シトリックス クラウド™

注記:

Citrix Virtual Apps EssentialsおよびCitrix Virtual Desktops Essentialsは、販売終了およびサポート終了となりました。詳細については、CTX583004を参照してください。

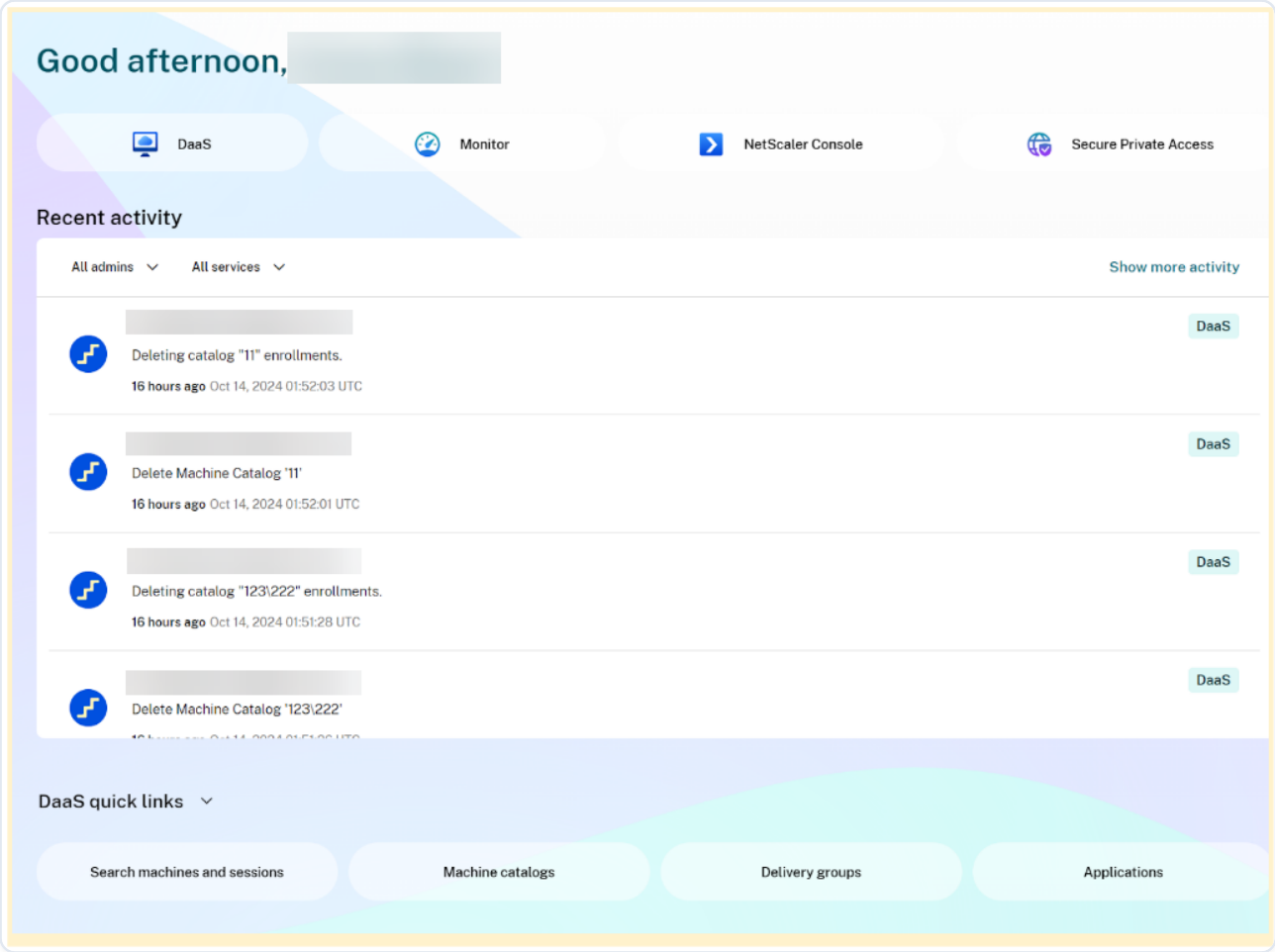
Citrix Cloudは、Citrixクラウドサービスをホストおよび管理するプラットフォームです。選択した任意のクラウドまたはインフラストラクチャ（オンプレミス、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド）上のコネクタを介して、リソースに接続します。単一のコンソールから、アプリとデータを含むストアを作成、管理し、エンドユーザーに展開できます。

Citrix Cloudを体験する

1つ以上のCitrix Cloudサービスについて、概念実証で完全な本番環境を体験してください。Citrix Cloudにサインアップした後、コンソール内で直接サービス試用版をリクエストできます。試用期間が終了したら、すべての構成を保持したまま本番環境に変換できます。詳細については、Citrix Cloud Service Trialsを参照してください。

新しいモダンなCitrix Cloud™ホームページと統合されたナビゲーションエクスペリエンス

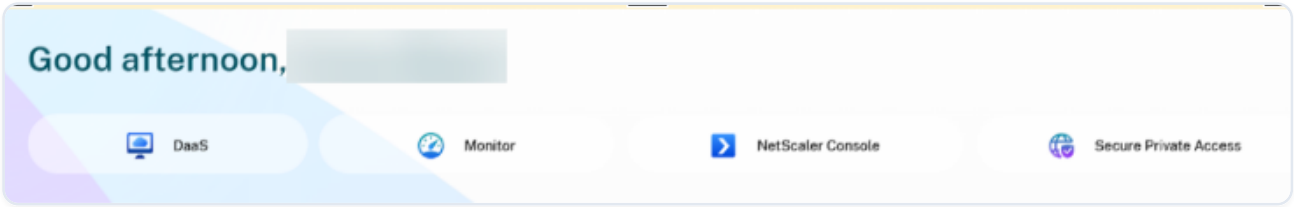
Citrix Platformの導入により、ゼロトラストアクセス、クラス最高のアプリおよびデスクトップ仮想化、包括的なセキュリティを備えた高性能なアプリケーション配信を提供する、簡素化された統合プラットフォームを提供することをお約束しました。 このコミットメントの一環として、管理者が環境を管理および操作する方法を向上させるために、新しく再設計されたCitrix Cloudホームページと統合されたナビゲーションエクスペリエンスが導入されています。



主な機能

- 運用効率
  - 主要サービスに直接アクセス
  - 最近のアクティビティを一目で確認
  - 製品内のアクションへのクイックリンク
- 学習ハブ
  - Citrix ロードマップ
  - 今後のイベント
  - トレーニング、コミュニティリソース、技術ドキュメントへのクイックリンク
- 改善されたナビゲーション
  - すべてのCitrixソリューションで一貫したルックアンドフィール
  - パンくずリストとページパスによるシンプルなナビゲーション
  - ピン留めなどのカスタマイズ可能な機能

サービスアクセス



これらのオプションを通じて、すべての主要サービスにアクセスできます。

- DaaS
- モニター
- NetScaler® コンソール
- セキュアプライベートアクセス

> **注:**
>
> 左上隅のワッフルメニューを使用して、追加のサービスにアクセスできます。

最近のアクティビティ

最近のアクティビティ(/en-us/citrix-cloud/media/recent-activity.png)

最近のアクティビティには、DaaS、NetScaler Console、Secure Private Access、Citrix Cloudなどのサービス全体で行われた構成変更が表示され、概要をすばやく確認できます。アクティビティをサービスでフィルタリングし、すべての管理者または自分自身のみが行った変更を表示するように選択できます。ウィジェットの右上にある を選択すると、最大100個のログを表示できます。詳細については、サービスをクリックして詳細ログを取得してください。

すべてのサービス(/en-us/citrix-cloud/media/all-services.png)

クイックリンク

クイックリンク(/en-us/citrix-cloud/media/quick-links.png)

クイックリンクは、より効率的に作業できるように設計されており、クリック数を減らして特定のサービスセクションに直接移動できます。アクセスしたいサービス（**DaaS**、**NetScaler Console**、または**Secure Private Access**など）のクイックリンクを選択します。

プラットフォームロードマップ

すべてのカテゴリ(/en-us/citrix-cloud/media/all-categories.png)

現在進行中、リリース中、テクニカルプレビュー中、または一般提供 (GA) 中のすべての項目を確認します。プロビジョニング、セキュアプライベートアクセスなどのカテゴリ、および/またはリリースステータスでフィルタリングできます。完全なリストを表示するには、 をクリックします。

すべてのステータス(/en-us/citrix-cloud/media/all-statuses.png)

今後のイベント

最新のイベントを常に把握し、**すべて表示**をクリックして完全なリストにアクセスしてください。これにより、Citrix Communityページ、Citrix Eventsに移動します。

リソース

プラットフォームを最大限に活用するために役立つ重要なリソースを以下に示します。

- **Citrix Community**: ディスカッションフォーラム、ビデオ、今後のイベントにアクセスできます。
- **トレーニング**: Pluralsightコースを含む包括的なトレーニングリソースを見つけることができます。
- **自動化**: プラットフォーム全体でSDK、REST API、移行ツールなどを探索できます。
- **Techwire**: 更新情報や主要なリリース機能を紹介する月刊プラットフォームニュースレターです。

これらの更新により、Citrix Cloudは完全に統合された高性能なエクスペリエンスを提供し、アクセシビリティ、ユーザビリティ、生産性の新しい標準を確立します。

フィードバック

画面右上の**Submit Feedback**をクリックして、バグ、機能強化、全体的な満足度に関するフィードバックを共有してください。

フィードバックを送信(/en-us/citrix-cloud/media/feedback.png)

Citrix Cloudサービスドキュメント

Citrix Cloudサービスのセットアップまたは管理に関する情報をお探しですか？Citrix Cloud Servicesにアクセスして、すべてのクラウドサービスの製品ドキュメントへのリンクを見つけてください。

アーキテクチャおよび展開リソース

Citrix Tech Zoneには、Citrix Cloudおよびその他のCitrix製品について詳しく学ぶのに役立つ豊富な情報が含まれています。ここでは、Citrixテクノロジーの設計、構築、展開に関する洞察を提供するリファレンスアーキテクチャ、図、技術文書を見つけることができます。

Citrix Cloudの主要なサービスコンポーネントの詳細については、以下のリソースを参照してください。

- Citrix® StoreFront Cloudの概念図: ID、ストアインテリジェンス、シングルサインオンなどの主要な領域の概要を提供します。
- リファレンスアーキテクチャ: ユースケース、推奨事項、関連リソースなど、StoreFront Cloudの実装を計画するための包括的なガイドを提供します。
- Citrix DaaSリファレンスアーキテクチャ：関連サービスとともにCitrix DaaS（旧Virtual Apps and Desktopsサービス）を展開するための詳細なガイダンスを提供します。

教育リソース

Citrix Cloudラーニングシリーズポータルは、Citrix Cloudとそのサービスを使い始めるための教育モジュールを提供しています。概要からサービスの計画、構築まで、すべてのモジュールを順を追って学習できます。以下のコースでクラウドジャーニーを始めましょう。

- Citrix Cloudの基礎
- 「Citrix Identityおよび認証の概要」(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/connect-azure-ad.html)

Citrix Educationビデオライブラリでは、Citrix Cloudサービスで使用する主要な展開タスクとコンポーネントのトラブルシューティングについて説明するオンラインビデオレッスンを提供しています。Cloud Connectorのインストールや VDAの登録などのタスク、およびこれらのコンポーネントのトラブルシューティングについて詳しく学びましょう。

Citrix Cloud™ の新機能

この記事では、Citrix Cloud リリースにおける新機能、機能強化、および修正について説明します。

2026年5月

- **Citrix Platform Flex のライセンス**. Citrix Platform Flex は、クラウド間でデジタルストアとプラットフォームサービスを安全、回復力があり、柔軟に提供するように設計された、管理されたクラウド提供プラットフォームです。詳細については、以下を参照してください。
  - Citrix Platform Flex のライセンス
  - Flex Credit の消費とレポート

2026年4月

- **コンソールでの非アクティブタイムアウトの構成**. フルアクセス管理者 は、Citrix Cloud コンソールでの非アクティブ状態の期間を構成できるようになりました。この期間が経過すると、管理者は自動的にサインアウトされます。構成可能な非アクティブタイムアウトは10分から12時間までで、デフォルトは60分です。詳細については、システム要件と接続要件を参照してください。
- **条件付き認証の機能強化**. 条件付き認証は、追加のIDプロバイダーとポリシー条件をサポートするようになりました。詳細については、条件付き認証を参照してください。

2026年1月

- **ゲストおよびB2B ID向けのEntra IDを使用したSAML**. Citrix Cloud は、SAMLプロバイダーとしてEntra IDを使用して、ゲストおよびB2BユーザーIDのストア認証をサポートするようになりました。詳細については、ストア認証用のゲストおよびB2B ID向けのEntra IDを使用したSAMLを参照してください。

2024年12月

- **条件付き認証**. Citrix Cloud は条件付き認証をサポートするようになり、管理者はコンテキストに応じたアクセス ポリシーを適用できるようになりました。詳細については、条件付き認証を参照してください。

2024年9月

- **パートナー向けの新規顧客のオンボーディング**. Citrix パートナーは、Citrix Cloud コンソールから直接新規顧客をオンボーディングできるようになりました。詳細については、新規顧客のオンボーディングを参照してください。
- **アカウント管理の更新**。アカウント管理のライセンス管理セクションが更新されました。詳細については、「アカウント管理」を参照してください。

2024年6月

- **ゲストおよびB2B ID向けのMicrosoft Entra IDを使用したSAML**。Citrix Cloudは、ゲストおよびB2Bユーザー IDのストア認証をサポートするようになりました。詳細については、「ストア認証用のゲストおよびB2B ID向けMicrosoft Entra IDを使用したSAML」を参照してください。

2024年4月

- **SAML署名証明書**。サービスプロバイダーとIDプロバイダーの両方のSAML署名証明書を更新できるようになりました。詳細については、以下を参照してください。
  - サービスプロバイダーSAML署名証明書の更新
  - IDプロバイダーSAML署名証明書の更新

2024年3月

- **カスタムランディングページ**。管理者は、Citrix Cloudのカスタムランディングページを設定できるようになりました。詳細については、「カスタムランディングページ」を参照してください。
- **PingFederateを使用したSAML**。Citrix Cloudは、オンプレミスのPingFederateサーバーをSAMLプロバイダーとして構成することをサポートするようになりました。詳細については、「PingFederateを使用したSAML」を参照してください。

2024年1月

- **Citrix IDプロバイダーのサポート**。Identity and Access ManagementにCitrix IDプロバイダーのサポートが追加されました。詳細については、「Identity and Access Management」を参照してください。
- **新しいサービスとしてのLicense Usage Insights**。License Usage Insightsが、サポートされているサービスで新しいサービスとして利用可能になりました。

サービスレベルアグリーメント

発効日: October 30, 2020

Citrix Cloud™は、高いサービス可用性を実現するために、業界のベストプラクティスを使用して設計されています。

> **注:**

- Citrix Cloud GovernmentのSLAについては、「サービスレベルアグリーメント」を参照してください。
- Citrix Platform FlexのSLAについては、「サービスレベルアグリーメント」を参照してください。

このサービスレベルアグリーメント（SLA）は、Citrix Cloudサービスの可用性に関するCitrixのコミットメントを記述しています。このSLAは、対象となるサービス（「サービス」）に関するCloud Software Groupのエンドユーザー契約（EULA）の一部です。

Citrixのサービスコミットメント（「サービスコミットメント」）は、サービスにおいて少なくとも99.9%の月間稼働時間（「月間稼働時間」）を維持することです。月間稼働時間は、サービスインスタンスが「利用不可」の状態であったサービスのある月の全期間中の時間の割合を100%から差し引くことによって計算されます。サービスとそれぞれの可用性の測定値は、以下の表に記載されています。月間稼働時間の割合の測定値には、以下に起因するダウンタイムは含まれません。

- 定期的にスケジュールされたメンテナンス期間。
- https://docs.citrix.comに記載されているサービスの構成要件を顧客が遵守しなかった場合、または不正な行為、あるいは誤った入力。
- Citrix®が顧客にサービスの使用方法の変更を助言した後、顧客がその変更を行わなかった場合の顧客によるサービスの使用。
- Citrixが管理していないコンポーネントによって引き起こされたもの。これには、顧客が管理する物理マシンおよび仮想マシン、顧客がインストールおよび保守するオペレーティングシステム、顧客がインストールおよび管理するソフトウェア、ネットワーク機器またはその他のハードウェア、顧客が定義および管理するセキュリティ設定、グループポリシーおよびその他の構成ポリシー、パブリッククラウドプロバイダーの障害、インターネットサービスプロバイダーの障害、またはCitrixの管理外にあるその他の顧客サポート要因が含まれますが、これらに限定されません。
- 顧客の従業員、代理人、請負業者、またはベンダー、または顧客のパスワードや機器を介してアクセスを得た者、あるいは顧客が適切なセキュリティ対策を講じなかったことに起因するもの。
- 顧客がサービスエンタイトルメントを超える操作を実行しようとした場合。
- 不可抗力によるサービスの中断。これには、自然災害、戦争またはテロ行為、政府の措置が含まれますが、これらに限定されません。

Citrixのトライアル、テクニカルプレビュー、ラボ、またはベータサービスには、サービスコミットメントは提供されません。

Citrixは、次の条件を満たすお客様にサービスコミットメントを提供します。

- 期間ベースのサブスクリプション (最低1年間のサブスクリプション期間) を利用してサービスを購入している。
- クレーム期間中、サービスに適用されるライセンスモデルに従って、少なくとも100ユニットのサブスクリプション (Citrix Service Providerの場合は最低1,000ユニット) を保有している。

Citrix Service Providers (CSPs) は October 1, 2018 より対象となります。

サービスごとの可用性測定基準

サービス	月間稼働時間の測定基準
シトリックス アナリティクス フォー パフォーマンス™	ユーザーがアプリとデスクトップのパフォーマンスにアクセスし、向上できる時間。
シトリックス アナリティクス フォー セキュリティ™	ユーザーがユーザーアクセスとアクティビティのリスクを検出および軽減できる時間。
NetScaler® Consoleサービス	すべてのPOPでサービスが利用可能である平均時間。
シトリックス エンドポイント マネジメント™	ユーザーがサービスを通じてCitrixが提供するモバイルアプリや登録済みデバイスにアクセスできる時間。
HDX™ Proxy 向け Citrix Gateway サービス	ユーザーがサービスを通じてアプリまたはデスクトップセッションにアクセスできる時間。
NetScaler SD-WAN オーケストレーター	ユーザーがサービスを通じてSD-WAN Orchestratorアカウントにアクセスし、SD-WANネットワークを管理できる時間。
Citrix セキュア プライベート アクセス™	ユーザーがサービスを通じてSaaSまたは社内Webアプリにアクセスできる時間。
シトリックス DaaS™	ユーザーがサービスを通じてアプリまたはデスクトップセッションにアクセスできる時間。
シトリックス® ストアフロント クラウド	コンポーネントサービスについては上記と同様ですが、各サービスの可用性を含みます。請

サービス	月間稼働時間の測定基準
	求がすべてのコンポーネントに満たない場合、クレジットは日割り計算されることがあります。
ライセンス アクティベーション サービス (LAS)	お客様が製品アクティベーションを利用できる時間。

> **注:**
>
> Citrix DaaS は、Citrix Virtual Apps サービス、Citrix Virtual Desktops サービス、および Citrix Virtual Apps and Desktops™ サービスの新しい名称です。

サービスコミットメントと救済措置

SLA発効日以降、Citrixが連続する5ヶ月のうち少なくとも3ヶ月でサービスコミットメントを満たさなかった場合、唯一の救済措置は、Citrixがサービスコミットメントを満たさなかった月に対して、月単位で10%のサービスクレジットが適用されることです。これは、影響を受けたサービスと同じサービス、同じユニット数に対するお客様の次回の年間サービス延長の直近の更新期間に適用されます。

- 月間稼働率: > 99.9%
- サービスクレジット: 該当する月に対して10%割引（お客様にはバウチャーとして提示されます）

上記の救済措置を受けるには、お客様はEULAに準拠している必要があり、クレジット請求が行われる連続する5ヶ月間の最終月の終了から30日以内にお客様が障害を報告する必要があります。このSLAの違反の可能性を報告する手順については、CTX237141を参照してください。

リクエストには、サービスを特定し、利用不能の日付、時刻、期間を定義し、利用不能を裏付けるログまたは記録を添付し、影響を受けたユーザーとその場所、ならびに要求された技術サポートまたは実施された是正措置を特定する必要があります。サービスごとに1つのサービスクレジットのみが発行され、該当する月数に対して、延長期間の全月に対して最大10%のサービスクレジットが1回限り発行されます。お客様は延長購入時にバウチャーを提示する必要があります。

リセラーを通じて延長を購入した場合、リセラーを通じてクレジットを受け取ります。直接購入に適用されるクレジット、または間接購入のためにリセラーに渡されるクレジットは、同じユニット数の延長に対する按分された混合推奨小売価格に基づきます。Citrixは再販価格や再販クレ

ジットを管理しません。クレジットには、Citrixまたはリセラーへの支払いに対する相殺権は含まれません。Citrixはこれらの条件を随時更新します。更新が行われた場合、Citrixはサービスレベルアグリーメントの冒頭にある公開日も改訂します。変更は、現在の公開日以降の新しいサービス購入またはサービス延長にのみ適用されます。

サードパーティ通知

- Citrix Cloud サードパーティ通知 (PDF)
- Citrix Analytics Service サードパーティ通知 (PDF)
- Citrix DaaS サードパーティ通知 (PDF)
- Citrix DaaS Standard for Azure サードパーティ通知 (PDF)
- リモートブラウザ分離 (旧 Secure Browser) (PDF)
- Citrix Endpoint Management サードパーティ通知 (PDF)
- Citrix Cloud Linux VDA Image Service サードパーティ通知 (PDF)
- Connector Appliance for Cloud Services サードパーティ通知 (PDF)
- Citrix Gateway Service サードパーティ通知 (PDF)
- Citrix Device Posture Service サードパーティ通知 (PDF)
- Citrix Secure Private Access サードパーティ通知 (PDF)

> **注:**
>
> Citrix DaaS は、以前は Citrix Virtual Apps and Desktops サービスでした。Citrix DaaS Azure向けスタンダード は、以前は Citrix Virtual Apps and Desktops Azure向けスタンダード でした。

ヘルプとサポートの利用方法

この記事では、Citrix Cloud™ またはその他の Citrix Web サイトでアカウントの作成またはサインイン時に問題が発生した場合のトラブルシューティングとヘルプの利用方法について説明します。この記事には、その他のセルフヘルプリソースとガイド付きサポートオプションも含まれています。

重要:

Citrix Web サイトへのサインインまたは多要素認証 (MFA) への登録で問題が発生した場合は、まずこの記事でトラブルシューティングリソースを確認してください。これらのリソースで問題が解決しない場合は、Citrix カスタマーサービスにhttps://www.citrix.com/contact/customer-service.html からお問い合わせください。

アカウントの作成

Citrix ディスカッションフォーラム、トレーニングコース、特定の製品ダウンロード、Citrix テクニカルサポートなど、Citrix Web サイト上の一部のリソースにアクセスするには、Citrix アカウントが必要です。

会社用の新しい Citrix アカウントを作成するには、以下のいずれかの方法で Citrix にお問い合わせください。

- Citrix カスタマーサービス にお問い合わせください。
- お住まいの地域の Citrix パートナー または Citrix 営業所 にお問い合わせください。

既に Citrix アカウントをお持ちの場合は、Citrix Cloud アカウントの作成 で説明されているタスクを完了することで、Citrix Cloud アカウントを作成し、オンボーディングプロセスを完了できます。

Citrix Cloud のサインアップ時に問題が発生した場合は、Citrix カスタマーサービス にお問い合わせください。

Citrix Web サイトと Citrix Cloud へのサインイン

Citrix アカウントで Citrix Web サイトにサインインできない場合は、以下のリソースを使用してトラブルシューティングを行ってください。

- CTX228792: Citrix Web サイトでのログインに関する問題のトラブルシューティング

MFA を設定できない、または Citrix アカウントへのサインイン時に MFA で認証できない

トラブルシューティング情報については、以下の記事を参照してください。

- CTX461297: 多要素認証 (MFA) への登録方法
- CIX463758: 回復用メールアドレスまたはバックアップコードを使用してCitrix MFAをリセットする方法

MFAでサインインできない場合は、Citrixカスタマーサービス（https://www.citrix.com/contact/customer-service.html）にお問い合わせください。

Citrixアカウントのユーザー名を見つける方法、またはCitrixパスワードをリセットする方法?

Citrixアカウントのユーザー名を確認し、パスワードをリセットするには、以下の手順を使用します。

1. https://www.citrix.com/welcome/request-password.htmlにアクセスします。
2. Citrixアカウントのユーザー名を確認するには：
    a. **「Find my account by」で、「Email」**を選択します。
    b. Citrixアカウントに関連付けられているメールアドレスを入力します。
3. Citrixアカウントのパスワードをリセットするには：
    a. **「Find my account by」で、「User name」**を選択します。
    b. Citrixアカウントのユーザー名を入力します。
4. **「Find my account」**をクリックします。

Citrixがメールアドレスを使用してアカウントを見つけた場合、Citrixはあなたのメールアドレスに関連付けられているユーザー名と会社名が記載されたメールを送信します。CitrixがCitrixユーザー名を使用してアカウントを見つけた場合、Citrixはパスワードをリセットするための指示が記載されたメールを送信します。

数分経ってもメールが届かない場合は、この記事のCitrix メールがメール受信トレイに表示されないを参照してください。

Citrix Cloud にサインインできません

- 正しいアカウント資格情報でサインインしていることを確認してください。アカウントのユーザー名を確認するには、https://citrix.cloud.com/にアクセスし、**ユーザー名を忘れましたか？**を選択して、メールアドレスを入力します。Citrix からアカウントのユーザー名が記載されたメールが送信されます。
- パスワードをリセットする必要がある場合があります。最近サインインしていない場合や、パスワードが十分に強力でない場合、Citrix Cloud はパスワードの変更を促します。詳細については、この記事のパスワードの変更を参照してください。
- カスタムサインイン URL を使用してサインインする必要がある場合があります。Citrix Cloud アカウントが管理者の認証にMicrosoft Entra ID、Google Cloud Identity、またはSAMLを使用している場合は、**会社の資格情報でサインイン**を選択し、会社のサインイン URL を入力します。その後、会社の資格情報を入力して、会社の Citrix Cloud アカウントにアクセスできます。会社のサインイン URL がわからない場合は、会社の管理者に問い合わせてください。

それでも Citrix Cloud にサインインできない場合は、Citrix カスタマーサービスにお問い合わせください。

Citrix からのメールがメール受信トレイに表示されない

Citrix が MFA の本人確認、Citrix アカウントの検索、またはパスワードの変更のためにメールを送信する場合、通常、メールは数分以内に届きます。これらのメールが届かない場合は、次の点を確認してください。

- Citrix アカウントに登録されているメールアドレスを確認し、それが正しいことを確認してください。最近メールアドレスを変更した場合、確認メールは古いアドレスに送信されている可能性があります。
- メールが誤ってフィルタリングされた可能性があります。メールクライアントの迷惑メールフォルダとゴミ箱フォルダを確認してください。また、`donotreplynotifications@citrix.com`または`cloud@citrix.com`からのメールをメールアカウントで検索することもできます。
- ファイアウォールがメールをブロックした可能性があります。以下のメールアドレスが信頼できる送信者としてリストされていることを確認してください。
  - `donotreplynotifications@citrix.com`
  - `cloud@citrix.com`

- `CustomerService@citrix.com`

数分経ってもメールが届かない場合、またはサインインに関して別の問題が発生した場合は、Citrix カスタマーサービスにお問い合わせください。

CitrixおよびCitrix Cloudアカウントの多要素認証

Citrixのお客様は、MFAを使用してCitrixアカウントおよびCitrix Cloudにサインインする必要があります。MFAへの登録は、次の場合に行われます。

- 新規のお客様がCitrixアカウントに初めてサインインする場合。
- Citrixのお客様が新しいCitrix Cloudアカウントをオンボードする(/ja-jp/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html)が、まだMFAに登録していない場合。
- 新しい管理者が既存のCitrix Cloudアカウントに参加する(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html)。

CitrixアカウントまたはCitrix Cloudにサインインする際にMFAへの登録を求められた場合は、CTX461297: 多要素認証 (MFA) への登録方法の手順に従ってください。

CitrixアカウントのMFAの詳細については、CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix propertiesを参照してください。

アカウントの回復

Citrixアカウントの資格情報の回復が必要な場合は、この記事の(#how-do-i-find-my-citrix-account-user-name-or-reset-my-citrix-password)を参照してください。

Citrix Cloudアカウントへのアクセスを回復する必要がある場合は、MFAに登録したときに構成した回復方法を使用できます。これらの回復方法には、次のものがあります。

- Citrixが回復用メールアドレスに送信するワンタイムコード。
- MFA登録時に生成したリストからのバックアップコード。
- Citrixサポートから回復用電話番号への電話で、本人確認を行い、アカウントへのアクセスを支援します。回復用電話番号の設定は、MFA登録時に必須です。

回復方法でサインインするには：

1. CitrixアカウントまたはCitrix Cloudのサインインページから、ユーザー名とパスワードを入力し、**サインイン**を選択します。

2. プライマリMFA方式からのコードを求められたら、**回復方法を使用**を選択します。

   「認証アプリをお持ちでない場合」がハイライト表示された検証プロンプト(/en-us/citrix-cloud/media/admin-mfa-no-auth-app.png)

3. 適用可能な場合は、使用したい回復方法を選択します。回復用電話番号以外に設定されている回復方法が1つしかない場合、Citrixはその方法を自動的に使用するよう促します。
4. 回復用メールアドレスを使用する場合は、Citrixから送信されたワンタイムコードを入力し、**確認**を選択します。しばらくコードが届かない場合は、**メールを再送信**を選択します。確認後、Citrix Cloudにサインインします。
5. バックアップコードを使用する場合は、プロンプトが表示されたらコードを入力し、**確認して続行**を選択します。Citrix Cloudにサインインすると、バックアップコードが使用されたことと、残りの有効なバックアップコードの数を通知するメールが送信されます。使用済みのバックアップコードをメモするか削除して、再度使用しないようにしてください。
6. 回復用メールまたはバックアップコードを使用できない場合:

   a. **Citrixサポートに連絡**を選択します。
   b. 問題の詳細をフォームに入力します。Citrixサポート担当者が、お客様の回復用電話番号を使用して本人確認を行います。その後、担当者からサインインに使用できる回復コードが送信されます。
   c. Citrix Cloudサインインページに戻り、Citrix Cloudの資格情報を使用してサインインします。
   d. コードの入力を求められたら、Citrixサポートから受け取った回復コードを入力し、**確認**を選択します。

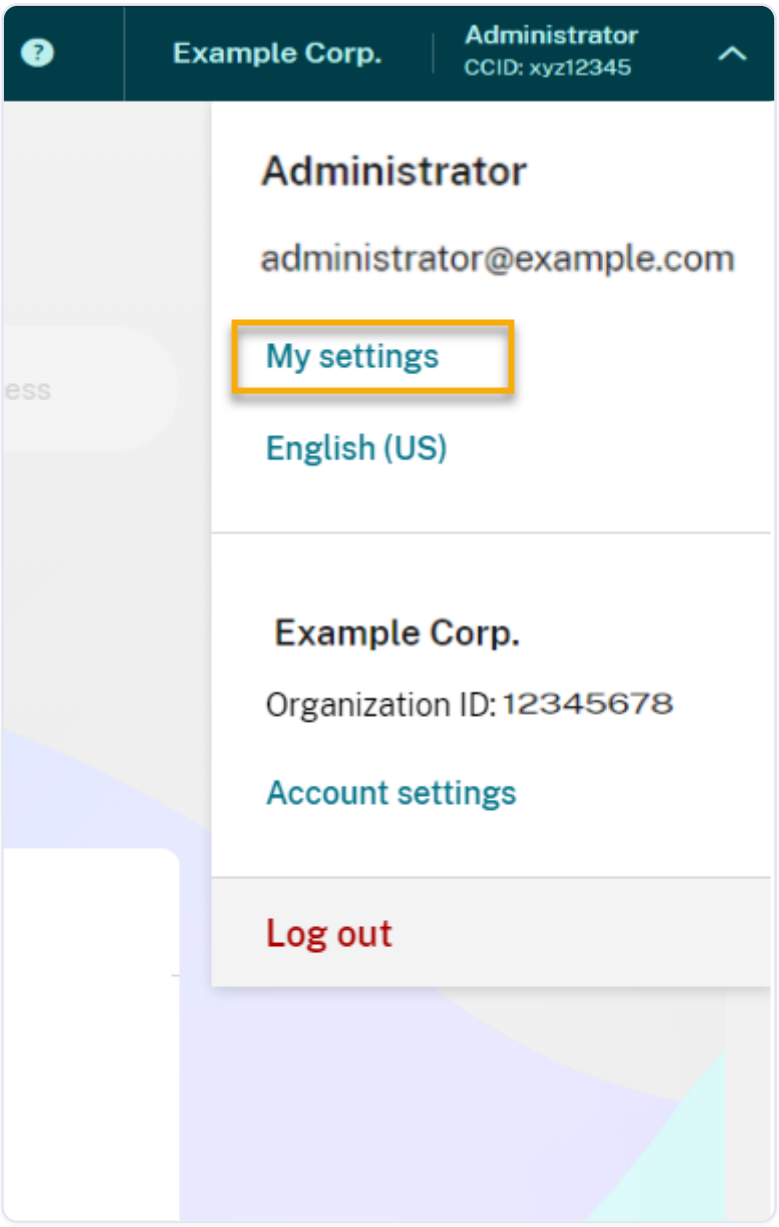
サインイン後、今後のサインインの遅延を避けるため、アカウントの回復方法を必ず更新してください。

MFA設定を更新する

マイ設定ページからMFAアクセスおよび回復設定を更新できます。このページには、CitrixアカウントまたはCitrix Cloudからアクセスできます。

マイ設定ページにアクセスするには:

1. CitrixアカウントまたはCitrix Cloudにサインインします。
2. Citrixアカウントから、https://accounts.cloud.com/core/profileにアクセスします。
3. Citrix Cloudで、右上のメニューから**マイ設定**を選択します。



MFA設定を変更するには、以下のセクションを参照してください。

- プライマリMFAメソッドを管理する
- MFAリカバリメソッドを管理する

パスワードの変更

アカウントのパスワードを忘れた場合は、**パスワードを忘れた場合**を選択し、プロンプトが表示されたらアカウントのユーザー名を入力します。Citrixは、新しいパスワードを設定するためのリンクを記載したメールを、お客様のアカウントのメールアドレスに送信します。数分経ってもこのメールが届かない場合、またはさらにサポートが必要な場合は、Citrixカスタマーサービスにお問い合わせください。

Citrix Cloudでは、サインインしようとするとパスワードのリセットを求められる場合があります。このプロンプトは、次の場合に表示されます。

- パスワードがCitrix Cloudの複雑さの要件を満たしていません。
- パスワードに辞書に載っている単語が含まれています。
- パスワードが、侵害されたパスワードの既知のデータベースにリストされています。
- 過去60日間Citrix Cloudにサインインしていません。

パスワードは8文字から128文字で、以下を含める必要があります。

- 少なくとも1つの数字
- 少なくとも1つの大文字
- 少なくとも1つの記号: ! @ # $ % \^ * ? + = -

プロンプトが表示されたら、**パスワードのリセット**を選択して、アカウントの新しい強力なパスワードを作成します。

クラウドサービスの正常性

Citrix Cloud Health Dashboard (https://status.cloud.com) は、各地理的リージョンにおけるCitrix Cloudプラットフォームおよびサービスのリアルタイムの可用性の概要を提供します。Citrix Cloudで問題が発生した場合は、Cloud Health Dashboardを確認して、Citrix Cloudまたは特定のサービスが正常に動作していることを確認してください。

Cloud Health Dashboardの詳細については、「サービスの正常性」を参照してください。

Citrix Cloudサポートフォーラム

Citrix Cloudサポートフォーラムでは、ヘルプの入手、フィードバックや改善提案の提供、他のユーザーとの会話の閲覧、独自のトピックの開始ができます。

Citrixのサポートスタッフはこれらのフォーラムを監視しており、お客様の質問に答える準備ができています。他のCitrix Cloudコミュニティメンバーも、ヘルプを提供したり、ディスカッションに参加したりできます。

フォーラムのトピックを読むためにサインインする必要はありません。ただし、トピックを投稿したり返信したりするにはサインインする必要があります。サインインするには、既存のCitrixアカウントの資格情報を使用するか、Citrix Cloudアカウントを作成したときに提供したメールアドレスとパスワードを使用します。

サポート記事とドキュメント

Citrixは、Citrix Cloudを最大限に活用し、Citrix製品で発生する可能性のある問題を解決するのに役立つ、豊富な製品およびサポートコンテンツを提供しています。

Citrixサポート知識センター

Knowledge Centerは、すべてのCitrix製品のトラブルシューティングコンテンツ、セキュリティ速報、およびソフトウェア更新通知を提供します。検索文字列を入力するだけで関連コンテンツを見つけることができます。製品と記事の種類に基づいて結果をフィルタリングできます。

シトリックス テックゾーン

Citrix Tech Zoneには、Citrix Cloudやその他のCitrix製品について詳しく学ぶのに役立つ情報が含まれています。ここでは、Citrixテクノロジーの設計、構築、展開に関する洞察を提供するリファレンスアーキテクチャ、図、ビデオ、技術文書を見つけることができます。

ユーザーヘルプセンター

Citrix User Help Centerでは、組織のエンドユーザー向けのCitrix製品ドキュメントを提供しています。ユーザーヘルプセンターでは、Citrix WorkspaceアプリやCitrix SSOなどのエンドユーザー向け製品について、読みやすい形式で手順を説明しています。ShareFileのエンドユーザー向けドキュメントについては、ShareFile製品ドキュメントWebサイトのCitrix Files appsを参照してください。

オンラインでカスタマーサービスケースを開く方法

> **注:**

> テレメトリーに準拠し、有効なアクティブな資格を持つお客様またはパートナーのみが、カスタマーサービスケースを開くことができます。 「ケースを作成」ボタンが利用できなくなった場合、お客様はチャットを使用してサポートに連絡する必要があります。アドバイザーがサポートケースの作成を支援したり、Web-to-Caseを開始したりできます。

> 新しいケースを作成するには、次の手順に従います。

1. Citrixサポートサイトにアクセスします。
2. Citrixの資格情報を使用してサインインします。

3. CitrixアカウントでCitrix Webサイトにサインインできない場合は、記事「CTX228792: Citrix Webサイトでのログインの問題のトラブルシューティング」を参照してください。
4. **ライブサポート**をクリックして、バーチャルアシスタントフローを開始します。

   ライブサポートオプションのヘルプ(/en-us/citrix-cloud/media/help-live-support-option.png)
5. 適切なケースタイプを選択し、利用可能なオプションから**関連する問題**を選択します。

   ケースタイプのヘルプ(/en-us/citrix-cloud/media/help-case-type.png)
6. 既存のケースをフォローアップしている場合は、**マイサポートケース**を選択し、プロンプトに従って続行します。ボットが問題に関連する記事またはドキュメントを提示します。



7. 役立つ場合は、 をクリックします。メインメニューに戻るか、チャットを終了するように求められます。
8. 記事が役に立たなかった場合は、 をクリックします。ボットが問題の再説明を求め、新しい入力に基づいてより関連性の高い記事を提供しようとします。
9. 2番目の記事でも解決しない場合は、もう一度 をクリックしてサポートに接続します。
10. 続行するには、 をクリックします。



11. ケース作成を開始するには、 をクリックします。



12. ドロップダウンリストから を選択します。
13. 利用可能なオプションから を選択します。



14. 次のメッセージが表示されます: **ケース作成後にライブエージェントに接続しますか？**
15. ライブエージェントとのチャットを開始するには、 を選択します。ケースが作成され、利用可能なアドバイザーに接続されます。
16. が選択された場合、ボットは追加情報を要求し、オフラインケースを作成します。

ライブサポートを介したオフラインケースの送信

仮想アシスタントが問題を解決できない場合、オフラインケースを作成するために追加の詳細を提供するよう求められることがあります。

1. **問題を10語以内で説明してください**: 問題またはリクエストの簡単な要約を提供します。
2. **ご希望のコールバック番号を入力してください**: Citrixカスタマーサービスアドバイザーがお客様に連絡できる有効な電話番号を提供してください。
3. 要求された情報を送信した後、オフラインケースが生成され、チャット開始者にメールで送信されます。カスタマーサービスアドバイザーは2時間以内にお客様に連絡します。

Citrix Cloud™ サービス稼働状況

Citrix Cloud Health Dashboardは、各地理的地域におけるCitrix Cloudプラットフォームとサービスのリアルタイムの可用性の概要を提供します。Citrix Cloudで問題が発生した場合は、Cloud Health Dashboardを確認して、Citrix Cloudまたは特定のサービスが正常に動作していることを確認してください。

クラウド ヘルス ダッシュボード(/en-us/citrix-cloud/media/service-health-dashboard.png)

以下の方法でCloud Health Dashboardにアクセスできます。

- Webブラウザーからhttps://status.cloud.comにアクセスします。
- Citrix Cloudのヘルプメニューから**サービス稼働状況**を選択します。

  サービス稼働状況オプションが強調表示されたヘルプメニュー(/en-us/citrix-cloud/media/help-menu-service-health.png)

ダッシュボードを使用して、以下の状況について詳細を確認できます。

- 地理的地域別にグループ化された、すべてのCitrix Cloudサービスの現在の稼働状況
- 過去7日間の各サービスの稼働状況の履歴
- 特定のサービスのメンテナンス期間

メンテナンス期間やサービスインシデントなどのイベントに関する通知を購読することもできます。

稼働状況とメンテナンスステータスの表示

各地理的地域におけるすべてのCitrix Cloudサービスとプラットフォームコンポーネントの現在の稼働状況を表示するには、**現在のステータス**を選択します。

現在のステータスが強調表示されたCloud Health Dashboard(/en-us/citrix-cloud/media/service-health-current-status-view.png)

過去7日間のすべてのCitrix Cloudサービスおよびプラットフォームコンポーネントの稼働状況を表示するには、「**履歴**」を選択します。過去7日間にメンテナンスまたは稼働状況イベントが発生したサービスのみを表示するには、「**影響を受けるサービスのみ表示**」を選択します。

「履歴」が強調表示されたCloud Health Dashboard (/en-us/citrix-cloud/media/service-health-list-view.png)

サービスメンテナンス期間の予定表ビューを表示するには、「**メンテナンス**」を選択します。今後の月に予定されているメンテナンスイベントを表示するには、「**次へ**」を選択します。今月のイベントに戻るには、「**前へ**」を選択します。

「メンテナンス」が強調表示されたCloud Health Dashboard (/en-us/citrix-cloud/media/service-health-calendar-view.png)

サービスインシデントの詳細を表示

影響を受けるサービスのサービス稼働状況インシデントに関する詳細情報を表示するには：

- 履歴ビューで、サービスインジケーターの横にあるアイコンをクリックして、サービス稼働状況インシデントに関する詳細情報を表示します。

  サービス稼働状況の詳細 (/en-us/citrix-cloud/media/service-health-event-details.png)
- メンテナンスビューで、サービスエントリをクリックして、スケジュールされたメンテナンス期間のステータスページを表示します。

  エントリが強調表示されたサービス稼働状況カレンダービュー (/en-us/citrix-cloud/media/service-health-calendar-events.png)

インシデント通知の頻度

サービス稼働状況インシデントが発生した場合、Citrixはstatus.cloud.comに投稿する際に以下の特性を考慮します。

- 影響の期間
- 影響の頻度

インシデントが対処されている間、Citrix®はCloud Health Dashboardに以下の種類の通知を投稿します。

- **調査中:** この通知は、Citrix が問題を緊急と認識し、調査中であることを示します。
- **監視中:** この通知は、Citrix が根本原因を特定し、問題の軽減に取り組んでいることを示します。
- **解決済み:** この通知は、Citrix が問題を解決し、サービスが正常な状態に復元されたことを示します。

インシデントの調査および監視中、Citrix は 60 分から 120 分間隔で更新情報を投稿します。これらの更新情報には、次のような情報が含まれる場合があります。

- インシデントに関する追加の詳細。

- Citrix がインシデントを解決するために講じている措置の説明。
- 前回の更新以降、新しい変更がないことを示す情報。

インシデントが解決されると、Citrix は最終更新情報を投稿します。この更新情報には、インシデントが解決され、サービスが正常な状態に復元されたことが示される場合があります。

通知を購読する

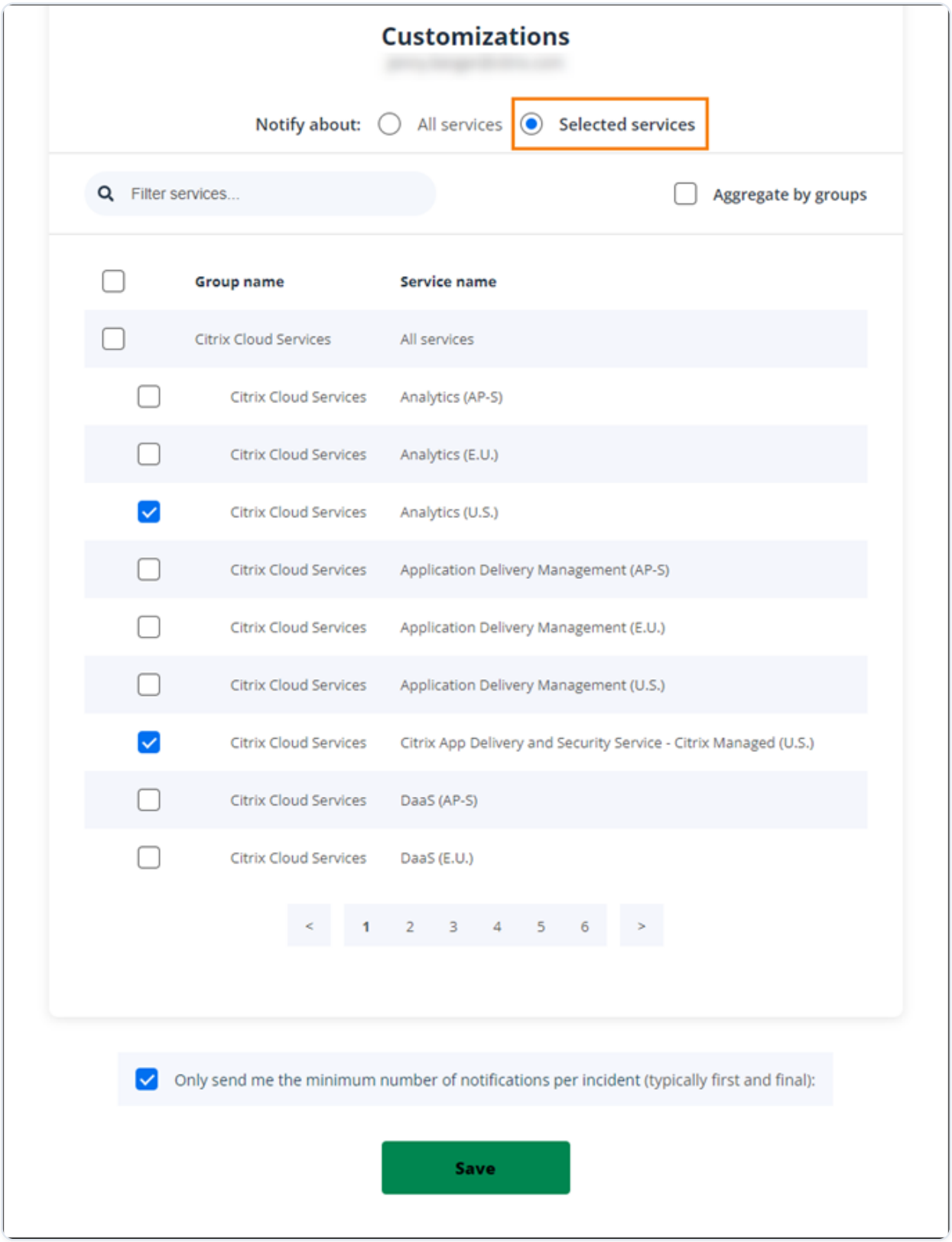
以下の方法でサービス稼働状況イベントに関する通知を受け取ることができます。

- ダッシュボードの右上にある「**購読**」を選択し、使用したい通知方法を選択します。電子メールや電話（テキストメッセージとして）など、いくつかの方法から選択できます。

  購読リンクが強調表示されたサービス稼働状況ダッシュボード(/en-us/citrix-cloud/media/service-health-subscribe-link.png)
- RSSリーダーに以下のURLを入力して、Citrix Cloud Health RSSフィードを購読します。
  - サービスインシデントとメンテナンスの通知を単一のフィードで受け取るには、`https://status.cloud.com/?format=atom`を購読してください。
  - サービスインシデントの通知のみを受け取るには、`https://status.cloud.com/atom/incidents`を購読してください。
  - メンテナンス通知のみを受信するには、`https://status.cloud.com/atom/maintenances`を購読してください。

特定のリージョンのサービスを購読する

1. ダッシュボードの右上隅にある を選択し、使用する通知方法を選択します。
2. 選択した購読方法の連絡先の詳細またはURLを入力し、 を選択します。 を選択します。 ページが表示され、デフォルトで が選択されています。
3. ページで、複数ページにわたるリストから、必要なリージョンのサービスを選択します。

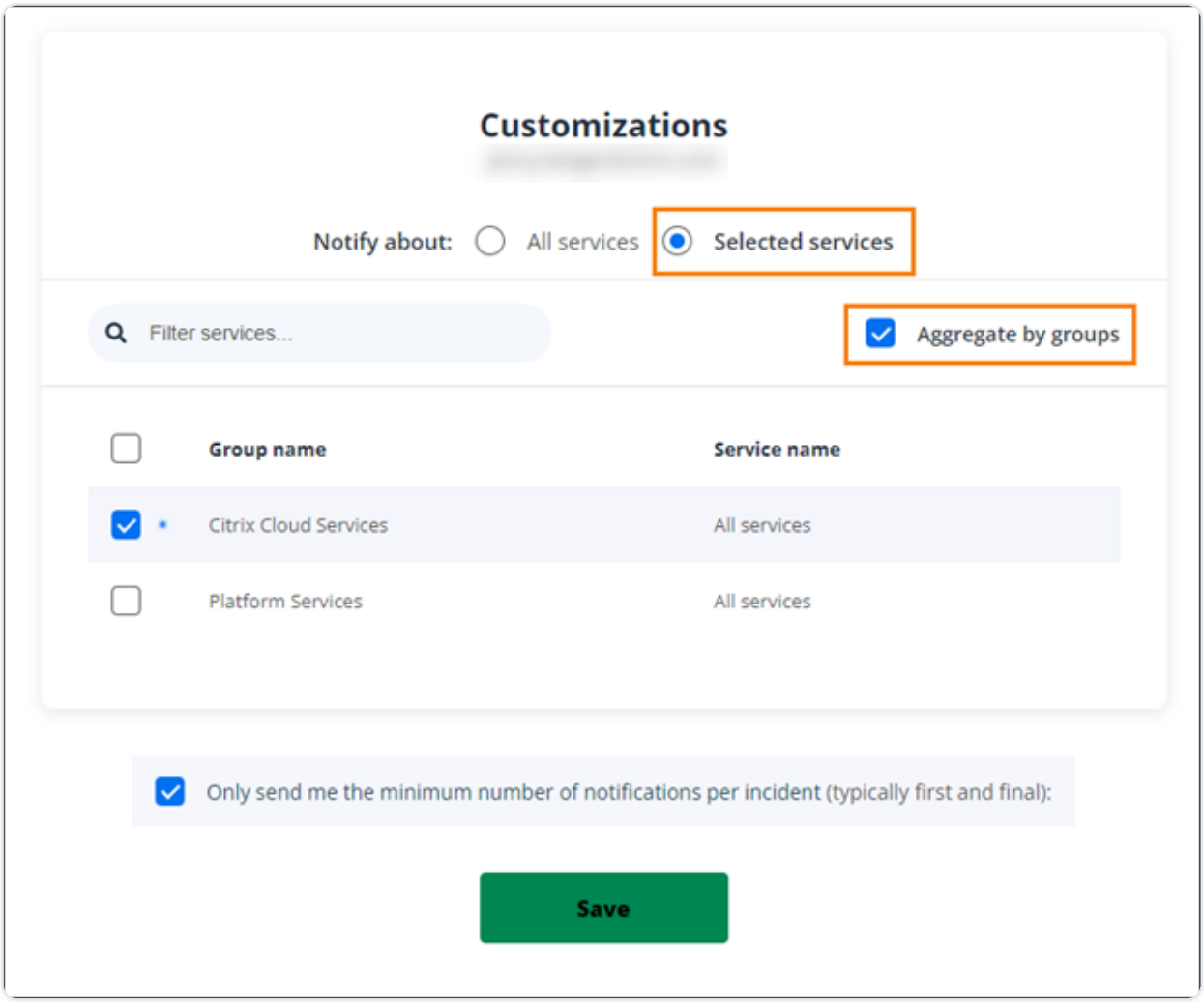


4. 各インシデントの最初と最後の通知のみを受信するには、 を選択します。
5. をクリックします。

特定のサービスグループを購読する

すべてのリージョンで、すべてのクラウドサービス（例: Analytics、DaaS）またはすべてのプラットフォームサービス（例: コントロールプレーン、クラウドAPI）の通知を購読できます。

1. ダッシュボードの右上隅にある を選択し、使用する通知方法を選択します。
2. 選択した購読方法の連絡先の詳細またはURLを入力し、 を選択します。 を選択します。 ページが表示され、デフォルトで が選択されています。
3. ページで、 を選択します。
4. または のいずれかを選択します。



5. 各インシデントの最初と最後の通知のみを受け取るには、**インシデントごとに最小限の通知のみを送信する** を選択します。
6. **保存** をクリックします。

通知の登録解除

購読方法に応じて、登録解除または購読変更のリンクは、受信する確認メッセージ（電話通知を購読する場合など）または各通知メッセージ（メール通知を購読する場合など）に含まれています。例：

- 購読オプション付きの電話通知：

  電話によるサービス正常性購読確認(/en-us/citrix-cloud/media/service-health-subscribe-confirm-phone.jpg)

- 購読オプション付きの通知メール

  購読オプションが強調表示されたサービス正常性通知メール(/en-us/citrix-cloud/media/service-health-subscribe-edit-email.png)

すべての通知の登録を解除し、すべての購読方法を削除するには：

1. 購読確認メッセージまたは既存の通知を見つけて、登録解除リンクを選択します。一部の購読方法では、購読を編集またはキャンセルするための単一のリンクが提供される場合があります。
2. 購読方法に応じて、**サブスクリプションの編集**ページで次のいずれかのオプションを使用します。

   - **すべてのサブスクリプションを削除** を選択します。
   - **登録解除** を選択します。**登録解除方法**ページから、**すべてのサブスクリプションを削除** を選択します。

特定の購読方法のすべての通知の登録を解除するには：

1. 購読確認メッセージまたは既存の通知を見つけて、登録解除リンクを選択します。一部の購読方法では、購読を編集またはキャンセルするための単一のリンクが提供される場合があります。
2. 購読方法に応じて、「**Edit Subscriptions**」ページで次のいずれかのオプションを使用します。

   - 削除する購読方法を選択します。購読はすぐに削除されます。
   - 「**Unsubscribe**」を選択します。「**Unsubscribe methods**」ページから、削除する購読方法を選択します。購読はすぐに削除されます。

サービス通知を変更する

1. 購読確認メッセージまたは既存の通知を見つけて、購読を編集するためのリンクを選択します。一部の購読方法では、購読を編集またはキャンセルするための単一のリンクが提供される場合があります。
2. 「**Edit Subscriptions page**」から、管理する購読方法を選択します。
3. 「**Customizations**」ページで、通知を受けたいサービスを選択するか、通知が不要になったサービスを必要に応じてクリアします。
4. 「**Save**」を選択します。

システムと接続要件

Citrix Cloud™ は、展開内のリソースに接続する管理機能 (Web ブラウザ経由) と運用要求 (他のインストール済みコンポーネントから) を提供します。この記事では、システム要件、必要な接続可能なインターネットアドレス、およびリソースと Citrix Cloud 間の接続を確立するための考慮事項について説明します。

システム要件

Citrix Cloud には、以下の最小構成が必要です。

- Active Directory ドメイン
- Citrix Cloud Connector 用に、ドメインに参加している物理マシンまたは仮想マシンを 2 台。詳細については、「Cloud Connector のシステム要件」を参照してください。
- ワークロードや StoreFront などの他のコンポーネントをホストするために、ドメインに参加している物理マシンまたは仮想マシン。特定のサービスのシステム要件の詳細については、各サービスの Citrix® ドキュメントを参照してください。

規模とサイズ要件については、「Cloud Connector の規模とサイズに関する考慮事項」を参照してください。

サポートされている Web ブラウザ

- Google Chrome の最新バージョン
- Mozilla Firefox の最新バージョン
- Microsoft Edge の最新バージョン
- Apple Safari の最新バージョン

トランスポート層セキュリティの要件

Citrix Cloud は、コンポーネント間の TCP ベースの接続に Transport Layer Security (TLS) 1.2 をサポートしています。Citrix Cloud は、TLS 1.0 または TLS 1.1 を介した通信を許可しません。

Citrix Cloud にアクセスするには、TLS 1.2 をサポートし、承認された暗号スイートが構成されているブラウザを使用する必要があります。詳細については、「暗号化とキー管理」を参照してください。

Citrix Cloud 管理コンソール

Citrix Cloud 管理コンソールは、https://citrix.cloud.com にサインインした後にアクセスできる Web ベースのコンソールです。コンソールを構成する Web ページは、サインイン時または特定の操作を実行する際に、インターネット上の他のリソースを必要とする場合があります。

プロキシ構成

プロキシサーバー経由で接続している場合、管理コンソールは Web ブラウザに適用されているのと同じ構成を使用して動作します。コンソールはユーザーコンテキスト内で動作するため、ユーザー認証を必要とするプロキシサーバーの構成はすべて期待どおりに機能するはずです。

ファイアウォール構成

管理コンソールを動作させるには、送信接続用にポート 443 を開いている必要があります。コンソール内を移動することで、一般的な接続をテストできます。必要なポートの詳細については、「受信および送信ポートの構成」を参照してください。

コンソール通知

管理コンソールは Pendo を使用して、重要なアラート、新機能に関する通知、および一部の機能とサービスに関する製品内ガイダンスを表示します。

管理コンソール内で Pendo コンテンツを表示できるようにするには、Citrix は以下の宛先に接続できることを推奨します。

- `https://citrix-cloud-content.customer.pendo.io/`
- `https://citrix-cloud-data.customer.pendo.io/`

Pendo サービスへの接続が制限されている場合、製品内ガイダンス、通知、および関連するユーザーエクスペリエンス機能が制限されたり、利用できなくなったりする可能性があります。Pendo サービスは米国 (US) でホストされており、Pendo によって収集されたデータはこの地域内で処理されます。詳細については、「地理的考慮事項」を参照してください。

> **注:**

両方の URL は、停止通知、新機能の発表、顧客フィードバック調査を含むメッセージングを完全に有効にするために必要です。

Pendoコンテンツを表示するサービスには、以下が含まれます。

- Citrix Cloud管理コンソール
- Citrix DaaS™ (Workspace Environment Management™、Web Studio、およびSession Recordingなどの機能を含む)
- Citrix Studio（オンプレミス）
- Citrix DirectorおよびMonitorの各機能
- NetScaler (ADC)
- NetScaler Console (ADM) およびNetScaler Consoleサービス
- セキュア デベロッパー スペース
- Citrix® StoreFront Cloud（デスクトップ、モバイル、タブレット - クラウド展開のみ）、ネイティブiOSおよびAndroidアプリケーションを含む

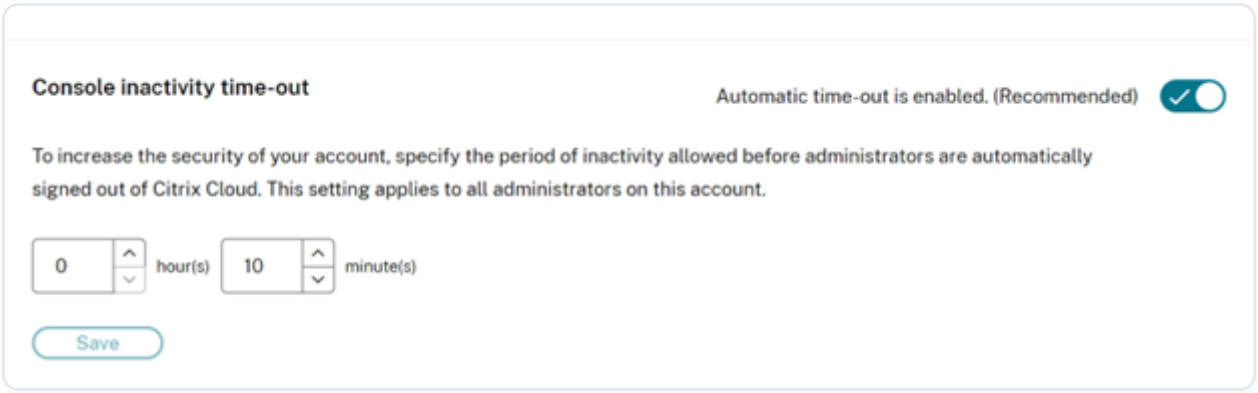
Pendoは、CitrixがCitrixのお客様にクラウドおよびサポートサービスを提供するために使用するサードパーティのサブプロセッサーです。これらのサブプロセッサーの完全なリストについては、「Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates」を参照してください。

セッションのタイムアウト

管理者がCitrix Cloudにサインインした後、管理コンソールセッションは72時間経過するとタイムアウトします。このタイムアウトは、コンソールのアクティビティに関係なく発生します。

コンソールの非アクティブタイムアウトの構成

フルアクセス管理者として、管理者が自動的にサインアウトされるまでのCitrix Cloudコンソールでの非アクティブ期間を構成できます。構成されると、指定されたタイムアウト期間はCitrix Cloudアカウントのすべての管理者に適用されます。



この機能が有効になっている場合、管理者は設定された非アクティブ期間の後にログアウトされ、その後のログインごとにセッションタイムアウトがリセットされます。

この機能が無効になっている場合、非アクティブタイマーはなく、管理者は72時間のセッション制限に達した場合にのみログアウトされます。

注:

- この機能はデフォルトで無効になっています。
- 設定可能な非アクティブタイムアウトは10分から12時間です。
- デフォルトの非アクティブタイムアウトは60分です。

Citrix Cloudへのライセンスサーバー接続

オンプレミス展開の使用状況を監視するために、オンプレミスのCitrix License ServerをCitrix Cloudに登録する場合は、オンプレミス展開の使用状況を監視する、次のアドレスに接続できることを確認してください。

- `https://trust.citrixnetworkapi.net` (コードを取得するため)
- `https://trust.citrixworkspacesapi.net/` (ライセンスサーバーが登録されていることを確認するため)
- `https://cis.citrix.com` (データアップロードのため)
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`

- `crl.entrust.net port 80`

Citrix License Serverでプロキシサーバーを使用している場合は、Licensing製品ドキュメントのプロキシサーバーの構成に記載されているとおりにプロキシサーバーが構成されていることを確認してください。

シトリックス クラウド コネクタ™

Citrix Cloud Connectorは、Microsoft Windowsサーバー上で実行される一連のサービスを展開するソフトウェアパッケージです。Cloud Connectorをホストするマシンは、Citrix Cloudで使用するリソースが存在するネットワーク内に配置されます。Cloud ConnectorはCitrix Cloudに接続し、必要に応じてリソースを操作および管理できるようにします。

Cloud Connectorのインストール要件については、システム要件を参照してください。動作には、Cloud Connectorはポート443でのアウトバウンド接続が必要です。インストール後、Cloud Connectorは使用するCitrix Cloudサービスに応じて追加のアクセス要件を持つ場合があります。

Cloud Connectorをホストするマシンは、Citrix Cloudとの安定したネットワーク接続が必要です。ネットワークコンポーネントは、HTTPSと長期間持続するセキュアなWebソケットをサポートする必要があります。ネットワークコンポーネントでタイムアウトが構成されている場合、それは2分より長くする必要があります。

Cloud ConnectorとCitrix Cloud間の接続のトラブルシューティングについては、Cloud Connector Advanced Connectivity Checksを使用してください。

Cloud Connectorの共通サービス接続要件

データセンターからインターネットに接続するには、ポート443をアウトバウンド接続用に開く必要があります。ただし、インターネットプロキシサーバーまたはファイアウォールの制限がある環境で動作させるには、さらなる構成が必要になる場合があります。詳細については、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。

この記事の各サービスのアドレスは、サービスを適切に運用および利用するためにアクセス可能である必要があります。次のリストには、ほとんどのCitrix Cloudサービスに共通するアドレスが含まれています。

- `https://*.citrixworkspacesapi.net` (サービスが使用するCitrix Cloud APIへのアクセスを提供します)
- `https://*.cloud.com` (Citrix Cloudサインインインターフェイスへのアクセスを提供します)

- `https://*.blob.core.windows.net` (Citrix Cloud Connectorの更新を保存するAzure Blob Storageへのアクセスを提供します)
- `https://*.servicebus.windows.net` (ログ記録とActive Directoryエージェントに使用されるAzure Service Busへのアクセスを提供します)

これらのアドレスは、Citrix Cloudサービスが動的であり、そのIPアドレスが定期的に変更される可能性があるため、ドメイン名としてのみ提供されます。

ベストプラクティスとして、これらのアドレスの設定と管理にはグループポリシーを使用してください。また、ご自身とエンドユーザーが利用しているサービスに適用されるアドレスのみを設定してください。

Citrix License Serverを使用してCitrix Cloudでオンプレミス製品を登録する場合は、追加で必要な接続可能アドレスについて、この記事のLicense ServerとCitrix Cloudの接続を参照してください。

Cloud Connectorで許可されるFQDN

必要なすべての完全修飾ドメイン名 (FQDN) がファイアウォールを通過できるように、Citrixは以下のリソースを提供しています。

- コネクタ許可リストAPI
- シトリックス ゲートウェイ サービス -- サービス拠点 (PoP)

ファイアウォールを設定する際は、これらの両方のリソースを参照して、サービス展開に必要なFQDNが許可されていることを確認してください。

ローカルホストキャッシュ (高可用性サービス)

コネクタでローカルホストキャッシュ (LHC) を使用する場合、コネクタがリソースロケーション内の他のすべてのコネクタの選出エンドポイントに到達できることを確認してください。選出エンドポイントはポート80にあり、次のURLからアクセスできます: `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`。

コネクタがこのアドレスで通信できない場合、LHCイベント中に複数のブローカーが選出され、仮想アプリとデスクトップの起動が断続的に失敗する可能性があります。詳細については、複数のCloud Connectorを持つリソースロケーションを参照してください。

アダプティブ認証

アダプティブ認証サービスへの接続にCloud Connectorを使用する場合、Citrix Cloud Connectorがアダプティブ認証インスタンス用に予約したドメインまたはURLにアクセスできるようにする必

要があります。たとえば、`https://aauth.xyz.com`を許可します。詳細については、アダプティブ認証を参照してください。

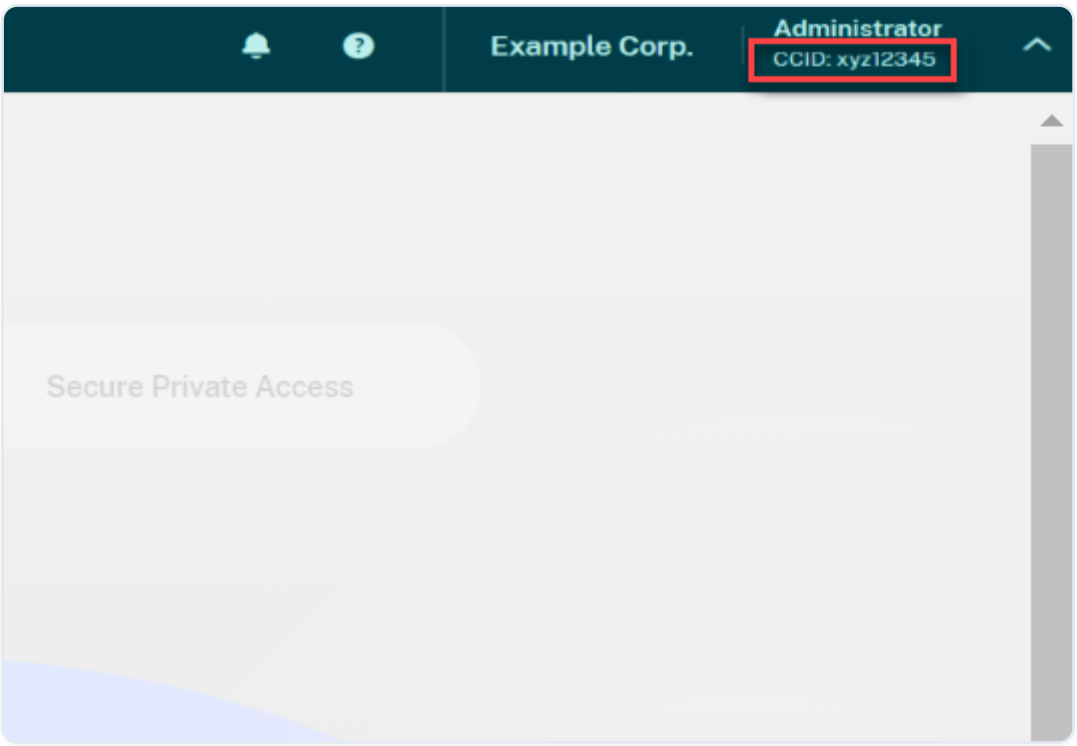
コネクタ許可リストAPI

可能な場合は、Cloud Connectorの共通サービス接続要件セクションのワイルドカードアドレスを使用してください。環境でワイルドカードが許可されていない場合は、コネクタ許可リストAPIを使用して、必要なFQDNの現在のリストを取得してください。

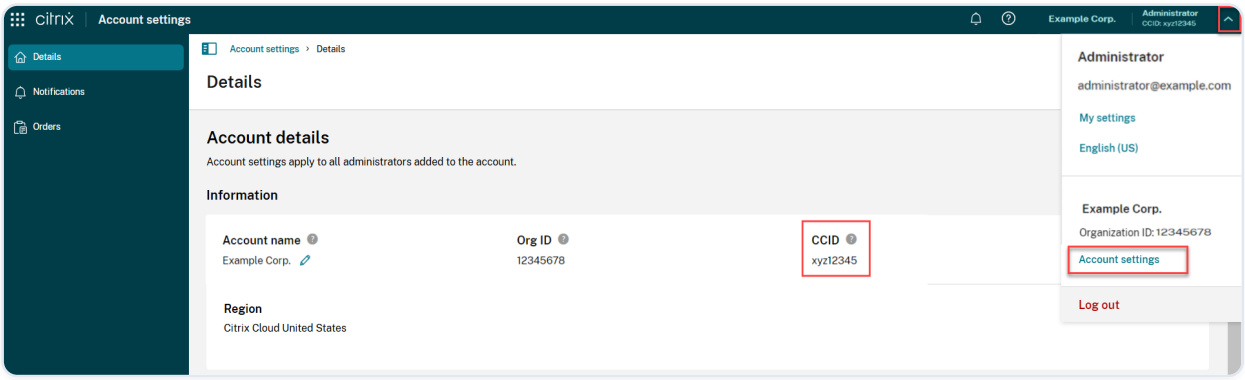
リストを以下から取得します: `https://api.cloud.com/connectivity/v2/allowlist?customerId=<CUSTOMER_ID>`

`<CUSTOMER_ID>`をCitrix CloudカスタマーID (CCID) に置き換えます。CCIDは、Citrix Cloudコンソールの以下の場所で確認できます。

- コンソールの右上、顧客名の下。



- アカウント設定ページで、**Citrix CloudカスタマーID (CCID)** の下。



クエリパラメータ

各名前と値のペアを `&` で区切って、エンドポイントにクエリパラメータを追加します。たとえば、EU地域の送信FQDNを取得するには、次のURLを使用します。

```
https://api.cloud.com/connectivity/v2/allowlist?customerId=<CCUSTOMER_ID>&direction=outbound&geo=EU
```

v2 APIは、以下のクエリパラメータをサポートしています。

- **CustomerId:** Citrix CloudカスタマーID (CCID)。customerIdを渡すと、APIはリストを返す前に、返されたFQDN内の `<CUSTOMER_ID>` プレースホルダーを置き換えます (例: `<CUSTOMER_ID>.xendesktop.net` が `abc123.xendesktop.net` になります)。以前のallowlist.jsonファイルで行っていたように、ファイルをダウンロードした後、各エントリでCCIDを手動で置き換える必要はなくなります。
- **Format:** `json` (デフォルト) または `zscaler` のいずれかを選択します。省略した場合、応答はjson (デフォルト) として返されます。Zscaler構成にインポートするために事前にフォーマットされた応答を受け取るには、format=zscalerを設定します。
- **Geo:** 省略した場合、デフォルトは `all` であり、すべてのCitrix Cloud地域に対するFQDNを返します。リソースの場所が提供する単一の地域に応答の範囲を限定するには、`geo` を `us`、`eu`、または `ap-s` のいずれかに設定します。範囲を限定することで、より短く、よりターゲットを絞ったリストが生成され、展開が到達しない地域を許可リストに登録することを回避できます。
- **Direction:** 省略した場合、デフォルトは `all` であり、インバウンドとアウトバウンドの両方のFQDNを返します。Cloud Connectorが到達する必要があるFQDNのみを取得するには (一般的なファイアウォールのエグレスユースケース)、`direction=outbound` を設定します。Citrix Cloudが環境に接続するFQDNについては、`direction=inbound` を設定します。

> **注:**

> `https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json` にある以前の許可リストファイルは、限られた移行期間中は引き続き利用可能ですが、お客様の使用には非推奨です。上記の API エンドポイントに移行してください。BLOB URL は、内部のコネクタ接続チェックのために一時的に保持されており、将来のリリースで削除されます。

> v2 API エンドポイントは現在、Citrix Cloud の商用顧客向けに利用可能です。

Gateway Service の拠点 (PoP)

allowlist.json ファイルに含まれる FQDN の一部は、Citrix Gateway Service -- 拠点 (PoP) にも含まれています。ただし、Citrix Gateway Service -- 拠点 (PoP) には、クライアントがアクセスする FQDN も含まれており、例えば以下のものがあります。

- グローバル-s.g.nssvc.net
- アズール-s.g.nssvc.net

証明書の検証

Cloud Connector のバイナリと、Cloud Connector が接続するエンドポイントは、ソフトウェアのインストール時に検証される X.509 証明書によって保護されています。これらの証明書を検証するには、各 Cloud Connector マシンが特定の要件を満たす必要があります。これらの要件の完全なリストについては、証明書の検証要件 を参照してください。

SSL 復号化

特定のプロキシで SSL 復号化を有効にすると、Cloud Connector が Citrix Cloud に正常に接続できなくなる可能性があります。この問題の解決に関する詳細については、CTX221535 を参照してください。

Citrix Connector™ Appliance クラウドサービス向け

Connector Appliance は、ハイパーバイザーに展開できるアプライアンスです。Connector Appliance をホストするハイパーバイザーは、Citrix Cloud で使用するリソースが存在するネットワーク内に配置されます。Connector Appliance は Citrix Cloud に接続し、必要に応じてリソースを操作および管理できるようにします。

Connector Appliance のインストール要件については、システム要件 を参照してください。

Connector Appliance を動作させるには、ポート 443 でのアウトバウンド接続が必要です。ただし、インターネットプロキシサーバーやファイアウォールの制限がある環境で動作させるには、さらなる設定が必要になる場合があります。

Citrix Cloud サービスを適切に運用および利用するには、次のアドレスに接続できる必要があります。

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`

  すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます

  - `https://*.g.nssvc.net`
  - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

ネットワーク要件

Connector Appliance環境に次の構成があることを確認してください。

- ネットワークがConnector ApplianceでDHCPを使用してDNSおよびNTPサーバー、IPアドレス、ホスト名、ドメイン名を取得できるようにするか、Connector Appliance consoleでネットワーク設定を手動で設定できます。
- ネットワークが、Connector Applianceによって内部的に使用されるリンクローカルIP範囲169.254.0.1/24、169.254.64.0/18、または169.254.192.0/18を使用するように構成されていないこと。
- ハイパーバイザーのクロックが協定世界時（UTC）に設定され、タイムサーバーと同期されているか、DHCPがNTPサーバー情報をConnector Applianceに提供していること。
- Connector Applianceでプロキシを使用する場合、プロキシは認証なしであるか、基本認証を使用する必要があります。

Citrix Analyticsサービス接続

- 新機能、重要な連絡事項、顧客アンケートなどの製品内メッセージについては、以下のURLにアクセスできる必要があります。
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`
- 追加要件: 前提条件

サービスへのデータソースのオンボーディングの詳細については、「サポートされているデータソース」を参照してください。

NetScaler® Consoleサービス接続

完全なインターネット接続要件については、NetScaler製品ドキュメントの「サポートされているポート」を参照してください。

Citrix DaaS接続

DaaSへのCloud Connector接続

Cloud Connectorの共通サービス接続要件に加えて、DaaSで使用する場合、Cloud Connectorは以下への接続が必要です。

- `https://[customerid].xendesktop.net`。ここで`[customerid]`は、Citrix Cloud管理コンソールの**サービスプリンシパル**タブ（**IDおよびアクセス管理 > APIアクセス > サービスプリンシパル**）に表示される顧客IDパラメーターです。
- Citrix DaaSをインストールするためにQuick Deployを使用するお客様は、これらの追加アドレスにアクセスできる必要があります。
  - `https://*.apps.cloud.com`
  - 「`AzureCloud` サービス タグ」
- `https://*.*.nssvc.net`
  - すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

Cloud Connectorがサービスとどのように通信するかについては、Citrix Tech Zone Webサイトの Citrix DaaS図を参照してください。

DaaS管理コンソールへの接続

DaaSを管理するには、Citrix Cloud管理コンソールに加えて、次に接続できる必要があります。

- `https://*.citrixworkspacesapi.net` (Rendezvousプロトコルには不要)
- `https://*.citrixnetworkapi.net` (Rendezvousプロトコルには不要)
- `https://*.cloud.com` (Rendezvousプロトコルには不要)
- `https://[customerid].xendesktop.net`。ここで、`[customerid]` は、Citrix Cloud管理コンソールの**サービスプリンシパル**タブ (**IDおよびアクセス管理 > APIアクセス > サービスプリンシパル**) に表示される顧客IDパラメーターです。
- `https://*.*.nssvc.net` (Citrix DaaS Standard for Azureには不要)
  - すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- 新機能や重要な連絡事項、顧客アンケートなどの製品内メッセージについては、以下のURLにアクセスできる必要があります。
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`

Citrix DaaS リモート PowerShell SDK

Citrix DaaS Remote PowerShell SDKを使用するには、以下のURLをホワイトリストに登録してください。

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

Rendezvousプロトコル使用時のVDA接続

Citrix Gateway Serviceを使用する場合、Rendezvousプロトコルにより、VDAはCitrix Cloud Connectorsをバイパスして、Citrix Cloudコントロールプレーンに直接かつ安全に接続できます。

使用しているプロトコルバージョンに関係なく、特に明記されていない限り、VDAは上記の管理コンソールのURLにアクセスできる必要があります。Rendezvousプロトコルの要件の完全なリストについては、Citrix DaaS製品ドキュメントの以下のセクションを参照してください。

- ランデブー V1
- ランデブー V2

ローカルホストキャッシュの要件

ファイアウォールがパケット検査を実行し、ローカルホストキャッシュ機能を使用する場合は、ファイアウォールがXMLおよびSOAPトラフィックを許可していることを確認してください。この機能では、Cloud ConnectorがCitrix Cloudと構成データを同期するときに発生するMDFファイルをダウンロードする機能が必要です。これらのファイルは、XMLおよびSOAPトラフィックを介してCloud Connectorに配信されます。ファイアウォールがこのトラフィックをブロックすると、Cloud ConnectorとCitrix Cloud間の同期は失敗します。停止が発生した場合、Cloud Connectorに存在する構成データが古いため、ユーザーは作業を続行できません。

この機能の詳細については、Citrix DaaS製品ドキュメントのローカルホストキャッシュを参照してください。

VDAアップグレードの要件

Citrix DaaSの完全構成インターフェイスを使用して、カタログごとまたはマシンごとにVDAをアップグレードできます。すぐにアップグレードすることも、スケジュールされた時間にアップグレードすることもできます。VDAアップグレード機能の詳細については、「完全構成インターフェイスを使用したVDAのアップグレード」を参照してください。

この機能を使用する場合は、次の接続要件を満たしていることを確認してください。

- 次のAzure CDN URLが許可リストに追加されています。この機能は、Azure CDNエンドポイントからVDAインストーラーをダウンロードします。
  - 本番環境 - 米国 (US): `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - 本番環境 - 欧州連合 (EU): `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - 本番環境 - アジア太平洋南部 (APS): `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - 本番環境 - 日本 (JP): `https://prod-jp-vus-storage-endpoint.azureedge.net/*`

- この機能は、VDAインストーラーが有効な証明書によって署名されていることを確認します。証明書の有効性と失効チェックのために、次のURLが許可リストに追加されていることを確認してください。
  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`
- この機能にはVDAアップグレードエージェントが必要です。VDA上で実行されているVDAアップグレードエージェントはCitrix DaaSと通信します。以下のURLが許可リストに追加されていることを確認してください。
  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`。ここで`[customerid]`は、Citrix Cloud管理コンソールの**サービスプリンシパル**タブ（**IDおよびアクセス管理 > APIアクセス > サービスプリンシパル**）に表示される顧客IDパラメーターです。
  - `http://xendesktop.net/citrix/VdaUpdateService/*`

Endpoint Managementサービス接続

Citrixリソースの場所 / Cloud Connector:

- Cloud Connector共通サービス接続要件
- 追加要件: /ja-jp/citrix-endpoint-management/endpoint-management.html

管理コンソール:

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- 追加要件: /ja-jp/citrix-endpoint-management/endpoint-management.html

Citrix Gatewayサービス接続

Cloud ConnectorからCitrix Gatewayサービスへの接続

Citrix Gateway Service を Cloud Connector 経由で使用する場合 (つまり Rendezvous v2 なしの場合)、Cloud Connector の共通サービス接続要件 に加えて、Cloud Connector は以下にアクセスする必要があります。

- `https://*.*.nssvc.net`

すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。

- `https://*.g.nssvc.net`
- `https://*.c.nssvc.net`

> **重要:**
>
> Citrix Gateway アドレスでは SSL インターセプトを実行できません。特定のプロキシで SSL インターセプトを有効にすると、Cloud Connector が Citrix Cloud に正常に接続できなくなる可能性があります。

Citrix Gateway Service へのクライアント接続

Citrix Gateway Service を使用するには、クライアントデバイスは以下にアクセスする必要があります。

- `https://*.*.nssvc.net`

すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。

- `https://*.g.nssvc.net`
- `https://*.c.nssvc.net`

SD-WAN Orchestrator サービス接続

完全なインターネット接続要件については、Citrix SD-WAN Orchestrator サービス使用の前提条件を参照してください。

リモートブラウザ分離 (旧Secure Browser) サービス

Cloud Connectorからリモートブラウザ分離サービスへの接続

Cloud Connectorは、Cloud Connector共通サービス接続要件以外の追加の接続は必要ありません。

管理コンソールへの接続

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://browser-release-a.azureedge.net`
- `https://browser-release-b.azureedge.net`

Citrix Secure Private Access™へのクライアント接続

- `https://*.netscalergateway.net`
- `https://*.*.nssvc.net`
    - すべてのサブドメインを有効にできないお客様は、代わりに以下のURLを使用できます。
        - `https://*.g.nssvc.net`
        - `https://*.c.nssvc.net`

Global App Configurationサービスへのクライアント接続

`https://discovery.cem.cloud.us`

このサービスの詳細については、「」を参照してください(/ja-jp/citrix-workspace/experience/workspace-app-settings.html)。

ストアへのエンドユーザー接続

このセクションでは、Citrix WorkspaceアプリまたはWebブラウザを使用してクラウドストアにアクセスする際に、クライアントが到達できる必要があるURLを一覧表示します。

ストアURL

ユーザーは、クラウドURL（例: `https://<customername>.cloud.com`）またはカスタムURLのいずれかを介してストアにアクセスします。詳細については、ストアへのアクセスを構成するを参照してください。

認証

シトリックス クラウド:

- `https://accounts.cloud.com`
- `https://accounts-dsauthweb.cloud.com`
- `https://accounts-webassets.cloud.com` - グラフィカルインターフェイスアセット用
- `https://login.cloud.com` - Active DirectoryまたはActive Directory + トークンをIDプロバイダーとして使用している場合にのみ必要です

シトリックス クラウド ジャパン:

- `https://accounts.citrixcloud.jp`
- `https://accounts-dsauthweb.citrixcloud.jp`
- `https://accounts-webassets.citrixcloud.jp` - グラフィカルインターフェースアセット用
- `https://login.citrixcloud.jp` - IDプロバイダーとしてActive DirectoryまたはActive Directory + Tokenを使用している場合にのみ必要です

シトリックス クラウド ガバメント:

- `https://accounts.cloud.us`
- `https://accounts-dsauthweb.cloud.us`
- `https://login.cloud.us` - IDプロバイダーとしてActive DirectoryまたはActive Directory + Tokenを使用している場合にのみ必要です

Citrix Cloud Governmentでは`https://accounts-webassets.cloud.us`は不要です。グラフィカルインターフェースアセットには`https://accounts.cloud.us`が使用されます。

サードパーティのIDプロバイダーを使用している場合は、必要なURLについてベンダーにお問い合わせください。

ストアのグラフィカルインターフェースアセット

- `https://ctx-ws-assets.cloud.com`

Citrix Cloud Governmentの場合、これは将来的に`https://ctx-ws-assets.cloud.us`に変更される可能性があります。

パーソナライゼーション、通知、および機能の展開

WebブラウザではなくCitrix Workspaceアプリを使用する場合、組織の地域に応じて以下のURLが必要です。

米国:

- `https://customer-interface-personalization.us.wsp.cloud.com`
- `https://user-personalization.us.wsp.cloud.com`
- `https://admin-notification.us.wsp.cloud.com`
- `https://feature-rollout.us.wsp.cloud.com`

EU:

- `https://customer-interface-personalization.eu.wsp.cloud.com`
- `https://user-personalization.eu.wsp.cloud.com`
- `https://admin-notification.eu.wsp.cloud.com`
- `https://feature-rollout.eu.wsp.cloud.com`

アジア太平洋南部:

- `https://customer-interface-personalization.ap-s.wsp.cloud.com`
- `https://user-personalization.ap-s.wsp.cloud.com`
- `https://admin-notification.ap-s.wsp.cloud.com`
- `https://feature-rollout.ap-s.wsp.cloud.com`

シトリックス クラウド ジャパン:

- `https://customer-interface-personalization.jp.wsp.citrixcloud.jp`
- `https://user-personalization.jp.wsp.citrixcloud.jp`
- `https://admin-notification.jp.wsp.citrixcloud.jp`
- `https://feature-rollout.jp.wsp.citrixcloud.jp`

シトリックス クラウド ガバメント:

- `https://customer-interface-personalization.us.wsp.cloud.us`
- `https://user-personalization.us.wsp.cloud.us`
- `https://admin-notification.us.wsp.cloud.us`
- `https://feature-rollout.us.wsp.cloud.us`

ブランディング画像

- 米国: `https://cips-iws-prod-eus2-cip-cdn.azureedge.net`
- EU: `https://cips-iws-prod-weu-cip-cdn.azureedge.net`
- AP-S `https://cips-iws-prod-aue-cip-cdn.azureedge.net`
- シトリックス クラウド ジャパン `https://cips-wspjp-prod-jpe-cip-cdn.azureedge.net`
- シトリックス クラウド ガバメント `https://cips-wspgov-prod-usgv-cip-cdn.azureedge.us`

プロフィール画像

ユーザーがプロフィール画像をアップロードする場合、以下のURLへのアクセスが必要です。

- 米国: `https://wups-us-iws-cloud.azureedge.net`
- EU: `https://wups-eu-iws-cloud.azureedge.net`
- AP-S: `https://wups-ap-s-iws-cloud.azureedge.net`
- シトリックス クラウド ジャパン: `https://wups-wspjp-jp-production.azureedge.net`

アプリケーションアイコン

シトリックス クラウド:

- `https://wscs-cdn.wsp.cloud.com/icons`

シトリックス クラウド ジャパン:

- `https://wscs-cdn.wsp.citrixcloud.jp/icons`

シトリックス クラウド ガバメント:

- `https://wscs-cdn.wsp.cloud.us/icons`

ペンド

新機能や重要な連絡事項を含む製品内メッセージ用。

- `https://citrix-cloud-content.customer.pendo.io`

シトリックス アナリティクス サービス

- `locus.analytics.cloud.com`

テナントのGEOに応じて、以下のリストから適切なURLへのアクセスを有効にします。

- 米国: `citrixanalyticseh.servicebus.windows.net`
- EU: `citrixanalyticseheu.servicebus.windows.net`
- APS: `citrixanalyticsehaps.servicebus.windows.net`

その他のサービス

クライアントが接続する必要があるその他のサービスについては、以下を参照してください。

- Citrix Gateway Serviceへのクライアント接続
- Citrix Secure Private Accessサービスへのクライアント接続
- Global App Configurationサービスへのクライアント接続

シトリックス フェデレーション認証サービス (FAS)

Citrix Federated Authentication ServiceとCitrix Cloud間の接続を参照してください。

ワークスペース エンバイロメント マネジメント™ サービス接続

Citrixリソースロケーション / Cloud Connector / エージェント:

`https://*.wem.cloud.com`

完全な要件については、Workspace Environment Management サービスのドキュメントの接続の前提条件を参照してください。

デプロイメントを計画する

この記事では、Citrix Cloud™のデプロイメントを計画する際の主要な考慮事項について概説します。サービス試用版、クラウドサブスクリプション、リージョン、およびデプロイメントと移行のためのリソースの概要を説明します。

サービス試用版とサブスクリプション

Citrix Cloudは、ほとんどのクラウドサービスで試用版を提供しています。試用版は有料サービスと同じ機能を持つため、概念実証またはパイロットデプロイメントに適しています。詳細については、「Citrix Cloud Service Trials」を参照してください。

一般に、有料サービスのエンタイトルメントは、月単位、年単位、または期間指定の期間を持つことができます。エンタイトルメントの期限が近づくと、Citrix Cloudはリマインダーを送信し、不必要なサービス中断なしにエンタイトルメントを更新できるようにします。エンタイトルメントの更新の詳細については、「Extend Citrix Cloud service subscriptions」を参照してください。

リージョンとサービスプレゼンス

Citrix Cloudは、米国、欧州連合、アジア太平洋南部の3つのリージョンでサービスを提供しています。Citrix Cloudにサインアップする際は、パフォーマンスとビジネスニーズに最適なリージョンを選択する必要があります。

リージョンの選択と各リージョンで利用可能なサービスの詳細については、「Geographical Considerations」を参照してください。

デプロイメントリソース

- Citrix Cloud の回復力
- Tech Zone の概念実証ガイド
- Tech Zone のリファレンスアーキテクチャ
- Cloud Connector のスケールとサイズに関する考慮事項
- ローカルホストキャッシュのスケールとサイズに関する考慮事項
- Citrix DaaS 向けオンプレミス StoreFront 認証リファレンスアーキテクチャ

移行リソース

- 概念実証: 自動構成ツール
- Citrix Virtual Apps and DesktopsオンプレミスからCitrix Cloudへの移行
- ヴイエムウェア ブイスフィアからマイクロソフト アジュール上のシトリックス ダースへのシトリックス バーチャルアップス アンド デスクトップスの移行
- シトリックス エンドポイント マネジメントを使用したアンドロイド デバイス アドミニストレーターからアンドロイド エンタープライズへの移行

詳細情報

- Citrix Discussions: Citrix Cloud: Citrix CloudおよびCitrixクラウドサービスに関するコミュニティサポートフォーラム
- Citrixトレーニング:
  - Citrix Cloudの基礎
  - シトリックス ID および認証の概要

Citrix Cloud™ サービス トライアル

個々のCitrix Cloudサービス向けトライアルは、Citrix Cloud管理コンソールを通じて提供されます。サービス トライアルの機能は、購入したサービスと同じであるため、概念実証 (POC) やパイロット展開に適しています。

Citrix Cloudサービスを購入する準備が整ったら、トライアルは本番サービスに変換されます。何も再構成したり、個別の本番アカウントを作成したりする必要はありません。

サービス トライアルの概要

このセクションの情報は、ほとんどのCitrix Cloudサービス トライアルに適用されます。トライアル条件が異なるサービスについては、別のセクションで説明しています。

	CITRIX CLOUD トライアル
許可されるエンドユーザー数	25
トライアルの最大期間	60暦日
データ保持期間	トライアルの有効期限切れ後90暦日

	CITRIX CLOUD トライアル
利用可能性	制限付き利用可能性
リソースの場所	顧客が提供し、構成
ユーザーセッションの長さ	無制限
ローカルのMicrosoft Active Directory統合	はい
リソースロケーションの選択	はい
オンプレミスへの展開	はい
シトリックス デスクトップ・アズ・ア・サービス (旧称: シトリックス バーチャルアプリ&デスクトップ™ サービス)	全機能セット
エンドポイント管理	全機能セット
カスタマイズ可能	はい

サービス試用版のリクエスト

Citrix Cloudの試用版アクセスは、サービスごとに管理されます。一部のサービスでは、この記事のサービス試用版のリクエストで説明されているように、試用版をリクエストできます。その他のサービスでは、試用版アクセスを受け取る前に、この記事のサービスデモのリクエストで説明されているように、デモをリクエストする必要があります。

サービス試用期間

ほとんどのサービスでは、試用版のリクエストが承認されてから60日間、サービスを試用できます。サービスの試用版は1回のみリクエストできます。

サービスサブスクリプションの購入

試用期間中またはデータ保持期間中であれば、いつでもサービスサブスクリプションを購入できます。詳しくは、Citrix Cloudサービスの購入を参照してください。

サブスクリプションを購入すると、試用版は本番サービスに変換されます。管理者とユーザーはサービスにアクセスでき、試用期間中に追加したデータはすべてそのまま保持されます。

Azure 向け Citrix DaaS スタンダード

このセクションでは、Citrix DaaS Standard for Azure（旧称：Citrix Virtual Apps and Desktops Standard for Azure）の以下の種類の試用版について説明します。

- **自動承認試用版:** Citrix Cloud管理コンソールから試用版をリクエストすると、試用版は自動的に承認され、すぐに使用できます。
- **営業担当者承認試用版:** Citrix®の営業担当者に連絡して試用版をリクエストすると、営業担当者が試用版を承認します。承認後、試用版はすぐに使用できます。

	自動承認試用版	営業担当者承認試用版
試用期間の最大長	7暦日	14暦日
データ保持期間	トライアルの有効期限切れ後30暦日	トライアルの有効期限切れ後90暦日

トライアルの種類に応じて、サービスを使用できる期間は7日間または14日間です。サービスのトライアルをリクエストできるのは1回のみです。

トライアルの種類に応じて、Citrixは、トライアルの有効期限が切れてから30日間または90日間、お客様がサービスに追加したデータを保持します。この保持期間中にサービスのサブスクリプションを購入した場合、管理者とユーザーはデータがそのままの状態でサービスにアクセスできます。

サービスのサブスクリプションは、Azure Marketplaceを通じて、またはCitrixの営業担当者に連絡することで購入できます。

サービスデモをリクエストする

一部のサービスでは、サービスを試す前にCitrixの営業担当者にデモをリクエストする必要があります。デモをリクエストすることで、組織のクラウドサービスのニーズについてCitrixの営業担当者と話し合うことができます。また、営業担当者は、サービスを正常に使用するために必要なすべての情報が揃っていることを確認します。

1. Citrix Cloudアカウントにサインインします。
2. 管理コンソールから、目的のサービスに対して**Request Demo**を選択します。サービスのデモリクエストページが表示されます。
3. フォームに記入して送信します。Citrixの営業担当者がお客様に連絡し、詳細情報を提供し、サービスの使用方法を説明します。

サービス試用版をリクエストする

1. Citrix Cloudアカウントにサインインします。
2. 管理コンソールから、試用したいサービスに対して**Request Trial**を選択します。

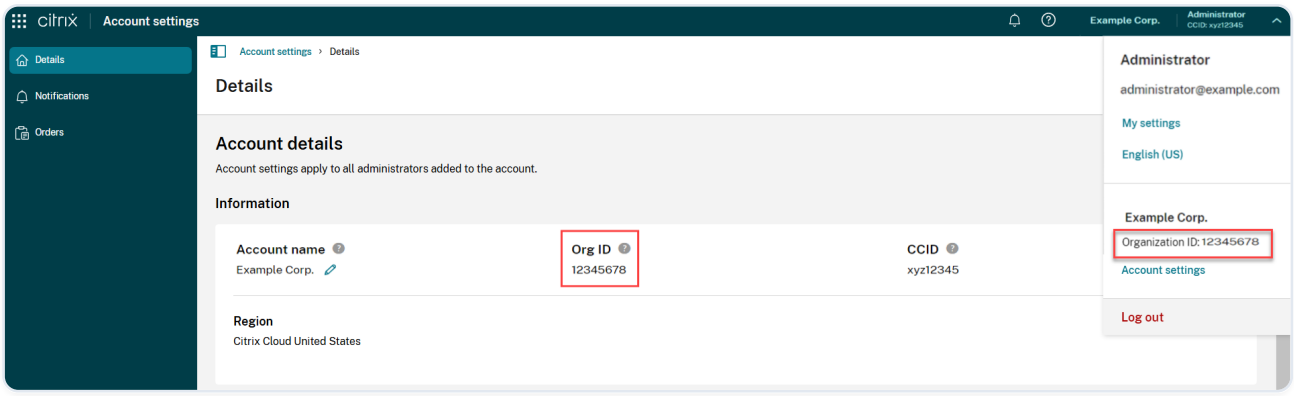
トライアルが承認され、使用可能になったら、Citrix からメール通知が送信されます。

> **注:**
>
> 最高の顧客エクスペリエンスを提供するため、Citrix は、いつでも限られた数の参加者に対してのみトライアルを承認する権利を留保します。

Citrix Cloud サービスを購入する

トライアルを本番サービスに変換する準備ができたら、https://www.citrix.com/buy/ にアクセスして、お近くの Citrix パートナーを見つけてください。

サービスを購入するには、組織ID (OrgID) が必要です。OrgID は、Citrix Cloud 管理コンソールの右上隅にある顧客メニューに表示されます。OrgID は、**アカウント設定**ページにも表示されます。



詳細情報

- Citrix Cloud サービスの利用規約
- Citrix Cloud の基礎 コースには、トライアルのリクエスト方法を説明する短いビデオが含まれています。このフルコースでは、Citrix Cloud プラットフォームとそのサービスのコンポーネントについても説明しています。

Citrix Cloud™ サービスサブスクリプションの延長

この記事では、Citrix Cloudサービスの購入済みサブスクリプションの有効期限が切れる仕組みと、サブスクリプションを延長する方法について説明します。

In this article, *monthly subscriptions* refer to services that are purchased on a month-to-month basis. *Annual subscriptions* refer to services that are purchased on a yearly basis. *Multiannual subscriptions* refer to services that are purchased on a multi-yearly basis.

> **注：**

> Citrix Service Providers (CSPs) can extend their subscriptions by submitting a zero-dollar purchase order to their CSP distributor. For more information about CSP product renewals and licensing, refer to the *Citrix Service Provider Licensing Guide for Citrix Cloud*, available through the Citrix Partner Central web site.

有効期限前

月次サブスクリプションの場合、Citrix Cloudは有効期限が切れる前に通知を送信しません。

年間および複数年サブスクリプションの場合、Citrix Cloudは既存のサブスクリプションの有効期限が近づくと、特定の期間で通知します。これらの通知は、サブスクリプションを延長してサービスの中断を回避するよう警告します。以下の通知がCitrix Cloud管理コンソールに表示されます。

- 有効期限の90日前：延長が必要なサービスとその有効期限を示す黄色のバナーが表示されます。この通知は、7日ごと、またはサービスが延長されるまでコンソールに表示されます。
- 有効期限の7日前：延長が必要なサービスとその有効期限を示す赤色のバナーが表示されます。この通知は、サービスが延長されるまでコンソールに表示されます。

これらの通知は表示されたときに閉じることができますが、7日後に再表示されます。

Citrix®は、延長が必要なサービスとその有効期限のリストを含むメール通知も送信します。Citrixは、以下の間隔でこの通知を送信します。

- 有効期限の90日前
- 有効期限の60日前
- 有効期限の30日前
- 有効期限の7日前
- 有効期限の1日前

有効期限の状態を通知するため、管理コンソールおよびエンドユーザーに追加の警告が表示されます。これらのメッセージは、サブスクリプション内のすべてのライセンスの有効期限が切れたとき（通常、12か月の期間が完了した後）にトリガーされます。

- 管理者への警告: サブスクリプションの有効期限が切れる30日前から、Studioコンソール内に警告が表示され、管理者に今後の有効期限を通知します。
- エンドユーザーへの警告: サブスクリプションの有効期限が切れた後、エンドユーザーはセッションを起動する際に警告メッセージを受け取ります。
    - メッセージテキスト: 「Citrix Virtual Apps and Desktops 警告: お客様の企業Citrix環境は現在サポートされていません。解決するにはIT部門にお問い合わせください。」

有効期限切れ後: サービスブロックとデータ保持

- Citrix Cloudサービスへのアクセスは、契約の有効期限が切れると直ちに停止されます。
- サービスを再開するには、お客様は担当のCitrix担当者またはアカウントチームに連絡して、更新プロセスを開始する必要があります。

お客様が管理するAzureサブスクリプション

Citrix Cloudサービスで独自のAzureサブスクリプションを使用している場合、Azureサブスクリプションをサービスに接続すると、サービスによってアプリがインストールされます。Citrix Cloudサービスサブスクリプションを延長しない場合、90日間の保持期間が終了しても、CitrixはこのアプリをAzureサブスクリプションから削除しません。サービスをAzureサブスクリプションから完全に削除するには、このアプリを削除する必要があります。アプリは次のいずれかの方法で削除できます。

- 管理者がまだサービスへのアクセスをブロックされていない場合は、サービス内からこのアプリを削除します。
- 管理者がサービスへのアクセスをブロックされている場合は、Azureポータル内からこのアプリを削除します。

サービス拡張機能の購入

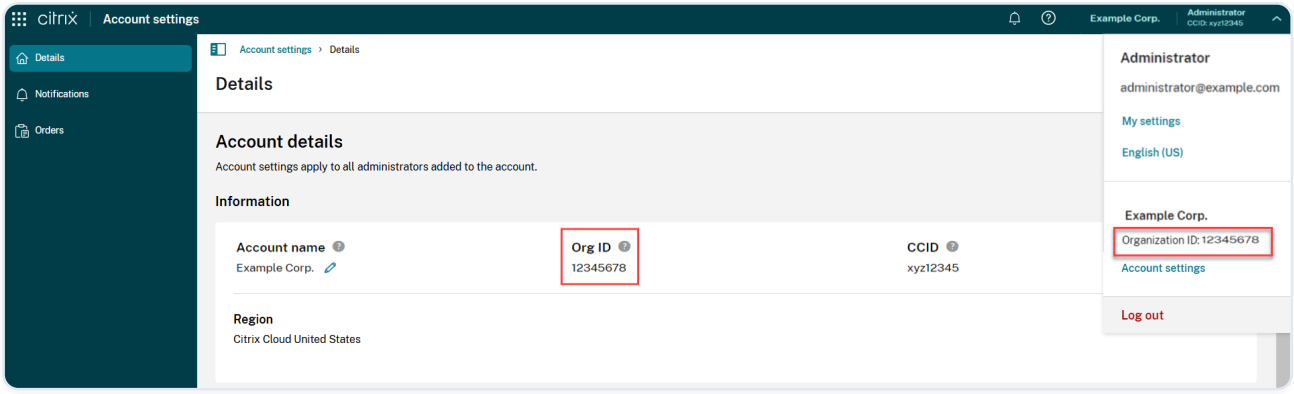
Citrix Cloudサービスへのサブスクリプションを延長するには、Citrixの営業担当者にお問い合わせください。営業担当者を見つけるには、次の手順を使用します。

1. Citrixアカウントにサインインします。
2. **Quoting (DOTI)** を選択し、次に **Transactions** を選択します。このビューの上部に、営業担当者とそのメールアドレスが表示されます。

または、お住まいの地域の連絡先情報については、Citrix Customer Service ページをご覧ください。

購入を完了するには、営業担当者にCitrix Cloudアカウントの組織IDが必要です。組織IDを見つけるには、Citrix Cloudアカウントにサインインします。組織IDは次の場所に表示されます。

- Citrix Cloudコンソールの右上隅にある顧客メニュー内。
- **アカウント設定**ページ。



地理的考慮事項

この記事では、Citrix Cloud™ が使用する商用リージョンと、各リージョンにおける Citrix Cloud 商用サービスの存在について説明します。

Citrix の公共部門および専用クラウドプラットフォームの地理的リージョンとサービスプレゼンスの詳細については、「Citrix のその他のクラウドプラットフォーム」(#other-cloud-platforms-from-citrix)を参照してください。

リージョンの選択

組織が Citrix Cloud にオンボーディングされ、初めてサインインするときに、次のいずれかのリージョンを選択するよう求められます。

- 米国
- 欧州連合
- アジア太平洋南部

リージョンを選択すると、可能な限り、その地理的リージョンでホストされているサービスが組織に関連するアクションに使用されます。ほとんどのユーザーとリソースが配置されている場所にマッピングされるリージョンを選択してください。

Citrix Cloud リージョン選択ページ(/en-us/citrix-cloud/media/region-select-v2.png)

> **重要な注意事項:**

- リージョンは、組織がオンボーディングされるときに一度だけ選択できます。後でリージョンを変更することはできません。
- あるリージョンにいて、別のリージョンのサービスを使用する場合でも、パフォーマンスへの影響は最小限です。Citrix Cloud サービスは、グローバルに利用できるように設計されています。たとえば、米国のお客様がオーストラリアにユーザーとコネクタを持っている場合でも、遅延による影響は最小限に抑えられます。
- お使いのリージョンで Citrix Cloud がサポートされていない場合は、ほとんどのユーザーとリソースが配置されている場所に最も近いリージョンを選択してください。

各リージョンでのサービスプレゼンス

ほとんどのCitrix Cloudサービスはグローバルにレプリケートされます。選択したリージョンは、接続が行われる場所の優先順位を示します。ただし、接続は他の地理的リージョンにも行われる可能性があります。サービスがグローバルにレプリケートされる場合、そのサービスのすべてのデータはすべてのリージョンに保存されます。

同様に、サービスを実行するために必要な場合、Citrixの関連会社またはサブプロセッサーによってお客様のデータがグローバルに処理されることがあります。

特定のサービスには専用のリージョンインスタンスがあります。一部のサービスには米国ベースのインスタンスのみがあります。これらの場合、接続とデータは地理的リージョン内に保持されます。

組織用に選択したリージョンでサービスが利用できない場合、特定の情報（認証データなど）が必要に応じてリージョン間で転送されることがあります。

サービス	米国	EU	アジア太平洋南部	注
Citrix Cloudコントロールプレーン	はい	はい	はい	
シトリックス アナリティクス フォー セキュリティ™	はい	はい	はい	

CITRIX CLOUD™

サービス	米国	EU	アジア太平洋南部	注
シトリックス アナリティクス フォー パフォーマンス™	はい	はい	はい	
NetScaler® コンソール (旧称 アプリケーション デリバリー マネジメント)	はい	はい	はい	この記事の Low-touch onboarding of NetScaler instances using Console Advisory Connectを参照してください。
				オンプレミスコンソールテレメトリプログラムについては、(https://docs.netscaler.com/ja-jp/netscaler-application-delivery-management-software/130-adm-0443.html)を参照してください。
Citrix DaaS™ (旧称 Virtual Apps and Desktopsサービス)	はい	はい	はい	サービスは Citrix Cloud リージョンを使用します。
シトリックス DaaS スタンダード Azure向	はい	はい	はい	サービスは Citrix Cloud

サービス	米国	EU	アジア太平洋南部	注
け (旧称 Virtual Apps and Desktops スタンダード Azure 向け)				リージョンを使用します。
シトリックス DaaS スタンダード Google Cloud向け (旧称 Virtual Apps and Desktops スタンダード Google Cloud向け)	はい	いいえ (米国リージョンを使用)	いいえ (米国リージョンを使用)	
シトリックス DaaS プレミアム for Google Cloud (旧称 バーチャルアプリ＆デスクトップ プレミアム for Google Cloud)	はい	いいえ (米国リージョンを使用)	いいえ (米国リージョンを使用)	
シトリックス エンドポイントマネジメント™	はい	はい	はい	複数のリージョンにわたる複数の場所から選択します。この記事のEndpoint Management service locationsを参照してください。
リモートブラウザ分離サービス	はい	はい	はい	サービスは Citrix Cloud リージョンを使用します。

サービス	米国	EU	アジア太平洋南部	注
SD-WAN オーケストレーター	はい	はい	はい	
シトリックス セキュア プライベート アクセス™	グローバルにレプリケート	グローバルにレプリケート	グローバルにレプリケート	この記事の Secure Private Accessのプレゼンスポイント を参照してください。
Session Recordingサービス	はい	はい	はい	
シトリックス バーチャル アプリ エッセンシャルズ™	はい	はい	はい	サービスは Citrix Cloud リージョンを使用します。
シトリックス バーチャル デスクトップ エッセンシャルズ™	はい	はい	はい	サービスは Citrix Cloud リージョンを使用します。
Web アプリケーション ファイアウォール	はい	はい	いいえ（米国リージョンを使用）	
ワークスペース環境管理™; Citrix 最適化パック	はい	はい	はい	
ネットワークサービス	はい	いいえ（米国リージョンを使用）	いいえ（米国リージョンを使用）	
ライセンス使用状況インサイト（CSPのみ）	グローバルにレプリケート	グローバルにレプリケート	グローバルにレプリケート	

サービス	米国	EU	アジア太平洋南部	注
シトリックス ゲートウェイ サービス アクセスノード/ポップ	複数のWWノード。最高の体験を保証するために必要に応じてトラフィックがルーティングされます。	複数のWWノード。最高の体験を保証するために必要に応じてトラフィックがルーティングされます。	複数のWWノード。最高の体験を保証するために必要に応じてトラフィックがルーティングされます。	ユーザーのトラフィックを特定のリージョンにルーティングできるように、リソースの場所を構成できます。詳細については、「地理的位置ルーティング - プレビュー」を参照してください。
ライセンスアクティベーション サービス	はい	はい	はい	

注:

特定の地域サービスは、上記の表に別途記載されている非地域コンポーネントサービスへのエンタイトルメントとともに提供される場合があり、お客様の選択により使用できます。

Citrix Cloudサービスは、お客様が指定した地域を使用して顧客コンテンツとログを保存します。ただし、Citrixのサブプロセッサーによって収集された一部のログ、またはサービスのパフォーマンスのために非地域ストレージが必要な場合は除きます。これには、サポートやトラブルシューティング、パフォーマンス監視、セキュリティ、監査、およびクロスリージョン認証を可能にするため（たとえば、EUを拠点とするサポートエンジニアが米国を拠点とする環境にアクセスする必要がある場合など）が含まれます。顧客コンテンツとログは、サービスを実行するために必要に応じてグローバルにアクセスされる場合があります。

個々のサービスによって保存されるデータに関する詳細については、各サービスの技術セキュリティ概要を参照してください。

Console Advisory Connectを使用したNetScaler Consoleインスタンスのロータッチオンボーディング

Console Advisory ConnectベースのConsoleインスタンスのロータッチオンボーディングの一部として、次のようになります。

- 既存のCitrix Cloudのお客様の場合、Consoleサービステナントは、Citrix Cloudアカウントを作成したときに選択したのと同じ地理的地域に作成されます。
- 既存のCitrix Cloudのお客様でない場合、Citrix.comポータルでそのお客様について言及されているアドレスが参照されます。この参照されたアドレスの地域に対応する地理的地域に、プレースホルダーのConsoleサービステナントが作成されます。将来Citrix Cloudにオンボーディングすることを選択した場合、Citrix Cloudアカウントを作成するときに選択したのと同じ地域に新しいConsoleサービステナントが作成されます。また、データはプレースホルダーのConsoleサービステナントから新しいConsoleサービステナントに移行されます。

Endpoint Managementサービスの場所

ホーム地域から以下のEndpoint Managementサービスの場所のいずれかを選択できます。

- 米国東部
- 米国西部
- EU西部
- 東南アジア
- シドニー

Secure Private Access のプレゼンスポイント

Secure Private Access が顧客へのサービスの継続性と品質を確保するために使用するプレゼンスポイント (PoP) のリストについては、Secure Private Access サービスドキュメントの「Secure Private Access PoP の場所はどこですか?」を参照してください。

Pendo のデータレジデンシーと地域に関する考慮事項

Citrix は Pendo を使用して、さまざまな製品やサービスで製品内ガイダンス、機能発表、および重要な通知を提供しています。Pendo によって収集されたすべてのデータは、米国 (US) 地域内でのみ処理および保存されます。

このデータレジデンシーは、以下の Citrix 製品およびサービスの **Pendo 処理データ**にのみ適用されます。

- Citrix Cloud 管理コンソール

- Citrix DaaS（ワークスペース環境管理、ウェブスタジオ、セッションレコーディングを含む）
- Citrix Studio (オンプレミス)
- Citrix Directorおよびモニター
- NetScaler (ADC)
- NetScaler Console (ADM) および NetScaler Console サービス
- セキュア デベロッパー スペース
- Citrix Workspace アプリ (デスクトップ、モバイル、タブレット – クラウド展開のみ)
- iOS用Citrix Workspaceアプリ (ネイティブ)
- Android用Citrix Workspaceアプリ (ネイティブ)

Citrixのその他のクラウドプラットフォーム

Citrix Cloudに加えて、CitrixはCitrix Cloudから分離された他のクラウドも提供しています。

Citrix Cloud ガバメント

Citrix Cloud Governmentは、米国の政府機関やその他の公共部門のお客様が、規制およびコンプライアンス要件に従ってCitrixクラウドサービスを利用できるようにします。Citrix Cloud Governmentは、CitrixがCitrix Cloud Governmentサービスを提供するために、サービスとデータを運用、保存、複製する地理的境界です。Citrixは、サービスを提供するために、米国内の1つまたは複数の州に配置された複数のパブリッククラウドまたはプライベートクラウドを使用する場合があります。

Citrix Cloud Governmentおよび提供されるサービスは、米国地域でのみ利用可能です。

詳細については、Citrix Cloud Government製品ドキュメントを参照してください。

Citrix Cloud ジャパン

Citrix Cloud Japanは、日本のお客様が専用のCitrix管理環境で特定のCitrix Cloudサービスを利用できるようにします。Citrix Cloud Japanおよび提供されるサービスは、日本でのみ利用可能です。

詳細については、Citrix Cloud Japan製品ドキュメントを参照してください。

Citrix Cloud™ Platform のセキュア展開ガイド

Citrix Cloud のセキュア展開ガイドでは、Citrix Cloud の使用におけるセキュリティのベストプラクティスの概要と、Citrix Cloud が収集および管理する情報について説明します。

サービスに関する技術セキュリティの概要

Citrix Cloud サービス内のデータセキュリティに関する詳細については、以下の記事を参照してください。

- アナリティクス技術セキュリティ概要
- Endpoint Management 技術セキュリティ概要
- リモートブラウザ分離技術セキュリティ概要
- Citrix DaaS 技術セキュリティ概要
- Citrix DaaS Standard for Azure 技術セキュリティ概要

管理者向けガイダンス

- 強力なパスワードを使用し、定期的にパスワードを変更してください。
- 顧客アカウント内のすべての管理者は、他の管理者を追加および削除できます。信頼できる管理者のみが Citrix Cloud にアクセスできるようにしてください。
- 顧客の管理者は、デフォルトで、すべてのサービスへのフルアクセス権を持っています。一部のサービスでは、管理者のアクセスを制限する機能が提供されています。詳細については、サービスごとのドキュメントを参照してください。
- Citrix Cloud 管理者向けの二要素認証は、デフォルトの Citrix ID プロバイダーを使用して実現されます。管理者が Citrix Cloud にサインアップするか、Citrix Cloud アカウントに招待された場合、多要素認証 (MFA) への登録が求められます。顧客が Microsoft Azure を使用して Citrix Cloud 管理者を認証する場合、多要素認証は Microsoft Web サイトの Configure Microsoft Entra ID Multi-Factor Authentication settings に記載されているとおりに構成できます。
- デフォルトでは、Citrix Cloud はコンソールアクティビティに関係なく、72 時間後に管理者セッションを自動的に終了します。このタイムアウトは変更できません。
- 管理者アカウントは最大100の顧客アカウントに関連付けることができます。管理者が100を超える顧客アカウントを管理する必要がある場合、追加の顧客アカウントを管理するために、別のメールアドレスで別の管理者アカウントを作成する必要があります。あるいは、管理する必要がなくなった顧客アカウントから管理者として削除することもできます。

パスワードのコンプライアンス

以下のいずれかの条件に該当する場合、Citrix Cloudは管理者にパスワードの変更を促します。

- 現在のパスワードが60日以上サインインに使用されていない。
- 現在のパスワードが、既知の侵害されたパスワードのデータベースにリストされている。

新しいパスワードは、以下のすべての条件を満たす必要があります。

- 8文字以上（最大128文字）
- 大文字と小文字をそれぞれ1文字以上含む
- 数字を1文字以上含む
- 特殊文字を1文字以上含む: ! @ # $ % \^ * ? + = -

パスワード変更のルール:

- 現在のパスワードを新しいパスワードとして使用することはできません。
- 過去5つのパスワードは再利用できません。
- 新しいパスワードは、アカウントのユーザー名と類似していてはなりません。
- 新しいパスワードは、既知の侵害されたパスワードのデータベースにリストされていてはなりません。Citrix Cloudは、新しいパスワードがこの条件に違反しているかどうかを判断するために、https://haveibeenpwned.com/が提供するリストを使用します。

暗号化とキー管理

Citrix Cloudコントロールプレーンは、機密性の高い顧客情報を保存しません。代わりに、Citrix Cloudは、管理者パスワードなどの情報をオンデマンドで（管理者に明示的にプロンプトを表示して）取得します。

保存データの場合、Citrix CloudストレージはAES-256ビット以上のキーを使用して暗号化されます。これらのキーはCitrixによって管理されます。

転送データの場合、Citrixは業界標準のTLS 1.2と最強の暗号スイートを使用します。Citrix CloudはCitrixが所有するcloud.comドメインでホストされているため、お客様は使用中のTLS証明書を制御できません。Citrix Cloudにアクセスするには、お客様はTLS 1.2に対応したブラウザを使用し、承認された暗号スイートが構成されている必要があります。

次の強力な暗号が推奨されます: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

> **注:**

> TLS 1.2は必須ですが、一部のサービスではセキュリティとパフォーマンスを向上させるためにTLS 1.3をネゴシエートできます。お客様は、クライアントがTLS 1.2とTLS 1.3の両方をネゴシエートできるようにすることをお勧めします。次の強力な暗号が推奨されます:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Citrix Cloudサービスのデータがどのように保護されているかについては、Citrix WebサイトのCitrix Cloud Services Data Protection Overviewを参照してください。

各クラウドサービス内の暗号化とキー管理の詳細については、サービスのドキュメントを参照してください。

データ主権

Citrix Cloudコントロールプレーンは、米国、欧州連合、およびオーストラリアでホストされています。お客様はこれを制御できません。

お客様は、Citrix Cloudで使用するリソースの場所を所有および管理します。リソースの場所は、お客様が希望する任意のデータセンター、クラウド、場所、または地理的領域に作成できます。すべての重要なビジネスデータ（ドキュメント、スプレッドシートなど）はリソースの場所に保存され、お客様の管理下にあります。

その他のサービスでは、データを異なるリージョンに保存するオプションがある場合があります。各サービスについては、Geographical ConsiderationsトピックまたはTechnical Security Overviews（この記事の冒頭に記載）を参照してください。

セキュリティ問題に関する洞察

ウェブサイトstatus.cloud.comは、お客様に継続的な影響を与えるセキュリティ問題に関する透明性を提供します。このサイトには、ステータスと稼働時間情報が記録されています。プラットフォームまたは個々のサービスへの更新を購読するオプションがあります。

シトリックス クラウド コネクタ™

Cloud Connectorのインストール

セキュリティとパフォーマンスの理由から、Citrix®は、お客様がCloud Connectorソフトウェアをドメインコントローラーにインストールしないことを推奨しています。

また、Citrixは、Cloud Connectorソフトウェアがインストールされているマシンが、お客様のプライベートネットワーク内にあり、DMZ内にないことを強く推奨しています。ネットワークおよびシステム要件、ならびにCloud Connectorのインストール手順については、Citrix Cloud Connectorを参照してください。

Cloud Connectorの構成

お客様は、Cloud ConnectorがインストールされているマシンをWindowsセキュリティ更新プログラムで最新の状態に保つ責任があります。

お客様は、Cloud Connectorと並行してウイルス対策ソフトウェアを使用できます。Citrixは、業界標準のAV製品を使用するお客様をサポートしています。

お客様のActive Directory (AD) では、CitrixはCloud Connectorのマシンアカウントを読み取り専用アクセスに制限することを強く推奨しています。これはActive Directoryのデフォルト構成です。また、お客様はCloud ConnectorのマシンアカウントでADログ記録と監査を有効にして、ADアクセスアクティビティを監視できます。

Cloud Connectorをホストするマシンへのログオン

Cloud Connectorは、機密性の高いセキュリティ情報がCitrix Cloudサービスの他のプラットフォームコンポーネントに渡されることを許可しますが、以下の機密情報も保存します。

- Citrix Cloudとの通信用のサービスキー
- Citrix DaaS (旧Citrix Virtual Apps and Desktops™サービス) における電源管理用のハイパーバイザーサービス資格情報

この機密情報は、Cloud ConnectorをホストするWindowsサーバー上でData Protection API (DPAPI) を使用して暗号化されます。Citrixは、最も特権のある管理者のみがCloud Connectorマシンにログオンすること (たとえば、メンテナンス操作を実行するため) を強く推奨しています。一般的に、管理者がCitrix製品を管理するためにこれらのマシンにログオンする必要はありません。Cloud Connectorはその点で自己管理型です。

エンドユーザーがCloud Connectorをホストするマシンにログオンすることを許可しないでください。

Cloud Connectorマシンへの他のソフトウェアのインストール

お客様は、Cloud Connectorがインストールされているマシンに、アンチウイルスソフトウェアやハイパーバイザーツール（仮想マシンにインストールされている場合）をインストールできます。ただし、Citrixは、これらのマシンに他のソフトウェアをインストールしないことを推奨します。他のソフトウェアは、潜在的なセキュリティ攻撃ベクトルを生み出し、Citrix Cloudソリューション全体のセキュリティを低下させる可能性があります。

インバウンドおよびアウトバウンドポートの設定

Cloud Connectorは、インターネットへのアクセスを伴うアウトバウンドポート443が開いている必要があります。Citrixは、Cloud Connectorがインターネットからアクセス可能なインバウンドポートを持たないことを強く推奨します。

お客様は、Cloud ConnectorをWebプロキシの背後に配置して、そのアウトバウンドインターネット通信を監視できます。ただし、WebプロキシはSSL/TLS暗号化通信をサポートしている必要があります。

Cloud Connectorは、インターネットへのアクセスを伴う他のアウトバウンドポートを持つ場合があります。他のポートが利用可能な場合、Cloud Connectorは広範囲のポート間でネゴシエートし、ネットワーク帯域幅とパフォーマンスを最適化します。

Cloud Connectorは、内部ネットワーク内で広範囲のインバウンドおよびアウトバウンドポートを開いている必要があります。以下の表に、必要なオープンポートの基本セットを示します。

クライアントポート	サーバーポート	サービス
49152 -65535/UDP	123/UDP	W32タイム
49152 -65535/TCP	135/TCP	RPC エンドポイントマッパー
49152 -65535/TCP	464/TCP/UDP	Kerberos パスワード変更
49152 -65535/TCP	49152-65535/TCP	エルエスエー、サム、ネットログオン 用 アールピーシー (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	ケルベロス
49152 -65535/TCP/UDP	445/TCP	SMB

Cloud Connector は、LDAP 署名とシーリングを使用して、ドメインコントローラーへの接続を保護します。これにより、LDAP over SSL (LDAPS) は不要になります。LDAP 署名の詳細については、Windows Server での LDAP 署名を有効にする方法 および LDAP チャネルバインディングと LDAP 署名を有効にするための Microsoft ガイダンス を参照してください。

Citrix Cloud 内で使用される各サービスは、必要なオープンポートのリストを拡張します。詳細については、以下のリソースを参照してください。

- 各サービスに関する(secure-deployment-guide-for-the-citrix-cloud-platform.html) (この記事の冒頭に記載)
- Citrix Cloud サービスに関する(requirements/internet-connectivity-requirements.html)
- コンソールサービスポートの要件
- Endpoint Managementポートの要件

送信通信の監視

Cloud Connectorは、Citrix CloudサーバーとMicrosoft Azure Service Busサーバーの両方に対して、ポート443でインターネットにアウトバウンド通信を行います。

Cloud Connectorは、Cloud Connectorをホストするマシンが存在するActive Directoryフォレスト内のローカルネットワーク上のドメインコントローラーと通信します。

通常の操作中、Cloud Connectorは、Citrix Cloudユーザーインターフェイスの****ページで無効になっていないドメインのドメインコントローラーとのみ通信します。

Citrix Cloud内の各サービスは、Cloud Connectorが通常の操作中に接続する可能性のあるサーバーと内部リソースのリストを拡張します。また、お客様はCloud ConnectorがCitrixに送信するデータを制御できません。サービスの内部リソースとCitrixに送信されるデータに関する詳細については、以下のリソースを参照してください。

- 各サービスの技術セキュリティ概要（この記事の冒頭に記載）
- Citrix Cloudサービスのインターネット接続要件

Cloud Connectorログの表示

管理者に関連する、または管理者が対処できる情報はすべて、Cloud ConnectorマシンのWindowsイベントログで確認できます。

Cloud Connectorのインストールログは、次のディレクトリで確認できます。

- %AppData%\\Local\\Temp\\CitrixLogs\\CloudServicesSetup

- %windir%\\Temp\\CitrixLogs\\CloudServicesSetup

クラウド コネクタがクラウドに送信するログは、%ProgramData%\\Citrix\\WorkspaceCloud\\Logsにあります。

WorkspaceCloud\\Logsディレクトリ内のログは、指定されたサイズしきい値を超えると削除されます。管理者は、レジストリキーHKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CloudServices\\AgentAdministration\\MaximumLogSpaceMegabytesの値を調整することで、このサイズしきい値を制御できます。

SSL/TLS構成

Cloud ConnectorをホストするWindows Serverには、暗号化とキー管理に詳述されている暗号が有効になっている必要があります。

Cloud Connectorは、Citrix Cloud SSL/TLS証明書およびMicrosoft Azure Service Bus SSL/TLS証明書が使用する認証局（CA）を信頼する必要があります。CitrixおよびMicrosoftは将来的に証明書とCAを変更する可能性がありますが、常に標準のWindows信頼済み発行元リストの一部であるCAを使用します。

Citrix Cloud内の各サービスには、異なるSSL構成要件がある場合があります。詳細については、各サービスの技術セキュリティ概要（この記事の冒頭に記載）を参照してください。

セキュリティコンプライアンス

セキュリティコンプライアンスを確保するため、Cloud Connectorは自己管理します。再起動を無効にしたり、Cloud Connectorに他の制限を設けたりしないでください。これらの操作は、重要な更新がある場合にCloud Connectorが自身を更新するのを妨げます。

お客様は、セキュリティ問題に対応するために他の措置を講じる必要はありません。Cloud Connectorは、セキュリティ修正を自動的に適用します。

クラウドサービス向けCitrix Connector™ Appliance

Connector Applianceのインストール

Connector Applianceはハイパーバイザー上でホストされます。このハイパーバイザーは、DMZではなくプライベートネットワーク内に配置する必要があります。

Connector Applianceが、デフォルトでアクセスをブロックするファイアウォール内にあることを確認してください。許可リストを使用して、Connector Applianceからの予期されるトラフィックのみを許可してください。

Connector Applianceをホストするハイパーバイザーに、最新のセキュリティ更新プログラムがインストールされていることを確認してください。

ネットワークおよびシステム要件、およびConnector Applianceのインストール手順については、Connector Appliance for Cloud Servicesを参照してください。

Connector Applianceをホストするハイパーバイザーへのログオン

Connector Applianceには、Citrix Cloudと通信するためのサービスキーが含まれています。Connector Applianceをホストするハイパーバイザーへのログオンは、最も特権のある管理者のみに許可してください（例えば、メンテナンス操作を実行するためなど）。一般的に、Citrix製品を管理するために管理者がこれらのハイパーバイザーにログオンする必要はありません。Connector Applianceは自己管理型です。

インバウンドおよびアウトバウンドポートの構成

Connector Applianceは、インターネットにアクセスするためにアウトバウンドポート443が開いている必要があります。Citrixは、Connector Applianceがインターネットからアクセス可能なインバウンドポートを持たないことを強く推奨します。

Connector Appliance を Web プロキシの背後に配置して、そのアウトバウンドインターネット通信を監視できます。ただし、Web プロキシは SSL/TLS 暗号化通信をサポートしている必要があります。

Connector Applianceは、インターネットにアクセスするための他のアウトバウンドポートを持つ場合があります。他のポートが利用可能な場合、Connector Applianceは広範囲のポート間でネゴシエートし、ネットワーク帯域幅とパフォーマンスを最適化します。

Connector Applianceは、内部ネットワーク内で広範囲のインバウンドおよびアウトバウンドポートを開いている必要があります。次の表に、必要なオープンポートの基本セットを示します。

接続方向	コネクタアプライアンス ポート	外部ポート	サービス
インバウンド	443/TCP	任意	ローカルWeb UI
アウトバウンド	49152-65535/UDP	123/UDP	NTP
送信	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
送信	67/UDP	68/UDP	DHCP とブロードキャスト

接続方向	コネクタアプライアンス ポート	外部ポート	サービス
送信	49152 -65535/UDP	123/UDP	W32タイム
送信	49152 -65535/TCP	464/TCP/UDP	Kerberos パスワード変更
送信	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
送信	49152 -65535/TCP	3268/TCP	LDAP GC
送信	49152 -65535/TCP/UDP	88/TCP/UDP	ケルベロス
送信	49152 -65535/TCP/UDP	445/TCP	SMB
送信	137/UDP	137/UDP	NetBIOSネームサービス
送信	138/UDP	138/UDP	NetBIOSデータグラム
送信	139/TCP	139/TCP	NetBIOSセッション

Citrix Cloud内で使用される各サービスは、必要なオープンポートのリストを拡張します。詳細については、以下のリソースを参照してください。

- 各サービスに関する技術セキュリティ概要（この記事の冒頭に記載）
- Citrix Cloudサービスに関するシステムおよび接続要件

送信通信の監視

Connector Applianceは、ポート443でCitrix Cloudサーバーにインターネット経由で送信通信を行います。

Citrix Cloud内の各サービスは、通常の操作中にConnector Applianceが接続する可能性のあるサーバーと内部リソースのリストを拡張します。また、お客様はConnector ApplianceがCitrixに送信するデータを制御できません。サービスの内部リソースおよびCitrixに送信されるデータに関する詳細については、以下のリソースを参照してください。

- 各サービスに関する技術セキュリティ概要（この記事の冒頭に記載）
- Citrix Cloudサービスに関するシステムおよび接続要件

Connector Applianceログの表示

さまざまなログファイルを含むConnector Applianceの診断レポートをダウンロードできます。このレポートの取得に関する詳細については、Connector Appliance for Cloud Servicesを参照してください。

SSL/TLS構成

コネクタアプライアンスには、特別なSSL/TLS構成は必要ありません。

Connector Applianceは、Citrix Cloud SSL/TLS証明書で使用される認証局（CA）を信頼します。Citrixは将来的に証明書とCAを変更する可能性がありますが、常にConnector Applianceが信頼するCAを使用します。

Citrix Cloud内の各サービスには、異なるSSL構成要件がある場合があります。詳細については、各サービス（この記事の冒頭に記載）の技術セキュリティ概要を参照してください。

セキュリティコンプライアンス

セキュリティコンプライアンスを確保するため、Connector Applianceは自己管理され、コンソールからログインすることはできません。

コネクタのセキュリティ問題に対応するために、他のアクションを実行する必要はありません。Connector Applianceは、セキュリティ修正を自動的に適用します。

Connector Applianceをホストするハイパーバイザーには、最新のセキュリティ更新プログラムがインストールされていることを確認してください。

Active Directory (AD) では、Connector Applianceのマシンアカウントを読み取り専用アクセスに制限することをお勧めします。これはActive Directoryのデフォルト設定です。また、お客様はConnector ApplianceのマシンアカウントでADログ記録と監査を有効にして、ADアクセスアクティビティを監視できます。

侵害されたアカウントを処理するためのガイダンス

- Citrix Cloudの管理者リストを監査し、信頼できない管理者を削除します。
- 会社のActive Directory内で侵害されたアカウントを無効にします。
- Citrixに連絡し、お客様のすべてのCloud Connectorに保存されている認証シークレットのローテーションを要求します。侵害の重大度に応じて、次のアクションを実行します。

- **低リスク:** Citrixは時間をかけてシークレットをローテーションできます。Cloud Connectorは正常に機能し続けます。古い認証シークレットは2〜4週間で無効になります。この期間中、予期しない操作がないことを確認するためにCloud Connectorを監視してください。
- **継続的な高リスク:** Citrixはすべての古いシークレットを取り消すことができます。既存のCloud Connectorは機能しなくなります。通常の操作を再開するには、お客様はすべての該当するマシンでCloud Connectorをアンインストールして再インストールする必要があります。

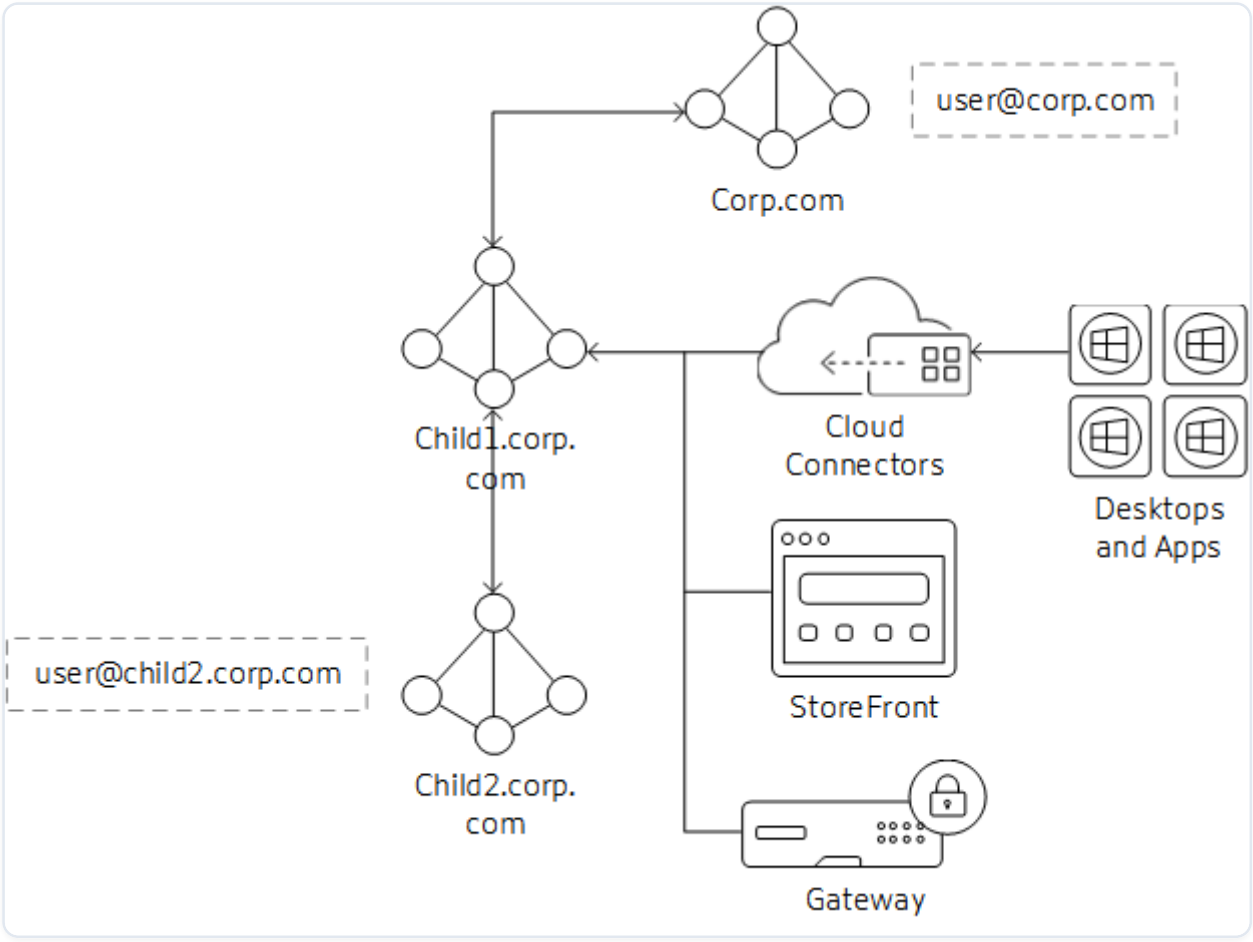
Citrix DaaS™ 向けオンプレミス StoreFront™ 認証リファレンスアーキテクチャ

Citrix® StoreFront Cloud は、Citrix DaaS (旧 Citrix Virtual Apps and Desktops™ サービス) のほとんどのユースケースの要件を満たすことができますが、StoreFront を顧客のデータセンターまたはリソースロケーションでホストする必要があるユースケースと要件がいくつかあります。この記事では、高レベルのアーキテクチャと、コンポーネントが Active Directory の設計でサポートされるさまざまな認証シナリオとどのように相互作用するかについて説明します。この記事では、StoreFront と Gateway コンポーネントが各データセンターで一緒にホストされていることを前提としています。

オンプレミス StoreFront を維持する理由

- インターネット接続がないクライアントをサポートする。
- 復元力を高めるために、ローカルホストキャッシュ機能を有効にする。
- ドメインパススルーおよびスマートカード認証。
- ストアプラグインなどの詳細なカスタマイズ。
- 異なる構成を持つ複数の StoreFront ストアをホストする。

リソースドメインとしての親子ドメイン



このシナリオでは、子ドメインが Virtual Desktop Agent (VDA) および StoreFront インスタンスのリソースドメインとして機能します。親ドメインには、子ドメインのリソースにアクセスするユーザーが保持されます。

1. Cloud Connector は子ドメインのみに参加します。子ドメインと親ドメイン間の双方向の推移的信頼により、Cloud Connector は親ドメインのグローバルカタログと通信できます。
2. StoreFront is joined to the child domain. Stores are configured for Username/Password and Pass-through from Citrix Gateway authentication. Username/Password authentication is configured to trust any domain.
3. Citrix Gateway 認証プロファイルは、UPN をプライマリログオン方法として使用するように親ドメイン用に構成されています。子ドメインから認証する必要があるユーザーがいる場合、子ドメインの LDAP 認証プロファイルとポリシーも Gateway vServer にバインドする必要があります。
4. Citrix Gateway セッション OS および Web プロファイルを編集し、公開アプリケーション/シングルサインオンドメイン設定を空白に設定します (上書き設定が必要な場合があります)。

接続ワークフロー

1. mailto:User@corp.com がCitrix Gatewayにログオンします。Gatewayは認証プロファイルを通じてユーザーを検索し、ポリシーアクションと照合します。
2. 資格情報はStoreFrontに渡されます。StoreFrontは資格情報を受け入れ、Cloud Connectorに渡します。
3. Cloud Connectorは、Citrix Cloudが必要とするユーザーオブジェクトの詳細を検索します。
4. Cloud ConnectorはID情報をCitrix Cloudに渡し、IDトークンがユーザーを認証し、ユーザーに割り当てられたリソースを列挙します。
5. Cloud Connectorは、ユーザー列挙のために割り当てられたリソースをStoreFrontに返します。
6. ユーザーがアプリケーションまたはデスクトップを起動すると、Citrix Gatewayは構成されたCloud Connectorを使用してSTAチケット要求を生成します。
7. Citrix Cloudブローカーは、リソースドメインのCloud Connectorと、そのリソースロケーションに登録されているVDA間のセッションを管理します。
8. クライアント、Citrix Gateway、および解決されたVDA間でセッションが確立されます。

リソースドメインへの外部信頼ドメイン

外部信頼ドメインからリソースドメインへ(/en-us/citrix-cloud/media/adv-concepts-external-trusted-resource-domain.png)

このシナリオでは、ビジネスパートナーは企業ユーザーに公開されているリソースへのアクセスを必要とします。企業ドメインはcorp.comで、パートナードメインはpartner.comです。

1. 企業ドメインはパートナードメインへの外部信頼を確立しています。パートナードメインのユーザーは、企業ドメインに参加しているリソースに対して認証できます。
2. Citrix Cloudのお客様は、2つのリソースロケーションを必要とします。1つはcorp.comのCloud Connector用、もう1つはpartner.comのCloud Connector用です。partner.comのCloud Connectorは、ドメインへの認証およびID呼び出しにのみ必要であり、VDAやセッションの仲介には使用されません。
3. StoreFrontサーバーはcorp.comドメインに参加しています。ストアは、corp.comドメイン内のCloud Connectorをリストするサイトで構成されています。ストアは、ユーザー名/パスワード認証とCitrix Gatewayからのパススルー認証用に構成されています。ユーザー名/パスワード認証は、任意のドメインを信頼するように構成されています。
4. Citrix Gateway認証プロファイルは、UPNをプライマリログオン方法として使用するようにcorp.comドメイン用に構成されています。UPNを使用するようにpartner.comドメイン用の2番

目のプロファイルとポリシーを構成し、corp.comドメインと同じGateway vServerにバインドします。

5. Citrix GatewayセッションOSおよびWebプロファイルを編集し、「公開アプリケーション/シングルサインオン ドメイン」設定を空白にします（オーバーライド設定が必要な場合があります）。

> **注：**
>
> 外部の信頼済みドメインの場所によっては、外部ドメインのユーザーは、リソースドメインまたは親ドメインのユーザーよりも起動時間が長くなる場合があります。

接続ワークフロー

1. mailto:User@partner.comがCitrix Gatewayにログオンします。Gatewayは、UPNルックアップと一致する認証プロファイルを通じてユーザーを検索し、ポリシーアクションと照合します。
2. 資格情報はStoreFrontに渡されます。StoreFrontは資格情報を受け入れ、Cloud Connectorsに渡します。
3. Cloud Connectorsは、Citrix Cloudに必要なユーザーオブジェクトの詳細を検索します。
4. Cloud ConnectorsはID情報をCitrix Cloudに渡し、IDトークンがユーザーを認証し、ユーザーに割り当てられたリソースを列挙します。
5. Cloud Connectorsは、ユーザー列挙のために割り当てられたリソースをStoreFrontに返します。
6. ユーザーがアプリケーションまたはデスクトップを起動すると、Citrix Gatewayは、構成されたCloud Connectors（この場合はchild1.corp.comから）を使用してSTAチケット要求を生成します。
7. Citrix Cloudブローカーは、リソースドメインのCloud Connectorsと、そのリソースの場所に登録されているVDA間のセッションを管理します。
8. クライアント、Citrix Gateway、および解決されたVDA間でセッションが確立されます。

リソースドメインへのフォレスト信頼/ショートカット信頼

フォレスト信頼およびショートカット信頼ドメインは、リソースドメインへの外部信頼関係として扱われる場合にのみサポートされます。フォレスト信頼の場合、「外部の信頼済みドメインからリソースドメインへ」セクションで説明されている手順と同じ手順に従うことができます。このセクションは、ユーザーとリソースドメイン/フォレスト間のネイティブフォレスト信頼のサポート状況に応じて、将来変更される可能性があります。

Citrix Cloud™ アカウントを作成する

この記事では、Citrix Cloud アカウントを作成し、アカウントを正常にオンボーディングするために必要なタスクを完了するプロセスについて説明します。

Citrix® と既存の関係があり、Citrix クラウドサービスを初めて利用するお客様は、この記事のタスクを使用してオンボーディングプロセスを完了できます。

新規 Citrix お客様のサインアッププロセス

Citrix および Citrix Cloud を初めてご利用になる場合は、Citrix に連絡して、会社用の新しい Citrix アカウントを作成する必要があります。以下のいずれかの連絡方法を使用してください。

- Citrix カスタマーサービス にお問い合わせください。
- お住まいの地域の Citrix パートナー または Citrix 営業所 にお問い合わせください。

Citrix に連絡すると、Citrix の担当者とビジネスニーズについて話し合うことができます。担当者は、サインアッププロセスを完了し、Citrix サインイン資格情報を提供するのに役立ちます。

Citrix アカウントの資格情報を受け取ったら、この記事のタスクを使用してサインインし、Citrix Cloud の利用を開始できます。

Citrix アカウントとは何ですか?

Citrix.com アカウントまたは My Citrix アカウントとも呼ばれる Citrix アカウントを使用すると、購入したライセンスへのアクセスを管理できます。Citrix アカウントは、一意の識別子として組織 ID (OrgID) を使用します。アカウントにリンクされている場合は、ユーザー名 (Web ログインとも呼ばれます) またはメールアドレスを使用して https://www.citrix.com にログインすることで、Citrix アカウントにアクセスできます。

> **重要:**

> ユーザー名は単一の一意の Citrix アカウントにマッピングされますが、メールアドレスは複数の Citrix アカウントにマッピングできます。

OrgID とは何ですか?

OrgID は、Citrix アカウントに割り当てられる一意の識別子です。OrgID は物理的なサイトアドレス、通常は会社の事業所住所に関連付けられています。通常、企業は単一の OrgID を持ちます。ただし、異なる支店がある場合や、異なる部門が資産を個別に管理している場合など、Citrix は単一の企業が複数の OrgID を持つことを許可する場合があります。

Citrix は定期的に特定の OrgID をクリーンアップし、場合によっては重複を統合します。会社に有効でアクティブな OrgID と統合したい OrgID がある場合は、統合したい OrgID を添えて Citrix カスタマーサポートに連絡できます。

> **注:**
>
> 企業は資産を管理する方法に基づいてすでに OrgID を設定しているため、使用する必要がある OrgID や所有している OrgID の数がわからない場合は、会社の IT 部門または Citrix 管理者に連絡してください。サポートが必要な場合は、OrgID を見つけるために、https://www.citrix.com/support/ の Citrix カスタマーサービスにお問い合わせください。

Citrix Cloud アカウントとは何ですか?

Citrix Cloud アカウントを使用すると、1つ以上のCitrixクラウドサービスを使用して、アプリとデータを安全に配信できます。Citrix Cloud アカウントは顧客IDによって識別され、OrgIDに関連付けられています。1つのOrgIDは複数のCitrix Cloud顧客IDに関連付けることができますが、1つの顧客IDは1つのOrgIDにのみ関連付けることができます。

組織がOrgIDを設定した方法に基づいて適切なCitrix Cloudアカウントを使用することが重要です。そうすることで、購入と管理者アクセスを同じOrgIDで継続できます。たとえば、OrgID 1234を使用している会社の設計部門がオンプレミスでVirtual Apps and Desktopsを使用しており、Citrix Cloudを試したい場合、OrgID 1234の管理者の1人が、Citrixアカウントのサインイン資格情報またはそのOrgIDに関連付けられたメールアドレスを使用して、そのOrgIDでCitrix Cloudにサインアップできます。会社がCitrix DaaS™サブスクリプションの購入を決定した場合、注文はOrgID 1234に正しく配置できます。

> **重要:**
>
> 特定のCitrixアカウントにアクセスできるユーザーは、そのCitrixアカウントのOrgIDに関連付けられたCitrix Cloudアカウントに自動的にアクセスできるわけではありません。Citrix Cloud

へのアクセスは、ユーザーがサービスに影響を与える可能性があるため、Citrix Cloudアカウントにアクセスするユーザーを制御することが重要です。



多要素認証

Citrix Cloudアカウントを安全に保つため、Citrixはすべてのお客様に多要素認証 (MFA) への登録を義務付けています。登録するには、コンピューターやモバイルデバイスなどのデバイスと、Citrix SSOなどの認証アプリがインストールされていることだけが必要です。認証アプリがインストールされたデバイスを使用できない場合は、代わりにメールアドレスを使用できます。

MFAにまだ登録していない場合、CitrixはCitrixアカウントの資格情報でサインインしたときに登録を促します。要件と手順については、この記事の「ステップ2：多要素認証を設定する」を参照してください。

ステップ1：Citrix Cloudウェブサイトにアクセスする

1. ウェブブラウザを使用して、https://onboarding.cloud.comにアクセスします。
2. **アカウントを作成**を選択します。

   「Citrix.comアカウントを使用」ボタンがあるサインアップページ(/en-us/citrix-cloud/media/create-cc-acct-page.png)
3. Citrix.comアカウントに関連付けられているユーザー名とパスワード、またはメールアドレスとパスワードを入力します。

アカウントがすでに使用されている場合はどうなりますか?

アカウント使用中の警告メッセージ(/en-us/citrix-cloud/media/cc-account-in-use-request-approval.png)

組織のCitrix Cloudアカウントがすでに使用中であることを示すメッセージが表示された場合、それはCitrixアカウントの別の管理者がすでにCitrix Cloudアカウントを作成していることを意味します。アカウントにアクセスするには、既存の管理者があなたを管理者として招待する必要があります。たとえあなたがすでにCitrixアカウントのメンバーであってもです。

Citrix Cloudアカウントは管理者にサービスに対するはるかに大きな制御を許可するため、Citrix Cloudアカウントを最初に作成した管理者は、たとえ他の管理者がすでにCitrixアカウントのメンバーであっても、明示的に他の管理者にアクセス権を付与する必要があると考えています。

Citrix Cloudアカウントへの招待をリクエストするには、**Request Approval**を選択します。アカウント上のすべての既存の管理者に、あなたのリクエストを通知するメールが届きます。既存の管理者がすでに組織にいない場合は、Citrixサポートにお問い合わせください。

管理者が承認リクエストを受け取ると、(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html#invite-individual-administrators)で説明されているように、あなたを管理者として招待します。

招待メールを受け取ったら、**サインイン**リンクをクリックして招待を承諾します。ブラウザが開くと、Citrix Cloudはパスワードを作成してCitrix Cloudアカウントにサインインするよう促します。

ステップ2：多要素認証を設定する

MFAに登録していない場合、Citrix Cloudはサインインする前に登録するよう促します。認証アプリ（推奨）またはメールアドレスを使用してMFAに登録することを選択できます。

> **注：**
>
> - Citrix IDプロバイダー配下の管理者のみがCitrix Cloudを通じてMFAを設定できます。Microsoft Entra IDを使用してCitrix Cloud管理者を管理している場合、Azureポータルを使用してMFAを構成できます。詳細については、Microsoft WebサイトのAzure Multi-Factor Authentication の設定を構成するを参照してください。
> - セットアッププロセスを完了すると、Citrix Cloudで所属するすべての顧客組織に対してMFAが使用されます。セットアッププロセス完了後にMFAを無効にすることはできません。
> - 登録できるデバイスは1つだけです。後で別のデバイスを登録した場合、Citrix Cloudは現在のデバイス登録を削除し、新しいデバイスに置き換えます。詳細については、(/ja-jp/

> citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html#manage-your-primary-mfa-method)を参照してください。

認証方法としてのメール

認証アプリを使用してCitrix Cloudにアクセスできない場合、メールを使用したMFAは便利な代替手段です。ただし、Citrixは、メールアドレスへのアクセスが安全であることを確認するために予防措置を講じることを強く推奨します。

MFAの要件

認証アプリでMFAを設定するには、スマートフォンやデスクトップコンピューターなどのデバイスに、Time-Based One-Time Password標準に準拠したアプリをインストールする必要があります。登録するデバイスによっては、アプリがQRコードをスキャンするためにデバイスのカメラにアクセスする必要がある場合があります。デバイスにカメラがない場合は、Citrix Cloudが提供するキーを入力できます。

メールアドレスでMFAを設定するには、以下の要件を満たすメールアドレスを使用する必要があります。

- そのメールアドレスは、Citrixアカウントで使用しているメールアドレスとは異なること。
- そのメールアドレスは、Citrixからの確認メールを受信するためにアクセスできるアドレスであること。

多要素認証に登録するには

1. MFAへの登録を求められたら、**Enroll now**を選択します。

   (/en-us/citrix-cloud/media/admin-mfa-enroll-now-prompt.png)

2. プロンプトが表示されたら、メールアドレスを入力し、**Send email**を選択します。Citrix Cloudから確認コードが記載されたメールが送信されます。
3. メールに記載されている確認コードとCitrixアカウントのパスワードを入力します。**Verify and continue**をクリックします。
4. 使用したい認証方法（認証アプリまたはメール）を選択します。
5. **Authenticator app**を選択した場合は、次の操作を実行します。

   a. 認証アプリからQRコードをスキャンするか、キーを手動で入力します。認証アプリにCitrix Cloudのエントリが表示され、6桁のコードが生成されます。

「QRコードとキーが強調表示された認証アプリのダウンロード画面」(/en-us/citrix-cloud/media/admin-mfa-qr-code-key.png)

b. 「**認証アプリを確認**」の下で、認証アプリのコードを入力し、「**コードを確認**」を選択します。

6. 「**次へ: 回復方法**」をクリックします。
7. 「**回復用電話番号を追加**」を選択し、Citrixサポートがお客様に電話して本人確認を行うために使用できる回復用電話番号を入力します。Citrixは固定電話番号の使用を推奨しています。完了したら、「**回復用電話番号を保存**」をクリックします。
8. 「**次へ**」を選択します。
9. 「**回復用メールアドレスを追加**」を選択し、Citrix Cloudで使用しているものとは異なる、アクセス可能なメールアドレスを入力します。Citrixはこのアドレスを使用して、本人確認のための検証コードを送信します。

   別のメールアドレスをお持ちでない場合は、「**回復用メールアドレスがありませんか？**」を選択して、代わりにバックアップコードのリストを生成します。バックアップコードは簡単に紛失する可能性があるため、推奨されません。このオプションを選択した場合は、コードをダウンロードし、必要なときにアクセスできる場所に保管してください。

10. 「**完了**」を選択して登録を完了します。

次回Citrix Cloud管理者資格情報でサインインすると、Citrix Cloudは選択したMFA方法からの検証コードを要求します。

「検証コード入力ページ」(/en-us/citrix-cloud/media/admin-mfa-sign-in-verification-code.png)

MFA登録の管理

デバイスを変更したり、別のMFA方法に切り替えたり、回復方法を更新したりするには、以下の記事を参照してください。

- プライマリMFA方法の管理
- MFA回復方法の管理

ステップ3：OrgIDの確認

Citrix Cloud を使い始める前に、OrgID を確認してください。

ご使用のアカウントの OrgID が、注文時に使用する OrgID と一致していることを確認してください。Citrix Cloud の利点の 1 つは、サービスを試用して購入を決定した場合、購入が同じアカウン

トで行われるため、試用版で行ったすべての構成が購入したサービスに保持されることです。したがって、適切な OrgID で試用を開始することで、購入を決定した際の労力を節約できます。

OrgID は、管理コンソールの次の場所に表示されます。

- お客様名の下のメニューに表示されます。メニューを表示するには、右上隅にあるお客様名をクリックします。

  アカウント名とともに表示される OrgID (/en-us/citrix-cloud/media/org-id-acct-name.png)
- ご自身の**アカウント設定**ページに表示されます。お客様メニューから**アカウント設定**を選択します。

  OrgID が強調表示されたアカウント設定ページ (/en-us/citrix-cloud/media/acct-settings-page-org-id.png)

次のステップ

オンボーディング後、次のタスクに進むことができます。

- 管理者またはエンドユーザーを認証するために、ID プロバイダーを追加します。
- Citrix Cloud アカウントに管理者を追加します。他の管理者が Citrix.com の Citrix アカウントにアクセスできる場合でも、Citrix Cloud アカウントに管理者を追加する必要があります。
- クラウドサービスの試用版をリクエストします。試用版は、選択したオンプレミスインフラストラクチャまたはパブリッククラウド、アプリケーション、および Microsoft Active Directory でテストできるように設計されています。
- アカウントへのライセンスの割り当て。この手順は、ユーザーへのライセンスの割り当てに役立ちます。

詳細情報

- Citrix トレーニング: Citrix Cloud の基礎
- YouTube の Citrix チャンネル: Citrix Cloud Master Class

Citrix Cloud™ のメールアドレスを確認する

Citrix は、Citrix Cloud アカウントの確認を求めることがあります。メールアドレスの確認を求められる理由としては、次のようなものがあります。

- しばらくの間、Citrix Cloud にログインしていない。

- メールアドレスを変更した。
- Citrix Cloud アカウントに新しい管理者を追加した。
- Citrix Cloud のセキュリティシステムアップデートにより、Citrix Cloud アカウントの再確認が必要です。

よくある質問

どのくらいの頻度で確認を求められますか?

アカウントの確認は一度限りのイベントです。Citrix Cloud は、サインインするたび、またはアカウントに変更があるたびに確認を求めることはありません。頻繁に確認を求められる場合は、Citrix テクニカルサポートにお問い合わせください。

アカウントに何か問題が発生しましたか?

いいえ、アカウントの確認を求められることは、アカウントまたは Citrix Cloud サービスに問題があることを意味するものではありません。これは、Citrix がお客様の情報を安全かつセキュアに保つための一環です。

確認メールが届かない場合の対処法?

次の手順を実行してください。

1. 受信トレイで「Citrix」からの確認メールを検索してください。確認メールは24時間で期限切れになります。新しい確認メールをトリガーするには、Citrix Cloud に再度サインインしてください。これは、ウェブログインごとに1回限りのプロセスです。
2. 受信トレイにない場合は、他のフォルダを確認してください。スパムフィルターやメールルールによってメールが移動された場合、スパムフォルダや迷惑メールフォルダに入っている可能性があります。ファイアウォールも確認してください。
3. 正しいメールアカウントを確認していることを確認してください。Citrix は、現在アカウントに登録されているメールアドレスに確認メールを送信します。多くの場合、これは Citrix Cloud に最初にサインアップしたメールアドレス、または Citrix Cloud アカウントへの招待を受けたメールアドレスです。
4. https://www.citrix.com/account で Citrix アカウントにサインインして、登録されているメールアドレスが有効であることを確認してください。メールが無効な場合は、メールアドレスを更新し、Citrix Cloud に再度サインインして、新しい確認メールをトリガーしてください。詳細については、Citrix サポート知識センターの CTX120355 を参照してください。
5. 確認メールがまだ届かない場合は、Citrix Support に連絡してサポートケースをオープンしてください。教育機関サイト（**Partner Services Delivery > eLearning > Citrix Training** を参照）

の場合は、教育チームにケースをオープンして、さらに調査を依頼してください。ケースをオープンするには、お問い合わせ ページで **General Support** をリクエストしてください。

メールの確認に成功したにもかかわらず、Citrix Cloud にサインインできない場合は、Citrix Web サイトでのログインに関する問題のトラブルシューティング を参照してください。

Citrix サポートへのお問い合わせ

ここに記載されていない問題が発生している場合は、Citrix Support に連絡してサポートケースをオープンしてください。

Citrix Cloud™ に接続する

Connecting your resources to Citrix Cloud involves deploying connectors in your environment and creating *resource locations*.

リソースの場所

リソースの場所には、エンドユーザー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ています。リソースの場所には、使用しているCitrix Cloudサービスと、ユーザーに提供したいサービスに応じて、さまざまなリソースが含まれます。

リソースの場所は、パブリッククラウド、プライベートクラウド、支社、データセンターのいずれであっても、リソースが存在する場所です。独自のクラウドまたはデータセンターにすでにリソースがある場合、リソースはそのままの場所に残ります。Citrix Cloudで使用するために、それらを別の場所に移動する必要はありません。

場所の選択は、次の要因によって影響を受ける可能性があります。

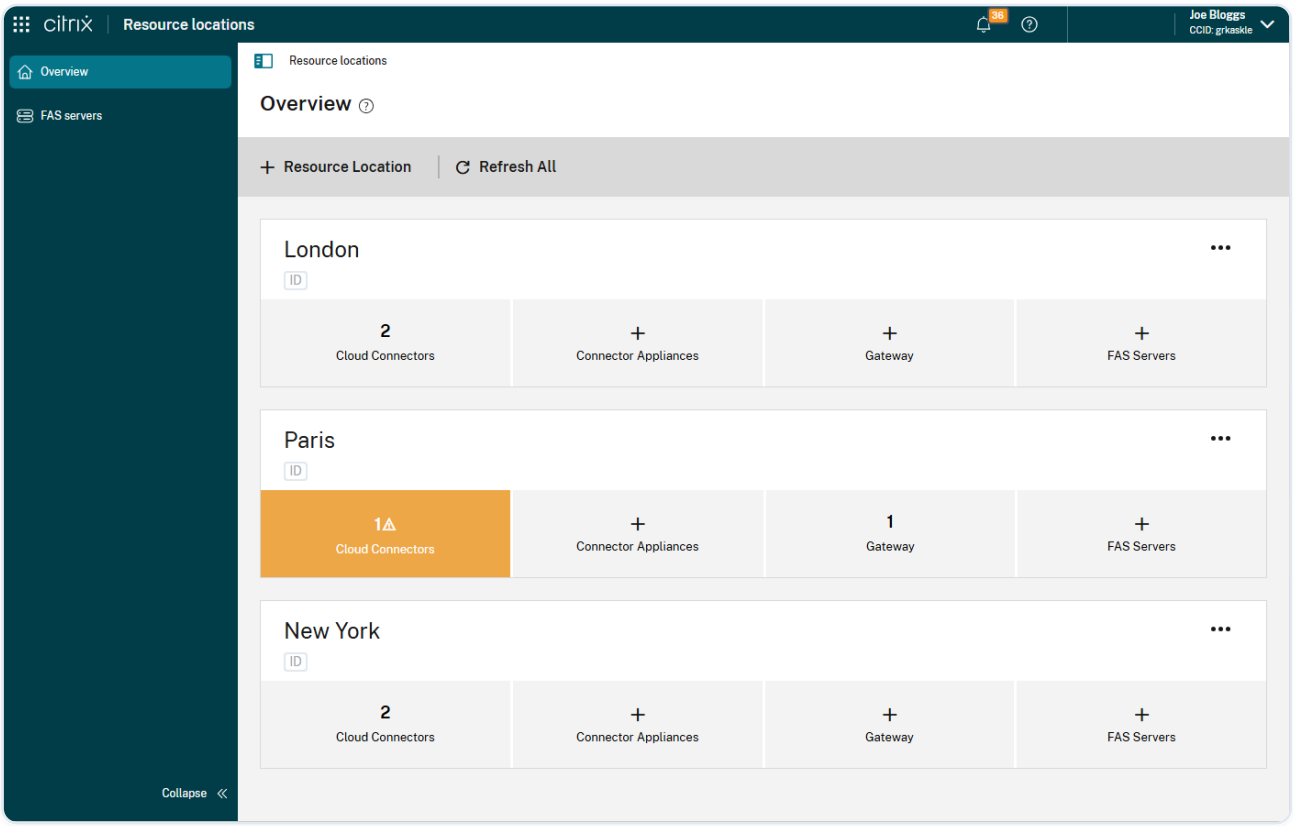
- エンドユーザーとの近接性
- データとの近接性
- スケール要件
- セキュリティ属性

リソースの場所の展開例

- データに近い必要があるユーザーとアプリケーションに基づいて、本社向けにデータセンターに最初のリソースの場所を構築します。
- グローバルユーザー向けに、パブリッククラウドに2番目のリソースの場所を追加します。あるいは、支社の従業員の近くで最も適切に提供されるアプリケーションを提供するために、支社に個別のリソースの場所を構築します。
- 制限されたアプリケーションを提供する別のネットワークに、別のリソースの場所を追加します。これにより、他のリソースの場所を調整することなく、他のリソースやユーザーへの可視性が制限されます。

リソースの場所の表示と管理

リソースロケーションを管理するには、Citrix Cloudにログインし、メインメニューから**リソースロケーション**を選択します。



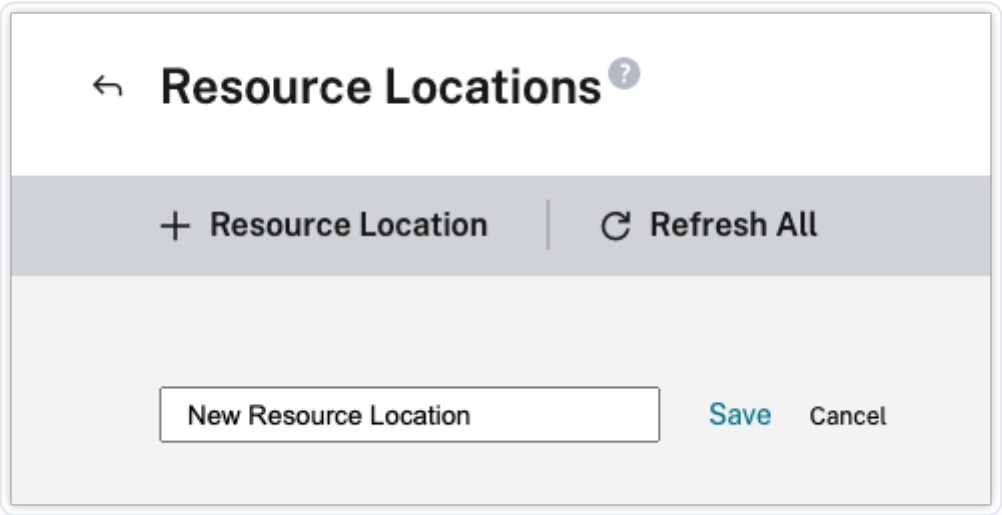
各リソースロケーションには、以下を追加できます。

- クラウドコネクタ
- コネクタアプライアンス
- シトリックス ゲートウェイ
- FASサーバー

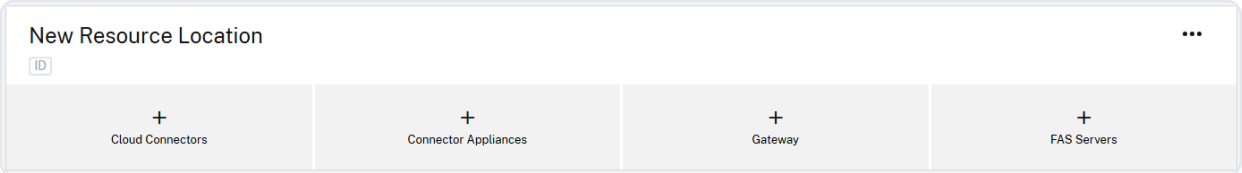
リソースロケーションを作成する

リソースロケーションを作成するには：

1. **+ リソースロケーション**を選択します



2. リソースロケーションの名前を入力します。名前付けの制限を参照してください。
3. **保存**を押します。新しいリソースロケーションが作成されます。



4. リソースロケーションに少なくとも2つのコネクタをインストールします。使用しているクラウドサービスに応じて、Citrix Cloudとリソース間の通信を有効にするには、Cloud ConnectorまたはConnector Applianceが必要です。適切なコネクタの選択については、リソースの種類を参照してください。コネクタを展開するには、以下の記事を参照してください。

   - 「Cloud Connectorのインストール」(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)
   - クラウドサービス用コネクタアプライアンス(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#obtain-the-connector-appliance)

リソースの種類

リソースの場所には、使用しているCitrix Cloudサービスや、エンドユーザーに提供したいサービスに応じて、さまざまなリソースが含まれます。さまざまなリソースが異なる種類のコネクタを使用します。ほとんどのサービスはCitrix Cloud Connector™を使用しますが、一部の特定のサービスではConnector Applianceが必要です。

Citrix Cloud Connectorを使用するサービス

- **Citrix DaaS**（旧Citrix Virtual Apps and Desktopsサービス）では、リソースの場所でアプリとデスクトップを公開し、マシンカタログをプロビジョニングするためにCloud Connectorが必

要です。Cloud Connectorがこのサービスとどのように通信するかについては、Citrix Tech Zoneの「Citrix DaaS図」を参照してください。

- **Citrix DaaS Standard for Azure**（旧Citrix Virtual Apps and Desktops Standard for Azure）では、マルチセッションマシンからCitrixホスト型Azure仮想デスクトップとアプリを配信するためにCloud Connectorが必要です。
- **Endpoint Management**では、アプリとデバイスのポリシーを管理し、ユーザーにアプリを配信するためにCloud Connectorが必要です。

Connector Applianceを使用するサービス

- **Image Portability Service**は、プラットフォーム間のイメージ管理を簡素化します。この機能は、オンプレミスのリソースの場所とパブリッククラウドのリソースの場所の間でイメージを管理するのに役立ちます。Citrix Virtual Apps and Desktops™ REST APIを使用して、Citrix Virtual Apps and Desktopsサイト内のリソースの管理を自動化できます。

  Image Portabilityワークフローは、Citrix Cloudを使用して、オンプレミスの場所からパブリッククラウドサブスクリプションへのイメージの移行を開始するときに始まります。イメージを準備した後、Image Portability Serviceはイメージをパブリッククラウドサブスクリプションに転送し、実行できるように準備するのに役立ちます。最後に、Citrix ProvisioningまたはMachine Creation Services™がパブリッククラウドサブスクリプションにイメージをプロビジョニングします。

  詳細については、「Image Portability Service」を参照してください。
- **Citrix Secure Private Access**を使用すると、管理者はシングルサインオン、リモートアクセス、コンテンツ検査をエンドツーエンドのアクセス制御のための単一ソリューションに統合する、一貫性のあるエクスペリエンスを提供できます。詳細については、「Secure Private Access with Connector Appliance」を参照してください。

Connector Applianceに依存するプレビュー中の他のサービスがある場合があります。

リソースの場所の制限

Citrix Cloudアカウントには、最大50個のリソースロケーションを設定できます。

命名規則

リソースロケーションに割り当てる名前は、以下の制限に従う必要があります。

- 最大長: 64文字

- 使用できない文字:
  - `#`, `$`, `%`, `\^`, `&`, `?`, `+`
  - 中括弧: `[]`, `{}`
  - パイプ (`|`)
  - 小なり記号 (`<`) および大なり記号 (`>`)
  - スラッシュとバックスラッシュ (`/`, `\`)
- Citrix Cloudアカウント内の他のリソースロケーション名と一致しないこと（大文字と小文字を区別しない）

プライマリリソースロケーション

プライマリリソースロケーションとは、ドメインとCitrix Cloud間の特定の通信において「最も優先される」ものとして指定するリソースロケーションです。プライマリリソースロケーション内のCloud Connectorは、ユーザーログオンおよびプロビジョニング操作に使用されます。「プライマリ」として選択するリソースロケーションには、ドメインへの最高のパフォーマンスと接続性を持つCloud Connectorが必要です。これにより、ユーザーはCitrix Cloudにすばやくログオンできます。

詳細については、「プライマリリソースロケーションの選択」を参照してください。

ゲートウェイ

デフォルトでは、クライアントは仮想アプリとデスクトップをホストしているマシンに直接アクセスできる必要があります。ゲートウェイを使用することで、リモートアクセスを有効にできます。Citrix Gateway Serviceを使用するか、独自のNetScaler®ゲートウェイを使用できます。

リモートアクセスを構成するには、リソースロケーションの**Gateway**タイルを選択します。

リソースロケーションページ(/en-us/citrix-cloud/media/resource-location-connectivity.png)

または、**StoreFront Cloud**から同じ構成画面にアクセスすることもできます。

ゲートウェイの構成の詳細については、ストアへのアクセスを構成する - 外部接続を参照してください。

シトリックス クラウド コネクタ™

Citrix Cloud™ Connectorは、Citrix Cloudとリソースの場所間の通信チャネルとして機能するCitrixコンポーネントであり、複雑なネットワークやインフラストラクチャの構成を必要とせずにクラウド管理を可能にします。これにより、配信インフラストラクチャの管理の煩わしさがすべて解消されます。ユーザーに価値を提供するリソースを管理し、集中できるようになります。

> **注:**

> Citrix DaaS Remote PowerShell SDKをCitrix Cloud Connectorマシンにインストールしないでください。同じリソースの場所内の、ドメインに参加している任意のコンピューターにインストールできます。

> Citrix®は、このSDKのコマンドレットをCloud Connectorで実行しないことを推奨します。SDKの操作にはCloud Connectorは関与しません。

Cloud Connectorを必要とするサービス

Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）にはCloud Connectorが必要です。Cloud Connectorがサービスとどのように通信するかについては、Tech ZoneのCitrix DaaS図を参照してください。

Citrix Endpoint Management™には、Endpoint Managementサービスへのエンタープライズ接続のためにCloud Connectorが必要です。Remote Browser Isolationサービスには、認証された外部WebアプリのためにCloud Connectorが必要です。

Cloud Connectorの機能

- **Active Directory (AD)**: AD管理を可能にし、リソースの場所内でADフォレストとドメインの使用を許可します。これにより、追加のAD信頼を追加する必要がなくなります。
- **仮想アプリとデスクトップの公開**: リソースの場所にあるリソースからCitrix DaaS™の公開を可能にします。
- **Endpoint Management**: デバイスとアプリのポリシーを管理し、ユーザーにアプリを配信するためのモバイルデバイス管理（MDM）およびモバイルアプリケーション管理（MAM）環境を可能にします。
- **マシンカタログのプロビジョニング**: マシンをリソースの場所に直接プロビジョニングすることを可能にします。

Cloud Connectorの通信

Cloud Connectorは、Citrix Cloudとリソースの場所間のすべての通信を認証および暗号化します。インストールされると、Cloud Connectorはアウトバウンド接続を介してCitrix Cloudとの通信を開始します。すべての接続は、標準のHTTPSポート（443）とTCPプロトコルを使用して、Cloud Connectorからクラウドへ確立されます。パブリックインターネットからのインバウンド接続は受け入れられません。

Cloud Connectorの可用性と負荷管理

継続的な可用性を確保し、負荷を管理するために、各リソースの場所に複数のCloud Connectorをインストールしてください。Citrix Cloudとの高可用性接続を確保するには、各リソースの場所に少なくとも2つのCloud Connectorが必要です。いずれかのCloud Connectorが一定期間利用できなくなった場合でも、他のCloud Connectorが接続を維持できます。各Cloud Connectorはステートレスであるため、利用可能なすべてのCloud Connectorに負荷を分散できます。この負荷分散機能を構成する必要はありません。完全に自動化されています。

Cloud Connectorが1つでも利用可能であれば、Citrix Cloudとの通信が失われることはありません。エンドユーザーのリソースの場所にあるリソースへの接続は、可能な限りCitrix Cloudへの接続に依存しません。これにより、リソースの場所は、Citrix Cloudへの接続が利用可能であるかどうかにかかわらず、ユーザーにリソースへのアクセスを提供できます。

Cloud Connectorの入手先

Cloud Connectorソフトウェアは Citrix Cloud内からダウンロードできます。

1. Citrix Cloudにサインインします。
2. 画面左上のメニューから、**Resource Locations**を選択します。
3. 既存のリソースの場所がない場合は、Resource Locationsページで**Download**をクリックします。プロンプトが表示されたら、**cwcconnector.exe**ファイルを保存します。
4. リソースの場所があるが、Cloud Connectorがインストールされていない場合は、Cloud Connectorsバーをクリックし、**Download**をクリックします。プロンプトが表示されたら、**cwcconnector.exe**ファイルを保存します。

必要なCloud Connectorの数?

Citrix Cloudとリソースの場所の間に高可用性接続を確立するには、最低2つのCloud Connectorが必要です。環境とサポートするワークロードによっては、ユーザーに最高の体験を提供するために、より多くのCloud Connectorが必要になる場合があります。

ベストプラクティスとして、Citrixは、展開する必要があるCloud Connectorの数を決定する際に、N+1冗長モデルを使用することを推奨しています。環境、ワークロード、Active Directory構成、およびサービスに基づいて、リソースの場所に必要となるCloud Connectorの数を決定します。この数に、回復性を提供するために少なくとも1つ以上のCloud Connectorを追加します。たとえば、5つのCloud Connectorが必要であると判断した場合、この合計にさらに1つ追加し、リソースの場所に6つのCloud Connectorをインストールします。

追加のスケールとサイジングのガイドラインについては、Cloud Connectorのスケールとサイズに関する考慮事項を参照してください。

Cloud Connectorのインストール場所

Cloud Connectorは、ドメインに参加しており、Citrix Cloudから管理したいリソースと通信できる専用マシンにインストールします。詳細については、システム要件を参照してください。

展開に関する詳細については、以下の記事を参照してください。

- Active DirectoryにおけるCloud Connectorの展開シナリオ(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/technical-details.html#deployment-scenarios-for-cloud-connectors-in-active-directory)
- Cloud Connectorのインストール(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)

Citrix Cloud Connector のシステム要件

Citrix Cloud Connector™ をホストするマシンは、以下の要件を満たす必要があります。高可用性を確保するため、本番環境では各リソースの場所に少なくとも2つのCloud Connectorが必要です。ベストプラクティスとして、Citrix®は、Citrix Cloudとの高可用性接続を維持するために、Cloud Connectorを展開する際にN+1冗長モデルを使用することを推奨しています。

ホストリソース要件

各Cloud Connectorには、最低限以下のものが必要です。

- 2 vCPU
- 4 GB メモリ
- 20 GB ディスク容量

ローカルホストキャッシュに使用されるCloud Connectorの場合、CitrixはCloud Connectorに最低4 vCPUと6 GBのメモリを推奨しています。

より多くのvCPUメモリにより、Cloud Connectorは大規模なサイト向けにスケールアップできます。推奨される構成については、Cloud Connectorのスケールとサイズに関する考慮事項を参照してください。

オペレーティングシステム

以下のオペレーティングシステムがサポートされています。

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2019
- ウィンドウズ サーバー 2016

Cloud Connector は Windows Server Core での使用はサポートされていません。

.NET の要件

各サーバーに以下の両方をインストールする必要があります。

- Microsoft .NET Framework 4.7.2 以降。これは Windows Server 2019 以降ではデフォルトでインストールされています。Windows Server 2016 では、Microsoft の Web サイトから 最新バージョンをダウンロードしてください。
- Microsoft .NET 8.0。Microsoft の Web サイトから最新バージョンをダウンロードしてください。

Citrix は、これらのパッケージを最新の状態に保つために、Windows Update を「他の Microsoft 製品の更新プログラムを受け取る」ように構成することを強くお勧めします。

サーバーの要件

Citrix DaaS™ (旧 Citrix Virtual Apps and Desktops サービス) で Cloud Connector を使用している場合は、マシンの構成ガイダンスについて Cloud Connector の規模とサイズに関する考慮事項を参照してください。

Cloud Connector がインストールされているすべてのマシンに、以下の要件が適用されます。

- Cloud Connector のホストには専用のマシンを使用してください。他の Citrix 製品や他のアプリケーションと同じマシンにはインストールしないでください。
- サーバーは Active Directory ドメインコントローラー、またはリソースロケーションインフラストラクチャにとって重要なその他のマシンであってはなりません。Cloud Connector の 定期メンテナンスは、これらの追加リソースに停止を引き起こすマシン操作を実行します。

- サーバーの時計が正しい UTC 時刻に設定されていること。
- グラフィカルインストーラーを使用する場合は、ブラウザーがインストールされており、デフォルトのシステムブラウザーが設定されている必要があります。
- Cloud Connector インストーラーは Citrix Cloud からダウンロードされるため、ブラウザーで実行可能ファイルのダウンロードが許可されている必要があります。

Windows Update のガイダンス

Citrixは、Cloud Connectorをホストするすべてのマシンで Windows Updateを有効にすることを強く推奨します。これには、「他のMicrosoft製品の更新プログラムをインストールする」ポリシーも含まれます。Cloud Connectorは、Windows Updateを含むさまざまな要因によってトリガーされる可能性のある保留中の再起動を5分ごとに定期的にチェックします。検出された再起動は、リソースの場所で設定された優先日スケジュールに関係なく、直ちに実行されます。このプロアクティブなアプローチにより、Cloud Connectorが長期間保留中の更新状態に置かれることがなく、システムの安定性が維持されます。

Citrix Cloudは、可用性を維持するために再起動を管理し、一度に1つのCloud Connectorのみが再起動することを許可します。Windows Updateを設定する際は、Windowsが営業時間外に更新プログラムを自動的にダウンロードしてインストールするように設定されていることを確認してください。ただし、Cloud Connectorが再起動プロセスを管理するのに十分な時間を確保するため、自動再起動は少なくとも4時間は許可されません。さらに、更新後にマシンを再起動する必要がある状況に備えて、グループポリシーまたはシステム管理ツールを使用してフォールバック再起動メカニズムを確立できます。詳細については、「Manage device restarts after updates」を参照してください。

> **注：**
>
> - 顧客がCloud Connectorを営業時間中に再起動させたくない場合は、営業時間外にWindows Updateを適切にスケジュールすることをお勧めします。
> - 各Cloud Connectorの再起動には約10分かかります。これには、Citrix Cloud Platformと同期して、一度に1つのCloud Connectorのみが再起動することを保証するために必要な時間が含まれます。したがって、前述の自動再起動に推奨される最低4時間の遅延は、テナント内のCloud Connectorの数に応じて、より短いまたはより長い期間に調整できます。

アンチウイルス構成

記事「Tech Paper: Endpoint Security, Antivirus, and Antimalware Best Practices」では、環境内のCloud Connectorのセキュリティとパフォーマンスの適切なバランスを決定するのに役立つガイドラインを提供しています。Citrixは、これらのガイドラインを組織のアンチウイルスチームおよびセキュリティチームと確認し、本番環境に適用する前に厳格なラボベースのテストを実施することを強く推奨します。

証明書の検証要件

Cloud Connectorは、インストールするソフトウェアパッケージの整合性と、接続するCitrix Cloudエンドポイントを検証するためにX.509証明書に依存しています。これらの証明書は、広く信頼されているエンタープライズ認証局（CA）によって発行されます。

この検証を実行するために、Cloud Connectorには次の要件があります。

- ルート証明書がホスト証明書ストアに存在している必要があります。
- 中間証明書がホスト証明書ストアに存在している必要があります。
- Cloud Connectorは、証明書の証明書失効リスト（CRL）を検証できる必要があります。

証明書のダウンロードとインストールの完全な手順については、「CTX223828」を参照してください。

ルート証明書の要件

以下のルート証明書をCloud Connectorホストにインストールする必要があります。

- `https://cacerts.digicert.com/DigiCertGlobalRootG3.crt`
- `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
- `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`
- `https://cacerts.digicert.com/DigiCertTrustedRootG4.crt`
- `https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt`
- `https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt`
- `https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt`
- `https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt`
- `https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt`

ルート証明書は通常、オペレーティングシステムの一部としてパッケージ化されるか、Windowsルート証明書プログラムによって配布されます。ただし、以下の場合は除きます。

- 自動ルート証明書更新を無効にするグループポリシーがルート証明書の更新をブロックするように設定されている場合、および
- Connectorホストサーバーからインターネットへの接続が制限されており、更新プログラムのダウンロードが妨げられている場合

いずれかの証明書が不足している場合、Cloud Connectorインストーラーは`http://cacerts.digicert.com`からダウンロードを試みます。

これが不可能な場合は、すべてのCloud Connectorホストにルート証明書を手動でインストールする必要があります。

中間証明書の要件

次の中間証明書をCloud Connectorホストにインストールする必要があります。

- `https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt`

中間証明書は通常、Windows証明書ストアに存在しない中間認証局によって発行された証明書がサーバーに提示されたときに、オンデマンドでダウンロードされます。

コネクタホストサーバーからインターネットへの接続が制限されている場合、このダウンロードは行われない可能性があります。このような場合、中間証明書はすべてのCloud Connectorホストに手動でインストールする必要があります。

証明書失効リスト (CRL) の要件

コンポーネントの検証に使用される証明書が侵害されていないことを確認することが重要です。これは、証明書失効リスト (CRL) を使用して実装されます。クライアントがファイルまたはエンドポイントの整合性を検証するために証明書を使用する場合、クライアントは証明書を発行したCAを信頼しているか、および証明書が失効しているかを確認します。証明書がCRLにある場合、その証明書は失効しており、信頼できません。

CRLサーバーは、ポート443のHTTPSではなく、ポート80のHTTPを使用します。Cloud Connectorコンポーネント自体は、外部ポート80を介して通信しません。外部ポート80の必要性は、オペレーティングシステムが実行する証明書検証プロセスの副産物です。

Cloud ConnectorがHTTPポート80で接続するために、次のCRLエンドポイントが利用可能である必要があります。

- `http://cacerts.digicert.com/`
- `http://dl.cacerts.digicert.com/`
- `http://crl3.digicert.com`
- `http://crl4.digicert.com`
- `http://ocsp.digicert.com`
- `http://www.d-trust.net`
- `http://root-c3-ca2-2009.ocsp.d-trust.net`
- `http://crl.microsoft.com`
- `http://oneocsp.microsoft.com`
- `http://ocsp.msocsp.com`

CRLおよびOCSP接続のテスト方法の詳細については、https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htmを参照してください。

顧客管理証明書

Citrix Cloudサービスとの通信に必要なCitrix管理証明書に加えて、顧客は他のオンプレミスコンポーネントとの通信を保護するために、Cloud Connectorに追加の証明書を展開できます。これらの証明書は顧客が管理し、顧客が監視および更新する必要があります。

次の表は、顧客管理証明書で保護できる通信フローの概要を示しています。

コンポーネント	コネクタからのトラフィックフロー	追加ドキュメント
StoreFront	インバウンド	HTTPS構成
NetScaler® ゲートウェイ	インバウンド	HTTPS構成
ハイパーバイザー	アウトバウンド	VMware環境への接続の保護

シトリックス DaaS

DaaSリソースへの接続にCloud Connectorを利用するには、追加の証明書のインストールと、拡張されたPKIインフラストラクチャへのアクセス許可が必要です。各Cloud Connectorマシンは、以下の要件を満たす必要があります。

- HTTPポート80は以下のIPアドレスに対して開いている必要があります。
  - `crl.*.amazontrust.com`

  - `ocsp.*.amazontrust.com`
  - `*.ss2.us`
- 以下のIPアドレスとの通信が有効になっている必要があります
  - `https://*.amazontrust.com`
  - `https://*.ss2.us`
- 以下のルート証明書がインストールされている必要があります。
  - `https://www.amazontrust.com/repository/AmazonRootCA1.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA2.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA3.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA4.cer`
  - `https://www.amazontrust.com/repository/SFSRootCAG2.cer`
- 以下の中間証明書がインストールされます:
  - `https://www.amazontrust.com/repository/G2-RootCA4.orig.cer`
  - `https://www.amazontrust.com/repository/R3-ServerCA3A.cer`
  - `https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer`
  - `https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA1.orig.cer`
  - `https://www.amazontrust.com/repository/R1-ServerCA1A.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA3.cer`
  - `https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA2.orig.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA4.cer`
  - `https://www.amazontrust.com/repository/R2-ServerCA2A.cer`
  - `https://www.amazontrust.com/repository/R4-ServerCA4A.cer`
  - `https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA1.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA2.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA3.orig.cer`

- `https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer`
- `https://www.amazontrust.com/repository/G2-ServerCA0A.cer`
- `https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer`
- `https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.cer`

どの証明書かが不足している場合、Cloud Connector はそれを `<https://www.amazontrust.com>` からダウンロードします。

証明書のダウンロードとインストールの完全な手順については、CTX223828 を参照してください。

Active Directory の要件

- サーバーは、ユーザー向けにサービスを作成するために使用するリソースとユーザーが含まれている Active Directory ドメインに参加している必要があります。マルチドメイン環境については、Cloud Connector の Active Directory 展開シナリオ を参照してください。
- Citrix Cloud で使用する予定の各 Active Directory フォレストは、常に2つの Cloud Connector から到達可能である必要があります。
- Cloud Connector は、フォレストのルートドメインと、Citrix Cloud で使用する予定のドメインの両方にあるドメインコントローラーに到達できる必要があります。詳細については、以下の Microsoft サポート記事を参照してください。
  - ドメインと信頼を構成する方法
  - Windows のサービス概要とネットワークポート要件の「システムサービスポート」セクション
- グローバルセキュリティグループの代わりにユニバーサルセキュリティグループを使用します。この構成により、フォレスト内の任意のドメインコントローラーからユーザーグループのメンバーシップを取得できます。

サポートされている Active Directory の機能レベル

Cloud Connector は、現在サポートされている Microsoft のバージョンと機能レベルをサポートしています。

> **注：**
>
> Windows Server 2025 の機能レベルは、データベースの32kページが無効になっている場合にのみサポートされます。

ネットワーク要件

- リソースの場所で使用するリソースに接続できるネットワークに接続されていること。詳細については、「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。
- インターネットに接続されていること。詳細については、「システムと接続の要件」の以下のセクションを参照してください。
  - Cloud Connector の共通サービス接続要件
  - Cloud Connector で許可される FQDN

連邦情報処理標準 (FIPS) のサポート

Cloud Connector は、FIPS対応マシンで使用されるFIPS検証済みの暗号化アルゴリズムをサポートしています。

Citrix Cloud Connector™ 技術詳細

Citrix Cloud™ Connector は、Citrix Cloud とリソースの場所との間に接続を確立するコンポーネントです。この記事では、展開要件とシナリオ、Active Directory と FIPS のサポート、およびトラブルシューティングのオプションについて説明します。

システム要件

システム要件を参照してください。

Cloud Connector のインストール済みサービス

このセクションでは、Cloud Connector とともにインストールされるサービスと、それらのシステム権限について説明します。

インストール中、Citrix Cloud Connector の実行可能ファイルは、機能するために必要なサービス構成をインストールし、デフォルト設定に設定します。デフォルト構成が手動で変更された場合、Cloud Connector は期待どおりに動作しない可能性があります。この場合、更新プロセスを処理するサービスがまだ機能していると仮定すると、次回の Cloud Connector の更新時に構成はデフォルトの状態にリセットされます。サービスは、サービスの追加または削除をサポートするために、「無効」状態でリリースされることがあります。

Citrix Cloud Agent System は、他の Cloud Connector サービスが機能するために必要なすべての昇格された呼び出しを容易にし、ネットワーク上で直接通信することはありません。Cloud Connector 上のサービスがローカルシステム権限を必要とするアクションを実行する必要がある場合、Citrix Cloud Agent System が実行できる事前定義された一連の操作を介してそれを行います。

サービス名	説明	実行ユーザー
Citrix Cloud エージェントシステム	オンプレミスエージェントに必要なシステムコールを処理します。インストール、再起動、レジストリアクセスが含まれます。Citrix Cloud Services Agent WatchDog のみから呼び出すことができます。	ローカルシステム
Citrix Cloud Services エージェント ウォッチドッグ	オンプレミスエージェントを監視およびアップグレードします (常時最新)。	ネットワークサービス
シトリックス クラウド サービス エージェント ロガー	Citrix Cloud Connectorサービス用のサポートログフレームワークを提供します。	ネットワークサービス
シトリックス クラウド サービス AD プロバイダー	Citrix Cloudが、インストールされているActive Directoryドメインアカウントに関連付けられたリソースの管理を容易にすることを可能にします。	ネットワークサービス
シトリックス クラウド サービス エージェント ディスカバリ	Citrix Cloudが、XenAppおよびXenDesktop®のレガシーなオンプレミスCitrix製品の管理を容易にすることを可能にします。	ネットワークサービス
シトリックス クラウド サービス 資格情報プロバイダー	暗号化されたデータの保存と取得を処理します。	ネットワークサービス
シトリックス クラウド サービス WebRelay プロバイダー	WebRelay Cloudサービスから受信したHTTPリクエストをオンプレミスWebサーバーに転送できるようにします。	ネットワークサービス
Citrix CDF キャプチャサービス	設定されているすべての製品とコンポーネントからCDFトレースをキャプチャします。	ネットワークサービス

サービス名	説明	実行ユーザー
Citrix 設定同期サービス	高可用性モードのために、ブローカー構成をローカルにコピーします。	ネットワークサービス
Citrix 接続リース交換サービス	Citrix® StoreFront Cloudのサービス継続性のために、WorkspaceアプリとCloud Connector間で接続リースファイルを交換できるようにします。	ネットワークサービス
Citrix 高可用性サービス	中央サイトの停止中にサービスの継続性を提供します。	ネットワークサービス
Citrix ITSM アダプタープロバイダー	仮想アプリとデスクトップのプロビジョニングと管理を自動化します。	ネットワークサービス
Citrix NetScaler® クラウドゲートウェイ	インバウンドファイアウォールルールを開いたり、DMZにコンポーネントを展開したりすることなく、オンプレミスのデスクトップおよびアプリケーションへのインターネット接続を提供します。	ネットワークサービス
Citrix リモートブローカープロバイダー	ローカルのVDAおよびStoreFront™サーバーからリモートのBroker Serviceへの通信を可能にします。	ネットワークサービス
Citrix リモート HCL サーバー	Delivery Controller™とハイパーバイザー間の通信をプロキシします。	ネットワークサービス
Citrix WEM クラウド認証サービス	Citrix WEMエージェントがクラウドインフラストラクチャサーバーに接続するための認証サービスを提供します。	ネットワークサービス

サービス名	説明	実行ユーザー
Citrix WEM クラウドメッセージングサービス	Citrix WEMクラウドサービスがクラウドインフラストラクチャサーバーからメッセージを受信するためのサービスを提供します。	ネットワークサービス
Citrix セキュア プライベートアクセス™	すべてのエンタープライズアプリケーションへのゼロトラストネットワークアクセス	ネットワークサービス
Citrix Cloud Services メッセージブローカー	Citrix Cloudプロバイダーと Citrix Cloudサービス間のメッセージを処理します。	ネットワークサービス
シトリックス セキュア チケッティング オーソリティ サービス	Citrix Cloudサービスにセキュアなチケット発行機関を提供します。	ネットワークサービス
Citrix 監視サービス	Citrix Monitorクラウドサービスがオンプレミスの Citrixコンポーネントを監視し、通信できるようにします。	ネットワークサービス

Active DirectoryにおけるCloud Connectorの展開シナリオ

Cloud Connector と Connector Appliance の両方を使用して Active Directory コントローラーに接続できます。使用するコネクタの種類は、展開によって異なります。

Active Directory で Connector Appliance を使用する方法の詳細については、「Active Directory での Connector Appliance の展開シナリオ」(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance/active-directory.html#deployment-scenarios-for-using-connector-appliance-with-active-directory)を参照してください。

Cloud Connector は、セキュリティで保護された内部ネットワーク内にインストールしてください。

単一フォレスト内に単一ドメインがある場合、そのドメインに Cloud Connector をインストールするだけで、リソースの場所を確立できます。環境内に複数のドメインがある場合は、ユーザーが利用可能なリソースにアクセスできるように、Cloud Connector をどこにインストールするかを検討する必要があります。

ドメイン間の信頼関係が親子関係でない場合、個別のドメインまたはフォレストごとに Cloud Connector をインストールする必要がある場合があります。この構成は、セキュリティグループを使用してリソースを割り当てる場合のリソース列挙を処理するため、またはどちらかのドメインからの VDA の登録のために必要になる場合があります。

> **注：**
>
> 以下のリソースの場所は、リソースがホストされている場所に応じて、他の物理的な場所で繰り返す必要があるブループリントを形成します。

単一フォレスト内の単一ドメインと単一の Cloud Connector セット

このシナリオでは、単一ドメインにすべてのリソースオブジェクトとユーザーオブジェクト (forest1.local) が含まれています。1 つの Cloud Connector セットが単一のリソースの場所に展開され、forest1.local ドメインに参加しています。

- 信頼関係：なし - 単一ドメイン
- **ID およびアクセス管理**にリストされているドメイン：forest1.local
- クラウドストアへのユーザーログオン：すべてのユーザーでサポート
- オンプレミスストアへのユーザーログオン：すべてのユーザーでサポート

> **注：**
>
> ハイパーバイザーインスタンスが別のドメインにある場合でも、ハイパーバイザーインスタンスと Cloud Connector が同じネットワーク経由で到達可能である限り、単一の Cloud Connector セットを展開できます。Citrix Cloud は、ホスティング接続と利用可能なネットワークを使用して、ハイパーバイザーとの通信を確立します。そのため、ハイパーバイザーが異なるドメインに存在する場合でも、Citrix Cloud がハイパーバイザーと通信できるように、そのドメインに別の Cloud Connector セットを展開する必要はありません。

単一フォレスト内の親ドメインと子ドメイン、単一のCloud Connectorセット

このシナリオでは、親ドメイン (forest1.local) とその子ドメイン (user.forest1.local) が単一のフォレスト内に存在します。親ドメインはリソースドメインとして機能し、子ドメインはユーザー ドメインです。単一のCloud Connectorセットが単一のリソースの場所に展開され、forest1.localドメインに参加しています。

- 信頼関係: 親/子ドメインの信頼
- **IDおよびアクセス管理**にリストされているドメイン: forest1.local、user.forest1.local
- クラウドストアへのユーザーログオン: すべてのユーザーでサポート
- オンプレミスストアへのユーザーログオン: すべてのユーザーでサポート

> **注:**
>
> Citrix Cloudが子ドメインを登録できるように、Cloud Connectorを再起動する必要がある場合があります。

単一のCloud Connectorセットを持つ、別々のフォレスト内のユーザーとリソース (信頼関係あり)

このシナリオでは、1つのフォレスト (forest1.local) にリソースドメインが含まれ、もう1つのフォレスト (forest2.local) にユーザー ドメインが含まれます。リソースドメインを含むフォレストがユーザー ドメインを含むフォレストを信頼する一方向の信頼が存在します。単一のCloud Connectorセットが単一のリソースの場所に展開され、forest1.localドメインに参加しています。

- 信頼関係: 一方向のフォレストの信頼
- **IDおよびアクセス管理**にリストされているドメイン: forest1.local
- クラウドストアへのユーザーログオン: forest1.localユーザーのみサポート
- オンプレミスストアへのユーザーログオン: すべてのユーザーでサポート

> **注:**
>
> 2つのフォレスト間の信頼関係により、ユーザーフォレストのユーザーがリソースフォレスト内のマシンにログオンできる必要があります。

> Cloud Connectorはフォレストレベルの信頼をトラバースできないため、Citrix Cloudコンソールの**IDおよびアクセス管理**ページにforest2.localドメインは表示されず、クラウド側の機能では使用できません。これにより、以下の制限が生じます。

- リソースは、Citrix Cloudのforest1.localに存在するユーザーとグループにのみ公開できます。ただし、オンプレミスストアを使用している場合、この問題を軽減するためにforest2.localのユーザーをforest1.localのセキュリティグループにネストできます。

- クラウドストアは、forest2.localドメインのユーザーを認証できません。
- Citrix DaaSのMonitorコンソールは、forest2.localドメインのユーザーを列挙できません。

これらの制限を回避するには、「各フォレストにCloud Connectorのセットを持つ、別々のフォレスト内のユーザーとリソース（信頼関係あり）」で説明されているようにCloud Connectorを展開します。

各フォレストにCloud Connectorのセットを持つ、別々のフォレスト内のユーザーとリソース（信頼関係あり）

このシナリオでは、1つのフォレスト（forest1.local）にリソースドメインが含まれ、もう1つのフォレスト（forest2.local）にユーザードメインが含まれます。リソースドメインを含むフォレストがユーザードメインを含むフォレストを信頼する一方向の信頼関係が存在します。Cloud Connectorの1つのセットはforest1.localドメイン内に展開され、2番目のセットはforest2.localドメイン内に展開されます。

- 信頼関係：一方向のフォレスト信頼
- **IDおよびアクセス管理**にリストされているドメイン：forest1.local、forest2.local
- クラウドストアへのユーザーログオン：すべてのユーザーでサポート
- オンプレミスストアへのユーザーログオン：すべてのユーザーでサポート

このシナリオでは、特に複数のユーザーフォレストがある場合、コストと管理オーバーヘッドを削減するために、リソースのないユーザーフォレストのCloud Connectorの代わりにConnector Applianceを使用できます。詳細については、「すべてのフォレストに単一のConnector Applianceセットを持つ、別々のフォレスト内のユーザーとリソース（信頼関係あり）」を参照してください。

Cloud Connectorの正常性を表示する

Citrix Cloudの「リソースの場所」ページには、リソースの場所にあるすべてのCloud Connectorの正常性ステータスが表示されます。また、個々のCloud Connectorの詳細なヘルスチェックデータも表示できます。詳細については、「Cloud Connectorの高度なヘルスチェック」を参照してください。

Windows イベントログ

Cloud Connector は、Windows イベントビューアーで表示できる特定の Windows イベントログを生成します。これらのログを監視ソフトウェアで確認できるようにしたい場合は、ZIPアーカイブとしてダウンロードできます。ZIPダウンロードには、以下のXMLファイルにこれらのログが含まれています。

- Citrix.CloudServices.Agent.Core.dll.xml (コネクタエージェントプロバイダー)

- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (コネクタ AgentWatchDog プロバイダー)

CITRIX.CLOUDSERIVCES.AGENTWATCHDOG

通常の操作中に、以下のイベントが発生する可能性があります。

イベントID	イベント	説明
10000	ConnectedToMessagingService	このイベントは、Connectorが Citrix Cloud との長期的なアウトバウンド WebSocket 接続を確立し、Citrix Cloud との双方向通信を可能にしたときに発生します。
10001	ConnectedToMessagingServiceWithWebProxy	アドレス「{0}」のWebプロキシを介してメッセージングサービスに接続しました。WebSocket接続は、構成されたプロキシを使用して設定されました。
10002	UnableToConnectToMessagingService	メッセージングサービス「{0}」に接続できません。Cloud ConnectorがCitrix CloudへのWebSocketを確立できませんでした。
10003	UnableToConnectToMessagingServiceWithWebProxy	アドレス「{0}」のWebプロキシを介してメッセージングサービスに接続できません。構成されたプロキシを使用しているときに、Cloud ConnectorがCitrix CloudへのWebSocketを確立できませんでした。
10004	ClockOutOfSyncError	Citrix Cloudとの通信に問題が発生しました。このマシンの時計が正しい時刻とタイムゾーン (UTC) に設定されていることを確認してください。問題を解決するには、マシン

イベントID	イベント	説明
		を再起動する必要がある場合があります。
10005	ConnectivityCheckHealthyToFailedStatus	Cloud Connectorの時間ごとのヘルスチェックで、以前は正常だったにもかかわらず障害が報告されました。
10006	ConnectivityCheckFailedStatus	Cloud Connectorの時間ごとのヘルスチェックで障害が報告されました。過去にも障害が発生しています。
10007	ConnectivityCheckFailedToHealthyStatus	Cloud Connectorの1時間ごとのヘルスチェックは、以前に障害が発生した後、正常なステータスを報告しました。
10008	ConnectivityCheckHealthyStatus	Cloud Connectorの1時間ごとのヘルスチェックは、以前から正常であった後、正常なステータスを報告しました。

CITRIX.CLOUDSERVICES.AGENT

通常の操作中に、次のイベントが発生する可能性があります。

10100	ConnectedToForest	ドメインコントローラーを持つフォレストに接続しました。
10101	UnableToConnectToForest	フォレストに接続できません。ホストコンピューターがドメインに参加しており、ネットワーク接続があることを確認してください。
10102	UnableToConnectToForestWithDomainName	ドメインに関連付けられたフォレストに接続できません。

10103	ClockOutOfSyncError	Citrix Cloudとの通信に問題がありました。このマシンの時計が正しい時刻とタイムゾーン (UTC) に設定されていることを確認してください。問題を解決するには、マシンを再起動する必要がある場合があります。

BrokerまたはLHCイベントログの詳細については、イベントログを参照してください。

Cloud Connectorイベントメッセージをダウンロードします。

コネクタログファイル

デフォルトでは、イベントログはCloud Connectorをホストしているマシンの`C:\ProgramData\Citrix\WorkspaceCloud\Logs`ディレクトリにあります。

トラブルシューティング

Cloud Connectorに関する問題を診断する最初のステップは、イベントメッセージとイベントログを確認することです。リソースの場所でCloud Connectorがリストされていない場合、または「連絡不能」である場合、イベントログはいくつかの初期情報を提供します。

Cloud Connector の接続

Cloud Connector が「切断」状態の場合、Cloud Connector Advanced Connectivity Check Tool を使用すると、Cloud Connector が Citrix Cloud および関連サービスに到達できることを確認できます。

詳細については、Cloud Connector Advanced Connectivity Check Tool を参照してください。

インストール

Cloud Connector が「エラー」状態の場合、Cloud Connector のホストに問題がある可能性があります。新しいマシンに Cloud Connector をインストールしてください。問題が解決しない場合は、Citrix Support にお問い合わせください。Cloud Connector のインストールまたは使用に関する一般的な問題のトラブルシューティングについては、CTX221535 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 は、認証されていない Web プロキシサーバーを介したインターネットへの接続をサポートしています。インストーラーと、それがインストールするサービスの両方が Citrix

Cloud への接続を必要とします。 インターネットアクセスは、これら両方のポイントで利用可能である必要があります。

接続要件

HTTP トラフィックにはポート 443 を使用し、エグレスのみを許可します。必要な接続可能アドレスのリストについては、以下のリソースを参照してください。

- システムおよび接続要件
- Cloud Connector 共通サービス接続要件

Citrix Cloud の必要な接続可能アドレスは、IP アドレスではなくドメイン名として指定されています。IP アドレスは変更される可能性があるため、ドメイン名を許可することで、Citrix Cloud への接続が安定した状態に保たれます。

必要なポートのリストについては、受信および送信ポートの構成を参照してください。

> **重要:**

> - 特定のプロキシで SSL インターセプトを有効にすると、Cloud Connector が Citrix Cloud に正常に接続できなくなる可能性があります。
> - Citrix Gateway アドレスでは SSL インターセプトを実行できません。詳細については、Citrix Gateway Services 接続要件を参照してください。
> - SSL インターセプトは、ネットワーク接続性や安定性に影響を与えてはなりません。詳細については、Citrix Cloud Connectorを参照してください。
> - プロキシを使用している場合、以下のトラフィックフローはプロキシをバイパスする必要があります。
>
> ◦ コネクタ間の通信（LHC イベント中など）。
>
> ◦ コネクタと VDA 間の通信（WCF 接続）。
>
> ◦ コネクタとドメインコントローラー間の通信 (ADリクエスト)。

> さらに、コネクタがWinHTTPプロキシ設定を利用することに注意することが重要です。構成設定については、CTX222727を参照してください。

Cloud Connectorの接続を確認する

Cloud Connector Advanced Connectivity Check Toolは、一連の接続チェックを使用して、Cloud ConnectorとCitrix Cloud間の接続を確認するのに役立ちます。

詳細については、Cloud Connector Advanced Connectivity Check Toolを参照してください。

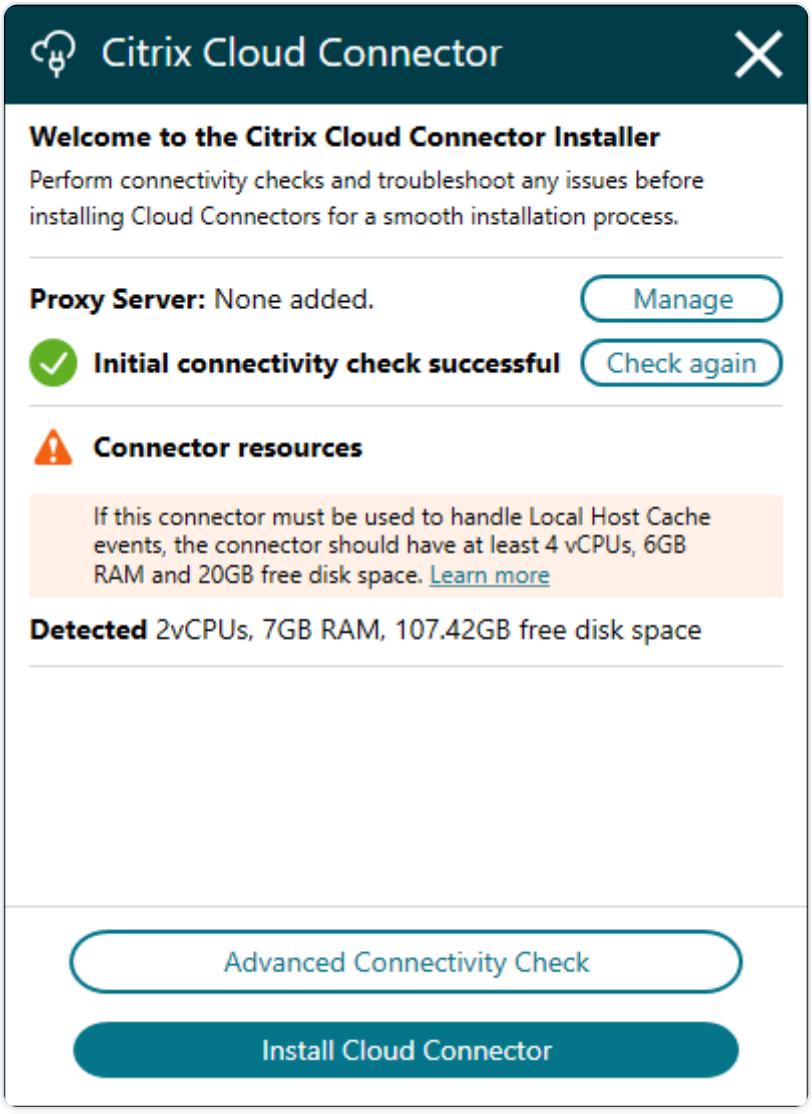
インストーラー

インストーラーは、インターネット接続用に構成された設定を使用します。マシンからインターネットを閲覧できる場合、インストーラーも機能するはずです。

ランタイム時のサービス

ランタイムサービスはローカルサービスのコンテキストで動作します。ユーザー用に定義された設定（上記参照）は使用しません。

インストールプロセス中にプロキシ設定を構成できます。



インストーラーが起動したら、Citrix Cloudにログインする前に、**Configure Proxy**をクリックします。プロキシ情報とプロキシをバイパスするアドレスを追加するよう求められます。バイパスアドレスを指定する際には、完全修飾ドメイン名 (FQDN) とワイルドカードアドレスの両方がサポートされます。

> **注:**
>
> プロキシサーバーを使用している場合は、手動プロキシ設定を使用する必要があります。自動検出またはPAC/セットアップスクリプトによる自動プロキシ設定はサポートされていません。

Cloud Connector のインストール

Cloud Connector ソフトウェアは、対話形式またはコマンドラインを使用してインストールできます。

インストールは、インストールを開始するユーザーの権限で実行されます。Cloud Connector がクラウドにアクセスする必要があるのは、次の目的のためです。

- インストールを実行するユーザーを認証する
- インストーラーの権限を検証する
- Cloud Connector サービスをダウンロードして構成する

インストール前に確認する情報

インストール前にシステム要件を確認してください。

展開後のガイダンス

インストール後、Citrix Cloud への常時接続を確保するために、すべての Cloud Connector の電源を継続的にオンにしたままにしてください。

アップグレード

アップグレードは通常、Citrix Cloud によって自動的に管理されます。手動でアップグレードするには、新しいバージョンをインストールする前に、古い Cloud Connector をアンインストールしてください。以前にインストールした Cloud Connector を新しいバージョンでアップグレードしないでください。Cloud Connector の個々のコンポーネントを個別にアップグレードしないでください。

マシンの名前変更

インストール後、Cloud Connector をホストしているマシンの名前を変更しないでください。後でサーバー名を変更する必要がある場合は、次のタスクを実行してください。

1. リソースの場所からマシンを削除する:
    a. Citrix Cloudメニューから、**リソースの場所**を選択します。
    b. 管理するリソースの場所を見つけて、**Cloud Connectors**タイルを選択します。
    c. 管理するマシンを見つけて、省略記号メニューをクリックします。**コネクタの削除**を選択します。
2. Cloud Connectorソフトウェアをアンインストールします。
3. マシンの名前を変更します。
4. この記事で説明されているように、Cloud Connectorソフトウェアの最新バージョンをインストールします。

マシンを別のドメインに移動する

インストール後、Cloud Connectorをホストしているマシンを別のドメインに移動しないでください。後でマシンを別のドメインに参加させる必要がある場合は、次のタスクを実行します。

1. リソースの場所からマシンを削除します。
2. Cloud Connectorソフトウェアをアンインストールします。
3. マシンを現在のドメインから切断し、新しいドメインに再参加させます。
4. この記事で説明されているように、Cloud Connectorソフトウェアの最新バージョンをインストールします。

クローン作成されたマシンに関する考慮事項

Citrix Cloudがリソースの場所にあるマシンと確実に通信できるように、Cloud Connectorをホストする各マシンには一意のSIDとコネクタIDが必要です。リソースの場所にある複数のマシンでCloud Connectorをホストし、クローン作成されたマシンを使用する場合は、次の手順を実行します。

1. 環境の要件に従ってマシンテンプレートを準備します。
2. Cloud Connectorとして使用する予定のマシンの数をプロビジョニングします。
3. 各マシンに、手動またはサイレントインストールモードを使用してCloud Connectorをインストールします。

マシンテンプレート（クローン作成前）にCloud Connectorをインストールすることはサポートされていません。Cloud Connectorがインストールされたマシンをクローンした場合、Cloud Connectorサービスは実行されず、マシンはCitrix Cloudに接続できません。

サービスに関する考慮事項

この記事のインストール手順では、Cloud Connectorが使用されるサービスに関係なく、Cloud Connectorを展開するプロセスについて説明します。

Citrix DaaS向けにCloud Connectorを展開する場合、コネクタが存在するADドメインがアクティブであり、Citrix Cloudコンソールで「未使用」と表示されていないことを確認してください。Citrix DaaSでマシンカタログ設定中に未使用のドメインを指定すると、エラーが発生する可能性があります。詳細については、Citrix DaaS製品ドキュメントのCitrix Cloudでリソースタイプを追加するか、未使用のドメインをアクティブ化するを参照してください。

その他のサービスに関する追加の考慮事項については、サービスのドキュメントを参照してください。

デフォルトのリソースロケーション

Citrix Cloudアカウントにリソースロケーションがなく、ドメインにCloud Connectorをインストールすると、Citrix Cloudが作成するリソースロケーションがデフォルトのリソースロケーションになります。アカウントにはデフォルトのリソースロケーションを1つしか持つことができません。必要に応じて、Citrix Cloudで追加のリソースロケーションを作成し、他のドメインにCloud Connectorをインストールする際に、目的のリソースロケーションを選択できます。

または、ドメインにCloud Connectorをインストールする前に、コンソールで必要なリソースロケーションを最初に作成することもできます。Cloud Connectorインストーラーは、インストール中に目的のリソースロケーションを選択するように求めます。

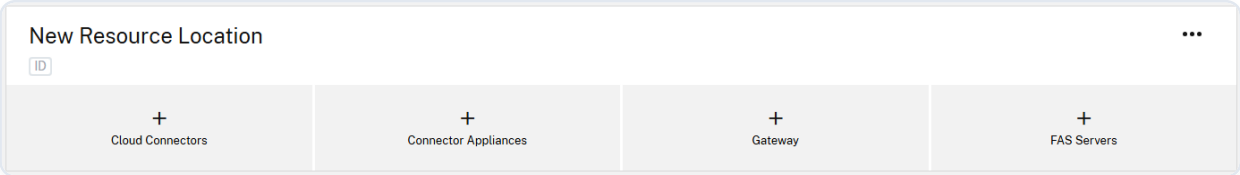
対話型インストール

グラフィカルインストーラーインターフェイスを使用してCloud Connectorをダウンロードおよびインストールできます。これを行う前に、Cloud Connectorを展開するために、Citrix Cloud管理コンソールで1つ以上のリソースロケーションを作成する必要があります。リソースロケーションの詳細については、リソースロケーションを参照してください。

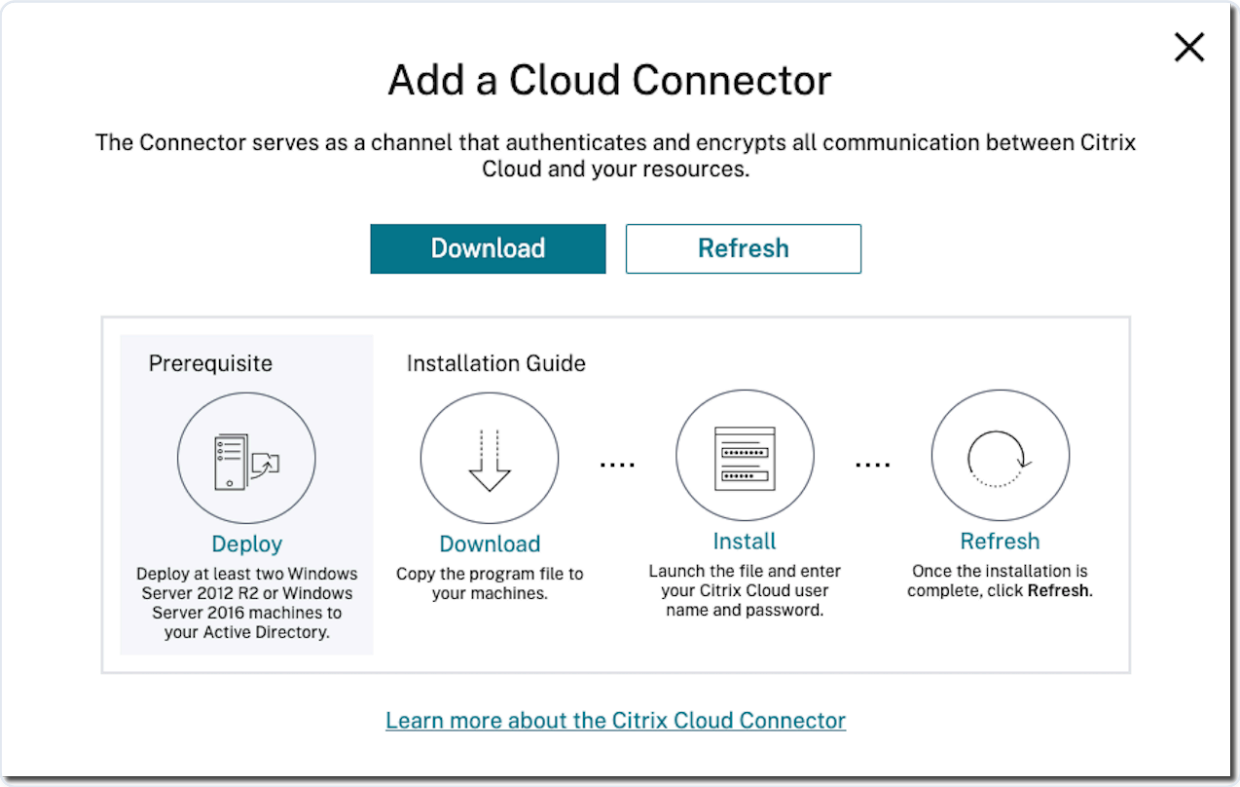
Citrix Cloud Connector™ソフトウェアをダウンロードする

1. Citrix Cloud Connectorをインストールする予定のマシンにWindows管理者としてサインインします。
2. https://citrix.cloud.comにアクセスし、管理者アカウントにサインインします。
3. Citrix Cloudコンソールで、メインメニューから**リソースの場所**に移動します。

4. リソースの場所がまだない場合は、プラスアイコン（+）をクリックするか、**リソースの場所を追加**を選択します。詳細については、リソースの場所を作成するを参照してください。
5. 管理したいリソースの場所を見つけて、**+ Cloud Connectors**を選択します。



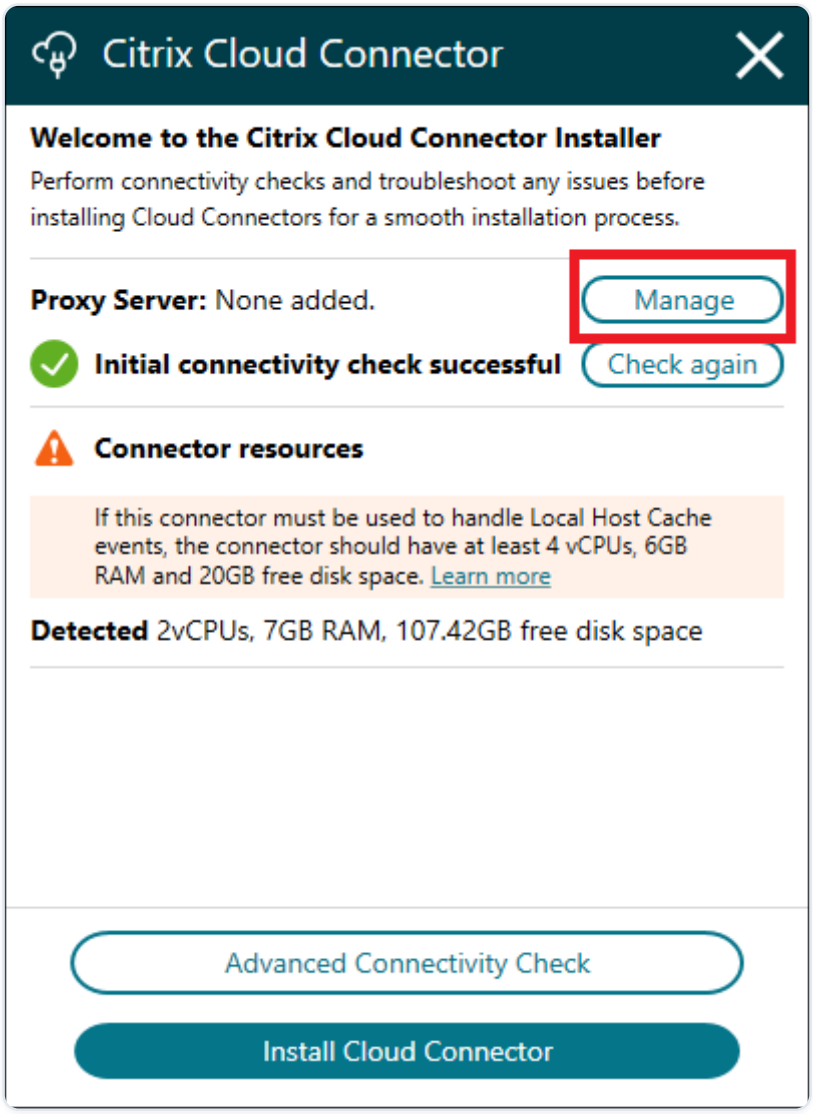
6. 開いたウィンドウで**ダウンロード**を選択します。**cwcconnector.exe**ファイルをコネクタマシンのローカルファイル場所に保存します。



Citrix Cloud Connectorソフトウェアをインストールする

前提条件

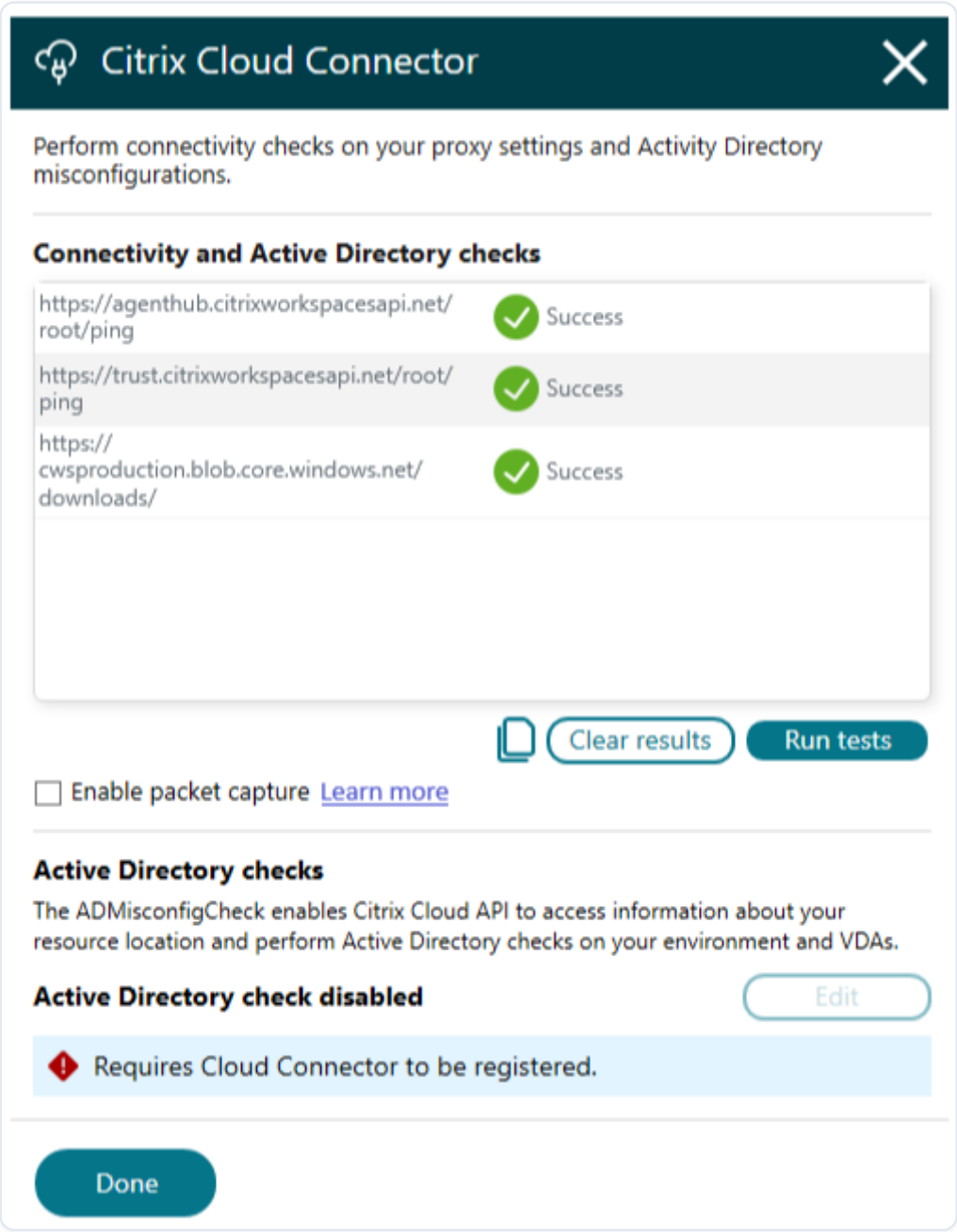
1. `cwcconnector.exe`インストーラーファイルを右クリックし、**管理者として実行**を選択します。インストーラーは、Cloud Connectorをインストールする前にCitrix Cloudに接続できることを確認するために、初期接続チェックを実行します。
2. プロキシサーバーを更新するには、**管理**をクリックします。



注:

Microsoft WinHTTPの制限により、サポートされるプロキシサーバーは1つだけです。詳細については、WinHTTPのAutoProxyに関する問題を参照してください。

1. **詳細接続チェック**をクリックして、コネクタのインストールに必要な基本的な接続要件がマシンで満たされていることを確認するための詳細なチェックを実行します。



初回アップグレードとテスト

1. **プロキシサーバー**を更新し、**高度な接続チェック**を確認した後、**Cloud Connectorのインストール**をクリックします。
2. **サインイン**ページで、**サインインしてインストール**をクリックします。

   Cloud Connectorのログイン(/en-us/citrix-cloud/media/cloud-connector-login.png)
3. **Citrix Cloud接続テスト**ウィンドウが表示され、初回アップグレードとテストのステータスがイベントログとともに表示されます。

   進行中の初回テスト(/en-us/citrix-cloud/media/initial-tests-in-progress.png)

4. **ログの表示**をクリックして、すべての接続チェックデバッグログを含むディレクトリ`(C:\ProgramData\Citrix\WorkspaceCloud\InstallLogs)`を開きます。
5. 初回アップグレードとテストが完了すると、次の図に示すように、Citrix Cloud接続テストが**成功**したことが表示されます。接続チェックの結果は、最初のアップグレード後にイベントログボックスに表示されます。

   初回テスト完了(/en-us/citrix-cloud/media/initial-tests-complete.png)

未使用のドメインをアクティブ化する

リソースの場所を作成し、Citrix DaaS™ 用にCloud Connectorを展開する場合は、Citrix DaaSで使用しているADドメインがアクティブであり、未使用と見なされていないことを確認してください。Citrix DaaSでマシンカタログを設定する際に未使用のドメインを指定すると、エラーが発生する可能性があります。

詳細については、Citrix DaaS製品ドキュメントのCitrix Cloudでリソースタイプを追加するか、未使用のドメインをアクティブ化するを参照してください。

追加のリソースの場所を作成する

1. Citrix Cloud管理コンソールから、メニューボタンをクリックし、**リソースの場所**を選択します。
2. **+ リソースの場所**をクリックし、意味のある名前を入力します。
3. 「**保存**」をクリックします。Citrix Cloud に新しいリソースロケーションのタイルが表示されます。
4. 「**Cloud Connectors**」をクリックし、次に「**ダウンロード**」をクリックして Cloud Connector ソフトウェアを入手します。
5. 準備された各マシンに、インストールウィザードまたはコマンドラインインストールを使用して Cloud Connector ソフトウェアをインストールします。Citrix Cloud は、Cloud Connector に関連付けるリソースロケーションを選択するように求めます。

複数の顧客と既存のリソースロケーションでのインストール

複数の顧客アカウントの管理者である場合、Citrix Cloud は、Cloud Connector に関連付ける顧客アカウントを選択するように求めます。

顧客アカウントに複数のリソースロケーションがすでに存在する場合、Citrix Cloud は、Cloud Connector に関連付けるリソースロケーションを選択するように求めます。

コマンドラインインストール

サイレントインストールまたは自動インストールがサポートされています。ただし、コネクタインストーラーは定期的に更新されるため、インストールごとに最新のインストーラーをダウンロードすることをお勧めします。Citrix Cloud コンソールの ページから新しい Cloud Connector インストーラーをダウンロードします。

要件

Citrix Cloud でコマンドラインインストールを使用するには、次の情報を提供する必要があります。

- Cloud Connector をインストールする Citrix Cloud アカウントの顧客 ID。この ID は、**Identity and Access Management** の「**API アクセス**」タブの上部に表示されます。
- Cloud Connector のインストールに使用するサービスプリンシパルの ID とシークレット。これらの値を取得するには、まずサービスプリンシパルを作成する必要があります。サービスプリンシパルは「Full Access」で作成する必要があります。サービスプリンシパルの作成の詳細については、「サービスプリンシパルの作成」を参照してください。サービスプリンシパルの ID とシークレットを取得したら、Cloud Connector のインストールを続行できます。
- Cloud Connector に関連付けるリソースロケーションのリソースロケーション ID。この値を取得するには、**リソースロケーション**ページの、リソースロケーション名の下にある「**ID**」ボタンを選択します。この値を指定しない場合、Citrix Cloud はデフォルトのリソースロケーションの ID を使用します。

サポートされているパラメーター

サービスプリンシパルの ID とシークレットのセキュリティを確保するために、JSON 構成ファイルをインストーラーに提供する必要があります。このファイルは、インストールが完了した後に削除する必要があります。構成ファイルのサポートされている値は次のとおりです。

- **customerName** 必須。Citrix Cloudコンソール（IDおよびアクセス管理内）のAPIアクセスページに表示される顧客ID。
- **clientId** 必須。APIアクセスページで管理者が作成できるサービスプリンシパルID。
- **clientSecret** 必須。サービスプリンシパル作成後にダウンロードできるサービスプリンシパルシークレット。APIアクセスページにあります。
- **resourceLocationId** 推奨。既存のリソースロケーションの一意の識別子。Citrix Cloudコンソールのリソースロケーションページで、IDボタンを選択してリソースロケーションIDを取得します。値が指定されていない場合、Citrix Cloudはアカウント内の最初のリソースロケーションのIDを使用します。
- **acceptTermsOfService** 必須。**true**に設定する必要があります。

サンプル構成ファイル

```
{

"customerName": "CustomerID",

"clientId": "clientID",

"clientSecret": "ClientSecret",

"resourceLocationId": "ResourceLocationId",

"acceptTermsOfService": "true"

}
```

サンプルコマンド

次のコマンドは、JSON構成ファイルを使用してCloud Connectorソフトウェアをサイレントインストールします：

```
CWCConnector.exe /q /ParametersFilePath:c:
\cwcconnector_install_params.json
```

サイレントインストールを指定するには、`/q`を使用します。

失敗した場合に潜在的なエラーコードを調べるには、**Start /Wait CWCConnector.exe /ParametersFilePath:value**を使用します。インストール完了後に**echo %ErrorLevel%**を実行する標準的なメカニズムを使用できます。

HTTPS構成

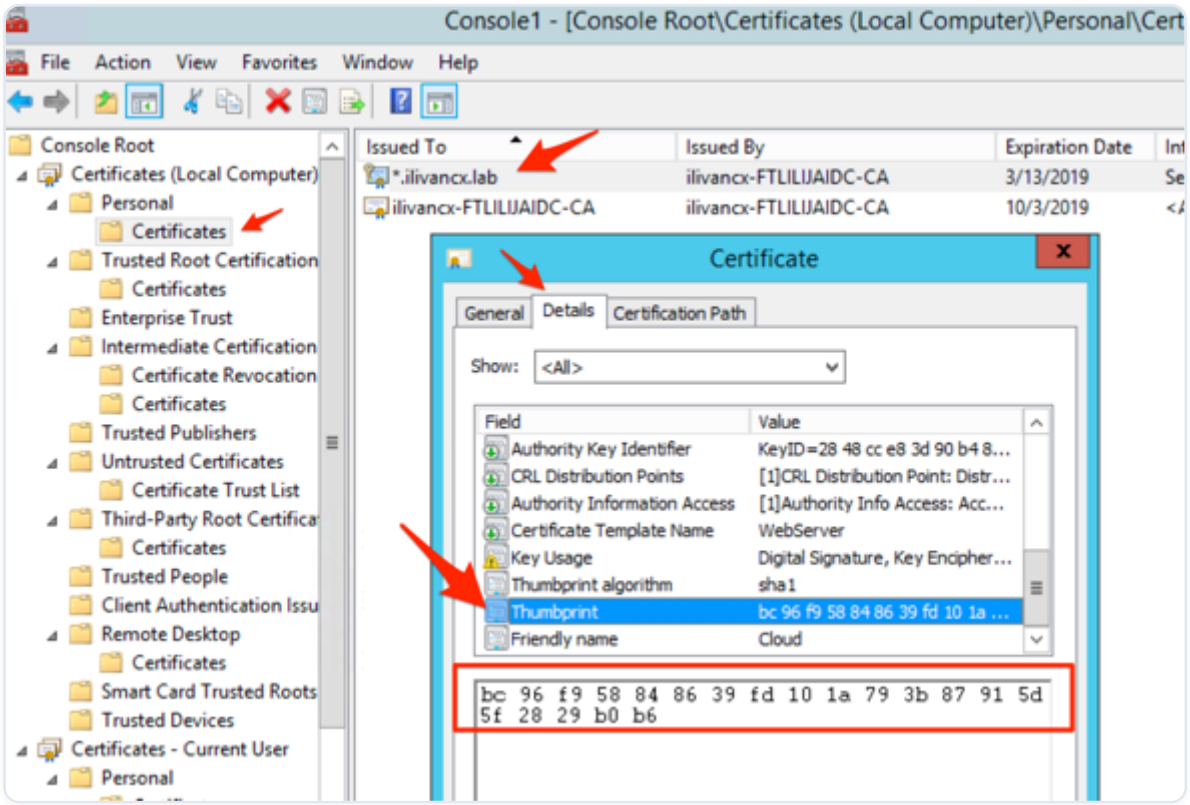
StoreFront™およびNetScaler GatewayアプライアンスがCloud Connectorに安全に接続し、すべてのデータを暗号化できるようにするには、HTTPSを有効にすることを強くお勧めします。これにはSSL証明書が必要です。

- 証明書には、コネクタに到達するために使用されるFQDNをコモンネームまたはサブジェクト代替名として含める必要があります。コネクタの前にロードバランサーを導入している場合は、ロードバランサーのFQDNを使用します。
- 証明書は、エンタープライズCAまたはパブリックCAによって署名できます。

- Cloud Connectorに接続するStoreFrontおよびゲートウェイサーバーは、証明書を信頼する必要があります。

HTTPSを有効にするには:

1. 証明書 MMC スナップインを開きます。
2. 個人証明書ストアに適切な証明書を作成またはインポートします。証明書の管理の詳細については、「証明書の管理」を参照してください。
3. 証明書を開き、**詳細**タブに移動して、**拇印**をメモします（スペースは無視してください）。



4. 証明書をバインドするIPアドレスを決定します。通常、すべてのIPv4アドレスに適用するには、`0.0.0.0`のIPアドレスを使用できます。IPv6が有効になっている場合は、すべてのIPv6アドレスに適用するために`[::]`を使用します。変更を特定のネットワークアダプターにのみ適用する場合は、そのネットワークアダプターのIPアドレスをメモしてください。
5. 管理者特権のコマンドプロンプトで実行します

```
netsh http add sslcert ipport=<IP address>:<Port number>
certhash=<Certificate Hash Number> appid={Any GUID}
```

AppIdには任意の有効なGUIDを使用できます。その目的は、どのアプリケーションがバインディングを追加したかを記録することです。ただし、バインディングはそのポートを使用するすべてのアプリケーションに適用されます。

例:

```
C:\> netsh http add sslcert ipport=0.0.0.0:443
certhash=BC96F958848639FD101A793B87915D5F2829B0B6 appid={6DE9BEFD-
F4CB-4D63-8681-E88012D6F5F1}



SSL Certificate successfully added
```

6. HTTPを無効にするには、レジストリで `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer` に移動し、名前が `XMLServicesEnableNonSSL` で値が0の `DWORD` を作成します。

次のステップ

1. Citrix Cloud Connectorの更新スケジュールを設定します。Citrix Cloud Connectorの更新と更新スケジュールの管理については、「コネクタの更新」を参照してください。
2. StoreFrontを使用している場合は、コネクタを使用してDaaSにアクセスし、リソースを列挙して起動できるようにStoreFrontを構成します。これが新しいDaaS展開における最初のコネクタである場合は、新しいリソースフィードを作成します。追加のコネクタである場合は、回復性を高めるために、既存のDaaSリソースフィードのサーバーリストにすべてのCloud Connectorを追加することをお勧めします。詳細については、「ストアで利用可能になったリソースの管理」を参照してください。
3. NetScaler GatewayでStoreFrontを使用している場合は、コネクタを使用してCitrix Cloud Secure Ticket Authority (STA) にアクセスできます。詳細については、「Citrix Gatewayの構成」を参照してください。
4. 特定のActive Directoryドメインでこれが最初のコネクタである場合は、そのドメインをCitrix Cloudに接続できます。詳細については、「Active DirectoryをCitrix Cloudに接続するには」を参照してください。

インストールに関する問題のトラブルシューティング

このセクションでは、インストール中に発生する可能性のある問題を診断し、修正する方法について詳しく説明します。インストールに関する問題のトラブルシューティングの詳細については、「Citrix Cloud Connectorトラブルシューティングガイド」を参照してください。

インストールログ

インストール中に発生した問題は、まず利用可能なログファイルを参照することでトラブルシューティングできます。

インストール中に発生したイベントは、**Windowsイベントビューアー**で確認できます。また、Cloud Connectorのインストールログは、**%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**にあります。 ログはインストール後、**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs**にも追加されます。

終了コード

インストールプロセスの成功または失敗に応じて、次の終了コードが返される場合があります。

- 1603 - 予期しないエラーが発生しました
- 2 - 前提条件チェックに失敗しました
- 0 - インストールが正常に完了しました

インストールエラー

インストーラーをダブルクリックしてCitrix Cloud Connectorソフトウェアをインストールすると、次のエラーメッセージが表示されることがあります。

`Can't reach this page.`.

このエラーは、Citrix Cloud Connectorをインストールするために管理者としてマシンにログインしている場合でも発生する可能性があります。このエラーを回避するには、インストーラーを右クリックして「管理者として実行」を選択し、Citrix Cloud Connectorソフトウェアを管理者として実行します。

接続障害

Cloud Connector が Citrix Cloud と通信できることを確認するには、以下の Citrix サービスが **開始済み** 状態であることを確認してください。

- Citrix Cloud AD プロバイダー
- Citrix Cloud エージェントロガー
- Citrix Cloud エージェントシステム
- Citrix Cloud エージェントウォッチドッグ
- Citrix Cloud 資格情報プロバイダー
- Citrix コンフィグ シンクロナイザー サービス
- Citrix 高可用性サービス

- Citrix ネットスケーラー® クラウドゲートウェイ
- Citrix リモートブローカープロバイダー
- Citrix リモート HCL サーバー
- Citrix セッションマネージャープロキシ

これらのサービスの詳細については、「インストールされているサービス」を参照してください。

Cloud Connector Advanced Connectivity Check Tool を使用すると、Cloud Connector が Citrix Cloud および関連サービスに到達できることを確認できます。

詳細については、「Cloud Connector Advanced Connectivity Check Tool」を参照してください。

接続チェックの失敗を解決する方法の詳細については、CTX224133: Cloud Connectorの接続チェックが失敗しましたを参照してください。

Cloud Connector の高度な接続チェック

Cloud Connector には、管理者が接続の問題を診断およびトラブルシューティングするのに役立つ2つのツールがパッケージ化されています。これらは、Cloud Connector インストーラーで利用できる `Advanced Connectivity Checks` と、Cloud Connector ソフトウェアと一緒にインストールされる `Citrix Cloud Services Connectivity Test Tool` です。

両方のツールには、以下のテストが含まれています。

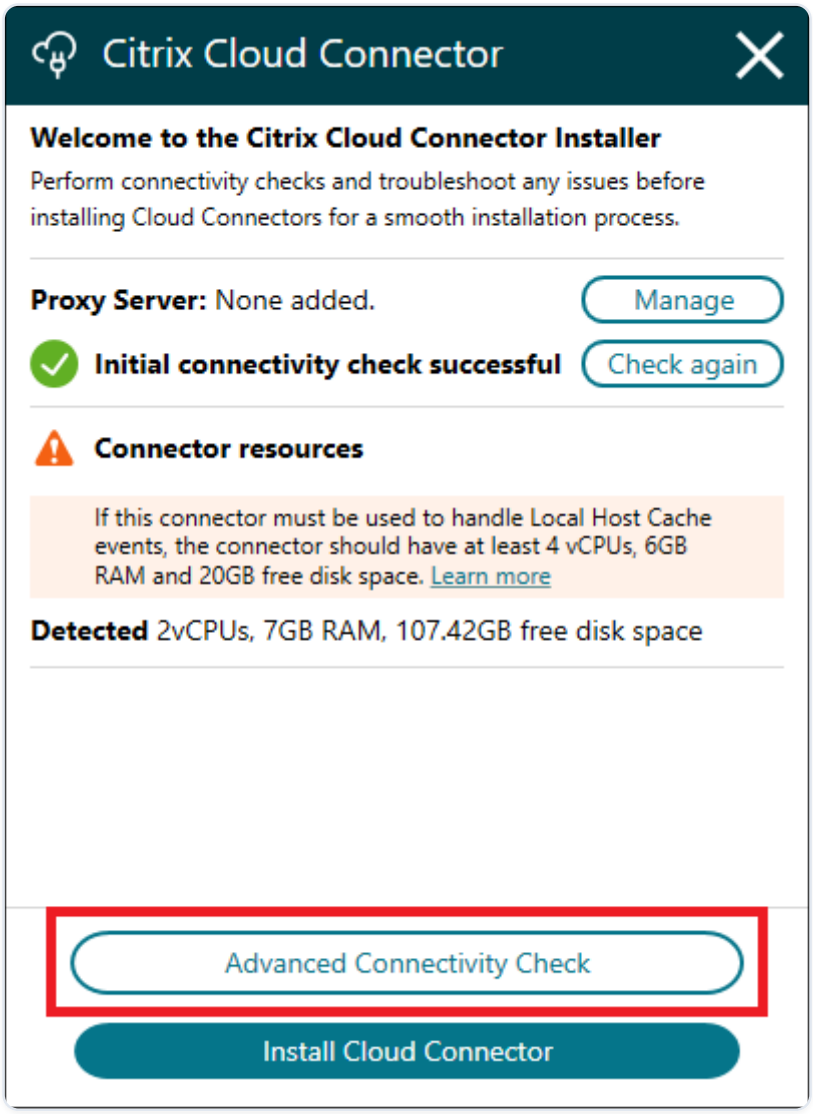
- Cloud Connector 接続要件 に準拠したプロキシおよびファイアウォールの構成
- 証明書検証要件 に準拠した証明書の要件

これらのツールは、接続の問題の診断とトラブルシューティングを支援するために、ネットワークパケットキャプチャを実行するためにも使用できます。

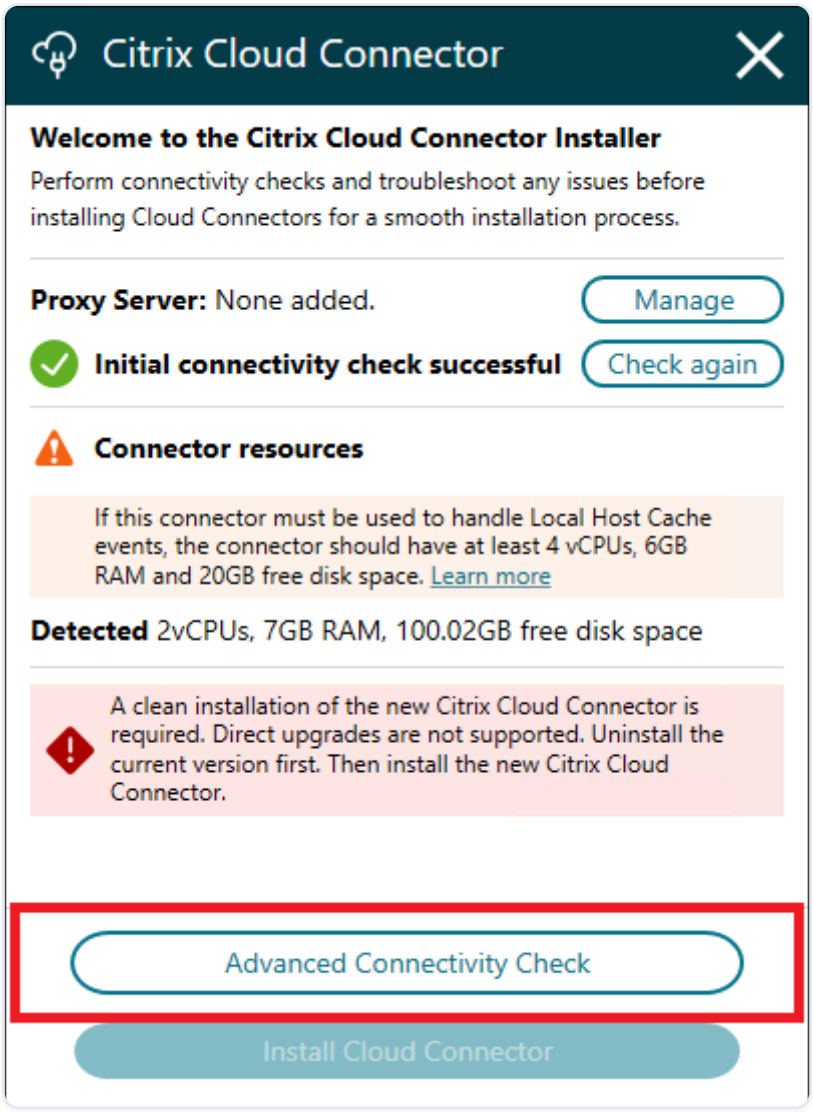
Cloud Connector インストーラーの高度な接続チェック

`Advanced Connectivity Checks` は Cloud Connector `cwcconnector.exe` インストーラーに含まれています。

チェックにアクセスするには、`cwcconnector.exe` インストーラーファイルを右クリックし、「管理者として実行」を選択します。「Advanced Connectivity Check」をクリックすると、Advanced Connectivity Check Tool にアクセスできます。



Cloud Connector ソフトウェアがホストマシンにすでにインストールされている場合、警告が表示され、`Install Cloud Connector` オプションは無効になりますが、「Advanced Connectivity Check」オプションは引き続き利用可能です。



インストーラーの高度な接続チェックによって実行されるチェック

Advanced Connectivity Check ツールによって実行されるチェックは、3つのカテゴリに分類されます。

- **初期チェック:** これらは、Cloud Connector をインストールして登録するために必要なプラットフォームサービスのチェックです。Cloud Connector のオーケストレーション、認証、およびアップグレードに関連するサービスへの接続を対象としています。
- **証明書チェック:** これらのテストは、Citrix Cloudへのセキュアな接続（TLS証明書）を検証するために必要なルート証明書と中間証明書の存在を検証し、アップグレードパッケージ（コード署名証明書）の整合性をチェックします。Cloud Connectorの証明書要件の詳細については、証明書検証要件を参照してください。
- **FQDNチェック:** これらのチェックは、Cloud Connector共通サービス要件で公開されている完全修飾ドメイン名（FQDN）AllowList.jsonに記載されている残りのサービスへの接続を対象としています。

Citrix Cloud Services接続テストツール

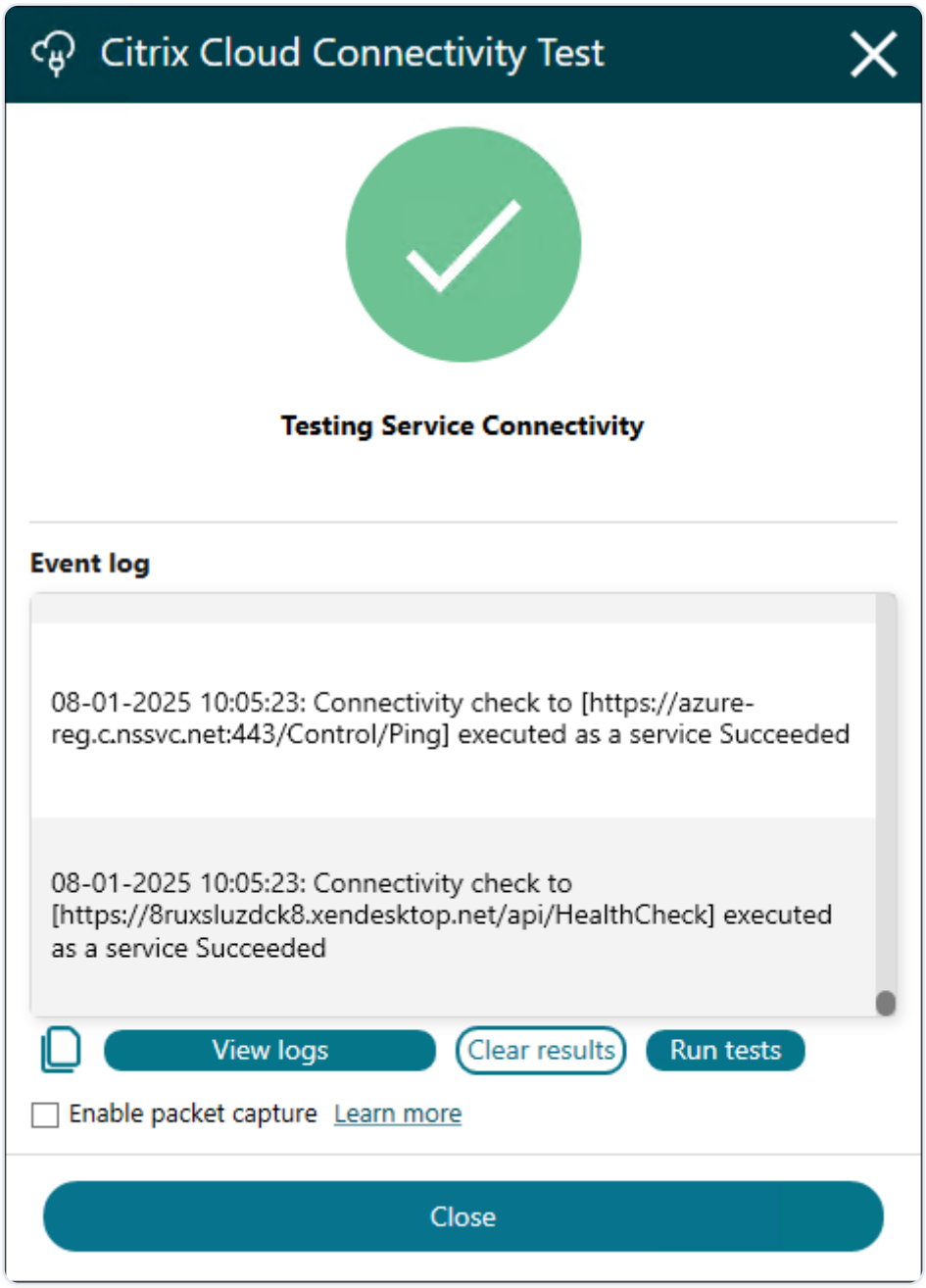
`Citrix Cloud Services Connectivity Test Tool`は、Cloud Connectorソフトウェアがすでにインストールされているホストマシンでのみ利用可能です。`Start Menu > Citrix > Citrix Cloud Services Connectivity Test Tool`に移動することでアクセスできます。

Citrix Cloud Services接続テストツールによって実行されるチェック

スタンドアロンの`Citrix Cloud Services Connectivity Test Tool`は、上記で説明した初期、証明書、およびFQDNチェックと同じセットを実行します。さらに、ユースケース固有の追加テストも実行します。

Citrix Cloud Connector™は、それぞれのユースケースに関連する多数のサービスをインストールします。これらの各サービスは、特定のユースケースに関連する一連の接続チェックを実装しています。Citrix Cloud Services接続テストツールは、各サービスにクエリを実行して、特定のユースケース向けに実装されたテストを実行します。

これらのテストの詳細は、ツールを実行することで確認できます。同じ内容のログファイルにアクセスすることも可能です。

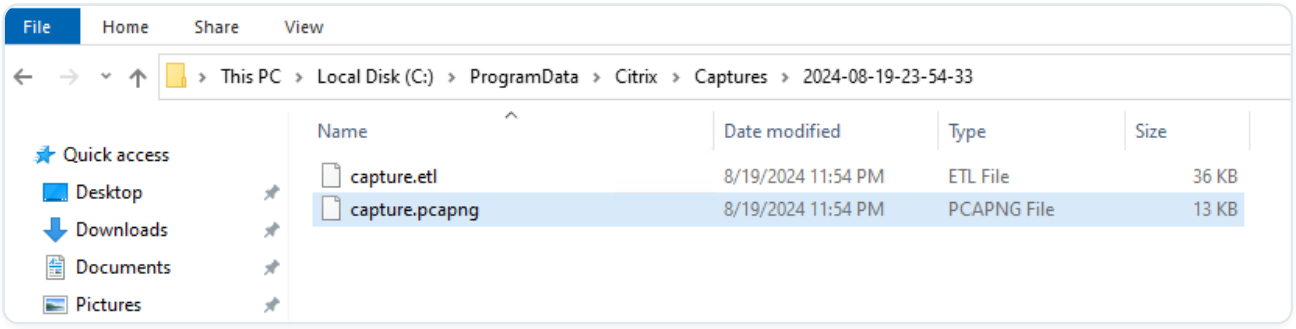


パケットキャプチャ

`Advanced Connectivity Checks`と`Citrix Cloud Services Connectivity Test Tool`の両方には、実行する接続チェックと並行してパケットキャプチャを実行する機能が含まれています。デフォルトでは、このチェックボックスは選択されていないため、明示的に有効にしない限りパケットキャプチャは実行されません。

アクティブ化すると、この機能はWindowsに組み込まれている`pktmon`ユーティリティを利用して、接続チェック中にネットワークトラフィックをキャプチャします。チェックが完了すると、キャプチャされたデータは`C:\ProgramData\Citrix\Captures`の下のタイムスタンプ付きサブディレクトリにローカルに保存されます。ファイルは.etl形式と.pcapng形式の両方で保存されま

す。.pcapngは、Wiresharkなどのツールと互換性のある広く使用されている形式です。これらのファイルはローカルマシンに残り、Citrix Cloudにはアップロードされません。



追加のサポートが必要な顧客の場合、これらのパケットキャプチャは、接続問題の診断を支援するために当社のサポートチームと共有できます。

注:

インストーラーの「Advanced Connectivity Check」画面または「Citrix Cloud Connectivity Test」ツールでパケットキャプチャ機能が有効化されると、接続性チェック中に発生するすべてのネットワークトラフィックが記録されます。これには、接続性チェックとその関連Cloud Connectorコンポーネントによって生成されるトラフィックだけでなく、Cloud Connector VM上の他のネットワークアクティビティによって生成されるトラフィックも含まれます。例えば、接続性チェック中に発生するログイン試行などの暗号化されていないHTTPトラフィックも、結果のパケットキャプチャファイルにキャプチャされます。

Cloud Connector の高度なヘルスチェック - 非推奨

注:

Cloud Connector のヘルス指標とアラートが Citrix DaaS™ Infrastructure Monitoring に追加されました。これは、インフラストラクチャに関する問題をプロアクティブに分析およびトラブルシューティングするための主要な場所となるはずです。

詳細については、Infrastructure Monitoring を参照してください。

更新の前後に、Cloud Connector はヘルスチェックを実行して、更新によってプロバイダーに不要なダウンタイムが発生しないことを確認します。Connector および Connector 上の各サービスまたはプロバイダーの接続性とヘルスステータスを確認できます。

Connector のヘルスチェックデータを表示する

1. Citrix Cloud™ メニューから、**リソースの場所**を選択します。
2. ヘルスチェックデータを表示したい Connector を選択します。
3. Connectors ページで、Connector の横にある省略記号メニューに移動し、**Connector データ表示**を選択します。

Connector データページが表示され、以下の情報が表示されます。

- **サービス接続ステータス**。Connector データページのこの領域には、以下が表示されます。
  - Connector がクラウドに接続されているかどうか
  - Connector とそのコンポーネントについて、現在インストールされているバージョンと、次回の更新でインストールされるターゲットバージョン
- **サービス接続履歴**。24 個のステータスインジケーターは、時間の経過に伴う Connector のヘルスステータスを示します。デフォルトでは、サービス接続履歴は過去 24 時間のステータスを 1 時間間隔で表示します。さらに履歴を表示するには、ドロップダウンメニューから**24 日**を選択します。このビューには、過去 24 日間のステータスが 1 日間隔で表示されます。
  - 緑色の点滅は、その時間間隔における正常なステータスを示します。
  - 赤い点は、その時間間隔における障害または例外ステータスを示します。詳細については、その点にカーソルを合わせます。
  - レンチアイコンは、その時間間隔中に更新が発生したことを示します。詳細については、レンチアイコンにカーソルを合わせます。
  - 灰色の点は、その時間間隔中にヘルスステータス情報が受信されなかったことを示します。

  Connector の高度なヘルスチェックメインページのサービス継続性履歴(/en-us/citrix-cloud/media/connector-data.png)
- **サービス**。この領域には、Connector で実行されている各サービスが一覧表示されます。
  - 各サービスの横にある点は、サービスの現在のステータスを示します。
  - サービスからのアラートが通知されるかどうかを制御するには、**アラートオン**と**アラートオフ**を使用します。アラートがオンに設定されている場合、サービスでの障害は、Connector の全体的な接続ステータスの障害を引き起こします。
  - サービスの経時的なヘルスステータスの詳細を表示するには、**詳細の表示**を選択します。

- **Connector メトリック**。この領域には、過去24時間または24日間のConnectorのメモリ使用量、CPU、ネットワークデータ、ディスクスペースの使用状況が表示されます。表示される期間を制御するには、**サービス接続履歴**領域のドロップダウンメニューを使用します。

サービスの詳細を表示

各サービスの接続ステータス履歴とメトリックを表示するには：

1. **サービス接続履歴**セクションのドロップダウンメニューを使用して、期間を選択します。過去24時間を1時間間隔で、または過去24日間を1日間隔で表示できます。
2. Connector データページで、サービスの横にある**詳細の表示**を選択します。

表示されるページには以下が表示されます。

- サービスの経時的なヘルスステータスを示す24個のステータスインジケーター。
  - 緑の点は、その時間間隔中の正常な状態を示します。
  - 赤い点は、その時間間隔中の障害または例外状態を示します。詳細については、点をポイントしてください。
  - レンチアイコンは、その時間間隔中に更新が発生したことを示します。詳細については、レンチアイコンをポイントしてください。
  - 灰色の点は、その時間間隔中にヘルスステータス情報が受信されなかったことを示します。
- 指定された期間中のサービスのメモリとプロセッサの使用状況を示すグラフ。

  コネクタの高度なヘルスチェックサービス詳細ページ(/en-us/citrix-cloud/media/connector-data-detail.png)

コネクタの通知

コネクタは、警告またはエラー状態が発生してから2時間以内に通知を生成します。新しい通知は、Citrix Cloud™ヘッダーのベルのアイコンで確認できます。

4つの通知が表示されているCitrix Cloudヘッダーバー。(/en-us/citrix-cloud/media/notifications.png)

通知を表示するには、このアイコンをクリックするか、コンソールメニューから**通知**を選択します。

詳細については、通知を参照してください。

> **注:**

Cloud Connectorで通知が発行された場合、Cloud Connectorソフトウェアを再インストールする前に根本原因を理解することが重要です。そうしないと、問題が再発する可能性があります。

再インストールが必要な場合は、リソースの場所にある他のCloud Connectorが正常であり、最初のCloud Connectorが削除された後も問題の影響を受けないことを確認することが重要です。そうしないと、サービスが中断される可能性があります。

クラウドコネクタ

次の表に、Cloud Connectorが発行できる通知を一覧表示します。

アラートメッセージ	アラートの種類	詳細	解決策
コネクタ *CONNECTOR_NAME* は、定期的なメンテナンスを実行できなかったため、オフラインで古くなっています。古いコネクタはサービスの可用性に影響を与え、メンテナンスを妨げます。	エラー	コネクタが長時間オフラインになっていて、その後オンラインに戻った場合、最新バージョンに更新できない古いバージョンである可能性があります。古いコネクタはメンテナンスを実行できず、環境内の他のコネクタのメンテナンスプロセスに影響を与える可能性があります。	古いCloud Connectorをアンインストールする前に、新しいCloud Connectorをインストールしてください。
コネクタ *CONNECTOR_NAME* がUTC時刻と同期していません。この状態のコネクタは、サービスの可用性、機能、またはパフォーマンスに影響を与える可能性があります。	エラー		Cloud Connectorの時刻を同期するには

アラートメッセージ	アラートの種類	詳細	解決策
コネクタ *CONNECTOR_NAME* のメンテナンスに失敗しました。このコネクタのメンテナンスの失敗は、環境内の他のコネクタのメンテナンスを妨げます。メンテナンスに失敗したコネクタは、サービスの可用性、機能、またはパフォーマンスに影響を与える可能性があります。	エラー	このコネクタで、コネクタのアップグレードまたはその他のメンテナンス操作が失敗しました。	Cloud Connectorのメンテナンス失敗を解決するには
コネクタ *CONNECTOR_NAME* が *NUMBER* 時間以上オフラインになっています。オフラインのコネクタは、サービスの可用性に影響を与え、メンテナンスを妨げます。	警告	コネクタが一定時間連絡不能な状態が続いた場合、オフラインと見なされます。	オフラインのCloud Connectorをオンライン状態に戻すには
コネクタ *CONNECTOR_NAME* が最近の接続性チェックに失敗しました。接続性チェックの失敗は、サービスの可用性または機能に影響を与える可能性があります。	警告	接続性チェックがエラーコード *HEALTH_CHECK_CODE* で失敗しました。このコネクタは、通知メッセージに記載されている特定のWebまたはIPアドレスに接続できませんでした。	Cloud Connectorの接続性チェックが失敗しました
コネクタ *CONNECTOR_NAME* のCPU使用率が高	警告	このコネクタは、1時間のサンプル期間	Cloud Connectorのリソース可用性ア

アラートメッセージ	アラートの種類	詳細	解決策
くなっています。リソースが制限された状態で動作するコネクタは、サービスの可用性、機能、またはパフォーマンスに影響を与える可能性があります。		でCPU使用率が80%を超えました。	ラートを解決するには
コネクタ *CONNECTOR_NAME* の空きディスク容量が少なくなっています。ディスク容量が制限された状態で動作するコネクタは、サービスのパフォーマンスとメンテナンスに影響を与えます。	警告	このコネクタの空きディスク容量は2GB未満です。	Cloud Connectorのリソース可用性アラートを解決するには
コネクタ *CONNECTOR_NAME* は、重要なプロセスまたはサービスが実行されていないことを検出しました。この状態は、サービスの可用性、機能、またはパフォーマンスに影響を与える可能性があります。	警告		

Citrix Cloud Connector™ のログ収集

CDFログは、Citrix製品内のトラブルシューティング目的で使用されます。Citrixサポートは、アプリケーションおよびデスクトップのブローカリング、ユーザー認証、Virtual Delivery Agent (VDA) の登録に関する問題を特定するためにCDFトレースを使用します。この記事では、お客様の環境で発生する可能性のある問題をトラブルシューティングおよび解決するために使用できるCloud Connectorデータのキャプチャ方法について説明します。

重要な注意事項：

- リソースの場所にあるすべてのCloud Connectorマシンでログ記録を有効にします。
- データの全範囲をキャプチャしていることを確認するために、CitrixはVDAに存在するCDFControlキャプチャツールを使用することをお勧めします。詳細については、Citrixサポート知識センターのCTX111961を参照してください。Citrix Workspaceアプリのログ収集の詳細については、CTX141751を参照してください。
- CitrixにCDFトレースを提出するには、Citrixサポートケースがオープンしている必要があります。Citrixサポート技術者は、既存のサポートケースに添付されていないCDFトレースをレビューできません。

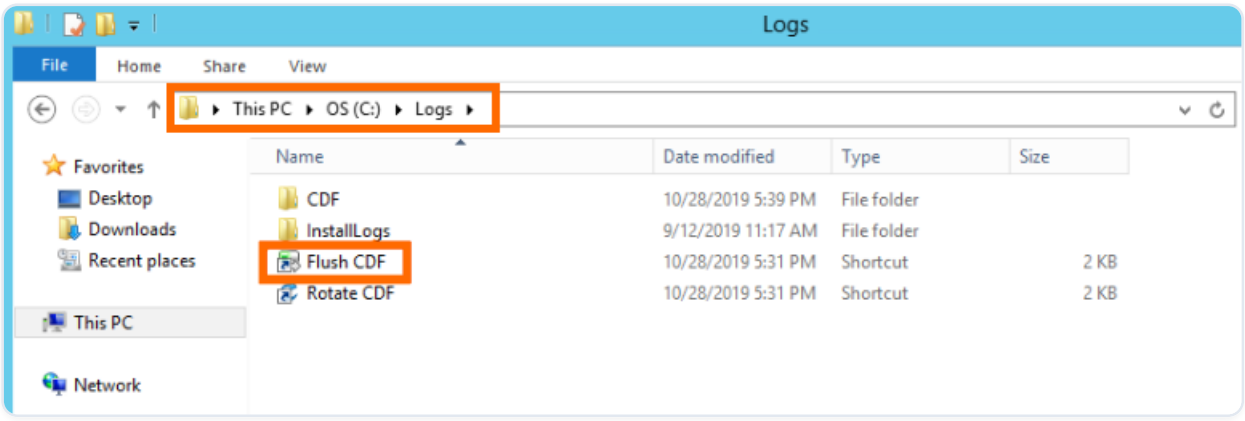
ステップ1：問題を再現する

このステップでは、お客様の環境で発生している問題を再現します。問題がアプリの起動またはブローカリングに関連している場合は、起動の失敗を再現します。問題がVDA登録に関連している場合は、VDAマシンでCitrix Desktop Serviceを手動で再起動して、VDA登録の試行を再現します。

ステップ2：CDFトレースを収集する

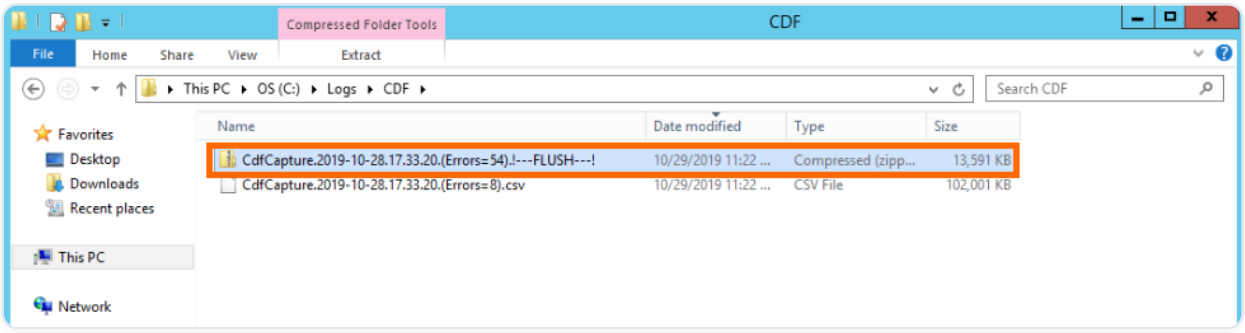
このステップでは、リソースの場所にある各Cloud ConnectorからCDFフラッシュトレースを収集します。

1. ドメイン管理者またはローカル管理者アカウントを使用してRDP接続を開始し、Cloud Connectorマシンにアクセスします。
2. Cloud Connectorマシンで、ファイルエクスプローラーを開き、`C:\logs`に移動します。



3. **Flush CDF**を実行します。Cloud Connectorマシンのタスクバーにアイコンが短時間表示され、その後消えます。

4. ファイルエクスプローラーから、C:\logs\CDFに移動し、**!--FLUSH--!**で終わる最新のフォルダーを特定します。

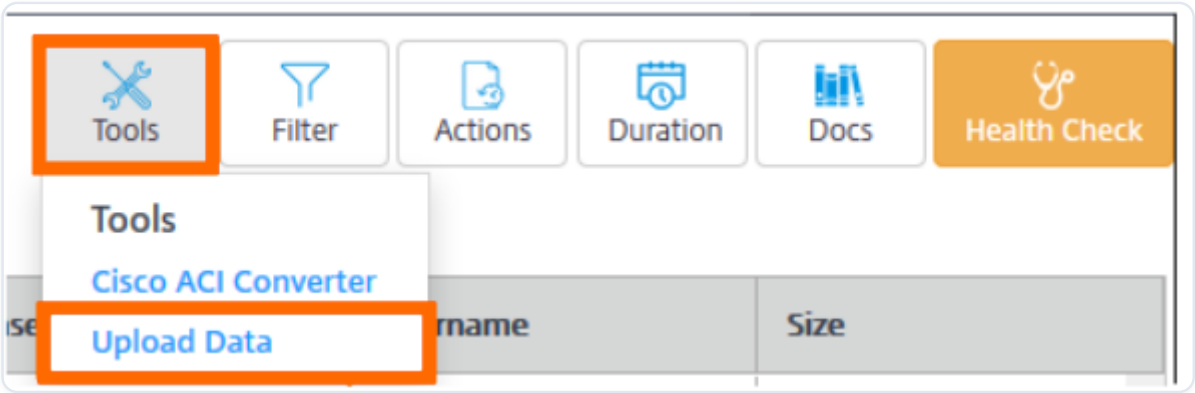


5. リソースの場所にあるすべてのCloud Connectorマシンでステップ1〜5を実行し、すべてのCloud Connectorフラッシュトレースを単一のZIPアーカイブに結合します。すべてのCloud Connectorマシンからのフラッシュトレースの ZIPアーカイブを作成しない場合、それらをCitrixに1つずつ提出する必要があります。

ステップ 3: Citrix にデータを送信する

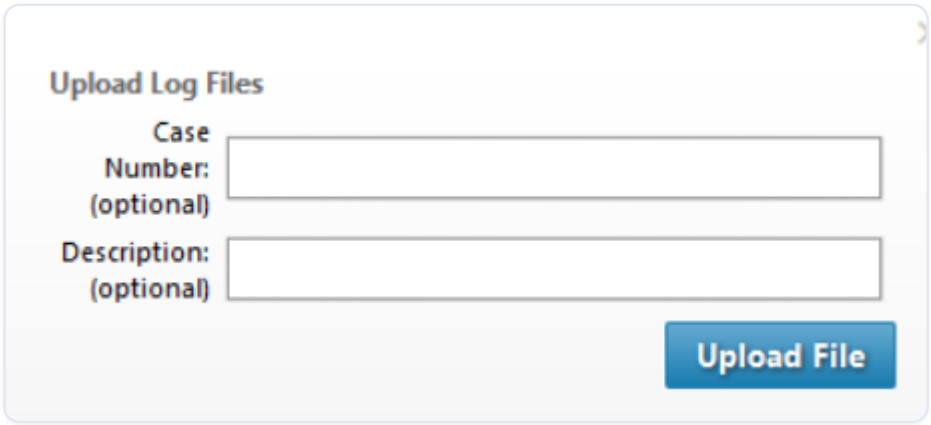
このステップでは、Citrix サポートケースにトレースを添付し、レビューのために提出します。

1. https://cis.citrix.com/ にアクセスし、Citrix.com の資格情報を使用してサインインします。
2. **Diagnostics** を選択します。
3. **Tools** を選択し、次に **Upload Data** を選択します。



4. **Case Number** に、既存のサポートケースの Citrix Support ケース番号を入力します。データアップロードにケース番号が添付されていないと、Citrix Support の技術者は CDF トレースを

適切にレビューできません。



5. **Description** (オプション) に、簡単な説明を入力するか、このフィールドを空白のままにすることができます。
6. **Upload File** を選択し、以前に作成した ZIP アーカイブを選択します。すべての Cloud Connector マシンからフラッシュトレースの ZIP アーカイブを作成しなかった場合は、手順 3～6 を繰り返して、提出する各フラッシュトレースを添付します。

フラッシュトレースを提出すると、Citrix Insight Services がそれらを処理し、指定したサポートケースに添付します。この処理には、ファイルのサイズに応じて最大 24 時間かかる場合があります。

プライマリリソースの場所を選択する

ドメイン内に複数のリソースの場所がある場合、Citrix Cloud の「プライマリ」または「最も優先される」場所として1つを選択できます。プライマリリソースの場所は、Citrix Cloud とドメイン間の最高のパフォーマンスと接続性を提供し、ユーザーが迅速にサインインできるようにします。

プライマリリソースの場所を選択すると、そのリソースの場所にあるCloud Connectorが、可能な限りユーザーログオンおよびプロビジョニング操作に使用されます。プライマリリソースの場所にあるCloud Connectorが利用できない場合、これらの操作はドメイン内の別のCloud Connectorを使用して実行されます。ユーザープリンシパル名（UPN）を使用したログオンにはドメイン名が含まれていない場合があり、プライマリリソースの場所が使用されない場合があります。

> **注：**
>
> どのリソースの場所でもCloud Connectorが常に利用可能であることを確認するために、各リソースの場所に少なくとも2つのCloud Connectorをインストールしてください。

> プライマリリソースの場所として使用するリソースの場所を決定するには、以下を考慮してください。

- そのリソースの場所は、ドメインへの最適な接続性を持っていますか？
- そのリソースの場所は、Citrix Cloud管理コンソールを使用する地理的地域に最も近いですか？たとえば、Citrix Cloudコンソールがhttps://us.cloud.comにある場合、選択するリソースの場所は米国地域に最も近いものになります。

プライマリリソースの場所を選択するには

1. Citrix Cloud管理コンソールから、メニューボタンをクリックし、 を選択します。
2. をクリックし、使用したいリソースの場所を含むドメインを展開します。
3. をクリックし、プライマリとして指定したいリソースの場所を選択します。
4. をクリックします。Citrix Cloudは、選択したリソースの場所の横に「プライマリ」と表示します。

> **注：**
>
> 別のドメインを展開する前に、必ず1つのドメインでの選択内容を保存してください。あるドメインを展開してから別のドメインを展開すると、以前に展開したドメインは折りたたまれ、保存されていない選択内容は破棄されます。

別のプライマリリソースの場所を選択する

1. Citrix Cloud管理コンソールから、メニューボタンをクリックし、 を選択します。
2. をクリックし、変更したいプライマリリソースの場所を含むドメインを展開します。
3. をクリックし、使用したいリソースの場所を選択します。
4. をクリックします。

プライマリリソースの場所をリセットする

プライマリリソースの場所をリセットすると、別のリソースの場所を選択せずに、リソースの場所から「プライマリ」の指定を削除できます。「プライマリ」の指定を削除すると、ドメイン内の任意のCloud Connectorがユーザーログオン操作を処理できるようになります。その結果、一部のユーザーはログオンが遅くなる可能性があります。

1. Citrix Cloud管理コンソールから、メニューボタンをクリックし、 を選択します。

2. を選択し、変更したいプライマリリソースの場所を含むドメインを展開します。
3. を選択し、 を選択します。ログオンパフォーマンスに影響が出る可能性があることを警告する通知が表示されます。
4. を選択し、 をクリックします。

クラウドサービス用Connector Appliance

Connector Applianceは、ハイパーバイザーまたはクラウドプロバイダーでホストされるCitrixコンポーネントです。Citrix Cloud™とリソースの場所間の通信チャネルとして機能し、複雑なネットワークやインフラストラクチャの構成を必要とせずにクラウド管理を可能にします。Connector Applianceを使用すると、ユーザーに価値を提供するリソースを管理し、それらに集中できます。

> **注：**
>
> Connector Applianceは、VDA登録、Storefront XMLトラフィック、Netscaler STAトラフィック、MCSのハイパーバイザー管理、またはDaaSリソースに関連するその他のユースケースには使用できません。これらのユースケースには、Cloud Connectorを使用してください。

コネクタ アプライアンスの機能

- **Active DirectoryをCitrix Cloudに接続する**ことで、AD管理が可能になり、リソースの場所内でADフォレストとドメインを使用できるようになります。これにより、追加のAD信頼を追加する必要がなくなります。Cloud Connectorとは異なり、単一のConnector Applianceを使用して、複数のActive Directoryドメインへの接続を提供できます。詳しくは、「Active Directory with Connector Appliance」を参照してください。
- **Image Portability Service**は、プラットフォーム間でのイメージの管理を簡素化します。この機能は、オンプレミスのリソースの場所とパブリッククラウド内のリソースの場所の間でイメージを管理するのに役立ちます。Citrix Virtual Apps and Desktops™ REST APIを使用して、Citrix Virtual Apps and Desktopsサイト内のリソースの管理を自動化できます。

  Image Portabilityワークフローは、Citrix Cloudを使用してオンプレミスの場所からパブリッククラウドサブスクリプションへのイメージの移行を開始すると開始されます。イメージの準備後、Image Portability Serviceはイメージをパブリッククラウドサブスクリプションに転送し、実行できるように準備するのに役立ちます。最後に、Citrix ProvisioningまたはMachine Creation Services™がパブリッククラウドサブスクリプションにイメージをプロビジョニングします。

詳しくは、「Image Portability Service」を参照してください。

- **Citrix Secure Private Access**を使用すると、管理者はシングルサインオン、リモートアクセス、コンテンツ検査を単一のソリューションに統合し、エンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。詳しくは、「Secure Private Access with Connector Appliance」を参照してください。

Connector Applianceに依存する他のプレビュー中のサービスがある場合があります。

Connector Applianceプラットフォームは、Citrix Cloud PlatformおよびCitrix Identity Platformの一部であり、以下の情報を含むデータを処理できます。

- IPアドレスまたはFQDN
- デバイス、ユーザー、およびリソースの場所の識別子
- タイムスタンプ
- イベントデータ
- Active Directoryからのユーザーとグループの詳細（例: ユーザーとグループの認証および検索に使用されます）

Connector Applianceによって処理される特定の情報の詳細は、Citrix Cloud Services Data Protection Overviewの「*Data Collected by Citrix Cloud Platform*」テーブルで確認できます。

Connector Applianceの可用性と負荷管理

継続的な可用性を確保し、負荷を管理するために、各リソースの場所に複数のConnector Applianceをインストールしてください。Citrixでは、各リソースの場所に少なくとも2つのConnector Applianceを配置することを推奨しています。いずれかのConnector Applianceが一時的に利用できなくなった場合でも、他のConnector Applianceが接続を維持できます。各Connector Applianceはステートレスであるため、利用可能なすべてのConnector Applianceに負荷を分散できます。この負荷分散機能を構成する必要はありません。自動化されています。少なくとも1つのConnector Applianceが利用可能であれば、Citrix Cloudとの通信が失われることはありません。

リソースの場所にコネクタが1つしか構成されていない場合、Citrix Cloudは、**リソースの場所**ページに警告を表示します。

コネクタアプライアンスの更新

Connector Applianceは自動的に更新されます。コネクタを更新するために、お客様が何らかの操作を行う必要はありません。

リソースの場所を構成して、更新が利用可能になり次第すぐに適用するか、またはスケジュールされた時間の後に適用することができます。

更新の構成について詳しくは、コネクタの更新を参照してください。

更新の一環として、Connector Applianceは一時的に利用できなくなります。更新は、テナント内のConnector Applianceに一度に1つずつ適用されます。このため、常に少なくとも1つのConnector Applianceが利用可能であることを保証するために、各リソースの場所に少なくとも2つのConnector Applianceを登録してください。

コネクタアプライアンスの通信

Connector Applianceは、Citrix Cloudとリソースの場所間のすべての通信を認証および暗号化します。インストールされると、Connector Applianceはアウトバウンド接続を介してCitrix Cloudとの通信を開始します。すべての接続は、標準のHTTPSポート（443）とTCPプロトコルを使用して、Connector Applianceからクラウドに確立されます。インバウンド接続は許可されません。

次の表に、Connector Applianceがアクセスする必要があるポートを一覧表示します。

サービス	ポート	サポートされるドメインプロトコル	構成の詳細
DNS	53	TCP/UDP	このポートはローカルセットアップに対して開いている必要があります
NTP	123	UDP	このポートはローカルセットアップに対して開いている必要があります
HTTPS	443	TCP	Connector Applianceはこのポートへのアウトバウンドアクセスを必要とします

Connector Appliance を構成するには、IT 管理者は Connector Appliance のポート 443 (HTTPS) で管理インターフェイスにアクセスできる必要があります。

> **注:**

> 管理インターフェイスにアクセスするには、IP アドレスの先頭に `https://` を含める必要があります。

> Connector Appliance は、リソースの場所にあるオンプレミスシステムと外部システムの両方と通信できます。Connector Appliance の管理インターフェイスで 1 つ以上の Web プロキシを定義した場合、Connector Appliance から外部システムへのトラフィックのみがこの Web プロキシを介してルーティングされます。オンプレミスシステムがプライベートアドレス空間にある場合、Connector Appliance からこのシステムへのトラフィックは Web プロキシを介してルーティングされません。

Connector Appliance は、プライベートアドレス空間を次の IPv4 アドレス範囲として定義します。

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

インターネット接続要件

データセンターからインターネットに接続するには、ポート 443 をアウトバウンド接続用に開く必要があります。ただし、インターネットプロキシサーバーまたはファイアウォールの制限がある環境で動作させるには、さらに構成が必要になる場合があります。

Citrix Cloud サービスを適切に運用および利用するには、次のアドレスに未変更の HTTPS 接続でアクセスできる必要があります。

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.nssvc.net`
    - すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。
        - `https://*.g.nssvc.net`
        - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`

- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

ネットワーク要件

環境が次の構成になっていることを確認してください。

- ネットワークがConnector ApplianceでDHCPを使用してDNSおよびNTPサーバー、IPアドレス、ホスト名、ドメイン名を取得できるようにするか、Connector Applianceコンソールでネットワーク設定を手動で設定できます。
- ネットワークは、Connector Applianceによって内部的に使用されるリンクローカルIP範囲169.254.0.1/24、169.254.64.0/18、または169.254.192.0/18を使用するように構成されていません。
- ハイパーバイザーのクロックが協定世界時 (UTC) に設定され、タイムサーバーと同期されているか、DHCPがNTPサーバー情報をConnector Applianceに提供している必要があります。
- Connector Applianceでプロキシを使用する場合、プロキシは認証なしであるか、基本認証を使用する必要があります。

システム要件

Connector Applianceは、次のハイパーバイザーでサポートされています。

- VMware ESXi バージョン 7 アップデート 2
- VMware ESXi バージョン 8
- ウィンドウズ サーバー 2016、ウィンドウズ サーバー 2019、ウィンドウズ サーバー 2022、または ウィンドウズ サーバー 2025 上の ハイパーV。
- ニュータニックス AHV
- マイクロソフト Azure
- AWS
- グーグル クラウド プラットフォーム
- XenServer® 8.4
- XenServer® 9

ハイパーバイザーは、以下の最小限の機能を提供する必要があります。

- 20 GB ルートディスク
- 2 vCPU
- 4 GB メモリ

- IPv4 ネットワーク

同じハイパーバイザーホスト上に複数のConnector Applianceをホストできます。同じホスト上のConnector Applianceの数は、ハイパーバイザーとハードウェアの制限によってのみ制約されます。

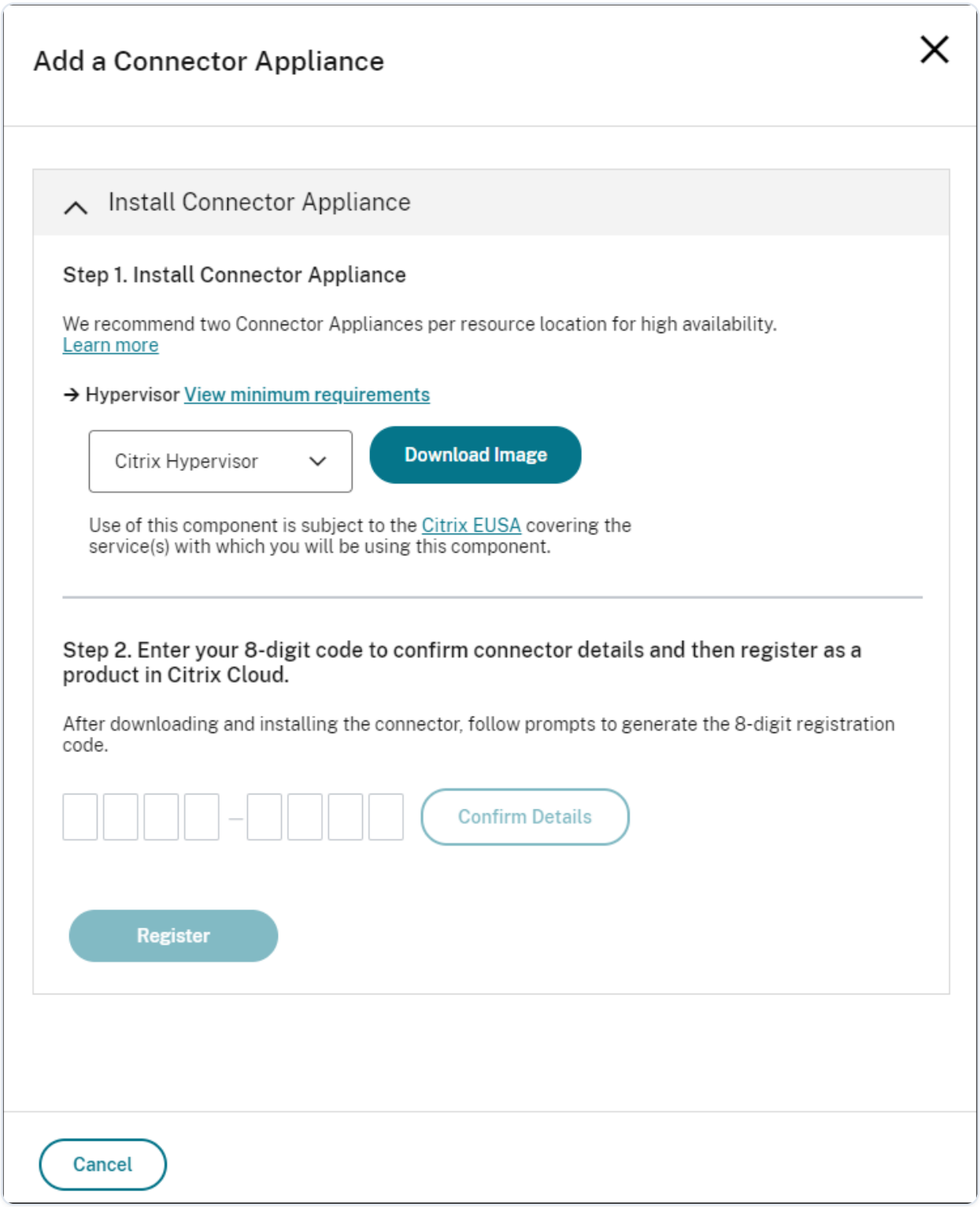
> **注：**
>
> Connector Appliance VM のクローン作成、一時停止、スナップショットの取得はサポートされていません。

コネクタ アプライアンスの入手

Citrix Cloud 内から Connector Appliance ソフトウェアをダウンロードします。

1. Citrix Cloud にサインインします。
2. 画面左上のメニューから、**リソースの場所**を選択します。
3. リソースの場所をまだ持っていない場合は、プラスアイコン (+) をクリックするか、**リソースの場所を追加**を選択します。詳細については、リソースの場所を作成するを参照してください。
4. Connector Appliance を登録するリソースの場所で、**Connector Appliances** のプラスアイコン (+) をクリックします。

   Connector Appliance の追加タスクが開きます。



5. **ステップ 1 のハイパーバイザー**リストから、Connector Appliance をホストするために使用するハイパーバイザーまたはクラウドプロバイダーの種類を選択します。

   - オンプレミスのハイパーバイザーおよびクラウド環境の場合、Citrix Cloud 内で Connector Appliance をダウンロードできます。

     a. **イメージのダウンロード**をクリックします。

b. Citrix エンドユーザーサービス契約を確認し、同意する場合は**同意して続行**を選択します。

c. プロンプトが表示されたら、提供された Connector Appliance ファイルを保存します。

Connector Appliance ファイルのファイル名拡張子は、選択したハイパーバイザーによって異なります。

- 一部のクラウド環境では、マーケットプレイスからConnector Applianceを入手できます:
  - AWS
  - マイクロソフト アジュール
  - グーグル クラウド

6. **Connector Applianceのインストール**タスクを開いたままにします。Connector Applianceのインストール後、登録コードを**手順2**に入力します。

Connectorsページから**Connector Applianceのインストール**タスクにアクセスすることもできます。プラスアイコン（+）を選択してコネクタを追加し、Connector Applianceを追加することを選択します。

ハイパーバイザーにConnector Applianceをインストールする

- XenServer™
- ヴイエムウェア ESXi
- ハイパーV
- ニュータニックス AHV
- マイクロソフト アジュール
- グーグル クラウド プラットフォーム
- AWS

XenServer

このセクションでは、XenCenter を使用して Connector Appliance を XenServer ホストにインポートする方法について説明します。

1. ダウンロードした Connector Appliance XVA ファイルにアクセスできるシステムで、XenCenter を使用して XenServer ホストまたはプールに接続します。
2. ［**ファイル**］ > ［**インポート**］ の順に選択します。

3. Connector Appliance XVA ファイルが保存されているパスを指定または参照します。［**次へ**］をクリックします。
4. Connector Appliance をホストする XenServer ホストを選択します。または、Connector Appliance をホストするプールを選択すると、XenServer が適切な利用可能なサーバーを選択します。［**次へ**］ をクリックします。
5. Connector Appliance に使用するストレージリポジトリを指定します。［**インポート**］ をクリックします。
6. ［**追加**］ をクリックして仮想ネットワークインターフェイスを追加します。［**ネットワーク**］リストから、Connector Appliance が使用するネットワークを選択します。［**次へ**］ をクリックします。
7. Connector Appliance の展開に使用するオプションを確認します。誤りがある場合は、［**戻る**］ を使用してこれらのオプションを変更します。
8. ［**インポートの完了後、新しいVMを自動的に起動する**］ が選択されていることを確認します。［**完了**］ をクリックします。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance の管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。環境で DHCP が利用できない場合は、Connector Appliance 管理コンソールにアクセスする前に、Connector Appliance コンソールでネットワーク構成を設定する必要があります。詳しくは、「Connector Appliance コンソールを使用してネットワーク構成を設定する」を参照してください。

次のステップ: Citrix Cloud に Connector Appliance を登録する。

ヴイエムウェア ESXi

このセクションでは、VMware vSphere Client を使用して VMware ESXi ホストに Connector Appliance を展開する方法について説明します。

1. ダウンロードした Connector Appliance OVA ファイルにアクセスできるシステムで、vSphere Client を使用して ESXi ホストに接続します。
2. **File** > **Deploy OVF Template...** を選択します。
3. Connector Appliance OVAファイルが置かれているパスを指定または参照します。**次へ**をクリックします。
4. テンプレートの詳細を確認します。**次へ**をクリックします。

5. Connector Applianceインスタンスに一意の名前を指定できます。デフォルトでは、名前は**Connector Appliance**に設定されています。このConnector Applianceインスタンスを、このESXiホストでホストされている他のインスタンスと区別できる名前を選択してください。**次へ**をクリックします。
6. Connector Applianceの保存先ストレージを指定します。**次へ**をクリックします。
7. 仮想ディスクを保存する形式を選択します。**次へ**をクリックします。
8. Connector Applianceを展開するために使用するオプションを確認します。誤りがある場合は、**戻る**を使用してこれらのオプションを変更します。
9. **展開後に電源をオンにする**を選択します。**完了**をクリックします。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。環境でDHCPが利用できない場合は、Connector Appliance UIにアクセスする前に、Connector Applianceコンソールでネットワーク構成を設定する必要があります。詳細については、「Connector Applianceコンソールを使用してネットワーク構成を設定する」を参照してください。

次のステップ：Citrix CloudにConnector Applianceを登録する。

ハイパーV

このセクションでは、Hyper-VホストにConnector Applianceを展開する方法について説明します。VMは、Hyper-Vマネージャーを使用するか、付属のPowerShellスクリプトを使用して展開できます。

Hyper-Vマネージャーを使用してConnector Applianceを展開する

1. Hyper-Vホストに接続します。
2. Connector Appliance ZIPファイルをHyper-Vホストにコピーまたはダウンロードします。
3. ZIPファイルの内容を抽出します。ZIPファイルには、PowerShellスクリプトとconnector-appliance.vhdxファイルが含まれています。
4. VHDXファイルをVMディスクを保持したい場所にコピーします。たとえば、`C:\ConnectorApplianceVMs`。
5. Hyper-Vマネージャーを開きます。
6. サーバー名を右クリックし、**新規 > 仮想マシン**を選択します。

7. **新しい仮想マシンウィザード**の**名前と場所の指定**パネルで、Connector Applianceを識別するための一意の名前を入力します。**次へ**をクリックします。
8. **世代の指定**パネルで、**第1世代**を選択します。**次へ**をクリックします。
9. **メモリの割り当て**パネルで、次の設定を構成し、**次へ**をクリックします。
    a. 4 GBのRAMを割り当てます。
    b. 動的メモリを無効にします。
10. **ネットワークの構成**パネルで、リストからスイッチを選択します（例: Default Switch）。**次へ**をクリックします。
11. **仮想ハードディスクの接続**パネルで、**既存の仮想ハードディスクを使用する**を選択します。
12. connector-appliance.vhdxファイルの場所に移動して選択します。**次へ**をクリックします。
13. **概要**パネルで、選択した値を確認し、**完了**をクリックしてVMを作成します。
14. **仮想マシン**パネルで、Connector Appliance VMを右クリックし、**設定**を選択します。
15. 「**設定**」ウィンドウで、「**ハードウェア > プロセッサ**」を選択し、次の操作を実行します。
    a. 「**仮想プロセッサの数**」で、値を「**2**」に変更します。
    b. 「**適用**」をクリックします。
    c. 「**OK**」をクリックします。
16. 「**仮想マシン**」パネルで、Connector Appliance VM を右クリックし、「**開始**」を選択します。
17. Connector Appliance VM を右クリックし、「**接続**」を選択してコンソールを開きます。

Connector Appliance が展開され、正常に起動した後、Hyper-V マネージャーを使用してコンソールに接続します。コンソールには、Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance の管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。環境で DHCP が利用できない場合は、Connector Appliance UI にアクセスする前に、Connector Appliance コンソールでネットワーク構成を設定する必要があります。詳細については、「Connector Appliance コンソールを使用してネットワーク構成を設定する」を参照してください。

次のステップ: 「Citrix Cloud に Connector Appliance を登録する」。

PowerShell スクリプトを使用して Connector Appliance を展開する

connector-appliance.zip ファイルには、新しい VM を作成して起動する PowerShell スクリプトが含まれています。

> 「**注:**」:

> この署名されていない PowerShell スクリプトを実行するには、Hyper-V システムの実行ポリシーを変更する必要がある場合があります。詳細については、`<https://go.microsoft.com/fwlink/?LinkID=135170>` を参照してください。または、提供されているスクリプトを基にして、独自のローカルスクリプトを作成または修正することもできます。

1. Hyper-V ホストに接続します。
2. Connector Appliance ZIP ファイルを Hyper-V ホストにコピーまたはダウンロードします。
3. ZIPファイルの内容を抽出します。PowerShellスクリプトとVHDXファイルです。
4. PowerShellコンソールで、ZIPファイルの内容が置かれているディレクトリにカレントディレクトリを変更し、次のコマンドを実行します。

   ```
   .\connector-appliance-install.ps1
   ```

5. プロンプトが表示されたら、VMの名前を入力するか、**Enter** を選択してデフォルト値の **Connector Appliance** を受け入れます。
6. プロンプトが表示されたら、ルートディスクの保存先を入力するか、Enterキーを押してVHDのシステムデフォルトディレクトリを使用します。
7. プロンプトが表示されたら、ルートディスクのファイル名を入力するか、**Enter** を選択してデフォルト値の connector-appliance.vhdx を受け入れます。
8. プロンプトが表示されたら、使用するスイッチを選択します。**Enter** を選択します。
9. VMインポート情報の概要を確認します。情報が正しい場合は、**Enter** を選択して続行します。スクリプトはConnector Appliance VMを作成して起動します。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用してConnector Applianceに接続し、登録プロセスを完了します。

次のステップ: Citrix CloudにConnector Applianceを登録する。

ニュータニックス AHV

このセクションでは、Nutanix Prism Webコンソールを使用して、`connector-appliance.vhdx` ファイルからNutanix AHVホストにConnector Applianceを展開する方法について説明します。

1. Nutanix Prism Webコンソールのメインメニューで、**Storage** ビューを選択します。
2. **+ Storage Container** をクリックして、Connector Applianceイメージファイルを保持するストレージコンテナを作成します。または、既存のストレージコンテナを使用することもできます。
3. `connector-appliance.vhdx` ファイルをストレージコンテナにアップロードします。
    a. Webコンソールのメインメニューで、**Settings** を選択します。
    b. 「**Image Configuration**」タブを選択し、「**+ Upload Image**」をクリックします。
    c. 「**Create Image**」で、イメージの「**Name**」を指定します。
    d. 「**Image Type**」リストから「**DISK**」を選択します。
    e. 「**Storage Container**」リストから、作成したストレージコンテナを選択します。
    f. 「**Upload a file**」を選択します。
    g. 「**Choose file**」をクリックし、ローカルシステム上の`connector-appliance.vhdx`ファイルに移動します。
    h. 「**Save**」をクリックします。
4. イメージが作成され、「**Image Configuration**」ページでその状態が「**ACTIVE**」と表示されるまで待ちます。
5. 「**Network Configuration**」タブを選択します。
6. 「**+ Create Network**」をクリックして、Connector Applianceが使用するネットワークを作成します。
7. 「**Create Network**」ページで、次の情報を指定します。
    - ネットワーク名。
    - ネットワークVLAN ID。
8. Webコンソールのメインメニューで、「**VM**」ビューを選択します。
9. 「**+ Create VM**」をクリックして、Connector Applianceインスタンスを作成します。
10. **VMの作成**にて、以下の情報を指定します:
    - VM名

- vCPUの数
- メモリ量 (GiB)

11. **Legacy BIOS**を使用するように選択します。
12. **+ 新規ディスクの追加**をクリックして、VMにディスクを追加します。
13. **ディスクの追加**にて、以下の情報を入力します:
    a. **種類**には**DISK**を選択します。
    b. **操作**には**イメージサービスからクローン**を選択します。
    c. **バスの種類**には**SCSI**を選択します。
    d. **イメージ**には、Connector Applianceファイルをアップロードしたときに作成したイメージを選択します。
14. **追加**をクリックして、ディスクの追加を完了します。
15. **VMの作成**で、**+ 新規NICの追加**をクリックします。
16. **NICの作成**で、VMを追加するネットワークを選択します。
17. **ネットワーク接続の状態**には**接続済み**を選択します。
18. 「**追加**」をクリックしてNICの追加を完了します。
19. 「**保存**」をクリックしてVMを作成します。

    デフォルトでは、新しいVMは電源オフになっています。
20. **VM**ビューで、VMを選択し、「**電源オン**」をクリックします。
21. VMが起動するまで待ちます。このプロセスには数分かかる場合があります。

Connector Applianceが展開され、正常に起動した後、Connector ApplianceのIPアドレスは次のいずれかの場所で見つけることができます。

- Nutanix Prism Webコンソールの**VM**ビュー。
- Connector Applianceコンソール。

このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。

次のステップ: Citrix CloudにConnector Applianceを登録する。

マイクロソフト アジュール

このセクションでは、Microsoft AzureにConnector Applianceを展開する方法について説明します。Connector Applianceは、Azure Marketplaceから、またはダウンロードしたディスクイメージから、付属のPowerShellスクリプトを使用して展開できます。

Azure MarketplaceからConnector Applianceを展開する

Azure MarketplaceからConnector Applianceを展開するには、次の手順を完了します。

1. Azure Marketplace のコネクタアプライアンスに移動します。(Azure Marketplace)

   または、マーケットプレイス検索で「Connector Appliance for Cloud Services」を検索することもできます。

2. **今すぐ入手**をクリックし、次に**作成**をクリックします。
3. **Citrix Connector™ Appliance for Cloud Services の作成**ページで、次の情報を入力します。

   - 使用する**サブスクリプション**を選択します。
   - 使用する**リソースグループ**を選択します。
   - Connector Appliance を配置する**リージョン**を選択します。
   - **VM 名**を指定します。
   - Connector Appliance を追加する**仮想ネットワーク**を選択します。このネットワークは、Citrix Cloud、ローカルリソース、およびConnector Appliance管理ページへのアクセスに使用されます。このネットワークは後で変更できません。
   - **サブネット**の値を指定します。

   次へ : タグ > をクリックします。
4. **タグ**タブで、必要に応じて必須タグを追加します。

   次へ : 確認 + 作成 > をクリックします。
5. 展開の詳細を確認したら、**作成**をクリックします。

Connector Appliance が展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用して、Connector Appliance管理ページに接続し、登録プロセスを完了します。

次のステップ: Citrix Cloud に Connector Appliance を登録する。

PowerShellスクリプトを使用してConnector Appliance VMを展開する

`connector-appliance-azure.zip`ファイルには、新しいVMを作成して起動するPowerShellスクリプトが含まれています。提供されたスクリプトを基にして、独自のローカルスクリプトを作成または修正できます。

スクリプトを実行する前に、以下の前提条件を満たしていることを確認してください。

- Az PowerShellモジュールをローカルの PowerShell環境にインストールします。
- VHDファイルが置かれているディレクトリでPowerShellスクリプトを実行します。

次の手順を完了します。

1. Connector ApplianceのZIPファイルをWindowsシステムにコピーまたはダウンロードします。
2. ZIPファイルの内容（PowerShellスクリプトとVHDファイル）を抽出します。
3. 管理者としてPowerShellコンソールを開きます。
4. 現在のディレクトリをZIPファイルの内容が置かれている場所に移動し、次のコマンドを実行します。

   ```
   .\connector-appliance-upload-Azure.ps1
   ```

5. Microsoft Azureへのログインを促すダイアログが表示されます。資格情報を入力します。
6. PowerShellスクリプトによってプロンプトが表示されたら、使用するサブスクリプションを選択します。Enterキーを押します。
7. スクリプトのプロンプトに従って、イメージのアップロードと仮想マシンの作成を行います。
8. 最初のVMを作成した後、スクリプトはアップロードされたイメージから別のVMを作成するかどうかを尋ねます。
   - 別のVMを作成するには、`y`と入力します。
   - スクリプトを終了するには、`n` と入力します。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance の管理ページに接続し、登録プロセスを完了します。

次のステップ: Citrix Cloud に Connector Appliance を登録する。

AWS

このセクションでは、AWS に Connector Appliance を展開する方法について説明します。Connector Appliance は AWS Marketplace で AMI として利用可能であり、AMI から Connector Appliance をインストールすることをお勧めします。または、AWS UI を使用するか、付属の PowerShell スクリプトを使用して、ダウンロードしたディスクイメージを展開することもできます。

ネットワークの前提条件

AWS に Connector Appliance を展開するには、Connector Appliance が作成されるサブネットから Citrix Cloud にアクセスできることを確認してください。

アプライアンスにはプライベート IP アドレスを使用することをお勧めします。これには、Citrix Cloud へのアクセスを提供するための特定の構成が必要です。この構成を実現するには、**AWSManagement Console** で次の手順を完了します。

1. NAT ゲートウェイを作成します。
    a. 上部のナビゲーションバーで、**Services > VPC > NAT Gateways** を選択します。
    b. 右上隅で、**Create NAT Gateway** をクリックします。次の情報を入力します。
        - **Name** を入力します。
        - リストから **subnet** を選択します。
        - **Connectivity type** を **Public** に設定します。
        - リストから **Elastic IP allocation ID** を選択します。利用可能な Elastic IP がない場合は、**Allocate Elastic IP** をクリックし、指示に従って作成します。
    c. 「**NAT Gateway の作成**」をクリックします。
2. NAT ゲートウェイを含むルートテーブルエントリを作成します。
    a. 上部のナビゲーションバーで、**Services > VPC > Route Tables** を選択します。
    b. 右上隅で、**ルートテーブルの作成** をクリックします。次の情報を入力します。
        - **名前** を入力します。
        - リストから、NAT ゲートウェイの作成時に選択したサブネットを含む VPC を選択します。
    c. **ルートテーブルの作成** をクリックします。

d. 作成したルートテーブルの **ルート** タブで、**ルートの編集 > ルートの追加** をクリックします。

e. 新しいルートエントリの **送信先** と **ターゲット** を入力します。

- 送信先を 0.0.0.0/0 に設定します。
- ターゲットには、リストから作成した **NAT Gateway** を選択します。

f. **変更を保存** をクリックします。

3. Connector Appliance に使用するサブネットをこのルートテーブルにアタッチします。

a. 上部のナビゲーションバーで、**Services > VPC > Route Tables** を選択します。

b. NAT ゲートウェイを含むルートテーブルを選択します。

c. 表示ページで、**サブネット関連付け**タブに移動します。

d. **サブネット関連付けの編集**をクリックします。

e. ルートテーブルにアタッチするサブネットを選択します。

f. **関連付けの保存**をクリックします。

AWS Marketplace から Connector Appliance を展開する

開始する前に、次の前提条件を満たしていることを確認してください。

- EC2 リソースを操作する権限があること。
- ネットワークの前提条件 の構成が完了していること。
- (オプション) Connector Appliance へのアクセスを許可する IP アドレスを制限するセキュリティグループを作成できます。

次の手順を実行します。

1. **AWS Management Console** にログインします。
2. AWS Marketplace で Connector Appliance AMI を見つけます。これには、次のいずれかの方法を使用できます。

- Citrix Cloud で提供されているマーケットプレイスのリンクをたどります。(AWS Marketplace)
- AWS Management Console で AMI を検索します。

a. **サービス > コンピューティング > EC2 > AMI** に移動します。

b. US East (オハイオ) リージョンにいることを確認してください。

c. **パブリックイメージ**で、「Citrix Connector Appliance」またはAMI ID「ami-026eaf9b3b232577f」を検索します。

3. AMI ID (ami-026eaf9b3b232577f) と所有者ID (414337923189) を確認して、正しいAMIであることを検証します。
4. AMIをサブスクリプションにコピーします。

   a. **アクション > AMIのコピー**に移動します。
   b. **AMIのコピー**ダイアログで、必要な**送信先リージョン**を選択できます。
   c. **AMIのコピー**をクリックします。

5. コピーしたAMIの概要ページから、**AMIからインスタンスを起動**をクリックします。
6. **インスタンスの起動**ダイアログで、次の手順を完了します。

   a. 作成するインスタンスの数を選択します。回復性のため、各リソースの場所に2つ以上のConnector Applianceを配置することをお勧めします。
   b. インスタンスの名前を指定します。
   c. **インスタンスタイプ**には、**t2.medium**を選択します。インスタンスタイプは、少なくとも4 GBのメモリと2つのCPUを備えている必要があります。
   d. **キーペア (ログイン)**には、**キーペアなしで続行**を選択します。Connector ApplianceへのSSHログインは許可されていないため、キーペアは不要です。
   e. **ネットワーク設定**の**ファイアウォール (セキュリティグループ)**セクションで、次の設定を構成します。

      i. **セキュリティグループの作成**または**既存のセキュリティグループの選択**のいずれかを選択します。
      ii. 「**インターネットからのSSHトラフィックを許可**」の選択を解除します。
      iii. 「**インターネットからのHTTPSトラフィックを許可**」を選択します。
      iv. 「**インターネットからのHTTPトラフィックを許可**」を選択します。

   「**インスタンスの起動**」をクリックします。

7. インスタンスが作成されたら、「**成功**」セクションでインスタンスIDリンクをクリックし、Connector Applianceインスタンスを表示します。

   または、このページの「**すべてのインスタンスを表示**」ボタンをクリックするか、AWS Management Consoleで「**サービス > EC2 > インスタンス**」に移動して、インスタンスのリストを表示することもできます。

8. 「**インスタンスの状態**」が「**実行中**」に変わったら、インスタンスの詳細に入り、「**プライベートIPv4アドレス**」を使用してConnector Appliance管理ページに接続し、登録プロセスを完了します。

ブラウザから内部IPアドレスでConnector Appliance管理ページにアクセスし、登録プロセスを完了するために、踏み台ホストを使用する必要がある場合があります。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。このネットワーク構成は、Connector ApplianceのWebインターフェイスを使用して編集できます。詳細については、「Connector Appliance管理ページでのネットワーク設定の構成」を参照してください。

次のステップ: Citrix CloudへのConnector Applianceの登録。

AWS UIを使用してConnector Applianceを展開する

開始する前に、次の前提条件を満たしていることを確認してください。

- S3およびEC2リソースを操作する権限があること。
- VMインポートアクセス権を持つサービスロールとポリシーを作成していること。詳細については、`<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`を参照してください。

  > **注:**
  >
  > サービスロールを作成するには、S3バケットを作成する必要があります。ポリシーを作成する際、作成したS3バケットにVMインポートアクセスを設定します。

- AWS CloudShellにアクセスできます。これは特定のリージョンでのみ利用可能です。AWS CloudShellがサポートされているリージョンのリストについては、`<https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html>`を参照してください。
- ネットワークの前提条件で構成を完了しています。

次の手順を完了します。

1. ローカルシステムで、`connector-appliance-aws.zip`の内容を抽出します。
2. **AWS Management Console**にログインします。

3. 次の手順を完了してストレージバケットを作成します。（または、これらの手順をスキップして既存のストレージバケットを使用することもできます。）

   a. 上部のナビゲーションバーで、**Services** > **S3** > **Create bucket**を選択します。

   b. バケットの一意の名前を入力します。Amazon S3のバケットの命名規則については、`<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html>`を参照してください。

   c. バケットのリージョンを選択します。AWSリージョンと同じリージョンを選択していることを確認してください。これらのリージョンが異なる場合、バケット内のファイルを使用できないためです。

   d. 残りの設定はデフォルトのままにして、**Create bucket**をクリックします。

4. 作成したバケットの名前をクリックします。**Upload** > **Add files**をクリックし、`connector-appliance.vhd`ファイルを選択します。残りの設定はデフォルトのままにして、**Upload**をクリックします。

5. アップロードしたファイルをクリックします。**Copy S3 URI**をクリックします。

6. 上部のナビゲーションバーにある**AWS CloudShellアイコン**をクリックし、次のコマンドを実行します。

   a. VHDファイルをスナップショットに変換するタスクを作成します。

   ```
   aws ec2 import-snapshot --disk-container
   Format=VHD,Url="&lt;S3_URI>"
   ```

   プレースホルダーの値を、前の手順でコピーしたS3 URIに置き換えます。例: `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`。

   次のコマンドが`"Status": "completed"`を含むJSON文字列を返すと、このコマンドは完了です。JSON出力の`ImportTaskId`の値をメモしておきます。

   b. 次のコマンドを実行します。

   ```
   aws ec2 describe-import-snapshot-tasks --import-task-ids
   &lt;ImportTaskId>
   ```

プレースホルダーの値を、前の手順でコピーした`ImportTaskId`に置き換えます。例: `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`。

7. **AWS Management Console** の上部のナビゲーションバーで、**Services** > **EC2** を選択します。
8. 画面左側のメニューから、**Snapshots** をクリックします。
9. 作成したスナップショットを右クリックし、**Create Image** をクリックします。
10. 開いたペインで、次の手順を実行します。

    a. AMIの名前を入力します。

    b. **Hardware-assisted virtualization** を選択します。

    Create をクリックします。
11. 画面左側のメニューから、**AMIs** をクリックします。
12. 作成したAMIを右クリックし、**Launch** をクリックします。
13. 開いたペインで、次の手順を実行します。

    a. インスタンスタイプを選択します。

    b. (オプション) **インスタンスの設定**タブでネットワークをカスタマイズします。

    c. (オプション) **ストレージの追加**タブで別のボリュームをアタッチします。

    d. **セキュリティグループの設定**タブでセキュリティグループのルールを設定します。

    インスタンスの起動を確認したら、**確認と起動**をクリックします。

Connector Applianceが展開され、正常に起動したら、**サービス** > **EC2** > **インスタンス**に移動し、作成したインスタンスを選択します。**プライベートIPv4アドレス**を使用してConnector Appliance管理ページに接続し、登録プロセスを完了します。インストールプロセスを続行するには、ブラウザから内部IPアドレスでConnector Appliance管理ページにアクセスするために、踏み台ホストを使用する必要がある場合があります。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。このネットワーク構成は、Connector ApplianceのWebインターフェイスを使用して編集できます。詳細については、「Connector Appliance管理ページでのネットワーク設定の構成」を参照してください。

次のステップ: Citrix CloudにConnector Applianceを登録する。

PowerShellスクリプトを使用してConnector Applianceを展開する

`connector-appliance-aws.zip`ファイルには、新しいVMを作成して起動するPowerShellスクリプトが含まれています。スクリプトを実行する前に、次の前提条件を満たしていることを確認してください。

- システムにAWS.Tools、AWSPowerShell.NetCore、またはAWSPowerShellのいずれかがインストールされていること。詳細については、`<https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html>`を参照してください。
- VMインポートアクセス権を持つサービスロールとポリシーを作成していること。このPowerShellスクリプトが機能するには、サービスロールとポリシーの両方に`vmimport`という名前を付ける必要があります。詳細については、`<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`を参照してください。

  > **注：**
  >
  > サービスロールを作成するには、S3バケットを作成する必要があります。ポリシーを作成する際は、作成したS3バケットにVMインポートアクセスを設定してください。

- Amazon EC2セキュリティグループを作成していること。
- S3のアクセス許可とAPIアクセス権があること。
- (#networking-prerequisites)の構成は完了しています。

次の手順を完了します。

1. ローカルシステムで、`connector-appliance-aws.zip`の内容をフォルダーに抽出します。
2. PowerShellで、次のコマンドを実行します。

   a. ローカル環境でAWSコマンドレットを実行できるようにするには、AWS SDKストアに新しいプロファイルを追加するために、次のコマンドを実行します。

   ```
   Set-AWSCredential -AccessKey &lt;access_key_ID> -SecretKey
   &lt;secret_key> -StoreAs MyProfile
   ```

   プレースホルダーの値をアクセスキーとシークレットキーに置き換えます。一意のプロファイル名を指定します。提供されている例では、`MyProfile`です。

   b. プロファイルをデフォルトに設定します。

```
Initialize-AWSDefaultConfiguration -ProfileName MyProfile
```

c. 現在のディレクトリを抽出されたファイルが保存されているフォルダーに変更し、次のコマンドを実行します。

```
.\connector-appliance-upload-aws.ps1
```

3. スクリプトのプロンプトに従って、Connector Applianceの展開リージョンの選択、選択したバケットへのイメージのアップロード、およびVMの名前の入力を行います。

   - 以前に作成した、VMインポートアクセス権を持つバケットを使用する必要があります。
   - 使用するVPCを選択するよう求められたら、NATゲートウェイとルートテーブルが構成されているVPCを選択します。
   - 使用するサブネットを選択するよう求められたら、NATゲートウェイを含むルートテーブルにアタッチされているサブネットを選択します。

   詳細については、(#networking-prerequisites)を参照してください。

Connector Applianceが展開され、正常に起動すると、スクリプトはConnector ApplianceのプライベートIPアドレスを表示します。ブラウザから内部IPアドレスでConnector Appliance管理ページにアクセスし、登録プロセスを完了するために、踏み台ホストを使用する必要がある場合があります。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。このネットワーク構成は、Connector ApplianceのWebインターフェイスを使用して編集できます。詳細については、(#configuring-network-settings-on-the-connector-appliance-administration-page)を参照してください。

次のステップ: Connector ApplianceをCitrix Cloudに登録する(#register-your-connector-appliance-with-citrix-cloud)。

グーグル クラウド プラットフォーム

このセクションでは、Google Cloud PlatformにConnector Applianceを展開する方法について説明します。Connector ApplianceはGoogle Cloud Marketplaceからインストールできます。または、ダウンロードしたディスクイメージをGoogle Cloud Platform Consoleを使用するか、付属のPowerShellスクリプトを使用して展開することもできます。

ファイル`connector-appliance-gcp.zip`には以下が含まれます。

- `connector-appliance.tar.gz`は、Connector Applianceのディスクイメージです
- `connector-appliance-upload-gcp.ps1`は、Connector Applianceを自動的に展開するために使用できるPowerShellスクリプトです

Google Cloud Marketplace からコネクタアプライアンスを展開する

1. Googleアカウントにログインします。
2. Citrix Cloudで提供されているMarketplaceリンクに従います。（Google Cloud Marketplace）

   または、Marketplace検索で「Connector Appliance for Cloud Services」を検索できます。
3. **起動**をクリックします。
4. **New Citrix Connector Appliance for Cloud Services deployment**ページで、次の情報を入力します。

   - デプロイジョブの**デプロイ名**を指定します。
   - Connector Applianceを配置する**ゾーン**を選択します。
   - 使用する**マシンファミリー**、**シリーズ**、および**マシンタイプ**を選択します。
   - 使用する**ブートディスクの種類**と**ブートディスクのサイズ（GB）**を選択します。
   - **ネットワーク**セクションで、Connector Applianceが使用するネットワークインターフェイスを指定します。パブリックネットワークから管理ページに接続できるようにする場合は、**外部IP**を指定します。

   展開をクリックします。**Deployment Manager**ページに移動します。

   > **注：**
   >
   > Connector Applianceが展開され、正常に起動すると、Connector ApplianceがGoogle Cloud Platformに展開されたことを確認するメールが届きます。

5. **Deployment Manager**ページで、インスタンス名をクリックします。または、**Compute Engine**で作成したConnector Applianceインスタンスを検索することもできます。
6. Connector Applianceのネットワークインターフェイスを設定する際に以前に**外部IP**を指定した場合は、**詳細**タブの**ネットワークインターフェイス**セクションにある**外部IPアドレス**をコピーします。このIPアドレスを使用してConnector Applianceの管理ページに接続し、登録プロセスを完了します。または、Connector Applianceと同じサブネットにある別のマシンから**プライマリ内部IPアドレス**を使用してConnector Applianceの管理ページにアクセスすることもできます。

次のステップ：Citrix CloudにConnector Applianceを登録する。

Google Cloud Platformコンソールを使用してConnector Applianceを展開する

1. ローカルシステムで、`connector-appliance-gcp.zip`の内容を抽出します。
2. Google Cloud Platformプロジェクトで、ストレージバケットを作成します。（または、既存のストレージバケットを使用することもできます。）」
   a. メインメニューから、**Cloud Storage**を選択します。
   b. メインペインで、**バケットを作成**を選択します。
   c. バケットの名前を指定します。
   d. 必要なデータストレージとアクセス設定を構成します。これらの設定はデフォルトのままにしておくことができます。
   e. 「**作成**」をクリックします。
3. ストレージバケット内で、「**ファイルをアップロード**」を選択し、ファイル`connector-appliance.tar.gz`を選択します。ファイルがアップロードされるまでお待ちください。
4. アップロードされたファイルを選択して詳細を表示します。「**gsutil URI**」の値をクリップボードにコピーします。
5. ヘッダーバーの「**Cloud Shell をアクティブにする**」アイコンをクリックして、Cloud Shell を開きます。
6. Cloud Shell で、次のコマンドを実行してイメージを作成します。

```
gcloud compute images create "Image name" --guest-os-
features=MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded
connector-appliance.tar.gz file"
```

7. メインメニューから、「**Compute Engine**」>「**VM インスタンス**」を選択します。
8. 「**インスタンスを作成**」を選択します。開いたペインで、次の情報を指定します。
   a. 「**名前**」フィールドに、Connector Appliance インスタンスの名前を指定します。
   b. Connector Appliance を配置するリージョンを選択します。
   c. マシン構成を選択します。
   d. 「**ブートディスク**」セクションで、「**変更**」をクリックします。
   e. 開いたセクションで、「**カスタムイメージ**」タブに移動します。
   f. 「**イメージ**」リストから、作成したイメージを選択します。

g. 「**選択**」をクリックします。

h. 「**ファイアウォール**」セクションで、HTTPS トラフィックを有効にして、Connector Appliance 管理ページへのアクセスを許可します。

i. 必要な追加設定を指定します。たとえば、デフォルトのネットワーク構成を使用しない場合があります。

作成をクリックします。

9. **VMインスタンス**セクションで、新しく作成したVMを選択して詳細を表示します。

Connector Applianceが展開され、正常に起動すると、**VMインスタンス**セクションにConnector ApplianceのIPアドレスが表示されます。

Connector Applianceに外部IPアドレスがある場合、このIPアドレスを使用してブラウザからConnector Appliance管理ページにアクセスし、登録プロセスを完了できます。

Connector Applianceに内部IPアドレスしかない場合は、踏み台ホストを使用してブラウザからConnector Appliance管理ページにアクセスし、登録プロセスを完了します。詳細については、`<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`を参照してください。

次のステップ: Citrix CloudにConnector Applianceを登録する。

PowerShellスクリプトを使用してConnector Applianceを展開する

提供されているPowerShellスクリプトを使用してConnector Applianceを展開するには、システムにGoogle Cloud SDKがインストールされている必要があります。

1. ローカルシステムで、`connector-appliance-gcp.zip`の内容をフォルダに抽出します。
2. PowerShellで、抽出されたファイルが保存されているフォルダにディレクトリを変更します。
3. コマンド`.\connector-appliance-upload-GCP.ps1`を実行します。
4. 開いたブラウザウィンドウで、Connector Applianceを展開するプロジェクトへのアクセス権を持つアカウントでGoogle Cloud SDKに認証します。
5. Google Cloud Tools for PowerShellで、PowerShellスクリプトによってプロンプトが表示されたら、使用するプロジェクトを選択します。Enterキーを押します。
6. スクリプトのプロンプトに従って、ディスクのアップロード、イメージの作成、仮想マシンの作成を行います。
7. 最初のVMを作成した後、スクリプトはアップロードされたイメージから別のVMを作成するかどうかを尋ねます。

- 別のVMを作成するには、`y`と入力します。
- スクリプトを終了するには、`n`と入力します。

Connector Applianceが展開され、正常に起動した後、スクリプトはConnector Applianceの内部IPアドレスを表示します。または、Google Cloud Platformコンソールにアクセスして、Connector Applianceの内部IPアドレスを見つけることもできます。**Compute Engine** > **VM Instances**セクションに、Connector ApplianceのIPアドレスが表示されます。

バスティオンホストを使用して、ブラウザから内部IPアドレスにあるConnector Appliance管理ページにアクセスし、登録プロセスを完了します。詳細については、`<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`を参照してください。

次のステップ: Citrix CloudにConnector Applianceを登録する。

Citrix CloudにConnector Applianceを登録する

Citrix Cloudとリソースの場所間の通信チャネルを提供するために、Citrix CloudにConnector Applianceを登録します。

ハイパーバイザーにConnector Applianceをインストールして起動すると、コンソールにConnector ApplianceのIPアドレスが表示されます。コンソールには、Connector Appliance UIへの接続を検証するために使用できるSSLフィンガープリントも表示されます。



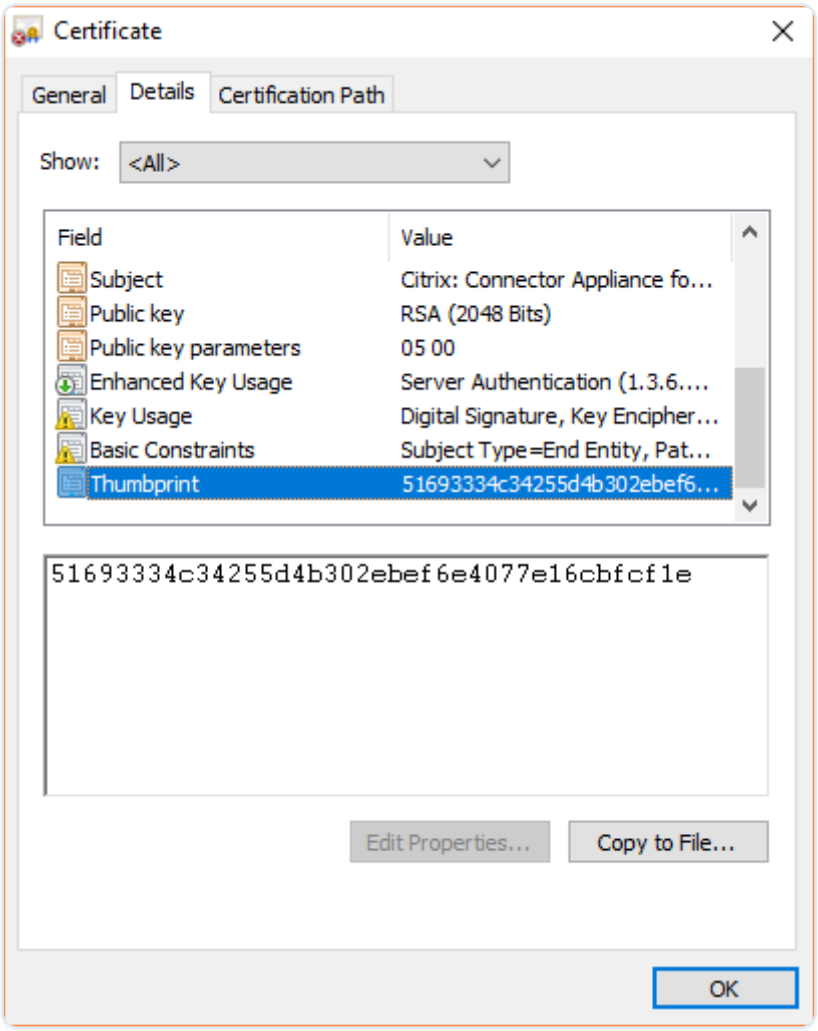
1. Connector ApplianceのIPアドレスをブラウザのアドレスバーにコピーします。

> **注:**
>
> IPアドレスの先頭に`https://`を含める必要がある場合があります。
>
> Connector Appliance UIは、5年間有効な自己署名証明書を使用します。そのため、接続が安全でないというメッセージが表示される場合があります。Connector Applianceへの接続を検証するには、コンソールに表示されるSSLフィンガープリントと、ブラウザがウェブページから受信するフィンガープリントを比較できます。

たとえば、Google Chromeブラウザで、次の手順を完了します。

a. アドレスバーの横にある**安全ではありません**マーカーをクリックします。
b. **証明書**を選択します。**証明書**ウィンドウが開きます。
c. **詳細**タブに移動し、**サムプリント**フィールドを見つけます。

   サムプリントフィールドの値と、コンソールで提供されているSSLフィンガープリントが一致する場合、ブラウザがConnector Appliance UIに直接接続していることを確認できます。

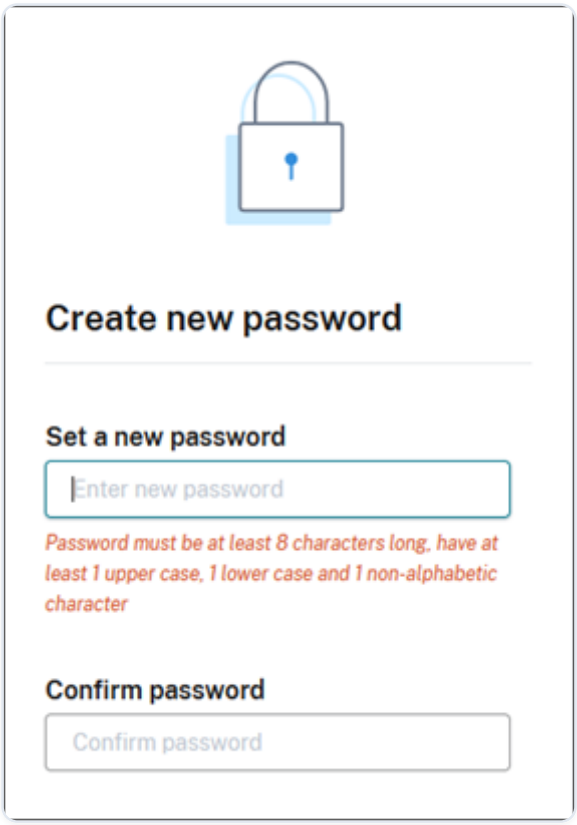


この自己署名証明書は、組織によって署名されたもの、または組織の信頼チェーンを使用して生成された独自の証明書に置き換えることができます。詳細については、「証明書の管理」を参照してください。

2. ブラウザがサイトへの続行を確認するために追加の手順を要求する場合は、今すぐその手順を完了してください。

   新しいパスワードの作成Webページが開きます。

3. Connector Appliance UIのパスワードを作成し、**パスワードを設定**をクリックします。



設定するパスワードは、次の要件を満たす必要があります。

- 8文字以上
- 大文字と小文字の両方を含む
- 少なくとも1つの英数字以外の文字を含む

このパスワードは、将来使用するために安全な場所に保管してください。

4. 設定したパスワードでサインインします。**コネクタ管理**ページが開きます。

   プロキシサーバーセクションのあるコネクタ管理ページ(/en-us/citrix-cloud/media/connector-appliance-register.png)

5. (オプション) 1つ以上のWebプロキシを使用している場合は、**プロキシサーバー**セクションでプロキシアドレスを追加できます。認証なしプロキシと認証済みプロキシの両方がサポートされています。認証なしプロキシを追加するには、有効な**プロキシIPアドレスとポート**を指定します。認証済みプロキシを追加するには、有効な**ユーザー名**と**パスワード**も指定します。

> **注：**
>
> 基本プロキシ認証のみがサポートされています。他の認証形式はサポートされていません。

> 外部システムへのトラフィックのみがWebプロキシを介してルーティングされます。詳細については、Connector Appliance communicationを参照してください。

6. (オプション) ネットワークがTLS傍受型Webプロキシを使用してインターネットにアクセスする場合、クラウドと正常に通信するために、コネクタがそのルート証明機関を信頼する必要がある場合があります。

   a. **ルート証明機関**の下で、**証明書の追加**を選択します。

   b. PEM形式で証明書の内容をコピーします。

   ```
   -----BEGIN CERTIFICATE-----

   <certificate-base64-bytes>

   -----END CERTIFICATE-----
   ```

   c. **完全な証明書の詳細**に、証明書の内容を貼り付けます。

   d. **証明書の追加**を選択します。

   Connector Appliance APIを使用してRootCAを追加するには、Citrix Developerドキュメントのルート証明機関の管理を参照してください。

> **注：**
>
> 有効期限が切れている、または今後30日以内に有効期限が切れる証明書には警告が表示されます。

7. **コネクタの登録**をクリックして、登録タスクを開きます。

8. Connector Applianceの名前を選択します。この名前は、リソースロケーションに存在するさまざまなConnector Applianceを区別するのに役立ちます。Connector Applianceを登録した後、名前は変更できません。

   Connector Appliance名フィールドに名前を入力し、**次へ**をクリックします。

   Connector Applianceに名前を付けます。(/en-us/citrix-cloud/media/connector-appliance-rename.png)

   ウェブページには、Citrix Cloudに登録するために使用するコードが表示されます。このコードは15分で期限切れになります。

Citrix Cloudに接続するために使用する生成されたコード(/en-us/citrix-cloud/media/connector-appliance-code.png)

9. **コピー**ボタンを使用して、コードをクリップボードにコピーします。
10. **リソースロケーション**ウェブページに戻ります。
11. **Connector Applianceのインストール**タスクの**ステップ2**にコードを貼り付けます。**詳細の確認**をクリックします。

    Citrix Cloudは、Connector Applianceが存在し、連絡可能であることを確認します。登録コードの有効期限が切れている場合は、新しいコードを生成するように求められます。

    ステップ2では、コネクタが登録準備完了であることを示します。(/en-us/citrix-cloud/media/connector-appliance-step-2.png)
12. **登録**をクリックします。

    ページには、登録が成功したかどうかが表示されます。登録に失敗した場合は、再試行するように求められます。
13. **閉じる**をクリックします。

Connector Appliance管理ページでは、Connector Applianceの診断レポートをダウンロードすることもできます。詳細については、「診断レポートの生成」を参照してください。

Connector Applianceの登録後

各リソースの場所について、2つ以上のConnector Applianceをインストールして登録することをお勧めします。この構成により、継続的な可用性が確保され、コネクタが負荷を分散できるようになります。

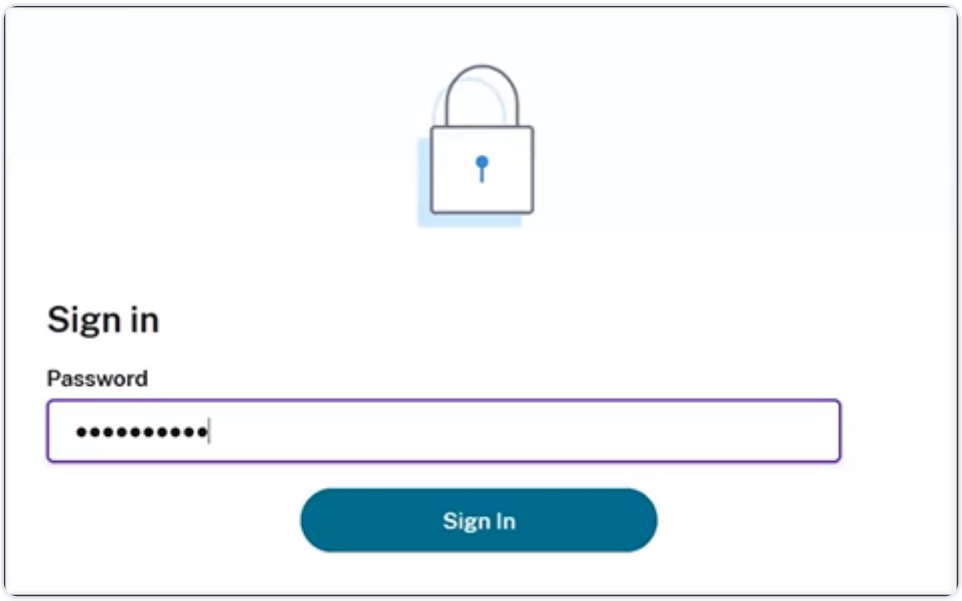
Connector Applianceを直接管理することはできません。

Connector Applianceは自動的に更新されます。コネクタを更新するために、お客様が何らかの操作を行う必要はありません。Connector Applianceの更新をリソースの場所に適用する日時を指定できます。詳細については、「コネクタの更新」を参照してください。

Connector Appliance VMのクローン作成、一時停止、またはスナップショットの取得は行わないでください。これらの操作はサポートされていません。

Connector Appliance UIに初めて接続するときにのみ、**新しいパスワードの作成**ページが表示されます。将来使用するために、このパスワードを安全な場所に保管してください。このパスワードはリセットできません。パスワードを忘れた場合は、Connector Applianceを再インストールする必

要があります。UIへのその後の接続では、Connector Applianceの登録時に設定したパスワードの入力を求められます。



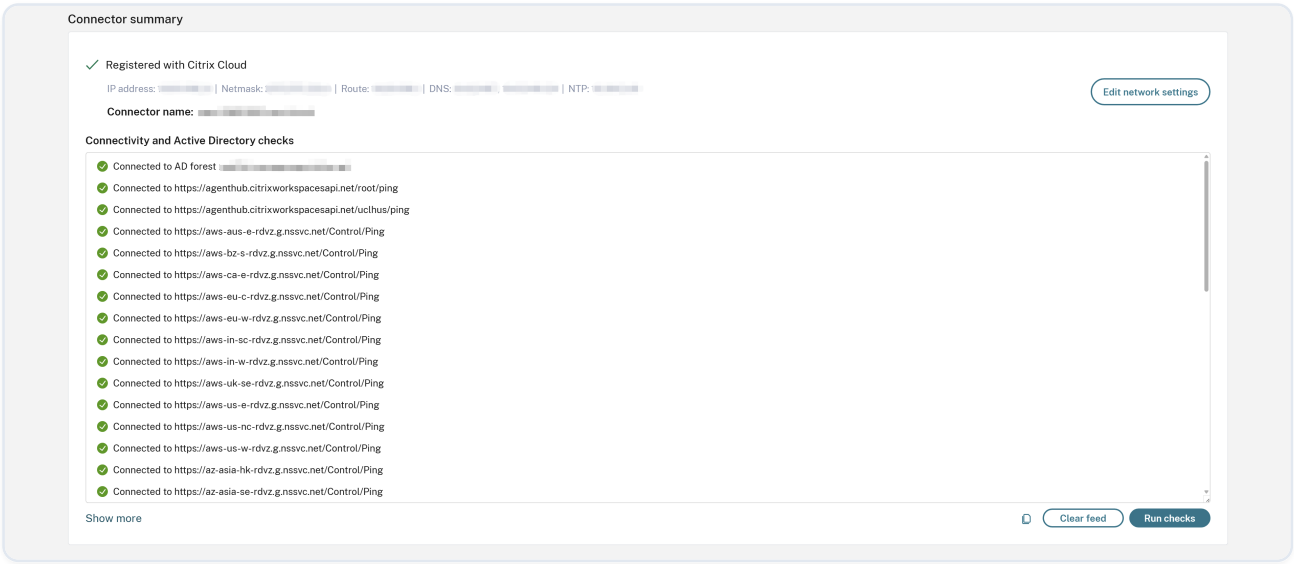
Connector Applianceの接続チェック

Connector Applianceは、Connector Applianceの接続に関するすべての要件が満たされていることを確認するために、一連の自動接続チェックを実装しています。接続要件の詳細については、「インターネット接続要件」を参照してください。

これらのチェックは手動でトリガーでき、結果はConnector Applianceの管理者ユーザーインターフェイスから表示できます。

接続チェックにアクセスして実行する手順

1. ハイパーバイザーのConnector Applianceコンソールから、IPアドレスをブラウザのアドレスバーにコピーします。
2. Connector Applianceを登録したときに設定したパスワードを入力します。
3. ページを読み込むと、テストが自動的に実行されます。
4. テストを再実行するには、**チェックの実行**をクリックします。
5. 結果をクリップボードにコピーするには、**コピー**アイコンをクリックします。



Active Directory のチェック

Active Directory に関連するチェックは、ドメインごとにグループ化されます。アプライアンスがどのドメインにも参加していない場合、Active Directory テストは実行されません。

参加している各ドメインに対して、次のチェックが実行されます。

- ドメイン接続
- ドメインとのクエリ時間同期
- Citrix Cloud からドメインへの要求を処理できることを検証する

ゲートウェイサービスプロバイダー

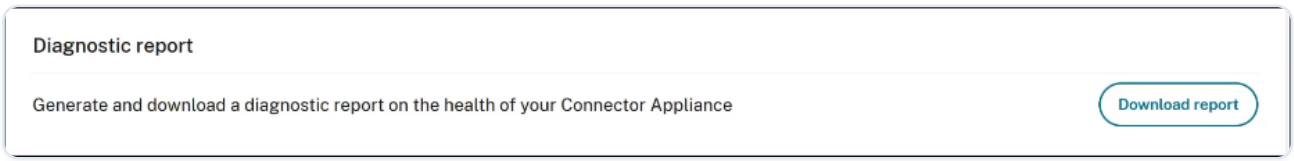
ゲートウェイサービスの場合、コネクタはプレゼンスポイントのリストを照会し、接続を検証します。

コアコネクタサービス

コアコネクタサービスの場合、Connector Appliance は、コア機能の一部として使用されるさまざまなクラウドサービスに対して HTTP GET リクエストを実行します。アプライアンスは、コネクタの新しいバージョンをダウンロードするために使用される Azure Container Registry (ACR) への接続もテストします。

診断レポートの生成

Connector Appliance 管理ページから診断レポートを生成してダウンロードできます。



1. ハイパーバイザーの Connector Appliance コンソールから、IP アドレスをブラウザーのアドレスバーにコピーします。
2. Connector Applianceを登録したときに設定したパスワードを入力します。
3. ページの**診断レポート**セクションで、**レポートのダウンロード**をクリックします。

診断レポートは`.zip`ファイルで提供されます。

ネットワーク接続を確認する

TCPキャプチャ診断チェックを使用して、**Connector Appliance管理ページ**からネットワーク接続を確認できます。

1. **Connector Appliance管理ページ**で、ヘッダーバーのアカウント名をクリックし、**ネットワーク診断**を選択します。
2. （オプション）**TCPキャプチャ**セクションで、TCPキャプチャを制限するために、ターゲットIPアドレス、ホスト名、またはポートを入力します。
3. **トレース期間**メニューから、トレースを実行する期間を選択します。
4. （オプション）パケットの内容をキャプチャするには、**パケットトレース**を有効にします。

   パケットトレースが無効になっている場合、TCPキャプチャ機能は、診断のためにヘッダーをキャプチャするためにベストエフォート型のアプローチを使用します。このベストエフォート型のアプローチでは、各パケットの最初の512バイトがキャプチャされます。ただし、ヘッダーは固定サイズではないため、このアプローチではヘッダーのすべてをキャプチャできない場合があります。
5. **トレースの開始**をクリックします。
6. トレースが完了するまで待ちます。トレースが完了したら、トレースレポートをダウンロードするか、新しいトレースを開始できます。

   - **ダウンロード**をクリックしてトレースレポートをダウンロードします。トレースレポートは`.pcap`ファイルで提供されます。
   - 別のトレースを開始するには、**新しいトレースの開始**をクリックします。

ネットワーク接続プローブツール

Connector Appliance Network Connectivity Probeは、オプションのプロキシ選択とパケットキャプチャを使用して、複数のプロトコルでサポートされているネットワークターゲットへの接続をオンデマンドでテストする方法を提供します。サポートされているプロトコル、プロキシの動作、許可されているターゲット、およびプローブ結果の解釈の詳細については、Connector Appliance Network Connectivity Probeのページを参照してください。

Active DirectoryをCitrix Cloudに接続する

Connector Applianceを使用して、Citrix Virtual Apps and Desktopsリソースを含まないフォレストにリソースの場所を接続できます。たとえば、Citrix Secure Private Access™のお客様の場合や、ユーザー認証のみに使用される一部のフォレストを持つCitrix Virtual Apps and Desktopsのお客様の場合などです。

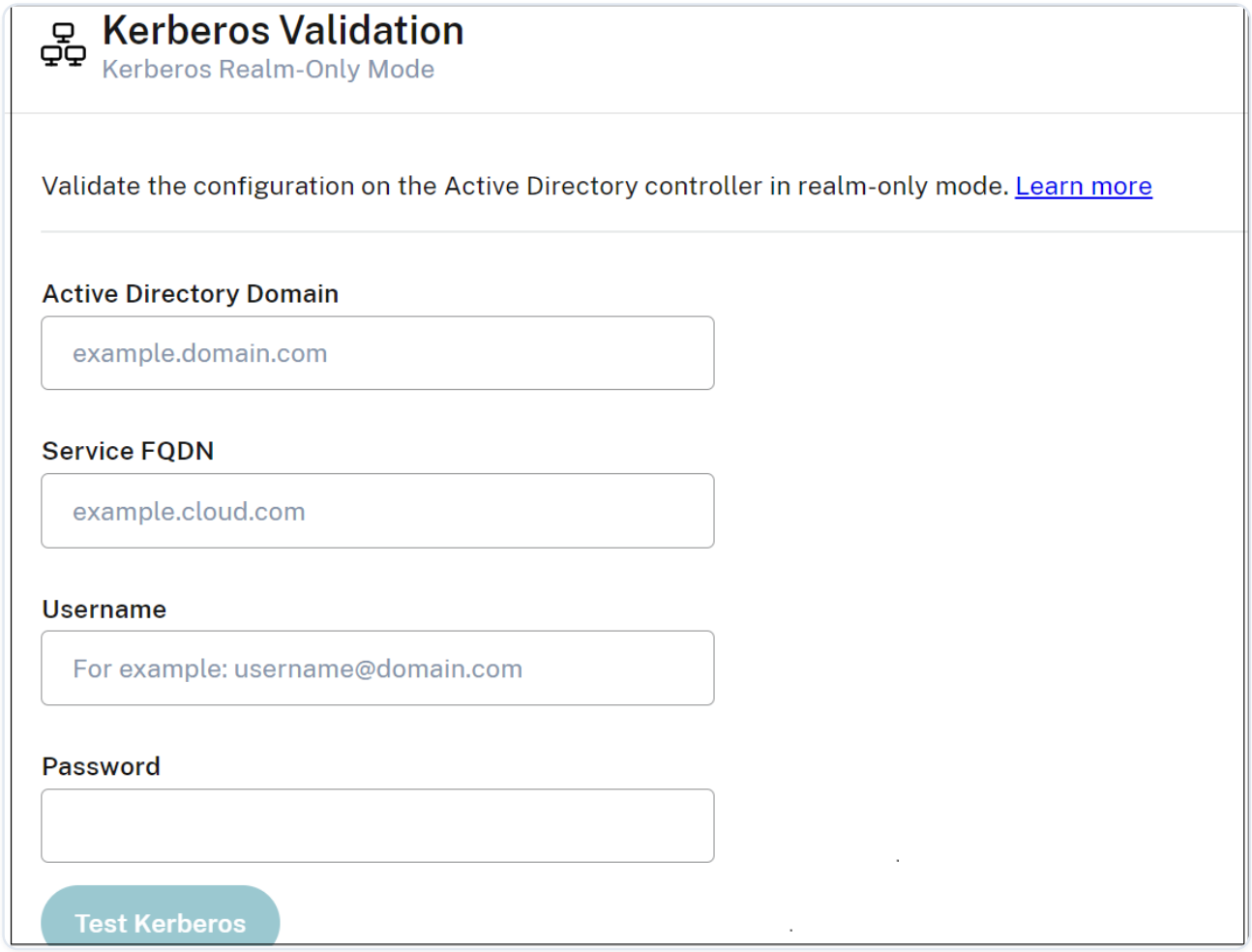
詳細については、Connector ApplianceでのActive Directoryを参照してください。

Kerberos構成の検証

シングルサインオンにKerberosを使用している場合、**Connector Appliance管理**ページからActive Directoryコントローラーの構成が正しいことを確認できます。**Kerberos検証**機能を使用すると、Kerberosレルムのみモード構成またはKerberos Constrained Delegation (KCD)モード構成を検証できます。

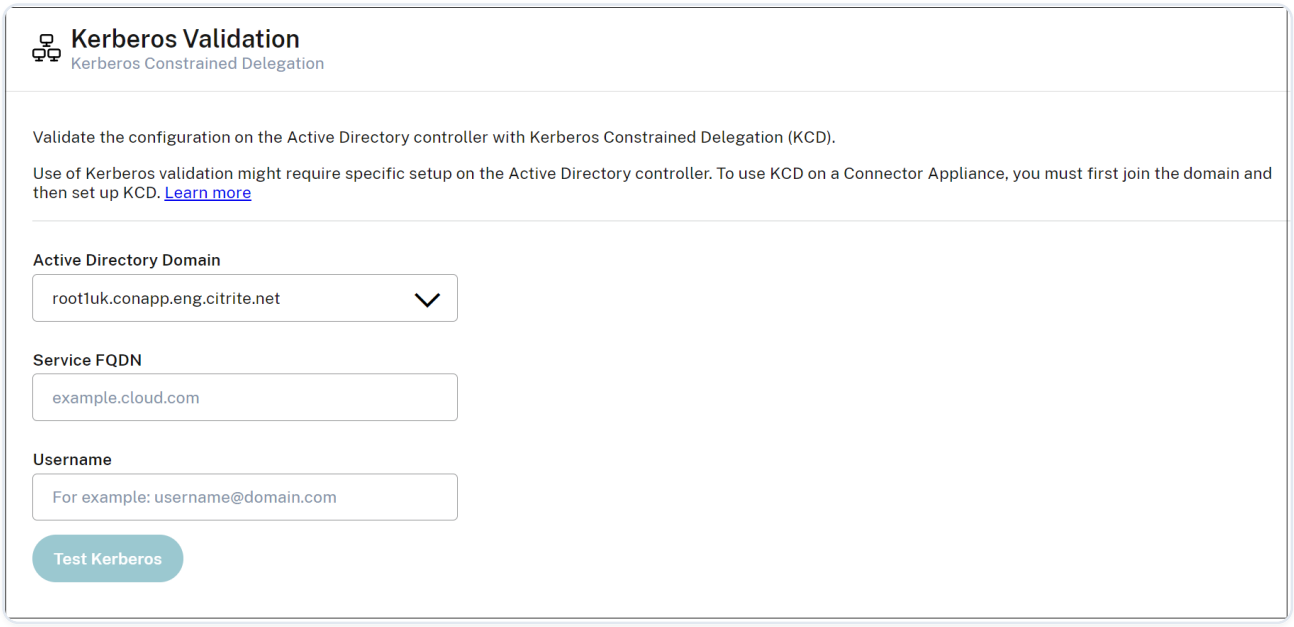
Kerberosレルムのみ構成を検証する:

1. **Connector Appliance管理**ページに移動します。
2. ハイパーバイザーのConnector Applianceコンソールから、IPアドレスをブラウザのアドレスバーにコピーします。
3. Connector Applianceを登録したときに設定したパスワードを入力します。
4. レルムのみのKerberos構成を検証するには、**Active Directoryドメイン**セクションで**Kerberos Validation Realm-Only**を選択します。
5. **Active Directoryドメイン**を指定します。
    - Kerberosレルムのみモード構成を検証している場合、任意のActive Directoryドメインを指定できます。このモードはドメインへの参加に依存しません。
6. **サービスFQDN**を指定します。デフォルトのサービス名は「https」と見なされます。「computer.example.com」を指定した場合、この値は「`<https://computer.example.com>`」と同じと見なされます。
7. **ユーザー名**を指定します。
8. 「**パスワード**」を指定します。
9. 「**Kerberosのテスト**」をクリックします。



「**Kerberosの制約付き委任（KCD）構成を検証する:**」:

1. 「**Connector Applianceの管理**」ページに移動します。
2. Connector Applianceが参加しているドメインに対して「**Kerberosの制約付き委任（KCD）**」モードを検証するには、該当するドメインの省略記号メニュー（...）から「**Kerberosの検証**」を選択します。
3. 「**Active Directoryドメイン**」を指定します。
   - Kerberosの制約付き委任構成を検証する場合は、参加しているドメインのリストから選択する必要があります。
4. 「**サービスFQDN**」を指定します。デフォルトのサービス名は「https」と見なされます。たとえば、「computer.example.com」と指定すると、この値は「`<https://computer.example.com”>`」と同じと見なされます。
5. 「**ユーザー名**」を指定します。
   - Kerberosの制約付き委任モードの場合、「**サービスアカウント**」タブを選択して、サービスアカウントを使用してKerberosのセットアップを検証することもできます。
6. 「**Kerberosのテスト**」をクリックします。



Kerberos構成が正しい場合、「Kerberosのセットアップが正常に検証されました」というメッセージが表示されます。Kerberos構成が正しくない場合、検証が失敗した理由に関する情報を提供するエラーメッセージが表示されます。

Kerberosの詳細については、Microsoftのドキュメントを参照してください。

Connector Appliance のネットワーク設定

デフォルトでは、Connector Appliance の IP アドレスとネットワーク設定は DHCP を使用して自動的に割り当てられます。

DHCP を使用して Connector Appliance を登録した後、**Connector Appliance administration page** でネットワーク設定を編集できます。

ただし、環境で DHCP が利用できない場合、または **Connector Appliance administration page** にアクセスできない場合は、Connector Appliance コンソールでネットワーク構成を直接設定できます。

Connector Appliance administration page でネットワーク設定を構成する

DHCP を使用して Connector Appliance を登録した後、**Connector Appliance administration page** でネットワーク設定を編集できます。

ネットワーク設定を手動で構成するには：

1. **Connector Summary** セクションで、**Edit network settings** を選択します。
2. **Network settings** ダイアログで、**Configure your own network settings** を選択します。
3. **IP address**、**Subnet mask**、および **Default gateway** を入力します。

4. 1つ以上の **DNS servers** を追加します。
5. 1つ以上の **NTP servers** を追加します。
6. **Save** をクリックします。

ネットワーク設定への変更を保存すると、Connector Appliance が再起動します。再起動中、Connector Appliance は一時的に利用できなくなります。**Connector Appliance administration page** からログアウトされ、このページの URL が変更されます。新しい URL は、Connector Appliance コンソールで確認するか、ハイパーバイザーのネットワーク情報を参照することで見つけることができます。

ネットワーク構成を自動割り当て値を使用するように変更するには：

1. 「**コネクタの概要**」セクションで、「**ネットワーク設定の編集**」を選択します。
2. 「**ネットワーク設定**」ダイアログで、「**IPアドレスを自動的に取得**」を選択します。
3. 「**保存**」をクリックします。

ネットワーク設定への変更を保存すると、Connector Applianceが再起動します。再起動中は、Connector Applianceは一時的に利用できなくなります。**Connector Appliance管理ページ**からログアウトされ、このページのURLが変更されます。新しいURLは、Connector Applianceコンソールで確認するか、ハイパーバイザーのネットワーク情報を参照することで見つけることができます。

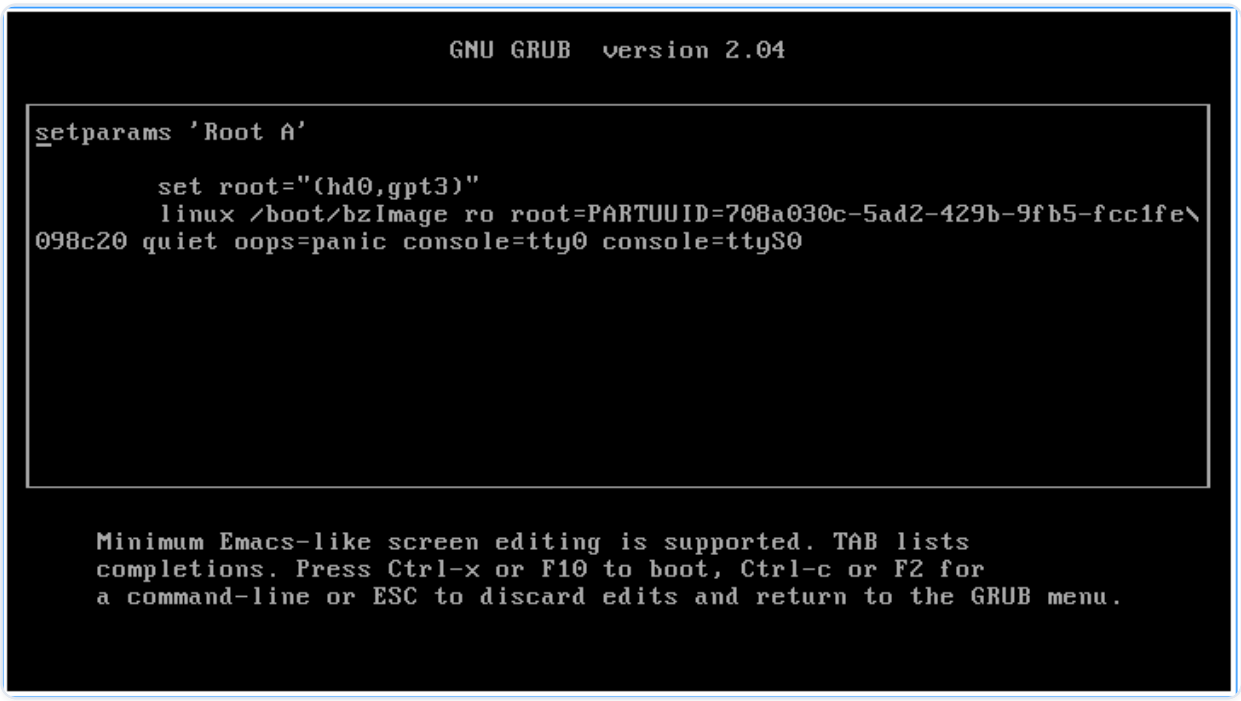
Connector Applianceコンソールを使用してネットワーク構成を設定する

デフォルトでは、Connector ApplianceのIPアドレスとネットワーク設定はDHCPを使用して自動的に割り当てられます。ただし、環境でDHCPが利用できない場合や、**Connector Appliance管理ページ**にアクセスできない場合は、Connector Applianceコンソールで直接ネットワーク構成を設定できます。

ネットワーク構成を設定するには：

1. ハイパーバイザーで、Connector Applianceを再起動します。
2. Connector Applianceの起動中に、コンソールでメッセージ`Welcome to GRUB!`が表示されるのを確認します。
3. このメッセージが表示されたら、**Esc**キーを押してGRUBメニューに入ります。
4. 起動パラメーターを編集するには、**e**キーを押します。

   次の画像のような画面が表示されます。



5. `linux`で始まる行を編集して、必要なネットワーク構成を含めます。

   - DHCPネットワークを指定するには、行の末尾に`network=dhcp`を追加します。
   - 静的ネットワークを指定するには、次のパラメータを行の末尾に追加します。

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route=<defau
     lt_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<ntp_server_1>,<nt
     p_server_2>
     ```

     プレースホルダーの値を、構成の値に置き換えます。

6. 新しい構成でConnector Applianceを起動するには、**Ctrl+X**を押します。

Connector Applianceの管理者ユーザーパスワードを変更する

1. コンソール右上のユーザーメニューから、**パスワードの変更**を選択します。

   メニューからパスワードの変更を選択します。(/en-us/citrix-cloud/media/connector-appliance-change-pw-menu.png)

   パスワード変更ページが表示されます。

   パスワード変更ページに移動します。(/en-us/citrix-cloud/media/connector-appliance-change-pw-page.png)

2. 現在のパスワードを入力し、新しいパスワードを入力して確認します。設定する新しいパスワードは、次の要件を満たす必要があります。

- 8文字以上
- 大文字と小文字の両方を含む
- 少なくとも1つの非英字文字を含む
- 現在のパスワードと同じであってはならない

3. 変更を保存するには、**パスワードの変更**を選択します。

Citrix Cloudは自動的にサインアウトし、サインインページにリダイレクトします。

サーバー証明書の置換

Connector Appliance を使用すると、管理者は管理 Web インターフェイスで使用されるデフォルトの自己署名 SSL または TLS 証明書を置き換えることができます。管理者は、組織によって署名されたカスタム証明書、または組織の信頼チェーンを使用して生成されたカスタム証明書を使用できます。

サーバー証明書管理インターフェイスにアクセスするには、Connector Appliance 管理者インターフェイスに移動します。「**Certificates**」に移動し、「**Server certificates**」タブを選択します。

デフォルトでは、Connector Appliance は自己署名証明書を使用します。カスタム証明書に置き換えた後、ブラウザが管理ページを信頼するためには、信頼された認証局が証明書を発行する必要があります。

サーバー証明書の置換オプション(/en-us/citrix-cloud/media/replace-server-certificate-option.png)

現在のサーバー証明書の表示

「**Server certificates**」タブには、現在の証明書に関する情報が記載されたカードが表示されます。

- **Subject** — 証明書のアルゴリズムとキーの長さ（例：RSA 2048）。
- **Owner** — 証明書の発行者または所有者（利用可能な場合）。
- **Expires on** — 証明書の有効期限。
- **Fingerprint** — 証明書の SHA-256 フィンガープリント。

証明書の詳細全体を表示するには、証明書カードの「**View details**」リンクをクリックします。サイドパネルが開き、解析された完全な証明書情報が表示されます。詳細パネルを閉じるには、「**Close**」をクリックします。

サーバー証明書の詳細表示を置換(/en-us/citrix-cloud/media/replace-server-certificate-view-details.png)

サーバー証明書の詳細全体を置換(/en-us/citrix-cloud/media/replace-server-certificate-full-details.png)

サーバー証明書の置換

サーバー証明書を、組織が署名したカスタム証明書に置き換えることができます。

前提条件: 証明書を置き換える前に、以下があることを確認してください。

- **PEM形式**の証明書ファイル。この証明書は、Connector Appliance管理ページにアクセスするブラウザによって信頼されている認証局によって発行されている必要があります。
- 対応する**秘密鍵（PEM形式）**。
- 秘密鍵が暗号化されている場合、その秘密鍵の**パスフレーズ**（オプション）。

証明書を置き換える手順

1. ハイパーバイザーのConnector Applianceコンソールから**IP**アドレスをコピーし、ブラウザのアドレスバーに貼り付けます。
2. Connector Applianceを登録したときに設定したパスワードを入力します。
3. 左側のメニューで**Certificates**に移動します。
4. **Server certificates**タブを選択します。
5. **Replace certificate**ボタンをクリックします。
6. ダイアログで、次のようにします。
    - PEM形式の証明書コンテンツを**Certificate (PEM format)**フィールドに貼り付けます。証明書は`-----BEGIN CERTIFICATE-----`で始まり、`-----END CERTIFICATE-----`で終わる必要があります。
    - PEM形式の秘密鍵を**Private key (PEM format)**フィールドに貼り付けます。鍵は`-----BEGIN PRIVATE KEY-----`で始まり、`-----END PRIVATE KEY-----`で終わる必要があります。
    - （オプション）秘密鍵が暗号化されている場合は、**Passphrase (optional)**フィールドにパスフレーズを入力します。
7. 「**証明書の置換**」をクリックして送信します。

置換が成功すると、システムは成功メッセージを表示し、証明書カードを新しい証明書情報で更新します。

サーバー証明書PEM形式の置換(/en-us/citrix-cloud/media/replace-server-certificate-pem-format.png)

証明書形式の要件

- 証明書と秘密鍵の両方が**PEM形式**である必要があります。
- 証明書フィールドは完全な証明書チェーンをサポートしています。中間CAが証明書に署名している場合は、完全なチェーン（サーバー証明書、その後に中間証明書）を貼り付けます。
- サポートされているキータイプは**RSA**と**ECDSA**です。

エラー処理

証明書の置換が失敗した場合、ダイアログにエラーメッセージが表示されます。失敗の一般的な原因は次のとおりです。

- 証明書と秘密鍵が一致しません。
- 証明書または秘密鍵が有効なPEM形式ではありません。
- 秘密鍵のパスフレーズが正しくありません。

エラーメッセージを確認し、問題を修正して、もう一度試してください。「**キャンセル**」をクリックすると、変更を加えずにダイアログが閉じます。

サーバー証明書PEM形式の置換(/en-us/citrix-cloud/media/replace-server-certificate-error-handling.png)

自己署名証明書への復元

デフォルトの自己署名証明書に戻すには、Connector Appliance を再展開する必要があります。現在、証明書を個別に元に戻すオプションはありません。

> **注**
>
> - 証明書を置き換えると、Connector Appliance 管理ページは、それ以降のすべてのHTTPS接続に新しい証明書を使用します。
> - **サーバー証明書**タブに表示される証明書情報は、30秒ごとに自動的に更新されます。
> - 証明書の置き換え操作には、有効なセッショントークンでログインしている必要があります。

コネクタアプライアンス を使用した Active Directory

Connector Appliance を使用すると、Citrix Virtual Apps and Desktops™ リソースを含まないフォレストにリソースの場所を接続できます。たとえば、Citrix Secure Private Access のお客様や、ユーザー認証のみに使用されるフォレストを持つ Citrix Virtual Apps and Desktops のお客様の場合などです。

Connector Appliance で複数ドメインの Active Directory を使用する場合、以下の制限が適用されます。

- VDA を含むフォレストでは、Cloud Connector の代わりに Connector Appliance を使用することはできません。

要件

Active Directory の要件

- ユーザー向けにサービスを作成するために使用するリソースとユーザーを含む Active Directory ドメインに参加していること。詳細については、この記事の「Active Directory での Connector Appliance の展開シナリオ」を参照してください。
- Citrix Cloud™ で使用する予定の各 Active Directory フォレストは、常に2つの Connector Appliance から到達可能である必要があります。
- Connector Appliance は、フォレストルートドメインと、Citrix Cloud で使用する予定のドメインの両方にあるドメインコントローラーに到達できる必要があります。詳細については、以下の Microsoft サポート記事を参照してください。
  - ドメインと信頼を構成する方法
  - Windows のサービス概要とネットワークポート要件 の「システムサービスポート」セクション
- グローバルセキュリティグループの代わりにユニバーサルセキュリティグループを使用してください。この構成により、フォレスト内の任意のドメインコントローラーからユーザーグループのメンバーシップを取得できます。

ネットワーク要件

- リソースの場所で使用するリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「システムおよび接続要件」を参照してください。

(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#connector-appliance-communication)に記載されているポートに加えて、Connector Applianceは、以下のポートを介してActive Directoryドメインへのアウトバウンド接続を必要とします。

サービス	ポート	サポートされるドメインプロトコル
ケルベロス	88	TCP/UDP
NetBIOSネームサービス	137	UDP
NetBIOSデータグラム	138	UDP
NetBIOSセッション	139	TCP
LDAP	389	TCP/UDP
TCP経由のSMB	445	TCP
ケルベロス kpasswd	464	TCP/UDP
グローバルカタログ	3268	TCP
動的RPCポート	49152–65535	TCP

コネクタアプライアンスは、LDAP署名を使用してドメインコントローラーへの接続を保護します。これは、SSL経由のLDAP (LDAPS) が不要であることを意味します。LDAP署名の詳細については、「Windows ServerでLDAP署名を有効にする方法」および「Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing」を参照してください。

サポートされているActive Directoryの機能レベル

コネクタアプライアンスは、Active Directoryの次のフォレストおよびドメインの機能レベルでテストされ、サポートされています。

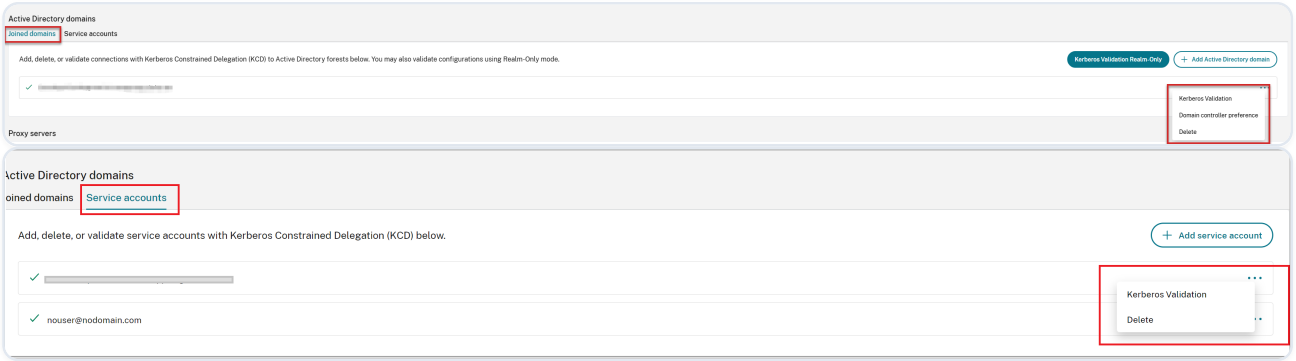
フォレストの機能レベル	ドメインの機能レベル	サポートされているドメインコントローラー
ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2019

ドメインコントローラー、フォレストの機能レベル、およびドメインの機能レベルのその他の組み合わせは、コネクタアプライアンスではテストされていません。ただし、これらの組み合わせは機能すると予想され、サポートもされています。

コネクタアプライアンスを使用してActive DirectoryドメインをCitrix Cloudに接続する

コネクタアプライアンスの管理Webページに接続すると、**Active Directoryドメイン**セクションに2つのタブが表示されます。

- **参加済みドメイン** – ドメイン内にアプライアンスのマシンアカウントを作成することによって、コネクタアプライアンスをADドメインに参加させるために使用されます。Kerberosは、参加済みドメインの右側にある省略記号メニューをクリックすることで検証できます。ドメイン内にマシンアカウントが存在する必要があります。
- **サービスアカウント** – Secure Private Access (SPA) ソリューションの一部として使用され、ドメイン参加によって作成されたマシンアカウントの代わりにサービスアカウントを使用してKerberos SSOを実現します。Kerberosは、サービスアカウントの右側にある省略記号メニューをクリックすることで検証できます。マシンに特定のドメインが関連付けられていることは必須ではありません。ただし、コネクタアプライアンスがドメインに接続されていない場合でも、ドメインコントローラーに接続できます。

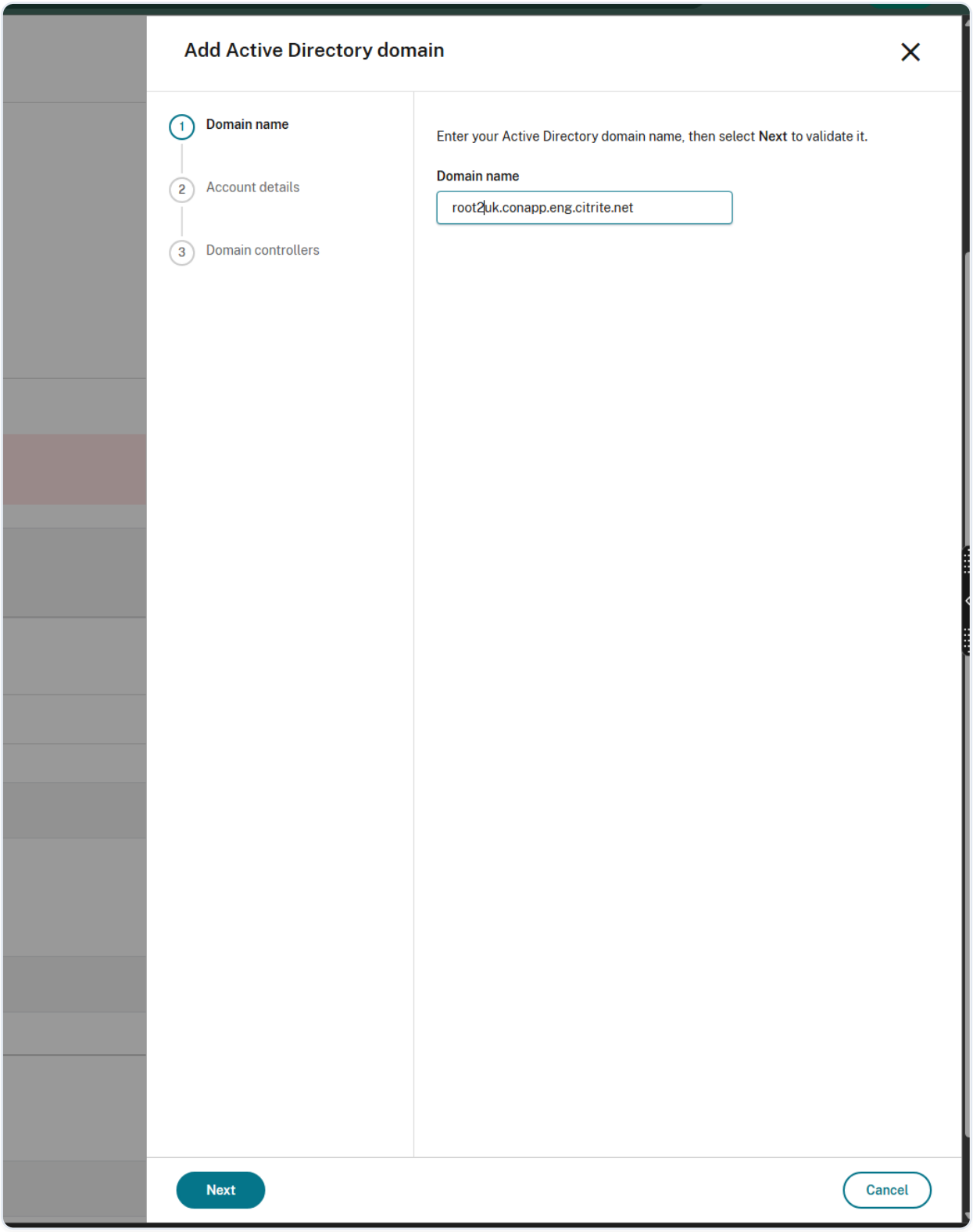


Connector Appliance を介して Active Directory を Citrix Cloud に接続するように構成するには、次の手順を実行します。

1. リソースの場所に **Connector Appliance** をインストールします。

   (/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html) の情報を参照してください。
2. **Connector Appliance** コンソールに表示されている IP アドレスを使用して、ブラウザで **Connector Appliance** 管理Webページに接続します。
3. **Active Directory ドメイン**セクションで、**参加済みドメイン**タブに移動します。
4. **+ Active Directory ドメインの追加**をクリックすると、ドメイン名を入力するための新しいポップアップウィンドウが表示されます。

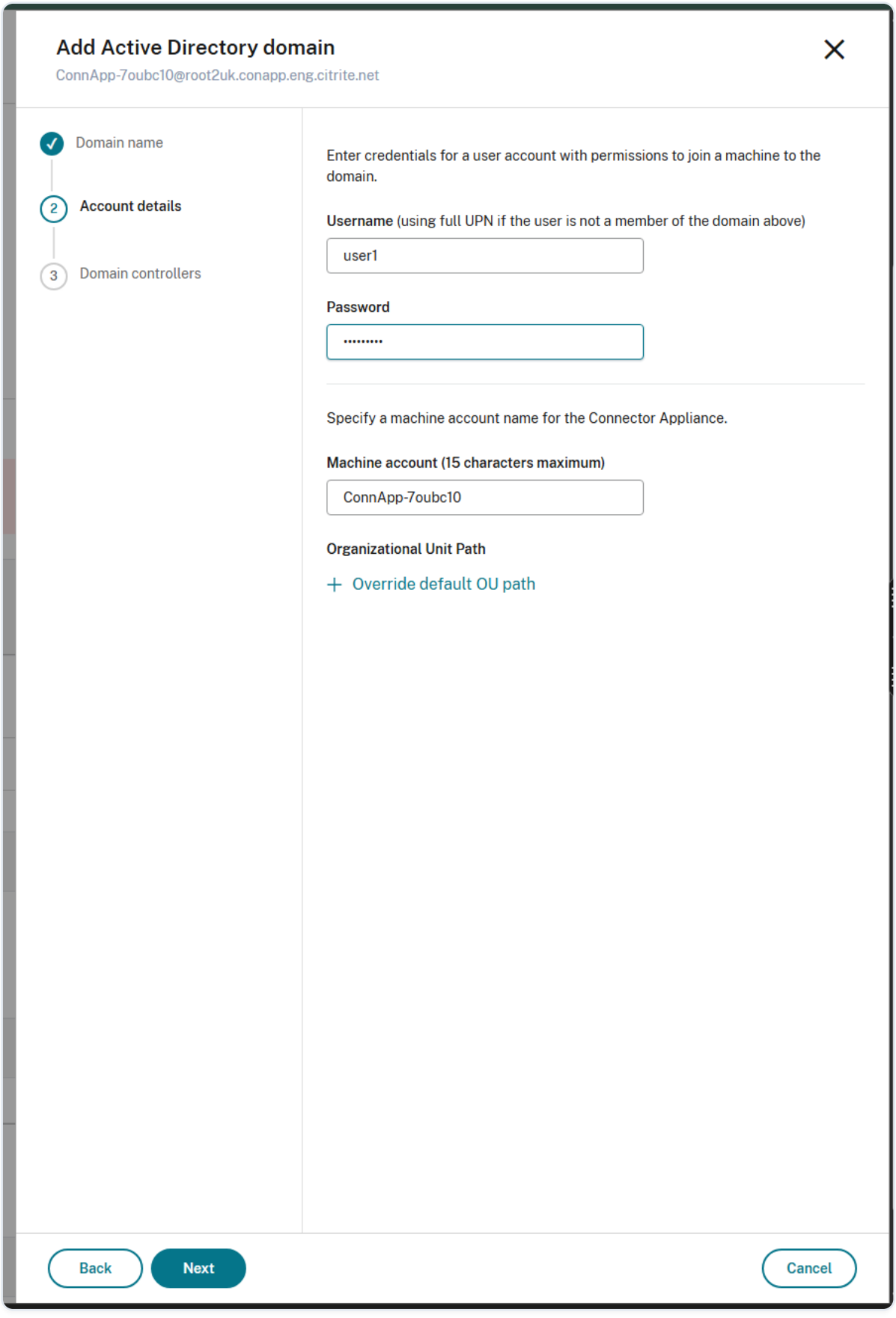
5. **ドメイン名**の手順で、Active Directory ドメイン名を入力し、**次へ**をクリックします。
   Connector Appliance がドメインをチェックします。チェックが成功すると、ウィザードは次の手順に進みます。



6. **アカウントの詳細**の手順で、次の情報を入力し、**次へ**をクリックします。

   - ドメインに参加する権限を持つ Active Directory ユーザーのユーザー名とパスワード。

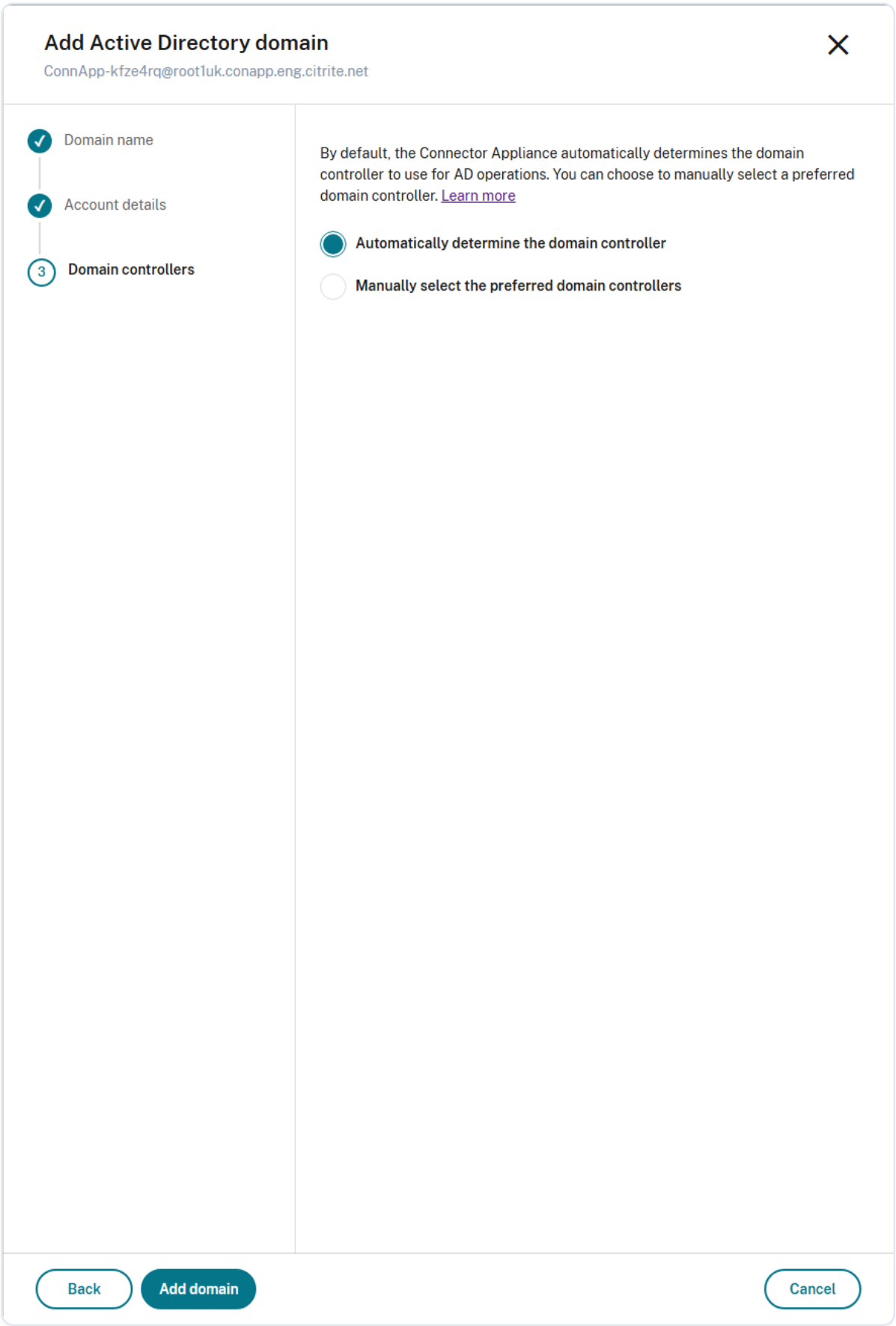
- マシン名。**Connector Appliance** はマシン名を提案します。最大15文字の独自のマシン名で上書きできます。このマシン名は、**Connector Appliance** が参加するときに Active Directory ドメインに作成されます。



7. **ドメインコントローラー**の手順で、**Connector Appliance** がこのドメインのドメインコントローラーを選択する方法について、次のいずれかのオプションを選択します。

   - **ドメインコントローラーを自動的に決定する** (デフォルト) – Connector Appliance は、Active Directory 操作に使用するドメインコントローラーを自動的に決定し、この選択を定

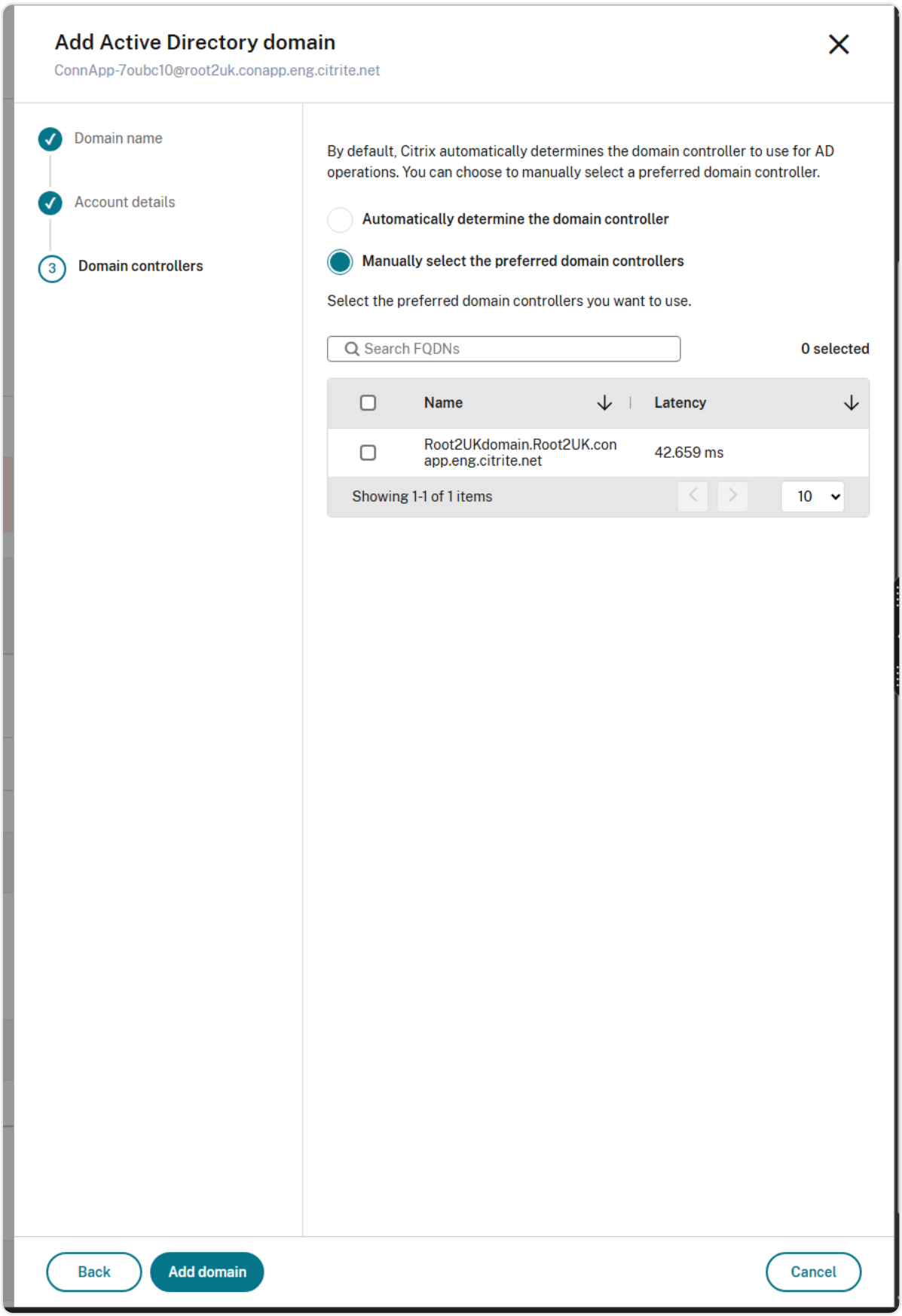
期的に再評価します。



- **優先ドメインコントローラーを手動で選択する** — **Connector Appliance** は、選択したドメインコントローラーのみを使用します。検索可能なテーブルには、測定された**待機時間**

(ミリ秒単位) とともに利用可能なドメインコントローラーが一覧表示されます。検索ボックスを使用して名前でフィルタリングするか、**名前**または**待機時間**で並べ替えてから、使用するドメインコントローラーのチェックボックスを選択します。ドメインコントロー

ラーを選択しない場合、**Connector Appliance** は自動選択に戻ります。



8. 「**ドメインの追加**」をクリックします。ドメインは、**Connector Appliance** UI の「**Active Directory ドメイン**」セクションに表示されます。

次のステップ

- このConnector Applianceにさらにドメインを追加できます。

> **注：**
>
> Connector Applianceは、最大10のフォレストでテストされています。

- 復元性を高めるため、各リソースの場所で、各ドメインを複数のConnector Applianceに追加します。

Active Directory構成の表示

リソースの場所にあるActive DirectoryドメインとConnector Applianceの構成は、次の場所で表示できます。

- Citrix Cloudの場合：
  a. メニューで、「**IDおよびアクセス管理**」ページに移動します。
  b. 「**ドメイン**」タブに移動します。

     Active Directoryドメインは、それらが属するリソースの場所とともに一覧表示されます。
- Connector ApplianceのWebページの場合：
  a. Connector Applianceコンソールで提供されているIPアドレスを使用して、Connector ApplianceのWebページに接続します。
  b. 初めて登録したときに作成したパスワードでログインします。
  c. ページの「**Active Directory ドメイン**」セクションで、このConnector Applianceが参加しているActive Directoryドメインのリストを確認できます。

Connector ApplianceからActive Directoryドメインを削除する

Active Directoryドメインから離脱するには、次の手順を実行します。

1. Connector Applianceコンソールに表示されているIPアドレスを使用して、Connector ApplianceのWebページに接続します。
2. 初めて登録したときに作成したパスワードでログインします。
3. ページの「**Active Directory ドメイン**」セクションで、参加しているActive Directoryドメインのリストから、離脱したいドメインを見つけます。

4. Connector Applianceによって作成されたマシンアカウントの名前を控えておきます。
5. ドメインの横にある削除アイコン（ゴミ箱）をクリックします。確認ダイアログが表示されます。
6. アクションを確定するには、**続行**をクリックします。
7. Active Directoryコントローラーに移動します。
8. コントローラーから、Connector Applianceによって作成されたマシンアカウントを削除します。

参加済みActive Directoryドメインのドメインコントローラー設定を変更する

Active Directoryドメインに参加した後、**Connector Appliance**がそのドメインに使用するドメインコントローラーをいつでも変更できます。デフォルトでは、**Connector Appliance**はドメインコントローラーを自動的に決定し、定期的に選択を再評価します。ドメインコントローラーが多数存在する環境で一貫性のないパフォーマンスが観察された場合は、1つ以上の優先ドメインコントローラーを手動で選択するように切り替えることができます。

参加済みドメインのドメインコントローラー設定を変更するには、次の手順を実行します。

1. **Connector Appliance**コンソールに表示されているIPアドレスを使用して、**Connector Appliance**管理Webページに接続します。
2. 初めて登録したときに作成したパスワードでログインします。
3. **Active Directory ドメイン**セクションの**参加済みドメイン**タブで、更新するドメインを見つけます。
4. ドメインの横にある省略記号 (**...**) メニューをクリックし、**ドメインコントローラーの優先設定**を選択します。

   ドメインコントローラーの優先設定ブレードが開きます。

   参加済みドメイン(/en-us/citrix-cloud/media/connector-appliance-joined-domains-tab.png)
5. このドメインのドメインコントローラーを**Connector Appliance**が選択する方法を選択します。

   - **ドメインコントローラーを自動的に決定する** – **Connector Appliance**は、Active Directory操作に使用するドメインコントローラーを自動的に決定し、この選択を定期的に再評価します。
   - **優先ドメインコントローラーを手動で選択する** – **Connector Appliance** は、選択したドメインコントローラーのみを使用します。検索可能な テーブルには、利用可能なドメインコントローラーが測定された **待機時間**（ミリ秒）とともに表示されます。検索ボックスを使

用して名前でフィルターするか、**名前**または**待機時間**で並べ替えてから、使用するドメインコントローラーのチェックボックスを選択します。

> **注:**
>
> **優先ドメインコントローラーを手動で選択する**を選択してもドメインコントローラーを選択しない場合、**Connector Appliance**は自動選択にフォールバックします。

6. **保存**をクリックして変更を適用します。

フォレストの優先コネクタタイプを設定する

Citrix Cloudテナントが、同じADフォレストに結合されたWindowsコネクタとコネクタアプライアンスの両方を持っている場合、優先コネクタタイプを設定できます。

特定のActive Directoryフォレストの優先コネクタタイプを設定するには、次の手順を実行します。

1. **IDとアクセス管理 > ドメイン**に移動し、優先コネクタタイプを設定したいADフォレストのドロップダウン矢印をクリックします。
2. 「**フォレスト優先コネクタタイプ**」を選択します。

フォレスト優先コネクタタイプ(/en-us/citrix-cloud/media/forest-preferred-connector-type.png)

Active Directory で Connector Appliance を使用するための展開シナリオ

Cloud Connector と Connector Appliance の両方を使用して、Active Directory コントローラに接続できます。使用するコネクタのタイプは、展開によって異なります。

Active Directory で Cloud Connector を使用する方法の詳細については、「Active Directory での Cloud Connector の展開シナリオ」を参照してください。

次の状況で、Connector Appliance を使用してリソースの場所を Active Directory フォレストに接続します。

- Secure Private Access を設定しています。詳細については、「Connector Appliance を使用した Secure Private Access」を参照してください。
- ユーザー認証のみに使用されるフォレストが 1 つ以上ある場合
- 複数のフォレストをサポートするために必要なコネクタの数を減らしたい場合
- その他のユースケースで Connector Appliance が必要な場合

すべてのフォレストに対して単一の Connector Appliance セットを持つ 1 つ以上のフォレスト内のユーザーのみ

このシナリオは、Standard のお客様、または Secure Private Access に Connector Appliance を使用しているお客様に適用されます。

このシナリオでは、ユーザーオブジェクトのみを含む複数のフォレスト (`forest1.local`、`forest2.local`) があります。これらのフォレストにはリソースは含まれていません。1 つの Connector Appliance セットがリソースの場所に展開され、これらの各フォレストのドメインに参加しています。

- 信頼関係: なし
- **ID およびアクセス管理**にリストされているドメイン: `forest1.local`、`forest2.local`
- クラウドストアへのユーザーログオン: すべてのユーザーでサポートされています
- オンプレミスストアへのユーザーログオン: すべてのユーザーでサポートされています

個別のフォレスト (信頼関係あり) に存在するユーザーとリソース、すべてのフォレストに単一のコネクタアプライアンスセットを使用

このシナリオは、複数のフォレストを持つ Citrix Virtual Apps and Desktops のお客様に適用されます。

このシナリオでは、一部のフォレスト (`resourceforest1.local`, `resourceforest2.local`) にはリソース (例: VDA) が含まれ、一部のフォレスト (`userforest1.local`, `userforest2.local`) にはユーザーのみが含まれます。これらのフォレスト間には、ユーザーがリソースにログオンできるようにする信頼関係が存在します。

`resourceforest1.local` フォレスト内に Cloud Connector のセットが 1 つ展開されます。`resourceforest2.local` フォレスト内には、別の Cloud Connector のセットが展開されます。

`userforest1.local` フォレスト内にコネクタアプライアンスのセットが 1 つ展開され、同じセットが `userforest2.local` フォレスト内にも展開されます。

- 信頼関係: 双方向フォレスト信頼、またはリソースフォレストからユーザーフォレストへの一方向信頼
- **ID およびアクセス管理**にリストされているドメイン: `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- Citrix® StoreFront Cloud へのユーザーログオン: すべてのユーザーでサポートされています
- オンプレミス StoreFront へのユーザーログオン: すべてのユーザーでサポートされています

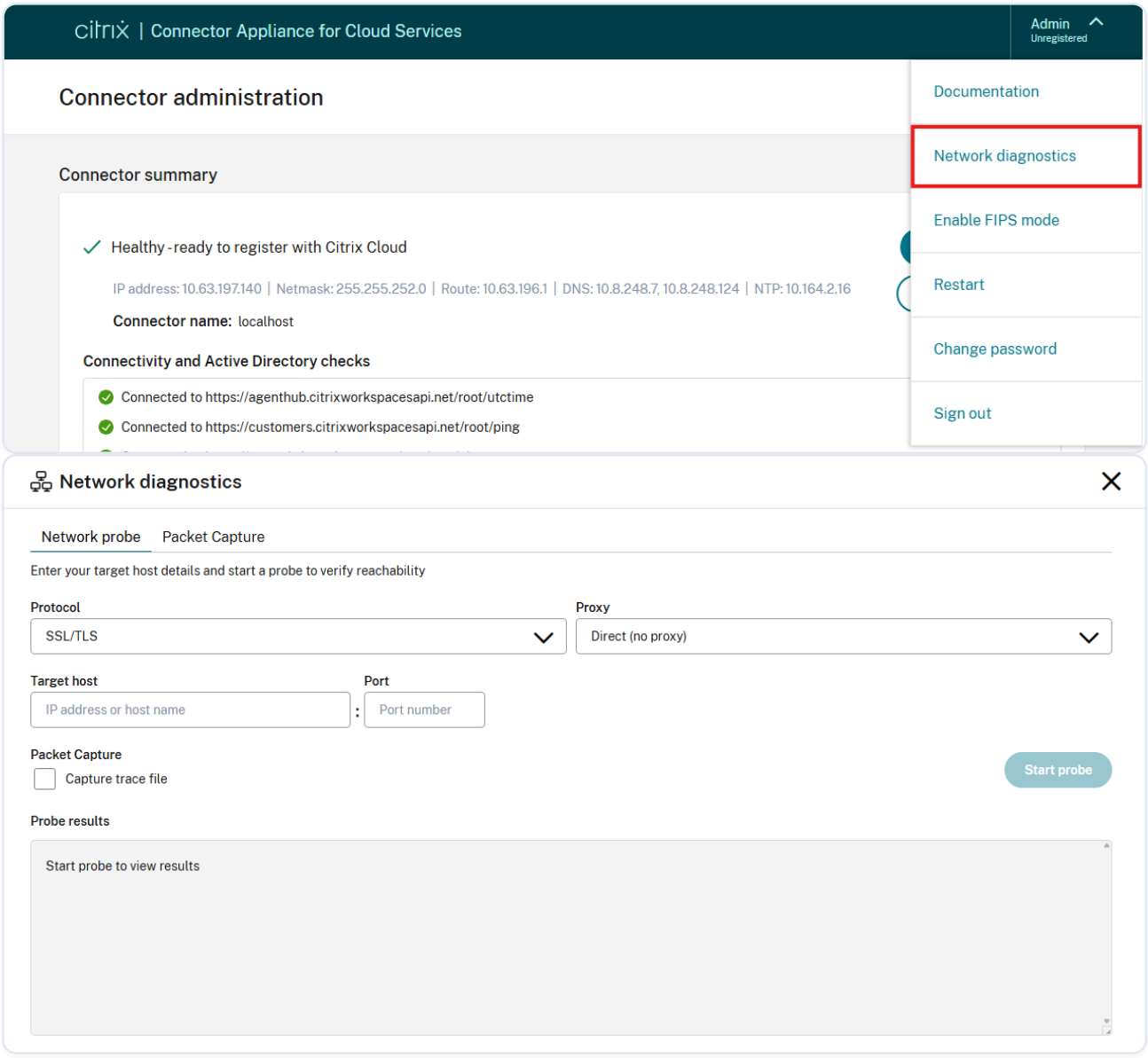
Connector Appliance ネットワーク接続プローブ

Connector Appliance ネットワーク接続プローブを使用すると、ユーザーはネットワークターゲットのオンデマンド接続チェックを実行できます。

ネットワークプローブのユーザーインターフェイスは、Connector Appliance 管理者インターフェイスから、右上隅のメニューにある **Network diagnostics** に移動することでアクセスできます。

以下のプロトコルがサポートされています。

- ICMP (ping リクエストの送信)
- TCP
- TLS
- HTTP
- HTTPS



プロキシの指定

デフォルトでは、ネットワークプローブはプロキシを使用せずに指定されたターゲットに直接接続します。

ICMP ネットワークプローブはプロキシを使用しません。

他のプロトコルについては、Connector Appliance で構成されているプロキシのいずれかを、**Proxy** ドロップダウンを使用してネットワークプローブ用に選択できます。その後、ネットワークプローブは選択されたプロキシを介して実行されます。

TCP、TLS、HTTPSプロトコルでは、プロキシはHTTPSプロキシとして使用され、ネットワークプローブは選択されたプロキシにHTTP CONNECTリクエストを送信して、指定されたネットワークターゲットへの接続を確立します。

HTTPプロトコルが選択されている場合、プロキシはネットワークプローブによってプレーンHTTPプロキシとして使用されます。

ネットワーク診断プロキシ(/en-us/citrix-cloud/media/network-diagnostics-proxy.png)

許可されるネットワークターゲット

すべてのプライベートネットワークターゲットに対してプローブが許可されます。外部のパブリックネットワークターゲットの場合、インターネット接続要件セクションに記載されているドメインのみが許可されます。これらのドメインはそれぞれ、Citrixが所有しているか、Connector Applianceの運用に必要なサービスに属しています。

パケットキャプチャ

トレースファイルのキャプチャチェックボックスをオンにすると、ネットワークプローブの期間中、パケットトレースを有効にできます。プローブが完了すると、プローブの**プローブ結果**の下にパケットキャプチャへのリンクが表示されます。このパケットトレースファイルは、ネットワークプローブの結果をさらに診断するのに役立ちます。

> **注：**
>
> パケットトレースは、ネットワークプローブの期間中、Connector Appliance上のすべてのトラフィックをキャプチャします。これはネットワークプローブ自体のトラフィックだけでなく、機密データや資格情報が含まれる場合があります。

> ネットワーク診断パケットキャプチャ(/en-us/citrix-cloud/media/network-diagnostics-packet-capture.png)

ネットワークプローブの結果

プローブの開始ボタンをクリックすると、**プローブ結果**ボックスにネットワークプローブの進行状況が表示されます。DNS解決、TCP接続など、ネットワークプローブの各ステップに関する情報が表示されます。ネットワークプローブが進行するにつれて、各ネットワークプローブステージの横にあるアイコンは、進行中、完了、失敗のいずれであるかを示し、各ステップのタイミング情報とエラー詳細が表示されます。

ネットワーク診断プローブ結果(/en-us/citrix-cloud/media/network-diagnostics-probe-results.png)

HTTPベースのプローブ結果の解釈

HTTPおよびHTTPSネットワークプローブは、返されるHTTPステータスコードに関係なく、ターゲットURLからHTTP応答が受信される限り、成功とマークされます。HTTP応答ステータスコードを含む応答のHTTPステータスラインは、**プローブ結果**に表示されます。

プロキシが選択されている場合、プレーンなHTTPネットワークプローブについても同様です。この場合、選択されたプロキシはプレーンなHTTPプロキシとして使用され、プロキシがHTTP応答を返す限り、プローブは成功と見なされます。エラー状態コードとともに**プローブ結果**に表示されるHTTPステータス行は、プロキシからのエラー、またはターゲットURLからのエラーを示している可能性があります。

コネクタの更新

定期的に、Citrix® は Cloud Connector または Connector Appliance のパフォーマンス、セキュリティ、信頼性を向上させるための更新をリリースします。

新しいコネクタバージョンが Citrix Cloud テナントで利用可能になると、デフォルトの動作として、テナント内の各コネクタは、ランダムな順序で一度に1つずつ、すぐに更新をインストールします。いずれかのコネクタが更新を実行できなかった場合、それ以降のすべてのコネクタが更新を開始するのを防ぎます。これは、テナント内のすべてのコネクタで更新の失敗が発生するのを防ぐためです。更新に失敗したコネクタが更新に成功するか、または削除されるとすぐに、それ以降のコネクタは直ちに更新を進めます。詳細については、「更新の失敗のトラブルシューティング」を参照してください。

更新がユーザーの Citrix Cloud™ エクスペリエンスに不必要に影響を与えることなくタイムリーにインストールされるように、コネクタの更新を次のように制御できます。

- 更新の開始時刻を、希望する時間帯と希望する曜日にスケジュールします。

- 1回限りの遅延を実行し、指定したコネクタがスケジュールより2週間後に更新されるようにします。
- ホストマシン上の問題が原因で更新が失敗した場合は、問題が解決された後に更新を再開します。

また、リソースロケーションの現在のコネクタバージョンと Citrix Cloud のターゲットバージョンを比較することで、コネクタが最新であることを確認できます。

> **注:**
>
> この記事では、Citrix Cloud 管理コンソールを使用してコネクタの更新をスケジュールする方法について説明します。Citrix Cloud API を使用してコネクタ更新の希望する時間帯と曜日を設定する方法については、Citrix Developer ドキュメントの「Citrix Cloud - メンテナンススケジュール」を参照してください。

希望する時間帯

希望する時間帯を指定すると、Citrix Cloud は更新が利用可能になってから24時間後に、指定した時間に更新のインストールを開始します。たとえば、希望する時間帯が米国太平洋時間の午前2時で、火曜日に更新が利用可能になった場合、Citrix Cloud は24時間待機し、翌日の午前2時に更新のインストールを開始します。

希望する曜日

希望する曜日を指定すると、Citrix Cloud は、指定した曜日に更新のインストールを開始する前に7日間待機します。この7日間の待機期間により、オンデマンドで更新をインストールするか、Citrix Cloud が指定した曜日にインストールを開始するのを待つかを選択する十分な時間が得られます。選択した曜日と更新が利用可能になる日によっては、Citrix Cloud は最大13日間更新のインストールを開始するのを待機する場合があります。

8日間の待機期間の例

月曜日に、更新の優先日として火曜日の午後6時を設定します。その日のうちに、Citrix Cloudから更新が利用可能であるという通知が届き、**更新**ボタンが表示されます。更新を開始しない場合、Citrix Cloudは7日間待機し、翌日の火曜日の午後6時に更新のインストールを開始します。

13日間の待機期間の例

更新の優先時間として月曜日の午後6時を設定しました。火曜日に、Citrix Cloudから更新が利用可能であるという通知が届き、**更新**ボタンが表示されます。更新を開始しない場合、Citrix Cloudは7日間待機し、その6日後の月曜日の午後6時に更新のインストールを開始します。

> **注:**
>
> 更新スケジュールは、コネクタが更新を試行し始める時間を示します。更新は各コネクタに1つずつインストールされるため、実際の更新はスケジュールされた時間よりも遅れる場合があります。たとえば、リソースロケーションで最初に更新されるコネクタが更新中に問題に遭遇し、更新の完了に4時間かかった場合、リソースロケーション内の後続のコネクタは、スケジュールされた時間から少なくとも4時間後まで更新を開始しません。

> この動作のため、失敗したコネクタの更新を再開したり、更新に失敗したコネクタをCitrix Cloudから削除したりする前に、残りのコネクタがすぐに更新を開始する可能性があり、この更新が営業時間中に発生する可能性があることに注意することが重要です。

更新通知とオンデマンド更新

更新が利用可能になると、Citrix Cloudは通知でアラートを送信して通知します。また、各コネクタには更新がインストールされる日付と時刻が表示されます。

Citrix Cloudから利用可能な更新の通知が届くと、各コネクタに**更新**ボタンが表示され、優先する時間や日よりも早く更新をインストールできます。各コネクタで**更新**を選択すると、Citrix Cloudは更新をキューに入れ、1つずつインストールします。更新を開始した後は、キャンセルできません。

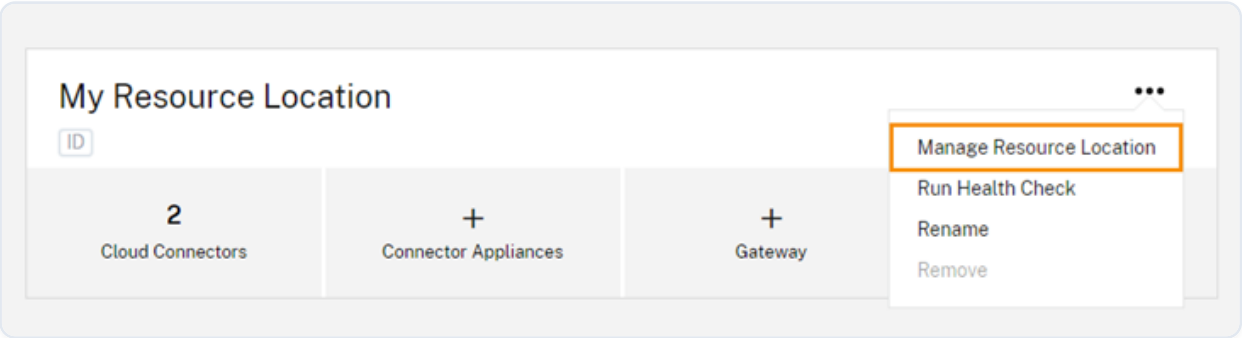
更新が完了すると、Citrix Cloudは最終更新日を表示します。一部の更新が完了できない場合は、通知が送信されます。

更新スケジュールを選択する

このセクションの手順を使用して、Citrix Cloud管理コンソールからコネクタの更新をスケジュールします。Citrix Cloud APIを使用した更新のスケジュールについては、Citrix Developerドキュメントの Citrix Cloud - Maintenance Schedules を参照してください。

1. Citrix Cloudメニューから、**リソースの場所**を選択します。

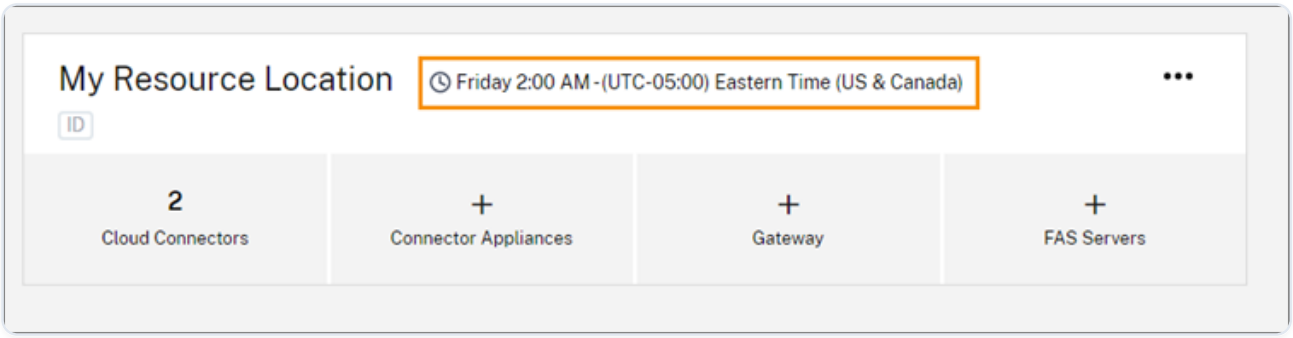
2. 変更したいリソースの場所を見つけ、省略記号メニューから**リソースの場所の管理**を選択します。



3. 「**更新方法の選択**」で、「**メンテナンス開始時刻の設定**」を選択し、更新をインストールする希望の日、時刻、タイムゾーンを選択します。

   - 希望する時刻のみを指定するには、更新をインストールする時間とタイムゾーンを選択します。Citrix Cloudは、更新が利用可能になってから24時間後に、指定された時刻に更新をインストールします。
   - 希望する曜日を指定するには、時間、曜日、タイムゾーンを選択します。Citrix Cloudは、更新が利用可能になってから7日間待機し、指定された曜日に更新をインストールします。

更新スケジュールを設定すると、Citrix Cloudは、リソースロケーション名の横にそれを表示します。



選択した開始時刻は、コネクタが配置されているタイムゾーンに関係なく、すべてのコネクタに適用されます。異なるタイムゾーンにコネクタがある場合、Citrix Cloudは選択した時刻とタイムゾーンで更新をインストールします。たとえば、米国太平洋時間の午前2時に更新をスケジュールし、ロンドンにコネクタがある場合、Citrix Cloudは米国太平洋時間の午前2時にそれらのコネクタへの更新のインストールを開始します。

> **注:**
>
> 更新スケジュールは、コネクタが更新を試行し始める時刻を示します。更新は各コネクタに1つずつインストールされるため、実際の更新はスケジュールされた時刻よりも遅れる場合

があります。たとえば、リソースロケーションで最初に更新されるコネクタが更新中に問題に遭遇し、更新の完了に4時間かかった場合、リソースロケーション内の後続のコネクタは、スケジュールされた時刻から少なくとも4時間後まで更新を開始しません。

この動作のため、失敗したコネクタの更新を再開したり、更新に失敗したコネクタをCitrix Cloudから削除したりする前に、残りのコネクタがすぐに更新を開始する可能性があり、この更新が営業時間中に発生する可能性があることに注意することが重要です。

更新の再開

コネクタが更新のインストール中に問題に遭遇した場合、問題が解決されるまでインストールは一時停止します。更新は各コネクタに1つずつインストールされるため、1つのコネクタで一時停止した更新は、Citrix Cloudアカウント内の残りのすべてのCloud Connectorの更新を妨げる可能性があります。問題が解決された後、更新を再開できます。

1. Citrix Cloudメニューから、**リソースロケーション**を選択します。
2. 管理するリソースロケーションを見つけ、**Cloud Connectors**または**Connector Appliances**タイルを選択します。
3. 管理するコネクタを見つけ、**更新の再開**を選択します。



アップデートを延期する

指定したコネクタに対して、予定されているアップデートを2週間後に発生するように延期できます。予定されているアップデートは1回のみ延期できます。一度延期すると、再度延期することはできません。また、デフォルトの2週間という期間を変更することはできません。

1. Citrix Cloudメニューから、**リソースの場所**を選択します。
2. 管理したいリソースの場所を見つけ、**Cloud Connectors**または**Connector Appliances**タイルを選択します。
3. 管理したいコネクタを見つけ、**アップデートを延期する**を選択します。

アップデート延期ボタンが強調表示されたコネクタタイル(/en-us/citrix-cloud/media/connector-update-delay-button.png)

予定日は、元の予定日より2週間後の日付に変更されます。

スケジュール外のアップデート

アップデートを後日または後刻にスケジュールした場合でも、Citrix Cloudは利用可能になり次第、可能な限り早くアップデートをインストールする場合があります。スケジュール外のアップデートは、次の場合に発生します。

- アップデートが利用可能になってから48時間以内に、希望する時間にインストールできない場合。たとえば、希望する時間が午前2時で、アップデートリリース後3日間コネクタがオフラインの場合、コネクタがオンラインに戻るとCitrix Cloudはすぐにアップデートをインストールします。
- アップデートに、重要なセキュリティまたは機能の問題に対する修正が含まれている場合。

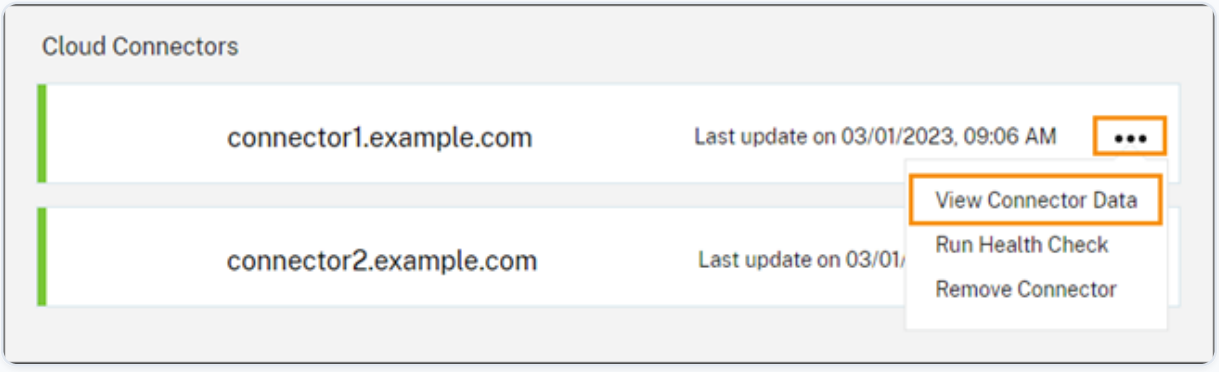
Cloud Connectorのバージョンを比較する

リソースの場所で実行されているCloud Connectorのバージョンと、それが最新バージョンであるかどうかを確認できます。この情報は、Cloud Connectorが正常にアップデートされていることを確認するのに役立ちます。

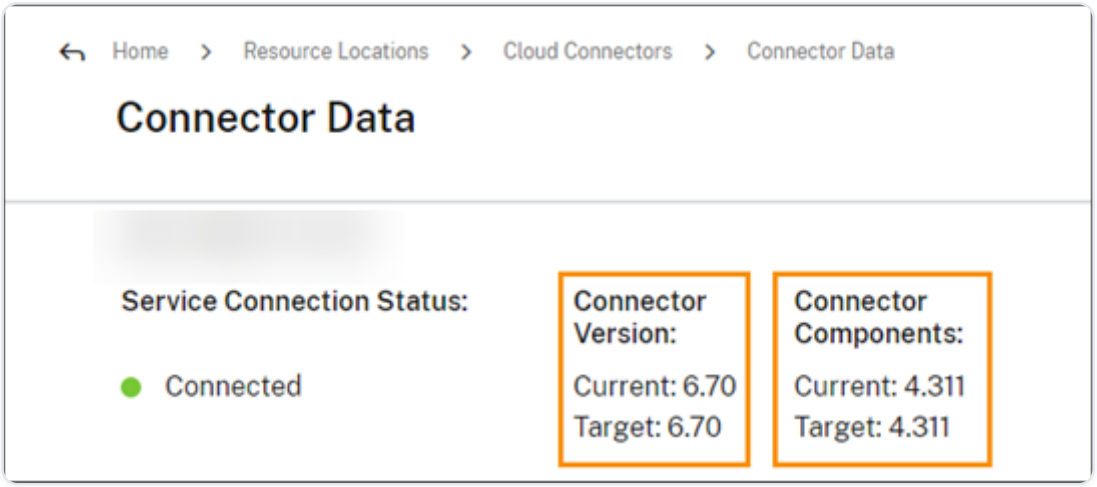
注：

この情報はConnector Appliancesでは利用できません。

リソースの場所ページから、管理するリソースの場所の**Cloud Connectors**タイルを選択します。確認するCloud Connectorを見つけ、省略記号メニューから**View Connector Data**を選択します。



Currentバージョン番号は、Cloud Connectorマシンで現在実行されているCloud Connectorソフトウェアのバージョンです。**Target**バージョン番号は、Citrixがリリースした Cloud Connectorソフトウェアの最新バージョンです。マシンが正常に更新された場合、Currentバージョン番号とTargetバージョン番号は一致します。



更新の失敗のトラブルシューティング

Cloud Connectorマシンにインストールされている競合するソフトウェアや、メンテナンス中の予期しないエラーにより、Cloud Connectorの更新失敗やサービス停止につながる可能性があります。Cloud Connectorのメンテナンス後に更新が失敗した場合の対処方法については、Resolve a Failed Cloud Connector Maintenanceを参照してください。

Cloud Connectorが正常に更新されない場合は、次の条件を確認することで、問題のトラブルシューティングを開始できます。

- Cloud Connectorの電源がオンになっており、Cloud Connector Advanced Connectivity Checksを使用してCitrix Cloudに接続されている。
- プロキシとファイアウォールが正しく構成されている。
- 必要なWindowsサービスが開始状態である。
- 詳細ログがCloud Connectorで有効になっている。

Cloud Connectorの更新失敗のトラブルシューティング手順については、Citrixサポート技術情報でCTX270718を参照してください。

トラブルシューティングの支援が必要な場合は、Citrix Cloud Connectorログを Citrixに送信できます。詳細については、Log Collection for Citrix Cloud Connectorを参照してください。

IDとアクセス管理

IDとアクセス管理は、Citrix Cloud™管理者およびエンドユーザーに使用されるIDプロバイダーとアカウントを定義します。

IDプロバイダー

Citrix Cloudでサポートされているプロバイダーは、Citrix Cloud管理者、エンドユーザー、またはその両方を認証するために使用できます。

IDプロバイダー	管理者認証	エンドユーザー認証
Citrix® IDプロバイダー	はい	いいえ
オンプレミスActive Directory	いいえ	はい
Active Directoryとトークン	いいえ	はい
Microsoft Entra ID (マイクロソフト エントラ ID)	はい	はい
Citrix Gateway (シトリックス ゲートウェイ)	いいえ	はい
グーグル クラウド アイデンティティ	はい	はい
オクタ	いいえ	はい
SAML 2.0	はい	はい

既定では、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。

Citrix ID プロバイダー

Citrix Cloud には、管理者がサインインするときに認証するための組み込みの Citrix ID プロバイダーが含まれています。Citrix Cloud コンソールでは、Citrix ID プロバイダーは Citrix Identity と表示されます。 管理者認証に別の ID プロバイダーを使用する場合、Citrix は、**Citrix ID プロバイダー**の下に少なくとも1人のフルアクセス管理者を持つことを推奨します。この条件により、以下が保証されます。

- プライマリ ID プロバイダーが利用できなくなった場合でも、Citrix Cloud アカウントからロックアウトされることはありません。
- Microsoft Entra ID などの別の ID プロバイダーでサインインしている場合は完了できない特定の操作を実行するために、Citrix Cloud アカウントにアクセスできます。たとえば、Microsoft Entra ID が選択した ID プロバイダーであり、Microsoft Entra ID と Citrix Cloud 間の接続を再開する必要がある場合、Citrix ID プロバイダーを使用してサインインした後にこのタスクを実行できます。

Citrix ID プロバイダーを削除する

Citrix ID プロバイダーは、すべての新しい Citrix Cloud アカウントで既定で接続されています。Citrix ID プロバイダーを使用しないことを選択した場合、必要に応じて接続を削除できます。たとえば、セキュリティおよび管理者管理に関する組織のポリシーに準拠するために、この接続を削除することを選択する場合があります。

この接続を削除すると、Citrix ID プロバイダーが無効になり、Citrix Cloud 管理者の認証に使用できなくなります。

Citrix ID プロバイダーの接続を削除する前に、Citrix Cloud で別の ID プロバイダーが構成されている必要があります。Citrix Cloud では、別の構成済み ID プロバイダーが存在しない限り、この接続を削除することはできません。

> **重要**
>
> 選択した ID プロバイダーへのアクセスを失った場合、Citrix サポートに連絡して Citrix Cloud アカウントを回復する必要があります。このプロセスには数日かかる場合があります。

Citrix ID プロバイダーの接続を削除するには:

1. Citrix Cloud メニューから、**ID およびアクセス管理**を選択します。

2. **認証**タブで、Citrix ID プロバイダーを見つけます。
3. 省略記号メニューをクリックし、**IDプロバイダーの削除**を選択します。



4. 削除の確認を求められたら、**このIDプロバイダーを削除すると、Citrix Cloud内のこのIDプロバイダーの構成データも削除されることを理解しています**を選択します。
5. **IDプロバイダーの削除**をクリックします。

Citrixフェデレーション認証サービス

Citrix Cloudは、Citrixフェデレーション認証サービスを使用してエンドユーザーにシングルサインオンアクセスを提供することもサポートしています。詳細については、以下の記事を参照してください。

- FASをCitrix Cloudに接続する: Citrixフェデレーション認証サービスを使用したストアのシングルサインオンを有効にする
- シトリックス テックゾーン:
  - 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
  - 技術インサイト: フェデレーション認証サービス

管理者

管理者は自身のIDを使用してCitrix Cloudにアクセスし、管理アクティビティを実行し、Citrix Cloud Connectorをインストールします。

CitrixのIDメカニズムは、メールアドレスとパスワードを使用して管理者に対して認証を提供します。管理者はMy Citrixの資格情報を使用してCitrix Cloudにサインインすることもできます。

多要素認証

Citrix Cloudは、管理者とエンドユーザーの両方に多要素認証方法を提供します。

管理者については、Citrix Cloudへのサインイン時に多要素認証が必要です。管理者は、Citrix Cloudアカウントをオンボーディングする際、または別の管理者からの招待を承諾した後に、デバイスを登録できます。詳細については、以下の記事を参照してください。

- 多要素認証を設定する
- プライマリMFA方法を管理する
- MFAリカバリ方法を管理する

エンドユーザーについては、管理者がActive Directoryプラス認証トークン認証方法を構成すると、多要素認証が有効になります。Active Directoryプラス認証トークンは、Citrix® StoreFront CloudのデフォルトのIDプロバイダーです。構成後、エンドユーザーは多要素認証のためにデバイスを登録します。詳細については、以下の記事を参照してください。

- Active Directoryプラス認証トークン認証を有効にする
- 2要素認証のためにデバイスを登録する
- デバイスを再登録する

または、Citrix Cloud管理者とエンドユーザーの両方にMicrosoft Entra ID多要素認証を使用することもできます。展開方法の詳細については、「Microsoft Azure MFAの展開方法」を参照してください。

新しい管理者の追加

アカウントのオンボーディングプロセス中に、最初の管理者が作成されます。最初の管理者として、Citrix Cloudアカウントに他の管理者を追加できます。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、必要に応じて新しいアカウントを設定できます。また、追加する管理者のアクセス権限を細かく調整することもできます。これらの権限を設定することで、組織における管理者の役割に合わせてアクセスレベルを調整できます。

管理者の追加とアクセス権限の設定の詳細については、「管理者アクセスを管理する」を参照してください。

パスワードをリセットする

パスワードを忘れた場合やリセットしたい場合は、Citrix Cloudサインインページの**「ユーザー名またはパスワードを忘れましたか？」**をクリックしてください。アカウントを見つけるためにメールアドレスまたはユーザー名を入力すると、Citrixからパスワードをリセットするためのリンクが記載されたメールが送信されます。

Citrixは、アカウントのパスワードを安全に保つために、特定の条件下でパスワードをリセットすることを要求します。これらの条件の詳細については、「パスワードの変更」を参照してください。

> **注：**

Citrix Cloudからのメールがスパムやゴミ箱フォルダに入らないように、許可されたメールアドレスのリストに**mailto:customerservice@citrix.com**を追加してください。

管理者を削除する

管理者タブで、Citrix Cloudアカウントから管理者を削除できます。管理者を削除すると、その管理者はCitrix Cloudにサインインできなくなります。

アカウントを削除したときに管理者がログインしていた場合、その管理者は最大1分間アクティブなままです。その後、Citrix Cloudへのアクセスは拒否されます。

注：

- アカウントに管理者が1人しかいない場合、その管理者を削除することはできません。Citrix Cloudでは、各顧客アカウントに少なくとも1人の管理者が必要です。
- Citrix Cloud Connectorは管理者アカウントにリンクされていません。そのため、Cloud Connectorをインストールした管理者を削除しても、Cloud Connectorは引き続き動作します。

エンドユーザー

エンドユーザーのIDは、Citrix Cloudでアクセスできるサービスを定義します。このIDは、リソースロケーション内のドメインから提供されるActive Directoryドメインアカウントから取得されます。エンドユーザーをライブラリオファリングに割り当てると、そのエンドユーザーはそのオファリングにアクセスする権限が与えられます。

管理者は、**ドメイン**タブで、これらのIDを提供するのに使用されるドメインを制御できます。複数のフォレストからドメインを使用する予定がある場合は、各フォレストに少なくとも2つのCitrix Cloud Connectorをインストールしてください。Citrixは、高可用性環境を維持するために、少なくとも2つのCitrix Cloud Connectorを推奨しています。Active DirectoryでのCloud Connectorの展開の詳細については、「Active DirectoryでのCloud Connectorの展開シナリオ」を参照してください。

注：

- ドメインを無効にすると、新しいIDが選択されることのみが防止されます。すでに割り当てられているIDをエンドユーザーが使用することを妨げるものではありません。
- 各Citrix Cloud Connectorは、インストールされている単一のフォレスト内のすべてのドメインを列挙して使用できます。

エンドユーザーの使用状況を管理する

個々のアカウントまたはActive Directoryグループを使用して、エンドユーザーをサービスに追加できます。Active Directoryグループを使用する場合、グループをサービスに割り当てた後は、Citrix Cloudを介した管理は不要です。

管理者が個々のエンドユーザーまたはエンドユーザーのグループをサービスから削除すると、それらのエンドユーザーはそのサービスにアクセスできなくなります。特定のサービスからエンドユーザーを削除する方法の詳細については、Citrix製品ドキュメント Webサイトでそのサービスのドキュメントを参照してください。

プライマリリソースの場所

プライマリリソースの場所とは、ドメインとCitrix Cloud間の通信で「最も推奨される」ものとして指定するリソースの場所です。プライマリリソースの場所には、ドメインへの最高のパフォーマンスと接続性を持つCitrix Cloud Connectorがあるリソースの場所を選択してください。このリソースの場所をプライマリリソースの場所とすることで、ユーザーはCitrix Cloudにすばやくログオンできるようになります。

詳細については、プライマリリソースの場所を選択するを参照してください。

詳細情報

- サポートされているIDプロバイダーの詳細については、CitrixトレーニングWebサイトのCitrix Identity and Authenticationの概要教育コースを参照してください。
- シトリックス テックゾーン:
  - Tech Brief: ワークスペースID
  - Tech Brief: ワークスペースシングルサインオン
  - Tech Insight: モバイルSSO

Citrix Cloudへの管理者アクセスを管理する

管理者はCitrix Cloudコンソールから管理されます。管理者の認証に使用するIDプロバイダーに応じて、個別に、またはグループを使用して管理者を追加できます。

すべての管理者は、Citrix Cloudにサインインする際に、認証の第二要素としてトークンを使用する必要があります。管理者を追加した後、管理者は多要素認証にデバイスを登録し、Citrix SSOなど、Time-Based One-Time Password標準に準拠する任意のアプリを使用してトークンを生成できます。

新しい管理者を追加する

Citrix Cloudは、管理者の認証に次のIDプロバイダーをサポートしています。

- Citrix IDプロバイダー: Citrix CloudのデフォルトのIDプロバイダーです。個々の管理者のみの追加をサポートします。
- Microsoft Entra ID: 個別に、およびME-IDグループを介して管理者を追加することをサポートします。詳細については、管理者グループの管理を参照してください。
- SAML 2.0: 個別に、およびADグループを介して管理者を追加することをサポートします。詳細については、Citrix CloudにSAMLをIDプロバイダーとして接続するを参照してください。
- Google: 個別に、およびGoogleグループを介して管理者を追加することをサポートします。詳細については、Google Cloud Identityを参照してください。

新しい管理者を追加するには、次のワークフローを使用します。

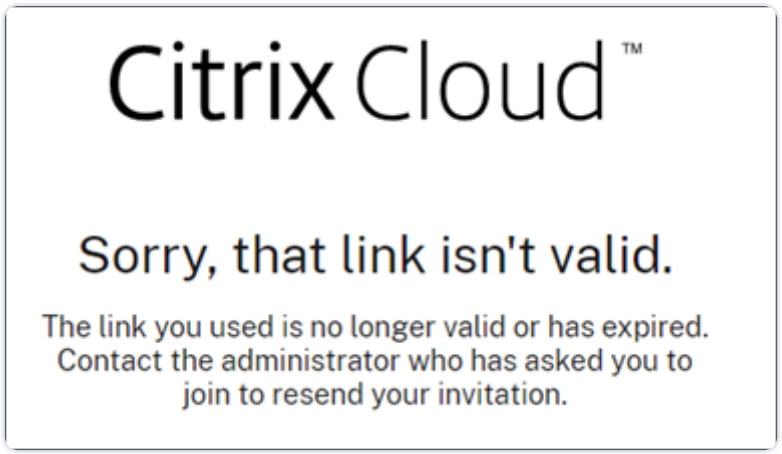
1. 管理者の認証に使用するIDプロバイダーを選択します。
2. IDプロバイダーに応じて、個々の管理者を招待するか、管理者が属するグループを選択します。
3. 組織における管理者の役割に合わせたアクセス権限を指定します。詳細については、この記事の管理者権限の変更を参照してください。

個々の管理者を招待する

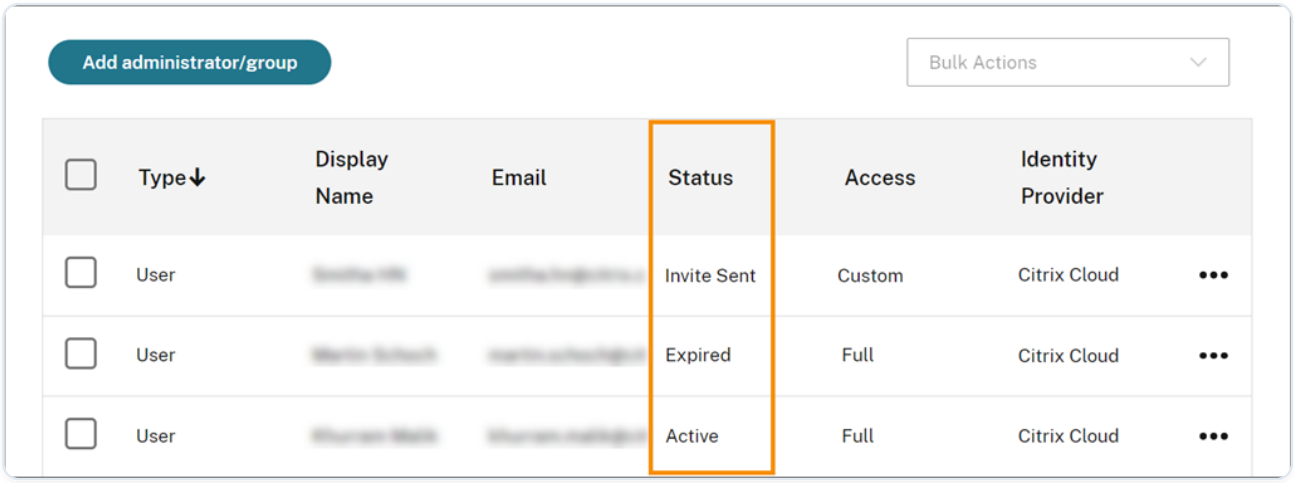
個々の管理者を追加するには、Citrix Cloudアカウントへの参加を招待します。管理者を追加すると、Citrixから招待メールが送信されます。管理者はサインインする前に、招待を承諾する必要があります。グループを介して追加された管理者は招待を受け取らず、追加後すぐにサインインできます。

招待メールは`cloud@citrix.com`から送信され、アカウントへのアクセス方法が説明されます。招待は送信日から5日間有効です。5日経過すると、招待リンクは期限切れになります。招待され

た管理者が期限切れのリンクを使用した場合、Citrix Cloudはリンクが無効であることを示すメッセージを表示します。



Citrix Cloudは招待のステータスも表示するため、管理者が招待を承諾してCitrix Cloudにサインインしたかどうかを確認できます。



注

管理者アカウントは、最大100の顧客アカウントに関連付けることができます。管理者が100を超える顧客アカウントを管理する必要がある場合は、追加の顧客を管理するために、別のメールアドレスで別の管理者アカウントを作成する必要があります。または、管理者が管理する必要がなくなった顧客アカウントから管理者アカウントを削除することもできます。

管理者を招待するには

1. Citrix Cloudにサインインし、メニューから を選択します。

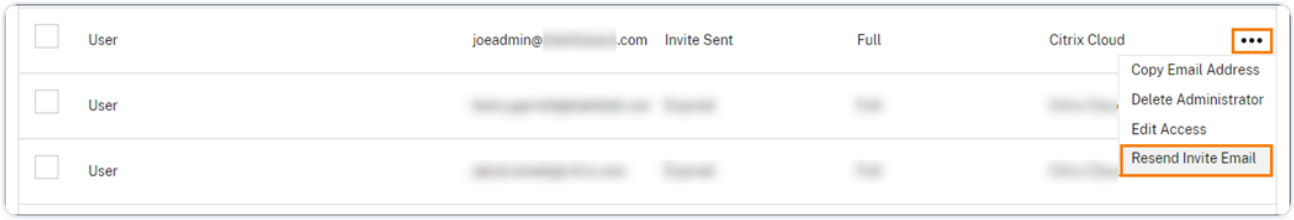
2. ページで、 を選択します。コンソールには、アカウント内の現在の管理者がすべて表示されます。

3. を選択します。
4. で、使用するIDプロバイダーを選択します。Microsoft Entra IDを使用している場合、Citrix Cloudは最初にサインインを求めることがあります。
5. が選択されている場合は、ユーザーのメールアドレスを入力し、 を選択します。
6. が選択されている場合は、追加するユーザーの名前を入力し、 をクリックします。ME-IDゲストユーザーの招待はサポートされていません。
7. **アクセス設定**で、管理者に対して適切な権限を構成します。**フルアクセス**（既定で選択）では、すべてのCitrix Cloud機能とサブスクライブ済みサービスを制御できます。**カスタムアクセス**では、選択した機能とサービスを制御できます。
8. 管理者の詳細を確認します。変更を加えるには、**［戻る］**を選択します。
9. **［招待状を送信］**を選択します。Citrix Cloudは、指定したユーザーに招待状を送信し、管理者をリストに追加します。

招待状を再送する

招待状を再送するには、コンソールの一番右にある省略記号メニューから**［招待メールを再送］**を選択します。招待状を再送しても、招待状の有効期限が切れるまでの5日間の制限には影響しません。



新しいサインインリンクで招待状を再送する

元の招待メールの有効期限が切れた場合は、管理者に新しいメールを送信できます。次の手順を実行します。

1. Citrix Cloudから管理者を削除します。**［管理者］ページで、リストから管理者を見つけ、省略記号メニューから［管理者の削除］**を選択します。
2. Citrix Cloudが削除を完了するまで数分間待ちます。場合によっては、削除直後に管理者を再度招待すると、サインインリンクが正しくない招待状が送信されることがあります。
3. 「管理者を招待するには」の説明に従って、管理者を再度招待します。

管理者招待を承諾する

Citrix Cloudアカウントに招待されると、Citrixから組織IDとアカウントの顧客名が記載されたメールが送信されます。

招待を承諾するには、**［サインイン］**をクリックします。その後、ブラウザウィンドウが開きます。Citrix Cloudアカウントをまだお持ちでない場合は、パスワードを作成するページがブラウザに表示されます。すでにアカウントをお持ちの場合は、既存のパスワードを使用してサインインするようCitrix Cloudから求められます。

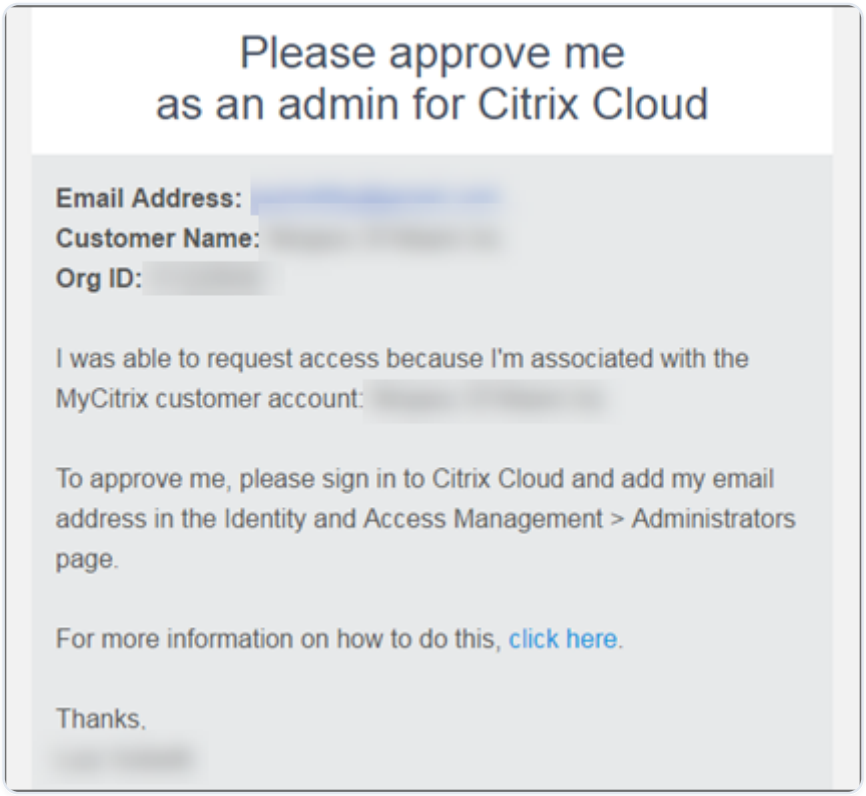
サインイン中に、多要素認証への登録を求められる場合があります。登録手順については、「多要素認証を設定する」を参照してください。

管理者グループの追加

管理者を追加するには、ADグループ（SAML認証の場合）、Microsoft Entra IDグループ（Microsoft Entra ID認証の場合）、またはGoogleグループ（Google認証の場合）を使用できます。詳細については、「管理者グループの管理」を参照してください。

Citrix Cloudへの参加リクエストを承認する

Citrix Cloudから、組織内の誰かが管理者としてCitrix Cloudアカウントに参加したいという承認リクエストを受け取ることがあります。



これらのリクエストを承認するには、この記事の「個々の管理者を招待する」で説明されているように、アクセスを要求しているユーザーを管理者として招待します。承認リクエストメールに記載されているものと同じメールアドレスを使用する必要があります。

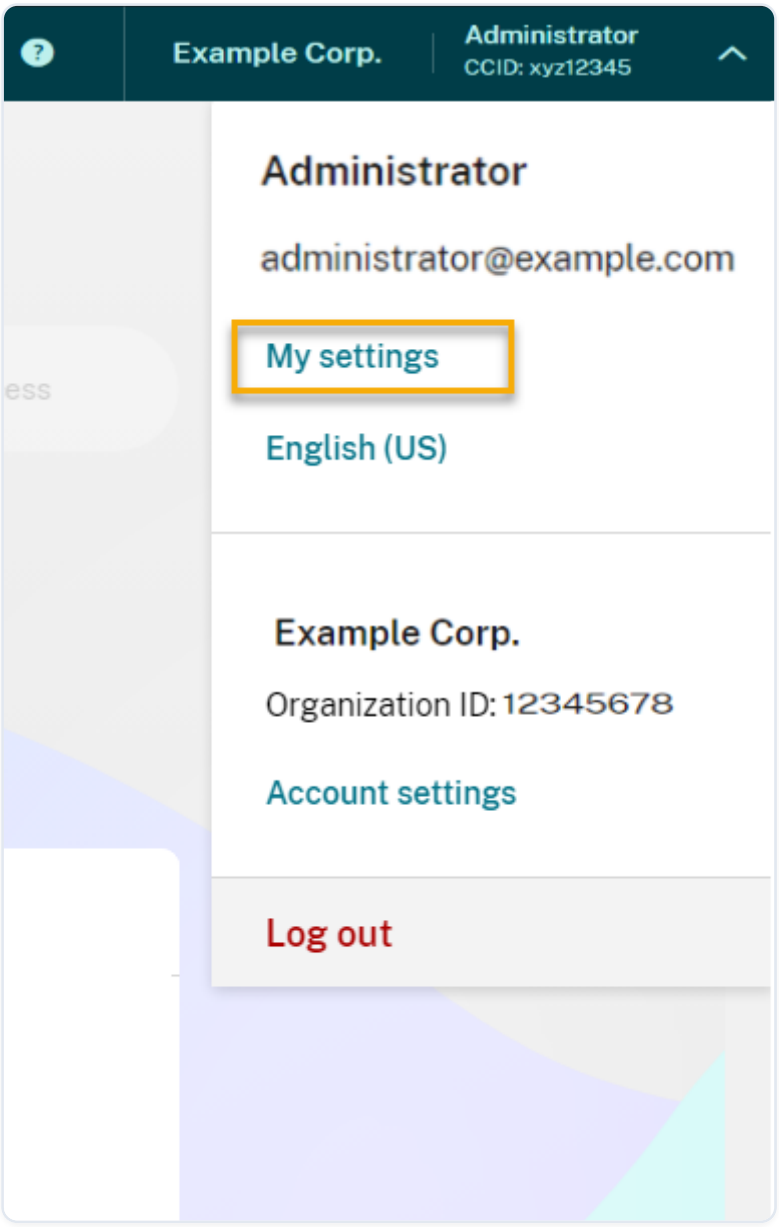
招待状を受け取った後、アクセスを要求しているユーザーは**サインイン**リンクをクリックして招待を承諾します。その後、Citrix Cloudのパスワードを作成し、アカウントにサインインできます。

承認リクエストがどのように生成されるかについては、「アカウントが既に使用されている場合はどうなりますか？」を参照してください。

メールアドレスを変更する

Citrix Cloudで自分のメールアドレスを変更できます。新しいアドレスは、多要素認証（MFA）のリカバリ用メールアドレスとは異なる必要があります。メールアドレスを変更すると、Citrix Cloudから新しいアドレスに確認メールが送信されます。確認後、Citrix Cloudは変更を完了するためにサインアウトします。数分後、新しいメールアドレスで再度サインインできます。

1. 右上隅のメニューから、**マイ設定**を選択します。



2. **メールアドレス**で、**メールアドレスの変更**を選択します。
3. 新しいメールアドレスを入力し、**確認メールを送信**を選択します。
4. メールに記載されている6桁の確認コードを入力し、**確認して完了**を選択します。
5. 変更を確定するには、**はい、メールアドレスを変更します**を選択します。

変更を確定すると、Citrix Cloudからサインアウトされます。数分後、新しいメールアドレスで再度サインインできます。

管理者権限の変更

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. By default, new administrators are assigned *full access permissions* to all Citrix Cloud account functions and available services. If

you want to limit access to certain areas of the management console or specific services, you can define *custom access permissions*.

フルアクセス権限を持つCitrix Cloud管理者のみが、他の管理者の権限を定義できます。

既存の管理者権限を変更するには：

1. Citrix Cloudに(https://citrix.cloud.com/)でサインインします。
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**［管理者］**を選択します。
3. 管理するIDプロバイダーを選択します：Citrix Identity（デフォルト）、Active Directory（IDプロバイダーとしてSAMLを使用している場合）、またはMicrosoft Entra ID（接続済みの場合）。
4. 管理する管理者またはグループを見つけ、省略記号ボタンをクリックして、**［アクセス権の編集］**を選択します。

   ［アクセス権の編集］メニューオプションが強調表示されたCitrix Cloud管理者リスト(/en-us/citrix-cloud/media/console-admin-edit-access.png)
5. 特定の権限を許可または拒否するには、**［カスタムアクセス］**を選択します。すべてのCitrix Cloud機能へのアクセスを許可するには、**［フルアクセス］**を選択します。
6. サービス権限をすばやく見つけるには、検索ボックスに入力し始めます。入力すると、Citrix Cloudは一致する権限を表示します。たとえば、「read only」と入力し始めると、タイトルに「read only」を含む権限が表示されます。権限の検索では大文字と小文字は区別されません。
7. Citrix Cloud管理コンソールのカスタムアクセス権限を定義するには、**［一般］**を展開します。

   ［カスタムアクセス］が強調表示されたCitrix Cloudアクセス権限(/en-us/citrix-cloud/media/console-admin-general-custom-access-new.png)
8. 特定のサービスに対するカスタムアクセス権限を定義するには、そのサービスを展開します。
9. 各権限について、必要に応じてチェックマークを選択または解除します。
10. **保存**を選択します。

コンソール権限

このセクションでは、Citrix Cloud管理コンソールで利用可能なカスタムアクセス権限について説明します。特定のサービスに対するカスタムアクセス権限の詳細については、そのサービスのドキュメントを参照してください。ほとんどのプラットフォームロールは**読み取り専用**アクセスをサ

ポートしていますが、一部のロールは**読み取り専用**または**フルアクセス**のみに制限されています（以下を参照）：

- **顧客ダッシュボード:** Citrix Service Provider (CSP) のみ。顧客ダッシュボードへの表示アクセスを許可します。(読み取り専用のみ)
- **ドメイン: IDおよびアクセス管理 > ドメイン**タブへのアクセスを許可します。管理者は、このタブからCitrix Cloud Connector™ソフトウェアをダウンロードし、ドメイン内のサーバーにインストールすることで、Active Directoryドメインを追加できます。
- **ライセンス: ライセンス**コンソールページの**クラウドサービス**タブと**ライセンス済み展開**タブへのアクセスを許可します。(読み取り専用のみ)
- **通知: 通知**コンソールページへのアクセスを許可します。管理者はCitrix Cloudの通知を表示および却下できます。
- **リソースの場所: リソースの場所**コンソールページへのアクセスを許可します。管理者は新しいリソースの場所を追加したり、シングルサインオン用のFASサーバーを追加したりできます。また、コネクタの更新を管理することもできます。
- **サポートチケット: サポートチケット**コンソールメニューオプションと**チケットを開く**ヘルプメニューオプションへのアクセスを許可します。これらのオプションのいずれかを選択すると、管理者はマイサポートポータルに移動します。詳細については、テクニカルサポートを参照してください。(フルアクセスのみ)
- **システムログ: システムログ**コンソールページへのアクセスを許可します。管理者はシステムログイベントを表示し、イベントをCSVファイルにエクスポートできます。(読み取り専用のみ)
- **StoreFront Cloud: StoreFront Cloud**コンソールページへのアクセスを許可します。管理者は、認証方法の変更、ストアの外観と動作のカスタマイズ、サービスの有効化と無効化、サイト集約の構成を行うことができます。詳細については、Citrix® StoreFront Cloud製品ドキュメントを参照してください。(フルアクセスのみ)
- **ストアOAuthクライアント (プレビュー): IDおよびアクセス管理 > APIアクセス > ストアAPI**タブへのアクセスを許可します。管理者は、StoreFront CloudプラットフォームAPIと連携するために独自のOAuthクライアントを作成および管理できます。OAuthクライアントはストアAPI専用に使用され、自動的に期限切れになるプライベートクライアントを作成するオプションが含まれています。

> **注:**

「**Store OAuth clients**」カスタムロールは慎重に割り当てることをお勧めします。このロールに関連付けられたアクセス権限により、管理者はストアプラットフォーム上のエンドユーザーのリソース（VDAまたはアプリケーション）にアクセスできる可能性があります。また、**フルアクセス**権限を持つ管理者は、「**Store OAuth clients**」権限を持つ管理者と同等のアクセス権限を自動的に持つことにも注意が必要です。

プライマリMFAメソッドを管理する

多要素認証（MFA）を使用してCitrix Cloudにサインインするには、認証アプリを使用するか、メールアドレスを使用できます。このセクションでは、MFAのデバイス登録を変更する方法、または別のMFAメソッドに切り替える方法について説明します。

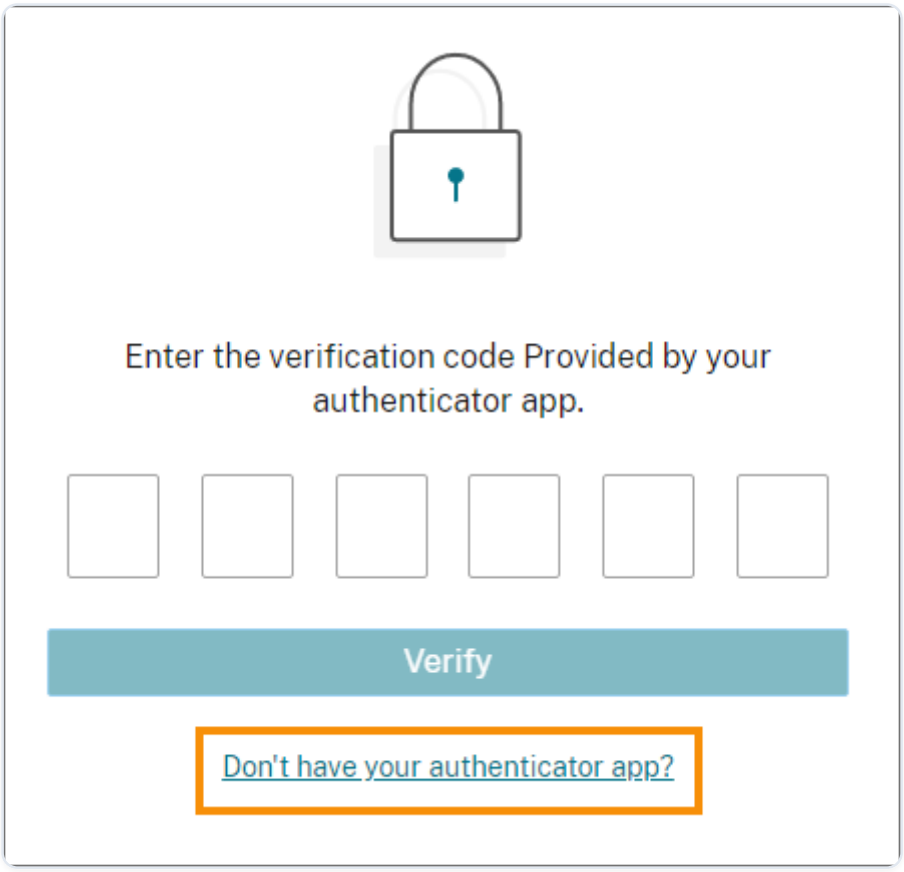
MFAのデバイスを変更する

登録済みのデバイスを紛失した場合、Citrix Cloudで別のデバイスを使用したい場合、または認証アプリをリセットした場合は、Citrix Cloud MFAに再登録できます。

注

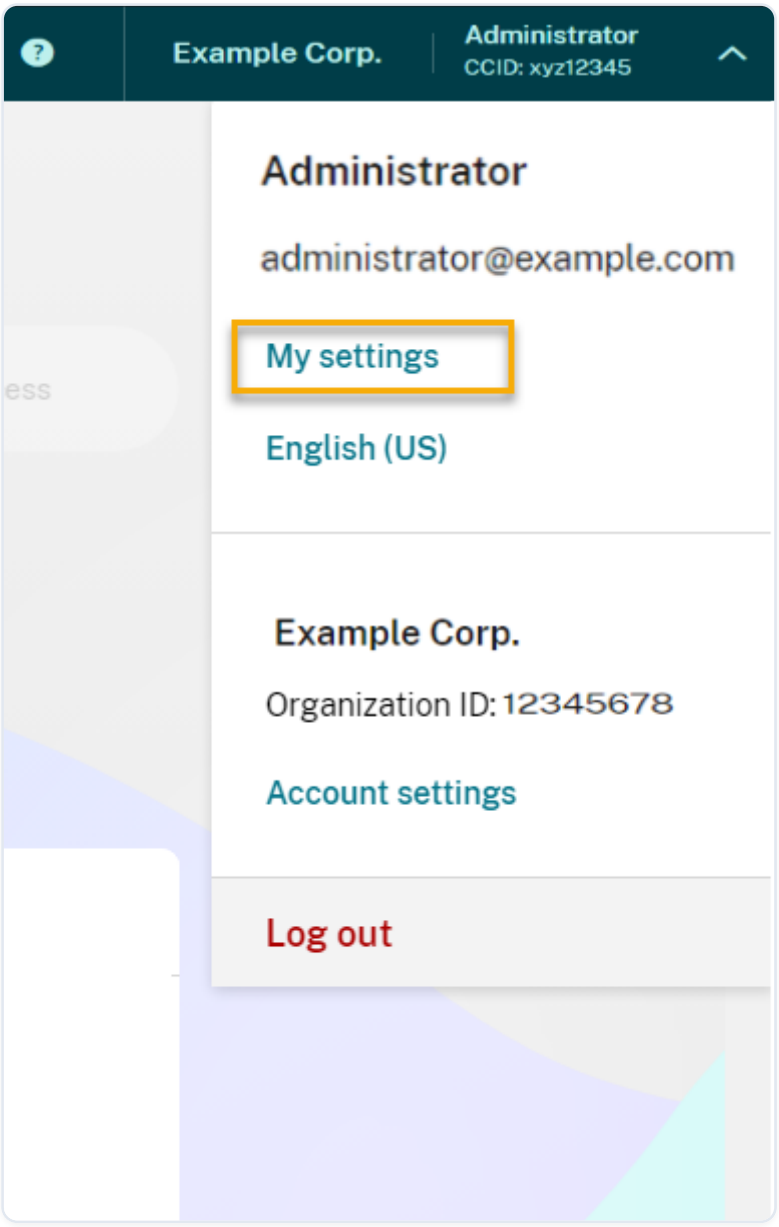
- デバイスを変更すると、現在のデバイス登録が削除され、新しい認証アプリキーが生成されます。
- 元の登録と同じ認証アプリで再登録する場合、再登録する前に認証アプリからCitrix Cloudのエントリを削除してください。このエントリに表示されるコードは、再登録完了後は機能しなくなります。再登録の前後にこのエントリを削除しない場合、認証アプリに異なるコードを持つ2つのCitrix Cloudエントリが表示され、Citrix Cloudへのサインイン時に混乱を招く可能性があります。
- 新しいデバイスで再登録し、認証アプリをお持ちでない場合、デバイスのアプリストアからダウンロードしてインストールしてください。よりスムーズなエクスペリエンスのために、Citrixはデバイスを再登録する前に認証アプリをインストールすることをお勧めします。

1. Citrix Cloudにサインインし、認証アプリのコードを入力します。



認証アプリをお持ちでない場合、**認証アプリをお持ちでない場合**をクリックし、サインインに役立つ回復方法を選択します。選択した回復方法に応じて、受け取った回復コードまたは未使用のバックアップコードを入力し、**確認**を選択します。

2. 複数の顧客組織の管理者である場合、任意の顧客組織を選択します。
3. 右上隅のメニューから、**マイ設定**を選択します。



4. 「**認証アプリ**」で、「**新しいデバイスを追加**」を選択します。

   「デバイスの変更」が強調表示されたログインセキュリティセクション(/en-us/citrix-cloud/media/admin-mfa-change-device-link.png)

5. デバイスの変更を確認するよう求められたら、「**はい、デバイスを変更します**」を選択します。
6. 認証アプリから確認コードを入力して、本人確認を行います。認証アプリをお持ちでない場合は、「**リカバリ方法を使用**」を選択して、選択したリカバリ方法で本人確認を行います。選択したリカバリ方法に応じて、受信した確認コードまたはリカバリコード、あるいは未使用のバックアップコードを入力します。「**確認して続行**」を選択します。
7. 最初に登録したデバイスと元の認証アプリを使用している場合は、認証アプリから既存のCitrix Cloudエントリを削除します。

8. 新しいデバイスを登録していて、認証アプリをお持ちでない場合は、デバイスのアプリストアからダウンロードしてください。
9. 認証アプリから、デバイスでQRコードをスキャンするか、キーを手動で入力します。
10. 認証アプリから6桁の確認コードを入力し、「**コードを確認**」を選択します。

デバイスを変更した後、Citrixは、マイプロファイルページの検証方法が最新であることを強く推奨します。

MFA方法を変更する

認証アプリを使用してMFAに登録し、メールアドレスの使用に切り替えたい場合は、認証方法を変更するとデバイスの登録が削除されることに注意してください。MFAに認証アプリを再度使用したい場合は、デバイスを再登録する必要があります。

1. Citrix Cloudコンソールの右上メニューから、「**マイ設定**」を選択します。
2. 「**多要素認証 (MFA)**」で、切り替えたい認証方法を選択します。
3. メールMFAに切り替える場合:
    a. MFA方法を変更することを確認するには、「**はい、メールに変更します**」を選択します。
    b. 認証アプリのコードを入力するか、復旧方法を使用して本人確認を行ってください。
    c. 変更を完了するには、**Verify and continue** を選択します。
4. 認証アプリに切り替える場合:
    a. プロンプトが表示されたら、Citrix Cloud からメールアドレスに送信された確認コードを入力し、**Verify and continue** を選択します。または、復旧方法を使用して本人確認を行ってください。
    b. 認証アプリを使用して、デバイスのカメラで QR コードをスキャンするか、英数字キーを入力します。
    c. **Verify your authenticator app** で、認証アプリの6桁のコードを入力します。
    d. **Verify code** をクリックして、デバイスの登録を完了します。

MFA復旧方法を管理する

> **重要:**

> Citrix Cloud アカウントのセキュリティを確保するため、確認方法を正確な情報で最新の状態に保ってください。認証アプリまたは MFA メールアドレスへのアクセスを失った場合、これらの確認方法がアカウントへのアクセスを回復する唯一の方法となります。

> My Profile コンソールの検証方法セクション(/en-us/citrix-cloud/media/console-admin-mfa-verification-methods-section.png)

復旧用メールアドレスの追加または変更

1. 右上隅のメニューから、**My settings** を選択します。
2. **Recovery methods** の **Recovery email** で、復旧用メールアドレスをまだ追加していない場合は **Add recovery email** を選択します。すでに復旧用メールアドレスを追加している場合は、**Change recovery email** を選択します。
3. プロンプトが表示されたら、認証アプリの確認コードまたはメールアドレスに送信されたコードを入力します。
4. 使用したい新しいメールアドレスを入力し、**確認メールを送信**を選択します。このメールアドレスは、Citrix Cloudアカウントで使用しているメールアドレスとは異なる必要があります。Citrix Cloudは、入力したメールアドレスに確認メールを送信します。
5. 確認メールに記載されているコードを入力し、**コードを確認して完了**をクリックします。

新しいバックアップコードを生成する

いつでも新しいバックアップコードを生成できます。バックアップコードを使用すると、Citrix Cloudは使用されたコードの数を「マイプロファイル」ページに記録します。

新しいバックアップコードを生成したら、必ず安全な場所に保管してください。

1. 右上隅のメニューから、**マイ設定**を選択します。
2. **回復方法**の下の**バックアップコード**で、以前にバックアップコードを生成していない場合は**新しいバックアップコードを生成**を選択します。以前にバックアップコードを生成している場合は、**バックアップコードを置き換える**を選択します。
3. バックアップコードの置き換えを求められたら、**はい、コードを置き換えます**を選択します。
4. 認証アプリからの確認コード、またはメールアドレスに送信されたコードを入力して、本人確認を行います。
5. **確認して続行**を選択します。Citrix Cloudは新しいバックアップコードのセットを生成して表示します。

6. 新しいコードをテキストファイルとしてダウンロードするには、**コードをダウンロード**を選択します。次に、**バックアップコードを保存しました**を選択します。
7. バックアップコードの置き換えを完了するには、**バックアップコードを保存しました**を選択します。

回復用電話番号を変更する

1. 右上隅のメニューから、**マイ設定**を選択します。
2. **回復方法**の下の**回復用電話番号**で、**回復用電話番号を変更**を選択します。
3. 認証アプリからの確認コード、またはメールアドレスに送信されたコードを入力します。「**確認して続行**」を選択します。
4. 使用する新しい電話番号を入力します。次に、確認のためにもう一度電話番号を入力します。
5. 「**リカバリ用電話番号を保存**」を選択します。

> **注：**
>
> Citrix Endpoint Management™ (CEM) 管理者の権限は、管理者が管理者招待を承諾し、CEM タイルで **管理** をクリックした後にのみ変更できます。すべての Citrix Cloud 管理者と同様に、CEM 管理者はデフォルトでフルアクセス権を持っています。

管理者グループを管理する

Active Directory、Microsoft Entra ID (ME-ID)、またはGoogle Cloud Identityのグループを使用して、Citrix Cloud™アカウントに管理者を追加できます。その後、グループ内のすべての管理者のサービスアクセス権限を管理できます。

ADの前提条件

Citrix CloudはSAML 2.0を介したADグループ認証をサポートしています。AD管理者グループのメンバーをCitrix Cloudに追加する前に、Citrix CloudとSAMLプロバイダー間の接続を構成する必要があります。詳細については、「SAMLをCitrix CloudのIDプロバイダーとして接続する」を参照してください。

Citrix CloudにSAML接続がすでにある場合は、AD管理者グループを追加する前に、SAMLプロバイダーをCitrix Cloudに再接続する必要があります。SAMLを再接続しないと、AD管理者グループの追加が失敗する可能性があります。詳細については、「管理者認証に既存のSAML接続を使用する」を参照してください。

Microsoft Entra IDの前提条件

Microsoft Entra IDグループ認証を使用するには、Microsoft Entra IDをCitrix Cloudに接続するためのMicrosoft Entra IDアプリケーションの最新バージョンが必要です。Citrix Cloudは、Microsoft Entra IDを初めて接続したときにこのアプリケーションを取得しました。2019年5月より前にMicrosoft Entra IDをCitrix Cloudに接続した場合、Citrix CloudはMicrosoft Entra IDへの接続に最新のアプリケーションを使用していない可能性があります。アカウントが最新のアプリケーションを使用していない場合、Citrix CloudはMicrosoft Entra IDグループを表示できません。

Citrix CloudでMicrosoft Entra IDグループを使用する前に、次のタスクを実行してください。

1. Microsoft Entra ID接続に最新のアプリケーションを使用していることを確認します。最新のアプリケーションを使用していない場合、Citrix Cloudは通知を表示します。
2. アプリケーションを更新する必要がある場合は、Microsoft Entra IDをCitrix Cloudに再接続します。Microsoft Entra IDに再接続することで、Citrix Cloudにアプリケーションレベルの読み取り専用権限を付与し、Citrix Cloudがユーザーに代わってMicrosoft Entra IDに再接続できるようにします。再接続中に、これらの権限のリストが表示され、確認できます。Citrix Cloudが要求する権限の詳細については、「Citrix CloudのMicrosoft Entra ID権限」を参照してください。

> **重要:**
>
> このタスクを完了するには、Microsoft Entra IDのグローバル管理者である必要があります。また、Citrix IDプロバイダーのフルアクセス管理者アカウントを使用してCitrix Cloudにサインインしている必要があります。Microsoft Entra IDの資格情報でサインインすると、再接続は失敗します。Citrix IDプロバイダーを使用している管理者がいない場合は、このタスクを実行するために一時的に追加し、後で削除できます。

Microsoft Entra IDへの接続を確認するには

1. Citrix IDプロバイダーのフルアクセス管理者アカウントを使用してCitrix Cloudにサインインします。
2. Citrix Cloudメニューから、 を選択し、次に を選択します。
3. 「**Microsoft Entra ID**」を見つけます。Citrix CloudがMicrosoft Entra ID接続用のアプリケーションを更新する必要がある場合、通知が表示されます。

   Citrix CloudコンソールでのMicrosoft Entra IDへの再接続プロンプト(/en-us/citrix-cloud/media/iam-aad-reconnect-message.png)

   Citrix Cloudがすでに最新のアプリケーションを使用している場合、通知は表示されません。

Microsoft Entra IDに再接続するには

1. Citrix CloudコンソールのMicrosoft Entra ID通知から、「**再接続**」リンクをクリックします。要求されたAzure権限のリストが表示されます。
2. 権限を確認し、「**承認**」を選択します。

グーグル クラウド アイデンティティ

Citrix Cloudは、Google Cloud Identityを介した管理者グループ認証をサポートしています。管理者グループをCitrix Cloudに追加する前に、Citrix CloudとGoogle Cloud Identity間の接続を構成する必要があります。詳細については、「Google Cloud IdentityをCitrix CloudのIDプロバイダーとして接続する」を参照してください。

サポートされている権限

サポートされている権限の説明については、こちらを参照してください。「コンソール権限」。

制限事項

通知機能のカスタムアクセス権限は、管理者グループのメンバーには利用できません。

次の画像に示すように、通知連絡先管理の下でグループのメンバーの通知連絡先を追加できます。

Citrix CloudコンソールでのMicrosoft Entra IDへの再接続プロンプト(/en-us/citrix-cloud/media/notifications-contact-settings.png)

Quick Deployユーザー割り当てなど、Citrix Cloudプラットフォームの機能に依存するCitrix DaaS™機能は利用できません。

すでにサインインしている管理者グループメンバーの権限変更は、サインアウトして再度サインインした後にのみ有効になります。

Citrix®、AD、Microsoft Entra ID、およびGoogle CloudのIDを持つ管理者の結果的な権限

管理者がCitrix Cloudにサインインする際、Citrix ID（Citrix CloudのデフォルトのIDプロバイダー）と、AD、Microsoft Entra ID、またはGoogle Cloud Identityを介したシングルユーザーまたはグループベースのIDの両方を持っている場合、特定の権限のみが利用可能になることがあります。このセクションの表は、これらのIDの各組み合わせで利用可能な権限について説明しています。

シングルユーザーID とは、個々のアカウントを通じて管理者に付与されるAD、Microsoft Entra ID、またはGoogle Cloud Identityの権限を指します。*グループベースID* とは、グループのメンバーとして付与されるAD、Microsoft Entra ID、またはGoogle Cloud Identityの権限を指します。

シトリックス ID	シングルユーザーADまたはMICROSOFT ENTRA IDのID	グループベースADまたはMICROSOFT ENTRA IDのID	シングルユーザーまたはグループベースのGOOGLE CLOUD IDENTITY	認証後に利用可能な権限
X	X			管理者は、Citrix ID、AD ID、またはMicrosoft Entra IDのいずれかで認証が成功した後、両方のIDの累積的な権限を持ちます。
X		X		各IDは独立したエンティティとして扱われます。利用可能な権限は、管理者がCitrix IDまたはMicrosoft Entra IDのいずれを使用して認証するかによって異なります。
X			X	各IDは独立したエンティティとして扱われます。利用可能な権限は、管理者がCitrix IDまたはGoogle Cloud Identityのどちらを使用して認

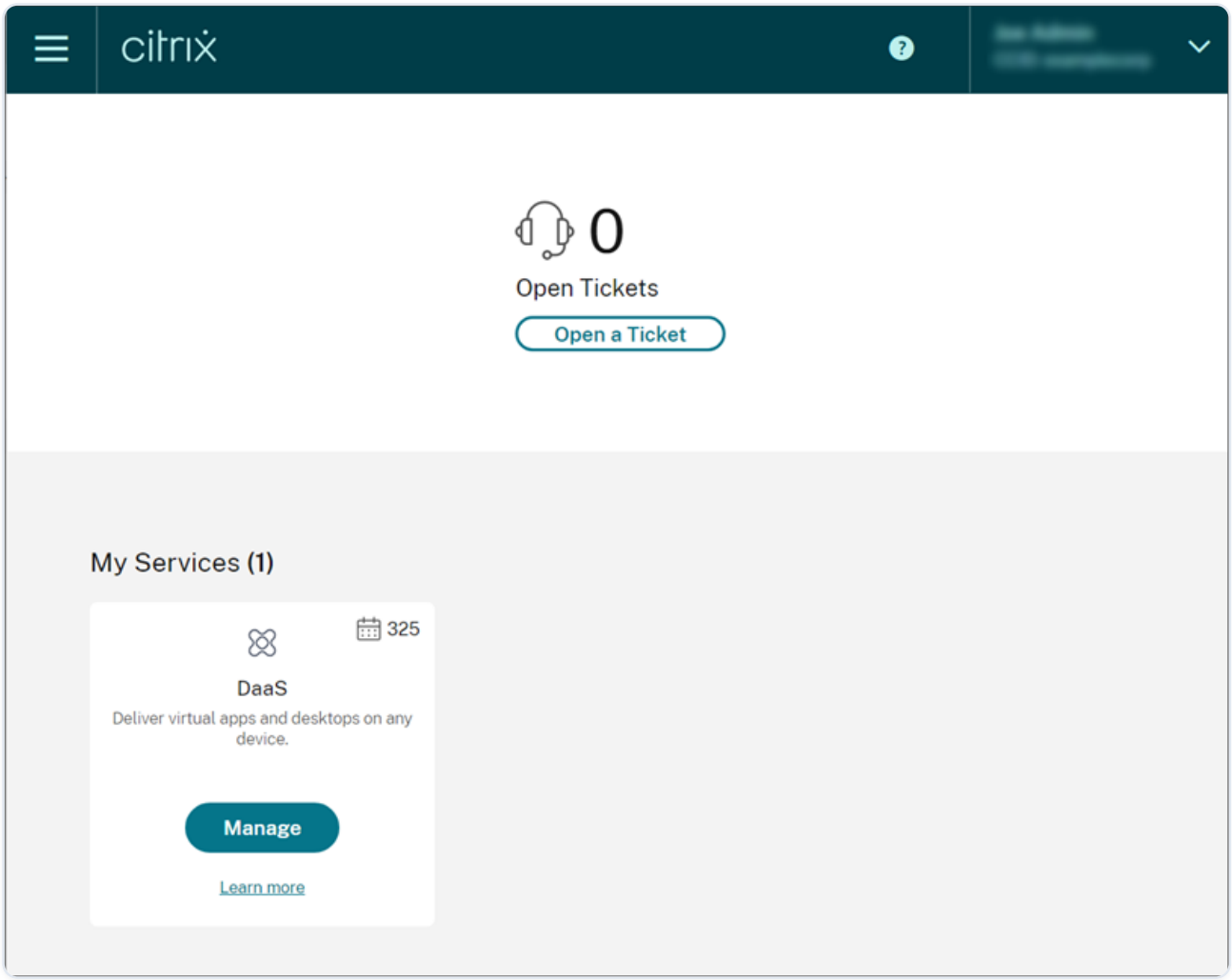
シトリックス ID	シングルユーザーADまたはMICROSOFT ENTRA IDのID	グループベースADまたはMICROSOFT ENTRA IDのID	シングルユーザーまたはグループベースのGOOGLE CLOUD IDENTITY	認証後に利用可能な権限
				証するかによって異なります。
	X	X		管理者は、ADまたはMicrosoft Entra IDでCitrix Cloudに認証する際に、両方のIDの累積的な権限を持ちます。
	X		X	各IDは独立したエンティティとして扱われます。利用可能な権限は、管理者がCitrix IDまたはGoogle Cloud Identityのどちらを使用して認証するかによって異なります。
		X	X	各IDは独立したエンティティとして扱われます。利用可能な権限は、管理者がCitrix IDまたはGoogle Cloud Identityのどちらを使用して認証するかによって異なります。

シトリックス ID	シングルユーザーADまたはMICROSOFT ENTRA IDのID	グループベースADまたはMICROSOFT ENTRA IDのID	シングルユーザーまたはグループベースのGOOGLE CLOUD IDENTITY	認証後に利用可能な権限
X	X	X		Citrix IDで認証する場合、管理者はCitrix IDとシングルユーザーのMicrosoft Entra IDの両方の累積的な権限を持ちます。Microsoft Entra IDで認証する場合、管理者は3つのIDすべての累積的な権限を持ちます。

管理者向けのサインインエクスペリエンス

Citrix Cloudにグループを追加し、サービス権限を定義すると、グループ内の管理者はCitrix Cloudサインインページで**会社の資格情報でサインイン**を選択し、アカウントのサインインURL（例: `https://citrix.cloud.com/go/mycompany`）を入力するだけでサインインできます。個々の管理者を追加する場合とは異なり、グループ内の管理者は明示的に招待されないため、Citrix Cloud管理者になるための招待を承諾するメールは届きません。

サインイン後、管理者はサービスタイルから**管理**を選択して、サービスの管理コンソールにアクセスします。



グループのメンバーとしてのみ権限を付与された管理者は、Citrix Cloudアカウントのサインイン URLを使用してCitrix Cloudアカウントにアクセスできます。

個別のアカウントを通じて、およびグループのメンバーとして権限を付与された管理者は、アクセスしたいCitrix Cloudアカウントを選択できます。管理者が複数のCitrix Cloudアカウントのメンバーである場合、認証に成功した後、顧客ピッカーからCitrix Cloudアカウントを選択できます。

既知の問題

Active Directoryでグループの名前を変更した後、新しい名前が表示されない場合があります。回避策として、**Citrix Identity and Access Management**で古いグループを削除し、名前が変更されたグループを追加します。

制限事項

複数のグループがアプリケーションパフォーマンスに与える影響

Citrixは、1人の管理者がCitrix Cloudに追加された20を超えるグループに属さないことを推奨しています。より多くのグループに属している場合、アプリケーションパフォーマンスの低下につながる可能性があります。

複数のグループが認証に与える影響

グループベースの管理者がADまたはMicrosoft Entra IDの複数のグループに割り当てられている場合、グループ数が多すぎるため認証が失敗する可能性があります。この問題は、Citrix CloudのADおよびMicrosoft Entra IDとの統合における制限が原因で発生します。管理者がサインインしようとすると、Citrix Cloudは取得されるグループ数を圧縮しようとします。Citrix Cloudが圧縮を正常に適用できない場合、すべてのグループを取得できず、認証が失敗します。

この問題は、ADまたはMicrosoft Entra IDを介してクラウドストアに認証するユーザーにも影響を与える可能性があります。ユーザーが複数のグループに属している場合、グループ数が多すぎるため、認証が失敗する可能性があります。

この問題を解決するには、管理者またはユーザーアカウントを確認し、組織内での役割に必要なグループにのみ属していることを確認してください。

割り当てられた役割/スコープのペアが多すぎるため、グループの追加に失敗する

複数の役割/スコープのペアを持つグループを追加すると、グループを作成できないことを示すエラーが発生する場合があります。このエラーは、グループに割り当てられている役割/スコープのペアの数が多すぎるために発生します。このエラーを解決するには、役割/スコープのペアを2つ以上のグループに分割し、管理者をそれらのグループに割り当てます。

Citrix Cloudに管理者グループを追加する

1. Citrix Cloudメニューから、 を選択し、次に を選択します。
2. を選択します。
3. で、使用するIDプロバイダーを選択します。Microsoft Entra IDが選択されている場合は、必要に応じてAzureにサインインします。 を選択します。
4. 必要に応じて、使用するドメインを選択します。
5. 追加するグループを検索し、そのグループを選択します。
6. で、グループに割り当てる役割を選択します。少なくとも1つの役割を選択する必要があります。
7. 完了したら、 を選択します。

管理者グループのサービス権限を変更する

1. Citrix Cloudメニューから、 を選択し、次に を選択します。

2. 管理する管理者グループを見つけ、省略記号メニューから を選択します。



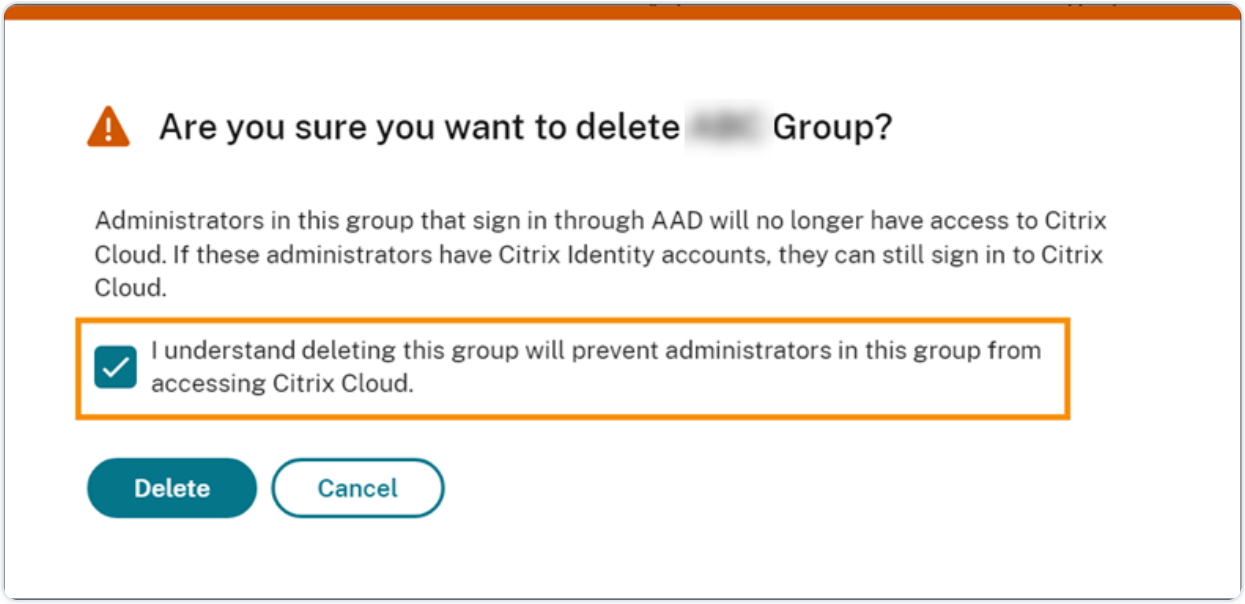
3. 必要に応じて、1つ以上の役割とスコープのペアの横にあるチェックマークをオンまたはオフにします。
4. 完了したら、 を選択します。

管理者グループを削除する

1. Citrix Cloudメニューから、 を選択し、次に を選択します。
2. 管理する管理者グループを見つけて、省略記号メニューから を選択します。



確認メッセージが表示されます。



3. グループの削除による影響を認識していることを確認するために、 を選択します。
4. を選択します。

複数のCitrix Cloudアカウントを切り替える

> **注：**

> このセクションでは、Microsoft Entra ID管理者グループのメンバーのみに影響するシナリオについて説明します。

> デフォルトでは、Microsoft Entra ID管理者グループのメンバーは、アクセスできる他のCitrix Cloudアカウントを切り替えることができません。これらの管理者には、以下の画像に示すオプションがCitrix Cloudユーザーメニューに表示されません。



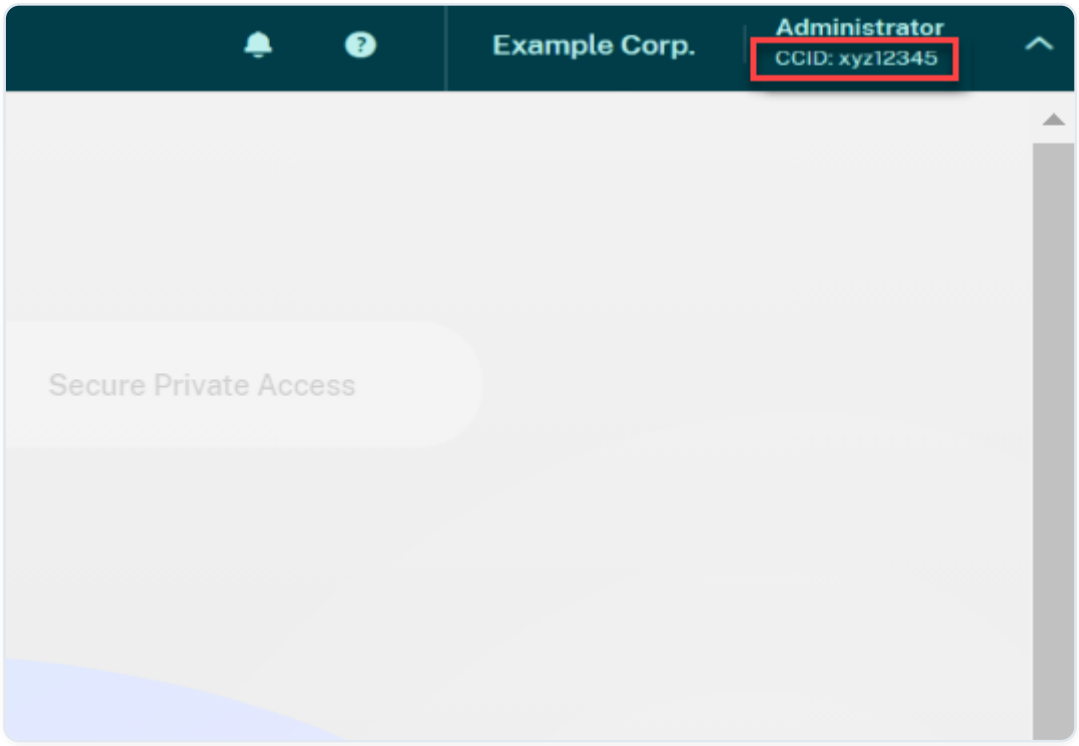
このメニューオプションを有効にし、Microsoft Entra IDグループメンバーが他のCitrix Cloudアカウントを切り替えられるようにするには、切り替えたいアカウントをリンクする必要があります。

Citrix Cloudアカウントのリンクには、ハブアンドスポークアプローチが関係します。アカウントをリンクする前に、他のアカウントがアクセスされる元となるアカウント（「ハブ」）として機能するCitrix Cloudアカウントと、顧客ピッカーに表示させたいアカウント（「スポーク」）を決定します。

アカウントをリンクする前に、以下の要件を満たしていることを確認してください。

- Citrix Cloud で完全なアクセス許可を持っていること。
- Windows PowerShell Integrated Scripting Environment (ISE) へのアクセス権を持っていること。

- リンクしたいCitrix Cloudアカウントの顧客IDを持っていること。顧客IDは、各アカウントの管理コンソールの右上隅に表示されます。



- ハブアカウントとしてリンクする Citrix Cloud アカウントの Citrix CWSAuth ベアラートークンを持っていること。このベアラートークンを取得するには、CTX330675 の手順に従ってください。Citrix Cloud アカウントをリンクする際に、この情報を提供する必要があります。

Citrix Cloud アカウントをリンクするには

1. PowerShell ISE を開き、次のスクリプトを作業ペインに貼り付けます。

```
$headers = @{}

$headers.Add("Accept","application/json")

$headers.Add("Content-Type","application/json")

$headers.Add("Authorization","CWSAuth bearer=XXXXXXX")



$uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"



$resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
```

```
$allLinks = $resp.linkedCustomers + @("SpokeCustomerID")



$body = @{"customers"=$allLinks}

$bodyjson = $body | ConvertTo-Json



$resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
-Body $bodyjson -ContentType 'application/json'

Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
```

2. 4 行目で、`CWSAuth bearer=XXXXXXX` を CWSAuth の値 (例: `CWSAuth bearer=AbCdef123Ghik…`) に置き換えます。この値は、証明書キーに似た長いハッシュです。
3. 6 行目で、`HubCustomerID` をハブアカウントの顧客 ID に置き換えます。
4. 9 行目で、`SpokeCustomerID` をスポークアカウントの顧客 ID に置き換えます。
5. スクリプトを実行します。
6. 手順 3〜5 を繰り返し、追加のアカウントをスポークとしてリンクします。

Citrix Cloud アカウントのリンクを解除するには

1. PowerShell ISE を開きます。PowerShell ISE がすでに開いている場合は、作業ペインをクリアします。
2. 次のスクリプトを作業ペインに貼り付けます。

```
$headers = @{}

$headers.Add("Accept","application/json")

$headers.Add("Content-Type","application/json")

$headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
```

```
$uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
SpokeCustomerID"



$resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers $headers

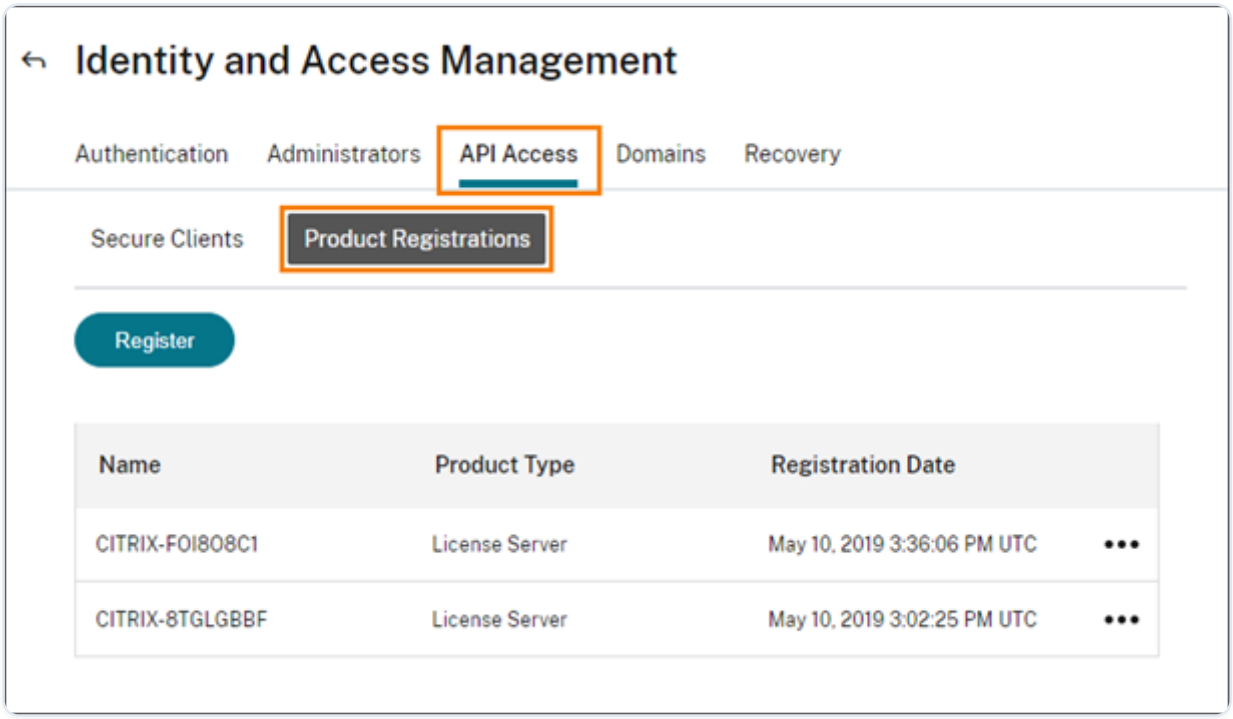
Write-Host "Response: $($resp.RawContent)"
```

3. 4 行目で、`CWSAuth bearer=xxxxxxx1` を CWSAuth の値 (例: `CWSAuth bearer=AbCdef123Ghik…`) に置き換えます。この値は、証明書キーに似た長いハッシュです。
4. 6行目で、`HubCustomerID` をハブアカウントの顧客IDに置き換えます。
5. 6行目で、`SpokeCustomerID` をスポークアカウントの顧客IDに置き換えます。
6. スクリプトを実行します。
7. 追加のアカウントのリンクを解除するには、手順4～6を繰り返します。

オンプレミス製品を Citrix Cloud™ に登録する

Citrix Cloud を介したショートコードアクティベーションを使用して、オンプレミスの Citrix 製品を簡単に登録できます。製品によっては、この8桁のコードは製品のインストールプロセス中、または製品の管理コンソールを実行したときに生成される場合があります。製品が登録を促すと、製品は Citrix Cloud からコードを要求し、それを表示します。その後、このコードをコピーして貼り付けるか、Citrix Cloud に手動で入力できます。

登録後、製品登録ページ（**ID およびアクセス管理 > API アクセス > 製品登録**）に、登録済みの製品が配置されているサーバーが表示されます。



Citrix Cloud に登録できるオンプレミス製品は次のとおりです。

- クラウドサービス用 Citrix Connector™ Appliance
- Citrix Federated Authentication Service（Citrixフェデレーション認証サービス）
- Citrix License Server（Citrixライセンスサーバー）
- Citrix Virtual Apps and Desktops（Citrix Analytics for Performance™ にサイトを登録する場合）

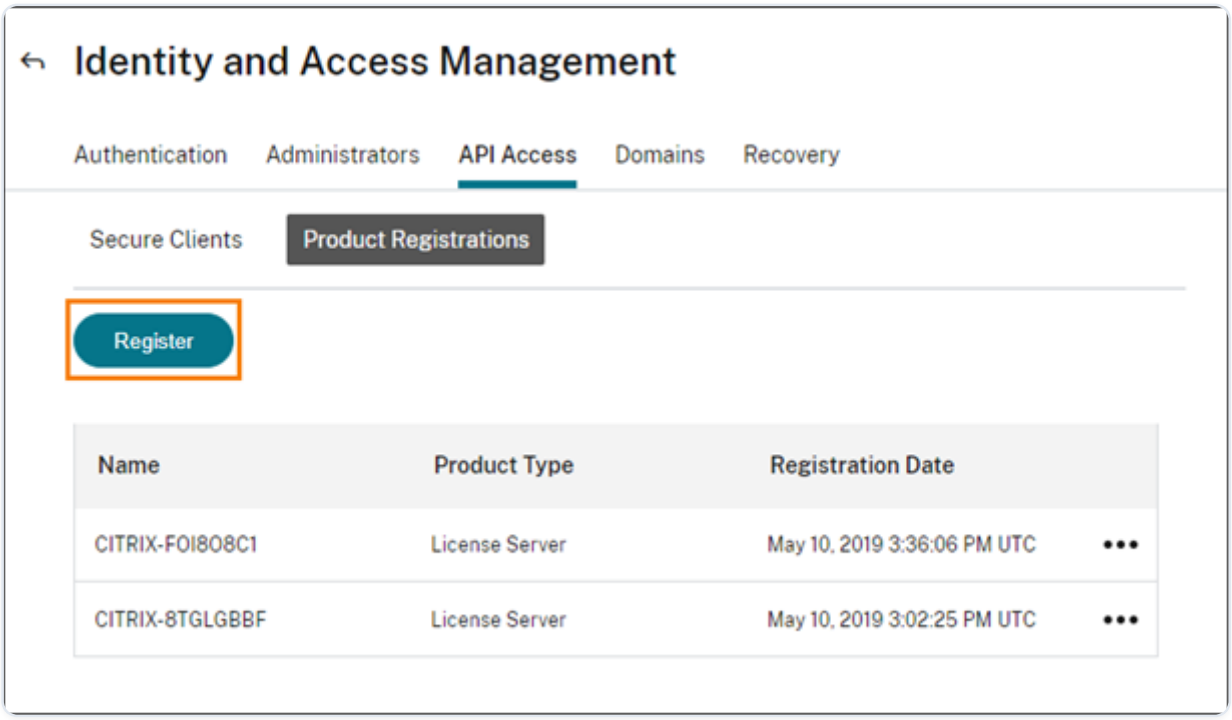
注:

この記事では、オンプレミス製品を Citrix Cloud に登録する手順について説明します。製品固有の要件については、その製品のドキュメントを参照してください。

製品を登録する

1. Citrix Cloud メニューから、**ID およびアクセス管理**を選択します。

2. **API アクセス > 製品登録**を選択し、次に**登録**を選択します。



3. Citrix 製品の8文字の英数字コードを入力し、**続行**をクリックします。
4. 登録の詳細を確認し、**登録**をクリックします。

製品登録を削除する

登録済みのCitrix製品を実行しているサーバーを環境から削除した場合、製品登録ページには引き続きそのサーバーが表示されます。以下の手順でCitrix Cloudからサーバーを削除します。必要に応じて、後で製品を再度登録して、製品登録ページにサーバーを表示させることができます。

1. 製品登録ページから、削除したいサーバーを見つけます。
2. 省略記号ボタンをクリックし、**登録の削除**を選択します。 (/en-us/citrix-cloud/media/prod-reg-remove-registration.png)
3. プロンプトが表示されたら、**削除**を選択します。

条件付き認証

条件付き認証は、ゼロトラストフレームワークをさらに強化するための新しいセキュリティ機能です。条件付き認証により、Citrix Cloud™管理者は、設定したポリシー条件に基づいて、ストアログインフロー中にエンドユーザーを異なるIdPに誘導できます。そのため、エンドユーザーは管理者によって確立されたリスク要因に基づいて、異なるレベルのアクセス検証を受けることになります。

本稿執筆時点では、定義したポリシーに基づいてエンドユーザーを異なるIdPインスタンスに誘導する5つの異なる切り替え条件がサポートされています。

条件付き認証(/en-us/citrix-cloud/media/conditional-authentication.png)

一般的なユースケース

- 合併・買収。大規模な親組織が、合併プロセス中の複数の小規模企業を傘下に持つ場合。
- 組織内の正社員が通常使用を許可されているものとは異なる、専用のIdP、OIDCアプリケーション、またはSAMLアプリケーションに誘導することで、サードパーティユーザーや請負業者にストアアクセスを許可する。
- 複数の支店や部門を持ち、異なる認証メカニズムを必要とする大規模組織。

前提条件

- Citrix Cloud Identity and Access Managementページで作成された2つ以上のIDプロバイダー

マルチIdP

従来、IDタイプの単一インスタンスのみが許可されていました。Citrix Cloud®は現在、同じIDプロバイダータイプの複数のインスタンスの追加をサポートしています。たとえば、それぞれ**異なる**IdPテナントを指す複数のEntraID IdP、Google IdP、またはOkta IdP接続を、IDおよびアクセス管理タブの下に追加できるようになりました。

マルチIdP(/en-us/citrix-cloud/media/mulitiidp-instances.png)

> **重要:**

> DaaSとSPAは現在複数のIdPをサポートしていますが、一部のサービスではこの機能の実装に取り組んでおり、まもなく利用可能になります。

条件付き認証の構成

1. **条件付き認証プロファイルの作成**をクリックします。

   条件付き認証プロファイルの作成(/en-us/citrix-cloud/media/create-conditional-authentication-profile.png)

2. プロファイルの名前を入力し、**認証ポリシーの作成**をクリックします。

   認証ポリシーの作成(/en-us/citrix-cloud/media/create-authentication-policy.png)

3. 必要に応じてポリシーに適用する条件を選択し、**保存**をクリックします。

   認証条件(/en-us/citrix-cloud/media/authentication-conditions.png)

4. **StoreFront Cloud**に移動し、**認証**をクリックして、IDプロバイダーまたは条件付き認証プロファイルを選択します。

   認証(/en-us/citrix-cloud/media/conditional-authentication-policy.png)

条件付き認証の概念

条件付き認証プロファイル

条件付き認証プロファイルは、定義した条件に応じてエンドユーザーがストアに認証する方法を制御する複数の条件付き認証ポリシーで構成されます。このプロファイルにより、ポリシーの優先順位付けと並べ替えが可能になり、ポリシーが評価される順序を指定できます。

条件付き認証ポリシー

条件付き認証ポリシーは、1つ以上の条件で構成されるポリシーです。これらの条件がANDロジックを使用して満たされると、エンドユーザーのログインプロセスは、Okta OIDC、SAML、またはGateway IDP接続などの特定のターゲットIdPインスタンスに誘導されます。個々のポリシーはクローン作成でき、必要に応じて変更および名前変更が可能です。

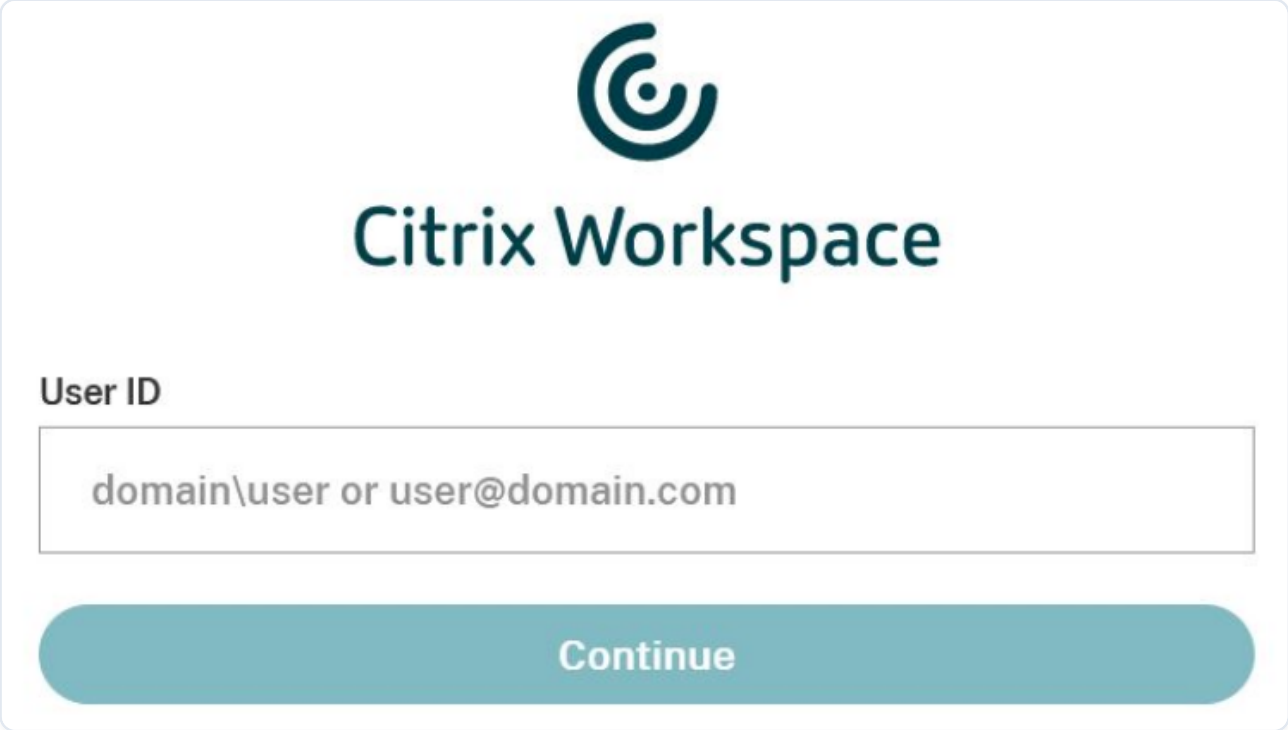
各条件付き認証ポリシーは、次のデータで構成されます。

- **ポリシー規則**。エンドユーザーを特定のIdPインスタンスに誘導するために満たされなければならない1つ以上の条件です。例: ストアURL 1が使用され、かつユーザーがAD Group1のメンバーである場合。
- **ポリシー結果IdP**。ログオンプロセス中にユーザーが誘導されるターゲットIdPインスタンスです。例: `store URL 1 is used AND user is a member of AD Group1 → EntraID SAML IDP Instance`。
- **ポリシー名**。ポリシーを識別し、説明するために使用される、管理者が分かりやすい名前です。 例: `store URL 1 AND Group1 - EntraID SAML`。
- **ポリシー優先度**。ポリシーが評価される順序を決定します。優先度は降順で評価されます。例: 優先度1は優先度2よりも高い。

条件付き認証の事前認証ページ

ストアの設定方法と条件付き認証プロファイルで設定された条件によっては、ストアユーザーはログインプロセス中に事前認証ページに遭遇する可能性があります。このページは、条件付き認証ポリシーに基づいて決定を下すために不可欠な、ストアユーザーのユーザー名形式をキャプチャ

するために重要です。これにより、ユーザーのログインフローが適切なIdPインスタンスに誘導されます。

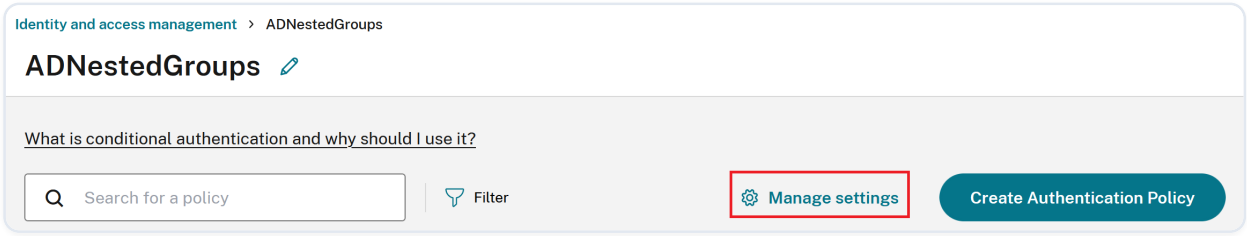


ログイン自動入力

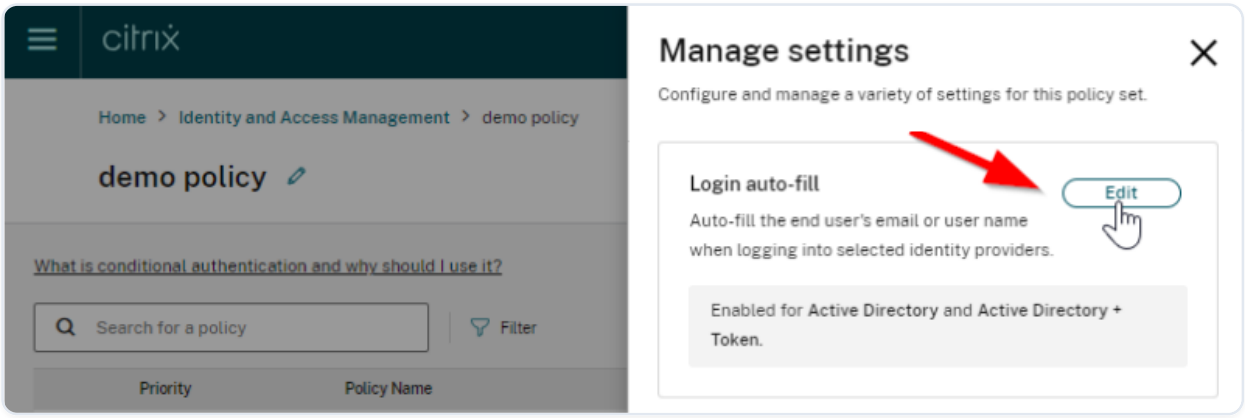
事前認証ページが必要な場合、ログインページでユーザー名フィールドに事前認証ページからのユーザー入力を自動的に入力するログイン自動入力機能を導入しました。これにより、ユーザーがユーザー名を2回入力する必要がなくなります。

ログイン自動入力機能は、以下に示すように、条件付き認証プロファイル設定で管理者によって管理および構成されます。

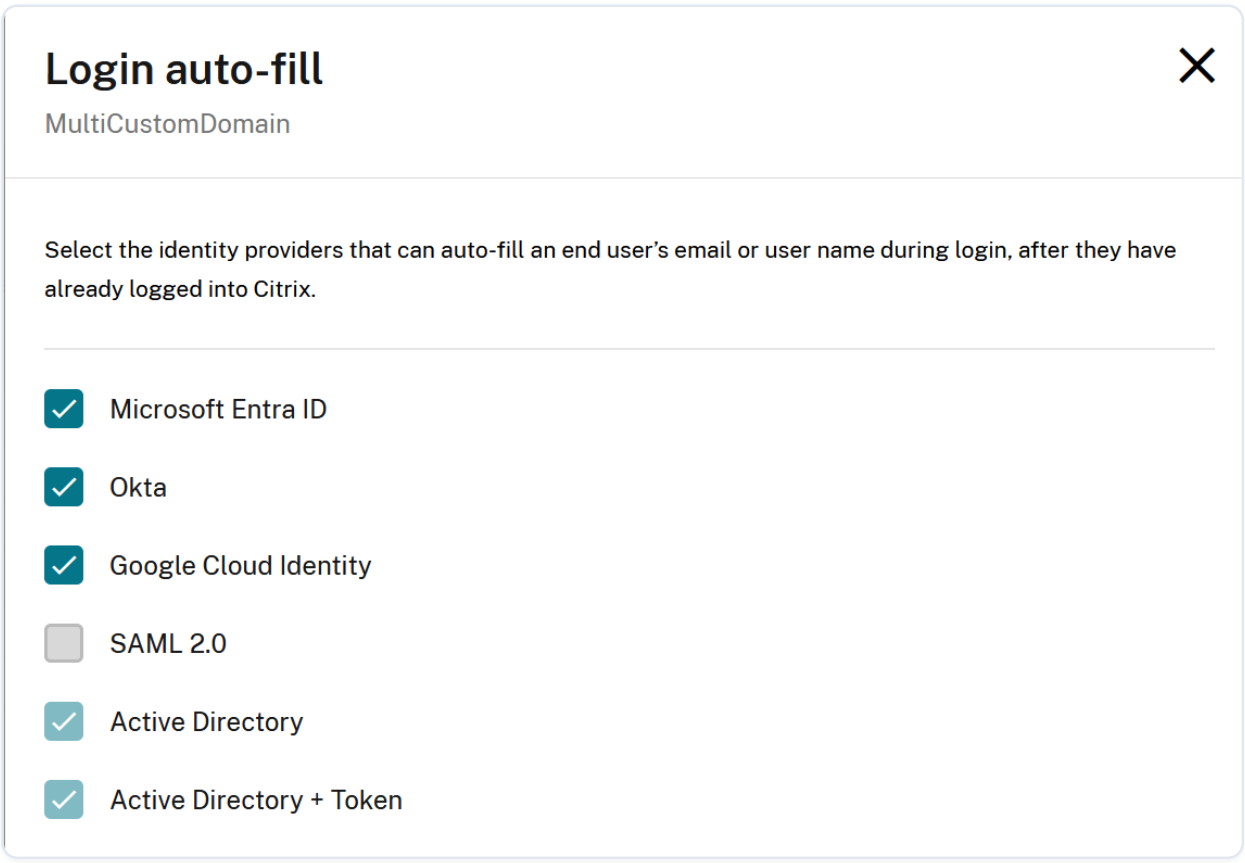
1. 条件付き認証プロファイルページで**設定の管理**をクリックします。



2. **編集**をクリックします



3. ログイン自動入力を有効にしたいIdPを選択します。



重要:

ログインの自動入力は、それをサポートするIdPでのみ利用可能であり、ADおよびAD+TOTPではデフォルトで有効になり、適用されます（デフォルト設定については上記のスクリーンショットを参照してください）。

特定のIdPは特定のログイン形式を期待し、一部のIdPは複数の種類のユーザー名形式をサポートできます。たとえば、Google Cloud Identityでは、ユーザーはメールアドレス（`user.name@domain.com`）でログインする必要がありますが、これはUPN

（`username@domain.com`）とは異なる場合があります。ストアのエンドユーザーが事前認証ページでダウンレベルのログオン名（domain\username）を入力した場合、ダウンレベルのログオン名はIdPログインページのユーザー名フィールドに事前入力され、ユーザーがログオンしようとするとエラーが発生します。管理者は、ログイン自動入力機能を構成する前に、最も適切なIdP切り替えポリシー条件と、特定のIdPがログオンプロセス中に受け取ることを期待するユーザー名形式を考慮する必要があります。

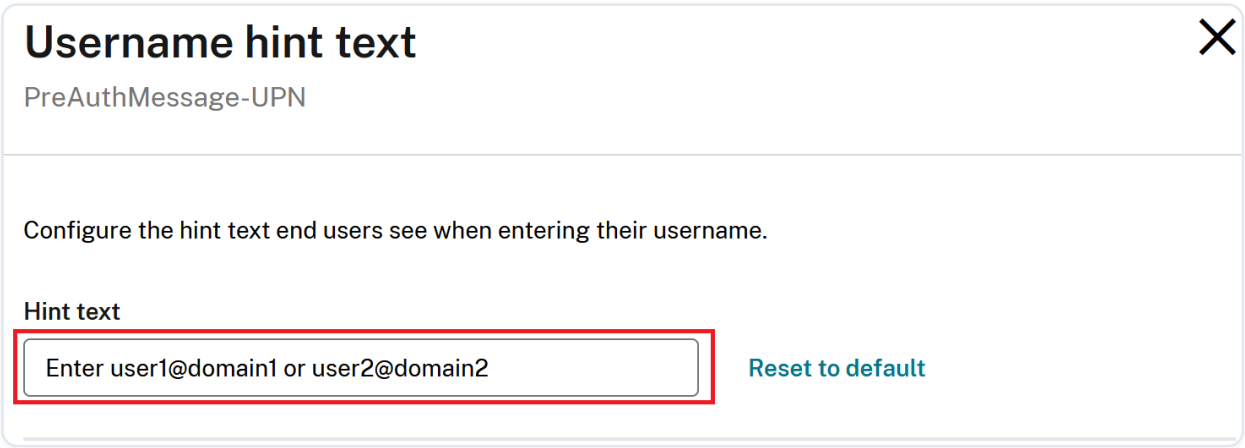
ユーザー名ヒントテキスト

条件付き認証でIDP切り替えの決定を行うために追加のADドメインまたはADグループユーザーコンテキストが必要な場合、ログオンフロー中にエンドユーザーに事前認証ページが表示されます。構成されているCAポリシーのいずれとも一致しない予期しない形式または誤った形式でユーザー名を入力すると、ユーザーはログインできなくなります。エンドユーザーが正しい予期される形式でユーザー名を入力できるように、事前認証ダイアログ内に表示されるユーザー名ヒントテキストをカスタマイズできます。

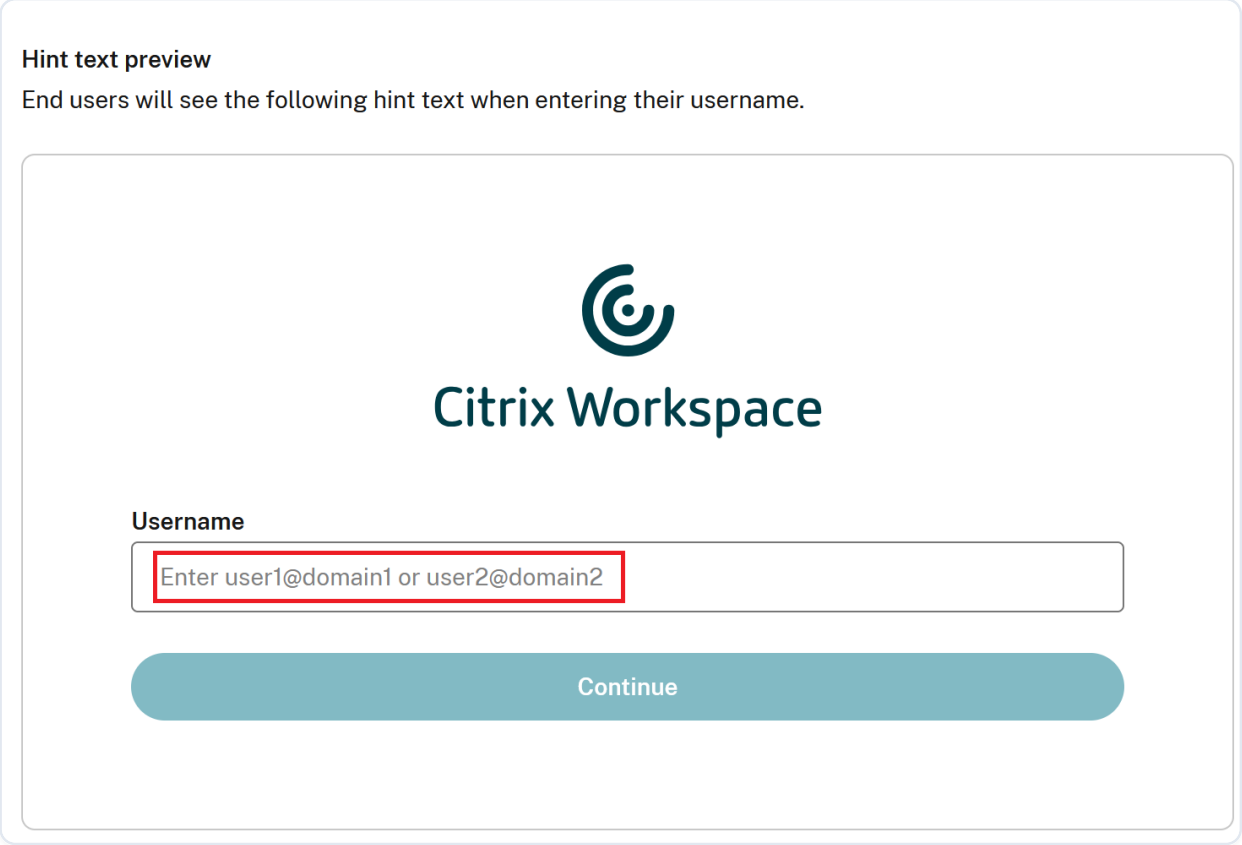
重要:

Citrix環境、ADドメイン、およびユーザーの詳細に関する機密情報を漏洩しないように、ユーザー名ヒントテキスト機能を適切に注意して使用してください。一般的なユーザー名の例を使用することをお勧めします。

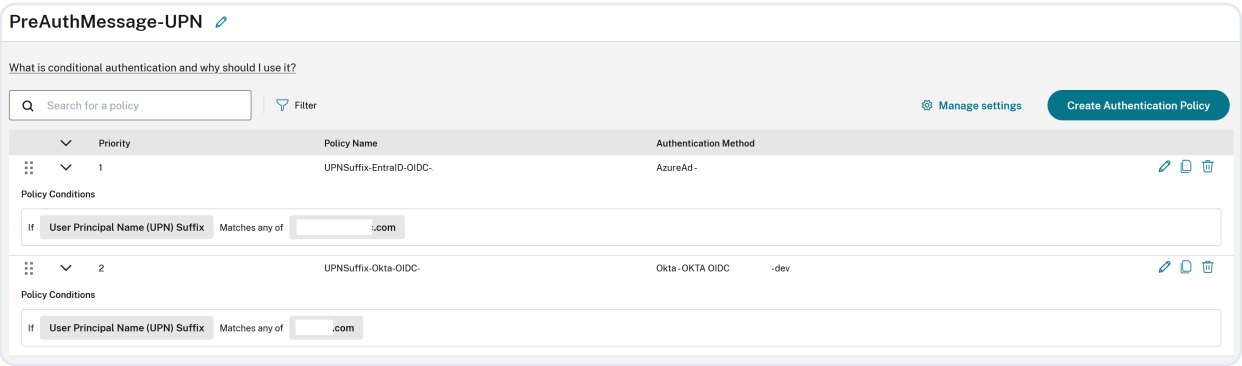
1. 条件付き認証プロファイルページで、 をクリックします。
2. で をクリックします。](/en-us/citrix-cloud/media/username-hint-text-upn-example.png)
3. 条件付き認証ログオンフロー中に事前認証ダイアログ内に表示する **ログオンヒントテキスト** を設定します。



4. プレビュー画像を表示して、ログオンヒントテキストがエンドユーザーにどのように表示されるかを確認します。



上記の例は、異なるIdP間のUPNベースの切り替えに適しています。



5. をクリックします。

ポリシー条件の種類

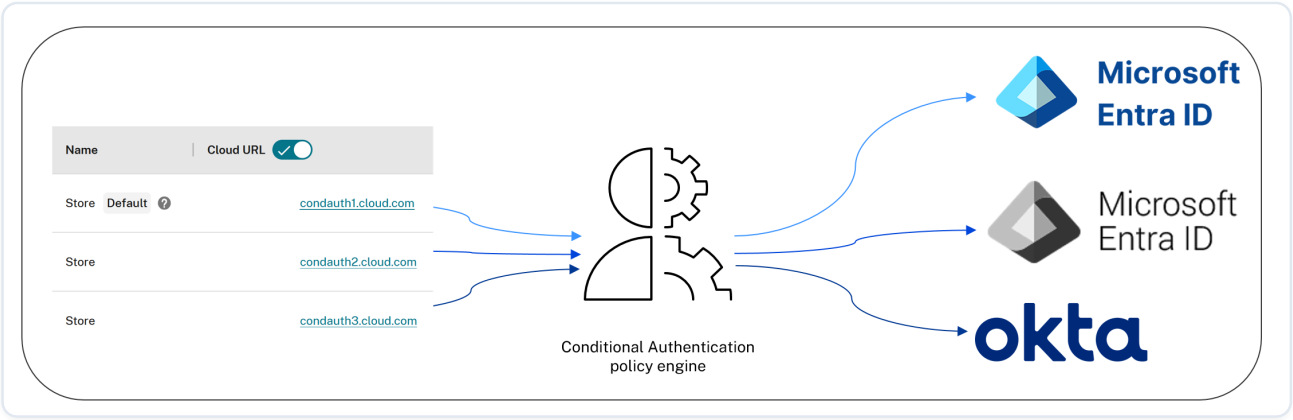
注:

条件付き認証プロファイルにストアURL条件タイプまたはネットワークロケーション名条件タイプのポリシーのみが含まれている場合、事前認証ページは表示されず、ユーザーはIdPに直接リダイレクトされます。プロファイルに他のポリシー条件タイプが含まれている場

> 合、事前認証ページがエンドユーザーに表示されます。これは、一致するポリシーがストアURLまたはネットワークロケーション名タイプである場合でも当てはまります。

ストアURL

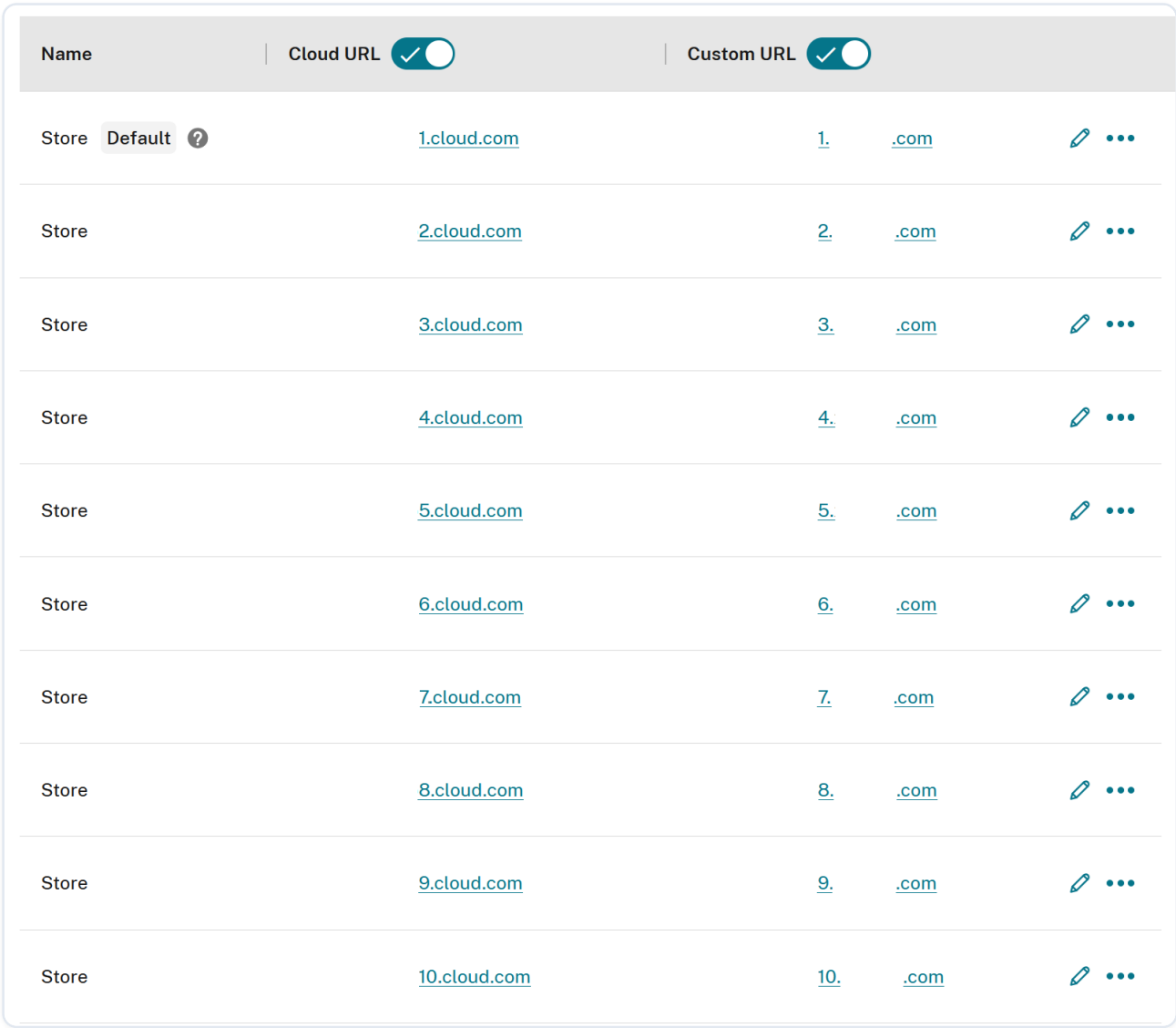
StoreFront Cloud > **アクセス**内で、各ストアURLを個別のIdPインスタンスにリンクできます。さらに、複数のストアURLを同じポリシーに関連付けて、エンドユーザーを同じIdPインスタンスに誘導します。



ストアURLまたはカスタムURLのいずれかを使用したストアへのアクセス

エンドユーザーは、ブラウザに入力するストアURLまたはカスタムURL、あるいはCitrix Workspaceアプリ内で構成するストアに基づいて、異なる結果のIdPに切り替えることができます。

CITRIX CLOUD™



エンドユーザーは、これらのURLのいずれかを使用して、特定の条件付き認証ポリシーの結果のIdPインスタンスに到達できます。Citrix Cloud管理者は、正しいストアURLをエンドユーザーに提供する必要があります。

`https://workspaces1.cloud.com` URL

または、,

`https://workspaces1.mycompany.com` カスタムURL

ドロップダウンリストを使用してURLのペアを選択し、条件付き認証ポリシーを構成します。

- **青色**で表示されるストアURL (例: `https://workspaces1.cloud.com`)
- **赤色**で表示されるカスタムURL (例: `https://workspaces1.mycompany.com`)

URLペアを使用して条件付き認証ポリシーを構成する：

条件付き認証プロファイルカスタムURL(/en-us/citrix-cloud/media/conditional-auth-profile-custom-urls.png)

条件付き認証ポリシーセットの概要(/en-us/citrix-cloud/media/conditional-auth-policy-set-summary.png)

> **重要：**
>
> 移行されていないレガシーカスタムドメインは、条件付き認証を使用してストアにアクセスするために使用できません。エンドユーザーにカスタムURLを提供する前に、これらのレガシーカスタムURLを最初に移行してください。条件付き認証ポリシーがSAML IdPインスタンスに解決される場合、追加の考慮事項もあります。

> SAMLとカスタムURLを使用して条件付き認証を構成する方法の詳細な手順については、カスタムドメインを使用してSAMLでストアにサインインするを参照してください。

ADユーザーグループメンバーシップ

ADユーザーグループメンバーシップを使用すると、グループメンバーシップに基づいて、特定のActive Directoryユーザーグループに IdPインスタンスを割り当てることができます。

UPNサフィックスまたはドメインダウンレベルログオン名は、相互に排他的な2つのポリシー条件です。 これらは、エンドユーザーが事前認証ページに入力する必要があるユーザー名形式を決定します。同じポリシー内でこれら両方の条件を使用することはできません。

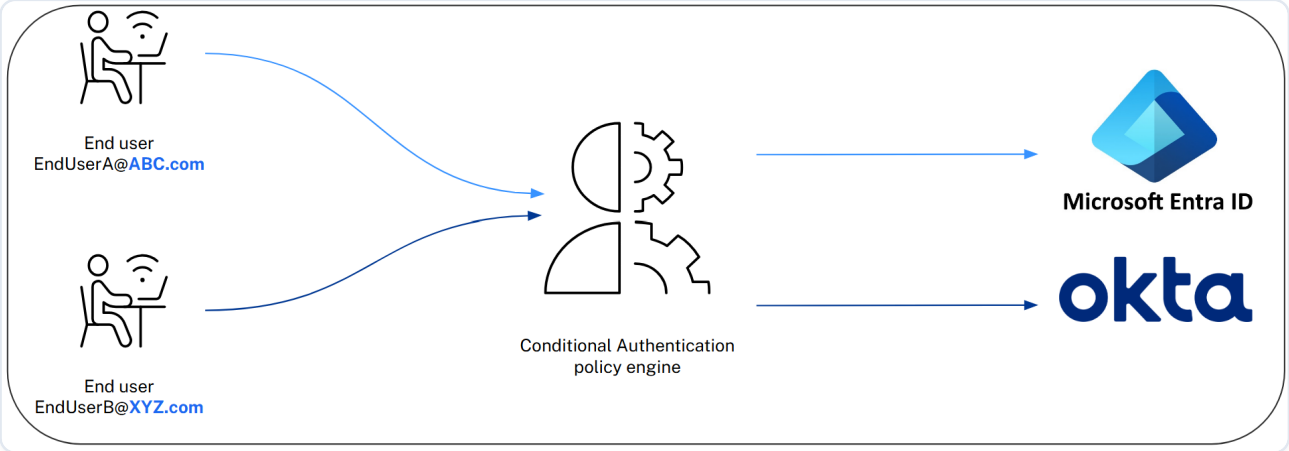
直接ADグループメンバーシップ（推奨）とネストされたADグループメンバーシップの両方がサポートされています。

要件：

- **ユニバーサル**ADグループのみがサポートされています。
- ユーザーがどのADグループのメンバーであるかを確認するために、必要なADフォレスト内でドメイン参加しているCitrix Cloud Connector。
- ADグループ条件の場合、ユーザーがUPNを入力すると、ユーザーのUPNサフィックスによって、ADグループメンバーシップの検索を実行するために使用されるドメインコンテキストが決定されます。

  \> **重要：**

> 一意のUPNサフィックスは、接続されている1つのADフォレストでのみ定義する必要があります。同じCitrix Cloudテナントに接続されている2つ以上のADフォレストで発生するあいまいなUPNサフィックスはサポートされていません。



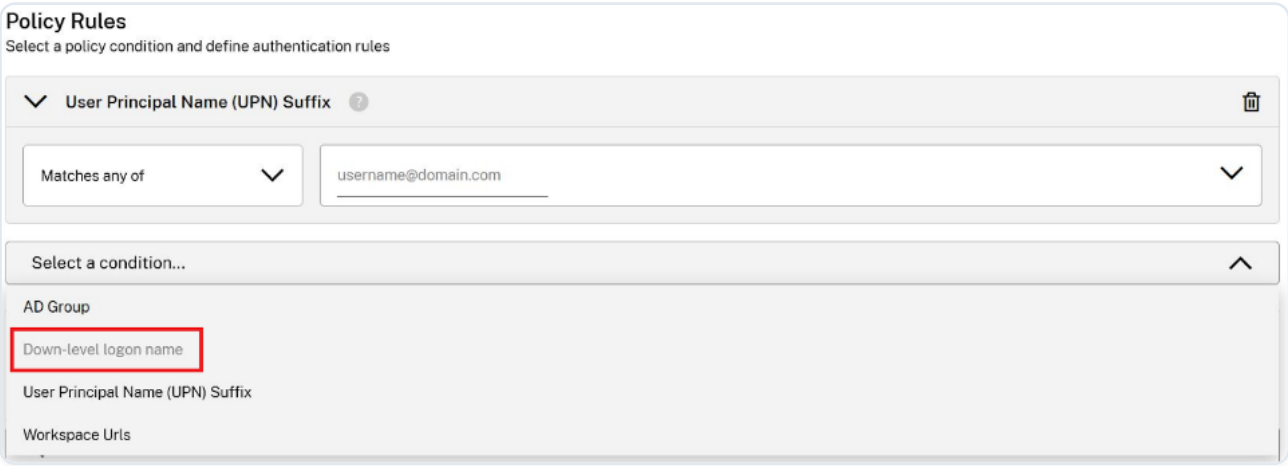
UPNサフィックス

`username1@domain.com`や`username2@domain.net`など、1つ以上のUPNサフィックスに対してIdPインスタンスを構成します。

ドメインダウンレベルログオン名

`DOMAIN1\username1`や`DOMAIN1.COM\username1`のような1つ以上のドメイン名にIdPインスタンスを割り当てます。

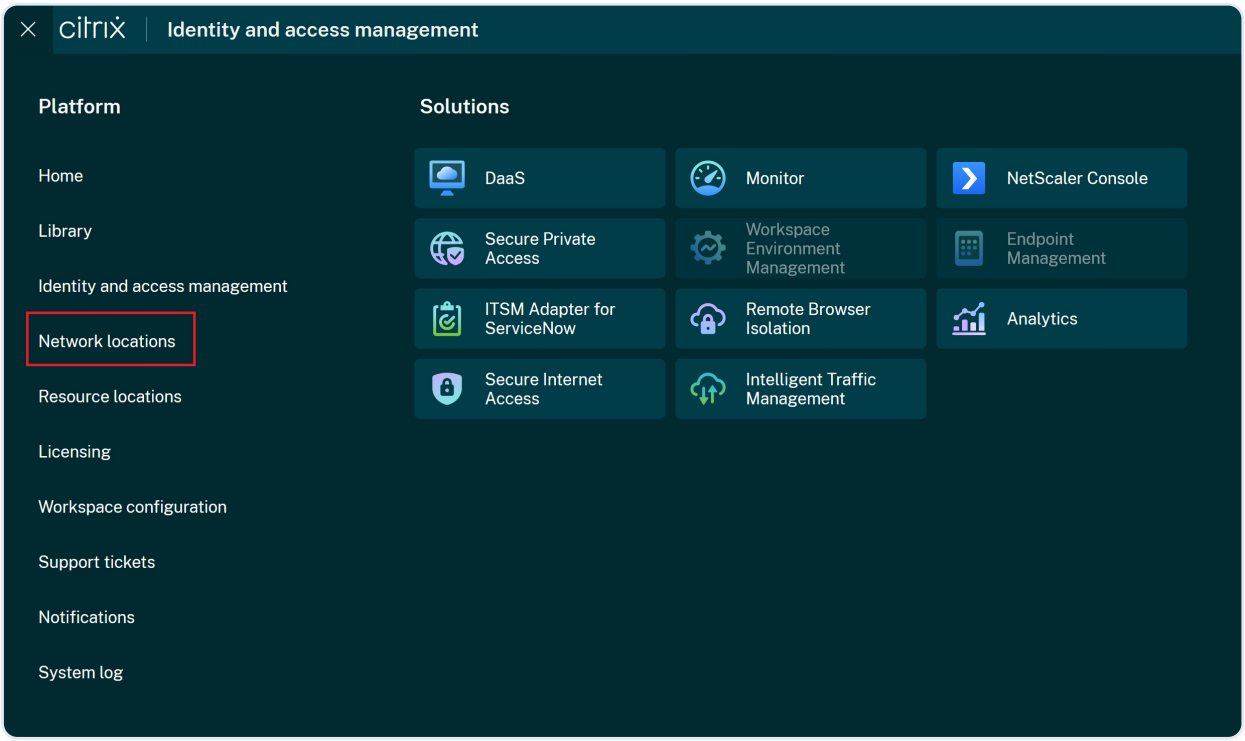
2つの相互排他的な条件のいずれかが選択されている場合、他方の条件のドロップダウンメニューオプションは無効になり、同じポリシーに追加されるのを防ぎます。



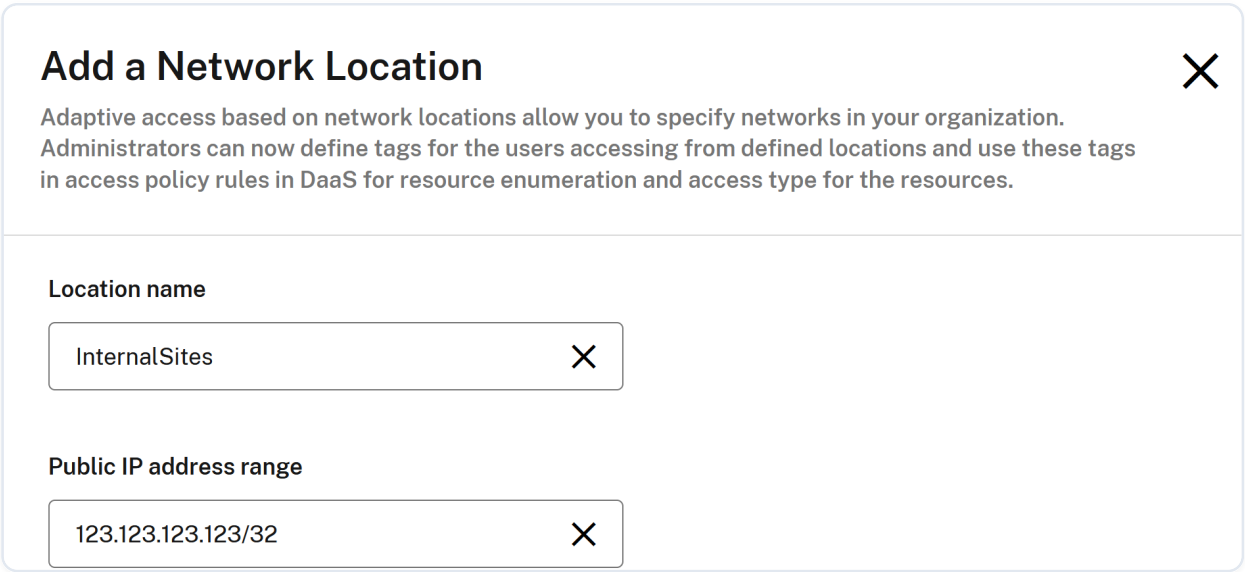
ネットワークロケーション名

クライアントのパブリックエグレスIPとネットワークロケーション名に基づいてIdPインスタンスを割り当てます。

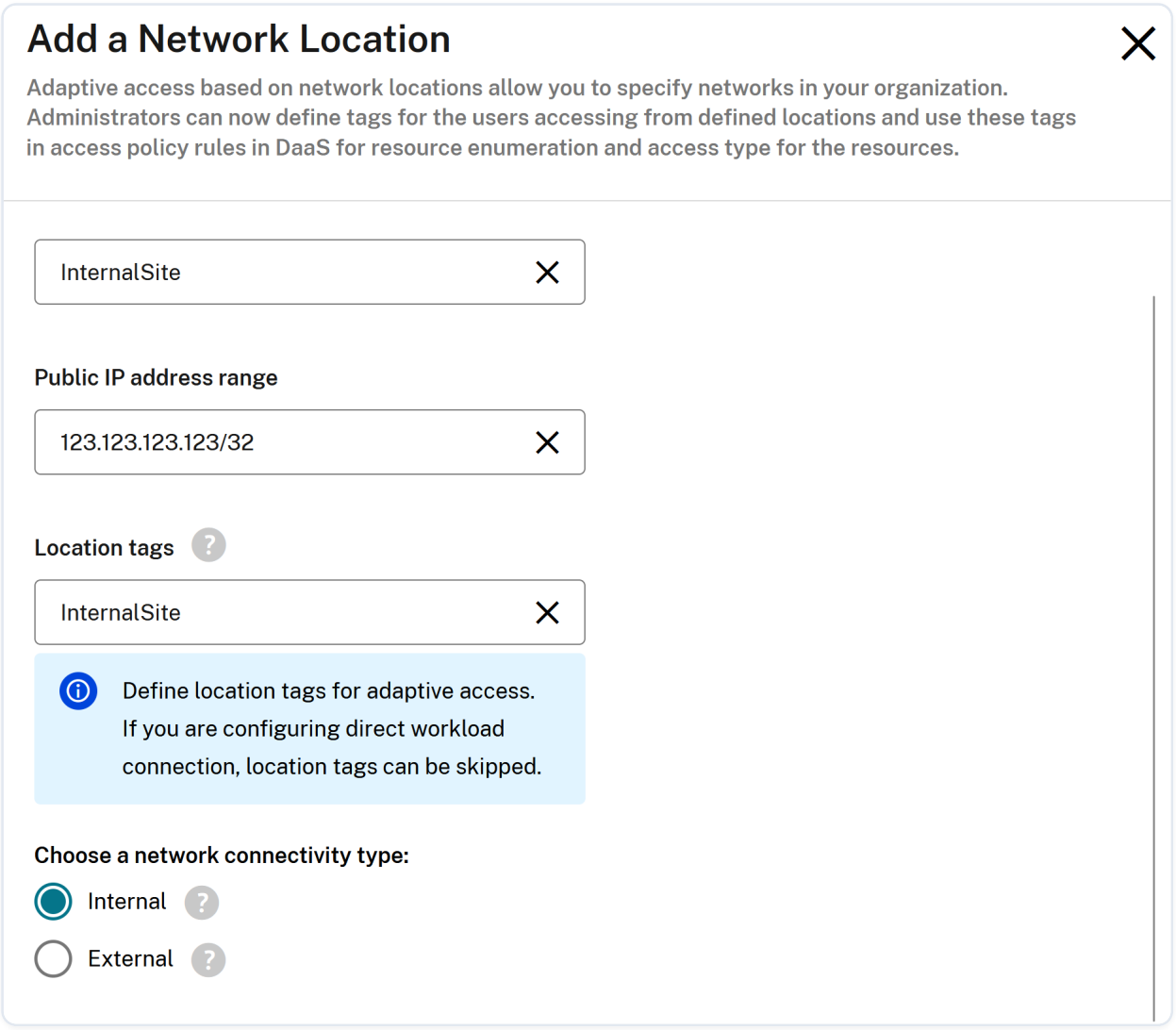
1. ネットワークロケーションの下にパブリックIPアドレス範囲を作成します。



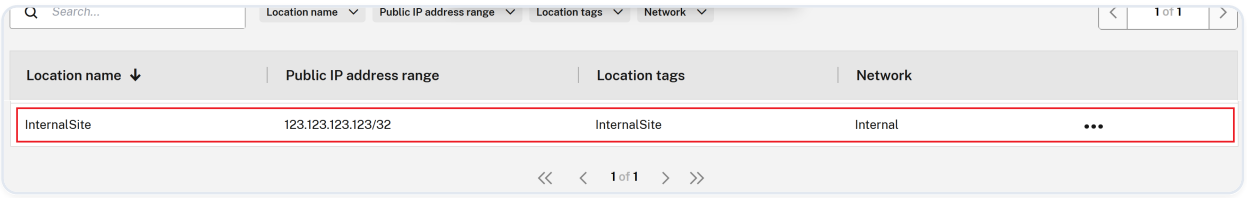
2. 「ネットワークロケーションの追加」をクリックし、名前とパブリックIPアドレス範囲（CIDR表記）を入力します。



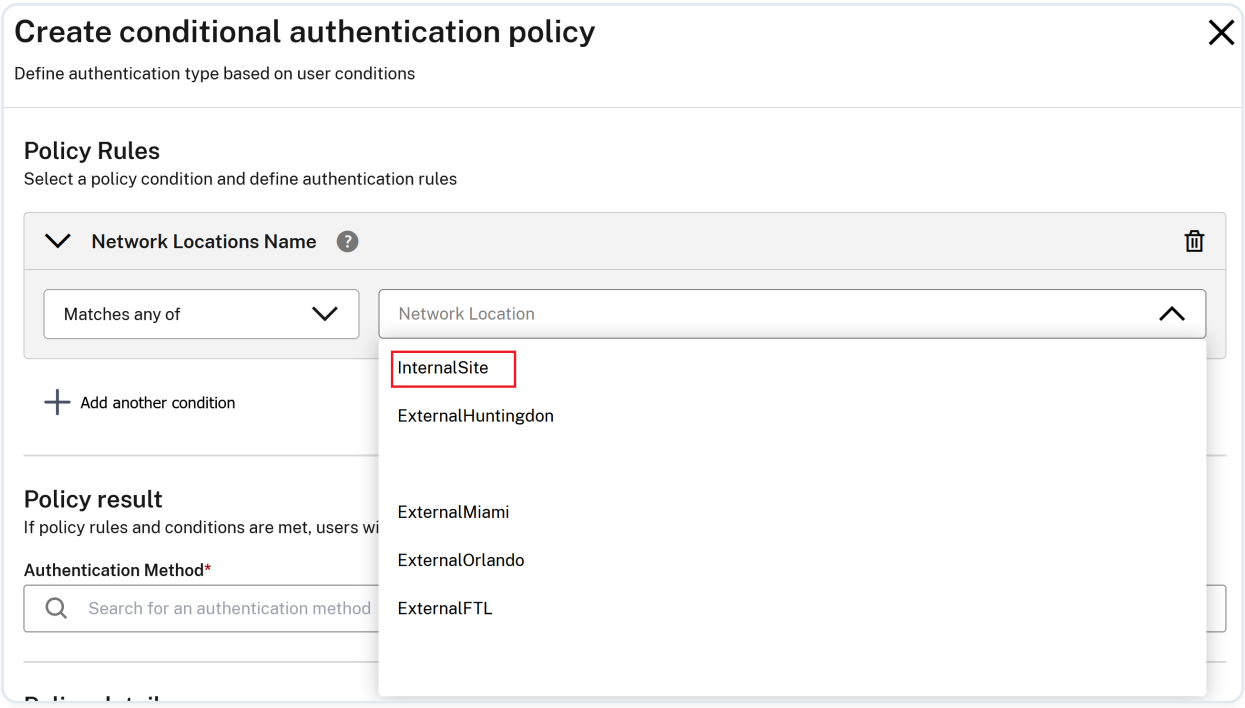
または、Citrix Cloudテナントでスマートアクセスタギングが有効になっている場合



3. ネットワークロケーションが適切に追加されていることを確認します。



4. 条件付き認証プロファイル内で、ロケーション名が事前に入力されます。目的のロケーション名を選択し、ターゲットIdPを割り当てます。



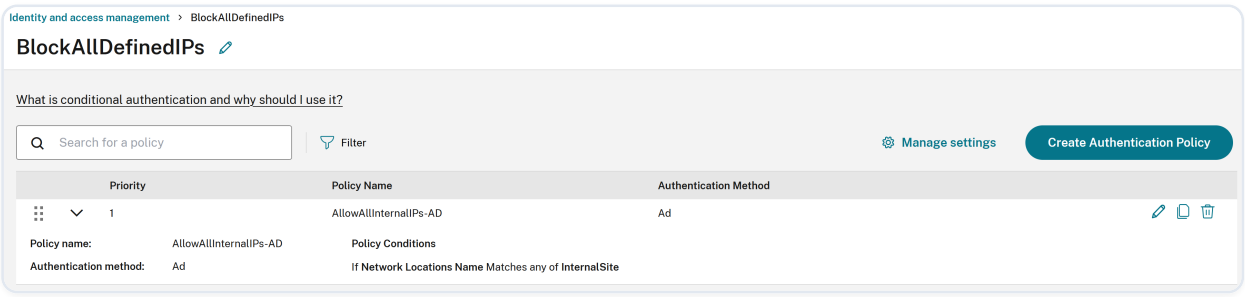
重要:

ネットワークロケーションサイト内で明示的に定義されておらず、かつネットワークロケーション名ポリシーによって参照されていないクライアントの送信元IPは、「未定義」として分類されます。

一般的なNLSのユースケース/構成:

1. **NLSシナリオ1**: 外部（未定義）IPが認証してストアにアクセスするのをブロックします。

   ポリシー1: AllInternalIPs NLSサイト内で定義された送信元IPを持つ内部クライアントのみが、ADを使用してストアにログインできます。

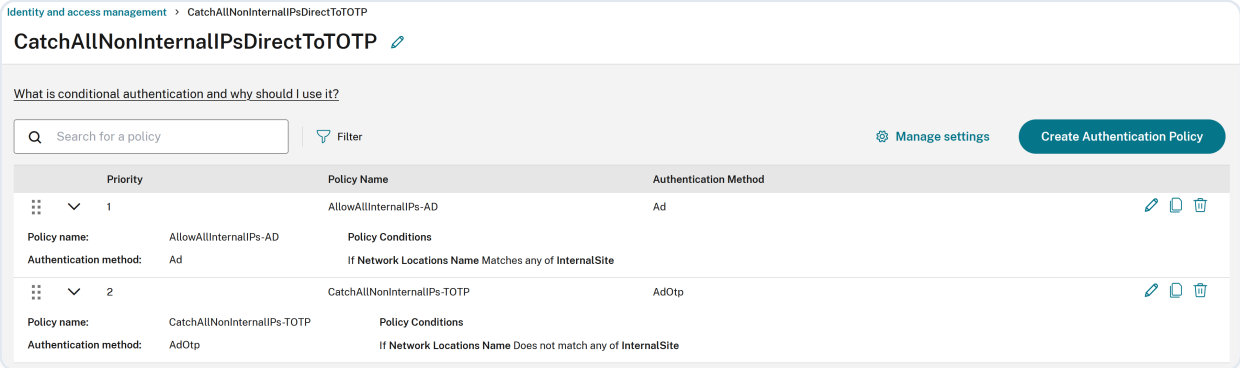


2. **NLSシナリオ2**: すべての「未定義」の送信元IPを、追加の認証要素やセキュリティ強化を伴う「すべてをキャッチするIdPインスタンス」に誘導します。「いずれにも一致しない」とすべて

の内部NLSサイトのリストを使用して、「すべての未定義の送信元IPをキャッチする」ポリシーを定義します。

ポリシー1: AllInternalIPs NLSサイト内で定義された送信元IPを持つ内部クライアントのみが、ADを使用してストアにログインできます。

ポリシー2: AllInternalIPs NLSサイト内で定義されていない外部の送信元IPは、TOTPを使用してストアにログインする必要があります。



条件付き認証プロファイルにカスタムエラーメッセージを設定する

ユーザーが入力した内容とポリシー条件のいずれも一致しない場合に、ストアのエンドユーザーに表示される、ユーザーフレンドリーなエラーメッセージを設定できます。

1. 条件付き認証プロファイル内で、**設定の管理**を選択します。

   CAプロファイル設定(/en-us/citrix-cloud/media/ca-profile-settings.png)

2. エンドユーザーに表示されるデフォルトのエラーメッセージを編集します。

   CAアクセス拒否メッセージ(/en-us/citrix-cloud/media/ca-denied-access-message.png) CAカスタムエラーメッセージ(/en-us/citrix-cloud/media/ca-custom-error-message.png)

Citrix Monitor連携によるトラブルシューティング

ユーザーのログイン試行が一致するポリシーがないために失敗した場合、トランザクションIDが表示されたエラーページが表示されます。ユーザーはこのトランザクションIDをCitrix Cloud管理者に提供して、さらなるサポートを受けることができます。

トランザクションIDのトラブルシューティング(/en-us/citrix-cloud/media/ts-monitor.png)

Citrix Cloud管理者は、ストアのエンドユーザーから提供されたトランザクションIDをCitrix Monitorに貼り付けることで、ポリシー、入力されたユーザー名、および関連する条件付き認証ポ

リシーに関する詳細にアクセスできます。この情報は、管理者が条件付き認証の問題をより効率的にトラブルシューティングし、解決するのに役立ちます。

1. **Monitor**を選択し、右上隅にある検索ボックスをクリックします。

   モニタータブ(/en-us/citrix-cloud/media/monitor-tab.png)

2. ドロップダウンリストからトランザクションIDを選択します。過去3日間のトランザクションのみが利用可能です。

   トランザクションIDの選択(/en-us/citrix-cloud/media/transaction-id.png)

3. エンドユーザーの失敗したトランザクションと、評価された条件付き認証ポリシーの詳細を表示します。シェブロンボタンをクリックすると、エンドユーザーに対して評価されたすべてのポリシー（例: <Policy 1 of 3>）をナビゲートできます。

   失敗したトランザクションID(/en-us/citrix-cloud/media/failed-transaction-id.png)

クラウドネイティブ条件付き認証とNetScalerベースの適応型認証の比較

クラウドネイティブ条件付き認証機能は、ほとんどの条件付き認証ユースケースをカバーするように設計されています。ただし、より高度な認証機能については、NetScalerベースの適応型認証が利用可能です。

NetScalerベースの適応型認証を使用するには、Citrix Cloudの**IDおよびアクセス管理**ページ > **条件付き認証プロファイル**セクションからリクエストを送信してください。

条件付き認証プロファイル(/en-us/citrix-cloud/media/conditional-auth-profiles.png)

既知の問題および制限事項

- ポリシーに負の優先度を設定すると、期待どおりに動作しません。今後のアップデートで対応予定です。
- 現在、グループ条件はActive Directoryのみでサポートされています。ネイティブのEntra IDグループ条件は今後追加される予定です。

IDプロバイダー

Active Directory を Citrix Cloud™ に接続する

Citrix Cloud は、オンプレミスの Active Directory (AD) を使用したエンドユーザー認証をサポートしています。また、一部のストア認証方法では、AD と Citrix Cloud の間に接続が必要です。詳細については、「認証方法の選択または変更」を参照してください。

Citrix Cloud は、Active Directory を介してストアにサインインするエンドユーザーの認証の第2要素としてトークンを使用することもサポートしています。エンドユーザーは、Citrix SSO など、Time-Based One-Time Password 標準に準拠する任意のアプリを使用してトークンを生成できます。

Active Directory とトークンを使用したエンドユーザー認証の詳細については、「Active Directory とトークン」を参照してください。

> **ヒント:**
>
> サポートされている ID プロバイダーの詳細については、教育コース「Citrix Identity and Authentication の概要」を参照してください。「Citrix Identity and Access Management の計画」モジュールには、この ID プロバイダーを Citrix Cloud に接続し、Citrix® StoreFront Cloud の認証を有効にする方法を説明する短いビデオが含まれています。

Active Directory の接続

Active Directory を Citrix Cloud に接続するには、ドメインにコネクタをインストールする必要があります。Active Directory のコネクタとして、Cloud Connector または Connector Appliance のいずれかを使用できます。環境で使用するコネクタの種類を選択するには、以下の記事を参照してください。

- Active Directory での Cloud Connector の展開シナリオ
- Active Directory での Connector Appliance の展開シナリオ

Connector Appliance を介した Active Directory の接続

Connector Appliance を使用して、Citrix Virtual Apps and Desktops™ リソースを含まないフォレストにリソースの場所を接続できます。たとえば、Citrix Secure Private Access のお客様や、ユーザー認証のみに使用されるフォレストを持つ Citrix Virtual Apps and Desktops のお客様の場合などです。

詳細については、「Connector Appliance を使用した Active Directory」を参照してください。

Cloud Connector を介した Active Directory の接続

Citrix Cloud への高可用性接続を確保するには、少なくとも2つの Cloud Connector が必要です。詳細については、以下の記事を参照してください。

- Cloud Connectorのシステム要件(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/system-requirements.html)。
- Cloud Connectorの技術詳細(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/technical-details.html): 展開の推奨事項。
- Cloud Connectorのインストール(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html): グラフィカルインターフェイスまたはコマンドラインのいずれかを使用したインストール手順。

Active DirectoryをCitrix Cloudに接続するには、以下のタスクが必要です。

1. ドメインにCloud Connectorをインストールする(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)。Citrixでは、高可用性のために2つのCloud Connectorをインストールすることを推奨しています。
2. 該当する場合、ユーザーデバイスのトークンを有効にします。エンドユーザーは一度に1つのデバイスしか登録できません。

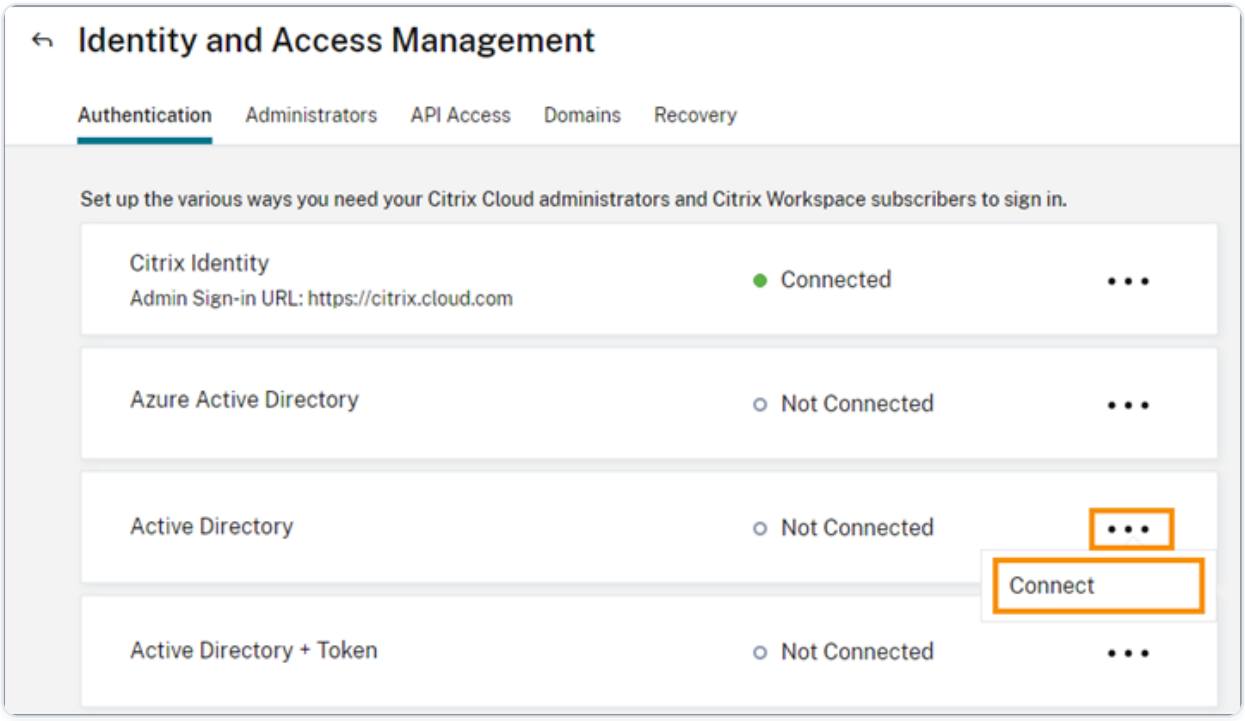
> **重要:**

> Citrix DaaSで使用するためにCloud Connectorを展開している場合、Cloud Connectorの展開後にADドメインが登録され、アクティブであることを確認するために追加の手順が必要になる場合があります。Citrix CloudでADドメインがアクティブであることを確認することで、マシンカタログのセットアップがスムーズに行われます。Citrix DaaSの展開後の手順の詳細については、Citrix DaaS製品ドキュメントの「Citrix Cloudでリソースの種類を追加または未使用のドメインをアクティブ化する」(/ja-jp/citrix-daas/install-configure/resource-

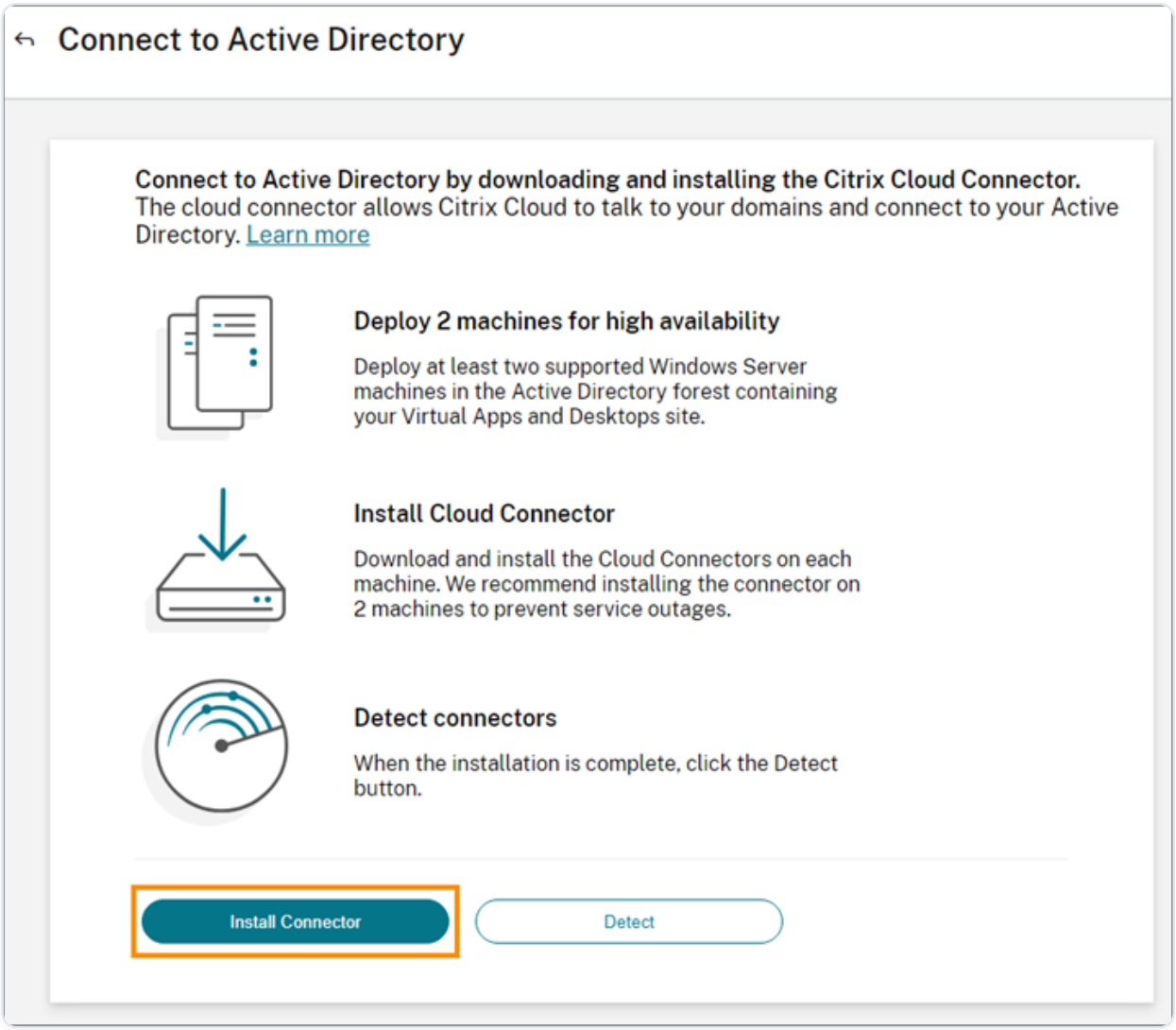
location.html#add-a-resource-type-or-activate-an-unused-domain-in-citrix-cloud)を参照してください。

Active DirectoryをCitrix Cloudに接続するには

1. Citrix Cloudメニューから、**IDおよびアクセス管理**を選択します。
2. **認証**タブで、**Active Directory**の省略記号メニューをクリックし、**接続**を選択します。



3. **コネクタのインストール**をクリックして、Cloud Connectorソフトウェアをダウンロードします。



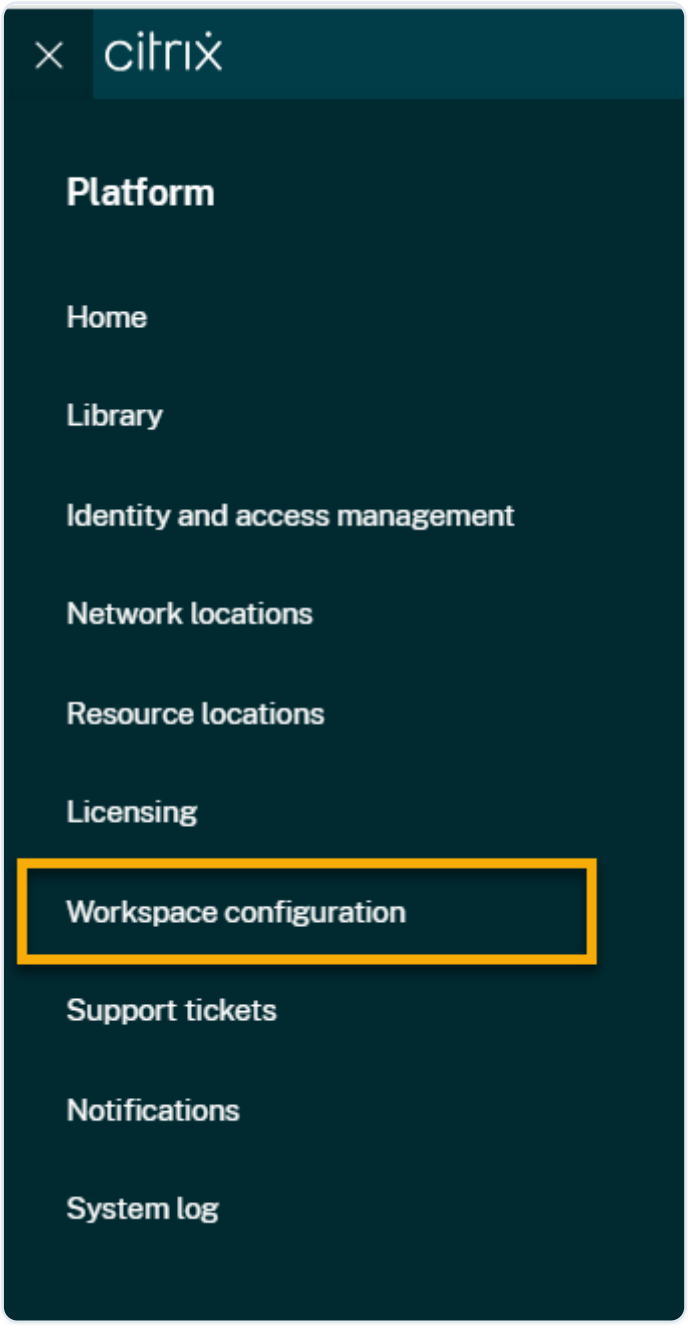
4. Cloud Connectorインストーラーを起動し、インストールウィザードに従います。
5. **Active Directoryへの接続**ページで、**検出**をクリックします。検証後、Citrix CloudはActive Directoryが接続されたことを示すメッセージを表示します。
6. **認証に戻る**をクリックします。**認証**タブで、**Active Directory**エントリが**有効**とマークされます。

Active Directory とトークン認証を有効にするには

1. Connector Appliances または Cloud Connectors を使用して、Active Directory を Citrix Cloud に接続します。
2. Citrix Cloud の セクションで、 タブの エントリが とマークされていることを確認します。
3. をクリックします。 ページが表示され、 オプションがデフォルトで選択されています。
4. をクリックして構成を完了します。 タブで、 エントリが とマークされます。

5. ストアのトークン認証を有効にするには：

   a. Citrix Cloud メニューから、 を選択します。



   b. タブから、 を選択します。

Active Directory とトークン認証を有効にすると、エンドユーザーはデバイスを登録し、認証アプリを使用してトークンを生成できます。エンドユーザーは一度に1つのデバイスのみを登録できます。エンドユーザーのデバイスを登録する手順については、「2要素認証 (オプション)」を参照してください。

エンドユーザーのデバイスを再登録するオプションについては、「デバイスの再登録」を参照してください。

詳細情報

Citrix テックゾーン：

- Tech Insight: 認証 - TOTP
- Tech Insight: 認証 - プッシュ

Microsoft Entra ID を Citrix Cloud™ に接続する

Citrix Cloud は、Citrix Cloud の管理者とエンドユーザーを認証するために Microsoft Entra ID (ME-ID) の使用をサポートしています。

Microsoft Entra ID を Citrix Cloud とともに使用することで、次のことが可能になります。

- 独自の Active Directory を活用して、監査、パスワードポリシーを制御し、必要に応じてアカウントを簡単に無効にできます。
- サインイン資格情報の盗難の可能性に対して、より高いレベルのセキュリティのために多要素認証を構成します。
- ブランド化されたサインインページを使用することで、ユーザーは正しい場所でサインインしていることを認識できます。
- ADFS、Okta、Ping など、選択した ID プロバイダーへのフェデレーションを使用します。

Microsoft Entra ID アプリと権限

Citrix Cloud には、アクティブな Microsoft Entra ID セッションにログインしていなくても Citrix Cloud が Microsoft Entra ID に接続できる Microsoft Entra ID アプリが含まれています。このアプリの導入以来、Citrix はパフォーマンスを向上させ、新しい機能と権限をサポートするアップデートをリリースしました。

Citrix Cloud への既存の Microsoft Entra ID 接続があり、最新の更新されたアプリを使用したい場合は、Citrix Cloud で Microsoft Entra ID 接続を更新する必要があります。詳細については、この記事の「更新されたアプリのために Microsoft Entra ID に再接続する」を参照してください。アプリを更新しないことを選択した場合でも、既存の接続は正常に機能し続けます。

Citrix Cloud が Microsoft Entra ID に接続するために使用する Microsoft Entra ID アプリと権限の詳細については、「Citrix Cloud の Microsoft Entra ID 権限」を参照してください。

> **ヒント:**

> Citrix Identity and Authentication の概要 教育コースで、サポートされている ID プロバイダーについて詳しく学びましょう。「Citrix Identity and Access Management の計画」モジュールには、この ID プロバイダーを Citrix Cloud に接続し、Citrix® StoreFront Cloud の認証を有効にする方法を説明する短いビデオが含まれています。

複数の Citrix Cloud アカウントでの認証

この記事では、Microsoft Entra ID を ID プロバイダーとして単一の Citrix Cloud アカウントに接続する方法について説明します。複数の Citrix Cloud アカウントをお持ちの場合は、それぞれを同じ Microsoft Entra ID テナントに接続できます。次のタスクを実行します。

1. Citrix Cloudアカウントにサインインし、顧客ピッカーから適切な顧客IDを選択します。
2. 選択した顧客がMicrosoft Entra IDに接続する最初の顧客である場合は、ADとMicrosoft Entra IDの同期、顧客のCitrix Cloudへの接続、および管理者の追加に関するこの記事のすべての手順に従ってください。
3. 別の顧客を接続するには、Citrix Cloudコンソールの右上隅にあるユーザーメニューをクリックし、**顧客の変更**を選択して、接続する次の顧客IDを選択します。
4. この記事のCitrix CloudをMicrosoft Entra IDに接続するで説明されているように、顧客をMicrosoft Entra IDに接続します。
5. 各顧客IDについて、手順3と4を繰り返します。

Active DirectoryとMicrosoft Entra IDを準備する

Microsoft Entra IDを使用する前に、以下の要件を満たしていることを確認してください。

- Microsoft Azureアカウントをお持ちであること。すべてのAzureアカウントには、Microsoft Entra IDが無料で付属しています。Azureアカウントをお持ちでない場合は、https://azure.microsoft.com/ja-jp/free/?v=17.36でサインアップしてください。
- Microsoft Entra IDでグローバル管理者ロールを持っていること。このロールは、Citrix CloudがMicrosoft Entra IDに接続するための同意を与えるために必要です。
- 管理者アカウントの「メール」プロパティがMicrosoft Entra IDで構成されていること。これを行うには、MicrosoftのMicrosoft Entra ID Connectツールを使用して、オンプレミスのActive DirectoryからMicrosoft Entra IDにアカウントを同期できます。または、同期されていないMicrosoft Entra IDアカウントをOffice 365メールで構成することもできます。

Microsoft Entra ID Connectでアカウントを同期する

1. Active Directoryアカウントにメールユーザープロパティが構成されていることを確認します。

a. Active Directoryユーザーとコンピューターを開きます。

b. **ユーザー**フォルダーで、確認したいアカウントを見つけ、右クリックして**プロパティ**を選択します。**全般**タブで、**メール**フィールドに有効なエントリがあることを確認します。Citrix Cloudでは、Microsoft Entra IDから追加された管理者は、Citrixホスト型IDを使用してサインインする管理者とは異なるメールアドレスを持っている必要があります。

2. Microsoft Entra ID Connectをインストールして構成します。詳細な手順については、Microsoft Azure Webサイトのエクスプレス設定を使用したMicrosoft Entra ID Connectの開始を参照してください。

Citrix Cloud を Microsoft Entra ID に接続する

Citrix Cloud アカウントを Microsoft Entra ID に接続する場合、Citrix Cloud は、Microsoft Entra ID 内のユーザーの基本プロファイルに加えて、ユーザープロファイル (またはサインインしているユーザーのプロファイル) にアクセスするためのアクセス許可を必要とします。Citrix は、お客様の名前とメールアドレス (管理者として) を取得し、後で他のユーザーを検索して管理者として追加できるようにするために、このアクセス許可を要求します。Citrix Cloud が要求するアプリのアクセス許可の詳細については、「Citrix Cloud の Microsoft Entra ID アクセス許可」を参照してください。

> **重要:**
>
> このタスクを完了するには、Microsoft Entra ID のグローバル管理者である必要があります。または、Citrix Cloud にサインインする前に、いずれかのグローバル管理者に前提条件を実行してもらう必要があります。

1. ページの左上隅にある をクリックし、 を選択します。
2. Microsoft Entra ID を見つけて、省略記号メニューから を選択します。
3. プロンプトが表示されたら、会社用の短く URL フレンドリな識別子を入力し、 をクリックします。選択する識別子は、Citrix Cloud 内でグローバルに一意である必要があります。
4. プロンプトが表示されたら、接続する Azure アカウントにサインインします。Azure には、Citrix Cloud がアカウントにアクセスし、接続に必要な情報を取得するために必要なアクセス許可が表示されます。これらのアクセス許可のほとんどは読み取り専用であり、Citrix Cloud が Microsoft Graph からグループやユーザープロファイルなどの基本情報を収集できるようにします。Citrix Endpoint Management または XenMobile Server を Microsoft Intune と統合している場合は、Microsoft Intune 関連の読み取り/書き込みアクセス許可を付与する必要がありま

す。詳細については、「Citrix Cloud の Microsoft Entra ID アクセス許可」を参照してください。

5. アクセス許可要求を承認するには、 をクリックします。

代替接続方法

接続フローは、次の2つのフェーズに分けることができます。

1. Azure での Microsoft Entra ID アプリの作成。
2. Citrix Cloud での Microsoft Entra ID アプリへの Citrix Cloud 接続。

まず、グローバル管理者がエンタープライズアプリをテナントに追加するために使用できる URL を構築する必要があります。詳細については、「テナント全体の管理者同意を付与するための URL の構築」を参照してください。

構築された URL の説明を次に示します。 `https://login.microsoftonline.com/<tenant url>/adminconsent?client_id=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.azure.com`

ここで: `tenant url` はテナントのURLまたはIDです。 `f9c0e999-22e7-409f-bb5e-956986abdf02` はCitrix Cloudのクライアントidです。

Microsoft Entra IDからCitrix Cloudに管理者を追加する

Citrix Cloudは、個別に、またはMicrosoft Entra IDグループとして管理者を追加することをサポートしています。

Microsoft Entra IDから個々の管理者を追加するには、「管理者のアクセスを管理する」を参照してください。

Microsoft Entra ID管理者グループをCitrix Cloudに追加するには、「管理者グループを管理する」を参照してください。

Microsoft Entra IDを使用してCitrix Cloudにサインインする

Microsoft Entra IDユーザーアカウントが接続されると、ユーザーは以下のいずれかの方法でCitrix Cloudにサインインできます。

- 会社用にMicrosoft Entra ID IDプロバイダーを最初に接続したときに構成した管理者サインインURLに移動します。例: `https://citrix.cloud.com/go/mycompany`
- Citrix Cloudサインインページで、 をクリックし、Microsoft Entra IDを最初に接続したときに作成した識別子（例: 「mycompany」）を入力して、 をクリックします。

ストアのMicrosoft Entra ID認証を有効にする

Microsoft Entra IDをCitrix Cloudに接続すると、エンドユーザーがMicrosoft Entra IDを介してストアに認証できるようにすることができます。

> **重要:**
>
> Microsoft Entra IDストア認証を有効にする前に、ストアでMicrosoft Entra IDを使用する際の考慮事項について、Microsoft Entra IDセクションを確認してください。

1. Citrix Cloudで、左上隅のメニューボタンをクリックし、 を選択します。
2. タブから、 を選択します。
3. 「**確認**」をクリックして、Microsoft Entra ID 認証が有効になったときに発生するストアエクスペリエンスの変更を承諾します。

高度なMicrosoft Entra ID機能を有効にする

Microsoft Entra IDは、高度な多要素認証、世界クラスのセキュリティ機能、20種類のIDプロバイダーへのフェデレーション、セルフサービスパスワード変更とリセットなど、多くの機能を提供します。これらの機能をMicrosoft Entra IDユーザーに対して有効にすると、Citrix Cloudはそれらの機能を自動的に活用できるようになります。

Microsoft Entra IDのサービスレベル機能と価格を比較するには、https://azure.microsoft.com/ja-jp/pricing/details/active-directory/を参照してください。

更新されたアプリのためにMicrosoft Entra IDに再接続する

Citrix Cloudには、アクティブなMicrosoft Entra IDセッションにログインしていなくてもCitrix CloudがMicrosoft Entra IDに接続できるMicrosoft Entra IDアプリが含まれています。このアプリの導入以来、Citrixはアプリを次のように更新しました。

- 2018年8月、アプリはパフォーマンスを向上させ、将来のリリースに備えられるように更新されました。
- 2019年5月、アプリはCitrix CloudへのMicrosoft Entra ID管理者グループの追加をサポートするように更新されました。
- 2022年4月、アプリはGroup.Read.All権限に代わるGroupMember.Read.All権限を使用するように更新されました。

これらの更新がリリースされる前にMicrosoft Entra IDをCitrix Cloudに接続していて、最新の更新されたアプリを使用したい場合は、Microsoft Entra IDをCitrix Cloudから切断し、再接続する必要があります。最新のアプリを使用することは任意です。アプリを更新しないことを選択した場合でも、既存の接続は正常に機能します。

要件

Microsoft Entra IDを再接続する前に、次の要件を満たしていることを確認してください。

- デフォルトのCitrix IDプロバイダーの下で、フルアクセス権限を持つ管理者である必要があります。Microsoft Entra IDの資格情報でCitrix Cloudにサインインしている場合、再接続は失敗します。アカウントにCitrix IDプロバイダーを使用している管理者がいない場合は、一時的に追加し、Microsoft Entra IDの再接続後に削除できます。手順については、個々の管理者を招待するを参照してください。
- エンドユーザーの認証にMicrosoft Entra IDを使用している場合は、一時的に別のIDプロバイダーを選択してください。Microsoft Entra IDがStoreFront Cloudの認証方法としても使用されている場合、Citrix CloudではMicrosoft Entra IDを切断できません。詳細については、StoreFront Cloudドキュメントの認証方法の選択または変更を参照してください。

Microsoft Entra IDを再接続するには

1. Citrix IDプロバイダーの下で、完全なアクセス権限を持つ管理者としてCitrix Cloud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**認証**を選択します。
3. **Microsoft Entra ID**を見つけ、ページの右端にある省略記号メニューから**切断**を選択します。
4. 省略記号メニューから、**接続**を選択します。

> **注:**
>
> ステップ3で述べたようにMicrosoft Entra IDを切断する場合、Citrix Cloudは、このIDプロバイダーの下にあるすべての管理者プロファイルを削除するよう管理者に要求します。 この手間を回避するには、管理者は以下の手順に従ってMicrosoft Entra ID IDプロバイダーを再接続できます。

1. グローバル管理者として、Azureに移動し、アプリを削除します。

2. Citrix Cloudにログインし、**IDおよびアクセス管理**に移動して**認証**をクリックします。**認証**タブから、Microsoft Entra IDがまだ接続されていることに気づくでしょう。
3. Citrix CloudでMicrosoft Entra ID用に新しい管理者を追加します。

これにより、アプリの再作成がトリガーされ、管理者を削除することなく再接続が行われます。

Citrix Cloud™ の Microsoft Entra ID アクセス許可

この記事では、Citrix Cloud が Microsoft Entra ID (ME-ID) に接続して使用する際に要求するアクセス許可について説明します。Microsoft Entra ID が Citrix Cloud アカウントでどのように使用されるかに応じて、ターゲットの Microsoft Entra ID テナントに1つ以上のエンタープライズアプリケーションが作成される場合があります。複数の Citrix Cloud アカウントを1つの Microsoft Entra ID テナントに接続し、アカウントごとにアプリケーションセットを作成することなく、同じエンタープライズアプリケーションを使用できます。

注記:

2022年4月現在、Citrix Cloud が Microsoft Entra ID に接続するために使用する Microsoft Entra ID アプリは、Group.Read.All アクセス許可の代わりに GroupMember.Read.All アクセス許可を使用するように更新されました。既存の Microsoft Entra ID 接続 (2022年4月以前) があり、アプリに新しいアクセス許可を使用させたい場合は、Microsoft Entra ID を Citrix Cloud から切断し、再接続する必要があります。この操作により、アカウントが Citrix Cloud で最新の Microsoft Entra ID アプリを使用していることが保証されます。詳細については、「アップグレードされたアプリのために Microsoft Entra ID に再接続する」を参照してください。

アプリを更新しないことを選択した場合でも、既存の接続は引き続き正常に機能します。

エンタープライズアプリケーション

次の表に、Citrix Cloud が Microsoft Entra ID に接続して使用する際に利用する Microsoft Entra ID エンタープライズアプリケーションと、各アプリケーションの使用目的を示します。

名前	アプリケーションID	用途
シトリックス クラウド	e95c4605-aeab-48d9-9c36-1a262ef8048e	ストアエンドユーザーログイン
シトリックス クラウド	f9c0e999-22e7-409f-bb5e-956986abdf02	Microsoft Entra ID と Citrix Cloud 間のデフォルト接続 (#default-connection-between-microsoft-entra-id-and-citrix-cloud)
シトリックス クラウド	1b32f261-b20c-4399-8368-c8f0092b4470	管理者への招待とログイン (#administrator-invitations-and-logins)
シトリックス クラウド	5c913119-2257-4316-9994-5e8f3832265b	Citrix Endpoint Management™ を使用した Microsoft Entra ID と Citrix Cloud 間のデフォルト接続 (#default-connection-between-microsoft-entra-id-and-citrix-cloud-with-endpoint-management)
シトリックス クラウド	e067934c-b52d-4e92-b1ca-70700bd1124e	Citrix Endpoint Management を使用した Microsoft Entra ID と Citrix Cloud 間のレガシー接続(#legacy-connection-between-microsoft-entra-id-and-citrix-cloud-with-endpoint-management)

アクセス許可

Citrix Cloud のエンタープライズアプリケーションのアクセス許可により、Citrix Cloud は Microsoft Entra ID テナント内の特定のデータにアクセスできます。Citrix Cloud はこれらのデータを使用して、Microsoft Entra ID テナントへの接続、専用のサインイン URL を使用した管理者による Citrix Cloud へのサインインの有効化、Microsoft Entra ID テナントと Endpoint Management の接続などの特定の機能を実行します。Citrix Cloud は、お客様の同意がある場合にのみこれらのデータにアクセスできます。これらのアクセス許可は、Citrix Cloud が Microsoft Entra ID と連携す

るために必要な最小限の特権を表します。Microsoft Entra ID のアクセス許可と同意の詳細については、Microsoft Azure ドキュメント Web サイトの Permissions and consent in the Microsoft identity platform を参照してください。

この記事では、Microsoft Entra ID アプリケーションの各アクセス許可セットに次の情報が含まれています。

- **API 名:** Citrix Cloud がアクセス許可を要求するリソースアプリケーション。これらのアプリケーションは Microsoft Graph と Windows Microsoft Entra ID です。Citrix Cloud は、これら両方のリソースアプリケーションから同じアクセス許可を要求します。
- **種類:** Citrix Cloud が特定のアクセス許可に対して要求するアクセスレベル。特定のエンタープライズアプリケーションのアクセス許可には、次のいずれかのアクセスレベルがあります。
  - **委任されたアクセス許可**は、サインインしているユーザーに代わって動作するために使用されます。たとえば、ユーザーのプロファイルを照会する場合などです。
  - **アプリケーションのアクセス許可**は、アプリケーションがユーザーの存在なしにアクションを実行する場合に使用されます。たとえば、特定のグループ内のユーザーを照会する場合などです。このアクセス許可タイプには、Microsoft Entra ID のグローバル管理者による同意が必要です。
- **クレーム値:** Microsoft Entra ID が特定のアクセス許可に割り当てる情報文字列。特定のエンタープライズアプリケーションのアクセス許可には、次のいずれかのクレーム値を含めることができます。
  - **User.Read:** Citrix Cloud管理者が、接続されたMicrosoft Entra IDのユーザーをCitrix Cloudアカウントの管理者として追加できるようにします。
  - **User.ReadBasic.All:** ユーザーのプロファイルから基本情報を収集します。User.Read.Allのサブセットですが、アクセス許可自体は下位互換性のために残されています。
  - **User.Read.All:** Citrix Cloudは、Microsoft Graphでユーザーのリストを呼び出し、顧客の接続されたMicrosoft Entra IDからユーザーの参照と選択を可能にします。たとえば、Microsoft Entra IDのユーザーには、ストアを持つCitrix DaaSリソースへのアクセス権を付与できます。Citrix Cloudは、基本プロファイル以外のプロパティ（`onPremisesSecurityIdentifier`など）にアクセスする必要があるため、`User.ReadBasic.All`を使用できません。
  - **GroupMember.Read.All:** Citrix Cloudは、Microsoft Graphでグループのリストを呼び出し、顧客の接続されたMicrosoft Entra IDからグループの参照と選択を可能にします。たとえば、Microsoft Entra IDのグループにもCitrix DaaSアプリケーションへのアクセス権を付与できます。

- **Directory.Read.All:** Citrix Cloudは、Microsoft GraphでmemberOfのリストを呼び出し、ユーザーのグループメンバーシップを取得します。これは、`Groups.Read.All`では不十分であるためです。
- **DeviceManagementApps.ReadWrite.All:** Citrix Cloudが、Microsoft Intuneによって管理されるプロパティ、グループ割り当て、アプリのステータス、アプリ構成、およびアプリ保護ポリシーを読み書きできるようにします。
- **Directory.AccessAsUser.All:** Citrix Cloudが、サインインしているユーザーと同じディレクトリ内の情報へのアクセス権を持つことを許可します。

> **注:**
>
> **Directory.Read.All**は、**Microsoft Entra IDとCitrix CloudのEndpoint Managementとの間のデフォルト接続**にのみ適用されます。

ストアエンドユーザーログイン

このCitrix Cloudアプリケーション（ID: e95c4605-aeab-48d9-9c36-1a262ef8048e）は、次のアクセス許可を使用します。

API名	クレーム値	権限名	タイプ
マイクロソフトグラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任

Microsoft Entra IDとCitrix Cloud間のデフォルト接続

このCitrix Cloudアプリケーション (ID: f9c0e999-22e7-409f-bb5e-956986abdf02) は、以下の権限を使用します:

API名	クレーム値	権限	タイプ
マイクロソフトグラフ	GroupMember.Read.All	すべてのグループを読み取る	委任
マイクロソフトグラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任

API名	クレーム値	権限	タイプ
マイクロソフトグラフ	User.Read.All	すべてのユーザーの完全なプロファイルを読み取る	委任
マイクロソフトグラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフトグラフ	GroupMember.Read.All	すべてのグループを読み取る	アプリケーション
マイクロソフト グラフ	User.Read.All	すべてのユーザーの完全なプロファイルを読み取る	アプリケーション

管理者への招待とログイン

このCitrix Cloudアプリケーション（ID: 1b32f261-b20c-4399-8368-c8f0092b4470）は、以下の権限を使用します。

API名	クレーム値	権限名	種類
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフト グラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任

Microsoft Entra ID と Endpoint Management を使用した Citrix Cloud との既定の接続

この Citrix Cloud アプリケーション (ID: 5c913119-2257-4316-9994-5e8f3832265b) は、次のアクセス許可を使用します。

API名	要求値	アクセス許可名	種類
マイクロソフト グラフ	GroupMember.Read.All	すべてのグループを読み取る	委任

API名	要求値	アクセス許可名	種類
マイクロソフト グラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフト グラフ	Directory.Read.All	ディレクトリデータを読み取る	アプリケーション
マイクロソフト グラフ	Directory.Read.All	ディレクトリデータを読み取る	委任
マイクロソフト グラフ	DeviceManagementApps.ReadWrite.All	Microsoft Intuneアプリの読み取りと書き込み	委任
マイクロソフト グラフ	Directory.AccessAsUser.All	サインインしているユーザーとしてディレクトリにアクセスする	委任

Microsoft Entra IDとCitrix Cloud (Endpoint Managementを使用) のレガシー接続

このCitrix Cloudアプリケーション (ID: e067934c-b52d-4e92-b1ca-70700bd1124e) は、以下の権限を使用します。

API名	要求値	権限名	種類
マイクロソフト グラフ	GroupMember.Read.All	すべてのグループを読み取る	委任
マイクロソフト グラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任

API名	要求値	権限名	種類
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフト グラフ	DeviceManagementApps.ReadWrite.All	Microsoft Intune アプリの読み書き	委任済み
マイクロソフト グラフ	Directory.AccessAsUser.All	サインインしているユーザーとしてディレクトリにアクセス	委任済み

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

Citrix Cloudは、オンプレミスのCitrix GatewayをIDプロバイダーとして使用し、ストアにサインインするエンドユーザーを認証することをサポートしています。

Citrix Gateway認証を使用すると、次のことが可能になります。

- 既存のCitrix Gatewayを介してユーザー認証を継続し、オンプレミスのVirtual Apps and Desktops展開内のリソースにCitrix® StoreFront Cloudを介してアクセスできるようにします。
- Citrix Gatewayの認証、承認、および監査 (AAA) 機能をStoreFront Cloudで使用します。
- パススルー認証、スマートカード、セキュアトークン、条件付きアクセスポリシー、フェデレーションなどの機能を使用し、StoreFront Cloudを介してユーザーが必要なリソースにアクセスできるようにします。

> **ヒント:**
>
> Citrix Identity and Authenticationの概要教育コースで、サポートされているIDプロバイダーについて詳しく学びましょう。「Citrix Identity and Access Managementの計画」モジュールには、このIDプロバイダーをCitrix Cloudに接続し、StoreFront Cloudの認証を有効にする手順を説明する短いビデオが含まれています。

サポートされているバージョン

Citrix Gateway認証は、以下のオンプレミス製品バージョンでの使用がサポートされています。

- Citrix Gateway 12.1 54.13 Advanced エディション以降
- Citrix Gateway 13.0 41.20 Advanced エディション以降

前提条件

クラウドコネクタ

Citrix Cloud Connector™ソフトウェアをインストールするためのサーバーが少なくとも2台必要です。これらのサーバーは、以下の要件を満たしている必要があります。

- (/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/system-requirements.html)に記載されているシステム要件を満たしていること。
- 他のCitrixコンポーネントがインストールされておらず、Active Directoryドメインコントローラーではなく、リソースロケーションインフラストラクチャにとって重要なマシンではないこと。
- サイトが存在するドメインに参加していること。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、各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。
- サイトに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、(/ja-jp/citrix-cloud/overview/requirements/internet-connectivity-requirements.html)を参照してください。
- Citrix Cloudとの高可用性接続を確保するには、少なくとも2つのCloud Connectorが必要です。インストール後、Cloud ConnectorはCitrix Cloudがサイトを特定し、通信できるようにします。

Cloud Connectorのインストールについて詳しくは、(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)を参照してください。

アクティブディレクトリ

Citrix Gateway認証を有効にする前に、次のタスクを実行します。

- エンドユーザーがActive Directory (AD) にユーザーアカウントを持っていることを確認します。ADアカウントを持たないエンドユーザーは、ストアに正常にサインインできません。
- エンドユーザーのADアカウントのユーザープロパティが入力されていることを確認します。Citrix Cloudは、エンドユーザーがサインインする際にユーザーコンテキストを確立するためにこれらのプロパティを必要とします。これらのプロパティが入力されていない場合、エンドユーザーはストアにサインインできません。これらのプロパティには以下が含まれます。

- メールアドレス
- 表示名
- 共通名
- SAMアカウント名
- ユーザープリンシパル名
- OID
- SID

- Active Directory (AD)をCitrix Cloudアカウントに接続します。このタスクでは、Cloud Connectorsセクションで説明されているように、準備したサーバーにCloud Connectorソフトウェアをインストールします。Cloud Connectorを使用すると、Citrix Cloudはオンプレミス環境と通信できます。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。
- Citrix Gateway認証でフェデレーションを実行している場合は、ADユーザーをフェデレーションプロバイダーに同期します。Citrix Cloudでは、エンドユーザーが正常にサインインできるように、ADユーザー属性が必要です。

要件

Citrix Gatewayの高度なポリシー

Citrix Gateway認証では、従来のポリシーが非推奨になったため、オンプレミスGatewayで高度なポリシーを使用する必要があります。高度なポリシーは、IDプロバイダーチェーンなどのオプションを含む、Citrix Cloudの多要素認証（MFA）をサポートします。現在従来のポリシーを使用している場合は、Citrix CloudでCitrix Gateway認証を使用するために、新しい高度なポリシーを作成する必要があります。高度なポリシーを作成する際に、従来のポリシーのAction部分を再利用できます。

署名用証明書

エンドユーザーをStoreFront Cloudに認証するためにGatewayを構成する場合、GatewayはOpenID Connectプロバイダーとして機能します。Citrix CloudとGateway間のメッセージはOIDCプロトコルに準拠しており、トークンのデジタル署名が含まれます。したがって、これらのトークンに署名するための証明書を構成する必要があります。この証明書は、パブリック認証局（CA）から発行されたものである必要があります。プライベートCAによって発行された証明書の使用はサポートされていません。これは、Citrix Cloudにプライベートルート CA証明書を提供する方法が

ないためです。そのため、信頼の証明書チェーンを確立できません。署名用に複数の証明書を構成した場合、これらのキーはメッセージごとにローテーションされます。

キーは**vpn global**にバインドされている必要があります。これらのキーがないと、エンドユーザーはサインイン後にストアに正常にアクセスできません。

クロック同期

OIDCのデジタル署名されたメッセージにはタイムスタンプが含まれるため、GatewayはNTP時刻に同期されている必要があります。クロックが同期されていない場合、Citrix Cloudはトークンの有効性を確認する際に、トークンが古いと見なします。

タスクの概要

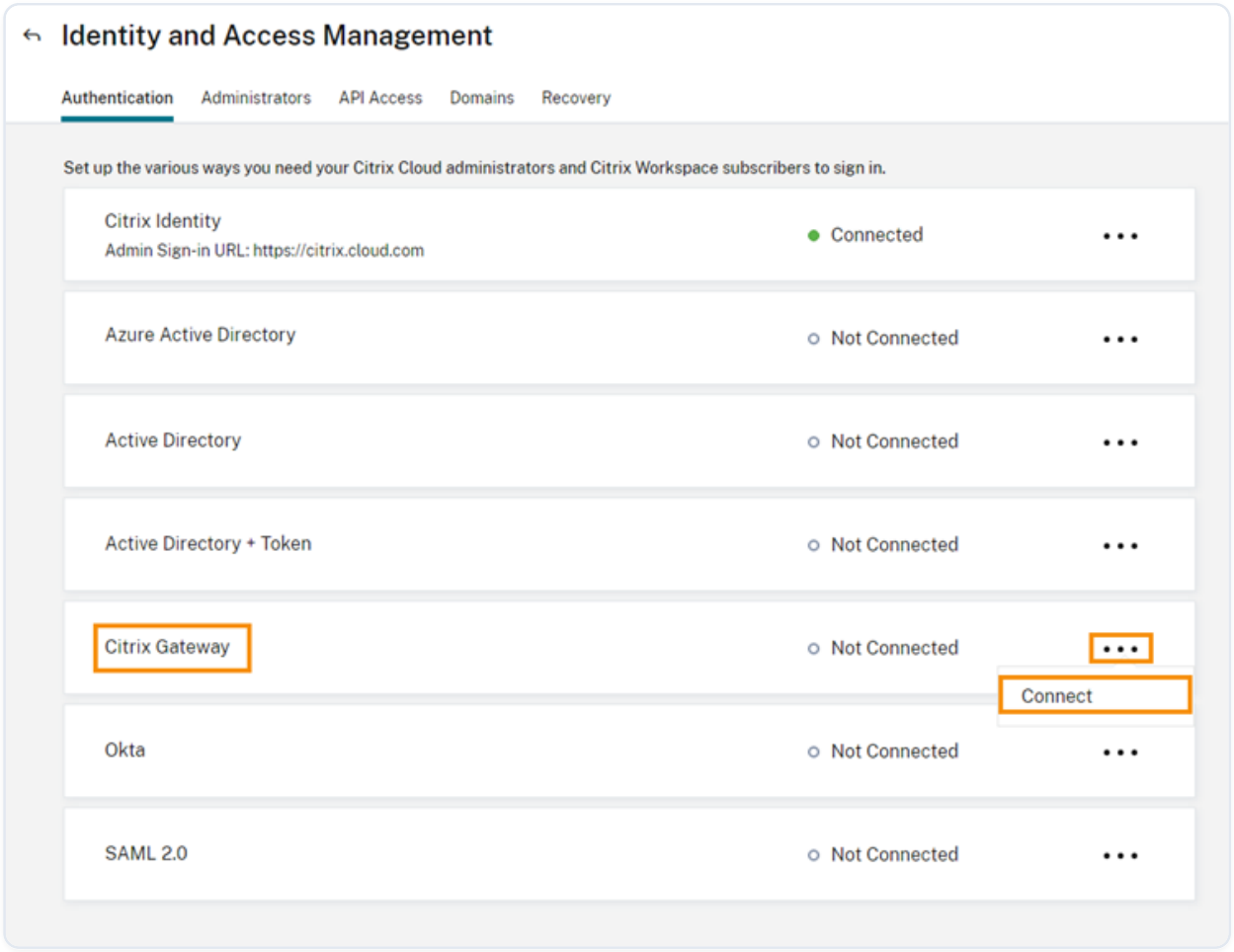
Citrix Gateway認証を設定するには、次のタスクを実行します。

1. 「**IDおよびアクセス管理**」で、Gatewayへの接続の構成を開始します。この手順で、GatewayのクライアントID、シークレット、およびリダイレクトURLを生成します。
2. Gatewayで、Citrix Cloudから生成された情報を使用してOAuth IdP詳細ポリシーを作成します。これにより、Citrix CloudはオンプレミスのGatewayに接続できるようになります。手順については、以下の記事を参照してください。
   - Citrix Gateway 12.1: オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する
   - Citrix Gateway 13.0: オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する
3. 「**StoreFront Cloud**」で、エンドユーザー向けのCitrix Gateway認証を有効にします。

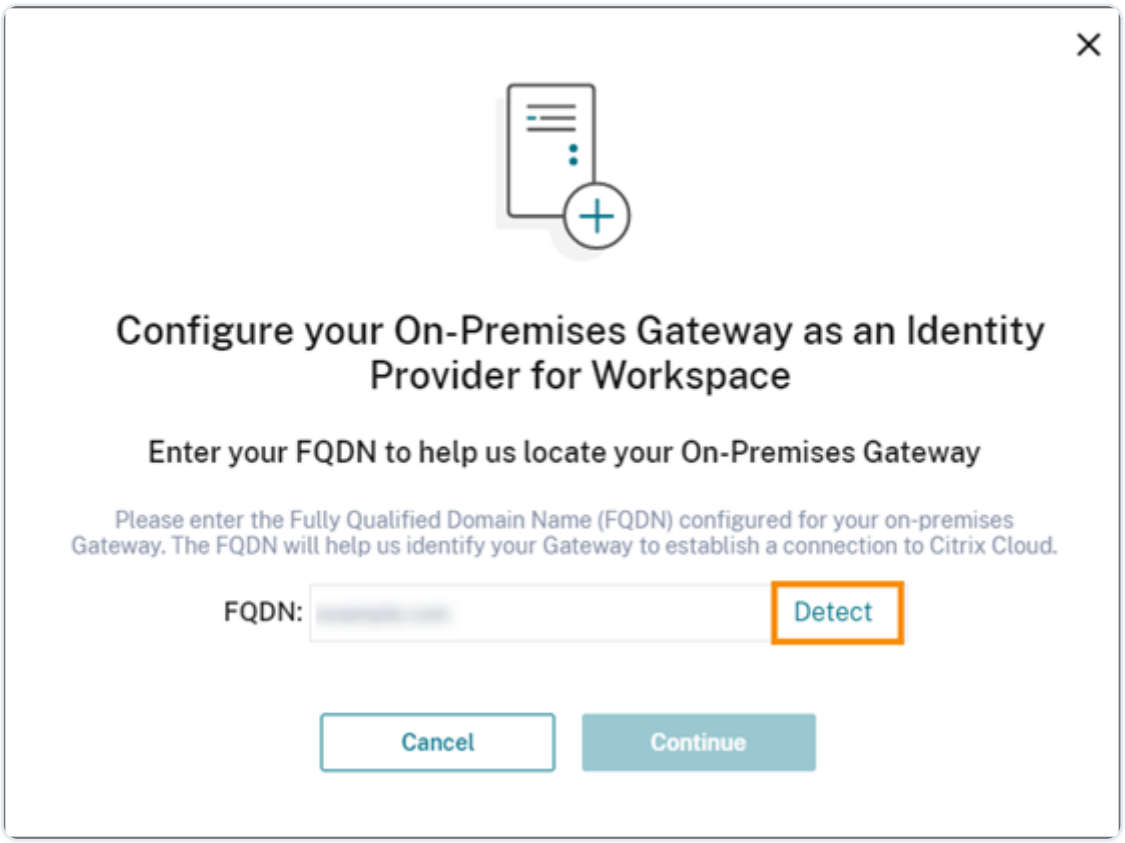
エンドユーザー向けのCitrix Gateway認証を有効にするには

1. Citrix Cloudメニューから、［**IDおよびアクセス管理**］ を選択します。

2. ［**認証**］ タブの ［**Citrix Gateway**］ で、省略記号メニューをクリックし、 ［**接続**］ を選択します。



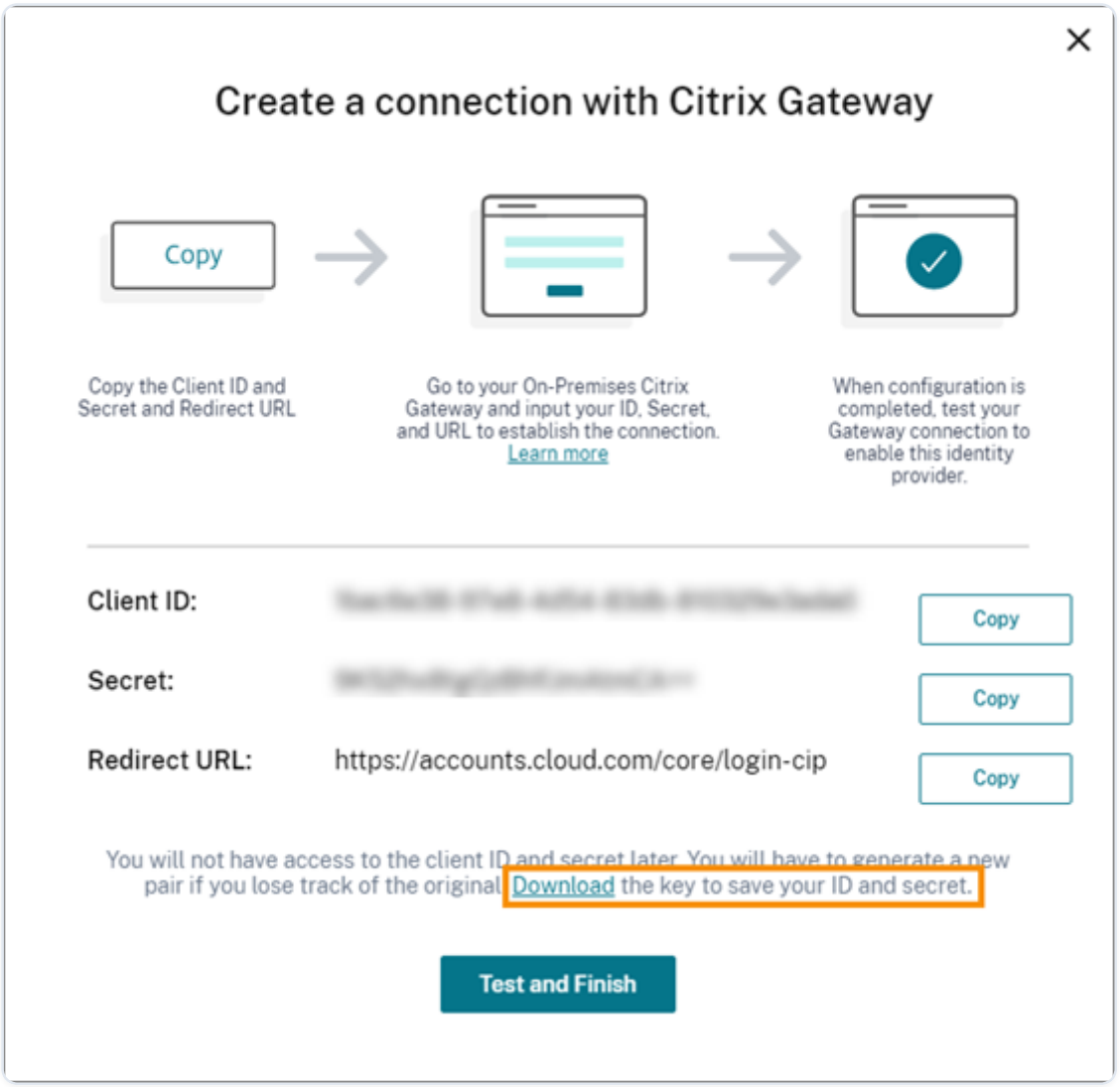
3. オンプレミスのGatewayのFQDNを入力し、 **［検出］** をクリックします。



Citrix Cloudが正常に検出したら、 **［続行］** をクリックします。

4. オンプレミスのGatewayとの接続を作成します。

   a. Citrix Cloudに表示されるクライアントID、シークレット、およびリダイレクトURLをコピーします。



ま

た、この情報のコピーをダウンロードし、参照用にオフラインで安全に保存してください。この情報は、生成後はCitrix Cloudでは利用できません。

b. Gatewayで、Citrix Cloudから取得したクライアントID、シークレット、およびリダイレクトURLを使用してOAuth IdP詳細ポリシーを作成します。手順については、以下の記事を参照してください。

- Citrix Gateway 12.1の場合: オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する
- Citrix Gateway 13.0の場合: オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する

c. **［テストして完了］** をクリックします。Citrix Cloudは、Gatewayに到達可能であり、正しく構成されていることを確認します。

5. ストアのCitrix Gateway認証を有効にする:

a. Citrix Cloudメニューから、**StoreFront Cloud**を選択します。

b. **認証**タブから、**Citrix Gateway**を選択します。

c. **エンドユーザーエクスペリエンスへの影響を理解しています**を選択し、**保存**をクリックします。

トラブルシューティング

最初のステップとして、この記事の前提条件と要件のセクションを確認してください。オンプレミス環境に必要なすべてのコンポーネントがあり、必要なすべての構成が行われていることを確認してください。これらの項目のいずれかが不足しているか、誤って構成されている場合、Citrix Gatewayを使用したストア認証は機能しません。

Citrix Cloudとオンプレミスgateway間の接続確立で問題が発生した場合は、次の項目を確認してください:

- Gateway FQDNがインターネットから到達可能であること。
- Citrix CloudにGateway FQDNを正しく入力していること。
- OAuth IdPポリシーの`-issuer`パラメーターにGateway URLを正しく入力していること。例: `-issuer https://GatewayFQDN.com`。`issuer`パラメーターは大文字と小文字を区別します。
- Citrix Cloudからのクライアントid、シークレット、およびリダイレクトURLの値が、OAuth IdPポリシーのClient ID、Client Secret、Redirect URL、およびAudienceフィールドに正しく入力されていること。ポリシーのAudienceフィールドに正しいクライアントIDが入力されていることを確認してください。
- OAuth IdP認証ポリシーが正しく構成されていること。手順については、次の記事を参照してください:
  - Citrix Gateway 12.1: Citrix CloudのIDプロバイダーとしてオンプレミスCitrix Gatewayを使用する
  - Citrix Gateway 13.0: Citrix CloudのIDプロバイダーとしてオンプレミスCitrix Gatewayを使用する
- 認証ポリシーのバインドに記載されているように、ポリシーがAAA認証サーバーに正しくバインドされていることを確認してください。

グローバルカタログサーバー

ユーザーアカウントの詳細を取得するだけでなく、Gateway はユーザーのドメイン名、AD NETBIOS 名、およびルート AD ドメイン名を取得します。AD NETBIOS 名を取得するために、

Gateway はユーザーアカウントが存在する AD を検索します。NETBIOS 名はグローバルカタログサーバーにはレプリケートされません。

AD 環境でグローバルカタログサーバーを使用している場合、これらのサーバーで構成された LDAP アクションは Citrix Cloud では機能しません。代わりに、LDAP アクションで個々の AD を構成する必要があります。複数のドメインまたはフォレストがある場合は、複数の LDAP ポリシーを構成できます。

Kerberos または IdP チェーンによるシングルサインオンのための AD 検索

エンドユーザーのサインインに Kerberos または SAML または OIDC プロトコルを使用する外部 ID プロバイダーを使用している場合は、AD ルックアップが構成されていることを確認してください。Gateway は、エンドユーザーの AD ユーザープロパティと AD 構成プロパティを取得するために AD ルックアップを必要とします。

認証がサードパーティサーバーによって処理される場合でも、LDAP ポリシーが構成されていることを確認してください。これらのポリシーを構成するには、次のタスクを実行して、既存のログインスキーマプロファイルに第2認証要素を追加します。

1. Active Directory から属性とグループの抽出のみを実行する LDAP 認証サーバーを作成します。
2. LDAP 高度認証ポリシーを作成します。
3. 認証ポリシーラベルを作成します。
4. プライマリ ID プロバイダーの後に、認証ポリシーラベルを次の要素として定義します。

LDAP を第2認証要素として追加するには

1. LDAP 認証サーバーを作成します。
    a. **システム > 認証 > 基本ポリシー > LDAP > サーバー > 追加** を選択します。
    b. 「**Create Authentication LDAP Server**」ページで、次の情報を入力します。
        - 「**Choose Server Type**」で、「**LDAP**」を選択します。
        - **Name** に、サーバーのわかりやすい名前を入力します。
        - **Server IP** を選択し、LDAPサーバーのIPアドレスを入力します。
        - **Security Type** で、必要なLDAPセキュリティの種類を選択します。
        - **Server Type** で、**AD** を選択します。

- **Authentication** では、チェックボックスを選択しないでください。この認証サーバーは、認証ではなく、Active Directoryからユーザー属性とグループを抽出するためのものであるため、このチェックボックスはオフにする必要があります。

c. **Other Settings** で、次の情報を入力します。

- **Server Logon Name Attribute** に、**UserPrincipalName** を入力します。
- **Group Attribute** で、**memberOf** を選択します。
- **Sub Attribute Name** で、**cn** を選択します。

2. LDAP高度認証ポリシーを作成します。

a. 「**セキュリティ > AAA - アプリケーショントラフィック > ポリシー > 認証 > 詳細ポリシー > ポリシー > 追加**」を選択します。

b. **Create Authentication Policy** ページで、次の情報を入力します。

- **Name** に、ポリシーのわかりやすい名前を入力します。
- **Action Type** で、**LDAP** を選択します。
- **Action** で、以前に作成したLDAP認証サーバーを選択します。
- 「**Expression**」に「**TRUE**」と入力します。

c. 構成を保存するには、**Create** をクリックします。

3. 認証ポリシーラベルを作成します。

a. **セキュリティ > AAA – アプリケーション トラフィック > ポリシー > 認証 > 高度なポリシー > ポリシーラベル > 追加**を選択します。

b. 「**Name**」に、認証ポリシーラベルのわかりやすい名前を入力します。

c. Login Schema で、**LSCHEMA_INT** を選択します。

d. 「**Policy Binding**」の下にある「**Select Policy**」で、以前作成したLDAP高度認証ポリシーを選択します。

e. 「**GoTo Expression**」で「**END**」を選択します。

f. 構成を完了するには、**Bind** をクリックします。

4. プライマリIDプロバイダーの後に、LDAP認証ポリシーラベルを次の要素として定義します。

a. **システム > セキュリティ > AAA - アプリケーション トラフィック > 仮想サーバー**を選択します。

b. プライマリIDプロバイダーのバインディングを含む仮想サーバーを選択し、**Edit** を選択します。

c. 「**Advanced Authentication Policies**」の下で、既存の「**Authentication Policy**」バインディングを選択します。

d. プライマリIDプロバイダーのバインディングを選択し、**Edit Binding** を選択します。

e. 「**Policy Binding**」ページで、「**Select Next Factor**」に、以前作成したLDAP認証ポリシーラベルを選択します。

f. 設定を保存するには、**バインド**をクリックします。

多要素認証の既定のパスワード

エンドユーザーに多要素認証 (MFA) を使用する場合、Gateway は最後の要素のパスワードをシングルサインオンの既定のパスワードとして使用します。このパスワードは、エンドユーザーがストアにサインインするときに Citrix Cloud に送信されます。環境内で LDAP 認証の後に別の要素が続く場合、Citrix Cloud に送信される既定のパスワードとして LDAP パスワードを設定する必要があります。LDAP 要素に対応するログインスキーマで **SSOCredentials** を有効にします。

詳細情報

Citrix Tech Zone: 技術インサイト: 認証 - Gateway

Google Cloud Identity を IDプロバイダー として Citrix Cloud™ に接続する

Citrix Cloud は、エンドユーザーがストアにサインインする際の認証に Google Cloud Identity を IDプロバイダー として使用することをサポートしています。組織のGoogleアカウントをCitrix Cloudに接続することで、Citrix® StoreFront CloudとGoogleリソースへのアクセスに統一されたサインインエクスペリエンスを提供できます。

ドメイン参加済みおよび非ドメイン参加済み構成の要件

ドメイン参加済みまたは非ドメイン参加済みのマシンを使用して、Citrix Cloud で Google Cloud Identity を IDプロバイダー として構成できます。

- ドメイン参加済みとは、マシンがオンプレミスの Active Directory (AD) のドメインに参加しており、認証にそこに保存されているユーザープロファイルを使用することを意味します。
- 非ドメイン参加済みとは、マシンが AD ドメインに参加しておらず、認証に Google Workspace ディレクトリに保存されているユーザープロファイル（Googleネイティブユーザーとも呼ばれる）を使用することを意味します。

次の表に、各構成タイプの要件を示します。

要件	ドメイン参加済み	非ドメイン参加済み	詳細情報
オンプレミス AD	はい	いいえ	この記事の「Active Directory と Citrix Cloud Connector の準備」を参照してください。
リソースの場所に展開されたCitrix Cloud Connector	はい	いいえ。ドメインに参加していないマシンにアクセスするためにCloud Connectorは必要ありません。	この記事の「Active DirectoryとCitrix Cloud Connectorの準備」を参照してください。
Google CloudとのAD同期	Gatewayサービスとその他のサービスを使用しない場合にのみオプションです。それ以外の場合は、このタスクが必要です。	いいえ	この記事の「Active DirectoryをGoogle Cloud Identityと同期する」を参照してください。
Google Cloud Platformコンソールにアクセスできる開発者アカウント。サービスアカウントとキーの作成、およびAdmin SDK APIの有効化に使用されます。	はい	はい	この記事の「サービスアカウントの作成」、「サービスアカウントキーの作成」、および「ドメイン全体の委任の構成」を参照してください。
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。ドメイン全体の委任と読み取り専用APIユーザーアカウントの構成に使用されます。	はい	はい	この記事の「ドメイン全体の委任を構成する」と「読み取り専用APIユーザーアカウントを追加する」を参照してください。

複数のCitrix Cloudアカウントでの認証

この記事では、Google Cloud Identityを単一のCitrix CloudアカウントのIDプロバイダーとして接続する方法について説明します。複数のCitrix Cloudアカウントをお持ちの場合、同じサービスアカウントと読み取り専用APIユーザーアカウントを使用して、それぞれを同じGoogle Cloudアカウントに接続できます。Citrix Cloudにサインインし、顧客ピッカーから適切な顧客IDを選択するだけです。

アクティブディレクトリとCitrix Cloud コネクタの準備

Google Cloud Identityで**ドメイン参加済み**マシンを使用している場合は、このセクションを使用してオンプレミスADを準備します。ドメインに参加していないマシンを使用している場合は、このタスクをスキップして、この記事の「サービスアカウントを作成する」に進んでください。

Citrix Cloud Connectorソフトウェアをインストールするには、Active Directoryドメイン内に少なくとも2台のサーバーが必要です。Cloud Connectorは、Citrix Cloudとリソースの場所間の通信を可能にするために必要です。Citrix Cloudとの高可用性接続を確保するには、少なくとも2台のCloud Connectorが必要です。これらのサーバーは、次の要件を満たしている必要があります。

- Cloud Connectorのシステム要件に記載されている要件を満たしていること。
- 他のCitrix®コンポーネントがインストールされておらず、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とって重要なマシンではないこと。
- Active Directory（AD）ドメインに参加していること。ストアのリソースとユーザーが複数のドメインに存在する場合は、各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。詳しくは、「Active DirectoryでのCloud Connectorの展開シナリオ」を参照してください。
- ユーザーがクラウドストアを介してアクセスするリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。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。

アクティブディレクトリとグーグルクラウドアイデンティティの同期

Google Cloud Identityで**ドメイン参加済み**マシンを使用している場合は、このセクションを使用してオンプレミスADを準備します。ドメインに参加していないマシンを使用している場合は、このタスクをスキップして、この記事の「サービスアカウントを作成する」に進んでください。

Citrix Gatewayサービスのみを使用し、他のサービスが有効になっていない場合、ADとGoogle Cloud Identityの同期はオプションです。これらのサービスのみの場合、ADと同期する必要なく、Googleネイティブユーザーを使用できます。

他のCitrix Cloudサービスを使用している場合、ADとGoogle Cloud Identityの同期が必要です。Google Cloudは、以下のADユーザー属性をCitrix Cloudに渡す必要があります。

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

ADをGoogle Cloudと同期するには

1. Googleウェブサイトから、Google Cloud Directory Syncユーティリティをダウンロードしてインストールします。このユーティリティの詳細については、GoogleウェブサイトのGoogle Cloud Directory Syncドキュメントを参照してください。
2. ユーティリティのインストール後、Configuration Managerを起動します（**スタート > Configuration Manager**）。
3. ユーティリティドキュメントのConfiguration Managerで同期を設定するに記載されているように、Googleドメイン設定とLDAP設定を指定します。
4. **General Settings**で、**Custom Schemas**を選択します。デフォルトの選択は変更しないでください。
5. すべてのユーザーアカウントに適用するカスタムスキーマを設定します。このセクションで指定されているとおりの正確な大文字/小文字とスペルを使用して、必要な情報を入力します。

    a. **Custom Schemas**タブを選択し、**Add Schema**を選択します。

    b. **Use rules defined in "User Accounts"**を選択します。

    c. **Schema Name**に「**citrix-schema**」と入力します。

    d. **Add Field**を選択し、以下の情報を入力します。

        - **Schema field template**の下にある**Schema Field**で、**userPrincipalName**を選択します。
        - 「**Googleフィールドの詳細**」で、「**フィールド名**」に「**UPN**」と入力します。

    e. 手順4を繰り返して、以下のフィールドを作成します。

        - objectGUID: 「**スキーマフィールドテンプレート**」で「**objectGUID**」を選択します。「**Googleフィールドの詳細**」で「**objectGUID**」と入力します。

- SID: 「**スキーマフィールドテンプレート**」で「**カスタム**」を選択します。「**Google フィールドの詳細**」で「**SID**」と入力します。
- objectSID: 「**スキーマフィールドテンプレート**」で「**カスタム**」を選択します。「**Googleフィールドの詳細**」で「**objectSID**」と入力します。

f. 「**OK**」を選択して、エントリを保存します。

6. 組織の残りの設定を完了し、ユーティリティドキュメントのConfiguration Managerとの同期を設定するに記載されているように同期設定を確認します。
7. 「**変更を同期して適用**」を選択して、Active DirectoryをGoogleアカウントと同期します。

同期が完了すると、Google Cloudのユーザー情報セクションにユーザーのActive Directory情報が表示されます。

サービスアカウントを作成する

このタスクを完了するには、Google Cloud Platform開発者アカウントが必要です。

1. https://console.cloud.google.comにサインインします。
2. ダッシュボードのサイドバーから「**IAMと管理**」を選択し、次に「**サービスアカウント**」を選択します。
3. 「**サービスアカウントを作成**」を選択します。
4. 「**サービスアカウントの詳細**」で、サービスアカウント名とサービスアカウントIDを入力します。
5. 「**完了**」を選択します。

サービスアカウントキーを作成する

1. 「**サービスアカウント**」ページで、作成したばかりのサービスアカウントを選択します。
2. 「**キー**」タブを選択し、「**キーを追加 > 新しいキーを作成**」を選択します。
3. デフォルトのJSONキータイプオプションが選択されたままにします。
4. 「**作成**」を選択します。キーは後でアクセスできる安全な場所に保存してください。Google Cloud IdentityをIDプロバイダーとして接続する際に、Citrix Cloudコンソールで秘密鍵を入力します。

ドメイン全体の委任を構成する

1. Admin SDK APIを有効にします。

a. Google Cloud Platformメニューから、「**APIとサービス > 有効なAPIとサービス**」を選択します。

b. コンソールの上部にある「**APIとサービスを有効にする**」を選択します。APIライブラリのホームページが表示されます。

c. 「**Admin SDK API**」を検索し、結果リストから選択します。

d. 「**有効にする**」を選択します。

2. サービスアカウントのAPIクライアントを作成します。

a. Google Cloud Platformメニューから、「**IAMと管理 > サービスアカウント**」を選択し、以前に作成したサービスアカウントを選択します。

b. サービスアカウントの「**詳細**」タブから、「**詳細設定**」を展開します。

c. **Domain-wide Delegation**の下で、クライアントIDをコピーし、**View Google Workspace Admin Console**を選択します。

d. 該当する場合は、使用するGoogle Workspace管理者アカウントを選択します。Google管理コンソールが表示されます。

e. Google管理サイドバーから、**Security > Access and data control > API controls**を選択します。

f. **Domain wide delegation**の下で、**Manage Domain Wide Delegation**をクリックします。

g. **Add new**を選択します。

h. **Client ID**に、手順CでコピーしたサービスアカウントのクライアントIDを貼り付けます。

i. **OAuth scopes**に、以下のスコープを単一のカンマ区切り行で入力します。

```
https://www.googleapis.com/auth/
admin.directory.user.readonly,https://www.googleapis.com/auth/
admin.directory.group.readonly,https://www.googleapis.com/auth/
admin.directory.domain.readonly
```

j. **Authorize**を選択します。

読み取り専用APIユーザーアカウントを追加する

このタスクでは、Citrix Cloudの読み取り専用APIアクセス権を持つGoogle Workspaceユーザーアカウントを作成します。このアカウントは他の目的には使用されず、他の特権も持ちません。

1. Google管理メニューから、**Directory > Users**を選択します。
2. **Add new user**を選択し、適切なユーザー情報を入力します。

3. **Add new user**を選択して、アカウント情報を保存します。
4. 読み取り専用ユーザーアカウントのカスタムロールを作成します。
    a. Google管理メニューから、**Account > Admin roles**を選択します。
    b. 「**新しいロールを作成**」を選択します。
    c. 新しいロールの名前を入力します。例: API-ReadOnly
    d. 「**続行**」を選択します。
    e. 「**管理者API権限**」の下で、次の権限を選択します。
        - ユーザー > 読み取り
        - グループ > 読み取り
        - ドメイン管理
    f. 「**続行**」を選択し、次に「**ロールを作成**」を選択します。
5. 以前に作成した読み取り専用ユーザーアカウントにカスタムロールを割り当てます。
    a. カスタムロールの詳細ページから、**管理者**ペインで「**ユーザーを割り当てる**」を選択します。
    b. 読み取り専用ユーザーアカウントの名前を入力し始め、ユーザーリストから選択します。
    c. 「**ロールを割り当てる**」を選択します。
    d. ロールの割り当てを確認するには、ユーザーページ（**ディレクトリ > ユーザー**）に戻り、読み取り専用ユーザーアカウントを選択します。カスタムロールの割り当ては「**管理者ロールと権限**」の下に表示されます。

Google Cloud IdentityをCitrix Cloudに接続する

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、 を選択します。
3. を見つけて、省略記号メニューから を選択します。
4. プロンプトが表示されたら、会社用の短くURLフレンドリーな識別子を入力し、 を選択します。選択する識別子は、Citrix Cloud内でグローバルに一意である必要があります。
5. を選択し、サービスアカウントのキーを作成したときに保存したJSONファイルを選択します。この操作により、プライベートキーと、作成したGoogle Cloudサービスアカウントのメールアドレスがインポートされます。
6. に、読み取り専用APIユーザーアカウントの名前を入力します。

7. を選択します。Citrix CloudはGoogleアカウントの詳細を確認し、接続をテストします。
8. リストされている関連ドメインを確認します。正しければ、 を選択して構成を保存します。

Citrix Cloudに管理者を追加する

Google Cloudを介して、個々のCitrix Cloud管理者と管理者グループを追加できます。詳しくは、以下の記事を参照してください。

- 個々の管理者向け：Citrix Cloudへの管理者アクセスを管理する
- 管理者グループ向け：管理者グループを管理する

Citrix Cloudに管理者を追加すると、以下のいずれかの方法でサインインできます。

- Google CloudをIDプロバイダーとして最初に構成したときに設定した管理者サインインURLに移動します。例：`https://citrix.cloud.com/go/mycompany`
- Citrix Cloudサインインページから、 を選択し、会社の一意の識別子（例：「mycompany」）を入力して、 をクリックします。

ストア認証のためにGoogle Cloud Identityを有効にする

1. 「Citrix Cloud」メニューから、「**StoreFront Cloud > 認証**」を選択します。
2. 「**Google Cloud Identity**」を選択します。プロンプトが表示されたら、「**エンドユーザーエクスペリエンスへの影響を理解しています**」を選択し、「**保存**」をクリックします。

Okta を ID プロバイダーとして Citrix Cloud™ に接続する

Citrix Cloud は、Okta を ID プロバイダーとして使用し、ストアにサインインするエンドユーザーを認証することをサポートしています。Okta 組織を Citrix Cloud に接続することで、エンドユーザーが Citrix® StoreFront Cloud のリソースにアクセスするための共通のサインインエクスペリエンスを提供できます。

StoreFront Cloud で Okta 認証を有効にすると、エンドユーザーのサインインエクスペリエンスが変わります。Okta 認証を選択すると、フェデレーションサインインが提供され、シングルサインオンではありません。エンドユーザーは Okta のサインインページからストアにサインインしますが、Citrix DaaS (旧 Citrix Virtual Apps and Desktops サービス) からアプリやデスクトップを開く際に、2 回目の認証が必要になる場合があります。シングルサインオンを有効にし、2 回目のログオンプロンプトを防ぐには、Citrix Federated Authentication Service を Citrix Cloud とともに使用する必要があります。詳細については、「Citrix Federated Authentication Service を Citrix Cloud に接続する」を参照してください。

前提条件

クラウドコネクタまたはコネクタアプライアンス

Citrix Cloud と リソースの場所 間の通信を有効にするには、Cloud Connector または Connector Appliance のいずれかが必要です。Citrix Cloud との高可用性接続を確保するには、少なくとも 2 つの Cloud Connector または Connector Appliance が必要です。Active Directory ドメインに参加しているコネクタが少なくとも 2 つ必要です。これらは Cloud Connector または Connector Appliance のいずれかです。

コネクタは次の要件を満たしている必要があります。

- 各ドキュメントに記載されている要件を満たしていること
- Active Directory (AD) ドメインに参加していること。ストアユーザーが複数のドメインに存在する場合、Connector Appliance のマルチドメイン機能 を使用して複数のドメインに参加できます。
- ユーザーがクラウドストアを介してアクセスするリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「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。 Connector Appliance のインストールについて詳しくは、「Connector Appliance のインストール」を参照してください。

Okta ドメイン

Okta を Citrix Cloud に接続する際は、組織の Okta ドメインを指定する必要があります。Citrix は以下の Okta ドメインをサポートしています。

- okta.com
- オクタ・イーユー・ドットコム
- oktapreview.com

Citrix CloudでOktaカスタムドメインを使用することもできます。カスタムドメインの使用に関する重要な考慮事項については、Okta WebサイトのOkta URLドメインのカスタマイズを参照してください。

組織のカスタムドメインの特定に関する詳細については、Okta WebサイトのOktaドメインの検索を参照してください。

Okta OIDC Webアプリケーション

OktaをIDプロバイダーとして使用するには、まずCitrix Cloudで使用できるクライアント資格情報を持つOkta OIDC Webアプリケーションを作成する必要があります。アプリケーションを作成および構成したら、クライアントIDとクライアントシークレットをメモしてください。Okta組織を接続する際に、これらの値をCitrix Cloudに提供します。

このアプリケーションを作成および構成するには、この記事の以下のセクションを参照してください。

- Okta OIDC Webアプリ統合の作成
- Okta OIDC Webアプリケーションの構成

ストアURL

Oktaアプリケーションを作成する際には、Citrix CloudからストアURLを提供する必要があります。ストアURLを見つけるには、Citrix Cloudメニューから**StoreFront Cloud**を選択します。ストアURLは**アクセス**タブに表示されます。

> **重要:**
>
> 後でストアURLを変更する場合は、Oktaアプリケーション構成を新しいURLで更新する必要があります。そうしないと、エンドユーザーがストアからのログオフで問題が発生する可能性があります。

Okta APIトークン

Citrix CloudでOktaをIDプロバイダーとして使用するには、Okta組織のAPIトークンが必要です。このトークンは、Okta組織の読み取り専用管理者アカウントを使用して作成します。このトークンは、Okta組織のユーザーとグループを読み取ることができる必要があります。

APIトークンを作成するには、この記事のOkta APIトークンを作成するを参照してください。APIトークンに関する詳細については、Okta WebサイトのAPIトークンを作成するを参照してください。

> **重要:**
>
> APIトークンを作成する際は、トークン値（例えば、一時的にプレーンテキストドキュメントに値をコピーするなど）をメモしておいてください。Oktaはこの値を一度しか表示しない

ため、Citrix CloudをOkta組織に接続するの手順を実行する直前にトークンを作成することをお勧めします。

Okta ADエージェントを使用してActive DirectoryアカウントをOktaに同期する

OktaをIDプロバイダーとして使用するには、まずオンプレミスのADをOktaと統合する必要があります。これを行うには、Okta ADエージェントをドメインにインストールし、ADをOkta組織に追加します。Okta ADエージェントの展開に関するガイダンスについては、Okta WebサイトのActive Directory統合の開始を参照してください。

その後、ADユーザーとグループをOktaにインポートします。インポートする際は、ADアカウントに関連付けられている以下の値を含めてください。

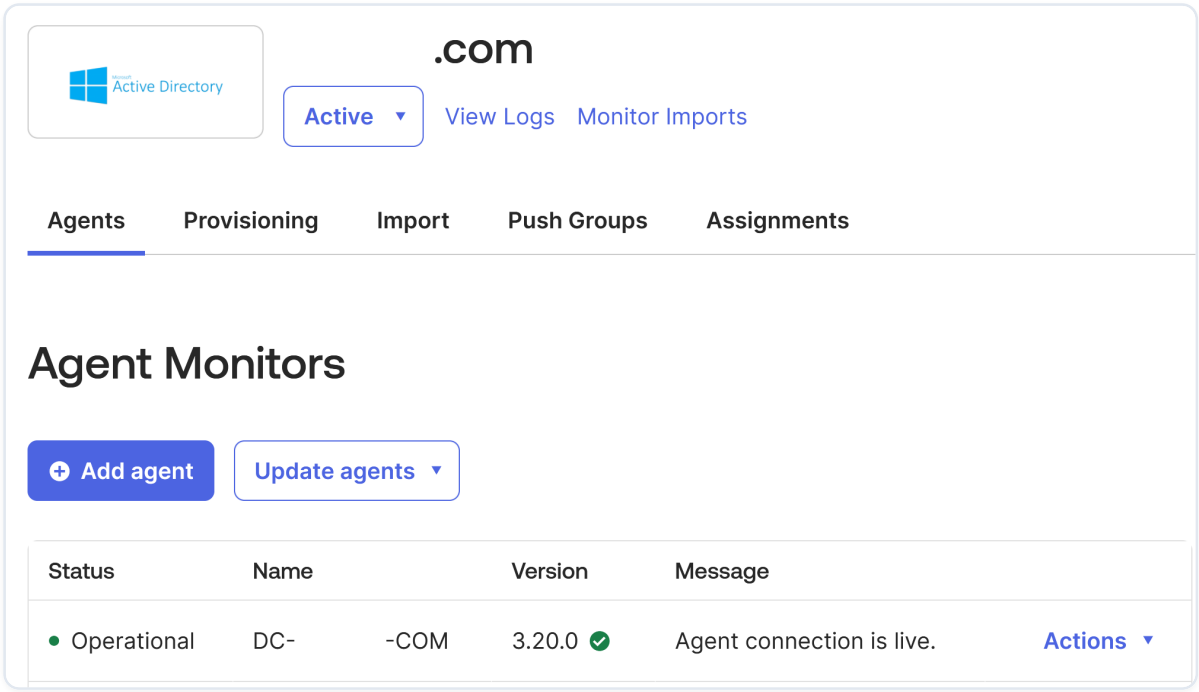
- メール
- SID
- UPN
- OID

注：

ストア付きのCitrix Gatewayサービスを使用している場合、ADアカウントをOkta組織と同期する必要はありません。

ADユーザーとグループをOkta組織と同期するには：

1. Okta ADエージェントをインストールして構成します。完全な手順については、Okta Webサイトの以下の記事を参照してください。
    - Okta Active Directoryエージェントをインストールする
    - Active Directory のインポートとアカウント設定を構成する
    - Active Directory のプロビジョニング設定を構成する



2. 手動インポートまたは自動インポートを実行して、ADユーザーとグループをOktaに追加します。Oktaのインポート方法と手順の詳細については、Okta WebサイトのActive Directoryユーザーとグループの管理を参照してください。

Okta OIDC Webアプリ統合を作成する

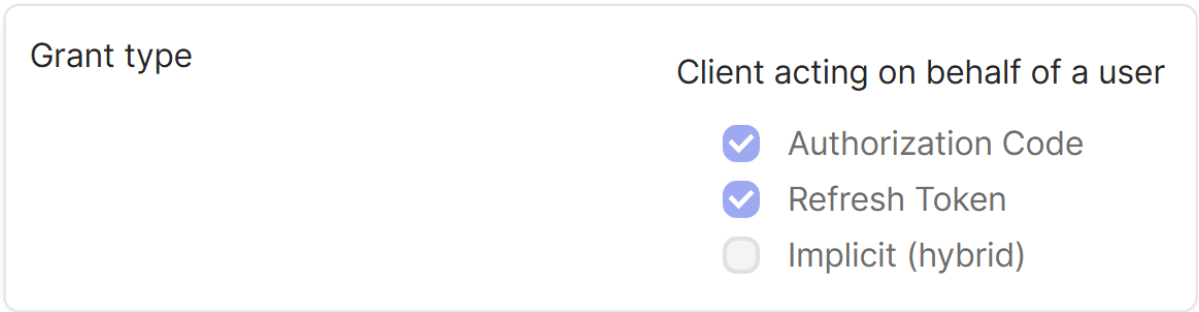
1. Okta管理コンソールで、**Applications**の下にある**Applications**を選択します。
2. **Create App Integration**を選択します。
3. **Sign in method**で、**OIDC - OpenID Connect**を選択します。
4. **Application type**で、**Web Application**を選択します。**Next**を選択します。
5. **App Integration Name**に、アプリ統合のわかりやすい名前を入力します。
6. **Grant type**で、**Authorization Code**を選択します（デフォルトで選択されています）。
7. **Sign-in redirect URIs**に、`https://accounts.cloud.com/core/login-okta`を入力します。
   - Citrix Cloudのお客様が欧州連合、米国、またはアジア太平洋南部地域にいる場合は、`https://accounts.cloud.com/core/login-okta`を入力します。
   - Citrix Cloudのお客様が日本地域にいる場合は、`https://accounts.citrixcloud.jp/core/login-okta`を入力します。
   - Citrix Cloudのお客様がCitrix Cloud Government地域にいる場合は、`https://accounts.cloud.us/core/login-okta`を入力します。
8. 「**サインアウト リダイレクト URI**」に、Citrix Cloud のストア URL を入力します。

9. ストアのカスタムドメインも使用している場合は、それも入力する必要があります。例:
   - `https://workspaceurl1.cloud.com`
   - `https://workspaceurl2.cloud.com`
   - `https://workspaceurl1.mycustomdomain.com`
10. 「**割り当て**」の「**制御されたアクセス**」で、アプリ統合を組織内の全員に割り当てるか、指定したグループのみに割り当てるか、または後でアクセスを割り当てるかを選択します。
11. 「**保存**」を選択します。アプリ統合を保存すると、コンソールにアプリケーション構成ページが表示されます。
12. 「**クライアント資格情報**」セクションで、「**クライアント ID**」と「**クライアント シークレット**」の値をコピーします。これらの値は、Citrix Cloud を Okta 組織に接続するときに使用します。

Okta OIDC Web アプリケーションを構成する

この手順では、Citrix Cloud に必要な設定で Okta OIDC Web アプリケーションを構成します。Citrix Cloud は、エンドユーザーがストアにサインインするときに Okta を介して認証するために、これらの設定を必要とします。

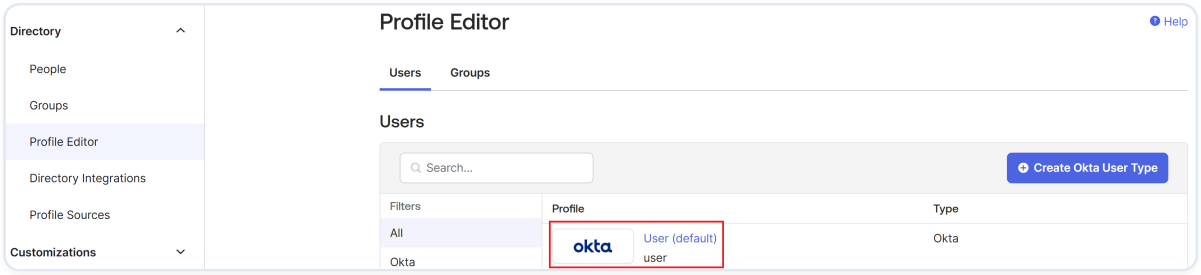
1. (オプション) 暗黙的な許可タイプに対するクライアント権限を更新します。この許可タイプに対して最小限の特権を許可することを希望する場合は、この手順を実行することを選択できます。
   a. Okta アプリケーション構成ページから、「**一般**」タブで「**一般設定**」セクションまでスクロールし、「**編集**」を選択します。
   b. 「**アプリケーション**」セクションの「**許可タイプ**」で、「**ユーザーに代わって動作するクライアント**」の下にある「**暗黙的な許可タイプでアクセストークンを許可する**」設定をオフにします。



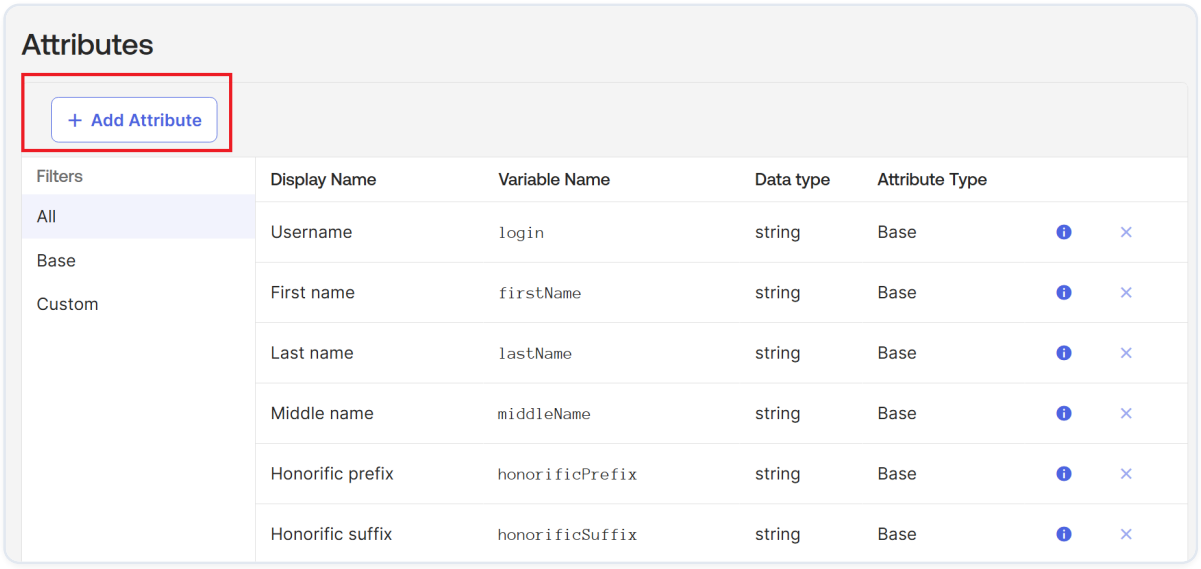
   c. 「**保存**」を選択します。
2. アプリケーション属性を追加します。これらの属性は大文字と小文字を区別します。

a. Oktaコンソールメニューから、**Directory > Profile Editor**を選択します。

b. Oktaの**User (default)プロファイルを選択します。OktaはUser**プロファイルページを表示します。

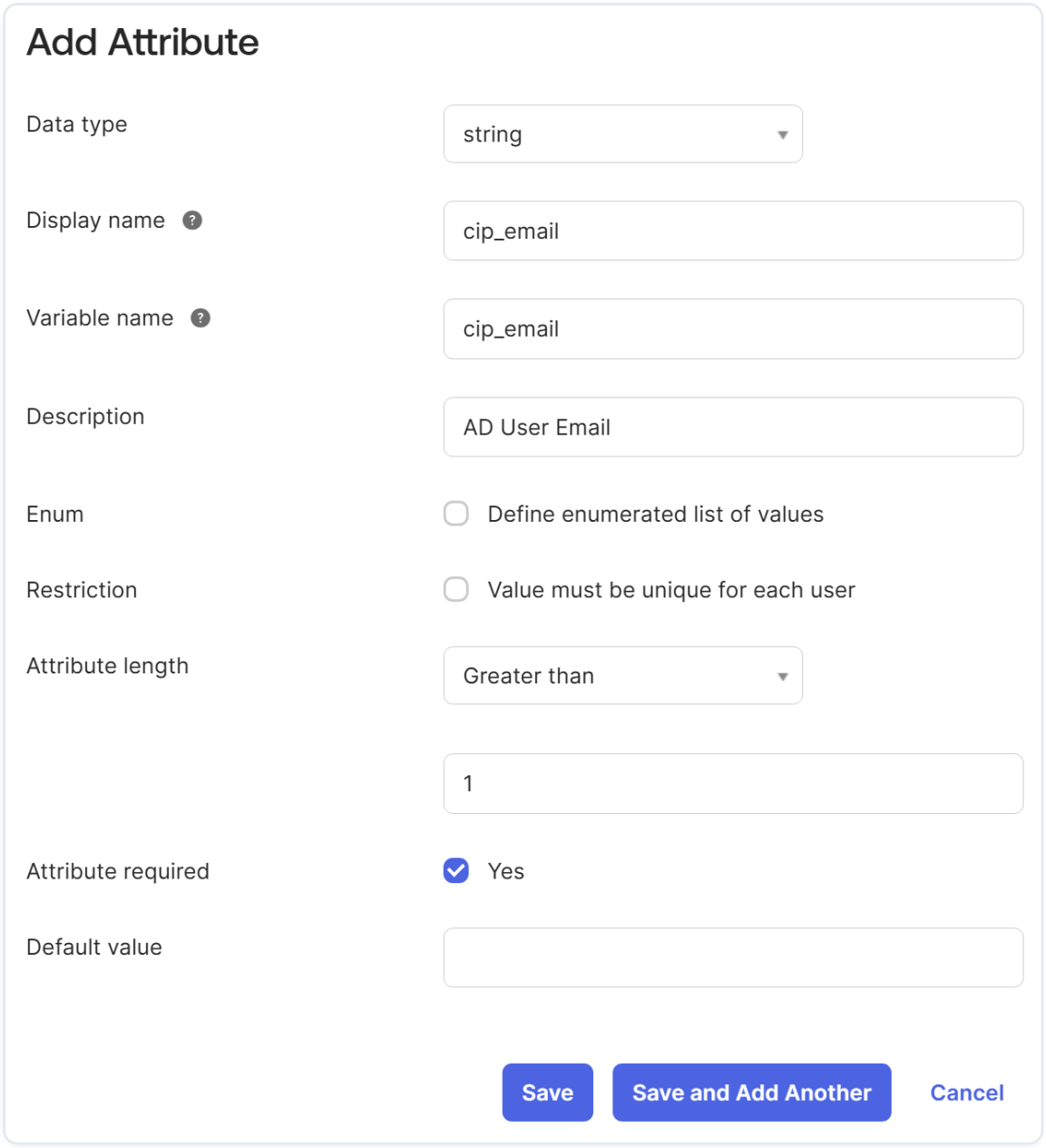


c. **Attributes**の下で、**Add attribute**を選択します。



d. 次の情報を入力します。

- 表示名: cip_email
- 変数名: cip_email
- 説明: AD User Email
- 属性の長さ: **Greater than**を選択し、**1**を入力します。
- 属性は必須: はい



e. **Save and Add Another**を選択します。

f. 次の情報を入力します。

- 表示名: cip_sid
- 変数名: cip_sid
- 説明: ADユーザーセキュリティ識別子
- 属性の長さ: 「**より大きい**」を選択し、「**1**」と入力します。
- 属性は必須: はい

g. 「**保存して別の項目を追加**」を選択します。

h. 次の情報を入力します。

- 表示名: cip_upn
- 変数名: cip_upn
- 説明: ADユーザープリンシパル名
- 属性の長さ: 「**より大きい**」を選択し、「**1**」と入力します。
- 属性は必須: はい

i. 「**保存して別の項目を追加**」を選択します。

j. 次の情報を入力します。

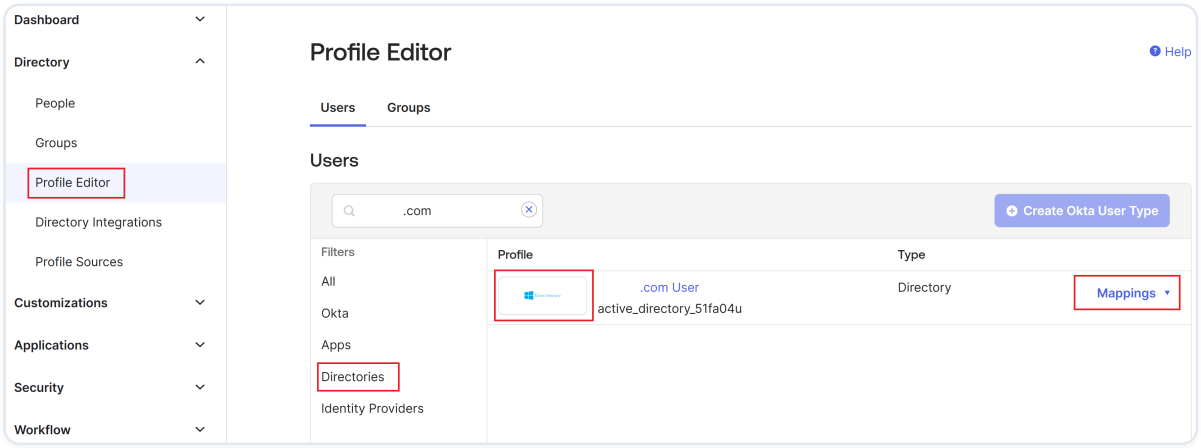
- 表示名: cip_oid
- 変数名: cip_oid
- 説明: AD ユーザー GUID
- 属性の長さ: **次より大きい**を選択し、**1**と入力します。
- 属性は必須: はい

k. **保存**を選択します。

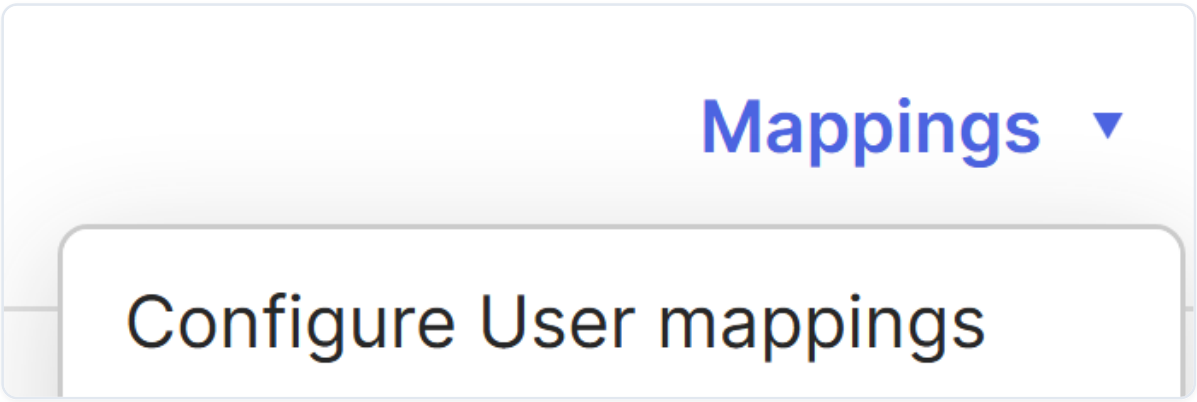
3. アプリケーションの属性マッピングを編集します:

a. Okta コンソールから、**Directory > Profile Editor > Directories**を選択します。

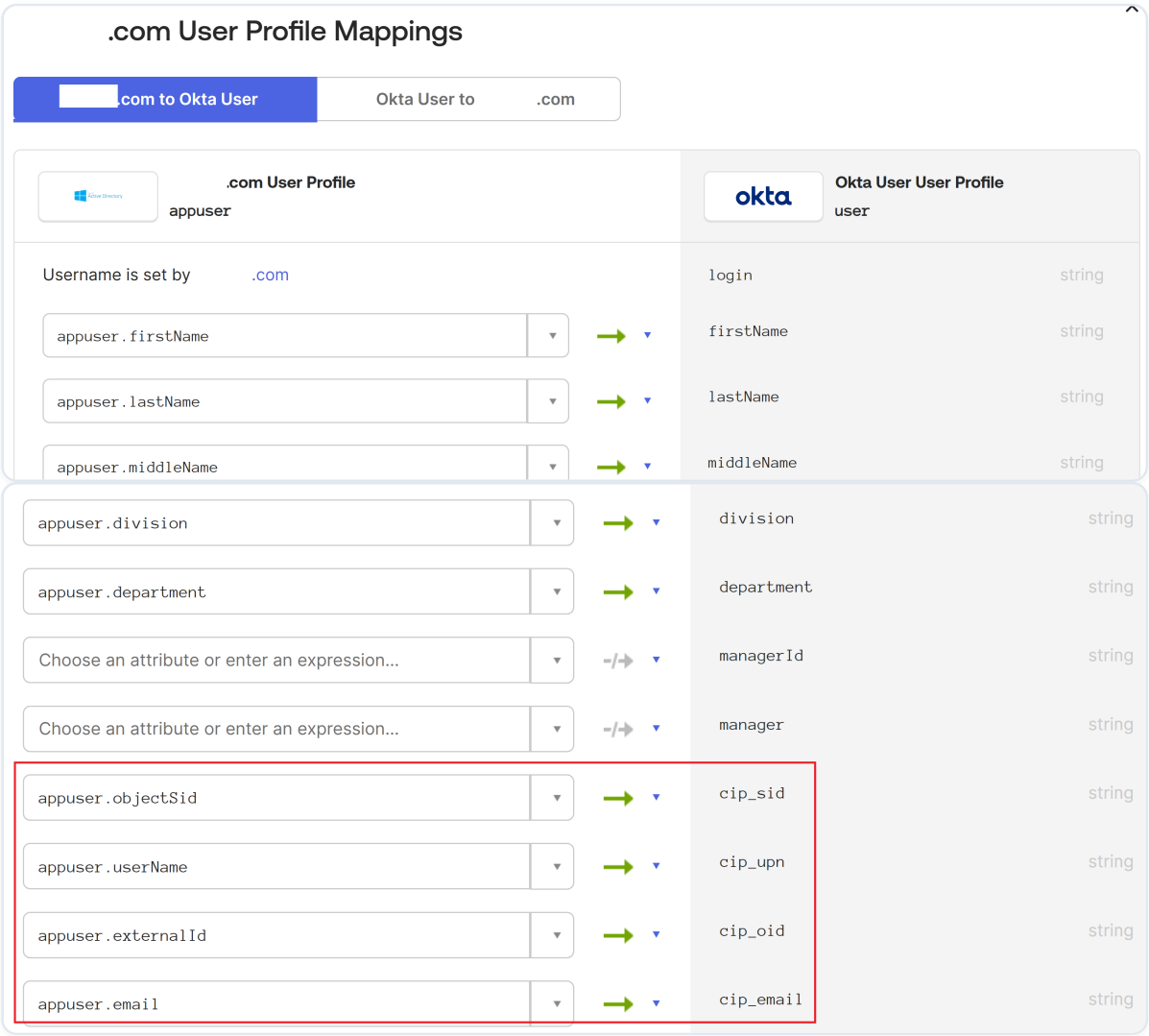
b. AD の **active_directory** プロファイルを見つけます。このプロファイルは、`myDomain User` の形式でラベル付けされている場合があります。ここで、`myDomain` は統合された AD ドメインの名前です。



c. **マッピング**を選択します。AD ドメインのユーザープロファイルマッピングページが表示され、AD を Okta ユーザーにマッピングするためのタブが選択されます。



d. **Okta User User Profile** 列で、手順 2 で作成した属性を見つけ、次のようにマッピングします:



- `cip_email` については、ドメインのユーザープロファイル列から `email` を選択します。選択すると、マッピングは `appuser.email` のように表示されます。
- 「`cip_sid`」については、お使いのドメインのユーザープロファイル列から「`objectSid`」を選択します。選択すると、マッピングは「`appuser.objectSid`」と表示されます。

- 「`cip_upn`」については、お使いのドメインのユーザープロファイル列から「`userName`」を選択します。選択すると、マッピングは「`appuser.userName`」と表示されます。
- 「`cip_oid`」については、お使いのドメインのユーザープロファイル列から「`externalId`」を選択します。選択すると、マッピングは「`appuser.externalId`」と表示されます。

e. を選択します。

f. を選択します。Oktaはマッピングを適用するジョブを開始します。

g. OktaをADと同期します。

i. Oktaコンソールから、 **>** を選択します。

ii. 統合されたADを選択します。

iii. タブを選択します。

iv. の下で、 を選択します。

v. セクションまでスクロールし、 を選択します。

Okta APIトークンを作成する

1. 読み取り専用管理者アカウントを使用してOktaコンソールにサインインします。
2. Oktaコンソールメニューから、 **>** を選択します。
3. タブを選択し、 を選択します。
4. トークンの名前を入力します。
5. **Create Token** を選択します。
6. トークン値をコピーします。この値は、Okta組織をCitrix Cloudに接続するときに指定します。

Citrix CloudをOkta組織に接続する

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、**Identity and Access Management** を選択します。
3. **Okta** を見つけて、省略記号メニューから **Connect** を選択します。
4. **Okta URL** に、Oktaドメインを入力します。
5. **Okta API Token** に、Okta組織のAPIトークンを入力します。
6. **Client ID** と **Client Secret** に、以前作成したOIDC Webアプリ統合のクライアントIDとシークレットを入力します。これらの値をOktaコンソールからコピーするには、**Applications** を選

択し、Oktaアプリケーションを見つけます。**Client Credentials** の下で、各値の **Copy to Clipboard** ボタンを使用します。

7. **Test and Finish** をクリックします。Citrix CloudはOktaの詳細を確認し、接続をテストします。

接続が正常に検証されたら、エンドユーザーに対してOkta認証を有効にできます。

ストアのOkta認証を有効にする

1. Citrix Cloudメニューから、**StoreFront Cloud > Authentication** を選択します。
2. **Okta** を選択します。
3. プロンプトが表示されたら、**エンドユーザーエクスペリエンスへの影響を理解しています**を選択します。
4. **保存**を選択します。

Okta認証に切り替えると、Citrix Cloudは一時的にストアを数分間無効にします。ストアが再度有効になると、エンドユーザーはOktaを使用してサインインできます。

詳細情報

- Citrix テックゾーン:
  - テックインサイト: 認証 - Okta
  - テックブリーフ: ワークスペース ID
  - テックブリーフ: ワークスペース SSO

トラブルシューティング

問題1

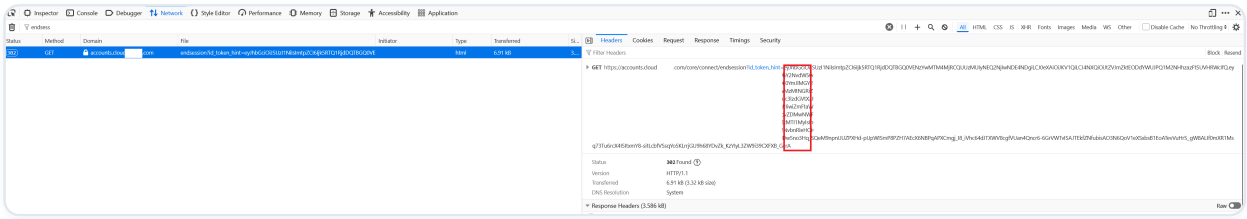
ストアへのOkta OIDC認証は成功しますが、ストア内でエンドユーザーのDaaSリソースが表示されません。これは、「ctx_user.sid」のような不足しているクレームがDaaSに送信されていないことが原因である可能性があります。

デバッグ手順1

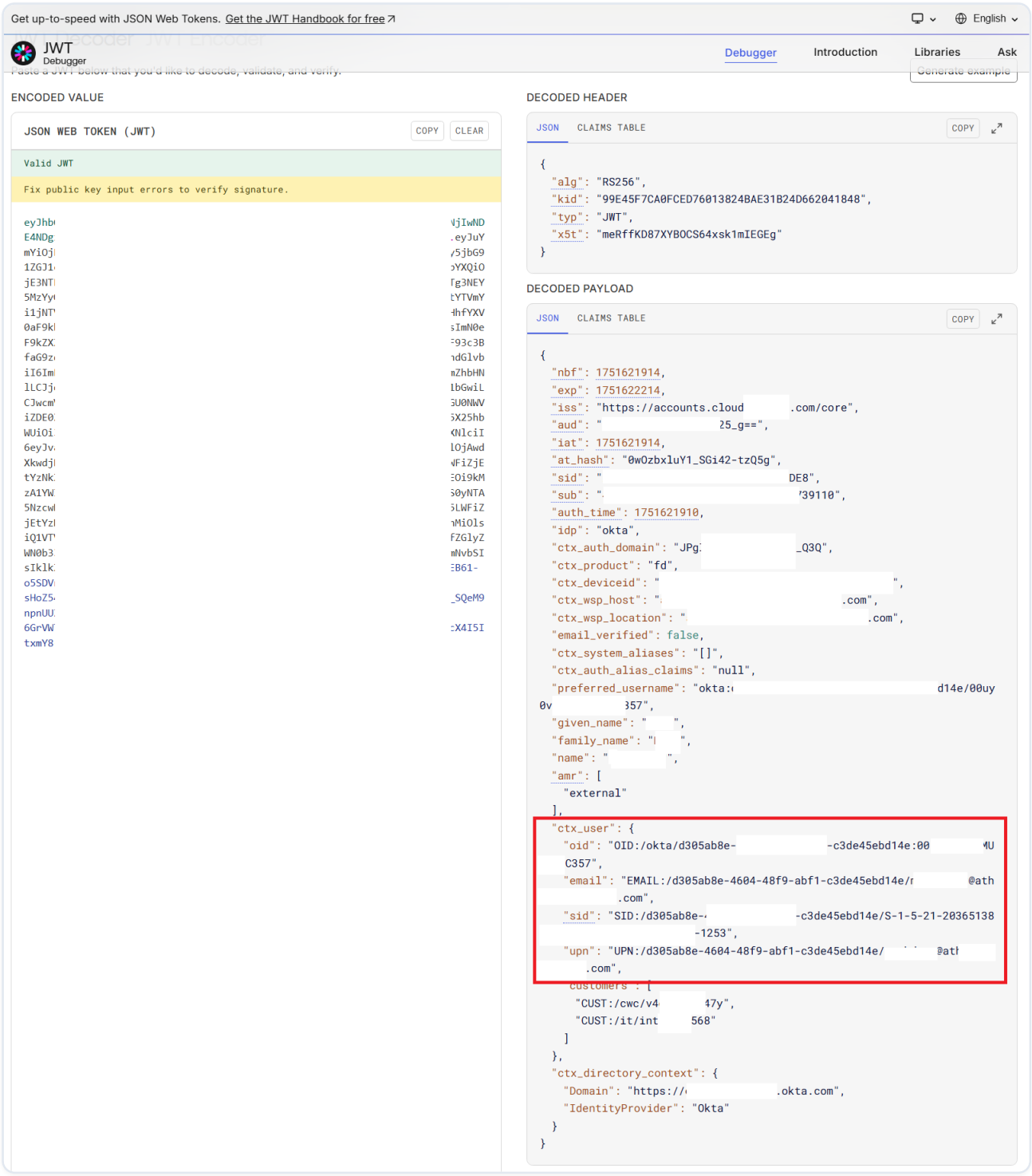
1. ブラウザを使用してHARファイルをキャプチャし、Okta OIDC認証を使用してストアにログインし、その後ストアからログアウトします。
2. ユーザーがストアから明示的なログアウトアクションを実行したときに、ブラウザの開発者ツール内で次の呼び出しを見つけます

GET `https://accounts.cloud.com/core/connect/endsession?id_token_hint=<base64string>`

3. `?id_token_hint=`の後のbase64文字列（JWTを含む）をコピーします。これはFireFox開発ツールからの例です。



このbase64文字列を`https://jwt.io`内の「Encoded Value JSON WEB TOKEN (JWT)」フィールドに貼り付け、Citrix CloudがOkta OIDCアプリケーションから受け取ったクレームを調べます。`"ctx_user": {}`内に必要なすべてのクレームが存在し、各クレームにストアにログインしたユーザーの正しいユーザーデータが含まれていることを確認します。`"ctx_user": {}`内に`"oid", "email", "sid", and "upn"`という名前の4つのクレームがあることを確認します。デコードされたJWTの例。



原因 1

お使いのOkta OIDCアプリケーションが必要な4つのcip_*クレームすべてを送信していないか、お使いのOktaユーザープロファイルに必要な属性が含まれていません。

解決策 1

Okta OIDCアプリケーションの設定とOktaユーザープロファイルの属性マッピングを確認してください。Okta OIDCアプリが正しいクレームを送信していることを確認してください。

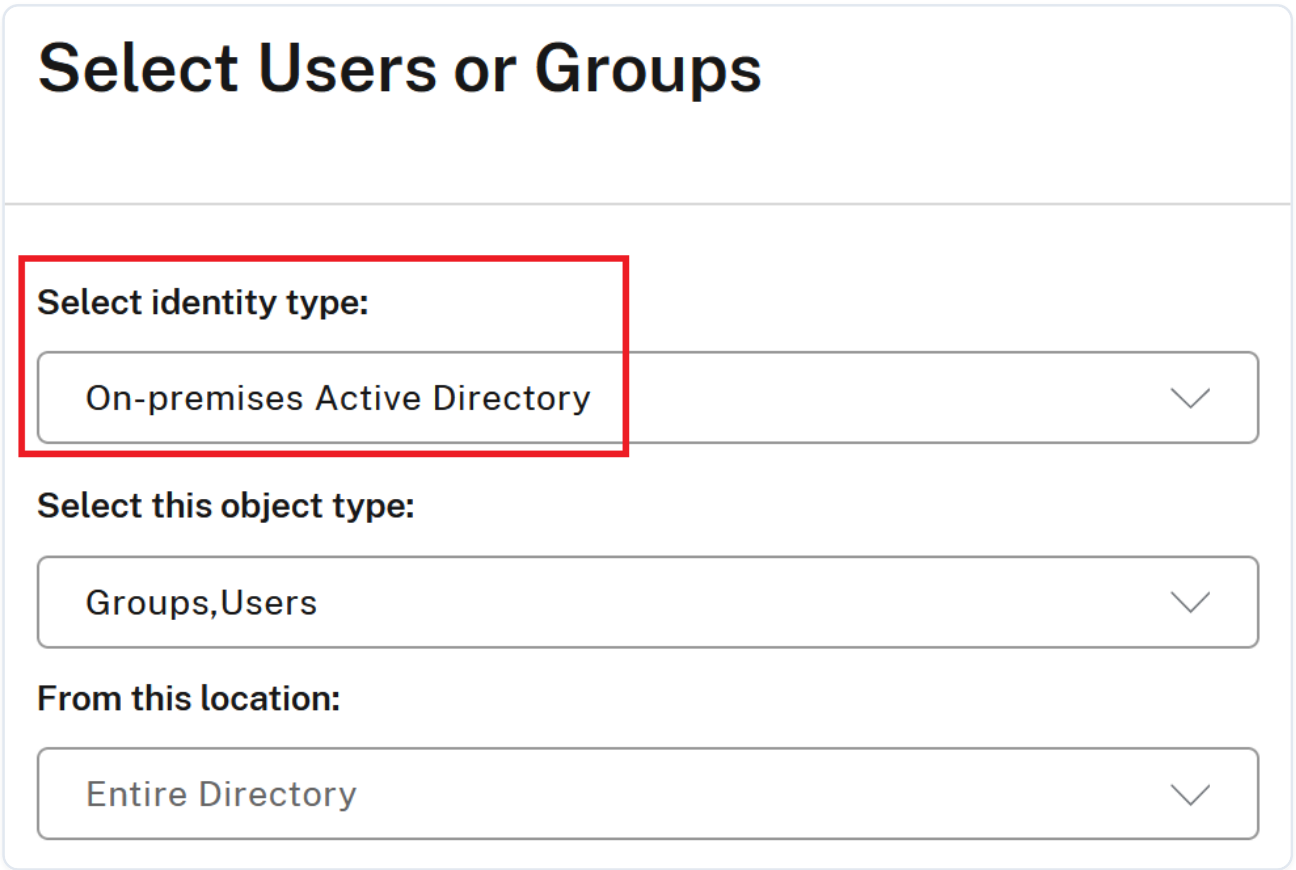
`cip_upn, cip_email, cip_sid, and cip_oid`のクレーム名を使用してください。すべてのクレーム名は小文字である必要があります。

原因 2

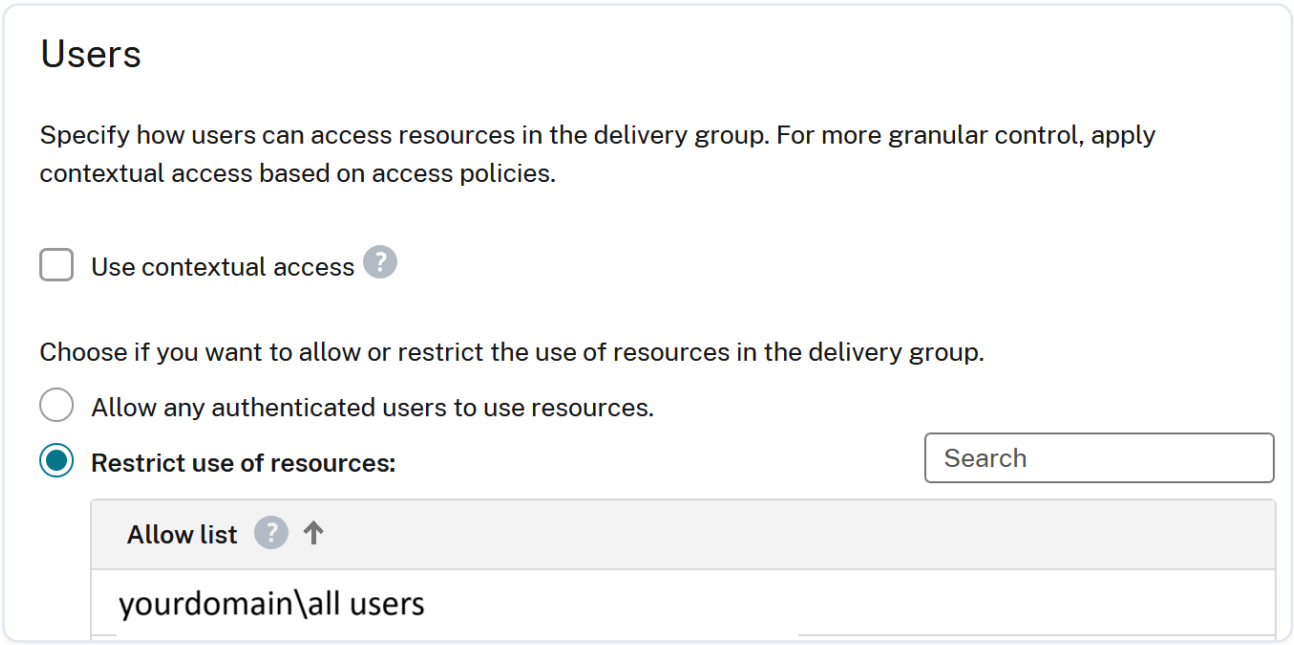
DaaSデリバリーグループが誤って構成されており、リソースが**Active Directory** IDではなく**Okta** IDにマッピングされています。

解決策 2

ADドメイン参加済みデリバリーグループとVDAを**Okta** IDではなく**Active Directory** IDにマッピングしてください。**Okta** IDは、**ドメインに参加していない**リソースの起動にのみ使用してください。



デリバリーグループを構成して、ADユーザーとグループに基づいて**リソースの使用を制限**します。



原因 3

Citrix Cloudの要件に従って**ADユニバーサルグループ**を使用していないか、Citrix Cloud Connectorが正しいADドメインレベルに参加していません。詳細については、この記事を参照してください Citrix Cloud Connectorのシステム要件

解決策 3

ユーザーをDaaSリソースに割り当てる際は、ユニバーサルグループを使用してください

または、,

ストアユーザーをデリバリーグループに直接割り当てます。

SAMLをIDプロバイダーとしてCitrix Cloud™に接続する

Citrix Cloudは、Citrix Cloud管理者とストアにサインインするエンドユーザーを認証するためのIDプロバイダーとしてSAML（Security Assertion Markup Language）の使用をサポートしています。オンプレミスのActive Directory（AD）で、任意のSAML 2.0プロバイダーを使用できます。

この記事について

この記事では、Citrix CloudとSAMLプロバイダー間の接続を構成するために必要な手順について説明します。これらの手順の一部は、SAMLプロバイダーの管理コンソールで実行するアクションについて説明しています。これらのアクションを実行するために使用する特定のコマンドは、選択したSAMLプロバイダーによって、記事に記載されているコマンドと異なる場合があります。これらのSAMLプロバイダーコマンドは、あくまで例として提供されています。SAMLプロバイダーの対応するコマンドの詳細については、SAMLプロバイダーのドキュメントを参照してください。

Citrix SAMLログオンのユースケース

- エンドユーザー向けのストアへのログイン。
- エンドユーザー向けのストアカスタムドメインを使用したストアへのログイン。
- 管理者ユーザー向けのCitrix Cloudへのログイン。

ユースケースに適したSAMLフローの選択

- SAMLプロバイダーにインポートされた**ADバックアップID**。これらのIDには、objectSIDやobjectGUIDなどのオンプレミスユーザー属性が含まれています。これらのインポートされたユーザーに対応するADアカウントはActive Directoryに既に存在するため、ADシャドウアカウントは必要ありません。
- Entra IDやOktaユーザーなど、SAMLプロバイダーディレクトリ内にのみ存在する**ネイティブID**。これらはAD内に対応するIDを持たず、ADドメイン参加済みVDAおよびDaaSカタログを使用する場合はADシャドウアカウントが必要です。これらのユーザーには埋め込みobjectSIDはありません。
- 他のEntra IDテナントから、またはゲストメールアドレスを使用してEntra IDに招待された**Entra IDゲスト/B2Bユーザー**。これらはAD内に対応するIDを持たず、ADドメイン参加済みVDAおよびDaaSカタログを使用する場合はADシャドウアカウントが必要です。これらのユーザーには埋め込みobjectSIDがない場合があります。一部のユーザーは、誤ったActive Directoryに誤ったobjectSIDを持っている場合があります。

サポートされているSAMLプロバイダー

公式のSAML 2.0仕様をサポートするSAMLプロバイダーは、Citrix Cloudでの使用がサポートされています。

Citrixは、Citrix Cloud管理者認証およびシングルサインオン（SSO）とシングルログアウト（SLO）を使用したCitrix® StoreFront Cloudエンドユーザー認証のために、以下のSAMLプロバイダーをテストしました。このリストにないSAMLプロバイダーもサポートされています。

- マイクロソフト ADFS
- マイクロソフト Entra ID
- Duo
- オクタ
- PingFederate

これらのプロバイダーをテストする際、Citrix は Citrix Cloud コンソールで SAML 接続を構成するために以下の設定を使用しました。

CITRIX CLOUD のこのフィールド	この値を入力
エンティティ ID	`https://entityid.com`
認証要求に署名	はい
SSO サービス URL	`https://yoursamlprovider/sso/saml2`
SSO バインディングメカニズム	HTTP ポスト
SAML レスポンス	レスポンスまたはアサーションのいずれかに署名
認証コンテキスト	未指定、厳密
ログアウト URL	`https://yoursamlprovider/slo/saml2`
ログアウトリクエストに署名	はい
SLO バインディングメカニズム	HTTP ポスト

これらの設定の詳細については、この記事の Citrix Cloud に SAML プロバイダーのメタデータを追加する を参照してください。

スコープ付きエンティティ ID のサポート

この記事では、単一の SAML アプリケーションと Citrix Cloud のデフォルトの汎用エンティティ ID を使用して SAML 認証を構成する方法について説明します。

SAML 認証の要件に、単一の SAML プロバイダー内で複数の SAML アプリケーションが必要な場合は、Citrix Cloud でスコープ付きエンティティ ID を使用して SAML アプリケーションを構成する を参照してください。

SAML 2.0 を使用した管理者認証

Citrix Cloud は、SAML 2.0 を使用して、個々の管理者と AD の管理者グループのメンバーを認証することをサポートしています。Citrix Cloud への管理者グループの追加について詳しくは、「管理者グループの管理」を参照してください。

管理者認証に既存の SAML 接続を使用する

Citrix Cloud に SAML 2.0 接続がすでにあり、それを使用して管理者を認証する場合は、まず で SAML 2.0 を切断してから、接続を再構成する必要があります。SAML 接続を使用して StoreFront Cloud エンドユーザーを認証している場合は、**StoreFront Cloud** で SAML 認証方法も無効にする必要があります。SAML 接続を再構成した後、個々の管理者または管理者グループを Citrix Cloud に追加できます。

SAML 2.0 を切断して再接続せずに個々の管理者または管理者グループを追加しようとすると、「Citrix Cloud に管理者グループを追加する」で説明されている ID オプションが表示されません。

新しい SAML 接続を設定するためのタスクの概要

Citrix Cloud で新しい SAML 2.0 接続を設定するには、次のタスクを実行します。

1. で、「Active Directory を Citrix Cloud に接続する」の説明に従って、オンプレミス AD を Citrix Cloud に接続します。
2. この記事の「Active Directory との SAML 統合」の説明に従って、SAML プロバイダーをオンプレミス AD と統合します。
3. 管理者が Citrix Cloud にサインインするために使用できるサインイン URL を構成します。
4. で、Citrix Cloud でSAML 認証を構成します。このタスクには、Citrix Cloud からの SAML メタデータで SAML プロバイダーを構成し、SAML 接続を作成するために SAML プロバイダーからのメタデータで Citrix Cloud を構成することが含まれます。

Citrix Cloud 管理者向けに既存の SAML 接続を使用するためのタスクの概要

Citrix Cloud に SAML 2.0 接続がすでにあり、それを管理者認証に使用する場合は、次のタスクを実行します。

1. 該当する場合、SAML 2.0 ストア認証を無効にします。 **>** で、別の認証方法を選択し、プロンプトが表示されたら を選択します。
2. 既存の SAML 2.0 接続を切断します。 **>** で、SAML 接続を見つけます。右端の省略記号メニューから を選択します。 を選択してアクションを確認します。
3. SAML 2.0を再接続し、接続を構成します。**SAML 2.0**の省略記号メニューから、**Connect**を選択します。
4. プロンプトが表示されたら、管理者がサインインに使用するサインインURLの一意の識別子を入力します。

5. この記事のSAMLプロバイダーメタデータの構成で説明されているとおりに、SAML接続を構成します。

SAML接続を構成した後、管理者グループの管理で説明されているとおりに、AD管理者グループをCitrix Cloudに追加できます。また、この記事で説明されているとおりに、エンドユーザー向けSAMLを再度有効にすることもできます。

カスタムSAML属性を作成してマッピングする

SAMLプロバイダーでSID、UPN、OID、email、およびdisplayName属性のカスタム属性がすでに構成されている場合は、このタスクを実行する必要はありません。SAMLコネクタアプリケーションの作成に進み、手順5で既存のカスタムSAML属性を使用してください。

注：

このセクションの手順では、SAMLプロバイダーの管理コンソールで実行するアクションについて説明します。これらのアクションを実行するために使用する特定のコマンドは、選択したSAMLプロバイダーによって、このセクションで説明されているコマンドとは異なる場合があります。このセクションのSAMLプロバイダーコマンドは、例としてのみ提供されています。SAMLプロバイダーの対応するコマンドの詳細については、SAMLプロバイダーのドキュメントを参照してください。

1. SAMLプロバイダーの管理コンソールにサインインし、カスタムユーザー属性を作成するオプションを選択します。たとえば、SAMLプロバイダーのコンソールによっては、**Users > Custom User Fields > New User Field**を選択する場合があります。
2. 次のADプロパティの属性を追加します。示されているデフォルト値を使用して属性に名前を付けます。

ADプロパティ	必須またはオプション	デフォルト値
userPrincipalName	SIDの属性を追加しない場合（推奨）は必須。	`cip_upn`
objectSID	UPNの属性を追加しない場合は必須です。	`cip_sid`
objectGUID	認証用オプション	`cip_oid`
メール	認証用オプション	`cip_email`

ADプロパティ	必須またはオプション	デフォルト値
displayName	ストアUIで必須	`displayName`
givenName	ストアUIで必須	`firstName`
sn	ストアUIで必要	`lastName`
ADフォレスト	認証にはオプション	`cip_forest`
ADドメイン	認証にはオプション	`cip_domain`

3. Citrix Cloudに接続したADを選択します。たとえば、SAMLプロバイダーのコンソールによっては、**ユーザー > ディレクトリ**を選択する場合があります。
4. ディレクトリ属性を追加するオプションを選択します。たとえば、SAMLプロバイダーのコンソールによっては、**ディレクトリ属性**を選択する場合があります。
5. 属性を追加するオプションを選択し、以下のAD属性を、手順2で作成したカスタムユーザー属性にマッピングします。

    - 手順2でSIDの属性を追加した場合（たとえば、`cip_sid`）、**objectSid**を選択し、作成した属性にマッピングします。
    - 手順2でUPNの属性を追加した場合（たとえば、`cip_upn`）、**userPrincipalName**を選択し、作成した属性にマッピングします。
    - ステップ2でObjectGUIDの属性を追加した場合（例: `cip_oid`）、**ObjectGUID**を選択し、作成した属性にマッピングします。
    - ステップ2でMailの属性を追加した場合（例: `cip_email`）、**mail**を選択し、作成した属性にマッピングします。
    - ステップ2で表示名（Display Name）の属性を追加した場合（例: `displayName`）、**displayName**を選択し、作成した属性にマッピングします。

管理者サインインURLを構成する

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、**IDおよびアクセス管理**を選択します。
3. **SAML 2.0**を見つけ、省略記号メニューから**接続**を選択します。
4. プロンプトが表示されたら、会社用の短くURLフレンドリーな識別子を入力し、**保存して続行**を選択します。**SAMLの構成**ページが表示されます。

5. 次のセクションに進み、Citrix CloudへのSAML接続を構成します。

SAMLプロバイダーのメタデータを構成する

このタスクでは、Citrix CloudからのSAMLメタデータを使用してコネクタアプリケーションを作成します。SAMLアプリケーションを構成した後、コネクタアプリケーションからのSAMLメタデータを使用してCitrix CloudへのSAML接続を構成します。

> **注:**
>
> このセクションの一部の手順では、SAMLプロバイダーの管理コンソールで実行するアクションについて説明しています。これらのアクションを実行するために使用する特定のコマンドは、選択したSAMLプロバイダーによって、このセクションで説明されているコマンドとは異なる場合があります。このセクションのSAMLプロバイダーコマンドは、あくまで例として提供されています。ご使用のSAMLプロバイダーに対応するコマンドの詳細については、SAMLプロバイダーのドキュメントを参照してください。

SAMLコネクタアプリケーションを作成する

1. SAMLプロバイダーの管理コンソールから、属性と署名応答を持つIDプロバイダーのアプリケーションを追加します。たとえば、プロバイダーのコンソールによっては、**Applications > Applications > Add App**を選択し、その後、**SAML Test Connector (IdP w/ attr w/ sign response)**を選択する場合があります。
2. 該当する場合、表示名を入力してアプリを保存します。
3. Citrix Cloudの**SAMLの構成**画面で、**SAMLメタデータ**の**ダウンロード**を選択します。メタデータXMLファイルが別のブラウザータブに表示されます。

   > **注：**
   >
   > 必要に応じて、`https://saml.cloud.com/saml/metadata.xml`からこのファイルをダウンロードすることもできます。このエンドポイントは、SAMLプロバイダーメタデータをインポートおよび監視する際に、一部のIDプロバイダーにとってより使いやすい場合があります。

4. コネクタアプリケーションについて、次の詳細を入力します。

   - **オーディエンス**フィールドに、`https://saml.cloud.com`を入力します。

- **受信者**フィールドに、`https://saml.cloud.com/saml/acs`を入力します。
- ACS URLバリデーターのフィールドに、`https://saml.cloud.com/saml/acs`を入力します。
- ACS URLのフィールドに、`https://saml.cloud.com/saml/acs`を入力します。

5. アプリケーションのパラメーター値として、カスタムSAML属性を追加します。

このフィールドを作成します	このカスタム属性を割り当てます
cip_sid	SID用に作成したカスタム属性。例：cip_sid
cip_upn	UPN用に作成したカスタム属性。例: cip_upn
cip_oid	ObjectGUID用に作成したカスタム属性。例: cip_oid
cip_email	Mail用に作成したカスタム属性。例: cip_email
displayName	表示名用に作成したカスタム属性。例: displayName

6. エンドユーザーをユーザーとして追加し、アプリケーションにアクセスできるようにします。

SAMLプロバイダーメタデータをCitrix Cloudに追加する

1. SAMLプロバイダーからSAMLメタデータを取得します。次の画像は、このファイルの例です。



```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app.[redacted].com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
  "urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID2DCCA[redacted]+w3PpA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-redirect/slo/1097253"/>

      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
    "https://citrixidentity-dev.[redacted].com/trust/saml2/soap/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

2. Citrix Cloudの**SAMLの構成**画面で、SAMLプロバイダーのメタデータファイルから次の値を入力します。

   - **IDプロバイダーエンティティID**に、メタデータ内の**EntityDescriptor**要素から**entityID**の値を入力します。

     ```
     <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
     https://app.[redacted].com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19"
     ```

   - **認証要求に署名**で、**はい**を選択すると、Citrix Cloudが認証要求に署名できるようになり、悪意のあるアクターからではなくCitrix Cloudから来たことを証明します。SAMLプロバイダーがSAML応答を安全に投稿するために使用する許可リストにCitrix ACS URLを追加することを希望する場合は、**いいえ**を選択します。
   - 「**SSOサービスURL**」に、使用するバインディングメカニズムのURLを入力します。HTTP-POSTまたはHTTP-Redirectバインディングのいずれかを使用できます。メタデータファイルで、バインディング値が**HTTP-POST**または**HTTP-Redirect**のいずれかである**SingleSignOnService**要素を見つけます。

SAMLメタデータファイルからのSSOサービスURL(/en-us/citrix-cloud/media/saml-sso-url.png)

- 「**バインディングメカニズム**」で、メタデータファイルから選択したSSOサービスURLのバインディングと一致するメカニズムを選択します。デフォルトでは、**HTTP Post**が選択されています。
- 「**SAML応答**」で、SAMLプロバイダーがSAML応答とSAMLアサーションに使用する署名方法を選択します。デフォルトでは、**応答またはアサーションのいずれかに署名**が選択されています。Citrix Cloudは、このフィールドで指定されたとおりに署名されていない応答を拒否します。

3. SAMLプロバイダーの管理コンソールで、次の操作を実行します。
   - SAML署名アルゴリズムに**SHA-256**を選択します。
   - X.509証明書をBase64エンコードされたPEM、CRT、またはCERファイルとしてダウンロードします。
4. Citrix Cloudの「**SAMLの構成**」ページで、「**X.509証明書**」の「**ファイルのアップロード**」を選択し、前の手順でダウンロードした証明書ファイルを選択します。
5. アップロードを完了するには、**続行**を選択します。
6. 「**認証コンテキスト**」で、使用するコンテキストと、Citrix Cloudがこのコンテキストをどの程度厳密に適用するかを選択します。「**最小**」を選択すると、選択したコンテキストでの認証を要求しますが、そのコンテキストでの認証は強制されません。「**厳密**」を選択すると、選択したコンテキストでの認証を要求し、そのコンテキストでのみ認証を強制します。SAMLプロバイダーが認証コンテキストをサポートしていない場合、または使用しない場合は、「**未指定**」と「**最小**」を選択します。デフォルトでは、「**未指定**」と「**厳密**」が選択されています。
7. 「**ログアウトURL**」（オプション）では、ストアまたはCitrix Cloudからサインアウトするユーザーが、SAMLプロバイダーを介して以前にサインインしたすべてのWebアプリケーションからもサインアウトするかどうかを決定します。
   - ユーザーがストアまたはCitrix Cloudからサインアウトした後もWebアプリケーションにサインインしたままにしたい場合は、「**ログアウトURL**」フィールドを空白のままにします。
   - ユーザーがストアまたはCitrix Cloudからサインアウトした後、すべてのWebアプリケーションからサインアウトするようにしたい場合は、SAMLプロバイダーのSingleLogout (SLO) エンドポイントを入力します。Microsoft ADFSまたはMicrosoft Entra IDをSAMLプロバイダーとして使用している場合、SLOエンドポイントはシングルサインオン (SSO) エンドポイントと同じです。

EntraIDシングルサインオンおよびシングルログアウトエンドポイントURLの例(/en-us/citrix-cloud/media/saml-idp-aad-sso-slo-example.png)

8. Citrix Cloudの以下のデフォルト属性値が、SAMLプロバイダーで構成されている対応する属性値と一致することを確認します。Citrix CloudがSAMLアサーション内でこれらの属性を見つけるには、ここに入力された値がSAMLプロバイダーの値と一致している必要があります。SAMLプロバイダーで特定の属性を構成しなかった場合、特に指定がない限り、Citrix Cloudのデフォルト値を使用するか、フィールドを空白のままにすることができます。

   - **ユーザー表示名のアトリビュート名**: デフォルト値は `displayName` です。
   - **ユーザー名のアトリビュート名**: デフォルト値は `firstName` です。
   - **ユーザー姓のアトリビュート名**: デフォルト値は `lastName` です。
   - **セキュリティ識別子 (SID) のアトリビュート名**: UPN のアトリビュートを作成しなかった場合は、SAML プロバイダーからこのアトリビュート名を入力する必要があります。デフォルト値は `cip_sid` です。
   - **ユーザープリンシパル名 (UPN) のアトリビュート名**: SID のアトリビュートを作成しなかった場合は、SAML プロバイダーからこのアトリビュート名を入力する必要があります。デフォルト値は `cip_upn` です。
   - **電子メールのアトリビュート名**: デフォルト値は `cip_email` です。
   - **AD オブジェクト識別子 (OID) のアトリビュート名**: デフォルト値は `cip_oid` です。
   - **AD フォレストのアトリビュート名**: デフォルト値は `cip_forest` です。
   - **AD ドメインのアトリビュート名**: デフォルト値は `cip_domain` です。

9. 接続が正常に構成されたことを確認するには、**テストと完了** を選択します。

AD から Citrix Cloud に管理者を追加する

Citrix Cloud で AD グループを追加および管理する手順については、「管理者グループの管理」を参照してください。

ストアの SAML 認証を有効にする

1. Citrix Cloud メニューから、**StoreFront Cloud** を選択します。
2. **認証** タブを選択します
3. 「**SAML 2.0**」を選択します。

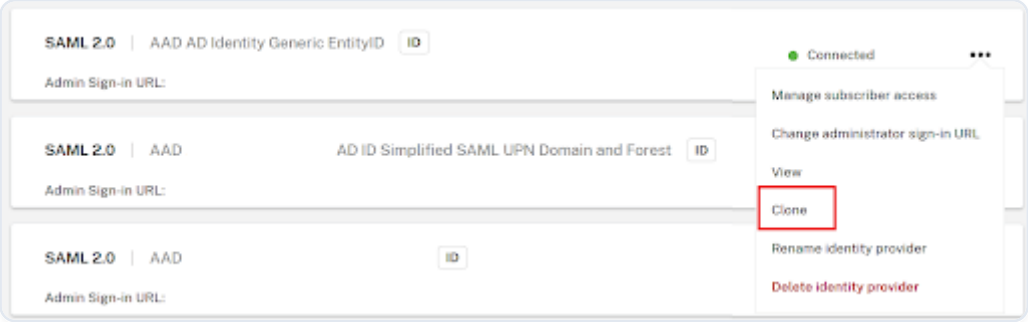
Identity and Access Management内での既存のSAML接続のクローン作成

> 「**重要:**」：

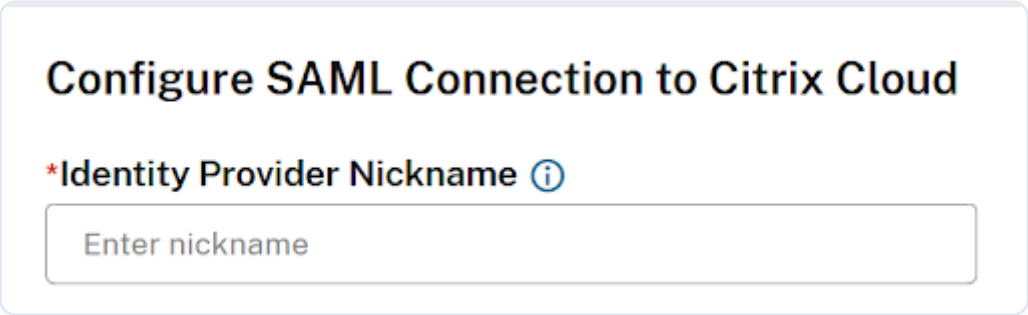
> SAML接続のクローンを作成しても、既存のスコープ付きエンティティIDはクローンされません。クローン作成プロセス中にスコープ付きエンティティIDを追加したり、新しいものを生成したりする場合は、SAMLアプリケーション構成を更新する必要がある場合があります。

> 既存のSAML接続をクローンするには、以下の手順に従います。

1. 既存のSAML接続の右側にある3つの点を選択し、アクションのリストから「**クローン**」を選択します。

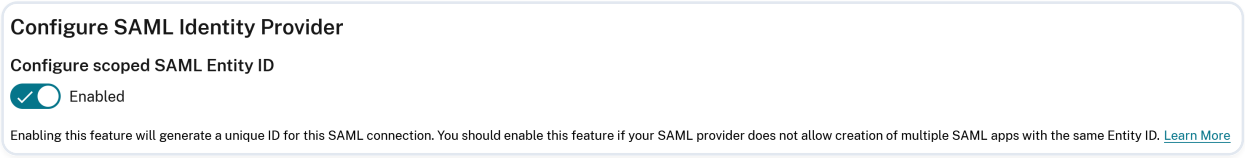


2. 新しいSAML接続用に、新しく一意のGO URLを入力します。これは必要に応じて後で変更できます。
3. 新しいSAML接続用に、新しい一意のニックネームを入力します。



4. 接続内の設定（スコープ付きエンティティIDの有効化、署名の有効化、不足しているログアウトURLの追加、最近期限切れになったSAMLプロバイダー証明書の更新など）を更新します。
5. 新しいSAML接続を保存するには、「Test and finish」をクリックします。
6. **StoreFront Cloud -> Authentication**内で、新しいSAML接続を使用するようにストアを切り替えます。

7. 新しいスコープ付きエンティティIDでSAMLアプリケーション構成を更新します（常に必要ではありません）。



前提条件

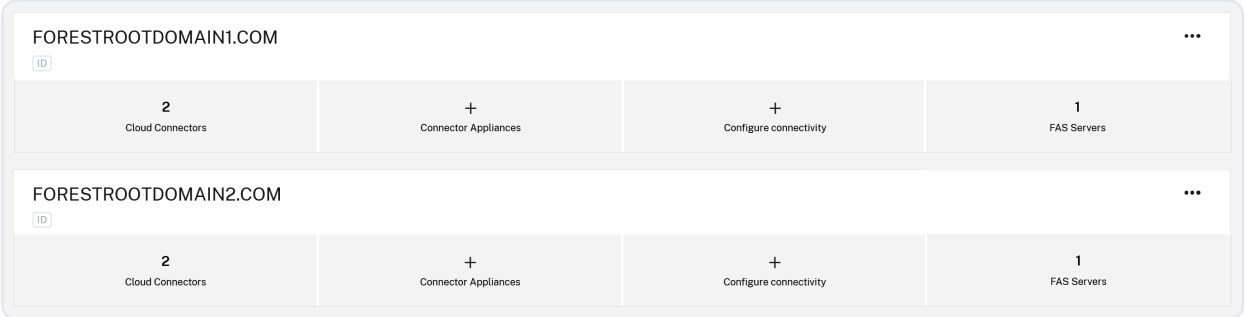
Citrix CloudでSAML認証を使用するには、次の要件があります。

- SAML 2.0をサポートするSAMLプロバイダー。
- オンプレミスのAD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。Cloud Connectorは、Citrix Cloudがリソースの場所と通信できるようにするために使用されます。
- SAMLプロバイダーとのAD統合。

クラウドコネクタ

Citrix Cloud Connector™ソフトウェアをインストールするには、少なくとも2台のサーバーが必要です。Citrixは、Cloud Connectorの高可用性のために少なくとも2台のサーバーを推奨しています。これらのサーバーは、次の要件を満たす必要があります。

- Cloud Connectorのシステム要件に記載されているシステム要件を満たしていること。
- 他のCitrix®コンポーネントがインストールされておらず、AD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とって重要なマシンではないこと。
- ADユーザーとリソースが存在するADドメインに参加していること。ユーザーが複数のドメインのリソースにアクセスする場合は、各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。



- エンドユーザーがストアを介してアクセスするリソースに接続できるネットワークに接続されていること。

- インターネットに接続されていること。詳細については、「システムと接続の要件」を参照してください。

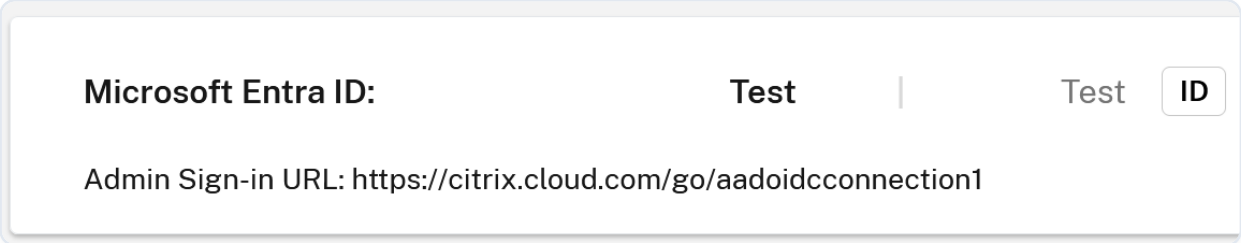
Cloud Connectorのインストールについて詳しくは、「Cloud Connectorのインストール」を参照してください。

Active Directory (デフォルトのAD ID SAMLフロー)

- エンドユーザーがADにユーザーアカウントを持っていることを確認してください。SAML認証が構成されている場合、ADアカウントを持たないエンドユーザーはストアに正常にサインインできません。
- オンプレミスのADにCloud Connectorを展開して、ADをCitrix Cloudアカウントに接続します。
- ADユーザーをSAMLプロバイダーに同期します。Citrix Cloudは、エンドユーザーが正常にサインインできるように、ADユーザー属性を必要とします。
- ユニバーサルADグループのみを使用してください。
- SAMLユーザーが使用するように構成されているUPNサフィックスは、Active Directory内で定義する必要があります。Citrix Cloud Connectorは、未定義または曖昧なUPNサフィックスを使用してActive Directoryドメインコンテキストを判断することはできません。
- デフォルトのSAMLフローではAD IDを使用するため、EntraID OIDC IdP接続は必要ありません。

EntraID ディレクトリ (EntraID アイデンティティ SAML フロー)

- EntraID B2Bおよび外部ユーザーのサポートには、EntraID内のFrontEndユーザーと一致するUPNを持つADシャドウアカウントが必要です。
- SAML with Entra ID identitiesに記載されているように、Entra ID IDを使用したSAMLフローを使用している場合は、**IDとアクセス管理 > 認証**内で正しいEntraIDテナントも接続する必要があります。



ADユーザー属性

すべてのActive Directoryユーザーオブジェクトには、次の属性が必要であり、入力されている必要があります。

- 共通名
- SAMアカウント名
- ユーザープリンシパル名 (UPN)
- オブジェクト GUID
- SID

Citrix Cloud は、エンドユーザーがストアにサインインする際に、AD の Object GUID 属性と SID 属性を使用してユーザーコンテキストを確立します。これらのプロパティのいずれかが入力されていない場合、エンドユーザーはサインインできません。

次の属性は、Citrix Cloud で SAML 認証を使用するために必須ではありませんが、Citrix は最高のユーザーエクスペリエンスを確保するために入力することを推奨します。

- メールアドレス
- 表示名

Citrix Cloud は、表示名属性を使用して、エンドユーザーの名前をストアに正しく表示します。この属性が入力されていない場合でも、エンドユーザーはサインインできますが、名前が期待どおりに表示されない場合があります。

Active Directory との SAML 統合

SAML 認証を有効にする前に、オンプレミスの AD を SAML プロバイダーと統合する必要があります。この統合により、SAML プロバイダーは次の必須 AD ユーザー属性を SAML アサーションで Citrix Cloud に渡すことができます。

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (メール)
- 表示名 (displayName)

これらの属性のサブセットを構成できます。ただし、SIDまたはUPN属性がSAMLアサーションに含まれている必要があります。Citrix Cloudは、必要に応じてADから他の属性を取得します。

> **注:**

> 最高のパフォーマンスを確保するために、Citrixは本セクションで言及されているすべての属性を構成することを推奨します。

> SAMLプロバイダーによって正確な統合手順は異なりますが、統合プロセスには通常、次のタスクが含まれます。

1. ADドメインに同期エージェントをインストールして、ドメインとSAMLプロバイダー間の接続を確立します。ADFSをSAMLプロバイダーとして使用している場合、この手順は不要です。
2. カスタム属性を作成し、本セクションで前述した必要なADユーザー属性にマッピングします。参考として、このタスクの一般的な手順は、この記事のカスタムSAML属性の作成とマッピングで説明されています。
3. ADユーザーをSAMLプロバイダーに同期します。

ADとSAMLプロバイダーの統合に関する詳細については、SAMLプロバイダーの製品ドキュメントを参照してください。

どのSAMLバインディングメカニズムを使用すべきですか?

SSOとSLOにHTTP POSTを使用するかHTTP Redirectを使用するかは、SAML IdPがサポートするSAMLバインディングによって決まります。SAMLプロバイダーが複数のバインディングメカニズムをサポートしている場合、CitrixはSAMLバインディングとしてHTTP RedirectよりもHTTP Postを選択することを推奨します。SAMLプロバイダーが両方をサポートしている場合でも、両方のSAMLバインディングメカニズムを有効にする必要はありません。SSOとSLOの両方に単一のSAMLバインディングタイプを選択することをお勧めします。

SAMLバインディングのサポート

SAMLバインディング	CITRIX CLOUDでサポート
HTTP POST	推奨。
HTTPリダイレクト	サポートされています。
SAMLアーティファクトバインディング	サポートされていません。
SOAP	サポートされていません。

> **重要:**

HTTP Post は、2つの理由からSSOおよびSLOリクエストの両方で推奨されるバインディングメカニズムです。

HTTP Post は、SAML接続の両側で署名強制が有効になっている場合、デバッグが容易です。これは、SAML XMLに、使用された署名と証明書を示す容易に識別可能なセクションが含まれているためです。この署名データが、URLデコードする必要がある非常に長いリダイレクトURI内に埋め込まれている場合よりも、人間にとって確認しやすく、デバッグしやすいと言えます。

HTTPリダイレクト URIは非常に長くなり、重大なしきい値を超える可能性があり、その結果、SAML認証中にエラーが発生し、ログインまたはログアウトの失敗を引き起こす可能性があります。GETバインディングタイプは、実際のパスの文字数を除いて、最大**2,048文字**に制限されています。POSTメソッドは、名前と値のペアを送信するためのURLのサイズによって制限されません。

サービスプロバイダー開始SSO 対 IDプロバイダー開始SSO

SP開始SSO - エンドユーザーは、ストアやCitrix CloudなどのWebアプリケーション（SP）から直接ログインし、その後、認証のためにSAML IdPにリダイレクトされます。認証が成功すると、エンドユーザーはWebアプリ（SP）にリダイレクトされ、ログインします。

IdP開始SSO - エンドユーザーはまずSAML IdPにログインし、その後、IDPポータルから起動したいアプリ（SP）を選択します。

IDプロバイダー開始SSOはストアまたはCitrix Cloudで使用できますか?

いいえ。ストアとCitrix Cloudはどちらも**SAMLのサービスプロバイダー開始SSO**ログオンのみをサポートしています。すべてのログオンフローは、エンドユーザーアクセス用のストアURL、またはCitrix Cloud管理者アクセス用のCitrix Cloud GO URLのいずれかを介して開始される必要があります。

SAMLプロバイダーをCitrix Cloudに直接接続する VS IDPチェーン

ストアまたはCitrix CloudへのSAMLログインでIDPチェーンはサポートされていますか?

IDPチェーンは、IDPチェーン内で最も近いSAML IDPが正しく構成され、Citrix CloudからのSAMLリクエストをIDPチェーンの先に転送し、IDPチェーンが正しいSAML応答をCitrix Cloudに返す場合にサポートされます。

IDPチェーンの例

- Citrix Cloud → F5 (SAMLプロバイダーとしてCitrix Cloudに直接接続) → Entra IDにフェデレーション
- Citrix Cloud → Entra ID (SAMLプロバイダーとしてCitrix Cloudに直接接続) → ADFSにフェデレーション
- Citrix Cloud → Entra ID (SAMLプロバイダーとしてCitrix Cloudに直接接続) → PingFederateにフェデレーション
- Citrix Cloud → Entra ID (SAMLプロバイダーとしてCitrix Cloudに直接接続) → Oktaにフェデレーション

IDPチェーンを使用している場合、SAMLの問題をデバッグする際にCitrixから支援やサポートを受けることはできますか?

CitrixサポートおよびCitrixエンジニアリングは、Citrix Cloudとチェーン内で最も近いSAML IDPとの間のSAML接続のみをデバッグできます。

> **重要:**
>
> Citrixは、直接接続されたSAMLプロバイダーの上流にある複雑なIDPチェーン内の問題のデバッグについて責任を負いません。

可能であればIDPチェーンを避けるべきですか?

Citrixは、SAML IDPをCitrix Cloudに直接接続することを推奨します。これにより、構成とデバッグの複雑さが大幅に軽減され、Citrix Cloudが複雑なIDPチェーンからの応答を待つ間に発生する可能性のあるエンドユーザーのログオン遅延が最小限に抑えられます。複数のIDPがチェーンされている場合、特にIDPチェーン内の異なるIDPによって異なるSAMLバインディングが使用されている場合、SSOとSLOの両方で多くの問題が発生する可能性があります。直接接続されたSAMLプロバイダーは、上流のIDPに依存するものよりも常にデバッグが容易で、パフォーマンスも優れています。

SAML ログアウトに関する考慮事項

IDプロバイダーログアウトURL (SLO) については、Citrix Cloudに接続するSAMLアプリケーションが他のサービスプロバイダー (SP) と共有されているかどうかに基づいて、組織に最も適したSAMLログアウト動作を決定してください。

Citrixは、SAMLプロバイダー内に、ストアおよび/またはCitrix Cloudのみで使用される新しい専用のSAMLアプリケーションを作成することを推奨します。CitrixのSAMLアプリケーション設定ガイドのいずれかに従い、ストアおよび/またはCitrix Cloudに専用のSAMLアプリケーションを使用している場合は、ログアウトURLを構成することが常に正しい対処法です。

オプション1 SLO構成済み (推奨): ストアおよび/またはCitrix Cloudからサインアウトしたユーザーは、接続されているSAML IDPからもサインアウトします。

ログアウト構成済み(/en-us/citrix-cloud/media/main-saml-article-logout-configured.png)

> **重要:**

> SAML SLOを成功させるには、SAML接続の両側でそれをサポートするように構成する必要があります。Citrix Cloudは、ログアウトが成功し、ユーザーがSAML IDPからログアウトされたことを示すSAMLアプリケーションからのSLO応答を受信することを期待しています。このSAMLログアウトエンドポイント `https://saml.cloud.com/saml/logout/callback` を使用して、SAMLアプリケーションがCitrix CloudにSLO応答を返すように構成されていることを確認してください。

> または

オプション2 SLO未構成: ユーザーがストアおよび/またはCitrix Cloudからサインアウトした後もSAMLアプリケーションにサインインしたままにしたい場合は、Citrix Cloud SAML接続内のログアウトURLフィールドを空のままにしてください。エンドユーザーがストアまたはCitrix Cloud UIで明示的なログアウトを実行した場合、ユーザーはストアまたはCitrix Cloudからのみログアウトされます。ユーザーはSAML IDPからログアウトされず、Citrix CloudからSAMLアプリケーションにSLOリクエストは送信されません。

ログアウトURLなし(/en-us/citrix-cloud/media/main-saml-article-no-logout-url.png)

> **重要:**

> ログアウトURLが構成されていないこのSAML接続構成は、Citrix Cloudに接続されているSAMLアプリケーションが他の非Citrixサービスプロバイダー (SP) と共有されている場合にのみ推奨されます。

ストアセッションの非アクティブタイムアウト動作

エンドユーザーがストア内で何も操作しない場合、セッションの非アクティブタイムアウトによりストアからログオフされます。ストアの非アクティブタイムアウトは、**StoreFront Cloud → カスタマイズ → 環境設定 → ストアセッション**で定義されます。

常にエンドユーザーに資格情報を要求(/en-us/citrix-cloud/media/main-saml-article-always-prompt-end-users-for-creds.png)

ストアの非アクティブタイムアウトは、エンドユーザーをSAML IdPからログアウトさせるためのSLOリクエストをトリガーしません。SAML IdPのアイドルセッションタイムアウトは、ストア内で設定されている値とは異なる場合があります。可能な場合は、同じ期間に設定することをお勧めします。

StoreFront Cloud → カスタマイズ → 環境設定内で、**エンドユーザーに常に資格情報を要求する**を**有効**に設定して、ユーザーのSAMLプロバイダーセッションがまだ存在する場合でも、エンドユーザーが常に再認証を求められるようにします。

エンドユーザーに常に資格情報を要求するを**有効**に設定すると、SAMLリクエスト内で**ForceAuthn**も**True**に設定されます。



メタデータURLモードを使用してSAML接続を作成する

Citrixは、すべての新しいSAML接続をメタデータURLモードを使用して作成することを推奨しています。IdP内からSAMLアプリケーションのメタデータURLを取得してください。Citrix Cloudは、SAML IdPメタデータを消費してSAML接続を自動的に構成できます。

メタデータURLモードがCitrix Cloud SAML接続を作成する推奨される方法であるのはなぜですか?

シンプルさ。 Citrix Cloud内のSAML接続は、デフォルトの接続設定値とメタデータ内から取得された値の組み合わせを使用して自動的に設定されます。

IdPメタデータには、Citrix Cloud内でSAML接続を設定するために必要な以下のすべての情報が含まれています。

- SAMLエンティティID
- SSOエンドポイント
- SLOエンドポイント（IdP内で構成されている場合）
- サポートされているSAMLバインディング
- 公開鍵と署名証明書

メンテナンスの削減。 SAML IdP内で行われた変更とIdP証明書のローテーションを自動的に処理します。

メタデータURLモードを使用する場合、Citrix CloudはIdP証明書のローテーションをどのように処理しますか?

自動的に。 SAML IdP管理者がSAMLアプリケーションを更新して新しいIdP署名証明書を含めるか、既存の証明書を置き換える場合、Citrix CloudはIdPメタデータ内で提供されるすべてのSAML署名証明書を暗黙的に信頼します。メタデータURLモードにより、Citrix Cloud内での手動によるIdP証明書のローテーションが不要になります。IdP管理者によって行われた変更はすべて自動的に検出されます。SAMLアプリケーションのメタデータURLは、SAMLログオンのたびに使用され、SAMLアプリケーションの署名証明書の最新コピーを取得します。

IdPメタデータURLを使用してCitrix Cloud SAML接続を構成する

1. SAMLアプリケーションのメタデータへのリンクを取得し、ブラウザに入力して、それがアクセス可能であり、Citrix Cloudからのアクセスをブロックするファイアウォールルールがないことを確認します。

   例:

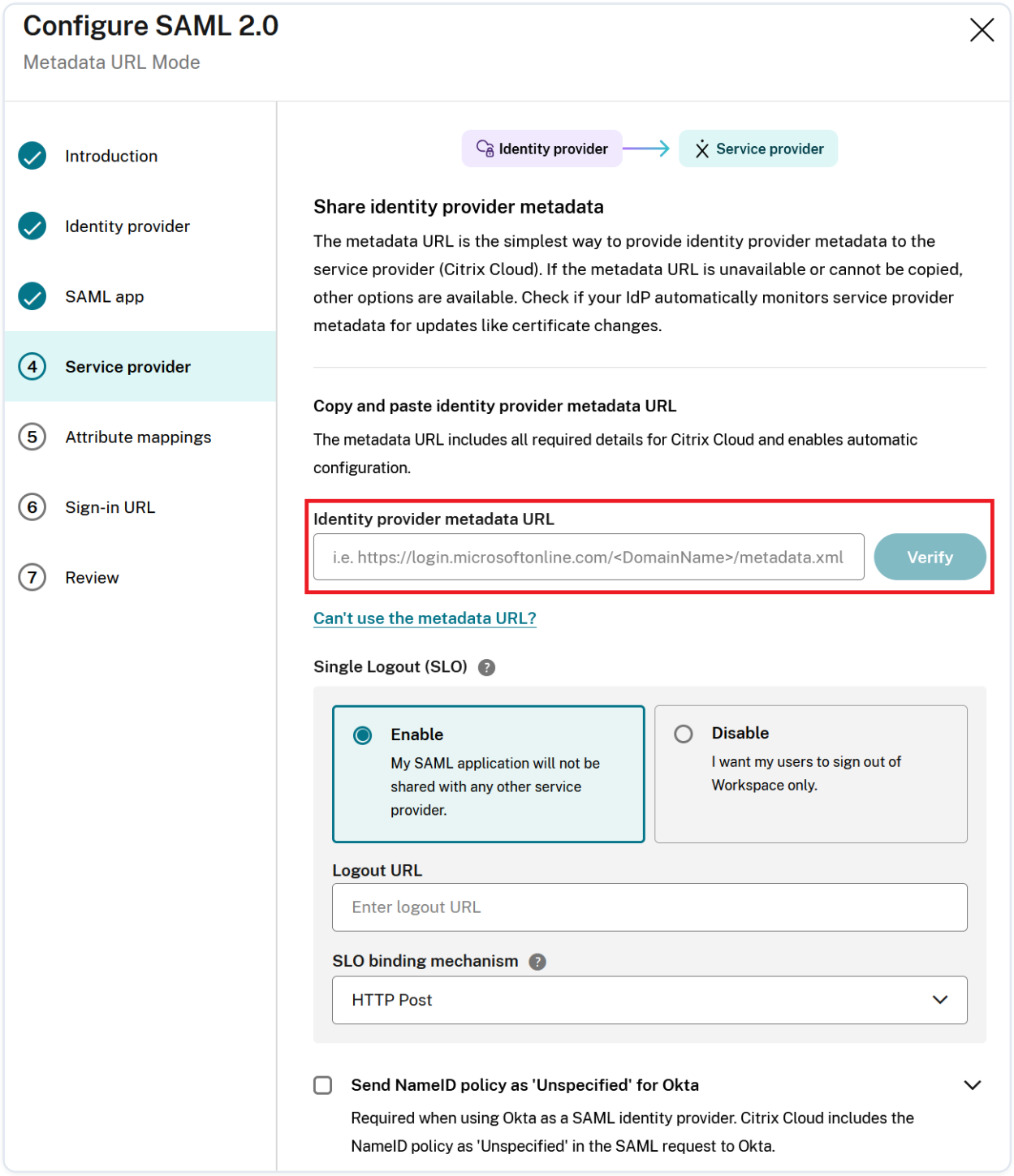
   `https://tenant.okta.com/app/zxv1r8qo70l2q5LNT359/sso/saml/metadata`

2. SAMLウィザードの**セクション4 サービスプロバイダー**セクションに到達したら、ここにSAMLアプリケーションのメタデータURLを入力し、**検証**をクリックします。

> **重要:**
>
> \> SAMLアプリケーションがADFSやPingFederateサーバーなどのオンプレミスサーバーに存在し、SAML IdPメタデータURLの検証に失敗した場合は、ファイアウォールルールを確認してください。組織外のクライアントからブラウザ内でメタデータURLにアクセスできることを確認してください。

3. Citrix CloudがメタデータURLを解析した後、この成功メッセージと「再検証」が表示されるはずです。

   これは、正常にインポートされたメタデータ接続のOktaの例です。



4. SLOを有効または無効にすることで、必要なSAMLログアウト動作を設定します。

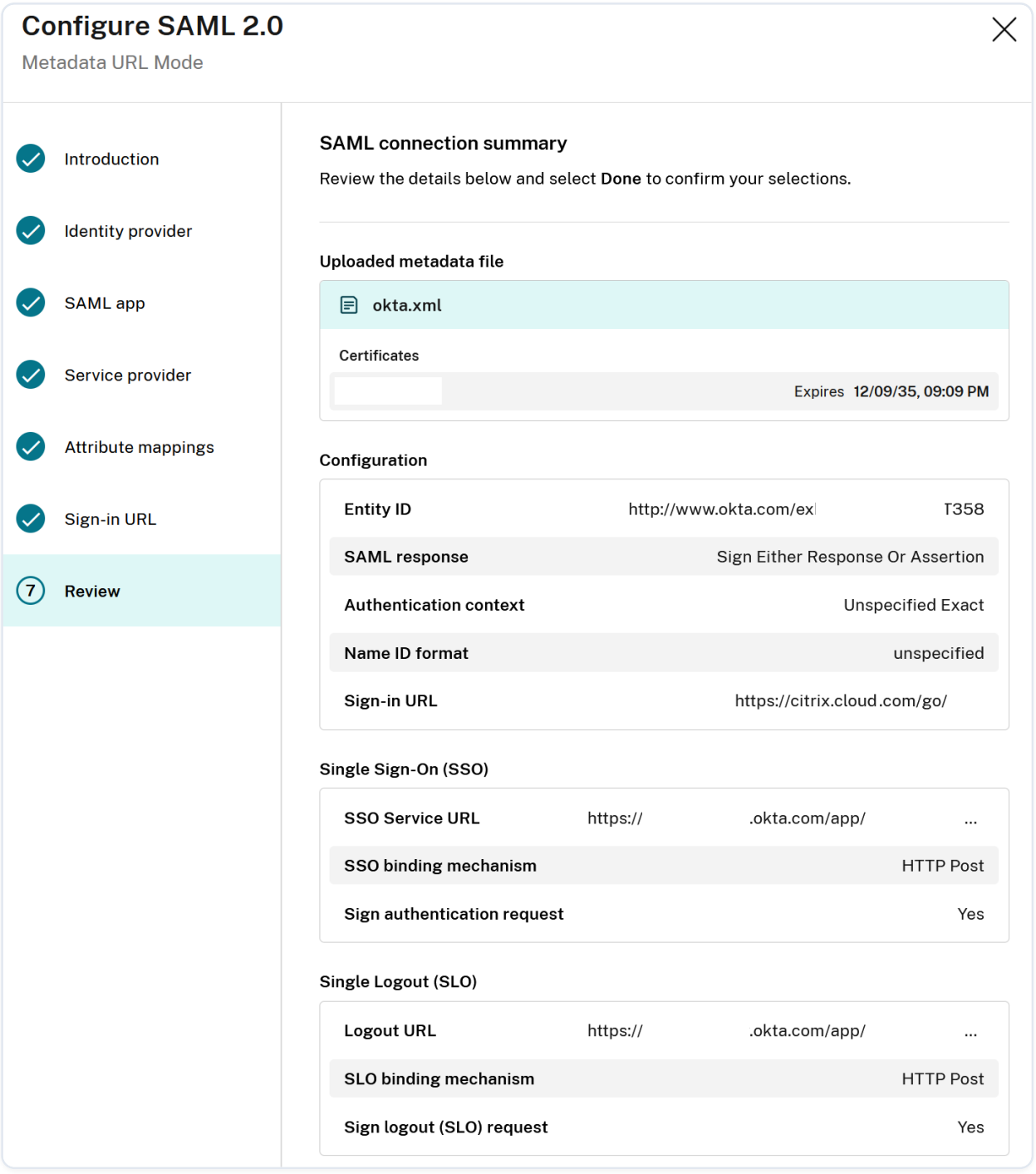
   ログアウトに関する考慮事項については、この詳細な記事を参照してください。

> **重要:**

> **Okta SAML接続のみ。**メタデータURLにSSOエンドポイントと「okta」を含むDNSドメイン文字列が含まれている場合、Oktaの「NameIDポリシーを未指定として送信」が自動的に有効になります。mytenant.domain.comのようなOktaカスタムドメインを使用す

> るOkta SAMLアプリケーションは自動検出できません。そのため、Citrix管理者はチェックボックスをクリックして、Oktaの「NameIDポリシーを未指定として送信」を手動で有効にする必要があります。

5. デフォルトの属性マッピングを受け入れます。
6. Citrix Cloud管理者サインインURLを設定します。
7. レビューセクション内のSAMLウィザードの概要を確認し、IdPメタデータURLの解析後、SAML構成が期待どおりであることを確認します。



メタデータファイルモードを使用してSAML接続を作成する

メタデータファイルモードはメタデータURLモードとどう違うのか?

ADFSやPingFederateサーバーなどのオンプレミスSAML IdPには、SAMLメタデータURLエンドポイントへのパブリックアクセスをブロックする制限があるため、メタデータURLモードを使用できない場合があります。Citrix Cloud管理者は、SAML IdPからエクスポートされたmetadata.xmlファイルが提供されれば、Citrix Cloud SAML接続の自動構成から引き続きメリットを得ることができます。Citrix Cloud管理者は、SAML接続作成ウィザード内でこのファイルをアップロードできます。

メタデータファイルモードはメタデータURLモードよりもどのように劣りますか?

メタデータファイルモードは、Citrix Cloud内に保存される静的な構成です。メタデータファイルモードを使用して作成されたCitrix Cloud SAML接続は、SAMLアプリケーションがCitrix Cloudにアップロードされた後の変更を検出できません。

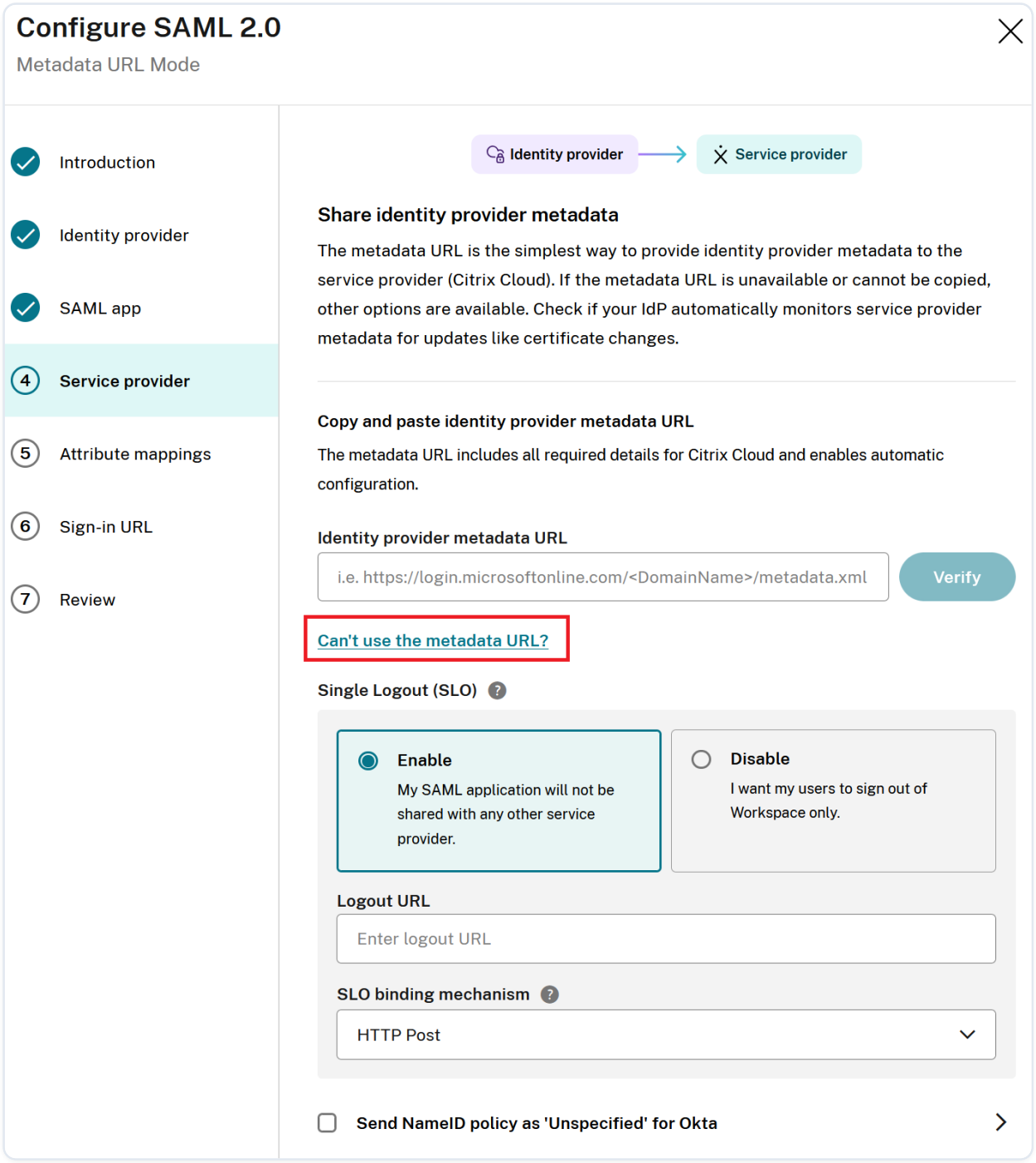
メタデータURLモードは、オンデマンドで取得される動的な構成です。メタデータURLモードはSAML IdPを継続的にポーリングし、SAMLアプリケーション構成内で行われた変更を、変更後すぐに検出できます。

IdPメタデータファイルを使用してCitrix Cloud SAML接続を構成する

1. Citrix Cloud内で新しいSAML IdP接続として構成したいSAMLアプリケーションからmetadata.xmlファイルをダウンロードします。
2. ファイルを`<filename>.xml`としてディスクに保存し、XMLの書式設定や内容を変更しないでください。SAML IdPからエクスポートされた後、完全に変更されていない、書式設定されていないmetadata.xmlファイルを直接使用することをお勧めします。

   > **重要:**
   >
   > metadata.xmlファイルは、改ざんを防ぐためにIdPによって署名されていることがよくあります。XML整形ツールを使用して書式を再設定するなど、metadata.xml内のデータを変更すると、埋め込まれた署名が無効になり、metadata.xmlのアップロードと解析が失敗します。

3. SAMLウィザードの**セクション4 サービスプロバイダー**に到達したら、*メタデータURLを使用できませんか？*を選択します。



4. 「メタデータファイルをアップロード」を選択し、metadata.xmlファイルをファイルアップロードダイアログにドラッグアンドドロップするか、ディスク上のmetadata.xmlファイルを参照します。

   以下は、正常にインポートされたメタデータファイルの**Okta**の例です。

Configure SAML 2.0

Metadata URL Mode

- Introduction
- Identity provider
- SAML app
- 4 Service provider
- 5 Attribute mappings
- 6 Sign-in URL
- 7 Review

Identity provider → Service provider

Share identity provider metadata

The metadata URL is the simplest way to provide identity provider metadata to the service provider (Citrix Cloud). If the metadata URL is unavailable or cannot be copied, other options are available. Check if your IdP automatically monitors service provider metadata for updates like certificate changes.

- ○ **Copy and paste identity provider metadata URL** — Recommended
  The metadata URL includes all required details for Citrix Cloud and enables automatic configuration.
- ◉ **Upload metadata file**
  The metadata file contains all the metadata details needed by Citrix Cloud. Download the file on your identity provider's configuration page and upload the file to Citrix Cloud.
- ○ **Manually enter metadata fields**
  You must locate the metadata fields in your identity provider and manually enter them into your service provider.

okta.xml

Certificates

Expires 12/09/35, 09:09 PM

Single Logout (SLO)

- ◉ **Enable**
  My SAML application will not be shared with any other service provider.
- ○ **Disable**
  I want my users to sign out of Workspace only.

Logout URL

https:// .okta.com/app/ oktasaml

SLO binding mechanism

HTTP Post

☑ **Send NameID policy as 'Unspecified' for Okta**

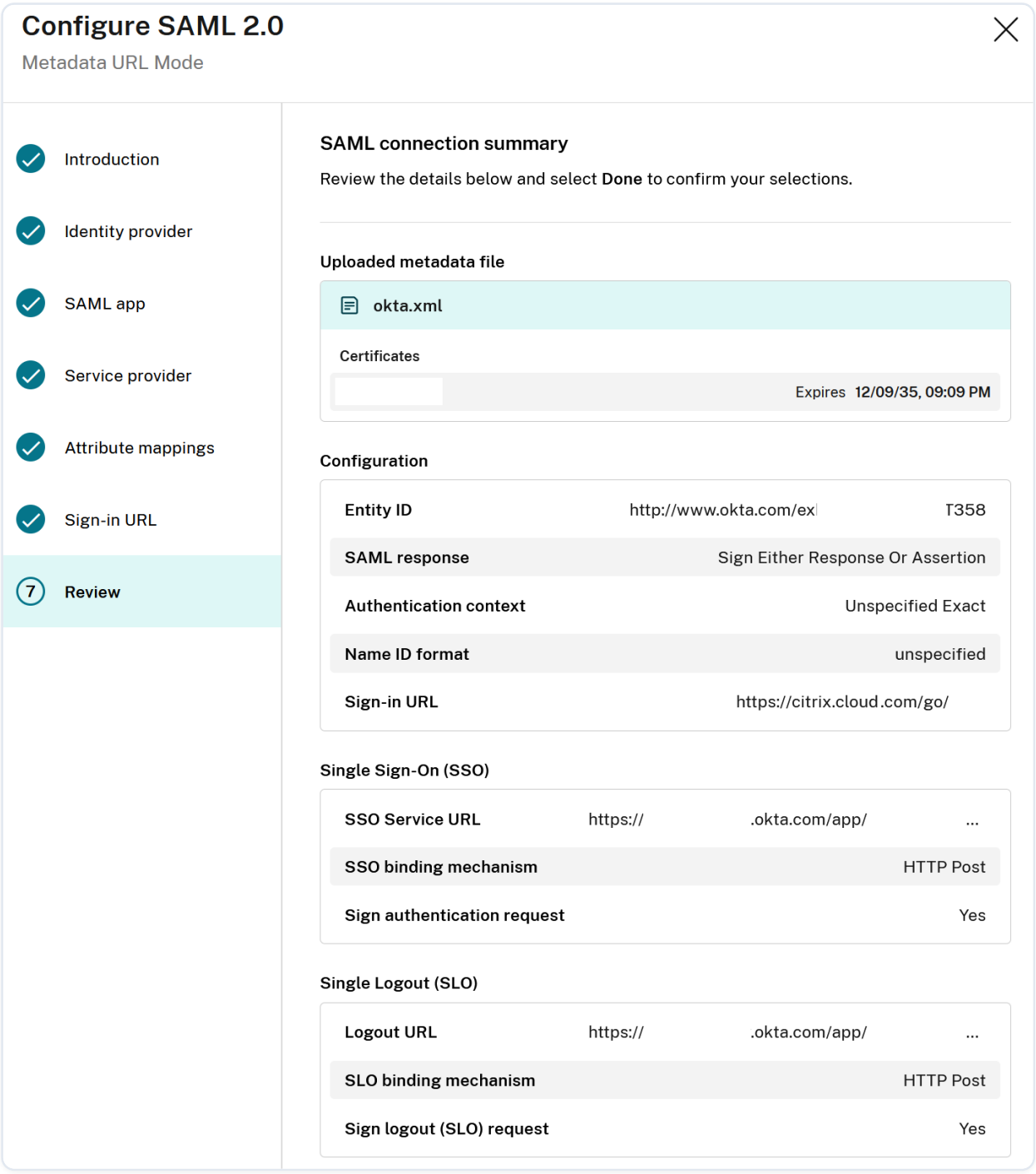
Required when using Okta as a SAML identity provider. Citrix Cloud includes the NameID policy as 'Unspecified' in the SAML request to Okta.

Already familiar with setting up SAML? Go to SAML advanced mode

5. SLOを有効または無効にすることで、希望するSAMLログアウト動作を設定します。

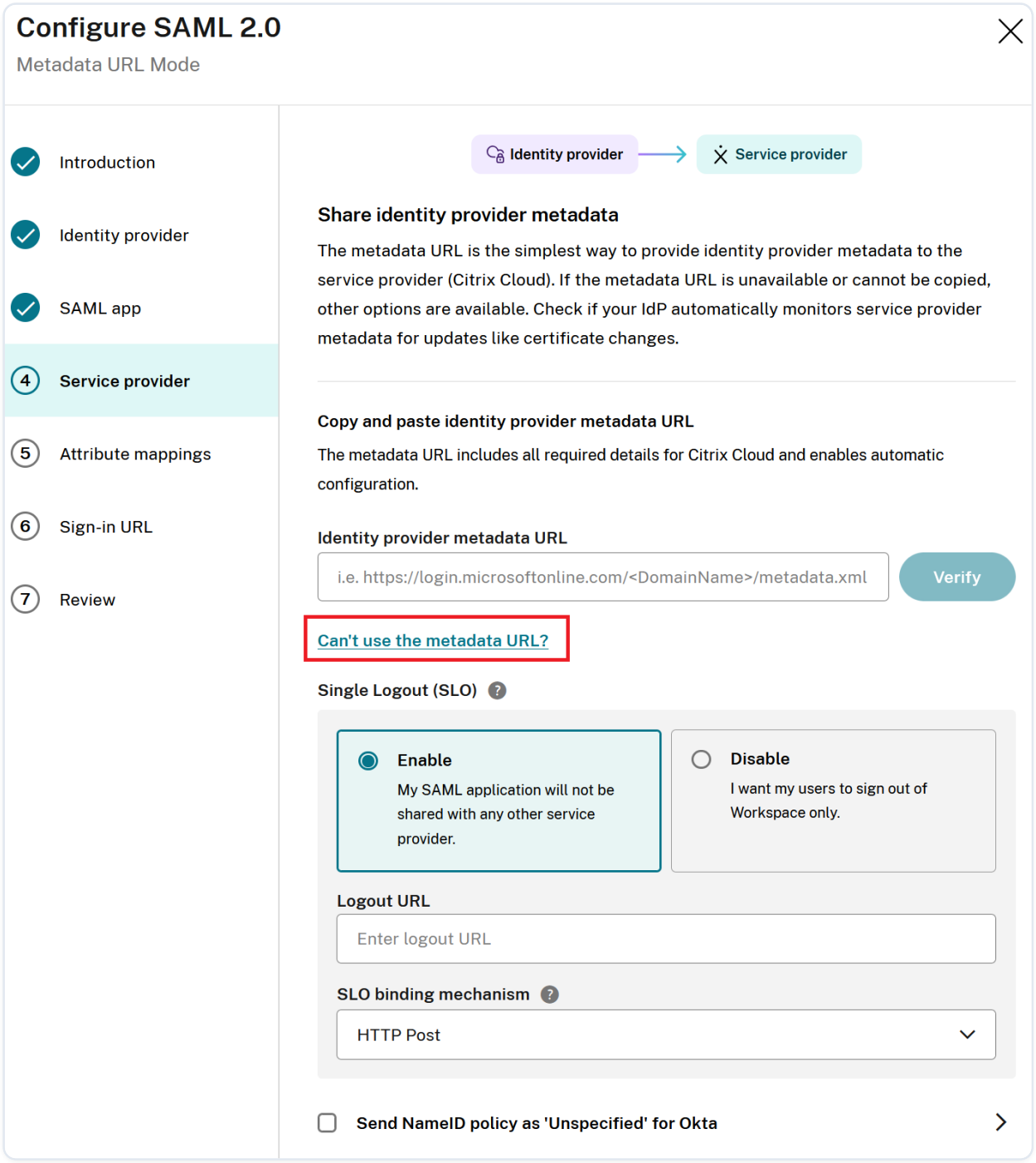
   ログアウトに関する考慮事項については、この詳細記事を参照してください。

6. Okta SAML接続のみ。メタデータファイルにSSOエンドポイントと「okta」を含むDNSドメイン文字列が含まれている場合、**OktaのNameIDポリシーを未指定として送信**が自動的に有効になります。mytenant.domain.comのようなOktaカスタムドメインを使用するOkta SAMLアプリケーションは自動検出できず、**OktaのNameIDポリシーを未指定として送信**は、Citrix管理者がチェックボックスをクリックして手動で有効にする必要があります。
7. デフォルトの属性マッピングを受け入れます。
8. Citrix Cloud管理者サインインURLを設定します。
9. レビューセクション内のSAMLウィザードの概要を確認し、IdPメタデータファイルの解析後、SAML構成が期待どおりであることを確認します。

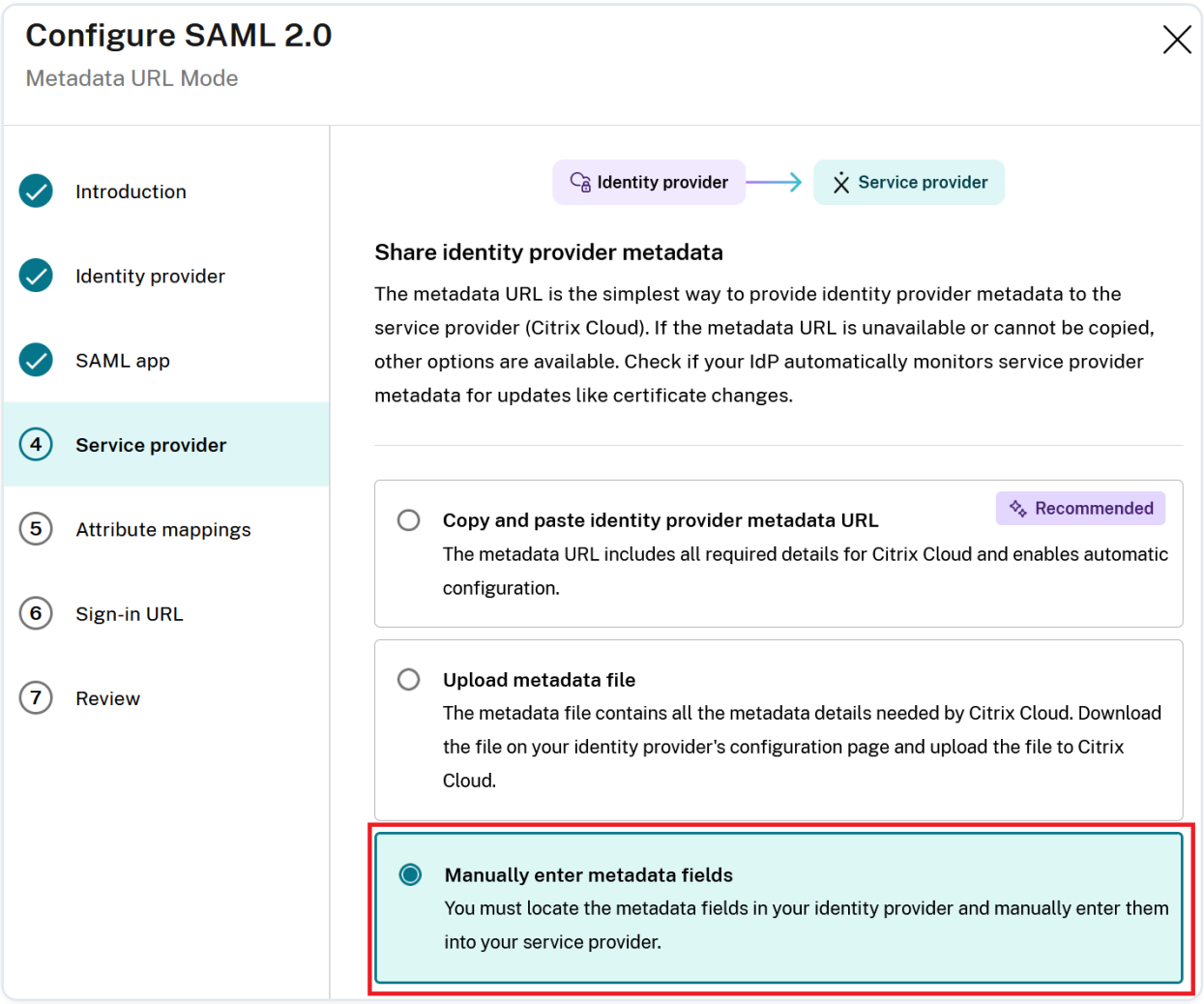


手動モードを使用してSAML接続を作成する

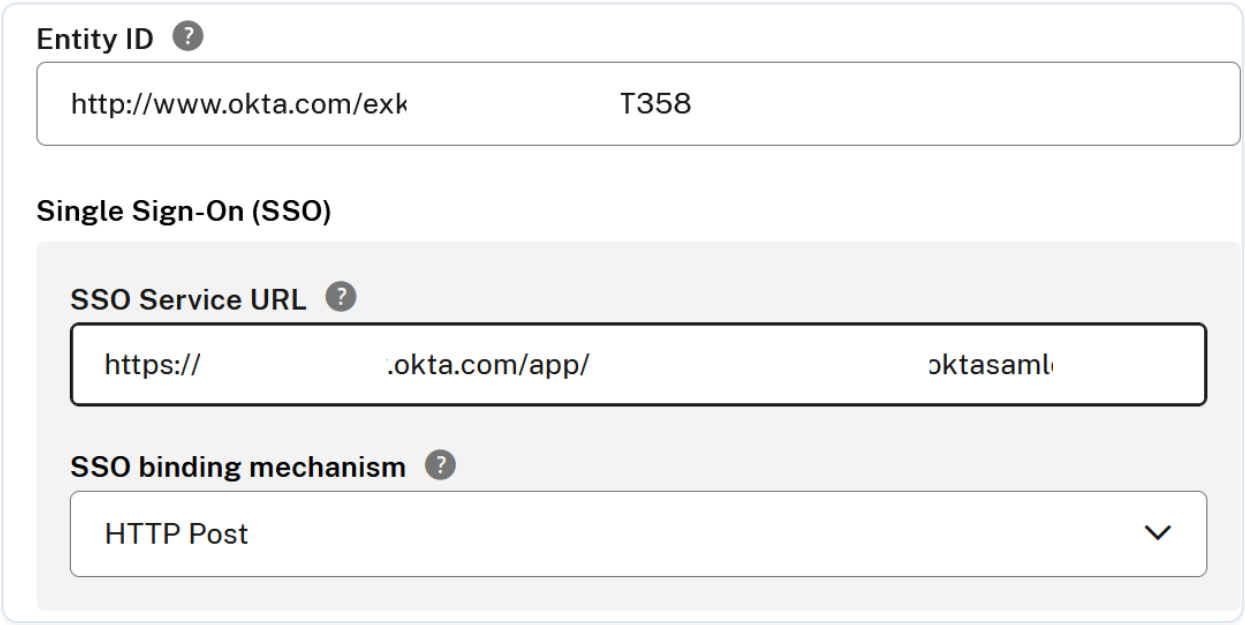
1. SAMLアプリケーションとそのSAMLエンドポイントの詳細を取得します。
2. SAMLアプリケーションからSAML署名証明書をダウンロードします。
3. SAMLウィザードの**セクション4 サービスプロバイダー**に到達したら、*メタデータURLを使用できませんか？*を選択します。



4. **メタデータフィールドを手動で入力**を選択します。



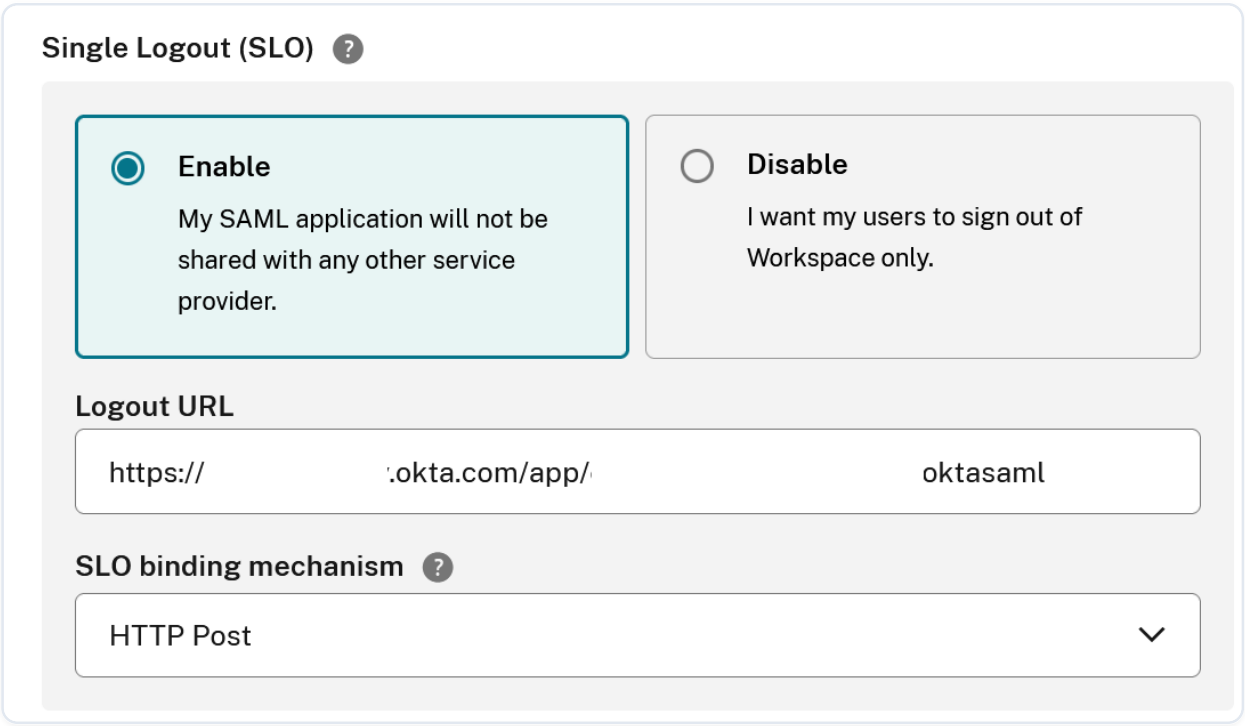
5. SAMLアプリケーションのエンティティIDとSSO URLを入力します。



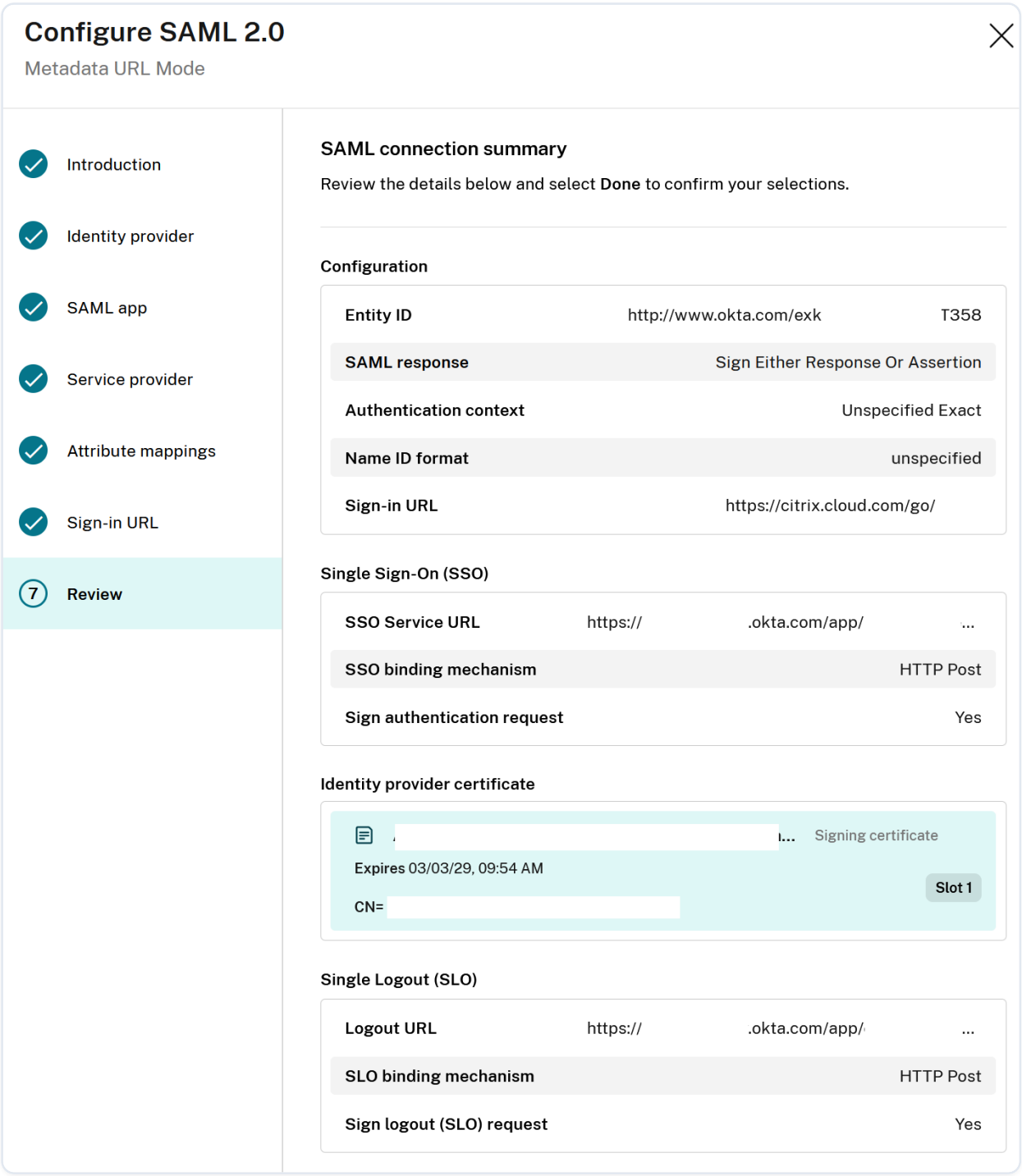
6. SAMLアプリケーションの署名証明書を、ファイルをファイルアップロードダイアログにドラッグアンドドロップするか、ディスク上のsamlapp.cerファイルを参照してアップロードします。

7. SLOを有効または無効にすることで、希望するSAMLログアウト動作を設定します。詳細については、ログアウトに関する考慮事項の記事を参照してください。

   SAMLアプリケーションのSLO URLを入力します（推奨）。



8. Okta SAML接続のみ。入力されたSSO URLに「okta」を含むDNSドメイン文字列が含まれている場合、**OktaのNameIDポリシーを未指定として送信**が自動的に有効になります。mytenant.domain.comのようなOktaカスタムドメインを使用するOkta SAMLアプリケーションは自動検出できないため、Citrix管理者はチェックボックスをクリックして**OktaのNameIDポリシーを未指定として送信**を手動で有効にする必要があります。
9. デフォルトの属性マッピングを受け入れます。
10. Citrix Cloud 管理者サインインURLを設定します。
11. レビューセクション内のSAMLウィザードの概要を確認し、接続を手動で構成した後、SAML構成が期待どおりであることを検証します。



トラブルシューティング

SAMLサポートケースをオープンする際、Citrixサポートおよびエンジニアリングに何を提供する必要があります?

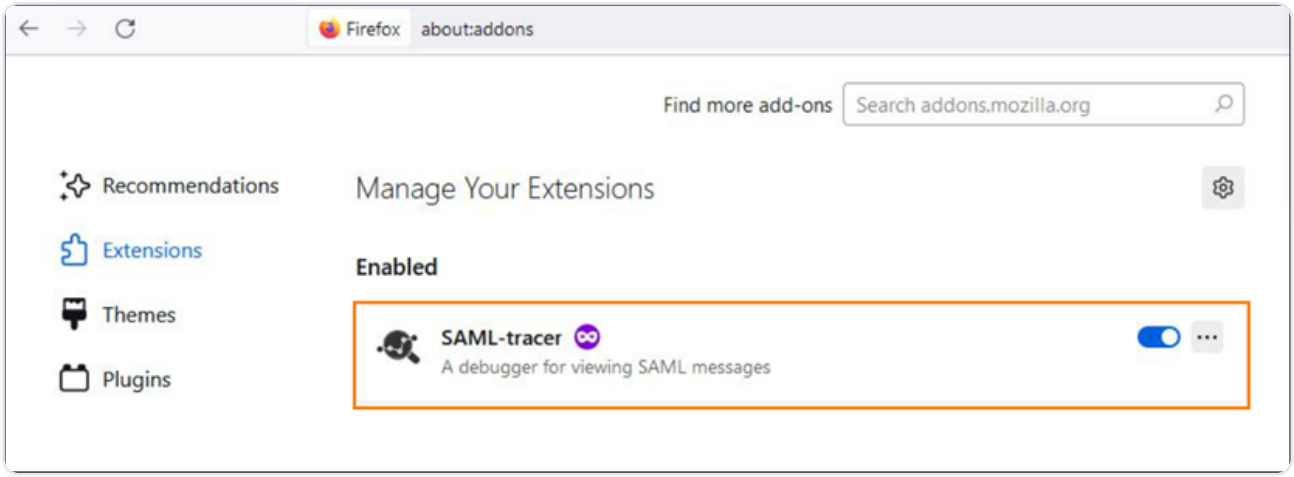
SAML関連の問題で支援が必要な場合、Citrixサポートおよびエンジニアリングは以下の情報を必要とします。

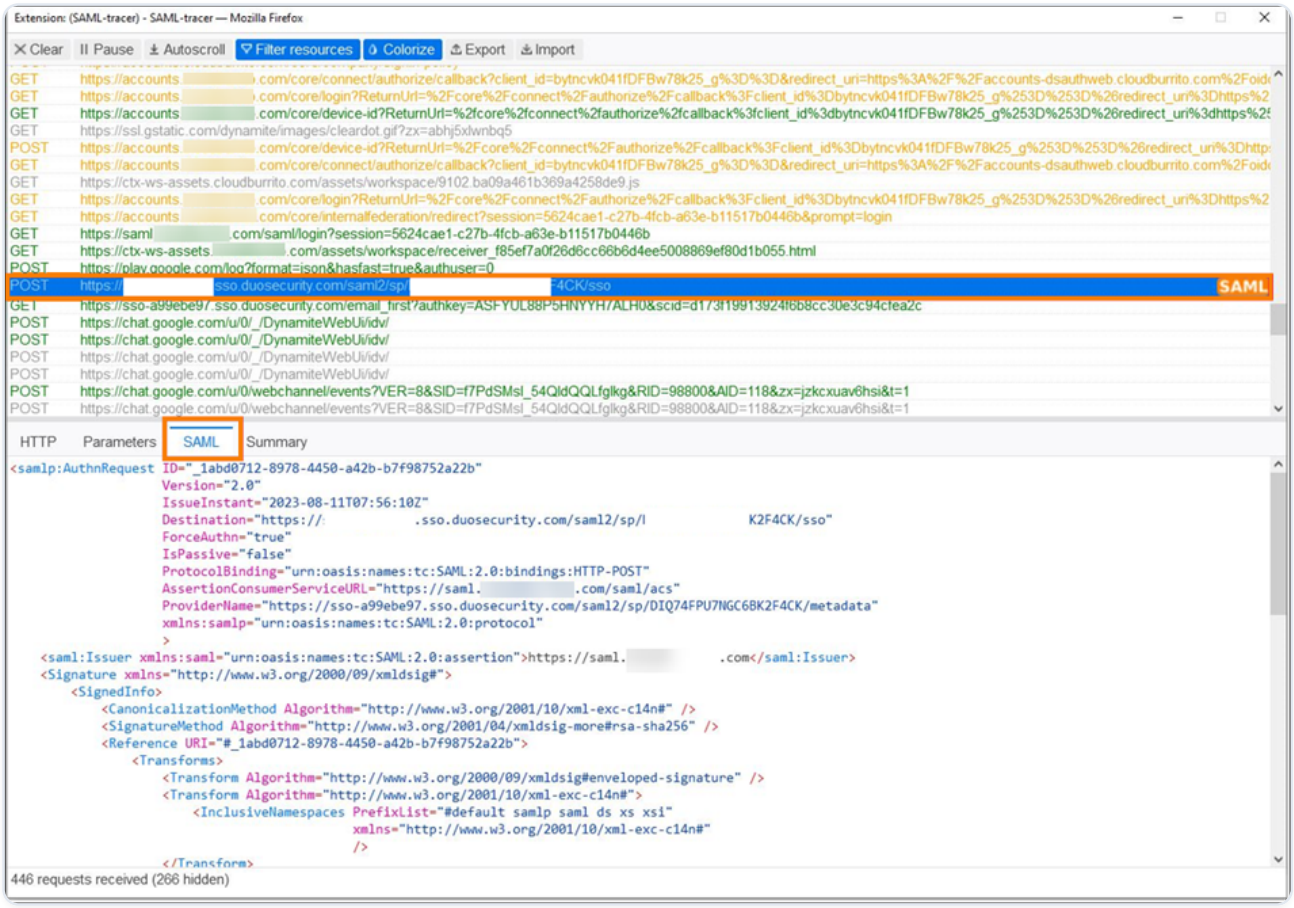
- 十分なコンテキストを含め、ログオンシナリオとCitrixまたはActive Directory環境を説明してください。

- 初期設定時にどのCitrix eDocsに従ったか。
- IdP内のSAMLアプリケーションのスクリーンショットと詳細。
- Active Directoryの詳細。
- SAMLトレーサーブラウザ拡張機能からのSAMLトレーサーファイル (`.json`) ファイル。
- ブラウザの開発者ツールから取得したHARファイル (`.har`)。
- 正常に動作しているエンドユーザーと、失敗しているエンドユーザー、またはCitrix Cloud管理者ユーザーの両方の詳細。
- ストアまたはCitrix CloudへのSAMLログオンを実行しているマシンのパブリック発信元IP。

Citrixサポートおよびエンジニアリングのための SAMLトレースの取得

Citrixエンジニアリングおよびサポートは、すべてのSAMLデバッグにSAMLトレーサーブラウザ拡張機能の使用を推奨しており、ブラウザ開発者ツールによって生成される`.HAR`ファイルも同様です。この拡張機能は、ほとんどの一般的なWebブラウザで利用でき、`.JSON`ファイルをエクスポートします。この拡張機能はSAMLリクエストとレスポンスをXMLにデコードし、人間が読める形式にして、理解とデバッグをはるかに容易にします。





ブラウザからHARファイルを収集してCitrixサポートおよびエンジニアリングに送信するにはどうすればよいですか?

詳細については、記事「HARファイルの収集」を参照してください。

役立つサードパーティ製SAMLデバッグツール

> **重要:**
>
> Citrixは、サードパーティ製ツールがデバッグ目的で使用された場合のいかなる責任も負いません。サードパーティ製ツールおよびウェブサイトの使用とアクセスは、お客様ご自身の責任で行ってください。

ツール	目的
https://www.samltool.io/	Base64 SAMLリクエストとレスポンスをデコードします

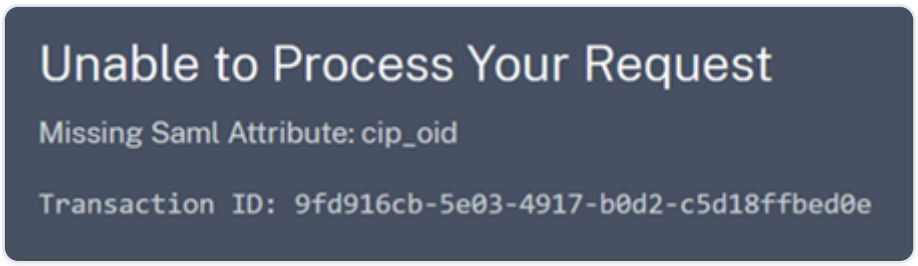
ツール	目的
https://www.sslshopper.com/certificate-decoder.html	証明書データをデコードします
https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract	SAMLメタデータから署名および暗号化証明書をファイルとして抽出します
https://www.whatismyip.com/	SAMLログオンを試行しているクライアントの発信元IPを提供します。

属性エラー

属性エラーは、以下のいずれかの条件下で発生する可能性があります。

- SAML構成で必要な属性が正しくエンコードされていません。
- `cip_sid`属性と`cip_upn`属性がSAMLアサーションにありません。
- `cip_sid`属性または`cip_oid`属性がSAMLアサーションにないか、接続の問題によりCitrix CloudがActive Directoryからそれらを取得できません。

属性エラーが発生すると、Citrix Cloudは問題のある属性を含むエラーメッセージを表示します。



この種のエラーを解決するには：

1. SAMLプロバイダーが、次の表に示すように、必要な属性を正しいエンコードで送信していることを確認してください。最低でも、SIDまたはUPN属性のいずれかが含まれている必要があります。

属性	エンコード	必須
cip_email	文字列形式である必要があります (`user@domain`)	
cip_oid	Base64または文字列形式である必要があります	

属性	エンコード	必須
cip_sid	Base64または文字列形式である必要があります	はい、`cip_upn`を使用しない場合
cip_upn	文字列形式である必要があります (`user@domain`)	はい、`cip_sid`を使用しない場合

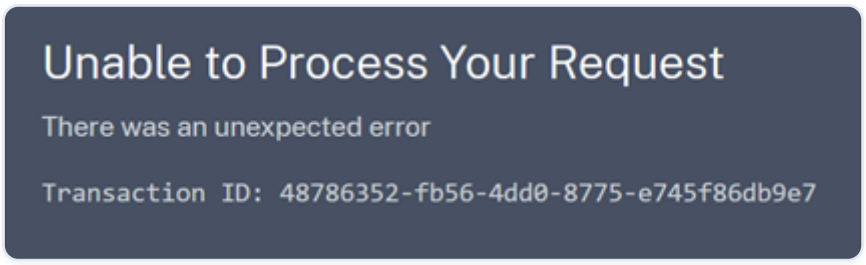
2. Citrix Cloudが必要とする不足している属性を取得できるように、Cloud Connectorがオンラインで正常であることを確認してください。詳細については、Cloud Connectorの高度なヘルスチェックを参照してください。

予期しないエラー

Citrix Cloudは、次の場合に予期しないエラーが発生する可能性があります。

- ユーザーがIDP開始フローを使用してSAMLリクエストを開始した場合。たとえば、ストアURLに直接移動する代わりに、IDプロバイダーのアプリポータルを介してタイルを選択することでリクエストが行われた場合 (`customer.cloud.com`)。
- SAML証明書が無効であるか、期限切れになっている場合。
- 認証コンテキストが無効である場合。
- SAMLアサーションと応答の署名が一致しない場合。

このエラーが発生すると、Citrix Cloudは一般的なエラーメッセージを表示します。



このエラーが、IDプロバイダーのアプリポータルを介してCitrix Cloudに移動した結果として発生する場合、以下の回避策を使用できます。

1. IDプロバイダーのアプリポータルで、ストアURLを参照するブックマークアプリを作成します（例: `https://customer.cloud.com`）。
2. SAMLアプリとブックマークアプリの両方にユーザーを割り当てます。
3. ブックマークアプリが表示され、SAMLアプリがアプリポータルで非表示になるように、SAMLアプリとブックマークアプリの可視性設定を変更します。

4. 追加のパスワードプロンプトを削除するには、Citrix® StoreFront Cloudで「**エンドユーザーに常に資格情報を要求する**」設定を無効にします。手順については、「エンドユーザーに常に資格情報を要求する」(/ja-jp/citrix-workspace/experience/sessions)を参照してください。

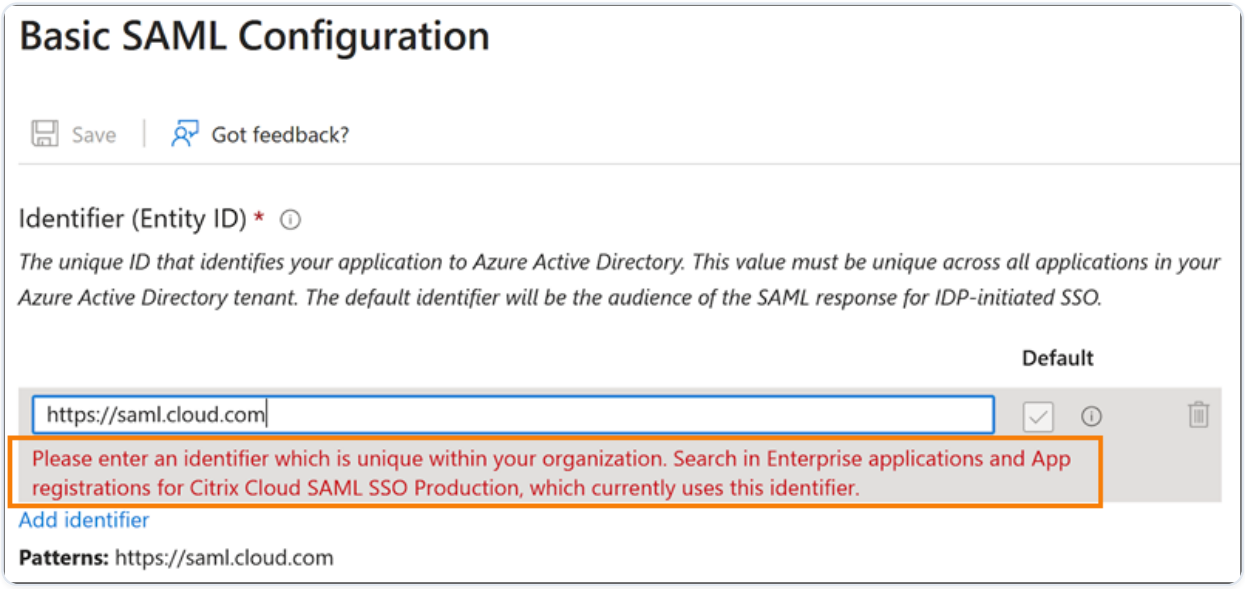
Citrix Cloud™ でスコープ付きエンティティIDを持つSAMLアプリケーションを構成する

この記事では、同じSAMLプロバイダー内で複数のSAMLアプリケーションをプロビジョニングする方法について説明します。

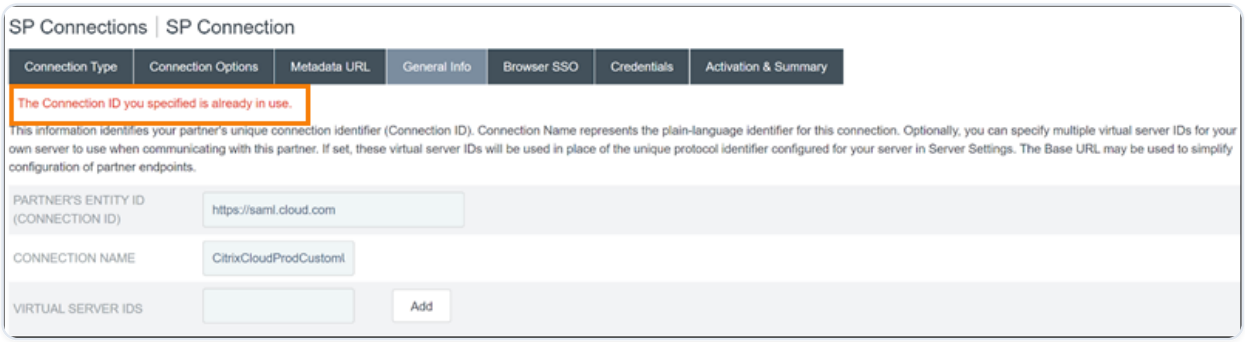
Microsoft Entra ID (ME-ID)、Active Directory Federation Services (ADFS)、PingFederate、PingSSOなどの一部のSAMLプロバイダーでは、複数のSAMLアプリケーション内で同じサービスプロバイダー (SP) エンティティIDを再利用することを禁止しています。そのため、同じSAMLプロバイダー内で2つ以上の異なるSAMLアプリケーションを作成する管理者は、それらを同じCitrix Cloudテナント、または異なるCitrix Cloudテナントにリンクできません。既存のSAMLアプリケーションがすでに使用しているSPエンティティID (`https:\\saml.cloud.com` など) を使用して2番目のSAMLアプリケーションを作成しようとすると、SAMLプロバイダーでエラーが発生し、エンティティIDがすでに使用されていることを示します。

次の画像は、このエラーを示しています。

- Microsoft Entra IDの場合:



- PingFederateの場合:



Citrix Cloudのスコープ付きエンティティ ID機能は、この制限に対処するため、SAMLプロバイダー (Microsoft Entra IDテナントなど) 内で複数のSAMLアプリケーションを作成し、それを単一の Citrix Cloudテナントにリンクできます。

エンティティIDとは何ですか?

SAMLエンティティIDは、SAML認証および認可プロトコルで特定のエンティティを識別するために使用される一意の識別子です。通常、エンティティIDは、エンティティに割り当てられ、SAMLメッセージおよびメタデータで使用されるURLまたはURIです。SAMLプロバイダー内で作成する各SAMLアプリケーションは、一意のエンティティと見なされます。

たとえば、Citrix CloudとMicrosoft Entra ID間のSAML接続では、Citrix Cloudがサービスプロバイダー (SP) であり、Microsoft Entra IDがSAMLプロバイダーです。どちらもSAML接続の反対側で構成する必要があるエンティティIDを持っています。これは、Citrix CloudのエンティティIDは Microsoft Entra ID内で構成する必要があり、Microsoft Entra IDのエンティティIDはCitrix Cloud内で構成する必要があることを意味します。

次のエンティティIDは、Citrix Cloudにおける汎用エンティティIDとスコープ付きエンティティIDの例です。

- 汎用: `https://saml.cloud.com`
- スコープ付き: `https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

地域別の汎用およびスコープ付きSPエンティティID

Citrix Cloudの既存のSAML接続（2023年11月より前に作成されたもの）は、各SAML接続および Citrix Cloudテナントで同じ汎用エンティティIDを使用します。新しいCitrix Cloud SAML接続のみが、スコープ付きエンティティIDを使用するオプションを提供します。

新しい接続にスコープ付きエンティティIDを使用することを選択した場合、既存のSAML接続はすべて、元の汎用エンティティIDを使用して引き続き機能します。

次の表に、Citrix Cloudの各地域における汎用およびスコープ付きSPエンティティIDを示します。

CITRIX CLOUD地域	汎用SPエンティティID	スコープ付きエンティティID
米国、欧州連合、アジア太平洋南部	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`
日本	`https://saml.citrixcloud.jp`	`https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29`
政府機関	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

新規および既存のSAML接続に一意のSPエンティティIDを生成する

新しいSAML接続を作成すると、Citrix Cloudは一意のID（GUID）を生成します。スコープ付きエンティティIDを生成するには、新しい接続を作成するときに**スコープ付きSAMLエンティティIDの構成**設定を有効にします。

既存のSAML接続を更新してスコープ付きエンティティIDを使用したい場合は、Citrix Cloudの**IDおよびアクセス管理 > 認証**ページからSAMLプロバイダーを切断し、再接続する必要があります。Citrix Cloudでは、既存のSAML接続を直接編集することはできません。ただし、構成を複製して、複製を変更することはできます。

> **重要：**
>
> SAML接続プロセスを完了する前に閉じると、Citrix Cloudが自動的に生成するエンティティIDは破棄されます。SAML接続プロセスを再開すると、Citrix Cloudは新しいスコープ付きエンティティID GUIDを生成します。SAMLプロバイダーを構成する際には、この新しいスコープ付きエンティティIDを使用してください。既存のSAML接続を更新してスコープ付きエンティティIDを使用する場合は、Citrix Cloudが生成するスコープ付きエンティティIDで、その接続のSAMLアプリケーションを更新する必要があります。

スコープ付きエンティティIDに関するよくある質問

同じMicrosoft Entra IDテナント内に複数のMicrosoft Entra ID SAMLアプリケーションを作成し、それを1つ以上のCitrix Cloudテナントにリンクできますか?

Citrix Cloudのスコープ付きエンティティ ID機能は、一部のSAMLプロバイダーが課す重複するエンティティIDの制限に対処します。この機能を使用すると、Microsoft Entra IDテナント内に複数のSAMLアプリケーションをプロビジョニングし、それぞれを単一のCitrix Cloudテナントからのスコープ付きエンティティIDで構成できます。

同じMicrosoft Entra ID SAMLアプリケーションを複数のCitrix Cloudテナントにリンクすることはできますか?

このシナリオはCitrix Cloudのお客様の間で一般的であり、Citrixは引き続きこれをサポートしています。このシナリオを実装するには、次の要件を満たす必要があります。

- `https://saml.cloud.com`のような汎用エンティティIDを使用します。
- SAML接続でスコープ付きエンティティIDを有効にしないでください。

SAMLプロバイダー内でスコープ付きエンティティIDを使用するかどうかをどのように決定しますか?

Citrix Cloudのスコープ付きエンティティIDは、要件に応じて汎用またはスコープ付きエンティティIDを使用する柔軟性を提供します。必要なSAMLアプリケーションの数と、所有しているCitrix Cloudテナントの数を考慮してください。また、各テナントが既存のSAMLアプリケーションを共有する可能性があるか、または独自のスコープ付きSAMLアプリケーションを必要とするかどうかも考慮してください。

> **重要:**
>
> SAMLプロバイダーが、同じエンティティIDを持つ複数のSAMLアプリケーションの作成をすでに許可している場合（`https://saml.cloud.com`など）、スコープ付きエンティティIDを有効にしたり、既存のSAML構成に変更を加えたりする必要はありません。Citrix CloudまたはSAMLアプリケーションのいずれにおいても、設定を更新する必要はありません。

影響を受けるSAMLプロバイダー

次の表に、重複するエンティティIDの使用を許可または制限するSAMLプロバイダーを示します。

SAMLプロバイダー	重複するエンティティIDをサポート
Microsoft Entra ID (クラウド)	いいえ
ADFS (オンプレミス)	いいえ
PingFederate (オンプレミス)	いいえ
PingOneSSO (クラウド)	いいえ
Okta (クラウド)	はい
Duo (クラウド)	はい
OneLogin (クラウド)	はい

影響を受けるユースケース

以下の表は、ユースケースで必要となるSAMLアプリケーションと、SAMLプロバイダーが重複するエンティティIDをサポートしているかどうかに基づいて、汎用またはスコープ付きのエンティティIDがサポートされているかどうかを示しています。

ユースケースの要件	SAMLプロバイダーは重複するエンティティIDをサポートしていますか？	サポートされる構成
SAMLアプリケーションは1つのみ	はい	汎用またはスコープ付きのエンティティID
SAMLアプリケーションは1つのみ	いいえ	汎用またはスコープ付きエンティティID
2つ以上のSAMLアプリケーション	はい	汎用またはスコープ付きエンティティID
2つ以上のSAMLアプリケーション	いいえ	スコープ付きエンティティID
カスタムURLとSAMLアプリケーションのペアを保存する	はい	汎用またはスコープ付きエンティティID
カスタムURLとSAMLアプリケーションのペアを保存する	いいえ	スコープ付きエンティティID

ユースケースの要件	SAMLプロバイダーは重複するエンティティIDをサポートしていますか？	サポートされる構成
同じSAMLアプリケーションを複数のCitrix Cloudテナントにリンクする	はい	汎用エンティティID
同じSAMLアプリケーションを複数のCitrix Cloudテナントにリンクする	いいえ	汎用エンティティID

スコープ付きエンティティIDでプライマリSAML接続を構成する

このタスクでは、プライマリSAMLアプリケーション（SAMLアプリ1）のスコープ付きエンティティIDを使用して、Citrix CloudでSAML接続を作成します。

1. Citrix Cloudメニューから、**［IDおよびアクセス管理］**を選択します。
2. **［認証］タブで、［SAML 2.0］を見つけ、省略記号メニューから［接続］**を選択します。
3. 一意のサインインURLを作成するよう求められたら、会社用の短くURLフレンドリな識別子（例：`https://citrix.cloud.com/go/mycompany`）を入力し、**［保存して続行］**を選択します。この識別子は、Citrix Cloud全体で一意である必要があります。
4. **［SAML IDプロバイダーの構成］で、［スコープ付きSAMLエンティティIDの構成］**を選択します。Citrix Cloudはスコープ付きエンティティを自動的に生成し、エンティティID、アサーションコンシューマーサービス、ログアウトURLのフィールドに入力します。
5. **［Citrix CloudへのSAML接続の構成］**で、SAMLプロバイダーからの接続詳細を入力します。
6. デフォルトのSAML属性マッピングを受け入れます。
7. **［テストして完了］**を選択します。

汎用エンティティIDでプライマリSAML接続を構成する

このタスクでは、プライマリSAMLアプリケーション（SAMLアプリ1）のデフォルトの汎用エンティティIDを使用して、Citrix CloudでSAML接続を作成します。

1. Citrix Cloudメニューから、**IDおよびアクセス管理**を選択します。
2. **認証**タブで、**SAML 2.0**を見つけ、省略記号メニューから**接続**を選択します。

3. 一意のサインインURLを作成するよう求められたら、会社用の短くURLフレンドリーな識別子（例: `https://citrix.cloud.com/go/mycompany`）を入力し、**保存して続行**を選択します。この識別子はCitrix Cloud全体で一意である必要があります。
4. **SAML IDプロバイダーの構成**で、**スコープ付きSAMLエンティティIDの構成**が無効になっていることを確認します。
5. **Citrix CloudへのSAML接続の構成**で、SAMLプロバイダーからの接続詳細を入力します。
6. **サービスプロバイダーSAMLメタデータ**で、必要に応じて**ダウンロード**をクリックして汎用SAMLメタデータのコピーを取得します。
7. デフォルトのSAML属性マッピングを受け入れます。
8. **テストして完了**を選択します。

Citrix® StoreFront Cloudカスタムドメインを使用したSAML接続の構成

このセクションでは、スコープ付きまたは汎用エンティティIDのいずれかを使用して、カスタムストアURLでSAML接続を構成する方法について説明します。

このセクションのタスクは、SAMLで使用している既存のカスタムストアURLがある場合にのみ適用されます。SAML認証でカスタムストアURLを使用していない場合は、このセクションのタスクをスキップできます。

詳細については、以下の記事を参照してください。

- カスタムドメインの構成
- カスタムドメインを使用してSAMLでストアにサインイン

ストアカスタムURLと汎用エンティティIDを使用したSAML接続の構成

このタスクでは、**スコープ付きエンティティIDの構成**設定は無効になっています。

1. Citrix Cloudメニューから、**ストア認証**を選択します。
2. **カスタムストアURL**で、省略記号メニューから**編集**を選択します。
3. **.cloud.com URLとカスタムドメインURLの両方を使用**を選択します。
4. SAML App 2の汎用エンティティID、SSO URL、およびオプションのSLO URLを入力し、SAMLプロバイダーから以前にダウンロードした署名証明書をアップロードします。
5. 必要に応じて、**カスタムドメインのサービスプロバイダーSAMLメタデータ**で、**ダウンロード**をクリックして、ストアカスタムURL SAMLアプリケーションの汎用SAMLメタデータのコピーを取得します。
6. **保存**をクリックします。

ストアカスタムURLとスコープ付きエンティティIDを使用してSAML接続を構成する

このタスクでは、**スコープ付きエンティティIDの構成**設定は有効になっています。

1. Citrix Cloudメニューから、**ストア認証**を選択します。
2. **カスタムストアURL**で、省略記号メニューから**編集**を選択します。
3. **.cloud.com URLとカスタムドメインURLの両方を使用**を選択します。
4. SAML App 2のスコープ付きエンティティID、SSO URL、およびオプションのSLO URLを入力し、SAMLプロバイダーから以前にダウンロードしたSAML署名証明書をアップロードします。
5. **保存**をクリックします。

構成を保存すると、Citrix Cloudは正しいGUIDを含むスコープ付きSAMLメタデータを生成します。必要に応じて、ストアカスタムURL SAMLアプリケーションのスコープ付きメタデータのコピーを取得できます。

1. 「**認証とアクセス管理**」ページで、SAML接続を見つけ、省略記号メニューから「**表示**」を選択します。
2. 「**カスタムドメインのサービスプロバイダーSAMLメタデータ**」で、「**ダウンロード**」をクリックします。

プライマリおよびカスタムストアURLのSAMLアプリケーション両方のSAML構成を表示する

スコープ指定されたSAML接続の構成詳細を表示すると、Citrix Cloudはプライマリ SAMLアプリケーションとストアカスタムドメインSAMLアプリケーションの両方のスコープ指定されたエンティティID設定を表示します。

たとえば、スコープ指定されたエンティティIDが有効になっている場合、「**サービスプロバイダーエンティティID**」および「**カスタムドメインのサービスプロバイダーエンティティID**」フィールドには、Citrix Cloudが生成するスコープ指定されたエンティティIDが含まれます。

スコープ指定されたエンティティIDが有効なSAML構成(/en-us/citrix-cloud/media/saml-entity-id-scoped-custom-domain-example.png)

スコープ指定されたエンティティIDが無効になっている場合、「**サービスプロバイダーエンティティID**」および「**カスタムドメインのサービスプロバイダーエンティティID**」フィールドには、汎用エンティティIDが含まれます。

汎用エンティティIDを使用したSAML構成(/en-us/citrix-cloud/media/saml-entity-id-generic-custom-domain-example.png)

既存のエンティティID値にスコープ指定されたエンティティIDを追加することで、SAMLプロバイダー内の既存のSAMLアプリケーションを更新できます。

スコープ指定されたエンティティIDを使用したSAMLプロバイダー構成

Citrix Cloudでスコープ指定されたエンティティIDを使用してSAML接続を構成した後、スコープ指定されたエンティティIDをSAMLプロバイダーに追加できます。

このセクションには、Microsoft Entra IDとPingFederateの構成例が含まれています。

スコープ指定されたエンティティIDを使用したMicrosoft Entra ID SAML構成

この例では、Citrix Cloudからのスコープ指定されたエンティティIDが、Microsoft Entra IDの「**識別子**」フィールドに入力されています。

エンティティIDが強調表示されたMicrosoft Entra IDのSAMLアプリケーション構成(/en-us/citrix-cloud/media/saml-entity-id-aad-example-config.png)

スコープ付きエンティティIDを使用したPingFederate SAML構成

この例では、Citrix Cloud のスコープ付きエンティティIDと汎用エンティティIDが、それぞれ **Partner's Entity ID** フィールドと **Base URL** フィールドに入力されます。

Summary

SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

トラブルシューティング

Citrixでは、SAML構成に関する問題をトラブルシューティングするために、SAML-tracerブラウザ拡張機能を使用することをお勧めします。この拡張機能は、Base64でエンコードされた要求と応答をSAML XMLにデコードし、情報を人間が読める形式で表示します。SAML-tracer拡張機能を使用して、Citrix Cloud（サービスプロバイダー）が生成してSAMLプロバイダー（IDプロバイダー）に送信するSSOおよびSLO SAML要求の両方を調べることができます。この拡張機能は、エンティティIDスコープ（GUID）が両方の要求に含まれているかどうかを示すことができます。

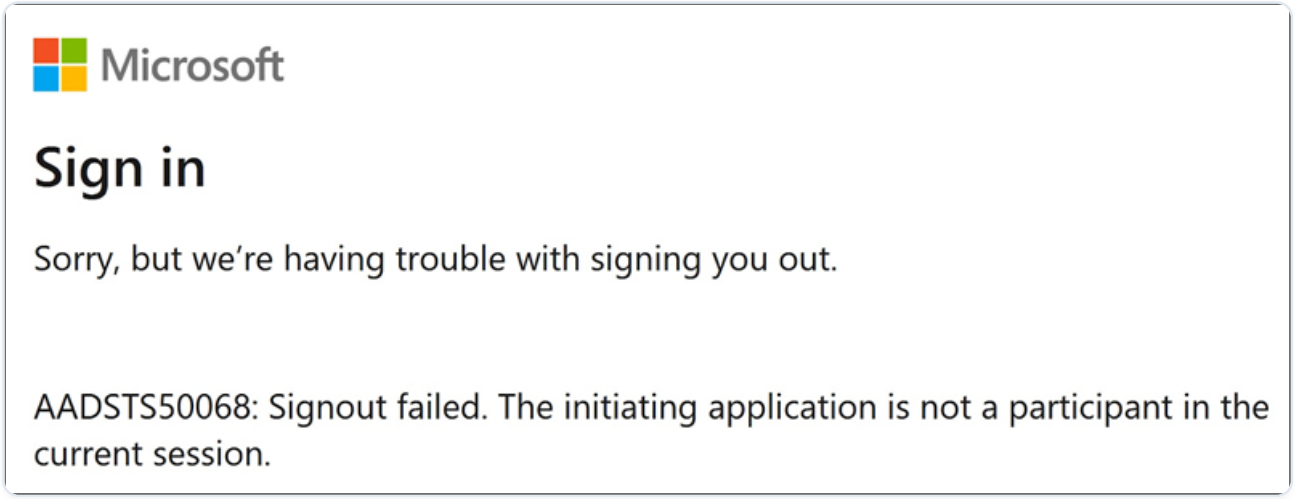
1. Webブラウザの拡張機能パネルから、SAML-tracer拡張機能をインストールして有効にします。
2. SAMLサインインおよびサインアウト操作を実行し、SAML-tracer拡張機能でフロー全体をキャプチャします。
3. SAML SSO要求またはSLO要求のいずれかから、次の行を見つけます。

   ```
   <saml:Issuer
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://
   saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</saml:Issuer>
   ```

4. エンティティIDがSAMLプロバイダーアプリケーションで構成されているエンティティIDと一致することを確認します。
5. スコープ付きエンティティIDが **Issuer** フィールドに存在することを確認し、SAMLプロバイダーで正しく構成されていることを確認します。
6. SAML-tracerのJSON出力をエクスポートして保存します。Citrixサポートと協力して問題を解決している場合は、出力をCitrixサポートケースにアップロードしてください。

Microsoft Entra IDのトラブルシューティング

問題: SLOが構成されている場合、Microsoft Entra IDからのサインアウトが失敗します。Microsoft Entra IDはユーザーに次のエラーを表示します。



Citrix CloudのSAML接続でスコープ付きエンティティIDが有効になっている場合、スコープ付きエンティティIDはSSO要求とSLO要求の両方で送信される必要があります。

原因: スコープ付きエンティティは構成されていますが、エンティティIDがSLOリクエストにありません。SAMLトレーサー出力で、スコープ付きエンティティIDがSLOリクエストに存在することを確認してください。

オンプレミスPingFederateのトラブルシューティング

問題: スコープ付きエンティティID設定を有効にした後、PingFederateへのサインインまたはサインアウトが失敗します。

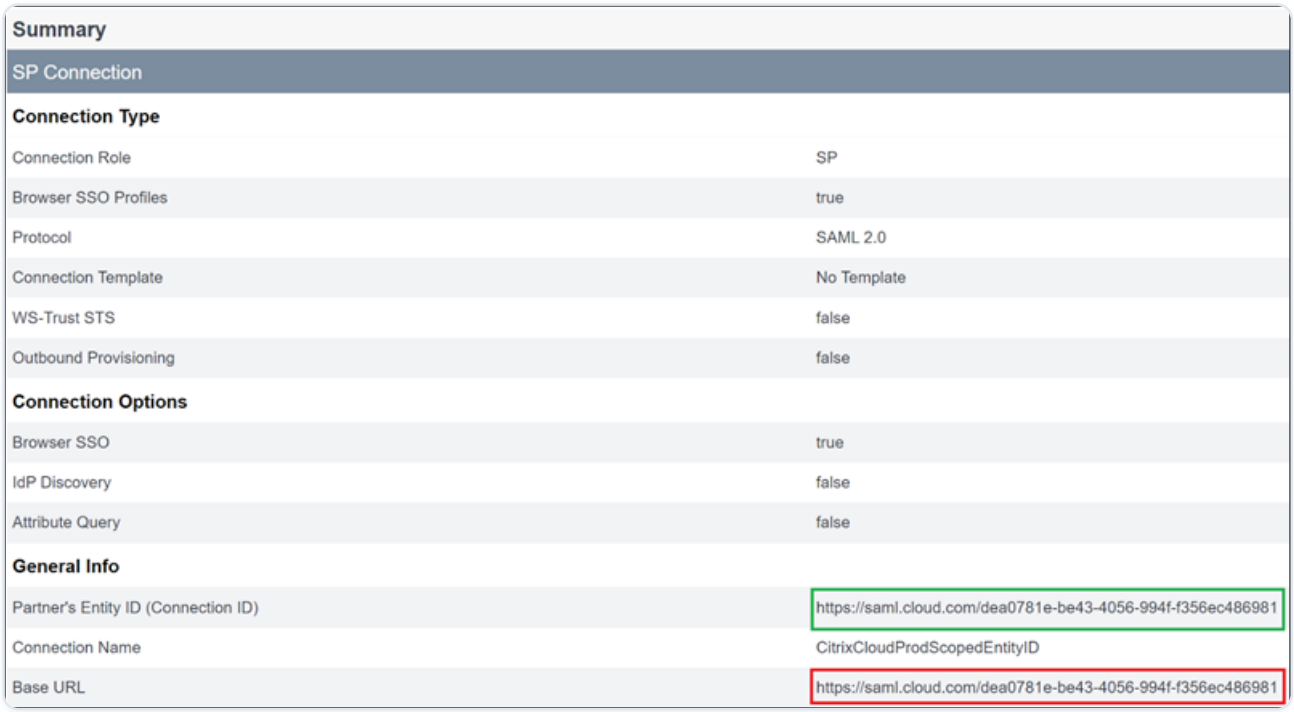
原因: PingFederate管理者が、スコープ付きエンティティIDをSP接続のベースURLに追加しました。

この問題を解決するには、スコープ付きエンティティIDを**Partner's EntityID**フィールドにのみ追加してください。スコープ付きエンティティIDをベースURLに追加すると、SAMLエンドポイントが不正な形式になります。Citrix Cloudのベース URLが誤って更新された場合、ベースURLから派生する他のすべてのSAMLエンドポイント相対URLでサインインエラーが発生します。

SAMLトレーサー出力に表示される可能性のある、不正な形式のCitrix Cloud SAMLエンドポイントの例を次に示します。

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

次の画像は、誤って構成されたPingFederate SAMLアプリケーションを示しています。正しく構成されたフィールドは緑色で表示されています。誤って構成されたフィールドは赤色で表示されています。



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

複数のカスタムURLを使用してSAMLでストアにサインインする

ストアのカスタムURLでSAMLをサポートするアーキテクチャは、SAML IdP内で構成された**1つのSAMLアプリケーション**のみを使用して、複数のカスタムドメインをサポートするように簡素化および更新されました。Citrix Cloudの認証プラットフォームとストアのカスタムURLサービス内で変更が行われ、SAMLと条件付き認証で最大10個のカスタムURLをサポートできるようになりました。従来、`cloud.com` SAMLエンドポイントを持つSAMLアプリケーションを1つ、カスタムURLを含むSAMLエンドポイントを持つSAMLアプリケーションをもう1つ構成する必要がありました。すべてのSAMLユースケースをサポートするために、複数の異なるSAMLアプリケーションを作成および維持する必要はなくなりました。

複数のカスタムURLをサポートする新しいアーキテクチャの利点。

Citrix CloudのSAMLエンドポイントを含むSAMLアプリケーションを1つだけ作成します。これは、`saml.cloud.com` (米国、EU、APS)、`saml.citrixcloud.jp` (日本)、`saml.cloud.us` (政府) など、Citrix Cloudの地域と一致します。

SAMLアプリケーションエンドポイントの例：

- エンティティID `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
- アサーションコンシューマーサービス (SSO): `https://saml.cloud.com/saml/acs`
- ログアウト (SLO): `https://saml.cloud.com/saml/logout/callback`

サポートされているSAMLログオンユースケース：

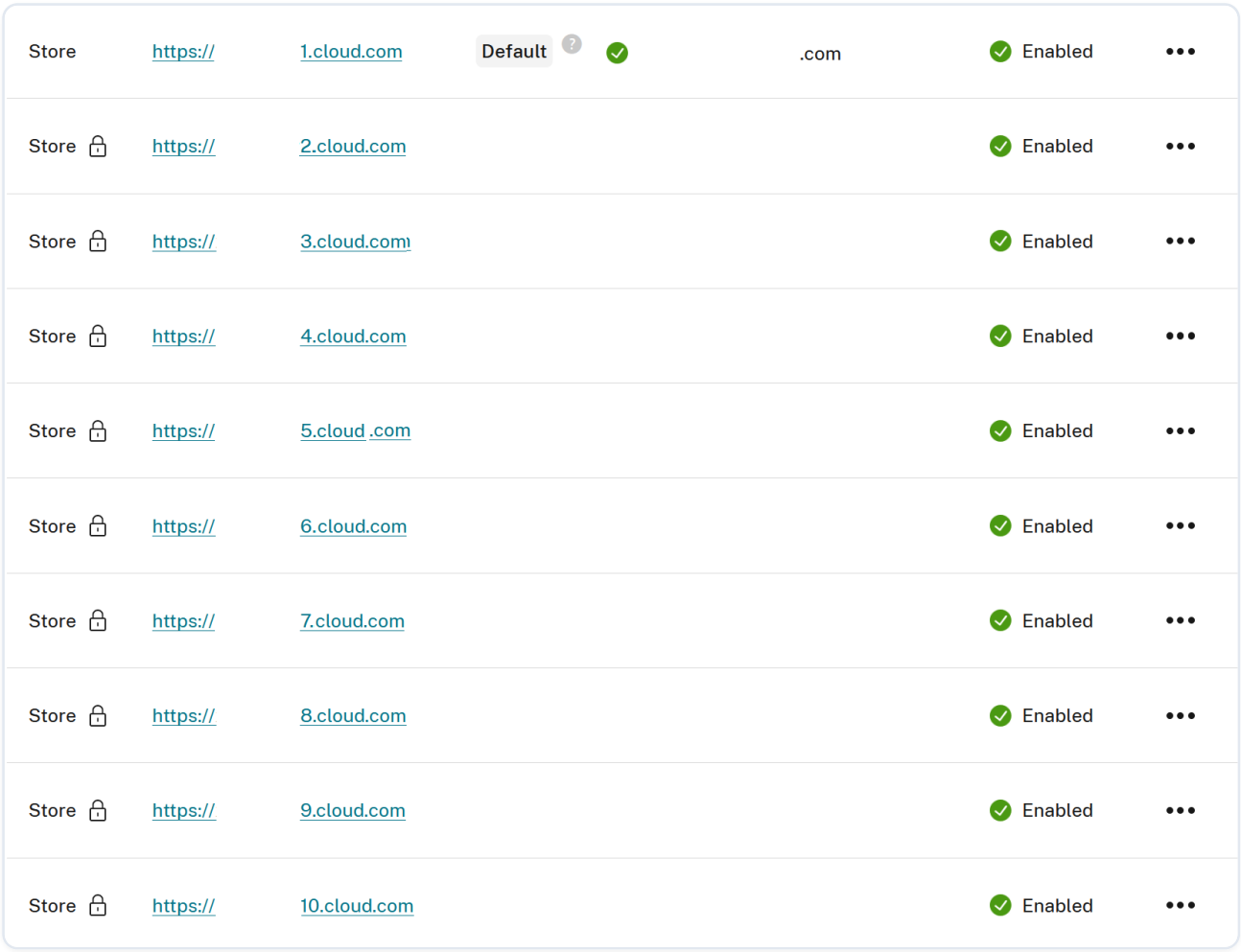
- 単一のSAMLアプリケーションを使用して、いずれかのストアURLでストアにログオンします。 `store.cloud.com` または `store.mycustomer.com`
- 管理者アクセス用のSAMLを使用してCitrix Cloudにログオンする場合も、同じ汎用SAMLアプリケーションを使用します。
- IdP内の単一のSAMLアプリケーションで、複数の異なるSAMLアプリケーションを作成および維持することなく、最大10個のストアカスタムURLをサポートできるようになりました。Citrix Cloudは、すべてのSAMLユースケースをサポートするために、カスタムURL SAMLエンドポイントを持つ追加のSAMLアプリケーションを必要としなくなりました。

よくある質問

ストアの複数カスタムURL機能とは何ですか?

従来、Citrix Cloudは最初のストア `cloud.com` URLにリンクされた単一のカスタムURLのみをサポートしていました。現在、最大10個のストア `cloud.com` URLそれぞれにカスタムURLを構成できます。これらはURLのペアを形成し、各カスタムURLは対応する `cloud.com` URLのDNSにおけるCNAMEです。

マルチカスタムURLのリリース前は、プライマリ `cloud.com` ストアURLに関連付けられたカスタムURLは1つのみ、**StoreFront Cloud > Access** でサポートされていました。



マルチカスタムURLのリリース後の **StoreFront Cloud > Access**。現在、1〜10個のカスタムURLがサポートされています。

CITRIX CLOUD™

Name	Cloud URL	Custom URL
Store Default	1.cloud.com	1. .com
Store	2.cloud.com	2. .com
Store	3.cloud.com	3. .com
Store	4.cloud.com	4. .com
Store	5.cloud.com	5. .com
Store	6.cloud.com	6. .com
Store	7.cloud.com	7. .com
Store	8.cloud.com	8. .com
Store	9.cloud.com	9. .com
Store	10.cloud.com	10. .com

カスタムURLを移行する必要があるかどうかは、どのように判断すればよいですか?

これは、Citrix Cloudとストアで使用したい認証機能の組み合わせ、現在のログオンシナリオ、および現在のSAMLソリューションによって決まります。ガイダンスについては、以下の表を使用してください。

SAMLログオンシナリオ	未移行のカスタムURL	移行済みのカスタムURL
カスタムURLエンドポイントを使用して1つのSAMLアプリでストアにログオン	サポートされています (カスタムURL 1つ)	サポートされていません (カスタムURL 1〜10個)
2つのSAMLアプリでストアにログオン	サポートされています (カスタムURL 1つ)	サポートされています (カスタムURL 1〜10個)
SAML 1xアプリと`cloud.com` URLエンドポイ	サポート対象	サポート対象

SAMLログオンシナリオ	未移行のカスタムURL	移行済みのカスタムURL
ントを使用したCitrix Cloud管理者ログイン		
2x SAMLアプリを使用したCitrix Cloud管理者ログイン	サポート対象	サポート対象
SAML 1xアプリと**カスタムURLエンドポイント**を使用したCitrix Cloud管理者ログイン	サポート対象外	サポート対象外
ストアURLとSAMLを使用した条件付き認証ポリシー	サポート対象	サポート対象
エンドユーザーがブラウザまたはCitrix Workspaceアプリに`cloud.com` **URL**を入力		
ストアURLとSAMLを使用した条件付き認証ポリシー	サポート対象外（カスタムURL 1つ）	サポート対象（URL 1〜10個）
エンドユーザーがブラウザまたはCitrix Workspaceアプリに**カスタムURL**を入力する		

複数のカスタムURLをサポートするために、SAMLとカスタムURLのアーキテクチャを変更する必要があったのはなぜですか?

スケーラビリティ。Citrix Cloudに複数のカスタムURLが導入されたことで、カスタムURLごとにSAMLアプリを必要とする従来のアーキテクチャではスケーリングできず、Citrix Cloud管理者とIdP管理者の両方にとって非現実的です。

従来のSAMLカスタムURLの要件:

- SAMLを使用したCitrix Cloud管理者ログオン用のSAMLアプリケーション`cloud.com` 1つ。
- カスタムURLごとにSAMLアプリケーション1つ。

IdP構成の複雑さ。各SAMLアプリケーションは、SAMLエンドポイントを除いて同一に構成する必要があり、SAML IdP内で追加の作業が発生していました。これにより、展開と構成の複雑さが増していました。新しいマルチカスタムドメインアーキテクチャでは、この必要がなくなり、IdP内で1つのSAMLアプリケーションだけで1〜10個のカスタムURLをサポートできます。

継続的なIdPメンテナンス作業。複数のSAMLアプリケーションを構成および維持し、複数のSAMLアプリケーションで継続的な年間証明書ローテーション作業を実行することは、Citrix Cloud管理者とIdP管理者の両方にとって労力がかかり、望ましくありません。この問題は、カスタムドメインが追加され、より多くのSAMLアプリケーションが必要になるにつれて、管理者にとってさらに増大します。新しいアーキテクチャでは、すべてのSAMLおよびカスタムURLのユースケースで1つのSAMLアプリケーションのみが必要となるため、このメンテナンスの問題が解消されます。

Citrixが現在のカスタムURL SAMLソリューションから新しいよりシンプルなソリューションへの移行を求めているのはなぜですか?

マルチカスタムURL機能とカスタムURLでの条件付き認証の両方を使用するには、従来の1xおよび2x SAMLアプリケーション構成を更新および移行する必要があります。このドキュメントには、従来の1xまたは2x SAMLアプリケーションソリューションのいずれかを使用しているお客様向けの移行方法に関する手順が含まれています。

StoreFront Cloud > アクセス内のこの警告は、1つ以上のカスタムURLが移行を必要としていることを示しています。

SAMLカスタムドメインURL警告(/en-us/citrix-cloud/media/saml-custom-domain-url-warning.png)

この警告は、**StoreFront Cloud > 認証**内でSAMLまたは条件付き認証のいずれかを有効にしている場合にのみ表示されます。

認証ページのスクリーンショット(/en-us/citrix-cloud/media/saml-custom-domain-workspace-config.png)

最大10個までのすべての新しいカスタムURLをサポートするために、SAML IdP構成は同じですか?

はい。ストアにアクセスするために1つだけ、または複数のカスタムURLを使用する意図がある場合は、SAMLアプリケーションを同一に構成してください。

複数のSAMLアプリと複数のカスタムドメインで、条件付き認証は現在サポートされていますか?

はい。これは、多くの大企業が利用したいと考える一般的なシナリオです。1〜10個の `cloud.com` URLのいずれかを使用して、異なるSAMLアプリケーションに解決する条件付き認証ポリシーを作成することは常に可能でした。これで、各`cloud.com` URLは独自のカスタムURL（URLのペア）を持つことができます。

エンドユーザーが使用するストアURLに基づいて異なるIdP間の切り替えに関する詳細な手順については、この記事条件付き認証の記事を参照してください。

複数のカスタムURLを使用しない場合、またはカスタムURLとSAMLで条件付き認証を使用しない場合、移行されていないレガシーSAML接続は引き続き機能します?

はい。既存のレガシー1xおよび2x SAMLアプリソリューションとの下位互換性は維持され、既存のSAMLアプリケーションソリューションは引き続き機能し、サポートされます。カスタムURLのいずれかが未移行の状態のままである場合、SAMLまたは条件付き認証でカスタムURLを使用することはできません。

マルチカスタムURL機能のリリース後に新しいカスタムURLをオンボードした場合、これらの新しいURLに対して移行を実行する必要があります?

いいえ。マルチカスタムURL機能のリリース後に新しくオンボードされたすべてのカスタムドメインは、新しいアーキテクチャをサポートし、移行する必要はありません。移行は、マルチカスタムURL機能のリリース前に作成されたカスタムURL構成にのみ適用されます。これは通常、複数のカスタムURLのサポートが導入される前に存在していた、Citrix Cloudテナント内で構成した最初で唯一のカスタムURLに該当します。

レガシーカスタムURLとSAML構成の移行

移行アクションを実行する前に、現在のカスタムURLとSAML構成、および現在**1xまたは2x SAMLアプリケーション**ソリューションで運用しているかどうかを理解するために、レガシーカスタムURL SAML構成セクション全体を読む必要があります。移行アクションは計画されたメンテナンス期間中に実施し、IdPから古いSAMLアプリケーションを削除する前に、移行後にテストを実施してSAMLログオンに影響がないことを確認する必要があります。

> **重要:**
>
> このドキュメントの「レガシーカスタムURL SAML構成」セクションで説明されている1xまたは2x SAMLアプリソリューションのいずれとも、Citrix CloudとSAML IdPの両方におけるレガシーSAML構成が正確に一致しない場合、サポートされていない状態になります。

現在の2x SAMLアプリケーションカスタムURLソリューションから、よりシンプルな新しいソリューションへ移行するにはどうすればよいか?

1. Citrix Cloud管理者は、Citrix CloudのカスタムURLサービスとSAML IdPの両方で必要な変更を行うために、IdP管理者と連携する必要があります。
2. SAML IdP内で、プライマリおよびセカンダリSAMLアプリケーションの両方の存在と構成を確認します。これは、EntraID、Okta、Duo、PingFederateなどのSAML IdPごとに異なります。

3. 既存のプライマリSAMLアプリケーションのCitrix Cloud SAMLエンドポイントを変更しないでください。これは、**Identity and Access Management > Authentication**内に表示されるSAMLアプリケーションであり、カスタムURLの移行後、すべてのSAMLログオンユースケースに使用されます。

   Citrix Cloud Commercial US、EU、およびAPSからのプライマリアプリケーションの例

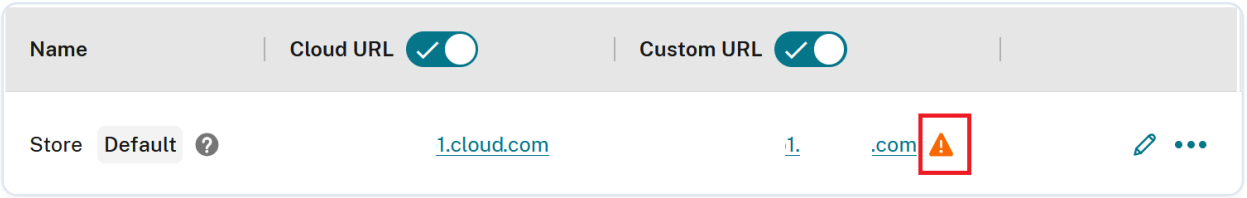
   - エンティティID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
   - アサーションコンシューマーサービス (SSO): `https://saml.cloud.com/saml/acs`
   - ログアウト (SLO): `https://saml.cloud.com/saml/logout/callback`

4. この廃止されたセカンダリSAMLアプリケーションを特定します。このSAMLアプリケーションの構成は、**StoreFront Cloud > Access**メニュー内で指定されています。

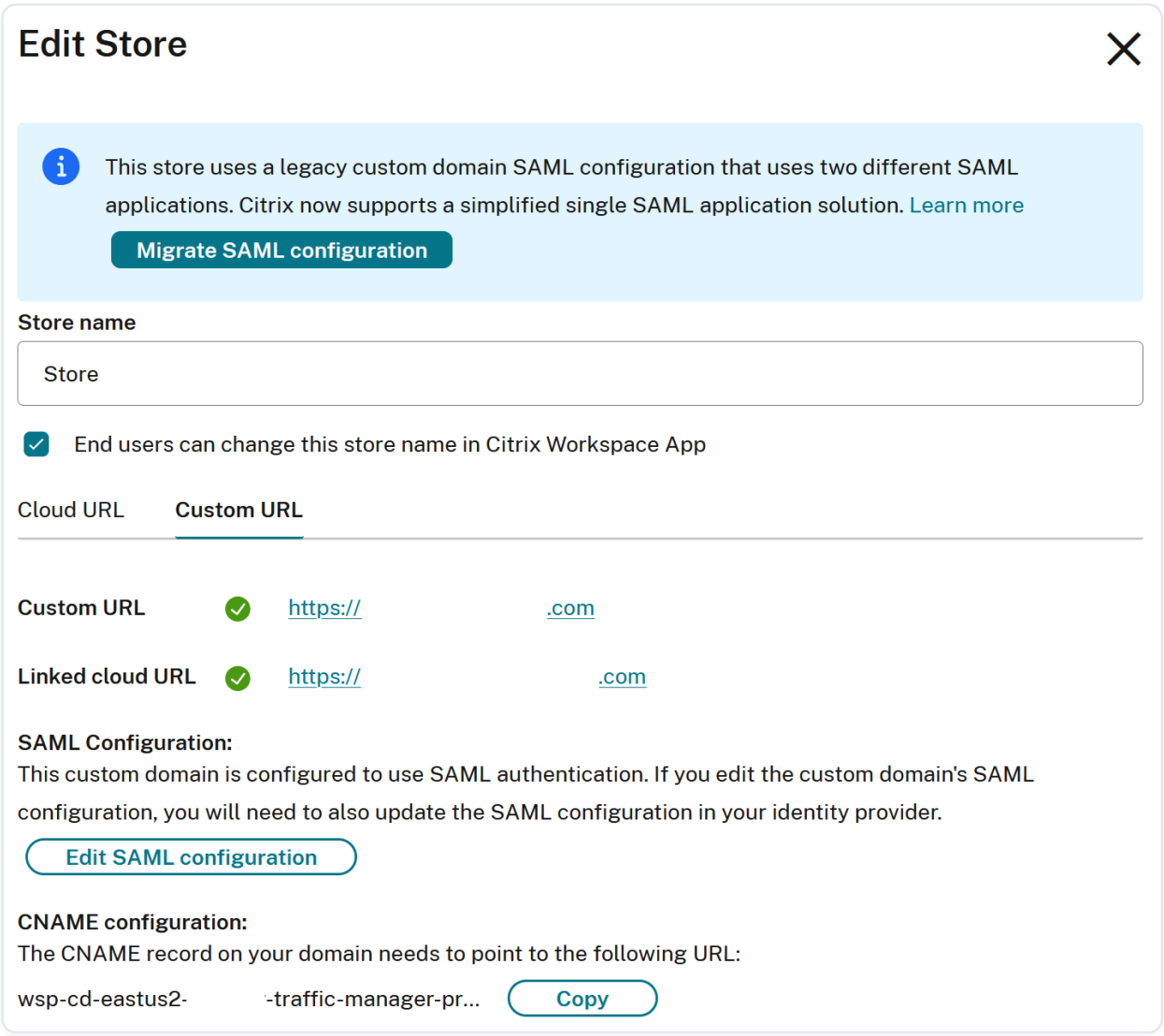
   セカンダリアプリケーションの例

   - エンティティID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
   - アサーションコンシューマーサービス (SSO): `https://workspaces.mycompany.com/saml/acs`
   - ログアウト (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

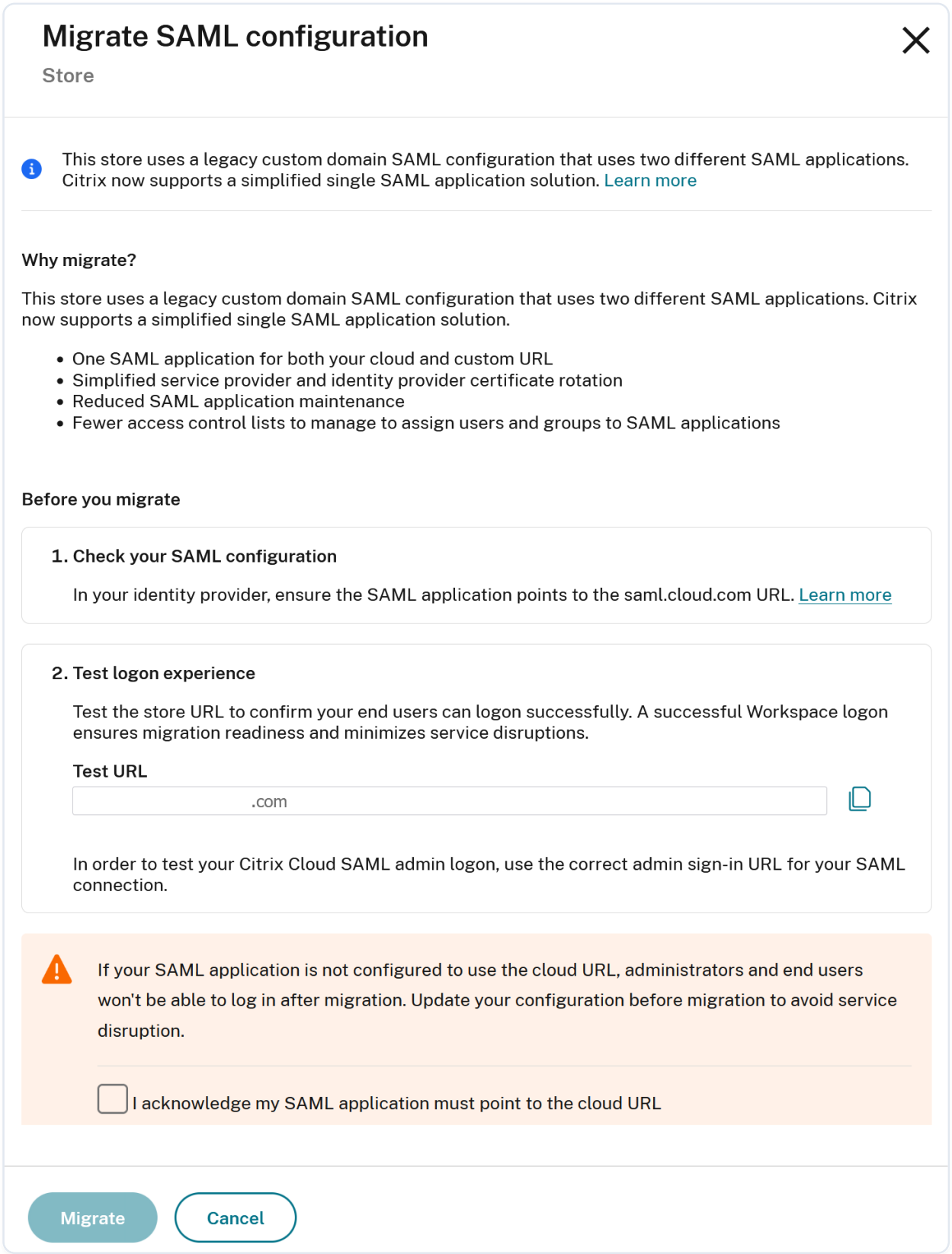
5. 「**StoreFront Cloud > アクセス**」に移動し、「**警告アイコン**」をクリックして移行UIを開きます。



6. 以下に示す「**SAML構成を移行**」ボタンをクリックします。



7. 警告を受け入れ、このUI内から移行を実行します。



8. 「**移行**」をクリックします。

> **重要:**

> 移行により、ストアのカスタムURLサービス内のレガシーバックエンドデータが更新されます。これは、ストアのカスタムURLサービスレコードに対する元に戻せない操作であり、一度実行すると元に戻すことはできません。

9. 移行が成功すると、カスタムURLの横にステップ4で表示された警告アイコンが消えるはずです。これは、ストアのカスタムURLサービス内のバックエンドデータが更新されたことを示します。

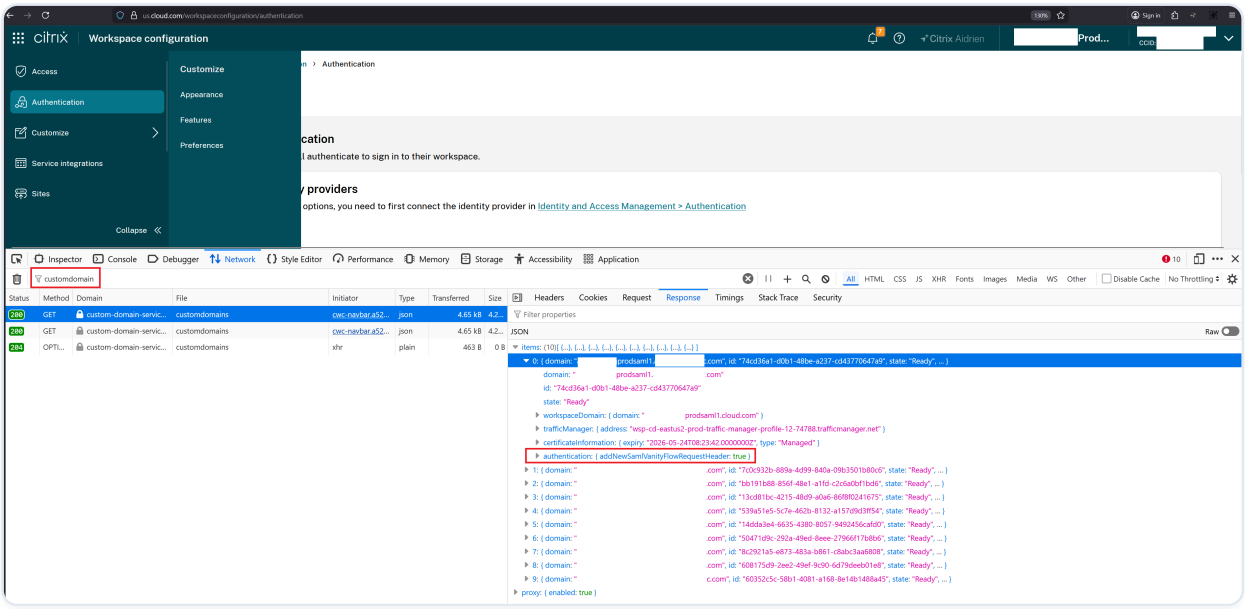
   移行後もすべてのSAMLログオンユースケースが正常に機能することを確認します。

   - `cloud.com` URLを使用して、ストアへのSAMLログオンをテストします。これはプライマリSAMLアプリケーションを使用します。
   - すべてのカスタムURLを使用して、ストアへのSAMLログオンをテストします。これは以前、移行**前**はセカンダリSAMLアプリケーションを使用していましたが、現在は変更されていないプライマリSAMLアプリケーションを使用します。
   - 移行前に構成されたAD管理者ユーザーおよびグループを使用して、管理者サインインURLを使用してCitrix CloudへのSAMLログオンをテストします。これはプライマリSAMLアプリケーションを使用します。

10. バックエンドストアのカスタムURLサービスデータが正常に更新されたことを確認します。

    例: FireFox開発者ツールを使用する場合。

    キーボードのF12キーを押してブラウザの開発者ツールを開き、開発者ツールがすでに実行されているCitrix Cloud UIの他のページから「**StoreFront Cloud > アクセス**」に移動します。これにより、Citrix Cloudコンソールが行うすべてのREST API呼び出しがキャプチャされ、カスタムURLのリストが返されます。



ネットワーク検索ダイアログに `customdomain` を入力して、正しい REST API 呼び出しをフィルタリングします。

この REST API 呼び出しを見つけます:

`GET https://custom-domain-service.us.wsp.cloud.com/services/custom-domain-service/customers/<CCID>/stores/<storeID>/customdomains`

移行されたカスタム URL オブジェクトには、この追加データが含まれます。

`"addNewSamlVanityFlowRequestHeader":true`

カスタム URL オブジェクトの例:

```
"items": [

    {

        "domain": "stores.mycompany.com",

        "id": "74cd36a1-d0b1-48be-a237-cd43770647a9",

        "state": "Ready",

        "workspaceDomain": {

            "domain": "stores.cloud.com"

        },
```

```
        "trafficManager": {

            "address": "wsp-cd-eastus2-prod-traffic-manager-
profile-12-74788.trafficmanager.net"

        },

        "certificateInformation": {

            "expiry": "2026-05-24T08:23:42.0000000Z",

            "type": "Managed"

        },

        "authentication": {

            "addNewSamlVanityFlowRequestHeader": true

        }

    }

]
```

11. カスタム URL SAML エンドポイントを使用するセカンダリアプリケーションを SAML IdP 内から削除します。セカンダリ SAML アプリケーションは、SAML ログオンフロー中に使用されなくなります。

> **重要:**
>
> セカンダリ SAML アプリケーションは、移行が成功したこと、および必要なすべての SAML ログオンシナリオがテストされたことを確認してから削除してください。

現在の 1x SAML アプリケーションカスタム URL ソリューションから新しいよりシンプルなソリューションへの移行方法?

1. Citrix Cloud 管理者は、IdP 管理者と連携して、Citrix Cloud のカスタム URL サービスと SAML IdP の両方で必要な変更を行う必要があります。

2. SAML IdP 内で、カスタム URL SAML アプリケーションの存在と構成を確認します。SAML IdP 内には、SAML アプリケーションが 1 つだけ構成されている必要があります。これは、EntraID、Okta、Duo、PingFederate など、SAML IdP ごとに異なります。

   既存のプライマリ SAML アプリケーションの Citrix Cloud SAML エンドポイントは、この例のようになります。

   プライマリアプリケーションの例

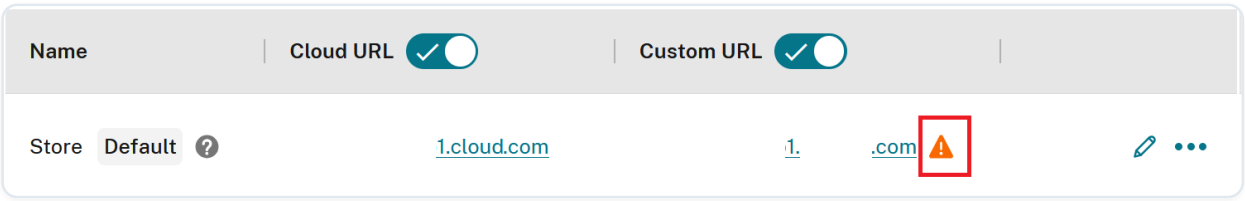
   - エンティティ ID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
   - アサーションコンシューマサービス (SSO): `https://workspaces.mycompany.com/saml/acs`
   - ログアウト (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

3. サポートケースを起票し、Citrixサポートおよびエンジニアリングに連絡して、カスタムドメインの移行支援を依頼してください。CitrixエンジニアリングがSAML構成を確認した後、お客様に代わってカスタムURLを移行します。
4. SAMLアプリケーションに安全に変更を加えるには、ステップ3を完了する必要があります。既存の**プライマリSAMLアプリケーション**のCitrix Cloud SAMLエンドポイントをこの例のように更新してください。

   > **重要:**
   >
   > **プライマリ** SAMLアプリケーションの既存のEntityID SAMLエンドポイントを更新または変更しないでください。これを変更する必要はありません。ACSおよびログアウトSAMLエンドポイントのみを更新する必要があります。
   >
   > **プライマリアプリケーションの例**

   - エンティティID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>` (変更しないでください)
   - アサーションコンシューマーサービス (SSO): `https://saml.cloud.com/saml/acs` (更新)
   - ログアウト (SLO): `https://saml.cloud.com/saml/logout/callback` (更新)

5. **StoreFront Cloud > アクセス**に移動し、**警告アイコン**をクリックして移行UIを開きます。



6. ステップ4でカスタムURLの横に表示されていた警告アイコンは、Citrixサポートおよびエンジニアリングが移行を完了すると消えます。これは、ストアのカスタムURLサービス内のバックエンドデータが正常に更新されたことを示します。
7. すべてのカスタムURL（移行前にセカンダリSAMLアプリケーションを使用していたもの）を使用して、ストアへのSAMLログオンをテストします。

    - `cloud.com` URL（引き続きプライマリSAMLアプリケーションを使用）を使用して、ストアへのSAMLログオンをテストします。
    - すべてのカスタムURL（移行前にセカンダリSAMLアプリケーションを使用していたもの）を使用して、ストアへのSAMLログオンをテストします。

レガシーカスタムURL SAML構成

Citrix Cloud環境に**1xまたは2x SAMLアプリケーション**ソリューションのいずれかを展開しているかどうかを判断するには、現在使用しているSAMLサインインシナリオの組み合わせを特定し、SAML IdP内の現在のSAMLアプリケーションを調べます。

以下のサインインシナリオは、デフォルトで同じSAMLアプリケーション（SAML App 1）を共有します。

- お使いの地域のストアサインインURL（`cloud.com`、`citrixcloud.jp`、`cloud.us`）がSAMLプロバイダーでSPエンティティIDとして構成されているSAML認証。
- 固有のサインインURL（例: `https://citrix.cloud.com/go/mycompany`）を使用したCitrix CloudのSAML認証。このシナリオでは、管理者はActive Directory（AD）グループメンバーシップに基づいて、SAMLを使用してCitrix Cloudに認証されます。

Citrix® StoreFront Cloudで構成するカスタムドメイン（例: `https://workspaces.mycompany.com`）を介してユーザーのSAML認証を追加するには、2番目のSAMLアプリケーション（SAML App 2）が必要です。

> **注：**

> カスタムURLの追加とSAMLの構成には、Citrix Cloudでのプロビジョニングに最大24時間かかります。

> 次の表に、サポートされているSAMLサインインシナリオの組み合わせと必要なSAMLアプリを示します。

ストアURLでストアにサインイン	カスタムドメインURLでストアにサインイン	SAMLサインインURLを使用してCITRIX CLOUDにサインイン	SAML APP 1は必要ですか？	SAML APP 2は必要ですか？
はい	いいえ	いいえ	はい - cloud.com SAMLエンドポイントを使用します	いいえ
いいえ	はい	いいえ	はい - カスタムドメインSAMLエンドポイントを使用します	いいえ
いいえ	いいえ	はい	はい - cloud.com SAMLエンドポイントを使用します	いいえ
はい	いいえ	はい	はい - cloud.com SAMLエンドポイントを使用	いいえ
いいえ	いいえ	はい	はい - cloud.com SAMLエンドポイントを使用	はい - カスタムドメインSAMLエンドポイントを使用
はい	はい	はい	はい - cloud.com	はい - カスタムドメインSAML

ストアURLでストアにサインイン	カスタムドメインURLでストアにサインイン	SAMLサインインURLを使用してCITRIX CLOUDにサインイン	SAML APP 1は必要ですか？	SAML APP 2は必要ですか？
			SAMLエンドポイントを使用	エンドポイントを使用

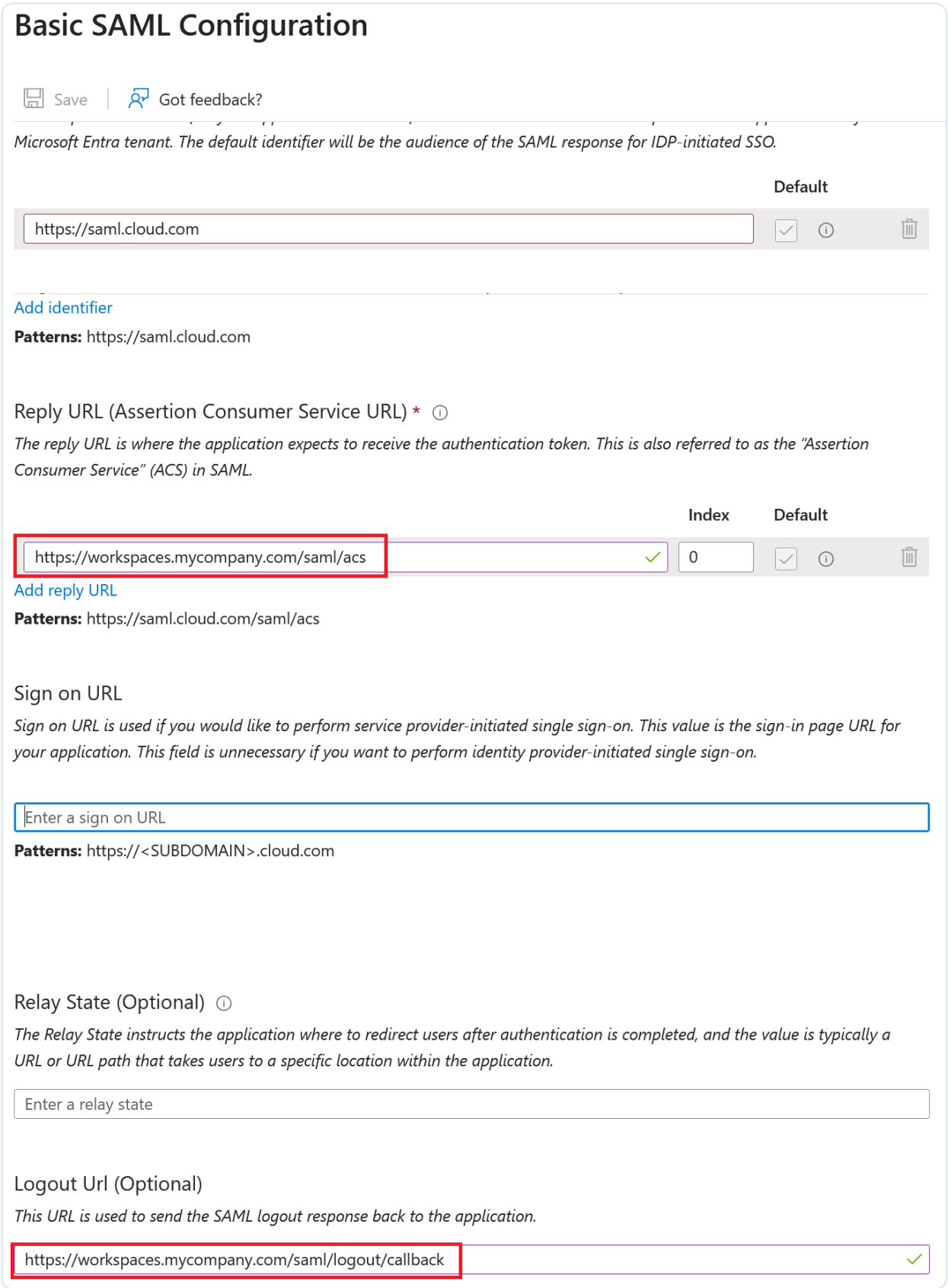
1x SAMLアプリケーション構成 (レガシーSAML構成)

1. Citrix Cloudで、**StoreFront Cloud > Access**内にカスタムURLを構成しました。
2. SAMLプロバイダーの管理コンソールで、ストアのカスタムURLをSPエンドポイントとして使用して、**1つのSAMLアプリケーション**を構成しました。

   レガシーカスタムURL SAMLアプリケーションエンドポイントの例

   - エンティティID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
   - アサーションコンシューマーサービス (SSO): `https://workspaces.mycompany.com/saml/acs`
   - ログアウト (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

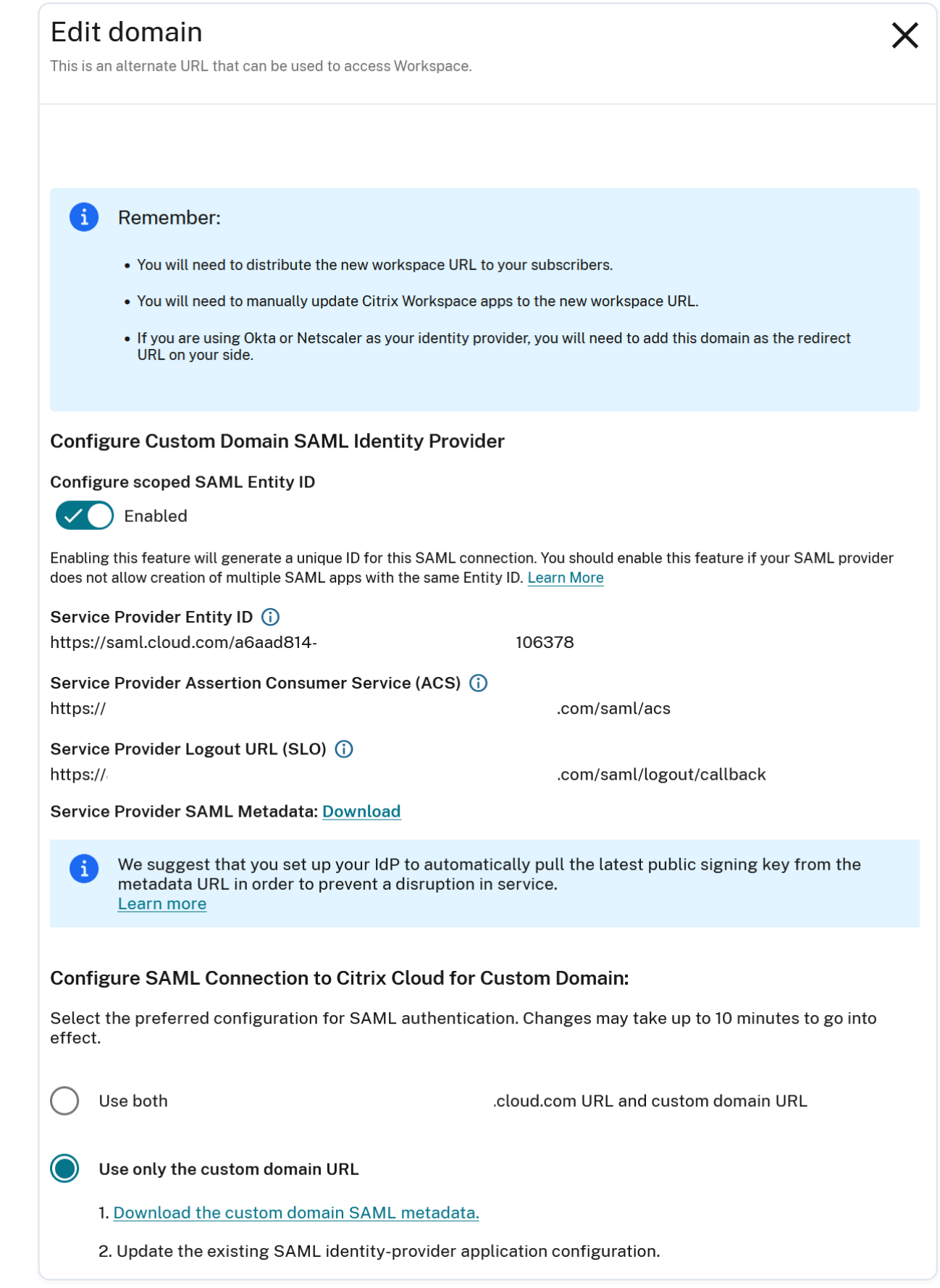
   次の例は、Entra ID のカスタムURL SAMLエンドポイント構成を示しています。



次の例は、Okta のカスタムURL SAMLエンドポイント構成を示しています。ここでは、オーディエンス制限にエンティティID値が含まれています。



3. **StoreFront Cloud > アクセス > 編集**内で、**カスタムドメインのみを使用**を選択しました。



2つのSAMLアプリケーション構成 (レガシーSAML構成)

1. Citrix Cloudで、**StoreFront Cloud > アクセス**内にカスタムドメインを構成しました。

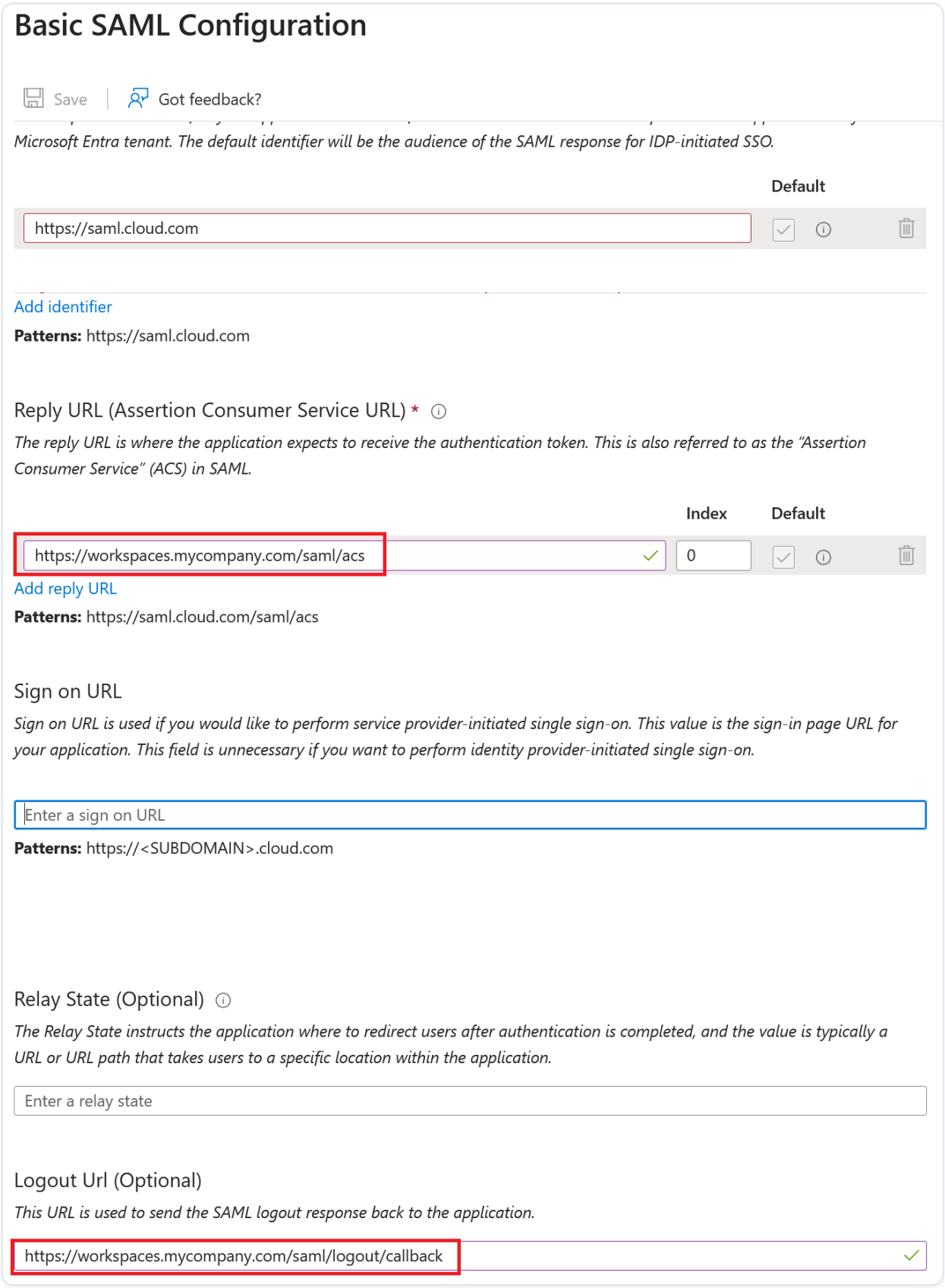
2. SAMLプロバイダーの管理コンソール内で、**2つのSAMLアプリケーション**を構成しました。
3. **プライマリSAMLアプリケーション**内で、次のcloud.com SPエンドポイントを構成しました。

   - エンティティID: `https://saml.cloud.com` または `https://saml.cloud.com/<guid>`
   - アサーションコンシューマーサービス (SSO): `https://saml.cloud.com/saml/acs`
   - ログアウト (SLO): `https://saml.cloud.com/saml/logout/callback`

   次の例は、Okta管理コンソールでのこのエンドポイント構成を示しています。



次の例は、Entra ID管理コンソールでのこのサービスプロバイダーエンドポイント構成を示しています。



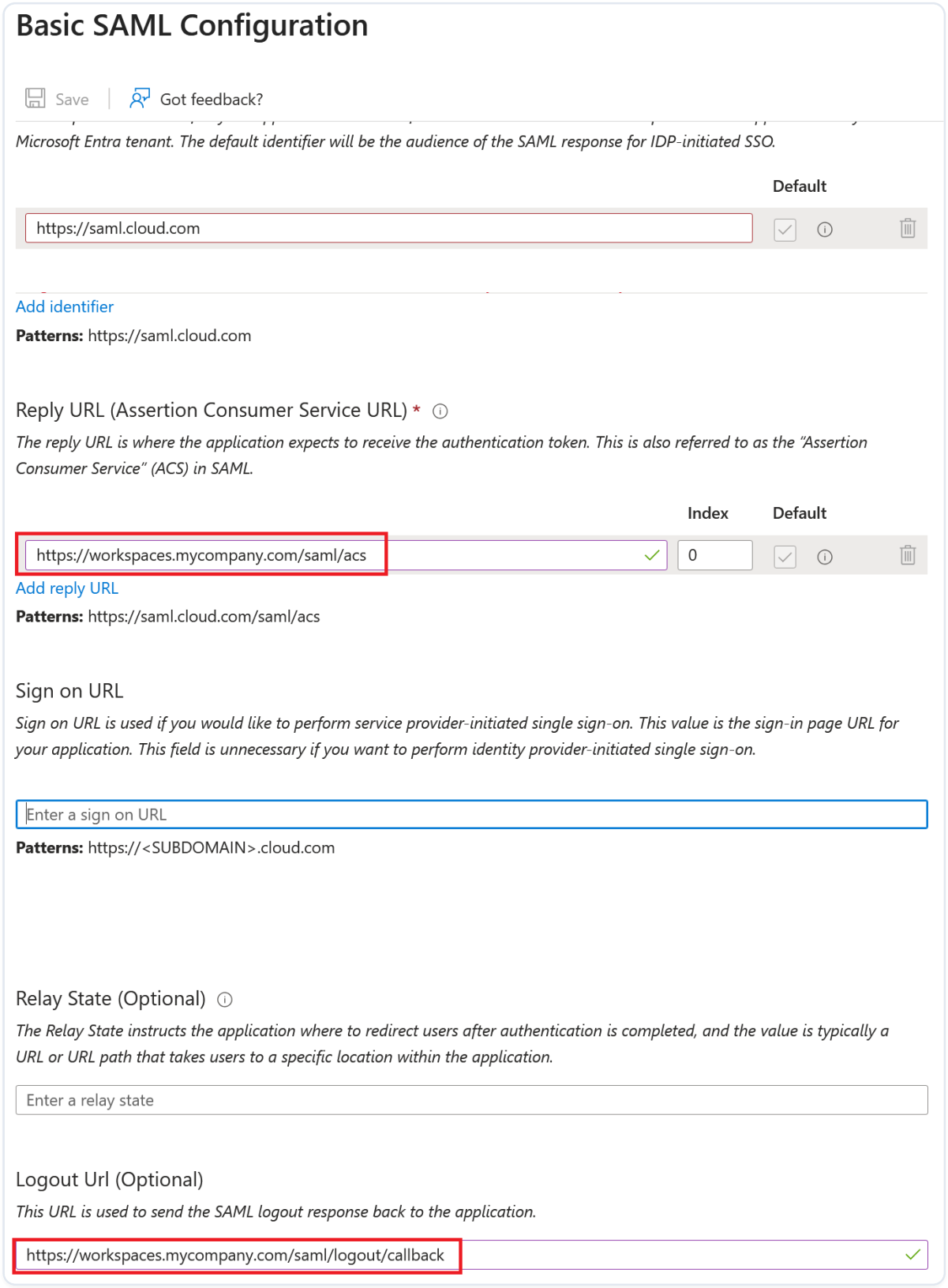
4. **セカンダリSAMLアプリケーション**内で、次のストアカスタムドメインSPエンドポイントを構成しました。

   - エンティティID: `https://saml.cloud.com`

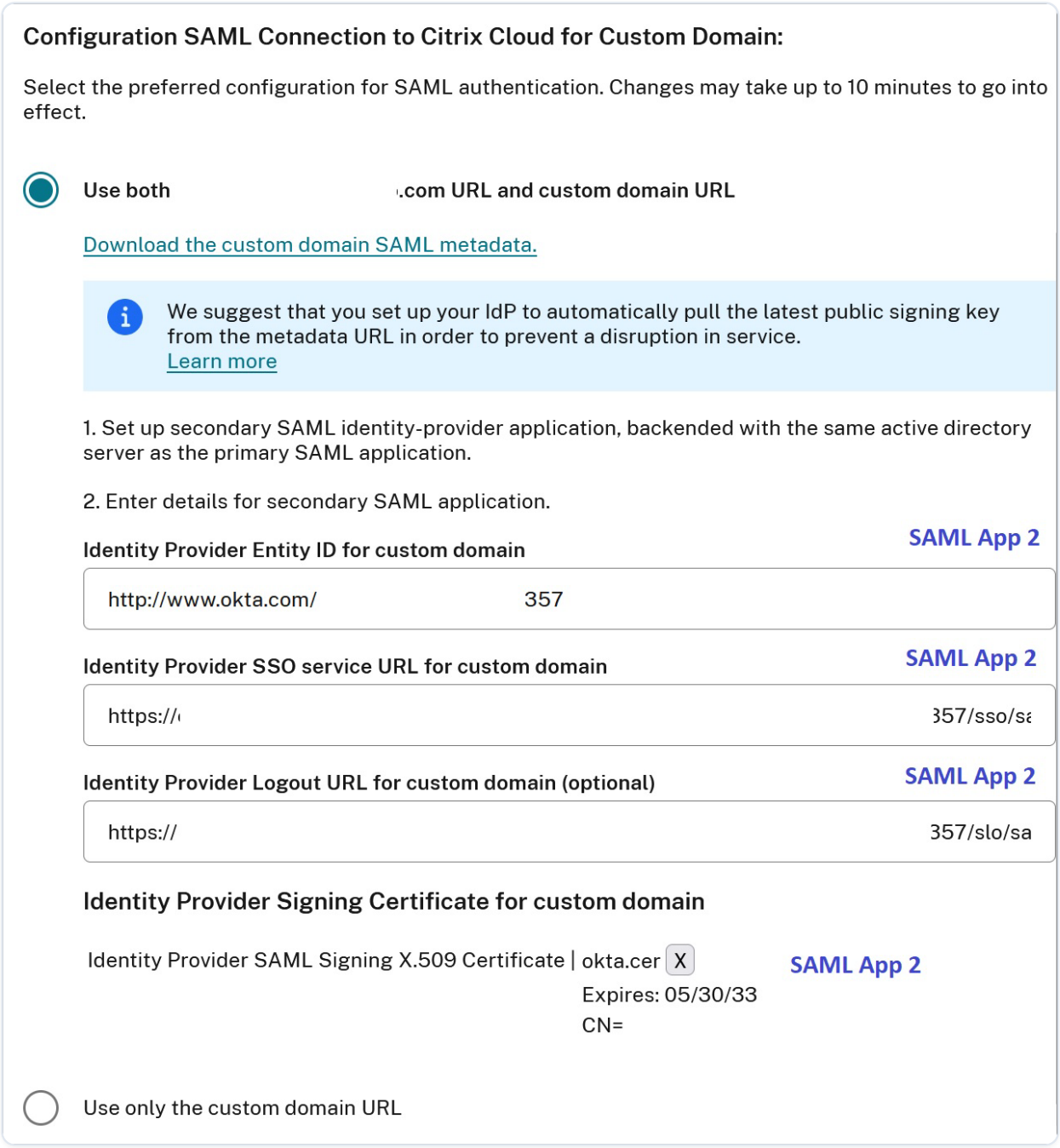
- アサーションコンシューマーサービス (SSO): `https://workspaces.mycompany.com/saml/acs`
- ログアウト (SLO): `https://workspaces.mycompany.com/saml/logout/callback` 次の例は、Oktaコンソールでのこのサービスプロバイダーエンドポイント構成を示しています。



- 次の例は、**Entra ID**コンソールでのこのサービスプロバイダーエンドポイント構成を示しています。

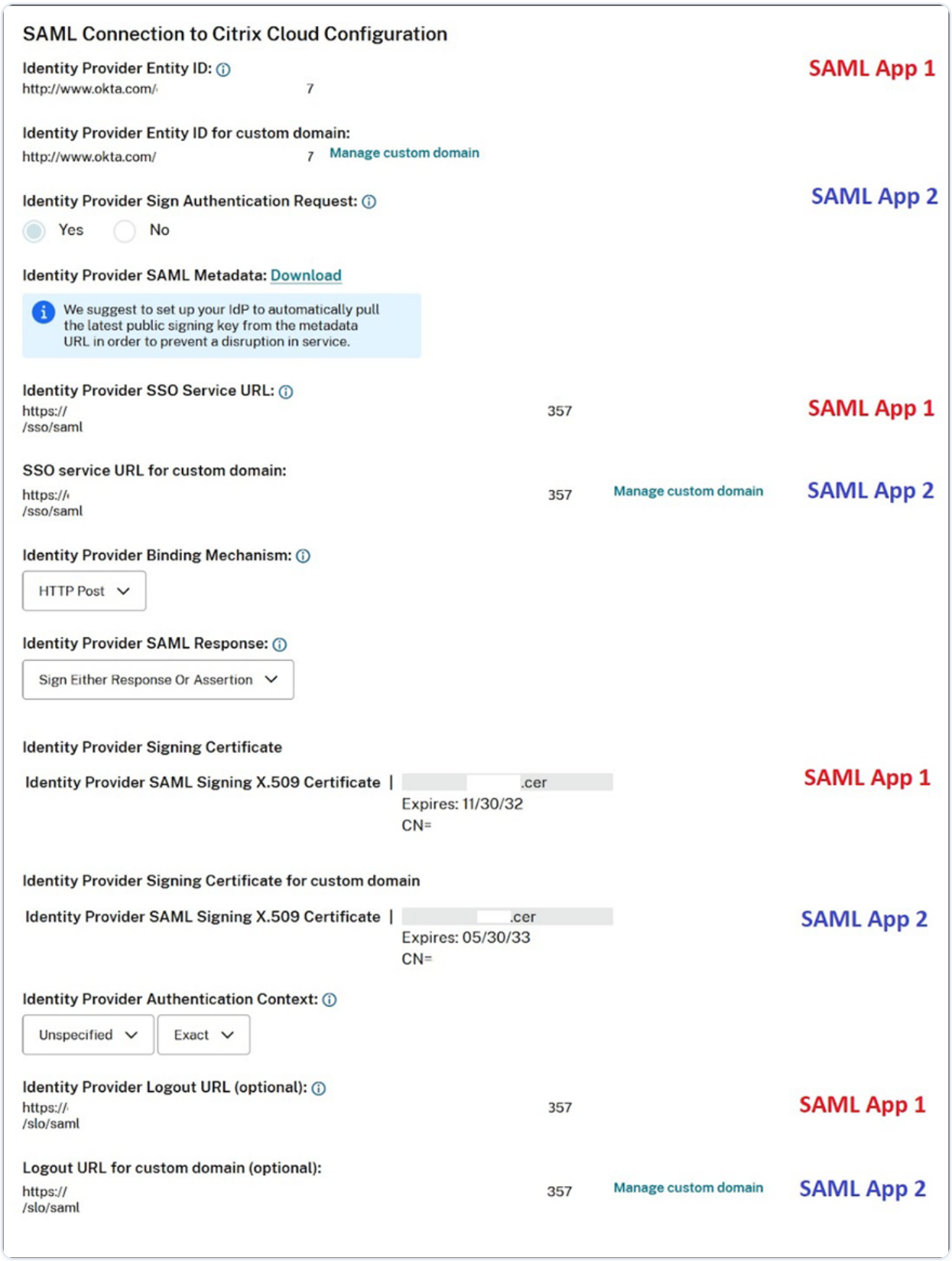


5. **StoreFront Cloud > アクセス > 編集**内で、`customer.cloud.com` **URLとカスタムURLの両方を使用**を選択しました。



6. 省略記号メニューから、 > 内で > を選択します。SAML構成ページには、エンティティID、SSO URL、およびログアウトURL用に構成されたSAMLエンドポイントのペアが表示されま

す。



サービスプロバイダーSAML署名証明書の更新

署名付きリクエストとレスポンスを使用するSAML接続は、2つの異なるSAML署名証明書に依存します。SAML接続の各サイドに1つずつです。

サービスプロバイダー署名証明書

この証明書は、Citrix Cloud™ SAMLメタデータを通じてCitrixによって提供され、SP署名証明書ローテーションの広告フェーズ中に更新されます。これは少なくとも暦年ごとに1回発生します。

SAML署名証明書は、Citrix Cloud管理者が展開の準備をする時間を確保するために、有効期限が切れる前にローテーションする必要があります。証明書のローテーションは、整合性を確保し、ダウンタイムを防ぐために、サービスプロバイダーとIDプロバイダーの両方で必要です。

選択したSAMLプロバイダーがSP SAML署名証明書の自動ローテーションをサポートしていない場合、期限切れの証明書を置き換えるために、SAMLプロバイダー内でSAML署名証明書の手動ローテーションを実行する必要があります。

> **重要:**
>
> このSAML eDocセクション内の既存のすべてのガイドには、SAML接続の両側で署名を設定する方法の詳細が含まれています。Citrix®は、署名付きSAML構成のみを推奨しています。これらはより安全であり、ログアウト（SLO）を成功させるために一部のSAMLプロバイダーで必要とされるためです。

FAQ

SAML署名とは何ですか?

SAMLプロトコルは、認証を要求し、IDのアサーションを送信するためにメッセージを使用します。これらのメッセージのセキュリティは、トランスポートとメッセージレベルのセキュリティの両方に依存します。メッセージは、XML署名構文に従って署名されたXMLドキュメントです。これにより、メッセージの整合性保証と、秘密鍵を保持していることを証明することによる送信者の認証の両方が提供されます。信頼モデルは、SAMLセキュリティとプライバシーに関する考慮事項によって記述されています。信頼される秘密鍵を定義するために使用される公開鍵は、任意の適切な形式で配布できます。Citrixは、鍵を配布および消費するための適切なコンテナとしてX.509証明書を使用します。

SAML署名済みリクエストの強制とは何ですか?

Citrix CloudがSAML接続内で署名済みリクエストを送信するように構成されているからといって、SAMLプロバイダーが署名の使用を強制し、署名されていない受信SAMLリクエストを拒否することを保証するものではありません。ほとんどのSAML IdPには、署名済みリクエストを強制するオプションがあります。SAMLプロバイダーへのログインのために署名されていないリクエストが受信された場合、SAMLログインは失敗します。Duoのような一部のSAML IdPは、このオプション

さえ提供していません。SAML IdPの構成ステータスを確認するのは、SAML IdP管理者の責任です。Citrixサポートは、SAMLアプリケーション内で署名済みリクエストが強制されているかどうかを制御したり、可視性を持ったりすることはありません。

CitrixはサービスプロバイダーSAML署名証明書をどのくらいの頻度でローテーションしますか?

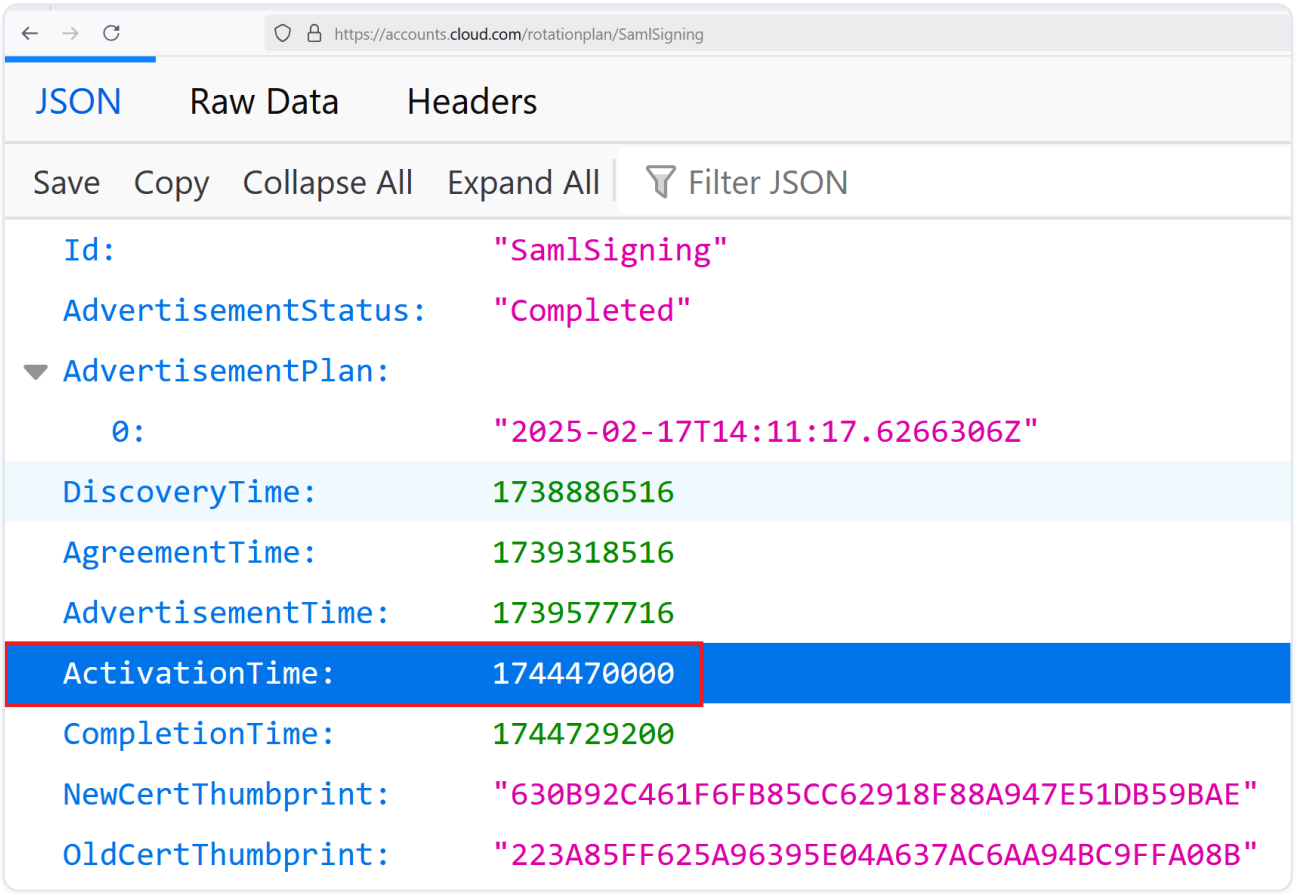
アクティブなサービスプロバイダー署名証明書と新しく発行された証明書との間に十分な重複期間を設けるため、Citrixは約11か月ごとにサービスプロバイダー署名証明書をローテーションします。これは、新しい証明書がアクティブ化される30日前に、Citrix Cloudのお客様が有効な証明書を利用できるようにするためです。

サービスプロバイダーSAML署名証明書の広告フェーズとは何ですか?

広告フェーズ中、現在および交換用のSAML署名証明書はCitrix Cloudのメタデータに存在します。ローテーション日時までは、アクティブな証明書のみがSAMLリクエストの検証に使用できます。これは、Citrix CloudのメールおよびCitrix Cloudコンソールの通知で指定された日時です。

> **重要:**
>
> 署名証明書の有効期限は、アクティベーション日とは異なります。CitrixおよびIdPの管理者が注意を払う必要があるのは、証明書の有効期限ではなく、アクティベーション日です。Citrix Cloudの署名証明書は、常に有効期限が切れる前にローテーションされます。
>
> このリンク ローテーション計画 を使用して、広告およびアクティベーション日時を確認できます。

サービスプロバイダー署名証明書のローテーションプロセスにおける各イベントの日時は、Unixエポックタイムスタンプとして提供されます。



Unixエポックタイムスタンプを人間が読める日時形式に変換するには、エポックコンバーター を使用します。

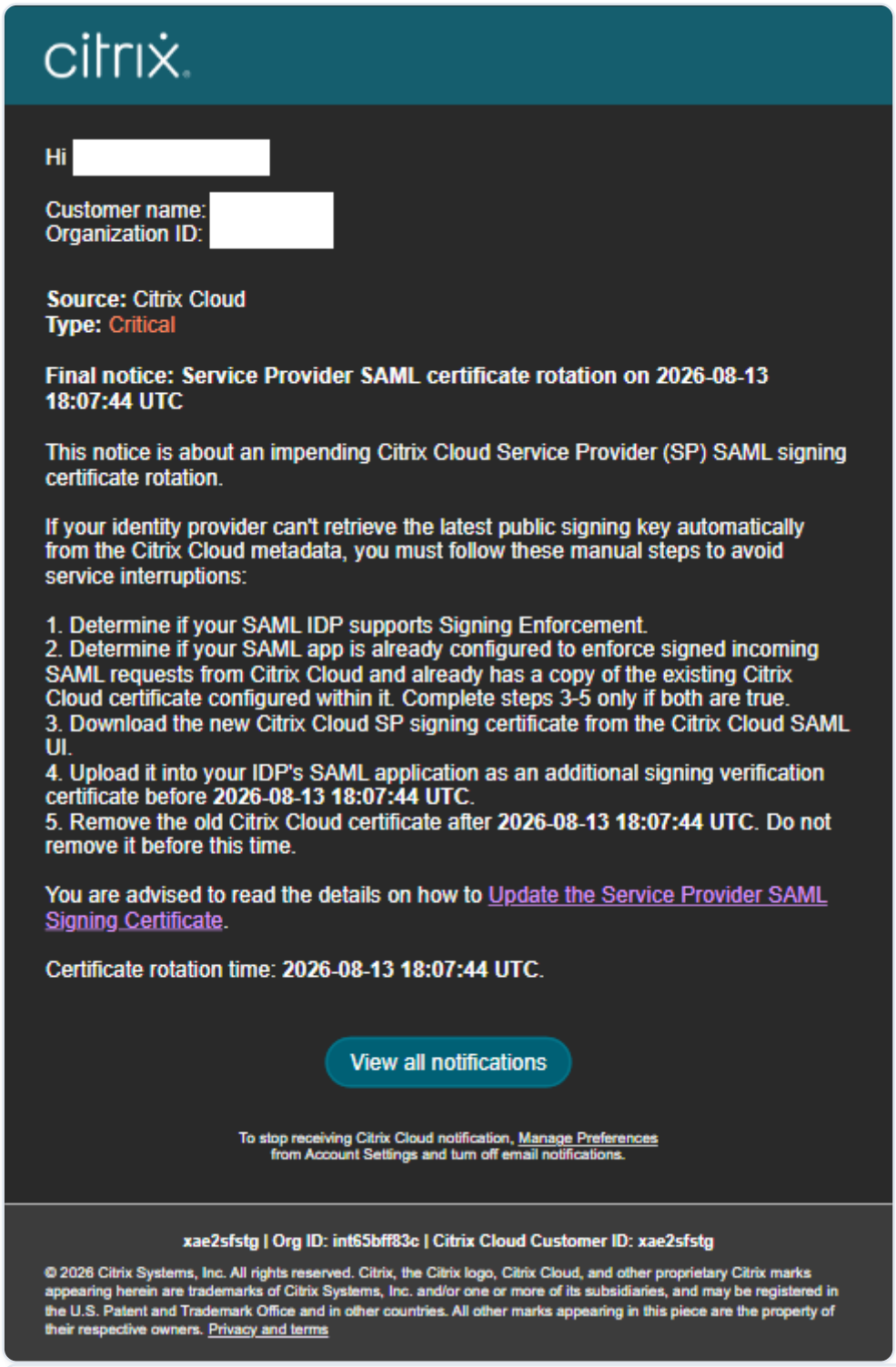


Citrixが、Digicertのような公開認証局によって署名された証明書ではなく、自己署名されたCitrix Cloud SAML署名証明書を使用することにしたのはなぜですか?

SAMLアプリケーションにアップロードする必要があるSAML署名証明書の最新バージョンにおける**発行者**は、Digicertのような公開認証局ではなく、「samlsigning.cloud.com, Citrix Systems Inc.」になりました。自己署名SP署名証明書の使用は、外部発行証明書に関連する既知のSAML脆弱性（「Silver SAML」と呼ばれる）を軽減するためです。

現在のCitrix Cloud SAML署名証明書が間もなく期限切れになり、交換する必要があることを示す通知を、メールおよびCitrix Cloudコンソール内で受け取ったのはなぜですか?

SAMLプロバイダー（IdP）は、ストアやCitrix Cloudコンソールなどのサービスプロバイダーからの受信SAMLリクエストの署名を検証するために、有効で期限内の証明書を必要とします。ストアまたはCitrix Cloudコンソールへのログオンに SAMLを使用しているCitrix Cloudのお客様には、SAML署名証明書のローテーションが間近であることを通知するために連絡が行われます。



citrix.

Hi

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

Final notice: Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

Certificate rotation time: **2026-08-13 18:07:44 UTC**.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

xae2sfstg | Org ID: int65bff83c | Citrix Cloud Customer ID: xae2sfstg

© 2026 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms

Citrix Cloud
Sep 22, 2026 7:08:11 PM

Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

Certificate rotation time: **2026-08-13 18:07:44 UTC**.

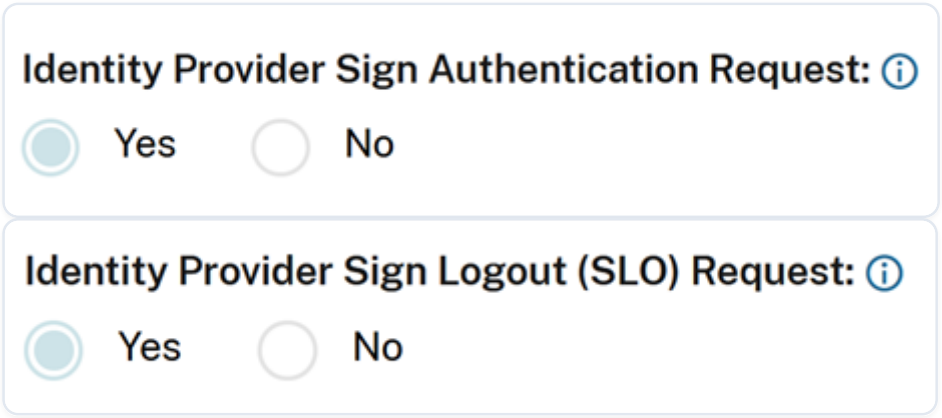
Citrix Cloud SAML署名証明書のローテーションによって、私のCitrix Cloudのお客様が影響を受けるかどうかをどのように知ることができますか?

これは、以下のSAML構成を持つCitrix Cloudのお客様に影響します。

- Citrix Cloud内のSAML接続が**認証要求の署名 = はい**で構成されている場合
- Microsoft Entra ID、ADFS、OktaなどのSAMLプロバイダーを、署名されていないSAML要求を拒否するように構成している場合（署名強制）。
- Citrix Cloud SAML接続内およびSAMLプロバイダー内でシングルログアウト（SLO）を構成している場合。SLO要求は、セキュリティのベストプラクティスの一環として署名される必要があります。

Citrix Cloud SAML接続の署名構成を確認するにはどうすればよいですか?

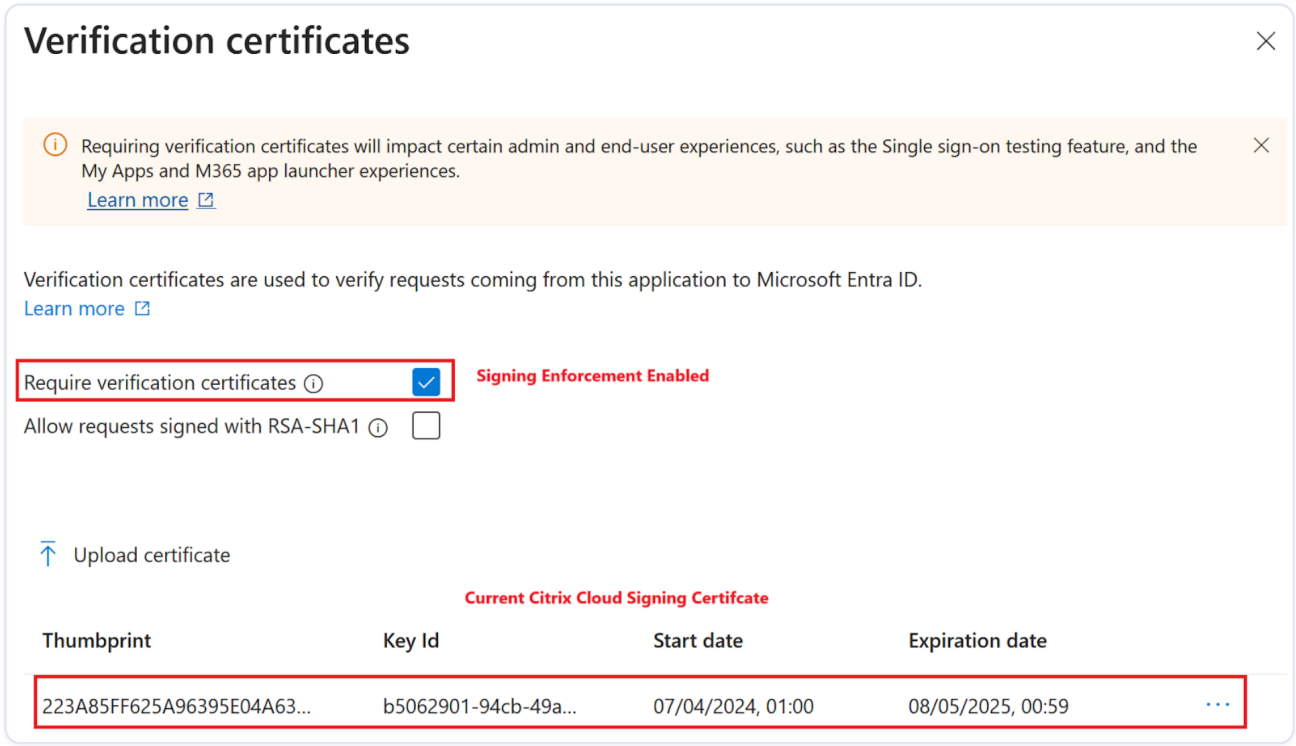
Citrix Cloud SAML接続内で**認証要求の署名**が有効になっているかを確認するには、**IDとアクセス管理** > **SAML 2.0** > **編集**に移動します。Citrix Cloud内のすべての新しいSAML接続は、ログオン（SSO）とログアウト（SLO）の両方で、デフォルトで**IDプロバイダーの認証/ログアウト要求の署名 = はい**になります。



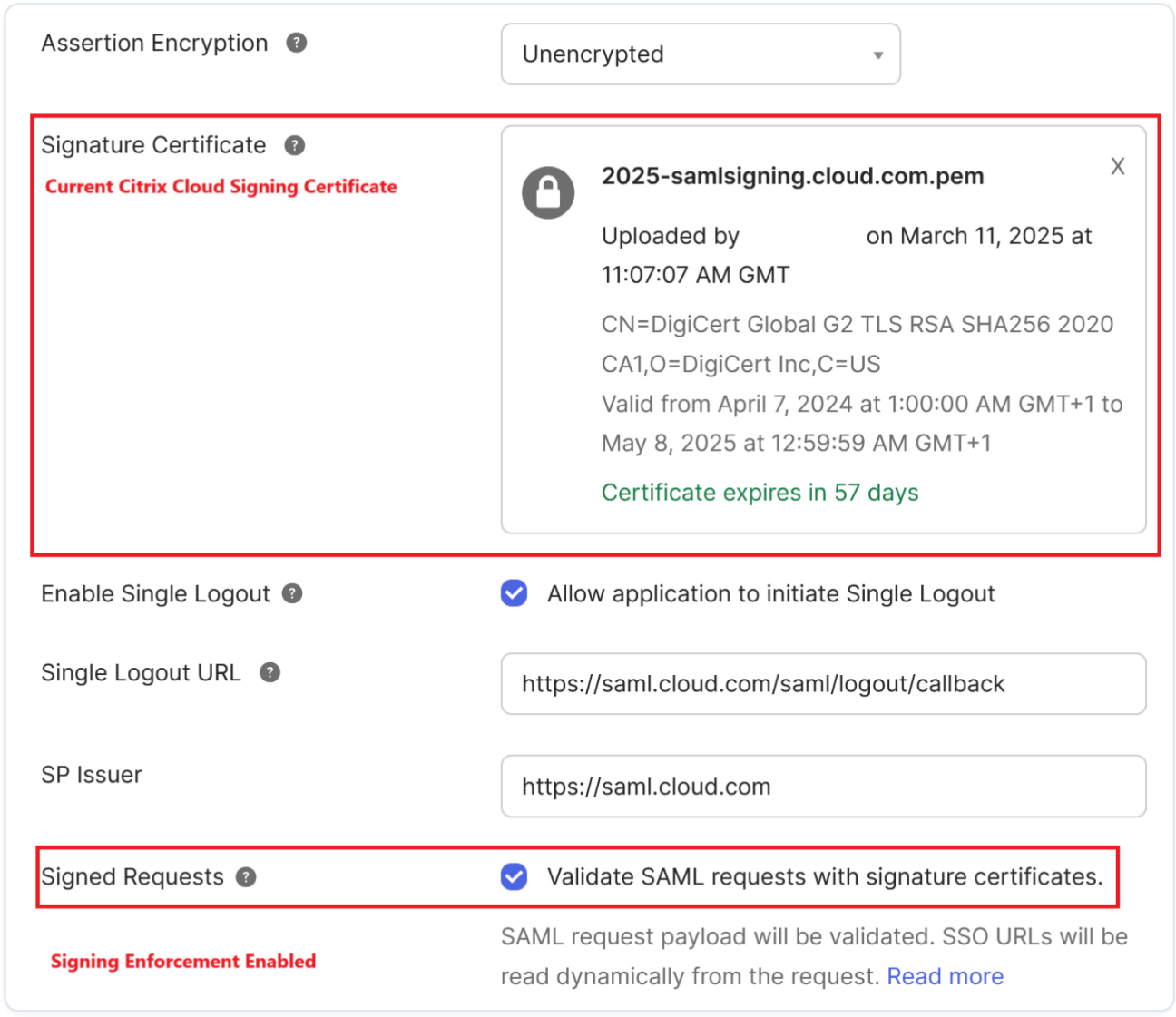
SAMLアプリ内で署名強制が構成されているかどうかを確認するにはどうすればよいですか?

これは使用しているSAMLプロバイダーによって異なります。Citrixが文書化したすべてのSAMLソリューションには、セキュリティのベストプラクティスの一環として署名強制を有効にする手順が含まれています。

EntraID署名強制の例:


Verification certificates
Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, and the My Apps and M365 app launcher experiences.
Learn more
Verification certificates are used to verify requests coming from this application to Microsoft Entra ID.
Learn more
Require verification certificates
Signing Enforcement Enabled
Allow requests signed with RSA-SHA1
Upload certificate
Current Citrix Cloud Signing Certifcate
Thumbprint
Key Id
Start date
Expiration date
223A85FF625A96395E04A63...
b5062901-94cb-49a...
07/04/2024, 01:00
08/05/2025, 00:59

Okta署名強制の例:


Assertion Encryption
Unencrypted
Signature Certificate
Current Citrix Cloud Signing Certificate
2025-samlsigning.cloud.com.pem
Uploaded by on March 11, 2025 at 11:07:07 AM GMT
CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,O=DigiCert Inc,C=US
Valid from April 7, 2024 at 1:00:00 AM GMT+1 to May 8, 2025 at 12:59:59 AM GMT+1
Certificate expires in 57 days
Enable Single Logout
Allow application to initiate Single Logout
Single Logout URL
https://saml.cloud.com/saml/logout/callback
SP Issuer
https://saml.cloud.com
Signed Requests
Validate SAML requests with signature certificates.
Signing Enforcement Enabled
SAML request payload will be validated. SSO URLs will be read dynamically from the request. Read more

最新のサービスプロバイダー (SP) 署名証明書のコピーはどこで入手できますか?

この証明書は、Citrix Cloud SAMLメタデータを通じてCitrixから提供され、SP署名証明書のローテーションの広告フェーズ中に定期的に更新されます。これは少なくとも暦年ごとに1回発生します。

米国、EU、およびAPS: `<https://saml.cloud.com/saml/metadata>`

日本: `<https://saml.citrixcloud.jp/saml/>`

政府: `<https://saml.cloud.us/saml/metadata>`

SAMLアプリが複数の検証証明書をサポートしている場合、古いCitrix Cloud SAML署名証明書を削除しても安全なのはいつですか?

古いCitrix Cloud署名証明書をSAMLアプリケーションから削除するのは、メールおよびCitrix Cloudコンソール通知に記載されている証明書の有効化日時以降にしてください。Oktaなどの一部のSAML IdPでは、一度に1つの署名証明書しかアップロードできません。この状況では、有効化日時以降に現在の証明書を新しい証明書で上書きするしかありません。これは有効化日時より前に行ってはなりません。

メタデータ交換を使用して、SAMLプロバイダーを最新のCitrix Cloud SP SAML署名証明書で自動的に更新する

SAMLメタデータ交換を使用すると、SAMLプロバイダーは、`<https://saml.cloud.com/saml/metadata>`のようなメタデータURLを監視することで、Citrix Cloud SAMLメタデータを自動的に消費します。SAMLプロバイダーがSAMLメタデータ交換をサポートしている場合、SP署名証明書はすでに自動的に更新されている可能性があります。 SAMLプロバイダーがメタデータ交換をサポートしていることを確認してください。その後、現在のSAML署名証明書の有効期限が切れる前に更新が行われたかどうかを確認できます。



> **重要**

各サードパーティSAMLプロバイダーがサポートするSAML機能には大きなばらつきがあります。使用しているSAMLプロバイダーの機能と要件を把握し理解することは、Citrix Cloud管理者の責任です。これは、Citrix Cloud SAML接続構成 (SP) とSAMLプロバイダー (IdP) 構成の両方が一致していることを確認するために必要です。署名検証をサポートしているか、およびSAMLリクエストとレスポンスに署名が必要かどうかを判断するには、SAMLプロバイダーのドキュメントを参照してください。

SAMLプロバイダーを最新のCitrix Cloud SP SAML署名証明書で手動で更新する

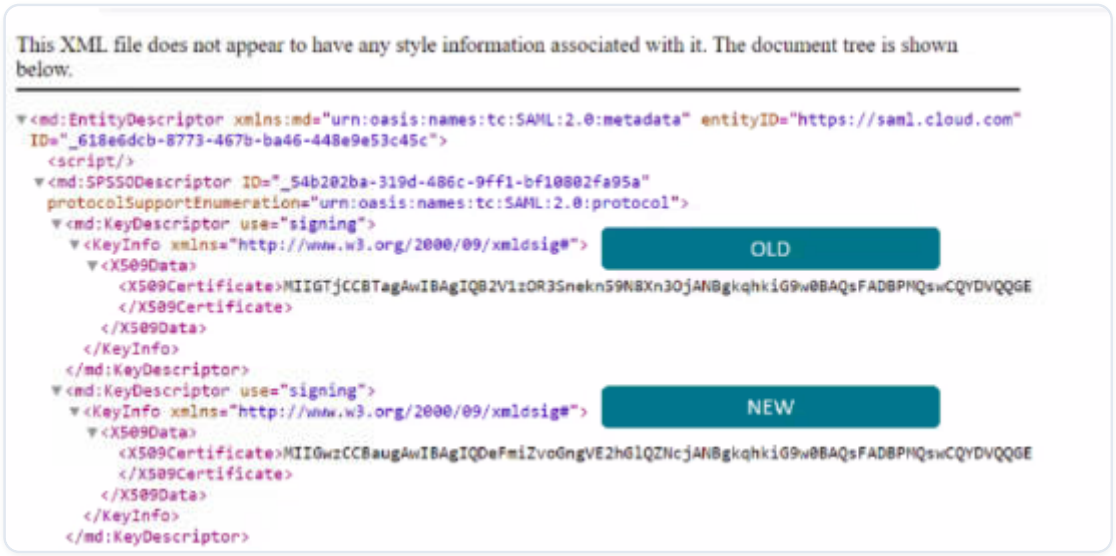
重要

Citrix Cloudから新しい証明書が発行されるたびにSP証明書のローテーションを行う必要があります。そうしないと、SAMLログオンに影響が出て、ダウンタイムが発生します。

Citrix Cloudメタデータから将来のサービスプロバイダー証明書のコピーを取得する

1. Citrix Cloudから最新のSAMLメタデータを取得するには、**Identity and Access Management**内で現在のSAML接続を表示し、**Authentication**をクリックし、**SAML Connection**を選択して**View**をクリックします。 以下の画像は、米国、EU、APSなどのCitrix Cloudリージョンにおけるこのファイルの例です。

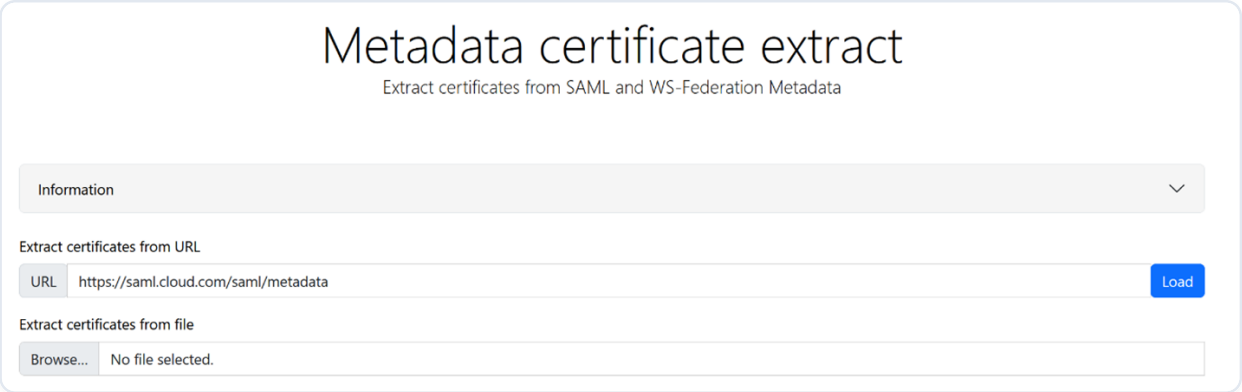
   `<https://saml.cloud.com/saml/metadata>`

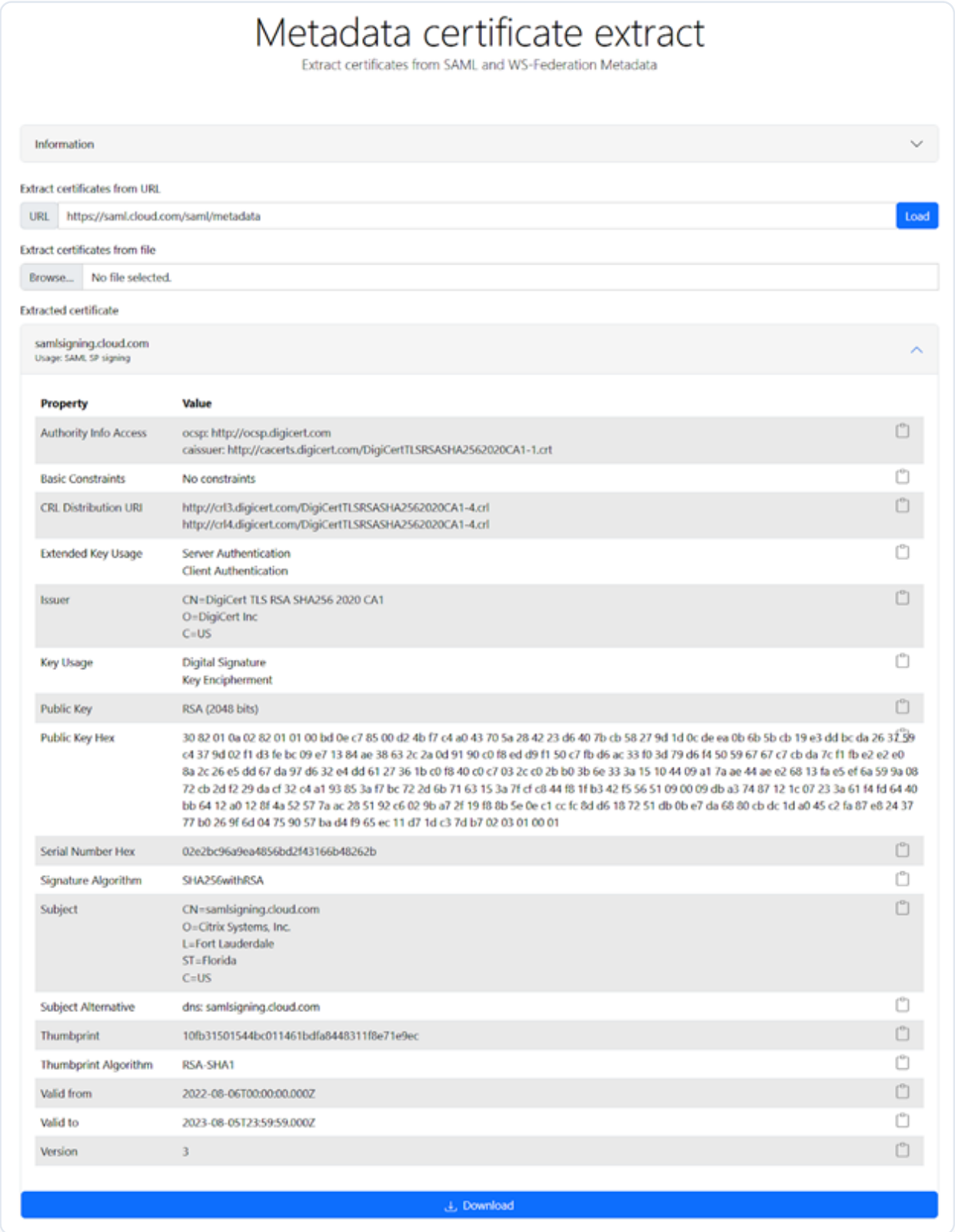
   このメタデータXMLファイルの例では、2つのx.509 Citrix Cloud SAML署名証明書があります。

2. XMLファイルをサードパーティツールにアップロードするか、メタデータURLを提供することで、メタデータからx.509証明書を抽出できます。

3. `<https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract>`に移動します
4. Citrix Cloudの顧客リージョンに対応するSAMLメタデータURLを入力します。
   - 米国、EU、APS: `<https://saml.cloud.com/saml/metadata>`
   - JP: `<https://saml.citrixcloud.jp/saml/metadata>`
   - GOV: `<https://saml.cloud.us/saml/metadata>`



`<https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract>`からSAML署名証明書をダウンロードします。



5. 新しく抽出したCitrix Cloud SP SAML証明書をSAMLプロバイダーにアップロードします。このプロセスはSAMLプロバイダーごとに異なります。特定のSAMLプロバイダーのドキュメントを使用して、適切なSP署名証明書のローテーション手順を確認してください。

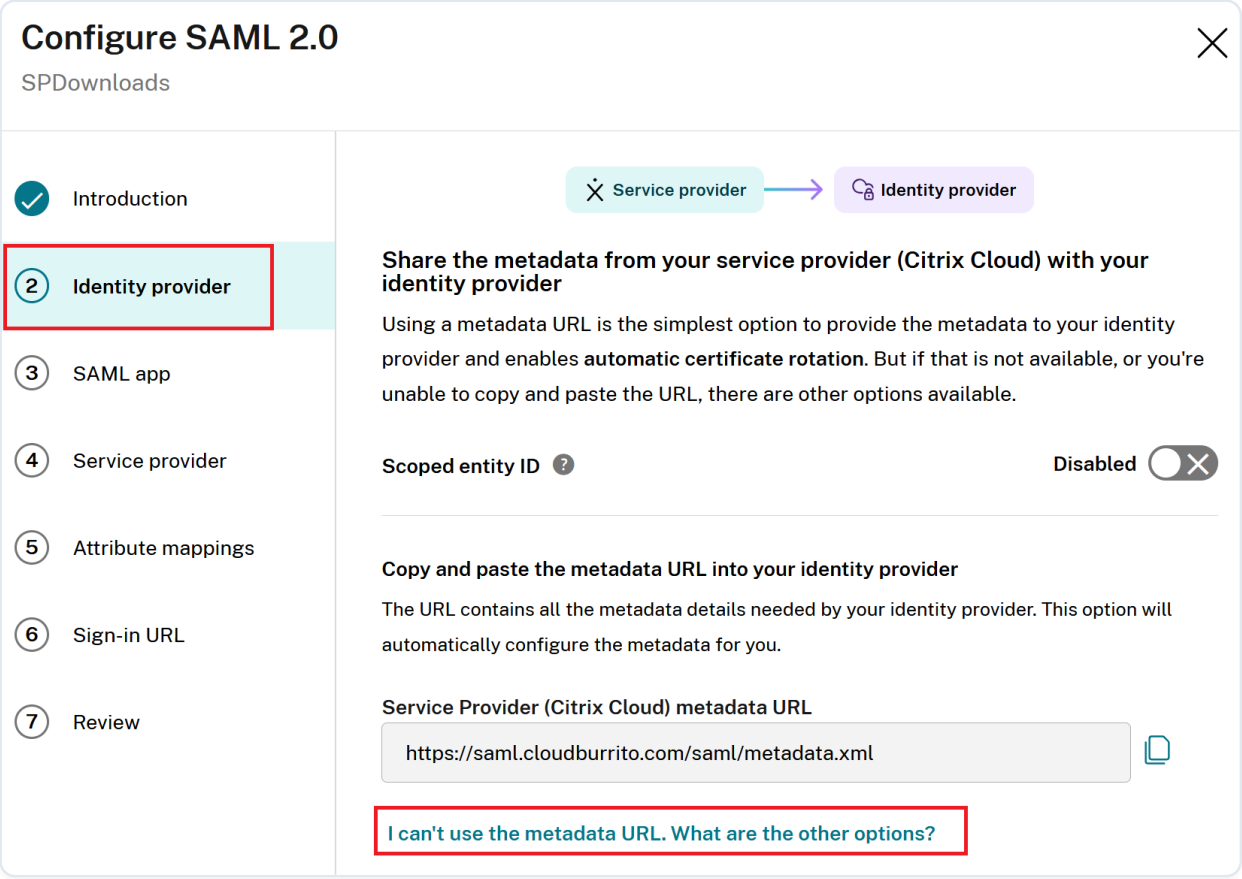
   SAMLプロバイダーによっては、既存のSAML署名証明書を新しいものに置き換える必要がある場合があります。SAMLプロバイダーが複数のSP署名証明書を同時にサポートしている場

合、新しいものをアップロードするだけで十分な場合があります。古い証明書は期限切れになったら削除することをお勧めします。

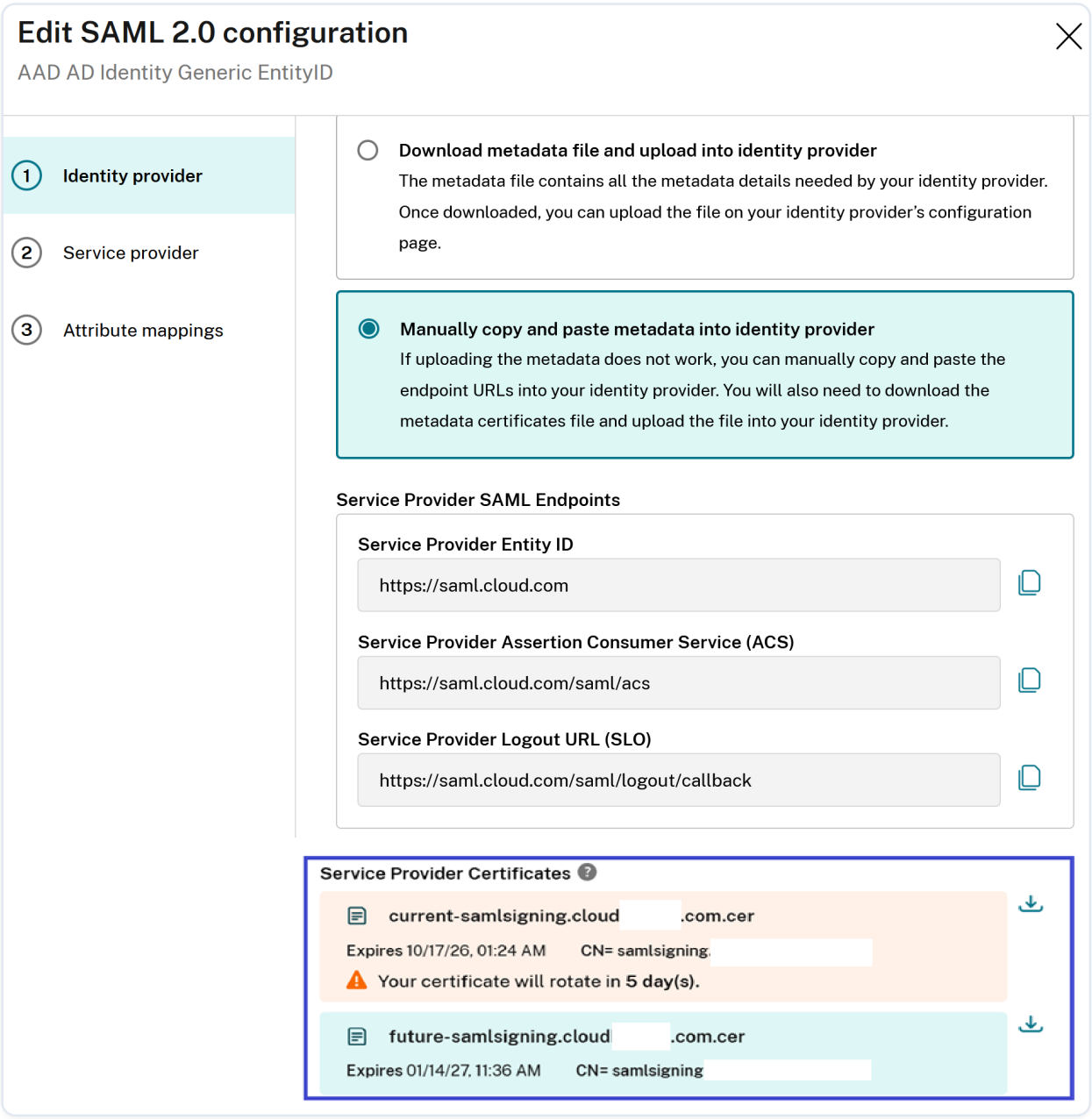
または、,

Citrix Cloud UI内から将来のサービスプロバイダー証明書のコピーを取得する

1. 新しく手動で作成された接続のSAML 2.0設定ウィザード内で。
2. ウィザードフロー内の**IDプロバイダー**ページに移動します。
3. **メタデータURLを使用できません。他のオプションは何ですか？**を選択します。



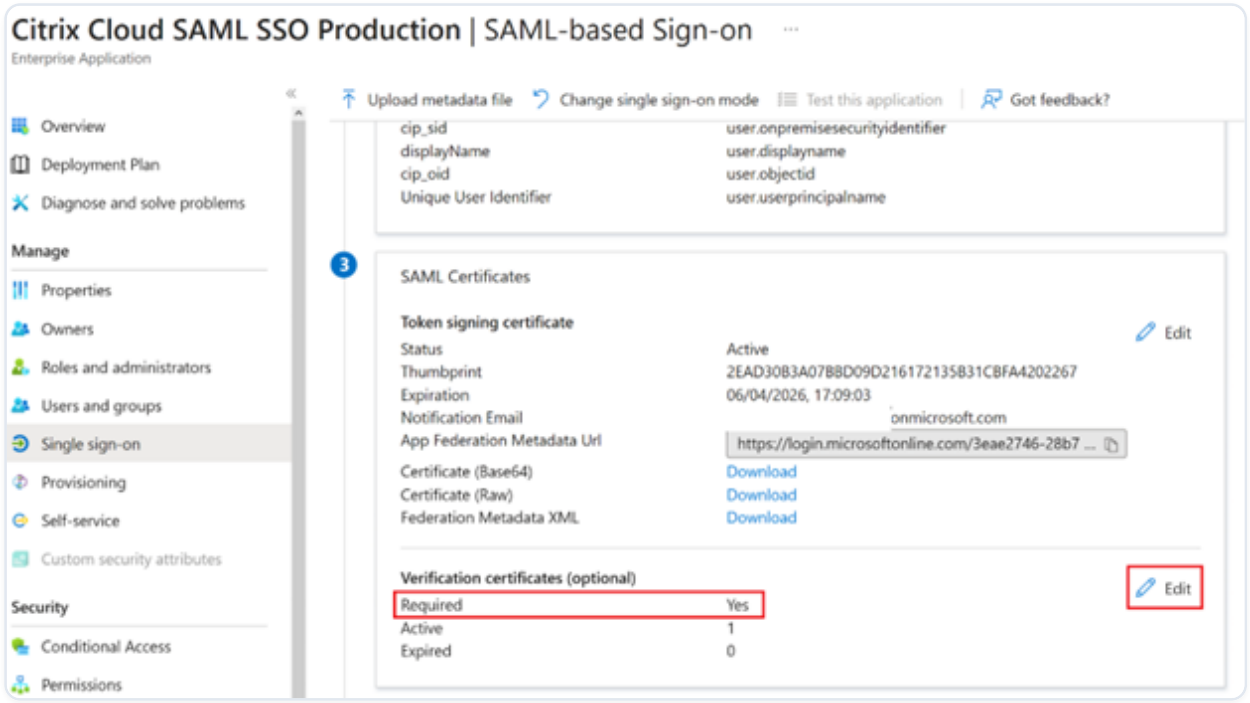
4. **メタデータフィールドを手動で入力**を選択し、**サービスプロバイダー証明書**セクションに移動します。
5. Citrix Cloud署名証明書の将来のバージョンをダウンロードします。



代替のCitrix Cloud SAML署名証明書をMicrosoft Entra ID SAMLアプリケーションにアップロードする

Microsoft Entra ID SAMLアプリを構成する前に、詳細についてはSAMLリクエスト署名検証を参照してください。

1. **Microsoft Entra ID**に移動し、**エンタープライズアプリケーション**を選択して「Your SAML App」をクリックします。
2. SAMLアプリケーション内のSAML証明書セクションを見つけます。



3. 「**証明書のアップロード**」を選択し、SAMLメタデータから取得したCitrix Cloud SAML署名証明書をアップロードします。

   検証証明書(/en-us/citrix-cloud/media/verification_cert.png)

> **注：**
>
> Microsoft Entra ID SAMLアプリは複数の署名検証証明書を設定できるため、現在の証明書の有効期限が切れるかなり前に代替証明書をアップロードすることが可能です。次のスクリーンショットは、2つの有効な証明書を示しています。そのうちの1つは近いうちに有効期限が切れる予定です。アップロードされた証明書のうち少なくとも1つが有効で、まだ有効期限が切れていない限り、ストアまたはCitrix CloudへのSAMLログインは引き続き成功し、サービス停止は発生しません。

検証証明書(/en-us/citrix-cloud/media/verif-cert.png)

> **重要：**
>
> メールおよびCitrix Cloudコンソール通知に記載されているSAMLローテーションの日時が過ぎるまで、既存の検証証明書を削除しないでください。新しいCitrix Cloud証明書は、これら2つの通知に記載されている日時になって初めてアクティブになります。

Okta SAMLアプリケーションにCitrix Cloud SAML署名証明書をアップロードする

Oktaは、複数のSP SAML署名証明書を同時にサポートしていません。現在使用している既存のCitrix Cloud SP署名証明書を新しいものに上書きするしかありません。これは、スケジュールされたメンテナンス期間中に実行することをお勧めします。

1. **アプリケーション**に移動し、**アプリケーション**を選択して、Okta SAMLアプリを検索します。

   Okta SAMLアプリケーションを検索(/en-us/citrix-cloud/media/okta-saml-app.png)

2. **一般**から**SAML設定**に移動し、**編集**をクリックし、**SAMLの構成**を選択し、**詳細設定を表示**を選択し、**署名証明書**をクリックして代替をアップロードします。Oktaは、アップロードUIに現在のCitrix Cloud SAML署名証明書を表示しません。アップロード後にのみ代替証明書が表示されます。

   署名証明書(/en-us/citrix-cloud/media/okta-signature-cert.png)

3. **署名証明書**を選択し、**ファイルの参照**をクリックして、Citrix Cloud SAMLメタデータから取得したCitrix Cloud SAML署名証明書をアップロードします。

   署名証明書(/en-us/citrix-cloud/media/signature-cert.png)

> **重要**
>
> メールおよびCitrix Cloudコンソール通知に記載されているSAMLローテーションの日時までは、既存の検証証明書を上書きしないでください。新しいCitrix Cloud証明書は、これら2つの通知に記載されている日時にのみアクティブになります。

IDプロバイダーSAML署名証明書の更新

署名付きリクエストとレスポンスを使用するSAML接続は、2つの異なるSAML署名証明書に依存します。SAML接続の両側に1つずつです。**IdP証明書のローテーション**プロセスは、すべてのCitrix Cloudのお客様が使用する`samlsigning.cloud.com`証明書の**サービスプロバイダー**による年次ローテーションと混同しないでください。Citrixは、SAMLアプリケーションのIDP証明書のローテーションを制御しません。それはCitrix CloudおよびIdP管理者が行います。

よくある質問

SAMLアプリケーションの署名証明書は何に使用されますか?

SAMLアプリケーションの署名証明書は、SAML接続を最初に作成するときにCitrix Cloudにアップロードされます。最初のSAML接続作成プロセスでは、1つのIdP署名証明書のみを提供する必要が

あります。IdP証明書は、Microsoft Entra ID、Okta、PingFederate、ADFSなどのSAMLプロバイダー内から取得されます。Citrix Cloudは、SAML認証プロセス中にSAMLアプリケーションからCitrix Cloudに送信されるSAML応答の署名を検証するために、IdP署名証明書を使用します。IdP証明書は、有効期限が切れるまでCitrix Cloudによって信頼されます。

SAMLアプリケーション署名証明書のローテーションとは何ですか?

IdP署名証明書のローテーションは、SAMLアプリケーションの署名証明書の有効期限が近づいている場合に必要となる計画的なメンテナンス作業です。管理者は、Citrix Cloud内のSAML接続で使用されるIdP署名証明書に注意を払う必要があります。証明書の有効期限が30日以内に切れる場合は、有効な代替証明書をCitrix Cloud SAML接続にアップロードしてください。現在の証明書が期限切れになる前に、この交換を行ってください。

SAMLアプリケーションの署名証明書はどのくらいの頻度でローテーションする必要がありますか?

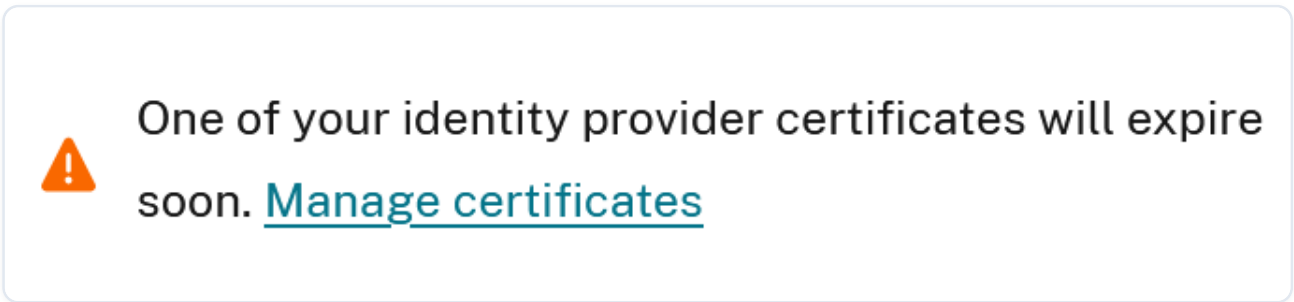
クラウドSAMLアプリケーション証明書は、通常、Duoでは16年、Oktaでは10年、Entra ID SAMLアプリケーションでは3年といった非常に長い有効期間を持ちます。PingFederateやADFSなどのオンプレミスSAML IdP内で使用される証明書は、環境内の他のx509証明書と同様に作成および維持されるため、通常、Digicertなどの商用認証局によって毎年交換されます。

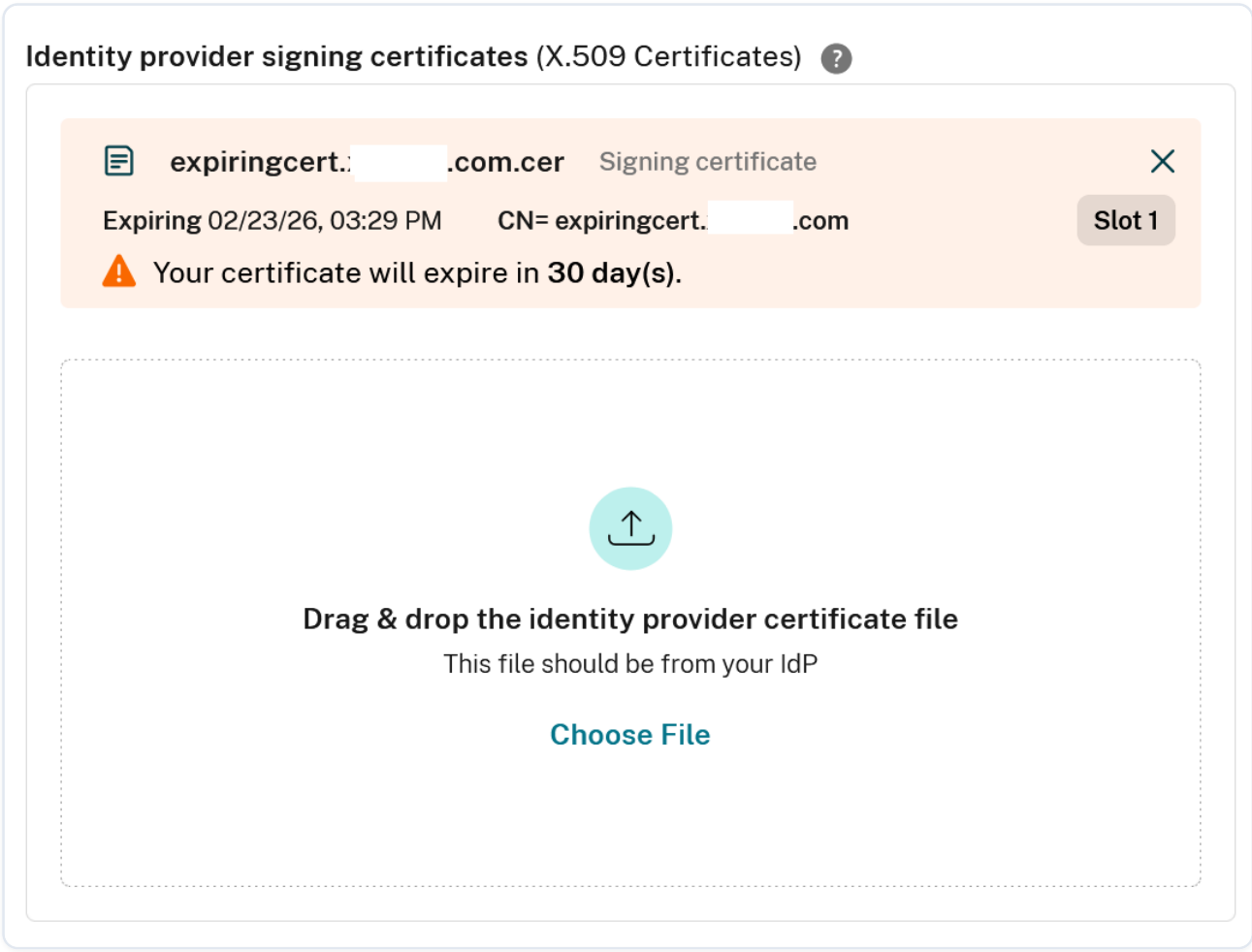
SAMLアプリケーションの署名証明書の有効期限が近づいていることをどのように知ることができますか?

IdPのSAMLアプリケーション内で現在アクティブな証明書の有効期限を確認する必要があります。

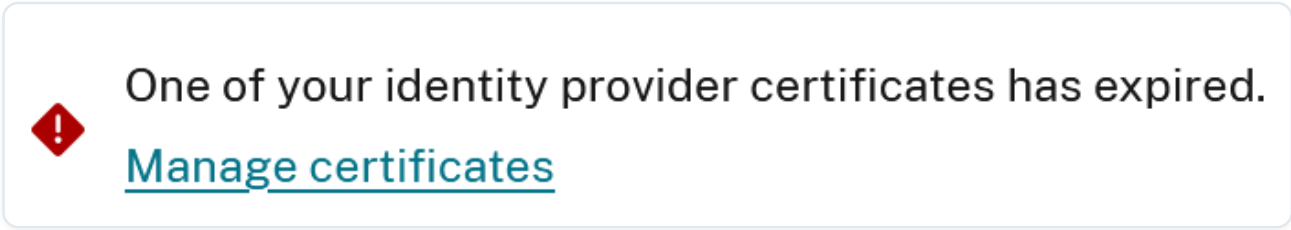
SAMLアプリケーションの署名証明書の有効期限が切れる30日前に、Citrix CloudはSAML接続の**IDおよびアクセス管理 > 認証**内にSAML IDP接続に関する警告を表示します。

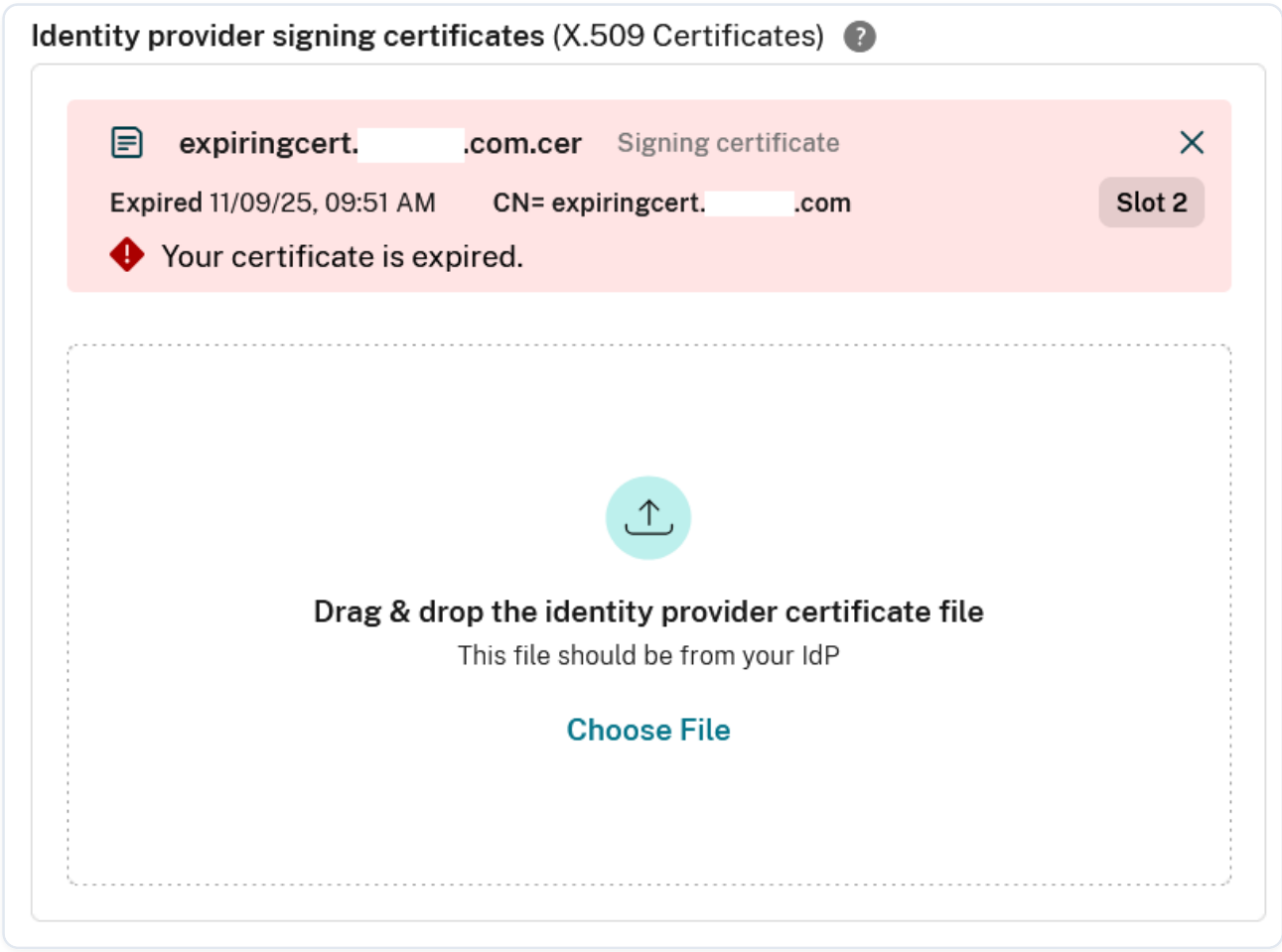
証明書の管理をクリックすると、新しい証明書をアップロードしたり、期限切れの証明書を削除したりできる**表示 > SAML接続**ページにリダイレクトされます。





Citrix Cloudは、以下に示すように、IdP証明書が実際にすでに期限切れになっている場合、SAML接続でエラーも表示します。期限切れのIdP証明書は、証明書が置き換えられるまでSAML接続を使用不能にします。





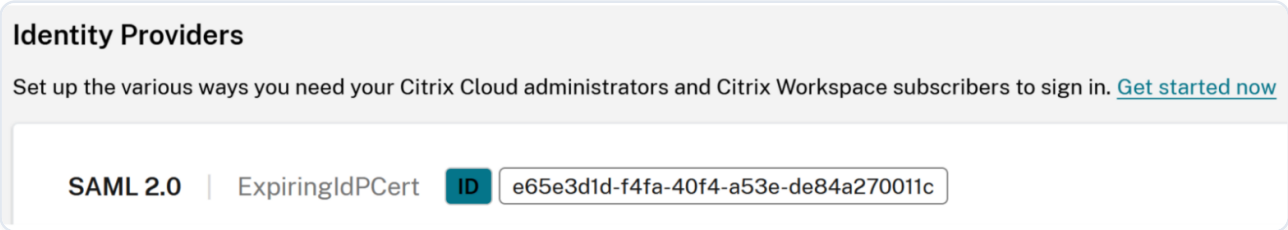
SAMLアプリケーションの署名証明書の有効期限が切れそうになった場合、Citrix Cloudからどのような通知を受け取りますか?

Citrix Cloud管理者は、**今後30日以内**に有効期限が切れるIDP証明書を持つSAML接続が1つ以上ある場合、**重要な通知**を受け取ります。Citrix Cloudはすべての SAML接続を監視し、今後30日以内に有効期限が切れる証明書を含む接続を検出します。Citrix Cloudテナントからの通知に加えて、SAML IdPからSAMLアプリ証明書の有効期限が近づいていることに関する通知を受け取る場合もあります。

重要:

Citrix Cloud管理者がすべてのメールおよびCitrix Cloudコンソール通知を無効にすることを選択した場合、SAML IdP証明書の有効期限が近づくと、これらの重要な警告を見逃す可能性があります。Citrix Cloud管理者は、少なくとも1人以上の有効な管理者ユーザーがこれらの重要な通知を受け取れるようにする責任があります。Citrix Cloud管理者が通知を管理する方法については、この記事を参照してください。

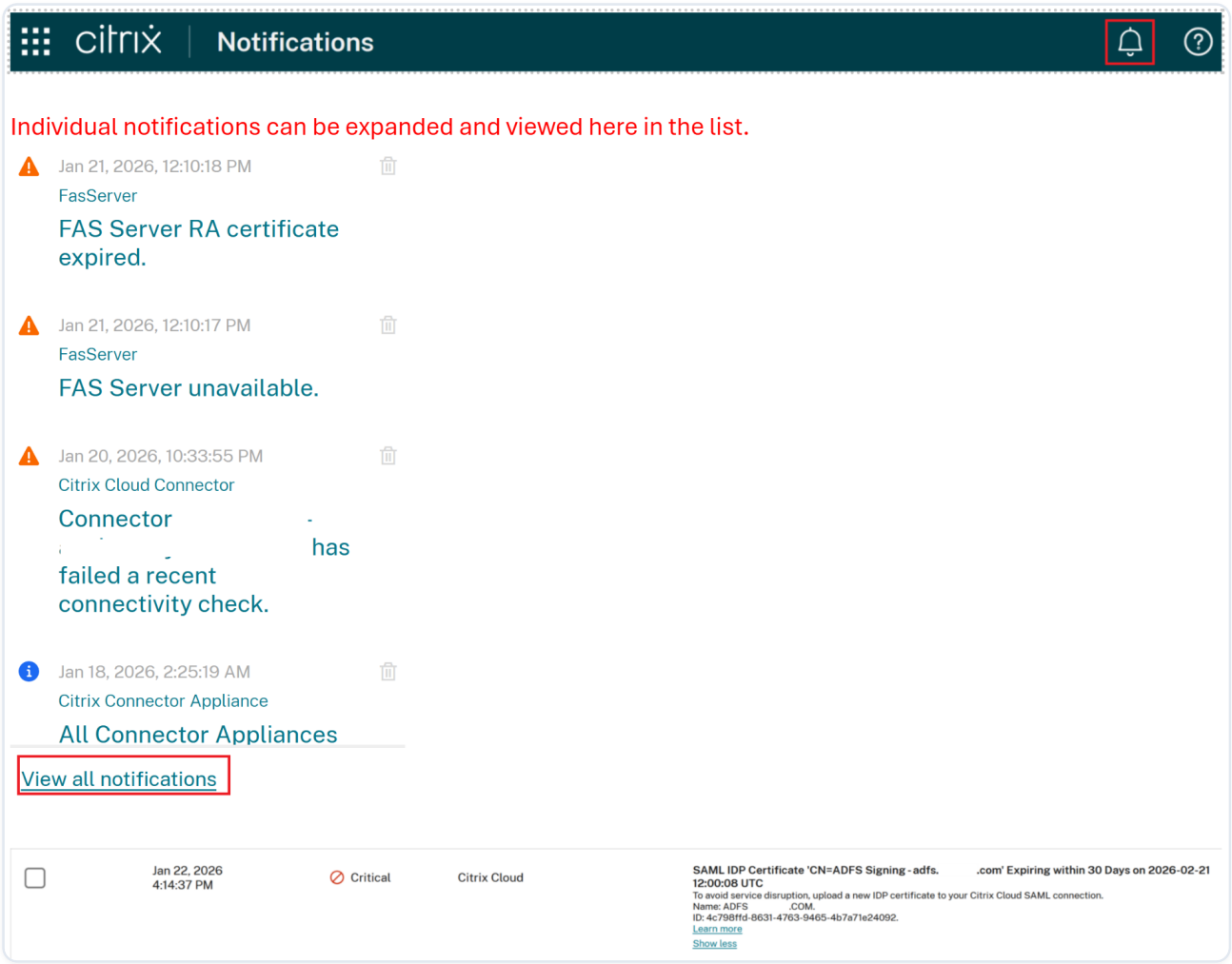
> すべてのIdP証明書の有効期限通知には、Citrix Cloud内のSAML接続と、IDプロバイダー内で有効期限が切れるIdP証明書を特定するのに役立つ詳細が含まれています。 > に移動してください。



- SAML接続ニックネーム: `ExpiringIdPCert`
- SAML接続ID: `e65e3d1d-f4fa-40f4-a53e-de84a270011c`
- 証明書の共通名: `CN=expiringcert.domain.com`
- 有効期限: `2025-12-27`

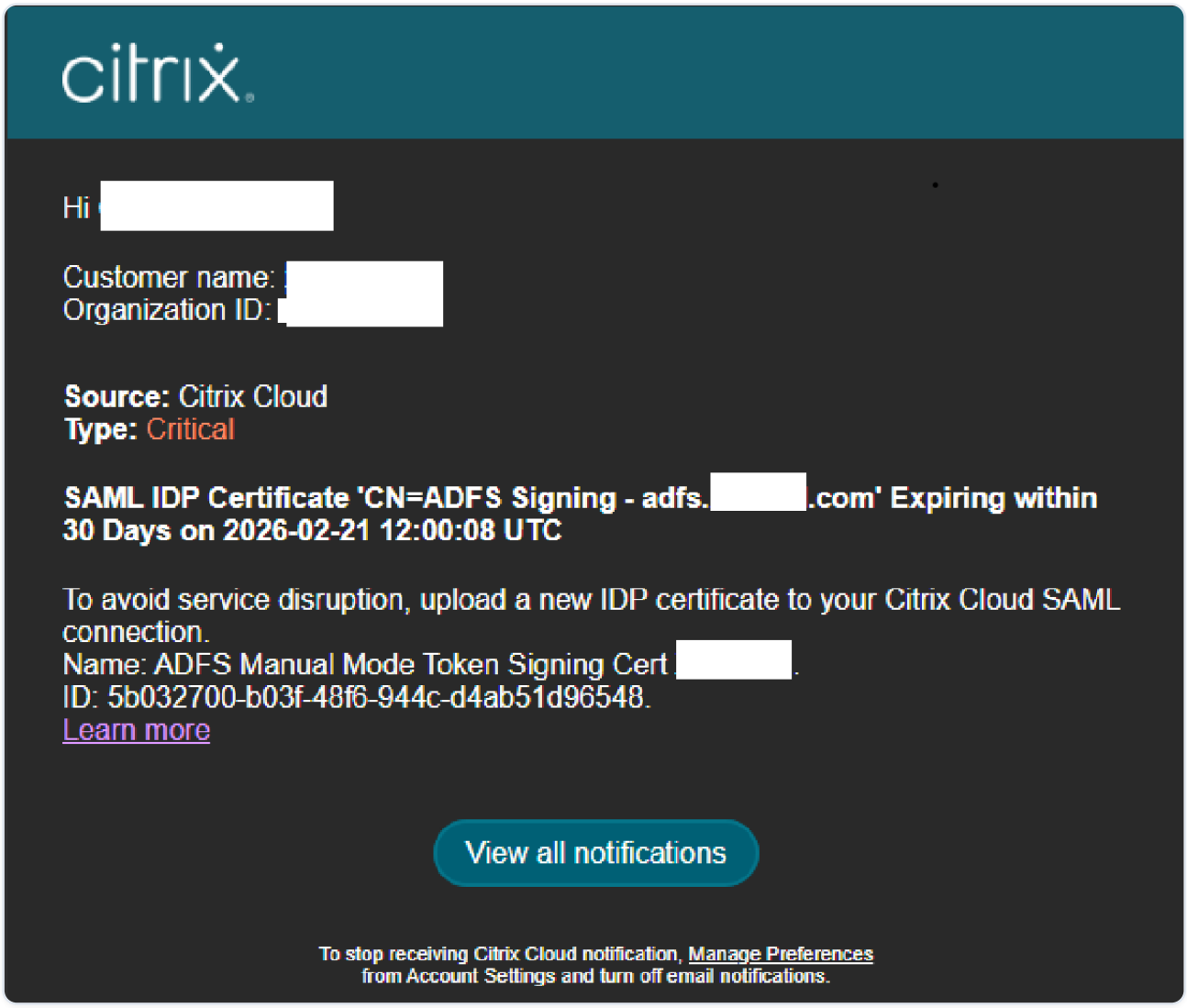
CITRIX CLOUDポータル内の管理者通知

Citrix Cloudのホームページに移動し、ベルのアイコンをクリックして「すべての通知を表示」を選択します。今後30日以内に有効期限が切れる証明書とSAML接続を示す重要なアラートを探してください。



メール通知

IdP証明書の有効期限通知が**一度送信されると**、再度送信されることはありません。これは、不要なメールのスパムを防ぎ、Citrix Cloud管理者が通知メールを一度だけ受け取り、有効期限が近づく30日間毎日別のメールを受け取らないようにするためです。Citrix Cloudの通知が却下された場合、再送信されることはありません。


citrix.

Hi [redacted]

Customer name: [redacted]
Organization ID: [redacted]

Source: Citrix Cloud
Type: Critical

SAML IDP Certificate 'CN=ADFS Signing - adfs.[redacted].com' Expiring within 30 Days on 2026-02-21 12:00:08 UTC

To avoid service disruption, upload a new IDP certificate to your Citrix Cloud SAML connection.
Name: ADFS Manual Mode Token Signing Cert [redacted].
ID: 5b032700-b03f-48f6-944c-d4ab51d96548.
Learn more

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

Citrix Cloud SAML接続を使用しながら、サービス停止を引き起こすことなくSAML IdP証明書を更新できますか?

はい。SAML IdP接続に2つ目のIdP証明書を導入することで、SAMLアプリケーション証明書のシームレスなロールオーバーが可能になります。現在の証明書の有効期限が切れる**少なくとも24時間前までに新しい証明書をアップロードしてください。この記事に正しく従っていれば、エンドユーザーまたはCitrix Cloud管理者ユーザーは影響を受けません。**

SAMLアプリケーションから最新のIDプロバイダー (IdP) 署名証明書のコピーはどこで入手できますか?

PingFederateなどのオンプレミスSAML IdP内で使用される証明書は、組織内のプライベート認証局またはDigicertのような商用認証局から取得されます。クラウドベースのSAML IdP SAMLアプリは、SAMLアプリUI内でいつでもオンデマンドで新しいIdP証明書を生成できます。新しいIdP署名証明書はいつでも生成でき、非アクティブに設定できます。

Citrix Cloudは同時に2つの異なるIdP署名証明書を信頼できますか?

はい。シームレスなIdP証明書のロールオーバーはこれに依存します。 Citrix Cloud SAML接続はSAML応答を信頼します。これらの応答は、SAML接続にアップロードされた2つの信頼されたIdP署名証明書のいずれかで署名されている必要があります。いずれかの証明書の有効期限が切れている場合、Citrix Cloudによって信頼されなくなり、SAMLアプリケーションでこれ以上使用すべきではありません。

Citrix Cloud SAML接続は、1つまたは2つのSAMLアプリケーション証明書を保存できます。

Slot1: は、Citrix Cloud SAML接続を最初に作成したときにアップロードした証明書を含みます。サービス停止を防ぐために、この証明書は有効期限が切れる前に交換する必要があります。

Slot2: は、SAML接続が作成された後は常に空ですが、**Slot1** の証明書の有効期限が切れる前に新しいSAMLアプリ証明書をアップロードするために使用できます。これは、有効期限が切れる **Slot1** の署名証明書に代わる代替の信頼された証明書を提供することを目的としています。

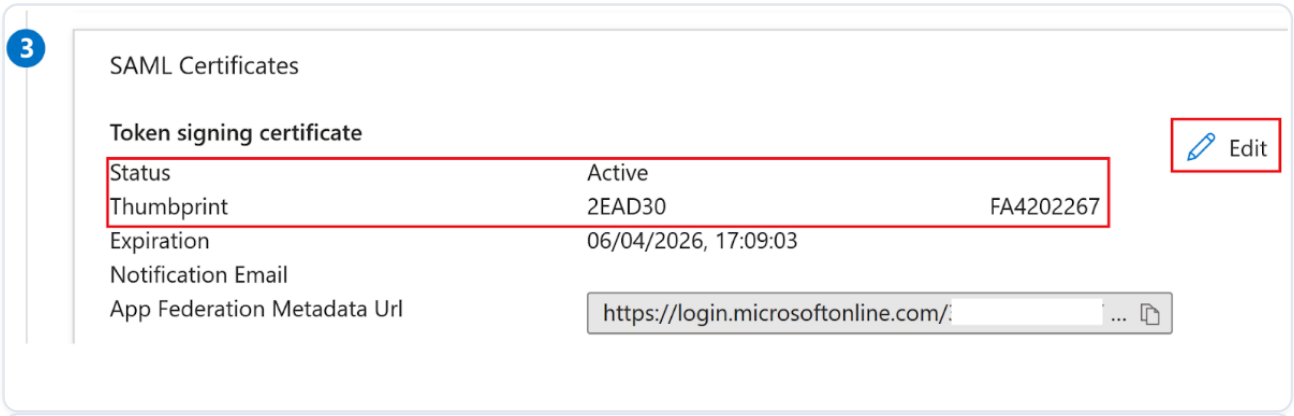
Citrix Cloud内のSAML接続から「古い」IDプロバイダー (IdP) 署名証明書を削除するのはいつですか?

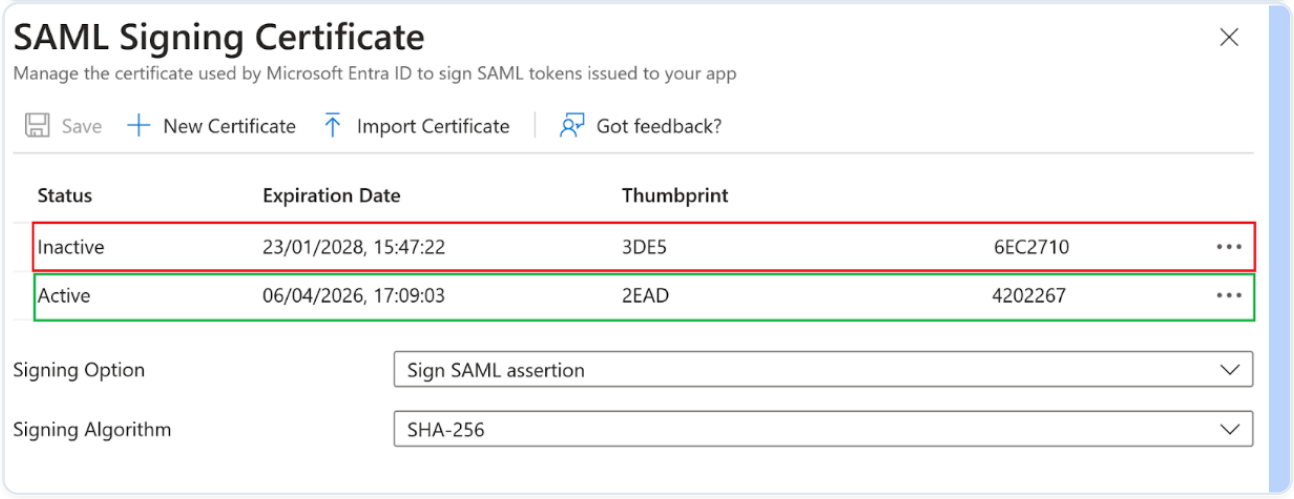
古い IDプロバイダー (IdP) 署名証明書は、SAMLアプリケーション内で「新しい」署名証明書が**アクティブ化された**ことを確認し、それを使用してストアおよび/またはCitrix Cloudに正常にログインした**後で**のみ、Citrix Cloud SAML接続から削除する必要があります。両方のIdP証明書がCitrix Cloud接続にまだ存在する場合、失敗したIdP証明書のローテーションメンテナンス作業をロールバックする方が簡単です。両方の証明書がまだ有効である限り、Citrix Cloudは両方を信頼できます。IdP証明書の有効期限がすでに切れている場合、それにロールバックすることはできません。

SAMLアプリケーションが現在SAML応答の署名にどのIdP署名証明書を使用しているかを確認するにはどうすればよいですか?

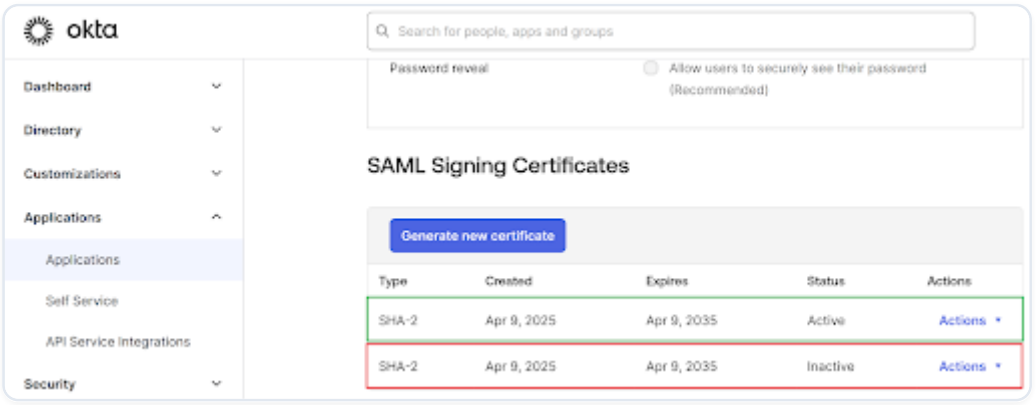
SAMLアプリケーションは、SAML応答に署名するために一度に1つの証明書のみを使用します。SAMLアプリケーションで現在**アクティブ**に設定されている証明書を使用します。**アクティブ**なIdP署名証明書は、SAMLアプリケーションのメタデータにも存在します。

以下のスクリーンショットは、Entra IDの例を示しています。





以下のスクリーンショットは、Oktaの例を示しています。



SAMLアプリケーションのIdP証明書ローテーションをスケジュールされたメンテナンス タスクとして実行する

> **重要:**

> サービス停止を防ぐため、SAML接続内のIdP証明書のうち少なくとも1つは、有効期限内でIdP内でアクティブである必要があります。Citrix Cloud証明書内に単一のIdP証明書のみが構成されており、その証明書の有効期限が切れた場合、ユーザーはサービス停止を経験し、

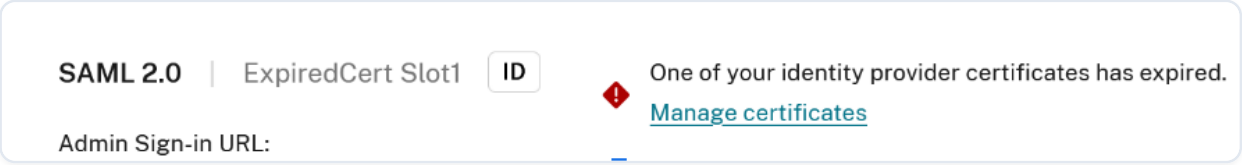
> SAMLログオンは失敗します。この状況は、SAML接続の使用方法に応じて、ストアユーザーやCitrix Cloud管理者ユーザーに影響を与えます。

1. 現在の証明書の有効期限が切れる数日前に、IdP証明書のローテーションを実行する計画を立ててください。
2. ローテーション先のSAMLアプリケーション内から、交換用のIdP証明書のコピーを入手してください。IdP証明書がPEM、CER、またはCRT形式であり、Citrix Cloud SAML接続にアップロードできる状態であることを確認してください。
3. SAMLアプリケーション内で証明書のローテーションをトリガーする少なくとも24時間前に、交換用のIdP証明書をCitrix SAML接続にアップロードしてください。

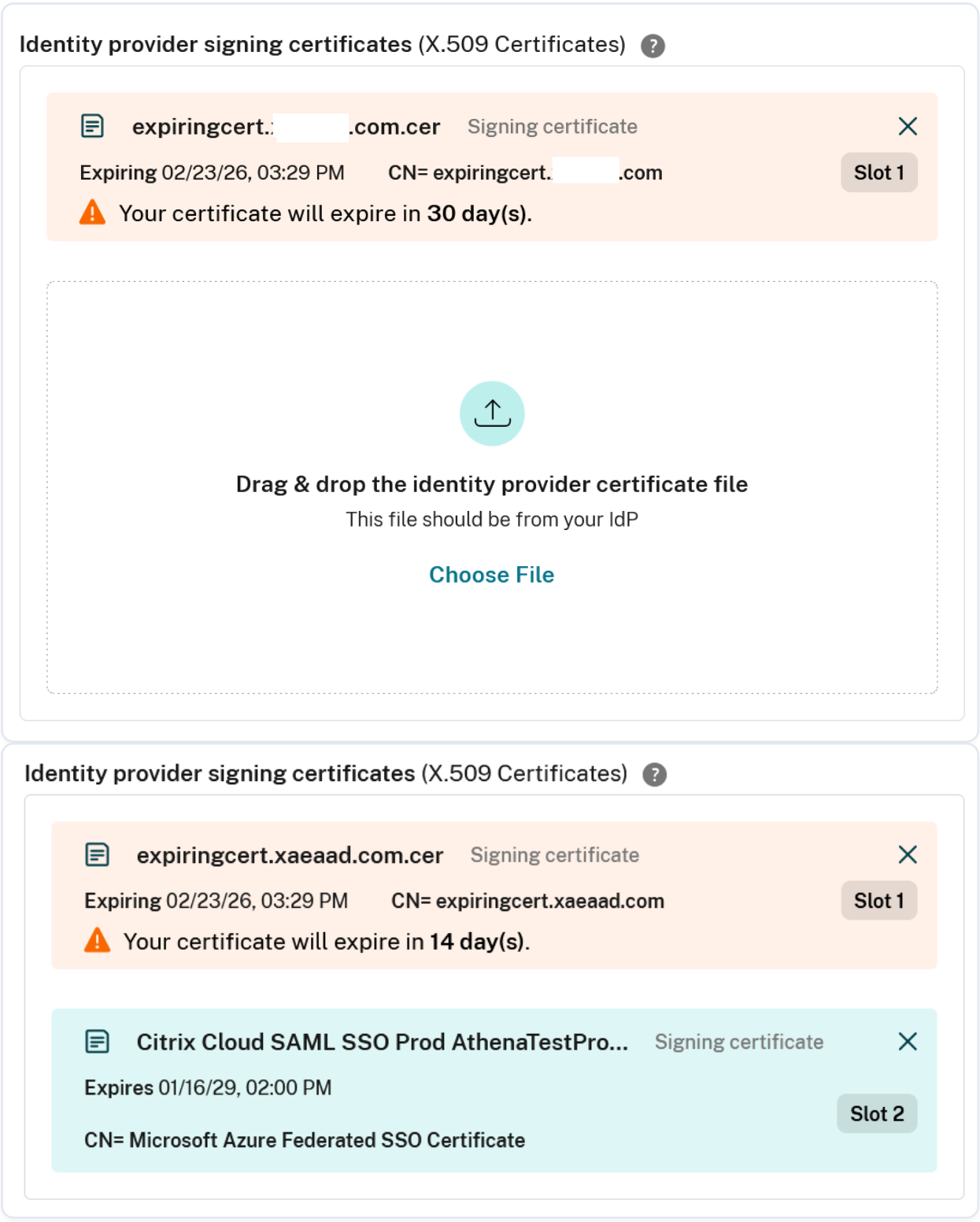
   Identity and Access Management > Authentication 内のSAML接続に移動します。今後30日以内に有効期限が切れる証明書を持つSAML接続の3つの点をクリックし、**View** をクリックします。

   または、,

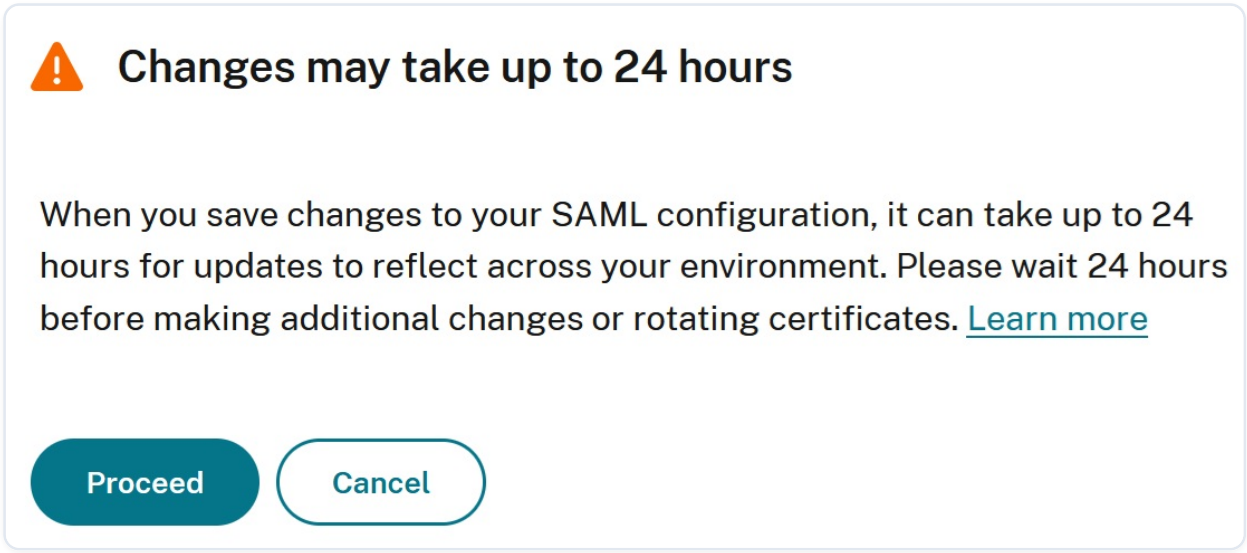
   「**証明書の管理**」をクリックします。

4. Citrix Cloud SAML接続内で**Slot2**アップロードオプションを使用して、2番目のIdP証明書をアップロードします。



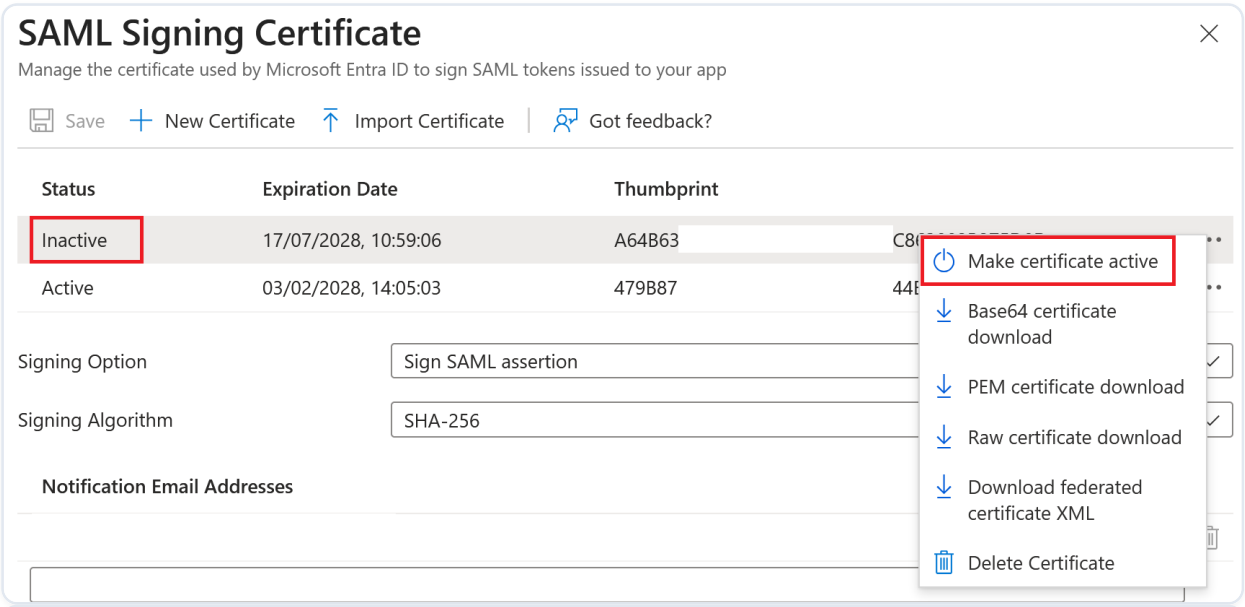
5. 新しい証明書をアップロードしたら、SAML接続を保存します。

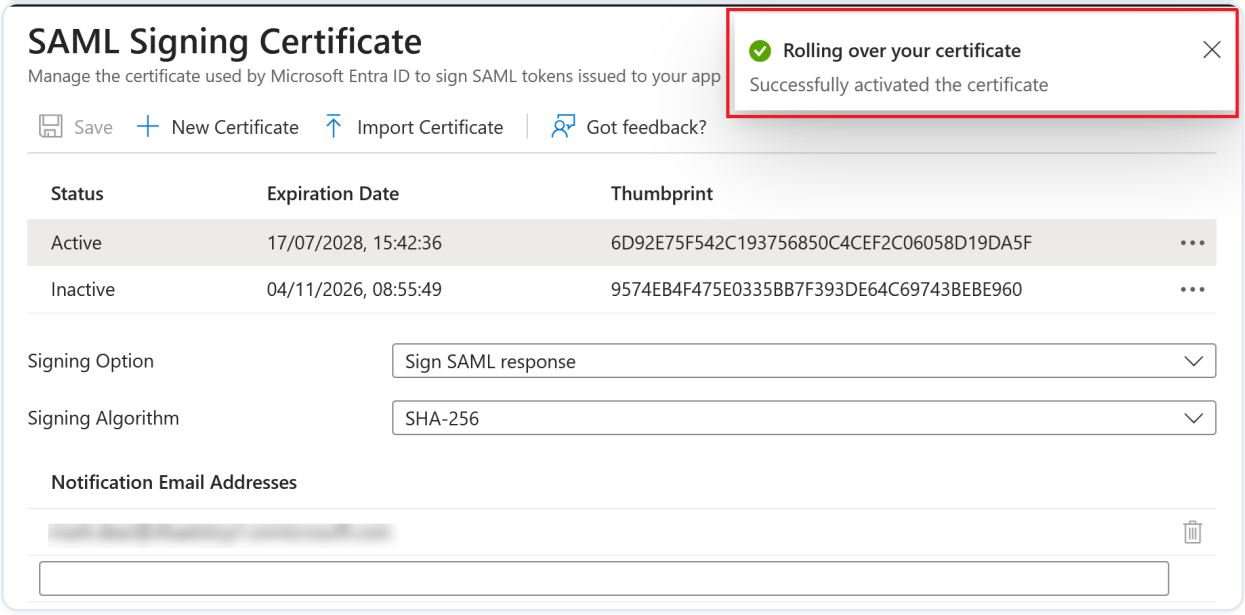


6. **約24時間待機**してから、IdP内で**ロールオーバーアクション**を実行し、セカンダリIdP証明書を**アクティブ**に設定します。証明書をロールオーバーする方法は、SAML IdPごとに異なります。

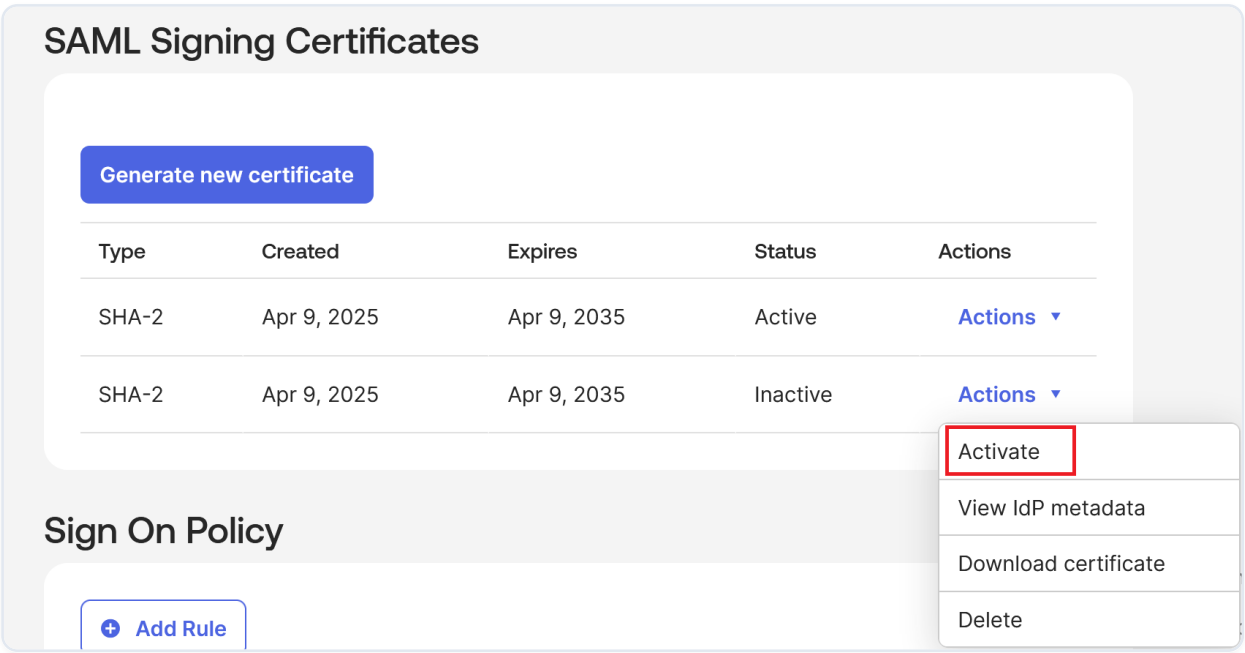
> **重要:**
>
> Citrixの認証プラットフォームは、復元力とパフォーマンスの理由から、すべてのIDP設定をキャッシュします。キャッシュされた値のため、Citrix Cloudに代替証明書をアップロードしてから、SAMLアプリケーション内で証明書をすぐにローテーションすることはできません。新しい証明書のアップロードとSAMLアプリ内での新しい証明書のアクティブ化の間には遅延が必要です。この遅延により、Citrix認証キャッシュが新しくアップロードされた証明書で更新されます。24時間の遅延は、キャッシュのTTL値よりも長いです。この期間により、SAMLアプリケーションが翌日に新しい証明書を使用するように切り替える際に、新しい証明書が利用可能になります。

> **Entra ID SAMLアプリケーション:**





Okta SAMLアプリケーション:



7. ストアURLまたはCitrix Cloud SAMLサインインURLのいずれかを使用してSAMLログオンが成功するかどうかをテストし、SAMLアサーション内の署名証明書の値を確認します。

既存のストアカスタムドメインSAML接続にセカンダリSAML IdP証明書をアップロードする?

ストアカスタムドメインをサポートするように構成されているセカンダリSAMLアプリケーションで使用されているIDP証明書を更新する必要がある場合は、上記と同じ手順に従ってください。

1. **StoreFront Cloud > Access > Custom store URL > 3つの点を選択 > Edit** に移動します。

セカンダリSAML証明書(/en-us/citrix-cloud/media/secondary-saml-cert.png)

IDP署名証明書のローテーションのトラブルシューティング

IdP証明書のローテーションを実行した後にSAMLログオンの問題が発生した場合は、SAMLトレーサーファイルを取得し、SAML応答内の証明書base64データを確認してください。

1. ブラウザにストアURLまたはCitrix Cloud GO URLのいずれかを入力する**前**に、SAMLトレーサーのキャプチャを開始します。認証プロセス全体を最初から最後までキャプチャしていることを確認してください。
2. IdPを使用してストアまたはCitrix Cloudのいずれかに SAMLログオンを実行し、資格情報の入力を求められたら認証ステップを完了します。
3. IdPからCitrix Cloud SAMLエンドポイント `https://saml.cloud.com/saml/acs` に送信されたSAML応答と、SAMLトレーサーファイル内のエントリをここで見つけます。

   SAMLトレーサーファイル内のエントリ(/en-us/citrix-cloud/media/entry-inside-saml-tracer-file.png)
4. SAML XML内の証明書セクションを見つけ、IDP署名証明書のbase64データを適切なツールにコピーしてデコードします。

   証明書コピーツールデコード(/en-us/citrix-cloud/media/certificate-copy-tool-decode.png)

   > **重要:**
   >
   > この手順は、CitrixのSAML推奨構成に従い、Citrix Cloud SAML接続内でSAMLバインディングとしてHTTP POSTを使用していることを前提としています。

5. 証明書をbase64データからデコードし、正しい日付と時刻でSAML IdPのアクティブな証明書と一致するか確認します。

   Openssl デコードコマンド(/en-us/citrix-cloud/media/decode-openssl-command.png)

6. ステップ4および5でSAML応答から取得した証明書が期待どおりでない場合、IdP内で正しい証明書をアクティブ化してください。SAMLアプリケーション内のアクティブな証明書を確認してください。この証明書はSAML応答に含まれています。

高度なSAMLシナリオと、SAMLアサーション内でのcip_forestおよびcip_domainの正しい使用法

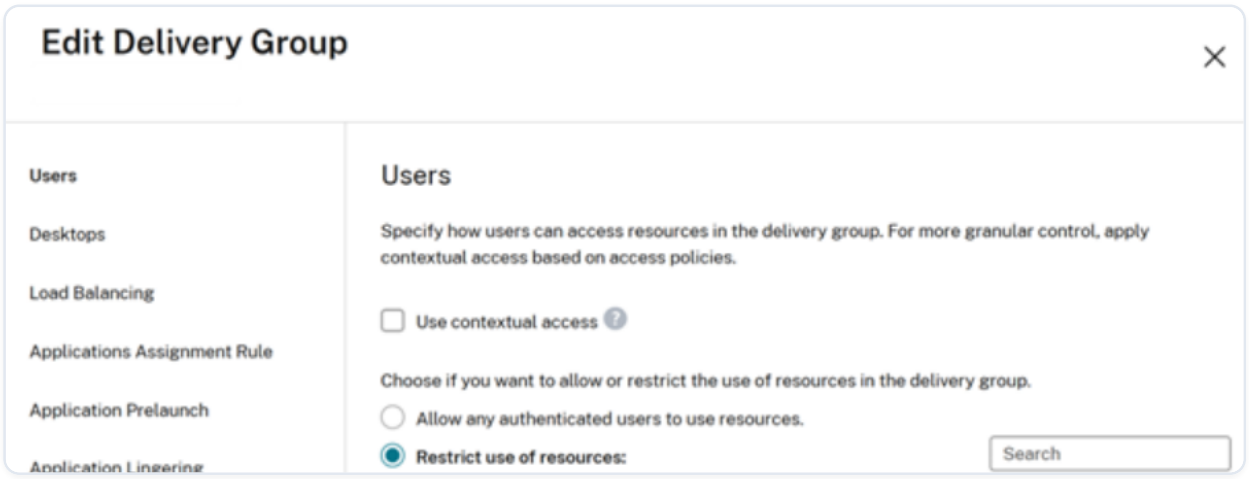
この記事では、複数の接続されたActive Directoryフォレストとドメインを含むCitrix Cloudまたはストアの高度なSAML構成について説明します。この記事は、複雑なAD展開を持つ大企業を対象としており、アーキテクトレベルのCitrix Cloud、IdP、およびAD管理者によって実装されるべきです。この高度なSAML構成の最も一般的な使用法は、異なるADインフラストラクチャ、複数のフォレスト、および異なるUPNを持つADバックエンドユーザーの異なる集団を持つ多くの小規模組織から大企業が形成される合併・買収シナリオです。条件付き認証も、合併・買収シナリオでしばしば必要とされます。

オプションのcip_forestおよびcip_domainクレームを使用すると、Citrix Cloud管理者は、SAML認証中にADバックエンドユーザーアカウントを検索するためにどのCitrix Cloud Connectorが使用されるかをより詳細に制御できます。SAMLを使用するCitrix Cloudは、Okta IdPやEntra ID IdPなどの他のCitrix Cloudフェデレーション OIDC認証方法では不可能な、多くの高度なアカウントマッピングユースケースをサポートしています。

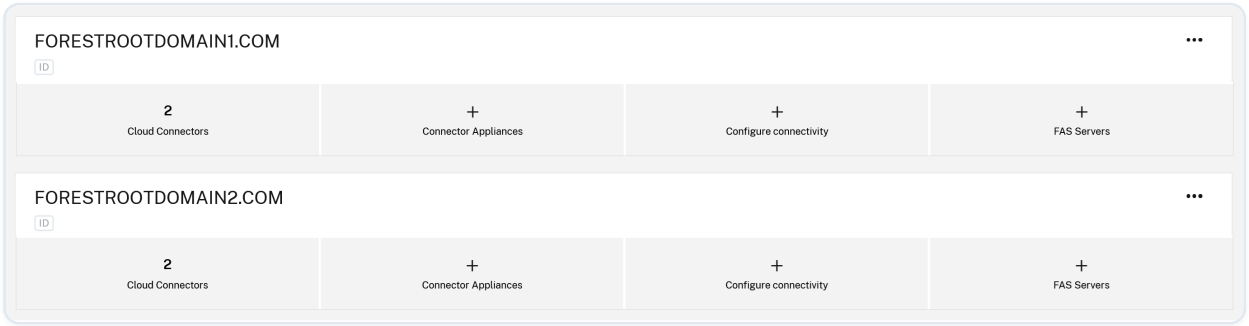
前提条件

- エンドユーザーを認証するためにAD IDを使用する、デフォルトのCitrix Cloud SAMLフローを使用します。
- ADフォレストまたはドメインインフラストラクチャと、ストアのエンドユーザーのIDがどこにあるかについて、広範な理解があること。
- 正しいADフォレストとドメインに参加し、正しいADドメインレベルで参加しているCitrix Cloud Connector。
- Citrix Cloudテナント内にすでに構成されている既存のリソースの場所とCitrix Cloud Connectorに関する知識。
- Citrix Cloudに接続されている複数のADフォレスト間に、Active Directoryの信頼関係がないこと。
- フロントエンド（Entra ID、Okta、Duo）とバックエンドユーザー（AD）のIDが何を意味するかを理解していること。
- フロントエンドとバックエンドのユーザーIDは、一致するUPNを介してリンクされている必要があります。一致するUPNを持たないフロントエンドとバックエンドのユーザーIDのペアをリンクすることはサポートされていません。

- 各UPNサフィックスがActive Directory内のどこに存在するか、および特定のUPNサフィックスがあいまいであり、複数の接続されたADフォレストに存在するかどうかを理解していること。
- DaaS VDAはADドメインに参加している必要があります。
- DaaSアプリケーションとデスクトップはAD IDに公開されている必要があります。
- DaaSでデリバリーグループのリソースをADグループにマッピングする場合、ユニバーサルADグループが必須です。
- DaaSデリバリーグループは「リソースの使用を制限する」に設定し、適切なユニバーサルADグループに割り当てる必要があります。DaaSデリバリーグループ内で「認証されたすべてのユーザーがリソースを使用できるようにする」を使用することはサポートされていません。



- FASサーバーは、適切なADフォレストに参加し、適切なADレベルでドメインに参加している必要があります。FASサーバーは、DaaS起動時のADドメイン参加済みVDAへのSSONに必要です。



- 複数のSAMLアプリがあり、接続されているADフォレストごとに1つのSAMLアプリが必要な場合は、条件付き認証を実装する必要がある場合もあります。合併・買収のシナリオでは、各SAMLアプリでcip_forestとcip_domainに異なる値のセットが必要になる場合があります。

FAQ

SAMLアサーションでcip_sidを送信する場合、cip_forestとcip_domainのオプションのクレームも送信する必要がありますか?

いいえ。SAMLアプリケーションがcip_sidクレームを送信するように構成されており、それがSAMLアサーションに含まれている場合、Citrix CloudはADバックエンドユーザーがどのフォレストとドメインにいるかを常に正しく識別できます。cip_forestとcip_domainは必須ではありません。

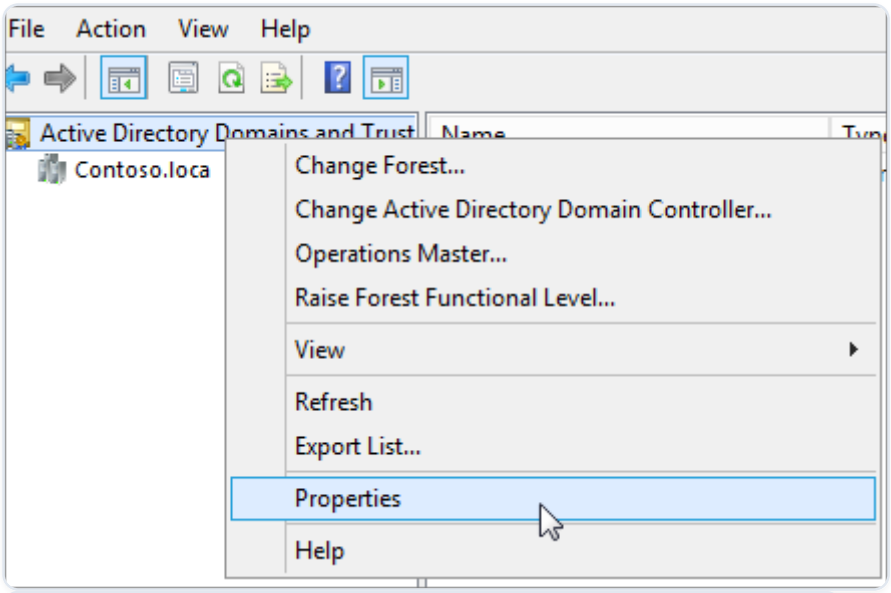
> **重要：**
>
> - SAMLアサーションでcip_sidを送信できないSAMLシナリオでは、代わりにcip_forestとcip_domainの使用が必要になる場合があります。
> - 誤ったSIDを含むフロントエンドユーザー。これは、DaaSデリバリーグループ内にマッピングされたバックエンドADユーザーのSIDと一致しません。
> - ADインポートツールを介してIdP内で作成されなかったネイティブのOkta、Entra ID、またはDuoユーザーなど、埋め込みSIDをまったく持たないフロントエンドユーザー。

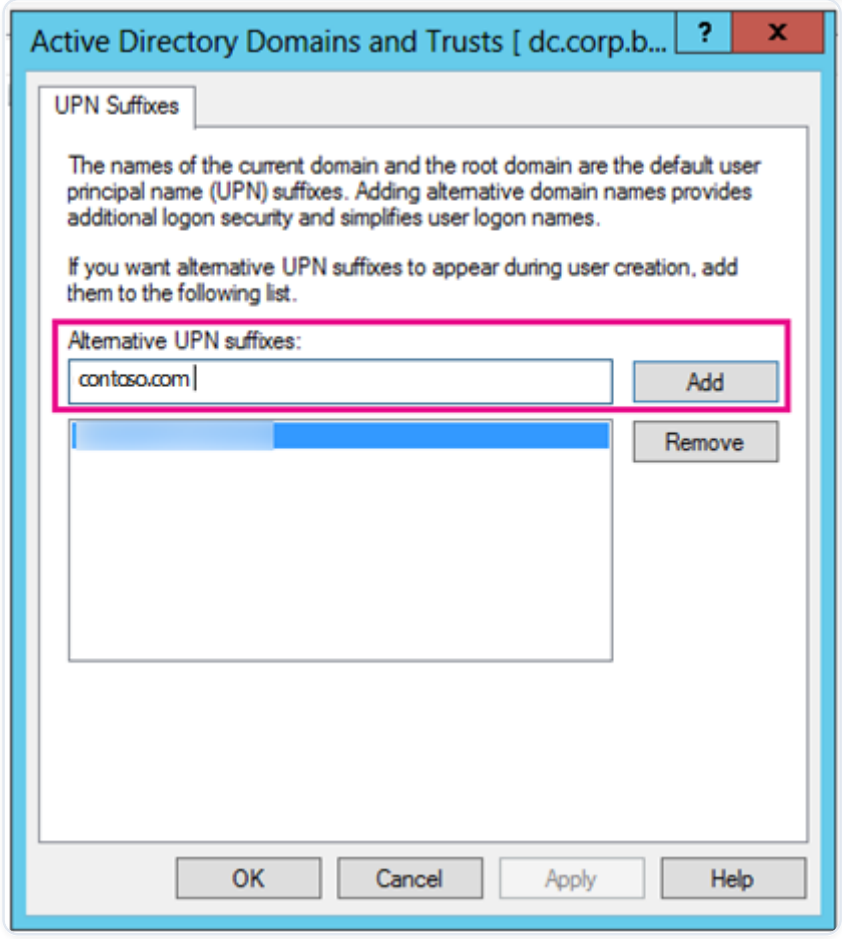
ADの暗黙的なUPNサフィックスとは?

暗黙的なUPNはActive Directoryによって自動的に作成され、ユーザーのsAMAccountNameとフォレストのDNS名に基づいています。暗黙的なUPNは、sAMAccountNameとドメインのDNS名から派生するため、ADフォレスト内で常に一意です。これらはADフォレスト内で一意です。例：`@rootforestdomain.local`

ADの明示的な (ALT) UPNサフィックスとは?

「明示的なUPNサフィックス」とは、AD管理者がActive Directoryドメインと信頼関係に追加するカスタムドメイン名です。例：`@rootforestdomain.local`





重要:

Windows AD PowerShellでは、指定したUPNサフィックスがADフォレスト内に存在しない場合でも、任意のUPNサフィックスを持つADユーザーを作成できます。使用したい代替UPNサフィックスは、Citrix Cloud Connectorがバックエンドアカウントユーザーを検索するためにこのリストに依存するため、ADフォレスト内に存在する必要があります。上記のスク

> リーンショットに示されているように、代替UPNサフィックスがADフォレストで構成されていない場合、Citrix CloudはフロントエンドIDを適切なバックエンドADアカウントと照合できません。

UPNの曖昧さとは何か、Citrix CloudおよびDaaSにとってなぜ問題となるのか?

UPNの曖昧さとは、Citrix Cloudに接続された2つ以上のADフォレストに`duplicateuser@domain.com`が存在する場合に発生する状況です。@domain.comというUPNサフィックスだけでは、`duplicateuser@domain.com`の2つのバージョンが存在する場合に正しいADバックエンドユーザーを特定することはできません。これにより、DaaSリソースの列挙がまったく失敗したり、ADドメイン参加済みVDAを使用して公開された誤ったDaaSリソースがストア内に表示されたりする可能性があります。

ユニバーサルADグループが要件となるのはなぜですか?

ユニバーサルADグループはグローバルカタログ (GC) に保存され、フォレスト内のすべてのドメインコントローラーから参照できます。これにより、同じフォレスト内の任意のドメインにあるリソースにアクセス許可を割り当てるために使用できます。

> **重要:**
>
> ADユニバーサルグループの使用は、cip_forestとcip_domainを含む高度な構成だけでなく、すべてのSAML構成の要件です。グローバルなどの他のADグループタイプを使用すると、ストアでのリソース列挙が失敗する可能性があります。

> ADグループスコープに関するこのMicrosoftの記事を読むことをお勧めします。

DaaSデリバリーグループ内で「認証済みユーザーがリソースを使用することを許可する」を使用することが推奨されないのはなぜですか?

認証済みユーザーがリソースを使用することを許可するを構成すると、ADドメイン参加済みVDAを使用して公開されたリソースが、同じドメインおよびフォレスト内にないADユーザーIDのストア内に表示されます。フォレスト1のストアADエンドユーザーIDを使用して、フォレスト2でドメイン参加したVDAからリソースを起動することは成功しません。

SAMLアサーションでcip_forestのみ、またはcip_domainのみを送信できますか?

いいえ。バックエンドユーザー検索のために特定のADフォレストとドメインコンテキストを指定したい場合は、SAMLアサーションで両方のオプションクレームを提供する必要があります。

cip_forestの値を指定する場合、どのUPNサフィックスを使用すべきですか?

ADフォレストの暗黙的なUPNサフィックスを使用する必要があります。cip_forestクレーム内でADフォレストに追加されたALT UPNサフィックスの値を指定しないでください。これは、Citrix Cloudに接続されている複数のADフォレストに同じALT UPNサフィックスが追加されているADトポロジが存在する可能性があるためです。暗黙的なUPNサフィックスとDNは、DC=duplicate,DC=comのような同じDNを持つ2つの異なるADフォレストがCitrix Cloudに接続されていない限り（これはありそうにないシナリオですが）、Citrix Cloudにとって曖昧になることはありません。

cip_forestとcip_domainの値は、いつ同じであるべきですか、それとも異なるべきですか?

シナリオ1: Citrix Cloud Connectorがフォレストルートレベルでドメイン参加しており、バックエンドADアカウントユーザーが接続されたADフォレスト内のルートドメイン内に存在する場合。

cip_domainとcip_forestは同じ値を持つべきです。

cip_forest = "forestrootdomain.com"

cip_domain = "forestrootdomain.com"

シナリオ2: Citrix Cloud ConnectorがADフォレスト階層の子ドメインにドメイン参加している場合。バックエンドADユーザーは、ADフォレスト内の「childdomain.forestrootdomain.com」内に存在します。

cip_domainとcip_forestは異なる値を持つべきです。

cip_forest = "forestrootdomain.com"

cip_domain = "childdomain.forestrootdomain.com"

SAMLアサーション内でcip_forestとcip_domainの値をハードコードできますか?

はい、ただし、DaaSリソースにマッピングされているバックエンドADユーザーの全人口が同じADフォレストに存在する場合に限ります。cip_forestとcip_domainの値をハードコードするには、すべてのフロントエンドユーザーが対応するバックエンドADアカウントを同じADフォレストとドメインに持つ必要があります。

SAMLアサーション内でcip_forestとcip_domainに異なる値を動的に指定できますか?

はい、SAMLプロバイダーがクレーム変換ルールを通じてこれを許可している場合です。異なるUPNサフィックスを持つ異なるフロントエンドユーザーの集団がいる場合、グループメンバーシップのような切り替え条件を使用して、cip_forestとcip_domainの値を動的に指定することが可能です。これはEntra ID SAMLアプリケーション内で可能であり、クレーム変換ルールをサポートする他のSAML IdPでも可能である場合があります。

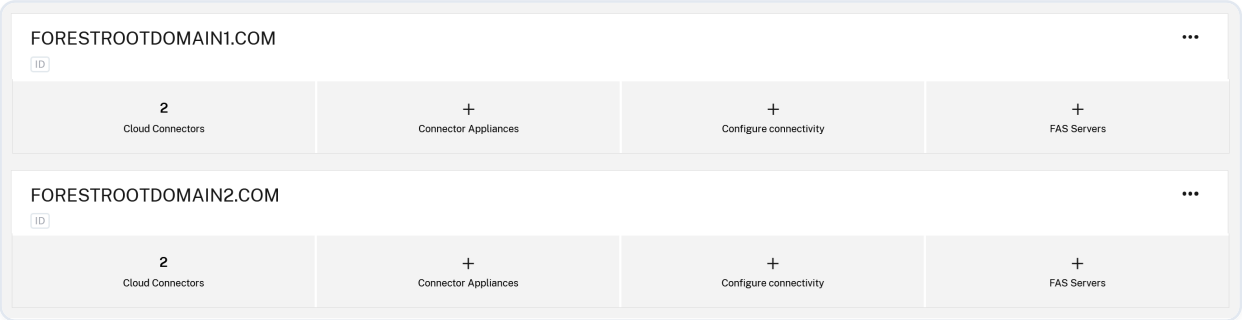
ADドメイン参加済みVDAへのSSON起動が成功するように、FASサーバーはどこに配置すべきですか?

FASサーバーは、バックエンドADアカウントが存在する各バックエンドADフォレスト内でドメイン参加され、構成されている必要があります。FASサーバーをADフォレストのルートドメインレベルでドメイン参加させることをお勧めします。

SAMLアサーションでcip_forestとcip_domainが必要とされるADトポロジ

シナリオ1：SAMLエンドユーザーのUPNがあいまいであり、Citrix Cloudに接続された複数のADフォレストに存在する

- Citrix Cloudテナントには、2つ以上のリソースロケーションと、Citrix Cloudに接続された複数のADフォレストまたはドメインがあります。



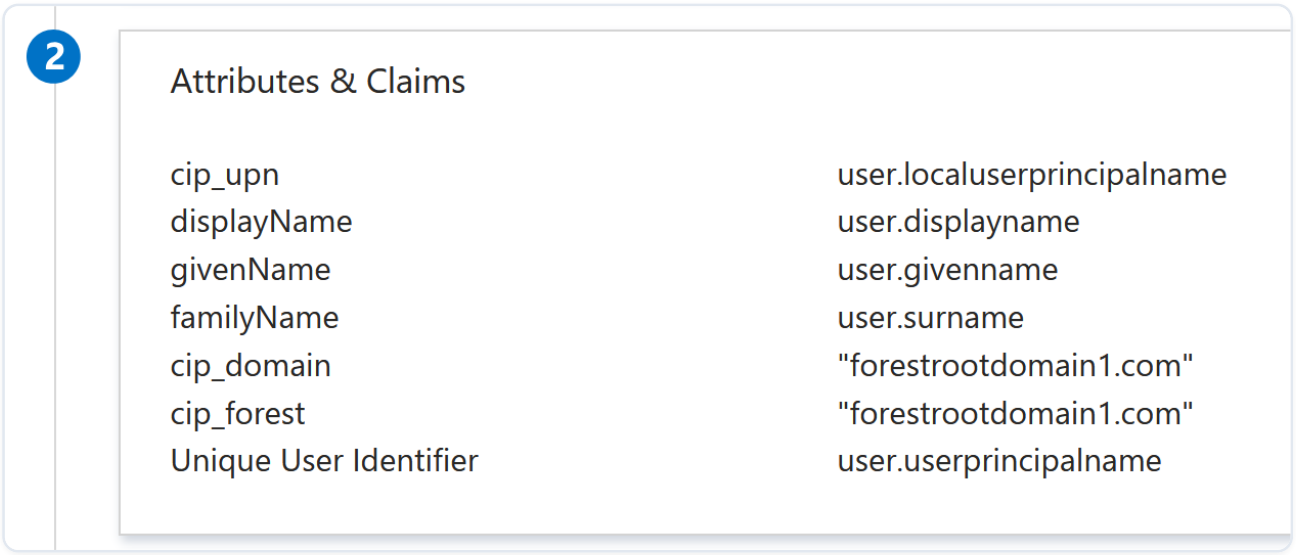
- リソースロケーション1にはCitrix Cloud Connectorが含まれており、これらはルートフォレストレベルでAD forestrootdomain1.comにドメイン参加しています。
- リソースロケーション2にはCitrix Cloud Connectorが含まれており、これらはルートフォレストレベルでAD forestrootdomain2.comにドメイン参加しています。
- forestrootdomain1.comとforestrootdomain2.comは両方とも同じUPN @domain.comサフィックスを持っています。
- forestrootdomain1.comとforestrootdomain2.com内には、同じUPN `duplicateuser@domain.com` を持つがSIDとOIDの値が異なる重複ユーザーも存在する可能性があります。

問題: `username@duplicatesuffix.com` を使用して正しいバックエンドADアカウントを検索しようとしても、UPNのあいまいさのため、常に正しいADバックエンドユーザーが返されるとは限りません。Citrix CloudはどのADフォレストとCitrix Cloud Connectorを使用すべきかを判断できないため、ストアに誤ったDaaSリソースが表示されたり、DaaSリソースがまったく返されない場合があります。

解決策: 接続されたADフォレストごとに2つの異なるSAMLアプリケーションを構成し、SAMLアサーションに正しいADフォレストに対応するcip_domainとcip_forestの値を含めます。これによ

り、Citrix Cloudに追加のフォレストとドメインのコンテキストが提供され、`username@duplicatesuffix.com`が複数の接続されたフォレストに存在する場合に、正しいバックエンドADユーザーが「検索される」ことを保証します。

SAMLアプリ1 forestrootdomain1.com:



SAMLアプリ2 forestrootdomain2.com:

フォレストルートドメイン2(/en-us/citrix-cloud/media/forest-root-domain2.png)

正しいADバックエンドグループを使用して、2つのDaaSデリバリーグループを正しくマッピングします。

シナリオ2：子ドメインレベルで結合されたCloud Connectorと子ドメインレベルのストアユーザー

Citrix Cloudテナントには、推奨される「forestrootdomain.com」レベルではなく、「childdomain.forestrootdomain.com」レベルでドメイン参加している2つのCitrix Cloud Connectorを含むリソースロケーションがあります。ストアユーザーはchilddomain.forestrootdomain.com子ドメイン内に存在します。ユーザーは、`username@forestrootdomain.com`のようなルートドメインUPNサフィックスを使用するように構成されています。

問題: Citrix Cloudは、「forestrootdomain.com」を使用してADアカウントの検索を実行しますが、これは接続されたADドメインと一致しません。

解決策: SAMLアサーションで子ドメインコンテキストを指定して、ADアカウントユーザーが正しいAD子ドメインおよびフォレストコンテキストから「検索」されるようにします。

cip_forest = `forestrootdomain.com`

cip_domain = `childdomain.forestrootdomain.com`

属性とクレーム(/en-us/citrix-cloud/media/saml-app-different-domain-to-forest.png)

ストア認証用のSAMLプロバイダーとしてADFSを構成する

この記事では、SAMLを使用してストアまたはCitrix Cloudにサインインするために Citrix Cloud™ が必要とする証明書利用者信頼を構成する方法について説明します。

この記事の手順を完了すると、(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html)で説明されているように、ADFSサーバーとCitrix Cloud間のSAML接続を構成できます。SAML接続に正しいADFS値を入力するためのガイダンスについては、この記事の(#saml-configuration-in-citrix-cloud)を参照してください。

前提条件

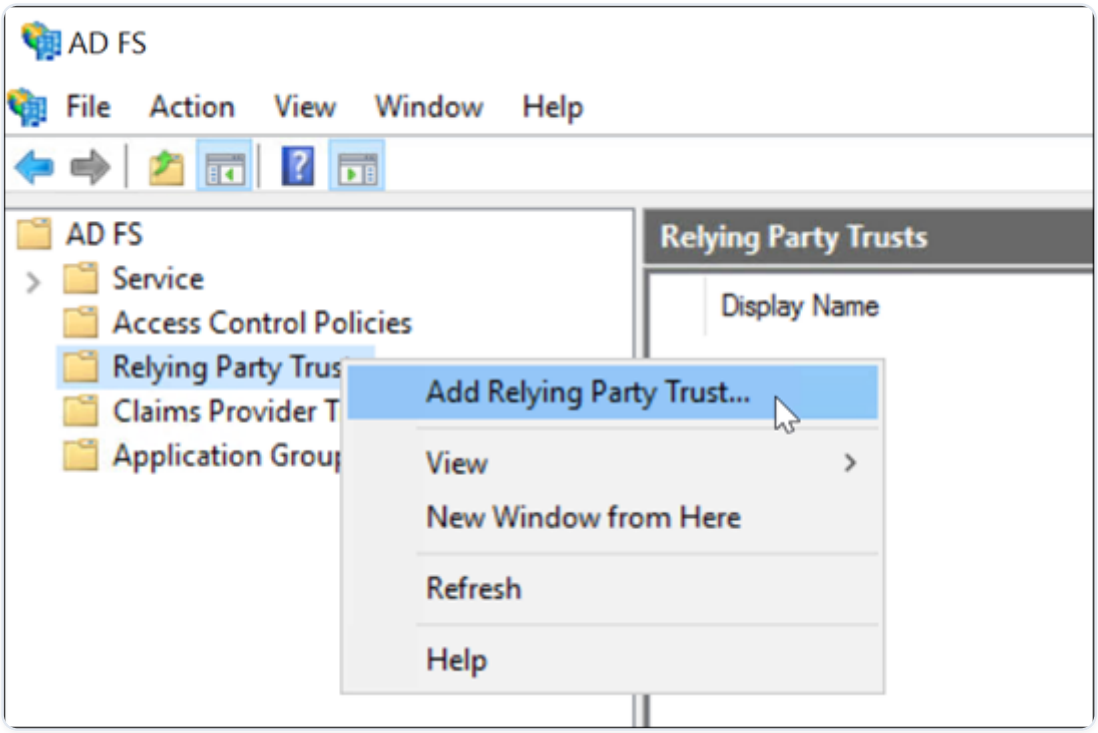
この記事の手順は、お客様の環境にCitrix FASを含む動作中のADFSサーバー展開があることを前提としています。セッション起動中にVDAへのシングルサインオンを提供するには、Citrix FASが必要です。

詳細については、次の記事を参照してください。

- Citrix FASドキュメント:
  - インストールと構成
  - ADFS展開
- Citrix Tech Zone: 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

Citrix Cloud用の証明書利用者信頼を構成する

1. AD FS管理コンソールから、左ペインの**AD FS**ノードを展開します。
2. **証明書利用者信頼**を右クリックし、**証明書利用者信頼の追加**を選択します。



証明書利用者信頼の追加ウィザードが表示されます。

3. 「**クレーム対応**」を選択し、「**次へ**」を選択します。

   クレーム対応オプションが選択されたADFS信頼ウィザード (/en-us/citrix-cloud/media/saml-adfs-trust-wizard-claims-aware-option.png)

4. 「**フェデレーションメタデータアドレス**」に`https://saml.cloud.com/saml/metadata.xml`と入力します。「**次へ**」を選択します。

   フェデレーションメタデータアドレスが入力されたADFS信頼ウィザード (/en-us/citrix-cloud/media/saml-adfs-trust-wizard-federation-metadata-address.png)

5. 表示名に`CitrixCloudProd`と入力します。「**次へ**」を選択します。

   表示名が入力されたADFS信頼ウィザード (/en-us/citrix-cloud/media/saml-adfs-trust-wizard-display-name.png)

6. アクセス制御ポリシーで、「**全員を許可**」を選択します。「**次へ**」を選択します。

   アクセス制御ポリシーが強調表示されたADFS信頼ウィザード (/en-us/citrix-cloud/media/saml-adfs-trust-wizard-access-control-policy.png)

7. 「**信頼の追加準備完了**」画面で、「**次へ**」を選択します。

8. 「**完了**」画面で、「**このアプリケーションのクレーム発行ポリシーを構成する**」を選択します。「**次へ**」を選択します。

   クレーム発行ポリシーの編集メニューオプションが選択されたADFSコンソール (/en-us/citrix-cloud/media/saml-adfs-edit-claim-issuance-policy.png)

9. 新しく作成した証明書利用者信頼を右クリックし、「**クレーム発行ポリシーの編集**」を選択します。
10. 「**ルールの追加**」をクリックし、「**LDAP属性をクレームとして送信**」を選択します。「**次へ**」を選択します。
11. 「**クレームルール名**」に`CitrixCloud`と入力します。
12. 「**属性ストア**」で、「**Active Directory**」を選択します。
13. 「**LDAP属性を送信要求タイプにマッピング**」の下で、以下のLDAP属性を、表示されているとおりに正確に追加します。

LDAP属性	送信要求タイプ
ユーザープリンシパル名	名前ID
ユーザープリンシパル名	cip_upn
表示名	displayName
名	givenName
姓	familyName

> **重要：**
>
> NameIDは常に、要求リストに追加される最初の要求である必要があります。そうしないと、シングルログアウト（SLO）が正しく機能しません。

> 構成されたクレームルール(/en-us/citrix-cloud/media/saml-adfs-edit-claim-issuance-rule-dialog.png)

14. **完了**を選択します。
15. 新しく作成された「CitrixCloudProd」という名前の証明書利用者信頼を右クリックし、プロパティを選択します。
16. **エンドポイント**タブを選択し、**SAMLの追加**をクリックします。
17. エンドポイントタイプのドロップダウンリストから**SAMLログアウト**を選択します。
18. バインディングのドロップダウンリストから**POST**を選択します。

19. 信頼されたURL: と応答URL: の両方に`https://saml.cloud.com/saml/logout/callback>`を入力します。

    SAMLエンドポイント(/en-us/citrix-cloud/media/saml-endpoint.png)

20. **OK**と**適用**をクリックします。

PowerShellを使用してCitrix Cloud証明書利用者信頼を変更する

ADFSサーバーを既定の「標準」構成で設定している場合、このセクションの手順に従って、Citrixが推奨する構成に適合するように更新できます。このタスクは、`nameidentifier`属性がクレームルールセットに含まれていないか、クレームルールセットの最初のSAML属性でない場合に、Citrix CloudまたはストアからのSAMLシングルログアウトが失敗する問題を解決するために必要です。

> **注:**
>
> この記事のCitrix Cloudの証明書利用者信頼を構成するの手順を使用してクレームルールセットを作成した場合、このタスクを実行する必要はありません。

> このタスクを完了するには、既存のルールセットをPowerShellを使用して新しいクレームルールセットに置き換えます。ADFS管理コンソールでは、この種の操作はサポートされていません。

1. ADFSサーバーでPowerShell ISEを見つけます。右クリックして**管理者として実行**を選択します。
2. 既存のADFSクレームルールをテキストファイルにバックアップします。

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudProd" | Select-Object
-ExpandProperty IssuanceTransformRules | Out-File
"$env:USERPROFILE\desktop\claimrulesbackup.txt"
```

3. Citrixが提供するclaimrules.txtファイルをこちらからダウンロードします。
4. claimrules.txtファイルをデスクトップにコピーします。
5. claimrules.txtファイルを使用して、必要なクレームルールをインポートします。

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `

                      -MetadataUrl "https://saml.cloud.com/saml/
metadata" `

                      -AutoUpdateEnabled $True `

                      -IssuanceTransformRulesFile
"$env:USERPROFILE\desktop\claimrules.txt" `

                      -SignedSamlRequestsRequired $True `

                      -SamlResponseSignature "MessageAndAssertion" `

                      -Enabled $True
```

PowerShellを使用して、証明書利用者信頼のSAML署名設定を更新する

デフォルトでは、ADFS証明書利用者信頼には次の設定があります。

- EncryptClaims: 真
- SignedSamlRequestsRequired: 偽
- SamlResponseSignature: AssertionOnly

セキュリティを強化するため、Citrixではシングルサインオン (SSO) とシングルログアウトの両方に署名付きSAML要求を使用することを推奨しています。このセクションでは、PowerShellを使用して既存の証明書利用者信頼の署名設定をCitrix推奨構成に適合するように更新する方法について説明します。

1. ADFSサーバーで現在のRelyingPartyTrust構成を取得します。

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
```

2. **CitrixCloudProd**証明書利用者信頼設定を更新します。

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `

                      -SignedSamlRequestsRequired $True `

                      -SamlResponseSignature "MessageAndAssertion"
```

Citrix CloudでのSAML構成

Citrix CloudでSAML接続を構成する際（(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html#add-saml-provider-metadata-to-citrix-cloud)で説明）、ADFSの値を次のように入力します。

Identity and Access Management > Authentication > Add an identity provider > SAML内のSAML接続には、デフォルトの推奨値を使用します。

CITRIX CLOUD のこのフィールドで	この値を入力します
エンティティID	`https://adfs.YourDomain.com/adfs/services/trust`。ここで `YourDomain.com` は ADFS サーバーのドメインです。
認証要求に署名	はい
SSOサービスURL	`https://adfs.YourDomain.com/adfs/ls`。ここで `YourDomain.com` は ADFS サーバーのドメインです。
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、正確
ログアウトURL	`https://adfs.YourDomain.com/adfs/ls`。ここで、`YourDomain.com`はお使いのADFSサーバーのドメインです。
ログアウト要求に署名	はい
SLOバインディングメカニズム	HTTP ポスト

MMC ADFS管理コンソール内からADFS署名証明書をエクスポートします。SAML接続内でCitrix Cloudにアップロードする3つの証明書のうち、どれが正しいものかについては、以下のスクリーンショットを参照してください。

ADFSのエクスポート(/en-us/citrix-cloud/media/export-adfs.png)

ストア認証用のSAMLプロバイダーとしてDuoを構成する

この記事では、Duo SAMLアプリケーションと、Citrix Cloud™とSAMLプロバイダー間のSAML接続を構成するために必要な手順について説明します。これらの手順の一部は、Duo SAMLプロバイダーの管理コンソールで実行するアクションについて説明しています。

前提条件

この記事のタスクを完了する前に、以下の前提条件を満たしていることを確認してください。

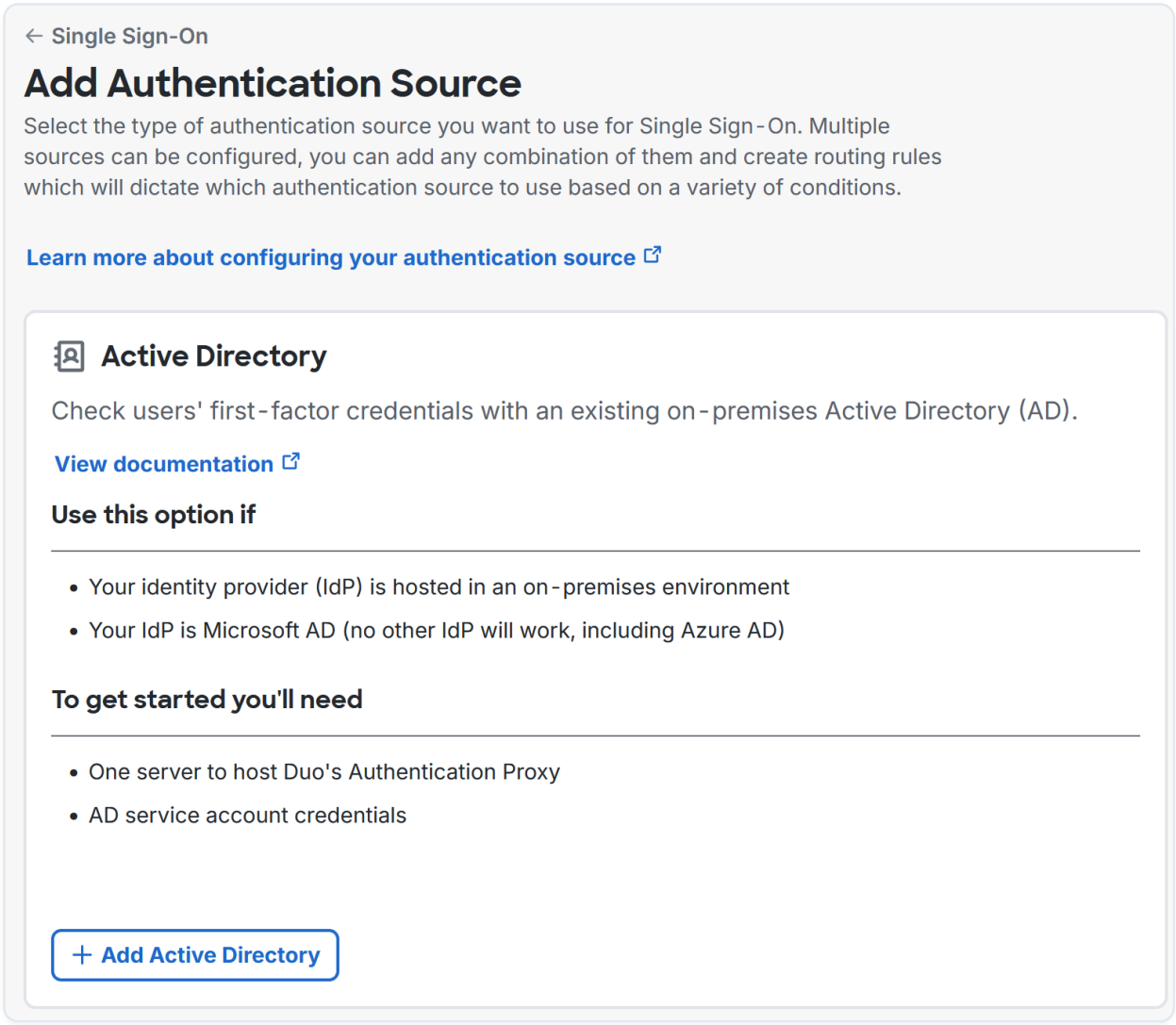
- Duoクラウドテナント。
- ADフォレスト内のDuo認証プロキシ。
- ADユーザーをDuoに同期するActive Directory LDAPS接続。

Active DirectoryのDuoテナントへの同期を構成する

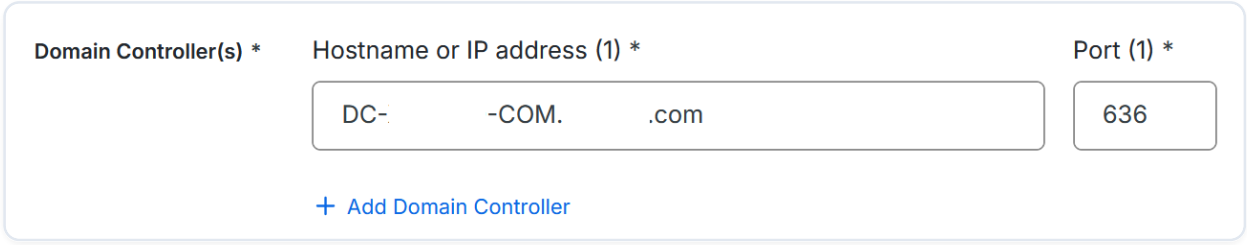
オンプレミスADをDuoに接続し、SAMLユーザーをインポートするに関するDuoのドキュメントに従ってください。

Active Directory LDAPS接続を作成する

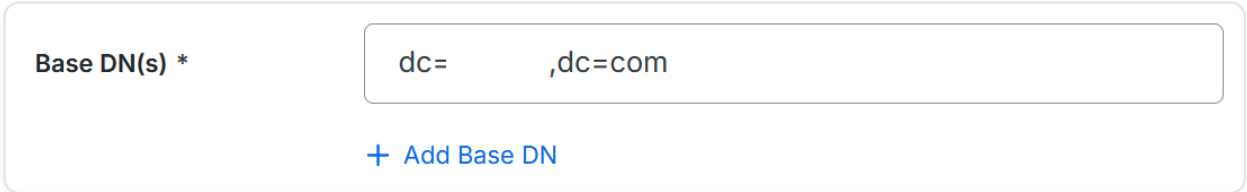
1. **アプリケーション > SSO設定 > ソースの追加 > Active Directory > Active Directoryの追加** を選択します。



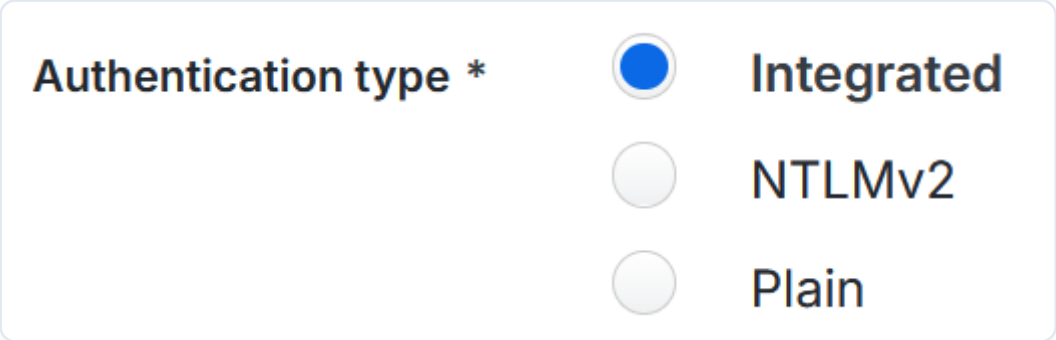
2. ADフォレストへのLDAPS接続の表示名を入力します。
3. ドメインコントローラーのFQDNを入力します。



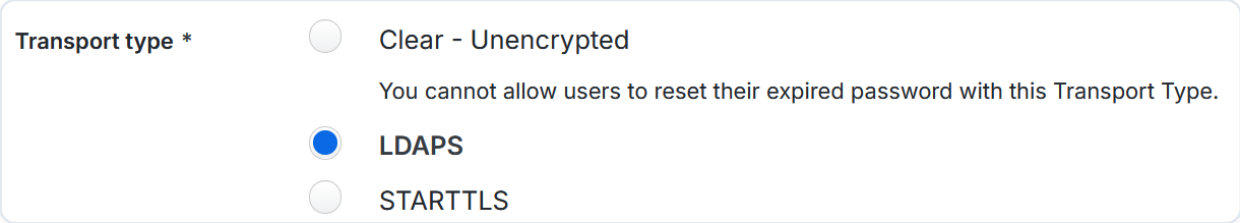
4. ADドメインのBase DNを設定します。



5. 認証タイプとしてIntegratedを選択します。



6. トランスポートタイプとしてLDAPSを選択します。



7. SSL Verify Hostnameのチェックボックスをオンにします。
8. ドメインコントローラー証明書と、ドメイン証明書の署名に使用されたプライベートエンタープライズ証明機関CA証明書の両方を入力します。
9. 次の例に従ってPEM形式の証明書を入力します。

```
-----BEGIN CERTIFICATE-----

`<base64 Domain Controller Certificate>`

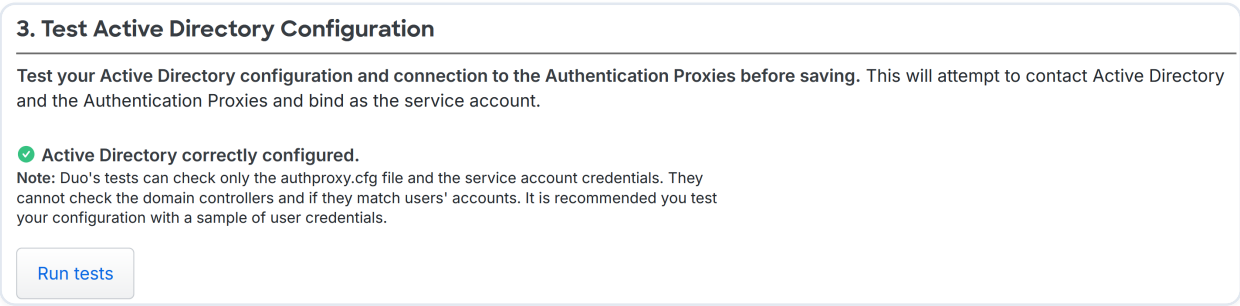
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

`<base64 Certificate Authority Certificate used to sign the Domain
Controller Certificate above>`

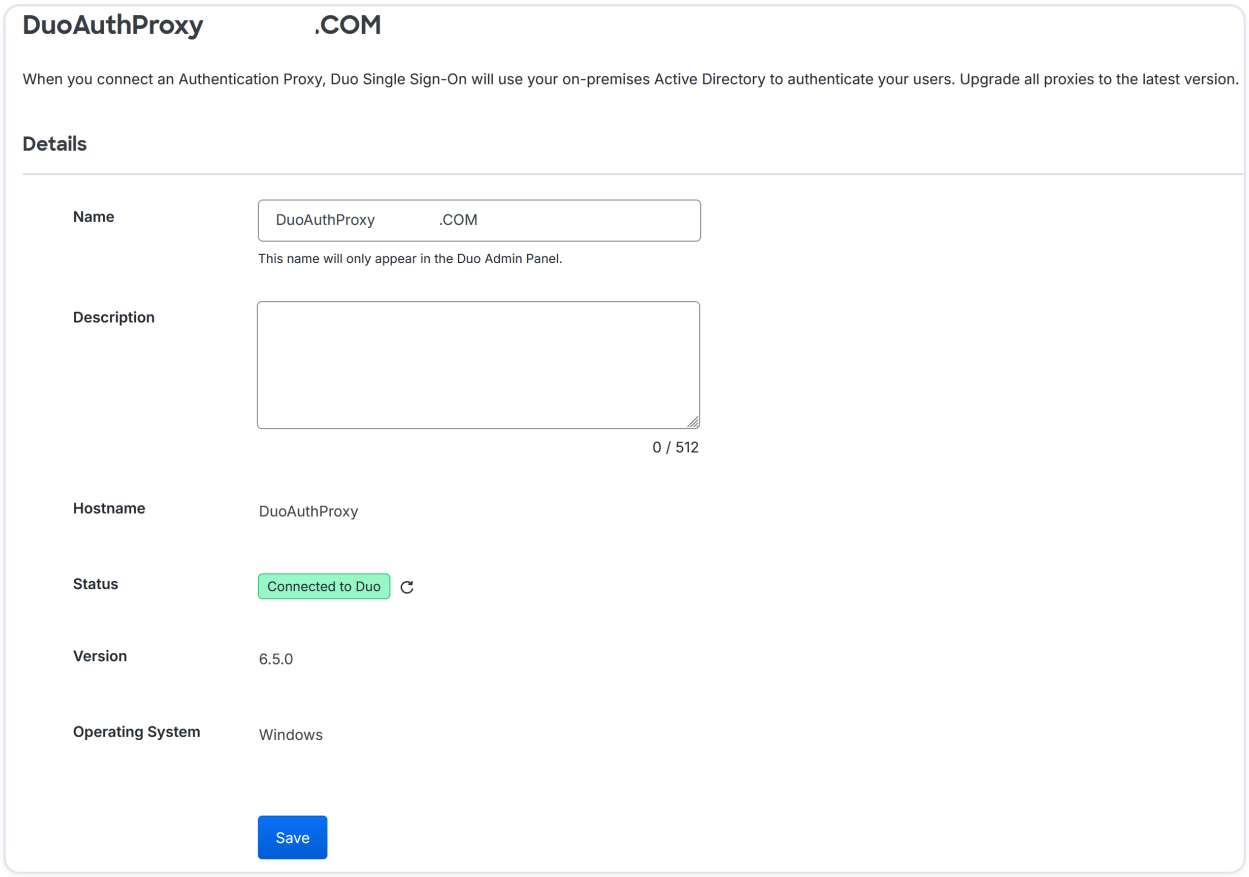
-----END CERTIFICATE-----
```

10. LDAPS接続をテストします。

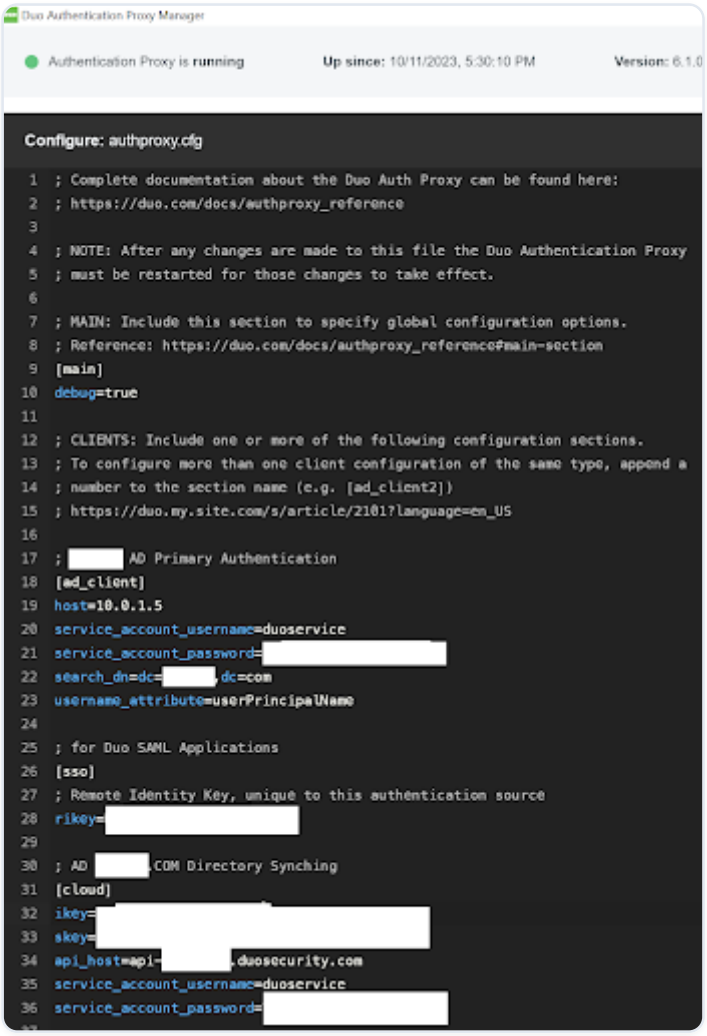


SAML用にDuo認証プロキシ設定ファイルを設定します

1. Duo Auth Proxy構成が正常であり、**Duoに接続済み**と表示されていることを確認します。

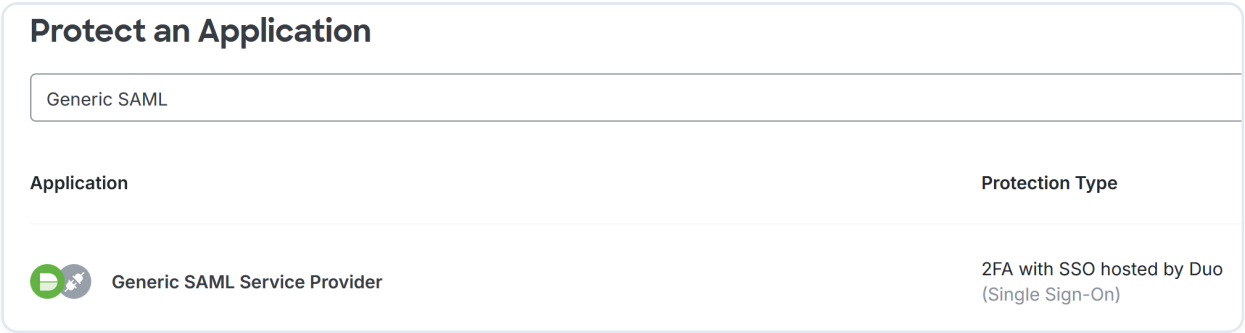


2. Duo認証プロキシにログインし、Duo管理コンソールから提供される**リモートID (rikey)**を使用して、その設定ファイルにSAML セクションを追加します。Duo Authentication Proxyは、Duoクラウドサービスと通信するために共有シークレットを使用します。このシークレットは、Authentication Proxyの初期インストールまたは構成中に生成されます。



ストアで使用するためのDuo SAMLアプリケーションを構成する

1. **アプリケーション > アプリケーションを保護**を選択します。**アプリケーションの追加**をクリックします。
2. 汎用SAMLサービスプロバイダーDuoアプリテンプレートのエントリを見つけます。Citrix®は、汎用SAMLサービスプロバイダーDuoテンプレートを推奨しています。これは最も柔軟性があり、ニーズに応じてSAML属性のさまざまな組み合わせやSAMLフローを構成できるためです。



> **重要:**

> Duo **Citrix Workspace** SAMLテンプレートの使用は推奨されません。これは柔軟性がなく、AD IDを使用したSAMLのみをサポートするためです。また、Duo **Citrix Workspace** SAMLテンプレートでは、一部の高度なM&A (合併・買収) SAML構成に必要となるcip_domainやcip_forestのようなオプション属性の追加も許可されません。Citrix Cloudのログアウトエンドポイントの構成も許可されません。

3. SAMLアプリケーションの**表示名**を、**Citrix Cloud Prod**などのように指定します。
4. **すべてのユーザーに対して有効にする**などの**ユーザーアクセス**を指定します。
5. **メタデータ検出**内で**なし (手動入力)**を選択し、以下のCitrix Cloud SAMLエンドポイントを入力します。
6. CCテナントが存在するCitrix Cloudリージョンに従って、**EntityID**を入力します。

URL	リージョン
`https://saml.cloud.com`	商用EU、米国、およびAPS
`https://saml.citrixcloud.jp`	JP
`https://saml.cloud.us`	GOV

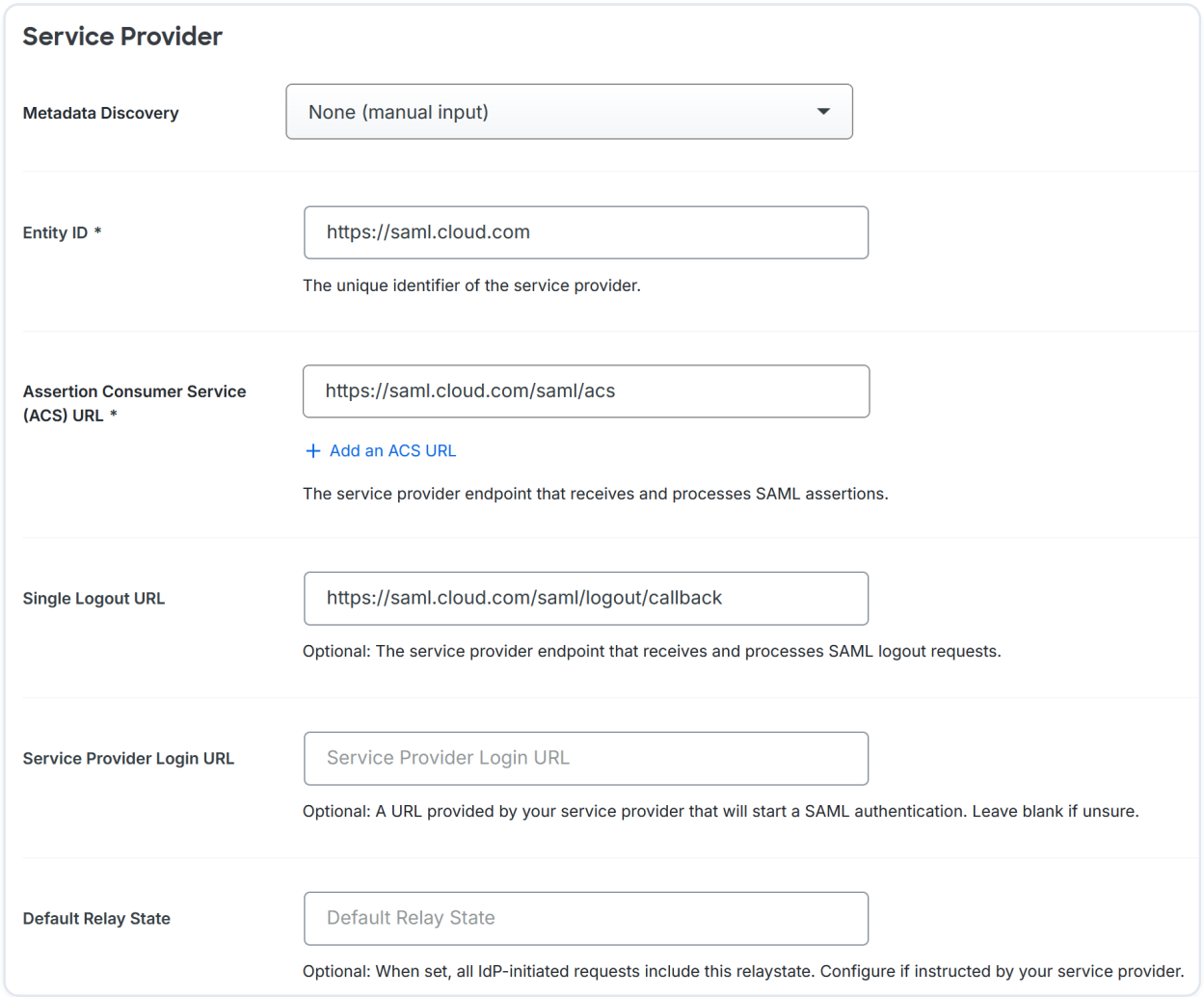
7. CCテナントが存在するCitrix Cloudリージョンに応じて、**シングルサインオンURL (ACS URL)**を構成します。

URL	リージョン
`https://saml.cloud.com/saml/acs`	商用 EU、米国、および APS
`https://saml.citrixcloud.jp/saml/acs`	JP
`https://saml.cloud.us/saml/acs`	GOV

8. CCテナントが存在するCitrix Cloudリージョンに応じて、**シングルログアウトURL** を構成します。

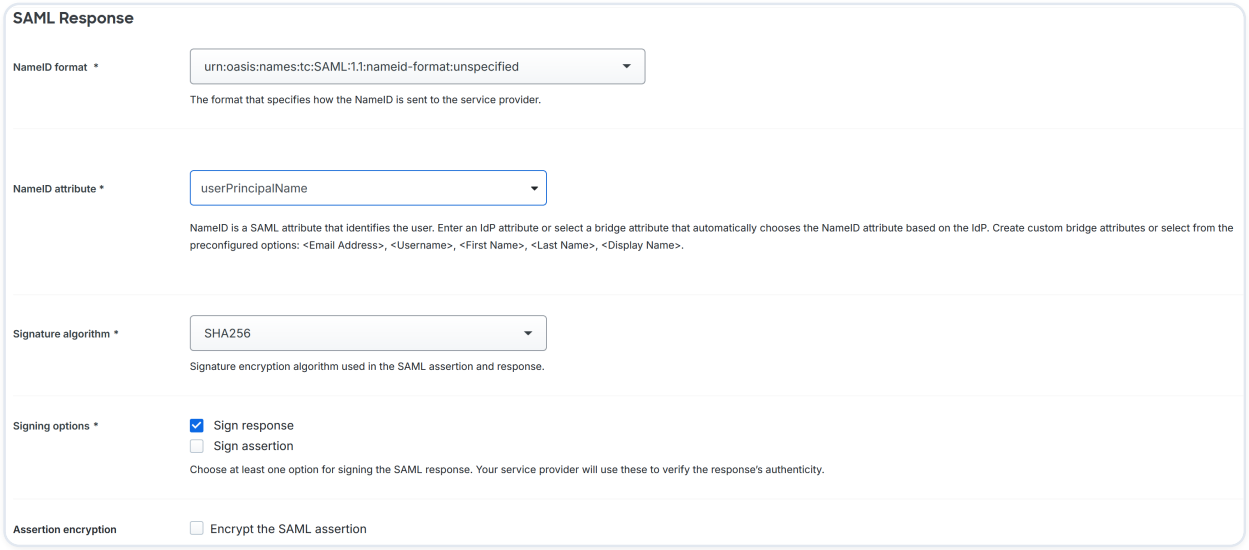
URL	リージョン
`https://saml.cloud.com/saml/logout/callback`	商用 EU、米国、および APS
`https://saml.citrixcloud.jp/samllogout/callback`	JP
`https://saml.cloud.us/saml/samllogout/callback`	GOV

9. **サービスプロバイダーログインURL** は必須ではなく、空　のままで構いません。
10. **デフォルトリレーステート** は必須ではなく、空　のままで構いません。

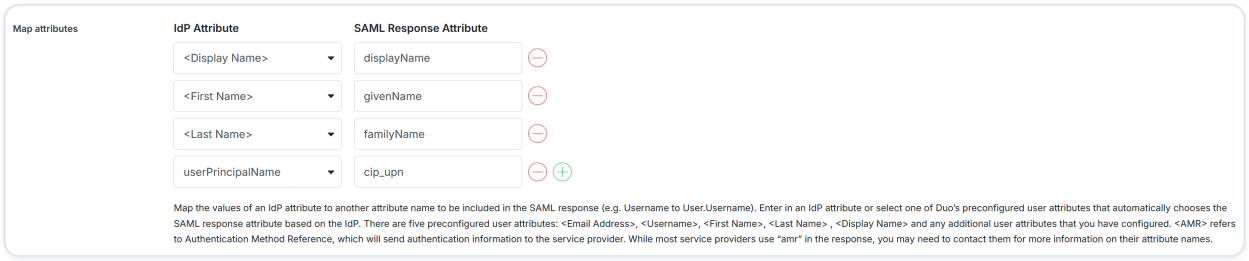


11. **名前ID形式** を **未指定** に構成します。
12. **名前ID属性** を **userPrincipalName** (大文字と小文字を区別) に構成します。
13. **署名アルゴリズム** を **SHA256** に構成します。

14. **署名オプション** を **応答に署名** に構成します。
15. **アサーション暗号化** を **無効** に構成します。



16. 左側にDuoブリッジ属性、右側にCitrix Cloud SAMLクレーム名を使用して、**属性のマップ**を設定します。



> **重要:**
>
> Duoブリッジ属性（左）とSAML属性クレーム名（右）は、大文字と小文字を区別します。Citrix Cloud SAML接続内で構成されているものと一致する必要があるのは、右側のクレーム名です。

Citrix Cloud SAML接続を構成する

1. すべてのCitrixログオンフローは、ストアURLまたはCitrix Cloud GO URLのいずれかを使用して、サービスプロバイダーによって開始される必要があります。
2. **IDおよびアクセス管理 > 認証 > IDプロバイダーの追加 > SAML**内のSAML接続には、デフォルトの推奨値を使用します。
3. Duo Active Directory Sync documentationにアクセスして、DuoポータルからCitrix Cloud SAML接続に入力するDuo SAMLアプリケーションのSAMLエンドポイントを取得します。

CITRIX CLOUD™



CITRIX CLOUDのこのフィールド	この値を入力します
エンティティID	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/metadata`
認証要求に署名	はい
SSOサービスURL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/sso`
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、正確
ログアウトURL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/slo`
ログアウトリクエストに署名	はい
SLOバインディングメカニズム	HTTP ポスト

Duo SAML ログアウトの動作

この記事の執筆時点では、Duo SAML は SAML SLO をサポートしていませんが、ユーザーがストアやCitrix Cloudから明示的にログアウトしたときに、Duo が IDP セッションを終了するように構成することは可能です。Duo SAML アプリケーションのログアウト設定を構成する前に、メインの SAML 記事にある「SAML ログアウトに関する考慮事項」セクションsaml logout considerationsを読むことをお勧めします。

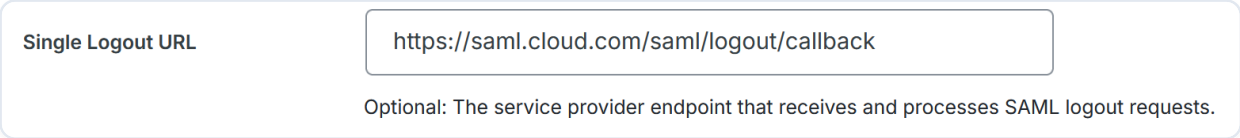
重要:

Duo のドキュメントDuo SSO Logout Behavior and Session Management Detailsから引用。

`Users that decide to log out and hit the SLO URL for Duo SSO will be logged out of Duo SSO and have their MFA remembered devices session deleted before redirecting them to the logout page`.

エンドユーザーがストアやCitrix Cloudからログアウトしたときに、Duo IDPセッションの明示的なログアウトを構成するには、以下の推奨手順に従ってください。

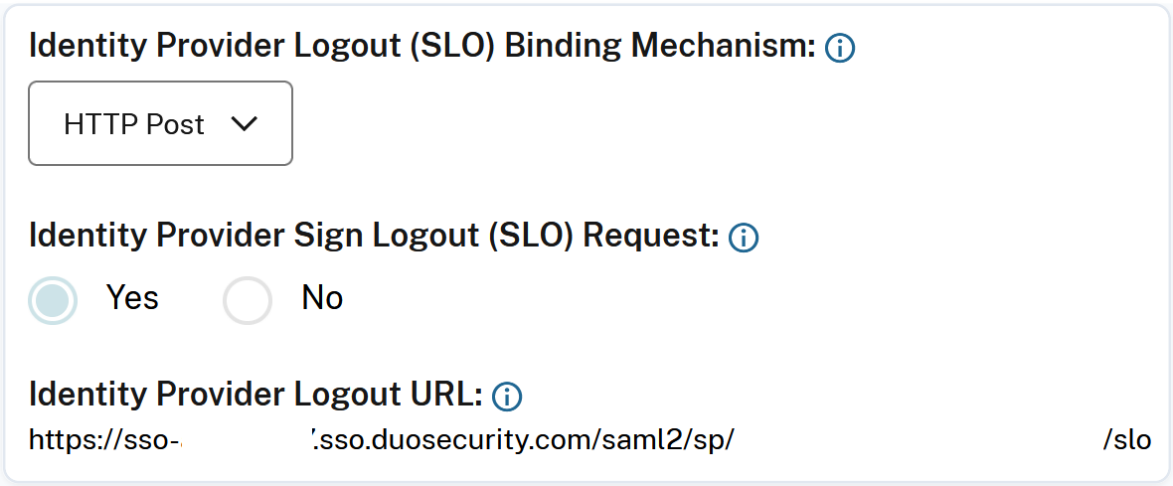
1. Duo SAML アプリ内で Citrix Cloud SAML ログアウトエンドポイントを構成します。



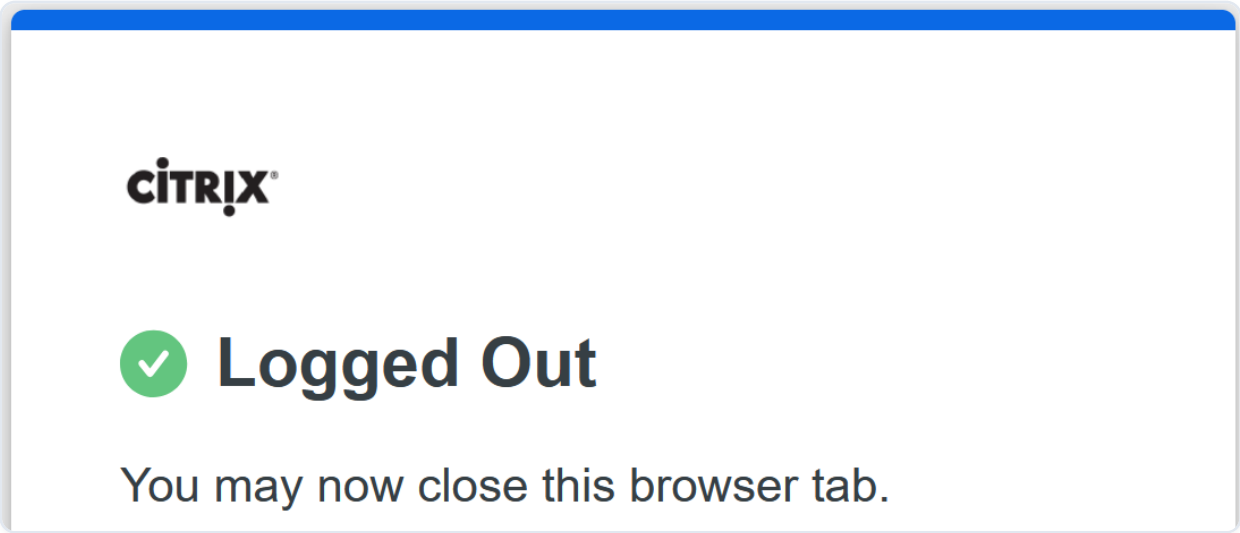
2. Citrix Cloud SAML 接続内で Duo SLO エンドポイントを構成します。

重要:

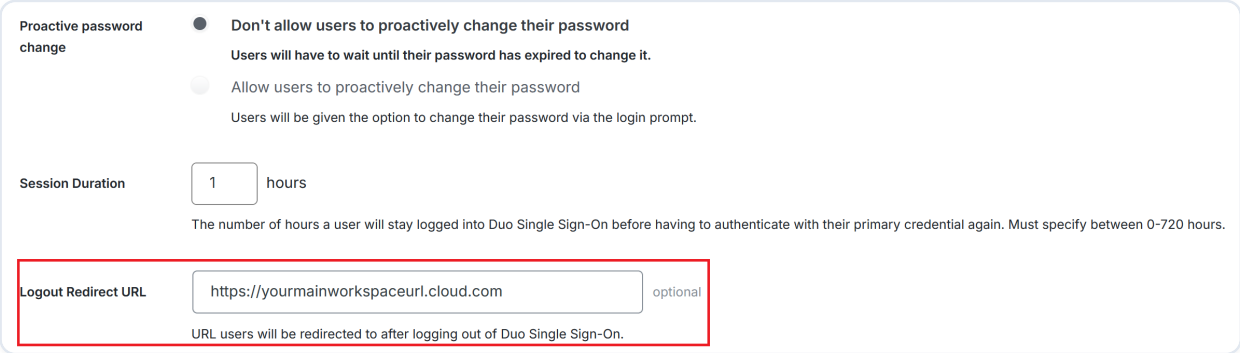
Generic SAML Provider Duo アプリテンプレートを使用していない場合、Citrix Cloud ログアウトエンドポイントを入力するオプションが利用できないため、この手順を完了することはできません。



3. ステップ 1 および 2 に従って SAML 接続の両側でログアウトが構成されている状態でストアからログアウトすると、Duo によって IDP セッションが終了したことを示す以下の UI が表示されます。



4. **オプション**: ストアのエンドユーザーのログアウトエクスペリエンスを向上させるために、Duo LDAPS 接続を単一の **Logout Redirect URL** で構成し、エンドユーザーをストアのログオンページにリダイレクトさせることが可能です。これは、AD フォレストの LDAPS 接続内で行われます。



> **重要：**
>
> 上記に示されているログアウトのリダイレクトURLフィールドでは、単一のストアURLのみを構成できます。Citrix Cloudテナント内で複数の異なるストアURLを使用する場合、Duoの単一のActive Directoryフォレスト接続内で構成することはできません。

ストア認証のためのEntra IDとAD IDを使用したSAML

本記事では、Active Directory (AD) IDを使用してストア認証のためのSAMLを構成する方法について説明します。Citrix Cloud™およびクラウドストアまたは Citrix CloudへのSAML認証のデフォル

トの動作は、使用されるSAMLプロバイダーに関係なく、ADユーザーIDに対してアサートすることです。本記事で説明する構成では、Entra ID Connectを使用してAD IDをEntra IDにインポートする必要があります。

> **重要:**

> エンドユーザーにとって適切なSAMLフローを決定することは、サインインプロセスとリソースの可視性に直接影響するため、非常に重要です。選択されたIDは、ストアのエンドユーザーがアクセスできるリソースの種類に影響を与えます。 ME-ID IDを使用してストアに認証するためのSAMLプロバイダーとしてEntra IDを利用する方法に関する指示を提供する関連記事があります。詳細な手順については、Microsoft Entra IDとME-ID IDを使用したストア認証のためのSAMLを参照してください。 通常、エンドユーザーはADドメイン参加済みVDAによって提供されるアプリやデスクトップを開く必要があります。組織にとって最適なSAMLフローを決定する前に、両方の記事で概説されているユースケースを慎重に確認することが不可欠です。不明な点がある場合は、Citrix®は最も一般的なDaaSシナリオと一致するため、**AD SAMLフロー**を使用し、本記事の指示に従うことを推奨します。

機能範囲

本記事は、Citrix CloudとAzureの以下の機能の組み合わせを使用するユーザーに適用されます。

- AD IDを使用したストア認証のためのSAML
- AD IDを使用したCitrix Cloud管理者ログインのためのSAML
- ADドメイン参加済みVDAを使用して公開されたリソースのCitrix DaaS™およびHDXリソース列挙
- ADドメイン参加済みVDAリソース列挙

AD IDとEntra ID、どちらが最適か?

ストアユーザーがSAML ADまたはSAML Entra IDのどちらのIDを使用して認証すべきかを判断するには：

1. ストアでユーザーに提供するリソースの組み合わせを決定します。
2. 以下の表を使用して、各リソースタイプに適したユーザーIDの種類を決定します。

リソースタイプ (VDA)	ストアにサインインする際のユーザーID	ENTRA ID を使用した SAML ID が必要ですか？	FAS は VDA へのシングルサインオン (SSO) を提供しますか？
AD参加済み	AD、ADからインポートされたEntra ID (SIDを含む)	いいえ。デフォルトのSAMLを使用します。	はい

カスタムのEntra IDエンタープライズSAMLアプリケーションを構成する

デフォルトでは、ストアへのSAMLサインインの動作は、ADユーザーIDに対してアサートすることです。

1. Azureポータルにサインインします。
2. ポータルメニューから、**Entra ID**を選択します。
3. 左ペインの**管理**の下で、**エンタープライズアプリケーション**を選択します。
4. 作業ペインのコマンドバーから、**新しいアプリケーション**を選択します。
5. コマンドバーから、**独自のアプリケーションを作成**を選択します。Citrix Cloud SAML SSOエンタープライズアプリケーションテンプレートは使用しないでください。このテンプレートでは、クレームとSAML属性のリストを変更できません。
6. アプリケーションの名前を入力し、**ギャラリーで見つからないその他のアプリケーションを統合 (非ギャラリー)** を選択します。**作成**をクリックします。アプリケーションの概要ページが表示されます。
7. 左ペインから、**シングルサインオン**を選択します。作業ペインから、**SAML**を選択します。
8. **基本的なSAML構成**セクションで、**編集**を選択し、次の設定を構成します。

    a. **識別子 (エンティティID)** セクションで、**識別子の追加**を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

    - 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com`を入力します。
    - 日本リージョンの場合は、`https://saml.citrixcloud.jp`を入力します。
    - Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us`を入力します。

b. **応答URL (アサーションコンシューマーサービスURL)** セクションで、**応答URLの追加**を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

- 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/acs`を入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/acs`を入力します。
- Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us/saml/acs`を入力します。

c. **ログアウトURL (オプション)** セクションで、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

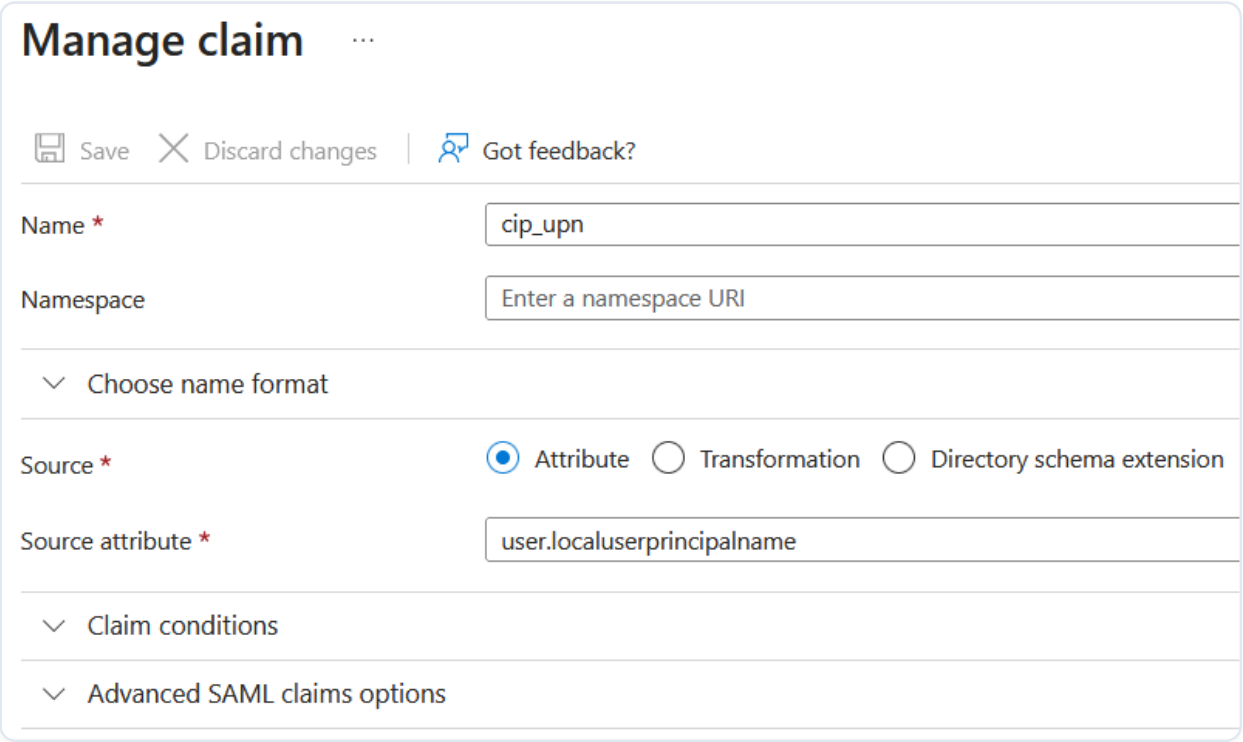
- 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/logout/callback`を入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/logout/callback`を入力します。
- Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us/saml/logout/callback`を入力します。

d. コマンドバーから、**保存**を選択します。

9. 「**属性とクレーム**」セクションで、「**編集**」をクリックして、次のクレームを構成します。これらのクレームは、SAML応答内のSAMLアサーションに表示されます。SAMLアプリの作成後、次の属性を構成します。

a. 「**一意のユーザー識別子 (Name ID)**」クレームの場合、デフォルト値を`user.localuserprincipalname`に更新します。

b. 「**cip_upn**」クレームの場合、デフォルト値を`user.localuserprincipalname`に更新します。



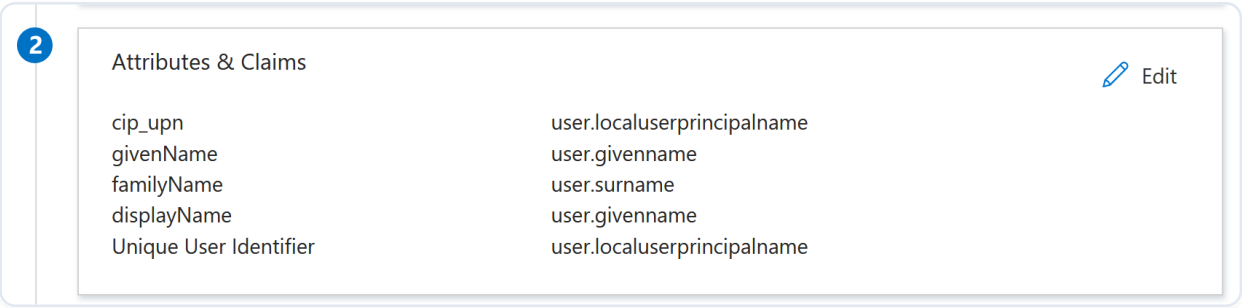
a. 「**displayName**」の場合、デフォルト値の`user.displayname`をそのままにします。

b. 「**givenName**」クレームの場合、デフォルト値を`user.givenname`に更新します。

c. 「**familyName**」クレームの場合、デフォルト値を`user.surname`に更新します。

d. 「**追加のクレーム**」セクションで、`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`名前空間を持つ残りのクレームについては、省略記号 (...) ボタンをクリックし、「**削除**」をクリックします。これらのクレームは上記のユーザー属性の重複であるため、含める必要はありません。

完了すると、「**属性とクレーム**」セクションは次のように表示されます。

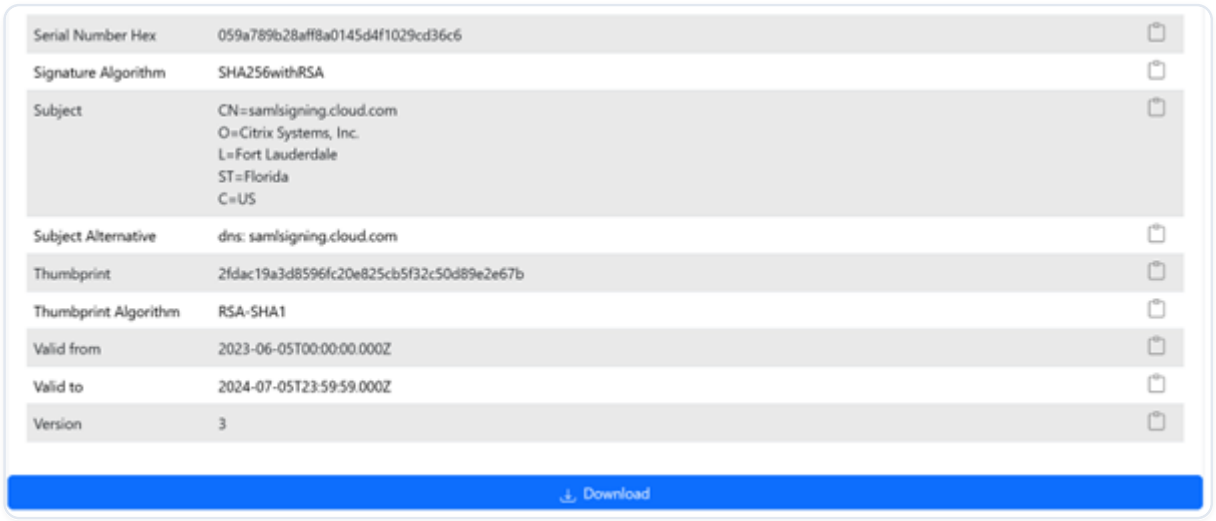


10. このサードパーティのオンラインツールを使用して、Citrix Cloud SAML署名証明書のコピーを取得します。

a. URLフィールドに`https://saml.cloud.com/saml/metadata`と入力し、「**読み込み**」をクリックします。



a. ページの下部までスクロールし、「**ダウンロード**」をクリックします。



「証明書のダウンロード」(/en-us/citrix-cloud/media/certificate_download.png)

11. Entra ID SAMLアプリケーションの署名設定を構成します。

    a. ステップ9で取得した本番SAML署名証明書をEntra ID SAMLアプリケーション内にアップロードします。

    b. **検証証明書を要求する**を有効にします。

「検証証明書」(/en-us/citrix-cloud/media/verification_cert.png)

「検証証明書」(/en-us/citrix-cloud/media/saml_certificate.png)

トラブルシューティング

1. SAML-tracerブラウザ拡張機能などのSAMLネットワークツールを使用して、SAMLアサーションに正しいユーザー属性が含まれていることを確認します。

「SAML-tracerブラウザ拡張機能」(/en-us/citrix-cloud/media/saml-tracer-browser-ext.png)

1. 黄色で表示されているSAML応答を見つけ、この例と比較します。

   「ネットワークツールからのSAML応答の例」(/en-us/citrix-cloud/media/saml-idp-aad-saml-tool-response.png)

2. 下部ペインの**SAML**タブをクリックして、SAML応答をデコードし、XMLとして表示します。
3. 応答の最後までスクロールし、SAMLアサーションに正しいSAML属性とユーザー値が含まれていることを確認します。

   「SAMLアサーション値が強調表示されたXMLファイル」(/en-us/citrix-cloud/media/saml-idp-aad-assertion-values.png)

エンドユーザーがストアにサインインできない場合、またはCitrix HDX™ Plus for Windows 365デスクトップが表示されない場合は、Citrixサポートに連絡して次の情報を提供してください。

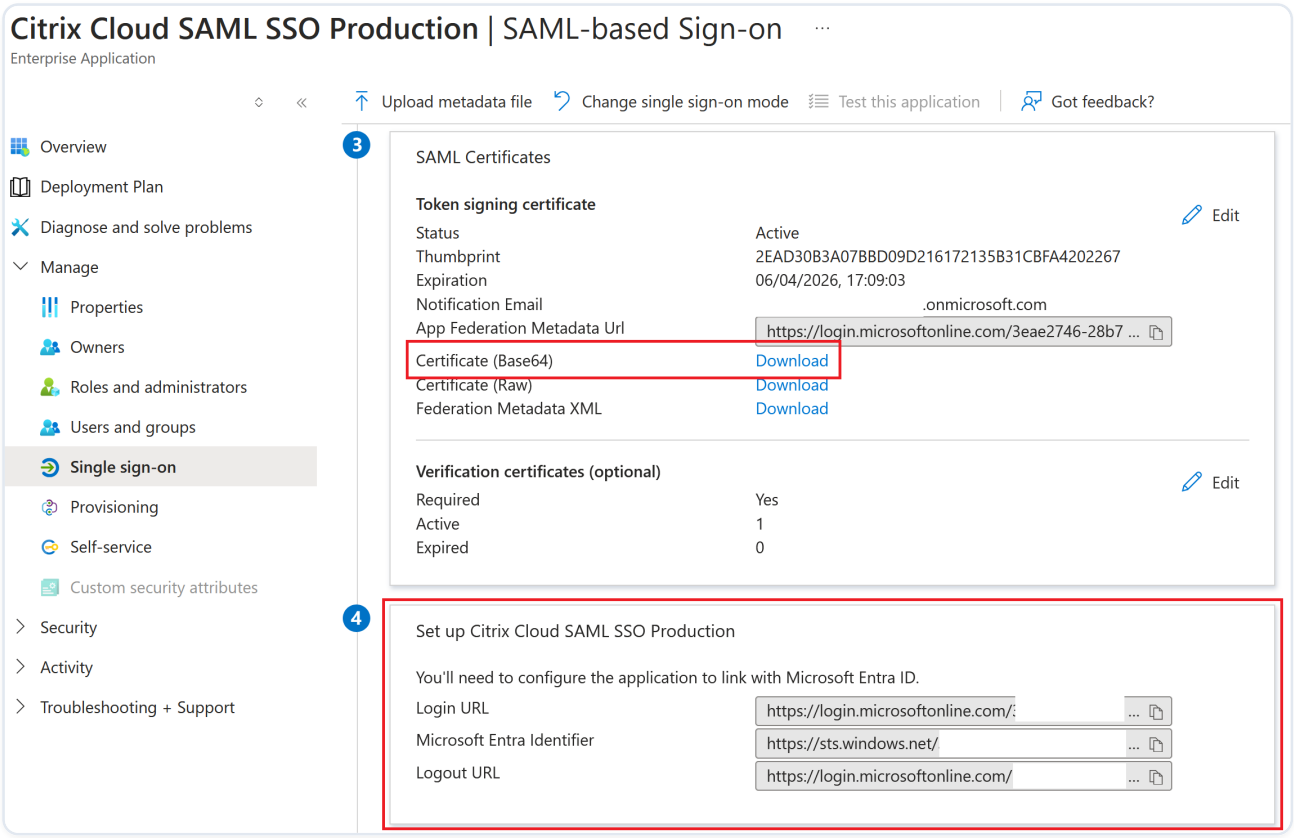
- SAMLトレーサーキャプチャ
- Citrix® StoreFront Cloudへのサインインが失敗した日時
- 影響を受けるユーザー名
- ストアへのサインインに使用したクライアントコンピューターの呼び出し元IPアドレス。このIPアドレスを取得するには、https://whatismyip.comのようなツールを使用できます。

Citrix Cloud SAML接続を構成する

すべてのCitrixログオンフローは、ストアURLまたはCitrix Cloud GO URLのいずれかを使用して、サービスプロバイダーによって開始される必要があります。

> > > 内のSAML接続には、デフォルトの推奨値を使用します。

Citrix Cloudに入力するために、Entra IDポータルからEntra ID SAMLアプリケーションのSAMLエンドポイントを取得します。



Citrix Cloud SAML接続内で使用されるEntra ID SAMLエンドポイントの例

> **重要：**
>
> EntraID SSOおよびログアウトSAMLエンドポイントは同じURLです。

CITRIX CLOUDのこのフィールド	この値を入力します
エンティティID	`https://sts.windows.net/<yourEntraIDTenantID>`
認証リクエストに署名	はい
SSOサービスURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名

CITRIX CLOUDのこのフィールド	この値を入力します
認証コンテキスト	未指定、正確
ログアウトURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
ログアウトリクエストに署名	はい
SLO バインディングメカニズム	HTTP ポスト

ストア認証にEntra IDとEntra ID IDを使用するSAML

この記事では、AD IDの代わりにEntra ID IDを使用してストア認証用のSAMLを構成する方法について説明します。デフォルトのSAML動作でストアにサインインした後、Entra IDユーザーがWindows 365 Cloud PCまたはEntra IDドメイン参加済みVDAを列挙できない場合に、この構成を使用してください。構成が完了すると、ユーザーはSAML認証を使用してストアにサインインし、Citrix DaaS™を介したHDXアプリとデスクトップ、およびAzureを介したWindows 365 Cloud PCの両方にアクセスできるようになります。

Citrix Cloud™およびCitrix® StoreFront CloudへのSAML認証のデフォルトの動作は、ADユーザーIDに対してアサートすることです。この記事で説明されている構成では、Entra ID Connectを使用してAD IDをEntra IDにインポートする必要があります。AD IDにはユーザーのSIDが含まれており、StoreFront CloudはこれをCitrix DaaSに送信して、HDXリソースの列挙と起動を可能にします。ユーザーのIDのEntra IDバージョンが使用されるため、ユーザーはStoreFront Cloud内からWindows 365 Cloud PCなどのAzureリソースを列挙および起動することもできます。

重要:

列挙とは、ユーザーがストアにサインインした後に表示されるリソースのリストを指します。特定のユーザーがアクセスを許可されているリソースは、そのユーザーIDと、Citrix DaaSでそのIDに関連付けられているリソースによって異なります。ストアへの認証のためのSAMLプロバイダーとしてEntra IDとAD IDを利用する方法に関する手順を提供する関連記事があります。詳細な手順については、ストア認証にEntra IDとAD IDを使用するSAMLを参照してください。

機能の範囲

この記事は、Citrix CloudとAzureの以下の機能の組み合わせを使用するユーザーに適用されます。

- ストア認証用のSAML
- ADドメイン参加済みVDAを使用して公開されたリソースのCitrix DaaSおよびHDX™リソース列挙
- Entra IDドメイン参加済みVDAリソース列挙
- Azureハイブリッドドメイン参加済みVDAリソース列挙
- W365 Cloud PCの列挙と起動

> **重要:**

> Citrix CloudへのSAMLログインには、このME-ID SAMLフローを使用しないでください。これは、Citrix Cloud管理者ユーザーがADグループのメンバーである必要があり、したがってADユーザーIDを使用する必要があるためです。詳細な手順については、ストア認証にEntra IDとAD IDを使用するSAMLを参照してください。

どちらが最適か：AD IDかEntra ID IDか?

ストアユーザーがSAML ADまたはSAML Entra IDのどちらのIDを使用して認証すべきかを判断するには、:

1. ストアでユーザーに提供するリソースの組み合わせを決定します。
2. 以下の表を使用して、各リソースタイプに適したユーザーIDのタイプを判断します。

リソースタイプ (VDA)	ストアにサインインする際のユーザーID	ENTRA ID を使用した SAML ID が必要ですか？	FAS は VDA へのシングルサインオン (SSO) を提供しますか？
AD参加済み	AD、ADからインポートされたEntra ID (SIDを含む)	いいえ。デフォルトのSAMLを使用します。	はい
ハイブリッド参加済み	AD、ADからインポートされたEntra ID (SIDを含む)	いいえ。デフォルトのSAMLを使用します。	はい、IDプロバイダーとしてのADの場合。VDAにEntra IDが選択されている

リソースタイプ (VDA)	ストアにサインインする際のユーザーID	ENTRA ID を使用した SAML ID が必要ですか？	FAS は VDA へのシングルサインオン (SSO) を提供しますか？
			場合、FASは不要です。
Entra参加済み	Entra IDネイティブユーザー、ADからインポートされたEntra ID (SIDを含む)	はい、Entra ID経由でSAMLを使用します。	いいえ
Windows 365 クラウド PC	Entra IDネイティブユーザー、ADからインポートされたEntra ID (SIDを含む)	はい、Entra ID経由でSAMLを使用します。	いいえ
AD参加済み、Entra ID参加済み、Windows 365 Cloud PC	ADからインポートされたEntra ID (SIDを含む)	はい、Entra ID経由でSAMLを使用します。	はい、AD参加済みの場合。いいえ、Entra ID参加済みおよびWindows 365 Cloud PCの場合。

詳細情報

- Citrix DaaSドキュメント:
  - マシンID
  - シトリックス HDX Plus for Windows 365
- Citrix FASドキュメント: 「インストールと構成」(/ja-jp/federated-authentication-service/current-release/install-configure.html)
- Microsoft Azureドキュメント: Entra ID Connectとは

要件

- Entra IDテナントはCitrix Cloudテナントに接続されている必要があります。Citrix Cloudコンソールで、 > を選択すると、既存のEntra ID接続を見つけることができます。

または、,

> --> --> を選択して、新しいEntra IDディレクトリ接続を作成できます。

接続状態が強調表示されたEntra IDプロバイダー(/en-us/citrix-cloud/media/iam-aad-connected.png)

> **重要:**
>
> ME-ID IDを使用する新しいSAMLアプリケーションを作成する予定のEntra IDテナントと同じテナントに接続する必要があります。

- ストア認証方法は**SAML 2.0**に設定する必要があります。Entra IDを認証方法として使用しないでください。ストア認証方法を変更するには、Citrix Cloudコンソールで** > ** に移動します。
- UPNサフィックス`@yourdomain.com`は、カスタムドメイン名としてEntra ID内にインポートおよび検証されている必要があります。Azureポータルでは、これは** > ** の下にあります。
- Entra IDユーザーIDは、Microsoft Entra ID Connectを使用してADからインポートする必要があります。これにより、ユーザーIDが正しくインポートされ、正しいUPNサフィックスが設定されていることが保証されます。`@yourtenant.onmicrosoft.com` UPNサフィックスを持つEntra IDユーザーはサポートされていません。
- Citrix FASは、Citrix Cloudテナントおよびリソースの場所に展開され、接続されている必要があります。FASは、StoreFront Cloudから起動されるHDXデスクトップおよびアプリケーションへのシングルサインオンを提供します。ADとEntra IDの両方のユーザーIDのUPN`user@customerdomain`が一致する必要があるため、ADシャドウアカウントを構成する必要はありません。FASは、正しいUPNを持つ必要なユーザー証明書を生成し、HDXリソースが起動されたときにスマートカードサインインを実行します。

カスタムEntra IDエンタープライズSAMLアプリケーションの構成

デフォルトでは、ストアへのSAMLサインインの動作は、ADユーザーIDに対してアサートすることです。**cip_directory** SAML属性は、すべてのエンドユーザーで同じハードコードされた文字列値であり、スイッチとして機能します。Citrix CloudとStoreFront Cloudは、サインイン中にこの属性を検出し、SAMLがユーザーIDのEntra IDバージョンに対してアサートするようにトリガーします。この属性で **azuread** パラメーターを使用すると、デフォルトのSAML動作が上書きされ、ストアユーザーはAD IDではなくEntra ID IDを使用して認証されるようになります。

このセクションの手順はEntra ID向けですが、同じタスクを実行すれば、別のSAML 2.0プロバイダー（ADFS、Duo、Okta、OneLogin、PingOneSSOなど）を使用して同様のSAMLアプリケーションを作成できます。SAMLプロバイダーは、SAMLアプリケーション内でハードコードされた

SAML属性（cip_directory = azuread）を構成できる必要があります。このセクションで説明されているのと同じSAML属性マッピングを作成するだけです。

1. Azureポータルにサインインします。
2. ポータルメニューから、**Entra ID** を選択します。
3. 左ペインの **管理** で、**エンタープライズ アプリケーション** を選択します。
4. 作業ペインのコマンドバーから、**新しいアプリケーション** を選択します。
5. コマンドバーから、**独自のアプリケーションを作成** を選択します。Citrix Cloud SAML SSOエンタープライズアプリケーションテンプレートは使用しないでください。このテンプレートでは、クレームとSAML属性のリストを変更できません。
6. アプリケーションの名前を入力し、**ギャラリーで見つからないその他のアプリケーションを統合します (ギャラリー以外)** を選択します。**作成** をクリックします。アプリケーションの概要ページが表示されます。
7. 左ペインから **シングル サインオン** を選択します。作業ペインから **SAML** を選択します。
8. **基本的な SAML 構成** セクションで、**編集** を選択し、次の設定を構成します。

    a. **識別子 (エンティティ ID)** セクションで、**識別子の追加** を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

    - 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com` と入力します。
    - 日本リージョンの場合は、`https://saml.citrixcloud.jp` と入力します。
    - Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us` と入力します。

    b. **応答 URL (Assertion Consumer Service URL)** セクションで、**応答 URL の追加** を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

    - 欧州連合、米国、およびアジア太平洋南部地域の場合は、`https://saml.cloud.com/saml/acs`と入力します。
    - 日本地域の場合は、`https://saml.citrixcloud.jp/saml/acs`と入力します。
    - Citrix Cloud Government地域の場合は、`https://saml.cloud.us/saml/acs`と入力します。

    c. **Logout URL (Optional)**セクションで、Citrix Cloudテナントが配置されている地域に関連付けられた値を入力します。

- 欧州連合、米国、およびアジア太平洋南部地域の場合は、`https://saml.cloud.com/saml/logout/callback`と入力します。
- 日本地域の場合は、`https://saml.citrixcloud.jp/saml/logout/callback`と入力します。
- Citrix Cloud Government地域の場合は、`https://saml.cloud.us/saml/logout/callback`と入力します。

d. コマンドバーから、**Save**を選択します。

9. **Attributes & Claims**セクションで、**Edit**を選択して以下のクレームを構成します。これらのクレームは、SAML応答内のSAMLアサーションに表示されます。

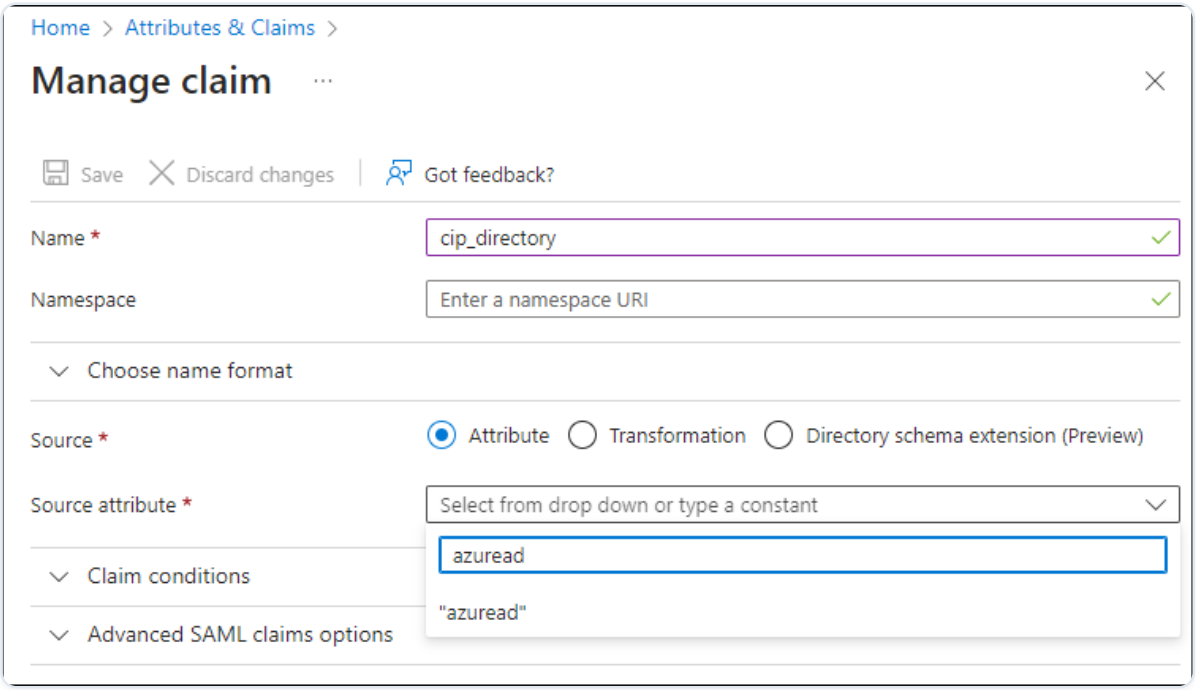
a. **Unique User Identifier (Name ID)**クレームの場合、デフォルト値を`user.localuserprincipalname`に更新します。

b. コマンドバーから、**Add new claim**を選択します。

c. **Name**に、**cip_directory**と入力します。

d. **Source**で、**Attribute**が選択されたままにします。

e. **Source attribute**に、**azuread**と入力します。この値は、入力後に引用符で囲まれて表示されます。



f. コマンドバーから、**保存**を選択します。

g. **名前**フィールドと**ソース属性**フィールドに以下の値を持つ追加のクレームを作成します。

名前	ソース属性
cip_fed_upn	user.localuserprincipalname
displayName	user.displayname
givenName	user.givenname
familyName	user.surname

UPN値を含むクレーム管理画面(/en-us/citrix-cloud/media/manage-claims-screen-with-upn-value.png)

> **重要:**
>
> これらの追加クレームは、各クレームに対して手順b～fを繰り返すか、上記の表に記載されているソース属性が既に設定されている**追加クレーム**セクションのデフォルトクレームを変更することで作成できます。デフォルトクレームには、名前空間 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` が含まれます。
>
> デフォルトのクレームを変更する場合は、各クレームから名前空間を削除する必要があります。新しいクレームを作成する場合は、名前空間を含むクレームを削除する必要があります。この名前空間を持つクレームが結果のSAMLアサーションに含まれている場合、アサーションは無効になり、誤ったSAML属性名が含まれます。

h. **追加クレーム**セクションで、`http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 名前空間を持つ残りのクレームについて、省略記号（...）ボタンをクリックし、**削除**をクリックします。

削除メニューが強調表示されています(/en-us/citrix-cloud/media/saml-idp-aad-delete-schema-claims.png)

完了すると、**属性とクレーム**セクションは以下に示すように表示されます。

Entra IDの属性とクレームが完了しました(/en-us/citrix-cloud/media/azure-ad-completed-attributes-and-claims.png)

10. このサードパーティのオンラインツールを使用して、Citrix Cloud SAML署名証明書のコピーを取得します。

11. URLフィールドに`<https://saml.cloud.com/saml/metadata>`を入力し、**読み込み**をクリックします。

    メタデータ証明書の抽出(/en-us/citrix-cloud/media/saml-meta-cert.png)

12. ページの下部までスクロールし、**ダウンロード**をクリックします。

    ダウンロード(/en-us/citrix-cloud/media/saml-certi-download.png)

    ダウンロードされたファイル(/en-us/citrix-cloud/media/saml-certi-file.png)

13. Entra ID SAMLアプリケーションの署名設定を構成します。
14. 手順10で取得した本番SAML署名証明書をEntra ID SAMLアプリケーション内にアップロードします。

    - **検証証明書を要求する**を有効にします。

    検証証明書(/en-us/citrix-cloud/media/saml-verify-certi.png)

    SAML証明書(/en-us/citrix-cloud/media/saml-certi.png)

トラブルシューティング

1. SAML-tracerブラウザ拡張機能などのSAMLネットワークツールを使用して、SAMLアサーションに正しいユーザー属性が含まれていることを確認します。
2. 黄色で表示されているSAML応答を見つけ、この例と比較します。

    ネットワークツールからのSAML応答の例(/en-us/citrix-cloud/media/saml-idp-aad-saml-tool-response.png)

3. 下部ペインの**SAML**タブをクリックして、SAML応答をデコードし、XMLとして表示します。
4. 応答の一番下までスクロールし、SAMLアサーションに正しいSAML属性とユーザー値が含まれていることを確認します。

    SAMLアサーション値が強調表示されたXMLファイル(/en-us/citrix-cloud/media/xml-file-with-saml-assertion-value-highlighted.png)

エンドユーザーがストアにサインインできない場合は、Citrixサポートに連絡し、次の情報を提供してください。

- SAML-tracerキャプチャ
- ストアへのサインインが失敗した日時
- 影響を受けるユーザー名

- ストアへのサインインに使用したクライアントコンピューターの発信元IPアドレス。このIPアドレスを取得するには、https://whatismyip.comのようなツールを使用できます。

Citrix Cloud SAML接続を構成する

すべてのCitrixログオンフローは、ストアURLまたはCitrix Cloud GO URLのいずれかを使用して、サービスプロバイダーによって開始される必要があります。

「**IDおよびアクセス管理 > 認証 > IDプロバイダーの追加 > SAML**」内のSAML接続には、デフォルトの推奨値を使用します。

Citrix Cloudに入力するために、Entra IDポータルからEntra ID SAMLアプリケーションのSAMLエンドポイントを取得します。

AAD SAMLエンドポイント(/en-us/citrix-cloud/media/aad-saml-endpoints.png)

Citrix Cloud SAML接続内で使用するEntra ID SAMLエンドポイントの例

> **重要:**
>
> EntraID SSOとログアウトSAMLエンドポイントは同じURLです。

CITRIX CLOUDのこのフィールド	この値を入力します
エンティティID	`https://sts.windows.net/<yourEntraIDTenantID>`
認証要求に署名	はい
SSOサービスURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、完全一致
ログアウトURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`

CITRIX CLOUDのこのフィールド	この値を入力します
ログアウトリクエストに署名	はい
SLOバインディングメカニズム	HTTP ポスト

ストア認証用のゲストおよびB2B ID向けEntra IDを使用したSAML

この記事に従う前に、B2B SAMLが認証ユースケースに適しているかどうかを理解することが不可欠です。この特定の特殊なSAMLソリューションを実装することを決定する前に、ユースケースの説明とFAQを徹底的に読んでください。続行する前に、B2B SAMLが適切なシナリオと、使用する必要があるIDの種類を完全に理解していることを確認してください。

前提条件

- SAMLアサーション内で認証のために**cip_upn**のみを送信する、B2B SAMLでの使用のために特別に構成されたSAMLアプリケーション。
- SAMLプロバイダー内のフロントエンドユーザー。
- ADシャドウアカウントが作成されるADフォレストおよびドメインに結合されたCitrix Cloud™コネクタのペアを含むリソースロケーション。
- 暗黙的なUPNを使用するか、ADシャドウアカウントが作成されるバックエンドADフォレストに代替UPNサフィックスを追加します。
- UPNが一致するバックエンドADシャドウアカウント。
- ADシャドウアカウントユーザーにマッピングされたDaaSまたはCVADリソース。
- 同じリソースロケーションにリンクされた1つ以上のFASサーバー。

よくある質問

B2B SAMLを使用する理由?

大規模な組織が請負業者や一時的な従業員をIDプラットフォームに招待することは非常に一般的です。その目的は、請負業者のメールアドレスや組織外のメールアドレスなど、ユーザーの既存のIDを使用して、請負業者にストアへの一時的なアクセスを許可することです。`B2B SAML` は、DaaSリソースが公開されているADドメイン内に存在しないネイティブまたはゲストのフロントエンドIDの使用を可能にします。

B2B SAMLとは?

AD属性	SAMLアサーション内のデフォルト属性名
userPrincipalName	cip_upn
メール	cip_email
objectSID	cip_sid
objectGUID	cip_oid

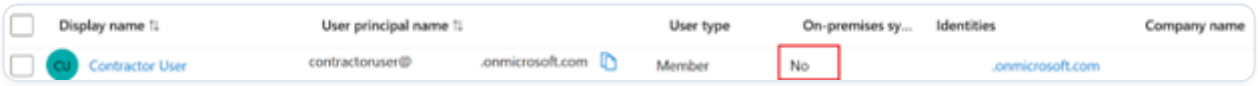
認証に必要な他の3つのADユーザー属性であるobjectSID、objectGUID、およびmailは、ADシャドウアカウントが存在するADドメインに結合されたCitrix Cloudコネクタを使用して取得されます。これらは、ストアまたはCitrix CloudのSAMLサインインフロー中にSAMLアサーションに含める必要がなくなりました。

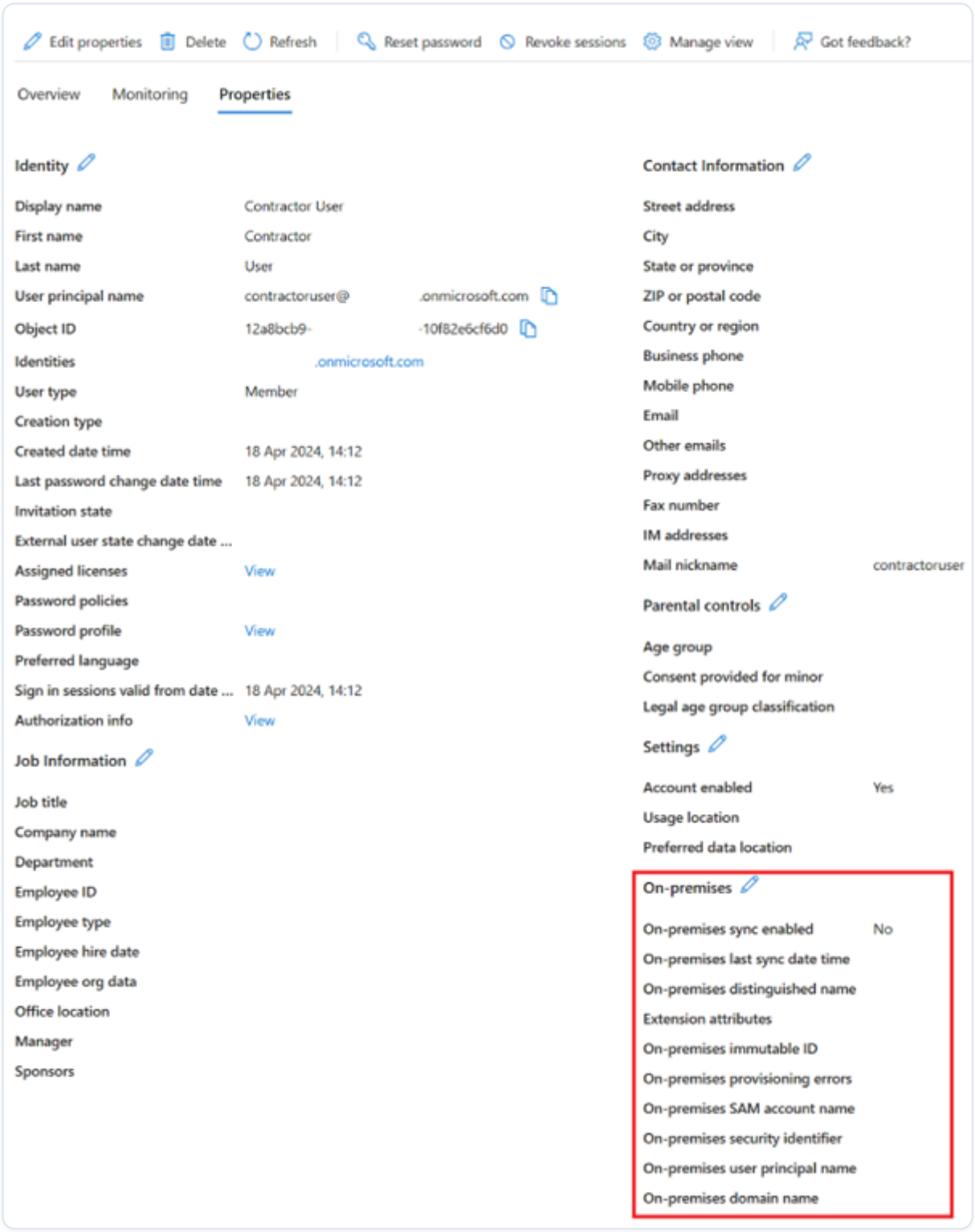
AD属性	SAMLアサーション内のデフォルト属性名
userPrincipalName	cip_upn

> **重要:**
>
> `B2B SAML`を含むすべてのSAMLフローで**displayName**を送信する必要があります。**displayName**は、ストアUIがストアユーザーのフルネームを正しく表示するために必要です。

ネイティブSAMLユーザーIDとは何ですか?

ネイティブSAMLユーザーとは、Entra IDやOktaなどのSAMLプロバイダーディレクトリ内にのみ存在するユーザーIDです。これらのIDは、Entra ID Connectのような AD同期ツールを介して作成されないため、オンプレミスのユーザー属性を含みません。DaaSリソースを列挙して起動できるようにするには、対応するADバックエンドシャドウアカウントが必要です。ネイティブSAMLユーザーは、Active Directory内の対応するアカウントにマッピングする必要があります。





別のEntra IDテナントからインポートされたB2Bユーザーとは何ですか?

B2Bユーザーとは、Entra IDテナント1内にメンバーとして存在し、Entra IDテナント2などの他のEntra IDテナントにゲストユーザーとして招待されるEntra IDユーザーです。B2B SAMLアプリはEntra IDテナント2内に構成され、SAML IdPとしてCitrix Cloudに接続されます。B2BユーザーがDaaSリソースを列挙して起動できるようにするには、対応するADバックエンドシャドウアカウン

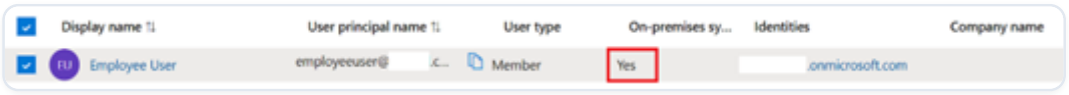
トが必要です。B2Bユーザーは、Active Directory内の対応するシャドウアカウントにマッピングする必要があります。

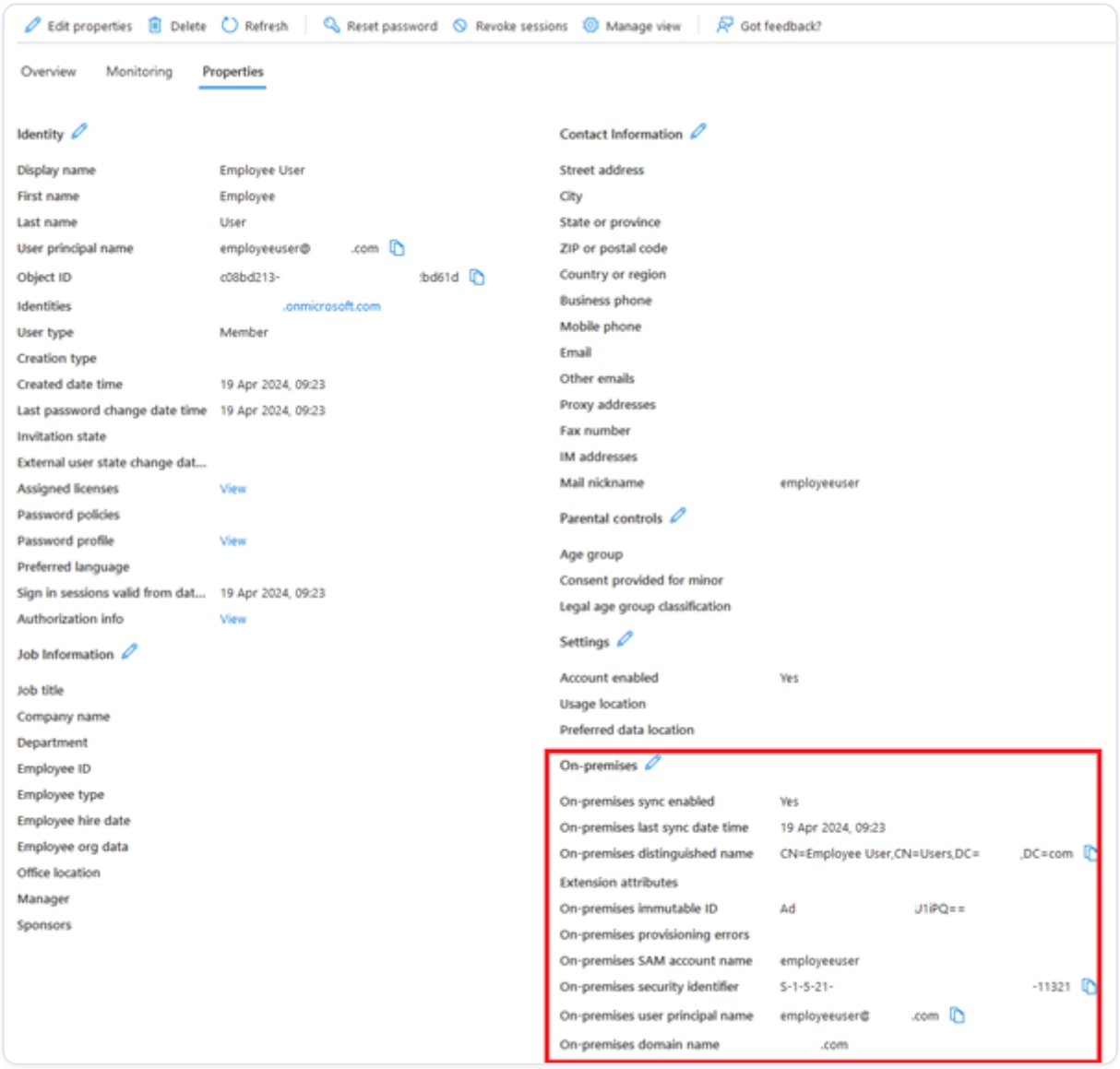
B2Bユーザーの詳細、および他のEntra IDテナントのメンバーユーザーをゲストユーザーとして自分のEntra IDテナントに招待する方法については、Microsoftのドキュメントを参照してください。

概要: 従業員向けの外部ゲストとのB2Bコラボレーション Microsoft Entra B2Bコラボレーション ユーザーのプロパティ

ADバックアップSAMLユーザーIDとは何ですか?

ADバックアップSAMLユーザーとは、Entra IDやOktaなどのSAMLプロバイダーディレクトリ内、およびオンプレミスのADフォレスト内に存在するユーザーIDです。これらのIDは、Entra ID ConnectのようなAD同期ツールを介して作成されるため、オンプレミスのユーザー属性を含みます。これらのユーザーはオンプレミスのSIDとOIDを含むため、ADバックエンドシャドウアカウントは必要ありません。そのため、ADドメイン参加済みVDAを使用して公開されたDaaSリソースを列挙して起動できます。



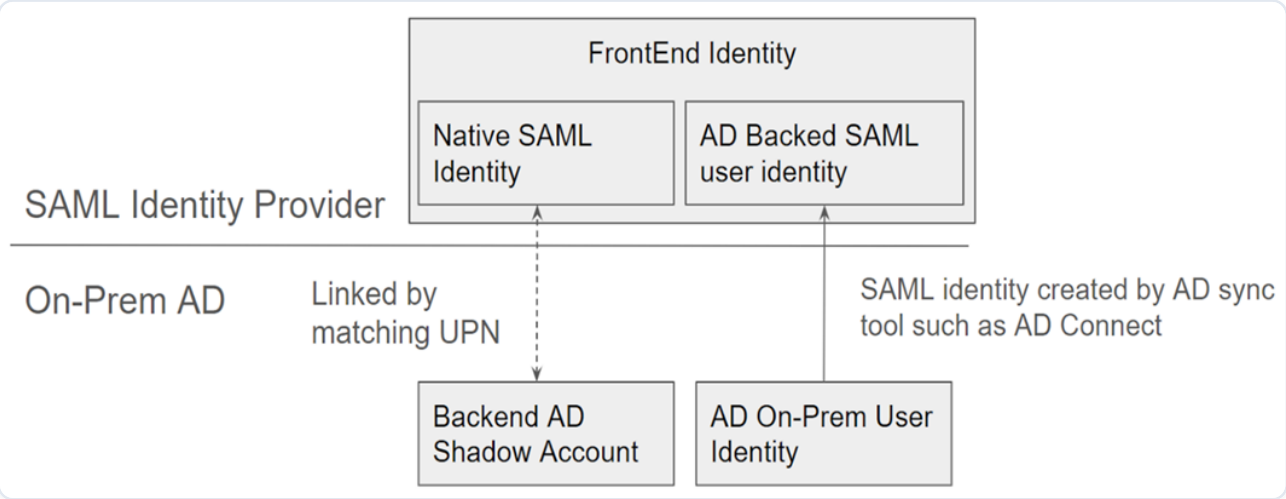


フロントエンドIDとは何ですか?

フロントエンドIDとは、SAMLプロバイダーとストアの両方にサインインするために使用されるIDです。フロントエンドIDは、SAMLプロバイダー内でどのように作成されたかによって、異なるユーザー属性を持ちます。

1. ネイティブSAMLユーザーID
2. ADバックSAMLユーザーID

SAMLプロバイダーには、これら2種類のIDが混在している場合があります。たとえば、IDプラットフォーム内に契約社員と正社員の両方がいる場合、`B2B SAML` は両方の種類のフロントエンドIDで機能しますが、ネイティブSAMLユーザーIDタイプのいくつかのアカウントがある場合にのみ必須です。



バックエンドADシャドウアカウントとは何ですか?

バックエンドADシャドウアカウントは、DaaSが使用するADアカウントであり、SAMLプロバイダー内の対応するフロントエンドIDにマッピングされます。

バックエンドADシャドウアカウントが必要な理由は何ですか?

ADドメイン参加済みVDAを使用して公開されたDaaSまたはCVADリソースを列挙するには、VDAが参加しているActive Directoryフォレスト内のADアカウントが必要です。DaaSデリバリーグループ内のリソースをシャドウアカウントユーザーにマッピングし、VDAを参加させたADドメイン内のシャドウアカウントを含むADグループにマッピングします。

> **重要:**

> ADドメイン属性を持たないネイティブSAMLユーザーのみが、一致するADシャドウアカウントを必要とします。フロントエンドIDがActive Directoryからインポートされている場合、`B2B SAML` を使用する必要はなく、バックエンドADシャドウアカウントを作成する必要もありません。

フロントエンドIDを対応するバックエンドADシャドウアカウントにリンクするにはどうすればよいですか?

フロントエンドIDとバックエンドIDをリンクする方法は、一致するUPNを使用することです。2つのリンクされたIDは同じUPNを持つ必要があり、これによりストアは、それらがストアにサインインし、DaaSリソースを列挙して起動する必要がある同じエンドユーザーを表していると判断できます。

> **重要**

> 単一のフロントエンドIDは、1つのADフォレスト/ドメイン内の単一のバックエンドIDにのみマッピングできます。DaaSリソースの列挙は、正しいCitrix Cloudコネクタによって実行されるADシャドウアカウントルックアップから取得された1つのSID値のみを使用して行われます。同じUPNサフィックスを持つ複数のADシャドウアカウントに一致する単一のフロントエンドユーザーを使用して、1対多の関係を作成することはできません。バックエンドADシャドウアカウントは、単一のADフォレスト/ドメイン内にのみ存在する必要があります。

> フロントエンドIDとバックエンドID間の明確なUPN一致を使用したサポート フロントエンドユーザー `(user@yourforest.com)` > ADフォレスト1のバックエンドユーザー `(UPN user@yourforest.com)`

> 1つのフロントエンドを1つのバックエンドIDに一致させようとすると、UPNの曖昧さがあるためサポートされていません。 フロントエンドユーザー `(user@yourforest1.com)` > ADフォレスト1のバックエンドユーザー `(UPN user@yourforest1.com)` > ADフォレスト2のバックエンドユーザー `(UPN user@yourforest1.com)`

B2B SAMLにCitrix FASは必要ですか?

はい。ストアへのサインインにフェデレーション認証方法を使用する場合、起動時にVDAへのSSONのためにFASが必要です。

「SID不一致の問題」とは何ですか、またいつ発生するか?

「SID不一致の問題」は、SAMLアサーションにフロントエンドユーザーのSIDが含まれており、それがADシャドウアカウントユーザーのSIDと一致しない場合に発生します。これは、SAMLプロバイダーにサインインするアカウントがオンプレミスのSIDを持っており、それがシャドウアカウントユーザーのSIDと同じではない場合に起こり得ます。これは、フロントエンドIDがEntra ID ConnectのようなAD同期ツールによってプロビジョニングされ、シャドウアカウントが作成されたADフォレストとは異なるADフォレストからである場合にのみ発生します。

`B2B SAML` は「SID不一致の問題」の発生を防ぎます。正しいSIDは、バックエンドADドメインに結合されたCitrix Cloudコネクタを介して、シャドウアカウントユーザーに対して常にフェッチされます。シャドウアカウントユーザーの検索は、フロントエンドユーザーのUPNを使用して実行され、その後、対応するバックエンドシャドウアカウントユーザーと照合されます。

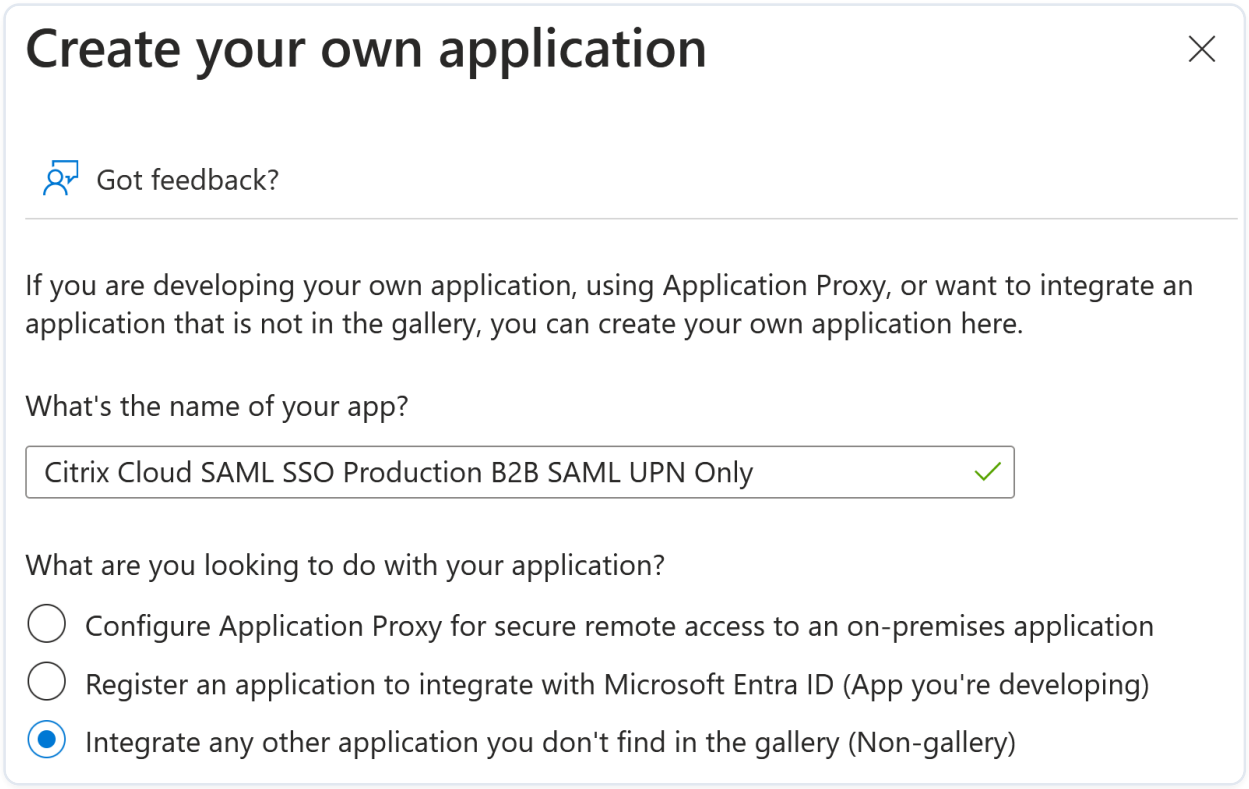
SID不一致の問題の例： **フロントエンドユーザー** はEntra ID Connectによって作成され、**ADフォレスト1** から同期されています。 `S-1-5-21-000000000-0000000000-0000000001-0001`

バックエンドシャドウアカウントユーザー は **ADフォレスト2** 内で作成され、DaaSリソースにマッピングされています `S-1-5-21-000000000-0000000000-0000000002-0002`

SAMLアサーションには4つのcip_*属性すべてが含まれており、**cip_sid** には値 `S-1-5-21-000000000-0000000000-0000000001-0001` が含まれていますが、これはシャドウアカウントのSIDと一致せず、エラーをトリガーします。

外部ゲストアカウント向けにEntra ID内でB2B SAMLアプリケーションを構成する

1. Azureポータルにサインインします。
2. ポータルメニューから、**Entra ID** を選択します。
3. 左ペインの **管理** の下にある **エンタープライズアプリケーション** を選択します。
4. **独自のアプリケーションを作成** を選択します。
5. SAMLアプリケーションに `Citrix Cloud SAML SSO Production B2B SAML UPN Only` のような適切な名前を入力します。



6. 左側のナビゲーションペインから「**シングルサインオン**」を選択し、作業ペインから「**SAML**」をクリックします。
7. 「**基本的なSAML構成**」セクションで「**編集**」をクリックし、次の設定を構成します。
   a. 「**識別子 (エンティティID)**」セクションで「**識別子の追加**」を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

- ヨーロッパ、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com`と入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp`と入力します。
- Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us`と入力します。

b. 「**応答URL (Assertion Consumer Service URL)**」セクションで「**応答URLの追加**」を選択し、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

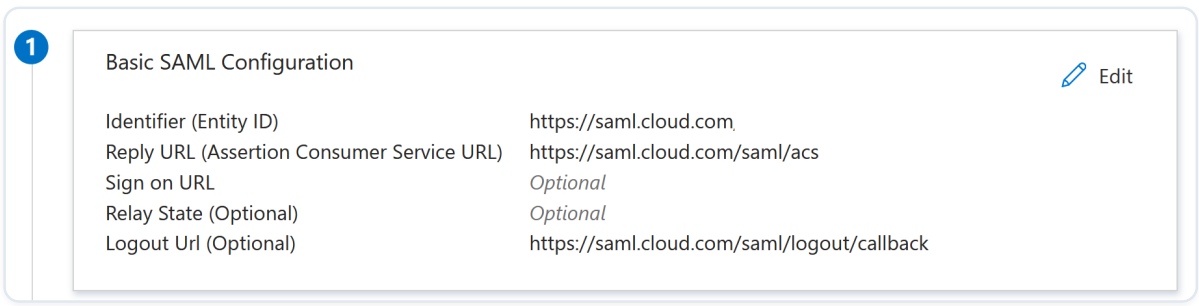
- ヨーロッパ、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/acs`と入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/acs`と入力します。
- Citrix Cloud Governmentリージョンの場合は、`https://saml.cloud.us/saml/acs`と入力します。

c. 「**サインオンURL**」セクションで、ストアURLを入力します。

d. 「**ログアウトURL (オプション)**」セクションで、Citrix Cloudテナントが配置されているリージョンに関連付けられた値を入力します。

- ヨーロッパ、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/logout/callback`と入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/logout/callback`と入力します。
- Citrix Cloud Governmentリージョンについては、`https://saml.cloud.us/saml/logout/callback`を入力します。

e. コマンドバーから、**保存**をクリックします。**基本SAML構成**セクションは次のように表示されます。



8. **属性とクレーム**セクションで、**編集**をクリックして、以下のクレームを構成します。SAMLアプリ作成後、以下の属性を構成します。

   a. 一意のユーザー識別子（名前ID）クレームについては、名前識別子形式を未指定に設定し、そのソース属性を`user.localuserprincipalname`とします。

   b. **cip_upn**クレームについては、デフォルト値の`user.localuserprincipalname`をそのままにします。

   c. **displayName**については、デフォルト値の`user.displayname`をそのままにします。

   d. **givenName**クレームについては、デフォルト値を`user.givenname`に更新します。

   e. **familyName**クレームについては、デフォルト値を`user.surname`に更新します。

   f. **追加クレーム**セクションで、`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`名前空間を持つ残りのクレームについては、省略記号（...）ボタンをクリックし、**削除**をクリックします。これらは上記のユーザー属性の重複であるため、これらのクレームを含める必要はありません。

      完了すると、**属性とクレーム**セクションは以下に示すように表示されます。



   g. このサードパーティのオンラインツールを使用して、Citrix Cloud SAML署名証明書のコピーを取得します。

   h. URLフィールドに`https://saml.cloud.com/saml/metadata`を入力し、**読み込み**をクリックします。



9. ページの一番下までスクロールし、**ダウンロード**をクリックします。

   メタデータ証明書のダウンロード(/en-us/citrix-cloud/media/metadata_cert_download.png)

   証明書のダウンロード(/en-us/citrix-cloud/media/certificate_download.png)

10. Entra ID SAMLアプリケーションの署名設定を構成します。
11. 手順10で取得した本番SAML署名証明書をEntra ID SAMLアプリケーション内にアップロードします。

    a. **検証証明書を要求する**を有効にします。

   検証証明書(/en-us/citrix-cloud/media/verification_cert.png)

   検証証明書(/en-us/citrix-cloud/media/saml_certificate.png)

Citrix Cloud B2B SAML接続を構成する

デフォルトでは、Citrix CloudはSAMLアサーションにcip_upn、cip_email、cip_sid、cip_oidが存在することを期待し、これらの属性が送信されない場合、SAMLサインインは失敗します。これを防ぐには、新しいSAML接続を作成する際に、これらの属性のチェックを削除してください。

1. デフォルト設定を使用して新しいSAML接続を作成します。
2. 下部にある**SAML属性マッピング構成**セクションに移動し、新しいSAML構成を保存する前に変更を加えます。
3. **cip_email**、**cip_sid**、**cip_oid**の各フィールドからSAML属性名を削除します。
4. **cip_upn**をそのフィールドから削除しないでください。
5. 他の属性をそれぞれのフィールドから削除しないでください。**displayName**はストアUIで引き続き必要であり、変更しないでください。

B2B SAML接続UPN(/en-us/citrix-cloud/media/simplified-saml-connection-upn.png)

ADシャドウアカウントのリソースロケーションとコネクタを構成する

バックエンドのシャドウアカウントADフォレスト内にリソースロケーションとコネクタのペアが必要です。SAMLアサーション内でcip_upnのみが直接提供される場合、Citrix Cloudは、シャドウアカウントのユーザーIDと、cip_email、cip_sid、cip_oidなどの属性を検索するために、このADフォレスト内のコネクタを必要とします。

1. バックエンドのシャドウアカウントADフォレストに結合されたCitrix Cloudコネクタを含む新しい**リソースロケーション**を作成します。

   ADシャドウアカウント(/en-us/citrix-cloud/media/ad-shadow-account.png)

2. 使用するバックエンドADシャドウアカウントを含むADフォレストと一致するように、リソースロケーションに名前を付けます。
3. 新しく作成したリソースロケーション内に、Citrix Cloudコネクタのペアを構成します。

例： `ccconnector1.shadowaccountforest.com` `ccconnector2.shadowaccountforest.com`

バックエンドADフォレスト内でFASを構成する

請負業者のフロントエンドユーザーは、FASを確実に必要とします。DaaSの起動中、請負業者のユーザーはADシャドウアカウントのパスワードを知らない可能性が高いため、起動を完了するためにWindows資格情報を手動で入力することはできません。

1. シャドウアカウントが作成されたバックエンドADフォレスト内に、1つ以上のFASサーバーを構成します。
2. シャドウアカウントが作成されたバックエンドADフォレストに結合されたCitrix Cloudコネクタのペアを含む同じリソースロケーションに、FASサーバーをリンクします。

FASを構成する(/en-us/citrix-cloud/media/configure-fas.png)

ADドメイン内で代替UPNサフィックスを構成する

> **重要:**

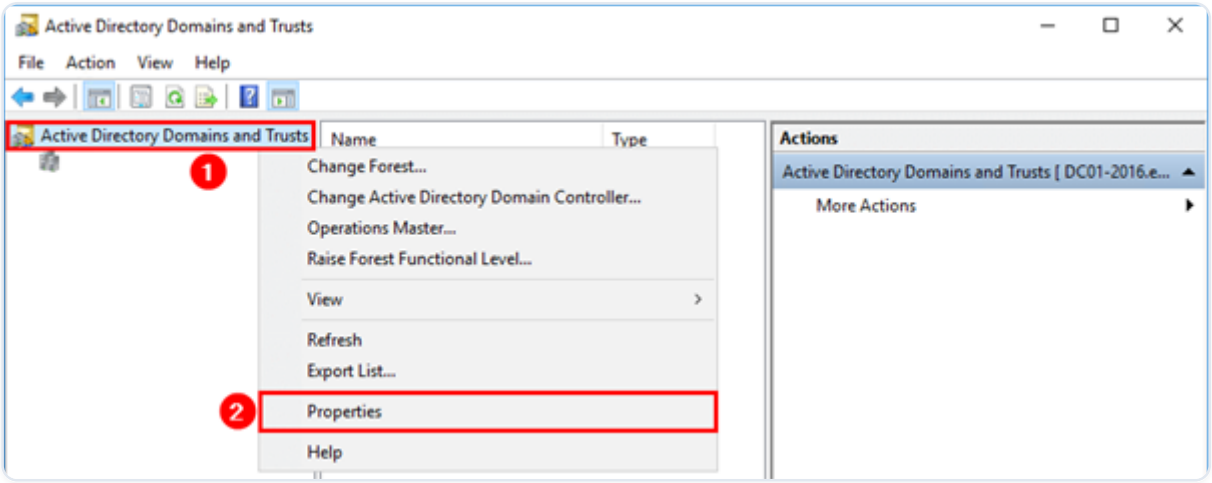
> UPNはユーザーのメールアドレスと同じではありません。多くの場合、使いやすさのために同じ値が使用されますが、UPNとメールは異なる値を持つことが多く、異なるActive Directory属性および異なるEntra IDユーザー属性で定義されます。このソリューションは、フロントエンドとバックエンドのID間のUPNの一致に依存し、メールの一致には依存しません。

> ドメインがDNSでパブリックにルーティング可能であれば、その暗黙的なUPNサフィックスを使用できます。または、OktaまたはEntra IDテナントに招待したいすべての外部フロントエンドユーザーに対して、一致する代替UPNサフィックスを追加できます。ADが暗黙的なUPNとして `yourdomain.local` を使用している場合、 `yourdomain.com` のような代替UPNサフィックスを選択する必要があります。Entra IDでは、カスタムドメイン名内に `yourdomain.local` を追加することはできません。

例えば、外部ユーザー `contractoruser@hotmail.co.uk` を招待し、これをバックエンドのADシャドウアカウント `contractoruser@yourforest.com` に関連付けたい場合、ADフォレスト内に `yourforest.com` をALT UPNサフィックスとして追加します。

Active Directoryドメインと信頼UIを使用してActive Directoryに代替UPNサフィックスを追加する

1. バックエンドADフォレスト内のドメインコントローラーにサインインします。
2. **ファイル名を指定して実行**ダイアログを開き、`domain.msc`と入力して、**OK**をクリックします。
3. Active Directoryドメインと信頼ウィンドウで、**Active Directoryドメインと信頼**を右クリックし、**プロパティ**を選択します。
4. **UPNサフィックス**タブの「代替UPNサフィックス」ボックスに代替UPNサフィックスを追加し、**追加**を選択します。



5. **OK**をクリックします。

PowerShellを使用してバックエンドADフォレストのUPNサフィックスを管理する

必要なシャドウアカウントUPNを作成するために、バックエンドADフォレストに多数の新しいUPNサフィックスを追加する必要がある場合があります。バックエンドADフォレストに追加する必要がある代替UPNサフィックスの数は、SAMLプロバイダーテナントに招待する外部ユーザーの数によって異なります。

多数の新しい代替UPNサフィックスを作成する必要がある場合に、これを実現するためのPowerShellを以下に示します。

```
# Get the list of existing ALT UPN suffixes within your AD Forest

(Get-ADForest).UPNSuffixes



# Add or remove ALT UPN Suffixes
```

```
$NewUPNSuffixes = @("yourforest.com","externalusers.com")



# Set action to "add" or "remove" depending on the operation you wish to
perform.

$Action = "add"

foreach($NewUPNSuffix in $NewUPNSuffixes)

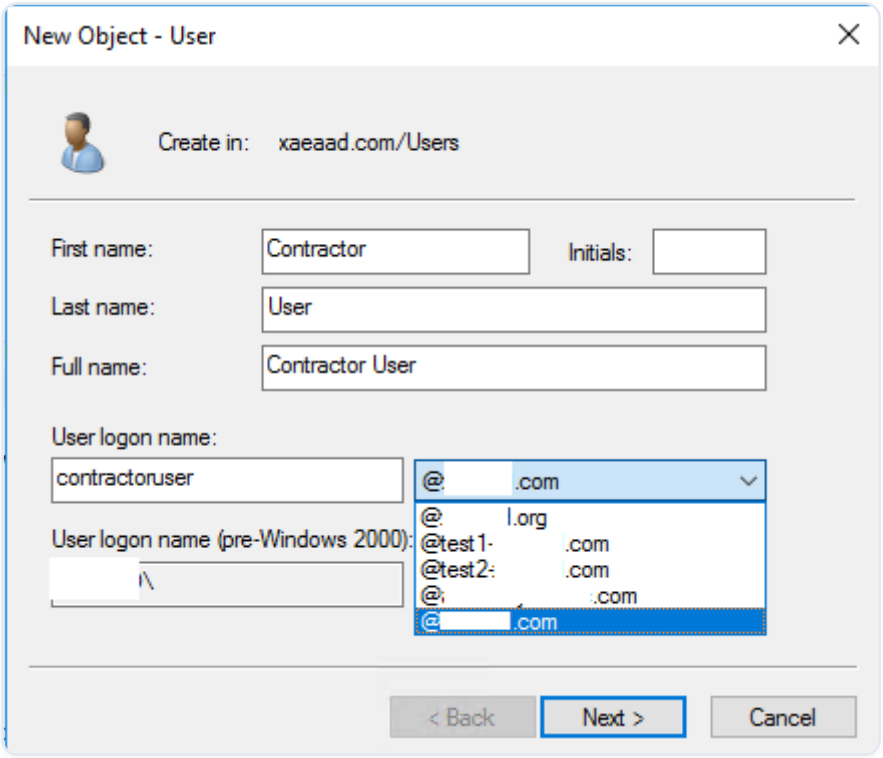
{

    Get-ADForest | Set-ADForest -UPNSuffixes @{ $Action=$NewUPNSuffix }

}
```

バックエンドADフォレスト内でADシャドウアカウントを構成する

1. 新しいADシャドウアカウントユーザーを作成します。
2. 新しいADユーザーには、`yourforest.local`のようなADフォレストの暗黙的なUPNがデフォルトで選択されます。以前に作成した適切な代替UPNサフィックスを選択してください。たとえば、シャドウアカウントユーザーのUPNサフィックスとして`yourforest.com`を選択します。



シャドウアカウントユーザーのUPNは、PowerShellを介して更新することもできます。

```
Set-ADUser "contractoruser" -UserPrincipalName
"contractoruser@yourforest.com"
```

重要

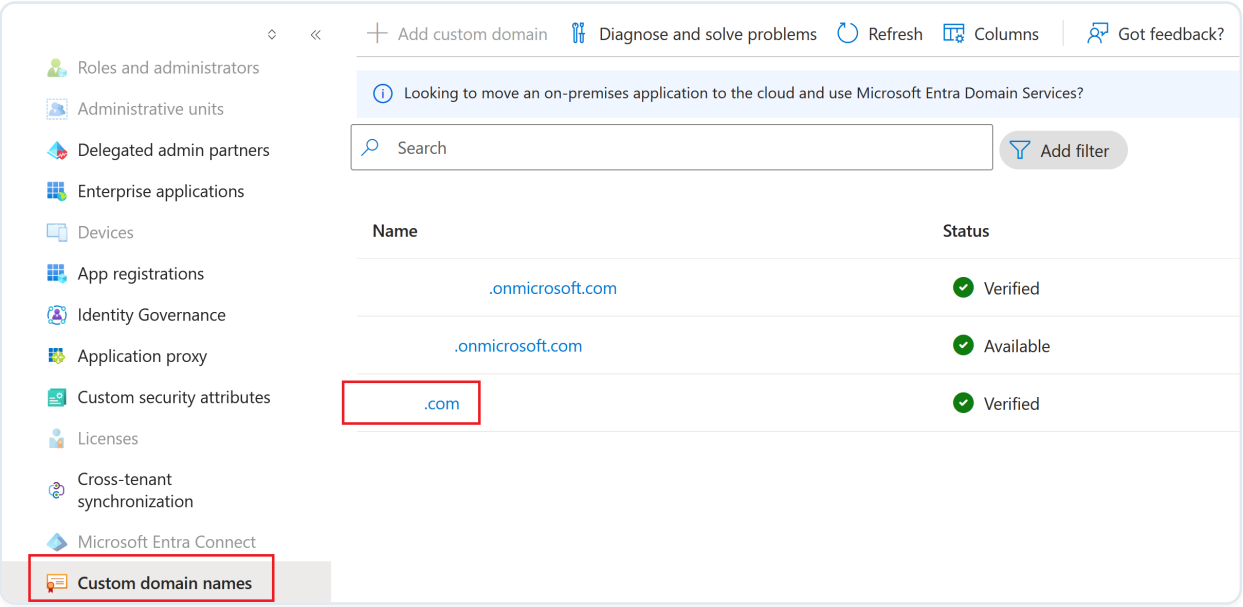
Windows AD PowerShellを使用すると、指定したUPNサフィックスがADフォレスト内に存在しない場合でも、任意のUPNサフィックスを持つシャドウアカウントユーザーを作成できます。使用したい代替UPNサフィックスはADフォレスト内に存在する必要があります。これは、Citrix Cloudコネクタがバックエンドのシャドウアカウントユーザーを検索するためにこのリストに依存するためです。上記のスクリーンショットのように代替UPNサフィックスがADフォレストに表示されない場合、Citrix Cloudはフロントエンドを適切なバックエンドADシャドウアカウントに一致させることができません。

3. シャドウアカウントユーザーのUPNは、外部のフロントエンドIDユーザーのUPNと完全に一致する必要があります。
4. フロントエンドユーザーのストアへのサインインをテストします。
5. サインインが成功した後、ストアにすべての期待されるリソースが列挙されていることを確認します。ADシャドウアカウントにマッピングされたリソースが表示されるはずです。

ゲストEntra IDユーザーのUPNをADシャドウアカウントのUPNと一致するように構成する

外部ゲストユーザーがEntra IDテナントに招待されると、ユーザーが外部であることを示す自動生成されたUPNが作成されます。外部Entra IDユーザーには、自動的に@Entra IDtenant.onmicrosoft.com UPNサフィックスが割り当てられますが、これはB2B SAMLでの使用には不適切であり、ADシャドウアカウントと一致しません。これは、Entra ID内のインポートされたDNSドメインと、ADフォレスト内に作成した代替UPNサフィックスに一致するように更新する必要があります。

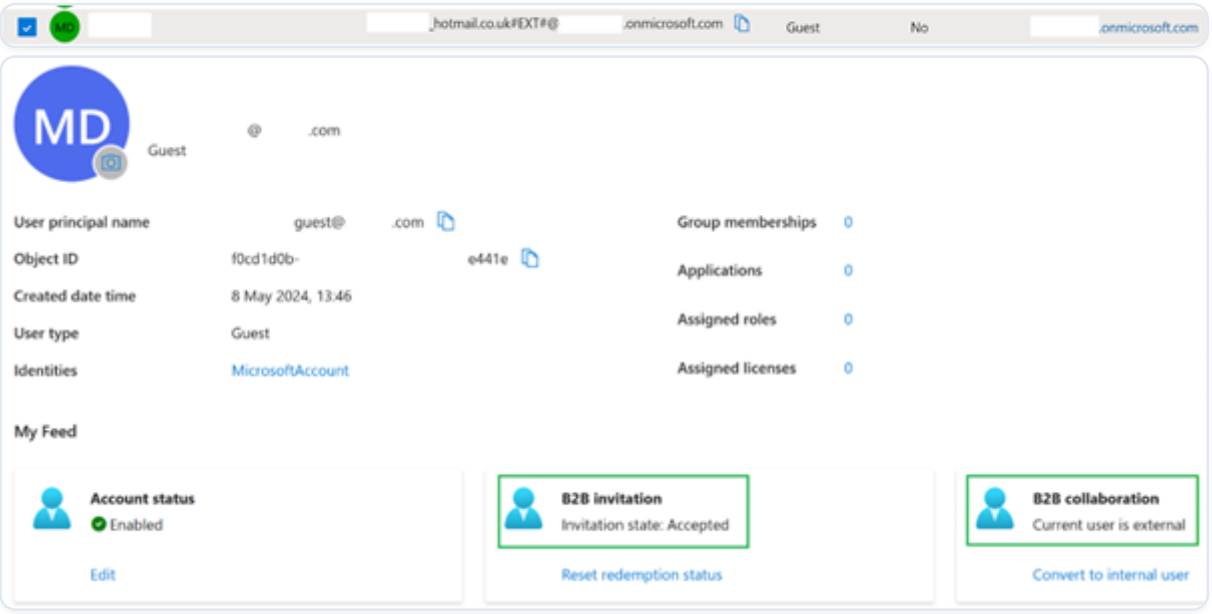
1. ADフォレストに追加した代替UPNサフィックスと一致するカスタムドメインをEntra IDにインポートします。



2. `contractoruser@hotmail.co.uk`のようなゲストユーザーを招待し、招待されたゲストユーザーがEntra IDテナントへのMicrosoft招待を受け入れることを確認します。

   Microsoftによって生成された外部ゲストユーザーUPN形式の例。

   `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



> **重要:**
>
> Citrix Cloudとストアは、SAML認証に#文字を含むUPNを使用できません。

3. Entra IDユーザーを管理できるように、必要なAzure PowerShell Graphモジュールをインストールします。

```
Install-Module -Name "Microsoft.Graph" -Force

Get-InstalledModule -Name  "Microsoft.Graph"
```

4. グローバル管理者アカウントを使用し、`Directory.AccessAsUser.All`スコープでEntra IDテナントにサインインします。

> **重要:**
>
> 権限の低いアカウントを使用するか、`Directory.AccessAsUser.All`スコープを指定しない場合、ステップ4を完了してゲストユーザーのUPNを更新することはできません。

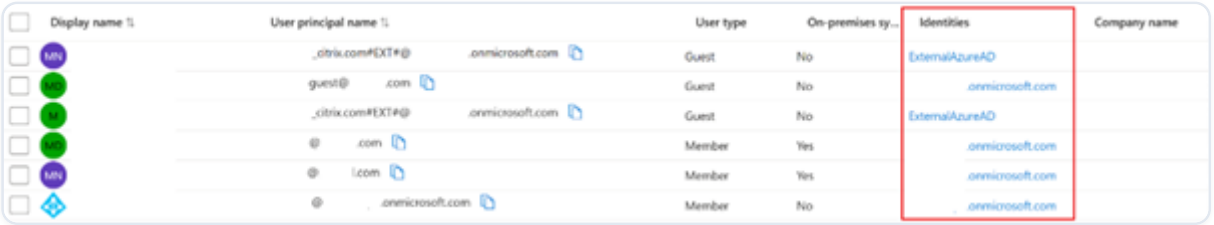
```
Connect-MgGraph -Scopes Directory.AccessAsUser.All
```

5. ADシャドウアカウント用に構成したUPNと一致するUPNでEntra IDユーザーを更新します。

```
$GuestUserId = (Get-MgUser -UserId
"contractoruser_hotmail.co.uk#EXT#@yourentraidtenant.onmicrosoft.com").
Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName
"contractoruser@your.com"
```

6. Entra IDテナント内の外部ゲストユーザーの全リストを取得します（オプション）。




```
Get-MgUser -filter "userType eq 'Guest'" | Select
Id,DisplayName,UserPrincipalName,Mail
```

7. UPNの更新が必要なゲストユーザーIDを取得し、そのUPNサフィックスを更新します。

```
$GuestUserId = (Get-MgUser -UserId
"contractoruser_hotmail.co.uk#EXT#@yourEntra
IDtenant.onmicrosoft.com").Id



Update-MgUser -UserId $GuestUserId -UserPrincipalName
"contractoruser@yourforest.com"
```

8. ゲストユーザーIDが、新しく更新されたUPNを使用して見つけられることを確認します。

```
Get-MgUser -UserId "contractoruser@yourforest.com"
```

B2B SAMLソリューションのテスト

AD、Citrix Cloud、およびSAMLプロバイダーで文書化されたすべての手順が完了したら、サインインをテストし、ストア内でゲストユーザーに正しいリソースリストが表示されることを確認する必要があります。

Citrixは、すべてのSAMLデバッグにSAML-tracerブラウザ拡張機能の使用を推奨しています。この拡張機能は、ほとんどの一般的なWebブラウザで利用できます。この拡張機能は、Base64エンコードされたリクエストとレスポンスをSAML XMLにデコードし、人間が読める形式で表示します。

SAMLトレーサー(/en-us/citrix-cloud/media/saml-tracer.png)

認証にcip_upnのみを使用したB2B SAMLアサーションの例で、SAMLトレーサーを使用してキャプチャされました。

B2B SAMLの例(/en-us/citrix-cloud/media/example-simplified-saml.png)

フロントエンドのテスト(/en-us/citrix-cloud/media/testing-with-frontend-identities.png)

1. 適切なDaaSリソースを、AD連携ユーザーおよびシャドウアカウントユーザー、またはそれらを含むグループにマッピングします。
2. SAMLトレーサーブラウザ拡張機能を起動し、ログオンおよびログオフのフロー全体をキャプチャします。
3. テストしたいフロントエンドユーザータイプについて、表に指定された属性を使用してストアにログインします。

ゲストEntra IDユーザーのログオン: ゲストユーザーとしてEntra IDテナントに招待した請負業者のユーザーのメールアドレスは`contractoruser@hotmail.co.uk`です。

Entra IDからプロンプトが表示されたら、ゲストユーザーの**メールアドレス**を入力します。

または

AD連携Entra IDユーザー/ネイティブEntra IDユーザーのログオン: これらのEntra IDユーザーは、`adbackeduser@yourforest.com`または`nativeuser@yourforest.com`の形式のUPNを持ちます。

Entra IDからプロンプトが表示されたら、ユーザーの**UPN**を入力します。

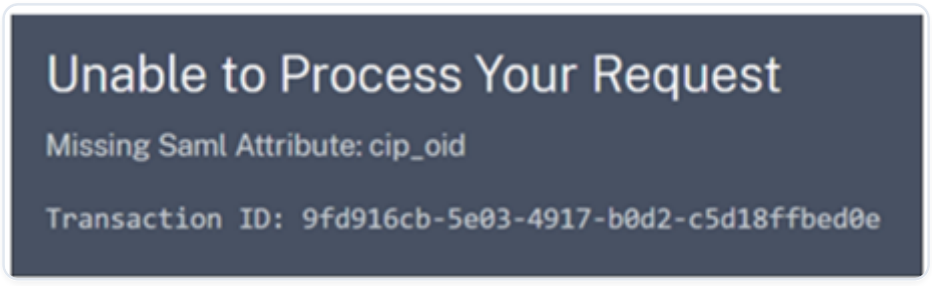
4. アサーションに認証用の**cip_upn**属性のみが含まれていること、およびストアUIで必要とされる**displayName**属性も含まれていることを確認します。
5. ユーザーが必要なDaaSリソースをUIで確認できることを確認します。

B2B SAMLソリューションのトラブルシューティング

SAMLアサーション内で誤ったUPNが送信されている

原因: これは、Entra IDテナント1からEntra IDテナント2にインポートされた**B2B**アカウントでのみ発生します。他のEntra IDテナントからインポートされた**B2B**ユーザーを使用する場合、SAMLアサーション内で誤ったUPNが送信されることがあります。`user.userprincipalname`が使用され、エンドユーザーが別のEntra IDテナントからインポートされたB2Bユーザーでログインすると、SAMLアサーションで**cip_upn**の誤った値が送信されます。SAMLアサーションで使用される**cip_upn**の値は、B2Bユーザーを**メンバー**として含むソースEntra IDテナントからのものになります。`user.localuserprincipalname`を使用すると、**cip_upn**の値が、B2Bユーザーが**ゲスト**として招待されたEntra IDテナントから取得されることが保証されます。

cip_*属性の欠落エラー



原因1: SAMLアサーションにSAML属性が存在しないにもかかわらず、Citrix Cloudがそれを受信することを期待するように構成されています。SAML属性セクション内のCitrix Cloud SAML接続から不要なcip_*属性を削除していません。SAMLを切断して再接続し、不要なcip_*属性への参照を削除してください。

原因2: このエラーは、Citrix CloudコネクタがバックエンドADフォレストで検索する対応するADシャドウアカウントがない場合にも発生する可能性があります。フロントエンドIDは正しく構成されているかもしれませんが、一致するUPNを持つバックエンドADシャドウアカウントIDが存在しないか、見つからない可能性があります。

ログオンは成功するが、ユーザーがストアにログオンした後、DaaSリソースが表示されない

原因: これは、フロントエンドからバックエンドへのID UPNマッピングが正しくないことが原因である可能性が最も高いです。

フロントエンドとバックエンドのIDの2つのUPNが完全に一致し、ストアにログオンしている同じエンドユーザーを表していることを確認してください。DaaSデリバリーグループに、正しいADシャドウアカウントユーザーまたはそれらを含むADグループへのマッピングが含まれていることを確認してください。

DaaSリソースの起動中に、ADドメインに参加しているVDAへのFAS SSONが失敗する

DaaSリソースを起動しようとすると、ストアのエンドユーザーはGINA内でWindows資格情報を入力するよう求められます。また、FASサーバーのWindowsイベントログにイベントID 103が表示されます。

サーバー がUPN `SID S-1-5-21-000000000-0000000000-0000000001-0001` を要求しましたが、ルックアップは `SID S-1-5-21-000000000-0000000000-0000000001-0002` を返しました。

原因: あなたのB2B SAML展開は「SID不一致の問題」に悩まされています。バックエンドのシャドウアカウントADフォレストとは異なるADフォレストからのSIDを含むフロントエンドIDを持っています。

SAMLアサーションで**cip_sid**を送信しないでください。

複数の接続されたADフォレストに同じUPNサフィックスが存在する場合、ADバックアップユーザーのログオンが失敗する

Citrix Cloudには複数のリソースロケーションと、異なるADフォレストに接続されたコネクタがあります。シャドウアカウントADフォレストとは異なるADフォレストからEntra IDにインポートされたADバックアップユーザーが使用されると、ログオンが失敗します。

AD Forest 1 は、`frontenduser@yourforest.com` のような UPN を持つフロントエンドユーザーを作成するために Entra ID に同期されます。

AD Forest 2 には、`frontenduser@yourforest.com` のような UPN を持つバックエンドのシャドウアカウントが含まれています。

原因: B2B SAML の展開で「UPN の曖昧さの問題」が発生しています。Citrix Cloud は、ユーザーのバックエンド ID を検索するためにどのコネクタを使用すべきかを判断できません。

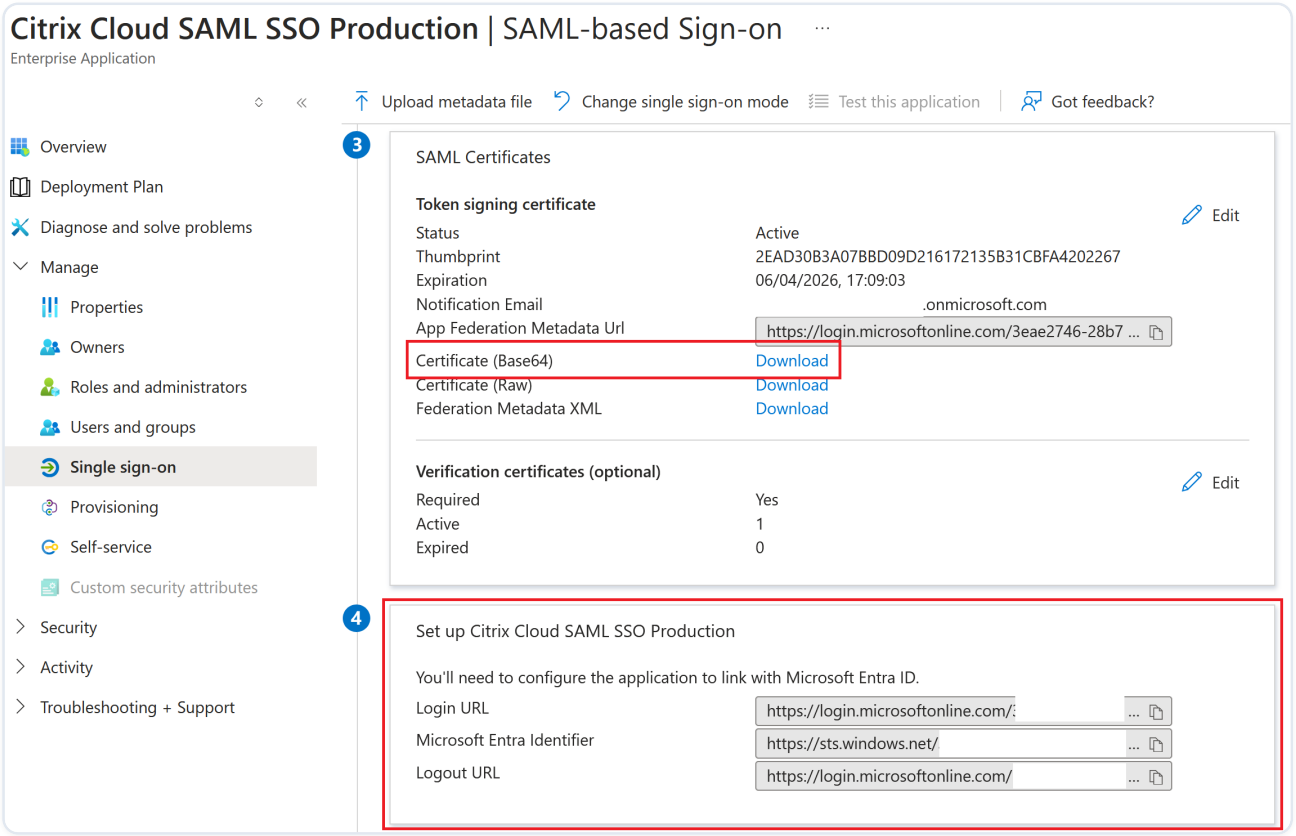
SAML アサーションで **cip_sid** を送信しないでください。

ユーザーの UPN は、Citrix Cloud に接続されている複数の AD フォレストに存在します。

Citrix Cloud SAML 接続を構成する

すべての Citrix ログオンフローは、ストア URL または Citrix Cloud GO URL のいずれかを使用して、サービスプロバイダーによって開始される必要があります。

Entra ID ポータルから Entra ID SAML アプリケーションの SAML エンドポイントを取得し、Citrix Cloud に入力します。



Citrix Cloud SAML 接続内で使用する Entra ID SAML エンドポイントの例

Identity and Access Management > Authentication > Add an identity provider > SAML 内の SAML 接続には、デフォルトの推奨値を使用します。

> **重要:**

> EntraID SSO およびログアウト SAML エンドポイントは同じ URL です。

CITRIX CLOUD のこのフィールド	この値を入力
エンティティ ID	`https://sts.windows.net/<yourEntraIDTenantID>`
認証リクエストに署名	はい
SSOサービスURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、正確
ログアウトURL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
ログアウトリクエストに署名	はい
SLOバインディングメカニズム	HTTP ポスト

ストア認証用のSAMLプロバイダーとしてOktaを構成する

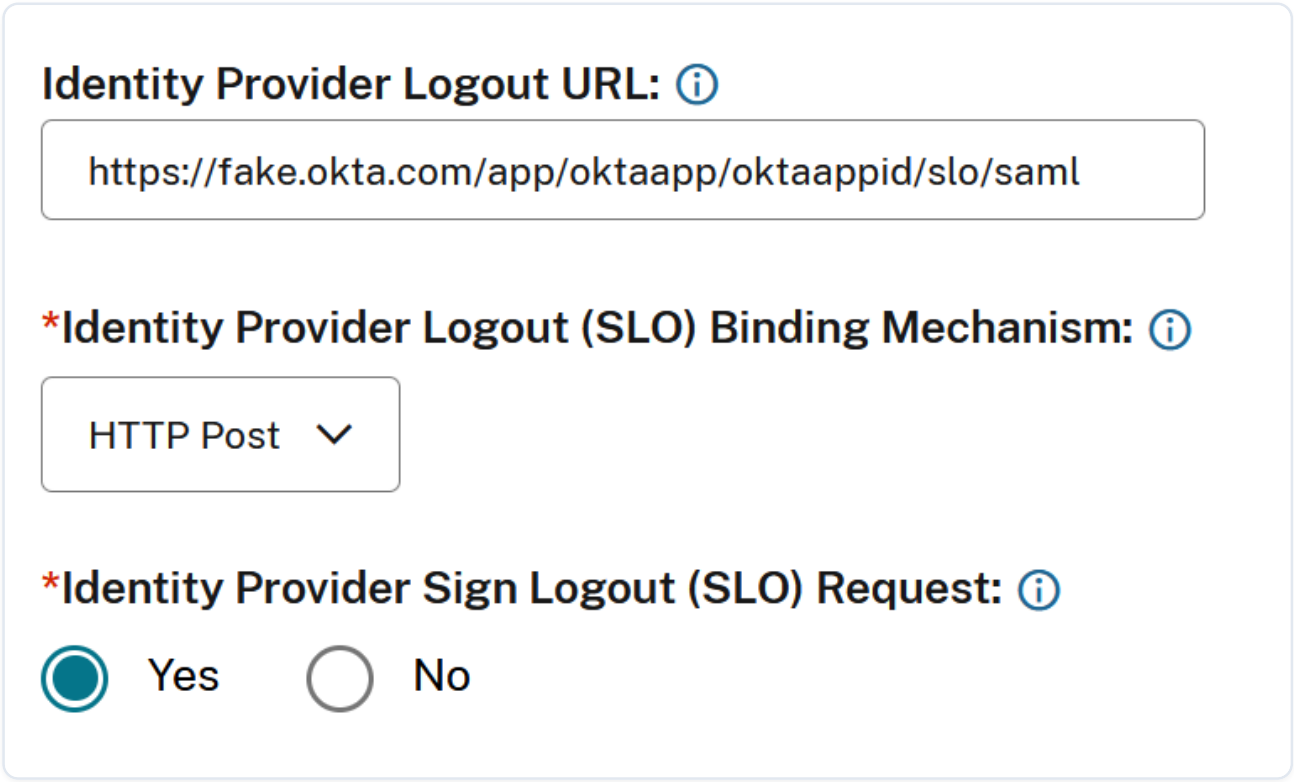
この記事では、Okta SAMLアプリケーションの構成と、Citrix Cloud™とSAMLプロバイダー間の接続に必要な手順について説明します。これらの手順の一部は、SAMLプロバイダーの管理コンソールで実行するアクションについて説明しています。

前提条件

この記事のタスクを完了する前に、以下の前提条件を満たしていることを確認してください。

- Citrix Supportは、Citrix Cloudで**SendNameIDPolicyInSAMLRequest**機能を有効にしています。この機能はリクエストに応じて有効になります。これらの機能の詳細については、「Oktaを使用したSAMLに必要なクラウド機能」を参照してください。
- 以下のいずれかのOktaドメインを使用するOkta組織があること。
  - okta.com
  - オクタ-イーユー・ドットコム
  - oktapreview.com

- Active Directory (AD) をOkta組織と同期していること。
- Okta組織で**認証リクエストの署名**が有効になっていること。
- Citrix CloudとOkta SAMLアプリケーションの両方で、**IDプロバイダーシングルログアウト (SLO)** が構成されていること。SLOが構成されている場合、エンドユーザーがストアからサインアウトすると、OktaおよびOkta SAMLアプリケーションを共有する他のすべてのサービスプロバイダーからもサインアウトします。
- Citrix Cloud内で**IDプロバイダーログアウト (SLO) リクエストの署名**が有効になっていること。
- Citrix Cloud内で**IDプロバイダーログアウトバインディング (SLO)** がHTTPPostであること。



Okta を使用した SAML に必要なクラウド機能

この記事のタスクを完了する前に、Citrix Support に連絡して **SendNameIDPolicyInSAMLRequest** 機能を有効にする必要があります。この機能により、Citrix Cloud は SAML リクエストで **NameID** ポリシーを SAML プロバイダーに **Unspecified** として提供できるようになります。この機能は Okta でのみ使用できます。

これらの機能は、Citrix アカウントにサインインし、Citrix Support Web サイト からチケットを開くことでリクエストできます。

要件

この記事には、Okta Admin コンソールで SAML アプリケーションを作成する タスクが含まれています。このアプリケーションには、Citrix Cloud リージョン用の SAML 署名証明書が必要です。

この証明書は、https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract にあるような抽出ツールを使用して、お使いのリージョンの Citrix Cloud SAML メタデータから抽出できます。Citrix は、必要に応じて提供できるように、Citrix Cloud SAML 証明書を事前に取得することをお勧めします。

このセクションの手順では、https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract の抽出ツールを使用して署名証明書を取得する方法について説明します。

お使いのリージョンの Citrix Cloud メタデータを取得するには：

1. 選択した抽出ツールで、Citrix Cloud リージョンのメタデータ URL を入力します。
    - 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/metadata` を入力します。
    - 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/metadata` を入力します。
    - Citrix Cloud Government リージョンの場合は、`https://saml.cloud.us/saml/metadata` を入力します。
2. **Load** をクリックします。抽出された証明書は、入力した URL の下に表示されます。
3. **Download** をクリックして、証明書を PEM 形式でダウンロードします。

Okta AD エージェントとアカウントを同期する

OktaをSAMLプロバイダーとして使用するには、まずオンプレミスのADをOktaと統合する必要があります。これを行うには、Okta ADエージェントをドメインにインストールし、ADをOkta組織に追加します。Okta ADエージェントの展開に関するガイダンスについては、Okta WebサイトのActive Directory統合の開始を参照してください。

その後、ADユーザーとグループをOktaにインポートします。インポート時には、ADアカウントに関連付けられている次の値を含めます。

- メール
- SID
- UPN
- OID

ADユーザーとグループをOkta組織と同期するには：

1. Okta ADエージェントをインストールして構成します。完全な手順については、Okta Webサイトの次の記事を参照してください。
   - Okta Active Directoryエージェントのインストール
   - Active Directoryのインポートとアカウント設定の構成
   - Active Directoryプロビジョニング設定の構成
2. 手動インポートまたは自動インポートを実行して、ADユーザーとグループをOktaに追加します。Oktaのインポート方法と手順の詳細については、Okta WebサイトのActive Directoryユーザーとグループの管理を参照してください。

ストア認証用のOkta SAMLアプリケーションを構成する

1. SAMLアプリケーションを追加および構成する権限を持つ管理者アカウントを使用して、Okta組織にサインインします。
2. 管理コンソールで、**Applications > Applications > Create App Integration** を選択し、次に **SAML 2.0** を選択します。**Next** を選択します。

   サインイン方法としてSAMLが選択されたOktaコンソール(/en-us/citrix-cloud/media/saml-okta-console-sign-in-method.png)
3. **App Name**に、アプリケーションのわかりやすい名前を入力します。**Next**を選択します。

   アプリ名フィールドが強調表示されたSAML統合構成画面の作成(/en-us/citrix-cloud/media/saml-okta-console-saml-integration-screen.png)
4. **SAML Settings**セクションで、Citrix Cloudサービスプロバイダー（SP）接続を構成します。
   a. **Single sign-on URL**に、Citrix Cloudのお客様のCitrix Cloudリージョンに対応するURLを入力します。
      - お客様IDが欧州連合、米国、またはアジア太平洋南部リージョンにある場合は、`https://saml.cloud.com/saml/acs`と入力します。
      - お客様IDが日本リージョンにある場合は、`https://saml.citrixcloud.jp/saml/acs`と入力します。
      - お客様IDがCitrix Cloud Governmentリージョンにある場合は、`https://saml.cloud.us/saml/acs`と入力します。

   b. **Use this for Recipient and Destination URL**を選択します。

c. **Audience URI (SP Entity ID)**に、Citrix Cloudのお客様のCitrix Cloudリージョンに対応するURLを入力します。

- お客様IDが欧州連合、米国、またはアジア太平洋南部リージョンにある場合は、`https://saml.cloud.com`と入力します。
- お客様IDが日本リージョンにある場合は、`https://saml.citrixcloud.jp`と入力します。
- お客様IDがCitrix Cloud Governmentリージョンにある場合は、`https://saml.cloud.us`と入力します。

d. **Name ID Format**で、**Unspecified**を選択します。Citrix CloudがSAMLリクエスト内で送信するNameIDポリシーは、Okta SAMLアプリケーション内で指定されたNameID形式と一致する必要があります。これらの項目が一致しない場合、**Sign Authentication Request**を有効にするとOktaからエラーが発生します。

e. **Application username**で、**Okta username**を選択します。

この構成の例として、次の図は、米国、EU、およびアジア太平洋南部リージョンでの正しい構成を示しています。

Oktaコンソールでの SAML設定（設定済み）(/en-us/citrix-cloud/media/saml-okta-console-app-configuration-complete.png)

> **重要:**
>
> **Name ID**設定は**Unspecified**として構成する必要があります。この設定に異なる値を使用すると、SAMLサインインが失敗します。

f. **Show Advanced Settings**をクリックし、次の設定を構成します。

- **Response**で、**Signed**を選択します。
- **Assertion Signature**で、**Signed**を選択します。
- **Signature Algorithm**で、**RSA-SHA256**を選択します。
- **Assertion Encryption**で、**Unencrypted**を選択します。

g. **Signature Certificate**で、Citrix Cloudリージョン用のSAML署名証明書をPEM形式でアップロードします。SAML署名証明書の取得手順については、この記事の要件を参照してください。

h. 「**シングルログアウトを有効にする**」で、「**アプリケーションによるシングルログアウトの開始を許可する**」を選択します。

i. **Single Logout URL**に、Citrix Cloudリージョンに対応するURLを入力します。

- 欧州連合、米国、およびアジア太平洋南部リージョンの場合は、`https://saml.cloud.com/saml/logout/callback`と入力します。
- 日本リージョンの場合は、`https://saml.citrixcloud.jp/saml/saml/logout/callback`と入力します。
- Citrix Cloud Governmentの場合は、`https://saml.cloud.us/saml/logout/callback`と入力します。

j. 「**SP Issuer**」に、以前「**Audience URI (SP Entity ID)**」に入力した値（このタスクのステップ4c）を入力します。

k. 「**署名済みリクエスト**」で、「**署名証明書でSAMLリクエストを検証する**」を選択します。

次の画像は、米国、EU、およびアジア太平洋南部リージョンにおける正しい構成を示しています。

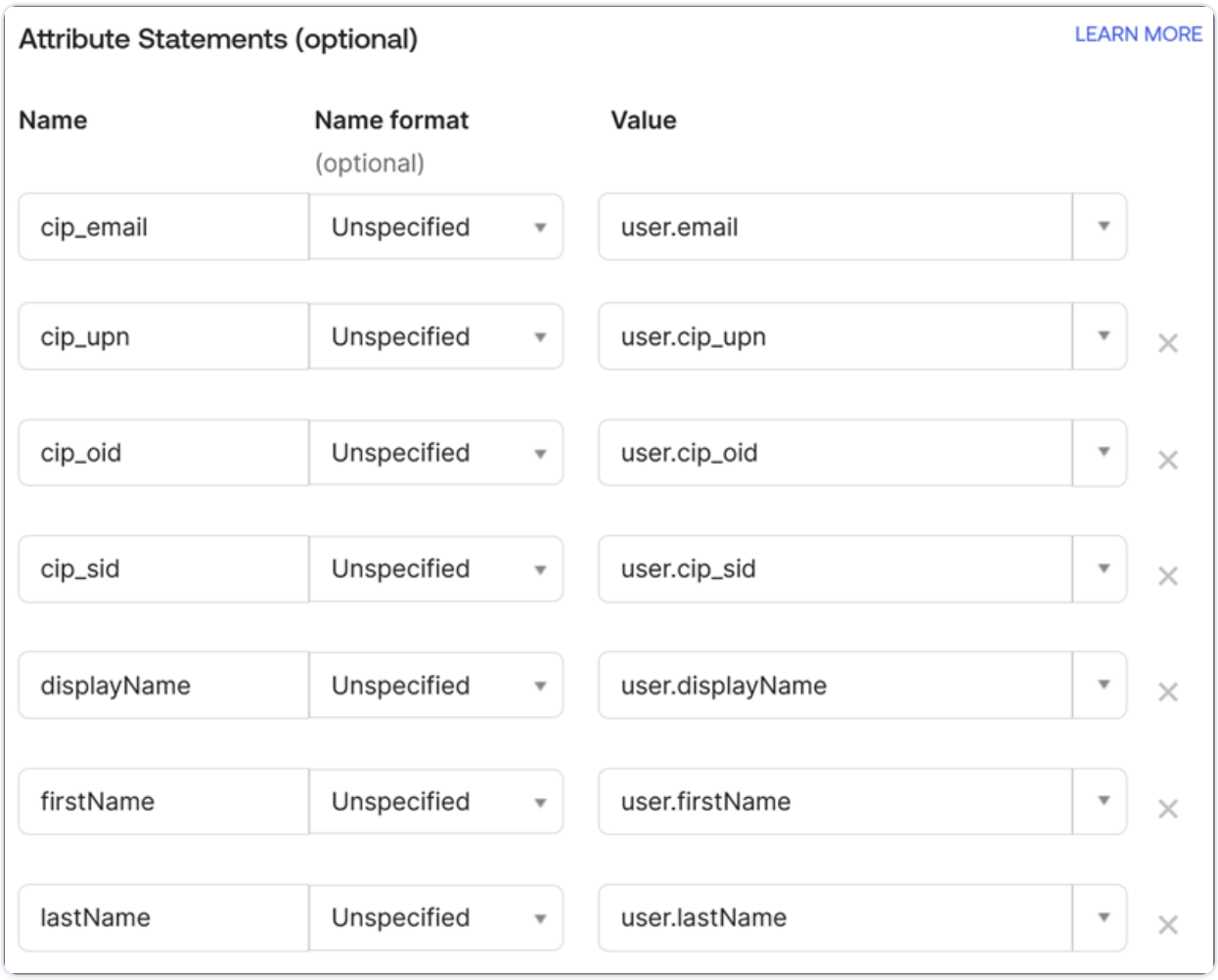
Oktaコンソールでの詳細SAML設定（設定済み）(/en-us/citrix-cloud/media/saml-okta-show-advanced-settings-console.png)

l. その他のすべての詳細設定については、デフォルト値を受け入れます。

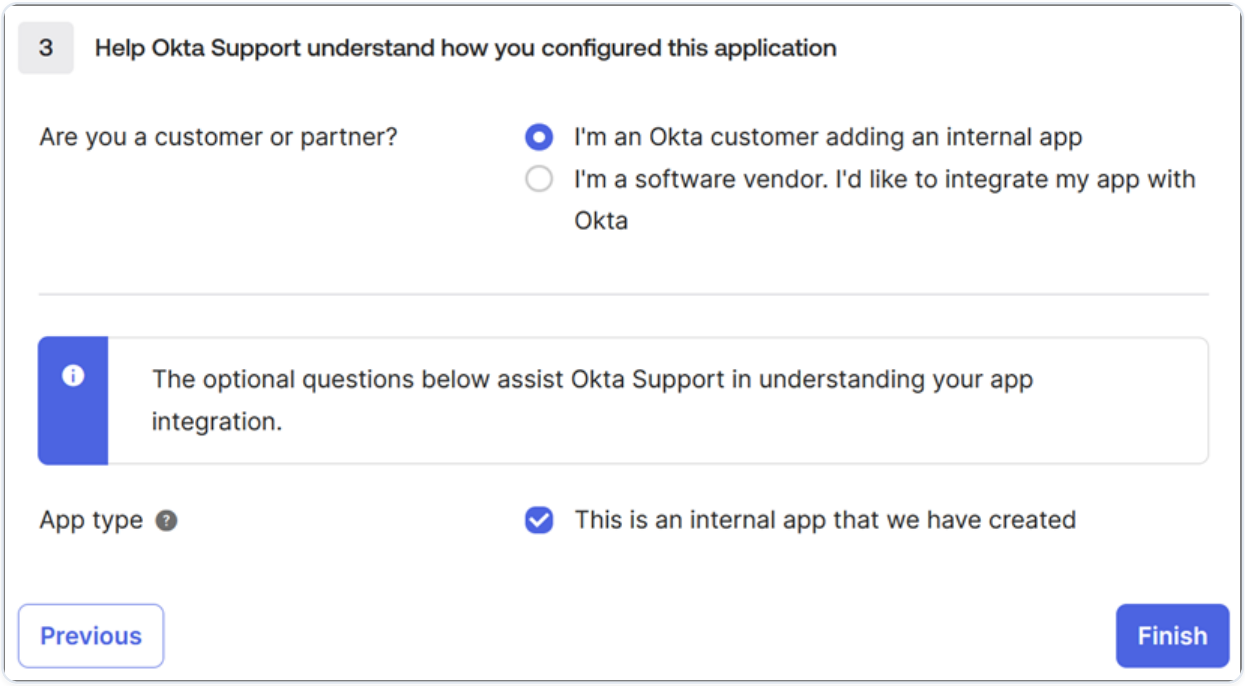
Oktaコンソールでの詳細設定（デフォルト値）(/en-us/citrix-cloud/media/saml-okta-default-advanced-settings.png)

5. 「**Attribute Statements (optional)**」の下で、次の表に示すように、「**Name**」、「**Name format**」、「**Value**」の値を入力します。

名前	名前形式	値
cip_upn	未指定	user.cip_upn
displayName	未指定	user.displayName
firstName	未指定	user.givenName
lastName	未指定	user.familyName



6. **次へ**を選択します。Okta構成ステートメントが表示されます。



7. **お客様ですか、それともパートナーですか？**で、**私は内部アプリを追加するOktaのお客様です**を選択します。

8. **アプリの種類**で、**これは当社が作成した内部アプリです**を選択します。
9. **Finish** を選択して構成を保存します。SAMLアプリケーションのプロファイルページが表示され、**Sign On** タブの内容が表示されます。

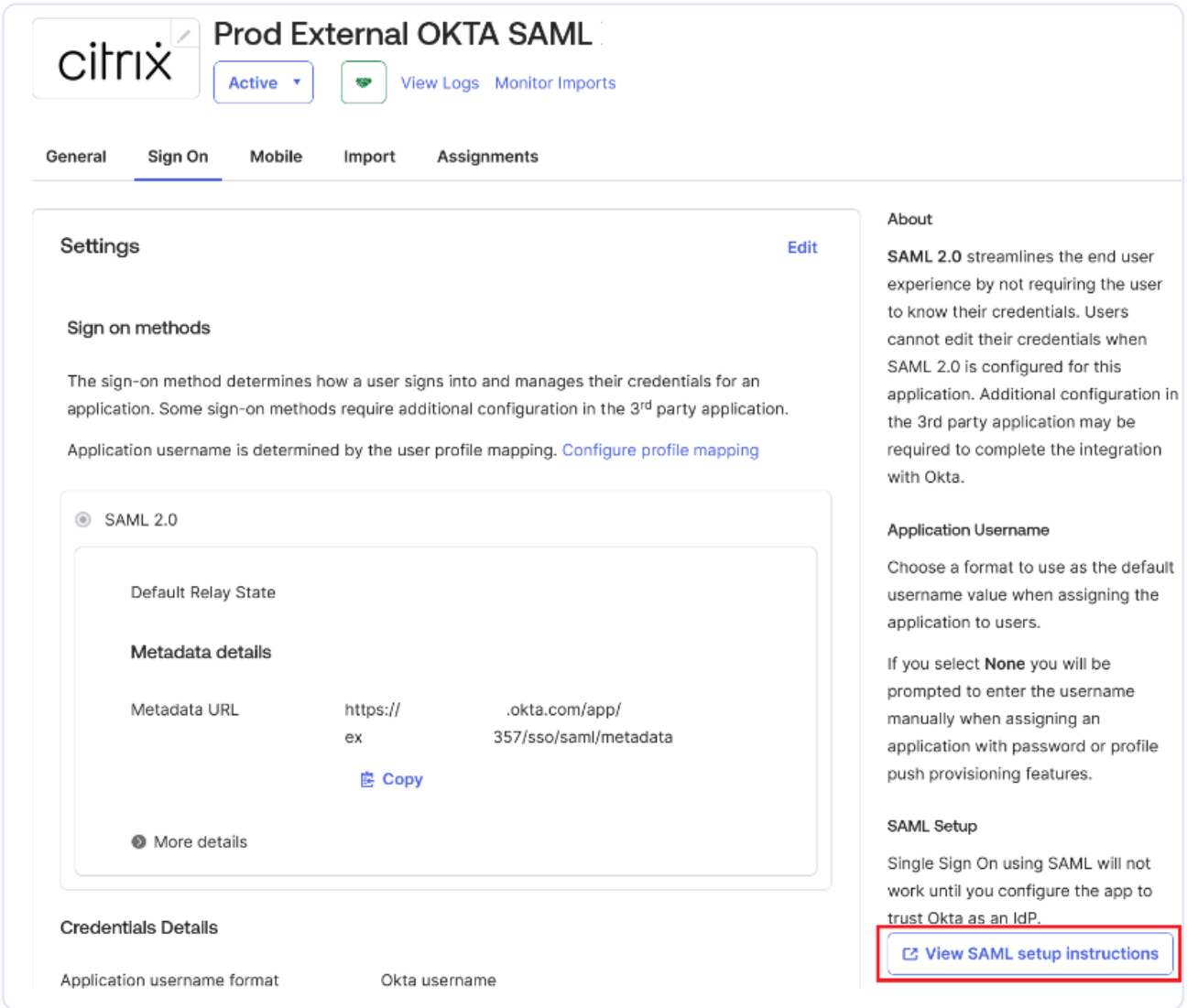
構成後、**Assignments** タブを選択し、ユーザーとグループをSAMLアプリケーションに割り当てます。

Citrix Cloud SAML接続を構成する

すべてのCitrixログオンフローは、ストアURLまたはCitrix Cloud GO URLのいずれかを使用して、サービスプロバイダーによって開始される必要があります。

IDおよびアクセス管理 → **認証** → **IDプロバイダーの追加** → **SAML** 内のSAML接続には、デフォルトの推奨値を使用します。

Oktaポータルから、Citrix Cloudに入力するOkta SAMLアプリケーションのSAMLエンドポイントを取得します。



How to Configure SAML 2.0 for Prod External OKTA SAML Application

Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure Prod External OKTA SAML

1. Identity Provider Single Sign-On URL:

```
https://                .okta.com/app/citrix-                                _1/exkp        HA357/sso/saml
```

2. Identity Provider Single Logout URL:

```
https://                .okta.com/app/citrix-                                _1/exkp        HA357/slo/saml
```

3. Identity Provider Issuer:

```
http://www.okta.com/ex              HA357
```

4. X.509 Certificate:

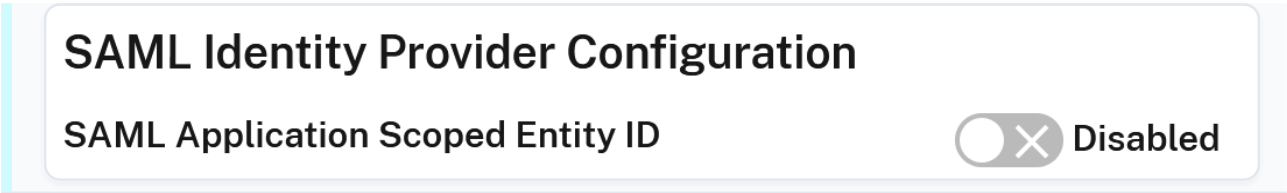
```
-----BEGIN CERTIFICATE-----
MIIDrDCCApSgAwIBAgIGAYXogrzaMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU

aQRZmmwyqNuSGN2CH1KVSkYZvSxxgn9LFA7Y/EER9lp08/qXGE3BgFm93m0fS2zB9HYDWA0L5+3h
bN9bf95Eozn6kii4JO7LP4pJRCTpLu7zgGcSeNneu+A=
-----END CERTIFICATE-----
```

Download certificate

重要:

Oktaはスコープ付きエンティティを必要としません。このドキュメントでは、スコープ付きエンティティが無効になっていることを前提としています。スコープ付きエンティティとは何か、およびいつ必要になるかについては、スコープ付きエンティティに関するCitrixドキュメントを参照してください。デフォルトのCitrix Cloud SAML接続設定を使用し、**スコープ付きエンティティ**を無効のままにします。



CITRIX CLOUDのこのフィールド	この値を入力
エンティティID	`http://www.okta.com/<oktaSAMLappID>`
認証リクエストに署名	はい
SSOサービスURL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/sso/saml`
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、完全一致
ログアウトURL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/slo/saml`
ログアウト要求に署名	はい
SLOバインディングメカニズム	HTTP ポスト

ストアおよび Citrix Cloud™ 用の SAML プロバイダーとしてオンプレミス PingFederate サーバーを構成する

この記事は、Citrix® と Ping の両方のエンジニアの協力によって作成され、執筆時点での技術的な正確性を確保するために両者によってレビューされています。SAML プロバイダーとして使用するためのオンプレミス PingFederate サーバーのプロビジョニング、構成、およびライセンス供与の方法については、Ping のドキュメントを参照してください。これは本記事の範囲外です。

このドキュメントは、PingFederate バージョン 11.3 および 12 を使用して作成されました。

前提条件

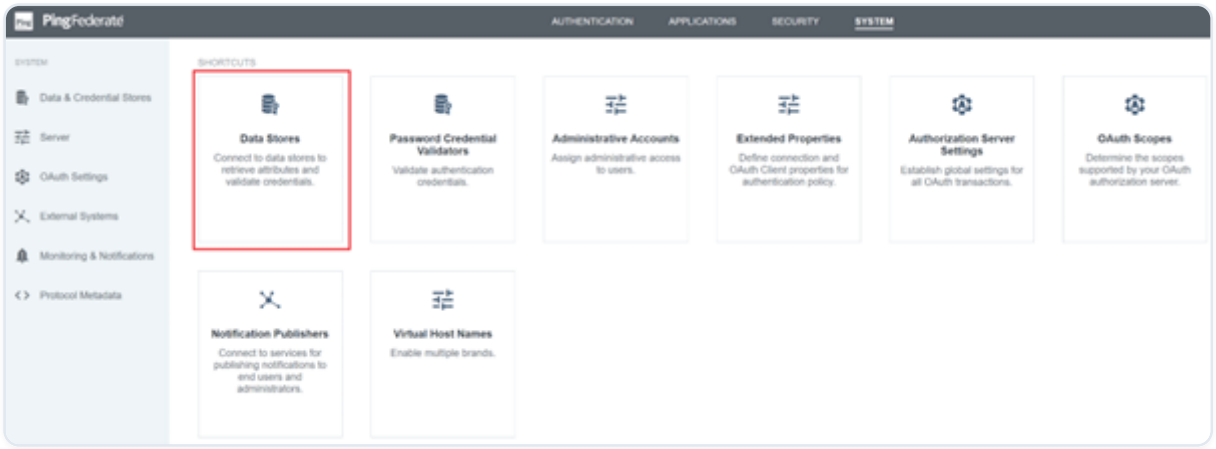
この記事では SAML 構成について具体的に説明します。以下の条件が満たされていることを確認してください。

- 組織内にオンプレミス PingFederate サーバーをすでにプロビジョニングし、必要なライセンスを取得していること。詳細については、「PingFederate のインストール」を参照してください。
- PingFederate サーバーにサポートされているバージョンの Java をインストールしている必要があります。サポートされている Java バージョンについては、Ping Identity のドキュメントを参照してください。詳細については、「Java PingFederate の要件」を参照してください。
- ストア/Citrix Cloud 管理コンソールの SAML ログオンプロセス中に、Citrix Cloud がオンプレミス PingFederate サーバーにリダイレクトできるように、必要なネットワークおよびファイアウォールルールを構成していること。詳細については、「PingFederate のネットワーク要件」を参照してください。
- PingFederate サーバーのサーバー証明書として機能できる、公開署名された x509 証明書を PingFederate サーバーにインポートしていること。
- IdP の SAML 署名証明書として機能できる、公開署名された x509 証明書を PingFederate サーバーにインポートしていること。この証明書は、SAML 接続プロセス中に Citrix Cloud にアップロードする必要があります。
- オンプレミス Active Directory を PingFederate に接続していること。詳細については、「PingFederate LDAP データストア」を参照してください。

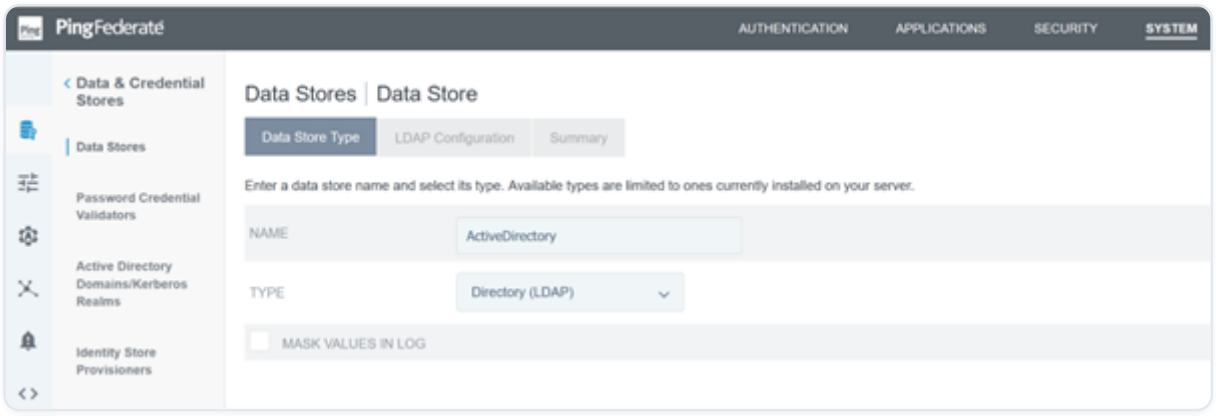
> **注:**
>
> Citrix Cloud およびストアで使用するために PingFederate を構成する際は、個々の SAML 設定が何をするのかを理解し、ここで提供される手順を補完するために PingFederate のドキュメントを参照してください。

PingFederate 内のデータストアを使用して AD ドメインへの Active Directory 接続を構成する

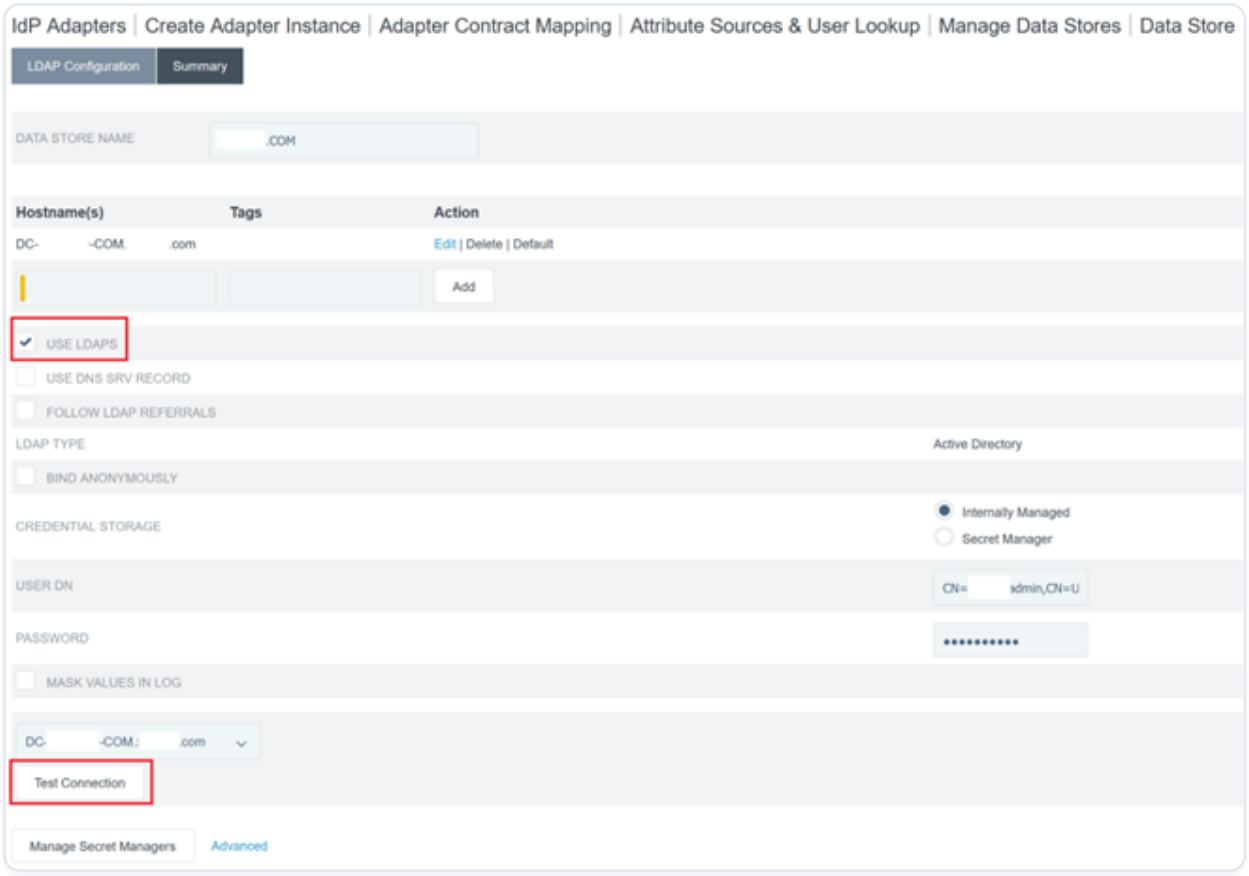
1. データストア内で Active Directory 接続を構成します。



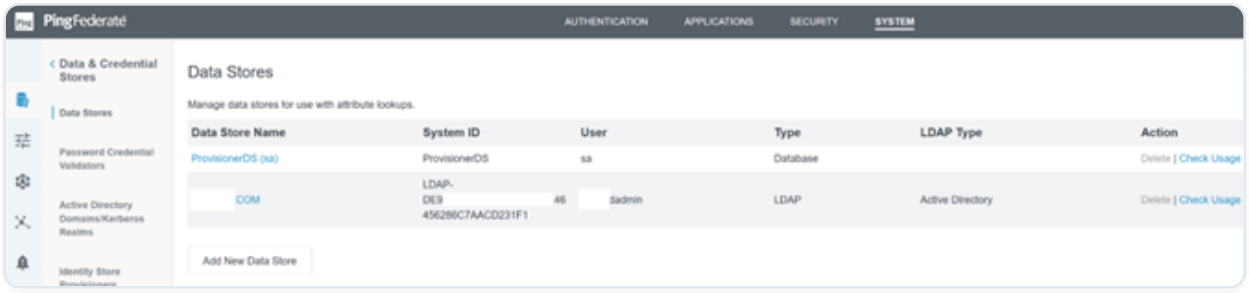
2. タイプを**Directory (LDAP)**として選択します。



3. LDAPS接続用にドメインコントローラーを構成し、ホスト名フィールドにドメインコントローラーのFQDNのリストを追加します。次に、**Test Connection**をクリックします。

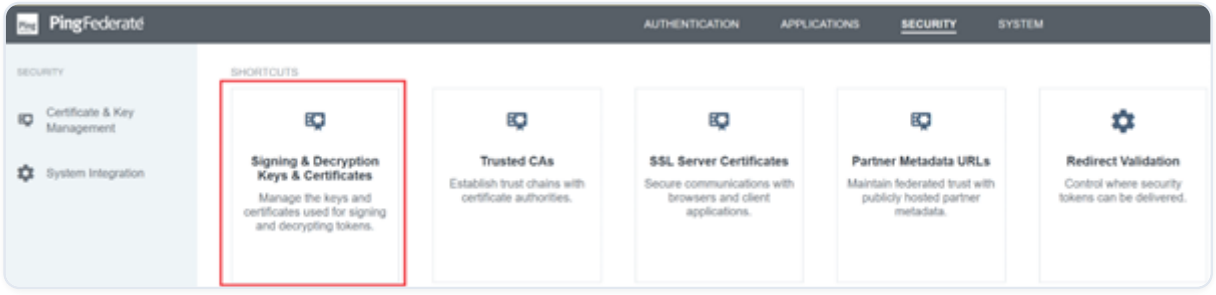


4. 構成が完了すると、Active Directory接続は次の例のようになります。



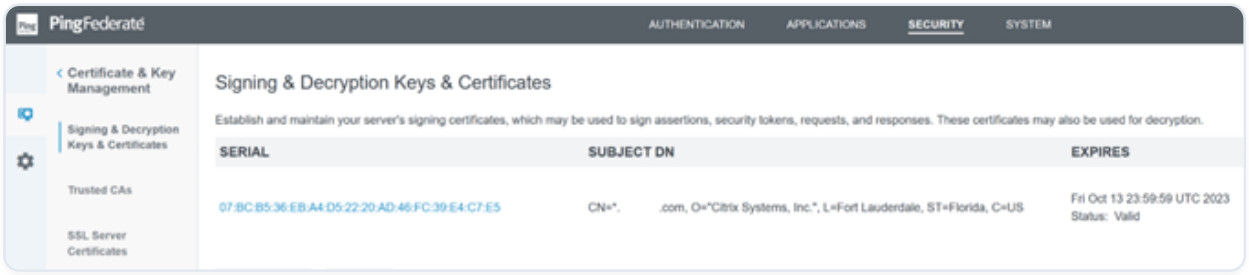
Citrix Cloud SAML署名証明書をアップロードする

1. **Security**タブをクリックします
2. **Signing & Decryption Keys and Certificates**内でPingFederateが使用するSAML署名証明書をアップロードします。

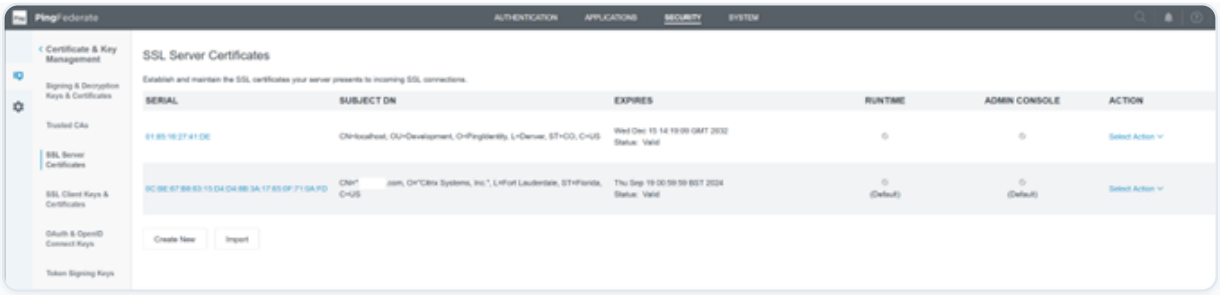


> **注：**
>
> この例で使用されている証明書は、公開署名されたDigicert `pingfederateserver.domain.com` 証明書です。

3. PingFederateサーバーのSAML署名証明書の署名に使用されたCA証明書をアップロードします。



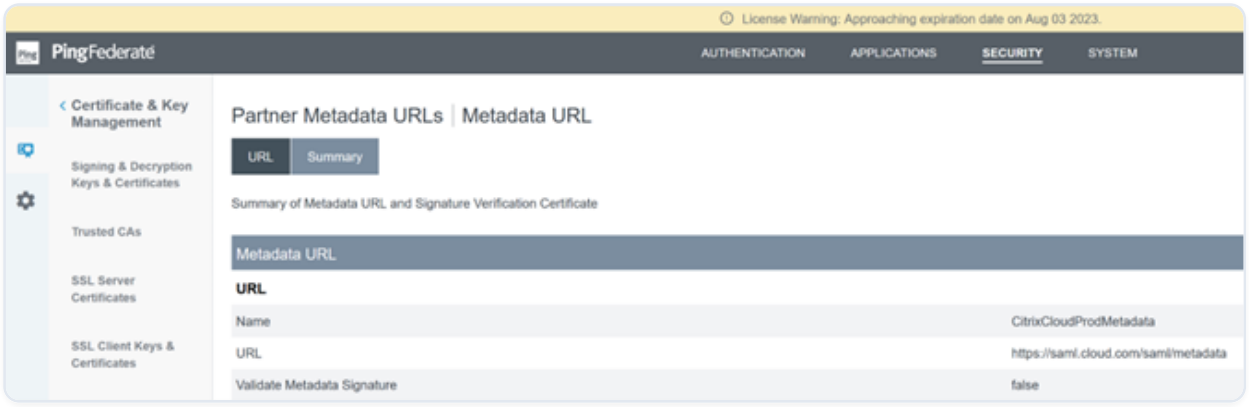
> **注:**
>
> PingFederateサーバー証明書とSAML署名証明書は、同じSSL証明書でも、異なるSSL証明書でも使用できます。SAML接続を構成する際に、SAML署名証明書のコピーをCitrix Cloudに提供する必要があります。



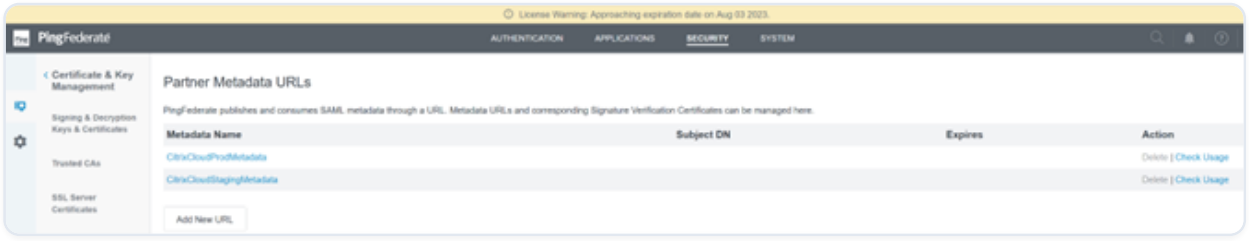
Citrix Cloudメタデータをアップロードする

1. Citrix Cloudメタデータの名前を指定し、Citrix Cloudテナントが配置されているCitrix Cloudリージョンに対応するメタデータURLを入力します。

   - `<https://saml.cloud.com/saml/metadata>` - 商用EU、米国、およびAPS
   - `<https://saml.citrixcloud.jp/saml/metadata>` - 日本
   - `<https://saml.cloud.us/saml/metadata>` - 政府



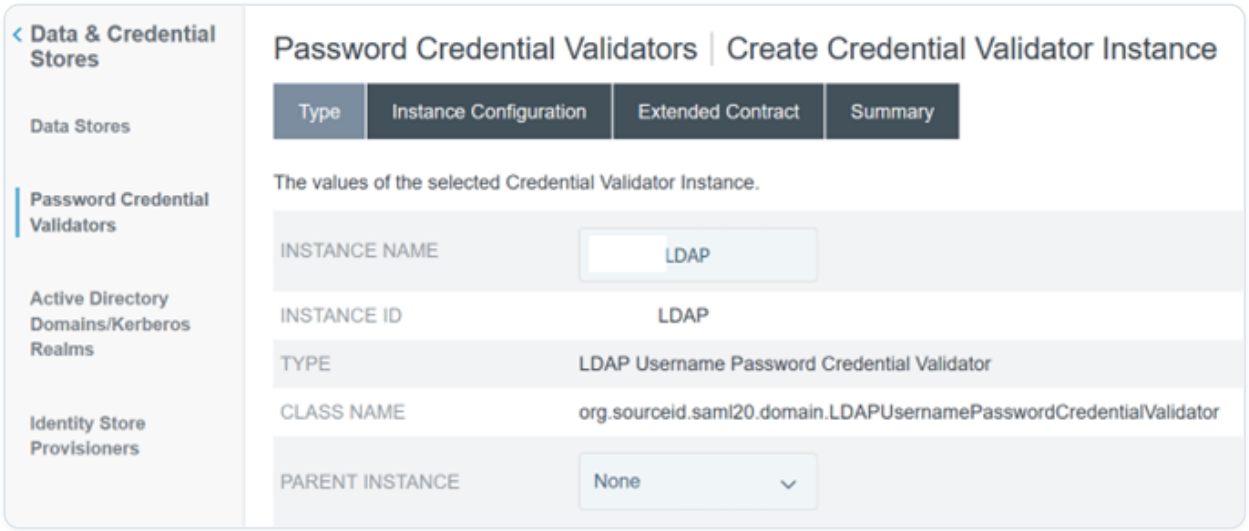
2. 構成が完了すると、Citrix Cloudメタデータ構成は次の例のようになります。



PingFederate内でパスワード資格情報バリデーターを構成する

詳細については、PingFederateパスワード資格情報バリデーターを参照してください。

1. パスワード資格情報バリデーターの種類をLDAPユーザー名とパスワードとして構成します。



2. 「**インスタンス構成**」を構成します。以前に構成したADドメイン接続とデータストアを選択しますPingFederate内でデータストアを使用してADドメインへのActive Directory接続を構成する。例に示すように、適切なLDAPフィルターを入力します。 `(((sAMAccountName=${username})(userPrincipalName=${username}))`

   インスタンス構成を構成する(/en-us/citrix-cloud/media/instance-config.png)

> **注:**

> この例のフィルターは、sAMAccountNameとuserPrincipalNameの両方のADユーザー名形式に対応しており、エンドユーザーはこれらの形式のいずれかを使用してストアまたはCitrix Cloudにサインインできます。

3. 「**拡張契約**」を構成します。

   拡張契約(/en-us/citrix-cloud/media/extended-contract.png)

4. 「**パスワード資格情報バリデーター**」の概要は、この例のようになるはずです。

   パスワード資格情報バリデーター(/en-us/citrix-cloud/media/password-credential-summary.png)

PingFederate内でIDPアダプターを構成する

詳細については、「PingFederate HTMLフォームアダプター」を参照してください。

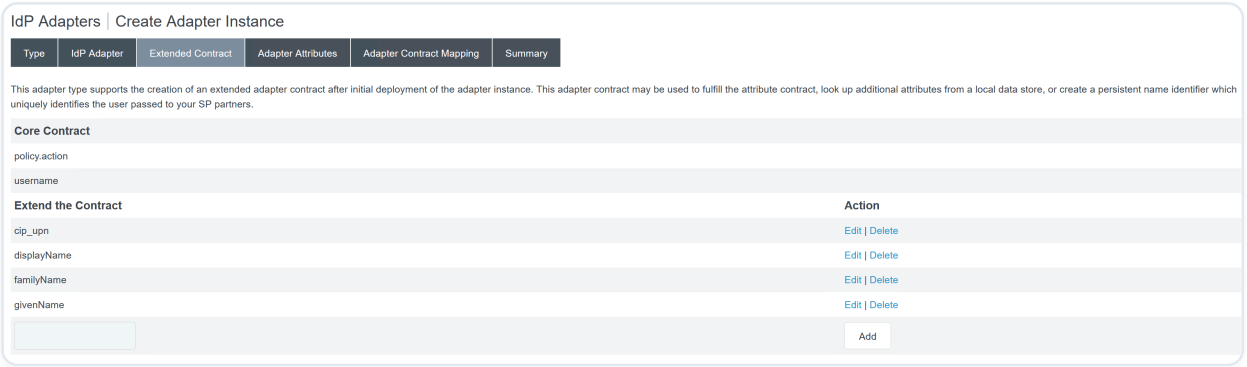
1. HTMLフォームIDPアダプタータイプの新しいIDPアダプターを作成します。

   アダプターインスタンスを作成する(/en-us/citrix-cloud/media/create-adapter-instance.png)

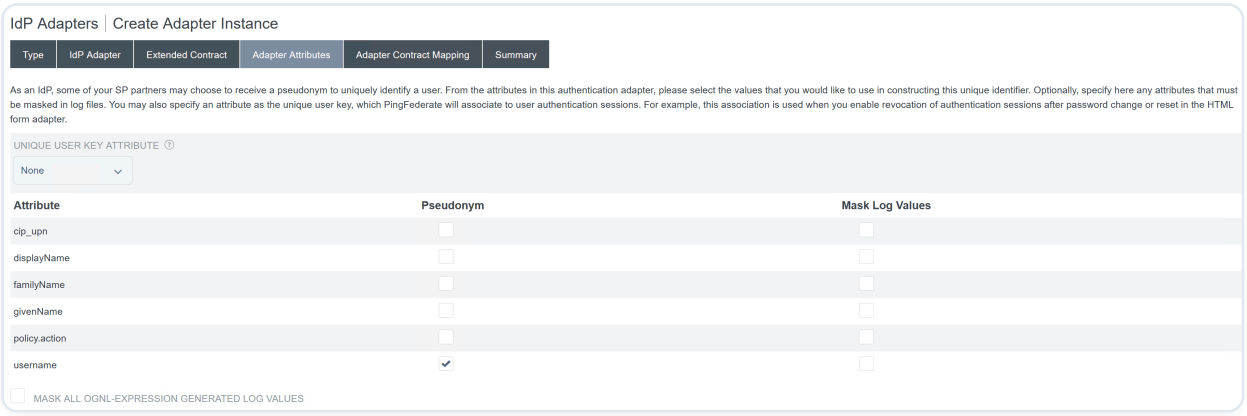
2. 以前に構成した既存の「**パスワード資格情報バリデーター**」を選択し、IDPアダプターを構成します。詳細については、「PingFederate内でパスワード資格情報バリデーターを構成する」を参照してください。

   パスワード資格情報バリデーター(/en-us/citrix-cloud/media/password-credential-validator.png)

3. SAMLログオン中にCitrix Cloudまたはストアに渡されるSAML属性を使用して、「**拡張契約**」を構成します。



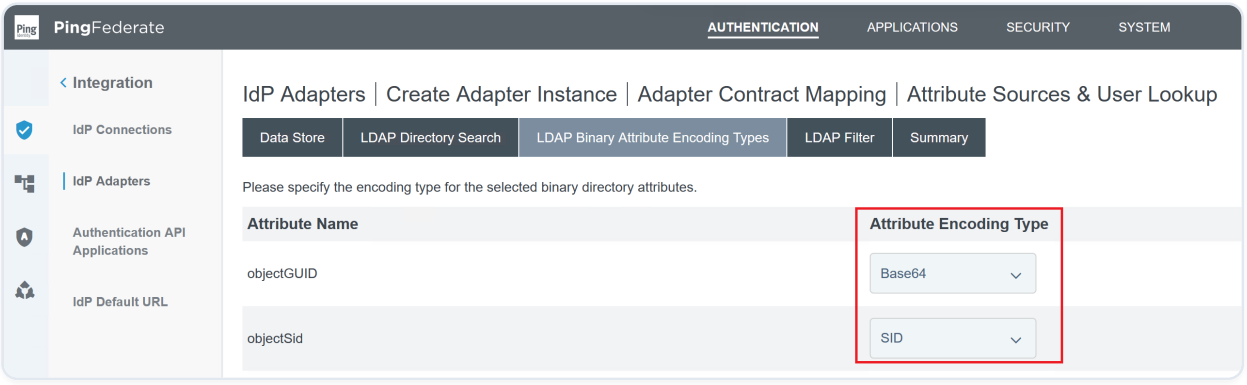
4. **アダプター属性**を構成します。



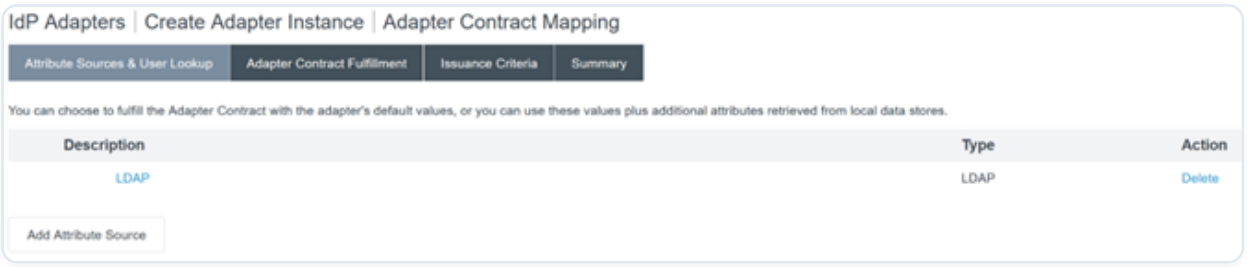
5. SAML属性がAD IDのLDAPユーザー属性にマッピングされる**アダプター契約マッピング**を構成します。**アダプター契約を構成**をクリックします。

   2つのバイナリ属性のエンコーディングを設定します。

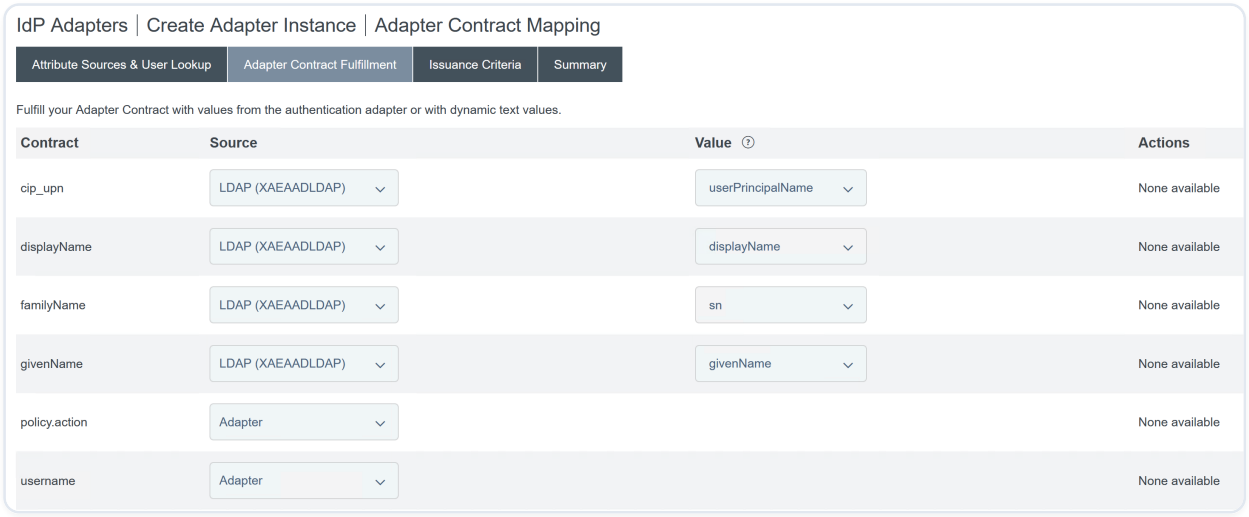
   - objectGUID = base64 (エンコード済み)
   - objectSid = SID (エンコードなし)



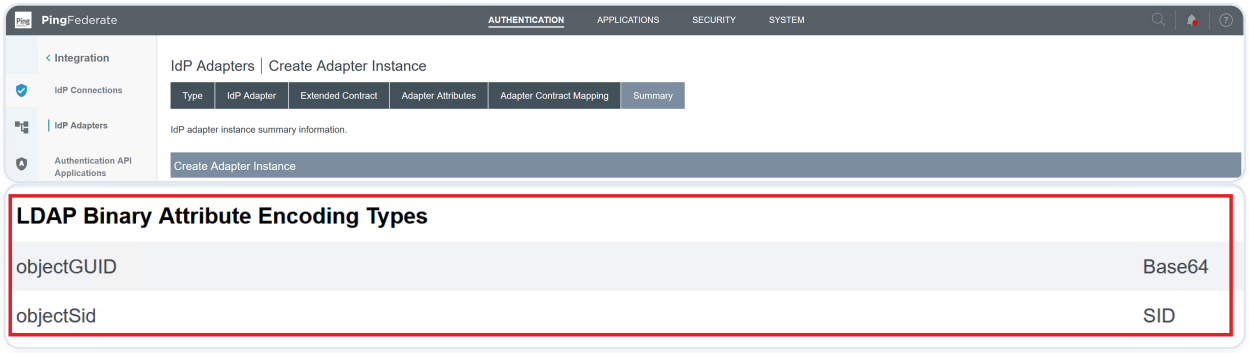
6. **属性ソースとユーザー検索**を構成します。



7. **アダプター契約の履行**を構成します。ユーザー属性データのソースとして、**LDAP**とActive Directoryデータストアの名前を選択します。値は、`objectGUID`や`objectSid`などのユーザーのActive Directory属性です。



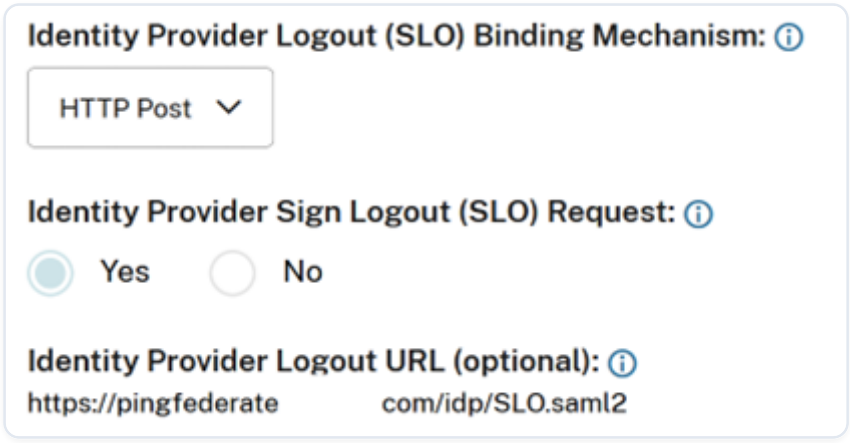
8. バイナリ属性のエンコーディングは、**HTMLフォームアダプター**の概要で、以下のスクリーンショットに示すように表示されます。



Citrix CloudまたはWorkspacesのサービスプロバイダー接続（SAMLアプリケーション）の構成

以下に示すPingFederateのサンプル構成は、組織内で以下のSAML認証要件が満たされていることを前提としています。

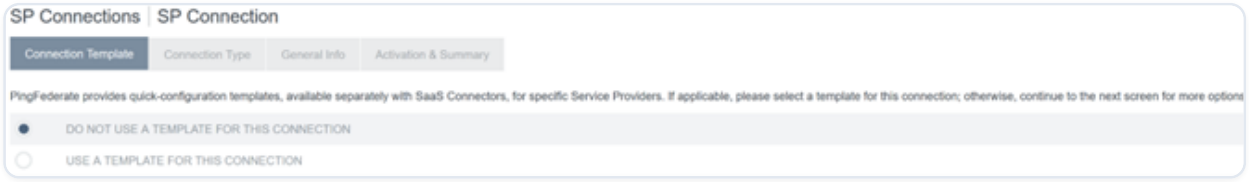
- ストア/Citrix Cloud管理コンソールから送信されるSAML認証要求は署名されている必要があります。
- SSOおよびSLO要求の両方にSAML HTTP POSTバインディングが使用されます。
- シングルログアウト（SLO）は組織内の要件です。エンドユーザーがストアまたはCitrix Cloud管理コンソールからサインアウトすると、ユーザーをサインアウトさせるためにSAML SLO要求がCitrix CloudからSAMLプロバイダー（IdP）に送信されます。
- PingFederateは、サインアウトを開始するために署名付きHTTP POST要求を必要とします。SAMLプロバイダーは署名付きSLO要求を必要とします。



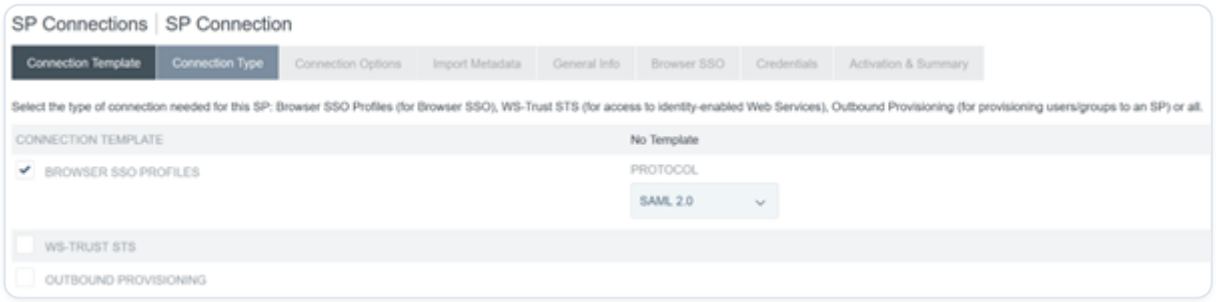
詳細については、「PingFederate SP管理」を参照してください。

手順

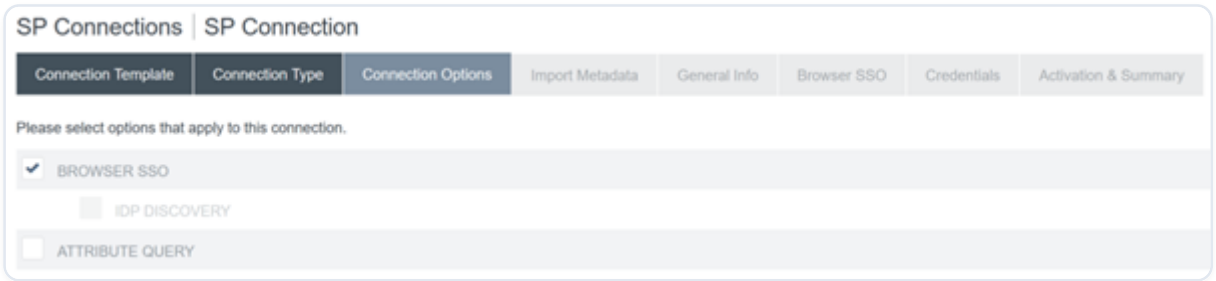
1. **接続テンプレート**を構成します。



2. **接続タイプ**を構成し、**ブラウザーSSOプロファイルとSAML 2.0**を選択します。



3. **接続オプション**を構成します。



4. Citrix Cloudメタデータをインポートします。URLを選択し、以前作成した `CitrixCloudProdMetadata` URLを選択して、**Load Metadata**をクリックします。

   Citrix Cloudメタデータのインポート(/en-us/citrix-cloud/media/import-cc-metadata.png)

5. **General Info**を構成します。サービスプロバイダー接続エンティティID、ベースURL、および接続名を、Citrix Cloudのお客様の地域に対応するCitrix Cloud SAMLエンドポイントに設定します。

   - `<https://saml.cloud.com>` - 商用EU、米国、およびAPS
   - `<https://saml.citrixcloud.jp>` - 日本
   - `<https://saml.cloud.us>` - 政府

   一般情報の構成(/en-us/citrix-cloud/media/configure-general-info.png)

6. **プロトコル設定**を構成します。

   プロトコル設定の構成(/en-us/citrix-cloud/media/configure-protocol-settings.png)

7. デフォルトの**アサーションの有効期間**設定を使用します。

   アサーションの有効期間設定(/en-us/citrix-cloud/media/default-assertion-lifetime-settings.png)

8. SAMLアサーションの作成を構成します。

   a. **アサーションの作成を構成**をクリックします。

      アサーション作成の構成(/en-us/citrix-cloud/media/configure-assertion-creation.png)

   b. **標準**を選択します。

      「標準を選択」(/en-us/citrix-cloud/media/standard.png)

9. 「**属性契約**」を構成します。

   「属性契約を構成」(/en-us/citrix-cloud/media/configure-attribute-contract.png)

10. 「**アダプターインスタンス**」を構成します。

    「アダプターインスタンスを構成」(/en-us/citrix-cloud/media/sp-connection-adapter-instance.png)

11. 「**マッピング方法**」を構成します。

    「マッピング方法を構成」(/en-us/citrix-cloud/media/sp-connection-mapping-method.png)

12. 「**属性契約の履行**」を構成します。

    「属性契約の履行を構成」(/en-us/citrix-cloud/media/sp-connection-attribute-contract-fulfillment.png)

13. 「**発行基準**」を条件なしのデフォルトとして構成します。

「発行基準を構成」(/en-us/citrix-cloud/media/configure-issuance-criteria.png)

14. 完了した「**IDPアダプターマッピング**」は次のようになります。

    「完了したIDPアダプターマッピング」(/en-us/citrix-cloud/media/sp-connection-adapter-instance-summary.png)

15. 「**プロトコル設定**」を構成します。Citrix Cloudで必要とされるSAMLパスは、PingFederateサーバーのベースURLに追加されます。エンドポイントURLフィールドに完全なパスを入力することでベースURLを上書きすることは可能ですが、通常は不要であり、推奨されません。
    ベースURL - `<https://youpingfederateserver.domain.com>`

    a. SAMLパスをPingFederateサーバーのベースURLに追加するアサーションコンシューマーサービスURLを構成します。エンドポイントURL - `/saml/acs`

       アサーションコンシューマーサービスURLを構成する(/en-us/citrix-cloud/media/assertion-consumer-service-url.png)

    b. **SLOサービスURL**を構成します。EndpointURL - `/saml/logout/callback`

       SLOサービスURLを構成する(/en-us/citrix-cloud/media/configure-slo-service-url.png)

> **重要:**
>
> ストアまたはCitrix Cloudからサインアウトする際にSLOを実行したい場合は、Citrix Cloud SAML接続で、これに一致するようにPingFederateログアウトURLを構成する必要があります。SAML接続内でログアウトURLを構成しないと、エンドユーザーはストアからのみサインアウトし、PingFederateからはサインアウトしません。

    a. **許可されるSAMLバインディング**を構成します。

       許可されるSAMLバインディングを構成する(/en-us/citrix-cloud/media/configure-allow-saml-bindings.png)

    b. **署名ポリシー**を構成します。

       署名ポリシーを構成する(/en-us/citrix-cloud/media/configure-signature-policy.png)

> **重要:**

> SAML署名設定は、SAML接続の両側で一貫して構成する必要があります。ストアまたはCitrix Cloud (SP) は、署名付きSSOおよびSLOリクエストを送信するように構成する必要があります。

a. PingFederate (IDP) は、Citrix Cloud SAML署名検証証明書を使用して、署名付きリクエストの適用を実行するように構成する必要があります。

   署名付きリクエストの適用(/en-us/citrix-cloud/media/signature-policy.png)

b. **暗号化ポリシー**を構成します。

   暗号化ポリシーを構成する(/en-us/citrix-cloud/media/sp-connection-encryption-policy.png)

> **注:**
>
> 最初のセットアップとテスト中は、アサーション内のSAML属性の欠落や誤りに関する問題をデバッグできるように、暗号化を**NONE**に設定することをお勧めします。暗号化されたアサーションが必要な場合は、ストアまたはCitrix Cloudへのログオンが成功し、すべてのリソースが正常に列挙されて起動できることを確認した後で、暗号化を有効にすることをお勧めします。暗号化が有効な状態でSAMLに関する問題をデバッグすることは、SAMLアサーションのプレーンテキストの内容を表示できない場合、不可能になります。

c. **概要**タブを確認します。

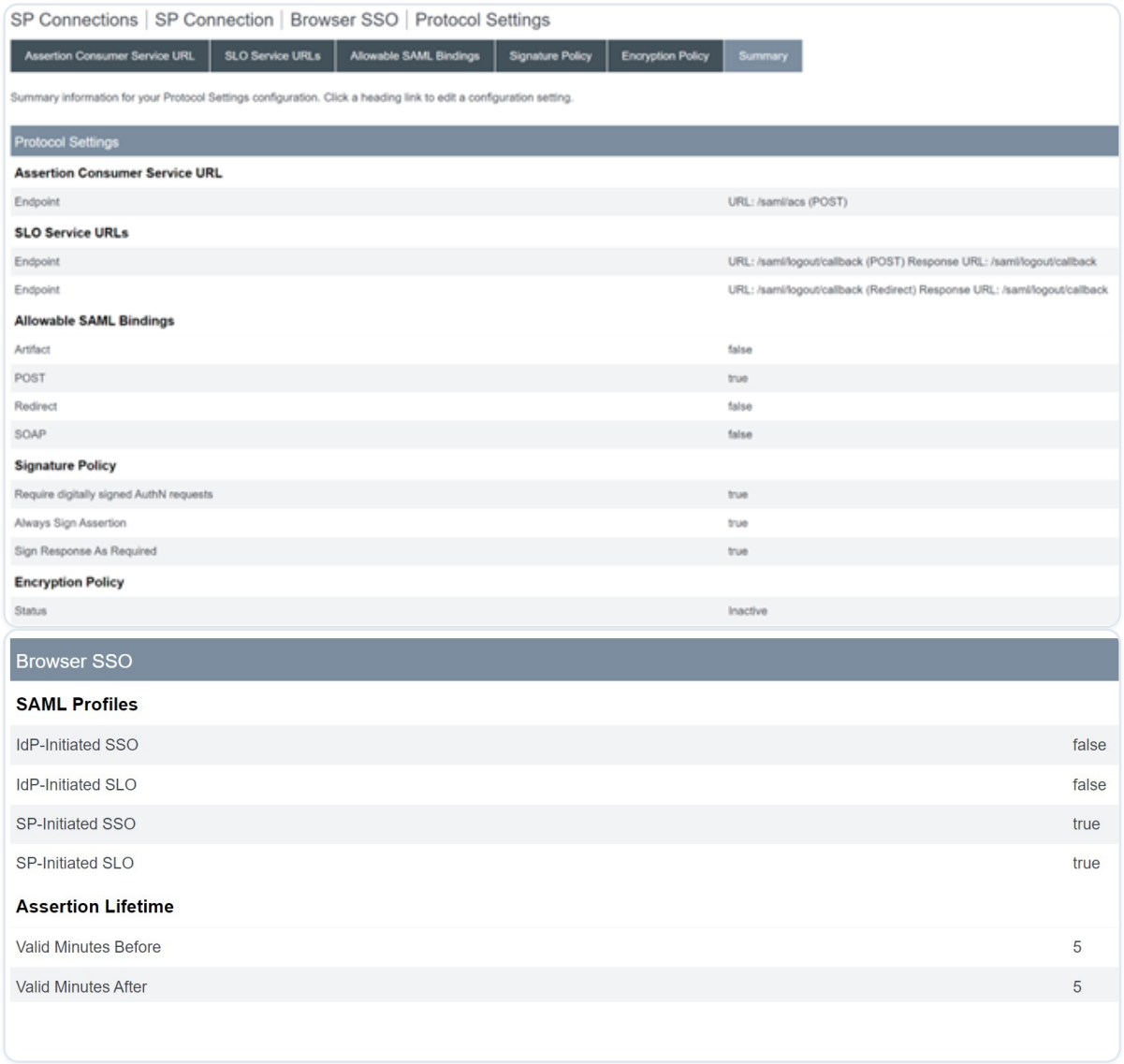
SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

d. **Citrix Cloudサービスプロバイダー (SP) 接続**を確認します。**Citrix Cloud SP接続**が構成されると、この例のようになります。



SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	familyName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	givenName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
familyName	familyName (Adapter)
givenName	givenName (Adapter)

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	CN=*. .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> **ヒント:**
>
> SP接続のアクティベーションと概要ページを使用して、SAMLアプリケーションを確認し、デバッグ目的で利用できます。このページでは、迅速かつ簡単に構成変更を行うことができます。SP接続のアクティベーションと概要ページでは、SAML構成の任意のサブセクションのタイトルをクリックすることで、そのセクションに移動できます。赤で強調表示されているいずれかのタイトルをクリックして、これらの設定を更新します。

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. 完了した**Citrix Cloud SP接続**は、リストにこのように表示されます。



17. SP接続をXMLファイルの形式でエクスポートできます。Citrixは、Citrix Cloudおよびストアでテストした後、SP接続のバックアップを取ることを推奨します。



Citrix Cloud SAML接続を構成する

すべてのCitrixログオンフローは、ストアURLまたはCitrix Cloud GO URLのいずれかを使用して、サービスプロバイダーによって開始される必要があります。

「**IDおよびアクセス管理 → 認証 → IDプロバイダーの追加 → SAML**」内のSAML接続には、推奨されるデフォルト値を使用します。

CITRIX CLOUD™

CITRIX CLOUDのこのフィールド	この値を入力
エンティティID	`https://yourpingfedbaseurl.domain.com`。ここで、`yourpingfedbaseurl.domain.com`はPingFederateサーバーのドメインです。
認証要求に署名	はい
SSOサービスURL	`https://yourpingfedbaseurl.domain.com/idp/SSO.saml2`。ここで、`yourpingfedbaseurl.domain.com`はPingFederateサーバーのドメインです。
SSOバインディングメカニズム	HTTP ポスト
SAML応答	応答またはアサーションのいずれかに署名
認証コンテキスト	未指定、完全一致
ログアウトURL	`https://yourpingfedbaseurl.domain.com/idp/SLO.saml2`。ここで、`yourpingfedbaseurl.domain.com`はPingFederateサーバーのドメインです。
ログアウト要求に署名	はい
SLOバインディングメカニズム	HTTP ポスト

重要:

- 不適切なPingFederate IDP開始SSOエンドポイント`https://yourpingfederateserver.domain.com/idp/startSSO.ping?PartnerSpId=https://saml.cloud.com`の使用はサポートされていません。Citrix CloudとストアはIDP開始SSOをサポートしていません。

- 以下はPingFederateのドキュメントからの抜粋です。 これは、アサーションを含むSAML応答がサービスプロバイダー (SP) に送信される、未承諾のIdP開始シングルサインオン (SSO) トランザクションを開始するために使用されるパスです。
- 不適切なSAMLエンドポイントを使用すると、SAMLログオンの失敗や、Citrix Cloudの認証プラットフォーム内で以下のエラーが発生することが知られています。
  `ExceptionMessage=An IdP-initiated SAML response from YourSAMLApp was received unexpectedly.`

Citrix Cloud™ のライセンス

Citrix Cloud は、特定のクラウドサービスに対してライセンスと使用状況の監視を提供します。また、Citrix License Server が Citrix Cloud に登録されているオンプレミス展開でも、ライセンスと使用状況の監視が利用できます。

エンタープライズ顧客向けライセンス

エンタープライズ顧客は、Citrix Cloud メニューから を選択することで、サポートされているクラウドサービスのライセンス割り当てと使用状況を監視できます。

Citrix Cloud のライセンスメニュー(/en-us/citrix-cloud/media/lic-usage-menu-v3.png)

クラウドサービスにおけるエンタープライズライセンスと使用状況の監視の詳細については、クラウドサービスのライセンスとアクティブな使用状況を監視するを参照してください。

オンプレミス展開向けライセンス

Citrix Virtual Apps and Desktops のオンプレミス展開を持つエンタープライズ顧客は、Citrix Cloud を使用して、ユーザー/デバイスおよび同時接続ライセンスモデルの両方のライセンスと使用状況を把握できます。Citrix License Server を Citrix Cloud に登録することで、顧客は Citrix Cloud のページを以下のタスクに利用できます。

- 登録済みライセンスサーバーのレポートステータスを監視する
- ユーザー/デバイスライセンスモデルを使用する展開のライセンス割り当てと使用状況の傾向を表示する。
- 同時接続ライセンスモデルを使用する展開のピークライセンス使用状況の傾向を表示する。

オンプレミスの Virtual Apps and Desktops 展開におけるライセンスと使用状況の監視の詳細については、オンプレミス展開のライセンスと使用状況を監視するを参照してください。

Citrix Service Providers (CSP) 向けライセンス

Citrix Service Providers は、製品ライセンスと使用状況を把握し、レポートするために以下のツールを使用できます。

- License Usage Insights は、Citrix Cloud の無料サービスであり、シングルテナントおよびマルチテナントの顧客全体で製品使用状況情報を収集および集計します。詳細については、Citrix Service Providers 向けライセンスを参照してください。
- The Licensing feature in Citrix Cloud enables customers of CSPs to monitor their licenses and usage for supported Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) products. CSPs can sign in under their customer's Citrix Cloud account to view and export this information as well. For more information, see the following articles:
  - Customer license and usage monitoring for Citrix DaaS

クラウドサービスのライセンスとアクティブな使用状況を監視する

Citrix Cloud™のライセンス機能を使用すると、購入したクラウドサービスのライセンス消費状況を常に把握できます。概要レポートと詳細レポートを使用して、次のことができます。

- ライセンスの利用状況と割り当てを一目で確認する
- 該当するクラウドサービスの毎日のアクティブな使用状況と月間のアクティブな使用状況の傾向を表示する
- 個々のライセンス割り当ての詳細と使用状況の傾向をドリルダウンして表示する
- ライセンス使用状況データをCSVにエクスポートする

クラウドサービスのライセンスデータを表示するには、コンソールメニューから を選択します。

Citrix Cloud ライセンス メニュー(/en-us/citrix-cloud/media/lic-usage-menu-v3.png)

> **注：**
>
> この記事では、サポートされているすべてのCitrix Cloudサービスに共通するライセンス機能について説明します。ライセンスの側面は、サービスによって異なる場合があります（例：ライセンスの割り当て）。各サービスのライセンスと使用状況の詳細については、以下の記事を参照してください。
>
> - Citrix DaaS のライセンスとアクティブな使用状況を監視する (ユーザー/デバイス)(/ja-jp/citrix-cloud/citrix-cloud-management/license-usage/virtual-apps-desktops-service-license-usage.html)

- Citrix DaaSおよびCitrix DaaS Standard for Azureのライセンスとピーク使用状況を監視する（同時接続）
- Citrix DaaS Standard for Azureのライセンスとアクティブな使用状況を監視する（ユーザー/デバイスのみ）
- Endpoint Managementサービスのライセンスとアクティブな使用状況を監視する
- Gatewayサービスの帯域幅使用状況を監視する
- Secure Private Access のライセンスと使用状況を監視する(/ja-jp/citrix-cloud/citrix-cloud-management/license-usage/secure-workspace-access-license-usage.html)

サポートされているリージョンとクラウドサービス

ライセンスは、米国、EU、およびアジア太平洋南部リージョンでのみ、サポートされているサービスで利用できます。

ライセンスは、以下のクラウドサービスでサポートされています。

- Citrix DaaS (ユーザー単位とデバイス単位、および同時接続のライセンスモデル) - 以前は Citrix Virtual Apps and Desktops service
- Citrix DaaS Standard for Azure (ユーザー単位またはデバイス単位でライセンスを付与するモデル) - 以前は Citrix Virtual Apps and Desktops Standard for Azure
- Endpoint Management
- Gateway
- Secure Private Access (以前は Secure Workspace Access と呼ばれていました)

Citrix DaaS™ の複数タイプライセンス

Citrix Cloud のライセンスは、Citrix DaaS の複数タイプライセンスをサポートしています。ユーザー/デバイスと同時接続の両方のライセンスモデルが単一の Citrix Cloud アカウントに導入されている場合、Citrix Cloud はライセンスコンソールページで各ライセンスモードのライセンス使用状況を表示します。

Citrix は、ライセンスページを確認する前に、サイトおよびデリバリーグループレベルで複数タイプライセンスを設定することをお勧めします。そうしないと、正しい情報が表示されない可能性があります。手順については、Citrix DaaS ドキュメントの「複数タイプライセンス」を参照してください。

Web Studio または PowerShell セットアップ方法を正常に使用した後でも、ライセンスコンソールページに正しい複数タイプライセンスの使用状況が表示されない場合は、次のオプションがあります。

- 30 日間待機し、未使用のライセンスを解放します。
- Citrix カスタマーサービスに連絡します。

ライセンスの割り当て

一般的に、ユーザーはクラウドサービスを初めて使用する際にライセンスが割り当てられます。一部のサービスでは、使用するライセンスモデルに基づいてライセンスの割り当て方法が異なる場合があります。各サービスでのライセンスの割り当て方法の詳細については、この記事の冒頭で参照されているライセンスに関する記事を参照してください。

ライセンスの概要と詳細

ライセンスの概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-v2.png)

ライセンスの概要には、サポートされている各サービスに関する以下の情報が一目でわかるように表示されます。

- 購入済みライセンス総数の割り当て済み割合。割合が100%に近づくと、緑から黄色に変わります。割合が100%を超えると、赤色に変わります。
- 割り当て済みライセンスと購入済みライセンスの比率、および残りの利用可能なライセンス数。
- クラウドサービスのサブスクリプションの有効期限が切れるまでの残り時間。サブスクリプションが今後90日以内に期限切れになる場合、警告メッセージが表示されます。

一部のサービスでは、この概要にアクティブな使用状況などの追加情報が含まれる場合があります。サービス固有の詳細については、この記事の冒頭で参照されているライセンスに関する記事を参照してください。

使用状況の傾向とライセンスアクティビティ

クラウドサービスライセンスの詳細を表示するには、**View Usage Details**をクリックします。その後、使用状況の傾向とクラウドサービスライセンスの利用者に関する内訳を確認できます。

ライセンス使用状況の割り当て傾向グラフ(/en-us/citrix-cloud/media/lic-usage-assignment-trends-v2.png)

この内訳には、クラウドサービスに応じてさまざまな情報が含まれます。サービス固有の使用状況の傾向とライセンスアクティビティの詳細については、この記事の冒頭で参照されているライセンスに関する記事を参照してください。

割り当て済みライセンスの解放

一般的に、割り当てられたライセンスは、利用者が30日間連続してクラウドサービスを使用しなかった場合に解放の対象となります。ライセンスが解放されると、残りのライセンス数が増加し、割り当て済みライセンス数がそれに応じて減少します。

一部のサービスでは、使用されるライセンスモデルによって、ライセンスの解放方法が異なる場合があります。特定のサービスのライセンス解放の詳細については、この記事の冒頭で参照されているライセンスに関する記事を参照してください。

よくある質問

- **Citrix®は、割り当てられたライセンスが購入したライセンスを超過した場合、クラウドサービスの使用を防止しますか？** いいえ、Citrixは、クラウドライセンスの量を使いすぎた場合でも、サービスの起動を妨げることはありません。ライセンス使用状況は、クラウドライセンスの使用状況を理解するための情報を提供するため、Citrixは、お客様がライセンスの割り当てを監視し、購入したライセンスの範囲内に収めることを期待しています。もし、いずれかの時点でサービスを使いすぎると考えられる場合は、Citrixは営業担当者に連絡してライセンス要件について話し合うことをお勧めします。
- **どのようなライセンス情報が取得されますか？** 現在、ユーザーログインに関連付けられたライセンス情報のみが取得されます。
- **Citrix DaaSでは、複数種類のライセンス（例：ユーザー/デバイスモデルと同時ユーザーモデルの両方を使用）がサポートされていますか？** はい。詳細については、この記事の複数種類のライセンスを参照してください。
- **Citrix DaaSでは、複数エディションのライセンスがサポートされていますか？たとえば、同じCitrix CloudアカウントでPremiumエディションとAdvancedエディションの両方を使用できますか？** いいえ、このユースケースはサポートされていません。Citrix DaaSサイトは1つのエディションのみライセンスできます。同じCitrix Cloudアカウントで複数のCitrix DaaSインスタンスを使用したい場合は、それらは同じエディションである必要があります。
- **Monitorレポート（Director内）と同時ライセンスインサイトの違いは何ですか？** Monitorレポートと同時セッションの説明は、使用中の同時ライセンスの測定とは異なる解釈とメトリックを提供します。ほとんどの場合、Director内の同時セッション数を、使用中のピーク同時ライセンスの表現または予測として使用すると、必要な同時ライセンス数が大幅に過大評価され

ます。DirectorのMonitorレポートを同時ライセンス使用状況レポートの代わりに使用しないでください。レポートツール間の主な違いは次の2点です。

- **サンプリング時間長：** ライセンスには5分間のサンプリング期間があります。Citrix Cloudは5分ごとに、現在サービスに接続されている一意のデバイスをカウントします。すべての5分間のサンプリング期間が集計され、24時間、月間、および契約期間におけるピーク使用量が決定されます。DirectorのMonitorレポートは、レポートの実行方法に応じて最大2時間の期間を表示できます。
- **一意性：** ライセンスは、セッションが起動されたときにデバイス間の一意性を探します。Monitorレポートは一意のデバイスを考慮しません。

- **ユーザーをクラウドサービスの新しいインスタンスに移行した後（たとえば、組織のドメイン名を変更した場合）、同じユーザーに対して使用中のライセンスが2回カウントされるのはなぜですか？*- Citrix Cloudは、一意のユーザーをカウントするためにユーザープリンシパル名（UPN）を使用します。ユーザーが移行前と移行後にクラウドサービスにアクセスした場合、Citrix Cloudはユーザーに対して2つの一意のUPNをキャプチャし、それぞれ異なるドメイン名を持ちます。したがって、Citrix Cloudは同じユーザーを2回カウントします。ユーザーが古いドメイン名でサービスにアクセスしないと仮定して、30日後に古いライセンス割り当てを解放できます。Citrixは、クラウドライセンスの量を使いすぎた場合でも、サービスの起動を妨げることはありません。
- **同じユーザーまたはデバイスに対して重複するライセンスが表示されるのはなぜですか？*- これは、HTML5用Workspaceアプリとローカルにインストールされ
たWorkspaceアプリの設計によるものです。HTML5用Workspaceアプリを介した起動はユーザー/デバイスライセンスを消費します。同様に、ローカルにインストールされたWorkspaceアプリを介した起動もユーザー/デバイスライセンスを消費します。したがって、ユーザーがHTML5用Workspaceアプリを介してアプリを起動し、その後ローカルにインストールされたWorkspaceアプリのバージョンを介して起動した場合、Citrix Cloudはユーザーが2つのライセンスを消費したと表示します。この動作はユーザー接続には影響しませんが、ライセンスコンソールでデバイスライセンス使用状況レポートが過大に表示される可能性があります。Citrixは、クラウドライセンスの量を使いすぎた場合でも、サービスの起動を妨げることはありません。

Citrix DaaS (ユーザー/デバイス) のライセンスとアクティブな使用状況を監視する

この記事では、Citrix Cloud のライセンスコンソールを使用して、クラウドサービスのライセンス割り当てを管理し、アクティブな使用状況を監視する方法について説明します。

サービス展開で利用するために Citrix Azure Consumption Fund を購入した場合は、詳細について Citrix DaaS の Citrix Managed Azure リソース消費量を監視する を参照してください。

ライセンスの割り当て

Citrix Cloud は、一意のユーザーまたは一意のデバイスが初めてアプリまたはデスクトップを起動したときにライセンスを割り当てます。

ドメイン名の切り捨て

複数のドメインをホストしており、それらのドメインに類似したアカウントを持つユーザーがいる場合 (例: `johnsmith@company.com` および `johnsmith@mycompany.com`)、Citrix Cloud でアカウントドメインを無視し、アカウントのユーザー名のみを考慮するように設定できます (例: johnsmith)。このプロセスは、*ドメイン名の切り捨て* と呼ばれます。デフォルトでは、ドメイン名の切り捨ては無効になっています。

ドメイン名の切り捨てが有効になっている場合、Citrix Cloud の一意のユーザーの計算方法が変わります。Citrix Cloud は、`johnsmith@company.com` と `johnsmith@mycompany.com` を2つの一意のユーザーとして数える代わりに、johnsmith のみを一意のユーザーとして数えます。この計算の変更は、以下のライセンスデータに影響します。

- ライセンスの割り当て
- アクティブな使用
- 経時的なライセンス使用状況の傾向
- リリース対象のライセンス

ライセンスコンソールからデータを CSV ファイルにエクスポートする際にも、これらのライセンスデータの変更が反映されます。

> **注:**
>
> ユーザー名がわずかに異なる類似のアカウントを持つ複数のドメインをホストしている場合 (例: 個々のユーザーが `johnsmith@company.com` と `jsmith@newcompany.com` のアカウントを持っている場合)、ドメイン名の切り捨ては Citrix Cloud の計算に影響しません。Citrix Cloud は、johnsmith と jsmith が同じ個人に属していても、それらを一意のユーザーとして数えます。

ドメイン名の切り捨てを有効または無効にする

デフォルトでは、ドメイン名の切り捨ては無効になっています。ドメイン名の切り捨ては、この機能を有効または無効にした時点から、ユーザー/デバイスの使用状況データに影響を与えます。たとえば、特定の月にドメイン名の切り捨てを有効にした場合、その月にCitrix Cloudが記録するデータは影響を受けます。ただし、この機能が無効になっていた以前の月の履歴データは影響を

受けません。同様に、特定の月にドメイン名の切り捨てを無効にした場合、その月にCitrix Cloudが記録するデータは影響を受けます。ただし、この機能が有効になっていた月の履歴データはそのまま残ります。

ドメイン名の切り捨てを有効または無効にするには：

1. ライセンスコンソールの右上にあるトグルをクリックします。

   ドメイン切り捨てトグルが強調表示されたライセンス概要ページ(/en-us/citrix-cloud/media/lic-usage-domain-trunc-toggle-daas.png)
2. 操作の確認を求められたら、**「はい、理解しました」**を選択します。

ライセンスの概要

ライセンス概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-daas.png)

ライセンスの概要には、以下の情報が一目でわかるように表示されます。

- 割り当て済みの購入済みライセンス総数の割合。この割合が100%に近づくと、緑色から黄色に変わります。100%を超えると、赤色に変わります。

  購入済みライセンスの総数は、ユーザー/デバイスライセンスモデルを使用するCitrix DaaSエディション向けに購入されたライセンスの合計です。
- 割り当て済みライセンスと購入済みライセンスの比率、および残りの利用可能なライセンス数。
- 月次および日次のアクティブな使用状況統計：
  - 月間アクティブ使用とは、過去30日間にサービスを使用したユニークユーザーまたはデバイスの数を指します。
  - 日間アクティブ使用とは、過去24時間以内にサービスを使用したユニークユーザーまたはデバイスの数を指します。
- クラウドサービスサブスクリプションの有効期限が切れるまでの残り時間。サブスクリプションが今後90日以内に期限切れになる場合、警告メッセージが表示されます。

割り当てられたライセンスとアクティブな使用状況の計算

Citrix DaaSのユーザー/デバイスライセンスモデルを正確に反映するため、Citrix Cloudはサービスを使用したユニークユーザーとユニークデバイスの数をカウントします。割り当てられたライセンスを測定するために、Citrix Cloudはこれらのカウントのうち少ない方を使用します。アクティブな使用状況を測定するために、Citrix Cloudは各カウントを特定の期間におけるアクティブユーザーとアクティブデバイスの数として使用します。

割り当てられたライセンスの計算例

100人のユニークユーザーと50台のユニークデバイスがサービスを使用した場合、Citrix Cloudは少ない方の数（50）を使用して、割り当てられたライセンスの数を決定します。使用されているライセンスの割合と利用可能なライセンスの数は、これら50の割り当てられたライセンスに基づいています。

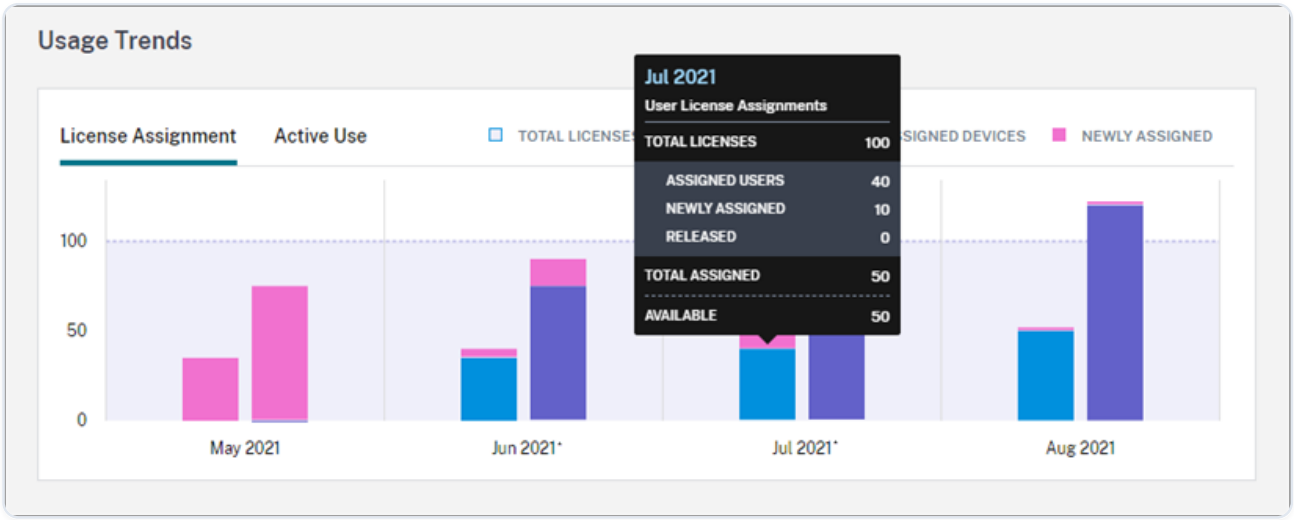
アクティブな使用状況の計算例

過去30日間に10人のユニークユーザーと20台のユニークデバイスがサービスを使用した場合、Citrix Cloudは月間アクティブ使用が10人のアクティブユーザーと20台のアクティブデバイスで構成されていると判断します。同様に、過去24時間に30人のユニークユーザーと15台のユニークデバイスがカウントされた場合、Citrix Cloudは日間アクティブ使用が30人のアクティブユーザーと15台のアクティブデバイスで構成されていると判断します。

使用状況の傾向

ライセンスの詳細を表示するには、概要の右端にある****をクリックします。その後、使用状況の傾向と、クラウドサービスライセンスを使用している個々のユーザーおよびデバイスの内訳を確認できます。

****セクションには、この内訳がグラフとして表示されます。



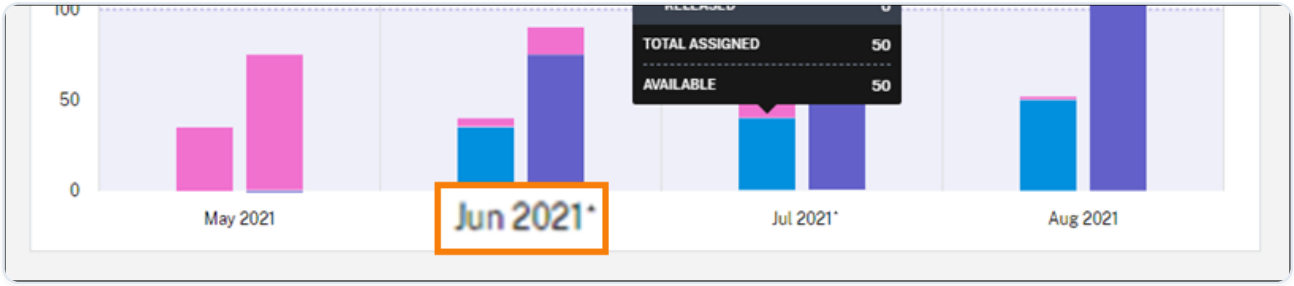
****グラフで、特定の月または日のバーをポイントすると、次の情報が表示されます。

- **合計ライセンス数:** すべてのエンタイトルメントにおけるクラウドサービスの購入済みライセンスの合計数。
- **割り当てられたユーザー数:** 現在の月までのユーザーに割り当てられたライセンスの累積数。
- **割り当て済みデバイス:** 現在の月までのデバイスに割り当てられたライセンスの累積数。特定の月でこの数が特に高いように見える場合、これはWebブラウザを介して発生するアプリまた

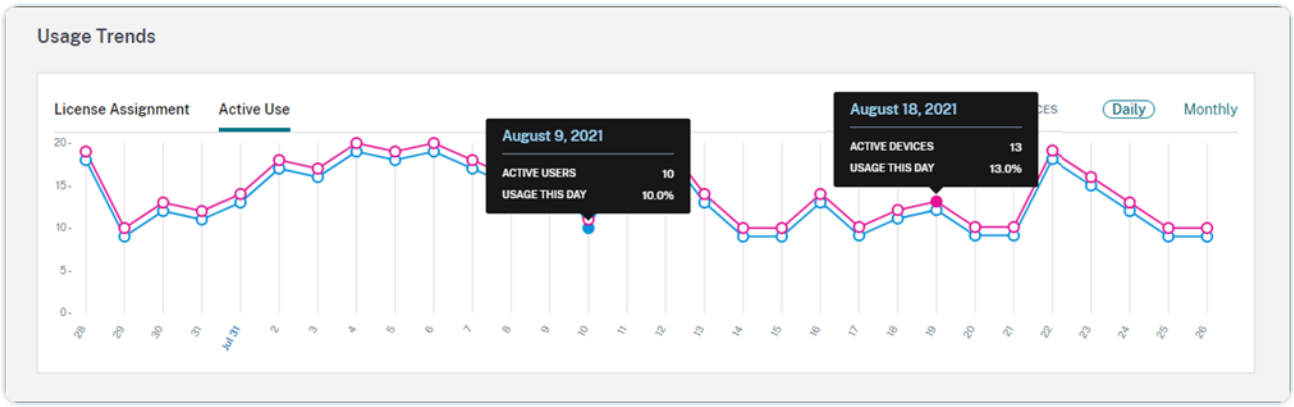
はデスクトップの起動の結果である可能性があります。この数を減らすには、Citrix®はローカルにインストールされたWorkspaceアプリを使用することをお勧めします。

- **新規割り当て:** 各月に割り当てられた新しいライセンスの数。たとえば、ユーザーが7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられたとします。このライセンスは、7月の「新規割り当て」としてカウントされます。
- **リリース済み:** 各月にリリースされた対象ライセンスの数。たとえば、20個のライセンスがリリース対象であり、7月にそのうち10個をリリースした場合、7月に表示されるリリース済みライセンスの数は10です。

ドメインの切り捨てが有効になっている期間は、アスタリスクでマークされます。



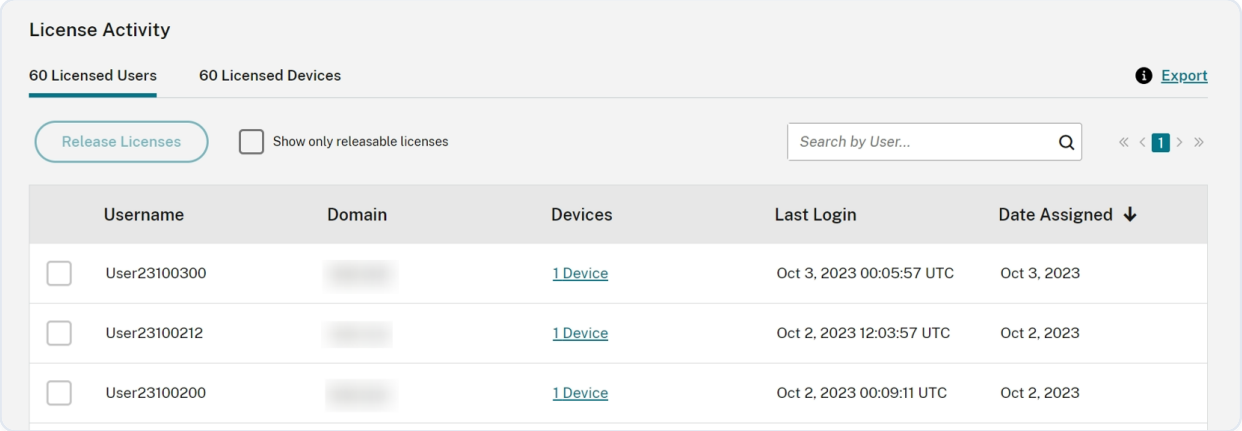
アクティブな使用状況グラフでは、前暦月および前暦年におけるアクティブなユーザーとデバイスをそれぞれ表示できます。グラフ上の特定の期間をポイントすると、アクティブなユーザーまたはデバイスの数と使用率が表示されます。



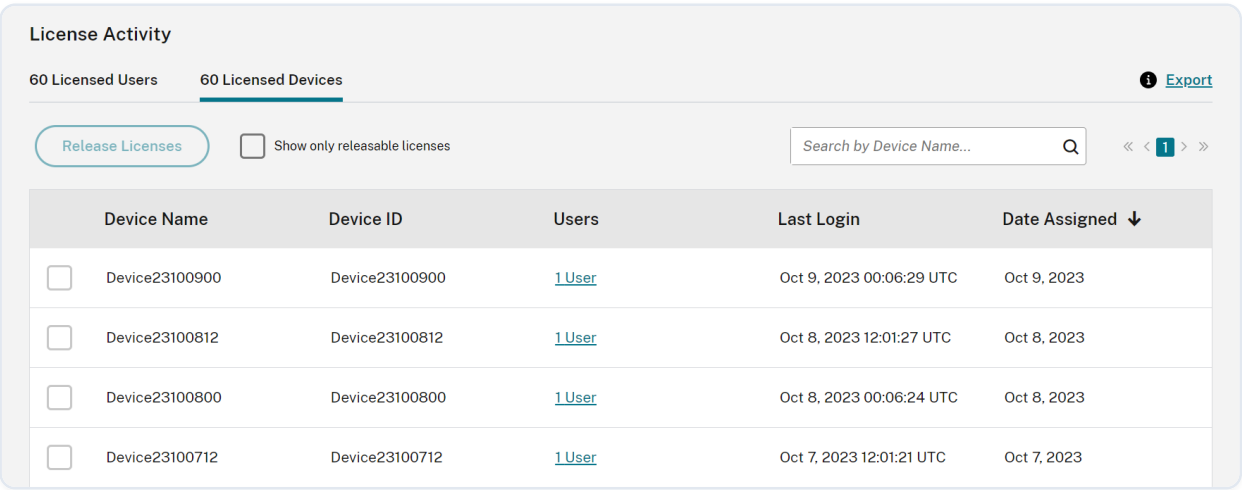
ライセンスアクティビティ

ライセンスアクティビティセクションには、次の情報が表示されます。

- ライセンスが割り当てられている個々のユーザーのリスト（関連付けられたデバイスを含む）。



- ライセンスが割り当てられているデバイスのリスト（関連付けられたユーザーを含む）。



- ユーザーまたはデバイスにライセンスが割り当てられた日付。

リストをフィルタリングして、リリース対象のライセンスのみを表示することもできます。詳細については、この記事の割り当てられたライセンスをリリースするにはを参照してください。

割り当てられたライセンスをリリースする

ライセンスが割り当てられると、割り当て期間は90日間であり、サービスへの接続が確立されます。ユーザーまたはデバイスが90日間アプリまたはデスクトップを起動していない場合、これらのライセンスは未使用のライセンスと見なされ、90日後にCitrix Cloudによってリリースされます。このプロセスは自動化されており、管理者による操作は不要です。

割り当て期間（90日）が経過した後、管理者は以下のシナリオでのみ、手動でライセンスを解放できます。

- ユーザーが会社に所属しなくなった場合。
- ユーザーが長期休暇中の場合。

管理者は、デバイスがサービス停止中の場合にのみ、デバイスのライセンスを解放できます。

注：

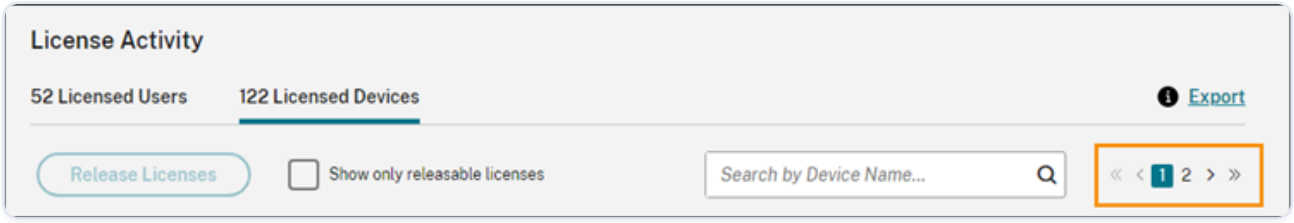
- ライセンスの解放は、自動プロセスに従うことをお勧めします。ただし、管理者が上記の理由以外で90日期間より前にライセンスを解放しようとすると、Citrix EULAに違反する可能性があります。この操作を実行する前に、Citrixにお問い合わせください。

- 管理者はUIを通じて単一のライセンスを手動で解放できます。または、クラウドライセンスAPIを使用してライセンスを解放することもできます。詳細については、「Citrixクラウドライセンスを管理するためのAPI」を参照してください。

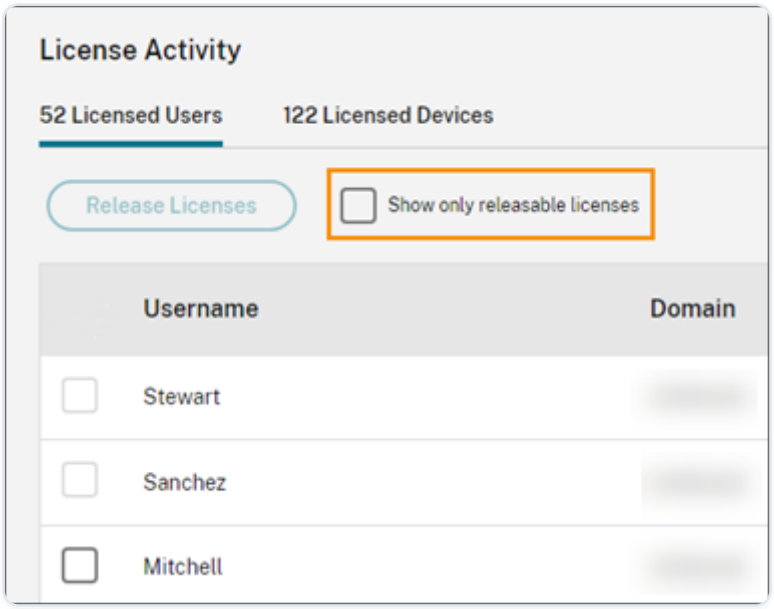
解放可能なライセンスを見つける

ユーザーまたはデバイスが30日間アプリまたはデスクトップを起動しなかった場合、Citrix Cloudはライセンスを解放可能な状態にします。解放可能なライセンスは、選択可能な濃い灰色のチェックボックスとともに、ライセンスユーザーまたはライセンスデバイスのリストに表示されます。解放できないライセンスは、選択できないことを示す薄い灰色のチェックボックスを表示します。

ライセンスアクティビティセクションに表示されるリストには、一度に最大100個の割り当て済みライセンスが表示されます。100個を超えるライセンスがある場合は、ページコントロールを使用してリストを移動します。



解放可能なライセンスをすばやく見つけるには、**ライセンスの解放**ボタンの横にある**解放可能なライセンスのみ表示**をクリックします。この操作により、まだ解放が許可されていない割り当て済みライセンスが非表示になります。



解放可能なライセンスを選択する

各ライセンスの横にある濃い灰色のチェックボックスを選択して、リリース対象として選択します。リストからライセンスを選択すると、**Release Licenses** ボタンがアクティブになります。

リリース可能なすべてのライセンスを1つずつ選択し、**Release Licenses** をクリックできます。

割り当てられたライセンスをリリースするには

1. **License Activity** で、**Licensed Users** タブまたは **Licensed Devices** タブをクリックします。
2. 必要に応じて、**Show releasable licenses** をクリックして、リリースが許可されているライセンスを持つユーザーのみを表示します。
3. 管理したいユーザーまたはデバイスを選択し、**Release Licenses** をクリックします。
4. 選択したユーザーまたはデバイスを確認し、**Release Licenses** をクリックします。

ライセンスの自動切り替え

アクティブなユーザー/デバイスライセンスの有効期限が切れ、同時使用ライセンスがテナントで唯一のアクティブなライセンスタイプである場合、サイトライセンスは自動的にアクティブな同時使用ライセンスに切り替わります。これにより、サイトでのアクティブなライセンス不足による停止が防止されます。

Citrix DaaS™ のライセンスとピーク使用状況を監視する（同時実行ユーザー）

この記事では、**Citrix DaaS** の同時実行ユーザーライセンスを管理するエクスペリエンスについてのみ説明します。

Citrix DaaS のユーザー/デバイスライセンスについては、「Citrix DaaS のライセンスとアクティブな使用状況を監視する（ユーザー/デバイス）」を参照してください。

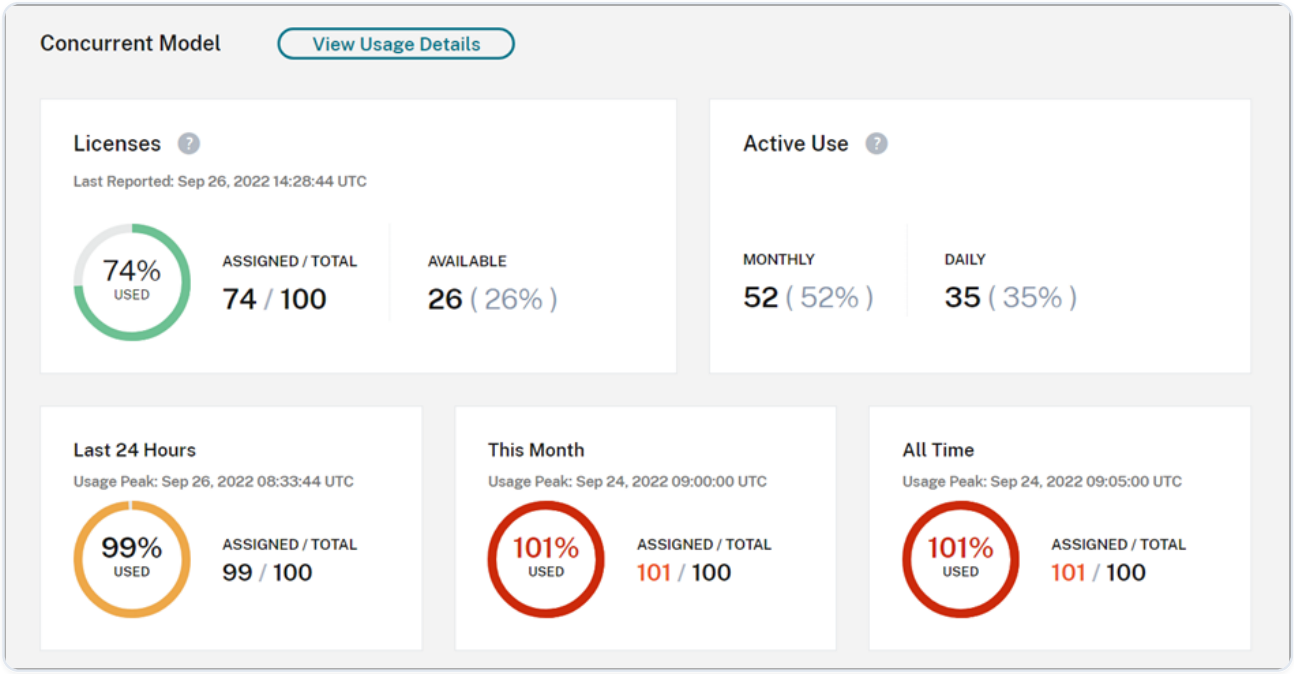
Citrix DaaS Standard for Azure のユーザー/デバイスおよび同時実行ユーザーライセンスについては、「Citrix DaaS Standard for Azure のライセンスと使用状況を監視する」を参照してください。

ライセンスの割り当て

Citrix Cloud™ は、ユーザーがデバイスでアプリまたはデスクトップを起動したときにライセンスを割り当てます。ユーザーがセッションからログオフまたは切断すると、ライセンスは割り当てられなくなります。これは、ライセンスの割り当てが、特定の時間にアプリまたはデスクトップにアクセスするデバイスの数によって変化する可能性があるためです。

同時実行ユーザーライセンスモデルの詳細については、ライセンス製品ドキュメントの「同時実行ライセンス」を参照してください。

ライセンスの概要



ライセンスの概要には、以下の情報が一目でわかるように表示されます。

- Citrix Cloud が最後に使用中のライセンスを評価した時点での、現在使用中の購入済みライセンス総数の割合。購入済みライセンス総数は、同時実行ユーザーライセンスモデルを使用する Citrix DaaS エディション用に購入されたライセンスの合計です。
- 現在割り当てられているライセンスと購入済みライセンス総数の比率、および残りの利用可能なライセンス数。この比率で示される**合計**の数値は、現在所有しているライセンスの総数（「最終報告」の日時時点）を表します。

- ピーク使用状況の統計。使用中のピークライセンスを計算する際、Citrix Cloud は以下の期間で使用されたライセンスの最大数を取得します。
  - **過去24時間:** 過去24時間で一度に使用されたライセンスの最大数。
  - **今月:** 現在の暦月の開始から一度に使用されたライセンスの最大数。
  - **全期間:** サブスクリプション開始から一度に利用されたライセンスの最大数。

  これらのピーク使用期間に表示される**合計**の数値は、その時点で所有されていたライセンスの総数を表します。所有ライセンスの総数が増減し、割り当てられたライセンスもそれに応じて増加した場合、**合計**の数値はその時点での新しい所有ライセンス数を反映するように変更されます。ただし、対応する使用ピークがない場合、**合計**の数値は変更されません。
- アクティブ使用統計。Citrix Cloudは、以下の期間における一意の接続の総数を表示します。
  - **月間:** 月間アクティブ使用とは、過去30日間にサービスを利用した一意のユーザーまたはデバイスの数を指します。
  - **日間:** 日間アクティブ使用とは、過去24時間以内にサービスを利用した一意のユーザーまたはデバイスの数を指します。これらの数値は、これらの期間中に所有されていたライセンス総数に対する割合としても表されます。

使用中のピークライセンスの計算

同時ユーザーライセンスモデルを正確に反映するため、Citrix Cloudはサービスに同時にアクセスしている一意のデバイスの数をカウントします。この数が現在表示されているピーク使用量よりも大きい場合、Citrix Cloudは新しいピーク使用量を、それが達成された日時とともに表示します。この数が現在のピーク使用量よりも小さい場合、現在のピーク使用量は変更されません。

> **重要:**
>
> DirectorのMonitorを使用して同時セッションに関する情報を取得する場合、Monitorレポートは同時セッションについて異なる解釈を提供し、使用中の同時ユーザーライセンス数を正確に反映しないことに注意してください。Monitorレポートとライセンスレポートの違いに関する詳細については、FAQを参照してください。

月間アクティブ使用の計算

毎月の初めに、Citrix Cloudは過去30日間のスナップショットを取得します。Citrix Cloudは、その暦月に発生した一意の接続の総数を表示します。

日間アクティブ使用の計算

毎日同じ時刻に、Citrix Cloudは過去24時間のスナップショットを取得します。Citrix Cloudは、その24時間期間中に発生した一意の接続の総数を表示します。

使用傾向とライセンスアクティビティ

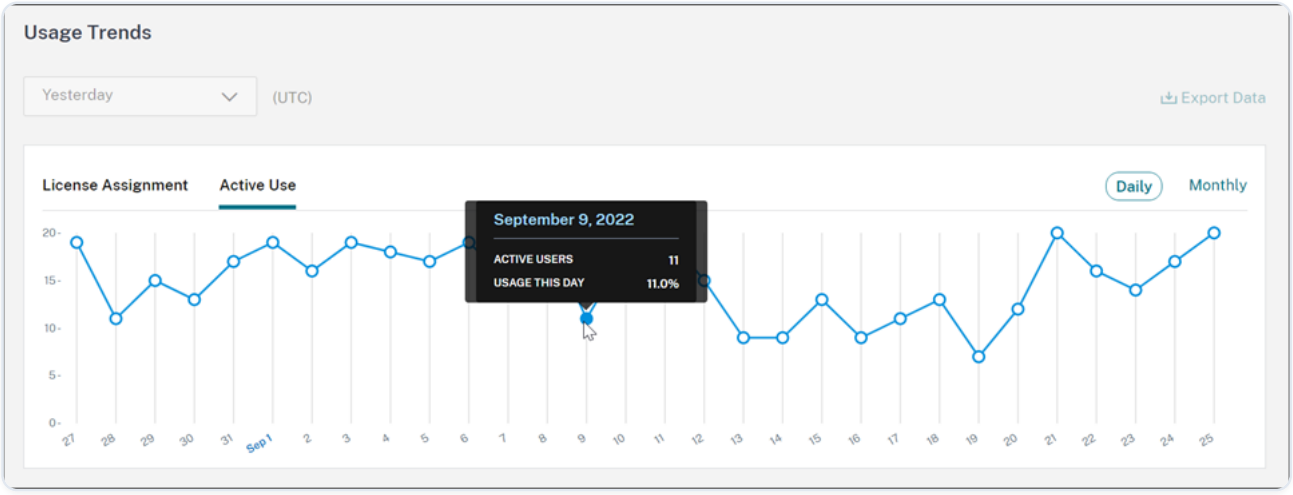
ライセンスの履歴を表示するには、**使用状況の詳細を表示**をクリックします。

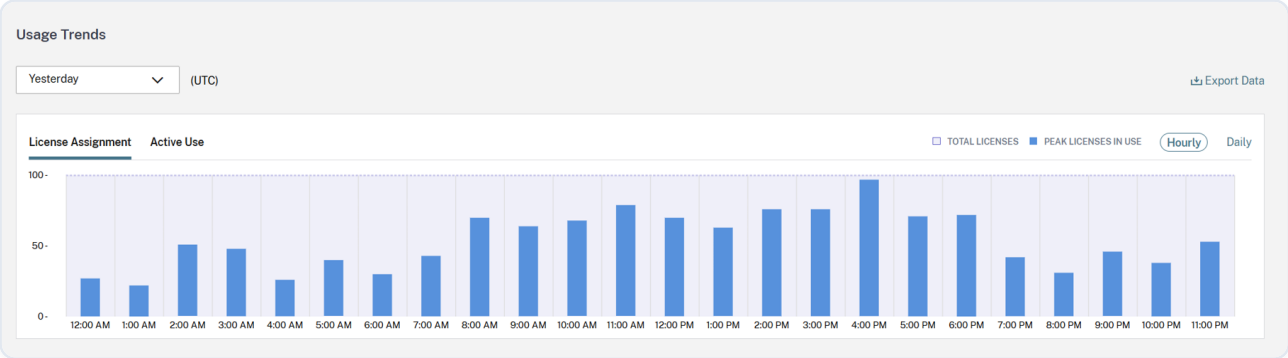
「**使用状況の傾向**」セクションには、次の情報が表示されます。

- 「**ライセンス割り当て**」には、次の情報を示すグラフが表示されます。
  - **合計ライセンス数:** 購入済みの同時実行ユーザーライセンスの合計数。
  - **使用中のピークライセンス数:** 選択した日付範囲に割り当てられたライセンスの最大数。デフォルトでは、Citrix Cloudは現在の暦年の各月のピーク使用状況を表示します。月別または時間別のピーク使用状況にドリルダウンするには、ドロップダウンメニューから表示したい暦月または日を選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloudは最新の時間間隔の現在のピーク使用状況を表示します。たとえば、まだ進行中の暦日にドリルダウンして表示する場合、現在の時刻までの各時間におけるライセンスの最大数が表示されます。次のカウント間隔でライセンスの最大数が増加した場合、Citrix Cloudは現在の時間のピーク使用状況を更新します。
- 「**アクティブな使用状況**」には、次の情報を示すグラフが表示されます。
  - **日別:** 過去30日間の各日における接続の合計数。
  - **月別:** 前の暦年の各月における接続の合計数。

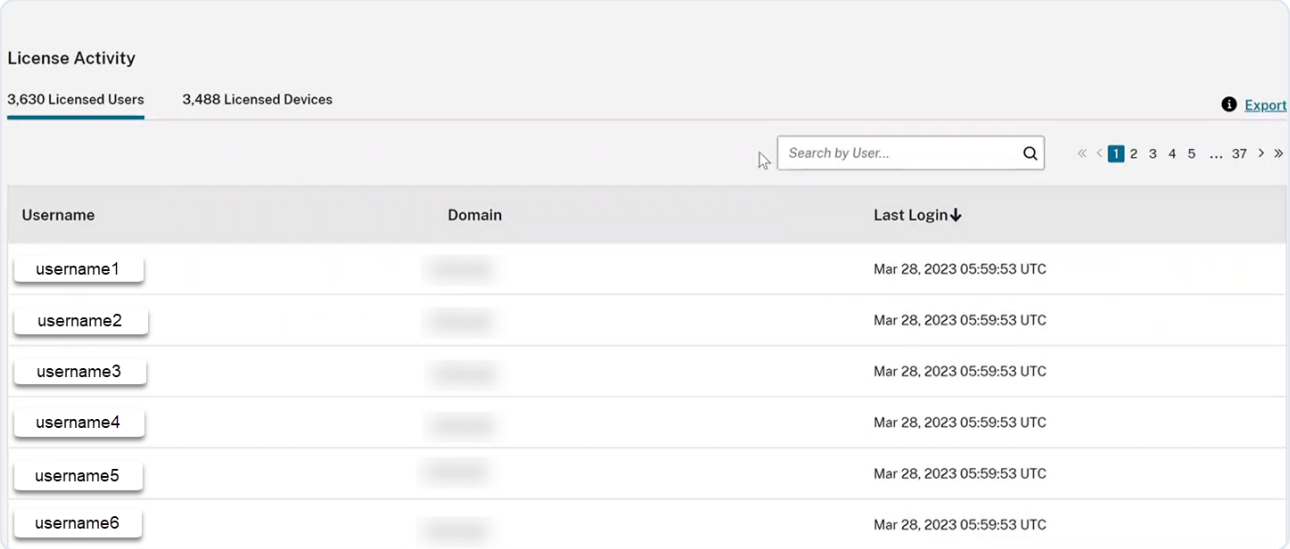
「**ライセンス割り当て**」または「**アクティブな使用状況**」グラフの期間をポイントすると、その期間の詳細が表示されます。





ユーザーとデバイスのライセンスアクティビティ

ユーザーまたはデバイスライセンスの場合、「**ライセンスアクティビティ**」セクションには、ライセンスが割り当てられている個々のユーザーのリストと、ユーザーにライセンスが割り当てられた日付が表示されます。



ライセンスの解放

ユーザーがセッションからサインアウトまたは切断すると、同時使用ユーザーライセンスは自動的に解放されます。これらのライセンスを手動で解放する必要はありません。

Citrix DaaS Standard for Azure のライセンスと使用状況を監視する

この記事では、ユーザー/デバイスおよび同時実行ユーザーの両方のライセンスモデルにおけるライセンス割り当ての管理エクスペリエンスについて説明します。

シトリックス アジュール コンサンプション ファンド (ユーザー/デバイスのみ)

サービス展開でCitrix Azure Consumption Fundを使用するために購入した場合、Citrix管理リソースの消費レポートの詳細については、「Citrix DaaS の Citrix 管理 Azure リソース消費を監視する」を参照してください。

ライセンスの割り当て

ユーザー/デバイスライセンスモデル: Citrix Cloud は、固有のユーザーまたは固有のデバイスが初めてデスクトップを起動したときにライセンスを割り当てます。

同時実行ユーザーライセンスモデル: Citrix Cloud™ は、ユーザーが自分のデバイスでデスクトップを起動したときにライセンスを割り当てます。ユーザーがセッションからログオフまたは切断すると、ライセンスは割り当てられなくなります。ライセンスの割り当ては、特定の時間にデスクトップにアクセスするデバイスの数によって変更される可能性があるため、Citrix Cloud は5分ごとに使用中のライセンス数を評価します。

同時実行ライセンスモデルの詳細については、ライセンス製品ドキュメントの「同時実行ライセンス」を参照してください。

使用中のピークライセンスの計算

同時実行ライセンスモデルを正確に反映するために、Citrix Cloud は5分ごとにサービスに同時にアクセスしている固有のデバイスの数をカウントします。カウントが表示されている現在のピーク使用量よりも大きい場合、Citrix Cloud は新しいピーク使用量を、それが達成された日時とともに表示します。カウントが現在のピーク使用量よりも少ない場合、現在のピーク使用量は変更されません。

ドメイン名の切り捨て

この機能は、**ユーザー/デバイス**ライセンスモデルでのみサポートされています。

複数のドメインをホストしており、それらのドメインに類似したアカウントを持つユーザーがいる場合（例: `johnsmith@company.com` および `johnsmith@mycompany.com`）、Citrix Cloud にアカウントドメインを無視させ、アカウントのユーザー名のみを考慮させることができます（例: johnsmith）。このプロセスは *ドメイン名の切り捨て* と呼ばれます。デフォルトでは、ドメイン名の切り捨ては無効になっています。

ドメイン名の切り捨てが有効になっている場合、Citrix Cloud の固有ユーザーの計算が変更されます。Citrix Cloud は `johnsmith@company.com` と `johnsmith@mycompany.com` を2つの固有ユーザーとしてカウントする代わりに、johnsmith のみを固有ユーザーとしてカウントします。この計算の変更は、以下のライセンスデータに影響します。

- ライセンスの割り当て
- アクティブな使用
- 経時的なライセンス使用状況の傾向
- リリース対象のライセンス

ライセンスデータのこれらの変更は、ライセンスコンソールからデータをCSVファイルにエクスポートする際にも反映されます。

> **注：**
>
> ユーザー名がわずかに異なる類似のアカウントを持つ複数のドメインをホストしている場合（たとえば、個々のユーザーが`johnsmith@company.com`と`jsmith@newcompany.com`のアカウントを持っている場合）、ドメイン名の切り捨てはCitrix Cloudの計算に影響しません。Citrix Cloudは、johnsmithとjsmithが同じ個人に属していても、それぞれを固有のユーザーとしてカウントします。

ドメイン名の切り捨てを有効または無効にする

デフォルトでは、ドメイン名の切り捨ては無効になっています。ドメイン名の切り捨ては、この機能を有効または無効にした瞬間から、ユーザー/デバイスの使用状況データに影響を与えます。たとえば、特定の月にドメイン名の切り捨てを有効にした場合、その月にCitrix Cloudが記録するデータは影響を受けます。ただし、機能が無効になっていた以前の月の履歴データは影響を受けません。同様に、特定の月にドメイン名の切り捨てを無効にした場合、その月にCitrix Cloudが記録するデータは影響を受けます。ただし、機能が有効になっていた月の履歴データはそのまま残ります。

ドメイン名の切り捨てを有効または無効にするには：

1. ライセンスコンソールの右上にあるトグルをクリックします。

   ドメイン名の切り捨てトグルが強調表示されたライセンス概要ページ(/en-us/citrix-cloud/media/lic-usage-domain-trunc-toggle-daas-azure.png)

2. 操作の確認を求められたら、**はい、理解しました**を選択します。

ライセンスの概要

Citrix Cloud は、ユーザー/デバイスおよび同時実行ユーザーのライセンスモデルにおける、使用中のライセンスの概要ビューを表示します。

ユーザーとデバイスの概要

「ユーザー/デバイス」モデルの場合、ライセンス概要には、お客様が所有するライセンスの総数に対して使用中のライセンスが表示されます。

ユーザー/デバイスモデルのライセンス概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-daas-azure.png)

割合が100%に近づくと、緑から黄色に変わります。割合が100%を超えると、赤に変わります。

Citrix Cloudは、割り当てられたライセンスと購入済みライセンスの比率、および残りの利用可能なライセンス数も表示します。

同時ユーザーの概要

「同時」モデルの場合、ライセンス概要には以下の情報が一目でわかるように表示されます。

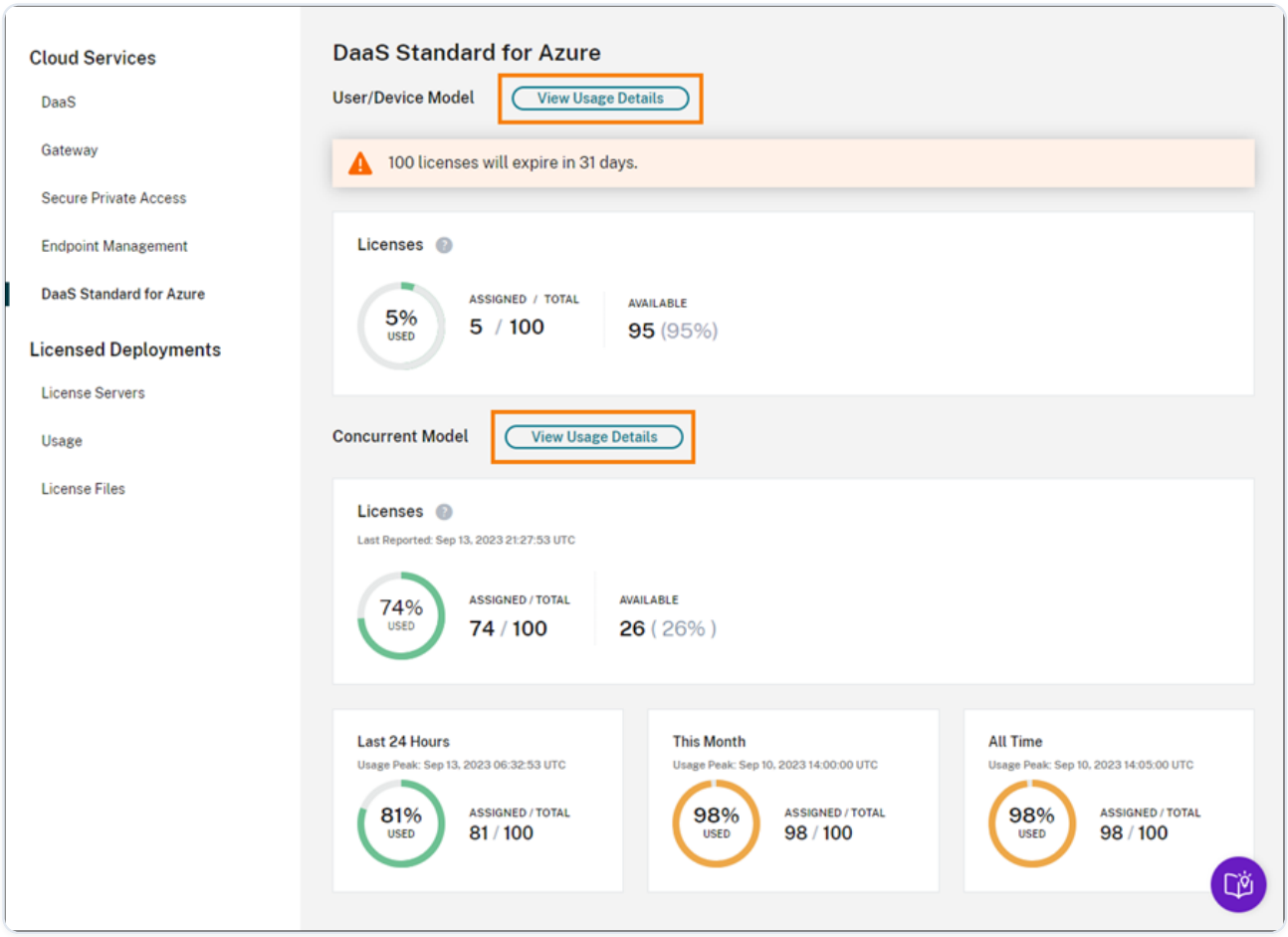
同時モデルのライセンス概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-daas-azure-concurrent.png)

- Citrix Cloudが使用中のライセンスを最後に評価した時点での、現在使用中の購入済みライセンス総数の割合。Citrix Cloudは、サービスへのアクティブな接続を持つ一意のデバイスに基づいて、この割合を5分ごとに計算します。購入済みライセンス総数は、同時ライセンスモデルを使用するCitrix DaaS Standard for Azure向けに購入されたライセンスの合計です。
- 現在割り当てられているライセンスと購入済みライセンス総数の比率、および残りの利用可能なライセンス数。この比率で示される**合計**の数値は、現在所有されているライセンスの総数（「最終報告」の日時時点）を表します。
- ピーク使用状況統計。使用中のピークライセンスを計算する際、Citrix Cloudは以下の期間で使用されたライセンスの最大数を取得します。
    - **過去24時間:** 過去24時間で一度に使用されたライセンスの最大数。
    - **今月:** 現在の暦月の開始から一度に使用されたライセンスの最大数。
    - **全期間:** サブスクリプションの開始から一度に使用されたライセンスの最大数。

    これらのピーク使用期間に表示される**合計**の数値は、その時点で所有されていたライセンスの総数を表します。所有ライセンスの総数が増減し、それに伴って割り当てライセンスが増加した場合、**合計**の数値はその時点での新しい所有ライセンス数を反映するように変更されます。ただし、対応する使用ピークがない場合、**合計**の数値は変更されません。

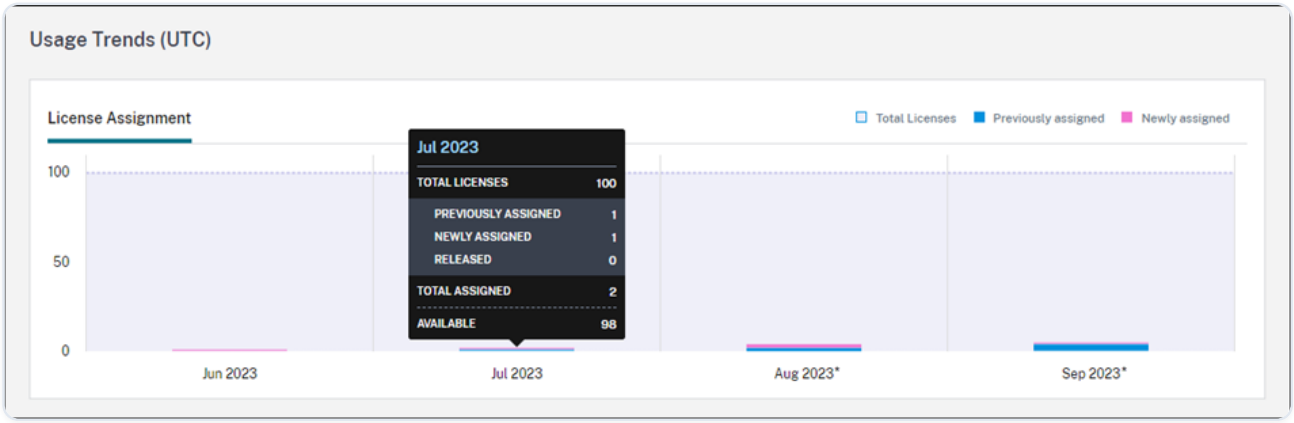
使用状況の傾向

Citrix Cloud は、ユーザー/デバイスライセンスまたは同時実行ユーザーライセンスのいずれかについて、使用状況の傾向の内訳を表示します。この内訳を表示するには、ライセンス概要ページから「**使用状況の詳細を表示**」を選択します。



ユーザーとデバイスの傾向

ユーザー/デバイスライセンスの場合、**使用状況の傾向**セクションでは、割り当てられたライセンスの内訳がグラフとして表示されます。



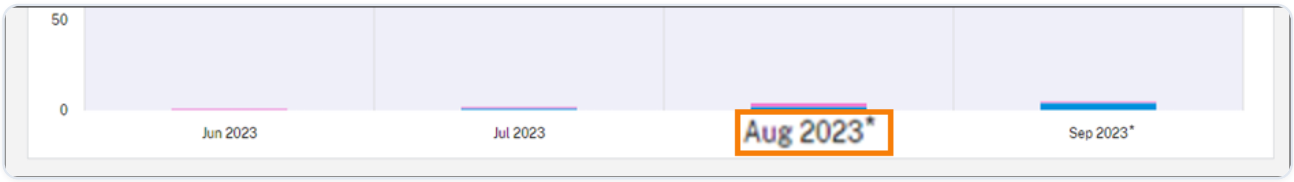
グラフ上の間隔をポイントすると、次の情報が表示されます。

- **合計ライセンス数:** すべてのエンタイトルメントにおけるクラウドサービス用に購入済みの合計ライセンス数。
- **以前に割り当て済み:** 前月に割り当てられたライセンスの数。たとえば、ユーザーが7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられたとします。このライセンス

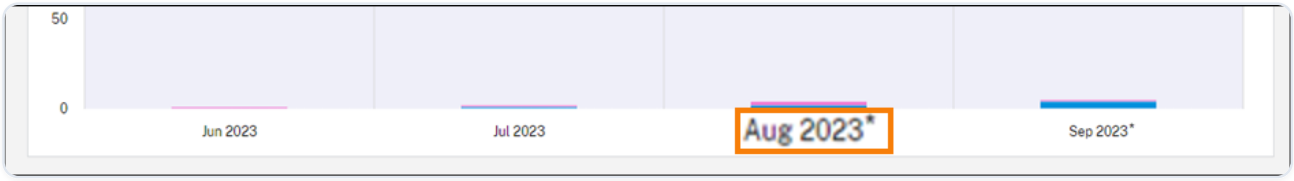
は、7月には「新規割り当て済み」としてカウントされます。8月には、このライセンスは「以前に割り当て済み」としてカウントされます。

- **新規割り当て済み:** 各月に割り当てられた新規ライセンスの数。たとえば、ユーザーが7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられたとします。このライセンスは、7月には「新規割り当て済み」としてカウントされます。

ドメインの切り捨てが有効になっている期間は、アスタリスクでマークされます。



ドメインの切り捨てが有効になっている期間は、アスタリスクでマークされます。



同時実行ユーザーの傾向

同時実行ユーザーライセンスの場合、**使用状況の傾向**セクションでは、次の情報が表示されます。

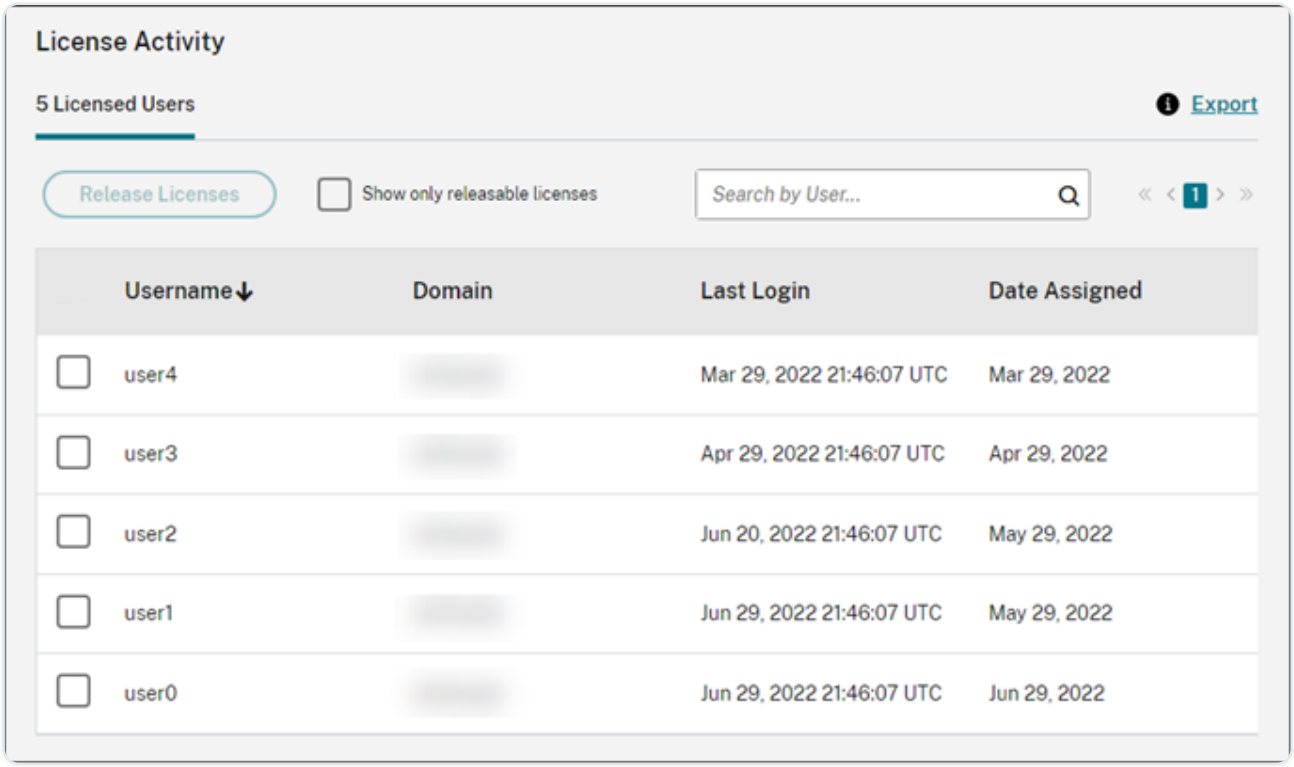
- **合計ライセンス:** 購入済みの同時使用ライセンスの合計数です。
- **ピーク使用ライセンス数:** 選択した日付範囲に割り当てられたライセンスの最大数です。デフォルトでは、Citrix Cloudは現在の暦年の各月のピーク使用状況を表示します。月別または時間別のピーク使用状況をドリルダウンするには、ドロップダウンメニューから表示したい暦月または日を選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloudは最新の時間間隔の現在のピーク使用状況を表示します。たとえば、まだ進行中の暦日を表示するためにドリルダウンした場合、現在の時刻までの各時間におけるライセンスの最大数が表示されます。次の5分間のカウント間隔でライセンスの最大数が増加した場合、Citrix Cloudは現在の時間のピーク使用状況を更新します。

グラフ上の間隔をポイントすると、その間隔の合計ライセンス数とピーク使用ライセンス数が表示されます。

ユーザーとデバイスのライセンスアクティビティ

ユーザー/デバイスライセンスの場合、**ライセンスアクティビティ**セクションには、ライセンスが割り当てられている個々のユーザーのリストと、そのユーザーにライセンスが割り当てられた日付が表示されます。このセクションは同時使用ライセンスでは利用できません。



リリース対象のライセンスのみを表示するようにリストをフィルタリングすることもできます。この記事の「割り当て済みライセンスのリリース」を参照してください。

ユーザー/デバイスライセンスのリリース

対象となるユーザー/デバイスライセンスのリリースは、サービスサブスクリプションの種類によって異なります。

- **年間サービスサブスクリプション:** 年間サブスクリプションをお持ちの場合、過去30日間にアプリまたはデスクトップを起動していないユーザーのライセンスをリリースできます。複数のライセンスを一括または個別にリリースできます。
- **月間サービスサブスクリプション:** 月間サブスクリプションをお持ちの場合、非アクティブ期間に関係なく、毎月1日にライセンスをリリースできます。

ライセンスが割り当てられると、割り当て期間は90日間となり、サービスへの接続が確立されます。ユーザーまたはデバイスが90日間アプリまたはデスクトップを起動しなかった場合、これらのライセンスは未使用ライセンスと見なされ、90日後にCitrix Cloudによってリリースされます。このプロセスは自動化されており、管理者の操作は不要です。

割り当て期間（90日間）が経過した後、管理者は以下のシナリオでのみ、手動でライセンスをリリースできます。

- ユーザーが会社に所属しなくなった場合。
- ユーザーは長期休暇中です。

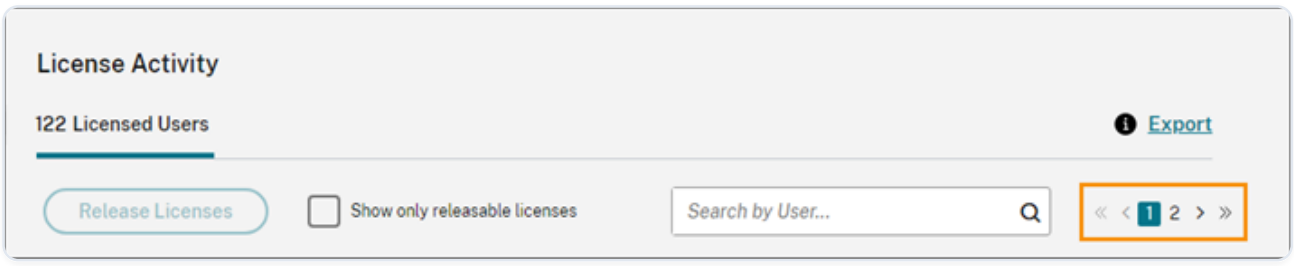
管理者は、デバイスがサービス停止中の場合にのみ、デバイスのライセンスを解放できます。

> **注:**
>
> - ライセンスの解放は、自動化されたプロセスに従うことをお勧めします。ただし、管理者が上記の理由以外で90日間の期間より前にライセンスを解放しようとすると、Citrix EULAに違反する可能性があります。この操作を実行する前に、Citrixにお問い合わせください。
>
> - 管理者は、UI を介して単一のライセンスを手動で解放できます。または、クラウドライセンス API を使用してライセンスを解放することもできます。詳細については、「Citrix Cloud ライセンスを管理するための API」を参照してください。

対象となるライセンスを見つける

ユーザーまたはデバイスが30日間アプリまたはデスクトップを起動していない場合、Citrix Cloud はライセンスを解放可能な状態にします。解放可能なライセンスは、選択可能な濃い灰色のチェックボックスとともに、ライセンスユーザーまたはライセンスデバイスのリストに表示されます。解放できないライセンスは、選択できないことを示す薄い灰色のチェックボックスを表示します。

ライセンスアクティビティセクションに表示されるリストには、一度に最大100個の割り当て済みライセンスが表示されます。100個を超えるライセンスがある場合は、ページコントロールを使用してリストを移動します。



対象となるライセンスをすばやく見つけるには、**ライセンスを解放**ボタンの横にある**解放可能なライセンスのみを表示**を選択します。この操作により、まだ解放の対象ではない割り当て済みライセンスが非表示になります。



対象となるライセンスを選択する

各ライセンスの横にある濃い灰色のチェックボックスを選択して、解放対象として選択します。ライセンスを選択すると、**ライセンスを解放**ボタンがアクティブになります。

解放可能なすべてのライセンスを1つずつ選択し、**ライセンスを解放**をクリックできます。

割り当てられたライセンスを解放する

1. 必要に応じて、**解放可能なライセンスを表示**をクリックして、解放が許可されているライセンスを持つユーザーのみを表示します。
2. 管理するユーザーを選択し、**ライセンスを解放**をクリックします。
3. 選択したユーザーを確認し、**ライセンスを解放**をクリックします。

同時ユーザーライセンスを解放する

同時ユーザーライセンスは、ユーザーがサインアウトするか、セッションから切断すると自動的に解放されます。これらのライセンスを手動で解放する必要はありません。

Endpoint Management のライセンスとアクティブな使用状況を監視する

ライセンスの割り当て

一般に、ユーザーはクラウドサービスを初めて使用する際にライセンスが割り当てられます。Endpoint Management の場合、ユーザーがデバイスを登録するとライセンスが割り当てられます。デバイスが登録されると、デバイスは定期的に Citrix Cloud にチェックインします。Citrix Cloud はこの「チェックインパルス」を使用して月間の使用状況を計算し、管理者がユーザーの最新のサービス使用状況を把握できるようにします。

初回使用は、ユーザーがデバイスを初めて登録したとき、またはデバイスの「チェックインパルス」が初めて発生したときに発生します。

ライセンスはユーザーごとに割り当てられます。したがって、2人のユーザーが同じデバイスを登録して使用する場合、2つのライセンスが割り当てられます。

ライセンスの概要と詳細

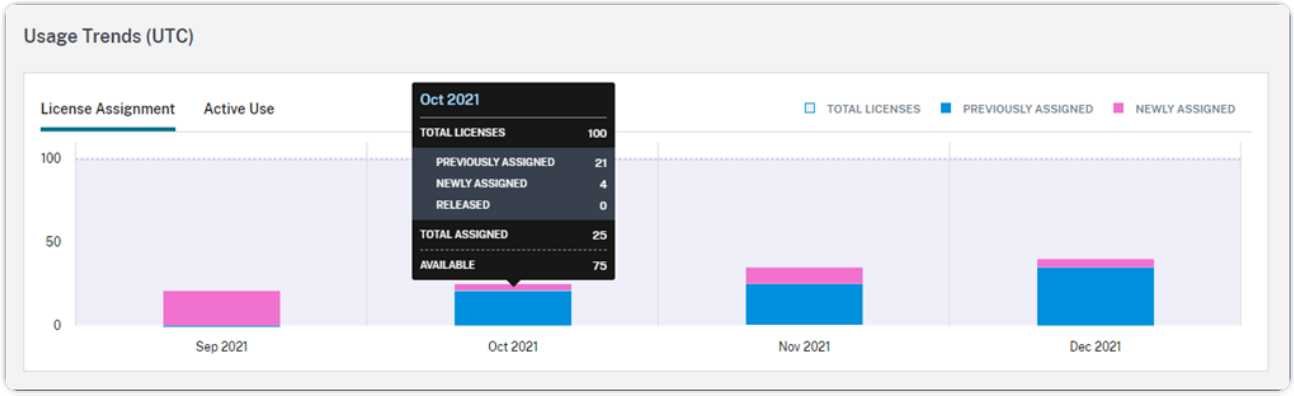
ライセンスと使用状況の概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-cem.png)

ライセンスの概要には、サポートされている各サービスについて、以下の情報が一目でわかるように表示されます。

- 割り当てられた購入済みライセンスの合計に対する割合。この割合が100%に近づくと、緑から黄色に変わります。100%を超えると、赤に変わります。
- 割り当てられたライセンスと購入済みライセンスの比率、および残りの利用可能なライセンス数。
- 月次および日次のアクティブな使用状況統計:
    - 月間アクティブ使用とは、過去30日間にサービスを使用したユニークユーザーの数を指します。
    - 日間アクティブ使用とは、過去24時間以内にサービスを使用したユニークユーザーの数を指します。
- クラウドサービスのサブスクリプションが期限切れになるまでの残り時間。サブスクリプションが今後90日以内に期限切れになる場合、警告メッセージが表示されます。

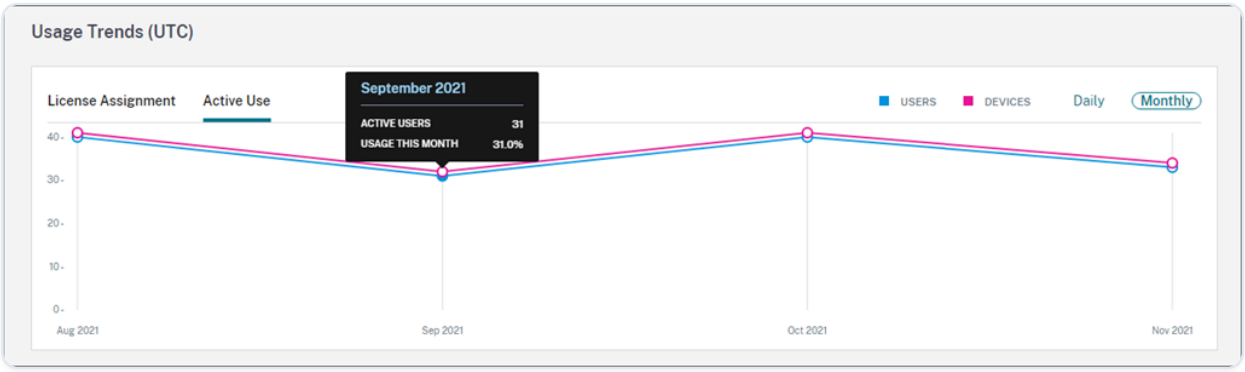
使用状況の傾向

ライセンスの詳細な表示については、**使用状況の詳細を表示**をクリックしてください。そうすると、使用状況の傾向、およびクラウドサービスライセンスを使用している個々のユーザーとデバイスの内訳を確認できます。



この内訳には、以下の情報が表示されます。

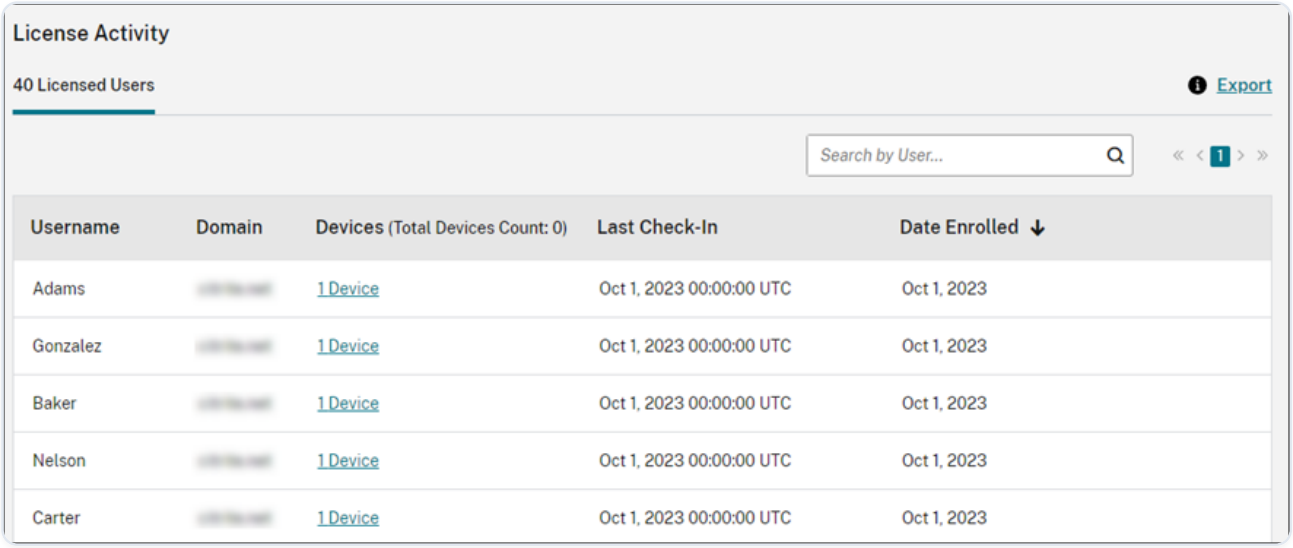
- **合計ライセンス数:** すべてのエンタイトルメントにおけるクラウドサービスの購入済みライセンスの合計数です。
- **以前に割り当て済み:** 各月の初めにすでに割り当てられていたクラウドサービスライセンスです。たとえば、ユーザーに7月にライセンスが割り当てられた場合、その割り当ては8月の「以前に割り当て済み」の数に含まれます。
- **新規割り当て済み:** 各月中に割り当てられたクラウドサービスライセンスの数です。たとえば、7月に初めてクラウドサービスにアクセスするユーザーにはライセンスが割り当てられます。このライセンスは、7月の「新規割り当て済み」の数に含まれます。
- **アクティブな使用状況:** それぞれ、前暦月および前暦年における日次および月次のアクティブな使用状況の傾向です。



ライセンスアクティビティ

ライセンスアクティビティセクションには、以下の情報を含むリストが表示されます。

- ライセンスが割り当てられている個々のコンシューマー
- ライセンスが割り当てられた日付
- 登録済みデバイスの数と、各ユーザーの最終チェックイン日



登録済みデバイスの表示

特定のユーザーの登録済みデバイスの数を表示するには、**デバイス**列のリンクをクリックします。

「デバイス」リンクが強調表示されたライセンスユーザー(/en-us/citrix-cloud/media/lic-usage-licensed-devices-select-cem.png)

Citrix Cloudは、ユーザーが登録したデバイスのリストと、各デバイスの最終チェックイン日時を表示します。

登録済みデバイスの詳細を含むライセンスユーザーメニュー(/en-us/citrix-cloud/media/lic-usage-licensed-devices-cem.png)

割り当てられたライセンスを自動的に解放する

Citrix Cloudは、過去30日間で以下の**すべて**の条件を満たすユーザーのライセンスを自動的に解放します。

- ユーザーが新しいデバイスを登録していない。
- ユーザーがCitrix Cloudにチェックインしていない既存のデバイスを持っている。

対象となるライセンスを解放するために、他のアクションは必要ありません。

対象となるライセンスが解放された後、ユーザーはデバイスを登録することで別のライセンスを取得できます。

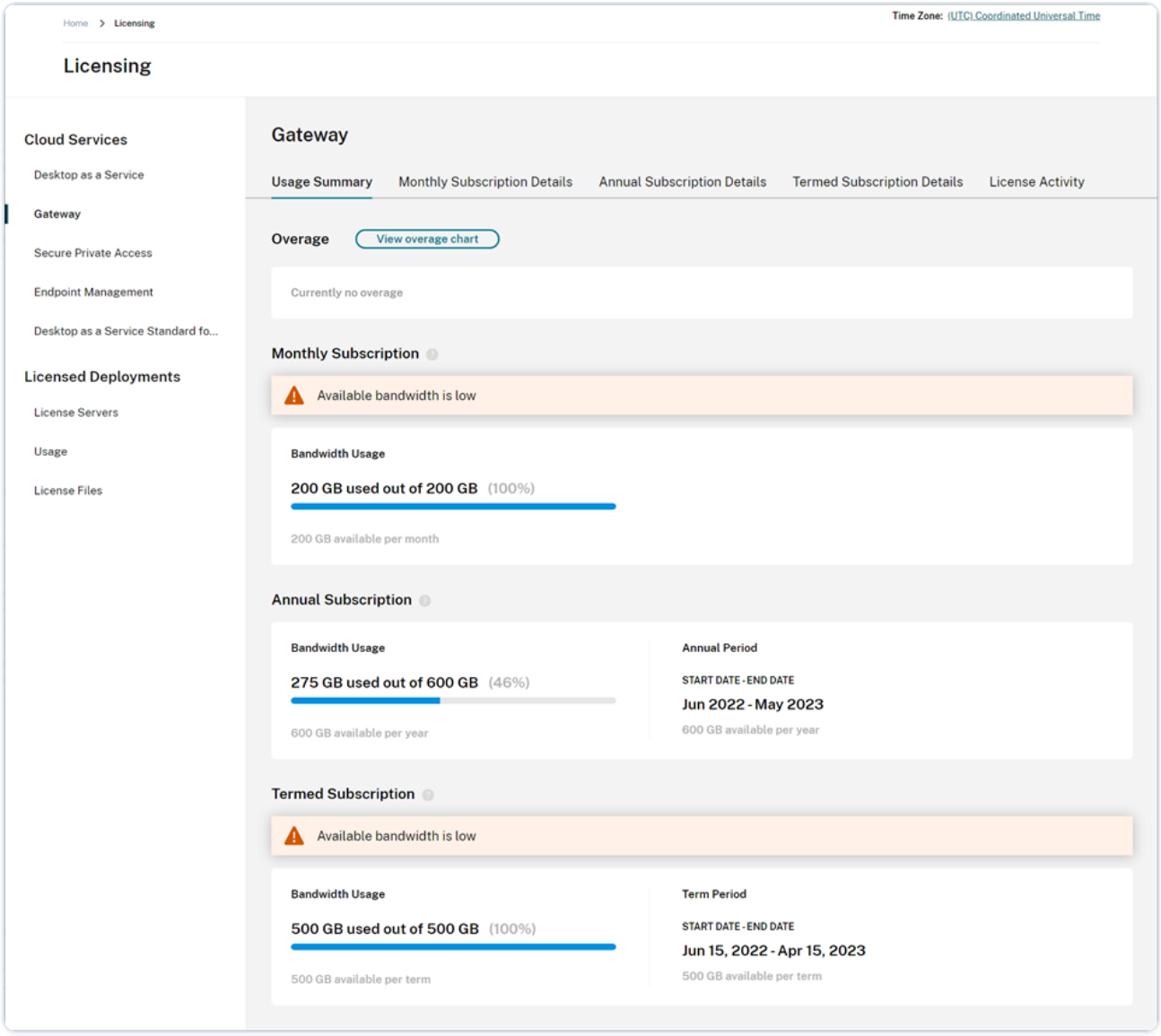
Gateway service の帯域幅使用量を監視する

この記事では、Citrix DaaS (旧称 Citrix Virtual Apps and Desktops™ service) および Citrix® StoreFront Cloud とともに使用される場合の Gateway service を介した帯域幅使用量について説明します。Virtual Apps Essentials service に含まれる Gateway service の帯域幅消費量は、Citrix Cloud 管理コンソールの ページには表示されません。

> **注:**
>
> Gateway service のライセンスは、仮想アプリとデスクトップの使用に関連する帯域幅使用量を理解するのに役立ちます。Citrix® は、お客様の環境における帯域幅使用量の割り当てを強制しません。帯域幅の割り当てを超過した場合でも、Citrix は本番ワークロードやサービスの運用に干渉しません。Citrix が Gateway service および帯域幅使用量のポリシーの適用方法を変更する場合、これらの変更が有効になる前に Citrix から通知されます。

使用状況の概要

使用状況の概要では、各 Gateway service サブスクリプションの帯域幅使用量と、すべてのサブスクリプション (月次、年次、期間) にわたる合計超過使用量を一目で確認できます。



Citrix Cloud™ は、各サブスクリプションタイプにおける帯域幅の合計量と消費された帯域幅の量を表示します。

サブスクリプションの種類に応じて、Citrix Cloud はサブスクリプションの請求期間も表示します。

- 月次サブスクリプション: Citrix Cloud は現在の請求期間を表示しません。これらのサブスクリプションの場合、請求期間は毎月1日に始まり、その月の最終日に終了します。
- 年次サブスクリプション: Citrix Cloud は請求期間の開始日と終了日を表示します。これらのサブスクリプションの場合、請求期間は1年間です。

- 期間サブスクリプション: Citrix Cloud は請求期間の開始日と終了日を表示します。これらのサブスクリプションの場合、請求期間はサブスクリプションが購入された期間の長さです。たとえば、3年間の期間サブスクリプションが購入された場合、請求期間の開始日と終了日はその3年間の間隔に対応します。

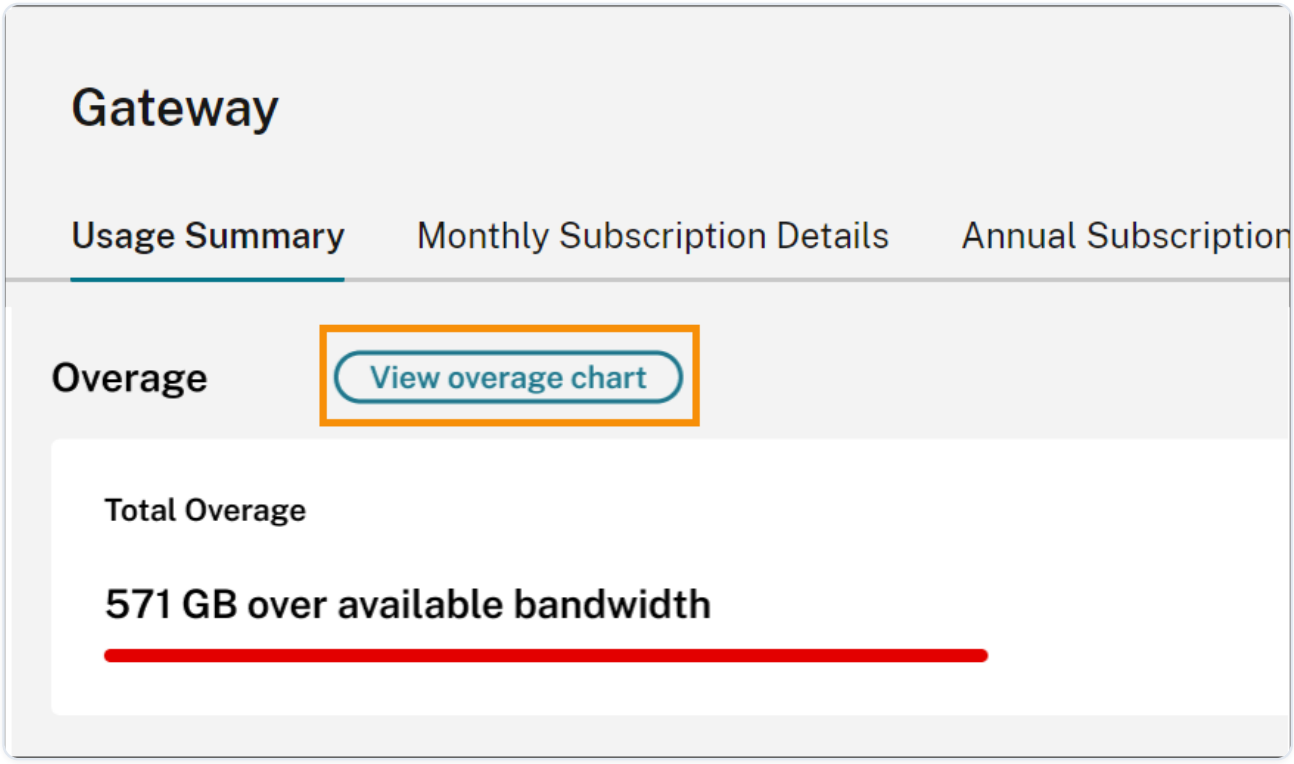
サブスクリプションが90日以内に期限切れになる場合、そのサブスクリプションに対して警告メッセージが表示されます。

超過使用量

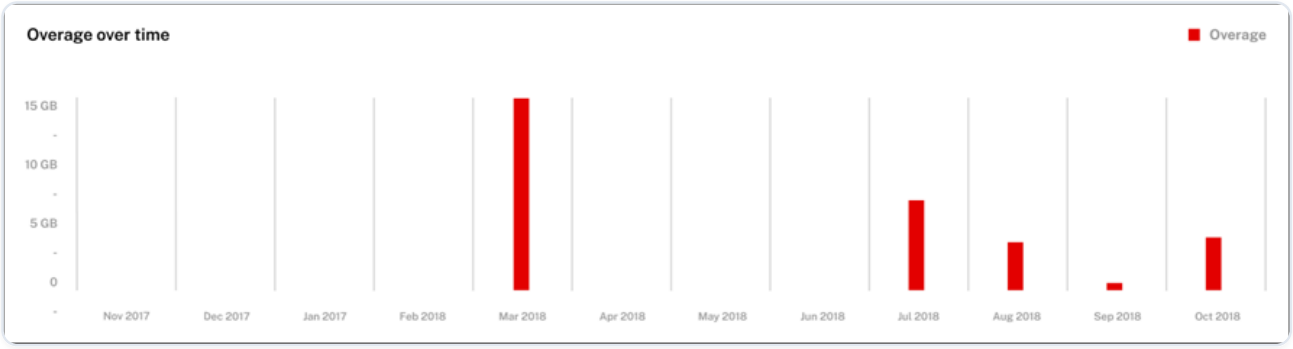
Citrix Cloud は、すべてのサブスクリプションにわたる超過使用量を月単位で計算します。購入した帯域幅よりも多く消費した場合、Citrix Cloud は超過帯域幅を超過使用量として表示します。

複数のサブスクリプションをお持ちの場合、Citrix Cloudは、最初に最も早く終了する日付のサブスクリプションに対して帯域幅の使用量を測定します。そのサブスクリプションの帯域幅割り当てを使い切ると、Citrix Cloudは次に最も早く終了する日付のサブスクリプションに対して帯域幅の使用量を測定します。すべてのサブスクリプションの帯域幅割り当てを使い切ると、Citrix Cloudは超過使用量を「超過分」として表示します。

使用状況の概要ページには、当月の合計超過分が表示されます。過去の超過分を表示するには、**「超過分グラフを表示」**を選択します。



Citrix Cloudは、過去12か月間の合計超過分のグラフを表示します。



当月の超過分は翌月に繰り越されません。翌月が始まると、合計超過分はゼロにリセットされます。

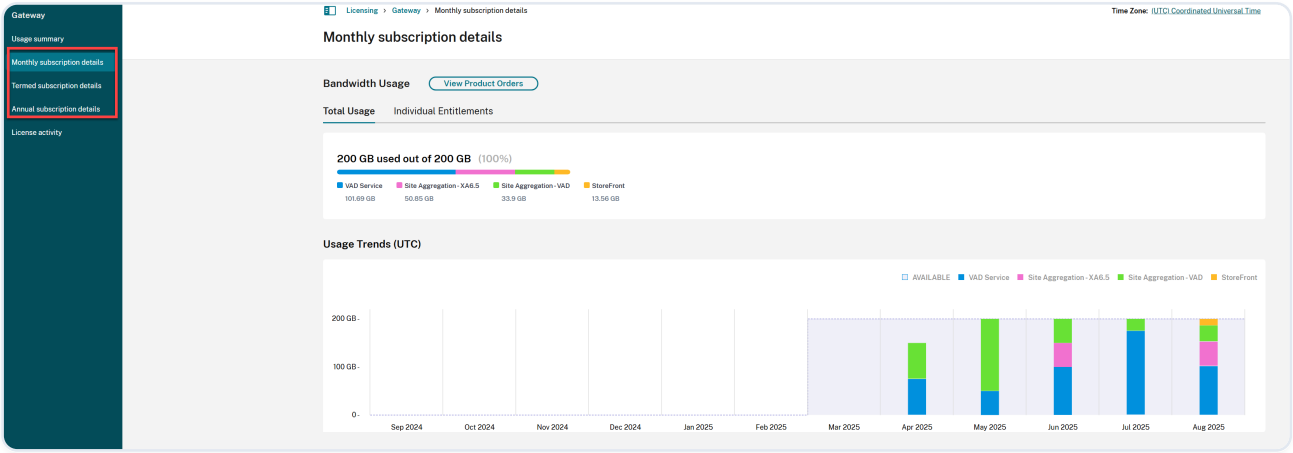
未使用の帯域幅

Citrix Cloudは、次回の請求期間にサブスクリプションの帯域幅使用量を自動的にリセットします。特定のサブスクリプション期間中に帯域幅の全量を使用しなかった場合でも、Citrix Cloudは未使用の帯域幅を次回の請求期間に繰り越しません。

たとえば、月額サブスクリプションに合計150 GBの帯域幅が含まれており、特定の月に100 GBの帯域幅を使用したとします。Citrix Cloudは使用量をゼロにリセットし、翌月の初めに150 GBを合計帯域幅として表示します。未使用の帯域幅は、合計帯域幅の割り当てに追加されません。

使用状況の詳細

サブスクリプションの詳細を表示するには、コンソールの上部にある月次、年次、または期間サブスクリプションの詳細タブを選択します。



各サブスクリプションタイプについて、詳細タブには次の情報が表示されます。

- **合計使用量:** 特定のタイプのすべてのサブスクリプションで利用可能な合計帯域幅のうち、消費された帯域幅の量。月次サブスクリプションの場合、合計使用量は当月分が表示されます。年次および期間サブスクリプションの場合、合計使用量はすべての年次または期間サブスクリプションにわたる累積値です。

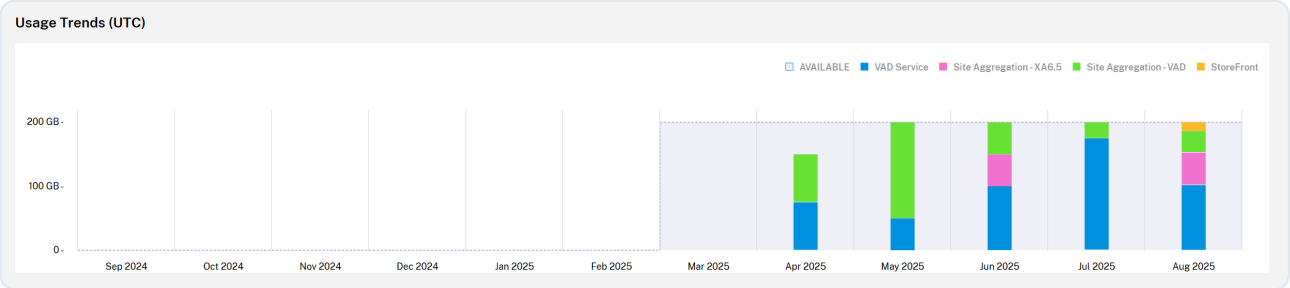
- **個別のエンタイトルメント:** 特定のタイプの各サブスクリプションで消費された帯域幅の合計量。たとえば、複数の年次サブスクリプションをお持ちの場合、このタブには各年次サブスクリプションの使用状況の内訳が個別に表示されます。

消費された帯域幅の量は、Citrix DaaS (**VAD Service**) を介したアクセス、または(/ja-jp/citrix-workspace/optimize-cvad/aggregate-sites.html)を使用してオンプレミスのVirtual Apps and Desktops展開を介したアクセスに基づいて分類されます。

使用状況の傾向

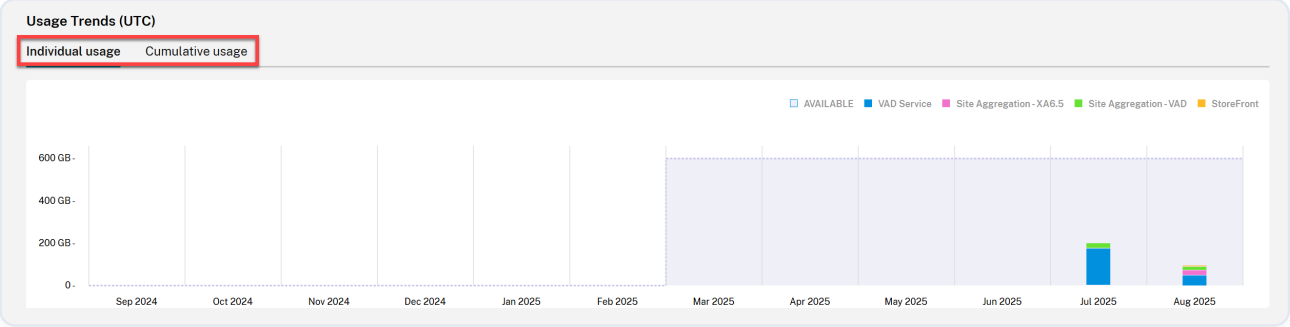
使用状況の傾向セクションには、過去12か月間の使用状況の内訳が表示されます。

月額サブスクリプションの場合、使用状況は使用された各月ごとに表示されます。

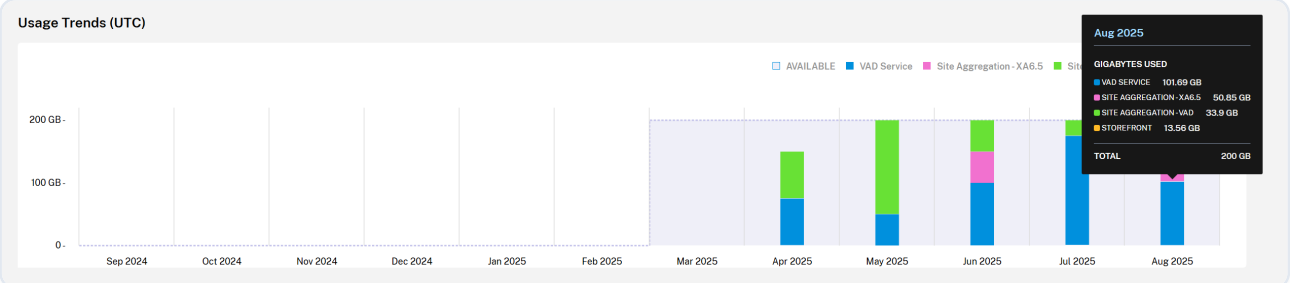


年間および期間サブスクリプションの場合、このセクションには次のビューが含まれます。

- **個別の使用状況:** 現在の請求期間の各月中に発生した帯域幅の使用状況。
- **累積使用状況:** 現在の請求期間の各月で累積された帯域幅の使用状況。



すべてのサブスクリプションタイプで、使用状況の傾向グラフのバーをポイントすると、その時点での帯域幅の使用状況がアクセス方法別に分類されて表示されます。



ライセンスアクティビティ

ライセンスアクティビティセクションには、次の情報が表示されます。

- **ライセンスユーザー:** 割り当てられたライセンスを持つ個々のユーザーのリストを表示します。このリストには、各ユーザーが属するドメイン、過去30日間に使用された帯域幅の量、およびユーザーが帯域幅の使用を必要とするサービスを最後に使用した日付が含まれます。
- **上位ユーザー:** 帯域幅の使用状況に基づいて上位10ユーザーのリストを表示します。このリストには、アクセスタイプ（Citrix DaaS™またはサイト集約によるオンプレミスのVirtual Apps and Desktops）に応じた、過去30日間の各ユーザーの使用状況の内訳が含まれます。

「ライセンスアクティビティ」セクション（「ライセンスユーザーテーブル」タブと「トップユーザー」タブが強調表示されています）(/en-us/citrix-cloud/media/lic-usage-license-activity-tabs-gateway.png)

Citrix Cloudは、特定のユーザーがライセンスを使用しなくなった場合でも、過去30日間の帯域幅使用量を表示します。Gatewayサービスサブスクリプションの有効期限が切れた場合でも、Citrix Cloudは個々のユーザーが30日間に消費した帯域幅を表示します。

特定のユーザーの使用状況の詳細を表示する

1. を選択し、表示したいユーザーをリストから見つけます。
2. ページの右端にある省略記号メニューから を選択します。

「ライセンスアクティビティ」リスト（「使用状況の表示」メニューが強調表示されています）(/en-us/citrix-cloud/media/lic-usage-license-activity-view-usage-gateway.png)

Citrix Cloudは、アクセス別に分類されたユーザーの帯域幅を表示します。

単一ユーザーの帯域幅詳細ビュー(/en-us/citrix-cloud/media/lic-usage-view-single-user-gateway.png)

トップユーザーの使用状況の詳細を表示する

を選択します。

「ライセンスアクティビティ」セクション（「トップユーザーの表示」が強調表示されています）(/en-us/citrix-cloud/media/lic-usage-view-top-users-gateway.png)

Citrix Cloudは、アクセス別に分類されたトップユーザーの帯域幅使用量のグラフを表示します。

デフォルトでは、 チャートには、過去30日間に最も多くの帯域幅を使用した上位10人のユーザーが表示されます。この表示を、上位5人、上位15人、または上位20人のユーザーを表示するように

変更できます。また、期間を に変更すると、サブスクリプションの有効期間全体で上位のユーザーが表示されます。この表示を変更するには、各メニューからオプションを選択します。

パラメーターメニューが強調表示されたトップユーザーチャート(/en-us/citrix-cloud/media/lic-usage-top-users-parameters-gateway.png)

Secure Private Access のライセンスと使用状況を監視する

ライセンスの割り当て

一意のユーザーが Web および SaaS アプリ、または TCP および UDP アプリを初めて起動したときに、ライセンスが割り当てられます。

ライセンスの概要

ライセンスの概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-swa.png)

ライセンスの概要には、次の情報が表示されます。

- 割り当てられている購入済みライセンス総数の割合。
  - 割合が 100% に近づくと、緑から黄色に変わります。割合が 100% を超えると、赤に変わります。
- 割り当て済みライセンスと購入済みライセンスの比率、および割り当て可能なライセンスの数。
- 月次および日次のアクティブな使用状況統計:
  - 月間アクティブ使用量とは、過去 30 日間にサービスを使用した一意のユーザーの数を指します。
  - 日間アクティブ使用量とは、過去 24 時間にサービスを使用した一意のユーザーの数を指します。
- すべてのサブスクリプションの帯域幅の総量に対して消費された帯域幅の量。
- クラウドサービスサブスクリプションの有効期限が切れるまでの残り時間。サブスクリプションが今後 90 日以内に期限切れになる場合、警告メッセージが表示されます。

使用されているライセンスと帯域幅

Secure Private Access Advancedサブスクリプションでは、各ユーザーは月あたり5 GBの帯域幅（ユーザーあたり年間60 GB）にアクセスできます。Secure Private Access Standardサブスクリ

プションでは、各ユーザーは月あたり1 GBの帯域幅（ユーザーあたり年間12 GB）にアクセスできます。この帯域幅は、ライセンス数とサブスクリプション期間全体でプールされます。

たとえば、3年間で100ライセンスを購入した場合、合計18000 GBの帯域幅（3年間で年間6000 GB）を利用できます。この帯域幅は、3年間の期間中、すべてのライセンスユーザーに分配されます。さらにサブスクリプションを購入すると、Citrix Cloud™はすべてのサブスクリプションの合計ライセンス数と帯域幅を表示します。

サブスクリプション期間中に帯域幅をすべて使用しなかった場合、Citrix Cloudは更新時に未使用の帯域幅を繰り越ししません。購入した帯域幅を超えて使用し、サブスクリプションが期限切れになった場合、サブスクリプションを更新しても利用可能な帯域幅はゼロのままです。

期間が重複する複数のサブスクリプションの場合、各サブスクリプションの有効期限が切れると、そのサブスクリプションに関連付けられた帯域幅はライセンスから削除されます。たとえば、2つのサブスクリプションを購入した場合、Citrix Cloudは両方のサブスクリプションの合計ライセンスと合計帯域幅を表示します。最初のサブスクリプションの有効期限が切れると、Citrix Cloudは有効期限が切れていないサブスクリプションに関連付けられた帯域幅のみを表示します。

使用状況の傾向

帯域幅の使用状況とライセンスの詳細を表示するには、 をクリックします。

が強調表示されたライセンス概要ビュー(/en-us/citrix-cloud/media/lic-usage-summary-view-details-button-swa.png)

Citrix Cloudは、ユーザーがアクセスできるアプリの種類に基づいて、帯域幅消費の内訳を表示します。

使用済みライセンスギガバイト(/en-us/citrix-cloud/media/lic-spa-gigabyte.png)

また、使用状況の傾向や、クラウドサービスライセンスと帯域幅を消費している個々のユーザーの内訳も確認できます。

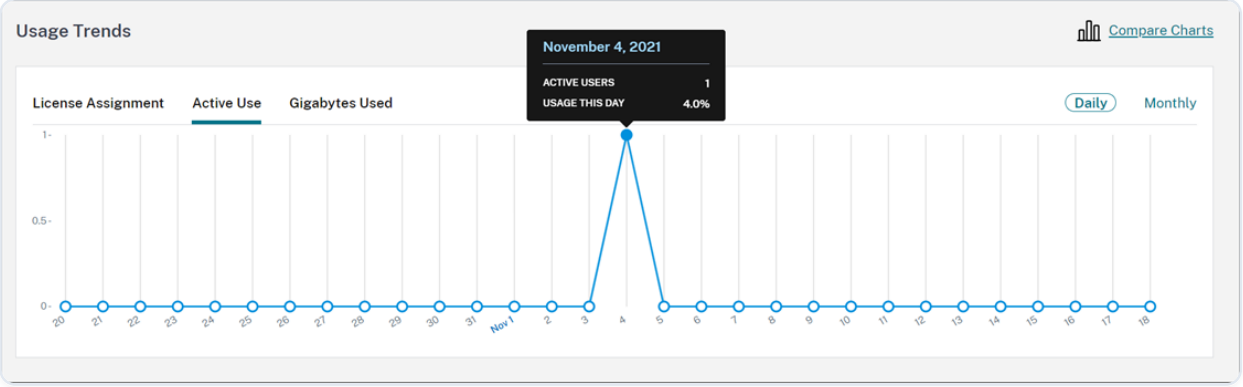
ライセンス使用状況割り当て傾向グラフ(/en-us/citrix-cloud/media/lic-usage-assignment-trends-callout-swa.png)

の下のこの内訳には、次の情報が表示されます。

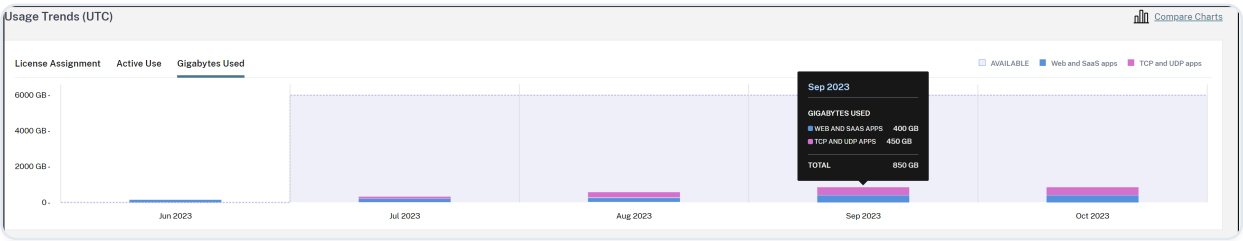
- タブで:
    - **合計ライセンス:** すべてのエンタイトルメントにおけるクラウドサービスの購入済みライセンスの合計。

- **以前に割り当て済み:** 各月の初めにすでに割り当てられていたクラウドサービスライセンス。たとえば、ユーザーに7月にライセンスが割り当てられた場合、Citrix Cloudはその割り当てを8月の「以前に割り当て済み」の数に含めます。
- **新規割り当て:** 各月に割り当てられたライセンスの数。たとえば、7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられた場合、Citrix Cloudはそのライセンスを7月の新規割り当て数に含めます。

- **アクティブな使用状況**タブ: 前の暦月と暦年における、それぞれの日次および月次のアクティブな使用状況の傾向。



- **使用ギガバイト数**タブ: 利用可能な総帯域幅のうち消費された帯域幅の量。Webアプリ、SaaSアプリ、TCPアプリ、UDPアプリなど、ユーザーごとの使用状況とアプリケーションごとの情報が表示されます。



ライセンス割り当て、アクティブな使用状況、帯域幅の使用状況の傾向を比較するには、**チャートの比較**を選択します。

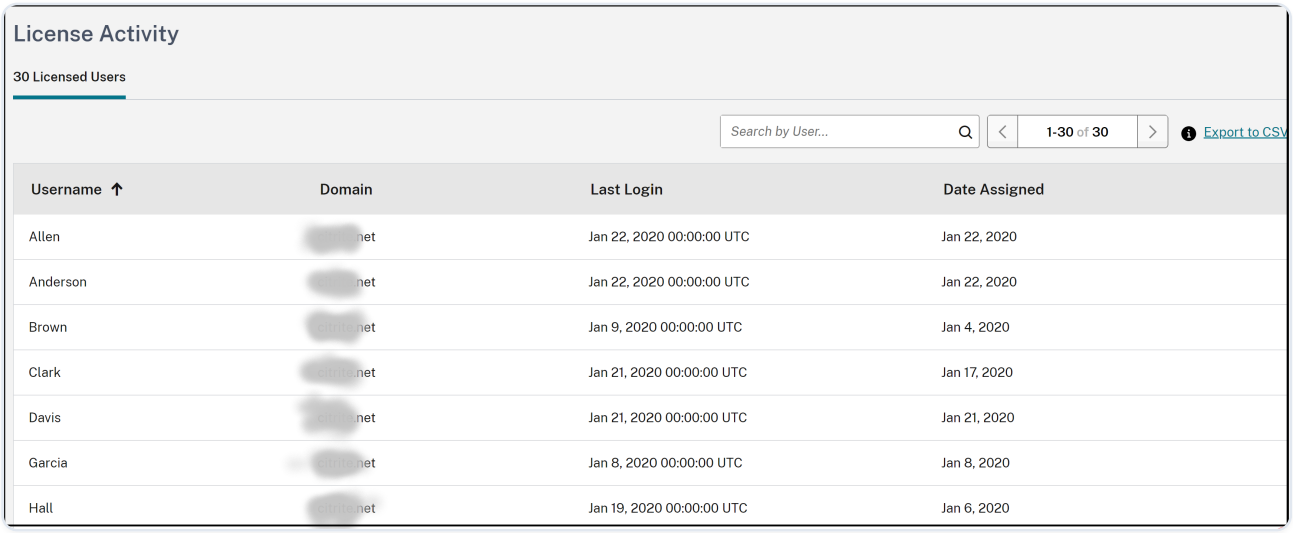


注：

使用状況の傾向は、現在のサブスクリプション期間の長さに対して累積されます。サブスクリプションを更新すると、新しいサブスクリプション期間の開始時に使用状況の傾向がリセットされます。

ライセンスアクティビティ

ライセンスアクティビティセクションには、次の情報も表示されます。



- ライセンスが割り当てられている個々のユーザーのリスト。
- ユーザーが属するドメイン。
- ユーザーが最後にサービスを使用した日付。
- ユーザーにライセンスが割り当てられた日付。

割り当てられたライセンスを解放する

Citrix Cloudは、過去30日間サービスを使用していない場合、自動的にライセンスを解放します。ライセンスを解放するためにCitrix管理者が行うべき操作はありません。

ライセンスが解放されると、残りのライセンス数が増加し、割り当てられたライセンス数がそれに応じて減少します。ライセンスが解放された後、クラウドサービスにサインインして使用することで、別のライセンスを取得できます。

Citrix DaaS™向けCitrix Managed Azureリソース使用状況の監視

Citrix DaaS (旧称 Citrix Virtual Apps and Desktops™ service) のエンタイトルメントを購入すると、Citrix Managed Azureサブスクリプション内のリソースを使用できるCitrix Azure Consumption Fundも購入できます。これらのリソースは、オンプレミスのVDAと並行して、ユーザーにアプリやデスクトップを配信するために使用できます。

Citrix Azure Consumption Fundを購入すると、以下のいずれかの方法で消費量を支払うことができます。

- 従量課金制: 特定の月に使用したCitrix Managed Azureリソースについて、Citrixは翌月に請求します。Citrix Cloud™は使用状況を「超過分」として表示します。

- 前払い消費: 消費量を月単位または年単位（期間指定）で前払いできます。前払い消費量を超過した使用量については、Citrix Cloudはこれを「超過分」として表示します。特定の月の超過分については、Citrixは翌月に請求します。

各消費単位は1.00米ドル相当です。Citrix Cloudのライセンスコンソールは、使用した単位を追跡するのに役立ちます。

消費コストを見積もるには、Citrix Managed Azure Consumption Calculatorを使用してください。Citrix DaaS Standard for Azure (旧称 Citrix Virtual Apps and Desktops Standard for Azure) の消費コストとライセンスコストを見積もるには、Licensing and Consumption Calculatorを使用してください。

サポートされている製品

Citrix DaaSの以下のエディションで消費量の監視が可能です。

- Citrix DaaS アドバンスト (旧称 Virtual Apps アドバンスト)
- Citrix DaaS プレミアム (旧称 Virtual Apps プレミアム)
- Citrix DaaS Advanced Plus (旧称 バーチャルアプリ&デスクトップ アドバンスト)
- Citrix DaaS Premium (旧称 バーチャルアプリ&デスクトップ プレミアム)
- Citrix DaaS スタンダード for Azure (旧称 Virtual Apps and Desktops スタンダード for Azure)

消費量の概要

Citrix Managed Consumptionセクションには、お客様のConsumption Fundで使用されたユニットの概要が表示されます。

シトリックス マネージド コンサンプションの概要(/en-us/citrix-cloud/media/lic-usage-cvads-managed-consumption-summary.png)

月間消費量には、お客様が購入した月間Consumption Fundユニットの総数のうち、当月に使用した消費ユニット数が表示されます。月間消費量は毎月リセットされます。未使用の消費ユニットは翌月に繰り越されません。

期間消費量には、お客様が購入した期間Consumption Fundユニットの総数のうち、使用した消費ユニット数が表示されます。月間消費ユニットと同様に、未使用の期間消費ユニットは翌年に繰り越されません。

超過消費量には、お客様のAzure Consumption Fundのユニット数を超えて使用した消費ユニット数が表示されます。Citrix Managed Azureリソースを従量課金制で使用する場合、消費量はデフォルトで超過として表示されます。

超過の測定方法

Azure Consumption Fundを従量課金制で使用する場合、Citrix Cloudは当月に使用した消費ユニット数を超過として表示します。

月単位または年単位で消費量を前払いした場合、Citrix Cloudは当月または当年に使用した月間または期間消費ユニット数を表示します。購入したユニット数よりも多く消費した場合、Citrix Cloudは超過ユニットを超過として表示します。

月単位と年単位の両方で消費量を前払いした場合、Citrix Cloudはまず購入した月間ユニットに対して消費量を測定します。それらのユニットが消費された後、Citrix Cloudは年間ユニットに対して消費量を測定します。それらのユニットが消費された後、Citrix Cloudは消費した超過ユニットを超過として表示します。

追加の消費ユニットを購入し、アカウントに既存の超過がある場合、新しい消費ユニットは超過には適用されません。新しい消費ユニットは、それらのユニットが購入された後に発生する使用量にのみ適用されます。

消費量の詳細

消費ユニットの詳細を表示するには、概要の右端にある**View Usage Details**をクリックします。詳細ページには、消費量と使用傾向の内訳が表示されます。

リソースの内訳を含む使用状況の詳細ページ(/en-us/citrix-cloud/media/lic-usage-cvads-consumption-usage-details.png)

使用状況レポート

指定した期間の使用状況情報をCSVファイルとしてダウンロードできます。**Download Data**をクリックして、CSVファイルを生成し、ローカルマシンにダウンロードします。

すべての使用状況が反映されるまで、データは日または月の終わりから最大72時間かかる場合があります。

CSVファイルには、次のセクションが含まれています。

- レポートの日付範囲の前後で利用可能な消費ユニット、合計使用料金、および保留中の超過分を示すレポートの概要。

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.

Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	

Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

- レポートの日付範囲の各日における合計使用料金、残りの月次および期間資金、および超過料金を示す日次概要。

Daily Summary

Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

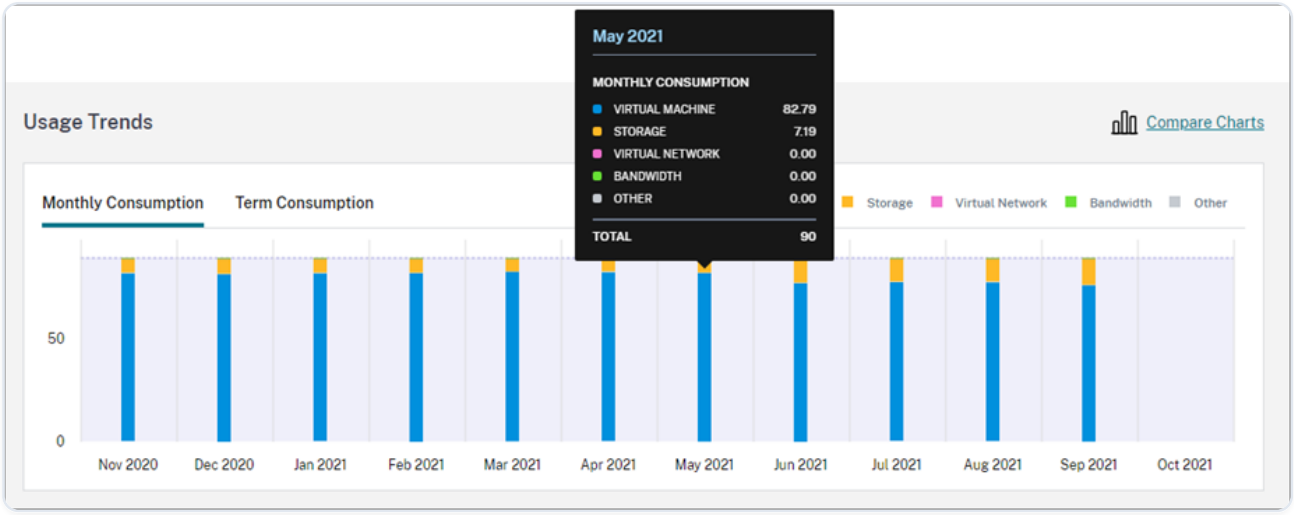
- レポートの日付範囲の各日におけるAzure VM、ネットワーク接続、Azureストレージ、および帯域幅の従量制使用量。

Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

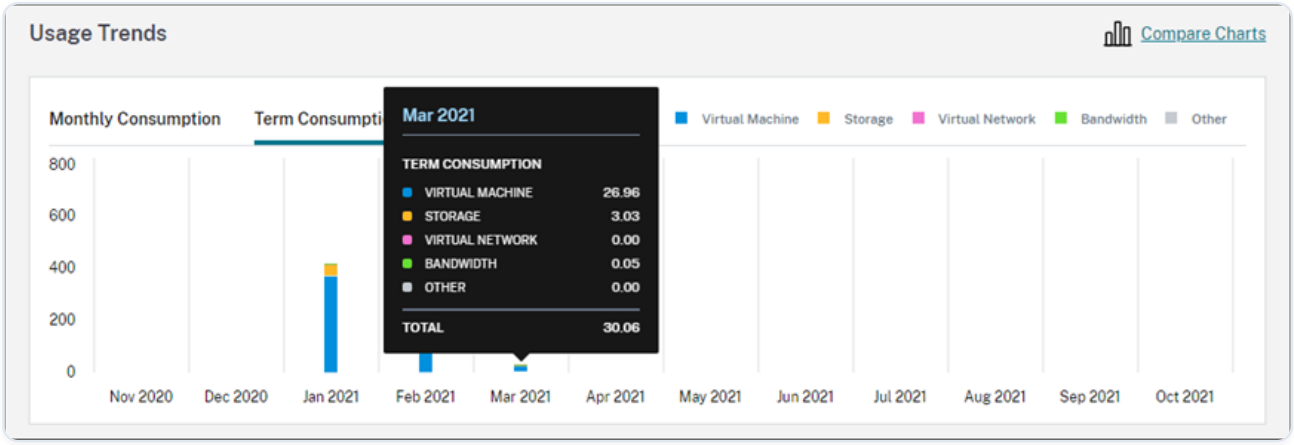
使用状況の傾向と消費アクティビティ

使用状況の傾向セクションには、使用したCitrix Managed Azureリソースのグラフが表示されます。グラフのバーをポイントすると、仮想マシン、ストレージ、仮想ネットワークリソース、帯域幅など、その月に消費したリソースの数量が表示されます。

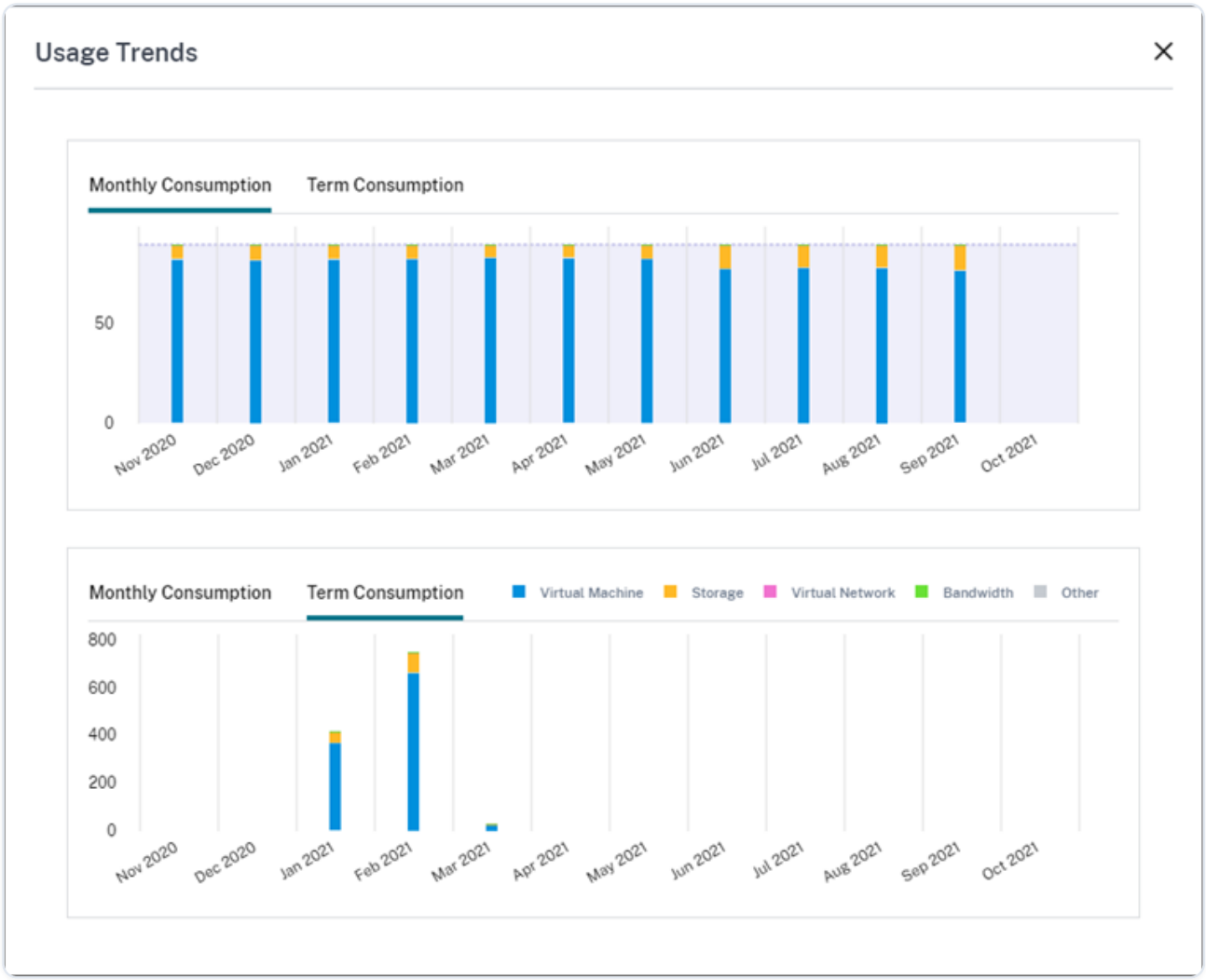
過去12か月間の月次消費量を表示するには、**月次消費量**を選択します。



前年の各月の期間消費量を表示するには、**期間消費量**を選択します。



月次および年次の両方の消費ユニットを購入した場合は、グラフの右端にある**グラフの比較**を選択して、月次および期間の消費傾向を単一のビューで表示します。



消費アクティビティセクションには、各月の消費ユニットのリストも表示されます。



Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

消費アクティビティには、次の情報が含まれます。

- **使用済み:** 各月に使用されたユニット数。
- **所有済み:** 各月に購入されたユニットの合計数。
- **残数:** 各月に未使用だった購入済みユニット数。
- **超過:** 各月に購入済みユニットを超過して消費されたユニット数。

割り当てられたライセンスを解放する

ライセンスの割り当てが解放の対象となる時期は、購入した消費ファンドユニットによって異なります。

次の場合は、30日後に非アクティブなライセンスを解放できます。

- サービス展開でCitrix Managed Azureサブスクリプションを使用していない場合。
- サービス展開で使用するために年間消費ユニットを購入した場合。

次の場合は、ユーザーまたはデバイスがアプリやデスクトップを起動していないことを条件に、当月中に非アクティブなライセンスを解放できます。

- サービス展開で使用するために月間消費ファンドユニットを購入した場合。
- 月間および年間の両方の消費ファンドユニットを購入した場合。

対象となるライセンスを解放する手順については、次の記事を参照してください。

- シトリックス DaaS（ユーザー/デバイスモデル）：割り当て済みライセンスを解放
- Citrix DaaS Standard for Azure: 割り当て済みライセンスを解放

オンプレミス展開のライセンスと使用状況を監視する

> **重要:**
>
> 使用状況インサイトは、従来のライセンスファイルにのみ適用され、ライセンスアクティベーションサービスには適用されません。

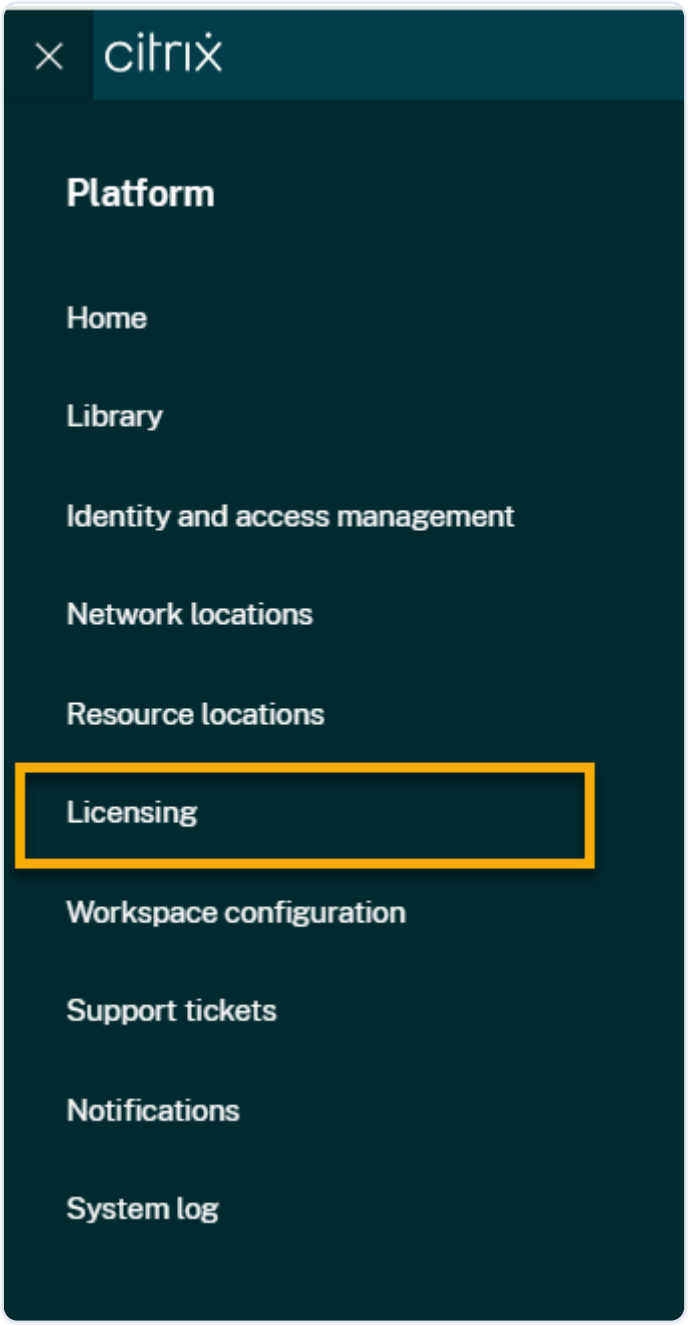
> Citrix Cloud™におけるライセンス展開のエクスペリエンスは、以下の機能で構成されています。

- 製品登録: 既存のCitrix License ServerをCitrix Cloudに登録して、展開に関する追加の使用状況インサイトとレポートを取得します。
- License Serverのステータス: Citrix License Serverのステータスを表示して、どのサーバーが正常に使用状況を報告しているか、およびいつCitrix Cloudに最後に使用状況を報告したかを把握します。
- 使用状況インサイト: Citrix License Server全体でインストールされ使用されているライセンスの数を確認し、過去のライセンス使用状況の傾向に関するインサイトを得ます。

サポートされている製品

Citrix License Serverの使用状況インサイトは、同時接続およびユーザー/デバイスライセンスモデルのすべてのVirtual Apps and Desktopsエディションで利用できます。

Citrix License Serverの使用状況インサイトを表示するには、コンソールメニューから**Licensing**を選択し、次に**Licensed Deployments**を選択します。



前提条件

Citrix License Serverの使用状況インサイトを使用するには、以下の項目があることを確認してください。

- Citrix License Serverバージョン11.15.0.0以降
- Citrix Cloudアカウント
- Citrix License Server から Citrix Cloud へのネットワークアクセス

接続要件

License Server を Citrix Cloud に正常に登録するには、次のアドレスに接続できることを確認してください。

- `https://las.cloud.com:443`
- `https://customers.citrixworkspacesapi.net:443`
- `https://citrix.cloud.com/` (コードを入力し、ライセンスサーバーのステータスを表示するための管理コンソールへのアクセス用)
- `https://trust.citrixnetworkapi.net` (コード取得用)
- `https://trust.citrixworkspacesapi.net/` (ライセンスサーバーが登録されていることの確認用)
- `https://cis.citrix.com` (データアップロード用)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Citrix Cloud に接続する

Citrix License Server の使用状況インサイトを有効にするには、次のタスクを実行します。

1. Licensing Manager コンソールを使用して、ライセンスサーバーの使用状況インサイトを有効にします。詳細については、ライセンス製品ドキュメントの「使用状況統計の共有」を参照してください。
2. この記事の「接続要件」に記載されている接続要件を確認し、アドレスにアクセスできることを確認します。Citrix License Server でプロキシサーバーを使用している場合は、ライセンス

製品ドキュメントの「ステップ 5 プロキシサーバーの構成」に記載されているとおりにプロキシサーバーが構成されていることを確認してください。

3. 「オンプレミス製品を Citrix Cloud に登録する」に記載されているとおりに、ライセンスサーバーを Citrix Cloud に登録します。

オンプレミス製品のライセンス使用状況を表示する

Citrix License Server の使用状況インサイトは、Citrix 環境全体のライセンス使用状況を可視化します。次のような使用状況レポートにアクセスできます。

- 展開および登録されているライセンスサーバーの数、およびそれらが Citrix Cloud に使用状況情報を報告しているかどうかを把握します。
- 仮想アプリとデスクトップの同時接続ライセンスとユーザー/デバイスライセンスの使用状況を可視化します。
- 複数の展開における同時接続ライセンスおよびユーザー/デバイスライセンスの集計使用状況に関するインサイトを得ます。
- 過去のライセンス使用状況と月ごとのライセンス使用状況の傾向を把握します。
- 特定のユーザーの最終ログイン時刻を表示します。
- Citrix License Server 全体で、インストールされているライセンス数と使用中のライセンス数を比較します。
- ライセンスの超過を監視します。
- 同時使用ライセンスとユーザー/デバイスライセンスの使用状況の内訳を表示します。

ライセンスサーバーのステータスを表示

ライセンスサーバーのステータスビューには、Citrix Cloudに利用状況を報告している各ライセンスサーバーが表示されます。

ライセンスコンソールのライセンスサーバータブ(/en-us/citrix-cloud/media/lic-usage-on-prem-lic-svr-tab-v2.png)

ライセンスサーバーは、過去3日間にCitrix Cloudに利用状況を正常にアップロードした場合、「Reporting」ステータスを表示します。過去30日間に利用状況を報告したが、過去3日間は報告していない場合、ライセンスサーバーは「Not Reporting」ステータスを表示します。過去30日間に利用状況を報告していないライセンスサーバーは、リストから削除されます。

ライセンスサーバーのステータスがライセンス利用状況ビューに与える影響

ライセンスサーバーのレポートステータスと最終報告日は、特定のライセンスサーバーからの利用状況が利用状況インサイトビューおよびレポートに含まれるかどうかを決定します。

- 現在インストールされ使用中のライセンスは、レポート中のライセンスサーバーからのデータのみに基づいています。ライセンスサーバーが「Not Reporting」と表示されている場合、そのライセンスサーバーからインストールされ使用中のライセンスは、利用状況インサイトエクスペリエンスに反映されません。
- 各ライセンスサーバーの最終報告日は、利用状況インサイトエクスペリエンスにおけるライセンス利用状況情報の最新性を決定します。表示されるライセンス利用状況レポートは、各ライセンスサーバーの最終報告時刻と同じくらい最新です。
- 利用状況インサイト用に構成され、Citrix Cloudに登録されているCitrixライセンスサーバーは、1日1回利用状況を更新します。必要に応じて、ライセンスサーバー上のCitrix License Manager管理コンソールから更新を強制できます。

ライセンス利用状況

タブには、Citrix展開全体でのライセンス利用状況の統合ビューが表示されます。各レポートライセンスサーバーからのライセンス情報は、単一のビューに統合されます。このビューにより、さまざまな展開とライセンスサーバーにわたる完全なライセンス状況を簡単に確認できます。

ライセンスコンソールのタブ(/en-us/citrix-cloud/media/lic-usage-on-prem-usage-tab-v3.png)

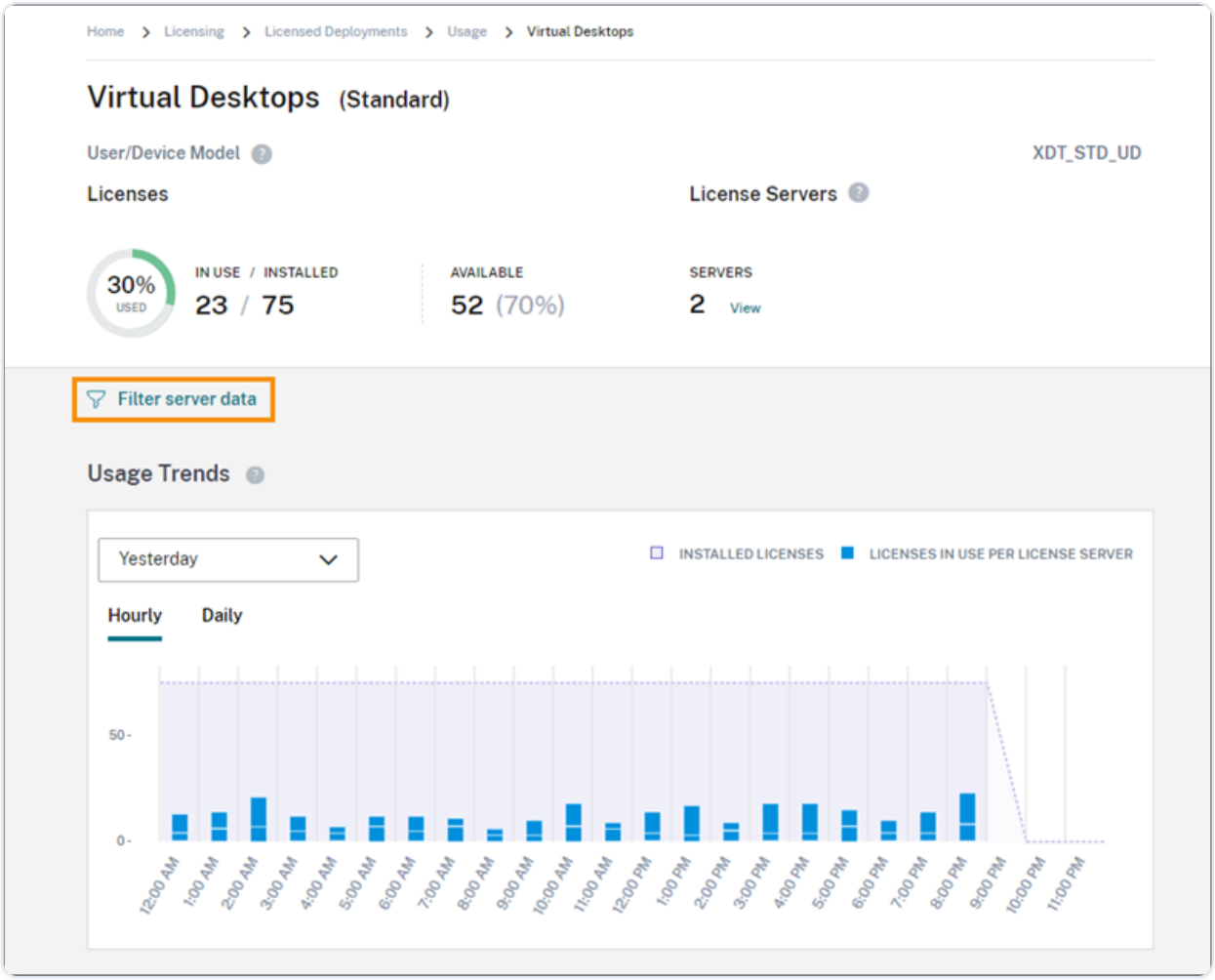
ライセンス利用状況は、製品エディションとライセンスモデルに基づいて、複数のライセンスサーバー間で整理および集計されます。すべてのレポートライセンスサーバーで見つかった一意のライセンスエディションごとに、ライセンス利用状況の概要カードが表示されます。検出された製品エディションごとに概要カードが表示されます。

ライセンスサーバーごとの利用状況

各ライセンスサーバーの製品ライセンス使用状況を表示するには、サーバーデータをフィルタリングできます。

1. **使用状況**ページで、管理する製品の**使用状況の詳細を表示**を選択します。

2. **サーバーデータをフィルタリング**をクリックし、使用状況を表示するライセンスサーバーを選択します。デフォルトでは、すべてのライセンスサーバーが選択されています。



3. **適用**を選択します。

フィルターを適用すると、Citrix Cloudは、選択したサーバーのみの使用状況の傾向、ライセンスサーバーの内訳、およびライセンスアクティビティを表示します。

同時ライセンスモデルのピークライセンス使用状況

同時ライセンスのレポート機能は、以下のデータポイントを中心に構成されています。

- インストール済みライセンス: 各ライセンスサーバーにインストールされているライセンスの数。
- ピーク使用中ライセンス: 特定の期間に使用されたライセンスの最大数。

ピーク使用中ライセンスを計算する際、Citrix Cloudは以下の期間に使用されたライセンスの最大数を取得します。

- 過去7日間: 過去7日間で一度に利用されたライセンスの最大数。
- 今月: 現在の暦月で一度に利用されたライセンスの最大数。

- 全期間: ライセンスサーバーがCitrix Cloudに登録されてから一度に利用されたライセンスの最大数。

重要:

これらの期間のデータは、ライセンスサーバーで使用中のライセンス数と一致しない場合があります。ライセンスサーバーは、特定の時点で使用中のライセンス数のみを報告します。Citrix Cloudはこれらの個々のデータポイントを受け取り、これらの期間のピークを計算します。

ライセンス使用状況の解釈に関する考慮事項

Citrixライセンスは多くの使用シナリオをサポートし、詳細な情報を含んでいます。使用状況を監視する際には、以下の考慮事項に留意してください。

- 使用状況情報は、レポート対象の各ライセンスサーバーにインストールされているライセンスに基づいています。ライセンスサーバーで利用可能なライセンスが不足している場合、追加のライセンスを割り当ててライセンスサーバーに配置することで、利用可能なライセンス数を増やすことができます。
- Citrix License Serverの使用状況インサイトビューで利用できる情報は、登録済みでアクティブにレポートしているCitrix License Serverによって収集および報告された情報のみを含みます。ライセンスされた展開の経験は、お客様が実際に所有または購入したライセンスの総数を表すものではなく、一致しない場合があります。
- 利用可能なライセンスの割合は、レポート対象のライセンスサーバーにインストールされているライセンスに対する使用中のライセンス数に基づいて計算されます。

ライセンスサーバー登録の削除

Citrix Cloudからライセンスサーバー登録を完全に削除するには、以下のタスクを実行します。

1. Citrix Licensing Managerコンソールを使用して、登録済みのライセンスサーバーをCitrix Cloudから削除します。詳細な手順については、「ライセンスサーバーの登録を削除する」を参照してください。
2. 以前に収集された使用状況データを削除します。
3. Citrix Cloudの製品登録ページにライセンスサーバーが表示されなくなったことを確認します。ライセンスサーバーがまだリストに表示されている場合は、「製品登録を削除する」の説明に従ってサーバーを削除します。

使用状況データの削除

登録済みのライセンスサーバーをCitrix Cloudから削除しても、以前に収集された使用状況データは引き続き保存されます。このデータを保持したくない場合は、削除できます。

> **重要:**
>
> 使用状況データの削除は永続的であり、元に戻すことはできません。使用状況データを削除しても、ライセンスサーバーの登録を削除しない場合、Citrix Cloudは引き続き使用状況データを収集します。

1. Citrix Cloudメニューから、**［ライセンス］**を選択します。
2. 「**ライセンスサーバー**」タブで、「**データの削除**」を選択します。
3. プロンプトが表示されたら、削除の影響を理解していることを確認するチェックボックスをオンにします。
4. 「**サーバーデータの削除**」を選択します。

Citrix Service Providers向けライセンス

Citrix Cloud™のLicense Usage Insightsサービスは、**Citrix Service Providers (CSP)** が製品ライセンスと使用状況を把握し、報告するのに役立つ無料のクラウドサービスです。CSPパートナーのみがLicense Usage Insightsにアクセスできます。

> **注:**
>
> Citrix DaaSは、以前はCitrix Virtual Apps and Desktopsサービスという名称でした。Citrix DaaS Standard for Azureは、以前はCitrix Virtual Apps and Desktops Standard for Azureという名称でした。一部の表示には以前の名称が含まれている場合があります。

> License Usage Insightsサービスを使用すると、次のことが可能になります。

- テレメトリから製品の使用状況情報を自動的に集計する
- シングルテナントおよびマルチテナントのお客様向けに、クラウドライセンスの使用状況と消費量を自動的に集計する
- 毎月、どのユーザーがVirtual Apps and Desktops展開にアクセスしているかを簡単に表示する

- ライセンス使用状況のお客様ごとの内訳を作成する
- Citrix®との過去のビジネスを表示して理解する
- Virtual Apps and DesktopsおよびCitrix DaaSのライセンス使用状況、NetScaler VPXの割り当てデータ、Citrix DaaS Standard for Azureのライセンスおよび消費データをCSVにエクスポートする

追加情報

要件とセットアップ手順については、License Usage Insightsの概要を参照してください。

シングルテナントおよびマルチテナントのお客様向けに集計された使用状況を表示するには、Citrix Service Providers向けクラウドサービスライセンスの使用状況とレポートを参照してください。

ライセンスコンソールを使用してサポートされているサービスの顧客の使用状況を表示するには、次の記事を参照してください。

- Citrix DaaS の顧客ライセンスと使用状況の監視(/ja-jp/citrix-cloud/license-usage-insights/virtual-apps-desktops-service-licensing-citrix-service-providers.html)

License Usage Insights の利用を開始する

サポートされているCitrix®製品

License Usage Insights サービスは、以下のCitrix製品の使用状況情報を提供します。

- Virtual Apps and Desktops (オンプレミス) 製品の使用状況
- Citrix DaaS™ Premium (旧称 バーチャル アプリ プレミアム および バーチャル アプリ アンド デスクトップ プレミアム サービス)
- Citrix DaaS Standard for Azure (旧称 シトリックス バーチャル アプリ アンド デスクトップ スタンダード フォー アジュール)
- NetScaler® Console VPX の割り当て

要件

Citrixオンプレミス製品のライセンスおよび使用状況情報を取得し、コンプライアンスを維持するには、Citrix License Server 11.17.2 build 51000以降が必要です。WindowsベースおよびVPXベースのライセンスサーバーのみがサポートされています。

Citrix License Server 11.17.2 build 51000以降には、Citrix Service Provider (CSP) パートナーにとって重要な主要機能が含まれています。

- 最適化された使用状況の収集: License Serverには、ライセンス動作と追跡を最適化し、CSPをより適切にサポートするための新機能が含まれています。
- コールホーム: License Serverには、CSPパートナー向けの製品使用状況の収集を自動化するコールホーム機能が含まれています。これらの機能はCSPパートナー専用であり、ライセンスサーバーでCSPライセンスが検出された場合にのみアクティブ化されます。
- License Activation Service (LAS) への移行、新しいイベントベースのテレメトリのサポート、および顧客サイト間のCSPオンプレミスライセンス配布の簡素化のためには、最小ライセンスサーバーバージョンは11.17.2 build 51000である必要があります。

ステップ1: Citrix License Server を更新する

バージョン11.17.2 build 51000より古いライセンスサーバーを実行している場合は、ライセンスサーバーをアップグレードする必要があります。インプレースアップグレードは簡単かつ迅速です。以下のタスクを完了してください。

1. 最新のライセンスサーバーをダウンロード。Citrix License Server の最新バージョンに関する詳細については、Citrix Licensing のドキュメントを参照してください。
2. 現在のライセンスサーバーをアップグレードします。
3. 各ライセンスサーバーでアップグレードプロセスを繰り返します。

ステップ2：My Citrixの資格情報を使用してCitrix Cloud™にサインインする

サインインする前に、CSPパートナークラウドアカウントをまだお持ちでない場合は、Citrix Cloudアカウントにサインアップする必要があります。(/ja-jp/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html)で説明されている手順に従ってください。

アカウントを作成する際は、citrix.comからCitrixライセンスを割り当ててダウンロードする際に使用するのと同じMy Citrixの資格情報を使用してください。Citrix Cloudは、My Citrixの資格情報に関連付けられたアドレスにメールを送信し、アカウントを確認します。

Citrix Cloudアカウントの準備が整ったら、メールアドレスとパスワードを使用して、https://citrix.cloud.comにサインインしてください。

ステップ3（オプション）：ライセンスサーバーを介してユーザー名を匿名化する

デフォルトでは、Virtual Apps and DesktopsまたはCitrix DaaSのライセンスチェックアウトに関連付けられたユーザー名は、Citrixに安全に送信されます。

ユーザー名がCitrixに送信されるのは、CSPパートナーがLicense Usage Insightsの機能とCSPライセンスプログラムを最大限に活用できるようにするためです。

ユーザー情報は単一のuser@domainエントリに限定されており、追加の個人識別可能データはCitrixに送信されません。Citrixはこの情報を共有しません。

ユーザー名情報のアップロードに懸念があるパートナーは、ユーザー名の匿名化を有効にできます。有効にすると、ユーザー名の匿名化は、アップロード前に読み取り可能なユーザー名を、安全で不可逆的なアルゴリズムを使用して一意の文字列に変換します。

License Usage Insightsは、実際のユーザー名の代わりにこれらの固有の識別子を使用して製品の使用状況を追跡します。このアプローチにより、サービスプロバイダーは、クラウドサービスのユーザーインターフェイスで実際のユーザー名を確認することなく、月ごとのインサイトを活用できます。

ユーザー名の匿名化を構成するには

1. ライセンスサーバーで、構成ファイルをテキストエディターで開きます。通常、構成ファイルはC:\Program Files\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xmlにあります。
2. 「**構成**」セクションで、**UsageBasedBillingScramble**設定を次のように追加します。

```
<?xml version="1.0" encoding="utf-8"?>

<Configurations>

<EncoreConfiguration>

<SamplingPeriod>15</SamplingPeriod>

<RetentionTime>180</RetentionTime>

<Enabled>true</Enabled>

</EncoreConfiguration>

<SARenewalConfigOptions>Notify</SARenewalConfigOptions>

<UsageBasedBillingScramble>1</UsageBasedBillingScramble>

</Configurations>
```

3. ファイルを保存します。

ステップ4：License Usage Insightsサービスを使用する

Citrix Cloudコンソールから、ワッフルメニューでLicense Usage Insightsサービスタイルを見つけてクリックします。サービスの主要機能の概要については、「製品の使用状況、ライセンスサーバー、および通知の管理」を参照してください。

その他の詳細

Citrix License ServerをLicense Usage Insightsと併用する場合は、次の項目を考慮してください。

- 新しく更新されたライセンスサーバーまたはサイトがLicense Usage Insights管理コンソールに表示されるまでに、最大24時間かかる場合があります。
- 使用状況データがライセンスサーバーからアップロードされると、License Usage Insightsが後日アクセスできるように、安全な方法で処理および保存されます。このプロセスが完了するまでに最大24時間かかる場合があります。
- デフォルトでは、Virtual Apps and DesktopsまたはCitrix DaaSのライセンスチェックアウトに関連付けられたユーザー名は、Citrixに安全に電話で報告されます。
- ユーザー名が電話で報告されるのは、CSPパートナーがLicense Usage Insightsの機能と、試用、テスト、および管理目的の製品使用における無料ユーザーをサポートするCSPライセンスプログラムを最大限に活用できるようにするためです。
- ユーザー情報は単一のuser@domainエントリに限定され、追加の個人識別可能データは電話で報告されません。Citrixがこの情報を共有することはありません。

ヘルプとサポート

License Usage Insightsに関する支援が必要な場合は、My Supportポータルでサポートチケットを開いてください。Citrix CloudからMy Supportにアクセスするには：

1. Citrix Cloudにサインインします。
2. 画面の右上にある「**ヘルプ**」アイコンをクリックします。
3. 「**チケットを開く**」を選択します。
4. 「**マイサポートに移動**」を選択し、My Citrixの資格情報でサインインします。
5. フォームに記入して送信します。

Citrixテクニカルサポートの担当者がお客様に連絡を取り、サポートします。

よくある質問

- 「**どのような情報がコールホームされていますか？ライセンスサーバーがCitrixに送信している情報を表示できますか？**」はい、Citrixにコールホームされている情報のコピーを表示でき

ます。詳細については、「アップロードに含まれるライセンスサーバー情報」を参照してください。

- **「License Usage Insightsは、Citrix Service ProviderではないCitrixのお客様またはパートナーも利用できますか？」**いいえ。License Usage Insightsは、有効なメンバーシップ契約を結んでいるCitrix Service Provider™パートナーのみが利用できます。
- **「ライセンスサーバーでコールホームを無効にできますか？」**いいえ。Citrix Service Providerライセンス契約に基づき、すべてのライセンスサーバーは製品の使用状況をコールホームする必要があります。コールホームのユースケースに懸念があるパートナーは、ユーザー名の匿名化機能を使用できます。詳細については、「ライセンスサーバーを介したユーザー名の匿名化」を参照してください。
- **「License Usage Insightsに表示される製品使用量に基づいて請求されますか？」**いいえ。License Usage Insightsは、パートナーが製品の使用状況を把握し、顧客を正確に監査および請求し、必要に応じて注文を拡大するのに役立ちます。

製品の使用状況、ライセンスサーバー、および通知を管理する

License Usage Insights を使用して、Citrix Cloud 展開の製品使用状況を監視し、ライセンスサーバーのステータスを追跡し、顧客通知を管理します。

> **注:**
>
> 復元されたユーザー情報（ユーザー名やドメインなど）を表示し、サイト名とデリバリーグループ名を正しく解決するには、Citrix Virtual Apps and Desktops™ Delivery Controller を以下のいずれかの最小サポートバージョンにアップグレードしてください。
>
> - **現在のリリース:** 2411以降
> - **LTSR:** 2203 CU7、2402 CU3、または 2507
>
> 以前のバージョンでは、デフォルトのデータスクランブルにより、フィールド値の代わりにGUIDが表示されます。

製品の選択

別の製品のライセンス詳細を表示するには、製品名の横にある矢印をクリックし、表示したい製品またはサービスを選択します。

License Usage Insights コンソールでサービスが選択された製品タブの画像(/en-us/citrix-cloud/media/lui-product-picker.png)

顧客通知

各展開を個別に訪問することなく、複数の顧客にわたるソリューションの健全性を監視します。Citrix Cloud の通知領域は、ダッシュボード上の顧客全体の通知を集約するため、アラートが対処され、サービスが稼働し続けることを確認できます。

マイカスタマー通知領域が強調表示されたCitrix Cloud通知アイコンの画像(/en-us/citrix-cloud/media/csp-notifications.png)

1. Citrix Cloud 管理コンソールから、**通知**アイコンをクリックし、**マイカスタマー**をクリックします。最新の通知のリストが表示されます。
2. 顧客通知の完全なリストを表示するには、**すべての通知を表示**をクリックします。

ライセンスサーバーのステータス

Citrix Service Provider™ のライセンスガイドラインに準拠するため、すべてのアクティブなライセンスサーバーは更新され、レポートを送信している必要があります。ライセンスサーバーのステータスには、所有しているライセンスサーバーと、License Usage Insights で使用するために更新されているかどうかが表示されます。

このサービスは、Citrix® バックオフィスに保存されている従来のライセンス割り当てデータを使用して、アクティブなライセンスサーバーのリストを表示します。ライセンスサーバーが更新され、正常にレポートを送信している場合、License Usage Insights は「レポート中」のステータスを表示し、最新のアップロードのタイムスタンプを含めます。

License Usage Insights コンソールで タブが選択された製品ページ(/en-us/citrix-cloud/media/lui-console.png)

アップロードに含まれるライセンスサーバー情報

ライセンスサーバーで Call Home がアクティブ化されている場合、以下の情報が毎日アップロードされます。

- ライセンスサーバーのバージョン
- ライセンスファイル情報:
  - サーバーにインストールされているライセンスファイル
  - ライセンスファイルの有効期限
  - 製品の機能とエディションの資格情報

    - ライセンス数

- ライセンスの使用状況:

    - 現在の暦月に使用されたライセンス
    - ライセンスチェックアウトに関連付けられているユーザー名
    - アクティブ化された製品機能とエディション

ライセンスサーバーのアップロードを表示する

CSPパートナーは、ライセンスサーバーがCitrixに送信するすべての詳細を完全に理解するために、ライセンスサーバー上の最後にアップロードされたペイロードを検査できます。このペイロードのコピーは、ライセンスサーバーに.zipファイルとして保存されます。デフォルトでは、この場所はC:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zipです。

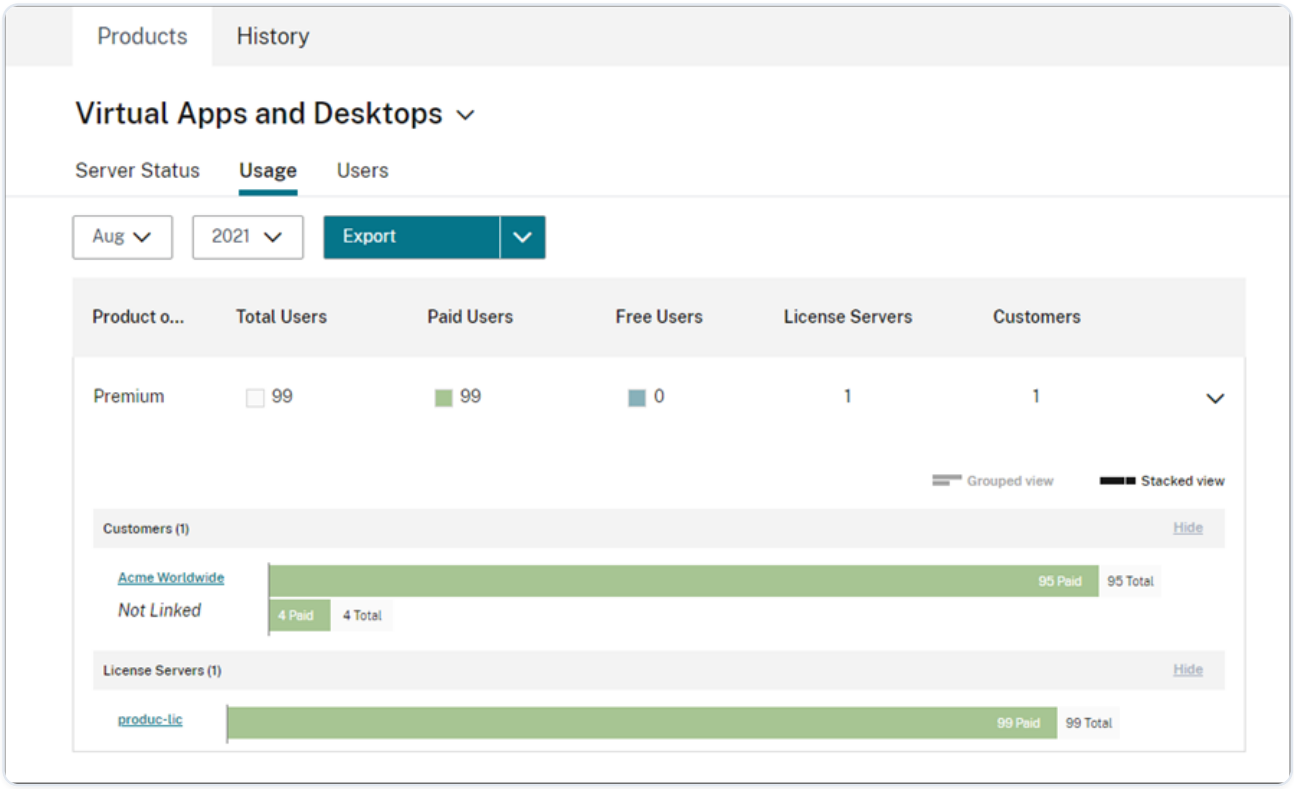
> **注：**
>
> 正常にアップロードされたファイルは、最後の1つを除いて削除されます。アップロードに失敗したファイルは、正常なアップロードが行われるまでディスクに残ります。正常なアップロードが行われると、最後の1つを除くすべてのアップロードが削除されます。

使用状況の収集

使用状況の収集は、自動化されたデータ収集と集計を通じて製品の使用状況を理解するのに役立ちます。追加のツールを導入する必要はありません。

License Usage Insightsは、すべてのCitrixライセンスサーバー（従来のライセンスサーバーコールホームの場合）およびサイト（License Activation Serviceの場合）にわたる製品の使用状況を自動的に集計し、すべての展開における使用状況の全体像を提供します。また、特定のユーザーを所属する顧客またはテナントに関連付けることで、ライセンス使用状況の内訳を作成することもできます。

ライセンスサーバーは、製品ライセンスの使用状況を収集および追跡し、セキュアな電話ホームチャネルを使用してCitrixに報告します。この自動化されたアプローチにより、更新された使用状況データが常に提供され、時間が節約され、パートナーが展開内の使用状況の傾向をよりよく理解するのに役立ちます。



Virtual Apps and Desktops製品使用状況の顧客別内訳のためのユーザー割り当て（タグ付け）

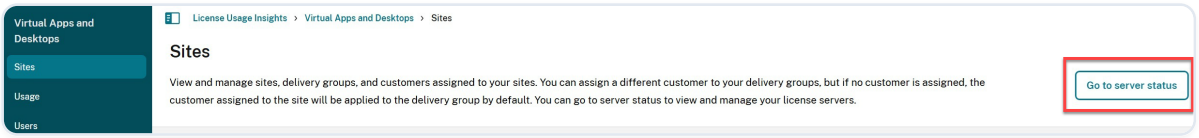
この機能は、各顧客のライセンス使用状況データの内訳を提供し、シングルテナントおよびマルチテナントサイト（LAS統合）またはライセンスサーバー（従来のコールホーム）アーキテクチャの両方での管理とレポート作成をサポートします。License Usage Insightsのオブジェクトは次のとおりです。

- **ライセンスサーバー**：リスト上の「レポート中」または「レポートなし」のライセンスサーバー。
- **サイト**：顧客専用、または複数のテナント顧客と共有されるVirtual Apps and Desktopsサイト。
- **デリバリーグループ**：通常、顧客専用のVirtual Apps and Desktopsデリバリーグループ。
- **ユーザー**: コールホーム使用状況データで見つかった単一のユーザー名。
- **NetScaler**: 単一のNetScaler VPX™ライセンス割り当て（VPXリスト上のVPX）。

> **注:**
>
> CSPは、前月と当月の顧客タグ付けを翌月の10日まで更新できます。

> 顧客ごとにライセンス使用状況を分類するには、まずユーザーを所属する顧客またはテナントに関連付ける必要があります。顧客ダッシュボードに顧客が定義されていない場合は、新しい顧客を追加するか、既存のCitrix Cloud顧客と接続できます。

1. 該当する場合は、顧客を顧客ダッシュボードに追加します。Citrix Cloud管理コンソールのワッフルメニューから、**My Customers**をクリックし、**Add or Invite**をクリックして、画面の指示に従います。
2. ワッフルメニューをクリックし、**License Usage Insights**タイルを選択します。
3. **Virtual Apps and Desktops**製品が選択されている場合、デフォルトでLicense Activation Service (LAS) を介してアクティブ化された**サイト**がロードされます。
4. LAS統合サイトからユーザーの割り当てを続行するには:
   a. **ユーザー**をクリックします。
   b. 関連付けたいユーザーを選択し、**一括操作 > 顧客に割り当て**をクリックします。
5. 従来のライセンスサーバーコールホームからユーザーを割り当てるには:
   a. **サーバーのステータスに移動**ボタンをクリックします。



   b. ライセンス**サーバーのステータス**ページがロードされたら（このページから**サイトに移動**をクリックしてLAS統合サイトに戻ることもできます）、メニューオプションから**すべてのユーザー**を選択します。
   c. ユーザーをフィルターして検索し、リンクされていないユーザーを選択してから、**一括操作 > 顧客へのリンクを管理**をクリックします。
6. 顧客リストから、ユーザーを関連付けたい顧客を選択します。
7. **割り当て**または**保存**をクリックします。
8. 顧客ごとの内訳を表示するには、**使用状況**ビューをクリックします。

ユーザー顧客タグ付け

この機能は、シングルテナントおよびマルチテナントのライセンスサーバーアーキテクチャの両方での管理とレポート作成のサポートを含め、顧客ごとのライセンス使用状況データの詳細を提供します。License Usage Insightsの要素は次のとおりです。

- ライセンスサーバー - リスト上の「レポート中」または「レポートなし」のライセンスサーバー。

- ユーザー - コールホーム使用状況データで見つかった単一のユーザー名。
- NetScaler® - 単一のNetScaler VPXライセンス割り当て（VPXリスト上のVPX）。

> **注：**
>
> ユーザー顧客タグ付け機能は、無料ユーザータグ付けと同じ動作をします。CSPは、現在の請求サイクルの顧客タグ付けを翌月の10日まで更新できます。

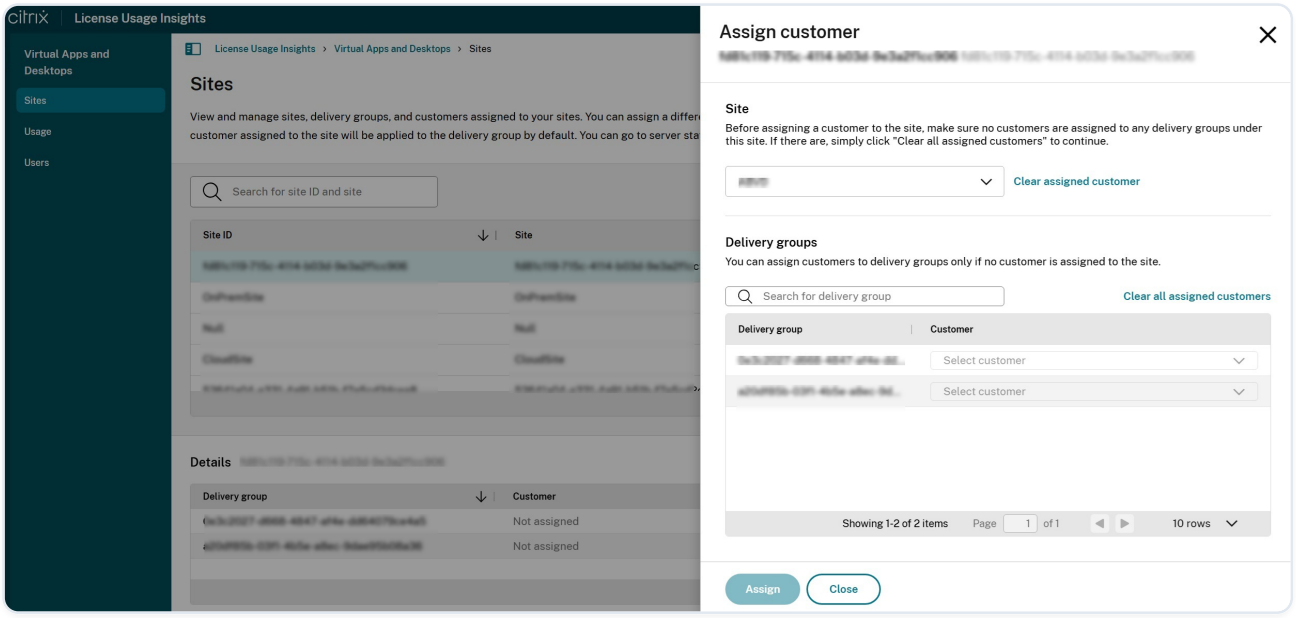
サーバー顧客タグ付け

この機能により、従来のコールホームに使用されるライセンスサーバーを特定の顧客にタグ付けまたは割り当てることができます。サーバー顧客タグ付けを利用することで、そのサーバーからのすべてのユーザーが自動的にタグ付けされた顧客に関連付けられ、管理者は異なる顧客に関連付けられたリソースを簡単に識別および追跡できるようになり、顧客への請求、レポート作成、およびより効率的なリソース割り当てが容易になります。

サイトおよびデリバリーグループ顧客タグ付け

サイト顧客タグ付け機能は、特定の顧客専用のVirtual Apps and Desktopsサイト（シングルテナントサイトとも呼ばれます）に適用され、LAS統合サイトを顧客にタグ付けして割り当てることができます。割り当てられると、そのサイトからのすべてのユーザーは、使用状況レポートの顧客内訳で自動的にタグ付けされた顧客に関連付けられます。

デリバリーグループの顧客タグ付け機能は、複数の顧客で共有されるVirtual Apps and Desktopsサイト（別名マルチテナントサイト）に適用されます。これにより、LAS統合サイトのデリバリーグループを関連する顧客にタグ付けできます。一度割り当てられると、そのデリバリーグループのユーザーは、使用状況レポートの顧客内訳でタグ付けされた顧客に自動的に関連付けられます。



サイトは、単一の顧客に排他的に割り当てられる（サイトタグ付け）か、またはデリバリーグループタグ付けを介して複数の顧客に割り当てられるかのいずれかであり、両方を同時に行うことはできません。

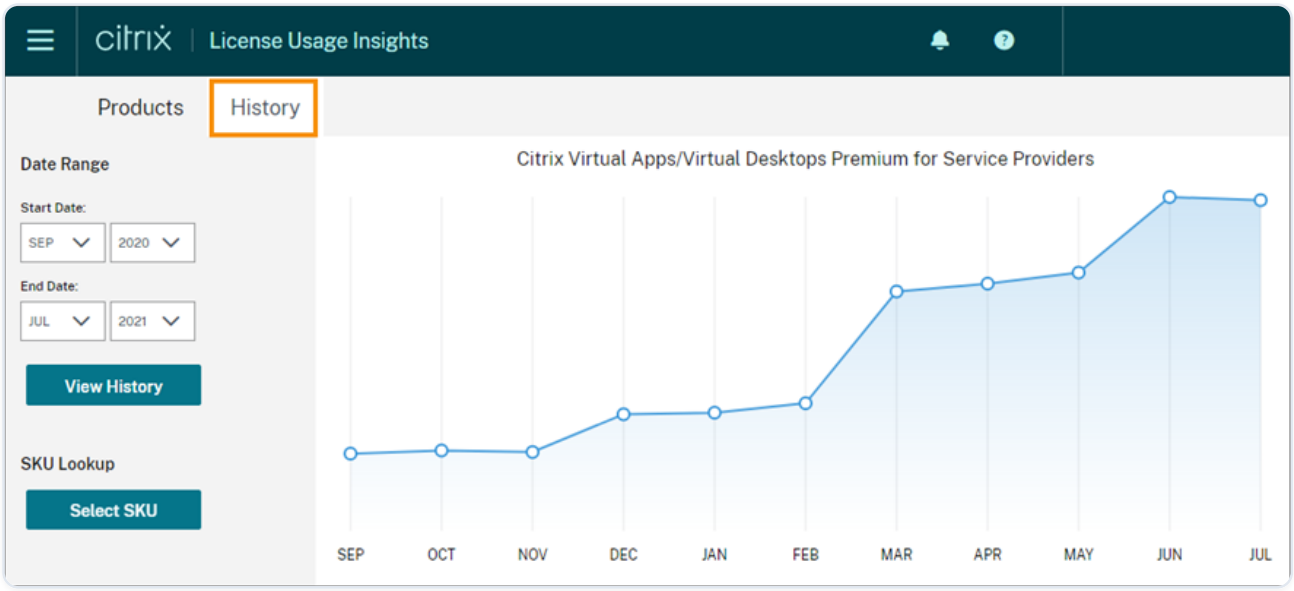
サイトまたはデリバリーグループのタグ付けにアクセスするには、ワッフルメニューからLicense Usage Insightsを選択し、**サイト**ページで、サイトテーブルからサイトを選択し、**顧客の割り当て**をクリックします。同じページは、デリバリーグループテーブルでデリバリーグループを選択することで、デリバリーグループのタグ付けにも使用できます。サイトがすでに顧客に排他的に割り当てられている場合、そのサイトのデリバリーグループは表示専用となり、サイトの顧客割り当てを解除するまで個別に顧客に割り当てることはできません。

サイトおよびデリバリーグループベースの顧客タグ付けは現在テクニカルプレビュー中です。プレビューへの参加をリクエストするには、こちらのフォームを使用できます。

履歴トレンド

従来のライセンスサーバーコールホームに基づいた、Citrixとの過去のビジネスの完全な履歴記録を表示できます。先月、昨年、または設定可能な期間に報告した使用状況を確認できます。

履歴ビューは貴重なビジネスインサイトを提供します。Citrixサービスプロバイダーとして、Citrixとのビジネスがどのように推移しているか、どの製品が顧客やエンドユーザー全体で最も成長しているかをすばやく把握できます。 サーバーのステータスページから、製品履歴の表示アイコンとリンクをクリックします。



使用状況と割り当てデータのエクスポート

License Usage Insightsから、次の種類のデータをCSVファイルとしてエクスポートできます。

- 指定された月のVirtual Apps and Desktops製品の使用状況とユーザーリスト
- 現在のNetScaler VPX割り当ての詳細

1. 製品リストから**Virtual Apps and Desktops**または**Networking**を選択します。
2. 該当する場合は、エクスポートするビューを選択します。たとえば、Virtual Apps and Desktopsの使用状況の詳細をエクスポートするには、**使用状況**ビューをクリックします。
3. 該当する場合は、エクスポートする月と年を選択します。
4. 画面の右側にある **Export** をクリックします。

API を使用してライセンスデータにアクセスする

Citrix は、Citrix Cloud の外部からライセンスデータにアクセスするために使用できるいくつかの API を提供しています。これらの API の詳細については、Citrix Developer ドキュメントの APIs to manage Citrix cloud licensing を参照してください。

これらの API を使用するには、まずサービスプリンシパルを作成し、ベアラートークンを生成する必要があります。サービスプリンシパルの作成については、Get started with Citrix Cloud APIs を参照してください。

API へのディストリビューターアクセス

Citrix ディストリビューターまたは認定されたサードパーティが、Citrix Cloud アカウントへの完全な管理者アクセス権を付与することなく、Citrix Cloud API を介してライセンスデータにアクセ

スできるようにすることができます。これは、ディストリビューターが使用状況レポートを検証し、正確な請求を保証できるようにするためです。

ディストリビューターにライセンスデータへのアクセスを提供するには、必要なカスタムアクセス権限を持つサービスプリンシパルを作成できます。サービスプリンシパルの作成については、Get started with Citrix Cloud APIs を参照してください。

このユースケースでは、**Custom** アクセスを選択し、次に **License Usage Insights** > **License Usage Insights: Distributor Access** を選択します。

ディストリビューターが利用できるライセンスデータ

このセクションでは、お客様が提供するサービスプリンシパルの詳細を使用して、Citrix ディストリビューターがアクセスできるライセンスデータと API について説明します。各 API の詳細については、以下のリンクを使用してください。

月次および履歴の Virtual Apps and Desktops ライセンス使用状況の CSP レポート (License Usage Insights):

- Virtual Apps and Desktops の現在の使用状況
- Virtual Apps and Desktops の過去の使用状況

シングルテナントおよびマルチテナントのクラウドライセンス使用状況の CSP レポート (License Usage Insights):

- DaaS 現在の使用状況
- DaaS 過去の使用状況

CSP のクラウドライセンス使用状況 (ライセンス):

- DaaS 現在の使用状況
- DaaS 過去の使用状況

テナントのクラウドライセンス使用状況 (顧客ダッシュボード -> ライセンスの表示)

- DaaS CCU 現在の使用状況
- DaaS CCU 過去の使用状況
- DaaS UD 現在の使用状況
- DaaS UD 過去の使用状況

Citrix Service Providers向けのクラウドサービスライセンスの使用状況とレポート

License Usage Insights は、クラウドサービスの使用状況を自動的に集計し、すべてのシングルテナントおよびマルチテナントのお客様にわたる完全なビューを提供します。また、特定の月のこれらの詳細をCSVファイルにエクスポートして、さらに分析することもできます。

Citrix DaaS の集約されたテナントビュー(/en-us/citrix-cloud/media/lui-cvad-single-multi-view.png)

サポートされているサービス

CSP DaaS のライセンス使用状況は、Citrix DaaS™ Premium（旧称 Virtual Apps and Desktops Premium service）のマルチテナントおよびシングルテナントのエンタイトルメントで利用できます。

> **注:**
>
> 同じクラウドアカウント内でCSP DaaSエンタイトルメントと他の非CSP DaaSエンタイトルメントを混在させることはサポートされていません。 シングルテナントのCSP DaaSエンタイトルメントは、同じCitrix Cloud™コントロールプレーン上のCSPアカウントにリンクされているテナント顧客アカウントにのみ提供できます。

ライセンスの概要

License Usage Insights は、Citrix Service Providers（CSP）向けのシングルテナントおよびマルチテナントの使用状況について、以下の内訳を提供します。

- テナントタイプ別にグループ化されたパートナーレベルの概要で、すべてのお客様にわたる顧客の総数、購入済みライセンスの総数、ユーザー数、および超過（過剰使用）ライセンスが含まれます。
- 各シングルテナント顧客の使用状況の概要で、使用中の総ライセンスの割合、購入済みライセンスの総数、ユーザー数、および過剰使用ライセンスの数が含まれます。

マルチテナントサービスの場合、使用状況の概要を展開して、顧客の内訳、アカウントID、および各テナント顧客に関連付けられている総ユーザー数を表示できます。

マルチテナントパートナー顧客の概要ビュー(/en-us/citrix-cloud/media/lui-cvad-multitenant-usage-detail.png)

リンクされていないテナント顧客

テナント顧客の一部のユーザーが、テナント自身のストアURLではなく、パートナーの共有ストアURLを介してセッションを起動していた場合、これらのユーザーは「リンクされていません」と表示されることがあります。

「リンクされていない」状態が強調表示されたマルチテナント顧客(/en-us/citrix-cloud/media/lui-multitenant-not-linked.png)

リンクされていないユーザーが、パートナーのストアURLにアクセスするユーザーを引き続き許可しながら、正確な請求とレポートのために適切なテナント顧客に適切に関連付けられるようにするため、サービスプロバイダー（パートナー）管理者は以下の2つの方法を利用してユーザーをリンクできます。

デリバリーグループベースの自動ユーザー割り当て（タグ付け）

License Usage Insights (LUI) サービスは、ユーザーがスコープ指定されたデリバリーグループからセッションを起動する際に、マルチテナントDaaSユーザーをテナント顧客に自動的にリンクできるようになりました。ただし、これらのデリバリーグループにはそれぞれ特定のテナントスコープが割り当てられている必要があります。スコープ指定されていない、または共有されているデリバリーグループからセッションを起動するユーザーはリンクできません。マルチテナントDaaSデリバリーグループの全体的なテナントスコープの割り当て（または未割り当て）は、**License Usage Insights > DaaS > Accounts** から確認できます。

デリバリーグループのスコープを割り当てるか更新するには、マルチテナントDaaSのStudioコンソールに移動する必要があります。

アカウントデリバリーグループ(/en-us/citrix-cloud/media/accounts-delivery-group.png)

テナント顧客へのユーザー割り当て（タグ付け）

テナントはマルチテナント環境で専用のデリバリーグループを持つべきですが、デリバリーグループが共有されている場合や、一部のCSP管理者が異なるスコープを持つ複数のデリバリーグループに属しているような特殊なユースケースでは、ユーザーをテナント顧客に割り当てたり、割り当てを解除したりするために手動のユーザータグ付けが必要です。

ワッフルメニュー > **License Usage Insights > DaaS > Users** から移動します。

- 個々のユーザーを割り当てるには、ユーザー行の末尾にある「…」をクリックし、**Assign to customer** を選択して、テナント顧客を選択します。

  テナント顧客(/en-us/citrix-cloud/media/assign-to-tenant-customer.png)

- 複数のユーザーを一括で割り当てるには、関連する条件でユーザーを検索し、ユーザー行のチェックボックスをオンにして、**Bulk actions** の下にある **Assign to customer** をクリックし、テナント顧客を選択して、**Assign** をクリックします。

  顧客名を入力(/en-us/citrix-cloud/media/assign-to-customer-enter-name.png)

- 同様のプロセスを使用して、顧客の割り当てを解除することもできます。

月間使用状況の表示とエクスポート

いつでも、すべての顧客の過去の月のライセンス使用状況を表示できます。このデータをCSVファイルにエクスポートして、さらに分析することもできます。

1. 製品メニューから、表示したい製品を選択します。

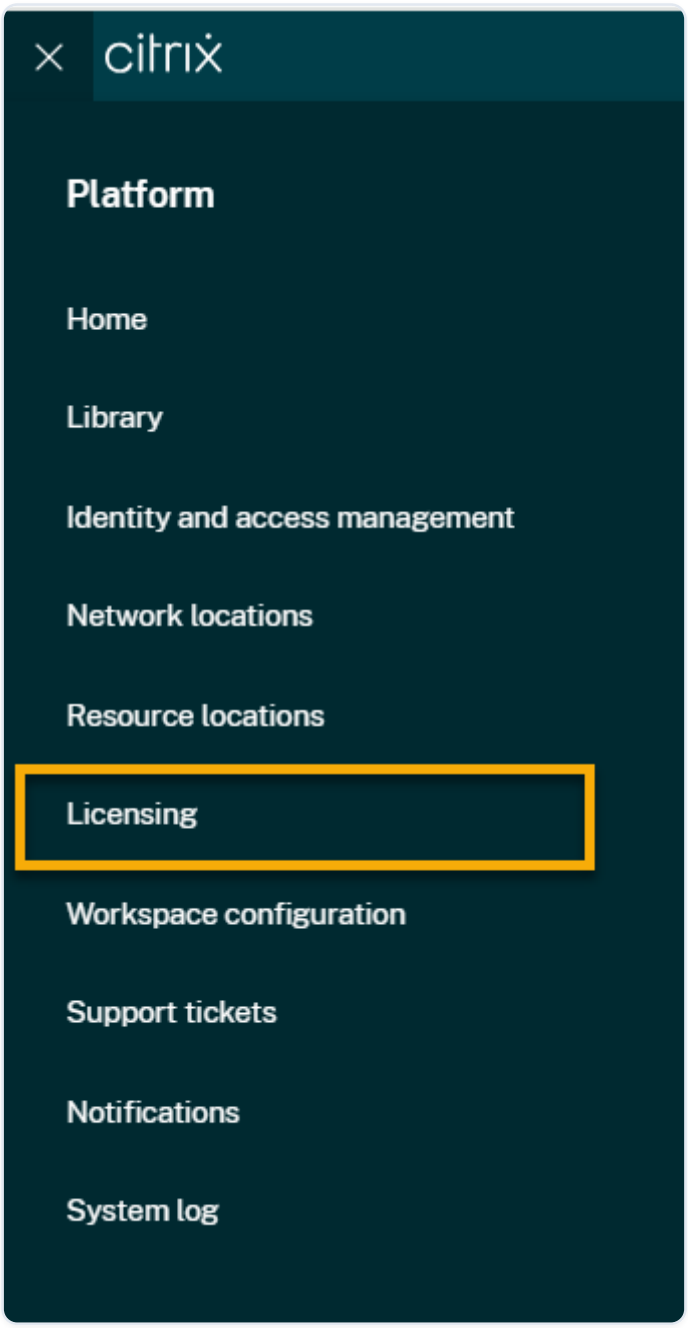
Citrix DaaS の場合、表示したい月と年を選択し、**エクスポート**を選択します。

Citrix DaaS の日付ピッカーと強調表示されたエクスポートリンク(/en-us/citrix-cloud/media/lui-cvad-svc-license-export.png)

Citrix DaaS™ の顧客ライセンスと使用状況の監視

Citrix Service Provider (CSP) のお客様は、Citrix Cloud でユーザーの Citrix DaaS ライセンスを簡単に監視できます。CSP として、Citrix Cloud でお客様のアカウントにサインインすることで、これらの詳細にアクセスできます。シングルテナントおよびマルチテナントのお客様全体の集計されたライセンス使用状況情報を表示するには、「Citrix Service Provider 向けクラウドサービスライセンスの使用状況とレポート」を参照してください。

お客様は、Citrix Cloud™ メニューから を選択して、ライセンスデータを確認できます。



ライセンスの割り当て

ユーザー/デバイスライセンスモデル: Citrix Cloud は、固有の顧客ユーザーが当月中に初めてアプリまたはデスクトップを起動したときにライセンスを割り当てます。

同時実行ユーザーライセンスモデル:

同時実行ライセンスモデルの詳細については、ライセンス製品ドキュメントの「同時実行ライセンス」を参照してください。

ライセンスの概要

Citrix Cloud は、ユーザー/デバイスおよび同時実行ユーザーライセンスモデルで使用中のライセンスの概要ビューを表示します。CSP が管理するシングルテナントのお客様の場合、同じ顧客アカウントで CSP ライセンスと非 CSP ライセンス（**同時実行**か**ユーザー/デバイス**かに関わらず）を混在させることはサポートされていません。

ユーザーとデバイスの概要

ユーザー/デバイスモデルの場合、ライセンスの概要は、所有しているライセンスの総数に対して使用中のライセンスを一目で確認できるビューを提供します。

割合が100%に近づくと、緑から黄色に変わります。割合が100%を超えると、赤に変わります。

Citrix Cloud は、割り当てられたライセンスと購入済みライセンスの比率、および残りの利用可能なライセンス数も表示します。

使用中のピークライセンスの計算

同時ライセンスモデルを正確に反映するため、Citrix Cloudは5分ごとにサービスに同時にアクセスしている一意のデバイスの数をカウントします。カウントが現在表示されているピーク使用量よりも大きい場合、Citrix Cloudは新しいピーク使用量とそれが達成された日時を表示します。カウントが現在のピーク使用量よりも少ない場合、現在のピーク使用量は変更されません。

> **重要:**
>
> DirectorのMonitorを使用して同時セッションに関する情報を取得する場合、Monitorレポートは同時セッションの異なる解釈を提供し、使用中の同時ユーザーライセンスの数を正確に反映しないことに注意してください。Monitorレポートとライセンスレポートの違いの詳細については、FAQを参照してください。

月間アクティブ使用量の計算

毎月初めに、Citrix Cloudは前月のスナップショットを取得します。Citrix Cloudは、その暦月中に発生した一意の接続の総数を表示します。

日間アクティブ使用量の計算

毎日同じ時刻に、Citrix Cloudは過去24時間のスナップショットを取得します。Citrix Cloudは、その24時間期間中に発生した一意の接続の総数を表示します。

使用状況の傾向

Citrix Cloudは、ユーザー/デバイスライセンスまたは同時ユーザーライセンスのいずれかの使用状況の傾向の内訳を表示します。この内訳を表示するには、ライセンス概要ページから**View Usage Details**を選択します。

ユーザーとデバイスの傾向

ユーザー/デバイスライセンスの場合、**Usage Trends**セクションには、割り当てられたライセンスの内訳がグラフとして表示されます。

グラフ上の間隔をポイントすると、次の情報が表示されます。

- **合計ライセンス数:** すべてのエンタイトルメントにおけるクラウドサービスのために購入したライセンスの総数。
- **以前に割り当て済み:** 前月に割り当てられたライセンスの数。たとえば、ユーザーが7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられたとします。このライセンスは7月には「新規割り当て済み」としてカウントされます。8月には、このライセンスは「以前に割り当て済み」としてカウントされます。
- **新規割り当て済み:** 各月に割り当てられた新しいライセンスの数。たとえば、ユーザーが7月に初めてクラウドサービスにアクセスし、ライセンスが割り当てられたとします。このライセンスは7月には「新規割り当て済み」としてカウントされます。

ライセンスユーザー

ライセンスアクティビティセクションには、今月中にライセンスが割り当てられた個々の顧客ユーザーのリストが表示されます。このリストには、各ユーザーが属するドメイン、ライセンスが割り当てられた日付、およびサービスが最後に使用された日時も表示されます。

ライセンスの月次リリース

毎月1日に、前月割り当てられたCSPライセンスは自動的にリリースされます。これにより、割り当てられたライセンスの数はゼロにリセットされ、ライセンスを持つ顧客ユーザーのリストはクリアされます。ライセンスは、ユーザーが新しい月に初めてアプリまたはデスクトップを起動したときに再割り当てされます。

月次ライセンス履歴の確認

毎月1日に、**ライセンスアクティビティ**の下にある前月のCSPのライセンスを持つ顧客ユーザーのリストは、割り当てられたライセンスの数がゼロにリセットされるとクリアされます。ただし、必要に応じて、いつでも過去の月のユーザー詳細にアクセスし、CSVファイルとしてダウンロードできます。

1. **ライセンスアクティビティ**セクションで、セクションの右端にある**ライセンス履歴の表示**を選択します。
2. 表示したい月を選択します。選択した月のユーザー詳細のリストが表示されます。
3. リストをエクスポートするには、セクションの右端にある**CSVにエクスポート**を選択し、ファイルを保存します。

ライセンス詳細のエクスポート

顧客はいつでも、ライセンスを持つユーザーの詳細をCSVファイルにエクスポートして、さらに分析できます。顧客は必要に応じてCSVファイルを使用してライセンスの詳細を分析できます。

今月の詳細をエクスポートするには、**ライセンスアクティビティ**セクションで、セクションの右端にある**CSVにエクスポート**を選択し、ファイルを保存します。

過去の月の詳細をエクスポートするには、月次ライセンス履歴の確認で説明されているように、選択した月のリストを生成します。**CSVにエクスポート**を選択し、ファイルを保存します。

Citrix Platform Flex のライセンス

Citrix Platform Flex は、セキュアで回復力があり、柔軟なデジタルワークスペースとプラットフォームサービスをクラウド全体で提供するために設計された、マネージド型のクラウド提供プラットフォームです。

Citrix Platform Flex は、お客様を厳格なインフラストラクチャ中心の展開モデルから、ペルソナベースの運用モデルへと移行させます。お客様は、インフラストラクチャを手動でサイジングおよび管理する代わりに、作業の実行方法に基づいてスケーリングする Citrix サービスを利用します。

Citrix Platform Flex は、その核となる部分で以下をサポートするように構築されています。

- 従業員の変動性（従業員、契約社員、パートナー、一時的なユーザー）
- Citrix が管理するインフラストラクチャによる運用上のシンプルさ
- 実際の使用状況に合わせた予測可能で柔軟な消費
- 地域全体にわたるエンタープライズグレードの回復力とセキュリティ

Citrix Platform Flex は、Citrix Cloud 上に構築されたマルチサービスプラットフォームとして設計されています。このプラットフォームを通じて提供されるサービスは、共通の運用、セキュリティ、経済的基盤を共有しており、お客様は環境を再構築することなく、時間の経過とともに機能を追加できます。Citrix Cloud の詳細については、こちらをご覧ください。

機能

Citrix Platform Flex は、以下のプラットフォームレベルの機能を提供します。

- **ペルソナベースのコンピューティング**: サービスは、静的なインフラストラクチャやVMごとのライセンスではなく、Citrix Flex Credits を使用してワーカーペルソナに基づいて消費されます。クレジットは、提供されるサービスに基づいて毎月消費されます。これにより、さまざまな種類のユースケースに対して、パフォーマンス、セキュリティ、コストを適切に調整できます。
- **Citrix が管理するインフラストラクチャ**: Citrix は、ライフサイクル管理、パッチ適用、回復力を含む基盤となるクラウドインフラストラクチャを所有および運用します。お客様は、インフラストラクチャの運用ではなく、アプリケーション、ポリシー、ユーザーエクスペリエンスに集中できます。
- **回復力**: プラットフォームサービスは、高可用性と事業継続性のために設計されており、マルチリージョン展開パターンと統合された回復力機能をサポートしています。
- **統合されたコントロールプレーン**: 管理、監視、アクセス、ポリシーは Citrix Cloud を通じて提供され、サービス全体で一貫した管理エクスペリエンスを提供します。

利用可能なサービス

Citrix Platform Flexは、プラットフォームのペルソナと機能モデルに対応するサービスを提供します。

現在のサービスは次のとおりです。

- **Citrix DaaS Flex**: Microsoft Azure上のCitrix管理インフラストラクチャを使用した、ペルソナベースの仮想アプリおよびデスクトップ配信。Citrix DaaS Flexを参照してください。
- **Citrix SecurSpaces™ Flex**: Microsoft Azure上のCitrix管理インフラストラクチャを使用した、開発者、データアナリスト、AIエージェント向けのペルソナベースのワークスペース。Citrix SecurSpaces Flexを参照してください。
- **Citrix Experience Insights Flex**: Citrix Experience Insights Flexは、組織がワークスペーステレメトリから、エクスペリエンス、パフォーマンス、運用回復力、セキュリティのユースケース全体にわたる実用的なインサイトへと、より迅速に移行できるよう支援します。Citrix管理の分析モデルを通じて提供され、Splunkによって強化されています。

時間の経過とともに、セキュリティ、運用、使用のための同じプラットフォーム基盤を活用して、追加のプラットフォームサービスがCitrix Platform Flexを通じて提供される可能性があります。

概念と用語

Flexクレジット

Citrix Platform Flexを購入するお客様は、所定の数のクレジット（**Flexクレジット**とも呼ばれます）のライセンスを取得します。Flexクレジットは柔軟性があり、上記の利用可能なサービスを利用するために活用できます。各ペルソナに関連付けられたクレジットについては、以下の表を参照してください。

ペルソナ

Citrix Platform Flexは、ワーカープロファイルを簡単に定義するために、ペルソナベースのコンピューティングアプローチを活用します。ペルソナは仮想アプリまたはデスクトップ配信モデルによって定義され、Citrixの主要なプラクティスに基づいて事前設定されます。カスタムペルソナは、Citrix DaaS Flexをさまざまなユーザー要件に適応させるように構成できます。

Citrix Platform Flexのサービスとペルソナは次のように定義されます。

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
Flexサービス	Citrix DaaS フレックス	タスクワーカー（ライト）	v1	日常の基本的な生産性向上、Webブラウジング、軽量なクラウドベースのSaaSアプリケーションに最適です。	VDAあたり16ユーザーのマルチセッション仮想アプリケーション。8 vCPU、32 GB RAM、128 GBストレージ。Windows Server OS、RDS
		タスクワーカー（ミディアム）	v1	現代の企業ワーカーの大部分の利用状況に合致します。現代のワーカーのアプ	VDAあたり8ユーザーのマルチセッション仮想アプリケーション。8 vCPU、32

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				リケーション要件は、一般的にSaaSと企業アプリケーションの組み合わせです。	GB RAM、128 GB ストレージ。Windows Server OS、RDS
		タスクワーカー (ヘビー)*	v2	タスクを完了するために企業アプリケーションへの頻繁なアクセスを必要とするユーザーに適合します。	VDAあたり4ユーザーのマルチセッション仮想アプリケーションおよびデスクトップ。8 vCPU、32 GB RAM、128 GB ストレージ (非永続)。Windows Server OS、RDS
		ナレッジワーカー (ライト)	v1	標準的な管理タスク、軽いマルチタスク、および主要なWebベースのコミュニケーションツール向けに設計されています。	シングルセッション仮想デスクトップ。2 vCPU、8 GB RAM、128 GB ストレージ。BYOL Windows 11
		知識労働者 (中)	v1	仮想デスクトップ環境	シングルセッション

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				(VDI) 内でのみ作業するユーザーに最適です。高度なセキュリティが求められるユースケース、コールセンター、またはシンクライアントやゼロクライアントの導入を検討している組織に最適です。	仮想デスクトップ。4 vCPU、16 GB RAM、128 GB ストレージ。BYOL Windows 11
		知識労働者 (高)	v1	複数のビジネスアプリケーション、大規模なスプレッドシート、データ分析を同時に実行するパワーユーザー向けに構築されています。	シングルセッション仮想デスクトップ。8 vCPU、32 GB RAM、128 GB ストレージ。BYOL Windows 11
		知識労働者 (超高)	v1	大規模なメモリ、大量のデータセット、および重いローカル処	シングルセッション仮想デスクトップ。8 vCPU、64 GB RAM、

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				理を必要とする複雑なマルチタスクワークフロー向けに最適化されています。	128 GBストレージ。BYOL Windows 11
		パワーワーカー (GPU)	v1	人工知能 (AI)、機械学習、データ視覚化などの、グラフィック要件の高いユーザーに最適です。	GPU対応シングルセッション仮想デスクトップ。6 vCPU、55 GB RAM、4 GB GPU (A10)、128 GBストレージ。BYOL Windows 11
		パワーワーカー (非GPU)	v1	専用のグラフィックレンダリングを必要としない、CPU負荷の高いコンピューティング、コードコンパイル、データ処理向けに設計されています。	シングルセッション仮想デスクトップ。16 vCPU、64 GB RAM、128 GBストレージ。BYOL Windows 11
	シトリックス セキュアスペース フレックス	開発者 (ライト)	v1	軽量な開発、スクリプト作成、コードレ	2vCPU、8 GB RAM、32 GB ストレージを備

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				ビュー、およびユーザーがソースコード、ツール、依存関係への安全なアクセスを必要とするが、控えめな計算要件しか持たない短期間のワークスペース向け。小規模なサービス、ドキュメント、自動化タスク、または時折の開発活動に取り組む開発者、請負業者、技術ユーザーに適しています。	えたLinuxコンテナ
		開発者 (ミディアム)	v1	ユーザーが追加のCPU、メモリ、ストレージ容量を備えたバランスの取れたワークスペースを必要とする、日常的	4vCPU、16 GB RAM、64 GB ストレージを備えたLinuxコンテナ

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				なアプリケーション開発、テスト、デバッグ向け。標準的なIDE、ビルドツール、アプリケーションランタイム、中規模のリポジトリを扱うフルタイムの開発者に適しています。	
		開発者 (ヘビー)	v1	計算集約型の開発、大規模なリポジトリ、複雑なビルド、ローカルテスト環境、およびより高いパフォーマンスとより多くのワークスペース容量を必要とする高度なワークロード向け。要求の厳しい開発ツールチェーンや頻繁なビルドおよびテ	8vCPU、32 GB RAM、128 GBストレージを搭載したLinuxコンテナ

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
				ストサイクルを実行するシニア開発者、プラットフォームエンジニア、データエンジニア、チームに適しています。	
同上	シトリックス エクスペリエンス インサイト フレックス	すべて	v1	企業全体にわたるすべてのプラットフォームで、エンドユーザーエクスペリエンスとセキュリティに関する実用的なインサイトを得るため。	デジタル従業員エクスペリエンス(DEX)。追加のクレジットでセキュリティ機能を追加するオプションがあります。
SaaS	シトリックス セキュアアクセス (Chrome Enterprise と連携)	すべて	v1	日常のWebまたはSaaSアプリケーションにChrome Enterprise Premiumを活用するユーザー向け。	DaaS Flexへのアドオン、またはスタンドアロンとしてのCE機能付きCSA
ソフトウェアのみ	シトリックス DaaS	すべて	v1	お客様のセルフホスト	お客様定義。スト

カテゴリ	サービス	ペルソナ	バージョン	説明	CITRIXデリバリーモデル
	(ローカル/クラウド)			オプション。	レージは適用されません

注:

- *Citrix は、今後のリリースでタスクワーカー（ヘビー）ペルソナを非推奨にする予定です。今後のマシンカタログには、利用可能な別のFlexペルソナを使用してください。
- 表示されているクレジットは、非永続的なプールされたワークロード用です。永続的な専用ワークロードには、追加オプションのセクションに記載されている追加のアドオン料金が発生します。

追加オプション

Citrix Flexは、エンドユーザーのニーズに合わせてワークロードをカスタマイズする柔軟性を提供します。追加オプションは、Flexペルソナと組み合わせて使用されるオプション機能またはサービスとして定義されます。

CITRIX DAAS フレックス

各ペルソナのオプションのディスクサイズとタイプは、イメージで使用されるディスクによって決定されます。それに対応するFlexクレジットコストは次のように定義されます。

説明	サイズ
シングルセッション永続ペルソナのディスクコスト	128 GB 標準 SSD ディスク
	256 GB 標準SSDディスク
	512 GB 標準SSDディスク
	1024 GB 標準SSDディスク
	128 GB プレミアムSSDディスク
	256 GB プレミアムSSDディスク
	512 GB プレミアムSSDディスク

説明	サイズ
	1024 GB プレミアムSSDディスク
マルチセッションの非永続的ペルソナのディスクコスト	128 GB プレミアム SSD ディスク

サービス

以下のCitrix Platform Flexサービスドキュメントを参照してください。

- シトリックス DaaS フレックス
- シトリックス セキュアスペース フレックス
- シトリックス エクスペリエンス インサイト フレックス

プラットフォーム Flex Credit の消費とレポート

Flex Credit は、ペルソナセクションで定義された Flex サービスに基づいて毎月消費されます。その他のサービスは Flex Credit を消費しません。全体的な使用パターンを把握するのに役立つ月次 Flex Credit 消費レポートが利用可能です。

サービス別の消費計算

- **Citrix DaaS Flex (マネージドキャパシティペルソナ)**: これは、Citrix マネージドキャパシティペルソナ（例：タスクワーカー（ヘビー、ミディアム）、ナレッジワーカー、パワーワーカー、カスタムペルソナ）および永続デスクトップ用ディスクなどの関連アドオンに適用されます。消費は、各ペルソナに設定された一意のユーザー数に基づきます。設定されたペルソナは、アクティブに使用されなくても Flex Credit を消費します。カタログの作成とキャパシティの増加は月単位で日割り計算されますが、キャパシティの削減と削除は日割り計算されません。カタログの作成が失敗した場合、Flex Credit は消費されません。

  例: タスクワーカーユーザー 100 人 × タスクワーカー Flex Credit 値 = 毎月差し引かれる Flex Credit の合計。

> **注:**
>
> 効率を維持するため、これらのインスタンスは非アクティブ期間中に休止状態になることがあります。Azure での通常の再開時間は 5 分未満です。

- **Citrix SecurSpaces™ Flex (マネージドキャパシティペルソナ)**: これは、Citrix マネージドキャパシティペルソナ（例：開発者（ライト、ミディアム、ヘビー））に適用されます。消費は、各ペルソナに設定された一意のワークスペース数に基づきます。設定されたペルソナは、アクティブに使用されなくても Flex Credit を消費します。Citrix SecurSpaces ワークスペースの作成とキャパシティの増加は月単位で日割り計算されます。SecurSpaces ワークスペースの作成が失敗した場合、Flex Credit は消費されません。

  例: 開発者（ミディアム）ユーザー 100 人 × 開発者（ミディアム）Flex Credit 値 = 毎月差し引かれる Flex Credit の合計。

- **Citrix Experience Insights Flex**: 消費は一意のユーザー数に基づきます。指定された各ユーザー数は、ユーザーがアクティブにオンボーディングされていなくても Flex Credit を消費します。ユーザーの追加は月単位で日割り計算されます。

  例:

  - ユーザーエクスペリエンスのユーザー 10,000 人 × ユーザーエクスペリエンスクレジット = 毎月差し引かれる Flex Credit の合計。
  - ユーザーエクスペリエンス + セキュリティのユーザー 10,000 人 × ユーザーエクスペリエンス + セキュリティクレジット = 毎月差し引かれる Flex Credit の合計。

- **Citrix DaaS Cloud/Local (Bring Your Own Infrastructure)**: これは、Citrix Virtual Apps and Desktops または Citrix DaaS を独自のインフラストラクチャ展開モデルで使用しているお客様に適用されます。消費は、アクセスするサービスの数に関係なく、一意のユーザーごとに計算されます。単一のユーザーが Citrix Virtual Apps and Desktops と Citrix DaaS の両方を使用する場合でも、1 ユーザーとしてのみカウントされます。月内の一部使用に対する日割り計算はありません。

  例: ユーザー 1,000 人 × ユーザーあたりの Flex Credit 値 = 毎月差し引かれる Flex Credit の合計。

- **Citrix Secure Access with Chrome Enterprise (CSA with CE)**: 消費量は一意のユーザーごとに厳密に計算されます。月ごとの部分的な使用に対する日割り計算はありません。

> **注:**
>
> Flexクレジットは、お客様の合計ライセンスユニット総数から毎月差し引かれます。これは、ビジネスユニットの利用規約において**Flex Credit Allotment**と呼ばれています。

追加条項

- **調整**: Flexクレジットの調整が必要であると判断される場合、サポートチケットを提出する必要があります。Citrixが調査し、適切な次のステップを決定します。
- **停止**: 合計ライセンス量を使い果たした場合、または残りのFlexクレジット残高が希望する使用量をカバーするのに不十分な場合、Flexクレジットベースのサービスを利用することはできません。
- **失効**: サブスクリプション期間中に消費されずに残ったFlexクレジットは、お客様の注文書に記載されている契約終了日に失効します。

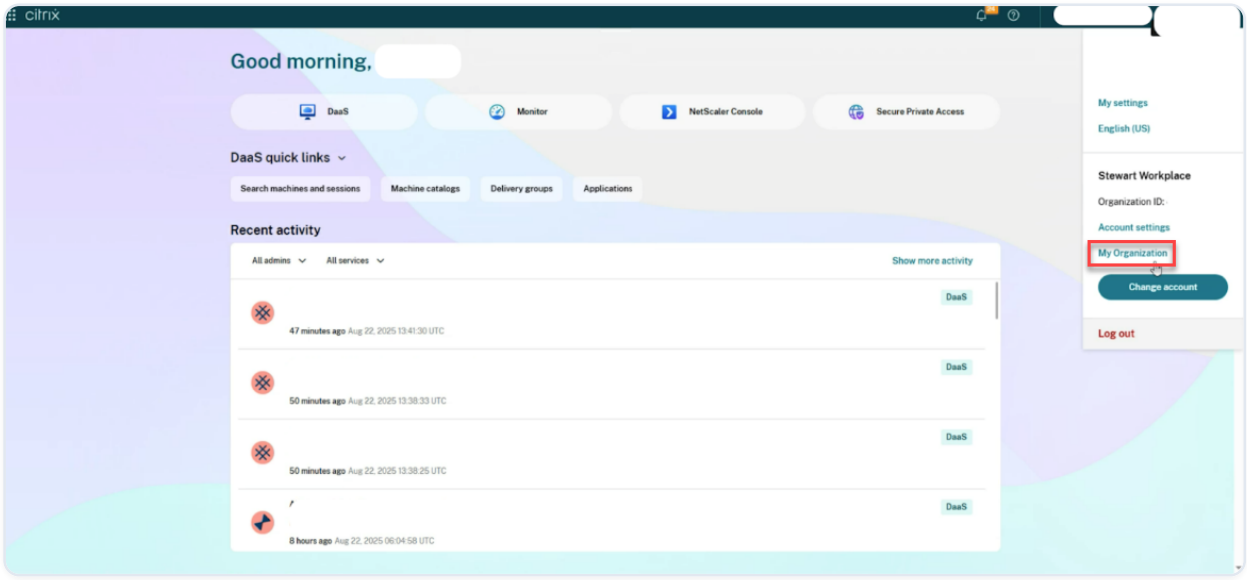
Citrix Cloudの管理

Citrix Cloud™ アカウント管理

この記事では、Citrix Cloudアカウントのオンボーディングプロセスと、アカウントのライセンス管理について説明します。

Citrix Cloudアカウントを作成する

1. Citrix **Cloud**コンソールで、**プロファイルメニュー**からMy Organizationをクリックして開始します。

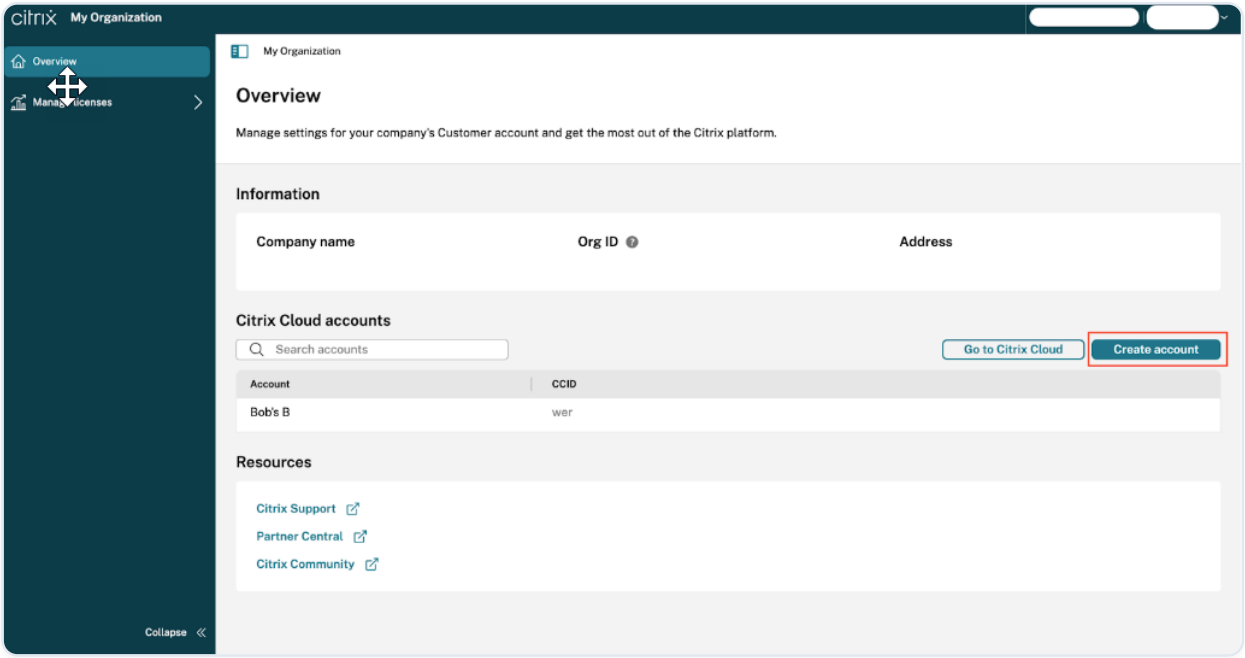


> **注：**
>
> My Organizationオプションが表示されない場合、アクセスする適切な権限がありません。ライセンス管理の正しい管理者として追加するよう、MyCitrix Account管理者に依頼してください。詳細については、サポートリンクを参照してください。

> 既存のCitrixのお客様でCitrix Cloudアカウントをお持ちでない場合は、My Organizationにアクセスしてクラウドテナントをオンボーディングし、Citrix Cloudアカウント管理の手順に従ってください。

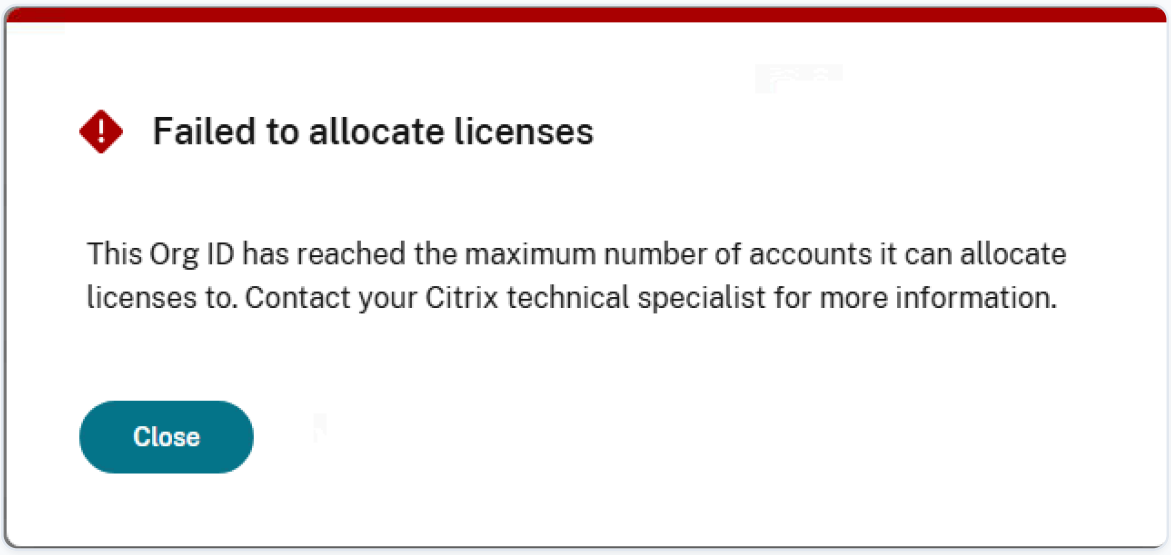
Citrix®を初めてご利用になる場合は、アカウント担当者に連絡してOrgIDを作成してもらい、サインアップしてください。

2. My Organizationのホームページから、**アカウントを作成**をクリックします。



注：

Citrixのお客様は、My Organization内で新しいクラウドテナントを個別に作成し、ライセンスを管理できます。オンボーディングされたクラウドテナントにライセンスを割り当てる際に以下のメッセージが表示される場合、合計ライセンス数量に基づいてライセンスを割り当てられるアカウントの最大数に達しています。詳細については、Citrix担当者にお問い合わせください。



> Citrix Partnerは、My Organizationから最初のパートナーCitrix Cloudアカウントのみをオンボーディングできます。新しいお客様をオンボーディングする場合は、My customers Dashboardを参照してください。

3. 「**アカウント名**」を入力し、ドロップダウンリストのオプションから「**クラウドタイプ**」を選択し、「**次へ**」をクリックします。

   アカウント名とクラウドタイプ(/en-us/citrix-cloud/media/account-name-cloud-type.png)

   > 「**注:**」:
   >
   > 利用可能なクラウドタイプのオプションは、Government、Japan、および Commercial です。

4. アカウントへの初期アクセス権を持つべき**Citrix Cloud管理者**を選択します。この管理者が初期ログイン情報を受け取ります。その後、「**次へ**」をクリックします。

   Citrix Cloud管理者(/en-us/citrix-cloud/media/select-citrix-cloud-admin.png)

5. 「**アカウント名**」、「**クラウドタイプ**」、および「**管理者**」の詳細を確認し、その後「**リクエストを送信**」をクリックします。

   クラウドアカウント管理者の詳細を確認(/en-us/citrix-cloud/media/cloud-account-admin-details.png)

6. アカウントが正常に作成されたことを示すポップアップメッセージが表示されます。

   割り当て成功(/en-us/citrix-cloud/media/account-successfully-created.png)

   > 「**注:**」:
   >
   > Citrix Cloudアカウント作成の申請が失敗した場合は、カスタマーサポートチームに連絡して支援を求めてください。

ライセンス管理

A. クラウドライセンス管理

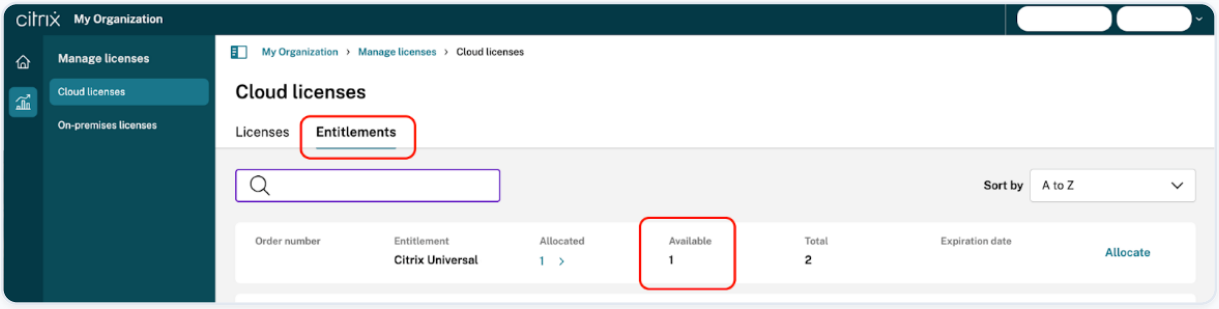
ライセンス割り当て

ユーザーは、Citrix Cloudカスタマーアカウントにライセンスを割り当てるアクセス権を持つようになりました。

注記:

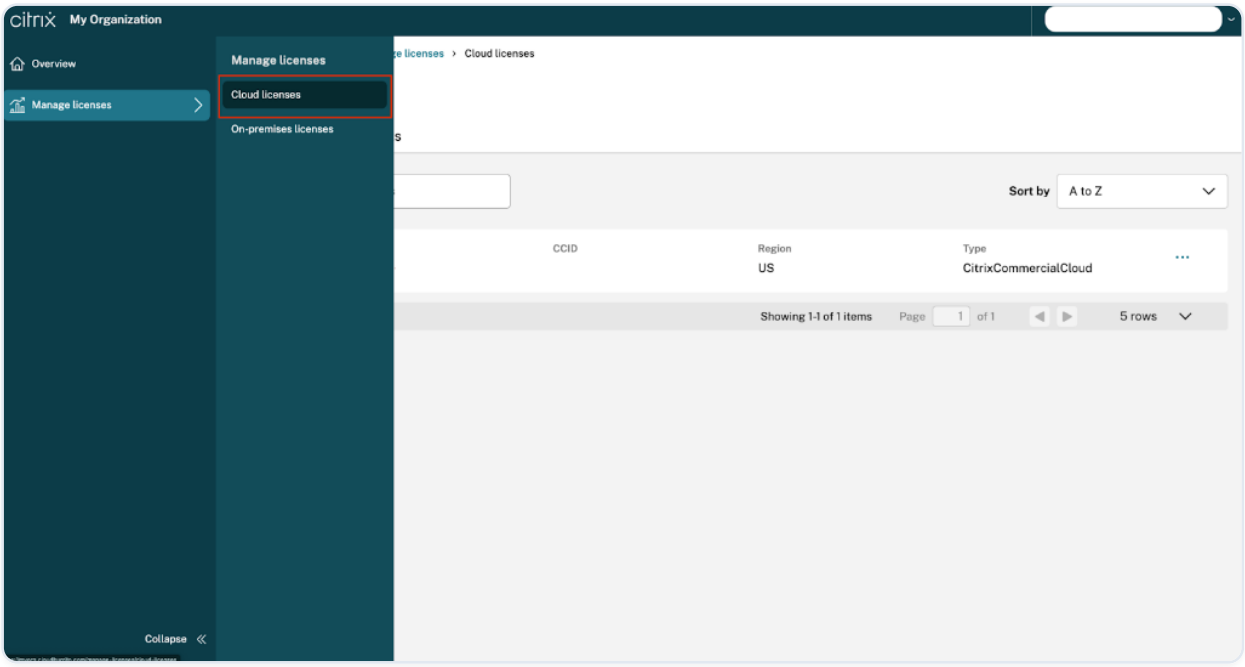
従来のライセンスモデル（UHMCおよびCPLを除く）からの異なるコントロールプレーン（政府機関、日本、商用など）間でのライセンス割り当てはサポートされていません。

Citrix Cloudアカウントに割り当てるために必要なライセンスが利用可能であることを確認してください。これについては、**My Organization > Manage Licenses > Cloud Licenses > Entitlements**で確認してください。そうでない場合は、適切なEntitlementsから割り当て解除を実行してライセンスを利用可能にしてください。割り当て解除の手順の詳細については、License Deallocationセクションを参照してください。

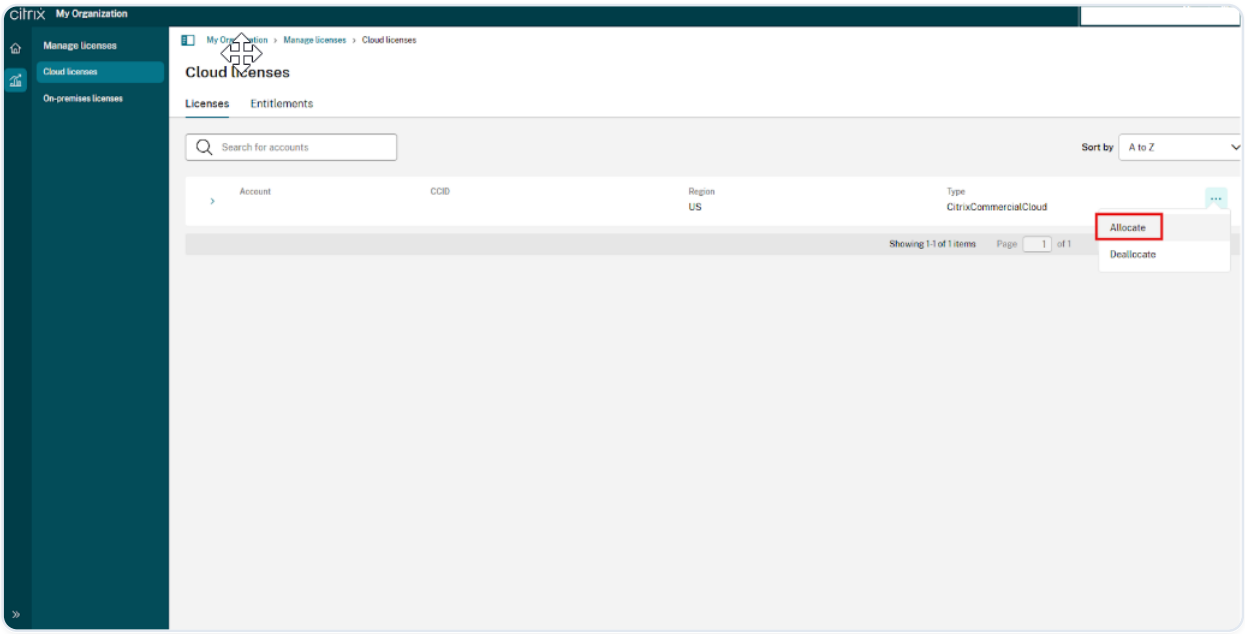


アカウントにライセンスを割り当てるには、次の手順を使用します。

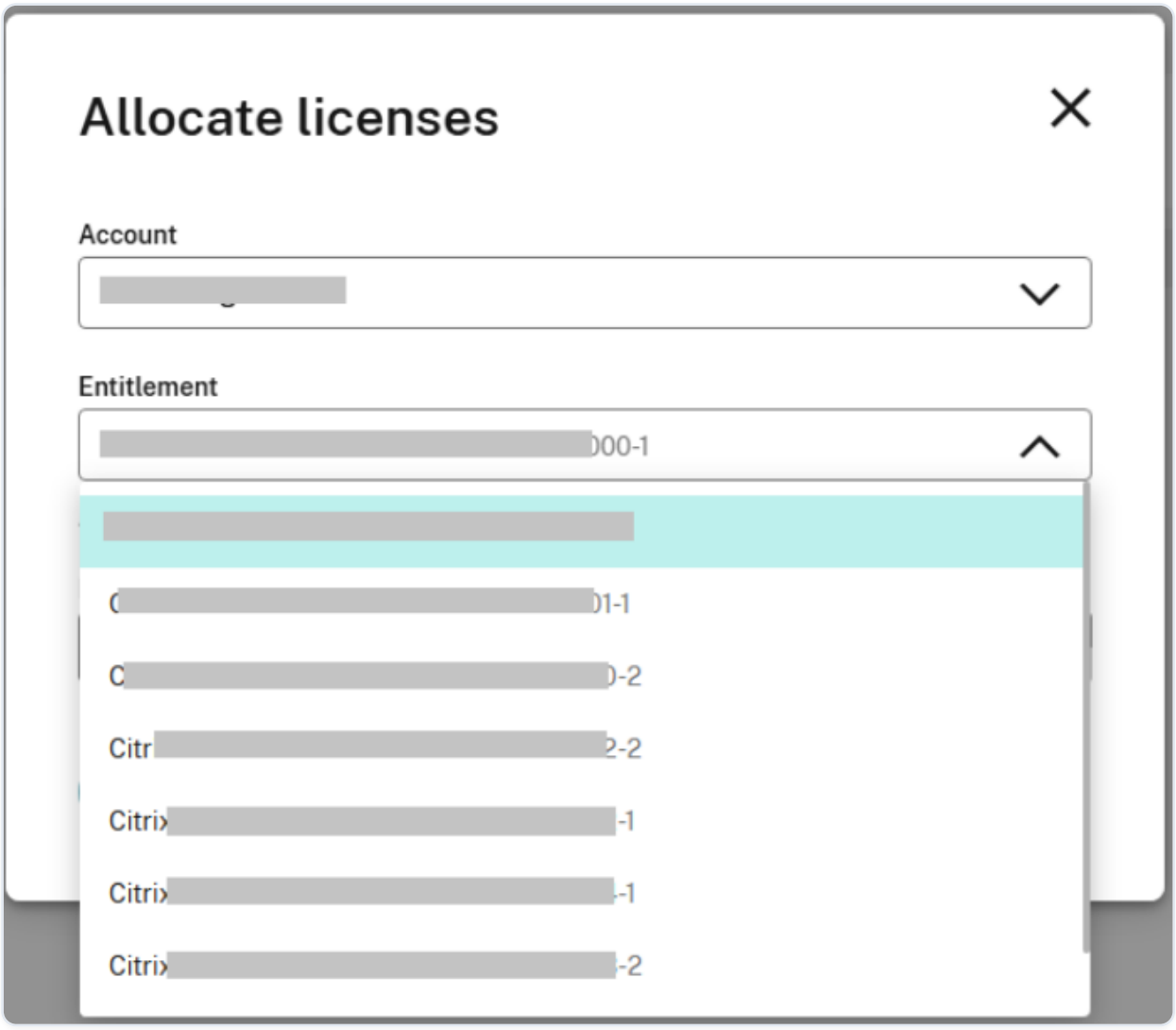
1. **Manage Licenses**セクションに移動し、**Cloud Licenses**をクリックします。



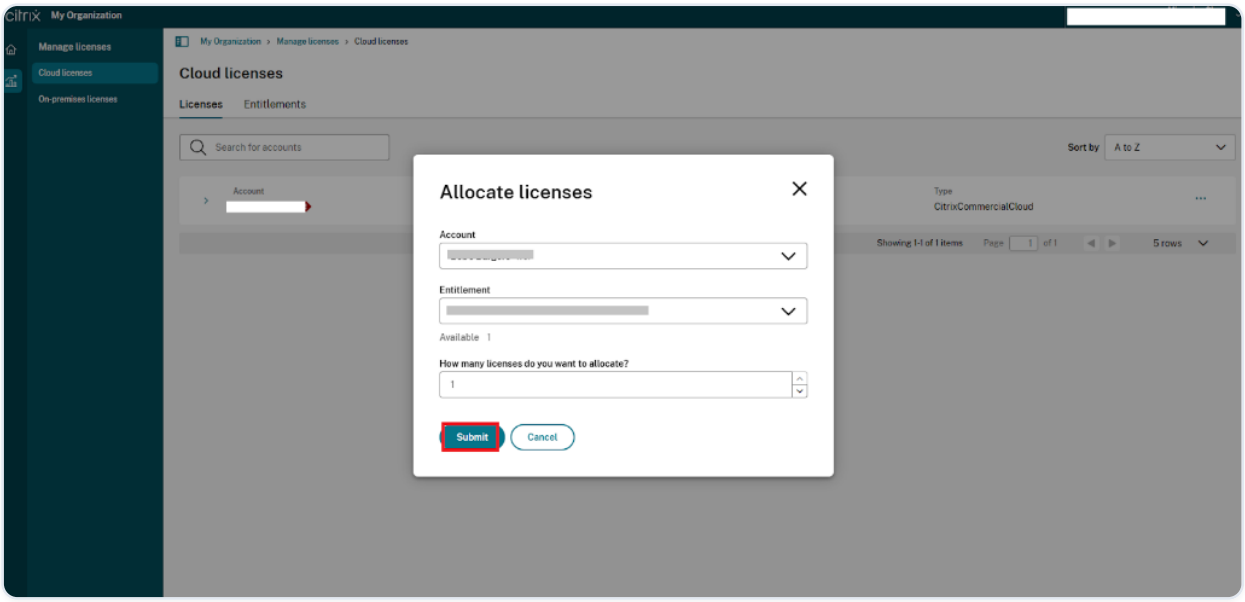
2. 新しいアカウントの省略記号をクリックし、**Allocate**を選択します。



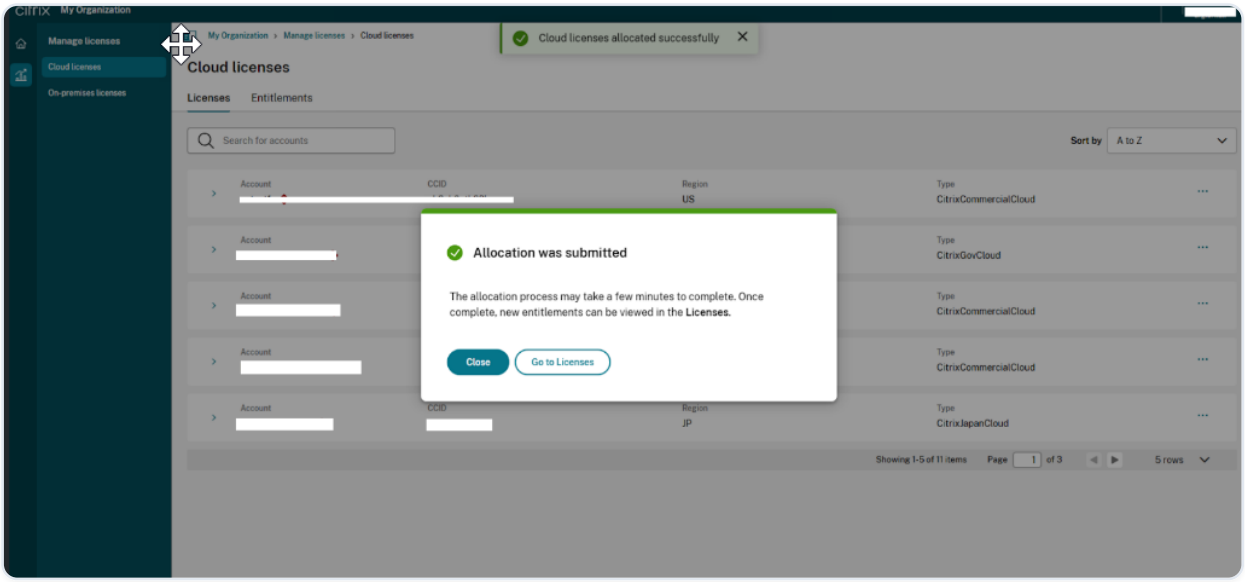
3. ドロップダウンリストオプションの利用可能なリストから**Entitlement**を選択します。



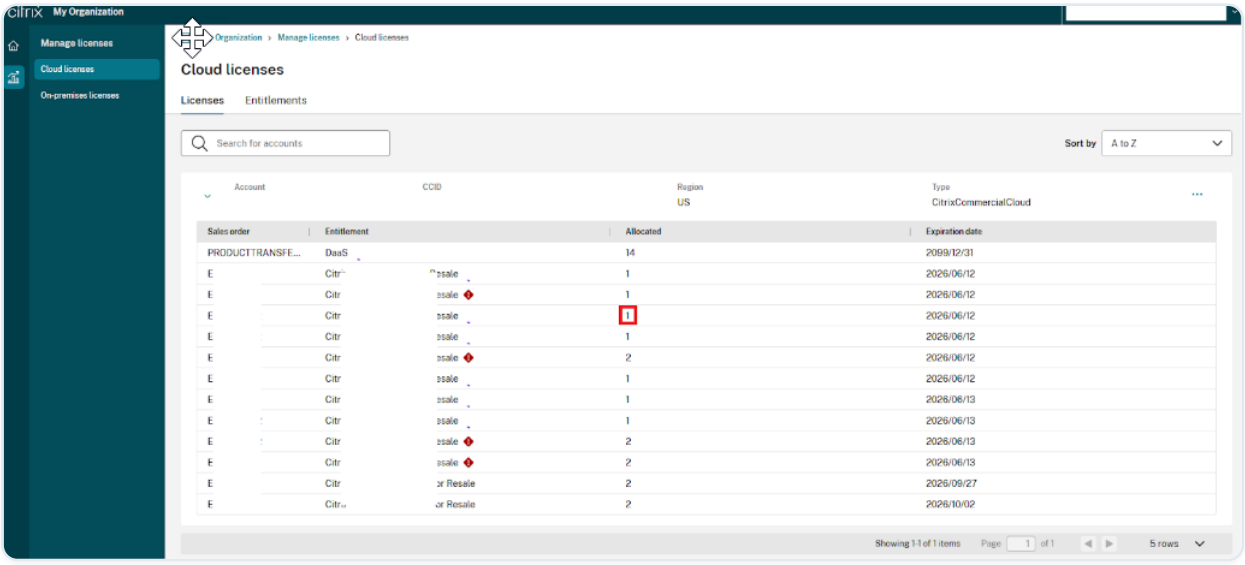
4. アカウントレベルで割り当てる各製品の数量を指定し、**Submit**をクリックします。



5. 割り当てリクエストを正常に送信した後、**Close**をクリックします。



6. 割り当てを確認するには、 > からアカウントを展開し、割り当て後の数量を確認します。



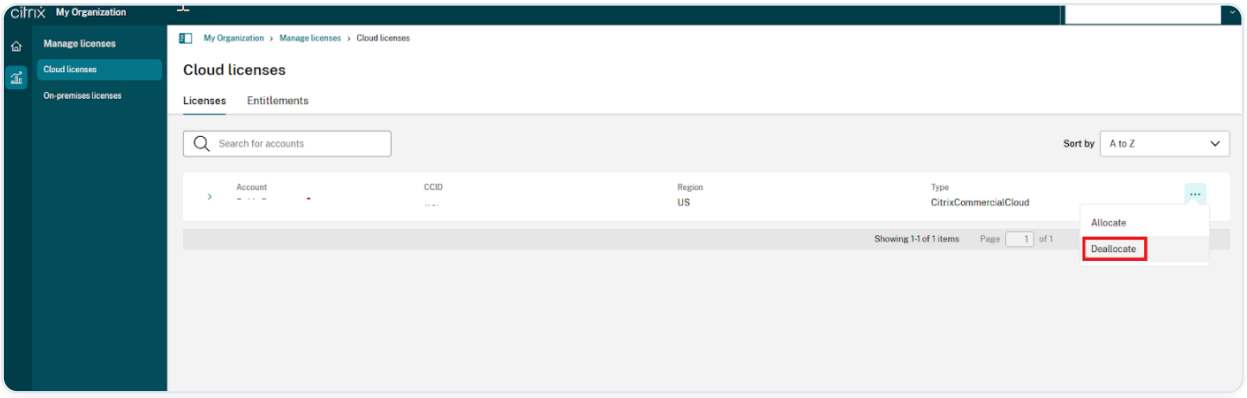
> **注:**
>
> 手順を完了すると、すべてのサービスを有効にし、アカウントにライセンスを割り当てるため、割り当ては数時間進行中になります。この間、お客様には処理状況を示すアイコンが表示されます。割り当てが完了すると、アイコンは消え、Cloud Adminコンソールに進んでサービスの使用を開始できるようになります。割り当てが失敗した場合は、Citrixカスタマーサポートにお問い合わせください。

ライセンスの割り当て解除

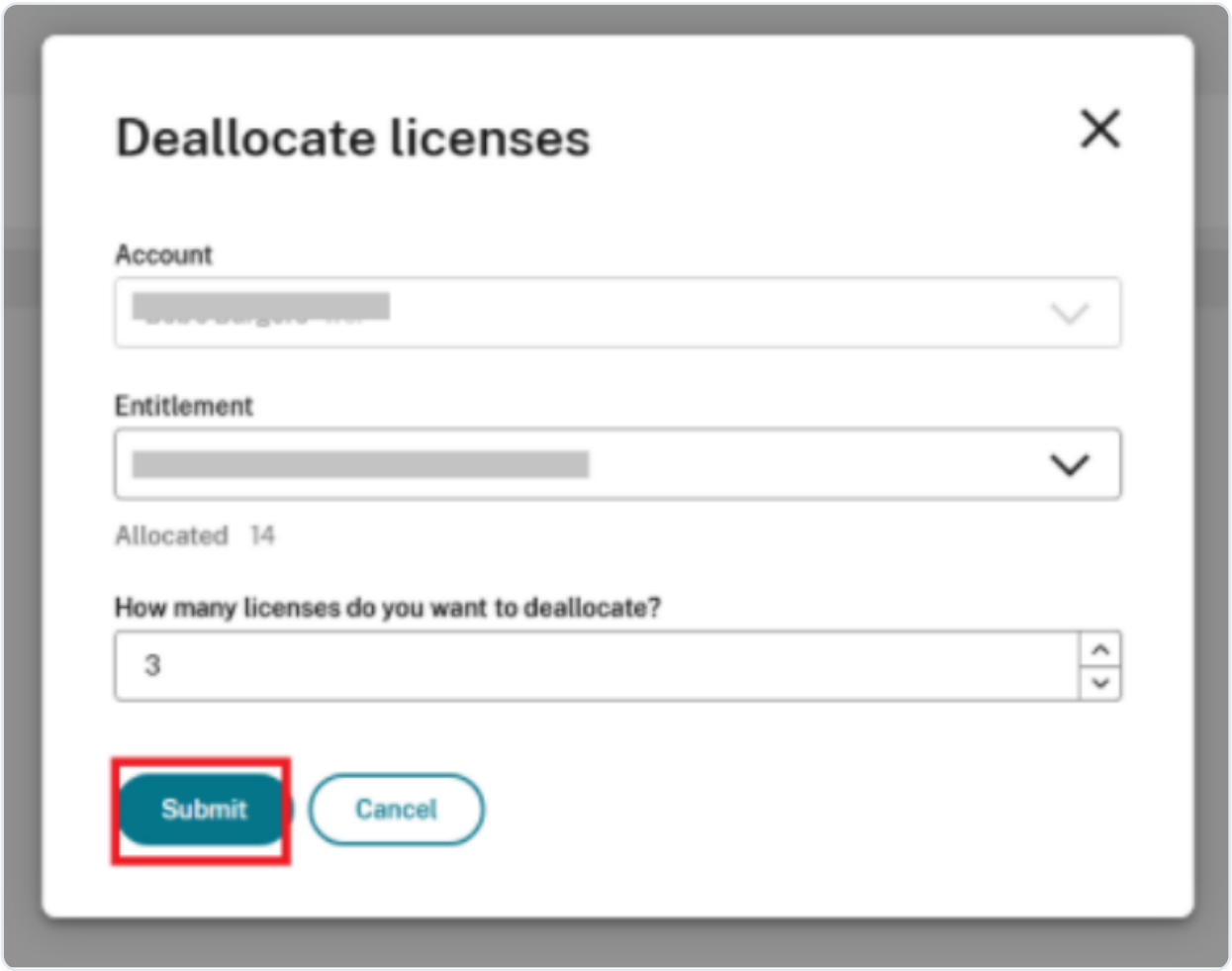
アカウントからライセンスの割り当てを解除するには、次の手順を使用します。

1. ページに移動し、 をクリックします。

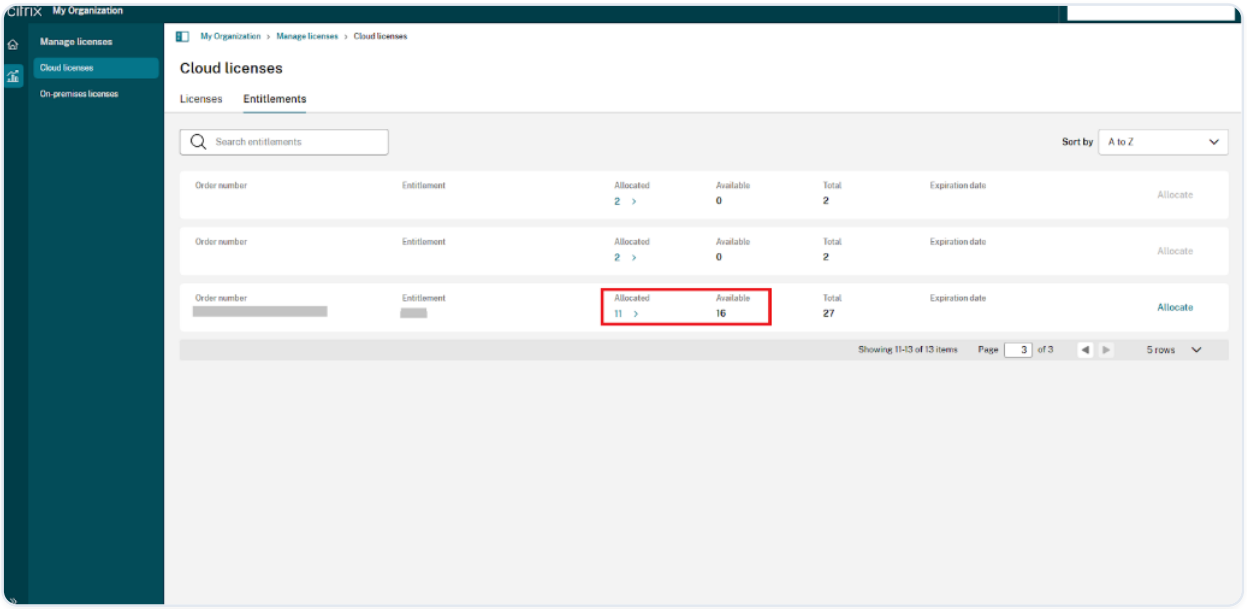
2. 新しいアカウントの省略記号をクリックし、 を選択します。



3. ドロップダウンリストから**** を選択します。正しいアカウントを選択していることを確認してください。
4. ドロップダウンリストから**** を選択し、 タブで割り当て解除するライセンス数を入力して**** をクリックします。



5. 割り当て解除を確認します。**ライセンスの管理** > **クラウドライセンス>エンタイトルメント** からアカウントを展開して、割り当て解除後の数量を確認します。



既知の問題

製品の重複 (ライセンスの管理 > クラウドライセンス) お客様は、単一の販売注文に関連付けられた同じライセンス数量を持つ重複した製品レコードに遭遇する可能性があります。これらの重複は、エンタイトルメント (**ライセンスの管理 > クラウドライセンス > エンタイトルメント**) の下に表示されるか、Citrix Cloudアカウントに直接割り当てられる場合があります。その結果、お客様は「アカウントの作成」ボタンで追加のCitrix Cloudアカウントを作成する権利を誤って付与されたり、重複した製品から新しいCitrix Cloudアカウントに追加のライセンスを割り当てたりする可能性があります。

推奨事項 これは既知の問題であり、Citrix は不適格な重複注文を削除することで、この問題の解決に積極的に取り組んでいます。お客様がクラウドテナントを作成し、これらのテナントへのライセンス割り当てまたは割り当て解除を実行した場合、Citrix からの今後の修正がサービスに影響を与える可能性があります。したがって、お客様がこの状況に陥った場合は、Citrix カスタマーサービスチームに連絡して、新しいCitrix Cloudテナントを作成する資格があることを確認し、クラウドテナントの作成、および/またはライセンスの割り当てまたは割り当て解除のための正しい権限を持っていることを確認する必要があります。

リブランドされた注文 お客様は、**ライセンスの管理**でリブランドされた製品に対して複数の割り当てがあることに気づく場合があります。元の製品割り当ては、ライセンス数量、有効期限、販売注文を共有する2つまたは3つの追加製品とともに表示されます。

お客様は、同じアセットに対して、ライセンス数量と有効期限が同じ複数の割り当てがある場合、リブランドされた注文を特定できます。すべての重複割り当ては、製品名として「DaaS」を表示します。お客様は、以下の方法でリブランドされた注文があるかどうかを確認できます。

- **ライセンスの管理 > クラウドライセンス > エンタイトルメント**で購入したアセットを確認し、割り当て用にリストされているパッケージと比較します。
- ブラウザでネットワークトレースを調べると、割り当てリストに`<Random_GUID>-<OrderId>`のパターンに従って複数のIDが表示され、`OrderId`は繰り返されますが、`Random_GUID`は繰り返されないことがわかります。

推奨事項 これは既知の問題であり、Citrix は無効な注文を削除することで、この問題の解決に積極的に取り組んでいます。アカウントを作成する前に、お客様はCitrix Cloudアカウントの作成に記載されている手順に従って、資格のあるアカウントを作成していることを確認し、資格のないアカウントを作成しないようにする必要があります。お客様がアカウントに無効な注文や重複した注文があることに気づいた場合は、カスタマーサービスチームに連絡できます。さらに、無効な注文による資格に基づいて作成されたCitrix Cloud顧客インスタンスは削除され、顧客の運用に影響を与える可能性があります。

カスタムランディングページ

多くの管理者はCloud Consoleにアクセスし、Web Studioコンソールでアプリケーションを管理したり、DaaS - Monitorでデータを表示したりするなどの特定のタスクを実行します。 しかし、これらのタスクは、管理者がログインするたびに複数回クリックし、複数のページを移動する必要があるため、時間がかかる場合があります。この新機能により、管理者はカスタムランディングページを設定または変更でき、時間を節約し、強化されたコンソールエクスペリエンスを提供します。

現在、カスタムランディングページとして構成できるページは以下のとおりです。今後、さらに追加される予定です。

- DaaS
- DaaS-モニター
- ネットスケーラー® コンソール
- CAS
- CASセキュリティ
- CASパフォーマンス
- WEM
- 一般

> **注:**

カスタムランディングページの設定はオプションであり、アカウントごとに設定されます。そのため、各管理者はCitrix Cloud内で独自のエクスペリエンスをカスタマイズできます。すべての管理者（カスタム管理者かフル管理者かを問わず）がこの機能にアクセスできます。

カスタムランディングページを構成する

1. プロファイル名をクリックし、**アカウント設定**を選択します。

   アカウント設定(/en-us/citrix-cloud/media/to-account-settings.png)

2. **カスタマイズ**をクリックします。

   カスタマイズ(/en-us/citrix-cloud/media/customization.png)

3. カスタムランディングページとして構成するサービスを選択します。

   サービス(/en-us/citrix-cloud/media/custom-service.png)

4. **適用**をクリックします。

   カスタムランディングページが設定されました。

注:

- **デフォルトにリセット**をクリックすると、いつでもカスタムランディングページをデフォルトのCloudホームページにリセットできます。
- ログアウトしたばかりの同じページで再度サインインした場合、新しいランディングページではなく、最後に表示したページに移動します。

Citrix Cloud™アカウントを削除して再オンボードする方法

Citrix Cloudは、お客様がCitrix Cloudアカウントを安全に削除し、必要に応じてシームレスに再オンボードできる機能を提供します。

前提条件

- アカウントにアクティブなDaaSエンタイトルメントがあり、DaaS環境がプロビジョニングされている場合は、続行する前にCitrixテクニカルサポートに連絡してFast Decommissionを実行してください。DaaS環境がプロビジョニングされているかを確認する方法の詳細については、Studio Console Shows "Enable DaaS" for First Time Useの記事を参照してください。

- このアカウントに関連付けられているすべてのCloud ConnectorおよびConnector Applianceを削除します。
- お客様は、削除リクエストを実行するためにCitrix Cloudアカウントへの管理者アクセス権を持っている必要があります。
  - Citrix Cloudアカウントへの管理者アクセス権を持たないお客様の場合、削除リクエストを進める前にSSAOを通じてアクセス権を取得する必要があります。
  - 管理者アクセス権を持つ管理者が1人だけの場合、その管理者は他の管理者を削除する必要があります。
- License Serverの登録を削除します。別のまたは新しいCitrix CloudアカウントにLicense Serverを登録したい場合は、必要な手順については、Remove Registrationを参照してください。

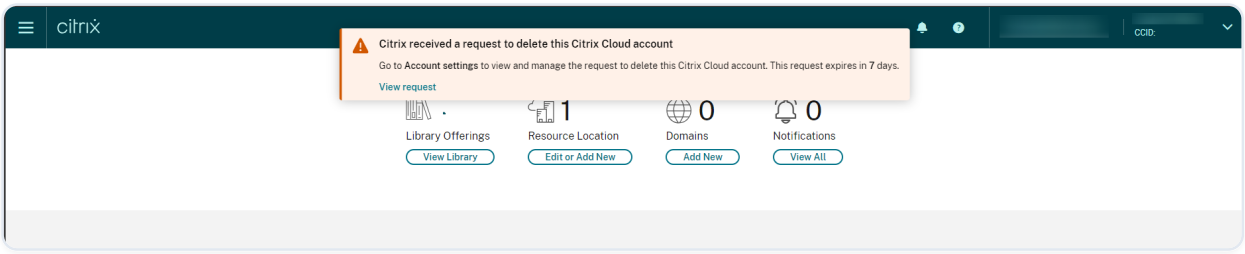
重要

Citrix Cloudアカウントを削除する前に、以下の点に留意してください。

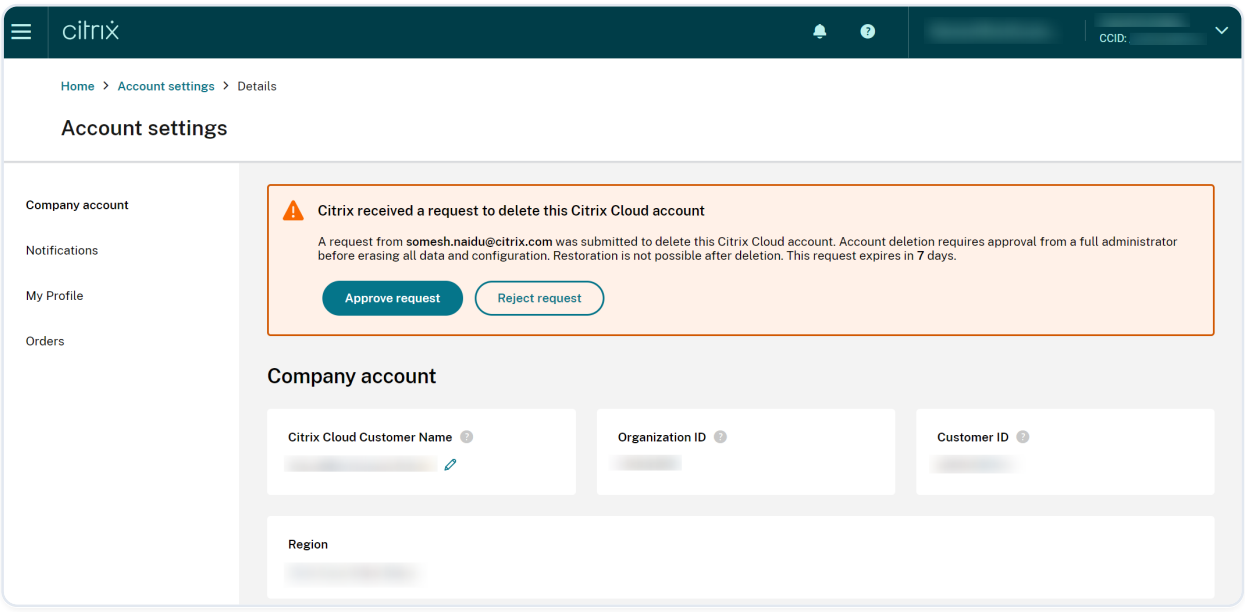
- すべての顧客関連データはCitrix®データベースから削除されます。
- Citrixがクラウド環境にプロビジョニングした、Citrix管理のVMを含むCitrix Cloudサービスに関連するすべてのリソースが削除されます。特定のCitrix Cloudサービスに含まれるCitrix管理コンポーネントの説明については、Citrix Cloud servicesを参照してください。
- Citrix Cloudおよびサービスへの管理者およびユーザーのアクセスは無効になります。
- サービスを積極的に利用している管理者またはユーザーは、サービスの中断を経験します。
- この操作は元に戻せません。データが削除されると、復元することはできません。

手順

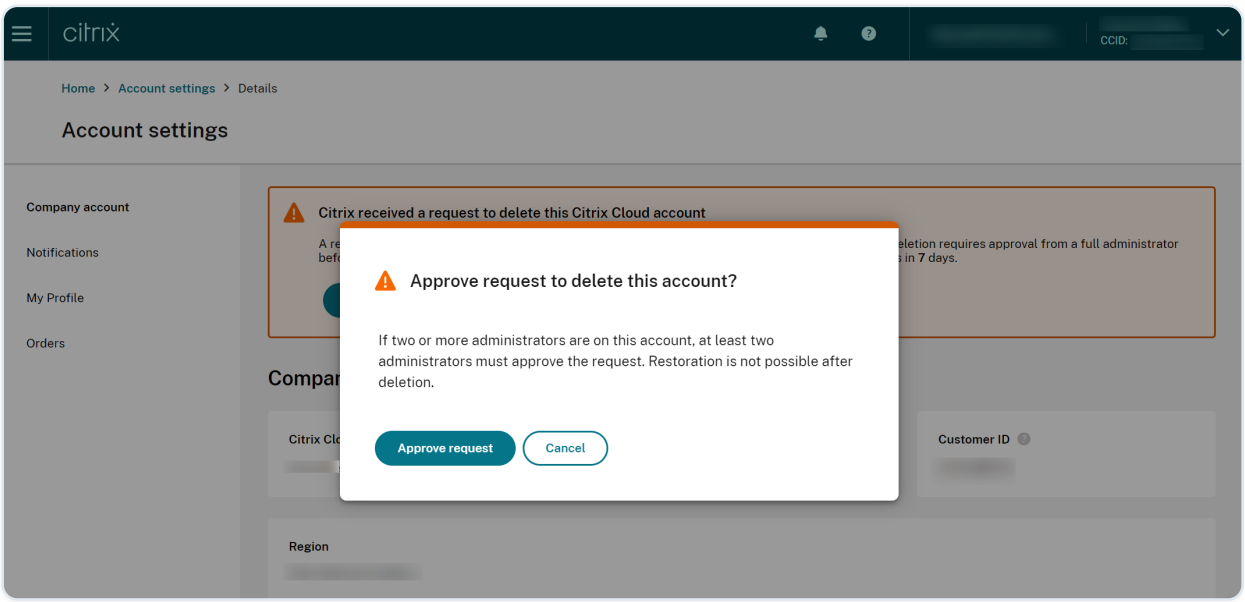
1. 削除リクエストを送信するには、Citrix Customer Service にお問い合わせください。このリクエストを送信するには、Citrix Cloudアカウントの *フル管理者* が必要です。
2. リクエストが開始されたら、Citrix Cloudアカウントにログインします。そこでCitrix Cloudアカウントの削除ワークフローが表示されます。



3. 画面の指示に従って、このリクエストを承認または拒否してください。



4. この削除リクエストを承認するには、アカウントにサインインし、**アカウント設定**に移動して、承認ワークフローバナーの**リクエストを承認**をクリックします。



削除リクエストをキャンセルするには、アカウントにサインインし、**アカウント設定**に移動して、削除承認ワークフローバナーの**リクエストを拒否して削除**をクリックします。

注：

- このアカウントに2人以上の管理者が関連付けられている場合、少なくとも2人の管理者がリクエストを承認する必要があります。
- 必要な承認が7日以内に得られない場合、このリクエストは期限切れになります。

ネットワークロケーション

Citrix Cloud™では、パブリックIPアドレスに基づいてネットワークロケーションを構成できます。これらのネットワークロケーションは、以下の目的で使用できます。

- Citrix® StoreFront Cloudは、ネットワークロケーションを使用して、クライアントにVDAに直接接続するよう指示するか、Citrix Gateway経由で接続するよう指示するかを決定します。詳しくは、「DaaSリソースへの接続」を参照してください。
- ユーザーがネットワークロケーションから接続すると、StoreFront Cloudは、Studio内のアクセスポリシーへの入力として使用できるスマートアクセスタグを追加できます。詳しくは、「ユーザーのネットワークロケーションに基づく適応型アクセス」を参照してください。この機能は、適応型アクセスが有効になっている場合にのみ利用できます。
- ユーザーのネットワークロケーションに基づいて、ユーザーの認証方法を選択できます。詳しくは、「条件付き認証」を参照してください。
- ネットワークロケーションの接続タイプに応じて、異なるタイムアウトを構成できます。詳しくは、「ネットワーク接続タイプごとのセッションの構成」を参照してください。

通常、各オフィスロケーションに対してネットワークロケーションを作成します。

注：

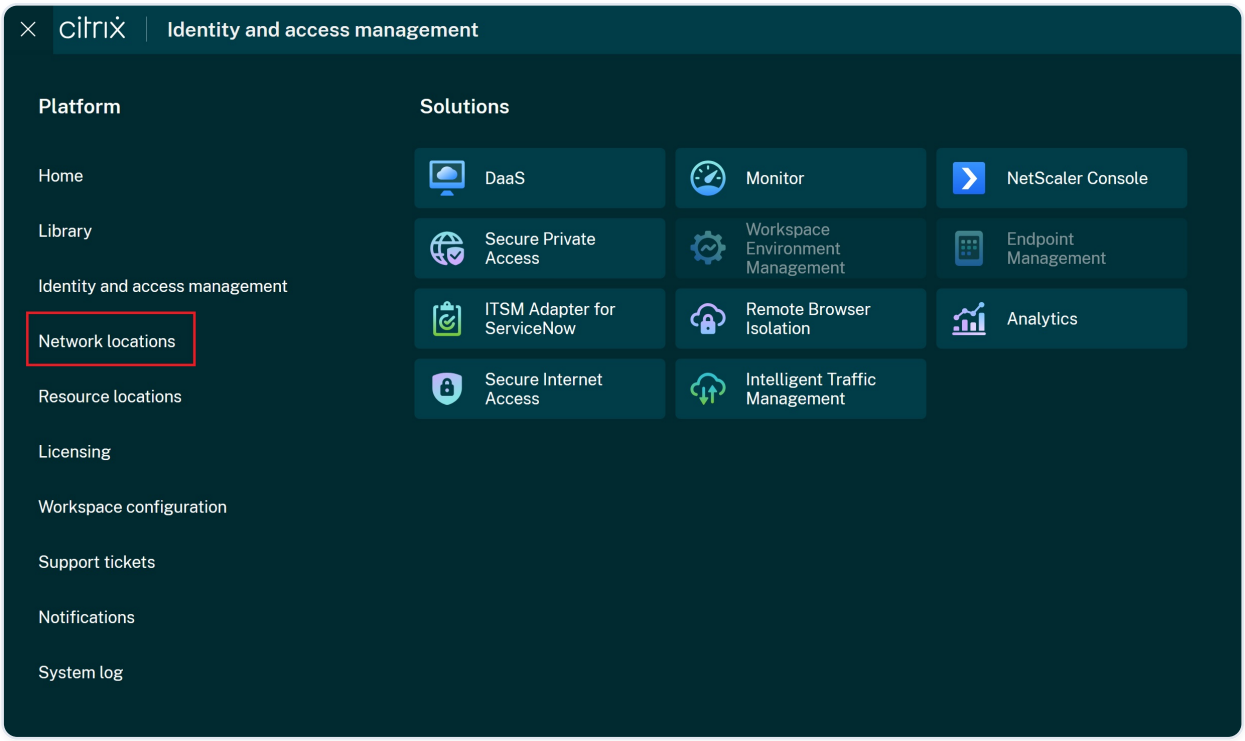
同じパブリックIPアドレスを持つ異なるネットワークを区別することはできません。たとえば、企業ネットワークとゲストWi-Fiネットワークが同じパブリックIPアドレスを共有している場合、それらは同じネットワークロケーションと見なされます。

ネットワークロケーションの表示

構成済みのネットワークロケーションを表示するには：

1. Citrix Cloudにログインします。
2. メインメニューを開きます。

3. メインメニューから、**［ネットワークロケーション］**を選択します。



4. 「ネットワークロケーション」画面が読み込まれます。

   ネットワークロケーション画面(/en-us/citrix-cloud/media/network-locations.png)

ネットワークロケーションの追加

1. 「ネットワークロケーション」画面で、**「ネットワークロケーションの追加」**をクリックします。

   ネットワークロケーションの追加(/en-us/citrix-cloud/media/network-locations-add.png)

   「ロケーションタグ」と「接続タイプ」のオプションは、Adaptive Accessが有効な場合にのみ利用できます。

2. **「ロケーション名」**を入力します。
3. **「パブリックIPアドレス範囲」**をCIDR形式で入力します。
4. Adaptive Accessが有効な場合、1つ以上の**「ロケーションタグ」**の名前をオプションで入力できます。複数のタグを区切るにはコンマを使用します。スマートアクセスタグは、サフィックス`LOCATION_TAG_`を追加することで生成されます。たとえば、ロケーションタグ`BranchOffice`を入力すると、Studioで使用できる`LOCATION_TAG_BranchOffice`というスマートアクセスタグが生成されます。
5. Adaptive Accessが有効な場合、ロケーションが**「内部」か「外部」かを選択できます。すべての内部ロケーションには、`LOCATION_internal`というスマートアクセスタグが生成されま

す。すべての外部ロケーションには、`LOCATION_external`というスマートアクセスタグが生成されます。クライアントのIPアドレスがネットワークロケーションと一致しない場合、そのネットワークロケーションは「未定義」**と見なされます。

Adaptive Accessが無効になっている場合、このオプションは非表示になります。構成されているすべてのネットワークロケーションは内部と見なされ、スマートアクセスタグは作成されません。

6. **「保存」**をクリックします。

ネットワークロケーションの編集

1. ネットワークロケーション画面に移動します。
2. 編集したい行で、**「...」**をクリックしてメニューを開き、**「編集」**を選択します。
3. 必要な変更を行います。
4. **保存**を押します。

ネットワークロケーションを削除

1. ネットワークロケーション画面を開きます。
2. 編集したい行で、**...**を押してメニューを開き、**削除**を選択します。
3. 確認画面で、**はい、削除します**を押します。

PowerShellでネットワークロケーションを管理する

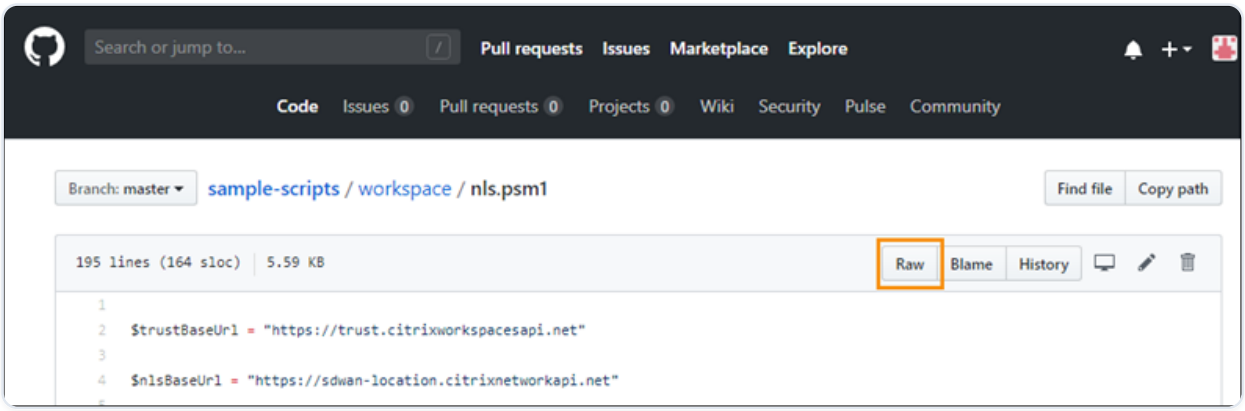
Citrix Cloud管理コンソールインターフェイスを使用する代わりに、PowerShellスクリプトを使用してダイレクトワークロード接続を構成できます。PowerShellによるダイレクトワークロード接続の構成には、次のものが含まれます。

1. PowerShellモジュールをダウンロードする。
2. Citrix Cloudでサービスプリンシパルを作成するし、クライアントIDとシークレットをメモします。
3. PowerShellモジュールをインポートするし、APIクライアントの詳細を使用してネットワークロケーションサービス (NLS) に接続します。
4. PowerShellコマンドレットを使用して、各ロケーションのネットワークロケーションを作成します。

PowerShellモジュールをダウンロードする

ネットワークロケーションを設定する前に、Citrix GitHubリポジトリからCitrix提供のPowerShellモジュール (nls.psm1) をダウンロードしてください。このモジュールを使用すると、VDAに必要な数のネットワークロケーションを設定できます。

1. Webブラウザで`<https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1>`にアクセスします。
2. 「**Raw**」を押します。



3. Ctrl+S を押して、ファイルを保存する場所を選択します。

サービスプリンシパルを作成する

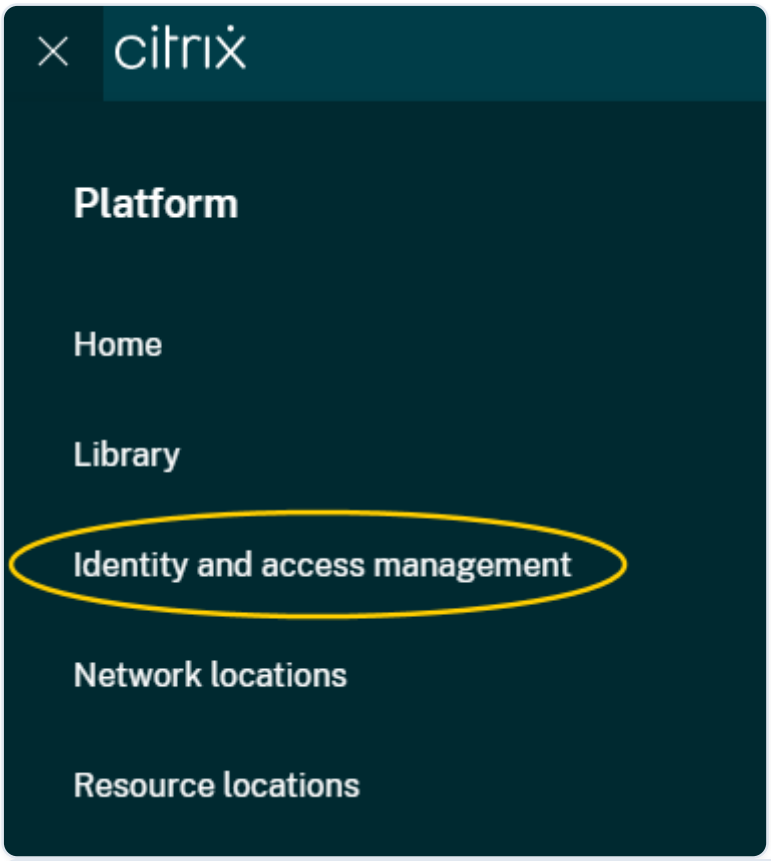
1. Citrix Cloud コンソールで、左上隅のメニューをクリックします。

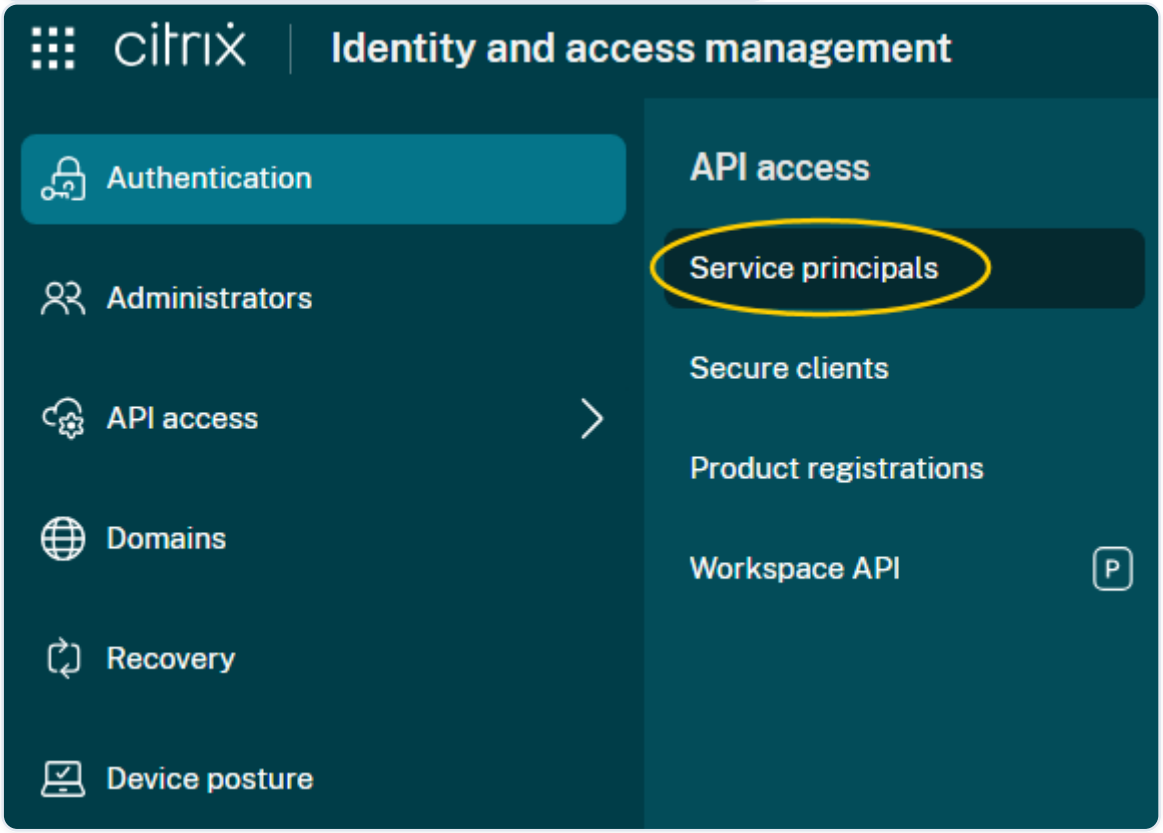


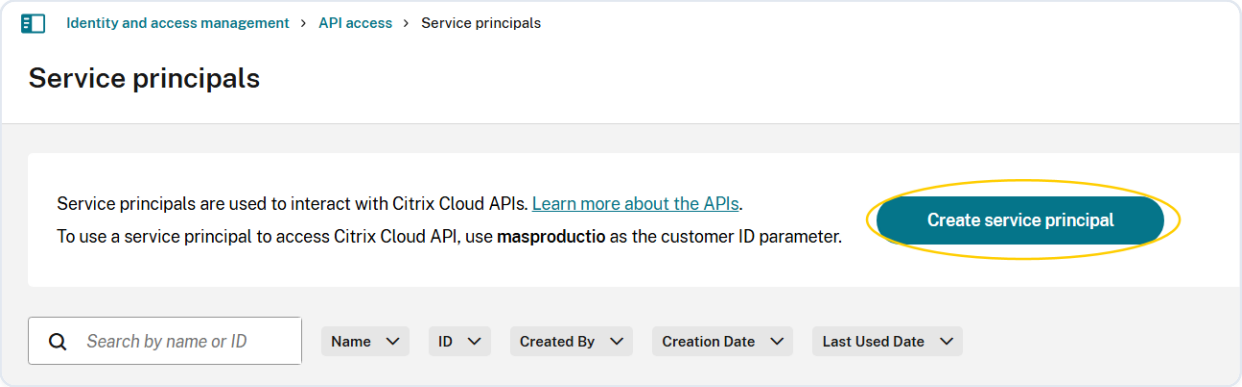
2. **ID およびアクセス管理** > **API アクセス** > **サービスプリンシパル** > **サービスプリンシパルの作成**を選択し、手順に従って完了します。

   これらのオプションが表示されない場合は、サービスプリンシパルを管理するための十分な権限がない可能性があります。必要なフルアクセス権限を取得するには、管理者に連絡してください。

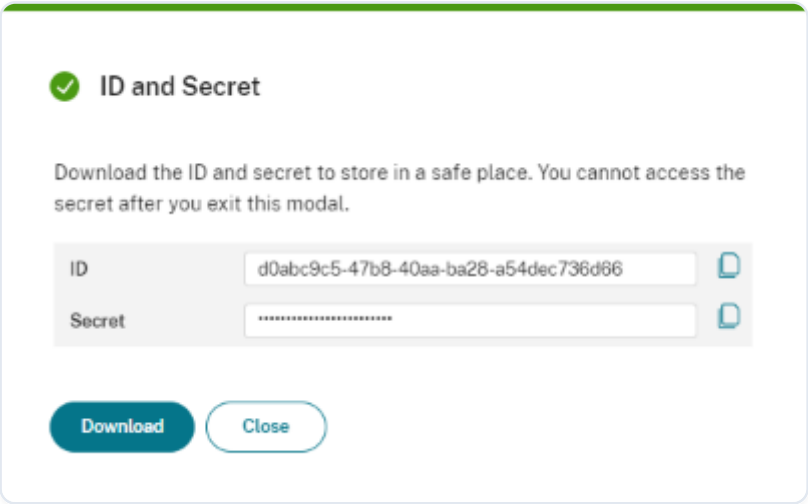
3. **サービスプリンシパル**タブで、顧客 ID をメモします。


citrix
Platform
Home
Library
Identity and access management
Network locations
Resource locations


citrix
Identity and access management
Authentication
Administrators
API access
Domains
Recovery
Device posture
API access
Service principals
Secure clients
Product registrations
Workspace API
P



4. シークレットは一度しか表示されないため、資格情報をシークレット管理ツールに追加します。



ネットワークロケーションを構成する

1. PowerShell コマンドウィンドウを開き、PowerShell モジュールを保存したのと同じディレクトリに移動します。
2. モジュールをインポートします: `Import-Module .\nls.psm1 -Force`
3. サービスプリンシパルを作成する から、サービスプリンシパル情報を使用して必要な変数を設定します。
   - `$clientId = "YourServicePrincipalClientId"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourServicePrincipalSecret"`
4. サービスプリンシパル資格情報を使用してネットワークロケーションサービスに接続します。

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
$customer
```

5. ネットワークロケーションを作成します。パラメーター値を、内部ユーザーが直接接続している内部ネットワークに対応する値に置き換えます。

```
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:

```
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場合、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なしでこのコマンドを実行すると、PowerShellは各パラメーターの適切な値を1つずつ入力するように求めます。`internal` プロパティは、PowerShellを介してUIにマッピングされる、`$True` または `$False` のいずれかの値を指定できる必須のブール型プロパティです。例: `(UI) Network Internal -> (PowerShell) –internal=$True`。

> ネットワークロケーション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ロケーションの詳細が表示されます。

6. ユーザーが接続しているすべてのネットワークロケーションに対して、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リストを返し、詳細が正しいことを確認します。

ネットワークロケーションの変更

既存のネットワークロケーションを変更するには:

1. PowerShellコマンドウィンドウから、既存のすべてのネットワークロケーションを一覧表示します: `Get-NLSSite`
2. 特定のネットワークロケーションのIP範囲を変更するには、次のように入力します。

```
(Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
```

ここで、`[N]`はリスト内のロケーションに対応する番号（ゼロから始まる）であり、`"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、リストの最初のロケーションを変更するには、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")
```

ネットワークロケーションを削除する

使用したくないネットワークロケーションを削除するには：

1. PowerShellコマンドウィンドウから、既存のすべてのネットワークロケーションを一覧表示します。`Get-NLSSite`
2. すべてのネットワークロケーションを削除するには、`Get-NLSSite | Remove-NLSSite`と入力します。
3. 特定のネットワークロケーションを削除するには、`(Get-NLSSite)[N] | Remove-NLSSite`と入力します。ここで、`[N]`はリスト内のロケーションに対応する番号です。たとえば、リストの最初のロケーションを削除するには、`(Get-NLSSite)[0] | Remove-NLSSite`と入力します。

スクリプトの例

このサンプルスクリプトには、ブランチロケーションのパブリックIPアドレス範囲を追加、変更、および削除するために必要なすべてのコマンドが含まれています。ただし、単一の機能を実行するために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、**Import-Module**から**Connect-NLS**までの最初の10行を常に含めてください。その後、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。

```
Import-Module .\nls.psm1 -Force



$clientId = "XXXX" #Replace with your clientId

$clientSecret = "YYY"    #Replace with your clientSecret

$customer = "CCCCCC"  #Replace with your customerid
```

```
# Connect to Network Location Service

Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
$customer



# Create a new Network Location Service Site (Replace with details
corresponding to your branch locations)

New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges
@("1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True



# Get the existing Network Location Service Sites (optional)

Get-NLSSite



# Update the IP Address ranges of your first Network Location Service Site
(optional)

$s = (Get-NLSSite)[0]

$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")

$s | Set-NLSSite



# Remove all Network Location Service Sites (optional)

Get-NLSSite | Remove-NLSSite



# Remove your third site (optional)
```

```
(Get-NLSSite)[2] | Remove-NLSSite
```

通知

通知は、管理者にとって関心のある可能性のある問題やイベントに関する情報を提供します。たとえば、新しいCitrix Cloud™機能やリソースの場所にあるマシンに関する問題などです。通知はCitrix Cloud内の任意のサービスから送信されます。

通知の表示

通知の数は、Citrix Cloudコンソールページの上部に表示されます。詳細については、コンソールの**Notifications**の下にある**View All**をクリックするか、コンソールメニューから**Notifications**を選択してください。

通知メニューが選択されたCitrix Cloudコンソール(/en-us/citrix-cloud/media/notifications-menu.png)

通知ページには、受信した通知が表示されます。最新の通知がリストの一番上に表示されます。

新しい通知が表示された通知ページ(/en-us/citrix-cloud/media/notifications-page.png)

通知を閉じる

通知は管理者ごとに管理されます。通知を閉じると、Citrix Cloudでご自身の管理者IDの下で閉じられます。他の管理者は、あなたがすべての通知を閉じたとしても、引き続き自身の通知を表示および閉じることができます。

受信したすべての通知を閉じるには、ページの上部にある**Dismiss All**を選択します。

個々の通知を閉じるには、各通知を選択し、**Dismiss**を選択します。

個々の通知と「Dismiss」ボタンが強調表示された通知ページ(/en-us/citrix-cloud/media/notifications-page-selections.png)

メール通知の受信

サインインして通知を表示する代わりに、メールで通知を受信することを選択できます。デフォルトでは、メール通知はオフになっています。

Citrix Cloudアカウントへの管理者アクセス権を持たない他の関係者（組織のセキュリティチームや監査チームのメンバーなど）に対しても、メール通知を有効にできます。

メール通知を有効にすると、Citrix Cloudは通知ごとにメールを送信します。通知は可能な限り早く送信されます。それらは単一のメールにまとめられたり、後で送信するためにバッチ処理されたりすることはありません。

自分のメール通知を有効にするには

1. Citrix Cloud管理コンソールから、**アカウント設定**を選択します。

   アカウント設定(/en-us/citrix-cloud/media/acct-settings-menu.png)
2. **通知**を選択します。
3. **自分のメール通知**設定をオンにします。
4. **自分の通知設定を管理**の下で、受信したい通知の種類を選択します。デフォルトでは、重大な種類のみが選択されています。
5. **適用**をクリックして設定を保存します。

非管理者向けにメール通知を有効にするには

このセクションの手順を使用して、非管理者をメール通知の連絡先として追加します。既存の管理者を連絡先として追加しようとすると、Citrix Cloudはエラーを表示します。

1. Citrix Cloud管理コンソールから、**アカウント設定**をクリックします。
2. **通知**を選択します。
3. **連絡先管理**の下で、**連絡先の追加**を選択します。
4. 連絡先の名前、メールアドレス、および希望する言語を入力します。
5. **通知設定を管理**の下で、送信する通知の種類を選択します。
6. **Add contact** を選択して、連絡先情報を保存します。

通知設定を変更する

管理者として、**Manage my notification settings** のチェックボックスをオンまたはオフにすることで、受信する通知の種類を変更できます。通知を変更しても、他の管理者が受信する通知には影響しません。

管理者以外のユーザーが受信する通知を変更することもできます。

管理者以外のユーザーの通知を変更するには

1. Citrix Cloud管理コンソールから、**Account Settings** をクリックします。
2. **Notifications** を選択します。

3. **Contact management** で、管理する連絡先を見つけます。
4. 連絡先にポインタを合わせ、鉛筆アイコンを選択します。
5. **Manage notification settings** で、各通知タイプのチェックボックスをオンまたはオフにします。

連絡先のメールアドレスを変更するには、まずその連絡先を削除し、新しいメールアドレスで新しい連絡先として追加する必要があります。

メール通知を無効にする

管理者として、**My email notifications** 設定をオフにすることで、いつでも自分のメール通知を無効にできます。

管理者以外のユーザーは、すべての通知メールに表示される購読解除リンクをクリックすることで、通知の受信を停止できます。購読解除した連絡先は、**Contact management** セクションのテーブルで **Unsubscribed** 通知ステータスになります。

管理者以外のユーザーの通知を無効にするには、次のいずれかの操作を実行します。

- 連絡先の「**通知設定の管理**」ですべてのチェックボックスをオフにします。
- 「**連絡先管理**」の下にあるテーブルから連絡先を削除します。

管理者以外の連絡先を削除する

1. Citrix Cloud管理コンソールから、「**アカウント設定**」をクリックします。
2. 「**通知**」を選択します。
3. 「**連絡先管理**」で、管理したい連絡先を見つけます。
4. 連絡先にポインターを合わせ、ごみ箱アイコンを選択します。

Citrix Cloudは、テーブルから連絡先を削除します。

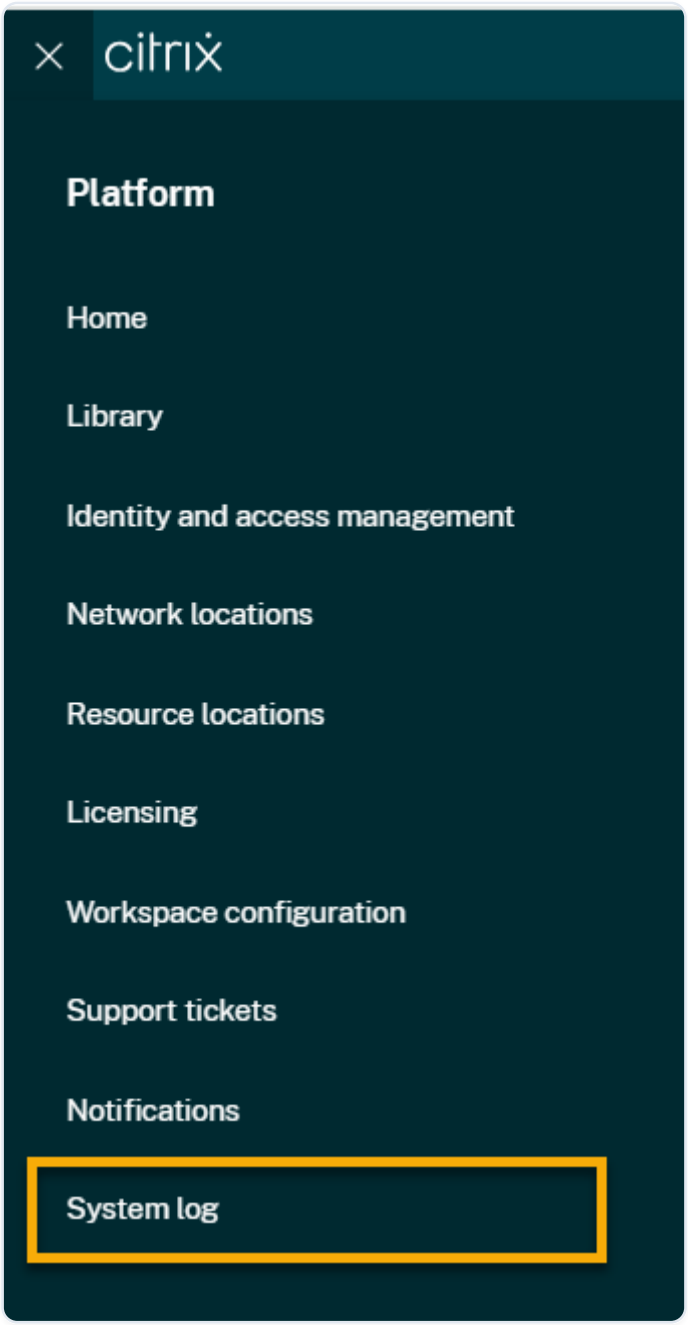
システムログ

システムログには、Citrix Cloud で発生したイベントのタイムスタンプ付きリストが表示されます。これには、構成の変更や、コネクタのアップグレードなどのその他のイベントが含まれます。これらの変更は、組織の規制コンプライアンス要件を満たすため、またはセキュリティ分析をサポートするために、CSVファイルとしてエクスポートできます。

> 注:

> DaaS Studio はログを別のログに書き込みます。詳細については、「構成ログ」を参照してください。

> システムログを表示するには、Citrix Cloud メニューから を選択します。

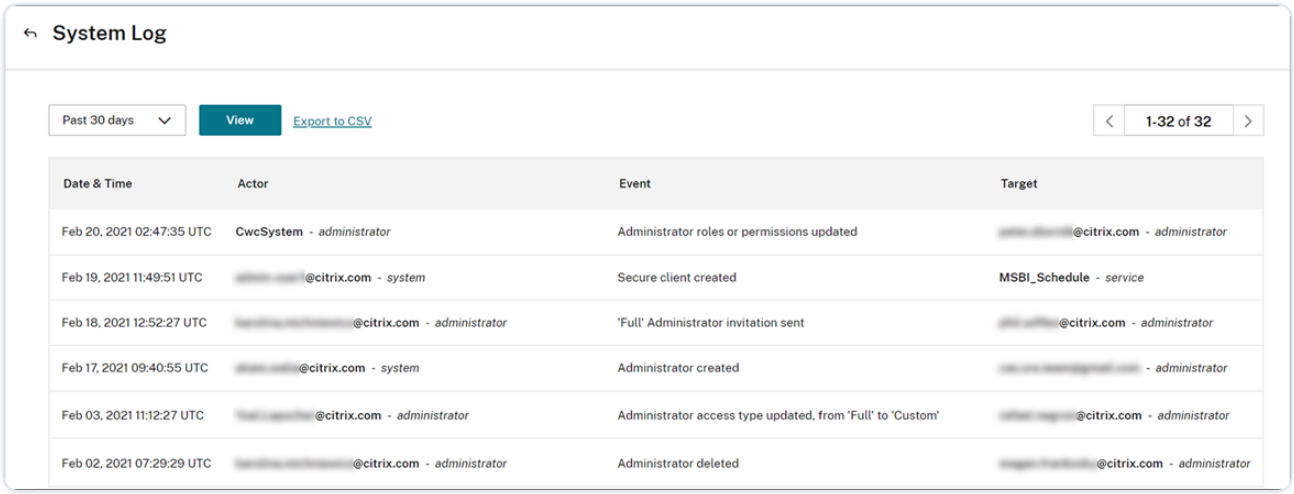


システムログにおけるデータの保持の詳細については、この記事の「データ保持」を参照してください。

ログイベント

システムログは、特定のCitrix Cloudプラットフォームおよびクラウドサービス操作のイベントをキャプチャします。これらのイベントとキャプチャされたデータの説明の完全なリストについては、「システムログイベントリファレンス」を参照してください。

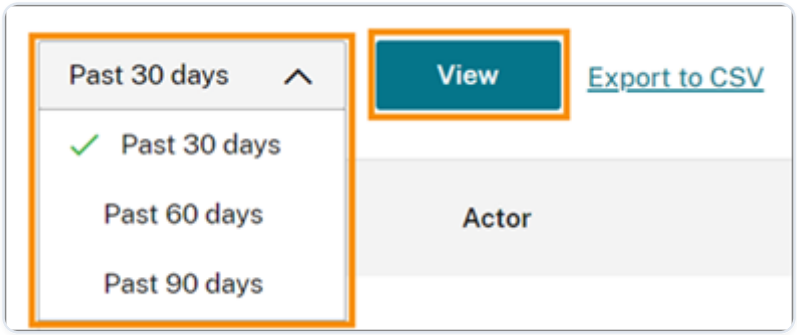
デフォルトでは、システムログには過去30日間に発生したイベントが表示されます。最新のイベントが最初に表示されます。



表示されるリストには、次の情報が含まれます。

- イベントが発生した日時 (UTC)。
- イベントを開始したアクター（管理者やサービスプリンシパルなど）。**CwcSystem** アクターのエントリは、Citrix Cloud が操作を実行したことを示します。
- イベントの簡単な説明（管理者の編集や新しいサービスプリンシパルの作成など）。
- イベントのターゲット。ターゲットとは、イベントの結果として影響を受けた、または変更されたシステムオブジェクトです。たとえば、管理者として追加されたユーザーなどです。

30日以上前のイベントを表示するには、表示したい期間を選択してリストをフィルターし、**「表示」**を選択します。最大90日前のイベントを表示できます。

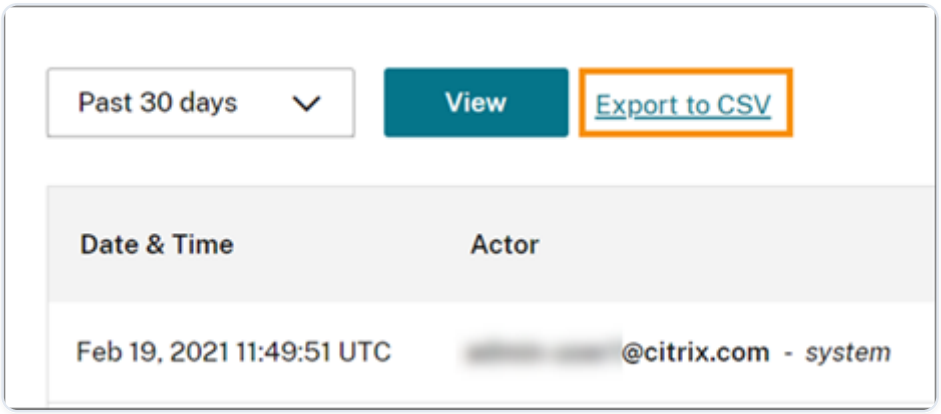


指定した期間に発生した古いイベントを取得するには、SystemLog APIを使用できます。詳細については、この記事の「特定の期間のイベントを取得する」を参照してください。

イベントのエクスポート

過去90日間に発生したシステムログイベントのCSVファイルをエクスポートできます。ダウンロードされるファイルの名前は、`SystemLog-CustomerName-OrgID-DateTimeStamp.csv`の形式に従います。

1. Citrix Cloudメニューから、**「システムログ」**を選択します。
2. 必要に応じて、イベントをエクスポートしたい期間を表示するようにリストをフィルターします。
3. **「CSVにエクスポート」**を選択し、ファイルを保存します。



CSVファイルには、次の情報が含まれています。

- 各イベントのUTCタイムスタンプ
- イベントを開始したアクターの詳細（名前とアクターIDを含む）。
- イベントの種類やイベントのテキストなどのイベント詳細
- イベントのターゲットの詳細（ターゲットID、管理者またはサービスプリンシパルの名前など）。

特定の期間のイベントを取得する

特定の期間のイベントを取得する必要がある場合は、SystemLog APIを使用します。

SystemLog API

SystemLog API を使用して、ログエントリを読み取り、別のシステムにエクスポートできます。API を使用する前に、Citrix Developer Docs Web サイトのGetting Startedで説明されているように、サービスプリンシパルを作成する必要があります。

SystemLog API の使用方法の詳細については、Citrix Developer Docs Web サイトのCitrix Cloud - SystemLogを参照してください。

Citrix DaaS ログについては、Citrix DaaS で構成操作を取得する方法を参照してください。

データ保持

Citrix は、Citrix Cloud がキャプチャするシステムログデータの保持について、お客様と責任を共有します。

Citrix® は、イベントが記録されてから 90 日間、システムログレコードを保持します。

お客様は、組織のコンプライアンス要件を満たすために保持したいシステムログレコードをダウンロードし、これらのレコードを長期ストレージソリューションに保存する責任があります。

システムログイベントリファレンス

Citrix Cloud™アカウントのすべてのシステムログイベントデータを表示するには、次のいずれかの方法を使用できます。

- 過去30日、60日、または90日間に発生したすべてのイベントのCSVファイルを(/ja-jp/citrix-cloud/citrix-cloud-management/system-log.html#export-events)ダウンロードする。
- SystemLog APIを使用して、(/ja-jp/citrix-cloud/citrix-cloud-management/system-log.html#retrieve-events-for-a-specific-time-period)特定の期間のイベントを取得します。

システムログイベントを取得する際にキャプチャされるデータの詳細については、この記事のイベントデータの説明を参照してください。イベントメッセージテキスト、イベントタイプ、およびイベント発生前後にオブジェクトフィールドデータが記録されるかどうかなどのイベント固有の値については、イベントを生成するクラウドコンポーネントとサービスを参照してください。

イベントを生成するクラウドコンポーネントとサービス

システムログは、以下のCitrix Cloudエンティティ、コンポーネント、およびサービスのイベントを記録します。

- Citrix Cloudプラットフォーム: 管理者の管理、Workspaceサブスクライバーのデバイスリセット、Microsoft Entra IDテナント、ドメインとネットワークロケーションの管理など、Citrix Cloudプラットフォーム機能に関連するイベント。
- コネクタ: Citrix Cloud ConnectorおよびConnector Applianceの登録と更新に関連するイベント。
- ライセンス: オンプレミスライセンスサーバーの登録、クラウドサービスに割り当てられたライセンスの管理、ライセンスデータのエクスポートに関連するイベント。
- Secure Private Accessサービス: Secure Private Accessサービスの設定に関連するイベント。

- Citrix Workspace: Workspace構成設定に関連するイベント。

イベントデータの説明

システムログイベントをダウンロードするか、SystemLog APIを使用して取得すると、以下のデータが含まれます。

- **RecordID:** イベントの一意の識別子。
- **UtcTimestamp:** イベントが発生した日付とUTC時刻。
- **CustomerID:** Citrix Cloudアカウントの一意の組織識別子。
- **EventType:** 記録されたイベントの種類の識別子。イベントの種類は`OriginatingService/Actor/Action`の形式で記録されます。たとえば、管理者を作成するためのイベントの種類は`platform/administrator/create`です。
- **TargetID:** 影響を受けた、または変更されたシステムオブジェクトのID。
- **TargetDisplayName:** 影響を受けた、または変更されたシステムオブジェクトの表示名。たとえば、作成された管理者の名前など。
- **TargetEmail:** システムオブジェクトのメールアドレス。たとえば、作成された管理者のメールアドレスなど。
- **TargetUserID:** 影響を受けた、または変更されたシステムオブジェクトのユーザーID。たとえば、管理者を作成する場合、ターゲットユーザーIDは作成された管理者のユーザーIDです。
- **TargetType:** イベントのターゲットカテゴリ。
- **BeforeChanges** および **AfterChanges:** イベント発生前と発生後のオブジェクトフィールドの内容。一部のイベントでは、これらのオブジェクトフィールドには以下が含まれます。
  - CustomerID
  - ユーザープリンシパル
  - UserID
  - 管理者アクセスタイプ（CustomまたはFullなど）
  - CreatedDate
  - UpdatedDate
  - 表示名
- **AgentID:** イベントカテゴリ。
- **ActorID:** イベントを開始したシステムオブジェクトのID。たとえば、管理者の作成の場合、これは別のユーザーをCitrix Cloudアカウントに招待した管理者のオブジェクトIDです。

- **ActorDisplayName:** イベントを開始した人物またはエンティティの表示名。たとえば、別のユーザーをCitrix Cloudアカウントに招待した管理者の名前です。
- **ActorType:** イベントを生成したサービス。
- **EventMessage:** 発生したイベントの簡単な説明。

Citrix Cloud™ プラットフォームのSystem Logイベント

この記事では、Citrix Cloudプラットフォーム向けにSystem Logがキャプチャするイベントデータについて説明します。System Logイベントデータの詳細については、System Logイベントリファレンスを参照してください。

System Logの詳細については、System Logを参照してください。

Microsoft Entra ID テナント

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Microsoft Entra ID テナントが接続されました	platform/identityprovider/azuread/connect	サービス	管理者	はい	いいえ	
Microsoft Entra ID テナントが切断されました	platform/identityprovider/azuread/disconnect	サービス	管理者	はい	いいえ	
Microsoft Entra ID 認証ドメイン名が変更されました	platform/identityprovider/azuread/authdomain/	シーダブリューエス	Customer ID	いいえ	いいえ	

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
	updatename					
Microsoft Entra ID 認証ドメイン名の変更に失敗しました	platform/identityprovider/azuread/authdomain/updatenamefailed	シーダブリューエス	Customer ID	いいえ	いいえ	

Citrix Cloud管理者とサービスプリンシパル

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
管理者が作成されました	platform/administrator/create	管理者	システム	いいえ	はい
管理者招待が送信されました	platform/administrator/invite	管理者	管理者	いいえ	はい
管理者の役割または権限が更新されました	platform/administrator/update	管理者	管理者	はい	はい
管理者が削除されました	platform/administrator/delete	管理者	管理者	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
管理者グループが作成されました	platform/administratorgroup/create	管理者グループ	いいえ	はい	
管理者グループの役割または権限が更新されました	platform/administratorgroup/update	管理者グループ	はい	はい	
管理者グループが削除されました	platform/administratorgroup/delete	管理者グループ	管理者	はい	いいえ

Citrix Cloud サービスプリンシパル

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
サービスプリンシパルが作成されました	platform/serviceprincipal/create	サービスプリンシパル	管理者	該当なし	はい
サービスプリンシパルの作成に失敗しました	platform/serviceprincipal/createfailed	サービスプリンシパル	管理者	該当なし	該当なし
サービスプリンシパルのロールまたは権限が	platform/serviceprincipal/	サービスプリンシパル	管理者	はい	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
更新されました	updatepolicyset				
サービスプリンシパルの更新に失敗しました	platform/serviceprincipal/updatefailed	サービスプリンシパル	管理者	該当なし	該当なし
サービスプリンシパルが削除されました	platform/serviceprincipal/delete	サービスプリンシパル	管理者	はい	該当なし
サービスプリンシパルの削除に失敗しました	platform/serviceprincipal/deletefailed	サービスプリンシパル	管理者	n/a	n/a
サービスプリンシパルのシークレットがローテーションされました	platform/serviceprincipal/secretrotation	サービスプリンシパル	管理者	はい	はい
サービスプリンシパルのシークレットのローテーションに失敗しました	platform/serviceprincipal/secretrotationfailed	サービスプリンシパル	管理者	該当なし	該当なし
サービスプリンシパルのセカンダリシーク	platform/serviceprincipal/secondarys	サービスプリンシパル	管理者	はい	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
レットが削除されました	ecretdeletion				
サービスプリンシパルのセカンダリシークレットの削除に失敗しました	platform/serviceprincipal/secondarysecretdeletionfailed	サービスプリンシパル	管理者	該当なし	該当なし

Active Directory Plusトークンのデバイスリセット

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
サブスクライバーデバイスのトークンリセットが完了しました	platform/authenticationdevice/delete	サブスクライバー	管理者	いいえ	はい

ドメイン管理

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクタータイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ドメインが削除されました	platform/domain/remove	サービス	管理者	いいえ	いいえ

ネットワークの場所

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ネットワークロケーションが作成されました	sdwan/networklocation/create	作成されたネットワークロケーションのID	ネットワークロケーションを追加した管理者の名前	いいえ	はい
ネットワークロケーションが更新されました	sdwan/networklocation/edit	変更されたネットワークロケーションのID	ネットワークロケーションを変更した管理者の名前	はい	はい
ネットワークロケーションが削除されました	sdwan/networklocation/delete	削除されたネットワークロケーションのID	ネットワークロケーションを削除した管理者の名前	はい	いいえ

リソースロケーション

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
リソースロケーションが作成されました	platform/resourcelocation/create	作成されたリソースロケーションの名前	リソースロケーションを作成した管理者の名前	はい	はい
リソースロケーションが更新されました	platform/resourcelocation/update	変更されたリソースロケーションの名前	リソースロケーションを変更した	はい	はい

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
			管理者の名前		
リソースロケーションが削除されました	platform/resourcelocation/delete	削除されたリソースロケーションの名前	リソースロケーションを削除した管理者の名前	はい	はい

アカウント名とロゴの変更

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
管理者アカウント名が更新されました	platform/account/name/update	顧客	管理者	はい	はい
管理者アカウントのロゴが更新されました	platform/account/logo/update	顧客	管理者	いいえ	いいえ

コネクタのシステムログイベント

この記事では、Citrix Cloud Connector および Connector Appliance for Cloud Services のシステムログがキャプチャするイベントデータについて説明します。システムログイベントデータの詳細については、システムログイベントリファレンスを参照してください。

システムログの詳細については、システムログを参照してください。

コネクタの登録

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
コネクタが登録されました	platform/edgeserver/create	**クラウドコネクタ** または **コネクタアプライアンス**	コネクタを登録した管理者	はい	はい
コネクタが削除されました	platform/edgeserver/delete	**クラウドコネクタ** または **コネクタアプライアンス**	コネクタを削除した管理者	はい	はい

コネクタの更新

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
リソースロケーションのメンテナンスウィンドウが更新されました	platform/resourcelocation/maintenancewindow	変更されたリソースロケーションの名前	構成を変更した管理者	はい	はい
管理者によってトリガーされたコネクタのアップグレード	platform/edgeserver/manualupgrade	**クラウドコネクタ** または **コネクタアプライアンス**	更新を開始した管理者	いいえ	いいえ

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
コネクタのアップグレードが開始されました	platform/edgeserver/upgradestarted	**クラウドコネクタ** または **コネクタアプライアンス**	**自動** または更新を開始した管理者	はい	いいえ
コネクタのアップグレードが完了しました	platform/edgeserver/upgradecompleted	**クラウドコネクタ** または **コネクタアプライアンス**	**自動**または更新を開始した管理者	いいえ	はい

コネクタの公開キー

イベントメッセージ	イベントタイプ	ターゲットID	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
信頼に追加された公開キー	platform/authentication/createedgeserverkey	操作を実行した管理者	いいえ	いいえ	
信頼から削除された公開キー	platform/authentication/deleteedgeserverkey	操作を実行した管理者	いいえ	いいえ	

Citrix Cloud™におけるライセンス供与のシステムログイベント

この記事では、オンプレミスCitrix LicensingのCitrix Cloudへの登録に関して、システムログがキャプチャするイベントデータについて説明します。システムログイベントデータの詳細については、「システムログイベントリファレンス」を参照してください。

システムログの詳細については、「システムログ」を参照してください。

オンプレミスライセンスサーバー

イベントメッセージ	イベントの種類	ターゲットの種類	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
オンプレミスライセンスサーバーが削除されました	lui/onpremlicenseservers/delete	ライセンス	ライセンスサーバーを削除した管理者	いいえ	なし
オンプレミスライセンスサーバーの削除に失敗しました	lui/onpremlicenseservers/deletefailed	ライセンス	ライセンスサーバーの削除を試みた管理者	なし	なし

クラウドサービスライセンス

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Citrix Cloud サービスライセンスがリリースされました	lui/cloudlicense/release	CloudLicense	クラウドサービスのライセンスをリリースした管理者	いいえ	いいえ
Citrix Cloud サービスライセンスのリリースに失敗しました	lui/cloudlicense/releasefailed	CloudLicense	クラウドサービスのライセンスをリリースしようとした管理者	いいえ	いいえ

Citrix Service Provider向けライセンス使用状況インサイト

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
パートナーのオンプレミスユーザーリストデータがエクスポートされました	lui/csp/userlistdataexport	ライセンス	パートナーユーザーリストデータをエクスポートした管理者	いいえ	いいえ
パートナーのオンプレミスユーザーリストデータのエクスポートに失敗しました	lui/csp/userlistdataexportfailed	ライセンス	パートナーユーザーリストデータのエクスポートを試みた管理者	いいえ	いいえ

クラウドサービスおよびオンプレミス製品のライセンス使用状況

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ライセンス使用状況データがエクスポートされました	lui/cloudlicense/usagedataexport	CloudLicense または Licensing	ライセンス使用状況データをエクスポートした管理者	いいえ	いいえ
ライセンス使用状況データのエクスポート	lui/cloudlicense/usagedataexportfailed	CloudLicense または Licensing	ライセンス使用状況データをエクスポート	いいえ	いいえ

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
に失敗しました			しようとした管理者		

Secure Private Access のシステムログイベント

この記事では、Secure Private Access サービス用にシステムログがキャプチャするイベントデータについて説明します。システムログイベントデータの詳細については、「システムログイベントリファレンス」を参照してください。

システムログの詳細については、「システムログ」を参照してください。

WebアプリケーションとSaaSアプリケーション

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Web/SaaSアプリケーションが作成されました	swa/websaaspplication/create	ウェブSaaSアプリケーション	いいえ	はい
Web/SaaSアプリケーションが更新されました	swa/websaaspplication/update	ウェブSaaSアプリケーション	はい	はい
Web/SaaSアプリケーションが削除されました	swa/websaaspplication/delete	ウェブSaaSアプリケーション	はい	いいえ
Web/SaaSアプリケーションの作成に失敗しました	swa/websaaspplication/createfailed	ウェブSaaSアプリケーション	いいえ	いいえ
Web/SaaSアプリケーションの	swa/websaaspplication/updatefailed	ウェブサースアプリケーション	はい	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
更新に失敗しました				
Web/SaaSアプリケーションの削除に失敗しました	swa/websaasppplication/deletefailed	ウェブサースアプリケーション	はい	はい

ユーザーとグループのサブスクリプション

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ユーザー/グループのサブスクリプションが追加されました	swa/websaasppplicationsubscribers/subscribe	ウェブサースアプリケーションサブスクライバー	いいえ	はい
ユーザー/グループのサブスクリプションが削除されました	swa/websaasppplicationsubscribers/unsubscribe	ウェブサースアプリケーションサブスクライバー	いいえ	はい
ユーザー/グループのサブスクリプションに失敗しました	swa/websaasppplicationsubscribers/subscribefailed	ウェブサースアプリケーションサブスクライバー	いいえ	いいえ
ユーザー/グループの登録解除に失敗しました	swa/websaasppplicationsubscribers/unsubscribefailed	ウェブSaaSアプリケーション購読者	いいえ	いいえ

コンテキストポリシー

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
コンテキストポリシーが作成されました	swa/contextualpolicy/create	コンテキストポリシー	いいえ	はい
コンテキストポリシーが更新されました	swa/contextualpolicy/update	コンテキストポリシー	はい	はい
コンテキストポリシーが削除されました	swa/contextualpolicy/delete	コンテキストポリシー	はい	いいえ
コンテキストポリシーの作成に失敗しました	swa/contextualpolicy/createfailed	コンテキストポリシー	いいえ	いいえ
コンテキストポリシーの更新に失敗しました	swa/contextualpolicy/updatefailed	コンテキストポリシー	いいえ	いいえ
コンテキストポリシーの削除に失敗しました	swa/contextualpolicy/deletefailed	コンテキストポリシー	はい	いいえ

アプリケーションドメイン

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
アプリケーションドメインが作成されました	swa/applicationdomain/create	アプリケーションドメイン	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
アプリケーションドメインが更新されました	swa/applicationdomain/update	アプリケーションドメイン	はい	はい
アプリケーションドメインが削除されました	swa/applicationdomain/delete	アプリケーションドメイン	はい	いいえ
アプリケーションドメインの作成に失敗しました	swa/applicationdomain/createfailed	アプリケーションドメイン	いいえ	いいえ
アプリケーションドメインの更新に失敗しました	swa/applicationdomain/updatefailed	アプリケーションドメイン	はい	いいえ
アプリケーションドメインの削除に失敗しました	swa/applicationdomain/deletefailed	アプリケーションドメイン	はい	いいえ

ブラウザ拡張機能の設定

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ブラウザ拡張機能の設定が更新されました	swa/browserextensionsettings/update	ブラウザ拡張機能設定	はい	はい
ブラウザ拡張機能の設定の更新に失敗しました	swa/browserextensi	ブラウザ拡張機能設定	はい	いいえ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
	onsettings/updatefailed			

WebサイトURLリストとフィルターカテゴリ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
有効なWebサイトフィルターリストとカテゴリ	swa/website/filterlistsenabledfiltercategoriesenabled/update	ウェブサイトURLリストカテゴリ機能	はい	はい
有効なWebサイトフィルターリストと無効なフィルターカテゴリ	swa/website/filterlistsenabledfiltercategoriesdisabled/update	ウェブサイトURLリストカテゴリ機能	はい	はい
Webサイトのフィルターリストを無効にし、フィルターカテゴリを有効にしました	swa/website/filterlistsdisabledfiltercategoriesenabled/update	ウェブサイトURLリストカテゴリ機能	はい	はい
Webサイトのフィルターリストとカテゴリを無効にしました	swa/website/filterlistsdisabledfiltercategoriesdisabled/update	ウェブサイトURLリストカテゴリ機能	はい	はい
Webサイトのフィルターリストとカテゴリを有効にできませんでした	swa/website/filterlistsenabledfiltercategoriesenabled/updatefailed	ウェブサイトURLリストカテゴリ機能	はい	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ウェブサイトフィルターリストの有効化とフィルターカテゴリの無効化に失敗しました	swa/website/filterlistsenabledfiltercategoriesdisabled/updatefailed	ウェブサイトURLリストカテゴリ機能	はい	はい
ウェブサイトフィルターリストの無効化とフィルターカテゴリの有効化に失敗しました	swa/website/filterlistsdisabledfiltercategoriesenabled/updatefailed	ウェブサイトURLリストカテゴリ機能	はい	はい
ウェブサイトフィルターリストとカテゴリの無効化に失敗しました	swa/website/filterlistsdisabledfiltercategoriesdisabled/updatefailed	ウェブサイトURLリストカテゴリ機能	はい	はい
WebサイトURLリストが作成されました	swa/websiteurlfilteringlist/create	ウェブサイトURLフィルタリングリスト	いいえ	はい
WebサイトURLリストが更新されました	swa/websiteurlfilteringlist/update	ウェブサイトURLフィルタリングリスト	はい	はい
WebサイトURLリストが削除されました	swa/websiteurlfilteringlist/delete	ウェブサイトURLフィルタリングリスト	はい	いいえ
ウェブサイトURLリストの作成に失敗しました	swa/websiteurlfilteringlist/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	いいえ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ウェブサイトURLリストの更新に失敗しました	swa/websiteurlfilteringlist/updatefailed	ウェブサイトURLフィルタリングリスト	はい	いいえ
ウェブサイトURLリストの削除に失敗しました	swa/websiteurlfilteringlist/deletefailed	ウェブサイトURLフィルタリングリスト	はい	いいえ
ウェブサイトURLフィルターカテゴリが作成されました	swa/websiteurlfiltercategory/create	ウェブサイトURLフィルターカテゴリ	いいえ	はい
ウェブサイトURLフィルターカテゴリが更新されました	swa/websiteurlfiltercategory/update	ウェブサイトURLフィルターカテゴリ	はい	はい
ウェブサイトURLフィルターカテゴリが削除されました	swa/websiteurlfiltercategory/delete	ウェブサイトURLフィルターカテゴリ	いいえ	いいえ
ウェブサイトURLフィルターカテゴリの作成に失敗しました	swa/websiteurlfiltercategory/createfailed	ウェブサイトURLフィルターカテゴリ	いいえ	いいえ
ウェブサイトURLフィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/updatefailed	ウェブサイトURLフィルターカテゴリ	はい	いいえ
ウェブサイトURLフィルター	swa/websiteurlfilterc	ウェブサイトURLフィルターカテゴリ	はい	いいえ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
カテゴリの削除に失敗しました	ategory/deletefailed			

Webサイトフィルターカテゴリのプリセット

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
更新されたWebサイトフィルターカテゴリプリセット	swa/websiteurlfiltercategorypreset/update	ウェブサイトURLフィルターカテゴリプリセット	はい	はい
ウェブサイトフィルターカテゴリプリセットの更新に失敗しました	swa/websiteurlfiltercategorypreset/updatefailed	ウェブサイトURLフィルターカテゴリプリセット	はい	はい

ブロックされたウェブサイトURLリストとフィルターカテゴリ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ブロックされたウェブサイトURLリストが作成されました	swa/websiteurlfilteringlist/blocked/create	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLリストが更新されました	swa/websiteurlfilteringlist/blocked/update	ウェブサイトURLフィルタリングリスト	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ブロックされたWebサイトURLリストが削除されました	swa/websiteurlfilteringlist/blocked/delete	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLリストの作成に失敗しました	swa/websiteurlfilteringlist/blocked/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLリストの更新に失敗しました	swa/websiteurlfilteringlist/blocked/updatefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLリストの削除に失敗しました	swa/websiteurlfilteringlist/blocked/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLフィルターカテゴリが作成されました	swa/websiteurlfiltercategory/blocked/create	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLフィルターカテゴリが更新されました	swa/websiteurlfiltercategory/blocked/update	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLフィルターカテゴリが削除されました	swa/websiteurlfiltercategory/blocked/delete	ウェブサイトURLフィルタリングリスト	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ブロックされたWebサイトURLフィルターカテゴリの作成に失敗しました	swa/websiteurlfiltercategory/blocked/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLフィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/blocked/updatefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
ブロックされたWebサイトURLフィルターカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/blocked/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい

許可されたWebサイトURLリストとフィルターカテゴリ

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
許可されたWebサイトURLリストが作成されました	swa/websiteurlfilteringlist/allowed/create	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLリストが更新されました	swa/websiteurlfilteringlist/allowed/update	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLリス	swa/websiteurlfilteri	ウェブサイトURLフィルタリングリスト	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
トが削除されました	nglist/allowed/delete			
許可されたWebサイトURLリストの作成に失敗しました	swa/websiteurlfilteringlist/allowed/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLリストの更新に失敗しました	swa/websiteurlfilteringlist/allowed/updatefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLリストの削除に失敗しました	swa/websiteurlfilteringlist/allowed/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLフィルターカテゴリが作成されました	swa/websiteurlfiltercategory/allowed/create	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLフィルターカテゴリが更新されました	swa/websiteurlfiltercategory/allowed/update	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLフィルターカテゴリが削除されました	swa/websiteurlfiltercategory/allowed/delete	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLフィルターカテゴリ	swa/websiteurlfiltercategory/	ウェブサイトURLフィルタリングリスト	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
の作成に失敗しました	allowed/createfailed			
許可されたWebサイトURLフィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/allowed/updatefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい
許可されたWebサイトURLフィルターカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/allowed/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい

リモートブラウザ分離（旧Secure Browser）WebサイトURLリストとフィルタカテゴリにリダイレクトされました

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド	
Secure Browser WebサイトURLリストが作成されました	swa/websiteurlfilteringlist/redirected/create	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browser WebサイトURLリストが更新されました	swa/websiteurlfilteringlist/redirected/update	ウェブサイトURLフィルタリングリスト	いいえ	はい	

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド	
Secure Browser にリダイレクトされた Web サイト URL リストが削除されました	swa/websiteurlfilteringlist/redirected/delete	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browser にリダイレクトされた Web サイト URL リストの作成に失敗しました	swa/websiteurlfilteringlist/redirected/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browser にリダイレクトされた Web サイト URL リストの更新に失敗しました	swa/websiteurlfilteringlist/redirected/updatedfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browserにリダイレクトされた Webサイト URLリストの削除に失敗しました	swa/websiteurlfilteringlist/redirected/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド	
Secure Browserにリダイレクトされた Webサイト URLフィルターカテゴリが作成されました	swa/websiteurlfiltercategory/redirected/create	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browserにリダイレクトされた Webサイト URLフィルターカテゴリが更新されました	swa/websiteurlfiltercategory/redirected/update	ウェブサイトURLフィルタリングリスト	いいえ	はい	
「Secure Browser」にリダイレクトされたウェブサイトURLフィルターカテゴリが削除されました	swa/websiteurlfiltercategory/redirected/delete	ウェブサイトURLフィルタリングリスト	いいえ	はい	
「Secure Browser」にリダイレクトされたウェブサイトURLフィルターカテ	swa/websiteurlfiltercategory/redirected/createfailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	

イベントメッセージ	イベントタイプ	ターゲットタイプ	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド	
ゴリの作成に失敗しました					
「Secure Browser」にリダイレクトされたウェブサイトURLフィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/redirected/updatefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	
Secure Browser にリダイレクトされたWebサイトURLフィルタカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/redirected/deletefailed	ウェブサイトURLフィルタリングリスト	いいえ	はい	

Citrix® StoreFront Cloud のシステムログイベント

この記事では、システムログがStoreFront Cloud用にキャプチャするイベントデータについて説明します。システムログイベントデータの詳細については、「システムログイベントリファレンス」を参照してください。

システムログの詳細については、「システムログ」を参照してください。

ストアURL

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ワークスペースURLが更新されました	wxp/url/update	購読者	URLを更新した管理者	はい	はい
ワークスペースURLの更新に失敗しました	wxp/url/updatefailed	サブスクライバー	URLの更新を試みた管理者	はい	はい
ワークスペースURLが有効になりました	wxp/url/enable	サブスクライバー	ワークスペースURLのカスタマイズを有効にした管理者	いいえ	はい
ワークスペースURLの有効化に失敗しました	wxp/url/enablefailed	購読者	ワークスペースURLのカスタマイズを有効にしようとした管理者	いいえ	はい
ワークスペースURLが無効になりました	wxp/url/disable	購読者	ワークスペースURLのカスタマイズを無効にした管理者	いいえ	はい
ワークスペースURLの無効化に失敗しました	wxp/url/disablefailed	購読者	ワークスペースURLのカスタマイズを無効	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
			にしようとした管理者		

ストア認証

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ワークスペースIDプロバイダーが更新されました	wxp/identityprovider/update	サブスクライバー	ワークスペース認証方法を更新した管理者	はい	はい
ワークスペースIDプロバイダーの更新に失敗しました	wxp/identityprovider/updatefailed	サブスクライバー	ワークスペース認証方法の更新を試行した管理者	はい	はい

Citrix フェデレーション認証サービス

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ワークスペースの Federated Authentication Service (FAS) が有効	wxp/fas/enable	サブスクライバー	FASを有効にした管理者	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Workspace Federated Authentication Service (FAS) の有効化に失敗しました	wxp/fas/enablefailed	サブスクライバー	FASの有効化を試みた管理者	いいえ	はい
Workspace Federated Authentication Service (FAS) が無効になりました	wxp/fas/disable	サブスクライバー	FASを無効にした管理者	いいえ	はい
Workspace フェデレーション認証サービス (FAS) の無効化に失敗しました	wxp/fas/disablefailed	サブスクライバー	FAS の無効化を試みた管理者	いいえ	はい

お気に入り

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Workspace のお気に入りが有効になりました	wxp/favorites/enable	サブスクライバー	お気に入りを有効にした管理者	いいえ	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Workspaceのお気に入りの有効化に失敗しました	wxp/favorites/enablefailed	サブスクライバー	お気に入りを有効にしようとした管理者	いいえ	はい
Workspaceのお気に入りが無効になりました	wxp/favorites/disable	サブスクライバー	お気に入りを無効にした管理者	いいえ	はい
ワークスペースのお気に入りの無効化に失敗しました	wxp/favorites/disablefailed	サブスクライバー	お気に入りを無効にしようとした管理者	いいえ	はい

パスワードの変更

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
ワークスペースのパスワード変更オプションポリシーが更新されました	wxp/changepasswordoptions/updatepolicy	加入者	Citrix Workspace内でパスワード変更ポリシーを更新した管理者	はい	はい
Workspaceのパスワード変更オプションポリシーの更新	wxp/changepasswordoptions/	加入者	Citrix Workspace内でパスワード変更ポリシーの	はい	はい

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
に失敗しました	updatepolicy failed		更新を試みた管理者		
Workspaceのパスワード変更オプションが有効になりました	wxp/changepasswordoptions/enable	加入者	Citrix Workspace内でパスワード変更設定を有効にした管理者	いいえ	はい
Workspaceのパスワード変更オプションの有効化に失敗しました	wxp/changepasswordoptions/enablefailed	サブスクライバー	Citrix Workspace内でパスワード変更設定を有効にしようとした管理者	いいえ	はい
Workspaceのパスワード変更オプションが無効になりました	wxp/changepasswordoptions/disable	サブスクライバー	Citrix Workspace内でパスワード変更設定を無効にした管理者	いいえ	はい
Workspaceのパスワード変更オプションの無効化に失敗しました	wxp/changepasswordoptions/disablefailed	サブスクライバー	Citrix Workspace内でパスワード変更設定を無効にしようとした管理者	いいえ	はい

長期間有効なトークン

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
Workspaceの長期間有効なトークン構成が更新されました	wxp/longlivedtoken/update	サブスクライバー	トークン構成を更新した管理者	はい	はい
Workspaceの長期トークン構成の更新に失敗しました	wxp/longlivedtoken/updatefailed	サブスクライバー	トークン構成の更新を試行した管理者	はい	はい

Webの非アクティブタイムアウト

イベントメッセージ	イベントの種類	ターゲットの種類	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新済みオブジェクトフィールド
Workspaceセッション構成が更新されました	wxp/sessions/update	サブスクライバー	Web設定の非アクティブタイムアウトのアイドル時間を更新した管理者	はい	はい
Workspaceセッション構成の更新に失敗しました	wxp/sessions/updatefailed	サブスクライバー	Web設定の非アクティブタイムアウトのアイドル時間を更新しよう	はい	はい

イベントメッセージ	イベントの種類	ターゲットの種類	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新済みオブジェクトフィールド
			とした管理者		

機能の展開

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
インテリジェントなWorkspaceエクスペリエンスのために更新された割り当て済みユーザーとグループ	wxp/iws/features/updateusersgroups	サブスクライバー	Citrix Workspaceでアクティビティフィード通知にアクセスするために、割り当てられたユーザーとグループを更新した管理者	いいえ	いいえ
インテリジェントなWorkspaceエクスペリエンスのために更新されたユーザーとグループの割り当てに失敗しました	wxp/iws/features/updateusersgroupsfailed	サブスクライバー	Citrix Workspaceでアクティビティフィード通知にアクセスするために、割り当てられたユーザーとグループの	いいえ	いいえ

イベントメッセージ	イベントタイプ	ターゲットタイプ	アクターID	イベント前に記録された現在のオブジェクトフィールド	イベント後に記録された更新されたオブジェクトフィールド
			更新を試みた管理者		
インテリジェントワークスペースエクスペリエンスが有効になりました	wxp/iws/features/enable	サブスクライバー	Citrix Workspaceでアクティビティフィード通知を有効にした管理者	いいえ	いいえ
インテリジェントワークスペースエクスペリエンスの有効化に失敗しました	wxp/iws/features/enablefailed	サブスクライバー	Citrix Workspaceでアクティビティフィード通知を有効にしようとした管理者	いいえ	いいえ
インテリジェントワークスペースエクスペリエンスが無効になりました	wxp/iws/features/disable	サブスクライバー	Citrix Workspaceでアクティビティフィード通知を無効にした管理者	いいえ	いいえ
インテリジェントなWorkspaceエクスペリエンスの無効化に失敗しました	wxp/iws/features/disablefailed	サブスクライバー	Citrix Workspaceでアクティビティフィード通知を無効にしようとした管理者	いいえ	いいえ

エスディーケーとエーピーアイ

Citrix Cloud™ は、情報の取得や、複雑で反復的なタスクの自動化に使用できるいくつかのAPIを提供しています。これには以下が含まれます。

- Citrix Cloud Connector™ をサイレントインストールする
- クラウドライセンス管理のためのレポートを作成および利用する
- 顧客の資格ステータスを判断する
- Citrix Cloud 管理者に通知を送信する
- システムログイベントを取得する
- 他のAPIで使用するリソースロケーションの詳細を取得する

いくつかのCitrix Cloudサービスも、情報の取得、データのクエリ、管理タスクの実行を可能にするSDKとAPIを提供しています。

APIには、セキュアクライアントまたはサービスプリンシパルの両方を通じてアクセスできます。

サービスプリンシパル

Citrix Cloud APIを使用するには、お客様に代わってCitrix Cloudにアクセスするサービスプリンシパルを作成する必要があります。サービスプリンシパルを作成するには、Citrix Cloudアカウントの顧客IDを提供する必要があります。顧客IDは、管理コンソールの以下の場所にあります。

- コンソールの右上隅、ユーザー名の下。

  顧客IDが強調表示されたユーザーメニュー(/en-us/citrix-cloud/media/customer-id-user-menu.png)
- あなたの**アカウント設定**ページ。

  アカウント設定が強調表示された顧客メニュー(/en-us/citrix-cloud/media/customer-id-acct-settings-page.png)
- **APIアクセス**ページ。

  APIアクセスの例(/en-us/citrix-cloud/media/api-access-example.png)

クラウドライセンスAPI

エンタープライズのお客様は、クラウドライセンスAPIを使用して、使用状況データのエクスポートや割り当て済みライセンスの解放などの管理タスクを実行できます。Citrixパートナーは、これらのAPIを使用して、オンプレミスのCitrix Virtual Apps and Desktops™およびCitrix DaaSの概要データと履歴データを取得できます。

詳細については、Citrix Developerドキュメントの「Citrixクラウドライセンスを管理するためのAPI」を参照してください。

SystemLog API

SystemLog APIを使用すると、指定した期間にCitrix Cloudアカウントで発生したイベントを取得できます。このAPIの使用方法の詳細については、Citrix Developerドキュメントの「Citrix Cloud - SystemLog」を参照してください。

リソースロケーションAPI

リソースロケーションAPIを使用すると、他のアプリケーションやスクリプトで使用するために、リソースロケーションに関する情報を取得できます。たとえば、Citrix Cloudアカウント内の複数のリソースロケーションのいずれかにCitrix Cloud Connectorをサイレントインストールしたいとします。このAPIを使用してリソースロケーションIDを取得し、インストールスクリプトに渡すことができます。

このAPIの使用方法の詳細については、Citrix Developerドキュメントの「Citrix Cloud - Resource Location」を参照してください。

サービスエンタイトルメントAPI

サービスエンタイトルメントAPIは、顧客が使用する権利のあるサービス、各エンタイトルメントの残り日数、および顧客が購入したエンタイトルメントの数量を取得します。このAPIの使用方法の詳細については、Citrix Developerドキュメントの「Citrix Cloud - Service Entitlement」を参照してください。

通知API

通知APIを使用すると、他のCitrix Cloud管理者へメッセージを送信できます。受信者は、管理コンソールの通知ページでメッセージを受信します。このAPIの使用方法の詳細については、「通知の作成と表示」を参照してください。

その他のサービス向けSDKとAPI

その他のCitrix Cloudサービスで利用可能なSDKとAPIの詳細については、以下の記事を参照してください。

- Citrix® StoreFront Cloud: StoreFront Cloud向けのSDKとAPIが含まれています。
- アプリ配信とセキュリティ: ConsoleやSD-WAN Orchestratorなどのネットワークおよびアプリ配信サービス向けのSDKとAPIが含まれています。

詳細情報

Citrix Cloud APIが、クラウドへの移行やプッシュトークンによる認証の構成といった複雑な操作をどのように支援できるかについては、以下のTech Zone記事を参照してください。

- 展開ガイド: VMware vSphereからMicrosoft Azure上のCitrix Virtual Apps and DesktopsサービスへのCitrix Virtual Apps and Desktopsの移行
- PoCガイド: 自動構成ツール

パートナー向けCitrix Cloud™

Citrix Cloudには、顧客とパートナーの両方のために設計されたサービス、機能、エクスペリエンスが含まれています。このセクションでは、CitrixパートナーがCitrix Cloudサービスとソリューションに関して顧客と共同作業を行うのに役立つ機能について説明します。

パートナーの識別

パートナーは、Citrix Organization ID (ORGID) に基づいてCitrix Cloudで識別されます。パートナーは、Citrix Cloud管理コンソールの次の場所で、Citrix Cloudアカウントに関連付けられているORGIDを表示できます。

- 顧客メニューから。コンソールの右上隅にある顧客名をクリックします。メニューに会社名の下にORGIDが表示されます。

  ORGIDが強調表示された顧客メニュー(/en-us/citrix-cloud/media/org-id-acct-name.png)

- 右上隅の顧客メニューから、**アカウント設定**を選択します。

  ORGIDが強調表示されたアカウント設定ページ(/en-us/citrix-cloud/media/acct-settings-page-org-id.png)

アカウントのORGIDがCitrixパートナープログラム（Citrix Solution AdvisorやCitrix Service Provider™など）のアクティブなメンバーである場合、プログラムバッジは、Citrixパートナーがこのアカウントを所有していることを示します。パートナーの識別は、追加のクラウドサービスまたは機能へのアクセスを管理するために使用されます。

Citrix Cloudコンソールのパートナーアカウント設定ページ(/en-us/citrix-cloud/media/partner-account-settings.png)

顧客ダッシュボード

マイ顧客ダッシュボードは、パートナーが複数のCitrix Cloud顧客のステータスを統合されたビューで表示できるように設計されています。顧客がダッシュボードに表示されるには、パートナーと顧客の間で接続が確立されている必要があります。マイ顧客ダッシュボードは、パートナーバッジ付きのCitrix Cloudアカウントで利用できます。

Citrix Cloudコンソールの顧客ダッシュボードページ(/en-us/citrix-cloud/media/partner-customer-dashboard-v2.png)

顧客ダッシュボードを表示できるユーザー?

デフォルトでは、フルアクセス管理者が顧客ダッシュボードを表示できます。**顧客ダッシュボード**権限が選択されている場合、カスタムアクセス管理者はダッシュボードを表示できます。Citrix Cloudの管理者権限の詳細については、「管理者権限の変更」を参照してください。

カテゴリと顧客ダッシュボードが強調表示されたカスタムアクセス管理者権限(/en-us/citrix-cloud/media/csp-customer-dashboard-permission-new.png)

顧客とのパートナー接続

Citrix Cloudソリューションで顧客と協力するパートナーは、アカウント間で信頼できるリンクを確立できます。このアカウントレベルの関係により、顧客は特定の情報をパートナーと簡単に共有できます。パートナーと接続することで、顧客はパートナーにCitrix Cloudアカウントに関する情報とCitrixとの関係への可視性を付与します。

パートナー接続を確立すると、次のことが可能になります。

- 顧客がパートナーのダッシュボードに表示される
- パートナーが顧客のアカウント設定でアクティブな接続として表示される
- パートナーはCitrix Cloudサービスの資格を可視化できる
- パートナーはCitrix Cloudの資格に対するライセンス使用状況とアクティブな使用状況を可視化できる

パートナーと顧客が接続すると、パートナー管理者は顧客の基本アカウント情報、顧客が発注した注文、およびサービス、ライセンス数、有効期限などの資格情報を表示できます。

顧客とのパートナー接続は期限切れになりません。

複数のパートナーまたは顧客との接続

パートナーは複数の顧客と接続を確立できます。あるいは、パートナーは管理する必要がなくなった顧客アカウントを削除することを検討してもよいでしょう。

顧客は複数のパートナーと接続を確立できます。顧客とパートナー間の接続数に制限はありません。

接続通知

Citrix Cloudは、次の場合にパートナーに通知を送信します。

- パートナーが顧客への接続を作成する
- 顧客がパートナーへの接続を終了する

パートナーが顧客との接続を終了すると、Citrix Cloud は顧客に通知を送信します。

サービスエンタイトルメントに対するパートナーの可視性

顧客に接続されている場合、パートナーはその顧客のサービスエンタイトルメントステータスを表示できます。この情報には、トライアルおよび非トライアルのエンタイトルメントの両方のステータスが含まれます。パートナーは以下の情報も表示できます。

- アクティブなサービスエンタイトルメント（顧客向けに購入またはその他の方法で付与または有効化されたサービス）
- エンタイトルメントのライセンス数と有効期限
- アクティブなサービス試用版
- 期限切れのサービス試用版

サービス] タブがあるパートナーダッシュボード(/en-us/citrix-cloud/media/partner-customer-services.png)

ライセンスの可視性は、ライセンス割り当てと過去の使用傾向の 概要 の表示に限定されます。

新しい顧客を追加する

新しい顧客を追加するには、次の手順に従います。

1. Citrix Cloud メニューから、 をクリックします。

   マイ顧客(/en-us/citrix-cloud/media/my-customers.png)
2. 「**顧客の管理 > クラウドテナント**」に移動し、「**顧客の追加**」をクリックします。

   顧客の管理(/en-us/citrix-cloud/media/manage-customers.png)
3. 次のスクリーンショットに示すように、以下のオプションから選択するよう求められます。

   招待または追加を選択(/en-us/citrix-cloud/media/select-add-or-invite.png)

> **注：**

- **顧客を招待**: このオプションを使用して、既存のシングルテナント顧客を招待します。招待された顧客は、独自のOrgIDを保持します。

顧客招待リンクの追加(/en-us/citrix-cloud/media/add-a-customer-invitation-link.png)

注：

- **顧客のオンボーディング**オプションは、シングルテナントおよびマルチテナントの顧客をオンボーディングする場合に適用されます。オンボーディングされた顧客は、パートナーと同じOrgIDを共有します。

顧客の追加(/en-us/citrix-cloud/media/add-a-customer.png)

4. **顧客を招待**フローを通じて追加された顧客は、シングルテナント顧客リストに表示されます。この招待された顧客は、独自のOrgIDを持っています。

   シングルテナント顧客を招待(/en-us/citrix-cloud/media/invite-single-tenant-customer.png)

5. **顧客のオンボーディング**フローを通じて追加された顧客は、クラウドテナント顧客リストに表示されます。このオンボーディングされた顧客は、パートナーと同じOrgIDを持っています。

   シングルテナント顧客を招待(/en-us/citrix-cloud/media/invite-cloud-tenant-customer.png)

追加された顧客のアクティブ化

クラウドテナントをマルチテナントDaaS顧客にする

1. **顧客の管理 > クラウドテナント**に移動し、**Citrix DaaS™の追加**をクリックして**DaaSサービス**を割り当てます。

   Citrix DaaSサービスの追加(/en-us/citrix-cloud/media/add-citrix-daas-service.png)

2. 顧客はマルチテナント顧客リストに表示されます。

   複数顧客リスト(/en-us/citrix-cloud/media/multi-customer-list.png)

クラウドテナントをシングルテナント顧客にする

1. **顧客の管理 > クラウドテナント**に移動し、**ライセンスの管理**をクリックして**ライセンスの割り当て**を選択します。

   シングル顧客としてのクラウドテナント(/en-us/citrix-cloud/media/cloud-tenant-as-single-customer.png)

2. 顧客はシングルテナント顧客リストに表示されます。

   シングルテナント顧客リスト(/en-us/citrix-cloud/media/single-tenant-customer-list.png)

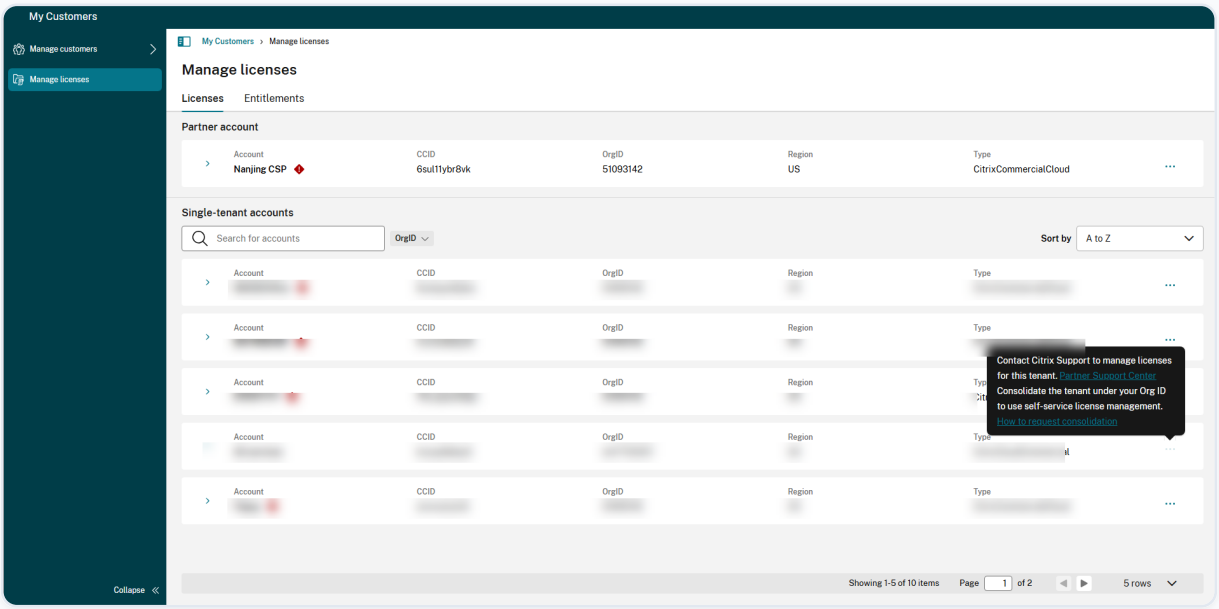
3. **ライセンスの管理 > ライセンス**タブから、「**割り当て**」または「**割り当て解除**」オプションのいずれかを選択してライセンスを更新できます。

   ライセンス割り当てオプション(/en-us/citrix-cloud/media/allocate-license-option.png)

   ライセンス割り当て解除オプション(/en-us/citrix-cloud/media/deallocate-license-option.png)

注:

顧客を招待オプションを通じて追加されたシングルテナント顧客は、独自のOrgIDを持っています。これらの顧客のライセンスを割り当てまたは割り当て解除するには、パートナーはCitrixカスタマーサービスに連絡する必要があります。CSPがシングルテナント顧客のライセンスをセルフサービスで管理（割り当てまたは割り当て解除）したい場合は、CTX695209に従って、CSPが所有するOrgIDの下にシングルテナント顧客を統合するためにCitrixにケースを提出する必要があります。UIのメッセージは、このプロセスについてパートナーに指示します。



顧客との接続を作成する

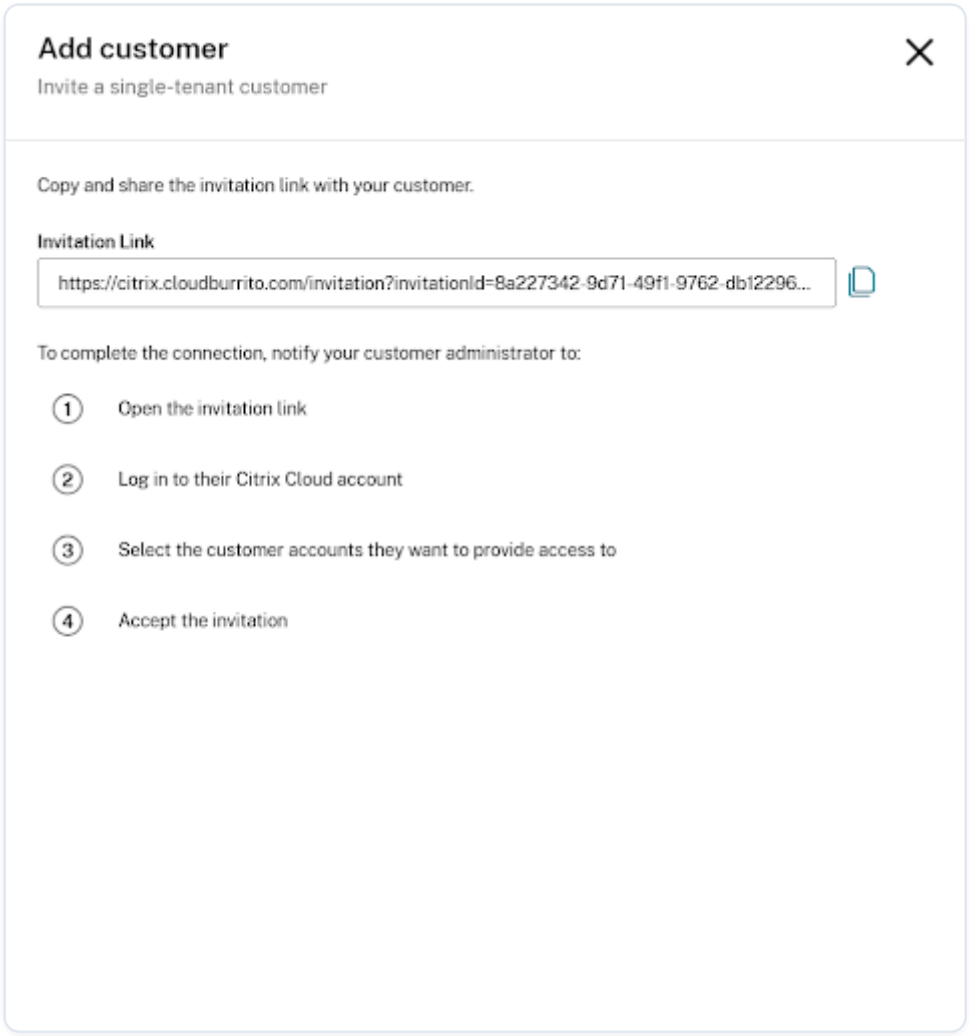
パートナーは、一意の招待リンクを使用して顧客との接続を作成します。このリンクは固定されており、変更またはカスタマイズすることはできません。

パートナーは、招待リンクを無制限に利用して接続を作成または再作成できます。招待リンクに有効期限はありません。

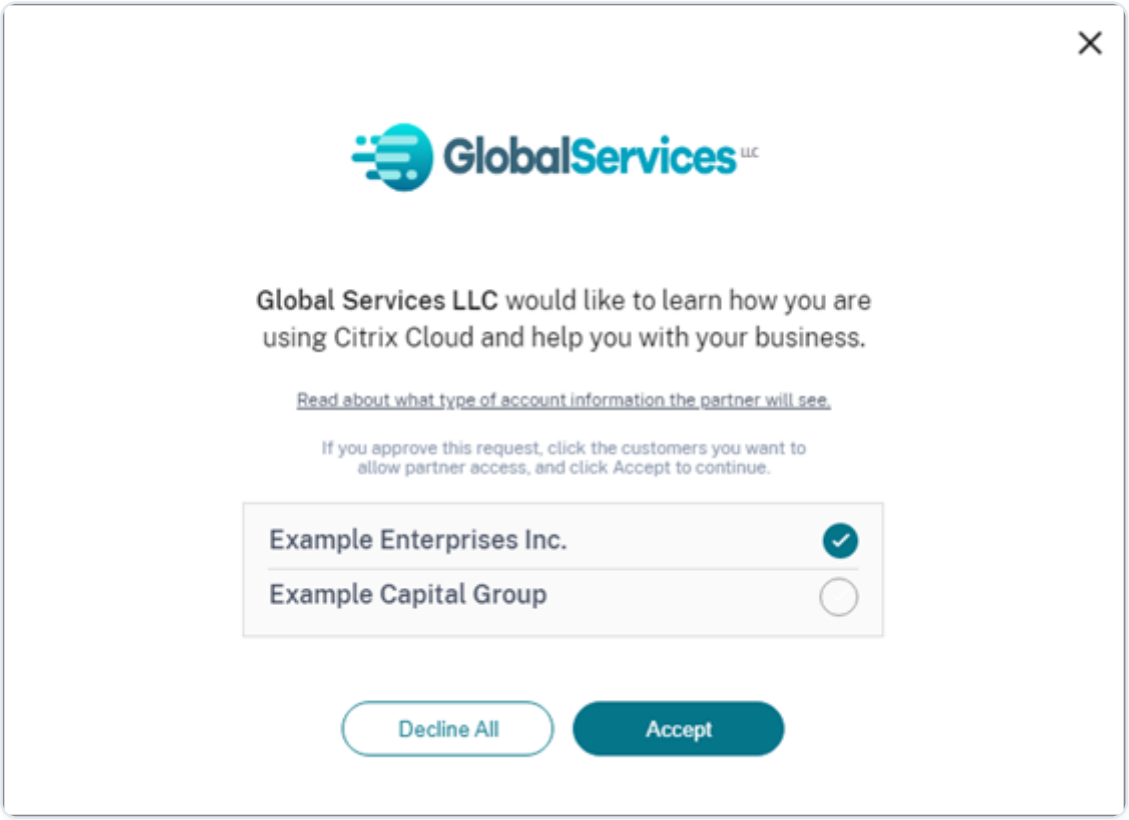
> **注:**
>
> このセクションで説明されている顧客の手動リンクは、既存の組織IDとそれに関連付けられたクラウドアカウントを既に持っているシングルテナント顧客をオンボーディングすることのみを目的としています。Citrix Cloud Commercialでは、パートナーは米国、EU、およびAPS地域の顧客と接続を作成できます。

接続を作成するには:

1. Citrix Cloudメニューから、 を選択します。
2. 顧客ダッシュボードのサイドバーから、 を選択します。
3. 既存のCitrix Cloud顧客と接続するには:
    a. を選択し、次に を選択します。
    b. 招待リンクをコピーして顧客に送信します。



接続を完了するには、顧客が招待リンクをクリックし、Citrix Cloudにサインインして、招待を承諾します。



4. Citrix Cloudアカウントをまだ持っていない新規顧客と接続するには：

   a. 「**顧客の追加**」を選択し、次に「**顧客のオンボーディング**」を選択します。

   b. 顧客のビジネス連絡先詳細を入力し、「**追加**」を選択します。Citrix Cloudが顧客の新しいアカウントを作成します。

   その後、顧客はパートナーが新しいアカウントの管理者として追加されたことを確認する通知を受け取ります。顧客は、Citrix Cloudサインインページの「パスワードを忘れた場合」リンクを使用して、アカウントのパスワードを設定できます。パスワードを設定した後、顧客はビジネスメールアドレスを使用してアカウントにサインインし、(/ja-jp/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html)に記載されているオンボーディングプロセスを完了できます。

パートナーまたは顧客の接続を削除する

パートナーまたは顧客のいずれかが、いつでも接続を終了できます。

顧客との接続を削除する

顧客との接続を終了するには、パートナーは次の手順を実行します。

1. コンソールの右上隅にあるCitrix Cloudメニューから、「**マイ顧客**」を選択します。
2. 顧客ダッシュボードから、管理したい顧客を見つけます。

3. 顧客の省略記号メニューをクリックし、「**顧客の削除**」を選択します。
4. 削除の確認を求められたら、「**削除**」を選択します。

パートナーとの接続を削除する

パートナーとの接続を終了するには、顧客は次の手順を実行します。

1. 左上隅のユーザーメニューから、「**アカウント設定**」を選択します。
2. 「**会社アカウント**」ページから、「**パートナー接続**」セクションを見つけます。
3. 管理するパートナーを見つけて、「**削除**」を選択します。
4. 削除の確認を求められたら、「**確認**」を選択します。

ライセンスの傾向

パートナーは、顧客ダッシュボードの詳細パネルで「**使用状況の表示**」をクリックすることで、顧客のライセンス情報を表示できます。

ライセンスメニューが選択された顧客ダッシュボード(/en-us/citrix-cloud/media/partner-customer-view-lic-usage-v2.png)

> **注：**

> Citrixパートナーは、ライセンス概要ビューと過去のアクティブな使用状況の傾向のみを表示できます。特定のサービスでライセンスを使用している個々のユーザーを表示することはできません。

> 各サービスの顧客のライセンス概要を表示するには、「**使用状況の表示**」タブをクリックします。詳細な使用状況情報を表示するには、表示したいサービスエンタイトルメントの「**使用状況の傾向を表示**」を選択します。

「使用状況の傾向を表示」が強調表示されたサービス概要(/en-us/citrix-cloud/media/partner-customer-lic-view-usage-trends.png)

サービスに応じて、使用状況の傾向には次の情報が含まれます。

- 割り当てられたライセンスと購入済みの合計ライセンスの比率
- 月間および日間のアクティブユーザー

- ライセンスの割り当て、アクティブな使用状況、エンタイトルメントごとの消費量、および超過使用量の視覚的な内訳。

使用状況の傾向を含む使用状況の概要(/en-us/citrix-cloud/media/partner-customer-active-use.png)

必要に応じて、パートナーはこの情報を.csvファイルとしてエクスポートできます。

帯域幅の使用状況

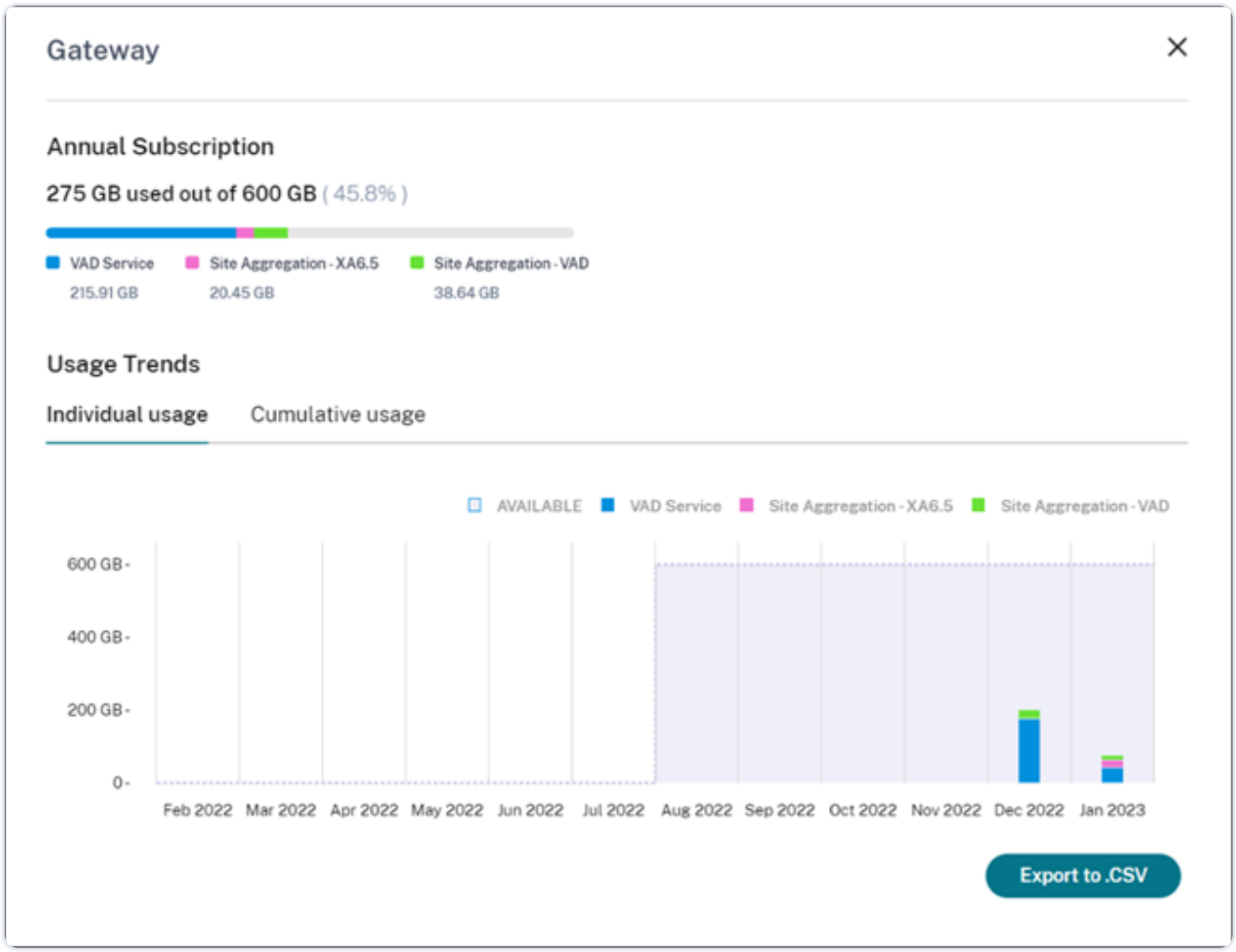
Citrix Gatewayサービスの場合、ライセンスの概要は以下の情報で構成されます。

- 顧客のすべてのエンタイトルメントにおける総帯域幅使用量。
- 顧客の月次、年次、および期間指定のエンタイトルメント別に分類された総帯域幅使用量。
- 今月の総超過使用量。超過使用量の計算方法の詳細については、「超過使用量」を参照してください。

エンタイトルメントの利用状況の概要を表示するには、ページの右端にある**使用状況トレンドの表示**を選択します。過去12か月間の超過使用量を表示するには、**超過使用量チャートの表示**を選択します。

エンタイトルメントに応じて、使用状況トレンドには以下の情報が含まれます。

- Citrix DaaS (**VADサービス**) およびサイト集約を使用したオンプレミスのVirtual Apps and Desktops展開における消費帯域幅の量。
- 帯域幅が使用された各月ごとの帯域幅使用量の視覚的な内訳。(月次エンタイトルメント)
- 請求期間の各月中に発生した帯域幅の**個別使用量**の視覚的な内訳。(年次および期間指定のエンタイトルメント)
- 請求期間の各月に蓄積された帯域幅の**累積使用量**の視覚的な内訳。(年次および期間指定のエンタイトルメント)



必要に応じて、パートナーはこの情報を.csvファイルとしてエクスポートできます。

Citrix Service Provider向けの顧客ライセンスと使用状況

Citrix Cloudのライセンス機能を使用すると、Citrix Service Provider (CSP) の顧客は、サポートされているCitrix DaaS (旧Citrix Virtual Apps and Desktops™) 製品のライセンスと使用状況を監視できます。CSPは、顧客のCitrix Cloudアカウントでサインインして、この情報を表示およびエクスポートすることもできます。詳細については、以下の記事を参照してください。

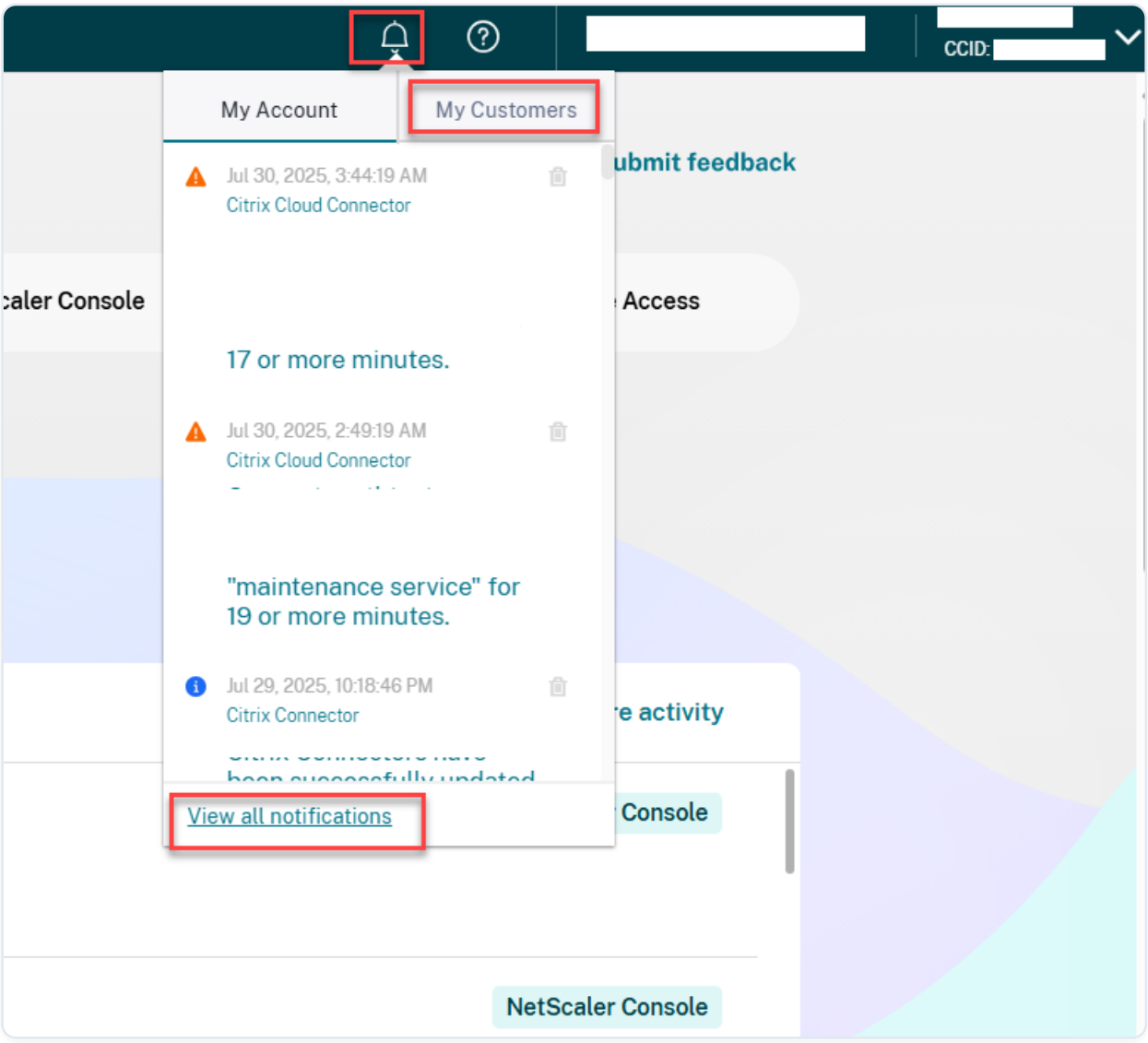
- Citrix DaaSの顧客ライセンスと使用状況の監視(/ja-jp/citrix-cloud/license-usage-insights/virtual-apps-desktops-service-licensing-citrix-service-providers.html)

パートナーによる顧客の通知の可視性

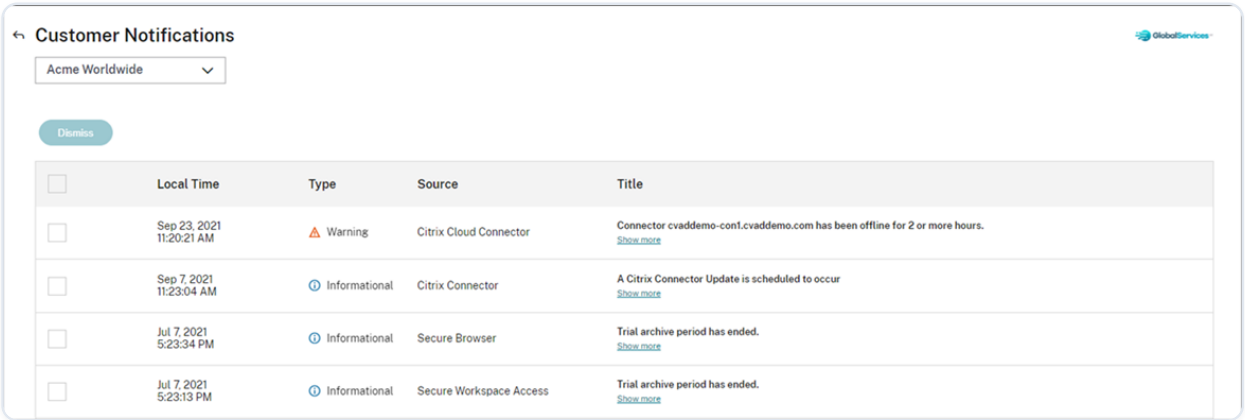
パートナーは、接続されている顧客の通知を表示できます。パートナーは、顧客固有の通知をフィルタリングし、通知を却下するなどのアクションを実行することもできます。却下された通知はパートナーには表示されません。ただし、顧客がCitrix Cloudにサインインすると、自分のアカウントで通知を引き続き表示できます。

顧客の通知を表示するには：

1. 管理コンソールの上部にあるベルのアイコンをクリックし、 を選択し、 を選択します。



2. ドロップダウンメニューから顧客を選択し、その顧客の通知を表示します。



Citrix Service Provider向けフェデレーションドメイン

フェデレーションドメイン を使用すると、顧客ユーザーはCSPリソースの場所に接続されたドメインの資格情報を使用してストアにサインインできます。これにより、*customer.cloud.com* のよ

うなカスタムストアURLを使用して、顧客ユーザーに専用ストアを提供できます。リソースの場所は、引き続きパートナーのCitrix Cloudアカウントにあります。顧客がCSPストアURL（例：csppartner.cloud.com）を使用してアクセスできる共有ストアと並行して、専用ストアを提供できます。顧客が専用ストアにアクセスできるようにするには、管理している適切なドメインに顧客を追加します。ストアを構成すると、顧客ユーザーはストアにサインインし、Citrix DaaSを通じて利用可能にしたアプリとデスクトップにアクセスできます。

フェデレーションドメインから顧客を削除すると、顧客のユーザーは、パートナーのドメインからの資格情報を使用してストアにアクセスできなくなります。

アプリとデスクトップを配信するためのフェデレーションドメインの使用について詳しくは、Citrix Service Provider向けCitrix DaaS を参照してください。

Citrix Service Provider向けストアの外観オプション

カスタムテーマを使用して、ストアの色とロゴを構成できます。カスタムテーマの作成方法については、ストアの外観をカスタマイズする を参照してください。

> **注**
>
> カスタムテーマはシングルテナント機能です。サービスプロバイダーテナントがリソースの場所、クラウドコネクタ、およびActive Directoryドメインを共有するCitrix Service Provider（マルチテナント）は、現在サポートされていません。独自の専用リソースの場所、クラウドコネクタ、および専用Active Directoryドメインを持つCitrix Service Providerテナント（シングルテナント）は完全にサポートされています。

クラウドサービス

この記事では、Citrix Cloud を通じて提供されるクラウドサービスと、各サービスの製品ドキュメントへのリンクを一覧表示します。これらのサービスとそれらが含まれる提供内容の説明については、「Citrix Services のサービス説明」を参照してください。

Citrix® サービス

アナリティクス

- セキュリティ向けアナリティクス
- パフォーマンス向けアナリティクス
- アナリティクス - 利用状況

シトリックス DaaS

シトリックス DaaS Standard for Azure

エンドポイント管理

ゲートウェイ

グローバルアプリ構成サービス

ServiceNow向けITSMアダプター

リモートブラウザ分離

セキュアプライベートアクセス

セッション記録サービス

仮想アプリ エッセンシャルズ

仮想デスクトップ エッセンシャルズ

ワークスペース環境管理

NetScaler® サービス

コンソール

アプリケーション配信とセキュリティ

SD-WANオーケストレーター

セキュアインターネットアクセス

Webアプリファイアウォール

Virtual Apps and Desktops Essentials

シトリックス バーチャルアプリ エッセンシャルズ™

注:

Citrix Virtual Apps EssentialsおよびCitrix Virtual Desktops Essentialsは、販売終了およびサポート終了となりました。詳細については、CTX583004を参照してください。

Citrix Virtual Apps™ Essentialsを使用すると、Microsoft AzureからWindowsアプリケーションと共有ホスト型デスクトップを、あらゆるデバイスのあらゆるユーザーに配信できます。このサービスは、業界をリードするCitrix Virtual Appsサービスと、Microsoft Azureのパワーおよび柔軟性を兼ね備えています。Virtual Apps Essentialsを使用して、Windows Serverデスクトップを公開することもできます。

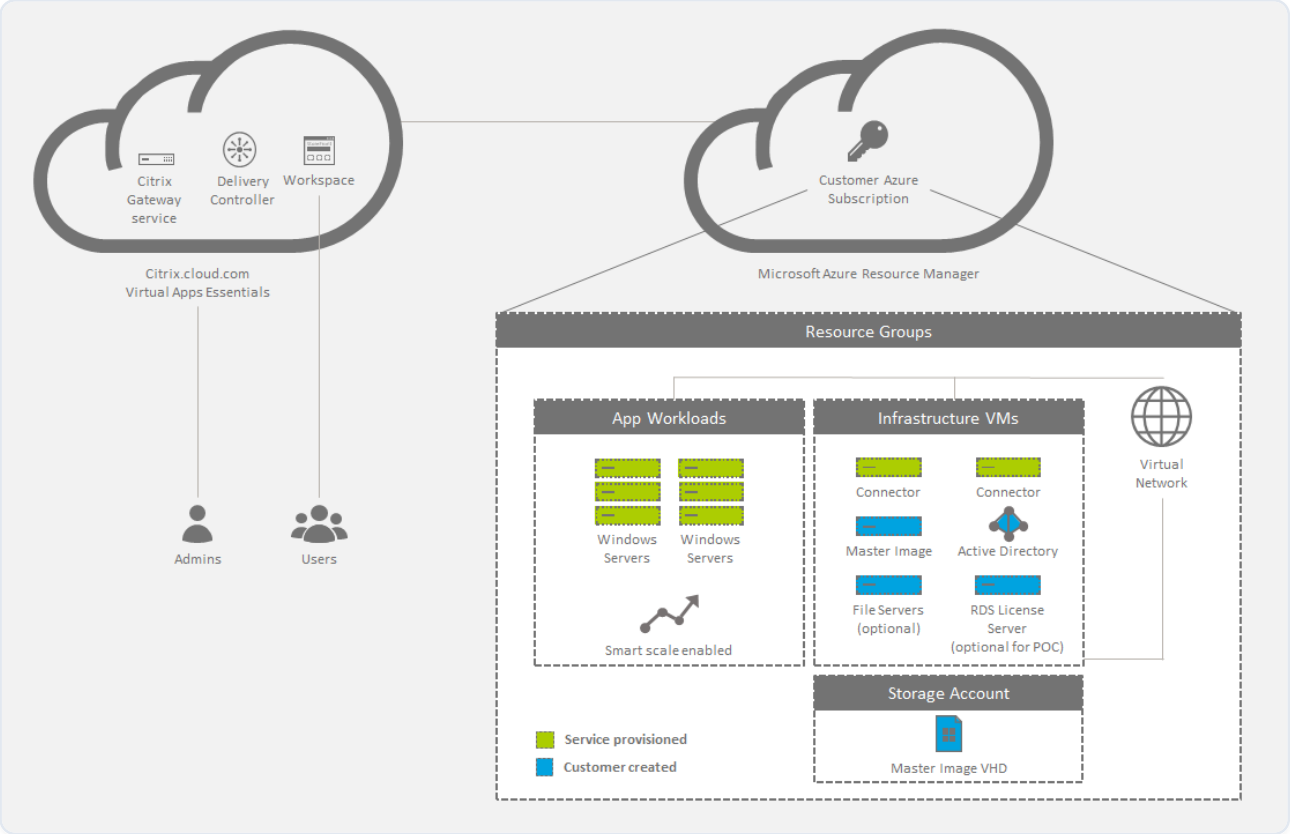
サーバーOSマシンは、1台のマシンから複数のセッションを実行し、複数のアプリケーションとデスクトップを、同時に接続された複数のユーザーに配信します。各ユーザーは、すべてのホスト型アプリケーションを実行できる1つのセッションを必要とします。

このサービスはCitrix Cloud™を通じて提供され、Azureサブスクリプション内にアプリケーションワークロードを簡単に展開するのに役立ちます。ユーザーがストアエクスペリエンスからアプリケーションを開くと、そのアプリケーションはユーザーのコンピューター上でローカルに実行されているように見えます。ユーザーは、あらゆるデバイスから、どこからでも安全にアプリにアクセスできます。

Virtual Apps Essentialsには、コア管理サービスに加えて、ストアエクスペリエンスとCitrix Gatewayサービスが含まれています。アプリワークロードはAzureサブスクリプションで実行されます。

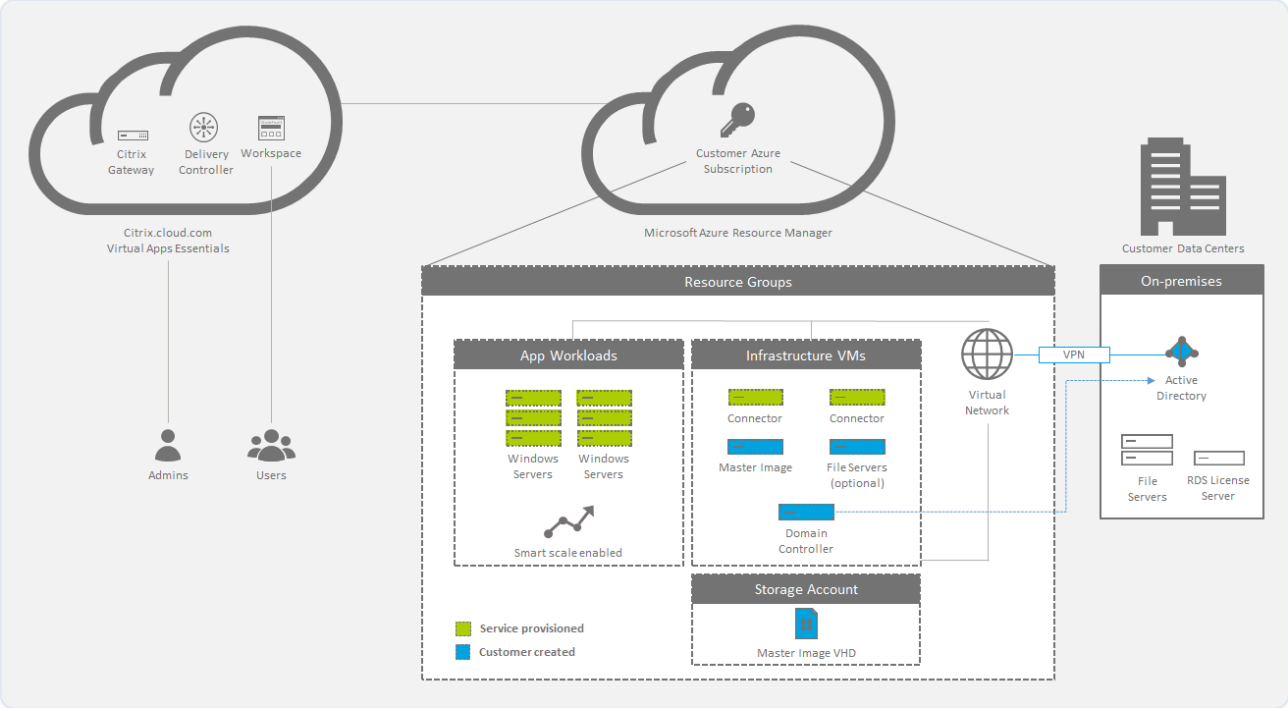
展開アーキテクチャ

次の図は、基本的なVirtual Apps Essentialsクラウド展開のアーキテクチャの概要を示しています。



ユーザーがオンプレミスデータセンターに接続できるようにすることもできます。Azureクラウドとオンプレミスデータセンター間の接続は、VPN接続を介して行われます。ユーザーはVirtual Apps Essentialsを介して、VPN接続経由でライセンスサーバー、ファイルサーバー、またはActive

Directoryに接続します。



展開の概要

Citrix Virtual Apps Essentialsを展開するには、次の手順に従います。

- アジュール マーケットプレイスからシトリックス バーチャルアプリ エッセンシャルズを購入する。
- Azureサブスクリプションを準備してリンクする。
- マスターイメージを作成してアップロードする。
- カタログを展開し、アプリとデスクトップを公開し、エンドユーザーを割り当てる

新機能

- 2018年12月: **クラウドホスト型StoreFront™が削除されました**

  クラウドホスト型StoreFrontは、Virtual Desktops Essentialsでは使用できなくなりました。2017年12月より前にVirtual Desktops Essentials（旧XenDesktop® Essentials）を購入されたお客様は、この記事で説明されているCitrix Workspaceを使用して、サブスクライバーにデスクトップへのアクセスを提供できます。

- 2018年8月: **新しい製品名**

  Citrix®のお客様またはパートナーとして長年ご利用いただいている方は、当社の製品および製品ドキュメントに新しい名前があることにお気づきでしょう。このCitrix製品を初めてご利用になる方は、製品またはコンポーネントに異なる名前が表示される場合があります。

新しい製品名とコンポーネント名は、Citrixの拡大するポートフォリオとクラウド戦略に由来しています。この記事では、以下の名前を使用します。

- **Citrix Virtual Apps Essentials:** XenApp®は、多くの種類のアプリが作業ツールにアクセスするための最適な場所に集まる、当社のストア戦略の一部です。統合されたコンテキスト対応のセキュアなストアの一部として、XenApp Essentialsは現在Citrix Virtual Apps Essentialsとなっています。
- **Citrix Workspace app:** Citrix Workspaceアプリは、既存のCitrix Receiver™テクノロジーとその他のCitrix Workspaceクライアントテクノロジーを統合しています。最高の仕事をするために必要なすべての作業アプリ、ファイル、デバイスとやり取りできる、統合されたコンテキスト対応のエクスペリエンスをエンドユーザーに提供するために、より多くの機能を提供するように強化されています。
- **Citrix Gateway:** 最高の仕事をするために必要なアプリとデータへのセキュアでコンテキスト対応のアクセスを可能にするNetScaler® Unified Gatewayは、現在Citrix Gatewayとなっています。

製品内のコンテンツには、以前の名前がまだ含まれている場合があります。たとえば、コンソールテキスト、メッセージ、ディレクトリ/ファイル名に以前の名前のインスタンスが表示されることがあります。一部の項目（コマンドやMSIなど）は、既存の顧客スクリプトを破損させないために、以前の名前を保持し続ける可能性があります。

関連する製品ドキュメント、その他のリソース（ビデオやブログ投稿など）、およびその他のサイト（Azure Marketplaceなど）には、以前の名前がまだ含まれている場合があります。この移行期間中の皆様のご理解に感謝いたします。新しい名前の詳細については、`<https://www.citrix.com/about/citrix-product-guide.html>`を参照してください。

- 2018年5月: **Virtual Apps Essentialsインターフェースからの追加イメージの構築**

  Azure Resource Managerインターフェースから本番イメージを作成した後、必要に応じてAzure経由で追加のイメージを作成できます。現在、Azureインターフェース経由で追加イメージを作成するオプションの代替として、Virtual Apps Essentialsインターフェースから新しいマスターイメージを構築できます。詳細については、マスターイメージの準備とアップロードを参照してください。

- 2018年5月: **モニター表示の機能強化**

  モニター表示に、アプリケーションと上位ユーザーに関する使用状況情報が含まれるようになりました。詳細については、「サービスの監視」を参照してください。

システム要件

マイクロソフト アジュール

Citrix Virtual Apps Essentialsは、Azure Resource Managerを介したマシンの構成のみをサポートしています。

Azure Resource Managerを使用して、次のことを行います。

- 仮想マシン（VM）、ストレージアカウント、仮想ネットワークなどのリソースを展開します。
- リソースグループ（グループとして管理するリソースのコンテナ）を作成および管理します。

Microsoft Azureでリソースをプロビジョニングおよび展開するには、次のものが必要です。

- Azureアカウント。
- Azure Resource Managerサブスクリプション。
- サブスクリプションに関連付けられているディレクトリ内のMicrosoft Entra IDグローバル管理者アカウント。リソースをプロビジョニングするために使用するAzureサブスクリプションに対して、ユーザーアカウントが所有者権限を持っている必要があります。Microsoft Entra IDテナントの設定方法の詳細については、「Microsoft Entra IDテナントの取得方法」を参照してください。

シトリックス クラウド

Virtual Apps EssentialsはCitrix Cloudを介して提供され、オンボーディングプロセスを完了するにはCitrix Cloudアカウントが必要です。トランザクションを完了するためにAzure Marketplaceにアクセスする前に、Citrix Cloudサインアップページでで Citrix Cloudアカウントを作成できます。

使用するCitrix Cloudアカウントは、既存のCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）またはCitrix Virtual Desktops Essentials™サービスアカウントと関連付けることはできません。

Virtual Apps Essentialsコンソール

Google Chrome ウェブブラウザで Virtual Apps Essentials 管理コンソールを開くことができます。

既知の問題

Virtual Apps Essentials には、以下の既知の問題があります。

- Windows Server 2019 VDA では、構成中およびユーザーのストアで一部のアプリケーションアイコンが正しく表示されない場合があります。回避策として、アプリが公開された後、**アイコンの変更**機能を使用して、正しく表示される別のアイコンを割り当ててください。
- Microsoft Entra ID Domain Services を使用している場合: ストアログオンUPNには、Microsoft Entra ID Domain Services を有効にしたときに指定されたドメイン名が含まれている必要があります。作成したカスタムドメインがプライマリとして指定されている場合でも、ログオンにそのカスタムドメインのUPNを使用することはできません。
- カタログのユーザーを構成し、ドメインを選択すると、Builtin\users グループのユーザーを表示して選択できます。
- 選択したリージョンで仮想マシンのサイズが利用できない場合、カタログの作成は失敗します。お住まいの地域で利用可能な仮想マシンを確認するには、Microsoft Web サイトの「Products available by region」のチャートを参照してください。
- スタートメニューから同じアプリの複数のインスタンスを同時に作成および公開することはできません。たとえば、スタートメニューから Internet Explorer を公開します。その後、起動時に特定のウェブサイトを開く Internet Explorer の2番目のインスタンスを公開したいとします。これを行うには、スタートメニューではなく、アプリのパスを使用して2番目のアプリを公開します。
- Virtual Apps Essentials は、Microsoft Entra ID ユーザーアカウントを使用したサブスクリプションのリンクをサポートしています。Virtual Apps Essentials は、Live.com 認証済みアカウントをサポートしていません。
- VDA上に既存のRemote Desktop Protocol (RDP) セッションがある場合、ユーザーはアプリケーションを開始できません。この動作は、他のユーザーがVDAにログオンしていないときにRDPセッションが開始された場合にのみ発生します。
- server.domain.subdomain よりも長いライセンスサーバーアドレスは入力できません。
- キャパシティ管理に対して複数の連続した更新を実行すると、更新された設定がVDAに適切に伝播されない可能性があります。
- 英語以外のウェブブラウザを使用している場合、テキストは英語とブラウザの言語の組み合わせで表示されます。

サービスの購入方法

> **注:**

> このセクションの情報は、PDF としても入手できます。そのコンテンツには、以前の製品名が含まれています。

> Citrix Virtual Apps Essentials は、Microsoft Azure アカウントを使用して、Azure Marketplace から直接購入できます。Citrix Virtual Apps Essentials には、最低 25 ユーザーが必要です。

このサービスは Citrix Cloud を介して提供され、オンボーディングプロセスを完了するには Citrix Cloud アカウントが必要です。詳細については、システム要件 > Citrix Cloud を参照してください。

Citrix Virtual Apps Essentials を購入する際は、注文を迅速に処理するために、住所フィールドを含むすべての詳細に正しい情報を入力してください。Virtual Apps Essentials を構成する前に、Azure Marketplace で以下を完了していることを確認してください。

- 連絡先情報と会社情報を提供します。
- 請求情報を提供します。
- サブスクリプションを作成します。

顧客と価格を設定するには：

1. で、顧客名を選択します。
2. の で、Virtual Apps Essentials にアクセスできるユーザー数を入力します。
3. で、同意チェックボックスを選択し、 をクリックします。

概要ページが表示され、リソースの詳細が表示されます。

アカウントがプロビジョニングされたら、 をクリックします。

> **重要：**

> Microsoft Azure がサービスをプロビジョニングするまでお待ちください。プロビジョニングが完了するまで、 リンクをクリックしないでください。このプロセスには最大 4 時間かかる場合があります。

> リンクをクリックすると、Citrix CloudがWebブラウザで開き、以下に説明する構成プロセスを開始できます。

Azureサブスクリプションを準備する

VDAsおよび関連リソースのホスト接続として使用するAzureサブスクリプションを選択します。これらのリソースには、使用量に基づいて料金が発生する場合があります。

> **注：**
>
> このサービスでは、Microsoft Entra IDアカウントでログオンする必要があります。Virtual Apps Essentialsは、live.comなどの他のアカウントタイプをサポートしていません。

Azureサブスクリプションを準備するには、Azure Resource Managerで以下を構成します。

1. リソースグループを作成し、以下を指定します。
   - リソースグループ名
   - サブスクリプション名
   - 場所
2. Azure Resource Managerで、リソースグループ内に仮想ネットワークを作成し、ネットワークの名前を指定します。その他のすべてのデフォルト設定はそのままにしておくことができます。ストレージアカウントは、マスターイメージを作成するときに作成します。
3. 既存のドメインコントローラーを使用するか、新規に作成します。ドメインコントローラーを作成する場合は、次の手順を実行します。
   a. リソースグループと仮想ネットワークで、A3 Standardまたはその他のサイズのWindows Server 2012 R2仮想マシンを使用します。この仮想マシンがドメインコントローラーになります。複数のドメインコントローラーを作成する予定がある場合は、可用性セットを作成し、すべてのドメインコントローラーをこのセットに配置します。
   b. 仮想マシンのネットワークアダプターにプライベート静的IPアドレスを割り当てます。このアドレスはAzureポータルで割り当てることができます。詳細については、MicrosoftドキュメントWebサイトのAzureポータルを使用して仮想マシンのプライベートIPアドレスを構成するを参照してください。
   c. Active Directoryユーザーとグループ、およびActive Directoryログを保存するために、新しいデータディスクを仮想マシンに接続します。詳細については、Azureポータルを使用してWindows VMにマネージドデータディスクを接続するを参照してください。ディスクを接続するときは、すべてのデフォルトオプションを選択して設定を完了します。

d. ドメインコントローラー仮想マシンのプライベートIPアドレスを仮想ネットワークDNSサーバーに追加します。詳細については、「Azure portal (クラシック) を使用して仮想ネットワーク (クラシック) で使用されるDNSサーバーを管理する」を参照してください。

e. Microsoft DNSサーバーに加えて、パブリックDNSサーバーを追加します。2番目のDNSサーバーには、IPアドレス168.63.129.16を使用します。

f. ドメインコントローラー仮想マシンにActive Directory Domain Servicesの役割を追加します。この手順が完了したら、ドメインコントローラー仮想マシンをドメインコントローラーおよびDNSに昇格させます。

g. フォレストを作成し、Active Directoryユーザーを追加します。詳細については、「Azure仮想ネットワークに新しいActive Directoryフォレストをインストールする」を参照してください。

ドメインコントローラーの代わりにMicrosoft Entra ID Domain Servicesを使用する場合は、Microsoft Webサイトのドキュメント「Microsoft Entra ID Domain Services for Beginners」を確認することをお勧めします。

Azureサブスクリプションをリンクする

Citrix Cloudで、Citrix Virtual Apps EssentialsをAzureサブスクリプションにリンクします。

1. Citrix Cloudにサインインします。左上のメニューで、 **>** を選択します。
2. タブで、 をクリックします。
3. をクリックします。Azure portalが開きます。
4. グローバル管理者Azure資格情報を使用して、Azureサブスクリプションにログオンします。
5. をクリックして、Virtual Apps EssentialsがAzureアカウントにアクセスすることを許可します。アカウントで利用可能なサブスクリプションが一覧表示されます。
6. 使用するサブスクリプションを選択し、 をクリックします。
7. Virtual Apps Essentialsコンソールに戻り、リンクされた状態のサブスクリプションを確認します。

AzureサブスクリプションをVirtual Apps Essentialsにリンクしたら、マスターイメージをアップロードします。

マスターイメージを準備してアップロードする

カタログの作成では、アプリケーションとデスクトップを含むVMを展開するためにマスターイメージを使用します。これは、お客様が準備したマスターイメージ（アプリケーションとVDAがインストールされているもの）でも、Citrixが準備したイメージでも構いません。本番環境への展

開では、Citrixは独自のマスターイメージを準備して使用することを推奨します。Citrixが準備したイメージは、パイロット展開またはテスト展開のみを目的としています。

最初の本番イメージは、Azure Resource Managerインターフェースから準備する必要があります。その後、必要に応じてAzureを通じて追加のイメージを作成できます。

Azureインターフェースを通じて追加のイメージを作成する代わりに、Virtual Apps Essentialsインターフェースから新しいマスターイメージを構築できます。

- この方法では、以前に作成されたマスターイメージを使用します。ネットワーク設定は、既存のカタログから取得するか、手動で指定できます。
- 既存のマスターイメージを使用して新しいイメージを作成した後、新しいイメージに接続してカスタマイズし、テンプレートからコピーされたアプリを追加または削除します。VDAはすでにインストールされているため、再度インストールする必要はありません。
- この方法により、Essentialsサービスを使い続けることができます。新しいイメージを作成するためにAzureに移動し、その後イメージをインポートするためにEssentialsサービスに戻る必要はありません。

たとえば、複数のHRアプリを含むマスターイメージを使用するHRという名前のカタログがあるとします。最近、HRカタログのユーザーに提供したい新しいアプリがリリースされました。Virtual Apps Essentialsのイメージ構築機能を使用して、現在のマスターイメージをテンプレートとして選択し、新しいマスターイメージを作成します。また、新しいマスターイメージが同じネットワーク接続設定を使用するようにHRカタログも選択します。最初のイメージ設定後、新しいイメージに新しいアプリをインストールします。テスト後、HRカタログを新しいマスターイメージで更新し、そのカタログのユーザーが利用できるようにします。元のHRマスターイメージは、再度必要になった場合に備えて「マイイメージ」リストに保持されます。

以下のセクションでは、Azureインターフェースを通じてマスターイメージを準備およびアップロードする方法について説明します。Virtual Apps Essentials内からイメージを構築する方法の詳細については、「Virtual Apps Essentialsでマスターイメージを準備する」を参照してください。

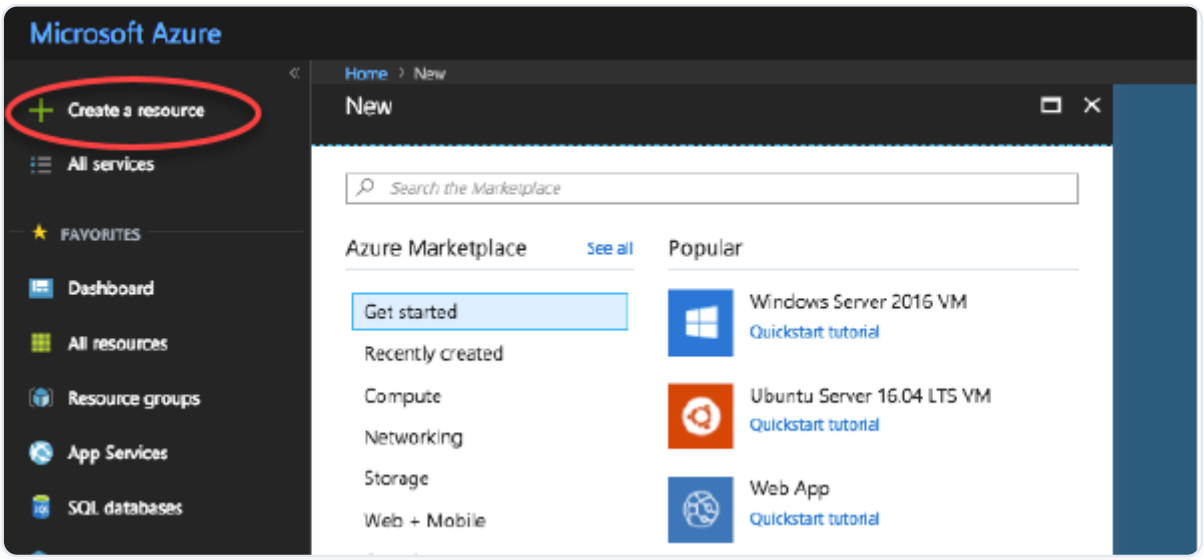
手順の概要

1. AzureまたはVirtual Apps EssentialsでマスターイメージVMを準備します。
2. マスターイメージにアプリをインストールします。
3. マスターイメージにCitrix VDAをインストールします。
4. マスターイメージをAzure Resource ManagerからVirtual Apps Essentialsにアップロードします（必要な場合）。

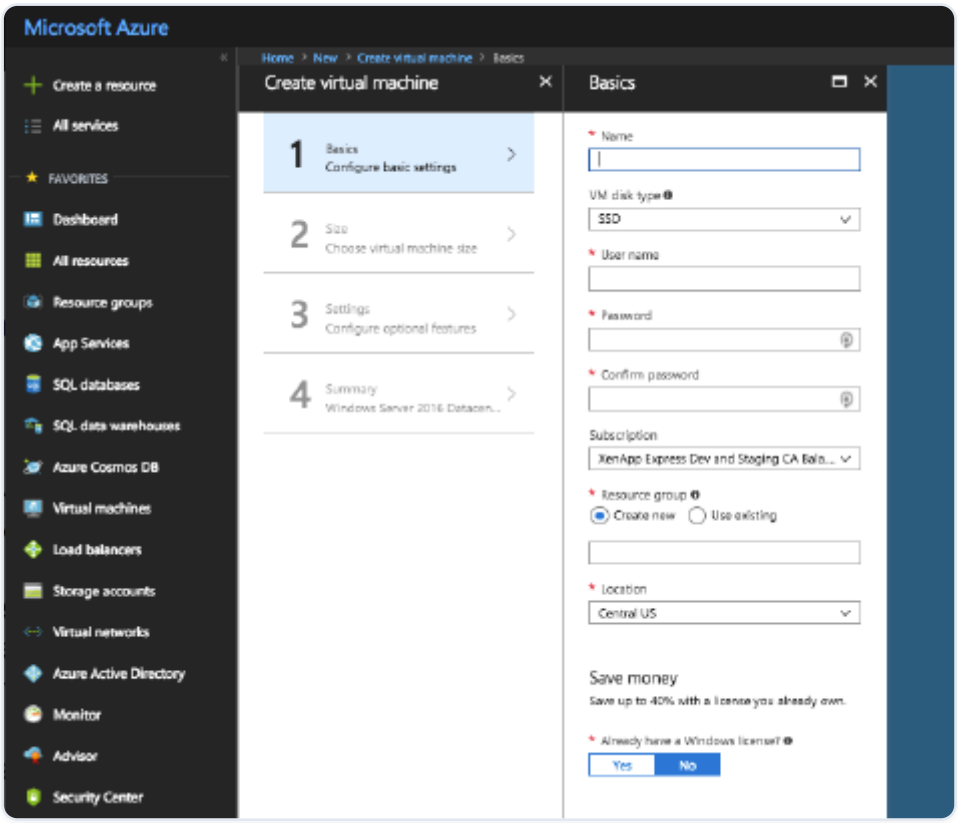
Citrixは、Windows Server 2016またはWindows Server 2012 R2マシンに、サーバーVDAの最新のCurrent Release (CR) またはServer VDA 7.15 Long Term Service Release (LTSR) の最新の累積更新プログラム (CU) をインストールすることを推奨します。Windows Server 2008 R2マシンをお持ちの場合は、サーバーVDA 7.15 LTSR（最新のCUを推奨）をインストールする必要があります。これはダウンロードページでも入手できます。CRおよびLTSR VDAのライフサイクルポリシーについては、「Citrix Virtual Apps and Desktops Serviceのライフサイクルポリシー」を参照してください。

Azure でマスターイメージ VM を作成する

1. Azure portal にサインインします。
2. ナビゲーションペインで をクリックします。Windows Server 2008 R2、Windows Server 2012 R2、または Windows Server 2016 のエントリを選択または検索します。 をクリックします。



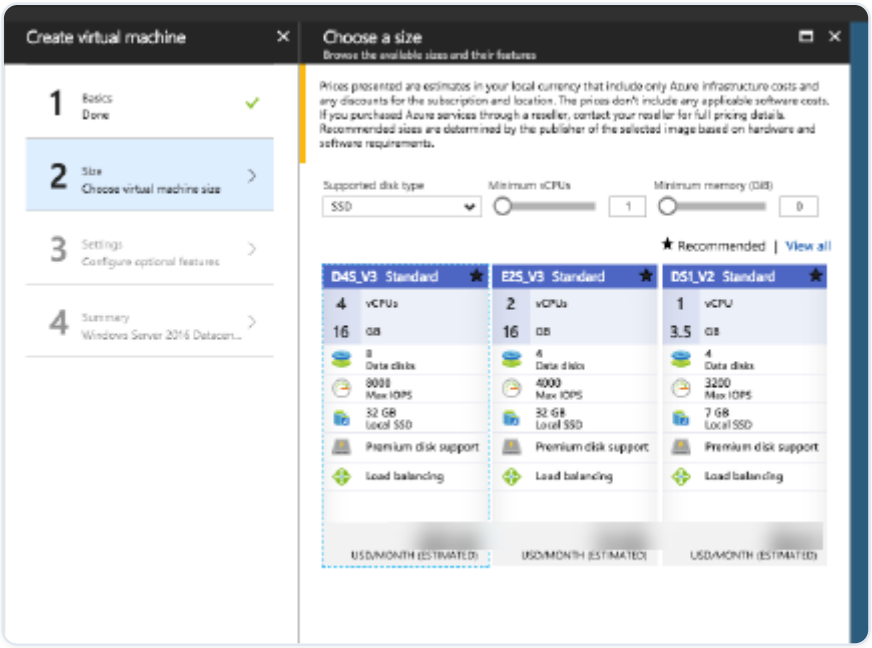
3. 「**仮想マシンの作成**」ページのパネル1「基本」で、次のようにします。
   a. VM の名前を入力します。
   b. VM ディスクの種類を選択します (オプション)。標準ディスクを作成します。
   c. ローカルユーザー名とパスワードを入力し、パスワードを確認します。
   d. サブスクリプションを選択します。
   e. 新しいリソースグループを作成するか、既存のリソースグループを選択します。
   f. 場所を選択します。
   g. リソースグループと場所を選択します。
   h. 既にお持ちの Windows ライセンスを使用するかどうかを選択します。
   i. をクリックします。



4. 「**仮想マシンの作成**」ページのパネル2「サイズ」で、仮想マシンのサイズを選択します。

   a. VMタイプを選択し、vCPUの最小数と最小メモリを指定します。推奨される選択肢が表示されます。すべての選択肢を表示することもできます。

   b. サイズを選択し、**Select**をクリックします。



5. **仮想マシンの作成**ページで、パネル3の「設定」にて:

   a. 高可用性を使用するかどうかを指定します。

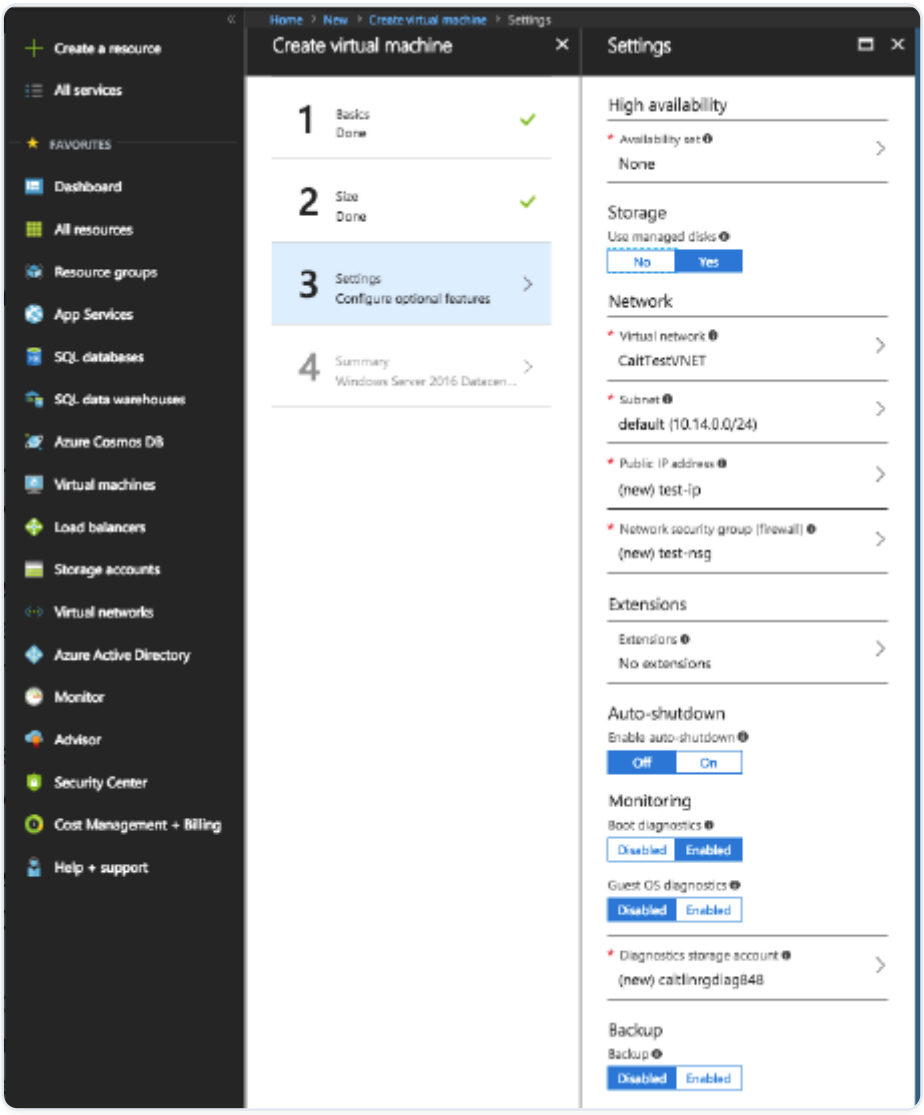
b. 仮想ネットワーク名、サブネット、パブリックIPアドレス、およびネットワークセキュリティを指定します。

c. 必要に応じて、拡張機能を選択します。

d. 自動シャットダウン、監視（ブート診断、ゲストOS診断、診断ストレージアカウント）を有効または無効にします。

e. バックアップを有効または無効にします。

f. **OK**をクリックします。



6. パネル4の「概要」で、**OK**をクリックしてVMの作成を開始します。

イメージをSysprepしないでください。

マスターイメージにアプリをインストールする

作成したばかりのマスターイメージVMに、ストアURLでログオンしたときにユーザーが利用できるアプリを追加します。（後で、このマスターイメージを使用するカタログを作成した後、指定したユーザーが利用できるアプリを正確に指定します。）

1. マスターイメージVMを作成後、実行中に接続します。
2. アプリケーションをインストールします。

マスターイメージにVDAをインストールする

1. マスターイメージVMに接続します（まだ接続していない場合）。
2. Citrix Cloudナビゲーションバーの**Downloads**リンクを使用して、サーバーOS用VDAをダウンロードできます。または、ブラウザを使用してCitrix DaaSダウンロードページに移動します。サーバーOS用VDAをVMにダウンロードします。（VDAバージョン情報については、上記のガイダンスを参照してください。）
3. ダウンロードしたファイルをダブルクリックして、VDAインストーラーを起動します。インストールウィザードが起動します。
4. **Environment**ページで、**Create a master image using MCS**を選択し、**Next**をクリックします。
5. **Core Components**ページで、**Next**をクリックします。
6. **Delivery Controller**ページで、**Let Machine Creation Services™ do it automatically**を選択し、**Next**をクリックします。
7. Citrixから別途指示がない限り、**Additional Components**、**Features**、および**Firewall**ページではデフォルト設定のままにします。各ページで**Next**をクリックします。
8. **Summary**ページで、**Install**をクリックします。前提条件のインストールが開始されます。再起動を求められたら、同意します。
9. VDAのインストールが自動的に再開されます。前提条件のインストールが完了し、コンポーネントと機能がインストールされます。**Call Home**ページで、デフォルト設定のままにし（Citrixから別途指示がない限り）、**Next**をクリックします。
10. **Finish**をクリックします。マシンが自動的に再起動します。
11. 構成が正しいことを確認するには、インストールしたアプリケーションを1つ以上起動します。
12. VMをシャットダウンします。イメージをSysprepしないでください。

マスターイメージをアップロードする

この手順では、Azure Resource ManagerからVirtual Apps Essentialsにマスターイメージをアップロードします。

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、 **>** を選択します。

2. タブで、 をクリックします。
3. をクリックします。
4. ページで、サブスクリプション、リソースグループ、ストレージアカウント、VHD、およびリージョンを選択して、イメージの場所を指定します。
5. マスターイメージの名前を入力します。
6. をクリックします。

サービスはマスターイメージを検証します。検証後、アップロードされたイメージは > の下に表示されます。

ヒント: カタログを作成する前にマスターイメージをアップロードする代わりに、カタログを作成するときにAzure Resource Managerからマスターイメージをインポートできます。

Virtual Apps Essentialsでマスターイメージを準備する

この方法では、既存のマスターイメージをテンプレートとして使用し（オプションで、既存のカタログからの接続詳細も使用）、別のマスターイメージを構築します。その後、新しいマスターイメージをカスタマイズできます。この手順は、Virtual Apps Essentialsインターフェイスを通じて完全に実行されます。

1. まだサインインしていない場合は、Citrix Cloudにサインインします。左上のメニューで、 > を選択します。
2. をクリックし、次に タブを選択します。
3. をクリックします。
4. ページで、 パネルでマスターイメージを選択します。新しいイメージの名前を指定します。 をクリックします。
5. パネルで、既存のカタログの設定を使用するか、設定を指定できます。設定は、サブスクリプション、仮想ネットワーク、リージョン、サブネット、ドメイン、およびVMインスタンスタイプです。（カタログがない場合は、設定を入力する必要があります。）

   「**カタログから設定をコピー**」を選択した場合、カタログを選択します。ネットワーク接続設定が表示されるので、新しいマスターイメージでそれらを使用したいことを視覚的に確認できます。ドメインに参加するためにサービスアカウントのユーザー名とパスワードを入力します。「**保存**」をクリックします。

   「**新しい設定を入力**」を選択した場合、適切な設定フィールドで値を選択します。ドメインに参加するためにサービスアカウントのユーザー名とパスワードを入力します。「**保存**」をクリックします。

6. 「**プロビジョニングの開始**」をクリックします。
7. 新しいイメージが作成されると、「**管理 > マスターイメージ**」リストに「**入力が必要です**」というステータスで表示されます。「**VMに接続**」をクリックします。RDPクライアントがダウンロードされます。RDPを使用して新しく作成されたVMに接続します。アプリケーションやその他のソフトウェアを追加または削除して、新しいイメージをカスタマイズします。すべてのマスターイメージと同様に、イメージをSysprepしないでください。
8. 新しいイメージのカスタマイズが完了したら、「**管理 > マスターイメージ**」ページに戻り、新しいマスターイメージの「**完了**」をクリックします。新しいイメージは検証プロセスに送られます。
9. 検証プロセスが完了すると、新しいイメージは「**マイイメージ**」リストに「**準備完了**」というステータスで表示されます。

後でカタログを作成し、「**マスターイメージの選択**」ページで「**既存のイメージをリンク**」を選択すると、新しいイメージが「**イメージ名**」の選択肢に表示されます。

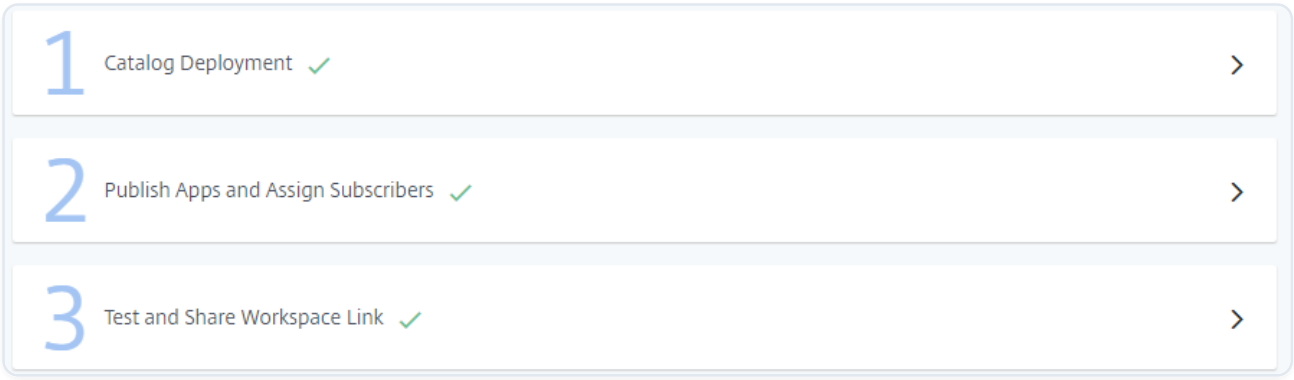
カタログを展開し、アプリとデスクトップを公開し、エンドユーザーを割り当てる

カタログには、選択したユーザーと共有することを選択したアプリとデスクトップが一覧表示されます。

他のCitrixアプリおよびデスクトップ配信製品に慣れている場合、このサービスにおけるカタログは、マシンカタログとデリバリーグループを組み合わせたものに似ています。ただし、他のサービスにおけるマシンカタログとデリバリーグループの作成ワークフローは、このサービスでは利用できません。

カタログを展開し、エンドユーザーとアプリを共有することは、複数のステップからなるプロセスです。

- カタログを作成する
- そのカタログのアプリを公開し、エンドユーザーを割り当てる
- エンドユーザーが使用するストアリンクをテストして共有する

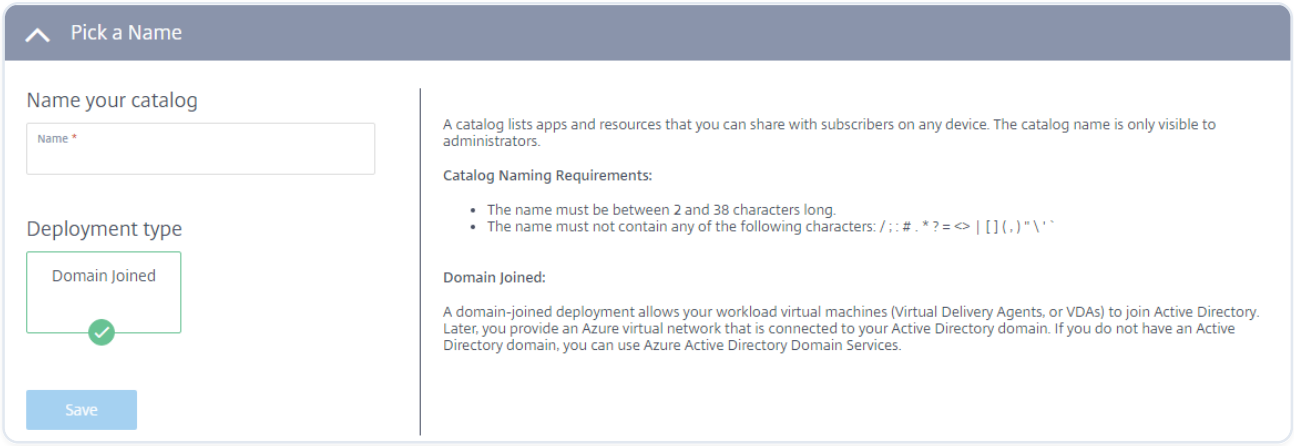


カタログを作成する

カタログを作成する際は、Microsoft Entra ID アカウント資格情報とサブスクリプション名を用意してください。

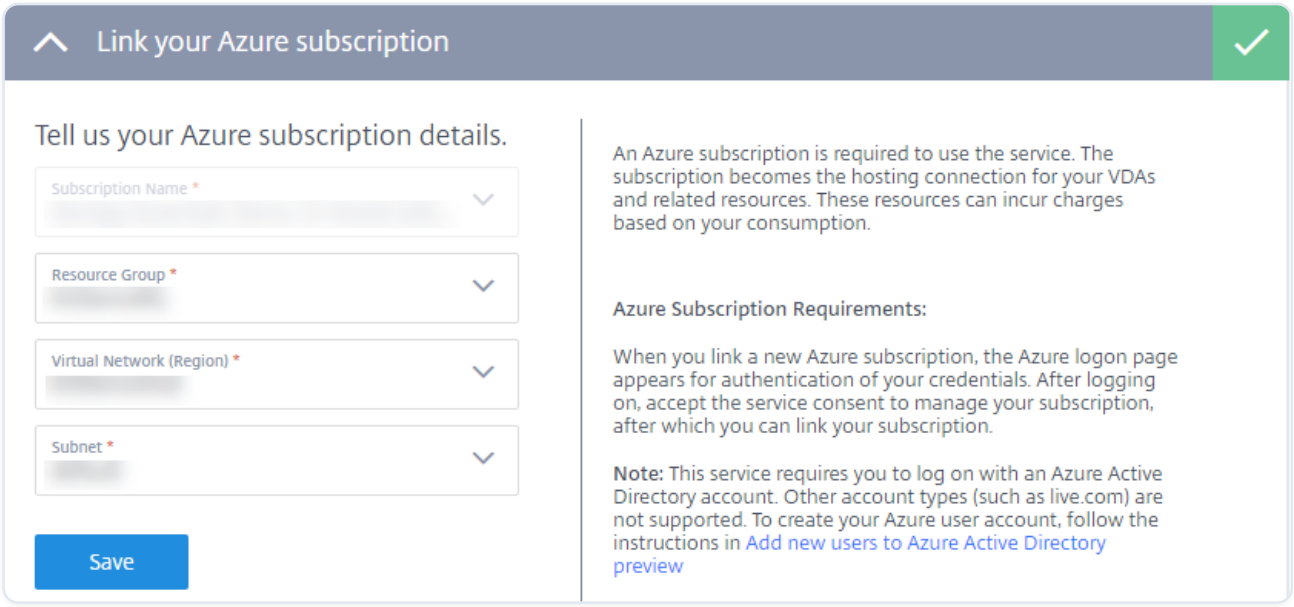
1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、**My Services > Virtual Apps and Desktops** を選択します。
2. **Manage** タブで、**Catalogs** をクリックし、次に **Add Catalog** をクリックします。
3. 以下のパネルに情報を入力します。各パネルの入力が完了したら、**Save** をクリックします。必須情報が不足しているか無効な場合、パネルのヘッダーに警告サインが表示されます。チェックマークは、情報が完全であることを示します。

名前を選択する



1. カタログの2〜38文字の名前を入力します。(文字と数字のみ。特殊文字は使用できません。) この名前は管理者のみに表示されます。
2. まだ選択されていない場合は、**Domain Joined** を選択します。ドメイン参加済み展開では、VDA を Active Directory に参加させることができます。後で、ドメインに接続されている Azure 仮想ネットワークを提供します。ドメインがない場合は、Microsoft Entra ID Domain Services を使用できます。
3. **Save** をクリックします。

Azure サブスクリプションをリンクする



1. Azure サブスクリプションを選択します。新しい Azure サブスクリプションをリンクすると、Azure 資格情報の認証のために Azure サインインページが表示されます。サインイン後、サブスクリプションを管理するためのサービス同意を受け入れます。その後、サブスクリプションをリンクできます。Virtual Apps Essentials では、Microsoft Entra ID アカウントでログオンする必要があります。その他のアカウントタイプ (live.com など) はサポートされていません。
2. リソースグループ、仮想ネットワーク (VNET)、およびサブネットを選択します。VNET は、リソースが展開される Azure リージョンを決定します。サブネットはドメインコントローラーに到達できる必要があります。
3. **Save** をクリックします。

ローカルドメインに参加

Virtual Apps Essentialsのローカルドメイン参加ページ(/en-us/citrix-cloud/media/xae-cat-join-local-domain.png)

1. ドメイン情報を入力します。

   - **完全修飾ドメイン名:** ドメイン名を入力します。この名前は、仮想ネットワークで提供されるDNSから解決できる必要があります。
   - **組織単位:** (オプション) Active Directoryに指定されたOUが含まれていることを確認してください。このフィールドを空白のままにすると、マシンはデフォルトのComputersコンテナに配置されます。
   - **サービスアカウント名**、**パスワード**、および**パスワードの確認**: マシンをドメインに追加する権限を持つアカウントのユーザープリンシパル名 (UPN) を入力します。次に、そのアカウントのパスワードを入力し、確認します。

2. **保存**をクリックします。

AzureサブスクリプションにVMを作成することで、仮想ネットワーク経由の接続をテストできます。VMは、カタログの展開に使用するのと同じリソースグループ、仮想ネットワーク、サブネット内にある必要があります。VMがインターネットに接続できることを確認してください。また、VMをドメインに参加させることでドメインに到達できることを確認してください。このカタログの展開に使用したのと同じ資格情報を使用してテストできます。

リソースの場所に接続する

各リソースの場所には、Citrix Cloudと通信する2つ以上のCloud Connectorが必要です。カタログが展開されると、サービスはCloud Connectorの展開を自動的に処理します。2つのWindows Server VMがAzure Resource Managerに作成され、その後、各サーバーにCloud Connectorが自動的にインストールされます。 選択したリソースの場所が利用可能な場合、接続は自動的に行われます。**保存**をクリックするだけです。 リソースの場所を作成するには、その名前を入力します。

- 特定のAzureリソースグループにCloud Connectorを作成するには、**Azureリソースグループ**の横にある**編集**をクリックしてリソースの場所を変更します。そうしないと、サービスはAzureサブスクリプションをリンクしたときに指定したリソースグループを使用します。
- Cloud Connectorを別のOUに配置するには、**組織単位**の横にある**編集**をクリックしてOUを変更します。そうしないと、Virtual Apps EssentialsはAzureサブスクリプションをリンクしたときに指定したリソースグループを使用します。

マスターイメージを選択する

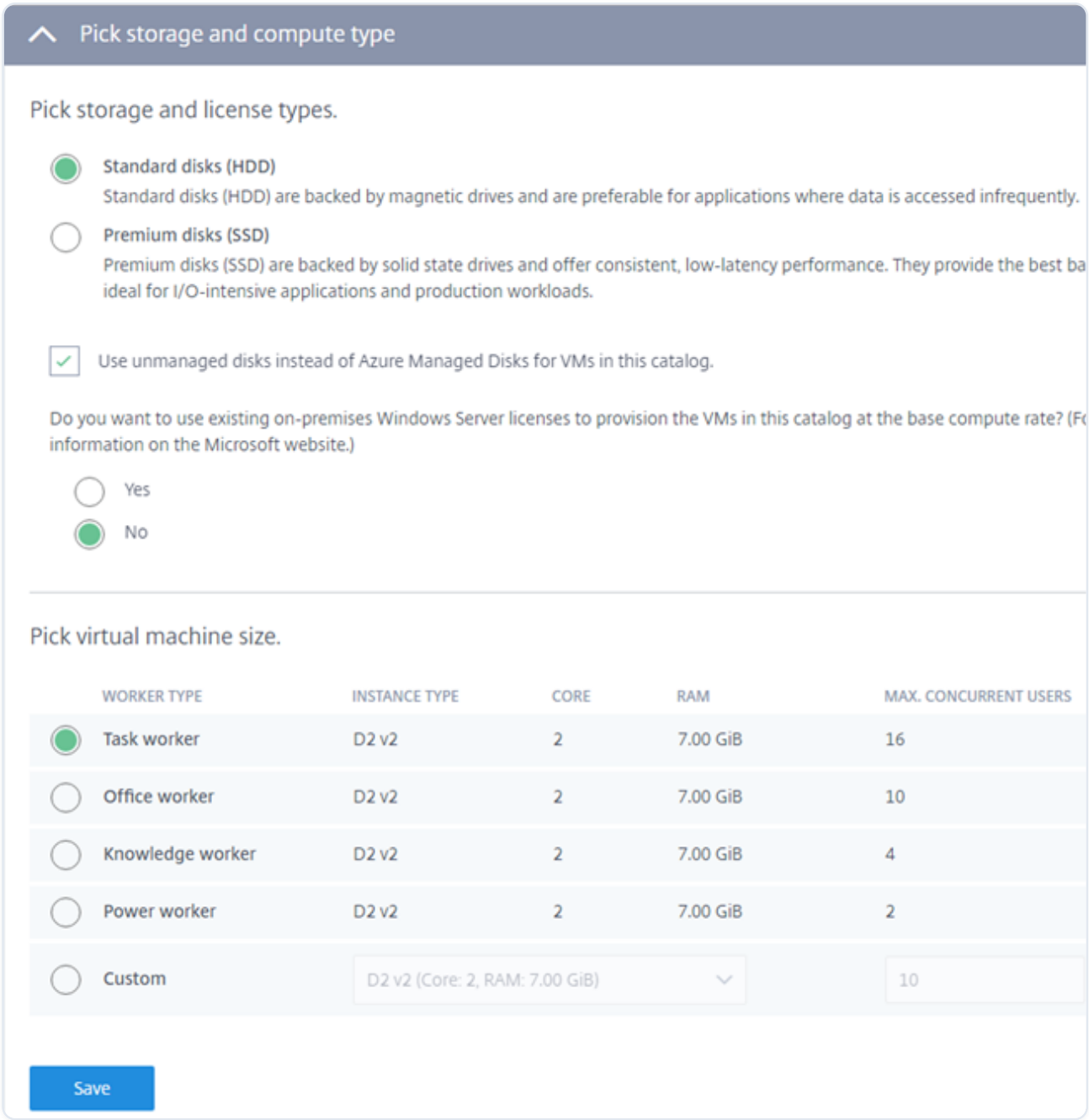
Virtual Apps Essentialsのマスターイメージ選択ページ(/en-us/citrix-cloud/media/xae-cat-master-image.png)

1. 次のいずれかを選択します。

    - **既存のイメージをリンク:** 以前にカスタムイメージをインポートしていて、このカタログで使用したい場合は、このオプションを使用します。イメージを選択し、必要に応じてリージョンを選択します。
    - **新しいイメージをインポート:** このカタログでカスタムイメージを使用したいが、まだインポートしていない場合は、このオプションを使用します。サブスクリプション、リソースグループ、ストレージアカウント、およびVHDを選択します。イメージの表示名を入力します。
    - **Citrixが準備したイメージを使用:** 独自のカスタムイメージを使用せずにサービスをテストするには、このオプションを使用します。これらのイメージはデモンストレーション環境にのみ適しており、本番環境での使用は推奨されません。準備されたイメージを選択します。

2. **保存**をクリックします。

ストレージとコンピューティングの種類を選択



1. 次の項目を構成します。

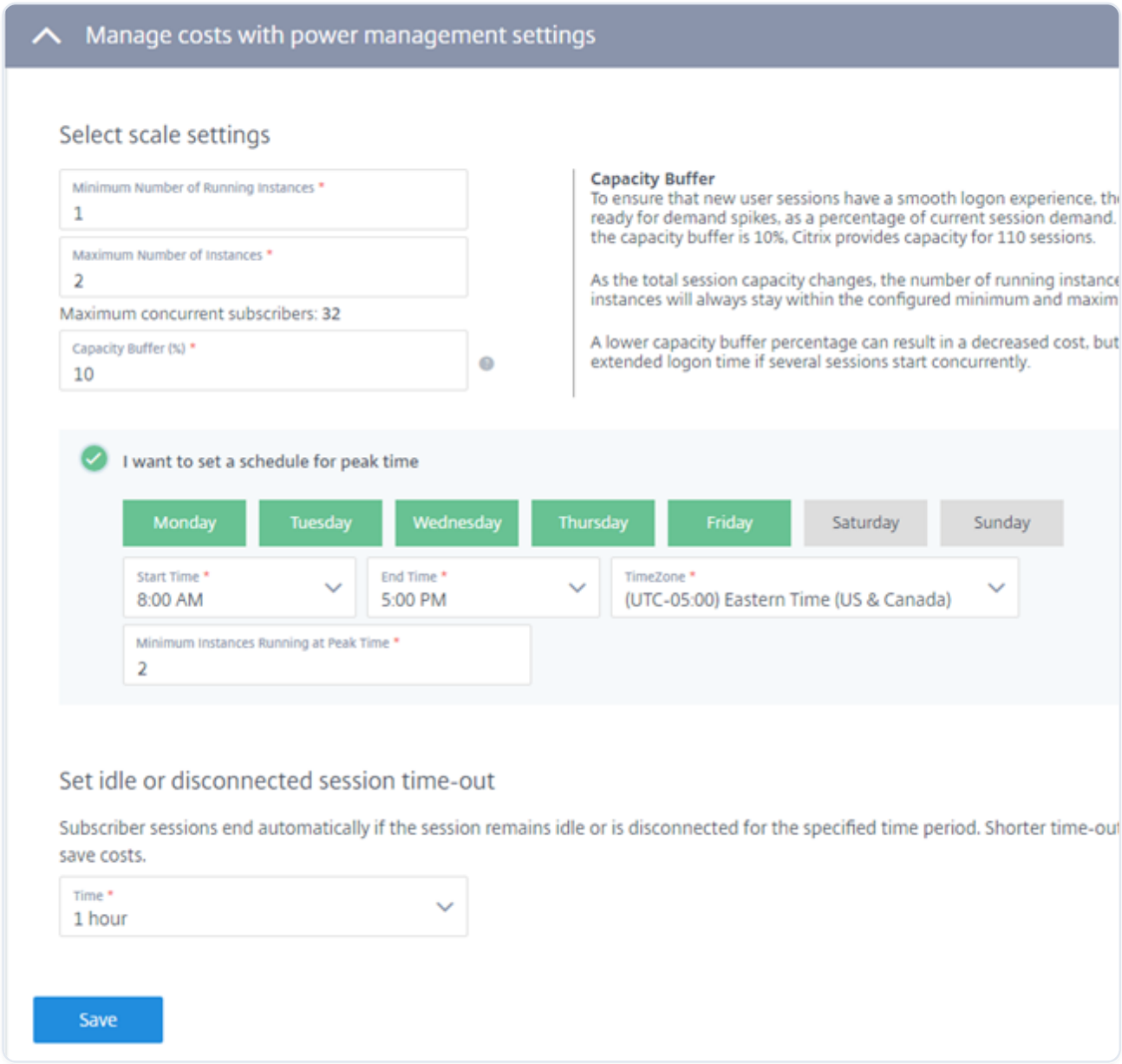
   - **標準ディスクまたはプレミアムディスク:** 標準ディスク (HDD) は磁気ドライブによってサポートされています。データへのアクセスが頻繁でないアプリケーションに適しています。プレミアムディスク (SSD) はソリッドステートドライブによってサポートされています。I/O集中型アプリケーションに最適です。
   - **Azureマネージドディスクまたはアンマネージドディスクを使用:** Azureマネージドディスクの詳細については、https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/managed-disks-overviewを参照してください。

- **Azureハイブリッド特典:** 既存のオンプレミスWindows Serverライセンスを使用するかどうかを選択します。この機能を有効にして既存のオンプレミスWindows Serverイメージを使用すると、Azureハイブリッド特典 (HUB) が適用されます。詳細については、https://azure.microsoft.com/pricing/hybrid-use-benefit/を参照してください。

  HUBは、Azureギャラリーからの追加のWindows Serverライセンスの料金を免除するため、AzureでVMを実行するコストを基本コンピューティング料金に削減します。HUBを使用するには、オンプレミスのWindows Serverイメージを Azureに持ち込む必要があります。Azureギャラリーイメージはサポートされていません。オンプレミスのWindowsクライアントライセンスは現在サポートされていません。Microsoft WebサイトのAzure Hybrid Benefit for Windows Serverを参照してください。
- **仮想マシンのサイズを選択:** ワーカーロール (例: タスク、オフィス、ナレッジ、パワー) を選択します。ワーカーロールは使用されるリソースを定義します。ワーカーロールを指定すると、サービスはインスタンスあたりの正しい負荷を決定します。オプションを選択するか、独自のカスタムオプションを作成できます。

2. **保存**をクリックします。

電源管理設定でコストを管理



1. 以下の情報を入力します。

   - **スケール設定:**

     - **実行中のインスタンスの最小数:** サービスは、この数のVMが常に電源オンの状態であることを保証します。
     - **実行中のインスタンスの最大数:** サービスは、この数のVMを超えることはありません。
     - **最大同時ユーザー数:** サービスは、この制限を超える同時ユーザーを許可しません。
     - **キャパシティバッファ:** 現在のセッション需要に対する割合として、需要の急増に備えて追加のセッションを準備できるようにします。たとえば、アクティブなセッションが

100あり、キャパシティバッファが10%の場合、サービスは110セッション分のキャパシティを提供します。

合計セッションキャパシティが変更されると、このカタログの実行中のインスタンス数はスケールアップまたはスケールダウンします。実行中のインスタンス数は、常に構成された最小値と最大値の範囲内に保たれます。キャパシティバッファの割合が低いと、コストが削減される可能性があります。ただし、複数のセッションが同時に開始された場合、一部のセッションでログオン時間が延長される可能性もあります。

- **ピーク時間のスケジュール:** ピーク時間中に非ピーク時間とは異なる数のVMを実行したい場合は、このオプションを選択します。ピーク時間の曜日、開始時刻と終了時刻、およびタイムゾーンを選択します。ピーク時間中の実行中のインスタンスの最小数を指定します。
- **アイドルまたは切断されたセッションのタイムアウト:** セッションが終了する時間を設定します。セッションが指定された期間アイドル状態のままか、切断された場合、ユーザーセッションは自動的に終了します。タイムアウト値を短くすると、未使用のVDAの電源をオフにしてコストを節約できます。

2. **保存**をクリックします。

カタログを展開する

構成パネルを完了したら、**展開の開始**をクリックしてカタログ作成を開始します。カタログの作成には1〜2時間（または、多数のVMを指定した場合はそれ以上）かかる場合があります。

カタログが作成されると:

- ワークロードマシン用のリソースグループ（およびそのリソースグループ内のストレージアカウント）がAzureに自動的に作成されます。
- VMの名前はXenappxx-xx-yyyとなり、xxは環境要因から派生し、yyは序数です。

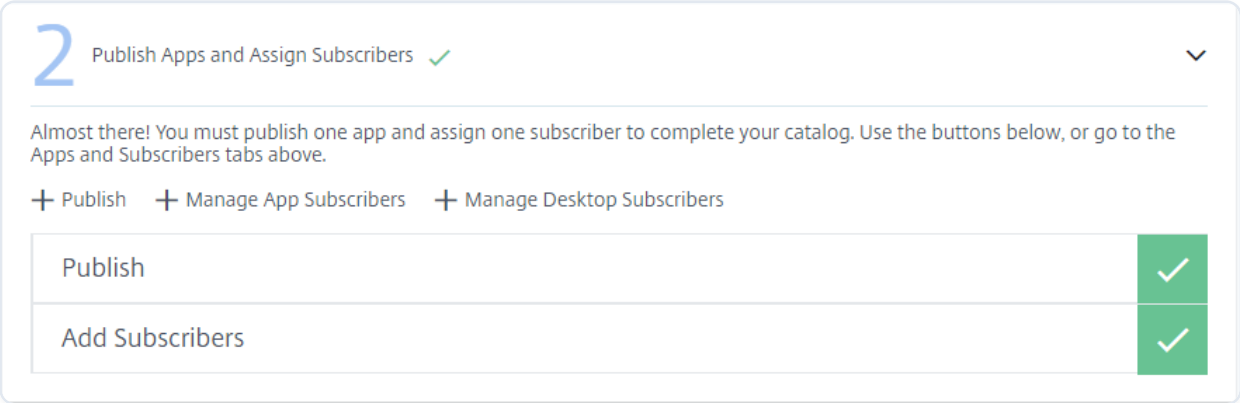
アプリを公開し、カタログにエンドユーザーを割り当てる

カタログの展開後、カタログを完成させるには、1つのアプリまたはデスクトップを公開し、少なくとも1人のエンドユーザーを割り当てる必要があります。

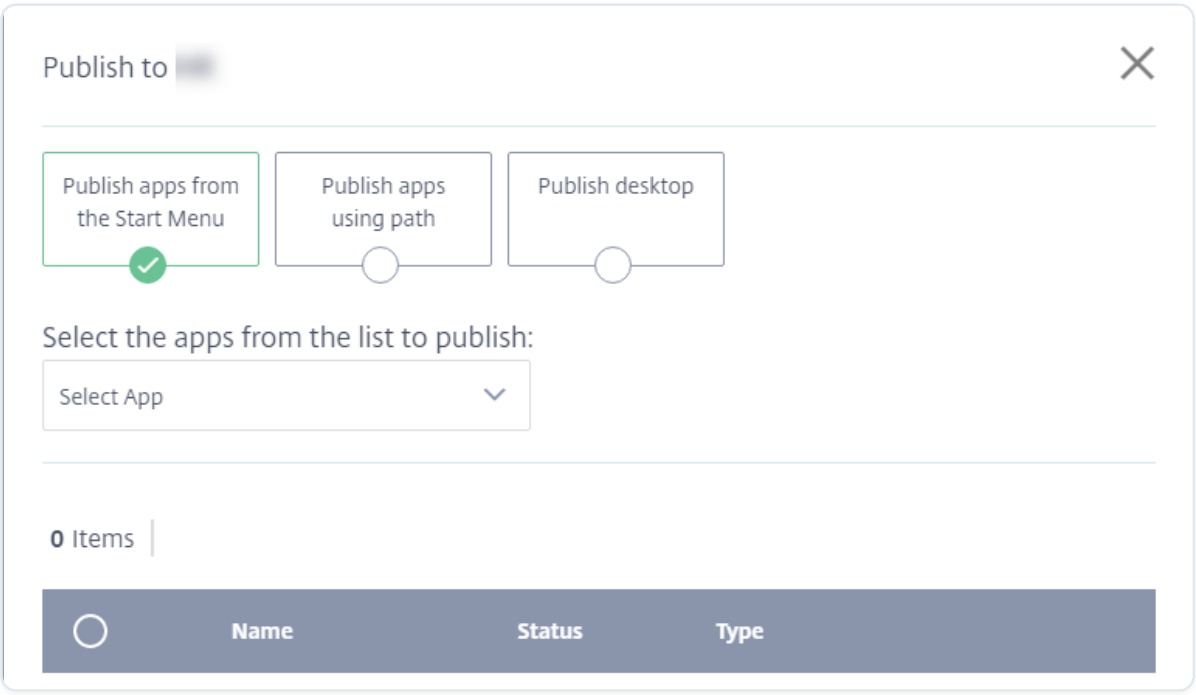
カタログの作成に使用したイメージには、公開できるアプリケーション（またはデスクトップ）が含まれています。スタートメニューからアプリケーションを選択するか、マシンのディレクトリパスを指定できます。

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**My Services > Virtual Apps and Desktops**を選択します。

2. **Manage**タブで、**Catalogs**をクリックします。
3. 作成されたカタログの省略記号メニュー（...）で、**Manage Catalog**を選択します。
4. **Publish Apps and Assign end users**を選択します。次のページが表示されます。



5. **Publish Apps and Assign end users**ダイアログボックスで、**Publish**をクリックします。「Publish to catalog-name」ページには3つの選択肢があります。少なくとも1つを完了してください。オプションで、別の選択肢を選ぶこともできます（たとえば、このカタログを使用してアプリとデスクトップの両方を公開する場合など）。
6. スタートメニューにあるアプリを公開するには：
   a. **Publish from Start Menu**を選択します。
   b. リストからアプリケーションを選択します。



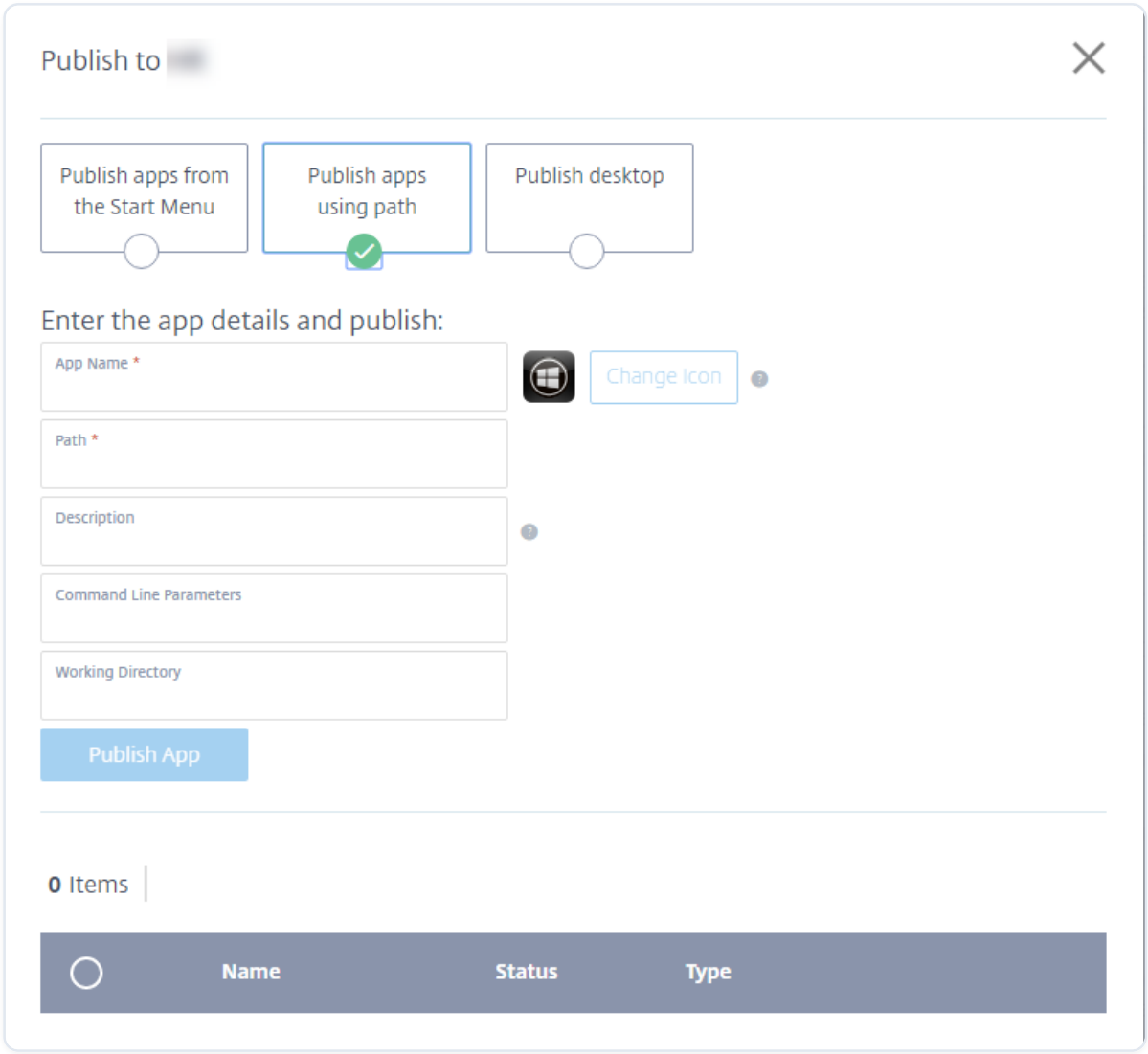
7. アプリの場所やその他の情報を指定して公開するには：
   a. **Publish using Path**を選択します。

b. 各アプリケーションの名前とパス（例：c:\Windows\system1\app.exe）を入力します。

c. オプションで、ユーザーのストア、コマンドラインパラメータ、および作業ディレクトリに表示される説明を入力します。

d. 公開されたアプリを表すアイコンを変更するには、**アイコンの変更**をクリックし、アイコンの場所へ移動します。選択したアイコンを抽出できない場合、メッセージが表示されます。その場合、再試行するか、既存のアイコンの使用を続行できます。

e. **アプリの公開**をクリックします。



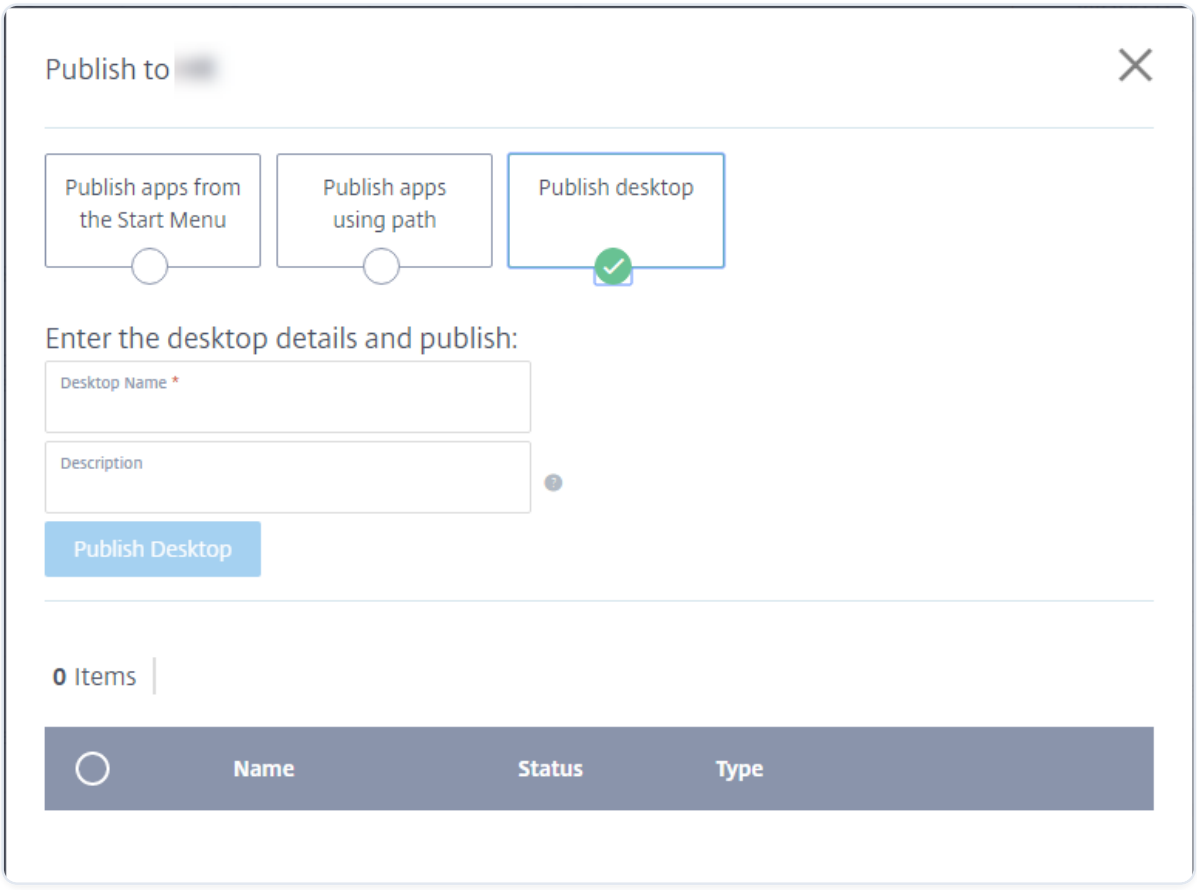
8. デスクトップを公開するには:

a. **デスクトップの公開**を選択します。

b. デスクトップの名前を入力します。

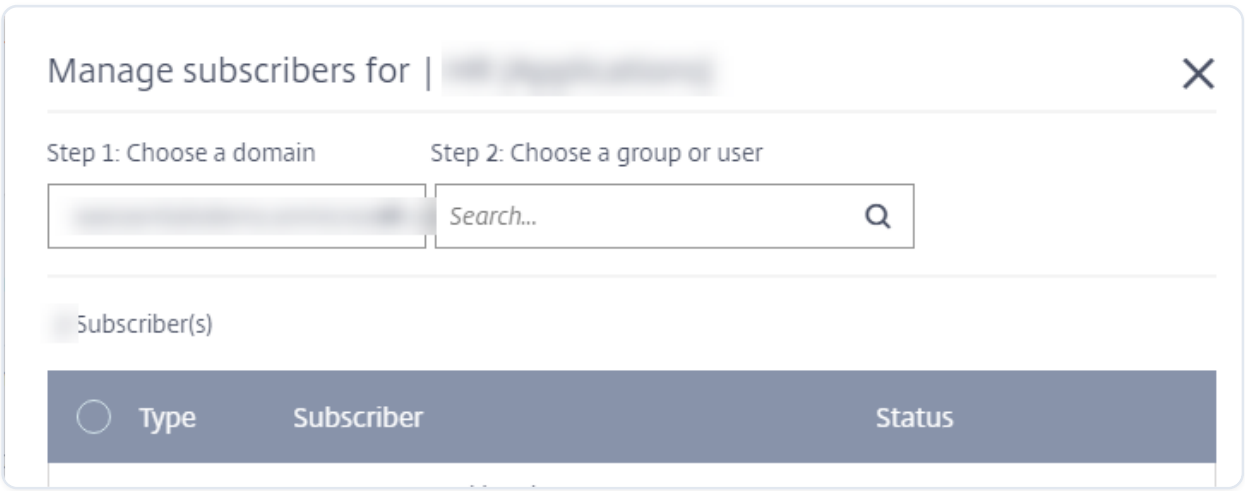
c. オプションで、ユーザーのストアに表示される説明を入力します。

d. **デスクトップの公開**をクリックします。



アプリまたはデスクトップを追加すると、セレクターの下のリストに表示されます。追加したアプリまたはデスクトップを削除するには、エントリの左側にあるボタンを選択するか（またはエントリの横にあるゴミ箱アイコンをクリックして）、**削除**をクリックします。後でアプリまたはデスクトップの公開を取り消したい場合は、エントリの左側にあるボタンを選択し、**公開取り消し**をクリックします。

9. **アプリの公開とエンドユーザーの割り当て**ダイアログボックスで、**アプリのエンドユーザーの管理**または**デスクトップのエンドユーザーの管理**のいずれかをクリックします。



10. ドメインを選択し、ユーザーまたはユーザーグループを検索します。

11. アプリとデスクトップのユーザー割り当ては別々です。ユーザーにアプリとデスクトップの両方へのアクセスを割り当てるには、そのユーザーを**アプリのエンドユーザーの管理**と**デスクトップのエンドユーザーの管理**の両方で割り当てます。

    ユーザーまたはグループを追加すると、セレクターの下のリストに表示されます。選択したユーザーまたはグループを削除するには、エントリの横にあるゴミ箱アイコンをクリックし、**Remove**をクリックします。後でユーザーを削除したい場合は、エントリの左側にあるボタンを選択し、**Remove Selected**をクリックします。

ストアリンクをテストして共有する

カタログを展開し、アプリを公開し、エンドユーザーを割り当てると、エンドユーザーが公開されたアプリやデスクトップにアクセスするために使用するリンクが提供されます。

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**My Services > Virtual Apps and Desktops**を選択します。
2. **Manage**タブで、**Catalogs**をクリックします。
3. カタログの省略記号メニュー（...）で、**Manage Catalog**を選択します。
4. **Test and Share store Link**を選択します。

以下のグラフィックでは、ストアリンクが丸で囲まれた領域に表示されています。このリンクをエンドユーザーと共有してください。ページの右側には、ストアURL、およびカタログのマスターイメージ、リソースの場所、Azureサブスクリプション、ドメインに関する情報が一覧表示されます。

ストアリンクが強調表示されています](/en-us/citrix-cloud/media/xae-workspace-link.png)

詳細については、store experienceを参照してください。

マスターイメージとカタログを更新する

アプリケーションを更新または追加するには、カタログのマスターイメージの作成に使用した仮想マシンを更新します。

マスターイメージを更新する

1. マスターイメージVMの電源を入れます。マシンの電源を入れても、Azure Resource Managerにインストールされているマスターイメージには影響しません。
2. VMに更新プログラムまたはアプリケーションをインストールします。
3. VMをシャットダウンします。

4. Virtual Apps Essentialsコンソールで、VMのVHDイメージへのパスを含む新しいイメージを追加します。

新しいイメージでカタログを更新する

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**My Services > Virtual Apps and Desktops**を選択します。
2. **Manage**タブで、**Catalogs**をクリックします。
3. カタログの省略記号メニューをクリックし、次に**Update Catalog Image**をクリックします。
4. **Link an existing image**または**Import a new image**のいずれかを選択します。選択に応じて適切な情報を入力します。
5. **Time until automatic log-off**で、セッションが終了するまでの時間を選択します。
6. **Update**をクリックします。

カタログの更新を開始すると、初期処理が完了するまで、ユーザーは作業を続行できます。その後、ユーザーには作業を保存してアプリケーションを閉じるよう警告メッセージが表示されます。VDA上のすべてのアクティブなセッションを閉じると、そのVDAでの更新が完了します。指定された時間内にユーザーがログオフしない場合、セッションは自動的に閉じられます。

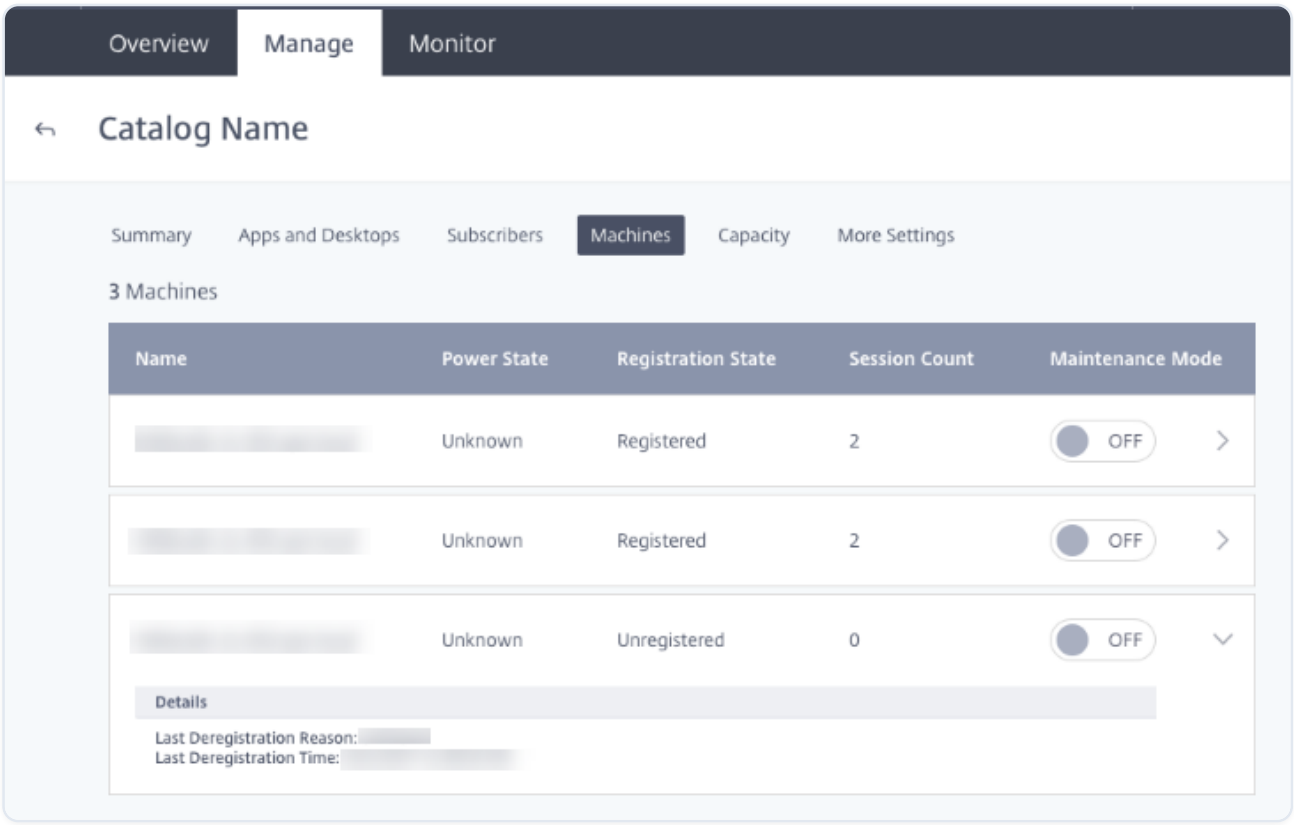
カタログ内のVDAの数を更新する

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**My Services > Virtual Apps and Desktops**を選択します。
2. **Manage**タブをクリックします。
3. **Catalogs**タブで、カタログを選択します。
4. **Capacity**タブで、**Select scale settings**の下にある**Edit**をクリックします。
5. カタログに必要なVDA数に合わせて、**実行中のインスタンスの最大数**の値を変更します。
6. **保存**をクリックします。

マシンの状態を監視する

カタログを選択すると、カタログの概要ページのタブに、そのカタログ内のすべてのマシンが一覧表示されます。表示には、各マシンの電源状態と登録状態、および現在のセッション数が含まれ

ます。



マシンのメンテナンスモードをオンまたはオフにできます。メンテナンスモードをオンにすると、マシンへの新しい接続が防止されます。ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。パッチを適用する前に、マシンをメンテナンスモードにする必要がある場合があります。

1台以上のマシンでメンテナンスモードをオンにすると、そのカタログ内のすべてのマシンでSmart Scaleが一時的に無効になります。次のいずれかのアクションを実行すると、Smart Scaleが再度有効になります。

- 画面上部の警告で**Smart Scaleを有効にする**をクリックします。このアクションにより、メンテナンスモードがオンになっているカタログ内のすべてのマシンのメンテナンスモードが自動的にオフになります。
- メンテナンスモードが現在オンになっている各マシンで、明示的にメンテナンスモードをオフにします。

Smart Scaleメンテナンスモードページ(/en-us/citrix-cloud/media/maint-mode-smart-scale.png)

サービスを監視する

1. Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**マイサービス > Virtual Apps and Desktops**を選択します。

2. **監視**タブをクリックします。

セッション情報

Citrix Virtual Apps Essentialsの全体的なパフォーマンスを監視するには：

1. 監視するカタログを選択します。セッション、ログオン期間、その他の情報を表示できます。
2. セッションを選択し、その後:
    - セッションを切断する
    - セッションからログオフする
    - メッセージを送信する
3. 各セッションをクリックすると、プロセス、実行中のアプリケーションなど、セッションに関する詳細が表示されます。

使用状況情報

使用状況情報には、すべてのカタログの集計データが表示されます（特定のカタログではなく）。

- **使用状況の概要**には、過去6週間のアプリケーション起動の合計数と、アプリを起動したユニークユーザーの数が表示されます。
- **上位アプリ**には、今月と前月に最も頻繁に使用されたアプリが一覧表示されます。エントリにカーソルを合わせると、そのアプリケーションが起動された回数が表示されます。
- **上位ユーザー**には、今月と前月の上位10人のユーザーと、彼らがアプリケーションを起動した回数が一覧表示されます。

週次データ間隔は、月曜日（UTC 00:00）からクエリ時間までです。月次データ間隔は、月の最初の日（UTC 00:00）からクエリ時間までです。

プロファイル管理

プロファイル管理は、ユーザーデバイスの場所に関係なく、個人の設定がユーザーの仮想アプリケーションに適用されるようにします。

プロファイル管理の構成はオプションです。

プロファイル最適化サービスを使用してプロファイル管理を有効にできます。このサービスは、Windowsでこれらの設定を管理するための信頼性の高い方法を提供します。プロファイルを管理することで、ユーザーに追従する単一のプロファイルを維持し、一貫したエクスペリエンスを保証します。ユーザープロファイルを自動的に統合および最適化し、管理とストレージの要件を最小限

に抑えます。プロファイル最適化サービスは、最小限の管理、サポート、およびインフラストラクチャしか必要としません。また、プロファイル最適化は、ユーザーに改善されたログオンおよびログオフエクスペリエンスを提供します。

プロファイル最適化サービスでは、すべての個人設定が保持されるファイル共有が必要です。ファイル共有はUNCパスとして指定する必要があります。パスには、システム環境変数、Active Directoryユーザー属性、またはProfile Management変数を指定できます。UNCテキスト文字列の形式の詳細については、「ユーザー ストアへのパスを指定するには」を参照してください。

Citrix CloudでProfile Managementを構成します。

Profile Managementを構成するには

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、**［マイサービス］>［Virtual Apps and Desktops］**の順に選択します。
2. **［管理］タブで、［カタログ］**をクリックします。
3. カタログの名前をクリックします。
4. **［詳細設定］**をクリックします。
5. **［AzureサブスクリプションでProfile Managementをセットアップ］**で、プロファイル共有へのパスを入力します。例：\\fileserver\share#sAMAccountName#
6. **［保存］**をクリックします。

Profile Managementを有効にする際は、ユーザープロファイルサイズの悪影響を最小限に抑えるために、フォルダーリダイレクトを構成してユーザープロファイルをさらに最適化することを検討してください。フォルダーリダイレクトを適用することで、Profile Managementソリューションが補完されます。詳しくは、「Microsoft Folder Redirection」を参照してください。

Microsoft RDSライセンスサーバーを構成する

Citrix Virtual Apps Essentialsは、通常、Remote Desktop Servicesクライアントアクセスライセンス（RDS CAL）を必要とするWindows Serverのリモートセッション機能にアクセスします。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳しくは、「Remote Desktop Servicesライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、Virtual Apps Essentialsでライセンスサーバー設定を適用できます。マスターイメージのRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳

しくは、「クライアントアクセスライセンス（CAL）を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには

1. 利用可能なVMのいずれかにRemote Desktop Servicesライセンスサーバーをインストールします。VMは常に利用可能である必要があります。Citrixサービスワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoft Group Policy を使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、「RD セッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。
3. Microsoft Remote Access から CAL ライセンスを購入した場合、ライセンスをインストールする必要はありません。Virtual Apps Essentials とともに、Azure Marketplace で Microsoft Remote Access からライセンスを購入できます。

RDS ライセンスサーバーを構成するには

1. Citrix Cloud にまだサインインしていない場合は、サインインします。左上のメニューで、 **>** を選択します。
2. タブで、 をクリックします。
3. カタログを選択し、 を選択します。
4. で、ライセンスサーバーの完全修飾ドメイン名を入力します。
5. をクリックします。

ユーザーを接続する

ストアエクスペリエンス

Citrix Cloud の Virtual Apps Essentials は、各顧客にストアエクスペリエンスを提供します。最初のカタログを作成すると、Virtual Apps Essentials はストア URL を自動的に構成します。この URL は、ユーザーがアプリケーションとデスクトップにアクセスできる URL です。ストア URL は、 タブのカタログ詳細パネルに表示されます。Virtual Apps Essentials は、オンプレミスの StoreFront 展開をサポートしていません。

カタログを作成した後、Citrix® StoreFront Cloud を使用して、ストア URL とストアの外観をカスタマイズできます。Microsoft Entra ID を使用したフェデレーション認証のプレビューバージョンを有効にすることもできます。

Microsoft Entra ID を使用したフェデレーション認証を有効にするには、次のタスクが含まれます。

- Microsoft Entra ID を ID プロバイダーとして設定します。詳細については、「Microsoft Entra ID を Citrix Cloud に接続する」を参照してください。
- クラウドストアへの認証のために Microsoft Entra ID を有効にします。

詳細については、StoreFront Cloudを参照してください。

Citrix Gatewayサービス

ユーザーが公開アプリケーションに安全にアクセスできるように、Virtual Apps EssentialsはCitrix Gatewayサービスを使用します。このサービスは、お客様による構成を必要としません。各ユーザーは、月あたり1GBの送信データ転送に制限されています。Azure Marketplaceから25GBのアドオンを購入できます。アドオンの料金は月単位です。

Virtual Apps Essentialsのキャンセル

Virtual Apps Essentialsにより、以下の要素でAzure料金が発生する可能性があります。

- Virtual Apps Essentialsサブスクリプション
- Virtual Apps Essentialsによって作成されたAzureリソース

Virtual Apps EssentialsサービスのMicrosoft Azure料金は月単位です。Virtual Apps Essentialsを購入すると、当月分の料金が請求されます。ご注文をキャンセルした場合、サービスは翌月には更新されません。Citrix Cloudを使用することで、当月末までVirtual Apps Essentialsへのアクセスを継続できます。

Azureの請求書には、Virtual Apps Essentialsに関する複数の明細が含まれる場合があります。

- Virtual Apps Essentialsサービスサブスクリプション
- Citrix Gatewayサービスアドオン（購入した場合）
- Microsoftリモートアクセス料金
- Virtual Apps Essentials使用時に作成されたAzureリソース

AzureでVirtual Apps Essentialsをキャンセルする

Virtual Apps Essentialsサブスクリプションをキャンセルするには、Azureポータルで注文リソースを削除します。

1. Azure portalにサインインします。
2. **すべてのリソース**をクリックします。

3. **種類**列で、Citrix Virtual Apps Essentials をダブルクリックして開きます。
4. ゴミ箱アイコンをクリックします。削除プロセスが開始されます。

Virtual Apps Essentials が作成した Azure リソースを削除する

Citrix Cloud で、アカウントに関連付けられているカタログとイメージを削除します。また、サブスクリプションリンクを削除し、Citrix Cloud から Cloud Connector VM が削除されていることを確認します。

Citrix Cloudにまだサインインしていない場合は、サインインします。左上のメニューで、**マイサービス > Virtual Apps and Desktops** を選択します。

カタログを削除するには

1. **管理**タブで、**カタログ**をクリックします。
2. 削除するカタログの横にある省略記号メニュー（...）で、**カタログの削除**を選択します。
3. 削除する各カタログに対して、前の手順を繰り返します。

マスターイメージを削除するには

1. **管理**タブで、**マスターイメージ**をクリックします。
2. イメージを選択し、**削除**をクリックします。
3. 削除する各マスターイメージに対して、前の手順を繰り返します。

Azureサブスクリプションへのリンクを削除するには

1. **管理**タブで、**サブスクリプション**をクリックします。
2. サブスクリプションの横にあるゴミ箱アイコンをクリックします。Azureポータルが開きます。
3. グローバル管理者Azure資格情報を使用して、Azureサブスクリプションにサインインします。
4. Virtual Apps EssentialsがAzureアカウントにアクセスすることを許可するには、**承諾**をクリックします。
5. サブスクリプションのリンクを解除するには、**削除**をクリックします。
6. 他のリンクされたAzureサブスクリプションについても、上記の手順を繰り返します。

Citrix Cloud Connector™ VMが確実に削除されるようにするには

1. 左上のメニューで、**リソースの場所**を選択します。
2. Cloud Connector VMを特定します。
3. Azureポータルにサインインします。

4. Azureのリソースページから VMを削除します。

パートナーリソース

このサービスは、Microsoft Cloud Solution Providerチャネルを通じて利用できるようになりました。詳細については、Citrix EssentialsのMicrosoft CSP有効化を参照してください。

ヘルプを見る

Virtual Apps Essentials で問題が発生した場合は、ヘルプとサポートの利用方法の手順に従ってチケットをオープンしてください。

詳細情報

- Virtual Apps Essentials環境でのCitrixポリシーの使用に関する情報については、CTX220345を参照してください。
- カタログ作成の失敗のトラブルシューティングを行うには、CTX224151を参照してください。

Citrix DaaS Standard for Azureへのアップグレード

Citrix Virtual Apps EssentialsからCitrix DaaS Standard for Azureへのアップグレードの方法を確認してください。

Citrix Virtual Desktops エッセンシャルズ™

> **注:**
>
> Citrix Virtual Apps EssentialsおよびCitrix Virtual Desktops Essentialsは、販売終了およびサポート終了となりました。詳細については、CTX583004を参照してください。

> Citrix Virtual Desktops™ Essentialsを使用すると、Microsoft AzureからWindows 10仮想デスクトップを管理および配信できます。

Virtual Desktops Essentialsは、Azure Marketplace向けに特別に設計されています。Citrix®とMicrosoftは提携し、Virtual Desktops EssentialsとAzure IaaS向けに統合されたエクスペリエンスを提供します。この提携により、単一のインターフェイスからAzureで完全なWindows 10デジタルストアを配信できます。

Virtual Desktops Essentialsを使用すると、次のことができます。

- Azure上でWindows 10仮想デスクトップを展開および保護する
- Citrix HDX™の機能を使用してクラス最高のユーザーエクスペリエンスを提供する
- Citrix Workspace™アプリを使用してあらゆるデバイスでセキュアなアクセスを提供する
- Microsoft AzureおよびCitrix Cloud™から展開を管理および運用する

Citrix Virtual Desktops Essentialsは、Windows 10の展開を簡素化します。単一の管理プレーンから、デスクトップを迅速に展開し、大規模に管理し、豊富なユーザーアクセスエクスペリエンスを提供できます。

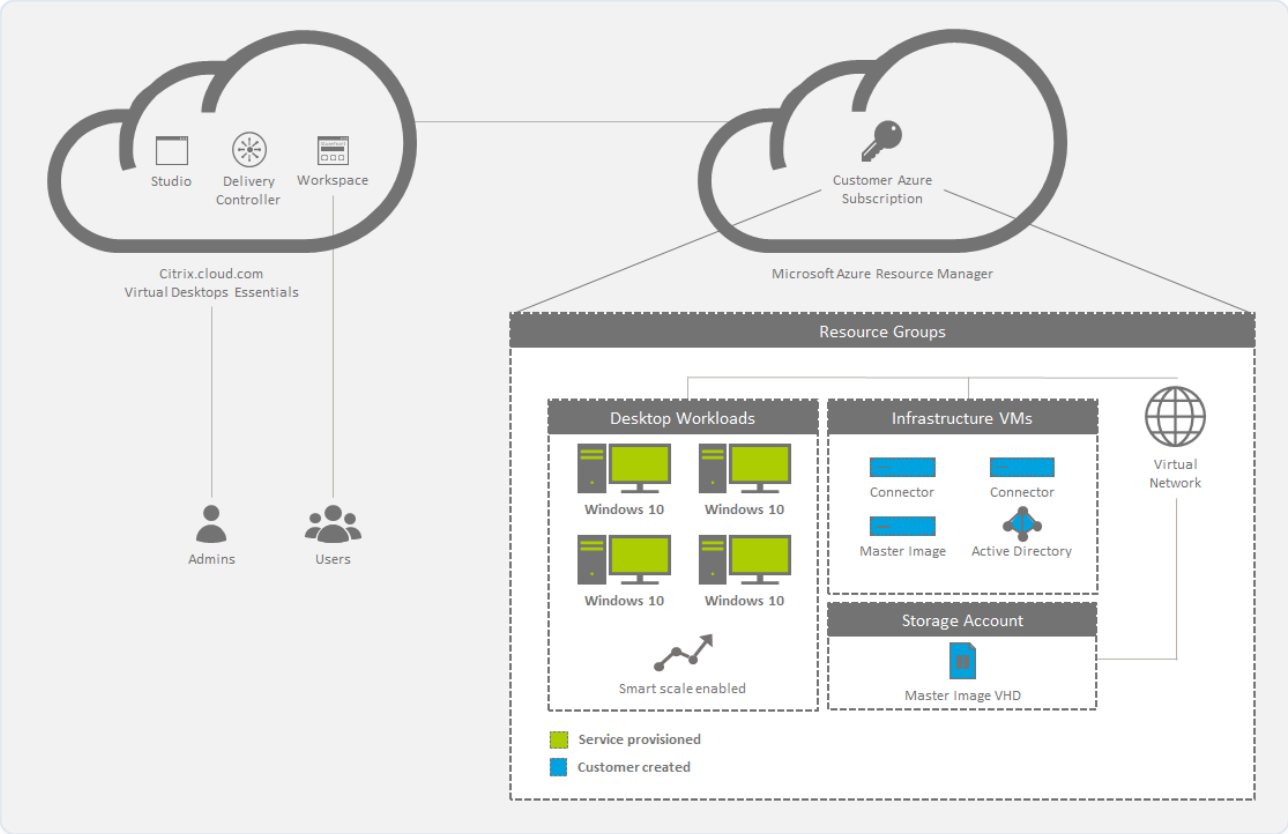
Studioを使用してWindows 10デスクトップを管理し、Directorを使用してセッションを監視します。ユーザーは、Citrix Workspaceアプリでログオンすることにより、Windows 10仮想デスクトップに接続します。

Citrix Virtual Desktops Essentialsを構成した後、ユーザーにCitrix® StoreFront CloudへのURLを提供します。ユーザーは、提供されたURLを使用して、デバイス上のCitrix Workspaceアプリを介してデスクトップに接続します。ユーザーがCitrix Workspaceアプリにログオンすると、ストアウィンドウにWindows 10デスクトップアイコンが表示されます。

> **重要:**
>
> Virtual Desktops EssentialsにはStoreFront Cloud URLが含まれており、通常、`https://<yourcompanyname>.cloud.com`の形式です。Virtual Desktops Essentialsをセットアップした後、ストアURLリンクをテストし、エンドユーザーと共有してデスクトップへのアクセスを許可します。Virtual Desktops Essentialsは、オンプレミスのStoreFrontをサポートしていません。

> ストアの詳細については、StoreFront Cloudを参照してください。

この図は、Virtual Desktops Essentials展開のアーキテクチャの概要を示しています。



新機能

2018年12月: **クラウドホスト型StoreFront™の削除**

クラウドホスト型StoreFrontは、Virtual Desktops Essentialsでは使用できなくなりました。2017年12月より前にVirtual Desktops Essentials（旧XenDesktop® Essentials）を購入されたお客様は、この記事で説明されているStoreFront Cloudを使用して、エンドユーザーにデスクトップへのアクセスを提供できます。

2018年8月: **新しい製品名**

Citrixのお客様またはパートナーとして長年ご利用いただいている場合は、当社の製品および製品ドキュメントに新しい名前があることにお気づきでしょう。このCitrix製品を初めてご利用になる場合は、製品またはコンポーネントに異なる名前が表示されることがあります。

新しい製品名とコンポーネント名は、Citrixの拡大するポートフォリオとクラウド戦略に由来しています。この記事では、以下の名前を使用します。

- **Citrix Virtual Desktops Essentials:** XenDesktopを業界のリーダーにしたテクノロジーは、現在Citrix Virtual Desktopsとなり、VDIを最新のコンテキスト対応のセキュアなアプリに導入し、すべての業務アプリケーションに安全にアクセスするための推奨される方法を提供します。XenDesktop Essentialsは現在Citrix Virtual Desktops Essentialsです。

- **Citrix Workspace app:** Citrix Workspaceアプリは、既存のCitrix Receiver™テクノロジーとその他のCitrix Workspaceクライアントテクノロジーを統合しています。最高の仕事をするために必要なすべての業務アプリ、ファイル、デバイスとやり取りできる、統合されたコンテキスト対応のエクスペリエンスをエンドユーザーに提供するために、追加機能が強化されています。
- **Citrix Gateway:** 最高の仕事をするために必要なアプリとデータへのセキュアでコンテキスト対応のアクセスを可能にするNetScaler® Gatewayは、現在Citrix Gatewayです。

製品内のコンテンツには、以前の名前がまだ含まれている場合があります。たとえば、コンソールテキスト、メッセージ、ディレクトリ/ファイル名に以前の名前のインスタンスがある場合などです。一部の項目（コマンドやMSIなど）は、既存の顧客スクリプトを破損させないために、以前の名前を保持し続ける可能性があります。

この製品のドキュメントからリンクされている関連製品ドキュメントやその他のリソース（ビデオやブログ投稿など）には、以前の名前がまだ含まれている場合があります。この移行期間中の皆様のご理解に感謝いたします。新しい名前の詳細については、`<https://www.citrix.com/about/citrix-product-guide.html>`を参照してください。

Virtual Desktops Essentialsの購入方法

Virtual Desktops Essentials の購入またはキャンセルに関する詳細については、Virtual Desktops Essentials Service の購入またはキャンセル方法 をダウンロードしてください。

システム要件、前提条件、および互換性

Virtual Desktops Essentials のインストール、構成、および操作には、特定の補完製品とコンポーネント、および特定のアカウント権限が必要です。

マイクロソフト Azure

Virtual Desktops Essentials は、Microsoft Azure のみをサポートするように設計されています。Virtual Desktops Essentials をサポートするには、Azure 環境が特定の最小要件を満たしている必要があります。

- エンタープライズ契約のある Azure サブスクリプション、または Microsoft CSP Azure サブスクリプション。
- Windows Server Active Directory または Microsoft Entra ID ドメイン サービス。
- Microsoft Entra ID テナント。

> **重要:**

> Microsoft は、Windows 10 デスクトップを展開するために、Azure サブスクリプションに Microsoft Entra ID テナントを要求します。承認されたユーザーを識別するために、Microsoft Entra ID テナントまたは別の Active Directory を使用できます。

- Active Directory ドメインコントローラー。
- 優先リージョンにある Azure Resource Manager (ARM) 仮想ネットワークとサブネット。仮想ネットワークを、ドメインコントローラーを指すカスタムドメインネームサーバー (DNS) エントリで構成します。仮想ネットワークには、デスクトップを収容するのに十分な大きさのサブネットが 1 つ必要です。

  DNS エントリとデスクトップサブネットには同じ仮想ネットワークを使用します。
- サブスクリプション内で共同作成者 (またはそれ以上) の権限を持つ Microsoft Entra ID ユーザー。
- Microsoft Windows 10 がインストールされ、必要なカスタマイズとアプリが含まれている仮想マシンが 1 台。

シトリックス クラウド コネクタ™

Citrix Cloud Connectorは、Citrix Cloudとリソースの場所の間で通信を認証し、暗号化します。Virtual Desktops Essentialsでは、リソースはMicrosoft Azureにあります。Citrix Cloudでは、リソースの場所の継続的な可用性を確保するために、2つのWindowsサーバーVMにCitrix Cloud Connectorをインストールする必要があります。

Cloud Connectorの詳細については、Citrix Cloud Connectorを参照してください。

シトリックス クラウド

- Citrix Cloudアカウント。
- Citrix Cloud内のCitrix DaaS™へのアクセス。これはVirtual Desktops Essentialsの購入の一部として有効になります。
- (オプション) 企業ネットワーク外からのアクセス用に、ICA®プロキシモードで構成された1つのNetScaler Console VPX。
  - ICAプロキシは、ユーザーに提供されるアプリケーションとデスクトップへの安全なアクセスを可能にします。
  - NetScaler Console VPXのセットアップについては、Microsoft AzureへのCitrix NetScaler VPXの展開を参照してください。

既知の問題

- Citrix Help Desk Administratorカスタムアクセスロールが正しく機能しません。回避策として、Cloud Administratorロールを使用するか、フルアクセスを有効にしてください。
- Microsoft Entra ID Domain Servicesを使用している場合: ログオンUPNには、Microsoft Entra ID Domain Servicesを有効にしたときに指定されたドメイン名が含まれている必要があります。作成したカスタムドメインのUPNは、そのカスタムドメインがプライマリとして指定されている場合でも、ログオンに使用できません。

ステップ1: AzureサブスクリプションをVirtual Desktops Essentialsに接続する

1. Azure portalにサインインします。
2. Azureで、ドメイン参加済みのWindows Server仮想マシンを開き、その後、Webブラウザを開きます。
3. VMのWebブラウザで、Citrix Cloudにサインインします。Citrix DaaSが開きます。
4. 左上のメニューから、**リソースの場所**を選択します。
5. **リソースの場所**ページで、**ダウンロード**をクリックします。ファイル`cwcconnector.exe`がダウンロードされます。
6. ダウンロードしたプログラムをダブルクリックして、インストーラーを起動します。
7. プロンプトが表示されたら、Citrix Cloudの資格情報を入力します。画面の指示に従って、Citrix Cloud Connectorをインストールおよび構成します。
8. 別のCloud Connectorをインストールするには、少なくともう1台のサーバーVMで手順4から7を繰り返します。

インストール中、Cloud ConnectorはCitrix Cloudにアクセスして認証を行い、インストーラーの権限を検証し、Cloud Connectorが提供するサービスをダウンロードして構成します。インストールは、インストールを開始したユーザーの権限を使用します。

インストール後、Citrix Cloudは**IDおよびアクセス管理**にドメインを登録します。詳細については、IDおよびアクセス管理を参照してください。

ステップ2：ホスト接続を作成する

開始する前に、Microsoft Entra IDの資格情報とサブスクリプションIDが利用可能であることを確認してください。ホスト接続を作成するMicrosoft Entra IDユーザーは、Microsoft Entra IDのネイティブクラウドユーザーであるか、エンタープライズドメイン用に同期されている必要がありま

す。ユーザーアカウントは、招待されたMicrosoftアカウントまたは委任されたMicrosoftアカウントであってはなりません。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、**マイサービス > Virtual Apps and Desktops**を選択します。
3. **管理**をクリックします。Studio管理コンソールが開きます。
4. Studioナビゲーションペインで、**構成 > ホスティング**を選択します。
5. アクションペインで、**接続とリソースの追加**をクリックします。
6. 「**接続とリソースの追加**」ページで、:
    a. 「**接続の種類**」で、「**Microsoft Azure**」を選択します。
    b. Azure環境で、「**Azure Global**」を選択し、「**次へ**」をクリックします。
7. 「**接続の詳細**」で、:
    a. 「**サブスクリプションID**」に、AzureサブスクリプションIDを入力します。
    b. 「**接続名**」に接続の名前を入力し、次のいずれかを実行します。
        i. 「**新規作成**」をクリックし、手順「オプション1：接続を作成する」に従います。
        ii. 「**既存を使用**」をクリックし、設定の構成を続行します。手順「オプション2：既存のホスト接続を使用する」に従います。

オプション1：接続を作成する

1. サブスクリプション共同作成者（またはそれ以上）のアカウントでAzureにサインインします。
2. Azureはホスト接続を自動的に作成します。Studioの「**接続とリソースの追加**」ページに、「**接続済み**」という単語と緑色のチェックマークが表示されます。
3. 「**次へ**」をクリックします。
4. 「**リージョン**」ページで、仮想ネットワークが存在するリージョンを選択し、「**次へ**」をクリックします。
5. 「**ネットワーク**」ページで、:
    a. リソースの名前を入力します。
    b. リソースグループの仮想ネットワークを選択します。
    c. リソースグループに適用されるサブネットを選択し、**次へ**をクリックします。

6. **概要**ページで、**完了**をクリックします。Microsoft Azure Resource Managerへのホスト接続が完了しました。

オプション2：既存のホスト接続を使用する

既存を使用をクリックすると、**既存のサービスプリンシパルの詳細**ページが表示されます。

1. **サブスクリプションID**に、Microsoft AzureサブスクリプションIDを入力します。
2. **サブスクリプション名**に、Azureサブスクリプションの名前を入力します。
3. **OK**をクリックします。
4. **接続**ページで：

    a. **新しい接続を作成**をクリックし、Microsoft AzureサブスクリプションIDと接続名（オプション）を入力して、**新規作成**をクリックします。Microsoft認証ダイアログボックスが表示されます。

    以前に作成した接続を使用する場合は、**既存の接続を使用**を選択します。次に、その接続を選択します。

    b. Microsoft Microsoft Entra ID ユーザーのユーザー名とパスワードを入力します。Citrix Cloud は、このサブスクリプションのマシンを作成および管理する権限を持つサービスプリンシパルを作成します。

5. **地域**ページで、Microsoft Azureリソースグループが配置されているAzure地域を選択します。
6. **ネットワーク**ページで：

    a. リソースの名前を入力します。接続名を入力した場合は、それをリソースの名前として使用します。

    b. Microsoft Azureリソースグループの仮想ネットワークを選択します。

    c. この接続に使用するサブネットを選択します。サブネットが1つしかない場合は、デフォルトで選択されます。

ステップ3：Windows 10デスクトップのプールを作成する

デスクトップをホストする準備として、Windows 10仮想マシンにCitrix Virtual Delivery Agent (VDA) ソフトウェアをインストールします。VDAは次の機能を提供します。

- マシンがVirtual Desktops Essentialsに登録できるようにします。
- マシンとユーザーデバイス間の接続を確立および管理します。
- ユーザーまたはセッションでCitrixライセンスが利用可能であることを確認します。

- セッションに設定されているポリシーを適用します。
- セッション情報をVirtual Desktops Essentialsに伝達します。

ベースイメージにVDAをインストールするには

1. Windows 10イメージを起動します。
2. https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.htmlにアクセスし、Desktop OS用VDAをダウンロードします。
3. VDAのインストールを開始します。
4. **Environment**ページで、**Create a master image using MCS**をクリックします。
5. **Additional Components**ページで、**Enable Citrix App-V**を除くすべてのコンポーネントを選択します。
6. 「**Delivery Controller™**」ページで、Cloud Connector仮想マシンの場所を入力します。「**次へ**」をクリックし、警告メッセージを確認します。
7. 「**機能**」ページで、デフォルト設定を維持し、「**次へ**」をクリックします。
8. 残りのページでデフォルト設定を受け入れるには、「**次へ**」をクリックします。
9. 「**概要**」ページで、「**インストール**」をクリックします。
10. 仮想マシンを再起動し、再度サインインします。
11. 設定が適用されたことを確認します。
12. 仮想マシンをシャットダウンします。仮想マシンのシャットダウンは、VDA登録に必要です。

ストレージアカウントを作成する

Microsoft Azureでは、ベースイメージの仮想ハードディスクをホストするためにストレージアカウントが必要です。既存のストレージアカウントにドライブをホストすることも、ストレージアカウントを新規作成することもできます。

> **重要:**
>
> マシンカタログを作成する前に、Windows 10マスターイメージをAzureの宛先ストレージアカウントにアップロードします。

イメージ用のストレージアカウントを作成するには

1. Microsoft Azureのナビゲーションペインで、「**ストレージアカウント**」をクリックします。
2. 「**ストレージアカウント**」ページで、「**追加**」をクリックします。

3. 「**名前**」に、名前を入力します。
4. 「**デプロイモデル**」で、「**リソースマネージャー**」を選択します。
5. 「**パフォーマンス**」で、「**標準**」を選択します。
6. 「**レプリケーション**」、「**ストレージサービス暗号化**」、および「**サブスクリプション**」については、既定の設定のままにします。
7. 「**リソースグループ**」で、次のいずれかをクリックします。
    a. 「**新規作成**」をクリックしてリソースグループを作成します。グループの名前を入力します。
    b. 「**既存のものを使用**」をクリックして既存のリソースグループを使用します。グループを選択します。
8. ストレージアカウントをダッシュボードに表示するには、「**ダッシュボードにピン留め**」をクリックします。
9. 「**作成**」をクリックします。

ストレージアカウントを作成したら、BLOBコンテナーを作成し、仮想ハードディスクを反映するように名前を付けます（例：「VHDs」）。

イメージVHD用のBLOBコンテナーを作成するには

1. Microsoft Azureのナビゲーションペインで、「**ストレージアカウント**」をクリックし、以前に作成したストレージアカウントに移動します。
2. 中央のナビゲーションペインで、「**BLOBサービス**」の下にある「**コンテナー**」をクリックします。
3. 詳細ペインで、「**コンテナー**」をクリックします。
4. 「**新しいコンテナー**」ペインで、コンテナーに名前を付けます。
5. 「**アクセスタイプ**」で「**BLOB**」を選択し、「**作成**」をクリックします。新しいBLOBコンテナーがペインに表示されます。
6. BLOB URLをコピーし、テキストファイルに保存します。このURLは、後で変換されたVHDをアップロードするために使用されます。

Citrix Virtual Desktops Essentials 用のマシンカタログを作成する

マシンカタログは、単一のエンティティとして管理する仮想デスクトップのコレクションです。これらの仮想デスクトップは、ユーザーに提供するリソースです。カタログ内のすべてのマシンには、同じオペレーティングシステムと、同じVDAがインストールされています。

通常、マスターイメージを作成し、それを使用してカタログ内に同一の仮想マシンを作成します。

1. Citrix Cloudにサインインします。左上のメニューで、**My Services > Virtual Apps and Desktops**を選択します。
2. **Manage**タブを選択します。
3. Studioナビゲーションペインで、**Machine Catalogs**をクリックします。
4. アクションペインで、**Create Machine catalog**をクリックします。
5. **Operating System**ページで、Desktop OSが唯一の利用可能なオプションです。これを選択し、**Next**をクリックします。
6. **Desktop Experience**ページで：
    a. **ユーザーがログオンするたびに同じ（静的）デスクトップに接続するようにする**を選択します。
    b. **はい、専用の仮想マシンを作成し、変更をローカルディスクに保存します**を選択します。
7. **Master Image**ページで：
    a. 以前に作成したBLOBストレージ内のVHDに移動して選択します。ナビゲーションツリーの構造は、Azureの階層に準拠しています。
        - リソースグループ
        - ストレージアカウント
        - コンテナ
        - 仮想ハードディスク (VHD)
        - イメージ名
    b. 「**Select the minimum functional level for this catalog**」でデフォルトの選択を維持します。
8. 「**Storage and License Types**」ページで、宛先ストレージの種類とライセンス設定を選択します。
9. 「**Virtual Machines**」ページで、仮想マシンの数とAzure仮想マシンのサイズを選択します。
10. 「**Network Interface Cards**」ページで、Citrixマシン用のAzureサブネット名に関連付けるネットワークアダプターを選択します。「**Add Card**」をクリックして、別のネットワークアダプターを追加することもできます。
11. 「**Computer Accounts**」ページで:

a. 「**Create new Active Directory accounts**」をクリックします。

b. コンピューターアカウントのドメインを選択します。

c. 新しいマシンの組織単位 (OU) に移動します。

d. 新しいマシンのアカウント命名スキームを入力します。数字を自動的に増やすには、2つのシャープ記号 (##) を含めます。数字または文字を選択します。シャープ記号は命名スキームに変換されます。たとえば、mymachcatalog## は mymachcatalog01 または mymachcatalogAB になります。

12. 「**Domain Credentials**」ページで「**Enter Credentials**」をクリックし、次に「**Windows Security**」ダイアログボックスでユーザー名とパスワードを入力します。このアカウントはコンピューターアカウントの作成に使用されます。
13. 「**Summary**」ページで、カタログの名前と管理者向けの記述を入力します。
14. 「**完了**」をクリックします。

仮想マシンが作成され、新しいストレージアカウントがMicrosoft Azureダッシュボードに表示されます。マシンカタログサービスが仮想マシンを展開している間、VHD を持つ準備用仮想マシンが Azure に一時的に作成されます。

Microsoft Azure でイメージ名を識別するには

1. Azure portalにサインインします。
2. ダッシュボードナビゲーションペインで、「**すべてのリソース**」をクリックします。サブスクリプションのリストが表示されます。
3. サブスクリプションを選択します。
4. 「**すべての設定**」をクリックします。
5. 「**リソースグループ**」をクリックします。
6. リソースグループを選択します。
7. Citrix VDA を含む Windows 10 仮想マシンを選択します。
8. 「**すべての設定**」をクリックします。
9. 「**ディスク**」をクリックします。
10. OS ディスクを選択します。OS ディスクウィンドウの最初のテキストボックスには、次の例に示すように構成されたイメージの URL が含まれています。URL からストレージアカウント名とイメージ名を取得できます。例: `https://<storage account name>.blob.core.window.net/vhds/<image name>`。

11. 「**マシン**」ページでは、一覧表示されているテンプレートが Azure サブスクリプションから直接取得されます。

ステップ 4: Windows 10 デスクトップをユーザーに割り当てる

デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンを使用できるかを指定します。

1. Studioのナビゲーションペインで**を選択し、アクションペインで**を選択します。
2. デリバリーグループで利用可能にするマシンの数を指定します。指定する数は、マシンカタログで利用可能なマシンの数を超えることはできません。
3. **ページで、**を選択します。
4. ****ページで、ユーザー管理をCitrix Cloudに任せるオプションを選択します。このオプションを選択すると、Citrix Cloudを使用して、デリバリーグループ内のマシンにアクセスできるユーザーを管理できます。（Studioからユーザーを追加することもできます。）
5. ****ページで、デリバリーグループの名前と（オプションで）説明を入力します。

これらの手順を完了したら、デリバリーグループを編集してユーザーのアクセスを設定します。ユーザーの追加または削除、およびユーザー設定の変更が可能です。

Studioを介してデリバリーグループのユーザーを追加または削除する

1. Studioのナビゲーションペインで****を選択します。
2. グループを選択し、アクションペインで****をクリックします。
3. **ページで、ユーザーを追加するにはをクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**をクリックします。認証されていないユーザーによるアクセスを有効または無効にするチェックボックスを選択またはクリアすることもできます。
4. ****をクリックします。

Studioを介してデリバリーグループのユーザー設定を変更する

このページの名前は、**または**のいずれかで表示されることがあります。

1. Studioのナビゲーションペインで****を選択します。
2. グループを選択し、 ペインで**デリバリーグループの編集**をクリックします。
3. **ユーザー設定** (**基本設定**または) ページで:
    a. **説明**に、ストアがユーザーに表示するテキストを入力します。

b. タイムゾーンをAzureのタイムゾーンと一致するように設定します。

c. **デリバリーグループを有効にする**を選択します。

d. ユーザーごとのデスクトップの最大数を設定します。

4. **OK**をクリックして設定を保存します。

Citrix Cloudを介してユーザーアクセスを追加する

1. Citrix Cloudにサインインし、**ライブラリの表示**をクリックします。
2. デスクトップタイルで、右隅にある省略記号（...）をクリックします。
3. デリバリーグループへのアクセスが許可されているユーザーグループを検索し、それらをリストに追加します。
4. 完了したら、**X**をクリックしてウィンドウを閉じます。

Windows 10仮想デスクトップは、エンドユーザーリストに追加されたグループに割り当てられます。

ステップ5: AzureでNetScaler Console VPXを構成する (オプション)

NetScaler Console VPX仮想アプライアンスは、Microsoft Azure Marketplaceでイメージとして利用できます。Microsoft Azure Resource ManagerにNetScaler Console VPXを展開すると、Azureのクラウドコンピューティング機能を使用できます。ビジネスニーズに合わせて、Citrix Gatewayの負荷分散およびトラフィック管理機能を使用できます。

NetScaler Console VPXインスタンスは、Azure Resource Managerに次の2つの方法のいずれかで展開できます。

- スタンドアロンインスタンス。
- アクティブ/アクティブモードまたはアクティブ/スタンバイモードの高可用性ペア。

リモートロケーションから接続するユーザーがいる場合は、AzureでNetScaler Console VPXを構成して、Citrix WorkspaceアプリとWindows 10デスクトップ間のセキュアな接続を作成します。

展開が完了したら、リモートデスクトッププロトコル（RDP）を使用してCloud Connectorマシンのいずれかに接続します。接続すると、Citrix Gateway管理コンソールからNetScaler Console VPXの構成に進みます。

完全な構成情報については、「Microsoft AzureへのNetScaler Console VPXインスタンスの展開」を参照してください。

AzureでNetScaler Console VPXを構成したら、Citrix CloudでCitrix Gatewayを有効にします。

セキュアなアクセス用にCitrix Gateway設定を構成するには

1. Citrix Gateway管理者資格情報を使用して管理コンソールにログオンします。追加のIPアドレスを構成する必要はありません。「**スキップ**」をクリックします。
2. **ホスト名**、**DNS IPアドレス**、および**タイムゾーン**には、仮想ネットワークのIPアドレスとDNS設定を使用します。設定はActive Directoryドメインコントローラーにあります。
3. 「**完了**」をクリックします。NetScaler Console VPXを今すぐ再起動する必要はありません。
4. 「構成」タブで「**ライセンス**」をクリックし、Citrix Gatewayを構成するために必要なライセンスをアップロードします。
5. ライセンスのアップロード後、アプライアンスを再起動します。
6. 仮想マシンが再起動したら、Citrix Gateway資格情報を使用して再度ログオンします。

Citrix GatewayでCitrix Virtual Desktops Essentials設定を構成する

以前の設定を構成したら、Citrix Gateway でクイック構成ウィザードを実行します。詳しくは、「クイック構成ウィザードを使用した設定の構成」を参照してください。

高可用性と負荷分散のためにCitrix Gatewayを構成する

Microsoft Azure展開では、2つのCitrix Gateway仮想マシンの高可用性構成は、Azureロードバランサーを使用して実現されます。ロードバランサーは、両方のCitrix Gatewayインスタンスで構成された仮想サーバー間でクライアントトラフィックを分散します。

クライアントトラフィックがインターネットから発信される場合は、インターネットとCitrix Gatewayインスタンスの間に外部ロードバランサーを展開して、クライアントトラフィックを分散します。この構成の詳細については、「単一IPアドレスと単一NICによる高可用性セットアップの構成」を参照してください。

Citrix GatewayのパブリックIPアドレスを使用してCitrix Gatewayを構成するために、インバウンドポート80を追加することもできます。構成が完了したら、インバウンドポート80ルールを削除して、管理コンソールへのアクセスを保護できます。

手順6：ユーザーを接続する

StoreFront Cloudは、ユーザーデバイスにサービスを提供します。Citrix Cloudコンソールで、左上のメニューから **StoreFront Cloud** を選択します。

最初のカタログを作成すると、Virtual Desktops EssentialsによってストアURLが自動的に構成されます。このURLはカタログの詳細の下に表示されます。ストアURLとストアの外観をカスタマイ

ズできます。Microsoft Entra ID を使用したフェデレーション認証のプレビューバージョンを有効にすることもできます。詳細については、「StoreFront Cloud」を参照してください。

1. Citrix Cloudコンソールで、左上のメニューから **StoreFront Cloud** を選択します。**Service Integrations** タブを選択します。サービスが一覧表示されます。
2. ドメイン資格情報を使用してストアURLにログオンし、デスクトップを起動して接続をテストします。
3. ユーザーにURLを提供し、ユーザーはそれをコピーできます。ユーザーは、ブラウザまたはCitrix Workspaceアプリのアドレスバーにそのを入力または貼り付けて、デスクトップにアクセスできます。

NetScaler Console VPX を使用したリモートアクセス

1. Citrix Cloudコンソールで、**Manage** をクリックし、次に **Service Delivery** をクリックします。
2. **Citrix Gateway** を有効にします。
3. リソースの場所で **Use your own Citrix Gateway** を選択します。
4. テキストフィールドにCitrix Gatewayのアドレスを入力します。プロトコルは含めないでください。ポート番号を含めることはできます。
5. この機能が必要な場合は、セッションの信頼性を有効にします。
6. 保存します。
7. ドメイン資格情報を使用してストアURLにログオンし、デスクトップを起動して接続をテストします。
8. ユーザーにURLを提供します。ユーザーはそのURLをコピーできます。ユーザーは、ブラウザーまたはCitrix Workspaceアプリのアドレスバーにを入力または貼り付けて、デスクトップにアクセスできます。

パートナーリソース

このサービスは、Microsoft Cloud Solution Providerチャネルでも利用できます。詳しくは、「Microsoft CSP enablement for Citrix Essentials」を参照してください。

Citrix DaaS Standard for Azureへのアップグレード

Citrix Virtual Desktops EssentialsからCitrix DaaS Standard for Azureにアップグレードする方法について説明します。

Citrix エッセンシャルズ向け Microsoft CSP の有効化

Citrix Virtual Apps Essentials および Citrix Virtual Desktops Essentials™ Service は、Microsoft Cloud Solution Provider チャネルを通じて利用できるようになりました。Microsoft Cloud Solution Provider として、お客様に代わって Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials を購入できます。Citrix Service Provider として、Citrix Cloud Partner アカウントにアクセスでき、お客様向けに新しい Citrix Cloud アカウントを作成できます。(Citrix Service Provider パートナーでない場合は、お客様が自身の Citrix Cloud アカウントへのアクセスを許可する必要があります。)

この記事全体を通して、*Citrix Essentials* は Citrix Virtual Apps Essentials™ または Citrix Virtual Desktops Essentials を指します。例とスクリーンショットは Citrix Virtual Apps Essentials を示しています。

新機能

製品名の変更:

- XenApp Essentials は **Citrix Virtual Apps™ Essentials** になりました。
- XenDesktop エッセンシャルズ は **Citrix Virtual Desktops™ エッセンシャルズ** になりました。

他のサイトや情報源には、以前の名称が含まれている場合があります。たとえば、この記事のいくつかのスクリーンショットには以前の名称が示されています。この移行期間中の皆様のご理解に感謝いたします。製品名の変更に関する詳細については、`<https://www.citrix.com/about/citrix-product-guide.html>` を参照してください。

要件

- Citrix Cloud パートナーアカウント: Citrix Service Provider である必要があります。
- Microsoft Azure アカウント: Microsoft Cloud Solution Provider (ティア 1 またはティア 2) であり、Microsoft Partner Center へのアクセス権が必要です。

手順の概要

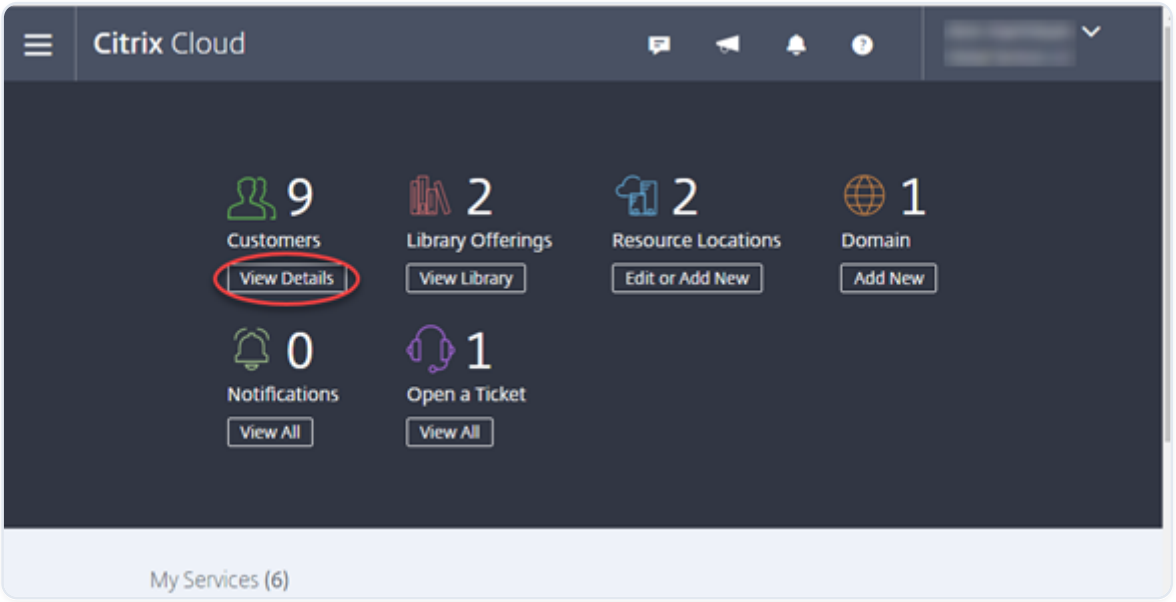
- Citrix Cloud™ から、お客様の Citrix Cloud アカウントを作成します。お客様がすでに Citrix Cloud アカウントをお持ちの場合は、この手順をスキップしてください。ただし、Citrix Essentials サービスを購入する際には、それらのアカウント詳細が必要になります。

- Microsoft Partner Center ポータルから、お客様の Azure サブスクリプションを作成します。お客様がすでに Azure サブスクリプションをお持ちの場合は、この手順をスキップしてください。
- Azure Marketplace から、お客様向けに Citrix Essentials サービスを購入します。

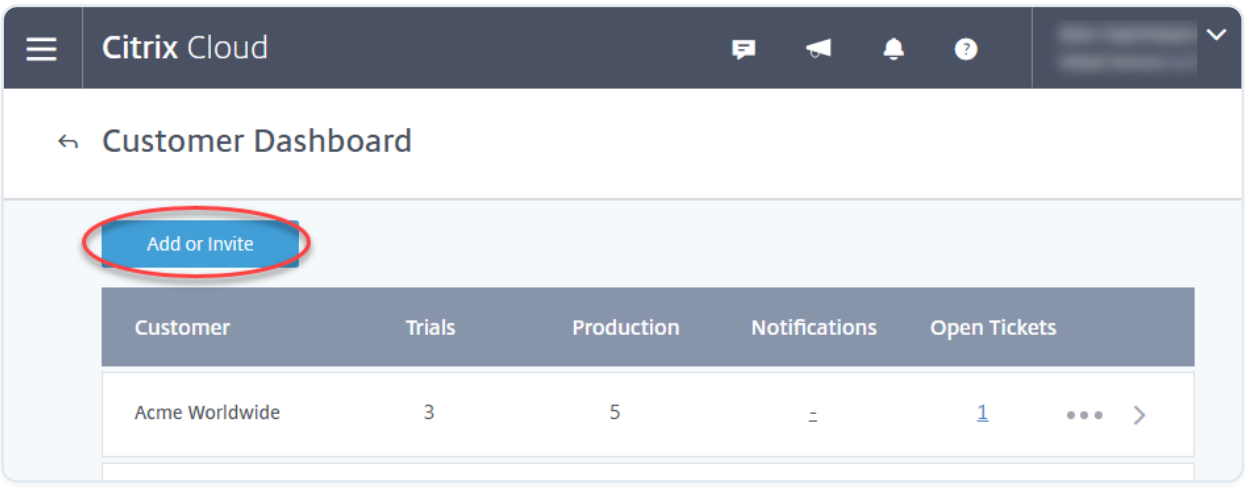
この記事で概説されているタスクを完了したら、Citrix Cloudから環境を展開します。詳細については、Essentials製品ドキュメントを参照してください。

顧客のCitrix Cloudアカウントを作成する

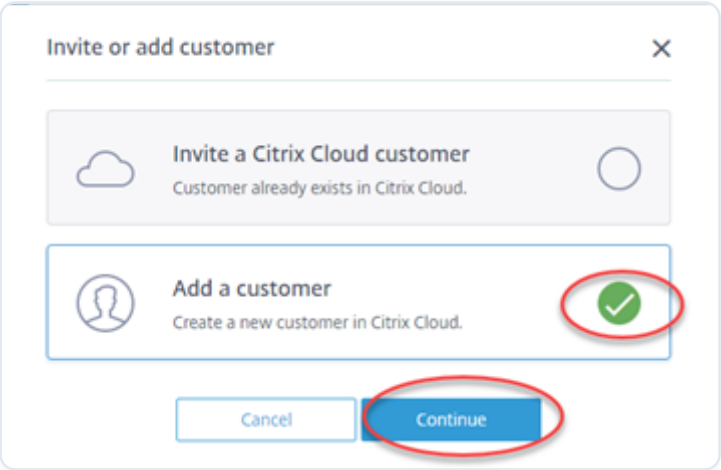
1. Citrix Cloudパートナーアカウントの資格情報を使用して、Citrix Cloudにサインインします。
2. **Customers**の下で、**View Details**をクリックします。



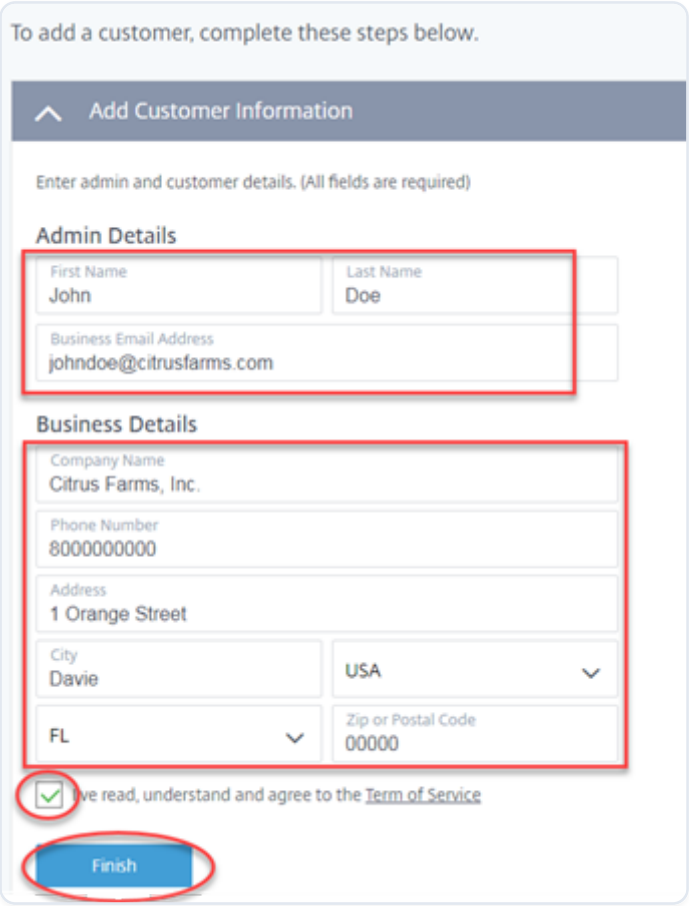
3. **Customer Dashboard**ページで、**Add or Invite**をクリックします。



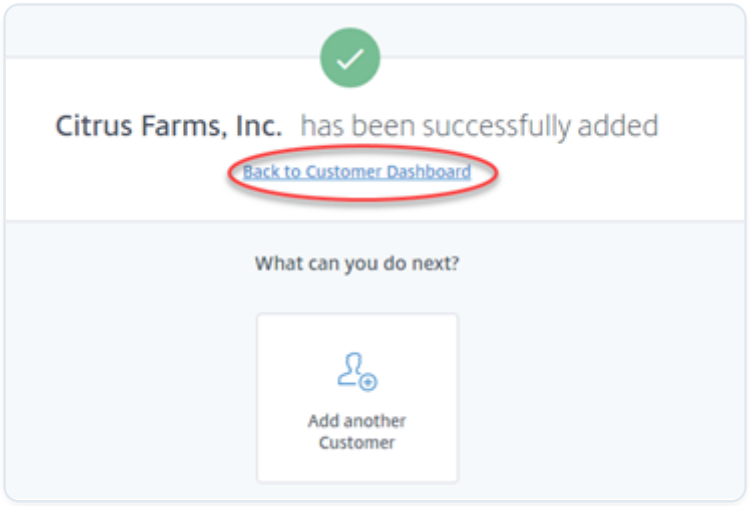
4. **Invite or add customer**ページで、**Add a customer**を選択し、**Continue**をクリックします。



5. 管理者とビジネスの詳細を入力します。すべてのフィールドは必須です。利用規約を確認し、確認チェックボックスを選択します。その後、**Finish**をクリックします。

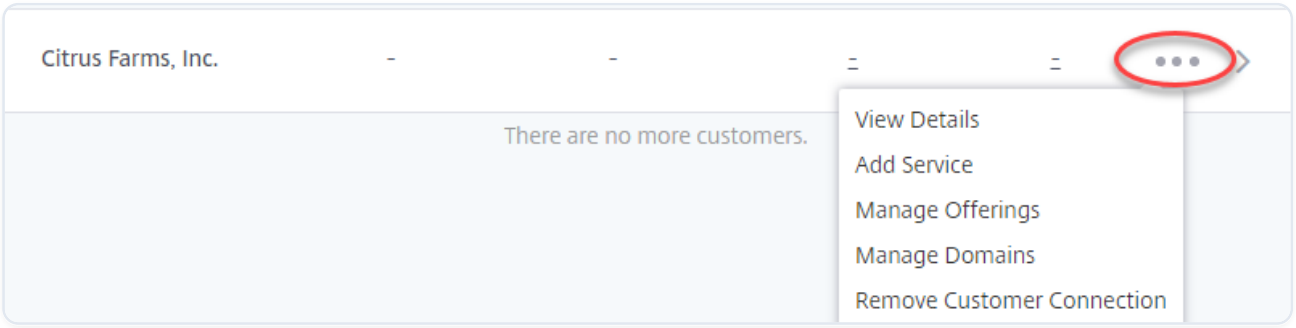


6. 顧客が正常に追加されたら、**Back to Customer Dashboard**を選択します。



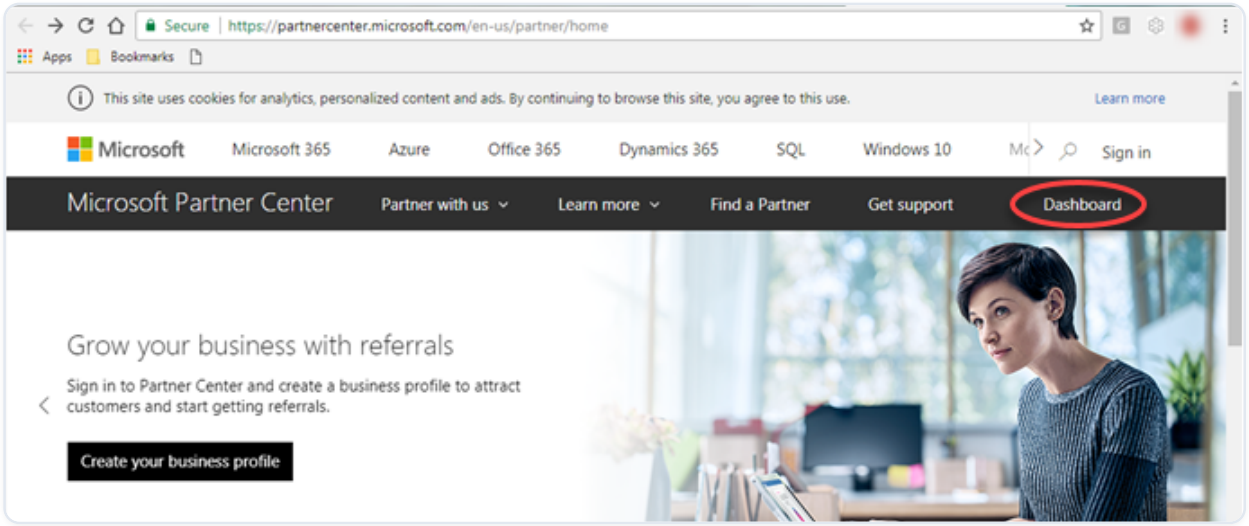
結果

Customer Dashboardに、追加した顧客が表示されるようになりました。顧客行の省略記号を選択すると、後で使用できるアクションメニューが表示されます。

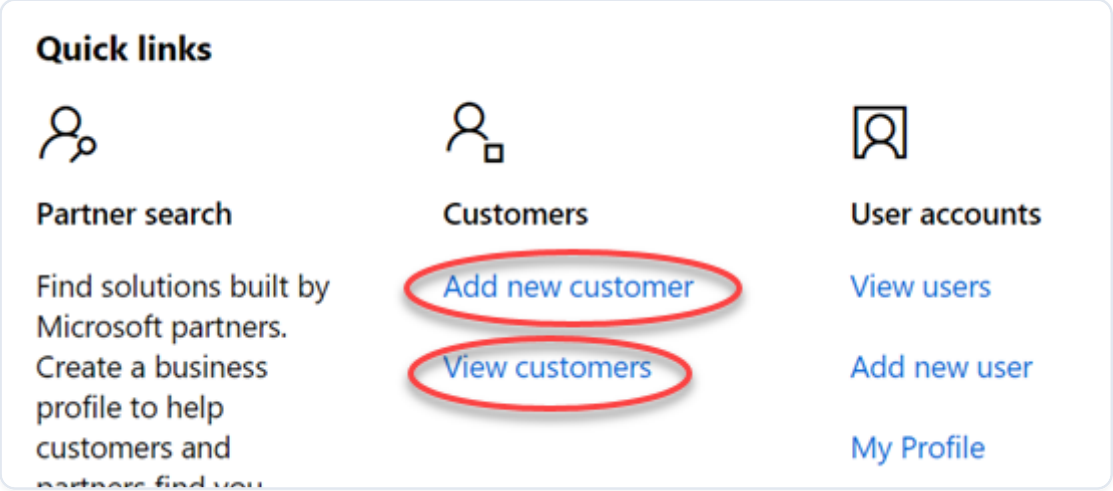


顧客のAzureサブスクリプションを作成する

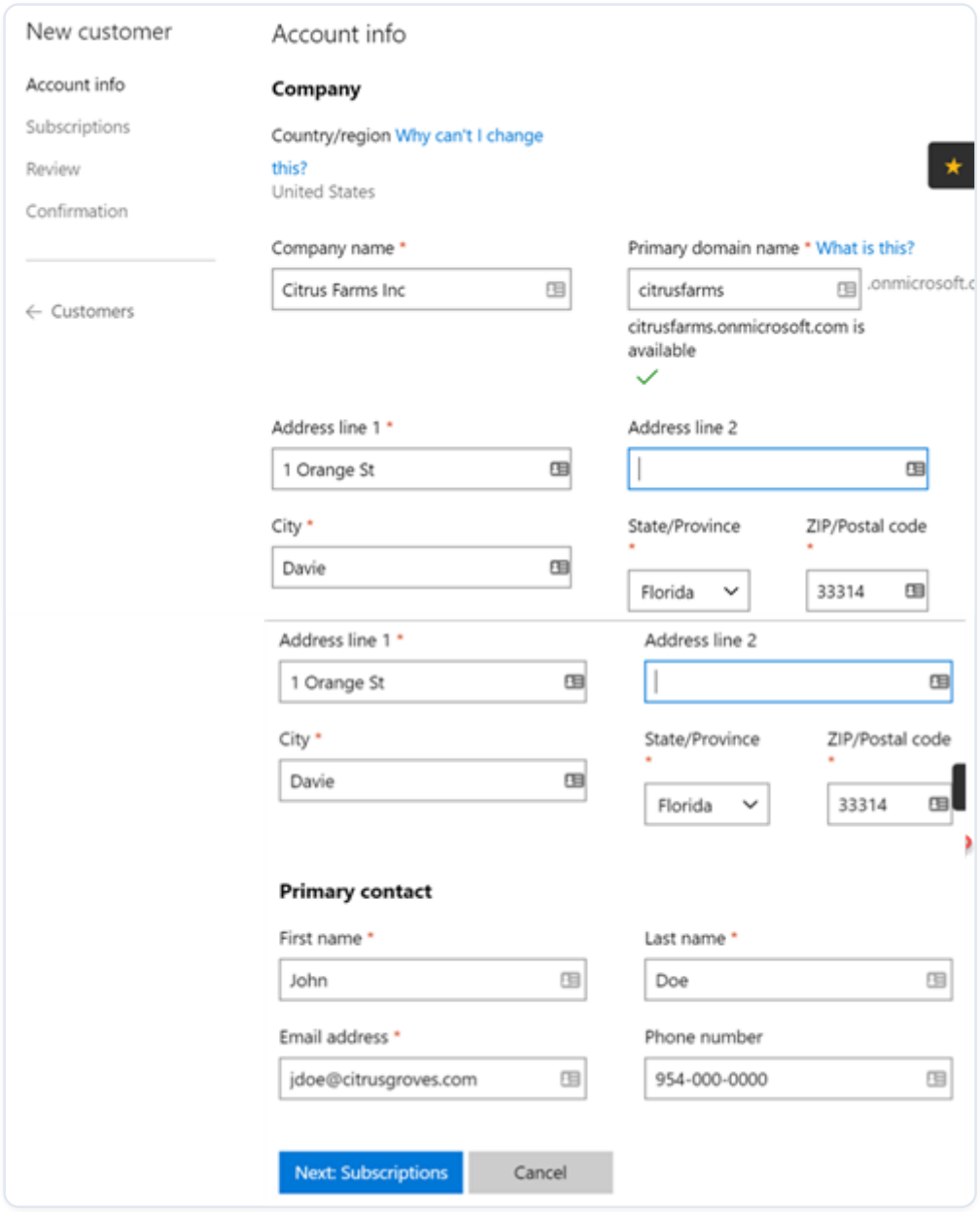
1. Microsoftアカウントの資格情報を使用して、Microsoft Partner Centerにサインインします。複数のCSPアカウントをお持ちの場合は、使用するアカウントを選択してください。
2. Partner Centerのホームページで、**ダッシュボード**をクリックします。



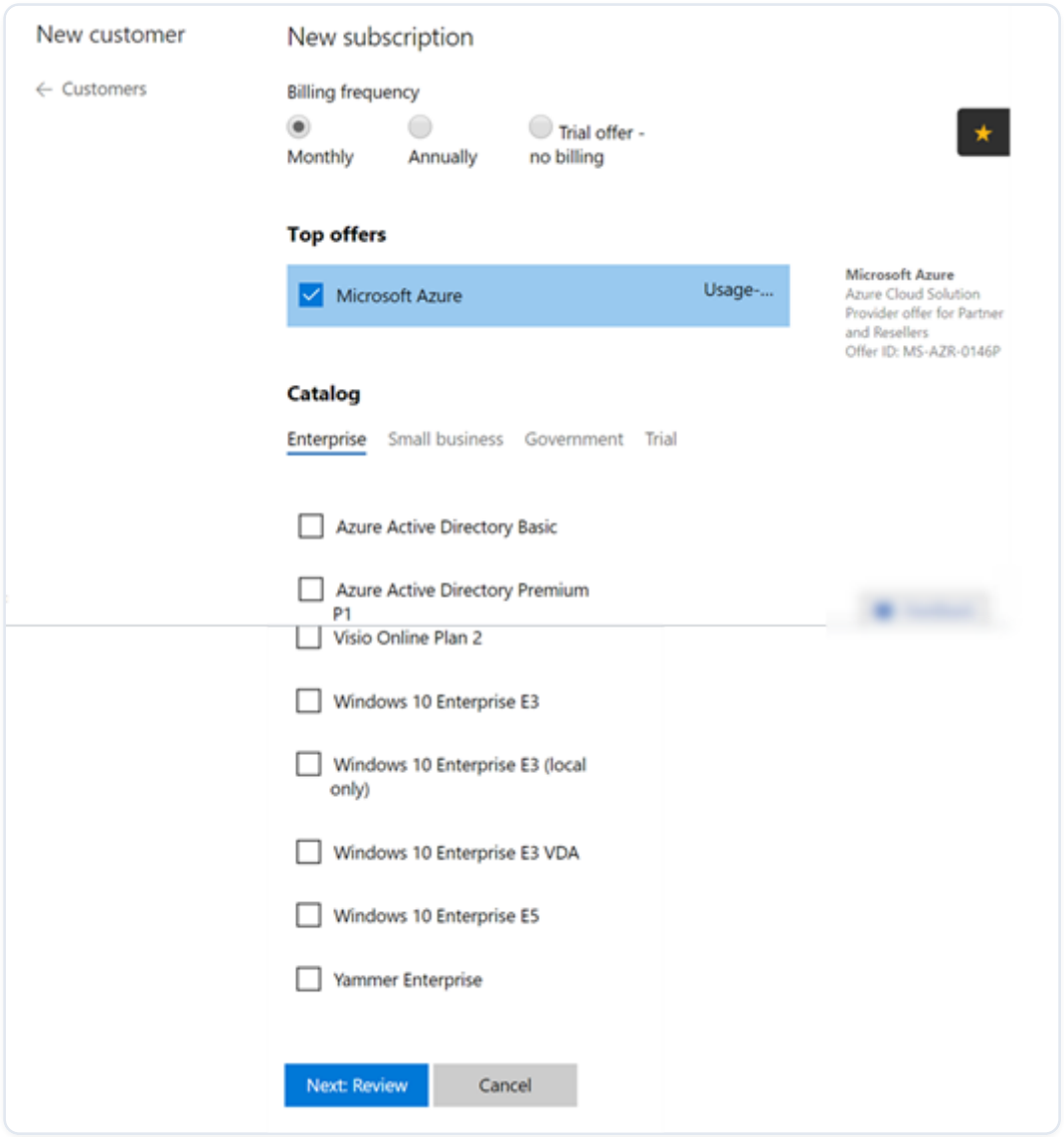
3. ダッシュボードの概要ページの**クイックリンク**セクションで、顧客を追加する場合は、**新しい顧客の追加**をクリックします。顧客がすでに存在する場合は、**顧客の表示**をクリックします。



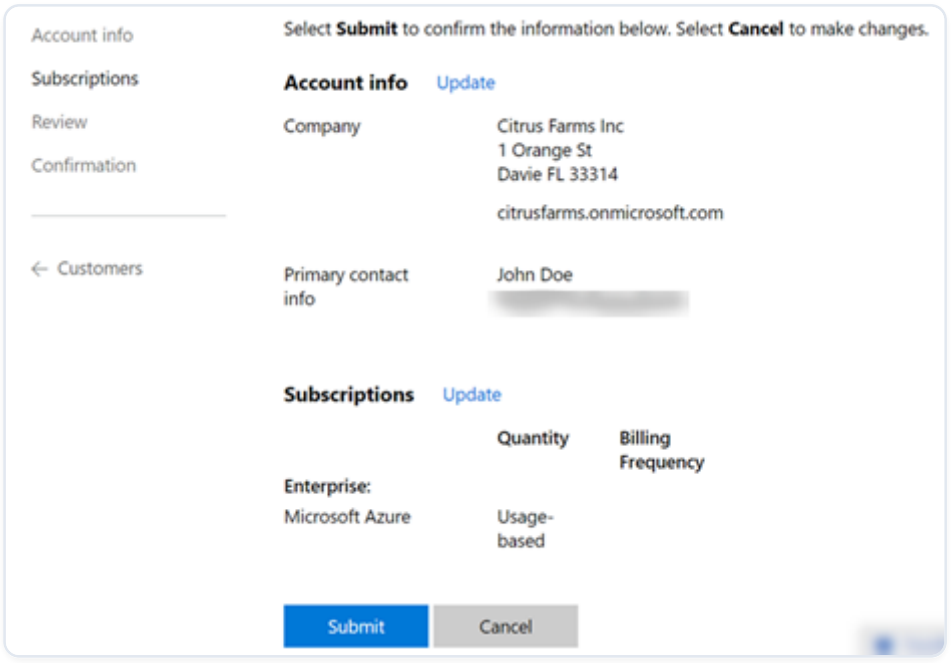
4. 顧客がすでに存在する場合は、顧客名の右側にあるクイックリンクメニューで、**サブスクリプションの表示**を選択します。顧客がMicrosoft Azureサブスクリプションを持っていない場合は、**サブスクリプションの追加**をクリックして、手順6に進みます。顧客がすでにMicrosoft Azureサブスクリプションを持っている場合は、このセクションの残りの部分をスキップして、顧客向けにCitrix Essentialsサービスを購入するに進みます。
5. 顧客を追加する場合は、**アカウント情報**ページで、会社名、ドメイン名、住所、連絡先の詳細を入力します。次に、**次へ: サブスクリプション**をクリックします。



6. **新しいサブスクリプション**ページで、請求頻度、**Microsoft Azure**のトップオファー、およびカタログタイプを選択します。次に、**次へ: レビュー**をクリックします。



7. **レビュー**ページで、情報が正しいことを確認します。次に、**送信**をクリックします。



8. **重要: 確認**ページからセットアップ情報（Microsoft ID、管理者ユーザーアカウント、パスワード）をコピーしてください。このページを離れると、パスワードを再度表示することはできません。

セットアップ情報をコピーしたら、左ペインで「**Customers**」を選択します。

顧客リストに戻る(/en-us/citrix-cloud/media/ms-newcustomer-confirm-60.png)

結果

「**Customers**」ページに、追加した顧客が表示されます。

顧客リストの新しいエントリ(/en-us/citrix-cloud/media/ms-customers-60.png)

「**Subscriptions**」ページに、追加した顧客に対して選択したサブスクリプションが表示されます。

サブスクリプションリストの新しいエントリ(/en-us/citrix-cloud/media/ms-subscriptions-60.png)

顧客向けにCitrix Essentialsを購入する

1. Microsoft Partner Centerにまだサインインしていない場合は、今すぐサインインしてください。
2. 「**Subscriptions**」ページで、「**Service management**」をクリックします。このページには、サービスの管理ポータルが一覧表示されます。「**Azure Management**」ポータルをクリックします。
3. 左ペインで「**New**」をクリックします。検索フィールドにCitrix Essentialsサービス名を入力し始めます。たとえば、「**Citrix Virtual Apps Essentials**」です。「**Results**」の下で、適切なエントリを選択します。たとえば、「**Citrix Virtual Apps**」です。

   Citrix Virtual Apps Essentialsを検索して選択する(/en-us/citrix-cloud/media/ms-xae.png)
4. 「**Create**」をクリックします。

   Citrix Virtual Apps Essentialsを作成する(/en-us/citrix-cloud/media/ms-xae-create-60.png)
5. 次の構成を完了し、「**Connect**」をクリックします。

   - **リソース名:** 認識しやすい名前を入力します。将来的にCitrix Essentialsサービスをキャンセルする場合、この名前を使用します。このリソースはCitrix Essentialsサービスの注文のみを表します。Azureでこのリソースを削除すると、Citrix Essentialsサービスのサブスクリプションがキャンセルされます。）」
   - **サブスクリプション:** 顧客のMicrosoft Azureサブスクリプションを選択します。

- **リソースグループ:** リソースグループを作成します。（デフォルトでは、このページで「既存を使用」が選択されています。このサブスクリプションと顧客に対して既にリソースグループがある場合は、それを選択します。そうでない場合は、新しいものを作成します。）」
- **場所:** リソースの場所を選択します。

  Citrix Virtual Apps Essentialsの構成と接続(/en-us/citrix-cloud/media/ms-xae-connect-60.png)

Citrix Cloudサインインページに自動的に移動します。

6. Citrix Cloudの資格情報を入力し、**サインイン**をクリックします。Microsoft Azureは資格情報を確認し、Azureポータルに戻ります。

Citrix Cloudドキュメント履歴

次の表に、Citrix Cloud製品のドキュメントに対する重要な変更点を示します。 これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
29 Jan 2025	サービスプリンシパル情報を追加	新しいセクション「サービスプリンシパル」を追加しました
16 Dec 2024	条件付き認証の新機能を追加	新機能条件付き認証を追加しました
27 Sep 2024	新しいセクション「新しい顧客を登録する」を追加	新しいセクション「新しい顧客を登録する」を追加しました
17 Sep 2024	アカウント管理セクションを更新	ライセンス管理の「アカウント管理」を更新しました
13 Sep 2024	新しいセクション「高度なトラブルシューティングのためのパケットキャプチャ機能」を追加	新しいセクション「高度なトラブルシューティングのためのパケットキャプチャ機能」を追加しました
10 Jun 2024	新しい記事を追加	新しい記事「Workspace認証でゲスト用のAzure AD IDとB2B IDを使用するSAML」を追加しました
29 Apr 2024	2つの新しいセクションを追加	「サービスプロバイダーSAML署名証明書の更新」と「IDプロバイダーのSAML署名証明書の更新」を追加しました

日付	変更	説明
08 Apr 2024	新しいセクション「ユーザーがCitrix Cloudアカウントを削除して再登録できる」を追加	新しいセクション「ユーザーがCitrix Cloudアカウントを削除して再登録できる」を追加
22 Mar 2024	新しいセクションを追加	新しいセクションを追加しました オンプレミスのPingFederateサーバーをWorkspaceとCitrix CloudのSAMLプロバイダーとして構成
19 Mar 2024	新しい注を追加しました	「ライブラリを使用してサービスオファリングにユーザーとグループを割り当てる」に新しい注を追加しました
14 Mar 2024	カスタムランディングページセクションを追加	新しいセクションを追加しました カスタムランディングページ
28 Feb 2024	NetScaler App Delivery and Security Service - Citrix管理を削除	「サービスレベルアグリーメント」から「NetScaler App Delivery and Security Service - Citrix管理」を削除しました
27 Feb 2024	使用状況収集セクションを更新	「使用状況収集」にユーザー顧客のタグ付け、無料サーバーのタグ付け、およびサーバー顧客のタグ付けに関するサブセクションを追加しました
19 Feb 2024	さらに証明書を追加	「証明書の検証要件」にCitrix DaaSの証明書をさらに追加しました
02 Feb 2024	新しいSAML IDプロバイダーの記事	新しい記事を追加しました：ワークスペース認証でAzure AD IDとAD IDを使用するSAML

日付	変更	説明
31 Jan 2024	サポートされているサービスを更新	「サポートされるサービス」のCitrix Application Delivery Managementサービスを NetScalerコンソールに変更しました
31 Jan 2024	新しいサービスとして License Usage Insightsサービスを追加	「サポートされるサービス」に新しいサービスとして License Usage Insightsを追加しました
23 Jan 2024	Citrix IDプロバイダーを追加	「IDおよびアクセス管理」にCitrix IDプロバイダーのセクションを追加しました
20 Dec 2023	「Citrix App Delivery and Security Service - Citrix管理」を削除	「地理的考慮事項」の「Citrix App Delivery and Security Service - Citrix管理」への参照を削除しました
20 Dec 2023	Citrix App Delivery and Security Serviceを削除	「Citrix Cloudでスコープ付きエンティティIDを使用したSAMLアプリケーションを構成する」からCitrix App Delivery and Securityサービスを削除しました
30 Nov 2023	IDプロバイダーとしてのSAMLに関する新しい機能	スコープ付きエンティティIDのサポートについて説明する新しい記事を追加しました：Citrix Cloudでスコープ付きエンティティIDを使用したSAMLアプリケーションを構成する
16 Nov 2023	Directory.Read.Allへの参照を削除しました	Directory.Read.Allへの参照がAzure ADとCitrix Cloud間のデフォルト接続から削除されました Citrix Cloud用のAzure Active Directoryの権限

日付	変更	説明
20 Oct 2023	ShareFileの参照を削除しました	ShareFileおよびCitrix Filesへの参照は、これらのサービスをCitrix Cloudから切り離すため削除されました：FAQ: Decouple your ShareFile account from your Citrix Workspace
19 Oct 2023	IDプロバイダーとしてのSAMLに関する新しい記事	OktaをSAMLプロバイダーとして使用してSAML認証を構成するための新しい記事を追加しました：Oktaをワークスペース認証用のSAMLプロバイダーとして構成する
18 Sep 2023	DaaS Standard for Azureライセンスの新機能	ユーザー/デバイスライセンスモデルでドメイン名の切り捨てがサポートされるようになりました：Citrix DaaS Standard for Azureのライセンスと使用状況の監視
18 Sep 2023	DaaSライセンスの新機能	ドメイン名の切り捨てがサポートされるようになりました：Citrix DaaSのライセンスおよびアクティブな使用状況の監視（ユーザー/デバイス）
07 Sep 2023	新しいSAML IDプロバイダーの記事	Azure ADベースのIDを使ってCitrix Workspace利用者のSAML認証を構成するという新しい記事を追加しました：Sign in to workspaces with SAML using Azure Active Directory identities
06 Sep 2023	SAML認証のアップデート	サポートされるプロバイダーを追加し、いくつかの手順を明確にしました：ADFSを使用してCitrix CloudでSAML認証を構成する

日付	変更	説明
04 Aug 2023	新しいSAML IDプロバイダーの記事	Citrix CloudのIDプロバイダーとしてSAMLで使用するためにADFSで証明書利用者の信頼を構成するという新しい記事を追加しました：ADFSを使用してCitrix CloudでSAML認証を構成する
01 Aug 2023	SAML認証のアップデート	SAMLカスタム属性とトラブルシューティング情報を更新しました：SAMLをIDプロバイダーとしてCitrix Cloudに接続する
21 Jul 2023	ITSM Adapterサービス2307の初期リリース	新機能の概要については、「新機能」を参照してください。
17 Jul 2023	管理者に関する更新	［サポートチケット］メニューオプションにアクセスするための管理者権限を追加：管理者権限を変更する
30 Jun 2023	システムログの更新	ネットワークの場所を管理するイベントを追加： Citrix Cloudプラットフォームのシステムログイベント
27 Jun 2023	IDおよびアクセス管理の更新	Google Cloud Identityを使用した管理者認証のサポートを追加：IDおよびアクセス管理
27 Jun 2023	IDおよびアクセス管理の更新	Google Cloud Identityを使用した管理者グループ認証のサポートを追加：管理者グループを管理する
21 Jun 2023	Service Health Dashboardの更新	Service Health Dashboardにアクセスするための方法を更新：Citrix Cloudのサービス正常性

日付	変更	説明
25 May 2023	管理者に関する更新	MFA検証方法を管理するための更新された手順：MFAの復旧方法を管理する
25 May 2023	管理者に関する更新	MFAデバイス、プライマリのMFAのサインイン方法を変更するための更新された手順：プライマリのMFAの方法を管理する
25 May 2023	管理者に関する更新	Citrix Cloud管理者向けのMFA方法として電子メールのサポートが追加されました：多要素認証を設定する
15 May 2023	Citrix Service Providerの更新	ディストリビューター向けのライセンスAPIアクセスのサポートが追加されました：APIへのディストリビューターアクセス
03 May 2023	システムログの更新	リソースの場所の作成、変更、削除に関するシステムログイベントを追加しました：Citrix Cloudプラットフォームのシステムログイベント
03 Apr 2023	管理者の管理の更新	特定のCitrix Cloudプラットフォーム機能へのカスタムアクセス権限を管理者グループに割り当てることができます： 管理者グループの管理
30 Mar 2023	Citrixパートナー向けの更新	パートナーは、顧客ダッシュボードを通じてCitrix Gatewayサービスの帯域幅の使用状況の傾向を表示できます： ライセンスの傾向
22 Mar 2023	停止されたコンテンツ	AppBuilderはCitrix Cloudで利用できなくなったため、この

日付	変更	説明
		サービスの記事を削除しました。
09 Jan 2023	Citrix Service Provider用のDaaSライセンスの更新	Citrix DaaS同時ユーザーモデルのアクティブな使用状況を追加して記事を更新：Citrix DaaSの顧客ライセンスと使用状況の監視
06 Jan 2023	DaaSライセンスの更新	Citrix DaaS同時ユーザーモデルのアクティブな使用状況を追加して記事を更新：Citrix DaaSのライセンスとピーク時の使用状況の監視（同時ユーザー）
06 Jan 2023	License Usage Insightsサービスの更新	無料ユーザーの管理の機能強化を追加して記事を更新：製品の使用状況、ライセンスサーバー、通知の管理
30 Nov 2022	廃止となったMDX Serviceの記事の削除	MDXサービスは2021年9月に製品終了（EOL）になりました。 詳しくは、CXM-100702を参照してください。
02 Nov 2022	サービスの利用に関する表の更新	Google CloudのCitrix DaaSのリージョン一覧にEUを追加しました：各リージョンでのサービスの利用
10 Oct 2022	更新の通知	非管理者の連絡先に関する通知を追加：通知
28 Sep 2022	Azure ADのIDに関する記事を更新	管理者の追加に関するセクションを更新：Azure ADから管理者をCitrix Cloudに追加
28 Sep 2022	管理者の管理の更新	個別のCitrix Cloud管理者追加のスクリーンショットとワークフローを更新：Citrix Cloud

日付	変更	説明
		への管理者のアクセスを管理する
22 Sep 2022	ITSM Adapterサービス2209の初期リリース	新機能の概要については、「新機能」を参照してください。
11 Aug 2022	SAML IDを更新	AD管理者グループ追加のスクリーンショットとワークフローを更新：ADから管理者をCitrix Cloudに追加
11 Aug 2022	Azure ADのIDに関する記事を更新	Azure AD管理者グループの追加を説明するスクリーンショットとワークフローを更新：管理者グループを管理する
11 Aug 2022	管理者の管理の更新	個別のCitrix Cloud管理者追加のスクリーンショットとワークフローを更新：Citrix Cloud管理者を管理する
25 Jul 2022	SAML IDを更新	ADグループのSAML認証のサポートを追加：SAMLをIDプロバイダーとしてCitrix Cloudに接続する
18 Jul 2022	Citrix DaaSライセンスの更新	Citrix DaaSとCitrix DaaS Standard for Azureの両方の同時ライセンスサポートを追加して記事を更新しました：Citrix DaaSのライセンスとピーク時の使用状況の監視（同時使用）
18 Jul 2022	Citrix DaaS Standardライセンスの更新	同時使用ライセンスモデルのサポートに関する参照を含むように記事を更新しました：Citrix DaaS Standard for

日付	変更	説明
		Azureのライセンスと使用状況の監視
29 Jun 2022	IDプロバイダーとしてのGoogleに関する新しい記事	Citrix Cloudは、Googleを使用したワークスペース認証をサポートするようになりました： GoogleをIDプロバイダーとしてCitrix Cloudに接続する
23 Jun 2022	ITSM Adapterサービス2206の初期リリース	新機能の概要については、「新機能」を参照してください。
05 May 2022	Cloud Connectorの高度なヘルスチェック機能に関する新しい記事	新しいCloud Connectorの高度なヘルスチェック機能について説明する記事の追加：Cloud Connectorの高度なヘルスチェック
02 May 2022	ライセンスの記事を更新	Citrix DaaSおよびEndpoint Managementの割り当て済みライセンスの解放機能が最適化され、ライセンスの解放を一括で行いやすくなりました：「Citrix DaaSのライセンスとアクティブな使用状況の監視」および「Endpoint Managementのライセンスとアクティブな使用状況の監視」
28 Apr 2022	パートナーの新しい管理者権限	顧客ダッシュボードにアクセスするための新しい権限を追加しました：パートナー向けのCitrix Cloud
28 Apr 2022	SDKとAPIに関する新しい記事	Citrix Cloudおよびクラウドサービスで利用可能なSDKとAPIをまとめた新しい記事を追加しました：SDKとAPI

日付	変更	説明
25 Apr 2022	Azure ADの権限の更新	新しいAzure AD接続に、Group.Read.Allの代わりとしてGroupMember.Read.All権限が追加されました：Citrix Cloud用のAzure Active Directoryの権限
15 Apr 2022	Cloud ConnectorでのWindowsサポートの更新	Citrix Cloud Connectorは、Windows Server 2022での展開をサポートします。 詳しくは、「Cloud Connectorの技術詳細」を参照してください。
30 Mar 2022	システムログの一般提供	システムログは一般提供されており、生成されたイベントの説明が含まれています。 機能について詳しくは、「システムログ」を参照してください。 イベントの説明については、「システムログイベントのリファレンス」を参照してください。
21 Mar 2022	Gatewayサービスライセンスの更新	ライセンスでは、Citrix Gatewayサービスについてユーザーごとの帯域幅の使用状況が表示されるようになりました：Gatewayサービスの帯域幅の使用状況の監視
17 Mar 2022	ITSMアダプターの記事を更新	ITSMアダプターの新機能の概要については、「新機能」を参照してください。
14 Mar 2022	Citrix Cloud管理者の更新	管理者はアカウント復旧用のメールアドレスを追加できます： 復旧用のメールアドレスを追加または変更する

日付	変更	説明
12 Jan 2022	ライセンスの更新	Citrix Virtual Apps and Desktopsのマルチタイプライセンスのサポートについて追加しました：クラウドサービスのライセンスおよびアクティブな使用状況の監視
17 Dec 2021	オンプレミス製品の登録の更新	登録済みのCitrixライセンスサーバーから収集された使用状況データの削除のサポート：Citrix Cloudを使用するオンプレミス製品の登録
13 Dec 2021	ITSMアダプターの記事を更新	新機能の概要については、「新機能」を参照してください。
08 Dec 2021	新しいクラウドライセンスの記事	ライセンスには、Citrix Managed Azureの消費量の監視のサポートが含まれています：Virtual Apps and DesktopsサービスのCitrix Managed Azureリソースの消費の監視
01 Dec 2021	新しいクラウドライセンスの記事	ライセンスには、Secure Private Accessサービスのサポートが含まれています：Secure Private Accessのライセンスと使用状況の監視
08 Nov 2021	Azure ADグループの追加に関する新しい記事	Azure ADグループを使用した管理者の追加のサポート：管理者グループを追加する
03 Nov 2021	Cloud Connectorネットワーク要件を更新	Cloud Connectorに完全修飾ドメイン名を使用する方法の詳細を追加しました。「インターネット接続の要件：Citrix Cloud Connector」を参照してください

日付	変更	説明
25 Oct 2021	ITSMアダプターの記事を更新	新機能の概要については、「新機能」を参照してください。
29 Sep 2021	Remote Browser Isolation（旧称Secure Browser）の記事を更新しました	「Remote Browser Isolation」を参照してください。
14 Sep 2021	IDに関する記事の更新	Citrix CloudのSAML認証は、顧客に一般公開されています：SAMLをIDプロバイダーとしてCitrix Cloudに接続する
26 Aug 2021	License Usage Insightsの更新	CSPの顧客のVirtual Apps and Desktopsサービスのライセンスと使用状況の監視に関する記事を追加しました：Citrix Virtual Apps and Desktopsサービスの顧客のライセンスと使用状況の監視
26 Aug 2021	License Usage Insightsの更新	ライセンス使用状況のシングルテナントおよびマルチテナントのアグリゲーションに関する記事を追加しました：Cloudサービスのライセンス使用状況とレポート（Citrix Service Providers向け）
19 Aug 2021	ITSMアダプターの記事を更新	新機能の概要については、「新機能」を参照してください。
20 Jul 2021	Cloud Connector更新のトラブルシューティングの詳細	Cloud Connectorの更新エラーのトラブルシューティングに関する情報を追加しました： 更新エラーのトラブルシューティング
14 Jul 2021	Azure Active Directoryの権限の追加	Azure Active Directoryに接続して使用するときにCitrix

日付	変更	説明
		Cloudが要求する権限に関する記事を追加しました：Citrix Cloud用のAzure Active Directoryの権限
13 Jul 2021	ライセンスの更新	移行により二重にカウントされたライセンスに関するよくある質問項目を追加しました： クラウドサービスのライセンスおよびアクティブな使用状況の監視
13 Jul 2021	ライセンスの更新	Technical Previewの注意書きを更新し、帯域幅の割り当ての強制について記載しました：Gatewayサービスの帯域幅の使用状況の監視
13 Jul 2021	新しい「IDおよびアクセス管理」記事	Citrix Cloudで使用されるエンタープライズアプリケーション用のAzure AD権限を追加しました：Citrix Cloud用のAzure Active Directoryの権限
01 Jul 2021	サービスレベルアグリーメントの更新	「サービス別の可用性の評価基準」の表にCitrix Wrikeを追加しました：サービスレベルアグリーメント
29 Jun 2021	システムログ機能に関する新しい記事	Citrix Cloudでの特定イベントのログ記録に関する新しいTechnical Preview記事を追加しました：システムログ
24 Jun 2021	ITSMアダプターの記事を更新	新機能の概要については、「新機能」を参照してください。
16 Jun 2021	Citrix Gatewayサービスの新しいライセンス記事	Citrix Gatewayサービスで帯域幅の使用状況を表示する方法について新しい記事を追加

日付	変更	説明
		しました：Gatewayサービスの帯域幅の使用状況の監視
27 Apr 2021	新しいCloud Connectorの記事	Cloud ConnectorのCDFログの収集に関する新しい記事を追加しました：ログ収集
23 Apr 2021	ITSMアダプターの記事を更新	新機能の概要については、「新機能」を参照してください。
16 Mar 2021	Remote Browser Isolation（旧称Secure Browser）の記事を更新しました	新機能および変更された機能の概要については、「Remote Browser Isolation」を参照してください。
17 Feb 2021	SLAの稼働時間の更新	Citrix Application Delivery Managementのサービス稼働時間をサービスレベルアグリーメントに追加しました：サービスレベルアグリーメント
08 Feb 2021	SLAの稼働時間の更新	Citrix Analyticsのサービス稼働時間をサービスレベルアグリーメントに追加しました：サービスレベルアグリーメント
05 Feb 2021	サービスを使用するリージョンの更新	セキュアインターネットアクセスサービスの場所を追加しました：セキュアインターネットアクセスサービスの場所
03 Feb 2021	Citrix Cloud Labsのコンテンツを削除	廃止されたCitrix Cloud Labsおよびセッションマネージャーの記事を削除しました。 Citrix Cloud Labsおよびセッションマネージャーサービスは廃止され、2020年9月

日付	変更	説明
		にCitrix Cloudから削除されました。
07 Dec 2020	Cloud Connectorスケジュール設定の機能強化	希望する時刻と曜日に合わせたCloud Connectorの更新：Cloud Connectorの更新
30 Oct 2020	SLAの稼働時間の更新	サービスレベルアグリーメントのサービス稼働時間を更新しました：サービスレベルアグリーメント
17 Sep 2020	古い機能に関する記事の削除	StoreFront用のアクセス制御Syncユーティリティに関する記事は古くなり、Citrix Cloudのドキュメントから削除されました。 このユーティリティはダウンロードできなくなり、Citrixでのサポートは終了しました。 現在サポートされている機能については、Secure Private Accessサービスのドキュメントを参照してください。
04 Sep 2020	Virtual Apps and Desktopsサービスの新しいライセンスに関する記事	Virtual Apps and Desktopsサービスの同時使用ライセンスサポートを追加しました：Citrix Virtual Apps and Desktopsサービスのライセンスとピーク時の使用状況の監視（同時使用）
19 Jun 2020	多要素認証登録の更新	すべてのCitrix Cloud管理者が多要素認証に登録する必要があります：多要素認証の要件
18 Jun 2020	Connector Applianceの一般提供	クラウドサービス用のConnector Applianceが、実稼働環境で一般提供されます。詳しくは、「クラウドサービ

日付	変更	説明
		ス用のConnector Appliance」を参照してください。
18 May 2020	Citrix Cloud管理者の多要素認証登録	Citrix Cloud管理者を多要素認証に登録し、デバイスを変更し、復旧方法を更新する新しいセクションを追加：多要素認証を設定する
27 Mar 2020	Cloud Connectorの証明書要件を更新	Cloud Connectorのインストール中に証明書を検証するためのポート要件を追加しました：Cloud Connectorの技術詳細
26 Mar 2020	ライセンスFAQを更新	マルチタイプのライセンスをVirtual Apps and Desktopsサービスで使用する場合のライセンスコンソールへの影響に関する項目を、よくある質問セクションに追加しました：クラウドサービスのライセンスおよびアクティブな使用状況の監視
26 Mar 2020	新しいコネクタを追加	新しい記事を追加しました：クラウドサービス用のConnector Appliance
28 Feb 2020	Managed Desktopsサービスのライセンスおよび使用状況に関する新しい記事	新しい記事を追加しました：Citrix Managed Desktopsサービスのライセンスとアクティブな使用状況の監視
07 Feb 2020	オンプレミスライセンス使用状況の記事に新しいセクションを追加	「同時使用ライセンスモデルのピーク時のライセンス使用状況」セクションを追加しました： オンプレミス展開のライセンスと使用状況の監視

日付	変更	説明
11 Dec 2019	WorkspaceのCitrixフェデレーション認証サービスに関する新しい記事	新しい記事を追加しました：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
03 Dec 2019	URLフィルタリングの新しいポリシー	新しい機能のURLフィルタリングを追加して記事を更新。詳しくは、「Remote Browser Isolation」を参照してください。
03 Dec 2019	ユーザーのセッション中にホスト名を追跡する新機能	新しい機能のURLフィルタリングを追加して記事を更新。詳しくは、「Remote Browser Isolation」を参照してください。
15 Nov 2019	内部ワークスペース利用者のVDAへの接続を改善するための新しい記事	新しい記事を追加しました：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
06 Nov 2019	Remote Browser Isolation（旧称Secure Browser）の新しい種類のブラウザー	共有パスコード認証を使用した新しい種類のブラウザーが追加されました。 詳しくは、「Remote Browser Isolation」を参照してください。
23 Oct 2019	Remote Browser Isolation（旧称Secure Browser）に関する新しいポリシー	ユーザーによるアプリの起動時に管理者が新しいセッションの開始URLを変更できるポリシーを追加しました。 詳しくは、「Remote Browser Isolation」を参照してください。
11 Sep 2019	Citrix Cloudでの顧客データとログの処理に関する新しい記事	新しい記事を追加しました：Citrix Cloudサービスの顧客コンテンツとログの処理

日付	変更	説明
09 Sep 2019	Virtual Apps and Desktops サービスのライセンスと使用状況の内容を更新	ユーザー/デバイスライセンスモデルのサポートを追加。サービス固有のライセンスおよび使用状況機能は専用の記事：Citrix Virtual Apps and Desktopsサービスのライセンスとアクティブな使用状況の監視
06 Sep 2019	Citrix Cloudに新しいIDプロバイダーを追加	Citrix CloudでサポートされているIDプロバイダーにOktaを追加しました：OktaをIDプロバイダーとしてCitrix Cloudに接続する
06 Sep 2019	Workspaceに新しいIDプロバイダーを追加	WorkspaceでサポートされているIDプロバイダーにOktaを追加しました：Okta
29 Aug 2019	オンプレミス製品のライセンスおよび使用状況に関する新しい記事	**［ライセンスおよび使用状況］**の**［ライセンス割り当て済みの展開］**タブで利用可能な分析情報に関する新しい記事を追加しました：オンプレミス展開のライセンスと使用状況の監視
27 Aug 2019	Citrix Cloud Connectorの技術詳細の記事を更新	Cloud Connectorインストールにおけるデジタル証明書の検証の要件を追加しました：証明書の検証要件
18 Jun 2019	Citrix Cloudのサービスレベルアグリーメントの記事を更新	CSPの資格および最小ユニットサブスクリプションを追加しました：Citrix Cloudサービスレベルアグリーメント
17 Jun 2019	Citrix Cloudに新しいIDプロバイダーを追加	Citrix CloudでサポートされているIDプロバイダーにCitrix Gatewayを追加しました：Citrix GatewayをIDプロバイ

日付	変更	説明
		ダーとしてCitrix Cloudに接続する
17 Jun 2019	Workspaceに新しいIDプロバイダーを追加	WorkspaceでサポートされているIDプロバイダーにCitrix Gatewayを追加しました：Citrix Gateway
05 Jun 2019	Remote Browser Isolationに関する新しいポリシー	公開ブラウザーを自動的に別のリージョンに転送できる新しいポリシーを追加しました。 詳しくは、「Remote Browser Isolation」を参照してください。
22 May 2019	新しい高度な概念に関する記事	オンプレミスStoreFrontを介してSaaSおよびWebアプリケーションに安全にアクセスする方法を説明した新しい記事を追加しました。 注：この記事は2020年9月17日に廃止されました。
17 May 2019	「Citrix Cloudの管理」セクションの新しい記事	Citrix Cloudにおけるオンプレミス製品の登録に関する新しい記事を追加しました：オンプレミス製品の登録の管理
14 May 2019	Azureサブスクリプションからの期限切れサービスの削除に関する新しいセクション	顧客自身が管理するAzureサブスクリプションからの期限切れサービスおよびブロックされたサービスの削除方法を記載した「顧客管理のAzureサブスクリプション」セクションを追加しました：Citrix Cloudサービスのサブスクリプション延長
09 May 2019	新しい高度な概念に関する記事	Citrix Virtual Apps and Desktopsサービスでオンプレミス StoreFrontを展開するためのシナリオを説明した新し

日付	変更	説明
		い記事を追加しました：Citrix Virtual Apps and Desktopsサービス用のオンプレミスStoreFront認証参照アーキテクチャ
07 May 2019	サービスサブスクリプション延長契約について更新しました	月単位サービスサブスクリプションの有効期限を更新しました：Citrix Cloudサービスのサブスクリプション延長
09 Apr 2019	更新	「Cloud Connectorのプロキシとファイアウォールの構成」に、ワイルドカード文字のドメインを指定する理由を追加しました
05 Apr 2019	更新	「MDX Service」記事のMDX Serviceのバージョンを更新しました
04 Apr 2019	更新	「ワークスペースアクセスの構成」に記載されたMacおよびiOSのWorkspaceアプリ向けAADサポートについて更新しました
22 Mar 2019	リリース	Citrix Cloudでの［Active Directory+トークン］認証の構成手順を追加しました：Active DirectoryをCitrix Cloudに接続する
22 Mar 2019	リリース	［Active Directory+トークン］認証のワークスペース要件を追加しました： Active Directory+トークン
22 Mar 2019	リリース	［Active Directory+トークン］認証のデバイスのリセッ

日付	変更	説明
		ト方法を追加しました：Active Directory+トークン
22 Mar 2019	リリース	［Active Directory+トークン］認証のデバイスの登録手順を追加しました：2要素認証（オプション）