Citrix Secure Private Access

Machine translated content

Disclaimer

Contents

新機能

June 19, 2024

2024 年 **6** 月 **11** 日

- ポリシー・モデリング・ツール

  ポリシーモデリングツール ([アクセスポリシー**] > [**ポリシーモデリング]) を使用すると、管理者は管理コンソール内から構成の問題の分析とトラブルシューティングを行うことができます。詳細については、ポリシーモデリングツールを参照してください。

- 診断ログチャートのフィルターのサポート

  診断ログチャートのフィルターオプションを使用すると、管理者はアプリの種類、カテゴリ、説明などのさまざまな条件に基づいて検索を絞り込むことができるため、ログの分析やトラブルシューティングが容易になります。詳細については、「診断ログ」を参照してください。

2024 年 **3** 月 **13** 日

- アクティブなユーザーセッションの終了と無効ユーザーリストへのユーザーの追加をサポート

  管理者はすべてのアクティブなエンドユーザーセッションをすぐに終了し、ユーザーを無効ユーザーリストに追加できるようになりました。この無効なユーザーリストにユーザーを追加すると、すべてのアクティブな Secure Private Access アプリケーションセッションが終了し、今後のアプリケーションアクセスがブロックされます。詳細については、「アクティブなユーザーセッションを終了し、無効ユーザーリストへのユーザーの追加」を参照してください。

2024 年 **2** 月 **12** 日

- ブラウザとウイルス対策スキャンの一般提供状況

  デバイスポスチャ サービスがサポートするブラウザとウイルス対策スキャンが一般公開されました。詳細については、「デバイスポスチャでサポートされるスキャン」を参照してください。

2024 年 **1** 月 **23** 日

- デバイスポスチャサービスによるデバイス証明書チェックの一般提供

  デバイスポスチャ サービスによるデバイス証明書チェックが一般利用できるようになりました。詳しくは、「デバイスポスチャサービスによるデバイス証明書チェック」を参照してください。

2023 年 12 月 20 日

- オンプレミスでの **Secure Private Access** の一般提供

  オンプレミス向けの Citrix Secure Private Access が一般公開されました。詳しくは、「新機能」を参照してください。

2023 年 10 月 16 日

- **Secure Private Access** オンプレミスソリューションプレビュー機能

  Secure Private Access のオンプレミス・ソリューションでは、次の機能が提供されるようになりました:

  - 初回セットアップ用の管理 UI。
  - アプリケーションとアクセスポリシーを設定するための管理 UI。
  - ログダッシュボード。

  詳細については、「オンプレミスの Secure Private Access」を参照してください。

- デバイスポスチャサービスのプレビュー機能

  デバイスポスチャサービスは次のチェックをサポートするようになりました:

  - デバイスポスチャサービスが IGEL プラットフォームでサポートされるようになりました。
  - デバイスポスチャ サービスがジオロケーションとネットワークロケーションのチェックをサポートするようになりました。

  詳細については、「デバイスポスチャ」を参照してください。

2023 年 9 月 11 日

- **Microsoft Intune** とのデバイスポスチャ統合の一般公開

  Microsoft Intune とのデバイスポスチャ統合が一般公開されました。詳しくは、「Microsoft Intune とデバイスポスチャの統合」を参照してください。

2023 年 8 月 30 日

- デバイスポスチャサービス用 **Citrix Endpoint Analysis** クライアントの管理

  EPA クライアントは NetScaler およびデバイスポスチャと一緒に使用できます。NetScaler とデバイスポスチャと併用する場合、EPA クライアントを管理するにはいくつかの設定変更が必要です。詳しくは、「デバイスポスチャサービス用 Citrix Endpoint Analysis クライアントの管理」を参照してください。

2023 年 8 月 28 日

- **iOS** プラットフォームでのデバイスポスチャサービスのサポート

  デバイスポスチャサービスが iOS プラットフォームでサポートされるようになりました。詳細については、「デバイスポスチャ」を参照してください。

  この機能はプレビュー段階です。

2023 年 8 月 22 日

- **Citrix** デバイスポスチャサービスによるデバイス証明書チェック

  Citrix デバイスポスチャサービスは、エンドデバイスの証明書を企業の認証局と照合してエンドデバイスが信頼できるかどうかを確認することで、Citrix DaaS および Secure Private Access リソースへのコンテキストアクセス (スマートアクセス) を有効にできるようになりました。詳しくは、「デバイスポスチャサービスによるデバイス証明書チェック」を参照してください。

  この機能はプレビュー段階です。

2023 年 8 月 17 日

- **Citrix DaaS** モニターのデバイスポスチャイベント

  デバイスポスチャサービスのイベントと監視ログを DaaS Monitor で検索できるようになりました。詳しくは、「Citrix DaaS モニターのデバイスポスチャイベント」を参照してください。

2023 年 6 月 7 日

- オンプレミスの **Secure Private Access** を設定するためのツール

  シンプルなユーザーインターフェイスを使用して、オンプレミスソリューション用の Secure Private Access を構成できるようになりました。構成ツールを Citrix Virtual Apps and Desktops の Delivery Controller で実行すると、SaaS または Web アプリケーションをすばやく作成できます。さらに、このツールを使用して、アプリケーション制限、トラフィックルーティング、および NetScaler Gateway の設定を設定できます。詳細については、/en-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.htmlを参照してください。

2023 年 5 月 29 日

- 複数のルールを含むアクセスポリシーの作成が一般に利用可能に

1 つのポリシー内で、複数のアクセスルールを作成し、さまざまなユーザーまたはユーザーグループにさまざまなアクセス条件を設定できます。これらのルールは、HTTP/HTTPS アプリケーションと TCP/UDP アプリケーションの両方に、すべて 1 つのポリシー内で個別に適用できます。詳細については、「複数のルールを含むアクセスポリシーの設定」を参照してください。

[SPA-746]

2023 年 4 月 10 日

- アプリケーションディスカバリー

  アプリケーション検出機能により、管理者は組織内の Web アプリやクライアントサーバーアプリ（TCP および UDP ベースのアプリ）などの内部のプライベートアプリケーションと、それらのアプリケーションにアクセスしているユーザーを把握できます。管理者は、ドメイン (ワイルドカードドメイン) または IP サブネットの範囲を指定してアプリを検索できます。詳細については、「アプリケーション検出」を参照してください。

  [ACS-2325]

2023 年 3 月 29 日

- オンプレミス導入用の **Secure Private Access** ソリューション

  Citrix StoreFront および NetScaler Gateway のお客様は、オンプレミス展開向けの Citrix Secure Private Access ソリューションを使用して、Citrix Virtual Apps and Virtual Desktops とともに Web アプリや SaaS アプリにシームレスにアクセスできるようになりました。詳細については、「オンプレミスの Secure Private Access」を参照してください。

  [SPAOP-1]

2023 年 3 月 7 日

- **DNS** サフィックスを構成する

  Citrix Secure Private Access サービスの DNS サフィックス機能は、以下の用途に使用できます。

  - Citrix Secure Access クライアントが、バックエンドサーバーの DNS サフィックスドメインを追加して、非完全修飾ドメイン名（ホスト名）を完全修飾ドメイン名（FQDN）に変換できるようにします。
  - 管理者が IP アドレス（IP CIDR/IP 範囲）を使用してアプリケーションを設定できるようにします。これにより、エンドユーザーは、DNS サフィックスドメインの対応する FQDN を使用してアプリケーションにアクセスできるようになります。

  詳細については、「FQDN を IP アドレスに変換する DNS サフィックス」を参照してください。

  [ACS-2490]

2023 年 1 月 23 日

- デバイスポスチャサービス

  Citrix デバイスポスチャサービスは、管理者が Citrix DaaS（仮想アプリおよびデスクトップ）または Citrix Secure Private Access リソース（SaaS、Web アプリ、TCP、および UDP アプリ）にアクセスするためにエンドデバイスが満たす必要のある特定の要件を管理者が適用できるようにするクラウドベースのソリューションです。詳細については、「デバイスポスチャ」を参照してください。

  [AAUTH-90]

- **Microsoft** エンドポイントマネージャーとデバイスポスチャの統合

  デバイスポスチャサービスが提供するネイティブスキャンに加えて、デバイスポスチャサービスは他のサードパーティソリューションと統合することもできます。デバイスポスチャは Windows および macOS 上の Microsoft エンドポイントマネージャ (MEM) と統合されています。詳細については、「Microsoft Endpoint Manager とデバイスポスチャの統合」を参照してください。

  [ACS-1399]

2022 年 12 月 22 日

- **Citrix Workspace** アプリ経由でログインしたユーザーのワークスペース **URL** のシングルサインオンサポート

  Citrix Secure Access クライアントは、すでに Citrix Workspace アプリ経由でログインしている場合、ワークスペース URL のシングルサインオンをサポートするようになりました。この SSO 機能により、複数の認証が回避されるため、ユーザーエクスペリエンスが向上します。詳細については、「Workspace URL のシングルサインオンサポート」を参照してください。

  [ACS-1888]

- アクセスポリシーを使用してアプリへのアクセスを有効にする

  ユーザーにアプリへのアクセスを許可するには、管理者はエンドユーザーがアプリを利用できるように、一致するユーザーサブスクリプションリストを含むアクセスポリシーを作成する必要があります。以前は、アクセスを有効にするには、管理者がユーザーをサブスクライバーとして追加する必要がありました。詳細については、「アクセスポリシーの作成」を参照してください。

  [ACS-3018]

2022 年 10 月 3 日

- アプリへのアクセスを許可するアクセスポリシー

  アプリ登録者設定オプションは、設定ウィザードのアプリケーションセクションから削除されました。ユーザーにアプリへのアクセスを許可するには、管理者がアクセスポリシーを作成する必要があります。アクセス

ポリシーでは、管理者がアプリの利用者を追加し、セキュリティコントロールを設定します。詳細については、「アクセスポリシーの作成」を参照してください。

[ACS-3018]

- **UDP** アプリのサポート

  Secure Private Access サービスが UDP アプリへのアクセスをサポートするようになりました。詳細については、「プレビュー機能」を参照してください。

  [ACS-1430]

2022 年 9 月 9 日

- ユーザーリスクスコアに基づくアダプティブアクセス

  管理者は、Citrix Analytics for Security（CAS）が提供するユーザーリスクスコアを使用してアダプティブアクセスポリシーを構成できるようになりました。詳細については、「ユーザーリスクスコアに基づくアダプティブアクセス」を参照してください。

  [ACS-877]

- ユーザーのネットワークロケーションに基づくアダプティブアクセス

  管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいてアダプティブアクセスポリシーを設定できるようになりました。ロケーションは、ユーザーがアプリケーションにアクセスしている国でも、ユーザーのネットワークロケーションでもかまいません。詳しくは、「場所に基づくアダプティブアクセス」を参照してください。

  [ACS-99]

- アダプティブアクセスポリシービルダーの強化

  アプリへのアクセスは、設定した条件が満たされた後にのみ有効になるようになりました。アプリのサブスクリプションだけでは、顧客はアプリケーションにアクセスできません。管理者は、アプリのサブスクリプションに加えてアプリへのアクセスを提供するためのアクセスポリシーを追加する必要があります。また、ユーザーまたはグループは、アプリにアクセスするために満たす必要があるアクセスポリシーの必須条件です。詳細については、「アクセスポリシーの作成」を参照してください。

  [ACS-1850]

- **SaaS/Web** アプリへのファイルのアップロードを制限する

  この機能により、顧客管理者は、ビジネスクリティカルなアプリケーションにファイルをアップロードできるユーザーを制御できます（許可または制限）。これにより、権限のあるユーザーのみがアプリケーションにファイルをアップロードできます。詳細については、「アクセスポリシーの作成」を参照してください。

  [ACS-655]

- ダッシュボードの強化

  Secure Private Access ダッシュボードでは、アプリの使用状況、上位のアプリユーザー、アクセスされた上位のアプリ、診断ログなど、複数のユーザー指標を詳細に確認できるようになりました。詳細については、「ダッシュボード」を参照してください。

  [ACS-2480]

- ライブラリ非推奨

  Secure Private Access アプリケーションは、Citrix Cloud Library 内では表示されなくなりました。Secure Private Access が設定されたすべてのアプリケーションは、Secure Private Access サービスタイル内のアプリケーションセクション内にあります。これにより、管理者はアプリケーションを簡単にナビゲート、編集、構成できます。

  [ACS-1546]

- **Secure Private Access** の監査ログ

  Citrix Secure Private Access サービス関連のイベントが、**Citrix Cloud >** システムログに記録されるようになりました。詳しくは、「監査ログ」を参照してください。

  [ACS-876]

- エンタープライズ **Web** および **SaaS** アプリアクセスの診断ログ

  Citrix Secure Private Access イベントは、Citrix Analytics と統合されました。Citrix Analytics は、管理者がイベントにアクセスしてダウンロードできるようにするパブリックエンドポイントを提供します。これらのイベントには、PowerShell スクリプトを使用してアクセスできます。詳しくは、「エンタープライズ Web および SaaS アプリアクセスの診断ログ」を参照してください。

  [ACS-805]

- トラブルシューティングガイド

  管理者はトラブルシューティングガイドを使用して構成関連の問題を解決できます。詳しくは、「アプリ関連の問題のトラブルシューティング」を参照してください。

  [ACS-2719]

2022 年 **7** 月 **15** 日

- アクセスポリシーが設定されている場合にのみアプリケーションへのアクセスを有効にする

  アプリへのアクセスは、管理者がアプリのサブスクリプションに加えてアクセスポリシーを追加した後にのみ有効になりました。アプリのサブスクリプションだけでは、アプリケーションにアクセスできません。この変更により、管理者はユーザー、場所、デバイス、リスクなどのコンテキストに基づいて適応型セキュリティを適用できます。管理者は、既存のアプリケーションセキュリティ制御とアクセスポリシーを新しいアクセスポ

リシーフレームワークに移行する必要があります。詳しくは、「アプリのセキュリティ制御とアクセスポリシーの移行」を参照してください。

[ACS-1850]

2022 年 6 月 1 日

- アダプティブ認証サービス

  アダプティブ認証が一般公開されました (GA)。アダプティブ認証の詳細については、「アダプティブ認証サービス」を参照してください。

  [CGS-6510]

2022 年 4 月 4 日

- リブランディングの変更

  Citrix Secure Workspace Access サービスは、Citrix Secure Private Access サービスにブランド変更されました。

  [ACS-2322]

- 簡単なオンボーディングとセットアップのための管理者向けガイド付きワークフロー

  SaaS アプリ、内部 Web アプリ、TCP アプリへのゼロトラストネットワークアクセスを段階的に設定するプロセスにより、Secure Private Access の管理作業が新しく簡素化されました。Adaptive Authentication、ユーザーサブスクリプションを含むアプリケーション、アダプティブアクセスポリシーなど、単一の管理コンソール内での設定が含まれます。詳しくは、「管理者ガイドによる簡単なオンボーディングとセットアップのワークフロー」を参照してください。

  この機能は現在一般提供されています (GA)。

  [ACS-1102]

- **Secure Private Access** ダッシュボード

  Secure Private Access ダッシュボードでは、管理者は上位のアプリ、上位ユーザー、コネクタの正常性ステータス、帯域幅の使用状況を完全に把握し、消費する場所を 1 か所で確認できます。このデータは Citrix Analytics から取得されます。詳しくは、「Secure Private Access ダッシュボード」を参照してください。

  この機能は現在一般提供されています (GA)。

  [ACS-1169]

- エンタープライズ **Web** アプリへの直接アクセス

顧客は、Chrome、Firefox、Safari、Microsoft Edge などのネイティブ Web ブラウザーから直接、内部 Web アプリへのゼロトラストネットワークアクセス（ZTNA）を有効にできるようになりました。詳しくは、「エンタープライズ Web アプリへの直接アクセス」を参照してください。

この機能は現在一般提供されています (GA)。

- **TCP/HTTPS** アプリへの **ZTNA** エージェントベースのアクセス

  Citrix 顧客は、内部 Web アプリケーションに加えて、すべてのクライアントサーバーアプリケーションと IP/ポートベースのリソースに対してゼロトラストネットワークアクセス（ZTNA）を有効にできるようになりました。詳しくは、「クライアントサーバーアプリのサポート」を参照してください。

  この機能は現在一般提供されています (GA)。

  [ACS-970]

- エンタープライズ **Web**、**TCP**、**SaaS** アプリケーションのアダプティブアクセスとセキュリティ制御

  Citrix Secure Private Access サービスのアダプティブアクセス機能は、アプリケーションへの安全なアクセスを提供する包括的なゼロトラストネットワークアクセス（ZTNA）アプローチを提供します。アダプティブアクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリに、きめ細かなレベルでアクセスできるようになります。ここで「コンテキスト」という用語は次のことを指します。

  - ユーザーとグループ (ユーザーとユーザーグループ)
  - デバイス (デスクトップまたはモバイルデバイス)
  - ロケーション (ジオロケーションまたはネットワークロケーション)
  - デバイスポスチャ (デバイスポスチャチェック)
  - リスク（ユーザーリスクスコア）

  詳しくは、「エンタープライズ Web、TCP、および SaaS アプリケーションのアダプティブアクセスとセキュリティ制御」を参照してください。

  この機能は現在一般提供されています (GA)。

  [ACS-878、ACS-879、ACS-882]

- **Secure Private Access** の監査ログ

  Citrix Secure Private Access サービス関連のイベントが、**Citrix Cloud >** システムログに記録されるようになりました。詳しくは、「監査ログ」を参照してください。

  この機能は現在一般提供されています (GA)。

  [ACS-876]

- エンタープライズ **Web** および **SaaS** アプリアクセスの診断ログ

  Citrix Secure Private Access イベントは、Citrix Analytics と統合されました。Citrix Analytics は、管理者がイベントにアクセスしてダウンロードできるようにするパブリックエンドポイントを提供します。これら

のイベントには、PowerShell スクリプトを使用してアクセスできます。詳しくは、「エンタープライズ Web および SaaS アプリアクセスの診断ログ」を参照してください。

この機能は現在一般提供されています (GA)。

[ACS-805]

- アダプティブ認証サービス

  Citrix Cloud のお客様は、Citrix Workspace を使用して Citrix Virtual Apps and Desktops にアダプティブ認証を提供できるようになりました。アダプティブ認証は、Citrix Workspace にログインしている顧客とユーザーに高度な認証を可能にする Citrix Cloud サービスです。アダプティブ認証サービスは、Citrix が管理し、Citrix Cloud がホストする ADC です。詳細については、「アダプティブ認証サービス」を参照してください。

  この機能はプレビュー段階です。

  [CGS-6510]

2022 年 2 月 16 日

- クライアントサーバーアプリのサポート Citrix Secure Private Access 内のクライアントサーバーアプリケーションのサポートにより、従来の VPN ソリューションへの依存を排除して、リモートユーザーにすべてのプライベートアプリへのアクセスを提供できるようになりました。

  詳しくは、「クライアント/サーバーアプリのサポート-プレビュー」を参照してください。

  [ACS-870]

2021 年 10 月 11 日

- **Citrix Gateway** サービスタイルを **Citrix Cloud** の単一の **Secure Private Access** に統合する

  Citrix Gateway サービスタイルは、Citrix Cloud の単一の Secure Private Access にマージされました。

  - Citrix Workspace Essentials や Citrix Workspace Standard を含むすべての Secure Private Access の顧客は、Web フィルタリングポリシーに加えて、SaaS およびエンタープライズ Web アプリケーション、強化されたセキュリティ制御、コンテキストポリシーを構成するために、1 つの Secure Private Access タイルを使用できるようになりました。
  - すべての Citrix DaaS ユーザーは、ワークスペース構成から Citrix Gateway サービスを HDX プロキシとして引き続き有効にすることができます。ただし、ゲートウェイサービスタイルから Citrix Gateway サービスを有効にするショートカットは削除されます。Citrix Gateway サービスは、［ワークスペース構成］**>**［アクセス］**>**［外部接続］から有効にすることができます。詳しくは、「外部接続」を参照してください。それ以外で、機能に変更はありません。

  [NGSWS-16761]

2021 年 7 月 30 日

- ユーザーの地理的位置に基づいて、エンタープライズ **Web** および **SaaS** アプリケーションのコンテキストに応じたアクセスとセキュリティ制御

  Citrix Secure Private Access サービスは、ユーザーの地理的位置に基づいて、エンタープライズ Web および SaaS アプリへのコンテキストアクセスをサポートするようになりました。

  [ACS-833]

- **Citrix Workspace** ポータルから特定の **Web** アプリまたは **SaaS** アプリを非表示にするオプション

  管理者は、特定の Web アプリまたは SaaS アプリを Citrix Workspace ポータルから非表示にできるようになりました。アプリが Citrix Workspace ポータルから非表示になっている場合、Citrix Gateway サービスは列挙中にこのアプリを返しません。ただし、ユーザーは非表示のアプリには引き続きアクセスできます。

  [ACS-944]

2021 年 6 月 9 日

- アプリトラフィックをルーティングするルールを定義するルートテーブル

  管理者は、ルートテーブルを使用して、アプリケーショントラフィックをインターネットに直接ルーティングするか、Citrix Gateway Connector を介してルーティングするルールを定義できるようになりました。管理者は、トラフィックフローの定義方法に応じて、アプリケーションのルートタイプを [外部]、[内部]、[内部バイパスプロキシ]、または [ゲートウェイコネクタ経由外部] として定義できます。

  [ACS-243]

2021 年 5 月 22 日

- エンタープライズ **Web** および **SaaS** アプリケーションへのコンテキストに応じたアクセス

  Citrix Secure Private Access サービスのコンテキストアクセス機能は、アプリケーションへの安全なアクセスを提供する包括的なゼロトラストアクセスアプローチを提供します。コンテキストに応じたアクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリへのきめ細かなレベルのアクセスを提供できます。ここでの「コンテキスト」という用語は、ユーザー、ユーザーグループ、およびユーザーがアプリケーションにアクセスしているプラットフォーム (モバイルデバイスまたはデスクトップコンピュータ) を指します。

  [ACS-222]

- **Citrix Gateway Connector** のユーザーインターフェイスのリブランディング

  Citrix Cloud Gateway Connector のユーザーインターフェイスは、Citrix ブランド化ガイドラインに従ってブランド変更されます。

  [NGSWS-17100]

2021 年 5 月 1 日

- **Citrix Secure Private Access** サービスのデータストアからの顧客データの削除

  バックアップを含む顧客データは、サービス資格の有効期限が 90 日経過すると、Citrix Secure Private Access サービスデータストアから削除されます。

  [ACS-388]

- **Azure AD** から **Citrix Workspace** にドメインをフェデレートするための簡略化された手順

  Azure AD から Citrix Workspace アプリにドメインをフェデレートする手順が簡素化され、Citrix WorkCitrix Workspace でのオンボーディングが高速になりました。ドメインフェデレーションは、シングルサインオンページから Citrix Gateway サービスのユーザーインターフェイスで実行できるようになりました。

  [ACS-351]

- 接続性テストツールの機能強化

  Citrix Gateway Connector の接続テストツールは、タイムアウトエラーを処理し、必要なログを生成するように拡張されました。

  [NGSWS-17212]

2021 年 3 月 15 日

- プラットフォームの機能強化

  お客様の管理構成を Citrix Gateway Connector に伝播する信頼性が向上するため、さまざまなプラットフォームが強化されています。

  [ACS-85]

- **Web** アプリのパフォーマンスの向上

  クライアントレス VPN を使用してシステムブラウザから Web アプリケーションにアクセスするときの Web アプリケーションのパフォーマンスが向上しました。

  [NGSWS-16469]

- **Citrix Gateway Connector** で **TLS1.2** グレード **A** 以上の暗号スイートを使用できるようにする

  Citrix Gateway Connector では、グレード A 以上の暗号スイートを持つ TLS1.2 を使用して、Citrix Cloud サービスおよびその他のバックエンドサーバーに接続できるようになりました。

  [NGSWS-16068]

2020 年 11 月 11 日

- **Citrix** アクセス制御サービスの名前の変更

  アクセス制御サービスの名前が「Secure Private Access」に変更されました。

  [NGSWS-14934]

2020 年 10 月 15 日

- リモートブラウザ分離サービス内で **SaaS** およびエンタープライズ **Web** アプリケーションを起動するためのセキュリティオプションの強化

  管理者は、セキュリティ強化オプションの「**Citrix Remote Browser Isolation** サービスで常にアプリケーションを起動する」を選択して、他のセキュリティ強化設定に関係なく、リモートブラウザ隔離サービスで常にアプリケーションを起動できるようになりました。

  [ACS-123]

2020 年 10 月 8 日

- **Citrix Secure Private Access** ブラウザ拡張機能のセッションタイムアウトを構成する

  管理者は、Citrix Secure Private Access ブラウザー拡張機能のセッションタイムアウトを構成できるようになりました。管理者は、Citrix Gateway サービスのユーザーインターフェイスの［管理］タブからこの設定を構成できます。

  [NGSWS-13754]

- **Citrix Secure Private Access** ブラウザ拡張機能の管理者設定に対する **RBAC** 制御

  RBAC 制御は、Citrix Secure Private Access ブラウザ拡張機能の管理者設定に適用されます。

  [NGSWS-14427]

2020 年 9 月 24 日

- ローカルブラウザを介したエンタープライズ **Web** アプリケーションへの **VPN** レスアクセスを有効にする

  Citrix Secure Private Access ブラウザー拡張機能を使用して、ローカルブラウザーを介したエンタープライズ Web アプリへの VPN レスアクセスを有効にできるようになりました。**Citrix Secure Private Access** ブラウザ拡張機能は、Google Chrome ブラウザと Microsoft Edge ブラウザの両方でサポートされています。

  [ACS-286]

2020 年 7 月 7 日

- **Citrix Gateway Connector** での **Kerberos** 構成を検証する

  シングルサインオンセクションの [テスト] ボタンを使用して Kerberos 構成を検証できるようになりました。

  [NGSWS-8581]

2020 年 6 月 19 日

- **Citrix Gateway** サービスおよび **Citrix Secure Private Access** サービスの管理者への読み取り専用アクセス

  Citrix Gateway サービスを使用するセキュリティ管理者チームは、Citrix Gateway サービスおよび Citrix Secure Private Access サービスの管理者に、読み取り専用アクセスなどのきめ細かい制御を提供できるようになりました。

  - Citrix Gateway サービスへの読み取り専用アクセス権を持つ管理者は、アプリの詳細のみを表示できます。
  - Citrix Secure Private Access サービスへの読み取り専用アクセス権を持つ管理者は、コンテンツアクセス設定のみを表示できます。

  [ACS-205]

2020 年 5 月 8 日

- **Citrix Gateway Connector** の新しいトラブルシューティングツール **13.0**

  - ネットワークトレース: トレース機能を使用して ** 、Citrix Gateway Connector の登録に関する問題をトラブルシューティングできるようになりました。トレースファイルをダウンロードして、トラブルシューティングのために管理者と共有できます。詳しくは、「Citrix Gateway Connector の登録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。

    [NGSWS-10799]

  - 接続テスト**:** 接続テスト機能を使用して、Gateway Connector の構成にエラーがなく、Gateway Connector が URL に接続できることを確認できます。詳しくは、「ログオンして Citrix Gateway コネクタをセットアップする」を参照してください。

    [NGSWS-8580]

V2019.04.02

- 送信プロキシへの **Citrix Gateway** コネクタの **Kerberos** 認証サポート [NGSWS-6410]

Kerberos 認証は、Citrix Gateway コネクタから送信プロキシへのトラフィックでサポートされるようになりました。Gateway Connector は、設定されたプロキシ資格情報を使用して、アウトバウンドプロキシへの認証を行います。

V2019.04.01

- **Web/SaaS** アプリケーションのトラフィックは、企業ネットワークでホストされる **Gateway-Connector** を介してルーティングできるようになり、**2** 要素認証を回避できるようになりました。顧客が企業ネットワークの外部でホストされている SaaS アプリを公開した場合、オンプレミスの Gateway Connector を経由するために、そのアプリのトラフィックを認証するためのサポートが追加されるようになりました。

  たとえば、顧客が Okta で保護された SaaS アプリ (Workday など) を持っているとします。この顧客は、実際の Workday のデータトラフィックが Citrix Gateway サービスを介してルーティングされない場合でも、Okta サーバーへの認証トラフィックは、オンプレミスの Gateway Connector を介して Citrix Gateway サービスを介してルーティングされます。これにより、ユーザは企業ネットワーク内から Okta サーバに接続している場合に、Okta サーバから 2 番目の要素認証を回避できます。

  [NGSWS-6445]

- **Web** サイトリストのフィルタリングと **Web** サイトの分類の無効化。管理者が特定の顧客にこれらの機能を適用しないことを選択した場合、Web サイトリストのフィルタリングと Web サイトの分類を無効にすることができます。

  [NGSWS-6532]

- リモートブラウザ隔離サービスリダイレクトの自動ジオルーティング。リモートブラウザ隔離サービスのリダイレクトで自動ジオルーティングが有効になりました。

  [NGSWS-6926]

V2019.03.01

- 「**Gateway Connector** の追加」ページに「検出」ボタンが追加されました。[検出] ボタンを使用してコネクタのリストを更新し、新しく追加されたコネクタを [Web アプリの接続] セクションに反映できるようにします。

  [CGOP-6358]

- 「アクセス制御 **Web** フィルタリング」カテゴリに、新しいカテゴリ「悪意のあるおよび危険」が追加されました。[アクセス制御**]** の **[Web** フィルタリング] カテゴリの [悪意のあるカテゴリと危険と危険です] という名前の新しいカテゴリが [マルウェアとスパム] グループに追加されます。

  [CGOP-6205]

機能の非推奨

June 19, 2024

この記事では、ビジネス上の意思決定をタイムリーに行うことができるように、段階的に廃止される Secure Private Access サービスの機能について事前に通知します。Citrix ではお客様の使用状況とフィードバックをチェックして、各機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。製品ライフサイクルサポートの詳細については、「製品ライフサイクルサポートポリシー」を参照してください。

次の表に、非推奨または廃止予定の Secure Private Access サービスの機能を示します。

項目	廃止が発表されたバージョン	廃止予定日	代替手段
Web アプリケーションアクセス用のクライアントレス VPN アクセス方式	2023 年 1 月	2023 年 10 月 17 日	ユースケースに応じて、Citrix Enterprise Browser またはダイレクトアクセスを使用してください。詳細については、「Web アプリケーションアクセスのクライアントレス VPN アクセスの廃止について」を参照してください。
カテゴリベースの Web フィルタリング	2022 年 12 月	2022 年 12 月 31 日	Citrix Enterprise Browser から仕事に関係のない Web サイトに選択的にアクセスできるように、Secure Private Access の Web サイトごとの許可、拒否、または RBI リダイレクト機能は維持されます。
ナビゲーションのセキュリティ制御を制限する	2022 年 4 月	2022 年 6 月 15 日	-

項目	廃止が発表されたバージョン	廃止予定日	代替手段
Citrix Gateway Connector	2022 年 5 月	2022 年 9 月 30 日	Connector Appliance。Gateway Connector を Connector Appliance に移行するには、「Connector Appliance への Gateway Connector の移行」を参照してください。

Web アプリケーションアクセス用のクライアントレス VPN アクセスの廃止について

- クライアントレス VPN アクセス方法とは何ですか?

  Citrix Secure Private Access は、強化されたセキュリティ制限なしで構成された内部 Web アプリに、Web 向け Workspace (HTML5 向け Citrix Workspace アプリ) を介してアクセスする場合に、CVPN ベースのアクセス方法を使用します。

  > 注:
  >
  > クライアントレス VPN アクセス方法は、内部アプリに、Web 向け Workspace (HTML5 向け Citrix Workspace アプリ) を介してアクセスする場合にのみ使用されます。強化されたセキュリティ制限が設定されていないアプリのみがブロックされます。

- この機能を廃止するのはなぜですか?

  クライアントレス VPN 方法はクライアント側の URL 書き換えを使用しますが、これには業界に共通の特定の技術的制限があります。場合によっては、Web アプリ内の特定のリンクが書き換えられると、アプリアクセスが失敗することがあります。これはエンドユーザーエクスペリエンスの低下につながります。顧客に最高のアプリアクセスエクスペリエンスを提供するために、この機能を廃止し、下記の代替手段のいずれかに移行することをお勧めします。

- Secure Private Access が設定されたアプリケーションにアクセスするエンドユーザーにはどのような影響がありますか?

  強化されたセキュリティ制限なしで構成された Web アプリに Workspace for Web 経由でアクセスすると、そのアプリケーションへのアクセスはブロックされます。
  Workspace アプリケーション、ダイレクトアクセス、リモートブラウザ分離サービス (RBI)、または Secure Access Agent を介してアプリケーションにアクセスするエンドユーザーには影響しません。

- 代替手段は何か、管理者は何をすべきか?

Citrix Enterprise Browser: Citrix Workspace アプリを使用して、Citrix Enterprise Browser 経由でこれらのアプリケーションにアクセスします。この方法では、強化されたセキュリティ設定 (ダウンロードの制限、印刷の制限、ウォーターマーク、クリップボード アクセスの制限など) とブラウザ管理により、最高のエンド ユーザーエクスペリエンスが提供されます。Citrix Secure Private Access への Secure Private Access ダイレクトアクセス**:** クライアントレス方法で Web アプリケーションにアクセスする場合は、ダイレクトアクセス方法を使用します。これにより、Chrome などのネイティブブラウザーからアプリに直接アクセスできます。この方法は、Citrix Workspace アプリをエンドデバイスにインストールできない場合や、管理対象外のデバイスにインストールできない場合に使用できます。詳細については、「エンタープライズ Web アプリへの直接アクセス」を参照してください。

- Citrix Workspace アプリまたは Secure Access Agent を介してアクセスされる既存のアプリケーションに影響はありますか?

  いいえ。ブロックしているのは、Web 向け Workspace を介してアクセスされるウェブアプリケーションへのアクセスだけです。この廃止は、エンドデバイスにインストールされている Citrix Workspace アプリまたは Secure Access クライアントを介してアクセスされるアプリには影響しません。セキュリティ制限が強化された Web アプリケーションに、Web 向け Workspace または Citrix Workspace アプリの HTML5 バリアントを介してアクセスすると、それらのアプリケーションへのアクセスはブロックされます。

- 他に質問がありますか?

  Citrix サポートにお問い合わせください。

Citrix Secure Private Access の使用開始

January 9, 2024

このドキュメントでは、SaaS アプリの配信を初めて開始し、オンボーディングを開始する方法と、SaaS アプリの配信の設定方法について説明します。このドキュメントは、アプリケーション管理者向けです。

システム要件

オペレーティングシステムのサポート： Citrix Workspace アプリは、Windows 7、8、10、および Mac 10.11 以降でサポートされています。

ブラウザーのサポート**:** 最新バージョンの Edge、Chrome、Firefox、または Safari を使用してワークスペースにアクセスします。

Citrix Workspace のサポート：任意のデスクトッププラットフォーム（Windows、Mac）で Citrix Workspace を使用してワークスペースにアクセスします。

機能

Citrix Secure Private Access は、IT 管理者およびセキュリティ管理者が、認可された SaaS およびエンタープライズホスト Web アプリへのエンドユーザーアクセスを管理するのに役立ちます。ユーザー ID と属性は、アクセス権限を決定するために使用され、アクセス制御ポリシーは、操作を実行するために必要な権限を決定します。ユーザーが認証されると、アクセス制御は、適切なレベルのアクセスと、そのユーザーの資格情報に関連付けられた許可されたアクションを承認します。

Citrix Secure Private Access は、いくつかの Citrix Cloud サービスの要素を組み合わせて、エンドユーザーと管理者に統合されたエクスペリエンスを提供します。

機能	機能を提供するサービス/コンポーネント
アプリにアクセスするための一貫したユーザーインターフェース	ワークスペース環境/Workspace アプリ
SaaS および Web アプリへの SSO	NetScaler Gateway Service Standard
Web フィルタリングと分類	Web フィルタリングサービス
SaaS の強化されたセキュリティポリシー	クラウドアプリコントロール
安全なブラウジング	リモートブラウザ分離サービス
Web サイトへのアクセスと危険な行動を可視化	Citrix Analytics

Citrix Secure Private Access サービスを開始する

1. Citrix Cloud ウドにサインアップします。
2. Secure Private Access サービスのエンタイトルメントを要求します。
3. エンタイトルメント後、Secure Private Access サービスは [マイサービス] の下でプロビジョニングされます。
4. Secure Private Access サービス UI にアクセスします。

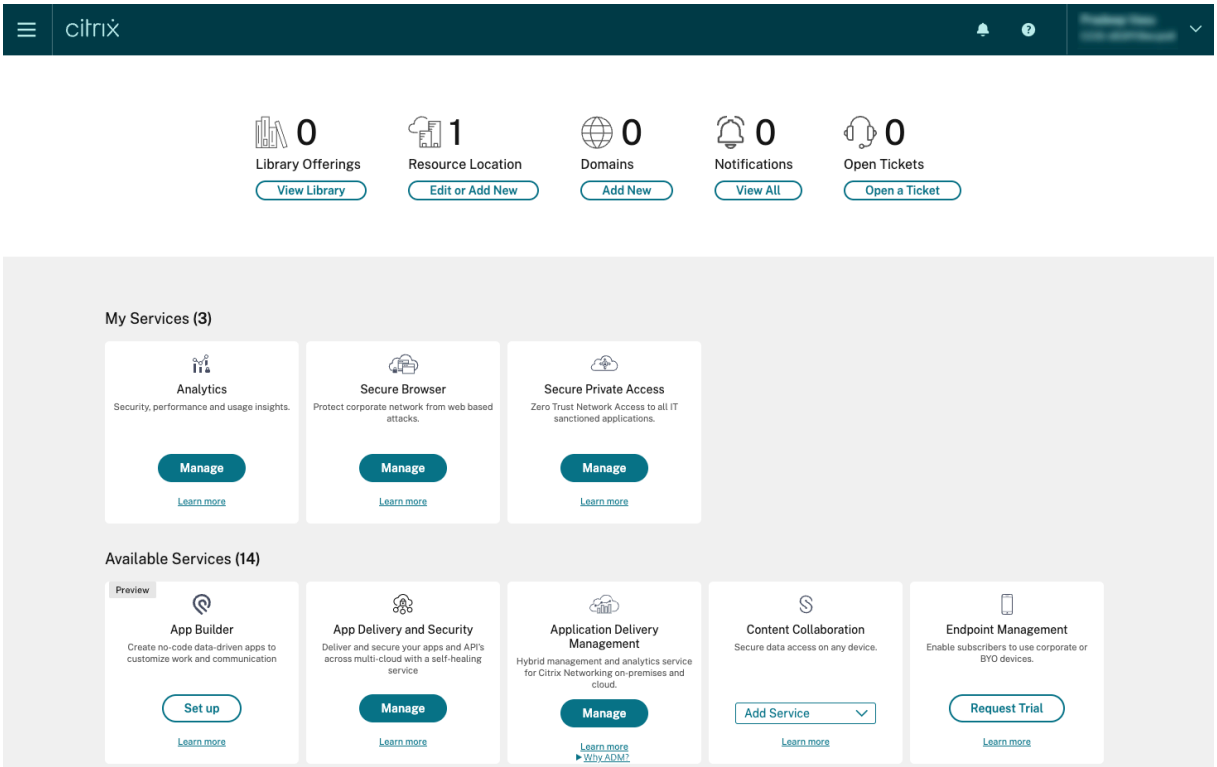
ステップ 1: **Citrix Cloud** にサインアップ

Secure Private Access サービスの使用を開始するには、まず Citrix Cloud アカウントを作成するか、社内の他のユーザーが作成した既存のアカウントに参加する必要があります。詳細なプロセスと手順については、「Citrix Cloud へのサインアップ」を参照してください。

ステップ 2: **Secure Private Access** サービスのエンタイトルメントをリクエストする

Secure Private Access サービスの資格を要求するには、**Citrix Cloud** 画面の［利用可能なサービス］セクションで、［Secure Private Access］サービスタイルにある［トライアルをリクエスト］タブをクリックします。

ライセンスの詳細については、https://www.citrix.com/buy/licensing/product.htmlを参照してください。



ステップ 3: エンタイトルメント後、**Secure Private Access** サービスは **[マイサービス]** でプロビジョニングされます

Secure Private Access サービスエンタイトルメントを受け取ると、Secure Private Access サービスタイルが [マイサービス] セクションに移動します。

ステップ 4: **Secure Private Access** サービス **UI** にアクセスする

タイルの「管理」タブをクリックして、Secure Private Access サービスの UI にアクセスします。

注:

- ワークスペースを介してアプリにアクセスするには、エンドユーザーが Citrix Workspace アプリをダウンロードして使用するか、ワークスペース URL を使用する必要があります。Citrix Secure Private Access ソリューションをテストするには、ワークスペースにいくつかの SaaS アプリを公開する必要があります。Workspace アプリはhttps://www.citrix.com/downloadsからダウンロードできます。ダウンロードの検索リストで、**Citrix Workspace** アプリを選択します。
- 送信ファイアウォールが構成されている場合は、次のドメインへのアクセスが許可されていることを確認してください。

  - *.cloud.com
  - *.nssvc.net
  - *.netscalergateway.net

  詳しくは、「Cloud Connector のプロキシとファイアウォールの構成」および「インターネット接続の要件」

を参照してください。

- Workspace アカウントは 1 つだけ追加できます。

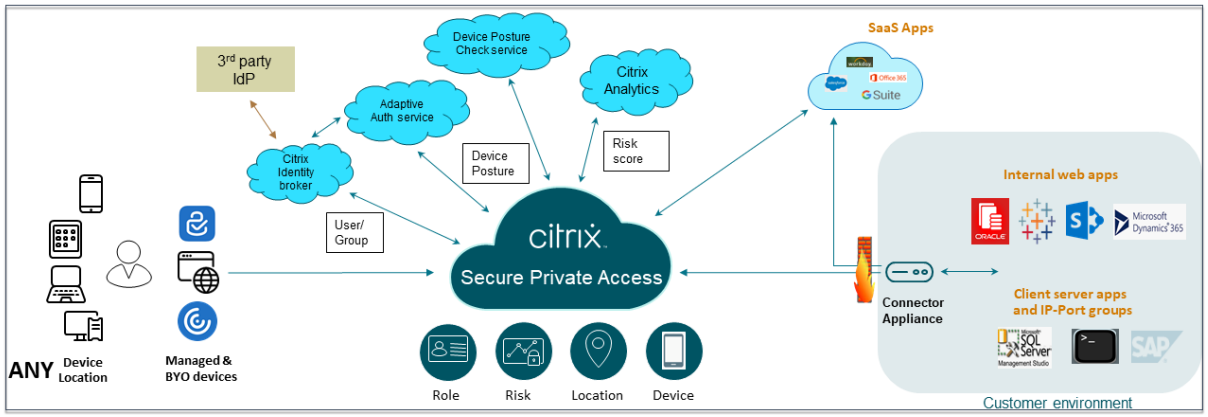
Secure Private Access サービス・ソリューションの概要

June 19, 2024

ソリューション概要

従来の VPN ソリューションでは、エンドユーザーのデバイスを管理し、ネットワークレベルでのアクセスを提供し、静的なアクセス制御ポリシーを適用する必要があります。Citrix Secure Private Access は、BYO デバイスからの脅威から保護するための一連のセキュリティ制御を IT 部門に提供します。これにより、ユーザーは、管理対象デバイスか BYO デバイスかを問わず、どのデバイスからでも IT 部門が認可したアプリケーションにアクセスできるようになります。

Citrix Secure Private Access は、アプリケーションの適応型認証、シングルサインオンのサポート、強化されたセキュリティ制御を提供します。Secure Private Access には、Device Posture サービスを使用してセッションを確立する前に、エンドユーザーのデバイスをスキャンする機能もあります。アダプティブ認証または Device Posture の結果に基づいて、管理者はアプリの認証方法を定義できます。



適応型セキュリティ

アダプティブ認証は、現在のリクエストに適した認証フローを決定します。適応型認証では、デバイスの姿勢、地理的位置、ネットワークセグメント、ユーザー組織/部門のメンバーシップを識別できます。取得した情報に基づいて、管理者は IT 部門が認可したアプリに対してユーザーを認証する方法を定義できます。これにより、組織はパブリック SaaS アプリ、プライベート Web アプリ、プライベートクライアントサーバーアプリ、Desktops as a Service（DaaS）など、すべてのリソースに同じ認証ポリシーフレームワークを実装できます。詳細については、「適応型セキュリティ」を参照してください。

アプリケーションアクセス

Secure Private Access は、VPN に依存せずにオンプレミスの Web アプリへの接続を確立できます。この VPN レス接続は、オンプレミスにデプロイされた Connector Appliance を使用します。Connector Appliance、組織の Citrix Cloud サブスクリプションへのアウトバウンド制御チャネルを作成します。そこから、Secure Private Access は、VPN を必要とせずに内部 Web アプリへの接続をトンネリングできます。詳細については、「アプリケーションアクセス」を参照してください。

シングルサインオン

適応型認証を使用すると、組織は強力な認証ポリシーを提供して、ユーザーアカウントが侵害されるリスクを軽減できます。Secure Private Access のシングルサインオン機能は、すべての SaaS、プライベートウェブ、およびクライアントサーバーアプリに同じ適応型認証ポリシーを使用します。詳細については、「シングルサインオン」を参照してください。

ブラウザセキュリティ

Secure Private Access により、エンドユーザーは一元管理されセキュリティ保護された Enterprise Browser を使用してインターネットを安全に閲覧できます。エンドユーザーが SaaS またはプライベート Web アプリを起動すると、このアプリケーションの最適な提供方法を決定するために、いくつかの決定が動的に行われます。詳細については、「ブラウザセキュリティ」を参照してください。

Device Posture

Device Posture サービスを使用すると、管理者は企業リソースにリモートでアクセスしようとしているエンドポイントデバイスのポスチャを確認するポリシーを定義できます。エンドポイントのコンプライアンス状態に基づいて、Device Posture サービスは企業のアプリケーションやデスクトップへのアクセスを拒否したり、制限付き/フルアクセスを提供したりできます。

エンドユーザーが Citrix Workspace との接続を開始すると、Device Posture クライアントはエンドポイントパラメータに関する情報を収集し、その情報を Device Posture サービスと共有して、エンドポイントのポスチャがポリシー要件を満たしているかどうかを判断します。

Device Posture サービスを Citrix Secure Private Access と統合することで、Citrix Cloud の耐障害性とスケーラビリティを利用して、どこからでも SaaS、Web、TCP、UDP アプリに安全にアクセスできるようになります。詳細については、「Device Posture」を参照してください。

TCP および **UDP** アプリケーションのサポート

リモートユーザーは、フロントエンドがエンドポイントに、バックエンドがデータセンターにあるプライベートクライアントサーバーアプリにアクセスする必要がある場合があります。組織はこれらの社内アプリやプライベートアプ

リに厳格なセキュリティポリシーを正当に適用できるため、リモートユーザーがセキュリティプロトコルを危険にさらすことなくこれらのアプリケーションにアクセスすることが困難になります。

Secure Private Access サービスは、ZTNA がこれらのアプリへの安全なアクセスを提供できるようにすることで、TCP と UDP のセキュリティ脆弱性に対処します。ユーザーは、TCP、UDP、HTTPS アプリを含むすべてのプライベートアプリに、ネイティブブラウザーまたはマシン上で実行されている Citrix Secure Access クライアント経由のネイティブクライアントアプリケーションを使用してアクセスできるようになりました。

ユーザーは、Citrix Secure Access クライアントをクライアントデバイスにインストールする必要があります。

- Windows の場合、クライアントバージョン (22.3.1.5 以降) はhttps://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.htmlからダウンロードできます。
- macOS の場合、クライアントバージョン (22.02.3 以降) は App Store からダウンロードできます。

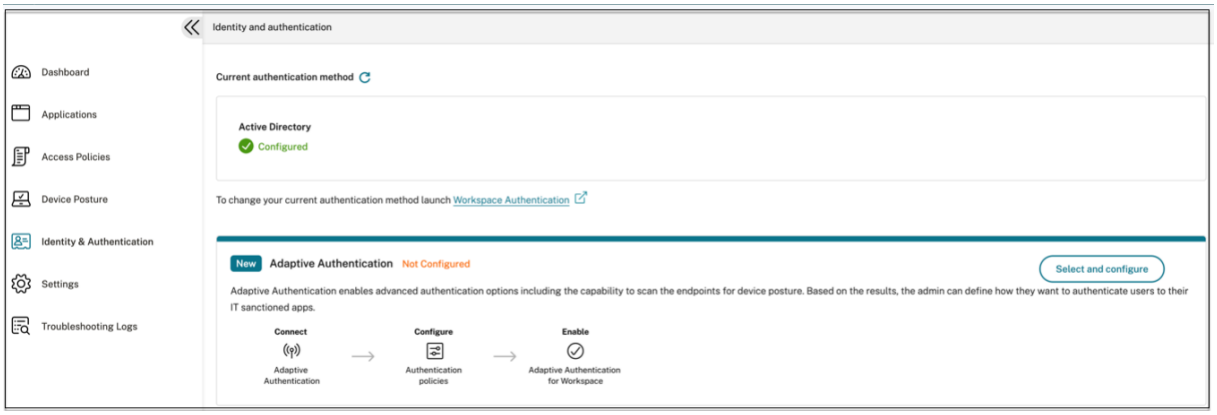
詳しくは、「クライアントサーバーアプリのサポート」を参照してください。

Citrix Secure Private Access セットアップ

Secure Private Access 管理コンソールを使用して、SaaS アプリ、社内 Web アプリ、TCP、および UDP アプリへのゼロトラストネットワークアクセスを有効にします。このコンソールには、アダプティブ認証、ユーザーサブスクリプションを含むアプリケーション、アダプティブアクセスポリシーの設定が含まれます。

ID と認証の設定

利用者が Citrix Workspace にログインするための認証方法を選択します。アダプティブ認証は、Citrix Workspace にログインしている顧客とユーザーに高度な認証を可能にする Citrix Cloud サービスです。



詳細については、「ID と認証の設定」を参照してください。

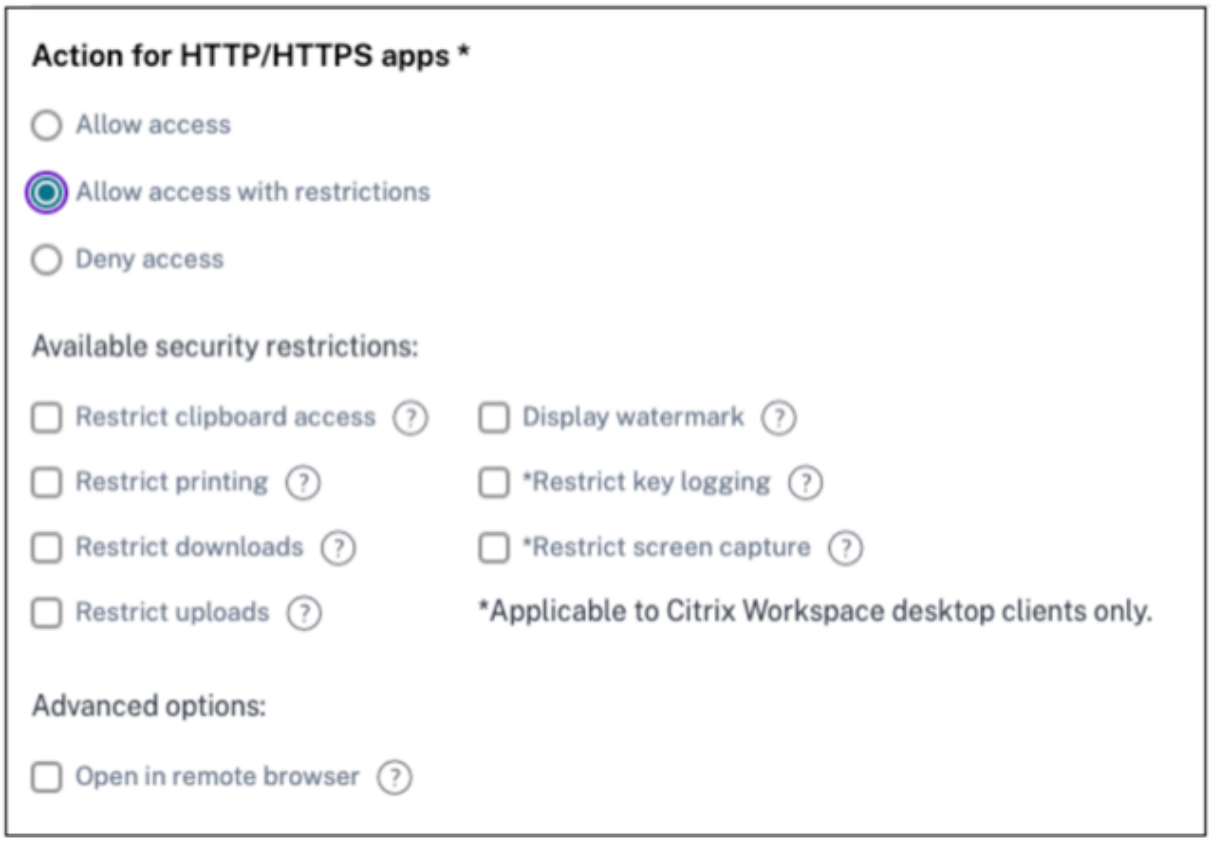
アプリを列挙して公開する

認証方法を選択したら、管理コンソールを使用して Web アプリ、SaaS アプリ、TCP アプリ、UDP アプリを設定します。詳しくは、「アプリの追加と管理」を参照してください。

セキュリティ制御の強化を有効にする

コンテンツを保護するために、組織は強化されたセキュリティポリシーを SaaS アプリケーション内に組み込んでいます。各ポリシーにより、デスクトップ用の Workspace アプリを使用する場合は Citrix Enterprise Browser、Web またはモバイル用の Workspace アプリを使用する場合は Secure Browser ser に制限が適用されます。

- クリップボードへのアクセスを制限する: アプリとシステムクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- 印刷制限： Citrix Enterprise Browser 内からの印刷機能を無効にします。
- ダウンロードを制限する: ユーザーがアプリ内からダウンロードできないようにします。
- アップロードを制限: ユーザーがアプリ内でアップロードできないようにします。
- ウォーターマークの表示: ユーザーの画面にウォーターマークを表示し、ユーザーのマシンのユーザー名と IP アドレスを表示します。
- キーロギングの制限: キーロガーから保護します。ユーザーがユーザー名とパスワードを使用してアプリにログオンしようとすると、すべてのキーがキーロガーで暗号化されます。また、ユーザーがアプリで実行するすべてのアクティビティは、キーロギングから保護されます。たとえば、Office 365 のアプリ保護ポリシーが有効になっていて、ユーザーが Office 365 の Word 文書を編集した場合、すべてのキーストロークはキーロガーで暗号化されます。
- 画面キャプチャを制限する: 任意の画面キャプチャプログラムまたはアプリを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとすると、空白の画面がキャプチャされます。



詳細については、「アクセスポリシーの設定」を参照してください。

アプリケーション起動時に **Citrix Enterprise Browser** を有効にする

Secure Private Access により、エンドユーザーは Citrix Enterprise Browser（CEB）を使用してアプリケーションを起動できます。CEB は、Citrix Workspace アプリと統合されたクロムベースのブラウザーです。これにより、Citrix Enterprise Browser 内の Web アプリや SaaS アプリにアクセスするためのシームレスで安全なアクセスが可能になります。

CEB は、セキュリティポリシーが適用された内部でホストされているすべての Web アプリまたは SaaS アプリの優先ブラウザまたは仕事用ブラウザとして構成できます。CEB を使用すると、ユーザーは安全で制御された環境内で、設定されたすべての SaaS/Web アプリケーションドメインを開くことができます。

Citrix Enterprise Browser を有効にする　管理者は、グローバルアプリ構成サービス（GACS）を使用して、Citrix Workspace アプリから Web アプリや SaaS アプリを起動するためのデフォルトブラウザーとして Citrix Enterprise Browser を構成できます。

API による設定**:**

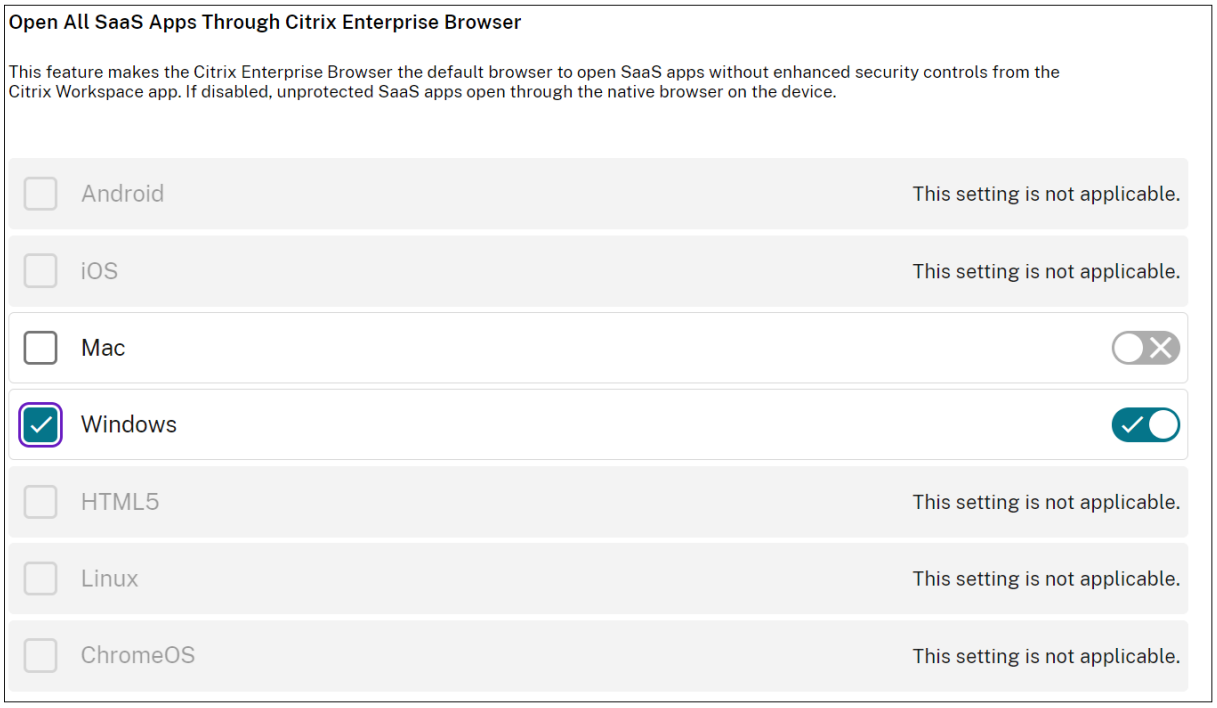
構成するには、すべてのアプリで Citrix Enterprise Browser をデフォルトで有効にする JSON ファイルの例を以下に示します:

```
"settings": [
                    {

                       "name": "open all apps in ceb",
                       "value": "true"
                     }

                    ]
<!--NeedCopy-->
```

デフォルト値は、true です。

GUI による設定**:**

CEB をアプリ起動のデフォルトブラウザにする必要があるデバイスを選択します。



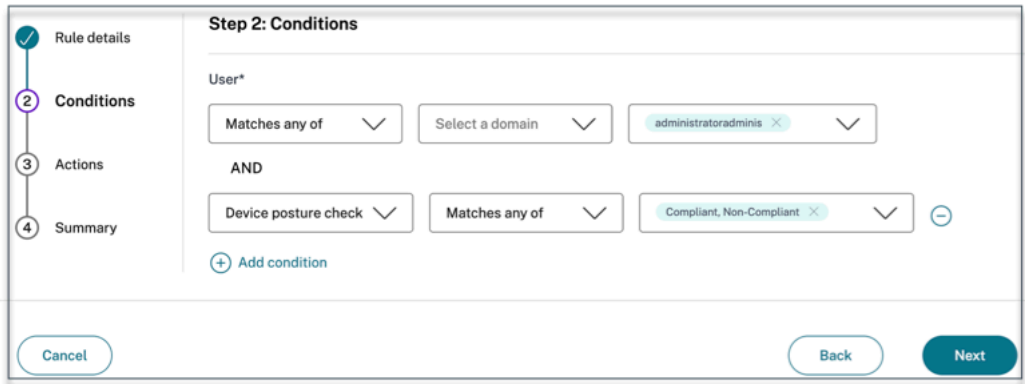
詳しくは、「GACS による Citrix Enterprise Browser の管理」を参照してください。

Device Posture を使用してコンテキストアクセス用のタグを設定します

デバイスのポスチャを確認すると、デバイスはログインを許可され、デバイスは準拠または非準拠に分類されます。この分類は Secure Private Access サービスにタグとして提供され、デバイスのポスチャに基づいてコンテキストに応じたアクセスを提供するために使用されます。

1. Citrix Cloud にサインインします。
2. 「Secure Private Access」タイルで、「管理」をクリックします。
3. 左側のナビゲーションで [アクセスポリシー] をクリックし、[ポリシーの作成] をクリックします。
4. ポリシー名とポリシーの説明を入力します。
5. 「アプリケーション」で、このポリシーを適用する必要があるアプリまたはアプリのセットを選択します。
6. 「**Create Rule** 」をクリックして、ポリシーのルールを作成します。
7. ルール名とルールの簡単な説明を入力して、[次へ] をクリックします。
8. ユーザーの条件を選択します。ユーザー条件は、ユーザーにアプリケーションへのアクセスを許可するための必須条件です。
9. **+** をクリックして、デバイスの姿勢条件を追加します。
10. ドロップダウンメニューから [デバイス姿勢チェック] と [論理式] を選択します。

11. カスタムタグに次のいずれかの値を入力します:



- 準拠-準拠デバイス用
- 非準拠-非準拠デバイス用

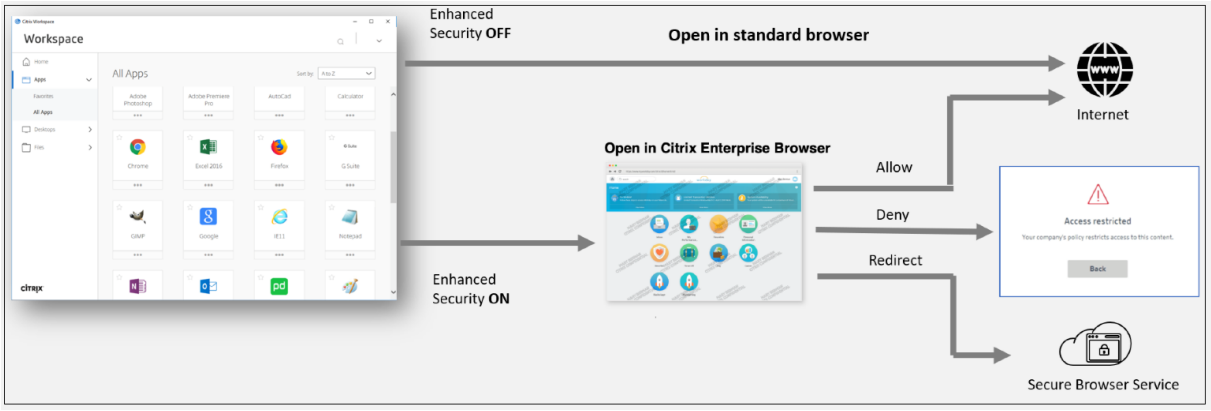
12. [次へ] をクリックします。
13. 条件評価に基づいて適用する必要があるアクションを選択し、「次へ」をクリックします。

    「概要」ページには、ポリシーの詳細が表示されます。
14. 詳細を確認し、[完了] をクリックします。

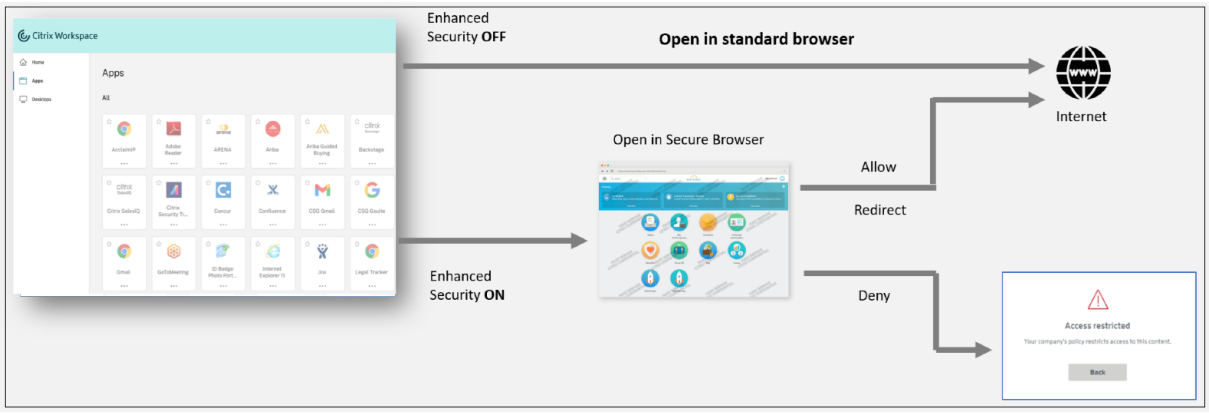
> 注:
>
> アクセスポリシーで準拠または非準拠としてタグ付けされていない Secure Private Access アプリケーションはデフォルトアプリケーションとして扱われ、デバイスの状態に関係なくすべてのエンドポイントからアクセスできます。

エンドユーザーエクスペリエンス

Citrix 管理者は、シトリック Citrix Secure Private Access してセキュリティ制御を拡張することができます。Citrix Workspace アプリは、すべてのリソースに安全にアクセスするためのエントリーポイントです。エンドユーザーは、Citrix Workspace アプリを介して仮想アプリ、デスクトップ、SaaS アプリ、ファイルにアクセスできます。Citrix Secure Private Access を使用すると、管理者は Citrix Workspace Experience Web UI またはネイティブの Citrix Workspace アプリクライアントを介してエンドユーザーが SaaS アプリケーションにアクセスする方法を制御できます。



ユーザーがエンドポイントで Workspace アプリを起動すると、アプリケーション、デスクトップ、ファイル、SaaS アプリが表示されます。セキュリティ強化が無効になっているときにユーザーが SaaS アプリケーションをクリックすると、アプリケーションはローカルにインストールされている標準ブラウザで開きます。管理者がセキュリティ強化を有効にしている場合、SaaS アプリは Workspace アプリ内の CEB で開きます。SaaS アプリおよび Web アプリ内のハイパーリンクへのアクセスは、許可されていない Web サイトのポリシーに基づいて制御されます。未認可の Web サイトの詳細については、「非認可の Web サイト」を参照してください。



同様に、Workspace Web ポータルでは、セキュリティ強化が無効になっている場合、SaaS アプリケーションはネイティブにインストールされている標準ブラウザで開かれます。セキュリティ強化を有効にすると、SaaS アプリは安全なリモートブラウザで開きます。ユーザーは、許可されていない Web サイトポリシーに基づいて、SaaS アプリ内の Web サイトにアクセスできます。未認可の Web サイトの詳細については、「非認可の Web サイト」を参照してください。

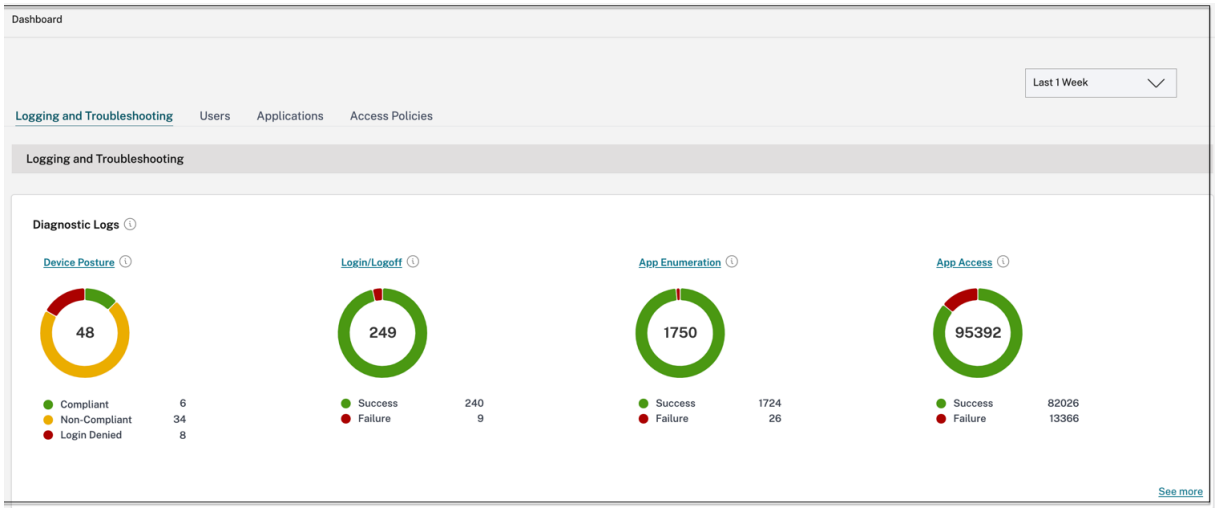
分析ダッシュボード

Secure Private Access サービス・ダッシュボードには、SaaS、Web、TCP、UDP アプリケーションの診断と使用状況データが表示されます。管理者は、管理者がアプリ、ユーザー、コネクタのヘルスステータス、帯域幅の使用状況を 1 か所で完全に把握して利用できます。このデータは Citrix Analytics から取得されます。メトリックは大きく次のカテゴリに分類されます。

- ロギングとトラブルシューティング

- ユーザー
- アプリケーション
- アクセスポリシー

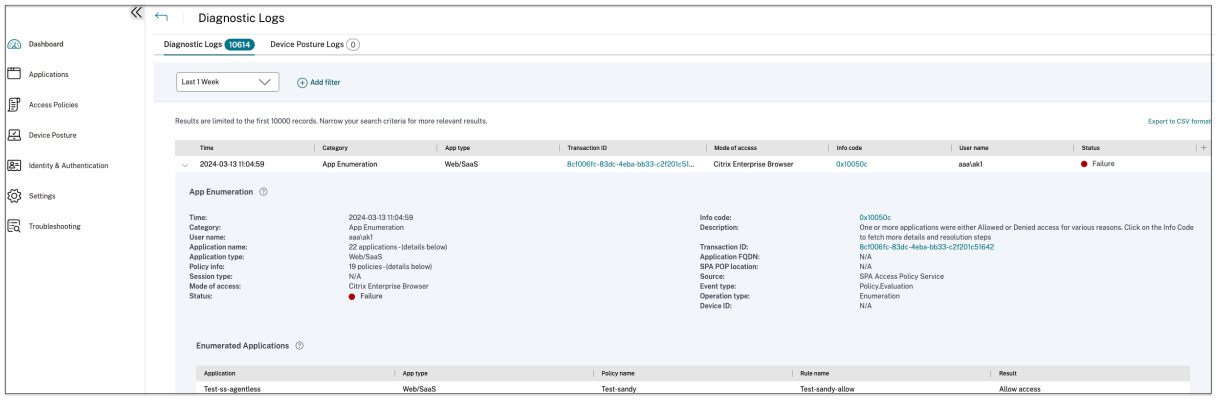
詳細については、「ダッシュボード」を参照してください。



アプリの問題のトラブルシューティング

Secure Private Access ダッシュボードの診断ログチャートでは、認証、アプリケーション起動、アプリケーション列挙、および Device Posture ログに関連するログを確認できます。

- 情報コード: 障害などの一部のログイベントには、情報コードが関連付けられています。情報コードをクリックすると、ユーザーは解決手順またはそのイベントに関する詳細情報にリダイレクトされます。
- トランザクション **ID**: 診断ログには、アクセス要求のすべての Secure Private Access ログを関連付けるトランザクション ID も表示されます。1 つのアプリアクセスリクエストで、認証、Workspace アプリ内でのアプリ列挙、アプリアクセス自体から複数のログを生成できます。これらのイベントはすべて独自のログを生成します。トランザクション ID は、これらすべてのログを関連付けるために使用されます。トランザクション ID を使用して診断ログをフィルタリングし、特定のアプリアクセスリクエストに関連するすべてのログを検索できます。
  詳細については、「Secure Private Access の問題のトラブルシューティング」を参照してください。



サンプルユースケース

- ファイアウォールで受信トラフィックを開かずにゼロトラストアプローチを使用して内部アプリケーション (Web/TCP/UDP) にアクセスする
- ユーザーがアクセスしたアプリケーションを検出してゼロトラストアプローチに移行
- SaaS アプリケーションへのアクセスを Citrix Enterprise Browser に制限する
- SaaS アプリケーションへのアクセスを会社所有のパブリック IP アドレスに制限する
- Azure マネージド SaaS アプリのセキュリティ強化
- Office 365 のセキュリティを強化
- Okta アプリのセキュリティ強化

参考記事

- Secure Private Access の概要Secure Private Access
- Tech brief
- リファレンスアーキテクチャ
- Citrix Enterprise Browser
- GACS による Citrix Enterprise Browser の管理
- 簡単なオンボードとセットアップの管理者向けガイドワークフロー

リファレンスビデオ

- アプリへのゼロトラストネットワークアクセス (ZTNA)
- Citrix Secure Private Access によるプライベート Web アプリケーションアクセス
- Citrix Secure Private Access によるパブリック SaaS アプリケーションアクセス
- Citrix Secure Private Access によるプライベートクライアント/サーバーアプリケーションアクセス
- Citrix Secure Private Access によるキーロガー保護
- Citrix Secure Private Access による画面共有保護

- Citrix Secure Private Access によるエンドユーザーエクスペリエンス
- Citrix Secure Private Access による ZTNA と VPN のログオンエクスペリエンスの比較
- Citrix Secure Private Access による ZTNA と VPN のポートスキャンの比較

関連製品の新着情報

- Citrix Enterprise Browser: このリリースについて
- Citrix Workspace: 新機能Citrix Workspace
- Citrix DaaS: 新着情報
- Citrix Secure Access クライアント NetScaler Gateway クライアント

簡単なオンボードとセットアップの管理者向けガイドワークフロー

June 19, 2024

SaaS アプリ、内部 Web アプリ、および TCP アプリへのゼロトラストネットワークアクセスを構成するステップバイステップのプロセスを備えた新しい合理化された管理エクスペリエンスは、Secure Private Access サービスで利用できます。Adaptive Authentication、ユーザーサブスクリプションを含むアプリケーション、アダプティブアクセスポリシーなど、単一の管理コンソール内での設定が含まれます。

このウィザードは、管理者がオンボーディング中または繰り返し使用中にエラーのない構成を実現するのに役立ちます。また、全体的な使用状況指標やその他の重要な情報を完全に可視化する新しいダッシュボードも利用できます。

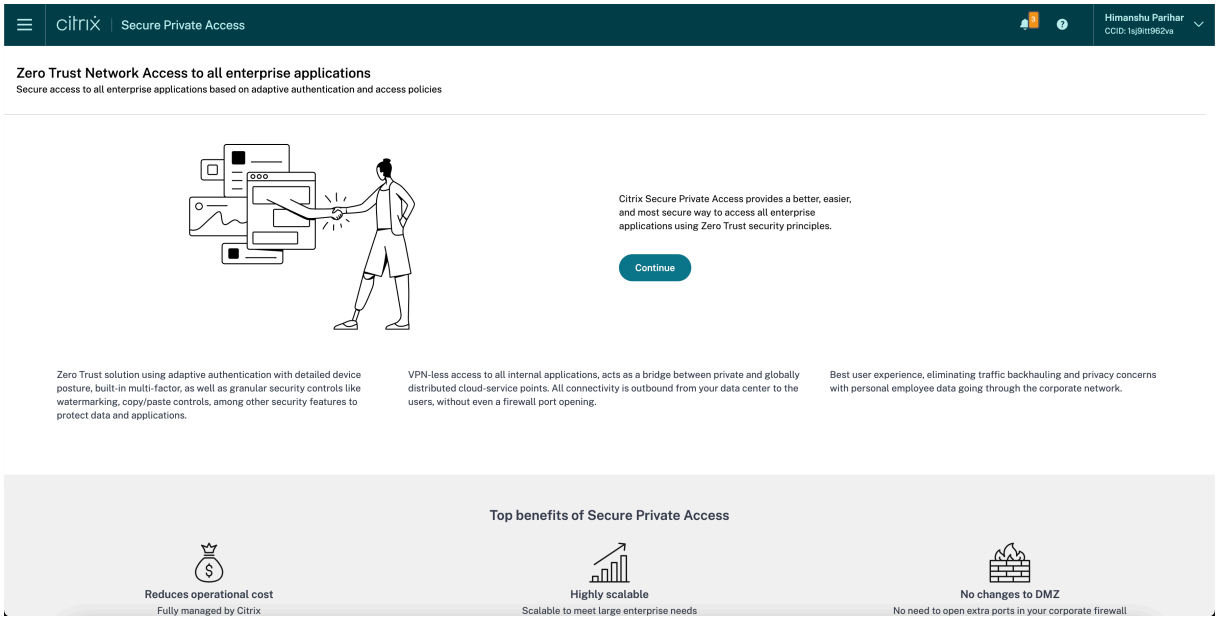
大まかな手順には以下が含まれます。

1. 利用者が Citrix Workspace にログインするための認証方法を選択します。
2. ユーザー用のアプリケーションを追加します。
3. 必要なアクセスポリシーを作成して、アプリアクセスの権限を割り当てます。
4. アプリの設定を確認します。

Secure Private Access 管理者によるワークフローウィザードにアクセスする

ウィザードにアクセスするには、次の手順を実行します。

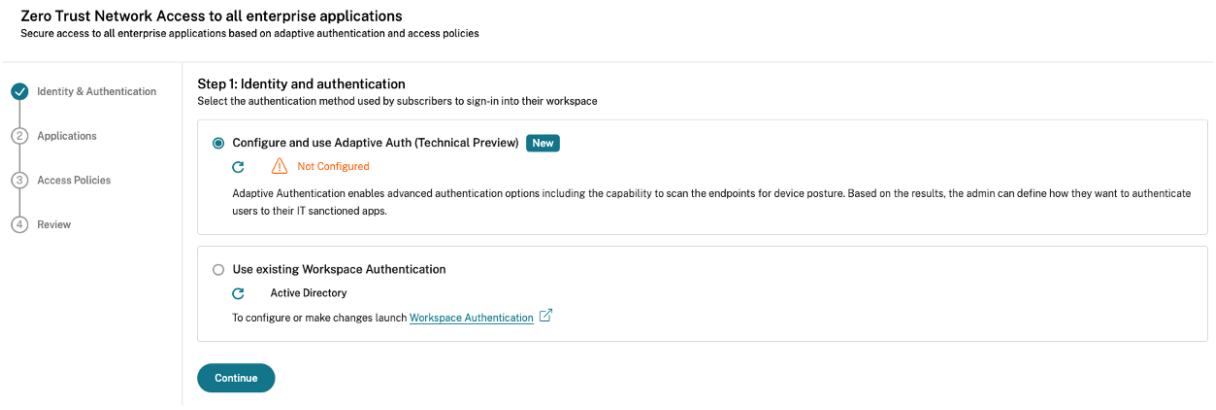
1.「**Secure Private Access** 」サービスのタイルで、「管理」をクリックします。
2. [概要] ページで、[続行] をクリックします。



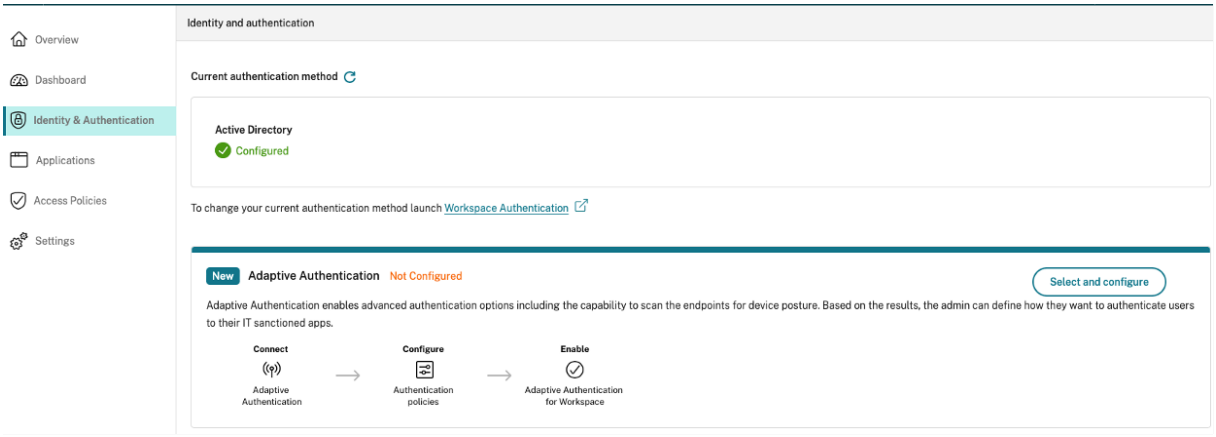
ステップ **1: ID** と認証を設定する

利用者が Citrix Workspace にログインするための認証方法を選択します。アダプティブ認証は、Citrix Workspace にログインしている顧客とユーザーに高度な認証を可能にする Citrix Cloud サービスです。アダプティブ認証サービスは、Citrix がホストする、Citrix itrix が管理する、クラウドでホストされる NetScaler ADC であり、次のような高度な認証機能をすべて提供します。

- 多要素認証
- デバイスポスチャスキャン
- 条件付き認証
- Citrix Virtual Apps and Desktops へのアダプティブアクセス
- アダプティブ認証を設定するには、[アダプティブ認証の設定と使用 **(**テクニカルプレビュー**)**] を選択し、構成を完了します。アダプティブ認証について詳しくは、「アダプティブ認証サービス」を参照してください。アダプティブ認証を設定した後、必要に応じて [管理] をクリックして設定を変更できます。



- 最初に別の認証方法を選択し、アダプティブ認証に切り替える場合は、**[**選択して設定**]** をクリックして構成を完了します。

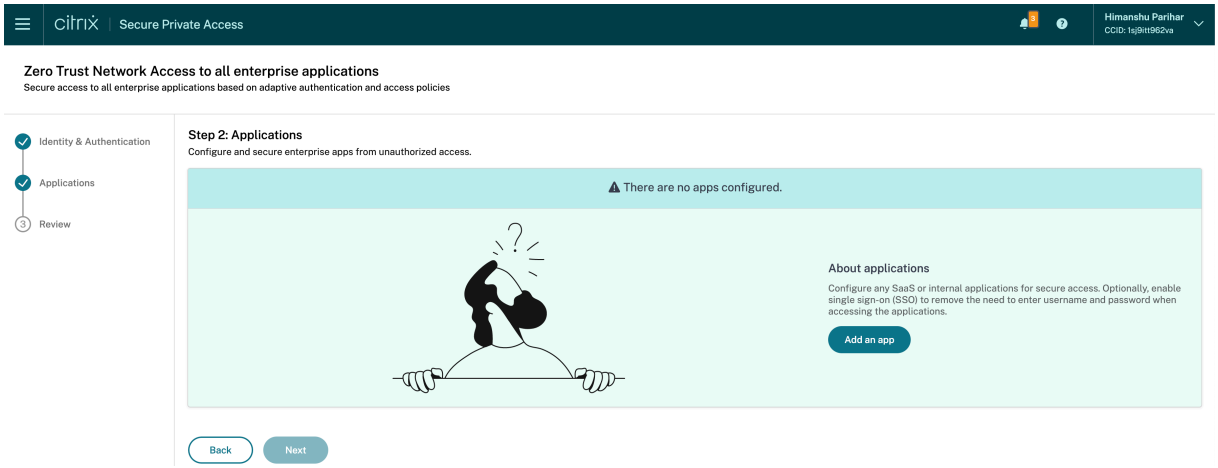


既存の認証方法を変更するか、既存の認証方法を変更するには、[ワークスペース認証] をクリックします。

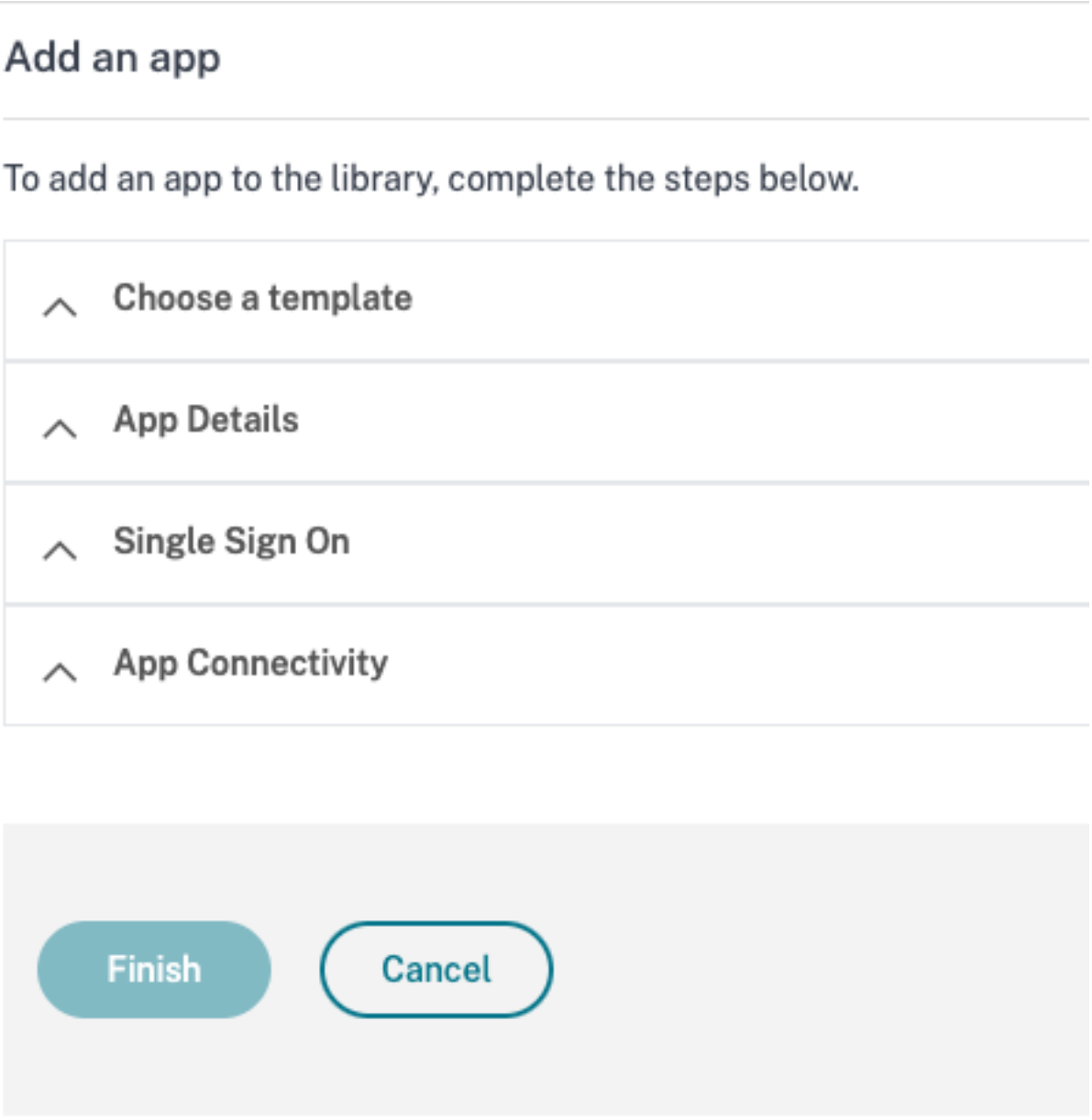
ステップ **2:** アプリケーションを追加して管理する

認証方法を選択したら、アプリケーションを設定します。初めて使用するユーザーの場合、[アプリケーション] ランディングページにはアプリケーションが表示されません。アプリを追加するには、[アプリを追加] をクリックします。このページから SaaS アプリ、Web アプリ、および TCP/UDP アプリを追加できます。アプリを追加するには、[アプリを追加] をクリックします。

アプリを追加すると、ここに一覧表示されます。



次の図に示す手順を完了して、アプリを追加します。



- エンタープライズ **Web** アプリを追加する
  - エンタープライズ Web アプリのサポート
  - Web アプリへの直接アクセスを構成する
- **SaaS** アプリを追加する
  - サービスとしてのソフトウェアアプリのサポート
  - SaaS アプリケーションサーバー固有の設定
- クライアントサーバーアプリを構成する
  - クライアントサーバーアプリのサポート

- アプリを起動する
  - 構成済みアプリの起動 - エンドユーザーのワークフロー
- 管理者への読み取り専用アクセスを有効にする
  - 管理者の SaaS および Web アプリへの読み取り専用アクセス

ステップ **3:** 複数のルールを使用してアクセスポリシーを設定する

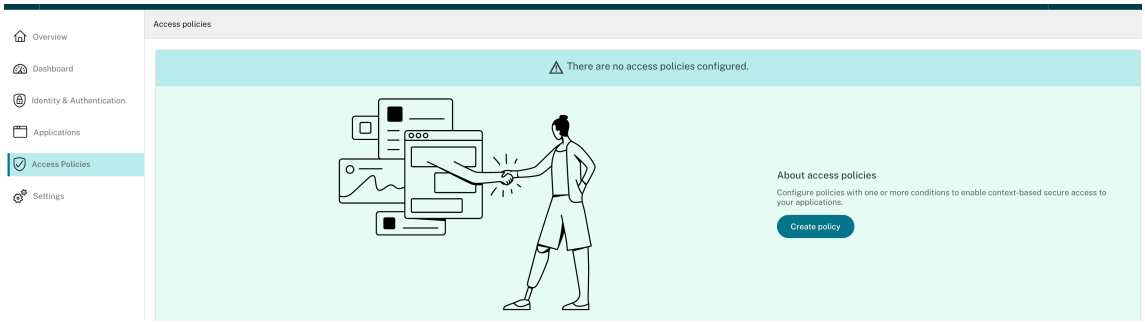
1 つのポリシー内で、複数のアクセスルールを作成し、さまざまなユーザーまたはユーザーグループにさまざまなアクセス条件を設定できます。これらのルールは、HTTP/HTTPS アプリケーションと TCP/UDP アプリケーションの両方に、すべて 1 つのポリシー内で個別に適用できます。

Secure Private Access のアクセスポリシーにより、ユーザーまたはユーザーのデバイスのコンテキストに基づいてアプリへのアクセスを有効または無効にできます。さらに、次のセキュリティ制限を追加することで、アプリへの制限付きアクセスを有効にできます。

- クリップボードへのアクセスを制限する
- 印刷を制限
- ダウンロードを制限
- アップロードを制限する
- ウォーターマークを表示
- キーロギングを制限する
- 画面キャプチャを制限する

これらの制限の詳細については、「利用可能なアクセス制限オプション」を参照してください。

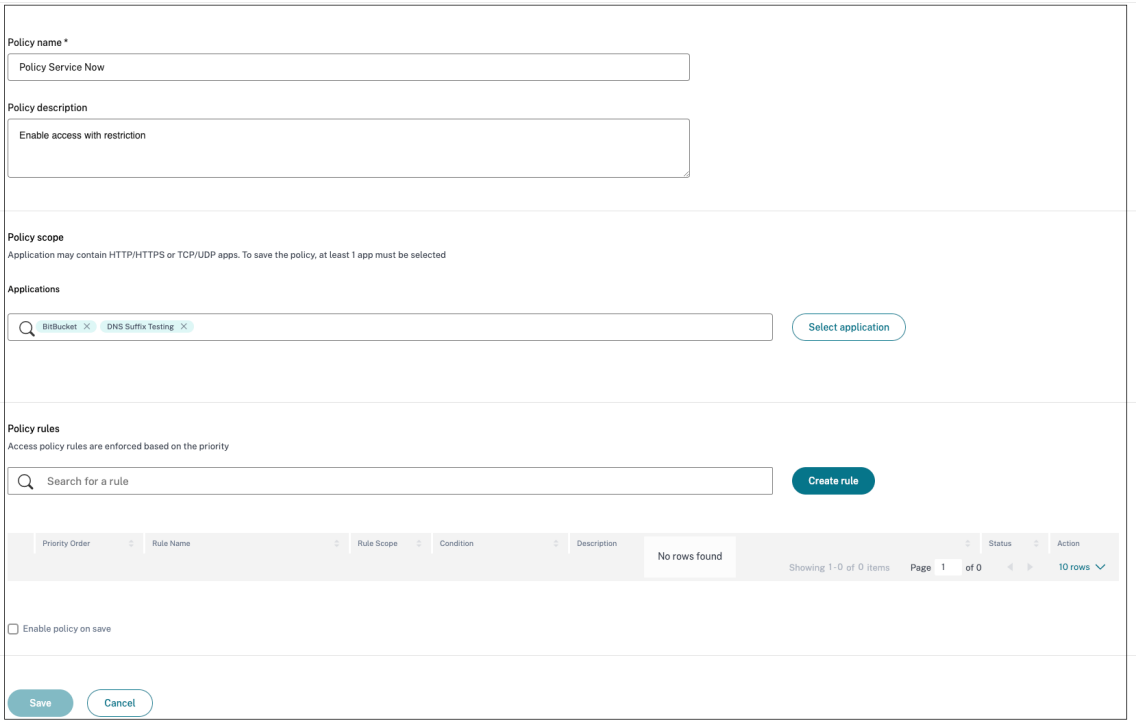
1. ナビゲーションペインで、[アクセスポリシー] をクリックし、[ポリシーの作成] をクリックします。



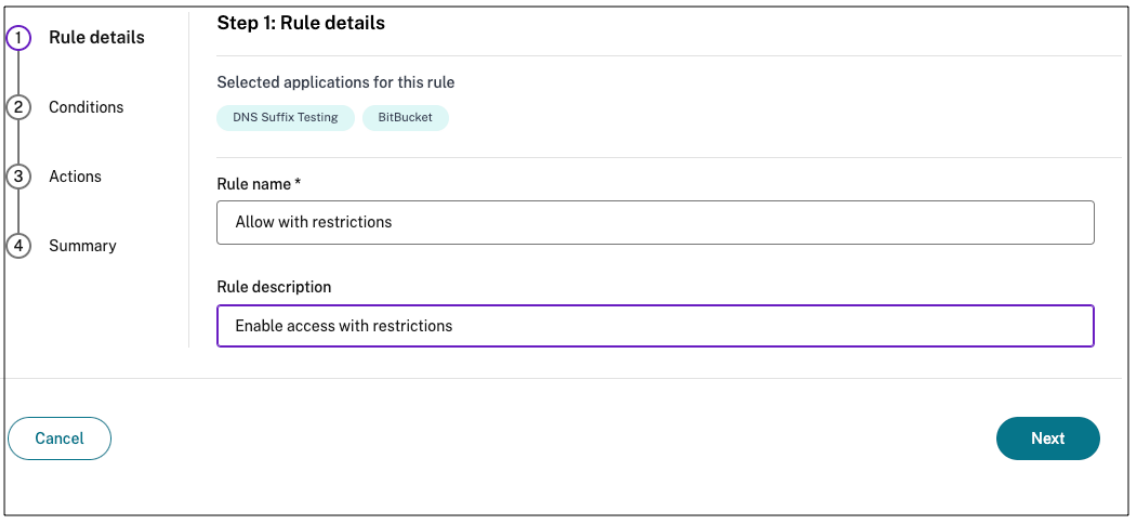
   初めてのユーザの場合、[アクセスポリシー（**Access** Policies）] ランディングページにはポリシーが表示されません。ポリシーを作成すると、ここに一覧表示されます。

2. ポリシー名とポリシーの説明を入力します。
3. 「アプリケーション」で、このポリシーを適用する必要があるアプリまたはアプリのセットを選択します。

4.「**Create Rule** 」をクリックして、ポリシーのルールを作成します。

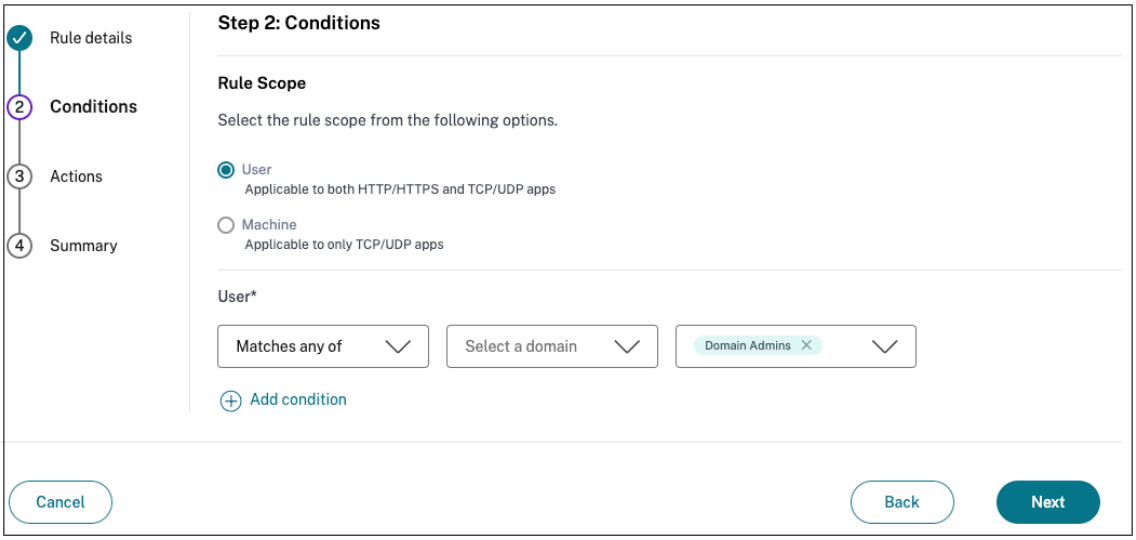


5. ルール名とルールの簡単な説明を入力して、[次へ] をクリックします。



6. ユーザーの条件を選択します。ユーザー条件は、ユーザーにアプリケーションへのアクセスを許可するための必須条件です。次のいずれかを選択します:

   - いずれかに一致—フィールドに表示されている名前のいずれかに一致し、選択したドメインに属するユーザーまたはグループのみがアクセスを許可されます。
   - いずれにも一致しない -フィールドに表示され、選択したドメインに属するユーザーまたはグループを除くすべてのユーザーまたはグループがアクセスを許可されます。



7. (オプション) コンテキストに基づいて複数の条件を追加するには、「+」をクリックします。

   コンテキストに基づいて条件を追加すると、ユーザーとオプションのコンテキストベースの条件が満たされた場合にのみポリシーが評価される条件に AND 操作が適用されます。状況に応じて次の条件を適用できます。

   - ** デスクトップまたはモバイルデバイス ** —アプリへのアクセスを有効にするデバイスを選択します。
   - 位置情報—ユーザーがアプリにアクセスしている条件と地理的位置を選択します。
     - いずれかにマッチ**:** リストされている地理的場所のいずれかからアプリにアクセスしているユーザーまたはユーザーグループのみがアプリへのアクセスを有効にします。
     - いずれにも一致しない**:** リストされている地域のユーザーまたはユーザーグループ以外のすべてのユーザーまたはユーザーグループがアクセス可能です。
   - ネットワークの場所—ユーザーがアプリにアクセスする際に使用する条件とネットワークを選択します。
     - いずれかにマッチ**:** リストされているネットワークロケーションのいずれかからアプリにアクセスするユーザーまたはユーザーグループのみが、アプリへのアクセスを有効にします。
     - どれにも一致しない**:** リストされているネットワークロケーション以外のすべてのユーザーまたはユーザーグループがアクセス可能です。
   - デバイスポスチャチェック—アプリケーションにアクセスするためにユーザーデバイスが通過しなければならない条件を選択します。
   - ユーザーリスクスコア—ユーザーにアプリケーションへのアクセスを提供する必要があるリスクスコアカテゴリを選択します。
   - ワークスペース **URL**-管理者は、ワークスペースに対応する完全修飾ドメイン名に基づいてフィルターを指定できます。
     - 次のいずれかに一致する -受信ユーザー接続が設定されたワークスペース URL のいずれかに一致する場合にのみアクセスを許可します。
     - すべて一致 -受信ユーザー接続が設定されたワークスペース URL のすべてを満たす場合にのみアクセスを許可します。

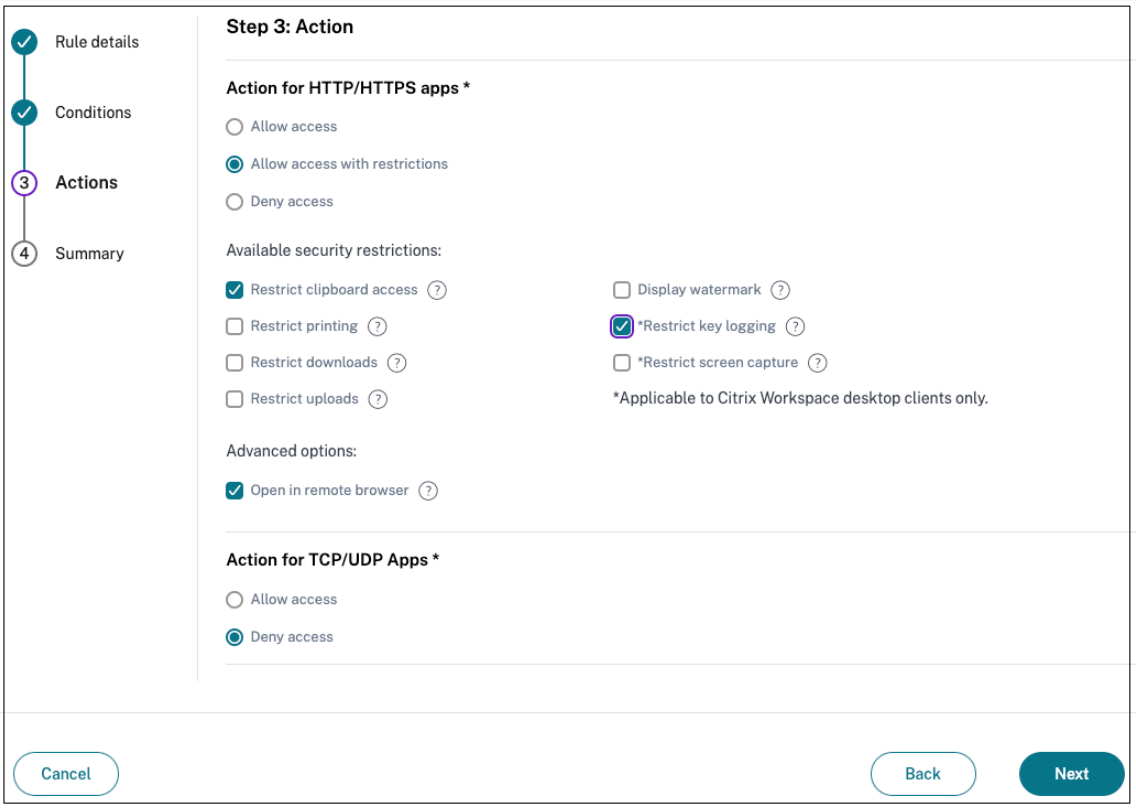
8. [次へ] をクリックします。

9. 条件評価に基づいて適用する必要があるアクションを選択します。

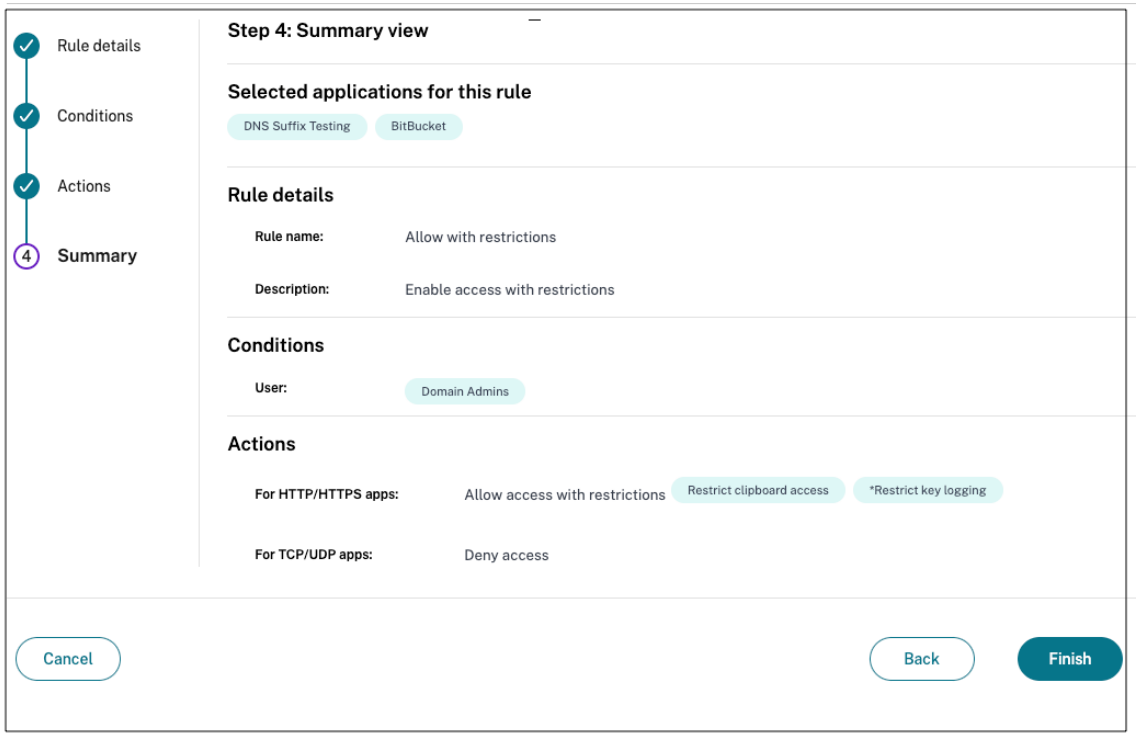
   - HTTP/HTTPS アプリの場合、以下を選択できます。
     - アクセスを許可
     - 制限付きでアクセスを許可
     - アクセスを拒否

     > 注:
     >
     > [制限付きアクセスを許可] を選択した場合は、アプリに適用する制限を選択する必要があります。制限の詳細については、「使用可能なアクセス制限オプション」を参照してください。また、アプリをリモートブラウザで開くか、Citrix Secure Browser で開くかを指定することもできます。

   - TCP/UDP アクセスでは、以下を選択できます。
     - アクセスを許可
     - アクセスを拒否



10. [次へ] をクリックします。「概要」ページには、ポリシーの詳細が表示されます。
11. 詳細を確認して [完了] をクリックします。



ポリシー作成後に覚えておくべきポイント

- 作成したポリシーは [ポリシールール] セクションに表示され、デフォルトで有効になっています。必要に応じてルールを無効にできます。ただし、ポリシーをアクティブにするには、少なくとも 1 つのルールが有効になっていることを確認してください。
- デフォルトでは、ポリシーには優先順位が割り当てられます。値が小さい優先度が最も高くなります。優先順位が最も低いルールが最初に評価されます。ルール (n) が定義された条件と一致しない場合、次のルール (n+1) が評価され、以降も同様です。

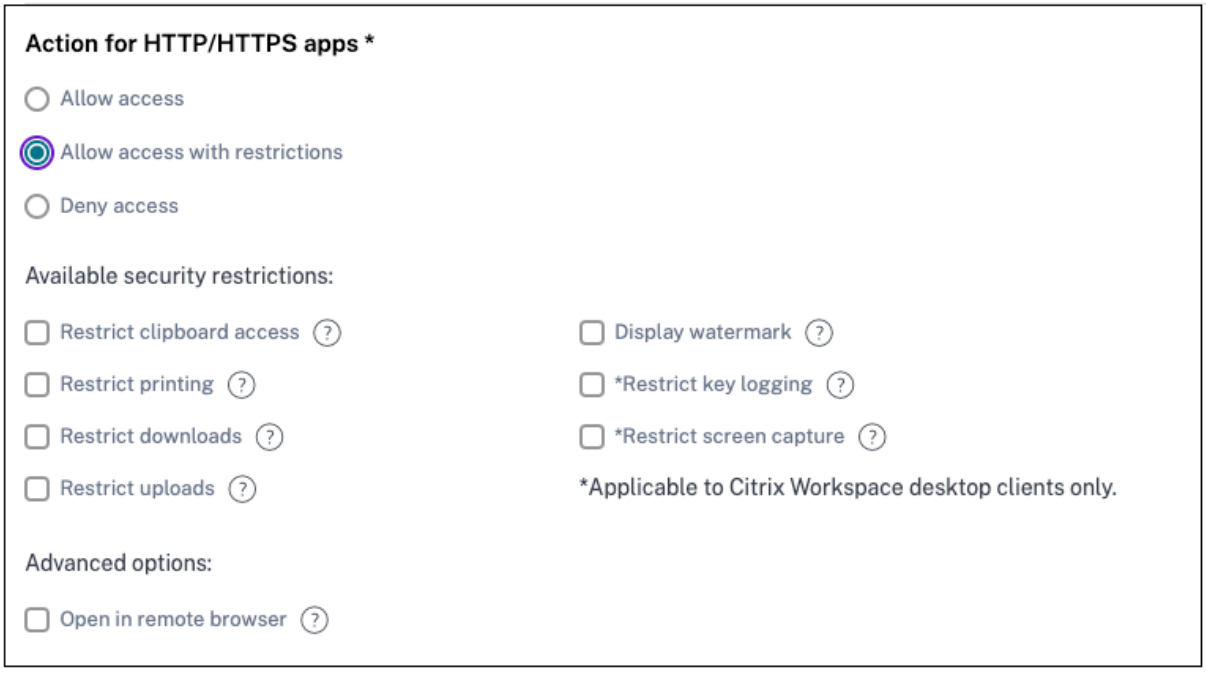
優先順位の例によるルールの評価**:**

ルール 1 とルール 2 の 2 つのルールを作成したとします。
ルール 1 はユーザー A に割り当てられ、ルール 2 はユーザー B に割り当てられます。その後、両方のルールが評価されます。
ルール 1 とルール 2 の両方がユーザー A に割り当てられているとします。この場合、ルール 1 の優先順位が高くなります。ルール 1 の条件が満たされると、ルール 1 が適用され、ルール 2 はスキップされます。それ以外の場合、ルール 1 の条件が満たされない場合、ルール 2 がユーザー A に適用されます。

> 注記**:**
>
> どのルールも評価されない場合、アプリはユーザーに列挙されません。

利用可能なアクセス制限オプション

「制限付きアクセスを許可する」アクションを選択するときは、セキュリティ制限を少なくとも 1 つ選択する必要があります。これらのセキュリティ制限は、システムであらかじめ定義されています。管理者は、他の組み合わせを変更したり追加したりすることはできません。次のセキュリティ制限をアプリケーションに対して有効にできます。



- クリップボードへのアクセスを制限**:** アプリとシステムクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- 印刷の制限：Citrix Enterprise Browser 内からの印刷機能を無効にします。
- ダウンロードを制限する**:** ユーザーがアプリ内からダウンロードできないようにします。
- アップロードを制限する**:** ユーザーがアプリ内でアップロードできないようにします。
- ウォーターマークを表示**:** ユーザーの画面にウォーターマークを表示し、ユーザーのマシンのユーザー名と IP アドレスを表示します。
- キーロギングの制限**:** キーロガーから保護します。ユーザーがユーザー名とパスワードを使用してアプリにログオンしようとすると、すべてのキーがキーロガーで暗号化されます。また、ユーザーがアプリで実行するすべてのアクティビティは、キーロギングから保護されます。たとえば、Office 365 のアプリ保護ポリシーが有効になっていて、ユーザーが Office 365 の Word 文書を編集した場合、すべてのキーストロークはキーロガーで暗号化されます。
- 画面キャプチャを制限する**:** 画面キャプチャプログラムまたはアプリのいずれかを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとすると、空白の画面がキャプチャされます。
- リモートブラウザーで開く：Citrix リモートブラウザーでアプリを開きます。
  - [リモートブラウザで開く] を選択し、Secure Private Access のリモートブラウザカタログが見つからない場合は、次のメッセージが表示されます：

    このアプリケーションをホストできる公開リモート隔離カタログはありません。*Remote Browser Isolation* コンソールに移動して、カタログを公開します。

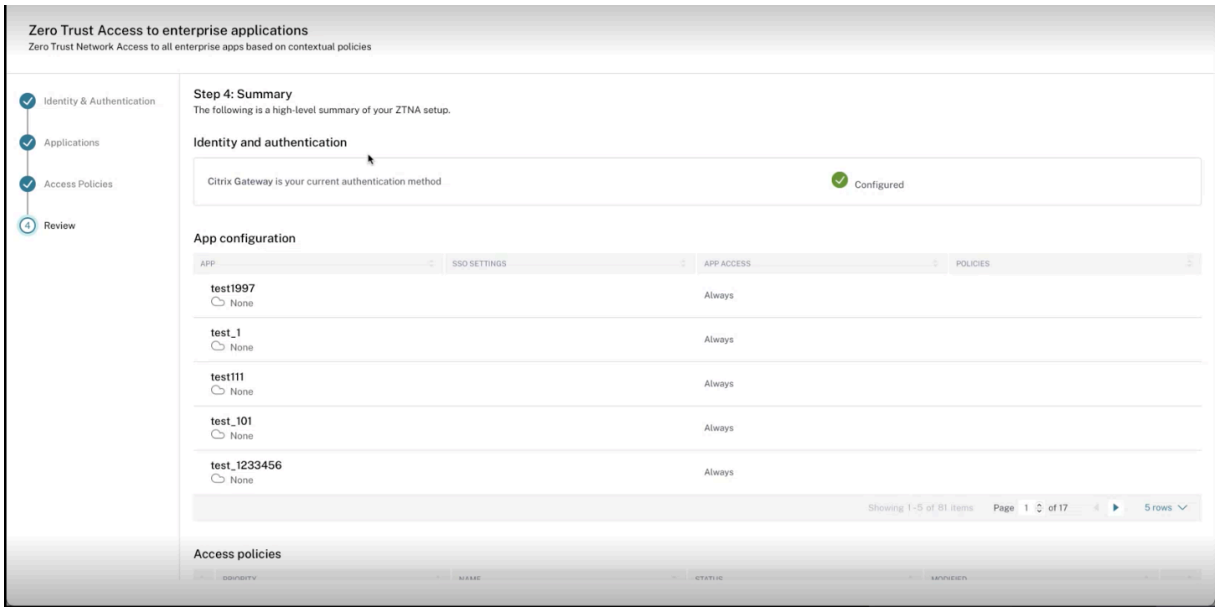
- また、Web アプリや SaaS アプリを起動しようとしたときに、RBI カタログが欠落していて次のメッセージが表示されると、アプリの起動が失敗します。

  このリクエストを処理するカタログは作成されていません。管理者に連絡してください。

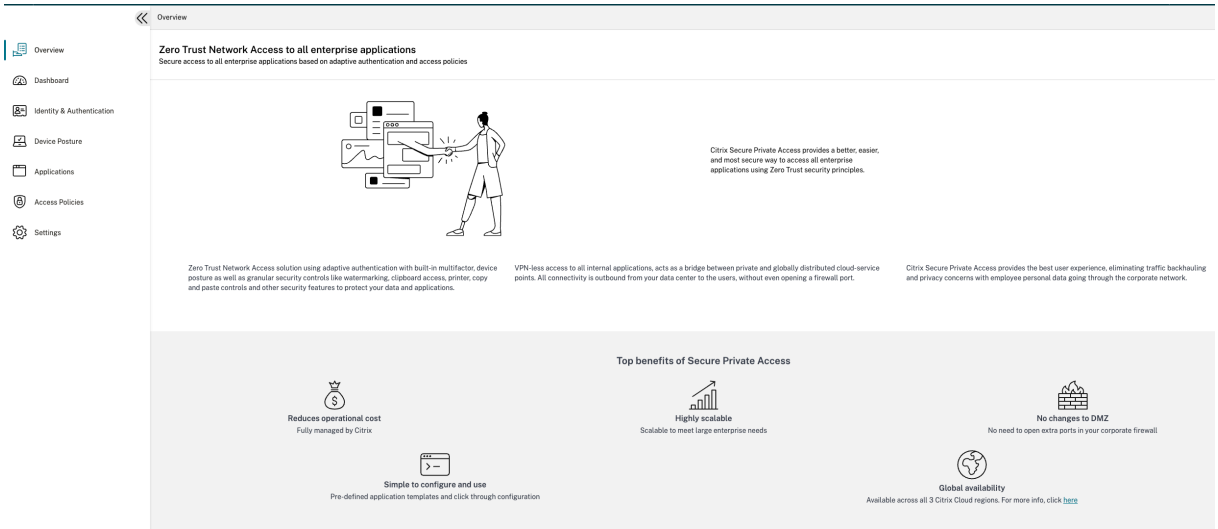
Citrix Remote Browser Isolation について詳しくは、「Remote Browser Isolation」を参照してください。

ステップ **4:** 各構成の概要を確認する

[Review] ページから、完全なアプリ構成を表示し、[閉じる] をクリックできます。



次の図は、4 ステップ構成を完了した後のページを示しています。



> 重要:
>
> - ウィザードを使用して構成を完了したら、そのセクションに直接移動してセクションの設定を変更できます。シーケンスに従う必要はありません。
> - 構成済みのアプリまたはポリシーをすべて削除した場合は、それらを再度追加する必要があります。この場合、すべてのポリシーを削除すると、次の画面が表示されます。

ポリシー・モデリング・ツール

June 19, 2024

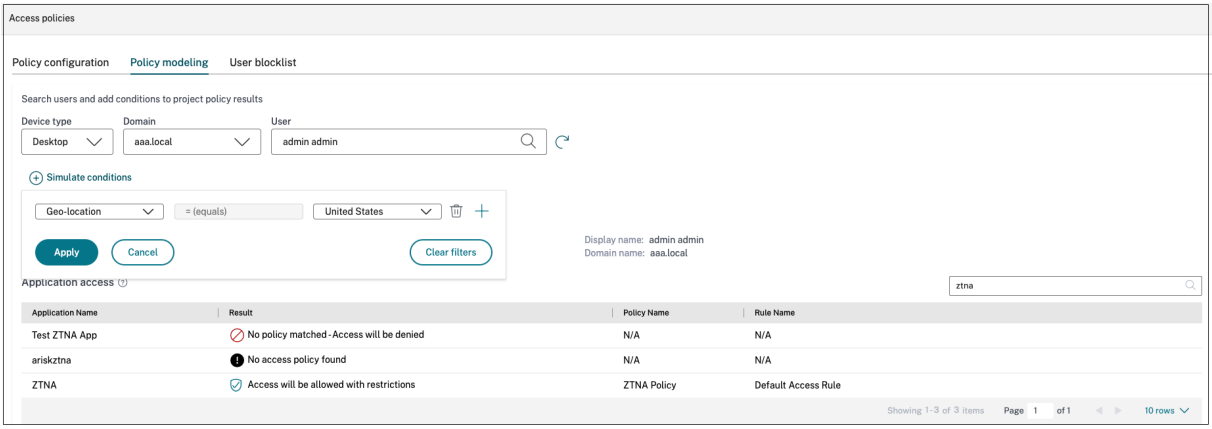
管理者は複数のポリシーを作成し、それらのポリシーを複数のアプリケーションに割り当てることができます。その結果、管理者がエンドユーザーのアプリケーションアクセス結果を理解するのが難しくなる可能性があります。つまり、エンドユーザーがアプリケーションとアクセスポリシーの設定に基づいてアクセスを許可または拒否された場合です。ポリシーモデリングツール ([アクセスポリシー**] > [**ポリシーモデリング]) は、予想されるアプリケーションアクセス結果 (許可/許可/制限/拒否) を管理者が完全に把握できるようにすることで、これらの問題を解決するのに役立ちます。管理者は特定のユーザーのアクセス結果を確認し、デバイスの種類、デバイスの状態、位置情報、ネットワークの場所、ユーザーリスクスコア、ワークスペースの URL などのユーザー条件を追加できます。このツールには、アプリケーションに関連するポリシーとルール名のリストも表示されます。

アクセスポリシーの設定を分析するには、次の手順を実行します。

1. Secure Private Access コンソールで、「アクセスポリシー」をクリックし、「ポリシーモデリング」タブをクリックします。
2. 次の詳細を追加します:
   - デバイスタイプ: エンドユーザーのデバイスタイプを選択します。(デフォルトでは [デスクトップ] が選択されています。)
   - ドメイン: ユーザーに関連付けられているドメインを選択します。
   - ユーザー: アプリケーションおよび関連するポリシーを分析するユーザー名を選択します。
3. また、エンドユーザーとそのデバイスで一連の条件/制約をシミュレートすることもできます。

4. [条件をシミュレート] をクリックします。
5. 条件 (デバイスポスチャ、位置情報、ネットワークロケーション、ユーザーリスクスコア、ワークスペース URL) を選択し、関連する値を選択します。
6. **+** 記号をクリックして条件を追加します。
7. [適用] をクリックします。

選択したユーザーのアプリケーション、関連するポリシー、およびルールが表形式で表示されます。



ダッシュボードの概要

June 19, 2024

Secure Private Access サービス・ダッシュボードには、SaaS、Web、TCP、UDP アプリケーションの診断と使用状況データが表示されます。管理者は、管理者がアプリ、ユーザー、コネクタのヘルスステータス、帯域幅の使用状況を 1 か所で完全に把握して利用できます。このデータは Citrix Analytics から取得されます。さまざまなエンティティのデータは、事前設定された時間またはカスタムタイムラインで表示できます。一部のエンティティでは、ドリルダウンして詳細を表示できます。

メトリックは大きく次のカテゴリに分類されます。

- ロギングとトラブルシューティング
  - 診断ログ: 認証、アプリケーションの起動、アプリケーションの列挙、デバイスポスチャのチェックに関連するログ。
- ユーザー
  - アクティブユーザー: 選択した時間間隔でアプリケーション (SaaS、Web、TCP) にアクセスしたユニークユーザーの総数。
  - アップロード: 選択した時間間隔で Secure Private Access サービスを介してアップロードされたデータ量の合計です。

  - ダウンロード: 選択した期間に Secure Private Access サービスを通じてダウンロードされたデータの総量。

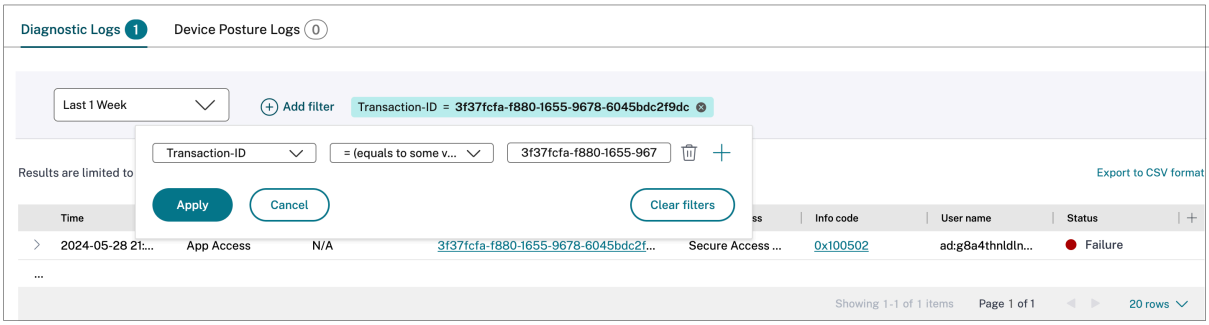
- アプリケーション**:**
  - アプリケーション: 現在設定されているアプリケーションの総数 (時間間隔は関係ありません)。
  - アプリケーション起動回数: 選択した時間間隔で各ユーザーが起動したアプリケーション (アプリセッション) の総数。
  - 設定済みドメイン: 選択した時間間隔に設定されたドメインの総数。
  - 検出されたアプリケーション: アクセスされたが、どのアプリとも関連付けられていない固有の個別ドメインの総数

- アクセスポリシー
  - アクセスポリシー: 現在設定されている（時間間隔に関係なく）アクセスポリシーの総数。

診断ログ

Diagnostics Logs チャートを使用すると、認証、アプリケーションの起動、アプリの列挙に関連するログだけでなく、デバイスの状態に関するログも確認できます。[**See more**] リンクをクリックすると、ログの詳細を表示できます。詳細は表形式で表示されます。事前に設定した時間またはカスタムタイムラインのログを表示できます。ダッシュボードに表示したい情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログは CSV 形式にエクスポートできます。

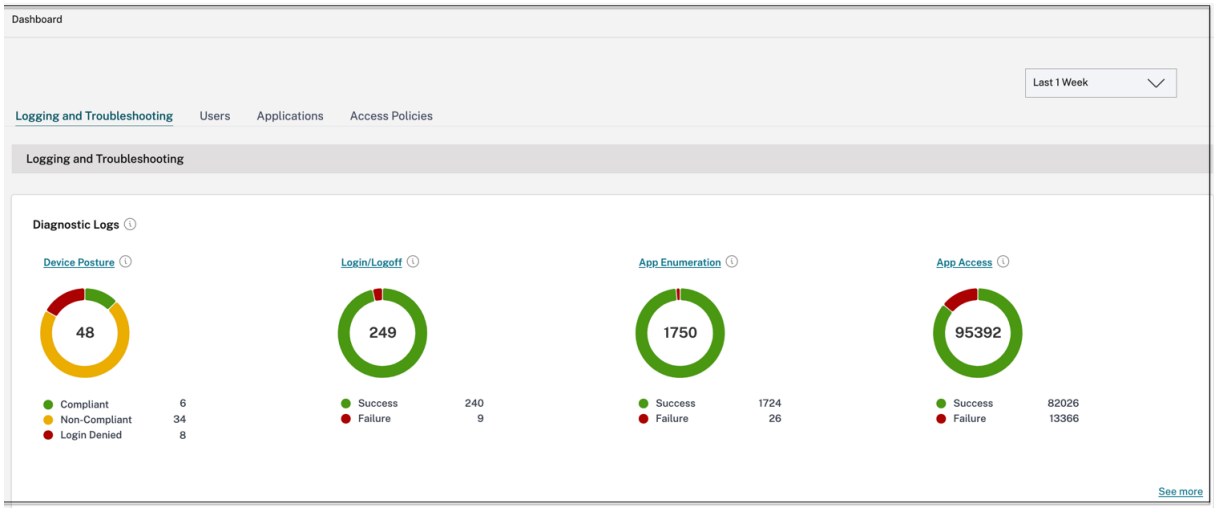
- [フィルターを追加] オプションを使用すると、アプリの種類、カテゴリ、説明などのさまざまな条件に基づいて検索を絞り込むことができます。たとえば、検索フィールドで、`Transaction ID`、`= (equals to some value)` を選択し、この順序で`7456c0fb-a60d-4bb9-a2a2-edab8340bb15`を入力すると、このトランザクション ID に関連するすべてのログを検索できます。フィルターオプションで使用できる検索演算子の詳細については、「検索演算子」を参照してください。



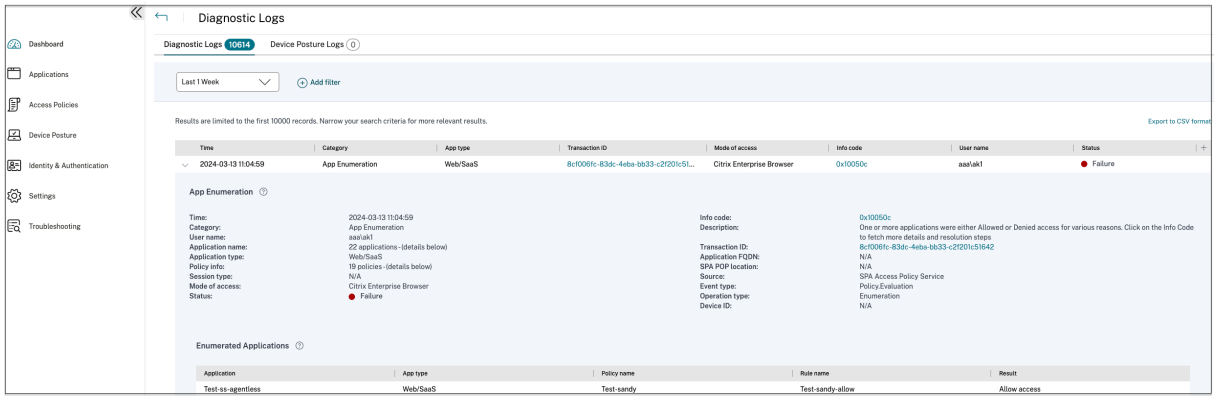
- デバイスポスチャログ**:** ポリシー結果 (準拠、非準拠、ログイン拒否) に基づいて検索を絞り込むことができます。デバイスポスチャについて詳しくは、「デバイスポスチャ」を参照してください。

注記:

- Secure Private Access 診断ログダッシュボード内のすべての障害イベントには、関連する情報コードがあります。詳細については、「情報コード」を参照してください。
- トランザクション ID は、アクセスリクエストのすべての Secure Private Access ログを関連付けます。詳細については、「トランザクション ID」を参照してください。



- 展開アイコン (>) をクリックすると、ログの詳細をすべて表示できます。
- 診断ログページには、アクセスされた各メイン URL の埋め込みドメインが表示されます。管理者は、メイン URL の展開アイコン (>) をクリックして埋め込みドメインを表示できます。管理者は埋め込みドメインリストを使用して、アプリアクセスやアプリのレンダリングに関連する問題に対処できます。たとえば、アプリケーション構成でドメインが見つからない場合、エンドユーザーは特定のアプリケーションにアクセスできません。この場合、管理者は埋め込みドメインのリストを表示し、見つからないドメインを特定し、見つからないドメインでアプリ設定を更新できます。



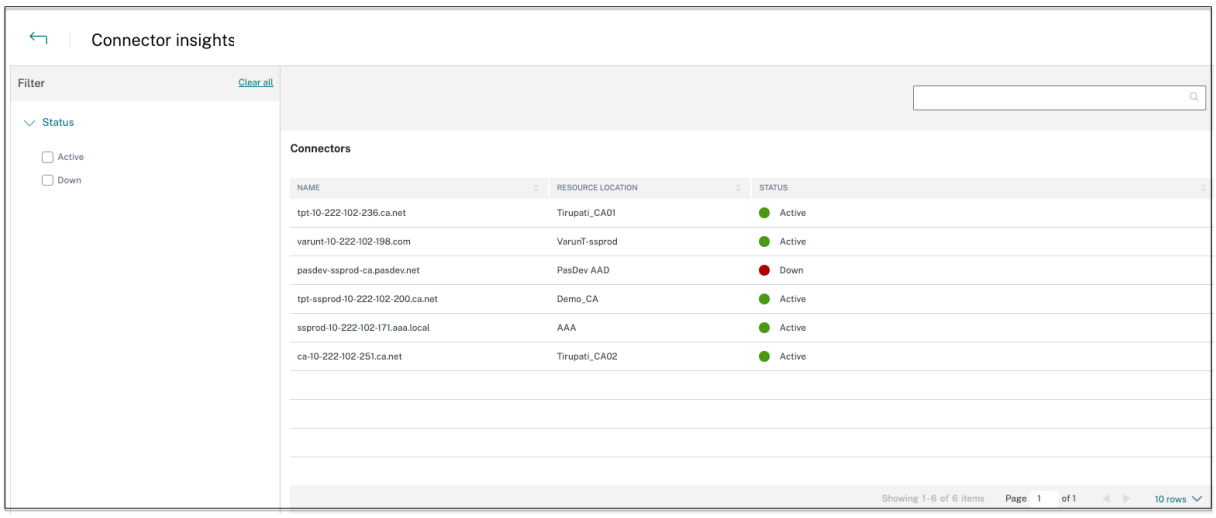
注記:

- デフォルトでは、診断ログページには今週のデータと最近の 10000 レコードのみが表示されます。カス

> タム日付検索とフィルターを使用して、検索結果をさらに絞り込みます。

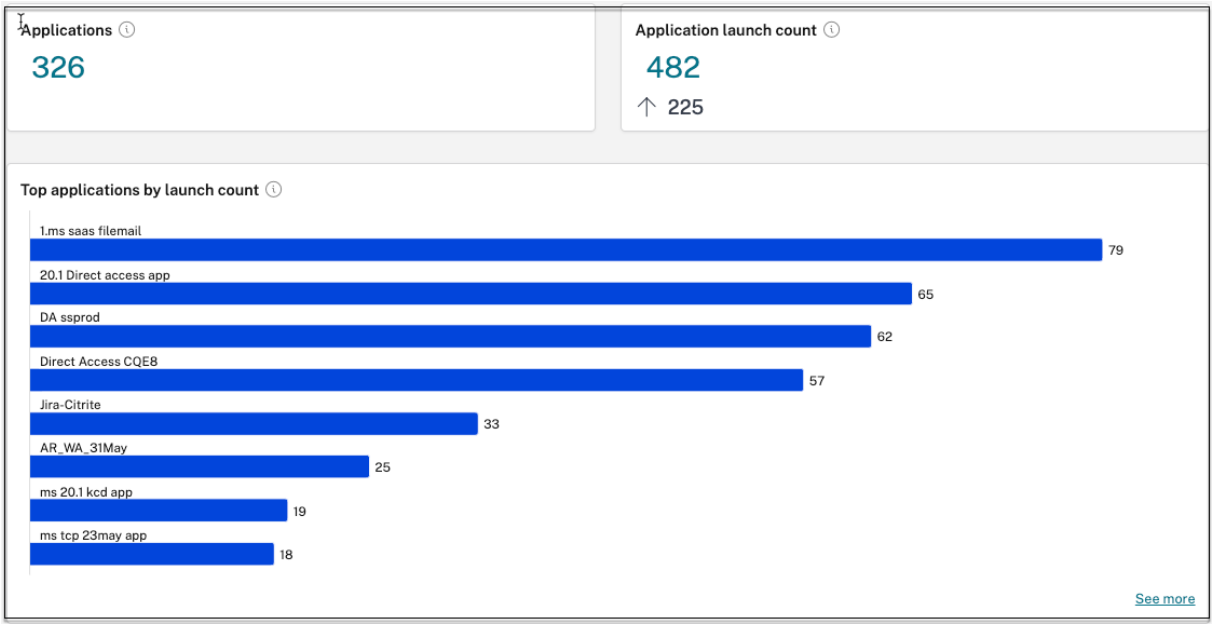
コネクタステータス

コネクタのステータスチャートを使用して、コネクタのステータスと、コネクタが展開されているリソースの場所を表示します。詳細を表示するには、**[**もっと見る] リンクをクリックします。[コネクタインサイト] ページでは、[アクティブ] または [非アクティブ] フィルタを使用して、ステータスに基づいてコネクタをフィルタリングできます。



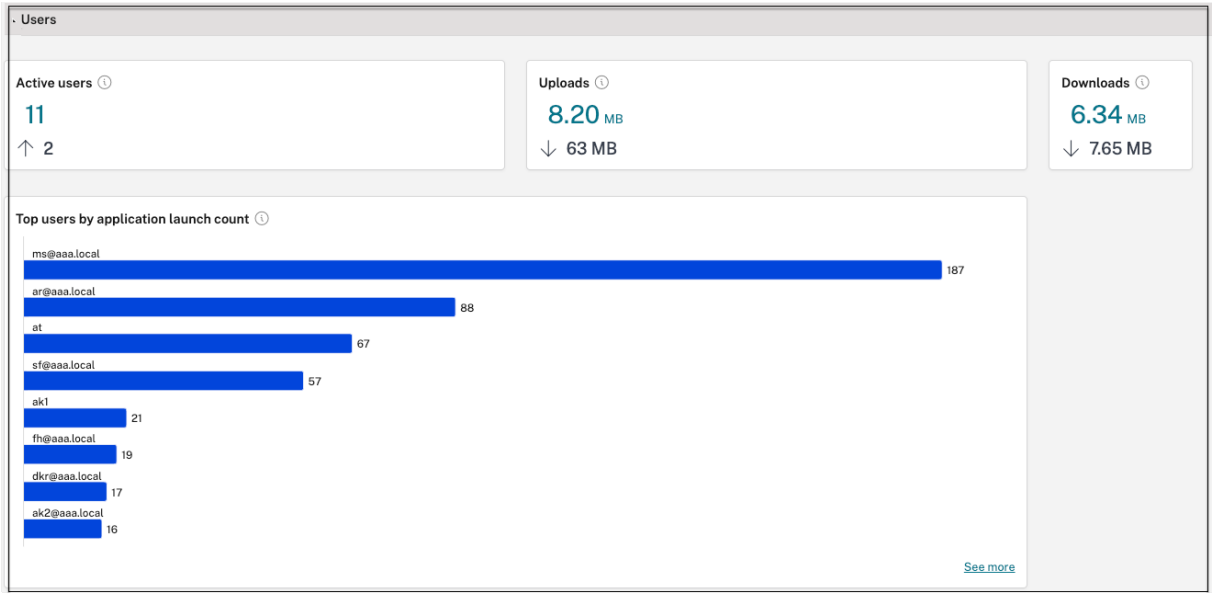
起動回数別の上位アプリケーション

「起動回数」グラフを使用すると、アプリの起動回数、アプリサーバーにアップロードされたデータの総量、およびアプリサーバーからダウンロードされたデータの総量に基づいて上位アプリケーションのリストが表示されます。**SaaS** アプリ、Web アプリ **、または **TCP/UDP** アプリのフィルターを適用して、特定のアプリに検索を絞り込むことができます。あらかじめ設定されたタイムラインまたはカスタムタイムラインのデータをフィルタリングできます。



アプリケーション起動数別の上位ユーザー数

「アプリケーション別上位ユーザー起動回数」グラフを使用して、ユーザーごとのデータを表示します。たとえば、ユーザーが TCP アプリを起動した回数、アプリサーバーにアップロードされたデータの総量、アプリサーバーからダウンロードされたデータの総量などです。あらかじめ設定されたタイムラインまたはカスタムタイムラインのデータをフィルタリングできます。

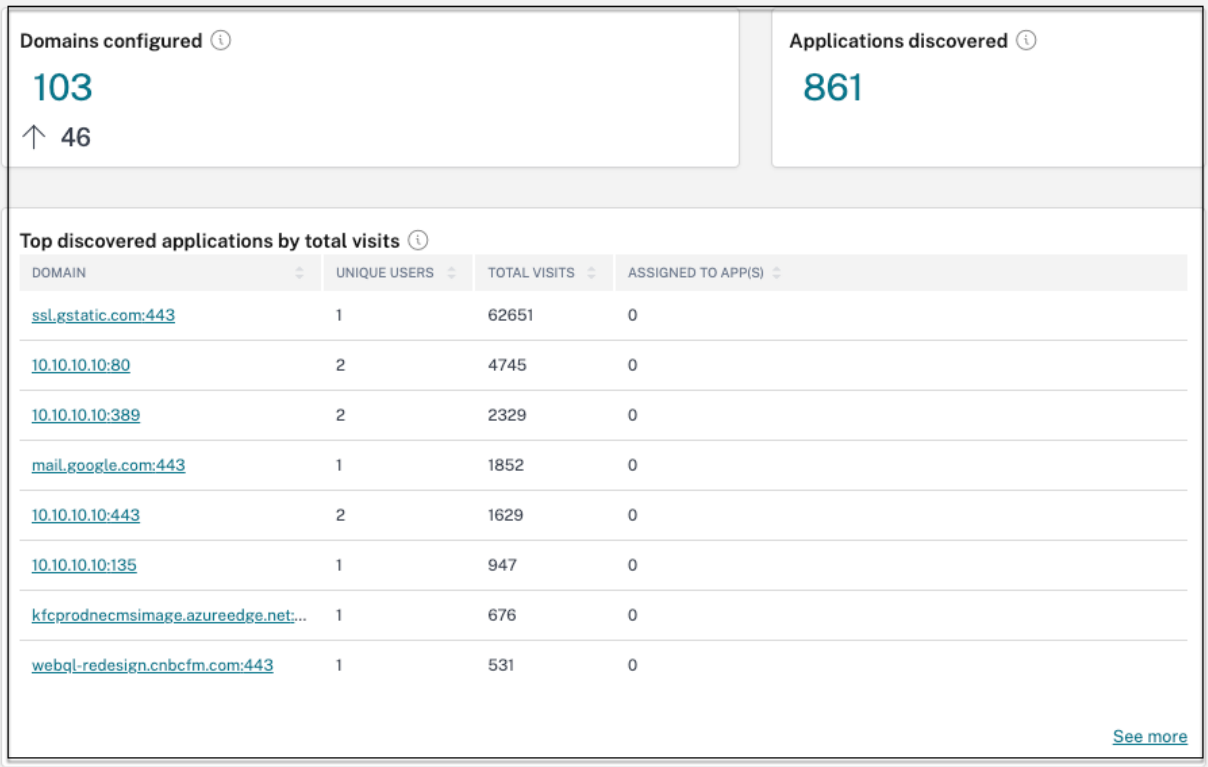


施行による上位のアクセスポリシー

[適用別の上位アクセスポリシー] グラフを使用して、アプリに適用されているアクセスポリシーのリストを表示します。[**See more**] リンクをクリックして、アプリに関連付けられているポリシーのリストと、ポリシーが適用される回数を表示します。また、[アクセスポリシー] ページの [検索] オプションを使用して、ポリシー名に基づいてポリシーをフィルタリングすることもできます。検索演算子を使用して特定のポリシーを検索し、検索をさらに絞り込むこともできます。詳細については、「検索演算子」を参照してください。

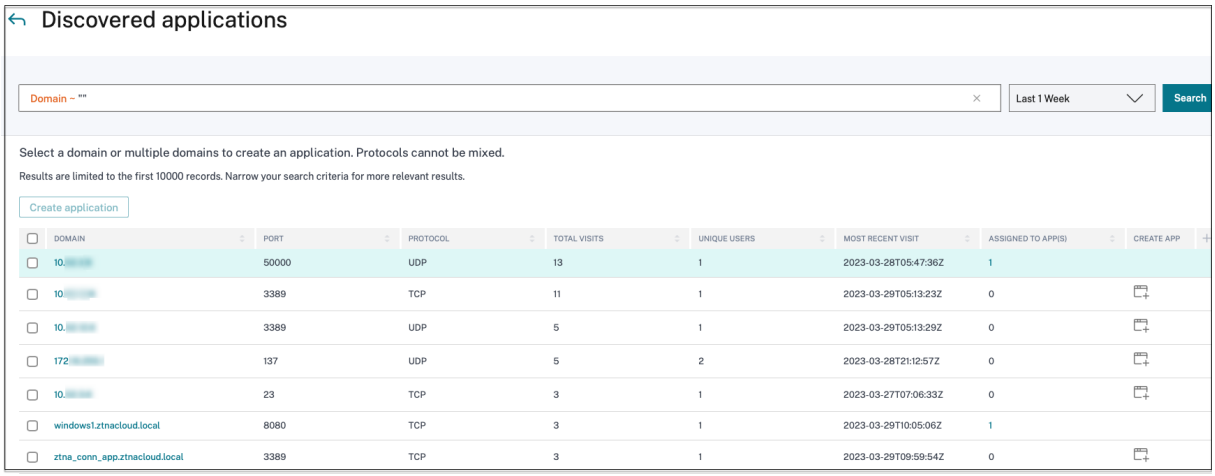
よく使われたアプリケーション

合計訪問数で上位に検出されたアプリケーションのグラフを使用すると、ある時点でアクセスされたが、どのアプリとも関連付けられていない固有の個別ドメインのリストを表示できます。これらのドメインは、それらのドメインへの総訪問数に基づいて一覧表示されます。管理者はこのグラフを使用して、特定の関心のあるドメインに多数のユーザーがアクセスしているかどうかを確認できます。このような場合、管理者は簡単にアクセスできるようにそのドメインでアプリを作成できます。



グラフの「ASSIGNED TO **APps** 」列には、このドメインが関連 URL または宛先 URL 値の一部として構成されているアプリケーションの総数が表示されます。番号をクリックすると、このドメインに割り当てられているアプリが表示されます。

「もっと見る」リンクをクリックすると、すべてのドメインの詳細を表示できます。



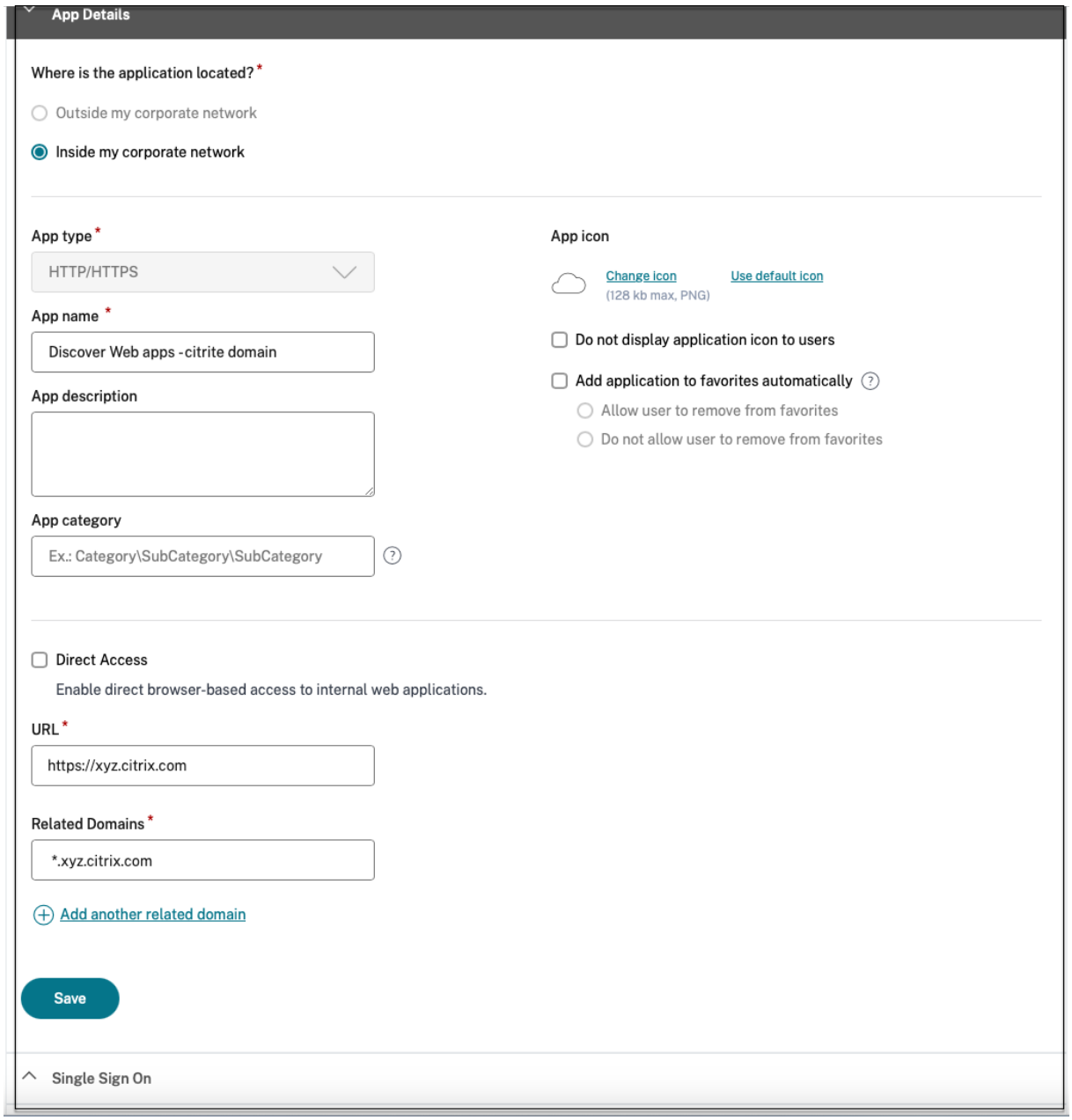
「検出されたアプリケーション」ページには、ドメイン名、ポート、プロトコル、総訪問数、ユニークユーザー数、最新の訪問日など、ドメインの詳細が表示されます。グラフのすべての列はソート可能です。検索バーを使用して、ドメインに基づいて検索できます。

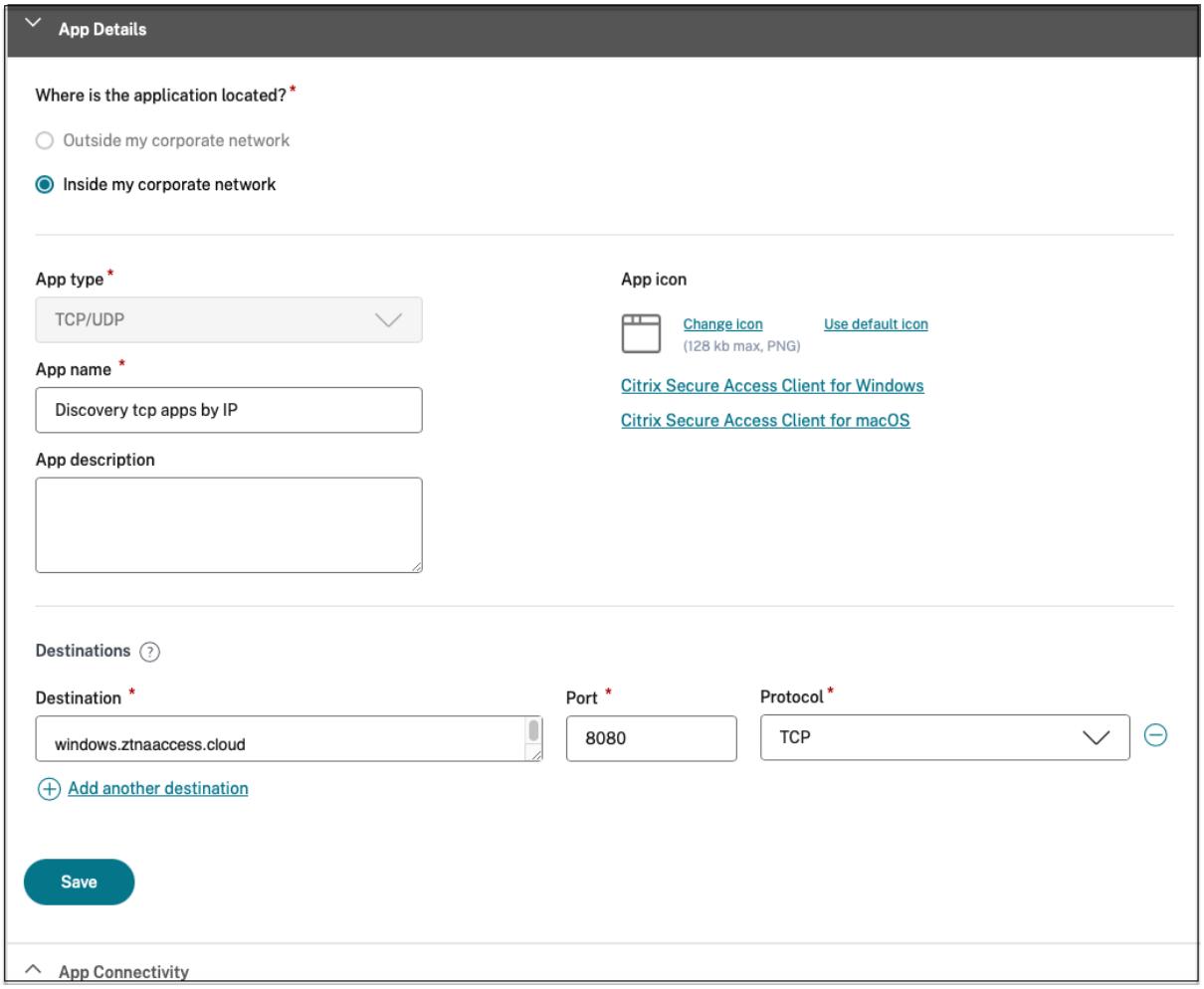
> 注記:
>
> - プロトコルは、お客様が使用する標準ポートに基づいて作成されます。
> - 検出されたドメインのリストは 10000 レコードに制限されています。

チャートからアプリを作成

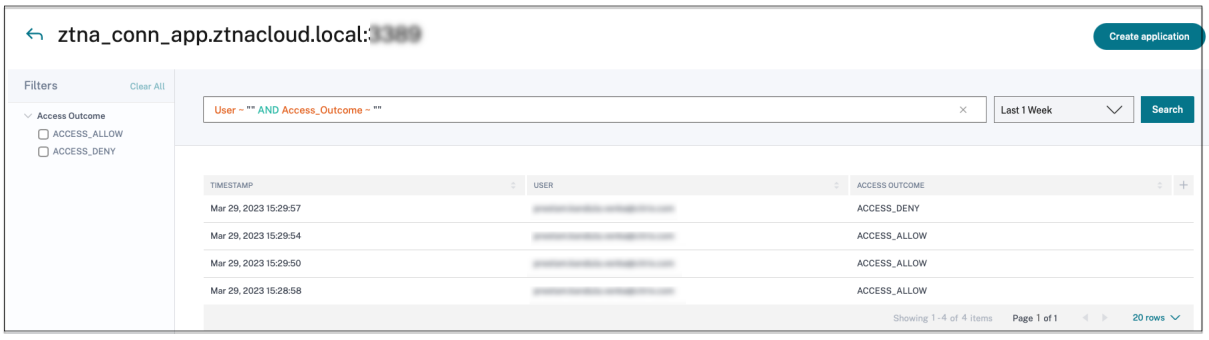
それぞれのドメインの横にある「**+**」アイコンをクリックして、アプリを作成します。アプリ構成ウィザードがポップアップします。同じドメイン、ポート、およびプロトコルの組み合わせでアプリがすでに作成されていて、完了状態にある行には、アプリ作成アイコンは表示されません。

- アプリタイプは、選択したアプリのプロトコルに基づいて自動入力されます。ただし、必要に応じてタイプを変更することができます。
- [**URL**]、**[**関連ドメイン**]**、**[**宛先**]**、**[**ポート**]**、**[**プロトコル] フィールドの値はすべて自動入力されます。アプリを追加する手順を完了します。詳しくは、簡単なオンボーディングとセットアップのための管理者ガイド付きワークフローをご覧ください。





また、固有のドメインのリンクをクリックして詳細を表示し、そのドメインのアプリケーションを作成することもできます。ドメインリンクをクリックすると、そのドメインのユーザー認証ログが表示されます。[アプリケーションの作成] ボタンをクリックします。アプリを追加する手順を完了します。



検索演算子

検索を絞り込むために使用できる検索演算子は次のとおりです:

- **= (**ある値と等しい**)**: 検索条件に完全に一致するログ/ポリシーを検索します。
- **!= (**一部の値と等しくない**)**: 指定された条件を含まないログ/ポリシーを検索します。
- **~ (**値を含む**)**: 検索条件に部分的に一致するログ/ポリシーを検索します。
- **!~ (**値を含まない**)**: 指定された条件の一部を含まないログ/ポリシーを検索します。

アプリケーションディスカバリー

January 9, 2024

アプリケーション検出機能により、管理者は組織内の Web アプリやクライアントサーバーアプリ（TCP および UDP ベースのアプリ）などの内部のプライベートアプリケーションと、それらのアプリケーションにアクセスしているユーザーを把握できます。管理者は、ドメイン (ワイルドカードドメイン) または IP サブネットの範囲を指定してアプリを検索できます。Citrix Secure Private Access サービスでアプリケーション検出機能を有効にするには、管理者はアプリケーションとユーザーアクセスを検出して報告する必要があるサブネットまたはワイルドカードドメイン、あるいはその両方を構成する必要があります。管理者は、アプリケーション構成ワークフローを使用して広範なサブネットとワイルドカードドメインを定義し、すべてのアプリケーション定義構成に使用されるのと同じアプリケーションアクセスポリシーワークフローを完了します。

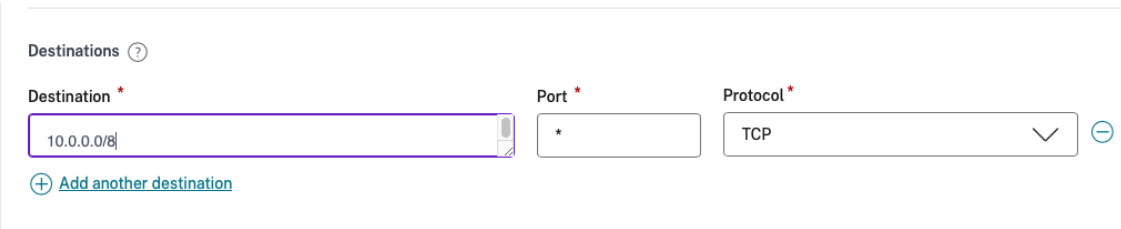
アプリケーションディスカバリーの設定

アプリケーションの検出は、次のいずれかの方法で行うことができます。

- TCP/UDP ベースの正確な IP アドレス宛先とポートを監視および報告するようにシステムを設定します。

  サブネットを TCP/UDP プロトコルとポートの範囲とともに指定します (範囲全体を含めるには * を入力してください)。これにより、セキュアアクセスエージェントからすべての TCP アプリと UDP アプリを検出できます。

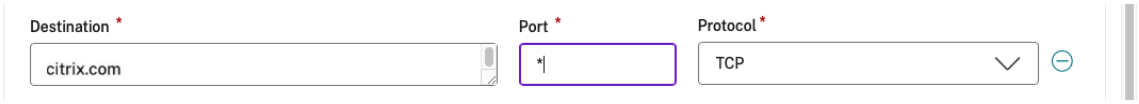
  例:10.0.0.0/8: TCP: ポート (*)



- TCP または UDP プロトコルを使用してアクセスされたアプリのホスト名または完全修飾ドメイン (FQDN)、あるいはその両方を監視して報告するようにシステムを設定します。

  監視および報告が必要なウェブアプリに属するワイルドカードドメインを指定します。

  例: `*.citrix.com : TCP : Port (*)`



- Citrix Enterprise Browser からアクセスされる可能性のある完全修飾ドメイン（FQDN）を監視して報告するようにシステムを構成します。

  内部 Web アプリを検索するドメインまたはサブドメインに属するウェブアプリには、少なくとも 1 つの FQDN を指定します。そのアプリが属するワイルドカードドメインを含むように関連ドメインを設定します。

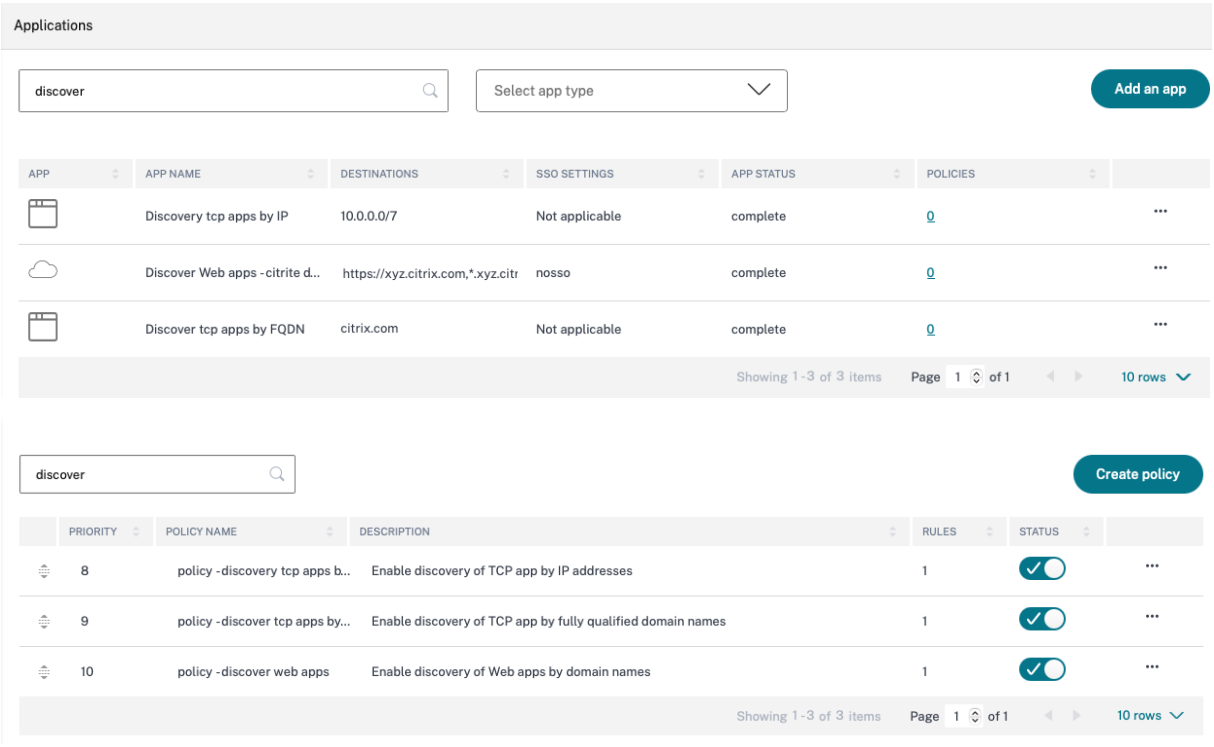
  例:

  Web アプリ URL: `https://test.citrix.com/`

  関連ドメイン:*.citrix.com

> 重要:
>
> - アプリの作成に加えて、設定されたドメインと IP サブネットを使用してアプリへのアクセスを許可するユーザーも定義する必要があります。これは、許可されているユーザーグループ外の他のユーザーグループからの不正または不注意によるアクセスを防ぐためです。
> - アプリ名に「**Discover**」というプレフィックスを追加して、これが検出の監視とレポート作成を可能にする特別なアプリ構成であることを示します。この名前を付けておくと、ワイルドカードドメインか IP サブネット、あるいはその両方を削除すべきかを判断しやすくなり、数週間後または 1 か月後に、アプリ

> アクセスゾーン全体を特定の FQDN と IP/ポートの組み合わせだけに減らすことができます。



アプリケーションと対応するアクセスポリシーを作成した後も、ユーザーは引き続き Citrix Workspace アプリからアプリケーションにアクセスし、さまざまなドメインにアクセスできます。TCP/UDP アプリにアクセスするには、ユーザーは Citrix Secure Access Agent を使用する必要があります。さまざまなアクセス方法からのアプリアクセスは、アプリのドメインとサブネットの設定に基づいて監視され、ダッシュボードに報告されます。

アプリの設定と管理

January 9, 2024

Citrix Secure Private Access サービスを使用したアプリ配信は、アプリを管理するための簡単、安全、堅牢でスケーラブルなソリューションを提供します。クラウドで配信されるアプリケーションには、次のような利点があります。

- シンプルな構成 - 操作、更新、使用が簡単です。
- シングルサインオン—シングルサインオンで手間のかからないログオン。
- さまざまな SaaS アプリ用の標準テンプレート—一般的なアプリのテンプレートベースの構成。これらのテンプレートには、アプリケーションの構成に必要な情報の多くがあらかじめ入力されています。ただし、顧客に固有の情報のみを提供する必要があります。

エンタープライズ **Web** アプリのサポート

June 21, 2024

Secure Private Access サービスを使用した Web アプリケーション配信により、企業固有のアプリケーションを Web ベースのサービスとしてリモートで配信できます。一般的に使用される Web アプリには、SharePoint、Confluence、OneBug などがあります。

Web アプリケーションには、Secure Private Access サービスを使用して Citrix Workspace を使用してアクセスできます。Secure Private Access サービスと Citrix Workspace を組み合わせることで、構成済みの Web アプリ、SaaS アプリ、構成済みの仮想アプリ、またはその他のワークスペースリソースに対して統合されたユーザーエクスペリエンスを提供します。

SSO と Web アプリケーションへのリモートアクセスは、次のサービスパッケージの一部として利用できます。

- Secure Private Access スタンダード
- Secure Private Access アドバンス

システム要件

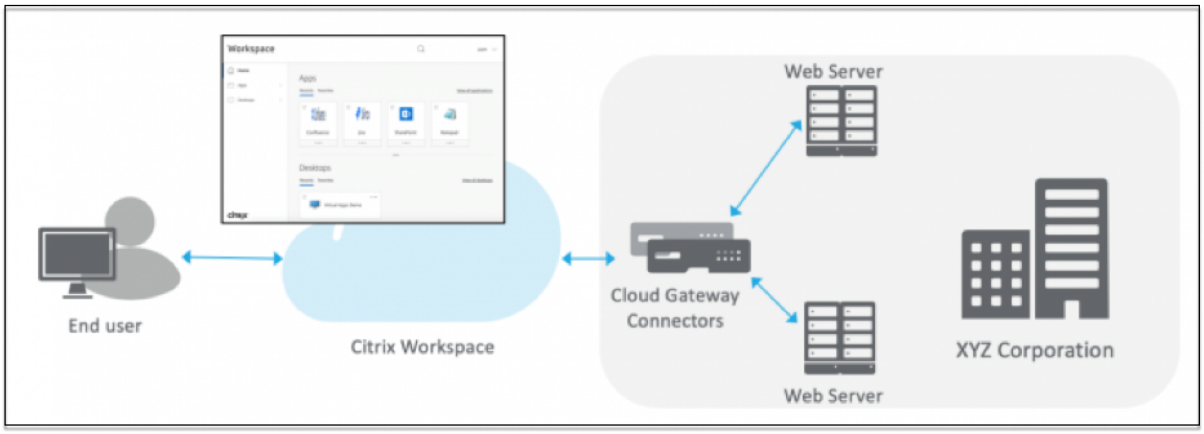
Connector Appliance -Connector Appliance を Citrix Secure Private Access サービスと併用すると、お客様のデータセンターのエンタープライズ Web アプリケーションへの VPN レスアクセスをサポートできます。詳しくは、「Connector Appliance による Secure Workspace Access」を参照してください。

機能

Citrix Secure Private Access サービスは、オンプレミスに展開されているコネクタを使用して、オンプレミスのデータセンターに安全に接続します。このコネクタは、オンプレミスで展開されるエンタープライズ Web アプリと Citrix Secure Private Access サービスの間のブリッジとして機能します。これらのコネクタは HA ペアで展開でき、送信接続のみが必要です。

Connector Appliance クラウド内の Citrix Secure Private Access サービス間の TLS 接続により、クラウドサービスに列挙されたオンプレミスアプリケーションが保護されます。Web アプリケーションは、VPN レス接続を使用して Workspace 経由でアクセスおよび配信されます。

次の図は、Citrix Workspace を使用した Web アプリケーションへのアクセスを示しています。



Web アプリを設定する

Web アプリの設定には、以下の大まかな手順が含まれます。

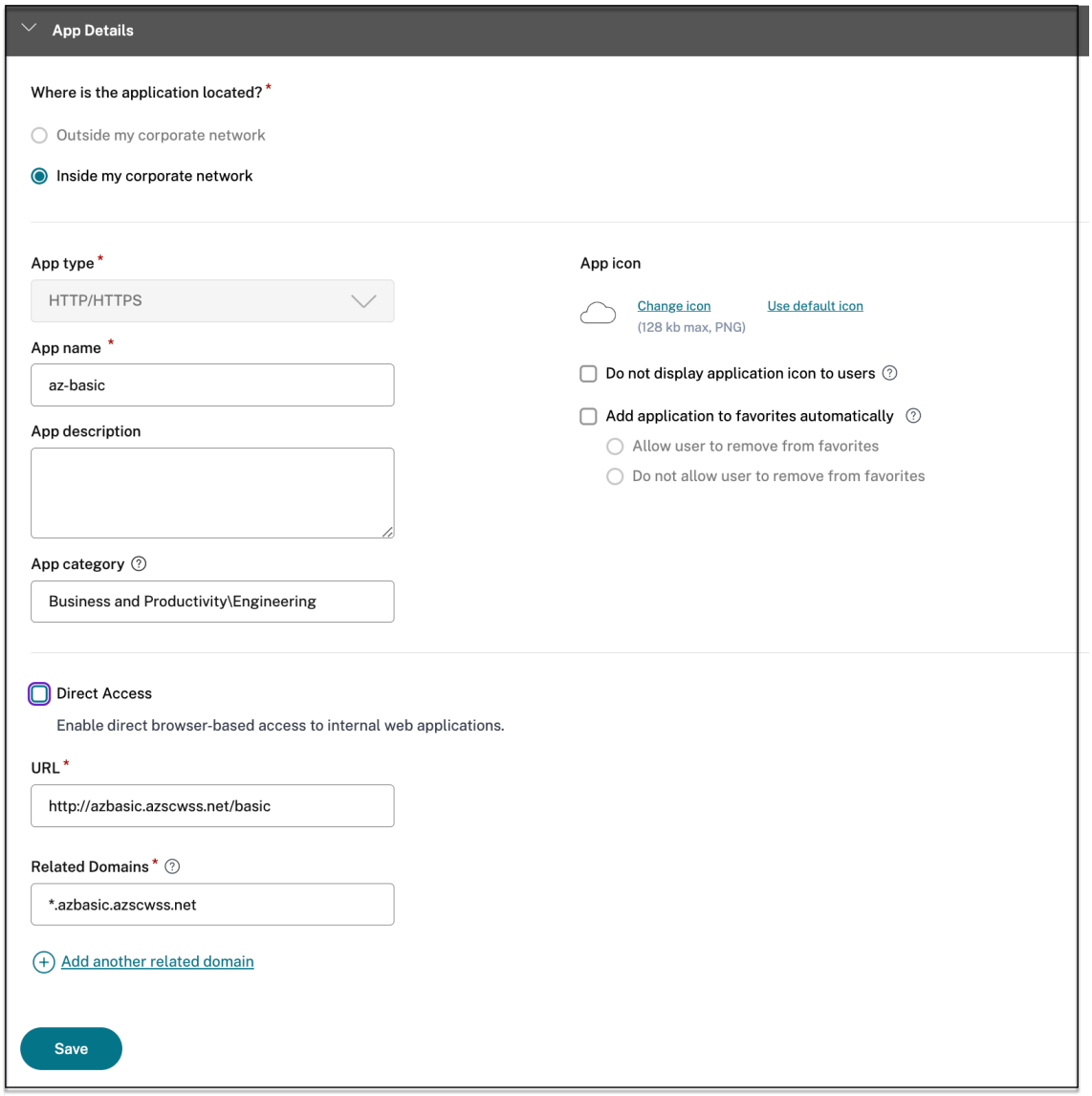
1. アプリケーションの詳細を設定
2. 希望するサインオン方法を設定する
3. アプリケーションルーティングの定義

アプリケーションの詳細を設定

1.「**Secure Private Access** 」タイルで、「管理」をクリックします。
2. Secure Private Access のランディングページで、[続行] をクリックし、[アプリの追加] をクリックします。

   > 注:
   >
   > [続行] ボタンは、ウィザードを初めて使用する場合にのみ表示されます。その後の使用では、[アプリケーション] ページに直接移動して [アプリの追加] をクリックできます。

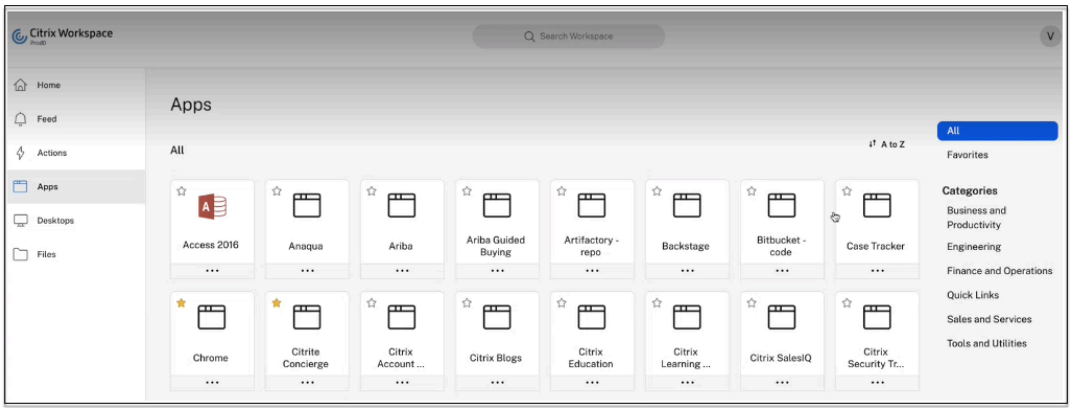
3. 追加するアプリを選択し、[スキップ] をクリックします。
4. アプリケーションの場所はどこですか? で、場所を選択します。
5. [アプリの詳細] セクションに次の詳細を入力し、[次へ] をクリックします。



- [アプリの種類] —アプリの種類を選択します。**HTTP/HTTPS** または **UDP/TCP** アプリから選択できます。
- アプリ名—アプリケーションの名前。
- アプリの説明 -アプリの簡単な説明。ここに入力するこの説明は、ワークスペースのユーザーに表示されます。
- アプリカテゴリ -公開するアプリが Citrix Workspace UI に表示される必要があるカテゴリとサブカテゴリ名（該当する場合）を追加します。アプリごとに新しいカテゴリを追加するか、Citrix Workspace UI から既存のカテゴリを使用できます。Web アプリまたは SaaS アプリのカテゴリを指定すると、そのアプリは Workspace UI の特定のカテゴリの下に表示されます。
  - カテゴリ/サブカテゴリは管理者が設定可能で、管理者はすべてのアプリに新しいカテゴリを追加できます。

- アプリカテゴリフィールドは HTTP/HTTPS アプリに適用され、TCP/UDP アプリには表示されません。
- カテゴリ/サブカテゴリの名前はバックスラッシュで区切る必要があります。たとえば、「ビジネスと生産性\エンジニアリング」などです。また、このフィールドは大文字と小文字が区別されます。管理者は、正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UI の名前と［アプリカテゴリ］フィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとして表示されます。

  たとえば、「ビジネスと生産性」カテゴリを「アプリカテゴリ」フィールドに「ビジネスと生産性」として誤って入力すると、「ビジネスと生産性」カテゴリに加えて、Citrix Workspace UI に「ビジネスと生産性」という名前の新しいカテゴリが表示されます。



- アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128 x 128 ピクセルにする必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリアイコンを表示したくない場合は、「ユーザーにアプリケーションアイコンを表示しない」を選択します。

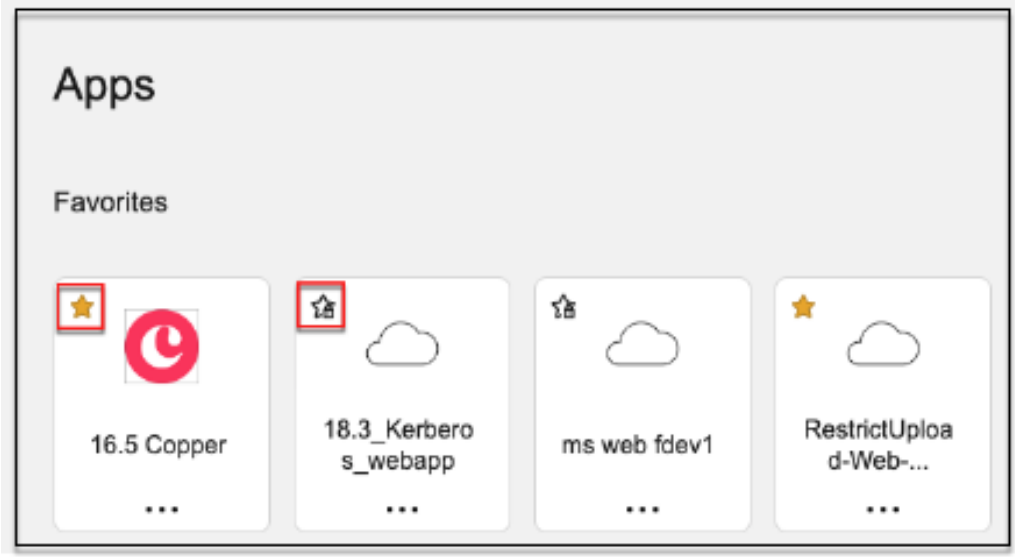
- ユーザーがクライアントブラウザから直接アプリにアクセスできるようにするには、[ダイレクトアクセス] を選択します。詳しくは、「エンタープライズ Web アプリへの直接アクセス」を参照してください。
- **URL** —顧客 ID を含む URL。URL には、顧客 ID（Citrix Cloud カスタマー ID）を含める必要があります。顧客 ID を取得するには、「Citrix Cloud にサインアップ」を参照してください。SSO が失敗した場合、または SSO を使用しない場合、ユーザーはこの URL にリダイレクトされます。

  顧客のドメイン名とカスタマードメイン **ID** -顧客のドメイン名と ID は、SAML SSO ページでアプリの URL とその他の後続の URL を作成するために使用されます。

  たとえば、Salesforce アプリケーションを追加する場合、ドメイン名が `salesforceformyorg`、ID が 123754 で、アプリケーション URL は`https://salesforceformyorg.my.salesforce.com/?so=123754.`になります

  顧客のドメイン名と顧客 ID フィールドは、特定のアプリに固有です。

- 関連ドメイン—関連ドメインは、指定した URL に基づいて自動入力されます。関連ドメインは、サービスが、アプリの一部として URL を識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。
- ［アプリケーションをお気に入りに自動的に追加］をクリックすると、このアプリが Citrix Workspace アプリのお気に入りアプリとして追加されます。
  - ［ユーザーにお気に入りからの削除を許可］をクリックすると、アプリ利用者は Citrix Workspace アプリのお気に入りアプリリストからアプリを削除できます。このオプションを選択すると、Citrix Workspace アプリのアプリの左上隅に黄色の星のアイコンが表示されます。
  - 利用者が Citrix **Workspace** アプリのお気に入りアプリリストからアプリを削除できないようにするには、［ユーザーにお気に入りからの削除を許可しない］をクリックします。このオプションを選択すると、Citrix Workspace アプリのアプリの左上隅に南京錠の付いた星のアイコンが表示されます。



お気に入りとしてマークされたアプリを Secure Private Access サービスコンソールから削除する場合、それらのアプリを Citrix Workspace のお気に入りリストから手動で削除する必要があります。Secure Private Access サービスコンソールからアプリを削除しても、Workspace アプリからは自動削除されません。

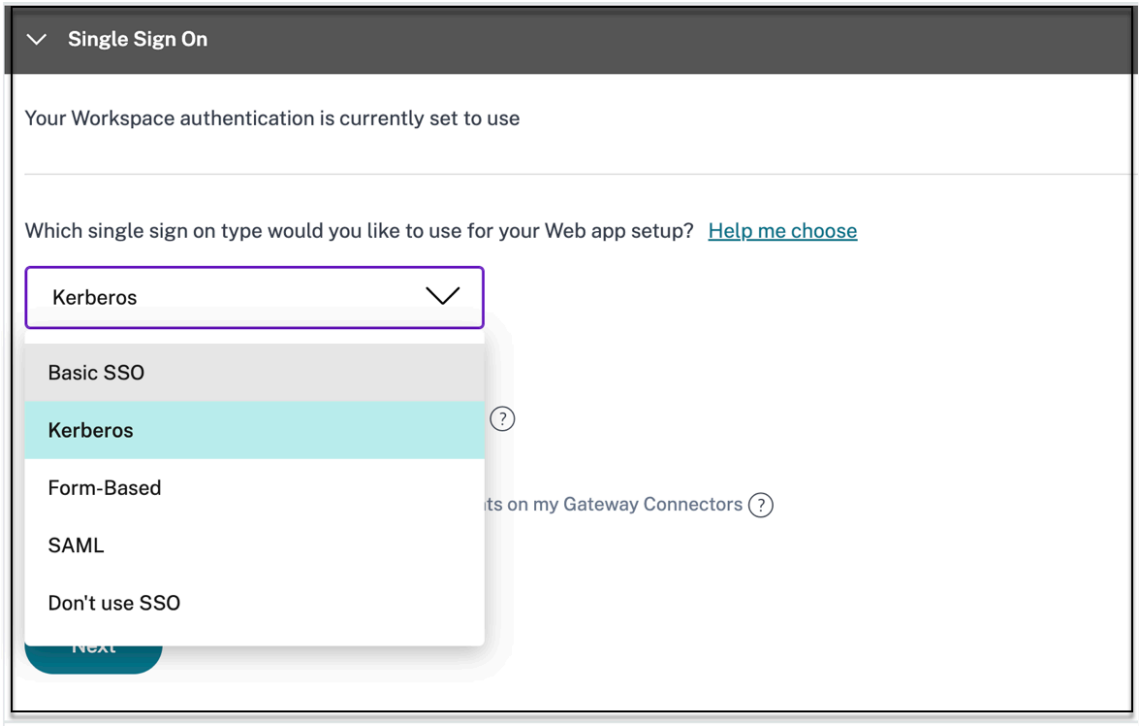
6. ［次へ］をクリックします。

> 重要:
>
> - アプリへのゼロトラストベースのアクセスを有効にするために、アプリはデフォルトでアクセスを拒否されます。アプリへのアクセスは、アクセスポリシーがアプリケーションに関連付けられている場合にのみ有効になります。アクセスポリシーの作成の詳細については、「アクセスポリシーの作成」を参照してください。
> - 複数のアプリが同じ FQDN またはワイルドカード FQDN のバリエーションで構成されている場合、構成

> が競合する可能性があります。構成の競合を防ぐには、「Web および SaaS アプリケーション構成のベストプラクティス」を参照してください。

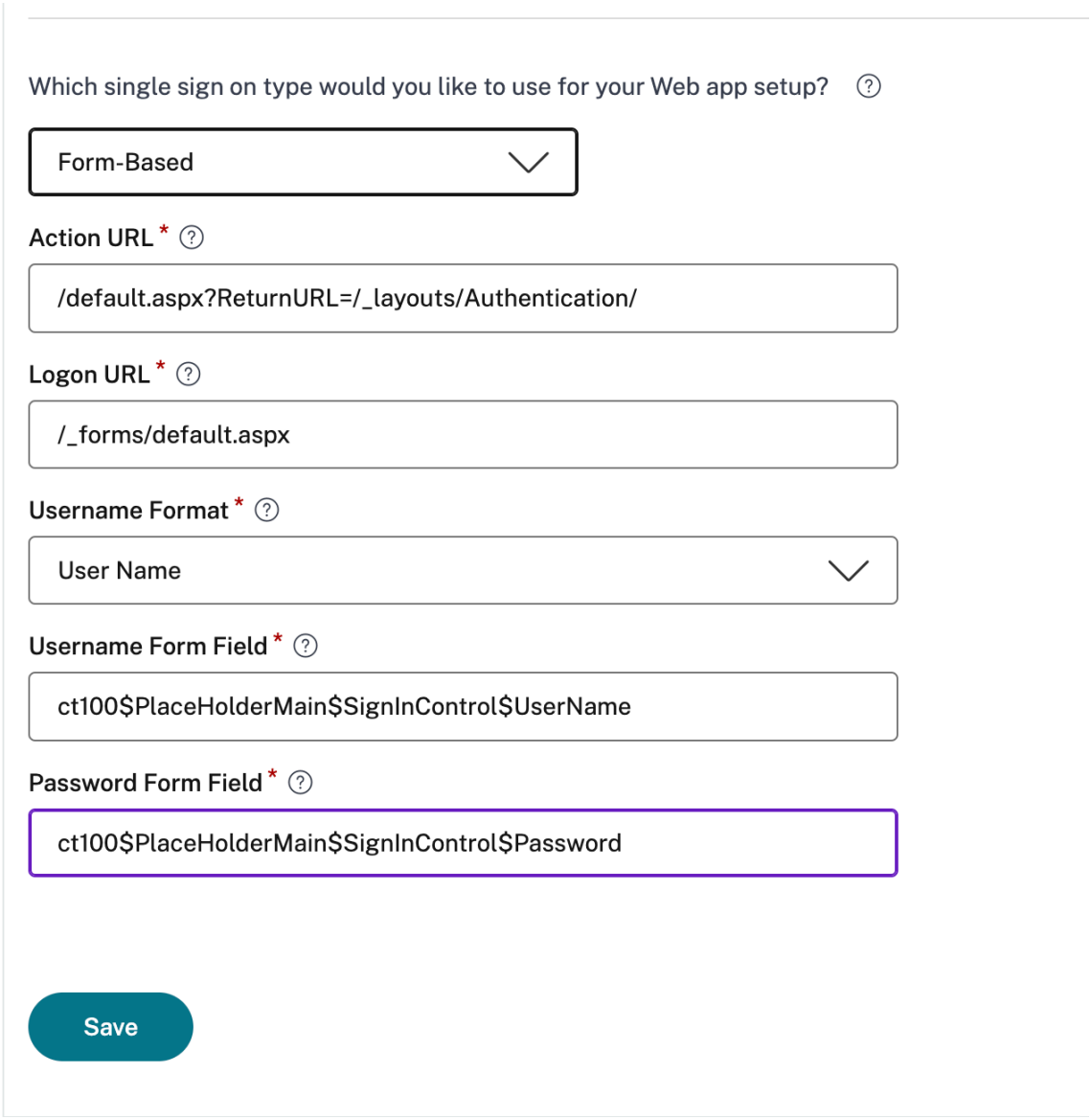
希望するサインオン方法を設定する

1. 「シングル・サインオン」セクションで、アプリケーションに使用したいシングル・サインオンの種類を選択し、「保存」をクリックします。次のシングルサインオンタイプを使用できます。



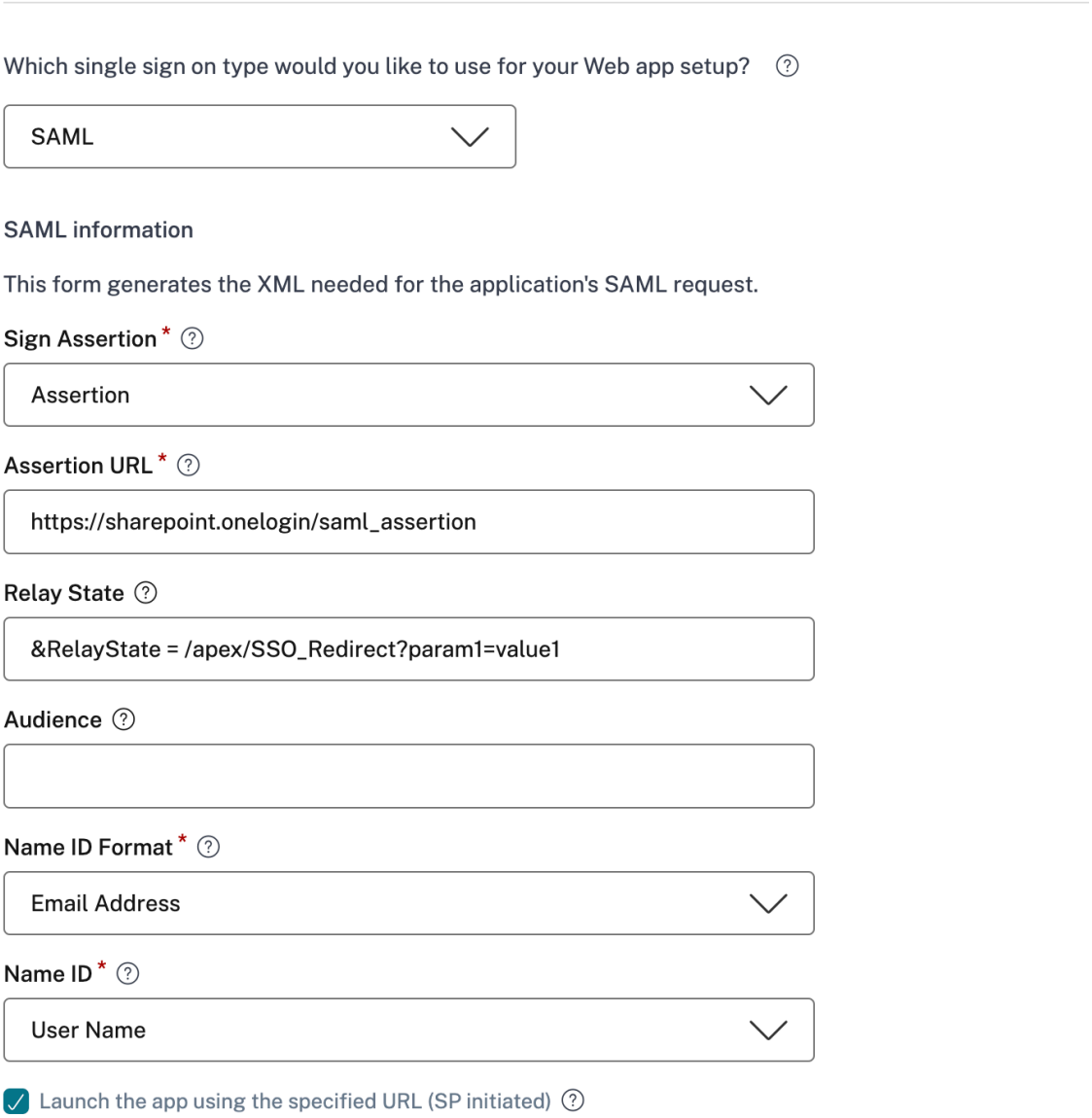
   - 基本—バックエンドサーバーから basic-401 チャレンジを提示する場合は、[**Basic SSO**] を選択します。基本 SSO タイプの構成の詳細を指定する必要はありません。
   - **Kerberos** —バックエンドサーバーがネゴシエート-401 チャレンジを提示する場合は、**Kerberos** を選択します。**Kerberos** SSO タイプの構成の詳細を指定する必要はありません。
   - フォームベース—バックエンドサーバーが認証用の HTML フォームを提示する場合は、[フォームベース] を選択します。フォームベースの SSO タイプの設定の詳細を入力します。
   - **SAML-Web** アプリケーションへの **SAML** ベースの **SSO** 用の **SAML** を選択します。**SAML** SSO タイプの設定の詳細を入力します。
   - [**SSO** を使用しない] —バックエンドサーバーでユーザーを認証する必要がない場合は、[**Don’ t use SSO**] オプションを使用します。[**SSO** を使用しない] オプションを選択すると、ユーザーは [アプリの詳細] セクションで構成された URL にリダイレクトされます。

   フォームベースの詳細**:**「シングルサインオン」セクションに次のフォームベースの構成の詳細を入力し、「保存」をクリックします。



- 「アクション **URL** 」-完成したフォームの送信先の URL を入力します。
- **[**ログオンフォームの **URL]** —ログオンフォームが表示されている URL を入力します。
- **[**ユーザー名の形式**]:** ユーザー名の形式を選択します。
- 「ユーザー名フォームフィールド」—ユーザー名属性を入力します。
- 「パスワードフォームフィールド」—パスワード属性を入力します。

SAML: [サインオン**]** セクションに次の詳細を入力し、**[**保存**]** をクリックします。



- 署名アサーション -署名アサーションまたは応答は、応答またはアサーションが証明書利用者 (SP) に配信されたときにメッセージの整合性を確保します。[アサーション]、[応答]、[両方]、[なし] を選択できます。
- アサーション **URL** —アサーション URL は、アプリケーションベンダーによって提供されます。SAML アサーションは、この URL に送信されます。
- **Relay State** —Relay State パラメーターは、ユーザーがサインインして依存パーティのフェデレーションサーバーに誘導された後にアクセスする特定のリソースを識別するために使用されます。リレー状態は、ユーザの 1 つの URL を生成します。ユーザーは、この URL をクリックして、ターゲットアプリケーションにログオンできます。
- 対象ユーザー—対象者は、アプリケーションベンダーによって提供されます。この値は、SAML アサーションが正しいアプリケーションに対して生成されていることを確認します。

- 「名前 **ID** 形式」—サポートされている名前識別子の形式を選択します。
- 「名前 **ID** 」—サポートされている名前 ID を選択します。

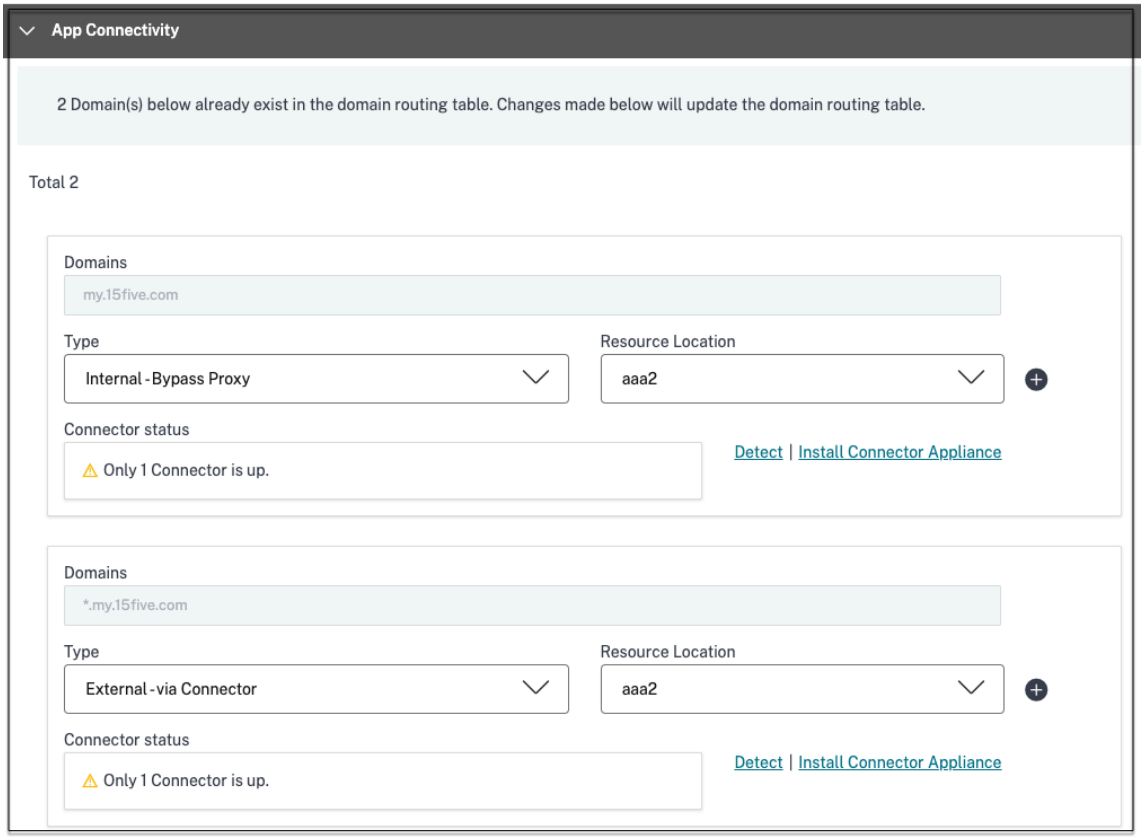
2. [詳細属性 **(**オプション**)**] に、アクセス制御の決定のためにアプリケーションに送信されるユーザーに関する追加情報を追加します。
3. **SAML** メタデータの下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaS アプリサーバーで SSO を構成します。

   > 注記**:**
   >
   > - 「ログイン **URL**」の下の **SSO** ログイン **URL** をコピーし、この **URL** を **SaaS** アプリケーションサーバーで **SSO** を構成するときに使用できます。
   > - 証明書の一覧から証明書をダウンロードし、**SaaS** アプリケーションサーバーで **SSO** を構成するときに証明書を使用することもできます。

4. [次へ**]** をクリックします。

アプリケーションルーティングの定義

1. アプリケーション接続セクションでは、アプリケーションの関連ドメインのルーティングを定義します（ドメインを Citrix ConConnector Appliance 介して外部または内部的にルーティングする必要がある場合）。詳しくは、「SaaS と Web アプリの両方の関連ドメインが同じ場合に競合を解決するためのルーティングテーブル」を参照してください。

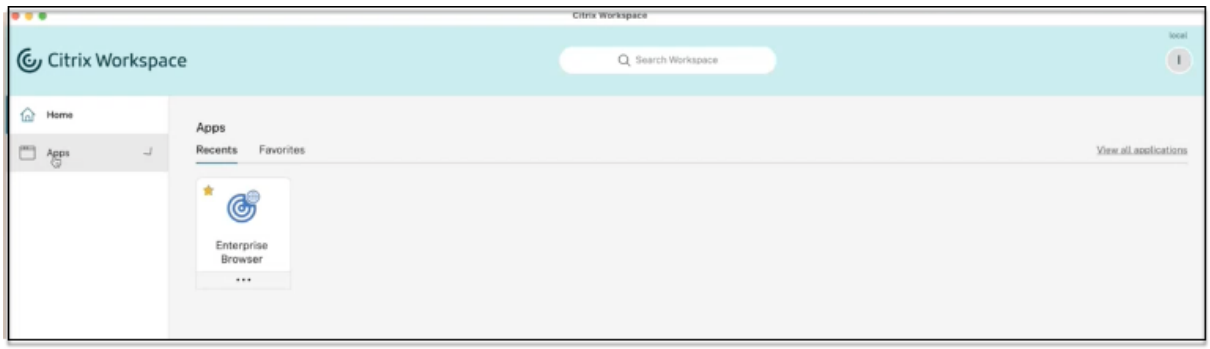


2. 「完了」をクリックします。

   [完了] をクリックすると、アプリケーションが [アプリケーション] ページに追加されます。アプリケーションを設定した後、アプリケーションページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

   - **[アプリケーションを編集]**
   - 削除

Secure Private Access サービスから Web アプリまたは SaaS アプリを公開し、そのアプリが非表示になっていない場合、Citrix Enterprise Browser アプリが自動的に Citrix Workspace UI に表示されます。さらに、Citrix Enterprise Browser もデフォルトでお気に入りアプリとして追加されます。エンドユーザーは URL なしでワークスペースブラウザーを起動し、ワークスペースブラウザーを使用して社内 Web サイトにアクセスできます。



> 重要:
>
> - ユーザーにアプリへのアクセスを許可するには、管理者がアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者がアプリの利用者を追加し、セキュリティコントロールを設定します。詳細については、「アクセスポリシーの作成」を参照してください。

Secure Private Access のための Connector Appliance

June 21, 2024

Connector Appliance は、ハイパーバイザーでホストされる Citrix コンポーネントです。Citrix Cloud とリソースの場所との間の通信チャネルとして機能し、複雑なネットワークやインフラストラクチャ構成を必要とせずにクラウドを管理できます。Connector Appliance を使用することで、リソースを管理しながら、ユーザーに価値を提供するリソースに集中することができます。

すべての接続が、標準 HTTPS ポート（443）と TCP プロトコルを使用して Connector Appliance からクラウドに対して確立されます。受信接続は受け入れられません。次の FQDN を持つ TCP ポート 443 は、アウトバウンドが許可されます。

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

Connector Appliance による Secure Private Access の構成

1. リソースの場所に 2 つ以上の Connector Appliance をインストールします。

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

2. KCD を使用してオンプレミス Web アプリに接続するように Secure Private Access を構成するには、次の手順を実行して KCD を構成します。

   a) Connector Appliance を Active Directory ドメインに参加させます。

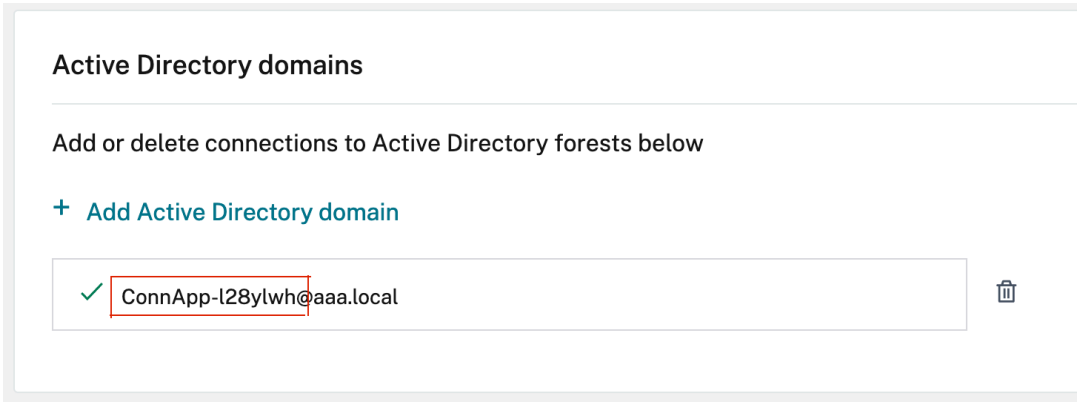
      Active Directory フォレストに参加すると、Secure Private Access を構成するときに Kerberos の制約付き委任を使用できますが、Connector Appliance を使用するための ID 要求または認証は有効になりません。

- Connector Appliance コンソールで提供される IP アドレスを使用して、Web ブラウザーで Connector Appliance の管理 Web ページに接続します。
- [**Active Directory** ドメイン] セクションで、[**+ Active Directory** ドメインを追加] をクリックします。

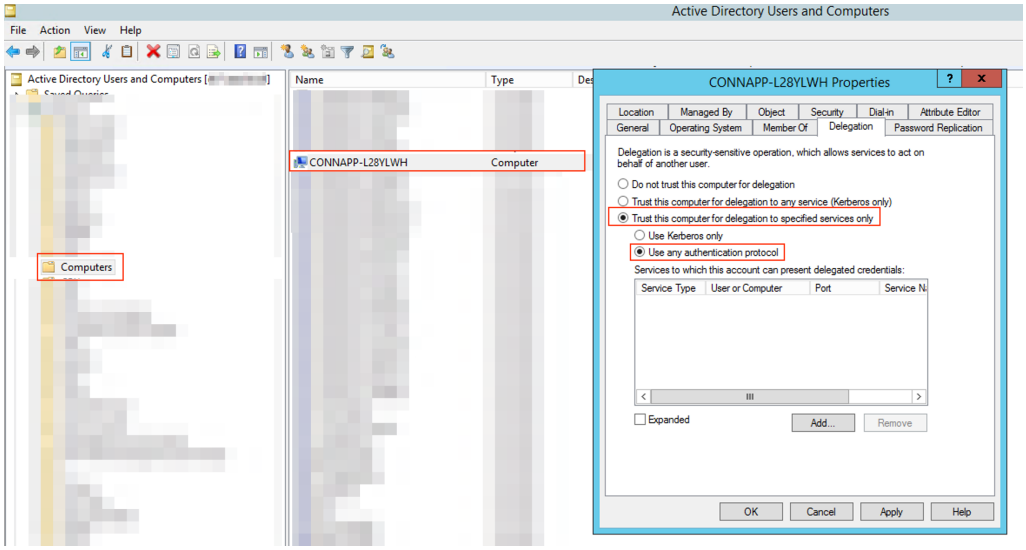
  管理ページに［**Active Directory** ドメイン］セクションがない場合は、Citrix に連絡してプレビューへの登録を依頼してください。
- ［ドメイン名］フィールドにドメイン名を入力します。［追加］をクリックします。
- Connector Appliance はドメインをチェックします。チェックで問題がなければ、［**Active Directory** に参加］ダイアログボックスが開きます。
- このドメインへの参加権限を持つ Active Directory ユーザーのユーザー名とパスワードを入力します。
- Connector Appliance からマシン名が提案されます。提案された名前を上書きして、独自のマシン名（最大 15 文字）を指定することもできます。マシンアカウント名をメモします。

  このマシン名は、Connector Appliance が参加したときに Active Directory ドメインに作成されます。
- ［参加］をクリックします。

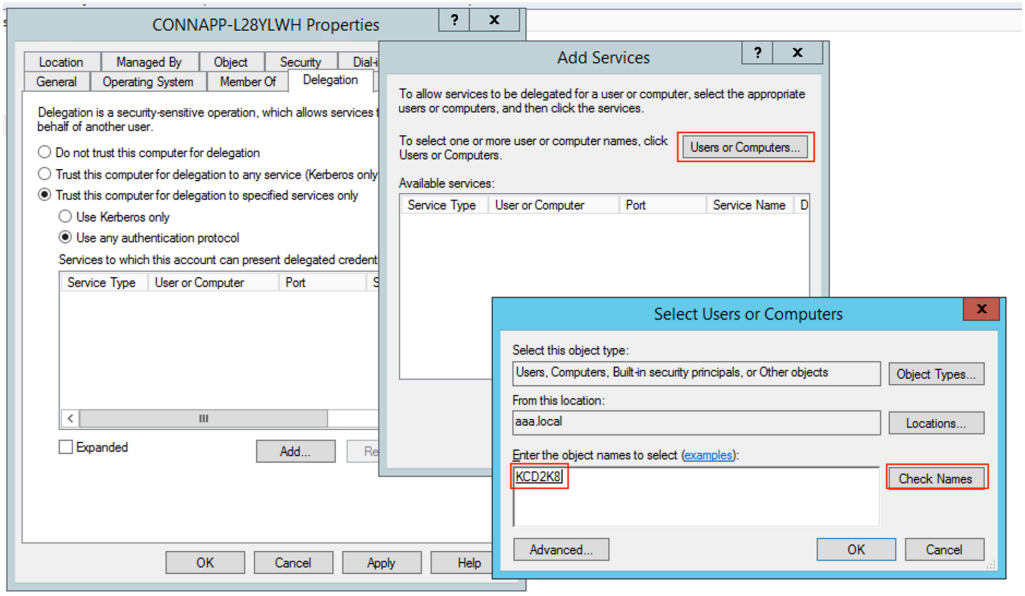
b) ロードバランサを使用しない Web サーバの Kerberos 制約委任を設定します。



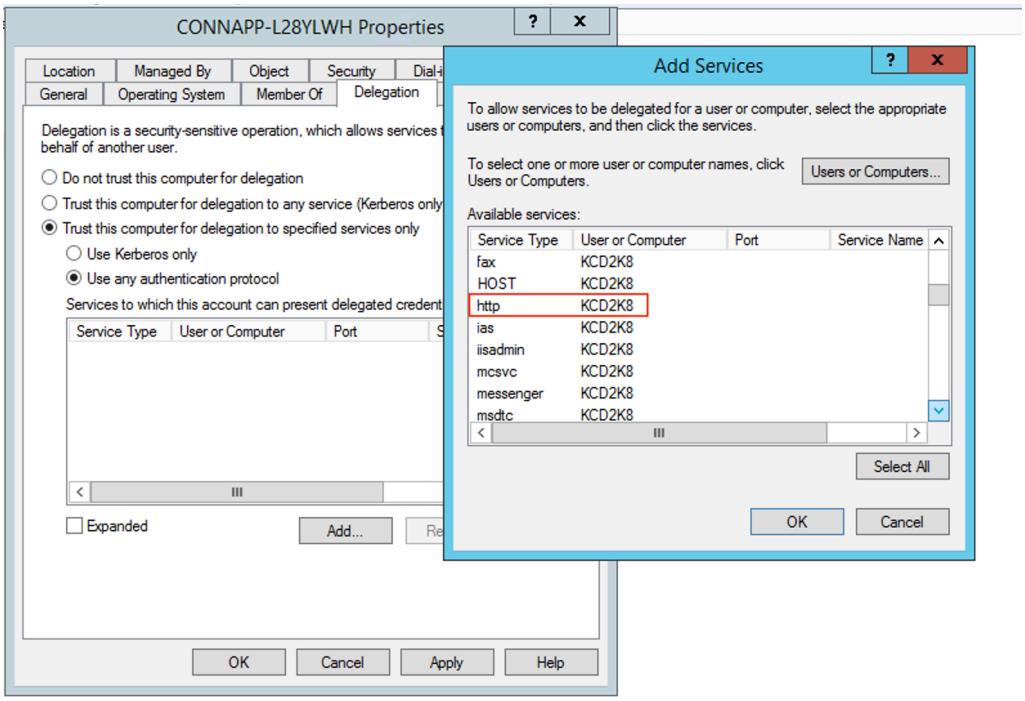
- Connector Appliance のコンピュータ名を識別します。この名前は、ホストした場所、または単にコネクタ UI から取得できます。
- Active Directory コントローラで、Connector Appliance コンピュータを探します。
- Connector Appliance コンピュータアカウントのプロパティに移動し、[委任] タブに移動します。
- [指定したサービスへの委任のみにコンピュータを信頼する] を選択します。次に、[任意の認証プロトコルを使用する] を選択します。



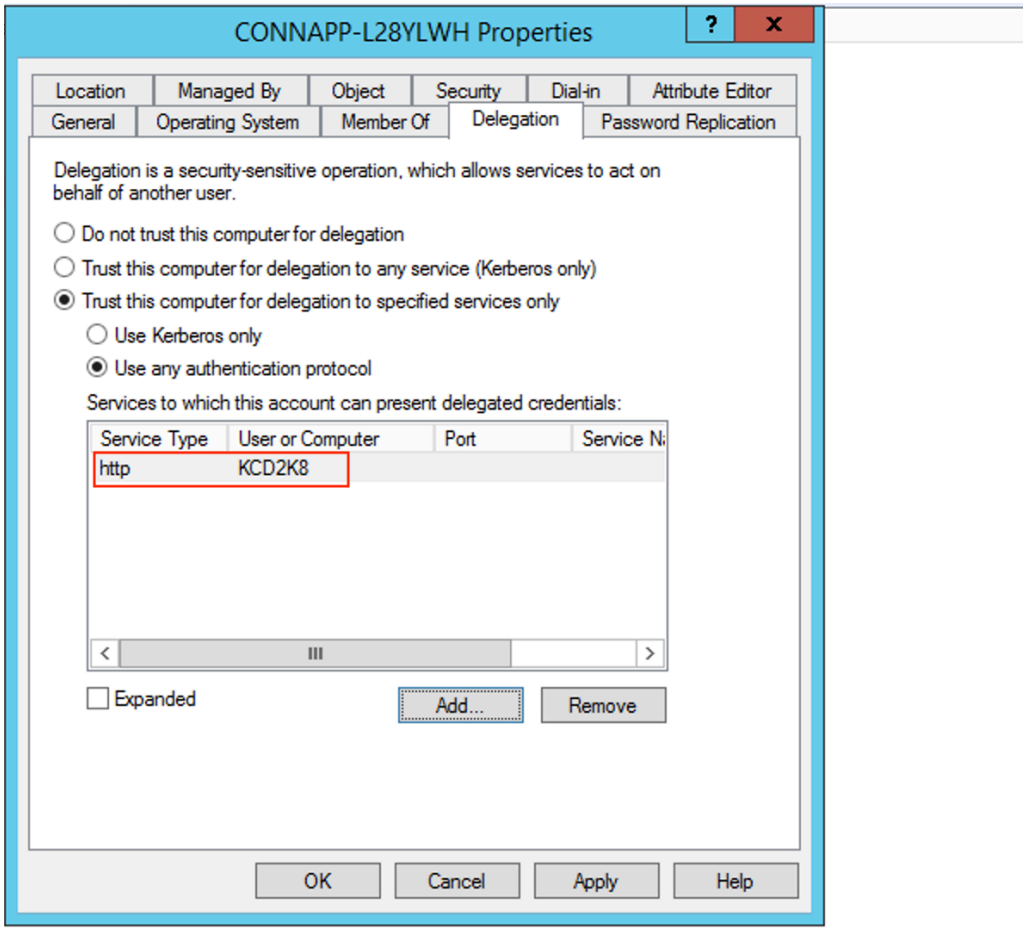
- 「追加」をクリックします。
- [ユーザー] または **[**コンピュータ**]** をクリックします
- ターゲット Web サーバーのコンピューター名を入力し、[名前の確認**]** をクリックします。上の画像では、**KCD2K8** が Web サーバーです。



- 「**OK**」をクリックします。
- サービスタイプ **http** を選択します。



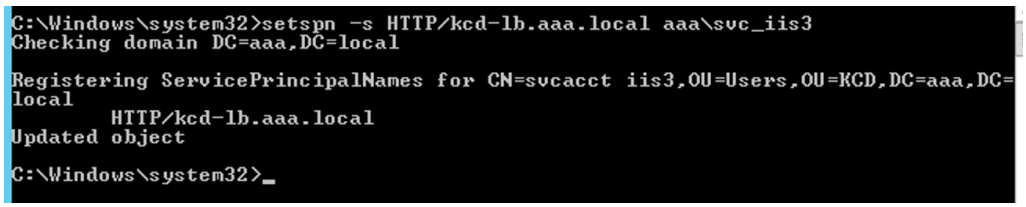
- [**OK**] をクリックします。
- 「適用」をクリックし、「**OK**」をクリックします。



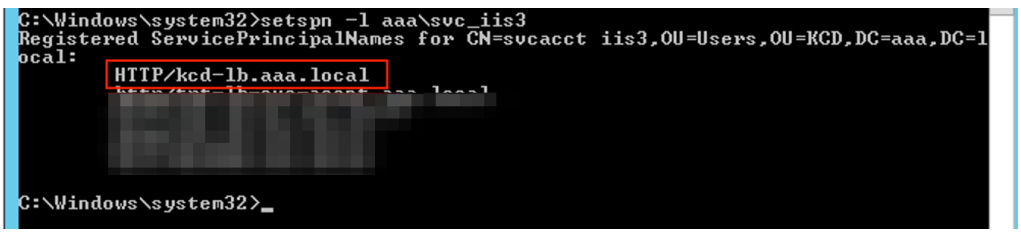
これで、Web サーバーの委任を追加する手順は完了です。

c) ロードバランサの背後にある Web サーバの Kerberos 制約委任 (KCD) を設定します。

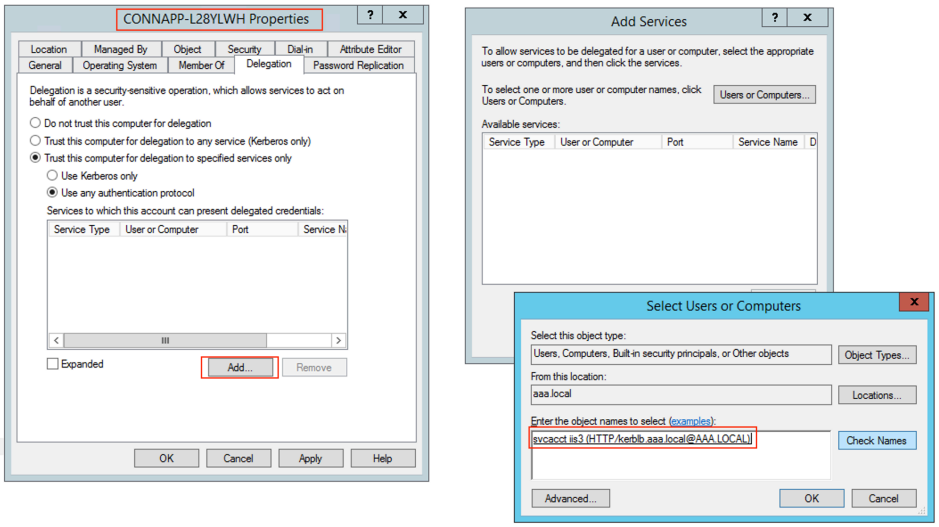
- `setspn`コマンドを使用して、ロードバランサー SPN をサービスアカウントに追加します。
  `setspn -S HTTP/<web_server_fqdn> <service_account>`



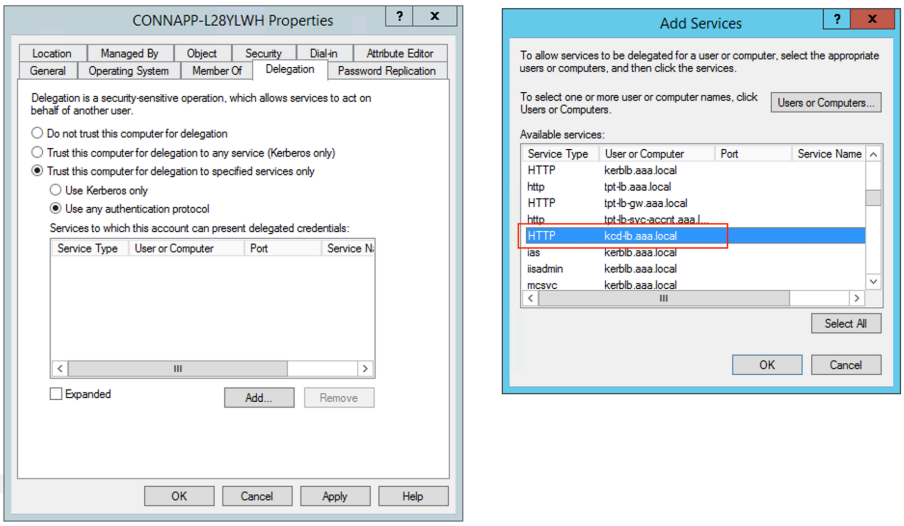
- 次のコマンドを使用して、サービスアカウントの SPN を確認します。
  `setspn -l <service_account>`



- Connector Appliance のコンピュータアカウントの委任を作成します。
  - 「ロードバランサを使用しない *Web* サーバーの *Kerberos* 制約委任の設定」の手順に従って、CA マシンを識別し、委任 UI に移動します。
  - [ユーザーとコンピューター] で、サービスアカウント (aaa\ svc_iis3 など) を選択します。

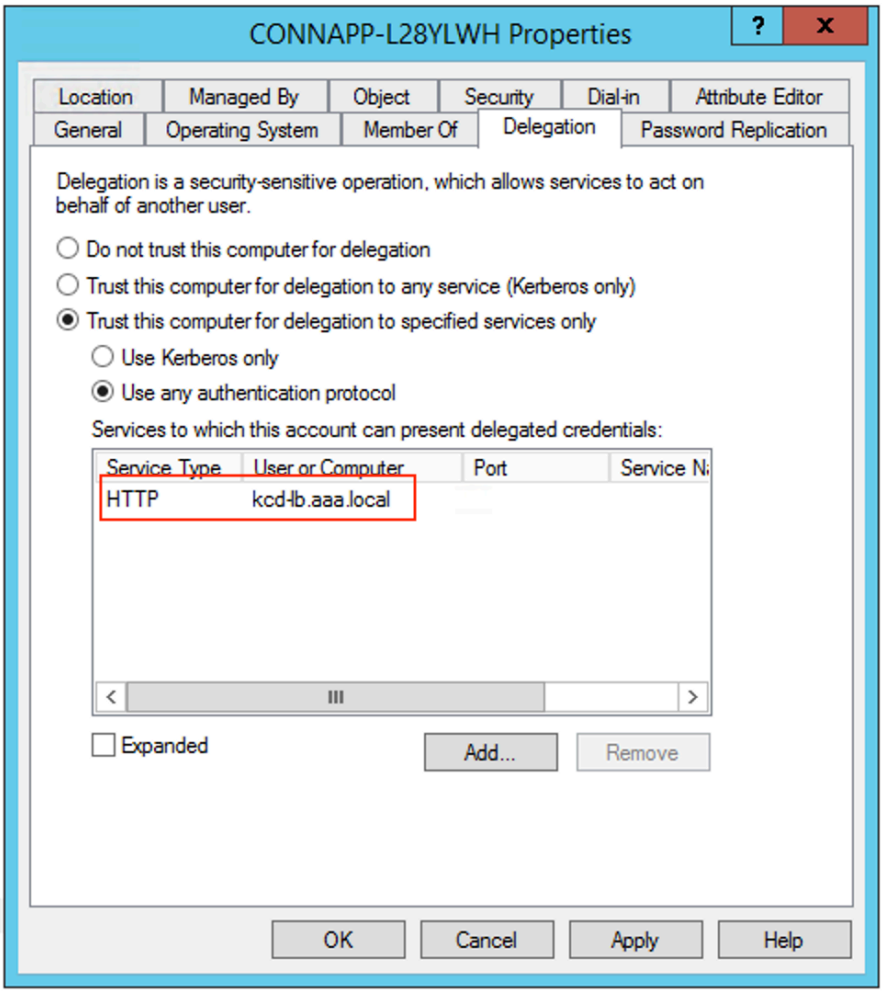


  - サービスで、**ServiceType: HTTP** とユーザーまたはコンピューター:Web サーバー (例: `kcd-lb.aaa.local`)



。

  - [**OK**] をクリックします。
  - 「適用」をクリックし、「**OK**」をクリックします。

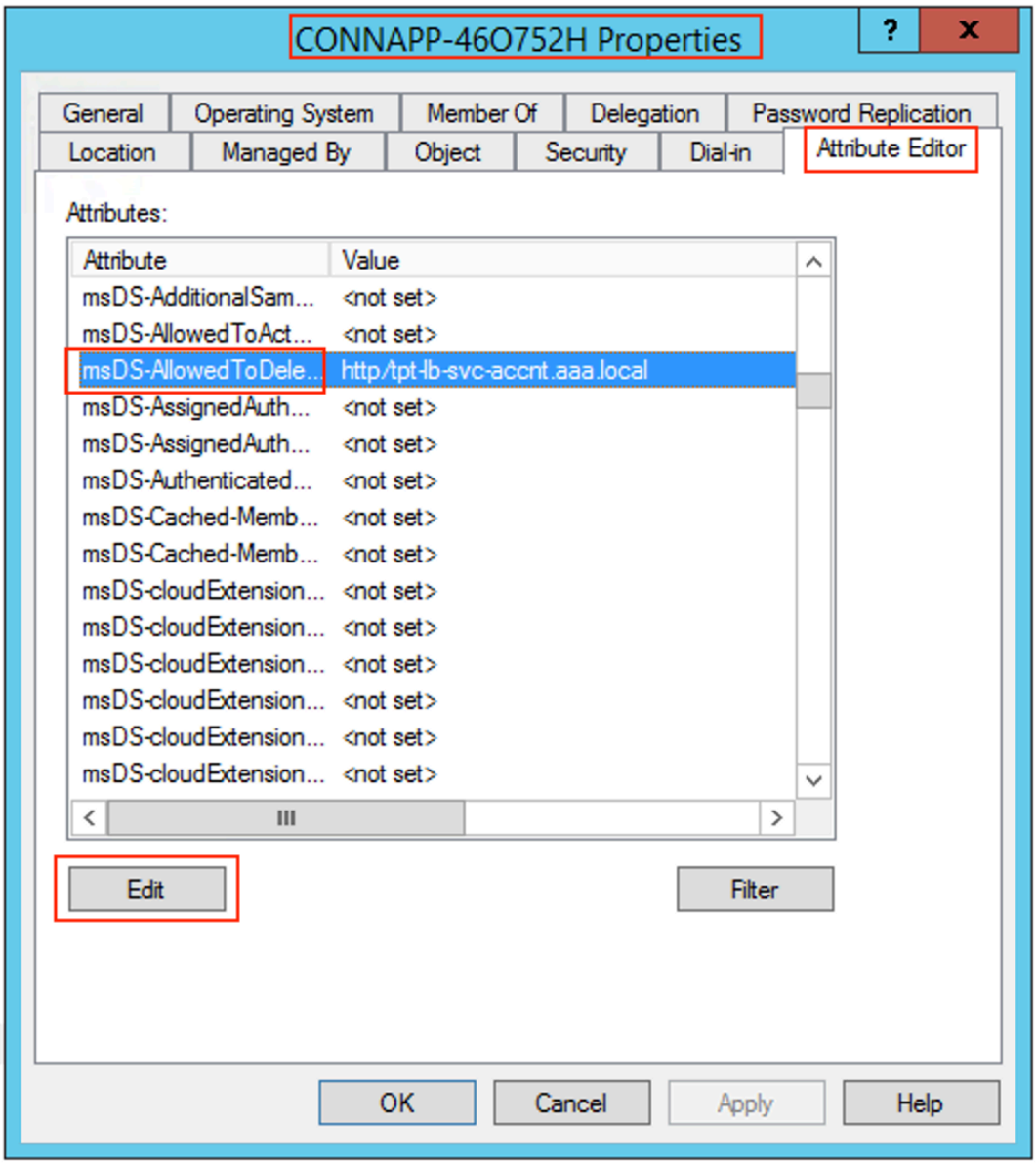


d) グループ管理サービスアカウントの Kerberos 制約付き委任 (KCD) を構成します。

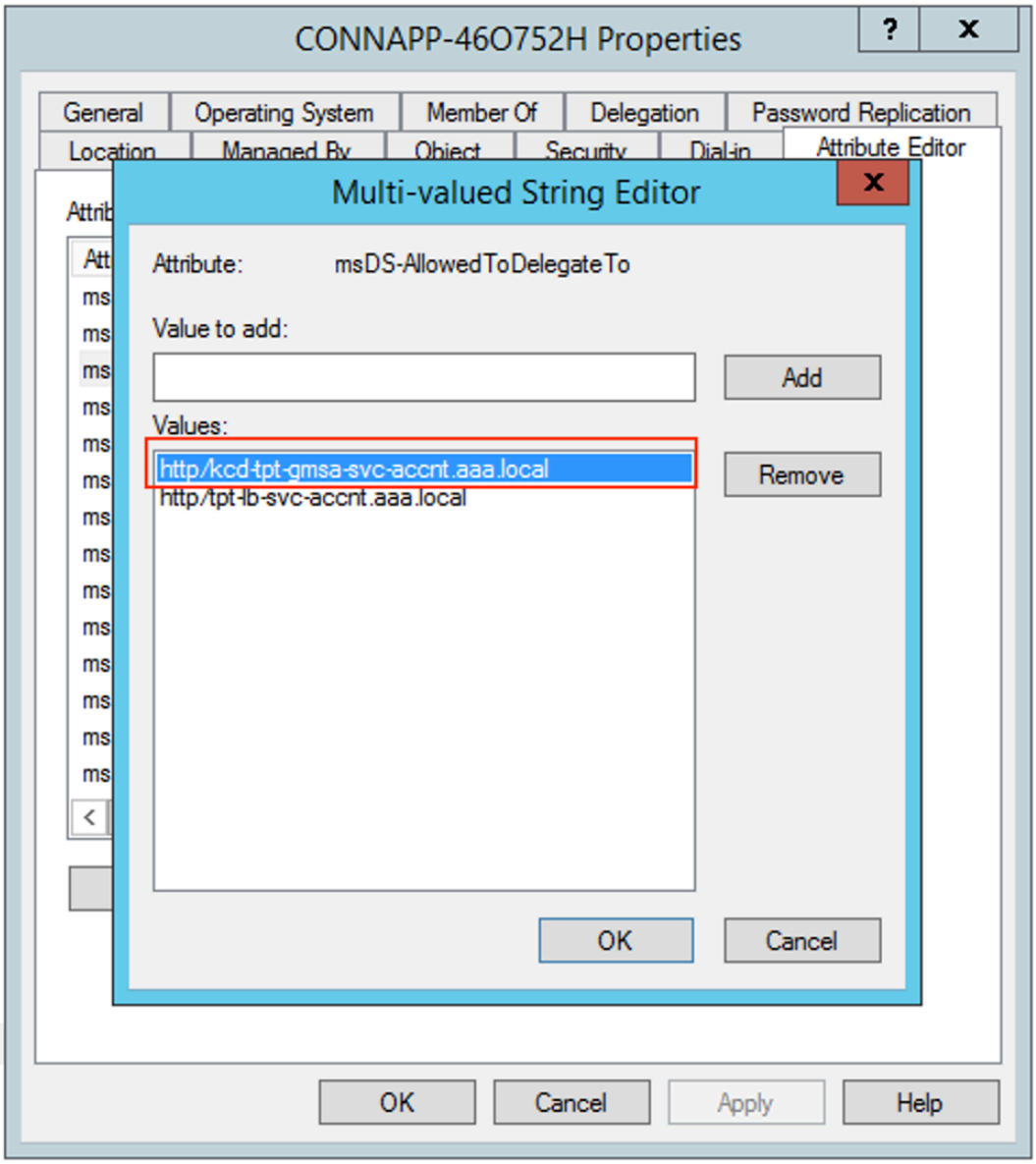
- まだ行っていない場合は、SPN をグループ管理サービスアカウントに追加します。
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- 以下のコマンドで SPN を確認します。
  `setspn -l <group_manged_service_account>`

コンピューターアカウントの委任エントリを追加している間は、グループ管理サービスアカウントを`Users and Computers`検索に表示できないため、通常の方法ではコンピューターアカウントの委任を追加できません。したがって、属性エディタを使用して、この SPN を CA コンピュータアカウントに委任されたエントリとして追加できます。

- Connector Appliance のコンピュータプロパティで、[属性エディタ] タブに移動し、`msDA-AllowedToDeleteTo` 属性を探します。
- `msDA-AllowedToDeleteTo attribute`を編集し、SPN を追加します。



)



)

e) NetScaler Gateway コネクタから Citrix Connector Appliance に移行します。

- SPNs はゲートウェイコネクタの構成時にサービスアカウントにすでに設定されているため、新しい kerberos アプリが構成されていない場合は、サービスアカウントに SPN を追加する必要はありません。次のコマンドを実行して、サービスアカウントに割り当てられているすべての SPN の一覧を表示し、それらを CA コンピューターアカウントの委任されたエントリとして割り当てることができます。

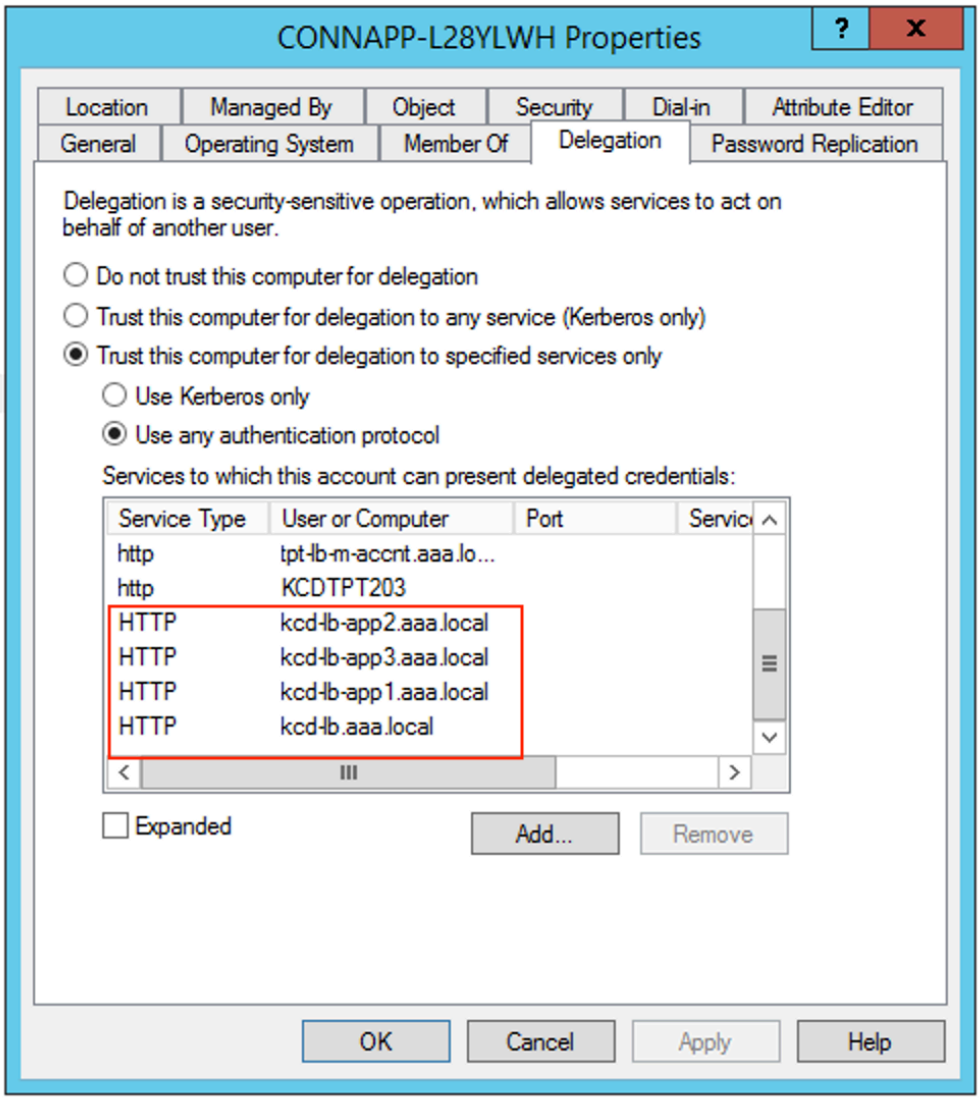
```
setspn -l <service_account>
```



```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

この例では、SPN (kcd-lb.aaa.local, kcd-lb-app1.aaa.local, kcd-lb-app2.aaa.local, kcd-lb-app3.aaa.local) は KCD 用に設定されています。

- 委任されたエントリとして、必要な SPN を Connector Appliance のコンピュータアカウントに追加します。詳細については、「*Connector Appliance* のコンピュータアカウントの委任を作成する」の手順を参照してください。



この例では、必要な SPN が CA コンピューターアカウントの委任されたエントリとして追加されます。

注**:** これらの SPN は、ゲートウェイコネクタの設定時に委任されたエントリとしてサービスアカウントに追加されました。サービスアカウントの委任から離れるときに、それらのエントリをサービスアカウントの [委任] タブから削除できます。

f) Citrix Secure Private Access のドキュメントに従って、Citrix Secure Private Access サービスをセットアップします。セットアップ中、Citrix Cloud は Connector Appliance の存在を認識し、それらを使用してリソースの場所に接続します。

- Citrix Secure Private Access の使用開始
- Citrix Secure Private Access 構成する
- クラウド サービス用の Connector Appliance
- インターネット接続の要件
- エンタープライズ Web アプリのサポート

Kerberos 構成の検証

シングルサインオンに Kerberos を使用している場合は、Connector Appliance 管理ページで Active Directory コントローラの構成が正しいことを確認できます。［**Kerberos** 検証］機能を使用すると、Kerberos 領域のみのモード構成または Kerberos の制約付き委任構成を検証できます。

1. **Connector Appliance** 管理ページに移動します。
   a) ハイパーバイザーの Connector Appliance コンソールから、IP アドレスを Web ブラウザーのアドレスバーにコピーします。
   b) Connector Appliance の登録時に設定したパスワードを入力します。
2. 右上の［管理］メニューから、［**Kerberos** 検証］を選択します。
3. ［**Kerberos** 検証］ダイアログボックスで、［**Kerberos** 検証モード］を選択します。
4. ［**Active Directory** ドメイン］を指定または選択します。
   - Kerberos 領域のみのモード構成を検証する場合は、任意の Active Directory ドメインを指定できます。
   - Kerberos の制約付き委任構成を検証する場合は、結合されたフォレスト内のドメインのリストから選択する必要があります。
5. ［サービス **FQDN**］を指定します。デフォルトのサービス名は、`http`と想定されます。「computer.example.com」を指定した場合、これは`http/computer.example.com`と同じと見なされます。
6. ［ユーザー名］を指定します。
7. Kerberos 領域のみのモード構成を検証する場合は、そのユーザー名の ［パスワード］を指定します。
8. ［**Kerberos** をテストする］をクリックします。

Kerberos 構成が正しい場合は、メッセージ`Successfully validated Kerberos setup`が表示されます。Kerberos 構成が正しくない場合、検証の失敗に関する情報を提供するエラーメッセージが表示されます。

Gateway Connector を Connector Appliance に移行

January 9, 2024

NetScaler Gateway Connector は廃止されました。Citrix では、自社の環境で NetScaler Gateway Connector を使用しているお客様に、以前は NetScaler Gateway Connector でサポートされていたすべての Secure Private Access のユースケース向けに Connector Appliance 導入を開始することを推奨しています。このトピックでは、Gateway Connector を Connector Appliance に移行するためのガイドラインを提供します。

Gateway Connector を Connector Appliance に移行する手順の概要

1. Gateway Connector に加えて Connector Appliance を同じリソースの場所にインストールします。
2. Gateway Connector をシャットダウンし、既存の Web アプリの接続をテストします。同じリソースの場所でホストされている Web アプリにアクセスできるかどうかを確認します。
3. テストが完了したら、NetScaler Gateway コネクタを取り外します。

Connector Appliance をインストールするには

Connector Appliance をインストールするには、次の手順を使用します。

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. Connector Appliance を追加するリソースの場所の [Connector Appliance] の横にあるプラスアイコンをクリックします。
4. ハイパーバイザーを選択し、[イメージのダウンロード] をクリックします。
5. ハイパーバイザーに Connector Appliance をダウンロードしてインストールします。
6. Web UI（ハイパーバイザーのコンソールで提供される IP アドレス）にログインし、必要に応じてプロキシを設定します。
7. [登録] ボタンをクリックして、ショートコードを取得します。
8. Connector Appliance のダウンロード時に使用する Citrix Cloud ユーザーインターフェイスにショートコードを貼り付けます（手順 5）。

   Connector Appliance が登録されています。

詳細な手順については、「クラウドサービス用 Connector Appliance」を参照してください。

よくある質問

- Connector Appliance をダウンロードするにはどうすればいいですか?

  Connector Appliance をダウンロードします。

- Connector Appliance をインストールするにはどうすればいいですか?

  Connector Appliance の設置。

- Connector Appliance の登録方法を教えてください。

  Connector Appliance を登録します。

- Connector Appliance の接続要件は何ですか?

  Connector Appliance のインターネット接続要件。

- Connector Appliance のシステム要件は何ですか?

  Connector Appliance のシステム要件。

- Connector Appliance はどのように更新されますか?

  Connector Appliance の更新

エンタープライズ **Web** アプリへの直接アクセス

June 19, 2024

SharePoint、JIRA、Confluence など、オンプレミスまたはパブリッククラウドで顧客がホストするエンタープライズ Web アプリケーションに、クライアントブラウザから直接アクセスできるようになりました。エンドユーザーは、Citrix Workspace エクスペリエンスからエンタープライズ Web アプリへのアクセスを開始する必要がなくなりました。また、この機能により、エンドユーザーは電子メール、コラボレーションツール、またはブラウザーのブックマークからリンクをクリックして Web アプリにアクセスできるようになります。これにより、真のゼロ・フットプリント・ソリューションを顧客に提供できます。

機能

- 構成済みのエンタープライズ Web アプリの新しい DNS レコードを追加するか、既存の DNS レコードを変更します。
- IT 管理者は、新しいパブリック DNS レコードを追加するか、構成済みのエンタープライズ Web アプリ FQDN の既存のパブリック DNS レコードを変更して、ユーザーを Citrix Secure Private Access サービスにリダイレクトします。

- エンドユーザーが構成済みのエンタープライズ Web アプリへのアクセスを開始すると、アプリのトラフィックは Citrix Secure Private Access サービスに誘導され、Citrix Secure Private Access サービスがアプリへのアクセスをプロキシします。
- 要求が Citrix Secure Private Access サービスに届くと、コンテキストアクセスポリシーのチェックなど、ユーザー認証とアプリケーション承認がチェックされます。
- 検証が成功すると、Citrix Secure Private Access サービスは、お客様の環境（オンプレミスまたはクラウド）に展開された Citrix Cloud Connector アプライアンスと通信して、構成済みのエンタープライズ Web アプリへのアクセスを可能にします。

エンタープライズ **Web** アプリに直接 **Citrix Secure Private Access** アクセスを構成する

前提条件

開始する前に、アプリケーションを構成するために次のものが必要です。

- アプリケーション FQDN
- SSL 証明書—設定するアプリのパブリック証明書
- リソースの場所—Citrix Cloud Connector アプライアンスのインストール
- パブリック DNS レコードにアクセスして、アプリの構成時に Citrix から提供された正規名（CNAME）で更新します。

エンタープライズ **Web** アプリへの直接アクセスを設定する手順**:**

> 重要**:**
>
> アプリの完全なエンドツーエンド構成については、「簡単なオンボーディングとセットアップのための管理者向けガイド付きワークフロー」を参照してください。

1. Secure Private Access のホームページで、[続行] をクリックします。

   > 注**:**
   >
   > [続行] ボタンは、ウィザードを初めて使用する場合にのみ表示されます。以降の使用方法では、[アプリケーション] ページに直接移動し、[アプリの追加] をクリックします。

2. ID と認証を設定します。詳しくは、「簡単なオンボーディングとセットアップのための管理者向けガイド付きワークフロー」を参照してください。
3. アプリの追加に進みます。詳しくは、「アプリケーションの追加と管理」を参照してください。
4. 追加するアプリを選択し、[スキップ] をクリックします。
5. アプリケーションの場所はどこですか? で、場所を選択します。
6. [アプリの詳細] セクションに次の詳細を入力し、[次へ] をクリックします。

- [アプリの種類] —アプリの種類 (HTTP または HTTPS) を選択します。
- アプリ名—アプリケーションの名前。
- アプリの説明 -アプリの簡単な説明。ここに入力するこの説明は、ワークスペースのユーザーに表示されます。
- アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128 x 128 ピクセルにする必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリアイコンを表示したくない場合は、「ユーザーにアプリケーションアイコンを表示しない」を選択します。

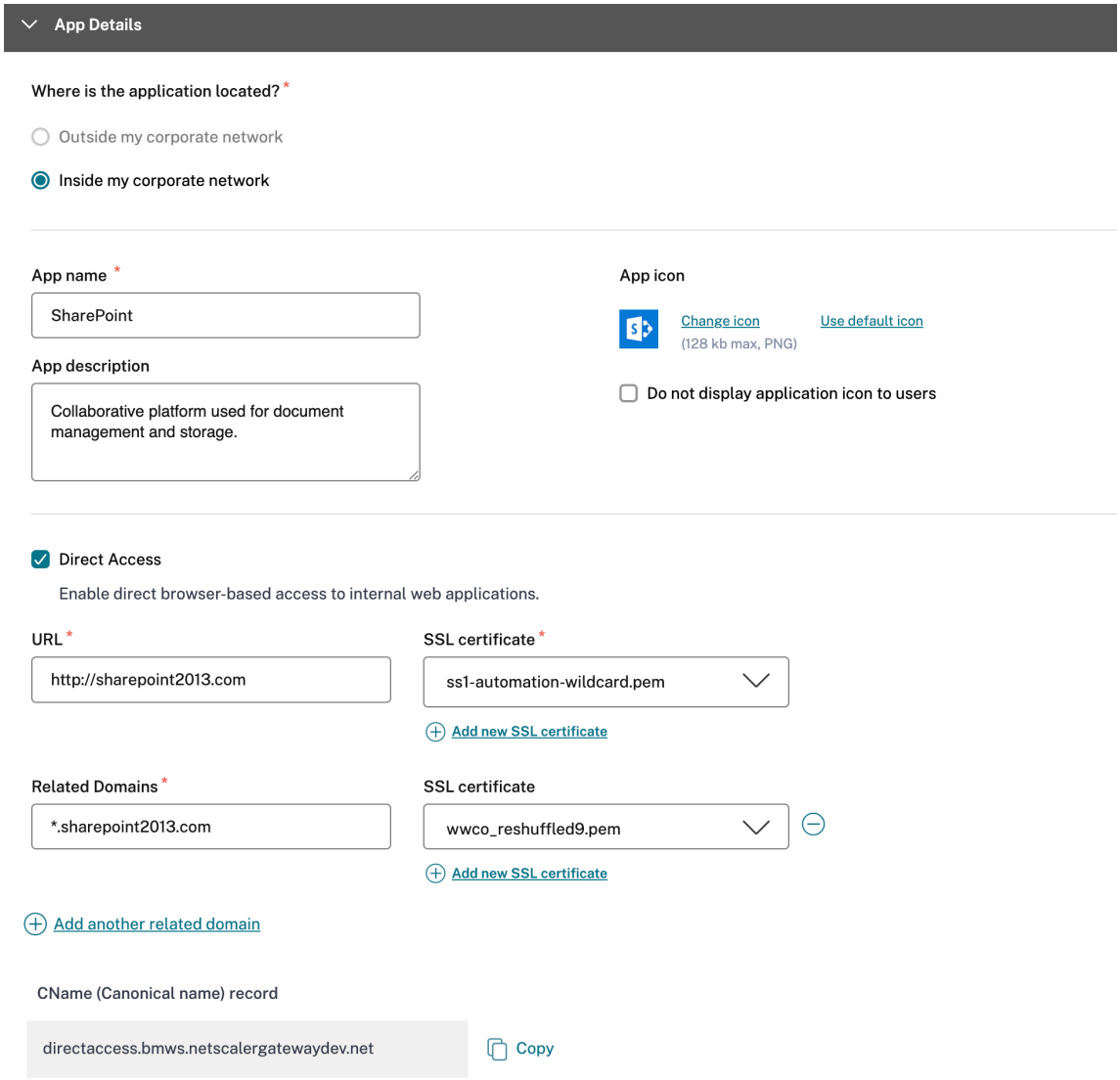
7. ユーザーがクライアントブラウザから直接アプリにアクセスできるようにするには、[ダイレクトアクセス] を選択します。次の詳細を入力します。

   - **URL** —バックエンドアプリケーションの URL。URL は HTTPS 形式で、対応する DNS エントリは管理者が追加する必要があります。
   - [**SSL** 証明書] —ドロップダウンメニューから既存の SSL 証明書を選択するか、[新しい SSL 証明書の追加**]** をクリックして新しい **SSL** 証明書を追加します。

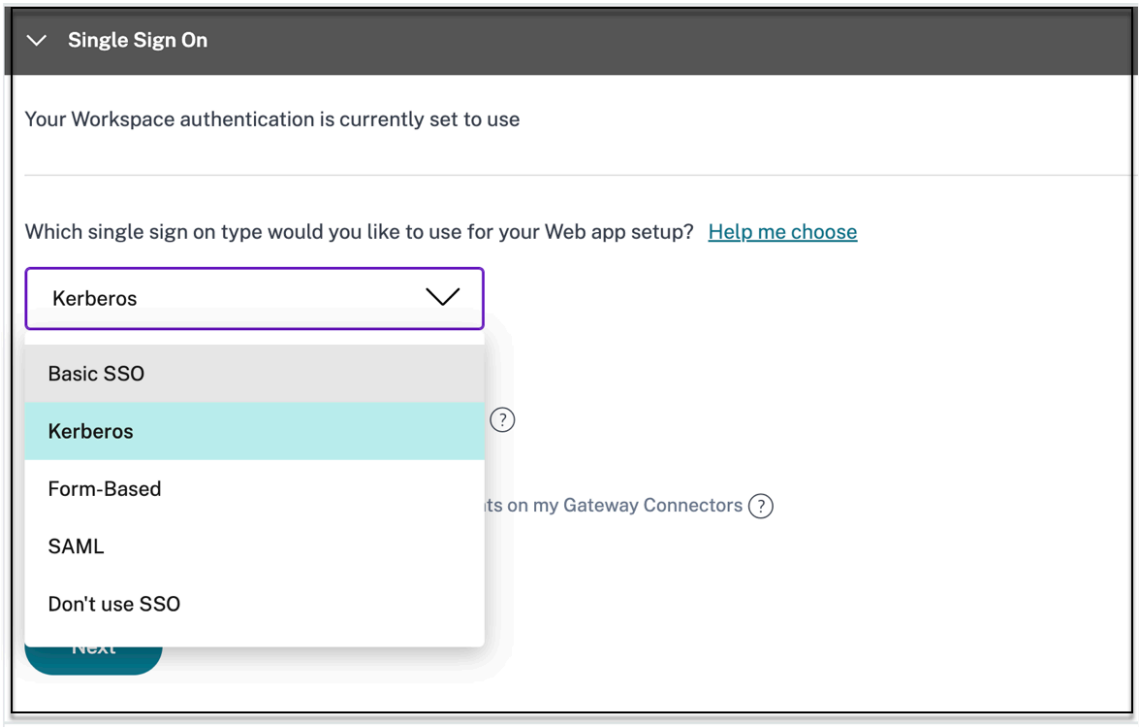
     注意事項

     - パブリック CA 証明書または信頼できる CA 証明書のみがサポートされます。自己署名証明書はサポートされていません。
     - 証明書一式をアップロードする必要があります。

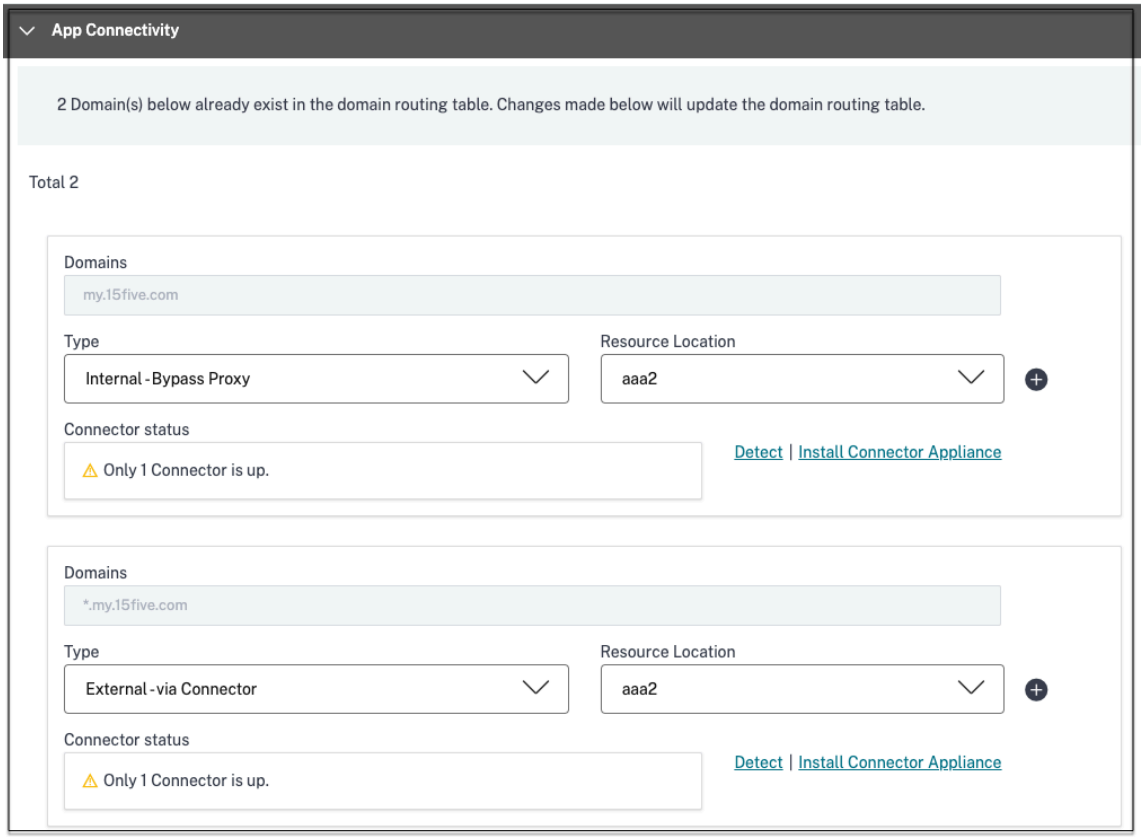
   - 関連ドメイン—関連ドメインは、指定した URL に基づいて自動入力されます。関連ドメインは、サービスが、アプリの一部として URL を識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。SSL 証明書は、関連する各ドメインにバインドできます。これはオプションです。
   - **CNAME** レコード—Secure Private Access によって自動生成されます。これは、アプリケーションへの直接アクセスを有効にするために DNS に入力する必要がある値です。



8. [次へ] をクリックします。
9. [シングルサインオン] セクションで、アプリケーションに使用するシングルサインオンの種類を選択し、[次へ] をクリックします。



10. アプリケーション接続セクションでは、既存のリソースロケーションを選択するか、リソースロケーションを作成して新しい Connector Appliance スを展開できます。既存のリソースの場所を選択するには、[My Resource Location] など、リソースの場所の一覧からリソースの場所の 1 つをクリックし、[次へ] をクリックします。詳しくは、「SaaS と Web アプリの両方の関連ドメインが同じ場合に競合を解決するためのルーティングテーブル」を参照してください。



11. [完了] をクリックします。アプリが [アプリケーション] ページに追加されます。アプリケーションを設定した後に、アプリケーションページからを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

    - **[アプリケーションを編集]**
    - 削除

> 重要:
>
> - アプリへのゼロトラストベースのアクセスを有効にするために、アプリはデフォルトでアクセスを拒否されます。アプリへのアクセスは、アクセスポリシーがアプリケーションに関連付けられている場合にのみ有効になります。アクセスポリシーの作成の詳細については、「アクセスポリシーの作成」を参照してください。
> - 複数のアプリが同じ FQDN またはワイルドカード FQDN のバリエーションで構成されている場合、構成が競合する可能性があります。構成の競合を防ぐには、「Web および SaaS アプリケーション構成のベストプラクティス」を参照してください。

SaaS アプリのサポート

June 19, 2024

SaaS（Software as a Service）は、Web ベースのサービスとしてソフトウェアをリモートで配信するためのソフトウェア配布モデルである。一般的に使用される SaaS アプリケーションには、Salesforce、Workday、Concur、GoToMeeting などがあります。

SaaS アプリには、Secure Private Access サービスを使用して Citrix Workspace を使用してアクセスできます。Secure Private Access サービスと Citrix Workspace を組み合わせることで、構成済みの SaaS アプリ、構成済みの仮想アプリ、またはその他のワークスペースリソースに対して統合されたユーザーエクスペリエンスを提供します。

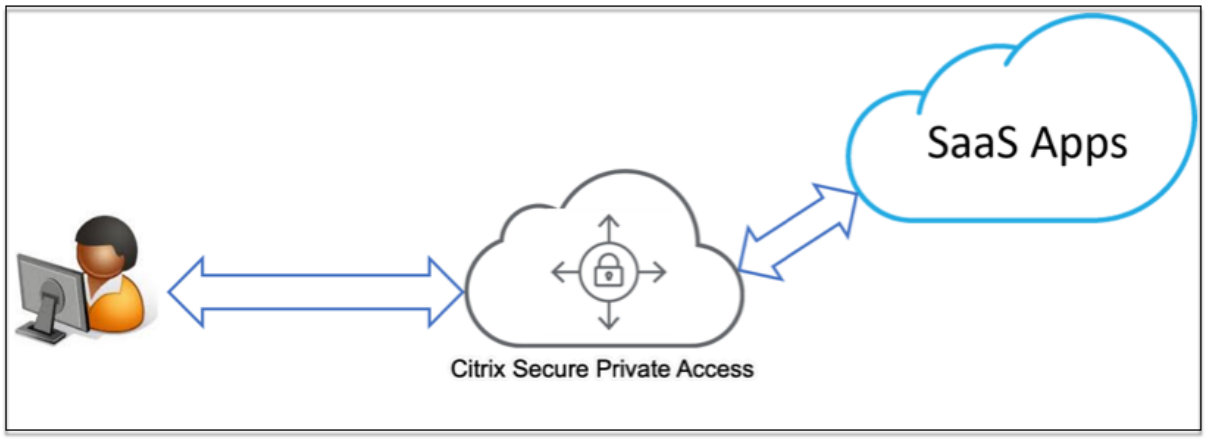
Secure Private Access サービスを使用した SaaS アプリ配信は、アプリを管理するための簡単、安全、強固でスケーラブルなソリューションを提供します。クラウドで提供される SaaS アプリには、次の利点があります：

- シンプルな構成—操作、更新、使用が容易
- シングルサインオン—シングルサインオンで簡単にログオンできます。
- 異なるアプリの標準テンプレート—一般的なアプリのテンプレートベースの構成。

Secure Private Access サービスで SaaS アプリがどのようにサポートされるか

1. 顧客管理者は、Secure Private Access サービスの UI を使用して SaaS アプリを構成します。
2. 管理者は、Citrix Workspace にアクセスするためのサービス URL をユーザーに提供します。
3. アプリを起動するには、列挙された SaaS アプリアイコンをクリックします。
4. SaaS アプリは、Secure Private Access サービスによって提供される SAML アサーションを信頼し、アプリケーションが起動します。

> 注記：
>
> - ユーザーにアプリへのアクセスを許可するには、管理者がアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者がアプリの利用者を追加し、セキュリティコントロールを設定します。詳細については、「アクセスポリシーの作成」を参照してください。
> - 構成済みの SaaS アプリは、仮想アプリやその他のリソースとともに Citrix Workspace に集約され、統一されたユーザーエクスペリエンスを実現します。



SaaS アプリを設定する

SaaS アプリの設定には、以下の大まかな手順が含まれます。

1. アプリケーションの詳細を設定
2. 希望するサインオン方法を設定する
3. アプリケーションルーティングの定義

アプリケーションの詳細を設定

1. 「**Secure Private Access** 」タイルで、「管理」をクリックします。
2. [続行] をクリックし、[アプリを追加] をクリックします。

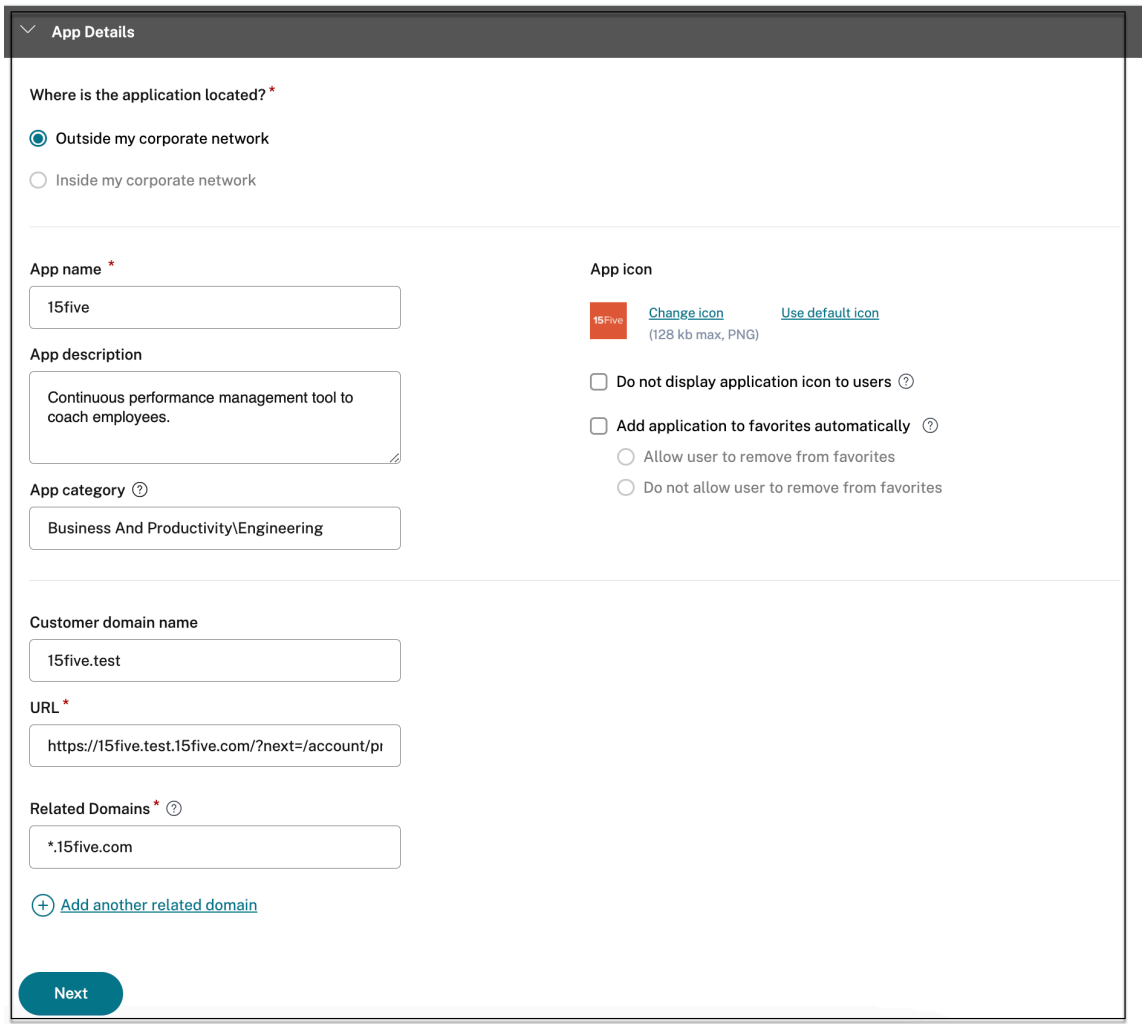
   > 注記:
   >
   > - [続行] ボタンは、ウィザードを初めて使用するときにのみ表示されます。その後の使用では、[アプリケーション] ページに直接移動して [アプリの追加] をクリックできます。
   > - アプリの詳細を入力するか、人気のある SaaS アプリのリストで使用できるアプリテンプレートを選択して、SaaS アプリを手動で追加できます。テンプレートには、アプリケーションの構成に必要な情報の大部分があらかじめ入力されています。ただし、顧客固有の情報は引き続き提供する必要があります。SaaS アプリ構成テンプレートについて詳しくは、「SaaS アプリケーションサーバー固有の構成」を参照してください。

3. アプリを構成します。

   - アプリの詳細を手動で入力するには、[スキップ] をクリックします。
   - テンプレートを使用してアプリを構成するには、[次へ] をクリックします。

   SaaS アプリでは、[社内ネットワーク外] がデフォルトで有効になっています。

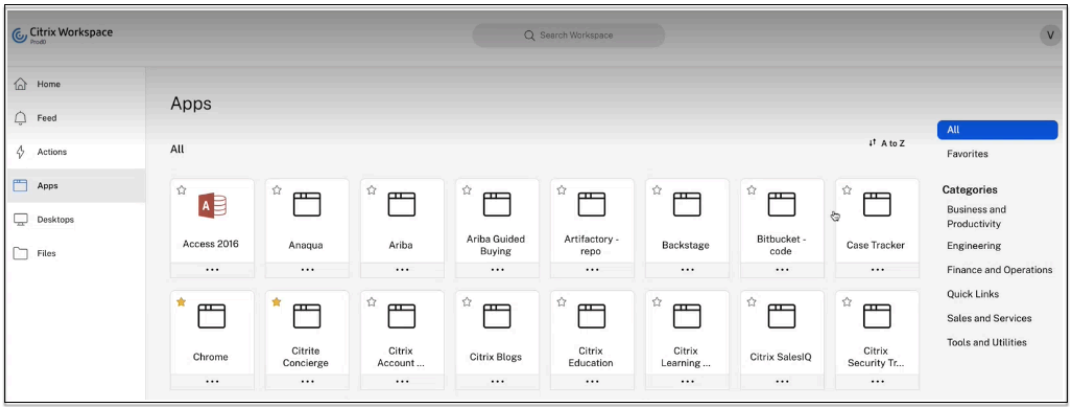
4. [アプリの詳細] セクションに次の詳細を入力し、[次へ] をクリックします。



- アプリ名—アプリケーションの名前。
- アプリの説明 -アプリの簡単な説明。ここに入力するこの説明は、ワークスペースのユーザーに表示されます。
- アプリカテゴリ -公開するアプリが Citrix Workspace UI に表示される必要があるカテゴリとサブカテゴリ名（該当する場合）を追加します。アプリごとに新しいカテゴリを追加するか、Citrix Workspace UI から既存のカテゴリを使用できます。Web アプリまたは SaaS アプリのカテゴリを指定すると、そのアプリは Workspace UI の特定のカテゴリの下に表示されます。
  - カテゴリ/サブカテゴリは管理者が設定可能で、管理者はすべてのアプリに新しいカテゴリを追加できます。
  - アプリカテゴリフィールドは HTTP/HTTPS アプリに適用され、TCP/UDP アプリには表示されません。
  - カテゴリ/サブカテゴリの名前はバックスラッシュで区切る必要があります。たとえば、「ビジネスと生産性\ エンジニアリング」などです。また、このフィールドは大文字と小文字が区別されます。

管理者は、正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UI の名前と［アプリカテゴリ］フィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとして表示されます。

たとえば、「ビジネスと生産性」カテゴリを「アプリカテゴリ」フィールドに「ビジネスと生産性」として誤って入力すると、「ビジネスと生産性」カテゴリに加えて、Citrix Workspace UI に「ビジネスと生産性」という名前の新しいカテゴリが表示されます。



- アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128 x 128 ピクセルにする必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリアイコンを表示したくない場合は、「ユーザーにアプリケーションアイコンを表示しない」を選択します。

- **URL** —顧客 ID を含む URL。URL には、顧客 ID（Citrix Cloud カスタマー ID）を含める必要があります。顧客 ID を取得するには、「Citrix Cloud にサインアップ」を参照してください。SSO が失敗した場合、または SSO を使用しない場合、ユーザーはこの URL にリダイレクトされます。

- 顧客のドメイン名とカスタマードメイン **ID** -顧客のドメイン名と ID は、SAML SSO ページでアプリの URL とその他の後続の URL を作成するために使用されます。

  たとえば、Salesforce アプリケーションを追加する場合、ドメイン名が `salesforceformyorg`、ID が 123754 で、アプリケーション URL は`https://salesforceformyorg.my.salesforce.com/?so=123754.`になります

  顧客のドメイン名と顧客 ID フィールドは、特定のアプリに固有です。

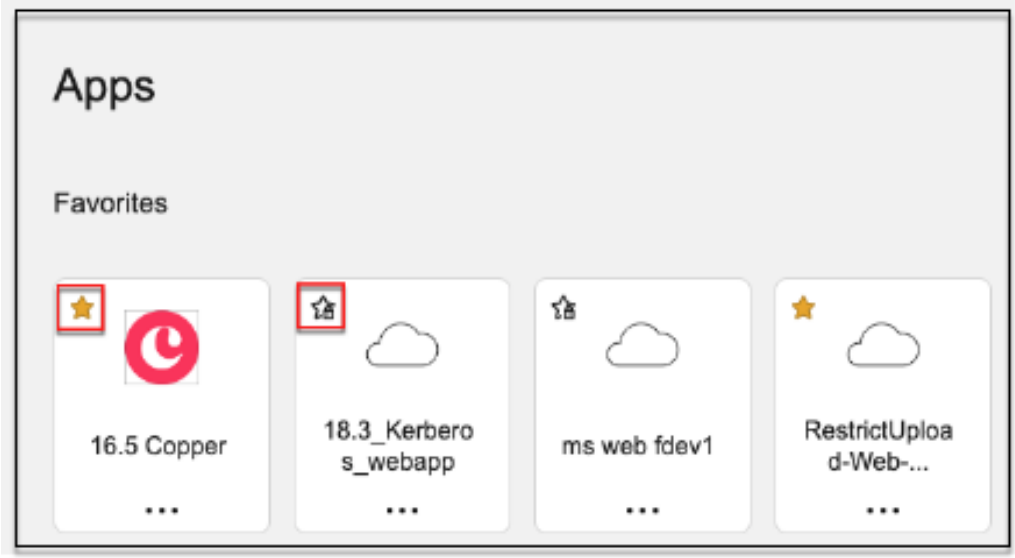
- 関連ドメイン—関連ドメインは、指定した URL に基づいて自動入力されます。関連ドメインは、サービスが、アプリの一部として URL を識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。

- ［アプリケーションをお気に入りに自動的に追加］をクリックすると、このアプリが Citrix Workspace アプリのお気に入りアプリとして追加されます。

  – ［ユーザーにお気に入りからの削除を許可］をクリックすると、アプリ利用者は Citrix Workspace

アプリのお気に入りアプリリストからアプリを削除できます。このオプションを選択すると、Citrix Workspace アプリのアプリの左上隅に黄色の星のアイコンが表示されます。

- 利用者が Citrix **Workspace** アプリのお気に入りアプリリストからアプリを削除できないようにするには、［ユーザーにお気に入りからの削除を許可しない］をクリックします。このオプションを選択すると、Citrix Workspace アプリのアプリの左上隅に南京錠の付いた星のアイコンが表示されます。



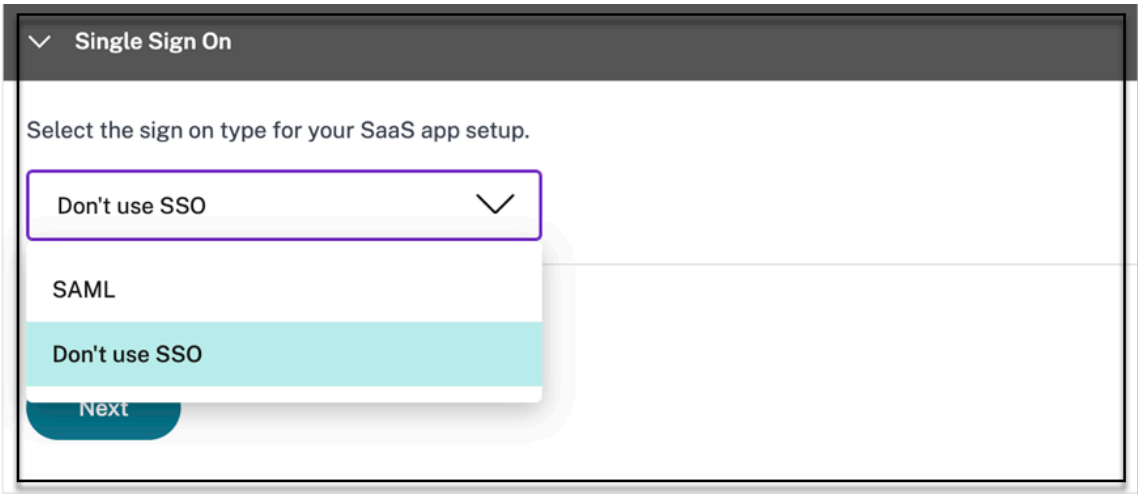
お気に入りとしてマークされたアプリを Secure Private Access サービスコンソールから削除する場合、それらのアプリを Citrix Workspace のお気に入りリストから手動で削除する必要があります。Secure Private Access サービスコンソールからアプリを削除しても、Workspace アプリからは自動削除されません。

5. [次へ] をクリックします。

> 重要:
>
> - アプリへのゼロトラストベースのアクセスを有効にするために、アプリはデフォルトでアクセスを拒否されます。アプリへのアクセスは、アクセスポリシーがアプリケーションに関連付けられている場合にのみ有効になります。アクセスポリシーの作成の詳細については、「アクセスポリシーの作成」を参照してください。
> - 複数のアプリが同じ FQDN またはワイルドカード FQDN のバリエーションで構成されている場合、構成が競合する可能性があります。構成の競合を防ぐには、「Web および SaaS アプリケーション構成のベストプラクティス」を参照してください。

優先サインオン方法を設定する

1.「シングル・サインオン」セクションで、アプリケーションに使用したいシングル・サインオンの種類を選択し、「保存」をクリックします。次のシングルサインオンタイプを使用できます。

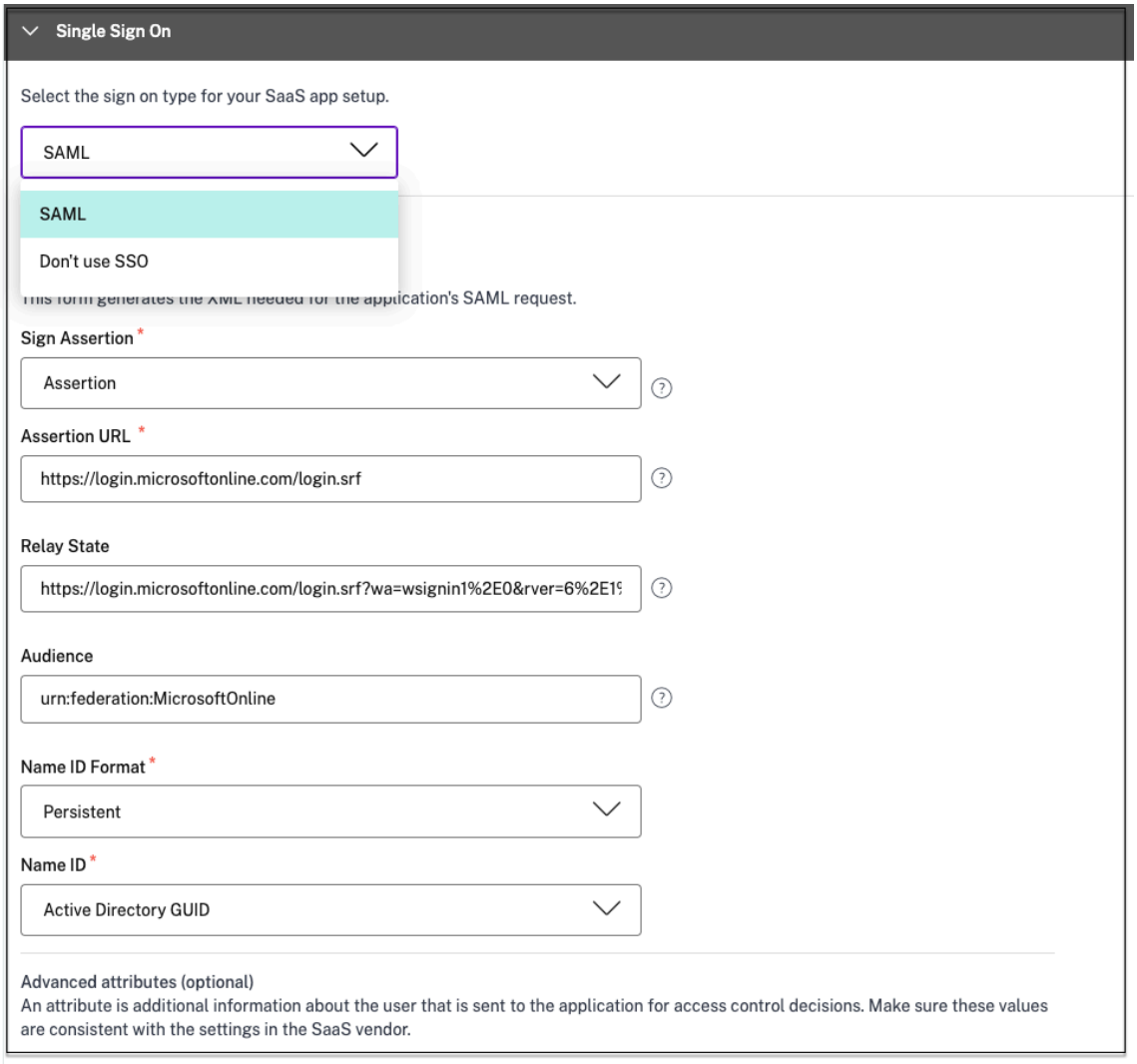


- [**SSO** を使用しない] —バックエンドサーバーでユーザーを認証する必要がない場合は、[**Don’t use SSO**] オプションを使用します。[**SSO** を使用しない] オプションを選択すると、ユーザーは [アプリの詳細] セクションで構成された URL にリダイレクトされます。
- **SAML-Web** アプリケーションへの **SAML** ベースの **SSO** 用の **SAML** を選択します。**SAML** SSO タイプの設定の詳細を入力します。

  [サインオン] セクションに次の詳細を入力し、[保存] をクリックします。

  - 署名アサーション -署名アサーションまたは応答は、応答またはアサーションが証明書利用者 (SP) に配信されたときにメッセージの整合性を確保します。[アサーション]、[応答]、[両方]、[なし] を選択できます。
  - アサーション **URL** —アサーション URL は、アプリケーションベンダーによって提供されます。SAML アサーションは、この URL に送信されます。
  - **Relay State** —Relay State パラメーターは、ユーザーがサインインして依存パーティのフェデレーションサーバーに誘導された後にアクセスする特定のリソースを識別するために使用されます。リレー状態は、ユーザの 1 つの URL を生成します。ユーザーは、この URL をクリックして、ターゲットアプリケーションにログオンできます。
  - 対象ユーザー—対象者は、アプリケーションベンダーによって提供されます。この値は、SAML アサーションが正しいアプリケーションに対して生成されていることを確認します。
  - 「名前 **ID** 形式」—サポートされている名前識別子の形式を選択します。
  - 「名前 **ID** 」—サポートされている名前 ID を選択します。
  - ID プロバイダーが開始するフローを上書きし、サービスプロバイダーが開始するフローのみを使用するには、[特定の **URL** を使用してアプリを起動する **(SP** 起動**)**] を選択します。

2. [詳細属性 **(**オプション**)**] に、アクセス制御の決定のためにアプリケーションに送信されるユーザーに関する追加情報を追加します。



3. **SAML** メタデータの下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaS アプリサーバーで SSO を構成します。

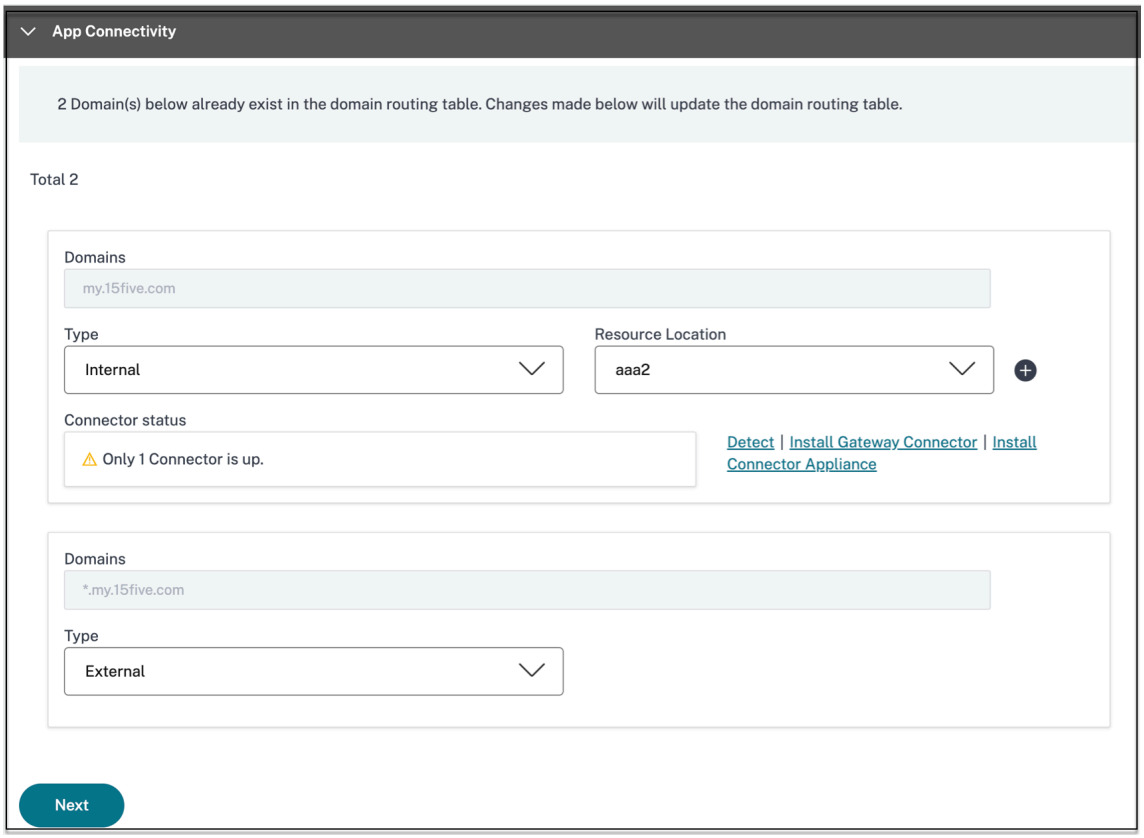
   > 注記:
   >
   > - 「ログイン **URL**」の下の **SSO** ログイン **URL** をコピーし、この **URL** を **SaaS** アプリケーションサーバーで **SSO** を構成するときに使用できます。
   > - 証明書の一覧から証明書をダウンロードし、**SaaS** アプリケーションサーバーで **SSO** を構成するときに証明書を使用することもできます。

4. [次へ] をクリックします。

アプリケーションルーティングの定義

1. ドメインを Citrix Connector アプライアンスを介して外部または内部でルーティングする必要がある場合は、「アプリケーション接続」セクションで、アプリケーションの関連ドメインのルーティングを定義します。

詳しくは、「SaaS と Web アプリの両方の関連ドメインが同じ場合に競合を解決するためのルーティングテーブル」を参照してください。

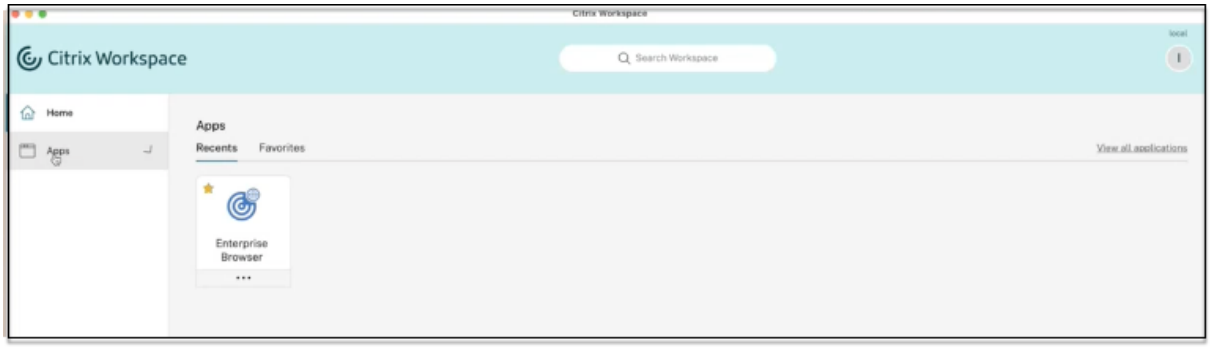


2. 「完了」をクリックします。

   [完了] をクリックすると、アプリケーションが [アプリケーション] ページに追加されます。アプリケーションを設定した後、アプリケーションページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

   - **[アプリケーションを編集]**
   - 削除

Secure Private Access サービスから Web アプリまたは SaaS アプリを公開し、そのアプリが非表示になっていない場合、Citrix Enterprise Browser アプリが自動的に Citrix Workspace UI に表示されます。さらに、Citrix Enterprise Browser もデフォルトでお気に入りアプリとして追加されます。エンドユーザーは URL なしでワークスペースブラウザーを起動し、ワークスペースブラウザーを使用して社内 Web サイトにアクセスできます。



参照ドキュメント

アプリの完全なエンドツーエンド構成については、「簡単なオンボーディングとセットアップのための管理者向けガイド付きワークフロー」を参照してください。

クライアントサーバーアプリのサポート

February 20, 2024

Citrix Secure Private Access を使用すると、TCP/UDP アプリや HTTPS アプリを含むすべてのプライベートアプリに、ネイティブブラウザまたはマシン上で実行されている Citrix Secure Access クライアント経由でネイティブクライアントアプリケーションにアクセスできるようになりました。

Citrix Secure Private Access 内のクライアント/サーバーアプリケーションの追加サポートにより、従来の VPN ソリューションへの依存を排除して、リモートユーザーにすべてのプライベートアプリへのアクセスを提供できるようになりました。

プレビュー機能

FQDN を IP アドレスに変換するための DNS サフィックスのサポート。

機能

エンドユーザーは、Citrix Secure Access クライアントをクライアントデバイスにインストールするだけで、認可されたすべてのプライベートアプリに簡単にアクセスできます。

- Windows の場合、クライアントバージョン (22.3.1.5 以降) はhttps://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.htmlからダウンロードできます。
- macOS の場合、クライアントバージョン (22.02.3 以降) は App Store からダウンロードできます。

管理者構成—**Citrix Secure Access** クライアントベースの **TCP/UDP** アプリケーションへのアクセス

前提条件

TCP/UDP アプリにアクセスするには、次の要件が満たされていることを確認してください。

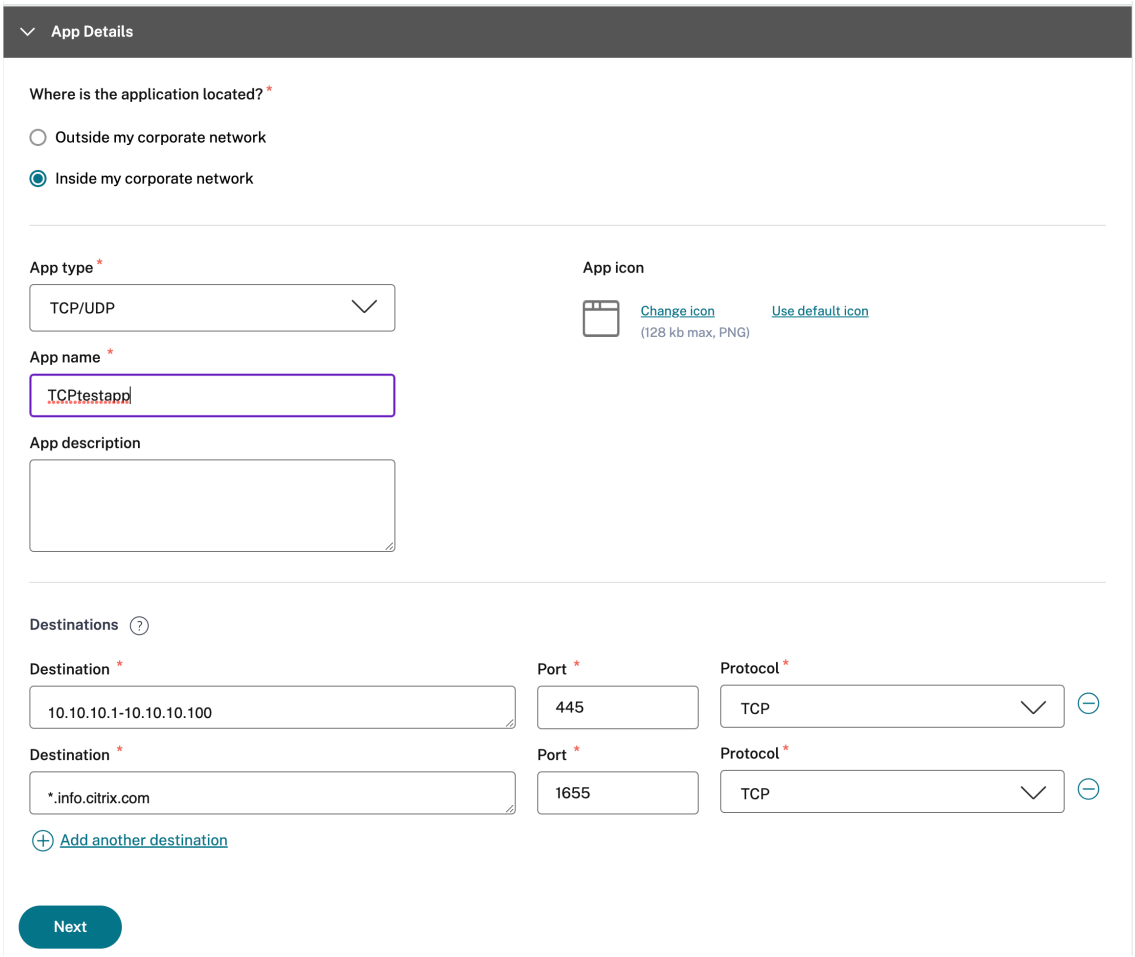
- Citrix Cloud の Citrix Secure Private Access へのアクセス。
- Citrix Cloud Connector-クラウドコネクタのインストールでキャプチャされた Active Directory ドメイン構成用の Citrix Cloud Connector
- ID とアクセス管理-設定を完了します。詳しくは、「ID とアクセス管理」を参照してください。
- Connector Appliance —Citrix では、リソースの場所にある高可用性セットアップに 2 つの Connector Appliance をインストールすることをお勧めします。コネクタは、オンプレミス、データセンターのハイパーバイザー、またはパブリッククラウドのいずれかにインストールできます。Connector Appliance とそのインストールについて詳しくは、「クラウドサービス用 Connector Appliance」を参照してください。
- TCP/UDP アプリには Connector Appliance 使用する必要があります。

> 重要:
>
> アプリの完全なエンドツーエンド構成については、「簡単なオンボーディングとセットアップのための管理者向けガイド付きワークフロー」を参照してください。

1. Citrix の Secure Private Access タイルで、「管理」をクリックします。
2. [続行] をクリックし、[アプリを追加] をクリックします。

   > 注:
   >
   > [続行] ボタンは、ウィザードを初めて使用する場合にのみ表示されます。その後の使用では、[アプリケーション] ページに直接移動して [アプリの追加] をクリックできます。

   アプリは宛先の論理的なグループです。複数の送信先に対してアプリを作成できます。各宛先は、バックエンドで異なるサーバーを意味します。たとえば、1 つのアプリケーションに 1 つの SSH、1 つの RDP、1 つのデータベースサーバー、および 1 つの Web サーバーを含めることができます。宛先ごとに 1 つのアプリを作成する必要はありませんが、1 つのアプリに複数の送信先を含めることができます。
3. [テンプレートの選択] セクションで、[スキップ] をクリックして TCP/UDP アプリを手動で構成します。
4. [アプリの詳細] セクションで、[社内ネットワークの内部] を選択し、次の詳細を入力し、[次へ] をクリックします。



- [アプリの種類] —[TCP/UDP] を選択します。
- アプリ名—アプリケーションの名前。
- アプリアイコン—アプリアイコンが表示されます。この情報は入力しなくても構いません。
- [アプリの説明] —追加するアプリの説明。この情報は入力しなくても構いません。
- 宛先—リソースの場所に存在するバックエンドマシンの IP アドレスまたは FQDN。次のように、1 つまたは複数の宛先を指定できます。
  - **IP** アドレス **v4**
  - **IP** アドレスの範囲：例:10.68.90.10-10.68.90.99
  - **CIDR** —例:10.106.90.0/24
  - マシンまたはドメイン名の **FQDN** —単一またはワイルドカードドメイン。例:ex.destination.domain.com、*.domain.com

    > 重要:
    >
    > 管理者が IP アドレスを使用してアプリを設定した場合でも、エンドユーザーは FQDN を使

> 用してアプリにアクセスできます。これが可能なのは、Citrix Secure Access クライアントが FQDN を実際の IP アドレスに解決できるためです。
> 次の表に、さまざまな宛先の例と、これらの宛先を使用してアプリにアクセスする方法を示します。

デスティネーション入力	アプリへのアクセス方法
10.10.10.1-10.10.10.100	エンドユーザーは、この範囲の IP アドレスを介してのみアプリにアクセスすることが期待されます。
10.10.10.0/24	エンドユーザーは、IP CIDR で構成された IP アドレスを介してのみアプリにアクセスすることが期待されます。
10.10.10.101	エンドユーザーは 10.10.10.101 からのみアプリにアクセスすることが期待されます
*.info.citrix.com	エンドユーザーは、info.citrix.com および info.citrix.com (親ドメイン) のサブドメインにもアクセスすることが期待されます。たとえば、info.citrix.com, sub1.info.citrix.com, level1.sub1.info.citrix.com 注: ワイルドカードは常にドメインの開始文字である必要があり、*. は 1 つだけ使用できます。
info.citrix.com	エンドユーザーは、info.citrix.com サブドメインにはアクセスしないことが期待されます。たとえば、sub1.info.citrix.com はアクセスできません。

- **Port** —アプリが実行されているポート。管理者は宛先ごとに複数のポートまたはポート範囲を設定できます。

  次の表に、宛先に設定できるポートの例を示します。

ポート入力	説明
*	デフォルトでは、ポートフィールドは “*” (任意のポート) に設定されています。宛先では、1 ～65535 のポート番号がサポートされています。
1300–2400	宛先では、1300 から 2400 までのポート番号がサポートされています。
38389	宛先ではポート番号 38389 だけがサポートされます。
22,345,5678	ポート 22、345、5678 は宛先でサポートされています。

ポート入力	説明
1300–2400, 42000-43000,22,443	ポート番号の範囲は 1300 ～2400、42000 ～43000 で、ポート 22 と 443 は宛先でサポートされます。

> 注:
>
> ワイルドカードポート (*) は、ポート番号または範囲と共存できません。

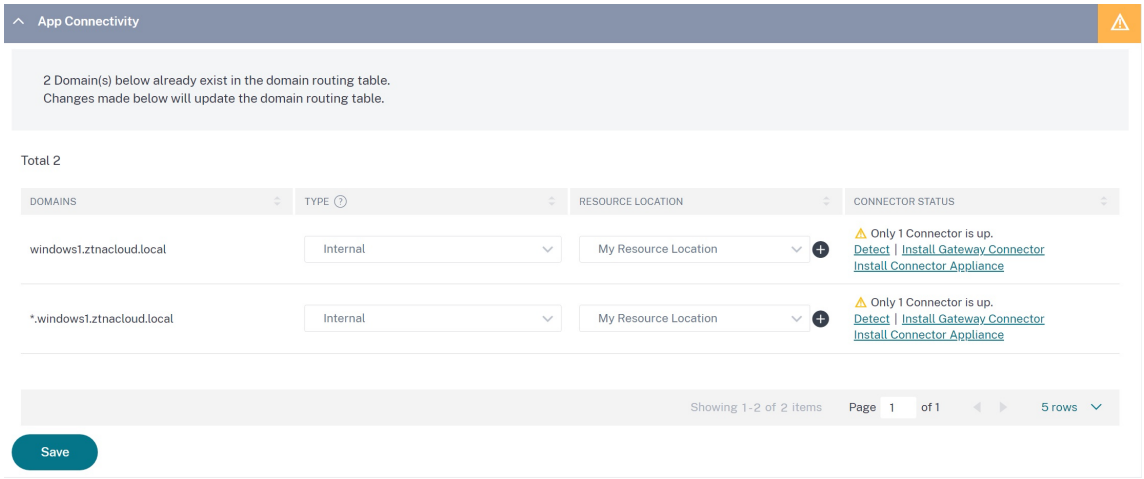
- プロトコル—TCP/UDP

5. アプリケーション接続セクションでは、アプリケーションドメインテーブルのミニバージョンを使用してルーティングを決定できます。宛先ごとに、異なるリソースの場所または同じリソースの場所を選択できます。前の手順で設定した送信先は、**DESTINATION** 列に入力されます。ここに追加された宛先は、メインのアプリケーションドメインテーブルにも追加されます。**Application Domains** テーブルは、接続の確立とトラフィックを正しいリソースロケーションに転送するためのルーティング決定を行うための信頼できる情報源です。アプリケーションドメインテーブルおよび考えられる IP 競合シナリオについて詳しくは、「アプリケーションドメイン-*IP* アドレスの競合解決」セクションを参照してください。
6. 次のフィールドでは、ドロップダウンメニューから入力を選択し、[次へ] をクリックします。

> 注:
>
> 内部ルートタイプのみがサポートされています。

- リソースの場所—ドロップダウンメニューから、少なくとも 1 つの Connector Appliance がインストールされたリソースの場所に接続する必要があります。

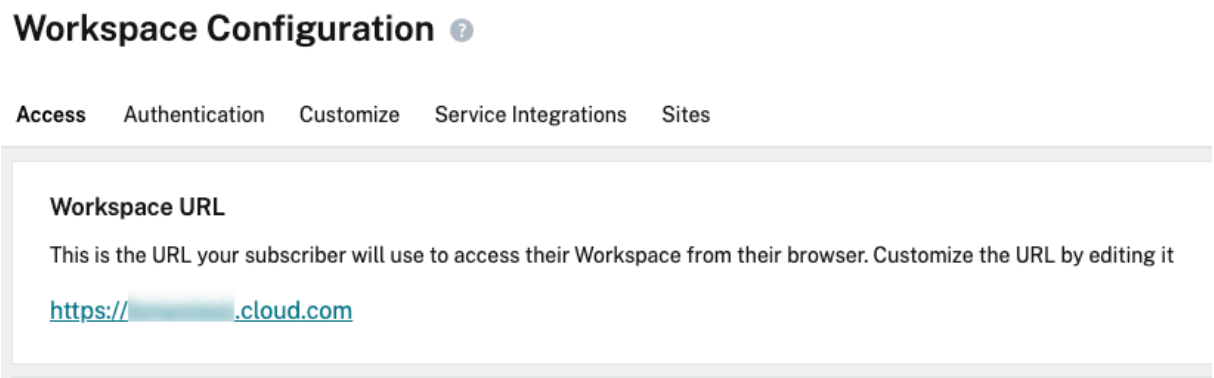
> 注:
>
> Connector Appliance のインストールは、[アプリケーション接続] セクションからサポートされます。Citrix Cloud ポータルの［リソースの場所］セクションにもインストールできます。リソースロケーションの作成について詳しくは、「リソースロケーションの設定」を参照してください。



7. [完了] をクリックします。アプリが [アプリケーション] ページに追加されます。アプリケーションを構成した後で、アプリケーションページからアプリケーションを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

   - **[アプリケーションを編集]**
   - 削除

> 注:
>
> - ユーザーにアプリへのアクセスを許可するには、管理者がアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者がアプリの利用者を追加し、セキュリティコントロールを設定します。詳細については、「アクセスポリシーの作成」を参照してください。
> - ユーザーに必要な認証方法を設定するには、「ID と認証の設定」を参照してください。
> - ユーザーと共有するワークスペース URL を取得するには、Citrix Cloud メニューから［ワークスペース構成］をクリックし、［アクセス］タブを選択します。



管理者設定—**Citrix Secure Access** クライアントベースの **HTTP/HTTPS** アプリケーションへのアクセス

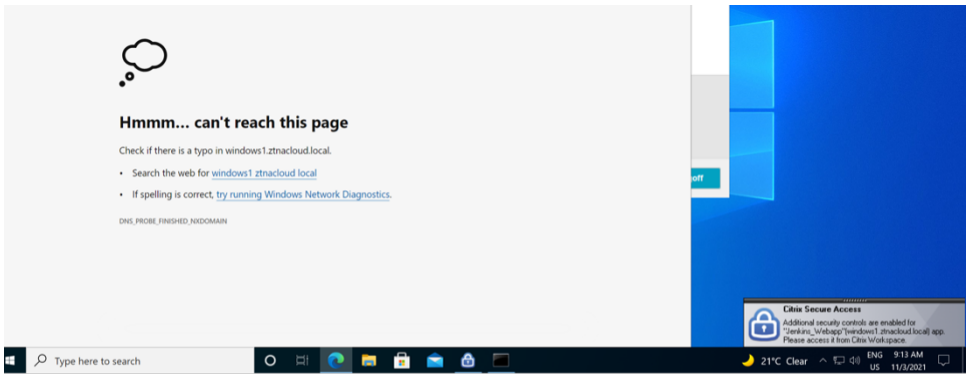
> 注:
>
> Citrix Secure Access クライアントを使用して既存または新規の HTTP/HTTPS アプリにアクセスするには、リソースの場所に少なくとも 1 つ（高可用性のためには 2 つを推奨）の Connector Appliance インストールする必要があります。コネクタアプライアンスは、オンプレミス、データセンターのハイパーバイザー、またはパブリッククラウドにインストールできます。Connector Appliance とそのインストールの詳細については、クラウドサービス用 Connector Appliance を参照してください。

前提条件

- Citrix Cloud の Citrix Secure Private Access へのアクセス。

注意事項

- セキュリティ制御が強化された内部 Web アプリには、Citrix Secure Access クライアントからはアクセスできません。
- 拡張セキュリティ制御が有効になっている HTTP (S) アプリケーションにアクセスしようとすると、次のポップアップメッセージが表示されます。**<”app name”(FQDN) >** アプリでは追加のセキュリティコントロールが有効になっています。**Citrix Workspace** からアクセスしてください。



- SSO エクスペリエンスを有効にする場合は、Citrix Workspace アプリまたは Web ポータルを使用して Web アプリにアクセスします。

HTTP (S) アプリを構成する手順は、「エンタープライズ Web アプリのサポート」で説明されている既存の機能と同じです。

TCP/UDP および HTTP (S) アプリへのアダプティブアクセス

アダプティブアクセスにより、管理者は、デバイスのポスチャチェック、ユーザーの位置情報、ユーザーの役割、Citrix Analytics サービスが提供するリスクスコアなど、複数のコンテキスト要因に基づいて、ビジネスクリティカルなアプリへのアクセスを管理できます。

> 注:
>
> - TCP/UDP アプリケーションへのアクセスを拒否できます。管理者は、ユーザー、ユーザーグループ、ユーザーがアプリケーションにアクセスするデバイス、およびアプリケーションにアクセスする場所（国）に基づいてポリシーを作成します。アプリケーションへのアクセスはデフォルトで許可されています。
> - アプリ用に作成されたユーザーサブスクリプションは、TCP/UDP アプリケーション用に構成されたすべての TCP/UDP アプリ宛先に適用されます。

アダプティブアクセスポリシーを作成するには

管理者は、管理者ガイド付きのワークフローウィザードを使用して、Secure Private Access サービス内の SaaS アプリ、内部 Web アプリ、TCP/UDP アプリへのゼロトラストネットワークアクセスを設定できます。

> 注:
>
> - アダプティブアクセスポリシーの作成について詳しくは、「アクセスポリシーの作成」を参照してください。
> - Secure Private Access サービスの SaaS アプリ、社内 Web アプリ、TCP/UDP アプリへのゼロトラストネットワークアクセスのエンドツーエンド構成については、簡単なオンボーディングとセットアップのための管理者ガイド付きワークフローをご覧ください。

注意事項

- セキュリティ強化が有効になっている既存の Web アプリへのアクセスは、Secure Access クライアント経由で拒否されます。Citrix Workspace アプリを使用したログインを促すエラーメッセージが表示されます。
- Citrix Workspace アプリを介したユーザーリスクスコアやデバイスポスチャチェックなどに基づく Web アプリのポリシー構成は、Secure Access クライアント経由でアプリにアクセスする際に適用されます。
- アプリケーションにバインドされたポリシーは、アプリケーション内のすべての宛先に適用できます。

DNS 解決

Connector Appliance には、DNS 解決のための DNS サーバー構成が必要です。

Citrix Secure Access クライアントを **Windows** マシンにインストールする手順

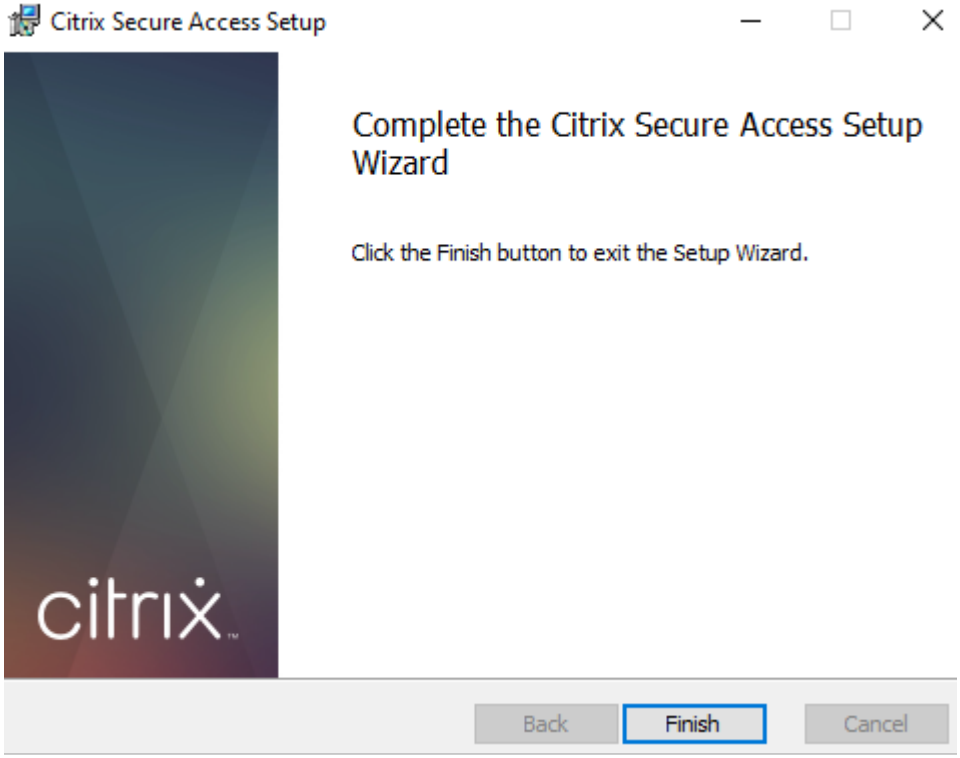
サポートされている **OS** バージョン**:**

Windows-Windows11、Windows10、Windows Server 2016、および Windows Server 2019。

Citrix Secure Access クライアントを Windows マシンにインストールする手順は次のとおりです。

1. Citrix Secure Access クライアントをhttps://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.htmlからダウンロードします。
2. [インストール] をクリックして、Windows マシンにクライアントをインストールします。既存の Citrix Gateway クライアントがある場合は、同じクライアントがアップグレードされます。

3. ［完了］をクリックして、インストールを完了します。



> 注:
>
> Windows のマルチユーザーセッションはサポートされていません。

Microsoft Edge ランタイムのインストール手順

Secure Access クライアントの認証 UI には Microsoft Edge ランタイムが必要になりました。
これは、最新の Windows 10 および Windows 11 マシンにデフォルトでインストールされます。それ以前のバージョンのマシンでは、次の手順を実行します。

1. 次のリンクに移動します https://go.microsoft.com/fwlink/p/?LinkId=2124703。
2. Microsoft Edge をダウンロードしてインストールします。ユーザーシステムに Microsoft Edge ランタイムがインストールされていない場合、ワークスペース URL に接続しようとすると、Citrix Secure Access クライアントからインストールを求めるメッセージが表示されます。

> 注:
>
> SCCM ソフトウェアやグループポリシーなどの自動化ソリューションを使用して、Citrix Secure Access クライアントまたは Microsoft Edge Runtime をクライアントマシンにプッシュできます。

Citrix Secure Access クライアントを **macOS** マシンにインストールする手順

前提条件:

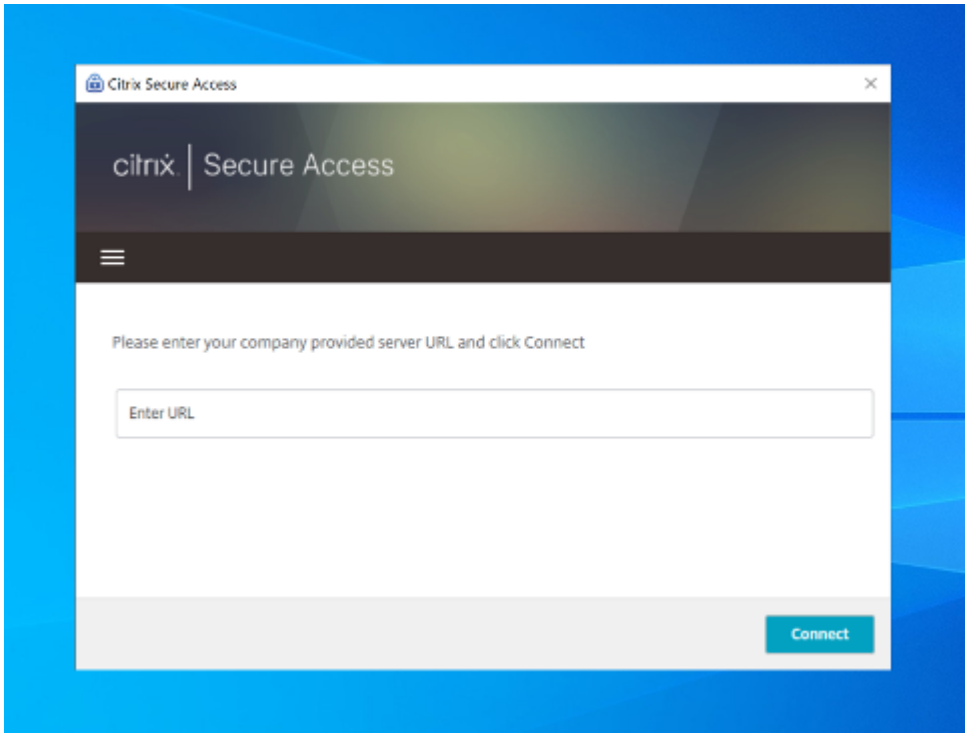
- macOS 向け Citrix Secure Access クライアントをアプリストアからダウンロードします。このアプリは macOS 10.15 (Catalina) 以降から利用できます。
- プレビュービルドは、macOS モントレー (12.x) の TestFlight アプリでのみ使用できます。
- App Store アプリと TestFlight プレビューアプリを切り替える場合は、Citrix Secure Access アプリで使用するプロファイルを再作成する必要があります。たとえば、で接続プロファイルを使用していた場合は `blr.abc.company.com`、VPN プロファイルを削除し、同じプロファイルをもう一度作成します。

サポートされている **OS** バージョン**:**

- macOS: 12.x (Monterey)、11.x (Big Sur)、10.15 (Catalina) がサポートされています。
- モバイルデバイス:iOS と Android はサポートされていません。

設定済みアプリの起動**-**エンドユーザーフロー

1. クライアントデバイス上で Citrix Secure Access クライアントを起動します。
2. Citrix Secure Access クライアントの［URL］フィールドに、顧客管理者から提供されたワークスペース URL を入力し、［接続］をクリックします。これは 1 回限りのアクティビティで、URL は後で使用できるように保存されます。



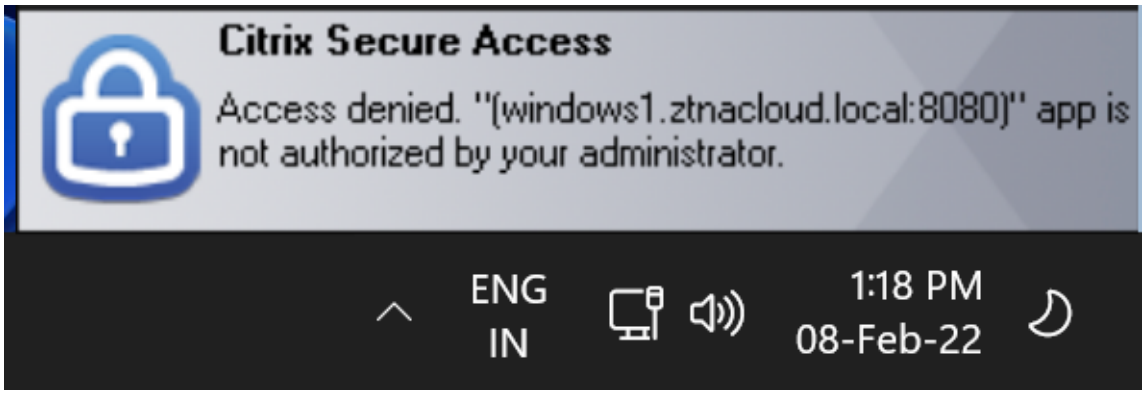
3. Citrix Cloud で構成された認証方法に基づいて、ユーザーに認証を求められます。
   認証に成功すると、ユーザーは構成済みのプライベートアプリにアクセスできます。

ユーザー通知メッセージ

次のシナリオでは、ポップアップ通知メッセージが表示されます。

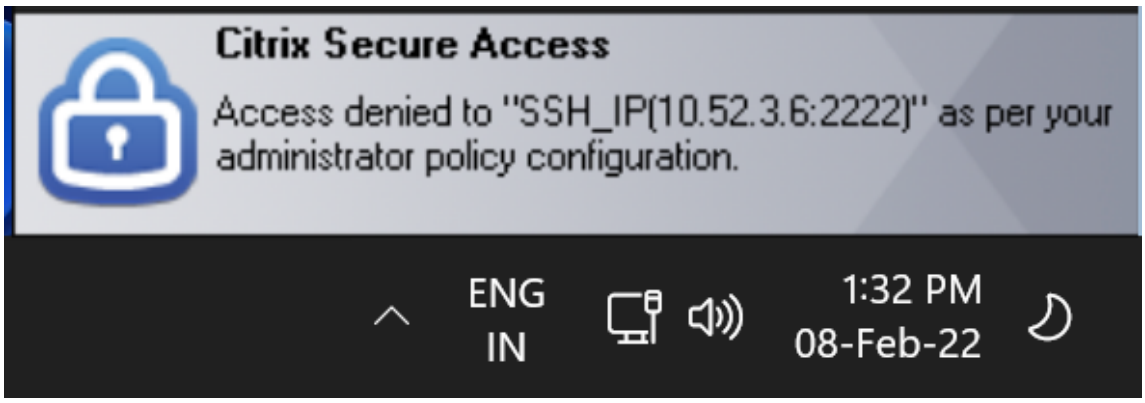
- このアプリは、管理者によってユーザーに対して承認されていません。

  原因**:** アクセスされた宛先 IP アドレスまたは FQDN 用に構成されたアプリケーションが、ログインしているユーザーに対してサブスクライブされていません。



- アクセスポリシーを評価すると、アクセスが拒否されます。

  原因**:** アプリケーションにバインドされたポリシーが、ログインしているユーザーに対して「Deny Access」と評価されたため、宛先 IP アドレスまたは FQDN へのアクセスが拒否されました。



- 拡張セキュリティ制御がアプリに対して有効になっている。

  原因**:** アクセス先のアプリケーションに対して、強化されたセキュリティ制御が有効になっています。このアプリケーションは、Citrix Workspace アプリを使用して起動できます。

追加情報

アプリケーションドメイン**-IP** アドレスの競合解決

アプリの作成中に追加された宛先は、メインのルーティングテーブルに追加されます。
ルーティングテーブルは、接続の確立とトラフィックを正しいリソースロケーションに転送するためのルーティング決定を行うための信頼できる情報源です。

- 宛先 IP アドレスは、リソースの場所全体で一意である必要があります。
- ルーティングテーブル内の IP アドレスまたはドメインが重複しないようにすることを Citrix ではお勧めします。オーバーラップが発生した場合は、解決する必要があります。

競合シナリオの種類は次のとおりです。完全重複は、競合が解決されるまで管理者構成を制限する唯一のエラーシナリオです。

競合シナリオ	既存のアプリケーションドメインエントリ	アプリ追加からの新規エントリー	動作
サブセットオーバーラップ	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	許可; 警告情報-IP ドメインと既存のエントリのサブセットオーバーラップ
サブセットオーバーラップ	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	許可; 警告情報-IP ドメインと既存のエントリのサブセットオーバーラップ
部分オーバーラップ	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	許可; 警告情報-IP ドメインと既存のエントリが部分的に重複しています
部分オーバーラップ	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	許可; 警告情報-IP ドメインと既存のエントリが部分的に重複しています
完全オーバーラップ	10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	エラー。<Completely overlapping IP domain's value> IP ドメインが既存のエントリと完全に重複しています。既存のルーティング IP エントリを変更するか、別の宛先を設定してください
完全オーバーラップ	10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	エラー。<Completely overlapping IP domain's value> IP ドメインが既存のエントリと完全に重複しています。既存のルーティング IP エントリを変更するか、別の宛先を設定してください
完全一致	20.20.0/29 RL1	20.20.20.0/29	許可。ドメインはドメインルーティングテーブルに存在します。加えられた変更により、ドメインルーティングテーブルが更新されます。

> 注:
>
> - 追加された宛先が完全に重複する場合は、**[App Details**] セクションにアプリの構成中にエラーが表示されます。管理者は、[**App Connectivity**] セクションで宛先を変更して、このエラーを解決する必要があります。
>
> アプリの詳細セクションにエラーがなければ、管理者はアプリの詳細を保存できます。ただし、[**App Connectivity**] セクションでは、宛先にサブセットがあり、相互に部分的に重複している場合や、メインルーティングテーブル内の既存のエントリが重複している場合は、警告メッセージが表示されます。この場合、管理者はエラーを解決するか、設定を続行するかを選択できます。
> - アプリケーションドメインテーブルはクリーンな状態に保つことをお勧めします。IP アドレスドメインが重複することなく適切なチャンクに分割されると、新しいルーティングエントリを簡単に設定できます。

ログインとログアウトのスクリプト構成レジストリ

Citrix Secure Access クライアントは、Citrix Secure Access クライアントが Citrix Secure Private Access クラウドサービスに接続するときに、次のレジストリからログインおよびログアウトスクリプト構成にアクセスします。

Registry: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- ログインスクリプトパス:SecureAccessLoginScript タイプ REG_SZ
- ログアウトスクリプトパス:SecureAccessLogoutScript タイプ REG_SZ

リリースノートリファレンス

- Citrix Secure Access for Windows リリースノート
- macOS 向け Citrix Secure Access リリースノート
- Citrix Secure Private Access リリースノート

TCP サーバーと UDP サーバー用に予約された CIDR アドレス

January 9, 2024

管理者は TCP/UDP サーバーの予約済み CIDR IP アドレスを設定できます。これらの IP アドレスは、DNS 解決時に実際の IP アドレスの代わりに DNS 応答で共有されます。

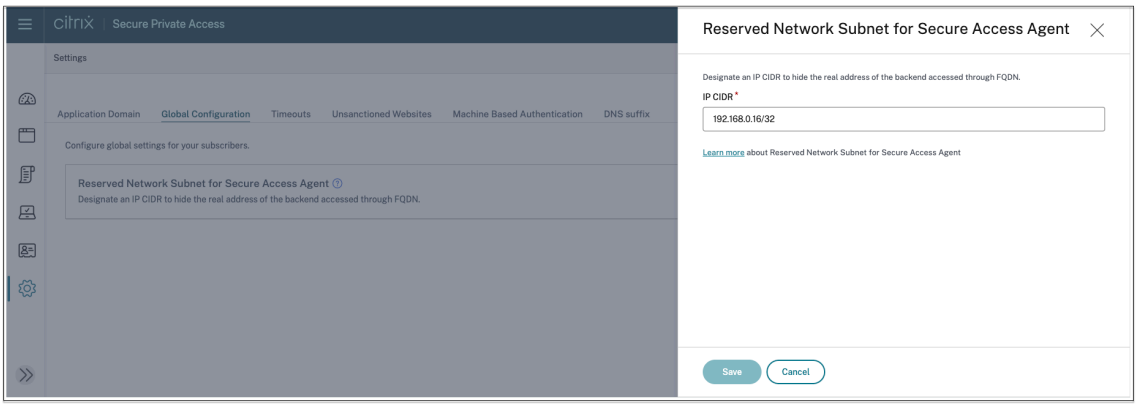
許可されている予約済み CIDR IP アドレスの範囲は次のとおりです。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> 注:
>
> 予約した IP アドレスが次のものと競合しないようにしてください。
>
> - 顧客のリソースの場所の TCP/UDP アプリケーション用に設定された IP アドレス。
> - クライアントマシンのネットワークサブネット。

予約済み **CIDR IP** アドレスの設定

1. **[設定]** をクリックし、**[グローバル設定]** をクリックします。



2. 「**Secure Access Agent** の予約済みネットワークサブネット」で、**[管理]** をクリックします。
3. **[IP CIDR]** にプライベート IP アドレス範囲を入力します。
4. ［保存］をクリックします。

FQDN を **IP** アドレスに変換するための **DNS** サフィックス

January 9, 2024

DNS サフィックスは、すべてのエンドユーザーに適用されるグローバル設定です。Citrix Secure Private Access サービスの DNS サフィックス機能は、以下の用途に使用できます。

- Citrix Secure Access クライアントが、バックエンドサーバーの DNS サフィックスドメインを追加して、非完全修飾ドメイン名（ホスト名）を完全修飾ドメイン名（FQDN）に変換できるようにします。
- 管理者が IP アドレス（IP CIDR/IP 範囲）を使用してアプリケーションを設定できるようにします。これにより、エンドユーザーは、DNS サフィックスドメインの対応する FQDN を使用してアプリケーションにアクセスできるようになります。

たとえば、非完全修飾ドメイン名「workday」を解決するときに、DNS サフィックス「citrix.net」が設定されている場合、オペレーティングシステムはサフィックス「citrix.net」を追加し、解決は「workday.citrix.net」になります。

複数の DNS サフィックスが設定されている場合、DNS サフィックスは順番に解決されます。たとえば、次のサフィックスが追加されたとします。

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

エンドユーザーが「workday」と入力すると、オペレーティングシステムは次の順序で FQDN の解決を試みます。1 つのサフィックスで成功すると、残りのサフィックスはスキップされます。

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> 重要:
>
> - DNS サフィックス設定では、DNS サフィックス機能を使用して設定されたドメインにサフィックスを付けることによってのみ、クライアントは完全修飾されていないドメイン名を解決できます。エンドユーザーが DNS サフィックスドメインの FQDN にアクセスするには、管理者がアプリケーションに IP アドレス、FQDN、またはワイルドカードドメインを設定する必要があります。詳細については、「ユースケース例」のポイント 4 を参照してください。
> - 2 つの異なるアプリケーション (1 つは FQDN、もう 1 つは IP アドレスで、どちらも同じバックエンドサーバーに対応する) が設定されている場合、IP アドレスを持つアプリケーションのポリシーが優先されます。詳細については、「ユースケース例」のポイント 5 を参照してください。

前提条件

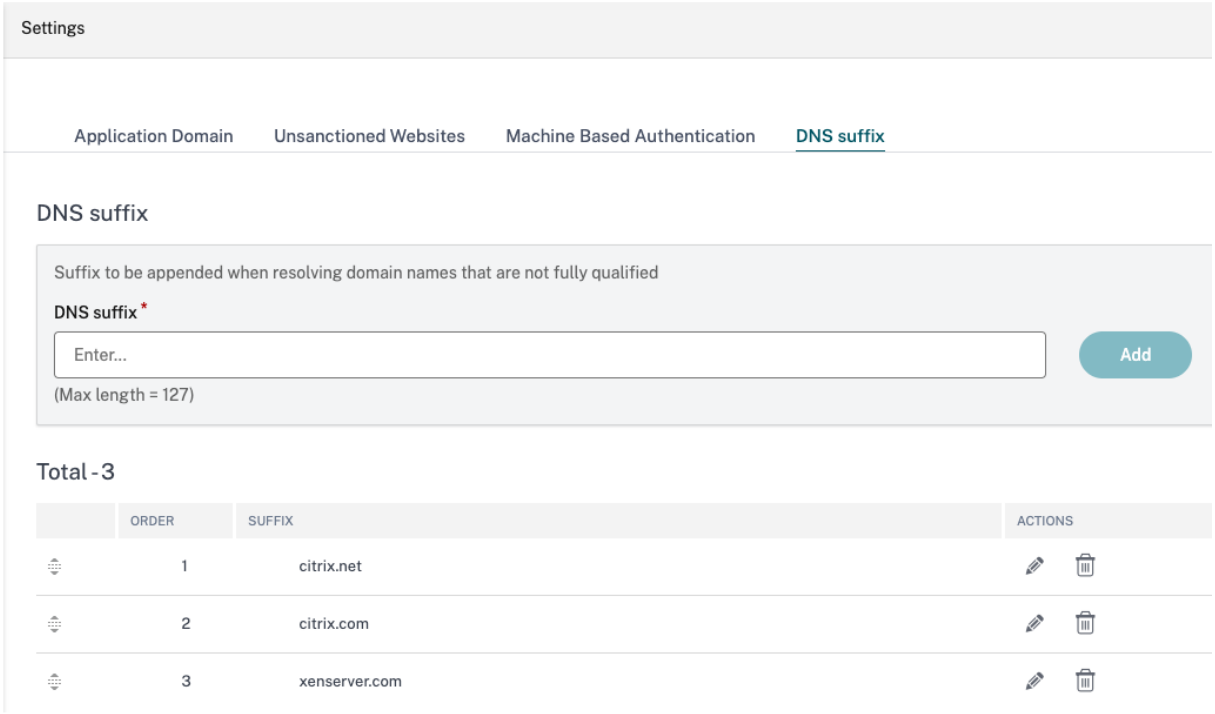
> - お客様が DNS サフィックス機能を使用するには、Secure Private Access アドバンスト・エディションの資格が必要です。
> - Citrix 製品管理チームに連絡して、DNS サフィックス機能フラグを有効にしてください。

DNS サフィックスを追加する方法

1. 「Secure Private Access」タイルで、「管理」をクリックします。
2. Secure Private Access のランディングページで、「設定」をクリックし、「**DNS** サフィックス」をクリックします。
3. 「**DNS Suffix** 」フィールドに、非完全修飾名を解決するときに追加する必要があるサフィックスを入力します。

4. ［追加］をクリックします。

サフィックスは、追加された順序に基づいて一覧表示されます。管理者はサフィックスを削除または変更できます。



ユースケースの例

以下に注意してください:

- 管理者が IP アドレス 192.0.2.1 をお客様のネットワーク内のマシンに割り当てました。
- マシンの FQDN（IP アドレスが 192.0.2.1 の）は、「citrix.net」というドメイン（たとえば、workday.citrix.net）にあります。

		DNS サフィックスとアプリ設定	エンドユーザーエクスペリエンス
	1	管理者は DNS サフィックスを「citrix.net」に設定し、ユーザー 1 のアクセスポリシーを「許可」に設定した IP アドレス 192.0.2.1 のアプリを作成します。	ユーザー 1 が「workday」に接続しようとすると、FQDN のサフィックスには「citrix.net」(workday.citrix.net) が付き、IP アドレスは 192.0.2.1 に解決されます。アプリが設定されているユーザー 1 には 192.0.2.1 が許可されているため、アクセスが許可されます。 注**:** エンドユーザーは、192.0.2.1 または workday.citrix.net または「workday」から Workday アプリにアクセスできます。 DNS サフィックスを設定しないと、「workday」および「workday.citrix.net」経由のアクセスは拒否されます。
	2	管理者は DNS サフィックスを「citrix.net」に設定し、FQDN（workday.citrix.net）を使用してアプリを作成し、ユーザー 1 のアクセスポリシーを「許可」に設定します。	ユーザー 1 が「作業日」に接続しようとすると、「citrix.net」の末尾に「workday」が付きます (workday.citrix.net)。アプリケーションが「workday.citrix.net」で構成され、ユーザー 1 のアクセスポリシーが「許可」に設定されているため、エンドユーザーは Workday にアクセスできます。

		DNS サフィックスとアプリ設定	エンドユーザーエクスペリエンス
			注**:** エンドユーザーは workday.citrix.net または「workday」から Workday アプリにアクセスできます。
	3	管理者は DNS サフィックスを「citrix.net」に設定し、ワイルドカードドメイン「*.citrix.net」を使用してアプリを作成し、ユーザー 1 のアクセスポリシーを「許可」に設定します。	この IP アドレスで設定されているアプリがないため、192.0.2.1 へのアクセスは拒否されます。 ユーザー 1 が「作業日」に接続しようとすると、「citrix.net」の末尾に「workday」が付きます (workday.citrix.net)。アプリケーションが「*.citrix.net」で構成され、ユーザー 1 のアクセスポリシーが「許可」に設定されているため、エンドユーザーは Workday にアクセスできます。 注**:** エンドユーザーは workday.citrix.net または「workday」を使用して Workday にアクセスできます。 この IP アドレスで設定されているアプリがないため、192.0.2.1 へのアクセスは拒否されます。

		DNS サフィックスとアプリ設定	エンドユーザーエクスペリエンス
	4	管理者は DNS サフィックスを「citrix.net」として設定します。ユーザー 1 には、FQDN (workday.citrix.net) または 192.0.2.1 のアプリケーションは設定されていません。	ユーザー 1 が「workday」に接続しようとすると、クライアントは「workday」のサフィックスに「citrix.net」を付け、「workday.citrix.net」を 192.0.2.1 と解決します。ただし、ユーザー 1 はプライベートサーバー (workday.citrix.net/192.0.2.1) に接続できません。これは、ユーザー 1 が 192.0.2.1 または workday.citrix.net または *.citrix.net で構成されているアプリがないため、ユーザー 1 はプライベートサーバー (workday.citrix.net/192.0.2.1) に接続できません。
	5	管理者は DNS サフィックスを「citrix.net」として設定します。IP アドレス 192.0.2.1 のアプリを追加し、user1 のアクセスポリシーを「拒否」に設定します。次に、解決が 192.0.2.1 となる FQDN を持つ別のアプリ（workday.citrix.net）を追加し、ユーザー 1 のアクセスポリシーを「許可」に設定します。	ユーザー 1 が「workday」に接続しようとすると、「citrix.net」のサフィックスが Workday (workday.citrix.net) になり、IP アドレスは 192.0.2.1 に解決されます。ただし、IP 192.0.2.1 で設定されたアプリケーションのポリシーが FQDN で設定されたアプリケーションよりも優先されるため、Workday へのアクセスは拒否されます。

Citrix Workspace アプリを介した Citrix Secure Access クライアントへのシングルサインオン

January 9, 2024

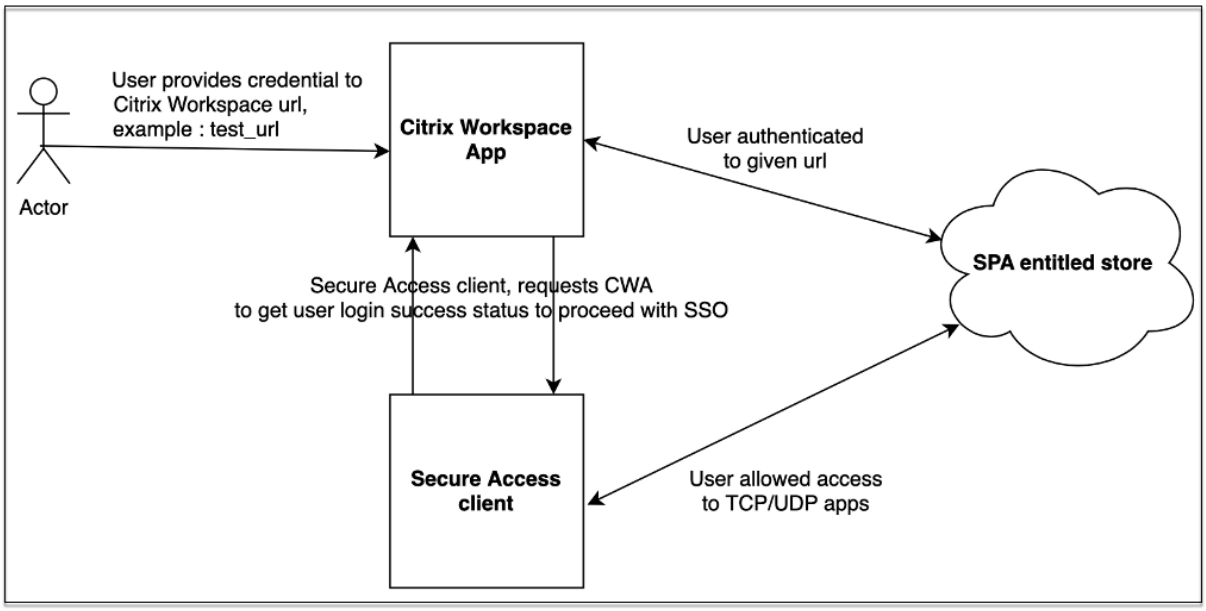
Citrix Secure Access クライアントは、すでに Citrix Workspace アプリ経由でログインしている場合、ワークスペース URL のシングルサインオンをサポートするようになりました。この SSO 機能により、複数の認証が回避されるため、ユーザーエクスペリエンスが向上します。

前提条件

- Citrix Workspace アプリとセキュアアクセスクライアントの両方がデバイスにインストールされている必要があります。
- Citrix Secure Access クライアントで自動 SSO を実行するには、ユーザーが最初に Citrix Workspace アプリにログインしている必要があります。

> 注:
>
> シングルサインオン機能は、Citrix Workspace アプリで構成されたプライマリストアでのみサポートされます。ユーザーがプライマリストア以外のストアにログインした場合、SSO は実行されません。ユーザーは Citrix Secure Access クライアントに手動でログインする必要があります。

次の図は、Citrix Workspace アプリと Citrix Secure Access クライアント間の SSO フローを示しています。



Windows の機能要件

- Citrix Workspace アプリバージョン- **Citrix Workspace 22.10.5.14 (2210.5)** 以上
- Citrix Secure Access バージョン- **22.10.1.9** 以降
- Citrix Secure Access Windows レジストリ- **CWASSO** を有効にする

SSO 機能はデフォルトでは無効になっています。この機能を有効にするには、エンドユーザーマシンに次のレジストリを追加します。

- レジストリ名- EnableCWASSO
- レジストリパス - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- レジストリタイプ-REG_DWORD
- レジストリ値-1

> 重要:
>
> Citrix Workspace アプリでのシングルサインオンを正常に確立するために、エンドユーザーのマシンを再起動する必要がある場合があります。

アクティブなユーザーセッションを終了し、無効ユーザーリストにユーザーを追加します

June 19, 2024

管理者はすべてのアクティブなエンドユーザーセッションをすぐに終了し、ユーザーを無効ユーザーリストに追加できます。この無効なユーザーリストにユーザーを追加すると、すべてのアクティブな Secure Private Access アプリケーションセッションが終了し、今後のアプリケーションアクセスがブロックされます。

Citrix Enterprise Browser、ダイレクトアクセス、CWA for HTML5、およびセキュアアクセスエージェントを介したアクティブなアプリケーションセッションはすべて終了され、ブロックされます。ファイル共有、RDP、SSH セッションなど、Secure Access エージェントを介して接続されているすべてのリソースも終了され、ブロックされます。ブロックされたユーザーは、無効ユーザーリストから削除されるまで、新しいアプリケーションを起動できません。

> 注記:
>
> - 無効なユーザーリストにユーザーを追加しても、設定されている Secure Private Access アクセスポリシーは変更または編集されません。アクセスの終了とブロックは、どのようなアクセスポリシーが設定されているかにかかわらず発生します。ユーザーをリストから削除すると、そのユーザーの既存の Secure Private Access ポリシーが復元されます。
> - ユーザーは 7 日後に無効ユーザーリストから自動的に削除されます。
> - 公開されている Secure Private Access アプリケーションへのアクセスのみがブロックされます。Citrix Enterprise Browser を介したインターネットアクセスは、ユーザーがブロックリストに追加された後

> でも（Web フィルタリング構成に基づいて）許可または拒否されます。

使用例

この機能は次のシナリオで使用できます。

- 従業員が組織を辞めるか、組織から解雇されます。この場合、管理者はアクティブな Secure Private Access セッションを終了し、今後のアプリアクセスをブロックすることで、すべての Secure Private Access アプリアクセスを取り消します。
- デバイスが紛失または盗難に遭った。この場合、アクセスはブロックされ、現在のセッションはすべて終了します。状況が制御されたら、そのユーザーを無効ユーザーリストから削除できます。
- ユーザーがアプリへのアクセスを悪用します。この場合、ユーザーのアクセス権を直ちに取り消すことができます。ユーザーがリストに追加されるまで、アクセスはブロックされます。

無効ユーザーリストへのユーザーの追加

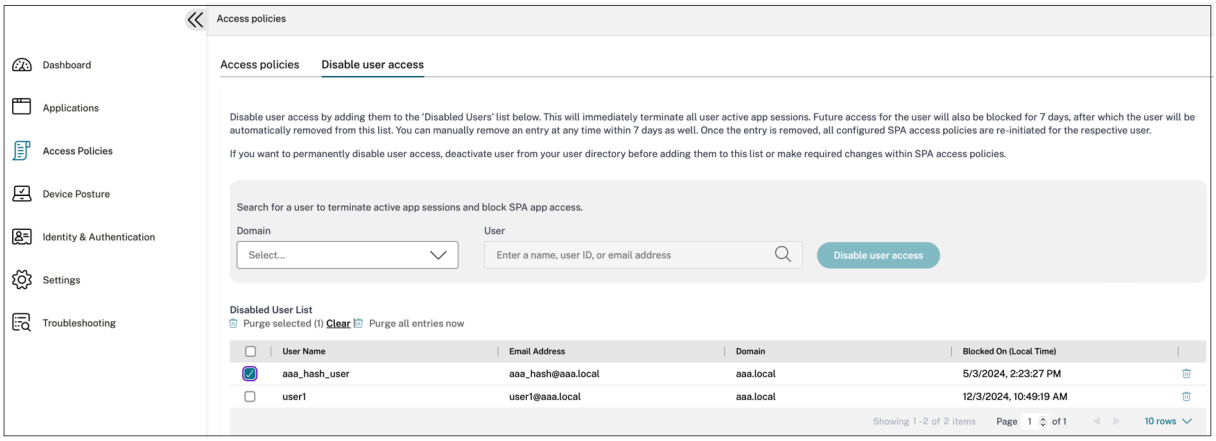
1. [**Secure Private Access] > [**アクセスポリシー] に移動し、[ユーザーアクセスを無効にする] タブをクリックします。
2. 「ドメイン」で、アクセスを無効にする必要があるドメインを選択します。
3. 「ユーザー」で、無効ユーザー・リストに追加する必要があるユーザー名を検索します。検索条件に一致するすべてのユーザー名が表示されます。ユーザーがディレクトリサービスから削除されると、そのユーザー名はユーザーリストに表示されません。
4. [ユーザーアクセスを無効にする] をクリックします。

   ユーザーは無効ユーザーリストに追加されます。ユーザーが無効ユーザーリストに追加されると、次のアクションが実行されます：

   - すべてのアクティブな Secure Private Access・セッションはただちに終了します。
   - すべての Secure Private Access 公開アプリケーションへの今後のアクセスはブロックされます。
   - Citrix Enterprise Browser を介したインターネットアクセスは、ユーザーが無効ユーザーリストに追加された後でも許可されます。公開されている Secure Private Access アプリケーションへのアクセスのみがブロックされます。
   - 無効になっているすべてのユーザーは、7 日後に無効ユーザーリストから自動的に削除されます。削除後は、Secure Private Access ポリシーが優先され、アクセスが回復します。

「選択項目の削除」オプションを使用して、無効になっているユーザーのリストからユーザーを削除できます。

「すべてのエントリを今すぐ削除」オプションを使用して、無効になっているユーザーリストからすべてのユーザーを削除できます。



推奨事項:

- ユーザーのアクセスを無期限に取り消すには、Active Directory などのそれぞれのディレクトリサービスからユーザーを削除し、無効ユーザーリストに追加します。これにより、ユーザーのアクティブな Secure Private Access セッションが終了し、今後のアプリアクセスがブロックされます。また、ユーザーが Workspace からログアウトすると、ディレクトリの認証情報がアクティブでないため、ユーザーは再度ログインできなくなります。
- ユーザーは 7 日後に無効ユーザーリストから自動的に削除され、その後既存の Secure Private Access ポリシーが復元されます。アクセスのブロックを延長したい場合は、7 日後にユーザーをリストに追加し直してください。

ユーザーセッションのタイムアウト

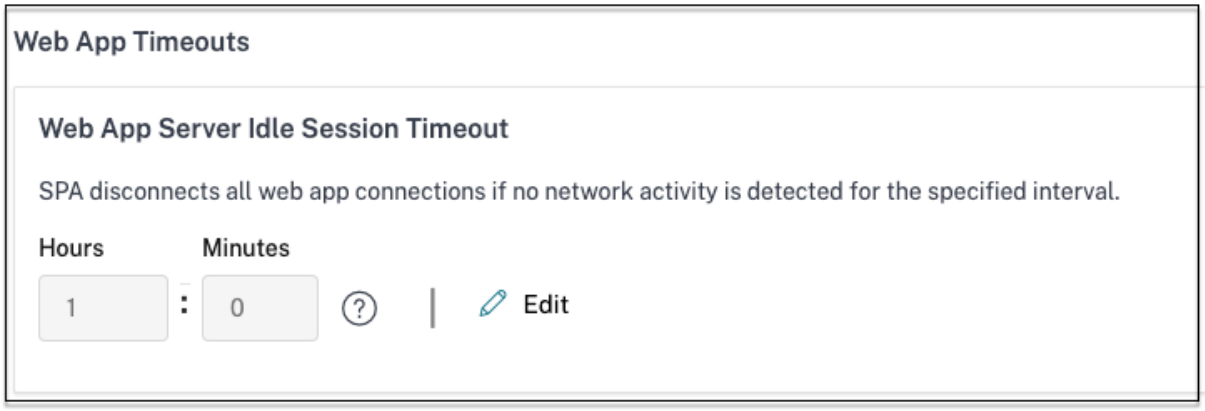
January 9, 2024

指定した期間にネットワークアクティビティがない場合に、Web アプリと Citrix Secure Access クライアントがユーザーセッションを終了するためのタイムアウト期間を設定できます。
Citrix Secure Access クライアントでは、指定した期間にユーザーアクティビティがない場合にセッションを終了するように Citrix Secure Access クライアントを構成することもできます。また、設定した期間が経過すると、ユーザーやネットワークのアクティビティに関係なく、Citrix Secure Access クライアントで強制切断を構成できます。

Web アプリケーションサーバーのタイムアウト

1. **[**設定**] > [**タイムアウト**]** に移動します。
2. **[Web** アプリサーバーのアイドルセッションのタイムアウト**]** で、Web アプリセッションをアイドル状態にできる期間を時間と分単位で選択します。Secure Private Access サービスは、セッションがアイドル状態のままの場合、この時間が経過した後にセッションを終了します。

最短時間は 1 時間、最長時間は 168 時間です。デフォルト値は 2 時間です。

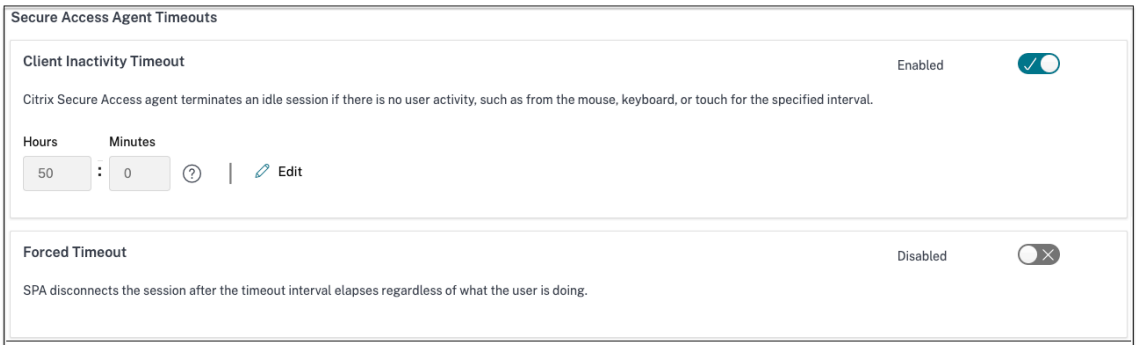


Citrix Secure Access クライアントのタイムアウト

Citrix Secure Access クライアントには次のタイムアウトを設定できます。

- クライアント非アクティブ
- 強制タイムアウト

1. **[設定] > [タイムアウト]** に移動します。



2. **[Secure Access Agent のタイムアウト]** で、適用するタイムアウトの期間を時間と分単位で選択します。

   - クライアント非アクティブタイムアウト: 設定した期間にユーザーアクティビティ (マウスまたはキーボード) がない場合に、Citrix Secure Access クライアントがセッションを終了するまでの時間。このオプションはデフォルトでは無効になっています。設定したタイムアウト期間を適用するには、トグルスイッチを使用してオプションを有効にする必要があります。ただし、設定を保存した後でトグルスイッチを無効にしても、クライアントはタイムアウトを開始しません。

     最短時間は 5 分、最長時間は 168 時間です。デフォルト値は 8 時間です。

   - 強制タイムアウト: ユーザーやネットワークのアクティビティに関係なく、Citrix Secure Access クライアントがセッションを終了するまでの時間。このオプションはデフォルトでは無効になっています。設定したタイムアウト期間を適用するには、トグルスイッチを使用してオプションを有効にする必要が

あります。ただし、設定を保存した後でトグルスイッチを無効にしても、クライアントはタイムアウトを開始しません。

セッション終了の 15 分前に通知メッセージが表示されます。

最短時間は 1 時間、最長時間は 168 時間です。デフォルト値は 168 時間です。

> 注:
>
> これらの設定を複数有効にすると、最初のタイムアウト間隔が経過すると、ユーザー接続は閉じられます。

新しいアクセスポリシーフレームワークへのアプリセキュリティ制御とアクセスポリシーの移行

January 9, 2024

Citrix は、製品でのアプリケーションアクセスの有効化に変更を加えました。以前は、アクセスを有効にするには、ウィザードの［アプリケーション］**>**［アプリサブスクライバー］セクションでユーザーまたはユーザーグループにアプリケーションをサブスクライブする必要がありました。今後、アプリケーションへのアクセスを有効にするには、少なくとも 1 つのアクセスポリシーが必要です。ポリシーを作成する際、ユーザーまたはグループの条件は、ユーザーにアプリケーションへのアクセスを許可するために満たすべき必須条件です。詳細については、「アクセスポリシーの作成」を参照してください。

また、アプリケーション構成の「強化されたセキュリティ」セクションは廃止されました。アクセスポリシーからリモートブラウザでアプリを開くなどの詳細オプションに加えて、クリップボード制限、ダウンロード制限、印刷制限などのきめ細かいセキュリティ制御を適用できるようになりました。この変更により、ユーザーはユーザー、場所、デバイス、リスクなどのコンテキストに基づいて適応型セキュリティを強化できます。

アプリのセキュリティ制御とアクセスポリシーを新しいアクセスポリシーフレームワークに移行し、アプリケーションアクセスのダウンタイムを回避するために、Citrix は必要な変更を加えました。その結果、ポリシーリストに次のような変更が加えられることがあります。

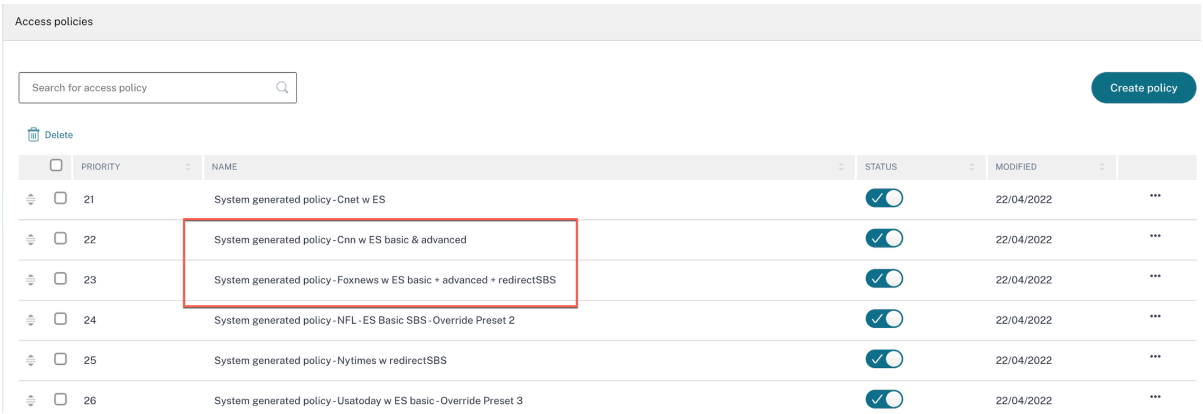
- 新しいポリシーが作成されました
- 1 つのポリシーが複数のポリシーに分割される
- プレフィックス<`System generated policy - App name`>が付いたポリシー名

> 注:
>
> アプリにユーザーまたはグループが追加されていない場合、新しいポリシーは作成されません。

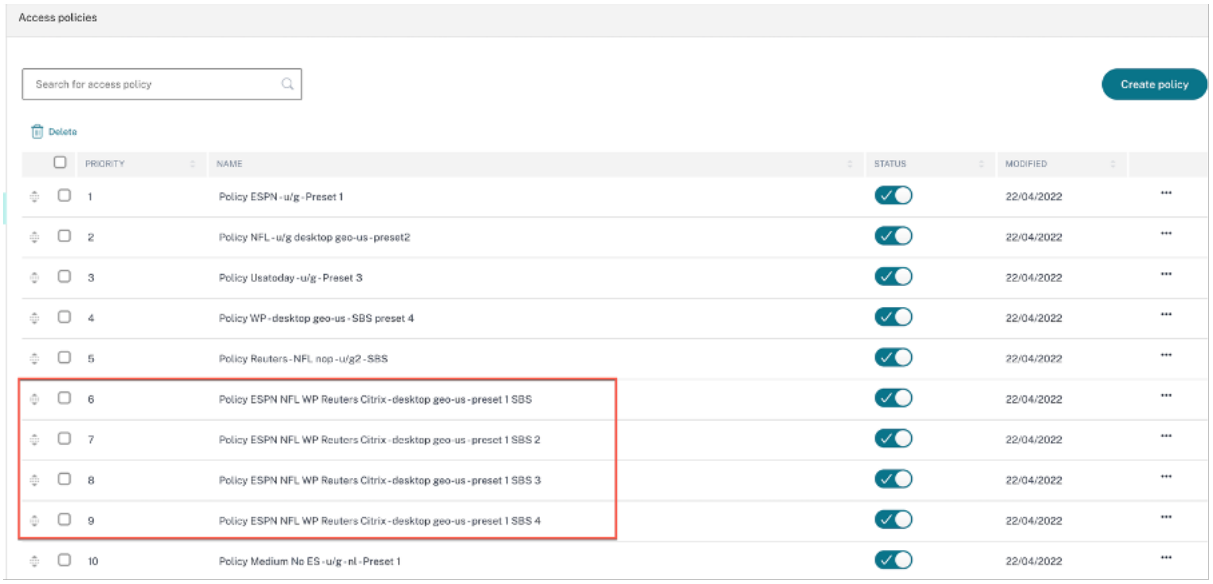
次の表に、変更の概要を示します。

もし…を設定していたら	Then …
強化されたセキュリティ条件のないアプリ	必須条件としてユーザーとグループを含む新しいポリシーが作成されます。ユーザーまたはグループはアクセスポリシーから派生します。アクションが [アクセスを許可] に設定されます。
セキュリティ条件が強化されたアプリ	必須条件としてユーザーとグループを含む新しいポリシーが作成されます。ユーザーまたはグループはアクセスポリシーから派生します。アクションは [制限付きで許可] に設定されています。以前に構成したアプリレベルのセキュリティ条件に基づきます。対応するセキュリティ制限は、ポリシーの作成時に選択されます。移行されたポリシーには、<System generated policy – App name>というプレフィックスが付きます。
プリセット付きのアクセスポリシー	ポリシーでユーザグループ条件がすでに選択されている場合は、新しいポリシーがそのまま作成され、対応するセキュリティ条件がプリセットに基づいてアクセスポリシーで選択されます。
ユーザーまたはグループの条件なしのアクセスポリシー	ユーザーまたはグループはアプリにアクセスするための必須条件であるため、複数のアプリに対して構成された 1 つのポリシーは、アプリごとに異なるユーザーまたはグループが含まれる可能性があるため、複数のポリシーに分割されるようになりました。ユーザーまたはグループはアクセスポリシーから派生します。ポリシーごとに、ユーザーまたはグループが必須条件として設定されます。

次の図は、プレフィックス<System generated policy – App name>が付いたサンプルポリシー名を示しています。



次の図は、複数のポリシーに分割された単一のポリシーの例を示しています。



テンプレートを使用したアプリの設定

January 9, 2024

Secure Private Access サービスでのシングルサインオンによる SaaS アプリの構成は、一般的な SaaS アプリのテンプレートリストをプロビジョニングすることで簡略化されます。設定する SaaS アプリをリストから選択できます。

テンプレートには、アプリケーションの構成に必要な情報の大部分があらかじめ入力されています。ただし、顧客固有の情報は引き続き提供する必要があります。

> 注:
>
> 次のセクションでは、テンプレートを使用してアプリを構成および公開するために、Secure Private Access サービスで実行する手順を示します。アプリケーションサーバーで実行する構成手順については、次のセクションで説明します。

テンプレートを使用してアプリを構成および公開する

「**Secure Private Access** 」タイルで、「管理」をクリックします。

1. [続行] をクリックし、[アプリを追加] をクリックします。

> 注:
>
> [続行] ボタンは、ウィザードを初めて使用する場合にのみ表示されます。その後の使用では、[アプリケーション] ページに直接移動して、[アプリを追加] をクリックできます。

2. [テンプレートの選択] リストで構成するアプリを選択し、[次へ] をクリックします。
3. [アプリの詳細] セクションに次の詳細を入力し、[保存] をクリックします。

   アプリ名—アプリケーションの名前。

   アプリの説明 -アプリの簡単な説明。ここに入力するこの説明は、ワークスペースのユーザーに表示されます。

   アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128 x 128 ピクセルにする必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

   アプリアイコンを表示したくない場合は、「ユーザーにアプリケーションアイコンを表示しない」を選択します。

   URL —顧客 ID を含む URL。ユーザーはこの URL にリダイレクトされます。
   - SSO が失敗した場合、または
   - **SSO** を使用しないオプションが選択されている場合、

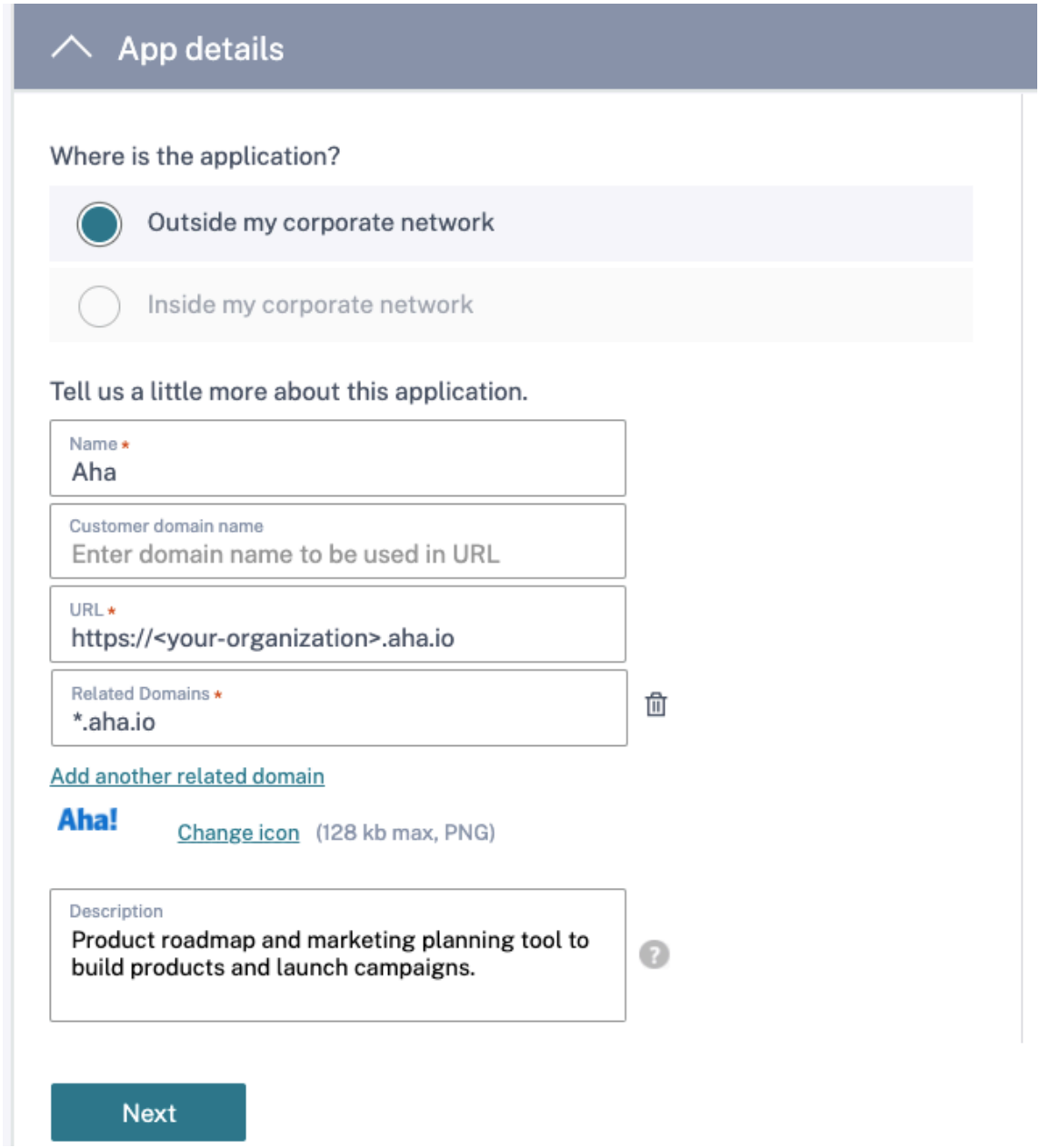
   顧客のドメイン名とカスタマードメイン **ID** -顧客のドメイン名と ID は、SAML SSO ページでアプリの URL とその他の後続の URL を作成するために使用されます。

   たとえば、Salesforce アプリケーションを追加する場合、ドメイン名は `salesforceformyorg`、ID が 123754 の場合、アプリケーション URL は `https://salesforceformyorg.my.salesforce.com/?so=123754.` です

   顧客のドメイン名と顧客 ID フィールドは、特定のアプリに固有です。

   関連ドメイン—指定した URL に基づいて、関連ドメインが自動的に入力されます。関連ドメインは、サービスが、アプリの一部として URL を識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。

   アイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128 x 128 ピクセルにする必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。



4. 次の SAML 構成の詳細を [シングルサインオン] セクションに入力し、[保存] をクリックします。

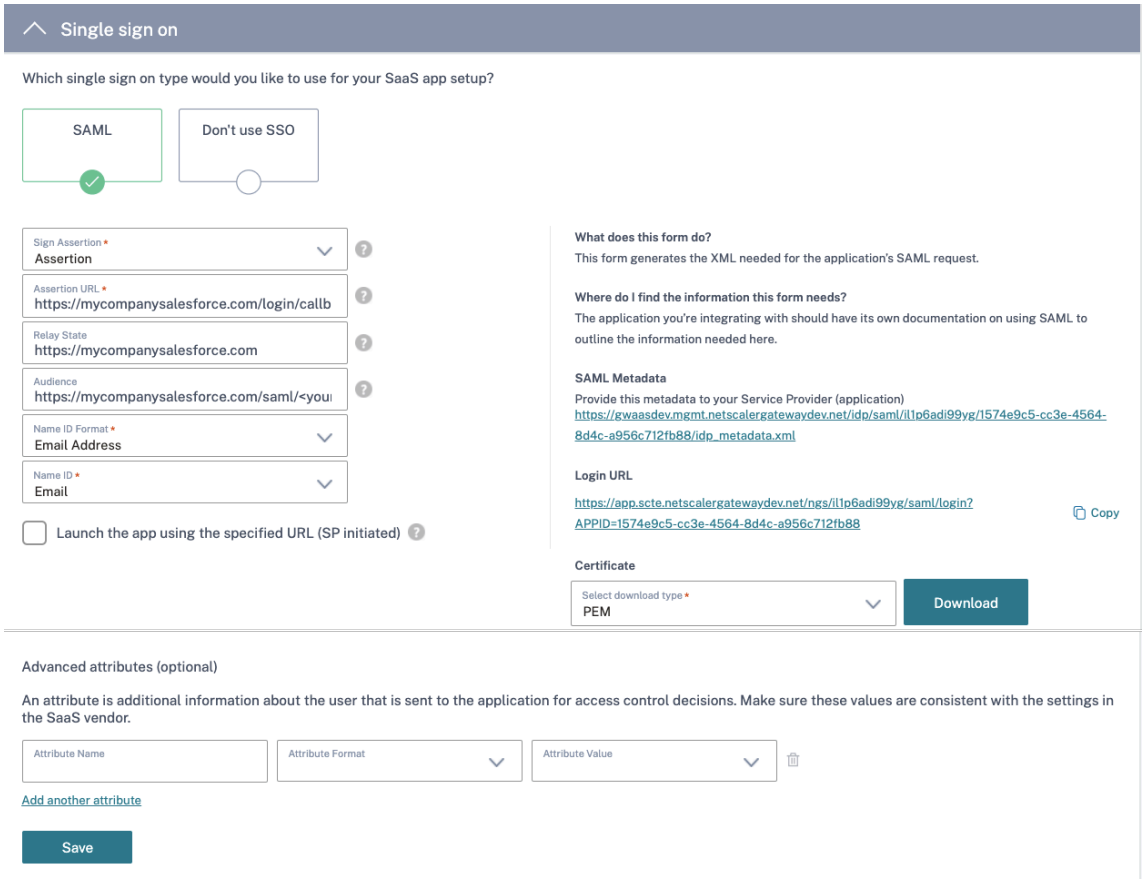
   アサーション **URL** —アプリケーションベンダーが提供する SaaS アプリケーションの SAML アサーション URL。SAML アサーションは、この URL に送信されます。

   Relay State —Relay State パラメーターは、ユーザーがサインインして証明書利用者のフェデレーションサーバーに送信された後にアクセスする特定のリソースを識別するために使用されます。リレー状態は、ユーザの 1 つの URL を生成します。ユーザーは、この URL をクリックして、ターゲットアプリケーションにログオンできます。

   対象者—アサーションの対象となるサービスプロバイダー。

   名前 **ID** 形式—サポートされているユーザーのフォーマットタイプ。

名前 **ID** —ユーザーの形式タイプの名前。



注:

SSO を使用しない] オプションを選択すると、ユーザーは [アプリの詳細] セクションで構成された URL にリダイレクトされます。

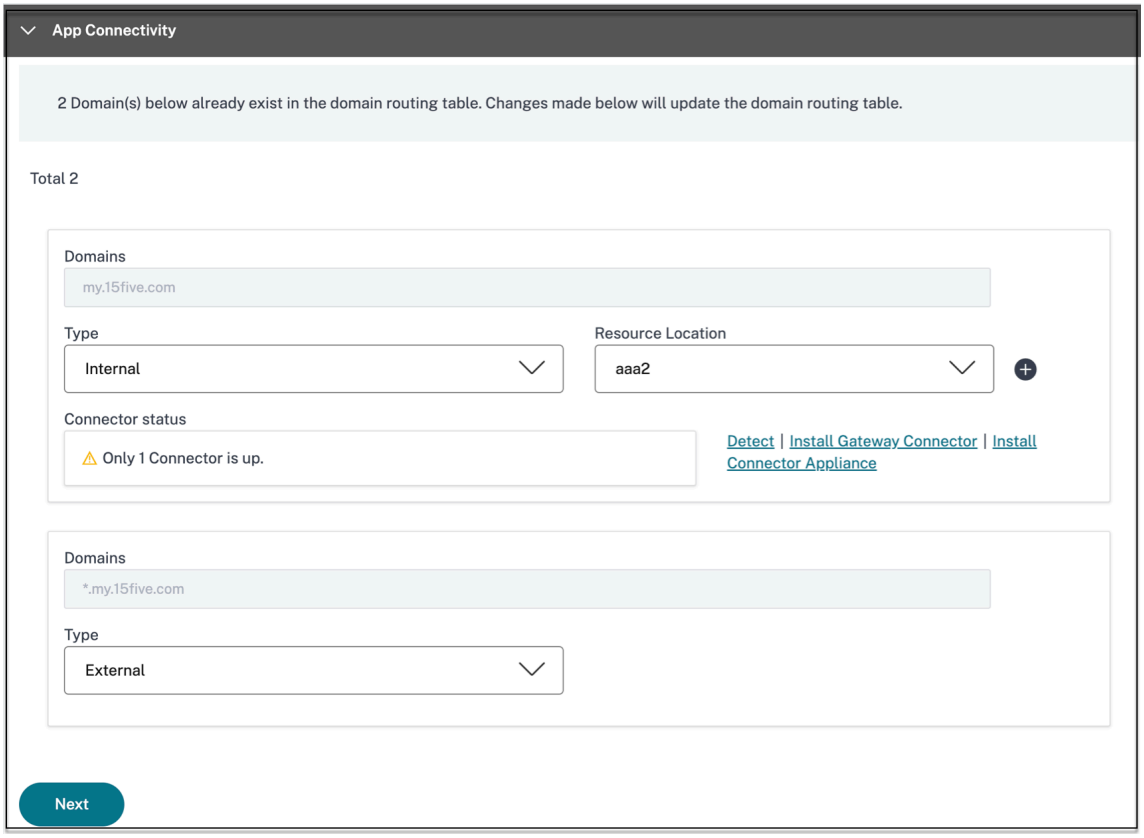
5. [**SAML** メタデータ**]** の下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaS アプリサーバーで SSO を構成します。

   注:

   - 「ログイン **URL**」の下の **SSO** ログイン **URL** をコピーし、この **URL** を **SaaS** アプリケーションサーバーで **SSO** を構成するときに使用できます。
   - 証明書の一覧から証明書をダウンロードし、**SaaS** アプリケーションサーバーで **SSO** を構成するときに証明書を使用することもできます。

6. [次へ] をクリックします

7. ドメインを Citrix ConneConnector **Appliance** 介して外部または内部でルーティングする必要がある場合は、「アプリケーション接続」セクションで、アプリケーションの関連ドメインのルーティングを定義します。詳しくは、「SaaS と Web アプリの両方の関連ドメインが同じ場合に競合を解決するためのルーティングテーブル」を参照してください。



8. 「完了」をクリックします。

   [完了] をクリックすると、アプリケーションが [アプリケーション] ページに追加されます。アプリケーションを構成した後で、アプリケーションページからアプリケーションを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

   - **[アプリケーションを編集]**
   - 削除

> 注:
>
> ユーザーにアプリへのアクセスを許可するには、管理者がアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者がアプリの利用者を追加し、セキュリティコントロールを設定します。詳細については、「アクセスポリシーの作成」を参照してください。

SaaS アプリサーバー固有の構成

January 9, 2024

以下は、テンプレートを使用してアプリサーバー固有の構成に関するガイダンスがあるドキュメントへのリンクです。

Citrix は現在、以下の SaaS アプリをサポートしており、また、さらに多くのアプリのサポートを継続して追加しています。

- 15Five -従業員をコーチするための継続的なパフォーマンス管理ツール。
- 10000 ft -成長を計画するためのプロジェクト管理ツール。
- 4me -内部、社外、および外部委託チーム間のコラボレーションのためのサービス管理ツール。
- Apacus -リアルタイムの経費報告ソフトウェア。
- Absorb -学習管理ツール。
- Accompa -製品を構築するための要件管理ツール。
- Adobe Captivate Prime -デバイス間でパーソナライズされた学習体験を提供する学習管理システム。
- Aha -製品を構築し、キャンペーンを開始するための製品ロードマップおよびマーケティング計画ツール。
- AlerTops -IT インシデントを管理するコラボレーションインシデント対応ツール。
- Allocadia -組織のマーケティング計画プロセスを管理するためのマーケティングパフォーマンス管理ツール。
  ‘
- Ana plan -データ、人、計画をつなげることで、組織の意思決定を支援する計画ツール。
- &frankly -職場の変化を促進するエンゲージメントツール。
- Anodot -時系列データを監視し、異常を検出し、リアルタイムで業績を予測する AI プラットフォーム。
- App Follow -グローバルなアプリケーションの成長を加速し、顧客ロイヤルティを高めるための製品管理ツール。
- Assembla -ソフトウェア開発のためのバージョン管理およびソースコード管理ツール。
- Automox -パッチ適用プロセスを追跡、制御、管理するためのパッチ管理ツール。
- Azendoo -チームが会話してコラボレーションするためのコラボレーションツール。
- BambooHR-従業員データを管理するための人事管理ツール 。
- Bananatag -電子メールの追跡とスケジュール、ファイルの追跡、電子メールテンプレートの作成ツール
- Base CRM -メール、電話、メモを管理する販売管理ツール。
- Beekeeper -デスクトップおよびモバイルデバイスからアクセス可能な 1 つの Secure Hub に複数の運用システムと通信チャネルを統合するツール。
- BitaBiz -休暇管理のための休暇と休暇の計画とコミュニケーションツール。
- BlazeMeter - テストスイート。
- Blissbook-従業員ハンドブックを作成するためのポリシー管理ツール 。
- BlueJeans -ビデオ会議ソリューション。

- Bold360 -カスタマーエンゲージメントのためのライブチャットツール。
- Bonusly -チームの貢献を認識するための従業員の認識と報酬管理ツール。
- Box -コンテンツを管理、共有、アクセスするためのコンテンツ管理およびファイル共有ツール。
- ブランチ - ディープリンクとモバイルを強化するモバイルリンクプラットフォーム。
- Brandfolder -デジタル資産を保存および共有するためのデジタル資産管理ツール。
- Breezy HR -リクルートソフトウェアと応募者追跡システム。
- Buddy Punch -従業員の出席状況を監視するための時間管理ツール。
- Bugsnag -アプリケーションの安定性を管理し、エラーと診断データを報告するための監視ツール。
- Buildkite -継続的インテグレーションソフトウェア開発のためのインフラストラクチャツール。
- Bullseye Locations -デバイス上の店舗またはディーラーを見つけるための店舗ロケーターツール。
- CA Flowdock - チームが会話や共同作業を行うためのコラボレーションツール。
- CakeHR-出席および業績管理のための人事管理ツール 。
- Cardboard -混乱した情報を追跡するための共同製品計画ツール。
- Citrix Cedexis -データセンター、クラウドプロバイダー、およびコンテンツ配信ネットワークのマルチベンダーソーシングを活用する大規模な Web サイト向けのトラフィック管理ツール。
- CipherCloud-クラウドベースのアプリケーションを採用する企業向けに 、エンドツーエンドのデータ保護と高度な脅威保護、包括的なコンプライアンス機能を提供するプラットフォーム。
- Celoxis -プロジェクト計画の作成、作業の自動化、コラボレーションのためのプロジェクト管理ツール。
- CircleHD -組織内でビデオやスライドを共有するためのトレーニング、学習、コラボレーションツール。
- Circonus-アラート、グラフ、ダッシュボード、機械学習インテリジェンスを提供するデータ分析および監視ツール。
- Cisco Umbrella -インターネット上の脅威に対する第一防衛線を提供するクラウドセキュリティプラットフォーム。
- Citrix RightSignature - ドキュメントを電子的に署名するためのソリューション。
- ClearSlide -ユーザーが顧客とのやり取りのためにコンテンツや販売資料を共有できるようにするセールスエンゲージメントツール。
- Cloudability -クラウド環境全体の可視性、最適化、ガバナンスを向上させるクラウドコスト管理プラットフォーム。
- CloudAMQP -プロセスと他のシステム間でメッセージを渡すためのメッセージキューツール。
- CloudCheckr —コスト管理、セキュリティ、レポート、分析ツールを使用して、AWS と Azure のデプロイを最適化できます。

- CloudMonix -クラウドおよびオンプレミスリソースのモニタリングと自動化のためのツール。
- CloudPassage -サイバーリスクを軽減し、コンプライアンスを維持するための可視性と継続的モニタリングツール。
- CloudRanger —AWS クラウドのバックアップ 、ディザスタリカバリ、サーバー制御を合理化するツール。
- Clubhouse -ソフトウェア開発のためのプロジェクト管理ツール。
- Coggle -分岐ツリーのような階層構造化されたドキュメントを作成するためのマインドマッピング Web アプリケーション。
- Comm100 -カスタマーサービスプロフェッショナル向けのカスタマーサービスソフトウェアおよびコミュニケーションツール。
- Confluence - チームのコラボレーションとナレッジの共有を支援するコンテンツコラボレーションツール。
- ConceptShare -より速く、より速く、より安価にコンテンツを配信するための校正ツール。
- Concur -外出先で経費を管理するための旅費および経費管理ツール。
- ConnectWise Control -リモートサポートとアクセスを提供するビジネス管理ツール。
- Contactzilla -最新の連絡先情報にアクセスするための連絡先管理ツール。
- ContractSafe -契約を追跡、保存、管理するための契約管理ツール。
- Contentful -コンテンツを作成、管理、および任意のプラットフォームに配信するためのコンテンツ用ソフトウェア。
- Convo -社内会話のためのチームコミュニケーションおよびコラボレーションツール。
- 銅 -CRM ツール。
- Cronitor -cron ジョブの監視ツール。
- Crowdin -開発者にシームレスで継続的なローカリゼーションを提供するソリューション。
- Dashlane -デジタルウォレットも管理するパスワード管理ツール。
- Declaree -出張のための旅費管理ツール。
- Dell Boomi -クラウドとオンプレミスのアプリケーションとデータを接続する統合ツール。
- Deskpro -チケット管理、顧客セルフヘルプ、および顧客フィードバックを容易にするヘルプデスクツール。
- Deputy -従業員の時間、タスク、コミュニケーションをスケジューリングおよび追跡するためのワークフォース管理ツール。
- DigiCert -Web サイト用の SSL 証明書の証明書管理およびトラブルシューティングツール。
- Dmarcian -スパム、マルウェア、フィッシングをフィルタリングするメール監視ツール。
- DocuSign -保険、医療、不動産などのさまざまな文書用のオンライン署名ツール。

- DOME9 ARC - パブリッククラウド環境を管理するためのセキュリティおよびコンプライアンスツール。
- Dropbox -安全なファイル共有とストレージのためのクラウドストレージツール。
- Duo -アプリケーションへの安全なアクセスを提供するセキュリティツール。
- Dynatrace -医療検査サービス。
- Easy Projects -プロジェクト管理ツール。
- EdApp -ワークスペース学習のための学習管理ツール。
- EduBrite -トレーニングプログラムを作成、提供、追跡するための学習管理ツール。
- Ekarda -電子カード設計ツール。
- Envoy -人とパッケージを管理する訪問者管理ツール。
- Evernote -メモの取り込み、整理、タスクリスト、アーカイブのためのアプリケーション。
- Expensify -経費精算書管理、領収書の追跡、出張のための経費管理ツール。
- ezeep -クラウド内の任意のデバイス、任意の場所、任意のプリンタから印刷するための印刷インフラストラクチャ管理ツール。
- EZOfficeInventory -すべての資産と機器を追跡するインベントリ管理ツール。
- EZRentOut -機器の品質と可用性を追跡するための機器レンタルツール。
- Fastly -ユーザーに近い場所にアプリケーションを提供、保護するためのエッジクラウドプラットフォーム。
- Favro -組織フローのための計画およびコラボレーションツール。
- Federated Directory -さまざまな会社の会社のアドレス帳を検索するための会社間の連絡先ディレクトリツール。
- Feeder
- Feedly -さまざまなソースからのニュースフィードをコンパイルするニュース集約ツール。
- FileCloud -堅牢で安全なファイルホスティングおよび共有プラットフォームを組織に提供するソフトウェアソリューション。
- Fivetran -アナリストがクラウドウェアハウスにデータを複製するのに役立つツール。
- Flatter Files -図面やドキュメント用のデジタルフラットファイルキャビネットで、コンテンツへのアクセスを安全かつ簡単に提供します。
- Float -プロジェクトのスケジューリングとチームの稼働率の管理のためのリソース計画ツール。
- Flock -コラボレーションツール。
- Formstack -オンラインフォームビルダおよびデータ収集ツール。
- FOSSA -CI/CD にネイティブに組み込まれている自動化されたオープンソースライセンススキャンおよび脆弱性管理ツール。

- Freshdesk -顧客のニーズをサポートするためのカスタマーサポートツール。
- Freshservice -IT 運用を簡素化する IT ヘルプデスクツール。
- FrontApp -すべての会話を 1 か所で管理するコラボレーションツール。
- Frontify -日々のブランディング、マーケティング、開発業務を促進し、合理化するプラットフォーム。
- Fulcrum -モバイルフォームを簡単に作成してデータを収集できるモバイルデータ収集プラットフォーム。
- Fusebill -請求管理と定期的な請求ソフトウェア。
- G-Suite -社内の人々をつなぐインテリジェントなアプリのセット。
- GetGuru - ナレッジ管理ソフトウェア。
- GitBook -ドキュメントを作成し、維持するためのツール。
- GitHub -企業のファイアウォールの内側でホストされているリポジトリに Git を使用する、バージョン管理のための Web ベースのホスティングサービス。
- GitLab -完全な DevOps プラットフォームで、単一のアプリケーションとして提供されます。
- GlassFrog -Holacracy プラクティス用のソフトウェア。
- GoodData -高速で信頼性が高く、使いやすいアナリティクスを提供する組み込み BI および分析プラットフォーム
- GoToMeeting -HD ビデオ会議機能を備えたオンライン会議ソフトウェア。
- HackerRank -消費者や企業に競争力のあるプログラミングの課題を提供します。
- HappyFox -オンラインヘルプデスクソフトウェアおよび Web ベースのサポートチケットシステム。
- Helpjuice -ナレッジベースを作成し、維持するためのナレッジ管理ソリューション。
- Help Scout -カスタマーサービスプロフェッショナル向けのカスタマーサービスソフトウェアおよびナレッジベースツール。
- Hello sign -電子署名インターフェイスにより、いつでも、どこからでも、どのデバイスからでも署名できます。
- HelpDocs-ユーザーが立ち往生したときにガイドするナレッジベースソフトウェア。
- Honeybadger -アプリケーションのヘルス監視ツール。
- Harness -Java、AWS、GCP、Azure、ベアメタルの.NET アプリケーションの継続的デリバリーと統合のためのツール。
- HelpDocs -ユーザーが行き詰まったときにガイドする信頼できるナレッジベースを作成するツール。
- Helpmonks -チームコラボレーションのためのコラボレーティブなメールプラットフォーム。
- Hoshinplan -戦略計画を視覚化し、1 つのキャンバスでステータスを追跡するツール。

- Hosted Graphite -Web サイト、アプリ、サーバー、コンテナのパフォーマンスを監視するツール。
- Humanity -シフト、スケジュール、給与、タイムクロックを管理するオンライン従業員スケジューリングソフトウェア。
- Igloo -組織全体の IT 課題を解決するデジタルワークプレースおよびイントラネットソリューションプロバイダー。
- iLobby -クラウドベースの訪問者登録管理ソリューション。
- Illumio -データセンターおよびクラウド環境内での侵害の拡散を防ぐためのセキュリティシステム。
- Image Relay -デジタルファイルを安全に整理して共有するためのデジタル資産管理およびブランド管理ソフトウェア。
- Informatica -SaaS アプリ統合ツール、およびカスタム統合サービスを開発および展開するためのプラットフォーム。
- Intelligent contract -契約管理ソフトウェア。
- iMeet Central -マーケティング担当者、クリエイティブエージェンシー、エンタープライズビジネス向けのプロジェクト管理ソフトウェア。
- InteractGo -システムパフォーマンスに関するリアルタイムおよび履歴データを測定するツール。
- iQualify One -本物の学習体験を提供する学習および管理ツール。
- InsideView - 販売、マーケティング、その他のビジネス上の課題を解決するためのデータおよびインテリジェンスソリューション。
- Insightly -中小規模企業向けのクラウドベースの顧客関係管理 (CRM) およびプロジェクト管理ツール。
- ITGlue -MSP によるドキュメントの標準化、ナレッジベースの作成、パスワードの管理、デバイスの追跡を支援するクラウドベースの IT ドキュメントプラットフォームです。
- Jitbit -受信したサポートリクエストメールとその関連チケットを管理および追跡するためのヘルプデスクソフトウェアおよびチケット発行システム。

JupiterOne -セキュリティプロセス全体を作成および管理するためのソフトウェアプラットフォーム。

- Kanbanize -リーン管理のためのオンラインポートフォリオかんばんソフトウェア。
- Klipfolio -チームやクライアント向けの強力なリアルタイムビジネスダッシュボードを構築するためのオンラインダッシュボードプラットフォーム。
- Jira -課題やプロジェクトを計画、追跡、管理するためのツール。
- Kanban Tool -チームのパフォーマンスを向上させ、生産性を向上させるビジュアル管理ソフトウェア。
- Keeper Security -パスワードと個人情報を保護するパスワードマネージャーとセキュリティソフトウェア。
- Kentik -ネットワークとパフォーマンスの監視、DDoS 保護、リアルタイムのアドホックネットワークフロー分析にビッグデータを適用するツール。

- Kissflow -ワークフロープロセスを自動化するためのワークフローツールとビジネスプロセスワークフロー管理ソフトウェア。
- KnowBe4 -セキュリティ意識向上トレーニングとフィッシングのシミュレーションを提供するツール。
- knowledGeowl -ナレッジベースとオーサリングツール。
- Kudos -小売、ジョブ、プロジェクト、およびフルフィルメントのプロセスシステム。
- LaunchDarkly -開発チームと運用チームが機能のライフサイクルを制御できるようにする機能管理プラットフォーム。
- Lifesize -ビデオ会議ソリューション。
- Litmos -従業員トレーニング、カスタマートレーニング、コンプライアンストレーニング、パートナートレーニングのための学習管理システム。
- LiquidPlanner -あなたのビジネスのためのオンラインプロジェクト管理ソフトウェア。
- LeanKit -リーンベースのエンタープライズプロセスおよび作業管理ソフトウェアで、企業が作業を視覚化し、プロセスを最適化し、より迅速に配信できるようにします。
- LiveChat -企業向けのライブチャットおよびヘルプデスクソフトウェア。
- LogDNA -1 つの集中ログツールですべてのソースからログを収集、監視、解析、分析するツール。
- Mango -サイロ化されたアプリケーションを 1 つのプラットフォームに統合して合理化するチームコラボレーションソフトウェア。
- Manuscript -作業の計画、編集、共有に役立つライティングツール。
- Marketo -マーケティングチームがデジタルマーケティングの芸術と科学を習得するのに役立つ自動化ソフトウェア。
- Matomo -Web サイトを訪問したすべての人のユーザージャーニー全体を評価する Web 分析プラットフォーム。
- Meisterplan -組織がプロジェクトポートフォリオを作成するのに役立つソフトウェア。
- Mingle -チーム全体に統合された職場を提供するアジャイルなプロジェクト管理およびコラボレーションツールです。
- MojoHelpDesk -ヘルプデスクソフトウェアとチケットシステム。
- Monday -すべての作業を 1 つのツールで計画、追跡、共同作業するためのチーム管理ソフトウェア。
- Mixpanel -Web やモバイルとのユーザーインタラクションを追跡するシステム。
- MuleSoft -クラウドとオンプレミスで SaaS とエンタープライズアプリケーションを接続するための統合ソフトウェア。
- MyWebTimeSheets -さまざまなプロジェクト/ジョブ/アクティビティに費やされた時間を追跡するオンライン時間追跡システム。

- New Edge -ハイブリッド IT 向けのセキュアなアプリケーションネットワーキングサービス。
- NextTravel -企業旅行管理ソフトウェアツール。
- N2F -あなたのビジネスと旅費を管理するための経費報告書管理ツール。
- New Relic -アプリケーションとインフラストラクチャのパフォーマンスを測定および監視するデジタルインテリジェンスプラットフォーム。
- Nmbrs -企業向けのクラウド人事および給与計算ソフトウェア。
- Nuclino -リアルタイムでコラボレーションして情報を共有するコラボレーションソフトウェア。
- Office365 -Microsoft のクラウドベースのサブスクリプションサービス。
- OfficeSpace -組織がワークスペースを割り当てるのに役立つクラウドベースのプラットフォーム。
- OneDesk -顧客とつながり、顧客をサポートするためのプロジェクト管理およびヘルプデスクソフトウェア。
- OpsGenie -DevOps および IT Ops チーム向けのインシデント管理プラットフォームで、アラートとインシデント解決プロセスを合理化します。
- Orginio -組織構造を視覚化するためのオンライン組織図作成ツール。
- Oomnitza -資産を追跡および管理するための IT 資産管理プラットフォームソリューション。
- OpenEye -Apex レコーダーでライブビデオと録画ビデオを表示するためのモバイルアプリ。
- Oracle ERP Cloud -エンタープライズ機能を管理するためのクラウドベースのソフトウェア・アプリケーション・スイート。
- Pacific Timesheet -給与、プロジェクト時間、経費用の Web ベースのタイムシートツール。
- PagerDuty -デジタル運用管理システム。
- PandaDoc -iPhone ユーザー向けのモバイルアプリで、ドキュメント、分析、ダッシュボードに携帯電話で直接アクセスできます。
- Panopta -インフラストラクチャ監視ツール。
- Panorama9 -エンタープライズネットワーク監視用のクラウドベースの IT 管理プラットフォーム。
- Papyrs -独自のイントラネットページをデザインするためのエディター。
- ParkMyCloud -AWS、Azure サービス、または GCP に接続するための単一目的の SaaS ツール。
- Peakon -従業員のエンゲージメントを測定し、改善するためのツール。
- People HR-すべての主要な人事機能のための人事ソフトウェアシステム。
- Pingboard -チームと要員計画を整理するための組織図を作成するためのツール。
- Pigeonhole Live -インタラクティブな Q&A プラットフォーム。
- Pipedrive -セールス CRM およびパイプライン管理ソフトウェア。

- PlanMyLeave -従業員の休暇を管理および追跡するための休暇管理システム。
- PlayVox -カスタマーサービス品質監視ツール。
- Podbean -ポッドキャストサービスプロバイダー。
- Podio -プロジェクト管理ワークスペース内のチームコミュニケーション、ビジネスプロセス、データ、コンテンツを整理するための Web ベースのツール。
- PoPin -問題解決のためのチームエンゲージメントを運用するクラウド解決プラットフォームとモバイルアプリ
- Postman -API 開発環境。
- Prescreen -オンラインとオフラインで求人情報を公開する応募者追跡ツール。
- ProductBoard -製品管理ツール。
- ProdPad -製品戦略を開発するための製品管理ソフトウェア。
- Proto.io -完全にインタラクティブで忠実度の高いプロトタイプを作成するためのアプリケーションプロトタイピングプラットフォーム。
- Proxyclick -訪問者を管理し、ブランドイメージを構築し、セキュリティを確保するためのクラウドベースの訪問者管理ソリューション。
- Pulumi -コンテナ、サーバーレス、インフラストラクチャ、Kubernetes 向けのクラウドネイティブ開発プラットフォーム。
- PurelyHR -従業員の休暇データにアクセスするための休暇管理ツール。
- Promapp - ビジネスプロセス管理（BPM）ツール。
- Prescreen - オンラインとオフラインで求人情報を公開するクラウドベースの応募者追跡システム。
- QAComplete - ソフトウェアテスト管理ツール。
- Qualaroo -顧客から洞察を得るためのフィードバックツール。
- Quality Built, LLC - 信頼性の高い革新的なサードパーティ品質保証サービスを提供する保険、金融、建設産業。
- Qubole -Amazon で構築されたビッグデータ分析のためのセルフサービスプラットフォーム。
- Questetra BPM Suite -ルーチンワークフローのための Web ベースのビジネスプロセスプラットフォーム。
- QuestionPro -アンケートやアンケートを作成するためのオンラインアンケートソフトウェア。
- Quandora -質問と回答ベースのナレッジ管理ソリューション。
- Quip -モバイルおよび Web 用の共同生産性ソフトウェアスイート。
- Rackspace -マネージド・クラウド・コンピューティング・サービス。
- ReadCube -Web、デスクトップ、およびモバイルのリファレンス管理のためのツール。

- RealtimeBoard -組織がフォーマット、ツール、場所、タイムゾーンを超えてコラボレーションするためのホワイトボードコラボレーションツールです。
- Receptive -顧客、チーム、市場からのフィードバックを 1 か所で収集するツール。
- Remedyforce -IT サービス管理およびヘルプデスクシステム。
- Retrace -バグ追跡、データ集約、自動アラートを提供するアプリケーションパフォーマンス管理ツール。
- Robin -会議の会議室やデスクの予約をスケジュールするためのワークプレイス・エクスペリエンス・ツール。
- Rollbar -開発者向けのリアルタイムのエラーアラートおよびデバッグツール。
- Really Simple Systems -中小企業が販売とマーケティングを管理するためのクラウドベースの CRM ソフトウェア。
- Reamaze -単一のプラットフォームでチャット、ソーシャル、SMS、FAQ、メールで顧客をサポート、エンゲージメント、変換するためのカスタマーサポートソフトウェア。
- Resource Guru -人、機器、およびその他のリソースをスケジュールするためのリソース管理ソフトウェア。
- Retrace-コードプロファイリング、エラー追跡、アプリケーションログ、およびメトリックを統合するアプリケーションパフォーマンス管理。
- Roadmunk -製品ロードマップを作成するための製品ロードマップソフトウェアおよびロードマップツール。
- Runscope -機能 API テストとモニターを作成、管理、実行するためのツール。
- Salesforce —顧客の連絡先情報を管理し、ソーシャルメディアを統合し、リアルタイムの顧客コラボレーションを促進する CRM ツールです。
- SalesLoft -売上を効率的かつ増収するためのセールスエンゲージメントプラットフォーム
- Salsify -製品エクスペリエンス管理 (PXM) プラットフォーム。
- Samanage -IT サービス管理のためのツール。
- Samepage -オンラインプロジェクトを管理するコラボレーションソフトウェア。
- Screencast-O-Matic —ビデオをスクリーンキャストして編集するためのツール。
- ScreenSteps —スクリーンキャプチャを中心とするビジュアルドキュメントを作成するツール。
- SendSafely —ファイルとメールの安全な交換のための暗号化プラットフォーム。
- Sentry -オープンソースのエラー追跡ソフトウェア。
- ServiceDesk Plus -IT サービスデスクのためのツール。
- ServiceNow -デジタルワークフローを作成するためのクラウドプラットフォーム。
- SharePoint - ドキュメントの管理と保存に使用されるコラボレーションプラットフォーム。
- Shufflrr -プレゼンテーションを作成、更新、共有、ブロードキャストするためのプレゼンテーション管理ツール。

- Sigma Computing —データの探索、分析、視覚化を行う分析ツールです。
- Signavio —ビジネスプロセスモデリングツール。
- Skeddly -AWS リソースを自動化するためのツール。
- Skills Base -従業員のパフォーマンスとスキルを追跡および文書化するタレント管理ツール。
- Skyprep -顧客と従業員を訓練するための学習管理システム (LMS)。
- Slack -情報を伝え、共有するためのコラボレーションツール。
- Slemma -複数のデータセットからデータレポートを作成するためのデータ分析ツール。
- Sli.do -ミーティング、イベント、および会議のためのインタラクションツール。
- SmartDraw -フローチャート、組織図、マインドマップ、プロジェクトチャート、およびその他のビジネスビジュアルを作成するために使用されるダイアグラムツール。
- SmarterU -顧客と従業員をトレーニングするための学習管理システム (LMS)。
- Smartsheet -タスクの割り当て、プロジェクトプロセスの追跡、カレンダーの管理、ドキュメントの共有を行うコラボレーションツール。
- SparkPost - メール配信サービス。
- Split -ビル分割アプリケーション。
- Spoke -サービスチケットをファイルするサービスデスクツール。
- Spotinst -企業がクラウドインフラストラクチャの容量を購入および管理するのに役立つ SaaS 最適化プラットフォーム。
- SproutVideo -ビジネスビデオをホストするプラットフォーム。
- Stackify -Prefix と Retrace を含む一連のツールをサポートするトラブルシューティングツール。
- StatusCast -従業員と顧客にダウンタイムと Web サイトのメンテナンスについて知らせるホストされたページ。
- StatusDashboard-ステータスダッシュボードをホストし 、顧客にインシデント通知をブロードキャストするためのコミュニケーションプラットフォーム。
- Status Hero -チームからのステータスの更新と毎日の目標を追跡するためのツール。
- StatusHub -サービス状態ページをホストするプラットフォーム。
- Statuspage -ステータスとインシデントを通信するツール。
- SugarCRM -Salesforce オートメーション、マーケティングキャンペーン、カスタマーサポート、コラボレーション、モバイル CRM、ソーシャル CRM、およびレポートのための CRM ツール。
- Sumo Logic -セキュリティ、運用、BI ユースケースに重点を置いたデータ分析ソフトウェア。
- Supermood -従業員のフィードバックをリアルタイムで収集する人事プラットフォーム。

- Syncplicity -ファイルを共有および同期するためのツール。
- Tableau -インタラクティブなデータビジュアライゼーションを作成するツール。
- TalentLMS -オンラインセミナー、コース、およびその他のトレーニングプログラムを促進する学習管理システム（LMS）。
- Tallie —領収書のキャプチャとアップロード、経費精算書の生成、経費詳細のカスタマイズを行うツール。
- Targetprocess -スクラム、かんばん、SAFe などへのアジャイルプロジェクト管理ソフトウェア。
- Teamphoria -リアルタイムの従業員エンゲージメント指標、従業員レビュー、認知度を提供するソフトウェア。
- TeamViewer -リモートコントロール、デスクトップ共有、オンラインミーティング、Web 会議、コンピュータ間のファイル転送のための独自のソフトウェアアプリケーション。
- Tenable.io -IT 環境における脆弱性や設定ミスの特定、調査、修復の優先順位付けを行うためのデータを提供するツール。
- Testable -行動実験や調査を作成するためのツール。
- TestingBot -ライブおよび自動テスト用のさまざまなブラウザバージョンを提供するツール。
- TestFairy -モバイルセッションのビデオ録画、ログ、クラッシュレポートを企業に提供するモバイルテストプラットフォーム。
- TextExpander -入力時に電子メールのリポジトリやその他のコンテンツからテキストのスニペットを挿入するコミュニケーションツール。
- TextMagic -顧客とつながるメッセージングサービス。
- ThousandEyes -ネットワークインフラストラクチャの監視、アプリケーション配信のトラブルシューティング、およびインターネットパフォーマンスのマッピングを行うツール。
- Thycotic Secret server -パスワードを管理するためのアカウント管理ソフトウェアツール。
- TimeLive —タイムシートを提供し、時間を追跡するツール。
- Tinfoil Security -脆弱性をチェックするためのセキュリティソリューションソフトウェア。
- Tisotech -顧客がデジタルエンタープライズを発見、モデル化、分析できるようにするツール。
- Trumba -オンライン、インタラクティブ、イベントのカレンダーを公開するためのツール。
- TwentyThree -動画をマーケティングスタックに統合して追加する動画マーケティングプラットフォーム。
- Twilio -コミュニケーションのための開発者プラットフォーム。
- Ubersmith -使用量ベースの請求、見積り、注文管理、インフラストラクチャ管理、ヘルプデスクチケット発行ソリューション用のビジネス管理ソフトウェア。
- UniFi -音声、Web コラボレーション、ビデオ会議機能を備えたコミュニケーションおよびコラボレーションソフトウェア。

- UPTRENDS —Web サイトの稼働時間とパフォーマンスを追跡する Web サイト監視ソリューション。
- UserEcho -企業が顧客からのフィードバックを管理するのに役立つコミュニティフォーラムツール。
- UserVoice -企業がデータドリブンな製品決定を下せるようにする製品フィードバック管理ソフトウェア。
- VALIMAIL -正当な電子メールを認証し、フィッシング攻撃をブロックする電子メール認証ソフトウェア。
- Veracode -ソースコードアナライザとコードスキャナは、サイバー脅威やアプリケーションのバックドアから企業を保護します。
- Velpic -職場のトレーニングを合理化するために設計された学習管理システム（LMS）。
- VictorOps -DevOps の可観測性、コラボレーション、リアルタイムアラートを提供するインシデント管理ソフトウェア。
- VIDIZMO -エンタープライズライブおよびオンデマンドのビデオストリーミングソフトウェア。
- Visual Paradigm -チームコラボレーションのためのビジュアルモデリングおよびダイアグラム作成オンラインプラットフォーム。
- Vtiger -営業、サポート、マーケティングの各チームが組織化およびコラボレーションできるようにする CRM ツール。
- WaveMaker —カスタム App を構築および実行するためのソフトウェア。
- Weekdone -企業のマネージャーのダッシュボードとチーム管理サービスを作成するためのツール。
- Wepow -モバイルおよびビデオ面接ソリューションを通じて、採用担当者、求職者、雇用者をつなぐツール。
- When I Work -従業員のスケジューリングと時間追跡のためのツール。
- WhoSonLocation —サイトやゾーンを通る人の流れを追跡するツール。
- Workable -申請者追跡システム。
- Workday -財務管理、人事、および計画のためのツール。
- Workpath -組織の目標とパフォーマンスを管理するためのツール。
- Workplace -Facebook によるコラボレーションツールで、従業員が使い慣れたインターフェイスを通じてコミュニケーションできるようにします。
- Workstars -ソーシャルおよびピアの従業員認識プログラムのためのプラットフォーム。
- Workteam -従業員の時間と出勤を追跡するツール。
- Wrike -ソーシャルプロジェクト管理およびコラボレーションソフトウェア。
- XaitPorter -入札や提案、その他のビジネス文書用の文書共同編集ソフトウェア。
- Ximble -従業員のスケジューリングと時間追跡のためのツール。
- XMatters -シームレスなプロセスと効果的なコミュニケーションを作成する他のツールと統合するアラートソフトウェアを備えたコラボレーションプラットフォーム。

- Yodeck -Web またはモバイルを介して、リモートで画面を管理するためのツール。
- Zendesk -カスタマーサービスを要求し、サポートチケットを記録するためのソフトウェア。
- Ziflow -クリエイティブ制作チームのためのツール。
- Zillable —コミュニケーション機能を備えたコラボレーションプラットフォーム。
- Zing tree -インタラクティブなデシジョンツリーとトラブルシューティングツールを作成するためのツールキット。
- ZIVVER -使い慣れた電子メールプログラムからの安全な電子メールおよびファイル転送を可能にするツール。
- Zoho -ビジネスアプリケーションスイート。
- Zoom -音声、Web コラボレーション、ビデオ会議機能を備えたコミュニケーションおよびコラボレーションソフトウェア。
- Zuora -会社の立ち上げ、管理、サブスクリプションビジネスへの転換を可能にするサブスクリプションベースのソフトウェア。

構成済みアプリの起動 - エンドユーザーのワークフロー

January 9, 2024

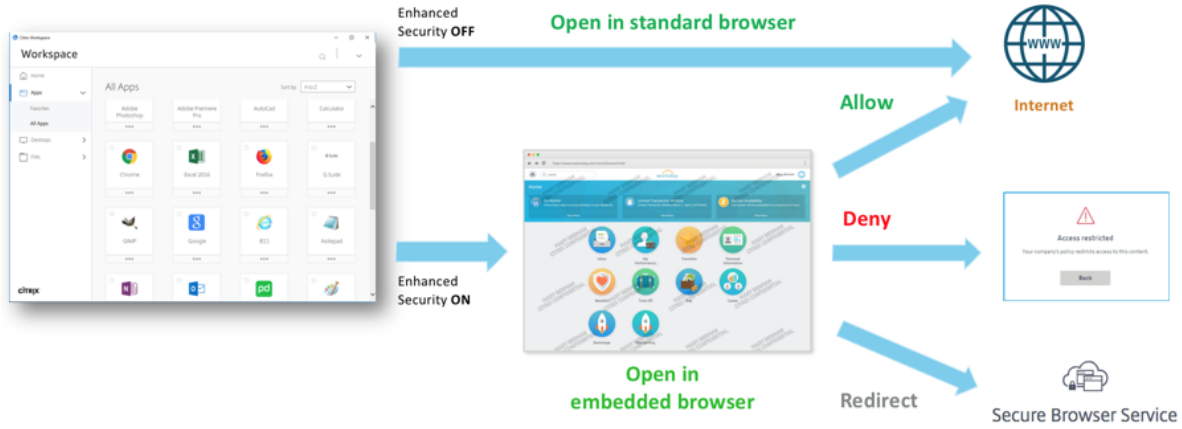
エンドユーザーは、次の操作を行う必要があります:

1. Citrix Workspace アプリをhttps://www.citrix.com/downloadsからダウンロードします。［**Downloads**］のリストから、［**Citrix Workspace app**］を選択します。
2. ログオンし、使用する SaaS アプリを検索します。アプリをクリックして起動します。

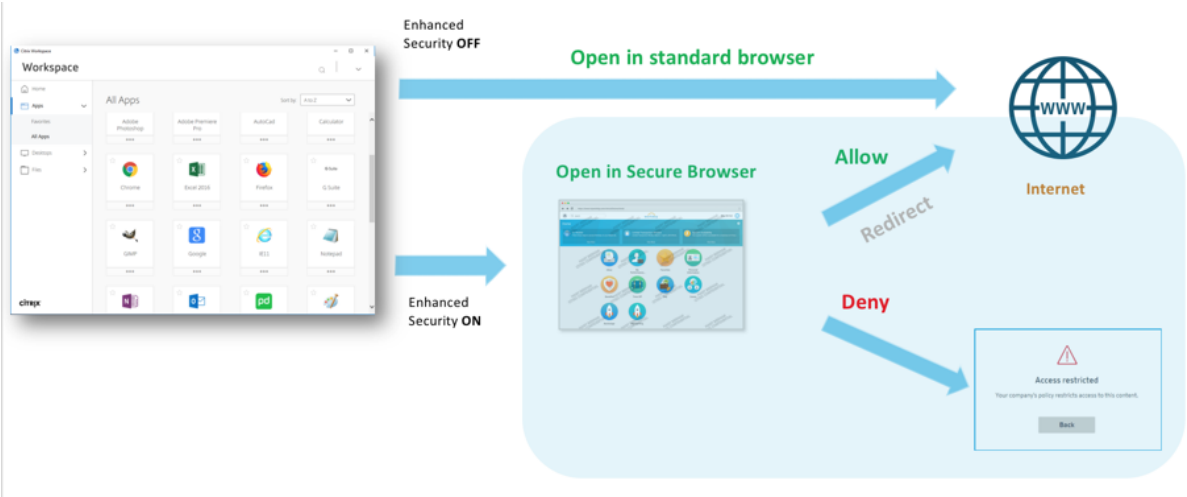
Citrix Workspace アプリ内または Citrix Workspace Web ポータルから SaaS アプリを使用できるようになりました。

管理者が構成した設定に応じて、SaaS アプリは Workspace アプリ内のブラウザーエンジンを使用して開くか、セキュリティで保護されたブラウザーにリダイレクトされます。

次の図は、Citrix Workspace アプリの基本フローを示しています。



次の図は、Citrix Workspace Web ポータルの基本フローを示しています。



管理者の **SaaS** および **Web** アプリへの読み取り専用アクセス

January 9, 2024

組織は通常、複数の管理者で構成され、管理者にはさまざまなレベルのアクセス権限を付与する必要があります。Secure Private Access サービスを使用するセキュリティ管理者チームは、管理者への読み取り専用アクセスなどのきめ細かな制御を提供できます。アプリを追加または変更しない管理者は、アプリの詳細を表示するための読み取り専用アクセスを提供できます。読み取り専用アクセス権を持つ Secure Private Access サービス管理者は、次のタスクを実行できません。

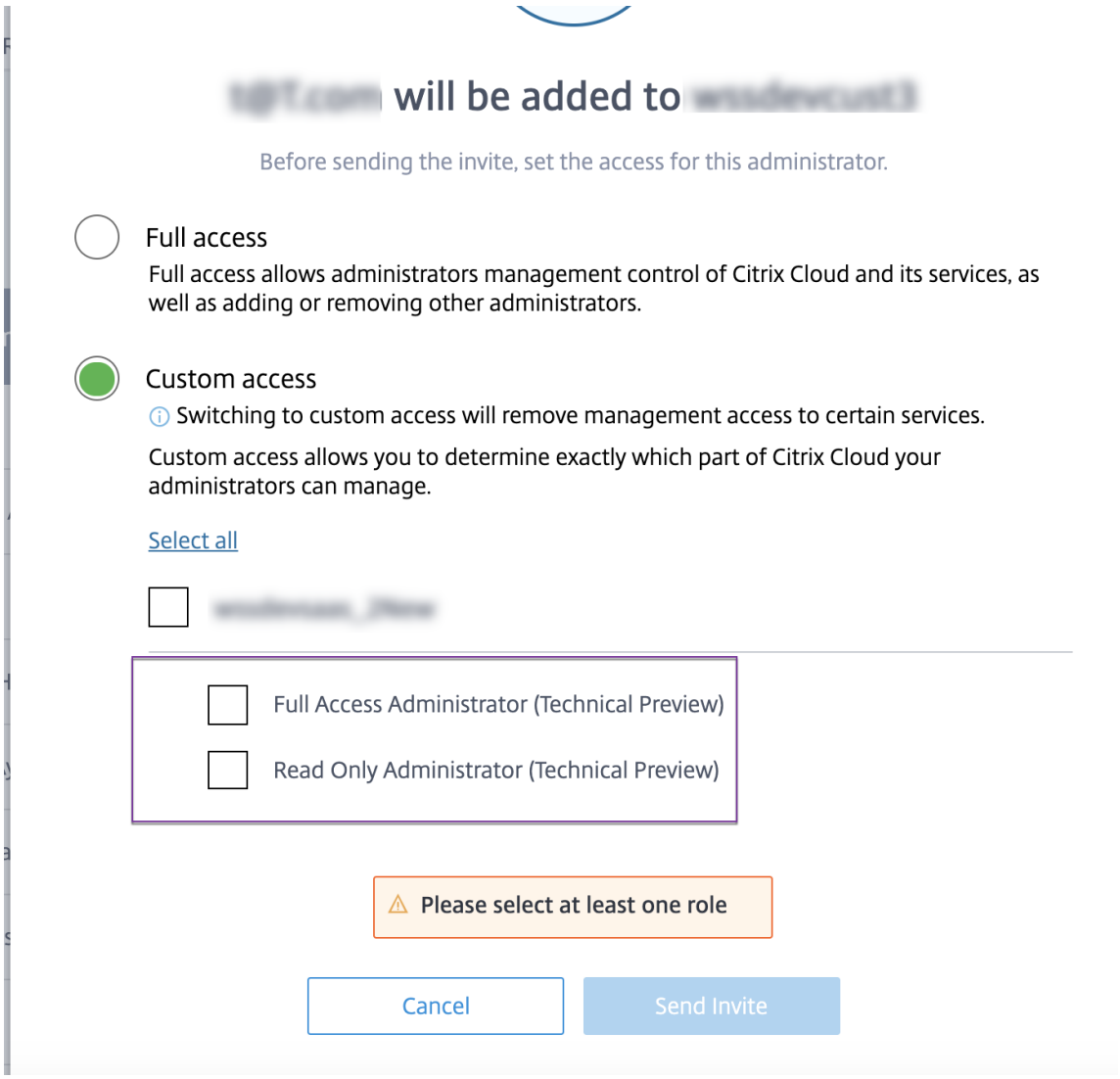
- エンタープライズ Web アプリまたは SaaS アプリを追加します。
- 既存または新規のリソースロケーションに新しいコネクタアプライアンスを追加します。

管理者に読み取り専用アクセスを提供する方法

Citrix Cloud にサインイン後、メニューで ［**ID** およびアクセス管理］を選択します。
[ID とアクセス管理] ページで、[管理者] をクリックします。コンソールに、アカウント内の現在の管理者全員が表示されます。

読み取り専用アクセス権を持つ管理者の追加

1. ［追加する管理者］で、管理者の選択先となる ID プロバイダーを選択します。Citrix Cloud では、最初にアイデンティティプロバイダー（Azure Active Directory など）にサインインするように求めるメッセージが表示されることがあります。
2. **Citrix Identity** を選択した場合は、ユーザーのメールアドレスを入力し、「招待」をクリックします。
3. Azure Active Directory を選択した場合は、追加するユーザーの名前を入力して［招待］をクリックします。
4. ［カスタムアクセス］を選択します。次のオプションが表示されます。
   - フルアクセス管理者の選択 **(**テクニカルプレビュー**)** —フルアクセスを提供します。
   - 読み取り専用管理者 **(**テクニカルプレビュー**)** —読み取り専用アクセスを提供します。
5. 読み取り専用管理者 **(**テクニカルプレビュー**)** を選択します。

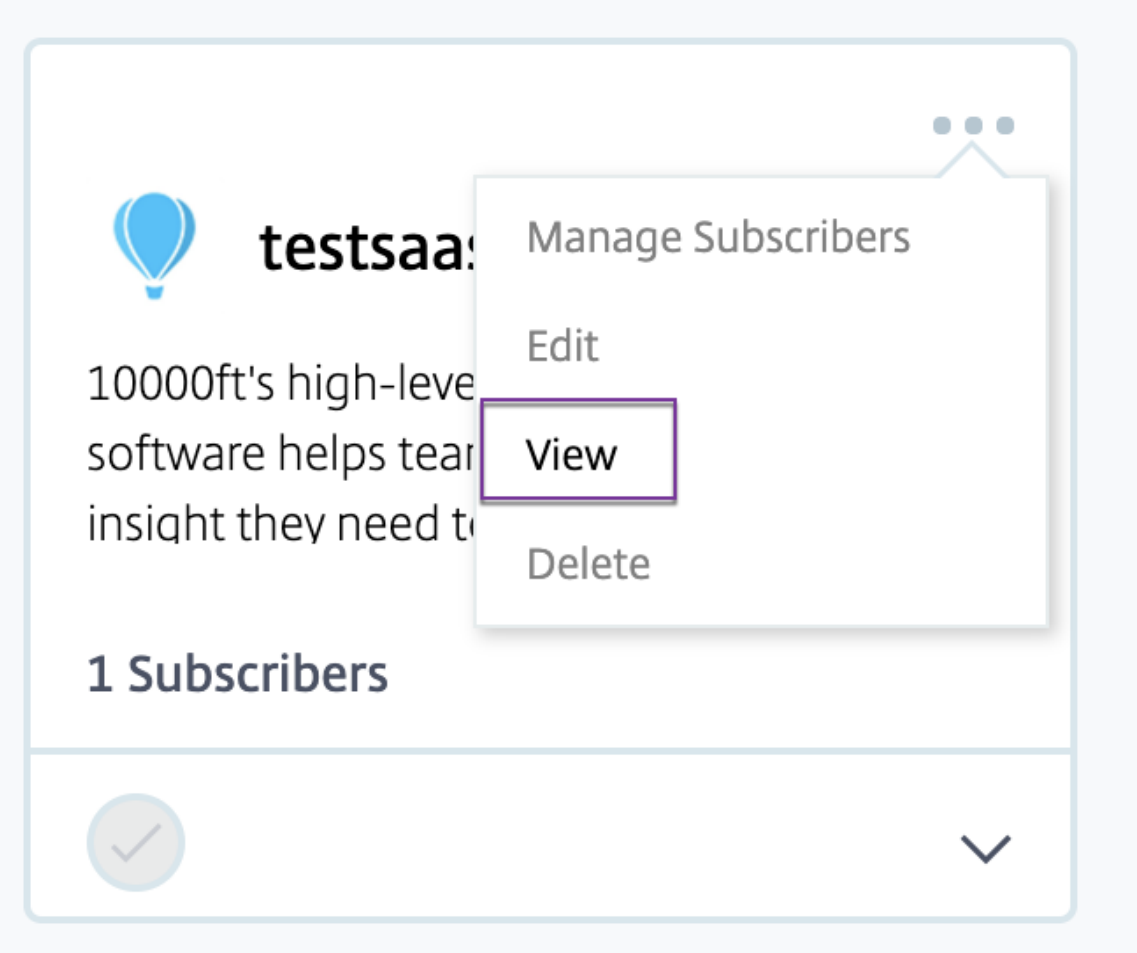


6. [招待を送信する] をクリックします。

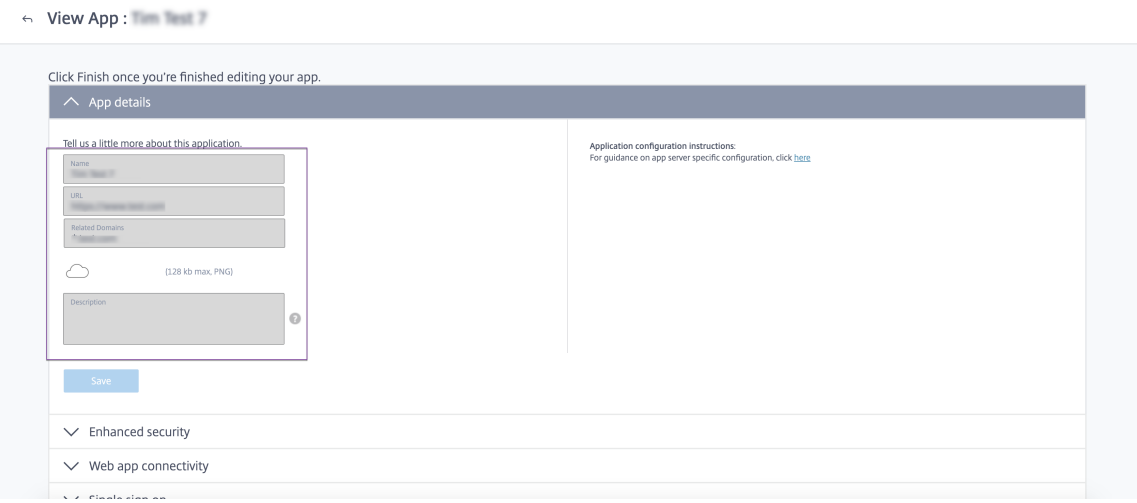
> 重要:
>
> - Citrix Gateway **Service** 管理者に読み取り専用管理者アクセスを提供する場合は、それらの管理者の [全般管理] リストから [ライブラリ] を有効にする必要があります。管理者に対してのみ、アプリの [表示] オプションが有効になります。
> - 読み取り専用管理者アクセス権を持つユーザーの場合、**[Web/SaaS** アプリケーションの追加] ボタンは無効になります。

管理者が読み取り専用アクセス権を持っているときにアプリの詳細を表示するには

1. Citrix Cloud にサインインした後、メニューから [ライブラリ] を選択します。
2. 詳細を表示するアプリを選択し、省略記号をクリックします。
   [表示] オプションのみが有効になります。その他のオプションはすべて無効になります。



3. [表示] をクリックします。



Web および SaaS アプリケーション構成のベストプラクティス

June 19, 2024

公開アプリと非公開アプリへのアプリケーションアクセスは、Secure Private Access サービス内で設定されているアプリケーションとアクセスポリシーによって異なります。

公開アプリと未公開アプリへの Secure Private Access 内のアプリケーションアクセス

- 公開されている **Web** アプリケーションおよび関連ドメインへのアクセス**:**
  - 公開されているウェブアプリに関連付けられた FQDN にエンドユーザーがアクセスする場合、アクセスポリシーがユーザーの [許可] または [制限付き許可] アクションで明示的に設定されている場合のみ、アクセスが許可されます。

    > 注**:**
    >
    > 完全に一致させるには、複数のアプリケーションで同じアプリケーション URL ドメインまたは関連ドメインを共有しないことをお勧めします。複数のアプリが同じアプリケーション URL ドメインまたは関連ドメインを共有している場合、完全な FQDN の一致とポリシーの優先順位に基づいてアクセスが提供されます。詳細については、「アクセスポリシーの照合と優先順位付け」を参照してください。

  - 公開アプリと一致するアクセスポリシーがない場合、またはアプリがどのアクセスポリシーにも関連付けられていない場合、アプリへのアクセスはデフォルトで拒否されます。アクセスポリシーについて詳しくは、「アクセスポリシー」を参照してください。
- 未公開の内部 **Web** アプリケーションおよび外部インターネット **URL** へのアクセス**:**

  ゼロトラストを有効にするために、Secure Private Access は、アプリケーションに関連付けられておらず、アプリケーションにアクセスポリシーが設定されていない内部 Web アプリケーションまたはイントラネット URL へのアクセスを拒否します。特定のユーザーにアクセスを許可するには、イントラネット Web アプリケーション用にアクセスポリシーが設定されていることを確認してください。

  Secure Private Access 内のアプリケーションとして設定されていない URL の場合、トラフィックはインターネットに直接流れます。

  - このような場合、イントラネット Web アプリケーション URL ドメインへのアクセスは直接ルーティングされるため、アクセスは拒否されます (ユーザーが既にイントラネット内にいる場合を除く)。
  - 未公開のインターネット URL では、許可されていないアプリに設定されているルール (有効になっている場合) に基づいてアクセスが行われます。デフォルトでは、このアクセスは Secure Private Access 内で許可されています。詳しくは、「認可されていない Web サイトのルール設定」を参照してください。

アクセスポリシーの照合と優先順位付け

Secure Private Access は、アクセスするアプリケーションを照合する際に次のことを行います:

1. アクセス先のドメインをアプリケーション URL のドメインまたは関連ドメインと照合して、完全に一致させます。
2. 完全な FQDN と一致するように設定された Secure Private Access アプリケーションが見つかると、Secure Private Access はそのアプリケーションに設定されたすべてのポリシーを評価します。
   - ポリシーは、ユーザーコンテキストが一致するまで優先順位で評価されます。アクション (許可/拒否) は、優先度順に一致する最初のポリシーに従って適用されます。
   - 一致するポリシーがない場合、アクセスはデフォルトで拒否されます。
3. 完全な FQDN 一致が見つからない場合、Secure Private Access は最も長い一致 (ワイルドカードの一致など) に基づいてドメインを照合し、アプリケーションと対応するポリシーを検索します。

   例 **1:** 以下のアプリとポリシーの設定を考えてみましょう。

アプリケーション	アプリケーション URL	関連ドメイン
イントラネット	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

ポリシー名	優先度	ユーザーおよび関連アプリ
PolicyA	High	Eng-User5 (Intranet)
PolicyB	Low	HR-User4 (Wiki)

`HR-User4`が`app.intranet.local`にアクセスすると、次のことが起こります:

a) Secure Private Access はすべてのポリシーを検索して、アクセス対象のドメインと完全に一致するものを探します。この場合、`app.intranet.local`。
b) Secure Private Access は`PolicyA`を検索し、条件が一致するかどうかを確認します。
c) 条件が一致しないため、Secure Private Access はここで停止し、ワイルドカードの一致の確認は続行されません。`PolicyB`が一致していて（`app.intranet.local`は Wiki アプリの関連ドメイン`*.intranet.local`では一致するため)、アクセスが許可されていたとしても、続行されません。
d) そのため `HR-User4`の Wiki アプリへのアクセスは拒否されます。

例 **2:** 同じドメインが複数のアプリケーションで使用されている以下のアプリとポリシー構成を考えてみます。

アプリケーション	アプリケーション URL	関連ドメイン
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

ポリシー名	優先度	ユーザーおよび関連アプリ
PolicyA	High	Eng-User5 (App1)
PolicyB	Low	HR-User7 (App2)

`Eng-User5`ユーザーが`app.intranet.local`にアクセスすると、App1 と App2 の両方が FQDN の完全一致に基づいて一致するため、`Eng-User5`ユーザーは`PolicyA`を介してアクセスできます。

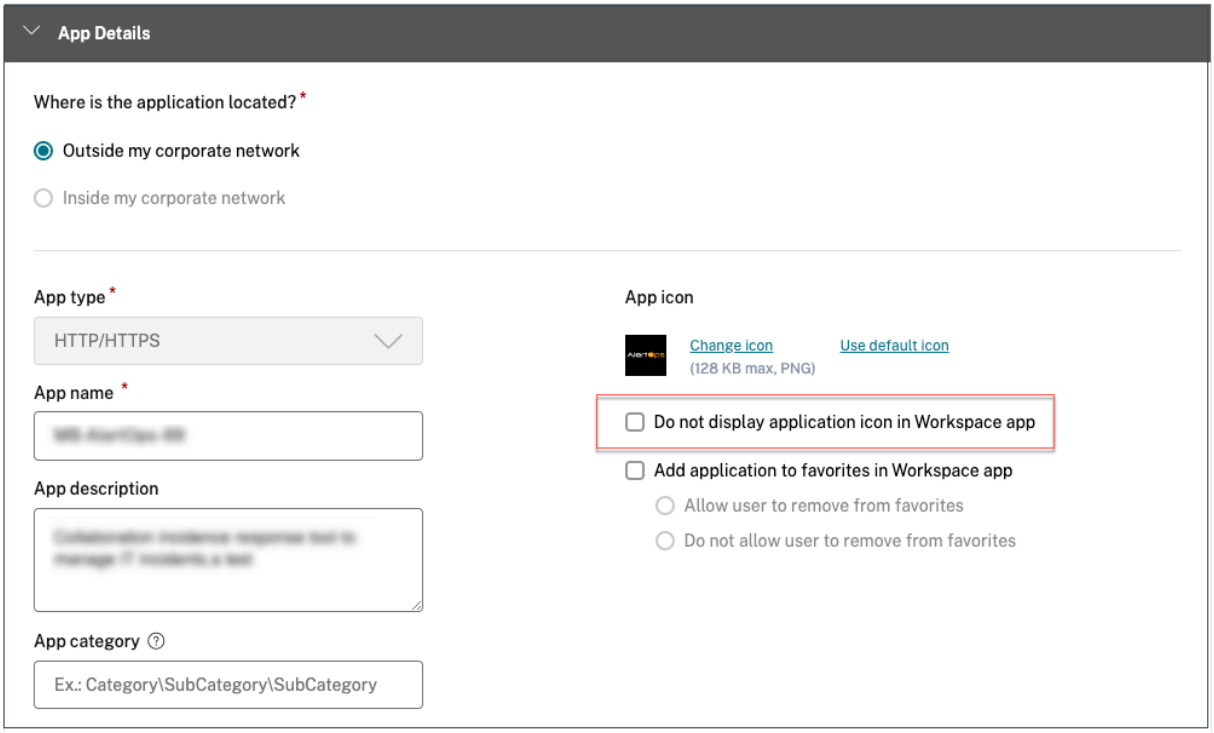
ただし、App1 に代わりに関連ドメインとして`*.intranet.local`がある場合、`app.intranet.local`が`PolicyB`に完全に一致することになるため、ユーザー`Eng-User5`にはアクセスできないため、`Eng-User5`へのアクセスは拒否されます。

アプリ設定のベストプラクティス

IDP ドメインには独自のアプリケーションが必要です

IDP ドメインを関連ドメインとしてイントラネットアプリの設定に追加する代わりに、次の方法をお勧めします:

- すべての IDP ドメイン用に個別のアプリケーションを作成します。
- IDP 認証ページへのアクセスを必要とするすべてのユーザーがアクセスできるようにするポリシーを作成し、そのポリシーを最優先にします。
- ワークスペースで列挙されないように、このアプリをアプリ構成から非表示にします（[アプリケーションアイコンをユーザーに表示しない] オプションを選択）。詳しくは、「アプリケーション詳細の設定」を参照してください。



> 注:
>
> このアプリ構成では、IDP 認証ページへのアクセスのみが有効になります。個々のアプリケーションへのさらなるアクセスは、やはり個々のアプリケーション構成とそれぞれのアクセスポリシーによって異なります。

設定例:

1. すべての一般的な FQDN を独自のアプリに設定し、必要に応じてグループ化してください。

   たとえば、Azure AD を IdP として使用するアプリがいくつかあり、`login.microsoftonline.com`およびその他の関連ドメイン（`*.msauth.net`）を設定する必要がある場合は、次の操作を行います:

   - `https://login.microsoftonline.com`をアプリケーション URL として、`*.login.microsoftonline.com`および`*.msauth.net`を関連ドメインとして、1 つの共通アプリケーションを作成します。

2. アプリの設定時に [ユーザーにアプリケーションアイコンを表示しない] オプションを選択します。詳細については、「アプリケーション詳細の設定」を参照してください。
3. 共通アプリケーションのアクセスポリシーを作成し、すべてのユーザーがアクセスできるようにします。詳細については、「アクセスポリシーの設定。
4. アクセスポリシーに最高の優先順位を割り当てます。詳細については、「優先順位」を参照してください。
5. 診断ログを確認して、FQDN がアプリと一致していること、およびポリシーが期待どおりに適用されていることを確認します。

同じ関連ドメインを複数のアプリケーションの一部にすることはできません

関連ドメインはアプリ固有のものでなければなりません。構成が競合すると、アプリへのアクセスに問題が生じる可能性があります。複数のアプリが同じ FQDN またはワイルドカード FQDN のバリエーションを使用して構成されている場合、次の問題が発生する可能性があります:

- Web サイトの読み込みが停止するか、空白のページが表示されることがあります。
- URL にアクセスすると、ブロックされたアクセスページが表示されることがあります。
- ログインページが読み込まれない可能性があります。

そのため、1 つのアプリ内で独自の関連ドメインを設定することをおすすめします。

正しくない設定例**:**

- 例**:** 複数のアプリケーションにわたる関連ドメインの複製

  両方とも Okta (example.okta.com) にアクセスする必要があるアプリが 2 つあるとします:

アプリ	アプリケーション URL ドメイン	関連ドメイン
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

ポリシー名	優先度	ユーザーおよび関連アプリ
HR へのアプリ 1 の拒否	High	HRのユーザーグループ App1
全員に App1 へのアクセス権を付与	中	ユーザーグループ「すべてのユーザー」へのアクセスを有効にする (App1)
全員に App2 へのアクセス権を付与	Low	App2 へのユーザーグループ「Everyone」へのアクセスを有効にする

  設定に関する問題**:** すべてのユーザーに App2 へのアクセスを許可することが目的でしたが、ユーザーグループ HR は App2 にアクセスできません。ユーザーグループ HR は Okta にリダイレクトされますが、App1（これも App2 と同じ関連ドメイン `example.okta.com`）へのアクセスを拒否した最初のポリシーに基づいてスタックします。

  このシナリオは、Okta などの ID プロバイダーでは非常に一般的ですが、共通の関連ドメインを持つ他の緊密に統合されたアプリでも発生する可能性があります。ポリシーの照合と優先順位付けの詳細については、「アクセスポリシーの照合と優先順位付け」を参照してください。

上記の構成に関する推奨事項**:**

1. example.okta.com を関連ドメインとしてすべてのアプリから削除します。
2. Okta 専用の新しいアプリを作成します（アプリケーション URL は`https://example.okta.com`で、関連ドメインは`*.okta.com`です）。
3. このアプリをワークスペースから非表示にします。
4. ポリシーに最優先度を割り当てて、競合を排除します。

ベスト・プラクティス**:**

- アプリの関連ドメインは、別のアプリの関連ドメインと重複してはいけません。
- このような場合は、共有関連ドメインに対応する新しい公開アプリを作成し、それに応じてアクセスを設定する必要があります。
- 管理者は、この共有関連ドメインを実際のアプリとして Workspace に表示する必要があるかどうかを評価する必要があります。
- アプリを Workspace に表示してはならない場合は、アプリの公開時に、［アプリケーションアイコンをユーザーに表示しない］オプションを選択して、そのアプリを Workspace から非表示にします。

ディープリンク **URL**

ディープリンク URL の場合、イントラネットアプリケーションの URL ドメインを関連ドメインとして追加する必要があります:

例:

イントラネットアプリでは URL が`https://example.okta.com/deep-link-app-1`をメインアプリケーション URL ドメインとして設定されており、関連ドメインにはイントラネットアプリケーション URL ドメイン（つまり`*.issues.example.net`）が設定されています。

この場合は、URL`https://example.okta.com`を使用して別に ID プロバイダーアプリを作成し、次に関連ドメインを`*.example.okta.com`として作成します。

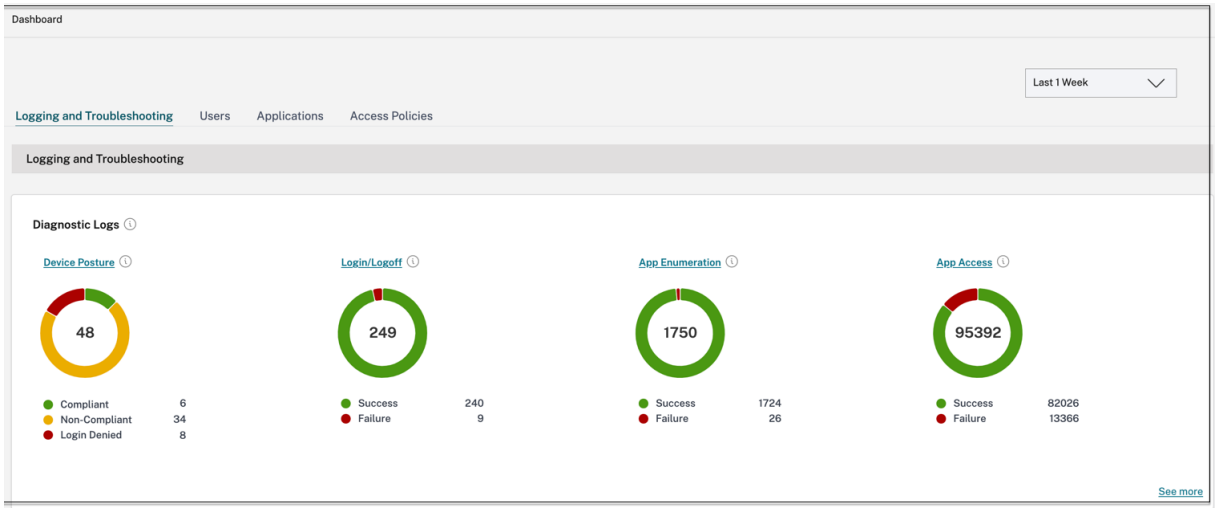
診断ログ

June 19, 2024

Secure Private Access サービス・ダッシュボードには、SaaS、Web、TCP、UDP アプリケーションの診断と使用状況データが表示されます。**Diagnostics Logs** チャートを使用すると、認証、アプリケーションの起動、アプリの列挙に関連するログだけでなく、デバイスの状態に関するログも確認できます。[**See more**] リンクをクリックすると、ログの詳細を表示できます。詳細は表形式で表示されます。事前に設定した時間またはカスタムタイムラインのログを表示できます。ダッシュボードに表示したい情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログは CSV 形式にエクスポートできます。

- [フィルターを追加] オプションを使用すると、アプリの種類、カテゴリ、説明などのさまざまな条件に基づいて検索を絞り込むことができます。たとえば、検索フィールドで`Transaction ID`、`= (equals to some value)`をクリックし、`7456c0fb-a60d-4bb9-a2a2-edab8340bb15`と入力すると、このトランザクション ID に関連するすべてのログを検索できます。フィルターオプションで使用できる検索演算子の詳細については、「検索演算子」を参照してください。
- デバイスポスチャログ**:** ポリシー結果 (準拠、非準拠、ログイン拒否) に基づいて検索を絞り込むことができます。デバイスポスチャについて詳しくは、「デバイスポスチャ」を参照してください。

> 注記**:**
>
> - Secure Private Access 診断ログダッシュボード内のすべての障害イベントには、関連する情報コードがあります。詳細については、「情報コード」を参照してください。
> - トランザクション ID は、アクセスリクエストのすべての Secure Private Access ログを関連付けます。詳細については、「トランザクション ID」を参照してください。



> 注記**:**
>
> - デフォルトでは、診断ログページには今週のデータと最近の 10000 レコードのみが表示されます。カスタム日付検索とフィルターを使用して、検索結果をさらに絞り込みます。

監査ログ

February 20, 2024

Secure Private Access サービス関連のイベントが、**Citrix Cloud >** システムログにキャプチャされるようになりました。管理者が Citrix Secure Private Access サービスで実行するすべてのイベントは、Citrix Cloud に送信され、システムログに記録されます。管理イベントには次のものがありますが、これらに限定されません:

- Web または SaaS アプリの構成
- アプリをサブスクライブする
- アプリを削除する
- アダプティブアクセスポリシーの設定

次の図は、システムログ内の **Secure Private Access** 関連のイベントを示しています。イベントのエクスポート、特定の期間のイベントの取得、ログイベントの転送、データ保持などについて詳しくは、「システムログ」を参照してください。

エンタープライズ **Web**、**TCP**、**SaaS** アプリケーションのアダプティブアクセスとセキュリティ制御

June 19, 2024

今日の絶え間なく変化する状況では、アプリケーションセキュリティはあらゆるビジネスにとって不可欠です。コンテキスト認識型のセキュリティ決定を行い、アプリケーションへのアクセスを有効にすると、ユーザーへのアクセスを有効にしながら、関連するリスクが軽減されます。

Citrix Secure Private Access サービスのアダプティブアクセス機能は、アプリケーションへの安全なアクセスを提供する包括的なゼロトラストアクセスアプローチを提供します。アダプティブアクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリに、きめ細かなレベルでアクセスできるようになります。ここで「コンテキスト」という用語は次のことを指します。

- ユーザーとグループ (ユーザーとユーザーグループ)
- デバイス (デスクトップまたはモバイルデバイス)
- ロケーション (ジオロケーションまたはネットワークロケーション)
- デバイスポスチャ (デバイスポスチャチェック)
- リスク（ユーザーリスクスコア）

アダプティブアクセス機能は、アクセスされているアプリケーションに適応ポリシーを適用します。これらのポリシーは、コンテキストに基づいてリスクを決定し、エンタープライズ Web、SaaS、TCP、および UDP アプリへのアクセスを許可または拒否する動的なアクセス決定を行います。

機能

アプリケーションへのアクセスを許可または拒否するために、管理者は、ユーザー、ユーザーグループ、ユーザーがアプリケーションにアクセスするデバイス、ユーザーがアプリケーションにアクセスしている場所（国またはネットワークの場所）、およびユーザーのリスクスコアに基づいてポリシーを作成します。

アダプティブアクセスポリシーは、Secure Private Access サービスに SaaS または Web アプリケーションを追加するときに構成されるアプリケーション固有のセキュリティポリシーよりも優先されます。アプリごとのセキュリティ制御は、適応型アクセスポリシーによって上書きされます。

アダプティブアクセスポリシーは、次の **3** つのシナリオで評価されます。

- Secure Private Access サービスからの Web、TCP、または SaaS アプリケーションの列挙中—このユーザーに対するアプリケーションアクセスが拒否された場合、ユーザーはこのアプリケーションをワークスペースに表示できません。
- アプリケーションの起動中—アプリを列挙した後、アダプティブポリシーがアクセスを拒否するように変更された場合、アプリが以前に列挙されていたとしても、ユーザーはアプリを起動できません。
- Citrix Enterprise Browser またはリモートブラウザ隔離サービスでアプリを開くと、Citrix Enterprise Browser はある程度のセキュリティ制御を行います。これらのコントロールは、クライアントによって強制されます。Citrix Enterprise Browser が起動すると、サーバーはユーザーの適応型ポリシーを評価し、それらのポリシーをクライアントに返します。その後、クライアントはポリシーを Citrix Enterprise Browser でローカルに適用します。

複数のルールを含む適応型アクセスポリシーの作成

1 つのポリシー内で、複数のアクセスルールを作成し、さまざまなユーザーまたはユーザーグループにさまざまなアクセス条件を設定できます。これらのルールは、HTTP/HTTPS アプリケーションと TCP/UDP アプリケーションの両方に、すべて 1 つのポリシー内で個別に適用できます。

Secure Private Access のアクセスポリシーにより、ユーザーまたはユーザーのデバイスのコンテキストに基づいてアプリへのアクセスを有効または無効にできます。さらに、次のセキュリティ制限を追加することで、アプリへの制限付きアクセスを有効にできます。

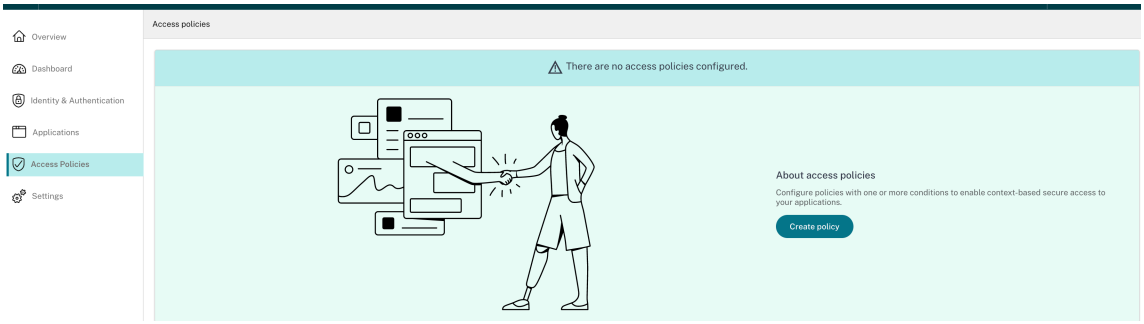
- クリップボードへのアクセスを制限する
- 印刷を制限
- ダウンロードを制限
- アップロードを制限する
- ウォーターマークを表示
- キーロギングを制限する
- 画面キャプチャを制限する

これらの制限の詳細については、「利用可能なアクセス制限オプション」を参照してください。

アクセスポリシーを設定する前に、次のタスクを完了していることを確認してください。

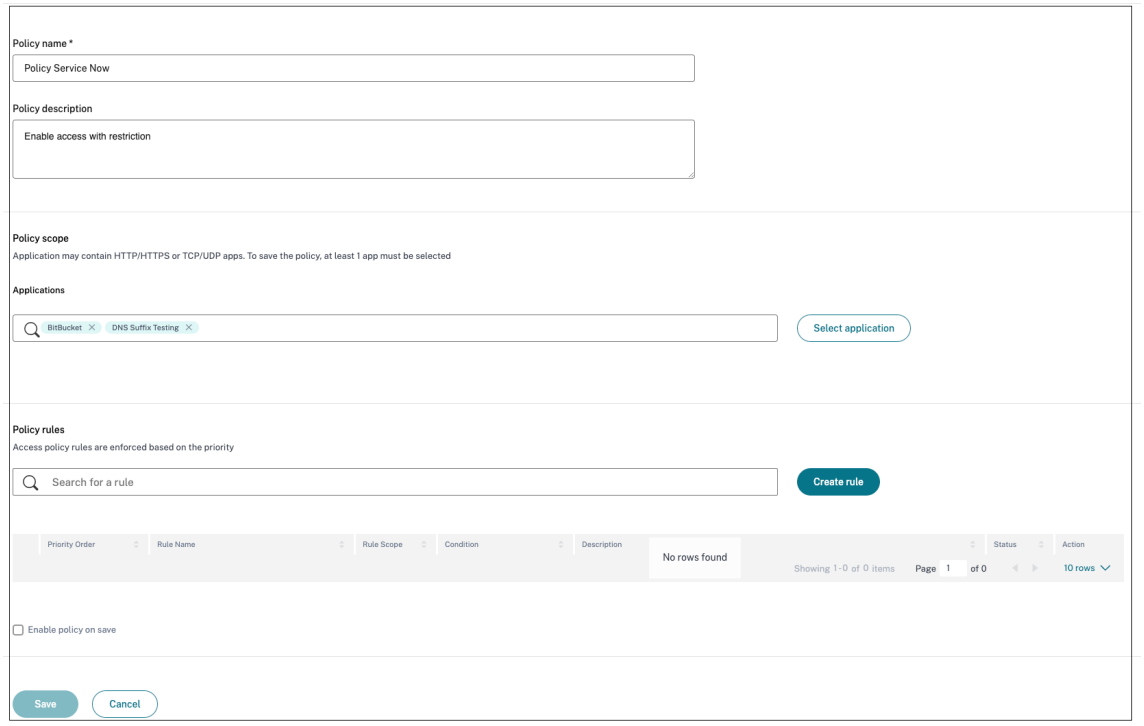
- ID と認証の設定
- 設定済みアプリケーション

1. ナビゲーションペインで、[アクセスポリシー] をクリックし、[ポリシーの作成] をクリックします。



初めてのユーザの場合、[アクセスポリシー（**Access** Policies）] ランディングページにはポリシーが表示されません。ポリシーを作成すると、ここに一覧表示されます。

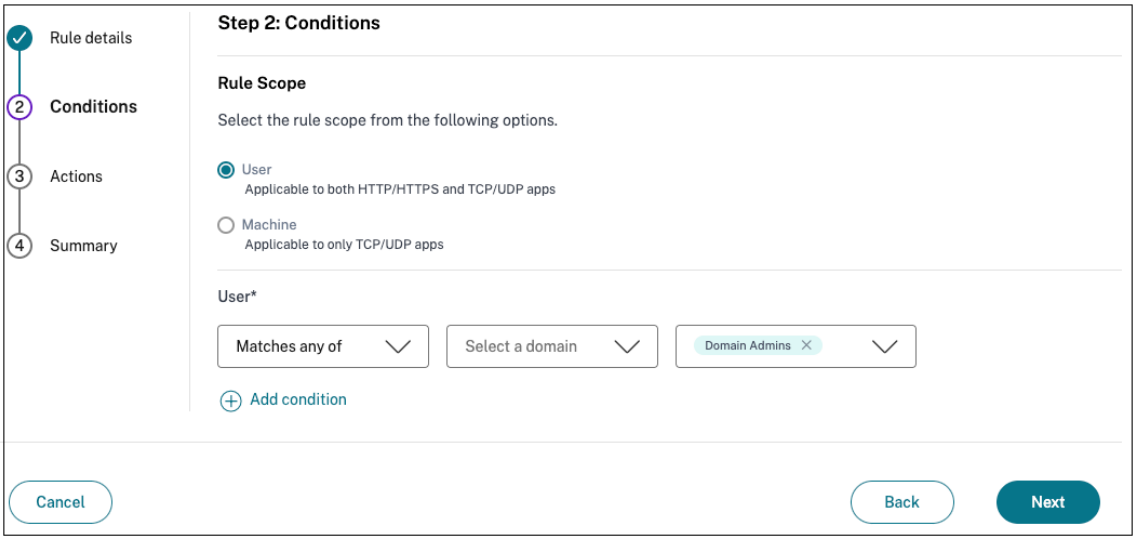
2. ポリシー名とポリシーの説明を入力します。
3.「アプリケーション」で、このポリシーを適用する必要があるアプリまたはアプリのセットを選択します。
4.「**Create Rule** 」をクリックして、ポリシーのルールを作成します。



5. ルール名とルールの簡単な説明を入力して、[次へ] をクリックします。

6. ユーザーの条件を選択します。ユーザー条件は、ユーザーにアプリケーションへのアクセスを許可するための必須条件です。次のいずれかを選択します:

   - いずれかに一致—フィールドに表示されている名前のいずれかに一致し、選択したドメインに属するユーザーまたはグループのみがアクセスを許可されます。
   - いずれにも一致しない -フィールドに表示され、選択したドメインに属するユーザーまたはグループを除くすべてのユーザーまたはグループがアクセスを許可されます。



7. (オプション) コンテキストに基づいて複数の条件を追加するには、「+」をクリックします。

   コンテキストに基づいて条件を追加すると、その条件に AND 演算が適用され、**Users*** とオプションのコンテキストベースの条件が満たされた場合にのみポリシーが評価されます。状況に応じて次の条件を適用できます。

   - ** デスクトップまたはモバイルデバイス ** —アプリへのアクセスを有効にするデバイスを選択します。
   - 位置情報—ユーザーがアプリにアクセスしている条件と地理的位置を選択します。
   - ネットワークの場所—ユーザーがアプリにアクセスする際に使用する条件とネットワークを選択します。

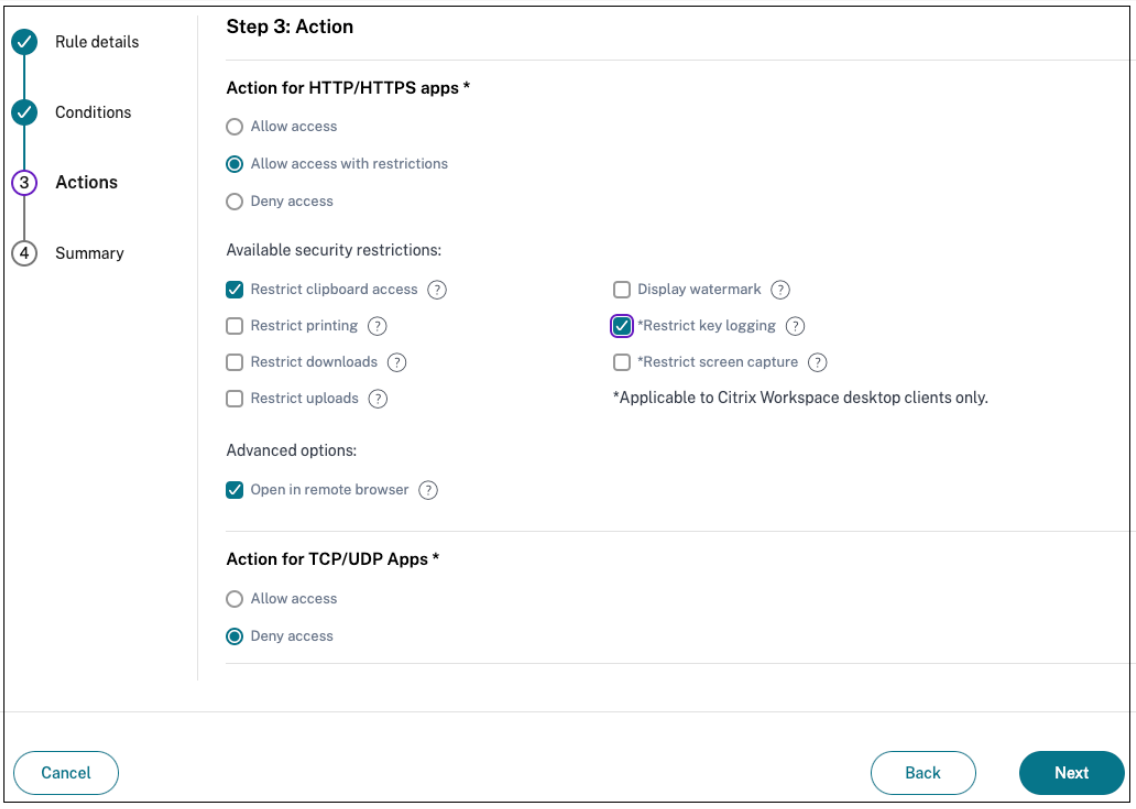
- デバイスポスチャチェック—アプリケーションにアクセスするためにユーザーデバイスが通過しなければならない条件を選択します。
- ユーザーリスクスコア—ユーザーにアプリケーションへのアクセスを提供する必要があるリスクスコアカテゴリを選択します。

8. [次へ] をクリックします。
9. 条件評価に基づいて適用する必要があるアクションを選択します。

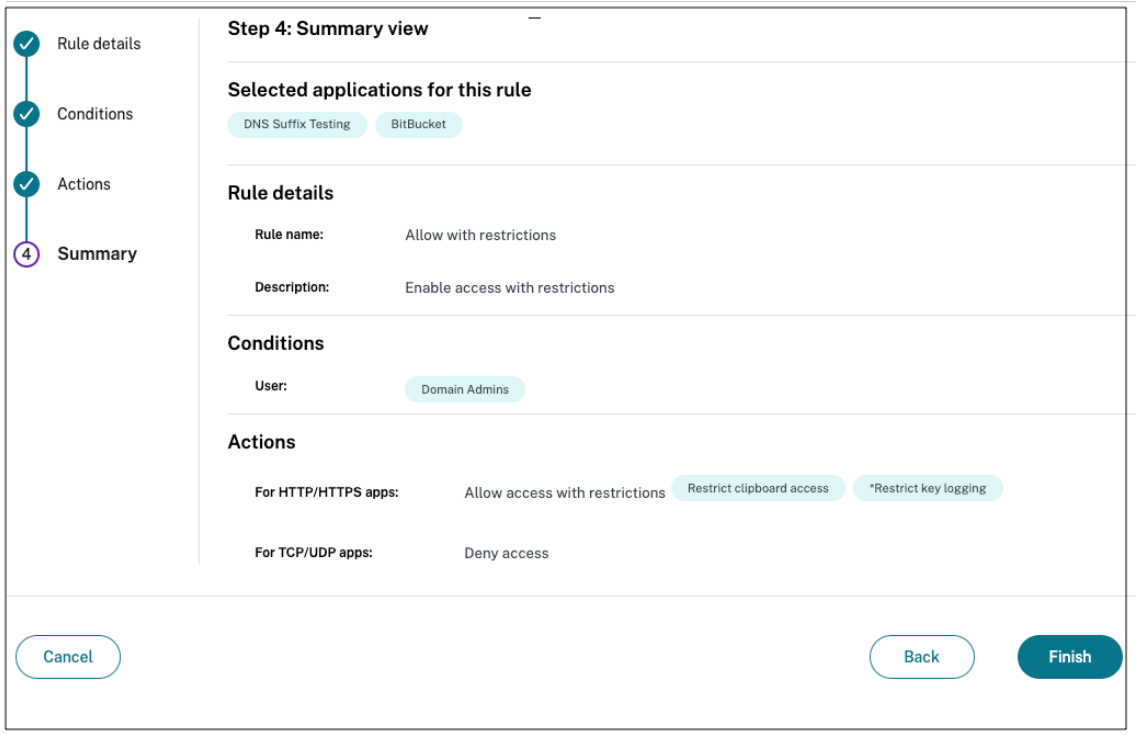
- HTTP/HTTPS アプリの場合、以下を選択できます。
  - アクセスを許可
  - 制限付きでアクセスを許可
  - アクセスを拒否

> 注:
>
> [制限付きアクセスを許可] を選択した場合は、アプリに適用する制限を選択する必要があります。制限の詳細については、「使用可能なアクセス制限オプション」を参照してください。また、アプリをリモートブラウザで開くか、Citrix Secure Browser で開くかを指定することもできます。

- TCP/UDP アクセスでは、以下を選択できます。
  - アクセスを許可
  - アクセスを拒否



10. ［次へ］をクリックします。「概要」ページには、ポリシーの詳細が表示されます。
11. 詳細を確認して [完了] をクリックします。



ポリシー作成後に覚えておくべきポイント

- 作成したポリシーは [ポリシールール] セクションに表示され、デフォルトで有効になっています。必要に応じてルールを無効にできます。ただし、ポリシーをアクティブにするには、少なくとも 1 つのルールが有効になっていることを確認してください。
- デフォルトでは、ポリシーには優先順位が割り当てられます。値が小さい優先度が最も高くなります。優先順位が最も低いルールが最初に評価されます。ルール (n) が定義された条件と一致しない場合、次のルール (n+1) が評価され、以降も同様です。

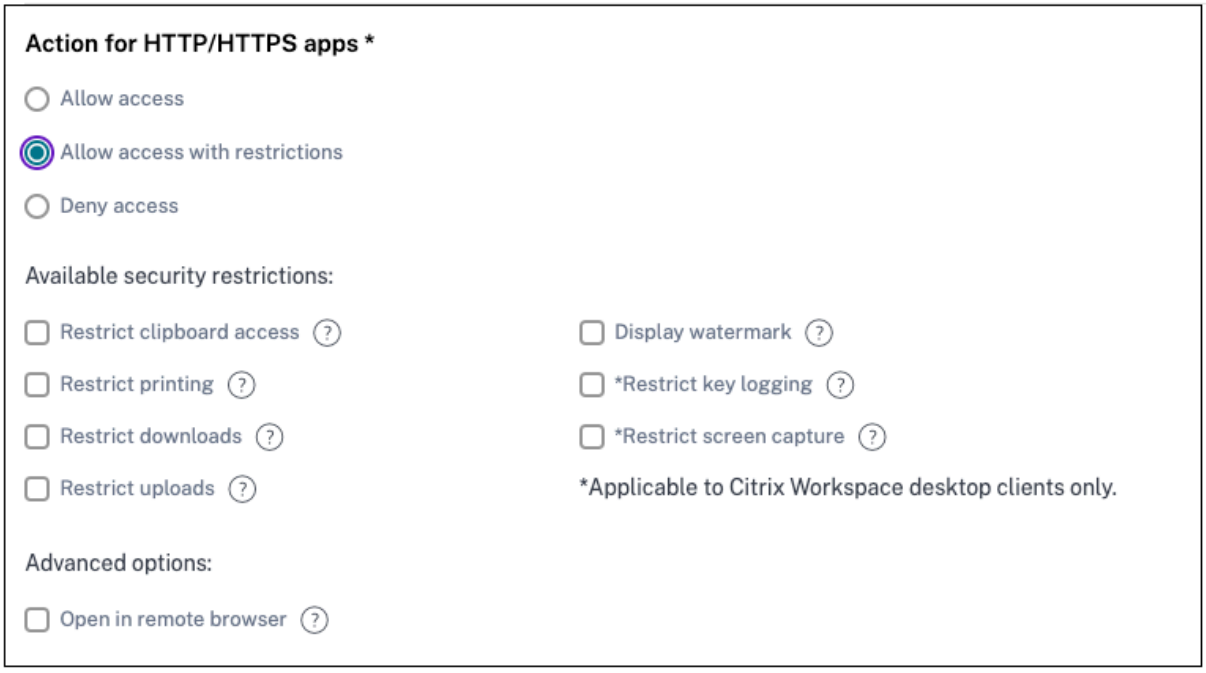
優先順位の例によるルールの評価**:**

ルール 1 とルール 2 の 2 つのルールを作成したと仮定します。
ルール 1 はユーザー A に割り当てられ、ルール 2 はユーザー B に割り当てられます。その後、両方のルールが評価されます。
ルール 1 とルール 2 の両方がユーザ A に割り当てられていると仮定します。この場合、ルール 1 の優先度が高くなります。ルール 1 の条件が満たされると、ルール 1 が適用され、ルール 2 はスキップされます。それ以外の場合、ルール 1 の条件が満たされない場合、ルール 2 がユーザー A に適用されます。

> 注記**:**
>
> どのルールも評価されない場合、アプリはユーザーに列挙されません。

利用可能なアクセス制限オプション

「制限付きアクセスを許可する」アクションを選択するときは、セキュリティ制限を少なくとも 1 つ選択する必要があります。これらのセキュリティ制限は、システムであらかじめ定義されています。管理者は、他の組み合わせを変更したり追加したりすることはできません。次のセキュリティ制限をアプリケーションに対して有効にできます。



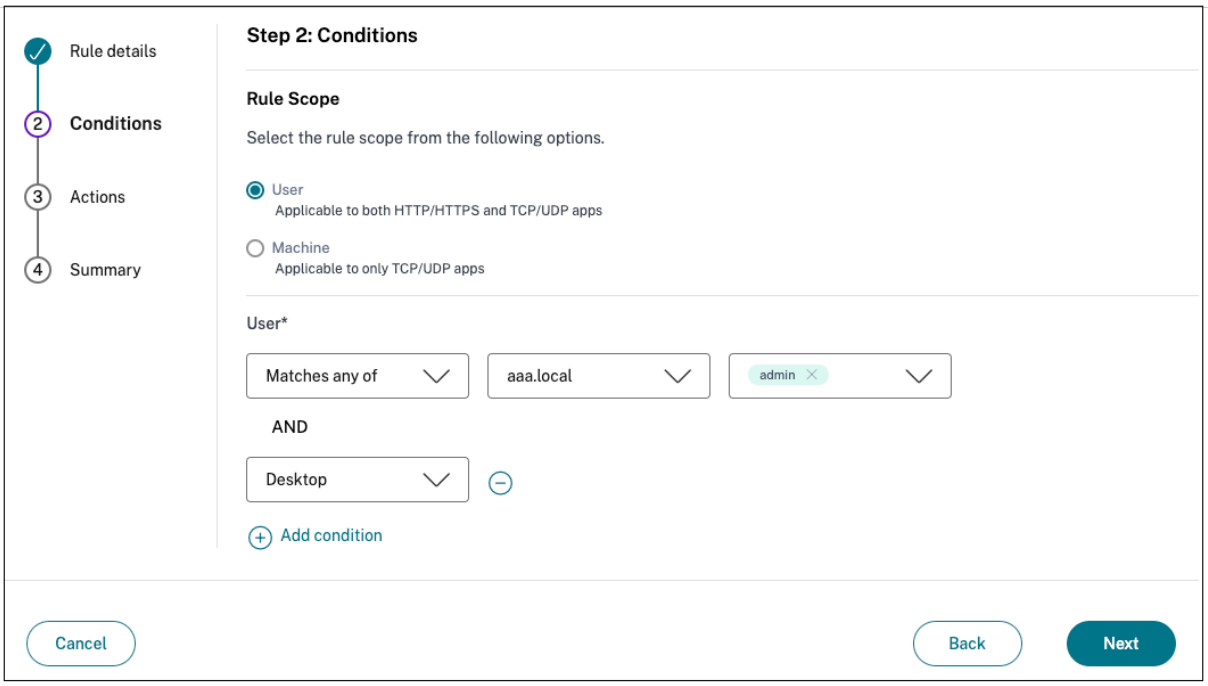
- クリップボードへのアクセスを制限**:** アプリとシステムクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- 印刷の制限：Citrix Enterprise Browser 内からの印刷機能を無効にします。
- ダウンロードを制限する**:** ユーザーがアプリ内からダウンロードできないようにします。
- アップロードを制限する**:** ユーザーがアプリ内でアップロードできないようにします。
- ウォーターマークを表示**:** ユーザーの画面にウォーターマークを表示し、ユーザーのマシンのユーザー名と IP アドレスを表示します。
- キーロギングの制限**:** キーロガーから保護します。ユーザーがユーザー名とパスワードを使用してアプリにログオンしようとすると、すべてのキーがキーロガーで暗号化されます。また、ユーザーがアプリで実行するすべてのアクティビティは、キーロギングから保護されます。たとえば、Office 365 のアプリ保護ポリシーが有効になっていて、ユーザーが Office 365 の Word 文書を編集した場合、すべてのキーストロークはキーロガーで暗号化されます。
- 画面キャプチャを制限する**:** 画面キャプチャプログラムまたはアプリのいずれかを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとすると、空白の画面がキャプチャされます。

デバイスに基づくアダプティブアクセス

ユーザーがアプリケーションにアクセスするプラットフォーム（モバイルデバイスまたはデスクトップコンピューター）に基づいて適応型アクセスポリシーを構成するには、「複数のルールを含む適応型アクセスポリシーの作成」手順に従い、次の変更を行います。

- 「ステップ **2:** 条件」ページで、「条件を追加」をクリックします。
- [デスクトップ] または [モバイルデバイス] を選択します。

- ポリシー設定を完了します。



場所に基づくアダプティブアクセス

管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいて、アダプティブアクセスポリシーを設定できます。ロケーションは、ユーザーがアプリケーションにアクセスしている国またはユーザーのネットワークロケーションです。ネットワークの場所は、IP アドレス範囲またはサブネットアドレスを使用して定義されます。

ロケーションに基づいてアダプティブアクセスポリシーを設定するには、以下の変更を加えた [複数のルールを含むアダプティブアクセスポリシーの作成] 手順を使用してください。

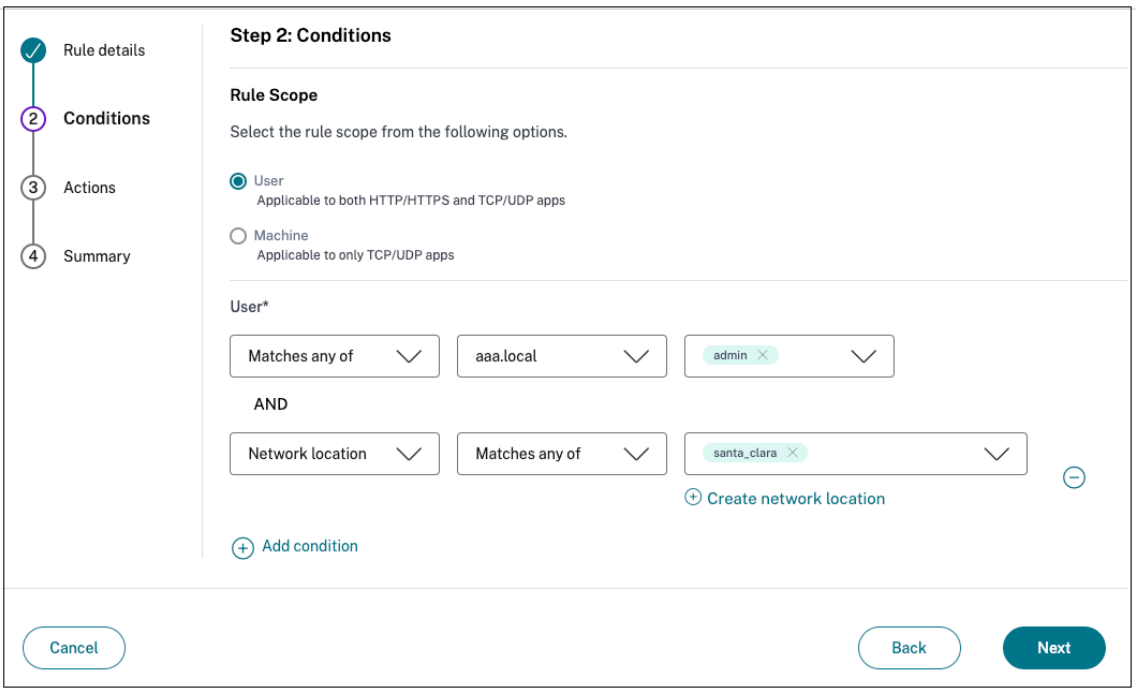
- 「ステップ **2:** 条件」ページで、「条件を追加」をクリックします。
- [位置情報 **]** または **[**** ネットワークロケーション ****]** を選択します。
- 複数のジオロケーションまたはネットワークロケーションを設定している場合は、要件に応じて次のいずれかを選択します。
  - [次のいずれかに一致] —地理的位置またはネットワーク位置が、データベースに構成されている地理的位置またはネットワーク位置のいずれかに一致します。
  - いずれにも一致しない—地理的位置またはネットワーク位置が、データベースに構成されている地理的位置またはネットワーク位置と一致しません。

  注記**:**

  - **Geo-location** を選択すると、ユーザーの送信元 IP アドレスが国データベースの IP アドレスで評価されます。ユーザーの IP アドレスがポリシー内の国にマップされている場合、ポリシーが適用されます。

国が一致しない場合、この適応ポリシーはスキップされ、次のアダプティブポリシーが評価されます。

- [ネットワークロケーション] では、既存のネットワークロケーションを選択するか、ネットワークロケーションを作成できます。新しいネットワークロケーションを作成するには、[ネットワークロケーションの作成] をクリックします。
- **Citrix Cloud > Citrix Workspace >** アクセス **>** アダプティブアクセスからアダプティブアクセスが有効になっていることを確認してください。そうでない場合は、ロケーションタグを追加できません。詳細については、「アダプティブアクセスを有効にする」を参照してください。
- Citrix Cloud コンソールからネットワークの場所を作成することもできます。詳しくは、「Citrix Cloud ネットワークの場所の構成」を参照してください。



- ポリシー設定を完了します。

デバイスポスチャに基づくアダプティブアクセス

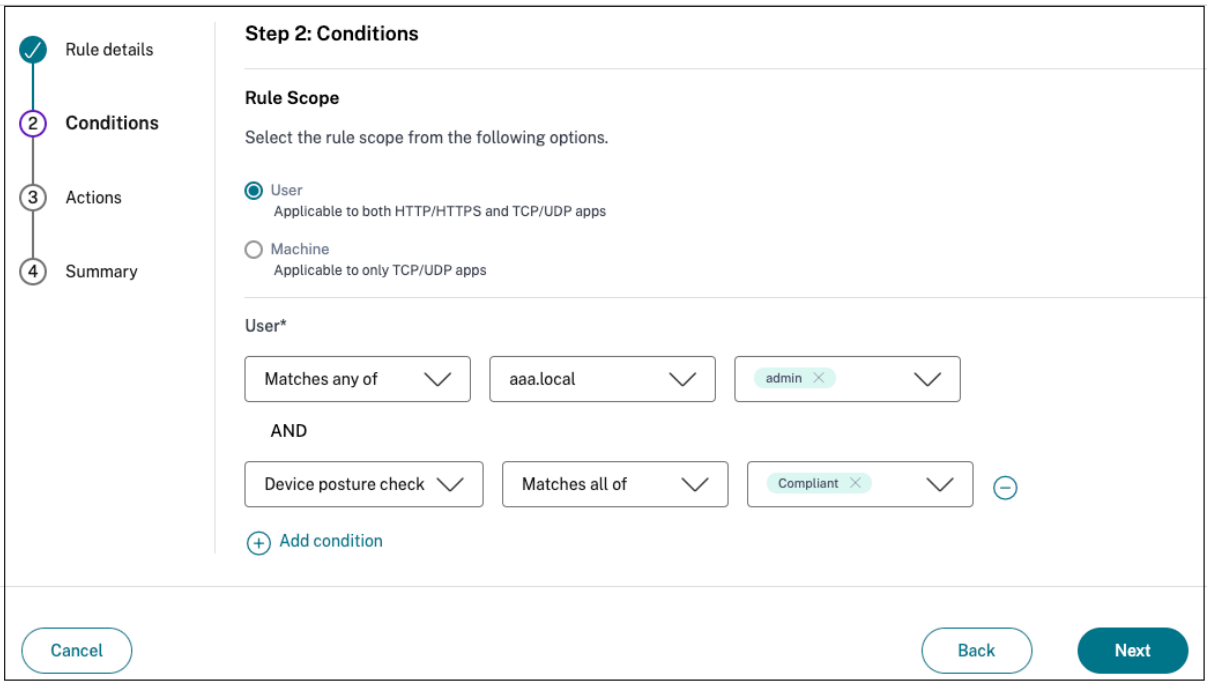
デバイスポスチャタグを使用してアクセス制御を強制するように Secure Private Access サービスを設定できます。デバイスポスチャ検証後にデバイスのログインが許可されると、そのデバイスは準拠または非準拠として分類できます。この情報は、Citrix DaaS サービスおよび Citrix Secure Private Access サービスにタグとして提供され、デバイスの状態に基づいてコンテキストアクセスを提供するために使用されます。

デバイスポスチャサービスの詳細については、「デバイスポスチャ」を参照してください。

デバイスポスチャに基づいてアダプティブアクセスポリシーを設定するには、「複数のルールを含むアダプティブアクセスポリシーの作成」の手順に従い 、以下の変更を加えます。

- 「ステップ **2:** 条件」ページで、「条件を追加」をクリックします。
- ドロップダウンメニューから [デバイスポスチャチェック] と [論理式] を選択します。
- カスタムタグに次のいずれかの値を入力します:
  - 準拠-準拠デバイス用
  - 非準拠-非準拠デバイス用

> 注:
>
> デバイス分類タグの構文は、先ほど説明したのと同じ方法、つまり頭文字を大文字 (Compliant)、非準拠 (Compliant) で入力する必要があります。そうしないと、デバイスポスチャポリシーが意図したとおりに機能しません。



ユーザーリスクスコアに基づくアダプティブアクセス

> 重要:
>
> この機能は、顧客が Security Analytics エンタイトルメントを持っている場合にのみ使用できます。

ユーザーリスクスコアは、企業内のユーザーアクティビティに関連するリスクを判断するためのスコアリングシステムです。リスク指標は、疑わしいと思われるユーザーアクティビティや、組織にセキュリティ上の脅威を与える可能性のあるユーザーアクティビティに割り当てられます。リスク指標は、ユーザーの行動が正常から逸脱したときにトリガーされます。各リスク指標には、1 つ以上のリスク要因を関連付けることができます。これらのリスク要因は、ユーザーイベントの異常の種類を判断するのに役立ちます。リスク指標とそれに関連するリスク要因は、ユーザーの

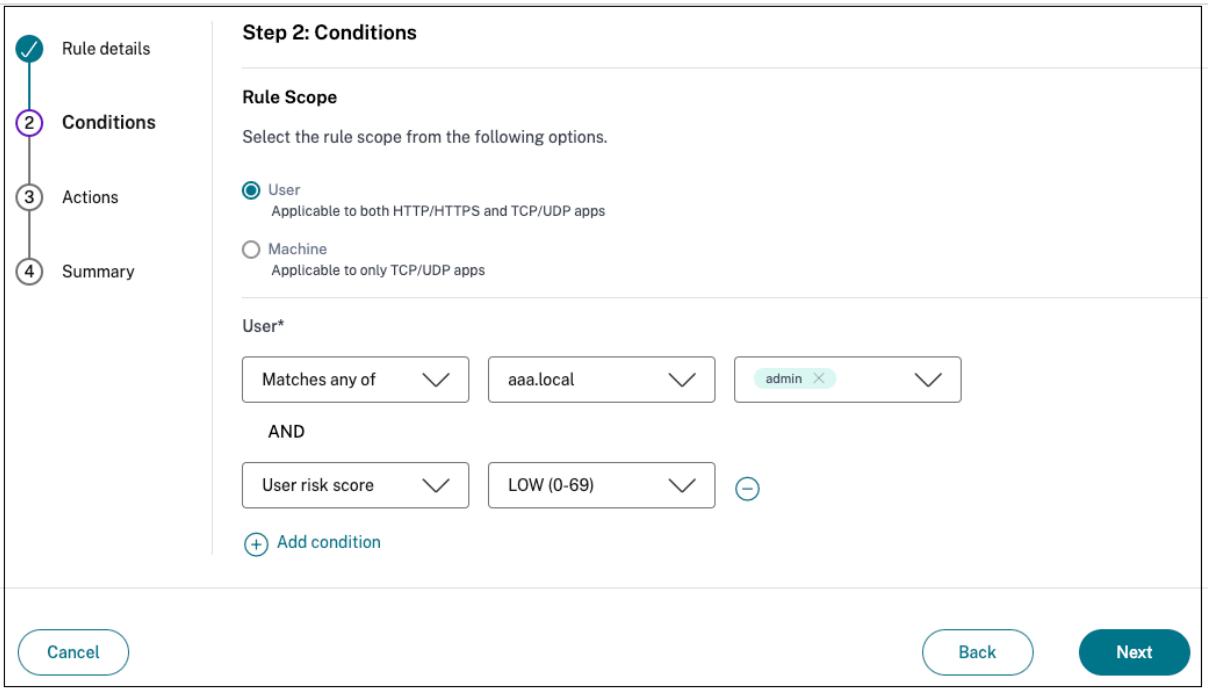
リスクスコアを決定します。リスクスコアは定期的に計算され、アクションとリスクスコアの更新の間には遅延があります。詳しくは、「Citrix ユーザーリスク指標」を参照してください。

リスクスコアを含む適応型アクセスポリシーを設定するには、以下の変更を加えた複数のルールを含む適応型アクセスポリシーの作成手順を使用してください 。

- 「ステップ **2:** 条件」ページで、「条件を追加」をクリックします。
- [ユーザーリスクスコア] を選択し、次にリスク条件を選択します。
  - CAS サービスから取得したプリセットタグ
    - 低 1—69
    - ミディアム 70—89
    - 高 90—100

    > 注記:
    >
    > リスクスコアが 0 の場合、リスクレベル「低」とは見なされません。

  - しきい値の種類
    - 次より大きい、または等しい
    - 次より小さいか等しい
  - 数値の範囲
    - 範囲



同じ関連ドメインに起因するコンフリクトを解決するためのルートテーブル

January 9, 2024

Citrix Secure Private Access サービスのアプリケーションドメイン機能により、お客様は、関連するアプリケーションのドメインをコネクタアプライアンスを介して外部または内部でルーティングできるようにするルーティングを決定できます。

顧客が SaaS アプリと内部 Web アプリの両方で同じ関連ドメインを設定しているとします。
たとえば、Okta が Salesforce (SaaS アプリケーション) と Jira (内部 Web アプリケーション) の両方の SAML IdP である場合、システム管理者は両方のアプリケーションの設定で`*.okta.com`を関連ドメインとして設定できます。これにより、競合が発生し、エンドユーザーには一貫性のない動作が発生します。このシナリオでは、管理者は要件に応じて、これらのアプリケーションをコネクタアプライアンスを介して外部または内部にルーティングするルールを定義できます。

アプリケーションドメイン機能により、管理者は、顧客の Web プロキシサーバーをバイパスして内部 Web サーバーにアクセスするようにコネクタアプライアンスを構成することもできます。これらのバイパスポリシーは、以前は Connector Appliance NSCLI コマンドを実行して手動で設定されていました。

ルートテーブルの仕組み

管理者は、トラフィックフローの定義方法に応じて、アプリのルートタイプを Connector Appliance 経由で外部、内部、または外部として定義できます。

- [外部]: トラフィックはインターネットに直接流れます。
- 内部—トラフィックは Connector Appliance スを経由して流れます。
  - Web アプリの場合、トラフィックはデータセンター内を流れます。
  - SaaS アプリケーションの場合、トラフィックは Connector Appliance 介してネットワーク外にルーティングされます。
- 内部—プロキシをバイパスする -ドメイントラフィックは、コネクタアプライアンス上で構成されたお客様の Web プロキシをバイパスして、Citrix Cloud Connector Appliance 経由してルーティングされます。
- コネクタ経由の外部 -アプリケーションは外部ですが、トラフィックは Connector Appliance 経由して外部ネットワークに流れる必要があります。

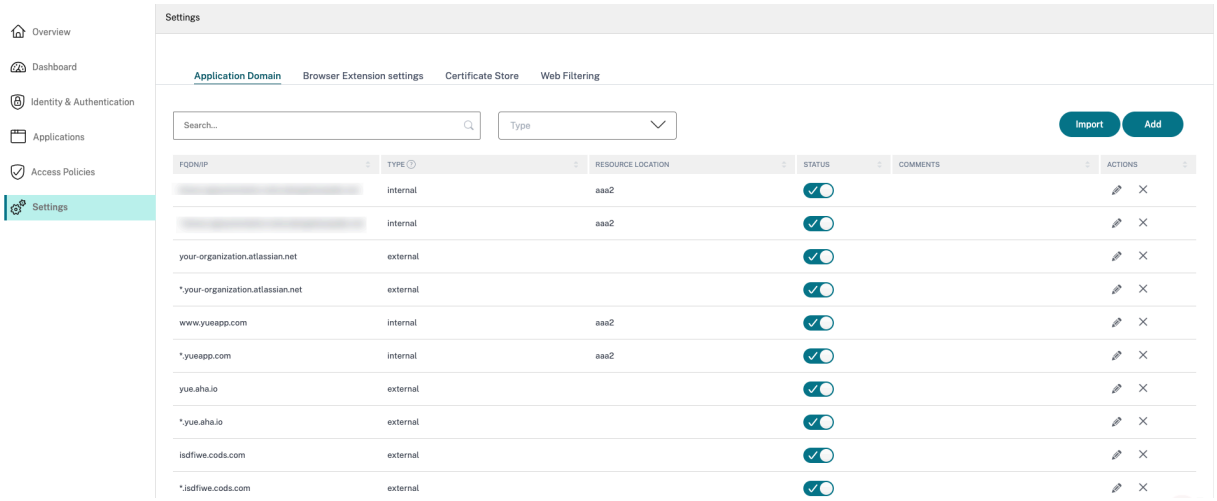
> 注:
>
> - ルートエントリは、アプリで構成されているセキュリティポリシーには影響しません。
> - 管理者がルートテーブル内のエントリを使用する予定がない場合、または対応するアプリが意図したとおりに動作しない場合、管理者はエントリを削除するのではなく、単純に無効にすることができます。

> - 特定のカスタマーのすべてのコネクタアプライアンスには、アプリケーションの種類に関係なく、SSO 設定が適用されます。以前は、特定のアプリの SSO 設定はリソースの場所に関連付けられていました。

メインルートテーブル

メインルートテーブルには、[**Secure Private Access**] タイルからアクセスできます。

1. Citrix Cloud アカウントにログオンします。
2.「Secure Private Access」タイルで、「管理」をクリックします。
3. ナビゲーションペインで、[設定] をクリックします。[アプリケーションドメイン] ページが表示されます。



メインルートテーブルには、次の列が表示されます。

- **FQDN/IP:** トラフィックルーティングのタイプを設定する FQDN または IP アドレス。
- タイプ: アプリの種類。アプリの追加時に選択した内部、外部、** または外部経由のコネクタ経由。**

  > 重要:
  >
  > コンフリクトがある場合、テーブル内の各行にアラートアイコンが表示されます。競合を解決するには、管理者は三角形のアイコンをクリックし、メインテーブルからアプリの種類を変更する必要があります。

- 生産資源事業所**:**「内部」タイプの工順の生産資源事業所。リソースの場所が割り当てられていない場合、それぞれのアプリの [リソースの場所] 列に三角形のアイコンが表示されます。アイコンにカーソルを合わせると、次のメッセージが表示されます。

  リソースの場所が見つかりません。リソースの場所がこの *FQDN* に関連付けられていることを確認します。

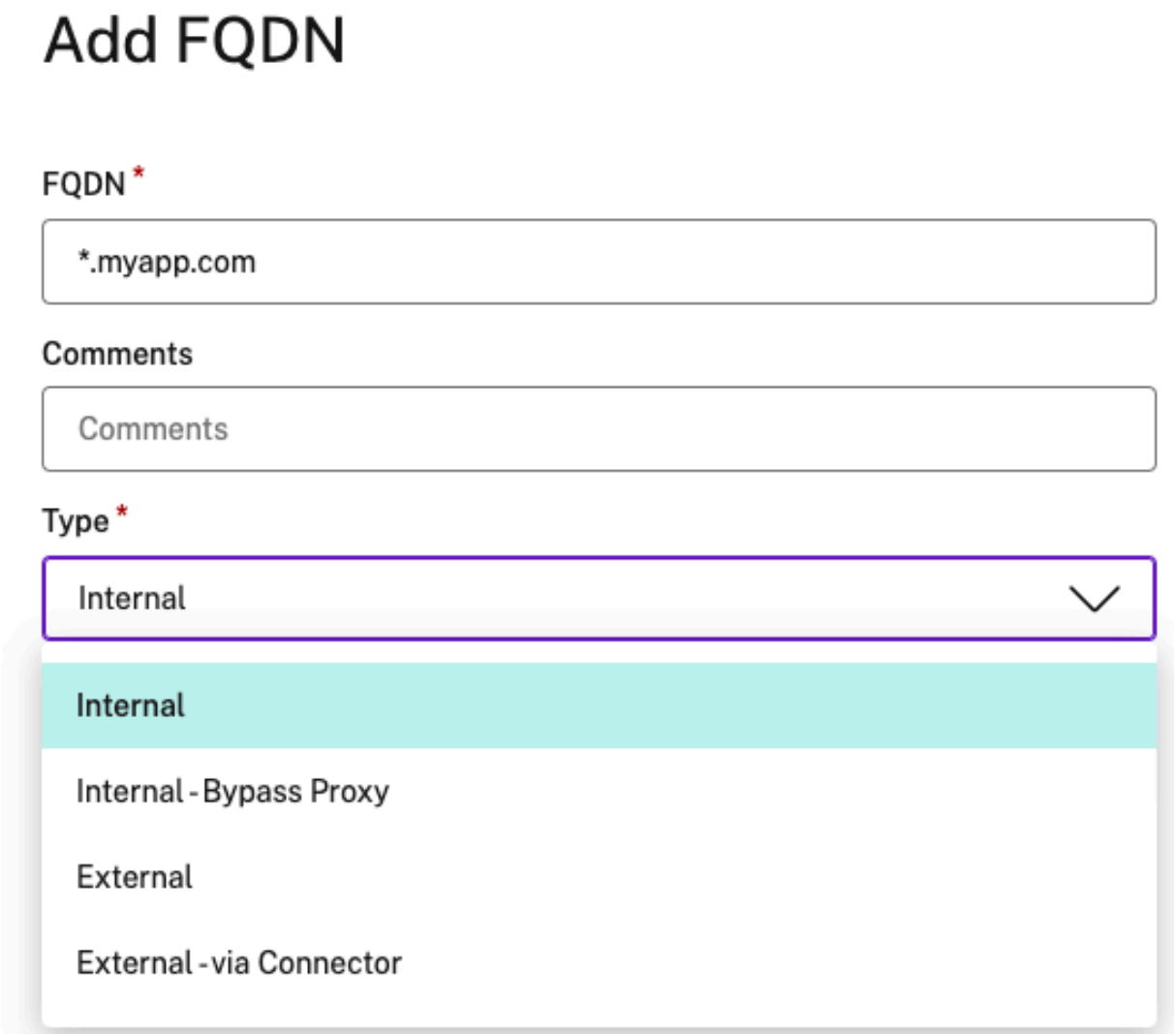
- ステータス**:** [**Status**] 列のトグルスイッチを使用すると、アプリを削除せずにルートエントリのルートを無効にできます。トグルスイッチが OFF の場合、ルートエントリは有効になりません。また、完全に一致する FQDN が存在する場合、管理者は有効または無効にするルートを選択できます。
- コメント**:** コメントがあれば表示します。

- アクション**:** 編集アイコンは、リソースの場所を追加したり、ルートエントリのタイプを変更したりするために使用されます。削除アイコンは、ルートを削除するために使用されます。

FQDN を **[**アプリケーションドメイン**]** テーブルに追加する

管理者は FQDN を [アプリケーションドメイン] テーブルに追加し、適切なルーティングタイプを選択できます。

1. [アプリケーションドメイン] ページで [追加] をクリックします。
2. FQDN 名を入力し、FQDN の適切なルーティングタイプを選択します。



ミニルートテーブル

アプリケーションドメインテーブルのミニバージョンを使用して、アプリケーションの構成中にルーティングを決定できます。ミニルートテーブルは、Citrix Secure Private Access サービスのユーザーインターフェイスの「アプリケーション接続」セクションにあります。

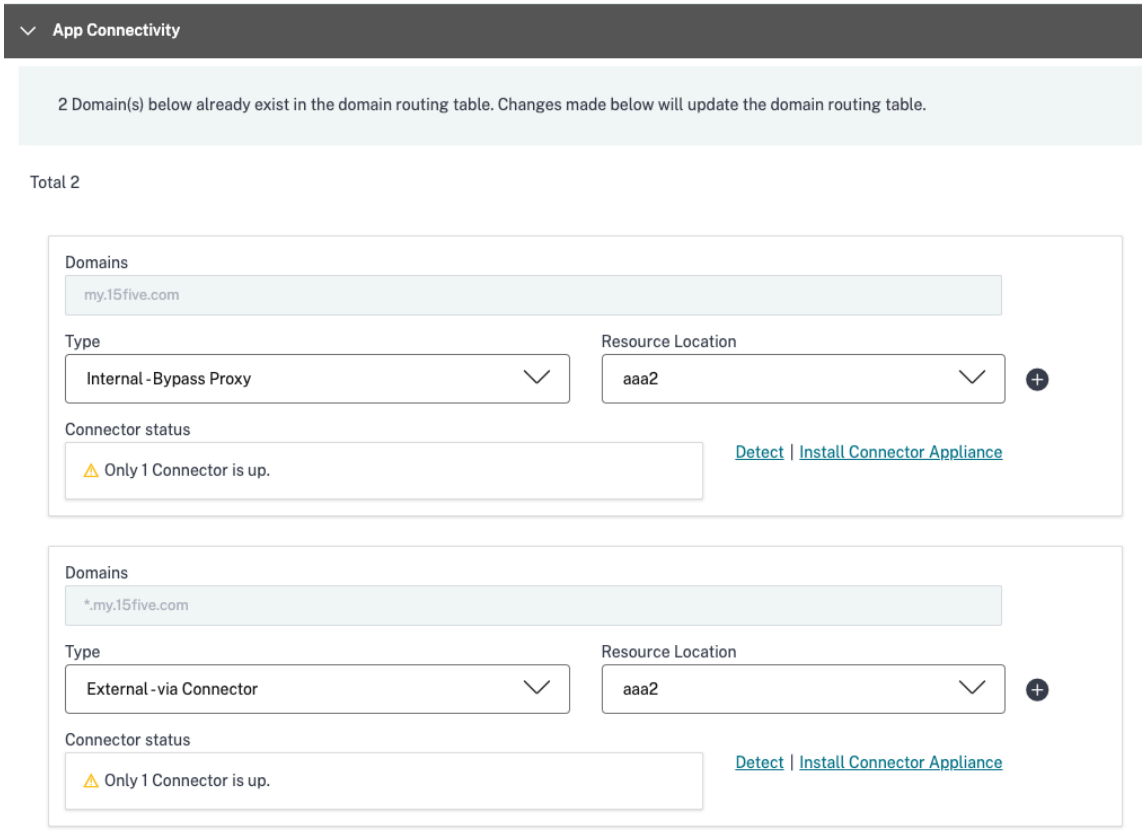
ミニルートテーブルにルートを追加するには

Citrix Secure Private Access サービスにアプリを追加する手順は、次の 2 つの変更点を除いて、「サービスとしてのソフトウェアアプリのサポート」および「エンタープライズ Web アプリのサポート」のトピックで説明されている手順と同じです。

1. 次の手順を実行します:

   - テンプレートを選択します。
   - アプリの詳細を入力します。
   - 必要に応じて、[拡張セキュリティ詳細] を選択します。
   - 必要に応じて、シングルサインオン方法を選択します。

2. [アプリの接続] をクリックします。-アプリケーションドメインテーブルのミニバージョンを使用して、アプリケーションの構成中にルーティングを決定できます。



   - ドメイン**:** [ドメイン] 列には、特定のアプリの 1 つ以上の行が表示されます。最初の行には、管理者がアプリの詳細を追加する際に入力した実際のアプリの URL が表示されます。その他の行は、アプリの詳細を追加するときに入力されるすべての関連ドメインです。アプリの URL と関連ドメインが同じ場合は、1 行に表示されます。

   SAML SSO が選択されている場合は、1 つの行に SAML アサーション URL が表示されます。

- タイプ**:** 次のいずれかのオプションを選択します。
  - [外部]: トラフィックはインターネットに直接流れます。
  - 内部—トラフィックは Connector Appliance 経由して流れ、アプリはウェブアプリとして扱われます。
    - Web アプリの場合、トラフィックはデータセンター内を流れます。
    - SaaS アプリケーションの場合、トラフィックは Connector Appliance 介してネットワーク外にルーティングされます。
  - 内部—プロキシをバイパスする -ドメイントラフィックは、コネクタアプライアンス上で構成されたお客様の Web プロキシをバイパスして、Citrix Cloud Connector アプライアンスを経由してルーティングされます。
  - コネクタ経由の外部—アプリケーションは外部ですが、トラフィックは Connector Appliance 経由して外部ネットワークに流れる必要があります。
- リソースの場所**:** アプリのタイプとして [内部] を選択すると自動入力されます。別のリソースの場所が必要な場合は、これを変更します。
- **Connector Appliance** ステータス**:** アプリの「内部」タイプを選択すると、リソースの場所とともに自動入力されます。

認可されていないウェブサイト

June 19, 2024

Secure Private Access 内で構成されていないアプリケーション (イントラネットまたはインターネット) は、「認可されていない Web サイト」とみなされます。デフォルトでは、Secure Private Access は、アプリケーションとアクセスポリシーが構成されていない限り、すべてのイントラネット Web アプリケーションへのアクセスを拒否します。

アプリが設定されていない他のすべてのインターネット URL または SaaS アプリケーションでは、管理者は管理コンソールから［設定］**>**［許可されていない **Web** サイト］タブを使用して、Citrix Enterprise Browser によるアクセスを許可または拒否できます。管理者はリモートブラウザ隔離 (RBI) 環境にアクセスをリダイレクトして、ブラウザベースの攻撃を防ぐこともできます。管理者が RBI への URL のリダイレクトを設定した場合、次のアクションが実行されます。

1. Secure Private Access がドメインを変換します。
2. その後、Citrix Enterprise Browser はこれらの URL を Secure Private Access に送り返します。
3. Secure Private Access は、これらの URL をリモートブラウザ分離サービスにリダイレクトします。

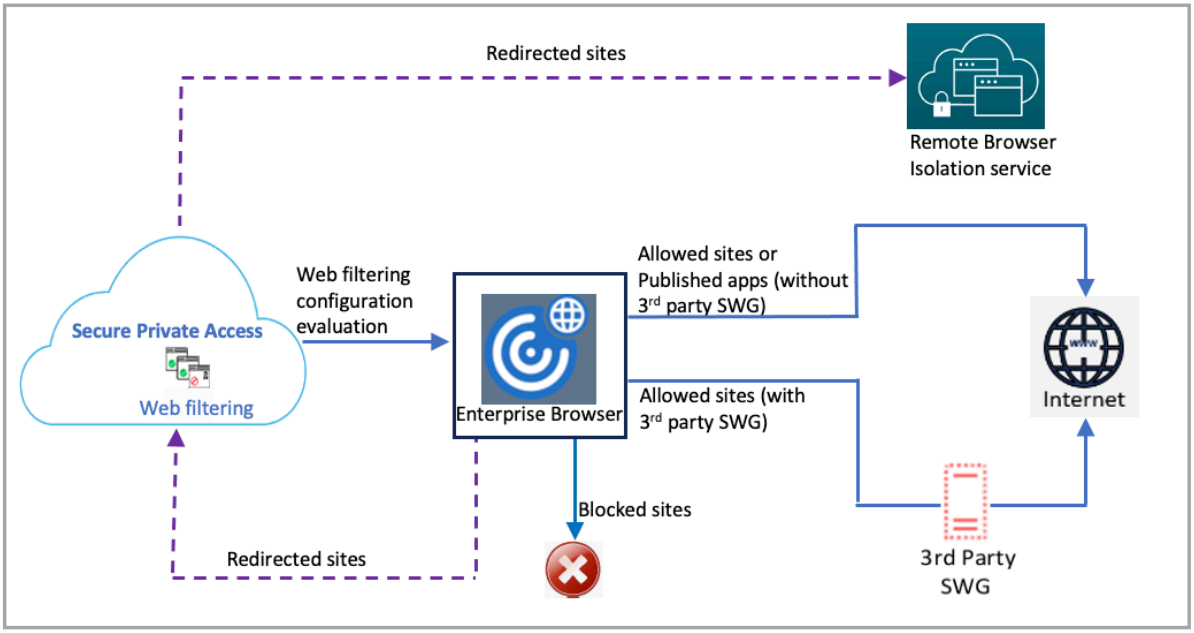
`*.example.com`などのワイルドカードを使用して、その Web サイトのすべてのドメインおよびそのドメイン内のすべてのページへのアクセスを制御できます。

> 注:
>
> デフォルトでは、Citrix Enterprise Browser 経由ですべてのインターネット URL または SaaS アプリへのアクセスを許可するように設定されています。

認可されていない **Web** サイトの仕組み

1. URL 分析チェックは、その URL が Citrix サービス URL であるかどうかを判断するために行われます。
2. その後、URL がエンタープライズ Web または SaaS アプリ URL であるかどうかが確認されます。
3. 次に、その URL がブロックされている URL であるかどうか、安全なブラウザセッションにリダイレクトする必要があるかどうか、URL へのアクセスを許可できるかどうかが確認されます。

次の図は、エンドユーザーのトラフィックフローを示しています。



要求が到着すると、次のチェックが実行され、対応するアクションが実行されます:

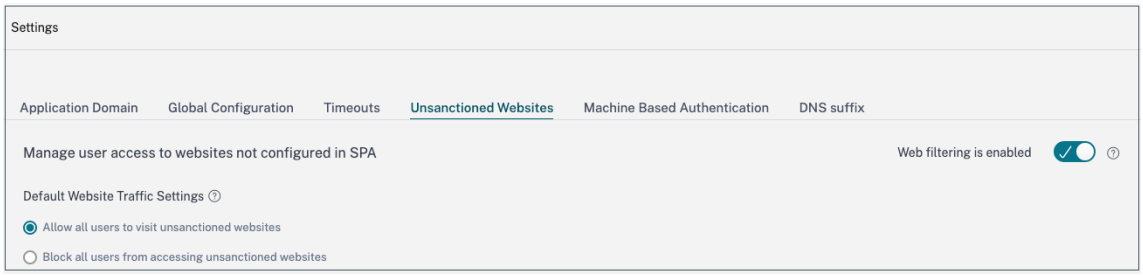
1. 要求はグローバル許可リストに一致していますか?
    a) 一致した場合、ユーザーは要求された Web サイトにアクセスできます。
    b) 一致しない場合、Web サイトリストがチェックされます。
2. 要求は顧客が構成した Web サイトリストに一致していますか?
    a) 一致する場合は、次の順序でアクションが決定されます。
        i. ブロック
        ii. リダイレクト

iii. 許可

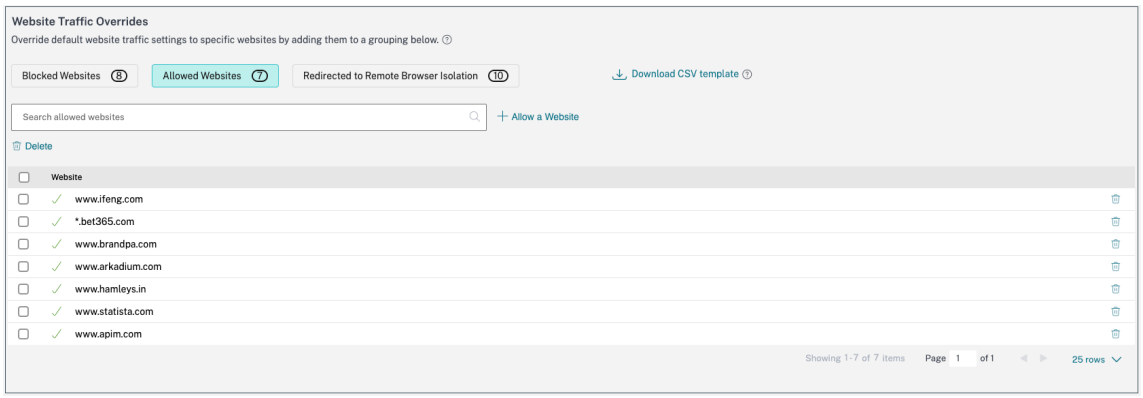
b) 一致しない場合、デフォルトのアクション（許可）が適用されます。デフォルトのアクションは変更できません。

認可されていない **Web** サイトのルールを設定

1. Secure Private Access コンソールで、**[** 設定**] > [**許可されていない **Web** サイト**]** をクリックします。



> 注記:
>
> - Web フィルタリング機能はデフォルトで有効になっており、許可されていないすべてのインターネット URL へのアクセスが許可されます。
> - 設定を「すべてのユーザーが認可されていない **Web** サイトにアクセスすることをブロックする」に変更して、すべてのユーザーが Citrix Enterprise Browser 経由ですべてのインターネット URL にアクセスすることをブロックできます。



特定の URL を、ブロックされている Web サイト、許可された Web サイトに追加したり、リモートブラウザ隔離リストにリダイレクトしたりして、設定を変更することもできます。

たとえば、許可されていないすべての URL へのアクセスをデフォルトでブロックしていて、一部の特定のインターネット URL のみへのアクセスを許可したい場合は、次の手順を実行してアクセスを許可できます:

a)「許可された **Web** サイト」タブをクリックし、「**Web** サイトを許可する」をクリックします。

b) アクセスを許可する必要がある Web サイトのアドレスを追加します。Web サイトのアドレスを手動で追加することも、Web サイトのアドレスを含む CSV ファイルをドラッグアンドドロップすることもできます。

c) [**URL** を追加] をクリックし、[保存] をクリックします。

URL が許可された Web サイトのリストに追加されます。

> 注:
>
> 有料のリモートブラウザ隔離標準サービスのお客様 (組織) は、デフォルトで年間 5,000 時間使用できます。さらに数時間かかる場合は、Secure Browser アドオンパックを購入する必要があります。リモートブラウザ隔離サービスの使用状況を追跡できます。詳しくは、次のトピックを参照してください:
>
> - Remote Browser Isolation を管理および監視する
> - リモートブラウザ分離。

ADFS と Secure Private Access の統合

January 9, 2024

要求ルールは、要求パイプラインを通る要求の流れを制御するために必要です。要求ルールは、要求ルールの実行プロセス中に要求フローをカスタマイズするためにも使用できます。クレームについて詳しくは、Microsoft のドキュメントを参照してください。

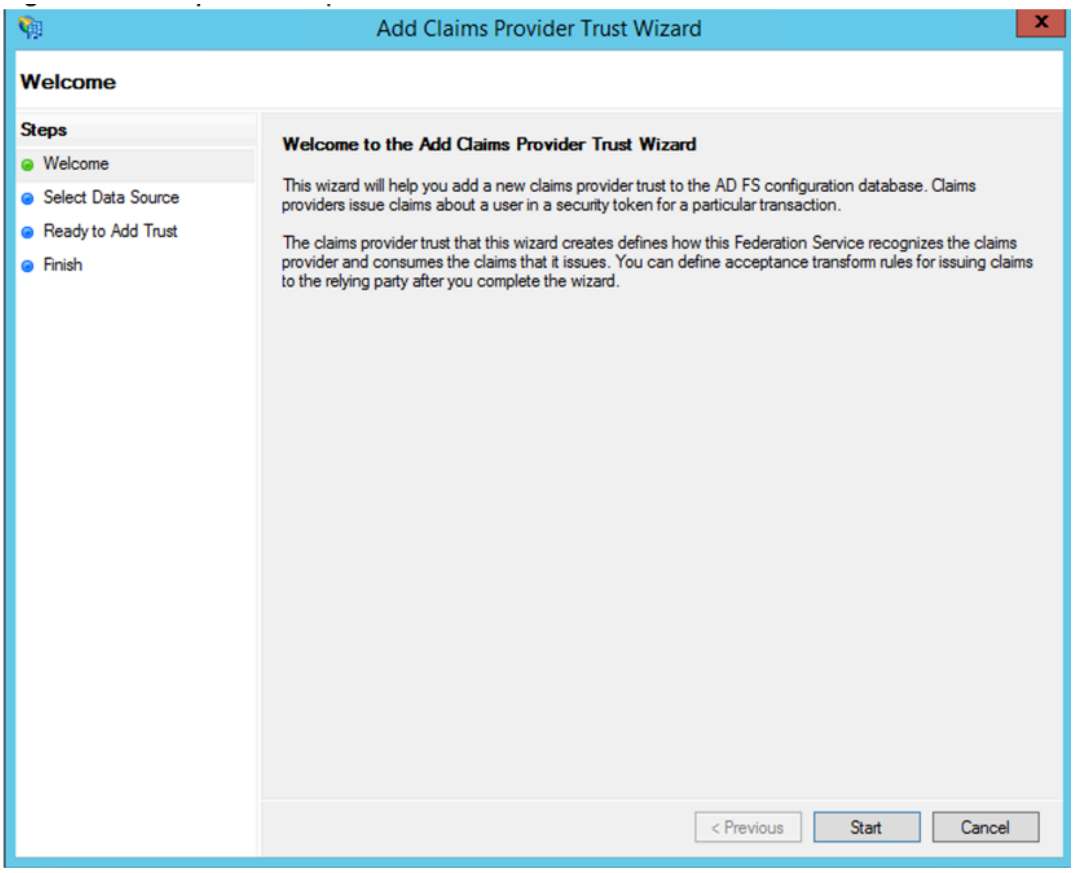
Citrix Secure Private Access からの要求を受け入れるように ADFS を設定するには、次の手順を実行する必要があります。

1. ADFS に要求プロバイダーの信頼を追加します。
2. Citrix Secure Private Access でアプリ構成を完了します。

ADFS にクレームプロバイダーの信頼を追加する

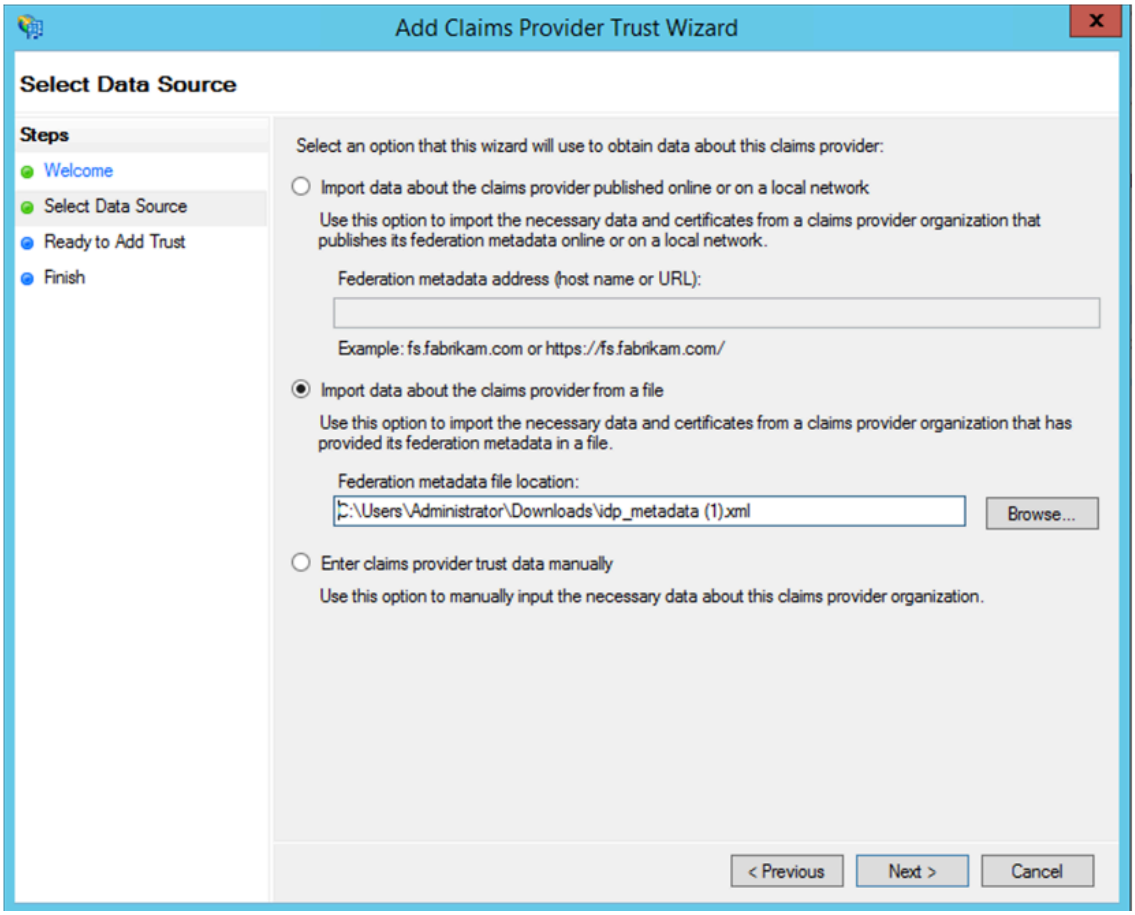
1. ADFS 管理コンソールを開きます。[**ADFS] > [**信頼関係**] > [**クレームプロバイダの信頼] に移動します。

   a) 右クリックして、[要求プロバイダの信頼を追加] を選択します。



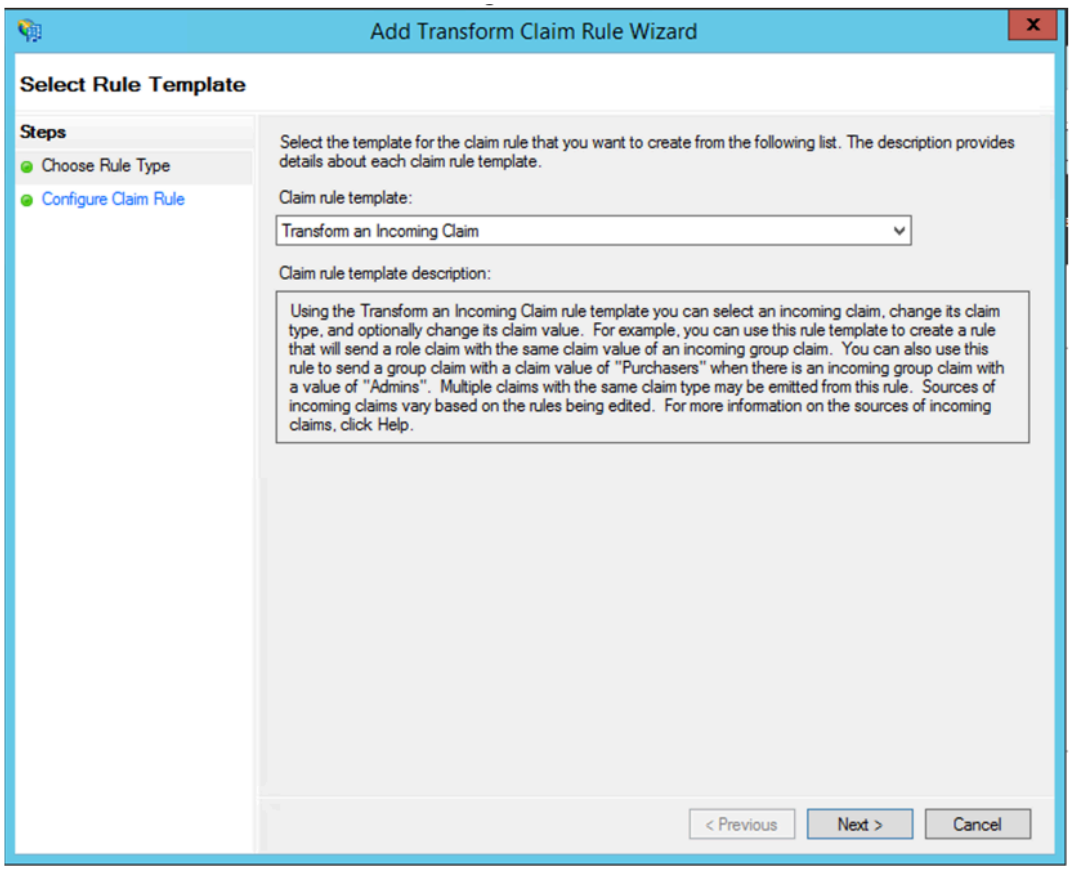
b) ADFS へのフェデレーションに使用されるアプリケーションを Secure Private Access に追加します。
詳しくは、「Citrix Secure Private Access でのアプリ構成」を参照してください。

> 注:
>
> まずアプリを追加し、アプリケーションの SSO 設定セクションから SAML メタデータファイルをダウンロードし、メタデータファイルを ADFS にインポートします。

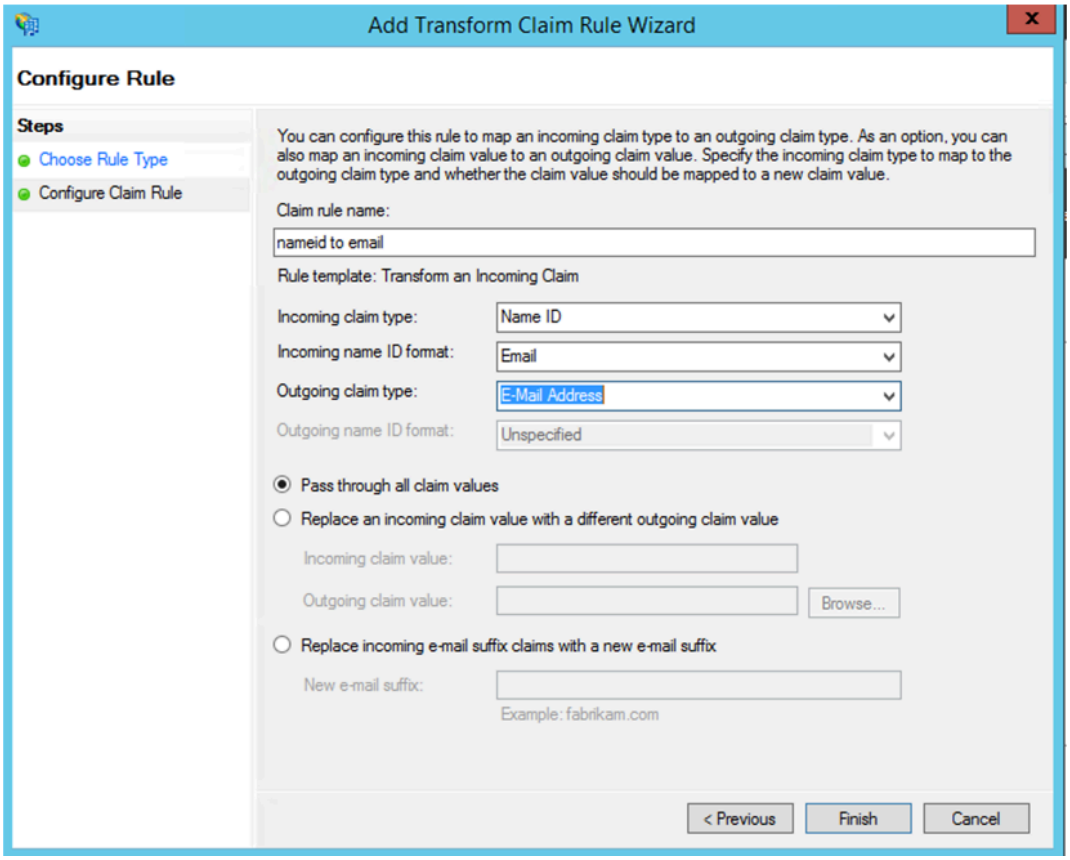


a) クレームプロバイダーの信頼の追加を完了する手順を完了します。要求プロバイダーの信頼の追加が完了すると、要求ルールを編集するウィンドウが表示されます。

b) [受信要求を変換] を使用して要求ルールを追加します。



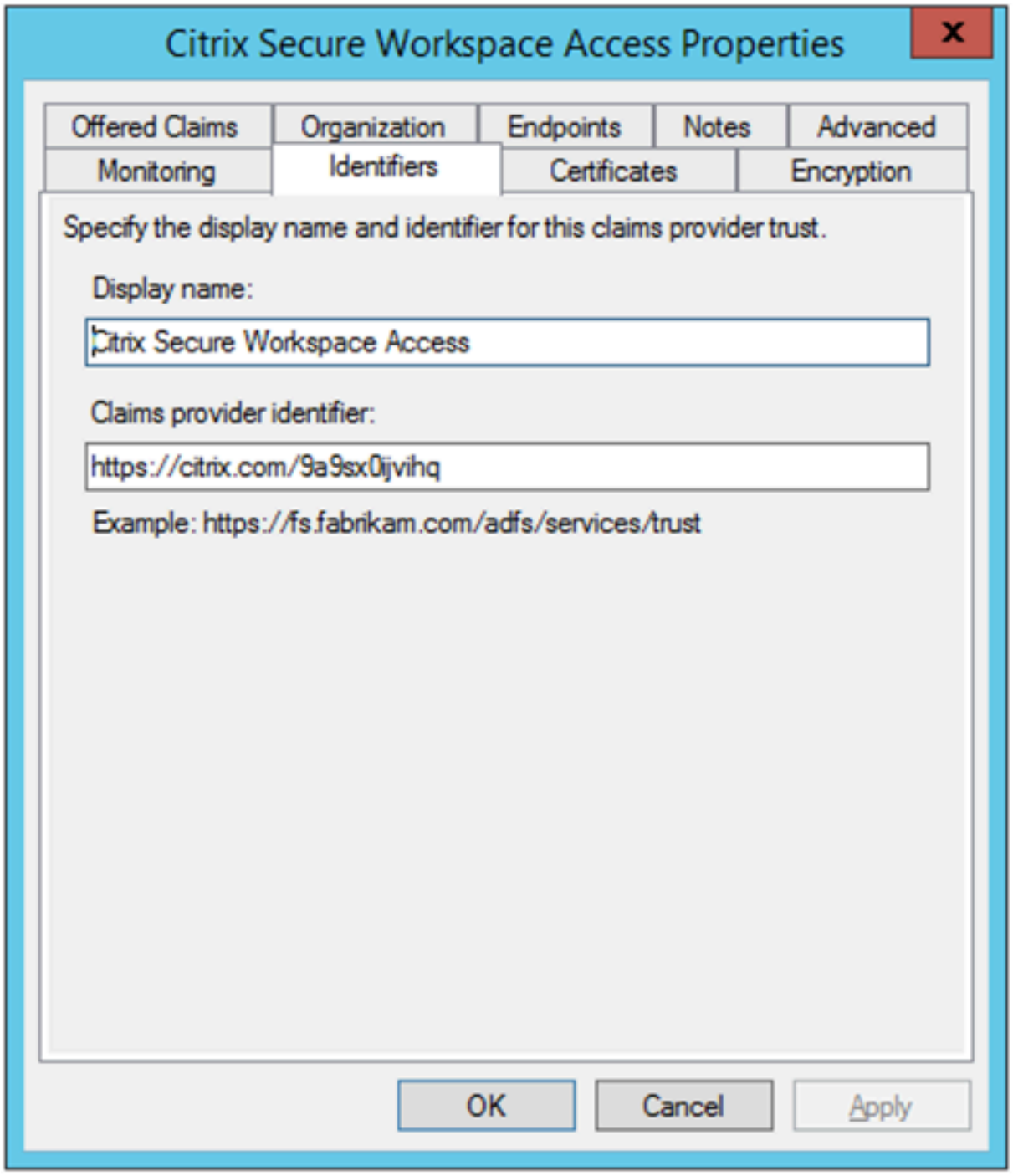
c) 次の図に示すように、設定を完了します。ADFS が他のクレームを受け入れる場合は、それらのクレームを使用し、それに応じて Secure Private Access で SSO も設定します。



これで、ADFS が SAML 用の Citrix Secure Private Access を信頼するようになったことを確認する要求プロバイダーの信頼が構成されました。

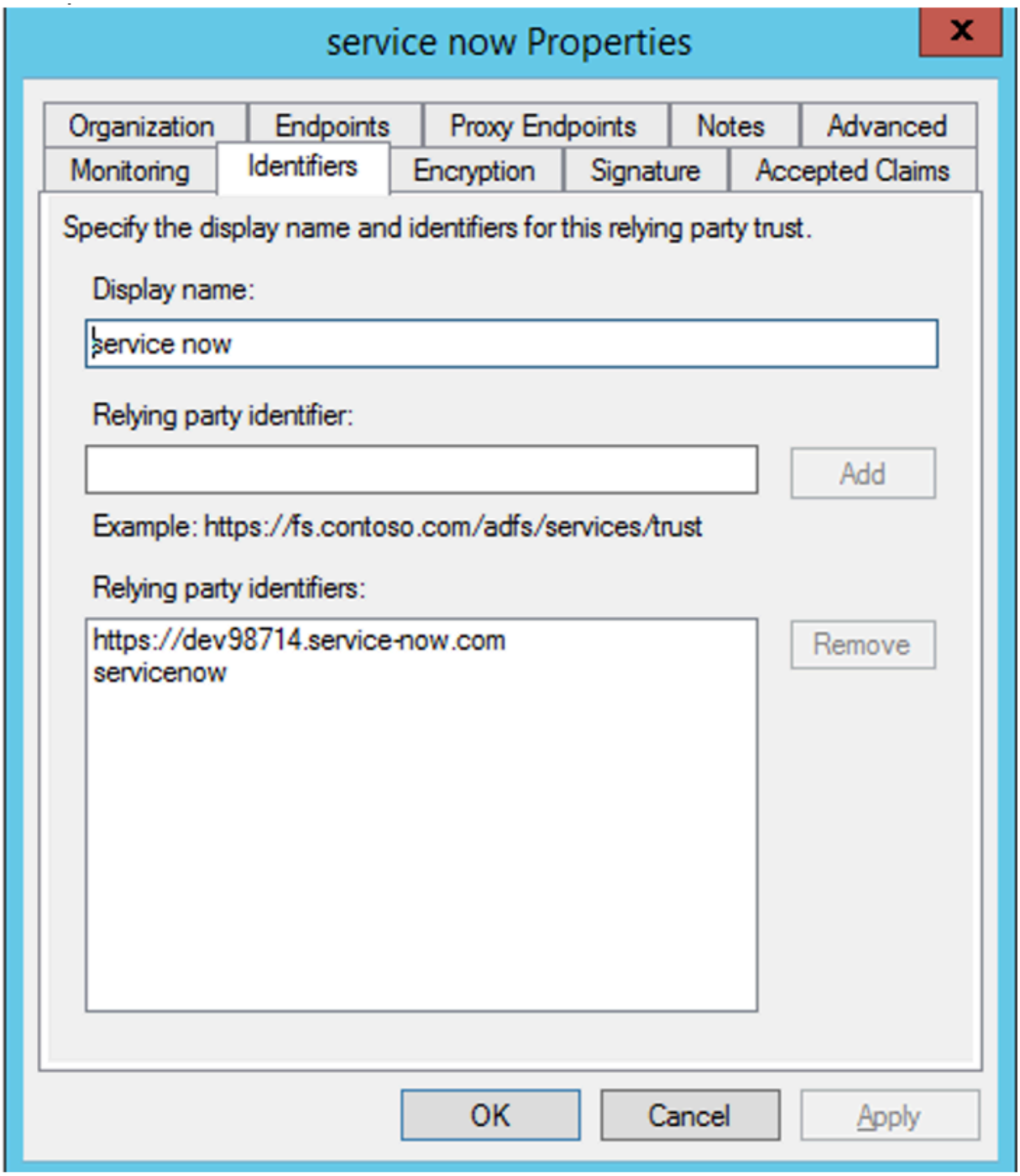
クレームプロバイダの信頼 **ID**

追加したクレームプロバイダーの信頼 ID を書き留めます。この ID は、Citrix Secure Private Access でアプリを構成する際に必要です。



パーティ識別子のリレー

SaaS アプリがすでに ADFS を使用して認証されている場合は、そのアプリに中継者信頼がすでに追加されている必要があります。この ID は、Citrix Secure Private Access でアプリを構成する際に必要です。



IdP 開始フローでリレー状態を有効にする

RelayState は SAML プロトコルのパラメーターで、ユーザーがサインインして証明書利用者のフェデレーションサーバーに送信された後にアクセスする特定のリソースを識別するために使用されます。RelayState が ADFS で有効になっていない場合、ユーザーはそれを必要とするリソースプロバイダーに対して認証した後にエラーが表示されます。

ADFS 2.0 では、RelayState サポートを提供する更新プログラム KB2681584 (更新プログラムのロールアップ 2) または KB2790338 (更新プログラムのロールアップ 3) をインストールする必要があります。ADFS 3.0 には RelayState サポートが組み込まれています。どちらの場合も、RelayState を有効にする必要があります。

ADFS サーバーで **RelayState** パラメーターを有効にするには

1. ファイルを開きます。
   - ADFS 2.0 の場合は、メモ帳に次のファイルを入力します:%systemroot%\ inetpub\ adfs\ ls\ web.config
   - ADFS 3.0 の場合は、メモ帳に次のファイルを入力します:%systemroot%\ ADFS\ Microsoft.IdentityServer.serviceHost.exe.config
2. Microsoft.IdentityServer.Web セクションで、次のように userelyStateForidpInitiatedSignon の行を追加し、変更を保存します。
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - ADFS 2.0 の場合は、`IISReset` を実行して IIS を再起動します。
3. どちらのプラットフォームでも、Active Directory フェデレーションサービスを再起動します。(`adfssrv`)`service`.
   注**:** Windows 2016 または Windows 10 を使用している場合は、次の PowerShell コマンドを使用して有効にします。
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

コマンドへのリンク- https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

Citrix Secure Private Access でのアプリ構成

IdP 開始フローまたは SP 開始フローを設定できます。Citrix Secure Private Access で IdP または SP が開始するフローを構成する手順は同じですが、SP が開始するフローの場合、UI で［指定された **URL** を使用してアプリを起動する（**SP** 開始)］チェックボックスをオンにする必要があります。

IdP 開始されたフロー

1. IdP 開始フローを設定するときに、次のように設定します。
   - [アプリ **URL**] —アプリ URL に次の形式を使用します。
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```


- **ADFS** 完全修飾名—ADFS セットアップの FQDN。
- **RP ID**： RP ID は、リレー当事者の信頼から取得できる ID です。これは、リレーパーティ識別子と同じです。それが URL であれば、URL エンコーディングが発生します。
- **IDP ID** —IdP ID は、クレームプロバイダーの信頼 ID と同じです。それが URL であれば、URL エンコーディングが発生します。

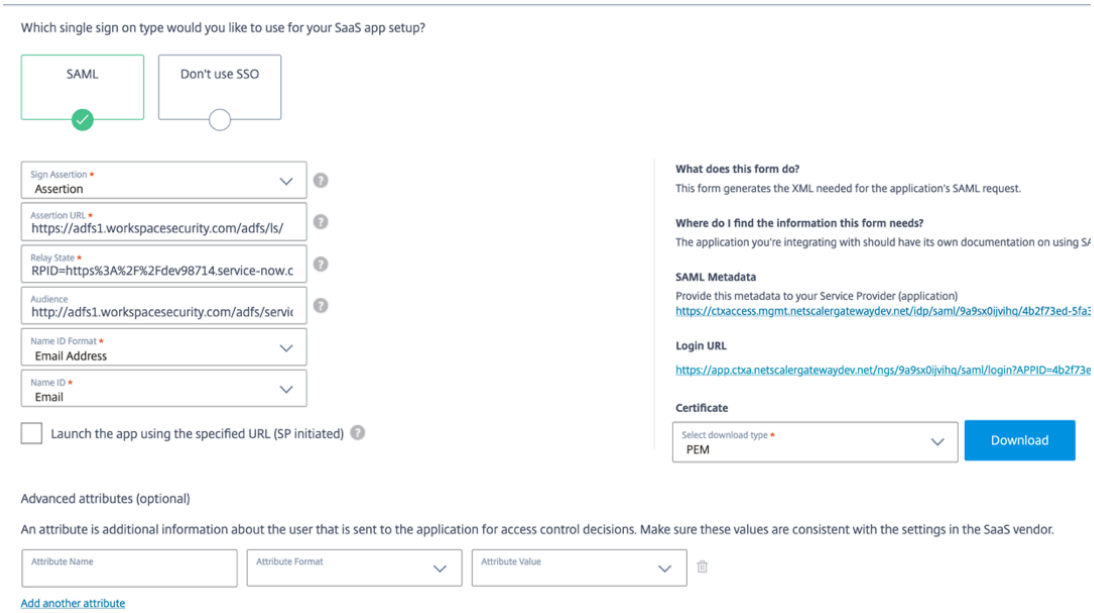
  例**:** https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. SAML SSO 設定。

   ADFS サーバーのデフォルト値は次のとおりです。いずれかの値を変更した場合は、ADFS サーバーのメタデータから正しい値を取得します。ADFS サーバーのフェデレーションメタデータは、そのフェデレーションメタデータエンドポイントからダウンロードできます。そのエンドポイントは、**ADFS >** サービス **>** エンドポイントから確認できます。

   - アサーション **URL** —`https://<adfs fqdn>/adfs/ls/`
   - リレー状態: IdP が開始したフローでは、リレーステートが重要です。それを正しく構築するには、このリンクに従ってください- `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     例**:** RPID=https%3A%2FDEV98714.service-now.com&relayState=https%3a%2FDEV98714.service-now.com%2F
   - オーディエンス—`http://<adfsfqdn>/adfs/services/trust`
   - その他の SAML SSO 構成設定については、次の図を参照してください。詳しくは、「https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html」を参照してください



3. アプリを保存し、ユーザーにサブスクライブします。

SP 開始されたフロー

SP 開始フローの場合は、[**IDP** 開始フロー] セクションでキャプチャされた設定を構成します。さらに、[指定した **URL (SP** 開始**)** を使用してアプリを起動する] チェックボックスをオンにします。

Secure Private Access の問題のトラブルシューティング

June 19, 2024

このトピックを使用して、アプリ構成、認証、SSO、またはアプリアクセス関連の問題のトラブルシューティングを行います。Secure Private Access 診断ログ内の「情報コード」列から情報コードをコピーし 、このページでそのコードを検索して、対応するトラブルシューティング手順を見つけてください。以下は、このトピックをよりよく理解するのに役立ついくつかの FAQ です。

よくある質問**?**

Secure Private Access 診断ログとは何ですか?

Secure Private Access ・ログはどこで確認できますか?

Secure Private Access の診断ログにはどのような詳細がありますか?

Secure Private Access の診断ログにはどのようなイベントが記録されますか?

Secure Private Access のトラブルシューティングトピックを使用して、発生した障害を解決する方法を教えてください。

情報コードとは? どこで見つけられますか?

トランザクション ID とは何ですか? どうやって使うの?

Secure Private Access の PoP ロケーションにはどのようなものがありますか?

情報コードとエラー検索テーブルを使用してもエラーを解決できない場合はどうすればよいですか?

情報コード検索テーブル

次のエラールックアップテーブルは、Secure Private Access サービスの使用時にユーザーが遭遇する可能性のあるさまざまなエラーの包括的な概要を示しています。

情報コード	Description	解像度
0x180006、0x1800B7	アプリの FQDN の長さを超えたため、アプリの起動に失敗しました	アプリの FQDN の長さを超えたため、アプリの起動に失敗しました
0x180022	認証サービスが停止しているため、アプリの起動に失敗しました	認証サービスが停止しているため、アプリの起動に失敗しました
0x180001、0x18001A、0x18001B、0x18008A 0x1800A9、0x1800AA、0x1800AB、0x1800AC 0x1800AD、0x1800AE、0x1800AF、0x1800B0 0x1800B1、0x1800B2、0x1800B3、0x180048	シングルサインオンエラー、Citrix Cloud とオンプレミスコネクタ間の接続確立の失敗、SAML SSO の失敗、アプリの FQDN が無効です	アプリアクセスが拒否されました
0x1800EF	Connector Appliance への接続に関する問題	Connector Appliance への接続に関する問題
0x18009D	DNS 検索/接続失敗	Secure Browser サービス-DNS ルックアップ/接続エラー
0x1800A0、0x1800A2、0x1800A3、0x1800A5 0x1800A6、0x1800A7	バックエンド Web アプリに接続できないため、Web アプリの起動に失敗しました	バックエンド Web アプリに接続できないため、Web アプリの起動に失敗しました
0x1800BC, 0x1800BF	ユーザーには Web/SaaS アプリにアクセスする権限がありません	ユーザーには Web/SaaS アプリにアクセスする権限がありません

情報コード	Description	解像度
0x1800BD	ユーザーには DirectAccess の Web/SaaS アプリケーションにアクセスする権限がありません	ユーザーには DirectAccess の Web/SaaS アプリケーションにアクセスする権限がありません
0x1800D0	アプリケーション構成を取得しているときに、Citrix Secure Access Agent のセッション起動が失敗しました	アプリケーション構成を取得しているときに、Citrix Secure Access Agent のセッション起動が失敗しました
0x1800CD、0x1800CE、0x1800D6、0x1800EA	Citrix Secure Access Agent のアプリケーション構成の取得中にセッションの起動が失敗しました、ポリシー評価中に Citrix Secure Access Agent アプリケーションの起動が失敗しました、Citrix Secure Access Agent アプリケーションの起動が失敗しました	不正な形式のクライアント要求
0x1800DE	ポリシー評価中に Citrix Secure Access Agent アプリケーションの起動に失敗しました	ポリシー評価中に Citrix Secure Access Agent アプリケーションの起動に失敗しました
0x180055、0x1800DF、0x1800E3	コンテキストポリシーによりアプリが制限されている、ポリシー設定によりアクセスが拒否された	ユーザーダッシュボードにリストされていない 1 つ以上のアプリ
0x1800EB	IPv6 がサポートされていないため、Citrix Secure Access Agent アプリケーションの起動に失敗しました	IPv6 がサポートされていないため、Citrix Secure Access Agent アプリケーションの起動に失敗しました
0x1800EC, 0x1800ED	IP アドレスが無効なため、Citrix Secure Access Agent アプリケーションの起動に失敗しました	IP アドレスが無効なため、Citrix Secure Access Agent アプリケーションの起動に失敗しました
0x10000001, 0x10000002, 0x10000003, 0x10000004	ネットワークの問題による Citrix Secure Access クライアントのログイン失敗	Citrix Secure Access クライアントでのネットワーク接続の接続性の問題
0x10000006	プロキシが途中で発生するため、Citrix Secure Access クライアントのログインが失敗する	プロキシサーバーがクライアントとサービスの接続を妨害している
0x10000007	信頼できない認証局による Citrix Secure Access クライアントのログイン失敗	信頼できないサーバー証明書の問題が確認されました

情報コード	Description	解像度
0x10000008	証明書が無効なため、Citrix Secure Access クライアントのログインが失敗しました	無効なサーバー証明書の問題が見つかりました
0x1000000A	構成の問題が原因で Citrix Secure Access クライアントにログインできない	ユーザーの構成が空であるため、ログインできませんでした
0x1000000B	接続障害による Citrix Secure Access クライアントのログイン障害	接続はネットワークまたはエンドユーザーによって終了されました
0x10000010	セッションの期限切れによる Citrix Secure Access クライアントのログイン障害	セッションの有効期限が切れたため、設定のダウンロードに失敗しました
0x10000013	構成リストが膨大なため、Citrix Secure Access クライアントのログインに失敗する	Citrix Secure Access クライアントがログインに失敗しました
0x11000003	コントロールチャネル作成の失敗による Citrix Secure Access クライアントのログイン障害	セッションの有効期限が切れたため、コントロールチャネルを確立できませんでした
0x11000004	コントロールチャネル作成の失敗による Citrix Secure Access クライアントのログイン失敗	コントロールチャネルを確立できませんでした
0x11000005	コントロールチャネル作成の失敗による Citrix Secure Access クライアントのログイン失敗	コントロールチャネルを確立できませんでした
0x11000006	コントロールチャネル作成の失敗による Citrix Secure Access クライアントのログイン失敗	ネットワークの問題により、コントロールチャネルを確立できませんでした
0x12000001	セッションがすでに期限切れになっているため、Citrix Secure Access クライアントのログアウトが失敗しました	セッションが終了したためログオフできません
0x12000002	セッションがすでにタイムアウトしているため、Citrix Secure Access クライアントのログアウトが失敗しました	セッションは強制終了されます

情報コード	Description	解像度
0x13000001	セッションの有効期限が切れたため、アプリケーションにアクセスできませんでした	セッションの有効期限が切れたため、アプリケーションを起動できませんでした
0x13000002	ライセンスが不十分なため、アプリにアクセスできませんでした	ライセンスの問題によりアプリケーションの起動に失敗しました
0x13000003、0x13000008、0x001800DF	アクセスが禁止されているためアプリへのアクセスが失敗し、ポリシーに従って TCP/UDP アプリの起動が拒否されました	サービスによってアクセスが拒否されたため、アプリケーションを起動できませんでした
0x13000004, 0x13000005	サーバーが使用できないため、アプリにアクセスできませんでした	クライアントがサービスにアクセスできないため、アプリケーションを起動できませんでした
0x13000007	アクセスポリシーが無効になっているか、ユーザーが登録されていないため、アプリにアクセスできませんでした	ポリシー評価と設定の検証が失敗したため、アプリケーションの起動に失敗しました
0x13000009	ルーティングエントリがないため、アプリにアクセスできませんでした	アプリケーションドメインテーブルの問題により、アプリケーションを起動できませんでした
0x1300000B	クライアントは接続を閉じました	クライアントは Secure Private Access ・サービスとの接続を終了しました
0x1300000C	ZTNA に関する FQDN 解決が失敗しました	DNS サーバーで FQDN を解決できません
0x001800D3	ログイン中にアプリケーション構成をダウンロードできない	設定済みのアプリケーション宛先リストを取得できませんでした
0x001800D9、0x001800DA	ポリシー評価応答の解析中に TCP/UDP アプリケーションの起動が失敗しました。ポリシー評価中に TCP/UDP アプリケーションの起動が失敗し、結果が無効になりました。	アプリケーション設定の問題
0x001800DB	リソースの場所の設定が無効なため、TCP/UDP アプリケーションの起動が失敗しました	リソースの場所に関する問題

情報コード	Description	解像度
0x13000006, 0x001800DC, 0x001800DD	TCP アプリに設定されたサポートされていない拡張セキュリティポリシーが原因で TCP アプリの起動が失敗しました。TCP アプリに設定された Secure Browser サービスリダイレクトがサポートされていないため、TCP アプリの起動が失敗しました	強化されたセキュリティポリシーは HTTP アプリケーションにバインドされます
0x001800DE	宛先のアプリケーション構成が見つからなかったため、TCP/UDP アプリケーションの起動に失敗しました	アプリケーションが見つからない
0x001800EA	宛先 FQDN が長すぎるため、TCP アプリの起動に失敗しました	ホスト名の長さが 256 文字を超えています
0x001800ED	宛先 IP が無効なため、TCP アプリケーションの起動に失敗しました	IP アドレスが無効です
0x001800EF	プライベート TCP サーバーへの接続確立中に TCP アプリの起動が失敗しました	エンドツーエンド接続を確立できません
0x001800F5	IPV6 アドレスが原因で UDP アプリケーションの起動に失敗しました	アプリリクエストで受信した IPv6
0x001800F9	クライアント接続が失われたため、UDP トラフィックを配信できませんでした	UDP トラフィックの配信失敗
0x001800FF	UDP データトラフィックの配信に失敗しました	UDP データトラフィックの配信に失敗しました
0x10000401	Citrix ランデブーサーバーのダイヤルが失敗しました	ネットワーク接続の問題によりアプリケーションの起動に失敗しました
0x10000402, 0x1000040C	Connector Appliance を登録できません。UDP ネットワーク接続の初期化が失敗しました	Connector Appliance は Secure Private Access サービスに登録できませんでした
0x10000403、0x10000404、0x10000407、0x1000040A 0x1000040B、0x1000040F、0x10000410	接続エラー、制御パケット送信失敗、ゲートウェイサービス読み取りエラー、制御パケット解析失敗、ゲートウェイサービス書き込みエラー	Connector Appliance との接続問題
0x10000405、0x10000408、0x10000409、0x1000040D 0x1000040E、0x10000412	バックエンド接続不可、UDP パケット送信失敗、UDP パケット受信失敗、バックエンド書き込みエラー、バックエンド接続クローズ	Connector Appliance バックエンドのプライベート TCP/UDP サーバーとの接続の問題

情報コード	Description	解像度
0x10000406	DNS 解決に失敗しました	Connector Appliance が FQDN の DNS を解決できない
0x10000411	ゲートウェイサービスが接続を終了しました	プライベートサーバー接続が終了しました
0x10000413	接続ティアダウンの理由を判断中にエラーが発生しました	プライベートサービス IP または FQDN に接続またはデータを送信できませんでした
0x100508	ユーザーコンテキストがアクセスルールの条件と一致しない	一致するポリシー条件なし
0x100509	アプリケーションに関連付けられていないアクセスポリシー	アプリケーションにはアクセスポリシーが関連付けられていません
0x10050C	ユーザーが利用資格を持つ可能性のある複数のアプリケーションのポリシー評価結果	アプリ列挙情報
0x00180101	アプリケーションドメインテーブルにルーティングエントリがないため、TCP/UDP アプリケーションの起動に失敗しました	アプリケーションドメインテーブルにルーティングエントリがないため、TCP/UDP アプリケーションの起動に失敗しました
0x00180102	コネクタが正常でないため、TCP/UDP アプリの起動に失敗しました	コネクタが正常でないため、TCP/UDP アプリの起動に失敗しました
0x00180103	コネクタにアクセスできないため、UDP/DNS 要求が失敗しました	コネクタにアクセスできないため、UDP/DNS 要求が失敗しました
0x20580001	NGS Cookie の有効期限が切れているため、ページを読み込めませんでした	NGS Cookie の有効期限が切れているため、ページを読み込めませんでした
0x20580002	ネットワーク障害のため、アクセスポリシーの取得に失敗しました	ネットワーク障害のため、アクセスポリシーの取得に失敗しました
0x20580003	JSON Web トークンの解析中にアクセスポリシーの取得が失敗しました	JSON Web トークンの解析中にアクセスポリシーの取得が失敗しました
0x20580004	ネットワークがアクセスポリシーの詳細を取得できませんでした	ネットワークがアクセスポリシーの詳細を取得できませんでした

情報コード	Description	解像度
0x20580005	パブリック証明書のフェッチ中にポリシーのフェッチが失敗しました	パブリック証明書のフェッチ中にポリシーのフェッチが失敗しました
0x20580007	JWT の署名を検証中にポリシーの取得に失敗しました	JWT の署名を検証中にポリシーの取得に失敗しました
0x20580008	公開証明書の検証中にポリシーの取得に失敗しました	公開証明書の検証中にポリシーの取得に失敗しました
0x2058000A	ポリシー URL を作成するためのストア環境を決定できませんでした	ポリシー URL を作成するためのストア環境を決定できませんでした
0x2058000B	アクセスポリシー取得要求の応答を取得できませんでした	アクセスポリシー取得要求の応答を取得できませんでした
0x2058000C	セカンダリ DS 認証トークンの期限が切れているため、アクセスポリシーの取得に失敗しました	セカンダリ DS 認証トークンの期限が切れているため、アクセスポリシーの取得に失敗しました
0x10200002	Connector Appliance が登録されていません	Connector Appliance が登録されていません
0x10200003	Connector Appliance に接続できません	Connector Appliance に接続できません
0x10000301	Citrix SPA サービスへの接続に失敗しました	Citrix Secure Private Access サービスへの接続に失敗しました
0x10000303, 0x10000304	プロキシサーバーにアクセスできない	プロキシサーバーにアクセスできない
0x10000305	プロキシサーバーの認証が失敗しました	プロキシサーバーの認証が失敗しました
0x10000306	設定したプロキシサーバーにアクセスできない	設定したプロキシサーバーにアクセスできない
0x10000307	バックエンドサーバーからエラー応答を受信しました	バックエンドサーバーからエラー応答を受信しました
0x10000005	ターゲット URL にリクエストを送信できません	ターゲット URL にリクエストを送信できません
0x10000107	SSO を処理できませんでした	SSO を処理できませんでした
0x10000108、0x1000010B	SSO を処理できませんでした。SSO 設定を確認できません	SSO を処理できませんでした。SSO 設定を確認できません

情報コード	Description	解像度
0x10000101, 0x10000102, 0x10000103, 0x10000104	FormFill SSO が失敗しました。フォームアプリの設定が正しくありません	FormFill SSO が失敗しました。フォームアプリの設定が正しくありません
0x1000010A	FormFill SSO が失敗しました。フォームアプリの設定が正しくありません	FormFill SSO が失敗しました。フォームアプリの設定が正しくありません
0x10000202	Kerberos SSO が失敗しました	Kerberos SSO が失敗しました
0x10000203	認証タイプの SSO を処理できませんでした	認証タイプの SSO を処理できませんでした
0x10000204	Kerberos SSO は失敗しましたが、NTLM にフォールバックしました	Kerberos SSO は失敗しましたが、NTLM にフォールバックしました
0x14000001	Citrix Workspace アプリケーションで構成された複数の ZTNA 資格のあるアカウント	Citrix Workspace アプリケーションで構成された複数の ZTNA 資格のあるアカウント

解決手順

以下のセクションでは、ほとんどの情報コードの解決手順を説明します。解決手順がキャプチャされていないコードについては、Citrix サポートにお問い合わせください。

ユーザーダッシュボードにリストされていない **1** つ以上のアプリ

情報コード**:** 0x180055、0x1800DF、0x1800E3

コンテキストポリシー設定により、一部のユーザーまたはデバイスではアプリが表示されない場合があります。信頼係数（デバイスポスチャまたはリスクスコア）などのパラメータは、アプリケーションのアクセシビリティに影響を与える可能性があります。

1. 診断ログ csv ファイルのエラーコード`0x18005C`の`reasons`列からトランザクション ID をコピーします。
2. CSV ファイルの`prod`列フィルタを変更して、`SWA.PSE`または`SWA.PSE.EVENTS`というコンポーネントからのイベントを表示します。このフィルタは、ポリシー評価に関連するログのみを表示します。
3. `reason` 列で評価されたポリシーペイロードを検索します。このペイロードは、ユーザーがサブスクライブしているすべてのアプリについて、ユーザーのコンテキストに対して評価されたポリシーを表示します。
4. ポリシー評価で、ユーザーに対してアプリが拒否されたと示される場合、考えられる理由は次のとおりです。
    - ポリシーの一致条件が正しくありません-Citrix Cloud のアプリポリシー構成を確認してください

- ポリシーの一致ルールが正しくありません-Citrix Cloud のアプリポリシー構成を確認してください
- ポリシーのデフォルトルールに正しく一致しない-これはフォールスルーケースです。条件を適宜調整します。

ユーザーには **Web/SaaS** アプリにアクセスする権限がありません

情報コード**:** 0x1800BC、0x1800BF

ユーザーがサブスクリプションを持っていないアプリのリンクをクリックした可能性があります。

ユーザーがアプリケーションのサブスクリプションを持っていることを確認します。

1. 管理ポータルのアプリケーションに移動します。
2. アプリを編集し、[サブスクリプション] タブに移動します。
3. 対象となるユーザーがサブスクリプションリストにエントリを持っていることを確認してください。

バックエンドアプリのパフォーマンスが遅い

情報コード**:**0x18000F

リソースの場所のコネクタがダウンしている場合や、バックエンドサーバー自体が応答していないために、お客様のネットワークが不安定な場合があります。

1. ネットワーク遅延が発生しないように、Connector Appliance がバックエンドサーバーに地理的に近い場所に配置されていることを確認してください。
2. バックエンドサーバーのファイアウォールが Connector Appliance をブロックしていないかどうかを確認します。
3. クライアントが最も近いクラウド POP に接続しているかどうかを確認します。

   たとえば、クライアントの`nslookup nssvc.dnsdiag.net`では、回答の正規名は次のような地域固有のサーバーを`aws-us-w.g.nssvc.net.`で示します。

アプリの **FQDN** の長さを超えたため、アプリの起動に失敗しました

情報コード**:** 0x180006、0x1800B7

アプリの FQDN は 512 文字を超えてはなりません。アプリ構成ページでアプリケーションの FQDN を確認します。長さが 512 バイトを超えないようにしてください。

1. 管理コンソールの [アプリケーション] タブに移動します。
2. FQDN が 512 文字を超えるアプリケーションを探します。
3. アプリケーションを編集し、アプリの FQDN の長さを修正します。

アプリの詳細の長さを超えました

情報コード**:** 0x18000E

ポリシーがアプリアクセスをブロックしているかどうかを確認してください。

1.「アクセスポリシー」に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザーのポリシールールと条件を確認します。

アプリアクセスが拒否されました

情報コード：0x180001、0x18001A、0x18001B、0x18008A、0x1800A9、0x1800AB、0x1800AC、0x1800AD、0x1800AE、0x1800AF、0x1800B0、0x1800B1、0x1800B2、0x1800B3、0x180048

これはコンテキストポリシーに関連しており、ポリシーによって特定のユーザーのアプリが拒否されます。

ポリシーがアプリアクセスをブロックしているかどうかを確認する

1.「アクセスポリシー」に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザーのポリシールールと条件を確認します。

アプリケーションが列挙されていません

ポリシーが拒否されたり、Secure Private Access 統合が有効になっていないために、アプリケーションが列挙されたリストから見つからないことがあります。

- 一部のアプリでアクセスを有効にする必要があるのにアプリが表示されない場合は、Secure Private Access 統合を有効にしてみてください。
  - Citrix Cloud にサインインします。
  - ハンバーガーメニューから「ワークスペース構成」を選択し、「サービス統合」をクリックします。
  - **Secure Private Access** の省略記号ボタンをクリックし、「有効にする」をクリックします。
- Secure Private Access 統合がすでに有効になっている場合は、無効にしてから再度有効にして、アプリがあるかどうかを確認してください。

Connector Appliance への接続に関する問題

情報コード**:** 0x1800EF

オンプレミスコネクタとの TCP 接続が利用できないため、アプリケーションのルーティングが失敗します。

コントローラーコンポーネントからのイベントを確認する

1. 診断ログ csv ファイルでエラーコード0x1800EFのtransaction IDを検索します。
2. csv ファイル内のトランザクション ID と一致するすべてのイベントをフィルタリングします。
3. また、SWA.GOCTRLに一致する CSV ファイルのprod列をフィルタリングします。

   connectTypeメッセージmulticonnect::successのイベントが表示されたら? 次に;

   - これは、トンネル確立要求がコントローラに正常に中継されたことを示します。
   - ログメッセージ内のResource Locationが正しいか確認してください。正しくない場合は、Citrix 管理ポータルのアプリ構成セクションでリソースの場所を修正します。
   - ログメッセージ内のVDA Ip and Portが正しいか確認してください。VDA IP とポートは、バックエンドアプリケーションの IP とポートを示します。正しくない場合は、Citrix 管理ポータルのアプリ構成セクションでアプリの FQDN または IP アドレスを修正します。
   - 前述の問題が見つからない場合は、コネクタのイベントを確認します 。

   connectTypeメッセージconnect::failureまたはmulticonnect::successの付いたイベントが表示された場合は、

   - このログメッセージに対する推奨される修正に-Check if connector is still connected to same popと記載されているかどうかを確認します。これは、リソースの場所にあるコネクタがダウンした可能性があることを示します。コネクタイベントの確認に進みます。
   - 前述のメッセージが表示されない場合は、Citrix カスタマーサポートに連絡してください。

   connectTypeメッセージIntraAll::failure付きのイベントが表示された場合は、Citrix カスタマーサポートに連絡してください。

コネクタコンポーネントからのイベントを確認する

1. 診断ログ csv ファイルでエラーコード0x1800EFのtransaction IDを検索します。
2. csv ファイル内のトランザクション ID と一致するすべてのイベントをフィルタリングします。
3. また、SWA.ConnectorAppliance.WebAppsに一致する CSV ファイルの列prodをフィルタリングします。
4. イベントのstatusがfailureとして表示された場合は、;

   - これらの各障害イベントのreasonメッセージを確認してください。
   - UnableToRegister は、コネクタが Citrix Cloud に正常に登録できなかったことを示します。Citrix サポートに問い合わせてください。
   - IsProxyRequiredCheckErrorまたはProxyDialFailed、ProxyConnectionFailedまたはProxyAuthenticationFailureまたはProxiesUnReachableは、コネクタがプロキシ設定を通じてバックエンド URL を解決できなかったことを示します。プロキシ構成が正しいか確認してください。
   - 詳細なデバッグについては、「コネクタ SSO イベント」を参照してください。

シングルサインオンエラー

シングルサインオンの場合、アプリ構成から異なる SSO 属性が抽出され、アプリの起動時に適用されます。その特定のユーザーが属性を持っていない場合、または属性が正しくない場合、シングルサインオンは失敗する可能性があります。設定が正しいことを確認してください。

1. 「アクセスポリシー」に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザーのポリシールールと条件を確認します。

フォーム SSO、Kerberos、NTLM などの SSO メソッドは、オンプレミスコネクタによって実行されます。コネクタの次の診断ログを確認します。

コネクタコンポーネントの **SSO** イベントを確認する

1. SWA.ConnectorAppliance.WebAppsに一致する CSV ファイル内のcomponent nameをフィルタリングします。
2. ステータスが「失敗」のイベントが表示されますか?

   - これらの各障害イベントのメッセージを確認します。
   - IsProxyRequiredCheckErrorまたはProxyDialFailed、ProxyConnectionFailedまたはProxyAuthenticationFailureまたはProxiesUnReachableは、コネクタがプロキシ設定を通じてバックエンド URL を解決できなかったことを示します。プロキシ構成が正しいか確認してください。
   - FailedToReadRequestまたはRequestReceivedForNonSecureBrowseまたはUnableToRetrieveUserCredentialsまたはCCSPolicyIsNotLoadedまたはFailedToLoadBaseClientまたはProcessConnectionFailureまたはWebAppUnSupportedAuthTypeは、トンネリングの失敗を示します。Citrix サポートに問い合わせてください。
   - UnableToConnectTargetServer は、バックエンドサーバーにコネクタからアクセスできないことを示します。バックエンドの設定をもう一度確認してください。
   - IncorrectFormAppConfigurationまたはNoLoginFormFoundまたはFailedToConstructまたはFailedToLoginViaFormBasedAuthは、フォームベースの認証の失敗を示します。Citrix 管理ポータルの［アプリ構成］の［SSO 構成］セクションを確認します。
   - NTLMAuthNotFoundは NTLM ベースの認証の失敗を示します。Citrix 管理ポータルのアプリ構成で［NTLM SSO 構成］セクションを確認します。
   - 詳細なデバッグについては、「コネクタイベント」を参照してください。

認証サービスが停止しているため、アプリの起動に失敗しました

情報コード**:** 0x180022

Secure Private Access により、管理者は従来の Active Directory、AAD、Okta、または SAML などのサードパーティ認証サービスを構成できます。これらの認証サービスが停止すると、この問題が発生する可能性があります。

サードパーティ製のサーバーが稼働していて、到達可能かどうかを確認します。

SAML SSO の失敗

情報コード**:** 0x18008A、0x1800A9、0x1800AA、0x1800AB、0x1800AC、0x1800AD、0x1800AE、0x1800AF、0x1800B0、0x1800B1、0x1800B2、0x1800B3

IdP 起動時にアプリの起動中にユーザーに認証エラーが発生するか、SP 起動時にアクセスできないリンクが表示される場合があります。Secure Private Access サービス側の SAML アプリ構成とサービスプロバイダーの構成も確認します。

Secure Private Access 構成**:**

1. [アプリケーション] タブに移動します。
2. 問題のある SAML アプリを探してください。
3. アプリケーションを編集し、[シングルサインオン] タブに移動します。
4. 次のフィールドを確認します。

    - アサーション URL
    - リレーステート
    - オーディエンス
    - 名前 ID 形式、名前 ID、およびその他の属性

サービスプロバイダの構成**:**

1. サービスプロバイダーにログインします。
2. **SAML** 設定に移動します。
3. IdP 証明書、対象ユーザー、および IdP ログイン URL を確認します。

構成が正しいと思われる場合は、Citrix サポートに連絡してください。

アプリ **FQDN** が無効です

情報コード**:** 0x180048

顧客管理者が無効な FQDN を提供したか、バックエンドサーバーで DNS 解決が失敗する FQDN を提供した可能性があります。

この場合、エンドユーザーには Web ページにエラーが表示されます。アプリケーション設定を確認します。

SaaS アプリ検証　ネットワークからアプリにアクセスできるかどうかを確認します。

Web アプリ検証

1. [アプリケーション] タブに移動します。
2. 問題のあるアプリケーションを編集します。
3. [アプリの詳細] ページに移動します。
4. URL を確認します。この URL は、イントラネットまたはインターネットのいずれかでアクセスできる必要があります。

Secure Browser サービス**-DNS** 検索**/**接続失敗

情報コード**:** 0x18009D

Remote Browser Isolation サービスによるブラウジングエクスペリエンスが壊れています。エンドユーザーが接続しようとしているバックエンドサーバーを確認します。

1. バックエンドサーバーに移動して、稼働していて、リクエストを受信できるかどうかを確認します。
2. バックエンドサーバーへの接続が停止している場合は、プロキシ設定を確認してください。

> 注**:**
>
> Citrix Remote Browser Isolation サービスは、以前は Secure Browser サービスと呼ばれていました。

CWA Web-Web アプリの **DNS** ルックアップ**/**接続エラー

情報コード**:** 0x1800A0、0x1800A2、0x1800A3、0x1800A5、0x1800A6、0x1800A7

企業ネットワーク内で実行されている Web アプリケーションのブラウジングエクスペリエンスが損なわれている。

1. 解決できない FQDN の診断ログをフィルタリングします。
2. 企業ネットワーク内からバックエンドサーバーにアクセスできるかどうかを確認します。
3. プロキシ設定をチェックして、コネクタがバックエンドサーバーに到達できないかどうかを確認します。

直接アクセス**-Web** アプリとして誤って構成されている

Web アプリのトラフィックは常にコネクタ経由でルーティングされるため、直接アクセスを構成するとアプリアクセスエラーが発生します。

ルーティングドメインテーブルとアプリ設定の間に競合する設定がないか確認します。

1. 管理ポータルのアプリケーションに移動します。
2. アプリを編集し、ダイレクトアクセスが有効になっているか確認します。
3. ルーティングドメインテーブル内のアプリの FQDN が内部としてマークされているかどうかを確認します。

ユーザーには **DirectAccess** の **Web/SaaS** アプリケーションにアクセスする権限がありません

情報コード**:** 0x1800BD

アプリの設定により、ブラウザベースのクライアントから発信されるトラフィックへの直接アクセスが無効になります。

ユーザーがアプリケーションのサブスクリプションを持っていることを確認します。

1. 管理ポータルのアプリケーションに移動します。
2. アプリを編集し、エージェントレスアクセス設定を確認します。

強化されたセキュリティポリシー**-Secure Browser** サービスの設定ミス

情報コード**:** 0x1800C3

ポリシールールで意図された動作よりも不正な動作が見られる。コンテキストに応じたアクセスポリシーを確認します。

1. [ポリシー] タブに移動します。
2. アプリケーションに関連するポリシーを確認してください。
3. これらのポリシーのルールを確認してください。

強化されたセキュリティポリシー**-**ポリシーの設定ミス

ポリシールールで意図された動作よりも不正な動作が見られる。強化されたセキュリティ設定を確認します。

1. アプリケーションに移動します。
2. [アクセスポリシー] タブをクリックします。
3. [利用可能なセキュリティ制限**:**] セクションの設定を確認します。

アプリケーション構成の取得中に **Citrix Secure Access Agent** セッションの起動が失敗しました

情報コード**:** 0x1800D0

Citrix Secure Access アプリが Citrix Cloud への完全なトンネルを正常に確立できない。

1. TCP/UDP アプリのルーティングドメイン構成を確認します。
2. 最大エントリ数が 16k の制限内に収まっていることを確認してください。

TCP/UDP アプリ**-**不正な形式のクライアント要求

情報コード**:** 0x1800CD、0x1800CE、0x1800D6、0x1800EA

VPN トンネルが確立されていないか、特定の FQDN がトンネリングされていない可能性があります。

1. リクエストが途中のプロキシによって偽造されたり再構築されたりしていないことを確認してください。
2. 中間者攻撃の疑い。

TCP/UDP アプリ**-Secure Browser** サービスのリダイレクト設定ミス

情報コード**:** 0x1800DD

Remote Browser Isolation サービスのリダイレクトは Web アプリにのみ適用でき、TCP/UDP アプリには適用できません。Secure Private Access サービスの GUI でアプリ構成を確認します。

> 注**:**
>
> Citrix Remote Browser Isolation サービスは、以前は Secure Browser サービスと呼ばれていました。

ポリシー評価中に **Citrix Secure Access Agent** アプリの起動に失敗しました

情報コード**:** 0x1800DE

Citrix Secure Access クライアントによってトンネリングされるすべての内部 FQDN のルーティングドメインテーブルに対応するエントリがあることを確認してください。

IPv6 がサポートされていないため、**Citrix Secure Access Agent** アプリケーションの起動に失敗しました

情報コード**:** 0x1800EB

ルーティングドメインエントリを確認します。テーブルに IPV6 エントリがないことを確認します。

IP アドレスが無効なため、**Citrix Secure Access Agent** アプリケーションの起動に失敗しました

情報コード**:**0x1800EC、0x1800ED

ルーティングドメインエントリを確認します。IP アドレスが有効で、正しいバックエンドを指していることを確認してください。

Citrix Secure Access クライアントでのネットワーク接続の接続性の問題

情報コード**:** 0x10000001、0x10000002、0x10000003、0x10000004

1. クライアントマシンネットワークにアクセスできるかどうかを確認してください。ネットワークにアクセスできる場合は、クライアントのデバッグログを添えて Citrix サポートに連絡してください。
2. プロキシまたはファイアウォールがネットワークをブロックしていないか確認してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

プロキシサーバーがクライアントとサービスの接続を妨害している

情報コード**:** 0x10000006

1. クライアントマシンネットワークにアクセスできるかどうかを確認してください。
2. プロキシがクライアントで正しく設定されているか確認してください。
3. 両方に問題がない場合は、クライアントのデバッグログを添えて Citrix サポートに連絡してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

信頼できないサーバー証明書の問題が確認されました

情報コード**:** 0x10000007

Citrix サポートに連絡して、サーバー証明書が有効な CA によって正しく生成されているかどうかを確認してください。

無効なサーバー証明書の問題が見つかりました

情報コード**:** 0x10000008

Citrix サポートに連絡して、サーバー証明書が自己署名なのか、期限切れなのか、信頼できない発行元からのものなのかを確認してください。

ユーザーの構成が空であるため、ログインできませんでした

情報コード**:** 0x1000000A

1. 少なくとも 1 つの TCP/UDP/HTTP アプリが設定されていることを確認します。詳細については、「アプリケーションの追加と管理」を参照してください。
2. [アプリケーションドメイン] テーブル ([**Secure Private Access] > [**設定**] > [**アプリケーションドメイン]) が空でないこと、またはすべてのエントリが無効になっていないことを確認します。TCP/UDP/HTTP アプリケーションで設定された宛先は、このテーブルに自動的に追加されます。

アクティブな TCP/UDP/HTTP アプリケーションの宛先や URL を削除したり無効にしたりしないことをお勧めします。

接続はネットワークまたはエンドユーザーによって終了されました

情報コード**:** 0x1000000B

ネットワークが中断されていないか、またはエンドユーザーが ZTNA セッション接続中に接続をキャンセルしていないかを確認します。

セッションの有効期限が切れたため、設定のダウンロードに失敗しました

情報コード**:** 0x10000010

ZTNA セッション設定のダウンロード要求中に VPN セッションが期限切れになった可能性があります。Citrix Secure Access クライアントに再ログインしてみてください。

Citrix Secure Access クライアントがログインに失敗しました

情報コード**:** 0x10000013

構成サイズが最大構成制限を超えているため、Citrix Secure Access クライアントはログインできませんでした。

1. [**Secure Private Access] > [**設定**] > [**アプリケーションドメイン] で TCP/UDP アプリケーションのルーティングドメイン構成を確認します。
2. エントリ数が多くないことを確認してください。エントリリストが膨大な場合は、未使用の宛先を無効にするか削除してください。

   宛先リストが 1000 を超えることが予想される場合は、ConfigSize レジストリキーを更新して、設定のダウンロードの最大サイズを増やしてみてください。詳しくは、「Citrix Gateway VPN クライアントのレジストリキー」を参照してください。

セッションの有効期限が切れたため、コントロールチャネルを確立できませんでした

情報コード**:** 0x11000003

セッションの有効期限が切れたため、DNS 要求確立の制御チャネルが失敗しました。

コントロールチャネルのセットアップ中に ZTNA セッションが期限切れになった可能性があります。

Citrix Secure Access クライアントに再ログインしてみてください。

コントロールチャネルを確立できませんでした

情報コード**:** 0x11000004

DNS リクエスト確立の制御チャネルが失敗しました。

- リソースの場所を正常に保つ**:**

1. Citrix Cloud にログオンします。
2. ハンバーガーメニューから「リソースの場所」をクリックします。
3. それぞれのリソースの場所でコネクタアプライアンスのヘルスチェックを実行します。
4. これで問題が解決しない場合は、コネクタ仮想マシンを再起動してみてください。

- **HA Connector Appliance** のメンテナンス**:**

1. Citrix Cloud にログオンします。
2. ハンバーガーメニューから「リソースの場所」をクリックします。
3. 想定されるリソースの場所に少なくとも 2 つの Connector Appliance があることを確認してください。

次の事項に留意してください。

- リソースの場所 LAN は動作中です。
- 中央には、サービスまたはバックエンドサーバーへの Connector Appliance ブロックしているファイアウォールやプロキシはありません。
- クライアントネットワークは正常です。
- バックエンドのプライベートサーバーが稼働しています。
- DNS サーバーは稼働しています。
- FQDN は解決可能です。

前述の推奨事項を満たしている場合は、次のことを行ってください。

1. このエラーの診断ログからトランザクション ID を取得します。
2. Secure Private Access ・ダッシュボードでトランザクション ID と一致するすべてのイベントをフィルタリングします。
3. クライアント、Connector Appliance、またはサービスの診断ログに、トランザクション ID と一致するエラーが発生していないか確認します。次に、それに応じて適切なアクションを実行します。
4. アプリケーションドメインテーブル（**Secure Private Access >** 設定 **>** アプリケーションドメイン）で、リソースの場所が宛先として正しく選択されているかどうかを確認します。
5. アプリケーションが正しいポート、IP 範囲、ドメインで構成されているか確認してください。詳細については、「アプリケーションの追加と管理」を参照してください。

それでも問題を解決できない場合は、トランザクション ID とクライアントログに対応するエラーコードを添えて Citrix サポートに連絡してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

コントロールチャネルを確立できませんでした

情報コード**:** 0x11000005

コントロールチャネル (DNS リクエスト用) を確立できませんでした。

1. Secure Private Access ・サービスのライセンス資格を確認してください。
2. 資格がない場合は、Citrix サポートに連絡してライセンスを確認してください。

詳しくは、https://www.citrix.com/buy/licensing/product.htmlを参照してください。

ネットワークの問題によりコントロールチャネルを確立できませんでした

情報コード**:** 0x11000006

ネットワークの問題により、コントロールチャネル (DNS リクエスト用) を確立できませんでした。

1. Secure Private Access ・サービスにアクセスできるかどうかを確認してください。
2. アクセスできない場合は、エラーコードとクライアントログを添えて Citrix サポートに連絡してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

IIP が不十分なため、制御チャネルを確立できませんでした

情報コード**:** 0x11000007

IIP が不十分なため、コントロールチャネル (DNS リクエスト用) を確立できませんでした。

エラーコードとクライアントログを添えて、Citrix サポートに連絡してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

セッションが終了したためログオフできません

この問題は、クライアントマシン (キーボードまたはマウス) が設定されたタイムアウト期間を超えてアイドル状態だったために発生した可能性があります。

情報コード**:** 0x12000001

Citrix Secure Access クライアントに再ログインしてみてください。

セッションは強制終了されます

設定された強制タイムアウトに達すると、セッションは強制終了されます。

情報コード**:** 0x12000002

Citrix Secure Access クライアントに再ログインしてみてください。

セッションの有効期限が切れたため、アプリケーションの起動に失敗しました

情報コード**:** 0x13000001

1. ZTNA セッションは、アプリの起動中に期限切れになりました。
2. Citrix Secure Access クライアントに再ログインしてみてください。

ライセンスの問題によりアプリケーションの起動に失敗しました

情報コード**:** 0x13000002

1. Secure Private Access ・サービスのライセンスがエンタイトルメントであることを確認してください。
2. 資格がない場合は、Citrix サポートに連絡してライセンスを確認してください。

詳しくは、https://www.citrix.com/buy/licensing/product.htmlを参照してください。

サービスによってアクセスが拒否されたため、アプリケーションを起動できませんでした

情報コード**:** 0x13000003、0x13000008、0x001800DF

アプリケーションの起動は、ユーザーとアプリケーションのポリシー設定に従って拒否されます。

次のことを確認してください。

- 同じ宛先を複数のアプリケーション（HTTP、HTTPS、TCP、UDP）で使用することはできません
- 複数のアプリケーションで宛先が重複することはありません。
- アクセスポリシーは、アプリケーションにバインドされます。

また、拒否されたアプリケーションに設定されているポリシーの条件とアクションも確認してください。次に、ポリシーの条件とアクションを確認します。

詳細については、「アクセスポリシー」を参照してください。

クライアントがサービスにアクセスできないため、アプリケーションを起動できませんでした

情報コード**:** 0x13000004、0x13000005

1. Secure Private Access ・サービスにアクセスできるかどうかを確認してください。
2. アプリを再度起動します。
3. 長時間アプリにアクセスできない場合は、Citrix サポートにエラーコードとクライアントログを添えて問い合わせてください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

ポリシー評価と設定の検証が失敗したため、アプリケーションの起動に失敗しました

情報コード**:** 0x13000007

Secure Private Access サービスによるポリシー評価と構成の検証が失敗したため、アプリケーションを起動できませんでした。

アクセス先のアプリケーションを見つけることができません。

サービスによってアクセスが拒否されたため、アプリケーションを起動できませんでした。

アプリケーションドメインテーブルの問題により、アプリケーションを起動できませんでした

情報コード**:** 0x13000009

アプリケーションドメインテーブルにアクセス先のエントリがないため、アプリケーションの起動に失敗しました。

Secure Private Access > 設定 **>** アプリケーションドメインで、ルートエントリがアプリケーションに正しく設定されていることを確認します。

クライアントは **Secure Private Access** ・サービスとの接続を終了しました

情報コード**:** 0x1300000B

1. エンドユーザーが手動で接続を閉じたかどうかを確認してください。
2. そうでない場合は、エラーコードとクライアントログを添えて Citrix サポートに連絡してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

DNS サーバーで **FQDN** を解決できません

情報コード**:** 0x1300000C

この問題は、Connector Appliance FQDN の DNS を解決できない場合に発生します。

1. DNS サーバーのそれぞれのアプリ FQDN の DNS エントリを確認します。
2. Connector Appliance で適切な DNS サーバーが設定されていることを確認します。詳細については、Connector Appliance 管理ページの「ネットワーク設定の構成」を参照してください。

アプリケーションが見つからない

情報コード**:** 0x001800DE

ユーザーがアクセスした宛先のアプリケーションが見つからない場合があります。これは、デスティネーションとリソースの場所のマッピングがアプリケーションドメインテーブルにない場合に発生する可能性があります。

- アクセス先に TCP/UDP または HTTP アプリケーションが設定されていることを確認します。
- ユーザーがアクセス先のアプリケーションを購読していることを確認します。

1. 管理ポータルのアプリケーションに移動します。
2. アプリを編集し、[サブスクリプション] タブに移動します。
3. 対象となるユーザーがサブスクリプションリストにエントリを持っていることを確認してください。
4. **Application Domain** テーブルに宛先と適切なリソースの場所があることを確認してください。

設定済みのアプリケーション宛先リストを取得できませんでした

情報コード**:** 0x001800D3

- 少なくとも 1 つの TCP/UDP/HTTP アプリが設定されていることを確認します。詳細については、「アプリケーションの追加と管理」を参照してください。
- 「アプリケーションドメイン」テーブル（「**Secure Private Access** 」**>**「設定」**>**「アプリケーション・ドメイン」）ページが空でないこと、またはすべてのエントリが無効になっていないことを確認してください。TCP/UDP/HTTP アプリケーションで設定された宛先は、このテーブルに自動的に追加されます。アプリケーションドメインテーブル内のアクティブな TCP/UDP/HTTP アプリケーションの宛先または URL を削除したり、無効にしたりしないことをお勧めします。

アプリケーション設定の問題

アプリケーション設定に特殊文字が含まれているか、ポリシー設定に問題があります。

情報コード**:** 0x001800D9、0x001800DA

次の事項に留意してください。

- アプリの設定には、サポートされていない文字は含まれていません。
- 宛先 IP アドレスまたは IP アドレス範囲、または IP CIDR は有効です。
- アプリケーションの宛先は、アプリケーションドメインテーブル（**Secure Private Access >** 設定 **>** アプリケーション・ドメイン）で有効になっています。
- ポリシーが設定され、それぞれのアプリケーションにバインドされます。
- アクセスポリシーの設定は正しい。

リソースの場所に関する問題

情報コード**:** 0x001800dB

- リソースの場所が設定されていることを確認します。

    1. Citrix Cloud のハンバーガーメニューで、「リソースの場所」を選択します。

2. 必要なリソースの場所が設定され、リソースの場所がアクティブステータスになっていることを確認します。

- アプリケーションドメインテーブル (**Secure Private Access >** 設定 **>** アプリケーションドメイン) で、ターゲットとして正しいリソースの場所が選択されていることを確認します。

TCP/UDP/HTTP アプリケーションで設定された宛先は、このテーブルに自動的に追加されます。アプリケーションドメインテーブル内のアクティブな TCP/UDP/HTTP アプリケーションの宛先または URL を削除したり無効にしたりしないことをお勧めします。

強化されたセキュリティポリシーは **HTTP** アプリケーションにバインドされます

情報コード**:** 0x001800DC、0x001800DD、0x13000006

セキュリティポリシーが強化された HTTP アプリケーションには、Citrix Secure Access クライアントを介してアクセスされます。

- TCP/UDP アプリケーションと HTTP アプリケーションの両方で同じ宛先が使用されていないことを確認してください。
- HTTP/HTTPS アプリケーションのセキュリティ強化ポリシーが有効になっている場合は、Citrix Workspace アプリまたは Citrix Remote Browser Isolation サービスを介してのみアプリにアクセスすることをお勧めします。
- HTTP/HTTPS アプリケーションが Citrix Secure Access クライアントを介してアプリケーションにアクセスするための拡張セキュリティ制御を無効にします。
  - Secure Private Access 管理ポータルにアクセスしてください。
  - 「アプリケーション」タブをクリックし、アクセス先の HTTP/HTTPS アプリケーションのポリシー名を検索します。
  - アクセスポリシータブをクリックし、先に示したポリシー名を検索します。
  - ポリシーを選択し、[編集] をクリックします。
  - アクションを [制限付きアクセスを許可] から **[**** アクセスを許可 **] に変更します。

構成の詳細については、「アプリケーションの追加と管理」を参照してください。

> 注**:**
>
> Citrix Remote Browser Isolation サービスは、以前は Secure Browser サービスと呼ばれていました。

ホスト名の長さが **256** 文字を超えています

情報コード**:** 0x001800EA

アプリケーション起動リクエストで受信したホスト名が 256 文字を超えています。

FDQN 文字は 256 文字を超えないようにすることをお勧めします。

IP アドレスが無効です

情報コード**:** 0x001800ED

アプリケーション起動リクエストで受け取った IP アドレスは無効です。

クライアントからの有効なプライベート IP アドレスのみにアクセスすることをお勧めします。

エンドツーエンド接続を確立できません

情報コード**:** 0x001800EF

クライアントとリソースの場所に設定されたサーバー間のエンドツーエンド接続を確立できません。

- リソースの場所がアクティブ状態であることを確認します。
  - Citrix Cloud のハンバーガーメニューで、「リソースの場所」を選択します。
  - それぞれのリソースの場所で Connector Appliance のヘルスチェックを実行します。
  - これで問題が解決しない場合は、コネクタ仮想マシンを再起動します。
- 高可用性 Connector Appliance 保守
  - Citrix Cloud のハンバーガーメニューで、「リソースの場所」を選択します。
  - リソースの場所に少なくとも 2 つの Connector Appliance があることを確認してください。
- 次の事項に留意してください。
  - リソースの場所 LAN は動作中です。
  - サービスまたはバックエンドサーバーへの Connector Appliance をブロックするファイアウォールやプロキシが中央にありません。
  - クライアントネットワークは正常です。
  - バックエンドのプライベートサーバーは正常です。
  - DNS サーバーは正常です。
  - FQDN は解決可能です。

これらに問題がない場合は、以下を実行してください。

1. このエラーの診断ログからトランザクション ID を取得します。
2. Secure Private Access サービスのダッシュボードで、トランザクション ID と一致するすべてのイベントをフィルタリングします。
3. Secure Private Access サービスのダッシュボードからトランザクション ID に対応する診断ログを確認し、それに応じて適切なアクションを実行します。
4. アプリケーションドメインテーブル (**Secure Private Access >** 設定 **>** アプリケーションドメイン) で、正しいリソースの場所が宛先として選択されていることを確認します。

5. アプリケーションが正しい IP アドレス、ポート、および FQDN で構成されているかどうかを確認します（「**Secure Private Access**」**>**「アプリケーション」）。

これらの手順を実行しても問題が解決しない場合は、トランザクション ID に対応するエラーコードを添えて Citrix サポートに連絡し、クライアントログを収集してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

アプリリクエストで受信した **IPv6**

情報コード**:** 0x001800F5

サポートされていない IPv6 がアプリリクエストで受信されました。現在、IPv4 のみがサポートされています。

アプリケーションを編集して、アプリケーションの IP アドレスの問題を修正します。

1. Secure Private Access 管理ポータルにアクセスしてください。
2. ［アプリケーション］タブをクリックします。
3. アプリを検索し、[編集] をクリックします。

詳しくは、「アプリの追加と管理」を参照してください。

UDP トラフィックの配信失敗

情報コード**:** 0x001800F9

クライアント接続が失われたため、UDP トラフィックの配信に失敗しました

1. クライアントセッションがアクティブかどうかを確認してください。
2. ログアウトしてから再ログインします。

UDP データトラフィックの配信に失敗しました

情報コード**:** 0x001800FF

- トランザクション ID でエラーコードを検索し、Secure Private Access サービスのダッシュボードでトランザクション ID と一致するすべてのイベントをフィルタリングします。
- トランザクション ID と一致する他のコンポーネントでエラーが発生していないか確認してください。他のコンポーネントに問題が見つかった場合は、それに応じて適切な処置を講じてください。
- それでも問題が解決しない場合は、エラーコードとそれぞれのトランザクション ID を添えて Citrix サポートに連絡してください。

ネットワーク接続の問題により、アプリケーションを起動できませんでした

情報コード**:** 0x10000401

Connector Appliance Secure Private Access ・サービス間のネットワーク接続の問題によるアプリケーションの起動失敗

1. Connector Appliance パブリックインターネット接続を確認します。
2. プロキシまたはファイアウォールのルールが接続をブロックしていないか確認してください。
3. いずれかのプロキシが問題の原因である場合は、プロキシをバイパスして、アプリを再度起動してみてください。
4. Connector Appliance スのヘルスステータス（**Citrix Cloud >** リソースの場所）を確認します。

ネットワーク設定の詳細については、「Connector Appliance ネットワーク設定」を参照してください。

Connector Appliance Secure Private Access サービスに登録できませんでした

情報コード**:** 0x10000402、0x1000040C

1. Connector Appliance の管理ページに移動し、コネクタの概要を確認してください。
2. コネクタの状態が良くない場合は、管理ポータル内のリソースの場所に移動してください。
3. それぞれのリソースの場所で Connector Appliance のヘルスチェックを実行します。
4. ヘルスチェックが失敗した場合は、コネクタ仮想マシンを再起動します。
5. コネクタの概要を確認して、ヘルスチェックを再実行してください。

ネットワーク設定の詳細については、「Connector Appliance ネットワーク設定」を参照してください。

Connector Appliance との接続問題

情報コード**:** 0x10000403、0x10000404、0x10000407、0x1000040A、0x1000040B、0x1000040F、0x10000410

- トランザクション ID でエラーコードを確認してください。
- Secure Private Access ・ダッシュボードでトランザクション ID と一致するすべてのイベントをフィルタリングします。
- トランザクション ID と一致する他のコンポーネントでエラーが発生していないかどうかを確認し、見つかった場合は、そのエラーコードに対応する回避策を実行します。
- 他のコンポーネントでエラーが見つからない場合は、次の操作を行います。
  - Connector Appliance の管理ページに移動します。
  - 診断レポートをダウンロードします。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。

  - パケットトレースをキャプチャします。詳細については、「ネットワーク接続の検証」を参照してください。

- この診断レポートとパケットトレース、およびエラーコードとトランザクション ID を添えて、Citrix サポートに連絡してください。

Connector Appliance バックエンドのプライベート **TCP/UDP** サーバーとの接続の問題

情報コード**:** 0x10000405、0x10000408、0x10000409、0x1000040D、0x1000040E、0x10000412

Connector Appliance には、バックエンドのプライベート TCP/UDP サーバーとの接続に問題があります。

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働していて、リクエストを受信できるかどうかを確認します。
- 企業ネットワーク内からバックエンドサーバーにアクセスできるかどうかを確認します。
- プロキシ設定をチェックして、コネクタがバックエンドサーバーに到達できないかどうかを確認します。
- FQDN ベースのアプリをリクエストする場合は、DNS サーバーでそれぞれのアプリの DNS エントリを確認します。

Connector Appliance が **FQDN** の **DNS** を解決できない

情報コード**:** 0x10000406

- DNS サーバーのそれぞれのアプリ FQDN の DNS エントリを確認します。
- Connector Appliance で適切な DNS サーバーが設定されていることを確認します。詳細については、Connector Appliance 管理ページの「ネットワーク設定の構成」を参照してください。

プライベートサーバー接続が終了しました

情報コード**:** 0x10000411

プライベートサーバーへの接続は、クライアントまたは Secure Private Access ・サービスによって終了されます。

1. エンドユーザーがアプリケーションを閉じたかどうかを確認してください。
2. このログのトランザクション ID と一致する他の診断ログを確認し、それに応じて適切なアクションを実行してください。
3. アプリを再度起動します。
4. それでも問題が解決しない場合は、エラーコードとトランザクション ID を Citrix サポートに問い合わせてください。

プライベートサービス **IP** または **FQDN** に接続またはデータを送信できませんでした

情報コード**:** 0x10000413

- プライベートサーバー接続が終了しました
- [Connector Appliance バックエンドプライベート TCP/UDP サーバーとの接続問題] (/en-us/citrix-secure-private-access/service/セキュア-プライベート-アクセスのトラブルシューティング。html#connectivity-issues-with-connector-appliance-and-backend-private-tcpudp-servers). ルーティングドメインエントリを確認します。IP アドレスが有効で、正しいバックエンドを指していることを確認します。

一致するポリシー条件なし

情報コード**:** 0x100508

ユーザーコンテキストが、アプリに割り当てられたポリシーで定義されているアクセスルール条件と一致しません。

ユーザーのコンテキストに合わせてポリシー設定を更新します。

アプリケーションにはアクセスポリシーが関連付けられていません

情報コード**:** 0x100509

1. Citrix Secure Private Access サービス GUI で、左側のナビゲーションにある「アクセスポリシー」をクリックします。
2. アクセスポリシーがそれぞれのアプリに関連付けられていることを確認してください。
3. アクセスポリシーがアプリに関連付けられていない場合は、アプリのアクセスポリシーを作成します。詳細については、「アクセスポリシーの作成」を参照してください。
4. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

FQDN または **IP** アドレスのアプリケーション構成が見つかりません

情報コード**:** 0x10050A

受信した FQDN または IP アドレス要求に一致するアプリケーションが見つかりませんでした。したがって、アプリは未公開アプリとして分類されます。これが期待できない場合は、次の操作を実行してください。

1. Secure Private Access サービスの管理ポータルにアクセスしてください。
2. 左側のナビゲーションで [アプリケーション] をクリックします。
3. アプリを検索し、[編集] をクリックします。

4. FQDN または IP アドレスをアプリケーションに追加します。正確なドメイン、IP アドレス、またはワイルドカードドメインを追加できます。

   注**:** [**Secure Private Access] > [**設定**] > [**アプリケーションドメイン] に FQDN または IP アドレスを追加しても、この問題は解決されません。アプリケーション構成の一部として追加する必要があります。

アプリ列挙情報

情報コード**:** 0x10050C

このコードは、ユーザーが利用できる可能性のある複数のアプリケーションのポリシー評価結果をキャプチャします。アプリへのアクセスは、次の理由で拒否される可能性があります。

- ユーザーコンテキストが、アプリに割り当てられたポリシーで定義されているアクセスルール条件と一致しません。詳細については、「ポリシー条件が一致しない」を参照してください。
- アクセスポリシーがアプリケーションに関連付けられていません。詳細については、「アプリケーションに関連付けられたアクセスポリシーなし」を参照してください。
- アプリケーションに関連するポリシーがアクセスを拒否するように設定されている—この場合、意図したとおりの操作は必要ありません。
- アクセスポリシーの適用中に予期しない内部エラーが発生しました。詳細については、Citrix サポートにお問い合わせください。

アプリケーションドメインテーブルにルーティングエントリがないため、**TCP/UDP** アプリケーションの起動に失敗しました

情報コード**:** 0x00180101

この問題は、アプリケーション構成は存在するが、ルーティングエントリがないか、以前に削除されていた場合に発生する可能性があります。

アクセス先のルーティングエントリ ([**Secure Private Access] > [**設定**] > [**アプリケーションドメイン]) を追加します。

コネクタが正常でないため、**TCP/UDP** アプリの起動に失敗しました

情報コード**:** 0x00180102

この問題は、どのコネクタも新しい接続に稼働していないか、応答していない場合に発生する可能性があります。

それぞれのリソースの場所で Connector Appliance のヘルスチェックを実行します。

コネクタにアクセスできないため、**UDP/DNS** 要求が失敗しました

情報コード**:** 0x00180103

この問題は、UDP/DNS トラフィックがコネクタに到達できない場合に発生する可能性があります。

それぞれのリソースの場所で Connector Appliance のヘルスチェックを実行します。

NGS Cookie の有効期限が切れているため、ページを読み込めませんでした

情報コード**:** 0x20580001

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

ネットワーク障害のため、アクセスポリシーの取得に失敗しました

情報コード**:** 0x20580002

1. URL とネットワーク接続を確認してください。
2. ブラウザを再起動して、アプリをもう一度開いてみてください。
3. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

JSON Web トークンの解析中にアクセスポリシーの取得が失敗しました

情報コード**:**0x20580003

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

ネットワークがアクセスポリシーの詳細を取得できませんでした

情報コード**:**0x20580004

1. アクセスポリシーが有効になっているか確認してください。
2. ブラウザを再起動して、アプリをもう一度開いてみてください。
3. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

パブリック証明書のフェッチ中にポリシーのフェッチが失敗しました

情報コード**:** 0x20580005

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

JSON Web トークンの署名を検証中にポリシーの取得に失敗しました

情報コード**:** 0x20580007

1. ネットワーク時刻とユーザーデバイスの時刻が同期しているかどうかを確認してください。
2. ブラウザを再起動して、アプリをもう一度開いてみてください。
3. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

公開証明書の検証中にポリシーの取得に失敗しました

情報コード**:** 0x20580008

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

ポリシー **URL** を作成するためのストア環境を決定できませんでした

情報コード**:** 0x2058000A

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

アクセスポリシーの取得要求に対する応答を取得できませんでした

情報コード**:** 0x2058000B

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

セカンダリ **DS** 認証トークンの期限が切れているため、アクセスポリシーの取得に失敗しました

情報コード**:** 0x2058000C

1. ブラウザを再起動して、アプリをもう一度開いてみてください。
2. それでも問題が解決しない場合は、Citrix サポートに連絡してください。

Connector Appliance 登録されていません

情報コード**:** 0x10200002

Connector Appliance 登録を確認します。

詳しくは、「Connector Appliance Citrix Cloud への登録」を参照してください。

Connector Appliance に接続できない

情報コード**:** 0x10200003

Connector Appliance、Citrix Cloud とリソースの場所間で通信できません。

コネクタの登録を確認してください。

詳しくは、「Connector Appliance Citrix Cloud への登録」を参照してください。

Citrix Secure Private Access サービスへの接続に失敗しました

情報コード**:** 0x10000301

Connector Appliance ネットワーク設定を確認します。詳細については、「Connector Appliance ネットワーク設定」を参照してください。

プロキシサーバーにアクセスできない

情報コード**:** 0x10000303、0x10000304

プロキシサーバーの設定を確認し、Connector Appliance にアクセスできることを確認します。詳しくは、「Connector Appliance Citrix Cloud への登録」を参照してください。

プロキシサーバーの認証が失敗しました

情報コード**:** 0x10000305

プロキシサーバーの資格情報を確認し、Connector Appliance で正しく構成されていることを確認します。詳細については、「Connector Appliance 登録後」を参照してください。

設定したプロキシサーバーにアクセスできない

情報コード**:** 0x10000306

Connector Appliance ネットワーク設定、ファイアウォール設定、またはプロキシサーバー設定を確認します。詳細については、以下のトピックを参照してください:

- Connector Appliance のネットワーク設定
- Connector Appliance を Citrix Cloud に登録する
- Connector Appliance の通信

バックエンドサーバーからエラー応答を受信しました

情報コード**:** 0x10000307

バックエンド Web サーバーの HTTP ステータスコードが期待どおりのコードでないかどうかを確認します。

ターゲット **URL** にリクエストを送信できません

情報コード**:** 0x10000005

ターゲット URL を確認するか、Connector Appliance ネットワーク設定を確認します。詳細については、「Connector Appliance ネットワーク設定」を参照してください。

SSO を処理できませんでした

情報コード**:** 0x10000107

Citrix Cloud からアプリ構成データを取得できません。

Connector Appliance ネットワーク設定をチェックし、NTP サーバーが設定されていて、タイムストリップの問題がないことを確認します。詳細については、「Connector Appliance ネットワーク設定」を参照してください。

Citrix Secure Private Access サービスへの接続に失敗しました

情報コード**:** 0x10000108、0x1000010B

Connector Appliance ネットワーク設定を確認します。詳細については、「Connector Appliance ネットワーク設定」を参照してください。

SSO を処理できませんでした。**SSO** 設定を確認できません

情報コード**:** 0x1000010A

SSO 構成をチェックし、サーバーが Connector Appliance にアクセスできることを確認します。

FormFill SSO が失敗しました。フォームアプリの設定が正しくありません

情報コード**:** 0x10000101、0x10000102、0x10000103、0x10000104

SSO フォームアプリの設定を確認し、ユーザー名、パスワード、アクション、ログイン URL の各フィールドがアプリ設定で正しく設定されていることを確認します。

Kerberos SSO が失敗しました

情報コード**:** 0x10000202

バックエンドサーバーとドメインコントローラーの Kerberos SSO 設定を確認します。フォールバック NTLM 認証設定も確認してください。

Kerberos SSO 設定については、「Kerberos 構成の検証」を参照してください。

認証タイプの **SSO** を処理できませんでした

情報コード**:** 0x10000203

Secure Private Access サービスとバックエンドサーバーの SSO 設定を確認します。Secure Private Access サービスについては、「優先サインオン方法の設定」を参照してください。

Kerberos SSO は失敗しましたが、**NTLM** にフォールバックしました

情報コード**:** 0x10000204

ドメインコントローラから Kerberos チケットを取得できませんでした。二次認証として、Connector Appliance フォールバック NTLM 認証を試みました。

Kerberos 認証を正常に実行できるようにするには、バックエンドサーバーとドメインコントローラーの Kerberos SSO 設定を確認します。

詳細については、「Kerberos 構成の検証」を参照してください。

Citrix Workspace アプリケーションで構成された複数の **ZTNA** 資格のあるアカウント

情報コード**:** 0x14000001

Citrix Workspace アプリケーションでは、ZTNA 資格のあるアカウントを 1 つだけ構成してください。

クライアントログの収集方法

- **Windows** クライアント:

  1. アプリを開いて、ロギングが有効になっていることを確認します。
  2. 次に、Secure Private Access ・サービスに接続して、直面している問題を再現してください。
  3. アプリで [ログ] に移動し、[ログファイルの収集] をクリックします。これにより、ログファイルが生成されます。
  4. ログファイルをクライアントマシンのデスクトップに保存します。

- **Mac** クライアント**:**

  1. アプリを開いて、[ログ**] > [Verbose**] に移動します。
  2. ログを消去して、問題の再現に進みます。
  3. [ログ**] > [**ログのエクスポート**]** に戻ります。これにより、ログファイルを含む zip ファイルが作成されます。

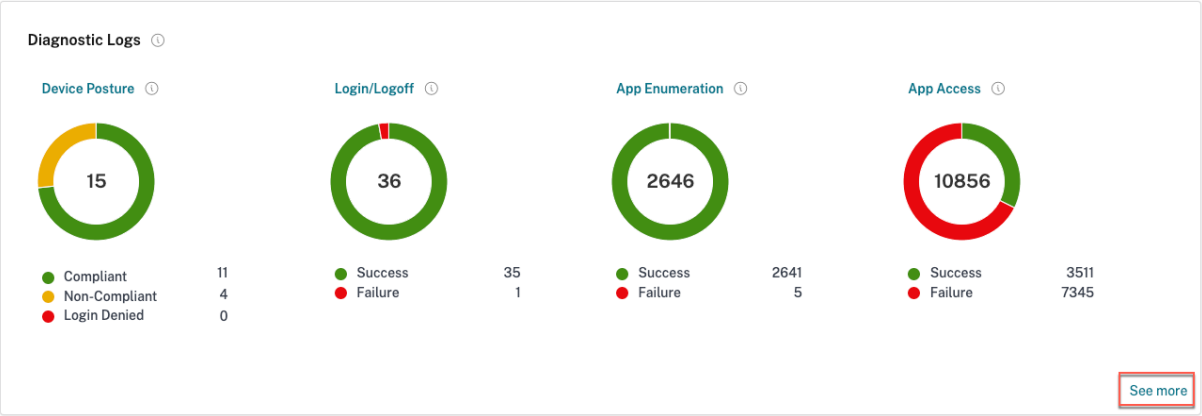
よくある質問への回答

Secure Private Access 診断ログとは何ですか**?**

Secure Private Access の診断ログは、ユーザーが任意のアプリケーション（Web/SaaS/TCP/UDP）にアクセスしたときに発生するすべてのイベントをキャプチャします。これらのログには、デバイスポスチャー、アプリ認証、アプリ列挙、アプリアクセスログが記録されます。

Secure Private Access ・ログはどこで確認できますか**?**

1. Citrix Cloud にログオンします。
2.「Secure Private Access」サービスのタイルで、「管理」をクリックします。
3. 管理者ユーザーインターフェースの左側のナビゲーションにある [ダッシュボード] をクリックします。
4.「診断ログ」チャートで、「詳細を表示」リンクをクリックします。



Secure Private Access の診断ログにはどのような詳細がありますか**?**

Secure Private Access ユーザー・ログ・ダッシュボードには、デフォルトで次の詳細が表示されます。

- タイムスタンプ -UTC でのイベントの時刻。
- ユーザー名 -アプリにアクセスするエンドユーザーのユーザー名。
- アプリ名 -アクセスされた 1 つまたは複数のアプリの名前。
- ポリシー情報 -イベント中にトリガーされた 1 つまたは複数のアクセスポリシーの名前が表示されます。
- ステータス -イベント、成功、または失敗のステータスが表示されます。
- 情報コード - 情報コードの詳細をご覧ください。
- 説明 -失敗の原因またはイベントの詳細が表示されます。
- **APP FQDN**: アクセスされたアプリケーションの FQDN
- イベントタイプ - 実行された操作に関連するイベントタイプが表示されます。
- 操作タイプ -ログが生成される操作を表示します。
- カテゴリ -イベントの種類に応じて、3 つのカテゴリがあります。それは、アプリ認証、アプリ列挙、またはアプリアクセスです。これらのオプションはフィルターオプションとしても使用できます。これらのオプションを使用して、直面している問題の種類に応じてログをフィルタリングできます。
- トランザクション **ID** - トランザクション ID の使い方をご覧ください
  。ダッシュボードの右端にある「+」ボタンをクリックすると、以下の詳細情報を取得できます。
- **SPA PoP** ロケーション -アプリケーションアクセス中に使用された Secure Private Access サービスの PoP ロケーションの名前/ID を表示します。Secure Private Access PoP ロケーションを見る

Secure Private Access の診断ログにはどのようなイベントが記録されますか**?**

Secure Private Access の診断ログには、次のイベントが記録されます。

- デバイスポスチャ**:** エンドユーザーのデバイスステータス。これらのログには、デバイスポスチャー結果に関する情報が記録されます。お使いのデバイスポスチャポリシーに基づいて、デバイスが準拠していると見なされたか、非準拠と見なされたか、またはアクセスが拒否されたか。
- ログイン**/**ログオフ: Citrix Secure Access クライアントへのエンドユーザーのログオンまたはログオフステータス、およびワークスペース（内部または外部プロバイダー）への認証に関するイベント。
- アプリ列挙:Secure Private Access サービスでは、管理者が設定したアクセスポリシーによって、どのユーザーがどのアプリにアクセスできるかが決まります。拒否されたアプリケーションは、Citrix Workspace アプリ内のエンドユーザーには表示されません（列挙されません）。これらのイベントは、Secure Private Access サービス内で設定されたアクセスポリシーに基づいて、どのアプリケーションがユーザーへのアクセスを許可または拒否されたかを知るのに役立ちます。
- アプリケーションアクセス: 選択した時間間隔に設定されたアクセスポリシーに基づく、エンドユーザーのアプリケーション/エンドポイントアクセス、許可/拒否ステータス、シングルサインオンステータス、接続ステータスのイベント。

Secure Private Access のトラブルシューティングトピックを使用して、発生した障害を解決する方法を教えてください

1. 解決しようとしている障害の情報コードを取得してください 。
2. エラー検索テーブルで情報コードを検索します。
3. その情報コードに記載されている解決手順に従ってください。

情報コードとは? どこで見つけられますか

障害などの一部のログイベントには、関連する情報コードがあります。エラー検索テーブル内でこの情報コードを検索して 、解決手順やそのイベントに関する詳細情報を確認してください。

トランザクション **ID** とは何ですか**?** どうやって使うの

トランザクション ID は、アクセスリクエストのすべての Secure Private Access ログを関連付けます。1 つのアプリアクセスリクエストで、認証、Workspace アプリ内でのアプリ列挙、アプリアクセス自体から複数のログを生成できます。これらのイベントはすべて独自のログを生成します。トランザクション ID は、これらすべてのログを関連付けるために使用されます。トランザクション ID を使用して診断ログをフィルタリングし、特定のアプリアクセスリクエストに関連するすべてのログを検索できます。

Secure Private Access の **PoP** ロケーションにはどのようなものがありますか

以下は、Secure Private Access の PoP ロケーションのリストです。

ポップネーム	ゾーン	リージョン
az-us-e	Azure eastus	バージニア
az-us-w	Azure westus	California
az-us-sc	Azure southcentralus	テキサス
az-aus-e	Azure australiaeast	ニューサウスウェールズ
az-eu-n	Azure northeurope	アイルランド
az-eu-w	Azure westeurope	オランダ
az-jp-e	Azure japaneast	東京、埼玉
az-bz-s	Azure brazilsouth	サンパウロ州
az-asia-se	Azure southeastasia	シンガポール
az-uae-n	Azure uaenorth	ドバイ

ポップネーム	ゾーン	リージョン
az-in-s	Azure southindia	チェンナイ
az-asia-hk	Azure eastasia	香港

情報コードとエラー検索テーブルを使用してもエラーを解決できない場合はどうすればよいですか**?**

Citrix サポートに問い合わせてください。

参照ドキュメント

- **Web** アプリを追加する
  - エンタープライズ Web アプリのサポート
  - Web アプリへの直接アクセスを構成する
- **SaaS** アプリを追加する
  - サービスとしてのソフトウェアアプリのサポート
  - SaaS アプリケーションサーバー固有の設定
- クライアントサーバーアプリを構成する
  - クライアントサーバーアプリのサポート
- アクセスポリシーの作成
  - アクセスポリシーの作成
- ルートテーブル
  - ルートテーブル