Citrix Cloud

Contents

Citrix Cloud

July 2, 2024

> 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になりました。詳しくは、CTX583004を参照してください。

Citrix Cloud は、Citrix のクラウドサービスをホストし管理するプラットフォームです。どのクラウドや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、またはハイブリッドクラウド）を使用する場合でも、コネクタ経由でローカルのリソースに接続します。単一のコンソールからエンドユーザーに対してアプリおよびデータとともにワークスペースを作成、管理、展開できます。

新機能

Citrix Cloud Updatesにアクセスして、Citrix Cloud の新機能と今後の機能、および次のサービスの最新情報を入手できます。

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

Citrix Cloud のトライアル

上記の 1 つまたは複数の Citrix Cloud サービスを、概念実証済みの製品版環境でお試しください。Citrix Cloud に登録後、コンソールからサービスごとのトライアルをリクエストできます。トライアルの終了後もすべての構成を保持できるように、製品版環境に移行することができます。詳しくは、「Citrix Cloud サービスのトライアル」を参照してください。

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に移動すると、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があります。

アーキテクチャのリソースと展開のリソース

Citrix Tech Zoneには、Citrix Cloud およびそのほかの Citrix 製品の詳細を知るために役立つさまざまな情報が含まれています。ここから、Citrix テクノロジの設計、構築、展開に関する知識情報を提供するリファレンスアーキテクチャ、図、技術資料を参照することができます。

Citrix Cloud の主要なサービスコンポーネントについて詳しくは、次のリソースを参照してください:

- Citrix Workspace の概念図: ID、ワークスペースインテリジェンス、シングルサインオンなどの主要分野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、Citrix Workspace 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 のリファレンスアーキテクチャ: Citrix DaaS（旧称 Virtual Apps and Desktops サービス）を関連するサービスとともに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 Learning シリーズポータルでは、Citrix Cloud とそのサービスを導入して実行するための教育モジュールを提供しています。概要から、計画と構築のサービスまで、すべてのモジュールを順番に確認できます。次のコースでクラウドの旅を始めましょう:

- Citrix Cloud の基礎
- Citrix ID と認証の概要
- StoreFront から Workspace への移行

Citrix Education ビデオライブラリでは、主要な展開タスクと、Citrix Cloud サービスで使用する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したオンライン動画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、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などのタスクに関する詳細をご覧ください。

サービスレベルアグリーメント

July 2, 2024

発効日: 2020 年 10 月 30 日

Citrix Cloud は、業界のベストプラクティスを使用して、高度なサービス可用性を実現するように設計されています。

このサービスレベルアグリーメント（SLA）では、Citrix Cloud サービスの可用性に関する Citrix の目標について説明します。この SLA は、対象サービス（「サービス」）に関する Cloud Software Group のエンドユーザーサービス契約（EULA）の一部です。

Citrix のサービス目標（「サービス目標」）は、サービスの月間稼働時間（「月間稼働時間」）を 99.9% 以上に維持することです。月間稼働時間は、当該サービスのインスタンスが 1 か月間に「使用不可」の状態にあった時間（分）のパーセント値を 100% から引いて計算します。サービスの種類およびサービス別の可用性の評価基準については、以下の表で定めるものとします。月間稼働時間（%）には次のような原因で生じたダウンタイムを含みません:

- 定期的にスケジュール設定された保守時間。
- 当該サービスの構成要件（https://docs.citrix.com）にお客様が従わなかった場合、不正なアクティビティがあった場合、または入力に問題があった場合。
- Citrix がお客様に当該サービスの使用について変更するよう勧めた後に、お客様がサービスを変更せずに使用した場合。
- Citrix が管理していないコンポーネント（次を含むがこれに限定されない）が原因である場合：お客様が管理している物理および仮想マシン、お客様がインストールし保守しているオペレーティングシステム、お客様がインストールし管理しているネットワーク機器またはその他のハードウェア、お客様が定義し管理してい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。Citrix の制御の及ばない他のカスタマーサポート要因。
- お客様の従業員、代理店、契約社員、もしくはベンダー、もしくは第三者がお客様のパスワードや機器を使用してアクセスした場合、またはお客様が適切なセキュリティ上の推奨事項に従わなかったその他の場合。
- お客様がサービス使用権を越える処理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（自然災害、戦争もしくはテロ行為、または政府の方針を含むがこれに限定されない）。

Citrix のトライアル、テクニカルプレビュー、Labs もしくはベータ版のサービスについては、サービス目標は提供されません。

Citrix は、次のお客様にサービス目標を提供します：

- 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）を使用して当該サービスを購入している。
- 請求期間中に当該サービスに適用できるライセンスモデルあたり少なくとも 100 ユニットのサブスクリプション（Citrix Service Provider で最小 1,000）がある。

Citrix Service Provider（CSP）は 2018 年 10 月 1 日に対象となりました。

サービス別の可用性の評価基準

サービス	月間稼働時間の評価基準
Citrix Analytics for Performance	ユーザーがアプリやデスクトップのパフォーマンスにアクセスして改善できる時間。
Citrix Analytics for Security	ユーザーがユーザーアクセスとユーザーアクティビティのリスクを検出して軽減できる時間。
NetScaler コンソールサービス	すべての POP でサービスを利用できる平均時間。
Citrix Endpoint Management	ユーザーがサービスを使用して、Citrix が配信したモバイルアプリおよび登録済みデバイスにアクセスできる時間。

サービス	月間稼働時間の評価基準
HDX プロキシ用の Citrix Gateway サービス	ユーザーがサービスを使用して、自分の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 Intelligent Traffic Management	ユーザーが DNS クエリまたは HTTP API コールを使用してトラフィック管理機能にアクセスできる時間。
NetScaler SD-WAN Orchestrator	ユーザーがサービスを使用して、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 Secure Private Access	ユーザーがサービスを使用して、SaaS または内部 Web アプリにアクセスできる時間。
Citrix DaaS	ユーザーがサービスを使用して、自分の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。
Citrix Workspace	上記コンポーネントサービスの場合と同じですが、可用性は個別に評価します。一部のコンポーネントに関するクレームの場合、クレジットはその割合で配分されることがあります。

> 注:
>
> Citrix DaaS は、Citrix Virtual Apps サービス、Citrix Virtual Desktops サービス、Citrix Virtual Apps and Desktops サービスの新しい名前です。

サービス目標と救済措置

Citrix が本 SLA 発効日から起算して連続 5 か月間に 3 回以上サービス目標を達成しなかった場合には、排他的な救済措置として、10% のサービスクレジットが、月単位で、Citrix がサービス目標を達成しなかった月数分、お客様が直近の更新期間に翌年度のサービスを延長されるときに、影響を受けたものと同じサービスおよびユニット数に関して計上されるものとします。

- 月間稼働時間（%）: > 99.9%
- サービスクレジット: 該当する月数分の 10%（お客様にバウチャーとして提供）

上記の救済を受けるためには、お客様は EULA に従い、サービスクレジットを請求する連続 5 か月間の最終月末から三十（30）日以内に目標未達成について報告する必要があります。この SLA に違反している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。

請求の際は、サービスを特定し、使用不可の状態にあった日時および期間と合わせて証拠となるログまたはレコードを明確にし、影響を受けたユーザーとその場所、およびテクニカルサポートの要求または修復アクションの実施についてもすべて明示する必要があります。1 サービスあたり 1 回のみ、該当する月数分のサービスクレジットが発行されます。延長期間全体に対して、10% のサービスクレジットが最大 1 回、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。

販売代理店経由で延長を購入する場合は、販売代理店経由でクレジットを受け取ります。直接購入に適用されるか間接購入で販売代理店経由で提示されるクレジットは、同じユニット数を延長する場合の混合レートでの希望小売価格を配分した額に基づきます。Citrix が再販価格および再販クレジットを制御することはありません。クレジットには Citrix または再販代理店への支払いを相殺する権利はありません。Citrix は、これらの規定を適宜変更することができるものとします。変更時に、Citrix は本サービスレベルアグリーメントの冒頭にある発行日を併せて変更します。変更はすべて、最新発行日以降のサービス新規購入あるい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

November 9, 2023

- Citrix Cloud サードパーティ通知（PDF）（英語）
- Citrix Analytics Service サードパーティ通知（PDF）（英語）
- Citrix DaaS サードパーティ通知（PDF）（英語）
- Citrix DaaS Standard for Azure サードパーティ通知（PDF）（英語）
- Remote Browser Isolation（旧称 Secure Browser）（PDF）
- Citrix Endpoint Management サードパーティ通知（PDF）（英語）
- Citrix Cloud Linux VDA Image Service サードパーティ通知（PDF）（英語）
- クラウドサービス用の Connector Appliance のサードパーティ製品についての通知（PDF）（英語）
- Citrix Gateway サービスのサードパーティ製品についての通知 （PDF）（英語）
- Citrix Device Posture サービスのサードパーティ通知（PDF）（英語）

> 注:
>
> Citrix DaaS は、以前は Citrix Virtual Apps and Desktops サービスと呼ばれていました。Citrix DaaS Standard for Azure は、以前は Citrix Virtual Apps and Desktops Standard for Azure と呼ばれていました。

ヘルプとサポートを受ける方法

July 2, 2024

この記事では、アカウントの作成時、または Citrix Cloud や別の Citrix Web サイトへのサインイン時に発生した問題のトラブルシューティング方法とヘルプの確認方法について説明します。この記事では、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紹介します。

> 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、最初にこの記事を参照して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を解決できない場合は、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。

アカウントの作成

Citrix Discussions 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 サイトの特定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。

会社用に新しい Citrix アカウントを作成するには、以下のいずれかの方法を使用して Citrix にお問い合わせください。

- Citrix カスタマーサービスに連絡する。
- お住まいの地域のCitrix パートナーまたはCitrix セールスオフィスに連絡する。

既に Citrix アカウントがある場合は、Citrix Cloud アカウントを作成し、「Citrix Cloud アカウントを作成する」で説明されているタスクを完了してオンボードプロセスを完了できます。

Citrix Cloud へのサインアップで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 サイトおよび **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、次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問題のトラブルシューティング
- CTX283814: Citrix アカウントを設定した後のサインインの問題

MFA を設定できない、または **Citrix** アカウントにサインインするときに **MFA** で認証できない

トラブルシューティングに関する情報については、以下の記事を参照してください。

- CTX461297: How to Enroll into Multi Factor Authentication (MFA)
- CIX463758: How to recover access to your account

MFA でも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確認したり、**Citrix** パスワードをリセットしたりする方法

次の手順に従って、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、以下を行います。
   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たメール 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、以下を行います。
   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 は、メールアドレスを使用してアカウントを見つけた場合、メールアドレスに関連付けられた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 は、Citrix ユーザー名を使用してアカウントを見つけた場合、パスワードをリセットする手順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「メールの受信トレイに Citrix メールが表示されない」を参照してください。

Citrix Cloud にサインインできない

- 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ます。アカウントのユーザー名を確認するには、https://citrix.cloud.com/にアクセスして [ユーザー名を忘れた場合] を選択し、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。
- パスワードのリセットが必要になる場合があります。最近サインインしていない場合や、パスワードの強度が十分でない場合、Citrix Cloud でパスワードの変更が要求されます。詳しくは、本記事の「パスワードを変更する」を参照してください。
- カスタムのサインイン 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 アカウントでAzure AD、Google Cloud IdentityまたはSAMLを使用して管理者を認証する場合は、[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。次に、会社の資格情報を入力すると、会社の Citrix Cloud アカウントにアクセスできます。会社のログイン URL がわからない場合、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。

メールの受信トレイに **Citrix** メールが表示されない

Citrix アカウントの検索時やパスワードの変更時に Citrix が多要素認証の ID の確認用としてメールを送信すると、そのメールは通常数分以内に届きます。メールが届かない場合は、以下を行います。

- 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、正しいことを確認します。最近メールアドレスを変更した場合、確認メールが古いアドレスに送信されることがあります。
- 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スパムフォルダーとゴミ箱フォルダーを確認します。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ている可能性があります。以下の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ます。
  - donotreplynotifications@citrix.com
  - cloud@citrix.com
  - CustomerService@citrix.com

数分経過してもメールが届かない場合、またはサインインで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 の顧客は、MFA を使用して自身の Citrix アカウントと Citrix Cloud にサインインする必要があります。MFA への登録は、以下の場合に行います。

- 新しい顧客が初めて Citrix アカウントにサインインする。
- Citrix の顧客が新しい Citrix Cloud アカウントのオンボードを行うが、MFA への登録が済んでいない。
- 新しい管理者が既存の Citrix Cloud アカウントに参加する。

Citrix アカウントまたは Citrix Cloud へサインインするときに多要素認証への登録を要求された場合は、「CTX461297: How to Enroll into Multi Factor Authentication (MFA)」の手順に従ってください。

Citrix アカウントの多要素認証について詳しくは、「CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix properties」を参照してください。

アカウントの復旧

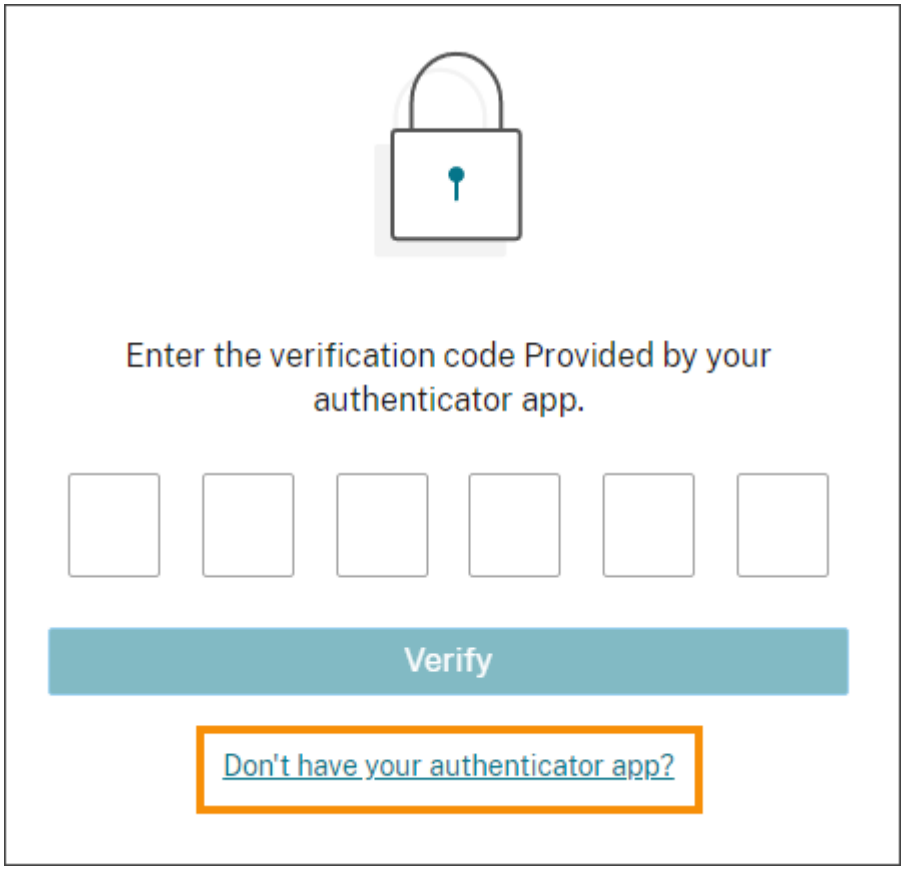
Citrix アカウントの資格情報を回復するためのサポートが必要な場合は、この記事の「Citrix アカウントのユーザー名を確認したり、Citrix パスワードをリセットしたりする方法」を参照してください。

Citrix Cloud アカウントへのアクセスを回復するためのサポートが必要な場合は、MFA に登録したときに構成した復旧方法を使用できます。これらの復旧方法には以下のようなものがあります。

- Citrix が復旧用のメールアドレスに送信するワンタイムコードの使用。
- MFA 登録時に生成したリストからのバックアップコードの使用。
- Citrix サポートからの復旧用の電話番号への電話による本人確認と、アカウントへのアクセスのサポート。多要素認証の登録時に復旧用の電話番号を設定する必要があります。

回復方法を使用して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で、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. プライマリの多要素認証の方法で、コードの入力を求められたら、［復旧方法を使用する］を選択します。



3. 必要に応じて、使用する回復方法を選択します。他の回復方法が 1 つしか構成されていない場合、復旧用の電話番号を除き、Citrix は自動的にプロンプトを表示してその方法を使用するように求めます。
4. 復旧用のメールアドレスを使用する場合は、Citrix から送信されるワンタイムコードを入力し、［確認］を選択します。しばらくしてもコードが届かない場合は、［メールを再送信する］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ときにコードを入力し、［確認して続行］を選択します。Citrix Cloud にサインインするとメールが届き、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が通知されます。使用したバックアップコードをメモするか削除して、二度と使用しないようにします。
6. 復旧用の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、復旧用の電話番号を使用して本人確認のために連絡します。その後、担当者から、サインインに使用できる復旧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復旧用のコードを入力し、［確認］を選択します。

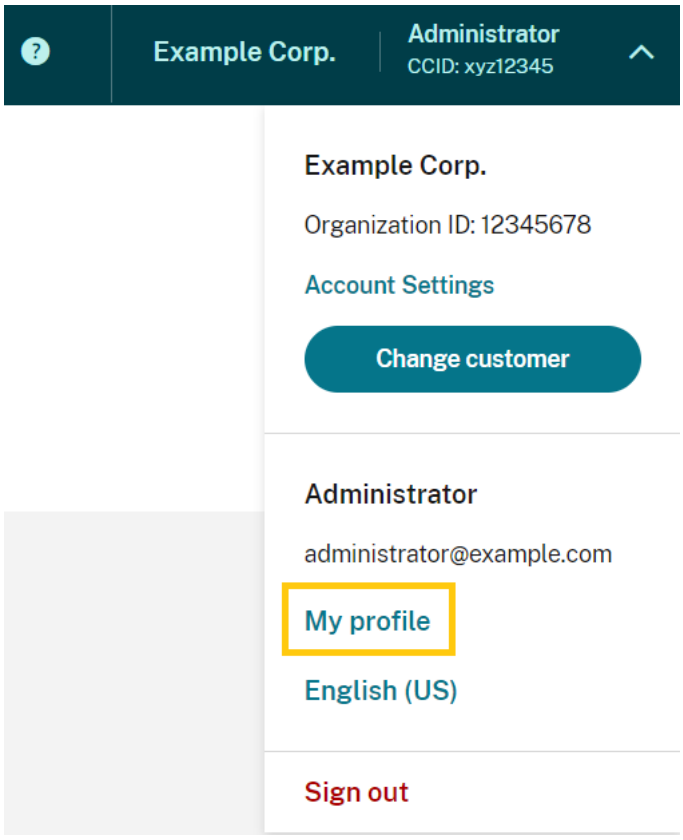
サインインしたら、今後のサインインの遅延を避けるために、必ずアカウントの復旧方法を更新してください。

多要素認証の設定の更新

［自分の設定］ページから多要素認証によるアクセスと復旧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。

［自分の設定］ページにアクセスするには、以下の手順を実行します:

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 ［自分の設定］を選択します。



多要素認証の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 の復旧方法を管理する

パスワードを変更する

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］を選択します。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が記載されたメールを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。

サインインしようとすると、Citrix Cloud からパスワードをリセットするように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。
- パスワードに辞書の単語が含まれています。
- 既知の侵害されたパスワードのデータベースに含まれるパスワードです。
- 過去 60 日間に Citrix Cloud にサインインしていません。

パスワードは 8〜128 文字の長さで、次が含まれている必要があります:

- 1 つ以上の数字
- 1 つ以上の大文字
- 1 つ以上の次の記号: ! @ # $ % ^ * ? + = -

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用の強力なパスワードを作成します。

クラウドのサービス正常性

Citrix Cloud Health Dashboard（https://status.cloud.com）は、各地理的リージョンにおける Citrix Cloud プラットフォームとサービスの可用性についてリアルタイムで概要を提供します。Citrix Cloud で問題が発生した場合は、Cloud Health Dashboard をチェックして、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 について詳しくは、「サービス正常性」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、ヘルプを要求したり、フィードバックや改善案を送信したり、他のユーザーの会話を表示したり、トピックを作成したりできます。

Citrix のサポートスタッフメンバーはこれらのフォーラムを追跡し、質問に回答します。他の Citrix Cloud コミュニティのメンバーも、支援を提供したりディスカッションに参加することがあります。

フォーラムのトピックを閲覧する場合、サインインする必要はありません。ただし、投稿したり、トピックに返信するためには、サインインが必要です。サインインするには、既存の Citrix アカウント資格情報を使用するか、Citrix Cloud アカウントの作成時に指定したメールアドレスとパスワードを使用してください。

サポート記事とドキュメント

Citrix Cloud を活用し、Citrix 製品で発生する可能性のある問題を解決するために、十分な製品とサポートコンテンツが用意されています。

Citrix Support Knowledge Center

Knowledge Centerでは、すべての Citrix 製品のトラブルシューティングコンテンツ、セキュリティ情報、およびソフトウェアアップデート通知を提供しています。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。製品と記事の種類でフィルタリングできます。

Citrix Tech Zone

Citrix Tech Zoneには、Citrix Cloud およびそのほかの Citrix 製品の詳細を知るために役立つ情報があります。ここで、Citrix テクノロジの設計、構築、展開に関する分析情報を提供するリファレンスアーキテクチャ、図、ビデオ、技術資料を参照できます。

ユーザーヘルプセンター

Citrix ユーザーヘルプセンターでは、組織のエンドユーザー向けに Citrix 製品ドキュメントを提供しています。Citrix Workspace アプリや Citrix SSO などのエンドユーザー向け製品の説明を、読みやすい形式で提供しています。ShareFile のエンドユーザー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 アプリ」を参照してください。

テクニカルサポート

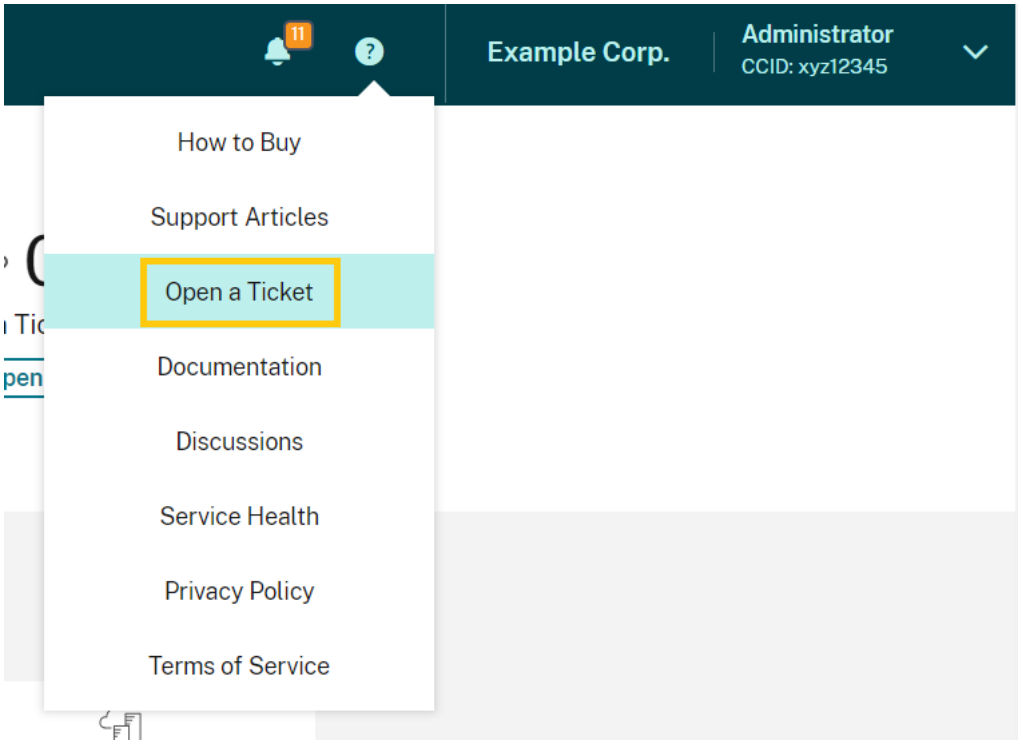
テクニカルサポートが必要な問題が発生した場合は、My Support ポータルにアクセスしてサポートケースを開くか、Citrix テクニカルサポートの担当者にご相談ください。

My Support ポータルを利用するには、https://support.citrix.com/case/manageにアクセスしてください。

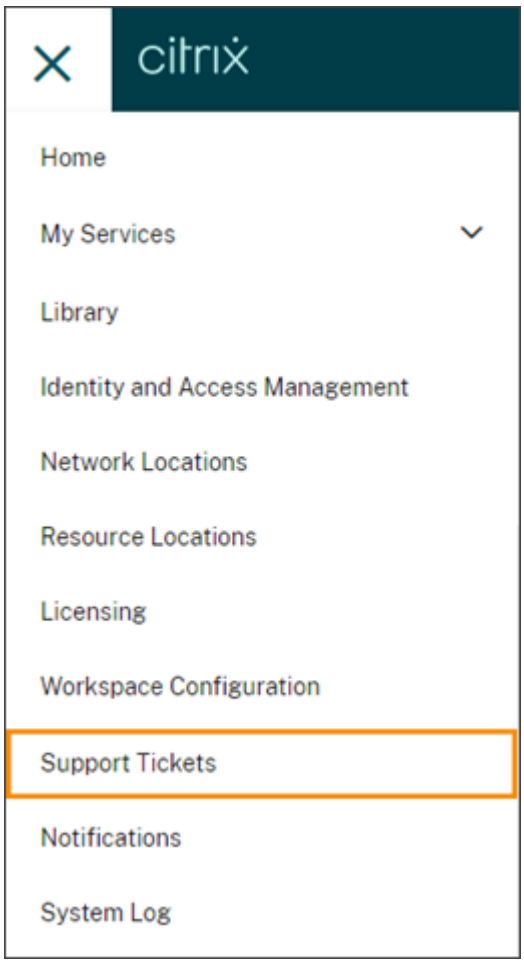
Citrix Cloud からポータルにアクセスするには、サポートチケットの権限が必要です。管理者権限について詳しくは、「管理者権限を変更する」を参照してください。

Citrix Cloud 管理コンソールから、次の方法を使用して My Support にアクセスできます:

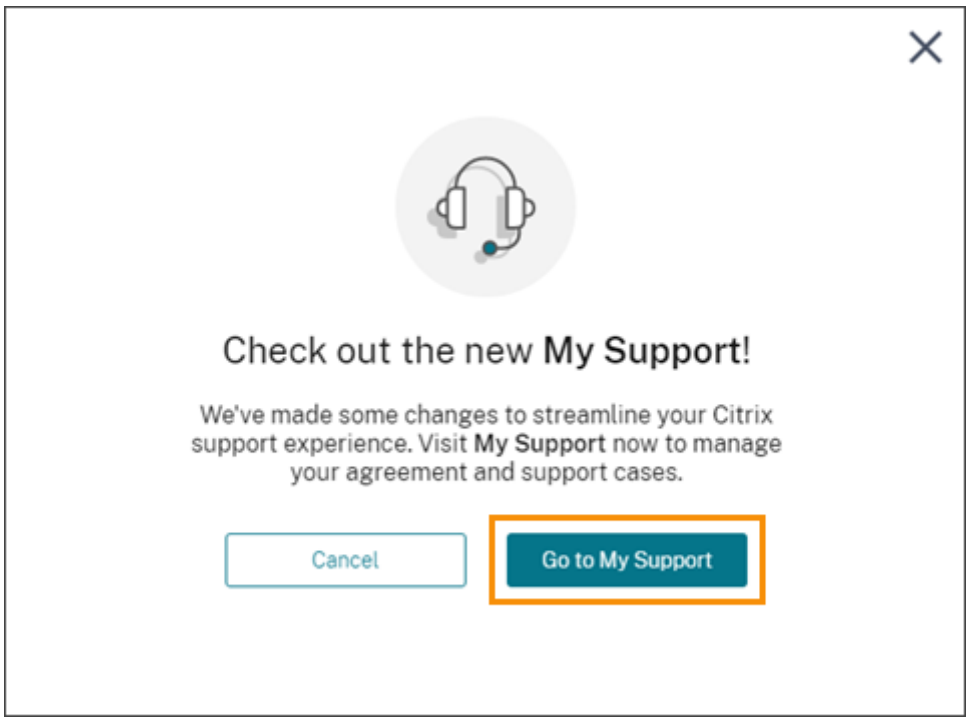
- 画面の右上付近にある ［ヘルプ］アイコンで、［チケットを開く］を選択します。



- 画面左上の Citrix Cloud メニューから、［サポートチケット］を選択します。

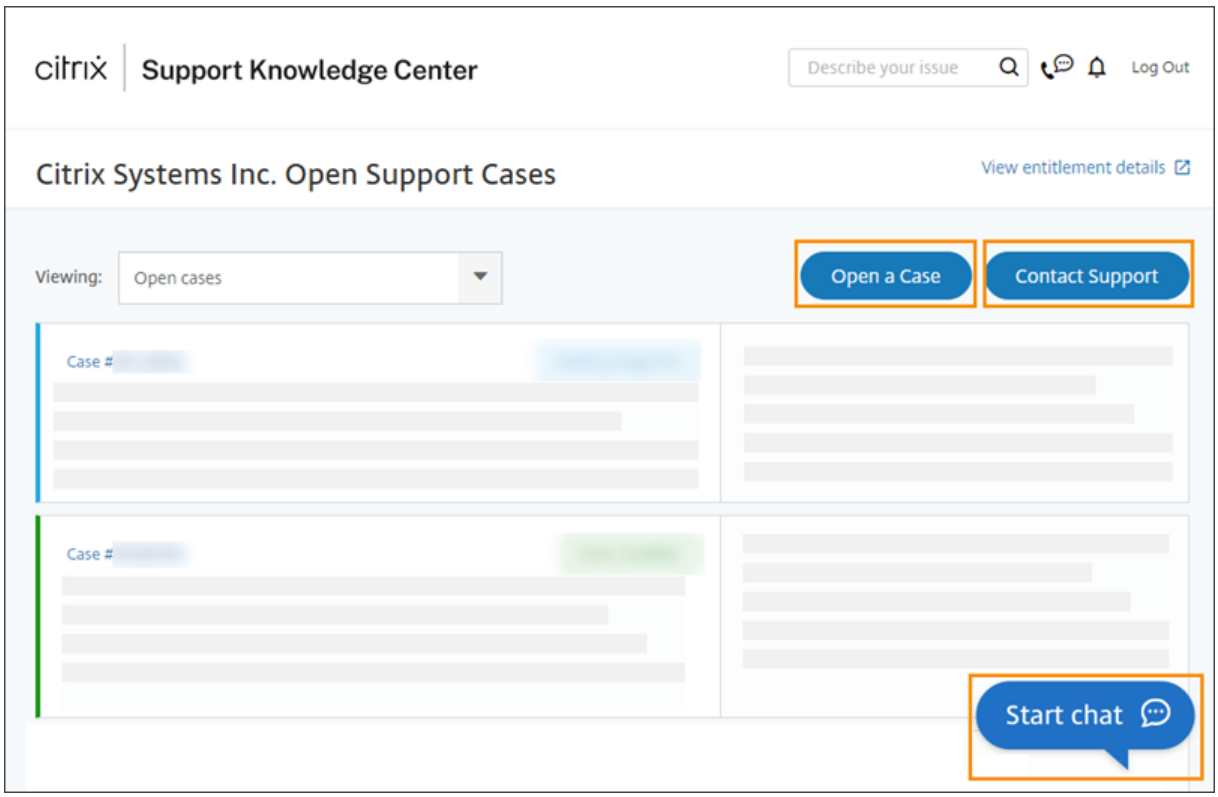


これらのオプションのいずれかを選択した後、［**My Support** に移動］を選択し、Citrix アカウントの資格情報を使用してサインインします。



サインイン後、次のいずれかの方法を使用して Citrix テクニカルサポートに連絡してください：

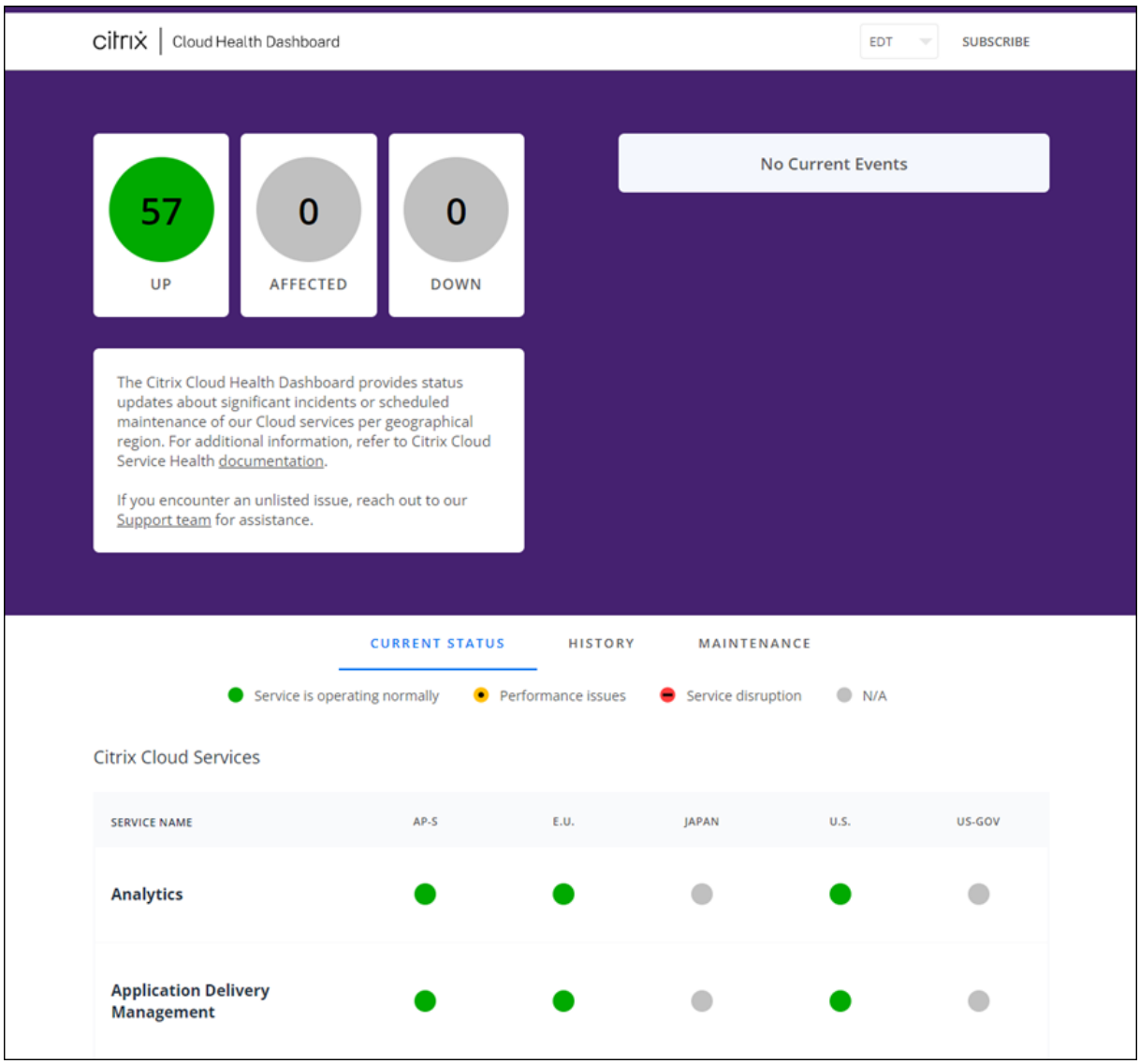
- サポートケースを開始する：［ケースを開く］を選択し、発生している問題の詳細を入力します。
- 電話：［サポートに連絡］を選択して、Citrix テクニカルサポートへの電話に使用できるリージョンの電話番号一覧を表示します。
- ライブチャット：ページの右下隅にある ［チャットを開始］を選択して、Citrix テクニカルサポートの担当者とチャットします。



Citrix Cloud のサービス正常性

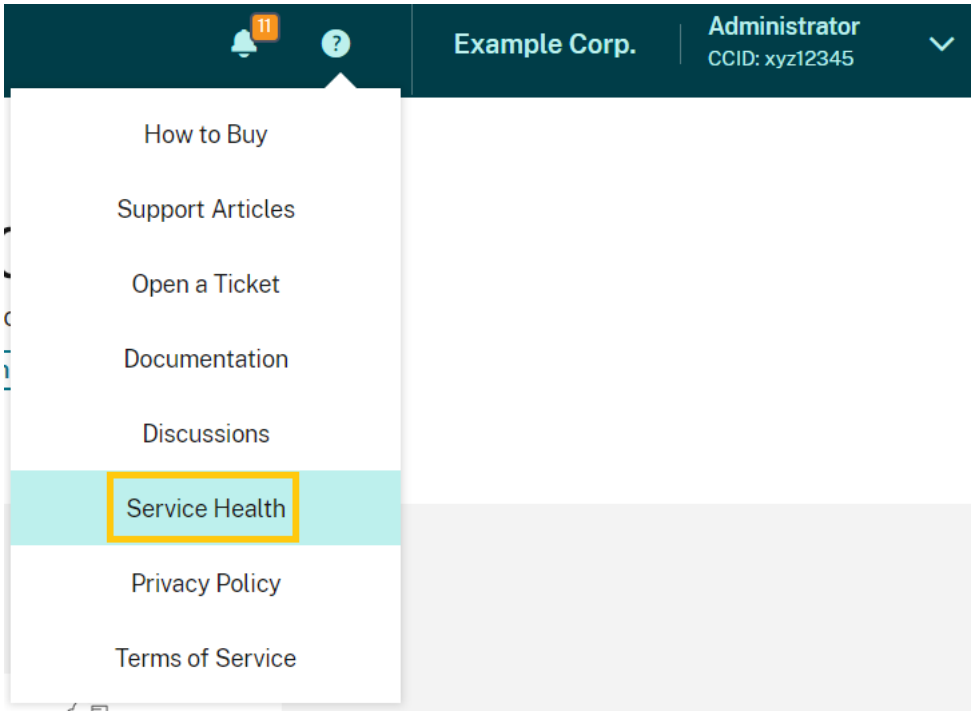
November 30, 2023

Citrix Cloud Health Dashboard は、各地理的リージョンにおける Citrix Cloud プラットフォームとサービスの可用性についてリアルタイムで概要を提供します。Citrix Cloud で問題が発生した場合は、Cloud Health Dashboard をチェックして、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。



次の方法を使用して、Cloud Health Dashboard にアクセスできます:

- ブラウザーでhttps://status.cloud.comに移動します。
- Citrix Cloud のヘルプメニューから ［サービス正常性］を選択します。



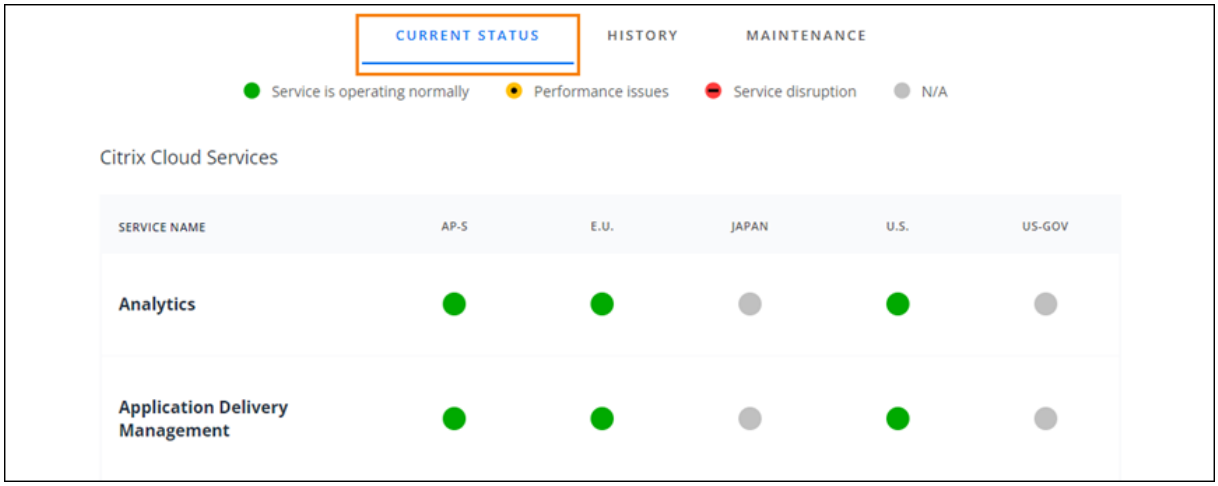
このダッシュボードを使用して、次の条件の詳細を確認します:

- 地理的リージョンごとにグループ化された、すべての Citrix Cloud サービスの現在のヘルス状況
- 過去 7 日間の各サービスのヘルス履歴
- 特定のサービスのメンテナンス期間

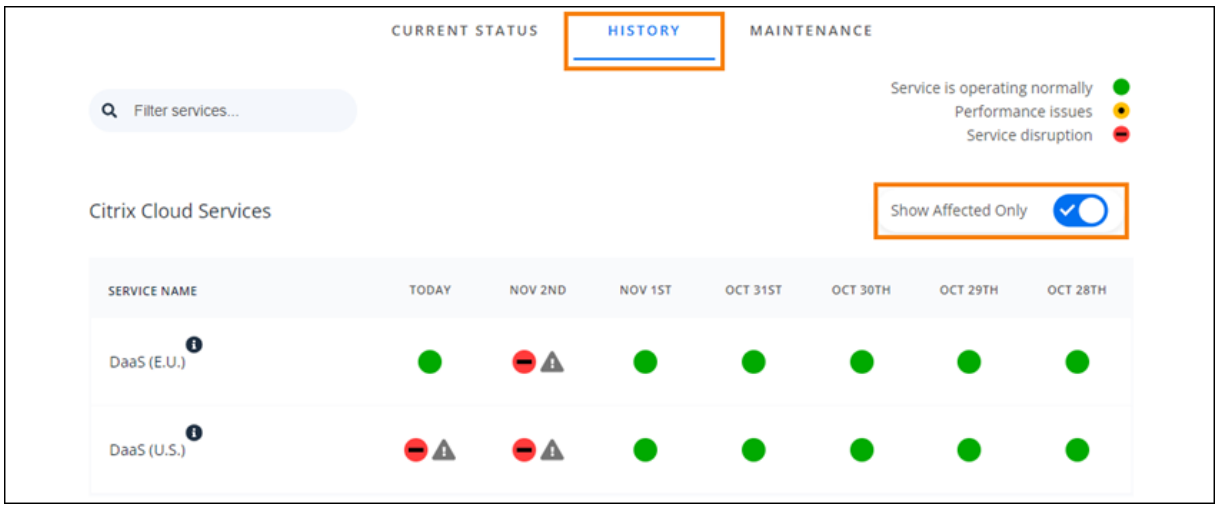
メンテナンスウィンドウやサービスインシデントなど、イベントに関する通知をサブスクライブすることもできます。

ヘルスおよびメンテナンスの状況を表示する

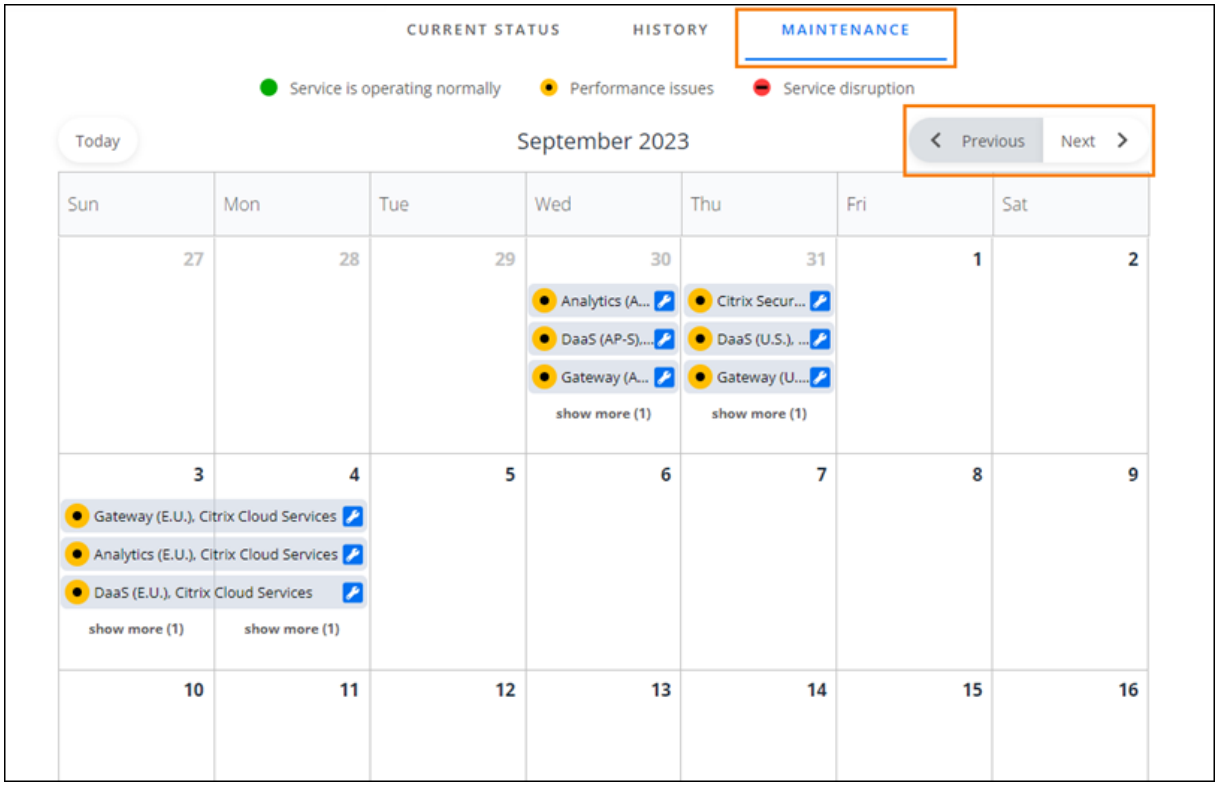
[**Current Status**] を選択して、各地理的リージョンのすべての Citrix Cloud サービスとプラットフォームコンポーネントの現在のヘルス状況を表示します。



[**History**] を選択して、過去 7 日間のすべての Citrix Cloud サービスとプラットフォームコンポーネントのヘルス状況を表示します。過去 7 日間にメンテナンスまたはヘルスイベントが発生したサービスのみを表示するには、[**Show Affected Only**] を選択します。



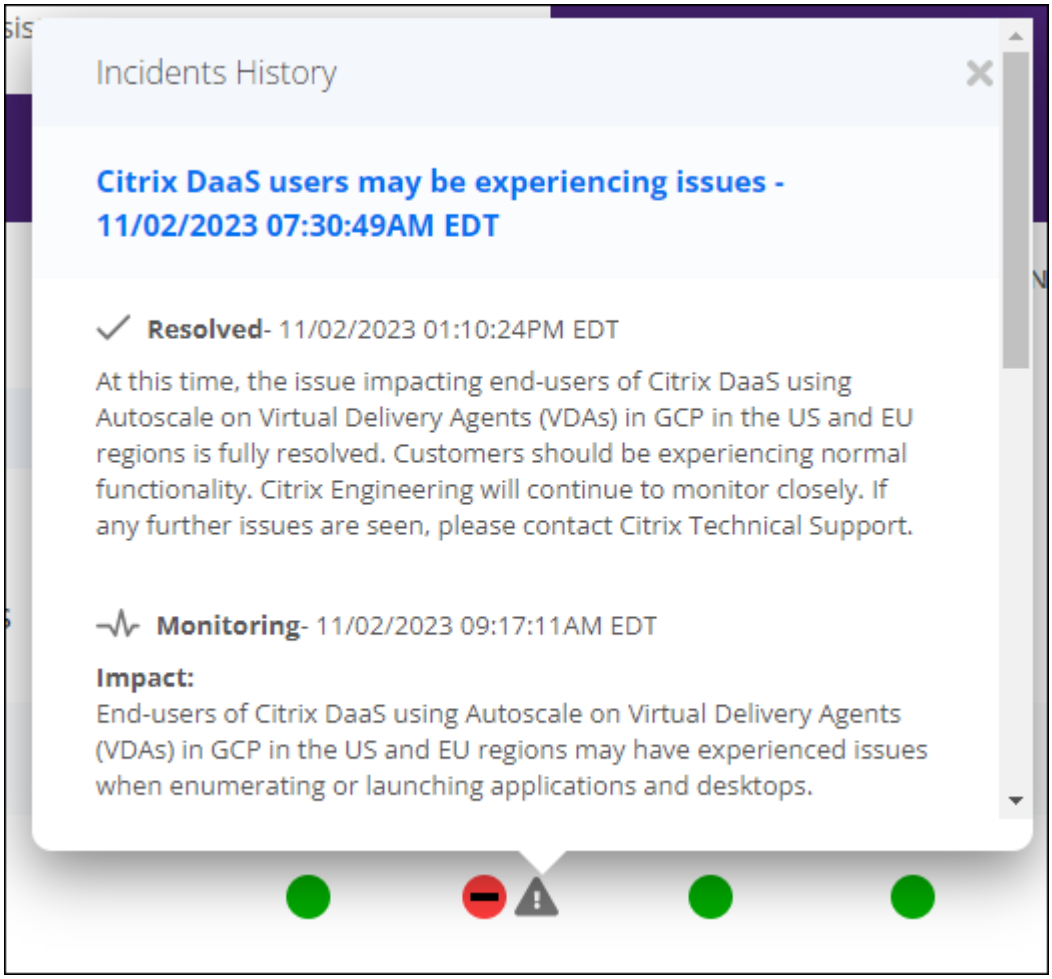
[**Maintenance**] を選択して、サービスのメンテナンス期間のカレンダービューを表示します。[**Next**] を選択して、今後の月にスケジュールされているメンテナンスイベントを表示します。今月のイベントに戻るには、[**Previous**] を選択します。



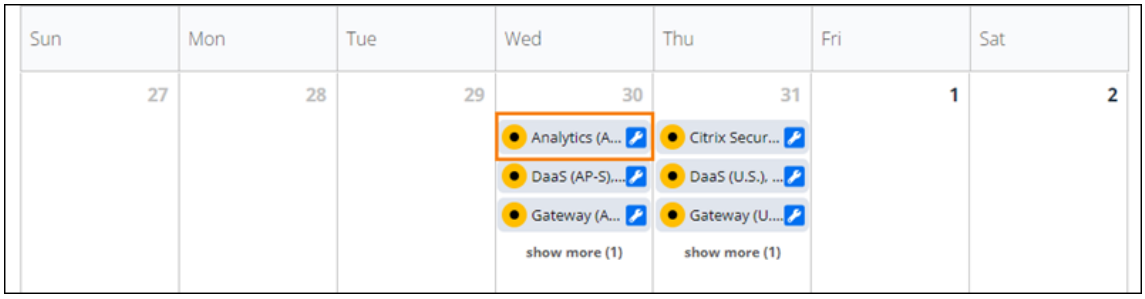
サービスインシデントの詳細を表示する

影響を受けるサービスのサービス正常性インシデントに関する詳細情報を表示するには、次の手順に従います:

- [History] 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、サービス正常性インシデントに関する詳細情報を表示します。



- [Maintenance] 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状況ページを表示します。



インシデント通知の頻度

サービス正常性インシデントが発生した場合、Citrix は status.cloud.com に投稿するときに次の特性を考慮します:

- 影響の持続時間
- 影響の頻度

このインシデントへの対応中、Citrix は次の種類の通知を Cloud Health Dashboard: に投稿します:

- **Investigating**: この通知は、Citrix が問題を緊急であると認識し、問題を調査していることを示します。
- **Monitoring**: この通知は、Citrix が根本原因を特定し、問題を軽減中であることを示します。
- **Resolved**: 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と監視中、Citrix は 60～120 分間隔で更新を投稿します。これらの更新には次のような情報が含まれる場合があります:

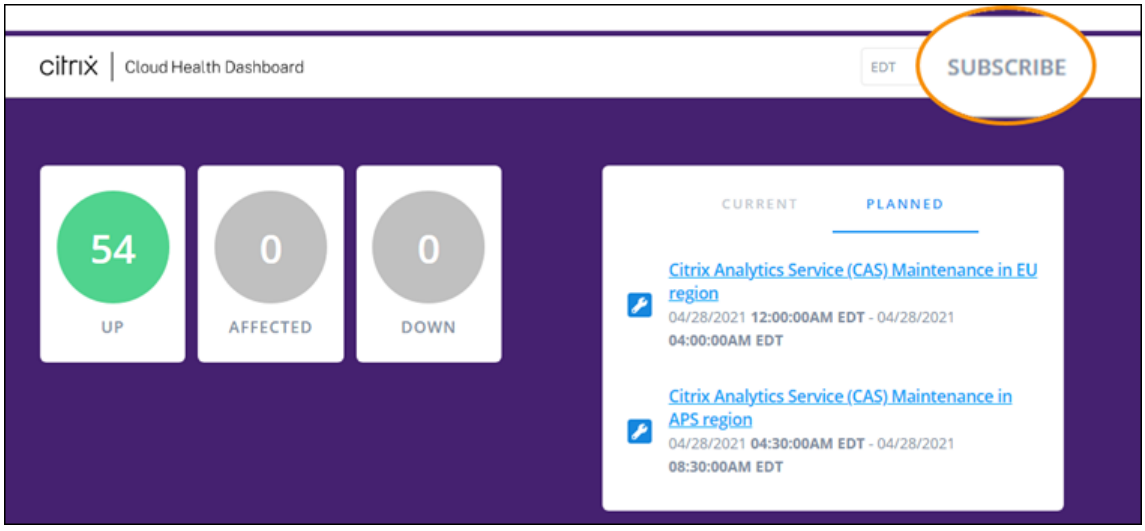
- インシデントに関する追加の詳細。
- インシデントを解決するために Citrix が実行しているアクションを説明する。
- 前回の更新以降、新しい変更が発生していないことを示す。

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を示している可能性があります。

通知にサブスクライブする

次の方法を使用して、サービス正常性イベントに関する通知を受け取ることができます:

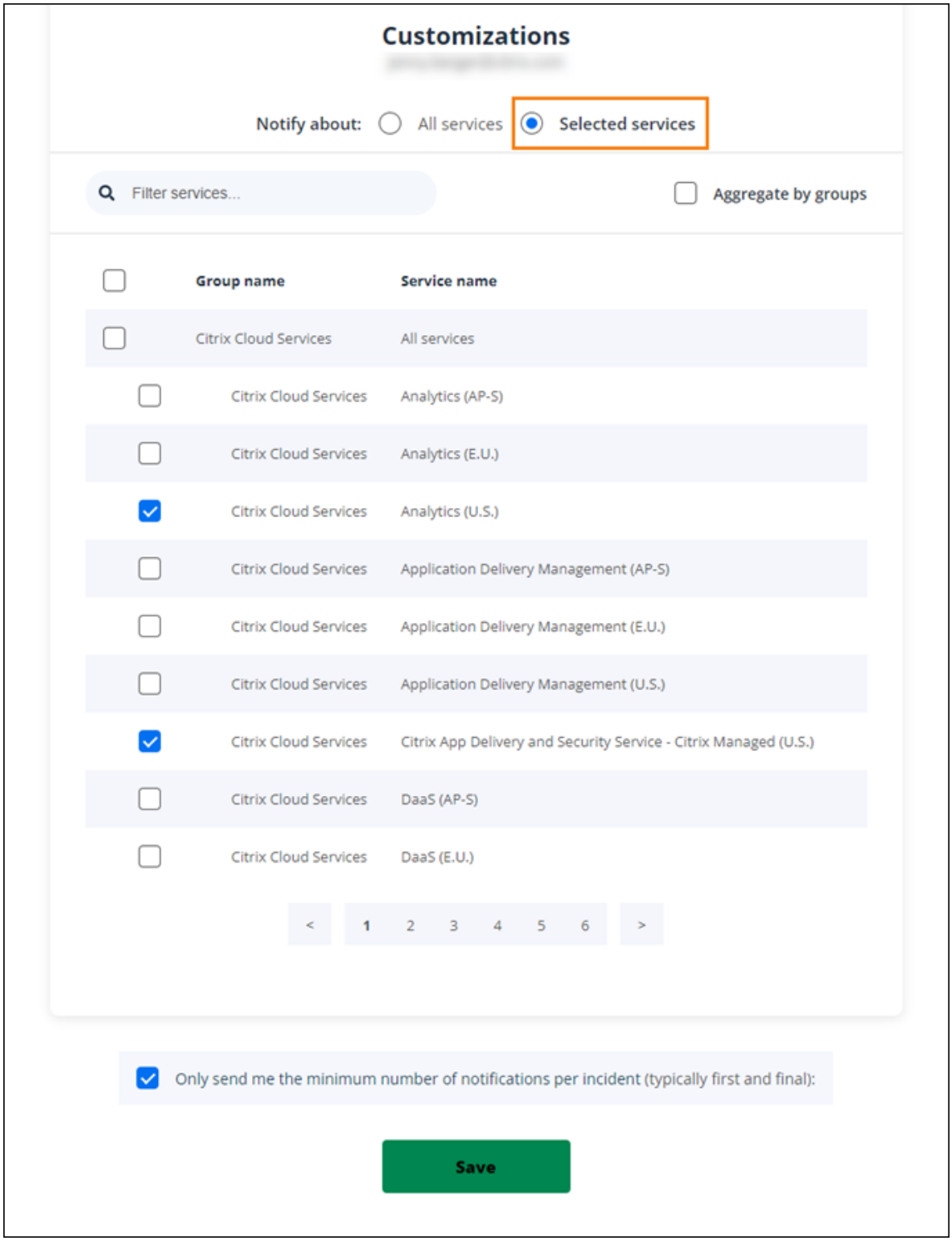
- ダッシュボードの右上にある［**Subscribe**］を選択し、使用する通知方法を選択します。メールや電話（ショートメッセージサービス）など、いくつかの方法から選択できます。



- RSS リーダーに次の URL を入力して、Citrix Cloud Health RSS フィードにサブスクライブします:
  - 1 つのフィードでサービスインシデントとメンテナンスの通知を受信するには、`https://status.cloud.com/?format=atom`にサブスクライブします。
  - サービスインシデント通知のみを受信するには、`https://status.cloud.com/atom/incidents`にサブスクライブします。
  - メンテナンス通知のみを受信するには、`https://status.cloud.com/atom/maintenances`にサブスクライブします。

リージョン内の特定のサービスにサブスクライブする

1. ダッシュボードの右上隅にある［**Subscribe**］を選択し、使用する通知方法を選択します。
2. 選択したサブスクライブ方法の連絡先の詳細または URL を入力し、［**accept terms & services**］を選択します。［次へ］を選択します。［**Customizations**］ページが表示され、デフォルトで［**Selected services**］が選択されています。
3. ［**Customizations**］ページで、複数ページの一覧から必要なリージョンのサービスを選択します。

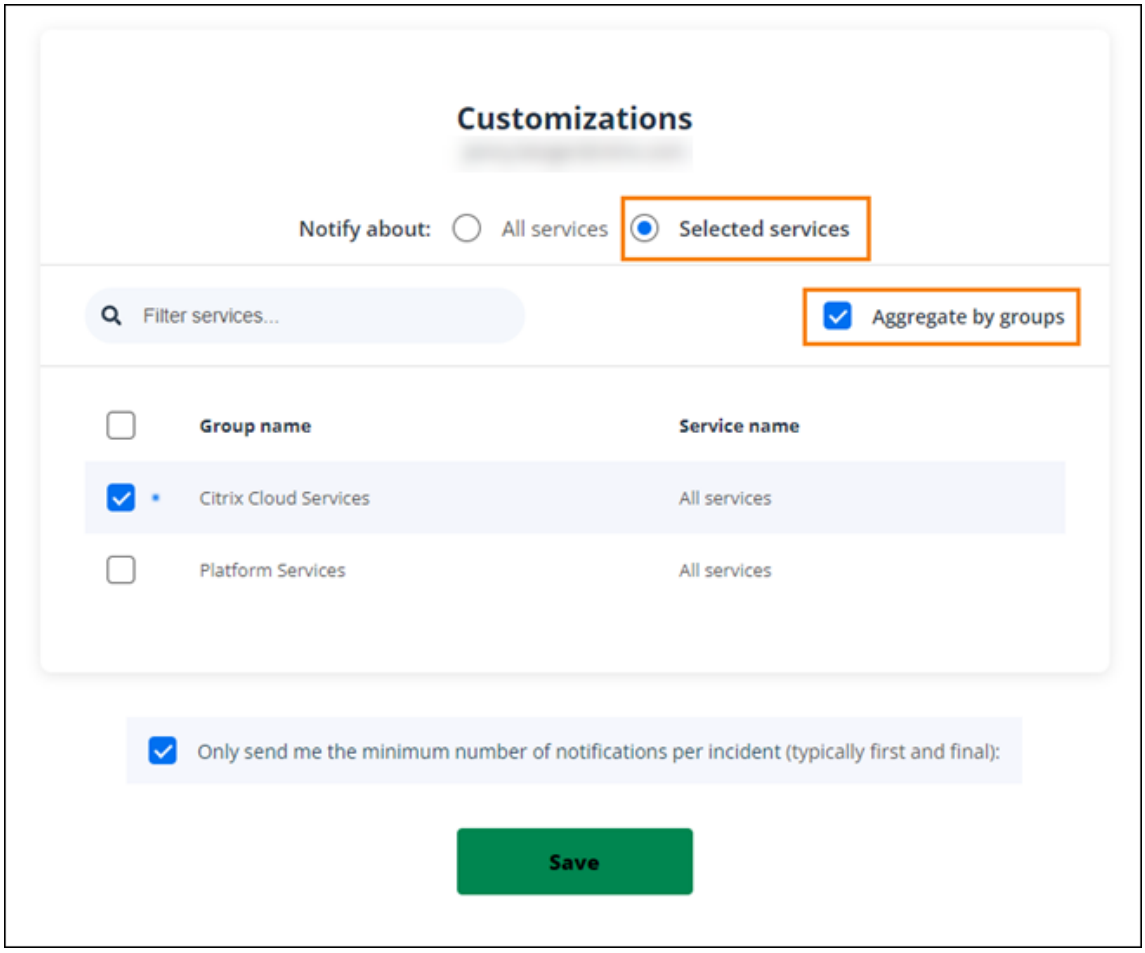


4. 各インシデントの最初と最後の通知のみを受信するには、［**Only send me the minimum number of notifications per incident**］を選択します。
5. ［保存］をクリックします。

特定のサービスグループにサブスクライブする

すべてのリージョンのすべてのクラウドサービス（Analytics や DaaS など）またはすべてのプラットフォームサービス（コントロールプレーンやクラウド API など）の通知にサブスクライブできます。

1. ダッシュボードの右上隅にある［**Subscribe**］を選択し、使用する通知方法を選択します。
2. 選択したサブスクライブ方法の連絡先の詳細または URL を入力し、［**accept terms & services**］を選択します。［次へ］を選択します。［**Customizations**］ページが表示され、デフォルトで［**Selected services**］が選択されています。
3. ［**Customizations**］ページで［**Aggregate by groups**］を選択します。
4. ［**Citrix Cloud Services**］または［**Platform Services**］のいずれかを選択します。

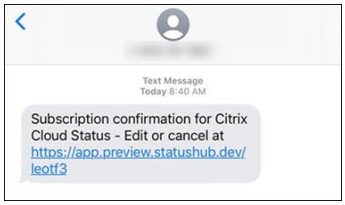


5. 各インシデントの最初と最後の通知のみを受信するには、［**Only send me the minimum number of notifications per incident**］を選択します。
6. ［保存］をクリックします。

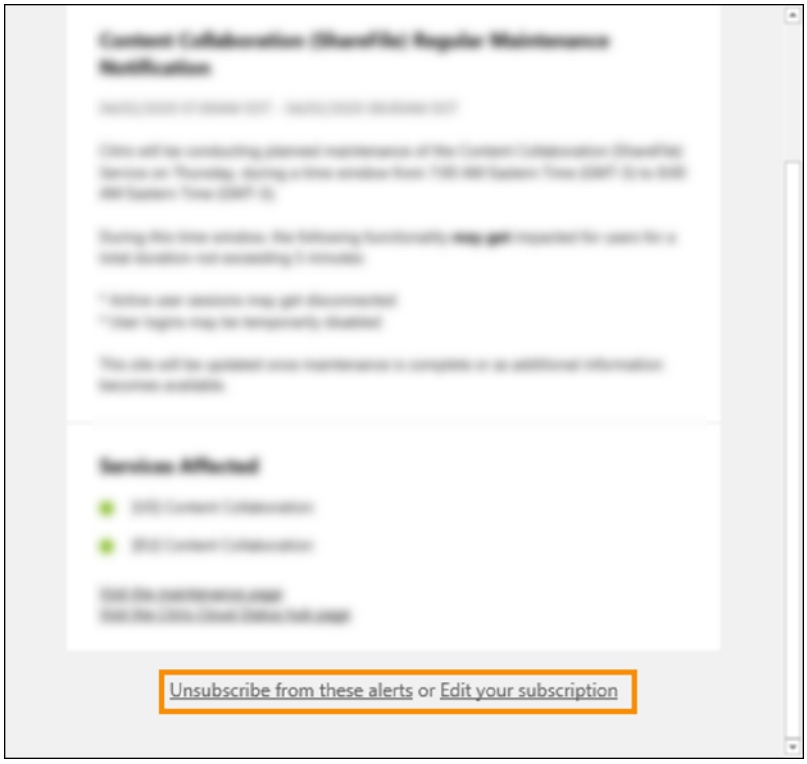
通知のサブスクリプション解除

サブスクリプション方法に応じて、サブスクリプションを解除または変更するためのリンクは、受信する確認メッセージ（電話通知にサブスクライブする場合など）または各通知メッセージ（メール通知にサブスクライブする場合など）に含まれます。例：

- サブスクリプションオプション付きの電話通知：



- サブスクリプションオプション付きの通知メール：



すべての通知のサブスクリプションを解除し、すべてのサブスクリプション方法を削除するには：

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを解除するリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. サブスクリプション方法に応じて、［**Edit Subscriptions**］ページで次のオプションのいずれかを使用します：
    - ［**Remove all subscriptions**］を選択します。

- [**Unsubscribe**]を選択します。[**Unsubscribe methods**]ページから、[**Remove all subscriptions**]を選択します。

特定のサブスクリプション方法のすべての通知からサブスクリプションを解除するには:

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを解除するリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. サブスクリプション方法に応じて、[**Edit Subscriptions**] ページで次のオプションのいずれかを使用します:

   - 削除するサブスクリプション方法を選択します。サブスクリプションはすぐに削除されます。
   - [**Unsubscribe**] を選択します。[**Unsubscribe methods**] ページから、削除するサブスクリプション方法を選択します。サブスクリプションはすぐに削除されます。

サービス通知の変更

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを編集するためのリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. [**Edit Subscriptions**] ページから、管理するサブスクリプション方法を選択します。
3. [**Customizations**] ページで、必要に応じて通知を受け取るサービスを選択するか、通知を不要にするサービスをオフします。
4. [**Save**] を選択します。

システムおよび接続要件

July 2, 2024

Citrix Cloud では、管理機能（Web ブラウザー経由）およびご利用中の展開環境のリソースに接続される（他のインストールされたコンポーネントからの）操作要求を使用できます。この記事には、ご利用中のリソースと Citrix Cloud 間の接続を確立するためのシステム要件、必要なアクセス可能インターネットアドレス、および考慮事項について記載されています。

システム要件

Citrix Cloud の最小構成要件は、以下のとおりです。

- Active Directory ドメイン

- ドメインに参加している Citrix Cloud Connector 用の 2 つの物理マシンまたは仮想マシン。詳しくは、「Citrix Cloud Connector の技術詳細」を参照してください。
- ワークロードおよび StoreFront などの他のコンポーネントをホストするための物理マシンまたは仮想マシン（ドメイン参加済み）。特定のサービスのシステム要件について詳しくは、各サービスの Citrix ドキュメントを参照してください。

スケールとサイズの要件について詳しくは、「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

サポートされる **Web** ブラウザー

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

Transport Layer Security（**TLS**）の要件

Citrix Cloud は、コンポーネント間の TCP ベースの接続で TLS（Transport Layer Security）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ていません。

Citrix Cloud にアクセスするには、TLS 1.2 対応のブラウザーを使用して、承認済みの暗号の組み合わせを構成している必要があります。詳しくは、「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にサインインすると使用できる Web ベースのコンソールです。コンソールの Web ページでは、サインイン時またはその後に特定の操作を実行するために、インターネットの他のリソースが必要になります。

プロキシ構成

プロキシサーバー経由で接続すると、使用している Web ブラウザーに適用された構成と同じ構成で管理コンソールが機能します。コンソールは、ユーザー環境で機能するため、ユーザー認証を必要とするプロキシサーバーの構成は通常どおりに機能します。

ファイアウォール構成

管理コンソールを機能させる場合、発信接続のためにポート 443 を開いている必要があります。コンソール内を移動して、一般的な接続性をテストできます。必要なポートの詳細については、「送受信ポートの構成」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、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 のコンテンツを表示できるようにするために、Citrix ではアドレス`https://citrix-cloud-content.customer.pendo.io/`を利用できるようにすることをお勧めします。

以下サービスは、Pendo コンテンツを表示します:

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

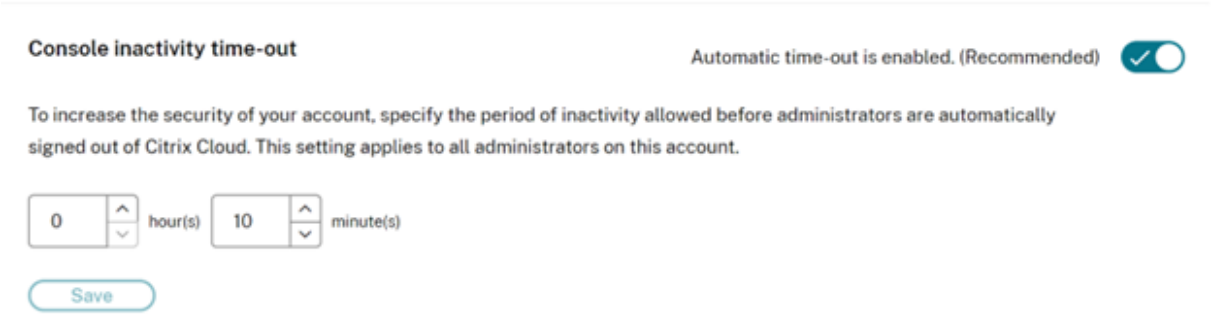
Pendo は、Citrix が顧客にクラウドサービスおよびサポートサービスを提供するために使用するサードパーティのサブプロセッサです。これらのサブプロセッサの完全な一覧については、「Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates」を参照してください。

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、72 時間が経過すると、管理コンソールセッションがタイムアウトします: このタイムアウトは、コンソールアクティビティの有無にかかわらず発生します。

コンソールの非アクティブタイムアウトを設定可能

フルアクセス管理者は、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。一度構成されると、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。



この機能を有効にすると、管理者は設定された非アクティブ期間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存在せず、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:
>
> - デフォルトでは、この機能は無効になっています。
> - 構成可能な非アクティブタイムアウトは 10 分から 12 時間です。
> - 非アクティブタイムアウトのデフォルト値は 60 分間です。

Citrix Cloud へのライセンスサーバーの登録

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 ライセンスサーバーを Citrix Cloud に登録する場合、次のアドレスを使用できることを確認します:

- `https://trust.citrixnetworkapi.net`（コードを取得する場合）
- `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場合）
- `https://cis.citrix.com`（データをアップロードする場合）
- `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 ライセンスサーバーにプロキシサーバーを使用している場合、プロキシサーバーがライセンスサーバー製品ドキュメントの「プロキシサーバーの構成」の説明どおりに構成されていることを確認します。

Citrix Cloud Connector

Citrix Cloud Connectorは、Microsoft Windows サーバーで実行されるサービスセット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あります。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することができます。

Cloud Connector をインストールするために必要な条件については、「システム要件」を参照してください。操作には、Cloud Connector がポート 443 を使用して発信する必要があります。インストール後、使用されている Citrix Cloud サービスに応じて、Cloud Connector にアクセス要件が追加される場合があります。

Cloud Connector をホストするマシンには、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、長期間有効で安全な Web ソケットをサポートしている必要があります。ネットワークコンポーネントでタイムアウトが設定されている場合、設定は 2 分より長くする必要があります。

Cloud Connector と Citrix Cloud との接続の問題をトラブルシューティングするには、Cloud Connector 接続性チェックユーティリティを使用してください。このユーティリティは、Cloud Connector マシンで一連のチェックを実行し、Citrix Cloud と関連サービスにアクセス可能であることを確認します。環境でプロキシサーバーを使用している場合、すべての接続チェックはプロキシサーバーを介してトンネリングされます。ユーティリティをダウンロードするには、Citrix サポートの Knowledge Center でCTX260337を参照してください。

Cloud Connector の一般的なサービス接続要件

データセンターからインターネットへの接続に必要なのは、発信接続のためにポート 443 を開くことです。ただし、インターネットの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操作するには、追加の構成が必要です。詳しくは、「Cloud Connector のプロキシとファイアウォールの構成」を参照してください。

サービスを適切に操作し、消費するには、この記事の各アドレスが利用可能である必要があります。次の一覧では、ほとんどの Citrix Cloud サービスに共通したアドレスを表示します:

- `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 の更新を格納する Azure Blob Storage へのアクセスを提供します）
- `https://*.servicebus.windows.net`（ログおよび 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）

Citrix Cloud サービスは動的であり、IP アドレスは定期的に変更されるため、これらのアドレスは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、グループポリシーを使用してこれらのアドレスを構成して管理します。また、組織で消費するサービスに適用できるアドレスのみを構成してください。

オンプレミス製品の登録を実行するために Citrix ライセンスサーバーで Citrix Cloud を使用している場合、追加で必要な連絡先アドレスに関しては、本記事の「Citrix Cloud へのライセンスサーバーの登録」を参照してください。

Cloud Connector で許可されている **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するために、Citrix は次のリソースを提供しています。

- allowlist.json
- CTX270584: Citrix Gateway Service –Points of Presence（PoPs）

ファイアウォールを構成するときは、これらの両方のリソースを参照して、サービスの展開に必要な 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）を使用する場合は、コネクタがリソースの場所にある他のすべてのコネクタの選出エンドポイントにアクセス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 上にあり、次の URL を通じてアクセスできます: `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`。

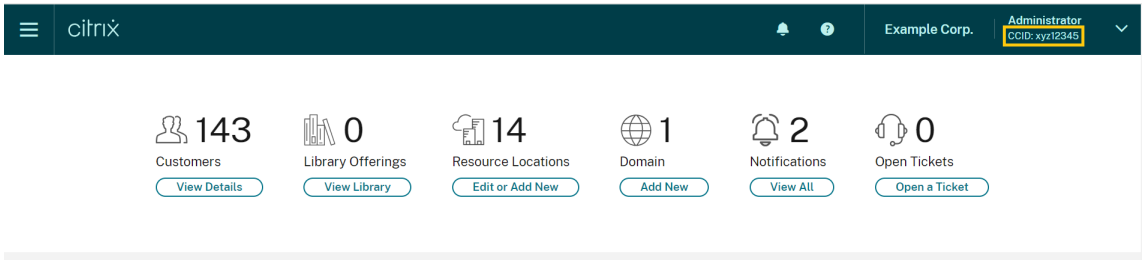
コネクタがこのアドレスで通信できない場合、LHC イベント中に複数のブローカーが選出され、仮想アプリとデスクトップの起動が断続的に失敗する可能性があります。詳しくは、「リソースの場所に Cloud Connector が複数存在する場合」を参照してください。

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 を使用する場合は、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 への Citrix Cloud Connector のアクセスを許可する必要があります。たとえば、`https://aauth.xyz.com`を許可します。詳しくは、「アダプティブ認証」を参照してください。

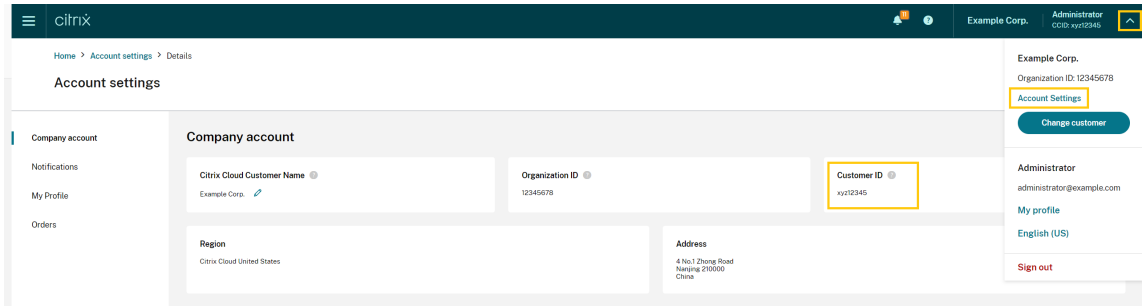
Allowlist.json　allowlist.json ファイルはhttps://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.jsonにあり、Cloud Connector がアクセスする FQDN がリストされています。この一覧は製品ごとにグループ化されており、一覧の中に FQDN の各グループの変更ログも記載されています。

これらの FQDN の一部は、顧客に固有のものであり、角かっこで囲まれたテンプレート化されたセクションがあります。これらのテンプレート化されたセクションは、使用する前に実際の値に置き換える必要があります。たとえば、<CUSTOMER_ID>.xendesktop.netの場合、<CUSTOMER_ID>を Citrix Cloud アカウントの実際の顧客 ID に置き換えます。顧客 ID は、次のコンソールの場所にあります:

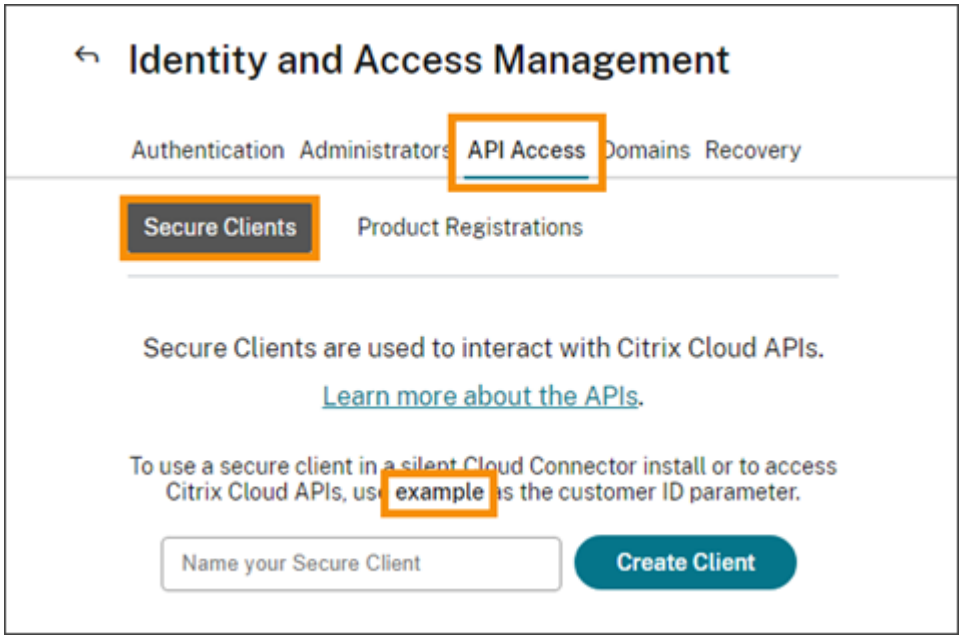
- 画面の右上隅、Citrix Cloud アカウントの顧客名の下。



- ［アカウント設定］ページ、**Citrix Cloud** の顧客 **ID**（**CCID**）の下。



- ［セキュアクライアント］タブ（［**ID** およびアクセス管理］**>**［**API** アクセス］**>**［セキュアクライアント］。



ゲートウェイサービスのポイントオブプレゼンス　allowlist.json ファイルに含まれる FQDN の一部は、CTX270584: Citrix Gateway Service –Points of Presence (PoPs)にも含まれています。ただし、CTX270584 には、クライアントがアクセスする次のような FQDN も含まれます:

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

証明書の検証

Cloud Connector が通信する Cloud Connector バイナリおよびエンドポイントは、ソフトウェアのインストール時に検証された X.509 証明書で保護されています。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している必要があります。これらの要件をまとめた一覧については、「証明書の検証要件」を参照してください。

SSL 暗号化解除

一部のプロキシで SSL 暗号化解除を有効にすると、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。この問題の解決について詳しくは、CTX221535を参照してください。

クラウドサービス用の **Citrix Connector Appliance**

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あります。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することができます。

Connector Appliance をインストールするために必要な条件については、「システム要件」を参照してください。

操作には、ポート 443 を使用して発信する必要があります。ただし、インターネットの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操作するには、追加の構成が必要です。

Citrix Cloud サービスを適切に操作し消費するには、以下のアドレスが利用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顧客は、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://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

ネットワークの要件

Connector Appliance 環境の構成が以下の要件を満たしていることを確認します:

- ネットワークにより、Connector Appliance は DHCP を使用して、DNS および NTP サーバー、IP アドレス、ホスト名、およびドメイン名を取得できます。または、Connector Appliance コンソールでネットワーク設定を手動で設定することもできます。
- このネットワークは、Connector Appliance によって内部的に使用される 169.254.0.1/24、169.254.64.0/18、または 169.254.192.0/18 というリンクローカル IP 範囲を使用するようには構成されていません。
- ハイパーバイザー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るか、DHCP が NTP サーバー情報を Connector Appliance に提供します。
- Connector Appliance でプロキシを使用する場合、プロキシは認証されていない、または基本認証が使用されている必要があります。

Citrix Analytics Service の接続性

- 新機能や重要なコミュニケーションを含む製品内メッセージの場合: `https://citrix-cloud-content.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ド（配布準備）について詳しくは、「サポートされるデータソース」を参照してください。

コンソールサービスの接続性

完全なインターネット接続要件については、NetScaler 製品ドキュメントにある「Supported ports」を参照してください。

Citrix DaaS サービスの接続性

Citrix リソースの場所/Cloud Connector:

- Cloud Connector の一般的なサービス接続要件
- `https://[customerid].xendesktop.net`。この`[customerid]`は、Citrix Cloud 管理コンソールの［セキュアクライアント］タブ（［**ID** およびアクセス管理］**>**［**API** アクセス］**>**［セキュアクライアント］）に表示される顧客 ID パラメーターです。
  - Citrix Virtual Apps Essentials を使用している顧客は、代わりに`https://*.xendesktop.net`を使用する必要があります。
- ［Quick Deploy］を使用して Citrix DaaS をインストールするお客様は、次の追加アドレスを連絡可能にしておく必要があります:
  - `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顧客は、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 がサービスと通信する方法の概要については、Citrix Tech Zone の Web サイトにある「Citrix DaaS の図」を参照してください。

管理コンソール:

- `https://*.citrixworkspacesapi.net`（Rendezvous プロトコルには必要ありません）

- https://*.citrixnetworkapi.net（Rendezvous プロトコルには必要ありません）
- https://*.cloud.com（Rendezvous プロトコルには必要ありません）
- https://[customerid].xendesktop.net。この[customerid]は、Citrix Cloud 管理コンソールの［セキュアクライアント］タブ（[**ID** およびアクセス管理］**>**［**API** アクセス］**>**［セキュアクライアント]）に表示される顧客 ID パラメーターです。
  - Citrix Virtual Apps Essentials を使用している顧客は、代わりにhttps://*.xendesktop.netを使用する必要があります。
- https://*.*.nssvc.net（Citrix DaaS Standard for Azure の場合は不要）
  - すべてのサブドメインを有効にできない顧客は、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
- 新機能や重要なコミュニケーションを含む製品内メッセージの場合: https://citrix-cloud-content.customer.pendo.io/

Rendezvous プロトコル

Citrix Gateway サービスを使用する場合、Rendezvous プロトコルにより、VDA が Citrix Cloud Connector 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の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アドレスに接続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次のセクションを参照してください。

- Rendezvous V1
- Rendezvous V2

ローカルホストキャッシュの要件

ファイアウォールで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。これには、Cloud Connector が構成データを Citrix Cloud と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。この MDF 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 間の同期が失敗します。停止状態が発生した場合、Cloud Connector にある構成データが古くなっているため、ユーザーは作業を続行できません。

この機能について詳しくは、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 のアップグレード要件

Citrix DaaS の［完全な構成］インターフェイスを使用すると、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、またはスケジュールした時間に、アップグレードできます。VDA のアップグレード機能について詳しくは、「［完全な構成］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 の URL が許可リストに追加されました。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。
  - 実稼働 - 米国（US）: `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - 実稼働 - 欧州連合（EU）: `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - 実稼働 - 南アジア太平洋（APS）: `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - 実稼働 - 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/*`
- この機能を使用するには、VDA Upgrade Agent が動作する必要があります。VDA で実行されている VDA Upgrade Agent は、Citrix DaaS と通信します。次の URL が許可リストに追加されていることを確認します:
  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`。この `[customerid]` は、Citrix Cloud 管理コンソールの［セキュアクライアント］タブ（［**ID** およびアクセス管理］**>**［**API** アクセス］**>**［セキュアクライアント］）に表示される顧客 ID パラメーターです。
  - `http://xendesktop.net/citrix/VdaUpdateService/*`

Endpoint Management サービスの接続性

Citrix リソースの場所/Cloud Connector:

- Cloud Connector の一般的なサービス接続要件

- 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 サービスの接続性

- Cloud Connector の一般的なサービス接続要件
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできない顧客は、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：
>
> SSL インターセプションは、Citrix Gateway アドレスでは実行できません。一部のプロキシで SSL インターセプションを有効にすると、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。

NetScaler Intelligent Traffic Management サービスの接続性

- https://*.cedexis-test.com
- https://*.citm-test.com
- https://cedexis.com
- https://cedexis-radar.net

SD-WAN Orchestrator サービスの接続性

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。

Remote Browser Isolation（旧称 Secure Browser）サービスの接続

Citrix リソースの場所/Cloud Connector：

Cloud Connector の一般的なサービス接続要件

管理コンソール：

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

Citrix Secure Private Access サービスの接続性

- https://*.netscalergateway.net
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできない顧客は、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

Citrix Workspace Service の接続性

- https://*.cloud.com
- https://*.citrixdata.com
- 新機能や重要なコミュニケーションを含む製品内メッセージの場合: https://citrix-cloud-content.customer.pendo.io/

Global App Configuration Service の接続性

https://discovery.cem.cloud.us

このサービスについて詳しくは、次のリソースを参照してください:

- Workspace アプリの設定のカスタマイズ - Citrix Workspace 製品ドキュメント
- Global App Configuration Service - Citrix 開発者向けドキュメント

Citrix Workspace アプリの接続

次の URL を許可リストに追加します:

- https://*.cloud.com
- ID プロバイダーのアドレス。対応する ID プロバイダーのドキュメントの手順を参照してください。
- https://*.wsp.cloud.com

特定の URL については、次のアドレスへのアクセスを許可します:

- <yourcustomer>.cloud.com

Citrix Secure Private Access

- ngspolicy.netscalergateway.net
- config.netscalergateway.net
- app.netscalergateway.net
- http://tunnel.netscalergateway.net/

Global App Configuration Service

この記事の「Global App Configuration Service の接続性」を参照してください。

認証

- accounts.cloud.com
- accounts-dsauthweb.cloud.com

ID プロバイダーの URL がエンドユーザーのデバイスからもアクセスできることを確認してください。

Citrix Analytics Service

- locus.analytics.cloud.com

場所に応じて、次の一覧から適切な URL へのアクセスを有効にします:

- US: citrixanalyticseh.servicebus.windows.net
- EU: citrixanalyticseheu.servicebus.windows.net
- APS: citrixanalyticsehaps.servicebus.windows.net

Workspace のグラフィカルインターフェイスアセット

- ctx-ws-assets.cloud.com

個人設定、通知、および機能のロールアウト

- customer-**interface**-personalization.us.wsp.cloud.com
- user-personalization.us.wsp.cloud.com
- admin-notification.us.wsp.cloud.com
- customer-**interface**-personalization.eu.wsp.cloud.com
- user-personalization.eu.wsp.cloud.com
- admin-notification.eu.wsp.cloud.com

- customer-**interface**-personalization.ap-s.wsp.cloud.com
- user-personalization.ap-s.wsp.cloud.com
- admin-notification.ap-s.wsp.cloud.com
- feature-rollout.us.wsp.cloud.com
- feature-rollout.eu.wsp.cloud.com
- feature-rollout.ap-s.wsp.cloud.com

デバイス登録サービス

- device-registration.us.wsp.cloud.com
- device-registration.eu.wsp.cloud.com
- device-registration.ap-s.wsp.cloud.com

プッシュ通知サービス

- push-events-signalr.us.wsp.cloud.com
- push-events-signalr.eu.wsp.cloud.com
- push-events-signalr.ap-s.wsp.cloud.com

Citrix Gateway サービス

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

Citrix フェデレーション認証サービス（**FAS**）を使用した **Workspace** のシングルサインオン

コンソールと FAS サービスは、それぞれユーザーのアカウントとネットワークサービスアカウントを使用して次のアドレスにアクセスします。

- ユーザーアカウントの下の FAS 管理コンソール:
  - https://*.cloud.com
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/
  - サードパーティの ID プロバイダーが必要とするアドレス（環境で使用されている場合）
- ネットワークサービスアカウントの下の FAS サービス:
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/

環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが環境に応じて適切に構成されていることを確認してください。

Citrix Workspace アプリの ID プロバイダーとして Active Directory または Active Directory および時間ベースのワンタイムパスワード（TOTP）を使用している場合は、`login.cloud.com`も許可リストに登録する必要があります。他の ID プロバイダーを使用している場合は、ID プロバイダーの URL を個別に許可します。

CAS のイベントハブの URL もリージョン固有です。citrixanalyticseh-alias.servicebus.windows.net

Workspace Environment Management サービスの接続性

Citrix リソースの場所/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。

展開計画

July 2, 2024

カスタマージャーニーの観点については、Citrix Success Centerにアクセスしてください。Success Center では、Citrix をご利用いただくにあたり通過する 5 つの主要な段階（プラン、ビルド、ロールアウト、管理、最適化）に関するガイダンスを提供しています。Success Center の記事とガイドはこのドキュメントの付属品であり、ソリューションに基づいた幅広い視点を提供しています。

サービストライアル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のトライアルを提供しています。トライアルには有料サービスと同じ機能が備わっているため、検証用の展開やパイロット展開に適しています。詳しくは、「Citrix Cloud サービスのトライアル」を参照してください。

一般に、有料サービスの使用権には、月単位、年単位、または期限付きの期間を設定できます。使用権の期限が近づくと、Citrix Cloud はリマインダーを送信し、サービスを過度に中断することなく使用権を更新できるように猶予期間を設けます。使用権の更新の詳細については、「Citrix Cloud サービスのサブスクリプション延長」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、南アジア太平洋の 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ときは、パフォーマンスとビジネスの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できるサービスの詳細については、「地理的な考慮事項」を参照してください。

展開リソース

- Citrix Cloud の回復性
- Tech Zone の概念実証ガイド
- Tech Zone リファレンスアーキテクチャ
- Cloud Connector のサイズおよびスケールの考慮事項
- ローカルホストキャッシュのスケールおよびサイズの考慮事項
- Citrix DaaS 用のオンプレミス StoreFront 認証参照アーキテクチャ

移行リソース

- 概念実証：自動構成ツール
- Citrix Virtual Apps and Desktops のオンプレミスから Citrix Cloud への移行
- Citrix Virtual Apps and Desktops の VMware vSphere から Microsoft Azure 上の Citrix DaaS サービスへの移行
- Citrix Endpoint Management を使用した Android Device Administrator から Android Enterprise への移行

追加情報

- Citrix Discussions：Citrix Cloud：Citrix Cloud および Citrix Cloud サービスの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
  - Citrix ID と認証の概要

Citrix Cloud サービスのトライアル

July 2, 2024

個別の Citrix Cloud サービスのトライアルは、Citrix Cloud 管理コンソールで配信されます。サービストライアルの機能は、製品版サービスと同じであるため、概念実証（POC）、パイロット展開などの用途に適しています。

Citrix Cloud サービスを購入する準備ができたら、トライアルは製品版サービスに変換されます。何かを再構成したり、別の実稼働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 サービスのトライアルに適用されます。トライアル期間が異なるサービスについては、別のセクションで説明します。

		Citrix Cloud トライアル
	許可される利用者の数	25
	トライアルの最大期間	60 暦日
	猶予期間	トライアル期間満了後 14 日
	データの保持期間	トライアル期間満了後 90 暦日
	可用性	制限された可用性
	リソースの場所	顧客が提供および構成
	ユーザーセッションの長さ	無制限
	ローカルの Microsoft Active Directory との統合	はい
	リソースの場所の選択	はい
	オンプレミスへの展開	はい
	Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）	完全な機能セット
	Endpoint Management	完全な機能セット
	カスタマイズ可能	はい

サービストライアルを要求する

Citrix Cloud トライアルアクセス権は、サービスごとに管理されます。一部のサービスでは、本記事の「サービストライアルの要求」で説明されているように、トライアルを要求できます。その他のサービスについては、本記事の「サービスデモの要求」で説明されているように、トライアルアクセス権を受け取る前にデモを要求する必要があります。

サービストライアル期間

ほとんどのサービスでは、トライアルリクエストが承認されてから 60 日間サービスを試すことができます。サービスのトライアルをリクエストできるのは一度のみです。

サービスサブスクリプションを購入する

トライアル期間中またはデータ保持期間中はいつでも、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 サービスを購入する」を参照してください。

サブスクリプションを購入すると、トライアルは製品版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、トライアル期間中に追加したデータはそのまま残っています。

Citrix DaaS Standard for Azure

このセクションでは、Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure）の以下の種類のトライアルについて説明します:

- 自動承認のトライアル: Citrix Cloud 管理コンソールからトライアルを要求すると、トライアルが自動的に承認され、使用できるようになります。
- 営業担当者承認のトライアル: Citrix の営業担当者に連絡をとってトライアルを要求すると、営業担当者がトライアルを承認します。承認後、トライアルを使用する準備が整います。

		自動承認のトライアル	営業担当者承認のトライアル
	トライアルの最大期間	7 暦日	14 暦日
	猶予期間	トライアル期間満了後 1 暦日	トライアル期間満了後 14 暦日
	データの保持期間	トライアル期間満了後 30 暦日	トライアル期間満了後 90 暦日

トライアルの種類に応じて、7 日または 14 日間サービスを使用できます。サービスのトライアルをリクエストできるのは一度のみです。

トライアルには、トライアル期間終了後にサービスにアクセスするための猶予期間が含まれます。この猶予期間により、サービスのサブスクリプションを購入したり、追加したデータを削除したりできます。猶予期間が終了すると、管理者とユーザーはサービスにアクセスできなくなります。

Citrix は、トライアルの種類に応じて、トライアル期間終了後 30 日間または 90 日間、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すると、管理者とユーザーはデータをそのまま引き継いでサービスにアクセスできます。

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

サービスデモの要求

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要求する必要があります。デモをリクエストすると、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、Citrix の営業担当者は、お客様が正常にサービスを使用するために必要なすべての情報を提供します。

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、試用するサービスの ［デモのリクエスト］を選択します。そのサービスのデモ要求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 の営業担当者が詳細について連絡し、サービスの利用方法について説明します。

サービストライアルの要求

1. Citrix Cloud アカウントにサインインします。
2. 管理コンソールで、試用するサービスの ［トライアルのリクエスト］を選択します。

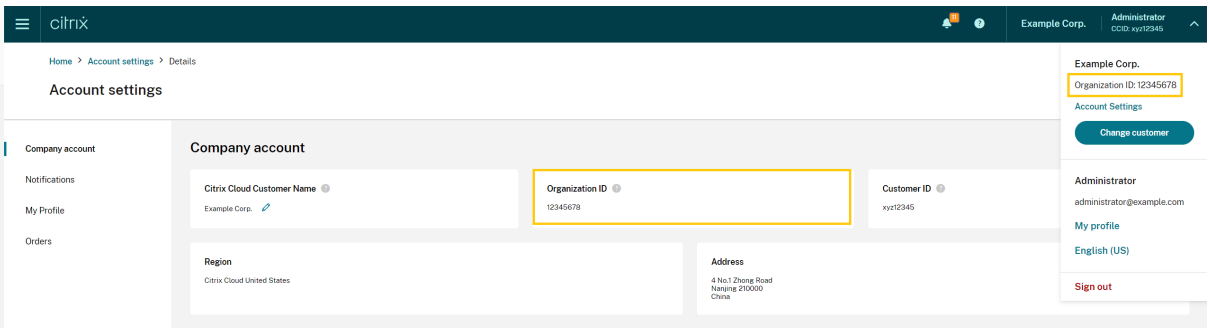
トライアルが承認されて使用できるようになると、Citrix からメール通知が送信されます。

> 注:
>
> 最高のカスタマーエクスペリエンスを提供するために、Citrix にはいつでも、トライアルの参加者数を制限して承認する権利があります。

Citrix Cloud サービスの購入

トライアルを製品版サービスに移行する場合は、https://www.citrix.com/buy/にアクセスし、地域の Citrix パートナーを検索してください。

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。



追加情報

- Citrix Cloud サービス利用規約
- 「Citrix Cloud の基礎」コースには、トライアルの申請方法について説明した短い動画があります。フルコースでは、Citrix Cloud プラットフォームのコンポーネントとそのサービスも説明します。

Citrix Cloud サービスのサブスクリプション延長

July 2, 2024

この記事では、購入した Citrix Cloud サービスのサブスクリプションがどのように期限切れになるのか、および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。

この記事の _ 月単位サブスクリプション _ とは、月ごとに購入されるサービスを指します。_ 年間サブスクリプション _ とは、年間ベースで購入されるサービスを指します。_ 複数年サブスクリプション _ とは、複数年ベースで購入されるサービスを指します。

> 注:
>
> Citrix Service Provider（CSP）は、CSP ディストリビューターにゼロドルの注文書を送信することにより、サブスクリプションを延長できます。CSP 製品の更新とライセンスについて詳しくは、Citrix Partner Central Web サイトから入手できる『*Citrix Service Provider Licensing Guide for Citrix Cloud*』を参照してください。

有効期限前

月単位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、既存のサブスクリプションの期限切れが近づいたときに、Citrix Cloud から一定の間隔で通知が送信されます。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促します。Citrix Cloud 管理コンソールには、次の通知が表示されます:

- 有効期限の 90 日前：黄色いバナーが開き、延長が必要なサービスとその有効期限が表示されます。この通知は 7 日ごとに、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：赤いバナーが開き、延長が必要なサービスと有効期限が表示されます。この通知は、サービスが延長されるまで、または 30 日間の猶予期間が経過するまでコンソールに表示されます。

これらの通知の表示は閉じることができますが、7 日後に再び表示されます。

また、延長が必要なサービスの一覧とその有効期限が記載されたメール通知も送信されます。この通知は、次の間隔で送信されます。

- 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

有効期限切れ後：サービスのブロックとデータの保持

猶予期間中にサービスサブスクリプションが延長されない場合、Citrix は次の方法でサービスへのアクセスをブロックします：

- 有効期限が切れた月単位サブスクリプションの場合、管理者とユーザーのアクセスは有効期限の 5 日後にブロックされます。
- 有効期限が切れた年間および複数年のサブスクリプションの場合、管理者とユーザーのアクセスは、有効期限の 30 日後にブロックされます。

サービスの有効期限日を過ぎてから 90 日間は、サービスに追加したデータは Citrix によって保持されます。90 日間の保持期間が終了する前にサブスクリプションを延長すると、管理者とユーザーはデータをそのまま使用してサービスにアクセスできます。延長されたサブスクリプションは次のように開始します：

- 月単位サブスクリプションの場合、最初の月のサブスクリプションの開始日は、延長契約を購入した日です。その後、サブスクリプションは翌月の 1 日に自動的に更新されます。
- 年間および複数年のサブスクリプションの場合、延長サブスクリプションの開始日は有効期限の翌日です。たとえば、サブスクリプションの有効期限が 9 月 30 日に切れ、サブスクリプションを 10 月 23 日に延長した場合、延長されたサブスクリプションの開始日は 10 月 1 日になります。

90 日間の保有期間が終了する前にサブスクリプションを延長しないと、Citrix によりサービスがリセットされ、追加したデータがすべて削除されます。Citrix によるクラウド環境の管理を許可することに同意した場合（たとえば、Citrix DaaS で Citrix Essentials サービスまたは Azure クイック展開オプションを使用する場合）、Citrix は 90 日間の保有期間終了後に次の操作を実行します：

- Citrix データベースからすべての顧客関連データを削除する。
- Citrix 管理の VM など、ご利用のクラウド環境で Citrix がプロビジョニングしている Citrix Cloud サービスに関連したすべてのリソースを削除する。特定の Citrix Cloud サービスに含まれる Citrix 管理のコンポーネントについて詳しくは、そのサービスのドキュメントを参照してください。

顧客管理の **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は、Azure サブスクリプションをサービスに接続するときに、そのサービスによってアプリがインストールされます。Citrix Cloud サービスのサブスクリプションを延長しない場合、90 日間の保有期間が終了してもこのアプリは Azure のサブスクリプションから削除されません。Azure サブスクリプションからサービスを完全に削除するには、このアプリを手動で削除する必要があります。次のいずれかの方法でこのアプリを削除できます：

- 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。

サービスの延長の購入

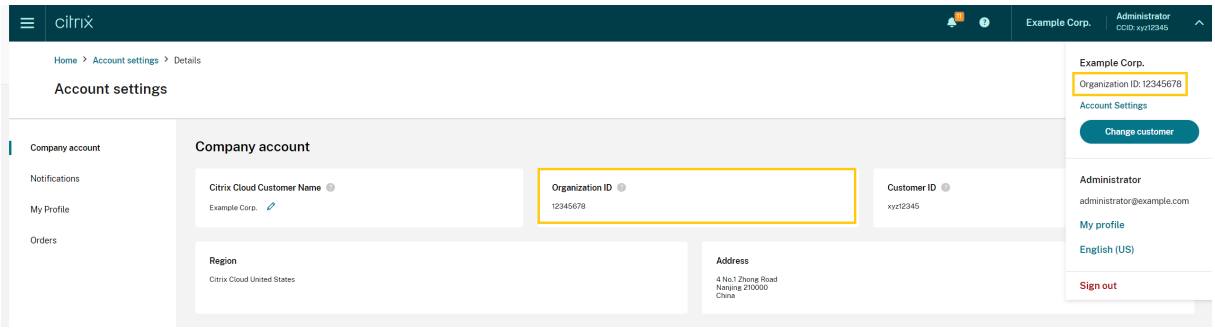
サブスクリプションを Citrix Cloud サービスに拡張するには、Citrix の営業担当者にお問い合わせください。営業担当者は、次の手順で見つけます:

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

また、お住まいの地域の連絡先情報については、Citrix Customer Serviceページにアクセスしてください。

購入を完了するために、営業担当者は Citrix Cloud アカウントの組織 ID を必要とします。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の顧客メニュー。
- [アカウント設定] ページ。



地理的な考慮事項

July 2, 2024

この記事では、Citrix Cloud が使用する商用リージョンと、各リージョン内での Citrix Cloud 商用サービスについて説明します。

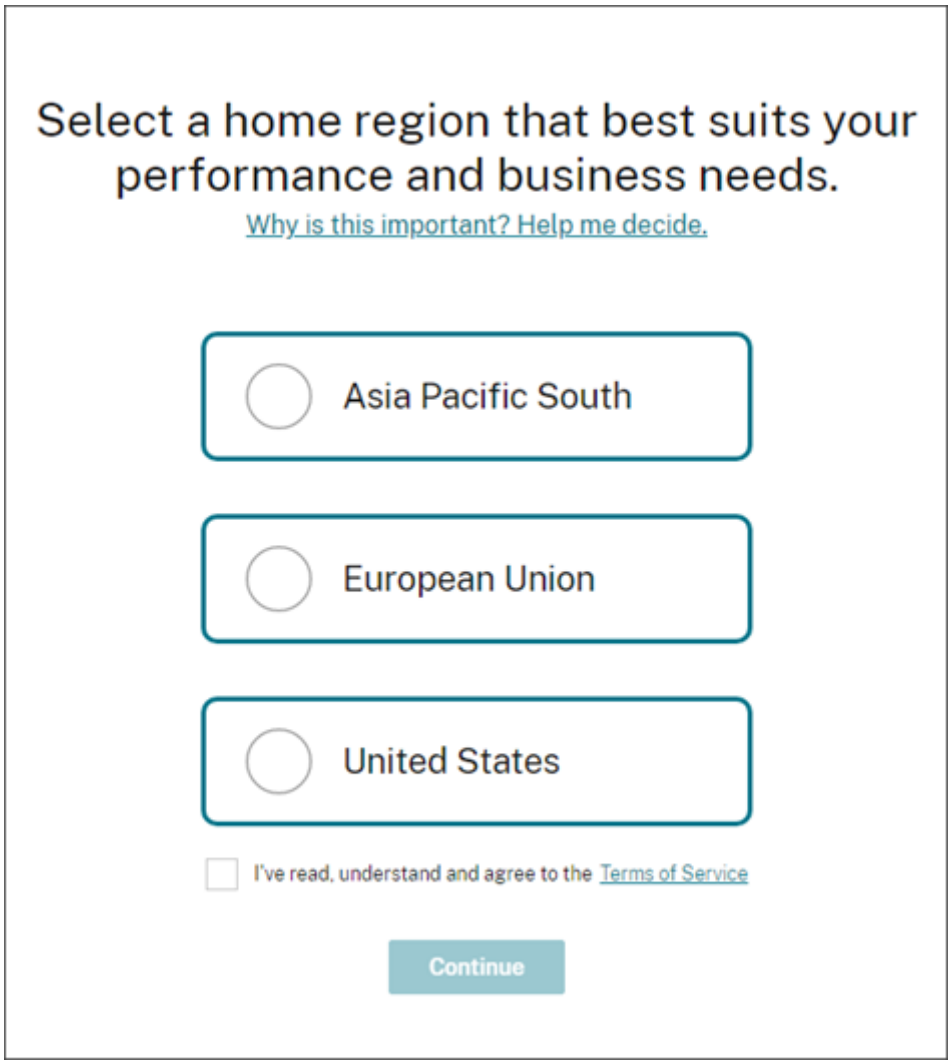
Citrix の公共部門および専用クラウドプラットフォームの地理的なリージョンとサービスについて詳しくは、「Citrix の他のクラウドプラットフォーム」を参照してください。

リージョンの選択

所属する組織が Citrix Cloud にオンボードされた後、最初のサインインで、以下のリージョンから選択するよう求められます:

- 米国
- 欧州連合
- 南アジア太平洋

リージョンを選択すると、可能な場合、その地理的リージョンでホストされているサービスが、組織に関連付けられたアクションに使用されます。組織のユーザーおよびリソースの大半が所在しているリージョンを選択してください。



> 重要な注意事項:
>
> - リージョンを選択できるのは、組織がサービスにオンボードされたときの 1 回のみです。後からリージョンを変更することはできません。

> - あるリージョンで他のリージョンのサービスを使用しても、パフォーマンスへの影響はほとんどありません。Citrix Cloud サービスは、グローバルでの使用を前提に設計されています。たとえば、オーストラリアにユーザーが存在し、コネクタがある米国の顧客は、遅延に関して最小限の影響しか受けません。
> - 所属するリージョンで Citrix Cloud がサポートされていない場合は、ユーザーとリソースの大半が存在す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の利用

大半の Citrix Cloud サービスはグローバルで複製されます。選択したリージョンは、優先して接続を確立する必要がある場所であることを意味します。ただし、他の地理的リージョンへの接続は引き続き行われる可能性があります。サービスがグローバルで複製されると、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格納されます。

また、サービスを実行するために、必要に応じて Citrix のアフィリエイトまたはサブプロセッサによってデータがグローバルに処理される場合があります。

一部のサービスには、リージョン専用のインスタンスがあります。ただし、一部のサービスは、米国ベースのインスタンスのみを利用できます。このような場合、接続とデータは地理的リージョン内に含まれます。

組織用として選択したリージョンでサービスが使用できない場合、必要に応じて特定の情報（認証データなど）が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	南アジア太平洋	メモ
Citrix Cloud コントロールプレーン	はい	はい	はい	
Citrix Analytics for Security	はい	はい	はい	
Citrix Analytics for Performance	はい	はい	はい	
NetScaler コンソール（旧称: Application Delivery Management）	はい	はい	はい	この記事の「Console Advisory Connect を使用した NetScaler インスタンスのロータッチオンボーディング」を参照してください。コンソールのオンプレミステレメトリプログラムについては、こちらを参照してください。

サービス	米国	EU	南アジア太平洋	メモ
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 のリージョンを使用します。
Citrix DaaS Standard for Azure（旧称 Virtual Apps and Desktops Standard for Azure）	はい	はい	はい	サービスは Citrix Cloud のリージョンを使用します。
Citrix DaaS Standard for Google Cloud（旧称 Virtual Apps and Desktops for Google Cloud）	はい	いいえ（米国リージョンの使用が必須）	いいえ（米国リージョンの使用が必須）	
Citrix DaaS Premium for Google Cloud（旧称 Virtual Apps and Desktops Premium for Google Cloud）	はい	いいえ（米国リージョンの使用が必須）	いいえ（米国リージョンの使用が必須）	
Citrix Endpoint Management	はい	はい	はい	複数のリージョンの複数の場所から選択します。本記事の「Endpoint Management サービスの場所」を参照してください。
Remote Browser Isolation サービス	はい	はい	はい	サービスは Citrix Cloud のリージョンを使用します。
SD-WAN Orchestrator	はい	はい	はい	

サービス	米国	EU	南アジア太平洋	メモ
Citrix Secure Internet Access ノード/POP	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	この記事の「Secure Internet Access サービスの場所」を参照してください。
Citrix Secure Private Access	グローバルで複製	グローバルで複製	グローバルで複製	この記事の「Secure Private Access のポイントオブプレゼンス」を参照してください。
Session Recording サービス	はい	はい	はい	
Citrix Virtual Apps Essentials	はい	はい	はい	サービスは Citrix Cloud のリージョンを使用します。
Citrix Virtual Desktops Essentials	はい	はい	はい	サービスは Citrix Cloud のリージョンを使用します。
Web App Firewall	はい	はい	いいえ（米国リージョンの使用が必須）	
Workspace Environment Management、Citrix Optimization Pack	はい	はい	はい	
ネットワークサービス	はい	いいえ（米国リージョンの使用が必須）	いいえ（米国リージョンの使用が必須）	
License Usage Insights（CSP のみ）	グローバルで複製	グローバルで複製	グローバルで複製	

サービス	米国	EU	南アジア太平洋	メモ
Citrix Gateway サービスアクセスノード/POP	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング	リソースの場所を構成して、ユーザートラフィックを特定のリージョンにルーティングできます。詳しくは、「Geo-location Routing - Preview」を参照してください

> 注:
>
> 特定のリージョンのサービスは、上記の表の別の場所に記載されているリージョンに依存しないコンポーネントサービスの権利とともに提供される場合があり、顧客の選択によって使用される場合があります。
>
> Citrix Cloud サービスは、顧客の指定したリージョンを使用して顧客のコンテンツやログを格納します。これは、Citrix のサブプロセッサが収集した一部のログを除きます。またサポートやトラブルシューティング目的のサービスや、パフォーマンス、セキュリティ、監査の監視、リージョン間認証（EU ベースのエンジニアが US ベースの環境にアクセスする必要がある場合など）を可能にするサービスを実行するための、リージョンに依存しないストレージが必要な一部のログも除きます。顧客の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。

各サービスで格納されるデータについて詳しくは、各サービスのセキュリティの技術概要を参照してください。

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

Console Advisory Connect ベースのコンソールインスタンスのロータッチオンボーディング:

- 既存の Citrix Cloud の顧客の場合、コンソール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リージョンと同じ地理的リージョンに作成されます。
- 既存の Citrix Cloud の顧客ではない場合、Citrix.com ポータルでその顧客の連絡先として記載されているアドレスが参照されます。プレースホルダーコンソールサービステナントは、この参照先アドレスのリージョンに対応した地理的リージョンに作成されます。あとで Citrix Cloud にオンボードすることにした場合、Citrix Cloud アカウントの作成時に選択したのと同じリージョンに新しいコンソール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コンソールサービステナントから新しいコンソールサービステナントに移行されます。

Endpoint Management サービスの場所

ホームリージョンから次の 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
- 欧州西部
- 東南アジア
- シドニー

Secure Internet Access サービスの場所

最高のエクスペリエンスを保証するために、可用性とエンドユーザーの近接性に基づいて、次の Secure Internet Access サービスの場所にトラフィックがルーティングされます。

北米

- 米国、バージニア州スターリング
- カナダ、トロント
- 米国、カリフォルニア州ロサンゼルス
- 米国、カリフォルニア州アーバイン
- 米国、ワシントン州シアトル
- 米国、コロラド州デンバー
- 米国、ノースカロライナ州シャーロット
- 米国、テキサス州ダラス
- 米国、テキサス州アレン
- 米国、フロリダ州マイアミ
- 米国、イリノイ州シカゴ
- 米国、ニューヨーク州ニューヨーク
- 米国、マサチューセッツ州ボストン
- カナダ、バンクーバー

南米

- メキシコ、ケレタロ
- ブラジル、サンパウロ
- アルゼンチン、ブエノスアイレス
- コロンビア、ボゴタ

アジア太平洋

- オーストラリア、パース
- オーストラリア、シドニー
- 日本、東京
- シンガポール、シンガポール
- インド、ムンバイ
- インド、デリー

アフリカ

南アフリカ、ヨハネスブルグ

中東

- アラブ首長国連邦、ドバイ
- トルコ、イスタンブール

西ヨーロッパ

- 英国、ロンドン
- 英国、マンチェスター
- ドイツ、フランクフルト
- ドイツ、デュッセルドルフ
- ドイツ、マンハイム
- フランス、パリ

ヨーロッパ

- フィンランド、ヘルシンキ
- オランダ、アムステルダム
- スウェーデン、ストックホルム
- ポーランド、ワルシャワ
- スペイン、マドリッド
- ブルガリア、ソフィア
- スイス、チューリッヒ
- イタリア、ミラノ

Secure Private Access のポイントオブプレゼンス

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ポイントオブプレゼンス（PoP）の一覧については、Secure Private Access サービスドキュメントの「すべての Secure Private Access の PoP の場所はどこですか?」を参照してください。

Citrix 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を提供しています。

Citrix Cloud Government

Citrix Cloud Government は、米国政府機関および米国内の他の公共部門の顧客が、規制およびコンプライアンスの要件に従って Citrix クラウドサービスを使用できるようにします。Citrix Cloud Government は、Citrix Cloud Government サービスを提供するためのサービスとデータを操作、保存、複製できる地理的境界です。サービスの提供には、米国内の 1 つまたは複数の州にある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が使用されることがあります。

Citrix Cloud Government および提供されるサービスは、米国リージョンでのみ使用できます。

詳しくは、Citrix Cloud Government製品ドキュメントを参照してください。

Citrix Cloud Japan

Citrix Cloud Japan は、日本のお客様が、Citrix が管理する専用環境で特定の Citrix Cloud サービスを使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、日本でのみ使用できます。

詳しくは、Citrix Cloud Japan製品ドキュメントを参照してください。

セキュリティで保護された **Citrix Cloud** プラットフォームの展開ガイド

July 2, 2024

セキュリティで保護された Citrix Cloud の展開ガイドは、Citrix Cloud を使用するときのセキュリティのベストプラクティスの概要と、Citrix Cloud が収集し管理する情報が記載されています。

サービスのセキュリティの技術概要

Citrix Cloud サービス内のデータセキュリティについて詳しくは、次の記事を参照してください:

- Analytics のセキュリティの技術概要
- Endpoint Management のセキュリティの技術概要
- Remote Browser Isolation のセキュリティの技術概要
- Citrix DaaS テクニカルセキュリティの概要
- Citrix DaaS Standard for Azure テクニカルセキュリティの概要

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。信頼できる管理者だけが Citrix Cloud にアクセスできるようにしてください。
- 顧客の管理者には、デフォルトですべてのサービスへのフルアクセス権があります。サービスによっては、管理者のアクセスを制限する機能があります。詳しくは、サービスごとのドキュメントを参照してください。
- Citrix Cloud 管理者の 2 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行されます。管理者が Citrix Cloud に新規登録する、または Citrix Cloud アカウントに招待される場合、多要素認証（MFA）に登録する必要があります。Microsoft Azure を使用して Citrix Cloud 管理者を認証する場合、Microsoft 社 Web サイトの「Azure AD Multi-Factor Authentication の設定を構成する」の説明に従うことで、多要素認証を構成できます。
- デフォルトでは、24 分間何も操作しないと、Citrix Cloud はコンソールアクティビティの有無にかかわらず、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。その管理者が 100 を超える顧客アカウントを管理する必要がある場合、追加の顧客を管理するには、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、管理する必要がなくなった顧客アカウントから管理者を削除することもできます。

パスワードコンプライアンス

Citrix Cloud は、次のいずれかの条件にあてはまる場合、管理者にパスワードを変更するよう要求します：

- 現在のパスワードが、サインインに使用されずに 60 日経った。
- 現在のパスワードが、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る。

新しいパスワードは、次のすべての基準を満たす必要があります：

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

パスワードの変更ルール：

- 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。

- 直近で使用した 5 個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に似たものにすることはできません。
- 新しいパスワードが、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るものであってはいけません。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https://haveibeenpwned.com/で提供されているリストを使用して判断します。

暗号化とキー管理

Citrix Cloud のコントロールプレーンには機密の顧客情報は保存されません。代わりに、Citrix Cloud は管理者のパスワードなどの情報をオンデマンドで取得します（管理者に明示的にプロンプトを表示します）。

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。

実行中のデータには、業界標準の TLS 1.2 と最も強力な暗号の組み合わせが Citrix では使用されます。Citrix Cloud は Citrix 所有の cloud.com ドメインでホストされているため、顧客は使用中の TLS 証明書を管理できません。Citrix Cloud にアクセスするには、TLS 1.2 対応のブラウザーを使用して、承認済みの強力な暗号の組み合わせを構成している必要があります。

- Windows Server 2016、Windows Server 2019、または Windows Server 2022 から Citrix Cloud コントロールプレーンにアクセスする場合、次の強力な暗号をお勧めします: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Windows Server 2012 R2 から Citrix Cloud コントロールプレーンにアクセスする場合、強力な暗号は使用できないため、次の暗号を使用する必要があります: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Citrix Cloud サービスのデータがどのように保護されるかについて詳しくは、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の暗号化とキー管理について詳しくは、サービスごとのドキュメントを参照してください。

TLS 1.2 構成について詳しくは、次の記事を参照してください:

- クライアントマシンで TLS 1.2 の使用を強制する: CTX245765、Monitoring Service の OData エンドポイントにクエリするときに、エラー:「基になっている接続が閉じられました: 送信時に予期しないエラーが発生しました。」
- Microsoft Docs Web サイトで TLS1.2 をサポートするように、.NET Framework を更新および構成します。

データ主権

Citrix Cloud コントロールプレーンは、米国および欧州連合でホストされています。顧客は管理できません。

顧客は、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、顧客が選択したデータセンター、クラウド、場所、または地理的な場所に作成できます。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、顧客が管理します。

他のサービスでは、異なるリージョンにデータを格納するオプションがあります。各サービスについては、「地理的な考慮事項」のトピックまたはこの記事の冒頭に記載されている「セキュリティの技術概要」を参照してください。

セキュリティ問題に関する情報

Web サイトstatus.cloud.comでは、顧客に継続的な影響を与えるセキュリティ問題について確認できます。このサイトは状態と稼働時間に関する情報を記録します。また、プラットフォームや個別サービスへの更新をサブスクライブするオプションがあります。

Citrix Cloud Connector

Cloud Connector のインストール

Citrix では、セキュリティとパフォーマンスの観点から、ドメインコントローラーに Cloud Connector ソフトウェアをインストールしないことをお勧めします。

さらに、Cloud Connector ソフトウェアがインストールされているマシンは、DMZ（Delimitarized Zone：非武装地帯）ではなく、顧客のプライベートネットワーク内に配置することを強くお勧めします。ネットワークとシステムの要件、および 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

顧客は、Cloud Connector がインストールされているコンピューターを Windows の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。

Cloud Connector は、ウイルス対策ソフトとともに使用できます。Citrix では McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8 でテスト済みです。これ以外の業界標準のウイルス対策製品も使用できます。

顧客の Active Directory（AD）では、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お勧めします。これは Active Directory のデフォルトの構成です。また、Cloud Connector のマシンアカウントで AD ログおよび監査を有効にして、すべての AD アクセスアクティビティを監視できます。

Cloud Connector をホストしているマシンへのログオン

Cloud Connector を使用すると、機密性の高いセキュリティ情報を 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すことができますが、次の機密情報も保存されます：

- Citrix Cloud と通信するためのサービスキー
- Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の電源管理に使用するハイパーバイザーサービスの資格情報

この機密情報は、Cloud Connector をホストしている Windows Server 上のデータ保護 API（DPAPI）を使用して暗号化されます。最も権限のある管理者だけが、Cloud Connector マシンに（メンテナンス操作のためなどに）ログオンできるようにすることを Citrix では強くお勧めします。通常、Citrix 製品を管理するために、管理者がこれらのマシンにログオンする必要はありません。Cloud Connector には、自己管理機能があります。

Cloud Connector をホストしているマシンには、エンドユーザーがログオンできないようにしてください。

Cloud Connector マシンへの他のソフトウェアのインストール

顧客は、Cloud Connector がインストールされているマシン上にウイルス対策ソフトウェアと（仮想マシンにインストールされている場合）ハイパーバイザーツール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お勧めします。他のソフトウェアによって、セキュリティ攻撃の可能性を高めることになり、Citrix Cloud ソリューション全体のセキュリティが低下することがあります。

送受信ポートの構成

Cloud Connector では、インターネットへのアクセスに送信ポート 443 を開く必要があります。Cloud Connector にインターネットからアクセス可能な受信ポートを設定しないことを Citrix では強くお勧めします。

顧客は、送信インターネット通信を監視するために、Web プロキシの背後に Cloud Connector を配置できます。ただし、Web プロキシは SSL/TLS 暗号化通信をサポートする必要があります。

Cloud Connector には、インターネットにアクセスできる送信ポートがある場合もあります。追加のポートが利用可能な場合、ネットワーク帯域幅とパフォーマンスを最適化するために、Cloud Connector は幅広いポートにわたってネゴシエートします。

Cloud Connector は、内部ネットワーク内で、広範囲の受信ポートと送信ポートを開く必要があります。次の表は、開放する必要があるポートの基本セットです。

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	W32Time
49152～65535/TCP	135/TCP	RPC エンドポイントマッパー
49152～65535/TCP	464/TCP/UDP	Kerberos パスワードの変更
49152～65535/TCP	49152～65535/TCP	LSA、SAM、Netlogon の RPC（*）
49152～65535/TCP/UDP	389/TCP/UDP	LDAP
49152～65535/TCP	3268/TCP	LDAP GC

クライアントポート	サーバーポート。	サービス
53、49152～65535/TCP/UDP	53/TCP/UDP	DNS
49152～65535/TCP	49152～65535/TCP	FRS RPC（*）
49152～65535/TCP/UDP	88/TCP/UDP	kerberos
49152～65535/TCP/UDP	445/TCP	SMB

Cloud Connector は、LDAP 署名と封印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。つまり、SSL 経由の LDAP（LDAPS）は必要ありません。LDAP 署名について詳しくは、「Windows Server で 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マイクロソフトガイダンス」を参照してください。

Citrix Cloud 内で使用される各サービスによっては、必要なオープンポート一覧は拡張されます。詳しくは、次のドキュメントを参照してください:

- 各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）
- Citrix Cloud サービスのインターネット接続の要件
- コンソールサービスのポート要件
- Endpoint Management のポート要件

外部通信の監視

Cloud Connector は、ポート 443 上で Citrix Cloud サーバーと Microsoft Azure Service Bus サーバーの両方でインターネットに送信します。

Cloud Connector は、ホストコンピューターが存在する Active Directory フォレスト内にある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。

通常の操作では、Cloud Connector は Citrix Cloud ユーザーインターフェイスの［**ID** およびアクセス管理］ページで無効になっていないドメイン内のドメインコントローラーとのみ通信します。

Citrix Cloud 内のサービスごとに、Cloud Connector が通常の操作の過程で通信する可能性があるサーバーと内部リソースの一覧は拡張されます。また、Cloud Connector が Citrix に送信するデータを顧客が管理することはできません。サービスの内部リソースと Citrix に送信されるデータについて詳しくは、次のドキュメントを参照してください:

- 各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）
- Citrix Cloud サービスのインターネット接続の要件

Cloud Connector ログの表示

管理者に関連する情報、または対応が必要な情報は、Cloud Connector マシンの Windows イベントログで確認できます。

次のディレクトリで Cloud Connector のインストールログを表示します:

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

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

WorkspaceCloud\Logs ディレクトリのログは、指定したサイズのしきい値を超えると削除されます。管理者は、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\MaximumLogSpaceMegabytes のレジストリキー値を調整することによって、このサイズの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 では、「暗号化とキー管理」で説明されている暗号を有効にする必要があります。

Cloud Connector が、Citrix Cloud SSL/TLS 証明書および Microsoft Azure Service Bus SSL/TLS 証明書で使用される証明機関（CA）を信頼する必要があります。Citrix と Microsoft は今後、証明書と CA を変更する可能性がありますが、Windows の標準の信頼された発行元一覧にある CA を常に使用します。

Citrix Cloud 内の各サービスの SSL 構成要件は異なることがあります。詳しくは、各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）を参照してください。

セキュリティコンプライアンス

Cloud Connector は、自己管理機能によって確実なセキュリティコンプライアンスを実現します。再起動を無効にしたり、Cloud Connector に他の制限を設定したりしないでください。こうした操作により、重要な更新があるときに Cloud Connector がアップデートされなくなります。

顧客側で、セキュリティ上の問題に対応するための特別な操作は必要ありません。セキュリティ上の修正プログラムは Cloud Connector により自動的に適用されます。

クラウドサービス用の **Citrix Connector Appliance**

Connector Appliance のインストール

Connector Appliance はハイパーバイザーでホストされます。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ある必要があります。

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 からの想定されるトラフィックのみを許可します。

Connector Appliance をホストするハイパーバイザーが、最新のセキュリティアップデートが適用された状態でインストールされていることを確認してください。

ネットワークとシステムの要件、および Connector Appliance のインストール手順については、「クラウドサービス用の Connector Appliance」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。最も権限のある管理者だけが、Connector Appliance をホストしているハイパーバイザーに（メンテナンス操作のためなどに）ログオンできるようにします。通常、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 には、自己管理機能があります。

送受信ポートの構成

Connector Appliance では、インターネットへのアクセスに送信ポート 443 を開く必要があります。Connector Appliance にインターネットからアクセス可能な受信ポートを設定しないことを Citrix では強くお勧めします。

送信インターネット通信を監視するために、Web プロキシの背後に Connector Appliance を配置できます。ただし、Web プロキシは SSL/TLS 暗号化通信をサポートする必要があります。

Connector Appliance には、インターネットにアクセスできる送信ポートがある場合もあります。追加のポートが利用可能な場合、ネットワーク帯域幅とパフォーマンスを最適化するために、Connector Appliance は幅広いポートにわたってネゴシエートします。

内部ネットワーク内では、広範囲の受信ポートと送信ポートを開く必要があります。次の表は、開放する必要があるポートの基本セットです。

接続方向	Connector Appliance ポート	外部ポート	サービス
受信	443/TCP	任意	ローカル Web UI
送信	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
送信	49152～65535/UDP	123/UDP	W32Time

接続方向	Connector Appliance ポート	外部ポート	サービス
送信	49152～65535/TCP	464/TCP/UDP	Kerberos パスワードの変更
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	kerberos
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によっては、必要なオープンポート一覧は拡張されます。詳しくは、次のドキュメントを参照してください:

- 各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）
- Citrix Cloud サービスのシステムと接続の要件

外部通信の監視

Connector Appliance は、ポート 443 において Citrix Cloud サーバーでインターネットに送信します。

Citrix Cloud 内のサービスごとに、Connector Appliance が通常の操作の過程で通信する可能性があるサーバーと内部リソースの一覧は拡張されます。また、Connector Appliance が Citrix に送信するデータを顧客が管理することはできません。サービスの内部リソースと Citrix に送信されるデータについて詳しくは、次のドキュメントを参照してください:

- 各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）
- Citrix Cloud サービスのシステムと接続の要件

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ついて詳しくは、「クラウドサービス用の Connector Appliance」を参照してください。

SSL/TLS 構成

Connector Appliance では、特に 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証明機関（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、必ず Connector Appliance が信頼する CA を使用します。

Citrix Cloud 内の各サービスの SSL 構成要件は異なることがあります。詳しくは、各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）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、コネクタコンプライアンスは自己管理機能を備えており、コンソールからはログインできません。

コネクタのセキュリティ上の問題に対応するための特別な操作は必要ありません。セキュリティ上の修正プログラムは自動的に適用されます。

Connector Appliance をホストするハイパーバイザーが、最新のセキュリティアップデートが適用された状態で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 のデフォルトの構成です。また、Connector Appliance のマシンアカウントで AD ログおよび監査を有効にして、すべての AD アクセスアクティビティを監視できます。

不正使用されたアカウントの処理に関するガイダンス

- Citrix Cloud の管理者リストを監査し、信頼されていないユーザーを削除してください。
- 社内の Active Directory 内の侵害されたアカウントを無効にしてください。
- Citrix に連絡して、すべての顧客の Cloud Connector に格納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てください。違反の重大度に応じて、次の処置を講じてください。
  - 低リスク： Citrix は、経過時間によってシークレットをローテーションできます。Cloud Connector は引き続き通常どおりに機能します。古い認証シークレットは 2〜4 週間で無効になります。この間 Cloud Connector を監視して、予期しない操作がないことを確認します。
  - 進行中の高リスク： 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、該当するすべてのマシンで 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 Cloud アカウントの作成

December 14, 2023

この記事では、Citrix Cloud アカウントを作成し、アカウントのオンボードに必要なタスクを正常に完了するプロセスについて説明します。

Citrix との関係が既にあり、Citrix Cloud サービスを初めて使用する顧客は、この記事のタスクを使用してオンボードプロセスを完了できます。

Citrix を初めて使用する顧客の新規登録プロセス

Citrix および Citrix Cloud を初めて使用する場合は、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ます。

- Citrix カスタマーサービスに連絡する。
- お住まいの地域のCitrix パートナーまたはCitrix セールスオフィスに連絡する。

Citrix に連絡することで、自社のビジネスニーズについて Citrix の担当者と話し合うことができます。担当者は、新規登録プロセスを完了できるようサポートし、Citrix でのサインイン資格情報を提供します。

Citrix アカウントの認証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 を使用開始できます。

Citrix アカウントとは何ですか?

Citrix アカウント（Citrix.com アカウントまたは My Citrix アカウント）では、購入したライセンスへのアクセスを管理できます。Citrix アカウントでは、組織 ID（OrgID）が一意の識別子として使用されます。Citrix アカウントにアクセスするには、ユーザー名（Web ログイン）またはアカウントにリンクされているメールアドレスでhttps://www.citrix.comにログインします。

> 重要:
>
> ユーザー名は単一で一意の Citrix アカウントに割り当てられますが、メールアドレスは複数の Citrix アカウントに割り当てることができます。

OrgID とは何ですか?

OrgID は、Citrix アカウントに割り当てられた一意の識別子です。OrgID は物理的なサイトアドレス（通常は所属する会社のビジネスアドレス）に関連付けられています。企業には通常、1 つの OrgID があります。ただし、ブランチオフィスが異なる場合や、部門ごとに資産を個別に管理する場合などは、単一の会社が複数の OrgID を所有できます。

特定の OrgID は定期的にクリーンアップされ、必要な場合、重複分がマージされます。有効かつアクティブな OrgID とマージする OrgID がある場合は、マージする OrgID を Citrix カスタマーサポートに連絡することができます。

> 注:
>
> 企業は資産の管理方法に基づいて OrgID を既に設定しているため、使用する OrgID や所有する OrgID の数が不明の場合は、お客様の会社の IT 部門または Citrix 管理者にお問い合わせください。サポートが必要な場合は、Citrix カスタマーサービス（https://www.citrix.com/support/）に問い合わせて OrgID を確認してください。

Citrix Cloud アカウントとは何ですか**?**

Citrix Cloud アカウントで 1 つまたは複数の Citrix Cloud サービスを使用して、アプリケーション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 に関連付けられます。OrgID は複数の Citrix Cloud 顧客 ID に関連付けることができますが、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 をセットアップした方法に基づいて、適切な Citrix Cloud アカウントを選択し、同じ OrgID を使用して購入と管理者のアクセスも実行できるようにすることが重要です。たとえば、OrgID 1234 を使用している会社の設計部門が Virtual Apps and Desktops をオンプレミスで使用している場合に Citrix Cloud を試用するには、OrgID 1234 の管理者が OrgID に関連付けられた Citrix アカウントのサインイン資格情報またはメールアドレスを使用して、その OrgID での Citrix Cloud への新規登録ができます。会社が Citrix DaaS サブスクリプションを購入することを決定した場合、OrgID 1234 で注文を正しく確定できます。

> 重要:
>
> 特定の Citrix アカウントにアクセスできるユーザーが、その Citrix アカウントの OrgID に関連付けられている Citrix Cloud アカウントに自動的にアクセスできるようになるわけではありません。ユーザーが Citrix Cloud にアクセスできるようになると、サービスに影響を及ぼす可能性があるため、Citrix Cloud アカウントにアクセスするユーザーを管理することが重要です。

多要素認証

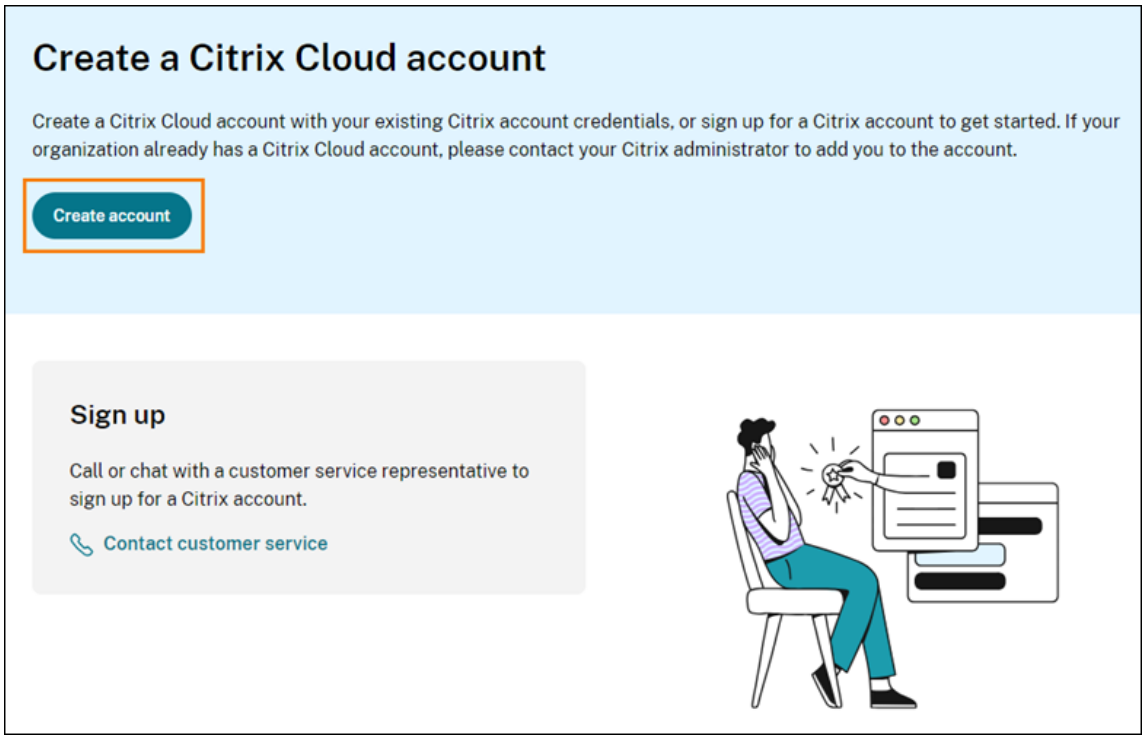
Citrix Cloud アカウントを安全に保つために、Citrix ではすべての顧客が多要素認証（MFA）に登録する必要があります。登録に必要なものは、Citrix SSO などの認証アプリがインストールされた、コンピューターやモバイルデバイ

スなどのデバイスのみです。認証アプリを備え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。

多要素認証にまだ登録していない場合は、Citrix アカウントの資格情報でサインインするときに Citrix から登録するよう求められます。要件と手順については、この記事の「手順 2：多要素認証を設定する」を参照してください。

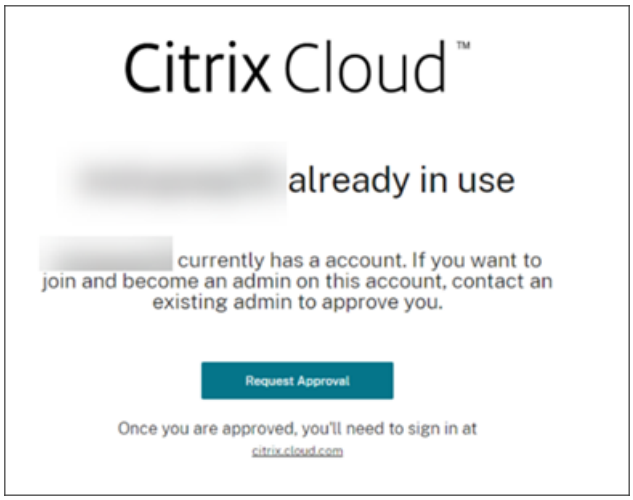
手順 **1**：**Citrix Cloud Web** サイトにアクセスする

1. Web ブラウザーを使用して、https://onboarding.cloud.comにアクセスします。
2. ［アカウントの作成］を選択します。



3. ユーザー名とパスワードを入力するか、Citrix.com アカウントに関連付けられているメールアドレスとパスワードを入力します。

アカウントが既に使用中の場合



組織の Citrix Cloud アカウントがすでに使用中であるというメッセージが表示された場合、利用中の Citrix アカウントの別の管理者が、Citrix Cloud アカウントを作成済みであることを意味します。このアカウントにアクセスするには、すでに Citrix アカウントのメンバーであっても、既存の管理者から管理者として招待される必要があります。

Citrix Cloud アカウントでは、管理者はサービスをより詳細に管理できるため、Citrix Cloud アカウントを作成する最初の管理者は、別の管理者が既に Citrix アカウントのメンバーであっても明示的にアクセス権を付与する必要があります。

Citrix Cloud アカウントへの参加の招待をリクエストするには、［承認のリクエスト］を選択します。アカウントの既存のすべての管理者は、メールでリクエストの通知を受け取ります。既存の管理者が組織を離れた場合は、Citrix サポートにお問い合わせください。

承認のリクエストを受け取った管理者は、「個別の管理者を招待する」の手順で送信者を管理者として招待します。

この招待メールを受け取ってから、［サインイン］をクリックして招待を承諾します。ブラウザーが開くと、Citrix Cloud から、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求められます。

手順 **2**：多要素認証を設定する

多要素認証に登録していない場合、サインインする前に登録するよう Citrix Cloud から求められます。認証アプリ（推奨）またはメールアドレスを使用して多要素認証に登録することを選択できます。

> 注：
>
> - Citrix Cloud 経由で MFA を設定できるのは、Citrix ID プロバイダーの管理者のみです。Azure AD を使用して Citrix Cloud 管理者を管理する場合、Azure ポータルを使用して MFA を構成できます。詳しくは、Microsoft Web サイトの「Azure AD 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が完了すると、Citrix Cloud で自分が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の完了後に 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。あとから別のデバイスを登録すると、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。詳しくは、「プライマリ MFA メソッドを管理する」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は、メールを使用した MFA が便利な代替手段です。ただし、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の予防措置を講じることを強くお勧めします。

MFA の要件

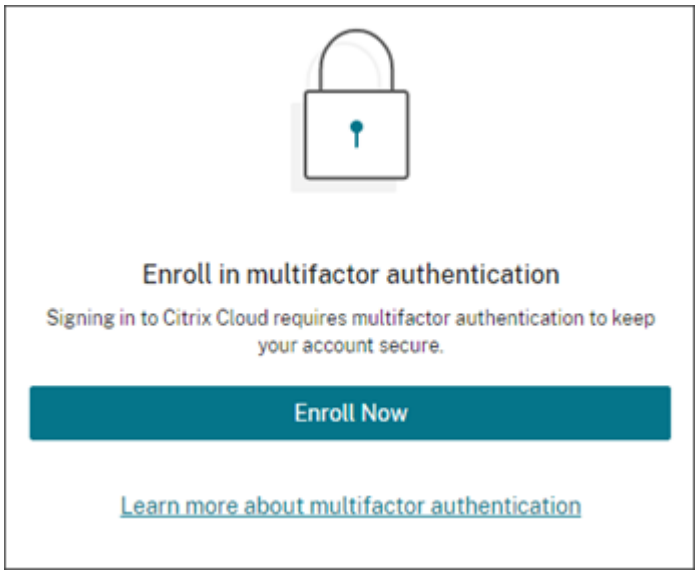
認証アプリを使用して MFA をセットアップするには、スマートフォンやデスクトップコンピューターなどのデバイスに、時間ベースのワンタイム パスワード標準に準拠するアプリをインストールする必要があります。登録しているデバイスによっては、QR コードをスキャンするためにアプリがデバイスのカメラにアクセスする必要があります。デバイスにカメラが搭載されていない場合は、Citrix Cloud が提供するキーを入力できます。

メールアドレスを使用して MFA をセットアップするには、次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。

- このメールアドレスは、Citrix アカウントに使用しているメールアドレスとは異なります。
- メールアドレスは、Citrix から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す。

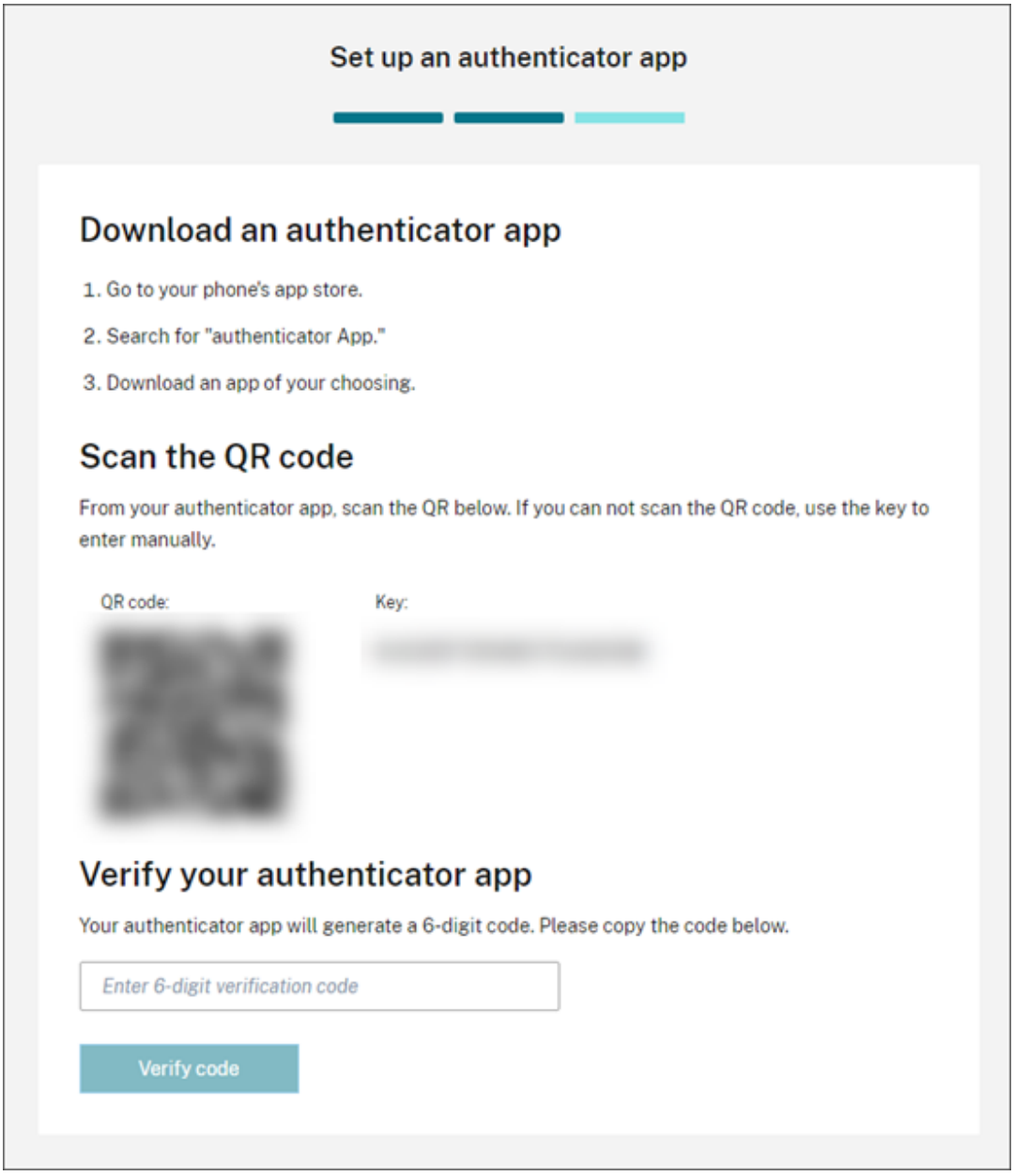
多要素認証に登録するには

1. 多要素認証（MFA）に登録するよう求められたら、［今すぐ登録］を選択します。



2. プロンプトが表示されたら、メールアドレスを入力し、［メールの送信］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. メールから確認コードと Citrix アカウントのパスワードを入力します。［確認して続行］をクリックします。
4. 認証方法として、認証アプリを使用するかメールを使用するかを選択します。
5. ［認証アプリ］を選択した場合は、以下のアクションを実行します。

   a) 認証アプリで QR コードをスキャンするか、キーを手動で入力します。認証アプリが Citrix Cloud のエントリを表示し、6 桁のコードを生成します。

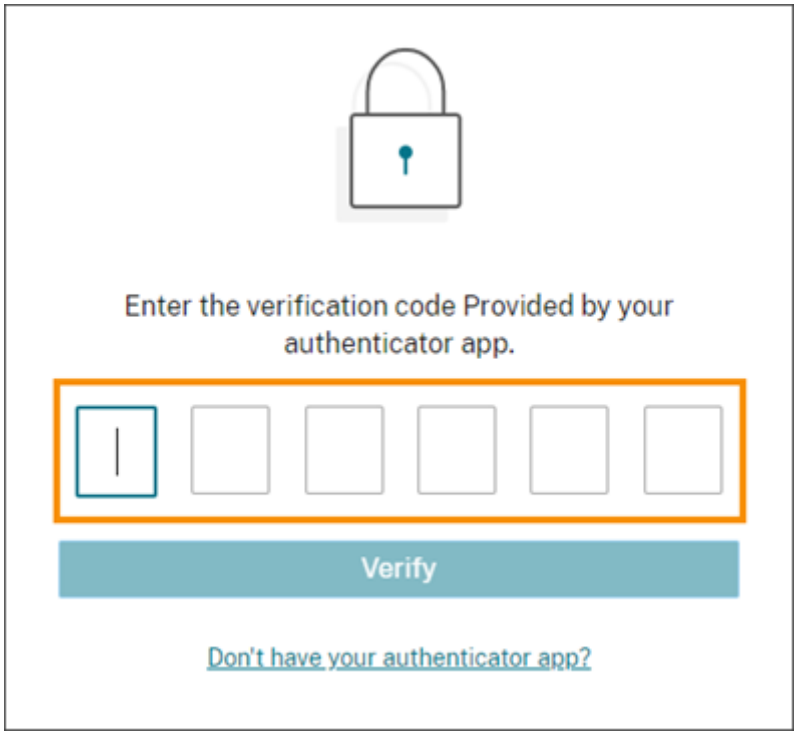


   b) ［認証アプリを確認する］で認証アプリのコードを入力して ［コードを確認する］を選択します。

6. ［次へ：復旧方法］をクリックします。
7. ［復旧用の電話番号を追加する］を選択して、Citrix サポートがユーザーの本人確認のために連絡できる復旧用の電話番号を入力します。固定電話の電話番号を使用することをお勧めします。完了したら、［復旧用の電話番号を保存］をクリックします。
8. ［**Next**］を選択します。
9. ［復旧用の電話番号を追加する］を選択して、Citrix Cloud で使用するメールアドレス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、ユーザーの本人確認のための確認コードを送信します。

   別のメール アドレスがない場合は、［復旧用のメール アドレスがない場合:］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紛失しやすいため、お勧めできません。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ます。
10. ［完了］を選択して登録を完了します。

次に Citrix Cloud 管理者の資格情報でサインインすると、Citrix Cloud は選択した MFA の方法から確認コードの入力を要求します。



MFA の登録を管理する

デバイスを変更する、別の多要素認証の方法に切り替える、または復旧方法を更新する方法については、以下の記事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 の復旧方法を管理する

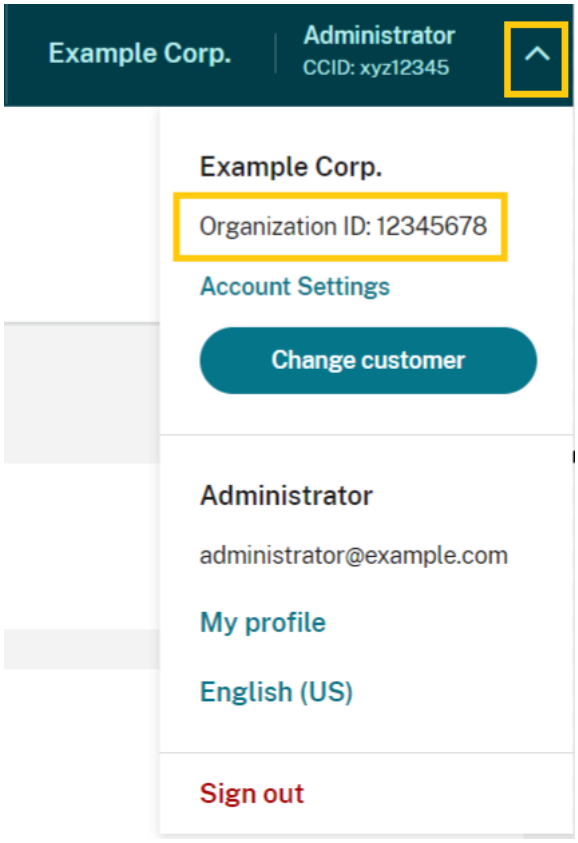
手順 **3**：**OrgID** を確認する

Citrix Cloud の使用を開始する前に、OrgID を確認します。

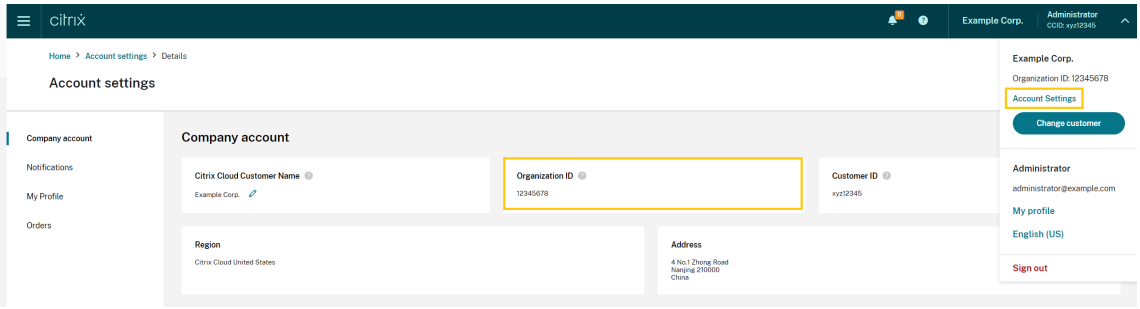
アカウントの OrgID が注文に使用する OrgID と一致していることを確認してください。Citrix Cloud のメリットの 1 つは、サービスを試用してから購入する場合、同じアカウントを使用できるため、トライアルで作成したすべての設定が購入後も保持されることです。つまり、正しい OrgID でトライアルを開始することは、購入時の手間を省くことになります。

OrgID は、管理コンソールの次の場所に表示されます：

- 顧客名の下のメニュー。右上隅にある顧客名をクリックして、メニューを表示します。



- ［アカウント設定］ページ。顧客メニューから ［アカウント設定］を選択します。



次の手順

オンボード後、以下のタスクに進むことができます。

- 管理者またはワークスペースユーザーを認証するための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、それらの管理者を Citrix Cloud アカウントに追加する必要があることに注意してください。
- Cloud サービスのトライアルを要求します。トライアルは、必要なオンプレミスの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、Microsoft Active Directory でのテスト用に設計されています。

追加情報

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

Citrix Cloud のアカウントの確認

October 26, 2023

ユーザーは、Citrix Cloud アカウントの確認を求められることがあります。以下のような場合、メールの確認が必要になります：

- 長期間 Citrix Cloud にログインしていなかった。
- メールアドレスを変更した。
- 新しい管理者を Citrix Cloud に追加した。
- Citrix Cloud のセキュリティシステムの更新のため、Citrix Cloud アカウントを再確認する必要がある。

よくある質問

確認の頻度はどのくらいですか**?**

アカウントの確認は一度きりのイベントです。サインインのたびに確認されたり、アカウントで何か変更を行うたびに確認されたりすることはありません。頻繁に確認が行われる場合、Citrix テクニカルサポートにお問い合わせください。

アカウントに何か不具合が発生したのですか**?**

いいえ。アカウントの確認を求められたからといって、アカウントや使用中の Citrix Cloud サービスに不具合が起こったというわけではありません。Citrix がお客様の情報を安全に保護するための手順の一部にすぎません。

確認メールを受信していません。どうすればよいでしょうか

次の手順を実行します:

1. 差出人が「Citrix」の確認メールを受信トレイで探してください。確認メールの有効期限は 24 時間後です。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ます。これは、Web ログインごとに 1 回限りです。
2. 受信トレイにない場合、フォルダーを検索してください。迷惑メールフィルターやメールルールによってメールが迷惑メールフォルダーや削除済みアイテムフォルダーに移動された可能性があります。ファイアウォールを確認します。
3. また、メールアカウントが正しいことも確認してください。確認メールは、アカウントのファイルで現在指定されているメールアドレスに送信されます。通常このメールアドレスは、Citrix Cloud に最初に登録したアドレス、または Citrix Cloud アカウントに招待された時のアドレスです。
4. 以下のサイトで Citrix アカウントにサインインし、記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ます。[https://www.citrix.com/account]（https://www.citrix.com/account）メールが無効な場合は、メールアドレスを更新してから 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。詳しくは、Citrix Support Knowledge Center のCTX126336またはCTX130452を参照してください。
5. それでも確認メールが届かない場合は、Citrix サポートに連絡してサポートケースを開いてください。教育サイト（[**Partner Services Delivery**] > [**eLearning**] > [**Citrix Training**] を参照）について、詳細な調査が必要な場合はケースを開いて教育チームにご連絡ください。ケースを開くには、［Contact Us］ページで ［**General Support**］を要求してください。

メール確認に成功しても Citrix Cloud にサインインできない場合は、Citrix Web サイトの「Troubleshooting login issues on Citrix websites」を参照してください。

Citrix サポートに連絡してください。」

ここで説明していない問題が発生している場合は、Citrix サポートに連絡してサポートケースを開いてください。

Citrix Cloud への接続

April 5, 2024

リソースを Citrix Cloud に接続するには、環境内でコネクタを展開し、_ リソースの場所 _ を作成します。

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

リソースの場所を作成するには、ドメインに少なくとも 2 つの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、Cloud Connector または Connector Appliance は、Citrix Cloud とリソースの間で通信するために必要です。コネクタの展開について詳しくは、以下の記事を参照してください:

- Cloud Connector の技術詳細
- クラウドサービス用の Connector Appliance

リソースの種類

リソースの場所に含まれるリソースは、使用している Citrix Cloud サービスおよび利用者に提供するサービスによって異なります。各リソースで異なるタイプのコネクタが使用されます。大半のサービスは Citrix Cloud Connector を利用しますが、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**（旧称 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 がサービスと通信する方法の概要については、Citrix Tech Zone の「Citrix DaaS の図」を参照してください。
- **Citrix DaaS Standard for Azure**（旧称 Citrix Virtual Apps and Desktops Standard for Azure）では、マルチセッションマシンから Citrix がホストする Azure の仮想デスクトップおよびアプリを提供するための 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、すべてのプラットフォームにおいてイメージを簡単に管理できるようにします。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との間でイメージを管理するのに役立ちます。Citrix Virtual Apps and Desktops の 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にイメージを移行しようとすると、開始されます。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、実行の準備を支援します。最終的に、Citrix Provisioning または Machine Creation Services は、パブリッククラウドサブスクリプションで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** により、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たエクスペリエンスを提供し、エンドツーエンドのアクセス制御を行うことができます。詳しくは、「Connector Appliance を使用した Secure Private Access」を参照してください。

Connector Appliance を使用するプレビュー段階のサービスがほかにも存在する可能性があります。

リソースの場所

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、ブランチオフィス、またはデータセンターのいずれであっても、リソースがある場所であればどこにでも配置できます。既にクラウドまたはデータセンターにリソースを所有している場合、リソースはそのまま残ります。Citrix Cloud で使用するために別の場所に移動する必要はありません。

場所の選択は、以下の要素の影響を受けることがあります:

- 利用者との距離
- データとの距離
- 拡張の必要性
- セキュリティ属性

リソースの場所の展開例

- データから近い距離に位置する必要がある利用者やアプリケーションのために、本社のデータセンターに最初のリソースの場所を構築する。
- グローバルユーザーのために、パブリッククラウドに 2 番目のリソースの場所を追加する。または、ブランチオフィスで別のリソースの場所を構築して、ブランチワーカーが最適に利用できるアプリケーションを提供する。

- 別のネットワークにさらにリソースの場所を追加して、限定されたアプリケーションを提供する。これによって、これ以外のリソースの場所を調整する必要なく他のリソースや利用者に表示される内容を制限できます。

リソースの場所の制限

Citrix Cloud アカウントには、最大 50 のリソースの場所を設定することができます。

命名制限

リソースの場所に割り当てる名前は、次の制限に準拠する必要があります:

- 最大文字数: 64 文字
- 許可されていない文字:
  - #、$、%、^、&、?、+
  - かっこ: [ ]、{ }
  - パイプ（|）
  - 小なり記号（<）と大なり記号（>）
  - スラッシュとバックスラッシュ（/、\）
- Citrix Cloud アカウントが使用する他のリソースの場所の名前と一致していない（大文字と小文字は区別）

プライマリのリソースの場所

プライマリのリソースの場所は、ドメインと Citrix Cloud 間の特定の通信に「最も優先される」と指定するリソースの場所です。プライマリのリソースの場所にある Cloud Connector が、ユーザーのログオンとプロビジョニング操作に使用されます。「プライマリ」として選択したリソースの場所には、ドメインに対するパフォーマンスや接続性が最も優れた 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。

詳しくは、「[プライマリのリソースの場所の選択]」を参照してください。(/en-us/citrix-cloud/citrix-cloud-management/identity-access-management/primary-resource-locations.html)

Citrix Cloud Connector

April 5, 2024

Citrix Cloud Connector は、Citrix Cloud とリソースの場所との間の通信チャネルとして機能する Citrix コンポーネントで、複雑なネットワークやインフラストラクチャ構成を必要とせずにクラウドを管理できます。これによって、配信インフラストラクチャを管理する手間が省けます。リソースを管理しながら、ユーザーに価値を提供するリソースに集中することができます。

> 注:
>
> 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参加済みマシンにはインストールできます。
>
> この SDK のコマンドレットは、Cloud Connector では実行しないことを Citrix ではお勧めします。これは、SDK の操作に Cloud Connector は関係しないためです。

Cloud Connector が必要なサービス

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）には Cloud Connector が必要です。Cloud Connector がサービスと通信する方法の概要については、Citrix Tech Zone の「Citrix DaaS の図」を参照してください。

Citrix Endpoint Management では、Endpoint Management サービスへのエンタープライズ接続に Cloud Connector が必要です。Remote Browser Isolation サービスでは、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 の管理を有効にし、リソースの場所内で AD のフォレストとドメインを使用できるようにします。これによって、さらに AD 信頼関係を追加する必要はなくなります。
- **Virtual Apps and Desktops** の公開: Citrix DaaS でリソースの場所にあるリソースから公開できるようにします。
- **Endpoint Management**: 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）環境を使用して、デバイスポリシーとアプリポリシーを管理し、ユーザーにアプリケーションを配信できるようにします。
- 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できます。

> 注:
>
> 操作は可能ですが、Citrix Cloud への接続が利用できない期間、機能が低下する可能性があります。Citrix Cloud コンソールから Cloud Connector の正常性を監視できます。

Cloud Connector の通信

Cloud Connector は、Citrix Cloud とリソースの場所の間で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 は発信接続を介して Citrix Cloud との通信を開始します。すべての接続が、標準 HTTPS ポート（443）と TCP プロトコルを使用して Cloud Connector からクラウドに対して確立されます。受信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て負荷を管理するために、各リソースの場所に複数の Cloud Connector をインストールします。Citrix Cloud との高可用性接続を確保するためには、各リソースの場所に少なくとも 2 つの Cloud Connector が必要です。ある Cloud Connector を一定期間使用できない場合、他の Cloud Connector がその接続を維持できます。各 Cloud Connector はステートレスであるため、使用可能なすべての 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。

1 つの Cloud Connector が利用可能である限り、Citrix Cloud との通信は失われません。エンドユーザーから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、Citrix Cloud に接続できるかに関係なく、リソースの場所でリソースにアクセスできるようになります。

Cloud Connector の入手場所

Citrix Cloud 内から Cloud Connector ソフトウェアを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で、［リソースの場所］を選択します。
3. 既存のリソースの場所がない場合、［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。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り Cloud Connector がインストールされていない場合は、Cloud Connector バーをクリックし、［ダウンロード］を選択します。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 とリソースの場所との間に高可用性接続を作成するには、2 つ以上の Cloud Connector が必要です。使用環境とサポートするワークロードによっては、ユーザーに最適なエクスペリエンスを提供するために、Cloud Connector の数を増やす必要がある場合があります。

ベストプラクティスとして、展開する必要のある Cloud Connector 数を決定する際には、N+1 の冗長モデルを使用することをお勧めします。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な 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 Cloud Connector をあと 1 つ追加します。たとえば、5 つの Cloud Connector が必要であると判断した場合は、この合計にさらに 1 つ追加して、リソースの場所に 6 つの Cloud Connector をインストールします。

スケールとサイジングのガイドラインについては、「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

Cloud Connector のインストール場所

サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。

Windows Server 2016、Windows Server 2019 または Windows Server 2022 を実行している専用マシンに Cloud Connector をインストールします。このマシンをドメインに参加させ、Citrix Cloud から管理するリソースと通信できるようにする必要があります。

> 重要:
>
> - Active Directory ドメインコントローラーに Cloud Connector やその他の Citrix コンポーネントをインストールしないでください。
> - 他の Citrix 展開の一部であるマシン（たとえば、オンプレミスの Virtual Apps and Desktops 展開の Delivery Controller）に Cloud Connector をインストールしないでください。

展開について詳しくは、次の記事を参照してください:

- Active Directory での Cloud Connector 展開シナリオ
- Cloud Connector のインストール

Citrix Cloud Connector の技術詳細

July 2, 2024

Citrix Cloud Connector は、Citrix Cloud とリソースの場所の接続を確立するコンポーネントです。本記事では、展開の要件とシナリオ、Active Directory と FIPS 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

Cloud Connector をホストするマシンは、次の要件を満たしている必要があります：高可用性を確保するために、それぞれのリソースの場所に 2 つ以上の Cloud Connector が必要です。ベストプラクティスとして、Citrix Cloud との高可用性接続を維持するために、Cloud Connector を展開する場合は、N+1 の冗長モデルを使用することをお勧めします。

ハードウェア要件

各 Cloud Connector には、少なくとも次のものが必要です:

- 仮想 CPU×2

- 4GB のメモリ
- 20GB のディスクスペース

仮想 CPU メモリを増やすと、Cloud Connector をより大規模なサイトにスケールアップできます。推奨の構成については、「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

オペレーティングシステム

次のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019
- Windows Server 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

Microsoft .NET Framework 4.7.2 以降が必要です。Microsoft の Web サイトから最新バージョンをダウンロードします。

> 注:
>
> Cloud Connector で Microsoft .NET Core を使用しないでください。.NET Framework の代わりに.NET Core を使用すると、Cloud Connector のインストールが失敗する場合があります。Cloud Connector では.NET Framework のみを使用してください。

サーバーの要件

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）で Cloud Connector を使用している場合、マシン構成の手順については「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

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

- Cloud Connector をホストするために専用のマシンを使用します。そのマシンには他のコンポーネントをインストールしないでください。
- マシンが Active Directory ドメインコントローラーとして構成されていないこと。ドメインコントローラーへの Cloud Connector のインストールはサポートされていません。
- サーバークロックを正しい UTC 時間に設定済み。
- グラフィカルインストーラーを使用する場合は、ブラウザーのインストールと、デフォルトのシステムブラウザーセットが必要です。

Windows Update のガイダンス

Citrix Cloud Connector をホストしているすべてのマシンで、Windows Update を有効にすることを Citrix では強くお勧めします。Citrix Cloud Connector は、保留中の再起動がないか定期的にチェックします。保留中の再起動は、Windows Update などのさまざまな要因によって起動される場合があり、5 分ごとに実行されます。検出された再起動は、リソースの場所に設定されている希望日のスケジュールに関係なく、ただちに実行されます。このプロアクティブなアプローチにより、Citrix Cloud Connector が長期間更新が保留状態のままになることがなくなり、システムの安定性が維持されます。

Citrix Cloud プラットフォームは、可用性を維持するために再起動を管理します。一度に再起動できる Citrix Cloud Connector は 1 つだけです。Windows Update をセットアップするときは、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 Windows が設定されていることを確認してください。ただし、Citrix Cloud Connector が再起動プロセスを管理するための十分な時間を確保できるように、少なくとも 4 時間は自動再起動が許可されません。さらに、更新後にマシンを再起動する必要がある場合に備えて、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。詳しくは、「更新後のデバイスの再起動の管理」を参照してください。

> 注:
>
> - お客様が Citrix Cloud Connector を営業時間中に再起動する予定がない場合は、それに応じて営業時間外に Windows Update をスケジュールすることをお勧めします。
> - 各 Citrix Cloud Connector の再起動には約 10 分かかります。これには、Citrix Cloud プラットフォームと同期して、特定の時点で 1 つの Citrix Cloud Connector のみが再起動されるようにするために必要な時間も含まれます。したがって、前述のように、推奨される自動再起動の最小遅延は 4 時間ですが、テナント内の Citrix Cloud Connector の数に応じて、時間を短くしたり長くしたりするように調整できます。

証明書の検証要件

Cloud Connector が通信する Cloud Connector バイナリとエンドポイントは、広く評価された商用証明機関（CA）が発行した X.509 証明書で保護されています。公開キー基盤（PKI）の証明書の検証機能には、証明書失効一覧（CRL）があります。証明書を受信すると、クライアントは証明書を発行した CA を信頼するか、および証明書が CRL に含まれるかをチェックします。証明書が CRL にある場合は失効し、有効であると表示された場合でも信頼できないと判断されます。

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、外部のポート 80 とは通信しません。外部ポート 80 が必要となるのは、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ためです。

X.509 証明書は、Cloud Connector のインストール時に検証されます。そのため、すべての Cloud Connector マシンは、これらの証明書を信頼するように構成して、Cloud Connector ソフトウェアを正常にインストールできるようにする必要があります。

Citrix Cloud エンドポイントは、DigiCert によって発行された証明書、または Azure によって使用されるルート認証局の 1 つにより保護されています。Azure で使用されるルート証明機関について詳しくは、https://docs.microsoft.com/ja-jp/azure/security/fundamentals/tls-certificate-changesを参照してください。

証明書を検証するには、各 Cloud Connector マシンが次の要件を満たしている必要があります:

- HTTP ポート 80 が、以下のアドレスに対して開かれている。このポートは、Cloud Connector のインストール時と定期的な CRL チェック中に使用されます。CRL および OCSP 接続をテストする方法について詳しくは、DigiCert Web サイトの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。
  - 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
- 以下のアドレスとの通信が有効になっている:
  - https://*.digicert.com
- 以下のルート証明書がインストールされている:
  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.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
- 以下の中間証明書がインストールされている:

  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt
  - https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt

いずれかの証明書がない場合、Cloud Connector インストーラーはhttp://cacerts.digicert.comから該当する証明書をダウンロードします。

証明書をダウンロードおよびインストールする手順について詳しくは、CTX223828を参照してください。

Citrix DaaS DaaS リソースへの接続に Cloud Connector を利用するには、追加の証明書をインストールし、拡張 PKI インフラストラクチャへのアクセスを許可する必要があります。各 Cloud Connector マシンは、次の要件を満たす必要があります:

- HTTP ポート 80 が、以下のアドレスに対して開かれている:
  - crl.*.amazontrust.com
  - ocsp.*.amazontrust.com
  - *.ss2.us
- 以下のアドレスとの通信が有効になっている:
  - 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:
  - 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ている:
  - 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
```

いずれかの証明書がない場合、Cloud Connector はhttps://www.amazontrust.comから該当する証明書をダウンロードします

証明書をダウンロードおよびインストールする手順について詳しくは、CTX223828を参照してください。

Active Directory の要件

- ユーザー用のオファリング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 ドメインに参加済み。マルチドメイン環境については、この記事の「Active Directory での Cloud Connector 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 フォレストには、常に 2 つの Cloud Connector がアクセスできるようにする必要があります。
- Cloud Connector 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のドメインコントローラーにアクセスできる必要があります。詳しくは、次の Microsoft のサポート文書を参照してください:
  - ドメインと信頼を構成する方法
  - 「Windows のサービス概要および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、ユーザーグループのメンバーシップをフォレスト内の任意のドメインコントローラーから確実に取得できます。

ネットワークの要件

- 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済み。詳しくは、「Cloud Connector のプロキシとファイアウォールの構成」を参照してください。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」の次のセクションを参照してください。

- Cloud Connector の一般的なサービス接続要件
- Cloud Connector で許可されている FQDN

サポートされる **Active Directory** の機能レベル

Citrix Cloud Connector は、Active Directory フォレストとドメインの以下の機能レベルをサポートします。

フォレスト機能レベル	ドメイン機能レベル	サポートされるドメインコントローラー
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016、Windows Server 2019、Windows Server 2022

FIPS（**Federal Information Processing Standard**）のサポート

Cloud Connector は現在、FIPS 対応の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。このサポートは、Citrix Cloud で利用可能な Cloud Connector ソフトウェアの最新バージョンにのみ含まれています。お使いの環境に既存の Cloud Connector マシンがあり（2018 年 11 月より前にインストール）、そのマシンで FIPS モードを有効にする場合は、次の操作を実行します：

1. リソースの場所にある各マシンで Cloud Connector ソフトウェアをアンインストールします。
2. 各マシンで FIPS モードを有効にします。
3. FIPS 対応の各マシンに最新バージョンの Cloud Connector をインストールします。

> 重要:
>
> - 既存の Cloud Connector インストールを最新バージョンにアップグレードしないでください。必ず古い Cloud Connector をアンインストールしてから、新しい Cloud Connector をインストールします。
> - 古いバージョンの Cloud Connector をホストするマシンでは、FIPS モードを有効にしないでください。バージョン 5.102 より古い Cloud Connector は FIPS モードをサポートしていません。古い Cloud Connector がインストールされているマシンで FIPS モードを有効にすると、Citrix Cloud が Cloud Connector の定期的なメンテナンス更新を実行できなくなります。

Cloud Connector の最新バージョンをダウンロードする手順については、「Cloud Connector の入手場所」を参照してください。

Cloud Connector でインストールされるサービス

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のシステム権限について説明します。

インストール中に、Citrix Cloud Connector 実行可能ファイルがインストールされ、機能に必要なサービス構成がデフォルトに設定されます。デフォルトの構成を手動で変更すると、Cloud Connector が正常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引き続き機能できると仮定すると、次の Cloud Connector 更新が発生したときに、構成はデフォルトの状態にリセットされます。

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呼び出しを昇格させ、ネットワーク上で直接通信しません。Cloud Connector 上のサービスがローカルシステム権限が要求されるアクションを実行する必要がある場合、Citrix Cloud Agent System によって可能な事前定義された一連の操作によって実行します。

サービス名	説明	実行アカウント
Citrix Cloud Agent System	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 によってのみ呼び出すことができます。	ローカルシステム
Citrix Cloud Services Agent WatchDog	オンプレミスエージェント（エバーグリーン）を監視およびアップグレードします。	ネットワークサービス

サービス名	説明	実行アカウント
Citrix Cloud Services Agent Logger	Citrix Cloud Connector サービス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
Citrix Cloud Services AD Provider	インストールされている Active Directory ドメインアカウントに割り当てられたリソースの Citrix Cloud による管理を容易にします。	ネットワークサービス
Citrix Cloud Services Agent Discovery	XenApp および XenDesktop のレガシーオンプレミス Citrix 製品の Citrix Cloud による管理を容易にします。	ネットワークサービス
Citrix Cloud Services Credential Provider	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
Citrix Cloud Services WebRelay Provider	WebRelay Cloud サービスから受信した HTTP 要求をオンプレミスの Web サーバーに転送できます。	ネットワークサービス
Citrix CDF Capture Service	すべての構成済み製品および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
Citrix Config Synchronizer Service	仲介の構成をローカルに高可用性モードでコピーします。	ネットワークサービス
Citrix Connection Lease Exchange Service	ワークスペース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 High Availability Service	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 Adapter Provider	Virtual Apps and Desktops 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 CloudGateway	受信ファイアウォール規則を開いたり、DMZ にコンポーネントを展開したりする必要なく、オンプレミスのデスクトップおよびアプリケーションに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

サービス名	説明	実行アカウント
Citrix Remote Broker Provider	ローカルの VDA および StoreFront サーバーからリモートの Broker Service への通信を有効にします。	ネットワークサービス
Citrix Remote HCL Server	Delivery Controller とハイパーバイザー間の通信をプロキシ接続します。	ネットワークサービス
Citrix WEM Cloud Authentication Service	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
Citrix WEM Cloud Messaging Service	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

Active Directory での **Cloud Connector** 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種類は、展開によって異なります。

Active Directory での Connector Appliance の使用について詳しくは、「Active Directory での Connector Appliance の展開シナリオ」を参照してください。

安全な内部ネットワーク内に Cloud Connector をインストールします。

単一フォレスト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、リソースの場所が確立されます。環境内に複数のドメインがある場合、利用可能なリソースにユーザーがアクセスできるよう、Cloud Connector をインストールする場所を検討する必要があります。

ドメイン間の信頼が親と子の信頼でない場合、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とき、またはいずれかのドメインからの VDA の登録を行うときに、リソースの列挙を処理する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、ブループリントの一部となります。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もこのブループリントを使用する必要がある場合があります。

単一フォレストに単一ドメインが存在する場合に、単一の **Cloud Connector** セットを展開

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

- 信頼関係：なし - 単一ドメイン
- ［**ID** およびアクセスの管理］に表示されるドメイン：forest1.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

> 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で到達可能な状態にある限りは、Cloud Connector の単一の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別のドメインにある場合でも、Citrix Cloud がハイパーバイザーと通信できるようにするために、そのドメインに別の Cloud Connector のセットを展開する必要はありません。

単一フォレストに親子ドメインが存在する場合に、単一の **Cloud Connector** セットを展開

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 1 つ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 1 つのリソースの場所に展開され、forest1.local ドメインに参加します。

- 信頼関係：親と子のドメインの信頼
- ［**ID** およびアクセスの管理］に表示されるドメイン：forest1.local、user.forest1.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

> 注:
>
> Citrix Cloud が子ドメインを認識するには、Cloud Connector の再起動が必要な場合があります。

別々のフォレストにユーザーとリソースが存在する場合に（信頼関係あり）、単一の **Cloud Connector** セットを展開

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。一方向の信頼関係は、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場合に存在します。単一の Cloud Connector セットが 1 つのリソースの場所に展開され、forest1.local ドメインに参加します。

- 信頼関係：一方向のフォレストの信頼

- [**ID** およびアクセスの管理] に表示されるドメイン: forest1.local
- Citrix Workspace にログオンできるユーザー: forest1.local のユーザーのみ
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

> 注:
>
> 2 つのフォレスト間の信頼関係は、ユーザーフォレスト内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ように設定する必要があります。

Cloud Connector はフォレストレベルの信頼を通過できないため、Citrix Cloud コンソールの [**ID** およびアクセスの管理] ページに forest2.local ドメインは表示されず、クラウド側の機能はそのドメインを使用できません。そのため、次の制限事項が発生します:

- リソースは、Citrix Cloud の forest1.local に配置されたユーザーとグループにのみ公開できます。ただし、StoreFront ストアを使用している場合、forest2.local のユーザーを forest1.local のセキュリティグループ内に入れ子にすることで、この問題に対処できます。
- Citrix Workspace は、forest2.local ドメインのユーザーを認証できません。
- Citrix DaaS の [監視] 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。

これらの制限事項の回避策としては、「別々のフォレストにユーザーとリソースが存在する場合に (信頼関係あり)、Cloud Connector セットを各フォレストに展開」の説明に従って、Cloud Connector を展開します。

別々のフォレストにユーザーとリソースが存在する場合に (信頼関係あり)、**Cloud Connector** セットを各フォレストに展開

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。一方向の信頼関係は、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場合に存在します。単一の Cloud Connector セットが forest1.local ドメインに展開され、2 つ目のセットが forest2.local ドメインに展開されます。

- 信頼関係: 一方向のフォレストの信頼
- [**ID** およびアクセスの管理] に表示されるドメイン: forest1.local、forest2.local
- Citrix Workspace にログオンできるユーザー: すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

このシナリオでは、コストや管理上のオーバーヘッドを削減するために、リソースがないユーザーフォレスト内で Cloud Connector の代わりに Connector Appliance を使用できます (特に複数のユーザーフォレストがある場合)。詳しくは、「別々のフォレストにユーザーとリソースが存在する場合に (信頼関係あり)、すべてのフォレストに単一の Connector Appliance セットを展開」を参照してください。

Cloud Connector の正常性を表示する

Cloud 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 の状態が表示されます。個々の Cloud Connector の高度なヘルスチェックデータを表示することもできます。詳しくは、「Cloud Connector の高度なヘルスチェック」を参照してください。

イベントメッセージ

Cloud Connector は、Windows イベントビューアーで表示できる特定のイベントメッセージを生成します。優先する監視ソフトウェアを有効にしてこれらのメッセージを検索する場合は、ZIP アーカイブとしてダウンロードできます。この ZIP ダウンロードでは、次の XML ファイルにこれらのメッセージが含まれます:

- Citrix.CloudServices.Agent.Core.dll.xml（Connector Agent Provider）
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml（Connector AgentWatchDog Provider）

Cloud Connector のイベントメッセージをダウンロードします。

イベントログ

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\Log ディレクトリにあります。

トラブルシューティング

Cloud Connector の問題を診断するための最初の手順は、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。Cloud Connector がリソースの場所に表示されない、または「接続していない」場合は、イベントログに初期情報が表示されます。

Cloud Connector 接続

Cloud Connector が「切断」になっている場合、Cloud Connector 接続チェックユーティリティによって、Citrix Cloud およびその関連サービスに到達できることを検証できます。

Cloud Connector 接続チェックユーティリティは、Cloud Connector をホストしているマシンで実行されます。環境でプロキシサーバーを使用している場合、ユーティリティはすべての接続チェックをプロキシサーバー経由でトンネリングし、接続を検証できます。このユーティリティは、必要に応じて不足している Citrix の信頼済みサイトを Internet Explorer の信頼済みサイトゾーンに追加することもできます。

このユーティリティのダウンロードおよび使用方法について詳しくは、Citrix サポートの Knowledge Center でCTX260337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。Cloud Connector を新しいマシンにインストールしてください。問題が解決されない場合は、Citrix サポートに連絡してください。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。

Secure Ticket Authority サーバーとしての **Cloud Connector** の展開

NetScaler コンソールを使用して、複数の Cloud Connector を Secure Ticket Authority（STA）サーバーとして使用している場合、各 STA サーバーの ID は、NetScaler コンソール管理と、アプリケーションおよびデスクトップ起動用の ICA ファイルの両方で、**CWSSTA** として表示されることがあります。その結果、STA チケットが正しくルーティングされず、セッションの起動に失敗します。この問題は、異なる顧客 ID を持つ別々の Citrix Cloud アカウントに Cloud Connector が展開されている場合に、発生することがあります。このシナリオでは、個別のアカウント間でチケットの不一致が発生し、セッションの作成が妨げられます。

この問題を解決するには、STA サーバーとしてバインドする Cloud Connector が、同じ顧客 ID を持つ同じ Citrix Cloud アカウントに属していることを確認してください。同じ NetScaler コンソール展開から複数のカスタマーアカウントをサポートする必要がある場合は、アカウントごとに Gateway 仮想サーバーを作成します。詳しくは、以下の記事を参照してください:

- Gateway 仮想サーバーの作成：仮想サーバーの作成
- Citrix Gateway での Secure Ticket Authority の構成
- 展開ガイド：Citrix Virtual Apps and Desktops のオンプレミスから Citrix Cloud への移行
- CTX232640：Cloud Connector を STA として使用するように Citrix Gateway を構成するにはどうすればよいですか

Cloud Connector のプロキシとファイアウォールの構成

April 6, 2024

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。インストーラーとインストールするサービスの両方が Citrix Cloud に接続します。
この両方が、インターネットアクセスを利用できるようにする必要があります。

接続の要件

HTTP トラフィックを使用するポート 443（送信のみ）を使用します。必須の接続可能アドレスのリストについては、次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 の一般的なサービス接続要件

Citrix Cloud に必要な連絡先アドレスは、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と、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、「送受信ポートの構成」を参照してください。

> 重要:
>
> - 一部のプロキシで SSL インターセプションを有効にすると、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。
> - SSL インターセプションは、Citrix Gateway アドレスでは実行できません。詳しくは、「Citrix Gateway サービスの接続要件」を参照してください。
> - SSL インターセプションが、ネットワークの接続性や安定性に影響を与えないようにする必要があります。詳しくは、「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は、次のトラフィックフローでプロキシをバイパスすることをお勧めします:
>
> - 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 要求）。

さらに、コネクタは WinHTTP プロキシ設定を利用することに注意してください。構成設定については、CTX222727を参照してください。

Cloud Connector 接続の確認

Cloud Connector 接続性チェックユーティリティでは、いくつかの接続チェックを使用して、Cloud Connector と Citrix Cloud 間の接続を確認できます。環境でプロキシサーバーを使用している場合、このユーティリティによって Cloud Connector でプロキシ設定を構成し、プロキシサーバー経由の接続をテストできます。プロキシサーバーが構成されると、接続テストはプロキシサーバー経由でトンネリングされます。

> 注:
>
> Cloud Connector 接続チェックユーティリティは、商用の Citrix Cloud アカウントでのみ使用できます。Citrix Cloud Government または Citrix Cloud Japan では使用しないでください。

Cloud Connector 接続チェックユーティリティのダウンロードおよび使用について詳しくは、CTX260337を参照してください。

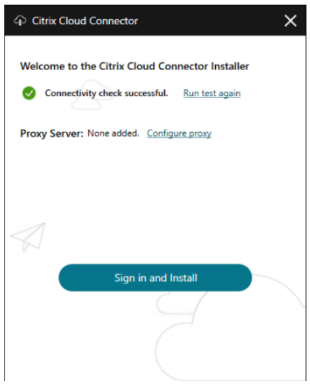
インストーラー

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のであれば、インストーラーも機能します。

ランタイムのサービス

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。（上記のように）ユーザー用の設定は使用されません。

インストール中にプロキシ設定を構成できます。



インストーラーの起動後、Citrix Cloud にログインする前に、［プロキシの構成］をクリックします。プロキシをバイパスするために、プロキシ情報とアドレスを追加するように求められます。バイパスのアドレスを指定する場合、完全修飾ドメイン名（FQDN）アドレス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、手動でプロキシを設定する必要があります。自動検出または PAC/setup スクリプトによる自動プロキシセットアップはサポートされていません。

Cloud Connector のインストール

July 2, 2024

Cloud Connector ソフトウェアは、対話形式で、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行われます。Cloud Connector は、次のことを行うためにクラウドにアクセスする必要があります:

- 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確認する
- 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

- システム要求：Cloud Connector をホストするマシンを準備するために確認します。
- Tech Zone 記事「エンドポイントのセキュリティとウイルス対策のベストプラクティス」の「ウイルス対策の除外」セクション：環境の Cloud Connector に対してセキュリティとパフォーマンスの適切なバランスを判断するためのガイドラインを提供しています。これらのガイドラインを組織のウイルス対策チームとセキュリティチームとともに確認し、実稼働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お勧めします。
- システムおよび接続要件：Cloud Connector をホストするすべてのマシンが Citrix Cloud と通信できることを確認してください。
- Cloud Connector のプロキシとファイアウォールの構成：Web プロキシまたは厳密なファイアウォールルールを持つ環境に Cloud Connector をインストールする場合。
- Cloud Connector のスケールおよびサイズの考慮事項：Cloud Connector をホストするマシンの構成に関する、テスト済み最大容量の詳細とベストプラクティスの推奨事項を提供します。

インストールの考慮事項とガイダンス

- Active Directory ドメインコントローラーや、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に Cloud Connector をインストールしないでください。Cloud Connector の定期的な保守では、これらの追加リソースの停止を引き起こすマシン操作を実行します。
- Cloud Connector をホストしているマシンに他の Citrix 製品をダウンロードしたりインストールしたりしないでください。
- 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。
- 他の Citrix 製品展開に属するマシン（たとえば、オンプレミスの Citrix Virtual Apps and Desktops 展開の Delivery Controller）に Cloud Connector をダウンロードまたはインストールしないでください。
- 以前にインストールした Cloud Connector を新しいバージョンにアップグレードしないでください。古い Cloud Connector をアンインストールしてから、新しいバージョンをインストールしてください。
- Cloud Connector のインストーラーは、Citrix Cloud からダウンロードします。そのため、ブラウザーが実行可能ファイルをダウンロードできるようにする必要があります。
- グラフィカルインストーラーを使用する場合は、ブラウザーのインストールと、デフォルトのシステムブラウザーセットが必要です。

導入後のガイダンス

インストールしたら、すべての Cloud Connector の電源をオンのままにして、Citrix Cloud への常時接続を確保します。

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ます:

1. リソースの場所からマシンを削除します:
    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 Connector**］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。［コネクタを削除］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. この記事の説明に従って、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. 現在のドメインからマシンの参加を解除し、マシンを新しいドメインに再度参加させます。
4. この記事の説明に従って、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。

クローンマシンに関する考慮事項

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。これにより、Citrix Cloud がリソースの場所内のマシンと確実に通信できるようになります。リソースの場所の複数のマシンで Cloud Connector をホストし、クローンマシンを使用する場合は、次の手順を実行します:

1. 使用環境に合わせてマシンテンプレートを準備します。
2. Cloud Connector として使用する数のマシンをプロビジョニングします。
3. 手動またはサイレントインストールモードを使用して、各マシンに Cloud Connector をインストールします。

(複製前に) Cloud Connector をマシンテンプレートにインストールすることはサポートされていません。Cloud Connector をインストールしたマシンを複製すると、Cloud Connector サービスは実行されず、マシンは Citrix Cloud に接続できなくなります。

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、使用す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 用の 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」が表示されていないことを確認します。Citrix DaaS でマシンカタログのセットアップ中に未使用のドメインを指定すると、エラーが発生する場合があります。詳しくは、Citrix DaaS 製品ドキュメントの「リソースの種類を追加するか、Citrix Cloud で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。

他のサービスに関するその他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の場所

Citrix Cloud アカウントにリソースの場所がなく、ドメインに Cloud Connector をインストールした場合、Citrix Cloud が作成するリソースの場所がデフォルトのリソースの場所になります。アカウントに設定できるデフォルトのリソースの場所は 1 つだけです。必要に応じて、Citrix Cloud で追加のリソースの場所を作成し、他のドメインに Cloud Connector をインストールするときにいずれかを選択できます。

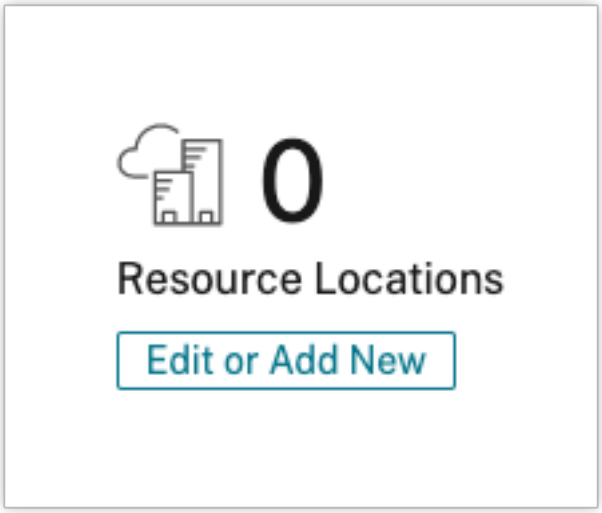
または、最初にコンソールで必要なリソースの場所を作成してから、ドメインに Cloud Connector をインストールすることもできます。Cloud Connector インストーラーは、インストール中に、必要なリソースの場所を選択するよう求めます。

インタラクティブインストール

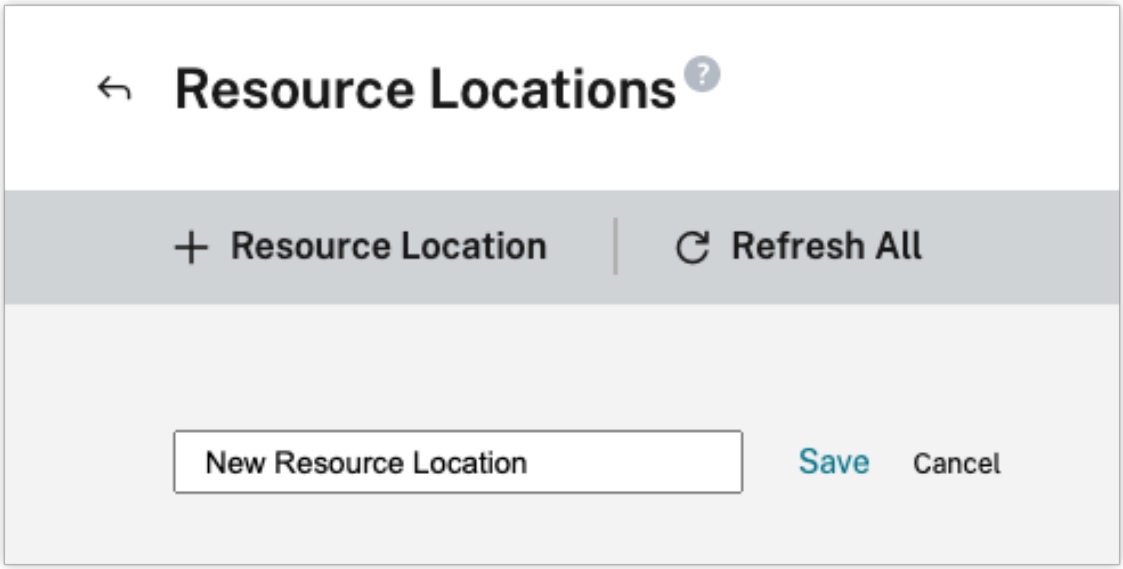
グラフィカルインストーラーインターフェイスを使用して、Cloud Connector をダウンロードしインストールできます。これを行う前に、Citrix Cloud 管理コンソールで 1 つまたは複数のリソースの場所を作成して、Cloud Connector を展開する必要があります。リソースの場所について詳しくは、「リソースの場所」を参照してください。

リソースの場所を作成するには

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にアクセスして、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］に移動する、またはページ上部の ［リソースの場所］にある ［編集または新規追加］を選択します。



4. ［リソースの場所］ページの上部にある ［**+** リソースの場所］を選択し、わかりやすい新しい名前で保存します。

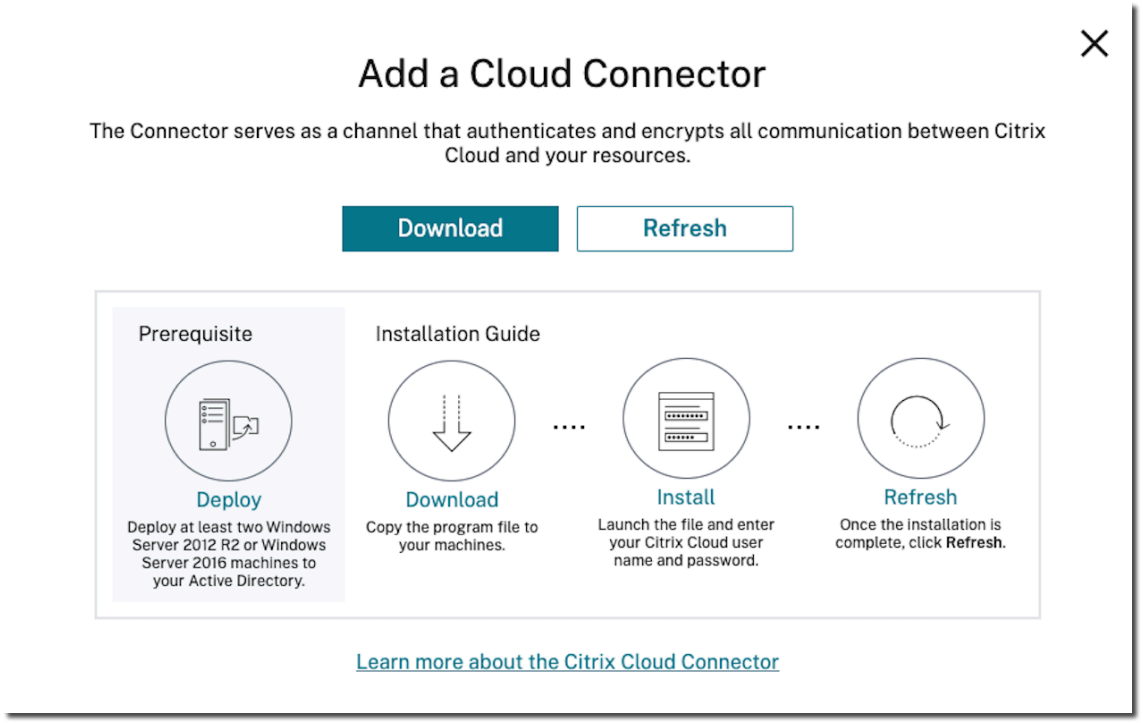


Citrix Cloud Connector ソフトウェアのダウンロード

1. 管理するリソースの場所を見つけて ［**+ Cloud Connectors**］を選択します。

2. 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

カルファイルの場所に保存します。



Citrix Cloud Connector ソフトウェアのインストール

1. **cwcconnector.exe** インストーラーファイルを右クリックして、［管理者として実行］を選択します。インストーラーは、最初の接続性チェックを実行して、Citrix Cloud に接続できることを確認します。
2. （オプション）必要に応じて、［プロキシの構成］をクリックしてプロキシサーバーを追加します。プロキシをバイパスするために、プロキシ情報とアドレスを追加するように求められます。バイパスのアドレスを指定する場合、完全修飾ドメイン名（FQDN）アドレスとワイルドカードアドレスの両方がサポートされます。
3. ［サインインしてインストール］をクリックして、Citrix Cloud にサインインします。
4. Cloud Connector をインストールして構成するには、ウィザードの指示に従います。インストールが完了すると、インストーラーは最終的な接続性チェックを実行して、Cloud Connector と Citrix Cloud 間の通信を検証します。
5. Citrix Cloud Connector として使用する他のマシンで、これらの手順を繰り返します。可用性を高めるため、リソースの場所ごとに Cloud Connector を 2 つ以上インストールすることをお勧めします。

Citrix Cloud では、リソースの場所の ［**Connectors**］ページに、新しくインストールした Cloud Connector が表示されます。

インストール後、Citrix Cloud の ［**ID** およびアクセス管理］**>**［ドメイン］にも管理者のドメインが登録されます。詳しくは、「ID およびアクセス管理」を参照してください。

未使用ドメインのアクティブ化

リソースの場所を作成し、Citrix DaaS 用の Cloud Connector を展開している場合は、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 でマシンカタログのセットアップ中に未使用のドメインを指定すると、エラーが発生する場合があります。

詳しくは、Citrix DaaS 製品ドキュメントの「リソースの種類を追加するか、Citrix Cloud で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

1. Citrix Cloud 管理コンソールで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］をクリックして、意味がわかる名前を入力します。
3. ［保存］をクリックします。Citrix Cloud は、新しいリソースの場所のタイルを表示します。
4. ［**Cloud Connector**］、［ダウンロード］の順にクリックして、Cloud Connector ソフトウェアを入手します。
5. 準備した各マシンで、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 Connector に関連付けるリソースの場所を選択するように求められます。

複数の顧客および既存のリソースの場所でのインストール

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要求します。

顧客アカウントに複数のリソースの場所が既に存在する場合、Citrix Connector に関連付けるリソースの場所を選択するように求められます。

コマンドラインインストール

サイレント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、同じインストーラーで繰り返しインストールしないでください。Citrix Cloud コンソールの［リソースの場所］ページから新しい Cloud Connector をダウンロードします。

要件

Citrix Cloud でコマンドラインを使用してインストールするには、次の情報を入力する必要があります:

- Citrix 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、［**ID** およびアクセス管理］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セキュア API クライアントのクライアント ID とシークレット。これらの値を取得するには、まずセキュアクライアントを作成する必要があります。クライアント ID とシークレットにより、Citrix Cloud API へのアクセスが適切に保護されます。セキュアクライアントを作成すると、クライアントは、作成するユーザーと同じレベルの管理者権限で動作します。Cloud Connector をインストールするには、フルアクセス権限を持つ管理者によって作成されたセキュアクライアントを使用する必要があります。これは、そのセキュアクライアントにもフルアクセス権限があることを意味します。
- Cloud Connector に関連付けるリソースの場所の ID。この値を取得するには、［リソースの場所］ページのリソースの場所の名前の下にある ［**ID**］ボタンを選択します。この値を指定しない場合、デフォルトのリソースの場所の ID が使用されます。

セキュアクライアントの作成

セキュアクライアントを作成する場合、Citrix Cloud により一意のクライアント ID とシークレットが生成されます。コマンドラインから API を呼び出すときに、これらの値を指定する必要があります。

1. Citrix Cloud メニューから、［**ID** およびアクセス管理］を選択し、次に ［**API** アクセス］を選択します。
2. ［セキュアクライアント］タブから、クライアントの名前を入力し、［クライアントの作成］を選択します。セキュアクライアントのクライアント ID とシークレットが生成されて表示されます。
3. ［ダウンロード］を選択して、クライアント ID とシークレットを CSV ファイルとしてダウンロードし、安全な場所に保存します。または、［コピー］を選択して、それぞれの値を手動で取得します。完了したら ［閉じる］を選択してコンソールに戻ります。

サポートされているパラメーター

セキュアクライアントのセキュリティの詳細を確保するには、インストーラーに JSON 構成ファイルを提供する必要があります。このファイルは、インストールの完了後に削除する必要があります。構成ファイルでサポートされている値は次のとおりです:

- **customerName**: 必須。[ID およびアクセス管理] の Citrix Cloud コンソールの [API アクセス] ページに表示される顧客 ID。
- **clientId**: 必須。管理者が作成できるセキュアクライアント ID で、[API アクセス] ページにあります。
- **clientSecret**: 必須。セキュアクライアントが作成された後にダウンロードできるセキュアクライアントシークレット。[API アクセス] ページにあります。
- **resourceLocationId**: 推奨。既存のリソースの場所の一意の識別子。Citrix Cloud コンソールの [リソースの場所] ページで、ID ボタンを選択してリソースの場所の ID を取得します。値を指定しない場合、Citrix Cloud はアカウント内の最初のリソースの場所の 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"
 }

<!--NeedCopy-->
```

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モードでインストールします。

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
<!--NeedCopy-->
```

/qを使用してサイレントインストールを指定します。

エラーが発生した場合に可能性のある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は、標準的なメカニズムである「**echo %ErrorLevel%**」を使用できます。

> 注:
>
> パラメーターを使用したクライアント ID とクライアントシークレットの指定はサポートされなくなりました。自動インストールには構成ファイルを使用する必要があります。

次の手順

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、「Connector の更新」を参照してください。
2. ワークスペース利用者を認証するための ID プロバイダーを設定します。［**ID** およびアクセス管理］コンソールで、デフォルトの Citrix ID プロバイダーを Active Directory などの ID プロバイダーに変更できます。詳しくは、「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がある問題を診断および修正するいくつかの方法について詳しく説明します。インストール問題のトラブルシューティングについて詳しくは、「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

利用可能なログファイルを最初に調べることで、インストール時に発生した問題のトラブルシューティングを行うことができます。

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。**%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup** にある Cloud Connector のインストールログを確認することもできます。
また、インストール後は**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** にもログが追加されます。

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ことがあります:

- 1603 - 予期しないエラーが発生しました
- 2 - 前提条件チェックが不合格でした
- 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場合があります:

```
Can't reach this page.
```

このエラーは、管理者としてマシンにログインして Citrix Cloud Connector をインストールする場合でも発生することがあります。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。

接続エラー

Cloud Connector が Citrix Cloud と通信できていることを確認するには、以下の Citrix サービスが ［開始］状態になっていることを確認します:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service
- Citrix High Availability Service
- Citrix NetScaler CloudGateway
- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

これらのサービスについて詳しくは、「インストールされているサービス」を参照してください。

接続エラーが引き続き発生する場合は、Citrix Support Knowledge Center で入手できる Cloud Connector 接続チェックユーティリティを使用してください。詳しくは、Knowledge Center Web サイトのCTX260337を参照してください。

このツールを使用して、次のタスクを実行できます:

- Citrix Cloud とその関連サービスにアクセスできるかどうかのテスト。
- 誤って構成されがちな設定のチェック。
- Citrix Cloud Connector のプロキシ設定の構成。

失敗した接続性チェックを解決する方法について詳しくは、「CTX224133: Cloud Connector 接続性チェックエラー」を参照してください。

Cloud Connector の高度なヘルスチェック

December 14, 2023

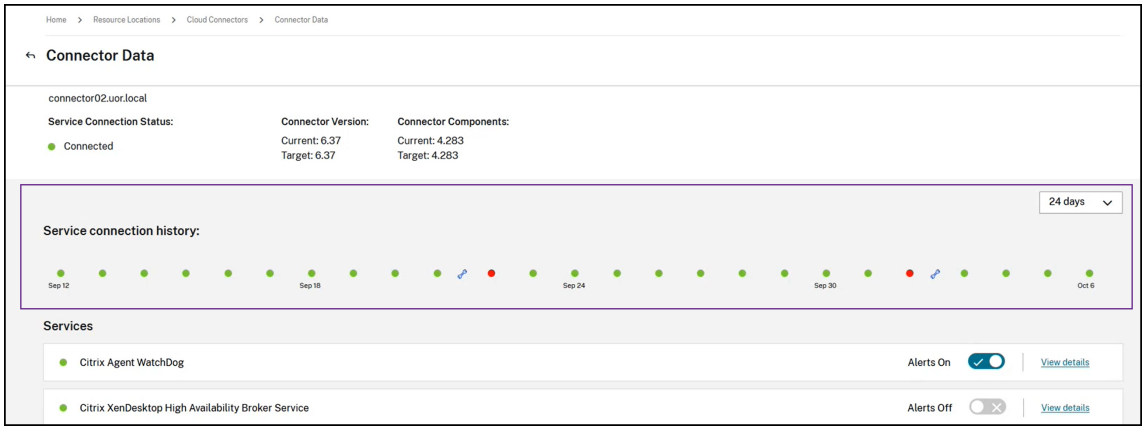
更新の前後に、Cloud Connector はヘルスチェックを実行して、更新によってプロバイダーに不要なダウンタイムが発生しないことを確認します。Connector と、Connector 上の各サービスおよびプロバイダーの接続とサーバーヘルスの状態を確認できます。

Connector ヘルスチェックデータの表示

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する Connector を選択します。
3. Connector ページで、Connector の横にある省略記号メニューに移動し、［**Connector** データの表示］を選択します。

Connector データのページが表示され、次の情報が表示されます。

- ［サービス接続状態］。Connector データページのこの領域には、次の情報が表示されます:
  - Connector が Cloud 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は、現在インストールされているバージョンと次のアップデートでインストールされる予定のターゲットバージョン
- ［サービス接続履歴］。24 のステータスインジケータは、時間の経過に伴う Connector のサーバーヘルスの状態を示します。デフォルトでは、サービス接続履歴には、過去 24 時間のステータスが 1 時間間隔で表示されます。その他の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。過去 24 日間のステータスが 1 日間隔で表示されます。
  - 緑色の丸印は、その期間においてステータスが正常だった時間を示します。
  - 赤い丸印は、その時間帯の障害または例外ステータスを示します。詳細については、丸印にカーソルを合わせてください。
  - レンチアイコンは、その時間帯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てください。
  - 灰色の丸印は、その時間帯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。



- ［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。
  - 各サービスの横の丸印は、サービスの現在のステータスを示します。
  - ［アラートがオンになっています］と ［アラートがオフになっています］を使用して、サービスからアラートを通知するかどうかを制御します。アラートがオンに設定されている場合、サービスで障害が発生すると、Connector 接続ステータス全体で障害が発生します。
  - 時間の経過に伴うサービスのサーバーヘルスの状態の詳細を表示するには、［詳細の表示］を選択します。
- ［コネクタメトリック］。この領域には、過去 24 時間または 24 日間の、メモリ、CPU、ネットワークデータ、およびディスク容量の Connector による使用量が表示されます。表示される期間を変更するには、［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。

サービスの詳細の表示

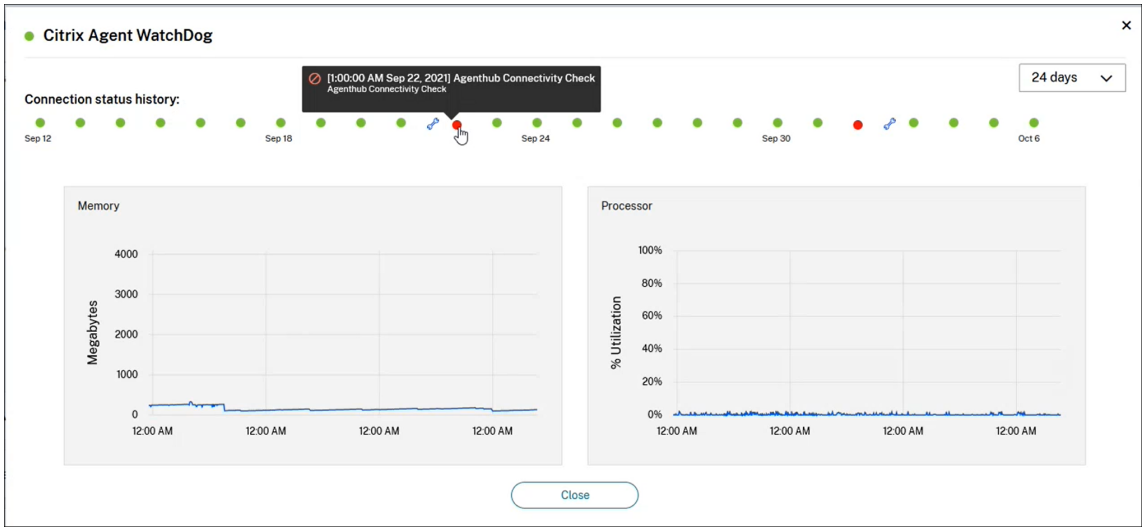
各サービスの接続ステータス履歴とメトリックを表示するには、次の手順に従います：

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、表示期間を選択します。過去 24 時間または 24 日間を、それぞれ 1 時間間隔または 1 日間隔で表示できます。
2. コネクタデータページで、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次の情報が表示されます：

- 時間の経過に伴うサービスのヘルスステータスを示す 24 のステータスインジケータ。
  - 緑色の丸印は、その期間においてステータスが正常だった時間を示します。
  - 赤い丸印は、その時間帯の障害または例外ステータスを示します。詳細については、丸印にカーソルを合わせてください。
  - レンチアイコンは、その時間帯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てください。
  - 灰色の丸印は、その時間帯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。

- 指定された期間における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。



コネクタの通知

November 4, 2022

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。Citrix Cloud ヘッダーのベルアイコンに新しい通知が表示されます。

このアイコンをクリックして通知を表示するか、コンソールメニューで ［通知］を選択します。

詳しくは、「通知」を参照してください。

Cloud Connector

次の表は、Cloud Connector で発生する可能性がある通知です:

アラートのメッセージ	アラートの種類	詳細	解像度
コネクタ *CONNECTOR_NAME* は定期的な保守を実行できなかったため、オフラインになり期限切れになりました。期限切れのコネクタはサービスの可用性に影響を与え、保守の妨げになります。	エラー	コネクタが長時間オフラインになってから後でオンラインに復帰した場合は、最新バージョンに更新できない古いバージョンの可能性があります。期限切れのコネクタは保守を実行できないため、環境内の他のコネクタの保守プロセスに影響を与える可能性があります。	古い Cloud Connector を更新する方法
コネクタ *CONNECTOR_NAME* は UTC 時間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する可能性があります。	エラー		Cloud Connector の時間を同期する方法
コネクタ *CONNECTOR_NAME* の保守に失敗しました。このコネクタでの保守に失敗すると、環境内の他のコネクタを保守できなくなります。保守が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やその他のメンテナンス操作が失敗しました。	Cloud Connector のメンテナンスに失敗した際の解決方法
コネクタ *CONNECTOR_NAME* は［数字］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、保守の妨げになります。	警告	コネクタが一定時間接続できない場合、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復元する方法

アラートのメッセージ	アラートの種類	詳細	解像度
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がサービスの可用性および機能に影響を与える可能性があります。	警告	エラーコード *HEALTH_CHECK_CODE* で接続性チェックに失敗しました。このコネクタは、通知メッセージに表示されている特定の Web アドレスまたは IP アドレスに接続できませんでした。	Cloud Connector 接続性チェックエラー
コネクタ *CONNECTOR_NAME* で CPU 使用率が高くなっています。制約のあるリソース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。	警告	このコネクタの CPU 使用率は、1 時間のサンプル期間で 80% を超えています。	Cloud Connector のリソース可用性アラートを解決する方法
コネクタ *CONNECTOR_NAME* の空きディスク領域が不足しています。制約のあるディスク領域で動作するコネクタは、サービスのパフォーマンスと保守に影響を与えます。	警告	このコネクタの空きディスク領域は、2GB 未満です。	Cloud Connector のリソース可用性アラートを解決する方法
コネクタ *CONNECTOR_NAME* の重要なプロセスまたはサービス可用性チェックが失敗した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する可能性があります。	警告		

Citrix Cloud Connector のログ収集

October 4, 2023

CDF ログは、Citrix 製品内のトラブルシューティングを目的として使用されます。Citrix サポートは、CDF トレースを使用して、アプリケーションとデスクトップの仲介、ユーザー認証、Virtual Delivery Agent（VDA）登録に関する問題を特定します。この記事では、環境で発生する可能性のある問題のトラブルシューティングと解決に使用できる Cloud Connector データをキャプチャする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 マシンでログを有効にします。
> - データの全範囲を確実にキャプチャするために、VDA にある CDFControl キャプチャツールを使用することをお勧めします。詳しくは、Citrix Support Knowledge Center のCTX111961を参照してください。Citrix Workspace アプリのログ収集について詳しくは、CTX141751を参照してください。
> - CDF トレースを Citrix に送信するには、Citrix サポートケースが開かれている必要があります。Citrix のサポート技術者は、既存のサポートケースに添付されていない CDF トレースを確認することはできません。

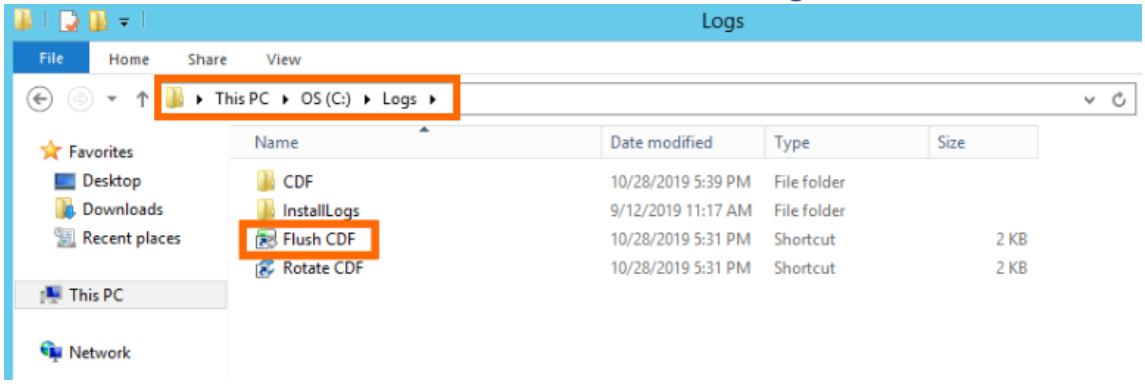
手順 **1**：問題を再現する

この手順では、使用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仲介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、再度 VDA 登録の作成を試みます。

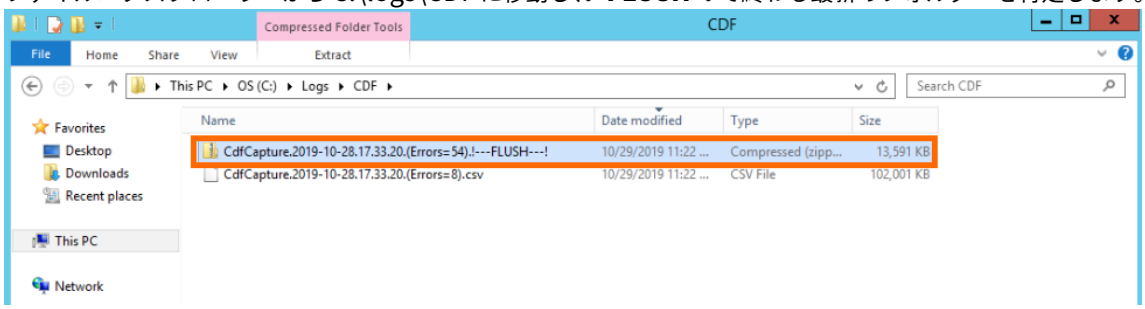
手順 **2**：**CDF** トレースを収集する

この手順では、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 接続を開始することにより、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. フラッシュ **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た後、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。

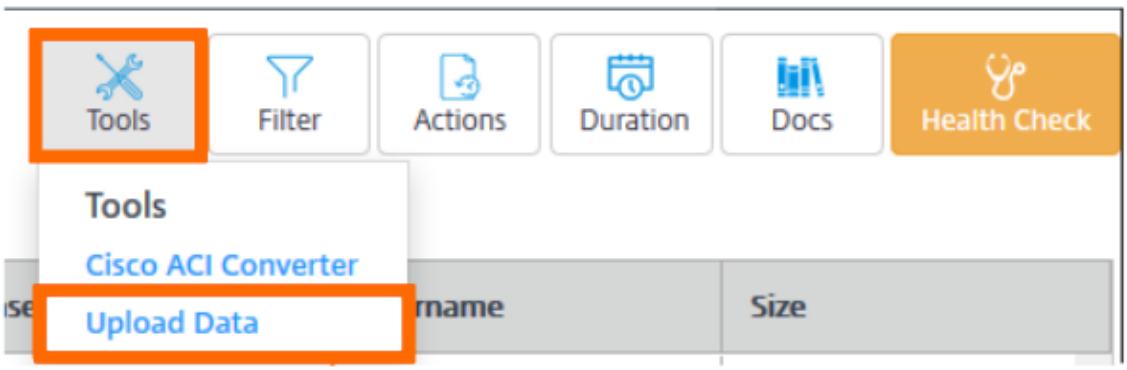


5. リソースの場所にあるすべての Cloud Connector マシンで手順 1～5 を実行し、すべての Cloud Connector のフラッシュトレースを 1 つの ZIP アーカイブに結合します。すべての Cloud Connector マシンからフラッシュトレースの ZIP アーカイブを作成しない場合は、一度に 1 ファイルずつ Citrix に送信する必要があります。

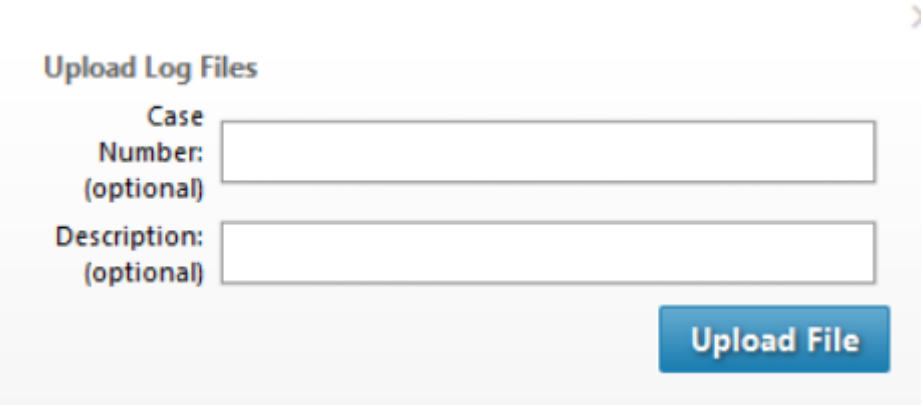
手順 **3**：**Citrix** にデータを送信する

この手順では、トレースファイルを Citrix サポートケースに添付し、レビューのために送信します。

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**]、[**Upload Data**] の順に選択します。



4. [**Case Number**] に、既存のサポートケースの Citrix サポートケース番号を入力してください。Citrix サポート技術者は、データのアップロードにケース番号が添付されていないと、CDF トレースを適切に確認できません。



5. ［説明（オプション）］には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、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、送信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送信すると、Citrix Insight Services はそれらを処理し、指定したサポートケースに添付します。このプロセスは、ファイルのサイズによっては最大 24 時間かかる場合があります。

プライマリのリソースの場所の選択

October 4, 2023

ドメイン内に複数のリソースの場所がある場合は、Citrix Cloud の「プライマリの」、つまり「最も優先される」場所を選択できます。プライマリのリソースの場所は、Citrix Cloud とドメイン間で最高のパフォーマンスと接続性を提供するため、ユーザーはすぐにサインインできるようになります。

プライマリのリソースの場所を選択すると、可能な場合は、そのリソースの場所にある Cloud Connector がユーザーのログオンとプロビジョニング操作に使用されます。プライマリのリソースの場所の 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）を使用するログオンには、ドメイン名が含まれていない場合があり、プライマリのリソースの場所を使用していない場合があります。

> 注:
>
> 任意のリソースの場所で常に Cloud Connector を使用できるようにするには、少なくとも 2 つの Cloud Connector を各リソースの場所にインストールすることをお勧めします。

プライマリのリソースの場所に使用するリソースの場所を決定するには、次の点を考慮してください。

- ドメインとの接続に優れたリソースの場所である。

- Citrix Cloud 管理コンソールを使用している地理的リージョンに最も近いリソースの場所である。たとえば、Citrix Cloud コンソールがhttps://us.cloud.comにある場合は、米国リージョンに最も近い場所をリソースの場所に選択します。

プライマリのリソースの場所を選択するには

1. Citrix Cloud 管理コンソールでメニューボタンをクリックし、[**ID** およびアクセス管理] を選択します。
2. [ドメイン] をクリックし、使用するリソースの場所を含むドメインを展開します。
3. [プライマリのリソースの場所を設定する] をクリックし、プライマリとして指定するリソースの場所を選択します。
4. [保存] をクリックします。選択したリソースの場所の横に「プライマリ」と表示されます。

> 注:
>
> 別のドメインを展開する前に、選択内容をドメインに保存してください。ドメインを展開してから別のドメインを展開すると、最初に展開されたドメインが折りたたまれ、保存されていない選択が破棄されます。

別のプライマリのリソースの場所を選択する

1. Citrix Cloud 管理コンソールでメニューボタンをクリックし、[**ID** およびアクセス管理] を選択します。
2. [ドメイン] をクリックし、変更するプライマリのリソースの場所を含むドメインを展開します。
3. [プライマリのリソースの場所を変更する] をクリックし、使用するリソースの場所を選択します。
4. [保存] をクリックします。

プライマリのリソースの場所をリセットする

プライマリのリソースの場所をリセットすると、別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、ドメイン内のどの Cloud Connector でも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、一部のユーザーのログオンが遅くなる可能性があります。

1. Citrix Cloud 管理コンソールでメニューボタンをクリックし、[**ID** およびアクセス管理] を選択します。
2. [ドメイン] を選択し、変更するプライマリのリソースの場所を含むドメインを展開します。
3. [プライマリのリソースの場所を変更する] を選択し、[リセット] を選択します。ログオンのパフォーマンスが影響を受ける可能性があることを警告する通知が表示されます。
4. [利用者に影響を与える可能性があることを了承します。] を選択し、[リセットの確認] をクリックします。

クラウドサービス用の **Connector Appliance**

April 5, 2024

Connector Appliance は、ハイパーバイザーでホストされる Citrix コンポーネントです。Citrix Cloud とリソースの場所との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構成を必要とせずにクラウドを管理できます。Connector Appliance を使用することで、リソースを管理しながら、ユーザーに価値を提供するリソースに集中することができます。

Connector Appliance は、次の機能を備えています:

- **Active Directory** を **Citrix Cloud** に接続することで、AD の管理を有効にし、リソースの場所内で AD のフォレストとドメインを使用できるようにします。これによって、さらに AD 信頼関係を追加する必要はなくなります。詳しくは、「Connector Appliance を使用した Active Directory」を参照してください。
- **Image Portability Service** は、すべてのプラットフォームにおいてイメージを簡単に管理できるようにします。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との間でイメージを管理するのに役立ちます。Citrix Virtual Apps and Desktops の 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にイメージを移行しようとすると、開始されます。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、実行の準備を支援します。最終的に、Citrix Provisioning または Machine Creation Services は、パブリッククラウドサブスクリプションで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** により、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たエクスペリエンスを提供し、エンドツーエンドのアクセス制御を行うことができます。詳しくは、「Connector Appliance を使用した Secure Private Access」を参照してください。

Connector Appliance を使用するプレビュー段階のサービスがほかにも存在する可能性があります。

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、次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
- Timestamp
- イベントデータ
- Active Directory からのユーザーとグループの詳細（ユーザーとグループの認証と検索などに使用されます）

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*」の表に記載されています。

Connector Appliance の可用性と負荷管理

継続的な可用性を確保して負荷を管理するために、各リソースの場所に複数の Connector Appliance をインストールします。Citrix では、各リソースの場所に少なくとも 2 つの Connector Appliance を使用することをお勧めしま

す。ある Connector Appliance を一定期間使用できない場合、他の Connector Appliance がその接続を維持できます。各 Connector Appliance はステートレスであるため、使用可能なすべての 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。この機能は自動化されています。少なくとも 1 つの Connector Appliance が利用可能である限り、Citrix Cloud との通信は失われません。

リソースの場所に対してコネクタが 1 つのみ構成されている場合、Citrix Cloud では ［リソースの場所］ページと［コネクタ］ページの両方に警告が表示されます。

Connector Appliance 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アクションを実行する必要はありません。

更新が利用可能になるとすぐに適用するか、指定した保守期間中に適用するかをリソースの場所で構成できます。

更新スケジュール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。

更新中に、Connector Appliance を一時的に利用できなくなります。更新は、リソースの場所の Connector Appliance に対して、一度に 1 つずつのみに適用されます。そのため、各リソースの場所に少なくとも 2 つの Connector Appliance を登録し、少なくとも 1 つの Connector Appliance を常に利用できるようにしてください。

Connector Appliance の通信

Connector Appliance は、Citrix Cloud とリソースの場所の間で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 は発信接続を介して Citrix Cloud との通信を開始します。すべての接続が、標準 HTTPS ポート（443）と TCP プロトコルを使用して Connector Appliance からクラウドに対して確立されます。受信接続は許可されません。

次の表は、Connector Appliance がサービスにアクセスするために必要なポートの一覧です:

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	このポートがローカル環境に対して開いている必要があります
NTP	123	UDP	このポートがローカル環境に対して開いている必要があります
HTTPS	443	TCP	Connector Appliance には、このポートへの送信アクセスが必要です

Connector Appliance を構成するには、IT 管理者が Connector Appliance のポート 443（HTTPS）の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:
>
> 注: IP アドレスの先頭に`https://`を追加する必要があります。

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どちらとも通信できます。Connector Appliance の登録時に 1 つ以上の Web プロキシを定義すると、Connector Appliance から外部システムへのトラフィックのみがこの Web プロキシ経由で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領域にある場合、Connector Appliance からこのシステムへのトラフィックは Web プロキシを経由してルーティングされません。

Connector Appliance では、プライベートアドレス領域が以下の IPv4 アドレス範囲として定義されます:

- 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の要件

データセンターからインターネットへの接続に必要なのは、発信接続のためにポート 443 を開くことです。ただし、インターネットの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操作するには、追加の構成が必要です。

Citrix Cloud サービスを適切に操作し消費するには、以下のアドレスが変更していない HTTPS 接続と通信可能である必要があります:

- `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顧客は、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://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

ネットワークの要件

環境の構成が以下の要件を満たしていることを確認します:

- ネットワークにより、Connector Appliance は DHCP を使用して、DNS および NTP サーバー、IP アドレス、ホスト名、およびドメイン名を取得できます。または、Connector Appliance コンソールでネットワーク設定を手動で設定することもできます。
- このネットワークは、Connector Appliance によって内部的に使用される 169.254.0.1/24、169.254.64.0/18、または 169.254.192.0/18 というリンクローカル IP 範囲を使用するようには構成されていません。
- ハイパーバイザー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るか、DHCP が NTP サーバー情報を Connector Appliance に提供します。
- Connector Appliance でプロキシを使用する場合、プロキシは認証されていない、または基本認証が使用されている必要があります。

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：

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi バージョン 7 Update 2
- Windows Server 2016、Windows Server 2019、または Windows Server2022 上の Hyper-V。
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

ハイパーバイザーは以下の最低要件を満たしている必要があります：

- 20GB ルートディスク
- 2 つの vCPU
- 4GB のメモリ
- IPv4 ネットワーク

同じハイパーバイザーホストで複数の 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限されます。

> 注：
>
> Connector Appliance VM のスナップショットの複製、一時停止、および作成はサポートされていません。

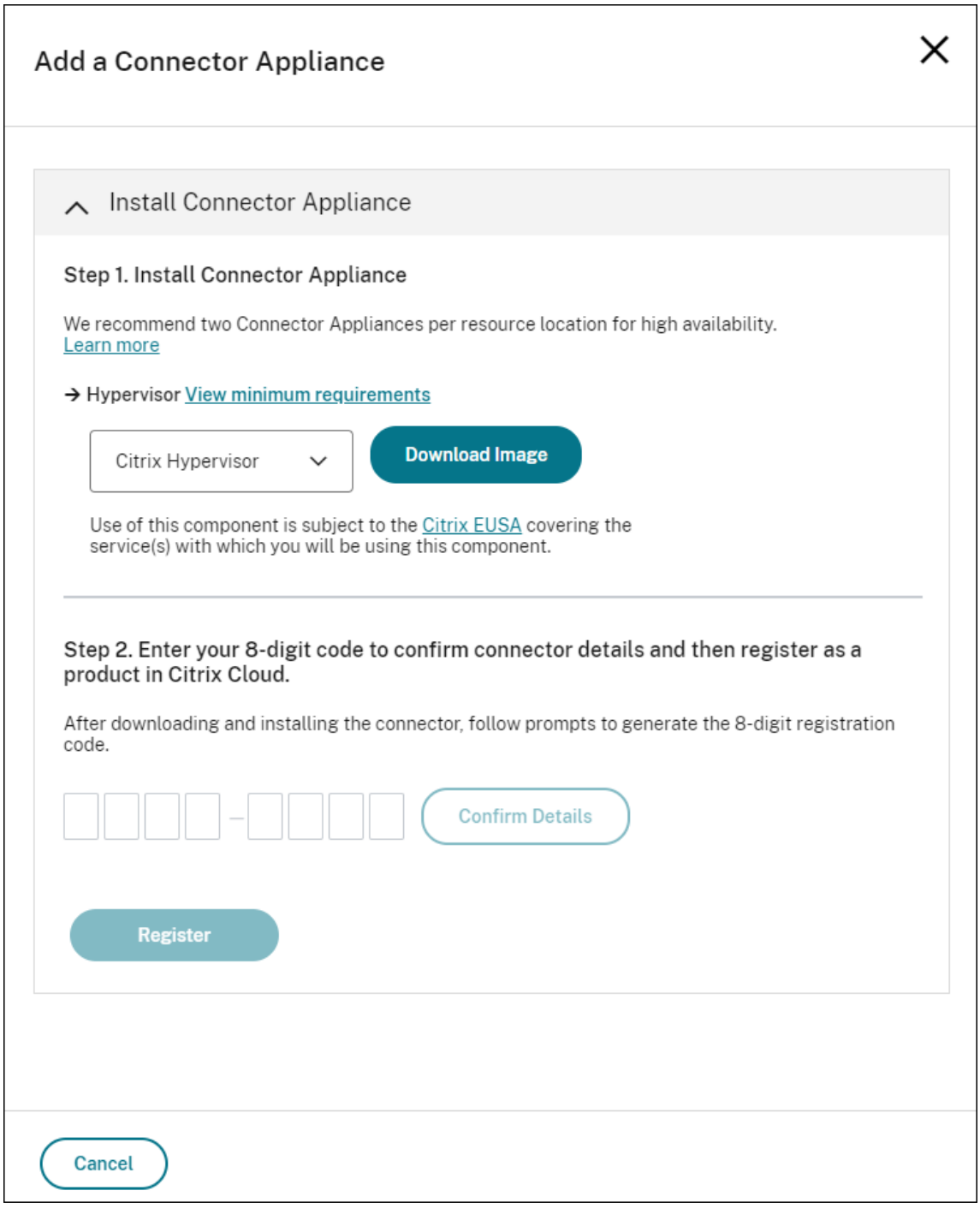
Connector Appliance の入手

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で、［リソースの場所］を選択します。
3. リソースの場所がない場合は、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する］を選択します。
4. Connector Appliance を登録するリソースの場所で、［**Connector Appliance**］プラスアイコン（+）をクリックします。

［**Connector Appliance** を追加する］タスクが開きます。



5. ［手順 **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タイプを選択します。

   - オンプレミスのハイパーバイザーとクラウド環境の場合、Connector Appliance は Citrix Cloud からダウンロードできます：

     a) ［画像のダウンロード］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て、同意する場合は ［同意して続行する］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拡張子は、選択する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、次のマーケットプレイスから Connector Appliance を入手することができます：

     - AWS
     - Microsoft Azure
     - Google Cloud

6. ［**Connector Appliance** のインストール］タスクは開いたままにします。Connector Appliance をインストールした後、［手順 **2**］に登録コードを入力します。

［コネクタ］ページから ［**Connector Appliance** のインストール］タスクに移動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 を追加します。

ハイパーバイザーへの **Connector Appliance** のインストール

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

このセクションでは、XenCenter を使用して Citrix Hypervisor サーバーに Connector Appliance を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 の XVA ファイルにアクセスできるシステムで XenCenter を使用し、Citrix Hypervisor サーバー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 の XVA ファイルが存在す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 Citrix Hypervisor サーバーを選択します。また、Connector Appliance をホストするプールを選択することもできます。それにより、Citrix Hypervisor で適切な使用可能サーバーが選択されます。［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、新しい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］リストで、使用する Connector Appliance の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. ［インポート完了後すぐに新規 **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 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。ご使用の環境で DHCP を使用できない場合は、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たネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

VMware 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 の OVA ファイルにアクセスできるシステムで vSphere Client を使用し、ESXi ホストに接続します。
2. ［ファイル］>［**OVF** テンプレートの展開…］の順に選択します。
3. Connector Appliance の OVA ファイルが存在す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 インスタンスに対する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。Connector Appliance のこのインスタンスを、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す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 に使用する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 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。
9. ［展開後に電源を入れる］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 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。ご使用の環境で DHCP を使用できない場合は、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。詳しくは、「Connector Appliance コンソールを使用したネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Hyper-V

このセクションでは、Hyper-V ホストで Connector Appliance を展開する方法について説明します。Hyper-V マネージャーまたは付属の PowerShell スクリプトを使用して仮想マシンを展開できます。

Hyper-V マネージャーを使用した **Connector Appliance** の展開

1. Hyper-V ホストに接続します。
2. Connector Appliance の ZIP ファイルを Hyper-V ホストにコピーするかダウンロードします。
3. ZIP ファイルの内容を展開します。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 ディスクを保持する場所にコピーします。例：`C:\ConnectorApplianceVMs`。
5. Hyper-V マネージャーを開きます。
6. サーバー名で右クリックして ［新規］**>**［仮想マシン］を選択します。
7. 仮想マシンの新規作成ウィザードの ［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) 4GB の RAM を割り当てる。
    b) 動的メモリを無効にする。
10. ［ネットワークの構成］パネルで一覧からスイッチ（Default Switch など）を選択します。［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 ファイルの場所を参照して、ファイルを選択します。［次へ］をクリックします。
13. ［要約］パネルで選択した値を確認し、［完了］をクリックして仮想マシンを作成します。
14. ［仮想マシン］パネルで Connector Appliance VM を右クリックして、［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］を選択して次のアクションを実行します：

    a) ［仮想プロセッサの数］の値を **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］パネルで作成した Connector Appliance VM を右クリックして、［開始］を選択します。
17. Connector Appliance VM を右クリックして ［接続］を選択してコンソールを開きます。

Connector Appliance が展開されて正常に起動した後、Hyper-V マネージャーを使用してコンソールに接続します。コンソールのランディングページに Connector Appliance の IP アドレスが表示されます。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。

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。ご使用の環境で DHCP を使用できない場合は、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。詳しくは、「Connector Appliance コンソールを使用したネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した **Connector Appliance** の展開　connector-appliance.zip ファイルには、新しい仮想マシンを作成して起動する PowerShell スクリプトが含まれています。

> 注：
>
> この無署名の PowerShell スクリプトを実行する場合、Hyper-V システムでの実行ポリシーの変更が必要な場合があります。詳しくは、https://go.microsoft.com/fwlink/?LinkID=135170を参照してください。また、提供されたスクリプトは独自のローカルスクリプトを作成するか修正するためのベースにも使用できます。

1. Hyper-V ホストに接続します。
2. Connector Appliance の ZIP ファイルを Hyper-V ホストにコピーするかダウンロードします。
3. ZIP ファイルのコンテンツを抽出：PowerShell スクリプトおよび VHDX ファイル。
4. PowerShell コンソールで ZIP ファイルのコンテンツが保存される現在のディレクトリを変更して、次のコマンドを実行します：

```
.\connector-appliance-install.ps1
<!--NeedCopy-->
```


5. プロンプトが表示されたら、仮想マシンの名前を入力するか、**Enter** キーを選択してデフォルト値「**Connector Appliance**」を使用します。
6. プロンプトが表示されたら、ルートディスク用の場所を入力するか、Enter キーを押してシステムのデフォルトの VHD 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** キーを選択して connector-appliance.vhdx のデフォルト値を使用します。
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** キーを選択します。
9. 仮想マシンのインポート情報の概要を表示します。情報が正しければ、**Enter** キーを押して続行します。スクリプトが Connector Appliance VM を作成し、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。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Nutanix 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格納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**] タブを選択して、[**+ 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**] 一覧で、[**DISK**] を選択します。
   e) [**Storage Container**] 一覧で、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**] をクリックして、ローカルシステムの`connector-appliance.vhdx`ファイルに移動します。
   h) [保存] 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**] を作成して、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. [**Create VM**] で、次の情報を指定します:
    - VM（仮想マシン）名
    - vCPU（仮想 CPU）の数
    - メモリ量（GiB）
11. [**Legacy BIOS**] を使用することを選択します。
12. [**+ Add New Disk**] をクリックして、VM にディスクを追加します。
13. [**Add Disk**] で、次の情報を入力します:
    a) [**Type**] で [**DISK**] を選択します。
    b) [**Operation**] で [**Clone from Image Service**] を選択します。
    c) [**Bus Type**] で [**SCSI**] を選択します。
    d) [**Image**] で、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. [**Add**] をクリックして、ディスクの追加を完了します。
15. [**Create VM**] で [**+ Add New NIC**] をクリックします。
16. [**Create NIC**] で、VM を追加するネットワークを選択します。
17. [**Network Connection State**] で [**Connected**] を選択します。
18. [**Add**] をクリックして、NIC の追加を完了します。
19. [**Save**] 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 の電源はオフになっています。
20. [**VM**] ビューで VM を選択し、[**Power on**] 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、正常に起動すると、次のいずれかの場所で Connector Appliance の IP アドレスを確認できます:

- Nutanix Prism Web コンソールの [**VM**] ビュー。
- Connector Appliance コンソール内。

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。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Microsoft Azure

このセクションでは、Microsoft Azure で Connector Appliance を展開する方法について説明します。組み込みの PowerShell スクリプトを使用して、Azure Marketplace またはダウンロードしたディスクイメージから Connector Appliance を展開できます。

Azure Marketplace から **Connector Appliance** を展開する　Azure Marketplace から Connector Appliance を展開するには、次の手順を実行します：

1. Azure Marketplace にある Connector Appliance に移動する（Azure Marketplace）。

   または、Marketplace 検索で「Connector Appliance for Cloud Services」を検索して移動することもできます。

2. ［**Get It Now**］、［**Create**］の順にクリックします。
3. クラウドサービス用の **Citrix Connector Appliance** の作成ページで、次の情報を入力します：

   - 使用する ［**Subscription**］を選択します。
   - 使用する ［**Resource group**］を選択します。
   - Connector Appliance を配置する ［**Region**］を選択します。
   - ［**VM name**］を指定します。
   - Connector Appliance を追加する ［**Virtual network**］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、Connector Appliance の管理ページにアクセスするために使用されます。このネットワークは後で変更できません。
   - ［**Subnet**］の値を指定します。

   ［**Next : Tags >**］をクリックします。

4. ［**Tags**］タブで、必要に応じて必要なタグを追加します。

   ［**Next : Review + create >**］をクリックします。

5. 環境の詳細を確認したら、［**Create**］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。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した Connector Appliance VM の展開 `connector-appliance-azure.zip`ファイルには、新しい仮想マシンを作成して起動する PowerShell スクリプトが含まれています。提供されているスクリプトは、独自のローカルスクリプトを作成したり修正したりするためのベースとして使用できます。

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:

- Az PowerShell モジュールをローカルの PowerShell 環境にインストールしてある。
- VHD ファイルが配置されているディレクトリで PowerShell スクリプトを実行する。

次の手順を実行します:

1. Connector Appliance の ZIP ファイルを Windows システムにコピーするかダウンロードします。
2. ZIP ファイルのコンテンツを抽出: PowerShell スクリプトと VHD ファイル。
3. 管理者として PowerShell コンソールを開きます。
4. ZIP ファイルのコンテンツが保存される現在のディレクトリを変更して、次のコマンドを実行します:

```
.\connector-appliance-upload-Azure.ps1
```

5. ダイアログボックスが表示され、Microsoft Azure にログインするよう求められます。資格情報を入力してください。
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、イメージをアップロードし、仮想マシンを作成します。
8. 最初の VM を作成した後、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られます。
    - 「y」と入力して、別の VM を作成します。
    - 「n」と入力して、スクリプトを終了します。

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。

次の手順: Connector Appliance を Citrix Cloud に登録する。

AWS

このセクションでは、AWS で 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 として入手できます。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、組み込みの 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できます。

ネットワークの前提条件　Connector Appliance を AWS に展開するには、Connector Appliance が作成されたサブネットから 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、**AWS** マネジメントコンソールで次の手順を実行します:

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) 右上の [**Create NAT Gateway**] をクリックします。次の情報を入力します:
        - [**Name**] に入力します。
        - 一覧からサブネットを選択します。
        - [**Connectivity type**] を [**Public**] を設定します。
        - 一覧から [**Elastic IP allocation ID**] を選択します。使用できる 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) [**Create NAT Gateway**] 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) 右上の [**Create route table**] をクリックします。次の情報を入力します:
        - [**Name**] に入力します。
        - 一覧から、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) [**Create route table**] をクリックします。
    d) 作成したルートテーブルの [**Routes**] タブで、[**Edit routes**] **>** [**Add route**] をクリックします。
    e) 新しいルートエントリの [**Destination**] と [**Target**] に入力します。
        - Destination（接続先）を「0.0.0.0/0」に設定します。
        - Target（ターゲット）については、作成した [**NAT Gateway**] を一覧から選択します。
    f) [**Save change**] 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接続します。
    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) 表示されたページで、[**Subnet Associations**] タブに移動します。
    d) [**Edit subnet associations**] をクリックします。
    e) ルートテーブルに接続する 1 つまたは複数のサブネットを選択します。
    f) [**Save Associations**] をクリックします。

AWS Marketplace から **Connector Appliance** を展開する　開始前に、以下の前提条件を満たしていることを確認します:

- EC2 リソースを操作する権限がある。
- 「ネットワークの前提条件」で構成を完了してある。
- （オプション）Connector Appliance にアクセスできる 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** マネジメントコンソールにログインします。
2. AWS Marketplace で Connector Appliance AMI を見つけます。これは次のいずれかの方法で実行できます:
   - Citrix Cloud に表示される Marketplace リンクに従います（AWS Marketplace）。
   - AWS マネジメントコンソールで AMI を検索する:
     a) [**Services**] **>** [**Compute**] **>** [**EC2**] **>** [**AMIs**] に移動します。
     b) リージョン（米国東部（オハイオ））を確認します。
     c) [**Public images**] で、「Citrix Connector Appliance」、または AMI ID の「ami-026eaf9b3b232577f」を検索します。
3. AMI ID（ami-026eaf9b3b232577f）と所有者 ID（414337923189）をチェックして、正しい AMI であることを確認します。
4. AMI を自分のサブスクリプションにコピーします:
   a) [**Actions**] **>** [**Copy AMI**] に移動します。
   b) [**Copy AMI**] ダイアログボックスで、必要な [**Destination Region**] を選択できます。
   c) [**Copy AMI**] をクリックします。
5. コピーした AMI の概要ページで、[**Launch instance from AMI**] をクリックします。
6. [**Launch an instance**] ダイアログボックスで、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。回復性のために、各リソースの場所に 2 つ以上の Connector Appliance を用意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) [**Instance type**] で、[**t2.medium**] を選択します。この種類のインスタンスには、少なくとも 4GB と 2 つの CPU が必要です。
   d) [**Key pair (login)**] で、[**Proceed without a key pair**] を選択します。Connector Appliance への SSH ログインは許可されないため、キーペアは必要ありません。
   e) [**Network settings**] の [**Firewall (security group)**] セクションで、次の設定を構成します:
      i. [**Create security group**] または [**Select existing security group**] を選択します。

ii. [**Allow SSH traffic from the internet**] の選択を解除します。
iii. [**Allow HTTPs traffic from the internet**] を選択します。
iv. [**Allow HTTP traffic from the internet**] を選択します。

[**Launch instance**] をクリックします。

7. インスタンスが作成されたら、[**Success**] セクションでインスタンス ID リンクをクリックして、Connector Appliance のインスタンスを表示します。

   または、このページの [**View All Instances**] ボタンをクリックするか、AWS マネジメントコンソールの [**Services**] > [**EC2**] > [**Instances**] に移動して、インスタンス一覧を表示します。

8. [**Instance state**] を [**Running**] に変更したらインスタンスの詳細ページに移動し、[**Private IPv4 address**] 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。

踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了する必要がある場合もあります。

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 Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

AWS UI を使用した **Connector Appliance** の展開　開始前に、以下の前提条件を満たしていることを確認します：

- S3 リソースと EC2 リソースを操作する権限がある。
- VM インポートアクセス権限があるサービス役割とポリシーを作成してある。詳しくは、https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-roleを参照してください。

  > 注：
  >
  > サービス役割を作成するには、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ときに、VM インポートアクセスで作成した S3 バケットを設定します。

- AWS CloudShell へのアクセス権限がある。これは、特定のリージョンでのみご利用いただけます。AWS CloudShell がサポートされているリージョンの一覧については、「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」で構成を完了してある。

次の手順を実行します：

1. ローカルシステムで、`connector-appliance-aws.zip`のコンテンツを抽出します。

2. **AWS** マネジメントコンソールにログインします。
3. 次の手順を実行して、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することはできません。
   d) 残りの設定を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**] をクリックしてから、`connector-appliance.vhd`ファイルを選択します。残りの設定を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て、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="<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"`。

      このコマンドは、`"Status": "completed"`を含む JSON 文字列を以下のコマンドが返すときに完了します。JSON 出力の`ImportTaskId`値をメモします。
   b) 次のコマンドを実行します:

      ```
      aws ec2 describe-import-snapshot-tasks --import-task-ids <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** マネジメントコンソール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て、[**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。

［作成］をクリックします。

11. 画面左側のメニューから、［**AMI**］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) インスタンスの種類を選択します。
b)（オプション）［**Configure Instance**］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）［**Add Storage**］タブで別のボリュームを接続します。
d) ［**Configure Security Group**］タブでセキュリティグループ規則を設定します。

インスタンスの起動を確認したら、［**Review and Launch**］をクリックします。

Connector Appliance が展開され、正常に起動したら、［**Services**］> ［**EC2**］> ［**Instances**］に移動し、作成したインスタンスを選択します。［**Private IPv4 address**］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。踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、インストールプロセスを続行する必要がある場合もあります。

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 Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した Connector Appliance の展開　`connector-appliance-aws.zip`ファイルには、新しい仮想マシン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。詳しくは、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限があるサービス役割とポリシーを作成してある。この PowerShell スクリプトを機能させるには、サービス役割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。詳しくは、https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-roleを参照してください。

> 注：
>
> サービス役割を作成するには、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ときに、VM インポートアクセスで作成した S3 バケットを設定します。

- Amazon EC2 セキュリティグループを作成してある。
- S3 権限と API アクセス権がある。
- 「ネットワークの前提条件」で構成を完了してある。

次の手順を実行します:

1. ローカルシステムで、connector-appliance-aws.zipのコンテンツ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、次のコマンドを実行して、AWS SDK ストアに新しいプロファイルを追加します:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   プレースホルダーの値をアクセスキーと秘密キーに置き換えます。一意のプロファイル名を入力します。入力例は、「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、抽出したファイルが保存されているフォルダーに変更して、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 展開用のリージョンを選択し、選択したバケットにイメージをアップロードして、VM の名前を入力します。

   - 以前に作成した VM インポートアクセスで、バケットを使用する必要があります。
   - 使用する VPC を選択するように求められたら、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に求められたら、NAT ゲートウェイを含むルートテーブルに接続されているサブネットを選択します。

   詳しくは、「ネットワークの前提条件」を参照してください。

Connector Appliance が展開され、正常に起動すると、スクリプトにより Connector Appliance のプライベート IP アドレスが表示されます。踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了する必要がある場合もあります。

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 Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順: Connector Appliance を Citrix Cloud に登録する。

Google Cloud Platform

このセクションでは、Google Cloud Platform で 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、Google Cloud Platform コンソールを使用するか、組み込みの 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できます。

`connector-appliance-gcp.zip`ファイルには、以下が含まれています:

- `connector-appliance.tar.gz`: Connector Appliance のディスクイメージ。
- `connector-appliance-upload-gcp.ps1`: 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。

Google Cloud Marketplace から **Connector Appliance** を展開する

1. Google アカウントにログインします。
2. Citrix Cloud に表示される Marketplace リンクに従います（Google Cloud Marketplace）。

   または、Marketplace 検索で「Connector Appliance for Cloud Services」を検索して移動することもできます。
3. ［起動］をクリックします。
4. クラウドサービス用の新しい **Citrix Connector Appliance** 展開のページで、次の情報を入力します:

   - 展開ジョブの ［展開名］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］、［シリーズ］、［マシンの種類］を選択します。
   - ［起動ディスクの種類］と ［起動ディスクのサイズ（**GB**）］を選択します。
   - ［ネットワーク］セクションで、Connector Appliance で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には、［外部 **IP**］を指定します。

   ［展開］をクリックします。［**Deployment Manager**］ページが開きます。

   > 注:
   >
   > Connector Appliance が展開され、正常に起動すると、Connector Appliance が Google Cloud Platform に展開されている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設定時に ［外部 **IP**］を指定したことがある場合は、［詳細］タブの ［ネットワークインターフェイス］セクションの ［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 管理ページに接続し、登録プロセスを完了します。また

は、［プライマリ内部 **IP** アドレス］を使用して、Connector Appliance と同じサブネット内の別のマシンから Connector Appliance 管理ページにアクセスすることもできます。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Google Cloud Platform コンソールを使用した **Connector Appliance** の展開

1. ローカルシステムで、`connector-appliance-gcp.zip`のコンテンツを抽出します。
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（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、［**Create bucket**］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いても構いません。
   e) ［作成］をクリックします。
3. ストレージバケット内で、［**Upload files**］を選択し、`connector-appliance.tar.gz`ファイルを選択します。ファイルがアップロードされるまで待ちます。
4. アップロードされたファイルを選択して、その詳細を表示します。クリップボードに ［**gsutil URI**］の値をコピーします。
5. ヘッダーバーの ［**Activate Cloud Shell**］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 Instances**］を選択します。
8. ［**Create Instance**］を選択します。開いたペインで、次の情報を指定します：
   a) ［**Name**］フィールドに、Connector Appliance インスタンスの名前を入力します。
   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) ［**Boot disk**］セクションで、［**Change**］をクリックします。
   e) 開いたセクションで、［**Custom images**］タブに移動します。
   f) ［**Image**］一覧から、作成したイメージを選択します。
   g) ［**Select**］をクリックします。
   h) ［**Firewall**］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) 必要な追加の構成を指定します。たとえば、デフォルトのネットワーク構成を使用したくない場合などです。

［作成］をクリックします。

9. ［**VM Instances**］セクションで、新しく作成した VM を選択して、その詳細を表示します。

Connector Appliance が展開され、正常に起動すると、［**VM Instances**］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は、この IP アドレスを使用して、Web ブラウザーから Connector Appliance 管理ページに移動し、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、Web ブラウザーから Connector Appliance 管理ページに移動し、登録プロセスを完了します。詳しくは、https://cloud.google.com/compute/docs/connect/ssh-using-bastion-hostを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した **Connector Appliance** の展開　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`のコンテンツをフォルダーに抽出します。
2. PowerShell で、抽出したファイルが配置されているこのフォルダー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 Web ブラウザーのウィンドウで、Connector Appliance の展開先であるプロジェクトへのアクセス権限があるアカウントを使用して、Google Cloud SDK で認証します。
5. Google Cloud Tools for PowerShell で、PowerShell スクリプトの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、ディスクをアップロードし、イメージを作成して、仮想マシンを作成します。
7. 最初の VM を作成した後、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られます。
   - 「`y`」と入力して、別の VM を作成します。
   - 「`n`」と入力して、スクリプトを終了します。

Connector Appliance が展開され、正常に起動すると、スクリプトにより Connector Appliance の内部 IP アドレスが表示されます。または、Google Cloud Platform コンソールで、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**］セクションには、Connector Appliance の IP アドレスが表示されます。

踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了します。詳しくは、https://cloud.google.com/compute/docs/connect/ssh-using-bastion-hostを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Connector Appliance を Citrix Cloud に登録する

Citrix Cloud とリソースの場所の間の通信チャネルを提供するため、Connector Appliance を Citrix Cloud に登録します。

Connector Appliance をハイパーバイザーに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 Web ブラウザー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://`を追加す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。その結果、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 への接続を確認するには、コンソールの SSL フィンガープリントを、ブラウザーが Web ページから受信したフィンガープリントと比較します。

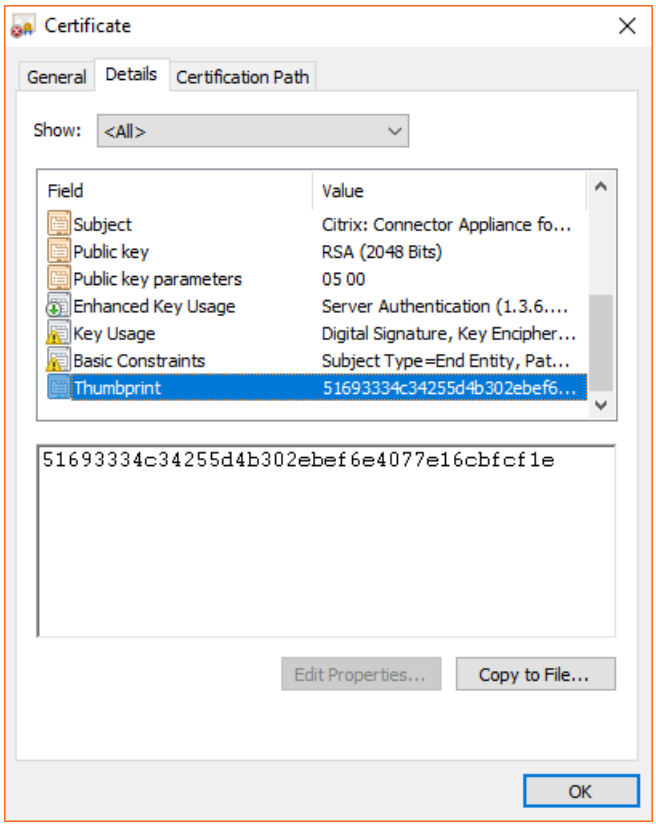
   たとえば、Google Chrome ブラウザーで、以下の手順を実行します：

   a) アドレスバーの横にある保護されていない通信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、拇印フィールドを見つけます。

拇印フィールドの値とコンソールで提供された SSL フィンガープリントが一致する場合、ブラウザーが Connector Appliance UI に直接接続していることを確認できます。

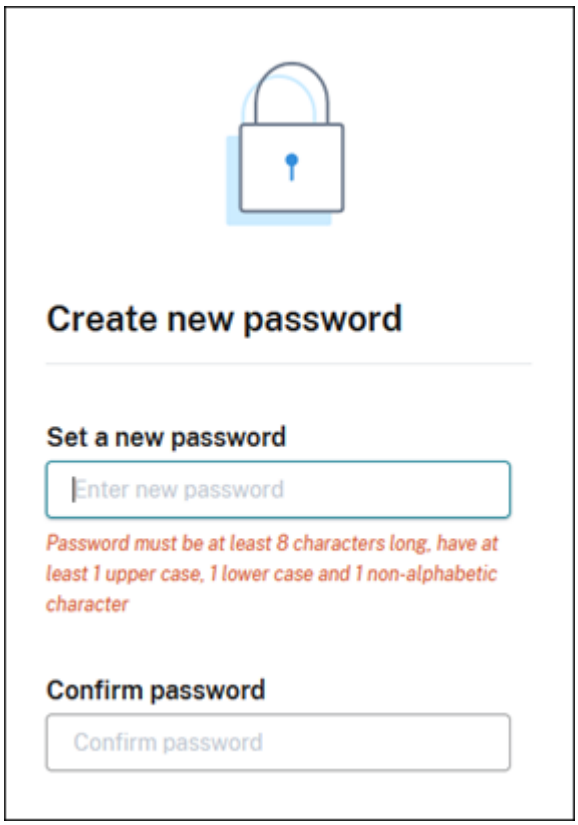


この自己署名証明書を組織によって署名された、または組織の信頼チェーンを使用して生成された独自の証明書に置き換えることができます。詳しくは、「証明書の管理」を参照してください。

2. ブラウザーがサイトへの移動を確認するために追加の手順を要求する場合は、こ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、［新しいパスワードの設定］をクリックします。

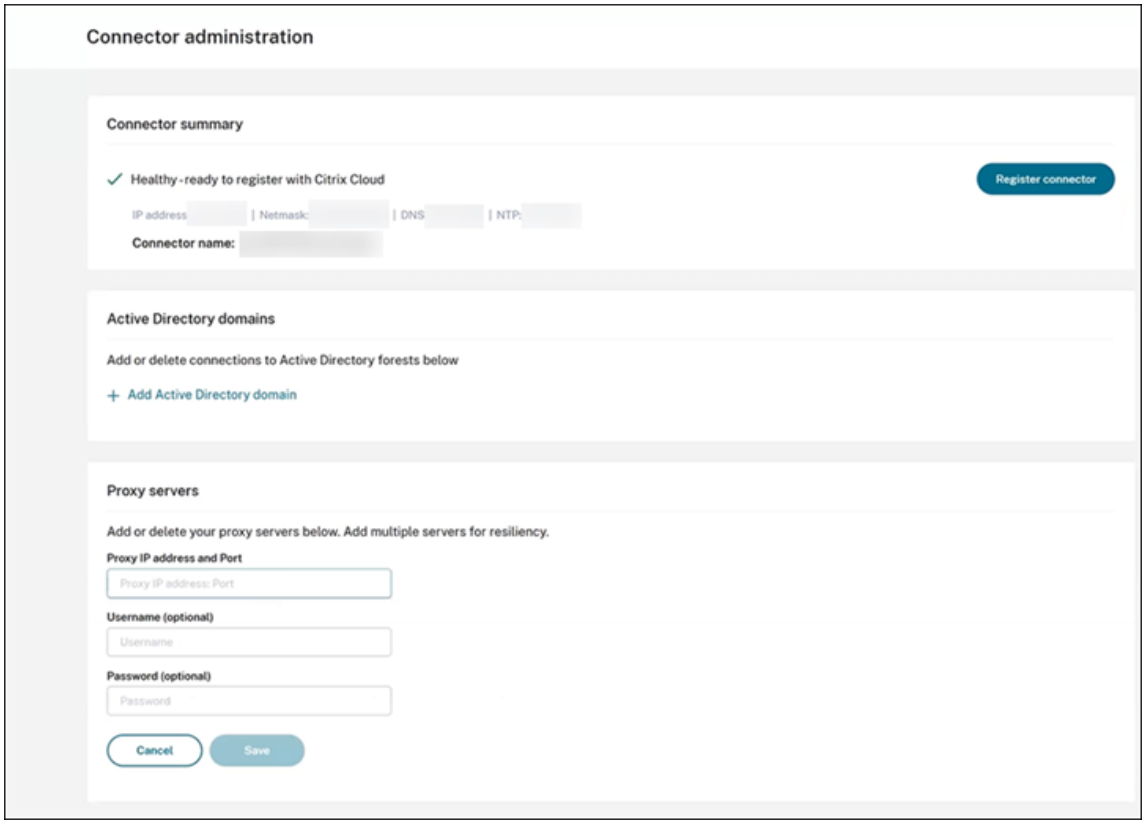


設定するパスワードは次の要件を満たしている必要があります:

- 8 文字以上
- 大文字と小文字の両方を含む
- アルファベット以外の文字を少なくとも 1 つ含む

このパスワードは、将来の使用に備えて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。［コネクタの管理］ページが開きます。



5. （オプション）1 つ以上の Web プロキシを使用する場合、［プロキシサーバー］セクションにプロキシアドレスを追加できます。認証されていないプロキシと認証されたプロキシの両方がサポートされています。認証されていない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入力します。認証された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:
   >
   > 基本的なプロキシ認証のみがサポートされています。他の形式の認証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 プロキシ経由でルーティングされます。詳しくは、「Connector Appliance の通信」を参照してください。

6. （オプション）ネットワークがインターネットにアクセスするために TLS インターセプト Web プロキシを使用している場合、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］で、［証明書を追加］を選択します。

   b) 証明書の内容を PEM 形式としてコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   <!--NeedCopy-->
   ```


c)［証明書の完全な詳細］に証明書の内容を貼り付けます。

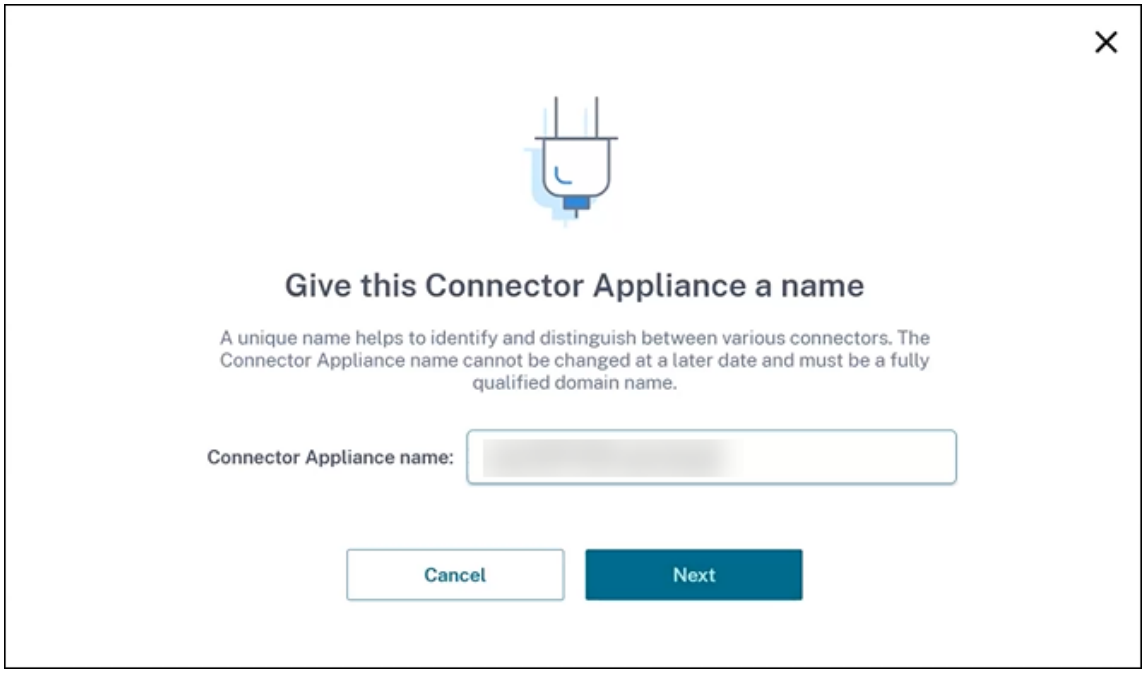
d)［証明書の追加］を選択します。

Connector Appliance API を使用してルート証明機関（RootCA）を追加するには、Citrix 開発者向けドキュメントの「Managing root certificate authorities」を参照してください。

> 注:
>
> 有効期限が切れた証明書、または今後 30 日以内に期限切れにな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、リソースの場所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 を登録した後は、名前を変更することはできません。

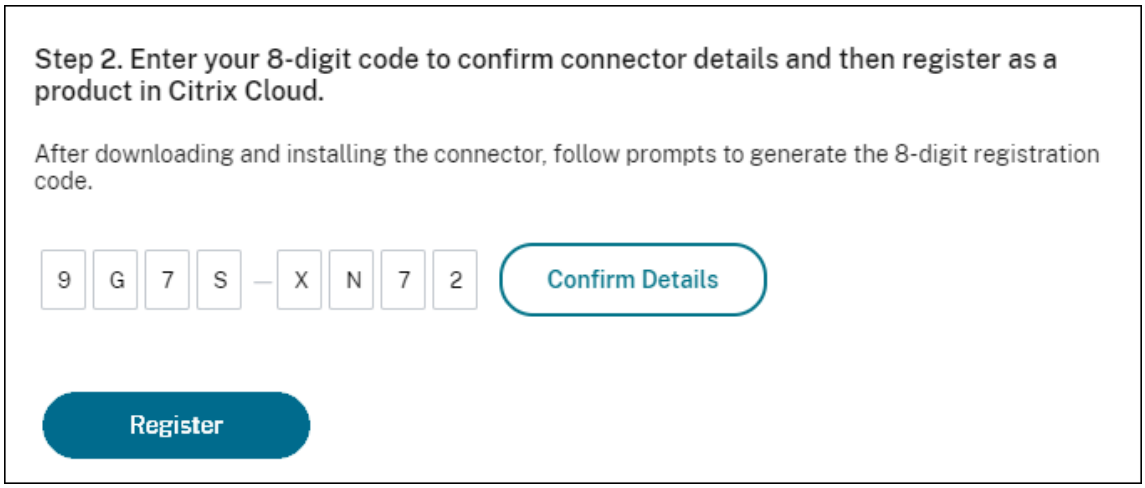
   ［**Connector Appliance** 名］フィールドに名前を入力し、［次へ］をクリックします。



   Web ページで、Citrix Cloud での登録に使用するコードが提供されます。このコードは 15 分で期限切れになります。

9. ［コピー］ボタンを使用し、コードをクリップボードにコピーします。
10. ［リソースの場所］ Web ページに戻ります。
11. ［**Connector Appliance** のインストール］タスクの ［手順 **2**］にコードを貼り付けます。［詳細を確認］をクリックします。

    Citrix Cloud で、Connector Appliance が存在し、接続でき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、新しいコードを生成するよう指示されます。



12. ［登録］をクリックします。

    このページに、登録が成功したかどうかが表示されます。登録が失敗した場合、再試行するよう指示されます。

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。詳しくは、「診断レポートの生成」を参照してください。

Connector Appliance の登録後

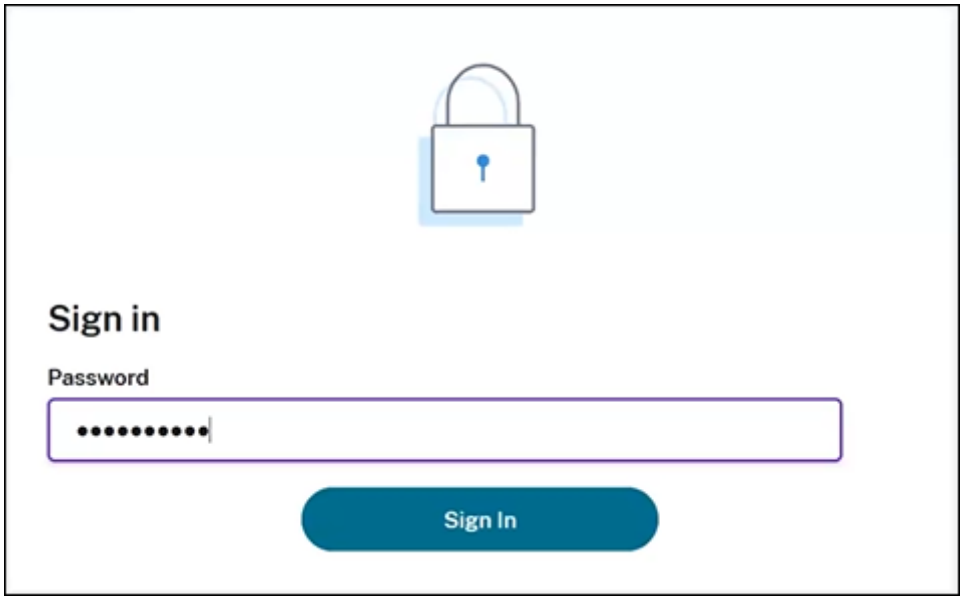
各リソースの場所で、2 つ以上の Connector Appliance をインストールして登録することをお勧めします。この構成により、継続的な可用性が確保され、コネクタ間で負荷を分散できます。

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アクションを実行する必要はありません。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。詳しくは、「コネクタの更新」を参照してください。

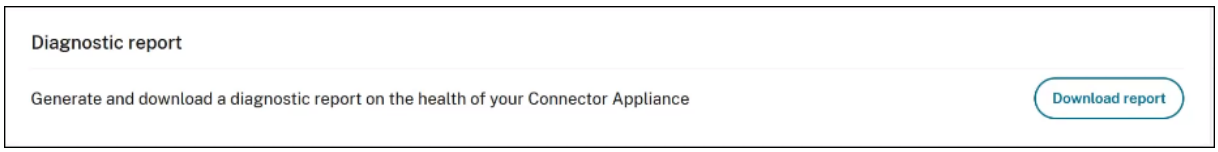
Connector Appliance VM のスナップショットを複製、一時停止、作成しないでください。これらの操作はサポートされていません。

Connector Appliance UI に初めて接続したときにのみ、［新しいパスワードの作成］ページが表示されます。このパスワードは、将来の使用に備えて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。その後の UI への接続では、Connector Appliance の登録時に設定したパスワードを入力するように求められます。



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 Web ブラウザーのアドレスバーにコピーします。
2. Connector Appliance の登録時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。

ネットワーク接続の確認

［**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** の管理ページで、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て、TCP キャプチャを制限します。
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）［パケットトレース］を有効にして、パケットの内容をキャプチャします。

   パケットトレースが無効になっている場合、TCP キャプチャ機能はベストエフォートアプローチをとり、診断用にヘッダーをキャプチャします。このベストエフォートアプローチは、各パケットの最初の 94 バイトをキャプチャします。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すべてのヘッダーをキャプチャできないことがあります。
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することができます。

   - ［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。
   - ［新しいトレースの開始］をクリックして、別のトレースを開始します。

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 の顧客や、一部のフォレストがユーザー認証にのみ使用される Citrix Virtual Apps and Desktops の顧客の場合。

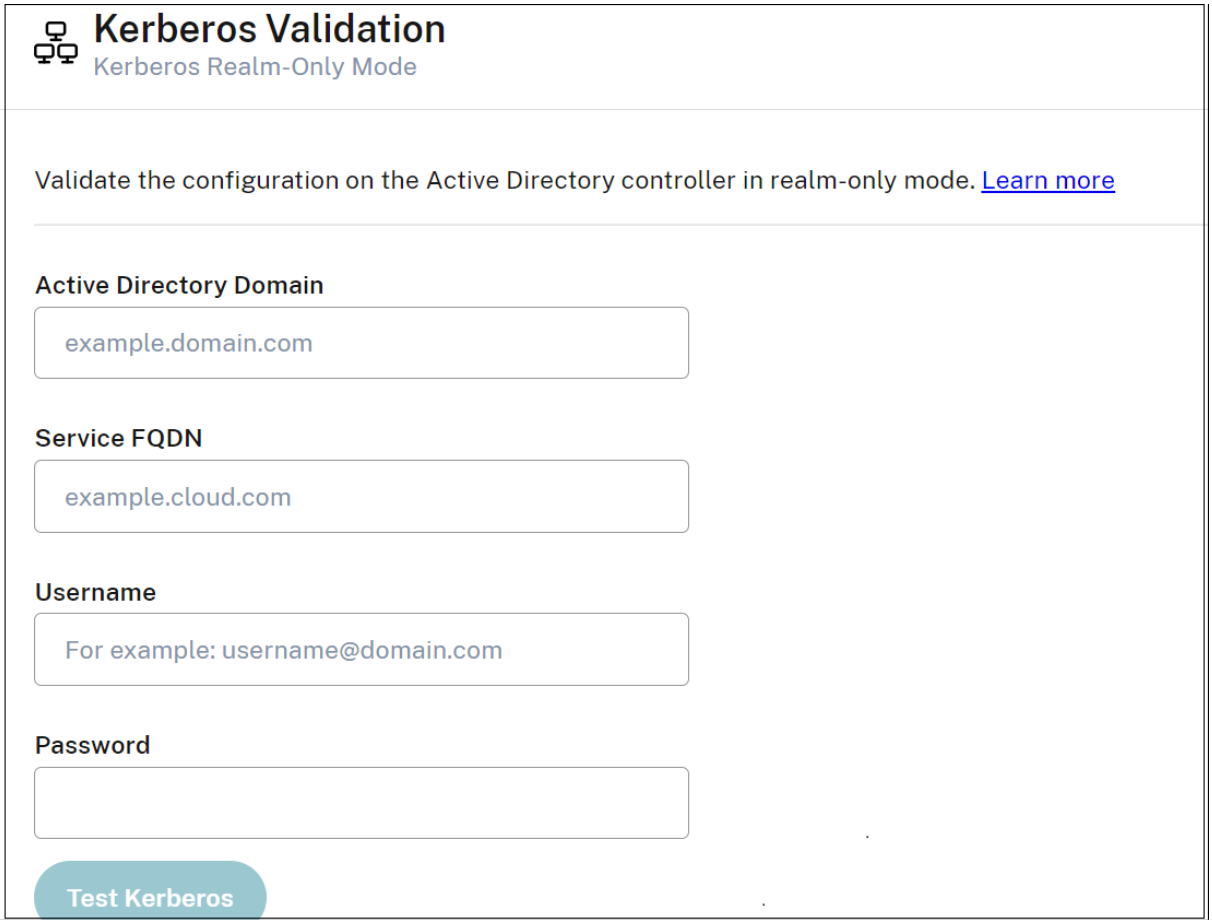
詳しくは、「Connector Appliance を使用した Active Directory」を参照してください。

Kerberos 構成の検証

シングルサインオンに Kerberos を使用する場合は、**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 領域のみモード構成または Kerberos の制約付き委任（KCD）モード構成を検証できます。

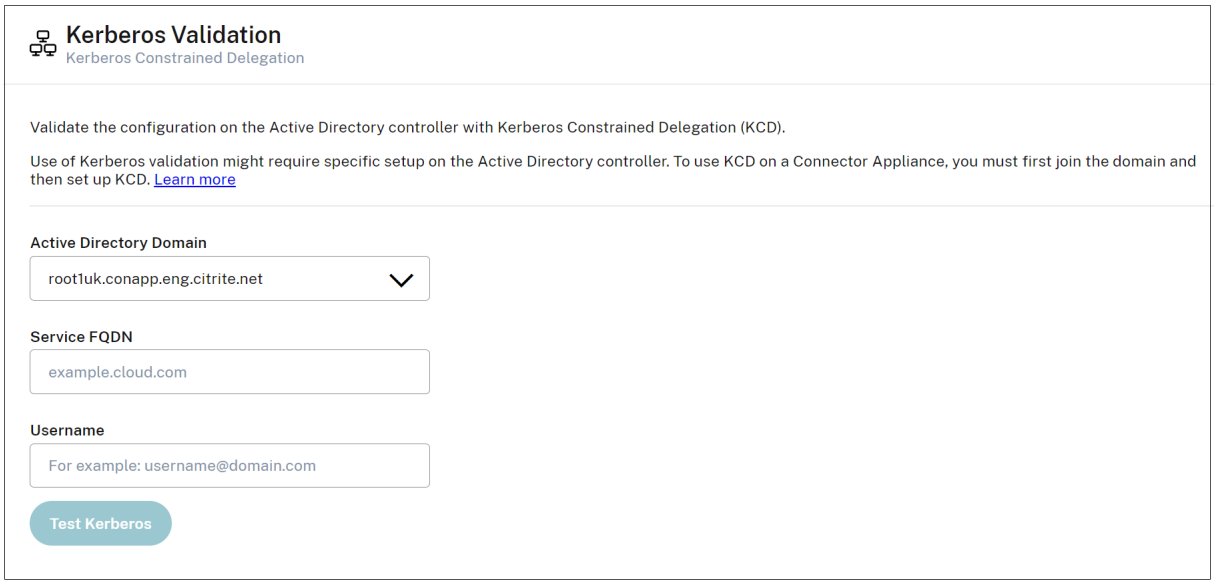
Kerberos 領域のみ構成を検証します：

1. **Connector Appliance** の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 Web ブラウザーのアドレスバーにコピーします。
3. Connector Appliance の登録時に設定したパスワードを入力します。
4. 領域のみの Kerberos 構成を検証するには、［**Active Directory** ドメイン］セクションで ［**Kerberos** 検証レルムのみ］を選択します。
5. ［**Active Directory** ドメイン］を指定します。
    - Kerberos 領域のみモード構成を検証する場合は、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」であると想定されています。「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** をテストする］をクリックします。



Kerberos の制約付き委任（**KCD**）の構成を検証します:

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の **Kerberos** 制約付き委任（**KCD**）モードを検証するには、関連するドメインの省略記号メニュー（…）から ［**Kerberos** 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、参加済みドメインの一覧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」であると想定されています。たとえば、「computer.example.com」を指定した場合、この値は「https://computer.example.com%E2%80%9D」と同じと見なされます。
5. ［ユーザー名］を指定します。
    - Kerberos 制約付き委任モードの場合は、［**Service Accounts**］タブを選択して、サービスアカウントを使用して Kerberos セットアップを検証することもできます。
6. ［**Kerberos** をテストする］をクリックします。



Kerberos の構成が正しい場合は、「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 の構成が正しくない場合は、検証がどのように失敗したかという情報を示すエラーメッセージが表示されます。

Kerberos について詳しくは、Microsoft 社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** 管理ページでネットワーク設定を編集できます。

ただし、ご使用の環境で DHCP を使用できない場合、または **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。

Connector Appliance 管理ページでのネットワーク設定の構成

DHCP を使用して Connector Appliance を登録した後、**Connector Appliance** 管理ページ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. ［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］ダイアログボックスで、［独自のネットワーク設定を構成する］を選択します。
3. **IP** アドレス、サブネットマスク、デフォルトゲートウェイを入力します。
4. 1 つまたは複数の **DNS** サーバーを追加します。

5. 1 つまたは複数の **NTP** サーバーを追加します。
6. ［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、Connector Appliance は一時的に使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 コンソール内で、またはハイパーバイザーでネットワーク情報を確認することで、見つけることができます。

自動的に割り当てられた値を使用するよう、ネットワーク構成を変更するには:

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］ダイアログボックスで、［**IP** アドレスを自動的に取得する］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、Connector Appliance は一時的に使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 コンソール内で、またはハイパーバイザーでネットワーク情報を確認することで、見つけることができます。

Connector Appliance コンソールを使用したネットワーク構成の設定

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。ただし、ご使用の環境で DHCP を使用できない場合、または **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!`」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。

   次の画像のようなビューが表示されます:

5. 「linux」で始まる行を編集して、必要なネットワーク構成を設定します。

   - DHCP ネットワークを指定するには、行末に「network=dhcp」を追加します。
   - 静的ネットワークを指定するには、行の最後に次のパラメーターを追加します:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     <!--NeedCopy-->
     ```

     プレースホルダーの値を構成の値に置き換えます。

6. **Ctrl+X** キーを押して、新しい構成で Connector Appliance を起動します。

Connector Appliance の管理者ユーザーパスワードの変更

1. コンソールの右上にあるユーザーメニューから、［パスワードの変更］を選択します。

   ［パスワードの変更］ページが表示されます。

2. 現在のパスワードを入力してから、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している必要があります:

   - 8 文字以上
   - 大文字と小文字の両方を含む
   - アルファベット以外の文字を少なくとも 1 つ含む
   - 現在のパスワードと同じものにしない

3. ［パスワードの変更］を選択して変更を保存します。

Citrix Cloud から自動的にサインアウトされ、サインインページにリダイレクトされます。

Connector Appliance を使用した Active Directory

April 5, 2024

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 の顧客や、一部のフォレストがユーザー認証にのみ使用される Citrix Virtual Apps and Desktops の顧客の場合。

Connector Appliance を使用したマルチドメイン Active Directory の場合、次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

- ユーザー用のオファリング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 ドメインに参加済み。詳しくは、「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 フォレストには、常に 2 つの Connector Appliance がアクセスできるようにする必要があります。
- 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のドメインコントローラーにアクセスできる必要があります。詳しくは、次の Microsoft のサポート文書を参照してください:
  - ドメインと信頼を構成する方法
  - 「Windows のサービス概要および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、ユーザーグループのメンバーシップをフォレスト内の任意のドメインコントローラーから確実に取得できます。

ネットワークの要件

- 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済み。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。

「Connector Appliance の通信」に記載されているポートに加えて、Connector Appliance には、次のポートを介して Active Directory ドメインに送信接続する必要があります:

サービス	ポート	サポートされるドメインプロトコル
kerberos	88	TCP/UDP
エンドポイントマッパー (DCE/RPC ロケーターサービス)	135	TCP
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
SMB over TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
グローバルカタログ	3268	TCP
動的 RPC ポート	49152～65535	TCP

Connector Appliance 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セキュリティで保護します。つまり、SSL 経由の LDAP（LDAPS）は必要ありません。LDAP 署名について詳しくは、「Windows Server で 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マイクロソフトガイダンス」を参照してください。

サポートされる **Active Directory** の機能レベル

Connector Appliance はテスト済みで、Active Directory のフォレストとドメインの以下の機能レベルでサポートされます。

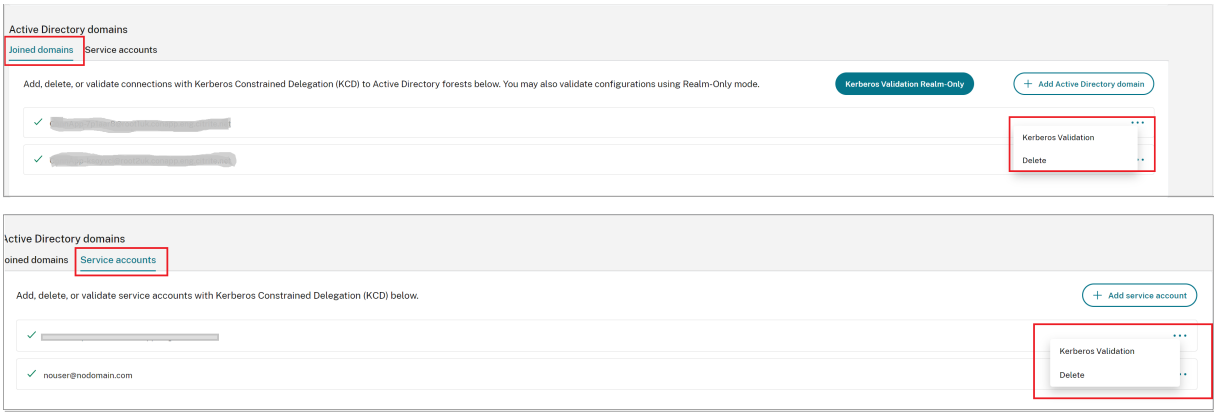
フォレスト機能レベル	ドメイン機能レベル	サポートされるドメインコントローラー
Windows Server 2016	Windows Server 2016	Windows Server 2019

ドメインコントローラ、フォレスト機能レベル、およびドメインの機能レベルの他の組み合わせは、Connector Appliance 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正常に動作することが期待されており、サポートされています。

Connector Appliance を使用して **Active Directory** ドメインを **Citrix Cloud** に接続する

Connector Appliance 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。

- **Joined Domains** –Connector Appliance を AD ドメインに参加させるために使用され、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します。Kerberos を検証するには、参加したドメインの右側にある省略記号メニューをクリックします。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。
- **Service Accounts** –Secure Private Access（SPA）ソリューションの一部として使用され、ドメインに参加することで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 を検証するには、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します。特定のドメインをマシンに関連付けることは必須ではありません。ただし、Connector Appliance 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 Citrix Cloud に接続するように Active Directory を構成するには、次の手順を実行します。

1. Connector Appliance をリソースの場所にインストールします。

   Connector Appliance の製品ドキュメントの情報を参照できます。

2. Connector Appliance コンソールで提供される IP アドレスを使用して、Web ブラウザーで Connector Appliance の管理 Web ページに接続します。
3. [**Active Directory** ドメイン] セクションで、[**Joined domains**] 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。

   Connector Appliance はドメインをチェックします。チェックで問題がなければ、[**Active Directory** に参加] ダイアログボックスが開きます。この新しいウィンドウでは、ドメインに参加するためのユーザー名とパスワードを入力できます。

5. [追加] をクリックします。
6. ドメインへの参加権限を持つ Active Directory ユーザーのユーザー名とパスワードを入力します。

7. Connector Appliance からマシン名が提案されます。提案された名前を上書きして、独自のマシン名（最大 15 文字）を指定することもできます。

   このマシン名は、Connector Appliance が参加したときに Active Directory ドメインに作成されます。

8. ［参加］をクリックします。

   これで、Connector Appliance のユーザーインターフェイス ［**Active Directory** ドメイン］セクションにドメインが一覧表示されます。

9. **Active Directory** ドメインをさらに追加するには、［**+ Active Directory** ドメインの追加］を選択して、上記の手順を繰り返します。

10. **Citrix Cloud** コンソールのドメインページに移動し、ドメインにサービスを提供する ［**Connector Appliance**］を選択します。

11. Connector Appliance をまだ登録していない場合は、「Connector Appliance を Citrix Cloud に登録する」で説明されている手順を続行します。

ドメインへの参加時にエラーが発生した場合は、お使いの環境が Active Directory の要件とネットワークの要件を満たしていることを確認してください。

次の操作

- この Connector Appliance には、さらにドメインを追加できます。

  > 注:
  >
  > Connector Appliance は最大 10 個のフォレストでテストされています。

- 耐障害性を向上させるため、各ドメインを各リソースの場所にある複数の Connector Appliance に追加します。

Active Directory 構成を表示する

リソースの場所の 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:

  1. メニューで、［**ID** およびアクセス管理］ページに移動します。
  2. ［ドメイン］タブに移動します。

     Active Directory ドメインは、そのドメインが属してい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:

1. Connector Appliance コンソールで提供される IP アドレスを使用して、Connector Appliance の Web ページに接続します。
2. 初回登録時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］セクションには、この Connector Appliance が参加している Active Directory ドメインの一覧が表示されます。

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 コンソールで提供される IP アドレスを使用して、Connector Appliance の Web ページに接続します。
2. 初回登録時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］セクションにある、参加している Active Directory ドメインの一覧で、離脱するドメインを探します。
4. Connector Appliance によって作成されたマシンアカウントの名前を記録します。
5. ドメインの横にある削除アイコン（ごみ箱）をクリックします。確認ダイアログボックスが開きます。
6. ［続行］をクリックして、その操作を確認します。
7. Active Directory コントローラに移動します。
8. Connector Appliance によって作成されたマシンアカウントをコントローラから削除します。

Active Directory で **Connector Appliance** を使用した展開シナリオ

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種類は、展開によって異なります。

Active Directory での Cloud Connector の使用について詳しくは、「Active Directory での Cloud Connector 展開シナリオ」を参照してください。

次の状況では、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 を設定している。詳しくは、「Connector Appliance を使用した Secure Private Access」を参照してください。
- ユーザー認証にのみ使用されるフォレストが 1 つ以上ある
- 複数のフォレストのサポートに必要なコネクタ数の削減を希望している
- 他のユースケースに Connector Appliance を必要としている

1 つ以上のフォレストにユーザーのみが存在する場合に、すべてのフォレストに対して **1** セットの **Connector Appliance** を展開

このシナリオは、Workspace Standard の顧客、または Secure Private Access のために Connector Appliance を使用する顧客に適用されます。

このシナリオでは、ユーザーオブジェクト（forest1.local、forest2.local）のみを含むフォレストがいくつかあります。これらのフォレストにはリソースは含まれていません。単一の Connector Appliance セットがリソースの場所に展開され、各フォレストのドメインに参加します。

- 信頼関係：なし
- [**ID** およびアクセスの管理］に表示されるドメイン：forest1.local、forest2.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

別々のフォレストにユーザーとリソースが存在する場合に（信頼関係あり）、すべてのフォレストに単一の **Connector Appliance** セットを展開

このシナリオは、複数のフォレストを持つ Citrix Virtual Apps and Desktops の顧客に適用されます。

このシナリオでは、一部のフォレスト（resourceforest1.local、resourceforest2.local）はリソース（VDA など）を含み、一部のフォレスト（userforest1.local、userforest2.local）ユーザーのみを含みます。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信頼関係が存在します。

単一の Cloud Connector セットがresourceforest1.localフォレストに展開されます。別の Cloud Connector セットがresourceforest2.localフォレスト内に展開されます。

単一の Connector Appliance セットがuserforest1.localフォレストに展開され、その同じセットがuserforest2.localフォレスト内に展開されます。

- 信頼関係：双方向のフォレストの信頼、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の信頼
- [**ID** およびアクセスの管理]に表示されるドメイン:resourceforest1.local、resourceforest2.local、userforest1.local、userforest2.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

コネクタの更新

August 9, 2023

Citrix では、Cloud Connector または Connector Appliance のパフォーマンス、セキュリティ、および信頼性を強化するための更新を定期的にリリースしています。デフォルトでは、これらの更新が利用可能になるとすぐ、Citrix Cloud により各コネクタに対して 1 つずつインストールされます。ユーザーの Citrix Cloud エクスペリエンスに過度の影響を与えず、これらの更新をタイムリーにインストールするため、以下のように更新のインストールのタイミングを選択できます：

- 希望の時間帯と曜日に更新をスケジュールします。

- 1 回限りの遅延を実行して、指定したコネクタがスケジュールより 2 週間遅れて更新されるようにします。
- ホストマシン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てください。

また、リソースの場所にある現在のコネクタのバージョンを Citrix Cloud の対象バージョンと比較することで、コネクタが最新であることを確認することができます。

> 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 を使用したコネクタ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 - メンテナンススケジュール」を参照してください。

希望する時刻

希望する時刻を指定すると、Citrix Cloud は、更新が利用可能になってから 24 時間後の希望する時刻に更新をインストールします。たとえば、希望の時刻を午前 2:00（米国太平洋時間）に設定してあり、火曜日に更新が利用可能になった場合、Citrix Cloud は 24 時間待機してから、翌日の午前 2:00 に更新をインストールします。

希望する曜日

希望する曜日を指定すると、Citrix Cloud は 7 日間待機してから、希望する曜日に更新をインストールします。この 7 日間の待機期間により、更新をオンデマンドでインストールするか、Citrix Cloud が希望の曜日にインストールするのを待つかを選択する十分な時間が与えられます。選択した曜日と更新が利用可能になる曜日によっては、Citrix Cloud は更新のインストールを最大 13 日間待機する場合があります。

待機期間が **8** 日間になる場合の例

月曜日に、更新の希望日時を火曜日の午後 6:00 に設定しました。その日遅く、Citrix Cloud は利用可能な更新があることを通知し、［更新］ボタンを表示します。そこで更新をしない場合、Citrix Cloud は 7 日間待機し、翌火曜日に更新をインストールします。

待機期間が **13** 日間になる場合の例

更新の希望日時を月曜日の午後 6:00 に設定しました。火曜日に、Citrix Cloud は利用可能な更新があることを通知し、［更新］ボタンを表示します。そこで更新をしない場合、Citrix Cloud は 7 日間待機してから、6 日後の月曜日の午後 6:00 に更新をインストールします。

更新の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」に記載された設定で通知します。また、各コネクタには、更新のインストール日時が表示されます。

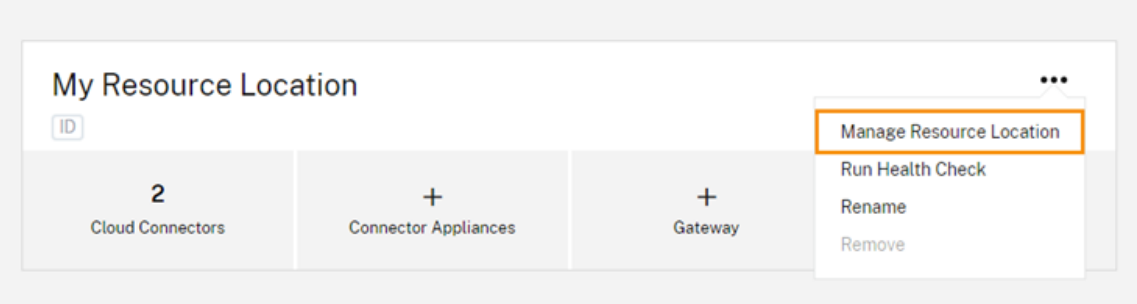
Citrix Cloud から更新が利用可能になったという通知が出されると、各コネクタに ［更新］ボタンが表示されるため、希望する日時よりも早く更新をインストールできます。コネクタごとの ［更新］を選択すると、Citrix Cloud はそれらの更新をキューに入れ、一度に 1 つずつインストールしていきます。更新を開始した後は、更新をキャンセルできません。

更新が完了すると、Citrix Cloud は最後に更新した日付を表示します。一部の更新が完了できない場合は、通知が送信されます。

更新スケジュールの選択

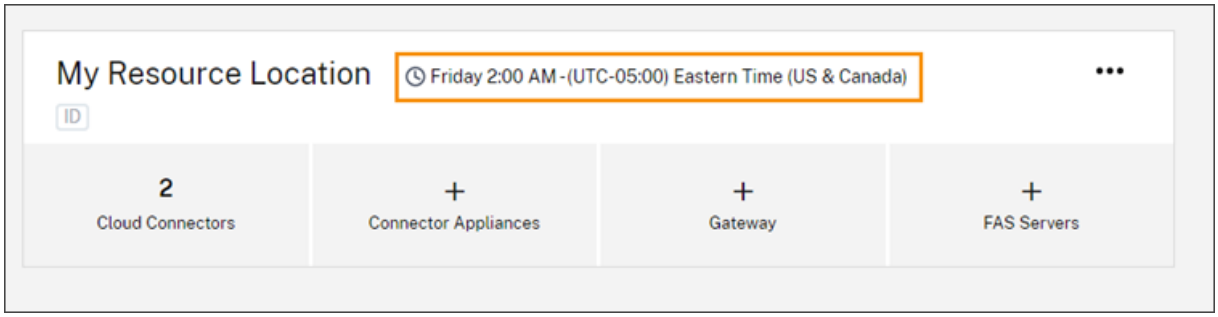
このセクションの手順を使用して、Citrix Cloud 管理コンソールを通じてコネクタの更新をスケジュールします。Citrix Cloud API を使用した更新のスケジュールについては、Citrix Developer ドキュメントの「Citrix Cloud - メンテナンススケジュール」を参照してください。

1. Citrix Cloud メニューから ［リソースの場所］を選択します。
2. 変更する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. ［更新方法を選択します］から ［保守開始時刻を設定］を選択し、更新をインストールする希望の曜日、時刻、タイムゾーンを選択します。
   - 希望の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 時間後の希望する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、時刻、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 日間待機した後、希望の曜日にインストールします。

更新スケジュールを構成すると、Citrix Cloud はリソースの場所の名前の横に更新スケジュールを表示します。



選択した開始時刻は、適用され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。コネクタが複数のタイムゾーンに存在する場合、Citrix Cloud により選択した時刻とタイムゾーンで更新がインストールされます。たとえば、更新を米国太平洋時間の午前 2 時にスケジュールし、コネクタがロンドンにある場合、Citrix Cloud ではこれらのコネクタに対する更新のインストールを米国太平洋時間の午前 2 時に開始します。

更新の再開

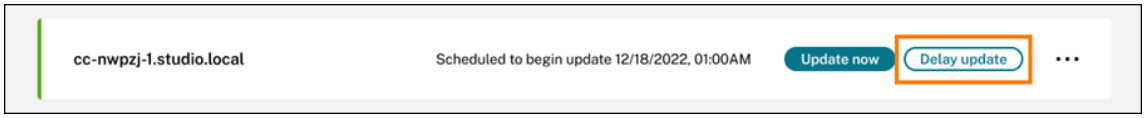
更新のインストール中にコネクタで問題が発生した場合、問題が解決されるまでインストールが一時停止します。更新は各コネクタに一度に 1 つずつインストールされるため、1 つのコネクタで更新を一時停止すると、Citrix Cloud アカウントに残っているすべてのコネクタの更新が妨げられる可能性があります。問題が解決したら、更新を再開できます。

1. Citrix Cloud メニューから ［リソースの場所］を選択します。
2. 管理するリソースの場所を見つけて ［**Cloud Connector**］または［**Connector Appliance**］タイルを選択します。
3. 管理するコネクタを見つけて、［更新の再開］を選択します。

更新の遅延

指定したコネクタに対して 2 週間後に更新が行われるように、スケジュールされた更新を遅らせることができます。スケジュールされた更新を延期できるのは 1 回だけです。更新を一度延期すると、再度延期することはできません。また、デフォルトの 2 週間の期間は変更できません。

1. Citrix Cloud メニューから ［リソースの場所］を選択します。
2. 管理するリソースの場所を見つけて ［**Cloud Connector**］または［**Connector Appliance**］タイルを選択します。
3. 管理するコネクタを見つけて、［更新の遅延］を選択します。



スケジュールした日は当初の予定より 2 週間後の日付に変更されます。

計画外の更新

更新のインストール日時を遅らせた場合でも、Citrix Cloud により利用可能になったの更新が即時にインストールされる場合があります。計画外の更新は、次のような状況で行われます:

- 更新を利用可能になってから 48 時間以内に希望の時刻でインストールできない。たとえば、希望時刻が午前 2 時で、コネクタが更新のリリース後 3 日間オフラインになった場合、コネクタがオンラインに戻ると Citrix Cloud によって即時に更新がインストールされます。
- 更新には、セキュリティまたは機能に関する重大な問題に対する修正が含まれている。

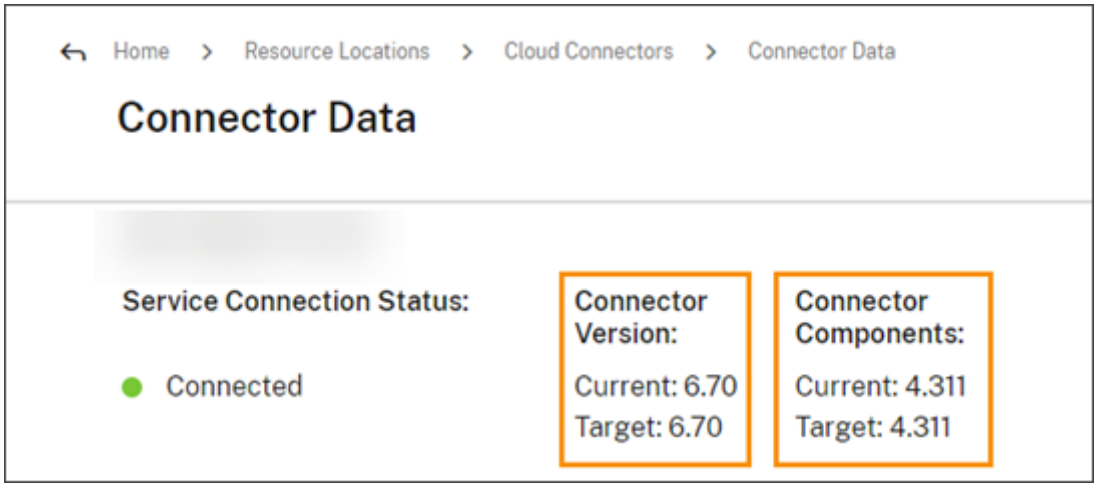
Cloud Connector のバージョンの比較

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 が正常に更新されていることを確認するのに役立ちます。

> 注:
>
> この内容は、Connector Appliance 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 を見つけて、省略記号メニューから ［コネクタデータの表示］を選択します。

［現在］のバージョン番号は、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。［ターゲット］のバージョン番号は、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、［現在］と［ターゲット］のバージョン番号は一致します。



更新エラー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ソフトウェアの競合、または保守中の予期しないエラーにより、Cloud Connector が更新に失敗してサービスが停止することがあります。Cloud Connector の保守後に更新に失敗した場合の対処方法については、「Cloud Connector の保守に失敗した際の解決方法」を参照してください。

Cloud Connector が正常に更新されない場合は、次の条件を確認して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 接続チェックユーティリティを使用して 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［開始済み］の状態になっている。
- Cloud Connector で詳細ログが有効になっている。

Cloud Connector の更新エラーのトラブルシューティング手順については、Citrix サポート Knowledge Center のCTX270718を参照してください。

Citrix Cloud Connector ログを Citrix に送信して、トラブルシューティングのサポートを受けることができます。詳しくは、「Citrix Cloud Connector のログ収集」を参照してください。

ID およびアクセス管理

July 2, 2024

ID およびアクセス管理は、Citrix Cloud 管理者とワークスペース利用者が使用する、ID プロバイダーおよび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 ID プロバイダーを使用して、Citrix Cloud 管理者、ワークスペース利用者、またはその両方を認証できます。

ID プロバイダー	管理者認証	利用者認証
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+ トークン	いいえ	はい
Azure Active Directory	はい	はい
Citrix Gateway	いいえ	はい
Google Cloud Identity	はい	はい
Okta	いいえ	はい
SAML 2.0	はい（AD グループのみ）	はい

デフォルトでは、Citrix Cloud は Citrix ID プロバイダーを使用して、Citrix Cloud アカウントを管理します。Citrix ID プロバイダーは、Citrix Cloud 管理者のみを認証します。

Citrix ID プロバイダー

Citrix Cloud には、管理者をサインイン時に認証する組み込みの Citrix ID プロバイダーが含まれます。Citrix Cloud コンソールでは、Citrix ID プロバイダーに「Citrix Identity」というラベルが付けられます。
管理者認証に別の ID プロバイダーを使用する場合、**Citrix ID** プロバイダーに少なくとも 1 つのフルアクセスの管理者を指定することをお勧めします。これにより、次のことが保証されます:

- 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。
- Citrix Cloud アカウントにアクセスすることで、他の ID プロバイダー（Azure AD など）経由でサインインした場合に完了できない特定の操作を実行できます。たとえば、選択した ID プロバイダーが Azure AD であり、Azure AD と Citrix Cloud の間の接続を再度開始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 アカウントにデフォルトで接続されます。Citrix ID プロバイダーを使用しないことを選択した場合は、必要に応じて接続を削除できます。たとえば、セキュリティと管理者の管理に関する組織のポリシーに従って、この接続を削除することを選択できます。

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 プロバイダー接続を削除するには、Citrix Cloud で別の ID プロバイダーを構成する必要があります。Citrix Cloud では、構成された別の ID プロバイダーが存在しない場合、この接続を削除することはできません。

> 重要
>
> 選択した ID プロバイダーにアクセスできなくなった場合は、Citrix サポートに連絡して Citrix Cloud アカウントを復旧する必要があります。このプロセスが完了するまでに数日かかる場合があります。

Citrix ID プロバイダー接続を削除するには、以下の手順を実行します:

1. Citrix Cloud メニューで、[**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** プロバイダーを削除する] を選択します。

4. 削除の確認メッセージが表示された場合、[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了承します] を選択します。
5. [**ID** プロバイダーを削除する] 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 では、Citrix フェデレーション認証サービス（FAS: Federated Authentication Service）を使用した、ワークスペース利用者のシングルサインオンアクセスがサポートされています。詳しくは、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ワークスペースに対するシングルサインオンの有効化
- 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
  - Tech Insight: フェデレーション認証サービス

管理者

管理者は、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、メールとパスワードを使用して管理者を認証します。My Citrix 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、管理者とワークスペース利用者の両方に多要素認証を提供します。

管理者の場合は、Citrix Cloud へのサインインに多要素認証の使用は必須です。管理者は、Citrix Cloud アカウントの作成過程において、または別の管理者からの招待を受け入れた後に、デバイスを登録できます。詳しくは、次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 メソッドを管理する
- MFA の復旧方法を管理する

ワークスペース利用者の場合、管理者が Active Directory+ 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+ トークンは、Citrix Workspace のデフォルトの ID プロバイダーです。完了後、利用者は多要素認証でデバイスを登録します。詳しくは、次の記事を参照してください:

- Active Directory+ トークン認証を有効にする
- 2 要素認証に対するデバイスの登録
- デバイスの再登録

また、Citrix Cloud 管理者とワークスペース利用者の両方に対して Azure Active Directory 多要素認証を使用できます。展開方法について詳しくは、「Microsoft Azure MFA の展開方法」を参照してください。

新しい管理者を追加する

アカウントの登録処理で、最初の管理者が作成されます。最初の管理者は、自分の 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セットアップすることができます。追加する管理者のアクセス権限を微調整することもできます。これらのアクセス権限の設定により、アクセスレベルを組織内の管理者の役割に対応させることができます。

管理者の追加およびアクセス権限の設定について詳しくは、「管理者の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する場合は、Citrix Cloud サインインページに表示される［ユーザー名またはパスワードを忘れた場合］をクリックします。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、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を受信します。

Citrix では、アカウントのパスワードを常に保護するために、特定の条件下ではパスワードをリセットする必要があります。これらの条件について詳しくは、「パスワードを変更する」を参照してください。

> 注:
>
> メールの許可リストに**customerservice@citrix.com**を追加して、Citrix Cloud のメールが迷惑メールやごみ箱のフォルダーに入らないようにしてください。

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、Citrix Cloud にサインインできなくなります。

アカウントが削除された時に管理者がログインしている場合、最大 1 分間、管理者はアクティブな状態のままでいられます。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 には、顧客アカウントごとに少なくとも 1 人の管理者が必要です。
> - Citrix Cloud Connector は管理者アカウントに関連付けられていません。Cloud Connector をインストールした管理者が顧客アカウントから削除されても、Cloud Connector は動作を続けます。

利用者

利用者の ID は、どの利用者が Citrix Cloud 経由でサービスにアクセスできるかを定義します。この ID は、リソースの場所内のドメインから指定された Active Directory ドメインアカウントによって提供されます。ライブラリのオファリングに利用者を割り当てると、利用者はそのオファリングにアクセスできます。

管理者は、これらの ID を提供するために使用するドメインを [ドメイン] タブで制御できます。複数のフォレストでドメインを使用する場合、各フォレストに Citrix Cloud Connector を 2 つ以上インストールします。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 のインストールをお勧めします。Active Directory での Cloud Connector の展開について詳しくは、「Active Directory での Cloud Connector 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 のみが選択されなくなります。利用者は既に割り当てられている ID を使用することはできます。
> - 各 Citrix Cloud Connector がインストールされた単一のフォレストからすべてのドメインを表示し、使用できます。

利用者の使用状況を管理する

個別のアカウントまたは Active Directory グループを使用して、オファリングに利用者を追加します。グループをオファリングに割り当てた後、Active Directory グループを使用すると Citrix Cloud 経由で管理する必要はありま

せん。

管理者がオファリングから利用者または利用者グループを削除すると、利用者は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利用者を削除する方法について詳しくは、Citrix の製品ドキュメントWeb サイトで該当サービスのドキュメントを参照してください。

プライマリのリソースの場所

プライマリのリソースの場所は、ドメインと Citrix Cloud 間の通信に「最も優先される」と指定するリソースの場所です。プライマリのリソースの場所については、ドメインに対するパフォーマンスや接続性が最も優れた Citrix Cloud Connector があるリソースの場所を選択します。このリソースの場所をプライマリのリソースの場所にすると、ユーザーは Citrix Cloud にすばやくログオンできます。

詳しくは、「プライマリのリソースの場所の選択」を参照してください。

追加情報

- Citrix トレーニング Web サイトの「Citrix ID と認証の概要」教育コースで、サポートされている ID プロバイダーの詳細をご覧ください。
- Citrix Tech Zone:
  - 技術概要: Workspace ID
  - 技術概要: Workspace のシングルサインオン
  - 技術概要: モバイル SSO

Citrix Cloud への管理者のアクセスを管理する

April 5, 2024

Citrix Cloud コンソールで管理者を管理します。管理者の認証に使用する ID プロバイダーに応じて、管理者を個別に追加することも、グループを使用して追加することもできます。

すべての管理者が、Citrix Cloud にサインインするときに認証の第 2 要素としてトークンを使用する必要があります。管理者として追加されると、デバイスを多要素認証に登録し、Citrix SSO などの時間ベースのワンタイムパスワード標準に準拠した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、管理者の認証で次の 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。個別の管理者の追加のみをサポートします。
- Azure AD：個別の、または AAD グループを使用しての管理者の追加をサポートします。AAD グループの管理者のアクセスは、カスタムアクセス権役割のみに限定されています。詳しくは、「管理者グループを管理する」を参照してください。
- SAML 2.0：AD グループによる管理者の追加のみをサポートします。詳しくは、「SAML を ID プロバイダーとして Citrix Cloud に接続する」を参照してください。

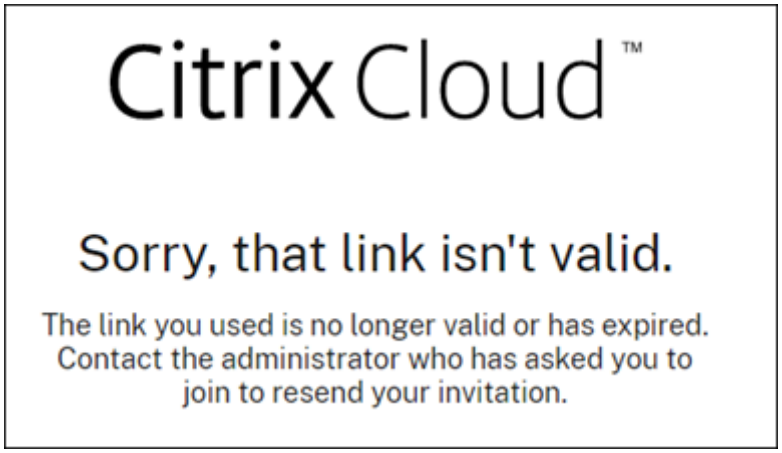
新しい管理者を追加するには、次のワークフローを使用します：

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、個別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. 組織内の管理者の役割に応じたアクセス権限を指定します。詳しくは、この記事の「管理者権限を変更する」を参照してください。

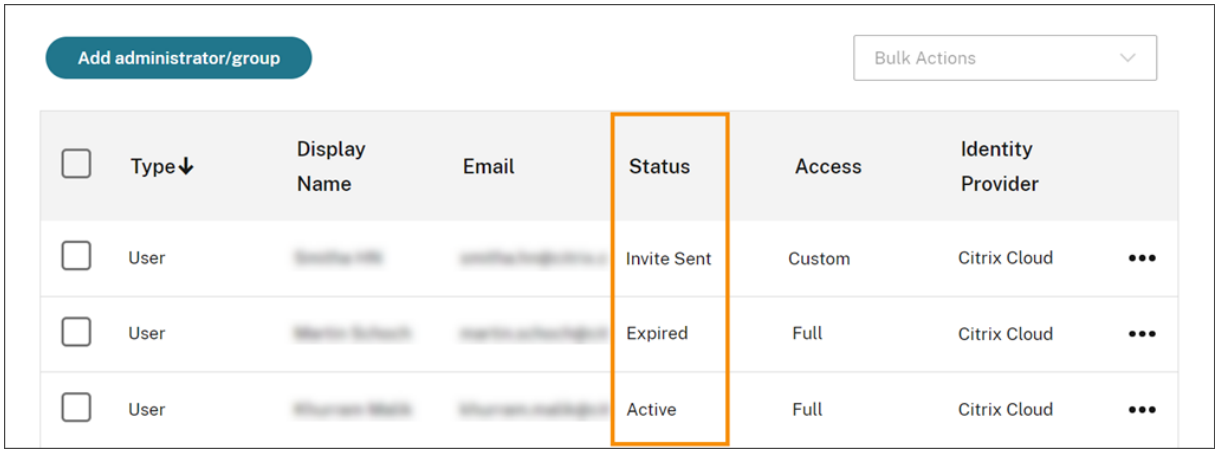
個別の管理者を招待する

個別の管理者を追加するには、Citrix Cloud アカウントに参加するよう招待します。管理者を追加すると、Citrix から相手に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。グループを通じて追加した管理者には招待は送信されず、追加後すぐにサインインできます。

cloud@citrix.comから送信された招待メールには、アカウントへのアクセス方法が記載されています。招待メールは送信日から 5 日間有効です。5 日が経過すると、招待リンクの有効期限が切れます。招待された管理者が期限切れのリンクを使用した場合、リンクが無効であることを知らせるメッセージが Citrix Cloud で表示されます。



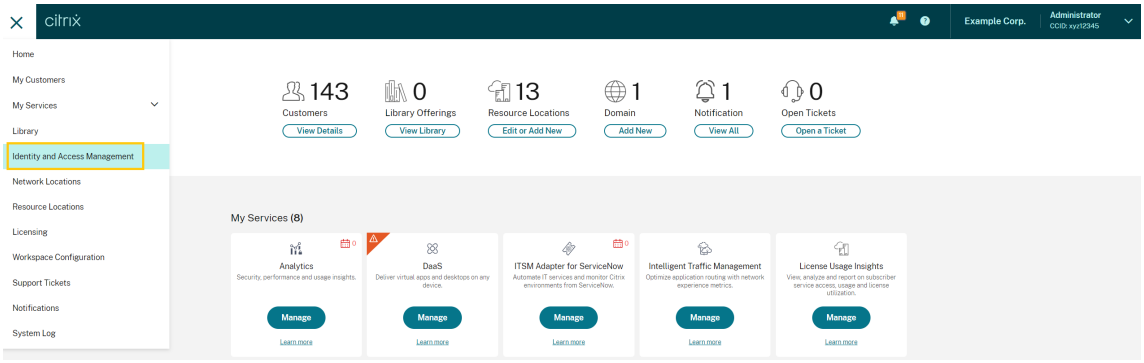
Citrix Cloud には招待メールのステータスも表示されるため、管理者が招待メールを受け入れて Citrix Cloud にサインインしたかどうかを確認できます。



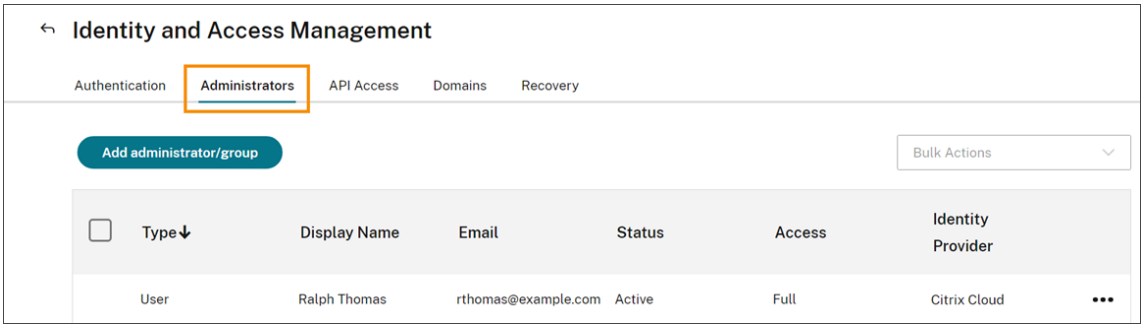
> 注
>
> 管理者アカウントは最大 100 の顧客アカウントに関連付けることができます。その管理者が 100 を超える顧客アカウントを管理する必要がある場合、追加の顧客を管理するには、別のメールアドレスで別の管理者アカウントを作成する必要があります。また、管理する必要がなくなった顧客アカウントから管理者を削除することもできます。

管理者を招待するには

1. Citrix Cloud にサインインしてから、メニューで ［**ID** およびアクセス管理］を選択します。



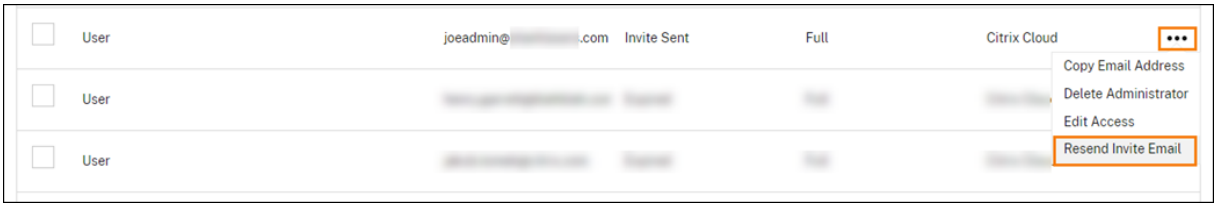
2. ［**ID** およびアクセス管理］ページで ［管理者］を選択します。コンソールに、アカウント内の現在の管理者全員が表示されます。



3. ［管理者/グループを追加する］を選択します。
4. ［管理者の詳細］で、使用する ID プロバイダーを選択します。Azure AD を使用している場合、最初にサインインするように求めるメッセージが Citrix Cloud に表示されることがあります。
5. **Citrix ID** を選択した場合は、ユーザーのメールアドレスを入力して ［次へ］をクリックします。
6. **Azure Active Directory** を選択した場合は、追加するユーザーの名前を入力して ［次へ］をクリックします。AAD ゲストユーザーの招待はサポートされていません。
7. ［アクセスの設定］で、管理者に適切な権限を設定します。フルアクセス（デフォルトで選択）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。変更するには、［戻る］を選択します。
9. ［招待を送信］を選択します。Citrix Cloud は、指定されたメールアドレスに招待メールを送信し、管理者を一覧に追加します。

招待メールを再送信する

招待メールを再送信するには、コンソールの右端にある省略記号（…）メニューから ［招待メールの再送信］を選択します。招待メールを再送信しても、招待メールの有効期限が切れるまでの 5 日間の制限に変更はありません。



新しいサインインリンクを含む招待メールを再送信する

元の招待メールの有効期限が切れた場合は、新しい招待メールを管理者に送信できます。次の手順を実行します:

1. Citrix Cloud から管理者を削除する:［管理者］ページで、一覧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、サインインのリンクが正しくない招待状が送信される可能性があります。
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。

管理者の招待を受け入れる

Citrix Cloud アカウントに招待された場合、アカウントの組織 ID と顧客名が記載されたメールが Citrix から送信されます。

招待を受け入れるには、［サインイン］をクリックします。その後、ブラウザー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、ブラウザーにパスワード作成ページが表示されます。既にアカウントをお持ちの場合は、Citrix Cloud は既存のパスワードを使用してサインインするように要求します。

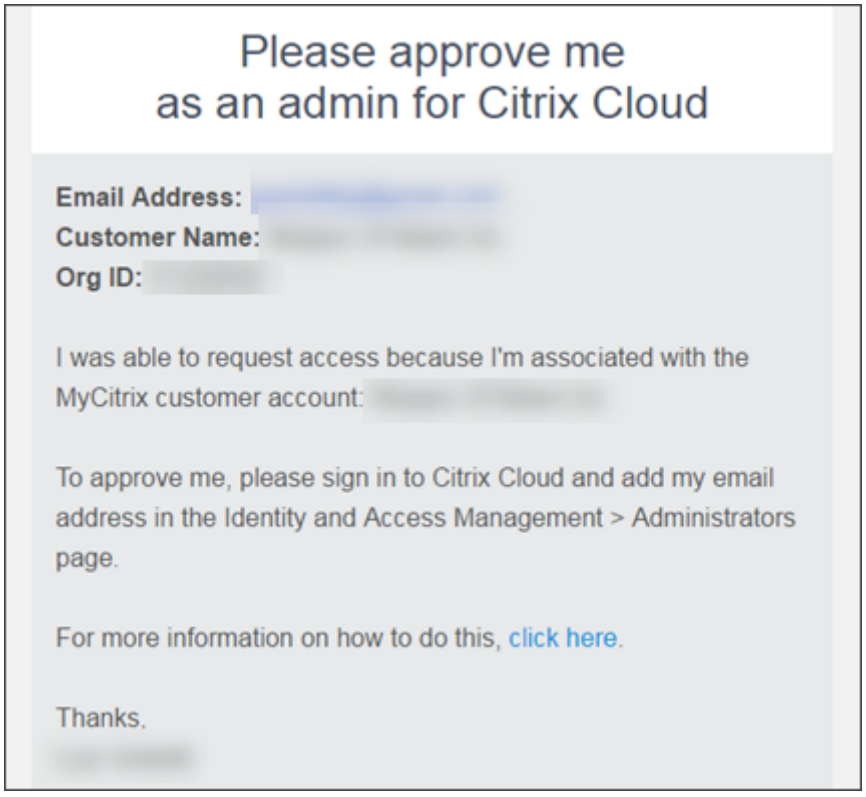
サインイン中に、多要素認証に登録するように求められる場合があります。登録手順については、「多要素認証を設定する」を参照してください。

管理者グループを追加する

AD グループ（SAML 認証用）または Azure AD グループ（Azure AD 認証用）を使用して管理者を追加できます。詳しくは、「管理者グループを管理する」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

管理者の Citrix Cloud アカウントに参加することを希望する組織内のユーザーからの承認リクエストを、Citrix Cloud で受け取ることがあります。



管理者がこれらのリクエストを承認するには、この記事の「個別の管理者を招待する」の説明に従って、アクセスをリクエストしているユーザーを管理者として招待します。この場合、承認リクエストのメールに表示されるメールアドレスと同じアドレスを使用する必要があります。

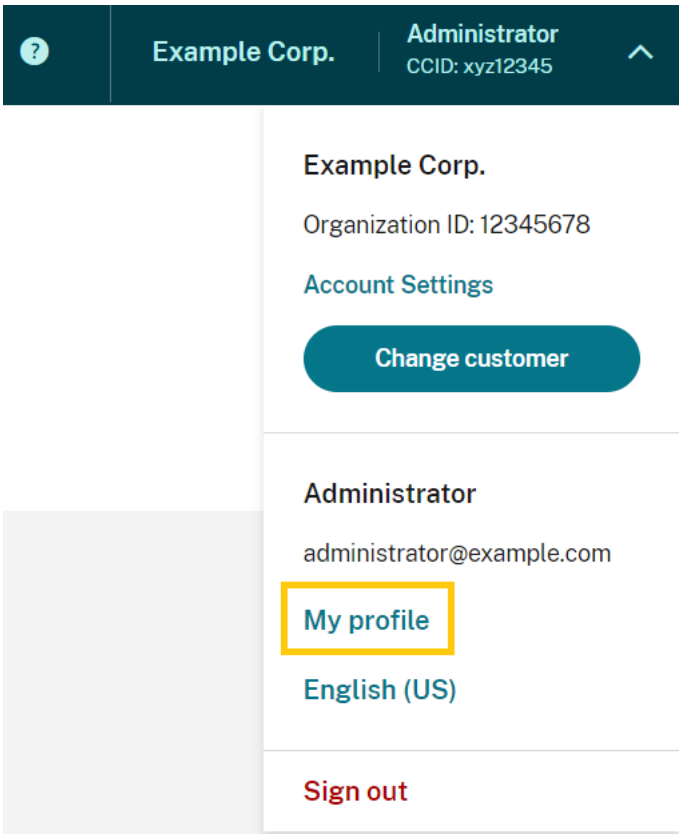
アクセスをリクエストしているユーザーは、招待を受信後、［サインイン］リンクをクリックして招待を承諾します。その後、ユーザーは Citrix Cloud のパスワードを作成し、管理者アカウントにサインインできます。

承認リクエストの生成方法について詳しくは、「アカウントが既に使用中の場合」を参照してください。

メールアドレスの変更

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）の復旧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へ確認メールが送信されます。確認したら Citrix Cloud からサインアウトされ、変更を完了できます。数分後に新しいメールアドレスで再度サインインできます。

1. 右上のメニューから ［自分の設定］を選択します。



2. ［メールアドレス］で、［メールの変更］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、［確認して完了する］を選択します。
5. ［はい、メールアドレスを変更します］を選択して変更を確認します。

変更を確認したら、Citrix Cloud からサインアウトされます。数分後に新しいメールアドレスで再度サインインできます。

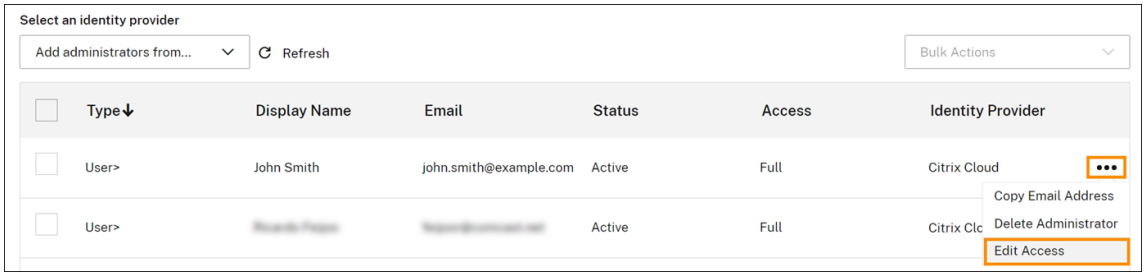
管理者権限を変更する

Citrix Cloud アカウントに管理者を追加するときは、組織内での役割に適した管理者権限を定義します。デフォルトでは、新しい管理者には Citrix Cloud アカウントのすべての機能と使用可能なサービスへの _ フルアクセス権限 _ が割り当てられています。管理コンソールの特定の領域または特定のサービスへのアクセスを制限する場合は、_ カスタムアクセス権限 _ を定義できます。

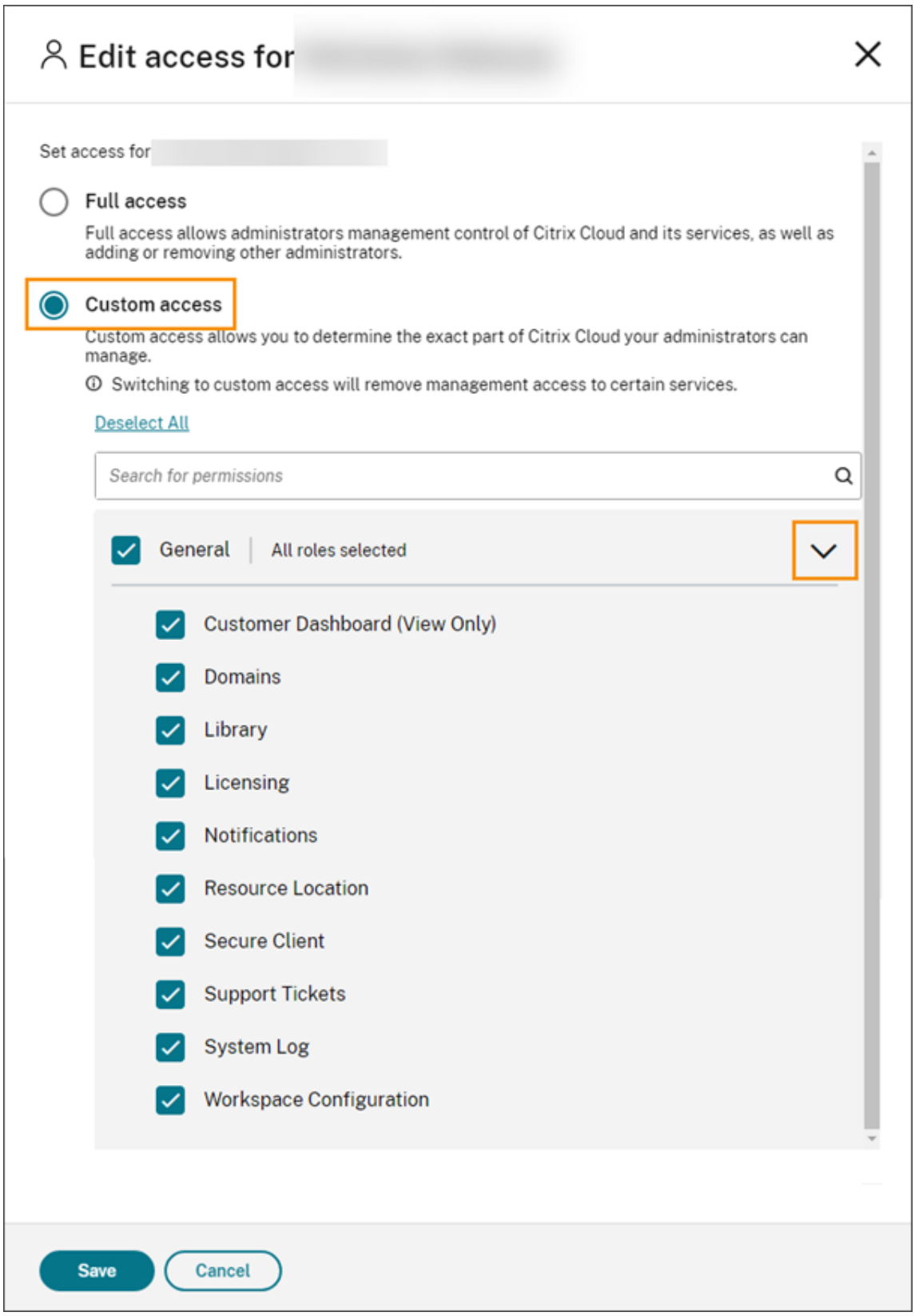
他の管理者の権限を定義できるのは、フルアクセス権限を持つ Citrix Cloud 管理者だけです。

既存の管理者権限を変更するには:

1. https://citrix.cloud.comで Citrix Cloud にサインインします。
2. Citrix Cloud メニューから、[**ID** およびアクセス管理] を選択し、[管理者] を選択します。
3. 管理対象の 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 Azure AD（接続されている場合）。
4. 管理対象の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、[アクセスの編集] を選択します。



5. 特定の権限を許可または禁止するには、[カスタムアクセス] を選択します。Citrix Cloud の全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、検索ボックスを使用します。入力したテキストに一致する権限が Citrix Cloud に表示されます。たとえば、「read only」（読み取り専用）と入力し始めると、タイトルに「read only」が含まれる権限が表示されます。アクセス権限の検索では、大文字と小文字が区別されません。
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、[全般] を開きます。



8. 特定のサービスのカスタムアクセス権限を定義するには、サービスを展開します。

9. 権限ごとに、必要に応じてチェックマークを選択またはクリアします。
10. [**Save**] を選択します。

コンソールの権限

このセクションでは、Citrix Cloud 管理コンソールで使用できるカスタムアクセス権限について説明します。特定のサービスのカスタムアクセス権限について詳しくは、サービスのドキュメントを参照してください。

- 顧客ダッシュボード（表示のみ）: 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。
- ドメイン: [**ID** およびアクセス管理] **>** [ドメイン] タブへのアクセスが許可されます。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。
- ライブラリ: [ライブラリ] コンソールページへのアクセスが許可されます。管理者にアクセス権限があるサービスでは、管理者は、Citrix DaaS のデリバリーグループにユーザーを割り当てたり、Endpoint Management からIntune 管理対象アプリを追加したり、Secure Private Access のアプリの詳細を表示する権限を読み取り専用管理者に付与したりすることができます。
- 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] タブおよび [ライセンス割り当て済みの展開] タブへのアクセスが許可されます。
- 通知: [通知] コンソールページへのアクセスが許可されます。管理者は Citrix Cloud の通知を表示したり閉じたりできます。
- 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が許可されます。管理者は、新しいリソースの場所を追加したり、Citrix Workspace の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。コネクタの更新を管理することもできます。
- セキュアクライアント: [**ID** およびアクセス管理] **>** [**API** アクセス] **>** [セキュアクライアント] タブへのアクセスが許可されます。管理者は、Citrix Cloud APIで使用する独自のセキュアクライアントを作成および管理できます。この権限には、[**ID** およびアクセス管理] **>** [**API** アクセス] **>** [製品の登録] タブへのアクセスは含まれません。[製品の登録] タブにアクセスできるのはフルアクセス管理者のみです。
- サポートチケット: [サポートチケット] コンソールのメニューオプションおよび [チケットを開く] のヘルプメニューオプションへのアクセスが許可されます。これらのオプションのいずれかを選択すると、管理者は [My Support] ポータルに送信されます。詳しくは、「テクニカルサポート」を参照してください。
- 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が許可されます。管理者は、システムログイベントを表示したり、イベントを CSV ファイルにエクスポートしたりできます。
- ワークスペース構成: [ワークスペース構成] コンソールページへのアクセスが許可されます。管理者は、認証方法の変更、ワークスペース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、サイトアグリゲーションの構成を行うことができます。詳しくは、Citrix Workspaceの製品ドキュメントを参照してください。
- **Workspace** の **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] **>** [**Workspace API**] タブへのアクセスが許可されます管理者は、Citrix Workspace プラットフォーム API と対話するための独自の 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 Workspace

API 専用として使用されます。また、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を含んでいます。

> 注:
>
> [**Workspace OAuth** クライアント］のカスタム役割を割り当てる場合は、慎重に実行することをお勧めします。この役割に関連付けられたアクセス権限により、管理者は Workspace 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）にアクセスできるようになります。［フルアクセス］権限を持つ管理者には、［**Workspace OAuth** クライアント］権限を持つ管理者と同等のアクセス権限が自動的に付与されることにも注意してください。

プライマリ **MFA** メソッドを管理する

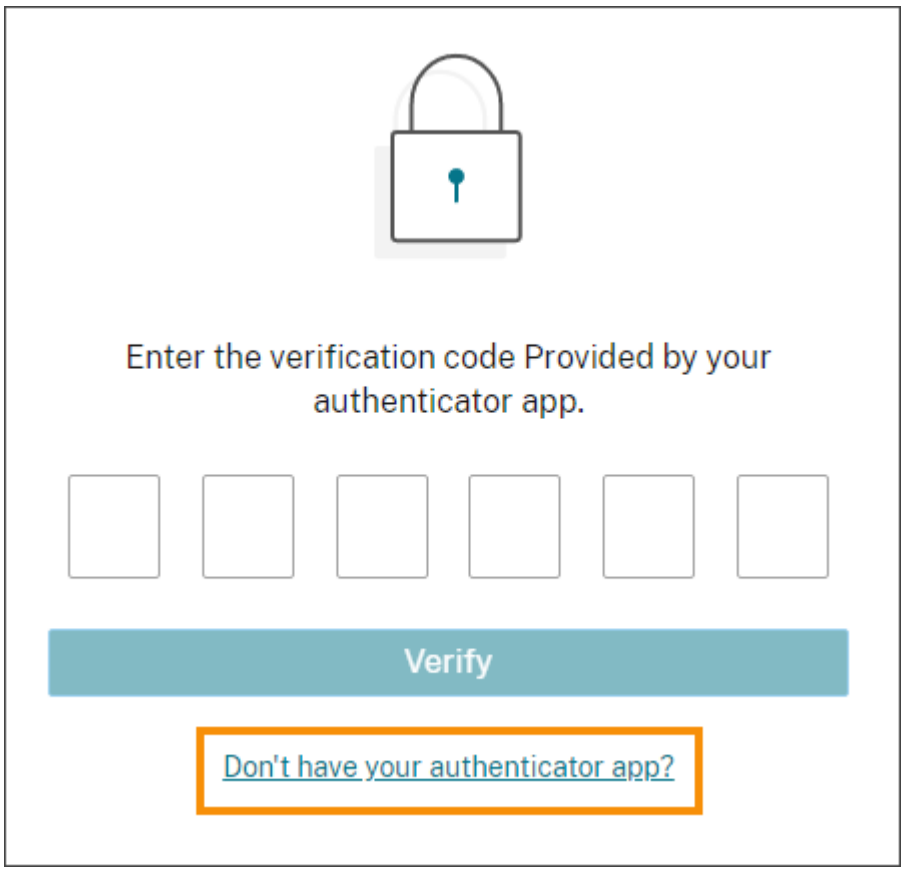
多要素認証（MFA）を使用して Citrix Cloud にサインインするには、認証アプリを使用するか、メールアドレスを使用できます。このセクションでは、MFA のデバイス登録を変更する方法、または別の多要素認証方法に切り替える方法について説明します。

MFA 用のデバイスを変更する

登録済みのデバイスを紛失し、Citrix Cloud で別のデバイスを使用する場合、または認証アプリをリセットする場合は、Citrix Cloud の多要素認証に再登録できます。

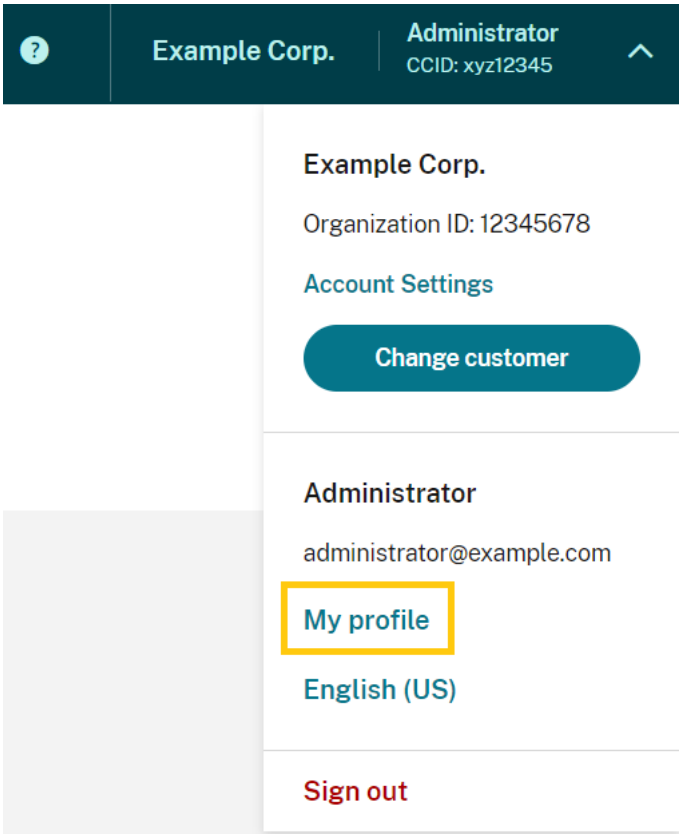
> メモ
>
> - デバイスを変更すると、現在のデバイス登録が削除され、新しい認証アプリキーが生成されます。
> - 元の登録から同じ認証アプリで再登録する場合は、再登録する前に、認証アプリから Citrix Cloud エントリを削除します。このエントリに表示されるコードは、再登録が完了すると機能しなくなるためです。再登録の前または後にこのエントリを削除しない場合、認証アプリには、異なるコードの 2 つの Citrix Cloud エントリが表示され、Citrix Cloud へのサインイン時に混乱を引き起こす可能性があります。
> - 新しいデバイスを再登録中で、認証アプリがない場合は、デバイスのアプリストアから認証アプリをダウンロードしてインストールします。操作をスムーズにするためには、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 Citrix ではお勧めします。

1. Citrix Cloud にサインインして認証アプリからのコードを入力します。

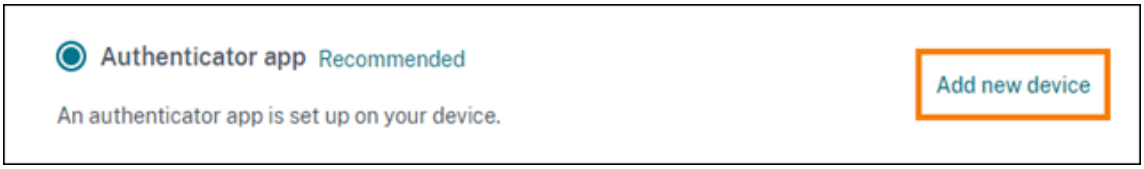


認証アプリがない場合は、［認証アプリがありませんか?］をクリックしてサインインに役立つ復旧方法を選択します。選択した復旧方法に応じて、受信した復旧コード、または未使用のバックアップコードを入力して［確認］を選択します。

2. 複数の顧客組織の管理者である場合は、任意の組織を選択します。
3. 右上のメニューから ［自分の設定］を選択します。



4. ［認証アプリ］で ［新しいデバイスの追加］を選択します。



5. デバイスの変更を確認するメッセージが表示されたら、［はい、自分の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。認証アプリがない場合は、［復旧方法を使用する］を選択して、選択した復旧方法で本人確認を行います。選択した復旧方法に応じて、受信した確認コードか復旧コード、また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中で、認証アプリがない場合は、デバイスのアプリストアからダウンロードします。
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. 認証アプリで 6 桁の確認コードを入力して、［コードを確認する］を選択します。

デバイスを変更したら、［マイプロファイル］ページの確認方法が最新であることを確認することを Citrix では強くお勧めします。

MFA の方法を変更する

認証アプリを使用して MFA に登録しており、メールアドレスの使用に切り替える場合は、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。認証アプリを使用した多要素認証に戻る場合は、デバイスを再登録する必要があります。

1. Citrix Cloud コンソールの右上のメニューから、［自分の設定］を選択します。
2. ［多要素認証（**MFA**）］で、切り替える認証方法を選択します。
3. メール MFA に切り替える場合:

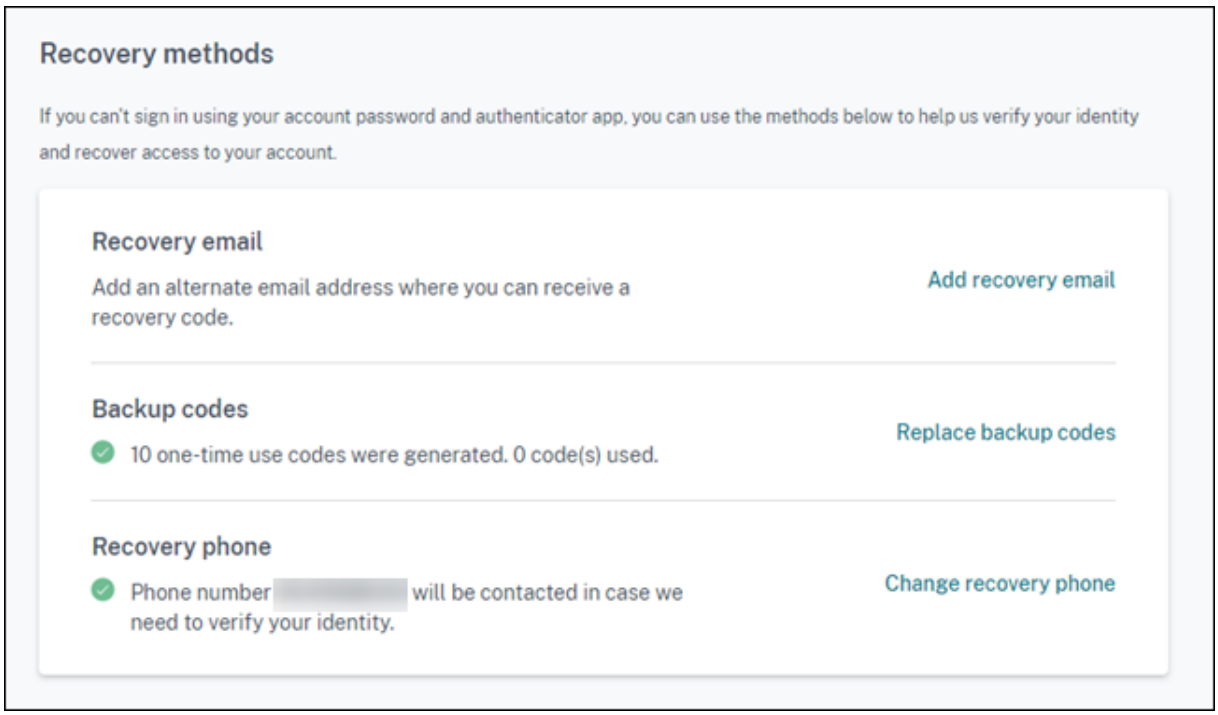
    a) ［はい、メールに変更します］を選択して、MFA の方法を変更することを確認します。
    b) 認証アプリからコードを入力するか、復旧方法を使用して ID を確認します。
    c) ［確認して続行］を選択して変更を完了します。

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 がメールアドレスに送信する確認コードを入力し、［確認して続行］を選択します。または、復旧方法を使用して ID を確認します。
    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) ［認証アプリを確認する］で認証アプリから 6 桁のコードを入力します。
    d) ［コードを確認する］をクリックしてデバイスの登録を完了します。

MFA の復旧方法を管理する

> 重要:
>
> Citrix Cloud アカウントの安全を確保するには、確認方法を最新の状態に保ち、正確な情報を使用します。認証アプリまたは MFA メールアドレスにアクセスできなくなった場合、これらの確認方法がアカウントへのアクセスを復旧する唯一の方法です。



復旧用のメールアドレスを追加または変更する

1. 右上のメニューから ［自分の設定］を選択します。
2. 復旧用のメールアドレスをまだ追加していない場合は、［復旧方法］の ［復旧用のメール アドレス］で ［復旧用のメールアドレスを追加する］を選択します。復旧用のメールアドレスを既に追加している場合は、［復旧用のメール アドレスを変更する］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を入力するか、メールアドレスに送信されたコードを入力します。
4. 使用する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 アカウントに使用するメールアドレスとは異なる必要があります。Citrix Cloud は、入力した電子メールアドレスに確認電子メールを送信します。
5. 確認メールにあるコードを入力し、［コードを確認して完了する］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のセットを生成できます。バックアップコードを使用するとき、Citrix Cloud は、［マイプロファイル］ページで使用された番号を記録します。

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. 右上のメニューから ［自分の設定］を選択します。

2. 以前にバックアップコードを生成したことがない場合は、[復旧方法] 下にある [バックアップコード] で、[新しいバックアップコードを生成する] を選択します。以前にバックアップコードを生成したことがある場合は、[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を置き換えるように求められたら、[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. [コードをダウンロードする] を選択して、新しいコードをテキストファイルとしてダウンロードします。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を保存しました] を選択して、バックアップコードの置き換えを完了します。

復旧用の電話番号を変更する

1. 右上のメニューから [自分の設定] を選択します。
2. [復旧方法] の [復旧用の電話番号] で [復旧用の電話番号を変更する] を選択します。
3. 認証アプリの確認コードを入力するか、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、確認のために電話番号を再入力します。
5. [復旧用の電話番号を保存] を選択します。

> 注:
>
> Citrix Endpoint Management（CEM）の管理者権限を変更できるのは、管理者が管理者への招待を受け入れ、CEM タイルで [管理] をクリックした後のみです。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限を持っています。

管理者グループを管理する

February 15, 2024

Active Directory、Azure Active Directory（AD）、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許可を管理できます。

AD の前提条件

Citrix Cloud は、SAML 2.0 による 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。詳しくは、「SAML を ID プロバイダーとして Citrix Cloud に接続する」を参照してください。

既に Citrix Cloud に SAML 接続している場合は、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に失敗する場合があります。詳しくは、「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。

Azure AD の前提条件

Azure AD グループ認証を使用するには、Azure AD を Citrix Cloud に接続する最新バージョンの Azure AD アプリケーションが必要です。このアプリケーションは、Azure AD に初めて接続したときに Citrix Cloud が取得しています。2019 年 5 月以前に Azure AD を Citrix Cloud に接続していた場合は、Citrix Cloud が Azure AD への接続で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。アカウントで使用しているアプリケーションが最新のものでない場合、Citrix Cloud で Azure AD グループを表示できません。

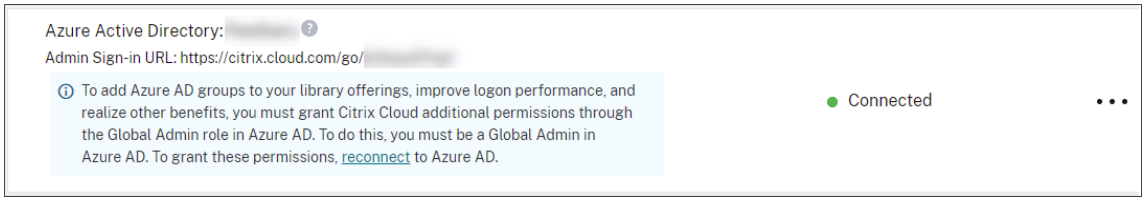
Citrix Cloud で Azure AD グループを使用する前に、次のタスクを実行します:

1. Azure AD 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 で通知が表示されます。
2. アプリケーションを更新する必要がある場合は、Azure AD を Citrix Cloud に再接続します。Azure AD に再接続することにより、アプリケーションレベルの読み取り専用権限が Citrix Cloud に付与され、Citrix Cloud が Azure AD に再接続できるようになります。再接続中に、これらの権限のリストが表示されるので確認してください。Citrix Cloud が要求する権限について詳しくは、「Citrix Cloud 用の Azure Active Directory の権限」を参照してください。

   > 重要:
   >
   > このタスクを完了するには、Azure AD 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。Azure AD の資格情報を使用してサインインすると、再接続に失敗します。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、管理者を一時的に追加してこのタスクを実行し、後で削除することができます。

Azure AD 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、[**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. **Azure Active Directory** を見つけます。Azure AD に接続するために Citrix Cloud でアプリケーションをアップデートする必要がある場合、通知が表示されます。



Citrix Cloud が既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。

Azure AD に再接続するには

1. Citrix Cloud コンソールの Azure AD の通知から、［再接続］の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. 権限を確認してから ［許可］を選択します。

Google Cloud Identity

Citrix Cloud は、Google Cloud Identity を使用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。詳しくは、「Google Cloud Identity を ID プロバイダーとして Citrix Cloud に接続する」を参照してください。

サポートされるサービス

次のサービスは、管理者グループのカスタムアクセス権限をサポートしています:

- Citrix Analytics
- NetScaler コンソール
- Citrix DaaS
- Workspace Environment Management サービス
- License Usage Insights

サポートされている権限

Citrix Cloud プラットフォームのサポートされているサービスと特定の機能に対してのみ、カスタムアクセス権限を割り当てることができます。フルアクセス権限はサポートされていません。

Citrix Cloud プラットフォーム機能では、次のカスタムアクセス権限がサポートされています:

- ドメイン
- ライセンス
- リソースの場所
- サポートチケット
- システムログ
- ワークスペース構成

これらの権限について詳しくは、「コンソールの権限」を参照してください。

管理者グループは、他のサービスにアクセスできません。アクセス権限のあるサポート対象サービスのみを管理できます。

既にサインインしている管理者グループメンバーのアクセス権限の変更は、サインアウトして再度サインインした後でのみ有効になります。

Citrix ID、**AD ID**、**Azure AD ID**、および **Google Cloud Identity** を持つ管理者の最終的な権限

管理者が Citrix Cloud にサインインするとき、管理者が Citrix ID（Citrix Cloud のデフォルトの ID プロバイダー）と、AD、Azure AD、または Google Cloud Identity で取得したシングルユーザー ID またはグループベース ID の両方を持っている場合、使用できるのは特定の権限のみである場合があります。このセクションの表では、これらの ID の各組み合わせで使用できる権限について説明します。

_ 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、Azure AD、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、Azure AD、Google Cloud Identity 権限を指します。

Citrix ID	シングルユーザーの AD または Azure AD の ID	グループベースの AD または Azure AD 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 と、AD ID または Azure AD ID のいずれかで認証に成功した後、両方の ID の累積的な権限を有します。
X		X		各 ID は独立したエンティティとして扱われます。使用可能な権限は、管理者が認証に Citrix ID と Azure AD ID のどちらを使用しているかによって異なります。

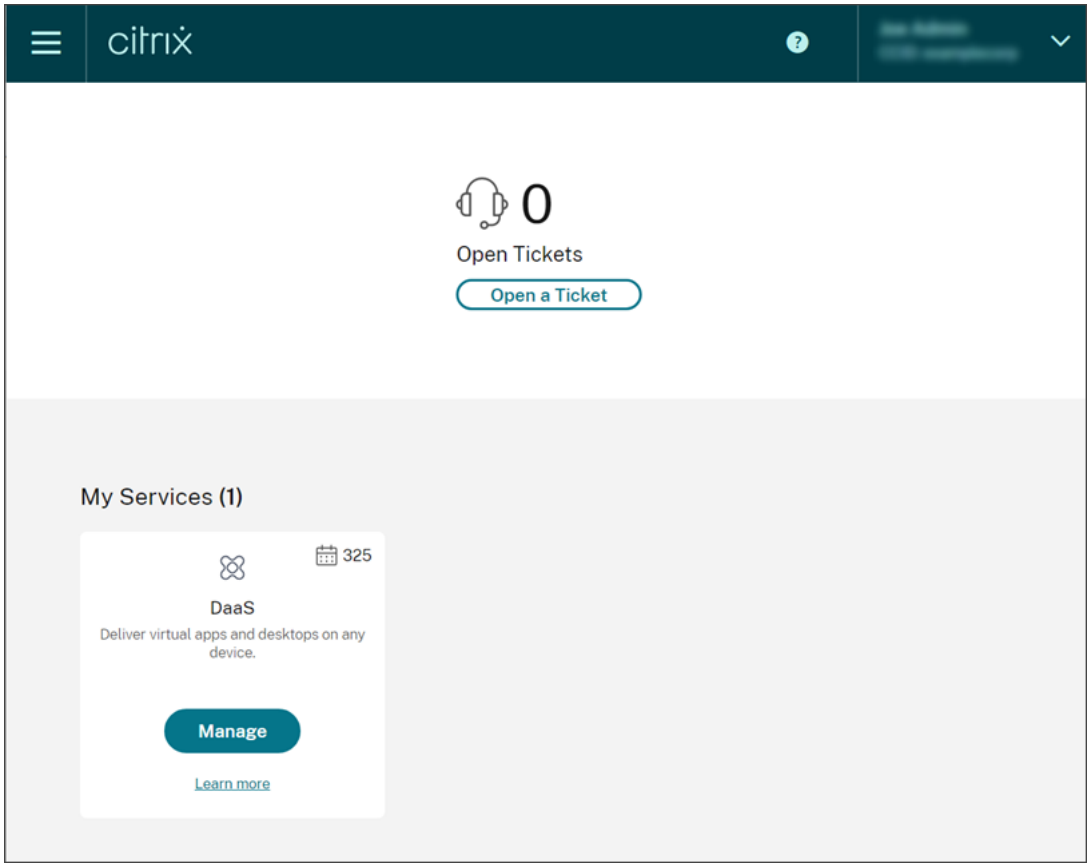
Citrix ID	シングルユーザーの AD または Azure AD の ID	グループベースの AD または Azure AD の ID	シングルユーザーまたはグループベースの Google Cloud Identity	認証後に利用可能な権限
X			X	各 ID は独立したエンティティとして扱われます。使用可能な権限は、管理者が認証に Citrix ID と Google Cloud Identity のどちらを使用しているかによって異なります。
	X	X		管理者は、AD または Azure AD を使用して Citrix Cloud に認証するときに、両方の ID の累積的な権限を有します。
	X		X	各 ID は独立したエンティティとして扱われます。使用可能な権限は、管理者が認証に Citrix ID と Google Cloud Identity のどちらを使用してい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。使用可能な権限は、管理者が認証に Citrix ID と Google Cloud Identity のどちらを使用しているかによって異なります。

Citrix ID	シングルユーザーの AD または Azure AD の ID	グループベースの AD または Azure AD 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		管理者は、Citrix ID を使用して認証する場合、Citrix ID とシングルユーザーの Azure AD ID の両方の累積的な権限を有します。Azure AD 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有します。

管理者のサインインエクスペリエンス

グループを Citrix Cloud に追加し、サービスの権限を定義した後、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 を入力してサインインするだけです（例: `https://citrix.cloud.com/go/mycompany`）。個々の管理者を追加するのとは異なり、グループの管理者は明示的に招待されないため、Citrix Cloud 管理者としての招待を受諾するためのメールを受信しません。

サインイン後、管理者はタイルから ［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権限しか付与されていない管理者は、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。

個々のアカウントを介して、およびグループのメンバーとして権限が付与されている管理者は、アクセスする 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、カスタマーピッカーから Citrix Cloud アカウントを選択できます。

制限事項

プラットフォームとサービス機能へのアクセス

管理者グループのメンバーは、次の Citrix Cloud プラットフォームの機能のカスタムアクセス権限を使用できません:

- ライブラリ
- 通知
- セキュアクライアント

利用可能なアクセス権限について詳しくは、この記事の「サポートされている権限」を参照してください。

クイック展開ユーザー割り当てなどの Citrix Cloud プラットフォーム機能に依存する Citrix DaaS の機能は使用できません。

アプリケーションのパフォーマンスに対する複数のグループの影響

1 人の管理者が属する Citrix Cloud に追加済みのグループの数は、20 個以下を推奨します。これより多くのグループに所属すると、アプリケーションのパフォーマンスが低下する可能性があります。

認証に対する複数のグループの影響

グループベースの管理者が AD または Azure AD の複数のグループに割り当てられている場合、グループの数が多すぎるために認証に失敗する可能性があります。この問題は、Citrix Cloud と AD または Azure AD との統合に制限があるために発生します。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の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、いずれのグループも取得できず、認証に失敗します。

この問題は、AD または Azure AD を介して Citrix Workspace 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、グループの数が多すぎるために認証に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ます。

役割/スコープのペアの割り当てが多すぎることによるグループの追加エラー

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きに、グループを作成できないことを示すエラーが発生する可能性があります。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大き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て、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、[**ID** およびアクセス管理] を選択し、[管理者] を選択します。
2. [管理者/グループを追加する] を選択します。
3. [管理者の詳細] で、使用する ID プロバイダーを選択します。Azure AD を選択している場合は、必要に応じて Azure にサインインします。[次へ] 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、グループを選択します。
6. [アクセスの設定] 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、[保存] 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

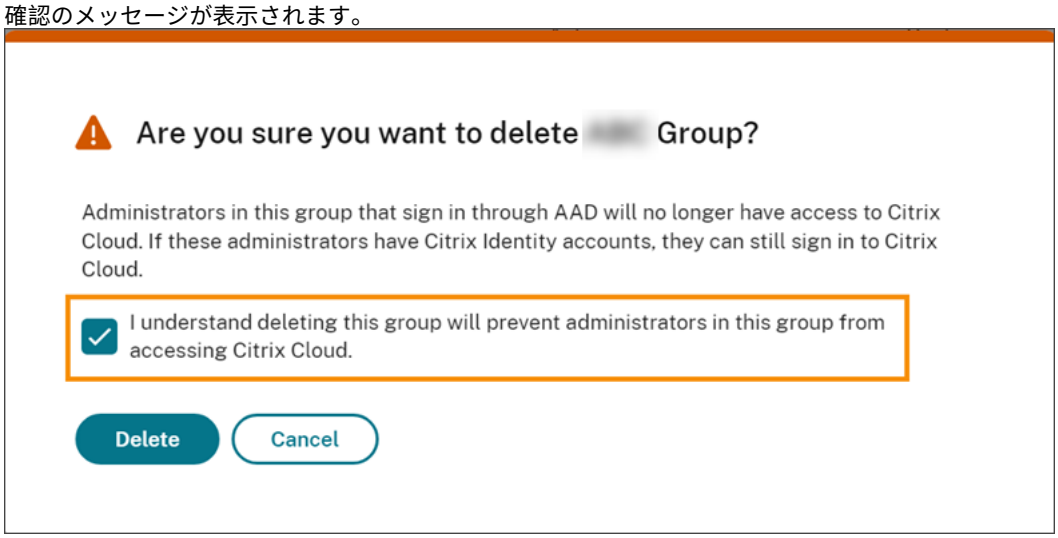
1. Citrix Cloud メニューから、[**ID** およびアクセス管理] を選択し、[管理者] を選択します。
2. 管理する管理者グループを見つけ、省略記号メニューから [アクセスの編集] を選択します。

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選択またはクリアします。
4. 完了したら、[保存] 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、[**ID** およびアクセス管理] を選択し、[管理者] を選択します。
2. 管理する管理者グループを見つけ、省略記号メニューから [グループの削除] を選択します。

確認のメッセージが表示されます。

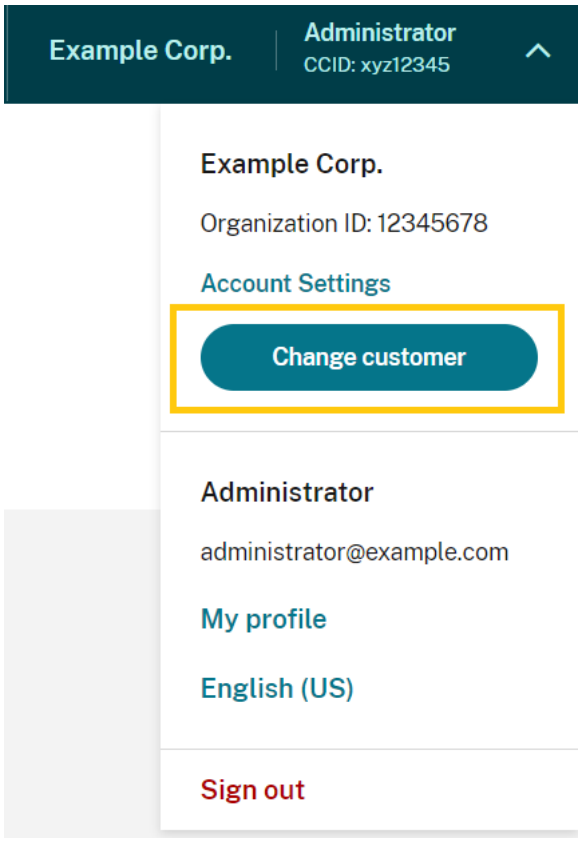


3. このグループを削除すると、グループの管理者が **Citrix Cloud** にアクセスできなくなることを了承し、グループを削除した場合の影響を認識していることを確認します。
4. [削除] を選択します。

複数の **Citrix Cloud** アカウントの切り替え

> 注:
>
> このセクションでは、Azure AD 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、Azure AD 管理者グループのメンバーは、アクセス可能な他の Citrix Cloud アカウントを切り替えることはできません。Azure AD 管理者グループの管理者の場合、Citrix Cloud ユーザーメニューに、下の画像に示されている ［顧客の変更］オプションが表示されません。

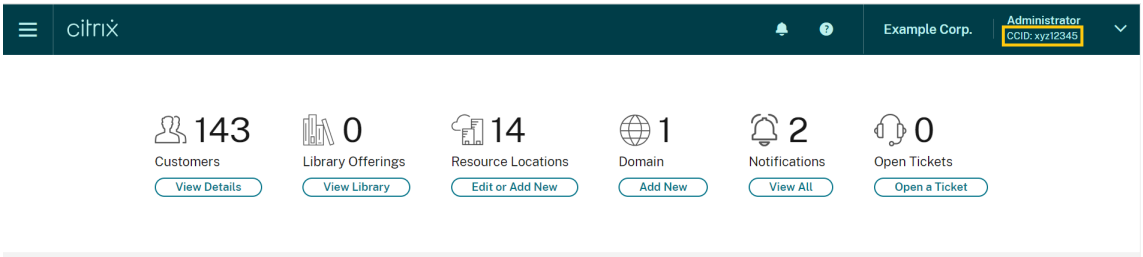


このメニューオプションを有効にして、Azure AD グループメンバーが他の Citrix Cloud アカウントを切り替えられるようにするには、変更するアカウントとアカウントをリンクする必要があります。

Citrix Cloud アカウントのリンクには、ハブ & スポークアプローチが用いられます。アカウントをリンクする前に、ほかのアカウントにアクセスするアカウント（「ハブ」）として機能する Citrix Cloud アカウントと、カスタマーピッカーに表示するアカウント（「スポーク」）を決定します。

アカウントをリンクする前に、次の要件を満たしていることを確認してください:

- Citrix Cloud のフルアクセス権限を有している。
- Windows PowerShell Integrated Scripting Environment（ISE）にアクセスできる。
- リンクする Citrix Cloud アカウントの顧客 ID がある。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有している。このベアラートークンを取得するには、CTX330675の指示に従います。Citrix Cloud アカウントをリンクするときに、この情報を入力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:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
20 <!--NeedCopy-->
```

2. 4行目で、CWSAuth bearer=XXXXXXXを CWSAuth 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 を繰り返して、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 が既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:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
       SpokeCustomerID"
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
12 <!--NeedCopy-->
```

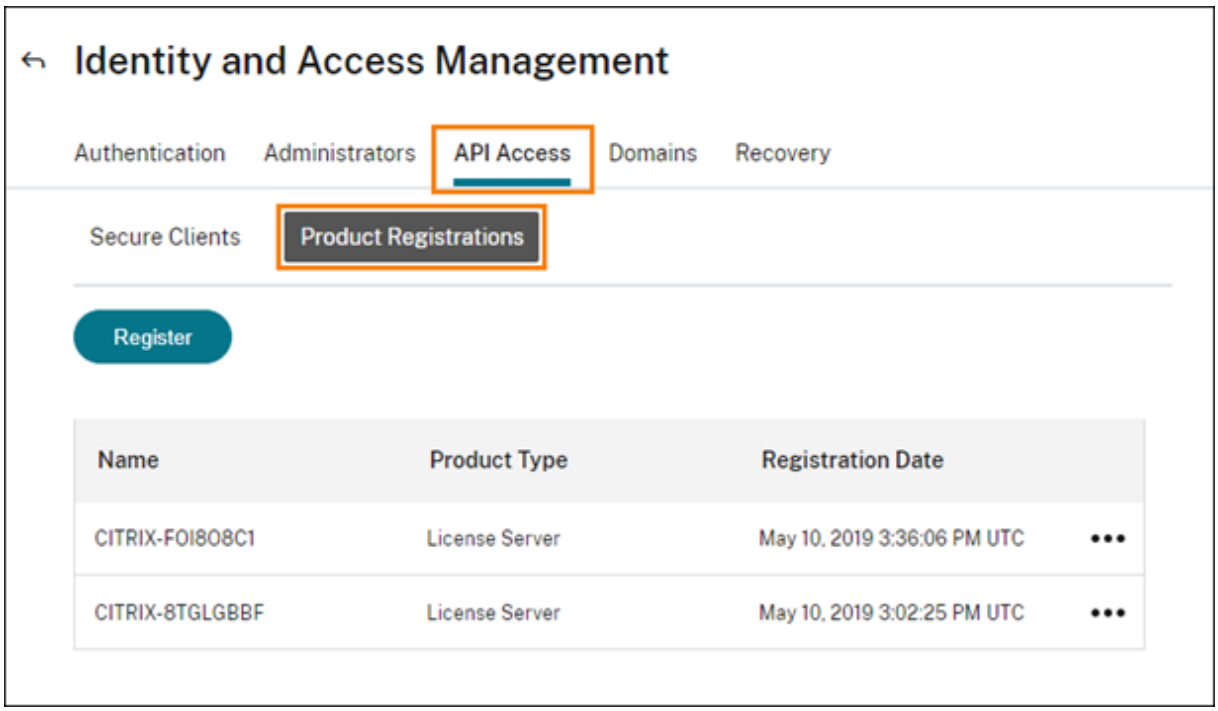
3. 4 行目で、`CWSAuth bearer=xxxxxxx1`を CWSAuth 値（例: `CWSAuth bearer=AbCdef123Ghik…`）に置き換えます。この値は、証明書キーに似た長いハッシュです。
4. 6 行目で、`HubCustomerID`をハブアカウントの顧客 ID に置き換えます。
5. 6 行目で、`SpokeCustomerID`をスポークアカウントの顧客 ID に置き換えます。
6. スクリプトを実行します。
7. 手順 4〜6 を繰り返して、追加のアカウントのリンクを解除します。

Citrix Cloud を使用するオンプレミス製品の登録

October 4, 2023

Citrix Cloud からの短いコードによるアクティブ化機能を使用して、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、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の実行中に、この 8 桁のコードが生成されます。製品がユーザーに登録を要求するとき、製品は Citrix Cloud からコードを要求して表示します。その後、Citrix Cloud でこのコードをコピーして貼り付けるか、手動で入力します。

登録後、[製品の登録] ページ（[**ID** およびアクセス管理] **>** [**API** アクセス] **>** [製品の登録]）に、登録された製品が存在するサーバーが表示されます。



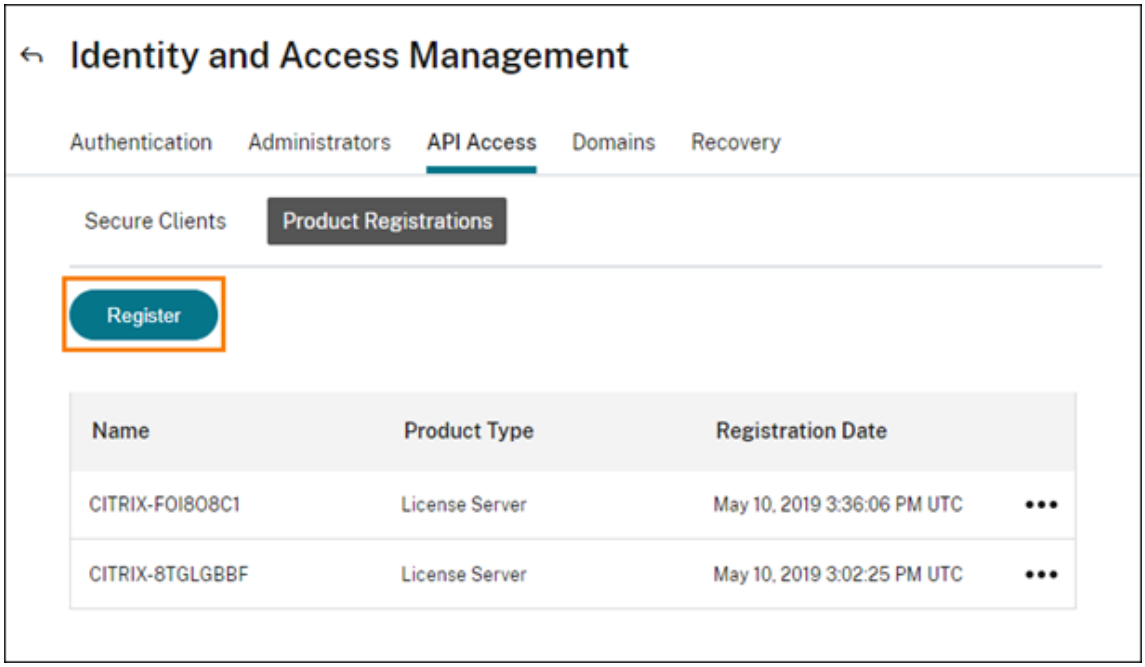
以下は、Citrix Cloud に登録できるオンプレミス製品です:

- クラウドサービス用の Citrix Connector Appliance
- Citrix フェデレーション認証サービス
- Citrix ライセンスサーバー
- Citrix Virtual Apps and Desktops（サイトを Citrix Analytics for Performance に登録する場合）

> 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、製品ごとのドキュメントを参照してください。

製品の登録

1. Citrix Cloud メニューで、[**ID** およびアクセス管理] を選択します。
2. [**API** アクセス] **>** [製品の登録] を選択して、[登録] を選択します。

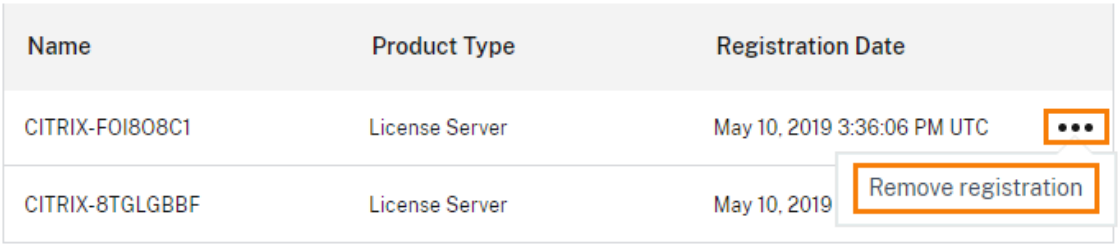


3. Citrix 製品の 8 文字の英数字コードを入力し、［続行］をクリックします。
4. 登録の詳細を確認してから、［登録］をクリックします。

製品登録の削除

環境から登録済みの Citrix 製品を実行しているサーバーを削除しても、製品登録ページにはこれらのサーバーが表示されます。サーバーを Citrix Cloud から削除するには、次の手順を実行します：必要に応じて後から製品を再度登録し、［製品登録］ページにサーバーを表示できます。

1. ［製品登録］ページで削除するサーバーを特定します。
2. 省略記号ボタンをクリックして、［登録を削除する］を選択します。



3. プロンプトが表示されたら、［削除］を選択します。

Active Directory を Citrix Cloud に接続する

July 2, 2024

Citrix Cloud は、オンプレミスの Active Directory（AD）を使用したワークスペース利用者の認証をサポートしています。また、一部のワークスペース認証方法では、Active Directory と Citrix Cloud 間の接続が必要です。詳しくは、「認証方法の選択または変更」を参照してください。

Citrix Cloud では、Active Directory を介して自分のワークスペースにサインインする利用者の認証の第 2 要素としてトークンを使用することをサポートしています。ワークスペースの利用者は、Citrix SSO などの時間ベースのワンタイムパスワード標準に従うアプリケーションを使用して、トークンを生成できます。

Active Directory とトークンを使用してワークスペースの利用者を認証する方法について詳しくは、「Active Directory+ トークン」を参照してください。

> ヒント：
>
> 「Citrix ID と認証の概要」教育コースで、サポートされている ID プロバイダーの詳細をご覧ください。「Planning Citrix Identity and Access Management」モジュールには、この ID プロバイダーを Citrix Cloud に接続して Citrix Workspace の認証を有効にする方法を説明した短い動画があります。

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。Cloud Connector または Connector Appliance のいずれかを Active Directory のコネクタとして使用できます。環境で使用するコネクタの種類を選択するには、次を参照してください：

- Active Directory での Cloud Connector 展開シナリオ
- Active Directory での Connector Appliance 展開シナリオ

Connector Appliance を使用した **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 の顧客や、一部のフォレストがユーザー認証にのみ使用される Citrix Virtual Apps and Desktops の顧客の場合。

詳しくは、「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実現するためには、少なくとも 2 つの Cloud Connector が必要です。詳しくは、次の記事を参照してください：

- Cloud Connector の技術詳細：システム要件と展開の推奨事項。
- Cloud Connector のインストール：グラフィカルインターフェイスまたはコマンドラインを使用したインストール手順。

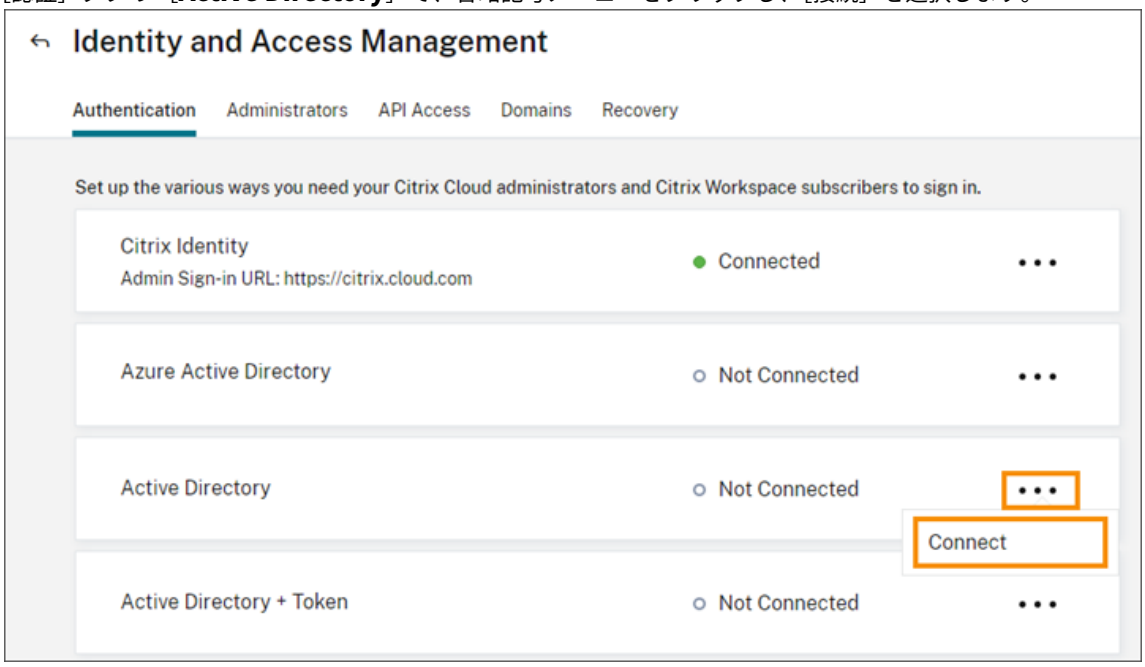
Active Directory を Citrix Cloud に接続するには、次の作業が必要です:

1. ドメインにCloud Connector をインストールします。可用性を高めるため、Cloud Connector を 2 つインストールすることを Citrix ではお勧めします。
2. 該当する場合は、ユーザーデバイスのトークンを有効にします。利用者は、一度に 1 つのデバイスしか登録できません。

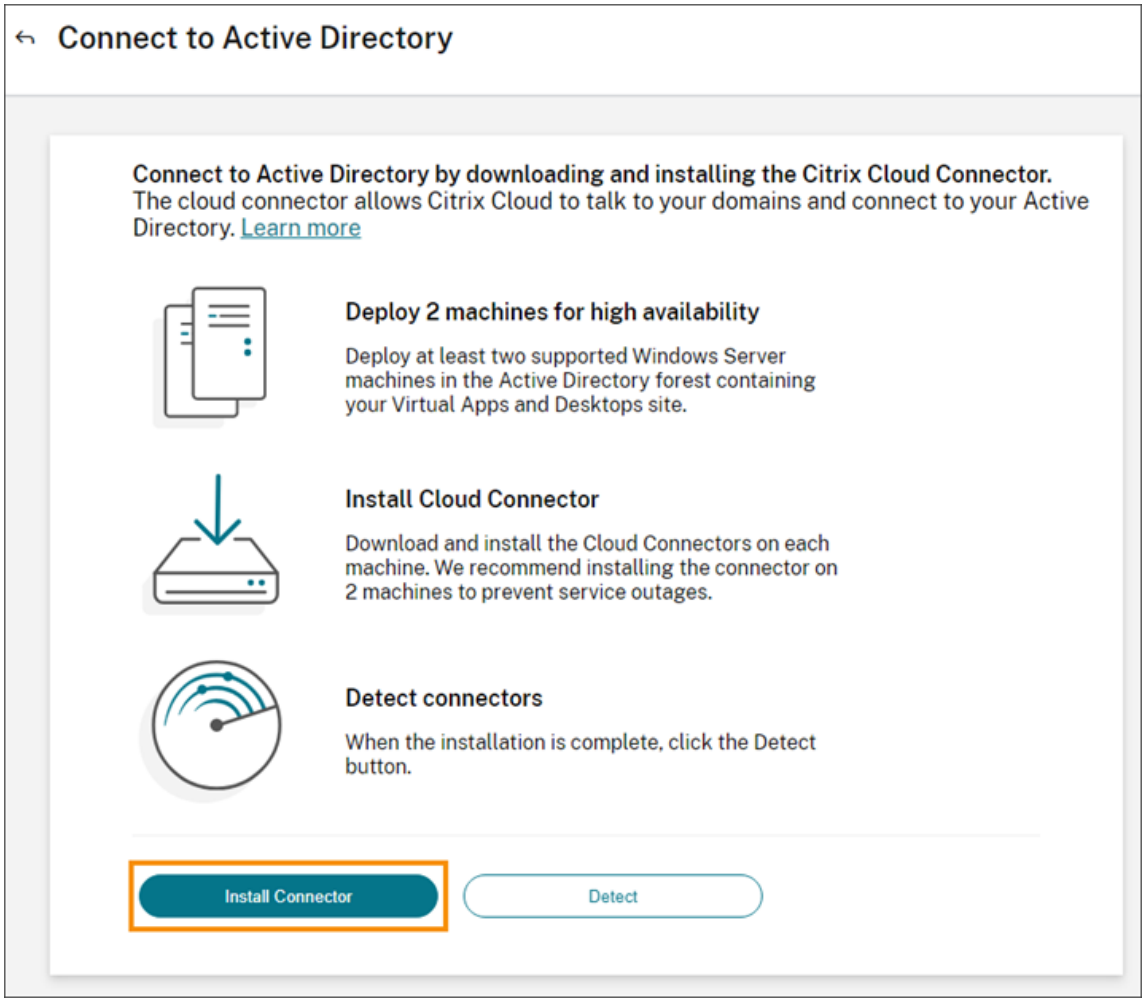
> 重要:
>
> Citrix DaaS で使用するために Cloud Connector を展開している場合、Cloud Connector の展開後に AD ドメインが登録され、アクティブになっていることを確認するために、追加の手順が必要になる場合があります。AD ドメインが Citrix Cloud でアクティブであることを確認すると、マシンカタログのセットアップがスムーズに行われます. Citrix DaaS の展開後の手順について詳しくは、Citrix DaaS 製品ドキュメントの「リソースの種類を追加するか、Citrix Cloud で未使用のドメインをアクティブ化する」を参照してください。

Active Directory を **Citrix Cloud** に接続するには

1. Citrix Cloud メニューで、[**ID** およびアクセス管理] を選択します。
2. [認証] タブの [**Active Directory**] で、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。

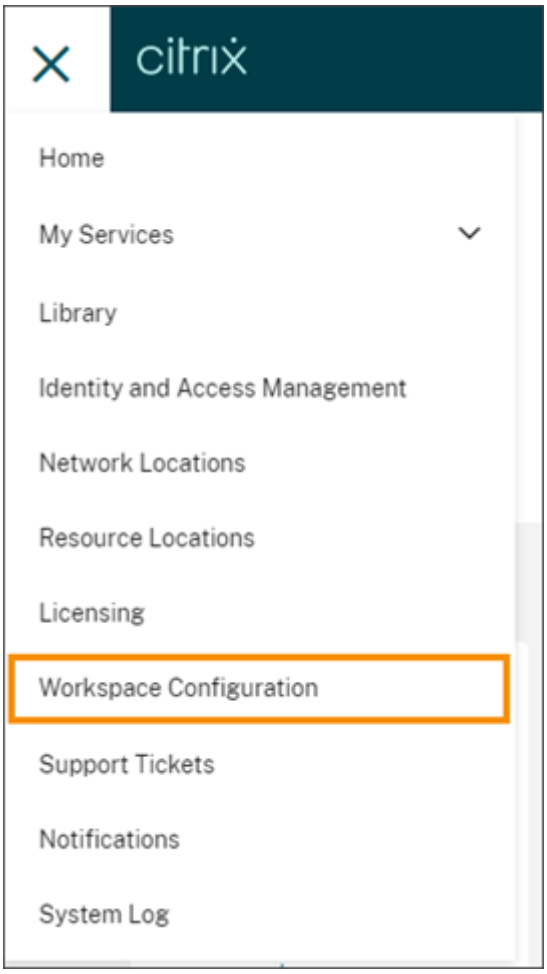


4. Cloud Connector インストーラーを起動し、インストールウィザードの指示に従って操作します。
5. [**Active Directory** に接続する] ページで、[検出] をクリックします。確認後、Citrix Cloud は Active Directory が接続されているというメッセージを表示します。
6. [認証に戻る] をクリックします。**Active Directory** エントリは、[認証] タブで [有効] とマークされます。

Active Directory+ トークン認証を有効にするには

1. Connector Appliance または Cloud Connector のいずれかを使用して、Active Directory を Citrix Cloud に接続します。
2. Citrix Cloud の [**ID** およびアクセス管理] セクションの [認証] タブで、**Active Directory** エントリが [有効] とマークされていることを確認します。
3. [次へ] をクリックします。[トークンの構成] ページが表示され、デフォルトで [単一のデバイス] オプションが選択されています。
4. [保存して終了] をクリックして、構成を完了します。[認証] タブで、[**Active Directory +** トークン] エントリが [有効] になっています。
5. ワークスペースのトークン認証を有効にします:

a) Citrix Cloud メニューから、［ワークスペース構成］を選択します。



b)［認証］タブで、［**Active Directory +** トークン］を選択します。

Active Directory とトークン認証を有効にしたあと、ワークスペースの利用者は自分のデバイスを登録し、認証アプリケーションを使用してトークンを生成できます。利用者は、一度に 1 つのデバイスしか登録できません。利用者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。

利用者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。

追加情報

Citrix Tech Zone:

- Tech Insight: 認証 - TOTP
- Tech Insight: 認証 - プッシュ

Azure Active Directory を Citrix Cloud に接続する

May 30, 2024

Citrix Cloud は、Azure Active Directory（AD）を使用した Citrix Cloud 管理者およびワークスペース利用者の認証をサポートしています。

Citrix Cloud で Azure AD を使用すると、次のことができるようになります:

- 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、必要に応じて簡単にアカウントを無効にできます。
- 多要素認証を構成して高レベルのセキュリティを実現し、盗まれたサインイン資格情報が使用される可能性を回避します。
- ブランド設定済みのログインページを使用するため、ユーザーは正しい場所にログインしていることを確認できます。
- ADFS、Okta、Ping などの任意の ID プロバイダーにフェデレーションを使用できます。

Azure AD アプリと権限

Citrix Cloud には Azure AD が含まれているため、アクティブな Azure AD セッションにログインする必要なく Azure AD に接続できます。このアプリの導入以降、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更新プログラムをリリースしました。

Citrix Cloud への既存の Azure AD 接続により、最新の更新済みアプリを使用する場合は、Citrix Cloud で Azure AD 接続を更新する必要があります。詳しくは、この記事の「アプリのアップデートに対応するため Azure AD 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ます。

Citrix Cloud が Azure AD との接続に使用する Azure AD アプリと権限について詳しくは、「Citrix Cloud 用の Azure Active Directory の権限」を参照してください。

> ヒント:
>
> 「Citrix ID と認証の概要」教育コースで、サポートされている ID プロバイダーの詳細をご覧ください。「Planning Citrix Identity and Access Management」モジュールには、この ID プロバイダーを Citrix Cloud に接続して Citrix Workspace の認証を有効にする方法を説明した短い動画があります。

Citrix Cloud アカウントが複数ある場合の認証

この記事では、ID プロバイダーとして Azure AD を単一の 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 アカウントがある場合は、それぞれを同じ Azure AD 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、カスタマーピッカーから適切なカスタマー ID を選択します。

2. 選択した顧客が Azure AD に初めて接続する顧客である場合は、この記事のすべての手順に従って、AD と Azure AD を同期し、顧客を Citrix Cloud に接続し、管理者を追加します。
3. 別の顧客に接続するには、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 Azure AD に接続する」の説明に従って、顧客を Azure AD に接続します。
5. 顧客 ID ごとに手順 3 と 4 を繰り返します。

Active Directory と **Azure AD** を準備する

Azure AD を使用する前に、次の要件を満たしていることを確認してください:

- Microsoft Azure アカウントを持っている。すべての Azure アカウントに無料の Azure AD が付属しています。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に登録してください。
- Azure AD にはグローバル管理者の役割があります。この役割は、Citrix Cloud が Azure AD と接続できるようにするために必要です。
- 管理者アカウントには、Azure AD で構成された「mail」プロパティがあります。Microsoft のAzure AD Connectツールを使用することで、オンプレミスの Active Directory アカウントを Azure AD と同期させることができます。または、Office 365 のメールで同期されていない Azure AD アカウントを構成することもできます。

Azure AD Connect でアカウントを同期する

1. Active Directory アカウントにメールの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) **Users** フォルダーで、確認するアカウントを見つけて右クリックし、［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、Azure AD から追加された管理者には、Citrix がホストする 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が必要です。
2. Azure AD Connect をインストールおよび構成します。詳しい手順については、Microsoft Azure Web サイトの「簡単設定を使用した Azure AD Connect の開始」を参照してください。

Citrix Cloud を **Azure AD** に接続する

Citrix Cloud アカウントを Azure AD に接続する場合、Azure AD のユーザーの基本プロファイルのほか、ユーザープロファイル（またはサインインユーザーのプロファイル）へのアクセス権限が必要です。Citrix はこの権限を要求し、（管理者の）名前とメールアドレスを取得して、管理者が後で他のユーザーを管理者として追加することができるようにします。Citrix Cloud が要求するアプリ権限について詳しくは、「Citrix Cloud 用の Azure Active Directory の権限」を参照してください。

> 重要:
>
> このタスクを完了するには、自分が Azure AD のグローバル管理者であるか、Citrix Cloud にサインインする前にグローバル管理者に前提条件を満たすよう依頼する必要があります。

1. ページの左上隅にあるメニューをクリックし、[**ID** およびアクセス管理] を選択します。
2. Azure Active Directory を見つけ、省略記号メニューから [接続] を選択します。
3. 入力画面が表示されたら、URL に適した短い会社の識別子を入力し、[接続] をクリックします。この識別子は、Citrix Cloud 内でグローバルに一意である必要があります。
4. 入力画面が表示されたら、接続する Azure アカウントにサインインします。Azure は、Citrix Cloud がアカウントにアクセスして接続に必要な情報を取得するためのアクセス権限を表示します。これらの権限のほとんどは読み取り専用であり、この権限により Citrix Cloud でグループやユーザープロファイルなどの基本情報を Microsoft Graph から収集できます。Citrix Endpoint Management または XenMobile Server を Microsoft Intune と統合した場合、Microsoft Intune 関連の読み取り/書き込み権限を付与する必要があります。詳しくは、「Citrix Cloud 用の Azure Active Directory の権限」を参照してください。
5. [承諾] をクリックして権限の要求を承諾します。

代替の接続方法

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 Azure AD（Entra ID）アプリを作成する。
2. Citrix Cloud で Azure AD（Entra ID）アプリに Citrix Cloud を接続する。

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 を作成する必要があります。詳しくは、「テナント全体の管理者の同意を付与するための URL を作成する」を参照してください。

これは構築された URL の説明です。

```
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。

Azure AD から **Citrix Cloud** に管理者を追加する

Citrix Cloud では、管理者を個別に追加、または Azure AD グループとして追加できます。

Azure AD から個々の管理者を追加する方法については、「管理者のアクセスを管理する」を参照してください。

Azure AD 管理者グループを Citrix Cloud に追加する方法については、「管理者グループを管理する」を参照してください。

Azure AD を使用して **Citrix Cloud** にサインインする

Azure AD ユーザーアカウントの接続後、ユーザーは次のいずれかの方法で Citrix Cloud にサインインできます:

- 会社の Azure AD ID プロバイダーを最初に接続した時に構成した管理者のサインイン URL に移動します。例: `https://citrix.cloud.com/go/mycompany`
- Citrix Cloud のサインインページで、［会社の資格情報でサインイン］をクリックし、最初に Azure AD を接続した時に作成した識別子（「mycompany」など）を入力し、［続行］をクリックします。

ワークスペースの **Azure AD** 認証を有効にする

Azure AD を Citrix Cloud に接続すると、Azure AD 経由で自分のワークスペースに認証する許可を利用者に付与できます。

> 重要:
>
> Azure AD ワークスペース認証を有効にする前に、ワークスペースで Azure AD を使用するための考慮事項について「Azure Active Directory」セクションで確認してください。

1. Citrix Cloud コンソールで左上隅のメニューボタンをクリックし、［ワークスペース構成］を選択します。
2. ［認証］タブで、［**Azure Active Directory**］を選択します。
3. ［確認］をクリックして Azure AD 認証を有効にした場合のワークスペース環境の変更を承諾します。

高度な **Azure AD** 機能を有効にする

Azure AD は、高度な多要素認証、国際的レベルのセキュリティ機能、20 種類の ID プロバイダーとのフェデレーション、セルフサービスパスワードの変更とリセットなどの機能を提供します。Azure AD ユーザーでこれらの機能を有効にすると、Citrix Cloud が自動的に活用できるようになります。

Azure AD サービスレベルの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。

アプリのアップデートに対応するため **Azure AD** に再接続する

Citrix Cloud には Azure AD が含まれているため、アクティブな Azure AD セッションにログインする必要なく Azure AD に接続できます。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 月に、アプリが更新されてパフォーマンスが向上し、今後のリリースにも対応できるようになりました。
- 2019 年 5 月に、アプリが更新され、Citrix Cloud へのAzure AD 管理者グループの追加がサポートされるようになりました。

- 2022 年 4 月に、アプリが更新され、Group.Read.All 権限の代わりに GroupMember.Read.All 権限を使用するようになりました。

これらの更新プログラムがリリースされる前に Azure AD を Citrix Cloud に接続しており、最新の更新済みアプリを使用する場合は、Azure AD を Citrix Cloud から切断してから、再接続する必要があります。最新のアプリの使用は任意です。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

Azure AD 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 プロバイダーのフルアクセス権限を持つ管理者である必要があります。Azure AD の資格情報を使用して 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する管理者がいない場合は、一時的にアカウントを追加して、Azure AD に再接続したあとにそのアカウントを削除できます。手順については、「個別の管理者を招待する」を参照してください。
- Azure AD を使用してワークスペース利用者を認証している場合は、一時的に別の ID プロバイダーを選択します。Azure AD が Citrix Workspace の認証方法としても使用されている場合、Citrix Cloud では Azure AD を切断できません。詳しくは、Citrix Workspace 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。

Azure AD を再接続するには

1. Citrix ID プロバイダーのフルアクセス権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. **Azure Active Directory** 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. 省略記号メニューの [接続] を選択します。

> 注:
>
> 手順 3 で説明したように Azure Active Directory を切断する場合、Citrix Cloud は管理者にこの ID プロバイダーのすべての管理者プロファイルを削除するように要求します。
> この手間を省くために、管理者は以下の手順に従って Azure AD の ID プロバイダーに再接続できます。
>
> 1. グローバル管理者として、Azure に移動して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] タブで、Azure AD がまだ接続されていることがわかります。
> 3. Citrix Cloud で Azure AD の新しい管理者を追加します。
>
> これにより、管理者を削除せずにアプリの再作成と再接続がトリガーされます。

Citrix Cloud 用の Azure Active Directory の権限

December 14, 2023

この記事では、Azure Active Directory（AD）を接続して使用するときに Citrix Cloud が要求する権限について説明します。Citrix Cloud アカウントで Azure AD がどのように使用されるかによって、ターゲットの Azure AD テナントに 1 つまたは複数のエンタープライズアプリケーションが作成されることがあります。アカウントごとにアプリケーションのセットを作成しなくても、複数の Citrix Cloud アカウントを 1 つの Azure AD テナントに接続し、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:
>
> 2022 年 4 月、Citrix Cloud が Azure AD の接続のために使用する Azure AD アプリは、Group.Read.All 権限の代わりに GroupMember.Read.All 権限を使用するように更新されました。既存の（2022 年 4 月より前の）Azure AD 接続により、アプリで新しい権限を使用する場合は、Azure AD を切断してから Citrix Cloud に再接続する必要があります。この操作により、Citrix Cloud で最新の Azure AD アプリが使用されるようになります。詳しくは、「アプリのアップグレードに対応するため Azure AD 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ます。

エンタープライズアプリケーション

次の表では、Citrix Cloud で Azure AD の接続時および使用時に使用される Azure AD 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。

Name	アプリケーション ID	使用状況
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	ワークスペース利用者ログイン
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Azure AD と Citrix Cloud 間のデフォルト接続
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	管理者の招待とログイン
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Citrix Endpoint Management を使用した Azure AD と Citrix Cloud 間のデフォルトの接続
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Citrix Endpoint Management を使用した Azure AD と Citrix Cloud 間の従来の接続

アクセス権

Citrix Cloud のエンタープライズアプリケーションの権限があれば、Citrix Cloud は Azure AD 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、Azure AD テナントに接続する、管理者が専用のサインイン URL を使用して Citrix Cloud にサインインする、Azure AD テナントと Endpoint Management を接続するなど、特定の機能を実行します。Citrix Cloud がこれらのデータにアクセスするには、管理者の同意が必要です。これらのアクセス権限は、Citrix Cloud が Azure AD と連携するための必要最低限の特権です。Azure AD の権限と同意について詳しくは、Microsoft Azure ドキュメント Web サイトの「Microsoft ID プラットフォームでのアクセス許可と同意」を参照してください。

本記事では、Azure AD アプリケーション権限の各セットについて次の情報を記載しています:

- **API** 名: Citrix Cloud が権限を要求するリソースアプリケーション。Microsoft Graph と Windows Azure Active Directory のことです。Citrix Cloud は、この 2 つのリソースアプリケーションに同じ権限を要求します。
- タイプ: Citrix Cloud が特定の権限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権限には、次のいずれかのアクセスレベルを設定できます:
  - 委任権限は、ユーザーのプロファイルを照会する場合など、サインインユーザーの代理として操作するために使用されます。
  - アプリケーション権限 は、特定のグループ内のユーザーを照会する場合など、ユーザー不在でアプリケーションが操作を実行するときに使用されます。この種類の権限を付与するには、Azure AD のグローバル管理者の同意が必要です。
- 要求値: Azure AD が特定の権限に割り当てる情報の文字列。特定のエンタープライズアプリケーションの権限には、次のいずれかの要求値を設定できます:
  - **User.Read**: Citrix Cloud 管理者が、接続された Azure AD 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。これは User.Read.All のサブセットですが、下位互換性のために権限自体は残ります。
  - **User.Read.All**: Citrix Cloud は、Microsoft Graph のList usersを呼び出して、顧客が接続した Azure AD からユーザーを参照および選択できるようにします。たとえば、Azure AD のユーザーに対し、ワークスペースを使用した Citrix DaaS リソースへのアクセス権限を付与できます。Citrix Cloud は、`onPremisesSecurityIdentifier`などの基本プロファイル以外のプロパティ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 のList groupsを呼び出して、顧客が接続した Azure AD からグループを参照および選択できるようにします。たとえば、Azure AD のグループに対しては、Citrix DaaS アプリケーションへのアクセス権限を付与することもできます。
  - **Directory.Read.All**: Citrix Cloud は、Microsoft Graph のList memberOfを呼び出して、ユーザーのグループメンバーシップを取得します（`Groups.Read.All`では不十分な場合）。
  - **DeviceManagementApps.ReadWrite.All**: Microsoft Intune によって管理されるプロパティ、グループ割り当て、アプリの状態、アプリの設定、およびアプリ保護ポリシーの読み取りと書き込みを、

Citrix Cloud が行えるようにします。
- **Directory.AccessAsUser.All**：サインインユーザーと同じように、Citrix Cloud がディレクトリ内の情報にアクセスできるようにします。

> 注：
>
> **Directory.Read.All** は、**Endpoint Management** を使用した **Azure AD** と **Citrix Cloud** 間のデフォルトの接続にのみ適用できます。

ワークスペース利用者ログイン

この Citrix Cloud アプリケーション（ID：e95c4605-aeab-48d9-9c36-1a262ef8048e）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任版

Azure AD 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、次の権限を使用します：

API 名	要求値	権限	種類
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	委任版
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任版
Microsoft Graph	User.Read.All	すべてのユーザーの完全なプロファイルの読み取り	委任版
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任版
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	アプリケーション
Microsoft Graph	User.Read.All	すべてのユーザーの完全なプロファイルの読み取り	アプリケーション
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	アプリケーション

管理者の招待とログイン

この Citrix Cloud アプリケーション（ID：1b32f261-b20c-4399-8368-c8f0092b4470）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任版
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任版

Endpoint Management を使用した **Azure AD** と **Citrix Cloud** 間のデフォルトの接続

この Citrix Cloud アプリケーション（ID：5c913119-2257-4316-9994-5e8f3832265b）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	委任版
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任版
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任版
Microsoft Graph	Directory.Read.All	ディレクトリデータの読み取り	アプリケーション
Microsoft Graph	Directory.Read.All	ディレクトリデータの読み取り	委任版
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune アプリの読み取りと書き込み	委任版
Microsoft Graph	Directory.AccessAsUser.All	ディレクトリに対するサインインしたユーザーと同じアクセス	委任版

Endpoint Management を使用した **Azure AD** と **Citrix Cloud** 間の従来の接続

この Citrix Cloud アプリケーション（ID：e067934c-b52d-4e92-b1ca-70700bd1124e）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	委任版
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任版
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任版
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune アプリの読み取りと書き込み	委任版
Microsoft Graph	Directory.AccessAsUser.All	ディレクトリに対するサインインしたユーザーと同じアクセス	委任版

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

July 2, 2024

Citrix Cloud では、オンプレミスの Citrix Gateway を ID プロバイダーとして使用してワークスペースにサインインする利用者が認証されるようにできます。

Citrix Gateway 認証を使用すると、以下のことを実行できます:

- 引き続き、既存の Citrix Gateway でユーザーを認証するため、Citrix Workspace 経由でオンプレミスの Virtual Apps and Desktops のリソースにアクセスできます。
- Citrix Workspace で Citrix Gateway の認証、承認、および監査（AAA: authentication, authorization, and auditing）機能を使用します。
- 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、その他多くの機能を使用しながら、ユーザーに必要なリソースへの Citrix Workspace 経由のアクセスを提供できます。

> ヒント:
>
> 「Citrix ID と認証の概要」教育コースで、サポートされている ID プロバイダーの詳細をご覧ください。「Planning Citrix Identity and Access Management」モジュールには、この ID プロバイダーを Citrix Cloud に接続して Citrix Workspace の認証を有効にする方法を説明した短い動画があります。

サポートされるバージョン

Citrix Gateway 認証は、次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 Edition 以降
- Citrix Gateway 13.0 41.20 Advanced Edition 以降

前提条件

Cloud Connector

Citrix Cloud Connector ソフトウェアのインストール先となる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、次の要件を満たしている必要があります:

- 「Citrix Cloud Connector の技術詳細」に記載されているシステム要件を満たしている。
- 他の Citrix コンポーネントは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不可欠なマシンでもない。
- サイトが存在するドメインに参加している。ユーザーが複数のドメインにあるサイトのアプリケーションにアクセスする場合は、各ドメインに Cloud Connector を少なくとも 2 つインストールする必要があります。
- サイトに接続可能なネットワークに接続している。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。
- Citrix Cloud との高可用性接続を実現するためには、少なくとも 2 つの Cloud Connector が必要です。インストール後、Citrix Cloud は Cloud Connector によりサイトを検出して通信できるようになります。

Cloud Connector のインストール手順について詳しくは、「Cloud Connector のインストール」を参照してください。

Active Directory

Citrix Gateway 認証を有効にする前に、次のタスクを実行します:

- ワークスペース利用者に Active Directory（AD）のユーザーアカウントがあることを確認します。AD アカウントがない利用者は、ワークスペースにサインインできません。
- 利用者の 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 では、利用者がサインインする際、ユーザーコンテキストを決定するためにこれらのプロパティが必要とされます。これらのプロパティが入力されていないと、利用者がワークスペース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 Connector」セクションの説明に従い、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 により、Citrix Cloud がオンプレミス環境と通信できるようになります。手順については、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。
- Citrix Gateway 認証を使用してフェデレーションを実行している場合、AD ユーザーをフェデレーションプロバイダーと同期します。Citrix Cloud では、サインインするワークスペース利用者の AD ユーザー属性が必要とされます。

要件

Citrix Gateway の拡張ポリシー

Citrix Gateway 認証では、クラシックポリシーが廃止されたため、オンプレミス Gateway の拡張ポリシーを使用する必要があります。拡張ポリシーでは、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）がサポートされています。現在クラシックポリシーを使用している場合、Citrix Cloud で Citrix Gateway 認証を使用するには、新しい拡張ポリシーを作成する必要があります。拡張ポリシーを作成する際に、クラシックポリシーのアクション部分を再利用できます。

署名用証明書

Citrix Workspace の利用者を認証するために 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、デジタル署名トークンが含まれます。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、公的証明機関（CA）から発行される必要があります。私的 CA が発行した証明書は使用できません。Citrix Cloud に私的な CA 証明書を提供する手段がないためです。そのため、信頼できる証明書チェーンを確立できません。署名用の証明書を複数構成する場合、各メッセージでこれらのキーがローテーションされます。

キーを **VPN** グローバルにバインドする必要がありますこれらのキーがないと、利用者はサインイン後にワークスペース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ているため、Gateway は NTP 時間に同期される必要があります。クロックが同期されていない場合、Citrix Cloud でのトークンの有効性チェックでトークンが古いと判断されます。

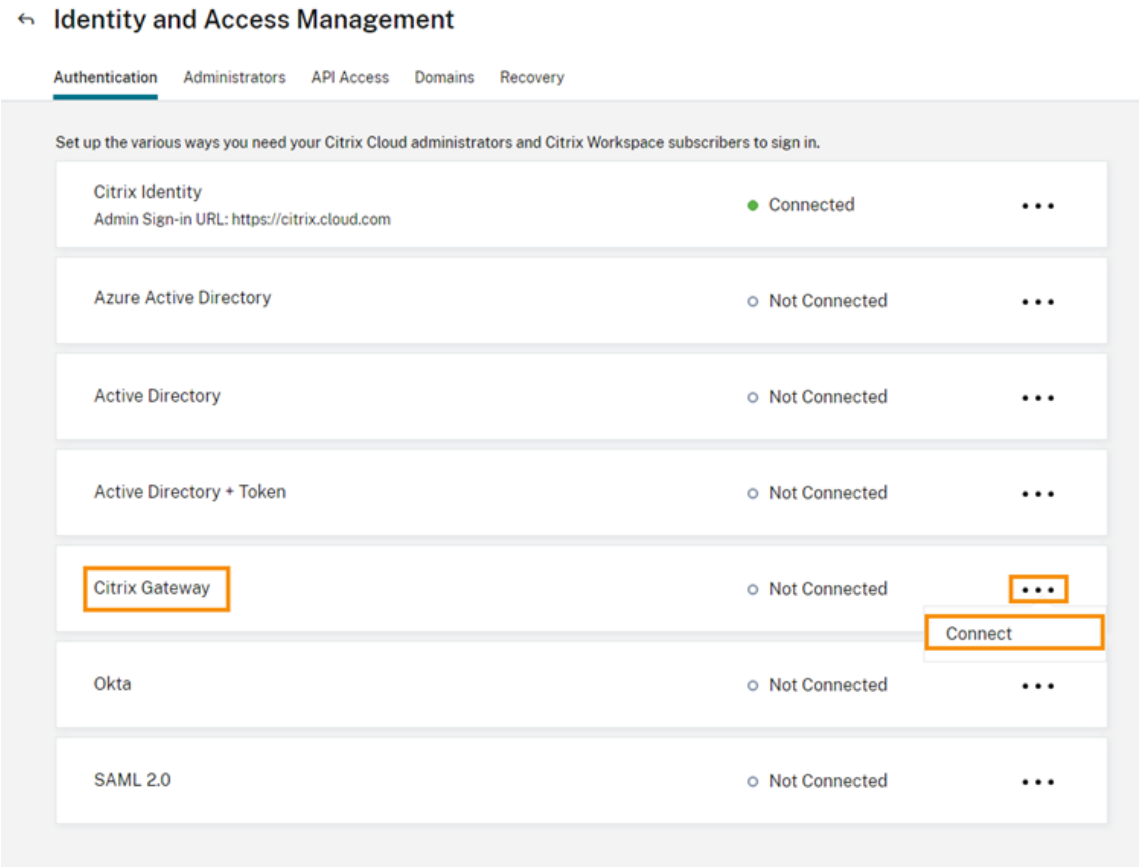
タスクの概要

Citrix Gateway 認証を設定するには、次のタスクを実行します：

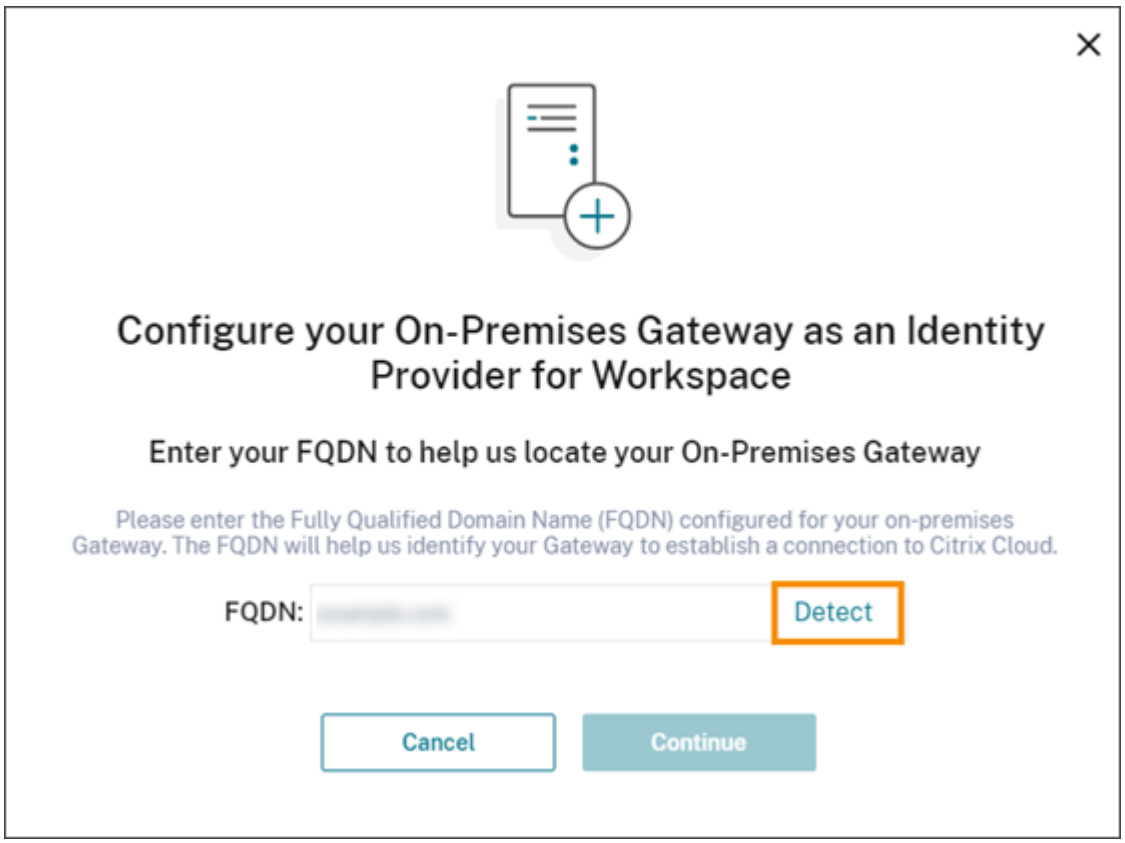
1. ［**ID** およびアクセス管理］で Gateway への接続を構成します。この手順では、Gateway のクライアント ID、シークレット、リダイレクト URL を生成します。
2. Gateway で、Citrix Cloud から生成された情報を使用して OAuth ID プロバイダー拡張ポリシーを作成します。これにより Citrix Cloud がオンプレミス Gateway に接続できるようになります。手順については、以下の記事を参照してください。
   - Citrix Gateway 12.1：オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
   - Citrix Gateway 13.0：オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
3. ［ワークスペース構成］で、利用者の Citrix Gateway 認証を有効にします。

ワークスペース利用者の **Citrix Gateway** 認証を有効にするには

1. Citrix Cloud メニューで、［**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。



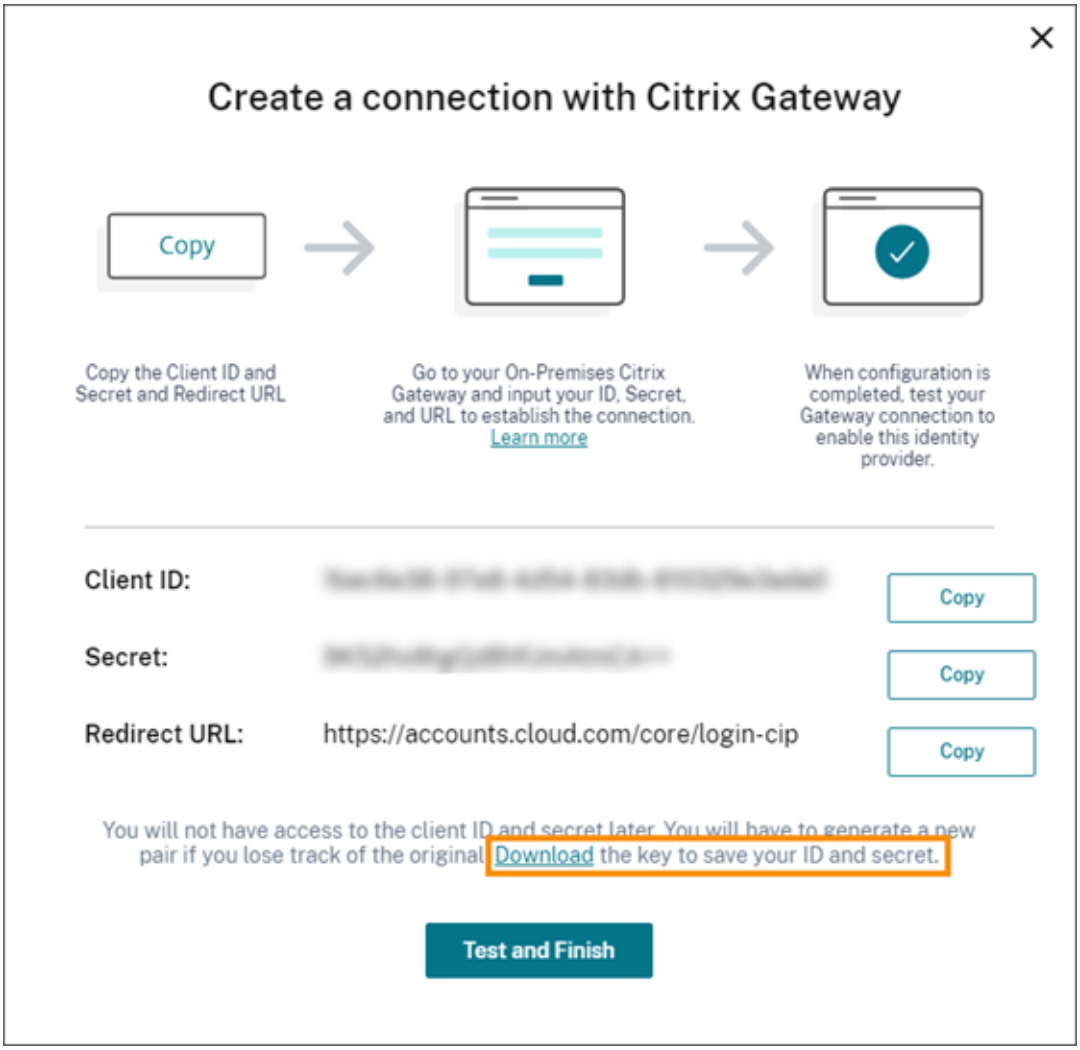
3. オンプレミス Gateway の完全修飾ドメイン名を入力して ［検出］をクリックします。



Citrix Cloud が正常に FQDN を検出したら、［続行］をクリックします。

4. オンプレミス Gateway との接続を作成します:

   a) Citrix Cloud で表示されるクライアント ID、シークレット、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、参照用としてオフラインで安全に保存します。この情報は生成後、Citrix Cloud で表示することはできなくなります。

b) Gateway で、Citrix Cloud のクライアント ID、シークレット、リダイレクト URL を使用して OAUth ID プロバイダー拡張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 Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
- Citrix Gateway 13.0 の場合：オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用

c) ［テストして終了］をクリックします。Citrix Cloud は、Gateway が到達可能であり、正しく構成されていることを確認します。

5. ワークスペースの Citrix Gateway 認証を有効にするには：

a) Citrix Cloud メニューから、［ワークスペース構成］を選択します。
b) ［認証］タブで ［**Citrix Gateway**］を選択します。
c) ［利用者のエクスペリエンスに与える影響を了承しています］を選択して ［保存］をクリックします。

トラブルシューティング

最初の手順として、この記事の「前提条件」および「要件」セクションを確認します。オンプレミス環境に必要なコンポーネントがすべて揃っており、必要な構成をすべて行ったことを確認してください。これらのアイテムのいずれかが欠落しているか、正しく構成されていないと、Citrix Gateway でのワークスペース認証が機能しません。

Citrix Cloud とオンプレミスの Gateway との間で接続の問題が発生した場合、以下の事項を確認してください:

- Gateway の完全修飾ドメイン名がインターネットで到達可能である。
- Citrix Cloud で Gateway の完全修飾ドメイン名を正しく入力した。
- OAuth ID プロバイダーポリシーの`-issuer`パラメーターに Gateway の URL を正しく入力した。例: `-issuer https://GatewayFQDN.com`。`issuer`パラメーターでは大文字と小文字は区別されません。
- Citrix Cloud のクライアント ID、シークレット、リダイレクト URL の値が、OAuth ID プロバイダーポリシーの［クライアント ID］［クライアントシークレット］、［リダイレクト URL］、［オーディエンス］フィールドに正しく入力されている。ポリシーの［オーディエンス］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ます。
- OAuth ID プロバイダー認証ポリシーが正しく構成されている。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 Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
  - Citrix Gateway 13.0: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
- ポリシーが「認証ポリシーのバインド」に記載されている手順で、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ます。

グローバルカタログサーバー

Gateway は、ユーザーアカウントの詳細に加えて、ユーザーのドメイン名、Active Directory の NETBIOS 名、およびルート Active Directory ドメイン名を取得します。Active Directory の 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 Active Directory を検索します。NETBIOS 名はグローバルカタログサーバーに複製されません。

Active Directory 環境でグローバルカタログサーバーを使用する場合、これらのサーバーで構成された LDAP アクションは Citrix Cloud で機能しません。代わりに、LDAP アクションで個別の Active Directory 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、複数の LDAP ポリシーを構成できます。

Kerberos または **ID** プロバイダーチェーンを使用したシングルサインオンの **Active Directory** 検索

Kerberos か、利用者のサインインに SAML または OIDC プロトコルを使用するまたは外部 ID プロバイダーを使用する場合、Active Directory 参照が構成されていることを確認します。Gateway では、利用者の Active Directory ユーザープロパティと Active Directory 構成プロパティを取得するために Active Directory 参照が必要です。

認証がサードパーティの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、以下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 の認証要素を追加します:

1. Active Directory から属性および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 拡張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 プロバイダーのあとの次の要素として認証ポリシーラベルを定義します。

LDAP を第 **2** の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) [**System**] > [**Authentication**] > [**Basic Policies**] > [**LDAP**] > [**Servers**] > [**Add**] 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**] でサーバーのフレンドリ名を入力します。
        - [**Server IP**] を選択してから 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オンにしないでください。この認証サーバーは、Active Directory からユーザー属性とグループを抽出するだけで認証用ではないので、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**] で、**UserPrincipalName** を選択します。
        - [**Group Attribute**] で **memberOf** を選択します。
        - [**Sub Attribute Name**] で **cn** を選択します。
2. LDAP 拡張認証ポリシーを作成します。
    a) [**Security**] > [**AAA - Application Traffic**] > [**Policies**] > [**Authentication**] > [**Advanced Policies**] > [**Policy**] > [**Add**] 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**] でポリシーのフレンドリ名を入力します。
        - [**Action Type**] で [**LDAP**] を選択します。
        - [**Action**] で作成済みの LDAP 認証サーバーを選択します。
        - [**Expression**] で **TRUE** と入力します。
    c) [作成] をクリックしてこの構成を保存します。
3. 認証ポリシーラベルを作成します:

a) [**Security**] > [**AAA - Application Traffic**] > [**Policies**] > [**Authentication**] > [**Advanced Policies**] > [**Policy Label**] > [**Add**] を選択します。
b) [**Name**] で認証ポリシーラベルのフレンドリ名を入力します。
c) ログインスキーマで **LSCHEMA_INT** を選択します。
d) [**Policy Binding**] の [**Select Policy**] で、作成済みの LDAP 拡張認証ポリシーを選択します。
e) [**GoTo Expression**] で **END** を選択します。
f) [**Bind**] をクリックして、構成を完了します。

4. LDAP 認証ポリシーラベルをプライマリ ID プロバイダーの次の要素として定義します:

a) [**System**] > [**Security**] > [**AAA - Application Traffic**] > [**Virtual Servers**] 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て、[**Edit**] を選択します。
c) [**Advanced Authentication Policies**] 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て、[**Edit Binding**] を選択します。
e) [**Policy Binding**] ページの [**Select Next Factor**] で、作成済みの LDAP 拡張認証ポリシーを選択します。
f) [**Bind**] をクリックして、構成を保存します。

多要素認証のデフォルトパスワード

ワークスペース利用者に多要素認証（MFA）を使用する場合、Gateway ではシングルサインオンのデフォルトパスワードとして最後の要素のパスワードが使用されます。このパスワードは、利用者がワークスペースにサインインする際に 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 に送信されるデフォルトパスワードとして LDAP パスワードを構成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。

追加情報

Citrix Tech Zone: Tech Insight: 認証 - Gateway

Google Cloud Identity を ID プロバイダーとして Citrix Cloud に接続する

October 4, 2023

Citrix Cloud では、ワークスペースにサインインする利用者を認証するための ID プロバイダーとして、Google Cloud Identity を使用できます。組織の Google アカウントを Citrix Cloud に接続することにより、Citrix Workspace と Google のリソースへのサインイン操作を統合できます。

ドメイン参加の構成とドメイン非参加の構成の要件

ドメイン参加のマシンまたはドメイン非参加のマシンを使用して、Google Cloud Identity を Citrix Cloud の ID プロバイダーとして構成できます。

- ドメイン参加とは、マシンがオンプレミスの Active Directory（AD）のドメインに参加し、認証ではそこに格納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。
- ドメイン非参加とは、マシンが AD ドメインに参加せず、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ます）が認証に使用されることを意味します。

次の表に、構成の種類別の要件を示します。

条件	ドメイン参加	ドメイン非参加	追加情報
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。Cloud Connector は、ドメイン非参加のマシンにアクセスする必要はありません。	この記事の「Active Directory と Citrix Cloud Connector の準備」。
AD と Google Cloud との同期	Gateway サービスを使用し、他のサービスを使用しない場合のみオプションです。それ以外の場合は、このタスクは必須です。	いいえ	この記事の「Active Directory と Google Cloud Identity との同期」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を作成し、Admin SDK API を有効にするために使用します。	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を構成」を参照してください。

条件	ドメイン参加	ドメイン非参加	追加情報
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」と「読み取り専用の API ユーザーアカウントを追加する」を参照してください。

Citrix Cloud アカウントが複数ある場合の認証

この記事では、ID プロバイダーとしての Google Cloud Identity を単一の 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、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、個々の Citrix Cloud アカウントを同一の Google Cloud アカウントに接続できます。Citrix Cloud にサインインし、カスタマーピッカーから適切なカスタマー ID を選択するだけです。

Active Directory と **Citrix Cloud Connector** の準備

ドメイン参加のマシンで Google Cloud Identity を使用している場合は、このセクションを参照してオンプレミス AD を準備します。ドメイン非参加のマシンを使用している場合は、スキップしてこの記事の「サービスアカウントの作成」に進んでください。

Active Directory ドメインで、Citrix Cloud Connector ソフトウェアのインストール先となるサーバーが少なくとも 2 台必要です。Cloud Connector は、Citrix Cloud とリソースの場所との間で通信するために必要です。Citrix Cloud との高可用性接続を実現するためには、少なくとも 2 つの 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:

- 「Citrix Cloud Connector の技術詳細」に記載されている要件を満たしている。
- 他の Citrix コンポーネントは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不可欠なマシンでもない。
- Active Directory（AD）ドメインに参加している。ワークスペース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 Cloud Connector を少なくとも 2 つ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 展開シナリオ」を参照してください。
- ユーザーが Citrix Workspace を介してアクセスするリソースにアクセスできるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。

Cloud Connector のインストール手順について詳しくは、「Cloud Connector のインストール」を参照してください。

Active Directory と **Google Cloud Identity** との同期

ドメイン参加のマシンで Google Cloud Identity を使用している場合は、このセクションを参照してオンプレミス AD を準備します。ドメイン非参加のマシンを使用している場合は、スキップしてこの記事の「サービスアカウントの作成」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、Active Derectory と Google Cloud Identity の同期はオプションです。これらのサービスだけなら、Active Derectory と同期しなくても 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は、Active Derectory を Google Cloud Identity と同期する必要があります。Google Cloud は、次の Active Derectory 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 Web サイトからGoogle Cloud Directory Sync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について詳しくは、Google Web サイトの「Google Cloud Directory Sync」の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、設定マネージャーを起動します（[スタート] **>** [設定マネージャー]）。
3. ユーティリティドキュメントの「設定マネージャーを使用した同期の設定」の説明に従って、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構成します。必要な情報を、大文字と小文字およびスペルをこのセクションに記載されているものと完全に一致させて入力します。

    a) [**Custom Schemas**] タブを選択して、[**Add Schema**] を選択します。
    b) ** [Use rules defined in < ユーザーアカウント名 >] ** を選択します。ユーザーアカウント名 >
    c) [**Schema Name**] に、「**citrix-schema**」と入力します。
    d) [**Add Field**] を選択して、次の情報を入力します:
        - [**Schema field template**] の [**Schema Field**] で、[**userPrincipalName**] を選択します。
        - [**Google field details**] の [**Field Name**] に、「**UPN**」と入力します。
    e) 手順 4 を繰り返して、次のフィールドを作成します:
        - objectGUID: [**Schema field template**] で、[**objectGUID**] を選択します。[**Google field details**] に、「**objectGUID**」と入力します。
        - SID: [**Schema field template**] で、[**Custom**] を選択します。[**Google field details**] に、「**SID**」と入力します。
        - objectSID: [**Schema field template**] で、[**Custom**] を選択します。[**Google field details**] に、「**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. ユーティリティドキュメントの「設定マネージャーを使用した同期の設定」の説明に従って、組織の残りの設定の構成を完了し、同期設定を確認します。
7. [**Sync & apply changes**] 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の作成

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. ダッシュボードサイドバーから、［**IAM** と管理］を選択し、［サービスアカウント］を選択します。
3. ［アカウントの作成］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の作成

1. ［サービスアカウント］ページで、今作成したサービスアカウントを選択します。
2. ［キー］タブを選択してから、［キーの追加］**>**［新しいキーの作成］を選択します。
3. デフォルトの JSON キータイプオプションは選択したままにします。
4. [**Create**] を選択します。後でアクセスできる安全な場所にキーを保存します。Google Cloud Identity を ID プロバイダーとして接続するときは、Citrix Cloud コンソールに秘密キーを入力します。

ドメイン全体の委任を構成

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** とサービスの有効化］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］をクリックします。

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、先ほど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］タブの、［詳細設定］を展開します。

c) ［ドメイン全体の委任］で、クライアント ID をコピーし、［**Google Workspace** 管理コンソールの表示］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、［セキュリティ］**>**［アクセスとデータ管理］**>**［**API** の制御］を選択します。

f) ［ドメイン全体の委任］で、［ドメイン全体の委任を管理］をクリックします。

g) ［新しく追加］を選択します。

h) ［クライアント **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** スコープ］で、次のスコープをコンマ区切りを使用して 1 行に入力します：

```
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
<!--NeedCopy-->
```

j) ［**Authorize**］を選択します。

読み取り専用の **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、他の特権もありません。

1. Google 管理メニューから、［ディレクトリ］**>**［ユーザー］を選択します。
2. ［新しいユーザーの追加］を選択して、適切なユーザー情報を入力します。
3. ［新しいユーザーの追加］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、［アカウント］**>**［管理者ロール］を選択します。
   b) ［新しいロールの作成］を選択します。
   c) 新しいロールの名前を入力します。例：API 読み取り専用
   d) 次に、［続行］を選択します。
   e) ［管理 **API** 権限］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］を選択してから、［ロールを作成］を選択します。

5. 先ほど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の ［管理］ペインで、［ユーザーへの割り当て］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の入力を開始し、ユーザーリストから選択します。
c) ［ロールの割り当て］を選択します。
d) ロールの割り当てを確認するには、［ディレクトリ］**>** ［ユーザー］で［ユーザー］ページに戻り、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 メニューで、［**ID** およびアクセス管理］を選択します。
3.「**Google Cloud Identity**」を見つけ、省略記号（…）メニューから ［接続］を選択します。
4. 入力画面が表示されたら、URL に適した短い会社の識別子を入力し、［保存して続行］を選択します。この識別子は、Citrix Cloud 内でグローバルに一意である必要があります。
5. ［ファイルのインポート］を選択してから、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。このアクションにより、作成した Google Cloud サービスアカウントの秘密キーとメールアドレスがインポートされます。
6. ［偽装ユーザー］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. ［次へ］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。正しい場合は、［確認］を選択して構成を保存します。

管理者を **Citrix Cloud** に追加する

Google Cloud を通じて、個人の Citrix Cloud 管理者と管理者グループを追加できます。詳しくは、次の記事を参照してください:

- 個人の管理者の場合: Citrix Cloud への管理者のアクセスを管理する
- 管理者グループの場合: 管理者グループを管理する

Citrix Cloud に管理者を追加後、管理者は次のいずれかの方法でサインインできます:

- 最初に Google Cloud を ID プロバイダーとして構成すると、構成した管理者のサインイン URL に移動します。例: `https://citrix.cloud.com/go/mycompany`
- Citrix Cloud のサインインページで、［会社の資格情報でサインイン］をクリックし、最初に Azure AD を接続したときに作成した識別子（「mycompany」など）を入力し、［続行］をクリックします。

ワークスペースの **Google Cloud Identity** を有効にする

1. Citrix Cloud メニューから ［ワークスペース構成］**>** ［認証］の順に選択します。
2. **Google Cloud Identity** を選択します。プロンプトが表示されたら、［利用者のエクスペリエンスに与える影響を了承しています］を選択して、［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

July 2, 2024

Citrix Cloud では、ワークスペースにサインインする利用者を認証するための ID プロバイダーとして使用して、Okta を使用できます。Okta 組織を Citrix Cloud に接続することにより、Citrix Workspace のリソースにアクセスする利用者に共通のサインイン操作を提供できます。

ワークスペース構成で Okta 認証を有効にした後、利用者のサインイン操作は変化します。Okta 認証を選択すると、シングルサインオンではなく、フェデレーション ID によるサインイン環境となります。利用者は、Okta サインインページからワークスペースにサインインしますが、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）からアプリまたはデスクトップを起動するときにもう一度認証する必要があります。シングルサインオンを有効にし、2 つ目のログオンプロンプトが表示されないようにするには、Citrix Cloud で Citrix フェデレーション認証サービスを使用する必要があります。詳しくは、「Citrix Cloud に Citrix フェデレーション認証サービスを接続する」を参照してください。

前提条件

Cloud Connector または Connector Appliance

Cloud Connector または Connector Appliance のいずれかが、Citrix Cloud とリソースの場所との間でやり取りするために必要です。Citrix Cloud との高可用性接続を実現するためには、少なくとも 2 つの Cloud Connector または Connector Appliance が必要です。また、使用している 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のいずれかを使用できます。

コネクタは、次の要件を満たしている必要があります：

- 各製品のドキュメントに記載されている要件を満たしている
- Active Directory（AD）ドメインに参加している。ワークスペース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 Citrix Workspace を介してアクセスするリソースにアクセスできるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。

Cloud Connector のインストール手順について詳しくは、「Cloud Connector のインストール」を参照してください。
Connector Appliance のインストール手順について詳しくは、「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 に接続する場合、組織の Okta ドメインを指定する必要があります。Citrix は、次の Okta ドメインをサポートしています:

- okta.com
- okta-eu.com
- 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。Okta Web サイトの「Okta URL ドメインのカスタマイズ」で、カスタムドメインの使用に関する重要な考慮事項をレビューします。

組織のカスタムドメインを見つける方法について詳しくは、Okta Web サイトで「自身の 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使用して 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して構成したら、クライアント ID とクライアントシークレットをメモします。Okta 組織の接続時に、これらの値を Citrix Cloud に入力します。

このアプリケーションを作成および構成するには、この記事の次のセクションを参照してください:

- Okta OIDC Web アプリケーション統合の作成
- Okta OIDC Web アプリケーションの構成

ワークスペース **URL**

Okta アプリケーションの作成時には、Citrix Cloud からのワークスペース URL を入力する必要があります。ワークスペース URL を見つけるには、Citrix Cloud メニューから ［ワークスペース構成］を選択します。ワークスペース URL は、［アクセス］タブに表示されます。

> 重要:
>
> 後でワークスペース URL を変更する場合、Okta アプリケーションの構成を新しい URL によって更新する必要があります。そうしないと、ワークスペースからのログオフ時に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。Okta 組織で読み取り専用の管理者アカウントを使用し、このトークンを作成します。このトークンは、Okta 組織内のユーザーとグループを読み取れる必要があります。

API トークンを作成するには、この記事の「Okta API トークンの作成」を参照してください。API トークンについて詳しくは、Okta ウェブサイトで「API トークンの作成」を参照してください。

> 重要:
>
> API トークンを作成する際には、トークンの値をメモしてください（たとえば、値を一時的にプレーンテキストドキュメントにコピーしてください）。Okta ではこの値が一度だけ表示され、「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場合があります。

Okta AD エージェントでアカウントを同期

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 Active Directory と Okta を統合する必要があります。そのためには、ドメイン内に Okta AD エージェントをインストールし、Okta Organization に Active Directory を追加します。Okta Active Directory エージェントを展開するためのガイダンスについては、Okta Web サイトで「Get started with Active Directory integration（Active Directory の統合を開始する）」を参照してください。

その後、Active Directory ユーザーおよびグループを Okta にインポートします。インポート時には、Active Directory アカウントに関連付けられている以下の値を含めます:

- メール
- SID
- UPN
- OID

> 注:
>
> ワークスペースで Citrix Gateway サービスを使用している場合、Active Directory アカウントを Okta 組織と同期する必要はありません。

Active Directory ユーザーおよびグループを Okta Organization と同期するには:

1. Okta Active Directory エージェントをインストールして構成します。詳しい手順については、Okta Web サイトの次の記事を参照してください:
   - Install the Okta Active Directory agent（Okta Active Directory エージェントのインストール）
   - Configure Active Directory import and account settings（Active Directory のインポートとアカウント設定の構成）
   - Configure Active Directory provisioning settings（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、Active Directory ユーザーおよびグループを Okta に追加します。Okta のインポート方法と手順について詳しくは、Okta Web サイトで「Manage Active Directory users and groups（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 アプリケーション統合の作成

1. Okta 管理コンソールの［**Applications**］から［**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**］にアプリ統合のフレンドリ名を入力します。
6. ［**Grant type**］で［**Authorization Code**］を選択します（デフォルトで選択済み）。
7. ［**Sign-in redirect URIs**］に「`https://accounts.cloud.com/core/login-okta`」を入力します。
8. ［**Sign-out redirect URIs**］に、Citrix Cloud からの Workspace URL を入力します。
9. ［**Assignments**］の［**Controlled access**］で、アプリ統合を割り当てるのが組織の全員または指定したグループのみか、または後からアクセスを割り当てるのかを選択します。
10. ［**Save**］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。
11. ［**Client Credentials**］セクションで、［**Client ID**］と［**Client Secret**］の値をコピーします。Citrix Cloud を Okta 組織に接続するときに、これらの値を使用します。

Okta OIDC Web アプリケーションの構成

この手順では、Citrix Cloud に必要な設定によって Okta OIDC Web アプリケーションを構成します。Citrix Cloud では、ワークスペースへのサインイン時に Okta を介して利用者を認証するため、これらの設定が必要です。

1. （オプション）暗黙的な許可タイプのクライアント権限を更新します。この付与タイプに最小限の権限を許可する場合に、この手順の実行を選択できます。

    a) Okta アプリケーション構成ページの［**General**］タブで［**General Settings**］セクションまでスクロールし、［**Edit**］をクリックします。
    b) ［**Application**］セクションの［**Grant type**］の［**Client acting on behalf of user**］で［**Allow Access Token with implicit grant type**］をオフにします。
    c) ［**Save**］を選択します。

2. アプリケーション属性を追加します。これらの属性では大文字と小文字が区別されます。

    a) Okta コンソールメニューから、［**Directory**］**>**［**Profile Editor**］の順に選択します。
    b) Okta［**User**］（デフォルト）プロファイルを選択します。Okta が［**User**］プロファイルページを表示します。
    c) ［**Attributes**］で、［**Add attribute**］を選択します。
    d) 次の情報を入力します：

        - Display Name：cip_email
        - Variable Name：cip_email
        - Description：AD ユーザーメール

- 属性の長さ：［次より大きい］を選択し、「**1**」と入力します。
- Attribute Required：Yes

e) ［**Save and Add Another**］を選択します。

f) 次の情報を入力します：

- Display Name：cip_sid
- Variable Name：cip_sid
- Description：Active Directory ユーザーセキュリティ識別子
- 属性の長さ：［次より大きい］を選択し、「**1**」と入力します。
- Attribute Required：Yes

g) ［**Save and Add Another**］を選択します。

h) 次の情報を入力します：

- Display Name：cip_upn
- Variable Name：cip_upn
- Description：AD ユーザープリンシパル名
- 属性の長さ：［次より大きい］を選択し、「**1**」と入力します。
- Attribute Required：Yes

i) ［**Save and Add Another**］を選択します。

j) 次の情報を入力します：

- Display Name：cip_oid
- Variable Name：cip_oid
- Description：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。
- Attribute Required：Yes

k) ［**Save**］を選択します。

3. アプリケーションの属性マッピングの編集：

a) Okta コンソールから、［**Directory**］**>**［**Profile Editor**］の順に選択します。

b) Active Directory 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`という形式で表示される場合があります。`myDomain`は統合された Active Directory ドメインの名前です。

c) ［**Mappings**］を選択します。Active Directory 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、Active Directory を Okta ユーザーにマップするためのタブが選択されています。

d) ［**Okta User Profile**］列で、手順 2 で作成された属性を見つけて以下のようにマップします：

- `cip_email`の場合、ドメインの［User Profile］列から`email`を選択します。選択すると、マッピングには`appuser.email`が表示されます。
- `cip_sid`の場合、ドメインの［User Profile］列から`objectSid`を選択します。選択すると、マッピングには`appuser.objectSid`が表示されます。
- `cip_upn`の場合、ドメインの［User Profile］列から`userName`を選択します。選択すると、マッピングには`appuser.userName`が表示されます。

- `cip_oid`の場合、ドメインの［User Profile］列から`externalId`を選択します。選択すると、マッピングには`appuser.externalId`が表示されます。

e) ［**Save Mappings**］を選択します。
f) ［**Apply updates now**］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 Active Directory と同期します。

i. Okta コンソールから ［**Directory**］**>** ［**Directory Integrations**］の順に選択します。
ii. 統合された Active Directory を選択します。
iii. ［**Provisioning**］タブを選択します。
iv. ［**Settings**］で ［**To Okta**］を選択します。
v. ［**Okta Attribute Mappings**］セクションまでスクロールして、［**Force Sync**］を選択します。

Okta API トークンの作成

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、［**Security**］**>** ［**API**］の順に選択します。
3. ［**Tokens**］タブを選択してから、［**Create Token**］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。Okta 組織の Citrix Cloud への接続時に、この値を入力します。

Citrix Cloud を **Okta** 組織に接続

1. https://citrix.cloud.comで Citrix Cloud にサインインします。
2. Citrix Cloud メニューで、［**ID** およびアクセス管理］を選択します。
3. 「**Okta**」を見つけ、省略記号（…）メニューから ［接続］を選択します。
4. ［**Okta URL**］に Okta ドメインを入力します。
5. ［**Okta API** トークン］に、Okta 組織の API トークンを入力します。
6. ［クライアント **ID**］と ［クライアントシークレット］に、先ほど作成した OIDC Web アプリ統合からクライアント ID とシークレットを入力します。Okta コンソールからこれらの値をコピーするには、［アプリケーション］を選択し、Okta アプリケーションを見つけます。［クライアント資格情報］で、［クリップボードにコピー］ボタンを各値に対して使用します。
7. ［テストして終了］をクリックします。Citrix Cloud で Okta の詳細が確認され、接続がテストされます。

接続が正常に検証されたら、ワークスペース利用者に対して Okta 認証を有効にできます。

ワークスペースの **Okta** 認証を有効にする

1. Citrix Cloud メニューから ［ワークスペース構成］**>** ［認証］の順に選択します。
2. ［**Okta**］を選択します。

3. プロンプトが表示されたら、［利用者のエクスペリエンスに与える影響を了承しています］を選択します。
4. ［**Save**］を選択します。

Okta 認証に切り替えた後、Citrix Cloud はワークスペースを数分間一時的に無効にします。ワークスペースが再度有効になると、利用者は Okta を使用してサインインできます。

追加情報

- Citrix Tech Zone:
  - Tech Insight：認証 - Okta
  - 技術概要：Workspace ID
  - 技術概要：Workspace SSO

SAML を ID プロバイダーとして Citrix Cloud に接続する

July 2, 2024

Citrix Cloud では、ワークスペースにサインインする Citrix Cloud 管理者および利用者を認証するための ID プロバイダーとして、SAML（セキュリティアサーションマークアップランゲージ）を使用できます。オンプレミスの Active Directory（AD）で、選択した 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。いくつかの手順では、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は、この記事で説明するコマンドとは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、例としてのみ提供されています。SAML プロバイダーが対応するコマンドについて詳しくは、SAML プロバイダーのドキュメントを参照してください。

SAML プロバイダーの構成

Citrix は、SAML プロバイダーが Citrix Cloud とスムーズに対話できるようにするために、次の構成ガイドを提供しています。

- Active Directory Federated Services（ADFS）を使用した SAML：「ADFS を使用した Citrix Cloud での SAML 認証の構成」を参照してください。

- Azure Active Directory ID を使用する SAML：「Azure Active Directory ID を使用する SAML でワークスペースにサインインする」を参照してください。
- Azure AD 用 Citrix Cloud SAML SSO アプリ：Microsoft Azure AD アプリドキュメント Web サイトの「チュートリアル：Azure Active Directory シングルサインオン（SSO）と Citrix Cloud SAML SSO の統合」を参照してください。
- Citrix Workspace のカスタムドメインを使用した SAML：「カスタムドメインを使用して SAML でワークスペースにサインインする」を参照してください
- Okta を使用した SAML：「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」を参照してください

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、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 Cloud 管理者の認証と Citrix Workspace 利用者の認証について、次の 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。

- Microsoft ADFS
- Microsoft Azure AD
- Duo
- Okta
- OneLogin
- PingOne SSO
- PingFederate

これらのプロバイダーをテストするとき、Citrix では次の設定を使用して Citrix Cloud コンソールで SAML 接続を構成しました。

- バインドメカニズム：HTTP Post
- SAML 応答：応答またはアサーションのいずれかに署名する
- 認証コンテキスト: 未指定、完全一致

これらの設定の値は、Citrix Cloud で SAML 接続を構成するときにデフォルトで構成されます。選択した SAML プロバイダーとの接続を構成する場合は、これらの設定を使用することをお勧めします。

これらの設定について詳しくは、本記事中の「SAML プロバイダーのメタデータを Citrix Cloud Japan に追加」を参照してください。

スコープ付きのエンティティ **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 認証要件で、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 でスコープ付きのエンティティ ID を使用した SAML アプリケーションを構成する」を参照してください。

前提条件

Citrix Cloud で SAML 認証を使用する場合、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するために使用されます。
- SAML プロバイダーとの AD 統合。

Cloud Connector

Citrix Cloud Connector ソフトウェアのインストール先となるサーバーが少なくとも 2 台必要です。Cloud Connector の可用性を高めるため、サーバーは 2 台以上用意することを Citrix ではお勧めします。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:

- 「Citrix Cloud Connector の技術詳細」に記載されているシステム要件を満たしている。
- 他の Citrix コンポーネントは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不可欠なマシンでもない。
- リソースが存在するドメインに参加している。ユーザーが複数のドメインにあるリソースにアクセスする場合は、各ドメインに Citrix Cloud を少なくとも 2 つインストールする必要がある。
- 利用者が Citrix Workspace を介してアクセスするリソースにアクセスできるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。

Cloud Connector のインストール手順について詳しくは、「Cloud Connector のインストール」を参照してください。

Active Directory

SAML 認証を構成する前に、次のタスクを実行します:

- ワークスペース利用者に AD のユーザーアカウントがあることを確認します。SAML 認証が構成されている場合、AD アカウントがない利用者はワークスペース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 では、サインインするワークスペース利用者の AD ユーザー属性が必要とされます。

AD ユーザー属性　次の属性はすべての Active Directory ユーザーオブジェクトに必要であり、設定する必要があります:

- 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 では、利用者が Citrix Workspace にサインインする際、ユーザーコンテキストを決定するために AD からのオブジェクト GUID および SID 属性が必要とされます。これらのプロパティのうちいずれかが入力されていないと、利用者がサインインできません。

Citrix Cloud で SAML 認証を使用する場合、次の属性は必須ではありませんが、最適なユーザーエクスペリエンスを確保するためにこれらの属性を設定することをお勧めします:

- メールアドレス
- 表示名

Citrix Cloud は表示名属性を使用して、Citrix Workspace で利用者の名前を正しく表示します。この属性が設定されていない場合でも、利用者はサインインできますが、名前が正常に表示されない可能性があります。

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 SAML アサーションで次の必要な AD ユーザー属性を Citrix Cloud に渡すことができます:

- objectSID（SID）
- objectGUID（OID）
- userPrincipalName（UPN）
- メール（email）
- 表示名（displayName）

SID 属性または UPN 属性のいずれかが SAML アサーションに含まれている場合、これらの属性のサブセットを構成できます。Citrix Cloud は、必要に応じて AD から他の属性を取得します。

> 注:
>
> 最適なパフォーマンスを確保するために、このセクションで説明するすべての属性を構成することをお勧めします。

正確な統合手順は SAML プロバイダーによって異なりますが、通常統合プロセスには、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。SAML プロバイダーとして ADFS を使用している場合、この手順は必要ありません。
2. カスタム属性を作成し、この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。このタスクの一般的な手順は、この記事の「カスタム SAML 属性の作成およびマッピング」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ついて詳しくは、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。

SAML 2.0 による管理者認証

Citrix Cloud は、SAML 2.0 を使用した AD 管理者グループメンバーの認証をサポートしています。管理者グループを Citrix Cloud に追加する方法について詳しくは、「管理者グループを管理する」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

既に Citrix Cloud に SAML 2.0 接続しており、それを使用して管理者を認証する場合は、最初に［**ID** およびアクセス管理］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。また、SAML 接続を使用して Citrix Workspace 利用者を認証している場合は、［ワークスペース構成］で SAML 認証を無効にする必要があります。SAML 接続を再構成した後、管理者グループを Citrix Cloud に追加できます。

最初に SAML 2.0 を切断して再接続せずに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 **Active Directory** の 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. ［**ID** およびアクセス管理］で、「Active Directory を Citrix Cloud に接続する」の説明に従って、オンプレミスの AD を Citrix Cloud に接続します。
2. 本記事の「Active Directory との SAML 統合」で説明されているように、SAML プロバイダーをオンプレミスの AD と統合します。
3. 管理者が Citrix Cloud へのサインインに使用できるサインイン URL を構成します。
4. ［**ID** およびアクセス管理］で、Citrix Cloud の SAML 認証を構成します。このタスクでは、Citrix Cloud からの SAML メタデータを使用して SAML プロバイダーを構成してから、SAML プロバイダーからのメタデータを使用して Citrix Cloud を構成して SAML 接続を作成します。

Citrix Cloud 管理者向けの既存の **SAML** 接続を使用するためのタスクの概要

既に Citrix Cloud に SAML 2.0 接続しており、それを使用して管理者を認証する場合は、次のタスクを実行します:

1. 該当する場合は、SAML 2.0 ワークスペース認証を無効にします：［ワークスペース構成］**>**［認証］で、別の認証方法を選択し、プロンプトが表示されたら ［確認］を選択します。
2. 既存の SAML 2.0 接続を切断します：［**ID** およびアクセス管理］**>**［認証］で、SAML 接続を見つけます。右端の省略記号メニューで ［切断］を選択します。［はい、切断します］をクリックして操作を確定します。
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で ［接続］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 プロバイダーのメタデータの構成」の説明に従って、SAML 接続を構成します。

SAML 接続を構成したら、「管理者グループを管理する」の説明どおりに、AD 管理者グループを Citrix Cloud に追加できます。この記事で説明されているように、ワークスペース利用者の SAML を再度有効にすることもできます。

カスタム **SAML** 属性の作成およびマッピング

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を既に構成している場合は、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 の既存のカスタム SAML 属性を使用します。

> 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は、このセクションで説明す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 プロバイダーが対応するコマンドについて詳しくは、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ための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**］を選択します。
2. 次の AD プロパティの属性を追加します。表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	必須かオプションか	デフォルト値
userPrincipalName	SID の属性を追加しない場合は必須（推奨）。	`cip_upn`
objectSID	UPN の属性を追加しない場合は必須。	`cip_sid`
objectGUID	認証用のオプション	`cip_oid`
mail	認証用のオプション	`cip_email`
displayName	ワークスペース UI で必須	`displayName`
givenName	ワークスペース UI で必須	`firstName`

AD プロパティ	必須かオプションか	デフォルト値
sn	ワークスペース UI で必須	`lastName`
AD フォレスト	認証用のオプション	`cip_forest`
AD ドメイン	認証用のオプション	`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、[**Users**] > [**Directories**] を選択します。
4. ディレクトリ属性を追加するための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、[**Directory Attributes**] を選択します。
5. 属性を追加するためのオプションを選択し、次の 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プします:
    - 手順 2 で SID の属性（`cip_sid`など）を追加した場合は、**objectSid** を選択し、作成した属性にマップします。
    - 手順 2 で UPN の属性（`cip_upn`など）を追加した場合は、**userPrincipalName** を選択し、作成した属性にマップします。
    - 手順 2 で ObjectGUID の属性（`cip_oid`など）を追加した場合は、**ObjectGUID** を選択し、作成した属性にマップします。
    - 手順 2 でメールの属性（`cip_email`など）を追加した場合は、**mail** を選択し、作成した属性にマップします。
    - 手順 2 で表示名の属性（`displayName`など）を追加した場合は、**displayName** を選択し、作成した属性にマップします。

管理者のサインイン **URL** の構成

1. https://citrix.cloud.comで Citrix Cloud にサインインします。
2. Citrix Cloud メニューで、[**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. 入力画面が表示されたら、URL に適した短い会社の識別子を入力し、[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の構成

このタスクでは、Citrix Cloud 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、SAML メタデータを使用して、コネクタアプリケーションから Citrix Cloud への SAML 接続を構成します。

> 注:
>
> このセクションのいくつかの手順では、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は、このセクションで説明す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 プロバイダーが対応するコマンドについて詳しくは、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の作成

1. SAML プロバイダーの管理コンソールから、属性付き、署名応答付き 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**］を選択して ［**SAML Test Connector (IdP w/ attr w/ sign response)**］を選択します。
2. 必要に応じて、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］画面の ［**SAML** メタデータ］で ［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、一部の ID プロバイダーにとって、SAML プロバイダーのメタデータをインポートおよび監視するときにより適している場合があります。

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:
   - **Audience** フィールドに、`https://saml.cloud.com`と入力します。
   - **Recipient** フィールドに、`https://saml.cloud.com/saml/acs`を入力します。
   - ACS URL 検証のフィールドに、`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. カスタム SAML 属性をアプリケーションのパラメーター値として追加します。

このフィールドを作成	このカスタム属性を割り当て
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	メール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. ワークスペース利用者をユーザーとして追加して、アプリケーションへのアクセスを許可します。

SAML プロバイダーのメタデータを **Citrix Cloud** に追加

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、このファイルのイメージ例です:

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** プロバイダーのエンティティ **ID**］で、メタデータの **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. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19"

   - ［認証要求に署名する］で ［はい］を選択して Citrix Cloud が認証要求に署名できるようにして、Citrix Cloud によるものであり、悪意のあるアクターによるものではないことを保証します。安全な SAML 応答のために SAML プロバイダーが使用する許可リストに Citrix ACS URL を追加する場合は、［いいえ］を選択します。

   - ［**SSO** サービス **URL**］で、使用するバインドメカニズムの URL を入力します。HTTP-POST または HTTP-Redirect バインドのいずれかを使用できます。メタデータファイルで、**HTTP-POST** または **HTTP-Redirect** のいずれかのバインド値を持つ **SingleSignOnService** 要素を見つけます。

- ［バインドメカニズム］で、メタデータファイルから選択した SSO サービス URL のバインドに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に署名する］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、次のアクションを実行します:
   - 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 でエンコードされた 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］ページの［**X.509** 証明書］で、［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. ［続行］を選択してアップロードを完了します。
6. ［認証コンテキスト］で、使用するコンテキストと Citrix Cloud がコンテキストを適用する厳格さのレベルを選択します。選択したコンテキストで認証を強制せずに、そのコンテキストで認証を要求するには、［最小］を選択します。選択したコンテキストで認証を要求し、そのコンテキストでのみ認証を強制するには、［完全一致］を選択します。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、または認証コンテキストを使用しないことを選択した場合は、［未指定］および ［最小］を選択します。デフォルトでは、［未指定］と［完全一致］が選択されています。
7. ［ログアウト **URL**］（オプション）では、Citrix Workspace または Citrix Cloud からサインアウトしたユーザーが、SAML プロバイダーを通じ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ようにするかを決定します。
   - ユーザーが Citrix Workspace 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する場合は、［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 Citrix Workspace または Citrix Cloud からサインアウトした後にすべての Web アプリケーションからサインアウトするようにするには、SAML プロバイダーから SingleLogout（SLO）エンドポイントを入力します。SAML プロバイダーとして Microsoft ADFS または Azure Active Directory を使用している場合、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。

8. Citrix Cloud の以下のデフォルトの属性値が、SAML プロバイダーで構成された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、ここに入力した値が SAML プロバイダーの値と一致する必要があります。SAML プロバイダーで特定の属性を構成していない場合は、特に記載がない限り、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。

    - ユーザー表示名の属性名：デフォルト値は`displayName`です。
    - ユーザーの名の属性名：デフォルト値は`firstName`です。
    - ユーザーの姓の属性名：デフォルト値は`lastName`です。
    - セキュリティ識別子（**SID**）の属性名：UPN の属性を作成しなかった場合は、SAML プロバイダーからこの属性名を入力する必要があります。デフォルトの値は`cip_sid`です。
    - ユーザープリンシパル名（**UPN**）の属性名：SID の属性を作成しなかった場合は、SAML プロバイダーからこの属性名を入力する必要があります。デフォルトの値は`cip_upn`です。
    - メールの属性名：デフォルト値は`cip_email`です。
    - **AD** オブジェクト識別子（**OID**）の属性名：デフォルト値は`cip_oid`です。
    - **AD** フォレストの属性名：デフォルト値は`cip_forest`です。
    - **AD** ドメインの属性名：デフォルト値は`cip_domain`です。

9. ［テストして終了］を選択して、正常に接続を構成したことを確認します。

AD から管理者を **Citrix Cloud** に追加

Citrix Cloud で AD グループを追加して管理する手順については、「管理者グループを管理する」を参照してください。

ワークスペースの **SAML** 認証を有効にする

1. Citrix Cloud メニューから、［ワークスペース構成］を選択します。
2. ［認証］タブを選択します。
3. ［**SAML 2.0**］を選択します。

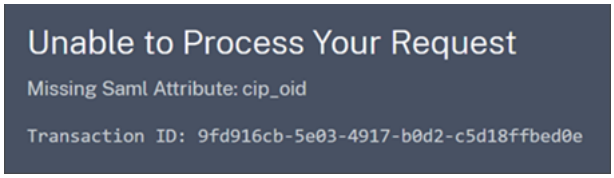
トラブルシューティング

属性エラー

属性エラーは、次のいずれかの状況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`および`cip_upn`属性が SAML アサーションにありません。
- SAML アサーションに`cip_sid`または`cip_oid`属性がなく、接続の問題により Citrix Cloud は Active Directory からこれらの属性を取得できません。

属性エラーが発生すると、Citrix Cloud は問題のある属性について説明したエラーメッセージを表示します。



この種類のエラーを解決するには、次の手順を実行します:

1. SAML プロバイダーが、次の表に示す正しいエンコーディングで必要な属性を送信していることを確認してください。少なくとも、SID 属性または UPN 属性のいずれかを含める必要があります。

属性	エンコーディング	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	
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）

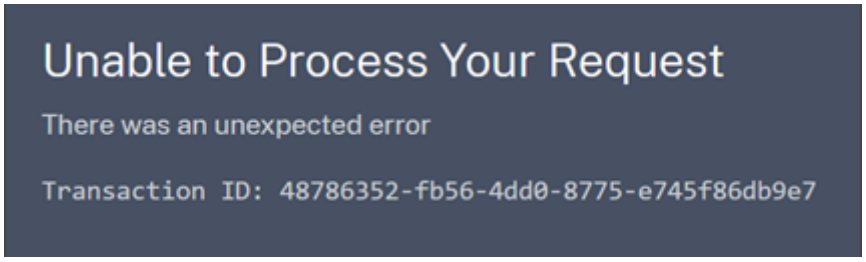
2. Citrix Cloud が不足している必要な属性を取得できるように、Cloud Connector がオンラインかつ正常であることを確認します。詳しくは、「Cloud Connector の高度なヘルスチェック」を参照してください。

予期しないエラー

次の場合、Citrix Cloud で予期しないエラーが発生することがあります:

- ユーザーが、IDP 開始のフローを使用して、SAML 要求を開始する。たとえば、ワークスペース URL（`customer.cloud.com`）に直接移動するのではなく、ID プロバイダーのアプリポータルからタイルを選択することによって、要求が行われるなど。
- SAML 証明書が無効であるか、有効期限が切れている。
- 認証コンテキストが無効である。
- SAML アサーションと応答署名が一致していない。

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。

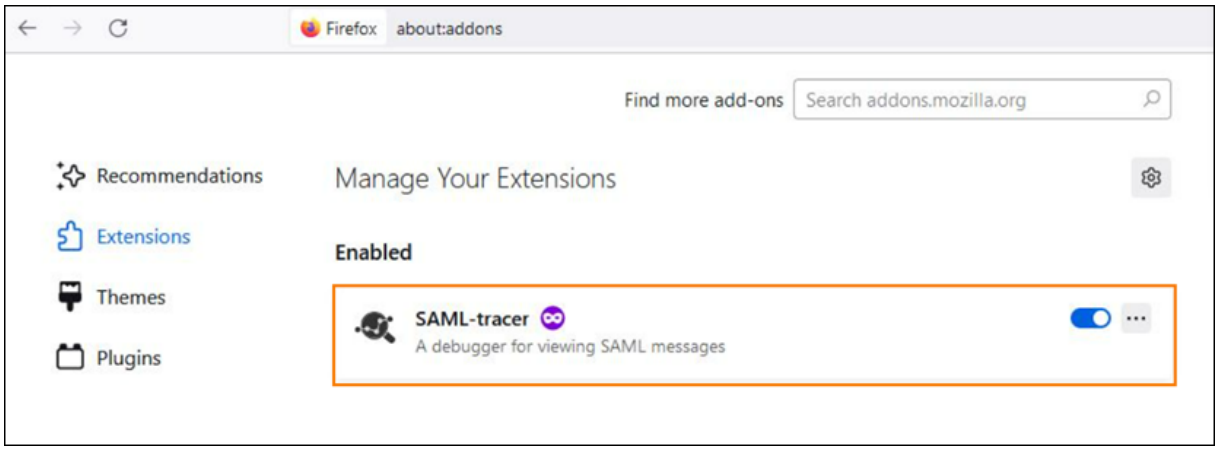


ID プロバイダーのアプリポータルを介して Citrix Cloud に移動した結果としてこのエラーが発生した場合は、次の回避策が考えられます:

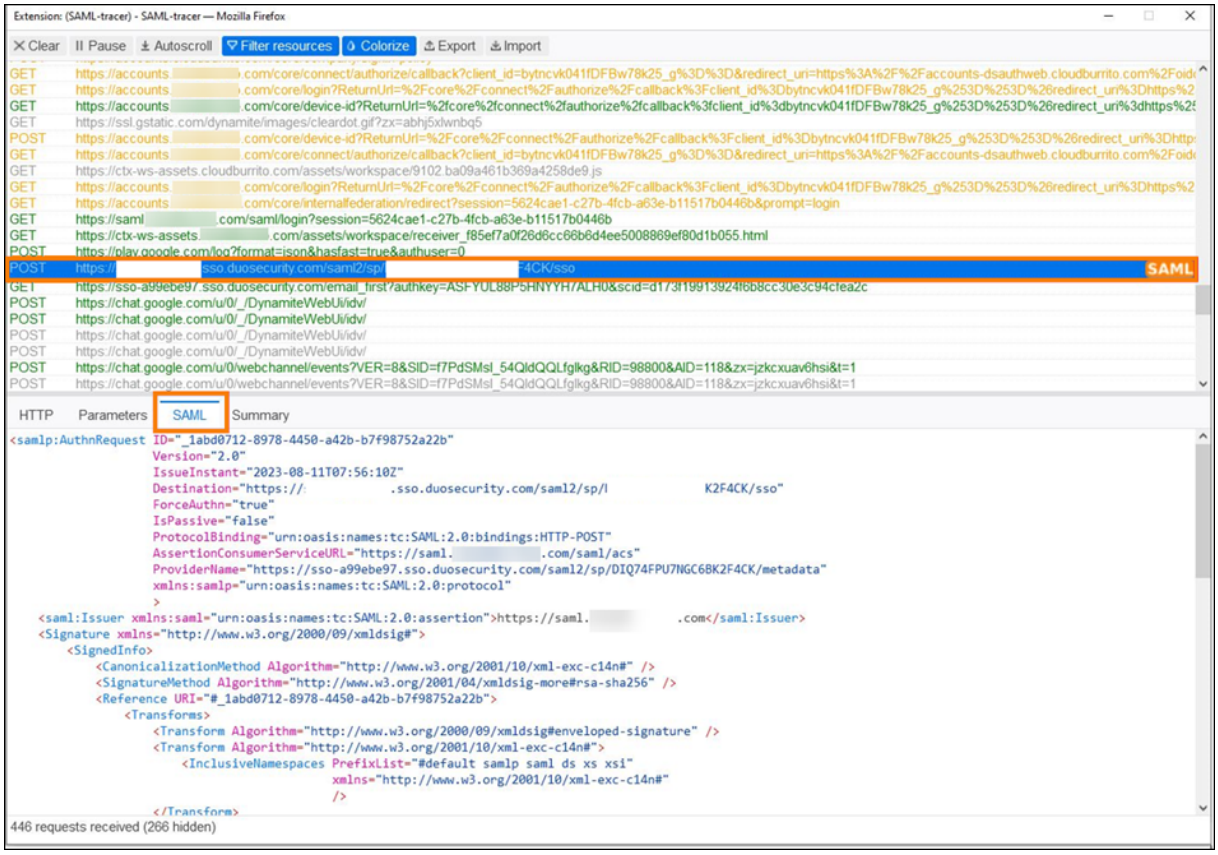
1. ワークスペース URL（`https://customer.cloud.com`など）を参照するブックマークアプリを、ID プロバイダーのアプリポータルに作成します。
2. SAML アプリとブックマークアプリの両方にユーザーを割り当てます。
3. SAML アプリとブックマークアプリの表示設定を変更して、ブックマークアプリが表示され、SAML アプリがアプリポータルで非表示になるようにします。
4. 追加のパスワードプロンプトを削除するには、ワークスペース構成の ［フェデレーション **ID** プロバイダーセッション］設定を無効にします。手順については、Citrix Workspace 製品ドキュメントの「フェデレーション ID プロバイダーセッション」を 参照してください。

デバッグに関する推奨事項

あらゆる SAML デバッグ作業には、ブラウザー拡張機能 SAML-tracer を使用することをお勧めします。この拡張機能は、よく知られている Web ブラウザーのほとんどで利用できます。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 にデコードすることで、人間が判読できるようにします。



このツールを使用すると、管理者は、ユーザーに送信される SAML 属性の値を確認し、SAML の要求および応答から署名を検索できます。SAML 関連の問題でサポートが必要な場合、Citrix サポートは、問題を理解してサポートケースを解決するために、SAML-tracer のファイルを要求してきます。



追加情報

- Microsoft ドキュメント: チュートリアル：Azure Active Directory シングル サインオン（SSO）と Citrix Cloud SAML SSO の統合
- Active Directory Federated Services（ADFS）を使用した SAML:「ADFS を使用した Citrix Cloud での SAML 認証の構成」
- Citrix Tech Zone：Tech Insight：認証 - SAML

Ciitrix Cloud でスコープ付きのエンティティ **ID** を使用した **SAML** アプリケーションを構成する

December 14, 2023

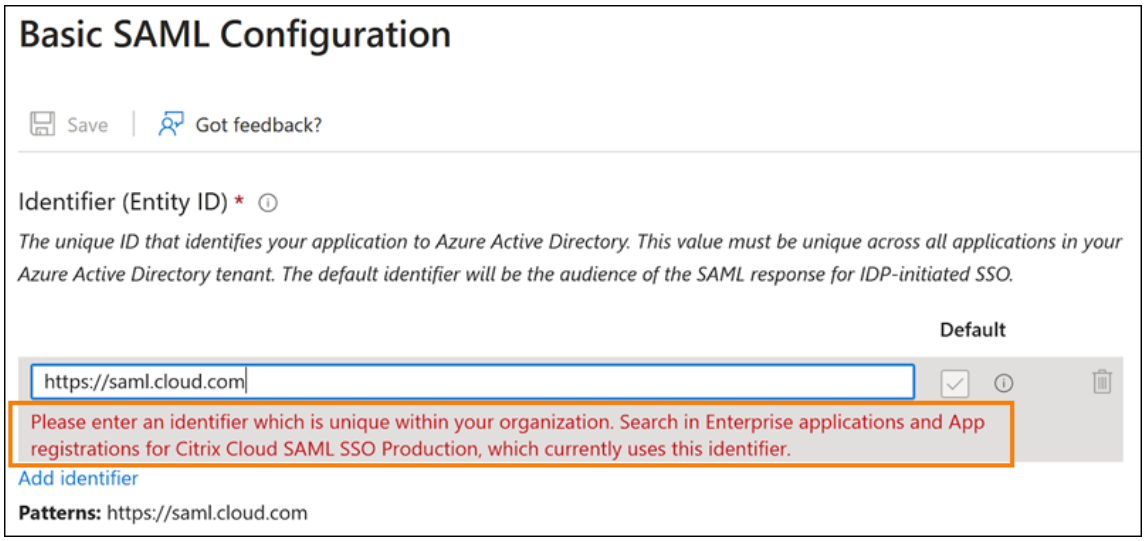
Author:
Mark Dear

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。

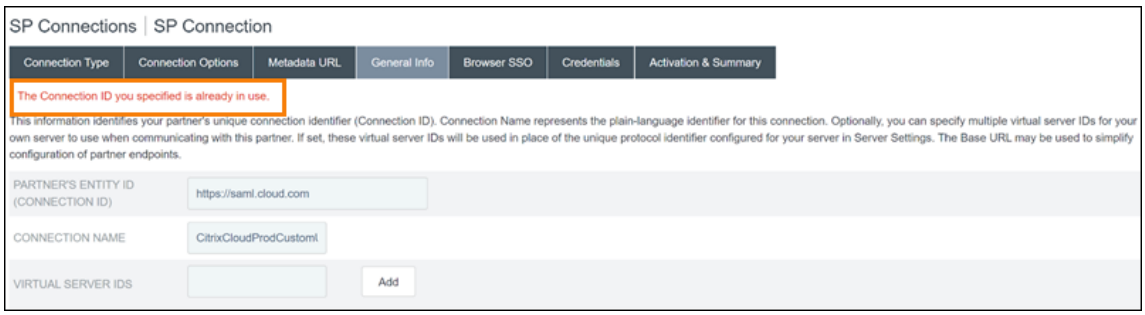
Azure Active Directory（AD）、Active Directory フェデレーションサービス（ADFS）、PingFederate、PingSSO などの一部の SAML プロバイダーでは、複数の SAML アプリケーション内で同じサービスプロバイダー（SP）のエンティティ ID を再利用することが禁止されています。その結果、同じ SAML プロバイダー内で 2 つ以上の異なる SAML アプリケーションを作成する管理者は、それらを同じまたは異なる Citrix Cloud テナントに関連付けられません。既存の SAML アプリケーションが既に使用している、同じ SP エンティティ 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トリガーされ、エンティティ ID が既に使用されていることが表示されます。

以下は、このエラーの画像です：

- Azure Active Directory の場合：



- PingFederate の場合：



Citrix Cloud のスコープ付きのエンティティ ID 機能はこの制限に対処するため、SAML プロバイダー（Azure AD テナントなど）内に複数の SAML アプリケーションを作成し、それを単一の Citrix Cloud テナントに関連付けられるようになります。

エンティティ **ID** とは何ですか**?**

SAML エンティティ ID は、SAML 認証および認証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した各 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 Azure AD 間の SAML 接続では、Citrix Cloud がサービスプロバイダー（SP）であり、Azure AD が SAML プロバイダーです。どちらにもエンティティ ID があり、SAML 接続の反対側に構成する必要があります。つまり、Citrix Cloud のエンティティ ID は Azure AD 内で構成する必要があり、Azure AD のエンティティ ID は Citrix Cloud 内で構成する必要があります。

次のエンティティ ID は、Citrix Cloud の汎用エンティティ ID とスコープ付きのエンティティ 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`

リージョン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 接続と Citrix Cloud テナントに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、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 リージョンごとの汎用 SP エンティティ ID とスコープ付き SP エンティティ ID を示します:

Citrix Cloud のリージョン	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`
自治体	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

新規および既存の **SAML** 接続用に一意の **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、新しい接続の作成時に ［スコープ付きの **SAML** エンティティ **ID** を構成する］設定を有効にします。

スコープ付きエンティティ ID を使用するように既存の SAML 接続を更新する場合は、Citrix Cloud の ［**ID** およびアクセス管理］**>**［認証］ページで SAML プロバイダーを切断してから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、構成のクローンを作成し、そのクローン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 が破棄されます。SAML 接続プロセスを再起動すると、Citrix Cloud は新しいスコープ付きエンティティ ID の GUID を生成します。SAML プロバイダーを構成する場合は、この新しいスコープ付きエンティティ ID を使用します。スコープ付きエンティティ ID を使用するために既存の SAML 接続を更新する場合は、Citrix Cloud が生成するスコープ付きエンティティ ID を使用して、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 **Azure AD** テナント内に複数の **Azure AD SAML** アプリケーションを作成し、それを **1** つ以上の **Citrix Cloud** テナントに関連付けられますか**?**

Citrix Cloud のスコープ付きエンティティ ID 機能は、一部の SAML プロバイダーが明記しているエンティティ ID の重複防止の制限に対処します。この機能を使用すると、Azure AD テナント内で複数の SAML アプリケーションをプロビジョニングし、単一の Citrix Cloud テナントのスコープ付きのエンティティ ID を使用して各アプリケーションを構成できます。

同じ **Azure AD SAML** アプリケーションを複数の **Citrix Cloud** テナントに関連付けられますか**?**

このシナリオは Citrix Cloud のお客様にとっては一般的な状況であり、Citrix は引き続きこの機能をサポートします。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:

- 汎用エンティティ ID（`https://saml.cloud.com`など）を使用します。
- SAML 接続に対して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決定するにはどうすればよいですか**?**

Citrix Cloud のスコープ付きエンティティ ID 機能では、要件に応じて汎用エンティティ ID またはスコープ付きエンティティ ID を柔軟に使用できます。必要な SAML アプリケーションの数と所有する Citrix Cloud テナントの数

を検討してください。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どうか、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（`https://saml.cloud.com`など）を使用して複数の SAML アプリケーションを作成することを既に許可している場合は、スコープ付きエンティティ ID を有効にしたり、既存の SAML 構成を変更し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	重複したエンティティ ID のサポート
Azure AD（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

次の表は、ユースケースで必要な SAML アプリケーションに基づいて、汎用エンティティ ID またはスコープ付きエンティティ ID がサポートされるかどうか、および SAML プロバイダーが重複するエンティティ ID をサポートす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したエンティティ 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

ユースケースの要件	SAML プロバイダーは重複したエンティティ ID をサポートしていますか?	サポートされる構成
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
ワークスペースのカスタム URL と SAML アプリケーションのペア	はい	汎用またはスコープ付きエンティティ ID
ワークスペースのカスタム URL と SAML アプリケーションのペア	いいえ	スコープ付きエンティティ ID
同じ SAML アプリケーションを複数の Citrix Cloud テナントに関連付ける	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 テナントに関連付ける	いいえ	汎用エンティティ ID

スコープ付きのエンティティ **ID** を使用してプライマリ **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 に SAML 接続を作成します。

1. Citrix Cloud メニューで、[**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**] を見つけて、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 を作成するプロンプトが表示されたら、URL に適した短い会社の識別子（`https://citrix.cloud.com/go/mycompany`など）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** プロバイダーを構成する] で、[スコープ付きの **SAML** エンティティ **ID** を構成する] を選択します。Citrix Cloud は、スコープ付きエンティティ ID を自動的に生成し、エンティティ ID、Assertion Consumer Service、およびログアウト URL のフィールドに値を入力します。
5. [**Citrix Cloud** への **SAML** 接続を構成する] で、SAML プロバイダーからの接続の詳細を入力します。
6. デフォルトの SAML 属性マッピングを受け入れます。
7. [テストして終了] を選択します。

汎用エンティティ **ID** を使用してプライマリ **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 に SAML 接続を作成します。

1. Citrix Cloud メニューで、[**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**] を見つけて、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 を作成するプロンプトが表示されたら、URL に適した短い会社の識別子（`https://citrix.cloud.com/go/mycompany`など）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** プロバイダーを構成する] で、[スコープ付きの **SAML** エンティティ **ID** を構成する] が無効になっていることを確認します。
5. [**Citrix Cloud** への **SAML** 接続を構成する] で、SAML プロバイダーからの接続の詳細を入力します。
6. 必要に応じて、[サービスプロバイダーの **SAML** メタデータ] で [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. [テストして終了] を選択します。

Citrix Workspace カスタムドメインを使用して **SAML** 接続を構成する

このセクションでは、スコープ付きエンティティ ID または汎用エンティティ ID を持つカスタムワークスペース URL を使用して 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ワークスペース URL がある場合にのみ該当します。SAML 認証でカスタムワークスペース 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。

詳しくは、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 でワークスペースにサインインする

ワークスペースのカスタム **URL** と汎用エンティティ **ID** を使用して **SAML** 接続を構成する

このタスクでは、[**Configure scoped Entity ID**] 設定は無効になっています。

1. Citrix Cloud メニューから [ワークスペース構成] を選択します。
2. [カスタムワークスペース **URL**] で、省略記号メニューから [編集] を選択します。
3. [**[customerName].cloud.com URL** とカスタムドメイン **URL** の両方を使用する] を選択します。
4. SAML アプリ 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 **SAML** メタデータ] で [ダウンロード] をクリックして、ワークスペース URL の SAML アプリケーション用に汎用 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。

ワークスペースのカスタム **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、［**Configure scoped Entity ID**］設定は無効になっています。

1. Citrix Cloud メニューから ［ワークスペース構成］を選択します。
2. ［カスタムワークスペース **URL**］で、省略記号メニューから ［編集］を選択します。
3. ［**[customerName].cloud.com URL** とカスタムドメイン **URL** の両方を使用する］を選択します。
4. SAML アプリ 2 のスコープ付きのエンティティ 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。

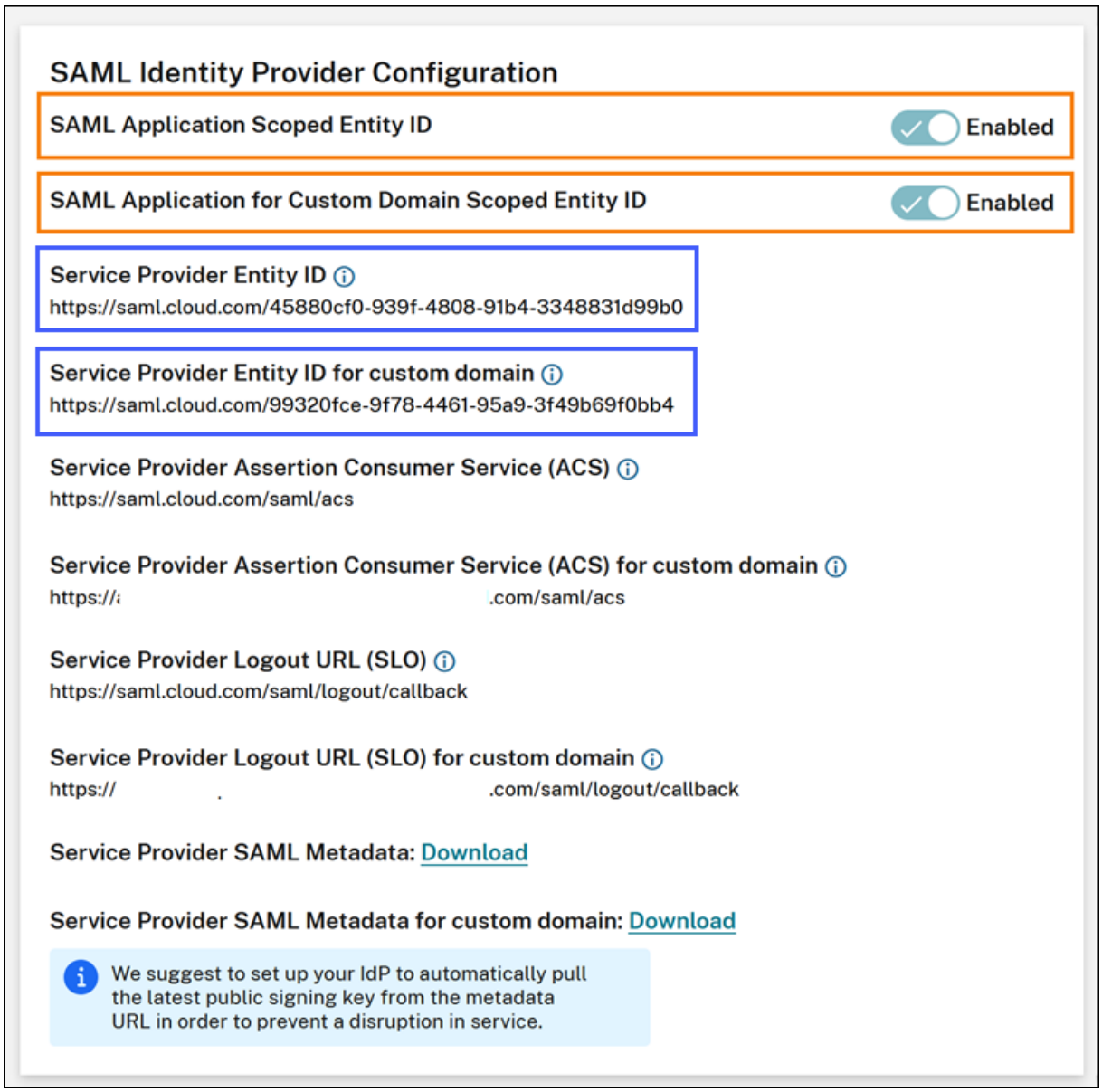
構成を保存すると、Citrix Cloud は正しい GUID を含むスコープ付き SAML メタデータを生成します。必要に応じて、ワークスペースカスタム URL SAML アプリケーションのスコープ付きメタデータのコピーを取得できます。

1. ［**ID** およびアクセス管理］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 **SAML** メタデータ］で、［ダウンロード］をクリックします。

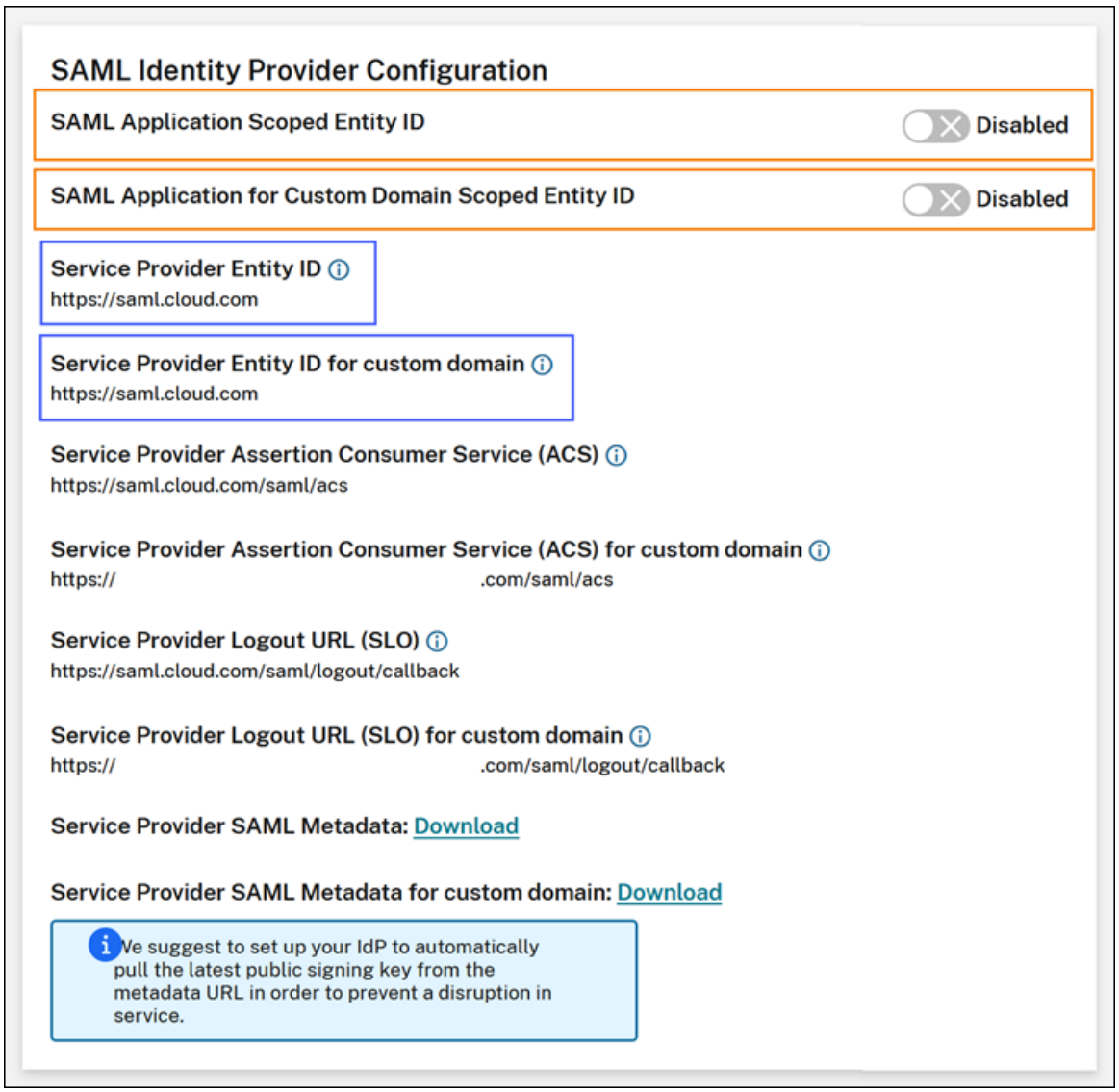
プライマリワークスペース **URL** の **SAML** アプリケーションとカスタムワークスペース **URL** の **SAML** アプリケーションの両方の **SAML** 構成を表示する

スコープ付き SAML 接続の構成の詳細を表示すると、Citrix Cloud はプライマリ SAML アプリケーションとワークスペースカスタムドメイン SAML アプリケーションの両方のスコープ付きのエンティティ ID 設定を表示します。

たとえば、スコープ付きエンティティ ID が有効になっている場合、［サービスプロバイダーのエンティティ **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付きエンティティ ID が含まれます。



スコープ付きエンティティ ID が無効になっている場合、［サービスプロバイダーのエンティティ **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。



スコープ付きエンティティ ID を既存のエンティティ ID 値に追加することで、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。

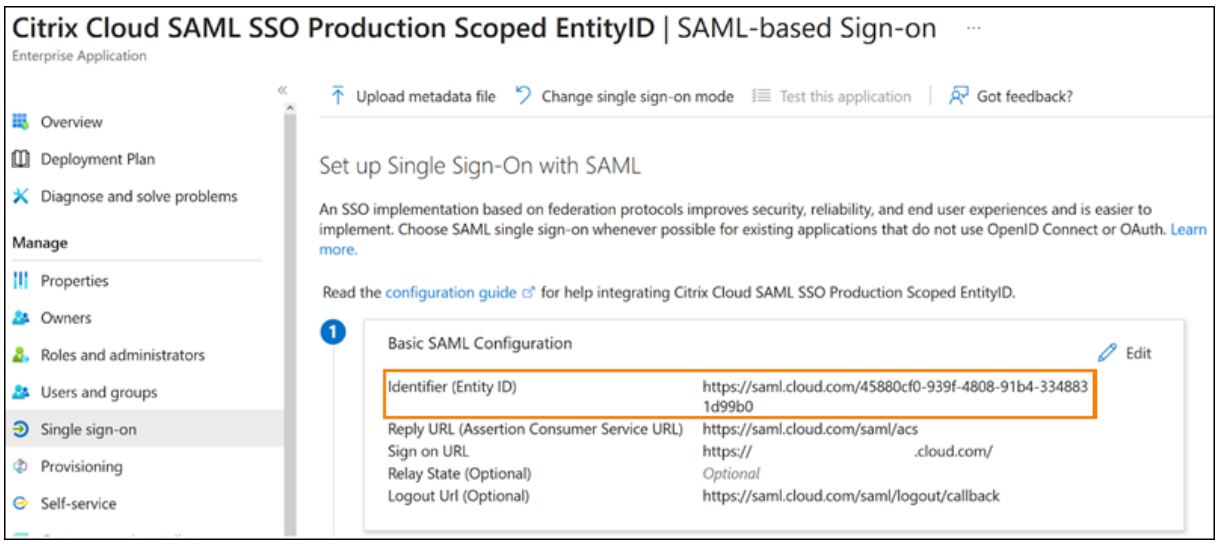
スコープ付きエンティティ **ID** を使用した **SAML** プロバイダー構成

スコープ付きエンティティ ID を使用して Citrix Cloud で SAML 接続を構成した後、スコープ付きエンティティ 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、Azure AD と PingFederate の構成例が含まれています。

スコープ付きエンティティ **ID** を使用した **Azure AD SAML** 構成

この例では、Citrix Cloud のスコープ付きエンティティ ID が Azure AD の ［**Identifier**］フィールドに入力されます。



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

SAML 構成に関する問題のトラブルシューティングには、SAML-tracer ブラウザー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 にデコードすることで、人間が判読できるようにします。SAML-tracer 拡張機能を使用すると、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 要求の両方を検査できます。この拡張機能では、エンティティ ID のスコープ（GUID）が両方の要求に含まれているかどうかを表示できます。

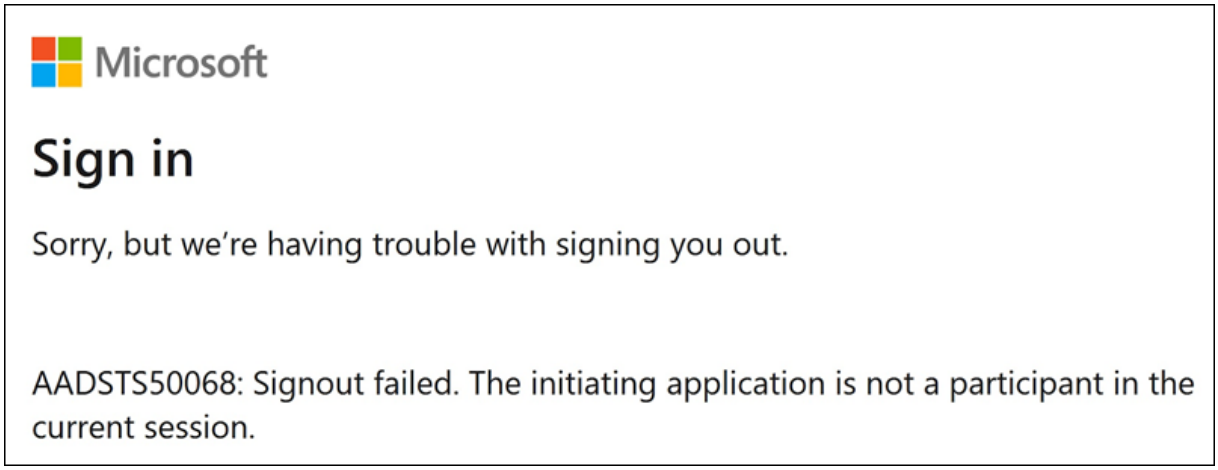
1. ブラウザーの拡張機能パネルから、SAML-tracer 拡張機能をインストールして有効にします。
2. SAML サインインおよびサインアウト操作を実行し、SAML-tracer 拡張機能を使用してフロー全体をキャプチャします。
3. SAML SSO 要求または SLO 要求内で次の行を見つけます。

```
1 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
     saml:Issuer>
2 <!--NeedCopy-->
```


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たエンティティ 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、出力結果を Citrix サポートケースにアップロードします。

Azure AD 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、Azure AD からのサインアウトが失敗します。Azure AD は次のエラーをユーザーに表示します：



Citrix Cloud の SAML 接続に対して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 を SSO 要求と SLO 要求の両方で送信する必要があります。

原因：スコープ付きエンティティは構成されていますが、SLO 要求にエンティティ ID がありません。SAML-tracer 出力の SLO 要求にスコープ付きのエンティティ ID が存在することを確認します。

オンプレミスの **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。

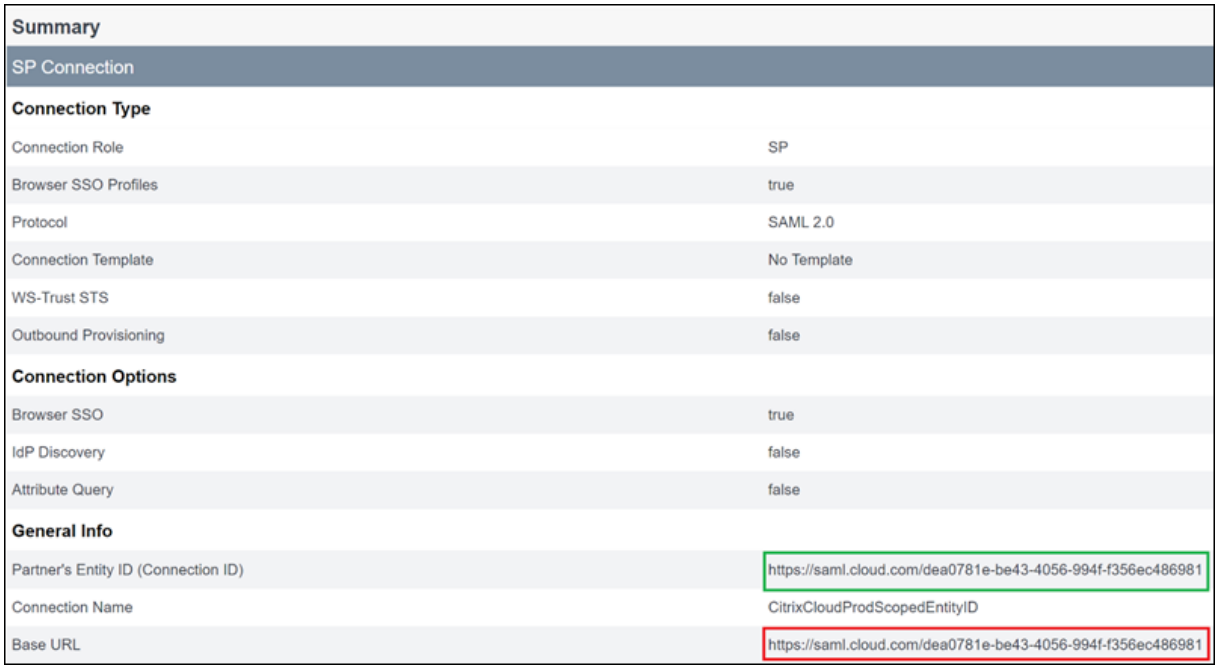
原因： PingFederate 管理者は、スコープ付きエンティティ ID を SP 接続ベース URL に追加しました。

この問題を修正するには、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ます。スコープ付きエンティティ ID をベース URL に追加すると、不正な形式の SAML エンドポイントになります。Citrix Cloud のベース URL が誤って更新されると、ベース URL から派生した他のすべての SAML エンドポイントの相対 URL でサインインが失敗します。

次のエンドポイントは、SAML-tracer 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です:

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

次の図は、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ます。正しく構成されていないフィールドは赤色で表示されます。



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/dea0781e-be43-4056-994f-f356ec486981

ワークスペース認証で **Azure AD ID** と **Azure Active Directory ID** を使用して **SAML** を構成する

March 11, 2024

Author:
Mark Dear

この記事では、AD ID の代わりに Azure Active Directory（AD）ID を使用する SAML をワークスペース認証用に構成する方法について説明します。Azure AD ユーザーがデフォルトの SAML 動作で Citrix Workspace にサインインした後、Windows 365 クラウド PC または Azure AD ドメインに参加している VDA を列挙できない場合は、この構成を使用します。構成が完了すると、ユーザーは SAML 認証を使用して Citrix Workspace にサインインすることで、Citrix DaaS 経由で HDX アプリとデスクトップに、および Azure 経由で Windows 365 クラウド PC に、それぞれアクセスできるようになります。

Citrix Workspace に対する Citrix Cloud および 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、Azure AD Connect を使用して AD ID を Azure AD 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、Citrix Workspace が Citrix DaaS に送信することで、HDX リソースを列挙して起動できるようになります。ユーザー ID の Azure AD バージョンが使用されるため、ユーザーは Citrix Workspace 内から、Windows 365 クラウド PC などの Azure リソースを列挙して起動することもできます。

> 重要:
>
> 列挙とは、ユーザーが Citrix Workspace にサインインした後に表示されるリソースのリストのことです。特定のユーザーがアクセスを許可されるリソースは、そのユーザーの ID と、Citrix DaaS でその ID にどのリソースが関連付けられているかによって異なります。Workspace への認証のための SAML プロバイダーとして Azure AD ID および AD ID を利用する手順を説明する関連記事があります。詳しい手順については、「ワークスペース認証で Azure AD ID と Azure Active Directory ID を使用して SAML を構成する」を参照してください

機能範囲

この記事は、Citrix Cloud の機能と Azure の機能を次のように組み合わせて使用するユーザーに適用できます:

- ワークスペースの SAML 認証
- AD ドメインに参加している 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
- Azure AD ドメインに参加している VDA リソースの列挙
- Azure ハイブリッドドメインに参加している VDA リソースの列挙
- W365 クラウド PC の列挙と起動

> 重要:
>
> Citrix Cloud への SAML ログインにはこの AAD SAML フローを使用しないでください。この場合、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、AD ユーザー ID を使用する必要があるためです。詳しい手順については、「ワークスペース認証で Azure AD ID と Azure Active Directory ID を使用して SAML を構成する」を参照してください

AD ID と **Azure AD ID** のどちらが最適か

管理対象のワークスペースユーザーに SAML AD または SAML Azure AD ID のどちらで認証させるかを判断するには、次のようにします:

1. Citrix Workspace でユーザーが利用できるようにするリソースの組み合わせを決定します。
2. 次の表を使用して、リソースの種類ごとにどの種類のユーザー ID が適切かを判断します。

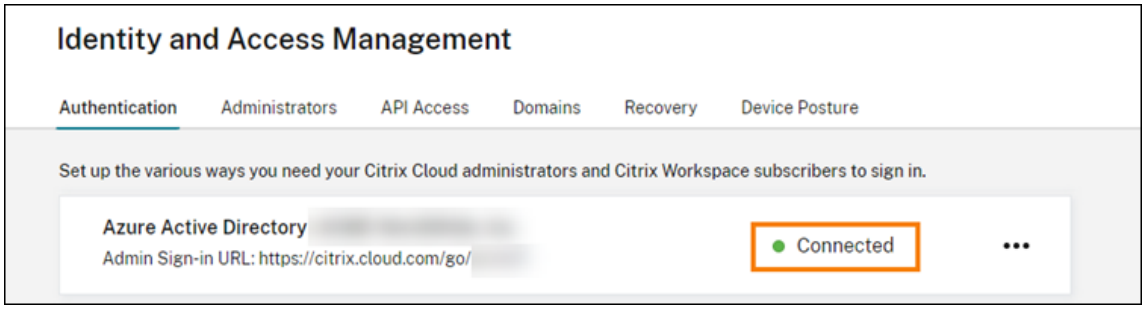
リソースの種類（VDA）	Citrix Workspace にサインインするときのユーザー ID	Azure AD を使用した SAML ID が必要ですか?	FAS は VDA にシングルサインオン（SSO）を提供しますか?
AD に参加済み	AD、AD からインポートされた Azure AD（SID を含む）	いいえ。デフォルトの SAML を使用します。	はい
ハイブリッドに参加済み	AD、AD からインポートされた Azure AD（SID を含む）	いいえ。デフォルトの SAML を使用します。	ID プロバイダーとして AD を使用する場合は提供します。VDA に Azure AD が選択されている場合、FAS は必要ありません。
Azure AD に参加済み	Azure AD ネイティブユーザー、AD からインポートされた Azure AD（SID を含む）	はい、Azure AD 経由で SAML を使用します。	SSO は Azure AD 先進認証と連携しています。FAS は必要ありません。
Windows 365 クラウド PC	Azure AD ネイティブユーザー、AD からインポートされた Azure AD（SID を含む）	はい、Azure AD 経由で SAML を使用します。	SSO は Azure AD 先進認証と連携しています。FAS は必要ありません。
AD に参加済み、Azure AD に参加済み、Windows 365 クラウド PC	AD からインポートされた Azure AD（SID を含む）	はい、Azure AD 経由で SAML を使用します。	AD に参加済みの場合は提供します。Azure AD に参加済みの場合と Windows 365 クラウド PC の場合は提供しません。

追加情報

- Citrix DaaS ドキュメント：
  - マシン ID
  - Citrix HDX Plus for Windows 365
- Citrix FAS ドキュメント：インストールと構成
- Microsoft Azure ドキュメント：Azure AD Connect とは

要件

- Azure AD テナントは Citrix Cloud テナントに接続する必要があります。Citrix Cloud コンソールで［**ID** およびアクセス管理］**>**［認証］を選択すると、Azure AD 接続を見つけることができます。



- ワークスペースの認証方法としては［**SAML 2.0**］を設定する必要があります。認証方法として［Azure AD］を使用しないでください。ワークスペースの認証方法を変更するには、Citrix Cloud コンソールで［ワークスペースを構成する］**>**［認証］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 Azure AD 内にインポートして検証する必要があります。Azure Portal では、これは ［**Azure Active Directory**］**>**［カスタムドメイン名］の下にあります。
- Azure AD のユーザー ID は、Microsoft Azure AD 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 サフィックスが付けられるようになります。`@yourtenant.onmicrosoft.com` UPN サフィックスがある Azure AD ユーザーはサポートされません。
- Citrix FAS を展開し、Citrix Cloud のテナントおよびリソースの場所に接続する必要があります。FAS は、Citrix Workspace 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 Azure AD の両方のユーザー ID に対する 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、HDX リソースの起動時に、正しい UPN を使用して必要なユーザー証明書を生成し、スマートカードサインインを実行します。

カスタム **Azure AD Enterprise SAML** アプリケーションを構成する

デフォルトでは、ワークスペースへの 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、どのサブスクライバに対しても不変となる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 および Citrix Workspace は、サインイン中にこの属性を検出し、Azure AD バージョンのユーザー ID に対してアサートするように SAML をトリガーします。この属性で **azuread** パラメータを使用すると、デフォルトの SAML 動作が Azure AD での SAML の使用のトリガーで上書きされます。

このセクションの手順は Azure AD を対象としていますが、同様の SAML アプリケーションを作成することもできます（ただし、同じタスクを実行する場合）。それには、別の SAML 2.0 プロバイダー（ADFS、Duo、Okta、OneLogin、PingOneSSO など）を使用します。SAML プロバイダーは、あなたが SAML アプリケーション内で SAML 属性をハードコードして（cip_directory = azuread）構成することを許可するプロバイダーである必要があります。構成すると言っても、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 Portal にサインインします。
2. Portal のメニューから、［**Azure Active Directory**］を選択します。

3. 左側のペインの［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、［**New Application**］を選択します。
5. コマンドバーから、［**Create your own application**］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、要求と SAML 属性のリストを変更できないためです。
6. アプリケーションの名前を入力し、［**Integrate any other application you don't find in the gallery (Non-gallery)**］を選択します。［**Create**］をクリックします。［application overview］ページが表示されます。
7. 左側のペインで、［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. ［**Basic SAML Configuration**］セクションで、［編集］を選択し、次の設定を構成します。

   a) ［**Identifier**（**Entity ID**）］セクションで、［**Add identifier**］を選択し、Citrix Cloud テナントが配置されているリージョンに対応する値を入力します：
      - 欧州連合、米国、およびアジア太平洋南部の各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) ［**Reply URL (Assertion Consumer Service URL)**］セクションで、［**Add reply URL**］を選択し、Citrix Cloud テナントが存在するリージョンに対応する値を入力します：
      - 欧州連合、米国、およびアジア太平洋南部の各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) ［ログアウト **URL**（オプション）］セクションで、Citrix Cloud テナントが存在するリージョンに対応する値を入力します：
      - 欧州連合、米国、およびアジア太平洋南部の各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［保存］を選択します。

9. ［**Attributes & Claims**］セクションで［編集］を選択し、以下の要求を構成します。これらの要求は、SAML 応答内の SAML アサーションに表示されます。

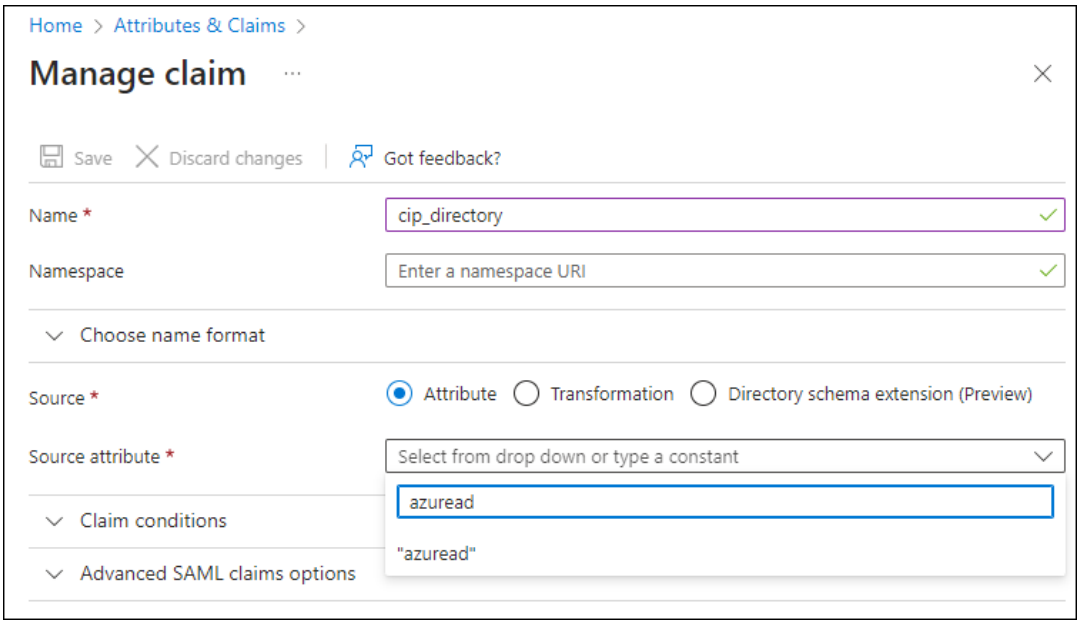
a) ［**Unique User Identifier (Name ID)**］要求については、`user.userprincipalname`のデフォルト値のままにします。

b) コマンドバーから［**Add new claim**］を選択します。

c) ［名前］に「**cip_directory**」と入力します。

d) ［ソース］で、［属性］を選択済みの値のままにします。

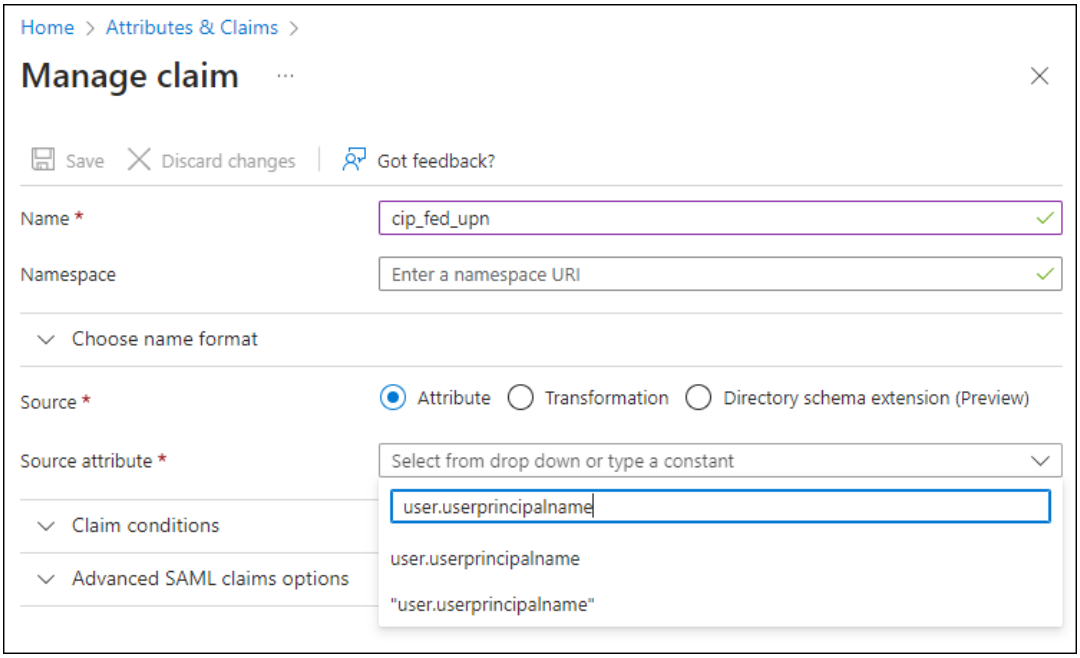
e) ［ソース属性］に「**azuread**」と入力します。この値は、入力後、引用符で囲まれて表示されます。



f) コマンドバーから［保存］を選択します。

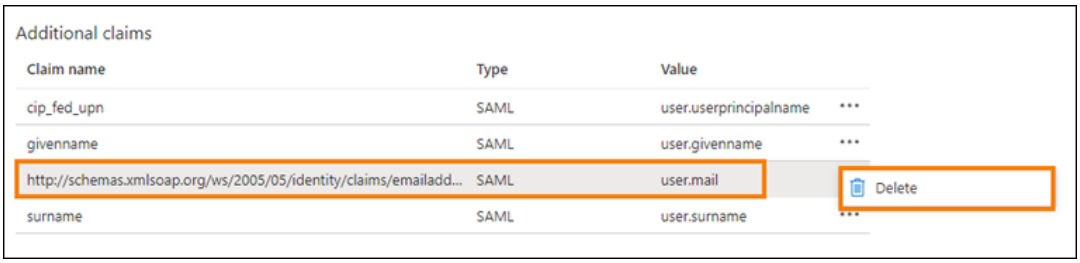
g) ［名前］フィールドと［ソース 属性］フィールドに以下の値を使用して、追加の要求を作成します。

名前	ソース属性
cip_fed_upn	user.userprincipalname
displayName	user.displayname
firstName	user.givenname
lastName	user.surname

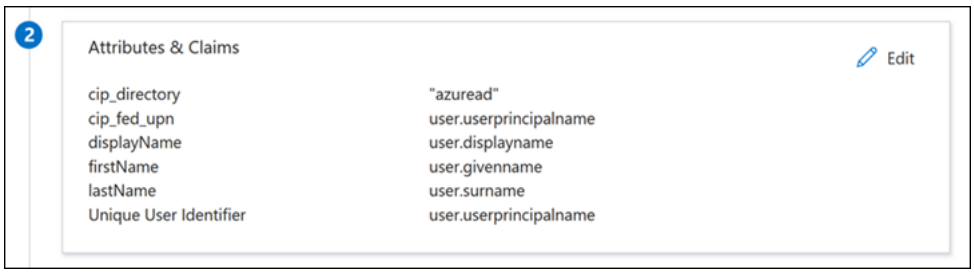


> 重要:
>
> これらの追加の要求を作成するには、要求ごとに手順 b～f を繰り返すか、上記の表にリストされているソース属性が既に含まれている［**Additional claims**］セクションのデフォルト要求を変更します。デフォルトの要求には名前空間 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`が含まれています。
>
> デフォルトの要求を変更する場合は、各要求から名前空間を削除する必要があります。新しい要求を作成する場合は、それらのうち、名前空間を含む要求を削除する必要があります。この名前空間を持つ要求が結果の SAML アサーションに含まれる場合には、そのアサーションは不正な SAML 属性名を含むことになって無効になります。

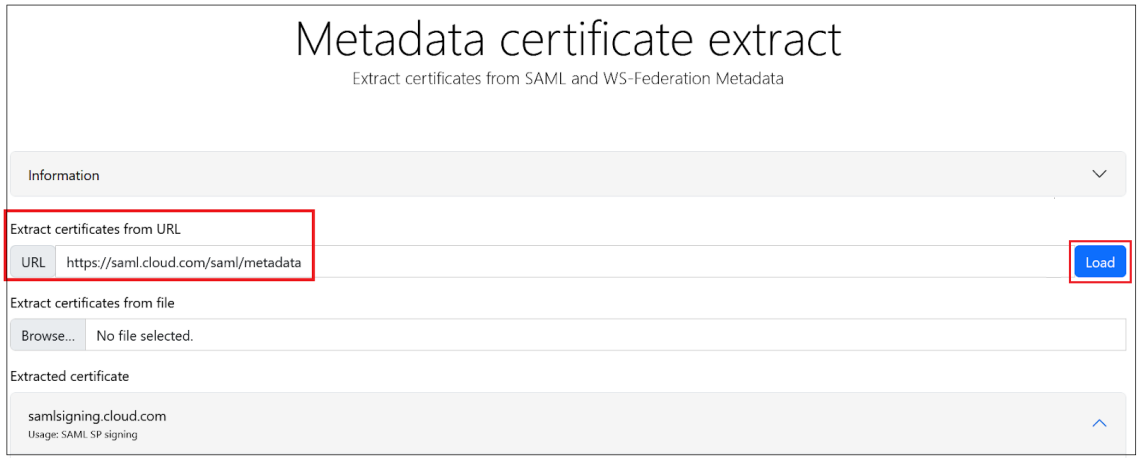
h) ［**Additional claims**］セクションで、名前空間`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`を持つ要求が残っていれば、［省略記号（…）］をクリックし、［削除］をクリックします。



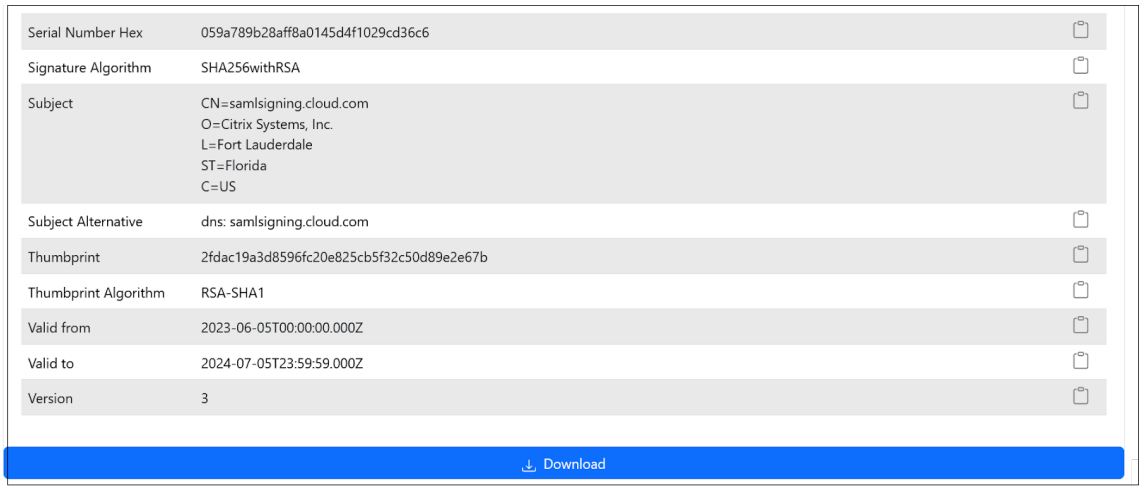
完了すると、下図のような［**Attributes & Claims**］セクションが表示されます。

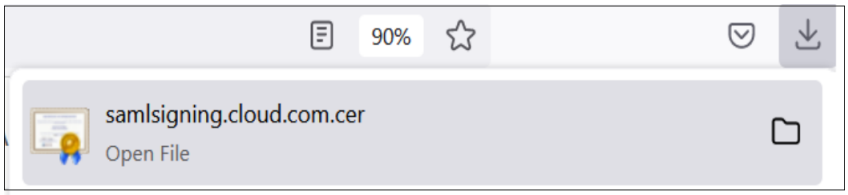


10. この サードパーティのオンラインツール を使用して、Citrix Cloud SAML 署名証明書のコピーを取得します。
11. URL フィールドにhttps://saml.cloud.com/saml/metadataを入力し、［読み込み］をクリックします。



12. ページの下までスクロールして、［ダウンロード］をクリックします。

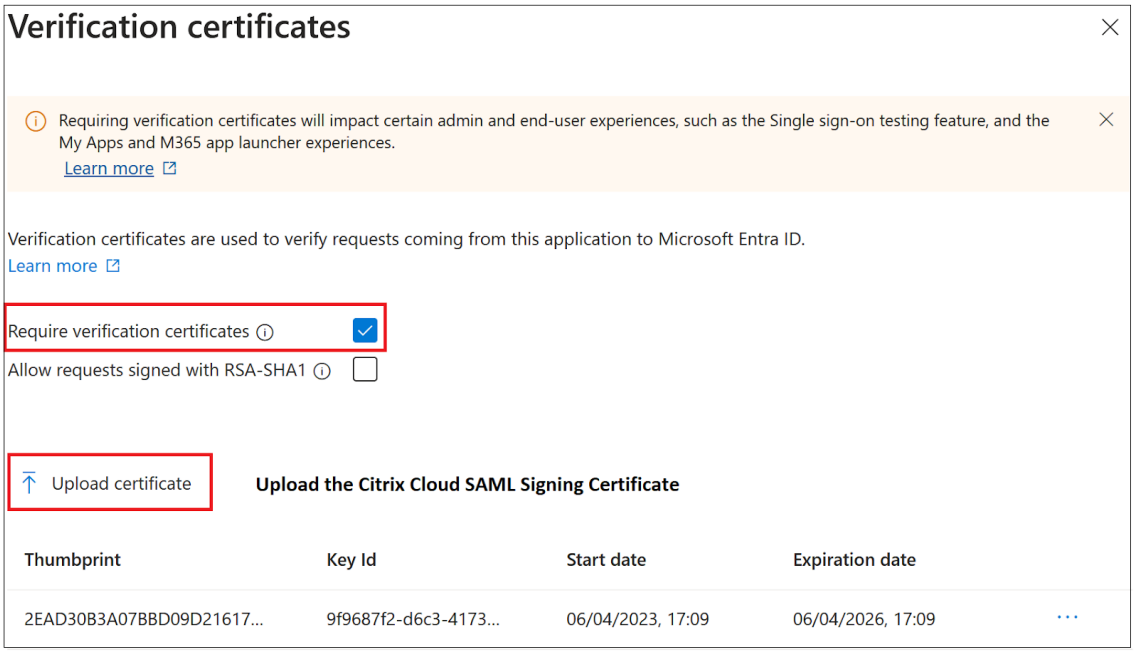


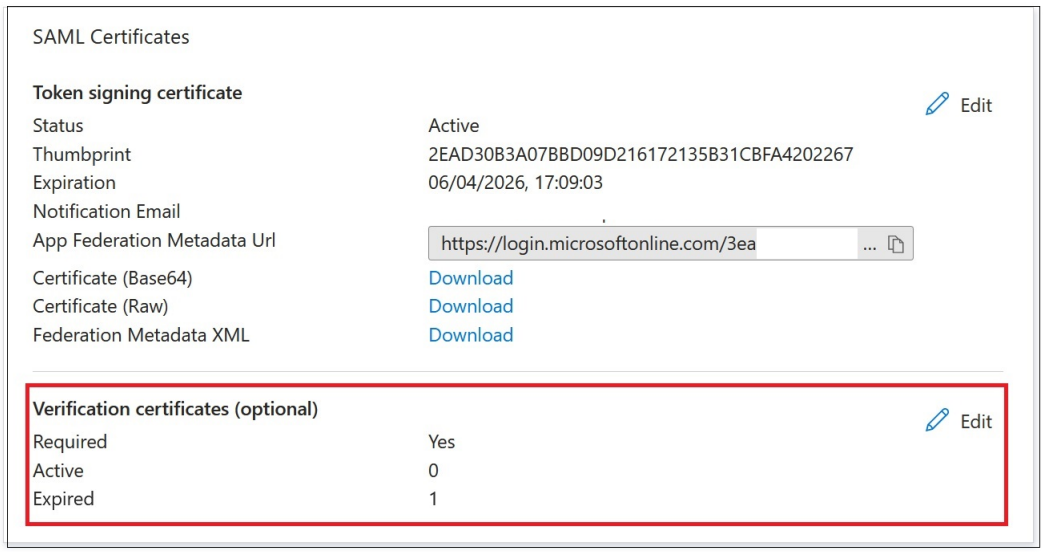


13. Azure Active Directory SAML アプリケーションの署名設定を構成します。

14. 手順 10 で取得した実稼働 SAML 署名証明書を Azure Active Directory SAML アプリケーション内にアップロードします。

    - ［検証証明書が必要］を有効にします。





トラブルシューティング

1. ブラウザー拡張機能 SAML-tracer 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かを確認します。
2. 黄色で示されている SAML 応答を見つけて、次の例と比較します：

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かを確認します。

それでも利用者がワークスペースにサインインできない場合、Citrix サポートに連絡し、次の情報を提供してください：

- SAML-tracer のキャプチャ
- Citrix Workspace へのサインインが失敗した日時
- 影響を受けているユーザー名
- Citrix Workspace 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などのツールを使用できます。

ワークスペース認証で **Azure AD ID** と **AD ID** を使用する **SAML**

May 30, 2024

Author:
Mark Dear

この記事では、Active Directory（AD）ID を使用する SAML をワークスペース認証用に構成する方法について説明します。Citrix Cloud、および Citrix Workspace または Citrix Cloud に対する SAML 認証のデフォルトの動作

は、SAML プロバイダーの使用にかかわらず、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、Azure AD Connect を使用して AD ID を Azure AD にインポートする必要があります。

> 重要:
>
> Workspace の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表示に直接影響するため、非常に重要です。選択した ID によって、Workspace のエンドユーザーがアクセスできるリソースの種類が変わります。
> AAD ID を使用した Workspace への認証のための SAML プロバイダーとして、Azure AD を利用する手順を説明する関連記事があります。詳しい手順については、「ワークスペース認証で Azure AD ID と AAD ID を使用した SAML」を参照してください。
> 通常、Workspace のエンドユーザーは、AD ドメインに参加している 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使用例を慎重に確認することが重要です。どちらを使用するか不明な場合は、最も一般的な DaaS シナリオに沿った **AD SAML** フローを使用し、記事の手順に従うことをお勧めします。

機能範囲

この記事は、Citrix Cloud の機能と Azure の機能を次のように組み合わせて使用するユーザーに適用できます:

- ワークスペース認証で AD ID を使用する SAML
- Citrix Cloud 管理者ログインで AD ID を使用する SAML
- AD ドメインに参加している 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 ドメインに参加している VDA リソースの列挙

AD ID と **Azure AD ID** のどちらが最適か

管理対象のワークスペースユーザーに SAML AD または SAML Azure AD ID のどちらで認証させるかを判断するには、次のようにします:

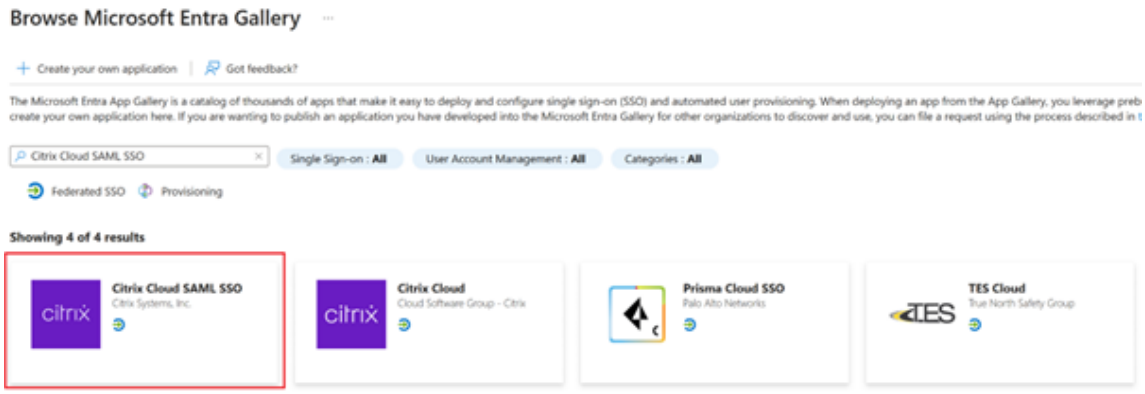
1. Citrix Workspace でユーザーが利用できるようにするリソースの組み合わせを決定します。
2. 次の表を使用して、リソースの種類ごとにどの種類のユーザー ID が適切かを判断します。

リソースの種類（VDA）	Citrix Workspace にサインインするときのユーザー ID	Azure AD を使用した SAML ID が必要ですか?	FAS は VDA にシングルサインオン（SSO）を提供しますか?
AD に参加済み	AD、AD からインポートされた Azure AD（SID を含む）	いいえ。デフォルトの SAML を使用します。	はい

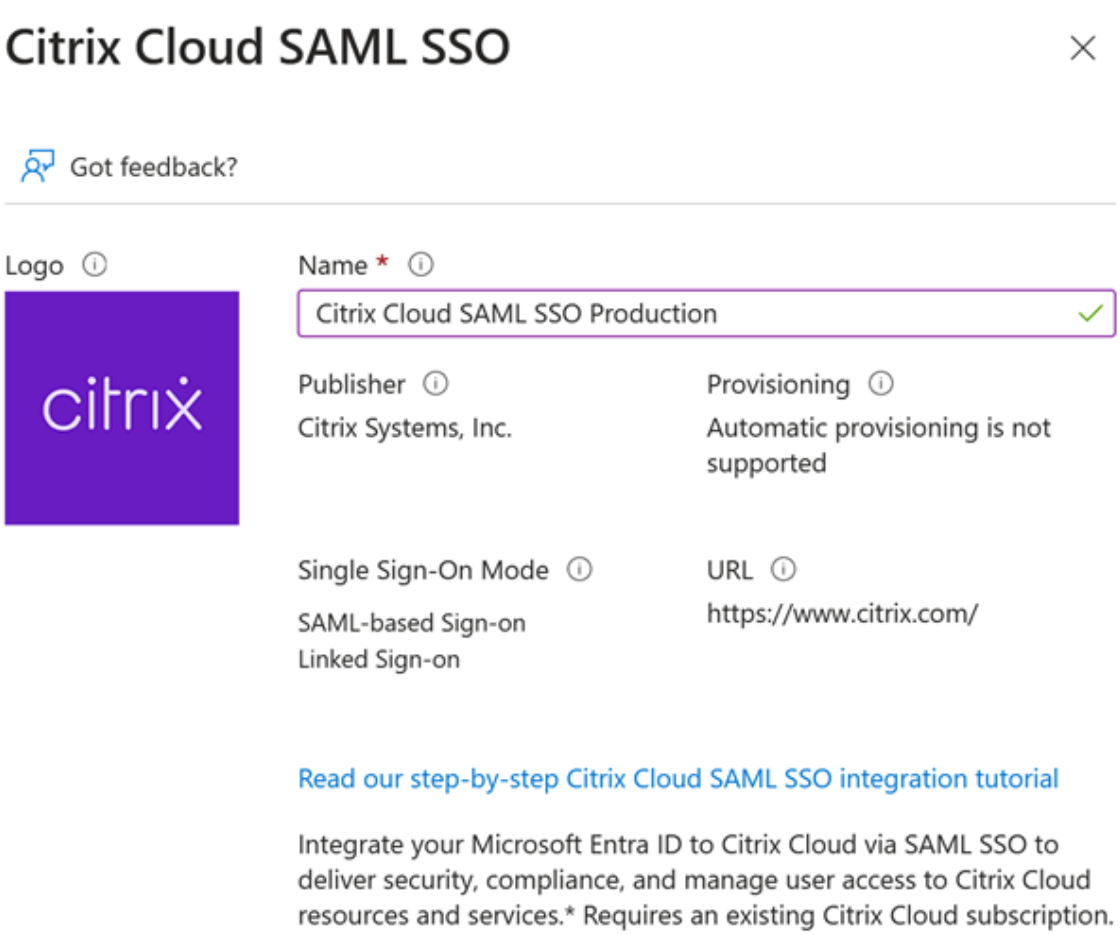
カスタム **Azure AD Enterprise SAML** アプリケーションを構成する

デフォルトでは、ワークスペースへの 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 Portal にサインインします。
2. Portal のメニューから、[**Azure Active Directory**] を選択します。
3. 左側のペインの［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. 検索ボックスに「`Citrix Cloud SAML SSO`」と入力して、Citrix SAML アプリケーションテンプレートを見つけます。



5. SAML アプリケーションの適切な名前を入力します。例:`Citrix Cloud SAML SSO Production`



6. 左側のナビゲーション ペインで ［**Single sign-on**］を選択し、作業ペインで ［**SAML**］をクリックします。
7. ［**Basic SAML Configuration**］セクションで、［**Edit**］を選択し、次の設定を構成します:

   a) ［**Identifier**（**Entity ID**）］セクションで、［**Add identifier**］を選択し、Citrix Cloud テナントが配置されているリージョンに対応する値を入力します:

   - 欧州、米国、およびアジア太平洋南部の各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) ［**Reply URL (Assertion Consumer Service URL)**］セクションで、［**Add reply URL**］を選択し、Citrix Cloud テナントが存在するリージョンに対応する値を入力します:

   - 欧州、米国、およびアジア太平洋南部の各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) [**Sign on URL**] セクションに、Workspace 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 テナントが存在するリージョンに対応する値を入力します：

- 欧州、米国、およびアジア太平洋南部の各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 リージョンの場合は、「https://saml.cloud.us/saml/logout/callback」と入力します。

e) コマンドバーで、[**Save**] をクリックします。[**Basic SAML Configuration**] セクションが以下のように表示されます：

8. [**Attributes & Claims**] セクションで［**Edit**］を選択し、以下の要求を構成します。これらの要求は、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。

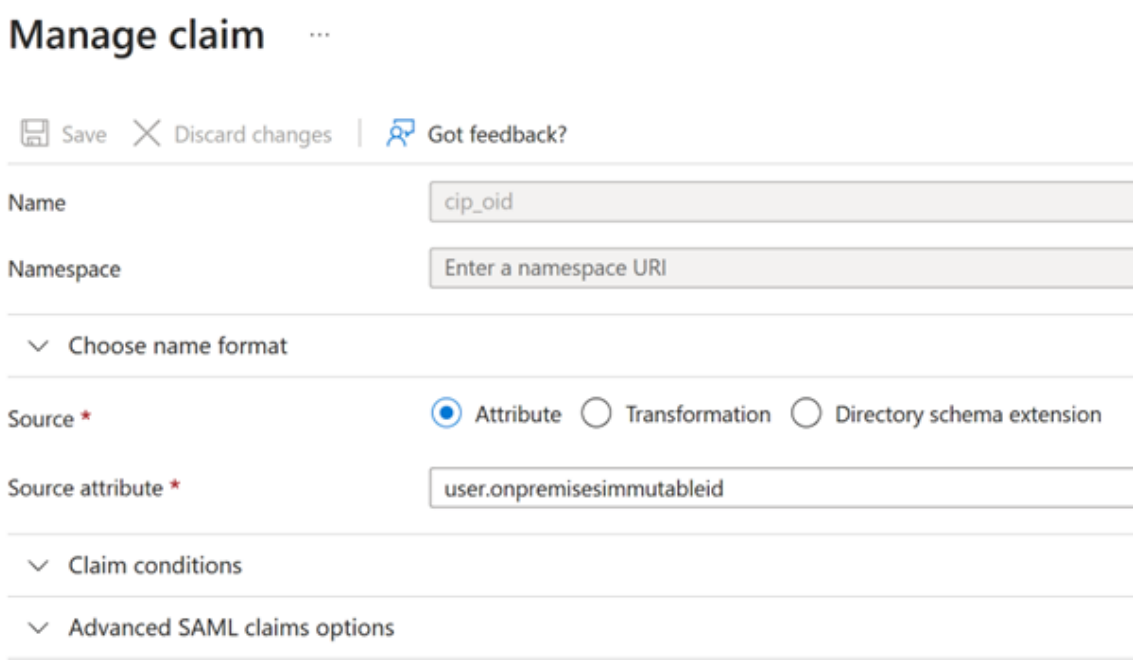
a) [**Unique User Identifier (Name ID)**] 要求については、user.userprincipalnameのデフォルト値のままにします。

b) **cip_upn** 要求では、デフォルト値のuser.userprincipalnameのままにします。

c) **cip_email** 要求では、デフォルト値のuser.mailのままにします。

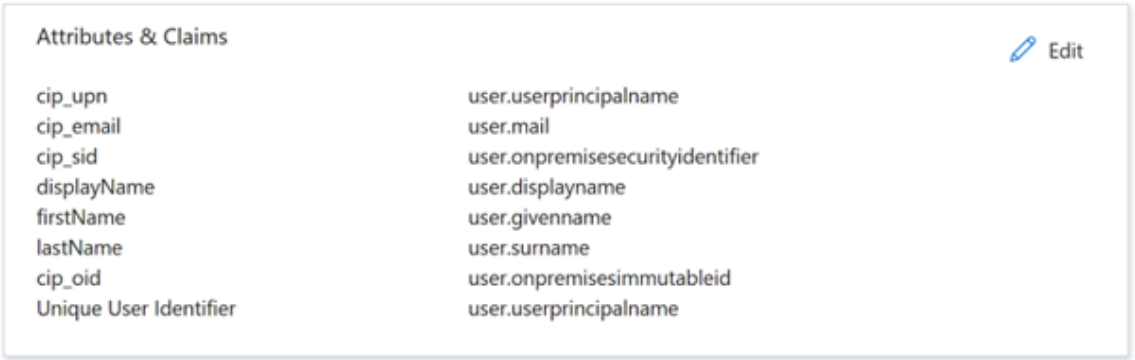
d) **cip_sid** 要求では、デフォルト値のuser.onpremisesecurityidentitierのままにします。

e) **cip_oid** 要求では、既存の要求を編集し、**Source** 属性を選択します。文字列`object`を検索し、`user.onpremisesimmutableid`を選択します。



a) **displayName** では、デフォルト値の`user.displayname`のままにします。

b) [**Additional claims**] セクションで、名前空間`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`を持つ要求が残っていれば、[省略記号 (…)] をクリックし、[削除] をクリックします。これらの要求は上記の user 属性と重複するため、含める必要はありません。

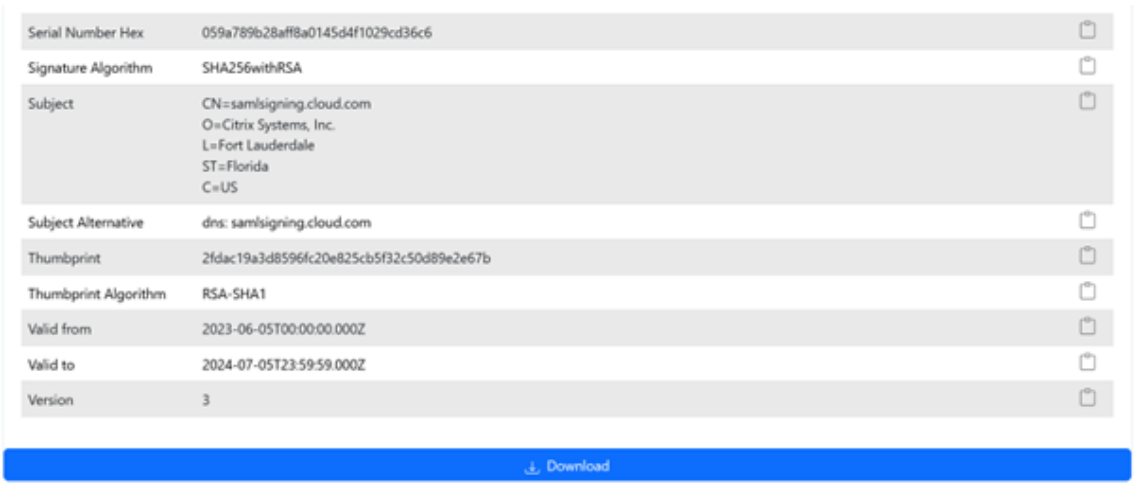


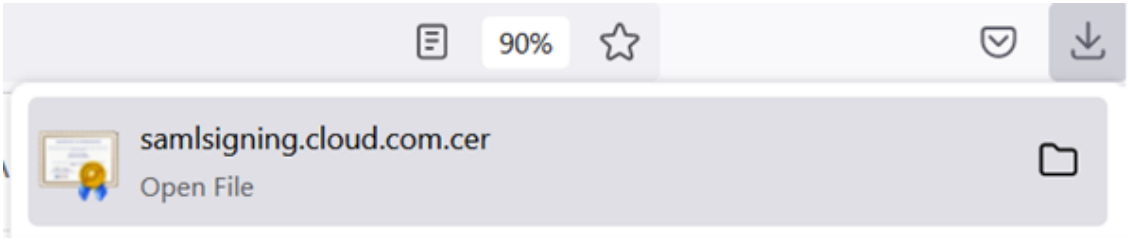
完了すると、下図のような [**Attributes & Claims**] セクションが表示されます。

a) 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。

b) URL フィールドに`https://saml.cloud.com/saml/metadata`を入力し、[**Load**] をクリックします。

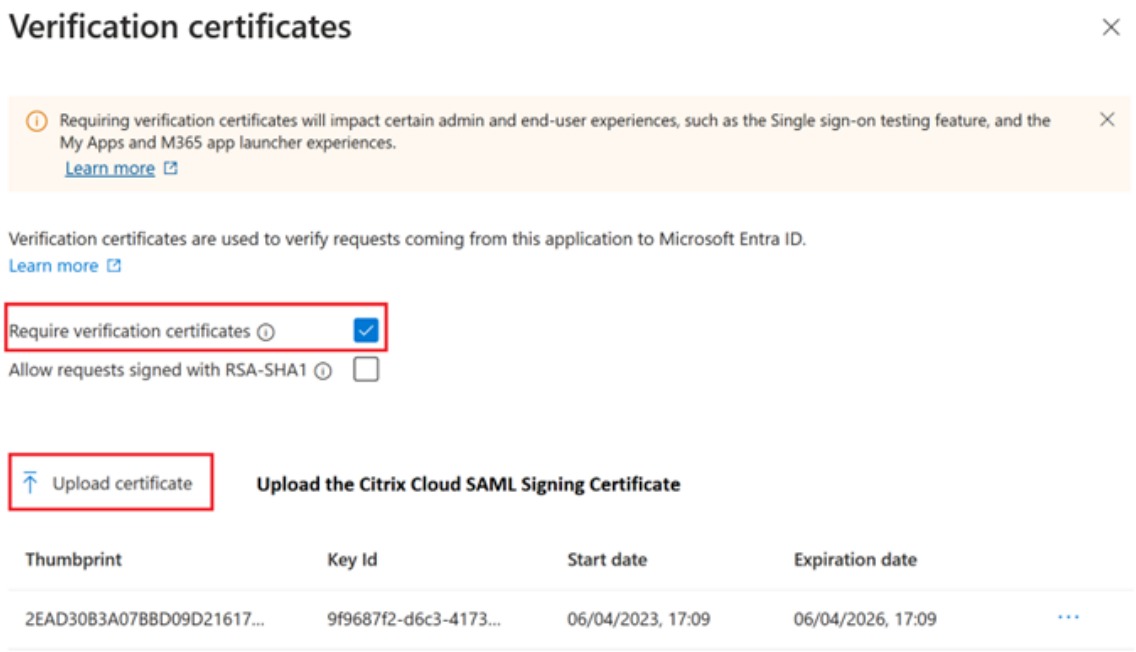
9. ページの下までスクロールして、[ダウンロード] をクリックします。

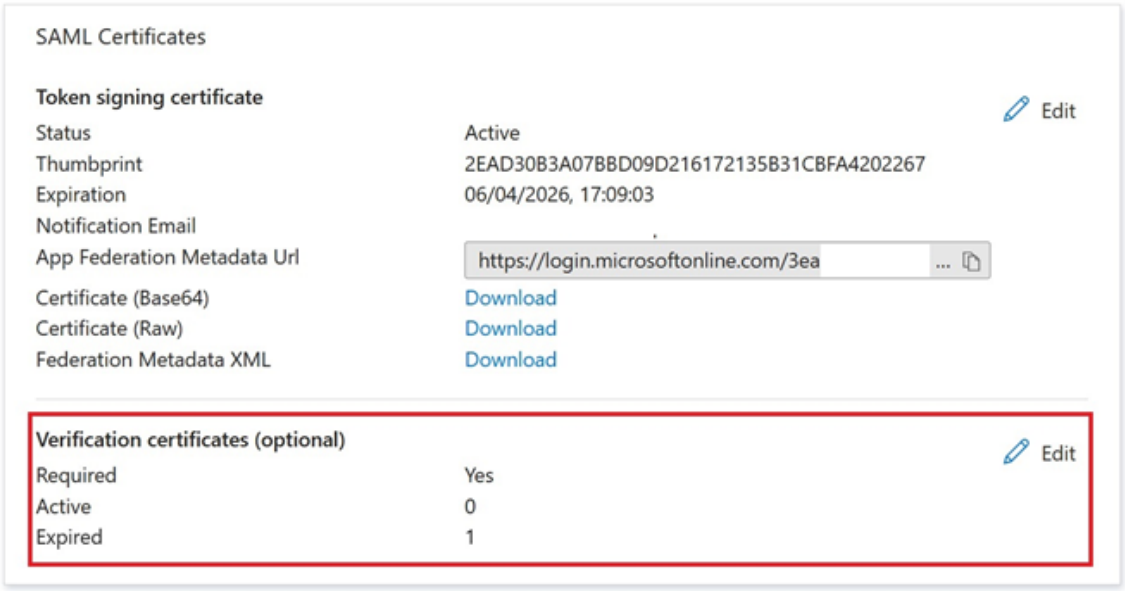




10. Azure Active Directory SAML アプリケーションの署名設定を構成します。
11. 手順 10 で取得した実稼働 SAML 署名証明書を Azure Active Directory SAML アプリケーション内にアップロードします

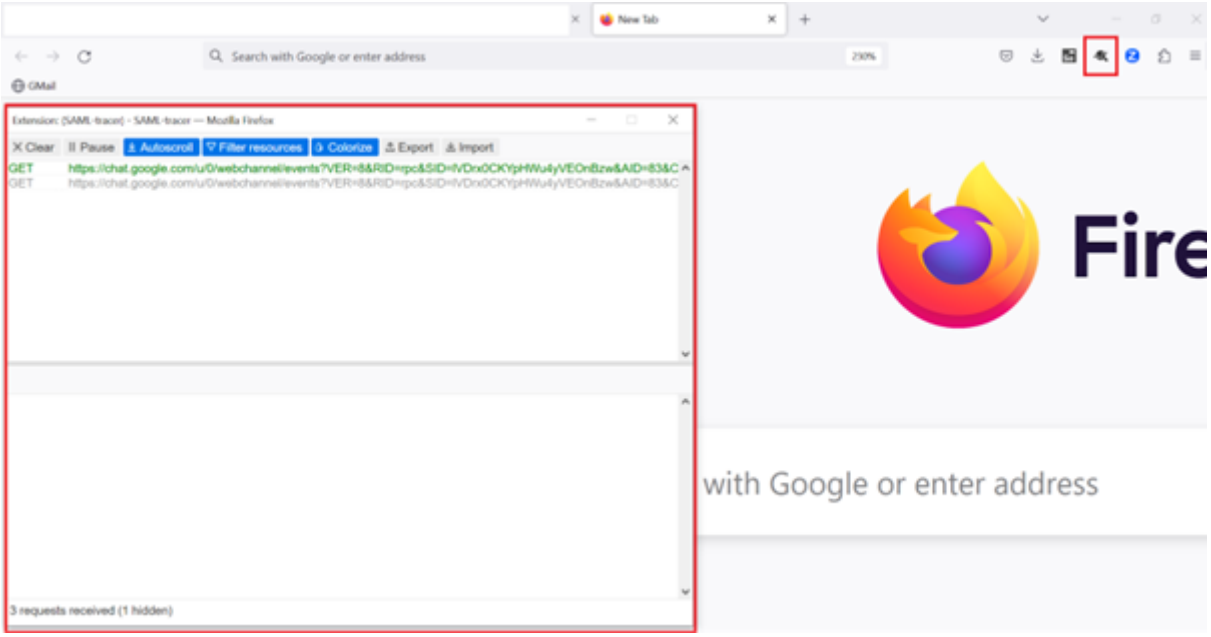
    a)［検証証明書が必要］を有効にします。





トラブルシューティング

1. ブラウザー拡張機能 SAML-tracer 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かを確認します。



1. 黄色で示されている SAML 応答を見つけて、次の例と比較します:

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かを確認します。

これでも利用者がワークスペースにサインインできないか、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、次の情報を提供してください。

- SAML-tracer のキャプチャ
- Citrix Workspace へのサインインが失敗した日時
- 影響を受けているユーザー名
- Citrix Workspace 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などのツールを使用できます。

ネイティブおよびゲスト **SAML** ユーザーに簡易 **SAML** の使用を構成

July 3, 2024

Author:
Mark Dear, Javier Lopez Santacruz

この記事を読む前に、「簡易 SAML」がご利用環境での認証のユースケースに適しているかどうかを理解しておく必要があります。この特別なケースの SAML ソリューションの実装を決定する前に、ユースケースの説明と FAQ をよくお読みください。先に進む前に、簡易 SAML の使用が適切なシナリオと、どの ID タイプを使用する必要があるかを十分に理解しておいてください。SAML の大半のユースケースでは、他の SAML の記事に記載されている、認証用に 4 つの cip_* 属性をすべて送信することで対応できます。

> 注:
>
> 「簡易 SAML」を使用すると、SAML アサーションによって提供される値ではなく、Workspace のエンドユーザーがログオンするたびにユーザーのメール、SID、OID を検索する必要があるため、Citrix Cloud Connector にかかる負荷が増加します。簡易 SAML が必須ではない場合は、Citrix Cloud Connector のパフォーマンスの観点から、SAML アサーションの 4 つの cip_* 属性をすべて送信することをお勧めします。

前提条件

- SAML アサーション内の認証で **cip_upn** のみを送信する、簡易 SAML で使用する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。
- リソースの場所に、AD シャドウアカウントが作成された AD フォレストとドメインに参加済みの Citrix Cloud Connector のペアが含まれる。
- AD シャドウアカウントが作成されるバックエンド AD フォレストに追加された、代替 UPN サフィックス。
- 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プされた DaaS または CVAD リソース。
- 同じリソースの場所にリンクされている 1 つまたは複数の FAS サーバー。

よくある質問

簡易 **SAML** を使うべきなのはなぜですか**?**

大規模な組織では、契約社員や派遣社員を ID プラットフォームに招待することがよくあります。目的は、こうした契約社員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、契約社員に Citrix Workspace への一時的なアクセスを許可することです。簡易 SAML では、DaaS リソースが公開されている AD ドメイン内には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 を使用できます。

簡易 **SAML** とは何ですか**?**

通常、Citrix Workspace にサインインする場合、4 つの SAML 属性 cip_* とそれに対応する AD ユーザー属性がエンドユーザーの認証に使用されます。これらの 4 つの SAML 属性は SAML アサーションに存在し、AD ユーザー属性を使用して入力されます。簡易 SAML では、認証を成功させるために必要なのは cip_upn SAML 属性のみであるという事実を利用します。

AD 属性	SAML アサーションのデフォルトの属性名
userPrincipalName	cip_upn
Mail	cip_email

AD 属性	SAML アサーションのデフォルトの属性名
objectSID	cip_sid
objectGUID	cip_oid

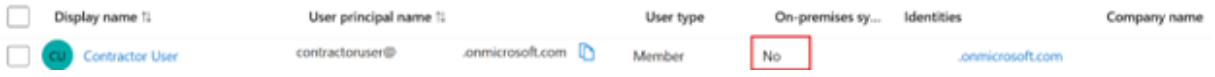
認証に必要な他の 3 つの AD ユーザー属性 objectSID、objectGUID、および mail は、AD シャドウアカウントが存在する AD ドメインに参加している Citrix Cloud Connector を使用して取得されます。Workspace または Citrix Cloud の SAML サインインフロー中に、これらを SAML アサーションに含める必要がなくなりました。

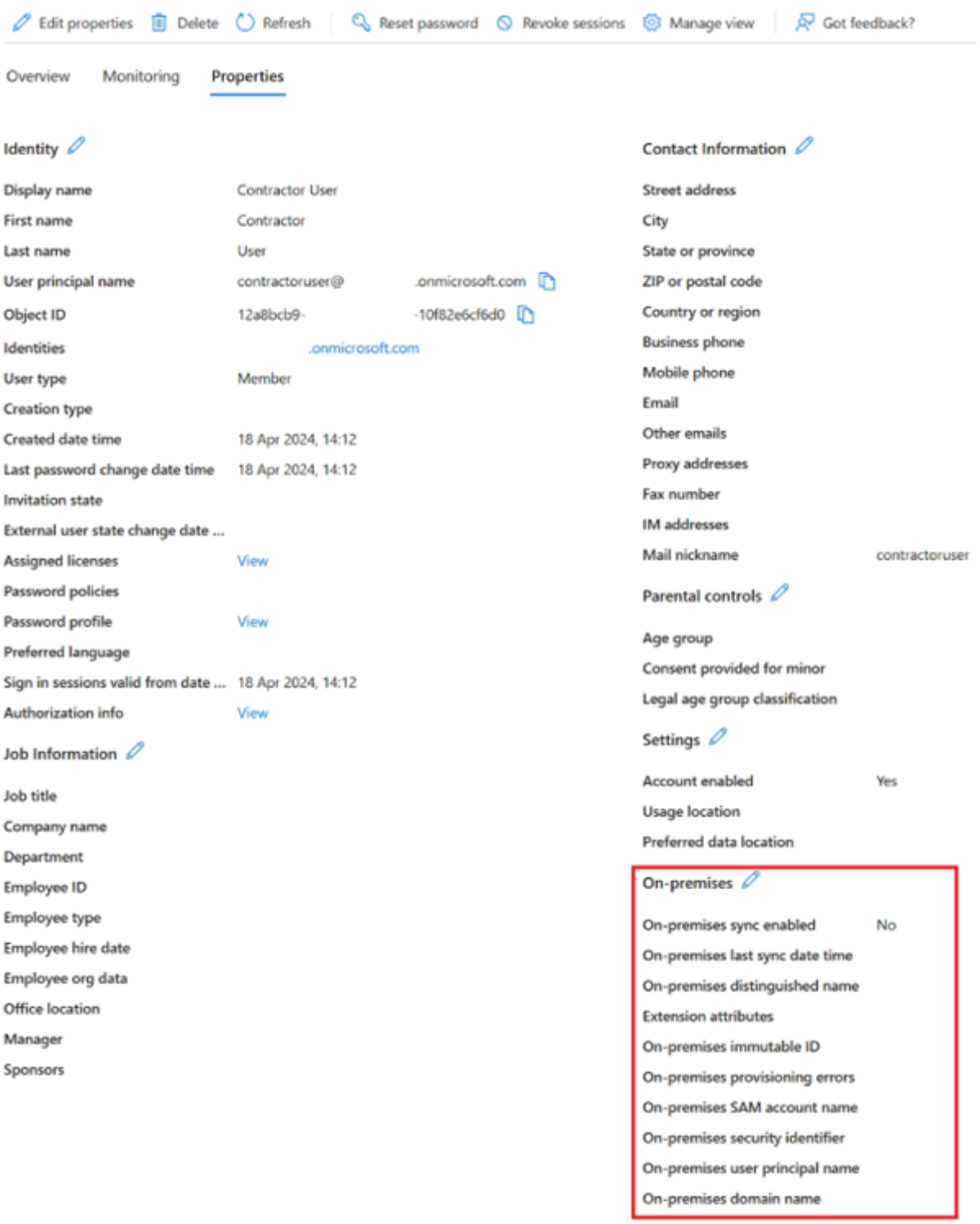
AD 属性	SAML アサーションのデフォルトの属性名
userPrincipalName	cip_upn

> 重要:
>
> ただし、簡易 SAML を含むすべての SAML フローで、依然として **displayName** は送信する必要があります。Workspace UI で Workspace ユーザーのフルネームを正しく表示するには、**displayName** が必要です。

ネイティブ **SAML** ユーザー **ID** とは何ですか**?**

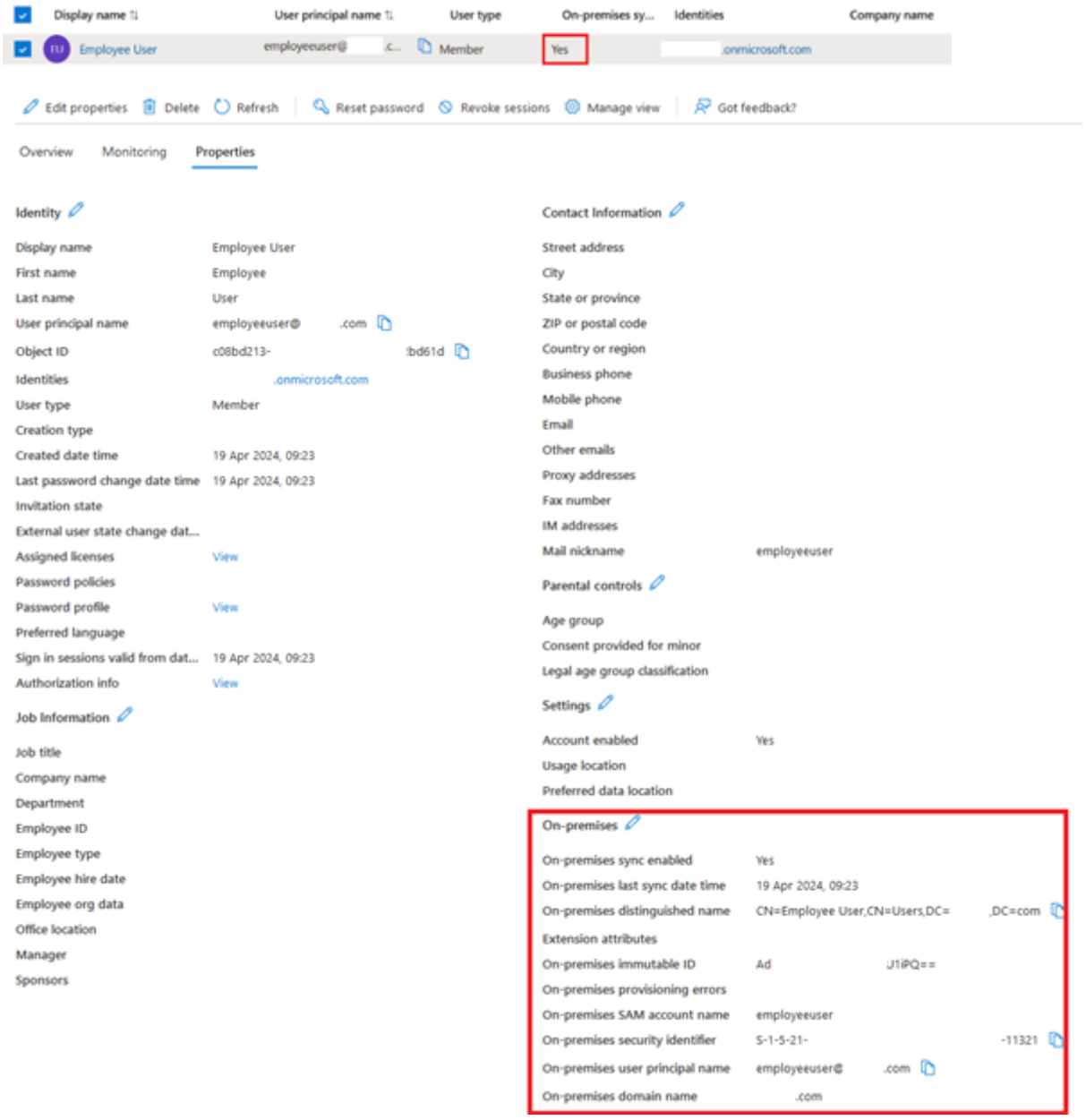
ネイティブ SAML ユーザーとは、Entra ID や Okta など、SAML プロバイダーディレクトリ内にのみ存在するユーザー ID です。これらの ID には、オンプレミスのユーザー属性は含まれていません。Entra ID Connect などの AD 同期ツールで作成されないためです。DaaS リソースを列挙して起動するには、一致するバックエンド AD シャドウアカウントが必要です。ネイティブ SAML ユーザーは Active Directory 内の対応するアカウントにマップされている必要があります。





AD ベースの **SAML** ユーザー **ID** とは何ですか**?**

AD ベースの SAML ユーザーは、Entra ID や Okta などの SAML プロバイダーディレクトリ内に存在するユーザー ID であり、オンプレミスの AD フォレスト内にも存在します。Entra ID Connect などの AD 同期ツールで作成されるため、これらの ID にはオンプレミスのユーザー属性が含まれます。オンプレミスの SID と OID が含まれ、DaaS リソースを列挙して起動できるため、これらのユーザーにはバックエンド AD シャドウアカウントは必要ありません。

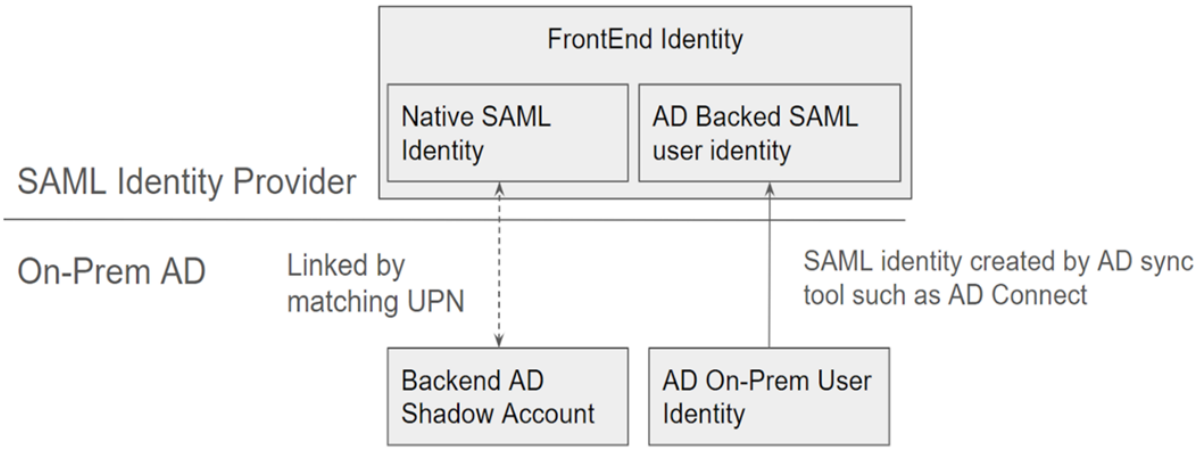


フロントエンド **ID** とは何ですか**?**

フロントエンド ID は、SAML プロバイダーと Workspace 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 のユーザー属性は、SAML プロバイダー内での作成方法によって異なります。

1. ネイティブ SAML ユーザー ID
2. AD ベースの SAML ユーザー ID

SAML プロバイダーには、これら 2 つの ID タイプが混在している場合があります。たとえば、ID プラットフォームに契約社員と正社員の両方がいる場合、簡易 SAML はどちらのタイプのフロントエンド ID でも機能しますが、ネイティブ SAML ユーザー ID タイプ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 にマップされます。

バックエンド **AD** シャドウアカウントが必要なのはなぜですか**?**

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と、VDA が参加している AD ドメイン内のシャドウアカウントを含む AD グループにマップします。

> 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 を Active Directory からインポートする場合、簡易 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方法を教えてください

フロントエンド ID とバックエンド ID をリンクする方法には、一致する UPN を使用する方法があります。Workspace へのサインインが必要な同じエンドユーザーであること、および DaaS リソースを列挙して起動する必要があることを Workspace が認識できるように、リンクされた 2 つの ID には同じ UPN が必要です。

簡易 **SAML** には **Citrix FAS** が必要ですか**?**

はい。任意のフェデレーション認証方法を使用して Workspace にサインインする場合、起動時に VDA への SSON に FAS が必要です。

「**SID** の不一致問題」とは何ですか**?** また、どのような場合に発生しますか**?**

「SID の不一致問題」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しているアカウントにオンプレミス SID があり、それがシャドウアカウントユーザーの SID とは異なる場合に発生する可能性があります。これは、フロントエンド ID が Entra ID Connect などの AD 同期ツールによってプロビジョニングされ、それがシャドウアカウントが作成された AD フォレストではないところからのプロビジョニングであった場合にのみ発生します。

簡易 SAML は、「SID の不一致問題」の発生を防ぎます。シャドウアカウントユーザーの正しい SID は、常にバックエンド AD ドメインに参加している Citrix Cloud Connector を使用して取得されます。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、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 の不一致問題の例:
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** から同期されました。
`S-1-5-21-000000000-0000000000-0000000001-0001`

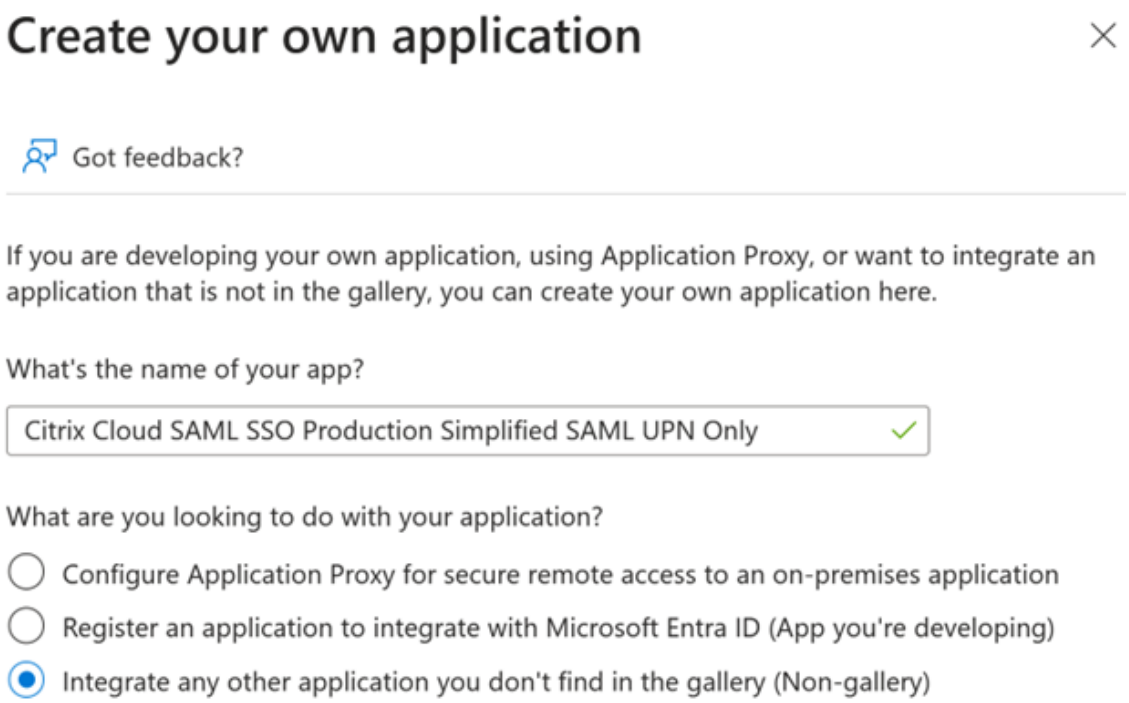
バックエンドシャドウアカウントユーザーは **AD** フォレスト **2** 内で作成され、DaaS リソースにマップされました
`S-1-5-21-000000000-0000000000-0000000002-0002`

SAML アサーションには 4 つの cip_* 属性がすべて含まれ、**cip_sid** には値`S-1-5-21-000000000-0000000000-0000`が含まれます。これはシャドウアカウントの SID と一致しないため、エラーが発生します。

外部ゲストアカウント用に **Entra ID** を使用して簡易 **SAML** を構成する

1. Azure Portal 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. 左側のペインの［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. [**Create your own application**] を選択します。
5. SAML アプリケーションの適切な名前を入力します。例:`Citrix Cloud SAML SSO Production Simplified SAML`。



6. 左側のナビゲーション ペインで [**Single sign-on**] を選択し、作業ペインで [**SAML**] をクリックします。
7. [**Basic SAML Configuration**] セクションで、[**Edit**] を選択し、次の設定を構成します:

   a) [**Identifier**（**Entity ID**）] セクションで、[**Add identifier**] を選択し、Citrix Cloud テナントが配置されているリージョンに対応する値を入力します:

   - 欧州、米国、およびアジア太平洋南部の各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) [**Reply URL (Assertion Consumer Service URL)**] セクションで、[**Add reply URL**] を選択し、Citrix Cloud テナントが存在するリージョンに対応する値を入力します:

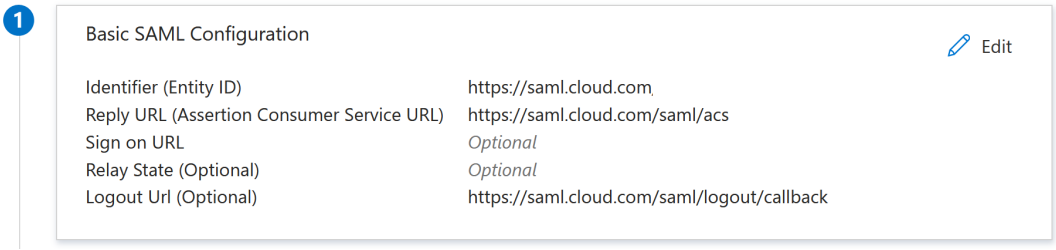
   - 欧州、米国、およびアジア太平洋南部の各リージョンの場合は、「`https://saml.cloud.com/saml/acs`」と入力します。
   - 日本リージョンの場合は「`https://saml.citrixcloud.jp/saml/acs`」と入力します。
   - Citrix Cloud Government リージョンの場合は、「`https://saml.cloud.us/saml/acs`」と入力します。

c) [**Sign on URL**] セクションに、Workspace 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 テナントが存在するリージョンに対応する値を入力します：

- 欧州、米国、およびアジア太平洋南部の各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 リージョンの場合は、「`https://saml.cloud.us/saml/logout/callback`」と入力します。

e) コマンドバーで、[**Save**] をクリックします。[**Basic SAML Configuration**] セクションが以下のように表示されます：



8. [**Attributes & Claims**] セクションで［**Edit**］を選択し、以下の要求を構成します。これらの要求は、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) [**Unique User Identifier (Name ID)**] 要求については、`user.userprincipalname`のデフォルト値のままにします。

b) **cip_upn** 要求では、デフォルト値の`user.userprincipalname`のままにします。

c) **displayName** では、デフォルト値の`user.displayname`のままにします。

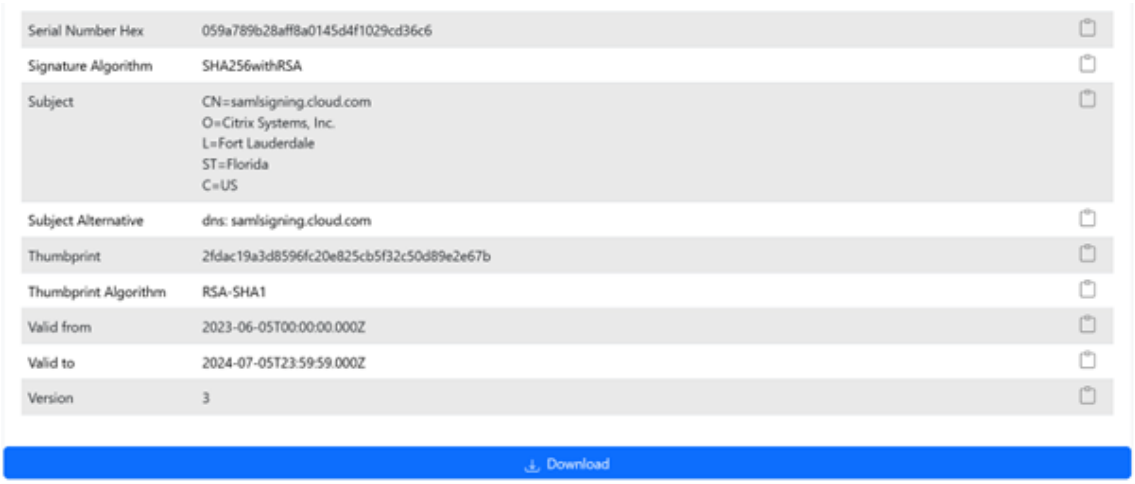
d) [**Additional claims**] セクションで、名前空間`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`を持つ要求が残っていれば、[省略記号 (…)] をクリックし、[削除] をクリックします。これらの要求は上記の user 属性と重複するため、含める必要はありません。

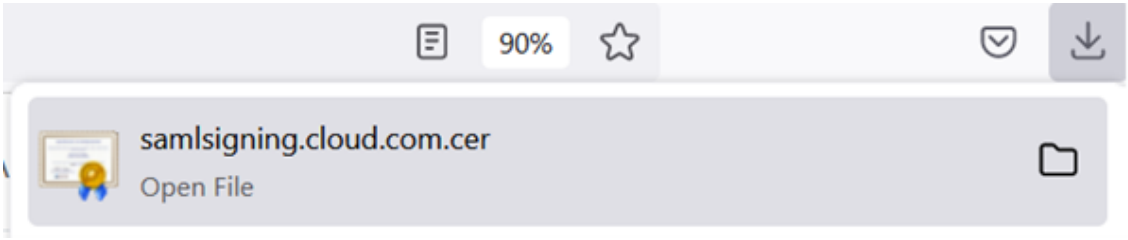
完了すると、下図のような［**Attributes & Claims**］セクションが表示されます：

e) 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。

f) URL フィールドに`https://saml.cloud.com/saml/metadata`を入力し、[**Load**] をクリックします。

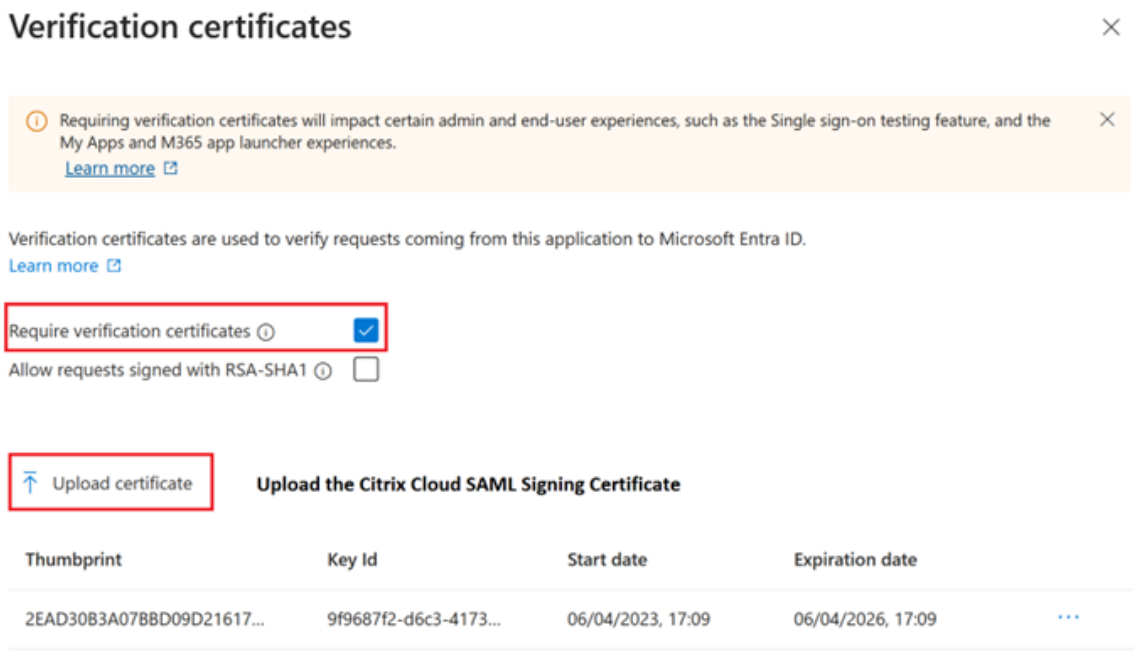
9. ページの下までスクロールして、[ダウンロード] をクリックします。

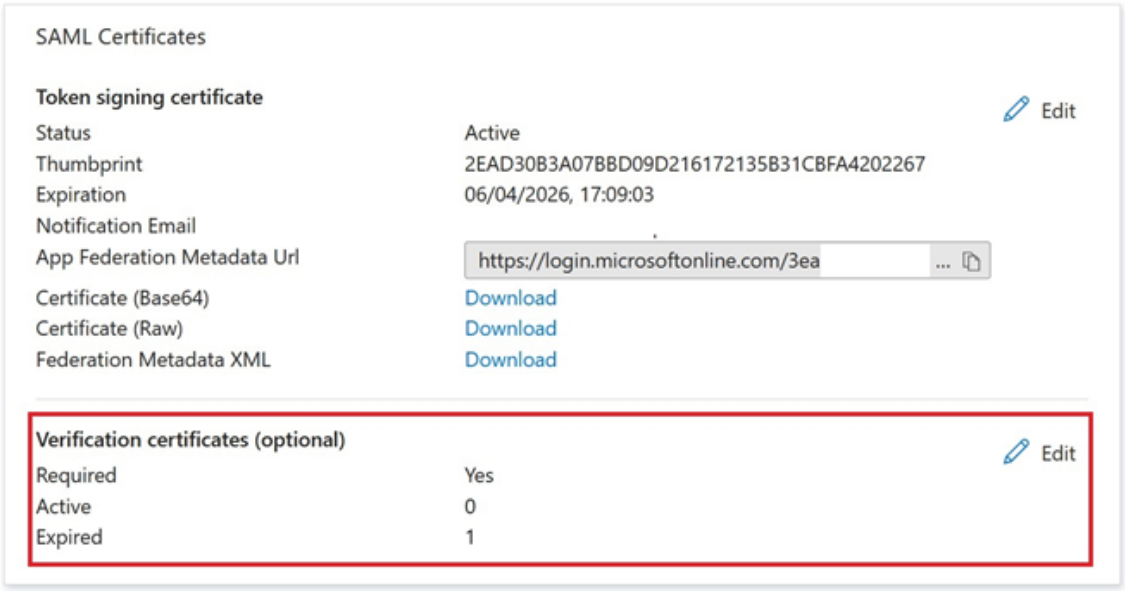




10. Azure Active Directory SAML アプリケーションの署名設定を構成します。
11. 手順 10 で取得した実稼働 SAML 署名証明書を Azure Active Directory SAML アプリケーション内にアップロードします

    a)［検証証明書が必要］を有効にします。

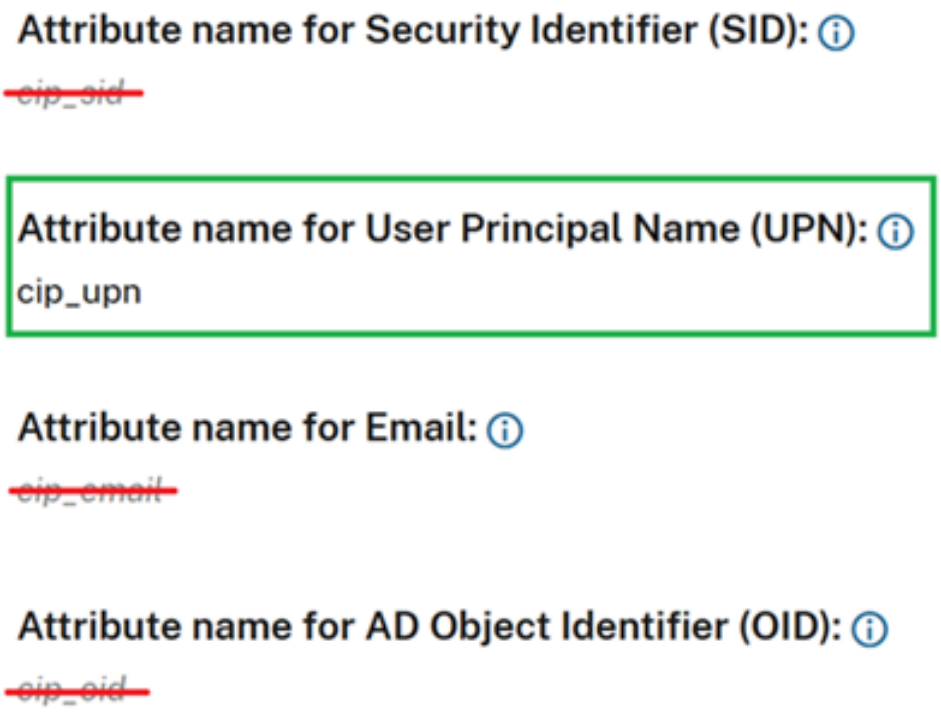




Citrix Cloud の簡易 **SAML** 接続の構成

デフォルトでは、Citrix Cloud では cip_upn、cip_email、cip_sid、cip_oid が SAML アサーションに含まれていることが想定されているため、これらの属性が送信されない場合は SAML サインインに失敗します。これを防ぐには、新しい SAML 接続を作成するときに、これらの属性のチェックを解除してください。

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. 下の ［**SAML Attribute Mappings Configuration**］セクションに移動し、新しい SAML 設定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** はフィールドから削除しないでください。
5. それぞれのフィールドから他の属性を削除しないでください。**displayName** は引き続き Workspace UI に必要であり、変更しないでください。



AD シャドウアカウントのリソースの場所とコネクタの構成

バックエンドシャドウアカウントの AD フォレスト内にリソースの場所とコネクタのペアが必要です。Citrix Cloud で、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 フォレスト内にコネクタが必要です（SAML アサーション内で cip_upn のみが直接指定されている場合）。

1. バックエンドシャドウアカウントの AD フォレストに参加済みの Citrix Cloud Connector を含む、新しいリソースの場所を作成します。

2. 使用するバックエンド AD シャドウアカウントが存在する AD フォレストと一致する、リソースの場所の名前を指定します。
3. 新しく作成したリソースの場所内で Citrix Cloud Connector のペアを構成します。

例

```
ccconnector1.shadowaccountforest.com
ccconnector2.shadowaccountforest.com
```


バックエンド **AD** フォレスト内での **FAS** の構成

契約社員のフロントエンドユーザーには必ず FAS が必要です。DaaS の起動中、契約社員ユーザーは 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、Windows 資格情報を手動で入力して起動を完了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 つまたは複数の 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 フォレストに参加している Citrix Cloud Connector のペアが含まれる同じリソースの場所に、FAS サーバーをリンクします。

AD ドメイン内での代替 **UPN** サフィックスの構成

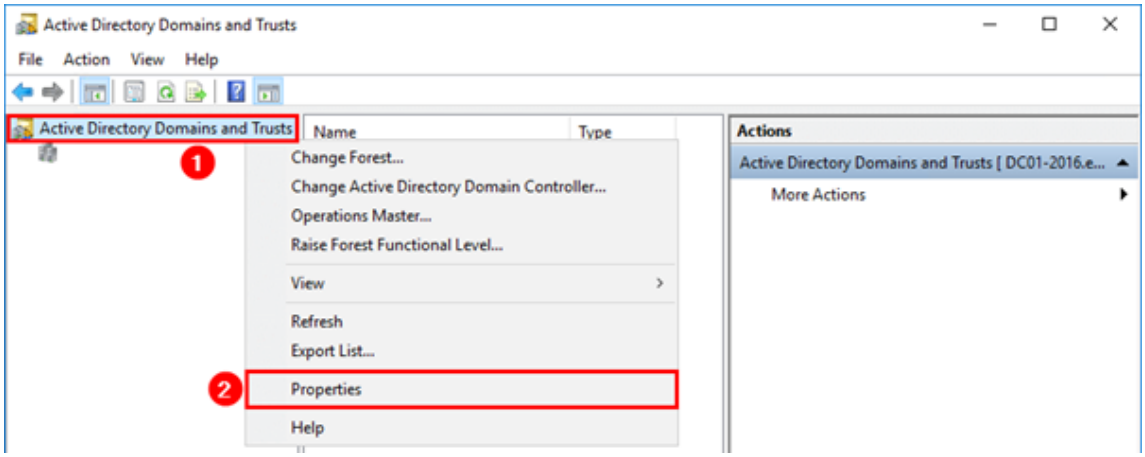
> 重要:
>
> UPN はユーザーのメールアドレスとは異なります。多くの場合、使いやすさの点で同様の価値がありますが、UPN とメールでは内部用途が異なり、異なる Active Directory 属性で定義されています。

ユーザープリンシパル名（UPN）サフィックスは、AD のサインオン名の一部です。新しいアカウントを作成すると、デフォルトで「yourforest.com」などの AD フォレストの暗黙的な UPN サフィックスが使用されます。Okta または Azure AD テナントに招待するすべての外部フロントエンドユーザーに、対応する代替 UPN サフィックスを追加する必要があります。

たとえば、外部ユーザー`contractoruser@hotmail.co.uk`を招待し、これをバックエンド AD シャドウアカウント`contractoruser@yourforest.com`に関連付ける場合は、`yourforest.com`を AD フォレスト内で代替 UPN サフィックスとして追加します。

Active Directory ドメインと信頼関係の **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. ［ファイル名を指して実行］を開いてから`domain.msc`を入力して、［**OK**］をクリックします。
3. ［Active Directory ドメインと信頼関係］ウィンドウで、［**Active Directory** ドメインと信頼関係］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［代わりの 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 を作成するには、バックエンド AD フォレストに多数の新しい UPN サフィックスの追加が必要な場合があります。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。

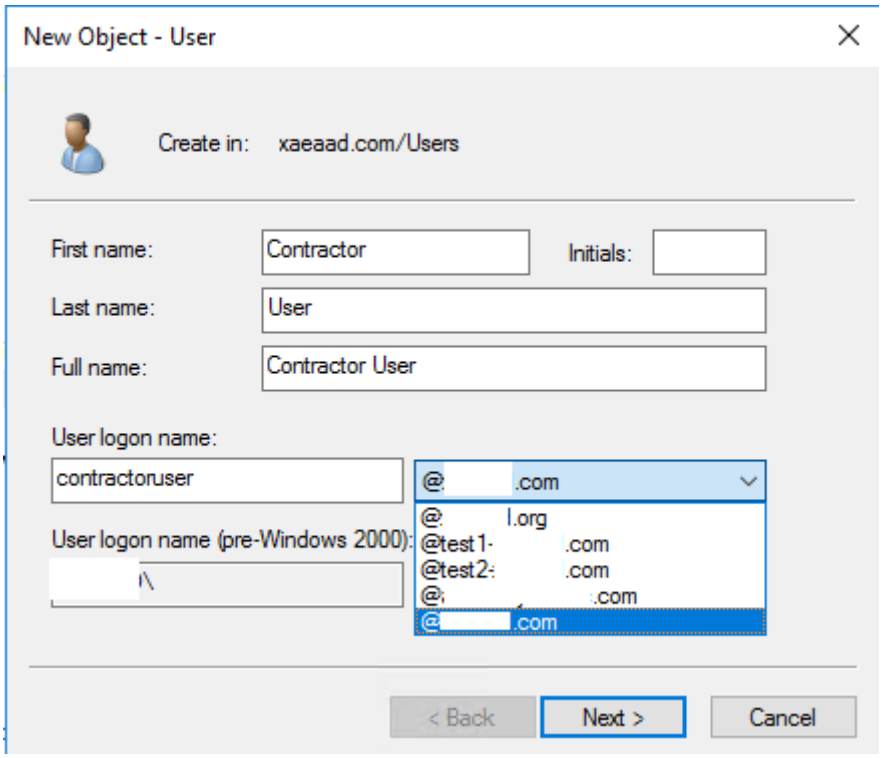
以下は、多数の新しい代替 UPN サフィックスを作成する必要がある場合に、これを実現するための PowerShell の例です。

```
# 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 }

 }

<!--NeedCopy-->
```

バックエンド **AD** フォレスト内の **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、AD フォレストの暗黙的な UPN（yourforest.localなど）がデフォルトで選択されます。上記で作成した適切な代替 UPN サフィックスを選択します。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 を使用して更新することもできます。

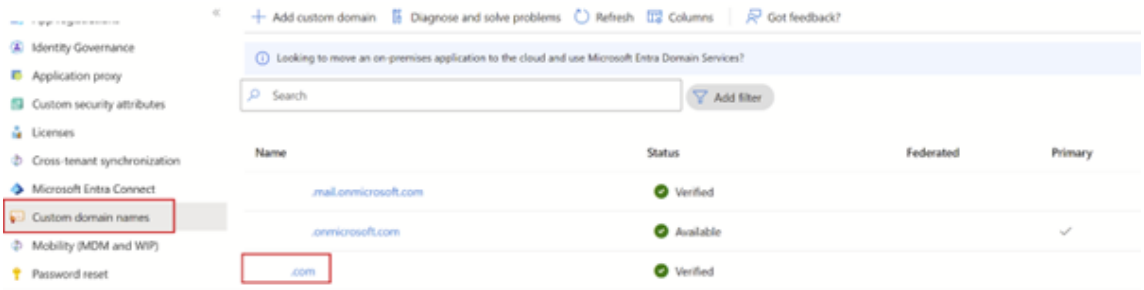
```
Set-ADUser "contractoruser" -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

3. シャドウアカウントユーザーの UPN は、外部フロントエンド 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 Workspace 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ら、必要なすべてのリソースが Workspace に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プされたリソースが表示されます。

ゲスト **Entra ID** ユーザー **UPN** を **AD** シャドウアカウント **UPN** と一致するように構成する

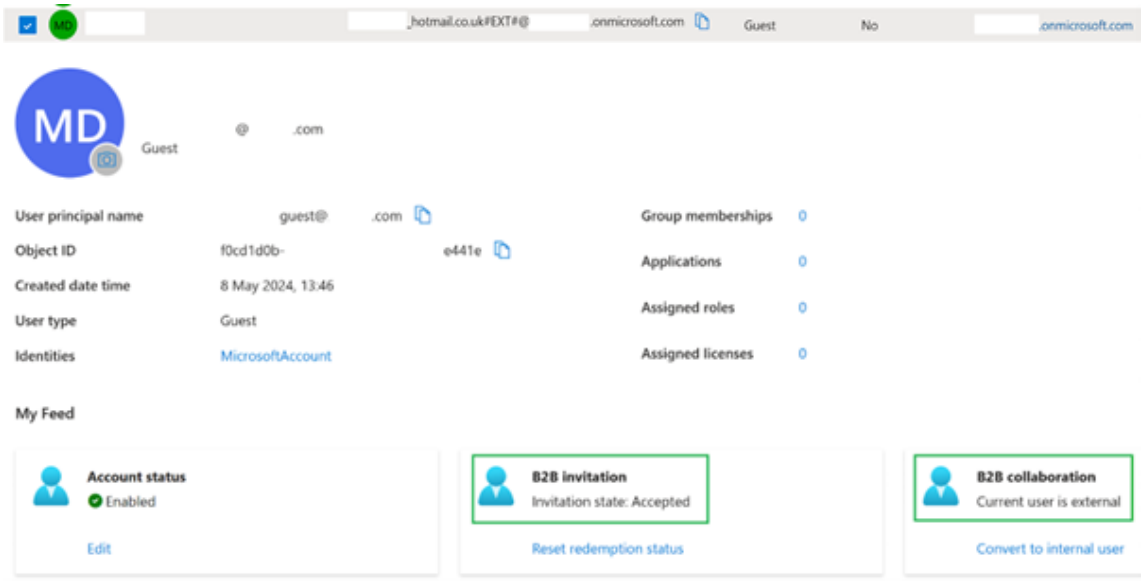
外部ゲストユーザーが Entra ID テナントに招待されると、そのユーザーが外部ユーザーであることを示す自動生成 UPN が作成されます。外部 Entra ID ユーザーには自動的に「@Entra IDtenant.onmicrosoft.com」UPN サフィックスが割り当てられます。これは簡易 SAML での使用には不適切であり、AD シャドウアカウントと一致しません。そのため、Entra ID 内のインポートされた DNS ドメインと、AD フォレスト内で作成した代替 UPN サフィックスとが一致するように更新する必要があります。

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などの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 の招待状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の UPN 形式の例。
   contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com



> 重要:
>
> Citrix Cloud と Workspace 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するには、必要な Azure PowerShell Graph モジュールをインストールしてください。

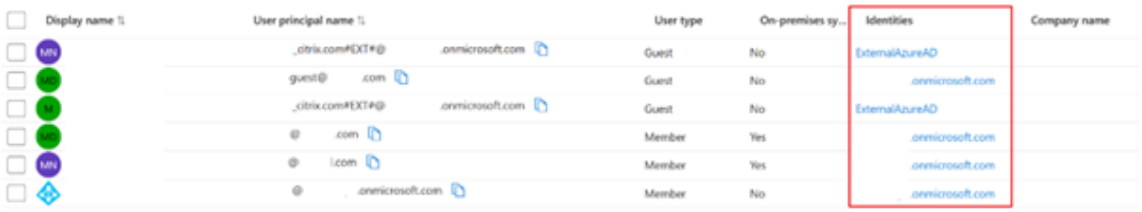
```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
<!--NeedCopy-->
```

4. グローバル管理者アカウントとDirectory.AccessAsUser.Allスコープを使用して 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したり、`Directory.AccessAsUser.All`スコープを指定しなかったりすると、手順 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。

```
$EntraTenantID = "<yourEntraTenantID>"
Connect-MgGraph -Tenant $EntraTenantID -Scopes "Directory.
    AccessAsUser.All"
<!--NeedCopy-->
```

5. Entra ID テナント内の外部ゲストユーザーの一覧をすべて取得できます（オプション）。




```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
<!--NeedCopy-->
```

6. UPN の更新が必要なゲストユーザー ID を取得し、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"
<!--NeedCopy-->
```

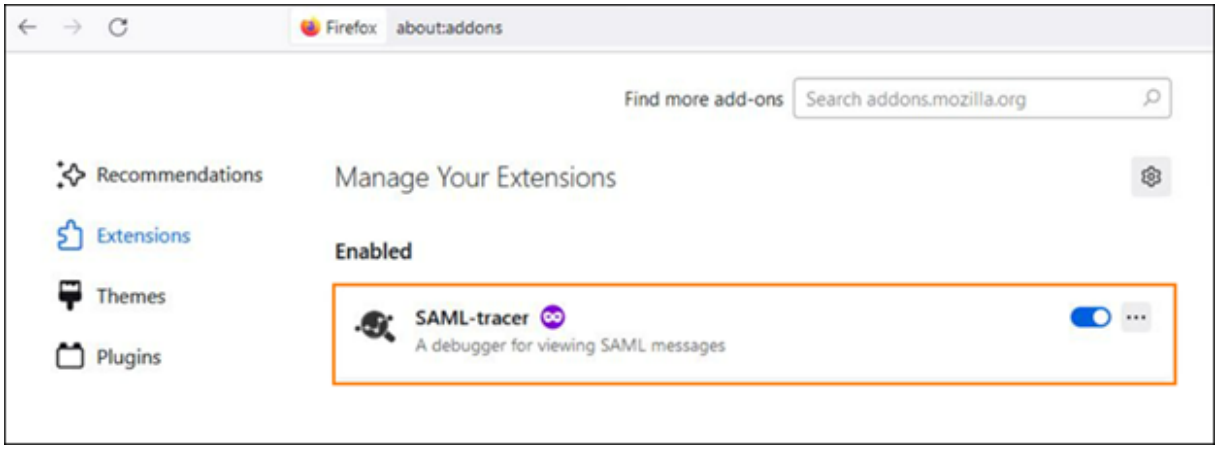
7. 新しく更新された UPN を使用してゲストユーザーの ID が見つかることを確認します。

```
Get-MgUser -UserId "contractoruser@yourforest.com"
<!--NeedCopy-->
```

簡易 **SAML** ソリューションのテスト

文書化されたすべての手順を AD、Citrix Cloud、および SAML プロバイダーで完了したら、サインインのテストをして、Workspace 内のゲストユーザーに正しいリソース一覧が表示されることを確認する必要があります。

あらゆる SAML デバッグ作業には、ブラウザー拡張機能 SAML-tracer を使用することをお勧めします。この拡張機能は、よく知られている Web ブラウザーのほとんどで利用できます。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 にデコードすることで、人間が判読できるようにします。



SAML-tracer を使用してキャプチャされた認証に cip_upn だけを使用する簡易 SAML アサーションの例。

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>        </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. 正しい DaaS リソースを、AD ベースの、およびシャドウアカウントのユーザー、またはそれらを含むグループにマッピングします。
2. SAML-tracer ブラウザー拡張機能を起動し、ログオンとログオフのフロー全体をキャプチャします。
3. テストするフロントエンドユーザータイプの表で指定されている属性を使用して、Workspace 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契約社員ユーザ

ーの場合は、メールアドレスcontractoruser@hotmail.co.ukを使用します。

Entra ID の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

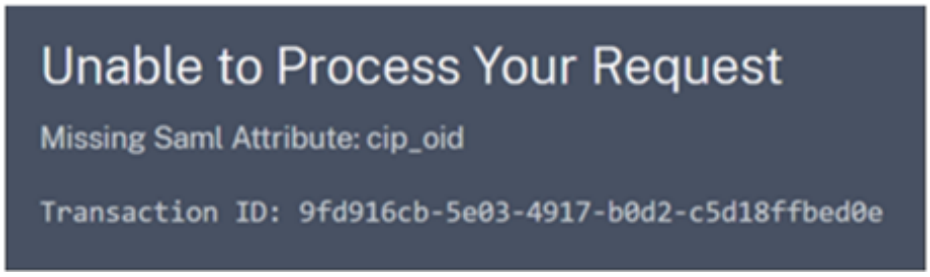
AD ベースの **Entra ID** ユーザー/ネイティブ **Entra ID** ユーザーのログオン：これらの Entra ID ユーザーには、adbackeduser@yourforest.comまたはnativeuser@yourforest.comの形式の UPN が割り当てられます。

Entra ID の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 Workspace UI で必要な **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 に表示できることを確認します。

簡易 **SAML** ソリューションのトラブルシューティング

cip_* 属性が見つからないというエラー



原因 1：SAML 属性が SAML アサーションに存在しないのに、Citrix Cloud がそれを受け取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_* 属性を削除できていません。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 Connector がバックエンド AD フォレストで検索できる、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 は正しく設定されているかもしれませんが、一致する UPN を使用したバックエンド 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 **Workspace** にログインした後に **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 の UPN マッピングが正しくないことが原因と考えられます。

フロントエンド ID とバックエンド ID の 2 つの UPN が完全に一致し、Workspace にログイ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ます。

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、Workspace エンドユーザーは GINA 内に Windows 資格情報を入力するように求められます。また、イベント ID 103 は、FAS サーバーの Windows イベントログに表示されます。

[S103] サーバー [CC: FASserver] は UPN [frontenduser@yourforest.com] `SID S-1-5-21-000000000-0000000` を要求しましたが、検索で`SID S-1-5-21-000000000-0000000000-0000000001-0002`が返されました。[correlation: cc#967472c8-4342-489b-9589-044a24ca57d1]

原因：簡易 SAML 展開が「SID の不一致問題」の影響を受けています。バックエンドシャドウアカウントの AD フォレストとは異なる AD フォレストの SID を含むフロントエンド ID があります。
SAML アサーションで **cip_sid** を送信しないでください。

接続された複数の **AD** フォレストに同じ **UPN** サフィックスが存在する場合、**AD** ベースのユーザーのログオンに失敗する

Citrix Cloud には、異なる AD フォレストに参加している複数のリソースの場所とコネクタがあります。シャドウアカウントの AD フォレストとは別の AD フォレストから Entra ID にインポートされた AD ベースのユーザーを使用すると、ログオンが失敗します。

AD フォレスト 1 は Entra ID と同期され、`frontenduser@yourforest.com`などの UPN を持つフロントエンドユーザーを作成します。

AD Forest 2 には、`frontenduser@yourforest.com`などの UPN を持つバックエンドシャドウアカウント が含まれています。

原因：簡易 SAML 展開が「UPN があいまいな問題」の影響を受けています。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る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 に接続された複数の AD フォレストに存在します。

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

April 26, 2024

Author:
Mark Dear

この記事は、Citrix と Ping の両方のエンジニアが共同で執筆したものであり、執筆時点での技術的な正確性を確認するために両社によってレビューされています。オンプレミスの PingFederate サーバーを SAML プロバイダーと

して使用するためのプロビジョニング、構成、ライセンス取得の方法については、この記事では扱わないため、Ping のドキュメントを参照してください。

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

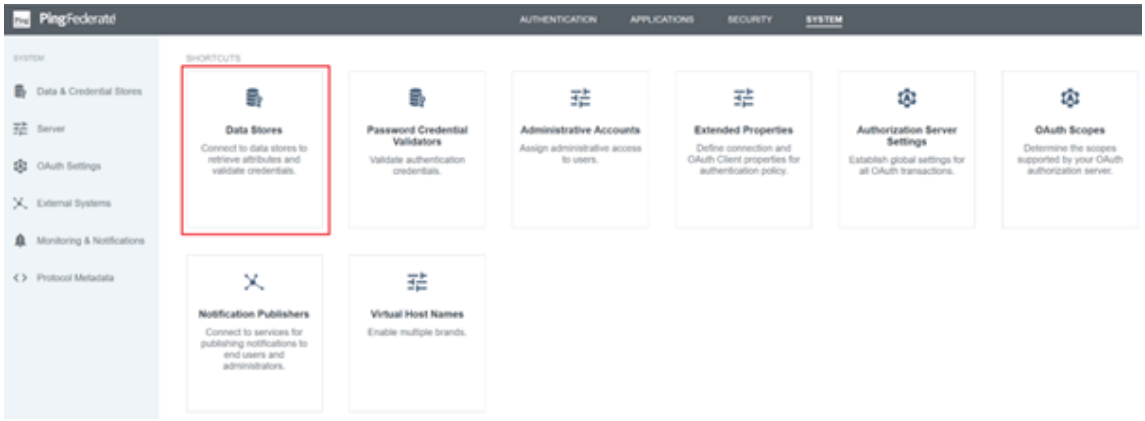
この記事では特に SAML 設定について説明し、以下の条件が満たされていることを確認します。

- 既に組織内でオンプレミスの PingFederate サーバーをプロビジョニングし、必要なライセンスを取得しています。詳しくは、「PingFederate Installation」を参照してください。
- サポートされているバージョンの Java が PingFederate サーバーにインストールされている必要があります。サポートされている Java のバージョンについては、Ping ID のドキュメントを参照してください。詳しくは、「Java PingFederate Requirement」を参照してください。
- Workspace/Citrix Cloud 管理者コンソールの SAML ログオンプロセス中に、Citrix Cloud と Workspace がオンプレミスの 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規則とファイアウォール規則を構成しています。詳しくは、「PingFederate Network Requirements」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する、パブリック署名済みの x509 証明書を PingFederate サーバーにインポートしています。
- ID プロバイダーの SAML 署名証明書として機能する、パブリック署名済みの x509 証明書を PingFederate サーバーにインポートしています。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。
- オンプレミスの Active Directory を PingFederate に接続しています。詳しくは、「PingFederate LDAP Datastore」を参照してください

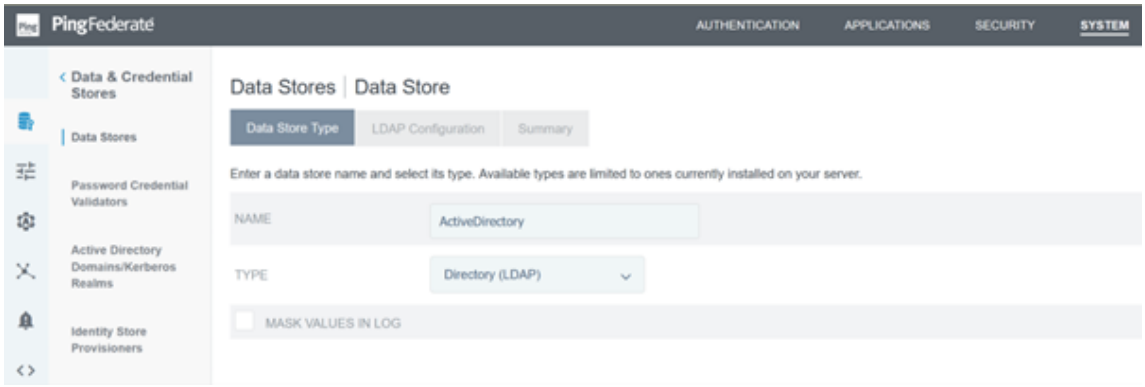
> 注:
>
> Citrix Cloud および Workspace で使用するように PingFederate を構成する場合は、PingFederate のドキュメントを参照して、個々の SAML 設定の機能を理解することで、ここに記載されている手順を補足してください。

PingFederate 内のデータストアを使用して **Active Directory** ドメインへの **AD** 接続を構成

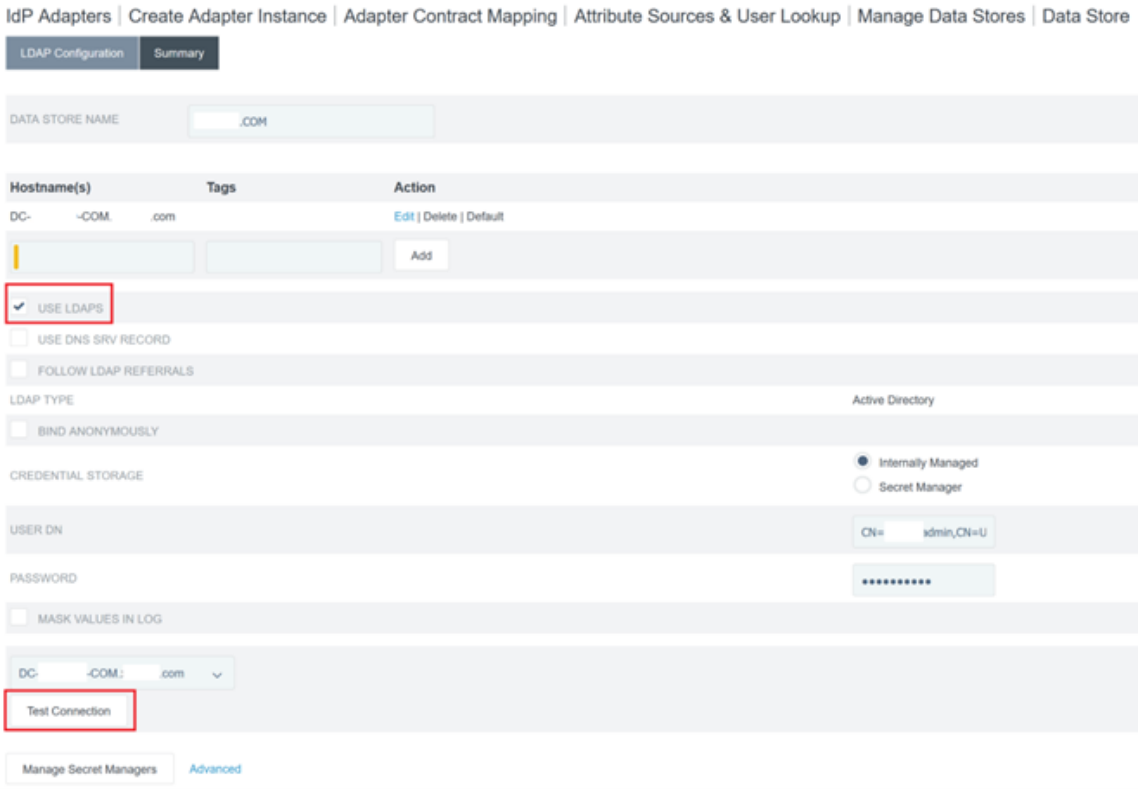
1. データストア内で Active Directory 接続を構成します。



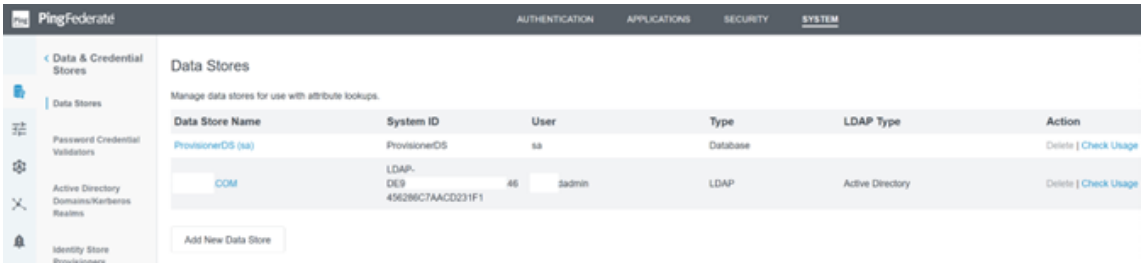
2. [TYPE] で [**Directory**（**LDAP**）] を選択します。



3. LDAPS 接続用にドメインコントローラーを設定し、ホスト名フィールドにドメインコントローラーの FQDN 一覧を追加します。次に、[**Test Connection**] をクリックします。

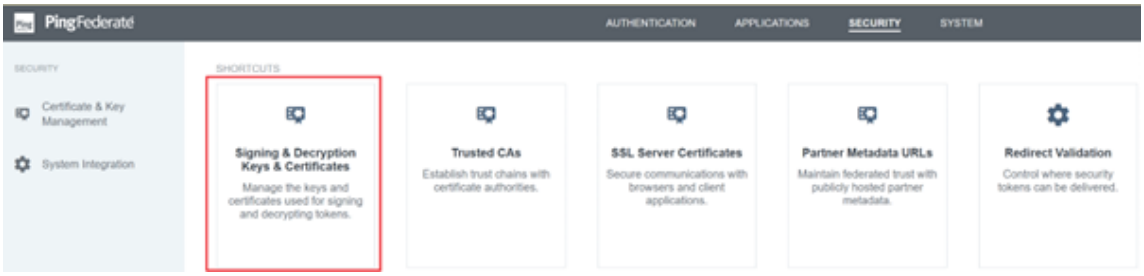


4. 構成後、Active Directory 接続は次の例のようになります:



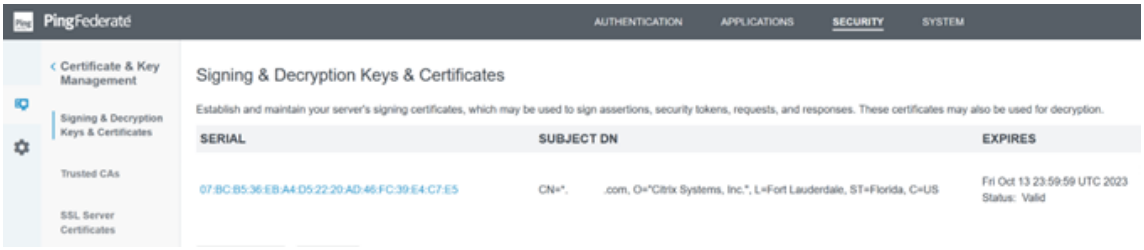
Citrix Cloud SAML 署名証明書のアップロード

1. [**Security**] タブをクリックします
2. [**Signing & Decryption Keys and Certificates**] で PingFederate に使用させる SAML 署名証明書をアップロードします。

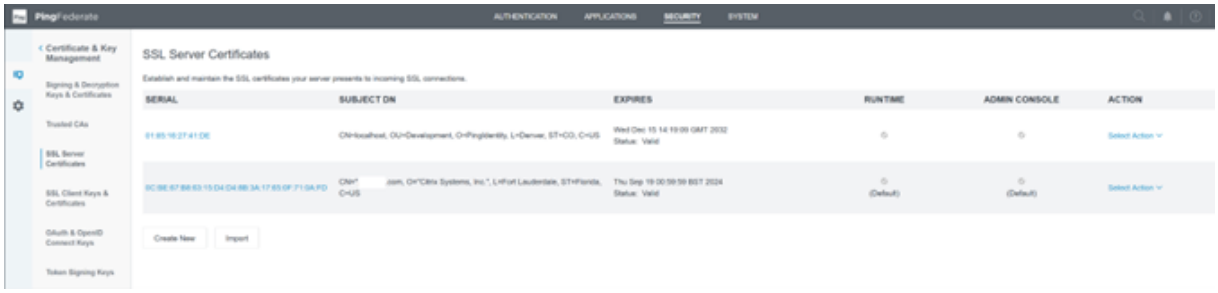


> 注:
>
> この例では、使用されている証明書はパブリック署名済みの Digicert `pingfederateserver.domain.com`証明書です。

3. PingFederate サーバーの SAML 署名証明書に署名するために使用するすべての CA 証明書をアップロードします。



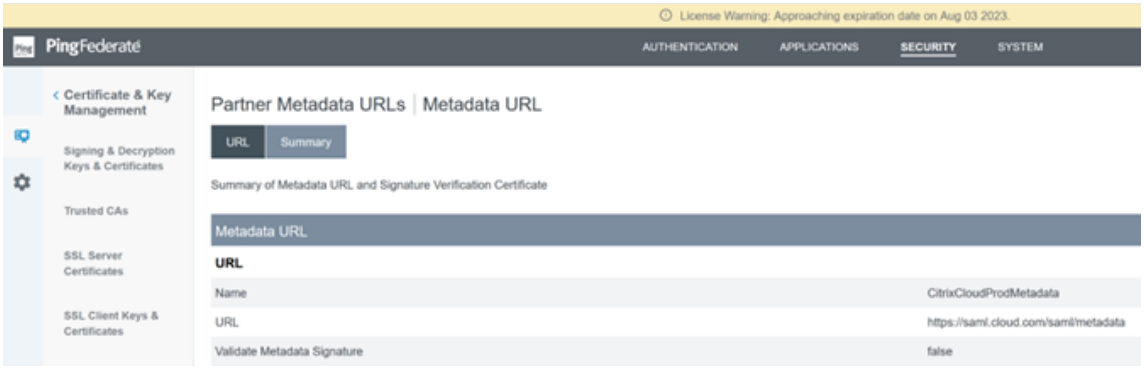
> 注:
>
> PingFederate サーバー証明書と SAML 署名証明書は、同じ SSL 証明書にすることも、異なる SSL 証明書を使用することもできます。SAML 接続を構成するときは、SAML 署名証明書のコピーを Citrix Cloud に提供する必要があります。



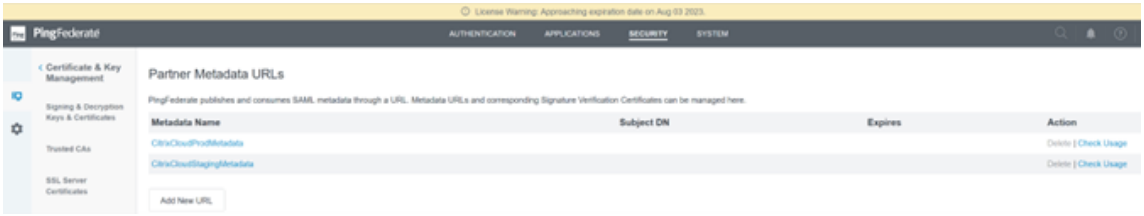
Citrix Cloud メタデータのアップロード

1. Citrix Cloud メタデータの名前を指定し、Citrix Cloud テナントがある 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 向け
   - https://saml.citrixcloud.jp/saml/metadata - 日本向け
   - https://saml.cloud.us/saml/metadata - 米国政府機関向け



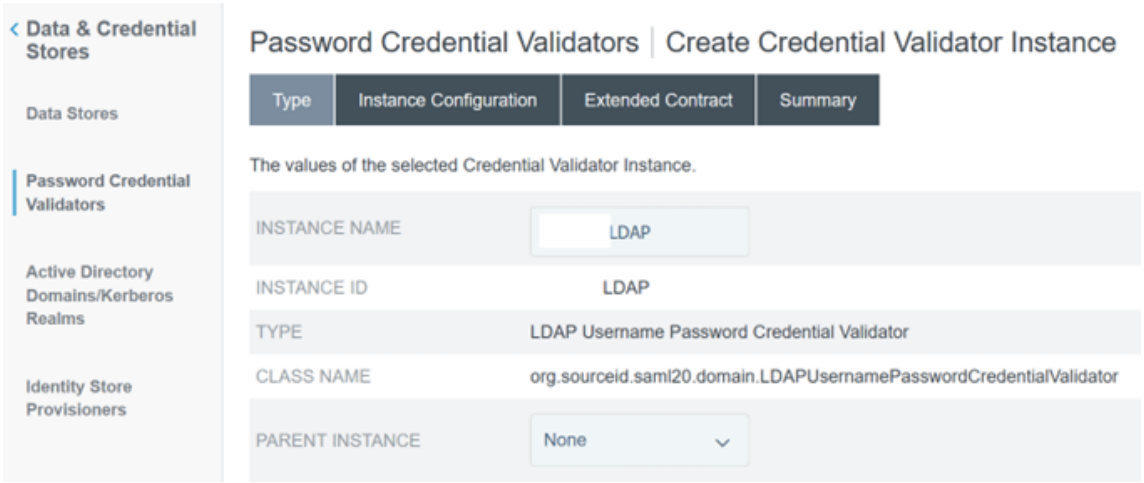
2. 構成が完了すると、Citrix Cloud メタデータ構成は次の例のようになるはずです。



PingFederate で Password Credential Validator を構成

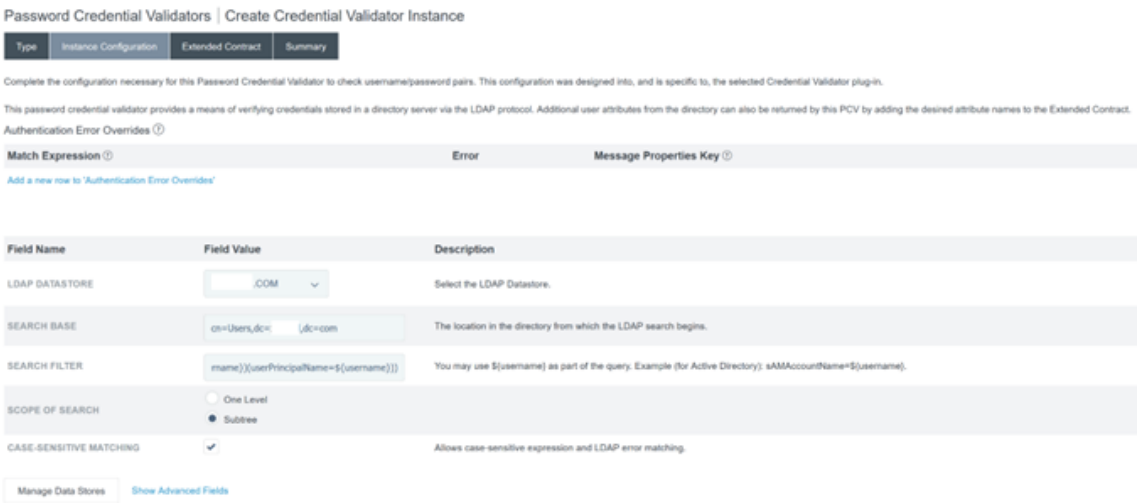
詳しくは、「PingFederate Password Credential Validator」を参照してください

1. [Password Credential Validator]（パスワードの資格情報の検証）の［TYPE］を、LDAP ユーザー名とパスワードとして設定します。



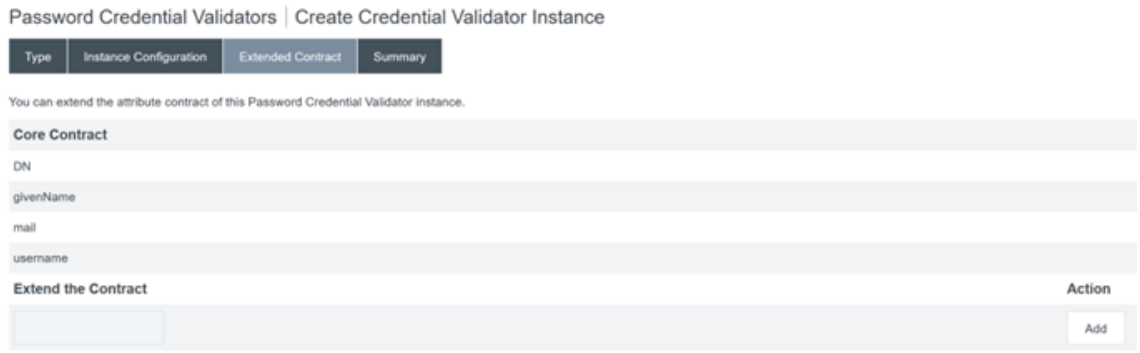
2. ［**Instance Configuration**］を構成します。「PingFederate 内のデータストアを使用して Active Directory ドメインへの AD 接続を構成」で既に構成した AD ドメイン接続とデータストアを選択します。例のように、適切な LDAP フィルターを入力します。

```
(((sAMAccountName=${ username } )(userPrincipalName=${ username } ))
```

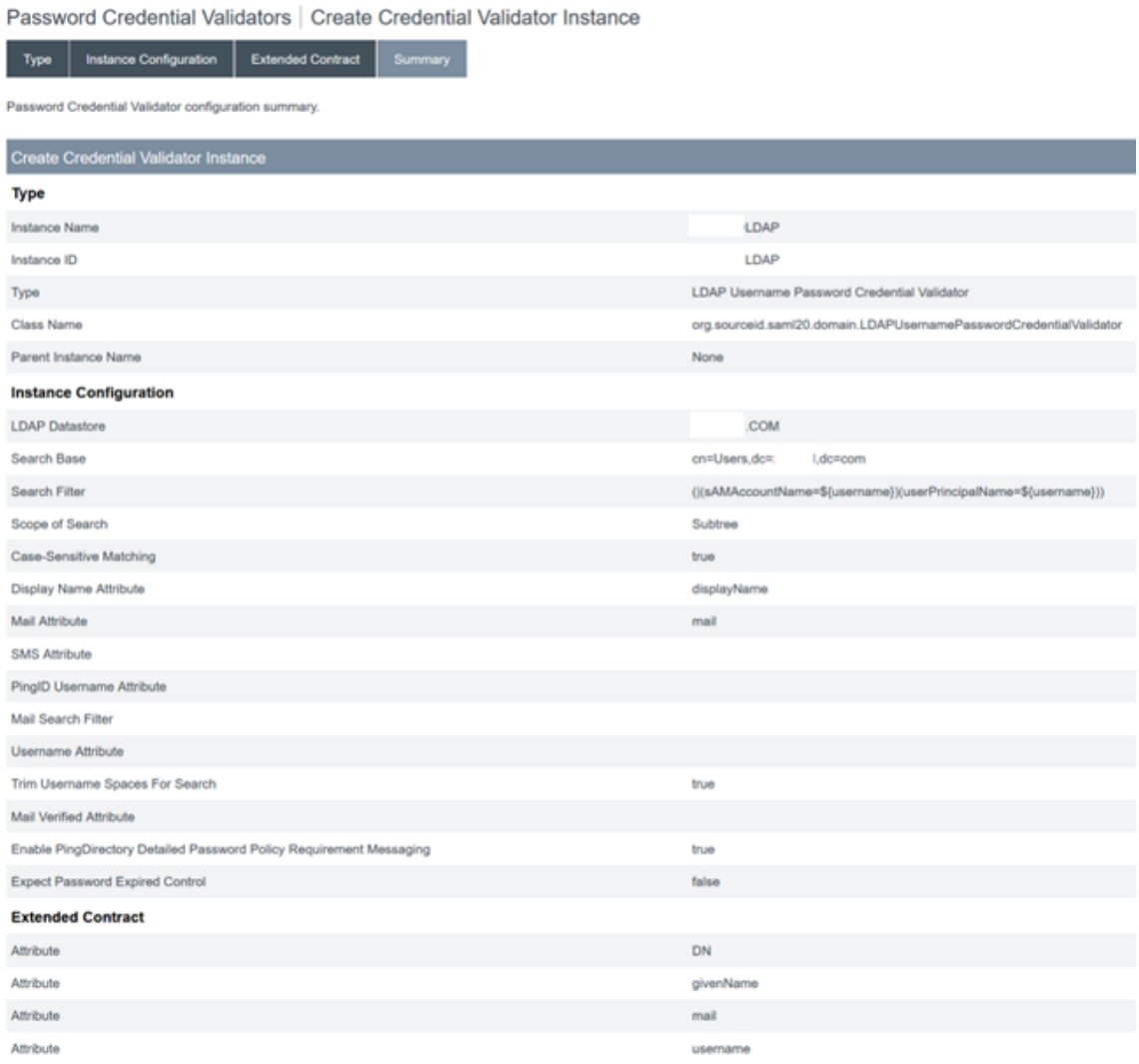



> 注：フィルター例は、sAMAccountName と userPrincipalName の両方の AD ユーザー名形式と一致しているため、エンドユーザーはこれらのいずれかを使用して Workspace または Citrix Cloud にサインインできます。フィルター例は、sAMAccountName と userPrincipalName の両方の AD ユーザー名形式に対応しているため、エンドユーザーはこれらの形式のいずれかを使用して Workspace または Citrix Cloud にサインインできます。

3. [**Extended Contract**] を構成します。



4. **Password Credential Validator** の概要は、この例のようになります。



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

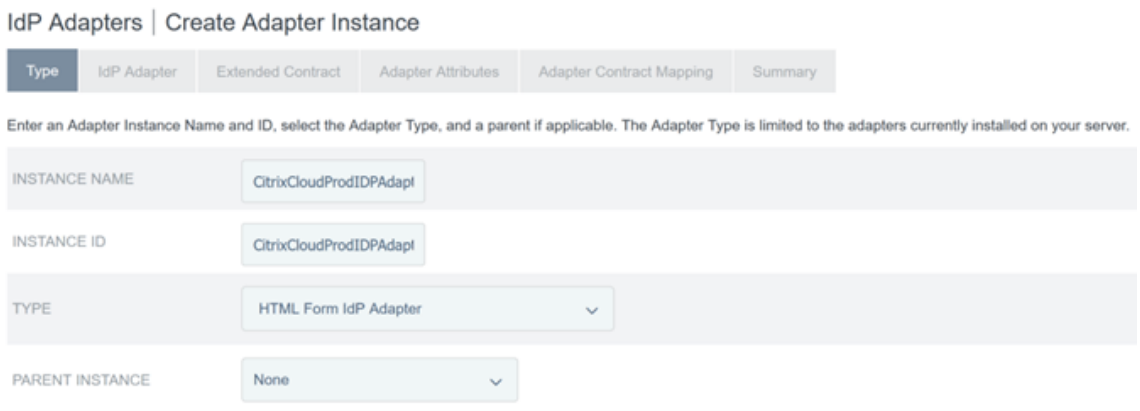
Password Credential Validator configuration summary.

Create Credential Validator Instance	
Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

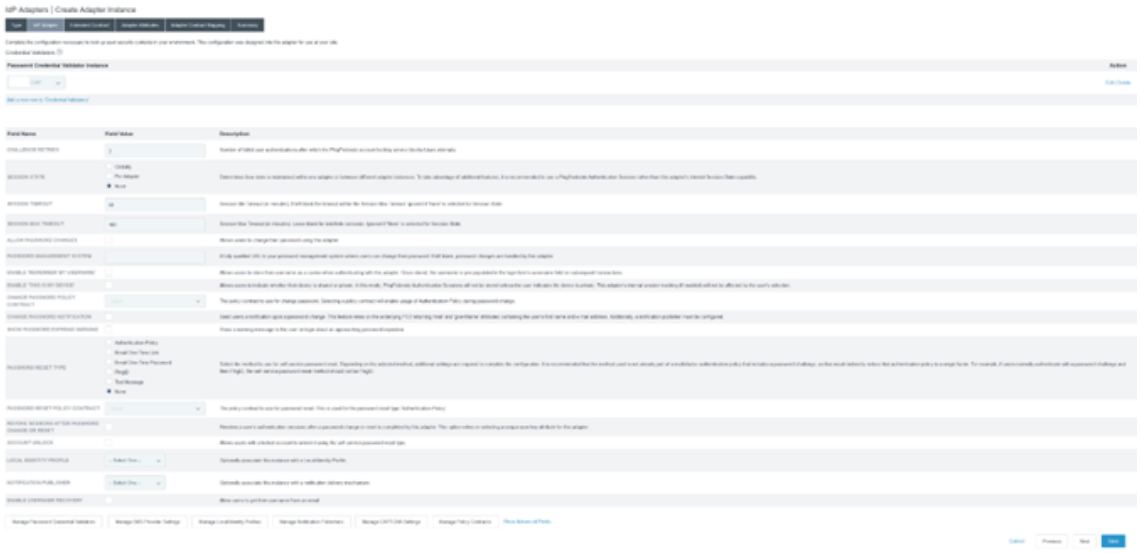
PingFederate 内の **IDP Adapter**（**ID** プロバイダーアダプター）の構成

詳しくは、「PingFederate HTML form adapter」を参照してください

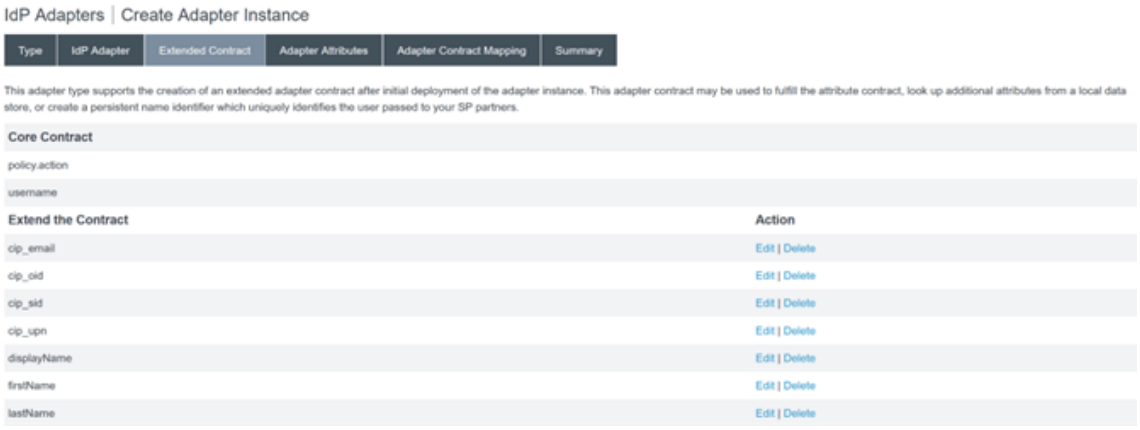
1. ［TYPE］が［HTMLForm IdP Adapter］の新しい ID プロバイダーアダプターを作成します。



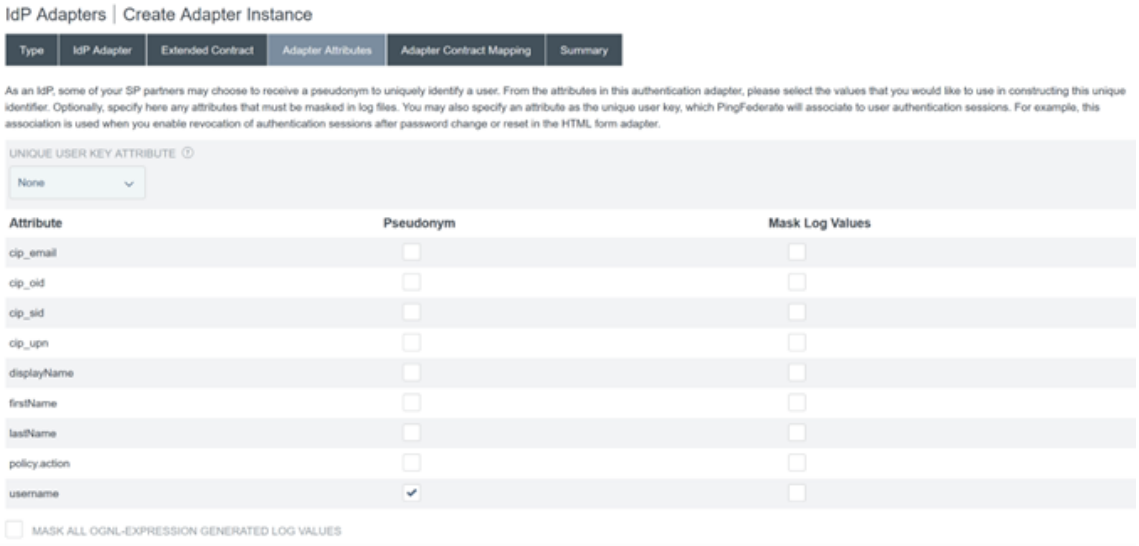
2. 前に構成した既存の **Password Credential Validator** を選択し、ID プロバイダーアダプターを構成します。詳しくは、「Configure a password credential validator within PingFederate」を参照してください。



3. SAML ログオン時に Citrix Cloud または Workspace に渡される SAML 属性を使用して、［**Extended Contract**］を構成します。



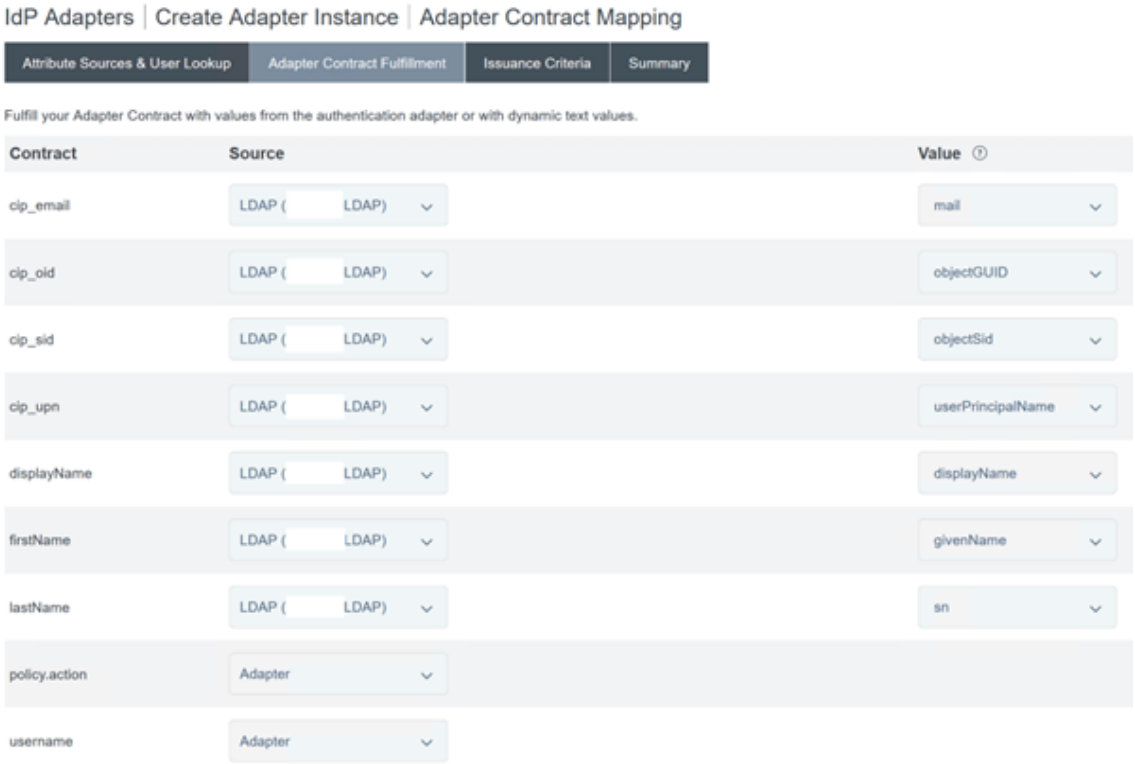
4. [**Adapter Attributes**] を構成します。



5. SAML 属性が AD ID の LDAP ユーザー属性にマッピングされる [**Adapter Contract Mapping**] を構成します。[**Configure the adapter contract**] をクリックします。

6. [**Attribute Sources & User Lookup**] を構成します。

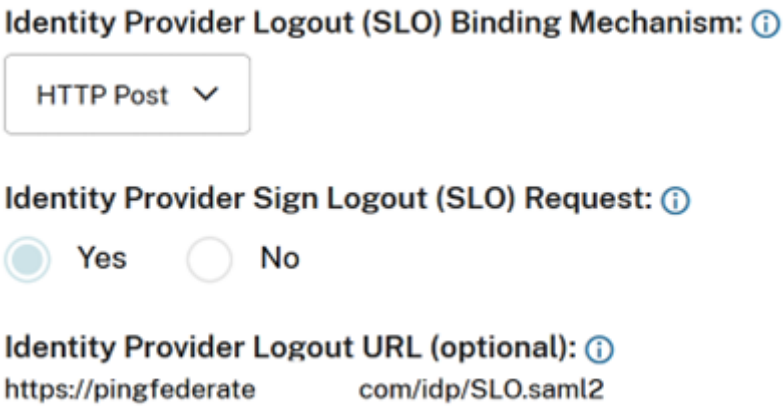
7. [**Adapter Contract Fulfilment**] を構成します。ユーザー属性データの [Source] として **LDAP** と Active Directory データストアの名前を選択します。[Value] は、`objectGUID`または`objectSid`などのユーザーの Active Directory 属性です。



Citrix Cloud または **Workspace** 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 構成の例は、組織内の次の SAML 認証要件を前提としています。

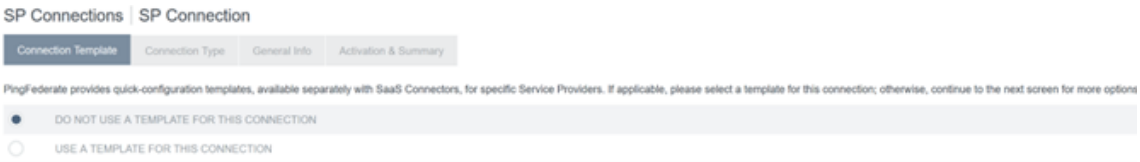
- Workspace/Citrix Cloud 管理者コンソールから送信される SAML 認証リクエストには署名が必要です。
- SAML HTTP POST バインドは、SSO リクエストと SLO リクエストの両方に使用されます。
- シングルログアウト（SLO）は組織内の要件です。エンドユーザーが Workspace または Citrix Cloud 管理者コンソールからサインアウトすると、ユーザーをサインアウトさせるための SAML SLO リクエストが Citrix Cloud から SAML プロバイダー（ID プロバイダー）に送信されます。
- PingFederate でサインアウトを開始するには、署名付きの HTTP POST リクエストが必要です。SAML プロバイダーには署名付きの SLO リクエストが必要です。



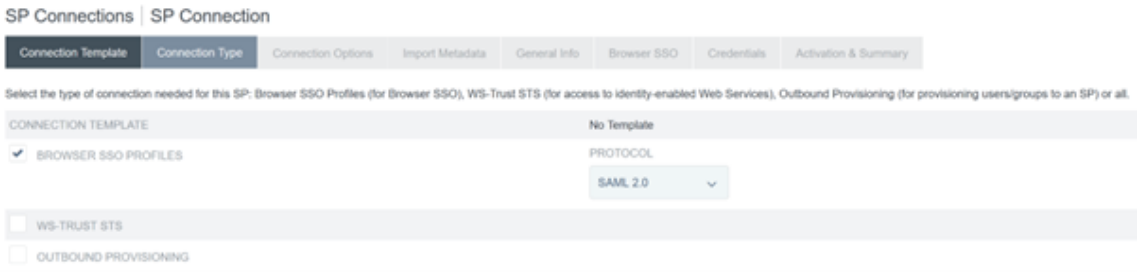
詳しくは、「PingFederate SP Management」を参照してください

手順

1. [**Connection Template**]（接続テンプレート）を構成します。

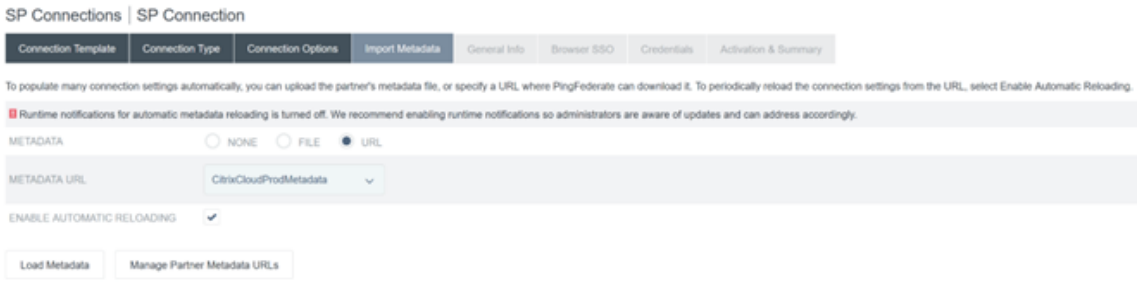


2. [**Connection Type**] を構成し、[**Browser SSO profiles and SAML 2.0**] を選択します。



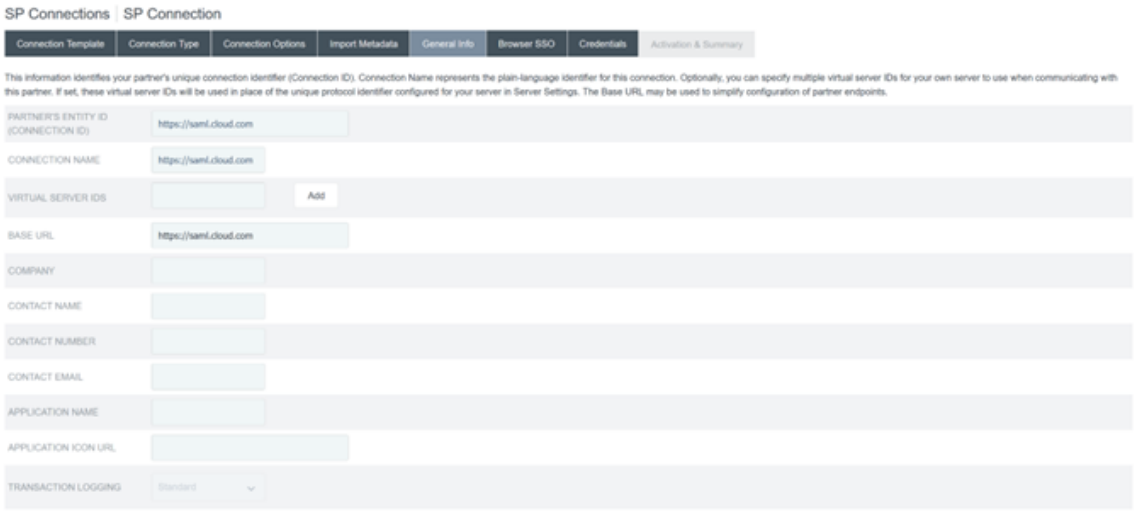
3. [**Connection Options**] を構成します。

4. Citrix Cloud メタデータをインポートします。先ほど作成した URL と `CitrixCloudProdMetadata` URL を選択し、[**Load Metadata**] をクリックします

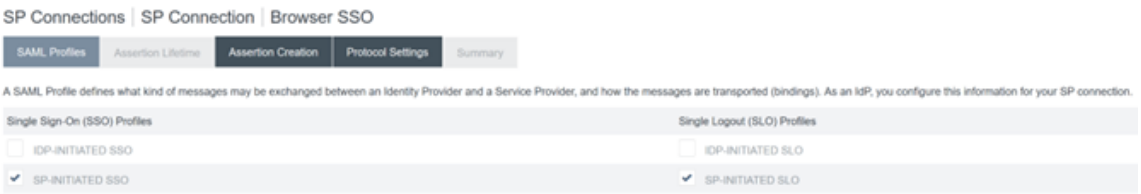


5. [**General Info**] を構成します。サービスプロバイダー接続エンティティ ID、ベース URL、および接続名を、Citrix Cloud の顧客リージョンの Citrix Cloud SAML エンドポイントに設定します。

   - https://saml.cloud.com - 商用 EU、米国および APS 向け
   - https://saml.citrixcloud.jp - 日本向け
   - https://saml.cloud.us - 米国政府機関向け



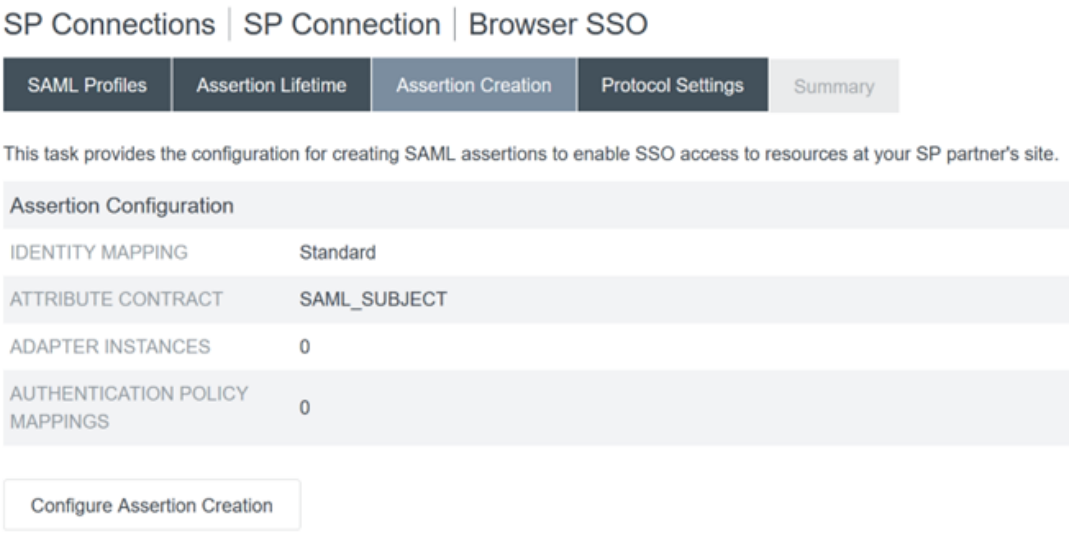
6. [**Protocol Settings**] を構成します。



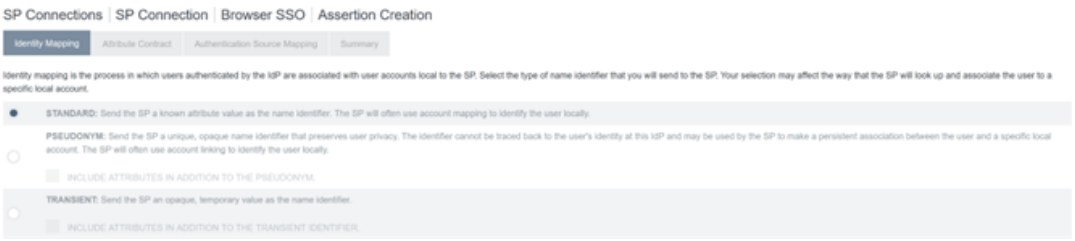
7. デフォルトの [**Assertion Lifetime**] 設定を使用します。

8. SAML アサーションの作成を構成します。

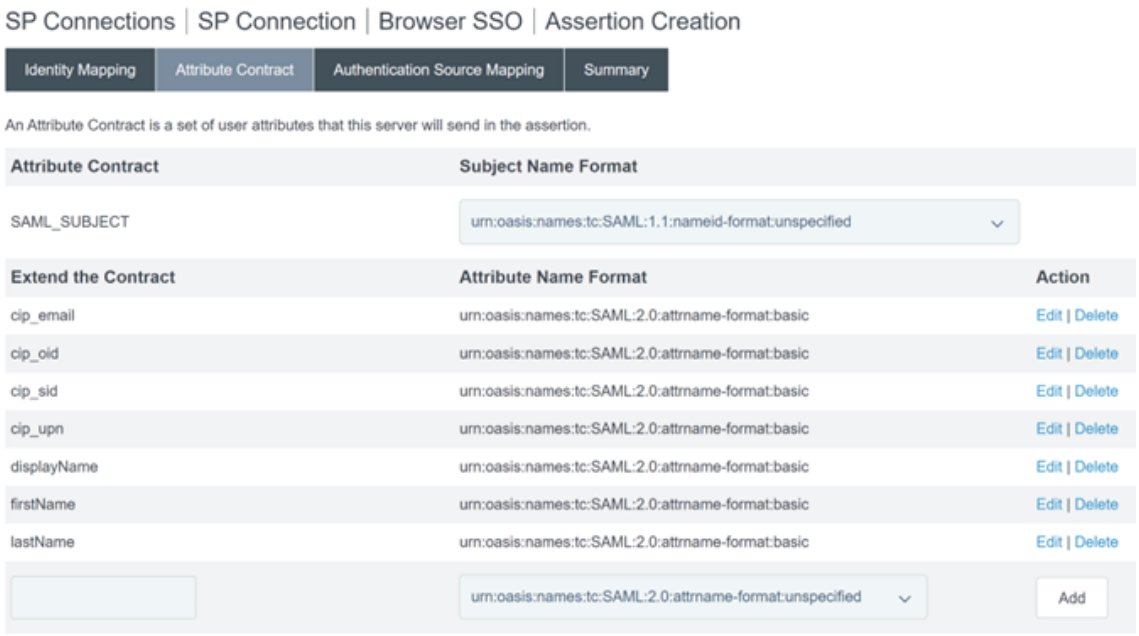
   a)［**Configure Assertion Creation**］をクリックします



   b)［**Standard**］を選択します。

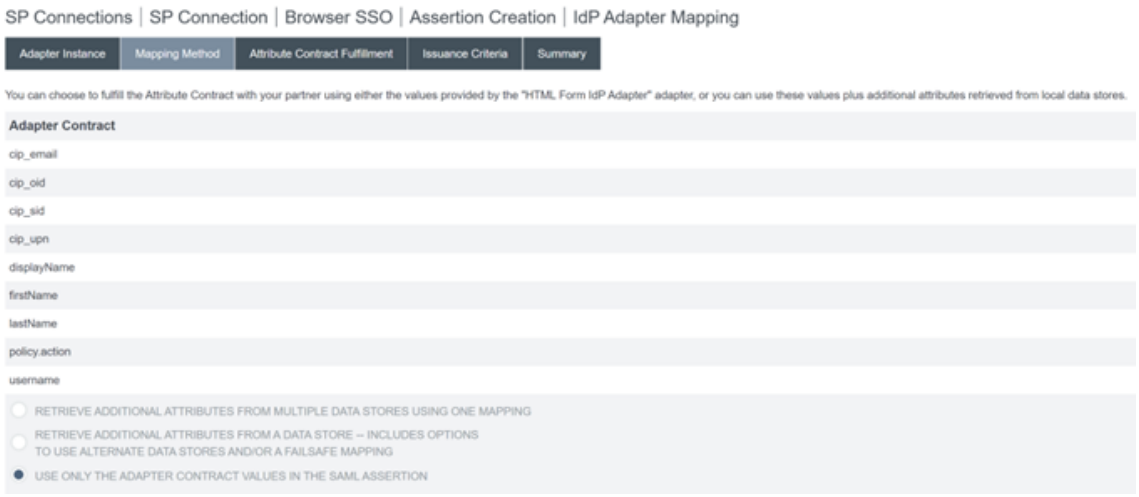


9. ［**Attribute Contract**］を構成します。

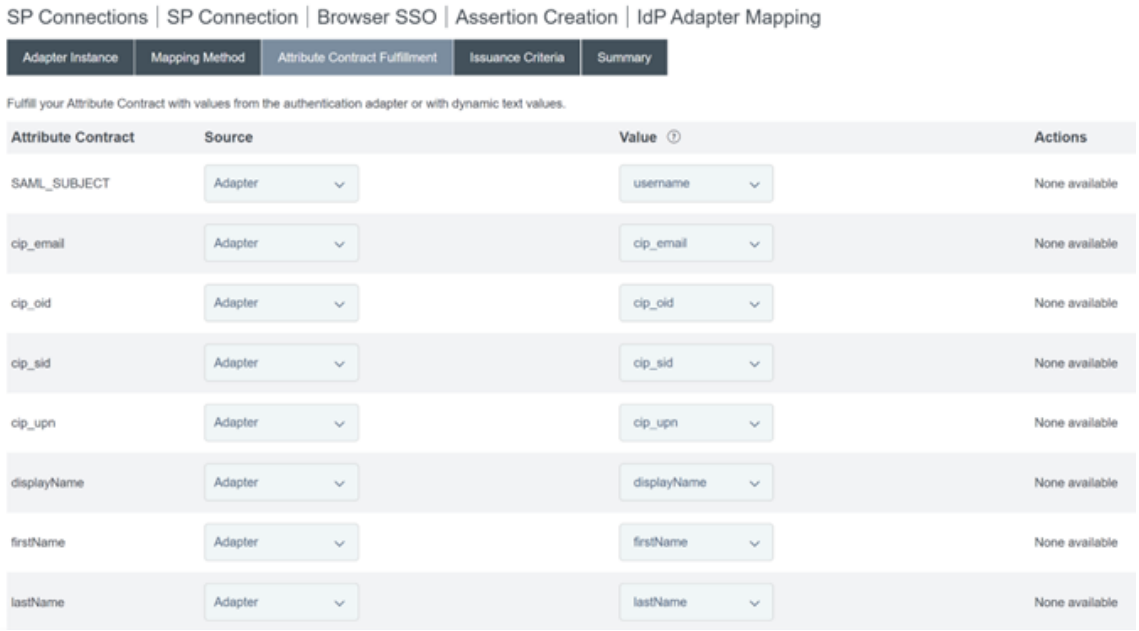


10. [**Adapter Instance**] を構成します。

11. [**Mapping Method**] を構成します。



12. [**Attribute Contract Fulfilment**] を構成します。



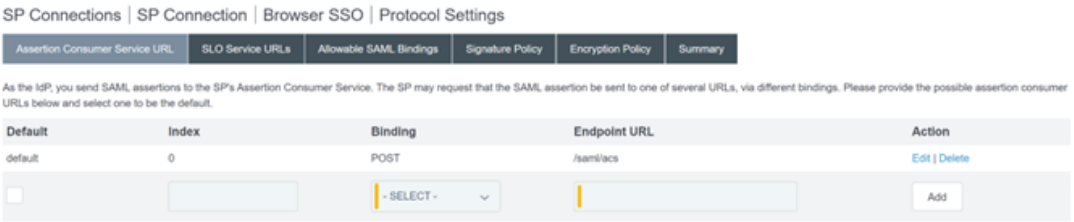
13. [**Issuance Criteria**] をデフォルトのまま、条件（Condition）なしで構成します。

14. 完了した [**IDP Adapter Mapping**]（ID プロバイダーアダプターマッピング）は、以下のように表示されます:

15. [**Protocol Settings**] を構成します。Citrix Cloud で必要な SAML パスが 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

きすることもできますが、これは通常は不要であり望ましくありません。
ベース URL - https://youpingfederateserver.domain.com

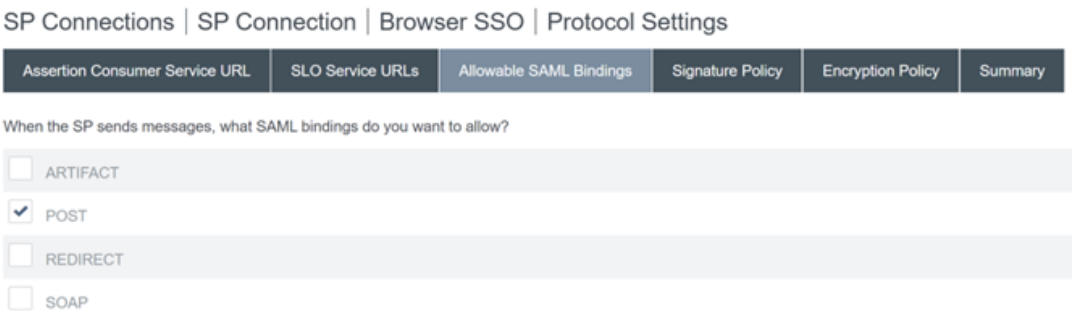
a) PingFederate サーバーのベース URL に SAML パスを追加する［Assertion Consumer Service URL］（アサーションコンシューマーサービス URL）を構成します。エンドポイント URL - /saml/acs



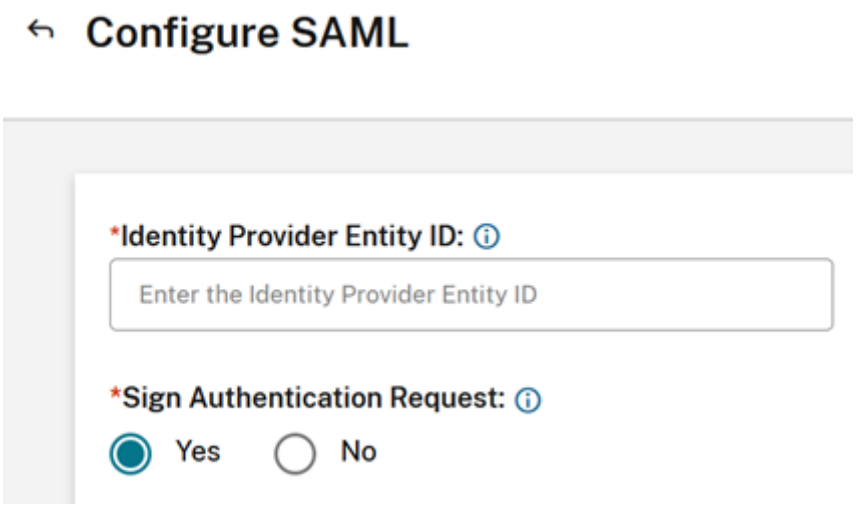
b) ［**SLO Service URL**］を構成します。エンドポイント URL - /saml/logout/callback

> 重要：
>
> Workspace または Citrix Cloud からサインアウトするときに SLO を実行する場合は、Citrix Cloud SAML 接続でこれと一致するように 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 Workspace からサインアウトされるだけで PingFederate からはサインアウトされなくなります。

a) ［**Allowable SAML Bindings**］（許容された SAML バインド）を構成します。

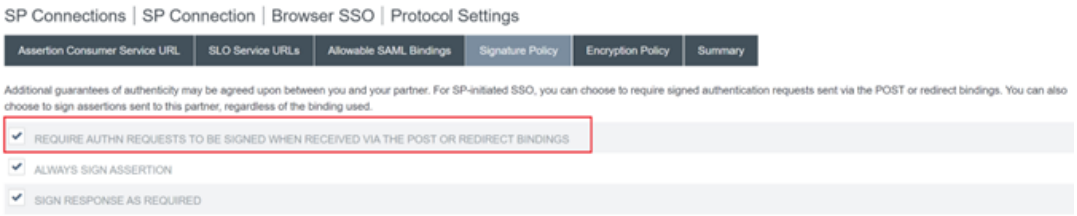


b) **Signature Policy**（署名ポリシー）を構成します。

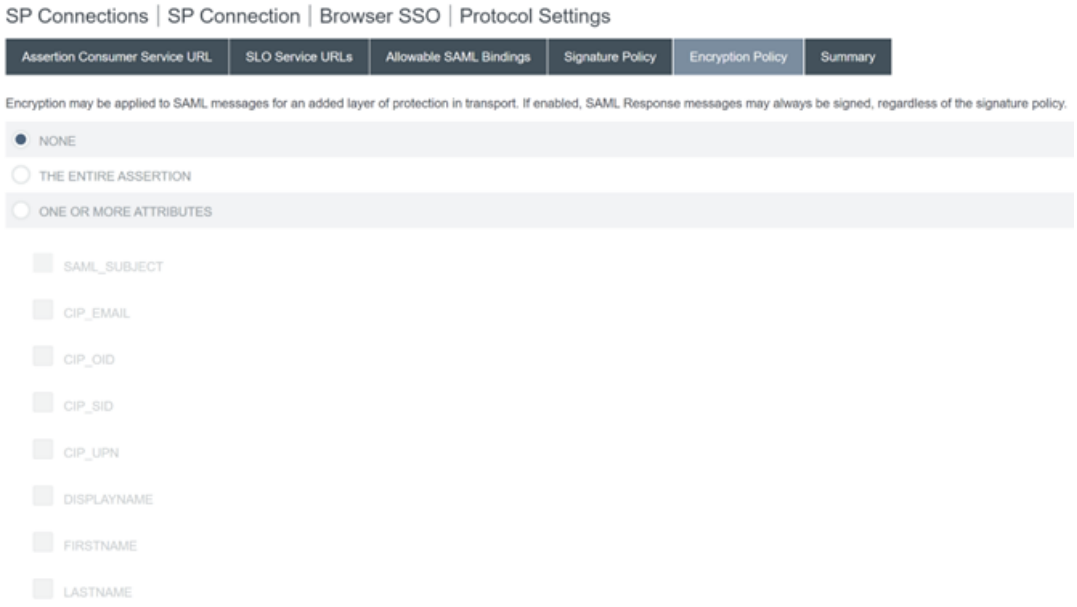


> 重要:
>
> SAML 署名設定は、SAML 接続の両側で一貫して構成する必要があります。Workspace または Citrix Cloud（SP）は、署名付き SSO および SLO リクエストを送信するように構成する必要があります。

a) Citrix Cloud の SAML 署名検証証明書を使用して署名付きリクエストを強制するように PingFederate（ID プロバイダー）を構成する必要があります。

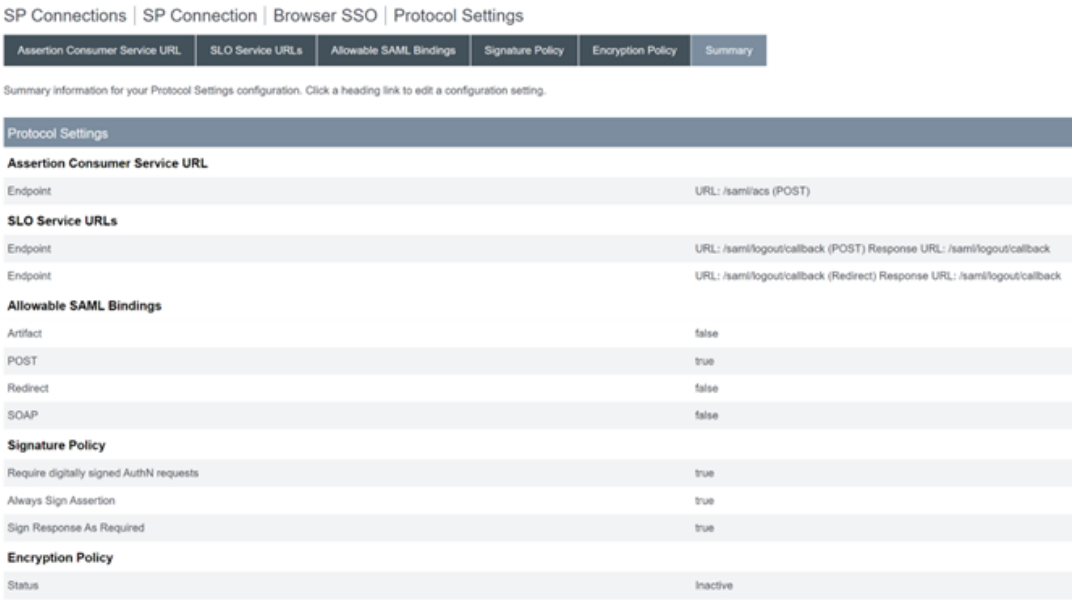


b) **Encryption Policy**（暗号化ポリシー）を構成します。



> 注：
>
> 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、初期設定およびテスト時には暗号化を［**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、Workspace 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証明した後で暗号化を有効にすることをお勧めします。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、暗号化が有効になっているときに SAML に関する問題をデバッグすることはできません。

c)［**Summary**］（概要）タブを確認します。



d) **Citrix Cloud** サービス プロバイダー（**SP**）接続 を確認します。**Citrix Cloud** の **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

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

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

Metadata URL

Metadata URL	https://saml.cloud .com/saml/metadata
Automatically Update Metadata	true

General Info

Partner's Entity ID (Connection ID)	https://saml.cloud com
Connection Name	CitrixCloudStaging
Base URL	https://saml.cloud .com

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_email
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_oid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_sid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
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	firstName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	lastName
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_email	cip_email (Adapter)
cip_oid	cip_oid (Adapter)
cip_sid	cip_sid (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
firstName	firstName (Adapter)
lastName	lastName (Adapter)
Issuance Criteria	
Criterion	(None)

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)

> 役に立つヒント：
>
> SP 接続の［Activation & Summary］ページを使用すると、構成をすばやく簡単に変更できるため、SAML アプリケーションを確認したり、デバッグを行ったりできます。SP 接続の［Activation & Summary］ページでは、セクションのタイトルをクリックすることで、任意の SAML 設定サブセクションに移動できます。これらの設定を更新するには、赤で強調表示されているタイトルのいずれかをクリックします。

16. 完了した **Citrix Cloud** の **SP** 接続はこのように一覧に表示されます。

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 Cloud と Workspace でテストした後は、SP 接続のバックアップを取ることをお勧めします。

ID プロバイダーの SAML 署名証明書の更新

May 30, 2024

Author:
Mark Dear

署名付きの要求と応答を使用する 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。

SAML プロバイダー署名証明書

この証明書は SAML プロバイダーによって提供され、SAML 接続を構成するときに Citrix Cloud にアップロードされます。

Citrix Cloud 管理者が展開の準備をする時間を確保するために、SAML 署名証明書は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。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が証明書のローテーションを行う必要があります。

よくある質問

SAML プロバイダー証明書は何に使用されますか**?**

SAML プロバイダー証明書は、認証プロセス中に SAML プロバイダーから Citrix Cloud に送信される SAML 応答の署名を検証するために使用されます。

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**?**

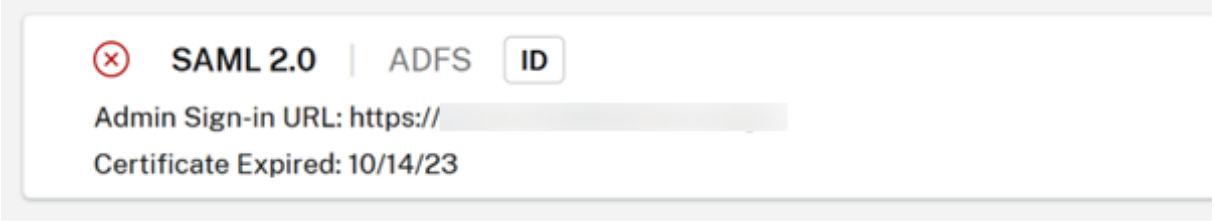
この証明書は、Azure AD、Okta、PingFederate、ADFS などの SAML プロバイダーによって提供されます。Citrix は、この証明書のローテーションと更新を管理していません。この証明書は、最初に SAML 接続を作成したときに Citrix Cloud にアップロードされます。**IDP** 署名証明書は通常、長期間有効です。**SP** 署名証明書よりも低い頻度で、数年おきに交換が必要な場合があります

SAML プロバイダー署名証明書の有効期限が迫っていて、**Citrix Cloud SAML** 接続に影響する可能性があることを知る方法はありますか**?**

Citrix Cloud は、SAML プロバイダー署名証明書の有効期限の 30 日前に警告を表示します。

```
Certificate Expiring Soon: <certExpirationDate>
```

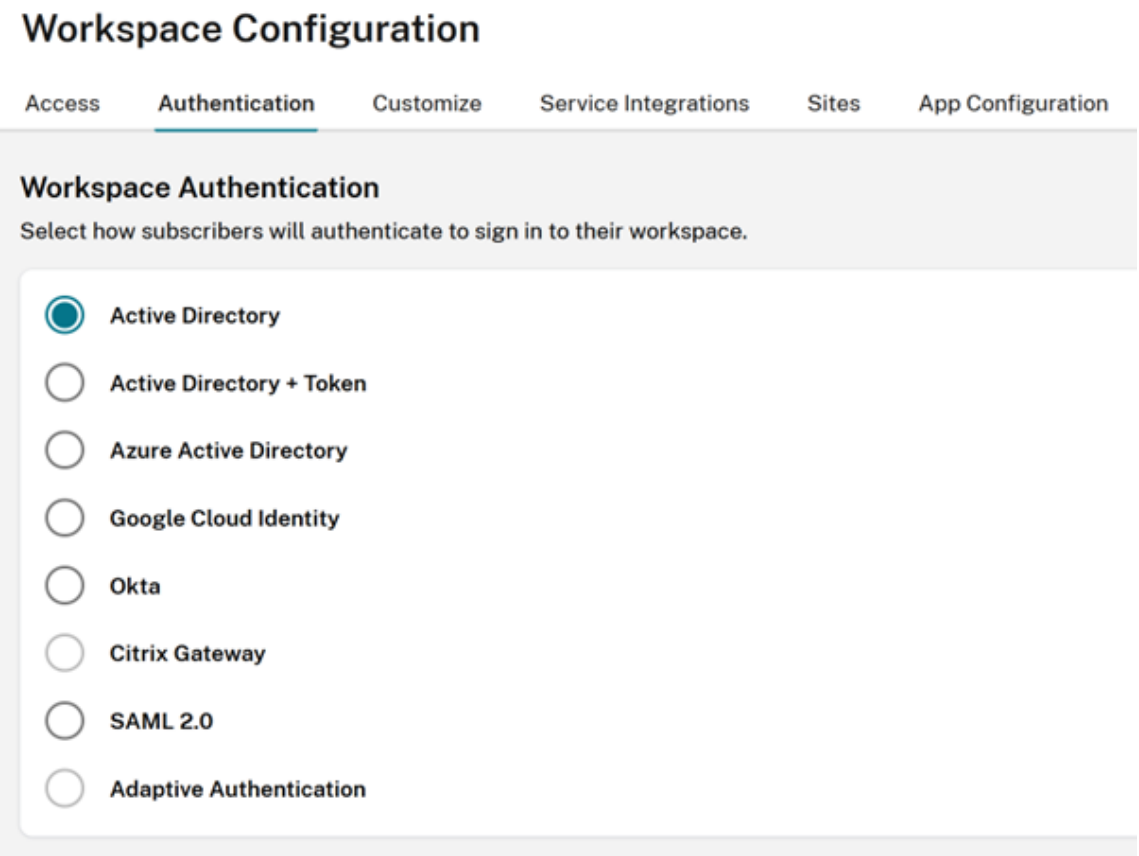
また、証明書の有効期限が実際に切れると、以下に示すようにエラーが表示されます。



SAML 接続を使用しながら、ダウンタイムなしで **SAML** プロバイダー証明書を更新できますか**?**

いいえ。定期的にスケジュール設定された保守時間中に SAML の切断と再接続を実行する必要があります。
ID プロバイダー（IdP）署名証明書を更新してください

1. Active Directory などの SAML の切断/再接続操作を実行するときは、［ワークスペース構成］内の代わりの ID プロバイダーを選択し、［認証］を選択します。



2. Citrix Cloud への SAML ログオンに使用される既存の GO URL（`https://citrix.cloud.com/go/<yourgourl>`など）をバックアップします。
3. 既存の SAML エンドポイントのバックアップを作成します。これらは Citrix Cloud コンソールからコピーできます。既存の SAML 接続内から次の SAML エンドポイントをバックアップします。

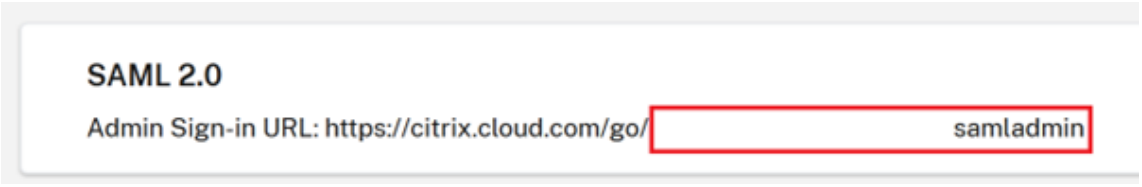
   - ID プロバイダーのエンティティ ID
   - ID プロバイダーの SSO サービス URL
   - ID プロバイダーのログアウト URL

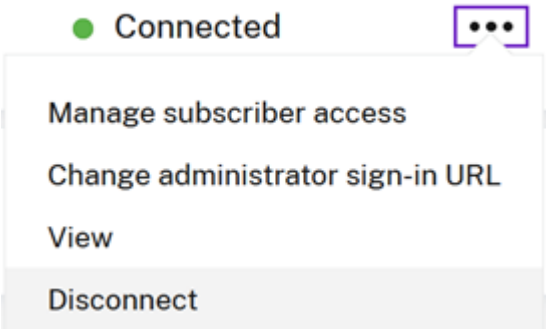
   エンティティ ID、SSO URL、およびログアウト URL をバックアップします。

> 重要:
>
> 切断を実行する前に、既存の IDP 署名証明書と代替の IDP 署名証明書の両方のコピーがあることを確認してください。これにより、新しい SAML プロバイダー証明書が無効で、ログオンの問題が発生した場合に、古い証明書にロールバックできます。切断を実行する前に、Citrix Cloud UI から古い証明書のコピーを取得することはできません。SAML アプリケーションから取得する必要があります。

1. ［**ID** およびアクセス管理］で SAML を切断し、［認証］に移動して SAML 接続を選択し、省略記号をクリックして ［切断］を選択します

2. [**ID** およびアクセス管理] で SAML を再接続し、[認証] をクリックします





3. デフォルトの SAML 接続設定をすべて受け入れます。
4. 以前にバックアップしたすべての SAML アプリケーションのエンドポイントを再入力するか、SAML プロバイダー UI 内から SAML アプリ用にこれらを再度取得します。

   - ID プロバイダーのエンティティ ID
   - ID プロバイダーの SSO サービス URL
   - ID プロバイダーのログアウト URL

> 重要:
>
> スコープ付きエンティティ ID 機能を使用している場合は、SAML の切断/再接続を実行した後に、SAML アプリケーションを新しいスコープ ID で更新する必要もあります。スコープ付きエンティティ ID 機能について詳しくは、「Citrix Cloud でスコープ付きのエンティティ ID を使用した SAML アプリケーションを構成する」を参照してください。新しく生成されたスコープ ID を Citrix Cloud の SAML UI からコピーし、SAML アプリケーションのエンティティ ID を新しいスコープ ID で更新します。
> エンティティ ID を`https://saml.cloud.com/<new scope ID after reconnect>`に更新する必要があります。

サービスプロバイダー **SAML** 署名証明書の更新

May 30, 2024

Author:
Mark Dear

署名付きの要求と応答を使用する 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。

サービスプロバイダー署名証明書

この証明書は Citrix によって定期的に提供され、SAML アプリケーションにアップロードされるか、Citrix Cloud の SAML メタデータ経由で取得されます。

Citrix Cloud 管理者が展開の準備をする時間を確保するために、SAML 署名証明書は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では、サービスプロバイダーと ID プロバイダーの両方が確実に連携し、ダウンタイムを防止する必要があります。

選択した SAML プロバイダーがサービスプロバイダー 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は、期限切れになる証明書を置き換えるために、SAML プロバイダー内で SAML 署名証明書を手動でローテーション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構成する方法に関して詳細が記載されています。Citrix では、署名付き SAML 構成のみをお勧めします。これらの構成はより安全であり、一部の SAML プロバイダーではログアウト（SLO）を成功させるために必要になるためです。

よくある質問

SAML 署名とは何ですか**?**

SAML 署名証明書は、サービスプロバイダー（SP）と SAML プロバイダー（IdP）間で送信されるデータを検証するために使用される X.509 証明書です。SAML プロバイダー（IdP）は、Citrix Cloud SAML 署名証明書を使用して、Citrix Cloud から SAML 認証要求内で送信された署名を検証します。Citrix Cloud は、SAML プロバイダー署名証明書を使用して、SAML 応答が信頼できる接続済みの IdP からのものであることを確認します。

SAML の署名付き要求の強制とは何ですか**?**

Citrix Cloud が署名付き要求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 SAML 要求の受信を拒否することを保証するわけではありません。大半の SAML プロバイダーには、署名付き要求を強制するオプションがあります。つまり、SAML プロバイダーへのログインを求める署名のない要求を受信すると、ログオンは失敗します。IdP 設定のステータスを確認するのは、SAML プロバイダー管理者の責任です。Citrix サポートは、署名付き要求がお客様の SAML アプリケーション内で強制されるかどうかを制御したり、それを表示したりすることはできません。

Citrix はサービスプロバイダーの **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**?**

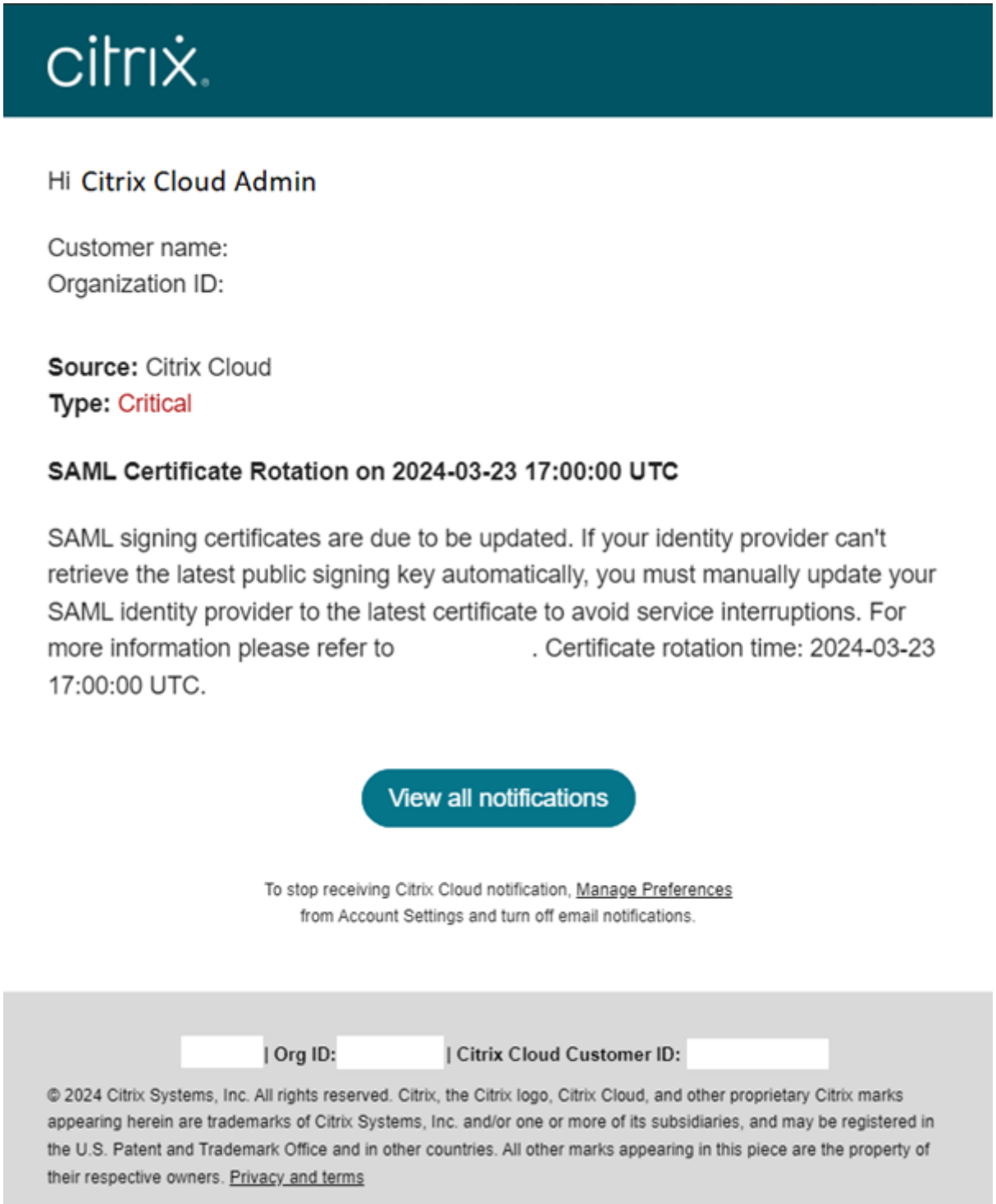
有効なサービスプロバイダー署名証明書と新しく発行された署名証明書が重複することがないようにするため、Citrix ではサービスプロバイダー署名証明書を約 11 か月ごとにローテーションしています。これは、既存の証明書の有効期限が切れる 30 日前に Citrix Cloud のお客様が有効な証明書を利用できるようにするためです。

サービスプロバイダー **SAML** 署名証明書のアドバタイズフェーズとは何ですか**?**

アドバタイズフェーズでは、現在の SAML 署名証明書と代わりの SAML 署名証明書が Citrix Cloud メタデータに表示されます。ローテーションの日時までは、アクティブな証明書のみを SAML 要求の検証に使用できます。

現在の **Citrix Cloud SAML** 署名証明書の有効期限が近づいているため交換が必要であることを示す通知が、メールと **Citrix Cloud** 管理コンソールで届いたのはなぜですか**?**

SAML プロバイダー（IdP）は、Workspace や Citrix Cloud 管理者コンソールなどのサービスプロバイダーからの受信 SAML 要求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。Workspace または Citrix Cloud 管理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に迫っていることが通知されます。



citrix.

Hi **Citrix Cloud Admin**

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

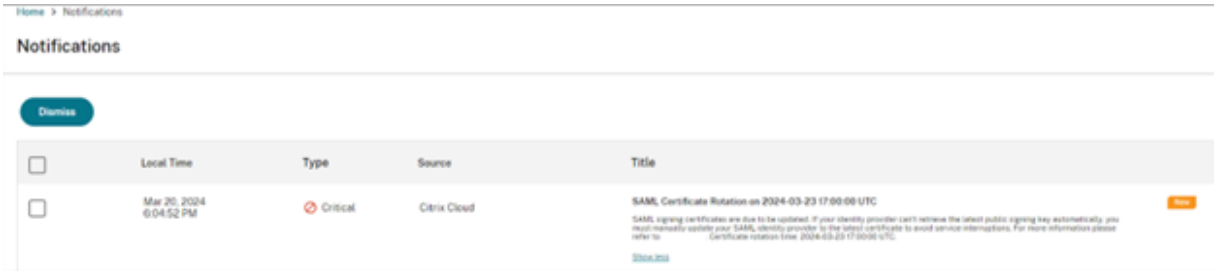
SAML Certificate Rotation on 2024-03-23 17:00:00 UTC

SAML signing certificates are due to be updated. If your identity provider can't retrieve the latest public signing key automatically, you must manually update your SAML identity provider to the latest certificate to avoid service interruptions. For more information please refer to . Certificate rotation time: 2024-03-23 17:00:00 UTC.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

| Org ID: | Citrix Cloud Customer ID:



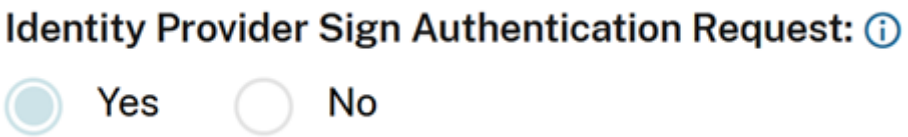
Citrix Cloud のお客様が **Citrix Cloud SAML** 署名証明書のローテーションの影響を受けているかどうかはどうすればわかりますか**?**

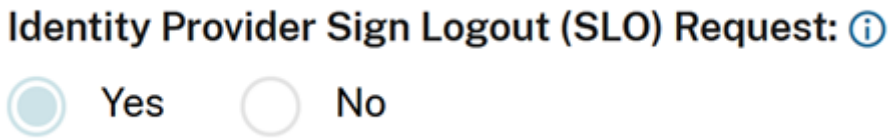
以下の SAML 構成を使用している Citrix Cloud のお客様が影響を受けます。

- Citrix Cloud 内の SAML 接続で ［認証要求に署名する］**=**［はい］が構成されています
- Azure Active Directory、ADFS、Okta などの SAML プロバイダーが、署名されていない SAML 要求を拒否するように構成されています（署名付き要求の強制）。
- 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）が構成されています。SAML プロバイダーによっては、Okta や PingFederate などの SLO 要求への署名が必要な場合があります。

Citrix Cloud SAML 接続の署名の構成を確認する方法を教えてください

［**ID** およびアクセス管理］>［**SAML 2.0**］>［表示］に移動して、Citrix Cloud SAML 接続内で ［認証要求に署名する］が有効になっているかどうかを確認します。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** プロバイダーの署名認証**/**ログアウト要求が［はい］になります。





SAML アプリ内で署名の強制が構成されているかどうかを確認する方法を教えてください

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。このオプションが提供されていない場合もあります。Azure AD、ADFS、Okta、および PingFederate はすべて署名の強制をサポートしています。SAML 管理者は、

SAML プロバイダーの機能とその最新の構成を把握しておくことが重要です。Citrix サポートはこれを制御したり把握したりすることはできません。

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 メタデータを使用して Citrix によって提供され、SP 署名証明書のローテーションのアドバタイズフェーズ中に定期的に更新されます。更新は、少なくとも 1 暦年に 1 回発生します。

米国、EU（欧州）、APS（南アジア太平洋）向け：https://saml.cloud.com/saml/metadata

日本向け：https://saml.citrixcloud.jp/saml/

米国政府機関向け：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どのタイミングですか**?**

古い Citrix Cloud 署名証明書は、メールと Citrix Cloud 管理者コンソールの通知に記載されている証明書のローテーション日時以降にのみ削除してください。

メタデータの交換を使用して、**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

SAML メタデータの交換を使用する場合、SAML プロバイダーは、https://saml.cloud.com/saml/metadataなどのメタデータ URL を監視することにより、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 メタデータの交換をサポートしている場合、SP 署名証明書は既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の交換をサポートしていることを確認します。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
>
> 各サードパーティの SAML プロバイダーがサポートする SAML 機能には大きな違いがあります。Citrix Cloud 管理者には、使用している SAML プロバイダーの機能と要件を把握して理解する責任があります。これは、

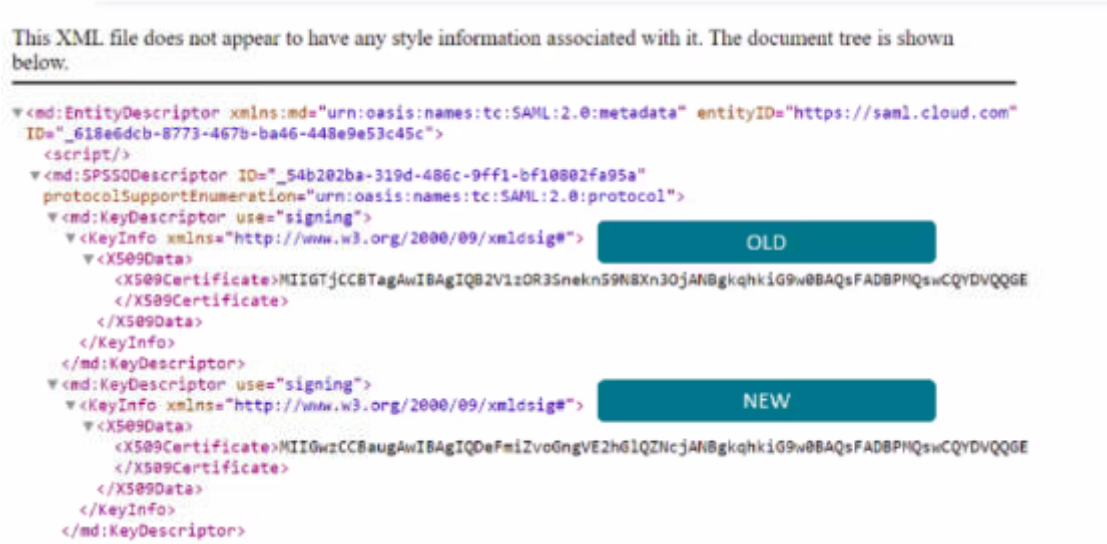
> Citrix Cloud SAML 接続構成（SP）と SAML プロバイダー（IdP）構成の両方が一致していることを確認するために必要です。SAML プロバイダーのドキュメントを参照して、署名検証がサポートされているかどうか、および SAML の要求と応答に署名が必要かどうかを確認してください。

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

> 重要
>
> SP 証明書のローテーションは、Citrix Cloud から新しい証明書が公開されるたびに実行する必要があります。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。

1. Citrix Cloud から最新の SAML メタデータを取得するには、［**ID** およびアクセス管理］で現在の SAML 接続を表示し、［認証］をクリックし、［**SAML** 接続］を選択して ［表示］をクリックします。
   次の画像は、米国、EU、APS などの Citrix Cloud 地域でこのファイルがどのように表示されるかを示す例です：

   https://saml.cloud.com/saml/metadata



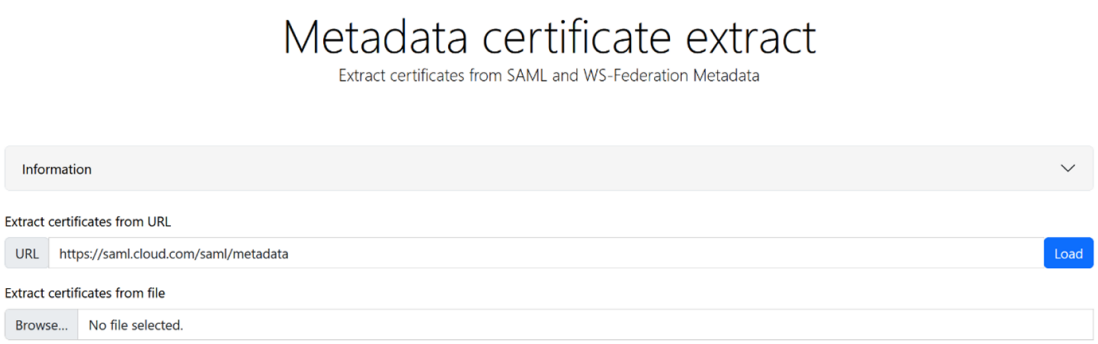
   このメタデータ XML ファイルの例には、x509 の Citrix Cloud SAML 署名証明書が 2 つあります。

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 を指定することで、メタデータから x509 証明書を抽出できます。

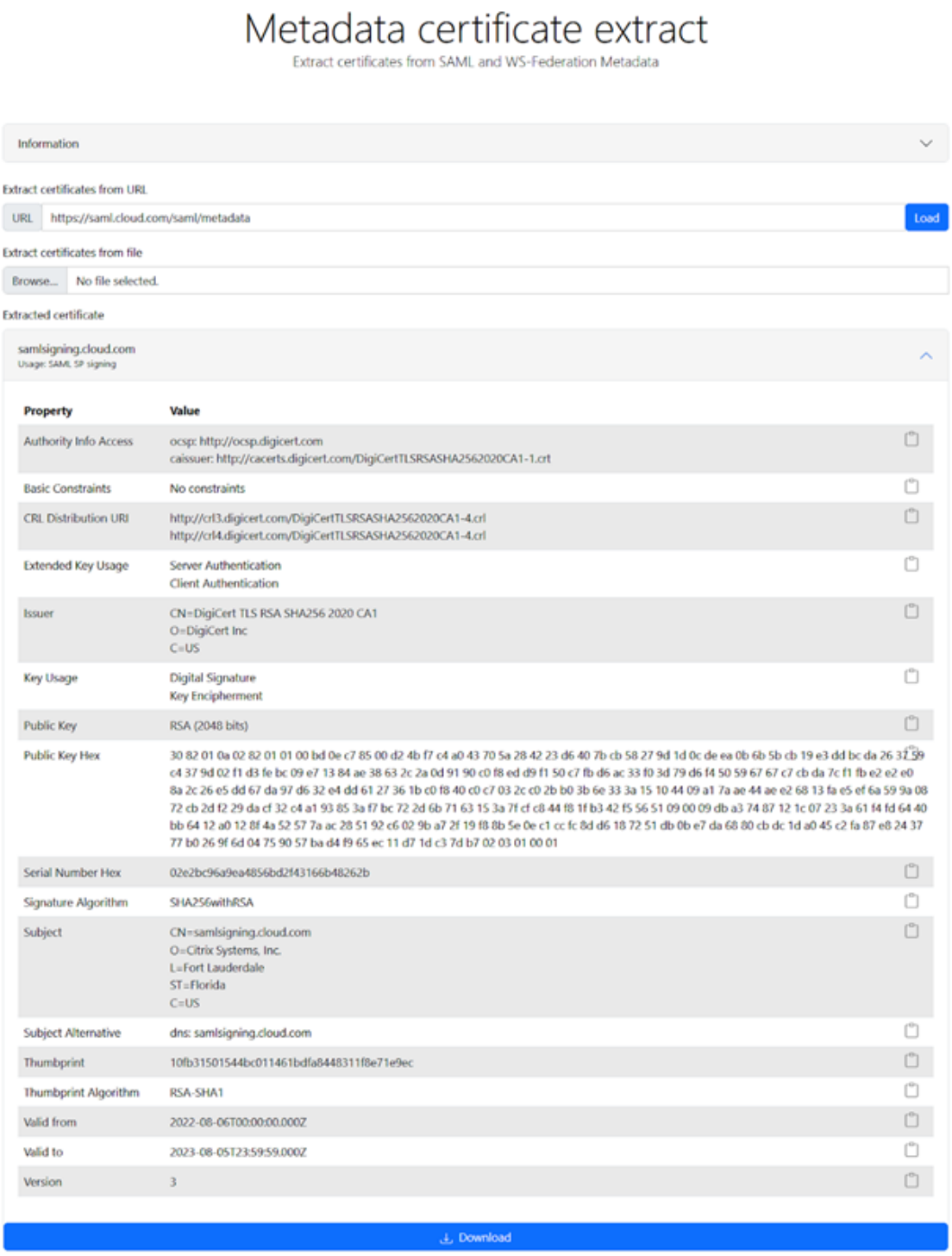
3. https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtractにアクセスします

4. Citrix Cloud のお客様の地域に対応する SAML メタデータの URL を入力してください：

   - 米国、EU（欧州）、APS（南アジア太平洋）向け：https://saml.cloud.com/saml/metadata
   - 日本向け：https://saml.citrixcloud.jp/saml/metadata
   - 米国政府機関向け：https://saml.cloud.us/saml/metadata



SAML 署名証明書をhttps://www.rcfed.com/SAMLWSFed/MetadataCertificateExtractから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。適切な SAML プロバイダーのマニュアルを使用して、SP 署名証明書のローテーション手順が適切であることを確認してください。

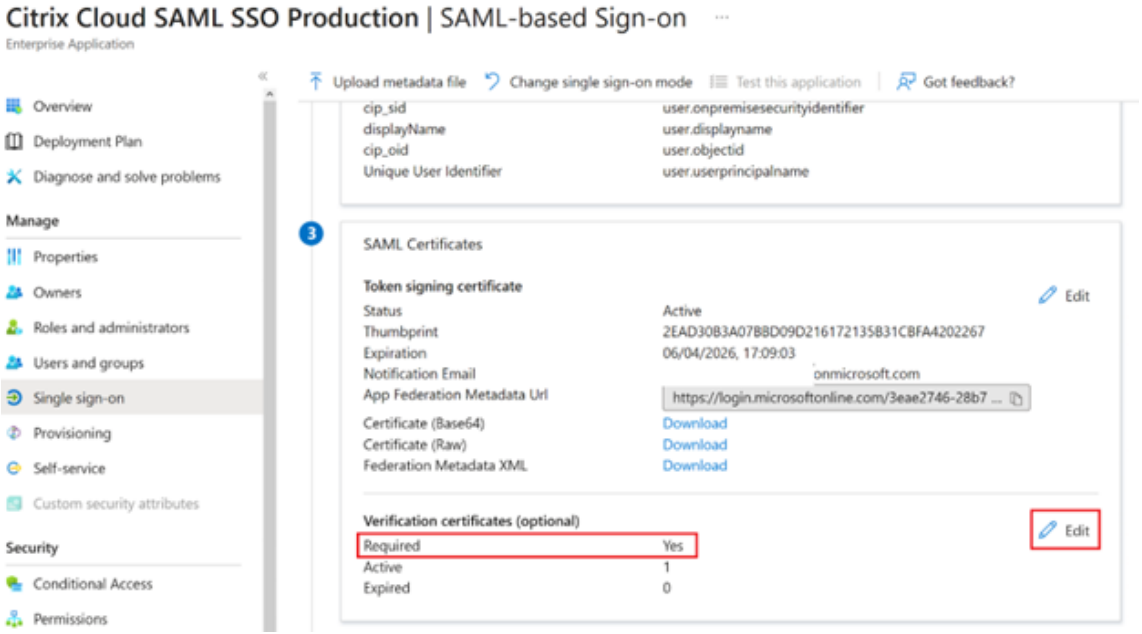
   SAML プロバイダーによっては、既存の SAML 署名証明書を新しい証明書に置き換える必要がある場合があります。場合によっては、SAML プロバイダーが複数の SP 署名証明書を同時にサポートする場合もあるため、

新しい署名証明書をアップロードするだけで十分です。有効期限が切れたら、古い証明書を削除することをお勧めします。

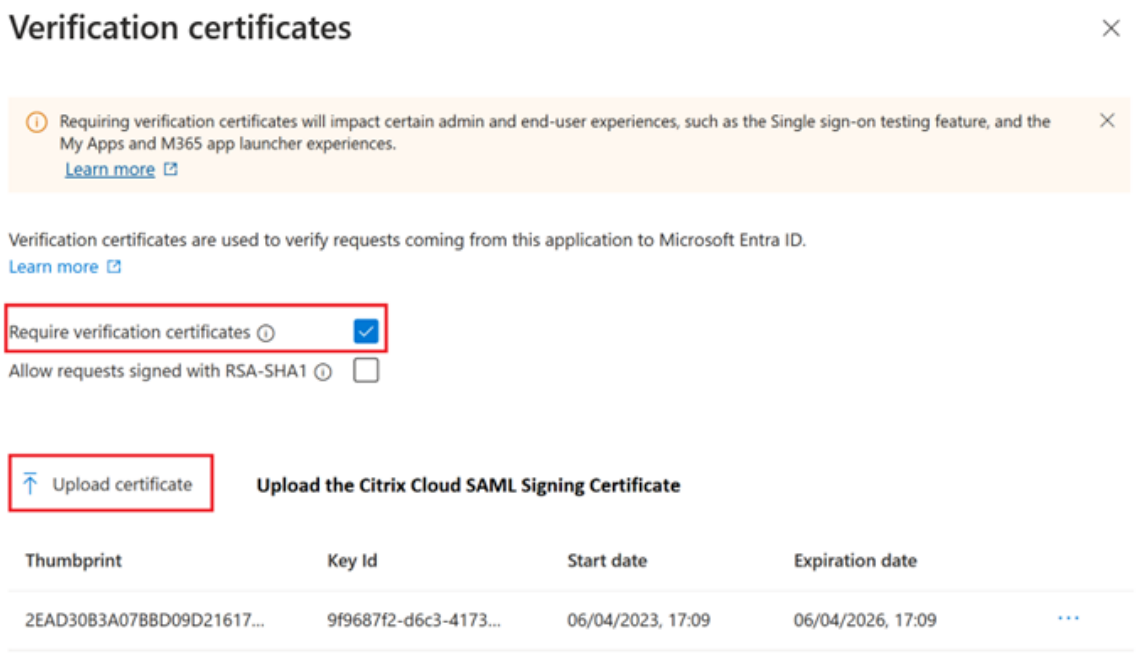
代わりの **Citrix Cloud SAML** 署名証明書を **Azure Active Directory SAML** アプリケーションにアップロード

Azure Active Directory SAML アプリを構成する前に、「SAML 要求の署名検証」で詳細を参照してください。

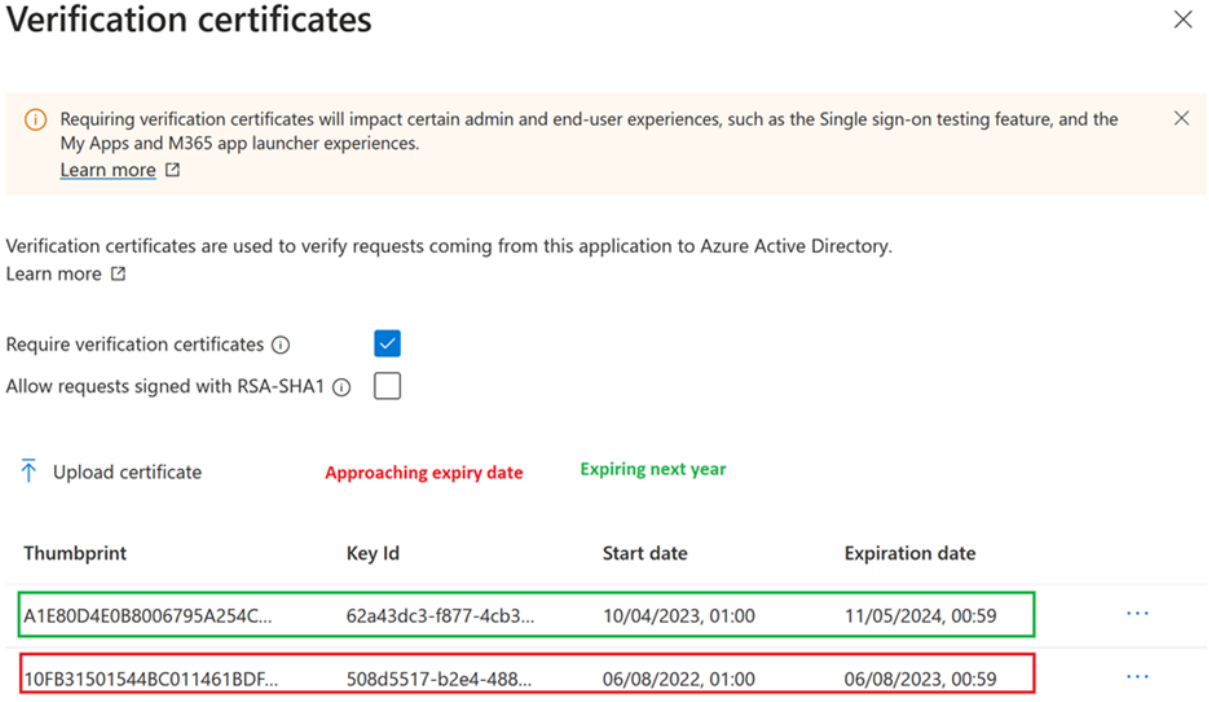
1. **Azure Active Directory** に移動し、**Enterprise Applications** を選択してお使いの SAML アプリをクリックします。
2. SAML アプリケーション内の SAML 証明書セクションを探します。



3. [**Upload Certificate**] を選択し、SAML メタデータから取得した代わりの Citrix Cloud SAML 署名証明書をアップロードします。



> 注:
>
> Azure Active Directory SAML アプリでは複数の署名検証証明書を構成できるため、現在の証明書の有効期限が切れる前に余裕をもって代わりの証明書をアップロードできます。次のスクリーンショットには、2 つの有効な証明書が表示されています。証明書の 1 つは、近い将来期限切れになる予定です。アップロードされた証明書の少なくとも 1 つが有効で、まだ有効期限が切れていない限り、Citrix Workspace および Citrix Cloud への SAML ログインは引き続き成功し、停止は発生しません。

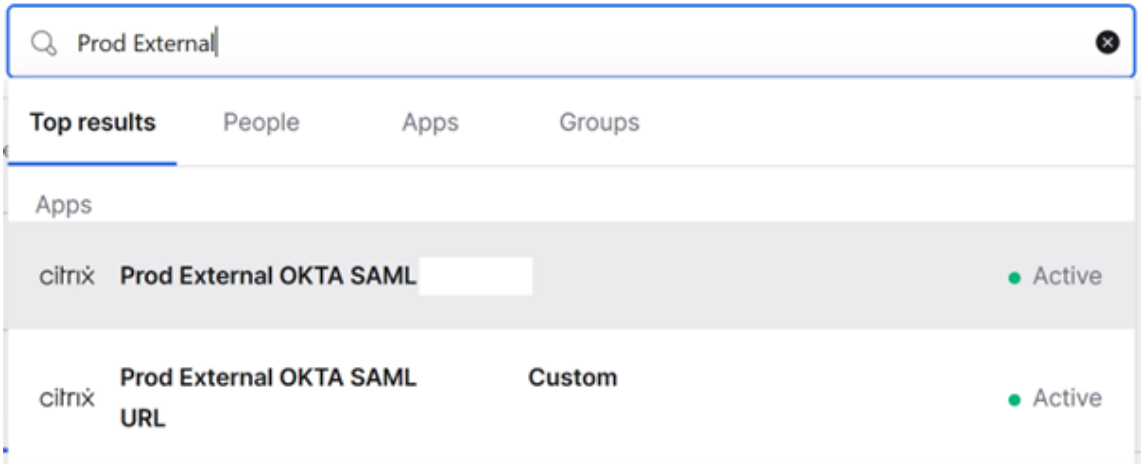


> 重要:
>
> メールや Citrix Cloud 管理コンソールの通知に記載されている SAML ローテーションの日時が経過するまで、既存の検証証明書は削除しないでください。新しい Citrix Cloud 証明書は、これら 2 つの通知で指定された日時にのみ有効になります。

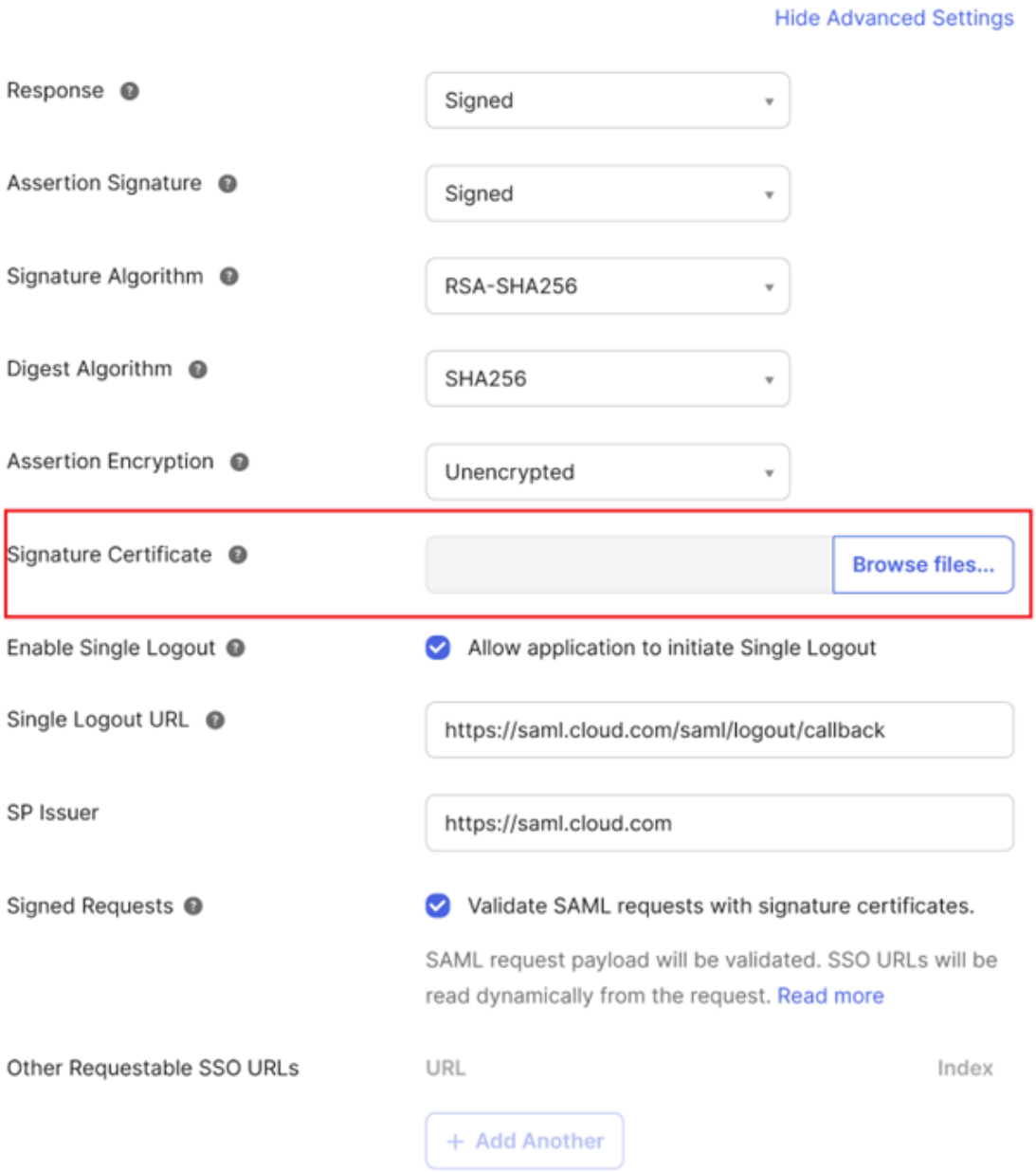
代わりの **Citrix Cloud SAML** 署名証明書を **Okta SAML** アプリケーションにアップロード

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証明書で上書きする以外の方法はありません。これは、定期的にスケジュール設定された保守時間に行うことをお勧めします。

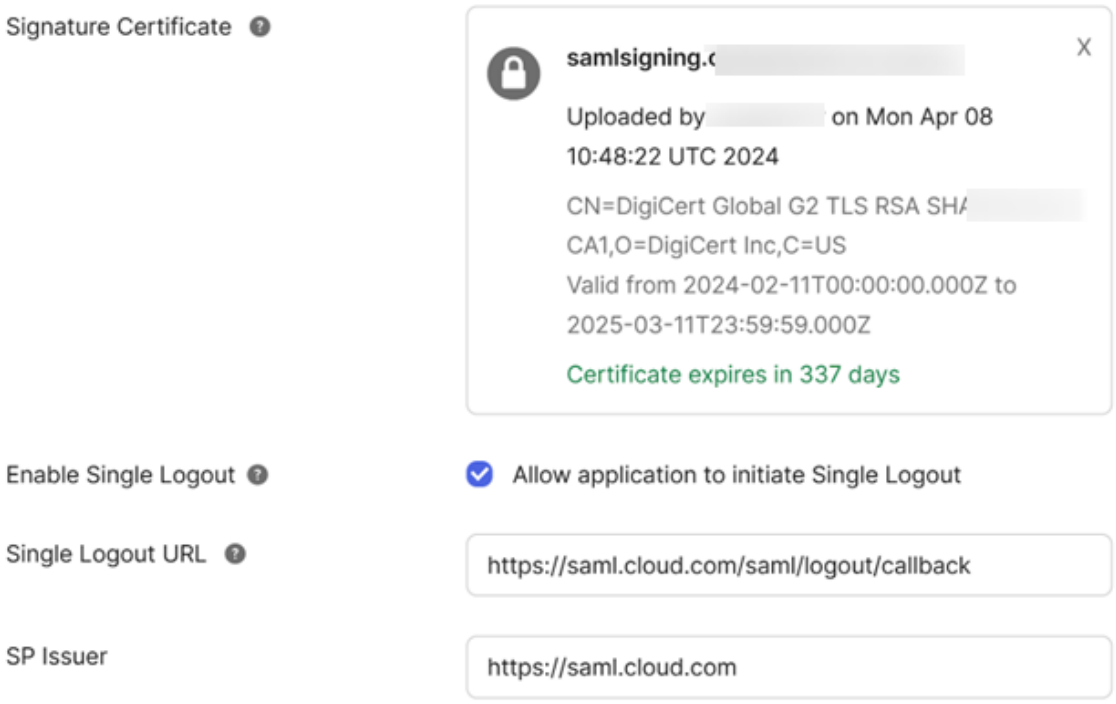
1. ［アプリケーション］に移動し、［アプリケーション］を選択して、Okta SAML アプリを検索します



2. ［一般］から ［**SAML** 設定］に移動し ［編集］をクリックして、［**SAML** の構成］、［詳細設定を表示する］、［署名付き証明書］の順に選択して代わりの証明書をアップロードします。Okta は、現在の Citrix Cloud SAML 署名証明書をアップロード UI に表示しません。これがアップロードされた後にのみ、代わりの証明書が表示されます。



3. ［署名付き証明書］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代わりの Citrix Cloud SAML 署名証明書をアップロードします。



> 重要
>
> メールと Citrix Cloud 管理コンソールの通知に記載されている SAML ローテーション日時まで、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 つの通知で指定された日時にのみ有効になります。

ADFS 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

July 2, 2024

Author:
Mark Dear

この記事では、SAML を使用して Citrix Workspace または Citrix Cloud にサインインするために Citrix Cloud が必要とする、証明書利用者の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、「Citrix Cloud で ID プロバイダーとして SAML を接続する」の説明に従って、ADFS サーバーと Citrix Cloud の間の 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「Citrix Cloud での SAML 構成」を参照してください。

前提条件

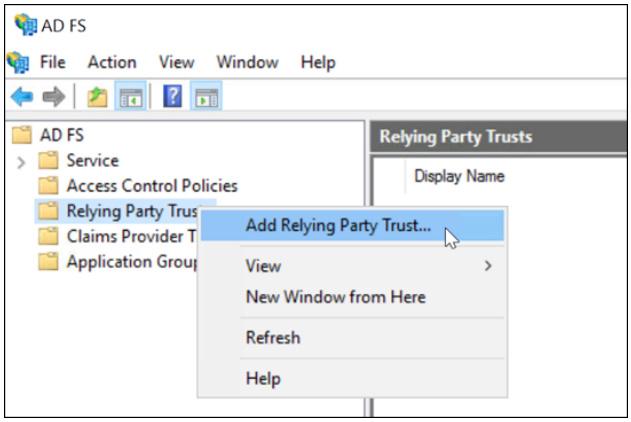
この記事の手順は、環境内の ADFS サーバー展開が Citrix FAS とともに既に稼働していることを前提としています。Citrix FAS は、セッションの起動中に VDA にシングルサインオンを提供するために必要です。

詳しくは、以下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 の展開
- 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

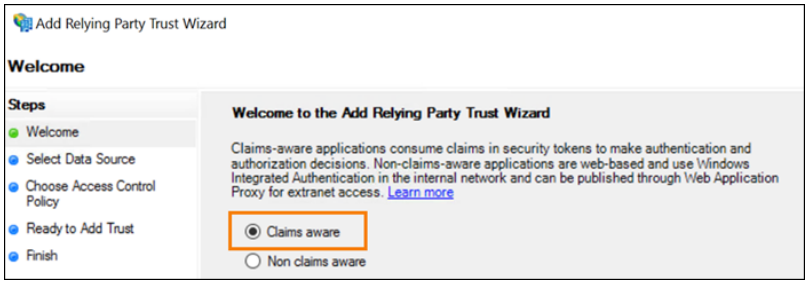
Citrix Cloud の証明書利用者の信頼を構成する

1. AD FS 管理コンソールから、左側のペインで ［**AD FS**］ノードを展開します。
2. ［証明書利用者の信頼］を右クリックし、［証明書利用者の信頼を追加］を選択します。

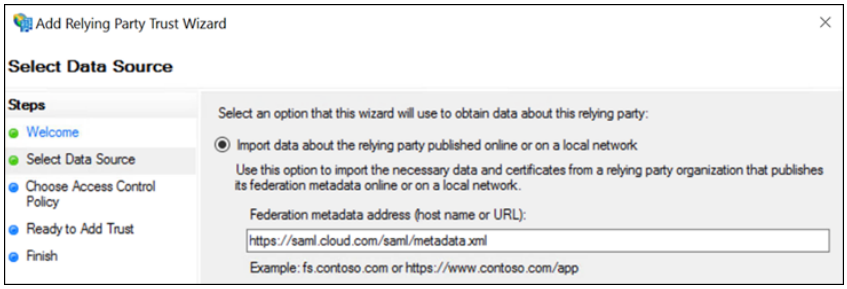


［証明書利用者の信頼を追加］ウィザードが表示されます。

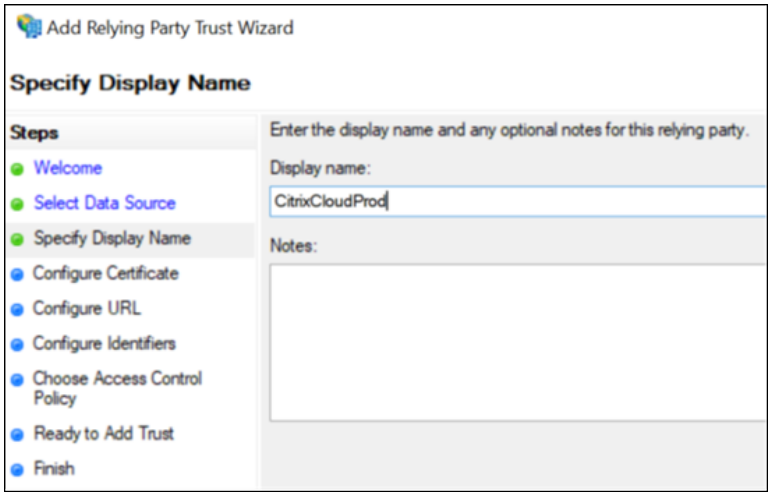
3. ［クレーム対応］を選択し、［次へ］を選択します。



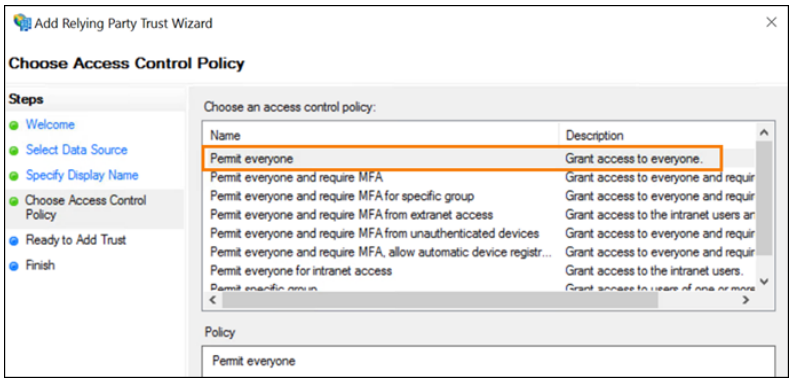
4. ［フェデレーションメタデータアドレス］に`https://saml.cloud.com/saml/metadata.xml`を入力します。［次へ］を選択します。



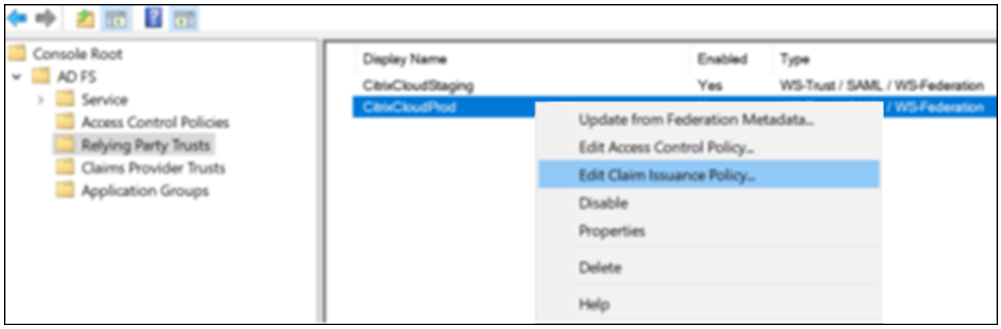
5. 表示名には `CitrixCloudProd` を入力します。［次へ］を選択します。



6. アクセス制御ポリシーとして、［すべてのユーザーを許可］を選択します。［次へ］を選択します。

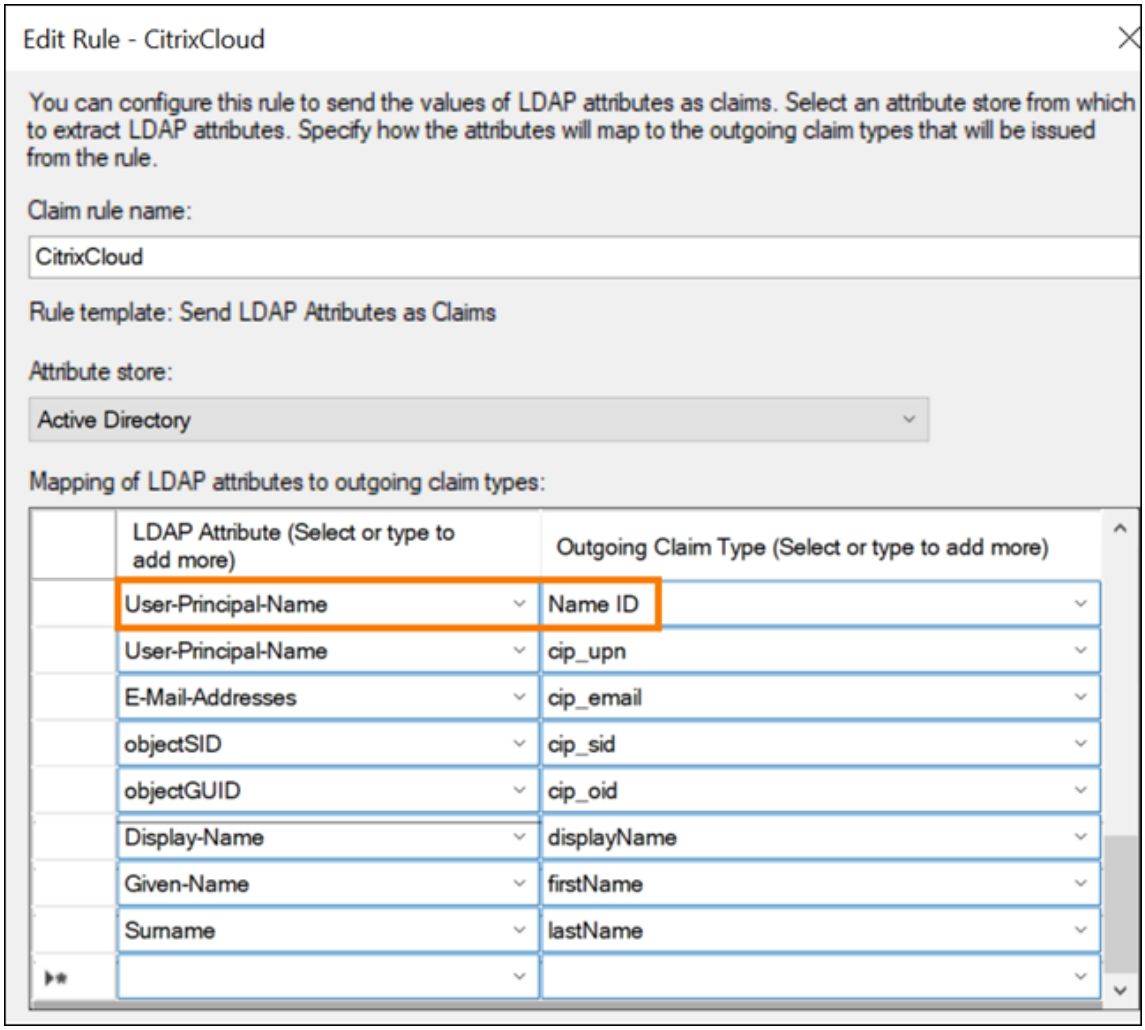


7. ［信頼を追加する準備ができました］画面で、［次へ］を選択します。
8. ［完了］画面で、［このアプリケーションの要求発行ポリシーを構成する］を選択します。［次へ］を選択します。



9. 新しく作成した証明書利用者を右クリックし、［要求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** 属性を要求として送信］を選択します。［次へ］を選択します。
11. ［要求ルール名］に`CitrixCloud`を入力します。
12. ［属性ストア］で、［**Active Directory**］を選択します。
13. ［**LDAP** 属性の送信要求タイプへのマッピング］で、次の LDAP 属性を表示されているとおりに追加します。

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
メールアドレス	cip_email
objectSID	cip_sid
objectGUID	cip_oid
表示名	displayName
指定の名前	firstName
姓	lastName



14. ［完了］を選択します。

PowerShell を使用して **Citrix Cloud** の証明書利用者の信頼を変更する

デフォルトの「すぐに使える」構成を使用して ADFS サーバーを構成している場合は、このセクションの手順を使用して、Citrix が推奨する構成を満たすようにサーバーを更新できます。このタスクは、`nameidentifier`属性が要求ルールセットに含まれていない場合、または要求ルールセットの最初の SAML 属性ではない場合に、Citrix Cloud または Citrix Workspace からの SAML の単一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 の証明書利用者の信頼を構成する」の手順を使用して要求ルールセットを作成した場合は、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、PowerShell を使用して既存のルールセットを新しい要求ルールセットに置き換えます。ADFS 管理コンソールは、このタイプの操作をサポートしていません。

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 要求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 "CitrixCloudStaging" | Select-
    Object -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
<!--NeedCopy-->
```

3. Citrix が提供する claimrules.txt ファイルをhttps://github.com/citrix/sample-scripts/tree/master/citrix-cloud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、必要な要求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
<!--NeedCopy-->
```

PowerShell を使用して証明書利用者の信頼の **SAML** 署名設定を更新する

デフォルトでは、ADFS 証明書利用者の信頼には次の設定があります。

- EncryptClaims：True
- SignedSamlRequestsRequired：False
- SamlResponseSignature：AssertionOnly

セキュリティを強化するために、Citrix 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 リクエストを使用することをお勧めします。このセクションでは、PowerShell を使用して既存の証明書利用者の信頼の署名設定を更新し、Citrix が推奨する構成を満たすようにする方法について説明します。

1. ADFS サーバー上の現在の RelyingPartyTrust 構成を取得します。

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
<!--NeedCopy-->
```

2. **CitrixCloudProd** 証明書利用者の信頼設定を更新します。

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
```



```
<!--NeedCopy-->
```

3. Citrix サポートに連絡し、Citrix Cloud 顧客で認証機能 **EnableSamlLogoutSigningAndPost** を有効にするようリクエストします。これにより、ユーザーが Citrix Workspace または Citrix Cloud からサインアウトするときに、Citrix Cloud は SAML シングルログアウトリクエストを署名なしのリダイレクトリクエストではなく、署名付き POST リクエストとして送信します。SAML プロバイダーがシングルログアウトの署名付きリクエストを要求し、署名なしのリダイレクトを拒否する場合は、署名付き POST リクエストを送信する必要があります。

Citrix Cloud の **SAML** 構成

Citrix Cloud で SAML 接続を構成するとき（「SAML プロバイダーのメタデータを Citrix Cloud に追加」を参照）、ADFS の値を次のように入力します。

Citrix Cloud のフィールド	入力する値
エンティティ ID	`https://adfs.YourDomain.com/adfs/services/trust`、`YourDomain.com`は ADFS サーバードメインです。
認証要求に署名する	はい
SSO サービス URL	`https://adfs.YourDomain.com/adfs/ls`、`YourDomain.com`は ADFS サーバードメインです。
バインドメカニズム	HTTP POST
SAML 応答	応答またはアサーションに署名する
認証コンテキスト	未指定、完全一致
ログアウト URL	`https://adfs.YourDomain.com/adfs/ls`、`YourDomain.com`は ADFS サーバードメインです。

カスタムドメインを使用して **SAML** でワークスペースにサインインする

November 30, 2023

Author:
Mark Dear

Citrix Workspace でカスタムドメイン（https://workspaces.yourdomain.comなど）を構成している場合、Citrix Cloud でサポートする SAML サインインシナリオに応じて、Citrix Cloud および SAML プロバイダーで追加の構成が必要になる場合があります。

この構成には、SAML アプリケーションのペアが必要になる場合があります。Citrix Cloud では、SAML アプリケーションがサインイン操作の実行に cloud.com URL を使用するか workspaces.yourdomain.com URL を使用するかに応じて、異なる SAML サービスプロバイダー（SP）エンドポイントが必要になります。

Citrix Workspace でのカスタムドメインの構成について詳しくは、Citrix Workspace 製品ドキュメントの「カスタムドメインの構成」を参照してください。

1 つまたは 2 つの SAML アプリケーションを展開する場合の考慮事項

シングルまたはデュアル SAML アプリケーションソリューションのどちらを展開する必要があるかを判断するには、SAML プロバイダーがサポートする必要がある SAML サインインシナリオの組み合わせを見つけます。

次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 アプリ 1）を使用します:

- リージョンのワークスペースサインイン URL（cloud.com、citrixcloud.jp、cloud.us）が SAML プロバイダーで SP エンティティ ID として構成された、Citrix Workspace の SAML 認証。
- 一意のサインイン 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）グループの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。

ワークスペース構成で構成するカスタムドメイン（https://workspaces.mycompany.comなど）を介してユーザーに SAML 認証を追加するには、2 つ目の SAML アプリケーション（SAML アプリ 2）が必要です。

次の表に、SAML サインインシナリオと必要な SAML アプリのサポートされている組み合わせを示します。

ワークスペース URL を使用して Workspace にサインイン	カスタムドメイン URL を使用して Workspace 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 アプリ 1 は必要ですか?	SAML アプリ 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	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	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	いいえ

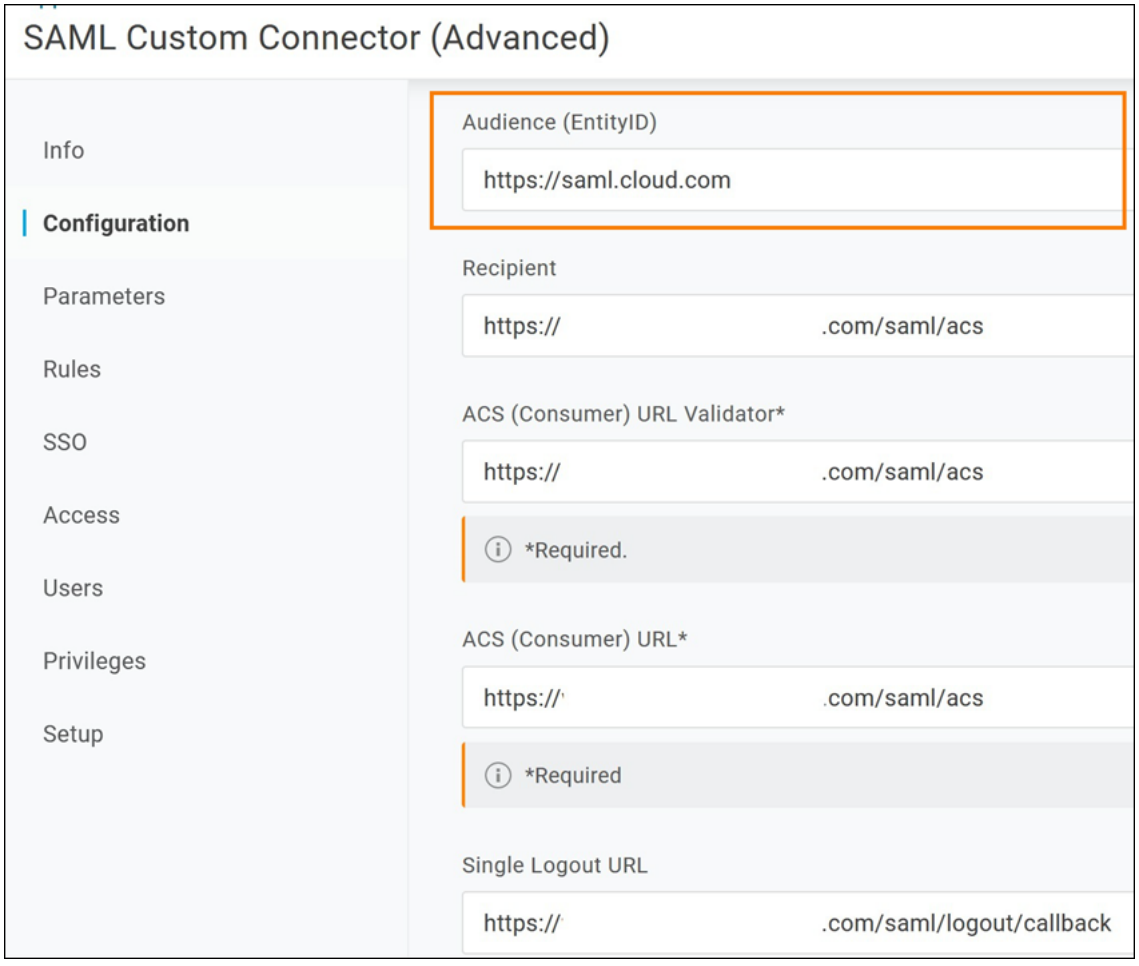
ワークスペース URL を使用して Workspace にサインイン	カスタムドメイン URL を使用して Workspace にサインイン	SAML サインイン URL を使用して Citrix Cloud にサインイン	SAML アプリ 1 は必要ですか?	SAML アプリ 2 は必要ですか?
はい	いいえ	はい	はい - cloud.com SAML エンドポイントを使用	いいえ
いいえ	いいえ	はい	はい - cloud.com SAML エンドポイントを使用	はい - カスタムドメイン SAML エンドポイントを使用
はい	はい	はい	はい - cloud.com SAML エンドポイントを使用	はい - カスタムドメイン SAML エンドポイントを使用

シングル **SAML** アプリケーション構成

1. Citrix Cloud で ［ワークスペース構成］**>**［アクセス］に移動し、カスタムドメインを構成します。詳しくは、「カスタムドメインの構成」を参照してください。
2. SAML プロバイダーの管理コンソールでカスタムドメインを SP エンドポイントとして使用して、単一の SAML アプリケーションを構成します。
3. SAML アプリケーションの SAML 署名証明書をダウンロードします。後の手順で、この証明書を Citrix Cloud にアップロードします。
4. エンティティ ID にはhttps://saml.cloud.comが入力されていることを確認してください。SAML プロバイダーによっては、この設定には代わりに **Audience** というラベルが付いている場合があります。他のすべてのエンドポイントで、https://saml.cloud.comを手順 1 で構成したワークスペースカスタムドメインに置き換えます。

   次の例は、Okta のエンドポイント構成を示しています。ここでは、**Audience Restriction** にエンティティ ID 値が含まれています:

次の例は、OneLogin のエンドポイント構成を示しています。ここでは、**Audience** にエンティティ ID 値が含まれています:



5. Citrix Cloud で ［**ID** およびアクセス管理］**>**［認証］に移動して、SAML 認証を構成します。
6. ［ワークスペース構成］**>**［認証］に移動して ［**SAML 2.0**］を選択します。

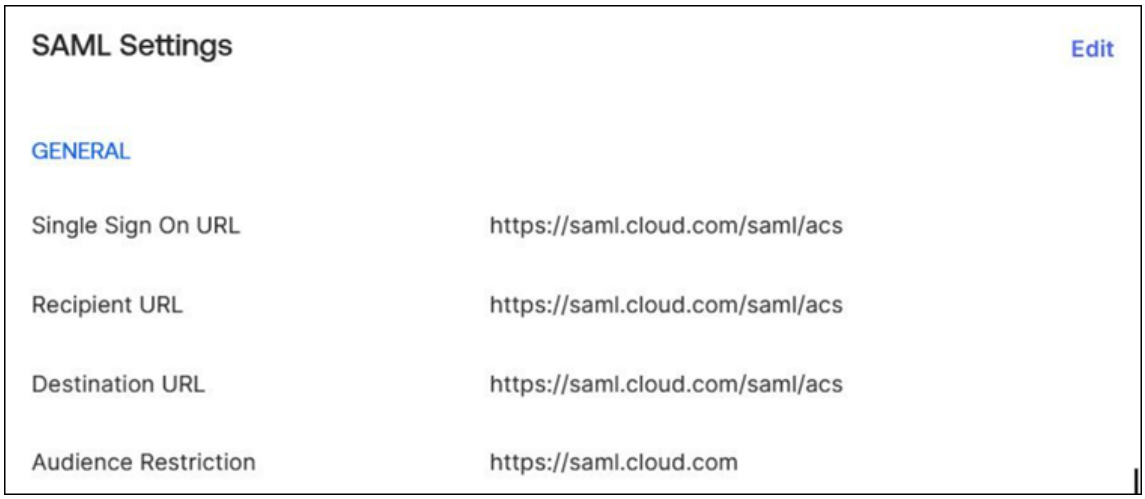
7. ［ワークスペース構成］**>**［カスタムワークスペース **URL**］**>**［編集］に移動して、［カスタムドメイン **URL** のみを使用する］を選択します。
8. ［保存］を選択して変更内容を保存します。
9. 構成をテストするには、カスタムワークスペース URL (`https://workspaces.mycompany.com`) を使用して Citrix Workspace にサインインします。

デュアル **SAML** アプリケーション構成

1. Citrix Cloud で ［ワークスペース構成］**>**［アクセス］に移動し、カスタムドメインを構成します。詳しくは、「カスタムドメインの構成」を参照してください。
2. SAML プロバイダーの管理コンソールで、2 つの SAML アプリケーションを構成します。これらのアプリケーションに対して、SSO および SLO 要求に関するサインイン設定、バインドの種類、ログアウト設定などを同一に構成します。これらの SAML アプリケーションの構成が一致しない場合、ワークスペース URL とワークスペースカスタムドメインを切り替えるときに、サインインとログアウトの動作に違いが生じる可能性があります。
3. 最初の SAML アプリケーションで、次の SP エンドポイントを構成します:

   - エンティティ ID: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://saml.cloud.com/saml/acs`
   - ログアウト: `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:

4. 2 つ目の SAML アプリケーションで、次の SP エンドポイントを構成します。ワークスペースカスタムドメインは、Assertion Consumer Service およびログアウトエンドポイントにのみ使用してください。

   - エンティティ ID: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://workspaces.mycompany.com/saml/acs`

- ログアウト: `https://workspaces.mycompany.com/saml/logout/callback`

次の例は、Okta 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。**Audience Restriction** にはエンティティ ID 値が含まれることに注意してください。

5. 両方の SAML アプリケーションの SAML 署名証明書をダウンロードします。これらは後の手順で Citrix Cloud にアップロードします。
6. Citrix Cloud 管理コンソールで、SAML 接続を構成します:

   a) Citrix Cloud メニューで、[**ID** およびアクセス管理] を選択します。
   b) [認証] タブで、[**SAML 2.0**] を見つけて省略記号ボタンをクリックし、[接続] を選択します。
   c) [**SAML** の構成] ページで、手順 2 で作成した最初の SAML アプリケーションの詳細を入力します。

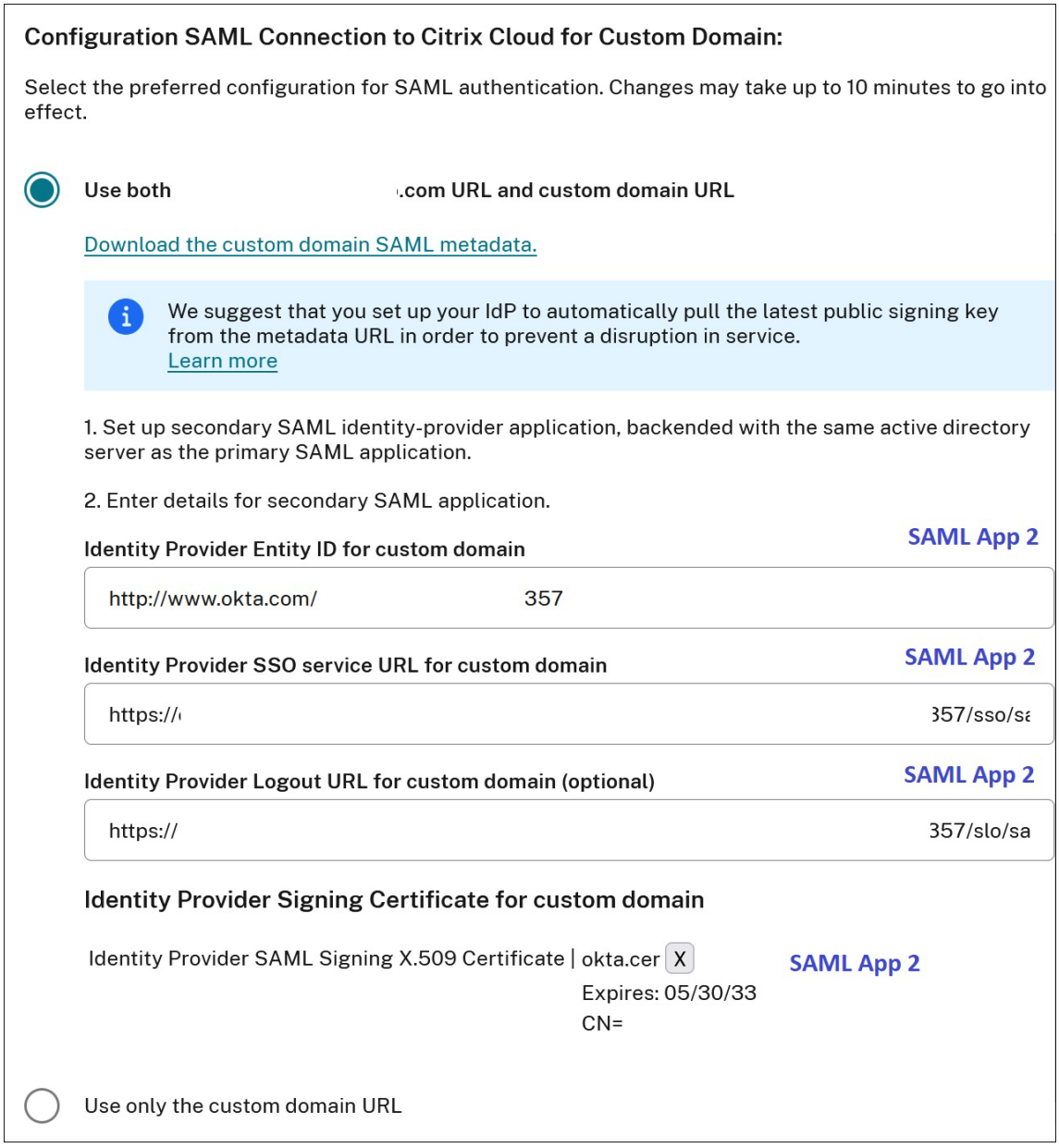
7. 新しい SAML 接続を使用するように Citrix Workspace を構成します:

   a) Citrix Cloud メニューから、[ワークスペース構成] を選択します。
   b) [認証] タブで、[**SAML 2.0**] を選択します。

8. [アクセス] タブの [カスタムワークスペース **URL**] で、[編集] を選択します。
9. [**SAML** を構成する] ページで、[**Use both customer.cloud.com URL and custom domain URL**] を選択します。
10. 次の情報を入力します:

    - [カスタムドメインの **ID** プロバイダーのエンティティ **ID**] に、手順 2 で作成した 2 つ目の SAML アプリケーションのエンティティ ID を入力します。
    - [カスタムドメインの **SSO** サービス **URL**] に、2 つ目の SAML アプリケーションからの SSO URL を入力します。
    - [カスタムドメインのログアウト **URL**] に、2 つ目の SAML アプリケーションからの SLO URL を入力します。

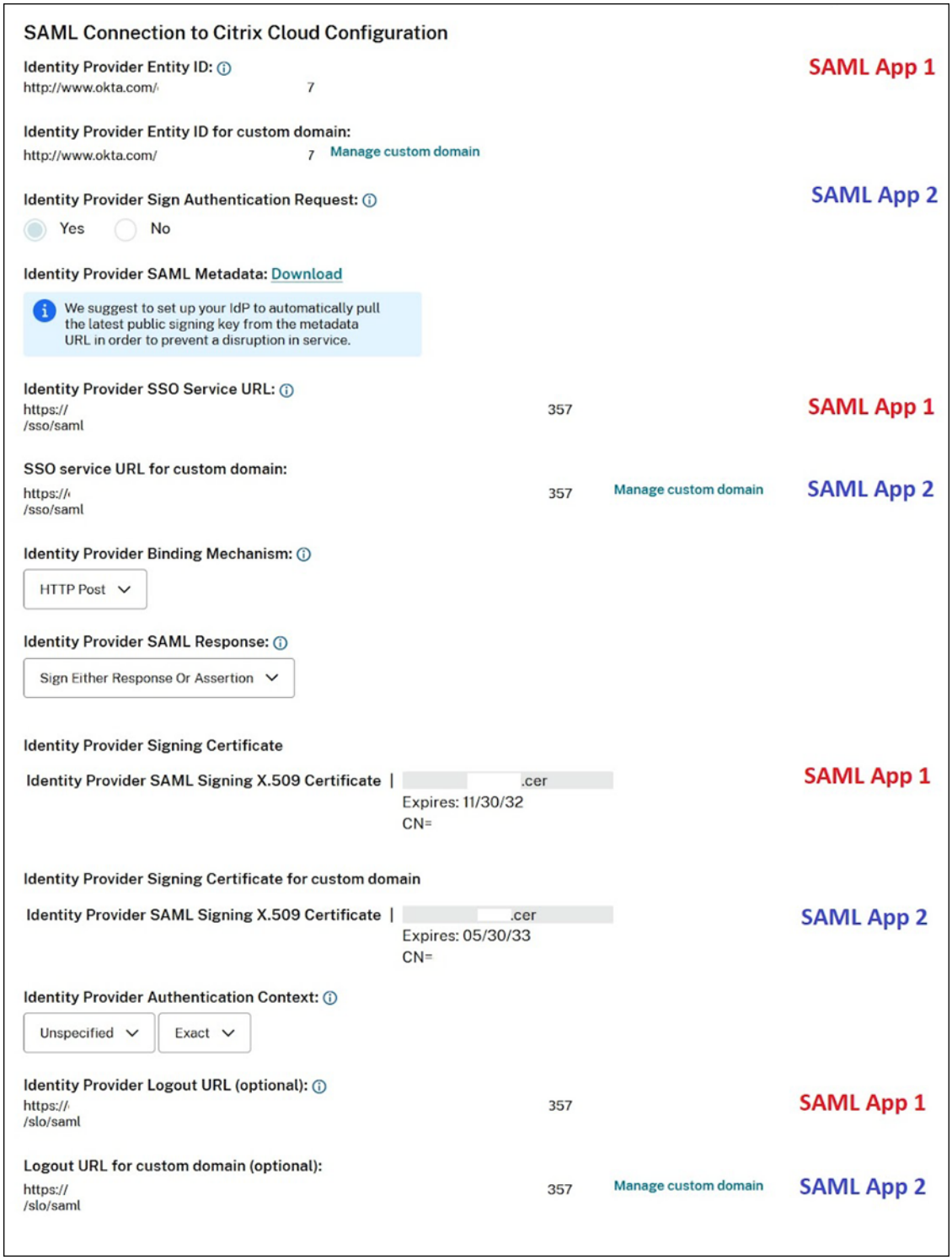
- ［カスタムドメインの **ID** プロバイダー署名証明書］で、2 つ目の SAML アプリケーションから SAML 署名証明書をアップロードします。



11. ［保存］を選択して変更内容を保存します。

SAML 接続の詳細の表示

構成後、［**ID** およびアクセス管理］**>** ［認証］に移動します。［**SAML 2.0**］で、省略記号メニューから ［**Select SAML Provider**］**>** ［**View**］を選択します。SAML の構成ページには、エンティティ ID、SSO URL、およびログアウト URL に対して構成された SAML エンドポイントのペアが表示されます。



他のすべての SAML 構成設定は、作成した 1 つ目と 2 つ目の SAML アプリケーションの両方に適用されます。

Citrix Workspace へのサインインを確認

構成したサインインおよびログアウトの動作を確認するには、次のテストを実行します:

- ワークスペース URL（`https://mycompany.cloud.com`）と SAML プロバイダーを使用して Citrix Workspace にサインインします。
- ワークスペースカスタムドメイン（`https://workspace.mycompany.com`）と SAML プロバイダーを使用して Citrix Workspace にサインインします。
- 一意のサインイン URL（`https://citrix.cloud.com/go/mycompany`）と SAML プロバイダーを使用して Citrix Cloud にサインインします。

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

March 11, 2024

Author:
Mark Dear

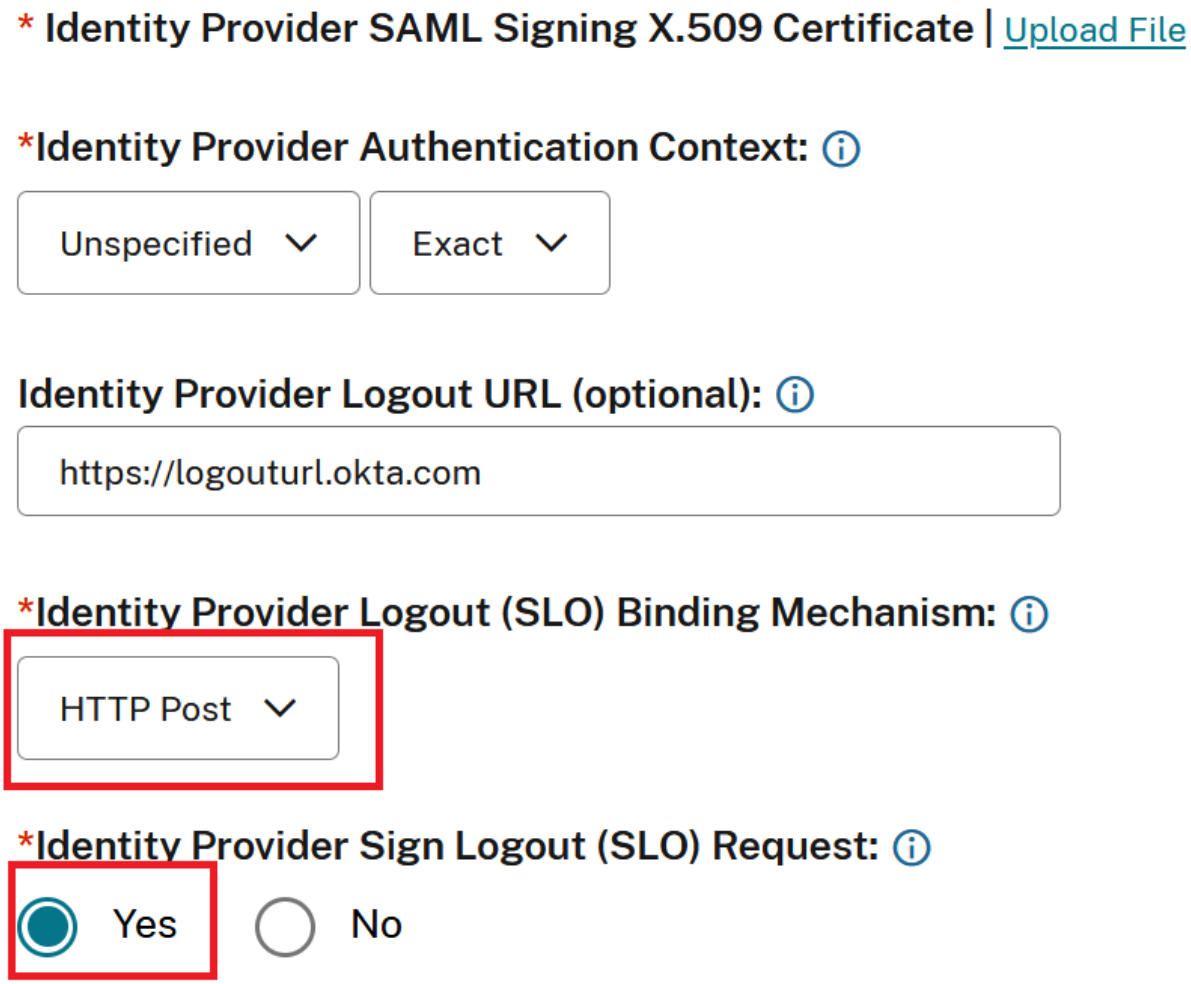
この記事では、Citrix Cloud と SAML プロバイダー間で Okta SAML アプリケーションおよび接続を構成するために必要な手順について説明します。いくつかの手順では、SAML プロバイダーの管理コンソールで実行するアクションについて説明します。

前提条件

この記事のタスクを完了する前に、次の前提条件を満たしていることを確認してください:

- Citrix サポートが、Citrix Cloud で **SendNameIDPolicyInSAMLRequest** 機能を有効にしている。この機能はリクエストに応じて有効になります。これらの機能について詳しくは、「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。
- 次の Okta ドメインのいずれかを使用する Okta Organization がある:
  - okta.com
  - okta-eu.com
  - oktapreview.com
- Active Directory（AD）を Okta Organization と同期している。
- Okta Organization で ［認証要求に署名する］が有効になってる。
- **ID** プロバイダーのシングルログアウト（**SLO**）が、Citrix Cloud と Okta SAML アプリケーションの両方内で構成されている。SLO が構成され、エンドユーザーが Citrix Workspace 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。

- **ID** プロバイダーのサインログアウト **(SLO)** リクエストが、Citrix Cloud 内で有効になっている。
- **ID** プロバイダーのログアウトバインディング（**SLO**）が、Citrix Cloud 内の HTTPPost である。



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 サポートに問い合わせて、**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 要求で **NameID** ポリシーを **Unspecified** として SAML プロバイダーに提供できるようになります。この機能は、Okta でのみ使用可能です。

これらの機能をリクエストするには、Citrix アカウントにサインインし、Citrix サポート Web サイトからチケットを開きます。

要件

この記事には、Okta 管理コンソールで 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 リージョンの SAML 署名証明書が必要です。

> 重要:
>
> 署名証明書は PEM 形式でエンコードする必要があります。Citrix Cloud は、他のエンコーディング形式での署名証明書を受け入れません。

この証明書は、次の場所にある抽出ツールを使用して、リージョンの Citrix Cloud SAML メタデータから抽出できます。https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract。必要なときに提供できるように、事前に Citrix Cloud SAML 証明書を取得しておくことをお勧めします。

このセクションの手順では、次の場所にある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。https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract。

リージョンの Citrix Cloud メタデータを取得するには、以下の手順を実行します:

1. 選択した抽出ツールに、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の各リージョンの場合は、「`https://saml.cloud.com/saml/metadata`」と入力します。
   - 日本リージョンの場合は「`https://saml.citrixcloud.jp/saml/metadata`」と入力します。
   - Citrix Cloud Government リージョンの場合は、「`https://saml.cloud.us/saml/metadata`」と入力します。
2. [**Load**] をクリックします。抽出された証明書が、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 エージェントでアカウントを同期

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 Active Directory と Okta を統合する必要があります。そのためには、ドメイン内に Okta AD エージェントをインストールし、Okta Organization に Active Directory を追加します。Okta Active Directory エージェントを展開するためのガイダンスについては、Okta Web サイトで「Get started with Active Directory integration（Active Directory の統合を開始する）」を参照してください。

その後、Active Directory ユーザーおよびグループを Okta にインポートします。インポート時には、Active Directory アカウントに関連付けられている以下の値を含めます:

- メール
- SID
- UPN
- OID

Active Directory ユーザーおよびグループを Okta Organization と同期するには:

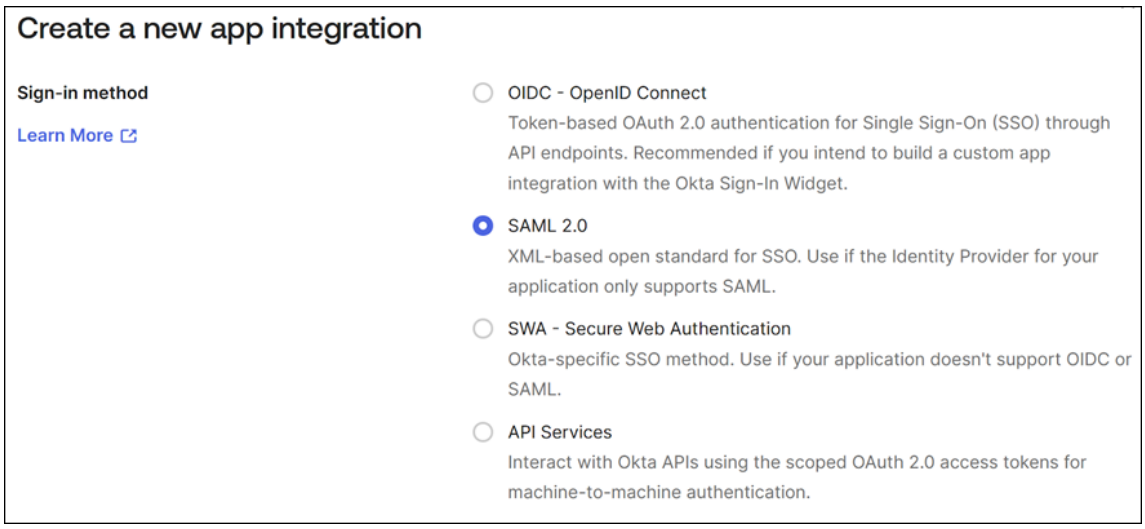
1. Okta Active Directory エージェントをインストールして構成します。詳しい手順については、Okta Web サイトの次の記事を参照してください:

   - Install the Okta Active Directory agent（Okta Active Directory エージェントのインストール）
   - Configure Active Directory import and account settings（Active Directory のインポートとアカウント設定の構成）
   - Configure Active Directory provisioning settings（Active Directory プロビジョニング設定の構成）

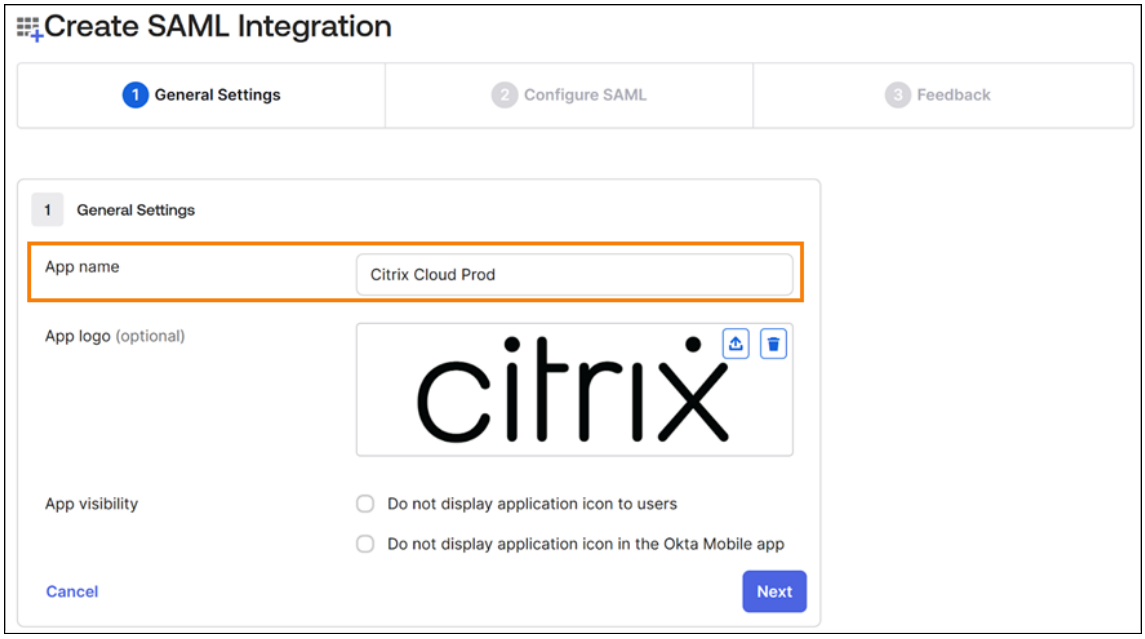
2. 手動インポートまたは自動インポートを実行して、Active Directory ユーザーおよびグループを Okta に追加します。Okta のインポート方法と手順について詳しくは、Okta Web サイトで「Manage Active Directory users and groups（Active Directory ユーザーとグループの管理）」を参照してください。

Okta SAML アプリケーションをワークスペース認証用で構成する

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 Organization 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、[**SAML 2.0**] を選択します。[次へ] を選択します。



3. [**App Name**] にアプリケーションのフレンドリ名を入力します。[次へ] を選択します。



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 の顧客の Citrix Cloud リージョンに対応する URL を入力します:

   - 顧客 ID が欧州連合、米国、およびアジア太平洋南部の各リージョンの場合は、「`https://saml.cloud.com/saml/acs`」と入力します。
   - 顧客 ID が日本リージョンの場合は、「`https://saml.citrixcloud.jp/saml/acs`」を入力します。
   - 顧客 ID が Citrix Cloud Government リージョンの場合は、「`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。

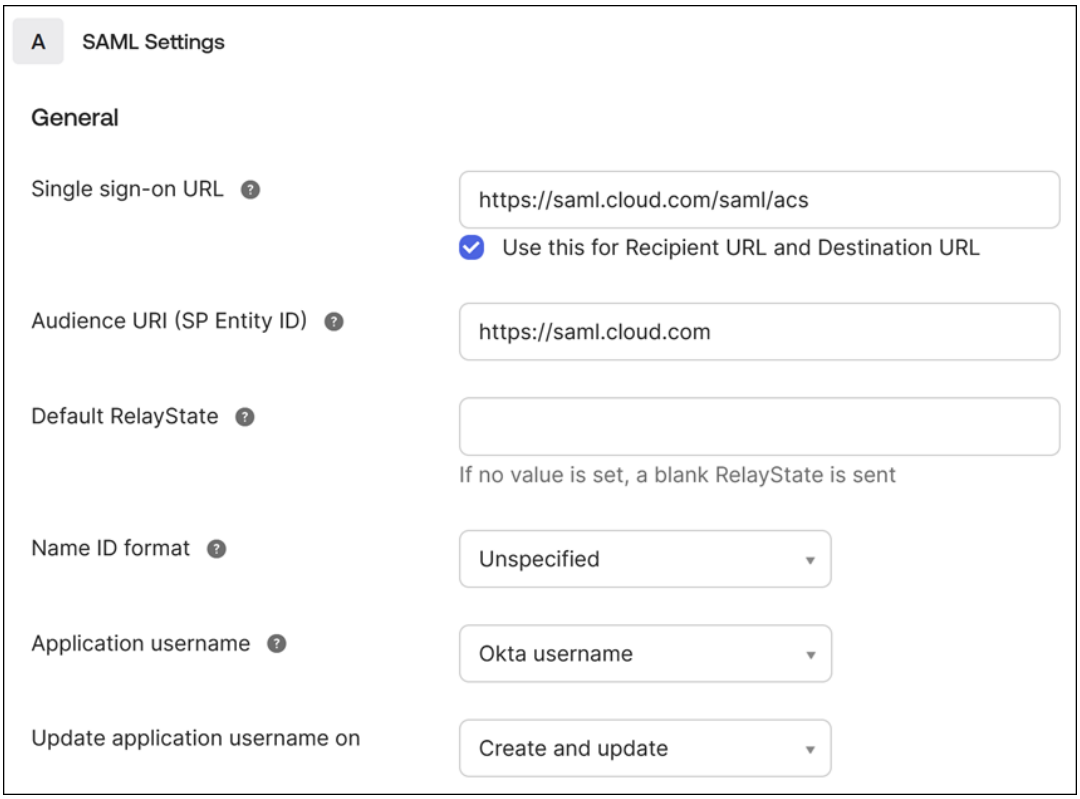
   c) [**Audience URI**（**SP Entity ID**）] に、Citrix Cloud の顧客の Citrix Cloud リージョンに対応する URL を入力します:

   - 顧客 ID が欧州連合、米国、およびアジア太平洋南部の各リージョンの場合は、「`https://saml.cloud.com`」と入力します。
   - 顧客 ID が日本リージョンの場合は、「`https://saml.citrixcloud.jp`」を入力します。
   - 顧客 ID が Citrix Cloud Government リージョンの場合は、「`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 要求内で送信する 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、[認証要求に署名する] を有効にすると、Okta でエラーが発生します。

e) [**Application username**] で [**Okta username**] を選択します。

次の図は、この構成の例として、米国、EU、およびアジア太平洋南部リージョンの正しい構成を示しています:



> 重要:
>
> [**Name ID**] 設定は、[**Unspecified**] で構成される必要があります。この設定に別の値を使用すると、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:

- [**Reponse**] 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 署名証明書を取得する手順については、この記事の「要件」を参照してください。

h) [**Enable Single Logout**] で [**Allow application to initiate Single Logout**] を選択します。

i) [**Single sign-on URL**] に、Citrix Cloud リージョンに対応する URL を入力します:

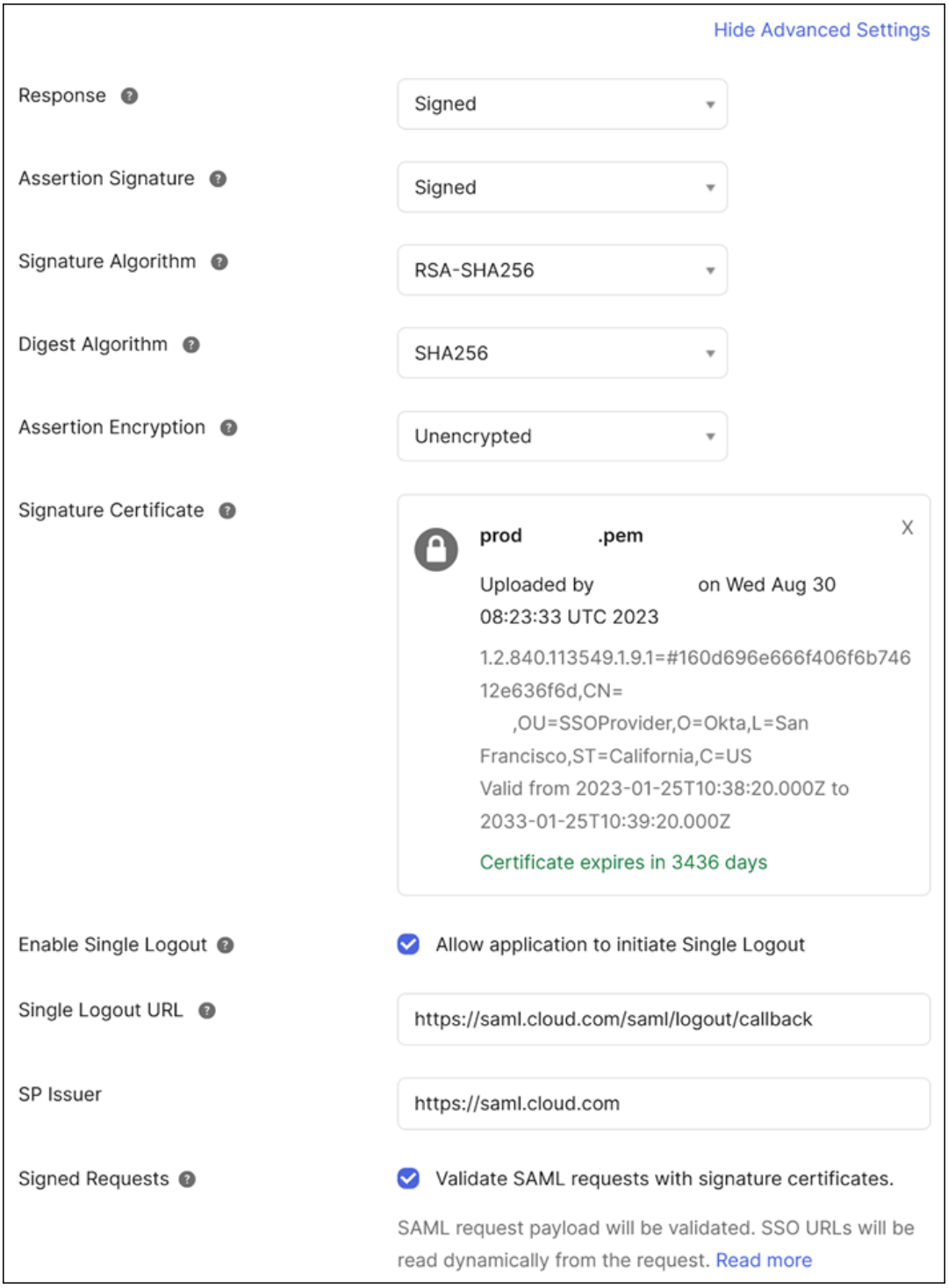
- 欧州連合、米国、およびアジア太平洋南部の各リージョンの場合は、「`https://saml.cloud.com/saml/logout/callback`」と入力します。

- 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 リージョンの場合は、「https://saml.cloud.us/saml/logout/callback」と入力します。

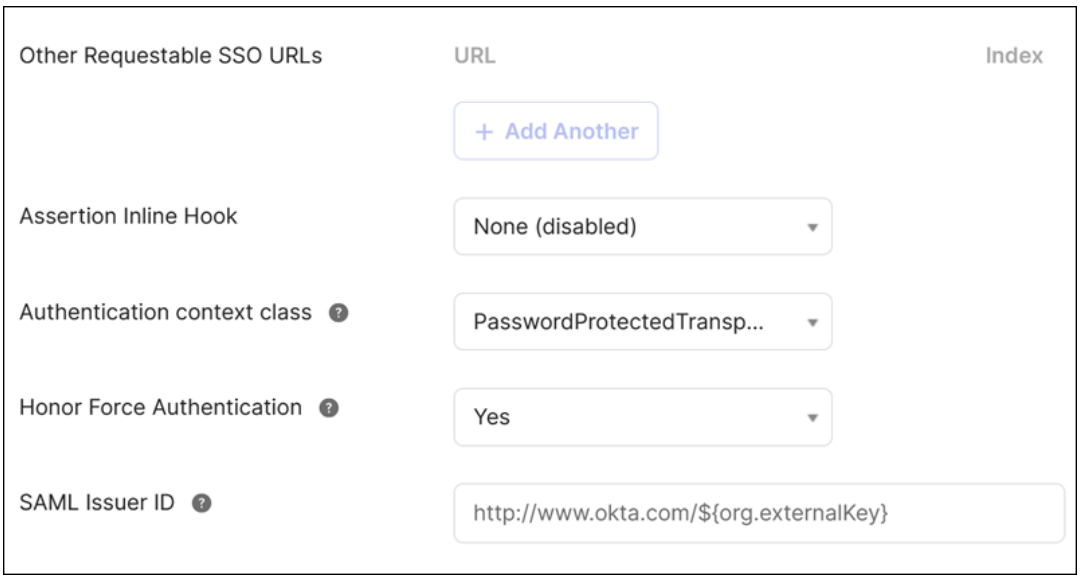
j) [**SP Issuer**] で、[**Audience URI**（**SP Entity ID**）に上記の手順（このタスクの手順 4c）で入力した値を入力します。

k) [**Signed Requests**] で [**Validate SAML requests with signature certificates**] を選択します。

次の図は、米国、EU、およびアジア太平洋南部リージョンの正しい構成を示しています：

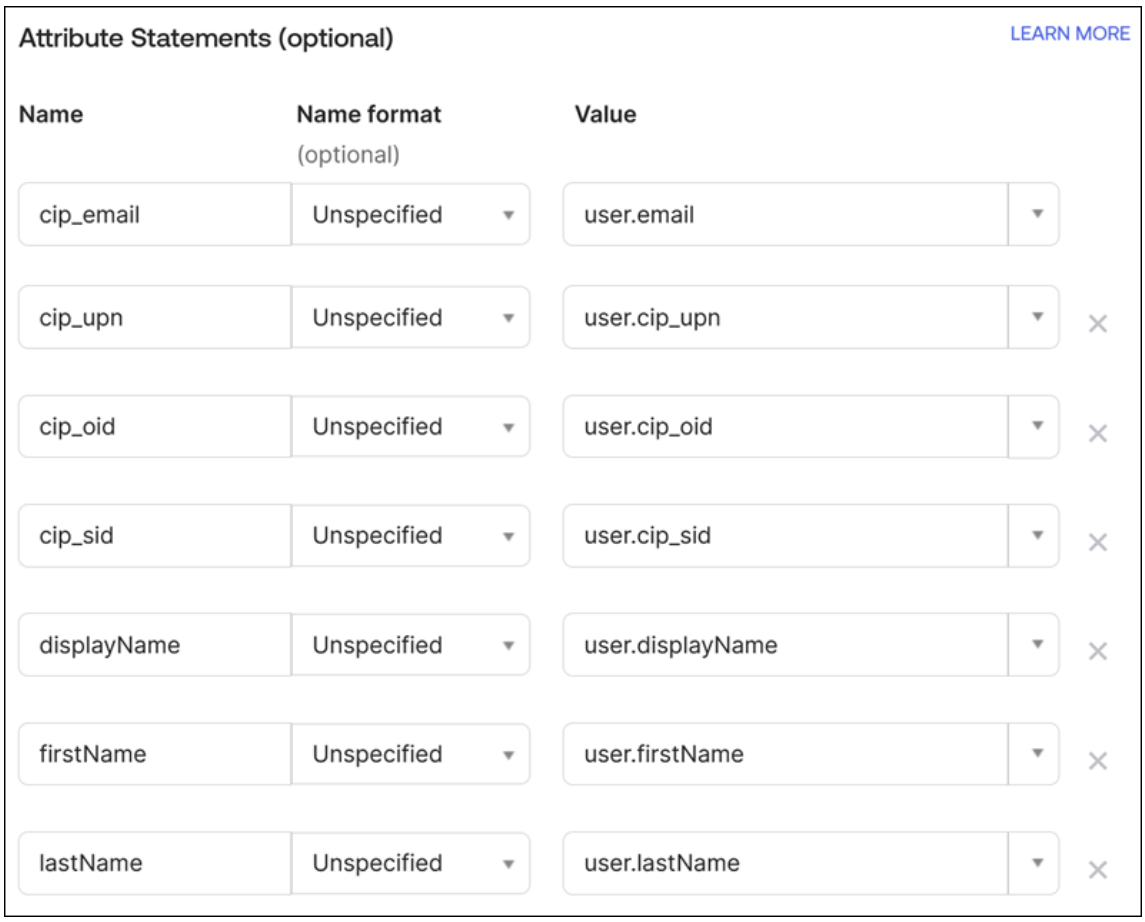


l) 残りのすべての詳細設定については、デフォルト値を使用します。

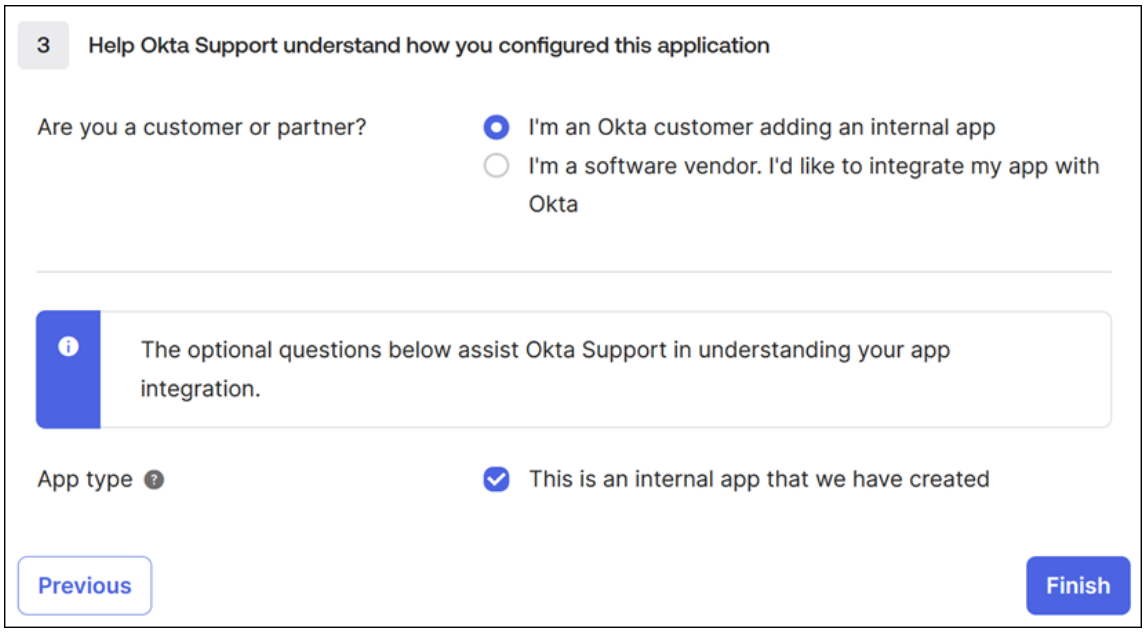


5. [**Attribute Statements （optional**)] で、[**Name**]、[**Name format**]、[**Value**] に次の表の値を入力します:

名前	Name format	値
cip_email	Unspecified	user.email
cip_upn	Unspecified	user.cip_upn
cip_oid	Unspecified	user.cip_oid
cip_sid	Unspecified	user.cip_sid
displayName	Unspecified	user.displayName
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName



6. ［次へ］を選択します。Okta の構成ステートメントが表示されます。



7. ［**Are you a customer or partner?**］で ［**I’m an Okta customer adding an internal app**］を選択します。

8. [**App type**] で [**This is an internal app that we have created**] 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。

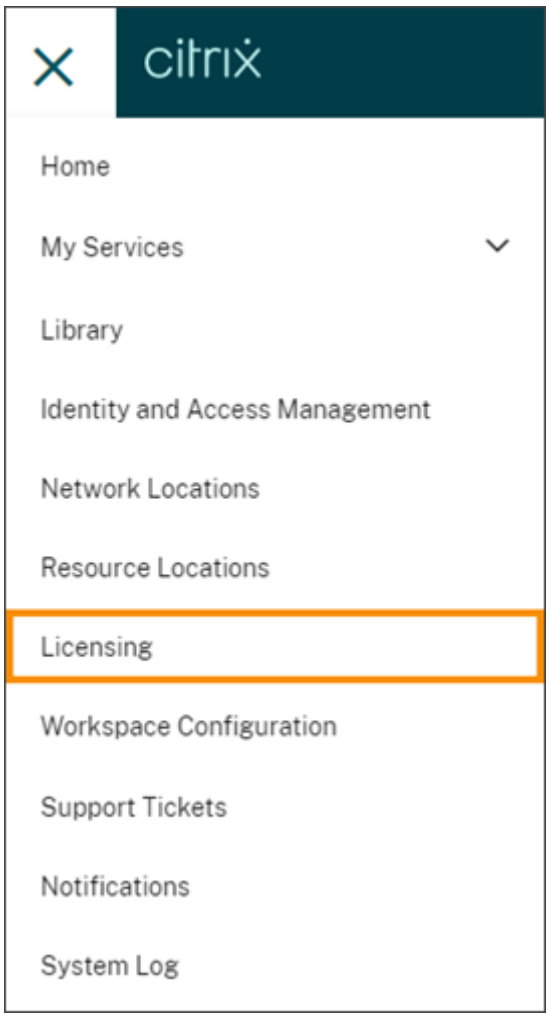
Citrix Cloud 用のライセンス

October 4, 2023

Citrix Cloud では、特定のクラウドサービスのライセンスと使用状況を監視できます。Citrix ライセンスサーバーが Citrix Cloud に登録されているオンプレミス環境でも、ライセンスと使用状況を監視できます。

企業顧客向けライセンス

法人顧客は、Citrix Cloud メニューの [ライセンス] 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。



クラウドサービスの企業ライセンスと使用状況の監視について詳しくは、「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」を参照してください。

オンプレミス環境用のライセンス

オンプレミス環境で Citrix Virtual Apps and Desktops を使用している法人顧客は、Citrix Cloud を使用して、ユーザー/デバイスモデルと同時使用ライセンスモデルの両方のライセンスと使用状況を常に監視できます。Citrix ライセンスサーバーを Citrix Cloud に登録することにより、顧客は Citrix Cloud の ［ライセンス割り当て済みの展開］ページで次のタスクを実行できます:

- 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環境のライセンス割り当てと使用状況を表示する
- 同時使用ライセンスモデルを使用する環境のピーク時のライセンス使用状況を表示する

オンプレミス Virtual Apps and Desktops 環境のライセンスおよび使用状況の監視について詳しくは、「オンプレミス展開のライセンスと使用状況の監視」を参照してください。

Citrix Service Provider（CSP）用のライセンス

Citrix Service Provider では、次のツールを使用することで、製品ライセンスと使用状況を把握し、レポートを作成することができます:

- License Usage Insights は、シングルテナントおよびマルチテナントの顧客間で製品の使用状況情報を収集および集約する Citrix Cloud の無料サービスです。詳しくは、「Citrix Service Provider 用のライセンス」を参照してください。
- Citrix Cloud のライセンス機能により、CSP の顧客は、サポートされている Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）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。詳しくは、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
  - Citrix DaaS Standard for Azure の顧客ライセンスと使用状況の監視

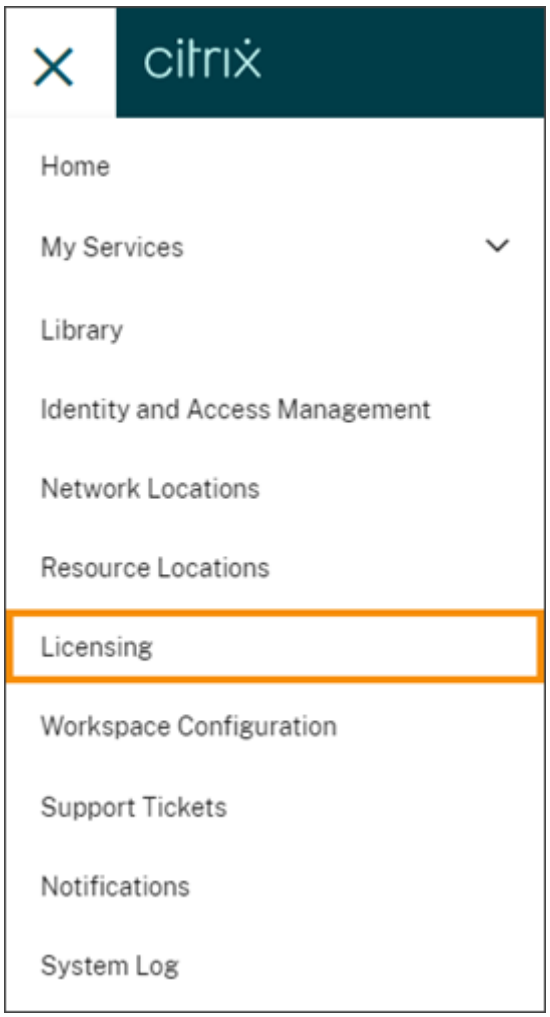
クラウドサービスのライセンスおよびアクティブな使用状況の監視

October 4, 2023

Citrix Cloud のライセンス機能により、購入したクラウドサービスのライセンス消費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すると、次のことが実行できます:

- ライセンスの可用性と割り当てを一目で把握する
- 関連するクラウドサービスの日次および月次のアクティブな使用状況の傾向を表示する
- 個別のライセンス割り当ての詳細と使用傾向をドリルダウンして確認する
- 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で ［ライセンス］を選択します。



注:

この記事では、サポートされているすべての Citrix Cloud サービスに共通のライセンス機能について説明します。ライセンスのいくつかの要素は、サービスによって異なる場合があります（ライセンスの割り当てなど）。各サービスのライセンスと使用状況について詳しくは、以下の記事を参照してください:

- 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）
- Citrix DaaS および Citrix DaaS Standard for Azure のライセンスとピーク時の使用状況の監視（同時使用）
- Citrix DaaS Standard for Azure のライセンスとアクティブな使用状況の監視（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の監視
- Gateway サービスの帯域幅使用量の監視
- Secure Workspace Access のライセンスと使用状況の監視

サポートされているリージョンとクラウドサービス

ライセンス機能は、米国、EU、南アジア太平洋リージョンでサポートされているサービスでのみ利用できます。

ライセンス機能は次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/デバイスと同時使用のライセンスモデル）- 旧称 Citrix Virtual Apps and Desktops サービス
- Citrix DaaS Standard for Azure（ユーザー/デバイスライセンスモデル）- 旧称 Citrix Virtual Apps and Desktops Standard for Azure
- Endpoint Management
- Gateway
- Secure Private Access（旧称 Secure Workspace Access）

Citrix DaaS のマルチタイプライセンス

Citrix Cloud のライセンスは、Citrix DaaS のマルチタイプライセンスをサポートしています。ユーザー/デバイスと同時使用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 ではライセンス使用状況がライセンスコンソールページの各ライセンスモードの下に表示されます。

ライセンスページを確認する前に、サイトレベルとデリバリーグループレベルで、マルチタイプの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場合があります。手順については、Citrix DaaS のドキュメントの「マルチタイプのライセンス」を参照してください。

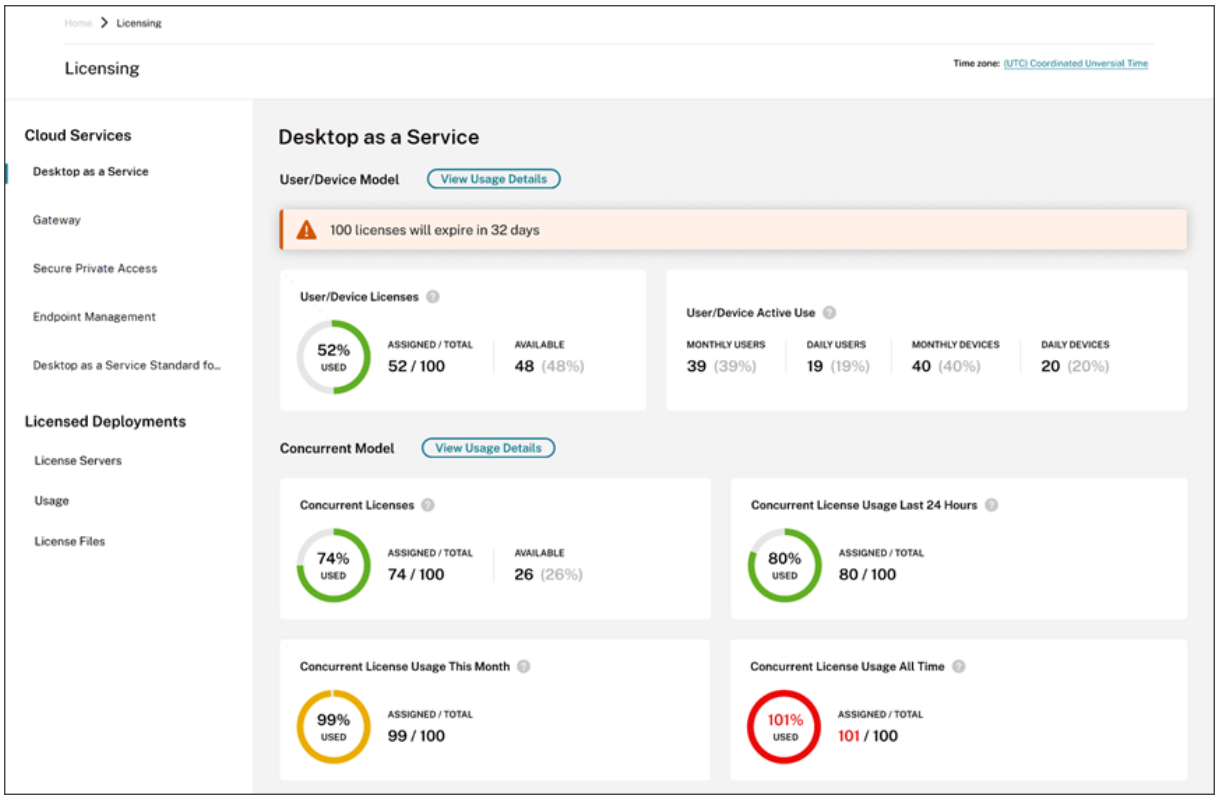
Web Studio または PowerShell のセットアップ方法を正常に使用した後、ライセンスコンソールページに正しいマルチタイプのライセンスの使用法が表示されない場合は、次のオプションがあります:

- 30 日経ってから、未使用のライセンスを解放する。
- Citrix カスタマーサービスに連絡する。

ライセンス割り当て

一般に、ユーザーには、クラウドサービスの最初の使用時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異なる方法でライセンスを割り当てる場合があります。各サービスのライセンスの割り当て方法について詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

ライセンスの概要と詳細



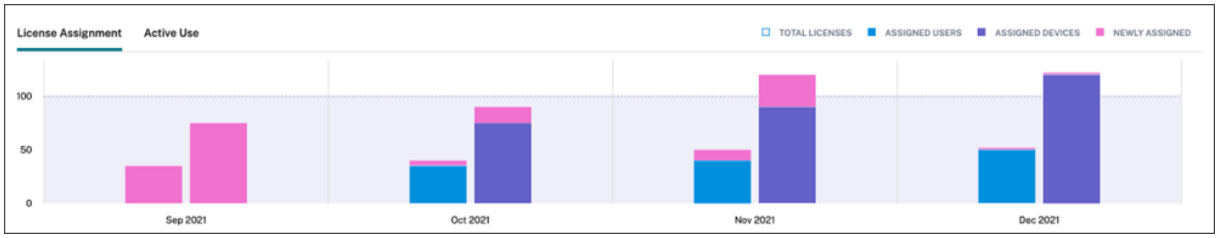
ライセンスの概要では、サポートされている各サービスに関する次の情報を一目で確認できます:

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 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 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詳しくは、この記事の上部で参照されているライセンスの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、［使用状況の詳細の表示］をクリックします。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ユーザーの内訳を確認できます。



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。使用状況の傾向とライセンスアクティビティについて詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

割り当て済みライセンスを解放する

一般に、割り当て済みライセンスは、ユーザーがクラウドサービスを 30 日間連続して使用していない場合、解放対象となります。ライセンスが解放されると、それに応じて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減少します。

一部のサービスでは、使用するライセンスモデルによって、ライセンスの解放が異なる場合があります。各サービスのライセンスの解放について詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

よくある質問

- 割り当てられたライセンス数が購入したライセンス数を超えた場合、クラウドサービスの使用が停止されますか**?** いいえ。購入済みクラウドライセンスの使用数を超過した場合でも、サービスは停止されません。［ライセンス使用状況］ではクラウドライセンスの使用数を把握するための情報が提供されるため、お客様はライセンスの割り当てを監視し、購入したライセンス数内でサービスを使用されることを期待されます。ライセンス数を超えてサービスを使用することが判明した場合、営業担当者にご連絡いただき、ライセンス要件の見直しについてご相談いただくようお願いします。
- どのようなライセンス情報がキャプチャされていますか**?** 現在、ユーザーログインに関連するライセンス情報のみがキャプチャされます。
- マルチタイプのライセンスは **Citrix DaaS** でサポートされていますか**?**（ユーザー**/**デバイスモデルおよび同時使用モデル両方の使用など）はい。詳しくは、本記事の「マルチタイプのライセンス」を参照してください。
- マルチエディションのライセンスは **Citrix DaaS** でサポートされていますか**?** たとえば、同一の **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、そのユースケースはサポートされていません。1 つの Citrix DaaS サイトには、1 つのエディションのライセンスのみが付与されます。同じ Citrix Cloud アカウントで複数の Citrix DaaS インスタンスを使用する場合は、それらが同じエディションである必要があります。
- 監視レポート（**Director** 内）と同時使用ライセンスの分析情報の違いは何ですか**?** 監視レポートと同時使用セッションの説明では、使用中の同時ライセンスの測定値とは異なる解釈と測定基準が提供されます。ほとんどの場合、Director 内の同時使用セッション数を、使用中のピーク時の同時使用ライセンスの表現または予測として使用すると、必要な同時使用ライセンスの数が多くなりすぎてしまいます。同時使用ライセンスの使

用状況レポートの代わりに、Director の監視レポートを使用しないでください。レポートツールの主な違いは次の 2 つです:

  - サンプリング時間の長さ：ライセンスには 5 分のサンプリング時間があります。Citrix Cloud は 5 分ごとに、現在サービスに接続されている固有のデバイスをカウントします。5 分のすべてのサンプリング期間が集計され、24 時間、毎月、および契約期間のピーク時の使用量が割り出されます。Director の監視レポートでは、レポートの実行方法に応じて、最大 2 時間の間隔を表示できます。
  - 一意性：ライセンスは、セッションが開始されたときにデバイス間の一意性を確認します。監視レポートでは、一意のデバイスかどうかは考慮されません。

- * 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、自分が所属する組織のドメイン名を変更した場合）、使用中の自分のライセンスが同じユーザーに対して *2* 回カウントされるのはなぜですか? - Citrix Cloud が一意のユーザーをカウントするのにユーザープリンシパル名（user principle name: UPN）を使用するからです。移行が発生する前後にユーザーがクラウドサービスにアクセスした場合、Citrix Cloud は、異なるドメイン名を持つ各ユーザーの一意の UPN を 2 つキャプチャします。そのため、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ければ、その古いライセンス割り当てを 30 日後に解放できます。購入済みクラウドライセンスの使用数を超過した場合でも、サービスは停止されません。
- * 同じユーザーまたはデバイスのライセンスが重複しているように見えるのはなぜですか?- これは、HTML5 向け 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 向け Workspace アプリで起動すると、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 アプリで起動すると、ユーザー/デバイスライセンスを消費します。そのため、ユーザーが HTML5 向け Workspace アプリでアプリを起動し、後でローカルにインストールされたバージョンの Workspace アプリで起動した場合、Citrix Cloud はユーザーが 2 つのライセンスを消費したものとして表示します。この動作はユーザーの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の利用状況レポートの数値が増大することがあります。購入済みクラウドライセンスの使用数を超過した場合でも、サービスは停止されません。

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）

November 9, 2023

この記事では、Citrix Cloud のライセンスコンソールを使用して、クラウドサービスライセンスの割り当てを管理し、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。

ご使用のサービス環境で使用する Citrix Azure Consumption Fund を購入した場合、詳しくは「Citrix DaaS の Citrix Managed Azure リソースの消費の監視」を参照してください。

ライセンス割り当て

Citrix Cloud では、一意のユーザーまたはデバイスによるアプリまたはデスクトップの初回起動時にライセンスが割り当てられます。

ドメイン名の切り捨て

複数のドメインをホストし、それらのドメイン内に互いに似たアカウントを持つ複数のユーザーがいる場合（たとえば、johnsmith@company.comと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（たとえば、johnsmith）のみを考慮させるように許可することができます。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ると、Citrix Cloud による一意ユーザーのカウント方法が変わります。Citrix Cloud が、johnsmith@company.comとjohnsmith@mycompany.comを 2 人の一意ユーザーとしてカウントするのではなく、johnsmith のみを一意ユーザーとしてカウントするようになります。このカウント方法の変更は、次のライセンスデータに影響します。

- ライセンス割り当て
- アクティブな使用
- ライセンスの経時的な使用傾向
- 解放対象のライセンス

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のデータをエクスポートした CSV ファイルにも反映されます。

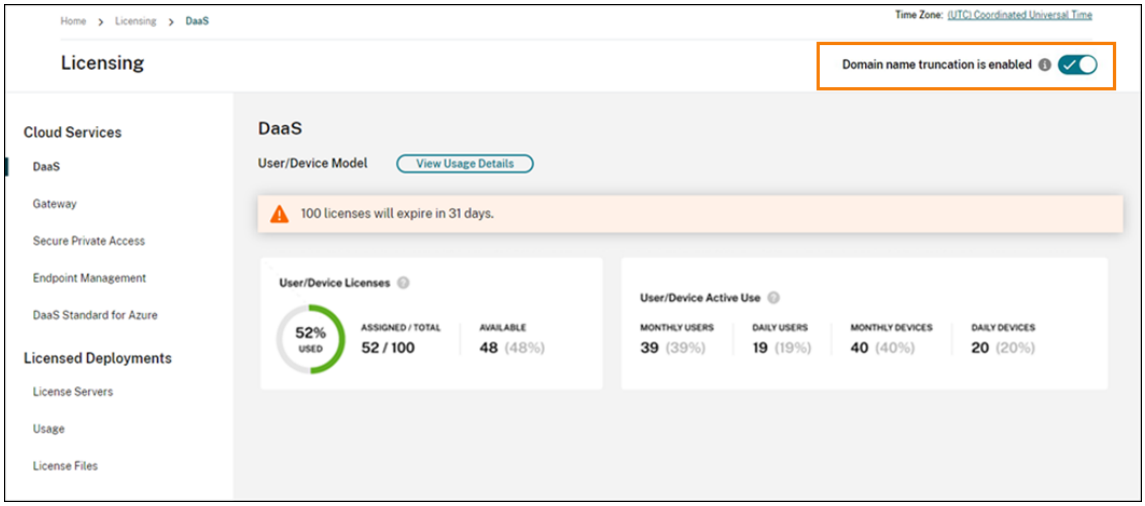
> 注:
>
> ユーザー名がわずかに異なる類似のアカウントが参加している複数のドメインをホストしている場合（たとえば、参加ユーザーのアカウントがjohnsmith@company.comとjsmith@newcompany.com）、ドメイン名の切り捨てを行っても、Citrix Cloud のユーザーカウント結果には影響しません。johnsmith と jsmith は、同じ個人のアカウントである場合でも、Citrix Cloud ではそれぞれ一意ユーザーとして引き続きカウントされます。

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/デバイス利用状況データに影響します。たとえば、特定の月にドメイン名の切り捨てを有効にすると、その月に Citrix Cloud が記録するデータが影響を受けます。ただし、この機能が無効になっていた前月の履歴データは以前のまま影響を受けません。同様に、特定の月にドメイン名の切り捨てを無効にすると、その月に Citrix Cloud が記録するデータが影響を受けます。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。

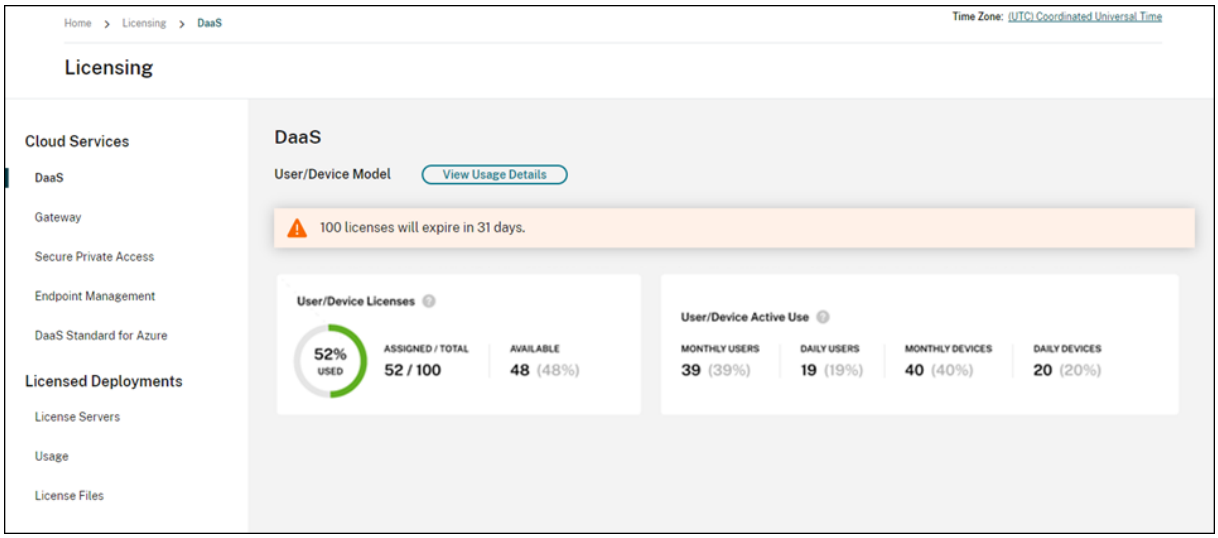
ドメイン名の切り捨てを有効または無効にするには:

1. ライセンスコンソールの右上近くにあるトグルをクリックします。



2. アクションの確認を求められたら、［はい。了承しています］を選択します。

ライセンスの概要



ライセンスの概要では、次の情報を一目で確認できます:

- 割り当てられた購入済みライセンスの合計パーセンテージ。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。

  購入した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 エディションのために購入したライセンスの合計です。

- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。

- 月次および日次のアクティブな使用状況の統計:
  - 月次のアクティブな使用状況とは、過去 30 日間にサービスを使用した一意のユーザーまたはデバイスの数を指します。
  - 日次のアクティブな使用状況とは、過去 24 時間以内にサービスを使用した一意の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 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が正確に反映されるよう、Citrix Cloud ではサービスを使用した一意のユーザー数とデバイス数がカウントされます。Citrix Cloud は、割り当て済みライセンスを計算するために、これらのうち少ない方の数を使用します。Citrix Cloud は、アクティブな使用状況を計算するために、特定の期間のアクティブなユーザーとアクティブなデバイスの数として、各カウントを使用します。

割り当て済みライセンスの計算例

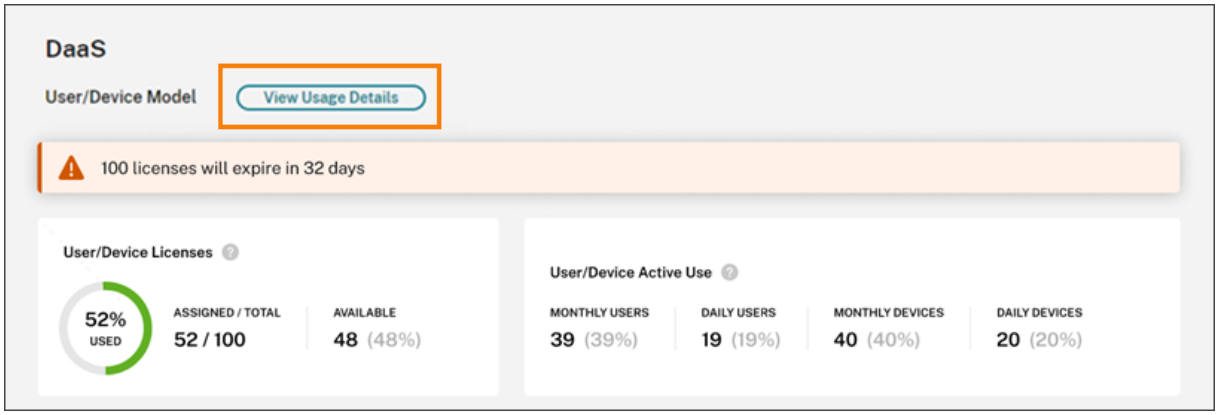
サービスを使用している一意のユーザー数が 100、一意のデバイス数が 50 の場合、Citrix Cloud では少ない方の数（50）を使用して割り当て済みライセンスの数を判断します。使用されているライセンスの割合と使用可能なライセンスの数は、割り当てられた 50 のライセンスに基づきます。

アクティブな使用状況の計算例

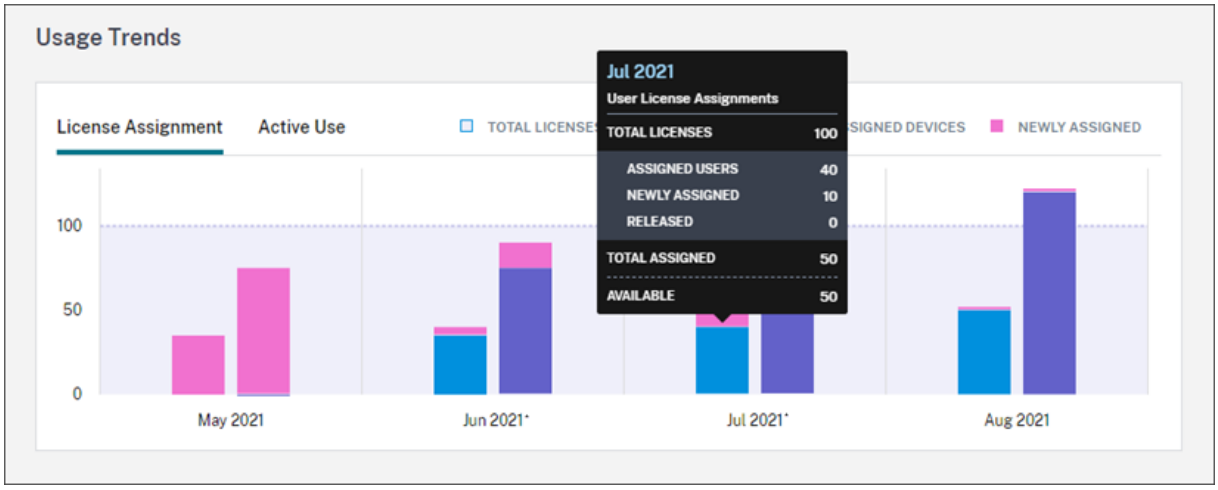
過去 30 日間に 10 人の一意のユーザーと 20 人の一意のデバイスがサービスを使用した場合、Citrix Cloud は、月次のアクティブな使用状況が 10 人のアクティブなユーザーと 20 人のアクティブなデバイスで構成されていると判断します。同様に、過去 24 時間以内に 30 人の一意のユーザーと 15 人の一意のデバイスがカウントされた場合、Citrix Cloud は、日次のアクティブな使用状況が 30 人のアクティブなユーザーと 15 人のアクティブなデバイスで構成されていると判断します。

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 ［使用状況の詳細の表示］をクリックします。使用傾向と、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。



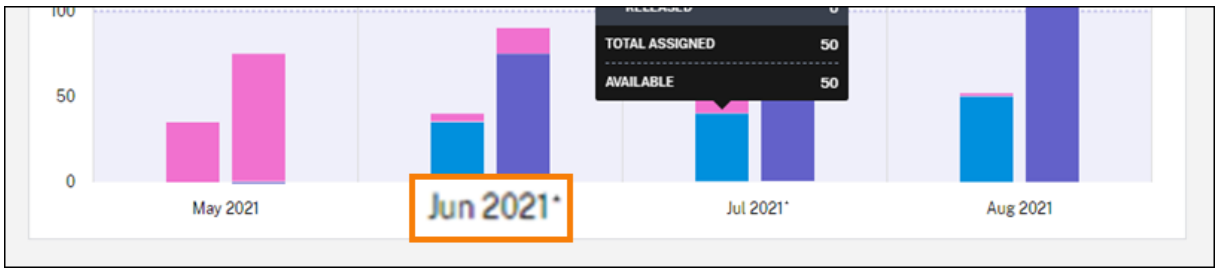
[使用状況の傾向] セクションでは、この内訳がグラフで表示されます。



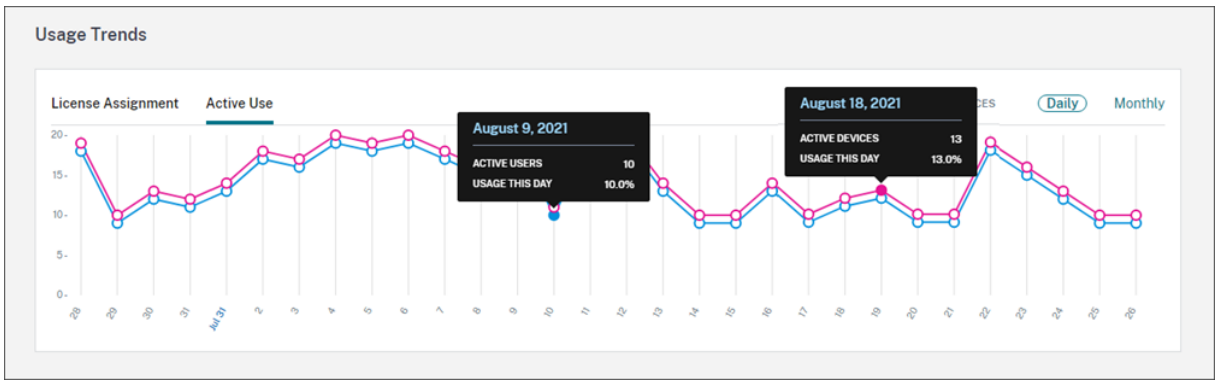
[ライセンス割り当て] グラフで、特定の月または日のバーをポイントすると、次の情報が表示されます:

- ライセンス合計: 合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 割り当てられたユーザー: 今月までにユーザーに割り当てられたライセンスの累積数。
- 割り当てられたデバイス: 今月までにデバイスに割り当てられたライセンスの累積数。特定の月にこの数が特に多いと思われる場合、アプリまたはデスクトップが Web ブラウザーを介して起動していることが原因である可能性があります。この数を減らすには、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。
- 新しく割り当て済み: 各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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 [新しく割り当て済み] 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の対象であり、7 月に 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 個です。

ドメインの切り捨てを有効にした期間にはアスタリスクが付いています。



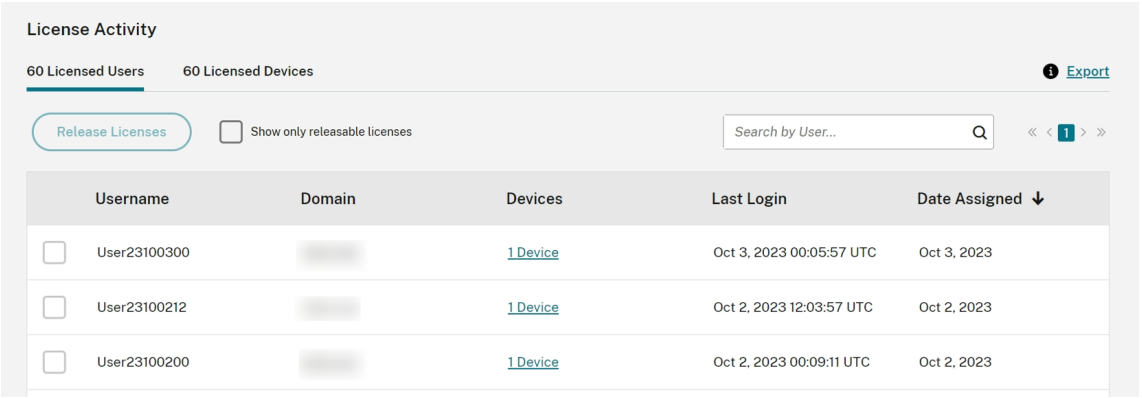
［アクティブな使用］グラフで、前の暦月と暦年の、アクティブなユーザーとデバイスをそれぞれ表示できます。グラフ上の特定の期間をポイントすると、アクティブなユーザーまたはデバイスの数と使用率が表示されます。



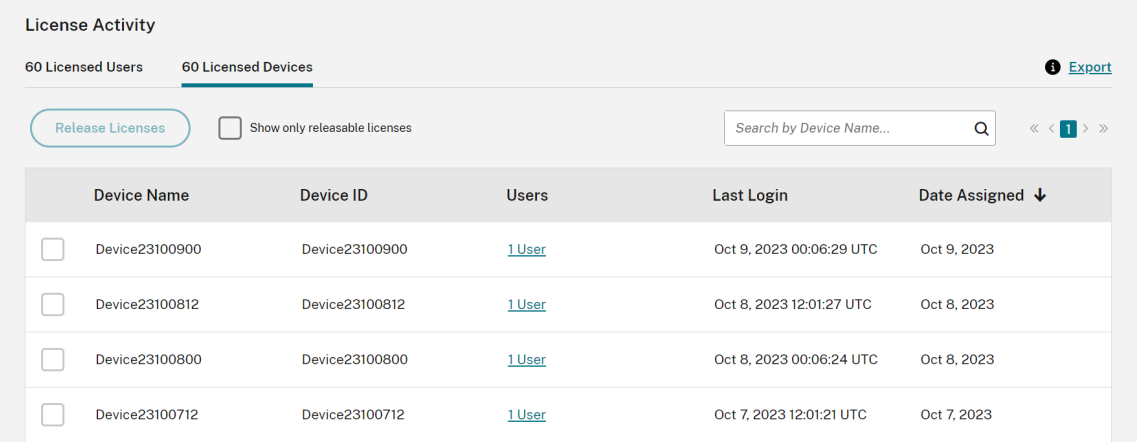
ライセンスアクティビティ

［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：

- 関連するデバイスを含む、ライセンスを割り当てた個々のユーザーのリスト。



- 関連するユーザーを含む、ライセンスを割り当てたデバイスのリスト。



- ライセンスがユーザーまたはデバイスに割り当てられた日付。

一覧をフィルタリングして、解放対象のライセンスのみを表示することもできます。本記事の「割り当て済みライセンスを解放するには」を参照してください。

割り当て済みライセンスを解放する

ライセンスが割り当てられる場合、割り当て期間はサービスへの接続が確立されてから 90 日間です。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みなされ、90 日後に Citrix Cloud によって解放されます。このプロセスは自動化されており、管理者による操作は必要ありません。

割り当て期間（90 日）が経過した場合、管理者は次のシナリオでのみライセンスを手動で解放できます：

- 会社への関連付けがなくなったユーザー。
- 長期休暇中のユーザー。

管理者は、デバイスが故障した場合のみ、デバイスのライセンスを解放できます。

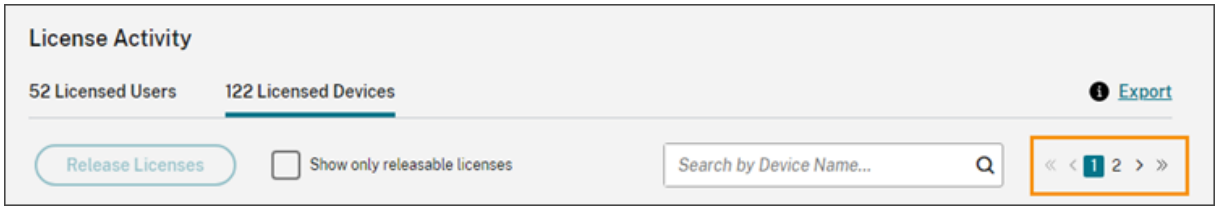
> 注：
>
> - ライセンスを解放するには、自動プロセスに従うことをお勧めします。ただし管理者が、90 日の期間が経過する前に、上記の理由ではなくライセンスを解放しようとする場合、Citrix EULA に違反する可能性があります。この操作を実行する前に、Citrix にお問い合わせください。
> - 管理者は、UI を使用して 1 つのライセンスを手動で解放できます。または、クラウドライセンス API を使用して、複数ライセンスを解放することを選択できます。詳しくは、「APIs to manage Citrix cloud licensing」を参照してください。

解放可能ライセンスを見つける

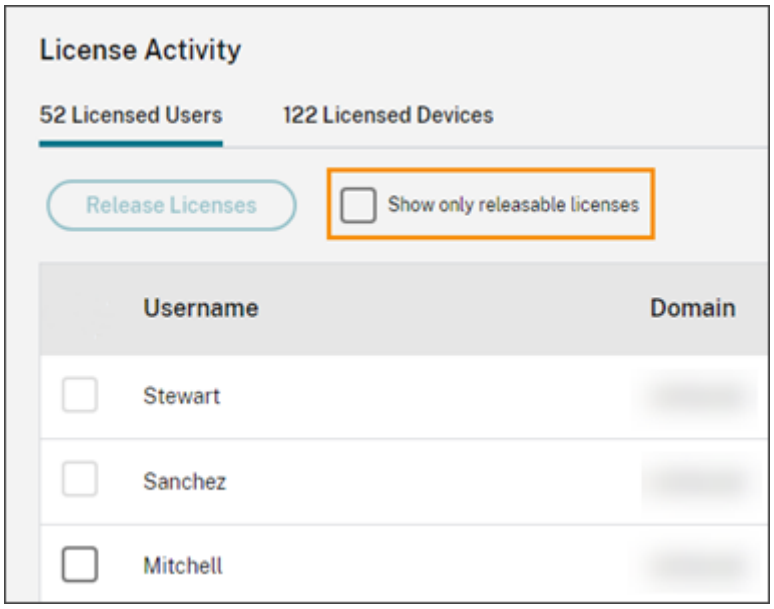
ユーザーまたはデバイスが 30 日以上アプリまたはデスクトップを起動していない場合、Citrix Cloud はライセンスを解放可能な状態にします。解放可能ライセンスは、選択できる濃い灰色のチェックボックスとともに［ライセンス

使用ユーザー］または［ライセンス使用デバイス］リストに表示されます。解放できないライセンスには、ライセンスを選択できないことを示す薄い灰色のチェックボックスが表示されます。

［ライセンスアクティビティ］セクションに表示される一覧には、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で一覧を移動します。



解放可能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 ［解放可能ライセンスのみを表示］を選択します。このアクションにより、まだリリースが許可されていない割り当てられたライセンスが非表示になります。



解放可能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、解放するライセンスを選択します。一覧から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。

解放可能なライセンスをすべて 1 つずつ選択し、［ライセンスの解放］を選択できます。

割り当て済みライセンスを解放するには

1. ［ライセンスアクティビティ］で、［ライセンス使用ユーザー］または ［ライセンス使用デバイス］タブを選択します。

2. 必要に応じて、［解放可能ライセンスを表示］を選択して、解放可能ライセンスを持つユーザーのみを表示します。
3. 管理するユーザーまたはデバイスを選択してから、［ライセンスを解放］を選択します。
4. 選択したユーザーまたはデバイスを確認してから、［ライセンスを解放］を選択します。

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）

October 4, 2023

この記事では、**Citrix DaaS** の同時ユーザーライセンスのみを管理するための操作について説明します。

Citrix DaaS のユーザー/デバイスライセンスについて詳しくは、「Citrix DaaS のライセンスとアクティブな使用状況の監視（ユーザー/デバイス）」を参照してください。

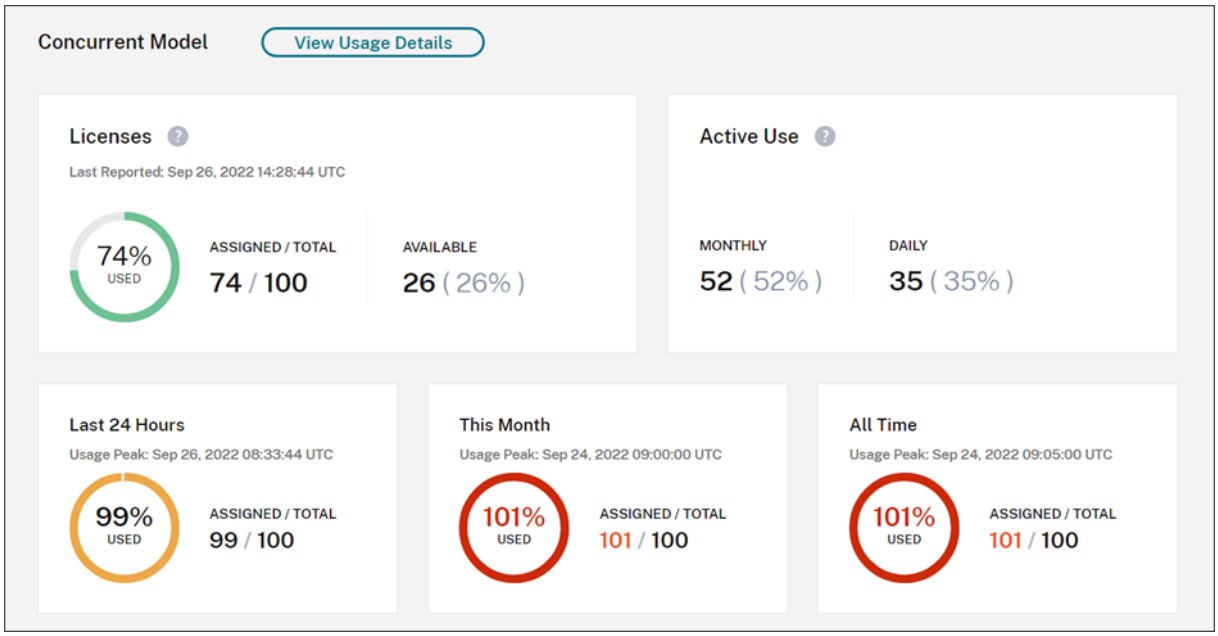
Citrix DaaS Standard for Azure のユーザー/デバイスライセンスおよび同時ユーザーライセンスについては、「Citrix DaaS Standard for Azure のライセンスと使用状況の監視」を参照してください。

ライセンス割り当て

Citrix Cloud では、デバイスにあるアプリまたはデスクトップをユーザーが起動したときにライセンスが割り当てられます。ユーザーがログオフするか、セッションから切断すると、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、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応じて変わる可能性が常にあるため、Citrix Cloud は 5 分ごとに使用中のライセンスの数を評価します。

同時ユーザーライセンスモデルについて詳しくは、ライセンスサーバー製品ドキュメントの「同時使用ライセンス」を参照してください。

ライセンスの概要



ライセンスの概要では、次の情報を一目で確認できます:

- Citrix Cloud が使用中のライセンスを最後に評価したときに使用中だった購入済みライセンスの合計の割合。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、5 分ごとにこの割合を計算します。購入したライセンスの総数は、同時ユーザーライセンスモデルを使用する Citrix DaaS エディションのために購入したライセンスの合計です。
- 購入したライセンスの合計に対する現在割り当てられているライセンスの比率、および使用可能なライセンスの残りの数。この比率に示す［合計］の数値は、現在所有しているライセンスの合計数を表します（[最新レポート］の日時の時点での内容）。
- ピーク時使用状況の統計。ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次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 **24** 時間：過去 24 時間で同時使用されたライセンスの最大数。
  - 今月：現在の暦月に入ってから同時使用されたライセンスの最大数。
  - 常時：サブスクリプションが開始してから同時使用されたライセンスの最大数。

  これらのピーク時使用状況期間に示される［合計］の数値は、その時点で所有していたライセンスの総数を表します。所有ライセンスの合計数が増加または減少し、それに伴って割り当てられたライセンスが増加した場合、［合計］の数値は、その時点における所有ライセンスの新しい数を反映して変更されます。ただし、対応する使用量のピークがない場合、［合計］の数値は変化しません。
- アクティブな使用統計。Citrix Cloud は、次の期間の一意の接続の合計数を表示します:
  - 月単位：前のカレンダー月の合計接続数。

- 日単位：過去 24 時間の合計接続数。
  これらの数値は、これらの期間中に所有されたライセンスの総数の割合でも表示されます。

ピーク時のライセンス使用の計算

同時ユーザーライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスに同時にアクセスする一意のデバイスの数が 5 分ごとにカウントされます。表示されている現在のピーク時使用状況よりもカウントが大きい場合、ピークに達した日時とともに新しいピーク時使用状況が Citrix Cloud に表示されます。カウントが現在のピーク使用量より少ない場合、現在のピーク使用量は変更されません。

> 重要：
>
> Director で［監視］を使用して同時セッションに関する情報を入手する場合、監視レポートで提供される同時セッションの解釈は異なり、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。監視レポートとライセンスレポートの違いについて詳しくは、「よくある質問」を参照してください。

毎月のアクティブ使用量の計算

毎月の初めに、Citrix Cloud は前月のスナップショットを作成します。Citrix Cloud は、そのカレンダー月に発生した一意の合計接続数を表示します。

日単位のアクティブな使用量の計算

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作成します。Citrix Cloud は、その 24 時間の間に発生した一意の合計接続数を表示します。

使用状況の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、［使用状況の詳細の表示］をクリックします。

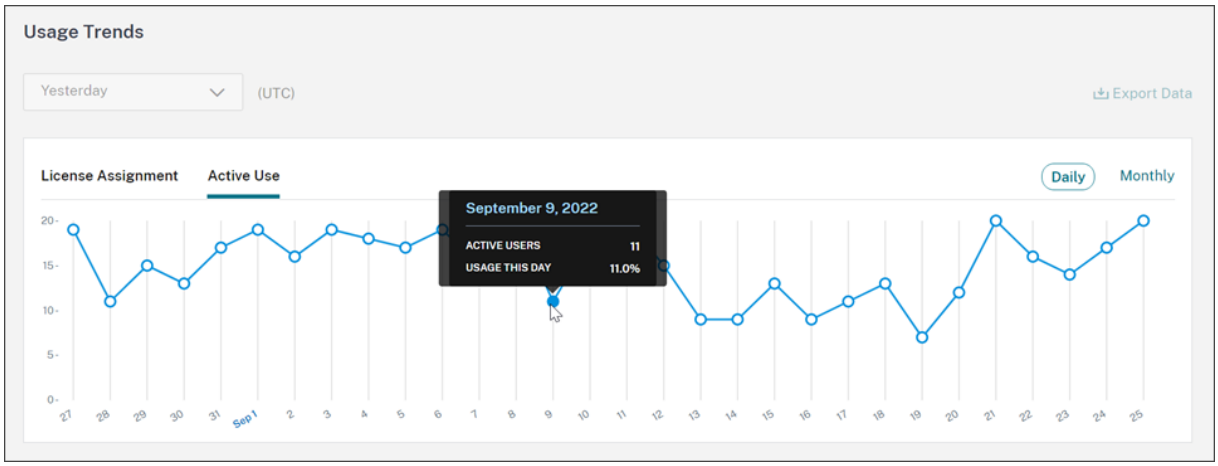
［使用状況の傾向］セクションに次の情報が表示されます：

- ［ライセンス割り当て］には、以下の情報のグラフが表示されます：
  - ［ライセンス - 合計］：購入した同時ユーザーライセンスの総数。
  - ［ピーク時のライセンス使用］：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量を表示します。月間または時間ごとのピーク使用量を確認するには、表示する暦月または暦日をドロップダウンメニューから選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloud にはその時点において最新の時間間隔のピーク使用量が表示されます。たとえば、現在進行中の暦日を確認する場合、その瞬間までの 1 時間ごとの最大ライセンス数が表示されます。次の 5 分のカウント間隔でライセンスの最大数が増えると、Citrix Cloud ではその 1 時間のピーク使用量が更新されます。

- ［アクティブな使用］には、以下の情報のグラフが表示されます：
  - 日単位：過去 30 日間の各日の合計接続数。
  - 月単位：前のカレンダー年における各月の合計接続数。

［ライセンス割り当て］または ［アクティブな使用］グラフの間隔をポイントすると、その間隔の詳細が表示されます。



ライセンスの解放

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。

Citrix DaaS Standard for Azure のライセンスと使用状況の監視

November 9, 2023

この記事では、ユーザー/デバイスライセンスモデルおよび同時ユーザーライセンスモデルの両方を使用したライセンス割り当ての管理について説明します。

Citrix Azure Consumption Fund（ユーザー/デバイスのみ）

ご使用のサービス環境で使用する Citrix Azure Consumption Fund を購入した場合、Citrix 管理リソースの消費レポートについて詳しくは、「Citrix DaaS の Citrix Managed Azure リソースの消費の監視」を参照してください。

ライセンス割り当て

ユーザー/デバイスライセンスモデル： Citrix Cloud では、一意のユーザーまたはデバイスによるデスクトップの初回起動時にライセンスが割り当てられます。

同時ユーザーライセンスモデル： Citrix Cloud では、デバイスにあるデスクトップをユーザーが起動したときにライセンスが割り当てられます。ユーザーがログオフするか、セッションから切断すると、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、デスクトップにアクセスするデバイスの数に応じて変わる可能性が常にあるため、Citrix Cloud は 5 分ごとに使用中のライセンスの数を評価します。

同時使用ライセンスモデルについて詳しくは、ライセンスサーバー製品ドキュメントの「同時使用ライセンス」を参照してください。

ピーク時のライセンス使用の計算

同時使用ライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスに同時にアクセスする一意のデバイスの数が 5 分ごとにカウントされます。表示されている現在のピーク時使用状況よりもカウントが大きい場合、ピークに達した日時とともに新しいピーク時使用状況が Citrix Cloud に表示されます。カウントが現在のピーク使用量より少ない場合、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、それらのドメイン内に互いに似たアカウントを持つ複数のユーザーがいる場合（たとえば、`johnsmith@company.com`と`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（たとえば、johnsmith）のみを考慮させるように許可することができます。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ると、Citrix Cloud による一意ユーザーのカウント方法が変わります。Citrix Cloud が、`johnsmith@company.com`と`johnsmith@mycompany.com`を 2 人の一意ユーザーとしてカウントするのではなく、johnsmith のみを一意ユーザーとしてカウントするようになります。このカウント方法の変更は、次のライセンスデータに影響します。

- ライセンス割り当て
- アクティブな使用
- ライセンスの経時的な使用傾向
- 解放対象のライセンス

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のデータをエクスポートした CSV ファイルにも反映されます。

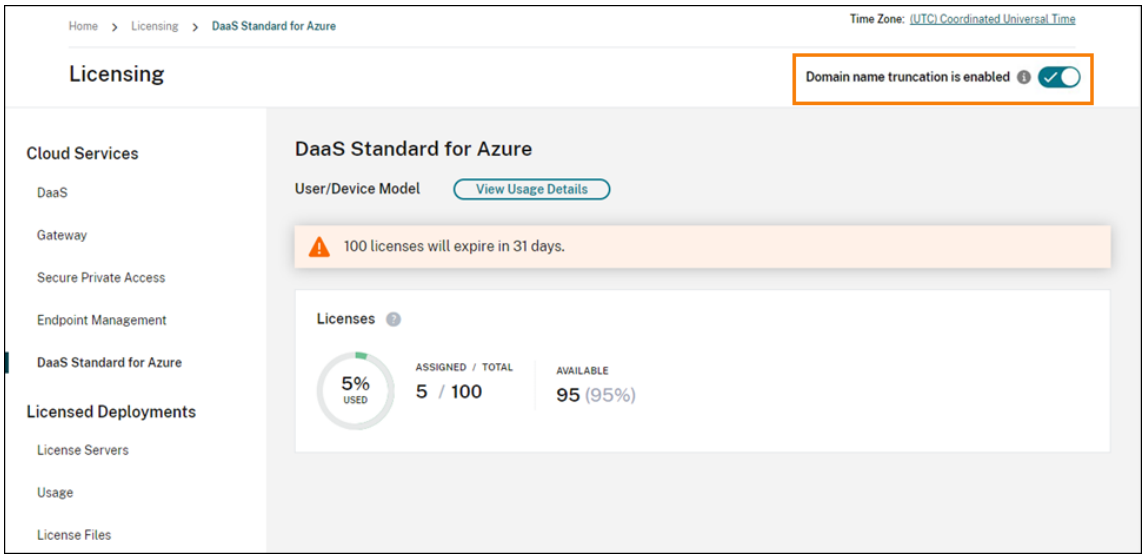
> 注:
>
> ユーザー名がわずかに異なる類似のアカウントが参加している複数のドメインをホストしている場合（たとえば、参加ユーザーのアカウントが`johnsmith@company.com`と`jsmith@newcompany.com`）、ドメイン名の切り捨てを行っても、Citrix Cloud のユーザーカウント結果には影響しません。johnsmith と jsmith は、同じ個人のアカウントである場合でも、Citrix Cloud ではそれぞれ一意ユーザーとして引き続きカウントされます。

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/デバイス利用状況データに影響します。たとえば、特定の月にドメイン名の切り捨てを有効にすると、その月に Citrix Cloud が記録するデータが影響を受けます。ただし、この機能が無効になっていた前月の履歴データは以前のまま影響を受けません。同様に、特定の月にドメイン名の切り捨てを無効にすると、その月に Citrix Cloud が記録するデータが影響を受けます。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近くにあるトグルをクリックします。



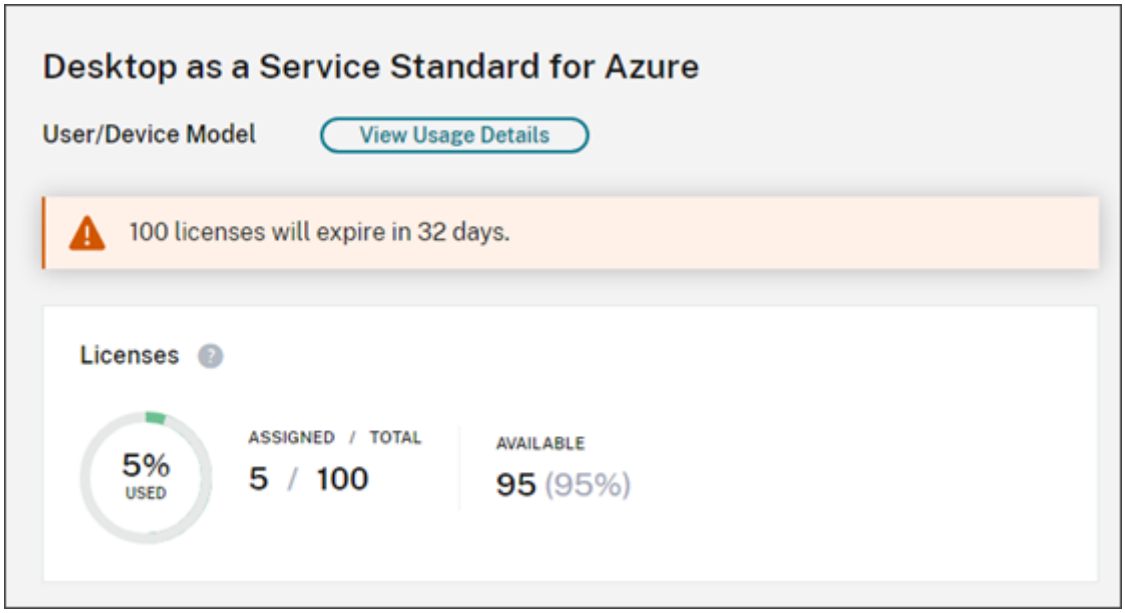
2. アクションの確認を求められたら、［はい。了承しています］を選択します。

ライセンスの概要

Citrix Cloud は、ユーザー/デバイスライセンスモデルおよび同時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。

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、ライセンスの概要では、所有しているライセンスの総数に対する使用中のライセンス数が表示されます。

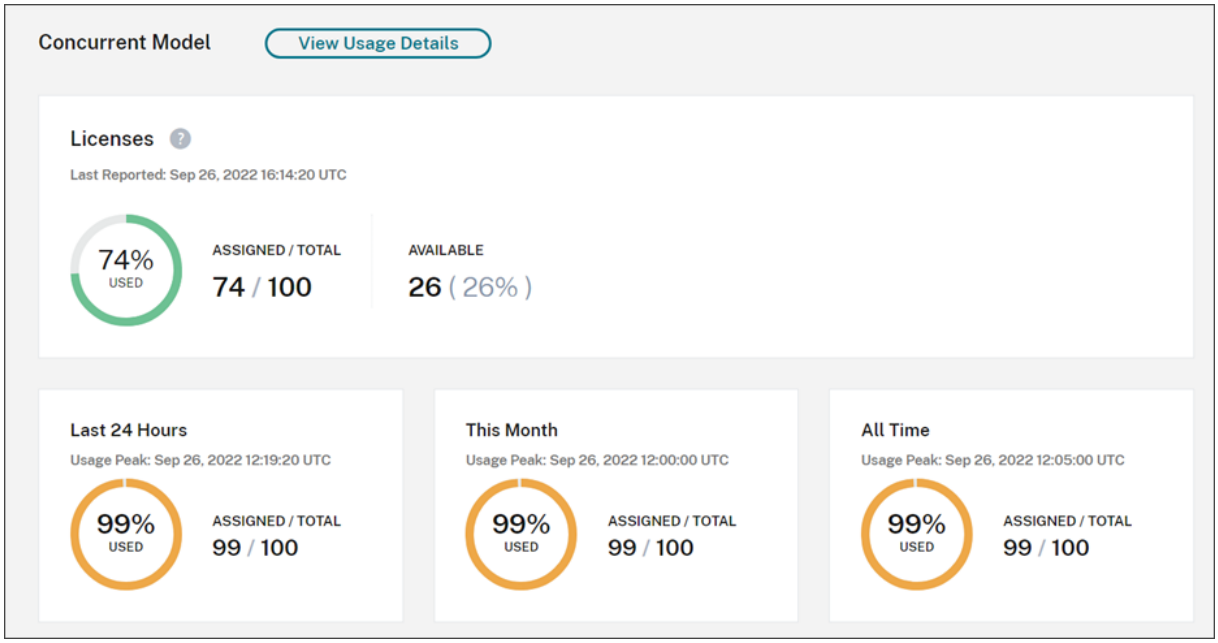


割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。

Citrix Cloud は、購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数も表示します。

同時ユーザーの概要

同時使用モデルの場合、ライセンスの概要で次の情報が一目でわかります:

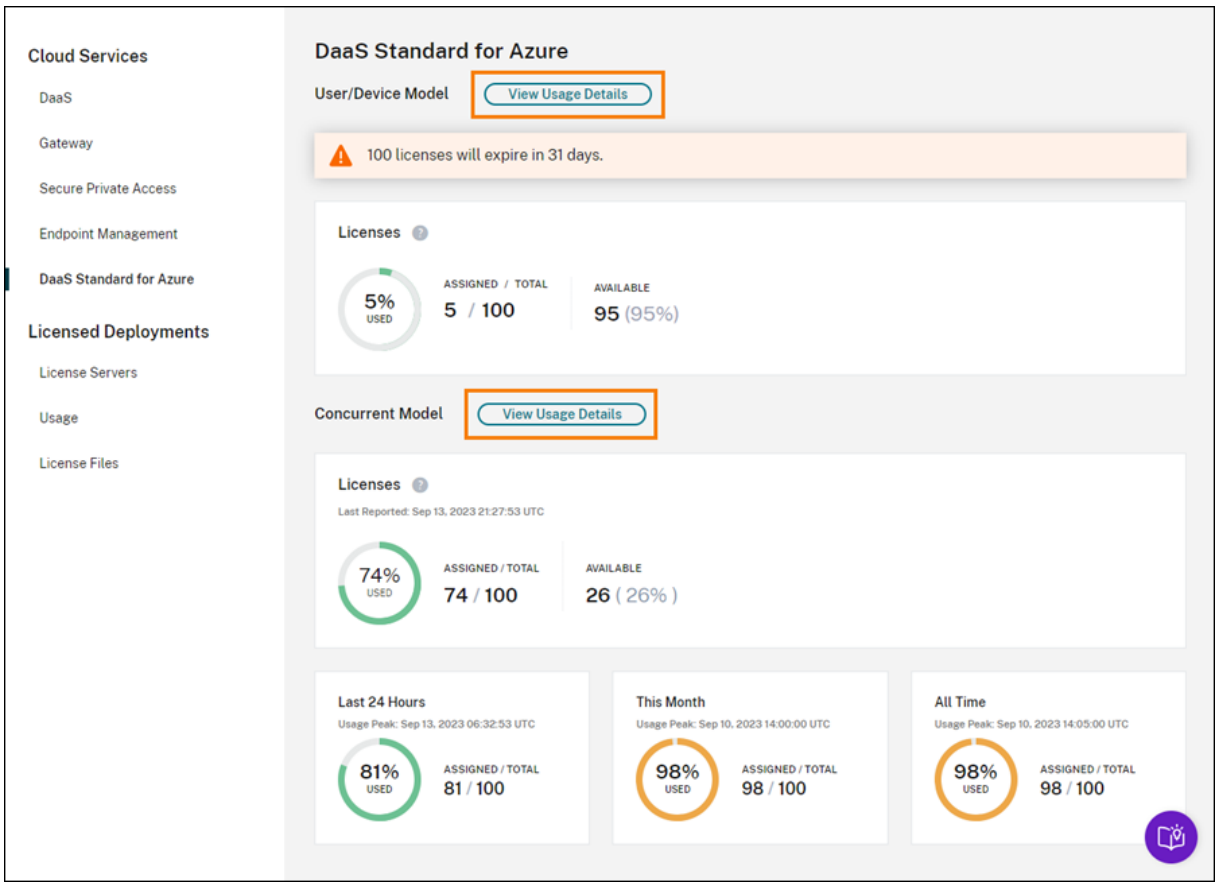


- Citrix Cloud が使用中のライセンスを最後に評価したときに使用中だった購入済みライセンスの合計の割合。Citrix Cloud は、サービスへのアクティブな接続を持つ一意のデバイスに基づいて、5 分ごとにこの割合を計算します。購入したライセンスの総数は、同時使用ライセンスモデルを使用する Citrix DaaS Standard for Azure のために購入したライセンスの合計です。
- 購入したライセンスの合計に対する現在割り当てられているライセンスの比率、および使用可能なライセンスの残りの数。この比率に示す［合計］の数値は、現在所有しているライセンスの合計数を表します（［最新レポート］の日時の時点での内容）。
- ピーク時使用状況の統計。ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次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 **24** 時間：過去 24 時間で同時使用されたライセンスの最大数。
  - 今月：現在の暦月に入ってから同時使用されたライセンスの最大数。
  - 常時：サブスクリプションが開始してから同時使用されたライセンスの最大数。

  これらのピーク時使用状況期間に示される［合計］の数値は、その時点で所有していたライセンスの総数を表します。所有ライセンスの合計数が増加または減少し、それに伴って割り当てられたライセンスが増加した場合、［合計］の数値は、その時点における所有ライセンスの新しい数を反映して変更されます。ただし、対応する使用量のピークがない場合、［合計］の数値は変化しません。

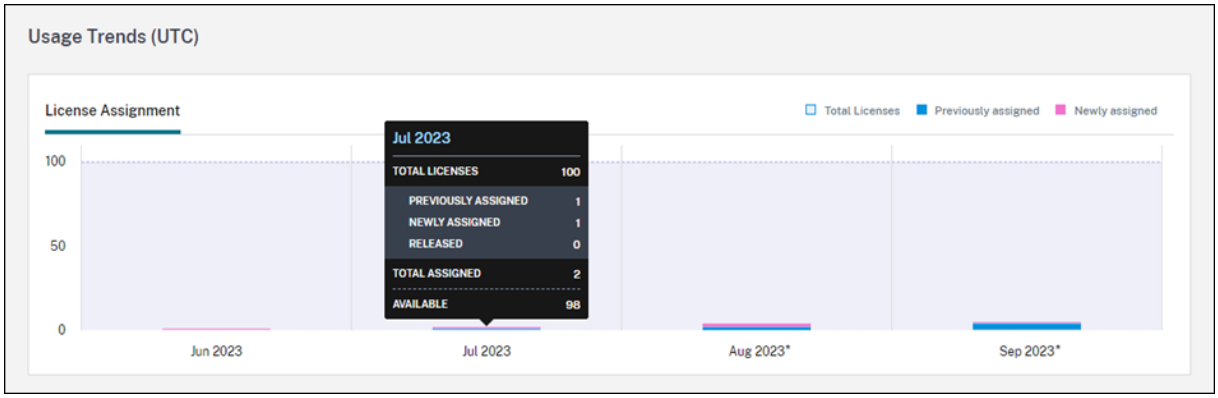
使用状況の傾向

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、ライセンスの概要ページから［使用状況の詳細の表示］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。



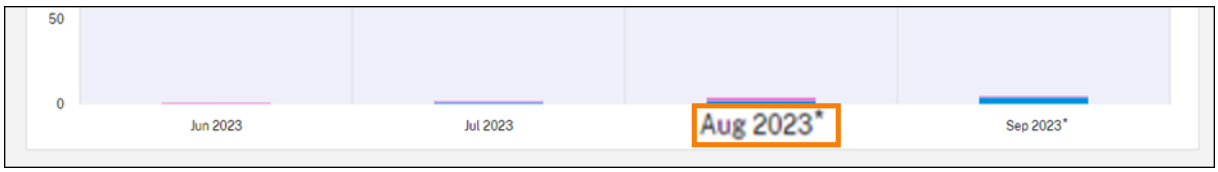
グラフ上の間隔をポイントすると、次の情報が表示されます：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 以前に割り当て済み：先月割り当てられたライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］

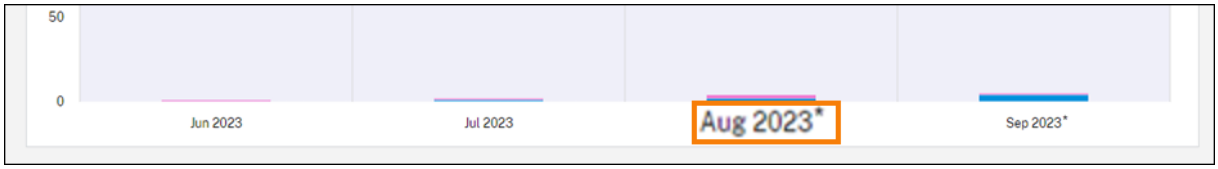
としてカウントされます。8 月には、「以前に割り当て済み」としてカウントされます。

- 新しく割り当て済み：各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］としてカウントされます。

ドメインの切り捨てを有効にした期間にはアスタリスクが付いています。



ドメインの切り捨てを有効にした期間にはアスタリスクが付いています。



同時ユーザーの傾向

同時ユーザーライセンスの場合、［使用状況の傾向］セクションに次の情報が表示されます：

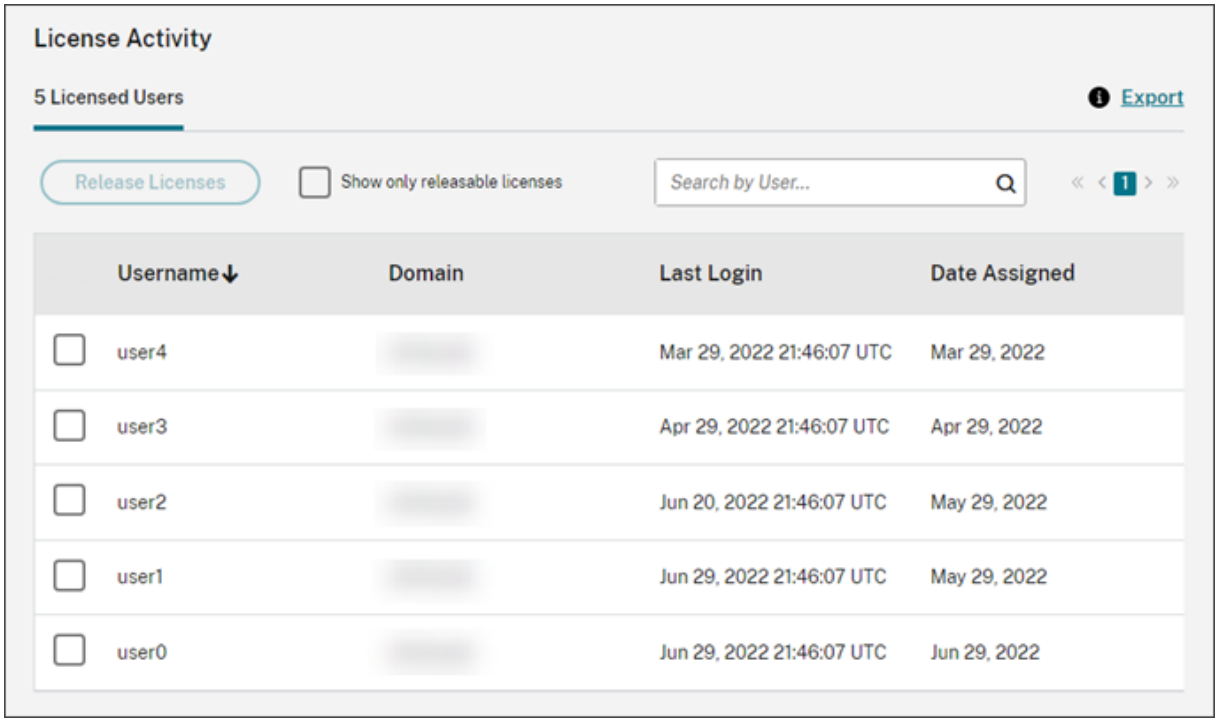
- ［ライセンス数合計］：購入した同時ライセンスの合計。
- ［ピーク時のライセンス使用］：選択した日付範囲に割り当てられたライセンスの最大数。デフォルトでは、Citrix Cloud は現在の暦年の各月のピーク使用量を表示します。月間または時間ごとのピーク使用量を確認するには、表示する暦月または暦日をドロップダウンメニューから選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloud にはその時点において最新の時間間隔のピーク使用量が表示されます。たとえば、現在進行中の暦日を確認する場合、その瞬間までの 1 時間ごとの最大ライセンス数が表示されます。次の 5 分のカウント間隔でライセンスの最大数が増えると、Citrix Cloud ではその 1 時間のピーク使用量が更新されます。

グラフの間隔をポイントすると、その間隔での合計ライセンス数とピーク時のライセンス使用が表示されます。

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］セクションでは、ライセンスを割り当てた個々のユーザーの一覧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。このセクションは同時ライセンスでは利用できません。



一覧をフィルタリングして、解放対象のライセンスのみを表示することもできます。本記事の「割り当て済みライセンスを解放する」を参照してください。

ユーザー/デバイスライセンスの解放

対象となるユーザー/デバイスライセンスの解放は、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。

- 年単位サービスサブスクリプション：年単位サブスクリプションがある場合は、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解放できます。ライセンスは複数を一括で解放するか、個別に解放できます。
- 月単位サービスサブスクリプション：月単位サブスクリプションがある場合は、非アクティブ期間に関係なく、各月の 1 日にライセンスを解放できます。

ライセンスが割り当てられる場合、割り当て期間はサービスへの接続が確立されてから 90 日間です。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みなされ、90 日後に Citrix Cloud によって解放されます。このプロセスは自動化されており、管理者による操作は必要ありません。

割り当て期間（90 日）が経過した場合、管理者は次のシナリオでのみライセンスを手動で解放できます：

- 会社への関連付けがなくなったユーザー。
- 長期休暇中のユーザー。

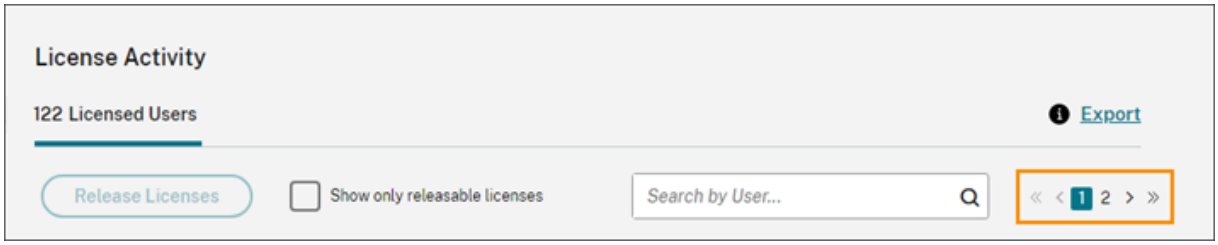
管理者は、デバイスが故障した場合のみ、デバイスのライセンスを解放できます。

> 注:
>
> - ライセンスを解放するには、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、90 日の期間が経過する前に、上記の理由ではなくライセンスを解放しようとする場合、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 を使用して 1 つ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、複数ライセンスを解放することを選択できます。詳しくは、「APIs to manage Citrix cloud licensing」を参照してください。

解放可能ライセンスの表示

ユーザーまたはデバイスが 30 日以上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。解放可能ライセンスは、選択できる濃い灰色のチェックボックスとともに［ライセンス使用ユーザー］または［ライセンス使用デバイス］リストに表示されます。解放できないライセンスには、ライセンスを選択できないことを示す薄い灰色のチェックボックスが表示されます。

［ライセンスアクティビティ］セクションに表示される一覧には、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で一覧を移動します。



解放可能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。

解放可能ライセンスの選択

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、解放するライセンスを選択します。一覧からライセンスを選択すると、［ライセンスを解放］がアクティブになります。

解放可能なライセンスをすべて 1 つずつ選択し、［ライセンスの解放］を選択できます。

割り当て済みライセンスを解放する

1. 必要に応じて、［解放可能ライセンスを表示］を選択して、解放可能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てから、［ライセンスを解放］を選択します。
3. 選択したユーザーを確認してから、［ライセンスを解放］を選択します。

同時ユーザーライセンスの解放

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の監視

November 30, 2023

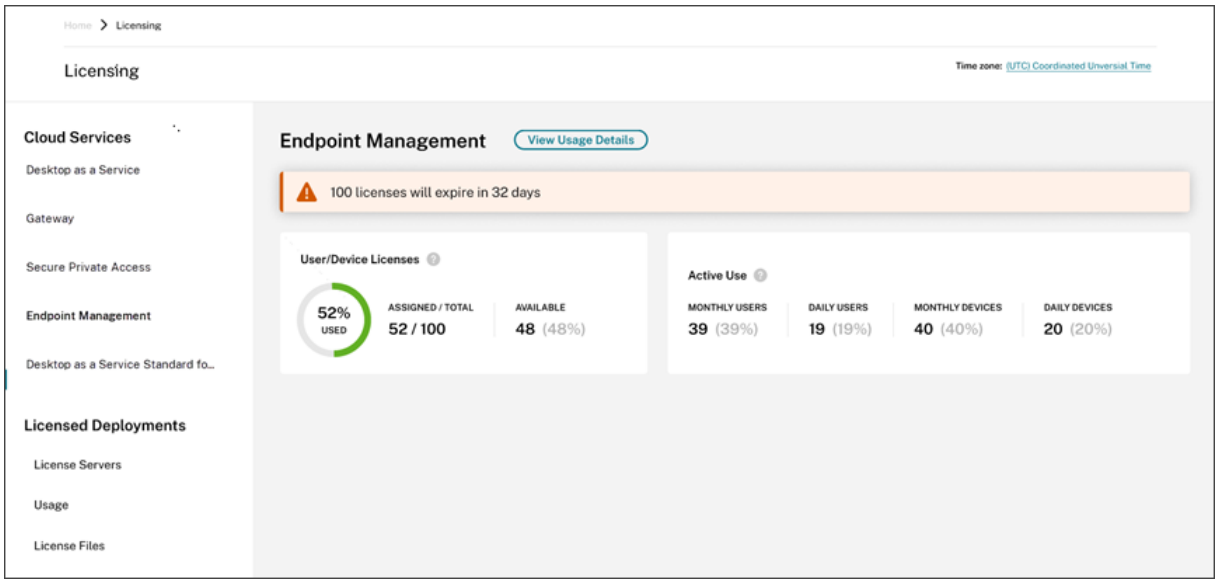
ライセンス割り当て

一般に、ユーザーには、クラウドサービスの最初の使用時にライセンスが割り当てられます。Endpoint Management では、ユーザーがデバイスを登録するときに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」を使用して毎月の使用量を計算し、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、またはデバイスに対して「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と、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

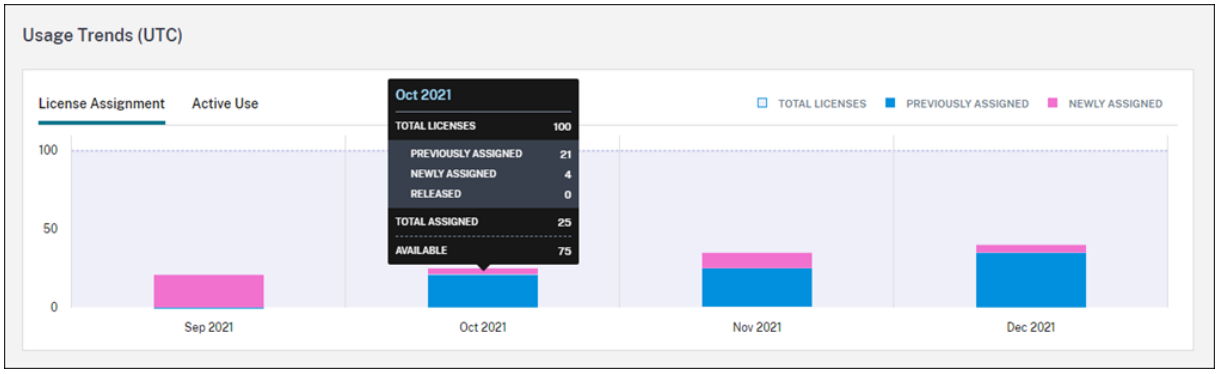


ライセンスの概要では、サポートされている各サービスに関する次の情報を一目で確認できます:

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 月次および日次のアクティブな使用状況の統計:
  - 月次のアクティブな使用状況とは、過去 30 日間にサービスを使用した一意のユーザー数を指します。
  - 日次のアクティブな使用状況とは、過去 24 時間以内にサービスを使用した一意のユーザー数を指します。
- 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 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。

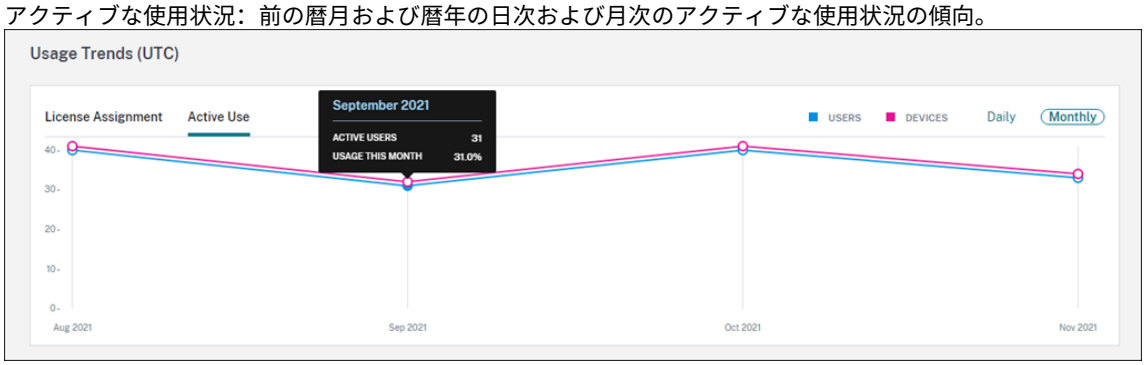
使用状況の傾向

ライセンスの詳細を表示するには、[使用状況の詳細の表示] をクリックします。使用傾向と、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。



この内訳では、次の情報を表示します：

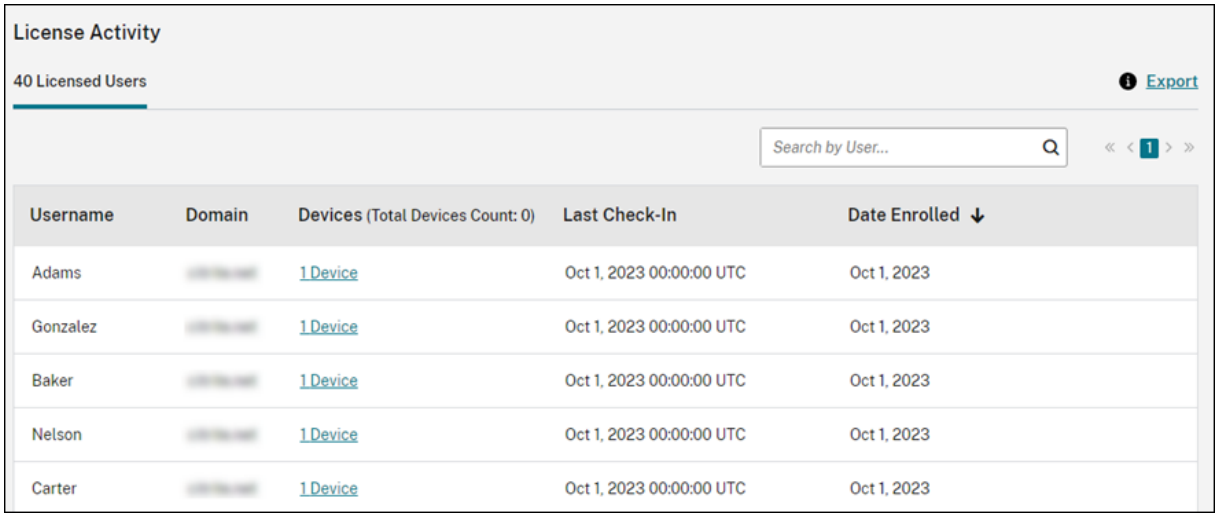
- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 事前割り当て済み：月ごとの初めに既に割り当てられているクラウドサービスライセンス。たとえば、7 月にユーザーにライセンスが割り当てられた場合、その割り当ては 8 月の事前割り当て済み数に含まれます。
- 新しく割り当て済み：月ごとに割り当てられたクラウドサービスライセンス数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーには、ライセンスが割り当てられます。このライセンスは、7 月の新しく割り当て済みの合計に含まれます。
- アクティブな使用状況：前の暦月および暦年の日次および月次のアクティブな使用状況の傾向。



ライセンスアクティビティ

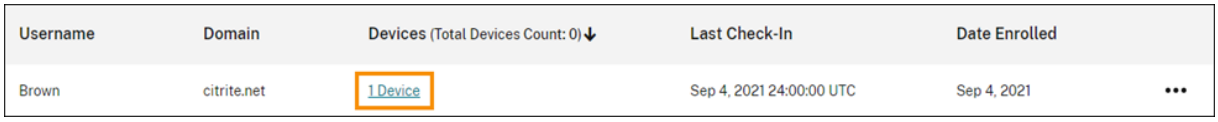
［ライセンスアクティビティ］セクションには、次の情報の一覧が表示されます：

- ライセンスを割り当てた個々のユーザー
- ライセンスが割り当てられた日付
- 登録されたデバイスの数と各ユーザーの最終チェックイン日

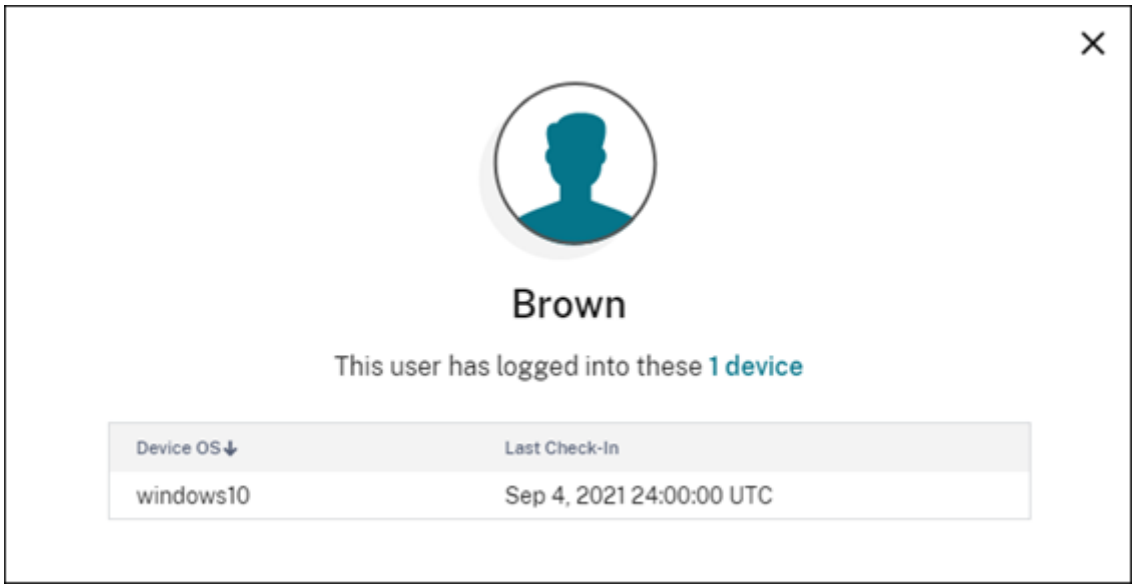


登録済みデバイスの表示

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。



Citrix Cloud には、ユーザーに登録されているデバイスの一覧と、各デバイスの最終チェックイン日が表示されます。



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 日間に次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の他の操作は必要ありません。

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 サービスの帯域幅使用量の監視

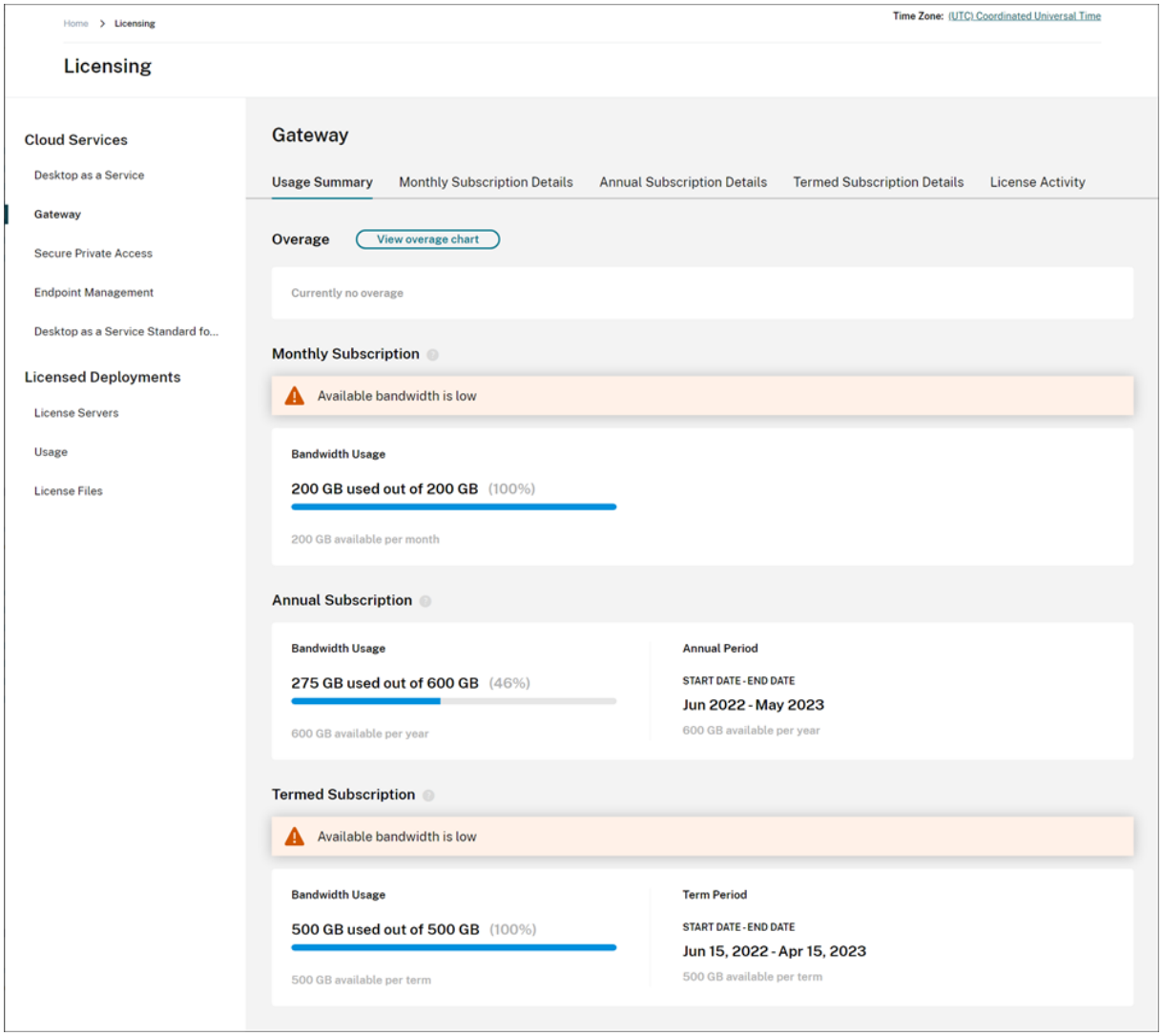
October 4, 2023

ここでは、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）と Citrix Workspace を使用する場合の Gateway サービスを通じた帯域幅の使用状況について説明します。Virtual Apps Essentials サービスに含まれる Gateway サービスの帯域幅消費量は、Citrix Cloud 管理コンソールの ［ライセンス］ページに表示されません。

> 注:
>
> Gateway サービスのライセンスは、仮想アプリおよび仮想デスクトップの使用に関連するため、帯域幅の使用状況を把握するのに役立ちます。Citrix が、使用環境での帯域幅の使用状況の割り当てを強制することはありません。帯域幅の割り当てを使いすぎても、Citrix が実稼動のワークロードやサービスの操作を妨げることはありません。Citrix が Gateway サービスと帯域幅の使用状況のポリシーの適用方法を変更する場合は、その変更が有効になる前にお知らせします。

使用状況の概要

使用状況の概要では、各 Gateway サービスのサブスクリプションの帯域幅の使用状況と、すべてのサブスクリプション（月間、年間、期限付き）の合計超過量が一目でわかります。



Citrix Cloud では、帯域幅の合計量と、サブスクリプションの種類ごとに消費された帯域幅の量が表示されます。

サブスクリプションの種類に応じて、サブスクリプションの課金期間も表示されます:

- 月間サブスクリプション: 現在の課金期間が表示されません。このサブスクリプションの場合、課金期間は毎月 1 日から始まり、その月の最終日に終了します。
- 年間サブスクリプション: 課金期間の開始日と終了日が表示されます。このサブスクリプションの場合、課金期間は 1 年間です。
- 期限付きサブスクリプション: 課金期間の開始日と終了日が表示されます。このサブスクリプションの場合、課金期間は、購入したサブスクリプションの期間です。たとえば、3 年間の期限付きサブスクリプションを購入した場合、課金期間の開始日と終了日はその 3 年間になります。

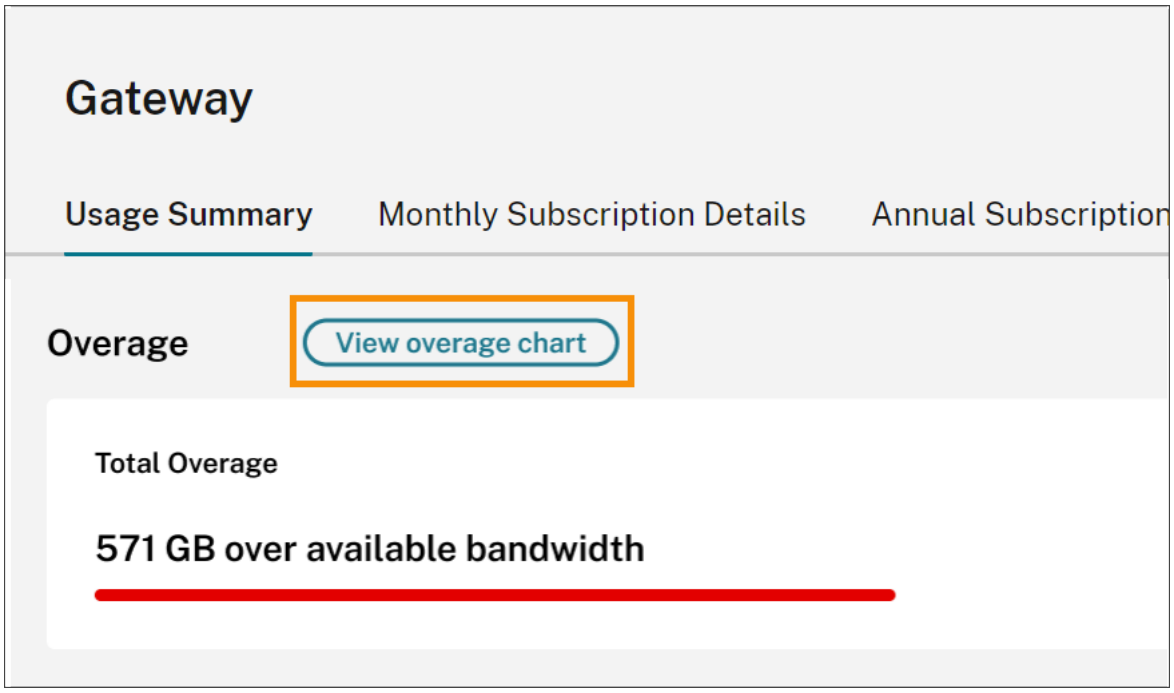
サブスクリプションが 90 日以内に期限切れになる場合、そのサブスクリプションに関する警告メッセージが表示されます。

超過

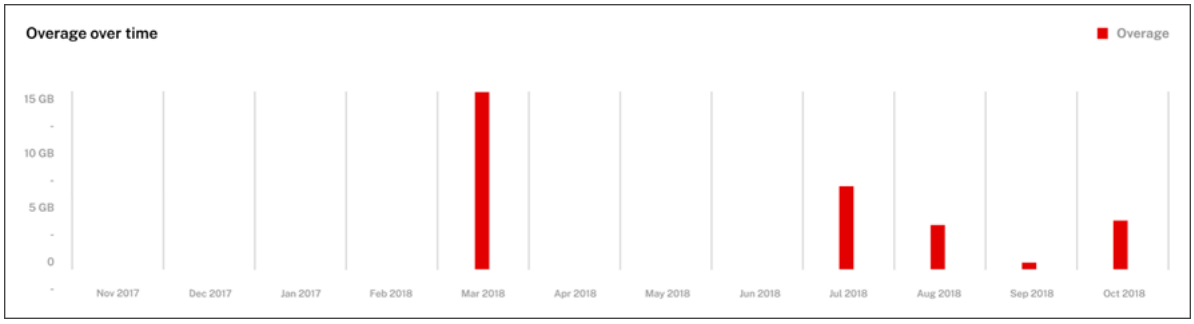
Citrix Cloud では、すべてのサブスクリプションの月間の超過分が計算されます。購入した帯域幅よりも多くの帯域幅を消費した場合、Citrix Cloud では超過した帯域幅が超過分として表示されます。

サブスクリプションが複数ある場合、最初に、終了日が最も早いサブスクリプションの帯域幅の使用状況が測定されます。そのサブスクリプションで割り当てられた帯域幅を使い果たした場合、次に早い終了日のサブスクリプションについて帯域幅の使用状況が測定されます。すべてのサブスクリプションで割り当てられた帯域幅を使い果たすと、超過した使用量が超過分として表示されます。

[使用状況の概要] ページには、当月の超過合計量が表示されます。一定期間の超過を表示するには、[超過消費グラフを表示] を選択します。



過去 12 か月間の合計の超過消費グラフが表示されます。



当月の超過分は翌月に繰り越されません。次の月が始まると、合計超過分はゼロにリセットされます。

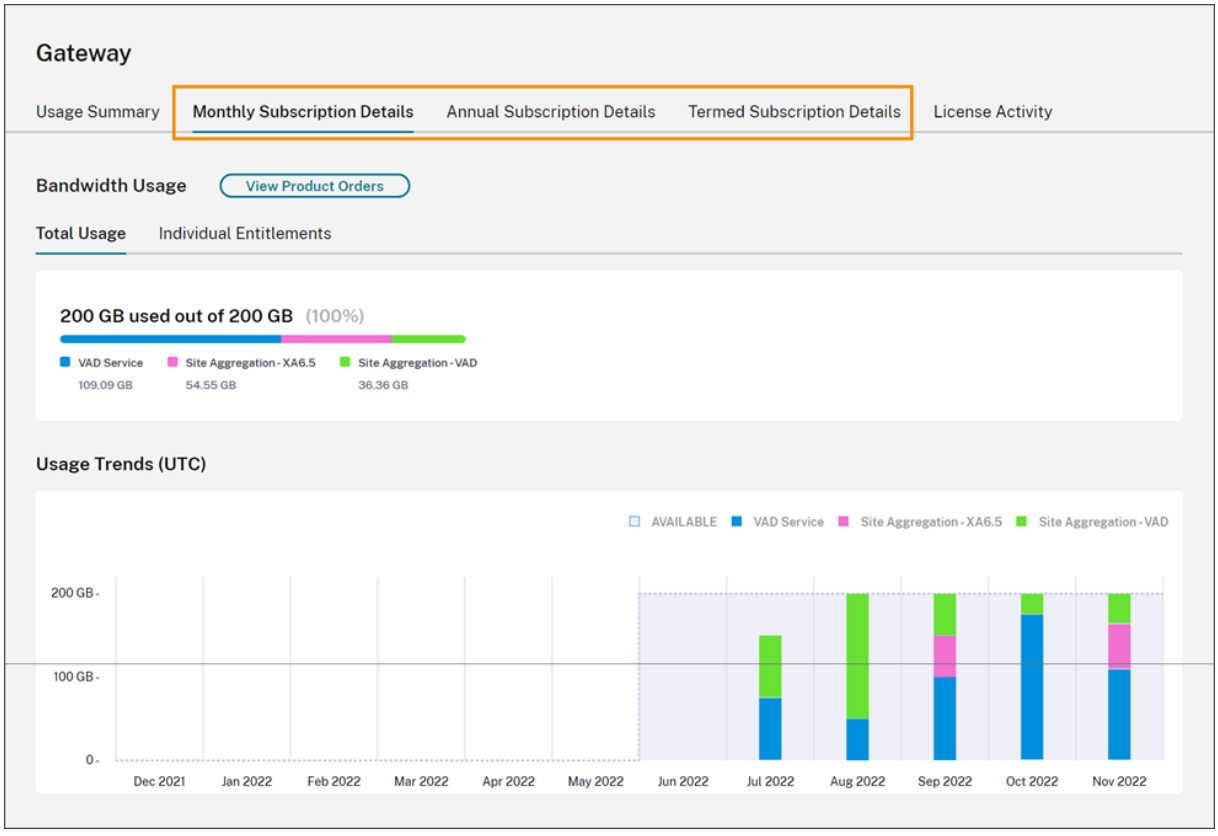
未使用の帯域幅

Citrix Cloud では、次の課金期間になると、サブスクリプションの帯域幅使用量が自動的にリセットされます。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、未使用の帯域幅は次の課金期間に引き継がれません。

たとえば、月間サブスクリプションに 150GB の合計帯域幅が含まれていて、特定の月に 100GB の帯域幅を使用した場合、翌月の初めに使用量がゼロにリセットされ、帯域幅の合計量として 150GB が表示されます。未使用の帯域幅が、合計の帯域幅の割り当て分に追加されることはありません。

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間、年間、または期限付きのサブスクリプションの詳細タブを選択します。



サブスクリプションの種類ごとに、詳細タブに次の情報が表示されます:

- 合計使用量：特定の種類のすべてのサブスクリプションで使用できる合計帯域幅のうち、消費された帯域幅の量。月間サブスクリプションの場合、当月の合計使用量が表示されます。年間サブスクリプションと期限付きサブスクリプションの場合、合計使用量は、すべての年間サブスクリプションまたは期限付きサブスクリプションで累積されます。

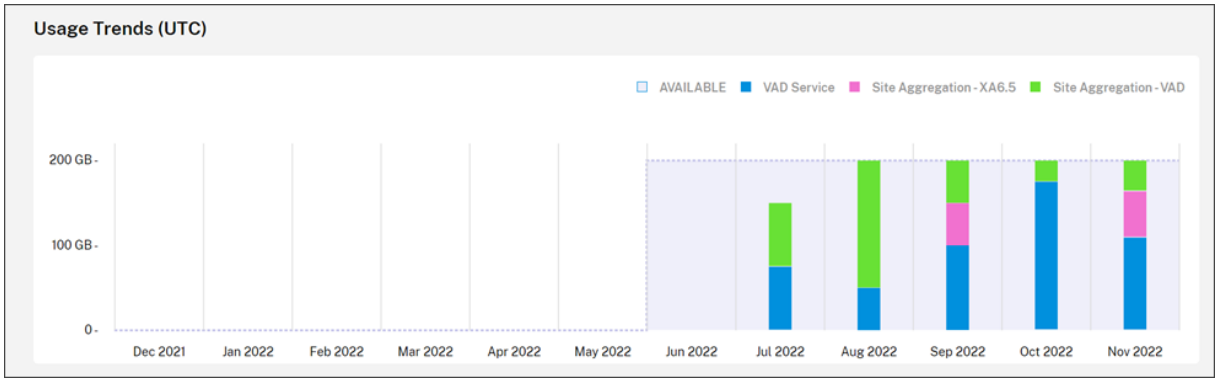
- 個別使用量：特定の種類の各サブスクリプションで消費された帯域幅の合計量。たとえば、複数の年間サブスクリプションがある場合、このタブには各年間サブスクリプションの使用量の内訳が個別に表示されます。

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Citrix Workspace のサイトアグリゲーションを使用したオンプレミスの Virtual Apps and Desktops 環境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

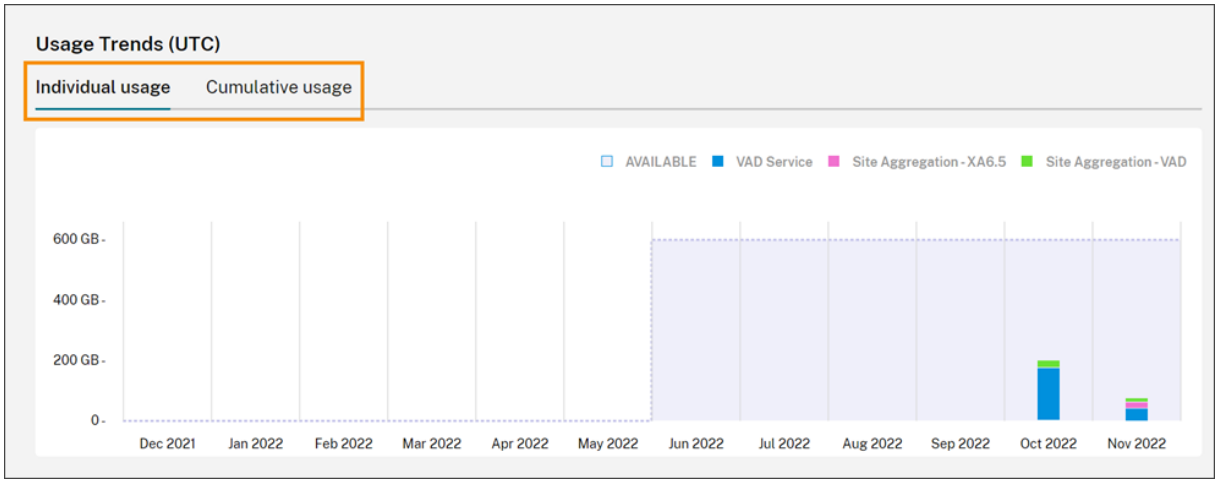
［使用状況の傾向］セクションでは、過去 12 か月間の使用量の内訳が表示されます。

月間サブスクリプションの場合、月ごとに使用量が表示されます。

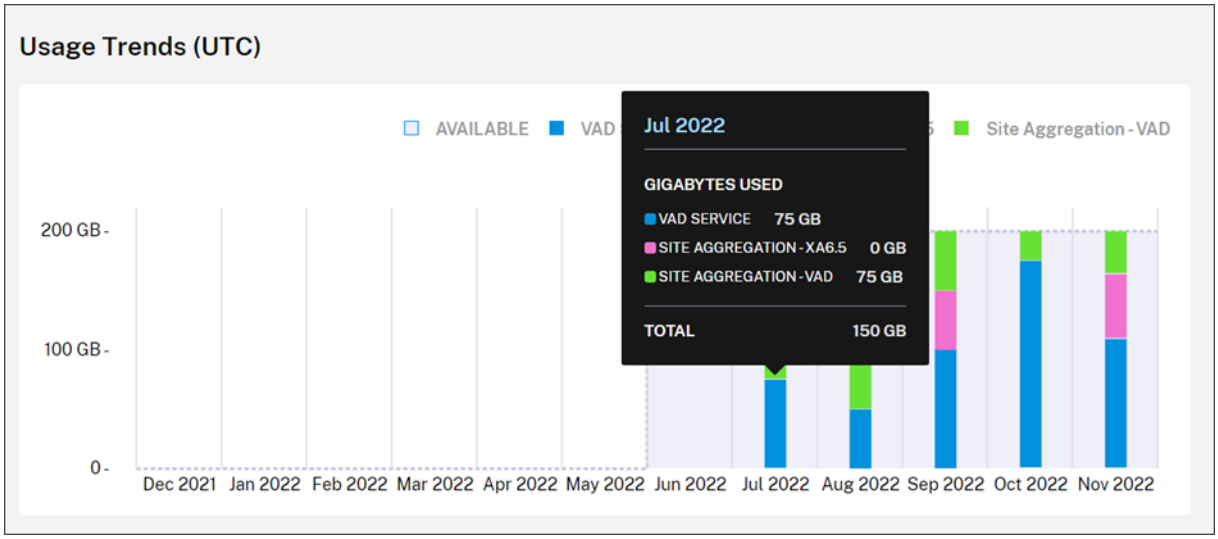


年間サブスクリプションと期限付きサブスクリプションの場合、このセクションには次のビューが表示されます：

- 個別使用量：現在の課金期間の各月に消費された帯域幅の使用状況。
- 累積使用量：現在の課金期間中に毎月累積された帯域幅の使用状況。



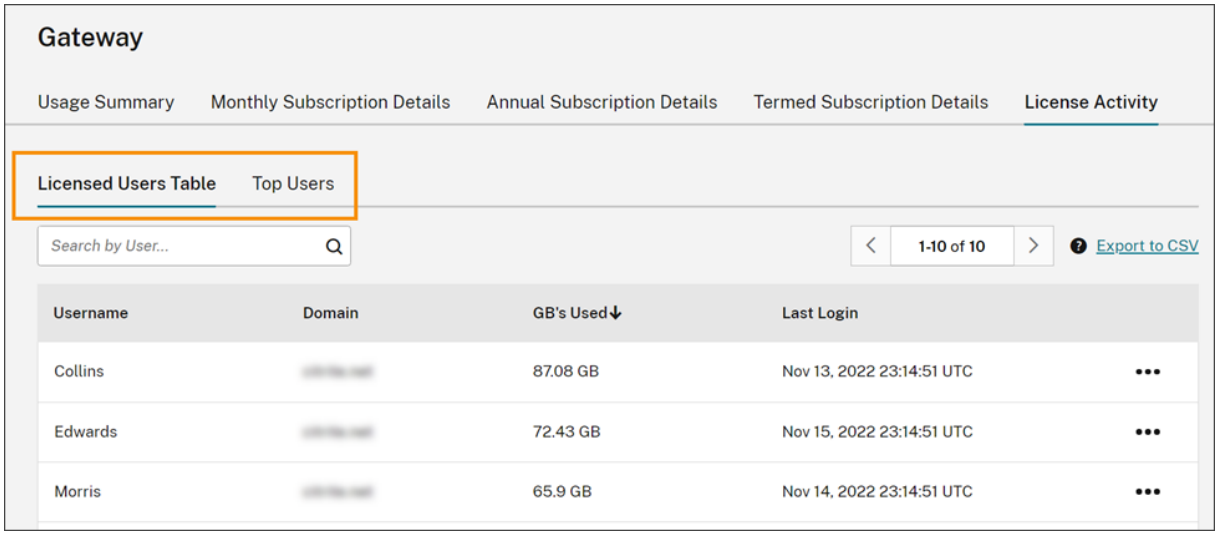
すべてのサブスクリプションの種類について、［使用状況の傾向］グラフのバーにマウスオーバーすると、その時点での帯域幅の使用状況がアクセス別に分類されて表示されます。



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：

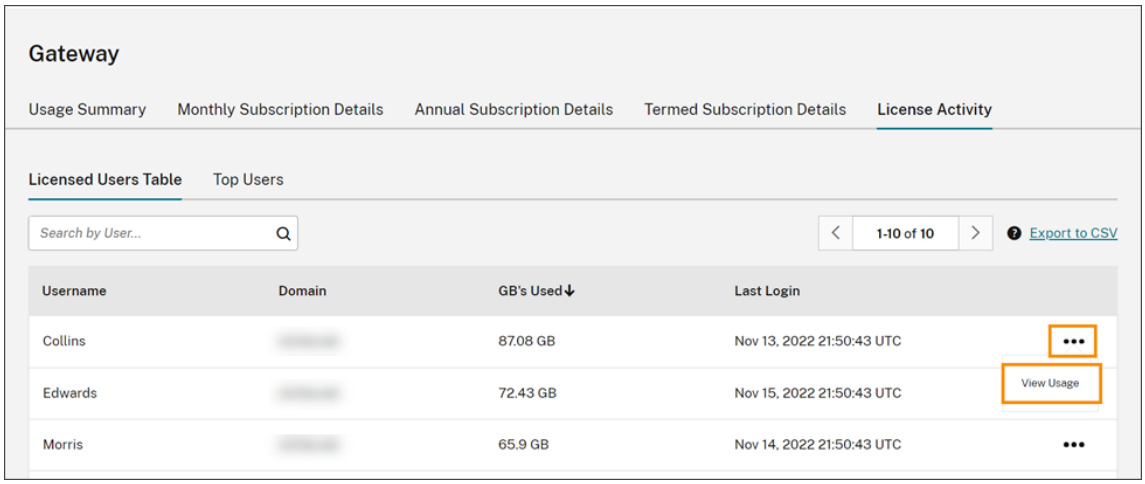
- ライセンス使用ユーザー：ライセンスが割り当てられた個々のユーザーの一覧が表示されます。この一覧には、各ユーザーが属するドメイン、過去 30 日間に使用された帯域幅の量、帯域幅を使用するサービスをユーザーが最後に使用した日付が含まれます。
- 上位ユーザー：帯域幅の使用状況に応じて、上位 10 人のユーザーの一覧が表示されます。この一覧には、アクセスの種類（Citrix DaaS またはサイトアグリゲーションを介したオンプレミスの Virtual Apps and Desktops）に応じた、過去 30 日間の各ユーザーの使用量の内訳が含まれます。



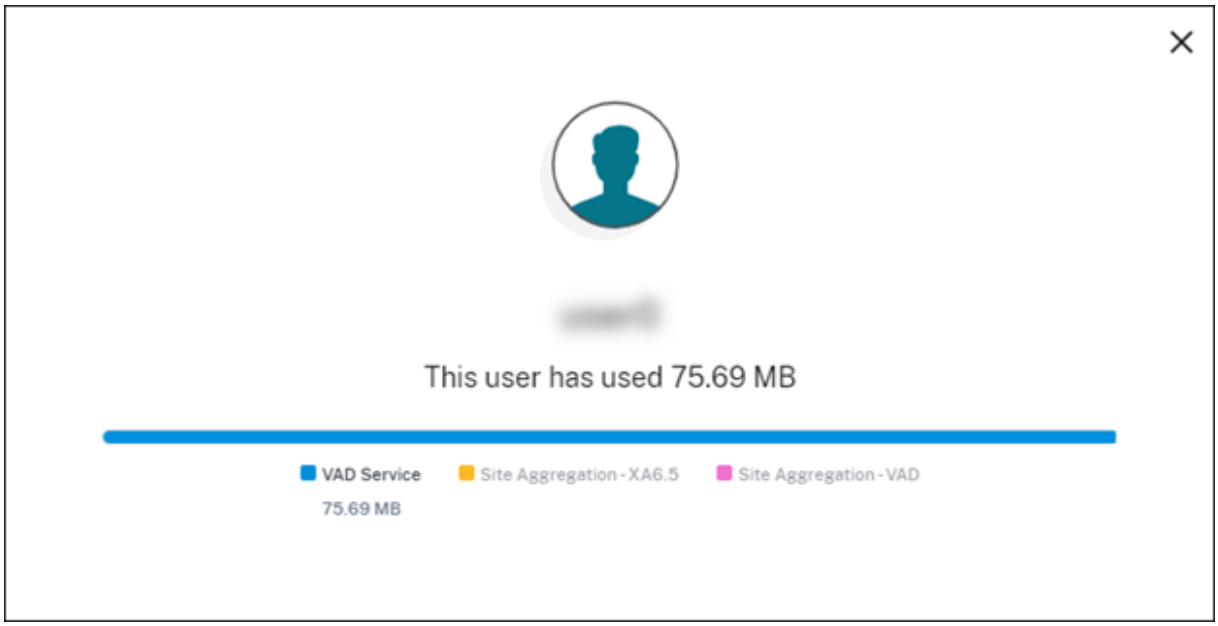
Citrix Cloud では、特定のユーザーがライセンスを使用しなくなった場合でも、過去 30 日間の帯域幅の使用状況が表示されます。Gateway サービスのサブスクリプションの有効期限が切れても、個々のユーザーが 30 日間で消費した帯域幅が表示されます。

特定のユーザーの使用状況の詳細を表示する

1. ［ライセンス使用ユーザーテーブル］を選択し、一覧で表示するユーザーを見つけます。
2. ページの一番右にある省略記号（…）メニューの ［使用状況を表示］を選択します。

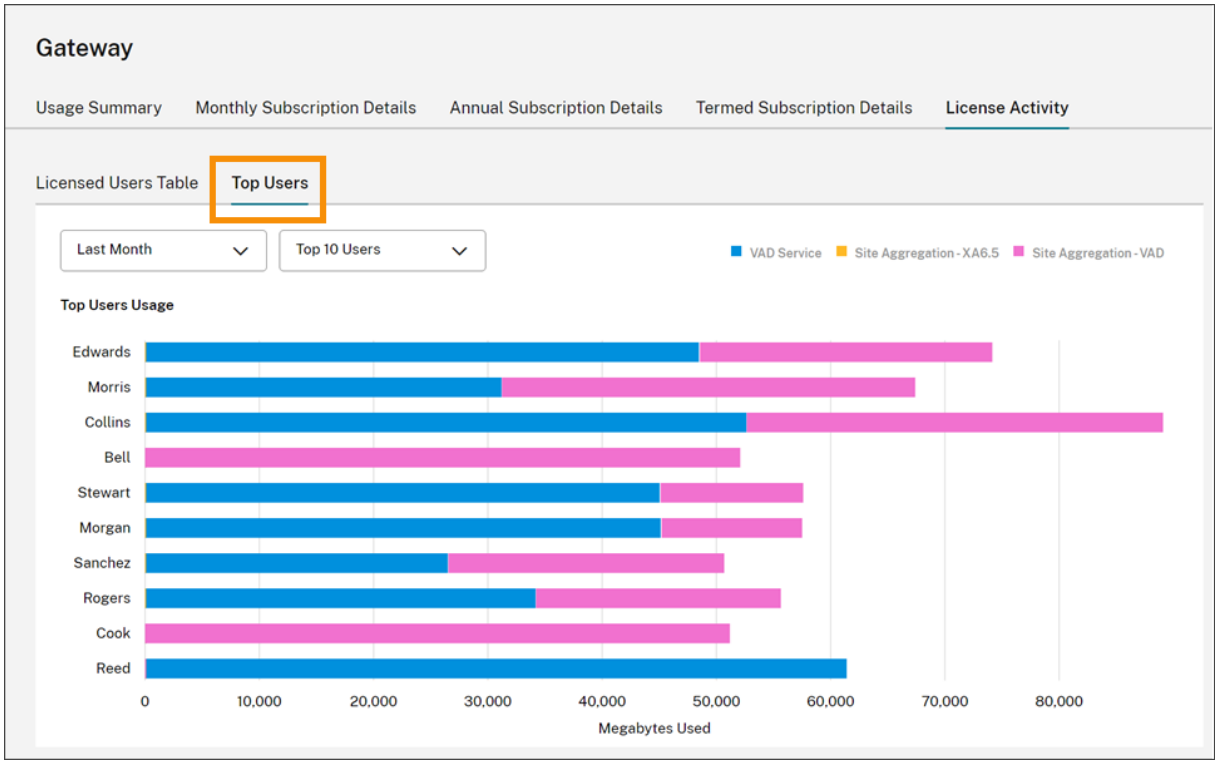


Citrix Cloud では、ユーザーの帯域幅がアクセス別に表示されます。



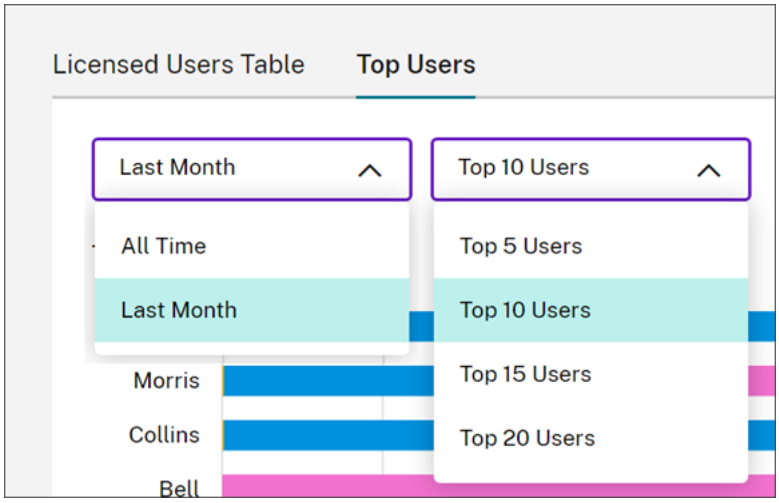
上位ユーザーの使用状況の詳細を表示する

［上位ユーザー］を選択します。



Citrix Cloud では、上位ユーザーの帯域幅の使用状況がアクセス別に分類されたグラフが表示されます。

デフォルトでは、［上位ユーザー］のグラフに、過去 30 日間で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。このビューを変更して、上位 5 人、上位 15 人、または上位 20 人のユーザーを表示できます。期間を［全期間］に変更することもできます。これにより、サブスクリプションの全期間の上位ユーザーが表示されます。このビューを変更するには、各メニューからオプションを選択します。



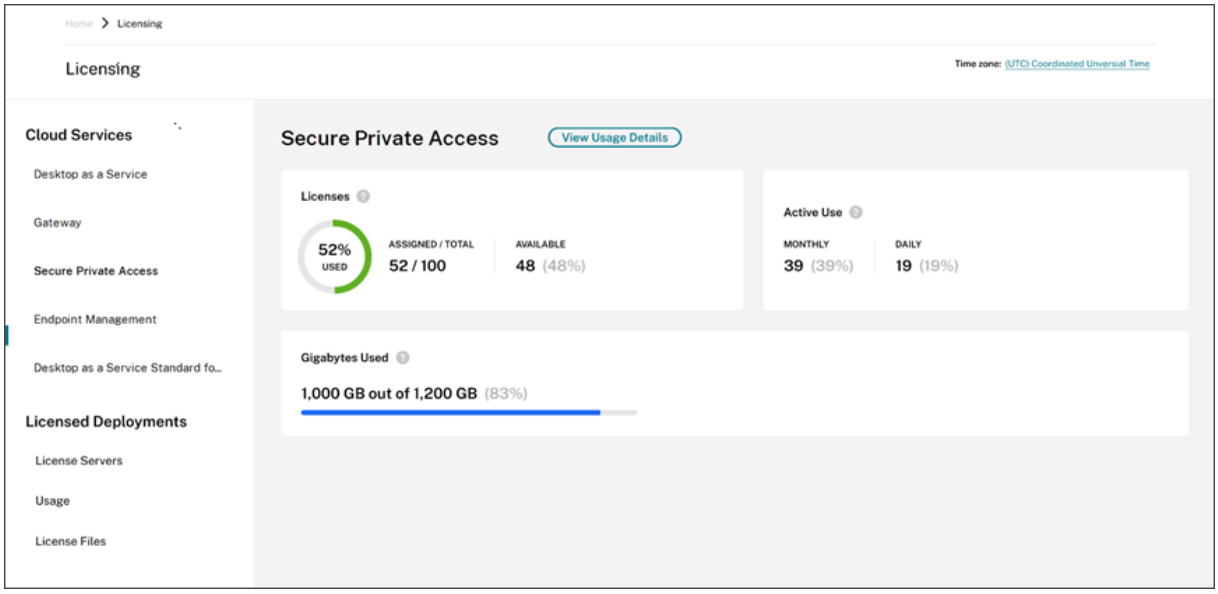
Secure Workspace Access のライセンスと使用状況の監視

November 30, 2023

ライセンス割り当て

ライセンスは、一意のユーザーが Web アプリや SaaS アプリ、または TCP アプリや UDP アプリを初めて起動したときに割り当てられます。

ライセンスの概要



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の合計パーセンテージ。
  - 割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、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の統計:
  - 月次のアクティブな使用状況とは、過去 30 日間にサービスを使用した一意のユーザー数を指します。
  - 日次のアクティブな使用状況とは、過去 24 時間以内にサービスを使用した一意のユーザー数を指します。
- すべてのサブスクリプションの帯域幅の合計量のうち、消費された帯域幅の量。

- 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 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。

使用されるライセンスと帯域幅

Secure Private Access Advanced サブスクリプションの場合、各ユーザーは 1 か月あたり 5GB の帯域幅にアクセスできます（ユーザーあたり 60GB/年）。Secure Private Access Standard サブスクリプションの場合、各ユーザーは 1 か月あたり 1GB の帯域幅にアクセスできます（ユーザーあたり 12GB/年）。この帯域幅は、複数のライセンスにまたがって、サブスクリプション期間中、プールされます。

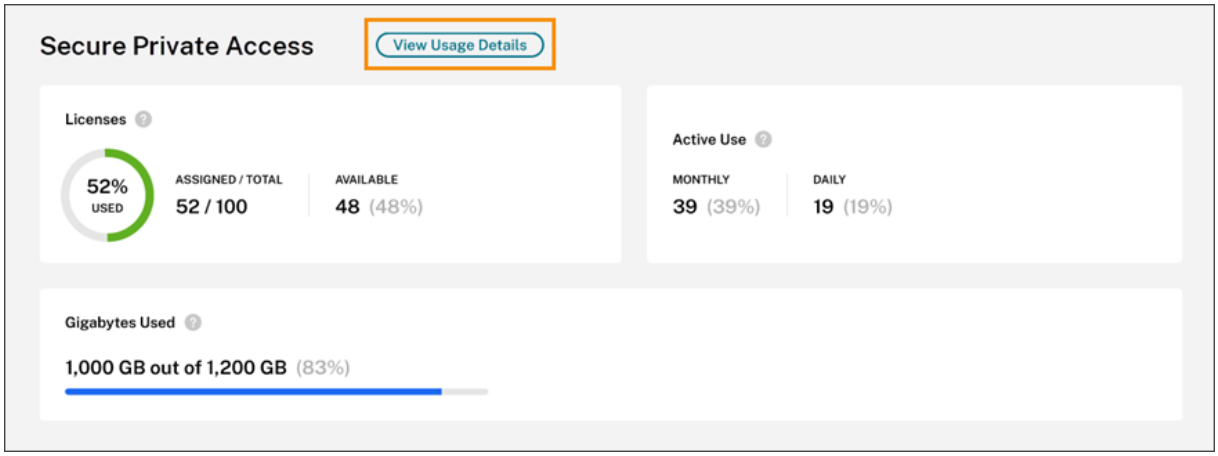
たとえば、3 年間で 100 ライセンスを購入した場合、合計帯域幅は 18000GB になります（3 年間で年間 6000GB）。この帯域幅は、3 年間、すべてのライセンスユーザーに分散されます。さらにサブスクリプションを購入すると、Citrix Cloud ではすべてのサブスクリプションのライセンスの総数と帯域幅が表示されます。

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、Citrix Cloud では更新時に未使用の帯域幅が引き継がれません。サブスクリプションの有効期限が切れたときに購入した帯域幅を超えて使用した場合、サブスクリプションを更新したときに使用可能な帯域幅の量はゼロのままです。

期間が重複する複数のサブスクリプションがある場合、各サブスクリプションの有効期限が切れると、各サブスクリプションに関連付けられた帯域幅の量が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 では両方のサブスクリプションの合計ライセンス数と合計帯域幅が表示されます。最初のサブスクリプションの有効期限が切れると、Citrix Cloud で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が表示されます。

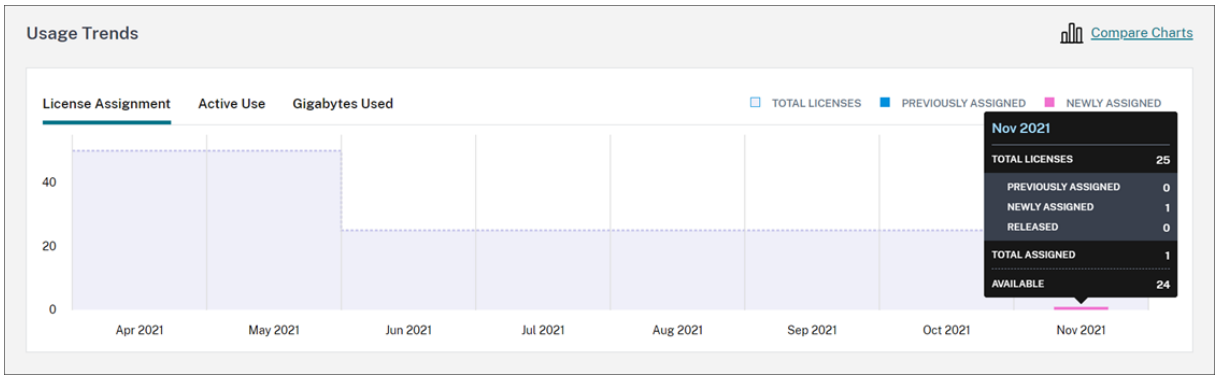
使用状況の傾向

帯域幅の使用状況とライセンスの詳細を表示するには、［使用状況の詳細の表示］をクリックします。



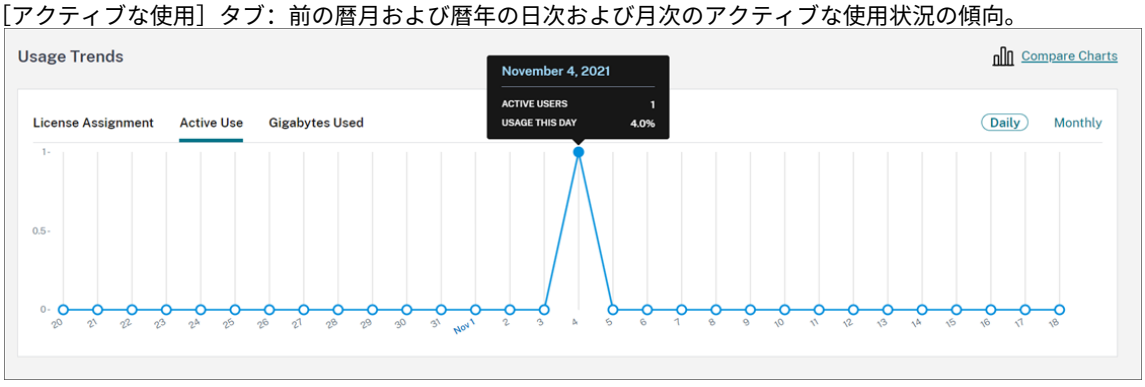
Citrix Cloud は、ユーザーがアクセスできるアプリの種類に基づいて帯域幅消費の内訳を表示します。

使用状況の傾向、およびクラウドサービスのライセンスと帯域幅を使用している個々のユーザーの内訳も確認できます。

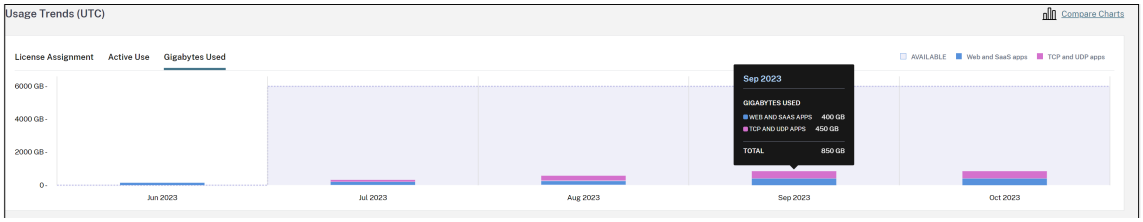


この内訳では、［使用状況の傾向］に次の情報が表示されます：

- ［ライセンス割り当て］タブ：
  - ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
  - 事前割り当て済み：月ごとの初めに既に割り当てられているクラウドサービスライセンス。たとえば、7 月にユーザー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［事前割り当て済み］の数にカウントされます。
  - 新しく割り当て済み：各月に割り当てられたライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］の数にカウントされます。
- ［アクティブな使用］タブ：前の暦月および暦年の日次および月次のアクティブな使用状況の傾向。



- ［使用帯域幅（**GB**）］タブ：使用可能な合計帯域幅のうち消費された帯域幅の量。ユーザーごとの使用状況と、Web アプリや SaaS アプリ、TCP アプリや UDP アプリなどのアプリケーションごとの情報が表示されます。

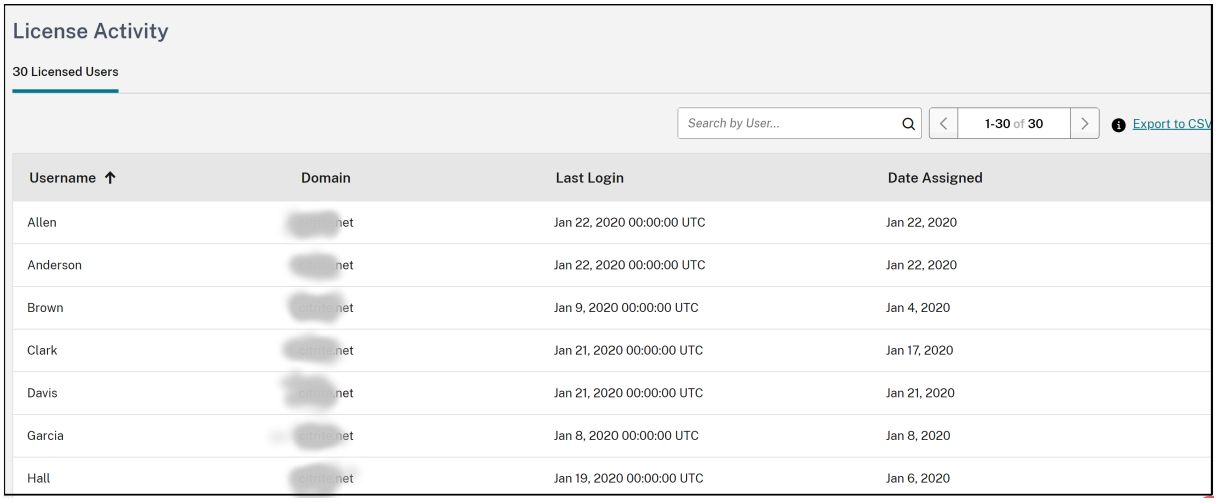


ライセンスの割り当て、アクティブな使用、および帯域幅の使用状況の傾向を比較するには、［グラフの比較］を選択します。

> 注:
>
> 使用状況の傾向は、現在のサブスクリプション期間中、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:



- ライセンスを割り当てた個々のユーザーのリスト。
- ユーザーが所属するドメイン。
- ユーザーが最後にサービスを使用した日付。
- ライセンスがユーザーに割り当てられた日付。

割り当て済みライセンスを解放する

過去 30 日間、サービスが使用されていない場合、Citrix Cloud はそのライセンスを自動的に解放します。Citrix 管理者がライセンスを解放するために操作する必要はありません。

ライセンスが解放されると、それに応じて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ログインして使用することによって、別のライセンスを取得できます。

Citrix DaaS の Citrix Managed Azure リソース消費の監視

October 4, 2023

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の使用権を購入すると、Citrix Managed Azure サブスクリプションのリソースを使用できる Citrix Azure Consumption Fund を購入することもできます。これらのリソースを使用して、オンプレミス VDA と一緒にアプリとデスクトップをユーザーに配信できます。

Citrix Azure Consumption Fund を購入すると、次のいずれかの方法を使用して消費分の支払いを行うことができます:

- 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、翌月に Citrix から請求を受けます。Citrix Cloud で、使用量は超過分として表示されます。
- 前払い消費：月間または年間（契約期間）ベースで消費量の前払いを行うことができます。前払い消費分を超えた使用量について、この使用量は Citrix Cloud で超過分として表示されます。超過分については、翌月に Citrix から請求を受けます。

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、使用する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を使用します。Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure）の消費量とライセンスのコストを見積もるには、Licensing and Consumption Calculatorを使用します。

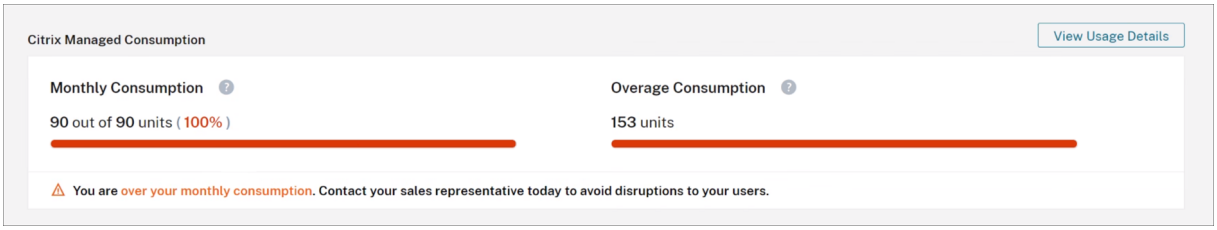
サポートされている製品

消費量の監視は、次のエディションの Citrix DaaS で利用できます:

- Citrix DaaS Advanced（旧称 Virtual Apps Advanced）
- Citrix DaaS Premium（旧称 Virtual Apps Premium）
- Citrix DaaS Advanced Plus（旧称 Virtual Apps and Desktops Advanced）
- Citrix DaaS Premium（旧称 Virtual Apps and Desktops Premium）
- Citrix DaaS Standard for Azure（旧称 Virtual Apps and Desktops Standard for Azure）

消費の概要

[Citrix 管理対象ライセンス消費］セクションには、Consumption Fund で使用した単位の概要が表示されます。



[消費（月単位）］には、購入した月間 Consumption Fund 単位の総数のうち、当月に使用した消費単位の数が表示されます。月間消費量は毎月リセットされます。未使用の消費単位は翌月に繰り越されません。

［消費（契約期間）］には、購入した期間 Consumption Fund 単位の総数のうち、使用した消費単位の数が表示されます。月間消費単位と同様に、未使用の期間消費単位は翌年に繰り越されません。

［超過消費］には、Azure Consumption Fund の単位の数を超えて使用した消費単位の数が表示されます。Citrix Managed Azure リソースを従量課金制で使用する場合、デフォルトでは、消費量は超過分として表示されます。

超過分の測定方法

Azure Consumption Fund を従量課金制で使用する場合、Citrix Cloud では、当月に使用した消費単位の数が超過分として表示されます。

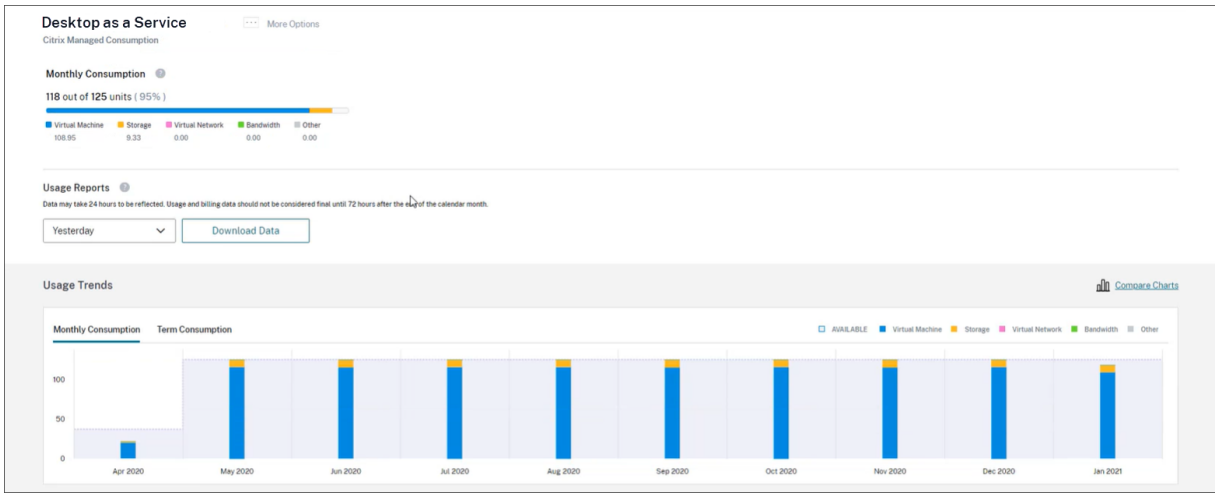
月間または年間ベースで消費量の前払いを行った場合、Citrix Cloud では、現在の月または年に使用した月間または期間の消費単位の数が表示されます。購入した単位よりも多くの単位を消費した場合、Citrix Cloud では超過した単位が超過分として表示されます。

月間ベースと年間ベースの両方で消費量を前払いした場合、まず、購入した月間単位に対して消費量が測定されます。これらの単位が消費された後、消費量の測定は年間単位に対して行われます。これらの単位が消費された後、消費した超過単位はすべて超過分として表示されます。

消費単位を追加購入し、かつアカウントに超過分が既にある場合、新しい消費単位は超過分には適用されません。新しい消費単位は、それらの単位の購入後に発生する使用分にのみ適用されます。

消費の詳細

消費単位の詳細を表示するには、概要の右端にある ［使用状況の詳細の表示］をクリックします。詳細ページには、消費量と使用状況の傾向の内訳が表示されます。



使用状況レポート

使用情報を、CSV ファイルとして、指定した間隔でダウンロードできます。[**Download Data**] をクリックし、CSV ファイルを生成して、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データに反映されるまで、1 日または 1 か月の終わりから最大 72 時間を要することがあります。

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使用可能な消費単位、合計使用料金、および保留中の超過分を示すレポートの要約。

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の合計使用料金、月単位および契約期間の残高、および超過料金を示す日次の概要。

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

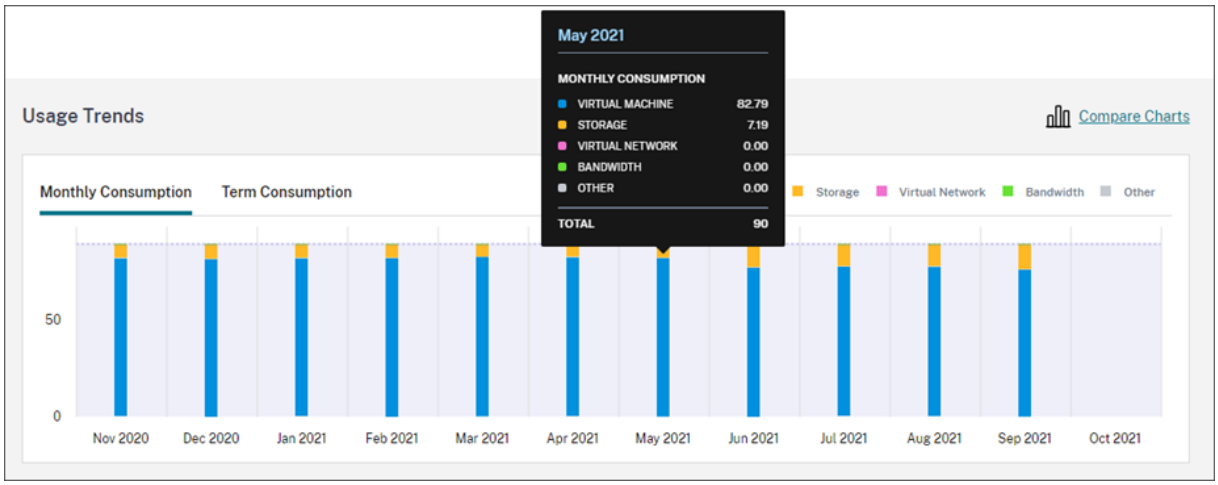
- レポートの日付範囲の各日の Azure VM、ネットワーク接続、Azure ストレージ、および帯域幅の従量制の使用量。

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

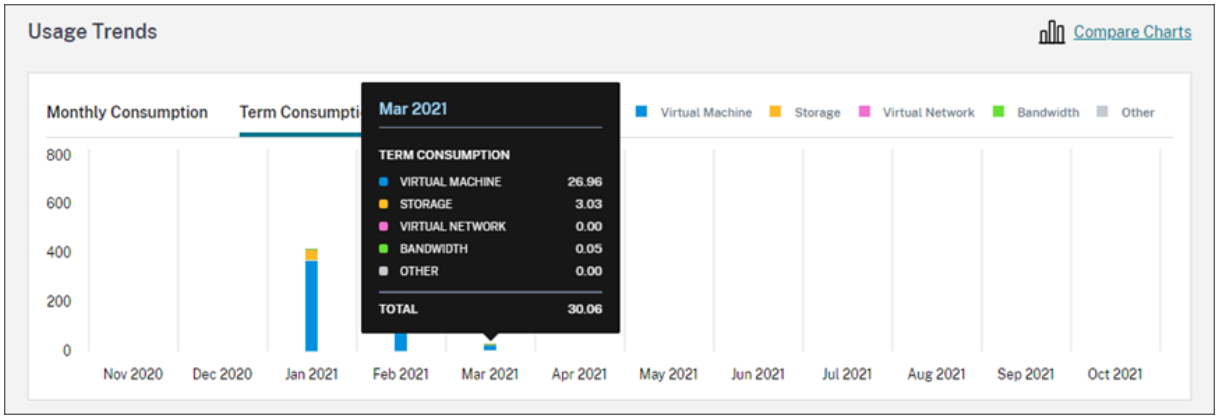
使用状況の傾向と消費アクティビティ

［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。グラフのバーにマウスを合わせると、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量が表示されます。

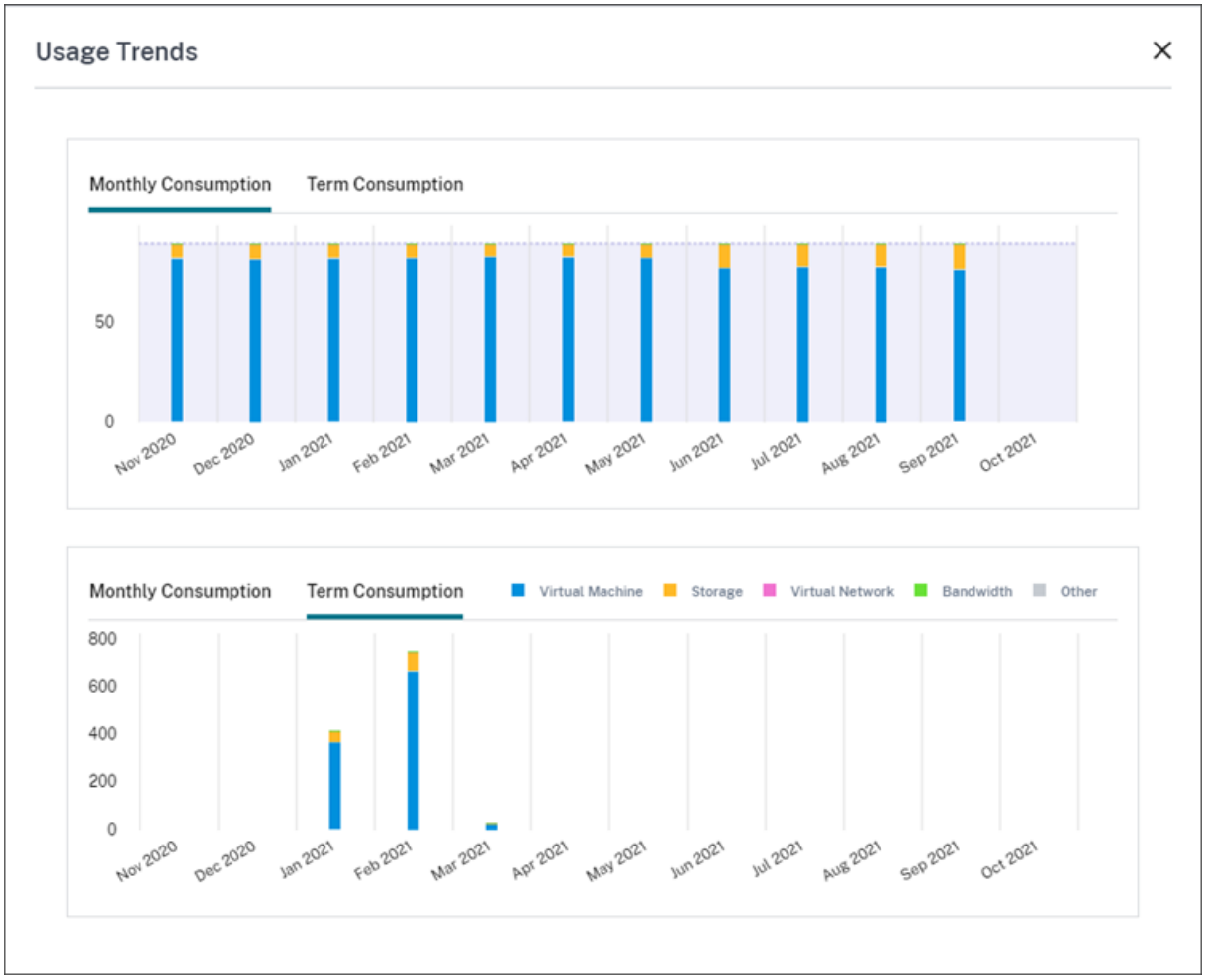
過去 12 か月分の月間消費量を表示するには、［消費（月単位）］を選択します。



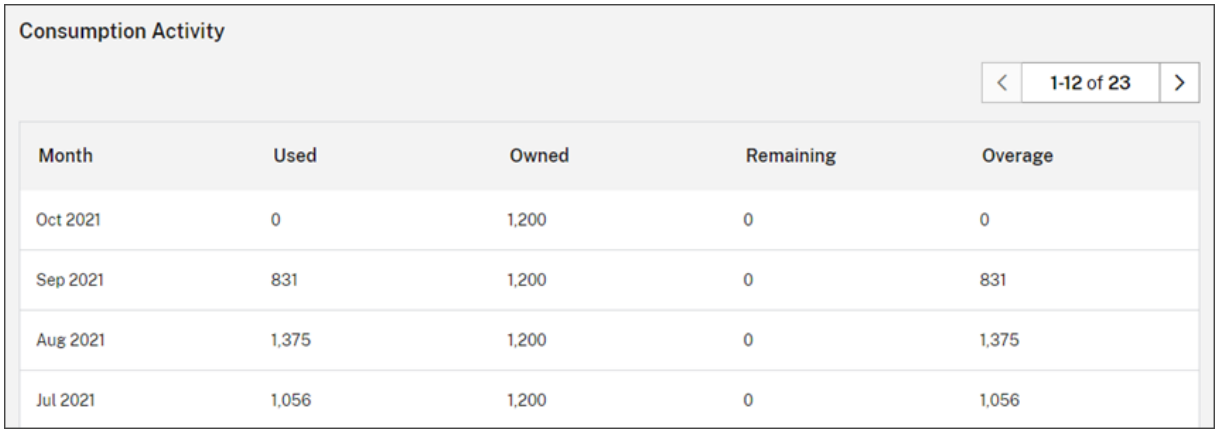
前年の各月の期間消費を表示するには、［消費（契約期間）］を選択します。



月次と年次の両方の消費単位を購入した場合は、グラフの右端にある ［グラフの比較］を選択すると、月次と期間の消費傾向が 1 つのビューで表示されます。



［消費アクティビティ］セクションには、各月の消費単位のリストも表示されます。



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：各月に使用された単位の数。
- 所有中：各月に購入した単位の総数。
- 残り：各月に使用されなかった購入済み単位の数。
- 超過：各月に購入した単位を超えた消費単位の数。

割り当て済み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 Consumption Fund の単位によって異なります。

次の場合、30 日後に非アクティブなライセンスを解放できます：

- サービス環境で、Citrix Managed Azure サブスクリプションを使用しない。
- サービス環境で使用するために、年間消費単位を購入した。

次の場合、ユーザーまたはデバイスがアプリまたはデスクトップを起動していなければ、当月中に非アクティブなライセンスを解放できます：

- サービス環境で使用するために、月間の Consumption Fund 単位を購入した。
- 月次および年次の両方の Consumption Fund 単位を購入した。

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：

- Citrix 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する
- Citrix DaaS Standard for Azure：割り当て済みライセンスを解放する

オンプレミス展開のライセンスと使用状況の監視

October 4, 2023

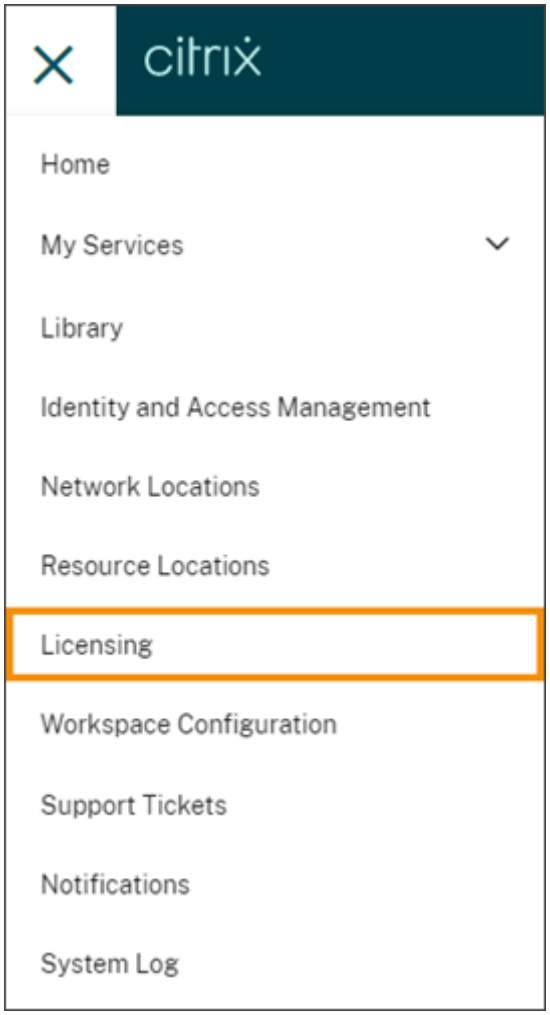
Citrix Cloud のライセンス割り当て済み展開画面には、次の機能があります：

- 製品登録：既存の Citrix ライセンスサーバーを Citrix Cloud に登録して、展開に関する使用状況の分析情報とレポートを追加で取得できます。
- ライセンスサーバーの状態：Citrix ライセンスサーバーの状態を表示して、使用状況を正常に報告しているサーバーと、Citrix Cloud に最後に使用状況を報告した日時を把握できます。
- 使用状況の分析情報：Citrix ライセンスサーバー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表示して、ライセンス使用傾向の履歴を把握できます。

サポートされている製品

Citrix ライセンスサーバーの使用状況の分析情報は、同時使用ライセンスモデルおよびユーザー/デバイスライセンスモデルで Virtual Apps and Desktops のすべてのエディションに関して利用できます。

Citrix ライセンスサーバーの使用状況の分析情報を表示するには、コンソールメニューで ［ライセンス］を選択し、［ライセンス割り当て済みの展開］を選択します。



前提条件

Citrix ライセンスサーバーの使用状況の分析情報を使用するには、次の要素が必要です:

- Citrix ライセンスサーバーバージョン 11.15.0.0 以降
- Citrix Cloud アカウント
- Citrix ライセンスサーバーから Citrix Cloud へのネットワークアクセス

接続の要件

ライセンスサーバーを 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ます:

- `https://citrix.cloud.com/` （管理コンソールにアクセスしてコードを入力し、ライセンスサーバーのステータスを表示する場合）
- `https://trust.citrixnetworkapi.net`（コードを取得する場合）
- `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場合）
- `https://cis.citrix.com`（データをアップロードする場合）
- `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 への接続

Citrix ライセンスサーバーの使用状況の分析情報を有効にするには、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の分析情報を有効にします。詳しくは、ライセンス製品ドキュメントの「使用統計の共有」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、アドレスが接続可能であることを確認します。Citrix ライセンスサーバーにプロキシサーバーを使用している場合、プロキシサーバーがライセンス製品ドキュメントの「手順 5 プロキシサーバーの構成」の手順どおりに構成されていることを確認します。
3. 「Citrix Cloud を使用するオンプレミス製品の登録」の手順どおりに、ライセンスサーバーを Citrix Cloud に登録します。

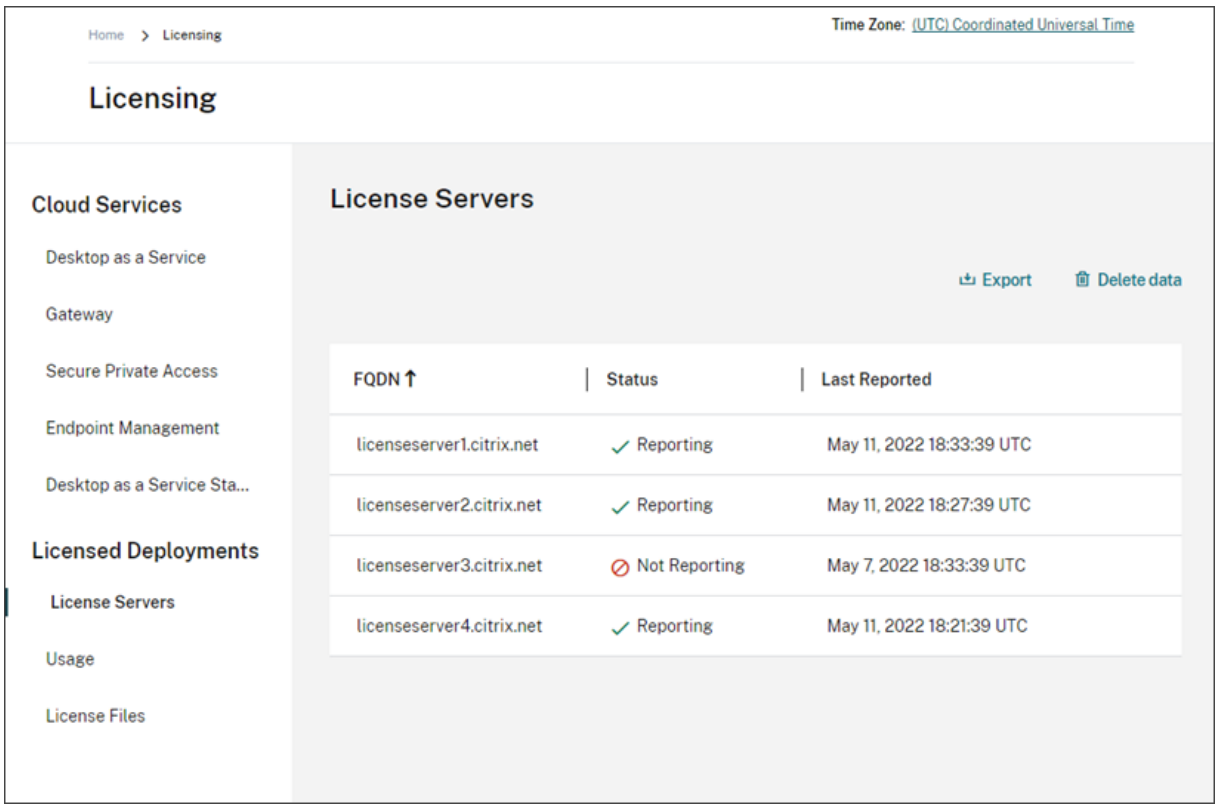
オンプレミス製品ライセンスの使用状況の表示

Citrix ライセンスサーバーの使用状況の分析情報により、Citrix 資産全体のライセンス使用状況を表示できます。以下の場合に役立つ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、およびこれらのサーバーが使用状況情報を Citrix Cloud に報告しているかどうかを把握できます。
- Virtual Apps and Desktops の同時使用ライセンスとユーザー/デバイスライセンス使用状況を表示できます。
- 複数展開の同時使用ライセンスとユーザー/デバイスライセンス使用状況が集約された分析情報を得ることができます。
- 過去のライセンス使用状況の傾向と毎月のライセンス使用状況の傾向を把握できます。
- 特定のユーザーの最終ログイン時間を表示できます。
- Citrix ライセンスサーバー全体で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の数を比較できます。
- ライセンスの超過使用保護を監視できます。
- 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できます。

ライセンスサーバーの状態の表示

ライセンスサーバーの状態には、Citrix Cloud に使用状況を報告する各ライセンスサーバーが表示されます。



ライセンスサーバーは、過去 3 日間に使用状況を Citrix Cloud に正常にアップロードしている場合、「レポート」状態を表示します。過去 30 日間の使用状況を報告し、過去 3 日間は報告していない場合、「レポートを送信していません」状態を表示します。過去 30 日間に使用状況が報告されていないライセンスサーバーは、一覧から削除されます。

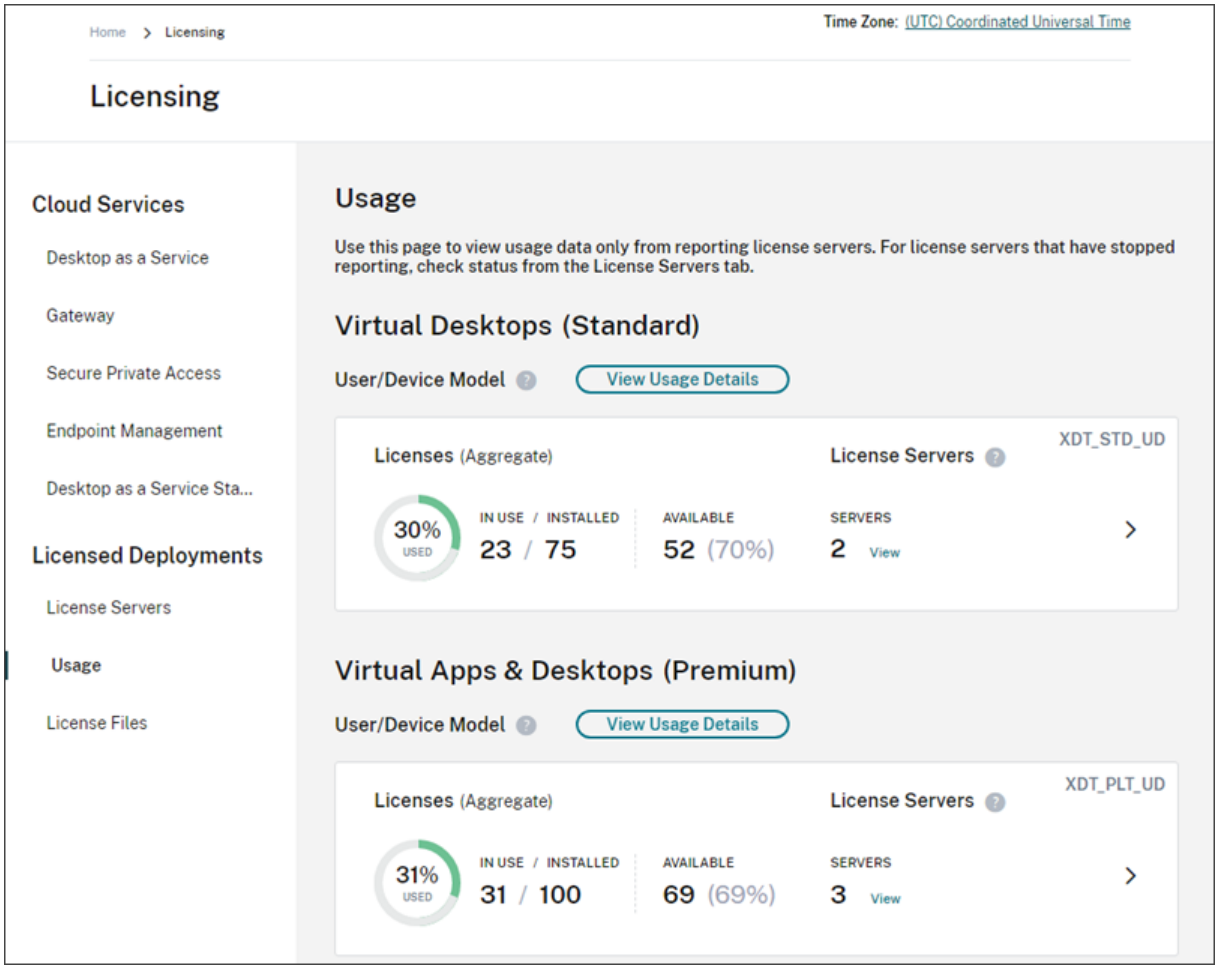
ライセンスサーバーの状態がライセンス使用状況表示に与える影響

ライセンスサーバーのレポートの状態と［最新レポート］の日付によって、使用状況の分析情報の表示およびレポートに特定のライセンスサーバーの使用状況が含まれるかどうかがわかります。

- 現在インストールされているライセンスおよび使用されているライセンスは、レポートライセンスサーバーからのデータのみに基づいて表示されます。ライセンスサーバーが「レポートを送信していません」として表示されている場合、このライセンスサーバーからインストールされているライセンスおよび使用されているライセンスは、使用状況の分析情報の画面に反映されません。
- 各ライセンスサーバーの［最新レポート］日によって、使用状況の分析情報の画面で表示されるライセンス使用状況の情報がどのくらい新しいかを判断できます。表示されるライセンス使用状況レポートは、各ライセンスサーバーの［最新レポート］時刻の時点での内容です。
- 使用状況の分析情報用に構成され、Citrix Cloud に登録された Citrix ライセンスサーバーは、1 日に 1 回使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。

ライセンス使用状況

［使用状況］タブは、Citrix 展開全体でのライセンス使用状況の統合ビューを提供します。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、シングルビューに結合されます。このビューを使用すると、さまざまな展開およびライセンスサーバー全体でのライセンスの概要を簡単に確認できます。

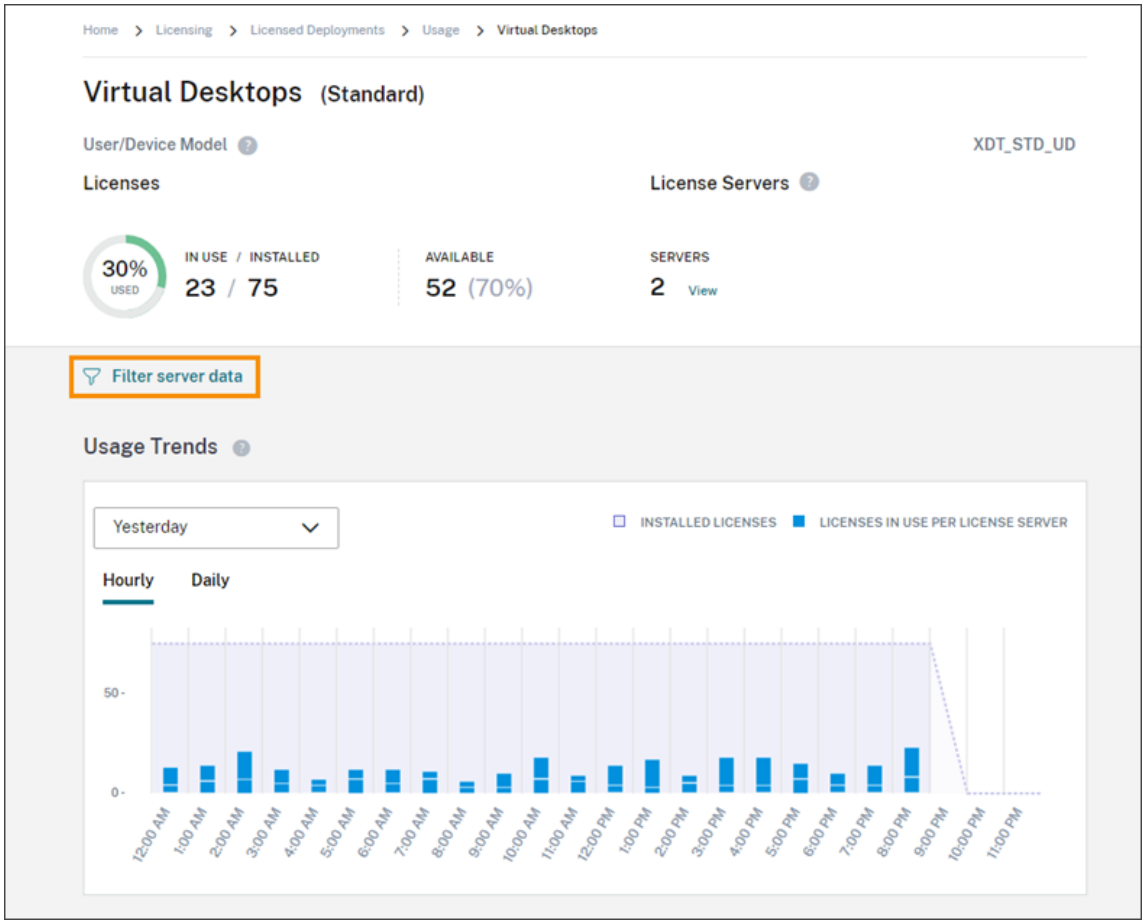


ライセンスの使用状況は、製品のエディションとライセンスモデルに基づいて、複数のライセンスサーバー間で整理および集約されます。すべてのレポートライセンスサーバーで検出された一意のライセンスエディションごとに、ライセンス使用状況の概要カードが表示されます。検出された製品エディションごとに概要カードが表示されます。

ライセンスサーバーごとの使用状況

各ライセンスサーバーの製品ライセンス使用状況は、サーバーデータをフィルタリングして表示することができます。

1. [使用状況] ページから、管理する製品の [使用状況の詳細の表示] を選択します。
2. [サーバーデータのフィルター処理] 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、選択したサーバーのみ、Citrix Cloud によって使用傾向、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が表示されます。

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

同時使用ライセンスのレポート内容は、次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。
- ピーク時のライセンス使用：特定の期間に使用されたライセンスの最大数。

ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次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 日間に同時使用されたライセンスの最大数。
- 今月：現在のカレンダー月に同時使用されたライセンスの最大数。
- 常時：ライセンスサーバーが Citrix Cloud に登録されてから同時使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上の使用中のライセンス数と一致しないことがあります。ライセンスサーバーが報告するのは、任意の時点で使用中のライセンス数だけです。Citrix Cloud は、これらの個別データポイントを受信して、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に対応し、詳細な情報を含みます。使用状況を監視するときは、次の考慮事項に留意してください:

- 使用情報は、各レポート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使用可能なライセンスが不足している場合は、ライセンスサーバーに追加のライセンスを割り当てて配置し、使用可能なライセンスの数を増やすことができます。
- Citrix ライセンスサーバーの使用状況の分析情報で利用可能な情報には、登録済みのアクティブなレポート用 Citrix ライセンスサーバーによって収集およびレポートされた情報のみが含まれます。ライセンス割り当て済みの展開環境は、実際に所有または購入したライセンスの総数ではないため、総数と一致しない場合があります。
- 使用可能なライセンスの割合は、レポート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の数に基づいて計算されます。

ライセンスサーバーの登録削除

ライセンスサーバーの登録を Citrix Cloud から完全に削除するには、次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。詳しい手順については、「ライセンスサーバーの登録削除」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［製品の登録］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。それでもライセンスサーバーが一覧に表示される場合は、「製品登録の削除」の説明に従ってサーバーを削除します。

利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、以前に収集された利用状況データは引き続き保存されます。このデータを保持する必要がなくなった場合は、削除できます。

> 重要:
>
> 利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。利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 は引き続き利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、削除による影響を理解していることを示す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 Provider 用のライセンス

July 2, 2024

Citrix Cloud の License Usage Insights サービスは、**Citrix Service Provider**（**CSP**）が製品のライセンスと使用状況を把握し報告するため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 サービスと呼ばれていました。Citrix DaaS Standard for Azure は、以前は Citrix Virtual Apps and Desktops Standard for Azure と呼ばれていました。一部の表示には、旧名称が含まれている場合があります。

LUI サービスでは、次のことを実行できます:

- Citrix ライセンスサーバーから製品使用情報を自動的に収集して集計する
- シングルテナントおよびマルチテナントの顧客の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 Virtual Apps and Desktops 展開環境にアクセスしているユーザーを簡単に確認する
- ライセンス使用状況に関する顧客の内訳を作成する
- 無料ユーザーを特定して追跡することにより、ライセンスコストを最適化する
- Citrix との過去のビジネス実績を表示し理解する
- Virtual Apps and Desktops と Citrix DaaS のライセンス使用状況、NetScaler VPX の割り当てデータ、および Citrix DaaS Standard for Azure のライセンスと消費データを 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 サービスの使用開始」を参照してください。

シングルテナントの顧客とマルチテナントのパートナーの集計された使用状況データを表示する方法については、「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）」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
- Citrix DaaS Standard for Azure の顧客ライセンスと使用状況の監視

License Usage Insights の使用開始

July 2, 2024

サポートされる Citrix 製品

License Usage Insights サービスは、以下の Citrix 製品の使用状況に関する情報を提供します:

- Virtual Apps and Desktops（オンプレミス）製品の使用状況
- Citrix DaaS Premium（旧称 Virtual Apps Premium および Virtual Apps and Desktops Premium サービス）
- Citrix DaaS Standard for Azure（旧称: Citrix Virtual Apps and Desktops Standard for Azure）
- NetScaler コンソール VPX の割り当て

要件

Citrix のオンプレミス製品のライセンスおよび使用状況の情報を取得するには、Citrix ライセンスサーバー 11.16.3.0 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 ライセンスサーバー 11.16.3.0 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収集機能: ライセンスサーバーには、ライセンスの動作と追跡を最適化する新しい機能が追加され、CSP をさらに適切にサポートできるようになりました。
- Call Home: ライセンスサーバーには、CSP パートナーの製品使用状況収集を自動化する Call Home 機能が含まれています。これらの機能は CSP パートナーに限定されており、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有効になります。

手順 1: Citrix ライセンスサーバーを更新する

バージョン 11.16.3.0 より古いライセンスサーバーを実行している場合は、License Usage Insights を使用する前に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シンプルかつ高速です。次の手順を実行します:

1. 最新のライセンスサーバーをダウンロードします。Citrix ライセンスサーバーの最新バージョンについて詳しくは、Citrix ライセンスサーバーのドキュメントを参照してください。
2. ライセンスサーバーをアップグレードします。
3. ライセンスサーバーごとにアップグレードプロセスを繰り返します。

手順 **2**：**My Citrix** の資格情報で **Citrix Cloud** にサインインする

サインインする前に、Citrix Cloud アカウントに登録する必要があります。「Citrix Cloud への登録」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時は、Citrix.com で Citrix ライセンスを割り当ててダウンロードするために使用した My Citrix 認証情報と同じ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宛てに、アカウントを確認するためのメールを送信します。

Citrix Cloud アカウントを使用する準備ができたら、メールアドレスとパスワードを使用してhttps://citrix.cloud.comにサインインします。

手順 **3**（オプション）：ライセンスサーバーにより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 のライセンスのチェックアウトに関連付けられたユーザー名が、安全に Citrix に送信されます。

ユーザー名の送信によって、CSP パートナーは License Usage Insights 機能、およびトライアル、テスト、管理用に製品を使用してい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フルに活用できます。

ユーザー情報は、単一の「ユーザー @ ドメイン」エントリのみです。それ以外の個人が識別可能なデータは送信されません。また、Citrix がこの情報を共有することはありません。

ユーザー名情報のアップロードに不安を覚えるパートナーは、ユーザー名の匿名化を有効にすることができます。有効にすると、ユーザー名の匿名化機能によって、アップロード前に安全で不可逆的なアルゴリズムを使用して、読み取り可能なユーザー名が一意の文字列に変換されます。

License Usage Insights サービスは、これらの一意の識別子を使用して、実際のユーザー名の代わりに製品の使用状況を追跡します。このアプローチにより、クラウドサービスのユーザーインターフェイスに実際のユーザー名が表示されることなく、サービスプロバイダーが月ごとの情報を活用できます。

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の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:\ProgramFiles\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml にあります。
2. ［構成］セクションで、次のように **UsageBasedBillingScramble** 設定を追加します：

```
<?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>
<!--NeedCopy-->
```

3. ファイルを保存します。

手順 **4**: **License Usage Insights** サービスを使用する

Citrix Cloud コンソールで、License Usage Insights サービスを見つけて ［管理］をクリックします。サービスの主な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。

追加の詳細

License Usage Insights とともに Citrix ライセンスサーバーを使用する場合は、次の点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が License Usage Insights 管理コンソールに表示されるまで、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、安全な方法で処理および保存され、後日 License Usage Insights がそのデータにアクセスできます。この処理が完了するまで最大 24 時間かかることがあります。
- デフォルトでは、Virtual Apps and Desktops または Citrix DaaS のライセンスのチェックアウトに関連付けられたユーザー名が、安全に Citrix に送信されます。
- ユーザー名の送信によって、CSP パートナーは License Usage Insights 機能、およびトライアル、テスト、管理用に製品を使用してい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フルに活用できます。
- ユーザー情報は、単一の「ユーザー @ ドメイン」エントリのみです。それ以外の個人が識別可能なデータは送信されません。また、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 についてサポートが必要な場合は、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. ［**My Support** に移動］を選択し、My Citrix 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メンバーが対応、サポートします。

よくある質問

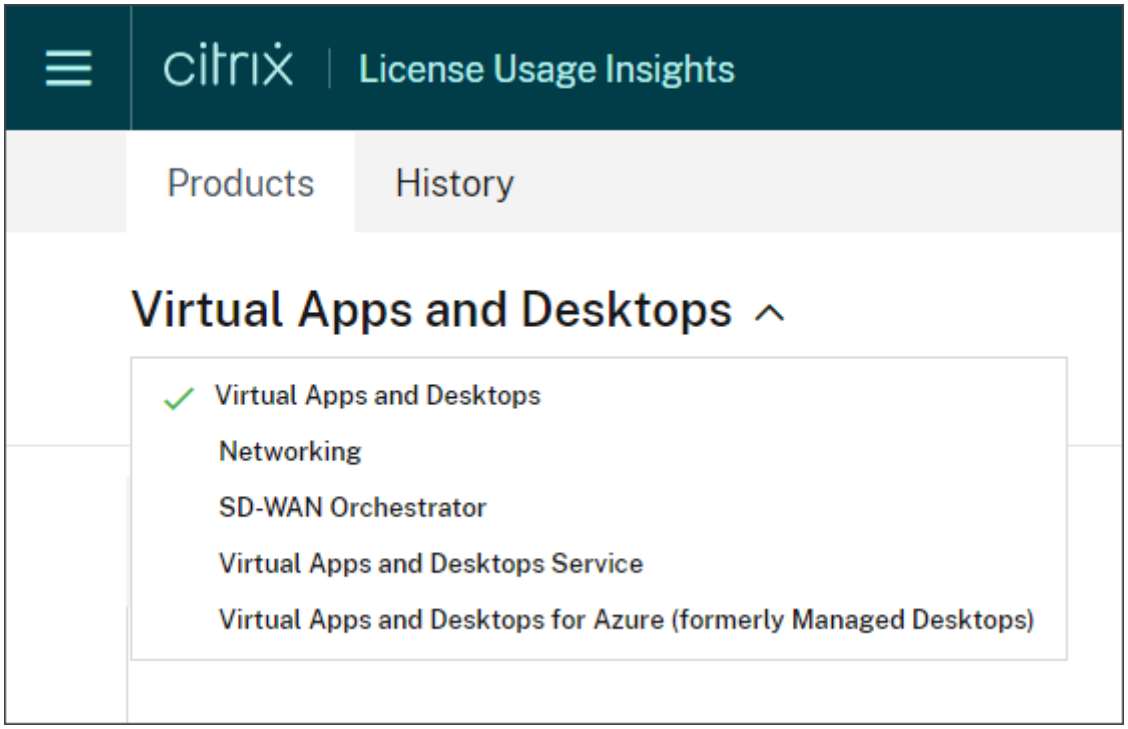
- どのような情報が送信されますか**?** ライセンスサーバーが **Citrix** に送信している情報を表示できますか**?** はい。Citrix に送信された情報のコピーを表示できます。詳しくは、「アップロードに含まれるライセンスサーバー情報」を参照してください。
- **Citrix Service Provider** ではない **Citrix** の顧客やパートナーは、**License Usage Insights** を利用できますか? いいえ。License Usage Insights を利用できるのは、パートナー契約がアクティブな Citrix Service Provider パートナーのみです。
- ライセンスサーバーで **Call Home** を無効にできますか? いいえ。Citrix Service Provider のライセンス契約の下では、すべてのライセンスサーバーが製品使用状況に関する情報を送信する必要があります。情報送信機能の使用に不安を覚えるパートナーは、ユーザー名の匿名化機能を使用できます。詳しくは、「ライセンスサーバーによるユーザー名の匿名化」を参照してください。
- 請求は **License Usage Insights** に表示される製品の使用状況に基づくものですか? いいえ。License Usage Insights はパートナーが製品使用状況を把握し、Citrix ディストリビューターに迅速かつ正確に報告するための機能です。Citrix Service Provider（CSP）パートナーへの請求は、これまで同様パートナーから Citrix ディストリビューターに報告する製品使用状況に基づきます。Citrix ディストリビューターと CSP パートナーとの請求関係に変更はありません。

製品の使用状況、ライセンスサーバー、通知の管理

July 2, 2024

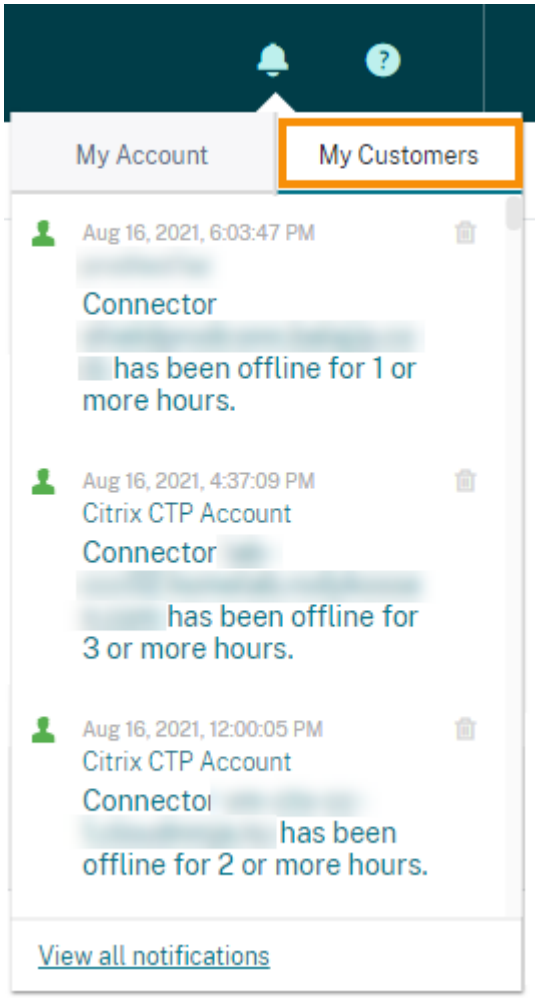
製品の選択

別の製品のライセンスの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、表示する製品またはサービスを選択します。



顧客通知

各展開環境に個別にアクセスすることなく、複数の顧客が使用するソリューションの正常性を監視します。Citrix Cloud の通知領域は、ダッシュボード上の顧客に関する通知が集約されるため、アラートが確実に対応され、サービスが中断なく実行されるようにすることができます。

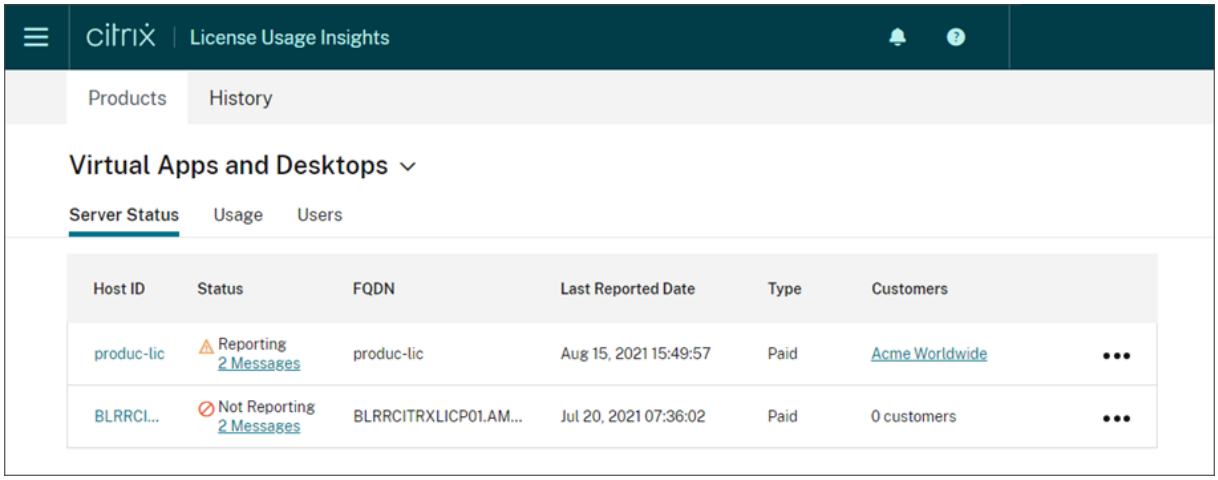


1. Citrix Cloud 管理コンソールで ［通知］アイコンをクリックし、［マイ顧客］をクリックします。最新の通知一覧が表示されます。
2. 顧客通知の全一覧を表示するには、［すべての通知を表示］をクリックします。

ライセンス サーバーの状態

Citrix Service Provider のライセンスガイドラインに準拠するには、アクティブなライセンスサーバーをすべて更新して報告する必要があります。ライセンスサーバーの状態として、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の情報が表示されます。

このサービスでは、Citrix のバックオフィスに格納されている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一覧を表示します。ライセンスサーバーが更新され、正常に報告が行われている場合、License Usage Insights は「報告」の状態を、最新のアップロード時刻とともに表示します。



アップロードに含まれるライセンスサーバー情報

Call Home がライセンスサーバー上でアクティブになると、次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
  - 製品機能およびエディションの使用権情報
  - ライセンス数量
- ライセンス使用状況:
  - 現在の暦月に使用されたライセンス
  - ライセンスのチェックアウトに関連付けられたユーザー名
  - アクティブ化された製品の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上に最後にアップロードされたペイロードを検査して、ライセンスサーバーが Citrix に送信する情報の詳細を完全に把握することができます。このペイロードのコピーは、ライセンスサーバー上に.zip ファイルとして保存されます。デフォルトでは、保存場所は C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip です。

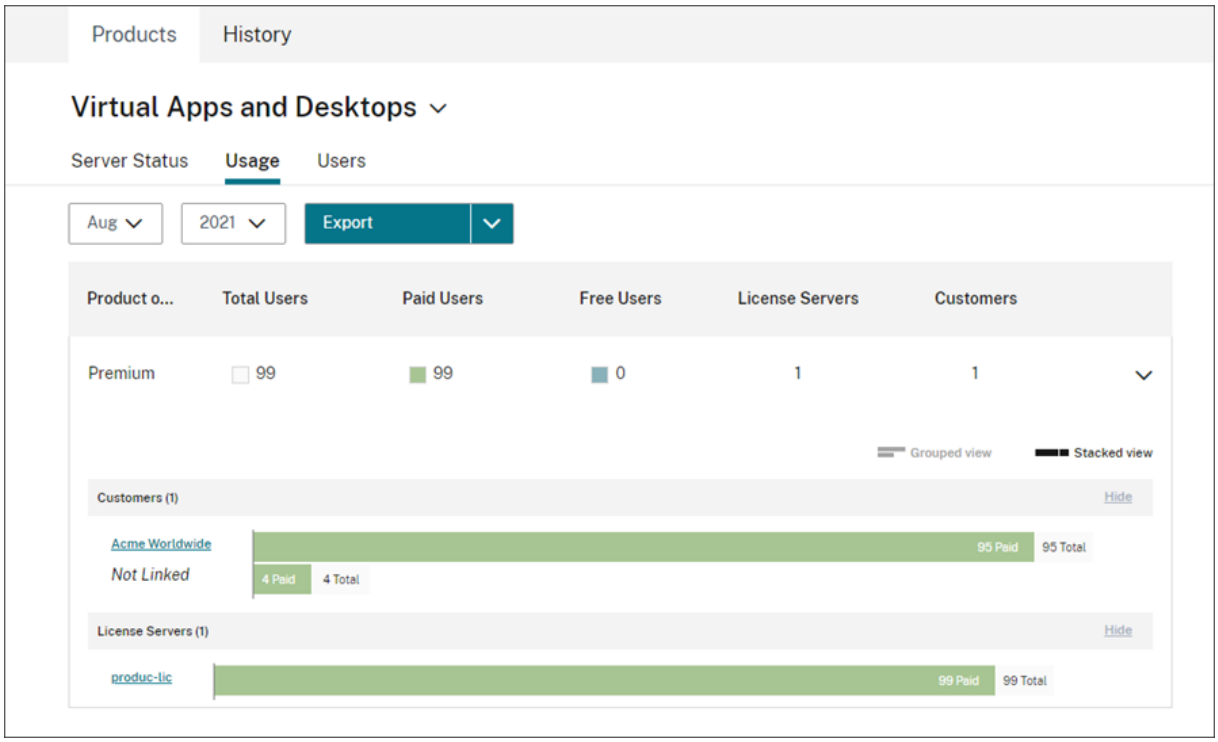
> 注:
>
> 成功したアップロードは最新のものを除いて削除されます。アップロードが成功するまで、失敗したアップロードはディスクに残ります。この場合、最新のアップロード以外すべてが削除されます。

使用状況収集

使用状況収集機能は、自動化されたデータ収集および集計によって製品の使用状況を把握するために役立ちます。追加のツールを展開する必要はありません。

License Usage Insights では、すべての Citrix ライセンスサーバーの製品使用状況を自動的に集計して表示するため、すべての環境の使用状況を完全に把握できます。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によって、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して追跡し、安全な送信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では、更新された使用状況データが常に提供されるため、時間を節約でき、パートナーが展開環境内の使用傾向をより適切に理解できるようになります。



Virtual Apps and Desktops 製品使用状況の顧客内訳の作成

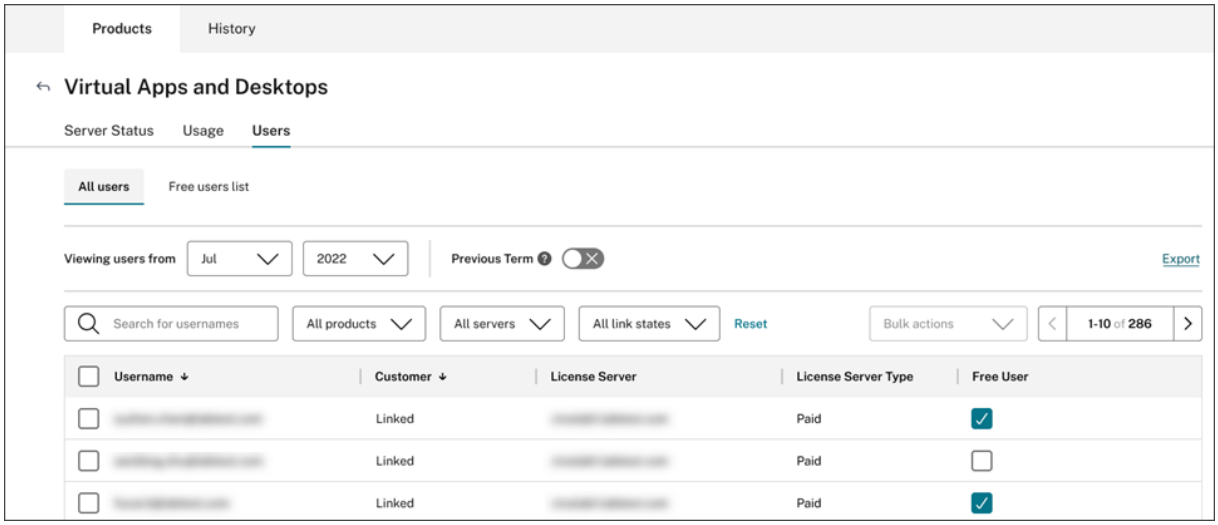
顧客ごとのライセンス使用状況内訳を作成するには、最初にユーザーを所属する顧客またはテナントに関連付ける必要があります。顧客ダッシュボードに顧客が定義されていない場合は、新しい顧客を追加したり、既存の Citrix Cloud 顧客に接続することができます。

1. 必要な場合は、［顧客］ダッシュボードに顧客を追加します：Citrix Cloud 管理コンソールのホームページで［顧客］を選択し、［追加または招待］をクリックして、画面の指示に従います。
2. メニューボタンをクリックし、［マイサービス］**>**［**License Usage Insights**］の順に選択します。
3. ［**Virtual Apps and Desktops**］製品を選択した状態で、［ユーザー］をクリックします。
4. 関連付けるユーザーを選択し、［一括操作］**>**［顧客へのリンクを管理］の順にクリックします。

5. 一覧から、ユーザーを関連付ける顧客を選択します。
6. [**Save**] をクリックします。
7. 顧客ごとの内訳を表示するには、[使用状況] タブをクリックします。

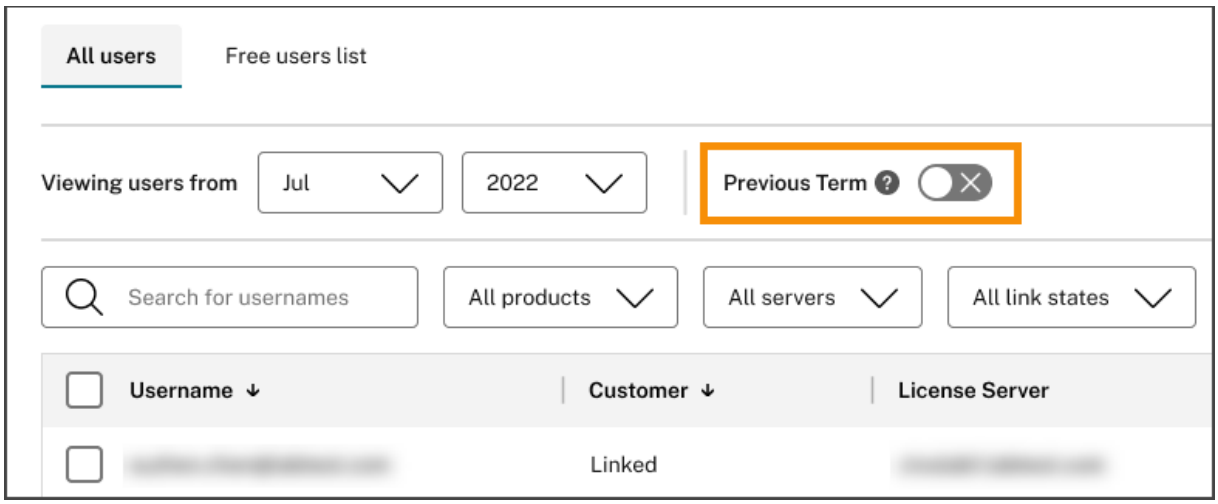
無料ユーザー管理

License Usage Insights では、トライアル、テスト、管理の各ユーザーをサポートする Citrix Service Provider ライセンスプログラムを最大限に活用しながら、すべての環境の製品使用状況を包括的に把握できます。



特定の請求サイクルで有料ユーザーに対して適切に請求されるようにするために、そのサイクル中に特定のユーザーを無料ユーザーとして指定できます。現在の請求サイクルの特定の月の間、翌月の 10 日まで、いつでも無料ユーザーを選択できます。たとえば、3 月の場合は 4 月 10 日までいつでも無料ユーザーを選択できます。

毎月 1 日から 10 日の間は、前の請求サイクルの無料ユーザーを選択することもできます。この期間中は、[前の期間] 設定をオンにして、その請求サイクルの無料ユーザーを選択できます。その月の 10 日を過ぎると、Citrix Cloud に [前の期間] 設定が表示されなくなります。



特定の月に選択した無料ユーザーは、有料ユーザーの請求時に計上されます。無料ユーザーのステータスを有料ユーザーに変更すると、Citrix は変更日を記録し、変更が発生した請求サイクルにそのユーザーを含めます。

ユーザー顧客のタグ付け

この機能は、シングルテナントとマルチテナントの両方のライセンスサーバーアーキテクチャの管理とレポートに関するサポートを含め、各顧客のライセンス使用状況データの内訳を提供します。License Usage Insight の対象は次のとおりです:

- ライセンスサーバー - 一覧上の「レポート送信中」のまたは「レポートを送信してません」のライセンスサーバー。
- ユーザー - Call Home の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 ライセンスの割り当て（VPX 一覧上の VPX）。

> 注
>
> ユーザー顧客のタグ付け機能は無料ユーザーのタグ付けと同じ動作で、CSP は翌月 10 日まで現在の請求サイクルで顧客タグ付けを更新できます。

無料サーバーのタグ付け

この機能により、管理者はライセンスへの影響を気にすることなく、特定の役割、場所、またはその他の関連基準に基づいてサーバーを編成および識別できるため、Citrix Cloud 環境内のリソース管理に柔軟性がもたらされます。

> 注
>
> CSP は、当月の無料のタグ付けまたは顧客のタグ付けを排他的に変更でき、変更は当月と今後の月の両方に適用されます。

サーバー顧客のタグ付け

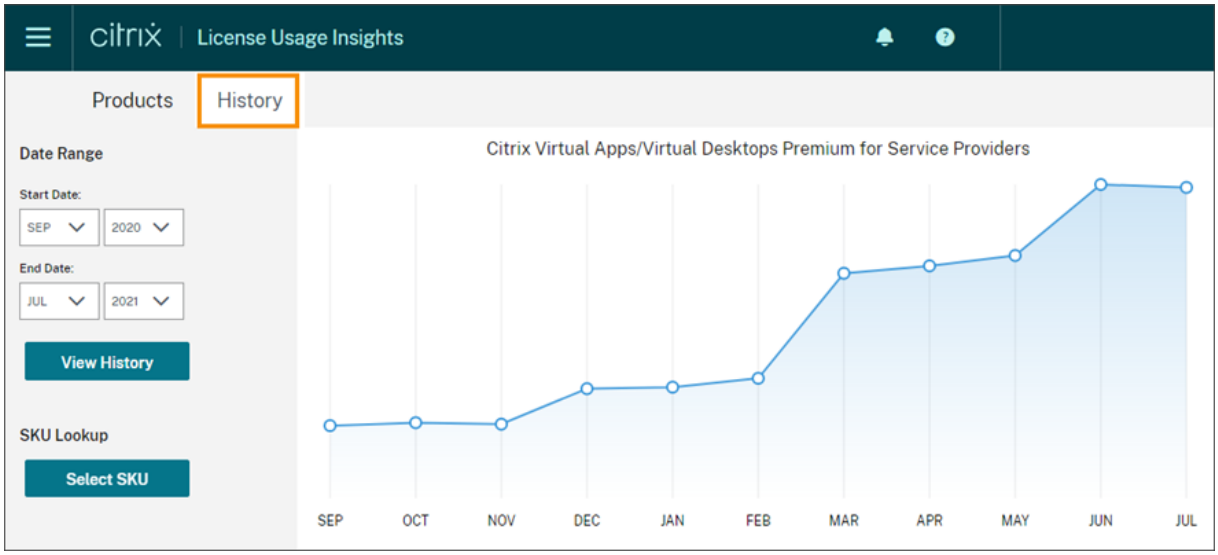
この機能により、Citrix Cloud 環境内のリソースの編成と管理能力が向上し、顧客固有のニーズに従ってサーバーが確実にタグ付けされるようになります。サーバー顧客のタグ付けを利用することで、管理者はさまざまな顧客に関連付けられたリソースを簡単に識別および追跡でき、より効率的なリソースの割り当てと管理が可能になります。

> 注
>
> CSP は、当月の無料のタグ付けまたは顧客のタグ付けを排他的に変更でき、変更は当月と今後の月の両方に適用されます。

履歴傾向

Citrix との過去のビジネスに関する完全な履歴を表示できます。先月、昨年、または設定可能な期間にわたって報告された使用状況を確認します。

履歴表示はビジネスに関する価値ある情報を提供します。Citrix Service Provider は、Citrix とのビジネス実績の推移や、顧客および利用者全体でどの製品が最も高い成長率を示しているかをすばやく把握できます。



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:

- 指定した月の Virtual Apps and Desktops 製品の使用状況とユーザー一覧
- 現在の NetScaler VPX 割り当ての詳細

1. 製品の一覧から、[**Virtual Apps and Desktops**] または ［ネットワーク］を選択します。
2. 該当する場合は、エクスポートするタブを選択します。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］タブをクリックします。
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. 画面右側の ［エクスポート］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 の外部でライセンスデータにアクセスするために使用できる API をいくつか提供しています。これらの API の詳細については、Citrix Developer ドキュメントの「Citrix Cloud ライセンスを管理する API」を参照してください。

これらの API を使用するには、まず安全なクライアントを作成し、ベアラートークンを生成する必要があります。セキュアクライアントを作成するには、Citrix Cloud でセキュアクライアント権限が必要です。詳細については、「コンソールの権限」を参照してください。

Citrix Cloud API を使用するために必要なタスクの詳細については、Citrix Developer ドキュメントの「Citrix Cloud API の使用を開始する」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 Cloud アカウントへの完全な管理者アクセス権を付与せずに、Citrix ディストリビューターが 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。これを行うと、ディストリビューターが使用状況レポートを検証し、正確な請求を行うことができるようになります。

ディストリビュータがライセンスデータにアクセスできるようにするには、安全なクライアントの作成および License Use Insights サービスへのアクセス権限のみを持つカスタムのアクセス管理者を作成します。このアカウントは Citrix Cloud API へのアクセスが制限されており、他の Citrix Cloud 機能にはアクセスできません。アカウントの作成後、ディストリビューターとアカウント資格情報を共有すると、ディストリビューターは、Citrix Cloud アカウントにサインインし、Citrix Cloud API の使用に必要な安全なクライアントを作成できるようになります。あるいは、カスタムアクセス管理者としてサインインし、セキュアクライアントを作成して、セキュアクライアントの詳細をディストリビューターと共有することもできます。

ディストリビューター用のカスタムアクセスアカウントを作成するには、次の手順を実行します。

1. Citrix ディストリビューター専用の新しい管理者アカウントを作成します。手順については、「個別の管理者を招待する」を参照してください。
2. ［アクセスの設定］で、［カスタムアクセス］を選択し、次の権限を選択します。
   - ［全般］**>**［セキュアクライアント］
   - ［**License Usage Insights**］**>**［**License Usage Insights**：ディストリビューターアクセス］

セキュアクライアントを作成するには：

1. 新しい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. 「Citrix Cloud API の使用を開始する」の説明に従って、新しいセキュアクライアントを作成します。
3. Citrix Cloud が生成するクライアント ID とクライアントシークレットをメモします。これらの詳細は、すべての Citrix Cloud API に必須の入力です。

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、提供したセキュアクライアントの詳細を使用して 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。

月間および過去の Virtual Apps and Desktops ライセンス使用状況（License Usage Insights）に関する CSP レポート：

- Virtual Apps and Desktops の現在の使用状況
- Virtual Apps and Desktops の使用履歴

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（License Usage Insights）に関する CSP レポート：

- DaaS の現在の使用状況

- DaaS の使用履歴

CSP のクラウドライセンス使用状況（ライセンス）:

- DaaS の現在の使用状況
- DaaS の使用履歴

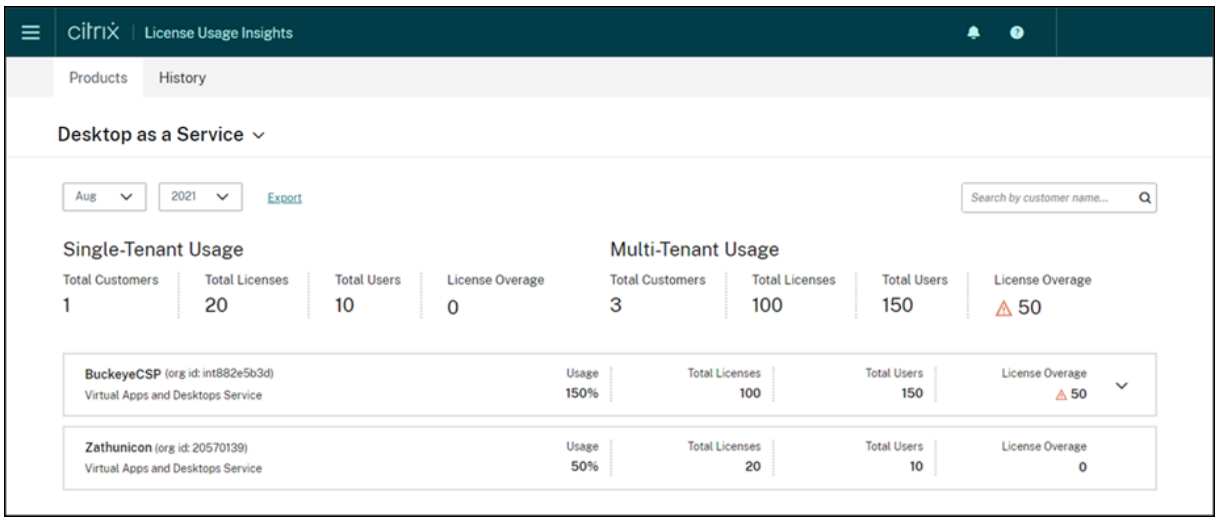
テナントのクラウドライセンス使用状況（[顧客ダッシュボード] -> [ライセンスの表示]）

- DaaS CCU の現在の使用状況
- DaaS CCU の使用履歴
- DaaS UD の現在の使用状況
- DaaS UD の使用履歴

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）

October 4, 2023

License Usage Insights では、クラウドサービスの使用状況が自動的に集計され、すべてのシングルテナントの顧客とマルチテナントのパートナーの全体を把握することができます。より詳しい分析のために、特定の月の詳細データを CSV ファイルとしてエクスポートすることもできます。



サポートされるサービス

シングルテナントのライセンス使用状況は、Citrix DaaS Premium（旧称 Virtual Apps Premium および Virtual Apps and Desktops Premium）向けに利用できます。

マルチテナントのライセンス使用状況は、次のサービス向けに利用できます:

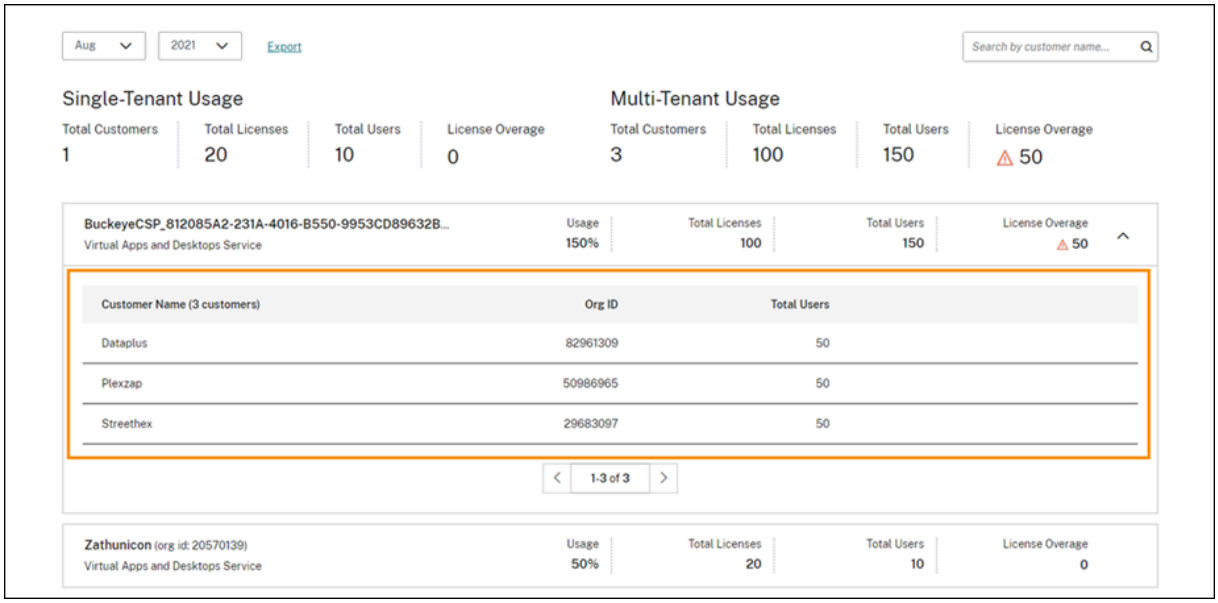
- Citrix DaaS（旧称 Virtual Apps and Desktops サービス）
- Citrix DaaS Standard for Azure（旧称 Virtual Apps and Desktops Standard for Azure）

ライセンスの概要

License Usage Insights は、Citrix Service Provider（CSP）のシングルテナントとマルチテナントの使用状況について、次の内訳を提供します:

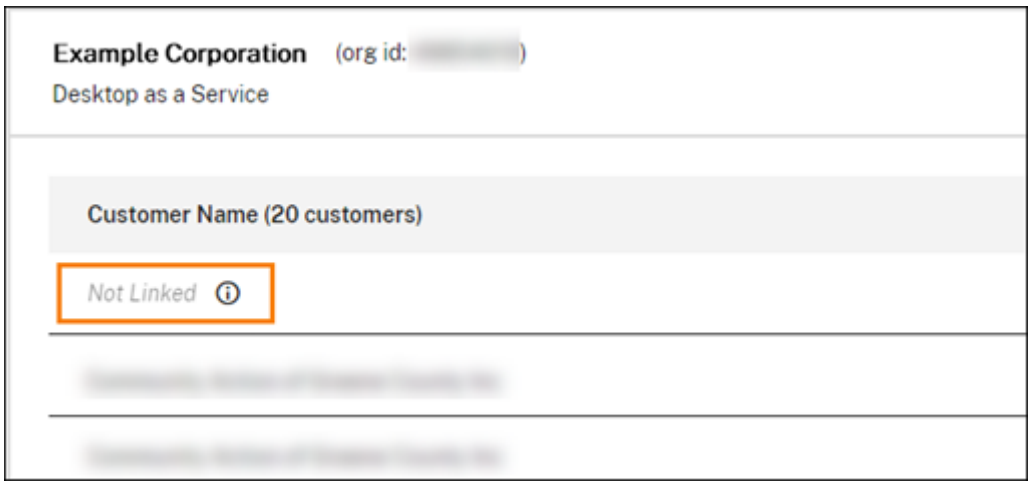
- 顧客の総数、すべての顧客の購入済みライセンス、ユーザー、および割り当て超過ライセンスの総数など、テナントの種類ごとにグループ化された一目でわかる概要。
- 使用中のライセンスの合計、購入済みライセンスの合計、ユーザー、および割り当て超過ライセンス数のパーセンテージなど、各顧客またはパートナーの使用状況の概要。

マルチテナントサービスの場合、使用状況の概要を開いて、各パートナーに関連付けられている顧客、組織 ID、および総ユーザーを表示できます。



リンクされていないテナントの顧客

場合によっては、テナントの顧客が「リンクされていません」と表示されることがあります。この状態は、そのテナントのユーザーが、テナントのワークスペース URL ではなく、CSP のワークスペース URL を介してクラウドサービスにアクセスする場合に発生する可能性があります。

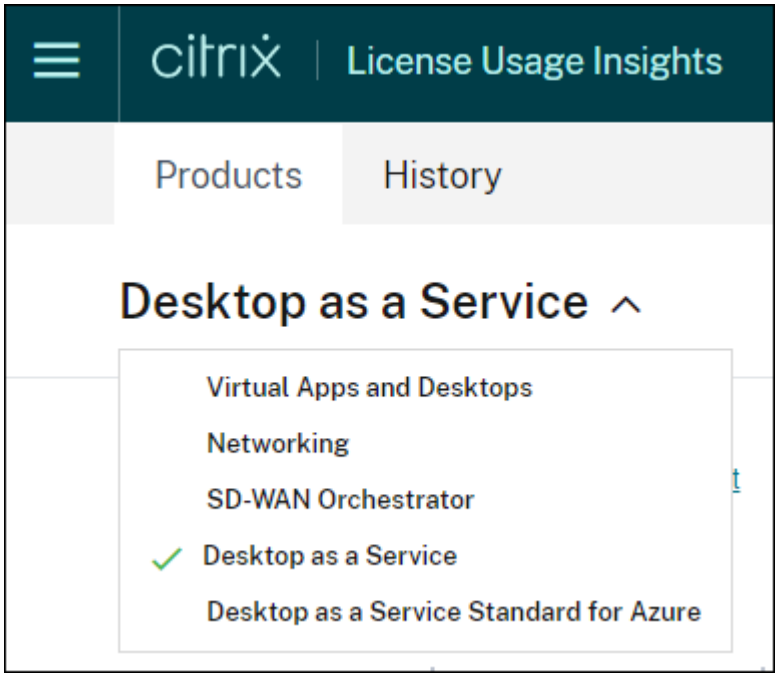


テナントのユーザーがテナントのワークスペース URL を介してサービスにアクセスすると、Citrix Cloud はそのユーザーをテナントに属するものとしてカウントし、「リンクされていません」というメッセージが削除されます。

毎月の使用状況の表示およびエクスポート

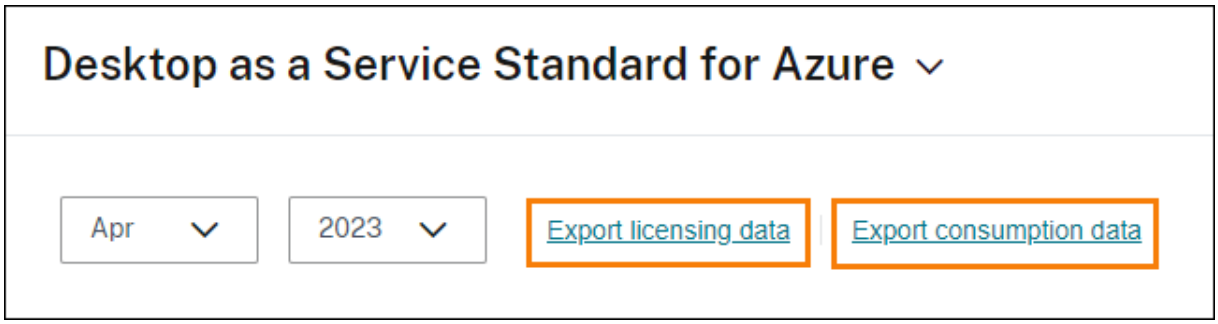
すべての顧客とパートナーの前月のライセンス使用状況をいつでも表示できます。このデータを CSV ファイルとしてエクスポートして、より詳しい分析ができます。Citrix DaaS Standard for Azure の場合、毎月の消費データをエクスポートすることもできます。

1. 製品メニューから、表示するクラウドサービスを選択します。



Citrix DaaS の場合、表示する月と年を選択し、［エクスポート］を選択します。

Citrix DaaS Standard for Azure の場合、表示する月と年を選択してから、［ライセンスデータのエクスポート］または ［消費データのエクスポート］を選択します。

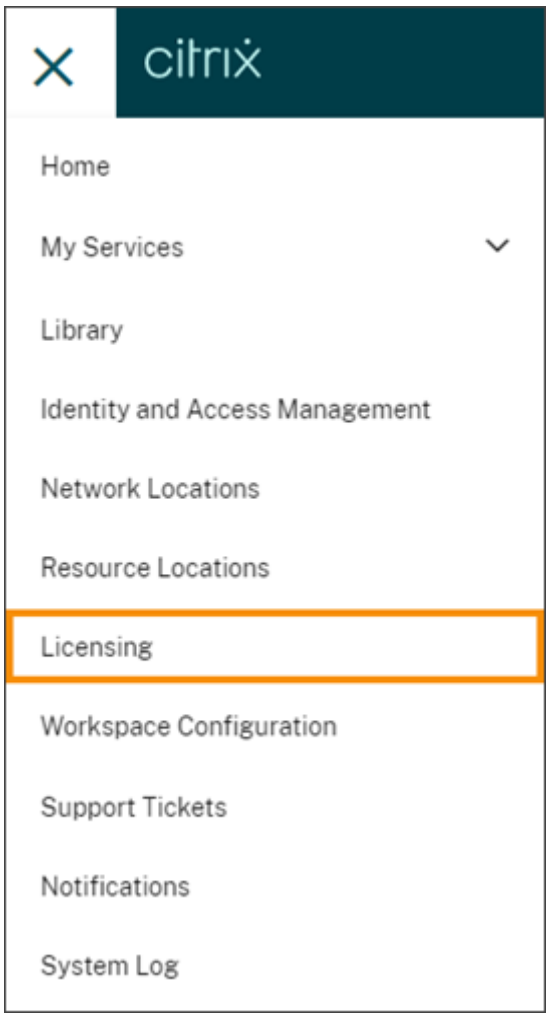


Citrix DaaS の顧客ライセンスと使用状況の監視

October 4, 2023

Citrix Service Providers（**CSP**）の顧客は、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 の顧客として、Citrix Cloud でご自身のアカウントにサインインすることにより、詳細情報にアクセスできます。シングルテナントとマルチテナントの顧客について集計されたライセンス使用状況データを表示する方法については、「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）」を参照してください。

顧客は、Citrix Cloud メニューで ［ライセンス］を選択することで、ライセンスデータを表示できます。



ライセンス割り当て

ユーザー/デバイスライセンスモデル： Citrix Cloud では、一意のカスタマーユーザーがアプリまたはデスクトップをその月で初めて起動したときに、ライセンスが割り当てられます。

同時ユーザーライセンスモデル： Citrix Cloud では、デバイスにあるアプリまたはデスクトップをユーザーが起動したときにライセンスが割り当てられます。ユーザーがログオフするか、セッションから切断すると、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、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応じて変わる可能性が常にあるため、Citrix Cloud は 5 分ごとに使用中のライセンスの数を評価します。

同時使用ライセンスモデルについて詳しくは、ライセンスサーバー製品ドキュメントの「同時使用ライセンス」を参照してください。

ライセンスの概要

Citrix Cloud は、ユーザー/デバイスライセンスモデルおよび同時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。

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、ライセンスの概要では、所有しているライセンスの総数に対する使用中のライセンス数が一目で確認できます。

割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。

Citrix Cloud は、購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数も表示します。

同時ユーザーの概要

同時ユーザーモデルの場合、ライセンスの概要で次の情報が一目でわかります:

- Citrix Cloud が使用中のライセンスを最後に評価したときに使用中だった購入済みライセンスの合計の割合。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、5 分ごとにこの割合を計算します。購入したライセンスの総数は、同時使用ライセンスモデルを使用する Citrix DaaS のために購入したライセンスの合計です。
- 購入したライセンスの合計に対する現在割り当てられているライセンスの比率、および使用可能なライセンスの残りの数。この比率に示す［合計］の数値は、現在所有しているライセンスの合計数を表します（[最新レポート］の日時の時点での内容）。
- ピーク時使用状況の統計。ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次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 **24** 時間：過去 24 時間で同時使用されたライセンスの最大数。
  - 今月：現在の暦月に入ってから同時使用されたライセンスの最大数。
  - 常時：サブスクリプションが開始してから同時使用されたライセンスの最大数。

  これらのピーク時使用状況期間に示される［合計］の数値は、その時点で所有していたライセンスの総数を表します。所有ライセンスの合計数が増加または減少し、それに伴って割り当てられたライセンスが増加した場合、［合計］の数値は、その時点における所有ライセンスの新しい数を反映して変更されます。ただし、対応する使用量のピークがない場合、［合計］の数値は変化しません。
- アクティブな使用統計。Citrix Cloud は、次の期間の一意の接続の合計数を表示します:
  - 月単位：前のカレンダー月の合計接続数。

- 日単位：過去 24 時間の合計接続数。これらの数値は、これらの期間中に所有されたライセンスの総数の割合でも表示されます。

ピーク時のライセンス使用の計算

同時使用ライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスに同時にアクセスする一意のデバイスの数が 5 分ごとにカウントされます。表示されている現在のピーク時使用状況よりもカウントが大きい場合、ピークに達した日時とともに新しいピーク時使用状況が Citrix Cloud に表示されます。カウントが現在のピーク使用量より少ない場合、現在のピーク使用量は変更されません。

> 重要：
>
> Director で［監視］を使用して同時セッションに関する情報を入手する場合、監視レポートで提供される同時セッションの解釈は異なり、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。監視レポートとライセンスレポートの違いについて詳しくは、「よくある質問」を参照してください。

毎月のアクティブ使用量の計算

毎月の初めに、Citrix Cloud は前月のスナップショットを作成します。Citrix Cloud は、そのカレンダー月に発生した一意の合計接続数を表示します。

日単位のアクティブな使用量の計算

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作成します。Citrix Cloud は、その 24 時間の間に発生した一意の合計接続数を表示します。

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、ライセンスの概要ページから ［使用状況の詳細の表示］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：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。

- 以前に割り当て済み：先月割り当てられたライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］としてカウントされます。8 月には、「以前に割り当て済み」としてカウントされます。
- 新しく割り当て済み：各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］としてカウントされます。

同時ユーザーの傾向

同時ユーザーライセンスの場合、［使用状況の傾向］セクションに次の情報が表示されます：

- ［ライセンス数合計］：購入した同時ライセンスの合計。
- ［ピーク時のライセンス使用］：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量を表示します。月間または時間ごとのピーク使用量を確認するには、表示する暦月または暦日をドロップダウンメニューから選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloud にはその時点において最新の時間間隔のピーク使用量が表示されます。たとえば、現在進行中の暦日を確認する場合、その瞬間までの 1 時間ごとの最大ライセンス数が表示されます。次の 5 分のカウント間隔でライセンスの最大数が増えると、Citrix Cloud ではその 1 時間のピーク使用量が更新されます。
- ［アクティブな使用］には、以下の情報のグラフが表示されます：
  - 日単位：過去 30 日間の各日の合計接続数。
  - 月単位：前のカレンダー年における各月の合計接続数。

［ライセンス割り当て］または ［アクティブな使用］グラフの間隔をポイントすると、その間隔の詳細が表示されます。

ライセンス使用ユーザー

［ライセンスアクティビティ］セクションには、当月中にライセンスが割り当てられた個別のカスタマーユーザーの一覧が表示されます。この一覧には、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。

ライセンスの毎月の解放

毎月 1 日に、前月の割り当て済みライセンスが自動的に解放されます。解放が行われると、割り当てられたライセンスの数が 0 にリセットされ、ライセンスを割り当てられたカスタマーユーザーの一覧がクリアされます。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、ライセンスが再割り当てされます。

毎月のライセンス履歴の確認

毎月 1 日に、割り当て済みライセンスの数が 0 にリセットされると、前月にライセンスを割り当てられたカスタマーユーザーの一覧（[ライセンスアクティビティ］の下にあります）がクリアされます。ただし、必要に応じていつでも、前月のユーザーの詳細にアクセスして、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［ライセンス履歴を表示］を選択します。
2. 表示する月を選択します。選択した月のユーザー詳細一覧が表示されます。
3. 一覧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］を選択して、ファイルを保存します。

ライセンス詳細のエクスポート

詳細な分析のために、顧客はいつでも、ライセンスを割り当てられたユーザーの詳細を CSV ファイルにエクスポートできます。その後、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。

当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］セクションの右端にある［**CSV** にエクスポート］を選択して、ファイルを保存します。

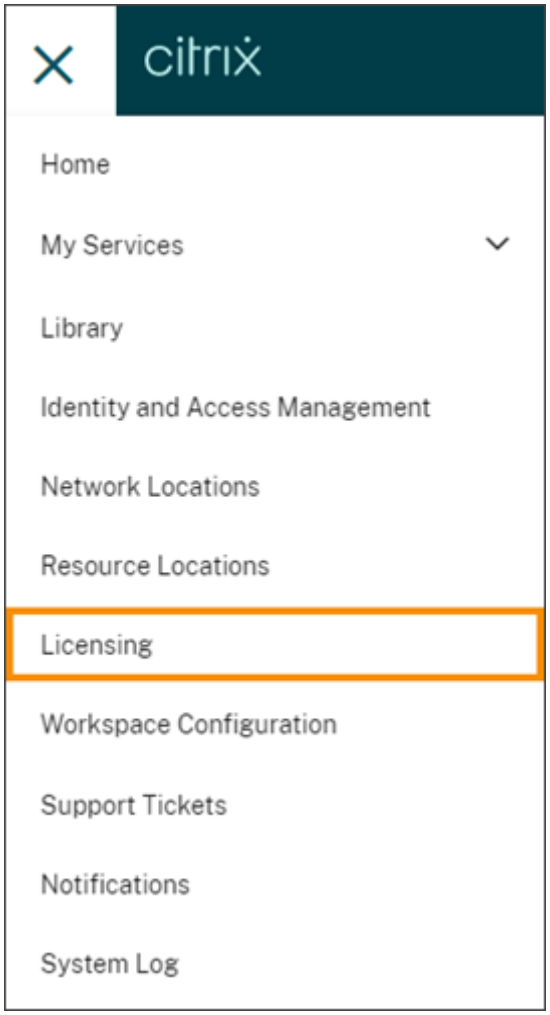
前月の詳細をエクスポートするには、「毎月のライセンス履歴の確認」の説明に従って、選択した月の一覧を生成します。［**CSV** にエクスポート］を選択してファイルを保存します。

Citrix DaaS Standard for Azure の顧客ライセンスと使用状況の監視

October 4, 2023

Citrix Service Providers（**CSP**）の顧客は、Citrix Cloud で、ユーザーの Citrix DaaS Standard for Azure ライセンスを簡単に監視できます。CSP の顧客として、Citrix Cloud でご自身のアカウントにサインインすることにより、詳細情報にアクセスできます。シングルテナントとマルチテナントの顧客について集計されたライセンス使用状況データを表示する方法については、「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）」を参照してください。

顧客は、Citrix Cloud メニューで ［ライセンス］を選択することで、ライセンスデータを表示できます。



ライセンス割り当て

ユーザー/デバイスライセンスモデル： Citrix Cloud では、一意のユーザーまたはデバイスによるデスクトップの初回起動時にライセンスが割り当てられます。

同時ユーザーライセンスモデル： Citrix Cloud では、デバイスにあるデスクトップをユーザーが起動したときにライセンスが割り当てられます。ユーザーがログオフするか、セッションから切断すると、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、デスクトップにアクセスするデバイスの数に応じて変わる可能性が常にあるため、Citrix Cloud は 5 分ごとに使用中のライセンスの数を評価します。

同時使用ライセンスモデルについて詳しくは、ライセンスサーバー製品ドキュメントの「同時使用ライセンス」を参照してください。

ライセンスの概要

Citrix Cloud は、ユーザー/デバイスライセンスモデルおよび同時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。

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、ライセンスの概要では、所有しているライセンスの総数に対する使用中のライセンス数が一目で確認できます。

割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。

Citrix Cloud は、購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数も表示します。

同時ユーザーの概要

同時使用モデルの場合、ライセンスの概要で次の情報が一目でわかります:

- Citrix Cloud が使用中のライセンスを最後に評価したときに使用中だった購入済みライセンスの合計の割合。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、5 分ごとにこの割合を計算します。購入したライセンスの総数は、同時使用ライセンスモデルを使用する Citrix DaaS Standard for Azure のために購入したライセンスの合計です。
- 購入したライセンスの合計に対する現在割り当てられているライセンスの比率、および使用可能なライセンスの残りの数。この比率に示す［合計］の数値は、現在所有しているライセンスの合計数を表します（[最新レポート］の日時の時点での内容）。
- ピーク時使用状況の統計。ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次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 **24** 時間：過去 24 時間で同時使用されたライセンスの最大数。
  - 今月：現在の暦月に入ってから同時使用されたライセンスの最大数。
  - 常時：サブスクリプションが開始してから同時使用されたライセンスの最大数。

  これらのピーク時使用状況期間に示される［合計］の数値は、その時点で所有していたライセンスの総数を表します。所有ライセンスの合計数が増加または減少し、それに伴って割り当てられたライセンスが増加した場合、［合計］の数値は、その時点における所有ライセンスの新しい数を反映して変更されます。ただし、対応する使用量のピークがない場合、［合計］の数値は変化しません。

ピーク時のライセンス使用の計算

同時使用ライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスに同時にアクセスする一意のデバイスの数が 5 分ごとにカウントされます。表示されている現在のピーク時使用状況よりもカウントが大きい場合、ピークに達した日時とともに新しいピーク時使用状況が Citrix Cloud に表示されます。カウントが現在のピーク使用量より少ない場合、現在のピーク使用量は変更されません。

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、ライセンスの概要ページから ［使用状況の詳細の表示］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:

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 以前に割り当て済み：先月割り当てられたライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］としてカウントされます。8 月には、「以前に割り当て済み」としてカウントされます。
- 新しく割り当て済み：各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーに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［新しく割り当て済み］としてカウントされます。

同時ユーザーの傾向

同時ユーザーライセンスの場合、［使用状況の傾向］セクションに次の情報が表示されます:

- ［ライセンス数合計］：購入した同時ライセンスの合計。
- ［ピーク時のライセンス使用］： 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量を表示します。月間または時間ごとのピーク使用量を確認するには、表示する暦月または暦日をドロップダウンメニューから選択します。

  選択した日付範囲がまだ終了していない場合、Citrix Cloud にはその時点において最新の時間間隔のピーク使用量が表示されます。たとえば、現在進行中の暦日を確認する場合、その瞬間までの 1 時間ごとの最大ライセンス数が表示されます。次の 5 分のカウント間隔でライセンスの最大数が増えると、Citrix Cloud ではその 1 時間のピーク使用量が更新されます。

グラフの間隔をポイントすると、その間隔での合計ライセンス数とピーク時のライセンス使用が表示されます。

使用状況レポート

使用状況の情報を標準の間隔、または指定の間隔でダウンロードできます。
情報には、次の項目に関するメーターの使用量が含まれます:

- Azure 仮想マシン
- ネットワーク接続（VNet ピアリングなど）
- Managed Disks、ブロック BLOB、ページ BLOB のような Azure ストレージの項目

すべての使用状況がデータに反映されるまで 1 日または 1 月の終わりから最大 72 時間を要することがあります。

［使用状況レポート］で、期間を選択し、［データのダウンロード］を選択して、CSV ファイルをローカルマシンにダウンロードします。

ライセンス使用ユーザー

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、当月中にライセンスが割り当てられた個別のカスタマーユーザーの一覧が表示されます。この一覧には、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。このセクションは、同時ユーザーライセンスでは利用できません。

ライセンスの毎月の解放

毎月 1 日に、前月の割り当て済みライセンスが自動的に解放されます。解放が行われると、割り当てられたライセンスの数が 0 にリセットされ、ライセンスを割り当てられたカスタマーユーザーの一覧がクリアされます。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、ライセンスが再割り当てされます。

毎月のライセンス履歴の確認

毎月 1 日に、割り当て済みライセンスの数が 0 にリセットされると、前月にライセンスを割り当てられたカスタマーユーザーの一覧（［ライセンスアクティビティ］の下にあります）がクリアされます。ただし、必要に応じていつでも、前月のユーザーの詳細にアクセスして、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［ライセンス履歴を表示］を選択します。
2. 表示する月を選択します。選択した月のユーザー詳細一覧が表示されます。
3. 一覧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］を選択して、ファイルを保存します。

ライセンス詳細のエクスポート

詳細な分析のためにいつでも、ライセンスを割り当てられたユーザーの単一の顧客の詳細を CSV ファイルにエクスポートできます。その後、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。

当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］セクションの右端にある ［**CSV** にエクスポート］を選択して、ファイルを保存します。

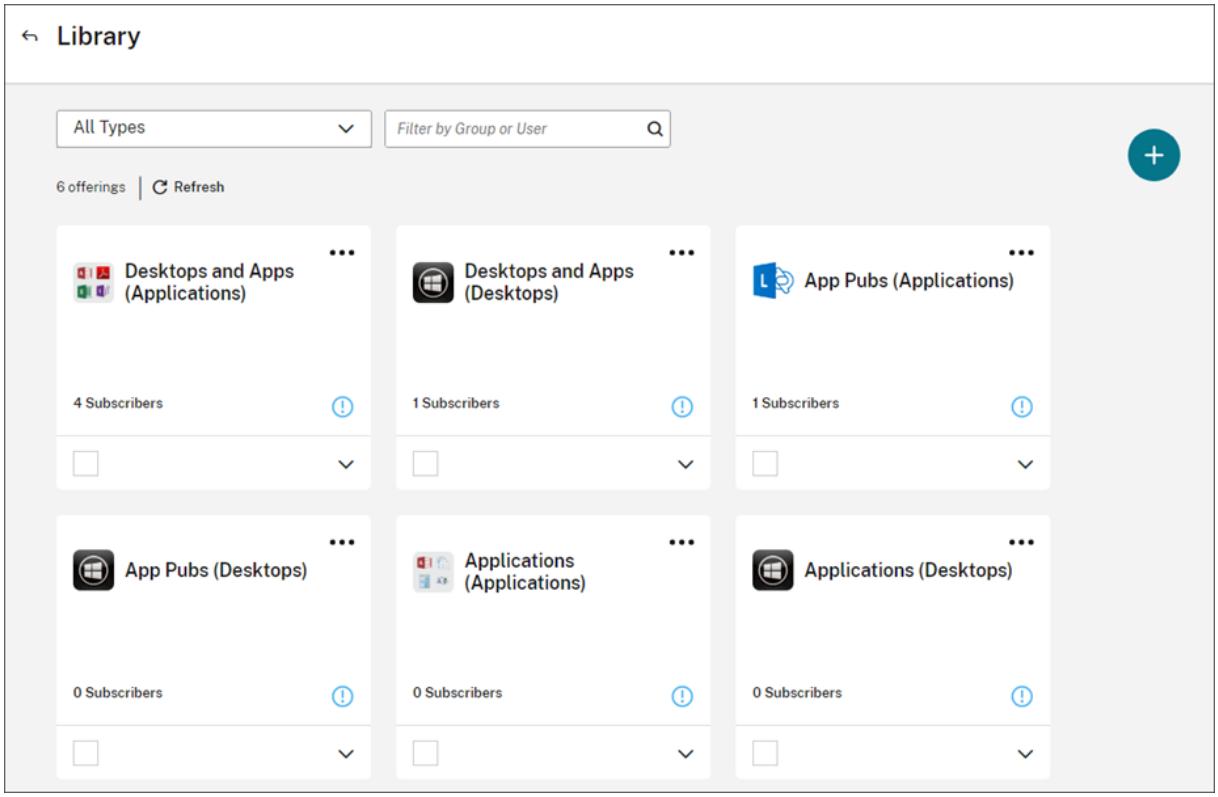
前月の詳細をエクスポートするには、「毎月のライセンス履歴の確認」の説明に従って、選択した月の一覧を生成します。［**CSV** にエクスポート］を選択してファイルを保存します。

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

April 26, 2024

> 注:
>
> *Citrix Cloud* で管理デリバリーグループでは、ユーザー割り当てを Web Studio コンソールで直接管理できるようになりました。詳しくは、DaaS のドキュメントを参照してください。以前は、これらのデリバリーグループの管理はライブラリに限定されていましたが、Web Studio コンソールでも同じ管理機能を使用できるようになりました。この機能は、すべてのお客様にご利用いただけるようになりました。2024 年 6 月に、クラウドライブラリ内の DaaS 固有のユースケースは完全に廃止される予定です。

ライブラリを使用して、Active Directory のユーザーやグループに、サービスで構成しているリソースなどの項目を割り当てることができます。オファリングは、Citrix サービスによって作成したアプリケーション、デスクトップ、データ共有、Web アプリケーションで構成されています。ライブラリには、すべてのオファリングが単一のビューで表示されます。



管理者アクセス

ライブラリにアクセスするには、管理者は次の要件を満たす必要があります:

- Citrix ID プロバイダーまたは Azure AD 経由で認証している。
- 管理者グループのメンバーとしてではなく、個別の管理者としてサインインしている。
- Citrix Cloud へのフルアクセス権限、または選択されたライブラリ役割のカスタムアクセス権限がある。

Citrix Cloud に個別の管理者アカウントおよびグループの管理者アカウントがある場合、ライブラリへのアクセスは、サインインするアカウントごとに有効な権限によって変わることがあります。詳しくは、「Citrix、AD、Azure AD および Google Cloud の ID を持つ管理者の最終的な権限」を参照してください。

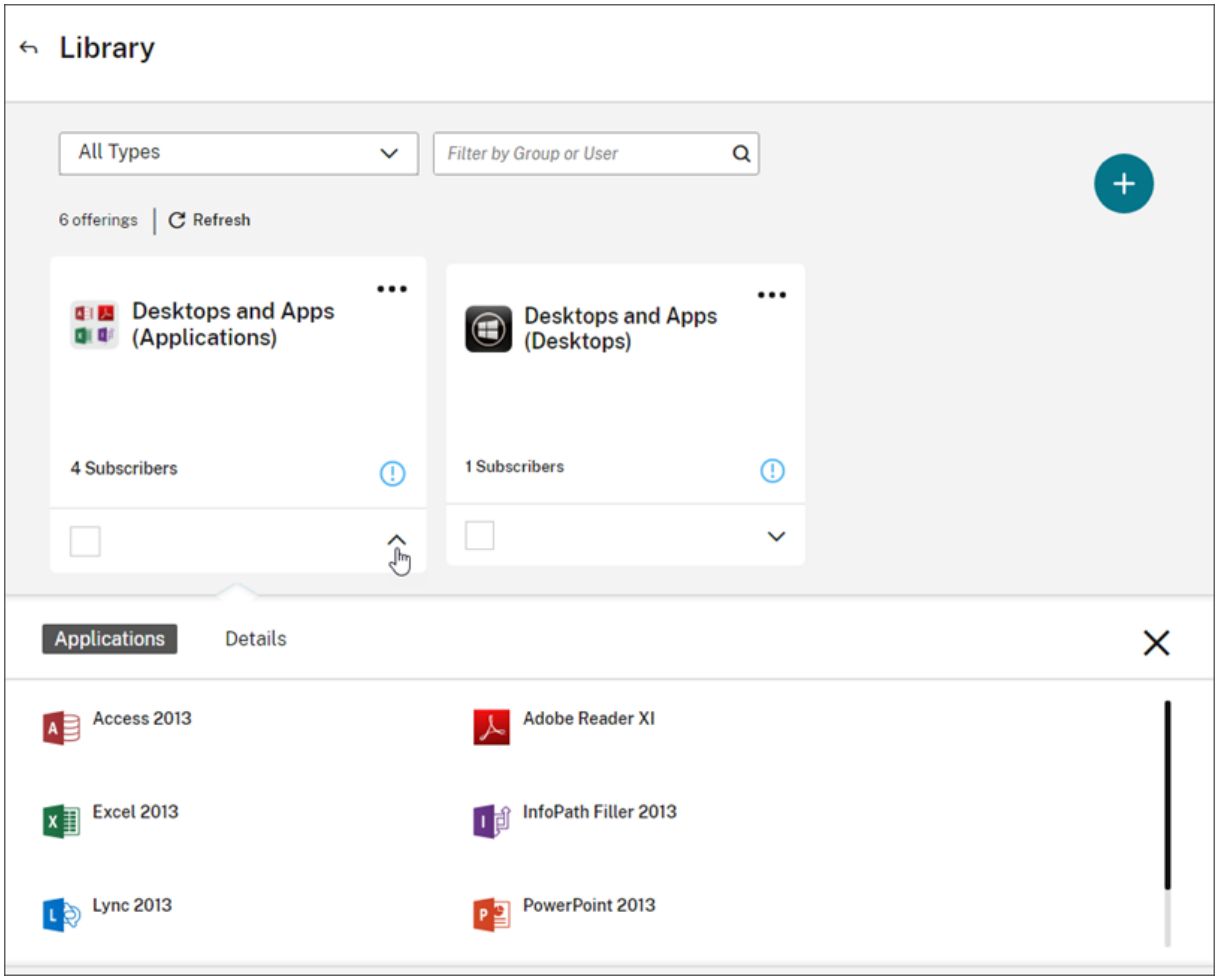
Citrix DaaS で **StoreFront** を使用する場合の考慮事項

Citrix DaaS でオンプレミスの StoreFront を使用している場合は、デリバリーグループを作成するときにライブラリを使用してリソースを割り当てないでください。代わりに、Studio を使用してリソースをユーザーに割り当てます。このシナリオでライブラリを使用する場合、リソースがユーザーに表示されない可能性があります。

Studio でデリバリーグループを作成する場合、［ユーザー］ページで、［ユーザー管理を **Citrix Cloud** に任せます］を選択しないでください。代わりに、別のオプションを選択します（［任意の認証ユーザーによるこのデリバリーグループの使用を許可します］または ［次のユーザーに対するこのデリバリーグループの使用を制限します］を選択します）。

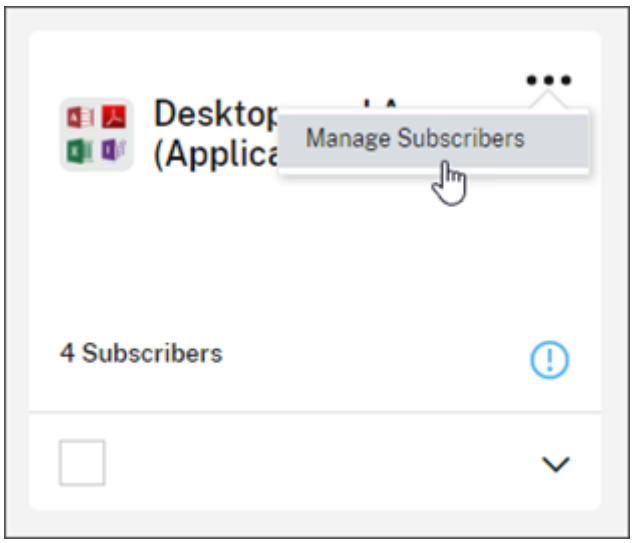
オファリングの詳細を表示する

オファリングカードで矢印ボタンをクリックすると、アプリケーション、デスクトップ、ポリシー、他のオファリング関連情報が表示されます。

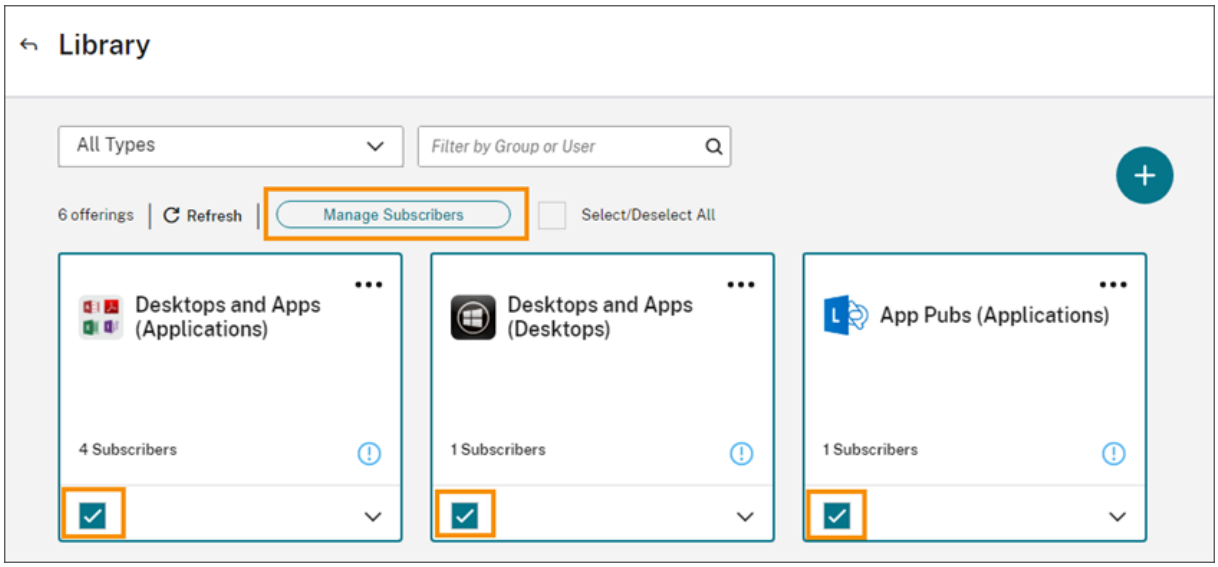


利用者を追加または削除する

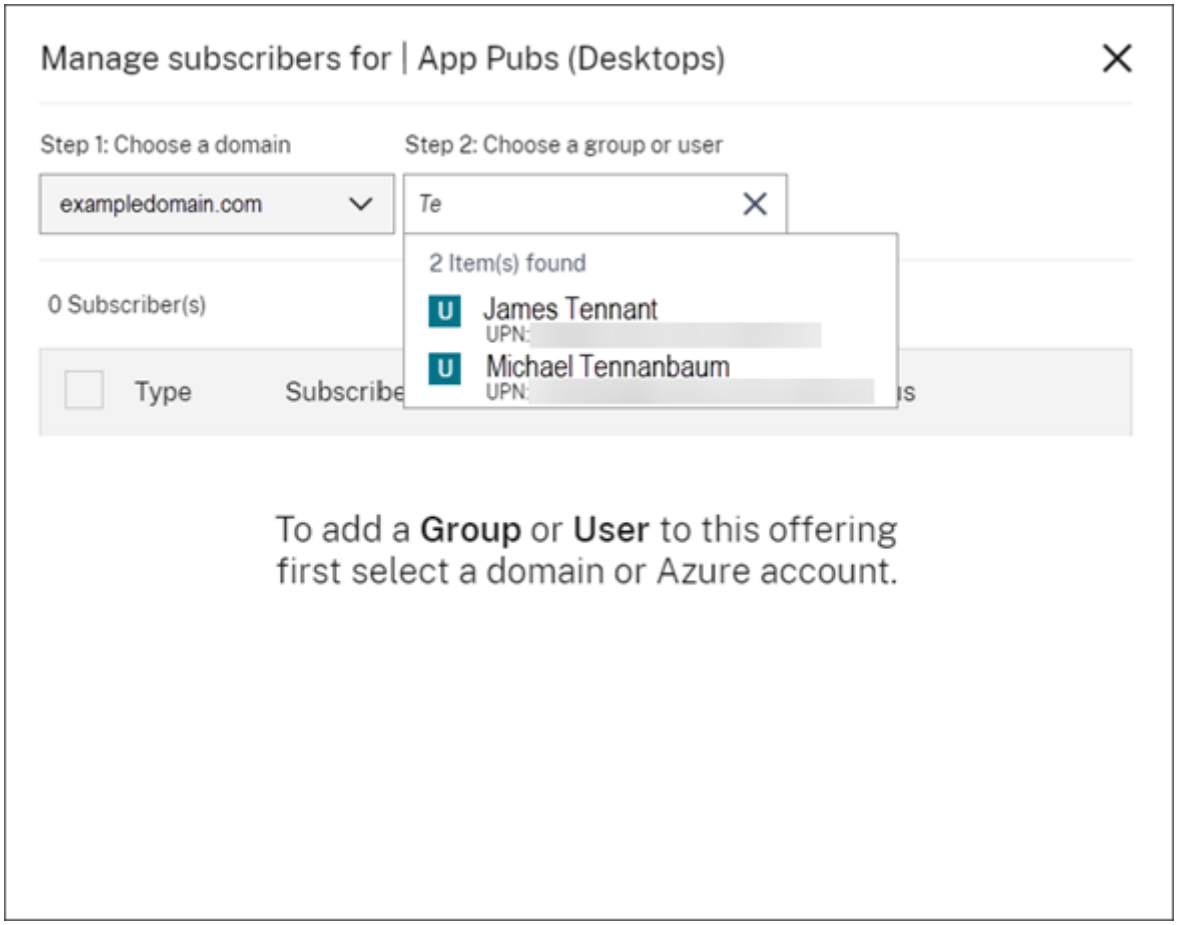
単一のオファリングについてユーザーまたはグループを管理するには、オファリングカードのメニューで ［利用者を管理］をクリックします。



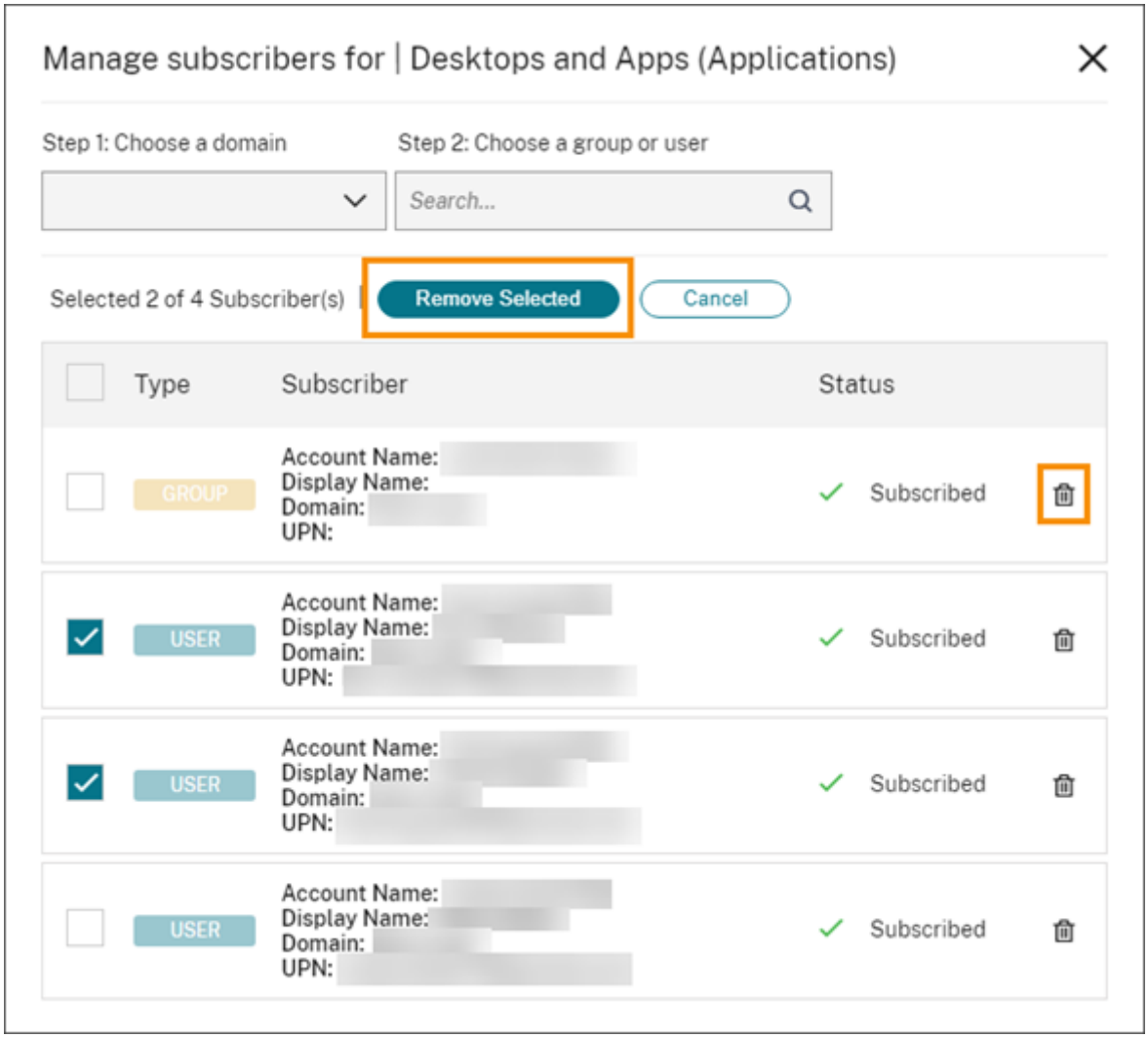
複数のオファリングについて利用者を管理するには、各オファリングのチェックマークを選択し、［利用者の管理］をクリックします。



オファリングに利用者を追加するには、ドメインを選択して、追加するユーザーまたはグループを選択します。



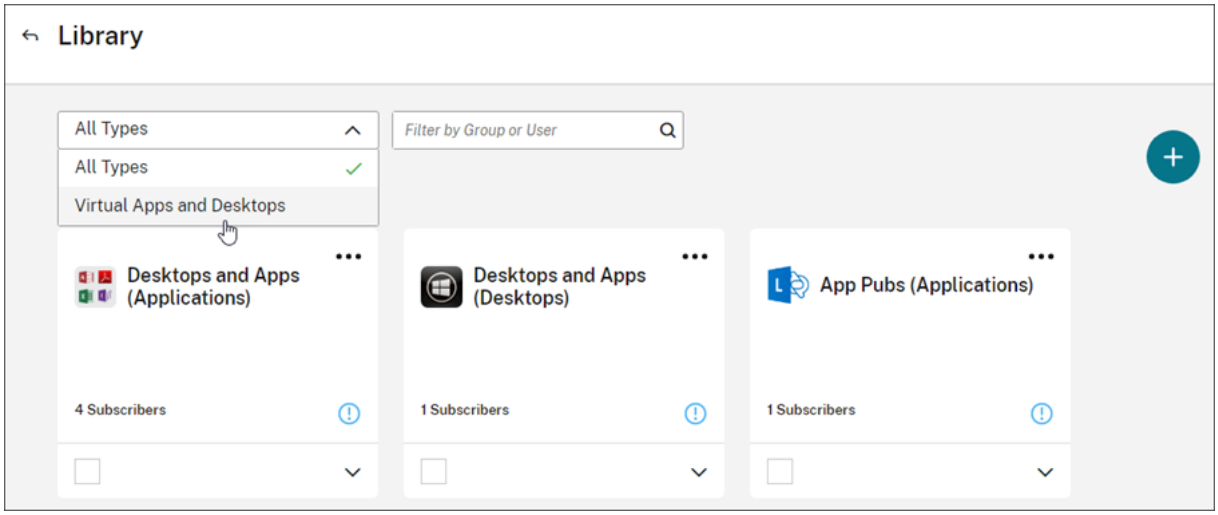
単一の利用者を削除するには、ユーザーまたはグループのごみ箱アイコンをクリックします。複数の利用者を削除するには、ユーザーまたはグループを選択し、［選択項目の削除］をクリックします。



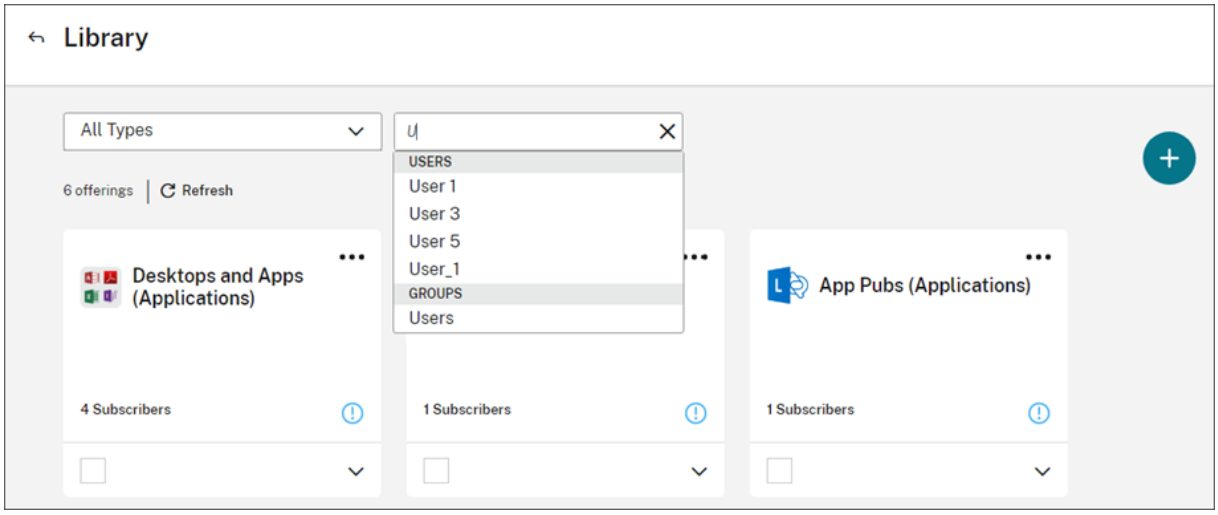
オファリングから利用者を追加または削除すると、オファリングカードには現在の利用者数が表示されます。

製品を絞り込む

デフォルトでは、ライブラリにすべてのオファリングが表示されます。特定のサービスのオファリングをすばやく表示するには、そのサービスのフィルターを選択します。



ライブラリ内のオファリングを現在利用しているすべてのユーザーまたはグループを検索できます。Citrix Cloud は、選択したユーザーまたはグループに関連するオファリングのみを表示します。すべてのユーザーのすべてのオファリングを表示するには、[X] をクリックしてフィルターをクリアします。



カスタムランディングページ

April 5, 2024

多くの管理者は Cloud コンソールにアクセスして、Web Studio コンソールでアプリケーションの管理や DaaS の Monitor でデータ表示などの特定のタスクを実行します。
ただし、これらのタスクでは、管理者がログインするたびに数回クリックし、複数のページ間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るため、時間を節約でき、コンソールエクスペリエンスが向上します。

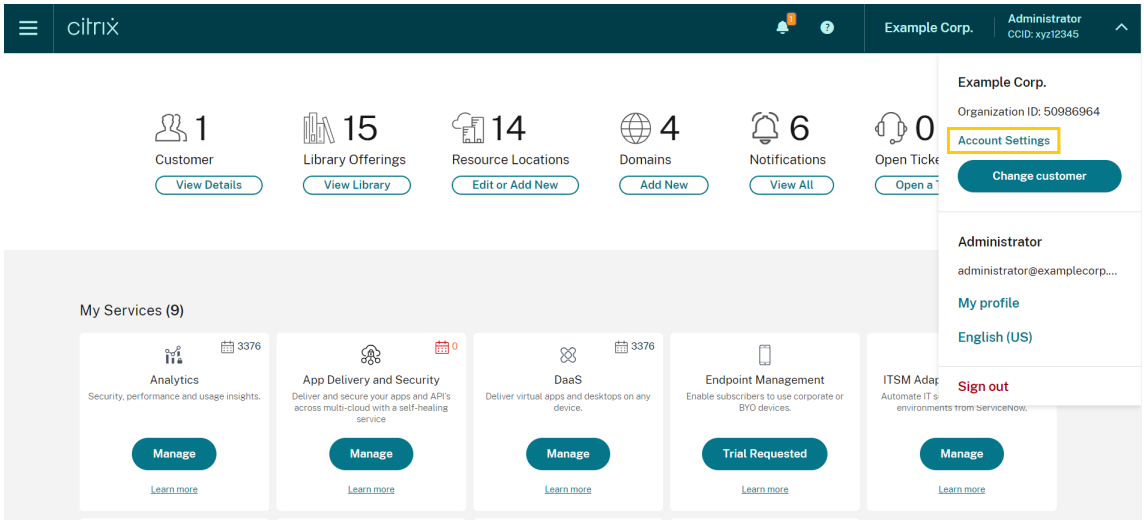
現在、次のページはカスタムランディングページとして設定できますが、今後さらに追加される予定です:

- DaaS
- DaaS の Monitor
- NetScaler コンソール
- CAS
- CAS セキュリティ
- CAS パフォーマンス
- WEM
- 一般

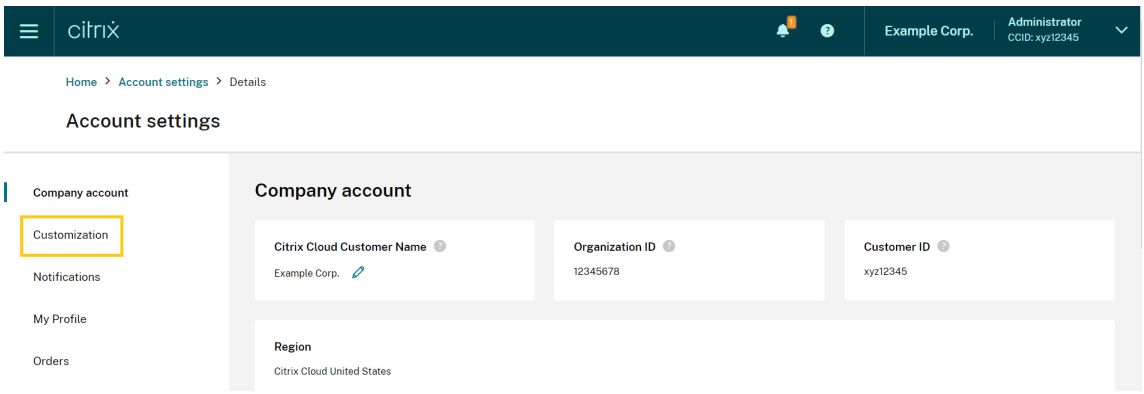
> 注:
>
> カスタムランディングページ設定はオプションで、アカウントごとに設定されます。そのため、各管理者は Citrix Cloud 内のエクスペリエンスをカスタマイズできます。すべての管理者（カスタム管理者、すべての管理権限を実行できる管理者）がこの機能にアクセスできます。

カスタムランディングページの設定

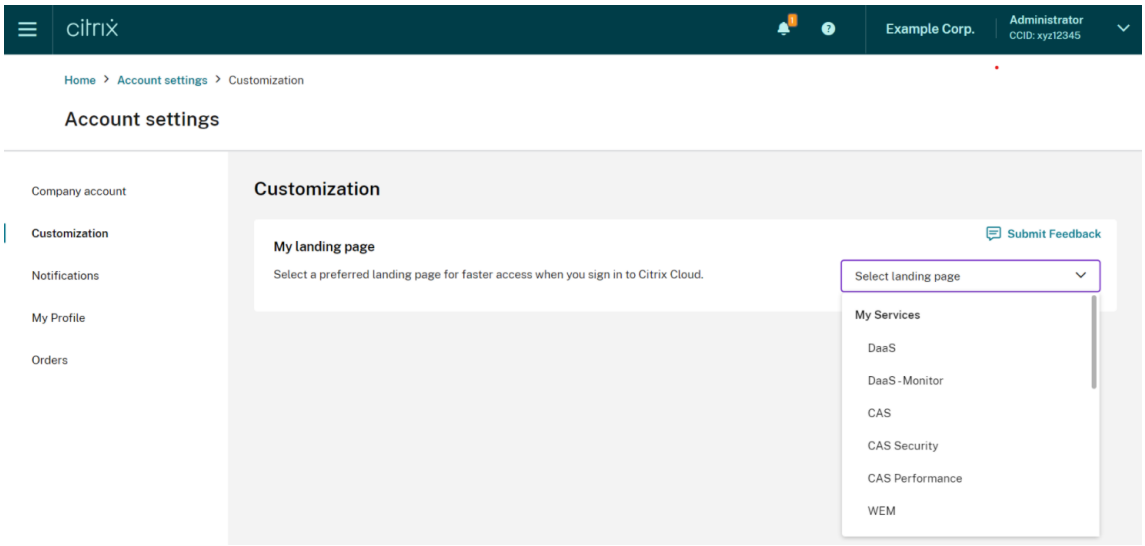
1. プロファイル名をクリックし、［アカウント設定］を選択します。



2. ［カスタマイズ］をクリックします。



3. カスタムランディングページとして設定したいサービスを選択します。



4. [適用] をクリックします。

   これで、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。
> - サインアウトした同じページで再度ログインすると、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。

ユーザーが **Citrix Cloud** アカウントを削除して再登録できる

April 26, 2024

Citrix Cloud では、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登録できる機能を提供しています。

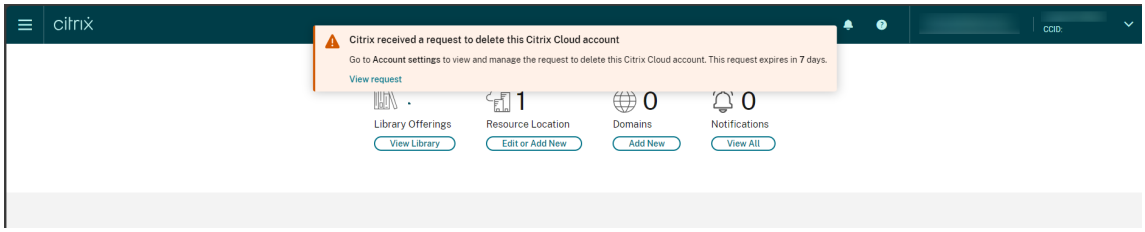
前提条件

- アカウントにアクティブな DaaS 使用権があり、DaaS 環境がプロビジョニングされている場合は、先に進む前に Citrix テクニカルサポートに連絡して「高速使用停止要求」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どう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」という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 と Connector Appliance を削除します。

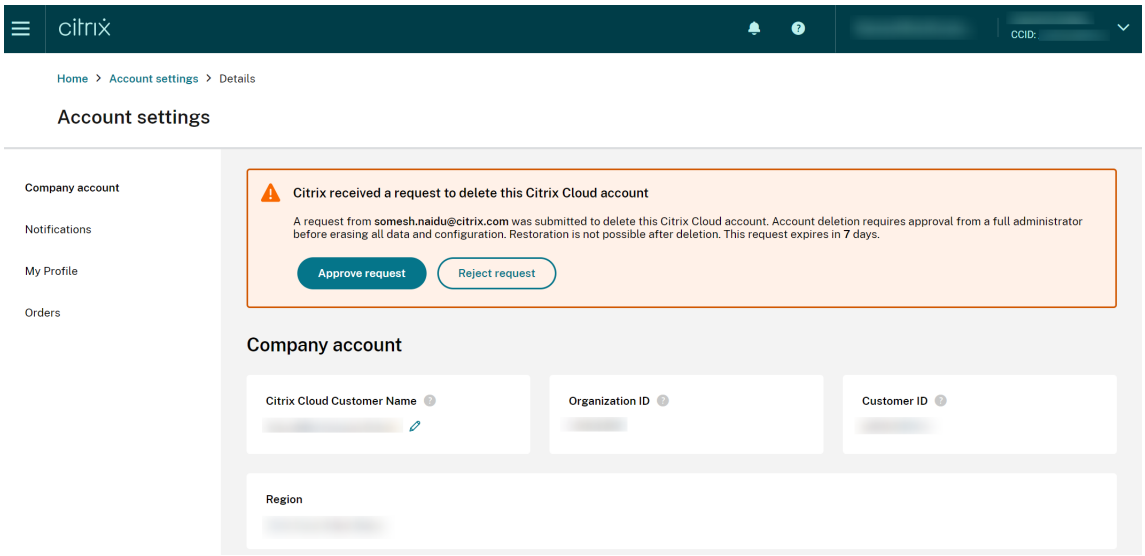
> 重要
>
> Citrix Cloud アカウントを削除する前に、次の点を考慮してください:
>
> - Citrix データベースからすべての顧客関連データが削除されています。
> - Citrix 管理の VM など、ご利用のクラウド環境で Citrix がプロビジョニングしている Citrix Cloud サービスに関連したすべてのリソースが削除されます。特定の Citrix Cloud サービスに含まれる Citrix 管理コンポーネントの説明については、「Citrix Cloud サービス」を参照してください。
> - Citrix Cloud とサービスへの管理者およびユーザーのアクセスが無効になっています。
> - このサービスをアクティブに使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。
> - このアクションは元に戻せません。いったん削除したデータは復元できません。

手順

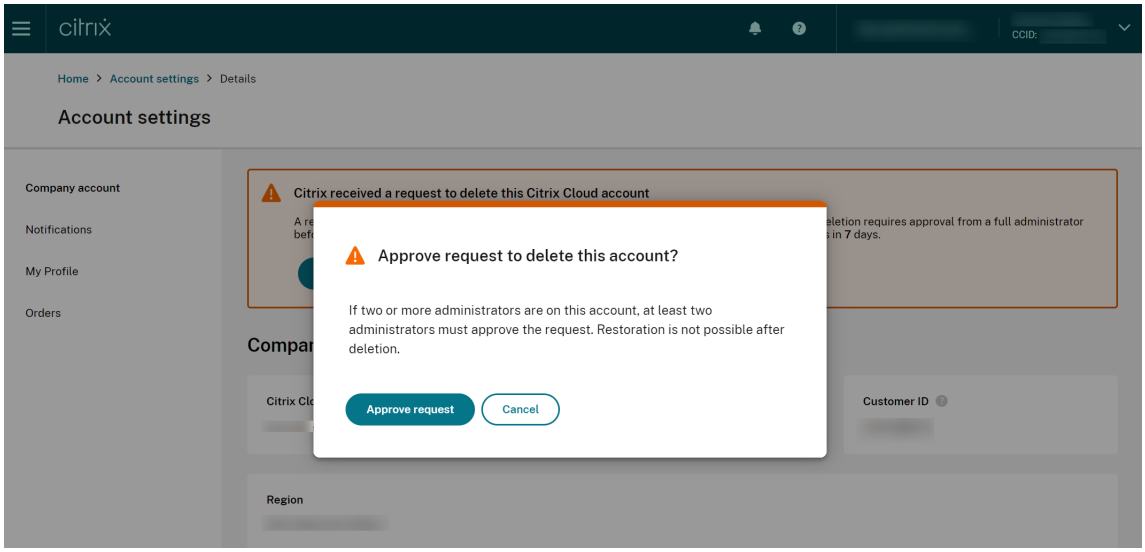
1. Citrix カスタマーサービスに連絡して、削除のリクエストを送信してください。このリクエストを送信するには、Citrix Cloud アカウントのすべての管理権限を実行できる管理者が必要です。
2. リクエストが開始されたら、Citrix Cloud アカウントにログインします。そこで Citrix Cloud アカウント削除ワークフローが表示されます。



3. 画面上のガイダンスに従って、このリクエストを承認または拒否します。



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て ［アカウント設定］に移動し、承認ワークフローバナーの ［リクエストの承認］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て ［アカウント設定］に移動し、削除の承認ワークフローバナーの ［リクエストを拒否して削除する］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は、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 日以内に受領されない場合、このリクエストは失効します。

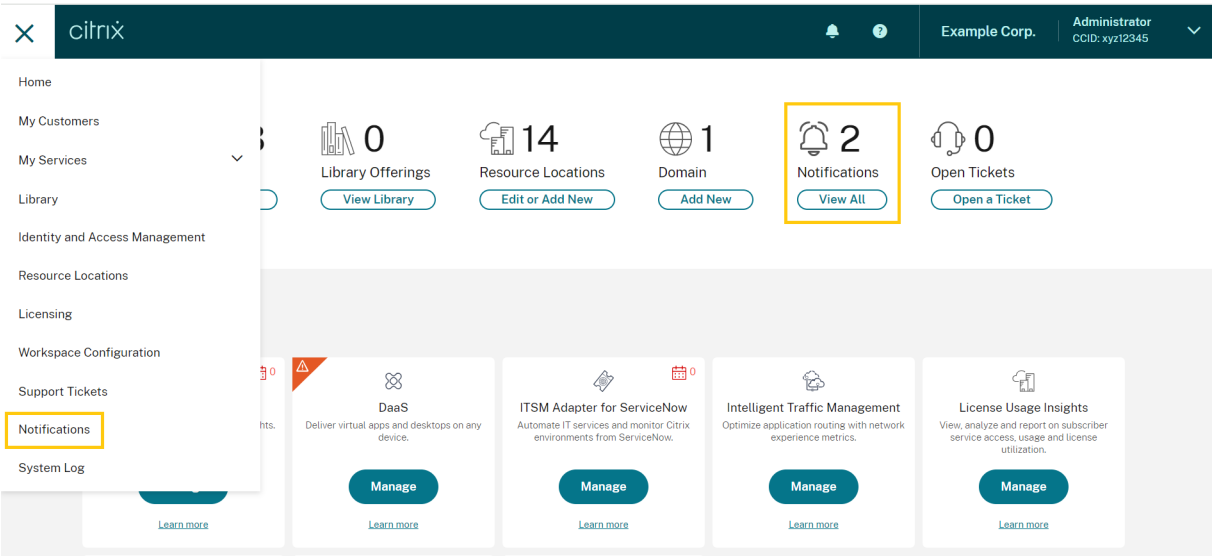
通知

October 4, 2023

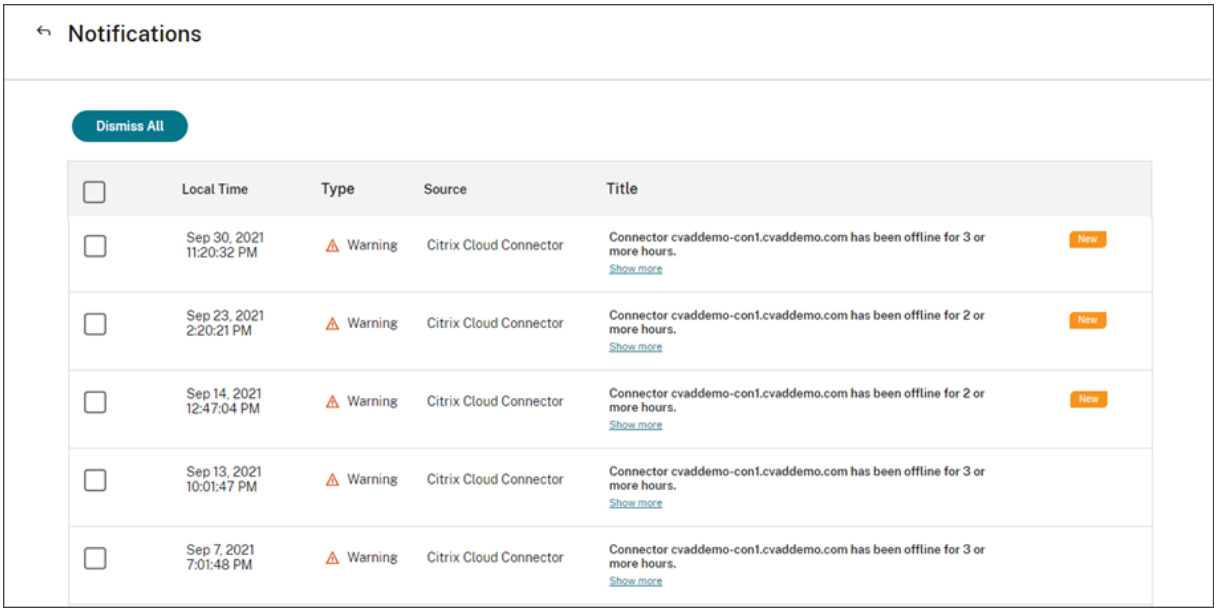
通知は、Citrix Cloud の新機能やリソースの場所内のマシンに関する問題など、管理者が関心がある問題またはイベントに関する情報を提供します。通知は Citrix Cloud のすべてのサービスで使用できます。

通知を表示する

通知の数は、Citrix Cloud コンソールページの上部付近に表示されます。詳しくは、コンソールの ［通知］で ［すべて表示］をクリックするか、コンソールメニューで ［通知］を選択してください。



［通知］ページには、受信した通知が表示されます。一覧の一番上が最新の通知です。

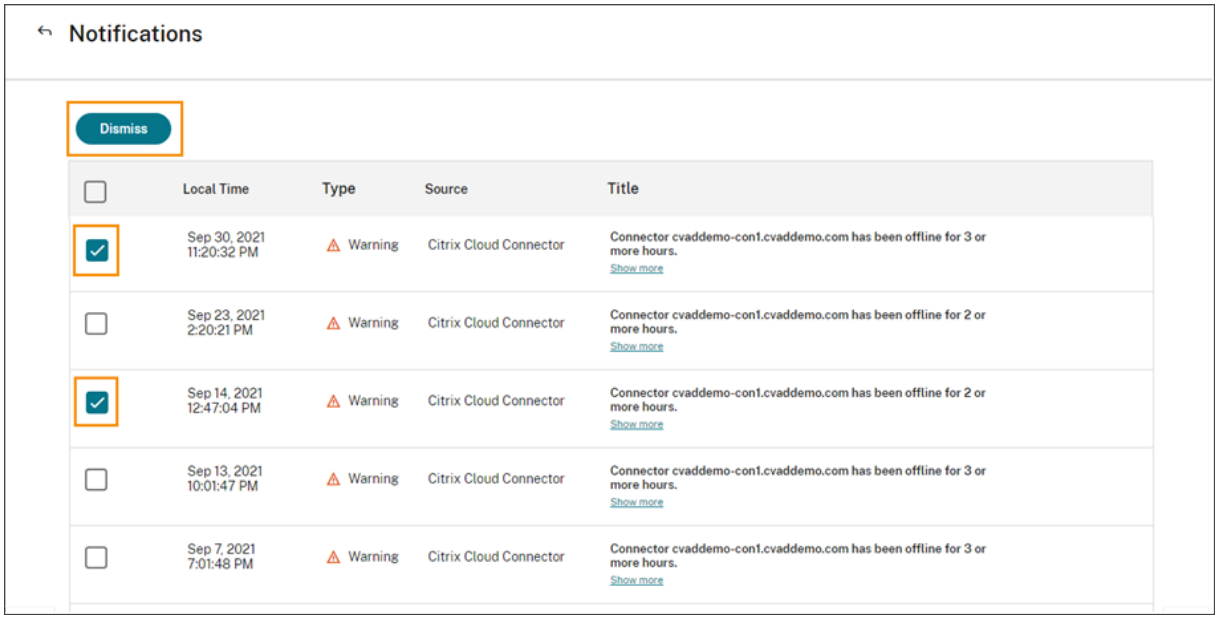


通知を削除する

通知は、管理者ごとに管理されます。通知を削除すると、Citrix Cloud の自分の管理者 ID の下で削除が実行されます。すべての通知を削除した場合でも、他の管理者は引き続きそれらの通知を表示して削除することができます。

受信したすべての通知を削除するには、ページの上部にある ［すべて閉じる］を選択します。

個々の通知を削除するには、各通知を選択し、［閉じる］を選択します。



メールで通知を受信する

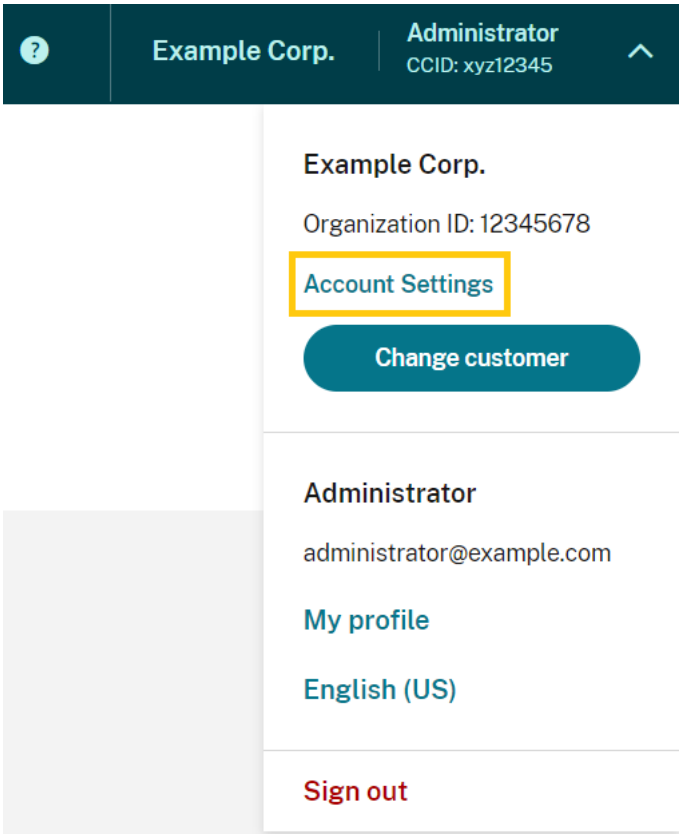
サインインする代わりにメールで通知を受信することを選択できます。デフォルトでは、メール通知は無効になっています。

組織のセキュリティチームおよび監査チームのメンバーなど、Citrix Cloud アカウントへの管理者アクセス権を持たない他の利害関係者のメール通知を有効にすることもできます。

メール通知を有効にすると、通知ごとに Citrix Cloud からメールが送信されます。通知は可能な限り早いタイミングで送信されます。1 通のメールにまとめられたり、何通かごとにまとめて後から送信されることはありません。

自分でメール通知を有効にするには

1. Citrix Cloud 管理コンソールで、［アカウント設定］を選択します。



2. ［通知］を選択します。
3. ［メール通知の受信］設定をオンにします。
4. ［通知設定を管理する］で、受信する通知の種類を選択します。デフォルトでは、すべての通知の種類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。

管理者以外のユーザーに対してメール通知を有効にするには

このセクションの手順に従って、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 でエラーが表示されます。

1. Citrix Cloud 管理コンソールで、［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. ［連絡先の管理］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、および表示言語を入力します。
5. ［通知設定を管理する］で、送信する通知の種類を選択します。
6. ［連絡先の追加］を選択して、連絡先の情報を保存します。

通知設定の変更

管理者は、［通知設定を管理する］のチェックボックスをオンまたはオフにして、受信する通知の種類を変更できます。通知を変更しても、他の管理者が受け取る通知には影響しません。

非管理者が受け取る通知を変更することもできます。

非管理者の通知を変更するには

1. Citrix Cloud 管理コンソールで、［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. ［連絡先の管理］で、管理する連絡先を見つけます。
4. 連絡先を指定し、鉛筆アイコンを選択します。
5. ［通知設定を管理する］で、通知の種類ごとに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、まず連絡先を削除し、新しいメールアドレスを持つ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

管理者は、［メール通知の受信］設定をオフにすることで、必要に応じて自身のメール通知を無効にできます。

非管理者は、すべての通知メールに表示されるサブスクリプションの解除リンクをクリックすると、通知の受信を停止できます。サブスクリプションが解除された連絡先は、［連絡先の管理］セクションの表に表示される通知ステータスが ［サブスクリプション解除］になります。

非管理者に対する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 ［通知設定を管理する］のチェックボックスをすべてオフにします。
- ［連絡先の管理］にある表から連絡先を削除します。

非管理者の連絡先の削除

1. Citrix Cloud 管理コンソールで、［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. ［連絡先の管理］で、管理する連絡先を見つけます。
4. 連絡先を指定し、ゴミ箱アイコンを選択します。

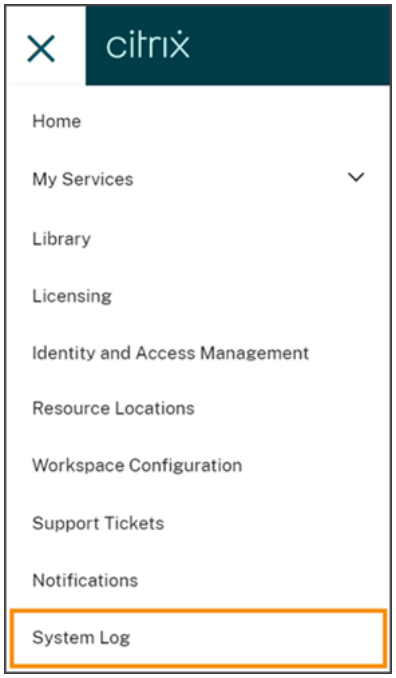
Citrix Cloud により、表から連絡先が削除されます。

システムログ

October 4, 2023

システムログには、Citrix Cloud で発生したイベントがタイムスタンプ付きで一覧表示されます。これらの変更を CSV ファイルとしてエクスポートして、組織の規制遵守要件を満たしたり、セキュリティ分析をサポートしたりすることができます。

システムログを表示するには、Citrix Cloud メニューで ［システムログ］を選択します。

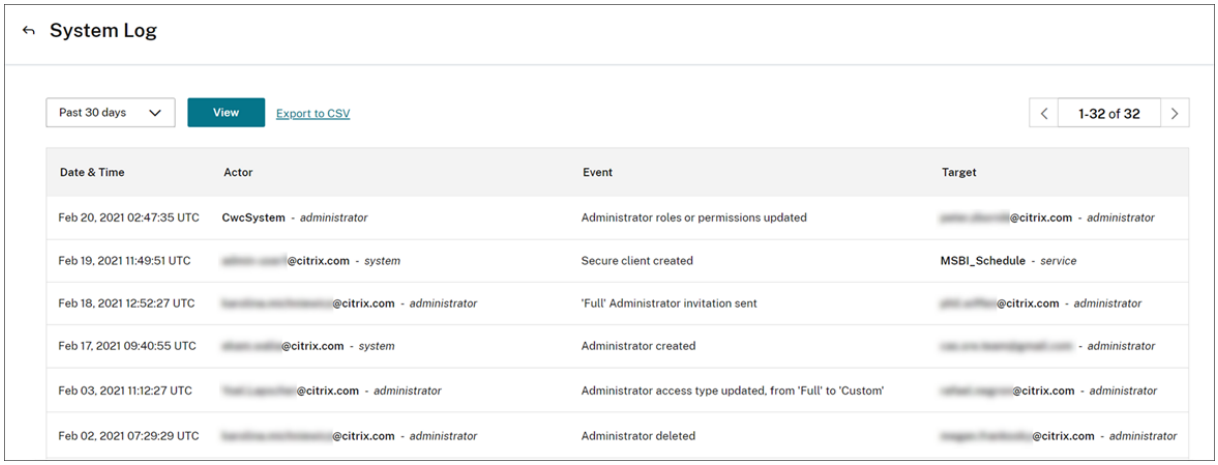


システムログのデータの保持について詳しくは、この記事の「データ保持」を参照してください。

ログに記録されたイベント

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。これらのイベントの完全な一覧とキャプチャされたデータの説明については、「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。

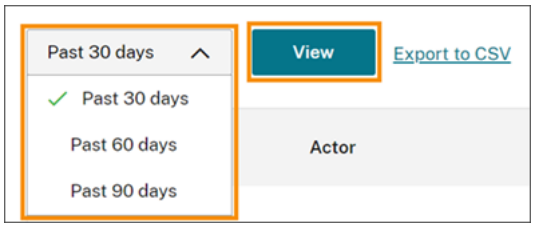
デフォルトでは、過去 30 日間に発生したイベントがシステムログに表示されます。最新のイベントが一番上に表示されます。



表示される一覧には、次の情報が含まれます:

- イベントが発生した日時（UTC）。
- 管理者やセキュアクライアントなど、イベントを開始したアクター。アクター **CwcSystem** のエントリは、Citrix Cloud がその操作を行ったことを示します。
- 管理者の編集や新しいセキュアクライアントの作成など、イベントの簡単な説明。
- イベントの対象。対象は、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。

過去 30 日間よりも前のイベントを表示するには、表示する期間でフィルタリングして ［表示］を選択します。過去 90 日間までに発生したイベントを表示できます。

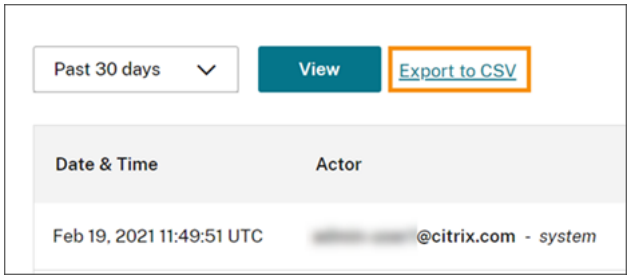


SystemLog API を使用して、指定した期間中に発生した古いイベントを取得できます。詳しくは、この記事の「特定期間のイベントの取得」を参照してください。

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。ダウンロードしたファイルの名前は、次の形式です。`SystemLog-CustomerName-OrgID-DateTimeStamp.csv`

1. Citrix Cloud メニューの ［システムログ］を選択します。
2. 必要に応じて一覧をフィルターして、イベントをエクスポートする期間を表示します。
3. ［**CSV** にエクスポート］を選択して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
- 名前やアクター ID など、イベントを開始したアクターの詳細。
- イベントの種類やイベントのテキストなど、イベントの詳細
- ターゲット ID、管理者またはセキュアクライアントの名前など、イベントの対象の詳細。

特定期間のイベントの取得

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セキュアクライアントを作成する必要があります。

SystemLog API の使用について詳しくは、Citrix Developer Docs Web サイトの「Citrix Cloud - SystemLog」を参照してください。

システムログイベントの転送

Splunk 用の Citrix システムログアドオンを使用すると、Splunk インスタンスを Citrix Cloud に接続できます。この接続で、システムログデータを Splunk に転送できます。詳しくは、GitHub の Citrix リポジトリの「add-on documentation」を参照してください。

データ保持

Citrix とお客様は、Citrix Cloud が記録したシステムログデータを保持する共同責任があります。

Citrix は、イベントの記録後 90 日間、システムログレコードを保持します。

お客様には、組織のコンプライアンス要件に合わせて保持する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格納する責任があります。

システムログイベントのリファレンス

October 4, 2023

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、次の操作を実行できます:

- 過去 30 日間、60 日間、または 90 日間に発生したすべてのイベントの CSV ファイルをダウンロードする。
- SystemLog API を使用して、特定の期間のイベントを取得する。

システムログイベントの取得時にキャプチャされるデータの説明については、「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、イベントの種類、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、イベント固有の値のイベントを生成するクラウドコンポーネントとクラウド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クラウドサービス

システムログには、次の Citrix Cloud のエンティティ、コンポーネント、およびサービスのイベントが記録されます:

- Citrix Cloud プラットフォーム: 管理者の管理、Workspace 利用者のデバイスリセット、Azure AD テナント、ドメインおよびネットワークの場所の管理など、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: オンプレミスのライセンスサーバーの登録、クラウドサービスの割り当て済みライセンスの管理、および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 サービスの構成に関連するイベント。
- Citrix Workspace: Workspace の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したり、SystemLog API を使用して取得したりすると、次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時と 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です。
- **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です。
- **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** と **AfterChanges**：イベント発生前後のオブジェクトフィールドの内容をそれぞれ返します。一部のイベントでは、次のオブジェクトフィールドが含まれます：
  - CustomerID
  - User principal
  - UserID
  - 管理者のアクセスの種類（Custom または Full など）
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **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、管理者を作成する場合、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個人またはエンティティの表示名。たとえば、Citrix Cloud アカウントに別のユーザーを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システムログイベント

July 12, 2023

ここでは、Citrix Cloud プラットフォームに対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について詳しくは、「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。

システムログについて詳しくは、「システムログ」を参照してください。

Azure AD テナント

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
Azure AD テナントが接続されています	platform/identityprovider/azuread/connect	serviceprincipal	administrator		はい	いいえ
Azure AD テナントが切断されました	platform/identityprovider/azuread/disconnect	serviceprincipal	administrator		はい	いいえ
Azure AD 認証ドメイン名が変更されました	platform/identityprovider/azuread/authdomainname/update	customerAD	administrator		いいえ	いいえ
Azure AD 認証ドメイン名の変更に失敗しました	platform/identityprovider/azuread/authdomainname/failed	customerAD	administrator		いいえ	いいえ

Citrix Cloud 管理者とセキュアクライアント

イベントメッセージ	イベントの種類	ターゲットの種類	アクターの種類	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
管理者が作成されました	platform/administrator/create	administrator	system	いいえ	はい
管理者への招待状が送信されました	platform/administrator/invite	administrator	administrator	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	administrator	administrator	はい	はい
管理者が削除されました	platform/administrator/delete	administrator	administrator	いいえ	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	アクターの種類	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
セキュアクライアントが作成されました	platform/clientadministrator/create	service	system	いいえ	はい
セキュア クライアントが削除されました	platform/clientadministrator/delete	administrator	administrator	はい	いいえ
管理者グループが作成されました	platform/administratorgroup/create	administratorgroup	administrator	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	administratorgroup	administrator	はい	はい
管理者グループが削除されました	platform/administratorgroup/delete	administratorgroup	administrator	はい	いいえ

Active Directory + トークンのデバイスのリセット

イベントメッセージ	イベントの種類	ターゲットの種類	アクターの種類	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
利用者のデバイスのトークンのリセットが完了しました	platform/authentication/device/delete	identityprovider	administrator	いいえ	はい

ドメイン管理

イベントメッセージ	イベントの種類	ターゲットの種類	アクターの種類	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
ドメインが削除されました	platform/domain/remove	service	administrator	いいえ	いいえ

ネットワークの場所

イベントメッセージ	イベントの種類	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済みオブジェクトフィールド
ネットワークの場所が作成されました	sdwan/networklocation/create	ネットワークの場所の ID	ネットワークの場所を追加した管理者の名前	いいえ	はい
ネットワークの場所が正常に更新されました	sdwan/networklocation/edit	変更されたネットワークの場所の ID	ネットワークの場所を変更した管理者の名前	はい	はい
ネットワークの場所が削除されました	sdwan/networklocation/delete	削除されたネットワークの場所の ID	ネットワークの場所を削除した管理者の名前	はい	いいえ

リソースの場所

イベントメッセージ	イベントの種類	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済みオブジェクトフィールド
リソースの場所が作成されました	platform/resourcelocation/create	作成されたリソースの場所の名前	リソースの場所を作成した管理者の名前	はい	はい
リソースの場所が更新されました	platform/resourcelocation/update	変更されたリソースの場所の名前	リソースの場所を変更した管理者の名前	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 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済みオブジェクトフィールド
リソースの場所が削除されました	platform/resourcelocation/delete	削除されたリソースの場所の名前	リソースの場所を削除した管理者の名前	はい	はい

コネクタのシステムログイベント

April 20, 2022

ここでは、クラウドサービス用の Citrix Cloud Connector およびコネクタアプライアンスに対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について詳しくは、「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。

システムログについて詳しくは、「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
コネクタが登録されました	platform/edgeserver/create	**Cloud Connector** 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	**Cloud Connector** 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	イベントの種類	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済みオブジェクトフィールド
リソースの場所のメンテナンス期間が更新されました	platform/resourcelocation/maintenancewindow/update	変更されたリソースの場所の名前	構成を変更した管理者	はい	はい
コネクタのアップグレードが管理者によってトリガーされました	platform/edgeservice/manualupgrade	**Cloud Connector** 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
コネクタのアップグレードが開始されました	platform/edgeservice/upgradestarted	**Cloud Connector** 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/edgeservice/upgradecompleted	**Cloud Connector** 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

コネクタ公開キー

イベントメッセージ	イベントの種類	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済みオブジェクトフィールド
公開キーが信頼に追加されました	platform/authentication/createedgepublickey	操作を実行した管理者		いいえ	いいえ
公開キーが信頼から削除されました	platform/authentication/deleteedgepublickey	操作を実行した管理者		いいえ	いいえ

Citrix Cloud でのライセンスのシステムログイベント

April 20, 2022

ここでは、Citrix Cloud へのオンプレミスの Citrix ライセンス登録に対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について詳しくは、「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。

システムログについて詳しくは、「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済み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/onpremlicenseserver/delete	Licensing	ライセンスサーバーを削除した管理者	いいえ	いいえ
オンプレミスライセンス サーバーを削除できませんでした	lui/onpremlicenseserver/deletefailed	Licensing	ライセンスサーバーを削除しようとした管理者	いいえ	いいえ

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
Citrix Cloud サービスライセンスが解放されました	lui/cloudlicense/release	CloudLicense	クラウドサービスのライセンスを解放した管理者	いいえ	いいえ

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
Citrix Cloud サービスライセンスの解放に失敗しました	lui/cloudlicense/releaseLicense/failed	CloudLicense	クラウドサービスのライセンスを解放しようとした管理者	いいえ	いいえ

Citrix Service Provider の License Usage Insights

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
パートナーのオンプレミス ユーザー一覧データがエクスポートされました	lui/csp/userlistdata/exporting	License	パートナーのユーザー一覧の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一覧データをエクスポートできませんでした	lui/csp/userlistdata/exportfailed	License	パートナーのユーザー一覧のデータをエクスポートしようとした管理者	いいえ	いいえ

クラウドサービスと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
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	CloudLicensing 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に失敗しました	lui/cloudlicense/usagedataexportfailed	CloudLicensing または Licensing	ライセンス使用状況データをエクスポートしようとした管理者	いいえ	いいえ

Secure Private Access のシステムログイベント

October 19, 2022

本記事では、Secure Private Access サービスに対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について詳しくは、「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。

システムログについて詳しくは、「システムログ」を参照してください。

Web および **SaaS** アプリケーション

イベントメッセージ	イベントの種類	ターゲットの種類	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
Web/SaaS アプリケーションが作成されました	swa/websaasppplicationcreate	websaasapplication	いいえ	はい
Web/SaaS アプリケーションが更新されました	swa/websaasppplicationupdate	websaasapplication	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	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
Web/SaaS アプリケーションが削除されました	swa/websaaspplicationdelete	websaasapplication	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/websaaspplicationcreatefailed	websaasapplication	いいえ	いいえ
Web/SaaS アプリケーションの更新に失敗しました	swa/websaaspplicationupdatefailed	websaasapplication	はい	はい
Web/SaaS アプリケーションの削除に失敗しました	swa/websaaspplicationdeletefailed	websaasapplication	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	イベントの種類	ターゲットの種類	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
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/websaaspplicationsubscriptionsubscribe	websaasapplicationsubscribers		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/websaaspplicationsubscriptionunsubscribe	websaasapplicationsubscribers		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/websaaspplicationsubscriptionsubscribefailed	websaasapplicationsubscribers		いいえ
ユーザー/グループのサブスクリプション解除に失敗しました	swa/websaaspplicationsubscriptionunsubscribefailed	websaasapplicationsubscribers		いいえ

コンテキストに基づくポリシー

イベントメッセージ	イベントの種類	ターゲットの種類	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
コンテキストに基づくポリシーが作成されました	swa/contextualpolicy/create	contextualpolicy	いいえ	はい
コンテキストに基づくポリシーが更新されました	swa/contextualpolicy/update	contextualpolicy	はい	はい
コンテキストに基づくポリシーが削除されました	swa/contextualpolicy/delete	contextualpolicy	はい	いいえ
コンテキストに基づくポリシーの作成に失敗しました	swa/contextualpolicy/createfailed	contextualpolicy	いいえ	いいえ
コンテキストに基づくポリシーの更新に失敗しました	swa/contextualpolicy/updatefailed	contextualpolicy	いいえ	いいえ
コンテキストに基づくポリシーの削除に失敗しました	swa/contextualpolicy/deletefailed	contextualpolicy	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	イベントの種類	ターゲットの種類	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
アプリケーションドメインが作成されました	swa/applicationdomain/create	applicationdomain	いいえ	はい
アプリケーションドメインが更新されました	swa/applicationdomain/update	applicationdomain	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	applicationdomain	はい	いいえ

イベントメッセージ	イベントの種類	ターゲットの種類	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
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	applicationdomain	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	applicationdomain	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	applicationdomain	はい	いいえ

ブラウザー拡張機能の設定

イベントメッセージ	イベントの種類	ターゲットの種類	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
ブラウザー拡張機能の設定が更新されました	swa/browserextensionsettings/updatesucceeded	browserextensionsettings	なし	はい
ブラウザー拡張機能の設定の更新に失敗しました	swa/browserextensionsettings/updatefailed	browserextensionsettings	なし	いいえ

Web サイトの **URL** 一覧とフィルターカテゴリ

イベントメッセージ	イベントの種類	ターゲットの種類	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
Web サイトのフィルター一覧とカテゴリを有効化しました	swa/website/filterlists/webfilterlistcategoryfeature/enabled/update	webfilterlistcategoryfeature	なし	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	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
Web サイトのフィルター一覧を有効化し、フィルター カテゴリを無効化しました	swa/website/filterlist/enabled/urlcategory/disabled/update	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧を無効化し、フィルターカテゴリを有効化しました	swa/website/filterlist/disabled/urlcategory/enabled/update	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧とカテゴリを無効化しました	swa/website/filterlist/disabled/urlcategory/disabled/update	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧とカテゴリを有効化できませんでした	swa/website/filterlist/enabled/urlcategory/enabled/updatefailed	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧を有効化できず、フィルターカテゴリを無効化できませんでした	swa/website/filterlist/enabled/urlcategory/disabled/updatefailed	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧を無効化できず、フィルターカテゴリを有効化できませんでした	swa/website/filterlist/disabled/urlcategory/enabled/updatefailed	websiteurlfiltercategoryfeature		はい
Web サイトのフィルター一覧とカテゴリを無効化できませんでした	swa/website/filterlist/disabled/urlcategory/disabled/updatefailed	websiteurlfiltercategoryfeature		はい
Web サイトの URL 一覧が作成されました	swa/websiteurlfilteringlist/create	websiteurlfilteringlist	いいえ	はい
Web サイトの URL 一覧が更新されました	swa/websiteurlfilteringlist/update	websiteurlfilteringlist	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	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
Web サイトの URL 一覧が削除されました	swa/websiteurlfiltering/deletelist	websiteurlfilteringlist	はい	いいえ
Web サイトの URL 一覧の作成に失敗しました	swa/websiteurlfiltering/createlistfailed	websiteurlfilteringlist	いいえ	いいえ
Web サイトの URL 一覧の更新に失敗しました	swa/websiteurlfiltering/updatelistfailed	websiteurlfilteringlist	はい	いいえ
Web サイトの URL 一覧の削除に失敗しました	swa/websiteurlfiltering/deletelistfailed	websiteurlfilteringlist	はい	いいえ
Web サイトの URL フィルターカテゴリが作成されました	swa/websiteurlfiltering/createcategory	websiteurlfilteringcategory	いいえ	はい
Web サイトの URL フィルターカテゴリが更新されました	swa/websiteurlfiltering/updatecategory	websiteurlfilteringcategory	はい	はい
Web サイトの URL フィルターカテゴリが削除されました	swa/websiteurlfiltering/deletecategory	websiteurlfilteringcategory	はい	いいえ
Web サイトの URL フィルターカテゴリの作成に失敗しました	swa/websiteurlfiltering/createcategoryfailed	websiteurlfilteringcategory	いいえ	いいえ
Web サイトの URL フィルターカテゴリの更新に失敗しました	swa/websiteurlfiltering/updatecategoryfailed	websiteurlfilteringcategory	はい	いいえ
Web サイトの URL フィルターカテゴリの削除に失敗しました	swa/websiteurlfiltering/deletecategoryfailed	websiteurlfilteringcategory	はい	いいえ

Web サイトのフィルターカテゴリプリセット

イベントメッセージ	イベントの種類	ターゲットの種類	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
Web サイトのフィルターカテゴリプリセットを更新しました	swa/websiteurlfilter/categoryupdate	category/urlfilter/categorypreset	category	はい
Web サイトのフィルターカテゴリプリセットを更新できませんでした	swa/websiteurlfilter/categoryupdatefailed	category/urlfilter/categorypreset	category	はい

禁止する **Web** サイトの **URL** 一覧とフィルターカテゴリ

イベントメッセージ	イベントの種類	ターゲットの種類	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
禁止する Web サイトの URL 一覧が作成されました	swa/websiteurlfilter/blockedlistcreate	website/urlfilter/blockedlist	いいえ	はい
禁止する Web サイトの URL 一覧が更新されました	swa/websiteurlfilter/blockedlistupdate	website/urlfilter/blockedlist	いいえ	はい
禁止する Web サイトの URL 一覧が削除されました	swa/websiteurlfilter/blockedlistdelete	website/urlfilter/blockedlist	いいえ	はい
禁止する Web サイトの URL 一覧の作成に失敗しました	swa/websiteurlfilter/blockedlistcreatefailed	website/urlfilter/blockedlist	いいえ	はい
禁止する Web サイトの URL 一覧の更新に失敗しました	swa/websiteurlfilter/blockedlistupdatefailed	website/urlfilter/blockedlist	いいえ	はい
禁止する Web サイトの URL 一覧の削除に失敗しました	swa/websiteurlfilter/blockedlistdeletefailed	website/urlfilter/blockedlist	いいえ	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	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
禁止する Web サイトの URL フィルターカテゴリが作成されました	swa/websiteurlfiltercategory/blocked/create	category/blocked/state	いいえ	はい
禁止する Web サイトの URL フィルターカテゴリが更新されました	swa/websiteurlfiltercategory/blocked/update	category/blocked/state	いいえ	はい
禁止する Web サイトの URL フィルターカテゴリが削除されました	swa/websiteurlfiltercategory/blocked/delete	category/blocked/state	いいえ	はい
禁止する Web サイトの URL フィルターカテゴリの作成に失敗しました	swa/websiteurlfiltercategory/blocked/create	category/blocked/state	failed	はい
禁止する Web サイトの URL フィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/blocked/update	category/blocked/state	failed	はい
禁止する Web サイトの URL フィルターカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/blocked/delete	category/blocked/state	failed	はい

許可する **Web** サイトの **URL** 一覧とフィルターカテゴリ

イベントメッセージ	イベントの種類	ターゲットの種類	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
許可する Web サイトの URL 一覧が作成されました	swa/websiteurlfilterwebsite/allowed/create	website/allowed/list	いいえ	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	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
許可する Web サイトの URL 一覧が更新されました	swa/websiteurlfilterwebsiteallowedlist/update	websiteallowedlist	いいえ	はい
許可する Web サイトの URL 一覧が削除されました	swa/websiteurlfilterwebsiteallowedlist/delete	websiteallowedlist	いいえ	はい
許可する Web サイトの URL 一覧の作成に失敗しました	swa/websiteurlfilterwebsiteallowedlist/createfailed	websiteallowedlist	いいえ	はい
許可する Web サイトの URL 一覧の更新に失敗しました	swa/websiteurlfilterwebsiteallowedlist/updatefailed	websiteallowedlist	いいえ	はい
許可する Web サイトの URL 一覧の削除に失敗しました	swa/websiteurlfilterwebsiteallowedlist/deletefailed	websiteallowedlist	いいえ	はい
許可する Web サイトの URL フィルターカテゴリが作成されました	swa/websiteurlfiltercategory/allowedlist/create	categoryallowedlist	いいえ	はい
許可する Web サイトの URL フィルターカテゴリが更新されました	swa/websiteurlfiltercategory/allowedlist/update	categoryallowedlist	いいえ	はい
許可する Web サイトの URL フィルターカテゴリが削除されました	swa/websiteurlfiltercategory/allowedlist/delete	categoryallowedlist	いいえ	はい
許可する Web サイトの URL フィルターカテゴリの作成に失敗しました	swa/websiteurlfiltercategory/allowedlist/createfailed	categoryallowedlist	いいえ	はい
許可する Web サイトの URL フィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/allowedlist/updatefailed	categoryallowedlist	いいえ	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	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
許可する Web サイトの URL フィルターカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/allowed/deletefailed	category/allowedlist		はい

Remote Browser Isolation（旧称 **Secure Browser**）の **Web** サイト **URL** 一覧およびフィルター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	イベントの種類	ターゲットの種類	アクターの種類	エージェント 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
Secure Browser にリダイレクトする Web サイトの URL 一覧が作成されました	swa/websiteurlfilteringlist/redirected/create	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL 一覧が更新されました	swa/websiteurlfilteringlist/redirected/update	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL 一覧が削除されました	swa/websiteurlfilteringlist/redirected/delete	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL 一覧の作成に失敗しました	swa/websiteurlfilteringlist/redirected/createfailed	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL 一覧の更新に失敗しました	swa/websiteurlfilteringlist/redirected/updatedfailed	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL 一覧の削除に失敗しました	swa/websiteurlfilteringlist/redirected/deletefailed	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリが作成されました	swa/websiteurlfiltercategory/redirected/create	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリが更新されました	swa/websiteurlfiltercategory/redirected/update	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリが削除されました	swa/websiteurlfiltercategory/redirected/delete	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリの作成に失敗しました	swa/websiteurlfiltercategory/redirected/createfailed	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリの更新に失敗しました	swa/websiteurlfiltercategory/redirected/updatefailed	websiteurlfilteringlist	いいえ			はい
Secure Browser にリダイレクトする Web サイトの URL フィルターカテゴリの削除に失敗しました	swa/websiteurlfiltercategory/redirected/deletefailed	websiteurlfilteringlist	いいえ			はい

Citrix Workspace のシステムログイベント

April 20, 2022

ここでは、Citrix Workspace に対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について詳しくは、「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。

システムログについて詳しくは、「システムログ」を参照してください。

ワークスペース URL

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
ワークスペース URL が更新されました	wxp/url/update	subscriber	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	subscriber	URL を更新しようとした管理者	はい	はい
ワークスペース URL が有効化されました	wxp/url/enable	subscriber	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 を有効にできませんでした	wxp/url/enablefailed	subscriber	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 が無効化されました	wxp/url/disable	subscriber	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 を無効にできませんでした	wxp/url/disablefailed	subscriber	ワークスペース URL のカスタマイズを無効にしようとした管理者	いいえ	はい

Workspace の認証

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
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	subscriber	ワークスペースの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	subscriber	ワークスペースの認証方法を更新しようとした管理者	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
ワークスペースフェデレーション認証サービス（FAS）が有効化されました	wxp/fas/enable	subscriber	FAS を有効にした管理者	いいえ	はい
ワークスペースフェデレーション認証サービス（FAS）を有効にできませんでした	wxp/fas/enablefailed	subscriber	FAS を有効にしようとした管理者	いいえ	はい
ワークスペースフェデレーション認証サービス（FAS）が無効化されました	wxp/fas/disable	subscriber	FAS を無効にした管理者	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
ワークスペースフェデレーション認証サービス（FAS）を無効にできませんでした	wxp/fas/disablefailed	subscriber	FAS を無効にしようとした管理者	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 のお気に入り機能が有効化されました	wxp/favorites/enable	subscriber	お気に入りを有効にした管理者	いいえ	はい
Workspace のお気に入り機能を有効にできませんでした	wxp/favorites/enablefailed	subscriber	お気に入りを有効にしようとした管理者	いいえ	はい
Workspace のお気に入り機能が無効化されました	wxp/favorites/disable	subscriber	お気に入りを無効にした管理者	いいえ	はい
Workspace のお気に入り機能を無効にできませんでした	wxp/favorites/disablefailed	subscriber	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
ワークスペースのパスワードの変更オプションポリシーが更新されました	wxp/changepasswordoption/updatepolicy	subscription	Citrix Workspace 内でパスワード変更のポリシーを更新した管理者	はい	はい
ワークスペースのパスワード変更オプションポリシーの更新に失敗しました	wxp/changepasswordoption/updatepolicyfailed	subscription	Citrix Workspace 内でパスワード変更のポリシーを更新しようとした管理者	はい	はい
ワークスペースのパスワードの変更オプションが有効化されました	wxp/changepasswordoption/enable	subscription	Citrix Workspace 内でパスワード変更の設定を有効にした管理者	いいえ	はい
ワークスペースのパスワード変更オプションを有効にできませんでした	wxp/changepasswordoption/enablefailed	subscription	Citrix Workspace 内でパスワード変更の設定を有効にしようとした管理者	いいえ	はい
ワークスペースのパスワードの変更オプションが無効化されました	wxp/changepasswordoption/disable	subscription	Citrix Workspace 内でパスワード変更の設定を無効にした管理者	いいえ	はい
ワークスペースのパスワード変更オプションを無効にできませんでした	wxp/changepasswordoption/disablefailed	subscription	Citrix Workspace 内でパスワード変更の設定を無効にしようとした管理者	いいえ	はい

長期有効トークン

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
ワークスペースの長期有効トークン構成が更新されました	wxp/longlivedtoken/update	subscriber	トークン構成を更新した管理者	はい	はい
ワークスペースの長期有効トークン構成の更新に失敗しました	wxp/longlivedtoken/updatefailed	subscriber	トークン構成を更新しようとした管理者	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
ワークスペースセッションの構成が更新されました	wxp/sessions/update	subscriber	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
ワークスペースセッションの構成を更新できませんでした	wxp/sessions/updatefailed	subscriber	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とした管理者	はい	はい

機能のロールアウト

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
インテリジェントなワークスペース環境用に割り当てられたユーザーとグループが更新されました	wxp/iws/features/subscribers/groups/update	subscribersgroups	Citrix Workspace の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ワークスペース環境に更新されたユーザーとグループを割り当てることができませんでした	wxp/iws/features/subscribers/groups/update/failed	subscribersgroups	Citrix Workspace の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ようとした管理者	いいえ	いいえ
インテリジェントなワークスペース環境が有効化されました	wxp/iws/features/subscriber/enable	subscriber	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
インテリジェントなワークスペース環境を有効にできませんでした	wxp/iws/features/subscriber/enable/failed	subscriber	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
インテリジェントなワークスペース環境が無効化されました	wxp/iws/features/disable	user	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ワークスペース環境を無効にできませんでした	wxp/iws/features/disablefailed	user	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

SDK および API

July 2, 2024

Citrix Cloud では、情報を取得する API や、複雑で反復的な以下のようなタスクを自動化するための API を複数提供しています:

- 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を管理するためのレポートを作成して利用する
- 顧客の使用権ステータスを確認する
- 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の場所に関する詳細を取得する

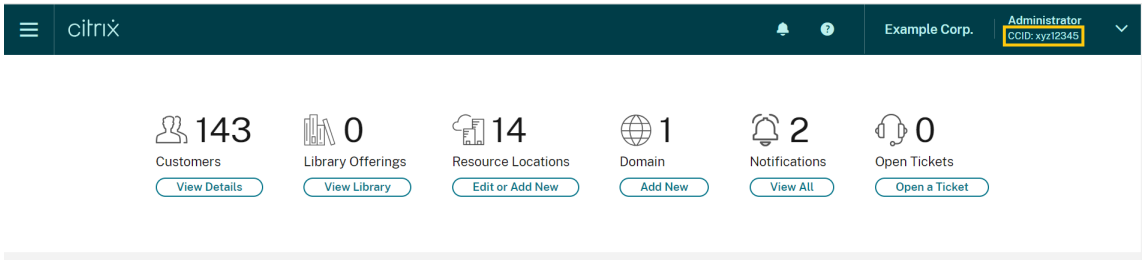
いくつかの Citrix Cloud サービスは、情報の取得、データのクエリ、および管理タスクの実行を可能にする SDK および API も提供します。

セキュアクライアント

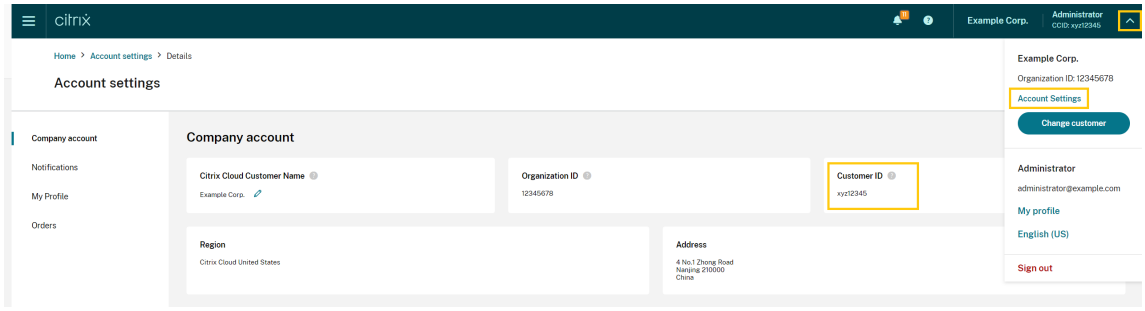
Citrix Cloud API を使用するには、ユーザーに代わって Citrix Cloud にアクセスするセキュアクライアントを作成する必要があります。セキュアクライアントを作成するには、Citrix Cloud アカウントの顧客 ID を提供する必要が

あります。顧客 ID は、管理コンソールの次の場所にあります:

- コンソールの右上隅、ユーザー名の下。



- ［アカウント設定］ページ。



- ［**API** アクセス］ページ。

継承された権限

セキュアクライアントは、Citrix Cloud の単一の管理者と単一の顧客 ID に関連付けられています。これは、特定の顧客 ID にある同じレベルの権限をセキュアクライアントが継承することを意味します。したがって、フルアクセス権限がある場合は、セキュアクライアントにもフルアクセス権限があります。後で権限レベルが低下した場合、既に作成したセキュアクライアントは、低下した権限を自動的に継承します。

セキュアクライアントを作成する手順については、Citrix Developer ドキュメントの「Get started with Citrix Cloud APIs」を参照してください。

クラウドライセンス **API**

企業のお客様は、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。シトリックスパートナーは、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。

詳しくは、Citrix Developer ドキュメントの「APIs to manage Citrix cloud licensing」を参照してください。

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 の使用について詳しくは、Citrix Developer ドキュメントの「Citrix Cloud - SystemLog」を参照してください。

リソースの場所 API

リソースの場所 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の、リソースの場所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の場所の 1 つに、Citrix Cloud Connector をサイレントインストールするとします。この API を使用して、リソースの場所 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 の使用について詳しくは、Citrix Developer ドキュメントの「Citrix Cloud - Resource Location」を参照してください。

サービス使用権 API

サービス使用権 API は、顧客に使用権があるサービス、各使用権の残り日数、および顧客が購入した使用権の数を取得します。この API の使用について詳しくは、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 管理者に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。

他のサービスの SDK と API

他の Citrix Cloud サービスで使用できる SDK および API について詳しくは、次の記事を参照してください:

- Digital workspaces: Citrix DaaS や Citrix Workspace などのワークスペースサービス用の SDK と API が含まれています。
- App delivery and security: コンソール、Intelligent Traffic Management、SD-WAN Orchestrator などのネットワーキングおよびアプリデリバリーサービス用の SDK と API が含まれています。

追加情報

Citrix Cloud API とセキュアクライアントが、クラウドへの移行やプッシュトークンを使用した認証の構成などの複雑な操作の実行にどのように役立つかについて詳しくは、次の Tech Zone の記事を参照してください:

- 概念実証ガイド：プッシュトークンを使用した Citrix Gateway 認証用の nFactor
- 展開ガイド：Citrix Virtual Apps and Desktops を VMware vSphere から Microsoft Azure 上の Citrix Virtual Apps and Desktops サービスに移行する
- 概念実証ガイド：自動構成ツール

パートナー向けの **Citrix Cloud**

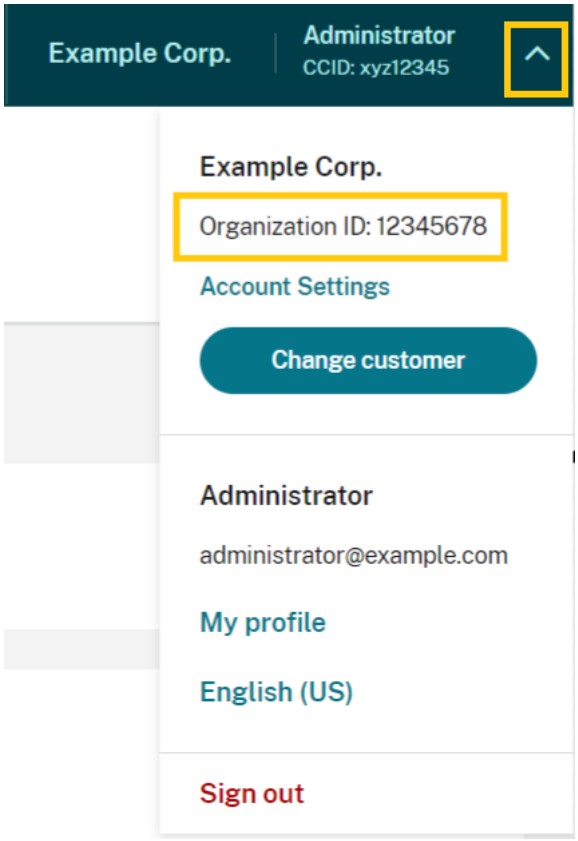
April 5, 2024

Citrix Cloud には、顧客とパートナーの両方用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 Cloud サービスおよびソリューション上で Citrix パートナーが利用できる、顧客とのコラボレーションに役立つ機能について説明します。

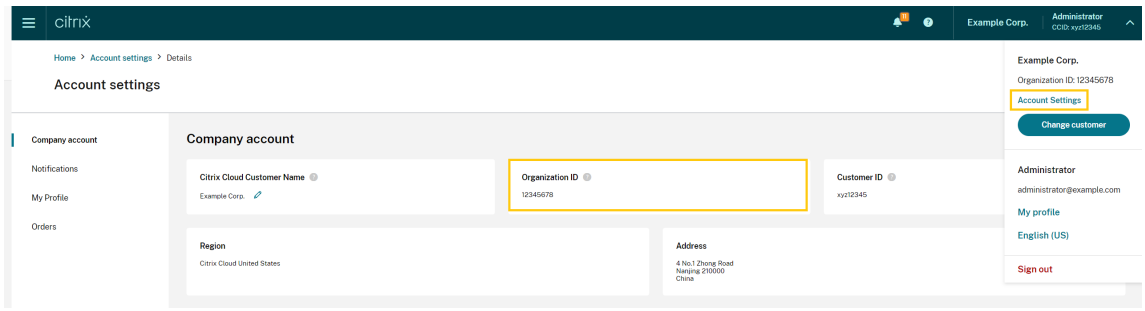
パートナー **ID**

パートナーは、Citrix 組織 ID（ORGID）に基づいて Citrix Cloud で識別されます。パートナーは、Citrix Cloud 管理コンソールの以下の場所で、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：

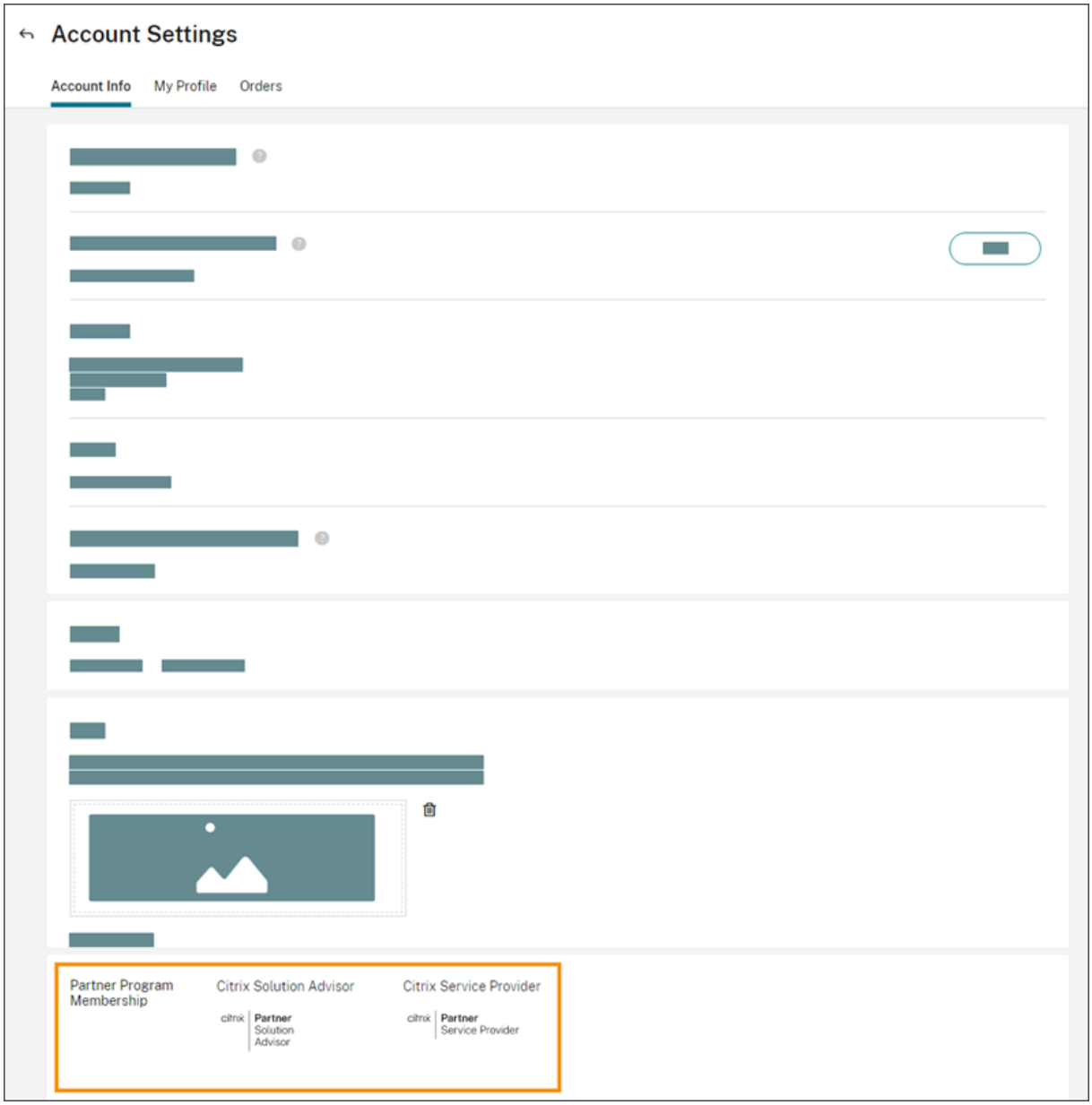
- 顧客メニューから。コンソールの右上隅にある顧客名をクリックします。メニューの会社名の下に ORGID が表示されます。



- ［アカウント設定］ページから。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。

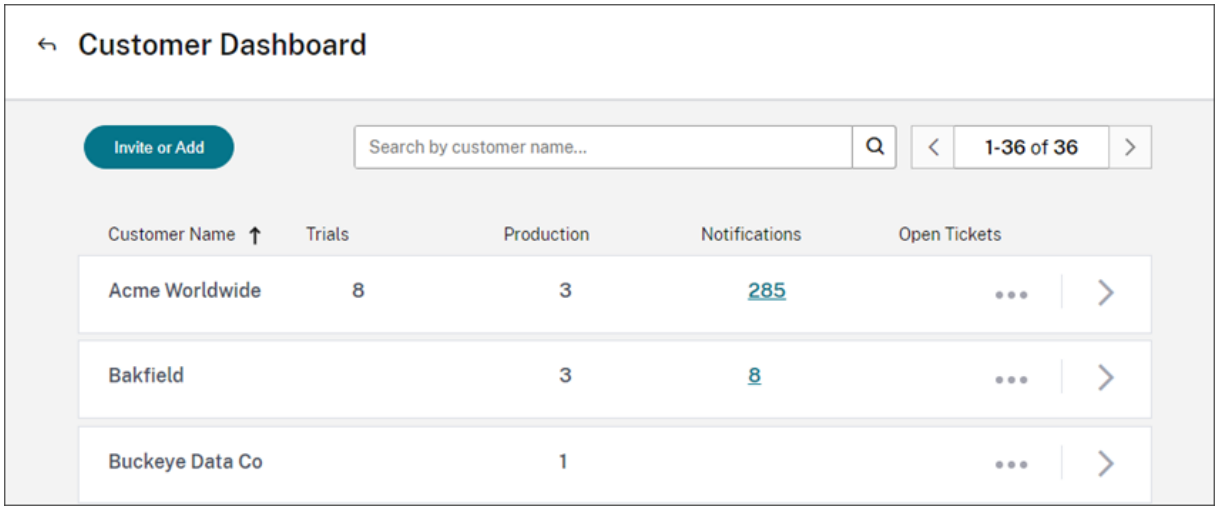


アカウントの ORGID が Citrix パートナープログラム（Citrix Solution Advisor や Citrix Service Provider）のアクティブなメンバーである場合は、Citrix パートナーがこのアカウントを所有していることを示すプログラムバッジが表示されます。パートナー ID は、追加のクラウドサービスや機能へのアクセスを管理するために使用されます。

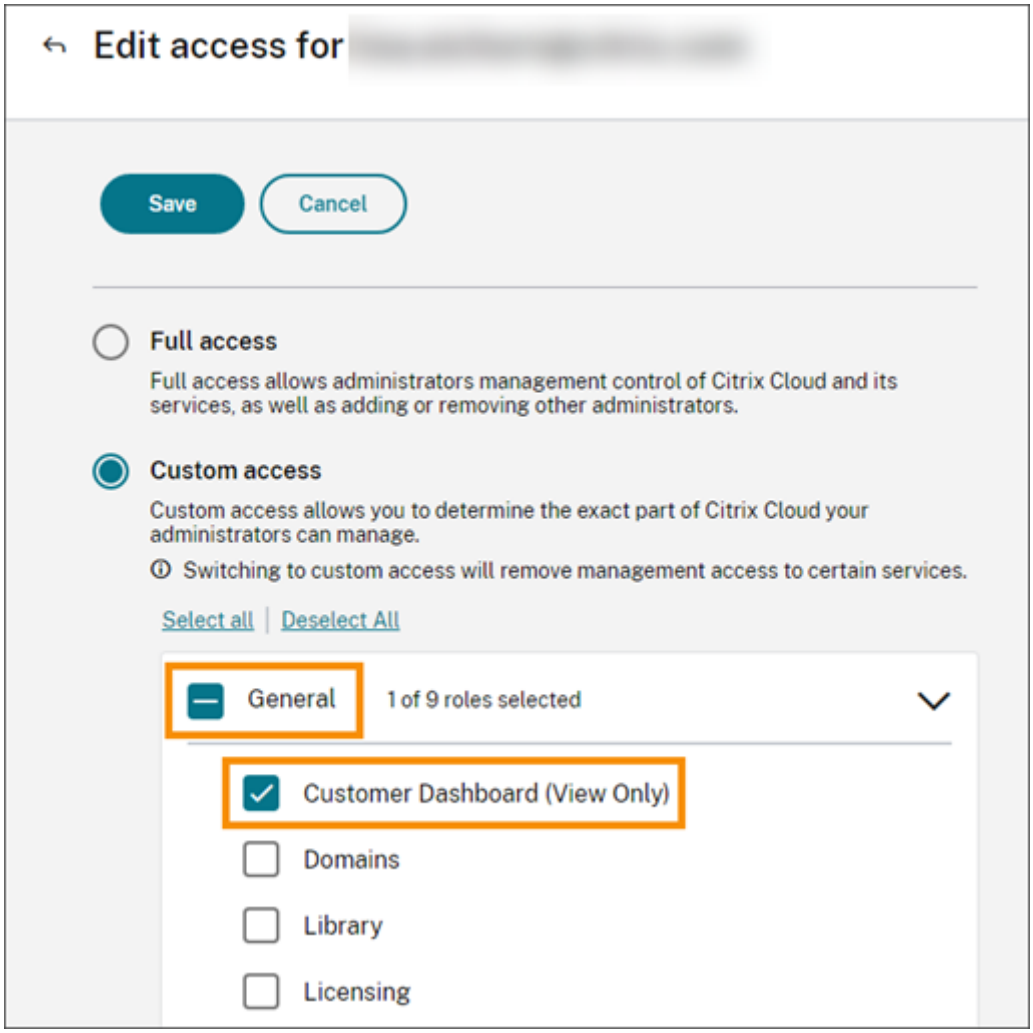


顧客ダッシュボード

顧客ダッシュボードは、パートナーが統合されたビューで複数の Citrix Cloud 顧客の状態を確認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ためには、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。顧客ダッシュボードは、パートナーバッジを持つ Citrix Cloud アカウントで使用できます。



デフォルトでは、フルアクセス権を持つ管理者は顧客ダッシュボードを表示できます。カスタムアクセス権の管理者は、顧客ダッシュボード（表示のみ）の権限がオンになっている場合に、顧客ダッシュボードを表示できます。Citrix Cloud の管理者権限について詳しくは、「管理者権限の変更」を参照してください。



パートナーと顧客の接続

Citrix Cloud ソリューションで顧客とコラボレーションしているパートナーは、アカウント間で信頼済み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って、顧客は特定の情報を簡単にパートナーと共有できるようになります。顧客はパートナーと接続することにより、Citrix Cloud アカウントおよび Citrix との関係に関する情報を閲覧する権限をパートナーに付与します。

パートナー接続を確立すると、以下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
- 顧客アカウントの設定にパートナーがアクティブな接続として表示される
- パートナーに Citrix Cloud サービス使用権が表示される
- パートナーにライセンス使用状況とアクティブな Citrix Cloud サービス使用権が表示される

パートナーと顧客が接続されると、パートナーの管理者は、顧客の基本アカウント情報、顧客の注文の詳細とともに、サービス、ライセンス数、有効期限などの使用権情報を表示できます。

パートナーと顧客の接続には有効期限がありません。

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の接続を確立できます。パートナーは最大 100 個の顧客アカウントに関連付けることができます。パートナーが 100 個を超える顧客アカウントを管理する必要がある場合、追加の顧客を管理するには、別のメールアドレスで別のパートナーアカウントを作成する必要があります。また、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もできます。

顧客は複数のパートナーとの接続を確立できます。顧客とパートナーと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。

- パートナーが顧客との接続を作成する
- 顧客がパートナーとの接続を終了する

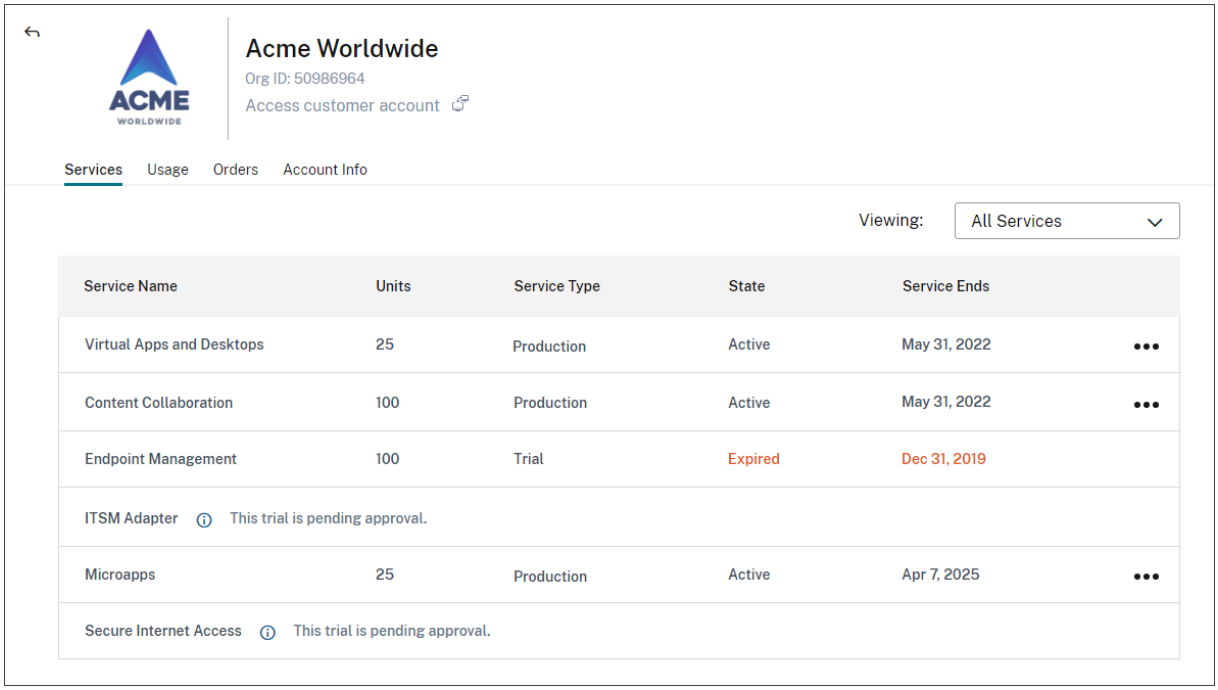
パートナーが顧客との接続を終了すると、Citrix Cloud は顧客に通知を送信します。

サービス使用権のパートナーへの表示

顧客に接続すると、パートナーはその顧客のサービス使用権のステータスを表示できます。この情報には、トライアルとトライアル以外の両方の使用権の状態が含まれます。パートナーは次の情報も表示できます。

- アクティブなサービストライアル

- 保留中のサービストライアルリクエスト
- 期限切れのサービストライアル
- アクティブなサービスの使用権（顧客が購入したサービス、または権限が付与されたサービスや有効なサービス）
- 使用権のライセンス数と有効期限



ライセンスの表示は、ライセンスの割り当てと使用状況の傾向の概要に限定されます。

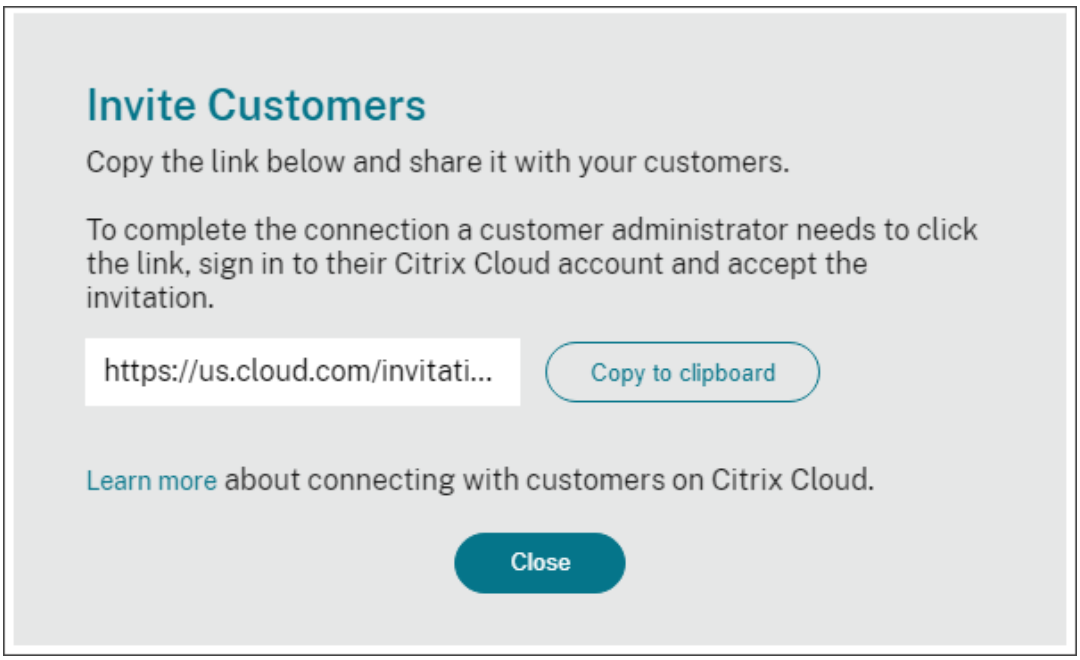
顧客との接続を作成する

パートナーは、独自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。

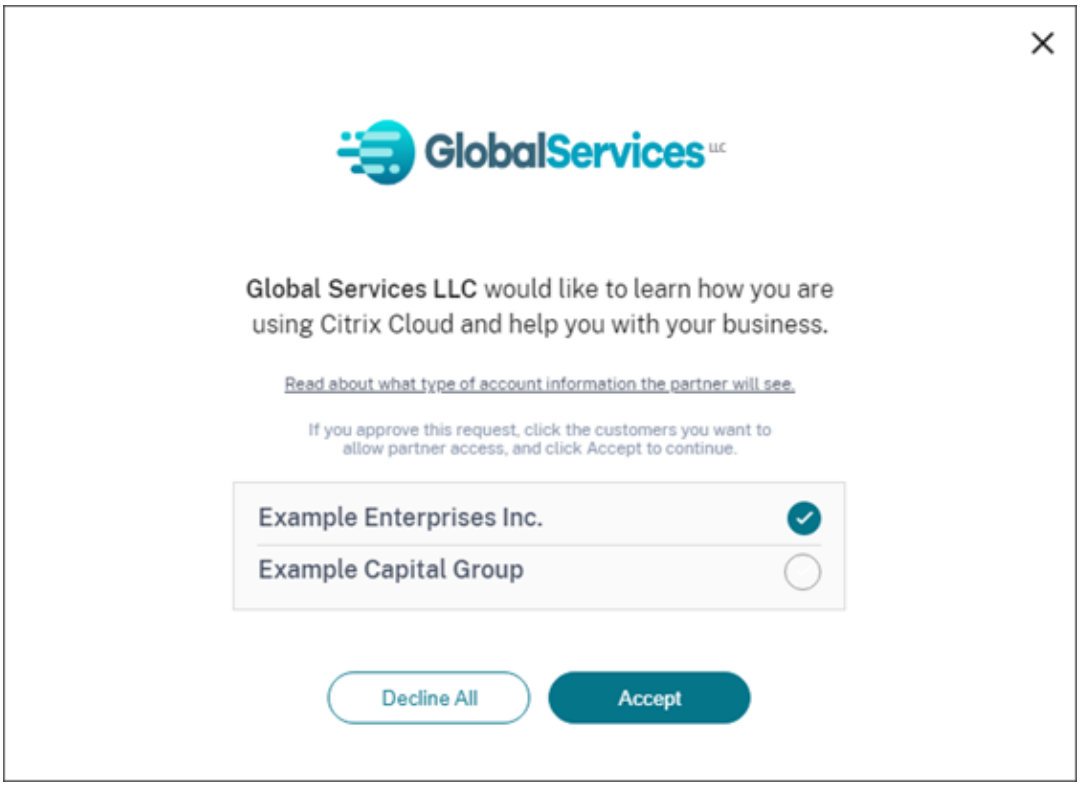
パートナーは、招待リンクを無制限に使用して、接続を作成または再作成できます。招待リンクには有効期限がありません。

接続を作成するには：

1. 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、［招待または追加］を選択します。
3. 既存の Citrix Cloud 顧客と接続するには：
    a) ［**Citrix Cloud** 顧客を招待］を選択し、［続行］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、顧客は招待リンクをクリックし、Citrix Cloud にサインインして、招待を受け入れます。



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、［続行］を選択します。

b) 顧客のビジネス連絡先の詳細を入力し、［完了］を選択します。Citrix Cloud は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管理者として新しいアカウントに追加されたという通知を受け取ります。顧客は、Citrix Cloud サインインページの「パスワードをお忘れですか。」リンクを使用して、新しい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、顧客はビジネス用メールアドレスを使用して自分のアカウントにサインインし、「Citrix Cloud へのサインアップ」の説明に従って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との接続を削除する

パートナーと顧客のいずれも、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、管理する顧客を見つけます。
3. 顧客の省略記号メニューをクリックし、［顧客の接続を削除］を選択します。
4. 削除を確認するプロンプトが表示されたら、［削除］を選択します。

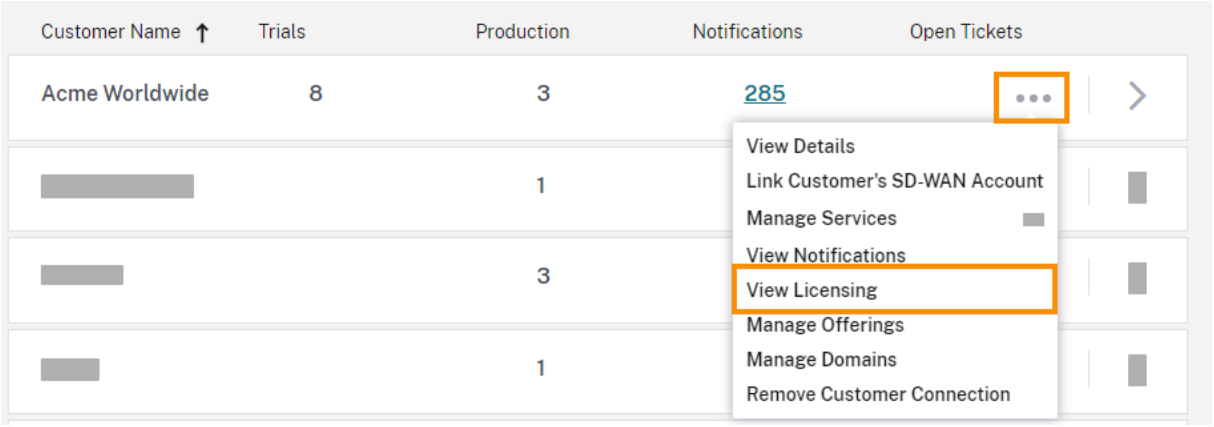
パートナーとの接続を削除する

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. 削除を確認するプロンプトが表示されたら、［確認］を選択します。

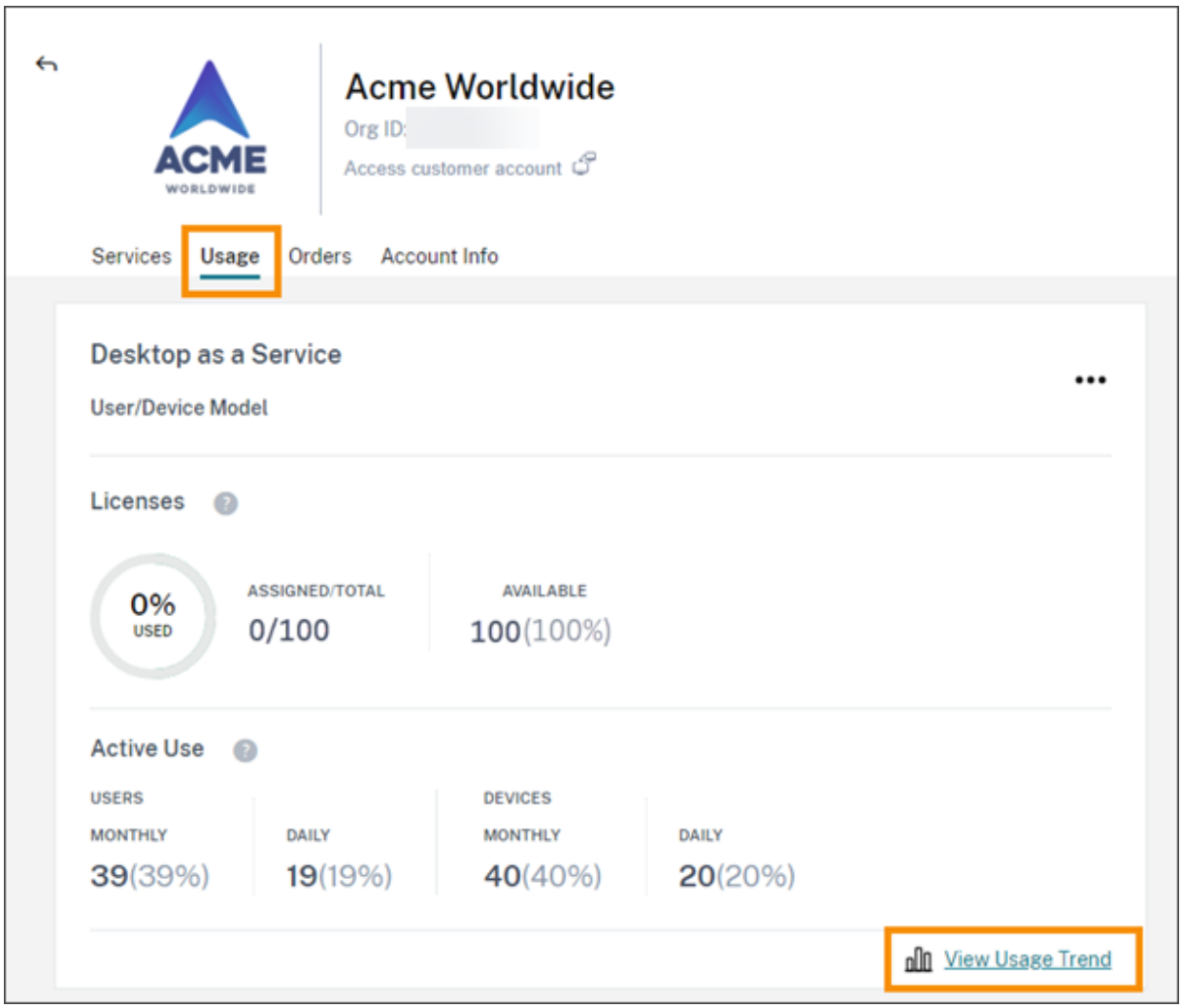
ライセンスの傾向

パートナーは、顧客ダッシュボードの省略記号メニューで ［ライセンスの表示］を選択することで、顧客のライセンス情報を表示できます。



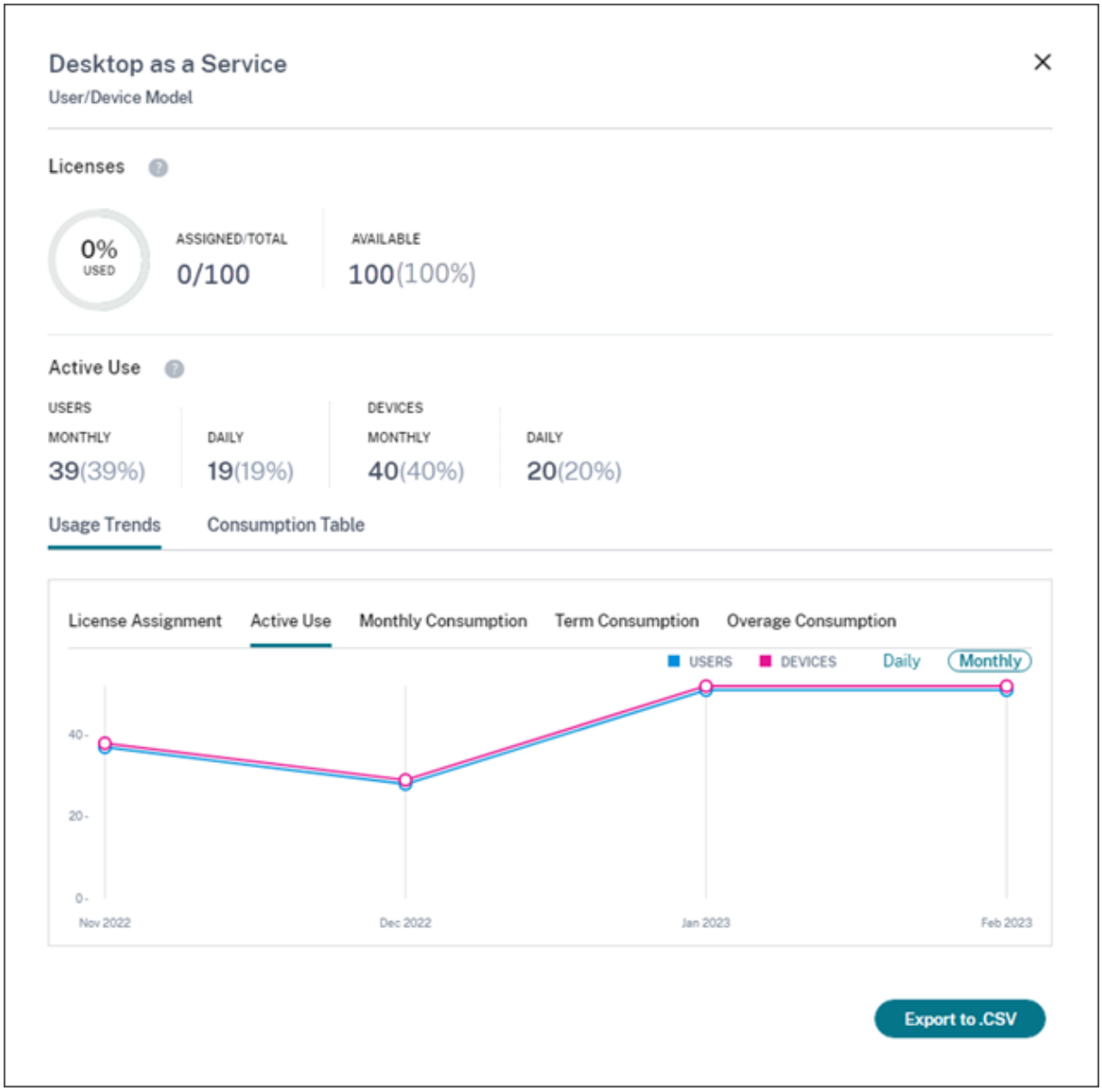
> 注:
>
> Citrix パートナーは、ライセンスの概要ビューと、アクティブな使用状況の履歴の傾向のみを表示できます。特定のサービスのライセンスを消費する個々のユーザーを表示することはできません。

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］タブを選択します。使用状況について詳しくは、表示するサービス使用権の ［使用状況の傾向の表示］を選択してください。



サービスによっては、使用状況の傾向には次の情報が含まれます:

- 購入済み合計ライセンスに対する割り当て済みライセンスの比率
- 月ごと/日ごとのアクティブユーザー数
- ライセンスの割り当て、アクティブな使用、使用権ごとの消費量、および超過量の内訳のビジュアル表示。



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。

帯域幅使用量

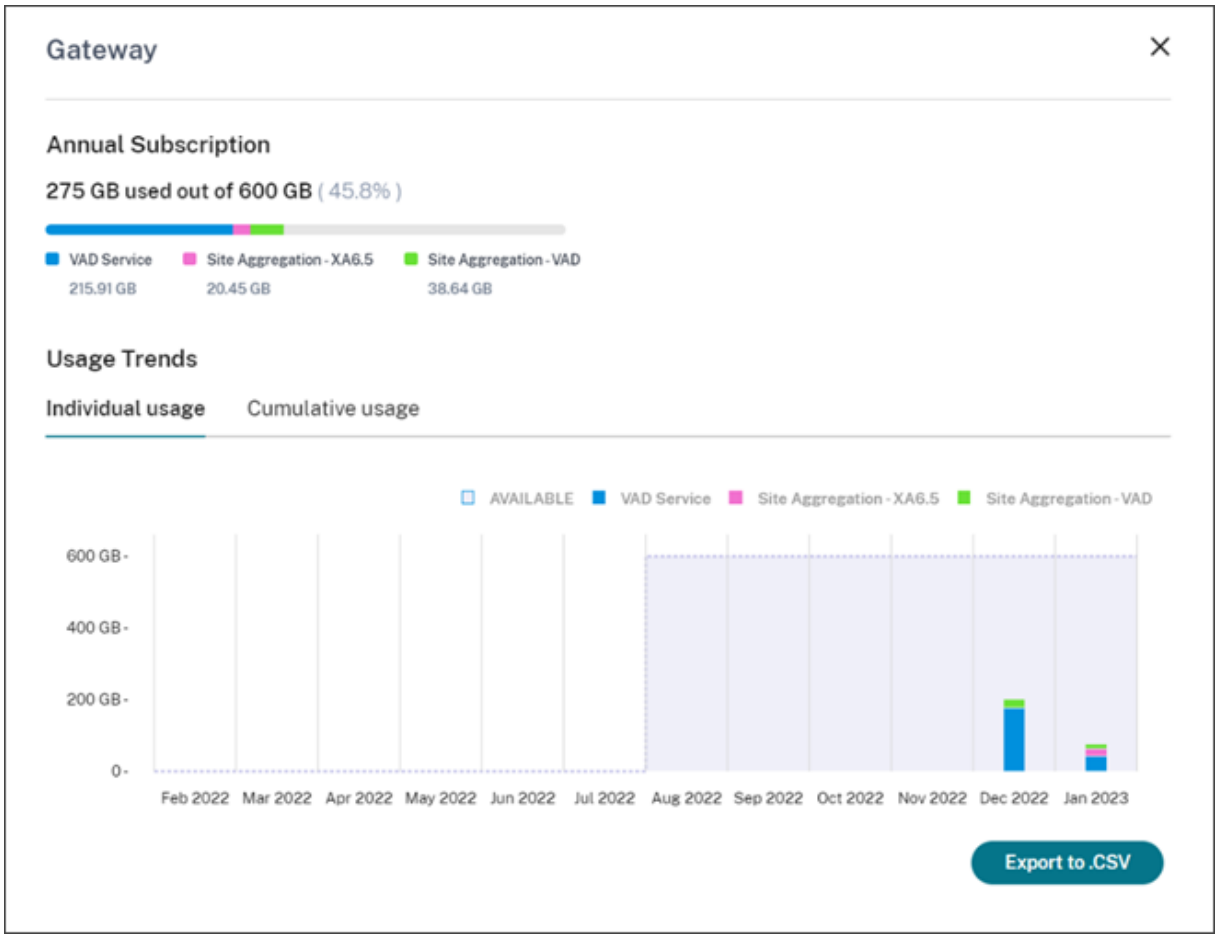
Citrix Gateway サービスの場合、ライセンスの概要には次の情報が含まれます:

- 顧客のすべての使用権に関する帯域幅の合計使用量。
- 月間、年間、期限付きごとの使用権で分類された帯域幅の合計使用量。
- 当月の合計超過量。超過分の計算方法について詳しくは、「超過」を参照してください。

使用状況の概要を表示するには、使用権のページの一番右側にある［使用状況の傾向の表示］を選択します。［超過消費グラフの表示］を選択して、過去 12 か月間の超過量を表示します。

使用権によっては、使用状況の傾向に次の情報が含まれます：

- Citrix DaaS（**VAD** サービス）と、サイトアグリゲーションを使用したオンプレミスの Virtual Apps and Desktops 展開の間で消費される帯域幅の量。
- 月ごとの帯域幅使用量の内訳に関するビジュアル表示。（月間の使用権）
- 課金期間の各月において発生した帯域幅の使用量（使用権別）に関する内訳のビジュアル表示。（年間および期限付きの使用権）
- 請求期間の各月において累積された帯域幅の使用量（累積）に関する内訳のビジュアル表示。（年間および期限付きの使用権）



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 の顧客のライセンスと使用状況

Citrix Cloud のライセンス機能により、Citrix Service Provider（CSP）の顧客は、サポートされている Citrix DaaS（旧称 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。詳しくは、次の記事を参照してください：

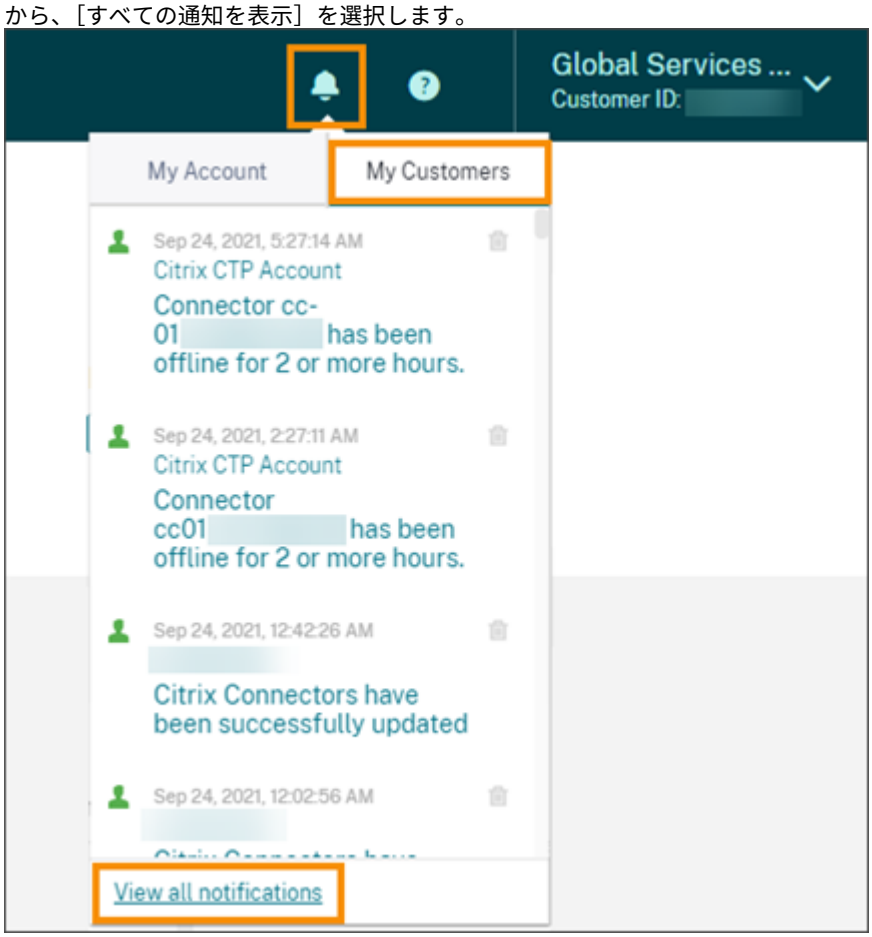
- Citrix DaaS の顧客ライセンスと使用状況の監視
- Citrix DaaS Standard for Azure の顧客ライセンスと使用状況の監視

顧客の通知およびサポートチケットをパートナーに表示

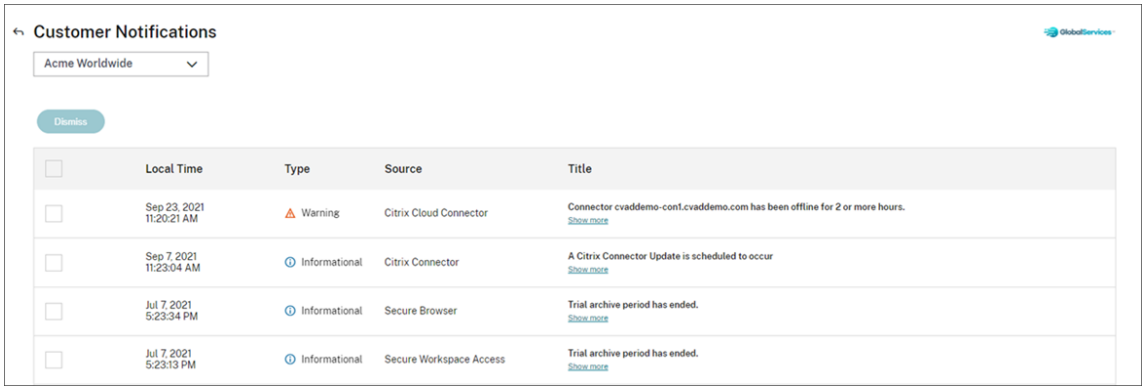
パートナーは、接続された顧客の通知を表示できます。また、特定の顧客ごとに通知を絞り込み、通知を消去するなどの対応を取ることもできます。消去された通知は、パートナーには表示されません。ただし、顧客は Citrix Cloud にサインインした後、アカウントで通知を表示できます。

顧客の通知を表示するには:

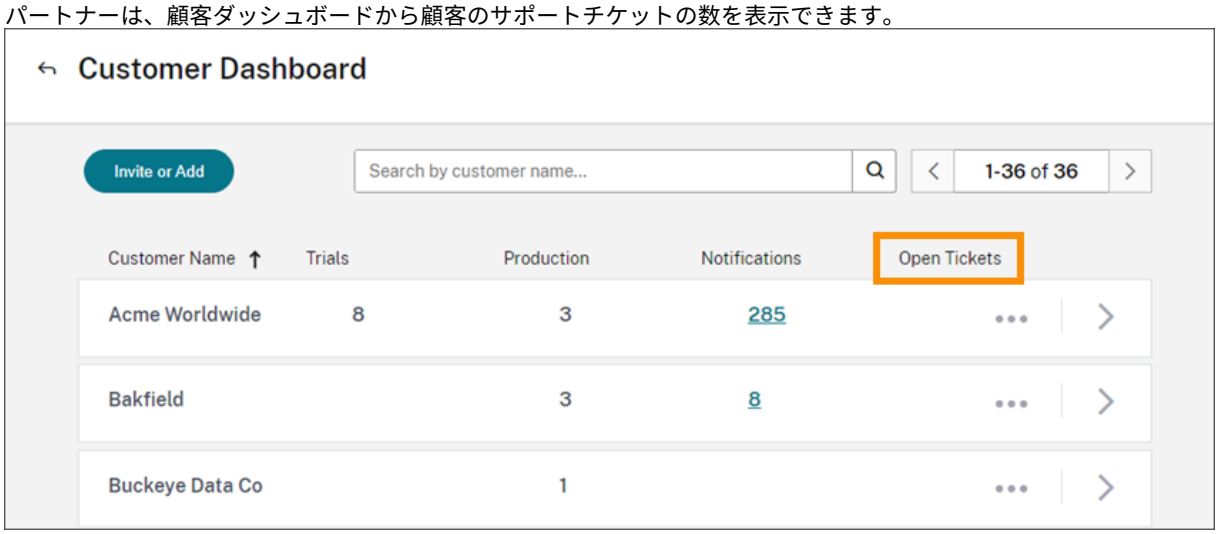
1. 顧客の通知を表示するには、管理コンソールの上部にあるベルアイコンをクリックし、[マイ顧客] を選択してから、[すべての通知を表示] を選択します。



2. ドロップダウンメニューから顧客を選択して、その顧客の通知を表示します。



パートナーは、顧客ダッシュボードから顧客のサポートチケットの数を表示できます。



Citrix Service Provider の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、Citrix Service Provider のリソースの場所に関連付けられたドメインの資格情報を使用して、ワークスペースにサインインできます。これにより、顧客ユーザーが _customer.cloud.com_ などのカスタムワークスペースの URL を使用してアクセスできる専用のワークスペースを提供できます。リソースの場所は引き続きパートナーの Citrix Cloud アカウント上にあります。顧客が Citrix Serivce Provider ワークスペースの URL（csppartner.cloud.com など）を使用してアクセスできる共有ワークスペースとともに、専用のワークスペースを提供できます。顧客が専用のワークスペースにアクセスできるようにするには、管理する適切なドメインに顧客を追加します。ワークスペースを構成した後、顧客ユーザーはワークスペースにサインインして、Citrix DaaS で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の資格情報を使用してワークスペースにアクセスできなくなります。

フェデレーションドメインを使用してアプリとデスクトップを配信する方法について詳しくは、「Citrix Service Provider 用の Citrix DaaS」を参照してください。

Citrix Service Provider のワークスペースの外観オプション

カスタムテーマを使用して、ワークスペースの色とロゴを構成できます。カスタムテーマを作成する方法については、「ワークスペースの外観をカスタマイズする」を参照してください。

> 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のテナントがリソースの場所、Cloud Connector、および Active Directory ドメイン（マルチテナント）を共有する Citrix Service Provider は、現在サポートされていません。専用のリソースの場所、Cloud Connector、および専用の Active Directory ドメイン（シングルテナント）を持つ Citrix Service Provider テナントが完全にサポートされています。

クラウドサービス

July 2, 2024

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掲載します。これらのサービス、およびこれらが含まれている製品の説明については、「Service Descriptions for Citrix Services」を参照してください。

Citrix サービス

分析

- Analytics for Security
- Analytics for Performance
- Analytics - Usage

Citrix DaaS

Citrix DaaS Standard for Azure

Endpoint Management

Gateway

ServiceNow 用の ITSM アダプター

Remote Browser Isolation

Secure Private Access

Session Recording サービス

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

NetScaler サービス

Console

App Delivery and Security

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall