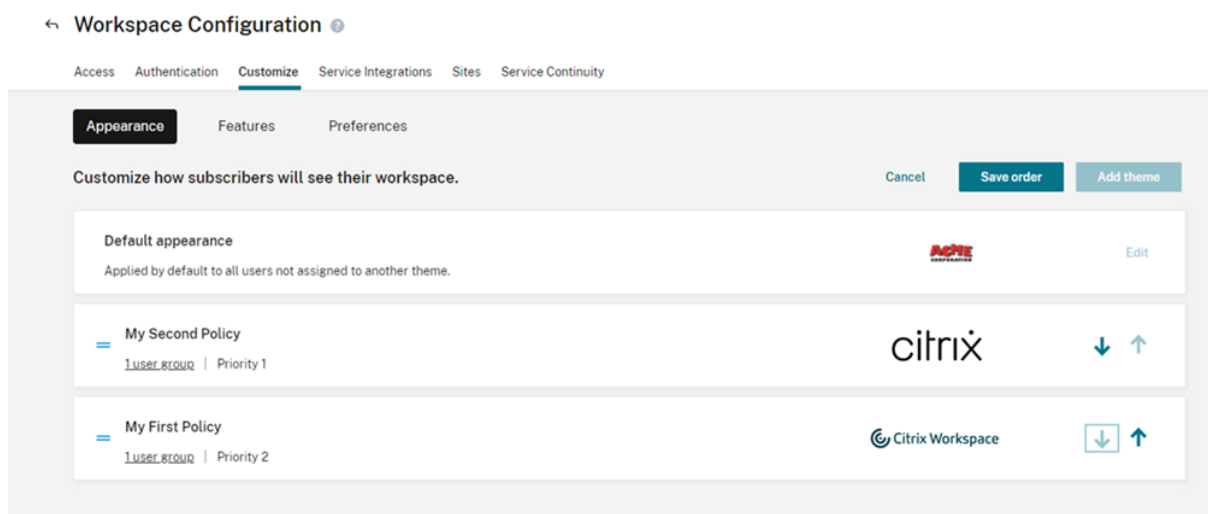
カスタムテーマに優先順位を付ける

ユーザーが複数のユーザーグループに属し、各ユーザーグループは異なるテーマに一致している場合があります。カスタムテーマの相互の優先度を設定することにより、利用者が複数のテーマに一致する場合に表示するテーマを定義できます。

重要

カスタムテーマの相対的な優先順位付けを機能させるには、デフォルトのテーマで 2 つ以上のカスタムテーマを構成する必要があります。

1. テーマの一覧の右上にある **[Add theme]** の横の **[優先度の編集]** を選択します。
2. 次の 2 つの方法のいずれかで、テーマの優先度を並べ替えることができます:
 - 各テーマの右側にある矢印を使用します。
 - カードの左側にあるハンドルを使用して、個々のテーマを一覧の上下にドラッグします。
3. 項目を並べ替えた後、**[順位を保存]** を選択します。



ワークスペース操作をカスタマイズする

November 28, 2023

[ワークスペース構成] > [カスタマイズ] > [基本設定] で、利用者がワークスペースを操作する方法をカスタマイズします。

サインインエクスペリエンスに影響を与えるワークスペース基本設定をカスタマイズして会社の要件に合わせる場合は、「[ワークスペースのセキュリティとプライバシーポリシーをカスタマイズする](#)」を参照してください。

ログイン前およびログイン後のワークスペースの外観をカスタマイズする場合は、「[ワークスペースの外観をカスタマイズする](#)」を参照してください。

キャッシュを許可

[キャッシュを許可] 設定は、Web ブラウザー経由で Citrix Workspace にアクセスする利用者のパフォーマンスを向上させます。サポートされている Web ブラウザーを使用して Citrix Workspace にアクセスする場合、キャッシュを使用できます。ローカルにインストールされた Citrix Workspace アプリを使用している場合、キャッシュは使用できません。

キャッシュを有効にすると、一部の機密データが利用者のデバイスにローカルに保存される場合があります。このデータはファイルのメタデータで構成され、利用者の認証済み ID に固有のキーで暗号化されます。暗号化されたデータは、利用者のデバイス上にある Web ブラウザーの `localStorage` プロパティに保存されます。

キャッシュを無効にすると、次に利用者が Web ブラウザーを介して Citrix Workspace にサインインしたときに、暗号化されたデータが削除されます。また利用者は、Web ブラウザーから閲覧データを消去することにより、このデータを手動でページできます。

お気に入りを許可

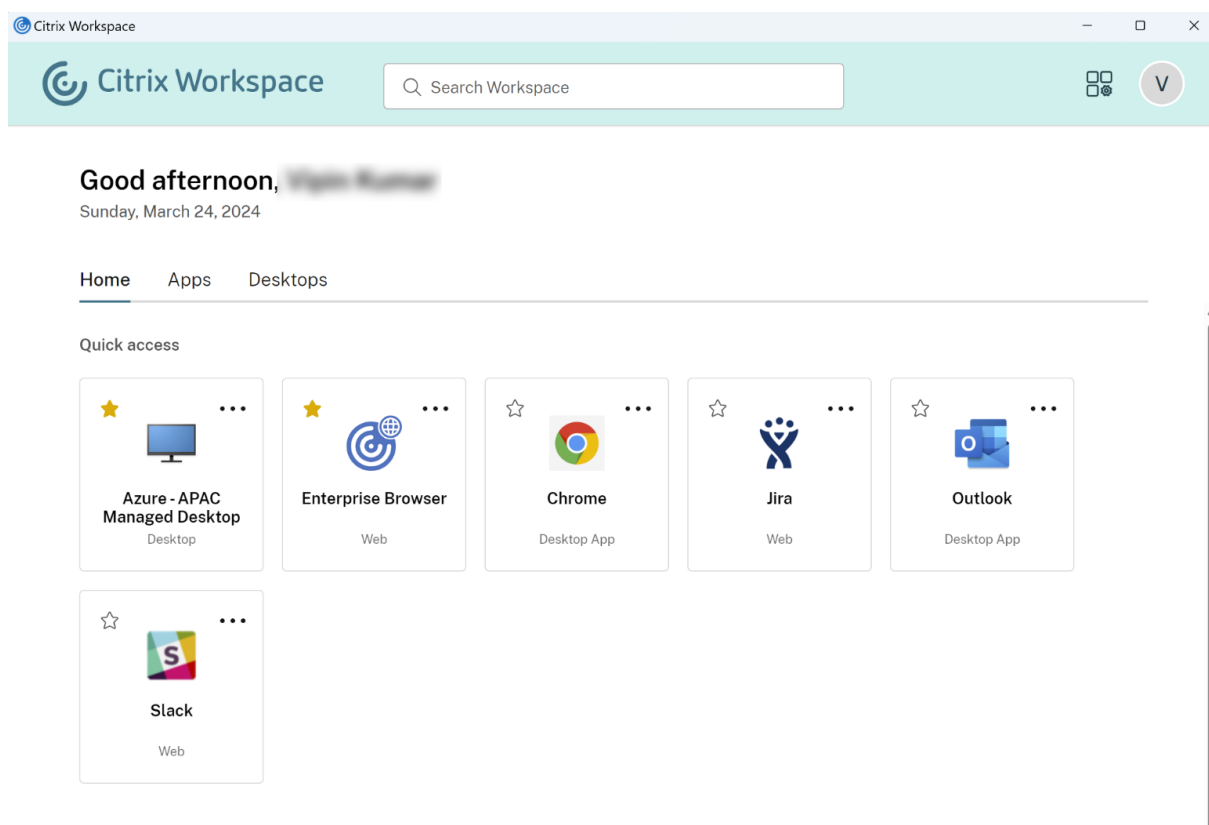
[ワークスペース構成] と新しい Workspace エクスペリエンスへのアクセス権がある顧客は、利用者がアプリとデスクトップのリソースをお気に入りに登録またはお気に入りから登録解除できるように設定できます。[お気に入りを許可] 機能はデフォルトで有効にされています。

注:

- 一部の既存の顧客（2017年12月から2018年4月の間にワークスペースの利用を開始した顧客）の場合、[お気に入りを許可] がデフォルトで [無効] になっています。管理者は、利用者に対してこの機能を有効にするタイミングを決定できます。

[お気に入りを許可] の利用者エクスペリエンス

有効な場合（デフォルト）、利用者は（必須ではない）各アプリおよびデスクトップカードの左上隅にある星アイコンを使用して、最大 250 までお気に入りを追加できます。お気に入りに追加されると、星は枠のみから黄色の塗りつぶしに変化します。



利用者が 250 個を超えてお気に入りを追加すると、「最も古いお気に入り」（または最新のお気に入りを保持するために必要な数）が削除されます。

無効にすると、ワークスペース利用者にアプリとデスクトップカードに星が表示されたり、ナビゲーションバーにこ

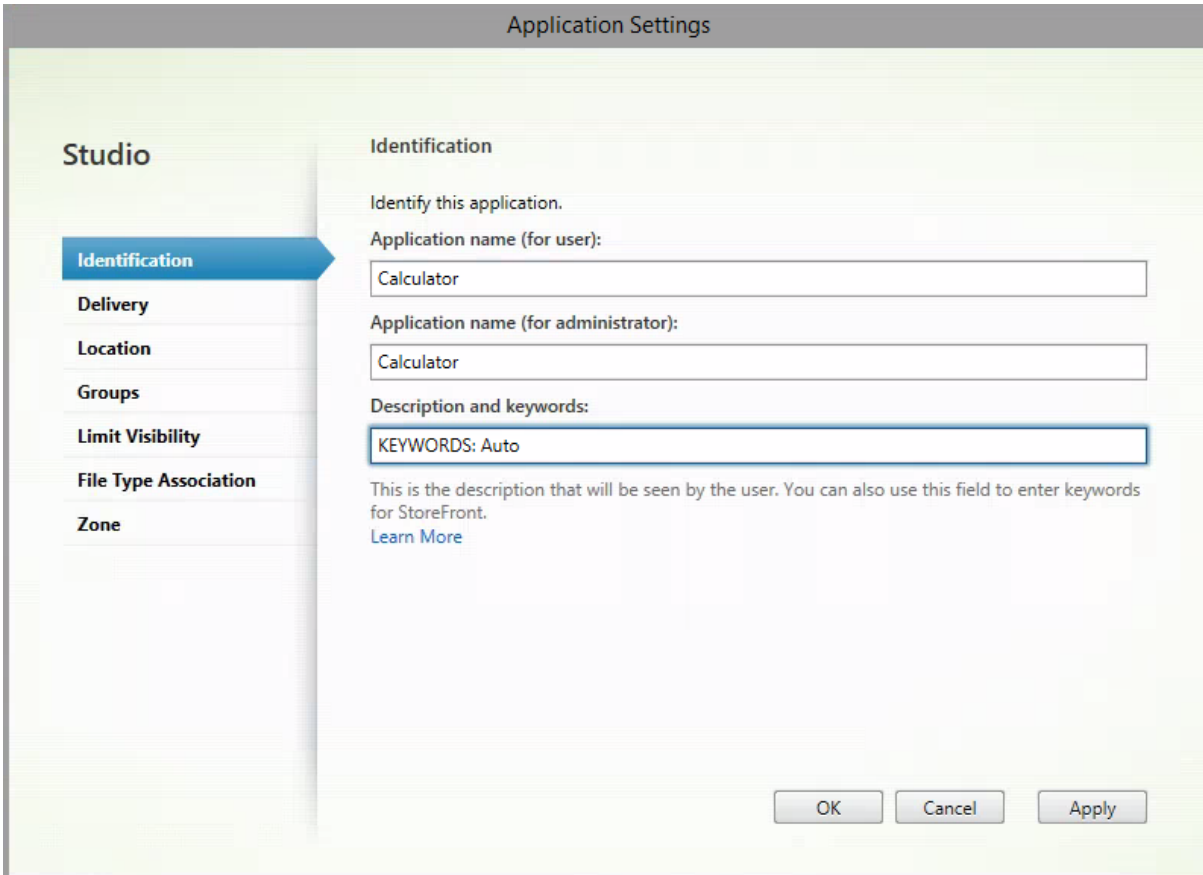
これらのリソースの [すべてのアプリ] と [お気に入り] サブメニューが表示されたりすることはありません。アプリおよびデスクトップのお気に入りは削除されません。お気に入りを再度有効にすると復元できます。

注:

利用者が構成されたデスクトップへのアクセス権を持っていない場合、サイドバーのデスクトップ選択は表示されません。

アプリとデスクトップのキーワード

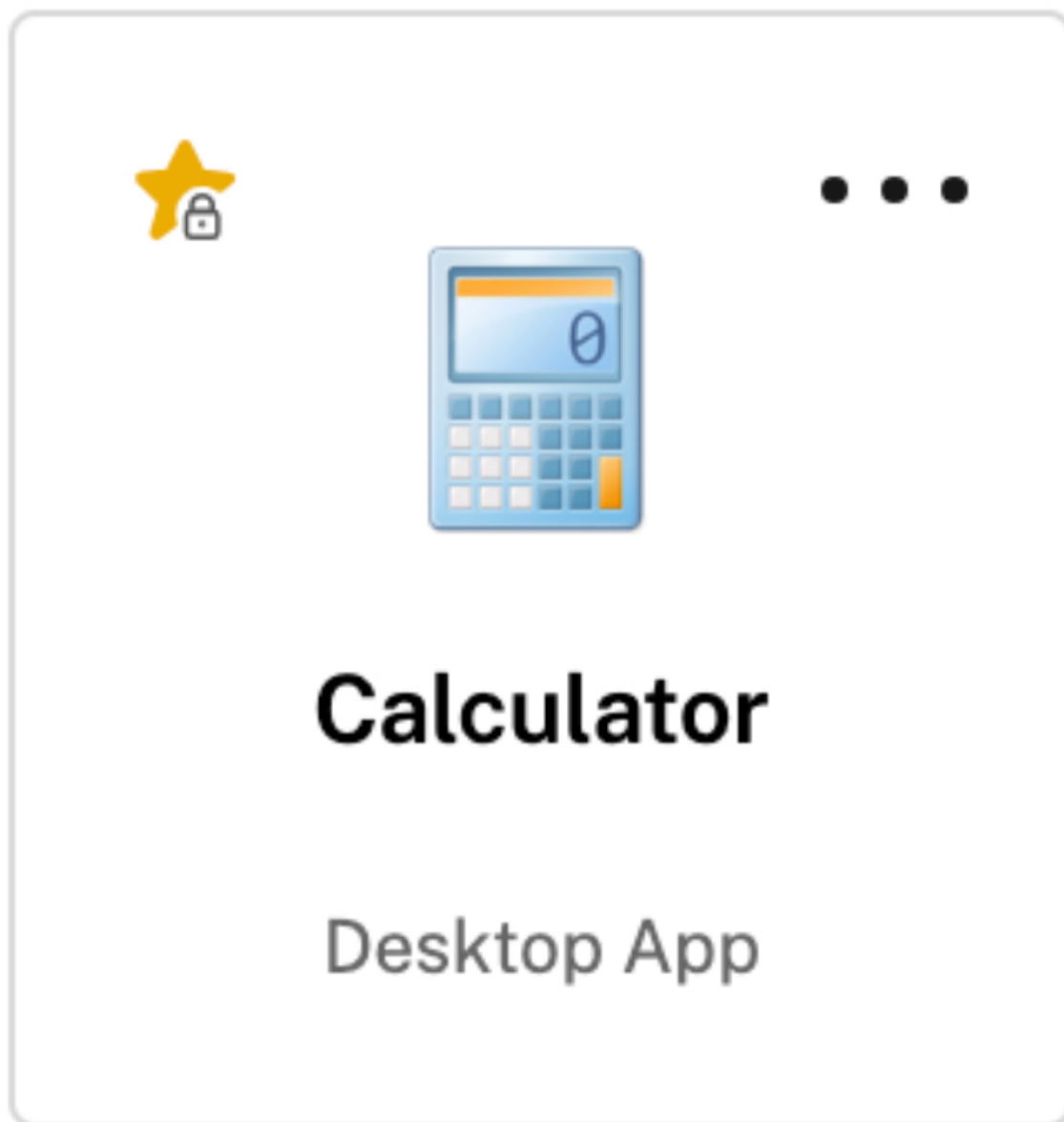
管理者は、Citrix DaaS ([管理] > [完全な構成] > [アプリケーション]) の [KEYWORDS:Auto] および [KEYWORDS:Mandatory] 設定を使用して、利用者のお気に入りのアプリを自動的に追加できます。



The screenshot shows the 'Application Settings' dialog box in Citrix Studio, with the 'Identification' tab selected. The left sidebar lists various settings: Identification, Delivery, Location, Groups, Limit Visibility, File Type Association, and Zone. The main area contains the following fields and text:

- Identification**
- Identify this application.
- Application name (for user): Calculator
- Application name (for administrator): Calculator
- Description and keywords: KEYWORDS: Auto
- This is the description that will be seen by the user. You can also use this field to enter keywords for StoreFront.
- [Learn More](#)
- Buttons: OK, Cancel, Apply

- **KEYWORDS:Auto**。アプリまたはデスクトップはお気に入りとして追加され、利用者はそのお気に入りを削除できます。
- **KEYWORDS:Mandatory**。アプリまたはデスクトップはお気に入りとして追加され、利用者はそのお気に入りを削除できません。Mandatory (必須) のアプリとデスクトップには、南京錠付きの星のアイコンが表示され、お気に入りから外すことができないことを示します。



注:

1つのアプリに **Mandatory** と **Auto** の両方のキーワードを使用する場合は、**Mandatory** キーワードが **Auto** キーワードを上書きします。お気に入りに登録されたアプリやデスクトップは削除できません。

Mandatory キーワードを持つアプリおよびデスクトップにのみアクセスできる利用者の場合:

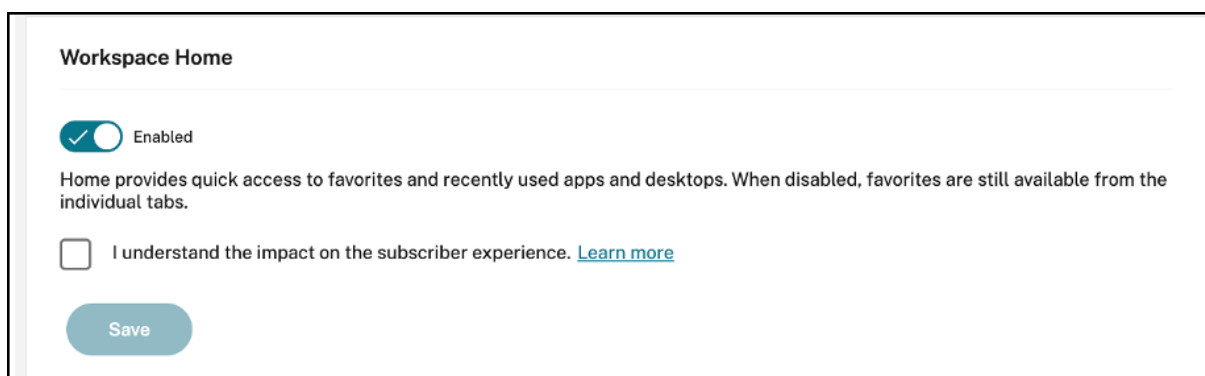
- 利用者には、Workspace の左側のナビゲーションペインに [アプリ] ページのみが表示されます。[アプリ] ページと [お気に入り] ページに表示されるアプリに違いはないため、[お気に入り] ページは左側のペインに表示されません。
- 利用者には、ホームページの [お気に入り] タブは表示されません。[最近] タブのみが表示されます。

ユーザーのホーム画面を有効または無効にする（プレビュー）

ユーザーの [ホーム] ページを有効または無効にして、アプリの構成を改善できます。

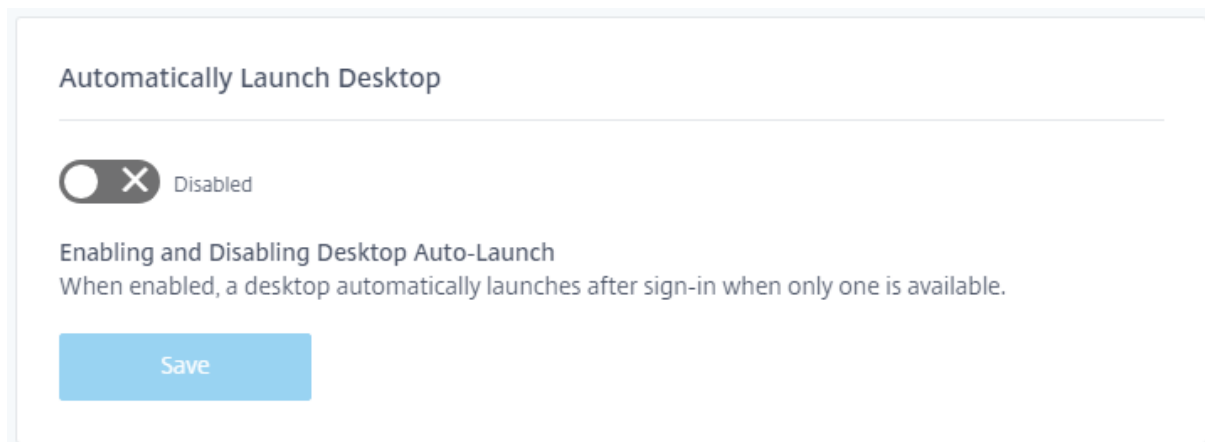
この機能はユーザーのデスクトップに 20 個を超えるアプリがある場合に適用されます。ユーザーのアプリが 20 個以下の場合は、ナビゲーションや検索オプションのない単一のビューが表示されます。

設定を構成するには、[ワークスペース構成] > [カスタマイズ] > [外観] に移動します。トグルがオンの場合、ユーザーは [ホーム] ページに移動します。トグルをオフにすると、ユーザーは直接 [アプリ] ページに移動します。デフォルトではトグルはオンになっており、この機能は有効になっています。



自動的にデスクトップを起動する

[自動的にデスクトップを起動する] は、[ワークスペース構成] および新しい Workspace 環境にアクセスできる顧客が利用できます。この設定は、Web ブラウザーからワークスペースにアクセスする場合にのみ適用されます。



無効にすると（デフォルト）、利用者がサインインしたときに Citrix Workspace により自動的にデスクトップが起動しません。サインイン後、利用者は手動でデスクトップを起動する必要があります。

有効にすると、利用者がデスクトップを 1 つしか使用できない場合は、ワークスペースにサインイン後、自動的にデスクトップが起動します。

利用者のアプリケーションは、Workspace コントロールの構成にかかわらず、再接続されません。

注:

Citrix Workspace によるデスクトップの自動起動を有効にするには、Internet Explorer でサイトにアクセスする利用者は [ローカルイントラネット] または [信頼済みサイト] のゾーンに Workspace URL を追加する必要があります。

フェデレーション ID プロバイダーセッション

Workspace がフェデレーション ID プロバイダーを使用するように構成されている場合、認証セッションとその有効期間は通常、ID プロバイダーによって制御されます。フェデレーション ID プロバイダーセッションの設定によって、コントロールをサービスプロバイダーに渡すことができます。有効にすると (デフォルト)、Workspace は、新しい Workspace セッションが必要になったときに、ID プロバイダーでのサインインプロンプトを強制します。無効にすると、有効なセッションで Workspace にアクセスする場合、利用者は ID プロバイダーでの認証を求められません。

この設定が有効で、ワークスペース認証に Azure AD を使用している場合、セッションに有効な Microsoft 認証トークンが存在する場合でも、利用者は再度サインインするように求められることがあります。このシナリオについて詳しくは、[CTX253779](#)を参照してください。


アプリとデスクトップを起動

[アプリとデスクトップを起動] 設定は、[ワークスペース構成] および新しい Workspace 環境にアクセスできる顧客が利用できます。この環境設定は、新規および既存の顧客が利用できます。ただし、この機能を導入しても、既存の顧客の設定は変更されません。

この設定は、**Citrix DaaS** のみが提供するアプリとデスクトップをユーザーが開く方法に適用されます。これは、**Citrix DaaS** サービス、または[サイトアグリゲーション](#)機能からのオンプレミスが該当します。[アプリとデスクトップを起動] 設定は、たとえば、Citrix Gateway サービスによって提供される SaaS アプリには適用されません。

Launching apps and desktops

Select how end users must launch apps and desktops when they access their workspace from a browser. (DaaS only)

Let end users choose 

Let end users choose between a locally installed version of the Workspace app or in a browser.

- If end users have the right to install software, prompt them to install the latest version of the Workspace app if a local app isn't detected automatically.

Do you want end users to download the Workspace Web Extension for a safer and more reliable app launch experience? Once the extension is downloaded, the Workspace detection step will no longer be displayed. [Learn more](#)

- Require end users to download the Workspace Web Extension and block access to Workspace until it is detected.
- Prompt end users to download the Workspace Web Extension but allow access to Workspace if it isn't detected.
- Do not prompt end users to download the Workspace Web Extension.

Save

次の設定のいずれかを選択します：

- ネイティブアプリの場合（デフォルト）：エンドユーザーは、ローカルにインストールされたバージョンの Workspace アプリを使用する必要があります。
- ブラウザーの場合：エンドユーザーは、HTML5 向け Workspace アプリのブラウザーバージョンを使用する必要があります。
- ユーザーが選択：エンドユーザーは、ローカルにインストールされたバージョンの Workspace アプリを選択するか、ブラウザーでアプリとデスクトップを起動するかを選択できます。

[ネイティブアプリ内] と [ユーザーが選択] の追加オプションを使用すると、ローカルアプリが自動的に検出されない場合に、Citrix Workspace アプリの最新バージョンをインストールするようユーザーに要求します。利用者がソフトウェアをインストールする権限を持っていない場合は、このオプションを削除します。

Microsoft Teams と Workspace の統合

Microsoft Teams との統合により、利用者は、Workspace アクティビティフィードのカードを、Microsoft Teams のチャンネルを介して、他の利用者と共有できます。

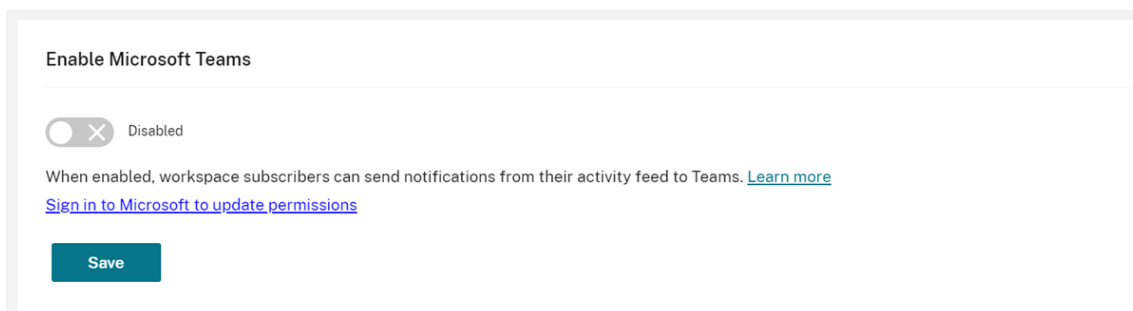
要件

- Microsoft Teams の統合を有効にするため、Citrix Cloud でフルアクセス権限を持つ管理者である必要があります。カスタムアクセス権限を持つ管理者には、Microsoft Teams 統合を有効にするために必要な権限がありません。
- [ID およびアクセス管理] で、Azure AD 認証を構成する必要があります。Azure AD 認証の構成について詳しくは、「[Azure Active Directory を Citrix Cloud に接続する](#)」を参照してください。

- Microsoft Teams で使用できる Azure AD インスタンスは 1 つのみです。構成する Azure AD インスタンスで、別の Citrix Cloud アカウントを使用して Microsoft Teams が有効になっている場合、Citrix Cloud アカウントの Microsoft Teams 統合を有効にすることはできません。
- 機能トグル **lwsMicrosoftTeams** を有効にする必要があります。
- ワークスペースに対し、[アクションとアクティビティフィード] 機能を有効にする必要があります。
- ワークスペース利用者が Microsoft Teams デスクトップクライアントをインストールしている必要があります。

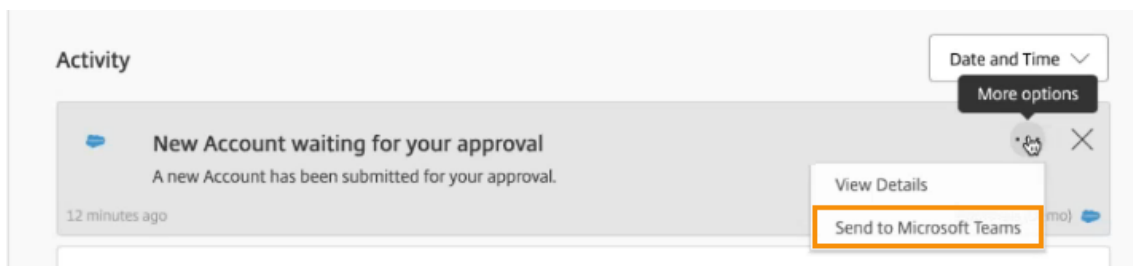
Microsoft Teams との統合を有効にする

1. Citrix Cloud にサインインした後、[ワークスペース構成] を選択します。
2. [カスタマイズ]、[基本設定] タブの順に選択します。
3. [**Microsoft Teams** を有効にする] で、トグルを選択して有効にします。



4. [**Save**] を選択します。

Workspace ユーザーは、[**Microsoft Teams** に送信] オプションを表示し、Workspace からカードを共有できるようになりました。ユーザーによる画面の更新が必要な場合もあります (Ctrl+F5 キー)。

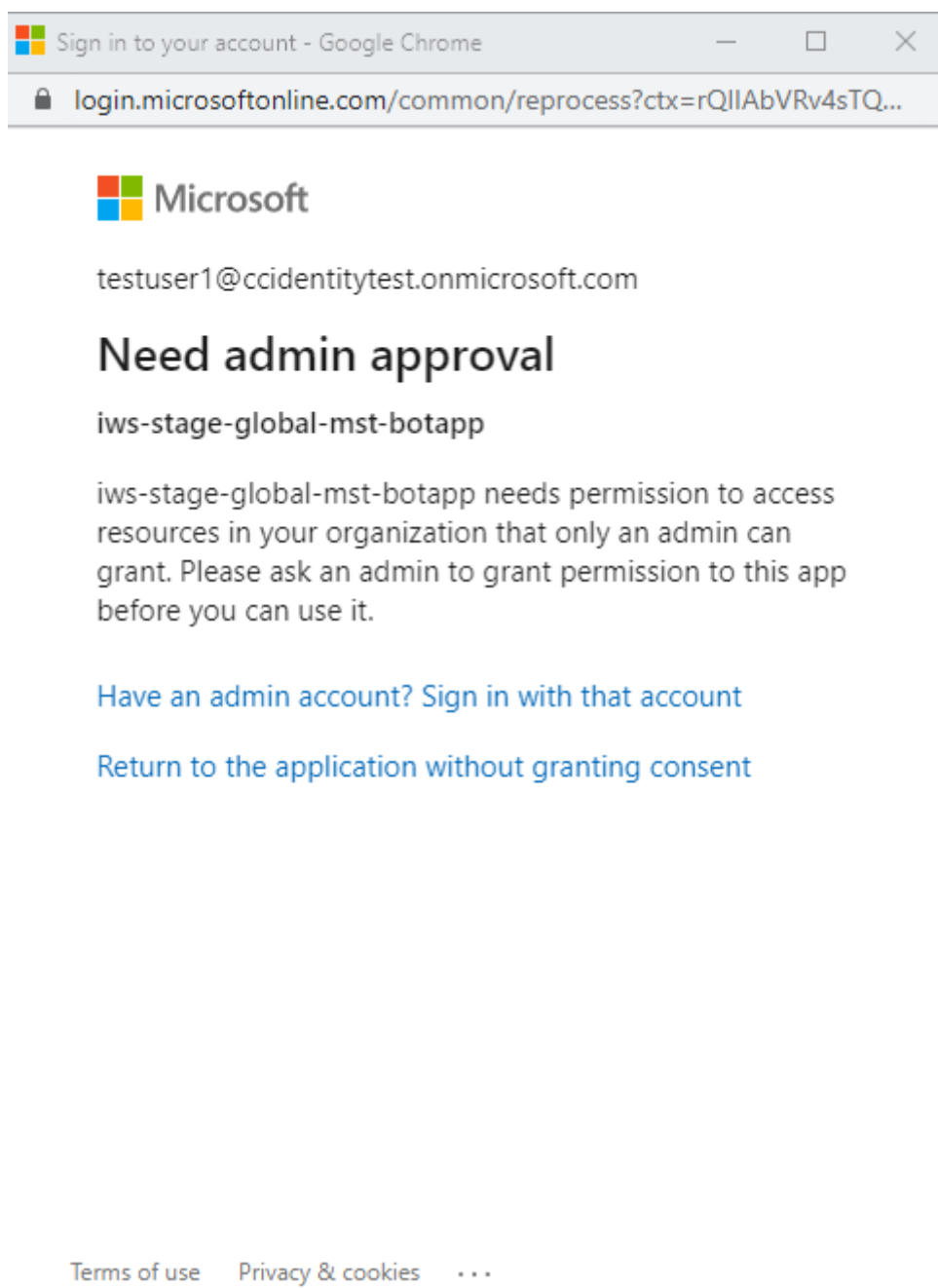


Workspace の権限を受け入れる

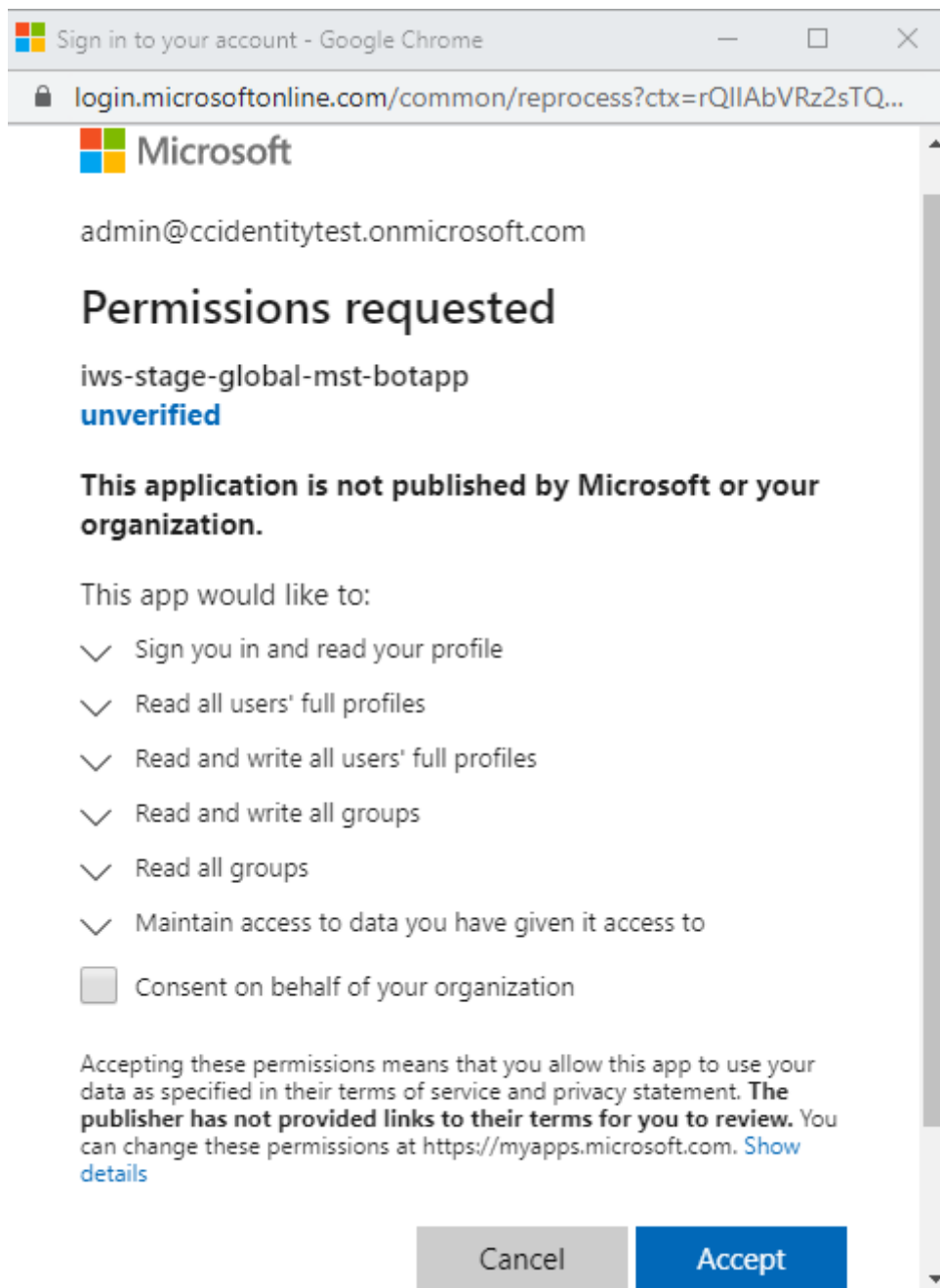
この統合を有効にするために必要なセットアップ手順はほかにもあります。組織のユーザーが Microsoft Teams とカードを共有できるように、**Microsoft** 管理者アカウントは Workspace UI で統合の権限を受け入れる必要があります。

1. ワークスペースアカウントにサインインして、カードの共有を試行してください。

2. **Microsoft** 管理者アカウントが Microsoft Teams との統合の権限を受け入れていない場合、非管理者アカウントでサインインしようとする、次のメッセージが表示されます:



3. 権限を受け入れるには、次を選択して管理者アカウントにサインインします: 管理者アカウントを持っている場合そのアカウントでサインインします。Microsoft Teams と Citrix Workspace の統合を有効にするには、データにアクセスするために次の権限が必要です:



4. [アクセス許可を承認済み] ダイアログボックスが開いたら、オプションを確認します。[所属組織の代わりに同意する] を選択して、この管理者のすべての Workspace 利用者に権限を付与します。それ以外の場合は、管理者アカウントにのみ権限が付与されます。
5. [同意] を選択します。

セキュリティとプライバシーポリシーをカスタマイズする

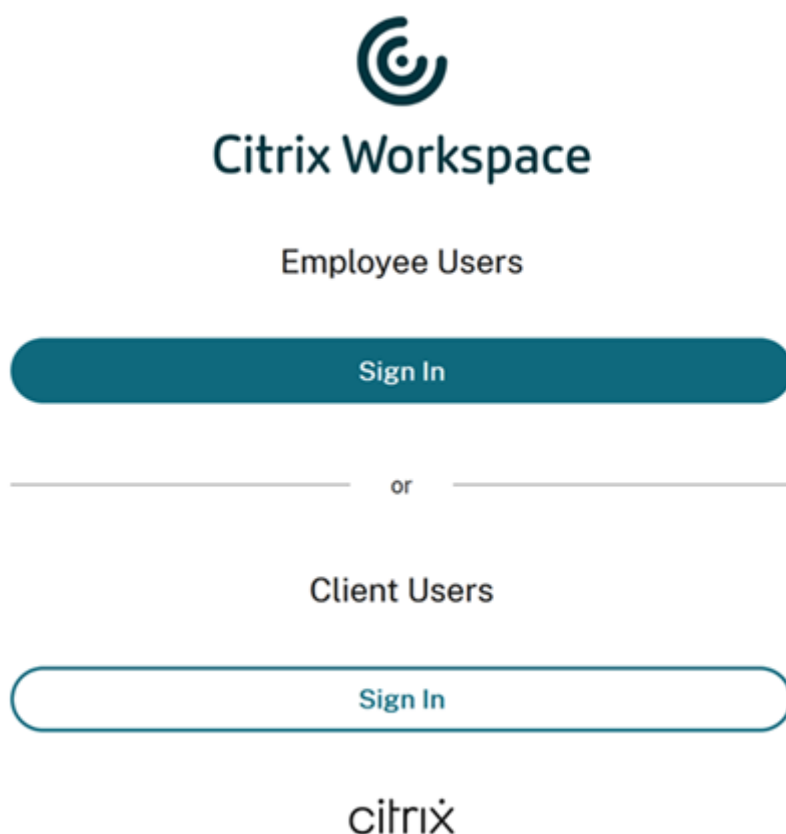
November 28, 2023

この記事では、ワークスペースへのアクセスと認証を構成した後で、サインインエクスペリエンスをカスタマイズする方法について説明します。

ワークスペースのアクセスと認証の構成に関連する手順の概要については、「[アクセスの構成](#)」を参照してください。ワークスペースへの利用者の認証の構成方法については、「[セキュアなワークスペース](#)」を参照してください。

統一されたユーザーサインインフローを作成する

デフォルトのサインインエクスペリエンスは、従業員ユーザーとクライアント（外部）ユーザーで画面が分割されています。



この分割画面を削除するには、[ワークスペース構成] > [認証] > [統合ユーザーサインインフロー] に移動して [有効化] を選択します。この機能を有効にすると、すべてのユーザーに同じサインインオプションが表示されます。



Citrix Workspace

Username

Password

Workspace アプリのデスクトップとモバイルで [Web の非アクティブタイムアウト] を設定する

[ワークスペース構成] > [カスタマイズ] > [基本設定] の [Web の非アクティブタイムアウト] 設定を使用して、利用者が Citrix Workspace から自動的にサインアウトされるまでのアイドル時間（最大 8 時間）を指定します。対応する設定のボックスを選択することで、デスクトップおよびモバイルで Workspace アプリの非アクティブタイムアウトを有効にすることもできます。

Workspace Sessions

Inactivity Timeout for Web

After this amount of idle time (maximum of 8 hours), your subscribers will be automatically signed out of Workspace. Applies to browser access only (not from a local Citrix Workspace app).

HOURS	MINUTES
<input type="text" value="0"/> ▾	<input type="text" value="20"/> ▾

DaaS のセッションを切断する手動サインアウトとは異なり、利用者は、操作が行われずにタイムアウトした後も、DaaS のセッションに接続したままになります。

Citrix Workspace アプリの再認証期間を設定する

[ワークスペース構成] > [カスタマイズ] > [基本設定] の [Workspace アプリの再認証期間] 設定を使用して、利用者が Citrix Workspace アプリにサインインしたままでいられる時間（再度サインインする必要が生じるまでの時間）を指定します。

Reauthentication Period for Workspace App ⓘ

This is the maximum time your subscribers can stay signed in to Workspace app before needing to reauthenticate (between 1 and 365 days).

Current Reauthentication Period: 1 Day(s) [Edit](#)

[Learn more](#) about Workspace reauthentication periods.

Save

デフォルトでは、利用者は 24 時間（1 日）ごとにサインインする必要があります。再認証期間は、より長く最大 365 日まで指定できます。再認証期間が長くなると、サインイン状態の維持に利用者の同意が必要になります。2021 年 9 月 27 日以降にプロビジョニングされたユーザーは、利用者が再度サインインするために 30 日間の期間が必要です。

設定した再認証期間の間、一度に 14 日以上非アクティブ状態でない限り、利用者はサインインしたままになります。利用者が 14 日以上非アクティブの場合、次にワークスペースにアクセスしようとしたとき、再認証を求められます。

こちらの [PowerShell スクリプト](#) をダウンロードし、ダウンロードファイルに含まれている指示に従うことで、利用者のセッションを無効にすることができます。セッションを無効にすると、利用者は 24 時間以内にワークスペースに再認証する必要があります。

Citrix Workspace アプリの再認証期間を 24 時間未満に設定する必要がある場合は、PowerShell で設定できます。詳しくは、「[Steps to configure InactivityTimeoutInMinutes](#)」を参照してください。

サポートされている **Workspace** アプリクライアント

次のバージョンの Citrix Workspace アプリは、この機能をサポートしています：

- Windows 向け Workspace アプリ 2106 以降
- Mac 向け Workspace アプリ 2106 以降
- iOS 向け Workspace アプリ 21.6.5 以降
- Android 向け Workspace アプリ 21.6.0 以降

サポートされている認証方法

Citrix Workspace アプリへのサインインの維持については、次の認証方法がサポートされています：

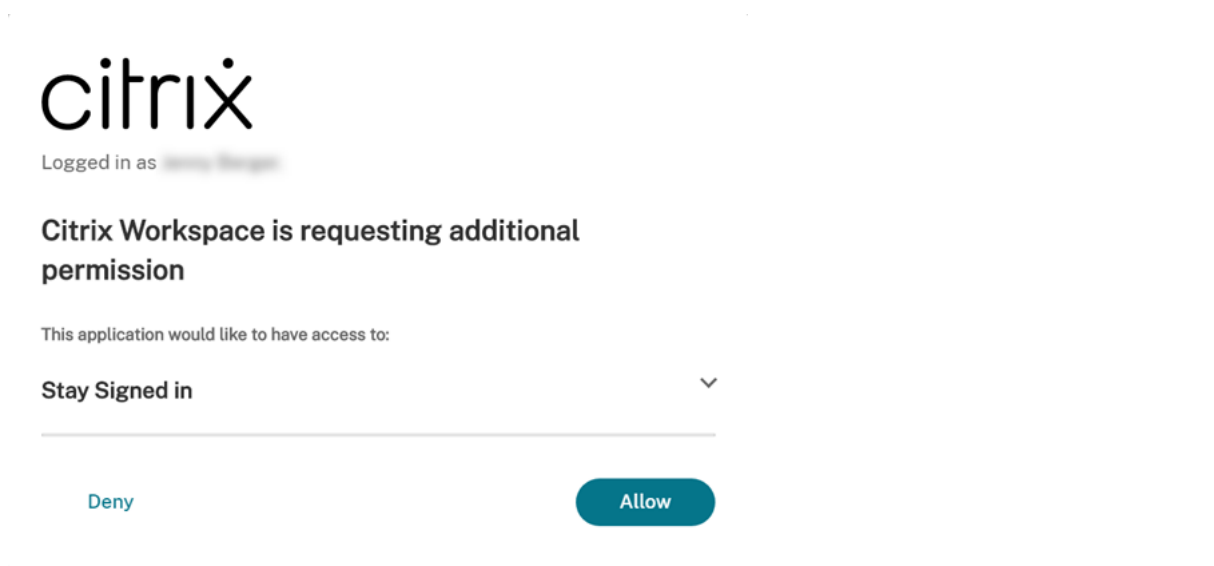
- Active Directory
- Active Directory+ トークン
- Azure Active Directory
- Citrix Gateway
- Okta

注：

Okta または Azure Active Directory を使用している Citrix DaaS の顧客と同じエクスペリエンスにするには、Citrix フェデレーション認証サービス (FAS) を構成します。FAS について詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

サインイン維持の利用者エクスペリエンス

利用者がデバイスで Workspace にサインインすると、サインインを維持することに同意するよう求めるプロンプトが表示されます。



利用者が [許可] を選択すると、再認証期間の間はサインインが維持されます。利用者のデバイスで 4 日間アクティビティが検出されない場合、利用者には再認証を求めるプロンプトが自動的に表示されます。Citrix Workspace アプリにサインインした後、デバイスでアプリとデスクトップを使用している限り、再認証期間は有効なままです。

利用者が [拒否] を選択すると、Workspace は利用者に再度サインインするよう求めます。その後、24 時間後に、Workspace は利用者に再度サインインするよう求めます。

利用者のパスワードが変更された場合、利用者は、再認証期間中に作業を継続するために、Citrix Workspace アプリでサインアウトし、再度サインインする必要があります。

利用者がアカウントのパスワードを変更できるようにする

注:

この機能は、段階的に顧客にロールアウトしています。ロールアウトプロセスが完了するまで、この機能が表示されない場合があります。

Citrix は、Citrix Workspace をご使用のお客様に、新機能と製品の更新情報をいち早くお届けするよう取り組んでいます。このプロセスは、わかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々にお客様の環境に適用されます。段階的に更新することによって、製品の品質を確保しながら、最大限の可用性を実現しています。

[ワークスペース構成] > [カスタマイズ] > [基本設定] の [アカウントパスワードの変更を許可] 設定は、利用者が Citrix Workspace 内からドメインパスワードを変更できるかどうかを制御します。また、組織のパスワードポリシーに従って有効なパスワードを作成できるように、利用者にガイダンスを提供することもできます。

有効にした場合（デフォルト）、利用者は組織の Active Directory 設定に基づいて、いつでもパスワードを変更できます。無効にすると、Workspace は有効期限が切れたときに利用者にパスワードを変更するよう求めますが、利用者が Workspace 内で有効期限が切れていないパスワードを変更することはできません。

サポートされている認証方法

- Active Directory
- Active Directory+ トークン

サポートされている **Workspace** アプリクライアント

次のバージョンの Citrix Workspace アプリは、この機能をサポートしています:

- Windows 向け Workspace アプリ 2101 以降
- Mac 向け Workspace アプリ 2012 以降
- Chrome 向け Workspace アプリ 2010 以降
- HTML5 向け Workspace アプリ 2101 以降
- Android 向け Workspace アプリ 21.1.0 以降

利用者は、Edge、Chrome、Firefox、または Safari ブラウザーの最新バージョンを使用してワークスペースにアクセスした場合も、この機能を使用できます。

この機能は、古いバージョンの Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリではサポートされません。

パスワードガイダンス

組織のセキュリティポリシーを満たすと同時に、ID プロバイダーが要求するパスワード要件を最大 20 個追加できます。利用者が Workspace の [アカウント設定] ページからパスワードを変更すると、Workspace はこれらの要件をガイドとして表示します。パスワード要件を追加しない場合、Workspace は「組織のパスワード要件は引き続き適用されます。」というメッセージを表示します。

重要:

Citrix Workspace は、利用者が入力した新しいパスワードを検証しません。利用者が Workspace 経由で有効なパスワードを無効なパスワードに変更しようとする、ID プロバイダーは新しいパスワードを拒否します。既存のパスワードは変更されません。

パスワード要件を追加するには:

1. [ワークスペース構成] > [カスタマイズ] > [基本設定] に移動します。
2. [アカウントパスワードの変更を許可] で、設定が有効になっていることを確認します。無効になっている場合は、有効にします。
3. [パスワード要件を追加する] を選択します。

Allow Account Password to be Changed

Enabled

When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

If no requirements are defined, subscribers see the message: **Your organization's password requirements still apply.**

[+ Add a password requirement \(20 max.\)](#)

Save

4. 有効なパスワードに関する組織のセキュリティ要件に一致する要件を入力します。たとえば、パスワードを特定の文字数にする必要があることを指定できます。利用者がパスワードを変更するときの利用者の要件項目を追加するには、[パスワード要件を追加する] を選択します。

Add a password requirement ✕

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

Password must meet the following requirements: ?

- 🗑️

[+ Add a password requirement \(20 max.\)](#)

⚠️ If no requirements are defined, subscribers see the message:
Your organization's password requirements still apply.

Save

Cancel

5. 要件の追加が終了したら、[保存] を選択します。
6. 設定の変更をすべて保存するには、再度 [保存] を選択します。

Allow Account Password to be Changed

Enabled

When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

^ Password must meet the following 4 requirements: ?

- At least 7 characters in length.
- Contain no personal information (Part of your name, social security number, birthday).
- Must contain 3 of the following: Lower Case Letter, Upper Case Letter, Number, Other Character (!@#%\).
- Must not be a password you have used before.

Save

Edit

パスワードを変更する場合の利用者エクスペリエンス

ヒント:

利用者に対するこの機能の認識を高めるために、利用者がワークスペースを介してドメインパスワードを変更するための推奨事項を内部ナレッジベースに含めることを検討してください。手順が記載された[こちらの PDF ファイルをダウンロード](#)して、ご自身が発信する記事やナレッジベースの記事に加えることができます。

[アカウントパスワードの変更を許可] が有効になると、利用者はワークスペースの [アカウント設定] > [セキュリティとサインイン] に移動してパスワードを変更できます。

[パスワードの要件を表示] を選択すると、[ワークスペース構成] で入力したすべての要件が表示されます。

Change Password

You'll have to sign back in to Workspace after changing your password.

Current Password:

New Password:

Confirm Password:

▼ Hide Password Requirements

Passwords must meet the following requirements:

- Be at least ten (10) characters in length
- Contain an upper case letter
- Contain a lower case letter
- Contain a number
- Contain a symbol (e.g., !, @, \$, %...)
- Be different than the 24 previously reset passwords
- Do not include a common dictionary word
- Do not include any part of the user or login name
- Avoid padding passwords with consecutive or repetitive numbers (e.g. 123, 1234, 1111, etc.)

パスワードを変更すると、利用者は自動的にワークスペースからサインアウトされ、新しいパスワードで再度サインインする必要があります。

カスタム通知の送信

カスタム通知を送信して、近日実施されるメンテナンス期間など、必要な期間限定のメッセージを表示します。

カスタム通知は、Web デバイスやモバイルデバイスを含むすべてのクライアントのすべての利用者に対して表示されます。利用者のサインイン後にメッセージが表示されます。利用者がこの通知を閉じることはできませんが、モバイルデバイスで折りたたむことはできます。

1. **Citrix Cloud** のメニューから、[ワークスペース構成] > [カスタマイズ] > [基本設定] > [Send custom announcement] > [構成] を選択します。
2. 表示するメッセージのタイトルとテキストを入力し、利用者にメッセージを表示する日時や場所（上部または下部）を選択します。
3. 利用者にメッセージがどのように表示されるかを確認するには、[プレビュー] を選択します。

4. 完了したら、[保存] を選択します。

サインインポリシーの構成

ワークスペースにサインインするときに、組織のライセンス契約書（EULA）を利用者に通知するカスタムサインインポリシーを作成します。

有効にして構成すると、Web デバイスやモバイルデバイスを含むすべてのクライアントでサインインポリシーが表示されます。利用者は、サインイン時にサインインポリシーを確認できます。利用者はこのポリシーを省略することはできず、ワークスペースにサインインするにはポリシーに同意する必要があります。

1. **Citrix Cloud** メニューから [ワークスペース構成] > [カスタマイズ] > [基本設定] を選択します。
2. [サインインポリシー] セクションで、[構成] を選択します。ポリシーが存在する場合、このボタンは [編集] と表示されます。
3. [ポリシーの有効化] 下のトグルを使用して、機能を有効にします。
4. [ポリシーヘッダー] にポリシーのタイトルを入力します。
5. サインインする前に利用者が同意する必要があるポリシーのテキストを入力します。必要に応じて、同じテキストボックスに他の言語に翻訳された文章を追加します。
6. ポリシーに同意するために利用者が選択する必要があるボタンの名前を入力します。

Sign In Policy ✕

Define the company usage policy that your subscribers must read and accept before signing in and accessing resources. [Learn more](#)

Enable policy
When enabled, the policy will be displayed to end users.

Policy header
Enter the header to display above the policy text.

Terms and Conditions


Policy text
Enter the text of the sign in policy you want to display to subscribers.

Normal ⇅ **B** *I* U

Enter policy text

Button text
Enter the text to display for the button that will allow subscribers to continue to sign in.

Accept Terms and Conditions



7. [プレビュー] を選択して、利用者のポリシーがどのように表示されるかを確認します。

8. 完了したら、[保存] を選択します。

注

Citrix Gateway を Workspace ID プロバイダーとして構成している場合は、AAA および nFactor 認証フローの一部としてサインインポリシーが既に設定されていることがあります。既存の nFactor 認証フローの一部として、またはフローの外部で、Citrix Cloud 管理コンソールを使用してサインインポリシーを 1 つだけ構成することをお勧めします。

Citrix Workspace での DaaS の最適化

October 12, 2023

次のオプションを使用することで、DaaS のアプリとデスクトップの効率と可用性を向上させることができます：

- [サイトアグリゲーション](#)を使用して、既存のオンプレミスの Virtual Apps and Desktops 展開を Workspace 利用者が利用できるようにする。
- [直接ワークロード接続](#)を使用して接続を最適化する。これには、Citrix Cloud でのネットワークの場所の構成が含まれます。
- オフラインの回復力のために、停止時の[サービス継続性](#)を確保する。
- [Citrix フェデレーション認証サービス \(FAS\)](#) を使用した DaaS へのシングルサインオン (SSO) を構成する。

サイトアグリゲーション

サイトアグリゲーションを使用すると、オンプレミスの Virtual Apps and Desktops 展開をワークスペースに追加して、クラウド管理のリソースとともに、利用者がこれらのリソースにアクセスできるようにすることができます。

詳しくは、「[オンプレミスの Virtual Apps and Desktops をワークスペースに集約](#)」を参照してください。

スケーラビリティの制限について詳しくは、「[Workspace platform scalability limits](#)」を参照してください。

直接ワークロード接続

直接ワークロード接続は、ネットワークの場所を使用して、Virtual Apps and Desktops をホストする仮想マシンへの内部ルートと外部ルートを切り替えます。

直接ワークロード接続を使用すると、社内ネットワーク内のクライアントが Citrix DaaS の直接起動に切り替えられるようになります。直接起動では、クライアントと VDA との間の HDX 接続をゲートウェイ経由でプロキシする必要はありません。直接ワークロード接続には、少なくとも 1 つの内部のネットワークの場所が必要です。

詳しくは、「[直接ワークロード接続で接続を最適化](#)」を参照してください。

サービス継続性

サービスの継続性により、Citrix Cloud が停止した場合でも、利用者は Citrix Workspace アプリを介して重要なアプリやデスクトップにアクセスできます。

サービス継続性は、Citrix Workspace アプリがインストールされているクライアントディスクに接続リースを保存します。クライアントが Workspace ストアにアクセスすると、接続リースが定期的に更新されます。クライアントは、停止前にアクセスできていた Citrix DaaS を起動できます。詳しくは、「[サービス継続性](#)」を参照してください。

Citrix フェデレーション認証サービス (FAS)

Citrix Workspace では、Citrix フェデレーション認証サービス (FAS) を使用した Citrix DaaS へのシングルサインオン (SSO) がサポートされています。FAS を使用すると、Azure AD や Okta などのフェデレーション ID プロバイダーを使用する利用者は、資格情報を 1 回入力するだけでワークスペースにサインインできます。FAS がないと、フェデレーション ID プロバイダーを使用している利用者は、Virtual Apps and Desktops にアクセスするために資格情報を複数回入力するように求められます。

Workspace で FAS を使用するには、次の要件があります：

- FAS 製品ドキュメントの「[要件](#)」セクションの説明に従って構成された FAS サーバー。
- FAS サーバーと Citrix Cloud との間の接続は、FAS インストーラーの「[Citrix Cloud への接続](#)」オプションを使用して作成されます。
- [ワークスペース構成] で FAS が有効になっているオンプレミス Active Directory ドメインと Citrix Cloud との間の接続。

FAS の実装について詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

オンプレミスの **Virtual Apps and Desktops** をワークスペースに集約

October 12, 2023

サイト (Virtual Apps and Desktops 展開) を Citrix Workspace に追加して、利用者が既存のアプリとデスクトップを使用できるようにすることができます。サイトの追加後、利用者が自分のワークスペースにサインインすると、すべての仮想アプリおよび仮想デスクトップと、ファイルやその他のリソースにアクセスできるようになります。このプロセスは、「[サイトアグリゲーション](#)」と呼ばれます。

サイトアグリゲーションは、Citrix Workspace のすべてのエディションで使用できます。Workspace の各エディションで使用できる機能については、「[Citrix Workspace の機能マトリックス](#)」を参照してください。

サポートされる環境

サイトアグリゲーションは、以下の Citrix 製品のオンプレミス展開でサポートされています：

- Virtual Apps and Desktops 7 1808 以降
- XenApp および XenDesktop 7.0~7.18

これより前のバージョンの XenApp、または XenApp および XenDesktop を実行しているオンプレミスサイトでは、Citrix Workspace は使用できません。

重要:

XenApp および XenDesktop 7.x には、End of Life (EoL) のバージョンが含まれています。XenApp および XenDesktop は、2018 年 6 月 30 日に 7.14 が EoL に達する前にリリースされました。XenApp および XenDesktop 7.x の EoL バージョンでのサイトアグリゲーションのサポートは、StoreFront 展開でのリソースの列挙と起動が成功するかどうかによります。

Citrix フェデレーション認証サービス (FAS: Federated Authentication Service) を含むオンプレミス展開でサイトアグリゲーションを使用するには、サイトで次の Citrix 製品バージョンのいずれかを使用する必要があります:

- Virtual Apps and Desktops 7 1808 以降
- XenApp および XenDesktop 7.16~7.18

Citrix Cloud に接続するには、Citrix Workspace で FAS を使用する必要があります。FAS サーバーを最新バージョンの FAS ソフトウェアに更新して、Citrix Cloud に接続できるようにします。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

Workspace プラットフォームのスケラビリティ制限

次のスケラビリティ制限が Workspace プラットフォームに適用されます:

制限の種類	SLI メトリック	SLO しきい値制限
使用制限	すべての集約済みオンプレミス Citrix 仮想アプリおよびデスクトップサイトの同時エンドユーザー	500
backend/frontend 統合に関する追加制限	オンプレミスの Citrix 仮想アプリおよびデスクトップサイトの数	4

注:

backend/frontend 統合サイトの数が 4 を超えると、サイトの応答時間が遅くなる可能性があります。オンプレミスサイトには、サービス継続性および LHC サポートはありません。

タスクの概要

オンプレミスサイトを Citrix Workspace に追加する場合は、[サイトの追加] ウィザードに従って次のタスクを実行します:

1. サイトの検出および使用するリソースの場所の選択。
2. Cloud Connector がインストールされている Active Directory ドメインの検出。

3. Citrix Cloud とサイト間で使用する接続の指定。

リソースの場所により、サイトにアクセスするすべてのユーザーのドメインと接続方法が決まります。このプロセス中に、Citrix Cloud は接続をテストして、サイトが Cloud Connectors からアクセス可能であることを確認します。次に、Citrix Cloud はリソースの場所の一覧を表示します。Cloud Connector をインストールしていないリソースの場所がある場合は、必要なソフトウェアをダウンロードしてインストールします。

外部接続の場合、独自の Citrix Gateway を使用するか、Citrix Gateway サービスを使用できます。サイトと同じネットワーク上のユーザーのみがアプリケーションにアクセスできるようにするには、内部専用アクセスを指定します。

前提条件

Cloud Connector

Citrix Cloud は Cloud Connector によりサイトを検出して通信できるようになります。中断を最小限に抑えるために、Citrix Workspace にサイトを追加する前に Cloud Connector をインストールすることをお勧めします。

高可用性を実現するために、Citrix Cloud Connector ソフトウェアのインストール先となるサーバーを少なくとも 2 台用意することをお勧めします。これらのサーバーには、以下が必要です：

- 「[Citrix Cloud Connector の技術詳細](#)」に記載されているシステム要件を満たしている。
- 他の Citrix コンポーネントがインストールされていない。
- Active Directory ドメインコントローラーではない。
- リソースの場所のインフラストラクチャにとって重要なマシンではない。
- サイトドメインに参加している。ユーザーが複数のドメインにあるサイトのアプリケーションにアクセスする場合は、各ドメインに Cloud Connector を少なくとも 2 つインストールします。
- サイトに接続可能なネットワークに接続している。
- インターネットに接続している。詳しくは、「[システムおよび接続要件](#)」を参照してください。

Cloud Connector のインストール手順について詳しくは、「[Cloud Connector のインストール](#)」を参照してください。

Web プロキシの構成

環境内に Web プロキシがある場合は、Cloud Connector がサイト内の XML Service への接続を検証できることを確認します。サイト内の各 XML サーバーを、各 Cloud Connector のバイパスプロキシ一覧に追加します。Cloud Connector は FQDN の処理のみをサポートしているため、ワイルドカード文字や IP アドレスは使用しないでください。

1. 使用しないプロキシの一覧に XML サーバーを追加します：

- a) Cloud Connector で、[スタート] を選択し、「インターネットオプション」と入力します。

- b) [接続] タブ、[LAN の設定] の順に選択します。
 - c) [プロキシサーバー] で、[詳細設定] を選択します。
 - d) [例外] で、サイト内の各 XML サーバーの FQDN を小文字で追加します。これらのエントリで大文字を使用したり、大文字と小文字が混在したりすると、サイトアグリゲーションが失敗する可能性があります。詳しくは、Citrix Support Knowledge Center の[CTX272160](#)を参照してください。
2. Cloud Connector サービスで例外が使用されるように、一覧をインポートします。コマンドプロンプトで「`netsh winhttp import proxy source=ie`」と入力します。
 3. サービスコンソールから、Cloud Connector をホストする各マシンのすべての Citrix Cloud サービスを再起動するか、各マシンを再起動します。

Active Directory

サイトアグリゲーションは、オンプレミス Active Directory を使用するサイトに対応しています。

Azure Active Directory の構成 Azure Active Directory を使用するサイトを Citrix Workspace に追加するには、XML Service からの要求を信頼するようにサイトを構成します。手順については、以下の記事を参照してください：

XenApp および XenDesktop 7.x と Virtual Apps and Desktops 7 1808 については、[CTX236929](#)を参照してください。

重要：

Azure Active Directory、Okta、SAML、またはワークスペースとサイトアグリゲーション機能を備えたその他のフェデレーション ID プロバイダーを使用する場合、ユーザーは起動する各アプリケーションに対して認証するように求められます。

FAS は、フェデレーション認証を使用して、リソースを起動するためのシングルサインオン (SSO) エクスペリエンスを提供します。利用者に対して SSO を有効にするには、サイトを追加するために構成したのと同じリソースの場所に、1 つまたは複数の FAS サーバーを登録します。

Active Directory の信頼関係 Active Directory でユーザーフォレストとリソースフォレストを分けている場合は、オンプレミスサイトを追加する前に、各フォレストに Cloud Connector をインストールする必要があります。Citrix Cloud により、サイトの検出プロセスで Cloud Connector を利用してこれらのフォレストが検出されます。検出されたフォレストのユーザーとリソースを使用して、ユーザー用のワークスペースを作成できます。

制限事項：

サイトを追加する場合、リソースの場所を定義するときに、ユーザーフォレストとリソースフォレストを別々に使用することはできません。フォレスト間の信頼が確立済みの場合でも、Cloud Connector はこれらの信頼に参加しないため、Citrix Cloud はこれらのフォレストの Cloud Connector を介してサイトを検出することはできません。こ

これらのフォレストは、ユーザーに異なる接続オプションを提供するセカンダリリソースの場所を定義する時に使用できます。詳しくは、「接続オプションごとの IP 範囲を追加する」を参照してください。

信頼されていないフォレストは、サイトアグリゲーションではサポートされていません。Citrix Cloud および Citrix Workspace は信頼されていないフォレストのユーザーをサポートしていますが、サイトアグリゲーションによってオンプレミスサイトが追加された後は、これらのユーザーは Citrix Workspace を使用できません。サイトが信頼するフォレスト内のユーザーのみがサインインして Citrix Workspace を使用できます。信頼されていないフォレストのユーザーが Citrix Workspace にサインインしようとする、次のエラーメッセージが表示されます: 「ログオンの有効期限が切れました。続行するには、もう一度ログオンしてください」

ワークスペースのリソースへの内部接続と外部接続

Citrix Workspace へのサイトの追加プロセスでは、ユーザーが使用できるリソースへ内部および外部からアクセス可能にするかどうかを指定できます。内部ユーザーのみが Citrix Workspace 経由でサイトにアクセスできるようにする場合、アプリケーションにアクセスするにはユーザーはサイトと同じネットワーク上にいる必要があります。

外部ユーザーがこれらのリソースにアクセスできるようにする場合は、次のオプションがあります:

- オンプレミスサイトと Citrix Cloud との間のトラフィックの処理に、既存の Citrix Gateway を使用する。Citrix Workspace にサイトを追加する前に、Cloud Connector を Secure Ticket Authority (STA) サーバーとして使用するように Citrix Gateway を構成する必要があります。手順については、[CTX232640](#)を参照してください。
- Citrix がサイトと Citrix Cloud との間のトラフィックを処理できるように、Citrix Gateway サービスを使用する。サイトの追加時に、サービストライアルを有効にしてこのサービスを構成できます。このオプションを選んだ場合、Citrix Gateway サービスに登録済みであれば、Citrix Cloud によりそのサブスクリプションが検出されます。

注:

Citrix Cloud で Citrix Gateway サービスのサブスクリプションが検出されるようにするには、Citrix Gateway サービスへの登録に使用したものと同一組織 ID (OrgID) を使用する必要があります。Citrix Cloud の OrgID について詳しくは、「[OrgID とは何ですか?]」を参照してください。(/en-us/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html#what-is-an-orgid)

サイト検出のための資格情報およびポート

Citrix Workspace へのサイトの追加プロセスでは、Citrix Cloud がサイトを検出し、指定した Delivery Controller が利用可能であることを確認します。オンプレミスサイトを追加する前に、以下を確認してください:

- 最低限の読み取り専用権限を持つ Citrix 管理者の資格情報があること。サイト検出プロセス中に、Citrix Cloud はこれらの資格情報を提供するように要求します。Citrix Cloud がこれらの資格情報を保存したり、これらの資格情報を使用してサイトを変更したりすることはありません。

サイトの資格情報なしでサイト検出を有効にするには **XenApp** および **XenDesktop 7.x** と **Virtual Apps and Desktops 7 1808** のみ: セキュリティ上の理由でサイトの資格情報を提供できない場合は、Citrix Cloud がサイトの資格情報を求めずにサイトを検出するようにすることができます。Citrix Workspace にサイトを追加する前に、次のタスクを行います。

1. サイトのドメインに Cloud Connector を少なくとも 2 つインストールします。
2. Active Directory セキュリティグループを作成して、このグループにドメイン内の Cloud Connector を追加します。
3. Cloud Connector を再起動します。
4. Citrix Studio で、このセキュリティグループに少なくとも読み取り専用権限を付与します。

タスク 1: サイトの検出

この手順では、Citrix Cloud がサイトを検出しリソースの場所を選択するために必要な情報を指定します。リソースの場所により、サイトにアクセスするすべてのユーザーのドメインと接続オプションが決まります。必要な場合、この手順でサイトのドメインに Cloud Connector をインストールすることができます。既に Cloud Connector がインストールされている場合は、メッセージが表示されたら Cloud Connector を選択できます。

1. Citrix Cloud メニューで [ワークスペース構成] > [サイト] > [サイトの追加] に移動します。
2. 追加して続行するオンプレミスサイトの種類を選択します。

Citrix Cloud は、ドメイン内のリソースの場所と Cloud Connector を検出しようとし、選択可能な一覧を表示します。

3. 次のいずれかの操作を実行します:
 - サイトのドメインに Cloud Connector をインストールしていない場合は、[コネクタのインストール] を選択します。Cloud Connector ソフトウェアをダウンロードしてインストールウィザードを完了するように求めるメッセージが表示されます。
 - Cloud Connector をインストール済みの場合は、検出されたドメインにある Cloud Connector が表示されます。Citrix Workspace に追加するリソースの場所を選択します。このリソースの場所が、デフォルトのリソースの場所になります。
 - Cloud Connector がインストール済みなのに表示されない場合は、[検出] を選択します。
4. サイトの検出に使用するリソースの場所と Cloud Connector のペアを選択します。
5. [サーバーアドレスの入力] に、サイト内の Delivery Controller の IP アドレスまたは完全修飾ドメイン名 (FQDN) を追加して、[検出] を選択します。

注:

FQDN を使用する場合は、検出する Delivery Controller を指し示す DNS レコードが必要です。

XenApp および XenDesktop 7.x サイトの場合は、Citrix Cloud が自動的に XML サーバーのポートを検出します。

6. プロンプトが表示されたら、サイトの Citrix 管理者の資格情報を入力します。

Citrix Cloud が接続テストを行って、サイトにアクセス可能であることを確認します。サイトの種類とサイズによっては、検出には数分かかることがあります。

7. サイトが正常に検出されたことを示す成功メッセージが表示された場合は、[続行] を選択します。

タスク 2: **Active Directory** の接続の確認

Citrix Cloud の [Active Directory の接続を確認] に、サイトで使用しているドメインと、これらのドメインに Cloud Connector がインストールされているかどうかが表示されます。

ドメイン内に Cloud Connector が存在しない場合、そのドメインのユーザーは、ワークスペースで公開されているアプリケーションに Citrix Workspace を使用してアクセスすることはできません。ドメインに Cloud Connector が 1 つしかない場合は、次の 2 つのオプションがあります：

- [コネクタのインストール] を選択して、さらに Cloud Connector をインストールします。
- [高可用性のためには、各ドメインに 2 つのコネクタをインストールする必要があることを理解しています] を選択し、Cloud Connector の追加インストールをせずに続行します。

サイトのアプリケーションにローカルユーザーを割り当てている場合は、[ユーザー一覧 (.csv) をダウンロード] を選択します。

Active Directory 接続を確認したら、[続行] を選択します。

タスク 3: 接続の構成

この手順では、Citrix Workspace を介したサイトへのアクセスを外部ユーザーに許可するか、内部ユーザーのみに許可するかを指定します。内部接続では、ユーザーはサイトおよび公開したリソースをホストする VDA と同じネットワーク上にいる必要があります。外部接続の場合、既存のオンプレミス Citrix Gateway を使用するか、クラウドホストの Citrix Gateway サービスを使用できます。

[接続の種類を選択] > [接続の構成] にある以下のオプションのいずれかを選択します：

- 既存の **Gateway** を追加：既存の Citrix Gateway を使用して外部からのアクセスを可能にする場合は、このオプションを選択します。
- **Citrix Gateway** サービス：サービストライアルを有効にするか、サイトで既存のサブスクリプションを使用する場合は、このオプションを選択します。
- 内部のみ：他の構成が必要ない場合は、このオプションを選択します。

[既存の **Gateway** を追加] を選択した場合は、次の操作を実行します：

1. [編集] を選択して、Citrix Gateway のパブリック URL を入力します。
2. Cloud Connector を STA サーバーとして使用するよう、[CTX232640](#)の説明に従って Citrix Gateway を構成していることを確認します。
3. [STA のテスト] を選択し、テストに成功したら [続行] します。テストが失敗した場合は、[CTX232517](#)のトラブルシューティングを参照してください。

[Citrix Gateway サービス] を選択した場合、Citrix Cloud アカウントでこのサービスがサービストライアルまたは購入品として有効になっていないときには、[60 日トライアルの開始] を選択できます。Citrix Cloud によりこのサービスがトライアルとして有効化されます。このサービスが以前に有効化されていた場合、Citrix Cloud はそのサービスを検出し、残りのトライアル日数を表示します。

上記のタスクを完了したら、[続行] を選択します。

タスク 4: サイトアグリゲーションの確認

この手順ではサイトアグリゲーションを確認し、これまでに選択した XML ポート、XML サーバー、Active Directory ドメイン、接続の種類を確認します。

Citrix Cloud は、接続できる最大 5 つの XML サーバーを表示します。サイトに複数の XML サーバーがあり、1 つしか表示されていない場合、Citrix Cloud はアラートを表示します。この問題を解決するには、[CTX232516](#)を参照してください。

1. [サイトアグリゲーションの確認] で、これまでに選択した XML ポート、XML サーバー、Active Directory ドメイン、接続の種類を確認します。
2. [保存して終了] を選択します。[サイト] ページに、新しく追加したサイトが表示されます。

別の XML サーバーを指定する場合は、[保存して終了] を選択した後にサイトを編集してこれらの値を変更できません。

タスク 5: サービス統合の管理

最初のサイトを追加した後、Virtual Apps and Desktops オンプレミスサイトの [サービス統合] を有効にする必要があります。これはデフォルトで無効になっています。利用者は、有効にするまでサイトのリソースを表示できません。

1. [ワークスペース構成] > [サービス統合] > [Virtual Apps and Desktops オンプレミスサイト] に移動し、省略記号 (…) を選択して、サイトの操作メニューを開きます。
2. サービス統合を有効にして、利用者がワークスペースにサインインしてサイトのリソースを表示できるようにします。

サイト構成の変更

サイトを再検出する

サイトに Delivery Controller を追加するか XML ポートを変更した場合は、Citrix Workspace でサイトが到達可能なままであることを再検出プロセスで確認できます。

1. [ワークスペース構成] > [サイト] に移動し、更新するサイトの省略記号 (...) を選択してから、[サイトの編集] を選択します。
2. [サーバーアドレス] にサイトの Delivery Controller の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力して、[再検出] を選択します。

XML サーバーを追加または変更する

Citrix Workspace にサイトを追加すると、サイト内の XML サーバーが Citrix Cloud により自動で検出され、構成に XML サーバーが 5 つまで表示されます。必要に応じて、XML サーバーを表示上限の 5 つまで構成に追加したり、構成から削除したりできます。

XML サーバーを追加するには

1. [ワークスペース構成] > [サイト] に移動し、更新するサイトの省略記号 (...) を選択して、[サイトの編集] を選択します。
2. [XML サーバー] セクションで、XML サーバーのポートを入力し、必要に応じて [SSL を使用] を選択します。
3. 接続方法を選択します：
 - 負荷分散：このオプションでは、Citrix Cloud は XML サーバーを一覧からランダムに選択します。
 - フェールオーバー：このオプションでは、Citrix Cloud は一覧の XML サーバーを一覧に表示されている順序で使用します。使用できない場合を除いて、一覧の最初の XML サービスのみが起動に使用され、その後、一覧の 2 番目のサーバーが使用されます。各サーバーをドラッグアンドドロップして、一覧を並び替えることができます。
4. [Save Changes] を選択します。

XML サーバーを追加時にエラーが発生した場合は、[CTX232516](#)でトラブルシューティングの手順を参照してください。

接続オプションごとの IP 範囲を追加する

複数のサブネットに VDA またはセッションホストを配置している場合、サブネットごとに接続の種類を変えて IP 範囲を指定できます。各 IP 範囲には、異なるリソースの場所を関連付けることもできます。たとえば、EU にあるマシン用に内部接続が可能な IP 範囲、EU にあるマシン用に Citrix Gateway 経由で接続可能な IP 範囲、および米国にあるマシン用に Citrix Gateway サービス経由で接続可能な IP 範囲をそれぞれ設定できます。

1. [ワークスペース構成] > [サイト] に移動し、更新するサイトの省略記号 (…) ボタンを選択して、[サイトの編集] を選択します。
2. [接続] セクションで、[異なる接続オプションの IP 範囲を追加] を選択し、CIDR (クラスレスドメイン間ルーティング) 形式の IP 範囲を入力します。

IP 範囲のリソースの場所を作成するには:

1. [新しいリソースの場所を追加する] を選択してわかりやすい名前を入力します。
2. [接続を選択する] で、内部アクセスのみを提供するか、Citrix Gateway または Citrix Gateway サービスを使用した外部アクセスを許可するかを選択します。

既存のリソースの場所を IP 範囲に割り当てるには:

1. [既存のリソースの場所を選択する] を選択します。
2. 使用するリソースの場所を選択します。
3. Cloud Connector が 1 つしかインストールされていないリソースの場所を選択した場合は、[高可用性のためには、リソースの場所に **2** つのコネクタをインストールする必要があることを了承します。] を選択します。
4. [Add] を選択します。

Active Directory ドメインを追加する

サイトの Active Directory ユーザーが存在する別のドメインに Cloud Connector をインストールした場合、Citrix Workspace のサイト構成にこれらのドメインが追加されたことを確認できます。

1. [ワークスペース構成] > [サイト] に移動し、更新するサイトの省略記号 (…) を選択してから、[サイトの編集] を選択します。
2. [Active Directory] の下にある [更新] を選択します。

サイトの無効化

オンプレミスサイトを Citrix Workspace のユーザーが使用できないようにする場合、サイトを無効にできます。個別のオンプレミスサイトを無効にすることも、Citrix Workspace に追加したオンプレミスサイトをすべて無効にすることもできます。

サイトが無効になっている場合、ユーザーは Citrix Workspace を介してそれらのサイトのオンプレミスアプリケーションにアクセスできません。ただし、これらのサイトの構成は保持されます。後でサイトを再度有効にすると、デフォルトのリソースの場所、ドメイン、XML サーバー、接続設定が保持されます。

1 つのオンプレミスサイトを無効にするには

1. [ワークスペース構成] > [サイト] に移動し、無効にするサイトの省略記号 (…) を選択してから、[無効] を選択します。
2. 確認のメッセージが表示されます。もう一度 [無効] を選択します。

オンプレミスサイトをすべて無効にするには

[サイト] ページのすべてのサイトを無効にするには、Virtual Apps and Desktops のすべてのオンプレミスサイトでワークスペースサービス統合を無効にします。手順については、「[サービスのワークスペース統合を無効にするには](#)」を参照してください。

個別のオンプレミスサイトを再度有効にするには、または後から別のサイトを追加するには、最初に [サービス統合] ページですべてのサイトのワークスペースサービス統合を再度有効にする必要があります。

Citrix Workspace からのサイトの削除

Citrix Workspace でオンプレミスサイト構成が不要になった場合、そのサイトを削除できます。サイトを削除しても、削除されるのは Citrix Workspace のサイトの構成のみです。Citrix Cloud はサイトを変更しません。

サイトを削除するには、[ワークスペース構成] > [サイト] に移動し、削除するサイトの省略記号 (...) を選択してから、[削除] を選択します。

直接ワークロード接続でワークスペースへの接続を最適化

November 28, 2023

Citrix Cloud の直接ワークロード接続を使用すると、ワークスペースのアプリとデスクトップへの内部トラフィックを最適化して、HDX セッションを高速化できます。通常、内部ネットワークと外部ネットワークの両方のユーザーが、外部ゲートウェイを経由して VDA に接続します。このゲートウェイは、組織内のオンプレミスであるか、Citrix からサービスとして提供され、Citrix Cloud 内のリソースの場所に追加されている場合があります。直接ワークロード接続により、内部ユーザーはゲートウェイを経由せずに VDA に直接接続できるため、内部ネットワークトラフィックの遅延が短縮されます。

直接ワークロード接続を設定するには、環境内でクライアントがアプリとデスクトップを起動する場所に対応したネットワークの場所が必要です。ネットワークの場所サービス (Network Location Service: NLS) を使用して、これらのクライアントが存在するオフィスの場所ごとにパブリックアドレスを追加します。ネットワークの場所を構成するには、次の 2 つのオプションがあります：

- Citrix Cloud の [ネットワークの場所] メニューオプションを使用する。
- Citrix が提供している PowerShell モジュールを使用する。

ネットワークの場所は、会社のオフィスやブランチの場所など、内部ユーザーの接続元であるネットワークのパブリック IP アドレス範囲に対応しています。Citrix Cloud は、パブリック IP アドレスを使用して、仮想アプリまたは仮想デスクトップを起動するネットワークが企業ネットワークの内部か外部かを判断します。利用者が内部ネットワークから接続している場合、Citrix Cloud では接続が NetScaler Gateway を経由せず VDA に直接ルーティングされます。利用者が外部から接続している場合、Citrix Cloud では利用者が NetScaler Gateway を経由してルー

ティングされ、セッショントラフィックが Citrix Cloud Connector 経由で内部ネットワークの VDA に送信されます。Citrix Gateway サービスが使用され、[\[Rendezvous プロトコル\]](#) が有効になっている場合、Citrix Cloud は Gateway サービスを使用して、外部ユーザーを内部ネットワークの VDA にルーティングします。ノート PC などのローミングクライアントは、起動時にクライアントが企業ネットワークの内部にあるか外部にあるかに応じて、これらのネットワークルートのいずれかを使用する可能性があります。

重要:

環境に Citrix DaaS Standard for Azure がオンプレミス VDA とともに含まれている場合、直接ワークロード接続を構成すると、内部ネットワークからの起動が失敗します。

Remote Browser Isolation、Citrix Virtual Apps Essentials、および Citrix Virtual Desktops Essentials リソースの起動は、常にゲートウェイを経由してルーティングされます。これらの起動では、直接ワークロード接続を構成してもパフォーマンスは向上しません。

要件

ネットワークの要件

- 社内ネットワークとゲスト Wi-Fi ネットワークには、個別のパブリック IP アドレスが必要です。企業ネットワークとゲストネットワークがパブリック IP アドレスを共有している場合、ゲストネットワーク上のユーザーは DaaS セッションを起動できません。
- 内部ユーザーの接続元であるネットワークのパブリック IP アドレス範囲を使用します。これらのネットワーク上の内部ユーザーは VDA に直接接続する必要があります。直接接続しない場合、Workspace は内部ユーザーを VDA に直接ルーティングしようとするため、仮想リソースを起動できません。
- 通常、VDA はオンプレミスネットワーク内にありますが、Microsoft Azure などのパブリッククラウド内でホストされている VDA を使用することもできます。クライアントの起動には、ファイアウォールによってブロックされずに VDA に接続するためのネットワークルートが必要です。これには、オンプレミスネットワークから、VDA がある仮想ネットワークへの VPN トンネルが必要です。

TLS の要件

ネットワークの場所を構成するときは、PowerShell で TLS 1.2 を有効にする必要があります。PowerShell で TLS 1.2 の使用を強制するには、PowerShell モジュールの使用前に次のコマンドを使用します：

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

ワークスペースの要件

- Citrix Cloud でワークスペースが構成されています。
- Citrix DaaS が [\[ワークスペース構成\]](#) > [\[サービス統合\]](#) で有効になっています。

HTML5 向け Workspace アプリの接続で TLS を有効にする

利用者が HTML5 向け Citrix Workspace アプリを使用してアプリやデスクトップを起動する場合、内部ネットワークで VDA の TLS を構成することをお勧めします。TLS 接続を使用するように VDA を構成すると、VDA を直接起動できるようになります。VDA で TLS が有効になっていない場合、利用者が HTML5 向け Citrix Workspace アプリを使用するときに、アプリとデスクトップの起動はゲートウェイを介してルーティングされる必要があります。Desktop Viewer を使用した起動は影響を受けません。TLS を使用した直接 VDA 接続について詳しくは、Citrix サポート Knowledge Center の [CTX134123](#) を参照してください。

GUI を使用してネットワークの場所を追加する

Citrix Cloud を介した直接ワークロード接続の構成には、内部ユーザーの接続元である各ブランチの場所のパブリック IP アドレス範囲を使用してネットワークの場所を作成することも含まれます。

1. Citrix Cloud コンソールで、[ネットワークの場所] に移動します。
2. [ネットワークの場所を追加] をクリックします。
3. ネットワークの場所名と、その場所のパブリック IP アドレス範囲を入力します。

Add a Network Location ✕

Adaptive access based on network locations allow you to specify networks in your organization. Administrators can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.

Location name

Argentina ✕

Public IP address range

✕

Save

4. [保存] をクリックします。
5. 追加する新しいネットワークの場所ごとに、上記の手順を繰り返します。

注:

接続の種類は常に [内部] であるため、直接ワークロード接続には場所のタグは必要ありません。[ネットワー

クの場所を追加] ページの [場所のタグ] フィールド ([Citrix Cloud] > [ネットワークの場所] > [ネットワークの場所を追加] > [場所のタグ]) は、アダプティブアクセス機能が有効になっている場合にのみ表示されます。詳しくは、「[アダプティブアクセス機能を有効にする](#)」を参照してください。

ネットワークの場所を変更または削除

1. Citrix Cloud コンソールで、メインメニューから [ネットワークの場所] に移動します。
2. 管理するネットワークの場所を見つけて、省略記号ボタンをクリックします。

Adaptive access based on network locations allow you to specify the internal networks in your organization. Admin can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.

Location name ↓	Public IP address range	
testloc02	192.167.100.100/32	⋮
testloc01	192.167.11.29	⋮
sydmobip02	144.273.9/32	⋮
sp_nls_nomatch	69.181.66.45/32	⋮
sp_mac_office_internal	192.221.154.0/24	⋮
sp_mac_internal	69.181.66.39/32	⋮

3. 次のいずれかのコマンドを選択します:

- [編集] を選択して、ネットワークの場所を変更します。変更したら、[保存] をクリックします。
- [削除] を選択して、ネットワークの場所を削除します。[はい、削除します] をクリックして削除を確定します。このアクションを元に戻すことはできません。

PowerShell を使用してネットワークの場所を追加および変更する

Citrix Cloud 管理コンソールインターフェイスを使用する代わりに、PowerShell スクリプトを使用して直接ワークロード接続を構成できます。PowerShell を使用した直接ワークロード接続の構成には、次のタスクが含まれます:

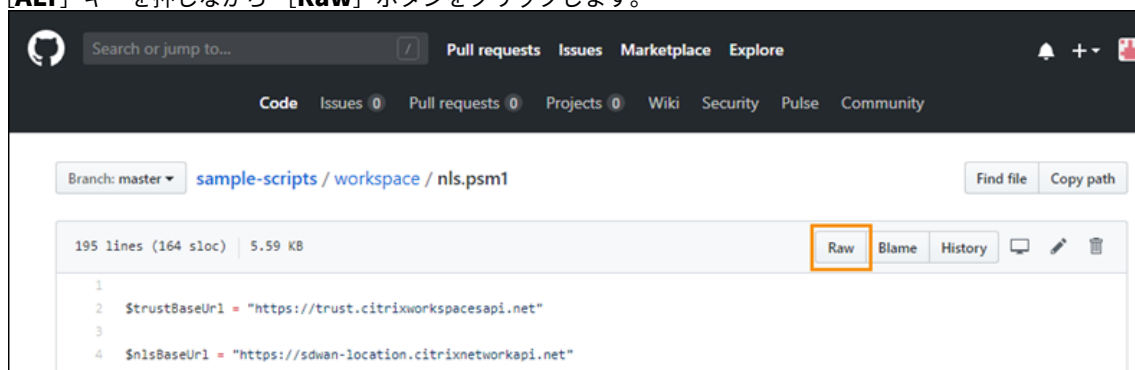
1. 内部ユーザーの接続元である各ブランチの場所のパブリック IP アドレス範囲を決定します。
2. PowerShell モジュールをダウンロードします。
3. Citrix Cloud でセキュア API クライアントを作成し、クライアント ID とシークレットを書き留めます。
4. PowerShell モジュールをインポートし、API クライアントの詳細を使用して、ネットワークの場所サービス (NLS: Network Location Service) に接続します。
5. 前述の決定したパブリック IP アドレス範囲を使用して、ブランチの場所ごとに NLS サイトを作成します。直接ワークロード接続は、指定した内部ネットワークの場所からのすべての起動に対して自動的に有効になります。
6. 内部ネットワーク上のデバイスからアプリまたはデスクトップを起動し、接続が Gateway を省略して VDA に直接接続されていることを確認します。詳しくは、この記事の「[ICA ファイルログ](#)」を参照してください。

PowerShell モジュールのダウンロード

ネットワークの場所を設定する前に、Citrix が提供している [PowerShell モジュール](#) (nls.psm1) を Citrix GitHub リポジトリからダウンロードします。このモジュールを使用して、VDA に必要な数のネットワークの場所を設定でき

ます。

1. Web ブラウザーで、<https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1>に移動します。
2. **[ALT]** キーを押しながら **[Raw]** ボタンをクリックします。



3. コンピューター上の場所を選択し、[保存] をクリックします。

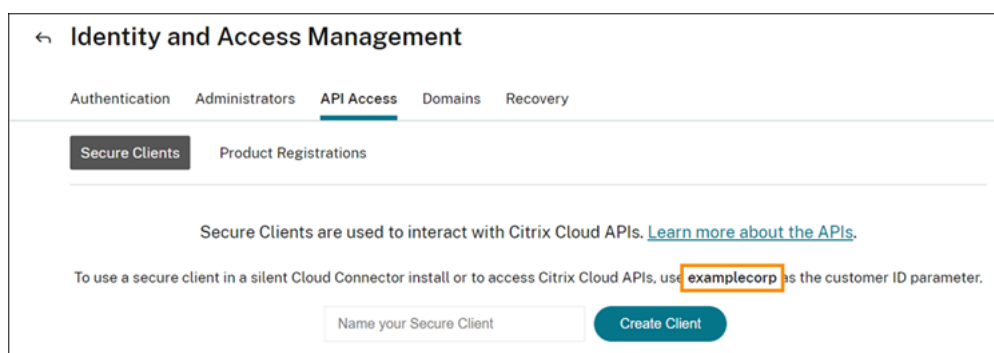
必要な構成の詳細

ネットワークの場所を設定するには、次の必須情報が必要です：

- Citrix Cloud セキュアクライアントの顧客 ID、クライアント ID、およびクライアントシークレット。これらの値を取得するには、本記事の「セキュアクライアントの作成」を参照してください。
- 内部ユーザーの接続元であるネットワークのパブリック IP アドレス範囲。これらのパブリック IP アドレス範囲について詳しくは、本記事の「要件」を参照してください。

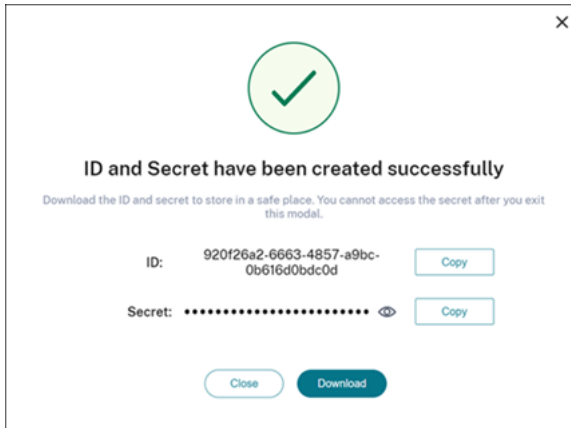
セキュアクライアントの作成

1. Citrix Cloud (<https://citrix.cloud.com>) にサインインします。
2. Citrix Cloud メニューから、**[ID およびアクセス管理]** を選択し、次に **[API アクセス]** を選択します。
3. **[セキュアクライアント]** タブで、顧客 ID をメモします。



4. クライアントの名前を入力し、**[クライアントの作成]** を選択します。

- クライアント ID とクライアントシークレットをコピーします。



ネットワークの場所の構成

- PowerShell コマンドウィンドウを開き、PowerShell モジュールを保存したディレクトリに移動します。
- 次のモジュールをインポートします: `Import-Module .\nls.psm1 -Force`
- 「セキュアクライアントの作成」のセキュアクライアント情報を使用して、必要な変数を設定します:

- `$clientId = "YourSecureClientID"`
- `$customer = "YourCustomerID"`
- `$clientSecret = "YourSecureClientSecret"`

- セキュアクライアント資格情報を使用してネットワークの場所サービスに接続します:

```
1 Connect-NLS -clientId $clientId -clientSecret $clientSecret -
  customer $customer
```

- ネットワークの場所を作成し、パラメーター値を内部ユーザーの直接接続元である内部ネットワークに対応する値に置き換えます:

```
1 New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
  ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
  12.3456 -internal $True
```

範囲ではなく単一の IP アドレスを指定するには、IP アドレスの末尾に **/32** を追加します。例:

```
1 New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
  ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
  12.3456 -internal $True
```

重要:

`New-NLSSite` コマンドを使用するときは、各パラメーターに少なくとも 1 つの値を含めます。コマンドライン引数を指定せずにこのコマンドを実行すると、PowerShell により、各パラメーターに適切

な値を1つずつ入力するように求められます。`internal`プロパティは、設定可能な値: `$True`または`$False` (PowerShell を使用して UI にマッピングされる) を持つ必須のブール値プロパティです。例: `(UI)Network Internal -> (PowerShell)-internal=$True`。

ネットワークの場所が正常に作成されると、コマンドウィンドウにネットワークの場所の詳細が表示されます。

6. ユーザーの接続元であるすべてのネットワークの場所で手順5を繰り返します。
7. コマンド`Get-NLSSite`を実行して、NLS で構成したすべてのサイトの一覧を返し、それらの詳細が正しいことを検証します。

ネットワークの場所の変更

既存のネットワークの場所を変更するには:

1. PowerShell コマンドウィンドウから、既存のネットワークの場所をすべて一覧表示します: `Get-NLSSite`
2. 特定のネットワークの場所の IP 範囲を変更するには、以下を入力します。

```
(Get-NLSSite) [N] | Set-NLSSite -ipv4Ranges @"1.2.3.4/32", "4.3.2.1/32"
```

[N] はリスト内の場所に対応する 0 から始まる番号で、`"1.2.3.4/32"`、`"4.3.2.1/32"` は使用するコンマ区切りの IP 範囲です。たとえば、リストの最初の場所を変更するには、次のコマンドを入力します:

```
(Get-NLSSite) [0] | Set-NLSSite -ipv4Ranges @"98.0.0.1/32", "141.43.0.0/24"
```

ネットワークの場所の削除

不要になったネットワークの場所を削除するには:

1. PowerShell コマンドウィンドウから、既存のネットワークの場所をすべて一覧表示します: `Get-NLSSite`
2. ネットワークの場所をすべて削除するには、「`Get-NLSSite | Remove-NLSSite`」を入力します。
3. 特定のネットワークの場所を削除するには、「`(Get-NLSSite) [N] | Remove-NLSSite`」を入力します。[N] は、リスト内の場所に対応する番号です。たとえば、リストの最初の場所を削除するには、「`(Get-NLSSite) [0] | Remove-NLSSite`」を入力します。

内部起動が正しくルーティングされていることの確認

内部起動が VDA に直接アクセスしていることを確認するには、次のいずれかの方法を使用します:

- DaaS コンソールから VDA 接続を表示します。
- ICA ファイルログを使用して、クライアント接続のアドレス指定が正しいことを確認します。

Citrix DaaS コンソール

[管理] > [監視] の順に選択し、アクティブなセッションがあるユーザーを検索します。コンソールの [セッションの詳細] セクションでは、直接 VDA 接続は UDP 接続として表示され、ゲートウェイ接続は TCP 接続として表示されます。

DaaS コンソールに UDP が表示されない場合は、VDA の HDX アダプティブトランスポートポリシーを有効にする必要があります。

ICA ファイルログ

「[launch.ica ファイルのログ作成を有効にするには](#)」の説明に従い、クライアントコンピューターで ICA ファイルログを有効にします。セッションを開始した後、ログファイルの **[Address]** および **[SSLProxyHost]** エントリを確認します。

直接 VDA 接続 直接 VDA 接続の場合、**[Address]** プロパティには VDA の IP アドレスとポートが含まれます。

クライアントが NLS を使用してアプリケーションを起動するときの ICA ファイルの例を次に示します：

```
1 [Notepad++ Cloud]
2 Address=;10.0.1.54:1494
3 SSLEnable=Off
4 <!--NeedCopy-->
```

このファイルには **SSLProxyHost** プロパティがありません。このプロパティは、ゲートウェイ経由の起動にのみ含まれます。

ゲートウェイ接続 ゲートウェイ接続の場合、**[Address]** プロパティには Citrix Cloud STA チケットが含まれ、**[SSLEnable]** プロパティは **[On]** に設定され、**[SSLProxyHost]** プロパティにはゲートウェイの FQDN とポートが含まれます。

クライアントが Citrix Gateway サービスを介して接続してアプリケーションを起動する場合の ICA ファイルの例を次に示します：

```
1 [PowerShell ISE Cloud]
2 Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
3 SSLEnable=On
4 SSLProxyHost=global.g.nssvcstaging.net:443
5 <!--NeedCopy-->
```

クライアントがオンプレミスゲートウェイを介して接続し、リソースの場所内で構成されているオンプレミスゲートウェイを使用してアプリケーションを起動する場合の ICA ファイルの例を次に示します：

```
1 [PowerShell ISE Cloud]
2 Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
```

```
3 SSLEnable=On
4 SSLProxyHost=onpremgateway.domain.com:443
5 <!--NeedCopy-->
```

注:

仮想アプリと仮想デスクトップの起動に使用されるオンプレミスゲートウェイ仮想サーバーは、nFactor 認証仮想サーバーではなく、VPN 仮想サーバーである必要があります。nFactor 認証仮想サーバーはユーザー認証専用であり、リソース HDX および ICA 起動トラフィックをプロキシしません。

スクリプト例

サンプルスクリプトには、遠隔地のパブリック IP アドレス範囲の追加、変更、削除に必要なすべてのコマンドが含まれています。ただし、1つの機能を実行するためにこのすべてのコマンドを実行する必要はありません。スクリプトを実行するには、常に **Import-Module** から **Connect-NLS** の最初の 10 行を含めます。それ以降は、実行したい機能のコマンドのみを含めることができます。

```
1 Import-Module .\nls.psm1 -Force
2
3 $clientId = "XXXX" #Replace with your clientId
4 $clientSecret = "YYY" #Replace with your clientSecret
5 $customer = "CCCCCC" #Replace with your customerid
6
7 # Connect to Network Location Service
8 Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
   $customer
9
10 # Create a new Network Location Service Site (Replace with details
   corresponding to your branch locations)
11 New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("
   1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True
12
13 # Get the existing Network Location Service Sites (optional)
14 Get-NLSSite
15
16 # Update the IP Address ranges of your first Network Location Service
   Site (optional)
17 $s = (Get-NLSSite)[0]
18 $s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
19 \ $s | Set-NLSSite
20
21 # Remove all Network Location Service Sites (optional)
22 Get-NLSSite | Remove-NLSSite
23
24 # Remove your third site (optional)
25 \ (Get-NLSSite)\[2] | Remove-NLSSite
```

トラブルシューティング

VDA の起動失敗

VDA セッションの起動に失敗する場合、正しいネットワークのパブリック IP アドレス範囲を使用していることを確認してください。ネットワークの場所を構成する場合、内部ユーザーの接続元であるネットワークのパブリック IP アドレス範囲を使用してインターネットに接続する必要があります。詳しくは、本記事の「要件」を参照してください。

内部 VDA 起動がゲートウェイを経由してルーティングされる

内部で起動された VDA セッションが外部セッションと同様にゲートウェイを経由してルーティングされる場合、内部ユーザーの接続元である正しいパブリック IP アドレスを使用してワークスペースに接続していることを確認してください。NLS サイトにリストされているパブリック IP アドレスは、リソースを起動するクライアントがインターネットへのアクセスに使用するアドレスに対応している必要があります。クライアントの正しいパブリック IP アドレスを取得するには、クライアントマシンにログオンし、検索エンジンにアクセスして検索バーに「what is my ip」（私の IP アドレスは何ですか?）と入力します。

通常、同じオフィスの場所内でリソースを起動するクライアントはすべて、同じネットワークのエグレス（送信）パブリック IP アドレスを使用してインターネットにアクセスします。これらのクライアントには、ファイアウォールによってブロックされていない、VDA が存在するサブネットへのインターネットネットワークルートが必要です。詳しくは、本記事の「要件」を参照してください。

Windows 以外のプラットフォームで PowerShell コマンドレットを実行するとエラーが発生する

PowerShell Core で正しいパラメーターを使用してコマンドレットを実行しているときにエラーが発生した場合は、操作が正常に実行されたことを確認してください。たとえば、New-NLSSite コマンドレットの実行中にエラーが発生した場合は、Get-NLSSite を実行してサイトが作成されたことを確認します。PowerShell Core を使用して macOS または Linux プラットフォームでコマンドレットを実行すると、操作が正常に実行された場合でもエラーが発生することがあります。

Windows プラットフォームで正しいパラメーターを使用して PowerShell でコマンドレットを実行しているときにこの問題が発生した場合は、PowerShell モジュールの最新バージョンを使用していることを確認してください。PowerShell モジュールの最新バージョンを使用すると、Windows プラットフォームでこの問題は発生しません。

追加のヘルプとサポート

トラブルシューティングのヘルプまたは質問については、Citrix 営業担当者または [Citrix サポート](#) にお問い合わせください。

サービス継続性

November 28, 2023

サービス継続性により、接続プロセスに関与するコンポーネントの可用性に依存することがなくなる、または最小限に抑えられます。ユーザーは、クラウドのサービス稼働状況に関係なく、Citrix DaaS のアプリと仮想デスクトップを起動できます。

サービス継続性により、ユーザーデバイスがリソースの場所へのネットワーク接続を維持している限り、ユーザーは停止中に DaaS のアプリとデスクトップに接続できます。ユーザーは、Citrix Cloud コンポーネント、またはパブリッククラウドとプライベートクラウドの停止中に DaaS のアプリとデスクトップに接続できます。ユーザーは、リソースの場所に直接接続するか、Citrix Gateway サービスを介して接続できます。

サービス継続性は、Progressive Web Apps サービスワーカーテクノロジーを使用してユーザーインターフェイスにリソースをキャッシュすることにより、停止中に公開リソースの視覚的表示を改善します。

サービス継続性は、Workspace 接続リースを使用して、ユーザーが停止中にアプリやデスクトップにアクセスできるようにします。Workspace 接続リースは、長期間有効な認証トークンです。Workspace 接続リースファイルは、ユーザーデバイスに安全にキャッシュされます。ユーザーが Citrix Workspace にサインインすると、Workspace 接続リースファイルは、ユーザーに公開された各リソースのユーザープロファイルに保存されます。サービス継続性により、ユーザーは、以前にアプリやデスクトップを起動したことがない場合でも、停止中にアプリやデスクトップにアクセスできます。Workspace 接続リースファイルは署名および暗号化されており、ユーザーとユーザーデバイスに関連付けられています。サービス継続性が有効になっている場合、Workspace 接続リースにより、ユーザーはデフォルトで 7 日間アプリとデスクトップにアクセスできます。最大 30 日間のアクセスを許可するように Workspace 接続リースを構成できます。

ユーザーが Citrix Workspace アプリを終了すると、Citrix Workspace アプリは閉じますが、Workspace 接続リースは保持されます。ユーザーは、システムトレイのアイコンを右クリックするか、ユーザーデバイスを再起動して、Citrix Workspace アプリを終了します。停止中にユーザーが Citrix Workspace からサインアウトしたときに、Workspace 接続リースを削除または保持するように、サービス継続性を構成できます。デフォルトでは、ユーザーが停止中にサインアウトすると、Workspace 接続リースはユーザーデバイスから削除されます。

Citrix Workspace アプリが仮想デスクトップにインストールされている場合、ダブルホップシナリオでサービスの継続性がサポートされています。

サービス継続性など、Citrix Cloud の回復性機能に関する詳細な技術記事については、「[Citrix Cloud の回復性](#)」を参照してください。

注:

Citrix DaaS の「接続リース」と呼ばれる廃止済みの機能は、停止時の接続の回復性を向上させるという点で、Workspace 接続リースに似ています。それ以外の点では、この廃止済み機能はサービス継続性とは無関係です。

ユーザーデバイスのセットアップ

停止中にリソースにアクセスするには、停止が発生する前にユーザーが Citrix Workspace にサインインする必要があります。サービス継続性を有効にする場合、ユーザーはデバイスで次の手順を実行する必要があります：

1. サポートされているバージョンの Citrix Workspace アプリをダウンロードしてインストールします。
2. 組織の Workspace URL を Citrix Workspace アプリに追加します (例: <https://example.cloud.com>)。
3. Citrix Workspace にサインインします。

ユーザーが Citrix Workspace に初めてサインインすると、サービス継続性により、Workspace 接続リースがユーザーデバイスにダウンロードされます。

Workspace 接続リースのダウンロードには、初回サインインに最大で 15 分かかることがあります。ユーザーは、ダウンロード期間中、公開リソースを引き続き起動できます。

停止中のユーザーエクスペリエンス

サービス継続性が有効になっている場合、停止中のユーザーエクスペリエンスは次の条件によって異なります：

- 停止のタイプ
- Citrix Workspace アプリがドメインパススルー認証で構成されているかどうか
- ユーザーが接続するアプリまたはデスクトップで、セッション共有が有効になっているかどうか

一部の停止では、ユーザーはユーザーエクスペリエンスを変更せずに、DaaS にアクセスし続けます。その他の停止の場合、ユーザーは Workspace の表示方法に変化が見られるか、何らかの操作を実行するように求められることがあります。

この表は、さまざまな種類の停止時にユーザーがアプリやデスクトップにアクセスするのに、サービス継続性がどのように役立つかをまとめたものです。

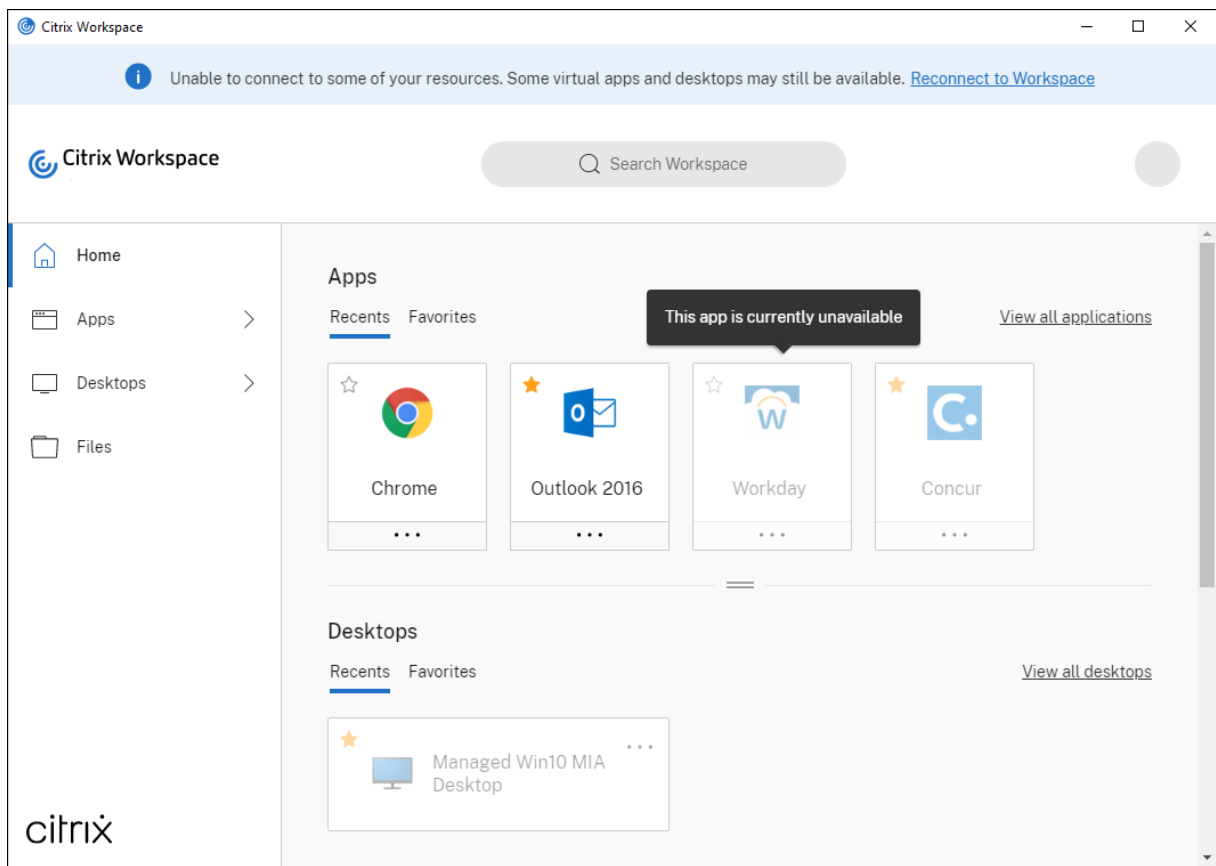
停止が発生する場所	サービス継続性によるユーザーアクセスの維持方法	停止中のユーザーエクスペリエンス
Citrix Workspace サービス	Citrix Workspace アプリは、ユーザーデバイスのローカルキャッシュに基づいてアプリとデスクトップを列挙します。	使用できないアプリやデスクトップのアイコンは選択不可の状態になります。ユーザーは、アイコンが選択不可になっていないアプリやデスクトップに引き続きアクセスできます。選択不可になっていないアイコンをクリックした後、ユーザーは VDA で資格情報を再入力するように求められることがあります。すべてのアプリとデスクトップへのアクセスを回復するには、ユーザーは [Workspace に再接続] リンクをクリックすることで、Workspace への接続を試してみることができます。
ID プロバイダー	Citrix Workspace アプリは、ユーザーデバイスのローカルキャッシュに基づいてアプリとデスクトップを列挙します。	ユーザーは Workspace にサインインできない場合があります。ユーザーは、[Workspace をオフラインで使用する] リンクをクリックして、Workspace サービスの停止と同じ操作で一部のアプリとデスクトップにアクセスします。
Citrix Cloud Broker Service	Cloud Connector の高可用性サービスが仲介を引き継ぎます。Cloud Broker Service に登録されたすべての VDA は、高可用性サービスに登録されます。	一部のユーザーは、VDA が高可用性サービスに登録している間は、仮想リソースにアクセスできない場合があります。既存のセッションは影響を受けません。ユーザーの操作は必要ありません。
Secure Ticket Authority	Workspace 接続リースは、ICA ファイルがアクセスできない場合に、仮想リソースへのアクセスを提供します。	セッションの起動には数秒かかる場合があります。ユーザーの操作は必要ありません。
Citrix Gateway サービス	ネットワークトラフィックは、最も近い正常な Citrix Gateway サービスのポイントオブプレゼンス (POP) にフェイルオーバーします。	既存のセッションは、再接続するのに数秒かかる場合があります。ユーザーの操作は必要ありません。

停止が発生する場所	サービス継続性によるユーザーアクセスの維持方法	停止中のユーザーエクスペリエンス
LAN 上のインターネット接続	Citrix Workspace アプリは、ユーザーデバイスのローカルキャッシュに基づいてアプリとデスクトップを列挙します。ユーザーがリソースの場所に直接ネットワーク接続している場合、選択不可になっていないアイコンをユーザーがクリックすると、Citrix Workspace アプリは Citrix Gateway サービスをバイパスします。Citrix Workspace アプリは、TCP 2598 を介して Cloud Connector に接続し、TCP 2598 または UDP 2598 を介して VDA に接続します。	使用できないアプリやデスクトップのアイコンは選択不可の状態になります。ユーザーは、アイコンが選択不可になっていないアプリやデスクトップに引き続きアクセスできます。選択不可になっていないアイコンをクリックした後、ユーザーは VDA で資格情報を再入力するように求められることがあります。すべてのアプリとデスクトップへのアクセスを回復するには、ユーザーは [Workspace に再接続] リンクをクリックすることで、Workspace への接続を試してみることができます。

注:

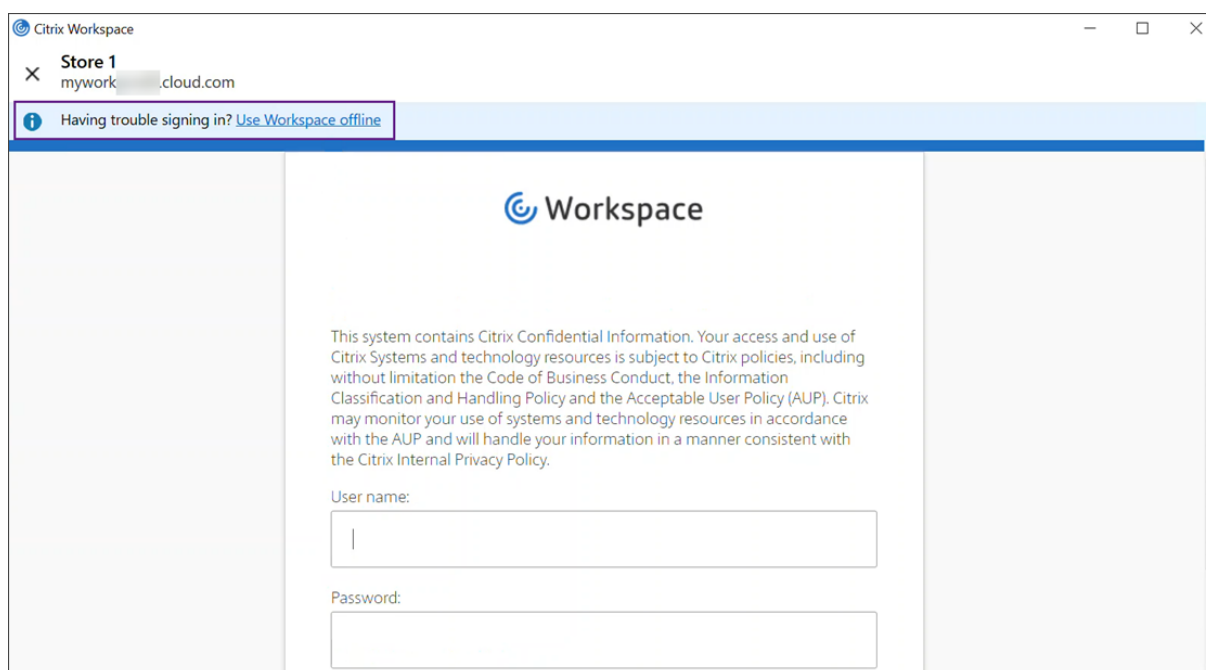
非実稼働環境での停止時の検証については、『[サービス継続性コンパニオンガイド](#)』（英語）を参照してください。

Citrix Workspace の停止中、ユーザーに対しては Citrix Workspace ホームページの上部に次のメッセージが表示されます: 「一部のリソースに接続できません。一部の仮想アプリとデスクトップは引き続き使用できる場合があります。」ユーザーには、停止中に接続できるアプリとデスクトップが表示されます。アプリまたはデスクトップが利用できない場合、アイコンは選択不可になります。



停止中に利用可能なリソースにアクセスするには、ユーザーは選択不可になっていないリソースアイコンを選択します。プロンプトが表示されたら、ユーザーは VDA で AD 資格情報を再入力して、リソースにアクセスします。

ワークスペース認証のための ID プロバイダーが停止している間は、ユーザーは Workspace サインインページから Citrix Workspace にサインインできない場合があります。40 秒後、このメッセージは Citrix Workspace ホームページの上部に表示されます。



その後、Citrix Workspace ホームページが表示されます。次に、ユーザーは Citrix Workspace の停止時と同じようにリソースにアクセスします。

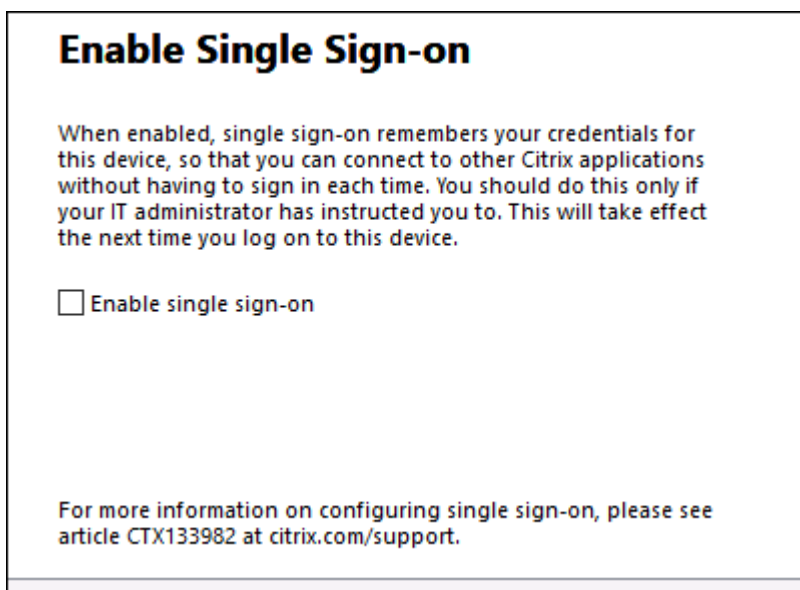
停止のタイプに関係なく、ユーザーは Citrix Workspace アプリを終了して再起動すると、引き続きリソースにアクセスできます。ユーザーは、リソースへのアクセスを失うことなく、ユーザーデバイスを再起動できます。

サービス継続性のデフォルト構成では、ユーザーは Citrix Workspace からサインアウトするとリソースにアクセスできなくなります。サインアウト後もリソースへのアクセスを維持できるようにする場合は、ユーザーがサインアウトするときに Workspace 接続リソースが維持されるように指定します。「サービス継続性を構成する」を参照してください。

Citrix Workspace アプリと VDA の構成方法によっては、停止中にユーザーは VDA から、Windows ログオンユーザーインターフェイスに資格情報を入力するよう求められる場合があります。このプロンプトが表示された場合、ユーザーは Active Directory (AD) 資格情報またはスマートカード PIN を入力して、アプリまたはデスクトップにアクセスします。この手順は、停止中にユーザー資格情報が渡されない場合に必要です。アプリまたはデスクトップにアクセスする前に、ユーザーは VDA に再認証する必要があります。

次の場合、ユーザーは AD 資格情報を入力せずにリソースにアクセスできます：

- Citrix Workspace は、シングルサインオンボックスを選択することにより、インストール中にシングルサインオン用に構成されます。



- Citrix Workspace アプリが、ドメインパススルー認証で構成されている。ユーザーは、資格情報を入力しなくても、Citrix Workspace の停止中に利用可能なリソースにアクセスできます。Windows 向け Citrix Workspace アプリのドメインパススルー認証の構成については、「[認証](#)」ドキュメントにある「[グラフィカルユーザーインターフェイスを使用したシングルサインオンの構成](#)」を参照してください。

注

停止中に VDA へのシングルサインオンを許可するために、StoreFront は必要ありません。

- セッション共有が有効になっている。ユーザーは、同じ VDA 上の 1 つのリソースの資格情報を提供した後、同じ VDA でホストされているアプリまたはデスクトップにアクセスできます。セッション共有は、VDA 上のリソースを含むアプリケーショングループに対して構成されます。アプリケーショングループの構成については、「[アプリケーショングループの作成](#)」を参照してください。

他のすべての構成では、ユーザーはリソースにアクセスする前に VDA で AD 資格情報を再入力するよう求められます。

要件および制限事項

サイトの要件

- Workspace Experience を使用する場合、Citrix DaaS および Citrix DaaS Standard for Azure のすべてのエディションでサポートされます。
- オンプレミスの Virtual Apps and Desktops へのサイトアグリゲーションを使用した Citrix Workspace でサポートされていません。
- オンプレミスの Citrix Gateway が ICA プロキシとして使用されている場合は、サポートされません (Workspace 認証方法として Citrix Gateway を使用する場合は、サポートされます)。

ユーザーデバイスの要件

サポートされている Citrix Workspace アプリの最小バージョン:

- Windows 向け Citrix Workspace アプリ 2106
- Linux 向け Citrix Workspace アプリ 2106
- Mac 向け Citrix Workspace アプリ 2106
- Android 向け Citrix Workspace アプリ 22.2.0
- iOS 向け Citrix Workspace アプリ 22.4.5
- ChromeOS 向け Citrix Workspace アプリ 2301

注:

サービス継続性のためのアプリのインストールなど、Linux 向け Citrix Workspace アプリのインストールに関する情報については、「[Linux 向け Citrix Workspace アプリ](#)」を参照してください。

- ブラウザーを使用してアプリやデスクトップにアクセスするユーザーの場合:
 - Google Chrome または Microsoft Edge。
 - Windows 向け Citrix Workspace アプリ 2109 以降。Google Chrome と Microsoft Edge でサポートされている。
 - Google Chrome で使用するには、Mac 向け Citrix Workspace アプリのバージョンが最低でも 2112 以降。
 - Safari ブラウザーで使用するには、Mac 向け Citrix Workspace アプリのバージョンが最低でも 2206 以降。

「ブラウザーのサービス継続性」を参照してください。

- デバイスごとに 1 人のユーザーのみがサポートされています。キオスクまたは「ホットデスク」ユーザーデバイスはサポートされていません。

サポートされているワークスペース認証方法

- Active Directory
- Active Directory+ トークン
- Azure Active Directory
- Okta
- Citrix Gateway (プライマリユーザーの要求は AD からのものである必要があります)
- SAML 2.0

認証の制限

- Citrix フェデレーション認証サービス (FAS) を使用したシングルサインオンはサポートされていません。ユーザーは、VDA の Windows ログオンユーザーインターフェイスに AD 資格情報を入力します。

- VDA へのシングルサインオンはサポートされていません。
- ローカルにマップされたアカウントはサポートされていません。
- Azure AD に参加している VDA はサポートされていません。すべての VDA は AD ドメインに参加する必要があります。

Citrix Cloud Connector のスケールとサイズ

- 4 vCPU 以上
- 4GB 以上のメモリ

Citrix Cloud Connector Powershell セキュリティ

実行ポリシーを環境に適した **remotedSigned** に設定して、スクリプトの実行が有効になっていることを確認します。

Default や **AllSigned** など、他のスクリプト実行権限も使用できます。

Citrix Cloud Connector の接続

Citrix Cloud Connector は <https://rootoftrust.apps.cloud.com> にアクセスできる必要があります。この接続を許可するようにファイアウォールを構成します。Cloud Connector のファイアウォールについて詳しくは、「[Cloud Connector のプロキシとファイアウォールの構成](#)」を参照してください。

Workspace アプリのネットワーク接続

LAN の外部からリソースの場所への接続を構成する場合、ユーザーデバイス上の Workspace アプリは、Citrix Gateway Service FQDN (https://*.g.nssvc.net) に到達する必要があります。ユーザーデバイスが Citrix Gateway Service にいつでも接続できるように、ファイアウォールが <https://global-s.g.nssvc.net:433> への送信トラフィックを許可するように構成されていることを確認してください。

接続の最適化の制限

Advanced Endpoint Analysis (EPA) は、サポートされていません。

Enlightened Data Transport (EDT) は、停止中はサポートされません。

VDA の要件と制限

- VDA 7.15 LTSR、または製品終了となっていない最新リリースはサポートされています。

- Azure AD に参加している VDA はサポートされていません。すべての VDA は AD ドメインに参加する必要があります。
- ユーザーが停止中に VDA リソースにアクセスするには、VDA がオンラインである必要があります。VDA が以下の停止の影響を受ける場合、VDA リソースは使用できません：
 - AWS
 - Azure
 - Cloud Delivery Controller (リソースを配信するデリバリーグループに対して Autoscale が有効になっている場合を除く)。
- 停止中にサポートされる VDA ワークロード：
 - ホストされている共有アプリと共有デスクトップ
 - 電源管理を使用するランダムな非永続デスクトップ (プールされた VDI デスクトップ)
 - 静的な非永続デスクトップ
 - リモート PC アクセスなどの静的な永続デスクトップ

注:

初回使用時の割り当ては、停止中はサポートされません。Cloud Connector が Citrix Cloud との接続を失った場合、デリバリーグループに `ReuseMachinesWithoutShutdownInOutage` が構成されていない限り、電源管理を備えたランダムな非永続デスクトップはデフォルトで使用不可となります。詳しくは、「[アプリケーションとデスクトップのサポート](#)」を参照してください。

停止中に使用可能な VDA 機能について詳しくは、「[停止中の VDA 管理](#)」を参照してください。

ローカルキーボードマッピングの要件と制限

VDA での再認証をユーザーに求める Windows ログオンユーザーインターフェイスは、ローカルキーボード言語マッピングをサポートしていません。デバイスにローカルキーボード言語マッピングがある場合にユーザーが停止中に再認証できるようにするには、これらのユーザーが必要とするキーボードレイアウトを事前ロードします。

警告:

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

VDA イメージで次のレジストリキーを編集します:

`HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`

仮想デスクトップイメージ内の対応する言語パックをインストールする必要があります。

キーボード言語に関連付けられているキーボード識別子の一覧については、「[Windows 用のキーボード識別子と入力システム](#)」を参照してください。

サービス継続性のためにリソースの場所のネットワーク接続を構成する

LAN の内部、外部、またはその両方からの接続を受け入れるように、リソースの場所を構成できます。

LAN の内部の接続を構成する

1. Citrix Cloud メニューから、**[Workspace の構成]** > [アクセス] の順に選択します。
2. [接続の構成] を選択します。
3. 接続タイプとして、[内部のみ] を選択します。
4. [保存] をクリックします。

Common Gateway Protocol(CGP)TCP ポート 2598 を介した接続を受け入れるように、Citrix Cloud Connector と VDA ファイアウォールを構成します。この構成はデフォルト設定です。

LAN の外部からの接続を構成する

1. Citrix Cloud メニューから、**[Workspace の構成]** > [アクセス] の順に選択します。
2. [接続の構成] を選択します。
3. 接続タイプとして、**[Gateway サービス]** を選択します。
4. [保存] をクリックします。

LAN の外部と内部の両方からの接続を構成する

次の PowerShell コマンドを実行します：

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocationExternalUid) -EnableHybridConnectivityForResourceLeases $true
```

`YourResourceLocationExternalUid`をリソースの場所の外部 UID に置き換えます。

このコマンドを使用すると、停止中に TCP 2598 を介して Citrix Cloud Connector の FQDN (完全修飾ドメイン名) に直接接続できます。その接続が失敗した場合、Gateway サービスがフォールバックとして使用されます。内部ユーザーがゲートウェイをバイパスしてリソースの場所に直接接続できるように許可することで、内部ネットワークのトラフィックの遅延を減らします。

注：

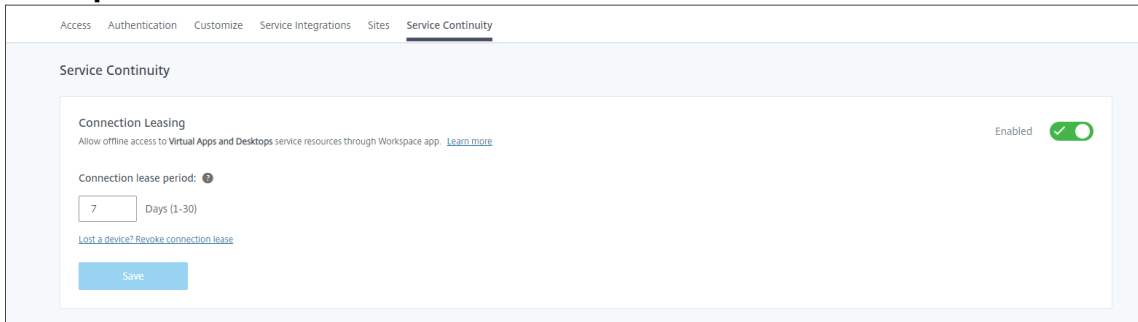
この PowerShell コマンドは、内部ユーザーがゲートウェイをバイパスして VDA に直接接続できるようにすることで、ワークスペースへの接続を最適化するという点で、直接ワークロード接続に似ています。サービス継

続性が有効になっている場合、停止中は直接ワークロード接続を使用できません

サービス継続性を構成する

サイトのサービス継続性を有効にするには：

1. Citrix Cloud メニューから、[**Workspace** の構成] > [サービス継続性] の順に選択します。
2. [**Workspace** の接続リース] を [有効] に設定します。



3. [接続リースの期間] で、Workspace 接続リースを使用して接続を維持できる日数を設定します。Workspace 接続リースの期間は、サイトを介したすべての Workspace 接続リースに適用されます。Workspace 接続リースの期間は、ユーザーが Citrix Cloud Workspace ストアに初めてサインインしたときに始まります。Workspace 接続リースは、ユーザーがサインインするたびに、最大 1 日 1 回更新されます。Workspace 接続リースの期間は、1 日～30 日間まで設定できます。デフォルト設定は、7 日間です。
4. [保存] をクリックします。

サービス継続性を有効にすると、サイト内のすべてのデリバリーグループに対して有効になります。デリバリーグループのサービス継続性を無効にするには、次の PowerShell コマンドを使用します：

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

`deliverygroup` をデリバリーグループの名前に置き換えます。

デフォルトでは、ユーザーが停止中に Citrix Workspace からサインアウトすると、Workspace 接続リースはユーザーデバイスから削除されます。ユーザーがサインアウトした後も Workspace 接続リースをユーザーデバイスに残したい場合は、次の PowerShell コマンドを使用します：

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

注：

Mac 向け Citrix Workspace アプリに接続するユーザーのために、ユーザーのサインアウト後に Workspace 接続リースをユーザーデバイスに残すように設定することはできません。Mac 向け Citrix Workspace は、`DeleteResourceLeaseOnLogOff` プロパティの値を読み取ることができません。

サービス継続性の仕組み

停止がない場合、ユーザーは ICA ファイルを使用して仮想アプリと仮想デスクトップにアクセスします。Citrix Workspace は、ユーザーが仮想アプリまたは仮想デスクトップのアイコンを選択するたびに、一意の ICA ファイルを生成します。各 ICA ファイルには、Secure Ticket Authority (STA) チケットと、仮想リソースへの許可されたアクセスを取得するために 1 回だけ引き換えることができるログオンチケットが含まれています。各 ICA ファイルのチケットは、約 90 秒後に期限切れになります。ICA ファイルのチケットが使用されるか期限切れになった後、ユーザーはリソースにアクセスするために Citrix Workspace からの別の ICA ファイルを必要とします。サービス継続性が有効になっていない場合、Citrix Workspace が ICA ファイルを生成できないと、停止によってユーザーがリソースにアクセスできなくなる可能性があります。

Citrix Workspace は、サービス継続性が有効になっているかどうかに関係なく、ユーザーが仮想アプリと仮想デスクトップを起動したときに ICA ファイルを生成します。サービス継続性が有効になっていると、Citrix Workspace は Workspace 接続リースを構成する一意のファイルセットも生成します。ICA ファイルとは異なり、Workspace 接続リースファイルは、ユーザーがリソースを起動したときではなく、ユーザーが Citrix Workspace にサインインしたときに生成されます。ユーザーが Citrix Workspace にサインインすると、そのユーザーに公開されたすべてのリソースに対して接続リースファイルが生成されます。Workspace 接続リースには、ユーザーに仮想リソースへのアクセスを許可する情報が含まれています。停止により、ユーザーが Citrix Workspace にサインインしたり、ICA ファイルを使用してリソースにアクセスしたりできない場合、接続リースがリソースへのアクセスを許可します。

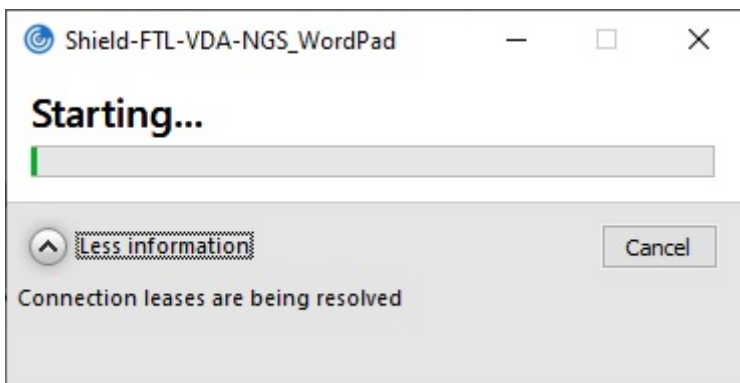
停止中にセッションを開始する方法

停止中にユーザーがアプリまたはデスクトップのアイコンをクリックすると、Citrix Workspace アプリは対応する Workspace 接続リースをユーザーデバイス上で検出します。次に、Citrix Workspace アプリが接続を開きます。アプリまたはデスクトップをホストするリソースの場所への接続が LAN の外部からの接続を受け入れるように構成されている場合、Citrix Gateway サービスへの接続が開きます。アプリまたはデスクトップをホストするリソースの場所への接続が LAN 内からの接続のみを受け入れるように構成した場合、Cloud Connector への接続が開きます。

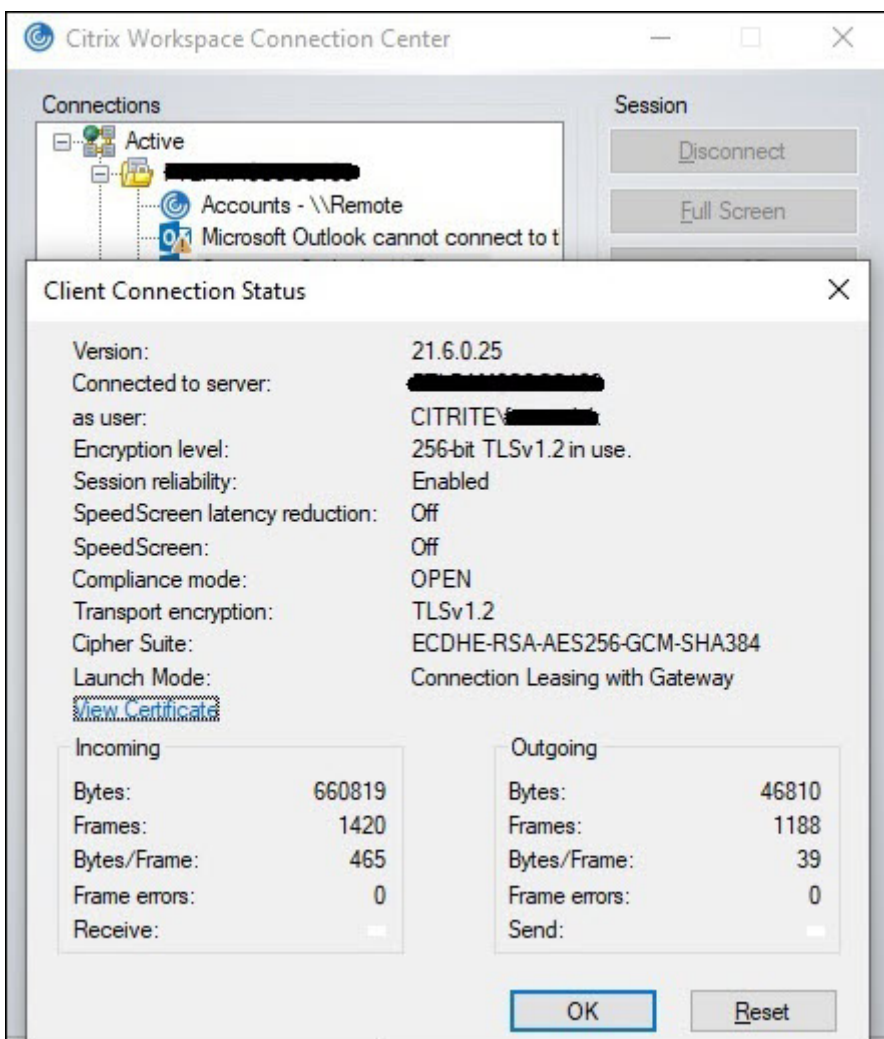
Citrix Cloud ブローカーがオンラインの場合、Cloud Connector は Citrix Cloud ブローカーを使用して、どの VDA が使用可能かを解決します。Citrix Cloud ブローカーがオフラインの場合、Cloud Connector のセカンダリブローカー（高可用性サービス）は、接続要求をリッスンして処理します。

接続済みのユーザーは、停止状態が発生した場合も途切れることなく作業を続行できます。再接続時および新規接続時の接続遅延は最小限に抑えられます。この機能はローカルホストキャッシュに似ていますが、オンプレミスの StoreFront を必要としません。

ユーザーが停止中にセッションを起動すると、このウィンドウが表示され、Workspace 接続リースがセッションの起動に使用されたことを示します：

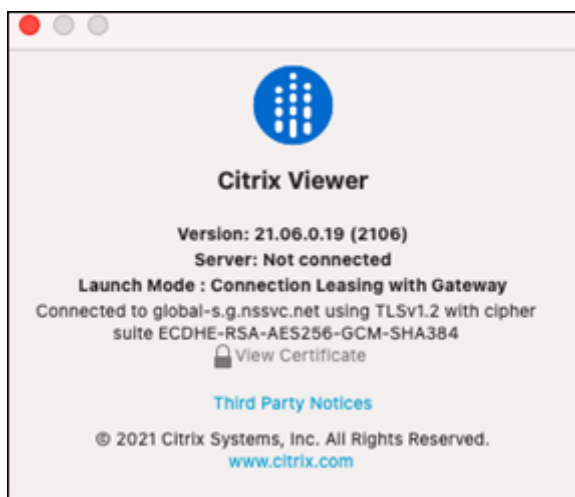


ユーザーがセッションへのサインインを完了すると、以下のプロパティが Workspace 接続センターに表示されます:



起動モードプロパティは、セッションの起動に使用される Workspace 接続リースに関する情報を提供します。

Mac 向け Citrix Workspace アプリを実行しているデバイス上の Citrix Viewer では、Workspace 接続リースがセッションの起動に使用されたことを示す情報が表示されます:



安全性を高めるもの

Workspace 接続リースファイル内のすべての機密情報は、AES-256 暗号で暗号化されます。Workspace 接続リースは、指定のクライアントデバイスに一意に関連付けられた公開/秘密キーペアに関連付けられ、別のデバイスでは使用できません。組み込みの暗号化メカニズムにより、各デバイスで一意的なキーペアが強制的に使用されます。

Workspace 接続リースは、AppData\Local\Citrix\SelfService\ConnectionLeases のユーザーデバイスに保存されます。

サービス継続性のセキュリティアーキテクチャは、公開キー基盤（PKI）と同様に、公開キー暗号化に基づいて構築されていますが、証明書チェーンと認証機関はありません。代わりに、すべてのコンポーネントは、認証機関のように機能する信頼のルートと呼ばれる新しい Citrix Cloud サービスに依存することにより、推移的な信頼関係を確立します。

接続リースの禁止

ユーザーデバイスの紛失や盗難、またはユーザーアカウントの閉鎖または侵害が発生した場合、Workspace 接続リースを禁止できます。ユーザーに関連付けられた Workspace 接続リースを禁止すると、ユーザーはリソースに接続できなくなります。Citrix Cloud は、ユーザーの Workspace 接続リースを生成または同期しなくなります。

ユーザーアカウントに関連付けられた Workspace 接続リースを禁止すると、そのアカウントに関連付けられているすべてのデバイスで、そのアカウントへの接続が禁止されます。ユーザーまたはユーザーグループ内のすべてのユーザーの Workspace 接続リースを禁止できます。

単一のユーザーまたはユーザーグループの Workspace 接続リースを取り消すには、次の PowerShell コマンドを使用します：

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays  
Days
```

`username`を、接続を禁止するアカウントに関連付けられたユーザーに置き換えます。`username`をユーザーグループに置き換えて、そのユーザーグループ内のすべてのアカウントからの接続を禁止します。`Days`を、接続を禁止する日数に置き換えます。

たとえば、次の7日間、`xd.local/user1`の接続を禁止するには、次のように入力します：

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
   LeaseRevocationDays 7
```

Workspace 接続リースが取り消されている期間を表示するには、次の PowerShell コマンドを使用します：

```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

`username`を、期間を表示する対象のユーザーまたはユーザーグループに置き換えます。

たとえば、`xd.local/user1`について、Workspace 接続リースを取り消している期間を表示するには、次のように入力します：

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

次の情報が表示されます：

```
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
```

この出力から、ユーザー `xd.local/user2` の Workspace 接続リースが、2020年12月17日から2020年12月19日までの2日間、毎日 17:34:25 (UTC) に取り消されていることがわかります。

Workspace 接続リースが取り消されているユーザーアカウントで再度接続できるようにするには、次の PowerShell コマンドを使用して禁止設定を削除します：

```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

`username`を、接続を受けつける禁止されたユーザーまたはユーザーグループに置き換えます。禁止されたすべてのユーザーアカウントで接続を受けつけるようにするには、`Name` オプションを削除します。

ダブルホップシナリオ

停止が発生する前にユーザーが Citrix Workspace にサインインしている場合、ダブルホップシナリオでは、サービス継続性によりユーザーは停止中に仮想リソースにアクセスできます。ダブルホップシナリオでは、物理ユーザーデバイスが Citrix Workspace アプリがインストールされている仮想デスクトップに接続します。次に、仮想デスクトップが別の仮想リソースに接続します。

ダブルホップシナリオでは、仮想デスクトップのタイプに関係なく、サービス継続性によりユーザーは停止中に仮想リソースにアクセスできます。仮想デスクトップがユーザーの変更を保持している場合、サービス継続性により、ユーザーがサインインしていないときに発生した停止時に仮想リソースへのアクセスを提供することもできます。

サービス継続性は、ダブルホップシナリオの物理ユーザーデバイスと仮想デバイスを個別のクライアントエンドポイントとして扱います。各デバイスには、独自の Workspace 接続リースのセットがあります。ユーザーが物理デバイスで Citrix Workspace にサインインすると、Workspace 接続リースファイルがダウンロードされ、物理デバイスのユーザープロファイルに保存されます。次に、ユーザーは仮想デスクトップにアクセスし、仮想デスクトップ上の Citrix Workspace にサインインします。この時点で、別の Workspace 接続リースのセットがダウンロードされ、仮想デスクトップにユーザープロファイルが保存されます。Workspace 接続リースファイルは、ダウンロード先のデバイスに関連付けられています。同じユーザーであっても、Workspace 接続リースファイルを別のデバイスにコピーして再利用することはできません。このため、仮想デスクトップがユーザーセッション中に行われた変更を破棄した場合、セッションの終了後に発生する停止中、サービス継続性がリソースへのアクセスを提供することはできません。この種類の仮想デスクトップの場合、Workspace 接続リースは破棄される変更の 1 つです。

サポートされている仮想デスクトップの種類ごとに、ダブルホップシナリオでサービス継続性がどのように機能するかを次に示します。

以下を含むダブルホップの場合…	サービス継続性により、停止時に仮想リソースへのアクセスを提供できます…
ホストされた共有デスクトップ	ユーザーが仮想デスクトップにサインインしているときに停止が発生した場合。
ランダムな非永続デスクトップ（プール型の VDI デスクトップ）	ユーザーが仮想デスクトップにサインインしているときに停止が発生した場合。
静的な非永続デスクトップ	ユーザーが最後にログインしてから仮想デスクトップが再起動していない場合。
静的な永続デスクトップ	停止が発生したときはいつでも。

停止中の VDA 管理

サービス継続性は、Citrix Cloud Connector 内のローカルホストキャッシュ機能を使用します。ローカルホストキャッシュを使用すると、Cloud Delivery Controller と Cloud Connector の間の接続に障害が発生した場合でも、サイトで接続仲介操作を続行できます。サービス継続性はローカルホストキャッシュに依存しているため、いくつかの制限をローカルホストキャッシュと共有しています。

注:

サービス継続性は Cloud Connector 内でローカルホストキャッシュを使用しますが、サービス継続性は、ローカルホストキャッシュとは異なり、オンプレミスの StoreFront ではサポートされていません。

停止中の **VDA** の電源管理

Cloud Connector が Citrix Cloud への接続を失うと、Connector は Citrix Cloud からハイパーバイザー資格情報を受信できなくなります。以下の点に注意してください：

- 停止中は、すべてのマシンの電力状態が不明となるため、電源操作を実行できなくなります。ただし、電源が入っているホスト上の VM を接続要求のために使用することができます。

Cloud Connector が Citrix Cloud との接続を失った場合、**ShutdownDesktopsAfterUse** プロパティが有効になっている、プールされたデリバリーグループ内の電源管理されたデスクトップ VDA を新しい接続に使用することはできません。Cloud Connector が Citrix Cloud との接続を失った場合でも、これらのデスクトップを使用できるようにこの設定を変更できます。それには、デリバリーグループに対して **ReuseMachinesWithoutShutdownInOutage** フラグを設定します。**ReuseMachinesWithoutShutdownInOutage** パラメータを `$true` に変更することで、VDA を再起動するまでこれまでのユーザーセッションのデータを VDA 上に残すことができます。

停止後に通常の運用が再開されると、電源管理が再開されます。

マシンの割り当てと自動登録

割り当てられたマシンは、通常の操作中に割り当てが発生した場合のみ使用できます。停止状態中は新しい割り当てはできません。

リモート PC アクセスマシンの自動登録と構成はできません。ただし、通常の操作中に登録、構成されたマシンは使用できます。

異なるゾーンの **VDA** リソース

サーバーでホストされるアプリケーションとデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。

ローカルホストキャッシュとは異なり、サービス継続性は、リソースが複数のゾーンで公開されている場合、異なるゾーンの登録済み VDA からアプリとデスクトップを起動できます。Citrix Workspace アプリは、Workspace 接続リリース内のすべてのゾーンを順番に循環するため、正常なゾーンを見つけるのに時間がかかる場合があります。

監視とトラブルシューティング

サービス継続性は、次の 2 つの主要なアクションを実行します：

- Workspace 接続リリースをユーザーデバイスにダウンロードする。Workspace 接続リリースが生成され、Citrix Workspace アプリと同期されます。
- 仮想デスクトップと仮想アプリは、Workspace 接続リリースを使用して起動されます。

Workspace 接続リースのダウンロードのトラブルシューティング

ユーザーデバイスの以下の場所で、Workspace 接続リースを表示できます。

Windows デバイスの場合：

```
C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\  
Store GUID\User GUID\leases
```

Usernameはユーザー名です。

Store GUIDは Workspace ストアのグローバルな一意の識別子です。

User GUIDはユーザーのグローバルな一意の識別子です。

Mac デバイスの場合：

```
$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot
```

たとえば、/Users/luca/Library/Application Support/Citrix Receiver/
CLSyncRootを開きます。

Linux の場合：

```
$HOME/.ICAClient/cache/ConnectionLease
```

たとえば、/home/user1/.ICAClient/cache/ConnectionLeaseを開きます。

Workspace 接続リースは、Citrix Workspace アプリが Workspace ストアに接続するときに生成されます。ユーザーデバイスのレジストリキー値を表示して、Citrix Workspace アプリが Citrix Cloud の Workspace 接続リースサービスに正常に接続したかどうかを確認できます。

ユーザーデバイスで regedit を開き、次のキーを表示します：

```
HKCU\Software\Citrix\Dazzle\Sites\store-xxxx
```

次の値がレジストリキーに表示される場合、Citrix Workspace アプリは Workspace 接続リースサービスに接続したか、接続を試みたこととなります：

- leaseLastCallHomeTime
- leaseLastSyncStatus

Citrix Workspace アプリが Workspace 接続リースサービスへの接続に失敗した場合、leaseLastCallHomeTime は次のように無効なタイムスタンプを付けてエラーを表示します：

```
leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM
```

leaseLastCallHomeTimeが初期化されていない場合、Citrix Workspace アプリは Workspace 接続リースサービスへの接続を試みなかったこととなります。この問題を解決するには、Citrix Workspace アプリからアカウントを削除して、再度追加します。

Workspace 接続リースの **Citrix Workspace** アプリエラーコード

ユーザーデバイスでサービス継続性エラーが発生すると、エラーメッセージにエラーコードが表示されます。一般的なエラーには次のものが含まれます：

エラーコード	説明
3000	接続リースファイルが存在しません
3002	接続リースが読み取れない、または見つかりません
3003	リソースの場所が見つかりません
3004	リースに接続の詳細がありません
3005	ICA ファイルが空です
3006	接続リースの期限が切れました。Workspace に再度ログインします。
3007	接続リースが無効です
3008	接続リースの検証結果：空
3009	接続リースの検証結果：無効
3010	パラメーターがありません
3020	接続リースの検証に失敗しました
3021	アプリが公開されているリソースの場所が見つかりません
3022	接続リースの検証結果：拒否
3023	Citrix Workspace アプリがタイムアウトしました
3024	処理中にユーザーがリースベースの起動をキャンセルしました
3025	起動-再試行回数を超えました
3026	ネゴシエートされたリソース（アプリまたはデスクトップ）を起動できません

selfservice.txt へのアクセス

セルフサービスのトラブルシューティングのために **selfservice.txt** ファイルにアクセスするには、次の手順を実行します：

1. 空白のテキストファイルを作成し、「**enablesieldandlogging.reg**」という名前を付けます。
2. 次のテキストをそのファイルにコピーして保存します：

Windows Registry Editor 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. 保存したファイルをクライアントエンドポイントに配置します。
4. `selfservice.txt`ファイルが次のパスで検出できるようになりました: `%LocalAppData%\Citrix\SelfService`。

ブラウザのサービス継続性

Google Chrome と Microsoft Edge の拡張機能により、これらの Web ブラウザーを使用してアプリやデスクトップにアクセスする Windows ユーザーがサービス継続性を利用できるようになります。この拡張機能は、Citrix Workspace の Web 拡張機能と呼ばれ、[Chrome ウェブストア](#)と[Microsoft Edge アドオン Web サイト](#)で利用できます。

これらの Web ブラウザー拡張機能は、サービス継続性をサポートするために、ユーザーデバイス上にネイティブの Citrix Workspace アプリを必要とします。以下のバージョンがサポートされています：

- Windows 向け Citrix Workspace アプリ 2109 以降。Google Chrome と Microsoft Edge でサポートされている。
- Mac 向け Citrix Workspace アプリバージョン 2112 以降。Google Chrome でサポートされている。
- Safari ブラウザーで使用するには、Mac 向け Citrix Workspace アプリのバージョンが最低でも 2206 以降。

Windows（ストア）用の Citrix Workspace アプリはサポートされていない。

ネイティブの Workspace アプリは、Web ブラウザー拡張機能用のネイティブメッセージングホストプロトコルを使用して、Citrix Workspace Web 拡張機能と通信します。ネイティブの Workspace アプリと Workspace Web 拡張機能は、Workspace 接続リソースを使用して、停止中に Web ブラウザーユーザーがアプリとデスクトップにアクセスできるようにします。

このビデオでは、ブラウザにサービス継続性をインストールして使用方法を説明しています。

[これは埋め込みビデオです。リンクをクリックしてビデオを見る](#)

Web ブラウザーユーザー向けのユーザーデバイスセットアップ

Web ブラウザーでサービス継続性を使用するには、ユーザーはデバイスで次の手順を実行する必要があります：

1. ブラウザーユーザー向けのサポートがあるバージョンの Citrix Workspace アプリをダウンロードしてインストールします。
2. Chrome または Edge 向け Citrix Workspace Web 拡張機能をダウンロードしてインストールします。

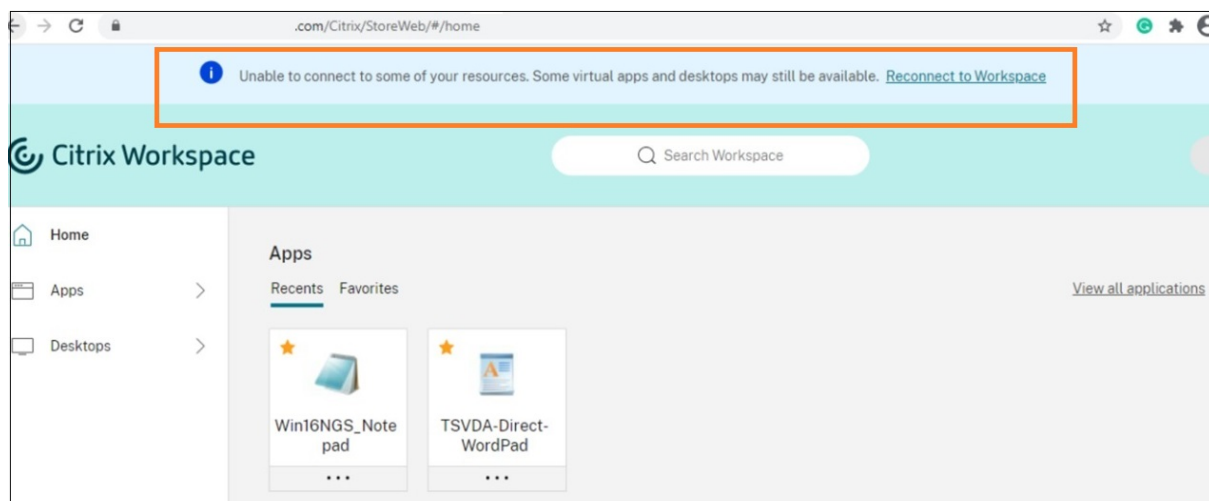
Web ブラウザーのユーザーエクスペリエンス

ユーザーがアプリまたはデスクトップをクリックすると、**Citrix Workspace Launcher** を開くよう求めるプロンプトがユーザーに表示されずに、アプリまたはデスクトップが開きます。

停止中の Web ブラウザーのユーザーエクスペリエンス

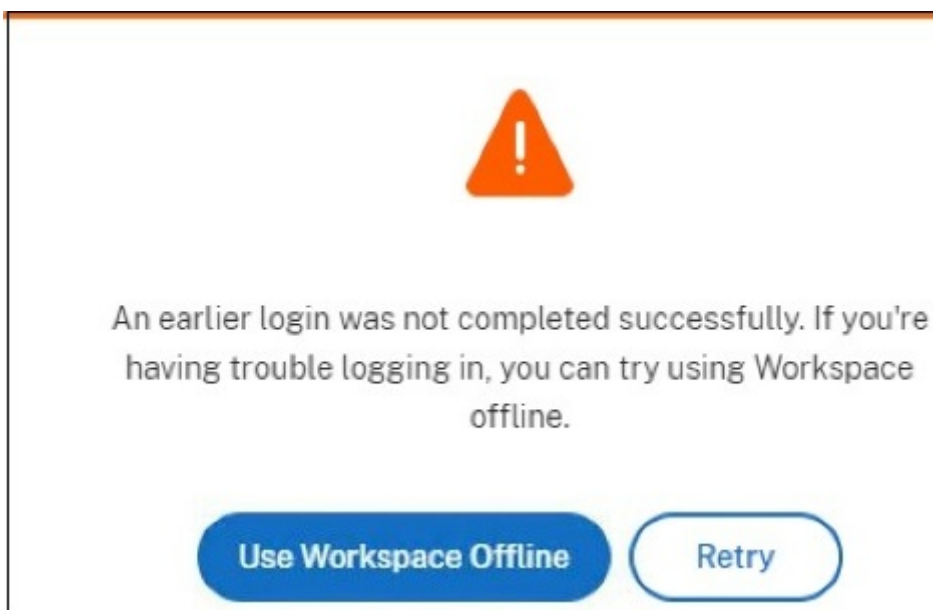
ユーザーデバイスがリソースの場所へのネットワーク接続を維持している限り、ユーザーは停止中に Web ブラウザーからアプリとデスクトップにアクセスできます。

ユーザーが Web ブラウザーで Workspace にログインしているときに停止が発生した場合、次のメッセージが Web ブラウザーウィンドウの上部に表示されます：



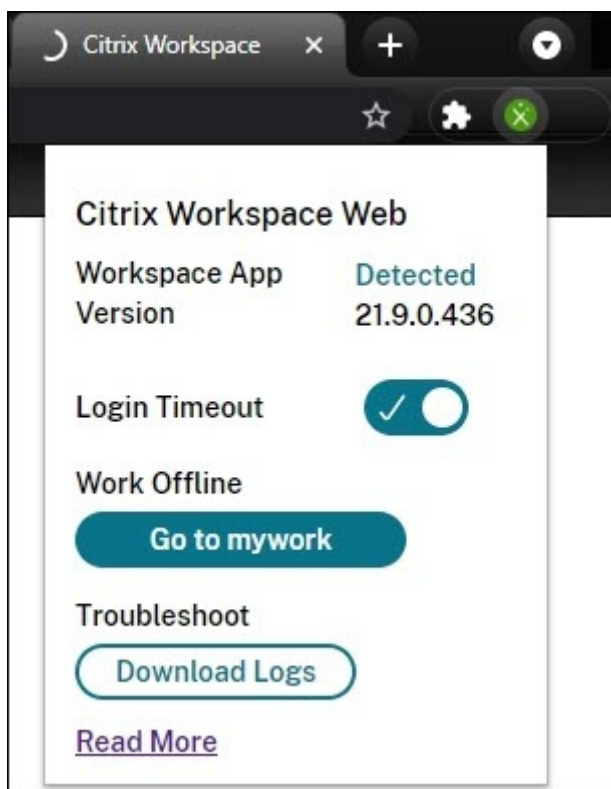
ユーザーは、選択不可になっていないアイコンをクリックして、オフラインで使用できるアプリとデスクトップにアクセスできます。ユーザーは、**[Workspace に再接続]** をクリックして、オンラインに戻ることを試すこともできます。

停止によりユーザーが Web ブラウザーで Workspace にログインできなくなった場合、オフラインで作業するか、ログインを再試行するよう求めるプロンプトがユーザーに表示されます。使用できるアプリやデスクトップにオフラインでアクセスするために、ユーザーは **[Workspace をオフラインで使用する]** をクリックします。



ユーザーが Workspace URL に移動した後、停止により Workspace にログインできない場合、指定したタイムアウト時間が経過した後にウィンドウが表示されます。デフォルトでは、ユーザーが Workspace URL に移動してから 30 秒後に、ウィンドウが表示されます。この値は 15、30、45、または 60 秒に設定できます。ログインタイムアウトを無効にすることもできます。ログインタイムアウトが無効になっている場合、ユーザーが Workspace URL に移動すると、オフラインで作業するように求めるウィンドウが表示されます。

ログインタイムアウト設定を構成するには、ユーザーデバイスの Web ブラウザーで拡張機能アイコンをクリックします。表示されるウィンドウでログインタイムアウトを有効または無効にし、タイムアウト期間を設定します：



Web ブラウザーがサードパーティの ID プロバイダー認証サイトにリダイレクトされた場合、停止によりユーザーがログインできないことがあります。この場合、ユーザーは Workspace URL を Web ブラウザーに入力することができ、入力するとオフラインで作業するように求めるウィンドウがユーザーに対して表示されます。ユーザーは、ウィンドウが表示されるまでログインタイムアウト時間を待つ必要はありません。

また、ユーザーは次の方法で、停止中に使用できるアプリやデスクトップにアクセスできます：

1. Web ブラウザーの拡張機能アイコンをクリックします。
2. 表示されたウィンドウで、[オフラインで実行] の下のボタンをクリックします。このボタンは […に移動] と表示され、「…」の部分に Workspace ストアの名前が表示されます。
3. 表示されたウィンドウで、[**Workspace** をオフラインで使用する] をクリックします。

停止中は、拡張機能が Workspace 側の問題を検出すると、オフラインで作業をするように求める警告ウィンドウがユーザーに対して自動的に表示されます。ユーザーは、操作したり、ログインタイムアウト時間を待つ必要はありません。

Web ブラウザーの制限

停止中、ユーザーが Web ブラウザーで Cookie やその他のサイトデータをクリアした場合、ユーザーが Workspace に再度認証するまで、サービス継続性は機能しません。

ユーザーが拡張機能をシークレットモードで動作させることを許可しない限り、シークレットモードではサービス継続性はサポートされません。

Web ブラウザーユーザー向けのトラブルシューティング

Citrix Workspace ブラウザーアプリアカウント設定の [詳細設定] メニューで、現在のアプリとデスクトップの起動設定方法が **[Citrix Workspace App を使用する]** に設定されていることを確認します。このオプションが **[Web ブラウザーを使用する]** に設定されている場合、Web ブラウザーではサービス継続性はサポートされません。

ブラウザーが Workspace URL を読み込んだ後、ブラウザーの拡張機能アイコンが緑色で表示されていることを確認します。

ログをダウンロードするには、Web ブラウザーの拡張機能アイコンをクリックします。次に、[ログのダウンロード] をクリックします。

Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化

October 12, 2023

Citrix フェデレーション認証サービス (FAS) は、Citrix Workspace で DaaS へのシングルサインオン (SSO) をサポートします。通常、FAS は、Citrix Workspace 認証に以下の ID プロバイダーのいずれかを使用している場合に採用されます：

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

FAS を使用すると、利用者は資格情報を 1 回入力するだけで DaaS のアプリとデスクトップにアクセスできます。

Active Directory (AD)、AD+ トークン、または Citrix Gateway の特定の構成を使用している場合、DaaS への SSO に FAS は必要ありません。Citrix Gateway の構成について詳しくは、「[オンプレミスの Citrix Gateway での OAuth ID プロバイダーポリシーの作成](#)」を参照してください。

FAS サーバー

各リソースの場所内で、負荷分散とフェールオーバーのために複数の FAS サーバーを Citrix Cloud に接続できます。

Citrix Cloud は、以下のシナリオで FAS サーバーの使用をサポートしています。

どちらのシナリオでも、フェデレーション ID プロバイダーを介してワークスペースにサインインする利用者は、アプリとデスクトップにアクセスするために資格情報を一度だけ入力します。

単一のリソースの場所に接続された **FAS** サーバー

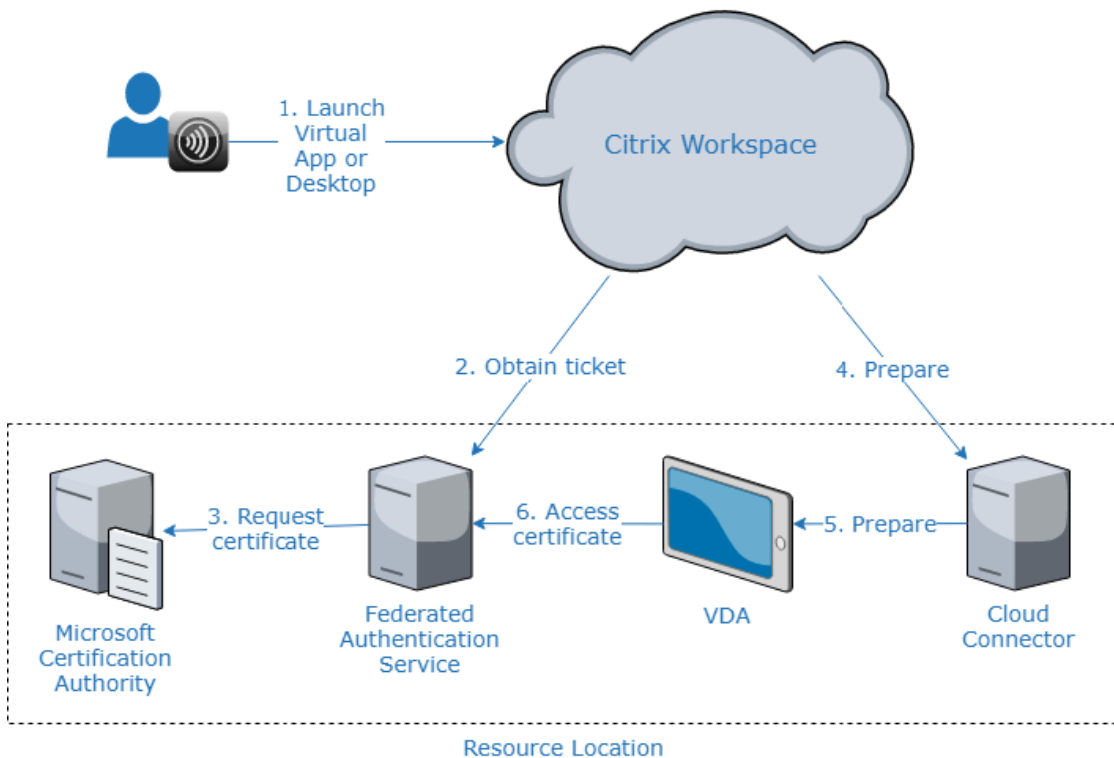
リソースの場所にさまざまなインフラストラクチャが含まれている場合（たとえば、さまざまなリソースの場所にさまざまな AD フォレストが含まれている場合）、FAS サーバーを VDA があるリソースの場所に展開します。SSO は、1 つまたは複数の FAS サーバーが接続するリソースの場所でのみアクティブになります。

複数のリソースの場所に接続された **FAS** サーバー

リソースの場所間にネットワーク接続があり、似たインフラストラクチャがそれらに含まれている場合、FAS サーバーを複数のリソースの場所に接続できます。SSO は、これらのリソースの場所にあるアプリおよびデスクトップに接続するワークスペース利用者が利用できます。このシナリオでは、個別の FAS サーバーを各リソースの場所に接続する必要はありません。

利用者が仮想アプリまたは仮想デスクトップを起動すると、Citrix Cloud は起動中の仮想アプリまたは仮想デスクトップと同じリソースの場所にある FAS サーバーを選択します。Citrix Cloud は、選択した FAS サーバーに接続して、FAS サーバーに保存されているユーザー証明書へのアクセスを許可するチケットを取得します。利用者を認証するため、VDA は FAS サーバーに接続してチケットを提供します。

適切なルール構成を使用して、オンプレミスと Citrix Cloud の両方に同じ FAS サーバーを使用できます。



複数のリソースの場所のフェイルオーバー優先度

複数のリソースの場所で FAS サーバーを使用する場合、1 つのリソースの場所にある FAS サーバーは、他のリソースの場所にある FAS サーバーにフェイルオーバーを提供できます。FAS サーバーを他のリソースの場所に追加するときは、各サーバーをプライマリまたはセカンダリとして指定します。利用者が仮想アプリまたは仮想デスクトップを起動すると、Citrix Cloud は次の方法で FAS サーバーを選択します：

- 指定されたリソースの場所でプライマリとして指定されている FAS サーバーが最初に考慮されます。
- 使用可能なプライマリサーバーがない場合は、セカンダリとして指定されている FAS サーバーが考慮されません。
- 使用可能なセカンダリサーバーがない場合、起動は続行されますが、シングルサインオンは発生しません。

ビデオの概要

Citrix Workspace 向けのフェデレーション認証サービスの概要については、この Tech Insight のビデオをご覧ください：



要件

接続の要件

FAS 管理コンソールを使用して、FAS サーバーを Citrix Cloud に接続します。このコンソールで、ローカルまたはリモートの FAS サーバーを構成できます。FAS を使用したワークスペースの SSO を有効にするには、FAS 管理コンソールと FAS サービスが、それぞれコンソールユーザーのアカウントとネットワークサービスアカウントを使用して、次のアドレスにアクセスします。

- コンソールユーザーのアカウントを使用した FAS 管理コンソール
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - サードパーティの ID プロバイダーが必要とするアドレス（環境で使用されている場合）
- ネットワークサービスアカウントを使用した FAS サービス:
 - *.citrixworkspacesapi.net
 - https://*.citrixnetworkapi.net/

環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが環境に応じて適切に構成されていることを確認してください。

FAS システム要件

このセクションの要件は、Citrix Cloud に接続する予定のすべての FAS サーバーに適用されます。

FAS サーバーの完全なシステム要件については、FAS 製品ドキュメントの「[システム要件](#)」セクションを参照してください。

オンプレミスの Citrix Virtual Apps and Desktops 環境の FAS サーバーには、フェデレーション認証サービス 2003（バージョン 10.1）以降がインストールされている必要があります。

既存の FAS サーバーがバージョン 10 よりも古い場合、Citrix から最新の FAS ソフトウェアをダウンロードし、この接続を作成する前にサーバーをインプレースでアップグレードできます。接続の作成時に、FAS サーバーのリソースの場所を選択します。SSO は、FAS サーバーが存在するリソースの場所でのみ利用者に対してアクティブになります。

既存の FAS サーバーのアップグレードについて詳しくは、FAS 製品ドキュメントの「[インストールと構成](#)」を参照してください。同じ FAS サーバーを Workspace とオンプレミスの展開に使用できます。

Citrix Workspace

Workspace で Citrix DaaS をプロビジョニングおよび有効化しておく必要があります。デフォルトでは、DaaS は、サービスへのサブスクリプション後に Workspace 構成で有効になります。ただし、このサービスでは、Citrix Cloud がオンプレミス環境と通信できるように、Citrix Cloud Connector を展開する必要があります。

Cloud Connector

Citrix Cloud Connector は、リソースの場所 (VDA がある場所) と Citrix Cloud との間の通信を可能にします。高可用性を確保するために、少なくとも 2 つの Cloud Connector を展開します。Cloud Connector ソフトウェアをインストールするサーバーは、次の要件を満たす必要があります：

- 「[Cloud Connector の技術詳細](#)」に記載されているシステム要件
- 他の Citrix コンポーネントがインストールされておらず、サーバーが Active Directory ドメインコントローラーではなく、リソースの場所のインフラストラクチャに不可欠なマシンでもない。
- VDA があるドメインに参加している。

Cloud Connector の展開について詳しくは、以下の記事を参照してください：

- [Cloud Connector のプロキシとファイアウォールの構成](#)
- [Cloud Connector のインストール](#)

セットアップの概要

1. 新しい FAS サーバーを展開する場合は、「要件」を確認し、本記事の「FAS のインストールと構成」の指示に従ってください。
2. 本記事の「FAS サーバーの Citrix Cloud への接続」の説明に従って、FAS サーバーを Citrix Cloud に接続します。このタスクを完了すると、FAS サーバーが単一のリソースの場所に接続されます。
3. FAS サーバーを複数のリソースの場所に接続する場合は、本記事の「FAS サーバーを複数のリソースの場所に追加する」で説明されている手順に従います。

FAS のインストールと構成

[FAS 製品ドキュメント](#)で説明されている FAS のインストールおよび構成プロセスに従います。StoreFront と Delivery Controller の構成手順は不要です。

ヒント：

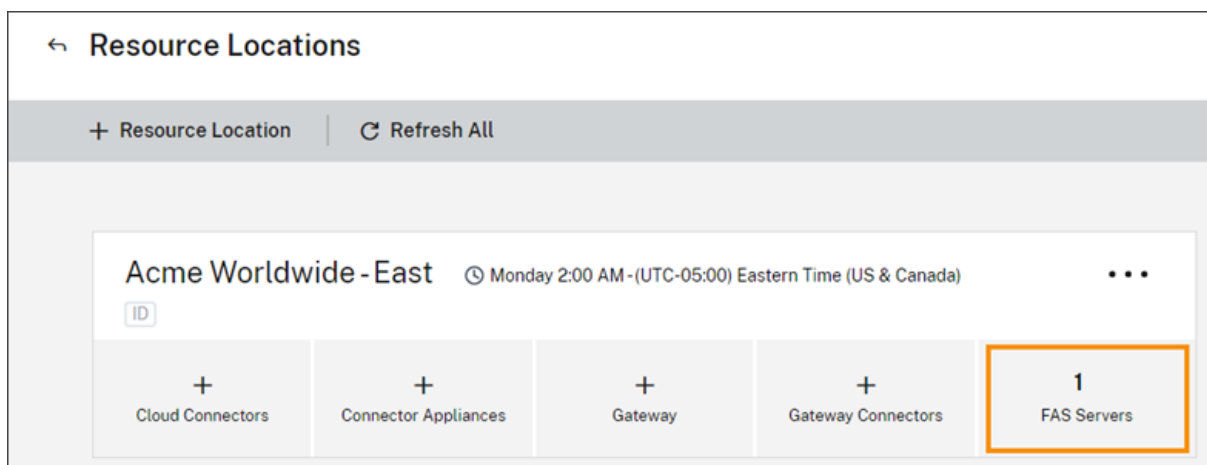
フェデレーション認証サービスインストーラーは Citrix Cloud コンソールからもダウンロードできます：

1. Citrix Cloud メニューから [リソースの場所] を選択します。
2. [FAS サーバー] タイルを選択し、[ダウンロード] をクリックします。

FAS サーバーを Citrix Cloud に接続する

FAS 製品ドキュメントの「[インストールと構成](#)」で説明されているとおり、FAS 管理コンソールを使用して FAS サーバーを Citrix Cloud に接続します。

Citrix Cloud に接続するための構成手順が完了すると、Citrix Cloud で FAS サーバーが登録され、Citrix Cloud アカウントの [リソースの場所] ページに表示されます。



Web ブラウザーに [リソースの場所] ページが既にロードされている場合は、ページを更新して登録済みの FAS サーバーを表示します。

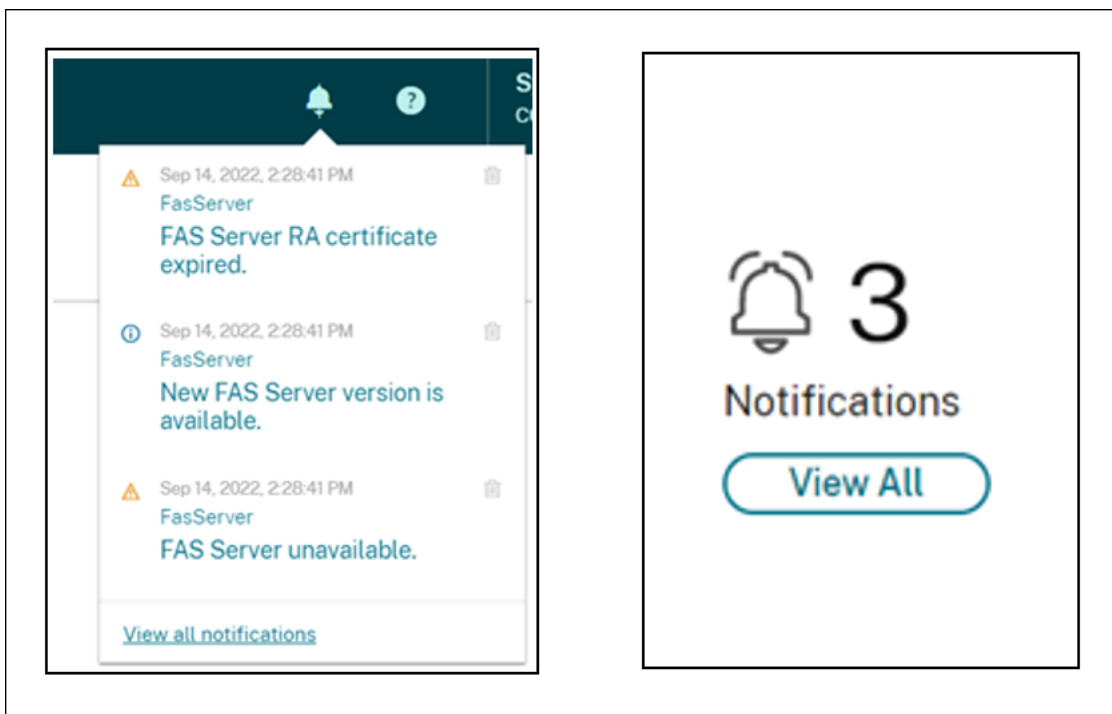
Cloud 通知のサポート

FAS は Cloud 通知をサポートするようになりました。FAS サーバーの新しい Cloud 通知では、次の場合に通知を受信します：

- FAS サーバーがダウンしているか使用できない。
- FAS サーバーの登録機関（RA）証明書の有効期限が切れているか、期限切れ間近である。
- 新しいバージョンの FAS がダウンロード可能である。

通知の発生

Citrix Cloud 管理コンソールで新しい通知がないかどうか定期的にチェックされ、あれば通知が行われます。通知は、Citrix Cloud 管理コンソールの右上隅にあるベルアイコンの下に表示されます。通知アイコンで [すべて表示] を選択して、すべての通知を表示します。詳しくは、「[通知](#)」を参照してください。



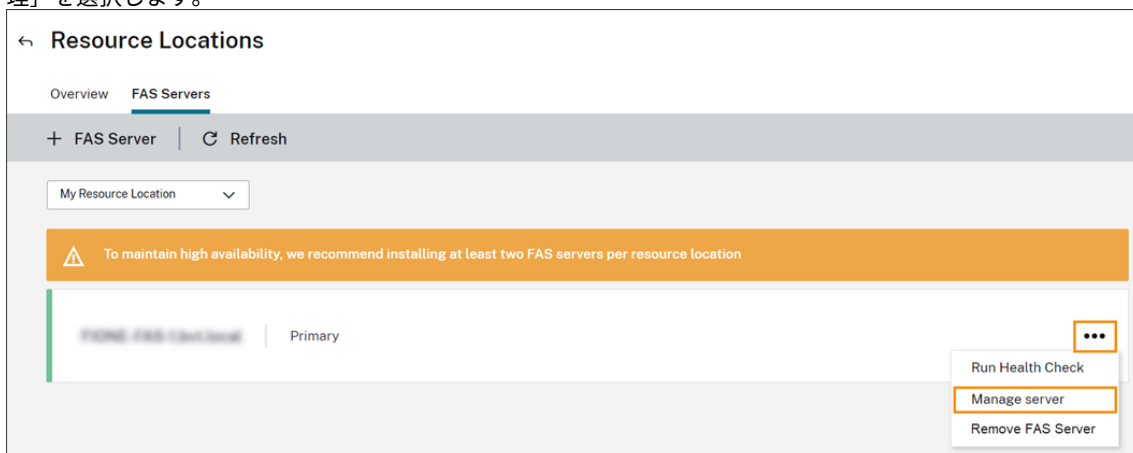
注:

通知が行われた場合、問題が解決されなかったときにのみ、定期的に再度通知が行われます。

すべての通知に、影響を受けた FAS サーバーの完全修飾ドメイン名が含まれます。RA 証明書の有効期限切れ通知は、バージョン 10.10.0.14 以降の FAS サーバーに関してのみ表示されます。

FAS サーバーを複数のリソースの場所に追加する

1. Citrix Cloud メニューの [リソースの場所] を選択してから、[FAS サーバー] タブを選択します。
2. 管理する FAS サーバーを見つけ、エントリの右側にある省略記号 (...) をクリックしてから、[サーバーの管理] を選択します。



3. [リソースの場所に追加] を選択してから、必要なリソースの場所を選択します。

Manage FAS Server ✕

Add or remove the FAS server in an existing resource location or change the FAS server's failover ranking.

Connected resource locations:

My Resource Location	Primary	✕
Resource Location 3	Secondary	✕

+ Add to a resource location

Cancel **Save Changes**

4. 選択した各リソースの場所で、FAS サーバーのフェイルオーバー優先度として [プライマリ] または [セカンダリ] を選択します。
5. [**Save Changes**] を選択します。

追加した FAS サーバーを表示するには、**Citrix Cloud** メニューの [リソースの場所] を選択してから、[FAS サーバー] タブを選択します。接続されているすべてのリソースの場所の全 FAS サーバー一覧が表示されます。特定のリソースの場所の FAS サーバーを表示するには、ドロップダウンリストからリソースの場所を選択します。

FAS サーバーのフェイルオーバー優先度を変更する

1. [リソースの場所] ページから、管理するリソースの場所の [**FAS サーバー**] タイルを選択します。
2. [**FAS サーバー**] タブを選択します。
3. 管理する FAS サーバーを見つけ、エントリの右側にある省略記号 (...) をクリックしてから、[サーバーの管理] を選択します。
4. 変更する優先度付きのリソースの場所を見つけて、ドロップダウンリストから新しい優先度を選択します。

Manage FAS Server ✕

Add or remove the FAS server in an existing resource location or change the FAS server's failover ranking.

Connected resource locations:

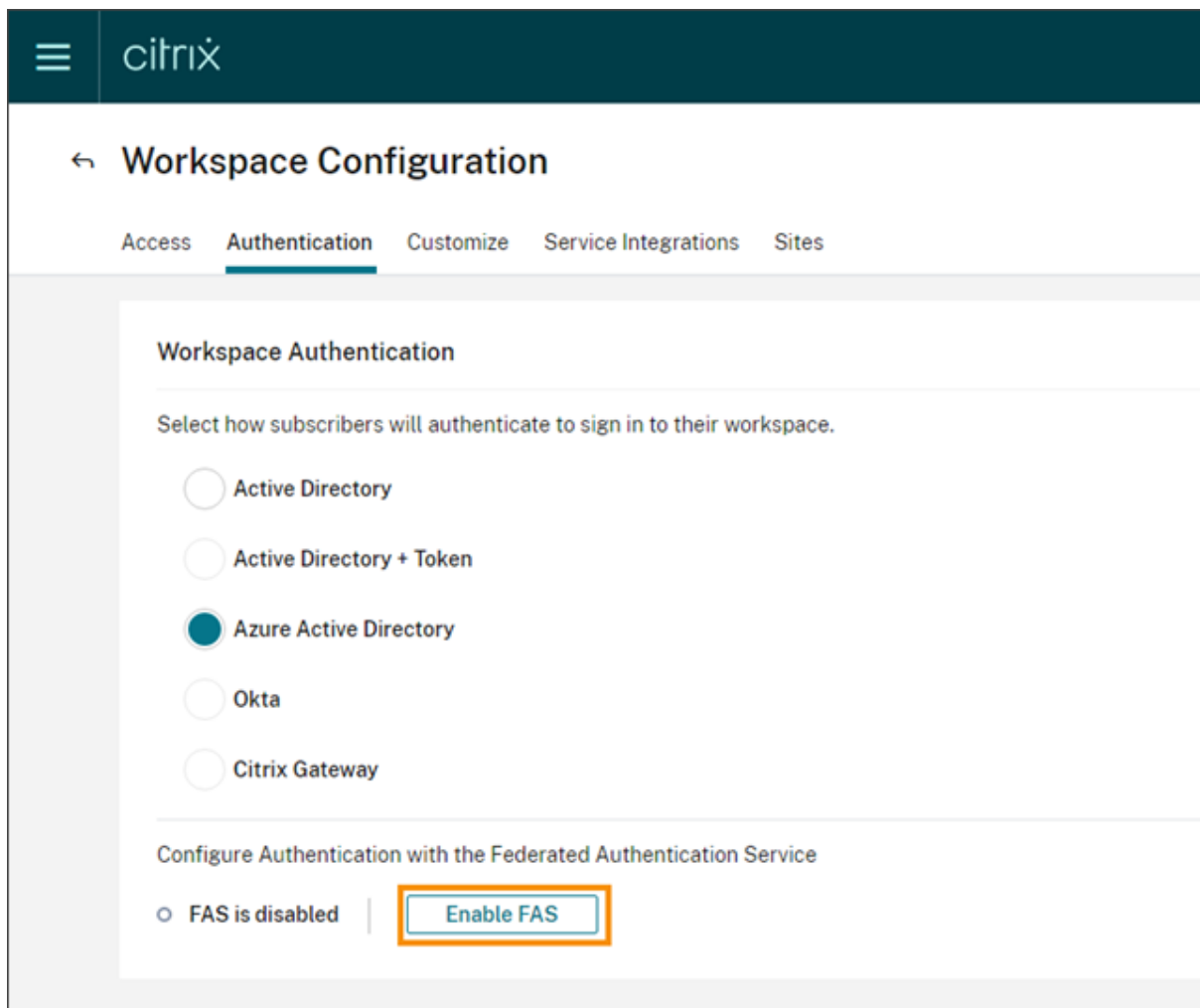
My Resource Location	Primary ▼	✕
Resource Location 3	Secondary ▼	✕

[+ Add to a resource location](#)

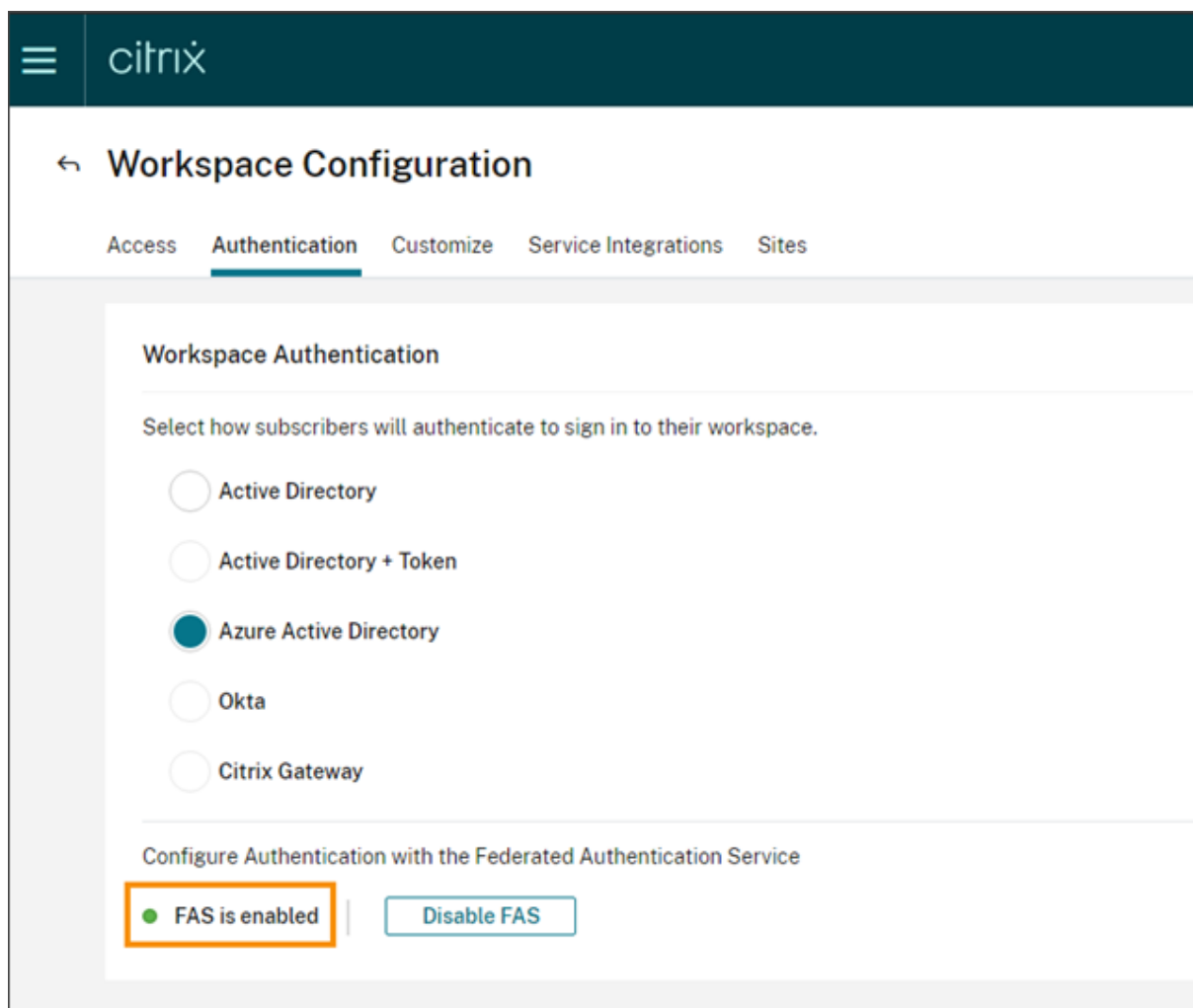
5. **[Save Changes]** を選択します。

ワークスペースのフェデレーション認証を有効にする

1. Citrix Cloud メニューから [ワークスペース構成] を選択し、[認証] を選択します。
2. **[FAS を有効にする]** をクリックします。この変更が利用者のセッションに適用されるまで、最大 5 分かかる場合があります。



その後、Citrix Workspace からのすべての仮想アプリおよびデスクトップの起動に対してフェデレーション認証がアクティブになります。



利用者が自分のワークスペースにログインして、FAS サーバーと同じリソースの場所で仮想アプリまたはデスクトップを起動すると、アプリまたはデスクトップは資格情報のプロンプトを表示せずに起動します。

注:

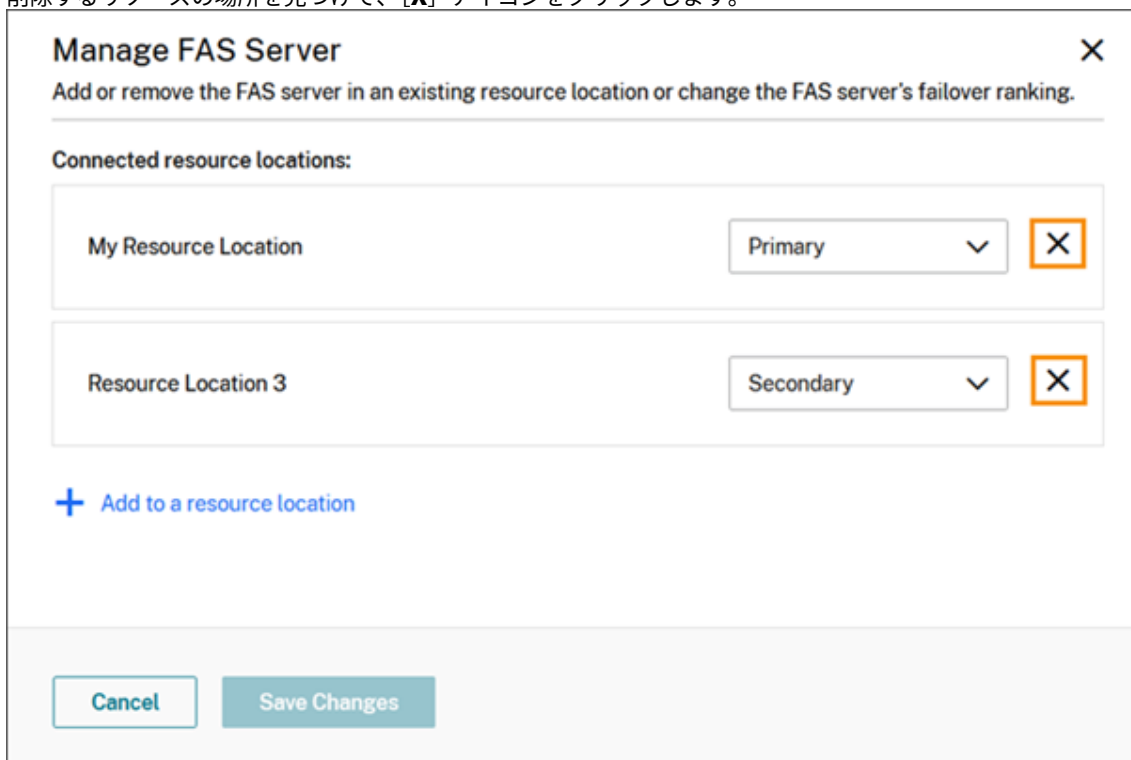
リソースの場所内のすべての FAS サーバーがダウンしているか、またはメンテナンスモードの場合、アプリケーションの起動は成功しますが、シングルサインオンはアクティブになりません。利用者は、各アプリケーションまたはデスクトップにアクセスするために Active Directory 資格情報の入力を求められます。

FAS サーバーの削除

単一のリソースの場所から FAS サーバーを削除するには:

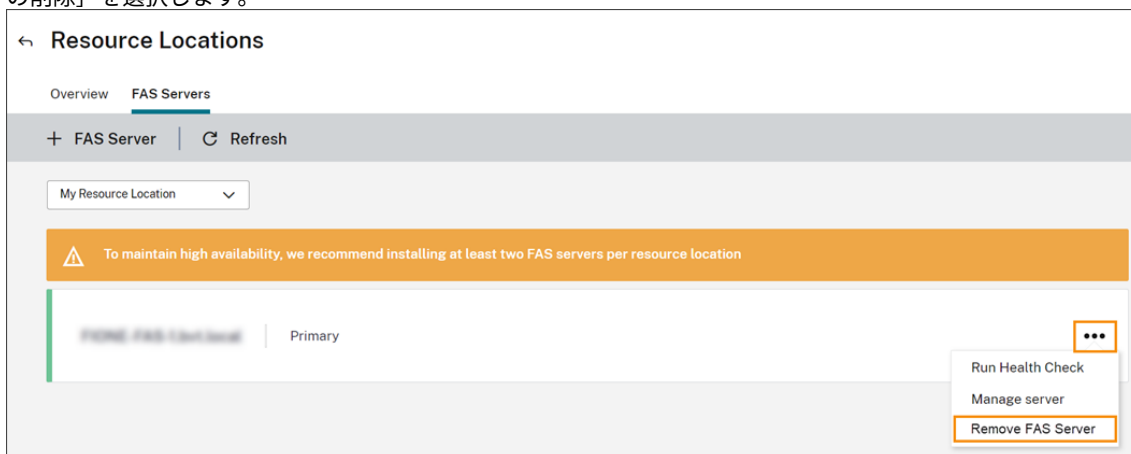
1. [リソースの場所] ページから、管理するリソースの場所の **[FAS サーバー]** タイルを選択します。
2. **[FAS サーバー]** タブを選択します。
3. 管理する FAS サーバーを見つけ、エントリの右側にある省略記号 (...) をクリックしてから、[サーバーの管理] を選択します。

4. 削除するリソースの場所を見つけて、[X] アイコンをクリックします。

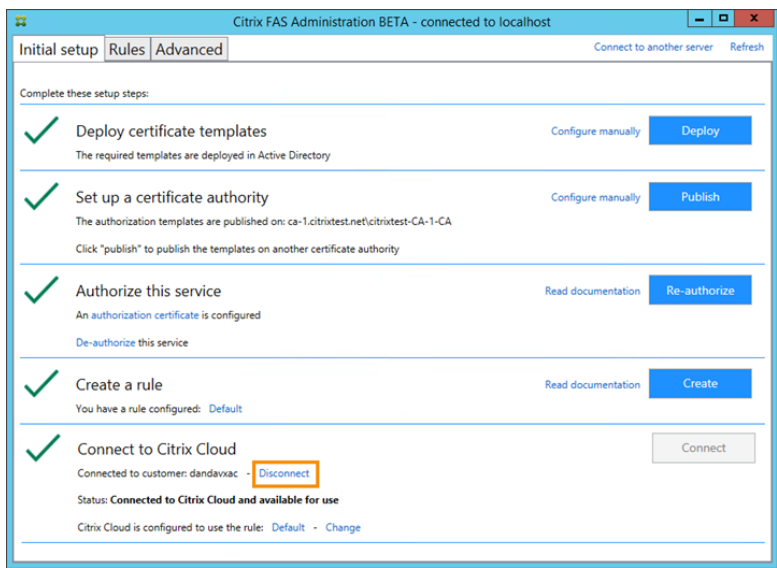


接続されたすべてのリソースの場所から FAS サーバーを削除するには:

1. Citrix Cloud メニューから [リソースの場所] を選択します。
2. 管理するリソースの場所を指定して [FAS サーバー] タイルを選択します。
3. 削除する FAS サーバーを見つけ、エントリの右側にある省略記号 (...) をクリックしてから、[FAS サーバーの削除] を選択します。

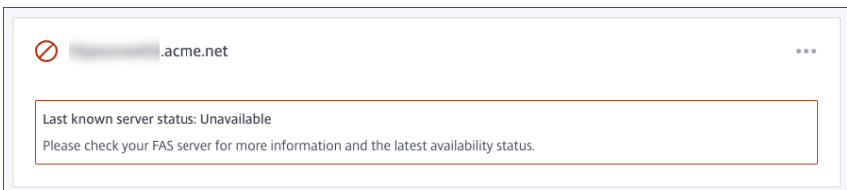


4. FAS 管理コンソール (オンプレミスの FAS サーバー上) の [Connect to Citrix Cloud] で [Disconnect] を選択します。また、FAS をアンインストールすることもできます。

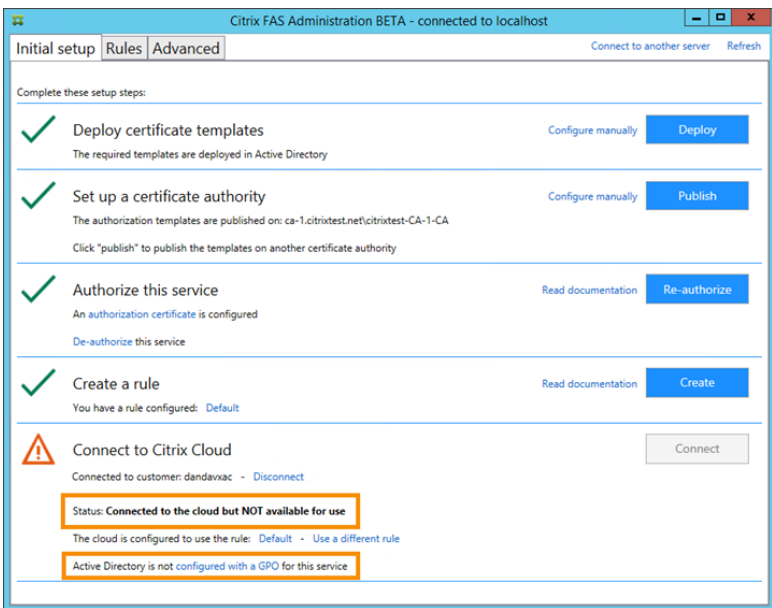


トラブルシューティング

FAS サーバーが利用できない場合、FAS サーバーページに警告メッセージが表示されます。



問題を診断するには、オンプレミスの FAS サーバーで FAS 管理コンソールを開き、状態を確認します。たとえば、FAS サーバーが FAS サーバーの GPO に存在しない場合：



サーバーが正常に動作していることを FAS 管理コンソールが示していても、VDA ログオンの問題が解決しない場合は、「[FAS トラブルシューティングガイド](#)」を確認してください。

追加情報

[Workspace アプリへのシングルサインオンの構成](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).