

シトリックス クラウド ジャパン

Citrix Cloud Japanは、Citrix Cloudから分離され、独立したクラウドであり、日本のお客様が専用のCitrix管理環境で特定のCitrix Cloudサービスを利用できるようにします。

Citrix Cloud Japanのドキュメントでは、アカウントの設定方法とサポートされているサービスについて詳しく説明しています。このドキュメントでは、Citrix Cloud Japanのサービスと機能が他のCitrix Cloudリージョンと比較してどのような違いがあるかについても説明しています。Citrix Cloud JapanとCitrix Cloudの両方で機能と性能が同じである場合、このドキュメントはCitrix Cloudドキュメント内の既存の情報へのリンクを提供します。

利用可能なサービス

Citrix Cloud Japanで利用できるサービスは次のとおりです。

- シトリックス ゲートウェイ
- シトリックス DaaS™ (旧称 Virtual Apps and Desktops)
- License Usage Insights (Citrixパートナーのみ)
- セキュア ブラウザ
- シトリックス ワークスペース™
- Workspace Environment Managementサービス (Citrix Cloud Connectorバージョン 6.29.0.58841 以降が必要)
- ライセンス アクティベーション サービス

詳細については、「[Feature availability for services](#)」を参照してください。

非地域データ

お客様によるクラウドサービスの利用に関する情報を含む特定のログは、地域に依存しない性質を持っています。このデータは、サポートやトラブルシューティング、パフォーマンス監視、セキュリティ、監査、およびクロスリージョン認証を可能にするためなど、クラウドサービスをサポートするために必要に応じて、地域外で複製およびアクセスされる場合があります。

サービスを実行するために必要に応じて、Citrixのサードパーティサプライヤーによってログが地域外で処理される場合があります。詳細については、[Citrix Cloud Services Data Protection Overview](#)を参照してください。

サードパーティ通知

Citrix Cloud Japanには、プラットフォームおよびサポート対象サービスに関するサードパーティ通知ドキュメントで定義されている条件に基づいてライセンス供与されたサードパーティソフトウェアが含まれる場合があります。詳細については、[Citrix Cloud Third Party Notifications](#)を参照してください。

新機能

Citrixは、利用可能になり次第、Citrix Cloud Japanのお客様に新機能とアップデートを提供することを目指しています。新しいリリースはより多くの価値を提供するので、アップデートを遅らせる理由はありません。

このプロセスは透過的です。最初のアップデートはCitrixの内部サイトにのみ適用され、その後、お客様の環境に段階的に適用されます。アップデートを段階的に提供することで、製品の品質と可用性が最大化されます。

クラウドの規模とサービスの可用性に関するサービスレベル契約の詳細については、[Citrix Cloud Service Level Agreement](#)を参照してください。サービスの中断とスケジュールされたメンテナンスを監視するには、[Service Health Dashboard](#)を参照してください。

2025年6月

Citrix Cloud Japanの[Citrix Workspace](#)で、以下の機能が利用可能になりました。

- [Activity Manager](#)を含むモダンUIエクスペリエンス。
- カスタムアナウンスメント。
- カスタムドメイン。
- [Citrix Workspace](#)アプリへのログイン状態を維持。
- 外観のカスタマイズ。

2025年3月

Cloud Services向けConnector Appliance: Citrix Cloud Japanは、ハイパーバイザーでホストされるCitrixコンポーネントとして利用可能なConnector Applianceをサポートするようになりました。これにより、Citrix Cloudとリソースの場所との間の安全な通信が可能になります。複雑な

ネットワークやインフラストラクチャの構成が不要になるため、クラウド管理が簡素化されます。詳しくは、「[Connector Appliance](#)」を参照してください。

2024年11月

Citrix Cloudの日本リージョンでSession Recordingサービスが利用可能に: Citrix Cloud Japanは、Session Recordingサービスをサポートするようになりました。これにより、展開の合理化と高度な管理により、Citrix DaaSのセキュリティが強化されます。組織に自動化、トラブルシューティングの高速化、および統合された管理エクスペリエンスを提供します。詳しくは、「[Session Recordingサービス](#)」を参照してください。

2023年10月

App Protection: Citrix Cloud Japanは、Workspace App Protectionサービスをサポートするようになりました。詳しくは、「[App Protection](#)」を参照してください。

2022年8月

管理者管理インターフェイスの改善: Citrix Cloud Japanには、個々の管理者と管理者グループを追加するための改善されたインターフェイスが含まれるようになりました。詳しくは、以下の記事を参照してください。

- [個々の管理者を招待する](#)
- [ADからCitrix Cloud Japanに管理者を招待する](#)

2022年7月

管理者向けSAML認証のプレビュー: Citrix Cloud Japanは、ADの管理者グループにSAML認証を使用することをサポートするようになりました。詳しくは、「[SAMLをCitrix Cloud JapanのIDプロバイダーとして接続する](#)」を参照してください。

2022年4月

顧客ダッシュボードへのアクセスを有効または無効にする: Citrix Cloud Japanは、管理者向けに顧客ダッシュボードへの読み取り専用アクセスを有効にすることをサポートするようになりました。詳しくは、「[Citrix Cloud for Partners](#)」を参照してください。

Citrix DaaSのライセンスリリースを改善: Citrix Cloud Japanには、割り当てられたライセンスを一括でリリースするための改善されたワークフローが含まれるようになりました。詳しくは、「[Citrix DaaSのライセンスとアクティブな使用状況を監視する（ユーザー/デバイス）](#)」を参照してください。

2022年3月

システムログの一般提供: システムログが一般提供されるようになりました。システムログには、Citrix Cloud Japan で発生したイベントのタイムスタンプ付きリストが表示されます。過去 90 日間のイベントを表示し、規制コンプライアンス要件を満たすため、またはセキュリティ分析のためにイベントをエクスポートできます。詳細については、「[システムログ](#)」を参照してください。

2022年2月

IDプロバイダーとしてのSAMLのサポート: Citrix Cloud Japan は、Citrix Workspace のサブスクライバーを認証するために、任意の SAML プロバイダーを使用できるようになりました。詳細については、「[IDプロバイダーとしてSAMLをCitrix Cloud Japanに接続する](#)」を参照してください。

2021年12月

Citrix Gateway サービスの一般提供: Citrix Gateway は、Citrix Workspace の外部ユーザーに安全なリモートアクセスを提供します。詳細については、「[Citrix Cloud Japan 向け Citrix Gateway サービス](#)」を参照してください。

2021年11月

Microsoft Entra ID グループでの管理者追加: Citrix Cloud Japan は、Microsoft Entra ID グループを使用して Citrix Cloud Japan アカウントに管理者を追加できるようになりました。詳細については、「[管理者グループの管理](#)」を参照してください。

2021年10月

Workspace Environment Management サービスのサポート: Citrix Cloud Japan は、Workspace Environment Management サービスをサポートするようになりました。このサービスは、インテリジェントなリソース管理およびプロファイル管理テクノロジーを使用して、Citrix DaaS 展開に最高のパフォーマンス、デスクトップログオン、およびアプリケーション応答時間を提供します。このサポートには、Citrix Cloud Connector バージョン **6.29.0.58841** 以降が必要です。

2021年9月

Citrix Workspace および Citrix Gateway サービスのサポート: Citrix Cloud Japan は、以下のサービスをサポートするようになりました。

- Citrix Workspace を使用すると、組織内の個人の役割に関連する情報、アプリ、その他のコンテンツへの安全なアクセスを提供できます。ユーザーは、利用可能なサービスを購読し、あらゆる場所から、あらゆるデバイスでアクセスできます。

- Citrix Gateway サービスは、Citrix Workspace の外部ユーザーに安全なリモートアクセスを提供します。

詳細については、「[サービスの機能の可用性](#)」を参照してください。

2021年6月

システムログプレビュー: Citrix Cloud Japan には、Citrix Cloud Japan で発生したイベントのタイムスタンプ付きリストを表示するシステムログプレビュー機能が搭載されました。過去90日間のイベントを表示し、規制コンプライアンス要件を満たすため、またはセキュリティ分析のためにイベントをエクスポートできます。詳細については、[システムログ](#)を参照してください。

サポートされているサービスの機能の可用性

一般的に、サービスの可用性とは、対応するすべてのサービス機能が利用可能であることを意味します。ただし、Citrix Cloud Japanにサービスが組み込まれた場合、特定のサービス機能がすぐに利用できないことがあります。

この記事のセクションでは、Citrix Cloud Japanでサポートされているサービスについて説明します。これらのセクションでは、現在利用できないサービス機能もリストされています。この記事に含まれていない機能は、Citrix Cloud Japanで利用可能であり、Citrix Cloudと同様に機能します。利用可能な機能について詳しく知るために、この記事には各サービスのドキュメントへのリンクが含まれています。

シトリックス DaaS™

Citrix DaaS（旧Virtual Apps and Desktopsサービス）は、安全な仮想アプリとデスクトップを提供することを可能にし、インストール、セットアップ、アップグレードのほとんどをCitrixに任せることができます。あらゆるデバイスで最高のユーザーエクスペリエンスを提供しながら、アプリケーション、ポリシー、ユーザーを完全に制御できます。

Citrix DaaSは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は利用可能であり、Citrix Cloudと同様に機能します。

詳細については、[Citrix DaaS](#)のドキュメントを参照してください。

アプリ保護

App Protection機能は、Citrix Virtual Apps and Desktops™およびCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）を使用する際に強化されたセキュリティを提供するアドオン機能です。この機能は、クライアントがキーロギングや画面キャプチャマルウェアによって侵害される能力を制限します。App Protectionは、ユーザー資格情報や画面上の機密情報などの機密情報の漏洩を

防ぎます。この機能は、ユーザーや攻撃者がスクリーンショットを撮ったり、キーロガーを使用して機密情報を収集および悪用したりすることを防ぎます。App Protectionは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は利用可能であり、Citrix Cloudと同様に機能します。

詳細については、[App Protection](#)のドキュメントを参照してください。App Protectionのサポートされている機能の詳細については、[App Protection Compatibility Matrix](#)のドキュメントを参照してください。

ライセンス使用状況インサイト

License Usage Insightsサービスは、Citrix Service Providerが製品ライセンスと使用状況を理解し、報告するのに役立つ無料のクラウドサービスです。このサービスは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は利用可能であり、Citrix Cloudと同様に機能します。

詳細については、Citrix Cloudドキュメントの[Licensing for Citrix Service Providers](#)を参照してください。

セキュアブラウザ

Citrix Secure Browserサービスは、Webブラウジングを分離して、企業ネットワークをブラウザベースの攻撃から保護します。ユーザーデバイスの設定を必要とせずに、インターネットホスト型Webアプリケーションへの一貫した安全なリモートアクセスを提供します。

Secure Browserサービスは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は、Citrix Cloudと同様に利用でき、機能します。

詳細については、Citrix Cloudドキュメントの[Secure Browser service](#)を参照してください。

シトリックス ワークスペース™

[Citrix Workspace](#)は、[Citrix StoreFront](#)の展開の代替として、Citrixが管理するCitrix DaaSのアクセス層です。Citrix Workspaceは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は、Citrix Cloudと同様に利用でき、機能します。

Citrix Gatewayサービス

Citrix Gatewayサービスは、Citrix Workspaceの外部ユーザーに安全なリモートアクセスを提供します。

Citrix Gatewayサービスは、Citrix Cloud Japanのお客様に一般提供されています。以下のサービス機能は利用できません。

- セキュアプライベートアクセスを介したSaaSおよびエンタープライズWebアプリのサポート。

詳細については、[Citrix Gateway service for Citrix Cloud Japan](#)を参照してください。

ワークスペース環境管理™

Workspace Environment Managementは、インテリジェントなリソース管理およびプロファイル管理テクノロジーを使用し、Citrix DaaS展開に最高のパフォーマンス、デスクトップログオン、およびアプリケーション応答時間を提供します。

Workspace Environment Managementサービスは、Citrix Cloud Japanのお客様に一般提供されています。すべてのサービス機能は、Citrix Cloudと同様に利用でき、機能します。

詳細については、[Workspace Environment Management](#)サービスドキュメントを参照してください。

その他のサービス

以下のその他のサービスは、Citrix Cloud Japanでは利用できません。

- デバイスポスチャサービス(/ja-jp/device-posture.html)
- アダプティブ認証サービス(/ja-jp/adaptive-authentication.html)
- セキュアプライベートアクセス(/ja-jp/citrix-secure-private-access/service/citrix-secure-private-access-overview.html)
- グローバルアプリ構成サービス(/ja-jp/citrix-workspace/global-app-config-service.html)

Citrix Cloud Japan のセキュア展開ガイド

Citrix Cloud Japan のセキュア展開ガイドでは、Citrix Cloud Japan を使用する際のセキュリティベストプラクティスの概要と、Citrix が収集および管理する情報について説明します。

その他のサービスに関する技術セキュリティ概要

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

- [Citrix Gateway service 技術セキュリティ概要](#)

- Citrix DaaS 技術セキュリティ概要 (旧 Virtual Apps and Desktops service)
- Workspace Environment Management service の顧客データ管理

管理者向けガイダンス

- 強力なパスワードを使用し、定期的にパスワードを変更してください。
- 顧客アカウント内のすべての管理者は、他の管理者を追加および削除できます。信頼できる管理者のみが Citrix Cloud Japan にアクセスできるようにしてください。
- 顧客の管理者は、デフォルトですべてのサービスにフルアクセスできます。一部のサービスでは、管理者のアクセスを制限する機能が提供されています。詳細については、サービスごとのドキュメントを参照してください。
- 管理者向けの二要素認証は、Citrix Cloud Japan と Microsoft Entra ID の統合を使用して実現されます。

パスワードのコンプライアンス

次のいずれかの条件が存在する場合、Citrix Cloud Japan は管理者にパスワードの変更を促します。

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

新しいパスワードは、以下のすべての条件を満たす必要があります。

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

パスワード変更のルール:

- 現在のパスワードを新しいパスワードとして使用することはできません。
- 過去5つのパスワードは再利用できません。
- 新しいパスワードは、アカウントのユーザー名と類似してはなりません。
- 新しいパスワードは、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はなりません。Citrix Cloudは、新しいパスワードがこの条件に違反するかどうかを判断するために、<https://haveibeenpwned.com/>が提供するリストを使用します。

暗号化とキー管理

Citrix Cloud Japanのコントロールプレーンは、機密性の高い顧客情報を保存しません。代わりに、Citrix Cloud Japanは、管理者パスワードなどの情報をオンデマンドで（管理者に明示的に要求することで）取得します。機密性のある、または暗号化された保存データはないため、キーを管理する必要はありません。

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

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

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

データ主権

Citrix Cloud Japan のコントロールプレーンは日本でホストされています。お客様はこれを制御できません。

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

セキュリティ問題の洞察

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

Citrix クラウドコネクタ™

インストール

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

また、Citrix は、Cloud Connector ソフトウェアがインストールされているマシンが、お客様のプライベートネットワーク内にあり、DMZ にはないことを強く推奨します。ネットワークおよびシ

システム要件、ならびに Cloud Connector のインストール手順については、「[リソースの場所を作成する](#)」を参照してください。

構成

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

お客様は、Cloud Connector とともにアンチウイルスを使用できます。Citrix は McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8 でテストを行っています。Citrix は、他の業界標準の AV 製品を使用するお客様をサポートします。

お客様の Active Directory (AD) では、Cloud Connector のマシンアカウントは読み取り専用アクセスに制限されるべきです。これは Active Directory のデフォルト設定です。さらに、お客様は Cloud Connector のマシンアカウントで AD のログ記録と監査を有効にして、AD アクセスタクティビティを監視できます。

Cloud Connector をホストするマシンへのログオン

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

- Citrix Cloud と通信するためのサービスキー
- Citrix DaaS™ での電源管理のためのハイパーバイザーサービス資格情報

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

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

Cloud Connector マシンへの追加ソフトウェアのインストール

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

インバウンドおよびアウトバウンドポートの設定

Cloud Connector は、インターネットへのアクセスを伴うアウトバウンドポート 443 が開いている必要があります。Cloud Connector は、インターネットからアクセス可能なインバウンドポートを持つべきではありません。

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

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

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

クライアントポート	サーバーポート	サービス
49152 -65535/UDP	123/UDP	W32タイム
49152 -65535/TCP	135/TCP	アールピーシー エンドポイントマッパー
49152 -65535/TCP	464/TCP/UDP	Kerberos パスワード変更
49152 -65535/TCP	49152-65535/TCP	エルエスエー、エスエーエム、ネットログオン用アールピーシー (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
49152 -65535/TCP	3269/TCP	LDAP GC SSL
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	ケルベロス
49152 -65535/TCP/UDP	445/TCP	SMB

Citrix Cloud Japan内で使用される各サービスは、必要なオープンポートのリストを拡張します。詳細については、[Citrix Cloud Japanの接続要件](#)を参照してください。

送信通信の監視

Cloud Connectorは、Citrix Cloud JapanサーバーとMicrosoft Azure Service Busサーバーの両方に対して、ポート443でインターネットに送信通信を行います。

Cloud Connectorは、Cloud Connectorをホストするマシンが存在するActive Directoryフォレスト内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。

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

- 各サービスに関する[技術セキュリティ概要](#) (この記事の冒頭に記載)
- サポートされているクラウドサービス向けの[接続要件](#)

Cloud Connectorログの表示

管理者に関連する、または管理者にとって実行可能な情報はすべて、Cloud ConnectorマシンのWindowsイベントログで利用できます。

Cloud Connectorのインストールログは、次のディレクトリで表示します。

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

SSL/TLS構成

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

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

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

コネクタの更新

Citrixソフトウェアの更新が利用可能になると、Cloud Connectorはデフォルトで自己管理します。更新スケジュールを構成する方法の詳細については、[コネクタの更新](#)を参照してください。

Cloud Connector の再起動を無効にしたり、その他の制限を設けたりしないでください。これらの操作は、重要な更新がある場合にCloud Connectorが自身を更新するのを妨げます。

お客様は、セキュリティ問題に対応するために他のアクションを実行する必要はありません。Cloud Connectorは、Citrixソフトウェアのセキュリティ修正と更新を自動的に適用します。

侵害されたアカウントを処理するためのガイダンス

- Citrix Cloud Japanの管理者リストを監査し、信頼できない管理者を削除します。
- 会社のActive Directory内で侵害されたアカウントを無効にします。
- Citrixに連絡し、お客様のすべてのCloud Connectorに保存されている認証シークレットのローテーションを要求してください。侵害の重大度に応じて、次のアクションを実行してください。
 - **低リスク:** Citrix は時間をかけてシークレットをローテーションできます。Cloud Connector は引き続き正常に機能します。古い認証シークレットは2〜4週間で無効になります。この期間中、予期せぬ動作がないことを確認するためにCloud Connector を監視してください。
 - **継続的な高リスク:** Citrix はすべての古いシークレットを失効させることができます。既存のCloud Connector は機能しなくなります。正常な動作を再開するには、お客様はすべての該当するマシンでCloud Connector をアンインストールして再インストールする必要があります。

ヘルプとサポートの利用方法

アカウントへのサインイン

Citrix Cloud Japanアカウントへのサインインで問題が発生した場合は、次の点を確認してください。

- <https://citrix.citrixcloud.jp/> でサインインしていること、およびサインインページにCitrix Cloud Japanのロゴが表示されていることを確認してください。Citrix Cloud JapanのサインインURLは、`.com` トップレベルドメインではなく、`.jp` トップレベルドメインを使用します。
- アカウント登録時に指定したメールアドレスとパスワードでサインインしていることを確認してください。アカウント登録で受け入れられるメールアドレスの詳細については、「[Citrix Cloud Japanへのサインアップ](#)」を参照してください。
- 組織がCitrix Cloud Japan管理者向けのIDプロバイダーとしてMicrosoft Entra IDを使用している場合は、をクリックし、組織のサインインURLを入力します。その後、組織の資格情報を入力して、組織のCitrix Cloud Japanアカウントにアクセスできます。組織のサインインURLが不明な場合は、組織の管理者に問い合わせてください。

注:

アカウントのIDプロバイダーとしてMicrosoft Entra IDが有効になっている場合、組織の資格情報でサインインできます。IDプロバイダーとしてMicrosoft Entra IDを使用する方法の詳細については、「[IDプロバイダーとしてMicrosoft Entra IDを接続する](#)」を参照してください。

サービスの購入

サービス試用版を製品版サービスに変換したり、既存のサブスクリプションを更新または延長したりするには、<https://www.citrix.com/buy/> にアクセスしてください。

購入を完了するには、Citrix Cloud Japan管理コンソールで利用可能な組織IDが必要です。



60日間の試用期間終了までに購入しなかった場合、サービスは終了し、Citrix®はすべてのデータと設定を90日間アーカイブします。

サブスクリプション期間終了までに購入しなかった場合:

- サービス有効期限が切れてから30日後に、管理者とユーザーに対してサービスがブロックされます。

- サービスは、サービス有効期限が切れてから90日後に終了し、Citrixは残りのデータをすべて削除します。

90日以内に購入した場合、期限切れのサービスは本番サービスとして再アクティブ化されます。

サブスクリプションの更新または延長に関して追加の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。

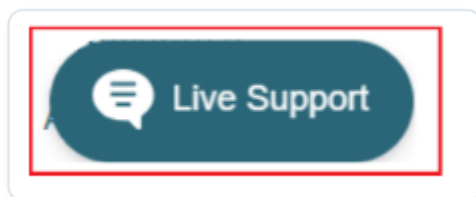
オンラインでカスタマーサービスケースを開く方法

注:

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

新しいケースを作成するには、次の手順に従います。

1. [Citrixサポートサイト](#)にアクセスします。
2. Citrixの資格情報を使用してサインインします。
3. CitrixアカウントでCitrixウェブサイトサインインできない場合は、記事[CTX228792: Citrixウェブサイトでのログインに関する問題のトラブルシューティング](#)を参照してください。
4. 仮想アシスタントフローを開始するには、[ライブサポート](#)をクリックします。



5. 適切なケースタイプを選択し、利用可能なオプションから[関連する問題](#)を選択します。



6. 既存のケースをフォローアップする場合は、**マイサポートケース**を選択し、プロンプトに従って続行します。ボットは、問題に関連する記事またはドキュメントを提示します。

「ヘルプサポートオプション」 (/en-us/citrix-cloud/media/help-support-options.png)

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

「ヘルプサポートを受ける」 (/en-us/citrix-cloud/media/help-get-support.png)

11. ケース作成を開始するには、**新規ケース**をクリックします。

「ヘルプサポートオプション」 (/en-us/citrix-cloud/media/help-support-options.png)

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

「ヘルプ優先言語を選択」 (/en-us/citrix-cloud/media/help-select-preferred-language.png)

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

ライブサポートを通じてオフラインケースを提出する

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

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

サポートフォーラム

Citrix Discussionsは、Citrix製品とサービスに関するヘルプを求めたり、知識を共有したりできるCitrix技術専門家のコミュニティです。Citrix Cloudコミュニティは、<https://community.citrix.com/forums/forum/1479-citrix-cloud/>でアクセスできます。

サポート記事とドキュメント

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

シトリックス ナレッジセンター

特定の技術的な問題については、[Citrix Knowledge Center](#)でヘルプを検索してください。作業中の製品を選択するか、問題の説明を入力するだけで検索できます。Knowledge Centerには、検索クエリに関連する記事、セキュリティ速報、および更新が表示されます。

シトリックス テックゾーン

([/ja-jp/tech-zone.html](#))には、Citrix製品とサービスについて詳しく学ぶのに役立つ豊富な情報が含まれています。ここでは、Citrixテクノロジーの設計、構築、展開に関する洞察を提供するリファレンスアーキテクチャ、図、ビデオ、技術文書を見つけることができます。

Citrix Cloud Japanへのサインアップ

この記事では、Citrix Cloud Japanへのサインアップと、アカウントを正常にオンボーディングするために必要なタスクの実行について説明します。

OrgIDとは?

OrgIDは、Citrix Cloud Japanアカウントに割り当てられる一意の識別子です。OrgIDは、通常、会社の事業所の住所である物理的なサイトの住所に関連付けられています。そのため、組織は通常、単一のOrgIDを持ちます。ただし、異なる支店がある場合や、異なる部門が資産を個別に管理している場合など、Citrixは組織が複数のOrgIDを持つことを許可する場合があります。

Citrix Cloud Japanアカウントとは?

Citrix Cloud Japanアカウントを使用すると、1つ以上のCitrix Cloudサービスを使用して、アプリとデータを安全に配信できます。Citrix Cloud JapanアカウントもOrgIDによって一意に識別されます。組織がOrgIDを設定した方法に基づいて、適切なCitrix Cloud Japanアカウントを使用することが重要です。これにより、購入と管理者アクセスを同じOrgIDで継続できます。

多要素認証の要件

アカウントを安全に保つため、Citrix Cloud Japanではすべてのお客様に多要素認証への登録を義務付けています。登録するには、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が必要です。

既存のCitrixのお客様の場合、Citrix Cloud Japanは、サインアップページにアクセスしてCitrix.comアカウントに関連付けられた資格情報を入力すると、登録を促します。Citrixを初めてご利用になる場合は、アカウント担当者に連絡してOrgIDを作成してください。

Citrix Cloudアカウントをオンボーディングする

- 既存のCitrixのお客様でCitrix Cloudアカウントをお持ちでない場合は、[My Organization](#)にアクセスし、[Citrix Cloud account management](#)の手順に従ってクラウドテナントをオンボーディングしてください。

- Citrix®を初めてご利用になる場合は、アカウント担当者に連絡してOrgIDを作成してください。

多要素認証に登録する

管理者アカウントを安全に保つため、Citrix Cloud Japanではサインイン時に多要素認証の使用を義務付けています。多要素認証に登録すると、管理者アカウントへの不正アクセスを防ぎ、Citrix SSOなど、[Time-Based One-Time Password](#)標準に準拠した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が必要です。

多要素認証に登録していない場合、Citrix Cloud Japanはサインイン時に登録を促します。

登録中に、Citrix Cloud Japan は QR コードとキーを表示します。認証アプリに応じて、QR コードをスキャンするか、キーを入力してデバイスを登録できます。スムーズな登録プロセスのため、Citrixはこのアプリを事前にデバイスにダウンロードしてインストールすることをお勧めします。Citrix Cloud Japan は、デバイスを紛失したり、認証アプリを使用できない場合にアカウントにアクセスするために使用できる、1回限りのバックアップコードも生成します。

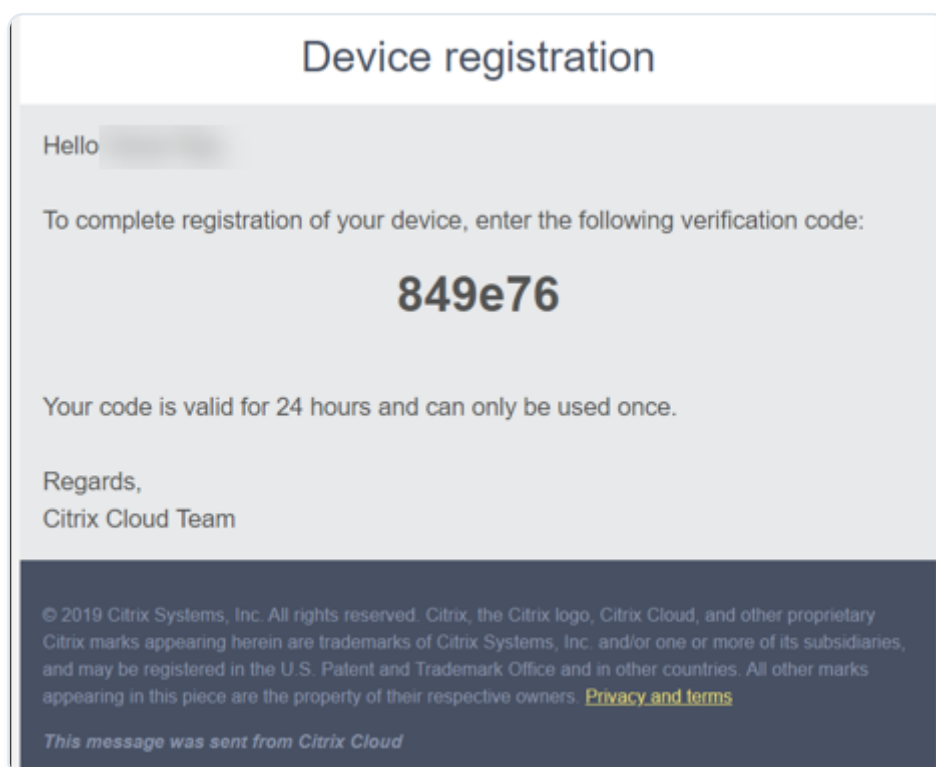
注：

- Citrix ID プロバイダーの管理者のみが、Citrix Cloud Japan を介して多要素認証に登録できます。Microsoft Entra ID を使用して Citrix Cloud Japan の管理者を管理している場合は、Azure ポータルを使用して多要素認証を構成できます。詳細については、Microsoft Web サイトの[Azure Multi-Factor Authentication 設定の構成](#)を参照してください。
- 登録後、Citrix Cloud Japan で所属するすべての顧客組織で多要素認証が使用されます。登録プロセスが完了すると、多要素認証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台のみです。後で別のデバイスを登録すると、Citrix Cloud Japan は現在のデバイス登録を削除し、新しいデバイスに置き換えます。詳細については、[ブライマリ MFA メソッドの管理](#)を参照してください。

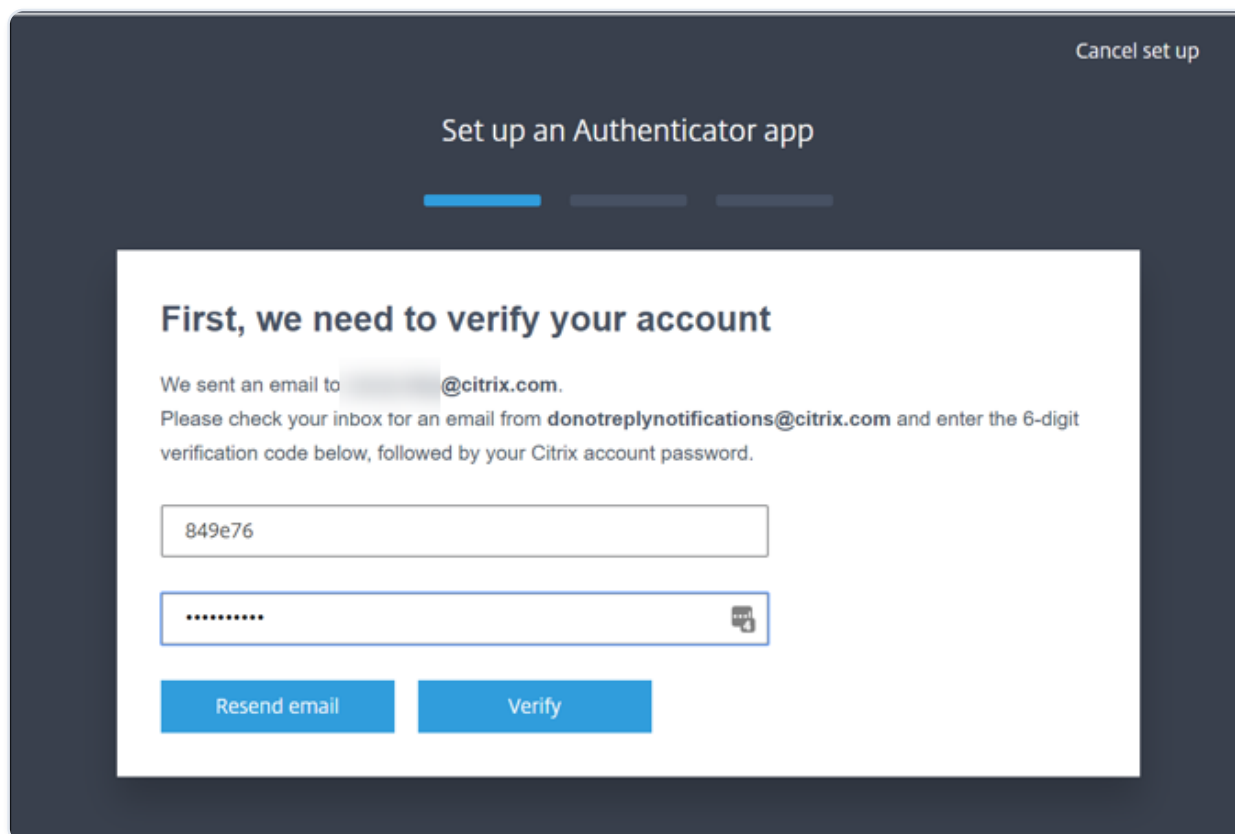
デバイスを多要素認証に登録するには

1. <https://citrix.citrixcloud.jp/>にアクセスし、Citrix Cloud Japan の資格情報を入力します。

2. 多要素認証への登録を求められたら、**今すぐ登録**を選択します。Citrix Cloud Japan から確認コードが記載されたメールが送信されます。



3. メールを受信したら、6桁の確認コードと Citrix Cloud Japan のパスワードを入力し、**確認**を選択します。



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

Set up an authenticator app

Download an authenticator app

1. Go to your phone's app store.
2. Search for "authenticator App."
3. Download one of your choosing

Scan the QR code

From your authenticator app, scan the QR below. If you can not scan the QR code, use the key to enter manually.

QR code:

Key:

Verify your authenticator app

Your authenticator app will generate a 6-digit code. Please copy the code below.

Enter 6-digit verification code

Verify code

5. **認証アプリを確認**の下で、認証アプリのコードを入力し、**コードを確認**を選択します。
6. デバイスを紛失したり、認証アプリを使用できない場合に備えて、次のアカウント回復方法を構成します。
- リカバリ電話 (必須): **リカバリ電話を追加**を選択し、Citrix サポート担当者がお客様に電話して本人確認を行うために使用できる電話番号を入力します。Citrix サポートは、サインインのヘルプを要求した場合にのみこの電話番号を使用します。Citrix は固定電話番号の使用をお勧めします。
 - バックアップコード (必須): **バックアップコードを生成**を選択して、認証アプリを使用できない場合にサインインに役立つ1回限りのバックアップコードのセットを作成します。プロンプトが表示されたら、**コードをダウンロード**を選択して、バックアップ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、**これらのコードを保存しました**を選択し、

閉じるを選択します。

Download your backup codes

Store these backup codes in a safe but accessible place. You'll need these codes handy if you can't sign in normally.

Backup codes:

adf1 026c	d812 57be	d2dd c9ee
8206 7b4d	7430 6698	da5e 734d
ab8d e45f	7398 668a	f6ee 9bdd
cbb3 68ae		

i You can use each backup code only once.

If you lose these backup codes, you'll need to replace them with new ones from your account's profile page.

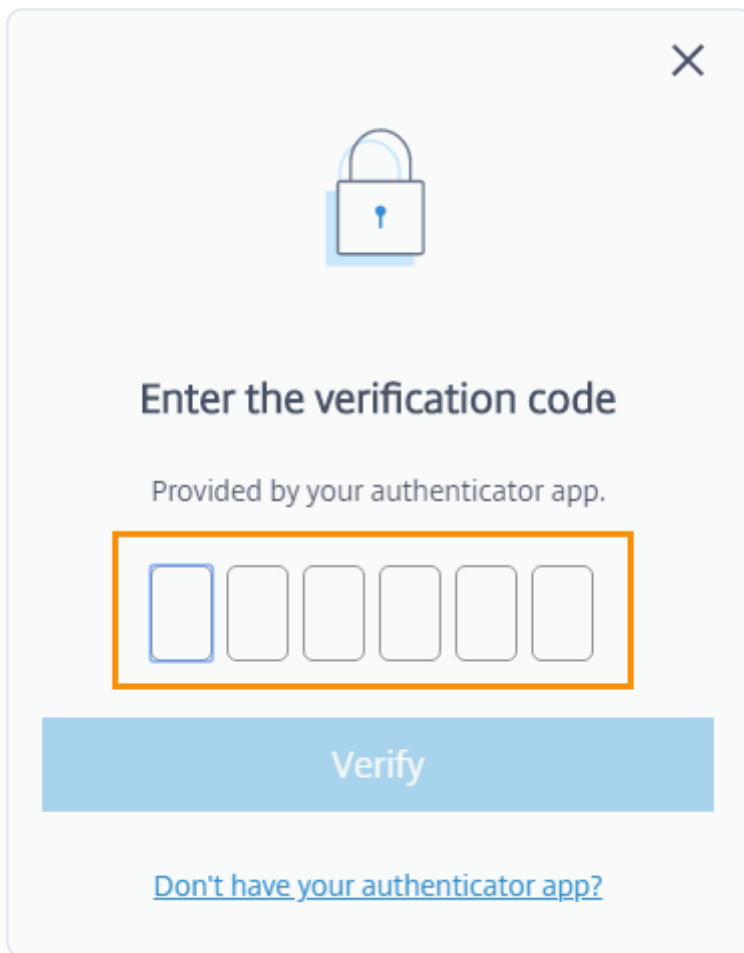
Backup codes generated by Citrix on Apr 28, 2020

☐ I've saved these codes.

CloseDownload codes

7. 完了を選択して登録を完了します。

次回、Citrix Cloud Japanの管理者資格情報でサインインすると、Citrix Cloud Japanは認証アプリからの確認コードを要求します。

A screenshot of a verification code entry screen. At the top right is a close button (X). Below it is a padlock icon. The text "Enter the verification code" is centered. Below that, it says "Provided by your authenticator app." There is a row of six input boxes for the code, with the first box highlighted by a blue border and the entire row enclosed in an orange border. Below the input boxes is a blue "Verify" button. At the bottom, there is a link: "Don't have your authenticator app?".

Enter the verification code

Provided by your authenticator app.

Verify

[Don't have your authenticator app?](#)

デバイス登録を管理する

別のデバイスを登録したり、追加のバックアップコードを生成したり、後で復旧用電話番号を更新したりする必要がある場合は、ページからこれらのタスクを実行できます。手順については、以下の記事を参照してください。

- [プライマリMFA方法を管理する](#)
- [MFA復旧方法を管理する](#)

Citrix Cloud Japanを購入する

組織向けにCitrix Cloud Japanを購入するには、Citrixの営業担当者にお問い合わせください。注文が完了すると、アカウント設定用のリンクが記載された確認メールが届きます。アカウント設定では、注文時に使用したメールアドレスと指定したパスワードを使用して、最初のアカウント管理者が作成されます。

注文を確認する

注文確認メールのリンクをクリックします。Citrix Cloud Japanのセットアップページがブラウザウィンドウに表示され、注文の詳細が表示されます。をクリックします。

パスワードを作成する

Citrix Cloud Japanアカウントで使用する強力なパスワードを入力して確認し、をクリックします。アカウントの最初の管理者として、このパスワードと注文時のメールアドレスを使用してCitrix Cloud Japanにサインインします。

Citrix Cloud Japanの資格情報でサインインする

1. 注文時に使用したメールアドレスと以前に選択したパスワードを使用して、<https://citrix.citrixcloud.jp>でCitrix Cloud Japanにサインインします。Citrix Cloud Japanにホームリージョンが表示されます。現在、Citrix Cloud Japanには1つの地理的リージョンしか含まれていないため、このリージョンのみが表示されます。
2. サービス規約に同意し、をクリックします。Citrix Cloud Japan管理コンソールが表示されます。

Citrix Cloud Japan 向けサービス試用版

個々のクラウドサービスの試用版は、Citrix Cloud Japan プラットフォームを通じて提供されます。サービス試用版の機能は、購入したサービスと同じであるため、概念実証 (POC)、パイロット、または同様の用途に適しています。

エクスペリエンスをカスタマイズし、ユーザーにとって最も重要なサービスを提供するために、試用版アクセスはサービスごとに管理されます。

サービスの購入準備が整ったら、試用版を本番アカウントに変換するため、何も再構成したり、別の本番アカウントを作成したりする必要はありません。

サービス試用版に関する概要

	CITRIX CLOUD JAPAN 試用版
許可されるサブスクリイバー数	25
最大期間	60暦日。サービスの試用版は1回のみリクエストできます。
提供状況	制限付き提供
リソースのロケーション	お客様が提供および構成
ユーザーセッション期間	無制限

	CITRIX CLOUD JAPAN 試用版
ローカルのMicrosoft Active Directory統合	はい
リソースロケーションの選択	はい
オンプレミスへの展開	はい
シトリックス DaaS™	全機能セット
カスタマイズ可能	はい

サービス試用版をリクエストする

サービス試用版をリクエストするには、Citrix®の営業担当者にご連絡いただき、組織ID (OrgID) を提供する必要があります。営業担当者が、サービスの利用を開始するために必要なすべての情報を提供します。

試用版をリクエストし、OrgIDを確認するには、次の手順を使用します。

1. Citrix Cloud Japanアカウントにサインインします。
2. 「利用可能なサービス」の下で、試用したいサービスを見つけて、「トライアルをリクエスト」をクリックします。
3. 表示される通知に表示されているOrgIDをメモしてください。
4. トライアルリクエストを登録するには、「営業担当者に相談」をクリックします。

トライアルが承認され、使用可能になると、メール通知が届きます。トライアルを完了するまで60日間あります。

注:

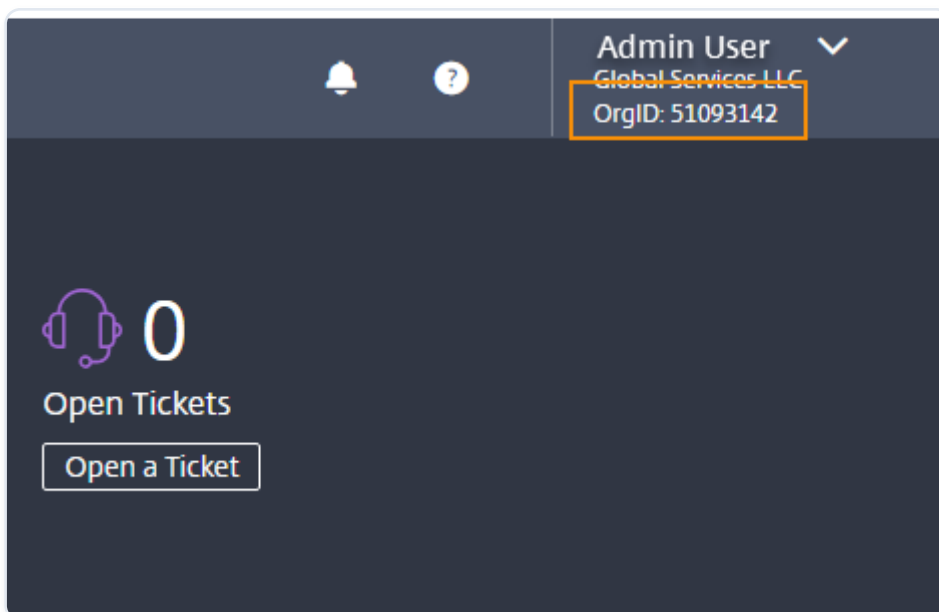
最高の顧客体験を保証するため、Citrixはいつでもトライアルの参加者数を制限する権利を留保します。

サービスの購入

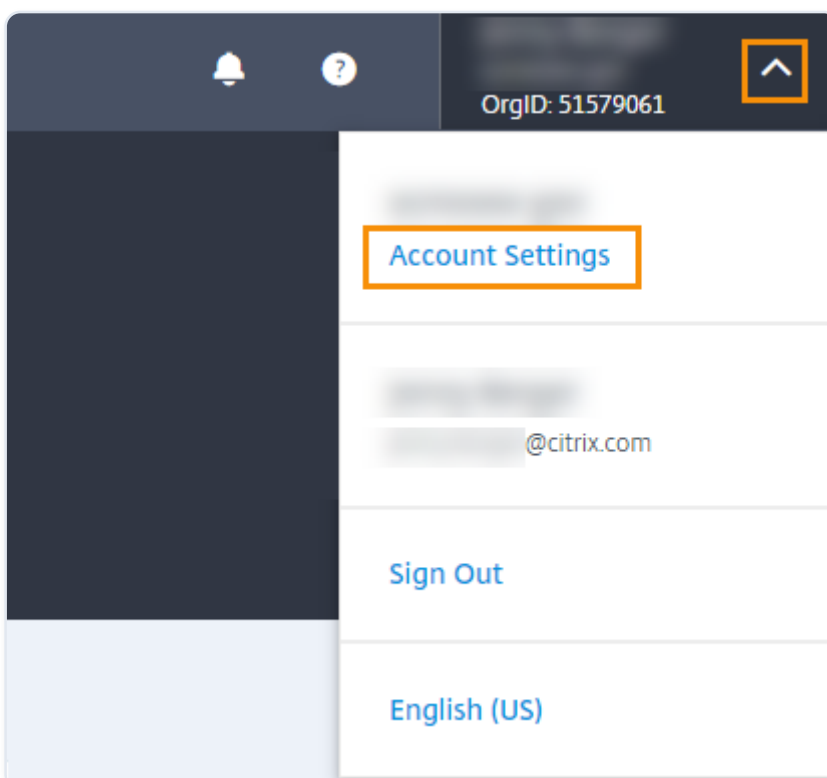
トライアルを本番サービスに移行する準備ができれば、<https://www.citrix.com/buy/>にアクセスしてください。

購入を完了するには、Citrix Cloud Japan管理コンソールで利用可能なOrgIDが必要です。OrgIDは以下の場所に表示されます。

- 管理コンソールの右上隅に、アカウント名の下にOrgIDが表示されます。



- 右上メニューから、「アカウント設定」をクリックします。



OrgIDは「Organization ID」フィールドに表示されます。

[←](#)

Account Settings

[Company Account](#) [My Profile](#) [Orders](#)

Account Name

Edit

Address

Organization ID

51579061

Region

重要:

60日間のトライアル期間終了までに購入しなかった場合、サービスは終了し、Citrixはすべてのデータと設定を90日間アーカイブします。90日以内に購入した場合、トライアルは再アクティブ化され、本番サービスに変換されます。

システム要件

ここで説明されていないコンポーネント（Workspaceアプリなど）のシステム要件については、それぞれのドキュメントで説明されています。

Windowsサーバーにインストールできる製品コンポーネントおよび機能については、特に記載がない限り、Server Coreインストールはサポートされていません。

デスクトップおよびアプリケーションを提供するVMのサイジングに関する具体的な推奨事項は、ハードウェア製品の複雑で動的な性質のため、提供できません。すべての展開には固有のニーズがあります。一般的に、VMのサイジングはユーザーのワークロードではなくハードウェアに基づいて行われます（RAMを除く。より多くのRAMを消費するアプリケーションには、より多くのRAMが必要です）。VMのサイジングに関するガイダンスについては、([/ja-jp/tech-zone.html](#)) Citrix Tech ZoneのWebサイトにある以下のリソースを参照してください。

- 設計上の決定事項: Azure上でのCitrix DaaS提供におけるスケーラビリティと経済性
- Google Cloud Compute EngineでのVDAインスタンスのサイジング
- リファレンスアーキテクチャ: Citrix DaaS - AWS
- 技術概要: Citrix Desktops-as-a-Service (DaaS) 向けローカルホストキャッシュ / 高可用性モード

最小システム要件

Citrix Cloud Japanには、以下のコンポーネントが必要です。

- Active Directoryドメイン
- ドメインに参加している2台の物理または仮想マシンで、Citrix Cloud Connectorソフトウェアがインストールされていること。詳細については、([/ja-jp/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/technical-details.html](#)) Citrix Cloud Connectorの技術詳細を参照してください。
- ワークロードや、ユーザーに提供したいサービスに必要なその他のコンポーネントをホストするために、ドメインに参加している物理または仮想マシン。

サポートされているWebブラウザ

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

トランスポート層セキュリティの要件

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

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

追加要件

- サービス接続: [接続要件](#)
- シトリックス クラウド コネクタ: [シトリックス クラウド コネクタ の要件](#)
- Citrix DaaS (旧 Virtual Apps and Desktops サービス): [システム要件](#)
- Workspace アプリ: 要件はプラットフォームによって異なります。詳細については、[Workspace アプリのドキュメント](#)を参照してください。

サービス接続要件

Citrix Cloud Japanは、お客様の展開環境内のリソースに接続する管理機能（Webブラウザ経由）と運用リクエスト（他のインストール済みコンポーネントから）を提供します。このドキュメントでは、お客様のリソースとCitrix Cloud Japan間の接続を確立するための要件と考慮事項を定義します。

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

管理コンソール

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

プロキシとファイアウォールの構成

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

管理コンソールを動作させるには、ポート443をアウトバウンド接続用を開く必要があります。コンソール内を移動することで、一般的な接続をテストできます。

詳細については、「[Citrix 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。

コンソール通知

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

管理コンソール内でPendoコンテンツを表示できるようにするため、Citrixは次のアドレスに接続できることを推奨します。

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

注：

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

Pendoコンテンツを表示するサービスには、以下が含まれます。

- Citrix DaaS™（旧バーチャルアプリおよびデスクトップサービス）
- シトリックスワークスペース™

Pendoは、CitrixがCitrixのお客様にクラウドおよびサポートサービスを提供するために使用するサードパーティのサブプロセッサです。これらのサブプロセッサの完全なリストについては、

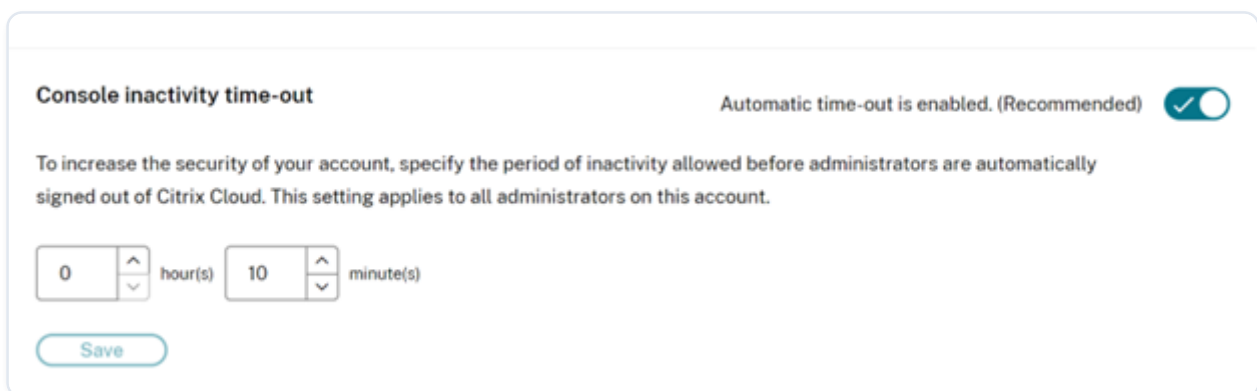
「Citrix Cloud & Support ServicesおよびCitrix関連会社向けのサブプロセッサ」を参照してください。

セッションタイムアウト

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

コンソールの非アクティブタイムアウトの構成

フルアクセス管理者として、管理者が自動的にサインアウトされるまでのCitrix Cloudコンソールでの非アクティブ期間を設定できます。一度設定すると、指定されたタイムアウト期間はCitrix Cloudアカウントのすべての管理者に適用されます。



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

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

注：

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

シトリックス クラウド コネクタ™

Citrix Cloud Connectorは、Microsoft Windowsサーバー上で動作する一連のサービスを展開するソフトウェアパッケージです。Cloud Connectorをホストするマシンは、Citrix Cloud Japanで使用す

るリソースが存在するネットワーク内に配置されます。Cloud ConnectorはCitrix Cloud Japanに接続し、必要に応じてリソースを操作および管理できるようにします。

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

一般的なサービス接続要件

次の表に、ほとんどのCitrix Cloud Japanサービスに共通するアドレスとその機能を示します。これらのアドレスは、Citrix Cloud Japanサービスが動的であり、IPアドレスが定期的に変更されるため、ドメイン名としてのみ提供されます。

必須アドレス	機能
<code>https://*.citrixworkspacesapi.jp</code>	サービスが使用するCitrix Cloud APIへのアクセスを提供します。
<code>https://*.citrixcloud.jp</code>	Citrix Cloud Japanの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。
<code>https://*.blob.core.windows.net</code>	Citrix Cloud Connectorの更新を保存するAzure Blob Storageへのアクセスを提供します。
<code>https://*.servicebus.windows.net</code>	ログ記録とActive Directoryエージェントに使用されるAzure Service Busへのアクセスを提供します。

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および管理してください。また、お客様とエンドユーザーが使用しているサービスに適用されるアドレスのみを構成してください。

証明書の検証

Cloud Connectorのバイナリと、Cloud Connectorが接続するエンドポイントは、ソフトウェアのインストール時に検証されるX.509証明書によって保護されています。これらの証明書を検証するには、各Cloud Connectorマシンが次の要件を満たしている必要があります。

- HTTPポート80が*.digicert.comに対して開いていること。このポートは、Cloud Connectorのインストール時および定期的な証明書失効リストの確認時に使用されます。
- 次のアドレスに接続する必要があります。

- `http://*.digicert.com`
- `https://*.digicert.com`
- `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
- `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`

これらの証明書の詳細については、「[証明書を検証要件](#)」を参照してください。

SSL復号化

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

シトリックス ゲートウェイ

- [共通サービス接続要件](#)
- `https://*.*.nssvc.jp`

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

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

シトリックス DaaS

注:

Citrix DaaSは、以前はVirtual Apps and Desktopsサービスでした。

Citrixリソースロケーション / Cloud Connector:

- [共通サービス接続要件](#)
- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixcloud.jp`
- `https://*.blob.core.windows.net`
- `https://*.citrixworkspacesapi.net`
- `https://*.servicebus.windows.net`

- 新機能、重要な連絡事項、顧客アンケートなどの製品内メッセージの場合:

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

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

管理コンソール:

- https://*.citrixworkspacesapi.jp
- https://*.citrixcloud.jp
- https://*.blob.core.windows.net
- https://*.apps.citrixworkspacesapi.net

Citrix DaaS リモート PowerShell SDK

Citrix DaaS Remote PowerShell SDK を使用するには、次の URL をホワイトリストに登録します:

- https://*.citrixcloud.jp
- [https://*.citrixworkspacesapi.net/\[customerid\]](https://*.citrixworkspacesapi.net/[customerid])
- [https://\[customerid\].xendesktop.net:443](https://[customerid].xendesktop.net:443)

シトリックス ワークスペース

- https://*.citrixcloud.jp
- https://*.citrixdata.com
- 新機能、重要な連絡事項、顧客アンケートなどの製品内メッセージの場合:
 - <https://citrix-cloud-content.customer.pendo.io/>
 - <https://citrix-cloud-data.customer.pendo.io/>

ワークスペース環境管理™ サービス

- https://*.wem.citrixcloud.jp

認証

- accounts.citrixcloud.jp
- accounts-dsauthweb.citrixcloud.jp

IDプロバイダーのURLがエンドユーザーデバイスからもアクセス可能であることを確認してください。

認証グラフィカルインターフェイスアセット

- `accounts-webassets.citrixcloud.jp`

Citrix Cloud™ コネクタの要件

Citrix Cloud Connectorは、Windows Server 2016、2019、または2022にインストールされるWindowsサービスで構成されています。

システム要件

Cloud Connectorをホストするマシンは、以下の要件を満たす必要があります。Citrix®は、高可用性を確保するために、各リソースロケーションに少なくとも2つのCloud Connectorをインストールすることを強く推奨します。

Citrix DaaS向けCloud Connectorマシンの構成に関するベストプラクティスについては、「[Cloud Connectorのスケーリングとサイジングに関する考慮事項](#)」を参照してください。

オペレーティングシステム

以下のオペレーティングシステムがサポートされています。

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

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

.NETの要件

Microsoft .NET Framework 4.7.2以降が必要です。

サーバー要件

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

- Cloud Connectorをホストするために専用のマシンを使用してください。これら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。

- マシンはActive Directoryドメインコントローラーとして構成されていません。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。
- サーバーの時計は正しいUTC時刻に設定されています。
- Internet Explorer拡張セキュリティ構成 (IE ESC) はオフになっています。Internet Explorer拡張セキュリティ構成がオンになっている場合、Cloud ConnectorはCitrix Cloud Japanとの接続を確立できない可能性があります。

Windows Updateのガイダンス

Citrixは、Citrix Cloud ConnectorをホストするすべてのマシンでWindows Updateを有効にすることを強く推奨します。Citrix Cloud Connectorは、Windows Updateを含む様々な要因によってトリガーされる可能性のある保留中の再起動を5分ごとに定期的にチェックします。検出された再起動は、リソースの場所で設定された優先日スケジュールに関係なく、速やかに実行されます。このプロアクティブなアプローチにより、Citrix Cloud Connectorが長期間にわたって保留中の更新状態に置かれることがなく、システムの安定性が維持されます。

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

注:

- 顧客が営業時間中にCitrix Cloud Connectorを再起動する意図がない場合、顧客は営業時間外にWindows Updateを適切にスケジュールすることをお勧めします。
- 各Citrix Cloud Connectorの再起動には約10分かかります。これには、一度に1つのCitrix Cloud Connectorのみが再起動することを保証するためにCitrix Cloudプラットフォームと同期するのに必要な時間が含まれます。したがって、前述の自動再起動の推奨される最低4時間の遅延は、テナント内のCitrix Cloud Connectorの数に応じて、より短いまたはより長い期間に調整できます。

証明書検証の要件

Cloud ConnectorのバイナリとCloud Connectorが接続するエンドポイントは、広く信頼されているエンタープライズ認証局 (CA) によって発行されたX.509証明書によって保護されています。公開鍵インフラストラクチャ (PKI) における証明書検証には、証明書失効リスト (CRL) が含まれます。クライアントが証明書を受信すると、CAの信頼性を検証し、その証明書が証明書失効リスト (CRL) に記載されているかどうかを確認します。証明書がCRLに記載されている場合、その証明書は失効しており、有効に見えても信頼すべきではありません。

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

X.509証明書はCloud Connectorのインストール中に検証されます。したがって、Cloud Connectorソフトウェアのインストールを成功させるには、すべてのCloud Connectorマシンがこれらの証明書を信頼する必要があります。

Citrix Cloud Japan のエンドポイントは、DigiCert または Azure が採用しているルート証明機関のいずれかによって発行された証明書によって保護されています。Azure で使用されているルートCAの詳細については、<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 は、次のアドレスに対して開かれています。このポートは、Cloud Connector のインストール時および定期的な CRL チェック時に使用されます。CRL および OCSP 接続をテストする方法の詳細については、DigiCert Web サイトの <https://www.digicert.com/kb/utility-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>
- 次のアドレスとの通信が有効になっています。
 - https://*.digicert.com
- 以下のルート証明書がインストールされています。
 - <https://cacerts.digicert.com/DigiCertGlobalRootG3.crt>
 - <https://cacerts.digicert.com/DigiCertGlobalRootG2.crt>
 - <https://cacerts.digicert.com/DigiCertGlobalRootCA.crt>
 - <https://cacerts.digicert.com/DigiCertTrustedRootG4.crt>
 - <https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt>
 - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
 - <https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt>
 - <https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt>
 - <https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt>
- 以下の中間証明書がインストールされています。
 - <https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt>

いずれかの証明書が見つからない場合、Cloud Connectorインストーラーは <http://cacerts.digicert.com> からダウンロードします。

証明書のダウンロードとインストールの詳細な手順については、[CTX223828](#)を参照してください。

Active Directoryの要件

- ユーザー向けにサービスを作成するために使用するリソースとユーザーを含むActive Directory ドメインに参加していること。
- Citrix Cloud Japan で使用する予定の各 Active Directory フォレストは、常に2つの Cloud Connector から到達可能である必要があります。

- Cloud Connector は、親ドメインコントローラーと子ドメインコントローラーの両方に到達できる必要があります。これは、Cloud Connector がインストールされている Active Directory ワークフローを完了するために不可欠です。

詳細については、以下のMicrosoftサポート記事を参照してください。

- [ドメインと信頼関係を構成する方法](#)
- [システムサービスポート](#)

ネットワーク要件

- リソースの場所で使用するリソースに接続できるネットワークに接続されていること。詳細については、「[Cloud Connector のプロキシとファイアウォールの構成](#)」を参照してください。
- インターネットに接続されていること。詳細については、「[インターネット接続要件](#)」を参照してください。

サポートされているActive Directoryの機能レベル

Citrix Cloud Connector は、Active Directory の以下のフォレストおよびドメインの機能レベルをサポートしています。

フォレストの機能レベル	ドメインの機能レベル	サポートされているドメインコントローラー
ウィンドウズ サーバー 2008 R2	ウィンドウズ サーバー 2008 R2	ウィンドウズ サーバー 2008 R2、ウィンドウズ サーバー 2012、ウィンドウズ サーバー 2012 R2、ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2008 R2	Windows Server 2012 がサポートされています	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 がサポートされています
ウィンドウズ サーバー 2008 R2	ウィンドウズ サーバー 2012 R2	ウィンドウズ サーバー 2012 R2、ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2008 R2	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016

フォレストの機能レベル	ドメインの機能レベル	サポートされているドメインコントローラー
ウィンドウズ サーバー 2012	ウィンドウズ サーバー 2012	ウィンドウズ サーバー 2012、ウィンドウズ サーバー 2012 R2、ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2012	ウィンドウズ サーバー 2012 R2	ウィンドウズ サーバー 2012 R2、ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2012	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2012 R2	ウィンドウズ サーバー 2012 R2	ウィンドウズ サーバー 2012 R2、ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2012 R2	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016
ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016、ウィンドウズ サーバー 2019、ウィンドウズ サーバー 2022

連邦情報処理標準 (FIPS) のサポート

Cloud Connector は現在、FIPS 対応マシンで使用される FIPS 検証済み暗号化アルゴリズムをサポートしています。Citrix Cloud Japan で利用可能な Cloud Connector ソフトウェアの最新バージョンのみがこのサポートを含んでいます。環境内に既存の Cloud Connector マシンがあり (2018 年 11 月より前にインストールされたもの)、これらのマシンで FIPS モードを有効にしたい場合は、次の操作を実行してください。

1. リソースの場所にある各マシンから 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. 各 FIPS 対応マシンに Cloud Connector の最新バージョン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ようとしないでください。常に古いCloud Connectorを最初にアンインストールし、その後で新しいものをインストールしてください。
- 古いCloud Connectorバージョンをホストしているマシンで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 JapanがCloud Connectorの定期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、[タスク3：Cloud Connectorのインストール](#)を参照してください。

Cloud Connectorで許可されるFQDN

Cloud Connectorがアクセスする完全修飾ドメイン名（FQDN）の完全なリストについては、

`<https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-japan/allowlist.json>` のJSONファイルを参照してください。このリストは製品ごとに整理されており、各FQDNグループには変更ログが付属しています。

これらのFQDNの一部は顧客固有のものであり、山括弧で囲まれたテンプレートセクションが含まれています。これらのテンプレートセクションは、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、**Identity and Access Management**のAPI **Access**タブの上部で確認できます。

インストール要件

- Cloud ConnectorソフトウェアはCitrix Cloud Japanからのみダウンロードし、準備されたマシンにインストールしてください。デフォルトでは、Cloud Connectorインストーラーはダウンロード元のコントロールプレーンに接続しようとします。そのため、Citrix Cloud (citrix.cloud.com) アカウントからダウンロードしたソフトウェアをインストールしようとすると、インストーラーはCitrix Cloud Japanに接続しません。
- Cloud Connectorソフトウェアはダウンロードされるため、ブラウザで実行可能ファイルのダウンロードを許可する必要があります。

クローンされたマシンに関する考慮事項

Citrix Cloud Japanがリソースロケーション内のマシンと通信できるように、Cloud Connectorをホストする各マシンは一意的なSIDとコネクタIDを持っている必要があります。Cloud Connectorをマシンテンプレートにインストールすること（クローン作成前）はサポートされていません。Cloud Connectorがインストールされたマシンをクローンすると、Cloud Connectorサービスが実行されなくなり、マシンがCitrix Cloud Japanに接続できなくなります。

リソースロケーション内の複数のマシンでCloud Connectorをホストし、クローンされたマシンを使用する場合は、次の手順を実行してください。

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

重要な使用上の考慮事項

- Citrix Cloud Japanへの常時接続を確保するため、すべてのCloud Connectorの電源は常にオンにしておいてください。
- 以前にインストールしたCloud Connectorを新しいバージョンにアップグレードしないでください。代わりに、古いCloud Connectorをアンインストールしてから、新しいCloud Connectorをインストールしてください。
- Citrixは、Cloud ConnectorをホストするすべてのマシンでWindows Updateを有効にすることを強く推奨します。
- Citrixは、各リソースの場所に少なくとも2つのCloud Connectorをインストールすることを強く推奨します。一般的に、インストールすべきCloud Connectorの数はN+1です。ここでNは、リソースの場所内のインフラストラクチャをサポートし、単一のCloud Connectorが利用できなくなった場合でもCitrix Cloud Japanとリソースの場所間の接続が維持されるようにするために必要な容量です。
- Citrix Cloud Japanで使用する予定の各Active Directoryフォレストは、常に2つのCloud Connectorから到達可能である必要があります。
- インストール後、Cloud Connectorをホストするマシンを別のドメインに移動しないでください。マシンを別のドメインに参加させる必要がある場合は、Cloud Connectorをアンインストールし、ドメイン参加後に再インストールしてください。

Cloud Connectorのインストール済みサービス

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

インストール中、Citrix Cloud Connector実行可能ファイルは、機能するために必要なサービス構成をデフォルト設定でインストールおよび設定します。デフォルト構成が手動で変更された場合、Cloud Connectorは期待どおりに動作しない可能性があります。この場合、更新プロセスを処理するサービスが引き続き機能すると仮定すると、次のCloud Connector更新時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昇格された呼び出しを促進し、ネットワーク上で直接通信することはありません。Cloud Connector上のサービスがローカルシステム権限を必要とするアクションを実行する必要がある場合、Citrix Cloud Agent Systemが実行できる事前定義された一連の操作を介してそれを行います。

サービス名	説明	実行ユーザー
Citrix Cloud エージェントシステム	オンプレミスエージェントに必要なシステムコールを処理します。インストール、再起動、レジストリアクセスが含まれます。Citrix Cloud Services Agent WatchDog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 エージェント ウォッチドッグ	オンプレミスエージェントを監視し、アップグレードします (常時最新)。	ネットワークサービス
Citrix Cloud Services エージェント ロガー	Citrix Cloud Connectorサービス用のサポートロギン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 プロバイダー	Citrix Cloud Japanが、インストールされているActive Directoryドメインアカウントに関連付けられたリソースの管理を容易にできるようにします。	ネットワークサービス

サービス名	説明	実行ユーザー
Citrix Cloud Services エージェント ディスカバリ	Citrix Cloud Japanが、XenAppおよびXenDesktop®のレガシーなオンプレミスCitrix製品の管理を容易にします。	ネットワークサービス
Citrix Cloud Services クレデンシャルプロバイダー	暗号化されたデータの保存と取得を処理します。	ネットワークサービス
Citrix Cloud Services WebRelay プロバイダー	WebRelay Cloudサービスから受信したHTTPリクエストをオンプレミスWebサーバーに転送できるようにします。	ネットワークサービス
Citrix CDF キャプチャサービス	設定されているすべての製品とコンポーネントからCDFトレースをキャプチャします。	ネットワークサービス
Citrix 構成同期サービス	高可用性モードのためにブローカリング構成をローカルにコピーします。	ネットワークサービス
Citrix 高可用性サービス	中央サイトの停止中にサービスの継続性を提供します。	ネットワークサービス
Citrix ITSM アダプタープロバイダー	仮想アプリとデスクトップのプロビジョニングと管理を自動化します。	ネットワークサービス
シトリックス NetScaler® クラウドゲートウェイ	インバウンドファイアウォールルールを開いたり、DMZにコンポーネントを展開したりすることなく、オンプレミスのデスクトップと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
Citrix Remote Broker プロバイダー	ローカルのVDAおよびStoreFront™サーバーからリモートのBrokerサービスへの通信を可能にします。	ネットワークサービス

サービス名	説明	実行ユーザー
シトリックス リモート HCL サーバー	Delivery Controller™と1つ以上のハイパーバイザー間の通信をプロキシします。	ネットワークサービス
Citrix Session Manager プロキシ	匿名で事前起動されたセッションを管理し、セッション数情報をクラウドベースの Session Manager サービスにアップロードします。	ネットワークサービス
Citrix WEM Cloud 認証サービス	Citrix WEM エージェントがクラウドインフラストラクチャサーバーに接続するための認証サービスを提供します。	ネットワークサービス
Citrix WEM Cloud メッセージングサービス	Citrix WEM クラウドサービスがクラウドインフラストラクチャサーバーからメッセージを受信するためのサービスを提供します。	ネットワークサービス
シトリックス セキュア プライベート アクセス™	すべてのエンタープライズアプリケーションへのゼロトラストネットワークアクセス	ネットワークサービス
シトリックス セキュア チケットティング オーソリティ サービス	Citrix Cloud サービスにセキュアなチケット発行機能を提供します。	ネットワークサービス

イベントメッセージとログ

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。これらのメッセージを監視ソフトウェアで検索できるようにしたい場合は、ZIP アーカイブとしてダウンロードできます。ZIP アーカイブには、次の XML ファイルにこれらのメッセージが含まれています。

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

Cloud Connector イベントメッセージをダウンロードします。(ZIPファイル)

トラブルシューティング

Cloud Connector に関する問題を診断する最初のステップは、イベントメッセージとイベントログを確認することです。リソースの場所に Cloud Connector が表示されない場合、または「接続されていません」と表示される場合、イベントログはいくつかの初期情報を提供します。

インストール

Cloud Connector が「エラー」状態の場合、Cloud Connector のホスティングに問題がある可能性があります。新しいマシンに Cloud Connector をインストールしてください。問題が解決しない場合は、Citrix サポートにお問い合わせください。Cloud Connector のインストールまたは使用に関する一般的な問題のトラブルシューティングについては、[CTX221535](#)を参照してください。

デプロイメントの計画と構築

Citrix Cloud Japan にサインアップした後、以下の手順で Citrix Cloud Japan への接続を設定します。事前にプロセス全体を確認して、何が必要か把握しておきましょう。

リソースの場所を設定する

リソースの場所には、Active Directory ドメインや Cloud Connector などのインフラストラクチャサーバーと、アプリケーションやデスクトップなどのリソースをユーザーに提供するマシンが含まれます。リソースの場所の設定は、Citrix DaaS™ (旧 Virtual Apps and Desktops service) を使用するために必要です。

手順については、「[リソースの場所を作成する](#)」を参照してください。

次のビデオでは、リソースの場所の作成と Cloud Connector の追加について説明しています。

```
<iframe src="https://www.youtube.com/embed/fLq6eI2x8uM" width="720px" height="480px"
frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
```

ID プロバイダーを接続する

ID プロバイダーは、Citrix Cloud Japan の管理者とワークスペースのサブスクライバーを認証し、サブスクライバーにライブラリの提供物を割り当てるためのユーザーリストへのアクセスを提供するために使用されます。

サポートされている ID プロバイダーの詳細については、「[ID およびアクセス管理](#)」を参照してください。

Citrix DaaS を設定する

Citrix DaaS を開始するには、次のタスクを完了します。

1. サブスクリプションをお持ちでない場合は、[サービス試用版をリクエスト](#)してください。サービス試用版は 60 日間有効で、製品版サービスとまったく同じ機能が提供されます。
2. Citrix DaaS 展開における顧客管理コンポーネントの[システム要件](#)を確認し、それに応じてマシンを準備します。

3. Citrix DaaS ドキュメントの「[展開の計画と構築](#)」にあるタスクの順序を確認し、各タスクの手順に従ってください。

Citrix Workspace の設定

エンドユーザー向けにワークスペースをセットアップするには、次のタスクが含まれます。

1. Workspace Configuration で Virtual Apps and Desktops サービス統合を有効にします。
2. 以前接続した ID プロバイダーをワークスペース認証方法として選択します。
3. エンドユーザーに提供するワークスペース機能を構成します。

Citrix Cloud Japan の Citrix Workspace で利用可能な機能の詳細については、「[ワークスペースのセットアップ](#)」を参照してください。

リソースロケーションを作成する

Citrix Cloud Japan にサインアップした後、リソースロケーションを作成してアカウントのセットアップを続行します。

リソースロケーションとは？

リソースロケーションには、ユーザーにサービスを提供するために必要なコンピューティングリソースとネットワークリソースが含まれています。リソースロケーションに含まれるリソースは、提供したいサービスによって異なります。たとえば、Citrix DaaS™（旧Virtual Apps and Desktops サービス）を介してアプリケーションとデスクトップを提供する場合、リソースロケーションには次のコンポーネントが含まれることがあります。

- アプリケーションとデスクトップにアクセスするユーザーを認証および承認するためのActive Directoryドメイン。
- 1つ以上のVirtual Delivery Agent (VDA) が必要です。これらは、提供したいアプリケーションとデスクトップをホストするマシン間の接続を管理します。また、それらのリソースにアクセスするために使用されるデバイスも処理します。
- アプリケーションとデスクトップを提供する仮想マシンをプロビジョニングするための、Citrix XenServer® 8、XenServer® 9、Microsoft Azureなどのサポートされているハイパーバイザーまたはクラウドサービス。

デフォルトのリソースロケーション

Citrix Cloud Japanアカウントにリソースロケーションがなく、ドメインにCloud Connectorをインストールする場合：

- Citrix Cloud Japanはリソースロケーションを作成します。
- この作成されたリソースロケーションがデフォルトのリソースロケーションになります。

アカウントにはデフォルトのリソースロケーションを1つしか持つことができません。必要に応じて、Citrix Cloud Japanで追加のリソースロケーションを作成できます。その後、他のドメインにCloud Connectorをインストールする際に、必要なものを選択します。

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

タスク1：マシンの準備

1. Citrix Cloud Connectorの要件を確認してください。

- 要件
- 重要な考慮事項
- サポートされているActive Directoryの機能レベル
- トラブルシューティング情報。

2. 構成要件を満たすマシンを準備します。
3. 準備したマシンをドメインに参加させます。

タスク2：接続の確認

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

1. 利用可能なサービスの連絡先アドレスのリストについては、接続要件を確認してください。
2. ポート443 (HTTPS) がアウトバウンド接続用に開いていることを確認します。
3. クラウドサービスの運用と利用を可能にするために、必要なアドレスに到達できることを確認します。
4. WebプロキシでCloud Connectorを使用する方法については、Citrix Cloud Connectorのプロキシとファイアウォールの構成を確認してください。

タスク3：Cloud Connectorのインストール

注：

Connector ApplianceはCitrix Cloud Japanでは利用できません。

インストール中、Cloud Connector は Cloud にアクセスする必要があります。

- インストールプロセスを承認するためにユーザーのIDを検証する
- インストーラーの権限を検証する
- Cloud Connector が提供するサービスをダウンロードして構成する。

インストールは、インストールを開始したユーザーの権限で実行されます。

1. Citrix Cloud Japan メニューから、**リソースの場所**を選択します。
2. **ダウンロード**をクリックして、Cloud Connector インストーラーをダウンロードします。
3. インストーラーをダブルクリックします。Citrix Cloud Japan は初期接続チェックを実行し、Citrix Cloud Japan 管理者のユーザー名とパスワードの入力を求めます。
4. ウィザードに従って Cloud Connector をインストールおよび構成します。インストールが完了すると、Citrix Cloud Japan は最終接続チェックを実行し、Cloud Connector が Citrix Cloud Japan と通信できることを確認します。

インストール後、Citrix Cloud Japan はお客様のドメインを **ID およびアクセス管理**に登録します。

注：

- 複数の組織アカウントの管理者である場合、Citrix Cloud Japan は Cloud Connector に関連付けるアカウントを選択するよう求めます。
- 組織アカウントにすでに複数のリソースの場所がある場合、Citrix Cloud Japan は Cloud Connector に関連付けるリソースの場所を選択するよう求めます。
- 長期間にわたって複数のインストールに同じ Cloud Connector インストーラーを使用することはお勧めしません。Citrix Cloud コンソールの ページから新しい Cloud Connector をダウンロードしてください。

追加のリソースの場所を作成する

1. Citrix Cloud Japan管理コンソールから、メニューボタンをクリックし、**リソースの場所**を選択します。

2. **リソースの場所**をクリックし、わかりやすい名前を入力します。
3. **保存**をクリックします。Citrix Cloud Japanに新しいリソースの場所のタイルが表示されます。
4. **Cloud Connectors**をクリックし、次に**ダウンロード**をクリックしてCloud Connectorソフトウェアを入手します。
5. 準備された各マシンで、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**のいずれかを使用してCloud Connectorソフトウェアをインストールします。

Cloud Connectorのインストールログ

Cloud Connector のインストールログは、`%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup` にあります。

すべてのログは、インストール後に`**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs**`に追加されます。

コマンドラインからCloud Connectorをインストールする

Citrix Cloud Connector™ソフトウェアは、対話形式でインストールすることも、サイレントインストールまたは自動インストールを使用することもできます。

インストール中、Cloud Connectorは、ユーザーの認証、権限の検証、サービスのダウンロードと構成のためにクラウドアクセスを必要とします。インストールは、それを開始したユーザーの権限で行われます。

重要:

繰り返しインストールする場合でも、同じインストーラーを使い続けしないでください。代わりに、Citrix Cloud Japanコンソールの「リソースの場所」ページから新しいCloud Connectorを入手してください。

要件

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

- Cloud ConnectorをインストールするCitrix Cloud Japan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、まずサービスプリンシパルを作成する必要があります。クライアントIDとシークレットは、Citrix Cloud APIへのアクセスが適切に保護されていることを保証します。サービスプリンシパルを作成すると、それはあなたが持つ管理者権限と同じ権限で動作します。Cloud Connectorをインストールするには、フルアクセス管理者によって作成されたサービスプリンシパルを使用してください。これにより、フルアクセス権限が保証されます。
- 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名のすぐ下にある**ID**ボタンを選択します。この値を指定しない場合、Citrix Cloud Japanはデフォルトのリソースの場所のIDを使用します。

サービスプリンシパルの作成

サービスプリンシパルを作成すると、Citrix Cloud Japanは一意的クライアントIDとシークレットを生成します。コマンドラインを通じてAPIを呼び出す際には、これらの値を指定する必要があります。

1. Citrix Cloud Japan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. **サービスプリンシパル**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。Citrix Cloud Japanは、サービスプリンシパルのクライアントIDとシークレットを生成して表示します。
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、各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

サービスプリンシパルのセキュリティ詳細については、インストーラーはJSON構成ファイルを必要とします。インストール完了後、このファイルを削除してください。サポートされている構成ファイルの値は次のとおりです。

- **customerName** 必須。Citrix Cloud Japan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。管理者によって作成されたサービスプリンシパルIDは、APIアクセスページにあります。
- **clientSecret** 必須。サービスプリンシパルが作成された後にダウンロードでき、APIアクセスページにあるサービスプリンシパルシークレット。

- **resourceLocationId** 推奨。既存のリソースロケーションの一意的識別子。Citrix CloudコンソールのリソースロケーションページでIDボタンを選択して、リソースロケーションIDを取得します。値が指定されていない場合、Citrix Cloudはアカウント内の最初のリソースロケーションのIDを使用します。
- **acceptTermsOfService** 必須。true に設定する必要があります。

構成ファイルの例：

```
{
  "customerName": "CustomerID",
  "clientId": "ClientID",
  "clientSecret": "ClientSecret",
  "resourceLocationId": "ResourceLocationId"
  "acceptTermsOfService": "true",
}
```

パラメーターファイルを使用してインストールするコマンドラインの例：

```
CWCCConnector.exe /q /ParametersFilePath:c:\cwccconnector_install_params.json
```

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

トラブルシューティング

インストールログ

インストールログは **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup** で利用できます。

また、インストール後にログは **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** に追加されます。

終了コード

- 1603 - 予期せぬエラーが発生しました。
- 2 - 前提条件の確認に失敗しました。
- 0 - インストールが正常に完了しました。

Citrix Cloud Connector™ プロキシおよびファイアウォール構成

ポート443はHTTPトラフィックを使用し、送信のみです。完全な接続の詳細については、以下の記事を参照してください。

- [接続要件](#)
- [シトリックス クラウド コネクタの要件](#)

Cloud Connectorは、Webプロキシサーバーを介したインターネットへの接続をサポートしています。インストーラーとそれがインストールするサービスの両方が、Citrix Cloud Japanへの接続を必要とします。インターネットアクセスは、これら両方のポイントで利用可能である必要があります。

重要:

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

ワイルドカードとFQDNを使用したトラフィックの除外

Cloud Connectorトラフィックを除外するようにプロキシサーバーを構成する場合は、Citrix Cloud Japanの[allowlist.json](#)ファイルに含まれている許可されたCloud Connector FQDNを使用してください。この種のトラフィックを除外するためにワイルドカードを使用しないでください。

次のコマンドは、Citrix Cloud Connectorで許可されているFQDNを使用してトラフィックを除外する例です。

```
netsh winhttp set proxy bypass-list agenthub-jp.citrixworkspacesapi.jp
```

詳細については、[Cloud Connectorで許可されているFQDN](#)を参照してください。

Cloud Connectorトラフィックを除外するためにワイルドカードアドレスを使用することはサポートされていません。バイパスリストをワイルドカードを使用して構成した場合、これらのアドレスは無視され、Cloud Connectorトラフィックが引き続き表示される可能性があります。

インストーラー

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

プロキシ設定の構成の詳細については、[Windowsでのプロキシサーバー設定の変更](#)を参照してください。

実行時のサービス

ランタイムサービスはローカルサービスのコンテキストで動作します。上記で説明したユーザーに対して定義された設定は使用しません。ブラウザから設定をインポートする必要があります。

これに対するプロキシ設定を構成するには、コマンドプロンプトウィンドウを開き、次のように **netsh** を使用します。

```
netsh winhttp import proxy source =ie
```

コマンドを実行した後、Cloud Connector をホストしているマシンを再起動して、サービスがこれらのプロキシ設定で起動するようにします。

詳細については、[Windows Hypertext Transfer Protocol \(WINHTTP\) 用 Netsh コマンド](#) を参照してください。

注:

自動検出またはPACスクリプトはサポートされていません。

クラウドサービス用コネクタアプライアンス

コネクタアプライアンスは、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™とリソースの場所間の通信チャネルとして機能し、複雑なネットワークやインフラストラクチャの構成を必要とせずにクラウド管理を可能にします。コネクタアプライアンスを使用すると、ユーザーに価値を提供するリソースを管理し、集中することができます。

コネクタアプライアンスは次の機能を提供します。

- **Active Directory**をCitrix Cloudに接続すると、AD管理が可能になり、リソースの場所内でADフォレストとドメインを使用できるようになります。これにより、追加のAD信頼を追加する必要がなくなります。詳細については、「[コネクタアプライアンスでのActive Directory](#)」を参照してください。

ただし、コネクタアプライアンスに依存するプレビュー中の他のサービスも存在する可能性があります。

- イメージポータビリティサービス
- シトリックス セキュア プライベート アクセス™

コネクタアプライアンス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
- タイムスタンプ
- イベントデータ
- Active Directoryからのユーザーおよびグループの詳細（例: ユーザーとグループの認証および検索に使用されます）

コネクタアプライアンスの可用性と負荷管理

継続的な可用性を確保し、負荷を管理するために、各リソースの場所に複数のコネクタアプライアンスをインストールします。Citrixは、各リソースの場所に少なくとも2つのコネクタアプライアンスを推奨しています。いずれかのコネクタアプライアンスが一時的に利用できなくなった場合でも、他のコネクタアプライアンスが接続を維持できます。各コネクタアプライアンスはステートレスであるため、負荷は利用可能なすべてのコネクタアプライアンスに分散されます。この負荷分散機能を構成する必要はありません。自動化されています。少なくとも1つのコネクタアプライアンスが利用可能であれば、Citrix Cloudとの通信が失われることはありません。

リソースの場所にコネクタが1つしか構成されていない場合、Citrix Cloudは**リソースの場所ページ**と**コネクタページ**の両方に警告を表示します。

コネクタ アプライアンスの更新

Connector Applianceは自動的に更新されます。コネクタを更新するために、お客様が何らかの操作を行う必要はありません。

リソースの場所を構成して、更新が利用可能になり次第すぐに適用するか、特定のメンテナンス期間中に適用するかを選択できます。

更新の一環として、Connector Applianceは一時的に利用できなくなります。更新は、リソースの場所にあるConnector Applianceのうち、一度に1つにのみ適用されます。このため、常に少なくとも1つのConnector Applianceが利用可能であることを保証するために、各リソースの場所に少なくとも2つのConnector Applianceを登録してください。

コネクタ アプライアンスの通信

Connector Applianceは、Citrix Cloudとリソースの場所間のすべての通信を認証および暗号化します。インストール後、Connector Applianceはアウトバウンド接続を介してCitrix Cloudとの通信を開始します。すべての接続は、標準のHTTPSポート（443）とTCPプロトコルを使用して、Connector Applianceからクラウドに確立されます。インバウンド接続は許可されません。

次の表に、Connector Applianceがアクセスする必要があるポートを示します。

サービス	ポート	サポートされるドメインプロトコル	構成の詳細
DNS	53	TCP/UDP	このポートはローカルセットアップに対して開いている必要があります。
NTP	123	UDP	このポートはローカルセットアップに対して開いている必要があります。
HTTPS	443	TCP	Connector Applianceはこのポートへのアウトバウンドアクセスを必要とします。

Connector Appliance を構成するには、IT 管理者は Connector Appliance のポート 443 (HTTPS) の管理インターフェイスにアクセスする必要があります。

注:

IP アドレスの先頭に `https://` を含める必要があります。

Connector Appliance は、リソースロケーション内のオンプレミスシステムと外部システムの両方と通信できます。Connector Appliance の登録中に 1 つ以上の Web プロキシを定義した場合、Connector Appliance から外部システムへのトラフィックのみがこの Web プロキシを介してルーティングされます。オンプレミスシステムがプライベートアドレス空間にある場合、Connector Appliance からこのシステムへのトラフィックは Web プロキシを介してルーティングされません。

Connector Appliance は、プライベートアドレス空間を以下の IPv4 アドレス範囲として定義します。

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

インターネット接続要件

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

Citrix Cloudサービスを適切に運用および利用するには、以下のIPアドレスに未変更のHTTPS接続でアクセスする必要があります。

- `https://*.citrixcloud.jp`
- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixnetworkapi.jp`
- `https://*.nssvc.jp`
 - すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます。
 - `https://*.g.nssvc.jp`
 - `https://*.c.nssvc.jp`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

ネットワーク要件

環境が以下の構成になっていることを確認してください。

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

システム要件

Connector Applianceは、以下のハイパーバイザーでサポートされています。

- シトリックス ハイパーバイザー 8.2 CU1 LTSR
- VMware ESXiバージョン7アップデート2
- Windows Server 2016、Windows Server 2019、またはWindows Server 2022上のハイパーV。
- ニュタニックス AHV
- マイクロソフト Azure
- AWS
- グーグル クラウド プラットフォーム

お使いのハイパーバイザーは、以下の最小要件を満たす必要があります。

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

同じハイパーバイザーホスト上に複数のConnector Applianceをホストできます。同じホスト上のConnector Applianceの数は、ハイパーバイザーとハードウェアの制限によってのみ制約されます。

注:

Connector Appliance VM のクローン作成、一時停止、およびスナップショットの取得はサポートされていません。

コネクタアプライアンスを入手する

Citrix Cloud 内からコネクタアプライアンスソフトウェアをダウンロードします。

1. Citrix Cloudにサインインします。
2. 画面左上のメニューから、**リソースの場所**を選択します。
3. リソースの場所がまだない場合は、プラスアイコン (+) をクリックするか、**リソースの場所を追加**を選択します。
4. Connector Appliance を登録するリソースの場所で、**Connector Appliances** のプラスアイコン (+) をクリックします。

Connector Appliance の追加タスクが開きます。

Connector Appliance のインストールタスク(/en-us/citrix-cloud-japan/media/connector-appliance-install.png)

5. **手順 1 の ハイパーバイザー** リストから、Connector Appliance のホストに使用するハイパーバイザーまたはクラウドプロバイダーの種類を選択します。
 - オンプレミスのハイパーバイザーおよびクラウド環境の場合、Citrix Cloud 内で Connector Appliance をダウンロードできます。
 - a. **イメージのダウンロード**をクリックします。
 - b. Citrix エンドユーザーサービス契約を確認し、同意する場合は、**同意して続行**を選択します。
 - c. プロンプトが表示されたら、提供された Connector Appliance ファイルを保存します。

Connector Appliance ファイルのファイル名拡張子は、選択したハイパーバイザーによって異なります。

- 一部のクラウド環境では、マーケットプレイスから Connector Appliance を入手できません。

- AWS
- マイクロソフト アジュール
- グーグル クラウド

6. **Connector Appliance** のインストールタスクを開いたままにします。Connector Appliance のインストール後、登録コードを**手順 2**に入力します。

Connectors ページから**Connector Appliance** のインストールタスクにアクセスすることもできます。プラスアイコン (+) を選択してコネクタを追加し、Connector Appliance を追加することを選択します。

ハイパーバイザーに Connector Appliance をインストールする

- シトリックス ハイパーバイザー™
- ヴィエムウェア イーエスエックスアイ
- ハイパーV
- ニュータニックス エーエイチブイ
- マイクロソフト アジュール
- グーグル クラウド プラットフォーム
- AWS

シトリックス ハイパーバイザー

このセクションでは、XenCenter を使用して Connector Appliance を Citrix Hypervisor サーバーにインポートする方法について説明します。

1. ダウンロードした Connector Appliance XVA ファイルにアクセスできるシステムで、XenCenter を使用して 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」を選択します。
3. Connector Appliance XVA ファイルが保存されているパスを指定または参照します。「次へ」をクリックします。
4. Connector Appliance をホストする Citrix Hypervisor サーバーを選択します。または、Connector Appliance をホストするプールを選択すると、Citrix Hypervisor が適切な利用可能なサーバーを選択します。「次へ」をクリックします。

5. Connector Appliance に使用するストレージリポジトリを指定します。「インポート」をクリックします。
6. 仮想ネットワークインターフェースを追加するには、「追加」をクリックします。「ネットワーク」リストから、Connector Applianceが使用するネットワークを選択します。「次へ」をクリックします。
7. Connector Applianceを展開するために使用するオプションを確認します。誤りがある場合は、「戻る」を使用してこれらのオプションを変更します。
8. 「インポート完了後、新しいVMを自動的に起動する」が選択されていることを確認します。「完了」をクリックします。

Connector Applianceが展開され、正常に起動すると、そのコンソールに、Connector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。環境でDHCPが利用できない場合、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。詳細については、「[Connector Applianceコンソールを使用してネットワーク構成を設定する](#)」を参照してください。

次のステップ: 「[Citrix CloudにConnector Applianceを登録する](#)」。

ヴィエムウェア ESXi

このセクションでは、VMware vSphere Clientを使用してVMware ESXiホストにConnector Applianceを展開する方法について説明します。

1. ダウンロードしたConnector Appliance OVAファイルにアクセスできるシステムで、vSphere Clientを使用してESXiホストに接続します。
2. 「ファイル」 > 「OVFテンプレートの展開...」を選択します。
3. Connector Appliance OVAファイルが配置されているパスを指定または参照します。「次へ」をクリックします。
4. テンプレートの詳細を確認します。「次へ」をクリックします。
5. Connector Applianceインスタンスに一意の名前を指定できます。デフォルトでは、名前は「**Connector Appliance**」に設定されています。このESXiホストでホストされている他のConnector Applianceインスタンスと区別できる名前を選択してください。「次へ」をクリックします。
6. Connector Applianceの保存先ストレージを指定します。「次へ」をクリックします。

7. 仮想ディスクを保存する形式を選択します。「次へ」をクリックします。
8. Connector Applianceを展開するために使用するオプションを確認します。誤りがある場合は、「戻る」を使用してこれらのオプションを変更します。
9. 「展開後に電源をオンにする」を選択します。「完了」をクリックします。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。環境でDHCPが利用できない場合は、Connector Appliance UIにアクセスする前に、Connector Applianceコンソールでネットワーク構成を設定する必要があります。詳細については、「[Connector Applianceコンソールを使用してネットワーク構成を設定する](#)」を参照してください。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

ハイパーV

このセクションでは、Hyper-VホストにConnector Applianceを展開する方法について説明します。Hyper-Vマネージャーを使用するか、付属のPowerShellスクリプトを使用してVMを展開できます。

Hyper-Vマネージャーを使用してConnector Applianceを展開する

1. Hyper-Vホストに接続します。
2. Connector ApplianceのZIPファイルをHyper-Vホストにコピーまたはダウンロードします。
3. ZIPファイルの内容を抽出します。ZIPファイルには、PowerShellスクリプトとconnector-appliance.vhdxファイルが含まれています。
4. VHDXファイルをVMディスクを保持したい場所にコピーします。例: `C:\ConnectorApplianceVMs`。
5. Hyper-Vマネージャーを開きます。
6. サーバー名を右クリックし、「新規 > 仮想マシン」を選択します。
7. 「新しい仮想マシンウィザード」の「名前と場所の指定」パネルで、Connector Applianceを識別するための一意の名前を入力します。「次へ」をクリックします。
8. **Specify Generation**パネルで、**Generation 1**を選択します。**Next**をクリックします。
9. **Assign Memory**パネルで、次の設定を構成してから**Next**をクリックします。
 - a. 4 GBのRAMを割り当てます。

- b. 動的メモリを無効にします。
- 10. **Configure Networking**パネルで、リストからスイッチ（例: Default Switch）を選択します。
Nextをクリックします。
- 11. **Connect Virtual Hard Disk**パネルで、**Use an existing virtual hard disk**を選択します。
- 12. connector-appliance.vhdxファイルの場所に移動して選択します。**Next**をクリックします。
- 13. **Summary**パネルで、選択した値を確認し、**Finish**をクリックしてVMを作成します。
- 14. **Virtual Machines**パネルで、Connector Appliance VMを右クリックし、**Settings**を選択します。
- 15. **Settings**ウィンドウで、**Hardware > Processors**を選択し、次のアクションを実行します。
 - a. **Number of virtual processors**で、値を2に変更します。
 - b. **Apply**をクリックします。
 - c. **OK**をクリックします。
- 16. **Virtual Machines**パネルで、Connector Appliance VMを右クリックし、**Start**を選択します。
- 17. Connector Appliance VMを右クリックし、**Connect**を選択してコンソールを開きます。

Connector Applianceが展開され、正常に起動した後、Hyper-Vマネージャーを使用してコンソールに接続します。コンソールには、Connector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。環境でDHCPが利用できない場合は、Connector Appliance UIにアクセスする前に、Connector Applianceコンソールでネットワーク構成を設定する必要があります。詳細については、「[Connector Applianceコンソールを使用してネットワーク構成を設定する](#)」を参照してください。

次のステップ: 「[Citrix CloudにConnector Applianceを登録する](#)」。

PowerShellスクリプトを使用してConnector Applianceを展開する

connector-appliance.zipファイルには、新しいVMを作成して起動するPowerShellスクリプトが含まれています。

注:

この署名されていないPowerShellスクリプトを実行するには、Hyper-Vシステムで実行ポリシーを変更する必要がある場合があります。詳細については、<https://go.microsoft.com/fwlink/?LinkID=135170>を参照してください。または、提供されているスクリプトを基にして、独自のローカルスクリプトを作成または修正することもできます。

1. Hyper-Vホストに接続します。
2. Connector Appliance ZIPファイルをHyper-Vホストにコピーまたはダウンロードします。
3. ZIPファイルの内容（PowerShellスクリプトとVHDXファイル）を抽出します。
4. PowerShellコンソールで、現在のディレクトリをZIPファイルの内容が配置されている場所に移動し、次のコマンドを実行します。

```
.\connector-appliance-install.ps1
```

5. プロンプトが表示されたら、VMの名前を入力するか、**Enter**キーを押してデフォルト値の**Connector Appliance**を受け入れます。
6. プロンプトが表示されたら、ルートディスクの保存先を入力するか、**Enter**キーを押してVHDのシステムデフォルトディレクトリを使用します。
7. プロンプトが表示されたら、ルートディスクのファイル名を入力するか、**Enter**キーを押してデフォルト値のconnector-appliance.vhdxを受け入れます。
8. プロンプトが表示されたら、使用するスイッチを選択します。**Enter**キーを押します。
9. VMインポート情報の概要を確認します。情報が正しい場合は、**Enter**を選択して続行します。スクリプトはConnector Appliance VMを作成して起動します。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用してConnector Applianceに接続し、登録プロセスを完了します。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

ニュータニックス エーエイチブイ

このセクションでは、Nutanix Prism Webコンソールを使用して、`connector-appliance.vhdx`ファイルからNutanix AHVホストにConnector Applianceを展開する方法について説明します。

1. Nutanix Prism Webコンソールのメインメニューで、**Storage** ビューを選択します。

2. **+ Storage Container** をクリックして、Connector Applianceイメージファイルを保持するストレージコンテナを作成します。または、既存のストレージコンテナを使用することもできます。
3. `connector-appliance.vhdx` ファイルをストレージコンテナにアップロードします。
 - a. Webコンソールのメインメニューで、**Settings** を選択します。
 - b. **Image Configuration** タブを選択し、**+ Upload Image** をクリックします。
 - c. **Create Image** で、イメージの**Name** を指定します。
 - d. **Image Type** リストから、**DISK** を選択します。
 - e. **Storage Container** リストから、作成したストレージコンテナを選択します。
 - f. **Upload a file** を選択します。
 - g. **Choose file** をクリックし、ローカルシステム上の `connector-appliance.vhdx` ファイルに移動します。
 - h. 「**保存**」をクリックします。
4. イメージが作成され、「**イメージ構成**」ページでその状態が「**ACTIVE**」と表示されるまで待ちます。
5. 「**ネットワーク構成**」タブを選択します。
6. Connector Applianceが使用するネットワークを作成するには、「**+ ネットワークの作成**」をクリックします。
7. 「**ネットワークの作成**」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. Connector Applianceインスタンスを作成するには、「**+ VMの作成**」をクリックします。
10. 「**VMの作成**」で、次の情報を指定します。
 - VM名
 - vCPUの数
 - GiB単位のメモリ量
11. 「**レガシーBIOS**」を使用するように選択します。
12. VMにディスクを追加するには、「**+ 新しいディスクの追加**」をクリックします。

13. 「ディスクの追加」で、次の情報を入力します。
 - a. 「タイプ」で「**DISK**」を選択します。
 - b. 「操作」で「**イメージサービスからクローン**」を選択します。
 - c. 「バスタイプ」で「**SCSI**」を選択します。
 - d. 「イメージ」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. 「追加」をクリックして、ディスクの追加を完了します。
15. 「VMの作成」で、「+ 新しいNICの追加」をクリックします。
16. 「NICの作成」で、VMを追加するネットワークを選択します。
17. 「ネットワーク接続状態」で「**接続済み**」を選択します。
18. 「追加」をクリックして、NICの追加を完了します。
19. 「保存」をクリックして、VMを作成します。

デフォルトでは、新しいVMは電源オフになっています。

20. 「**VM**」ビューで、VMを選択し、「**電源オン**」をクリックします。
21. VMが起動するまで待ちます。このプロセスには数分かかる場合があります。

Connector Applianceが展開され、正常に起動した後、次のいずれかの場所でConnector ApplianceのIPアドレスを見つけることができます。

- Nutanix Prism Webコンソールの「**VM**」ビューで。
- Connector Applianceコンソールで。

このIPアドレスを使用してConnector Applianceの管理ページに接続し、登録プロセスを完了します。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

マイクロソフト アジュール

このセクションでは、Microsoft AzureにConnector Applianceを展開する方法について説明します。Azure Marketplaceから、または付属のPowerShellスクリプトを使用してダウンロードしたディスクイメージから、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. アジュール マーケットプレイスでコネクタ アプライアンスに移動します。(アジュール マーケットプレイス)

または、マーケットプレイス検索で「Connector Appliance for Cloud Services」を検索することもできます。

2. 「今すぐ入手」をクリックし、次に「作成」をクリックします。
3. 「Citrix Connector™ Appliance for Cloud Servicesの作成」ページで、次の情報を入力します。

- 使用する「サブスクリプション」を選択します。
- 使用する「リソースグループ」を選択します。
- Connector Applianceを配置する「リージョン」を選択します。
- 「VM名」を指定します。
- Connector Applianceを追加する仮想ネットワークを選択します。このネットワークは、Citrix Cloud、ローカルリソース、およびConnector Appliance管理ページへのアクセスに使用されます。このネットワークは後で変更できません。
- 「サブネット」の値を指定します。

「次へ: タグ >」をクリックします。

4. 「タグ」タブで、必要に応じて必須タグを追加します。

「次へ: レビュー + 作成 >」をクリックします。

5. 展開の詳細を確認したら、「作成」をクリックします。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用してConnector Appliance管理ページに接続し、登録プロセスを完了します。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

PowerShellスクリプトを使用してConnector Appliance VMを展開する

`connector-appliance-azure.zip` ファイルには、新しいVMを作成して起動するPowerShellスクリプトが含まれています。提供されているスクリプトを基にして、独自のローカルスクリプトを作成または修正できます。

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ます。

- VHDファイルが配置されているディレクトリでPowerShellスクリプトを実行します。

次の手順を完了します。

1. Connector Appliance ZIPファイルをWindowsシステムにコピーまたはダウンロードします。
2. ZIPファイルの内容を抽出します。PowerShellスクリプトとVHDファイルです。
3. 管理者としてPowerShellコンソールを開きます。
4. 現在のディレクトリをZIPファイルの内容が保存されている場所に移動し、次のコマンドを実行します。

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

5. ダイアログが表示され、Microsoft Azureへのログインを求められます。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、イメージのアップロードと仮想マシンの作成を行います。
8. 最初のVMを作成した後、スクリプトはアップロードされたイメージから別のVMを作成するかどうかを尋ねます。
 - 別のVMを作成するには、**y**と入力します。
 - スクリプトを終了するには、**n**と入力します。

Connector Applianceが展開され、正常に起動すると、そのコンソールにConnector ApplianceのIPアドレスを含むランディングページが表示されます。このIPアドレスを使用してConnector Applianceの管理ページに接続し、登録プロセスを完了します。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

AWS

このセクションでは、AWSにConnector Applianceを展開する方法について説明します。Connector ApplianceはAWS MarketplaceでAMIとして利用可能であり、AMIからConnector Applianceをインストールすることをお勧めします。または、AWS UIを使用するか、付属のPowerShellスクリプトを使用して、ダウンロードしたディスクイメージを展開することもできます。

ネットワークの前提条件

AWSにConnector Applianceを展開するには、Connector Applianceが作成されるサブネットからCitrix Cloudへのアクセスがあ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。これは、Citrix Cloudへのアクセスを提供するために特定の構成を必要とします。この構成を実現するには、**AWS Management Console**で次の手順を完了してください。

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. 右上にある**Create NAT Gateway**をクリックします。次の情報を入力します。
 - **Name**を入力します。
 - リストから**subnet**を選択します。
 - **Connectivity type**を**Public**に設定します。
 - リストから**Elastic IP allocation ID**を選択します。利用可能なElastic IPがない場合は、**Allocate Elastic IP**をクリックし、指示に従って作成します。
- c. **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. 右上にある**Create route table**をクリックします。次の情報を入力します。
 - **Name**を入力します。
 - リストから、NATゲートウェイの作成時に選択したサブネットを含むVPCを選択します。
- c. 「**ルートテーブルの作成**」をクリックします。
- d. 作成したルートテーブルの「**ルート**」タブで、「**ルートの編集 > ルートの追加**」をクリックします。
- e. 新しいルートエントリの「**送信先**」と「**ターゲット**」を入力します。
 - 送信先を0.0.0.0/0に設定します。
 - ターゲットには、作成した「**NAT Gateway**」をリストから選択します。
- f. 「**変更を保存**」をクリックします。

3. Connector Applianceで使用するサブネットをこのルートテーブルにアタッチします。
 - a. 上部のナビゲーションバーで、「サービスを選択 > VPC > ルートテーブル」を選択します。
 - b. NATゲートウェイを含むルートテーブルを選択します。
 - c. 表示ページで、「サブネットの関連付け」タブに移動します。
 - d. 「サブネットの関連付けを編集」をクリックします。
 - e. ルートテーブルにアタッチするサブネットを選択します。
 - f. 「関連付けを保存」をクリックします。

AWS MarketplaceからConnector Applianceを展開する

開始する前に、以下の前提条件を満たしていることを確認してください。

- EC2 リソースを操作する権限があること。
- [Networking prerequisites](#) の構成が完了していること。
- (オプション) Connector Appliance へのアクセスを許可する IP アドレスを制限するセキュリティグループを作成できます。

次の手順を完了します。

1. **AWS Management Console** にログインします。
2. AWS Marketplace で Connector Appliance AMI を見つけます。これを行うには、次のいずれかの方法を使用します。
 - Citrix Cloud で提供されている Marketplace リンクをたどります。([AWS Marketplace](#))
 - AWS Management Console で AMI を検索します。
 - a. **Services > Compute > EC2 > AMIs** に移動します。
 - b. 米国東部 (オハイオ) リージョンにいることを確認します。
 - c. **Public images** で、「Citrix Connector Appliance」または AMI ID 「ami-026eaf9b3b232577f」を検索します。
3. AMI ID (ami-026eaf9b3b232577f) と所有者 ID (414337923189) を確認して、正しい AMI であることを検証します。
4. AMI をサブスクリプションにコピーします。
 - a. **Actions > Copy AMI** に移動します。
 - b. **Copy AMI** ダイアログで、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の概要ページから、「**Launch instance from AMI**」をクリックします。
 6. 「**Launch an instance**」ダイアログで、次の手順を実行します。
 - a. 作成するインスタンスの数を選択します。回復性を高めるため、各リソースの場所に2つ以上のConnector Applianceを配置することをお勧めします。
 - b. インスタンスの名前を指定します。
 - c. 「**Instance type**」には、「**t2.medium**」を選択します。インスタンスタイプは、少なくとも4 GBのメモリと2つのCPUを搭載している必要があります。
 - d. 「**Key pair (login)**」には、「**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ていないため、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**」のいずれかを選択します。
 - 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 Management Consoleで「**Services > EC2 > Instances**」に移動して、インスタンスのリストを表示することもできます。
8. インスタンスの**状態**が**実行中**に変わったら、インスタンスの詳細に入り、**プライベート IPv4 アドレス**を使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

ブラウザから内部 IP アドレスで Connector Appliance 管理ページにアクセスし、登録プロセスを完了するには、踏み台ホストを使用する必要がある場合があります。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。このネットワーク構成は、Connector Appliance の Web インターフェースを使用して編集できます。

詳細については、「[Connector Appliance 管理ページでのネットワーク設定の構成](#)」を参照してください。

次のステップ: [Connector Appliance](#) を Citrix Cloud に登録する。

AWS UI を使用して Connector Appliance を展開する

開始する前に、次の前提条件を満たしていることを確認してください。

- S3 および EC2 リソースを操作する権限があること。
- VM インポートアクセス権を持つサービスロールとポリシーを作成していること。詳細については、<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role> を参照してください。

注:

サービスロールを作成するには、S3 バケットを作成する必要があります。ポリシーを作成する際は、作成した S3 バケットに VM インポートアクセスを設定してください。

- AWS CloudShell へのアクセス権があること。これは特定のリージョンでのみ利用可能です。AWS CloudShell がサポートされているリージョンのリストについては、<https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html> を参照してください。
- [ネットワークの前提条件](#)の構成を完了していること。

次のステップを完了してください。

1. ローカルシステムで、[connector-appliance-aws.zip](#) の内容を抽出します。
2. **AWS Management Console**にログインします。
3. 以下の手順を完了してストレージバケットを作成します。(または、これらの手順をスキップして既存のストレージバケットを使用することもできます。)
 - a. 上部のナビゲーションバーで、**Services > S3 > Create bucket** を選択します。
 - b. バケットの一意的な名前を入力します。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ください。リージョンが異なる場合、バケット内のファイルを使用できません。

d. 残りの設定はデフォルトのままにし、**Create bucket** をクリックします。

4. 作成したバケットの名前をクリックします。**Upload > Add files** をクリックし、`connector-appliance.vhd` ファイルを選択します。残りの設定はデフォルトのままにし、**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 icon** をクリックし、以下のコマンドを実行します。

a. VHD ファイルをスナップショットに変換するタスクを作成します。

```
aws ec2 import-snapshot --disk-container
Format=VHD,Url="&lt;S3_URI>"
```

プレースホルダーの値を、前の手順でコピーした S3 URI に置き換えます。例: `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`。

このコマンドは、次のコマンドが `"Status": "completed"` を含む JSON 文字列を返すと完了します。JSON 出力内の `ImportTaskId` の値をメモしておきます。

b. 次のコマンドを実行します。

```
aws ec2 describe-import-snapshot-tasks --import-task-ids
&lt;ImportTaskId>
```

プレースホルダーの値を、前の手順でコピーした `ImportTaskId` に置き換えます。例: `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`。

7. **AWSManagement Console** の上部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、**イメージを作成** をクリックします。

10. 開いたペインで、次の手順を完了します。

a. AMI の名前を入力します。

b. **ハードウェア支援仮想化** 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、**起動**をクリックします。
13. 開いたペインで、次の手順を完了します。
 - a. インスタンスタイプを選択します。
 - b. (オプション) **インスタンスの設定**タブでネットワークをカスタマイズします。
 - c. (オプション) **ストレージの追加**タブで別のボリュームをアタッチします。
 - d. **セキュリティグループの設定**タブでセキュリティグループルールを設定します。

インスタンスの起動を確認したら、**確認と起動**をクリックします。

Connector Appliance が展開され、正常に起動したら、**サービス > EC2 > インスタンス**に移動し、作成したインスタンスを選択します。**プライベート IPv4 アドレス**を使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。インストールプロセスを続行するには、ブラウザから内部 IP アドレスで Connector Appliance 管理ページにアクセスするために、踏み台ホストを使用する必要がある場合があります。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。このネットワーク構成は、Connector Appliance の Web インターフェイスを使用して編集できます。詳細については、「[Connector Appliance 管理ページでのネットワーク設定の構成](#)」を参照してください。

次のステップ: [Citrix Cloud に Connector Appliance を登録する](#)。

PowerShellスクリプトを使用してConnector Applianceを展開する

`connector-appliance-aws.zip` ファイルには、新しいVMを作成して起動するPowerShellスクリプトが含まれています。スクリプトを実行する前に、以下の前提条件を満たしていることを確認してください。

- システムにAWS.Tools、AWSPowerShell.NetCore、またはAWSPowerShellのいずれかがインストールされていること。詳細については、<https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html> を参照してください。
- VMインポートアクセスを持つサービスロールとポリシーを作成していること。このPowerShellスクリプトが機能するには、サービスロールとポリシーの両方に `vmimport` という名前を付ける必要があります。詳細については、<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role> を参照してください。

注:

サービスロールを作成するには、S3バケットを作成する必要があります。ポリシーを作成する際は、作成したS3バケットにVMインポートアクセスを設定してください。

- Amazon EC2セキュリティグループを作成していること。
- S3権限とAPIアクセスがあること。
- ネットワークの前提条件で構成を完了していること。

次の手順を完了してください。

1. ローカルシステムで、`connector-appliance-aws.zip` の内容をフォルダーに抽出します。
2. PowerShellで、次のコマンドを実行します。
 - a. ローカル環境でAWSコマンドレットを実行できるようにするには、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シークレットキーに置き換えます。一意のプロファイル名を指定してください。提供されている例では、`MyProfile` です。

- b. プロファイルをデフォルトに設定します。

```
Initialize-AWSDefaultConfiguration -ProfileName MyProfile
```

- c. 現在のディレクトリを、抽出されたファイルが保存されているフォルダーに変更し、次のコマンドを実行します。

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

3. スクリプトのプロンプトに従って、Connector Applianceの展開リージョンの選択、選択したバケットへのイメージのアップロード、VM名の入力を行います。
 - 以前に作成した、VMインポートアクセス権を持つバケットを使用する必要があります。
 - 使用するVPCを選択するよう求められたら、NATゲートウェイとルートテーブルが構成されているVPCを選択します。

- 使用するサブネットを選択するよう求められたら、NATゲートウェイを含むルートテーブルにアタッチされているサブネットを選択します。

詳しくは、「[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Connector ApplianceのプライベートIPアドレスが表示されます。ブラウザから内部IPアドレスを使用してConnector Appliance管理ページにアクセスし、登録プロセスを完了するには、踏み台ホストを使用する必要があります。

デフォルトでは、Connector ApplianceはDHCPを使用してネットワーク構成を設定します。このネットワーク構成は、Connector ApplianceのWebインターフェイスを使用して編集できます。詳しくは、「[Connector Appliance管理ページでのネットワーク設定の構成](#)」を参照してください。

次の手順：[Citrix CloudへのConnector Applianceの登録](#)。

グーグルクラウド プラットフォーム

このセクションでは、Google Cloud PlatformにConnector Applianceを展開する方法について説明します。Connector Applianceは、Google Cloud Marketplaceからインストールできます。または、Google Cloud Platform Consoleを使用するか、付属のPowerShellスクリプトを使用して、ダウンロードしたディスクイメージを展開することもできます。

ファイル `connector-appliance-gcp.zip` には以下が含まれます。

- Connector Applianceのディスクイメージである `connector-appliance.tar.gz`
- Connector Applianceを自動的に展開するために使用できるPowerShellスクリプトである `connector-appliance-upload-gcp.ps1`

グーグルクラウド マーケットプレイス から コネクタ アプライアンス を展開する

1. Google アカウントにログインします。
2. Citrix Cloud で提供されているマーケットプレイスのリンクに従います。([Google Cloud Marketplace](#))

または、マーケットプレイス検索で「Connector Appliance for Cloud Services」を検索することもできます。

3. **起動** をクリックします。
4. **新しいCitrix Connector Appliance for Cloud Services展開** 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 **マシンファミリー**、**シリーズ**、および **マシンタイプ** を選択します。
- 使用する **ブートディスクタイプ** と **ブートディスクサイズ (GB)** を選択します。
- **ネットワーク** セクションで、Connector Appliance が使用するネットワークインターフェイスを指定します。パブリックネットワークから管理ページに接続できるようにする場合は、**外部IP** を指定します。

展開 をクリックします。デプロイメントマネージャー ページに移動します。

注:

Connector Appliance が展開され、正常に起動した後、Connector Appliance が Google Cloud Platform に展開されたことを確認するメールが届きます。

5. デプロイメントマネージャー 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ースを設定する際に、以前に**外部IP**を指定した場合は、**詳細タブ**の**ネットワークインターフェース**セクションにある**外部IPアドレス**をコピーします。このIPアドレスを使用して、Connector Applianceの管理ページに接続し、登録プロセスを完了します。あるいは、Connector Applianceと同じサブネットにある別のマシンから、**プライマリ内部IPアドレス**を使用してConnector Applianceの管理ページにアクセスすることもできます。

次のステップ: [Citrix CloudにConnector Applianceを登録する](#)。

Google Cloud Platformコンソールを使用してConnector Applianceを展開する

1. ローカルシステムで、`connector-appliance-gcp.zip` の内容を抽出します。
2. Google Cloud Platformプロジェクトで、ストレージバケットを作成します。(または、既存のストレージバケットを使用することもできます。)
 - a. メインメニューから、**Cloud Storage**を選択します。
 - b. メインペインで、**バケットを作成**を選択します。
 - c. バケットの名前を指定します。
 - d. 必要なデータストレージとアクセス設定を構成します。これらの設定はデフォルトのままにしておくことができます。
 - e. **作成**をクリックします。

3. ストレージバケット内で、**ファイルをアップロード**を選択し、ファイル `connector-appliance.tar.gz` を選択します。ファイルがアップロードされるまで待ちます。
4. アップロードされたファイルを選択して詳細を表示します。**gsutil URI**の値をクリップボードにコピーします。
5. ヘッダーバーの**Cloud Shellをアクティブにする**アイコンをクリックして、Cloud Shellを開きます。
6. Cloud Shellで、イメージを作成するために次のコマンドを実行します。

```
gcloud compute images create "Image name" --guest-os-features=MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-appliance.tar.gz file"
```

7. メインメニューから、**Compute Engine > VMインスタンス**を選択します。
8. 「**インスタンスを作成**」を選択します。開いたペインで、次の情報を指定します。
 - a. 「名前」フィールドに、Connector Applianceインスタンスの名前を指定します。
 - b. Connector Applianceを配置するリージョンを選択します。
 - c. マシン構成を選択します。
 - d. 「**ブートディスク**」セクションで、「**変更**」をクリックします。
 - e. 開いたセクションで、「**カスタムイメージ**」タブに移動します。
 - f. 「**イメージ**」リストから、作成したイメージを選択します。
 - g. 「**選択**」をクリックします。
 - h. 「**ファイアウォール**」セクションで、Connector Appliance管理ページへのアクセスを許可するためにHTTPSトラフィックを有効にします。
 - i. 必要な追加構成を指定します。たとえば、デフォルトのネットワーク構成を使用しない場合があります。
- 「**作成**」をクリックします。
9. 「**VMインスタンス**」セクションで、新しく作成したVMを選択してその詳細を表示します。

Connector Applianceが展開され、正常に起動した後、「**VMインスタンス**」セクションにConnector ApplianceのIPアドレスが表示されます。

Connector Applianceに外部IPアドレスがある場合、このIPアドレスを使用してブラウザからConnector Appliance管理ページにアクセスし、登録プロセスを完了できます。

Connector Applianceに内部IPアドレスしかない場合、bastionホストを使用してブラウザから Connector Appliance管理ページにアクセスし、登録プロセスを完了します。詳細については、[<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>](https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host) を参照してください。

次のステップ: Citrix Cloud に Connector Appliance を登録する。

PowerShell スクリプトを使用して Connector Appliance を展開する

提供されている PowerShell スクリプトを使用して Connector Appliance を展開するには、システムに Google Cloud SDK がインストールされている必要があります。

1. ローカルシステムで、`connector-appliance-gcp.zip` の内容をフォルダーに抽出します。
2. PowerShell で、抽出されたファイルが置かれている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. 開いたブラウザウィンドウで、Connector Appliance を展開するプロジェクトへのアクセス権を持つアカウントを使用して Google Cloud SDK で認証します。
5. Google Cloud Tools for PowerShell で、PowerShell スクリプトによってプロンプトが表示されたら、使用するプロジェクトを選択します。Enter キーを押します。
6. スクリプトのプロンプトに従って、ディスクのアップロード、イメージの作成、仮想マシンの作成を行います。
7. 最初の VM を作成した後、スクリプトはアップロードされたイメージから別の VM を作成するかどうかを尋ねます。
 - `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、正常に起動した後、スクリプトは Connector Appliance の内部 IP アドレスを表示します。または、Google Cloud Platform コンソールに移動して、Connector Appliance の内部 IP アドレスを見つけることもできます。**Compute Engine > VM インスタンス**セクションに Connector Appliance の IP アドレスが表示されます。

踏み台ホストを使用して、ブラウザから内部 IP アドレスにある Connector Appliance 管理ページにアクセスし、登録プロセスを完了します。詳細については、[<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>](https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host) を参照してください。

次のステップ: Citrix Cloud に Connector Appliance を登録する。

Citrix Cloud に Connector Appliance を登録する

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

このセクションでは、Key Registration Service (KRS) からの 8 桁のコードを使用して Connector Appliance を登録する方法について説明します。

ハイパーバイザーに Connector Appliance をインストールして起動すると、コンソールに Connector Appliance の IP アドレスが表示されます。コンソールには、Connector Appliance UI への接続を検証するために使用できる SSL フィンガープリントも表示されます。

```
Citrix
-----

Connector Appliance for Cloud Services 4.0.4.282
Downloaded from Citrix - https://citrix.cloud.com

Please go to:
https://10.71.57.66
to manage your deployment

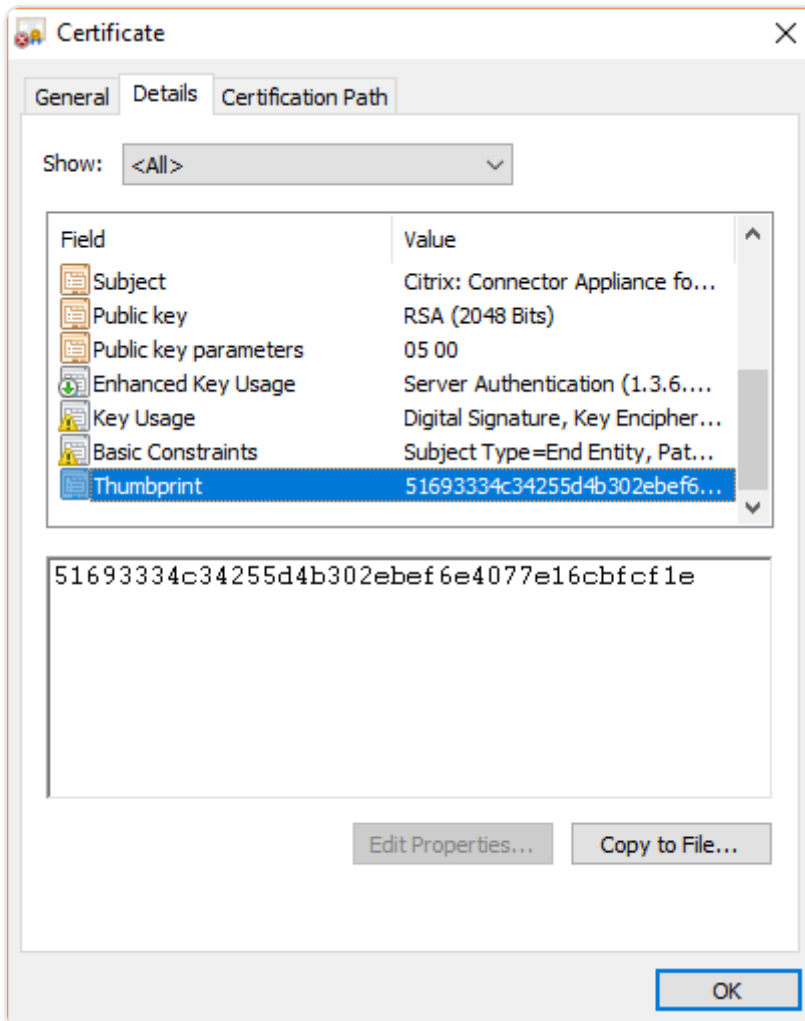
SSL Fingerprint: D5:0F:32:6D:57:4E:29:EF:41:65:62:0E:60:4B:4D:4F:C3:36:D0:B0
_
```

1. この形式で Connector Appliance の IP アドレスを入力します: `https://xx.xx.xx.xx/?deployment=productionjp` Connector Appliance UI は、5 年間有効な自己署名証明書を使用します。そのため、接続が安全でないというメッセージが表示される場合があります。Connector Appliance への接続を確認するには、コンソール内の SSL フィンガープリントと、ブラウザがウェブページから受信するフィンガープリントを比較できます。

たとえば、Google Chrome ブラウザで、次の手順を実行します。

- a. アドレスバーの横にある **安全ではありません** のマーカーをクリックします。
- b. **証明書** を選択します。証明書 ウィンドウが開きます。
- c. **詳細** タブに移動し、**サムプリント** フィールドを見つけます。

サムプリント フィールドの値と、コンソールに表示されている SSL フィンガープリントが一致する場合、ブラウザが Connector Appliance UI に直接接続していることを確認できます。



この自己署名証明書を、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。詳細については、「[証明書の管理](#)」を参照してください。

2. ブラウザがサイトへの続行を確認するための追加の手順を要求する場合は、今すぐこの手順を完了してください。

新しいパスワードの作成 ウェブページが開きます。

3. Connector Appliance UI のパスワードを作成し、**パスワードを設定**をクリックします。

新しいパスワードの作成ページ。(/en-us/citrix-cloud-japan/media/connector-appliance-pw-change-ui.png)

設定するパスワードは、次の要件を満たす必要があります。

- 8文字以上

- 大文字と小文字の両方を含む
- 少なくとも1つの非アルファベット文字を含む

このパスワードは、将来使用するために安全な場所に保管してください。

4. 設定したパスワードでサインインします。**コネクタ管理**ページが開きます。

プロキシサーバーセクションのあるコネクタ管理ページ(/en-us/citrix-cloud-japan/media/connector-appliance-register.png)

5. (オプション) 1つ以上のWebプロキシを使用している場合は、**プロキシサーバーセクション**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**を指定します。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プロキシを介してルーティングされます。詳細については、「[Connector Appliance communication](#)」を参照してください。

6. (オプション) ネットワークが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には、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、**証明書の追加**を選択します。
 - b. PEM形式の証明書の内容をコピーします。

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

- c. **Full Certificate Details**で、証明書の内容を貼り付けます。
- d. **Add Certificate**を選択します。

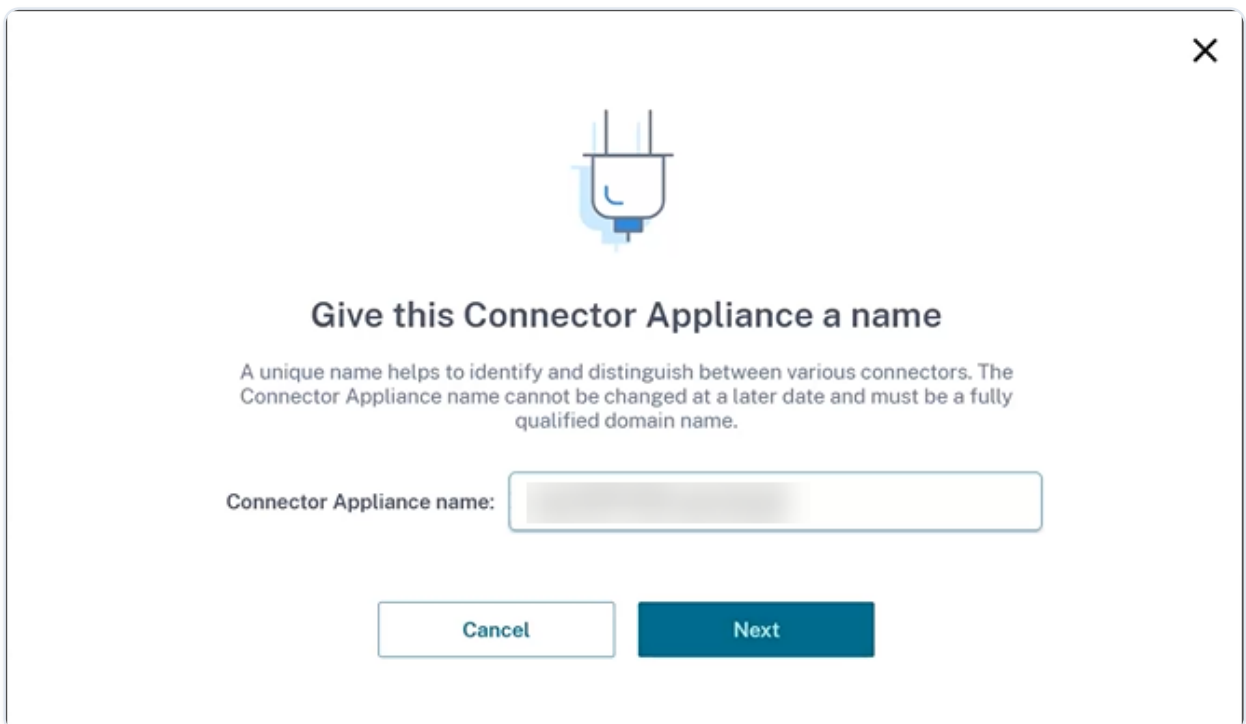
Connector Appliance APIを使用してRootCAを追加するには、Citrix Developerドキュメントの[ルート証明機関の管理](#)を参照してください。

注:

有効期限が切れている、または今後30日以内に有効期限が切れる証明書には警告が表示されます。

7. **Register Connector**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、名前は変更できません。

Connector Appliance nameフィールドに名前を入力し、**Next**をクリックします。

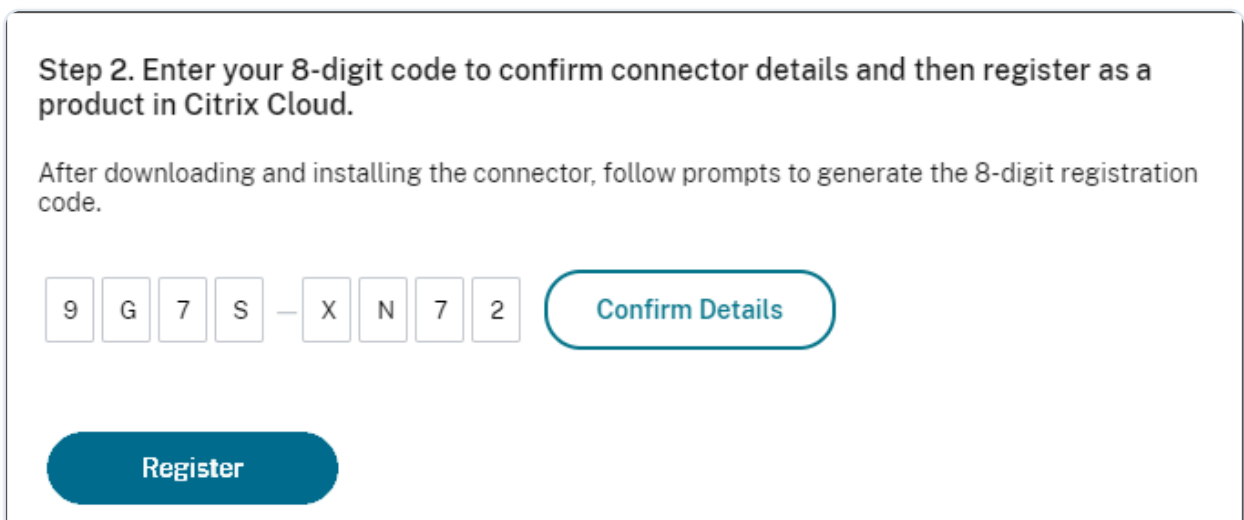


ウェブページには、Citrix Cloudに登録するために使用するコードが表示されます。このコードは15分で期限切れになります。



9. **Copy**ボタンを使用して、コードをクリップボードにコピーします。
10. **Resource Locations**ウェブページに戻ります。
11. **Install Connector Appliance**タスクの**Step 2**にコードを貼り付けます。 **Confirm Details**をクリックします。

Citrix Cloud は Connector Appliance が存在し、連絡可能であることを確認します。登録コードの有効期限が切れている場合は、新しいコードを生成するよう求められます。



12. **登録**をクリックします。

ページには登録が成功したかどうかが表示されます。登録に失敗した場合は、再試行するよう求められます。

13. 閉じるをクリックします。

Connector Appliance 管理ページでは、Connector Appliance の診断レポートをダウンロードすることもできます。詳細については、「[診断レポートの生成](#)」を参照してください。

セキュアクライアントを使用して Connector Appliance を登録することもできます。詳細については、「[Connector Appliance の無人登録](#)」を参照してください。 `deployment` には `productionjp` を入力します。

Connector Appliance の登録後

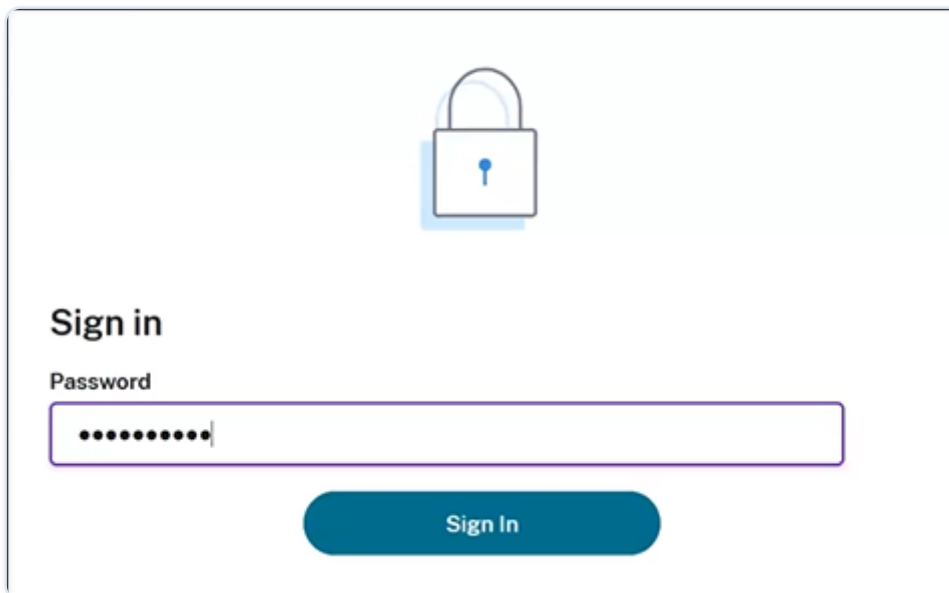
各リソースの場所には、2つ以上の Connector Appliance をインストールして登録することをお勧めします。この構成により、継続的な可用性が確保され、コネクタが負荷を分散できるようになります。

Connector Appliance を直接管理することはできません。

Connector Appliance は自動的に更新されます。コネクタを更新するために、お客様が何らかの操作を行う必要はありません。Connector Appliance の更新をリソースの場所に適用する日時を指定できます。

Connector Appliance VM のクローン作成、一時停止、またはスナップショットの取得は行わないでください。これらの操作はサポートされていません。

Connector Appliance UI に初めて接続するときのみ、**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、将来使用するために安全な場所に保管してください。このパスワードはリセットできません。パスワードを忘れた場合は、Connector Appliance を再インストールする必要があります。UI へのその後の接続では、Connector Appliance の登録時に設定したパスワードの入力を求められます。



Sign in

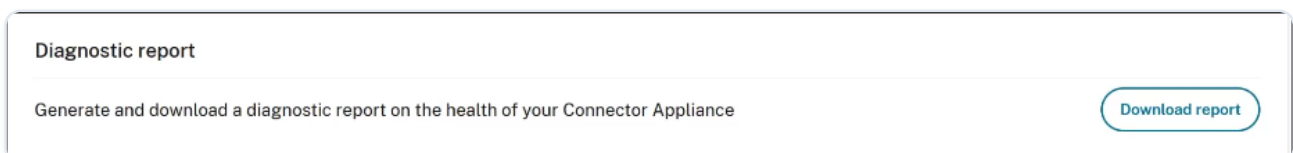
Password

.....

Sign In

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。



Diagnostic report

Generate and download a diagnostic report on the health of your Connector Appliance

Download report

1. ハイパーバイザーのConnector Applianceコンソールから、IPアドレスをブラウザーのアドレスバーにコピーします。
2. Connector Applianceを登録したときに設定したパスワードを入力します。
3. ページの**診断レポート**セクションで、**レポートのダウンロード**をクリックします。

診断レポートは `.zip` ファイルで提供されます。

ネットワーク接続を確認する

Connector Appliance管理ページから、**TCPキャプチャ**診断チェックを使用してネットワーク接続を確認できます。

1. **Connector Appliance**管理ページで、ヘッダーバーのアカウント名をクリックし、**ネットワーク診断**を選択します。
2. (オプション) **TCPキャプチャ**セクションで、TCPキャプチャを制限するターゲットIPアドレス、ホスト名、またはポートを入力します。
3. **トレース期間**メニューから、トレースを実行する期間を選択します。
4. (オプション) パケットの内容をキャプチャするには、**パケットトレース**を有効にします。

パケットトレースが無効になっている場合、TCPキャプチャ機能は、診断のためにヘッダーをキャプチャするためにベストエフォート型のアプローチを使用します。このベストエフォート型のアプローチでは、各パケットの最初の94バイトがキャプチャされます。ただし、ヘッダーは固定サイズではないため、このアプローチではヘッダーのすべてをキャプチャできない場合があります。

5. **トレースの開始**をクリックします。
6. トレースが完了するまで待ちます。トレースが完了したら、トレースレポートをダウンロードするか、新しいトレースを開始できます。
 - トレースレポートをダウンロードするには、「**ダウンロード**」をクリックします。トレースレポートは `.pcap` ファイルで提供されます。
 - 別のトレースを開始するには、「**新しいトレースを開始**」をクリックします。

Active DirectoryをCitrix Cloudに接続する

Connector Applianceを使用すると、Citrix Virtual Apps and Desktops™リソースを含まないフォレストにリソースの場所を接続できます。たとえば、Citrix Virtual Apps and Desktopsのお客様の場合、一部のフォレストはユーザー認証にのみ使用されます。

詳細については、[Connector ApplianceでのActive Directory](#)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、環境でDHCPが利用できない場合、または**Connector Appliance管理ページ**にアクセスできない場合は、Connector Applianceコンソールでネットワーク構成を直接設定できます。

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**ダイアログで、**独自のネットワーク設定を構成**を選択します。

3. IPアドレス、サブネットマスク、およびデフォルトゲートウェイを入力します。
4. 1つ以上のDNSサーバーを追加します。
5. 1つ以上の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は一時的に利用できなくなります。**Connector Appliance管理ページ**からログアウトされ、このページのURLが変更されます。新しいURLは、Connector Applianceコンソールで確認するか、ハイパーバイザーのネットワーク情報を参照することで見つけることができます。

ネットワーク構成を自動割り当て値を使用するように変更するには：

1. **コネクタの概要**セクションで、**ネットワーク設定の編集**を選択します。
2. **ネットワーク設定**ダイアログで、**IPアドレスを自動的に取得**を選択します。
3. **保存**をクリックします。

ネットワーク設定への変更を保存すると、Connector Applianceが再起動します。再起動中、Connector Applianceは一時的に利用できなくなります。**Connector Appliance管理ページ**からログアウトされ、このページのURLが変更されます。新しいURLは、Connector Applianceコンソールで確認するか、ハイパーバイザーのネットワーク情報を参照することで見つけることができます。

Connector Applianceコンソールを使用してネットワーク構成を設定する

デフォルトでは、Connector ApplianceのIPアドレスとネットワーク設定はDHCPを使用して自動的に割り当てられます。ただし、環境でDHCPが利用できない場合や、**Connector Appliance管理ページ**にアクセスできない場合は、Connector Applianceコンソールで直接ネットワーク構成を設定できます。

ネットワーク構成を設定するには：

1. ハイパーバイザーで、Connector Applianceを再起動します。
2. Connector Applianceの起動中に、コンソールで `Welcome to GRUB!` というメッセージが表示されるのを確認します。
3. このメッセージが表示されたら、**Esc**を押してGRUBメニューに入ります。
4. ブートパラメータを編集するには、**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。

```

GNU GRUB  version 2.04

setparams 'Root A'

    set root="(hd0,gpt3)"
    linux /boot/bzImage ro root=PARTUUID=708a030c-5ad2-429b-9fb5-fcc1fe\
098c20 quiet oops=panic console=tty0 console=ttyS0

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.

```

5. 必要なネットワーク構成を含めるように、`linux` で始まる行を編集します。

- DHCPネットワークを指定するには、行の末尾に `network=dhcp` を追加します。
- 静的ネットワークを指定するには、次のパラメータを行の末尾に追加します。

```

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

```

プレースホルダーの値を、ご使用の構成の値に置き換えます。

6. 新しい構成でConnector Applianceを起動するには、**Ctrl+X**を押します。

Connector Applianceの管理者ユーザーパスワードを変更する

1. コンソールの右上にあるユーザーメニューから、**Change password**を選択します。



パスワード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、新しいパスワードを入力して確認します。設定する新しいパスワードは、次の要件を満たす必要があります。

- 8文字以上
- 大文字と小文字の両方を含む

- 少なくとも1つの英字以外の文字を含む
- 現在のパスワードと同じであってはなりません

3. **パスワードの変更**を選択して、変更を保存します。

Citrix Cloud は自動的にサインアウトし、サインインページにリダイレクトします。

コネクタ アプライアンス を使用した Active Directory

Connector Appliance を使用すると、Citrix Virtual Apps and Desktops™ リソースを含まないフォレストにリソースの場所を接続できます。たとえば、Citrix Virtual Apps and Desktops の場合、一部のフォレストを持つお客様はユーザー認証にのみ使用されます。

Connector Appliance で複数ドメインの Active Directory を使用する場合、以下の制限が適用されます。

- VDA を含むフォレストでは、Cloud Connector の代わりに Connector Appliance を使用することはできません。

要件

Active Directory の要件

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

ネットワーク要件

- リソースの場所で使用するリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「[システムおよび接続要件](#)」を参照してください。

(/ja-jp/citrix-cloud-japan/install-configure/connector-appliance.html#connector-appliance-communication)に記載されているポートに加えて、Connector Appliance は、これらのポートを介して Active Directory ドメインへのアウトバウンド接続を必要とします。

サービス	ポート	サポートされているドメインプロトコル
ケルベロス	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 名サービス	137	UDP
NetBIOS データグラム	138	UDP
NetBIOSセッション	139	TCP
LDAP	389	TCP/UDP
TCP経由のSMB	445	TCP
ケルベロス kpasswd	464	TCP/UDP
グローバルカタログ	3268	TCP
動的RPCポート	49152–65535	TCP

Connector Appliance は、ドメインコントローラーへの接続を保護するために LDAP 署名を使用します。これは、LDAP over SSL (LDAPS) が不要であることを意味します。LDAP 署名の詳細については、「[Windows Server で LDAP 署名を有効にする方法](#)」および「[LDAP チャネルバインディングと LDAP 署名を有効にするための Microsoft ガイダンス](#)」を参照してください。

サポートされている Active Directory の機能レベル

Connector Appliance は、Active Directory の以下のフォレストおよびドメイン機能レベルでテストされ、サポートされています。

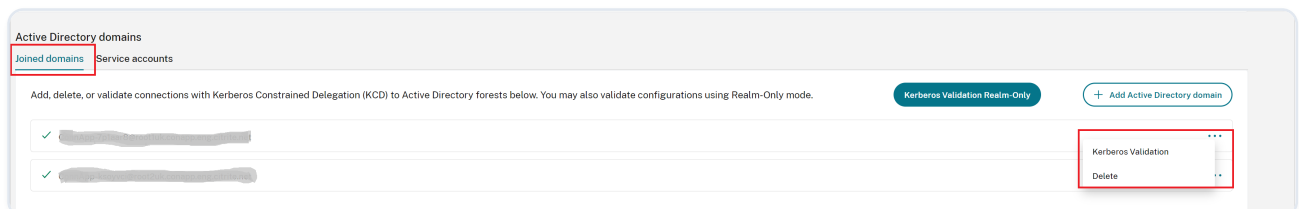
フォレストの機能レベル	ドメインの機能レベル	サポートされているドメインコントローラー
ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2019

ドメインコントローラー、フォレストの機能レベル、およびドメインの機能レベルのその他の組み合わせは、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機能すると予想され、サポートもされています。

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

Connector Applianceの管理Webページに接続すると、「Active Directory domains」セクションに2つのタブが表示されます。

- **参加済みドメイン** – Connector Applianceのドメインにマシンアカウントを作成して、Connector ApplianceをADドメインに参加させるために使用します。Kerberosは、参加済みドメインの右側にある省略記号メニューをクリックして検証できます。ドメイン内にマシンアカウントが存在している必要があります。



Connector Applianceを介してActive DirectoryをCitrix Cloudに接続するように構成するには、次の手順を実行します。

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

[Connector Appliance製品ドキュメント](#)の情報を参照してください。

2. Connector Applianceコンソールに表示されているIPアドレスを使用して、ブラウザでConnector Appliance管理Webページに接続します。
3. **Active Directory domains**セクションで、**Joined domains**タブに移動します。
4. **+ Add Active Directory domain**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がドメインをチェックします。チェックが成功すると、**Join Active Directory**ダイアログが開きます。この新しいウィンドウで、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. **Add**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はマシン名を提案します。提案された名前を上書きして、最大15文字の独自のマシン名を入力することもできます。

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

8. **Join**をクリックします。

ドメインは、Connector Appliance UI の **Active Directory domains** セクションに表示されるようになりました。

9. さらに **Active Directory domains** を追加するには、**+ Add Active Directory domain** を選択し、前の手順を繰り返します。
10. **Citrix Cloud Console** のドメインページに移動し、ドメインをサービスするために **Connector Appliance** を選択します。
11. Connector Appliance をまだ登録していない場合は、[Register your Connector Appliance with Citrix Cloud](#) に記載されている手順を続行してください。

注

ドメインへの参加中にエラーが発生した場合は、お使いの環境が必要な [Active Directory requirements](#) および [network requirements](#) を満たしていることを確認してください。

次のステップ

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

注:

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

- 復元性を高めるため、各リソースの場所で、各ドメインを複数の Connector Appliance に追加します。

Active Directory 構成の表示

リソースの場所にある Active Directory ドメインと Connector Appliance の構成は、次の場所で表示できます。

- シトリックス クラウドで:
 - a. メニューで、**Identity and access management** ページに移動します。
 - b. 「ドメイン」タブに移動します。

Active Directory ドメインは、所属するリソースの場所とともに一覧表示されます。

- Connector Appliance のWebページで:
 - a. Connector Appliance コンソールに表示されているIPアドレスを使用して、Connector Appliance のWebページに接続します。
 - b. 初めて登録したときに作成したパスワードでログインします。
 - c. ページの「**Active Directory ドメイン**」セクションで、このConnector Applianceが参加しているActive Directory ドメインのリストを確認できます。

Connector Appliance からActive Directory ドメインを削除する

Active Directory ドメインから離脱するには、次の手順を実行します。

1. Connector Appliance コンソールに表示されているIPアドレスを使用して、Connector Appliance のWebページに接続します。
2. 初めて登録したときに作成したパスワードでログインします。
3. ページの「**Active Directory ドメイン**」セクションで、参加しているActive Directory ドメインのリストから離脱したいドメインを見つけます。
4. Connector Appliance によって作成されたマシンアカウントの名前をメモします。
5. ドメインの横にある削除アイコン（ゴミ箱）をクリックします。確認ダイアログが表示されます。
6. アクションを確定するには、** [続行] **をクリックします。
7. Active Directory コントローラーに移動します。
8. 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ーから削除します。

Active DirectoryでConnector Applianceを使用するための展開シナリオ

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

以下の状況で、Connector Applianceを使用してリソースの場所をActive Directoryフォレストに接続します。

- ユーザー認証のみに使用される1つ以上のフォレストがある場合
- 複数のフォレストをサポートするために必要なコネクタの数を減らしたい場合
- 他のユースケースでConnector Applianceが必要な場合

すべてのフォレストに対して単一のConnector Applianceセットを持つ1つ以上のフォレスト内のユーザーのみ

このシナリオは、Workspace Standardのお客様、またはSecure Private AccessにConnector Applianceを使用しているお客様に適用されます。

このシナリオでは、ユーザーオブジェクトのみを含む複数のフォレスト（`forest1.local`、`forest2.local`）があります。これらのフォレストにはリソースは含まれていません。1セットのConnector Applianceがリソースの場所に展開され、これらの各フォレストのドメインに参加しています。

- 信頼関係: なし
- **Identity and Access Management**にリストされているドメイン: `forest1.local`、`forest2.local`
- Citrix Workspace™へのユーザーログオン: すべてのユーザーでサポート
- オンプレミスのStoreFront™へのユーザーログオン: すべてのユーザーでサポート

すべてのフォレストに対して単一のConnector Applianceセットを持つ、個別のフォレスト（信頼関係あり）内のユーザーとリソース

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

このシナリオでは、一部のフォレスト（`resourceforest1.local`、`resourceforest2.local`）にリソース（VDAなど）が含まれ、一部のフォレスト（`userforest1.local`、`userforest2.local`）にはユーザーのみが含まれます。これらのフォレスト間には、ユーザーがリソースにログオンできるようにする信頼関係が存在します。

`resourceforest1.local` フォレスト内に1セットのCloud Connectorが展開されます。

`resourceforest2.local` フォレスト内には別のCloud Connectorセットが展開されます。

`userforest1.local` フォレスト内に1セットのConnector Applianceが展開され、同じセットが
`userforest2.local` フォレスト内にも展開されます。

- 信頼関係: 双方向フォレスト信頼、またはリソースフォレストからユーザーフォレストへの単方向信頼
- IDおよびアクセス管理にリストされているドメイン: `resourceforest1.local` , `resourceforest2.local` , `userforest1.local` , `userforest2.local`
- Citrix Workspaceへのユーザーログオン: すべてのユーザーでサポート
- オンプレミスStoreFrontへのユーザーログオン: すべてのユーザーでサポート

ワークスペースのセットアップ

Citrix Workspaceは、エンドユーザーがいつでも、どこからでも、あらゆるデバイスで作業を完了できるようにする、完全なデジタルワークスペースソリューションです。ユーザーは、WebブラウザーまたはデバイスにインストールされているWorkspaceアプリを介してCitrix Workspaceにサインインします。サインイン後、ユーザーは使用を許可されているアプリケーションとデスクトップにアクセスできます。

ワークスペースの機能

- Citrix Federated Authentication Serviceを介したシングルサインオンを有効にします。
- 組織のリソースの適切な使用方法を説明するサインインポリシーをエンドユーザー向けに作成します。
- ネットワークロケーションを使用して、社内ユーザーがワークスペースリソースにすばやく接続できるようにし、Citrix Gatewayを介してワークスペースにルーティングされるようにします。
- エンドユーザーがCitrix Workspaceを離れることなく、必要に応じてドメインパスワードを変更できるようにします。
- サイト集約を使用して、StoreFrontではなくCitrix Workspaceを介してオンプレミスのVirtual Apps and Desktops展開のリソースへのアクセスを提供します。
- クラウドサービスの停止が発生した場合でも、エンドユーザーがワークスペースリソースにアクセスできるように、サービス継続性を有効にします。

詳細情報

- Citrix Cloud Japan向けWorkspaceの相違点: [サービスで利用可能な機能](#)

- シングルサインオン: Citrix Federated Authentication Serviceを使用したワークスペースのシングルサインオンを有効にする
- ネットワークロケーション: Direct Workload Connectionを使用したワークスペースへの接続の最適化
- サイト集約: ワークスペースでのオンプレミス仮想アプリとデスクトップの集約
- サービス継続性
- ドメインパスワードの変更: サブスクライバーがアカウントパスワードを変更できるようにする
- サインインポリシー: サインインポリシーを構成する

ワークスペースを構成する

Citrix DaaS展開のセットアップ後、次のタスクを実行してワークスペースを構成します。

1. Citrix Workspaceとのサービス統合を有効にします。Citrix DaaSのサービス統合は、以前の名称であるVirtual Apps and Desktopsのままになっている場合があります。Citrix Workspaceのドキュメントの[ワークスペースへのサービス統合](#)を参照してください。
2. **Workspace Configuration > Authentication**で、以前に構成したIDプロバイダーを、エンドユーザーの優先ワークスペース認証方法として選択します。
3. オンプレミスのCitrix GatewayまたはCitrix Gatewayサービスを介して、リモートエンドユーザー向けに[ワークスペースへのセキュアなアクセス](#)を構成します。
4. シングルサインオンやサービス継続性などのワークスペース機能を構成します。

ワークスペースをカスタマイズする

1. ワークスペースの[デフォルトテーマ](#)をカスタマイズします。
2. エンドユーザーがアクセスする[ワークスペースURL](#)をカスタマイズします。
3. エンドユーザーのワークスペースでお気に入りの[アプリとデスクトップ](#)がどのように表示されるかをカスタマイズします。
4. WebブラウザーまたはWorkspaceアプリを介してワークスペースにアクセスするエンドユーザー向けに[非アクティブタイムアウト](#)を構成します。
5. Citrix DaaS展開を通じて提供するアプリとデスクトップを、エンドユーザーがどのように起動するかをカスタマイズします。

ID およびアクセス管理

IDプロバイダーは以下の目的で使用されます。

- Citrix Cloud Japanにサインインする際に管理者を認証する
- ワークスペースサブスクライバーにライブラリの提供物を割り当てるためのユーザーリストへのアクセスを提供する
- Citrix Workspace™アプリを介してサインインする際にワークスペースサブスクライバーを認証する。

Citrix Cloud Japanは以下のIDプロバイダーをサポートしています。これらのIDプロバイダーは、Citrix Cloud管理者、ワークスペースサブスクライバー、またはその両方を認証するために使用できます。

IDプロバイダー	管理者認証	サブスクライバー認証
Citrix® IDプロバイダー (デフォルト)	はい	いいえ
オンプレミスActive Directory (AD)	いいえ	はい
マイクロソフト エントラ アイディー	はい	はい
オンプレミス Citrix Gateway	いいえ	はい
オクタ	いいえ	はい
SAML 2.0	はい (ADグループのみ - プレビュー)	はい

管理者認証

デフォルトでは、Citrix Cloud Japan は、管理者がサインインする際に、組み込みのCitrix IDプロバイダーを使用して認証します。あるいは、Microsoft Entra ID をIDプロバイダーとして接続し、

Citrix Cloud Japan の管理者を認証することもできます。また、SAML 2.0 を使用して、AD内の管理者グループを認証することも可能です。

管理者認証に Microsoft Entra ID または SAML 2.0 を使用する場合、管理者は一意のURLを使用してCitrix Cloud Japan にサインインできます。サインインするには、管理者はCitrix Cloud Japan アカウントの識別子を入力します。

注記:

管理者認証にMicrosoft Entra IDを使用している場合、Citrixは、以下のことを確実にするために、Citrix IDプロバイダーの下に少なくとも1つのフルアクセスアカウントを維持することを推奨します。

- 代替のIDプロバイダーを設定する前にMicrosoft Entra IDが切断された場合でも、Citrix Cloud Japanアカウントからロックアウトされることはありません。
- Microsoft Entra IDを介して管理者としてサインインしているときに完了できない特定の操作を実行するために、Citrix Cloud Japanアカウントにアクセスできます。たとえば、CitrixがMicrosoft Entra IDに接続するMicrosoft Entra IDアプリケーションを更新した場合、Citrix Cloud Japanアカウントでも更新されていることを確認してください。この更新を実行できるのは、Citrix IDプロバイダーの下のフルアクセス管理者のみです。

ワークスペース認証

Citrix IDプロバイダーを除き、Citrix Workspaceアプリを介してサインインするワークスペースサブスクリバラーの認証には、サポートされているすべてのIDプロバイダーを使用できます。

IDプロバイダーの前提条件

Citrix Cloud Japanと連携する前に、以下のサポートされているIDプロバイダーについては、オンプレミス環境にCitrix Cloud Connector™をインストールする必要があります。

- アクティブディレクトリ
- オンプレミスCitrix Gateway
- オクタ
- SAML 2.0

サポートされている各IDプロバイダーの前提条件の詳細については、この記事の[詳細情報](#)の項目を参照してください。

ユーザーへのアプリケーションおよびデスクトップの配信

Citrix DaaS™を使用する場合、以下のいずれかの方法で、ADまたはMicrosoft Entra IDのユーザーとグループをリソースに割り当てます。

- Studioで、目的のアプリケーションとデスクトップで構成されるデリバリーグループを作成し、アクセスを許可するADのユーザーを指定します。
- Studioで、配信する目的のアプリケーションとデスクトップを含むデリバリーグループを作成し、それをライブラリで提供します。次に、ライブラリを使用して、デリバリーグループ内のリソースへのアクセスを許可されているADまたはMicrosoft Entra IDのユーザーを選択します。この方法では、ADまたはMicrosoft Entra IDをCitrix Cloud JapanにIDプロバイダーとして接続する必要があります。

詳細情報

IDプロバイダーをCitrix Cloud Japanに接続する手順については、以下の記事を参照してください。

- [IDプロバイダーとしてActive Directoryを接続する](#)
- [IDプロバイダーとしてMicrosoft Entra IDを接続する](#)
- [IDプロバイダーとしてオンプレミスのCitrix Gatewayを接続する](#)
- [IDプロバイダーとしてOktaを接続する](#)
- [IDプロバイダーとしてSAMLを接続する](#)

Active Directory を Citrix Cloud Japan に接続する

デフォルトでは、Citrix Cloud Japan は Citrix Identity プロバイダーを使用して、Citrix Cloud Japan アカウント内のすべてのユーザーの ID 情報を管理します。これを Active Directory (AD) を使用するように変更できます。

オンプレミスの Active Directory を Citrix Cloud Japan に接続するには、ドメインに Cloud Connector をインストールする必要があります。Citrix では、高可用性のために 2 つの Cloud Connector をインストールすることをお勧めします。要件と手順については、「[Citrix Cloud Connector の要件](#)」を参照してください。

Active Directory を Citrix Cloud Japan に接続するには

1. Citrix Cloud メニューから、**【ID およびアクセス管理】** を選択します。
2. **【認証】** タブの **【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に従います。
5. **【Active Directory に接続】** ページで、**【検出】** をクリックします。検証後、Citrix Cloud に Active Directory が接続されたことを示すメッセージが表示されます。
6. **【認証に戻る】** をクリックします。**【認証】** タブで、**【Active Directory】** エントリが **【有効】** とマークされます。

ワークスペースの AD 認証を有効にする

AD を Citrix Cloud Japan に接続した後、サブスクライバーが AD を介してワークスペースに認証できるようにすることができます。

1. Citrix Cloud Japan 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】** タブから、**【Active Directory】** を選択します。
3. **【確認】** をクリックして、Microsoft Entra ID 認証が有効になったときに発生するワークスペースエクスペリエンスの変更を受け入れます。

Microsoft Entra ID を ID プロバイダーとして接続する

デフォルトでは、Citrix Cloud Japan は Citrix ID プロバイダーを使用して、Citrix Cloud Japan アカウント内のすべてのユーザーの ID 情報を管理します。これを変更して、Microsoft Entra ID を使用して Citrix Cloud Japan 管理者とワークスペースサブスクライバーを認証できます。

Citrix Cloud Japan で Microsoft Entra ID を使用すると、次のことができます。

- 独自の Active Directory を使用して、監査、パスワードポリシーを制御し、必要に応じてアカウントを簡単に無効にできます。
- 盗まれたサインイン資格情報の可能性に対するセキュリティレベルを向上させるために、多要素認証を構成します。
- ブランド化されたサインインページを使用して、ユーザーが正しい場所でサインインしていることを認識できるようにします。

- ADFS、Okta、Ping など、選択した ID プロバイダーへのフェデレーションを使用します。

Microsoft Entra ID アプリケーションとアクセス許可

Citrix Cloud Japan には Microsoft Entra ID アプリが含まれており、アクティブな Microsoft Entra ID セッションにログインしていなくても、Citrix Cloud Japan が Microsoft Entra ID に接続できます。Citrix Cloud Japan が Microsoft Entra ID に接続するために使用する Microsoft Entra ID アプリケーションとアクセス許可の詳細については、「[Citrix Cloud Japan の Microsoft Entra ID アクセス許可](#)」を参照してください。

Active Directory と Microsoft Entra ID を準備する

Microsoft Entra ID 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こと。すべての Azure アカウントには、Microsoft Entra ID が無料で付属しています。Azure アカウントをお持ちでない場合は、<https://azure.microsoft.com/ja-jp/free/?v=17.36> でサインアップしてください。
- Microsoft Entra ID でグローバル管理者ロールを持っていること。このロールは、Citrix Cloud Japan が Microsoft Entra ID に接続するための同意を与えるために必要です。
- 管理者アカウントの「メール」プロパティが Microsoft Entra ID で構成されていること。これを行うには、Microsoft の [Microsoft Entra ID Connect](#) ツールを使用して、オンプレミスの Active Directory から Microsoft Entra ID にアカウントを同期できます。または、同期されていない Microsoft Entra ID アカウントを Office 365 メールで構成することもできます。

Microsoft Entra ID Connect とアカウントを同期する

1. Active Directory アカウントにメールユーザープロパティが構成されていることを確認してください。
 - a. Active Directory ユーザーとコンピューターを開きます。
 - b. ユーザーフォルダーで、確認したいアカウントを見つけ、右クリックしてプロパティを選択します。全般タブで、メールフィールドに有効なエントリがあることを確認します。
Citrix Cloud Japan では、Microsoft Entra ID から追加された管理者は、Citrix ホスト型 ID を使用してサインインする管理者とは異なるメールアドレスを持つ必要があります。
2. Microsoft Entra ID Connect をインストールして構成します。詳細な手順については、Microsoft Azure の Web サイトで「[オンプレミスディレクトリを Microsoft Entra ID と統合する](#)」を参照してください。

Citrix Cloud JapanをMicrosoft Entra IDに接続する

Citrix Cloud JapanアカウントをMicrosoft Entra IDに接続する際、Citrix Cloud Japanは、お客様のユーザープロファイル（またはサインインしているユーザーのプロファイル）と、Microsoft Entra ID内のユーザーの基本プロファイルにアクセスする許可を必要とします。Citrixがこの許可を要求するのは、お客様の名前とメールアドレス（管理者として）を取得し、後で他のユーザーを検索して管理者として追加できるようにするためです。

1. <https://citrix.citrixcloud.jp>でCitrix Cloud Japanにサインインします。
2. ページの左上隅にある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。
3. **Microsoft Entra ID**を見つけ、省略記号ボタンをクリックし、**接続**を選択します。
4. プロンプトが表示されたら、会社用の短くURLフレンドリーな識別子を入力し、**接続**をクリックします。選択する識別子は、Citrix Cloud Japan内でグローバルに一意である必要があります。
5. プロンプトが表示されたら、接続したいAzureアカウントにサインインします。Azureは、Citrix Cloud Japanがアカウントにアクセスし、接続に必要な情報を取得するために必要な権限を表示します。
6. **承認**をクリックして、権限要求を承認します。

Microsoft Entra IDからCitrix Cloud Japanに管理者を追加する

1. Citrix Cloud Japan管理コンソールの**IDおよびアクセス管理**ページから、**管理者タブ**をクリックします。
2. **管理者/グループの追加**を選択します。
3. 「**管理者詳細**」で、「**Microsoft Entra ID**」を選択します。
4. 追加するユーザーの名前を入力し、「**次へ**」をクリックします。Microsoft Entra IDゲストユーザーの招待はサポートされていません。
5. 「**アクセス設定**」で、管理者に対して適切な権限を構成します。
6. 管理者詳細を確認します。変更を加えるには、「**戻る**」を選択します。
7. 「**招待を送信**」を選択します。Citrix Cloud Japanは、指定したユーザーに招待を送信し、管理者をリストに追加します。

メールリンクをクリックすると、ユーザーは会社のMicrosoft Entra IDにサインインします。これにより、ユーザーのメールアドレスが検証され、Microsoft Entra IDユーザーアカウントとCitrix Cloud Japan間の接続が完了します。

Microsoft Entra ID管理者グループをCitrix Cloud Japanに追加する

Microsoft Entra IDグループを使用して、Citrix Cloud Japan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に対してサービスアクセス権限を管理できます。

この機能は、**Citrix DaaS™**（旧Virtual Apps and Desktopsサービス）でのみサポートされています。グループ内の管理者は、Citrix Cloud Japanアカウント内の他のサービスを管理するアクセス権を持ちません。

詳細については、「[管理者グループの管理](#)」を参照してください。

Microsoft Entra IDを使用してCitrix Cloud Japanにサインインする

Microsoft Entra IDユーザーアカウントが接続された後、管理者は次のいずれかの方法でCitrix Cloud Japanにサインインできます。

- 会社のMicrosoft Entra ID IDプロバイダーを最初に接続したときに構成した管理者サインインURLに移動します。例: `https://citrix.citrixcloud.jp/go/myorganization`
- Citrix Cloud Japanのサインインページから、「**会社の資格情報でサインイン**」をクリックし、Microsoft Entra IDを最初に接続したときに作成した識別子を入力して、「**続行**」をクリックします。

ワークスペースのMicrosoft Entra ID認証を有効にする

Microsoft Entra IDをCitrix Cloud Japanに接続すると、サブスクライバーがMicrosoft Entra IDを介してワークスペースに認証できるようになります。

重要:

Microsoft Entra IDワークスペース認証を有効にする前に、Citrix WorkspaceでMicrosoft Entra IDを使用する際の考慮事項について、[Microsoft Entra ID](#)セクションを確認してください。

1. 左上隅にあるCitrix Cloud Japanメニューから、**Workspace Configuration**を選択します。
2. **Authentication**タブを選択し、**Microsoft Entra ID**を選択します。
3. **Confirm**をクリックして、Microsoft Entra ID認証が有効になったときに発生するワークスペースエクスペリエンスの変更を受け入れます。

高度なMicrosoft Entra ID機能を有効にする

Microsoft Entra IDは、高度な多要素認証、世界クラスのセキュリティ機能、20種類のIDプロバイダーへのフェデレーション、セルフサービスパスワード変更とリセットなど、多くの機能を提供します。これらの機能をMicrosoft Entra IDユーザーに対して有効にすると、Citrix Cloud Japanはそれらの機能を自動的に使用できるようになります。

更新されたアプリのためにMicrosoft Entra IDに再接続する

2022年4月、Citrix Cloud Japanで使用されているMicrosoft Entra IDアプリが更新され、Group.Read.All権限に代わってGroupMember.Read.All権限を使用するようになりました。

2022年4月より前にMicrosoft Entra IDをCitrix Cloud Japanに接続しており、最新の更新されたアプリを使用したい場合は、Microsoft Entra IDをCitrix Cloud Japanから切断し、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

Microsoft Entra IDを再接続する前に、以下の要件を満たしていることを確認してください。

- Microsoft Entra IDのグローバル管理者である必要があります。Microsoft Entra IDを再接続する際、Microsoft Entra IDのグローバル管理者ロールを通じてCitrix Cloud Japanにアプリケーションレベルの権限を付与します。これにより、Citrix Cloud Japanはユーザーに代わってMicrosoft Entra IDに再接続できます。詳細については、「[Citrix Cloud JapanのMicrosoft Entra ID権限](#)」を参照してください。
- デフォルトのCitrix IDプロバイダーの下で、フルアクセス権限を持つ管理者である必要があります。Microsoft Entra IDの資格情報でCitrix Cloud Japanにサインインしている場合、再接続は失敗します。アカウントにCitrix IDプロバイダーを使用している管理者がいない場合は、一時的に管理者を追加し、Microsoft Entra IDの再接続後に削除できます。手順については、「[個々の管理者を招待する](#)」を参照してください。
- ワークスペースサブスクリバラーの認証にMicrosoft Entra IDを使用している場合は、一時的に別のIDプロバイダーを選択してください。Citrix Workspaceの認証方法としても使用されている場合、Citrix Cloud JapanではMicrosoft Entra IDを切断することはできません。詳細については、Citrix Workspaceのドキュメントにある「[認証方法の選択または変更](#)」を参照してください。

Microsoft Entra IDを再接続するには

1. Citrix IDプロバイダーで、完全なアクセス権限を持つ管理者としてCitrix Cloud Japanにサインインします。

2. Citrix Cloud Japanメニューから、 を選択し、次に を選択します。
3. を見つけ、ページの右端にある省略記号メニューから を選択します。
4. 省略記号メニューから を選択します。
5. プロンプトが表示されたら、グローバル管理者資格情報を使用してAzureアカウントにサインインします。Azureは、Citrix Cloud Japanがアカウントにアクセスし、接続に必要な情報を取得するために必要な権限を表示します。
6. 権限要求を承認するには、 を選択します。

Citrix Cloud™ Japan の Microsoft Entra ID アクセス許可

この記事では、Citrix Cloud Japan が Microsoft Entra ID (AD) に接続して使用する際に要求するアクセス許可について説明します。Citrix Cloud Japan アカウントで Microsoft Entra ID をどのように使用するかにによって、ターゲットの Microsoft Entra ID テナントに 1 つ以上のエンタープライズアプリケーションが作成される場合があります。複数の Citrix Cloud Japan アカウントを 1 つの Microsoft Entra ID テナントに接続し、アカウントごとにアプリケーションのセットを作成することなく、同じエンタープライズアプリケーションを使用できます。

注記:

2022 年 4 月現在、Citrix Cloud Japan が Microsoft Entra ID への接続に使用する Microsoft Entra ID アプリは、Group.Read.All アクセス許可の代わりに GroupMember.Read.All アクセス許可を使用するように更新されました。既存の Microsoft Entra ID 接続 (2022 年 4 月以前) があり、アプリに新しいアクセス許可を使用させたい場合は、Microsoft Entra ID を Citrix Cloud Japan から切断し、再接続する必要があります。この操作により、アカウントが Citrix Cloud Japan で最新の Microsoft Entra ID アプリを使用していることが保証されます。詳細については、「[更新されたアプリのために Microsoft Entra ID に再接続する](#)」を参照してください。

アプリを更新しないことを選択した場合でも、既存の接続は引き続き正常に機能します。

エンタープライズアプリケーション

次の表に、Citrix Cloud Japan が Microsoft Entra ID に接続して使用する際に利用する Microsoft Entra ID エンタープライズアプリケーションと、各アプリケーションの使用目的を示します。

名前	アプリケーション ID	用途
シトリックス クラウド プロダクションJP	f751768a-a91d-4306-af65-448ab59e2c85	Workspace サブスクライバー ログイン
CC-Directory-プロダクション JP	6550e1c7-8970-46bc-82b6-ebd920ff255d	Microsoft Entra ID と Citrix Cloud Japan 間の既定の接続 (#default-connection-between-azure-ad-and-citrix-cloud-japan)
アテナ プロダクションJP	6464247d-8d40-42b9-a75e-4660db847454	管理者への招待およびログイン(#administrator-invitations-and-logins)

アクセス許可

Citrix Cloud Japan のエンタープライズアプリケーションにおけるアクセス許可により、Citrix Cloud Japan はお客様の Microsoft Entra ID テナント内の特定のデータにアクセスできます。Citrix Cloud Japan はこれらのデータを使用して、Microsoft Entra ID テナントへの接続や、専用のサインイン URL を使用して管理者が Citrix Cloud Japan にサインインできるようにするなど、特定の機能を実行します。Citrix Cloud Japan は、お客様の同意がある場合にのみこれらのデータにアクセスできます。これらのアクセス許可は、Citrix Cloud Japan がお客様の Microsoft Entra ID と連携するために必要な最小限の特権を表します。Microsoft Entra ID のアクセス許可と同意の詳細については、Microsoft Azure ドキュメント Web サイトの「[Microsoft ID プラットフォームのアクセス許可と同意](#)」を参照してください。

この記事では、Microsoft Entra ID アプリケーションの各アクセス許可セットには以下の情報が含まれています。

- **API 名:** Citrix Cloud Japan がアクセス許可を要求するリソースアプリケーション。これらのアプリケーションは Microsoft Graph と Windows Microsoft Entra ID です。Citrix Cloud Japan は、これら両方のリソースアプリケーションから同じアクセス許可を要求します。
- **種類:** Citrix Cloud Japan が特定のアクセス許可に対して要求するアクセスレベル。特定のエンタープライズアプリケーションのアクセス許可には、次のいずれかのアクセスレベルがあります。
 - **委任されたアクセス許可**は、サインインしているユーザーに代わって動作するために使用されます。たとえば、ユーザーのプロファイルを照会する場合などです。

- **アプリケーションのアクセス許可**は、アプリケーションがユーザーの存在なしにアクションを実行する場合に使用されます。たとえば、特定のグループ内のユーザーを照会する場合などです。このアクセス許可の種類には、Microsoft Entra ID のグローバル管理者による同意が必要です。
- **要求値:** Microsoft Entra ID が特定のアクセス許可に割り当てる情報文字列。特定のエンタープライズアプリケーションのアクセス許可には、次のいずれかの要求値があります。
 - **User.Read:** Citrix Cloud Japan の管理者が、接続されている Microsoft Entra ID からユーザーを Citrix Cloud Japan 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、アクセス許可自体は下位互換性のために残されています。
 - **User.Read.All:** Citrix Cloud Japan は、Microsoft Graph の [ユーザーの一覧表示](#) を呼び出して、顧客の接続済み Microsoft Entra ID からユーザーの参照と選択を可能にします。たとえば、Microsoft Entra ID のユーザーには、ワークスペースで Citrix DaaS リソースへのアクセス権を付与できます。Citrix Cloud Japan は、基本プロファイル以外のプロパティ (`onPremisesSecurityIdentifier` など) にアクセスする必要があるため、`User.ReadBasic.All` を使用できません。
 - **GroupMember.Read.All:** Citrix Cloud Japan は、顧客が接続している Microsoft Entra ID からグループの参照と選択を可能にするために、Microsoft Graph の [List groups](#) を呼び出します。たとえば、Microsoft Entra ID のグループには、Citrix DaaS アプリケーションへのアクセスも許可できます。

Workspace サブスクリャーのログイン

Citrix Cloud ProductionJP アプリケーション (ID: f751768a-a91d-4306-af65-448ab59e2c85) は、Microsoft Graph と Windows Microsoft Entra ID リソース アプリケーションの両方で同じ権限を使用します。

API名	クレーム値	権限名	種類
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
ウィンドウズ マイクロソフト Entra ID	User.Read	サインインしてユーザープロファイルを読み取る	委任

Microsoft Entra ID と Citrix Cloud™ Japan 間の既定の接続

CC-Directory-ProductionJP アプリケーション (ID: 6550e1c7-8970-46bc-82b6-ebd920ff255d) は次のアクセス許可を使用します:

API 名	要求値	アクセス許可	種類
マイクロソフトグラフ	GroupMember.Read.All	すべてのグループを読み取る	委任
マイクロソフトグラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任
マイクロソフトグラフ	User.Read.All	すべてのユーザーの完全なプロファイルを読み取る	委任
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフト グラフ	GroupMember.Read.All	すべてのグループを読み取る	アプリケーション
マイクロソフト グラフ	User.Read.All	すべてのユーザーの完全なプロファイルを読み取る	アプリケーション

管理者への招待とログイン

Athena ProductionJP アプリケーション (ID: 6464247d-8d40-42b9-a75e-4660db847454) は、次の権限を使用します。

API名	クレーム値	権限名	タイプ
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任
マイクロソフト グラフ	User.ReadBasic.All	すべてのユーザーの基本プロファイルを読み取る	委任

オンプレミスのCitrix GatewayをIDプロバイダーとして接続する

Citrix Cloud™ Japanは、オンプレミスのCitrix GatewayをIDプロバイダーとして使用し、ワークスペースにサインインするサブスクライバーを認証することをサポートしています。

Citrix Gateway認証を使用すると、次のことが可能になります。

- 既存のCitrix Gatewayを介してユーザー認証を継続し、オンプレミスのVirtual Apps and Desktops展開内のリソースにCitrix Workspace経由でアクセスできるようにします。
- Citrix WorkspaceでCitrix Gatewayの[認証、承認、および監査 \(AAA\) 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、フェデレーションなど、さまざまな機能を使用しながら、Citrix Workspaceを介してユーザーが必要なリソースにアクセスできるようにします。

ヒント:

サポートされているIDプロバイダーの詳細については、[Citrix Identity and Authenticationの概要教育コース](#)をご覧ください。「Citrix Identity and Access Managementの計画」モジュールには、このIDプロバイダーをCitrix Cloud Japanに接続し、Citrix Workspaceの認証を有効にする方法を説明する短いビデオが含まれています。

サポートされているバージョン

Citrix Gateway認証は、以下のオンプレミス製品バージョンでの使用がサポートされています。

- Citrix Gateway 12.1 54.13 Advanced エディション以降
- Citrix Gateway 13.0 41.20 Advanced エディション以降

前提条件

クラウドコネクタ

Citrix Cloud Connector™ソフトウェアをインストールするには、少なくとも2台のサーバーが必要です。これらのサーバーは、以下の要件を満たしている必要があります。

- 「[Cloud Connector requirements](#)」に記載されているシステム要件を満たしていること。

- 他のCitrixコンポーネントがインストールされておらず、Active Directoryドメインコントローラーではなく、リソースロケーションインフラストラクチャにとって重要なマシンではないこと。
- サイトが存在するドメインに参加していること。ユーザーが複数のドメインにあるサイトのアプリケーションにアクセスする場合、各ドメインに少なくとも2つのCloud Connectorをインストールする必要があります。
- サイトに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「[Service connectivity requirements](#)」を参照してください。
- Citrixでは、Cloud Connectorの高可用性のために2台のサーバーを推奨しています。インストール後、Cloud ConnectorはCitrix Cloud Japanがサイトを特定し、通信できるようにします。

Cloud Connectorのインストールに関する詳細については、以下の記事を参照してください。

- [クラウドコネクタをインストールする](#)
- [コマンドラインからクラウドコネクタをインストールする](#)

Active Directory (アクティブディレクトリ)

Citrix Gateway認証を有効にする前に、以下のタスクを実行してください。

- ワークスペースのサブスクリイバーがActive Directory (AD) にユーザーアカウントを持っていることを確認してください。ADアカウントを持たないサブスクリイバーは、ワークスペースに正常にサインインできません。
- サブスクリイバーのADアカウントのユーザープロパティが入力されていることを確認してください。Citrix Cloud Japanは、サブスクリイバーがサインインする際にユーザーコンテキストを確立するためにこれらのプロパティを必要とします。これらのプロパティが入力されていない場合、サブスクリイバーは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 Japan アカウントに接続します。このタスクでは、[Cloud Connectors](#) セクションで説明されているように、準備したサーバーに Cloud Connector ソフトウェアをインストールします。Cloud Connector は、Citrix Cloud Japan がオンプレミス環境と通信できるようにします。手順については、[Active Directory を Citrix Cloud Japan に接続する](#) を参照してください。
- Citrix Gateway 認証でフェデレーションを実行している場合は、AD ユーザーをフェデレーションプロバイダーに同期します。Citrix Cloud Japan は、ワークスペースのサブスクライバーが正常にサインインできるように、AD ユーザー属性を必要とします。

要件

Citrix Gateway の高度なポリシー

クラシックポリシーの廃止に伴い、Citrix Gateway 認証ではオンプレミス Gateway で高度なポリシーを使用する必要があります。高度なポリシーは、ID プロバイダーチェーンなどのオプションを含め、Citrix Cloud Japan の多要素認証をサポートします。現在クラシックポリシーを使用している場合は、Citrix Cloud Japan で Citrix Gateway 認証を使用するために、新しい高度なポリシーを作成する必要があります。高度なポリシーを作成する際に、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 のサブスクライバーを認証するために 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 Japan と Gateway 間のメッセージは OIDC プロトコルに準拠しており、トークンのデジタル署名が含まれます。したがって、これらのトークンに署名するための証明書を構成する必要があります。この証明書は、公開認証局 (CA) から発行されたものである必要があります。プライベート CA によって発行された証明書の使用はサポートされていません。Citrix Cloud Japan にプライベート ルート CA 証明書を提供する方法がないためです。そのため、信頼の証明書チェーンを確立できません。署名用に複数の証明書を構成した場合、これらのキーはメッセージごとにローテーションされます。

キーは **vpn global** にバインドされている必要があります。これらのキーがないと、サブスクライバー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 時刻に同期されている必要があります。クロックが同期されていない場合、Citrix Cloud Japan はトークンの有効性を確認する際に、トークンが古くなっていると見なします。

タスクの概要

Citrix Gateway認証を設定するには、次のタスクを実行します。

1. で、Gatewayへの接続の構成を開始します。この手順で、GatewayのクライアントID、シークレット、およびリダイレクトURLを生成します。
2. Gatewayで、Citrix Cloud Japanから生成された情報を使用してOAuth IdP詳細ポリシーを作成します。これにより、Citrix Cloud JapanがオンプレミスのGatewayに接続できるようになります。手順については、次の記事を参照してください。
 - Citrix Gateway 12.1: [オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する](#)
 - Citrix Gateway 13.0: [オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する](#)
3. で、サブスクリバターのCitrix Gateway認証を有効にします。

Citrix Gateway認証を構成する

1. Citrix Cloud Japanメニューから、[接続](#)を選択します。
2. **Authentication** 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。 (/en-us/citrix-cloud-japan/media/id-access-mgmt-ad-gateway-connect-menu.png)
3. オンプレミスのGatewayのFQDNを入力し、**検出** をクリックします。 (/en-us/citrix-cloud-japan/media/workspace-gateway-idp-detect-fqdn.png) Citrix Cloud Japanが正常に検出したら、**続行** をクリックします。
4. オンプレミスのGatewayとの接続を作成します。
 - a. Citrix Cloud Japanに表示されるクライアントID、シークレット、およびリダイレクトURLをコピーします。 (/en-us/citrix-cloud-japan/media/workspace-gateway-idp-connect-info.png) また、この情報のコピーをダウンロードし、参照用にオフラインで安全に保存してください。この情報は、生成後はCitrix Cloud Japanでは利用できません。
 - b. Gatewayで、Citrix Cloud JapanのクライアントID、シークレット、およびリダイレクトURLを使用してOAuth IdP詳細ポリシーを作成します。手順については、次の記事を参照してください。
 - Citrix Gateway 12.1の場合: [オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する](#)
 - Citrix Gateway 13.0の場合: [Citrix CloudのIDプロバイダーとしてオンプレミスのCitrix Gatewayを使用する](#)

- c. **Test and Finish**をクリックします。Citrix Cloud Japanは、Gatewayに到達可能で正しく構成されていることを確認します。

ワークスペースサブスクライバーのCitrix Gateway認証を有効にする

1. Citrix Cloud Japanメニューから、**Workspace Configuration**を選択します。
2. **Authentication**タブから、**Citrix Gateway**を選択します。
3. **I understand the impact on subscriber experience**を選択し、**Save**をクリックします。

トラブルシューティング

まず、この記事の[前提条件](#)と[要件](#)のセクションを確認してください。オンプレミス環境に必要なすべてのコンポーネントがあり、必要なすべての構成が行われていることを確認してください。これらの項目のいずれかが不足しているか、誤って構成されている場合、Citrix Gatewayによるワークスペース認証は機能しません。

Citrix Cloud JapanとオンプレミスGateway間の接続確立で問題が発生した場合は、次の項目を確認してください。

- Gateway FQDNがインターネットから到達可能であること。
- Citrix Cloud JapanにGateway FQDNを正しく入力していること。
- OAuth IdPポリシーの `-issuer` パラメーターにGateway URLを正しく入力していること（例: `-issuer https://GatewayFQDN.com`）。`issuer` パラメーターは大文字と小文字を区別します。
- Citrix Cloud JapanからのクライアントID、シークレット、およびリダイレクトURLの値が、OAuth IdPポリシーのClient ID、Client Secret、Redirect URL、およびAudienceフィールドに正しく入力されていること。ポリシーのAudienceフィールドに正しいクライアントIDが入力されていることを確認してください。
- OAuth IdP認証ポリシーが正しく構成されていること。手順については、以下の記事を参照してください。
 - Citrix Gateway 12.1: [Citrix CloudのIDプロバイダーとしてオンプレミスのCitrix Gatewayを使用する](#)
 - Citrix Gateway 13.0: [オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして使用する](#)
- ポリシーが[認証ポリシーのバインド](#)で説明されているように、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

ユーザーアカウントの詳細を取得するだけでなく、Gatewayはユーザーのドメイン名、AD NETBIOS名、およびルートADドメイン名を取得します。AD NETBIOS名を取得するために、Gatewayはユーザーアカウントが存在するADを検索します。NETBIOS名はグローバルカタログサーバーにはレプリケートされません。

AD環境でグローバルカタログサーバーを使用している場合、これらのサーバーで構成されたLDAPアクションはCitrix Cloud Japanでは機能しません。代わりに、LDAPアクションで個々のADを構成する必要があります。複数のドメインまたはフォレストがある場合は、複数のLDAPポリシーを構成できます。

KerberosまたはIdPチェイニングによるシングルサインオンのためのAD検索

サブスクリバラーのサインインにKerberosまたはSAMLまたはOIDCプロトコルを使用する外部IDプロバイダーを使用している場合は、ADルックアップが構成されていることを確認してください。Gatewayは、サブスクリバラーのADユーザープロパティとAD構成プロパティを取得するためにADルックアップを必要とします。

認証がサードパーティサーバーによって処理される場合でも、LDAPポリシーが構成されていることを確認してください。これらのポリシーを構成するには、次のタスクを実行して、既存のログインスキーマプロファイルに第2認証要素を追加します。

1. Active Directoryから属性とグループの抽出のみを実行するLDAP認証サーバーを作成します。
2. LDAP高度認証ポリシーを作成します。
3. 認証ポリシーラベルを作成します。
4. プライマリIDプロバイダーの後に、認証ポリシーラベルを次の要素として定義します。

LDAPを第2認証要素として追加するには

1. LDAP認証サーバーを作成します。
 - a. システム > 認証 > 基本ポリシー > LDAP > サーバー > 追加 を選択します。
 - b. 「認証LDAPサーバーの作成」 ページで、次の情報を入力します。
 - 「サーバータイプの選択」で、「LDAP」を選択します。
 - 「名前」に、サーバーのわかりやすい名前を入力します。
 - 「サーバーIP」を選択し、LDAPサーバーのIPアドレスを入力します。
 - 「セキュリティタイプ」で、必要なLDAPセキュリティタイプを選択します。
 - 「サーバータイプ」で、「AD」を選択します。

- 「**認証**」で、チェックボックスを選択しないでください。この認証サーバーは、認証ではなく、Active Directoryからユーザー属性とグループを抽出するためだけに使用されるため、このチェックボックスはオフにする必要があります。

c. 「**その他の設定**」で、次の情報を入力します。

- 「**サーバーログオン名属性**」に、「**UserPrincipalName**」と入力します。
- 「**グループ属性**」で、「**memberOf**」を選択します。
- 「**サブ属性名**」で、「**cn**」を選択します。

2. LDAP高度認証ポリシーを作成します。

a. セキュリティ > AAA - アプリケーショントラフィック > ポリシー > 認証 > 高度なポリシー > ポリシー > 追加を選択します。

b. 「**認証ポリシーの作成**」ページで、次の情報を入力します。

- 「**名前**」に、ポリシーのわかりやすい名前を入力します。
- で、 を選択します。
- で、以前に作成したLDAP認証サーバーを選択します。
- に「**TRUE**」と入力します。

c. をクリックして構成を保存します。

3. 認証ポリシーラベルを作成します。

a. >>>>> の順に選択します。

b. に、認証ポリシーラベルのわかりやすい名前を入力します。

c. ログインスキーマで、**LSCHEMA_INT**を選択します。

d. の で、以前に作成したLDAP高度認証ポリシーを選択します。

e. で、 を選択します。

f. 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. >>> の順に選択します。

b. プライマリIDプロバイダーのバインドを含む仮想サーバーを選択し、 を選択します。

c. で、既存の**** バインドを選択します。

- 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、**バインディングの編集**を選択します。
- e. **ポリシーバインディング**ページで、**次の要素の選択**から、以前作成したLDAP認証ポリシーラベルを選択します。
- f. 設定を保存するには、**バインド**をクリックします。

多要素認証のデフォルトパスワード

ワークスペースのサブスクライバーに多要素認証を使用する場合、Gatewayは最後の要素のパスワードをシングルサインオンのデフォルトパスワードとして使用します。このパスワードは、サブスクライバーがワークスペースにサインインするときにCitrix Cloud Japanに送信されます。環境でLDAP認証の後に別の要素が続く場合は、LDAPパスワードをCitrix Cloud Japanに送信されるデフォルトパスワードとして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。

Okta を ID プロバイダーとして接続する

Citrix Cloud™ Japan は、ワークスペースにサインインするサブスクライバーを認証するための ID プロバイダーとして Okta の使用をサポートしています。Okta 組織を Citrix Cloud Japan に接続することで、サブスクライバーが Citrix Workspace のリソースにアクセスするための共通のサインインエクスペリエンスを提供できます。

Workspace Configuration で Okta 認証を有効にすると、サブスクライバーのサインインエクスペリエンスが変わります。Okta 認証を選択すると、シングルサインオンではなくフェデレーションサインインが提供されます。サブスクライバーは Okta の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 Virtual Apps and Desktops サービス) からアプリまたはデスクトップを開く際に、2 度目の認証が必要になる場合があります。シングルサインオンを有効にし、2 度目のログオンプロンプトを防ぐには、Citrix Cloud Japan で Citrix Federated Authentication Service を使用する必要があります。詳細については、「[Citrix Federated Authentication Service を使用してワークスペースのシングルサインオンを有効にする](#)」を参照してください。

前提条件

クラウドコネクタ

Citrix Cloud Connector™ ソフトウェアをインストールするには、Active Directory ドメイン内に少なくとも 2 台のサーバーが必要です。Cloud Connector は、Citrix Cloud Japan とリソースの場所

間の通信を可能にするために必要です。Citrix は、Cloud Connector の高可用性のために 2 台のサーバーを推奨しています。これらのサーバーは、次の要件を満たしている必要があります。

- [Cloud Connector の要件](#) に記載されている要件を満たしていること。
- 他の Citrix® コンポーネントがインストールされておらず、Active Directory ドメインコントローラーではなく、リソースの場所のインフラストラクチャにとって重要ではないマシンであること。
- Active Directory (AD) ドメインに参加していること。ワークスペースのリソースとユーザーが複数のドメインに存在する場合は、各ドメインに少なくとも 2 つの Cloud Connector をインストールする必要があります。詳細については、「[Active Directory での Cloud Connector の展開シナリオ](#)」を参照してください。
- ユーザーが Citrix Workspace を介してアクセスするリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「[サービス接続要件](#)」を参照してください。

Cloud Connector のインストールに関する詳細については、以下の記事を参照してください。

- [Cloud Connector のインストール](#)
- [コマンドラインからの Cloud Connector のインストール](#)

Okta ドメイン

OktaをCitrix Cloud Japanに接続する際、組織のOktaドメインを指定する必要があります。Citrixは以下のOktaドメインをサポートしています。

- okta.com
- okta-eu.com
- oktapreview.com

Citrix Cloud JapanでOktaカスタムドメインを使用することもできます。カスタムドメインの使用に関する重要な考慮事項については、Oktaウェブサイトの[Customize the Okta URL domain](#)を参照してください。

組織のカスタムドメインの特定に関する詳細については、Oktaウェブサイトの[Finding Your Okta Domain](#)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 Japanで利用できるクライアント資格情報を持つOkta OIDC Webアプリケーションを作成する必要があります。アプリケーションを作成および構成したら、クライアントIDとクライアントシークレットを控えてください。Okta組織を接続する際に、これらの値をCitrix Cloud Japanに提供します。

このアプリケーションを作成および構成するには、この記事の以下のセクションを参照してください。

- [Okta OIDC Webアプリ統合の作成](#)
- [Okta OIDC Webアプリケーションの構成](#)

ワークスペースURL

Oktaアプリケーションを作成する際、Citrix Cloud JapanのワークスペースURLを指定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 Japan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**した場合、Oktaアプリケーション構成を新しいURLで更新する必要があります。そうしないと、サブスクライバーがワークスペースからのサインアウトで問題が発生する可能性があります。

Okta APIトークン

Citrix Cloud JapanでOktaをIDプロバイダーとして使用するには、Okta組織のAPIトークンが必要です。このトークンは、Okta組織の読み取り専用管理者アカウントを使用して作成します。このトークンは、Okta組織のユーザーとグループを読み取ることができる必要があります。

APIトークンを作成するには、この記事の「[Okta APIトークンを作成する](#)」を参照してください。APIトークンの詳細については、Okta Webサイトの「[APIトークンを作成する](#)」を参照してください。

重要:

APIトークンを作成する際は、トークン値をメモしてください（たとえば、値を一時的にブレーンテキストドキュメントにコピーするなど）。Oktaはこの値を一度しか表示しない

め、「Citrix Cloud JapanをOkta組織に接続する」の手順を実行する直前にトークンを作成することをお勧めします。

Okta ADエージェントでアカウントを同期する

OktaをIDプロバイダーとして使用するには、まずオンプレミスのADをOktaと統合する必要があります。これを行うには、ドメインにOkta ADエージェントをインストールし、ADをOkta組織に追加します。Okta ADエージェントの展開に関するガイダンスについては、Okta Webサイトの「[Active Directory統合の開始](#)」を参照してください。

その後、ADユーザーとグループをOktaにインポートします。インポートする際は、ADアカウントに関連付けられている次の値を含めます。

- メール
- SID
- UPN
- OID

注：

WorkspaceでCitrix Gatewayサービスを使用している場合、ADアカウントをOkta組織と同期する必要はありません。

ADユーザーとグループをOkta組織と同期するには：

1. Okta ADエージェントをインストールして構成します。詳細な手順については、Oktaウェブサイトの以下の記事を参照してください。
 - [Okta Active Directoryエージェントのインストール](#)
 - [Active Directoryのインポートとアカウント設定の構成](#)
 - [Active Directoryプロビジョニング設定の構成](#)
2. 手動インポートまたは自動インポートを実行して、ADユーザーとグループをOktaに追加します。Oktaのインポート方法と手順の詳細については、Oktaウェブサイトの[Active Directoryユーザーとグループの管理](#)を参照してください。

Okta OIDC Webアプリ統合の作成

1. Okta管理コンソールで、**Applications**の下にある**Applications**を選択します。
2. **Create App Integration**を選択します。
3. **Sign in method**で、**OIDC - OpenID Connect**を選択します。
4. **Application Type**で、**Web Application**を選択します。**Next**を選択します。
5. **App Integration Name**に、アプリ統合のわかりやすい名前を入力します。
6. **Grant type**で、以下のオプションを選択します。
 - Authorization Code (デフォルトで選択済み)
 - 暗黙的 (ハイブリッド)
7. **Sign-in redirect URIs**に、`https://accounts.citrixcloud.jp/core/login-okta`を入力します。
8. 「サインアウト リダイレクト URI」に、Citrix Cloud Japan のワークスペース URL を入力します。
9. 「割り当て」の「制御されたアクセス」で、アプリ統合を組織内の全員に割り当てるか、指定したグループのみに割り当てるか、または後でアクセスを割り当てるかを選択します。
10. 「保存」を選択します。アプリ統合を保存すると、コンソールにアプリケーション構成ページが表示されます。
11. 「クライアント資格情報」セクションで、「クライアント ID」と「クライアント シークレット」の値をコピーします。これらの値は、Citrix Cloud Japan を Okta 組織に(#connect-citrix-cloud-japan-to-your-okta-organization)接続するときに使用します。

Okta OIDC Web アプリケーションを構成する

この手順では、Citrix Cloud Japan に必要な設定で Okta OIDC Web アプリケーションを構成します。Citrix Cloud Japan は、サブスクライバーがワークスペースにサインインする際に Okta を介して認証するために、これらの設定を必要とします。

1. (オプション) 暗黙的な許可タイプに対するクライアント権限を更新します。この許可タイプに対して最小限の特権を許可することを希望する場合、この手順を実行することを選択できます。
 - a. Okta アプリケーション構成ページで、「一般設定」の下にある「編集」を選択します。
 - b. 「アプリケーション」セクションの「ユーザーに代わって動作するクライアント」で、「暗黙的な許可タイプでアクセストークンを許可する」のチェックを外します。

- c. 「保存」を選択します。
2. アプリケーション属性を追加します。これらの属性は大文字と小文字を区別します。
 - a. Okta コンソールメニューから、「ディレクトリ > プロファイルエディター」を選択します。
 - b. Okta の「ユーザー (デフォルト)」プロファイルを選択します。Okta に「ユーザー」プロファイルページが表示されます。
 - c. 「属性」の下にある「属性の追加」を選択します。
 - d. 次の情報を入力します。
 - 表示名: cip_email
 - 変数名: cip_email
 - 説明: ADユーザーセキュリティ識別子
 - 属性の長さ: 1より大きい
 - 属性は必須: はい
 - e. 保存して別の項目を追加を選択します。
 - f. 次の情報を入力します:
 - 表示名: cip_sid
 - 変数名: cip_sid
 - 説明: ADユーザーセキュリティ識別子
 - 属性の長さ: 1より大きい
 - 属性は必須: はい
 - g. 保存して別の項目を追加を選択します。
 - h. 次の情報を入力します:
 - 表示名: cip_upn
 - 変数名: cip_upn
 - 説明: ADユーザープリンシパル名
 - 属性の長さ: 1より大きい
 - 属性は必須: はい
 - i. 保存して別の項目を追加を選択します。

j. 次の情報を入力します。

- 表示名: cip_oid
- 変数名: cip_oid
- 説明: ADユーザーGUID
- 属性の長さ: 1より大きい
- 属性は必須: はい

k. **保存**を選択します。

3. アプリケーションの属性マッピングを編集します。

a. Oktaコンソールから、**Directory > Profile Editor**を選択します。

b. ADの**active_directory**プロファイルを見つけます。このプロファイルは、`myDomain User`という形式でラベル付けされている場合があります。ここで、`myDomain`は統合されたADドメインの名前です。

c. 「**マッピング**」を選択します。ADドメインのユーザープロファイルマッピングページが表示され、ADをOktaユーザーにマッピングするためのタブが選択されます。

d. 「**Oktaユーザープロファイル**」列で、ステップ2で作成した属性を見つけ、次のようにマッピングします。

- `cip_email`については、ドメインのユーザープロファイル列から `email` を選択します。選択すると、マッピングは `appuser.email` として表示されます。
- `cip_sid`については、ドメインのユーザープロファイル列から `objectSid` を選択します。選択すると、マッピングは `appuser.objectSid` として表示されます。
- `cip_upn`については、ドメインのユーザープロファイル列から `userName` を選択します。選択すると、マッピングは `appuser.userName` として表示されます。
- `cip_oid`については、ドメインのユーザープロファイル列から `externalId` を選択します。選択すると、マッピングは `appuser.externalId` として表示されます。

e. 「**マッピングを保存**」を選択します。

f. 「**今すぐ更新を適用**」を選択します。Oktaはマッピングを適用するジョブを開始します。

g. OktaをADと同期します。

i. Oktaコンソールから、「**Directory > Directory Integrations**」を選択します。

ii. 統合されたADを選択します。

iii. 「**プロビジョニング**」タブを選択します。

- iv. 「設定」の下で、「Oktaへ」を選択します。
- v. 「Okta属性マッピング」セクションまでスクロールし、「強制同期」を選択します。

Okta APIトークンを作成する

1. 読み取り専用管理者アカウントを使用してOktaコンソールにサインインします。
2. Oktaコンソールメニューから、**Security > API**を選択します。
3. **Tokens**タブを選択し、次に**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。この値は、Okta組織をCitrix Cloud Japanに接続するときに指定します。

Citrix Cloud JapanをOkta組織に接続する

1. Citrix Cloud Japanにサインインします <https://citrix.citrixcloud.jp>。
2. 管理コンソールの左上隅にあるCitrix Cloud Japanメニューから、**Identity and access management**を選択します。
3. **Okta**を見つけて、省略記号メニューから**Connect**を選択します。
4. **Okta URL**に、Oktaドメインを入力します。
5. **Okta API Token**に、Okta組織のAPIトークンを入力します。
6. **Client ID**と**Client Secret**に、以前に作成したOIDC Webアプリ統合のクライアントIDとシークレットを入力します。これらの値をOktaコンソールからコピーするには、**Applications**を選択し、Oktaアプリケーションを見つけます。**Client Credentials**の下で、各値の**Copy to Clipboard**ボタンを使用します。
7. **Test and Finish**をクリックします。Citrix Cloud JapanはOktaの詳細を確認し、接続をテストします。

ワークスペースのOkta認証を有効にする

1. 「Citrix Cloud Japan」メニューから、**ワークスペース構成 > 認証**を選択します。
2. **Okta**を選択します。プロンプトが表示されたら、**サブスクライバーエクスペリエンスへの影響を理解しています**を選択します。
3. 権限リクエストを承認するには、**承認**をクリックします。

SAMLをCitrix Cloud JapanのIDプロバイダーとして接続する

Citrix Cloud Japanは、管理者（プレビュー版）およびワークスペースにサインインするサブスクライバーを認証するためのIDプロバイダーとして、SAML（Security Assertion Markup Language）の使用をサポートしています。オンプレミスのActive Directory（AD）と連携して、任意のSAML 2.0プロバイダーを使用できます。

ほとんどのSAMLプロバイダーの場合、この記事の情報をを使用してSAML認証を設定します。

Microsoft Entra IDでSAML認証を使用するには、Microsoft Entra IDアプリギャラリーにあるCitrix Cloud Japan SAML SSOアプリを選択できます。Citrix Cloud JapanでSAML認証を設定するためのCitrix Cloud Japan SAML SSOアプリの使用に関する詳細については、Microsoft Entra IDアプリのドキュメントWebサイトにある[チュートリアル: Microsoft Entra ID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。

前提条件

Citrix Cloud JapanでSAML認証を使用するには、次の要件があります。

- SAML 2.0をサポートするSAMLプロバイダー
- オンプレミスADドメイン
- リソースの場所に展開され、オンプレミスADドメインに参加している2つのCloud Connector。Cloud Connectorは、Citrix Cloud Japanがリソースの場所と通信できることを保証するために使用されます。
- SAMLプロバイダーとのAD統合。

クラウドコネクタ

Citrix Cloud Connector™ソフトウェアをインストールするためのサーバーが少なくとも2台必要です。Citrixは、Cloud Connectorの高可用性のために少なくとも2台のサーバーを推奨しています。これらのサーバーは次の要件を満たす必要があります。

- [Citrix Cloud Connectorの要件](#)に記載されているシステム要件を満たしていること。
- 他のCitrix®コンポーネントがインストールされておらず、ADドメインコントローラーではなく、リソースの場所のインフラストラクチャにとって重要ではないマシンであること。
- リソースが存在するドメインに参加していること。ユーザーが複数のドメインのリソースにアクセスする場合は、各ドメインに少なくとも2つのCloud Connectorをインストールする必要があります。

- サブスクライバーがCitrix Workspaceを介してアクセスするリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。詳細については、「[接続要件](#)」を参照してください。

Cloud Connector のインストールについて詳しくは、「[タスク 3: 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。

- ワークスペースのサブスクライバーが Active Directory (AD) にユーザーアカウントを持っていることを確認します。SAML 認証が構成されている場合、AD アカウントを持たないサブスクライバーはワークスペースに正常にサインインできません。
- サブスクライバーの AD アカウントのユーザープロパティが入力されていることを確認します。Citrix Cloud Japan は、サブスクライバーが Citrix Workspace にサインインする際にユーザーコンテキストを確立するためにこれらのプロパティを必要とします。これらのプロパティが入力されていない場合、サブスクライバーは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 (オプション)
 - 共通名
 - SAM アカウント名
 - ユーザープリンシパル名
 - オブジェクト GUID
 - SID
- Cloud Connector を展開して、オンプレミスの Active Directory (AD) と Citrix Cloud Japan アカウント間の接続を確立します。
- AD ユーザーを SAML プロバイダーに同期します。Citrix Cloud Japan は、ワークスペースのサブスクライバーが正常にサインインできるように、AD ユーザー属性を必要とします。

SAMLとActive Directoryの統合

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須ADユーザー属性をCitrix Cloud Japanに渡すことができます。

- SecurityIdentifier (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- メール (email)

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、統合プロセスには通常、次のタスクが含まれます。

1. ADドメインに同期エージェントをインストールして、ドメインとSAMLプロバイダー間の接続を確立します。
2. 前述のADユーザー属性に対応するカスタム属性が利用できない場合は、カスタム属性を生成し、それらをActive Directory (AD) にリンクします。参考として、このタスクの一般的な手順は、この記事の[カスタムSAML属性の作成とマッピング](#)で説明されています。
3. ADユーザーをSAMLプロバイダーに同期します。

注:

リストされているADユーザー属性にマッピングするカスタム属性をすでに作成している場合は、それ以上の作成やマッピングは必要ありません。代わりに、Citrix Cloud Japanで[SAMLプロバイダーからのメタデータを構成](#)するときに、既存のカスタム属性を使用してください。

ADとSAMLプロバイダーの統合の詳細については、SAMLプロバイダーの製品ドキュメントを参照してください。

SAML 2.0による管理者認証

注:

Citrix Cloud Japan管理者向けのSAML認証はテクニカルレビュー段階です。Citrixでは、レビュー機能は非本番環境でのみ使用することをお勧めします。

ADグループ

Citrix Cloud Japanに管理者をADグループのみを使用して追加できます。SAML認証を使用している場合、管理者を個別に追加することはできません。

サインインURL

SAML認証を構成する際、管理者がCitrix Cloud Japanにサインインするために使用できるサインインURLを構成します。このURLは `https://citrix.citrixcloud.jp/go/myorganization` の形式を使用し、「myorganization」は組織用に選択した一意の識別子です。

ADグループを追加すると、グループ内の管理者は、指定したサインインURLを使用してCitrix Cloud Japanにすぐにサインインできます。Citrixは、管理者にCitrix Cloud Japanへのアクセス権があることを知らせる通知を送信しません。

サポートされる権限

カスタムアクセス権限のみがサポートされています。ADグループを追加する際は、グループ内の管理者に付与する権限を選択する必要があります。フルアクセス権限はサポートされていません。

タスクの概要

SAML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、「[Active DirectoryをCitrix Cloud Japanに接続する](#)」の説明に従って、オンプレミスのADをCitrix Cloud Japanに接続します。
2. この記事の「[Active DirectoryとのSAML統合](#)」の説明に従って、SAMLプロバイダーをオンプレミスのADと統合します。
3. **IDおよびアクセス管理**で、Citrix Cloud Japanで[SAML認証を構成](#)し、SAML接続を確立するために、SAMLプロバイダーをCitrix Cloud Japanのメタデータで構成し、Citrix Cloud JapanをSAMLプロバイダーのメタデータで相互に構成します。
4. SAMLを使用して管理者を認証する場合：
 - a. 管理者がCitrix Cloud Japanにサインインするために使用できる[サインインURL](#)を構成します。
 - b. 所属するADグループを指定して、Citrix Cloud Japanに管理者を追加します(#add-administrators-to-citrix-cloud-japan-from-ad)。
5. ワークスペースサブスクリバの認証にSAMLを使用している場合は、**Workspace Configuration**でSAML認証方法を有効にします(#enable-saml-authentication-for-workspaces)。Citrix Cloud管理者の認証にのみSAMLを使用している場合は、このタスクを実行する必要はありません。

カスタムSAML属性を作成してマッピングする

SAMLプロバイダーでSID、UPN、OID、およびメール属性のカスタム属性をすでに構成している場合は、このタスクを完了する必要はありません。(#create-a-saml-connector-application)SAMLコネクタアプリケーションを作成するに進み、手順8で既存のカスタムSAML属性を使用してください。

注：

このセクションの手順では、SAMLプロバイダーの管理コンソールで実行するアクションについて説明します。これらのアクションを実行するために使用する特定のコマンドは、選択したSAMLプロバイダーによって、このセクションで説明されているコマンドとは異なる場合があります。このセクションのSAMLプロバイダーコマンドは、あくまで例として提供されています。SAMLプロバイダーに固有の関連コマンドの詳細については、SAMLプロバイダーのドキュメントを参照してください。

1. SAMLプロバイダーの管理コンソールにサインインし、カスタムユーザー属性を作成するオプションを選択します。たとえば、SAMLプロバイダーのコンソールによっては、**Users > Custom User Fields > New User Field**を選択する場合があります。
2. 次の属性を追加します。
 - cip_sid
 - cip_upn
 - cip_oid
 - cip_email
3. Citrix Cloud Japan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**を選択する場合があります。
4. ディレクトリ属性を追加するオプションを選択します。たとえば、SAMLプロバイダーのコンソールによっては、**Directory Attributes**を選択する場合があります。
5. 属性を追加するオプションを選択し、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ピングします。
 - 「objectSid」を選択し、「cip_sid」属性にマッピングします。
 - 「userPrincipalName」を選択し、「cip_upn」属性にマッピングします。
 - 「ObjectGUID」を選択し、「cip_oid」属性にマッピングします。

- 「mail」を選択し、「cip_email」属性にマッピングします。

管理者サインインURLを構成する

1. <https://citrix.citrixcloud.jp>でCitrix Cloudにサインインします。
2. Citrix Cloudメニューから、[設定](#)を選択します。
3. [設定](#)を見つけて、省略記号メニューから[サインインURL](#)を選択します。
4. プロンプトが表示されたら、会社の短くURLフレンドリーな識別子を入力し、[サインインURL](#)を選択します。ページが表示されます。
5. 次のセクションに進み、Citrix CloudへのSAML接続を構成します。

SAMLプロバイダーのメタデータを構成する

このタスクでは、Citrix Cloud Japanから取得したSAMLメタデータを使用してコネクタアプリケーションを作成します。SAMLアプリケーションを構成した後、コネクタアプリケーションのSAMLメタデータを使用して、Citrix Cloud JapanへのSAML接続を構成します。

注：

このセクションの一部の手順では、SAMLプロバイダーの管理コンソールで実行するアクションについて説明しています。これらのアクションを実行するために使用する特定のコマンドは、選択したSAMLプロバイダーによって、このセクションで説明されているコマンドとは異なる場合があります。このセクションのSAMLプロバイダーコマンドは、あくまで例として提供されています。SAMLプロバイダー固有の関連コマンドの詳細については、SAMLプロバイダーのドキュメントを参照してください。

SAMLコネクタアプリケーションを作成する

1. SAMLプロバイダーの管理コンソールから、属性と署名応答を持つIDプロバイダーのアプリケーションを追加します。たとえば、プロバイダーのコンソールによっては、**Applications > Applications > Add App**を選択し、次に**SAML Test Connector (IdP w/ attr w/ sign response)**を選択する場合があります。
2. 該当する場合は、表示名を入力してアプリを保存します。
3. Citrix Cloud Japanの**SAMLの構成**画面で、**SAMLメタデータ**の下にある**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タブに表示されます。

注：

必要に応じて、このファイルを <https://saml.citrixcloud.jp/saml/metadata.xml> からダウンロードすることもできます。このエンドポイントは、SAMLプロバイダーのメタデータをインポートおよび監視する際に、一部のIDプロバイダーにとってより使いやすい場合があります。

4. コネクタアプリケーションに次の詳細を入力します。

- **Audience**フィールドに、<https://saml.citrixcloud.jp> と入力します。
- **Recipient**フィールドに、<https://saml.citrixcloud.jp/saml/acs> と入力します。
- ACS URLバリデーターのフィールドに、<https://saml.citrixcloud.jp/saml/acs> と入力します。
- ACS URLのフィールドに、<https://saml.citrixcloud.jp/saml/acs> と入力します。

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る
cip_sid	cip_sid または既存のSID属性
cip_upn	cip_upn または既存のUPN属性
cip_oid	cip_oid または既存のOID属性
cip_email	cip_email または既存のメール属性

6. Workspaceのサブスクライバーをユーザーとして追加し、アプリケーションにアクセスできるようにします。

Citrix Cloud JapanにSAMLプロバイダーのメタデータを追加する

1. SAMLプロバイダーからSAMLメタデータを取得します。このファイルの例を次の図に示します。



2. Citrix Cloud Japan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。

- **エンティティID**に、メタデータ内の**EntityDescriptor**要素から**entityID**の値を入力します。

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://app. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
```

- **認証要求に署名**で、Citrix Cloud Japanが認証要求に署名し、悪意のあるアクターではなくCitrix Cloud Japanからのものであることを証明するには、**はい**を選択します。SAMLプロバイダーがSAML応答を安全に投稿するために使用する許可リストにCitrix ACS URLを追加する場合は、**いいえ**を選択します。
- **SSOサービスURL**に、使用するバインディングメカニズムのURLを入力します。HTTP-POSTまたはHTTP-Redirectバインディングのいずれかを使用できます。メタデータファイルで、バインディング値が**HTTP-POST**または**HTTP-Redirect**の**SingleSignOnService**要

素を見つけます。

```
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings HTTP-Redirect Location="
https://citrixidentity-dev. /trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings HTTP-POST Location="
https://citrixidentity-dev. .com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
```

- **バインディングメカニズム**で、メタデータファイルから選択したSSOサービスURLのバインディングと一致するメカニズムを選択します。
- **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、Citrix Cloud Japanは、このフィールドで指定された通りに署名されていない応答をすべて拒否します。

3. SAMLプロバイダーの管理コンソールで、次の操作を実行します。

- SAML署名アルゴリズムに**SHA-256**を選択します。
- X.509証明書をPEMファイルとしてダウンロードします。

4. Citrix Cloud Japanの**SAMLの構成**画面で、**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PEM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 Japanがこのコンテキストをどの程度厳密に適用するかを選択します。選択したコンテキストで認証を適用せずに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適用するには、**厳密**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、または使用しない場合は、**未指定**と**最小**を選択します。

7. **ログアウトURL**で、SAMLプロバイダーのメタデータファイルにあるHTTP-Redirectバインディングを持つ**SingleSignOnService**要素を見つけて、URLを入力します。ログアウトURLを省略することを選択した場合、Citrix Cloud JapanはIDプロバイダーにログオフ要求を送信しません。代わりに、Citrix Cloud JapanはWorkspace URLにリダイレクトします。Citrix Cloud Japanは、シングルログアウト（SLO）または署名付きログアウト要求の送信をサポートしていません。

8. Citrix Cloud Japanの次のデフォルトの名前属性値が、SAMLプロバイダーの管理コンソールにある対応する属性値と一致することを確認します。SAMLプロバイダーの値が異なる場合は、Citrix Cloud Japanでこれらの値を変更して、SAMLプロバイダーと一致するようにできます。

- ユーザー表示名の属性名: `displayName`
- ユーザー名の属性名: `givenName`
- ユーザー姓の属性名: `familyName`

9. Citrix Cloud Japanで、SAMLプロバイダーからのカスタムSAML属性を入力します。

- セキュリティ識別子 (SID) の属性名に、カスタムSID属性名を入力します。デフォルト値は `cip_sid` です。
- ユーザープリンシパル名 (UPN) の属性名に、カスタムUPN属性名を入力します。デフォルト値は `cip_upn` です。
- メールの属性名に、カスタムメール属性名を入力します。デフォルト値は `cip_email` です。
- ADオブジェクト識別子 (OID) の属性名で、カスタムOID属性名を入力します。デフォルト値は `cip_oid` です。

10. テストと完了を選択して、接続が正常に構成されたことを確認します。

ADからCitrix Cloud Japanに管理者を追加する

1. Citrix Cloud Japanで、IDおよびアクセス管理ページから**管理者**タブを選択します。 (/en-us/citrix-cloud-japan/media/id-access-mgmt-admins-page.png)
2. **管理者詳細**で、**Active Directory**を選択し、使用するドメインを選択します。
3. **追加するグループを検索**で、検索ボックスに追加するグループの名前を入力し始めます。表示されたら、プラス記号 (+) をクリックしてグループを選択します。
4. **次へ**を選択します。
5. グループに割り当てるカスタムアクセス権限または役割を選択します。**次へ**を選択します。
6. 管理者詳細を確認します。変更を加えるには**戻る**を選択します。
7. 完了したら、**保存**を選択します。

ワークスペースのSAML認証を有効にする

1. Citrix Cloud Japan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

SAML構成で必要な属性が正しくエンコードされていない場合、属性エラーが発生する可能性があります。属性エラーが発生すると、Citrix Cloud Japanは、問題のある属性を含むエラーメッセージを表示します。

cip_oidが引用された属性エラーメッセージ(/en-us/citrix-cloud-japan/media/saml-idp-missing-attribute-error.png)

この種のエラーを解決するには、次の表に記載されているように、これらの属性がエンコードされていることを確認してください。

属性	エンコード
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
cip_upn	文字列形式である必要があります (user@domain)

予期しないエラー

Citrix Cloud Japan で予期せぬエラーが発生する場合があります。次の場合です。

- ユーザーがIDP開始フローを使用してSAMLリクエストを開始した場合。例えば、ワークスペースURLに直接アクセスするのではなく、IDプロバイダーのアプリポータル内のタイルを選択することによってリクエストが開始されます (customer.citrixcloud.jp)。
- SAML証明書が無効であるか、または期限切れである。
- 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ない。

このエラーが発生すると、Citrix Cloud Japan は一般的なエラーメッセージを表示します。

予期せぬエラーメッセージ(/en-us/citrix-cloud-japan/media/saml-idp-flow-error.png)

このエラーが、IDプロバイダーのアプリポータルを介してCitrix Cloud Japanに移動した結果である場合、以下の回避策を使用できます。

1. IDプロバイダーのアプリポータルに、ワークスペースURLを参照するブックマークアプリを作成します (例: https://customer.citrixcloud.jp)。
2. ユーザーをSAMLアプリとブックマークアプリの両方に割り当てます。

3. アプリポータルで表示設定を変更し、SAMLアプリを非表示にしてブックマークアプリを表示します。
4. Prompt=Login パラメーターを無効にして、追加のパスワードプロンプトを削除します。

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、オンプレミスのCitrixライセンスサーバー向けの最新のクラウドベースのライセンスソリューションです。従来のCitrixレガシーライセンスに代わる合理化されたソリューションとして設計されたLASは、製品アクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスなアプローチを保証します。

ライセンスファイルのライフサイクルを手動で管理する代わりに、ライセンスサーバーをCitrix Cloud™に接続してオンラインアクティベーションを行うことができます。登録後、ライセンスサーバーはLASエンドポイントと定期的に通信し、アクティベーションが最新の状態に保たれ、エンタイトルメントの有効期限または契約終了日に合わせて調整されるようにします。

詳細については、「[License Activation Service](#)」を参照してください。

Citrix Cloud Japan の管理

Citrix Cloud Japan には、次の管理機能が含まれています。

- 管理者の招待とクラウドサービスへのアクセス委任
- ライブラリ内のサービス提供へのユーザーの割り当て
- サービス通知の監視
- Citrix Cloud Japan で発生したイベントのシステムログの表示

管理者

管理者は、自身のIDを使用してCitrix Cloud Japanにアクセスし、管理アクティビティを実行し、Citrix Cloud Connectorをインストールします。

CitrixのIDメカニズムは、メールアドレスとパスワードを使用して管理者の認証を提供します。管理者は、My Citrixの資格情報を使用してCitrix Cloud Japanにサインインすることもできます。

新しい管理者の追加

アカウントのオンボーディングプロセス中に、最初の管理者が作成されます。この管理者は、他の管理者をCitrix Cloud Japanに招待できます。これらの新しい管理者は、既存のCitrix Cloud Japan アカウントの資格情報を使用するか、必要に応じて新しいアカウントを設定できます。招待する管理者のアクセス権限を細かく調整することもできます。これにより、組織内での管理者の役割に合わせたアクセスを定義できます。

他の管理者を招待し、Citrix Cloud Japanへのアクセスを細かく調整するには、「[Citrix Cloud Japanアカウントへの管理者の追加](#)」を参照してください。

パスワードの変更

Citrix Cloud Japan内からパスワードを変更したい場合は、**アカウント設定**に移動し、**マイプロフィール**を選択します。**パスワードの変更**をクリックして、現在のパスワードを入力し、新しいパスワードを確認します。

管理者の削除

管理者は、Citrix Cloud Japanアカウントの「管理者」タブから削除できます。管理者を削除すると、その管理者はCitrix Cloud Japanにサインインできなくなります。管理者を削除したときにその管理者がログインしていた場合、最大1分間はアクティブな状態が維持されます。その後、Citrix Cloud Japan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 Japanでは、各顧客アカウントに少なくとも1人の管理者が必要です。
- Cloud Connectorは管理者アカウントにリンクされていません。そのため、Cloud Connectorをインストールした管理者を削除しても、Cloud Connectorは引き続き動作します。

サブスクライバー

サブスクライバーのIDは、Citrix Cloud Japanでアクセスできるサービスを定義します。このIDは、リソースの場所内のドメインから提供されるActive Directoryドメインアカウントから取得されます。サブスクライバーをライブラリ提供に割り当てると、そのサブスクライバーはその提供にアクセスする権限が与えられます。

重要：

Citrix DaaS™ (formerly Virtual Apps and Desktops service)でオンプレミスのStoreFrontを使用している場合、デリバリーグループの作成時にリソースを割り当てるためにライブラリを使用しないでください。代わりに、Studioを使用してユーザーにリソースを割り当ててください。このシナリオでライブラリを使用すると、リソースがユーザーに列挙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際、ページで**「ユーザー管理をCitrix Cloudに任せる」を選択しないでください。代わりに、別のオプション（「認証済みユーザーなら誰でもこのデリバリーグループを使用できるようにする」または「このデリバリーグループの使用を以下のユーザーに制限する」**）を選択してください。

管理者は、タブで、これらのIDを提供するドメインを制御できます。複数のフォレストからドメインを使用する予定がある場合は、各フォレストに少なくとも2つのCloud Connectorをインストールしてください。Citrix®は、高可用性環境を維持するために少なくとも2つのCloud Connectorを推奨しています。

ユーザーをライブラリ提供に割り当てるプロセスは、Citrix Cloud JapanとCitrix Cloud (citrix.cloud.com)で同じです。手順については、「[ライブラリを使用してユーザーとグループをサービス提供に割り当てる](#)」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。すでに割り当てられているIDをサブスクリバイバーが使用することを妨げるものではありません。
- 各Cloud Connectorは、インストールされている単一のフォレストからすべてのドメインを列挙して使用できます。

サブスクリバイバー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、サブスクリバイバーをオフリングに追加できます。Active Directoryグループを使用する場合、グループをオフリングに割り当てた後は、Citrix Cloud Japanを介した管理は不要です。

管理者が個々のサブスクリバイバーまたはサブスクリバイバーのグループをオフリングから削除すると、それらのサブスクリバイバー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サブスクリバイバーを削除する方法の詳細については、[Citrix Product Documentation Webサイト](#)でサービスのドキュメントを参照してください。

プライマリリソースの場所

プライマリリソースの場所とは、お客様のドメインとCitrix Cloud Japan間の通信で「最も優先される」ものとして指定するリソースの場所です。「プライマリ」として選択するリソースの場所には、お客様のドメインに対して最高のパフォーマンスと接続性を持つCloud Connectorが必要です。これにより、ユーザーはCitrix Cloud Japanにすばやくログオンできます。

プライマリリソースの場所を選択するプロセスは、Citrix Cloud JapanとCitrix Cloud (citrix.cloud.com)で同じです。詳細については、「[プライマリリソースの場所を選択する](#)」を参照してください。

通知

通知は、新しいCitrix Cloud Japanの機能やリソースの場所にあるマシンの問題など、管理者にとって関心のある問題やイベントに関する情報を提供します。通知は、Citrix Cloud Japan内の任意のサービスから送信されます。

通知の管理は、Citrix Cloud JapanとCitrix Cloud (citrix.cloud.com)で同じです。通知の詳細については、「[通知](#)」を参照してください。

システムログ

システムログには、Citrix Cloud Japanで発生したイベントのタイムスタンプ付きリストが表示されます。これらの変更は、組織の規制コンプライアンス要件を満たすため、またはセキュリティ分析をサポートするために、CSVファイルとしてエクスポートできます。

システムログの機能は、Citrix Cloud JapanとCitrix Cloud (citrix.cloud.com)で同じですが、いくつかの重要な制限があります。詳細については、「[システムログ](#)」を参照してください。

Citrix Cloud Japan管理者管理

管理者はCitrix Cloud Japanコンソールから管理されます。管理者の認証に使用するIDプロバイダーに応じて、個別に、またはグループを使用して管理者を追加できます。

デフォルトでは、新しい管理者にはCitrix Cloud Japanアカウントのすべての機能に対するフルアクセス権限が付与されます。アカウント管理を委任する方法については、この記事の「[管理者権限の構成](#)」を参照してください。

新しい管理者の追加

Citrix Cloud Japanは、管理者の認証に以下の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。個々の管理者のみの追加をサポートします。
- Microsoft Entra ID：個別に、およびMicrosoft Entra IDグループを介した管理者の追加をサポートします。Microsoft Entra IDグループの管理者は、Citrix DaaSへのアクセスのみに制限されます。詳細については、「[管理者グループの管理](#)」を参照してください。
- SAML 2.0：ADグループを介した管理者のみの追加をサポートします。ADグループの管理者は、Citrix DaaSの管理のみに制限されます。詳細については、「[SAMLをCitrix Cloud JapanのIDプロバイダーとして接続する](#)」を参照してください。

新しい管理者の追加には、以下のワークフローを使用します。

1. 管理者の認証に使用するIDプロバイダーを選択します。
2. IDプロバイダーに応じて、個々の管理者を招待するか、管理者が属するグループを選択します。
3. 組織における管理者の役割に合わせたアクセス権限を指定します。詳細については、この記事の「[管理者権限の構成](#)」を参照してください。

個々の管理者を招待する

個々の管理者を追加するには、Citrix Cloud Japanアカウントへの参加を招待します。管理者を追加すると、Citrixから招待メールが送信されます。管理者はサインインする前に、招待を承諾する必要があります。グループを介して追加された管理者は招待を受け取らず、追加後すぐにサインインできます。

招待メールは cloud@citrix.com から送信され、アカウントへのアクセス方法が説明されています。メールは送信日から5日間有効です。5日経過すると、招待リンクは期限切れになります。招待された管理者が期限切れのリンクを使用した場合、Citrix Cloud Japanはリンクが無効であることを示すメッセージを表示します。

「リンクが無効なメッセージ」 (</en-us/citrix-cloud-japan/media/onboarding-link-invalid.png>)

Citrix Cloud Japanは招待のステータスも表示するため、管理者が招待を承諾してCitrix Cloud Japanにサインインしたかどうかを確認できます。

「ステータス列が強調表示されたCitrix Cloudコンソール」 (</en-us/citrix-cloud-japan/media/admin-invite-status.png>)

管理者を招待するには

1. [Citrix Cloud Japan](#)にサインインした後、メニューから** [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。コンソールには、アカウント内の現在の管理者がすべて表示されます。
3. ** [管理者/グループの追加] **を選択します。
4. ** [管理者詳細] **で、使用するIDプロバイダーを選択します。Microsoft Entra IDを使用している場合、Citrix Cloud Japanは最初にサインインを求めることがあります。
5. ** [Citrix Identity] が選択されている場合は、ユーザーのメールアドレスを入力し、[次へ] **を選択します。

6. ** [Microsoft Entra ID] が選択されている場合は、追加するユーザーの名前を入力し、[次へ] **をクリックします。Microsoft Entra IDゲストユーザーの招待はサポートされていません。
7. [アクセス設定] で、管理者に適切な権限を構成します。[フルアクセス]（デフォルトで選択）では、Citrix Cloud Japanのすべての機能とサブスクライブされた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. 管理者詳細を確認します。変更を行うには、** [戻る] **を選択します。
9. ** [招待状を送信] **を選択します。Citrix Cloud Japanは、指定したユーザーに招待状を送信し、管理者をリストに追加します。

招待状を再送する

招待状を再送するには、コンソールの右端にある省略記号メニューから** [招待メールを再送] **を選択します。招待状を再送しても、招待状の有効期限が切れるまでの5日間の制限には影響しません。

Citrix Cloudコンソールで「招待メールを再送信」が強調表示されています(/en-us/citrix-cloud-japan/media/resent-invite-email.png)

新しいサインインリンクで招待を再送信する

元の招待メールの有効期限が切れて、管理者に新しいメールを送信したい場合は、Citrix Cloud Japanから管理者を削除し、再度招待してください。

管理者招待を承諾する

Citrix Cloud Japanアカウントに招待された場合、Citrix Cloud Japanから、組織IDとアカウントの顧客名を含むメールが送信されます。

招待を承諾するには、**サインイン**をクリックします。その後、ブラウザウィンドウが開きます。Citrixアカウントをまだお持ちでない場合は、パスワードを作成するページがブラウザに表示されます。すでにアカウントをお持ちの場合は、Citrix Cloud Japanから既存のパスワードを使用してサインインするよう求められます。

管理者グループを追加する

ADグループ（SAML認証の場合）またはMicrosoft Entra IDグループ（Microsoft Entra ID認証の場合）を使用して管理者を追加できます。詳細については、以下の記事を参照してください。

- [管理者グループを管理する](#)
- [SAMLをCitrix Cloud JapanのIDプロバイダーとして接続する](#)

管理者権限を構成する

Citrix Cloud Japanアカウントに管理者を追加する際、次のような異なるレベルのアクセス権を割り当てる必要がある場合があります。

- Citrix DaaS™のヘルプデスクアクセス
- 1つまたは複数の特定のクラウドサービスを管理するためのアクセス
- ライブラリやリソースの場所など、特定のCitrix Cloud Japan機能を管理するためのアクセス

委任管理を使用すると、組織内での役割に応じて、すべての管理者に必要なアクセス許可を構成できます。

コンソール権限

Citrix Cloud Japan管理コンソールへのカスタムアクセスを構成するには、以下の権限を使用します。

- **顧客ダッシュボード (表示のみ):** Citrix Service Provider (CSP) のみ。(/ja-jp/citrix-cloud/citrix-cloud-management/features-for-citrix-partners#customer-dashboard)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**へのアクセスを許可します。管理者は、このタブからCitrix Cloud Connector™ソフトウェアをダウンロードし、ドメイン内のサーバーにインストールすることで、Active Directoryドメインを追加できます。
- **ライブラリ:** ライブラリコンソールページへのアクセスを許可します。
- **ライセンス:** ライセンスコンソールページのクラウドサービスタブとライセンス済み展開タブへのアクセスを許可します。
- **通知:** 通知コンソールページへのアクセスを許可します。管理者はCitrix Cloudの通知を表示および却下できます。
- **リソースの場所:** リソースの場所コンソールページへのアクセスを許可します。管理者は、新しいリソースの場所を追加し、(/ja-jp/citrix-workspace/optimize-cvad/workspace-federated-authentication.html)ことができます。また、(/ja-jp/citrix-cloud-japan/install-configure/create-resource-location.html)や(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-updates.html)こともできます。
- **システムログ:** システムログコンソールページへのアクセスを許可します。管理者は(/ja-jp/citrix-cloud-japan/manage/system-log.html)ことができ、イベントをCSVファイルにエクスポートできます。
- **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を許可します。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、サイト集約の構成を行うことができます。詳細については、(/ja-jp/citrix-workspace)製品ドキュメントを参照してください。

既存の権限を変更するには

フルアクセス権を持つCitrix管理者のみが、他の管理者のアクセス許可を定義できます。

1. <https://citrix.citrixcloud.jp>でCitrix Cloud Japanにサインインします。
2. ページの左上隅にある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。
3. 「**管理者**」タブをクリックします。
4. 管理する管理者を見つけ、省略記号ボタンをクリックし、「**アクセスを編集**」を選択します。
5. 「**カスタムアクセス**」を選択します。
6. 必要に応じて、各権限を選択またはクリアします。
7. 「**保存**」をクリックします。

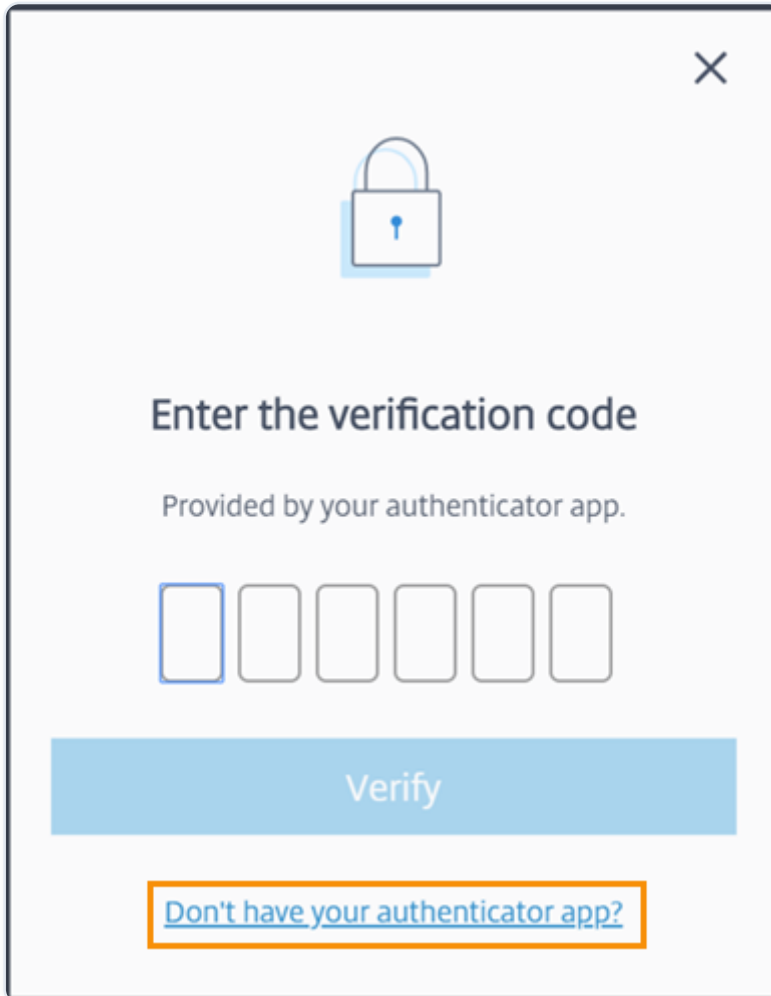
多要素認証用のデバイスを変更する

登録済みのデバイスを紛失した場合、Citrix Cloud Japanで別のデバイスを使用したい場合、または認証アプリをリセットした場合は、Citrix Cloud Japanの多要素認証に再登録できます。

注

- デバイスを変更すると、現在のデバイス登録が削除され、新しい認証アプリキーが生成されます。
- 元の登録と同じ認証アプリで再登録する場合は、再登録する前に認証アプリからCitrix Cloud Japanのエントリを削除してください。このエントリに表示されるコードは、再登録が完了すると機能しなくなります。再登録の前後にこのエントリを削除しないと、認証アプリに異なるコードを持つ2つのCitrix Cloud Japanエントリが表示され、Citrix Cloud Japanへのサインイン時に混乱を招く可能性があります。
- 新しいデバイスで再登録していて、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てインストールしてください。よりスムーズなエクスペリエンスのために、Citrixはデバイスを再登録する前に認証アプリをインストールすることをお勧めします。

1. Citrix Cloud Japanにサインインし、認証アプリからコードを入力します。

A screenshot of a verification code input screen. At the top right is a close button (X). Below it is a padlock icon. The main heading is "Enter the verification code". Below that is the text "Provided by your authenticator app.". There are six empty square boxes for entering the code. Below the boxes is a blue "Verify" button. At the bottom is a link "Don't have your authenticator app?" which is highlighted with an orange border.

認証アプリをお持ちでない場合は、「**認証アプリをお持ちでない場合**」をクリックし、サインインに役立つ回復方法を選択します。選択した回復方法に応じて、受け取った回復コードまたは未使用のバックアップコードを入力し、「**確認**」を選択します。

2. 複数の顧客組織の管理者である場合は、いずれかの顧客組織を選択します。
3. 右上のメニューから「**マイプロフィール**」を選択します。

マイプロフィールメニューリンク(/en-us/citrix-cloud-japan/media/console-my-profile-menu-link.png)

4. 「**認証アプリ**」で、「**デバイスの変更**」を選択します。 (/en-us/citrix-cloud-japan/media/admin-mfa-change-device-link.png)
5. デバイスの変更を確認するよう求められたら、「**はい、デバイスを変更します**」を選択します。
6. 認証アプリから確認コードを入力して、本人確認を行います。認証アプリをお持ちでない場合は、「**認証アプリをお持ちではありませんか？**」を選択し、復旧方法を選択します。選択した

復旧方法に応じて、受け取った確認コードまたは復旧コード、あるいは未使用のバックアップコードを入力します。「**確認**」を選択します。

- 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 Japan エントリを削除します。
- 新しいデバイスを登録していて、認証アプリをお持ちでない場合は、デバイスのアプリストアからダウンロードしてください。
- 認証アプリから、デバイスでQRコードをスキャンするか、手動でキーを入力します。
- 認証アプリから6桁の確認コードを入力し、「**コードを確認**」を選択します。

確認方法を管理する

重要:

Citrix Cloud Japan アカウントのセキュリティを確保するため、確認方法を正確な情報で最新の状態に保ってください。認証アプリへのアクセスを失った場合、これらの確認方法がアカウントへのアクセスを復旧できる唯一の方法です。

マイプロフィールコンソールの確認方法セクション(/en-us/citrix-cloud-japan/media/console-admin-mfa-verification-methods-section.png)

新しいバックアップコードを生成する

ワンタイム使用のバックアップコードを紛失したり、さらに生成する必要がある場合は、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。新しいバックアップコードを生成したら、安全な場所に保管してください。

- Citrix Cloud Japan にサインインし、認証アプリからコードを入力します。
- 複数の顧客組織の管理者である場合は、いずれかの顧客組織を選択します。
- 右上のメニューから、**My Profile** を選択します。
- 「**認証方法**」の「**バックアップコード**」で、「**バックアップコードの置き換え**」を選択します。
- 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。
- バックアップコードの置き換えを求められたら、**Yes, replace** を選択します。Citrix Cloud Japan 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。

7. **Download codes** 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、**I've saved these codes** を選択し、**Close** を選択します。

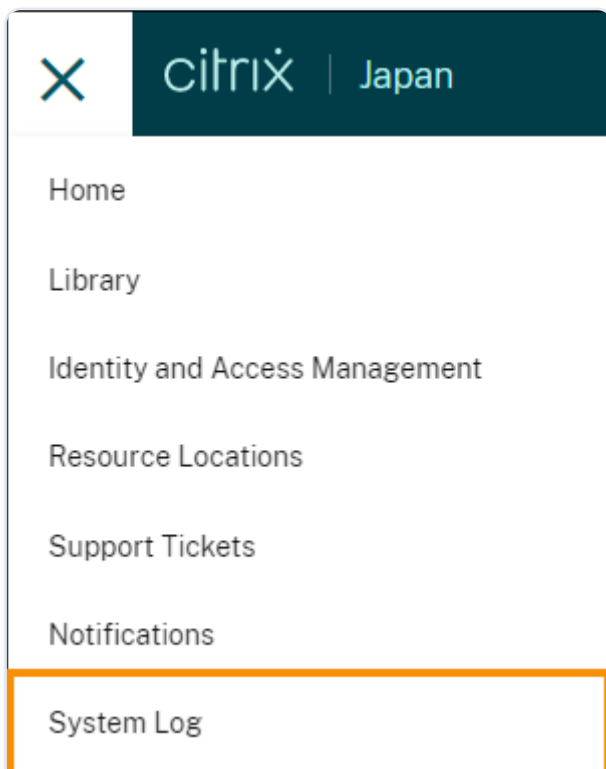
リカバリ用の電話番号を変更する

1. Citrix Cloud Japan にサインインし、認証アプリからコードを入力します。
2. 複数の顧客組織の管理者である場合は、多要素認証に最初に登録した顧客組織を選択します。
3. 右上のメニューから、**My Profile** を選択します。
4. 「認証方法」の「リカバリ電話」で、「リカバリ電話の変更」を選択します。
5. 使用する新しい電話番号を入力し、**Save** を選択します。

システムログ

システムログには、Citrix Cloud Japanで発生したイベントのタイムスタンプ付きリストが表示されます。これらの変更は、組織の規制コンプライアンス要件を満たすため、またはセキュリティ分析をサポートするために、CSVファイルとしてエクスポートできます。

システムログを表示するには、Citrix Cloud Japanメニューから **System Log** を選択します。



システムログデータの保持の詳細については、この記事の[データ保持](#)を参照してください。

制限事項

システムログはCitrix Cloud JapanとCitrix Cloud (citrix.cloud.com) で同じように機能しますが、Citrix Cloud Japanでは以下の項目は使用できません。

- SystemLog API
- システムログ用Splunkアドオン

ログに記録されたイベント

システムログは、特定のCitrix Cloud Japan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リストとキャプチャされたデータの詳細については、[システムログイベントリファレンス](#)を参照してください。

注：

システムログイベントリファレンスには、Citrix Cloudで発生するプラットフォームおよびサービス関連のイベントが含まれています。Citrix Cloud Japanで生成されるイベントは、リファレンス記事に記載されているイベントのサブセットです。Citrix Cloud Japanでサポートされている新しいイベントに関する通知については、[Citrix Cloud Japanの新機能](#)を参照してください。

システムログには、デフォルトで過去30日間に発生したイベントが表示され、最大90日まで表示されます。最新のイベントが最初に表示されます。

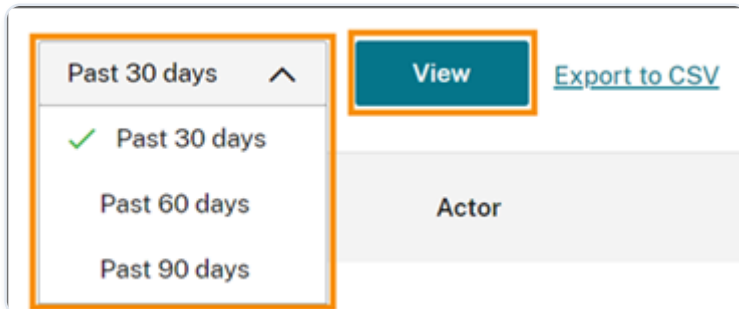
System Log			
Past 30 days View Export to CSV 1-32 of 32			
Date & Time	Actor	Event	Target
Feb 20, 2021 02:47:35 UTC	CwcSystem - administrator	Administrator roles or permissions updated	@citrix.com - administrator
Feb 19, 2021 11:49:51 UTC	@citrix.com - system	Secure client created	MSBI_Schedule - service
Feb 18, 2021 12:52:27 UTC	@citrix.com - administrator	'Full' Administrator invitation sent	@citrix.com - administrator
Feb 17, 2021 09:40:55 UTC	@citrix.com - system	Administrator created	@citrix.com - administrator
Feb 03, 2021 11:12:27 UTC	@citrix.com - administrator	Administrator access type updated, from 'Full' to 'Custom'	@citrix.com - administrator
Feb 02, 2021 07:29:29 UTC	@citrix.com - administrator	Administrator deleted	@citrix.com - administrator

表示されるリストには、次の情報が含まれます。

- イベントが発生した日時 (UTC)。

- 管理者やサービスプリンシパルなど、イベントを開始したアクター。アクターが**CwcSystem**のエントリは、Citrix Cloud Japanが操作を実行したことを示します。
- 管理者編集や新しいサービスプリンシパル作成など、イベントの簡単な説明。
- イベントのターゲット。ターゲットは、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。

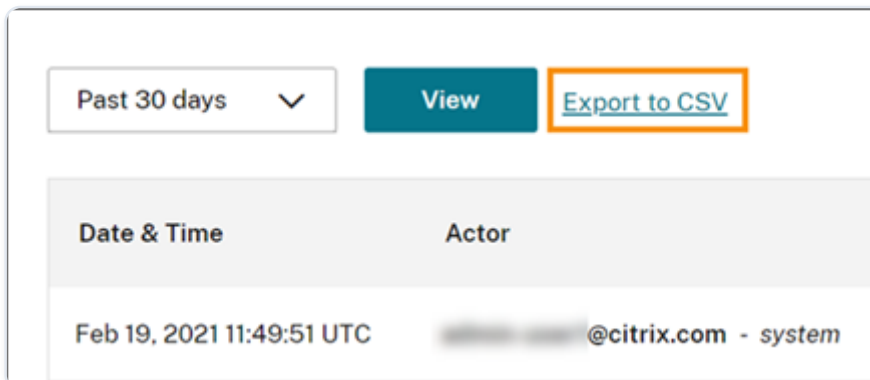
過去90日間に発生したイベントを表示するには、表示したい期間を選択してリストをフィルターし、**View**を選択します。



イベントのエクスポート

過去90日間に発生したシステムログイベントのCSVファイルをエクスポートできます。ダウンロードされるファイル名は、`SystemLog-CustomerName-OrgID-DateTimeStamp.csv` の形式に従います。

1. Citrix Cloud Japanメニューから、**System Log**を選択します。
2. 必要に応じて、イベントをエクスポートしたい期間を表示するようにリストをフィルターします。
3. **Export to CSV**を選択してファイルを保存します。



CSVファイルには、次の情報が含まれます。

- 各イベントのUTCタイムスタンプ
- イベントを開始したアクターの詳細（名前とアクターIDを含む）。

- イベントの種類やイベントのテキストなどのイベントの詳細
- ターゲットID、管理者名、またはサービスプリンシパルなどのイベントのターゲットの詳細。

データ保持

Citrix は、Citrix Cloud Japan が取得するシステムログデータの保持について、お客様と責任を共有します。

Citrix® は、イベントが記録されてから90日間、システムログレコードを保持します。

お客様は、組織のコンプライアンス要件を満たすために保持したいシステムログレコードをダウンロードし、これらのレコードを長期保存ソリューションに保存する責任があります。

パートナー向け Citrix Cloud Japan

Citrix Cloud Japan には、顧客とパートナーの両方のために設計されたサービス、機能、およびエクスペリエンスが含まれています。Citrix Cloud Japan のパートナーエクスペリエンスは、Citrix Cloud のパートナーエクスペリエンスと同じです。

パートナーは次の機能を活用できます。

- 顧客を Citrix Cloud Japan に接続するよう招待する。
- 試用版を含む顧客のサービス資格を表示する。
- 管理者コンソールを通じて、顧客ダッシュボードへのアクセスを有効または無効にする。
- 顧客ダッシュボードからライセンスの傾向を表示する。
- ライセンスコンソールを通じて、Citrix DaaS™ の資格に関する顧客のライセンスと使用状況を表示する。
- Citrix Cloud Japan 管理コンソールから顧客の通知を表示する。

パートナーエクスペリエンスの詳細については、「[Citrix Cloud for Partners](#)」を参照してください。

SDK

Citrix DaaS™ Remote PowerShell SDK は、複雑で反復的なタスクを自動化します。これにより、Studio ユーザーインターフェイスを使用せずに、Citrix DaaS (旧 Virtual Apps and Desktops) 環境をセットアップおよび管理するメカニズムが提供されます。

要件

マシンに PowerShell 3.0 以降がインストールされていることを確認してください。

Remote PowerShell SDK のインストールまたは削除

Citrix Cloud Japan で使用するために Remote PowerShell SDK をインストールするには：

1. インストーラーをダウンロードします: <https://download.apps.cloud.com/CitrixPoshSdk.exe>。
2. コマンド `CitrixPoshSdk.exe EnvironmentName=Japan` を実行します。このコマンドにより、SDK はデフォルトで Citrix Cloud Japan のコンテキストで実行できるようになります。

注:

または、SDK インストーラーを実行し、ダイアログに従ってインストールを完了することもできます。ただし、Get-XdAuthentication コマンドレットを使用して認証する際に、Citrix Cloud Japan 環境を指定する必要があります。この記事の「[Remote PowerShell SDK を実行するには](#)」を参照してください。

インストールログは %TEMP%\CitrixLogs\CitrixPoshSdk に作成されます。ログはインストールに関する問題の解決に役立ちます。

Remote PowerShell SDK をアンインストールするには：

1. プログラムの削除または変更を行う Windows 機能から、**Citrix DaaS Remote PowerShell SDK** を選択します。
2. 右クリックして、**アンインストール** を選択します。
3. ダイアログに従います。

Remote PowerShell SDK を実行するには

Remote PowerShell SDK は、そのリソースの場所にあるドメイン参加済みコンピューターで実行します。

1. PowerShell コマンドプロンプトを開きます。管理者として実行する必要はありません。
2. Citrix® スナップインを追加します: `asnp citrix.*`.
3. コマンド `Get-XdAuthentication` を実行して明示的に認証できます。または、最初の Remote PowerShell SDK コマンドを実行すると、Get-XdAuthentication と同じ認証が求められます。ただし、この記事の冒頭にある [Remote PowerShell SDK のインストールまたは削除](#) で説明されているように SDK をインストールしなかった場合は、コマンド `Get-XdAuthentication -EnvironmentName Japan` を使用して Citrix Cloud Japan に認証する必要があります。
4. PS SDK コマンドレットまたは PS SDK 自動化スクリプトの実行を続行します。スクリプトの例については、Citrix DaaS ドキュメントの [アクティビティの例](#) を参照してください。

注記:

- 一度認証されると、現在の PowerShell セッションでのリモートアクセスは 24 時間有効です。この時間を過ぎると、資格情報を入力する必要があります。
- Citrix は、この SDK のコマンドレットを Cloud Connector で実行しないことを推奨します。SDK の操作には Cloud Connector は関与しません。

サポートされているスナップインと無効になっているスナップインの完全なリストについては、Citrix DaaS ドキュメントの [サポートと制限事項](#) を参照してください。

Citrix Cloud Japanサービス

Citrix Cloud JapanにおけるCitrix Gatewayサービス

Citrix Gatewayサービスは、Citrix Cloud Japanで一般提供されています。すべての顧客トラフィックは、専用のCitrix Cloud Japan PoPのみを通過します。詳細については、「[CTX340508: Citrix Gateway Service Points of Presence \(PoPs\) - Citrix Cloud Japan](#)」を参照してください。Citrix DaaS（旧Virtual Apps and Desktopsサービス）を使用している場合、Citrix Cloud Japan内でHDXプロキシ用のゲートウェイサービスを使用できるようになりました。Citrix Gatewayサービスは、東京と大阪の2つのリージョン（PoP）で利用できます。

サポートされているCitrix Gatewayサービス機能

以下は、Citrix Cloud JapanでCitrix Gatewayサービスがサポートする機能の一部です。

HDX™ プロキシ

Citrix Gatewayサービス内のHDXプロキシ機能は、Citrix Virtual Apps and Desktopsへの安全で信頼性の高いアクセスを提供します。

高可用性

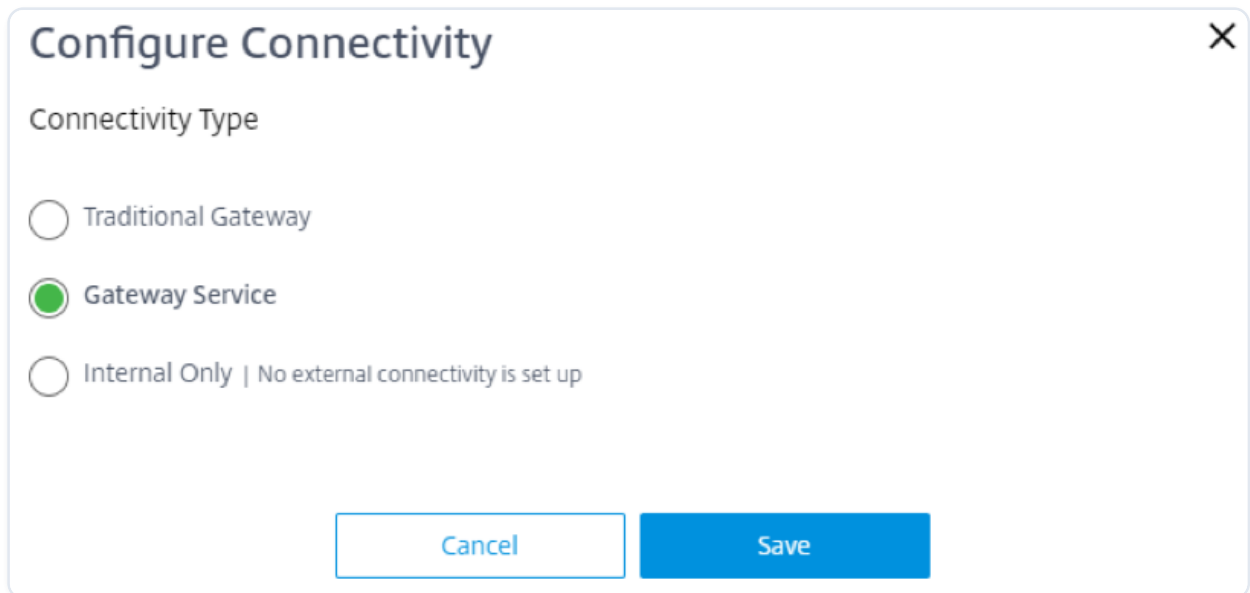
Citrix Gatewayサービスによる多層的な回復性アプローチは、あらゆるレベルで回復性を提供します。特定のCitrix GatewayサービスPOP内では、サービスを構成するマイクロサービスとテナントが高可用性形式で展開されます。コンポーネントはN+1モデルで展開されます。このモデルでは、すべてのコンポーネントがロードバランシングされ、障害が発生した場合でもスタンバイによる迅速なフェールオーバーが可能です。まれに、POP内の特定のコンポーネントのすべてのサービスが停止した場合、Citrix Gatewayサービスは自身をダウンとマークします。これにより、DNSサーバーはユーザーを次に近いPOPにリダイレクトし、POPレベルの高可用性を提供します。

最適なゲートウェイルーティング

Citrix Gatewayサービスは日本全国の複数のリージョンに展開されており、最高のパフォーマンスを得るために最適なPOPを選択するメカニズムが必要です。最適なゲートウェイルーティング、または近接ルーティングと呼ばれるDNSベースのサービスは、エンドユーザーがCitrix Gatewayサービスに接続しようとしたときに、最も近いPOPロケーションを返すために使用されます。このDNSサービスは、クエリの送信元IPアドレスをメタデータのの一つとして使用し、最も近いCitrix GatewayサービスPOPのIPアドレスを返します。

Citrix Gatewayサービスを有効にする方法

1. 「リソースの場所」ページから、構成するリソースの場所を見つけて「Gateway」をクリックします。「接続の構成」ダイアログが表示されます。

A screenshot of the 'Configure Connectivity' dialog box. It has a title bar with a close button (X) in the top right corner. Below the title bar, the text 'Connectivity Type' is displayed. There are three radio button options: 'Traditional Gateway' (unselected), 'Gateway Service' (selected, indicated by a green dot), and 'Internal Only | No external connectivity is set up' (unselected). At the bottom of the dialog, there are two buttons: 'Cancel' (light blue) and 'Save' (dark blue).

2. 外部ユーザーにアプリケーションとデスクトップへの安全なアクセスを提供するには、**Citrix Gatewayサービス**をクリックします。
3. **保存**をクリックします。

Citrix Cloud Connector™ 接続要件

Citrix Cloud Connector は、Microsoft Windows Server 上で実行される一連のサービスを展開するソフトウェアパッケージです。Cloud Connector をホストするマシンは、Citrix Cloud Japan で使用するリソースが存在するネットワーク内に配置されます。Cloud Connector は Citrix Cloud Japan に接続し、必要に応じてリソースを運用および管理できるようにします。Citrix リソースの場所/Cloud Connector の詳細については、「Cloud Connector 共通サービス接続要件」を参照してください。

ゲートウェイサービスを使用するには、次の URL にアクセスする必要があります: `https://*.*.nssvc.jp`。

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

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

オンプレミスの Citrix Gateway からクラウドベースの Citrix Gateway サービスへの移行

オンプレミスの Citrix Gateway からクラウドベースの Citrix Gateway サービスに移行できます。

詳細については、「[HDX プロキシ用の Citrix Gateway サービスへの Citrix Gateway の移行](#)」を参照してください。

Citrix Cloud Japanドキュメント履歴

次の表に、Citrix Cloud Japanの製品ドキュメントに対する重要な変更点を示します。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
13 May 2024	コンソールで構成可能な非アクティブタイムアウトを追加しました	「コンソールで構成可能な非アクティブタイムアウト」を追加しました
27 Feb 2024	クラウドサービス用 Connector Applianceおよび Connector Applianceを使用したActive Directoryを追加	「クラウドサービス用の Connector Appliance」および「Connector Applianceを使用したActive Directory」を追加しました
20 Nov 2023	サービスの購入セクションを削除	ヘルプとサポートの利用から「サービスの購入」セクションを削除しました
20 Nov 2023	Citrix Cloudのサービス正常性セクションを追加	Citrix Cloudのサービス正常性セクションを追加しました
15 Nov 2023	Azure Active Directoryの権限の更新	Citrix Cloud Japan用のAzure Active Directoryの権限からDirectory.Read.Allの権限を削除しました
16 Oct 2023	Cloud Connectorの更新	機能上の既知の問題により、Cloud Connectorの接続性チェックユーティリティへの参照を削除しました： CTX260337 - Cloud Connector Connectivity Check Utility

日付	変更	説明
09 Oct 2023	App Protectionの詳細を追加	サポートされているサービスの機能の可用性にApp Protectionの詳細を追加しました
11 Aug 2022	管理者の管理の更新	個別のCitrix Cloud Japan管理者を追加するためのワークフローを更新しました： Citrix Cloud Japan管理者を管理する
25 Jul 2022	SAML IDを更新	ADグループのSAML認証のサポートを追加しました： SAMLをIDプロバイダーとしてCitrix Cloud Japanに接続する
06 Jul 2022	リージョンに依存しないデータの新しいセクション	リージョンに依存しないデータの使用に関するセクションを追加しました： リージョンに依存しないデータ
23 Jun 2022	IDプロバイダーとしてのAzure ADに関する新しい記事	Azure ADテナントとの接続に必要なアプリの権限について説明する新しい記事を追加しました： Citrix Cloud Japan用のAzure Active Directoryの権限
04 May 2022	ライセンスに関する新しい記事	ライセンスに関する新しい記事を追加しました： ライセンス
30 Mar 2022	システムログの一般提供	システムログが一般提供されるようになりました： システムログ
16 Nov 2021	IDプロバイダーとしてのAzure ADに関する記事の更新	Virtual Apps and Desktops サービスを管理するためにAzure ADグループを使用して新しい管理者を追加するため

日付	変更	説明
		のサポートについての記載を追加しました： Azure ADからCitrix Cloud Japanに管理者を追加する
16 Nov 2021	管理者の追加に関する更新	Virtual Apps and Desktops サービスを管理するために、Azure ADグループを使用して新しい管理者を追加するためのサポートについての記載を追加しました： 個別の管理者を招待する
08 Oct 2021	サービス機能の可用性に関する記事の更新	Workspace Environment Managementサービスのセクションを新規追加しました： サービスの機能の可用性
30 Sep 2021	サービス機能の可用性に関する新しい記事	サポートされているサービスでの機能の可用性について説明する新しい記事を追加しました： サービスの機能の可用性
30 Sep 2021	サービス接続の記事を更新	Citrix GatewayおよびCitrix Workspace接続のセクションを追加しました： サービス接続要件
30 Sep 2021	Gatewayサービスの新しい記事	Citrix Gatewayサービスの有効化に関する新しい記事を追加しました： Citrix Cloud JapanでのCitrix Gatewayサービス
30 Sep 2021	新しいIDプロバイダー	Citrix GatewayをIDプロバイダーとして設定するための新しい記事を追加しました： オンプレミスのCitrix GatewayをIDプロバイダーとして接続

日付	変更	説明
30 Sep 2021	Oktaサポートの新しい記事	Citrix GatewayをIDプロバイダーとして設定するための新しい記事を追加しました： OktaをIDプロバイダーとして接続
30 Sep 2021	サポートされているIDプロバイダーの新しい記事	サポートされているIDプロバイダーと認証の概要を追加しました： IDおよびアクセス管理
30 Sep 2021	ワークスペースのセットアップに関する新しい記事	Citrix Workspaceの機能とセットアップタスクの概要に関する記事を追加しました： ワークスペースのセットアップ
29 Jun 2021	システムログ機能に関する新しい記事	Citrix Cloud Japanでの特定イベントのログ記録に関する新しいTechnical Preview記事を追加しました： システムログ
04 Dec 2020	初版	Citrix Cloud Japanがリリースされました。