Citrix Secure Private Access

Machine translated content

Disclaimer

Contents

Citrix Secure Private Access

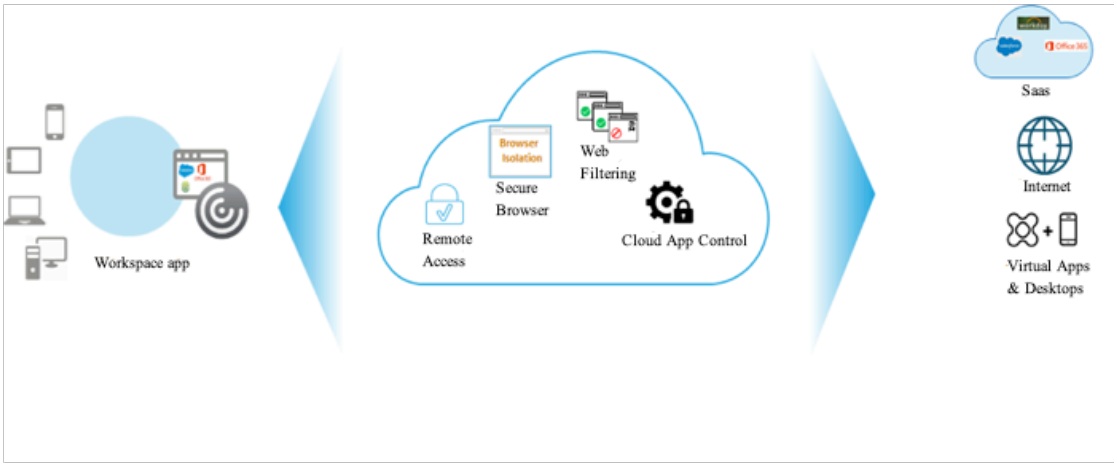
October 21, 2024

Citrix Secure Private Access サービスを使用すると、管理者は、シングル サインオン、リモート アクセス、コンテンツ検査を単一のソリューションに統合し、エンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。IT 管理者は、簡素化されたシングル サインオン エクスペリエンスを使用して、承認された SaaS アプリへのアクセスを管理できます。Citrix Secure Private Access サービスを使用すると、管理者は特定の Web サイトや Web サイト カテゴリへのアクセスをフィルタリングすることで、組織のネットワークとエンド ユーザー デバイスをマルウェアやデータ漏洩から保護することもできます。管理者は、SaaS アプリケーションへの安全なアクセスのために、強化されたアクセス セキュリティ ポリシーを適用できます。認証されると、従業員はオフィス内、自宅、出張先など、どこにいてもあらゆるデバイスからすべての重要なビジネス アプリケーションにアクセスできるようになります。

管理者は、悪意のある、危険な、または不明な Web サイトへのアクセス、消費された帯域幅、危険なダウンロードおよびアップロード動作などのユーザー アクティビティを監視できます。アクセスされた Web サイトと Web サイト カテゴリに関する分析を使用すると、管理者は企業ネットワークを保護するための是正措置を講じることができます。同時に、このサービスは、エンドユーザーにホストされているすべてのアプリへのシームレスで安全なアクセスを提供します。

管理者は、制限された印刷、ダウンロード、クリップボード アクセス (コピー アンド ペースト) などのアクションを制限することもできます。

次の図は、Secure Private Access サービスを視覚的に表したものです。



Citrix Secure Private Access の主な機能

Citrix Secure Private Access サービスを使用して実行できる主なタスクの一部を次に示します。

- シングル サインオン アクセスで **SaaS** アプリを公開する - ユーザーがプライマリ ID を使用して Citrix Workspace に認証されると、SaaS および Web アプリに対する後続の認証チャレンジは、SAML アサーションを使用する Citrix Cloud のシングル サインオン機能によって自動的に実行されます。

デフォルトでは、SAML アサーションは、ユーザーの Active Directory アカウント (ID プロバイダー) に関連付けられた電子メール アドレスと、ユーザーの SaaS または Web アプリ アカウント (サービス プロバイダー) に関連付けられた電子メール アドレスを利用します。

- **SaaS** アプリの強化されたセキュリティ ポリシーを設定します。**(**たとえば、透かし、コピー アンド ペーストの制限、ダウンロードの防止など**)** - コンテンツを保護するために、組織は SaaS アプリケーション内に強化されたセキュリティ ポリシーを組み込みます。各ポリシーは、デスクトップ用の Workspace アプリを使用する場合は Citrix Enterprise Browser に制限を適用し、Workspace アプリの Web またはモバイルを使用する場合は Secure Browser に制限を適用します。
  - 優先ブラウザ: ローカル ブラウザの使用を無効にし、Citrix Enterprise Browser エンジン (Workspace アプリ - デスクトップ) または Secure Browser (Workspace アプリ - モバイルおよび Web) に依存します。
  - クリップボード アクセスの制限: アプリとエンドポイント 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。
  - 印刷を制限する: アプリ ブラウザ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 SaaS アプリ内からダウンロードできないようにします。
  - ウォーターマークを表示: エンドポイントのユーザー名と IP アドレスを表示する画面ベースのウォーターマークをオーバーレイします。ユーザーが印刷したりスクリーンショットを撮ろうとすると、画面に表示されている通りの透かしが表示されます。
- コンテキスト アクセスを提供する - 承認された SaaS アプリは安全であると考えられていますが、SaaS アプリ内のコンテンツは実際には危険な場合があり、セキュリティ リスクとなります。ユーザーが SaaS アプリ内のハイパーリンクをクリックすると、トラフィックは Web フィルタリング機能を経由してルーティングされ、ハイパーリンクのリスク評価が提供されます。ハイパーリンクのリスク評価とカスタマイズされた URL カテゴリのリストに基づいて、Web フィルタリング機能は、ユーザーからのハイパーリンク要求を次のように許可、拒否、またはリダイレクトします。
  - 承認済み: ハイパーリンクは安全であると見なされ、Citrix Enterprise Browser は Workspace アプリ内でハイパーリンクにアクセスします。
  - 拒否: ハイパーリンクは危険であると判断され、アクセスが拒否されます。
  - リダイレクト: ハイパーリンク要求はセキュア ブラウザ サービスにリダイレクトされ、ユーザーのインターネット閲覧アクティビティはエンドポイント デバイス、企業ネットワーク、および SaaS アプリから分離されます。

- セキュリティとパフォーマンス分析 - ユーザーは必ず、セキュリティが強化された SaaS アプリにアクセスします。Workspace アプリ、Secure Private Access サービス、および Secure Browser サービスは、次のユーザーおよびアプリケーションの動作に関する情報をセキュリティ分析サービスに提供します。これらの分析は、ユーザーの全体的なリスク スコアに影響します。
  - アプリの起動時間
  - アプリ終了時間
  - 印刷アクション
  - クリップボードへのアクセス
  - URL アクセス
  - データのアップロード
  - データのダウンロード
- **Web** フィルタリング**:** Web フィルタリング機能は、SaaS アプリケーション内で選択された各ハイパーリンクのリスクを評価します。これらのサイトにアクセスし、ユーザーの行動の変化を監視すると、エンドポイント デバイスが侵害され、データの感染や暗号化が開始されたか、ユーザーとデバイスが知的財産を盗んでいることが示されるため、ユーザーの全体的なリスク スコアが高くなります。
- セキュリティ情報およびイベント管理 **(SIEM)** との統合 - セキュア プライベート アクセス ログは、Kafka 経由で Splunk、Sentinel、Elastic などの SIEM にエクスポートできます。ログを SIEM にエクスポートすると、セキュリティ機能が強化され、インシデント対応の有効性が向上します。詳細については、セキュア プライベート アクセス イベントを参照してください。

新機能

October 21, 2024

2024 年 **9** 月 **23** 日

- コンテキストベースのアプリルーティングとリソースの場所の選択をサポート

  アクセス ポリシーの動的ドメイン ルーティング構成により、管理者はユーザー コンテキストに基づいて URL ごとに内部ルーティング タイプを編集できるようになりました。管理者は、ユーザー要求が最適なデータ センターにルーティングされるようにリソースの場所を変更し、ユーザー要求が効率的に処理され、パフォーマンスが最適化されるようにすることができます。詳細については、コンテキストベースのアプリ ルーティングとリソースの場所の選択を参照してください。

2024 年 **8** 月 **15** 日

- ブロックされたユーザーリストのエントリを消去する期間を設定するオプション

管理者は、ブロックされたユーザー リスト内のエントリを消去するための特定の期間 (1 ～99 日) を設定できるようになりました。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、ユーザーをユーザー ブロック リストに追加する」を参照してください。

- 追加のセキュリティ制御

  アプリケーション アクセスを制限するために、次の追加のセキュリティ コントロールが利用できるようになりました。

  - マイク
  - Web カメラ
  - 通知
  - ポップアップ
  - 安全でないコンテンツ

  詳細については、アクセス制限オプションを参照してください。

- 非承認ウェブサイト（ウェブフィルタリング）機能の強化

  未承認の Web サイト (Web フィルタリング) 機能を使用すると、管理者は Citrix Enterprise Browser 経由ですべての未承認のトラフィックへのアクセスをデフォルトでブロックしたり、デフォルトで許可したりすることができます。詳細については、「非公認ウェブサイト」をご覧ください。

2024 年 7 月 16 日

- 追加のセキュリティ制御

  アプリケーション アクセスを制限するために、次の追加のセキュリティ コントロールが利用できます。

  - ファイルタイプによるダウンロード制限
  - ファイルタイプによるアップロード制限
  - 個人データのマスキング
  - プリンター管理
  - セキュリティ グループのクリップボード制限

  詳細については、アクセス制限オプションを参照してください。

- アプリ検出ページでの埋め込みドメインの表示

  アプリ検出機能を使用すると、メイン ドメインまたは埋め込みドメイン (HTTP/HTTPS) または宛先 IP アドレス (TCP/UDP) がアプリケーションに関連付けられていない場合、管理者は新しいアプリケーションを作成したり、既存のアプリケーションにそれらのドメインを追加したりできます。アプリ検出 ページには、メインドメインとその基礎となる埋め込みドメインの両方がツリー構造で表示されます。詳細については、「エンドユーザーがアクセスするドメインまたは IP アドレスを検出する」を参照してください。

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) は、管理者が管理コンソール内から構成の問題を分析し、トラブルシューティングするのに役立ちます。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基準に基づいて検索を絞り込み、ログの分析とトラブルシューティングを簡単に行うことができます。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を終了し、無効なユーザーリストにユーザーを追加するサポート

  管理者は、すべてのアクティブなエンドユーザー セッションを直ちに終了し、ユーザーを無効なユーザー 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、アクティブな Secure Private Access アプリケーション セッションがすべて終了し、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、無効なユーザー リストにユーザーを追加する」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

  Device Posture サービスでサポートされているブラウザ スキャンとウイルス対策スキャンが一般提供されました。詳細については、「デバイス姿勢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開始

  Device Posture サービスによるデバイス証明書チェックが一般提供されました。詳細については、「デバイス ポスチャ サービスによるデバイス証明書のチェック」を参照してください。

2023 年 12 月 20 日

- オンプレミスのセキュアプライベートアクセスの一般提供

  オンプレミス向け Citrix Secure Private Access が一般提供されました。詳細については、「新機能」をご覧ください。

2023 年 10 月 16 日

- セキュアプライベートアクセスオンプレミスソリューションのプレビュー機能

  Secure Private Access 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 ポリシーを構成するための管理 UI。
  - ログダッシュボード。

  詳細については、「オンプレミスのセキュア プライベート アクセス」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 サービスでは、次のチェックが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 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 サービスでは、地理位置情報とネットワーク ロケーションのチェックがサポートされるようになりました。

  詳しくは、「Device Posture」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提供開始

  Microsoft Intune とのデバイス ポスチャ統合が一般提供されました。詳細については、「Microsoft Intune と Device Posture 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 サービス用の **Citrix** エンドポイント分析クライアントを管理する

  EPA クライアントは、NetScaler および Device Posture と併用できます。NetScaler および Device Posture 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構成変更が必要です。詳細については、「Citrix Endpoint Analysis Client for Device Posture サービスの管理」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。詳しくは、「Device Posture」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 Device Posture** サービスによるデバイス証明書のチェック

  Citrix Device Posture サービスでは、エンド デバイスの証明書を企業の証明機関と照合してエンド 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。詳細については、「デバイス ポスチャ サービスによるデバイス証明書のチェック」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が DaaS モニターで検索できるようになりました。詳細については、「Citrix DaaS Monitor 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

- オンプレミスのセキュアプライベートアクセスを構成するためのツール

  オンプレミス ソリューションの Secure Private Access を構成するための簡素化されたユーザー インターフェイスが利用できるようになりました。構成ツールを Citrix Virtual Apps and Desktops 配信コントローラーで実行して、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、アプリケーションの制限、トラフィック ルーティング、および NetScaler Gateway 設定を設定することもできます。詳細については、/en-us/citrix-secure-private-access/service/secure-private-access-for-on-plex-config-tool.htmlを参照してください。

29 May 2023

- 複数のルールを含むアクセスポリシーの作成の一般提供

  複数のアクセス ルールを作成し、単一のポリシー内で異なるユーザーまたはユーザー グループに対して異なるアクセス条件を設定できます。これらのルールは、単一のポリシー内で、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 ポリシーを構成する」を参照してください。

  [SPA-746]

2023 年 4 月 10 日

- アプリケーションの検出

  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) などの内部プライベート アプリケーションや、それらのアプリケーションにアクセスするユーザーを可視化できます。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出できます。詳細については、アプリケーションの検出を参照してください。

  [ACS-2325]

2023 年 3 月 29 日

- オンプレミス展開向けの安全なプライベートアクセスソリューション

  Citrix StoreFront および NetScaler Gateway のお客様は、オンプレミス展開用の Citrix Secure Private Access ソリューションを使用して、Citrix Virtual Apps および仮想デスクトップとともに、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、「オンプレミスのセキュア プライベート アクセス」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、次のユースケースで使用できます。

  - バックエンド サーバーの DNS サフィックス ドメインを追加することで、Citrix Secure Access クライアントが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) に解決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構成できるようにすることで、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 アドレスに解決するための DNS サフィックス 」を参照してください。

  [ACS-2490]

2023 年 1 月 23 日

- デバイス姿勢サービス

  Citrix Device Posture サービスは、Citrix DaaS (仮想アプリとデスクトップ) または Citrix Secure Private Access リソース (SaaS、Web アプリ、TCP、UDP アプリ) にアクセスするためにエンド デバイスが満た

す必要がある特定の要件を管理者が強制するのに役立つクラウド ベースのソリューションです。詳しくは、「Device Posture」を参照してください。

[AAUTH-90]

- **Microsoft Endpoint Manager** と **Device Posture** 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。Device Posture は、Windows および macOS 上の Microsoft Endpoint Manager (MEM) と統合されています。詳細については、「Microsoft Endpoint Manager と Device Posture 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向けの **Workspace 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、Citrix Workspace アプリ経由ですでにログインしている場合、Workspace URL へのシングル 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、複数の認証を回避することでユーザー エクスペリエンスが向上します。詳細については、ワークスペース 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、エンドユーザーがアプリを利用できるように、管理者が一致するユーザー 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ことが必要になりました。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

  構成ウィザードのアプリケーション セクションから、アプリ サブスクライバー構成オプションが削除されます。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、管理者はアプリ サブスクライバーを追加し、セキュリティ制御を構成します。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。

  [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適応型アクセス

  管理者は、Citrix Analytics for Security (CAS) によって提供されるユーザー リスク スコアを使用して、適応型アクセス 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適応型アクセス」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適応型アクセス

  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、適応型アクセス ポリシーを構成できるようになりました。場所は、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の場所になります。詳細については、「場所に基づいた適応型アクセス」を参照してください。

  [ACS-99]

- 強化された適応型アクセス ポリシー ビルダー

  設定された条件が満たされた後にのみ、アプリへのアクセスが有効になります。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 (許可または制限) できます。これにより、許可された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るようになります。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]

- 強化されたダッシュボード

  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、いくつかのユーザーメトリックの詳細な可視性が提供され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]

- ライブラリの廃止

  Secure Private Access アプリケーションは、Citrix Cloud ライブラリ内に表示されなくなりました。Secure Private Access が構成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、構成できるようになります。

  [ACS-1546]

- セキュアプライベートアクセスの監査ログ

  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。詳細については、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 イベントが 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 スクリプトを通じてアクセスできます。詳細については、「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。詳細については、「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構成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

  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、アプリへのアクセスが有効になります。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することはできません。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るようになります。管理者は、既存のアプリ 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。詳細については、「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

  Adaptive Authentication が一般提供 (GA) されました。Adaptive Authentication の詳細については、Adaptive Authentication 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名が変更されました。

  [ACS-2322]

- 管理者ガイドによるワークフローでオンボーディングとセットアップが簡単

  Secure Private Access には、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 アクセスを構成するための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が追加されました。これには、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、適応型アクセス ポリシーなどの構成が単一の管理コンソール内に含まれています。詳細については、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参照してください。

  この機能は現在、一般提供 (GA) されています。

  [ACS-1102]

- セキュアプライベートアクセスダッシュボード

  Secure Private Access ダッシュボードでは、管理者は、トップ アプリ、トップ ユーザー、コネクタの正常性状態、帯域幅の使用状況を 1 か所で完全に把握できます。このデータは Citrix Analytics から取得されます。詳細については、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 (GA) されています。

  [ACS-1169]

- エンタープライズウェブアプリへの直接アクセス

  お客様は、Chrome、Firefox、Safari、Microsoft Edge などのネイティブ Web ブラウザから直接、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。

  この機能は現在、一般提供 (GA) されています。

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

Citrix のお客様は、内部 Web アプリに加えて、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。詳細については、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 (GA) されています。

[ACS-970]

- エンタープライズ **Web**、**TCP**、**SaaS** アプリケーション向けの適応型アクセスおよびセキュリティ制御

  Citrix Secure Private Access サービスの適応型アクセス機能は、アプリケーションへの安全なアクセスを実現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、ユーザーによるアプリへのアクセスを、コンテキストに基づいて詳細なレベルで設定できます。ここでの「コンテキスト」という用語は、次のものを指します。

  - 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）
  - 場所（位置情報またはネットワークの場所）
  - Device posture（デバイスの態勢チェック）
  - リスク（ユーザーリスクスコア）

  詳細については、「エンタープライズ Web、TCP、および SaaS アプリケーション向けの適応型アクセスおよびセキュリティ制御」を参照してください。

  この機能は現在、一般提供 (GA) されています。

  [ACS-878、ACS-879、ACS-882]

- セキュアプライベートアクセスの監査ログ

  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。詳細については、監査ログを参照してください。

  この機能は現在、一般提供 (GA) されています。

  [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 イベントが 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 スクリプトを通じてアクセスできます。詳細については、「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 (GA) されています。

  [ACS-805]

- 適応型認証サービス

Citrix Cloud のお客様は、Citrix Workspace を使用して、Citrix Virtual Apps and Desktops に Adaptive Authentication 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。Adaptive Authentication 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、Adaptive Authentication 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 アプリケーションのサポート 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、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。

  詳細については、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** の単一のセキュア プライベート アクセスに統合

  Citrix Gateway サービス タイルは、Citrix Cloud 内の単一の Secure Private Access に統合されました。

  - Citrix Workspace Essentials および Citrix Workspace Standard を含むすべての Secure Private Access のお客様は、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、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 顧客は、引き続き Workspace 構成から Citrix Gateway サービスを HDX プロキシとして有効にできます。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ための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できます。詳細については、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たエンタープライズ **Web** および **SaaS** アプリのコンテキスト アクセスとセキュリティ制御

Citrix Secure Private Access サービスでは、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 アクセスがサポートされ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、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、ユーザーは引き続き非表示のアプリにアクセスできます。

  [ACS-944]

2021 年 6 月 9 日

- アプリの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 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 経由で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 フローを定義する方法に応じて、アプリのルート 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 コネクタ経由の外部として定義できます。

  [ACS-243]

22 May 2021

- 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 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実現する包括的なゼロ 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 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い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 コンピューター) を指します。

  [ACS-222]

- **Citrix Gateway Connector** ユーザーインターフェイスのブランド変更

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

  [NGSWS-17100]

01 May 2021

- **Citrix Secure Private Access** サービス 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、サービス利用資格の有効期限が切れてから 90 日後に 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ションする手順を簡略化

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

  [ACS-351]

- 接続テストツールの強化

  Citrix Gateway Connector の接続テスト ツールが強化され、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なりました。

  [NGSWS-17212]

2021 年 3 月 15 日

- プラットフォームの強化

  顧客の管理構成を Citrix Gateway コネクタに伝播する際の信頼性を高めるために、さまざまなプラットフォームの機能強化が行われます。

  [ACS-85]

- ウェブ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 ブラウザーから Web アプリケーションにアクセスする場合の 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 は、Citrix Cloud サービスおよびその他のバックエンド サーバーに接続するために、グレード A 以上の暗号スイートを備えた TLS1.2 を使用するようになりました。

  [NGSWS-16068]

2020 年 11 月 11 日

- **Citrix Access Control** サービスの名前変更

  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** アプリを起動するためのセキュリティ オプションが強化されました

  管理者は、強化されたセキュリティ オプションを使用できるようになりました。「**Citrix** リモート ブラウザー分離サービスで常にアプリケーションを起動する」を選択すると、他の強化されたセキュリティ設定に関係なく、常にリモート ブラウザー分離サービスでアプリケーションを起動できます。

  [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設定における **RBAC** 制御

  Citrix Secure Private Access ブラウザ拡張機能の管理設定で RBAC 制御が適用されるようになりました。

  [NGSWS-14427]

2020 年 9 月 24 日

- ローカルブラウザ経由でエンタープライズ **Web** アプリへの **VPN** なしのアクセスを有効にする

  Citrix Secure Private Access ブラウザ拡張機能を使用して、ローカル ブラウザ経由でエンタープライズ Web アプリに VPN なしでアクセス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** 構成の検証

  これで、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 サービスの管理者への読み取り専用アクセスなど、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、アプリの詳細を表示する権限のみを持ちます。
  - 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 アクセス設定の表示のみが可能です。

  [ACS-205]

08 May 2020

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

  - 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。詳細については、「Citrix Gateway Connector 登録の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**:** これで、接続テスト 機能を使用して、ゲートウェイ コネクタの構成にエラーがないこと、およびゲートウェイ コネクタが URL に接続できることを確認できます。詳細については、「Citrix Gateway Connector にログオンしてセットアップする」を参照してください。

    [NGSWS-8580]

2019.04.02 更新

- **Citrix Gateway Connector** から送信プロキシへの **Kerberos** 認証のサポート [NGSWS-6410]

  Citrix Gateway Connector から送信プロキシへのトラフィックに対して Kerberos 認証がサポートされるようになりました。ゲートウェイ コネクタは、構成されたプロキシ資格情報を使用して、送信プロキシに対して認証します。

2019.04.01 更新

- **Web/SaaS** アプリのトラフィックを企業ネットワークでホストされたゲートウェイコネクタ経由で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外でホストされている SaaS アプリを公開している場合、そのアプリのトラフィックがオンプレミスのゲートウェイ コネクタを通過するように認証するためのサポートが追加されました。

  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。実際の Workday データ トラフィックが Citrix Gateway サービス経由で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がオンプレミスの Gateway Connector 経由で Citrix Gateway サービス経由でルーティングされることを顧客が希望する場合があります。これにより、ユーザーは企業ネットワーク内から Okta サーバーに接続するときに、Okta サーバーからの 2 要素認証を回避できます。

  [NGSWS-6445]

- ウェブサイトリストのフィルタリングとウェブサイトの分類を無効にする。管理者が特定の顧客に対して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 ブラウザ分離サービスのリダイレクトの自動地理ルーティング。リモート ブラウザ分離サービスのリダイレクトに対して自動地理ルーティングが有効になりました。

  [NGSWS-6926]

2019.03.01 更新

- 「ゲートウェイコネクタの追加」ページに「検出」ボタンが追加されました。検出 ボタンを使用すると、コネクタのリストが更新され、新しく追加されたコネクタが Web アプリ接続セクションに反映されます。

  [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「悪意のある危険なもの」が追加されました。アクセス制御 **Web** フィルタリング カテゴリの 悪意のある危険 という名前の新しいカテゴリが、マルウェアとスパム グループの下に追加されます。

  [CGOP-6205]

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。

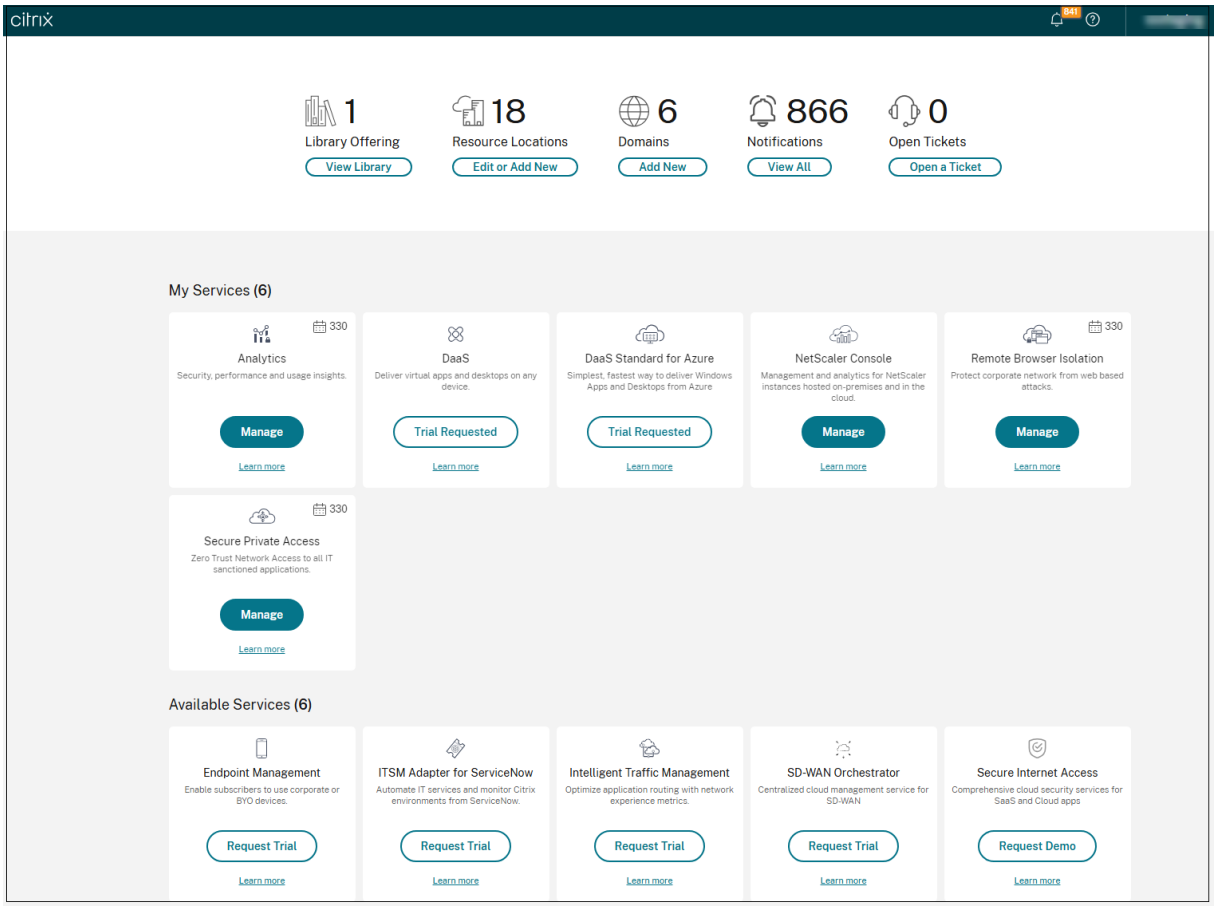
ステップ 1: **Citrix Cloud** にサインアップ

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

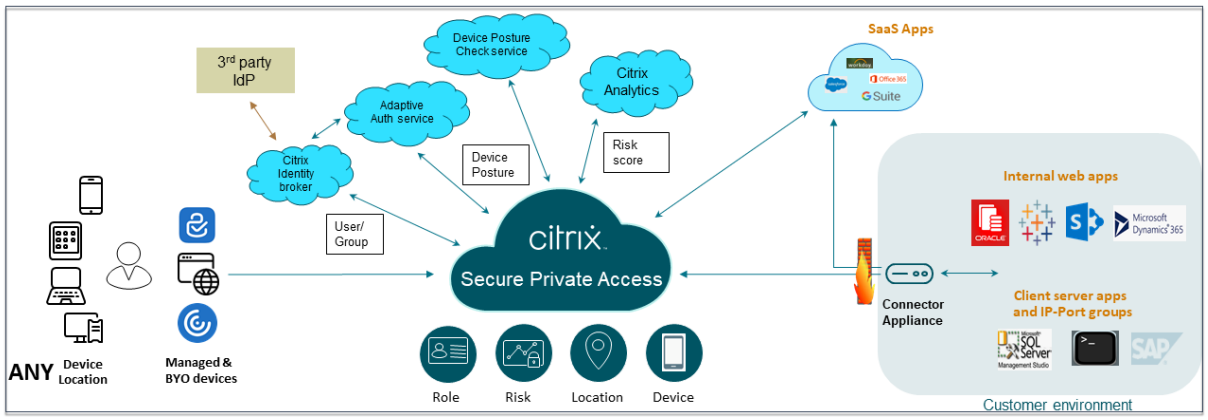
October 21, 2024

ソリューションの概要

従来の VPN ソリューションでは、エンドユーザー デバイスを管理し、ネットワーク レベルでアクセスを提供し、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 に提供し、管理対象デバイスか BYO デバイスかを問わず、あらゆるデバイスから IT 承認アプリケーションにアクセスする選択肢をユーザーに提供します。

Citrix Secure Private Access は、適応型認証、シングル サインオン サポート、アプリケーションの強化されたセキュリティ制御を提供します。Secure Private Access は、デバイス ポスチャ 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提供します。管理者は、適応認証またはデバイス ポスチャの結果に基づいて、アプリの認証方法を定義できます。



適応型セキュリティ

適応認証は、現在のリクエストに適した認証フローを決定します。適応認証は、デバイスの状態、地理的な場所、ネットワーク セグメント、ユーザーの組織/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 承認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わたって同じ認証ポリシー フレームワークを実装できます。詳細については、アダプティブ 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 を使用すると、VPN に依存せずにオンプレミスの Web アプリへの接続を作成できます。この VPN なしの接続では、オンプレミスに展開されたコネクタ アプライアンスが使用されます。コネクタ アプライアンスは、組織の Citrix Cloud サブスクリプションへの送信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

Adaptive Authentication 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 Web、クライアント サーバー アプリに対して同じ Adaptive Authentication 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。

ブラウザのセキュリティ

Secure Private Access により、エンド ユーザーは集中管理され、セキュリティ保護されたエンタープライズ ブラウザー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を最適に提供する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。

デバイスの姿勢

デバイス ポスチャ 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するエンドポイント デバイスのポスチャをチェックするためのポリシーを定義できます。デバイス ポスチャ サービスは、エンドポイントのコンプライアンス ステータスに基づいて、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、デバイス ポスチャ 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、この情報をデバイス ポスチャ 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 サービスと Citrix Secure Private Access を統合すると、Citrix Cloud の回復力と拡張性を活かして、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、「デバイスの状態」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、エンドポイントにフロントエンドがあり、データ センターにバックエンドがあるプライベート 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対して厳格なセキュリティ ポリシーを適切に適用できるため、リモート ユーザーがセキュリティ プロトコルに違反する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は困難になります。

セキュア プライベート アクセス 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 および UDP のセキュリティ脆弱性に対処します。ユーザーは、自分のマシンで実行されている Citrix Secure Access クライアントを介して、ネイティブ ブラウザーまたはネイティブ クライアント アプリケーションを使用して、TCP、UDP、HTTPS アプリを含むすべてのプライベート アプリにアクセスできるようになりました。

ユーザーは、クライアント デバイスに Citrix Secure Access クライアントを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。

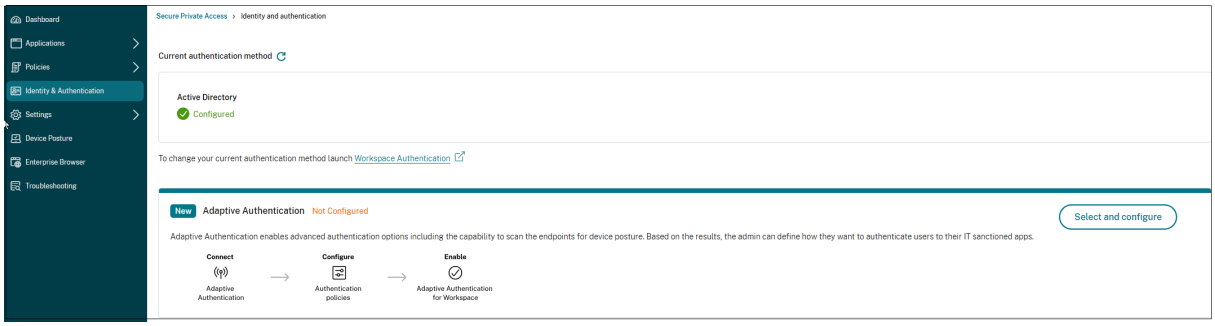
詳細については、クライアント サーバー アプリのサポートを参照してください。

Citrix セキュアプライベートアクセスを設定する

Secure Private Access 管理コンソールを使用して、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 アクセスを有効にします。このコンソールには、適応型認証、ユーザー サブスクリプションを含むアプリケーション、適応型アクセス ポリシーの構成が含まれています。

ID と認証を設定する

加入者が 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

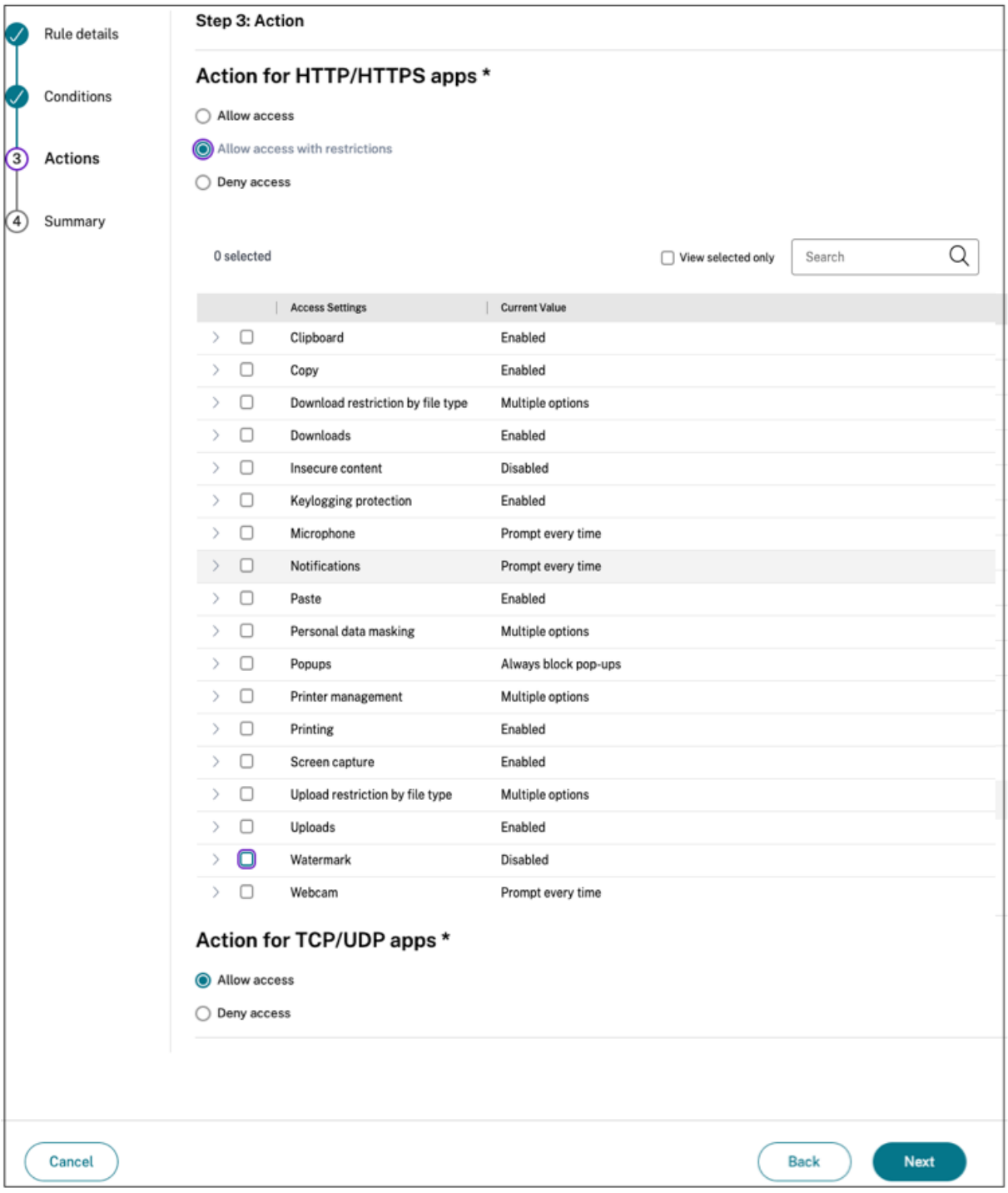
認証方法を選択したら、管理コンソールを使用して Web、SaaS、または TCP および UDP アプリを構成します。詳細については、「アプリの追加と管理」を参照してください。

強化されたセキュリティ制御を有効にする

コンテンツを保護するために、組織は SaaS アプリケーション内に強化されたセキュリティ ポリシーを組み込みます。各ポリシーは、デスクトップ用の Workspace アプリを使用する場合は Citrix Enterprise Browser に制限を適用し、Workspace アプリの Web またはモバイルを使用する場合は Secure Browser に制限を適用します。

- 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。
- 印刷を制限する: 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、ユーザー名とユーザーのマシンの IP アドレスを表示するウォーターマークを表示します。

- キーロギングを制限: 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、ユーザーがアプリ上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 で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 文書を編集する場合、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 ポリシーを構成する」を参照してください。

アプリケーションの起動に **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) を使用してアプリを起動できるようになります。CEB は、Citrix Workspace アプリと統合された Chromium ベースのブラウザーであり、

Citrix Enterprise Browser 内で Web アプリや SaaS アプリにシームレスかつ安全にアクセスできます。

CEB は、セキュリティ ポリシーを備えたすべての内部ホスト Web アプリまたは SaaS アプリの優先ブラウザーまたは作業用ブラウザー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構成されたすべての SaaS/Web アプリ 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、Global App Configuration サービス (GACS) を使用して、Citrix Enterprise Browser をデフォルトのブラウザーとして構成し、Citrix Workspace アプリから Web アプリや SaaS アプリを起動できます。

API による設定**:**

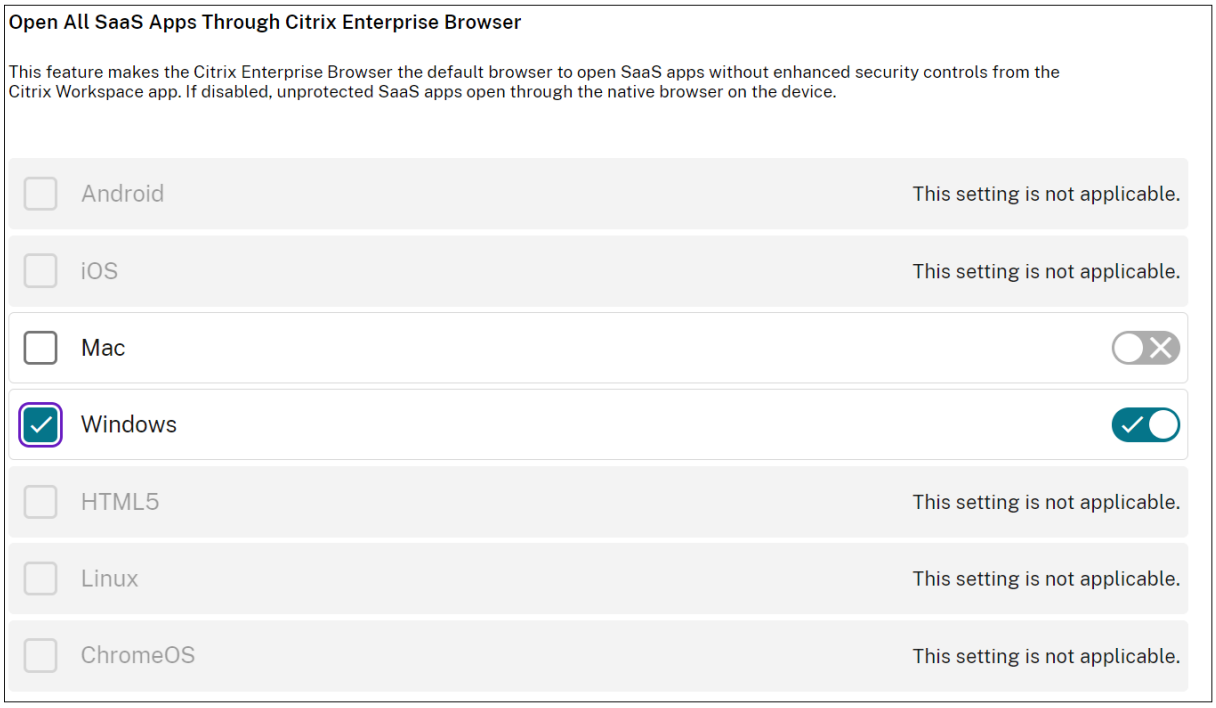
構成するには、デフォルトですべてのアプリに対して Citrix Enterprise Browser を有効にする JSON ファイルの例を次に示します。

```
"settings": [
                    {

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

                    ]
```

デフォルト値は、true です。

GUI による構成**:**

アプリの起動時に CEB をデフォルトのブラウザにする必要があるデバイスを選択します。

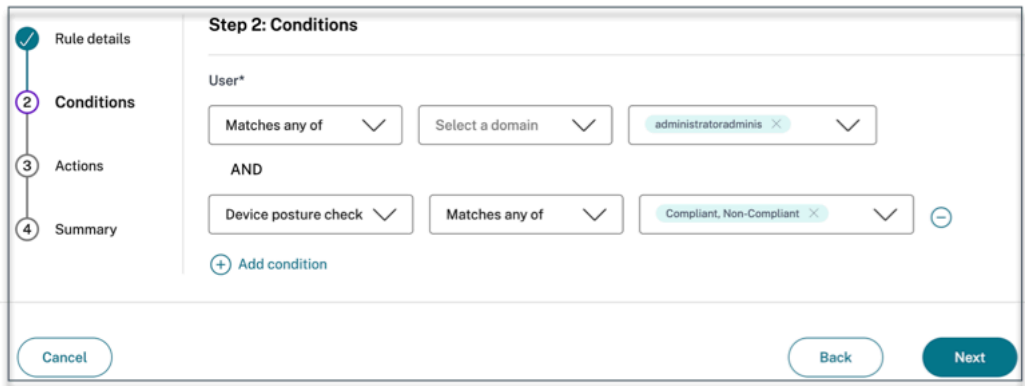


詳細については、「GACS を介して Citrix Enterprise Browser を管理する」を参照してください。

デバイス姿勢を使用してコンテキストアクセス用のタグを構成する

デバイスの姿勢の検証後、デバイスのログインが許可され、デバイスは準拠または非準拠として分類されます。この分類は、Secure Private Access サービスへのタグとして利用可能になり、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。

1. Citrix Cloud にサインインします。
2. 「セキュア プライベート アクセス」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アプリまたはアプリのセットを選択します。
6. ポリシーのルールを作成するには、[ルールの作成] をクリックします。
7. ルール名とルールの簡単な説明を入力し、[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に満たす必要がある必須条件です。
9. デバイスの姿勢条件を追加するには、**+** をクリックします。
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 - 準拠デバイスの場合
   - 非準拠 - 非準拠デバイスの場合

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。

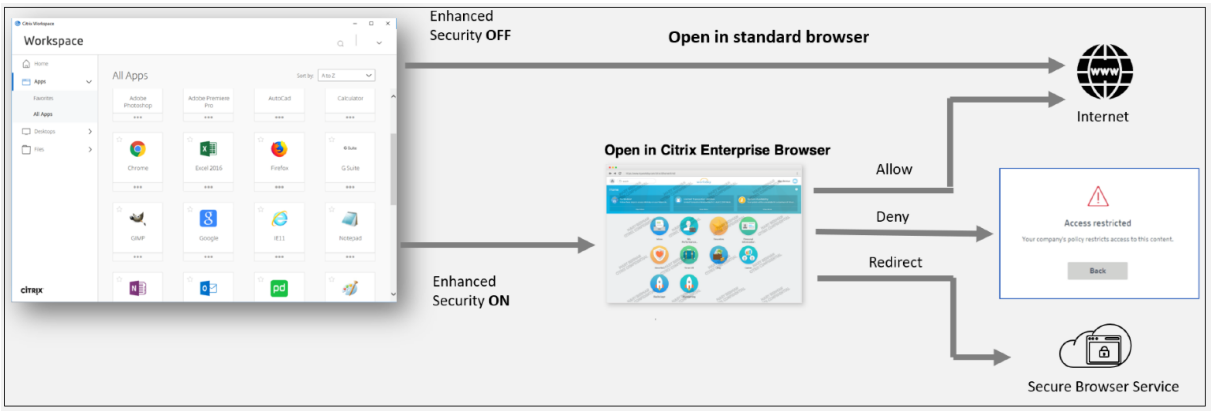
    概要ページにはポリシーの詳細が表示されます。

14. 詳細を確認し、[完了] をクリックします。

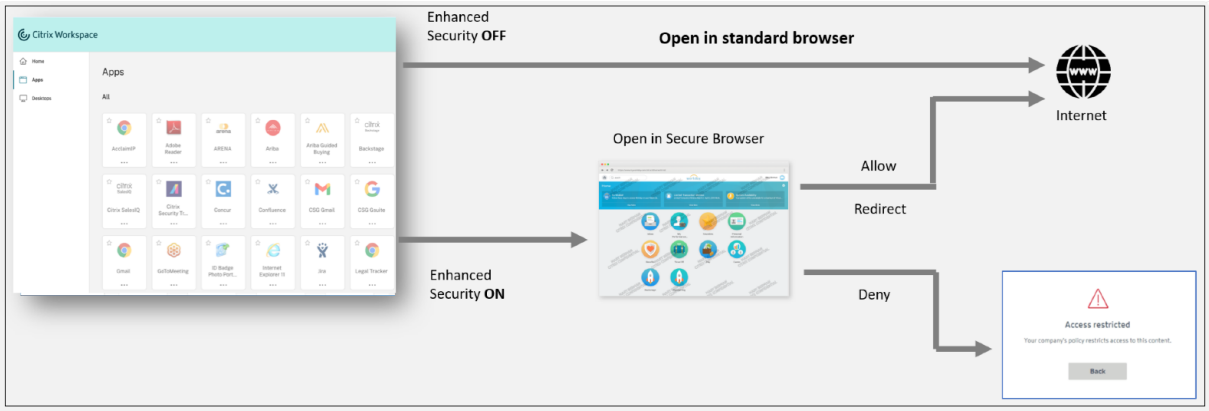
> 注意:
>
> アクセス ポリシーで準拠または非準拠としてタグ付けされていない Secure Private Access アプリケーションは、デフォルトのアプリケーションとして扱われ、デバイスの状態に関係なくすべてのエンドポイントでアクセス可能になります。

エンドユーザーエクスペリエンス

Citrix 管理者は、Citrix Secure Private Access を利用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 ポイントです。エンドユーザーは、Citrix Workspace アプリを通じて仮想アプリ、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。強化されたセキュリティ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。管理者が強化されたセキュリティ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、未承認の Web サイト ポリシーに基づいて制御されます。非公認ウェブサイトの詳細については、「非公認ウェブサイト」を参照してください。



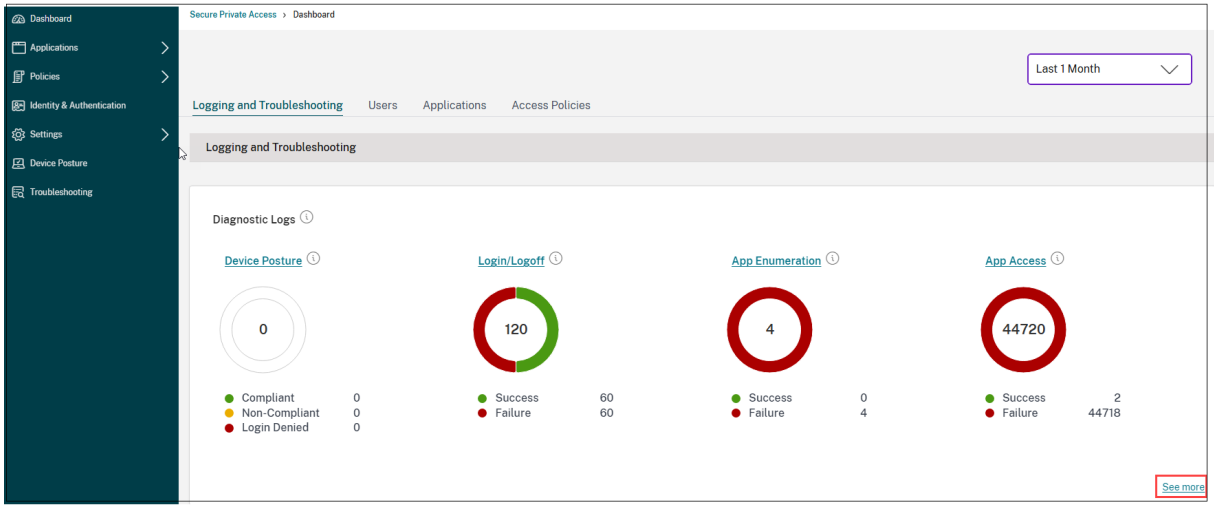
同様に、Workspace Web ポータルでは、強化されたセキュリティが無効になっている場合、SaaS アプリケーションはネイティブにインストールされた標準ブラウザで開かれます。強化されたセキュリティを有効にすると、SaaS アプリは安全なリモート ブラウザーで開かれます。ユーザーは、未承認の Web サイト ポリシーに基づいて、SaaS アプリ内の Web サイトにアクセスできます。非公認ウェブサイトの詳細については、「非公認ウェブサイト」を参照してください。

分析ダッシュボード

Secure Private Access サービスのダッシュボードには、SaaS、Web、TCP、UDP アプリの診断データと使用状況データが表示されます。ダッシュボードを使用すると、管理者はアプリ、ユーザー、コネクタの正常性状態、帯域幅の使用状況を 1 か所で完全に把握できます。このデータは Citrix Analytics から取得されます。メトリックは、大きく分けて次のカテゴリに分類されます。

- ログ記録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

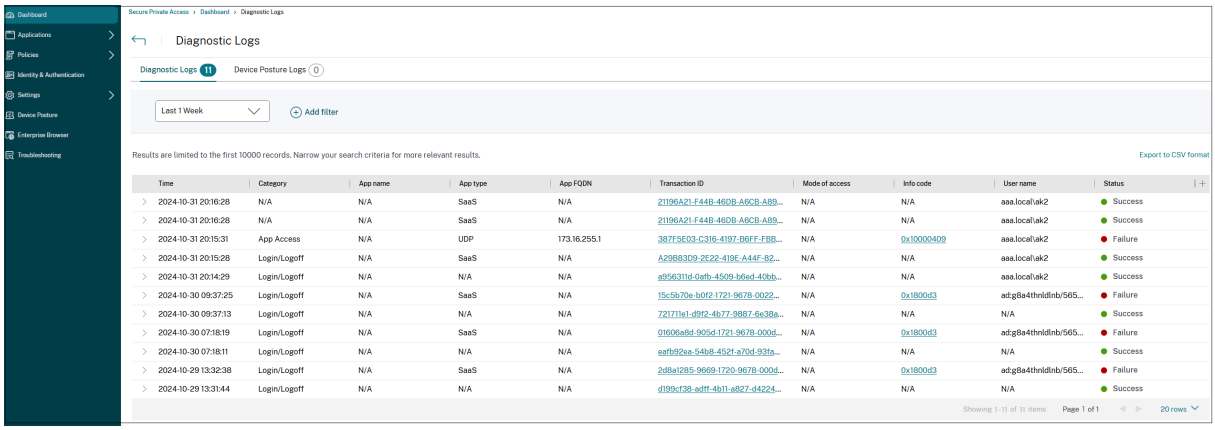
詳細については、ダッシュボードを参照してください。



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、アプリケーションの起動、アプリの列挙、デバイスのポスチャ 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、関連付けられた情報コードがあります。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の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 アクセス要求で、認証から始まり、ワークスペース アプリ内でのアプリの列挙、そしてアプリ アクセス自体まで、複数のログが生成される場合があります。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 アクセス要求に関連するすべてのログを見つけることができます。詳細については、「セキュア プライベート アクセスの問題のトラブルシューティング」を参照してください。



使用例の例

- 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）にアクセスします。
- ユーザーがアクセスする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する
- 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 管理の SaaS アプリのセキュリティ強化
- Office 365 のセキュリティ強化
- Okta アプリのセキュリティ強化

参考記事

- セキュアプライベートアクセスの概要
- 技術概要
- 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
- 管理者ガイド付きのワークフローでオンボーディングとセットアップが簡単

参考動画

- 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 アクセス
- Citrix Secure Private Access によるパブリック SaaS アプリへのアクセス
- 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 アクセス
- Citrix Secure Private Access によるキーロガー保護
- Citrix Secure Private Access による画面共有の保護
- 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 を使用した ZTNA と VPN ログオン エクスペリエンスの比較
- Citrix Secure Private Access を使用した ZTNA と VPN 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 DaaS: 新機能
- Citrix Secure Access クライアント NetScaler Gateway クライアント

管理者ガイド付きのワークフローでオンボーディングとセットアップが簡単

October 21, 2024

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 アクセスを構成するためのステップバイステップのプロセスを備えた、合理化された新しい管理エクスペリエンスが、Secure Private Access サービスで利用できます。これには、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、適応型アクセス ポリシーなどの構成が単一の管理コンソール内に含まれています。

このウィザードは、オンボーディング中または繰り返し使用中に管理者がエラーのない構成を実現するのに役立ちます。また、全体的な使用状況メトリックやその他の重要な情報を完全に表示できる新しいダッシュボードも利用できます。

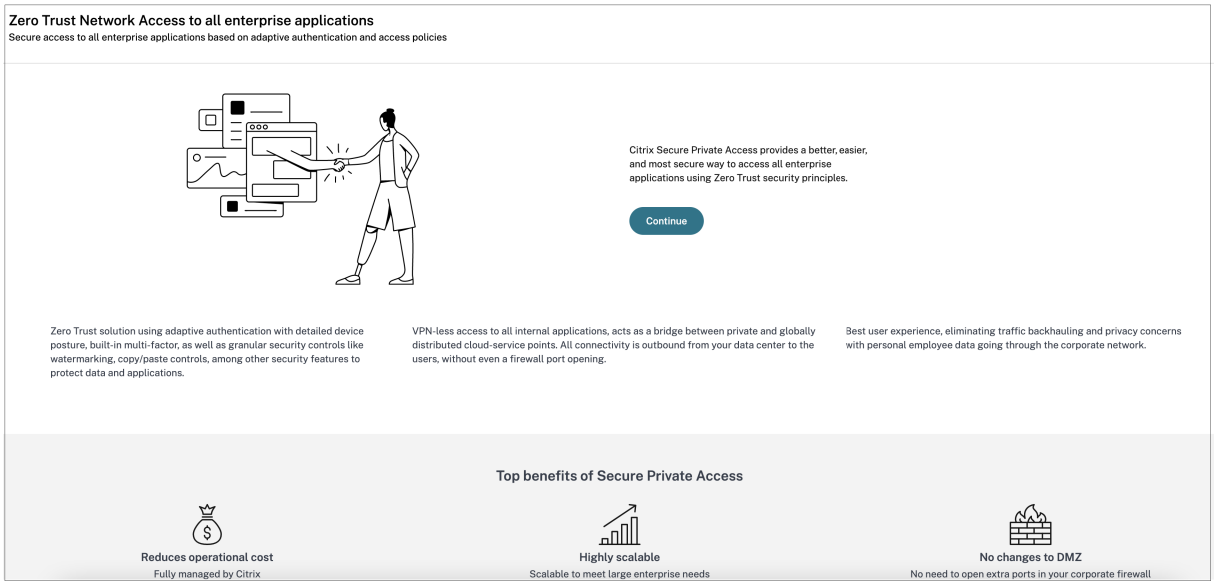
大まかな手順は次のとおりです。

1. 加入者が Citrix Workspace にログインするための認証方法を選択します。
2. ユーザー向け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. アプリの構成を確認します。

セキュアプライベートアクセス管理者ガイド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。

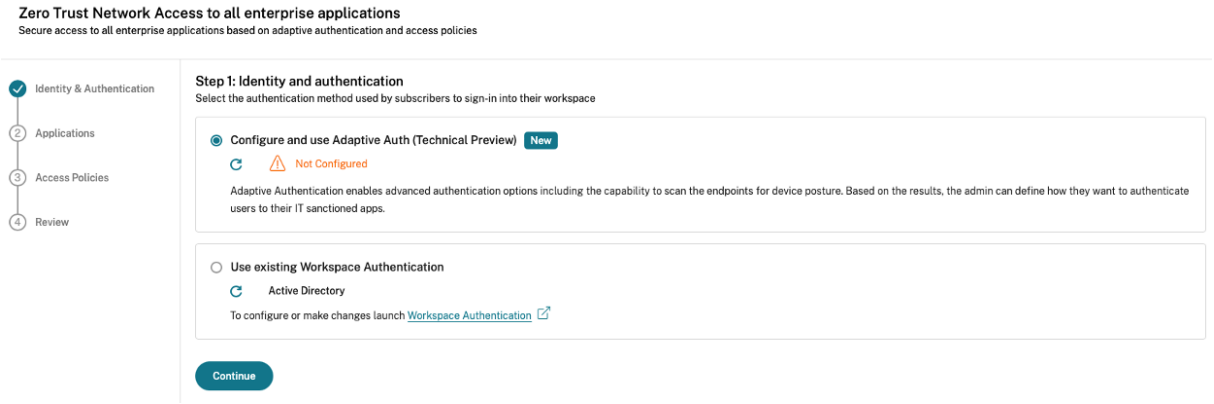
1. **Secure Private Access** サービス タイルで、管理をクリックします。
2. 概要ページで、[続行] をクリックします。



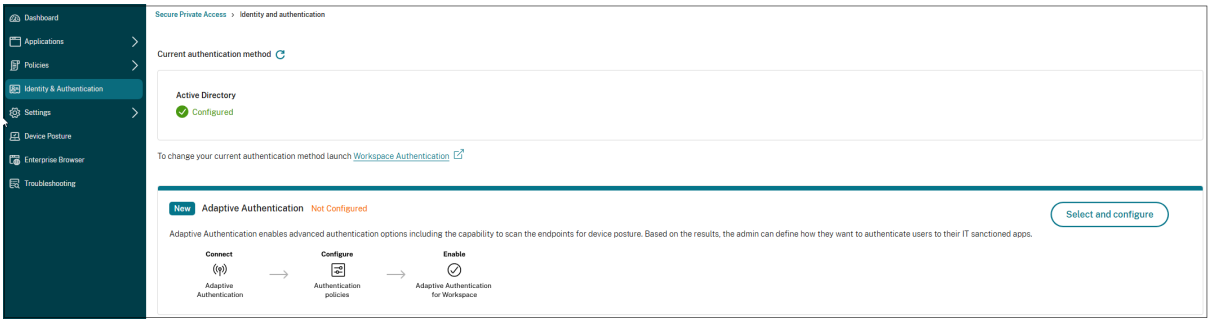
ステップ **1: ID** と認証を設定する

加入者が 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。Adaptive Authentication サービスは、Citrix がホストし、Citrix が管理し、クラウドでホストされる Citrix 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
- デバイスの姿勢スキャン
- 条件付き認証
- Citrix Virtual Apps and Desktops への適応型アクセス
- Adaptive Authentication を構成するには、**Adaptive Auth (**テクニカル プレビュー**)** を構成して使用するを選択し、構成を完了します。Adaptive Authentication の詳細については、Adaptive Authentication サービスを参照してください。Adaptive Authentication を構成した後、必要に応じて 管理 をクリックして構成を変更できます。



- 最初に別の認証方法を選択し、Adaptive Authentication に切り替える場合は、をクリックして を選択し、構成を完了します。



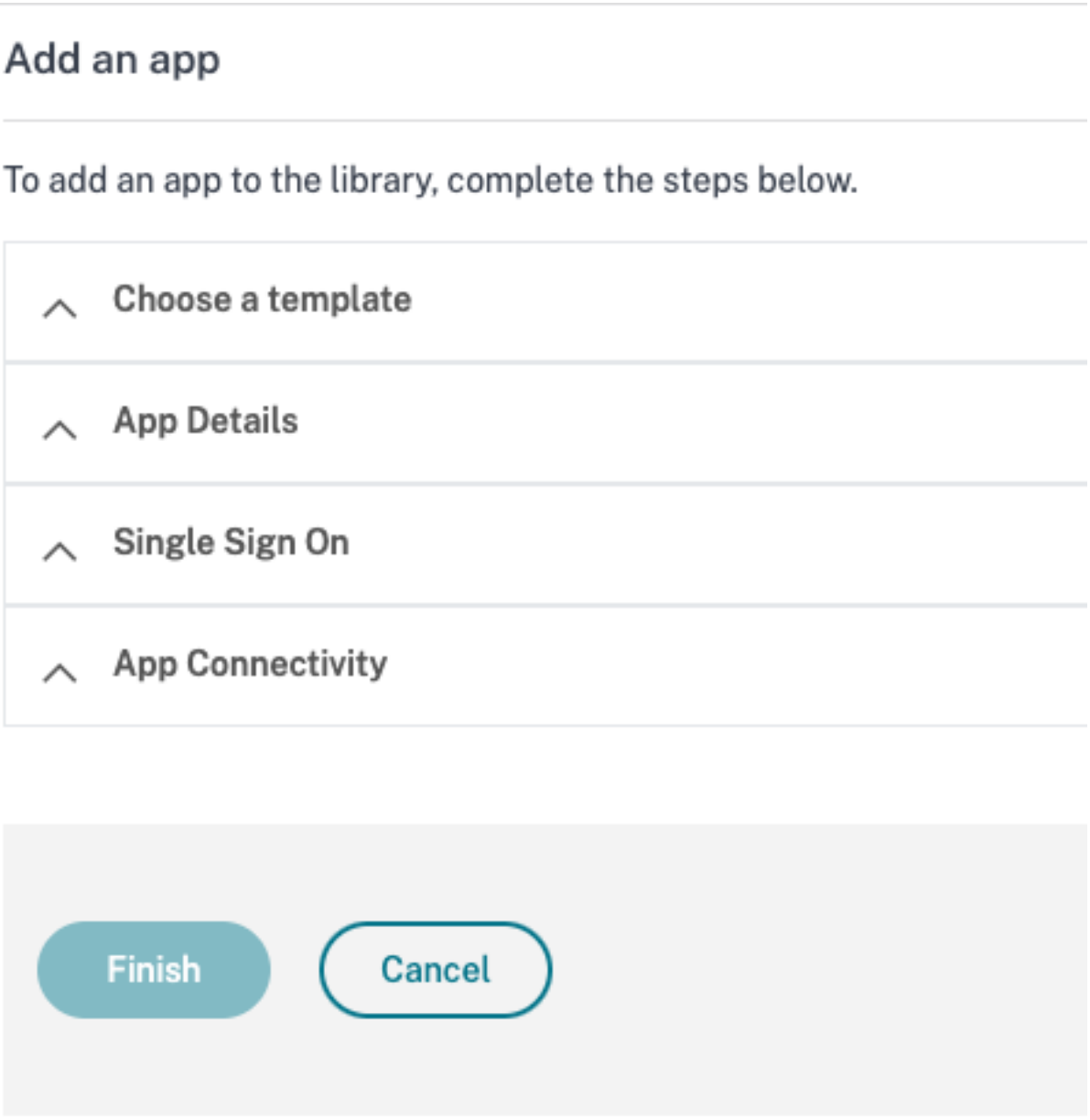
既存の認証方法を変更するには、ワークスペース認証をクリックします。

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構成します。初めてのユーザーの場合、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。アプリを追加をクリックしてアプリを追加します。このページから、SaaS アプリ、Web アプリ、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、ここにリストされます。

アプリを追加するには、次の図に示す手順を完了します。



- エンタープライズ **Web** アプリを追加する
  - エンタープライズウェブアプリのサポート
  - 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 サーバー固有の構成
- 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
  - 構成されたアプリを起動する - エンドユーザー ワークフロー
- 管理者に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:** 複数のルールを含むアクセスポリシーを構成する

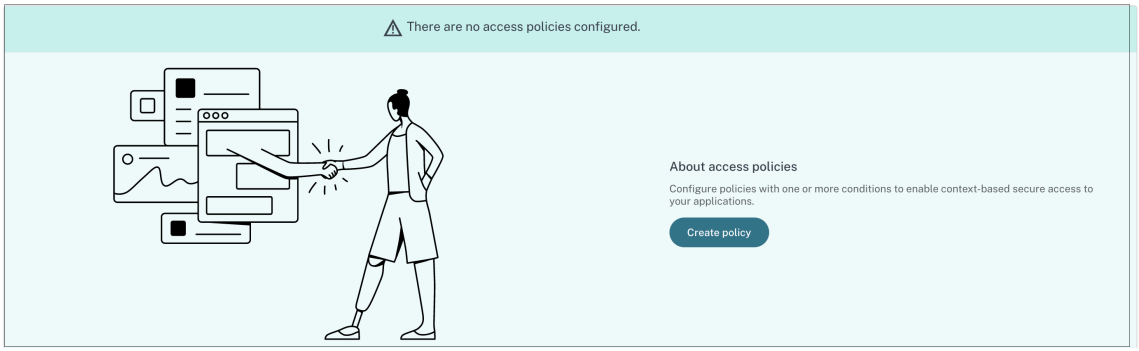
複数のアクセス ルールを作成し、単一のポリシー内で異なるユーザーまたはユーザー グループに対して異なるアクセス条件を設定できます。これらのルールは、単一のポリシー内で、HTTP/HTTPS アプリケーションと TCP/UDP アプリケーションの両方に個別に適用できます。

Secure Private Access 内のアクセス ポリシーを使用すると、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することができます。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。

- クリップボードアクセスを制限
- 印刷を制限する
- ダウンロードを制限する
- アップロードを制限する
- 透かしを表示
- キーロギングを制限する
- スクリーン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」を参照してください。

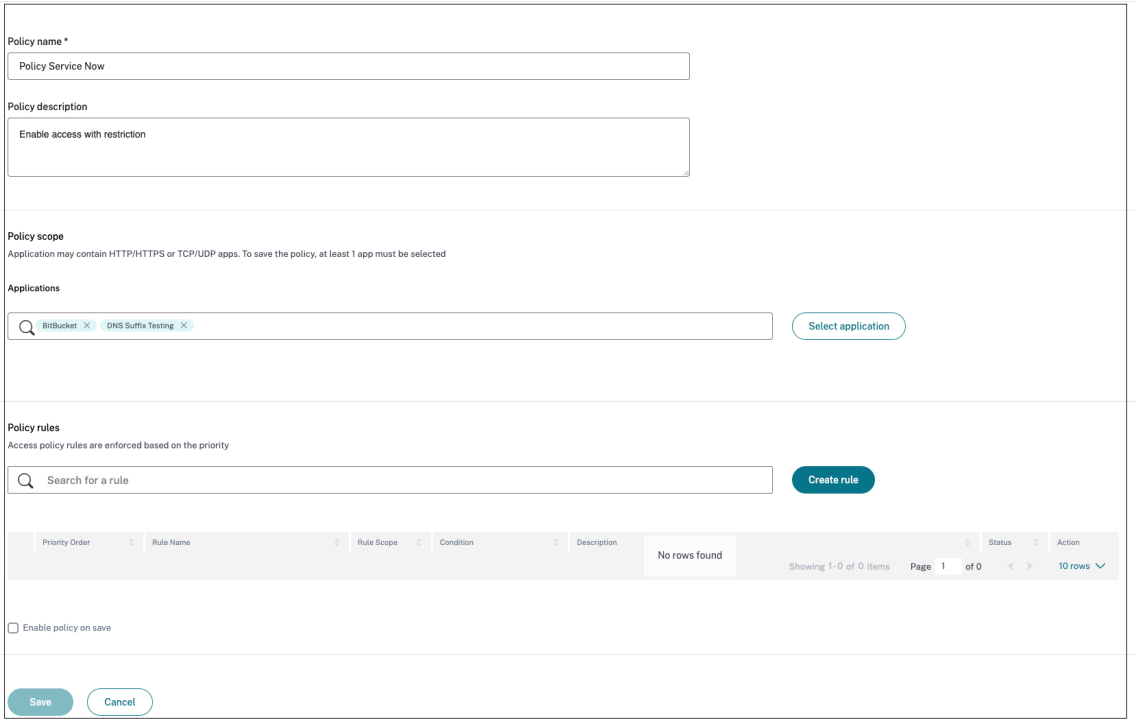
1. ナビゲーション ペインで、[アクセス ポリシー] をクリックし、[ポリシーの作成] をクリックします。



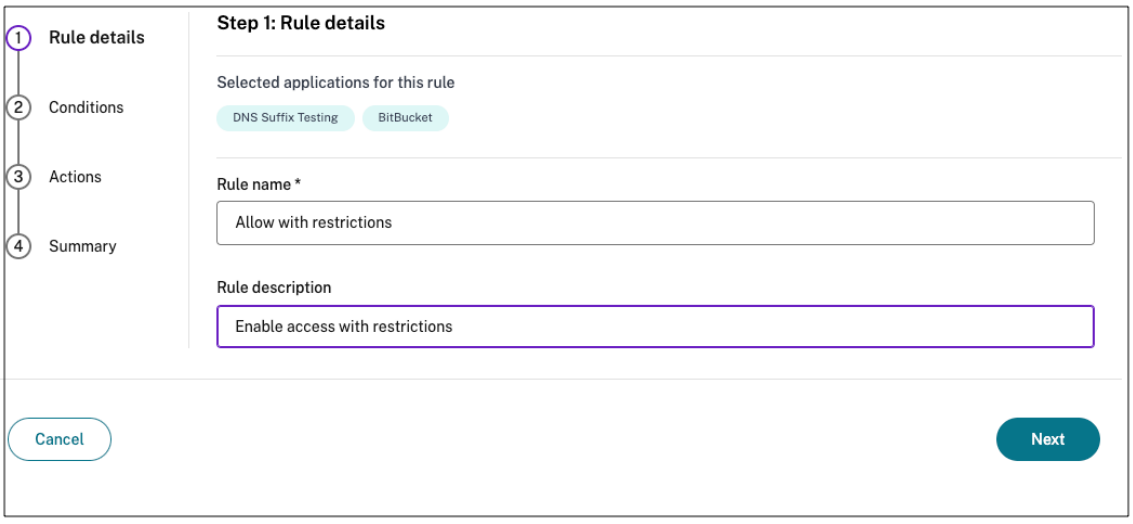
   初めてのユーザーの場合、アクセス ポリシー ランディング ページにはポリシーが表示されません。ポリシーを作成すると、ここにリストされます。

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アプリまたはアプリのセットを選択します。

4. ポリシーのルールを作成するには、[ルールの作成] をクリックします。

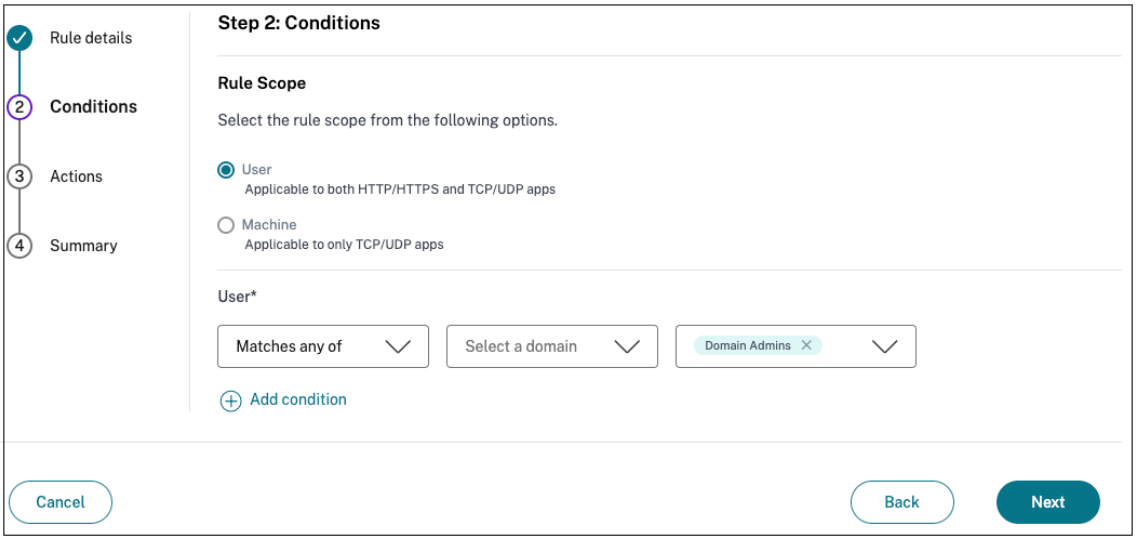


5. ルール名とルールの簡単な説明を入力し、[次へ] をクリックします。



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に満たす必要がある必須条件です。次のいずれかを選択します:

   - のいずれかに一致–フィールドにリスト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にアクセスが許可されます。
   - いずれにも一致しません - フィールドにリストされ、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にアクセスが許可されます。



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、条件に AND 演算が適用され、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ます。コンテキストに応じて次の条件を適用できます。

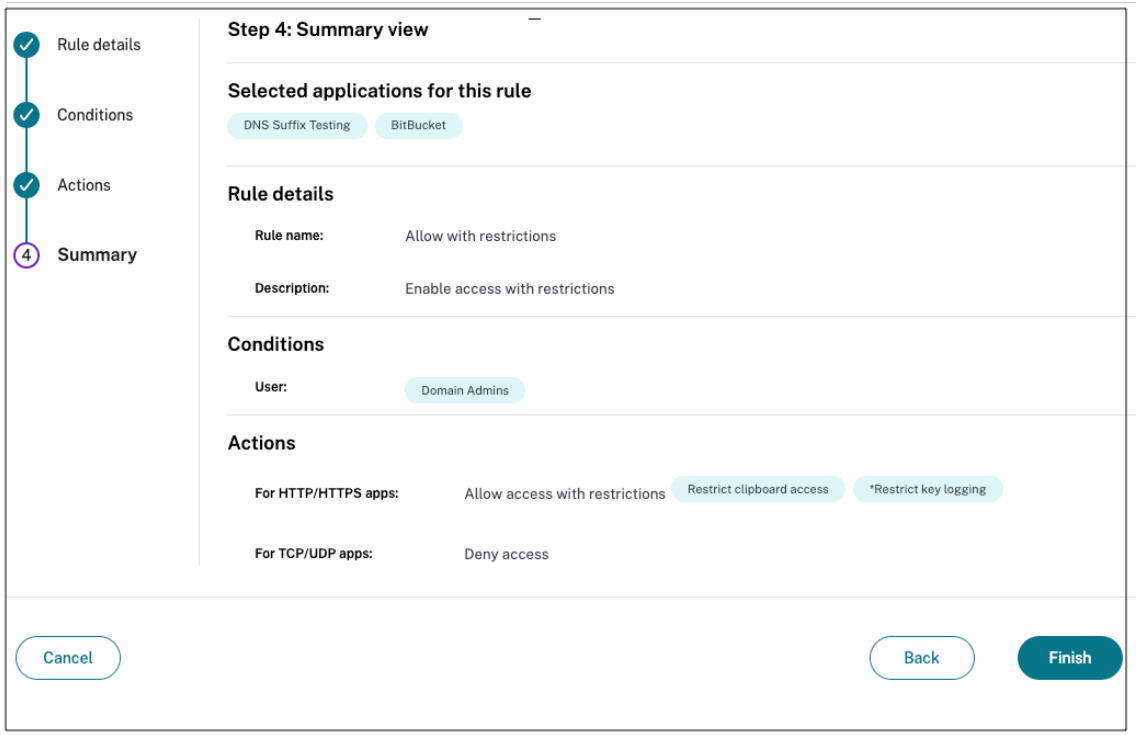
   - デスクトップ または モバイル デバイス–アプリへのアクセスを有効にするデバイスを選択します。
   - 地理的位置–ユーザーがアプリにアクセスしている条件と地理的位置を選択します。
     - 次のいずれかに一致**:** リストされているいずれかの地理的な場所からアプリにアクセスするユーザーまたはユーザー グループのみがアプリにアクセスできます。
     - いずれにも一致しません**:** リストされた地理的な場所以外のすべてのユーザーまたはユーザー グループにアクセスが有効になります。
   - ネットワークの場所–ユーザーがアプリにアクセスする際に使用する条件とネットワークを選択します。
     - は次のいずれかに一致します**:** リストされているいずれかのネットワークの場所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にアクセスできます。
     - いずれにも一致しません**:** リストされたネットワークの場所以外のすべてのユーザーまたはユーザー グループにアクセスが有効になります。
   - デバイスの状態チェック–ユーザー デバイスがアプリケーションにアクセスするために満たす必要がある条件を選択します。
   - 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。
     - は のいずれかに一致します - 着信ユーザー接続が構成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。
     - は のすべてに一致します - 着信ユーザー接続が構成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 アプリの場合は、以下を選択できます。
        - アクセスを許可する
        - 制限付きでアクセスを許可する
        - アクセスを拒否

> 注意:
>
> 制限付きアクセスを許可するを選択した場合は、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、「利用可能なアクセス制限」を参照してください。アプリをリモート ブラウザーで開くか、Citrix Secure Browser で開くかを指定することもできます。

```
- TCP/UDP アクセスの場合、以下を選択できます。
    - **アクセスを許可する**
    - **アクセスを拒否**

![ルールアクションの作成](/en-us/citrix-secure-private-access/media/secure-private-access-policy-rule-actions.png)
```

1. ［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。
2. 詳細を確認して、「完了」をクリックします。



ポリシー作成後に留意すべき点

- 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ります。必要に応じてルールを無効にすることができます。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、ポリシーに優先順位が割り当てられます。値の低い優先度が最も高くなります。優先度番号が最も低いルールが最初に評価されます。ルール (n) が定義された条件に一致しない場合は、次のルール (n+1) が評価され、これが繰り返されます。

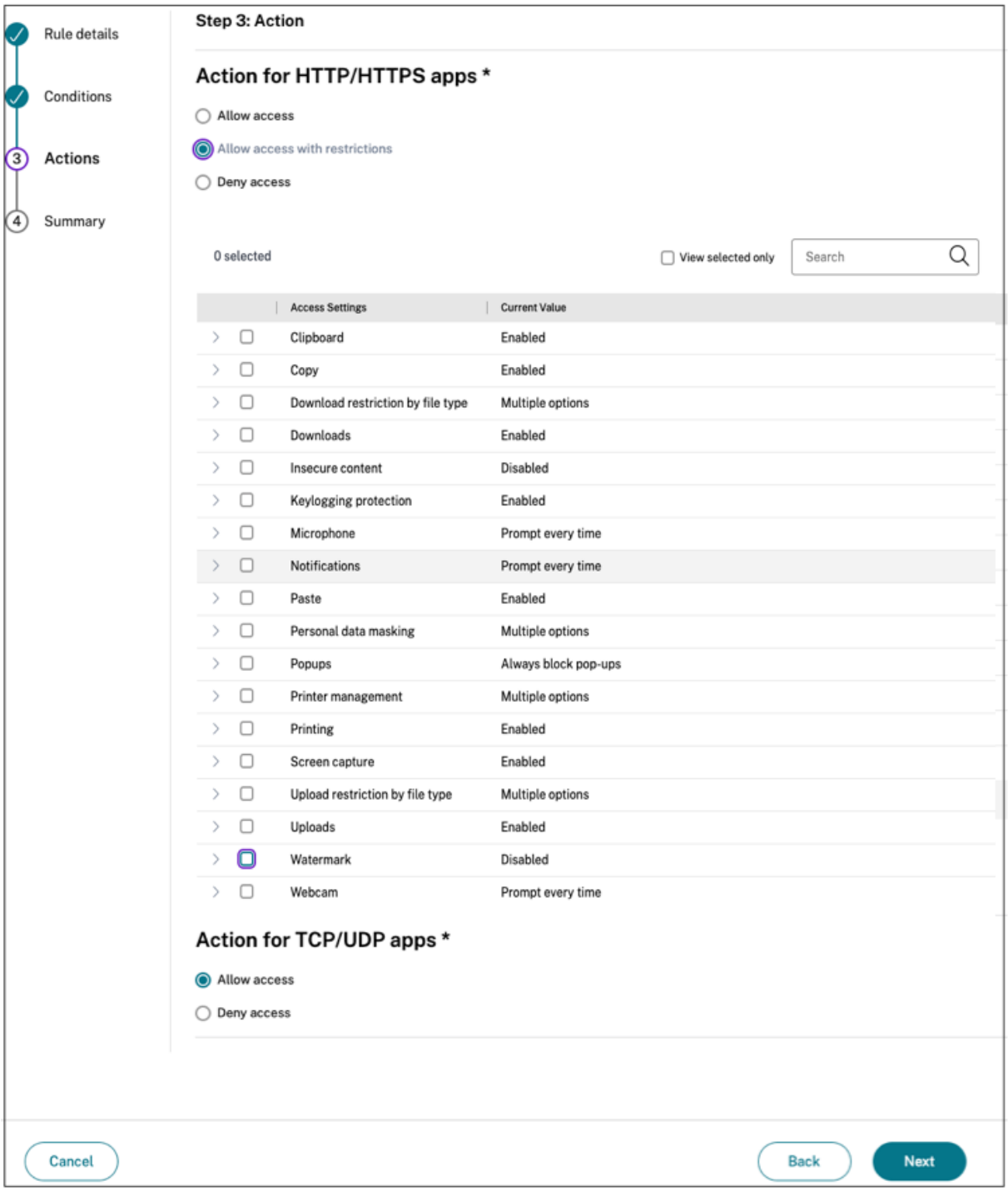
優先順位によるルールの評価例**:**

ルール 1 とルール 2 という 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、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 が優先されます。ルール 1 の条件が満たされた場合、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は、ユーザー A にルール 2 が適用されます。

> 注意**:**
>
> いずれ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。

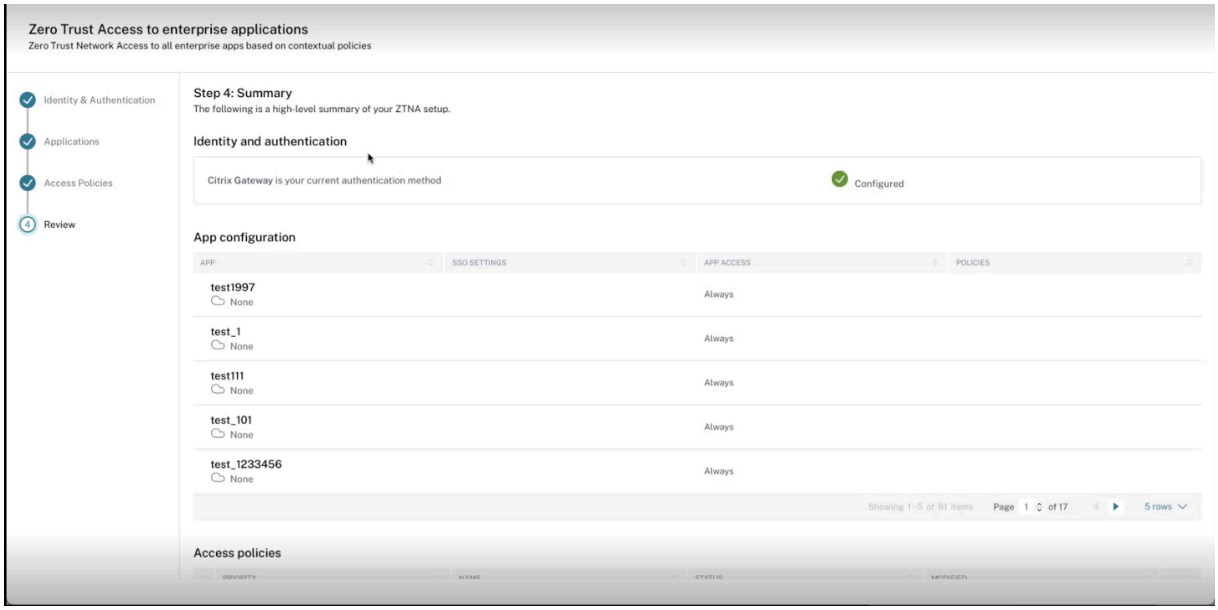
利用可能なアクセス制限オプション

アクション 制限付きアクセスを許可するを選択する場合は、少なくとも 1 つのセキュリティ制限を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内で事前定義されています。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。アプリケーションに対して次のセキュリティ制限を有効にすることができます。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。

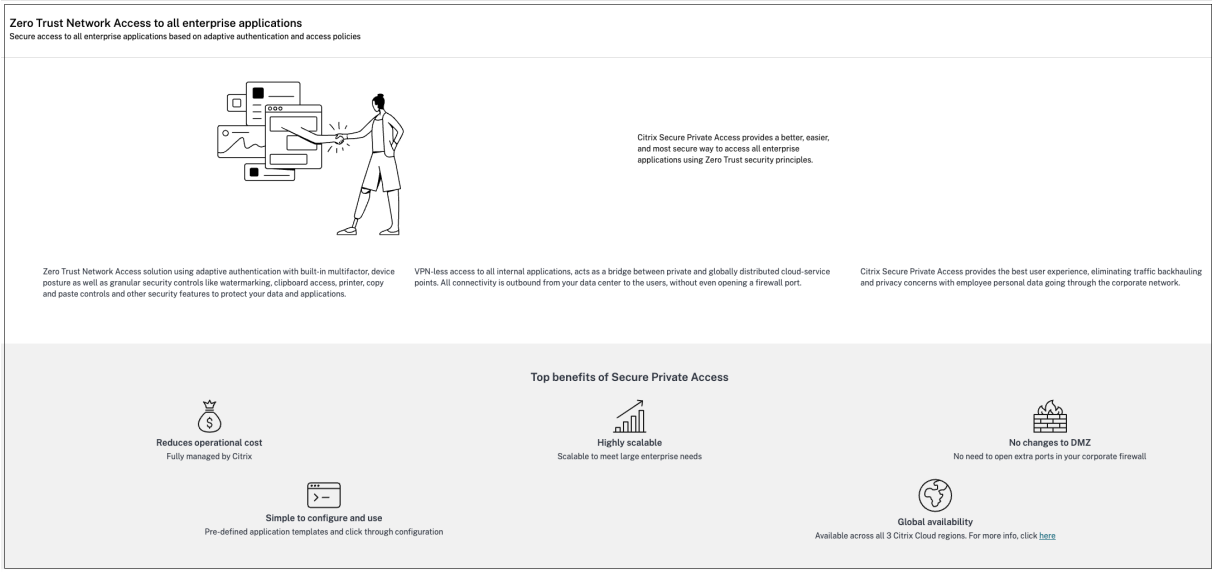


ステップ **4:** 各構成の概要を確認する

[レビュー] 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。

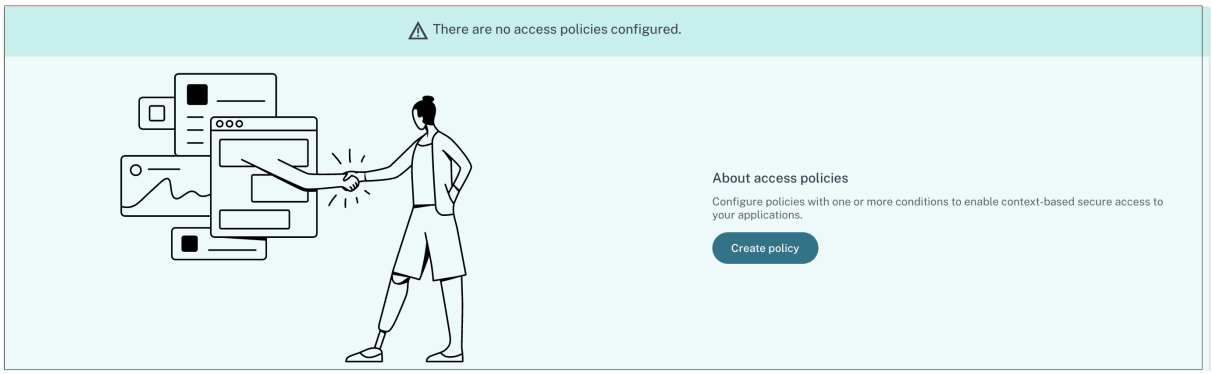


次の図は、4 つのステップの構成を完了した後のページを示しています。



重要:

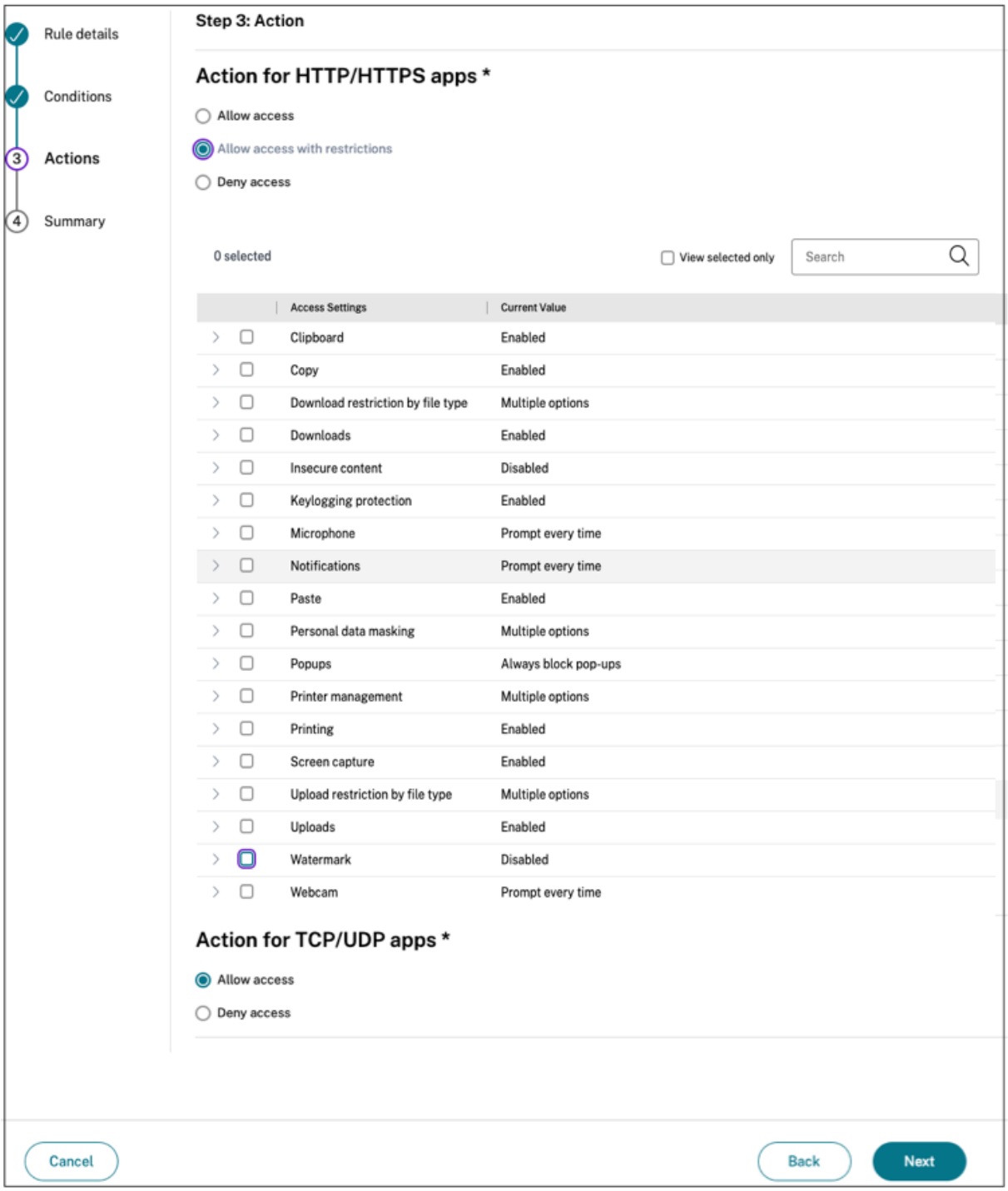
- ウィザードを使用して構成を完了した後、そのセクションに直接移動して、セクションの構成を変更できます。順序に従う必要はありません。
- 構成されたアプリまたはポリシーをすべて削除した場合は、再度追加する必要があります。この場合、すべてのポリシーを削除すると次の画面が表示されます。



アクセス制限オプション

October 21, 2024

アクセス ポリシーの作成時にアクション 制限付きアクセスを許可する を選択すると、アクセス制限を選択できます。これらの制限はシステム内で事前定義されています。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。アクセス ポリシーの作成とアクセス制限の有効化の詳細については、「アクセス ポリシーの構成」を参照してください。



クリップボード

Citrix Enterprise Browser 経由でアクセスする場合、このアクセス ポリシーを使用して SaaS または内部 Web アプリでの切り取り/コピー/貼り付け操作を有効/無効にします。デフォルト値: 有効。

コピー

Citrix Enterprise Browser 経由でアクセスする場合、このアクセス ポリシーを使用して SaaS または内部 Web アプリからのデータのコピーを有効/無効にします。デフォルト値: 有効。

> 注意:
>
> - ポリシーで クリップボード と コピー の両方の制限が有効になっている場合、クリップボード の制限がコピー の制限よりも優先されます。
> - この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 2405 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。
> - アプリ内のコピー操作を細かく制御するために、管理者は セキュリティ グループ 制限を使用できます。詳細については、セキュリティ グループのクリップボード制限を参照してください。

ファイルタイプによるダウンロード制限

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、SaaS または内部 Web アプリ内から特定の MIME (ファイル) タイプをダウンロードするユーザーの機能を有効/無効にします。

> 注意:
>
> - ダウンロード 制限に加えて、ファイル タイプによる ダウンロード制限 制限も利用できます。
> - ポリシーで「ダウンロード」と「ファイル タイプによるダウンロード制限」の両方の制限が有効になっている場合、「ダウンロード」の制限が「ファイル タイプによるダウンロード制限」の制限よりも優先されます。
> - この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 2405 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。

MIME タイプのダウンロードを有効にするには、次の手順を実行します。

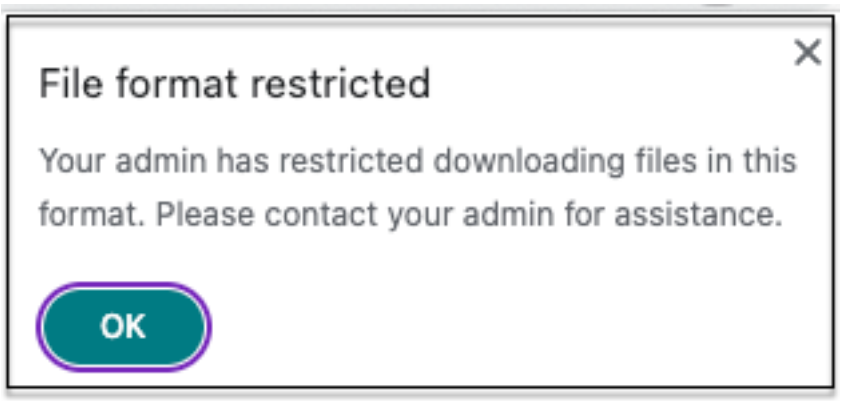
1. アクセス ポリシーを作成または編集します。詳細については、「アクセス ポリシーの作成」を参照してください。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. ファイルタイプによるダウンロード制限 をクリックし、次に 編集をクリックします。
4. ファイルタイプ別のダウンロード制限設定 ページで、次のいずれかを選択します。
   - 例外を除いてすべてのダウンロードを許可します–ブロックする必要があるタイプを選択し、他のすべてのタイプを許可します。
   - 例外を除いてすべてのダウンロードをブロックします–アップロードできるタイプのみを選択し、他のすべてのタイプをブロックします。

5. ファイル タイプがリストに存在しない場合は、次の手順を実行します。

   a) カスタム **MIME** タイプの追加をクリックします。
   b) **MIME** タイプの追加で、カテゴリ/サブカテゴリ<extension>の形式で MIME タイプを入力します。たとえば、image/pngです。
   c) [完了] をクリックします。
   d) [次へ]、[完了] の順にクリックします。

   MIME タイプが例外リストに表示されます。

エンド ユーザーが制限されたファイルの種類をダウンロードしようとすると、Citrix Enterprise Browser に次のメッセージが表示されます。



ダウンロード

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、ユーザーが SaaS または内部 Web アプリ内からダウンロードする機能を有効/無効にします。デフォルト値: 有効。

> 注意:
>
> ポリシーで「ダウンロード」と「ファイル タイプによるダウンロード制限」の両方の制限が有効になっている場合、「ダウンロード」の制限が「ファイル タイプによるダウンロード制限」の制限よりも優先されます。

安全でないコンテンツ

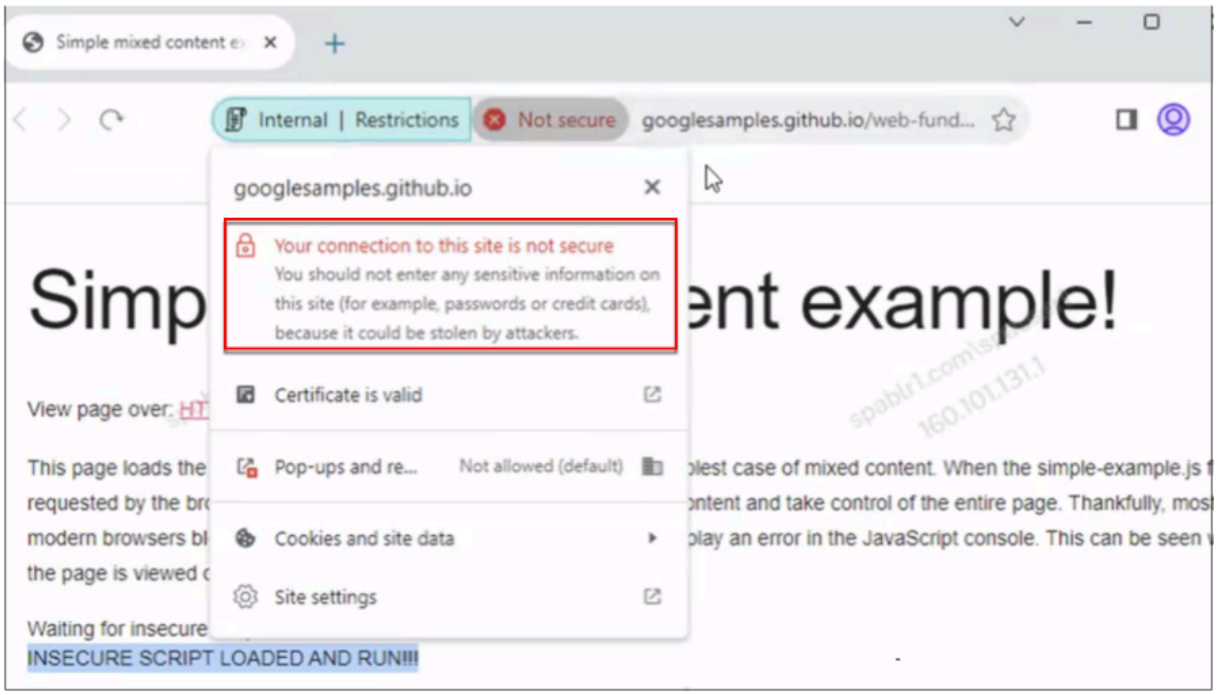
Citrix Enterprise Browser 経由でアクセスする場合、このポリシーで構成された SaaS または内部 Web アプリ内の安全でないコンテンツへのエンドユーザーによるアクセスを有効/無効にします。安全でないコンテンツとは、HTTPS リンクではなく HTTP リンクを使用して Web ページからリンクされているファイルのことです。デフォルト値：無効.

安全でないコンテンツへのアクセスを無効にするには、エンド ユーザーは Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

安全でないコンテンツへのアクセスを有効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. 安全でないコンテンツを選択します。
4. [次へ]、[完了] の順にクリックします。

次の図は、安全でないコンテンツにアクセスしたときに表示される通知の例を示しています。



キーロギング保護

このアクセス ポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、キーロガーが SaaS または内部 Web アプリからキーストロークをキャプチャすることを有効/無効にします。デフォルト値: 有効。

マイク

Citrix Enterprise Browser 経由でアクセスする場合、このポリシーで構成された SaaS または内部 Web アプリ内でマイクにアクセスするたびにユーザーにプロンプトを表示するか、表示しません。デフォルト値: 毎回プロンプトを表示します。

エンドユーザーは、マイク 制限が有効になっているアプリケーションにアクセスするには、Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

プロンプトが表示されずに毎回マイクを許可するには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. マイク をクリックし、次に 編集をクリックします。
4. マイクの設定 ページで、常にアクセスを許可するをクリックします。
5. [保存] をクリックします。
6. [次へ]、[完了] の順にクリックします。

> 注意**:**
>
> - セキュアプライベートアクセスポリシーで「マイク 制限」が有効になっている場合、Citrix Enterprise Browser には「許可」の設定が表示されます。
> - セキュアプライベートアクセスポリシーでオプション 毎回プロンプトを表示 が選択されている場合、Citrix Enterprise Browser に適用される設定は、Citrix Enterprise Browser の管理に Global App Configuration サービス (GACS) が使用されているかどうかによって異なります。
> - GACS が使用されている場合、Citrix Enterprise Browser に GACS 設定が適用されます。
> - GACS が使用されていない場合、Citrix Enterprise Browser には設定 **Ask** が表示されます。

GACS の詳細については、「グローバルアプリ構成サービスによる Citrix Enterprise Browser の管理」を参照してください。

通知

Citrix Enterprise Browser 経由でアクセスしたときに、このポリシーで構成された SaaS または内部 Web アプリ内の通知をユーザーに毎回表示することを許可/プロンプトします。デフォルト値: 毎回プロンプトを表示します。

この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

プロンプトなしで通知をブロックするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. 通知 をクリックし、次に 編集をクリックします。
4. 通知設定 ページで、常に通知をブロックをクリックします。
5. [保存] をクリックします。
6. [次へ]、[完了] の順にクリックします。

ペースト

Citrix Enterprise Browser 経由でアクセスする場合、このアクセス ポリシーを使用して、コピーされたデータを SaaS または内部 Web アプリに貼り付けることを有効/無効にします。デフォルト値: 有効。

> 注意:
>
> - ポリシーで クリップボード と 貼り付け の両方の制限が有効になっている場合、クリップボード の制限が 貼り付け の制限よりも優先されます。
> - この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。
> - アプリ内の貼り付け操作を細かく制御するために、管理者は セキュリティ グループ 制限を使用できます。詳細については、セキュリティ グループのクリップボード制限を参照してください。

個人データのマスキング

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスする場合、SaaS または内部 Web アプリ上の個人を特定できる情報 (PII) の編集またはマスキングを有効/無効にします。個人を特定できる情報には、クレジットカード番号、社会保障番号、日付などがあります。特定の種類の機密情報を検出し、それに応じてマスクするためのカスタム ルールを定義することもできます。個人データのマスキング制限では、情報を完全にまたは部分的にマスキングするオプションも提供されます。

> 注意:
>
> この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 2405 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。

個人を特定できる情報を編集またはマスクするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. 個人データのマスキング をクリックし、次に 編集をクリックします。
4. 隠したりマスクしたりする情報の種類を選択し、[追加] をクリックします。

   情報タイプが定義済みリストに表示されない場合は、カスタム情報タイプを追加できます。詳細については、「カスタム情報タイプの追加」を参照してください。
5. マスキングタイプを選択します。

   - 完全マスキング–機密情報を完全に覆い、読み取れないようにします。
   - 部分マスキング–機密情報を部分的に隠します。関連するセクションのみがカバーされ、残りの部分はそのまま残ります。

     部分マーキングを選択した場合は、文書の先頭または末尾から文字を選択する必要があります。最初のマスク文字 と 最後のマスク文字 フィールドに数字を入力する必要があります。

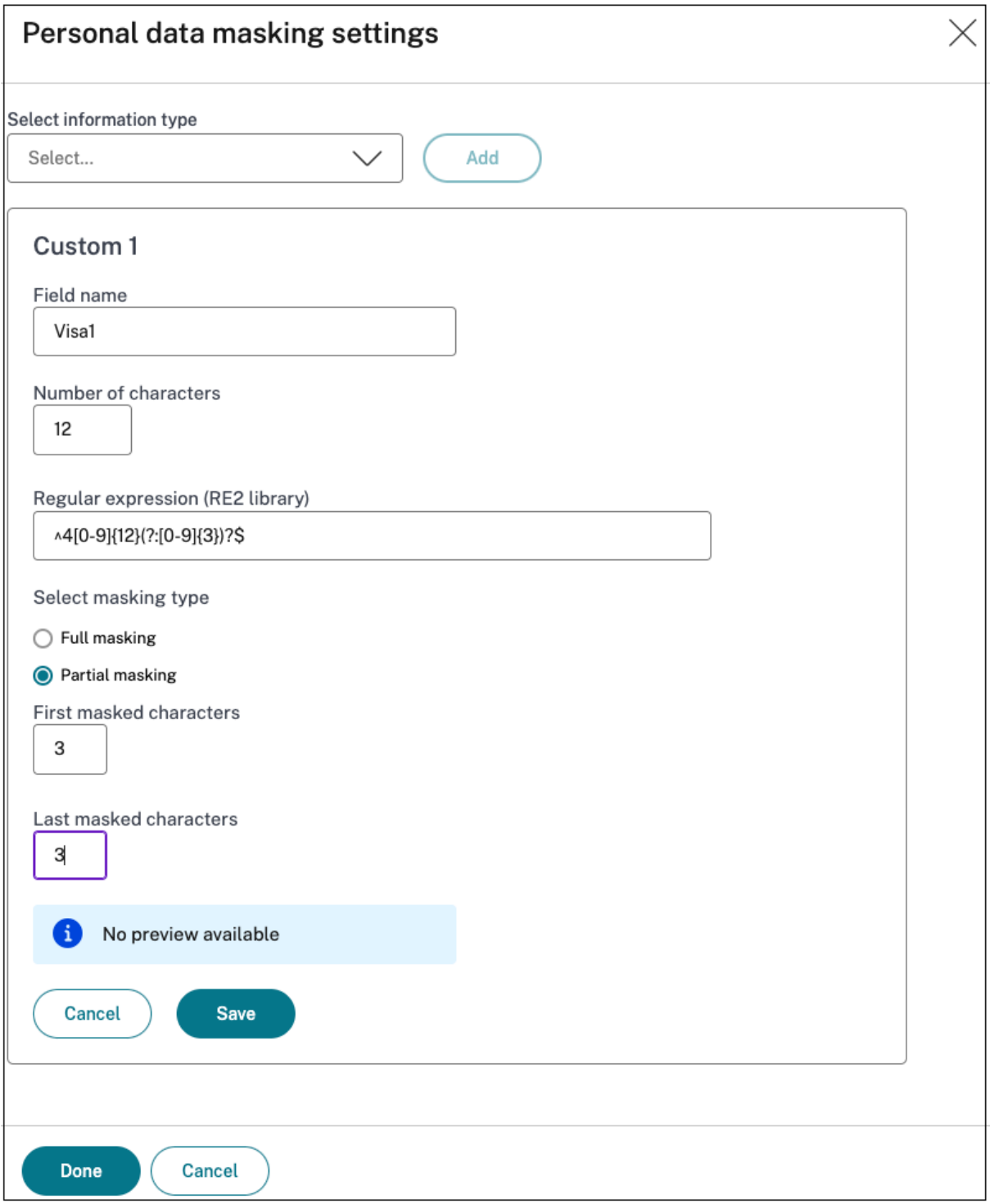
プレビュー フィールドにマスキング形式が表示されます。このプレビューはカスタム ポリシーでは使用できません。

6. 保存 をクリックし、次に 完了をクリックします。
7. [次へ]、[完了] の順にクリックします。

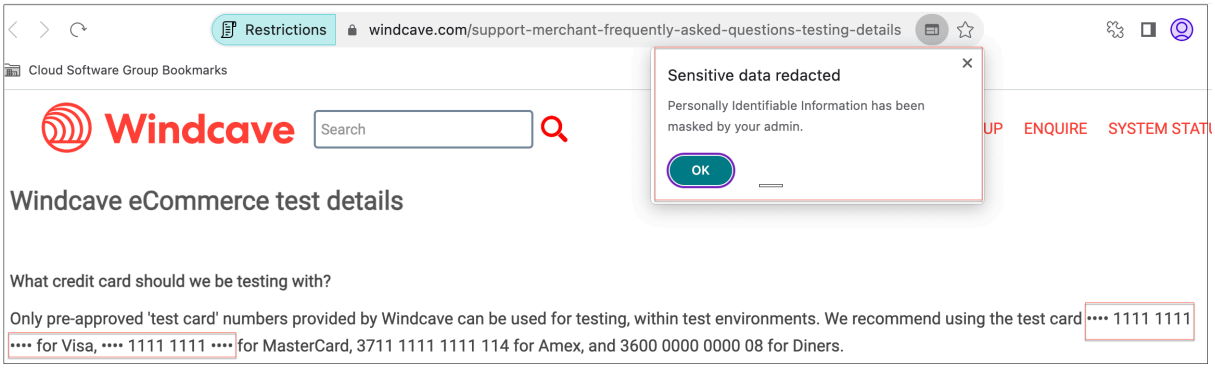
カスタム情報タイプを追加する

情報タイプの正規表現を追加することで、カスタム情報タイプを追加できます。

1. 情報タイプを選択で、カスタムを選択し、追加をクリックします。
2. フィールド名に、マスクする情報タイプの名前を入力します。
3. で 文字数で、情報タイプの文字数を入力します。
4. 正規表現 **(RE2** ライブラリ**)** に、カスタム情報タイプの式を入力します。たとえば、`^4[0-9]{ 12 }(?:[0-9]{ 3 } )?$`。
5. 完全な情報、または最初または最後の数文字をマスクする場合は、マスク タイプを選択します。
6. 保存をクリックし、次に 完了をクリックします。
7. [次へ]、[完了] の順にクリックします。



次の図は、PII がマスクされたサンプル アプリを示しています。この図には、PII のマスキングに関連する通知も表示されています。



ポップアップ

Citrix Enterprise Browser 経由でアクセスしたときに、このポリシーで構成された SaaS または内部 Web アプリ内のポップアップの表示を有効/無効にします。デフォルトでは、Web ページ内のポップアップは無効になっています。デフォルト値: ポップアップを常にブロックします。

この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

ポップアップの表示を有効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. ポップアップ をクリックし、次に 編集をクリックします。
4. ポップアップ設定 ページで、ポップアップを常に許可するをクリックします。
5. [保存] をクリックします。
6. [次へ]、[完了] の順にクリックします。

印刷

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、構成された SaaS または内部 Web アプリからのデータの印刷を有効/無効にします。デフォルト値: 有効。

印刷制限が有効になっているアプリケーションからエンド ユーザーがコンテンツを印刷しようとすると、次のメッセージが表示されます。

> 注意:
>
> ポリシーで「印刷」と「プリンター管理」の両方の制限が有効になっている場合、「印刷」の制限が「プリンター管理」の制限よりも優先されます。

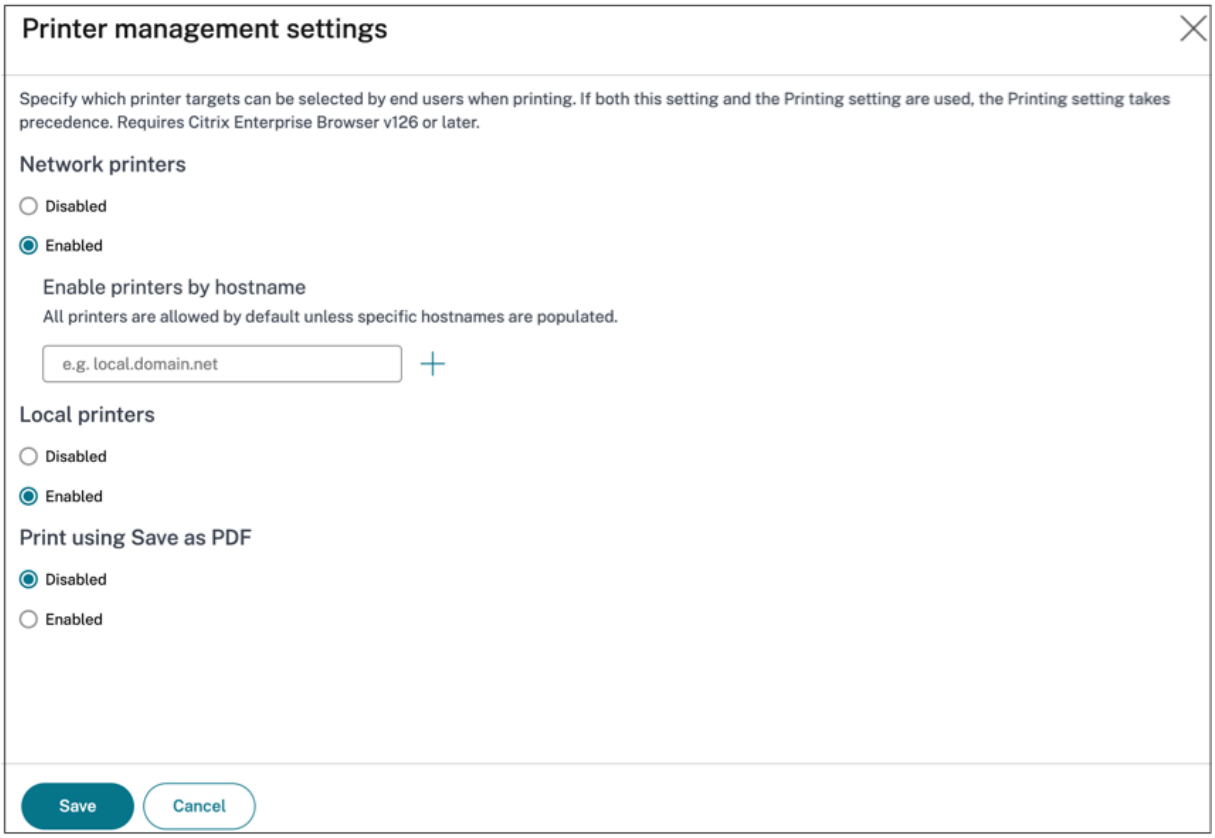
プリンター管理

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、構成された SaaS または内部 Web アプリから管理者が構成したプリンターを使用してデータの印刷を有効/無効にします。

> 注意:
>
> - 印刷を有効または無効にする 印刷 制限に加えて、プリンター管理 制限も使用できます。アクセス ポリシーで「印刷」と「プリンター管理」の両方の制限が有効になっている場合、「印刷」の制限が「プリンター管理」の制限よりも優先されます。
> - この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 2405 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。

印刷制限を有効/無効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. プリンター管理 をクリックし、次に 編集をクリックします。



1. 要件に応じて例外を選択してください。

   - ネットワーク プリンター - ネットワーク プリンターは、ネットワークに接続して複数のユーザーが使用できるプリンターです。
     - **Disabled**：ネットワーク内のすべてのネットワークプリンターからの印刷が無効になります。
     - **Enabled**：すべてのネットワークプリンターからの印刷が有効になります。プリンタのホスト名が指定されている場合、指定されたプリンタ以外のすべてのネットワーク プリンタがブロックされます。

     注意**:** ネットワーク プリンターはホスト名で識別されます。
   - ローカル プリンター - ローカル プリンターは、有線接続を介して個々のコンピューターに直接接続されたデバイスです。この接続は通常、USB、パラレル ポート、またはその他の直接インターフェイスを介して実現されます。
     - **Disabled**：すべてのローカルプリンターからの印刷が無効になります。
     - **Enabled**：すべてのローカルプリンターからの印刷が有効になります。
   - **Print using Save as PDF**
     - 無効: アプリケーションのコンテンツを PDF 形式で保存することは無効です。
     - 有効**:** アプリケーションのコンテンツを PDF 形式で保存することが有効になります。

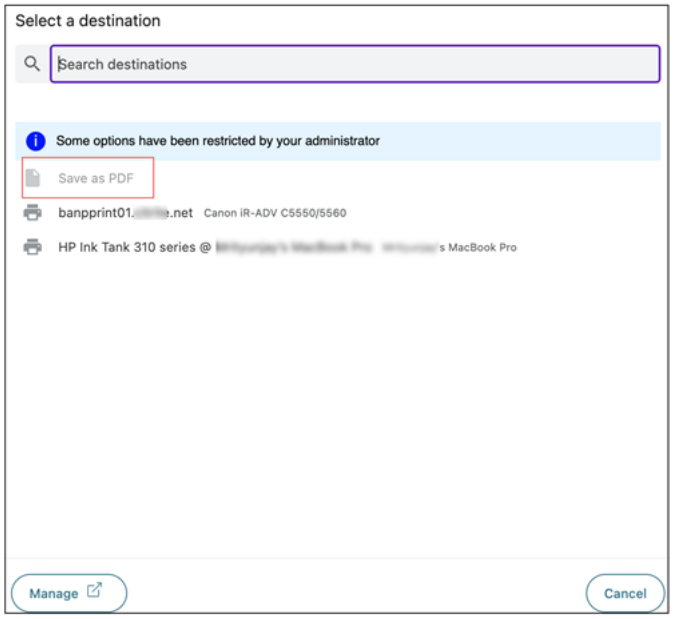
2. ［保存］をクリックします。

3. ［次へ］、［完了］の順にクリックします。

ネットワーク プリンターが無効になっている場合、エンド ユーザーが 宛先 フィールドでプリンターを選択しようとすると、特定のプリンター名がグレー表示されます。

また、**[PDF** として保存して印刷**]** が無効になっている場合、**[**保存先**]** フィールドの **[**詳細を表示**]** リンクをクリックすると、**[PDF** として保存**]** オプションがグレー表示されます。

エンドユーザーがネットワーク プリンターの名前を変更すると、ネットワーク プリンターを使用できなくなります。



スクリーンキャプチャ

いずれかの画面キャプチャ プログラムまたはアプリを使用して Citrix Enterprise Browser 経由でアクセスしたときに、このポリシーで SaaS または内部 Web アプリから画面をキャプチャする機能を有効/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。デフォルト値: 有効。

ファイルタイプによるアップロード制限

このポリシーを使用して、Citrix Enterprise Browser 経由でアクセスしたときに、ユーザーが SaaS または内部 Web アプリから特定の MIME (ファイル) タイプをダウンロードする機能を有効/無効にします。

> 注意**:**
>
> - アップロード 制限に加えて、ファイル タイプによるアップロード制限 制限も利用できます。
> - ポリシーで「アップロード」と「ファイル タイプによるアップロード制限」の両方の制限が有効になっている場合、「アップロード」の制限が「ファイル タイプによるアップロード制限」の制限よりも優先され

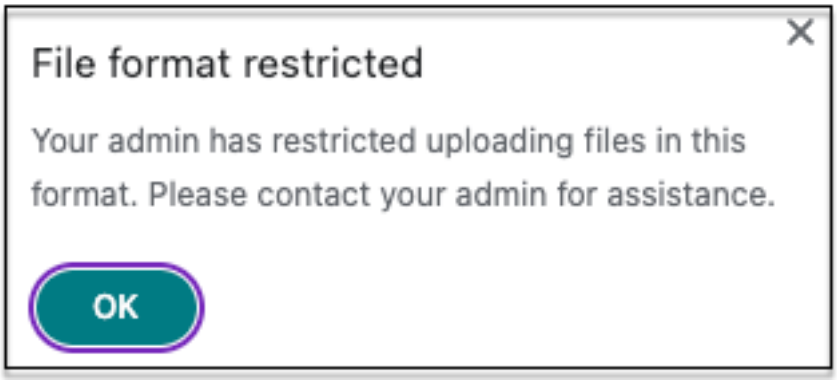
> ます。
> - この制限が有効になっているアプリケーションにアクセスするには、エンド ユーザーは Citrix Enterprise Browser バージョン 2405 以降を使用する必要があります。それ以外の場合、アプリケーションへのアクセスは制限されます。

MIME タイプのアップロードを有効/無効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. ファイルタイプによるアップロード制限 をクリックし、次に 編集をクリックします。
4. ファイルタイプ別のアップロード制限設定 ページで、次のいずれかを選択します。
   - 例外を除いてすべてのアップロードを許可します–選択したタイプを除くすべてのファイルをアップロードします。
   - 例外を除いてすべてのアップロードをブロックします–選択した種類を除くすべてのファイルタイプのアップロードをブロックします。
5. ファイル タイプがリストに存在しない場合は、次の手順を実行します。
   a) カスタム **MIME** タイプの追加をクリックします。
   b) **MIME** タイプの追加で、カテゴリ/サブカテゴリ<extension>の形式で MIME タイプを入力します。たとえば、image/pngです。
   c) [完了] をクリックします。
   d) [次へ]、[完了] の順にクリックします。

   MIME タイプが例外リストに表示されます。

エンドユーザーが制限されたファイルの種類をアップロードしようとすると、Citrix Enterprise Browser に警告メッセージが表示されます。



アップロード

Citrix Enterprise Browser 経由でアクセスしたときに、このポリシーで構成された SaaS または内部 Web アプリ内でのユーザーのアップロード機能を有効/無効にします。デフォルト値: 有効。

> 注意:
>
> ポリシーで「アップロード」と「ファイル タイプによるアップロード制限」の両方の制限が有効になっている場合、「アップロード」の制限が「ファイル タイプによるアップロード制限」よりも優先されます。

ウォーターマーク

ユーザーの画面にユーザー名とユーザーのマシンの IP アドレスを表示する透かしを有効/無効にします。デフォルト値：無効.

Web カメラ

Citrix Enterprise Browser 経由でアクセスする場合、このポリシーで構成された SaaS または内部 Web アプリ内で Web カメラにアクセスするたびにユーザーにプロンプトを表示するか、表示しません。デフォルト値: 毎回プロンプトを表示します。

エンドユーザーは、**Web** カメラ 制限が有効になっているアプリケーションにアクセスするには、Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

プロンプトが表示されずに毎回ウェブカメラを許可するには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。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。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. ウェブカメラ をクリックし、次に 編集をクリックします。
4. ウェブカメラ設定 ページで、常にアクセスを許可するをクリックします。
5. [保存] をクリックします。
6. [次へ]、[完了] の順にクリックします。

> 注意:
>
> - セキュアプライベートアクセスポリシーで **Web** カメラ 制限が有効になっている場合、Citrix Enterprise Browser には 許可の設定が表示されます。
> - セキュアプライベートアクセスポリシーでオプション「毎回プロンプトを表示」が有効になっている場合、Citrix Enterprise Browser に適用される設定は、Citrix Enterprise Browser の管理に Global App Configuration サービス (GACS) が使用されているかどうかによって異なります。

> - GACS が使用されている場合、Citrix Enterprise Browser に GACS 設定が適用されます。
> - GACS が使用されていない場合、Citrix Enterprise Browser には設定 **Ask** が表示されます。

GACS の詳細については、「グローバルアプリ構成サービスによる Citrix Enterprise Browser の管理」を参照してください。

セキュリティ グループのクリップボード制限

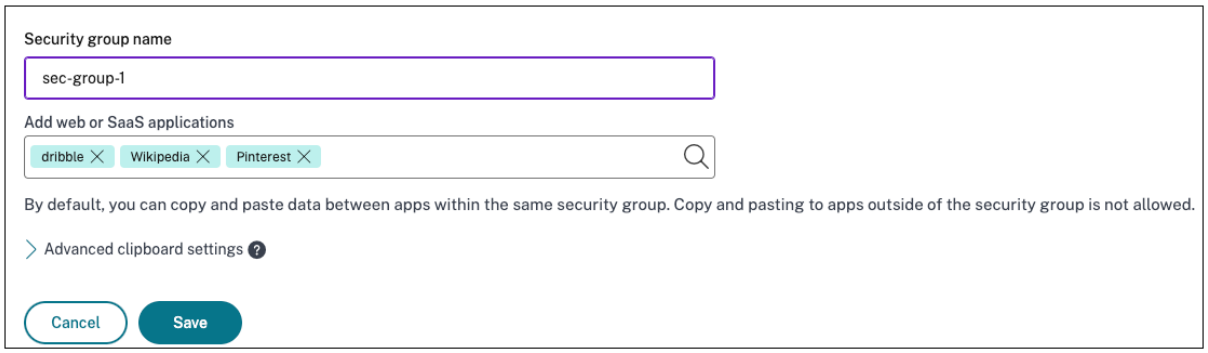
指定したアプリのグループへのクリップボード アクセスを制限できます。これらの指定されたアプリ グループはセキュリティ グループとして作成されるため、エンド ユーザーはそのセキュリティ グループ内でのみコンテンツのコピーと貼り付けが許可されます。セキュリティ グループ内のアプリ内でクリップボード アクセスを有効にするには、アクセス設定を選択せずに、アクション 許可 または 制限付きで許可 でアクセス ポリシーを構成する必要があります。

- セキュリティ グループ 制限が有効になっている場合、異なるセキュリティ グループ内のアプリケーション間でデータをコピー/貼り付けすることはできません。たとえば、アプリ「ProdDocs」がセキュリティ グループ「SG1」に属し、アプリ「Edocs」がセキュリティ グループ「SG2」に属している場合、両方のグループに対して コピー / 貼り付け 制限が有効になっている場合でも、「Edocs」から「ProdDocs」にコンテンツをコピー/貼り付けすることはできません。
- セキュリティ グループに属していないアプリの場合は、アクション 制限付きで許可 と制限 (コピー、貼り付け、または クリップボード) を選択してアクセス ポリシーを作成できます。この場合、アプリはセキュリティ グループの一部ではないため、そのアプリに コピー/貼り付け 制限を適用できます。

> 注意:
>
> また、Global App Configuration サービス (GACS) を通じて、Citrix Enterprise Browser 経由でアクセスされるアプリのクリップボード アクセスを制限することもできます。GACS を使用して Citrix Enterprise Browser を管理している場合は、サンドボックス クリップボードを有効にする オプションを使用してクリップボード アクセスを管理します。GACS を介してクリップボードへのアクセスを制限すると、Citrix Enterprise Browser 経由でアクセスされるすべてのアプリに適用されます。

セキュリティ グループを作成するには、次の手順を実行します。

1. Secure Private Access コンソールで、[アプリケーション] をクリックし、[セキュリティ グループ] をクリックします。
2. 新しいセキュリティ グループの追加をクリックします。

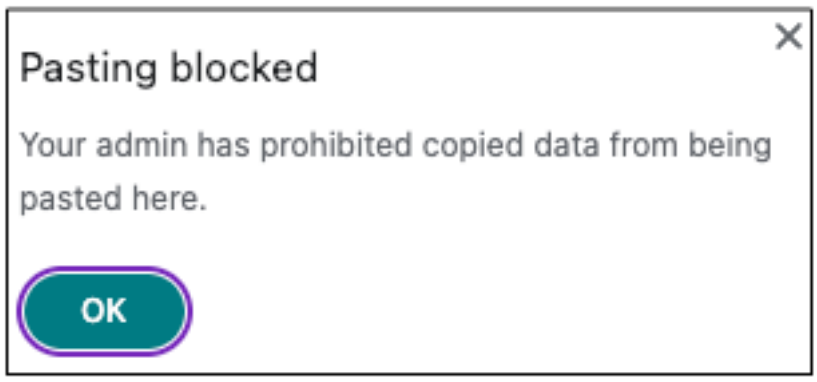


1. セキュリティ グループの名前を入力します。
2. **Web** または **SaaS** アプリケーションの追加で、グループ化するアプリケーションを選択して、コピーと貼り付けのコントロールを有効にします。たとえば、Wikipedia、Pinterest、Dribble などです。
3. [保存] をクリックします。

高度なクリップボード 設定の詳細については、「ネイティブ アプリケーションと未公開アプリのコピー/貼り付けコントロールを有効にする」を参照してください。

エンドユーザーが Citrix Workspace からこれらのアプリケーション (Wikipedia、Pinterest、Dribble) を起動する場合、セキュリティ グループ内の 1 つのアプリケーションから他のアプリケーションにデータを共有 (コピー/貼り付け) できる必要があります。コピー/貼り付けは、アプリケーションに対して既に有効になっているその他のセキュリティ制限に関係なく実行されます。

ただし、エンド ユーザーは、自分のマシン上のローカル アプリケーションまたは未公開のアプリケーションからこれらの指定されたアプリケーションにコンテンツをコピーして貼り付けることはできません (その逆も同様)。指定されたアプリケーションから別のアプリケーションにコンテンツがコピーされると、次の通知が表示されます。



> 注意:
>
> 詳細なクリップボード設定のオプションを使用すると、セキュリティ グループ内のアプリと、マシン上の他のローカル アプリまたは未公開の Web アプリ間でコンテンツをコピーして貼り付けることができます。詳細については、「ネイティブ アプリケーションと未公開アプリのコピー/貼り付けコントロールを有効にする」を参照してください。

詳細なレベルのクリップボードアクセスを有効にする

指定されたグループ内のアプリケーション内で、きめ細かいレベルのクリップボード アクセスを有効にすることができます。これを行うには、アプリケーションのアクセス ポリシーを作成し、要件に応じて コピー/貼り付け 制限を有効にします。

> 注意:
>
> 詳細レベルのクリップボード アクセス用に作成した特定のアクセス ポリシーの優先度が、セキュリティ グループ用に作成したポリシーよりも高いことを確認します。

例:

Wikipedia、Pinterest、Dribble という 3 つのアプリケーションを含むセキュリティ グループを作成したとします。

ここで、Wikipedia または Dribble からのコンテンツの Pinterest への貼り付けを制限します。そのためには、次の手順に従います。

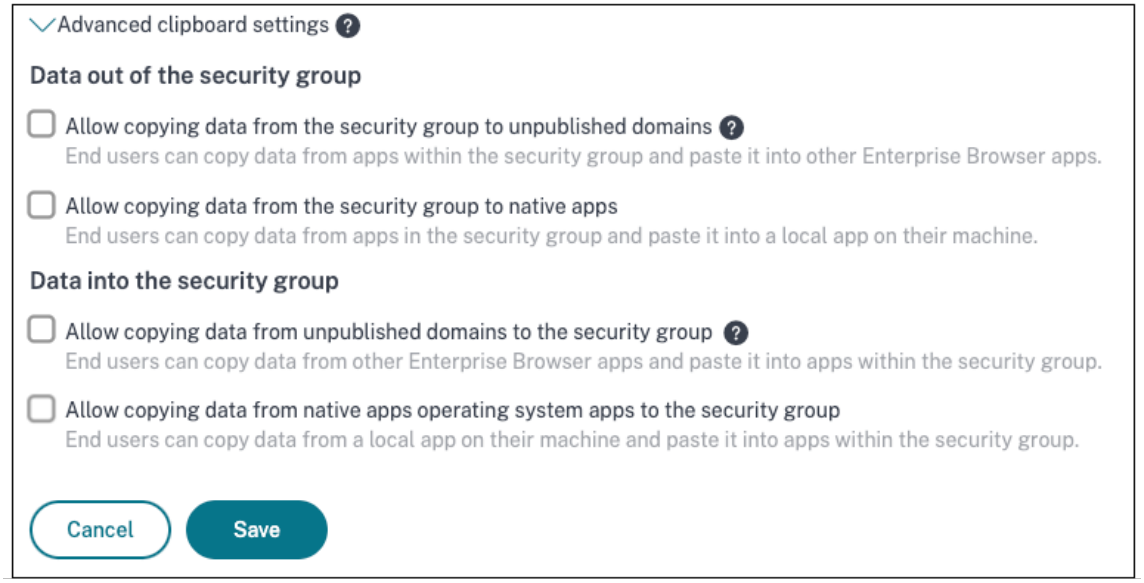
1. アプリケーション `Pinterest`に割り当てられたアクセス ポリシーを作成または編集します。アクセス ポリシーの作成の詳細については、「アクセス ポリシーの作成」を参照してください。
2. ステップ **3:** アクション ページで、制限付きで許可を選択します。
3. を選択してを貼り付けます。

Pinterest は、Wikipedia や Dribble も含まれるセキュリティ グループの一部ですが、Pinterest に関連付けられたアクセス ポリシーで 貼り付け 制限が無効になっているため、ユーザーは Wikipedia または Dribble から Pinterest にコンテンツをコピーできません。

ネイティブアプリケーションと未公開アプリのコピー/貼り付けコントロールを有効にする

高度なクリップボード設定のオプションを使用すると、セキュリティ グループ内のアプリとマシン上の他のローカル アプリまたは未公開の Web アプリ間でコンテンツをコピーして貼り付けることができます。

1. セキュリティ グループを作成します。詳細については、「セキュリティ グループの作成」を参照してください。
2. 詳細なクリップボード設定を展開します。



3. 要件に応じて、次のいずれかのオプションを選択します。

   - セキュリティ グループから未公開ドメインへのデータのコピーを許可します–セキュリティ グループ内のアプリケーションから、Secure Private Access で公開されていないアプリへのデータのコピーを有効にします。
   - セキュリティ グループからネイティブ アプリへのデータのコピーを許可します - セキュリティ グループ内のアプリケーションからマシン上のローカル アプリケーションへのデータのコピーを有効にします。
   - 未公開ドメインからセキュリティ グループへのデータのコピーを許可します–セキュリティ グループ内のアプリケーションへの Secure Private Access を通じて公開されていないアプリからのデータのコピーを有効にします。
   - ネイティブ アプリのオペレーティング システムのセキュリティ グループからのデータのコピーを許可します - マシン上のローカル アプリケーションからアプリケーションへのデータのコピーを有効にします。

既知の問題

- (設定 **>** アプリケーション ドメイン) のルーティング テーブルには、削除されたアプリケーションのドメインが保持されます。したがって、これらのアプリケーションは、Secure Private Access では公開アプリケーションとしても扱われます。これらのドメインに Citrix Enterprise Browser から直接アクセスする場合、詳細なクリップボード設定で選択したオプションに関係なく、これらのアプリケーションからのコピー/貼り付けは無効になります。

  たとえば、次のシナリオを想定します。

  – セキュリティ グループの一部であった Jira2 (`https://test.citrite.net`) という名前のアプリケーションを削除しました。

  - オプション セキュリティ グループから未公開ドメインへのデータのコピーを許可するが有効になりました。

  このシナリオでは、ユーザーがこのアプリケーションから同じセキュリティ グループ内の別のアプリケーションにデータをコピーしようとすると、貼り付けコントロールが無効になります。それに関する通知がユーザーに表示されます。

- SaaS アプリの場合、アプリケーションがアクション アクセス拒否を含むアクセス ポリシーで構成されている場合、アプリ アクセスを拒否できます。アプリのトラフィックはセキュア プライベート アクセスを介してトンネリングされないため、エンド ユーザーは引き続きアプリにアクセスできます。また、アプリケーションがセキュリティ グループの一部である場合、セキュリティ グループの設定は考慮されないため、アプリケーションからコンテンツをコピー/貼り付けすることはできません。

ポリシーモデリングツール

October 21, 2024

複数のアプリケーションと複数のアクセス ポリシーがあると、すべての構成に基づいてエンド ユーザーがアプリケーションへのアクセスを許可されているか拒否されているかという、エンド ユーザーのアプリ アクセス結果を正確に管理者が把握することが困難になる可能性があります。

ポリシー モデリング ツール (A アクセス ポリシー **>** ポリシー モデリング) は、既存の構成に基づいて、管理者が予想されるアプリ アクセス結果 (許可/制限付きで許可/拒否) を完全に把握できるようにすることで、この問題を解決します。管理者は、デバイスの種類、デバイスの姿勢、地理的位置、ネットワークの場所、ユーザーのリスク スコア、ワークスペース URL などのユーザー条件に基づいて、任意のユーザーのアクセス結果を確認できます。

アクセス ポリシー構成を分析するには、次の手順を実行します。

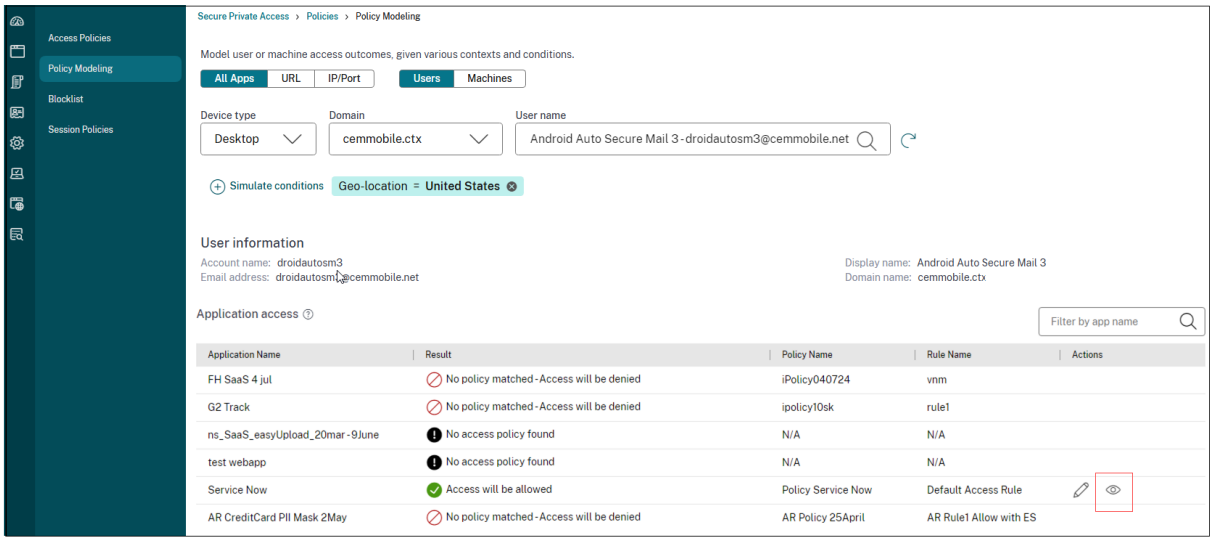
1. Secure Private Access コンソールで、[アクセス ポリシー] をクリックし、[ポリシー モデリング] タブをクリックします。
2. 次の詳細を追加します。

   - 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: アプリケーションと関連ポリシーを分析するユーザー名を選択します。

3. エンド ユーザーとそのデバイスに対する一連の条件/制約をシミュレートすることもできます。> 注**:** > > 正確な結果を取得するには、正確なユーザー条件を追加します。
4. 条件をシミュレートをクリックします。
5. 条件 (デバイスの状態、地理的位置、ネットワークの場所、ユーザーのリスク 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. さらに条件を追加するには、+ 記号をクリックします。
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、関連付けられたポリシー、およびルールが表形式で表示されます。



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。

エンタープライズウェブアプリのサポート

October 21, 2024

Secure Private Access サービスを使用した Web アプリ配信により、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るようになります。よく使用される Web アプリには、SharePoint、Confluence、OneBug などがあります。

Web アプリには、Citrix Workspace の Secure Private Access サービスを使用してアクセスできます。Citrix Workspace と連携した Secure Private Access サービスは、構成された Web アプリ、SaaS アプリ、構成された仮想アプリ、またはその他のワークスペース リソースに対して統一されたユーザー 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。

- 安全なプライベートアクセス標準
- Secure Private Access Advanced

システム要件

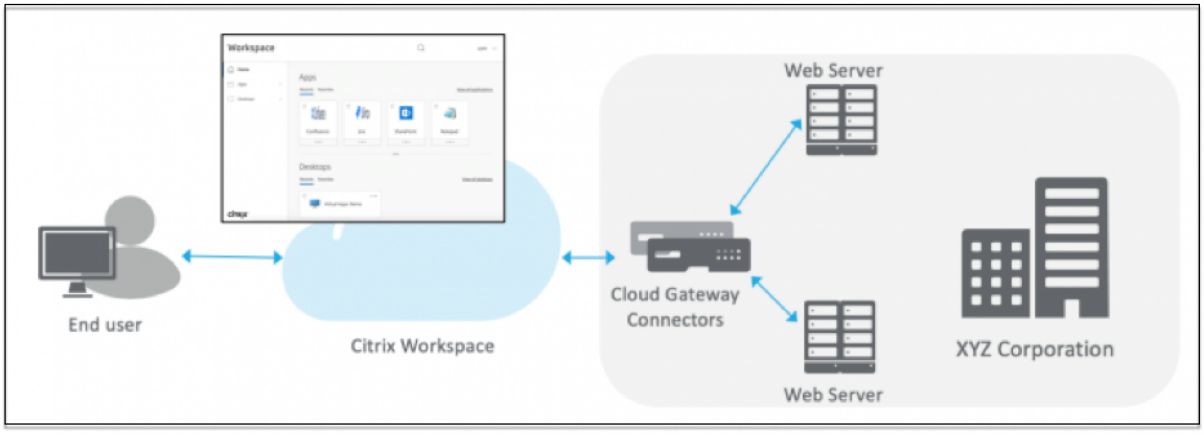
コネクタアプライアンス - コネクタアプライアンスを Citrix Secure Private Access サービスと共に使用して、顧客のデータセンター内のエンタープライズ Web アプリへの VPN なしのアクセスをサポートします。詳細については、「コネクタ アプライアンスを使用したワークスペース アクセスのセキュリティ保護」を参照してください。

機能

Citrix Secure Private Access サービスは、オンプレミスに展開された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、オンプレミスに展開されたエンタープライズ Web アプリと Citrix Secure Private Access サービス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。

コネクタ アプライアンスとクラウド内の 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るオンプレミス 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 なしの接続を使用して Workspace 経由でアクセスおよび配信されます。

次の図は、Citrix Workspace を使用して Web アプリケーションにアクセスする方法を示しています。



Web アプリを構成する

Web アプリを構成するには、次の大まかな手順を実行します。

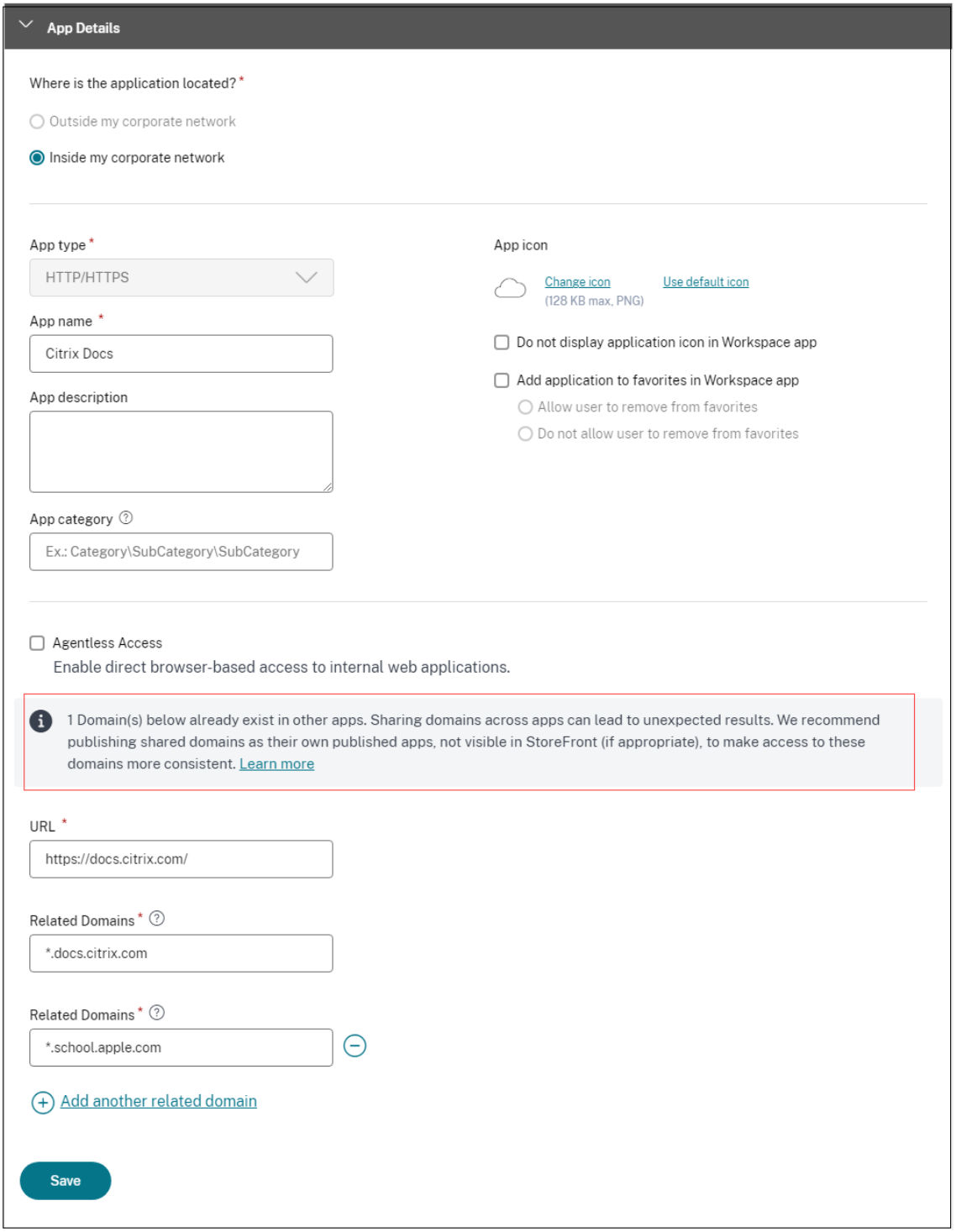
1. アプリケーションの詳細を設定する
2. 優先サインオン方法を設定する
3. アプリケーションルーティングを定義する

アプリケーションの詳細を構成する

1. セキュア プライベート アクセス タイルで、管理をクリックします。
2. Secure Private Access ランディング ページで、続行 をクリックし、次に アプリの追加 をクリックします。

> 注意:
>
> 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。以降の使用では、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。

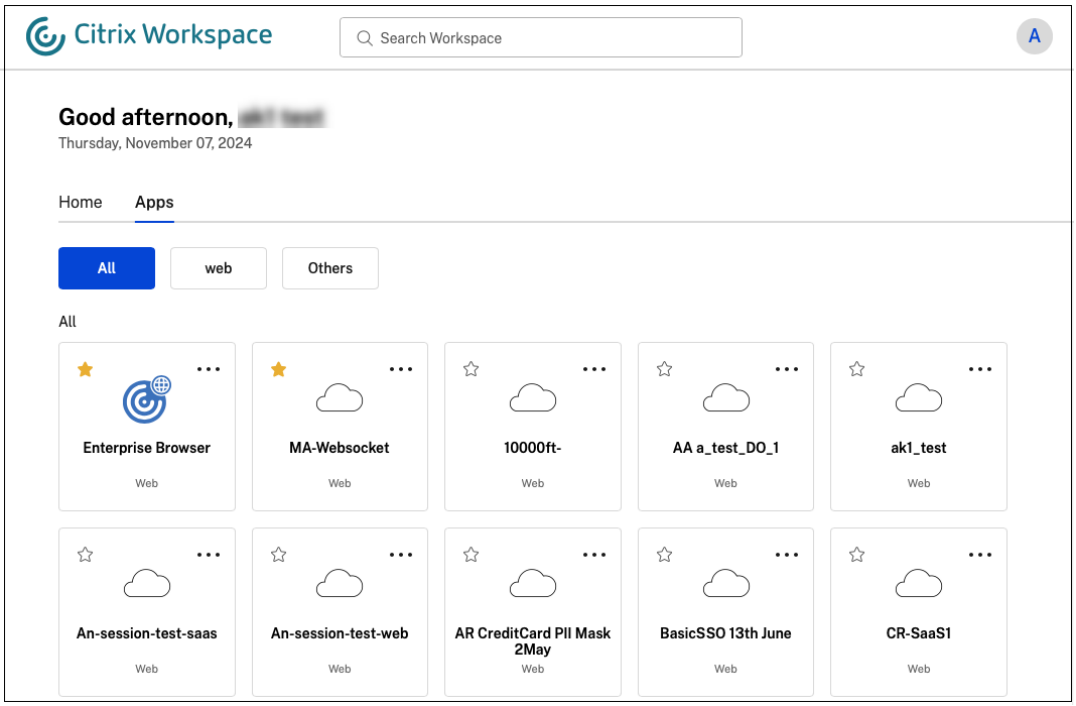
1. 追加したいアプリを選択し、スキップをクリックします。
2. アプリケーションの場所はどこにありますか? で、場所を選択します。
3. アプリの詳細 セクションに次の詳細を入力し、次へ をクリックします。



- 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。ここで入力した説明は、ワークスペース内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 に表示されるカテゴリとサブカテゴリ名（該当する場合）を追加します。各アプリ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、管理者はアプリごと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 アプリでは非表示になります。
  - カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。たとえば、**Business And Productivity\Engineering** などです。また、このフィールドで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リストされます。

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



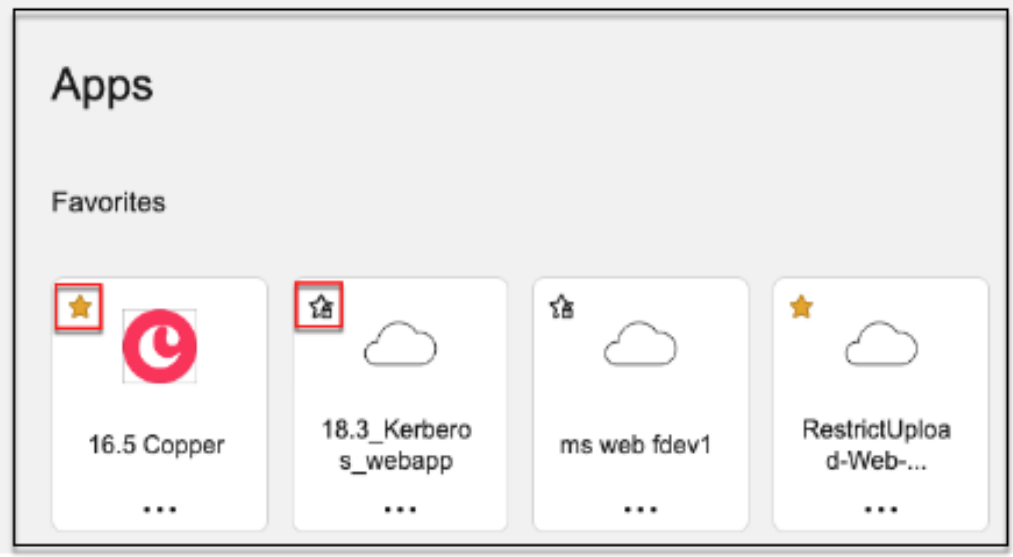
- アプリアイコン–アプリアイコンを変更するには、アイコンの変更 をクリックします。アイコン ファイルのサイズは 128 x 128 ピクセルである必要があります。アイコンを変更しない場合は、デフォルトのアイコンが表示されます。

```
If you do not want to display the app icon, select **Do not display application icon to users.**
```


- ユーザーがクライアント ブラウザーから直接アプリにアクセスできるようにするには、直接アクセス を選択します。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。
- **URL** –顧客 ID を含む URL。URL には顧客 ID (Citrix Cloud 顧客 ID) が含まれている必要があります。顧客 ID を取得するには、「Citrix Cloud へのサインアップ」を参照してください。SSO が失敗した場合、または SSO を使用しない場合は、ユーザーはこの URL にリダイレクトされます。

```
**Customer domain name** and **Customer domain ID** -
    Customer domain name and ID are used to create the app URL
     and other subsequent URLs in the SAML SSO page.

For example, if you're adding a Salesforce app, your domain
    name is `salesforceformyorg` and ID is 123754, then the
    app URL is `https://salesforceformyorg.my.salesforce.com/?
    so=123754.`

Customer domain name and Customer ID fields are specific to
    certain apps.
```

- 関連ドメイン–関連ドメインは、指定した URL に基づいて自動的に入力されます。関連ドメインは、サービスが URL をアプリの一部として識別し、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。関連するドメインを複数追加できます。
- このアプリを Citrix Workspace アプリのお気に入りアプリとして追加するには、「アプリケーションを自動的にお気に入りに追加」をクリックします。
  - アプリの利用者が 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るようにするには、［ユーザーがお気に入りから削除できるようにする］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、［ユーザーがお気に入りから削除することを許可しない］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。



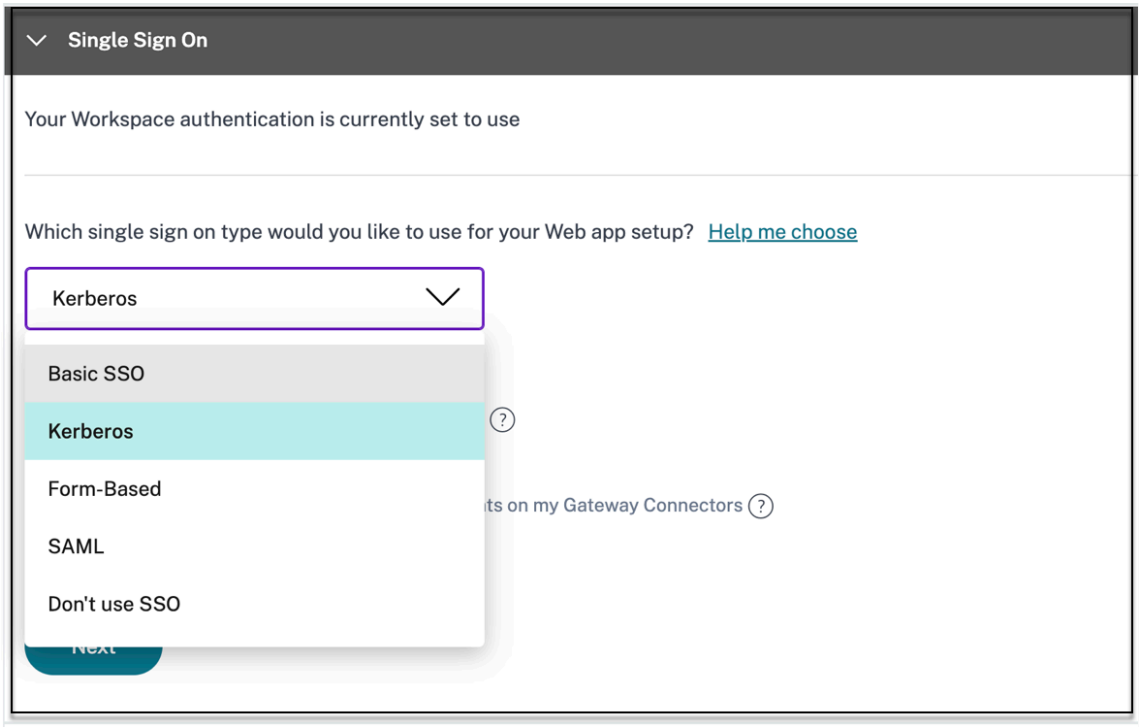
Secure Private Access サービス コンソールからお気に入りとしてマークされたアプリを削除する場合、これらのアプリは Citrix Workspace のお気に入りリストから手動で削除する必要があります。Secure Private Access サービス コンソールから削除された場合でも、アプリは Workspace アプリから自動的に削除されません。

4. 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。アプリケーションにアクセス ポリシーが関連付けられている場合にのみ、アプリへのアクセスが有効になります。詳細については、「デフォルトでアプリへのアクセスが拒否されます」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。詳細については、「アプリのアクセスの問題を引き起こす可能性のある競合する構成」を参照してください。

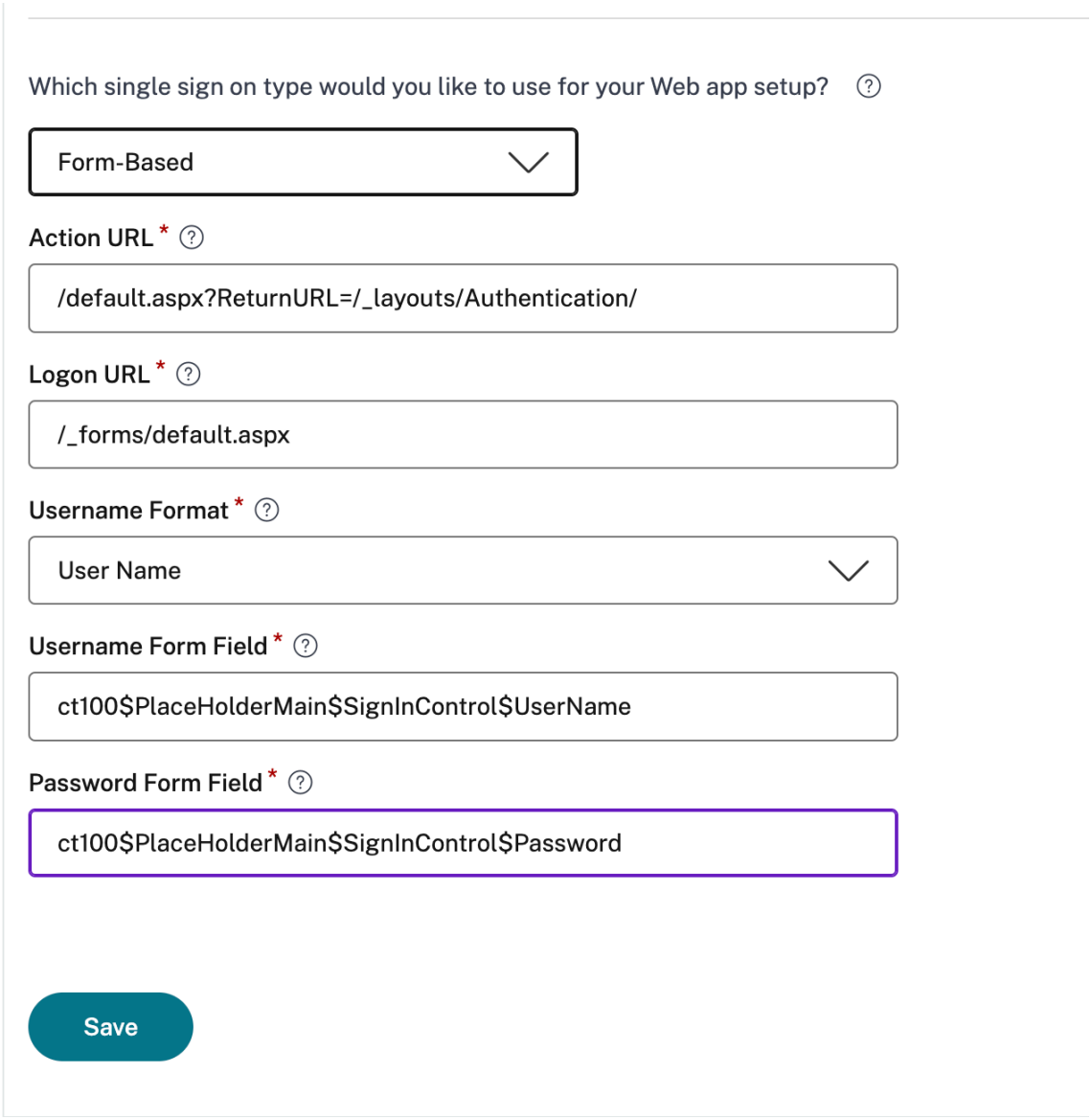
優先サインオン方法を設定する

1. シングル サインオン セクションで、アプリケーションで使用する優先シングル サインオン タイプを選択し、保存をクリックします。利用可能なシングル サインオンの種類は次のとおりです。



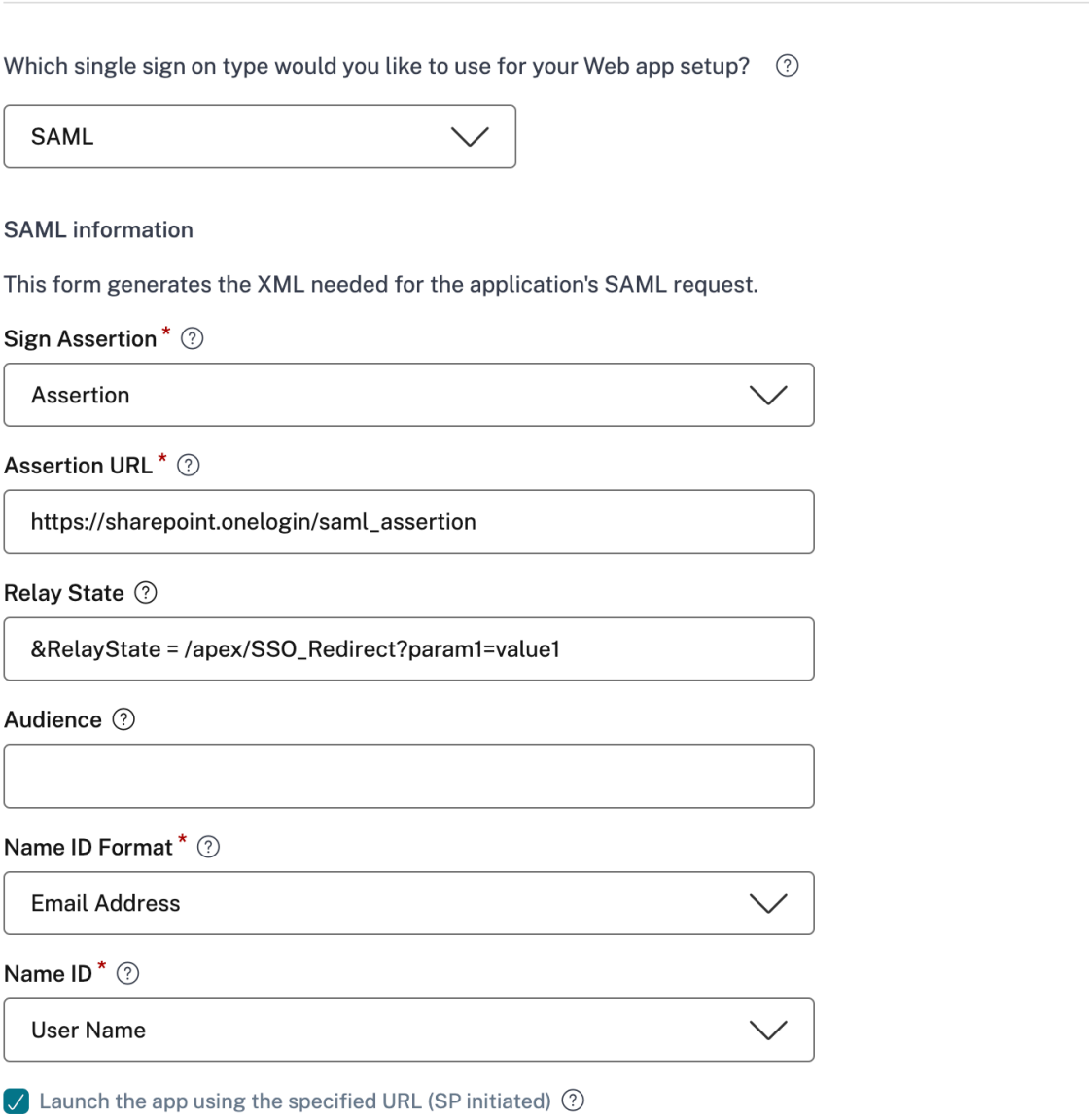
- 基本–バックエンド サーバーが基本 401 チャレンジを提示する場合は、基本 **SSO** を選択します。基本 SSO タイプについては、構成の詳細を指定する必要はありません。
- **Kerberos** –バックエンド サーバーがネゴシエート 401 チャレンジを提示する場合は、**Kerberos** を選択します。**Kerberos** SSO タイプについては、構成の詳細を指定する必要はありません。
- フォームベース–バックエンド サーバーが認証用に HTML フォームを提示する場合は、フォームベースを選択します。フォームベース SSO タイプの構成詳細を入力します。
- **SAML** - Web アプリケーションへの SAML ベースの SSO の場合は、**SAML** を選択します。**SAML** SSO タイプの設定詳細を入力します。
- **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、**SSO** を使用しない オプションを使用します。**SSO** を使用しない オプションが選択されている場合、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** - 完了したフォームが送信される URL を入力します。
- ログオン フォーム **URL** –ログオン フォームが表示される 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。



- アサーションの署名 - アサーションまたは応答に署名すると、応答またはアサーションが依存パーティ (SP) に配信されたときにメッセージの整合性が保証されます。アサーション、レスポンス、両方、または 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。
- リレー状態–リレー状態パラメーターは、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 ステートは、ユーザーに対して単一の URL を生成します。ユーザーはこの URL をクリックして、対象アプリケーションにログオンできます。
- 対象者–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たことを確認します。

- 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**)** で、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。

> 注意**:**
>
> - ログイン **URL** の下の SSO ログイン URL をコピーし、SaaS アプリ サーバーで SSO を構成するときにこの URL を使用できます。
> - また、証明書 リストから証明書をダウンロードし、SaaS アプリ サーバーで SSO を構成するときにその証明書を使用することもできます。

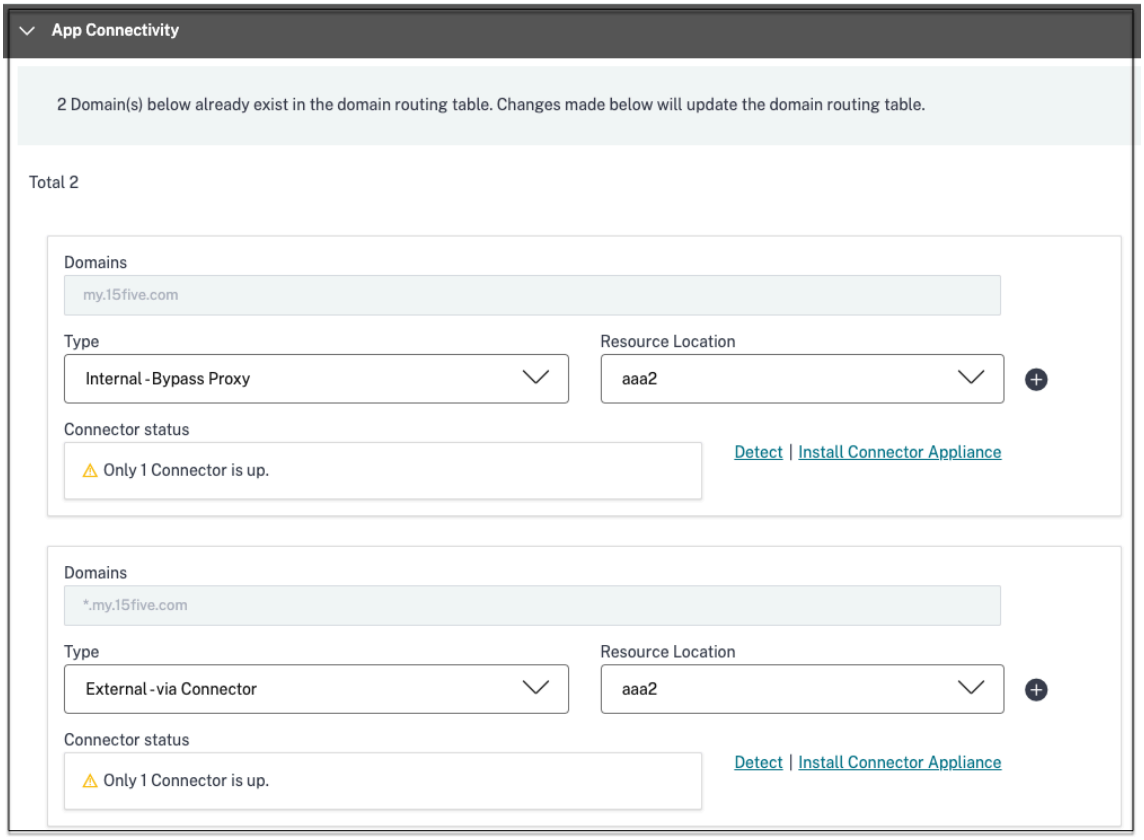
1. 次へをクリックします。

アプリケーションルーティングを定義する

1. **App Connectivity** セクションでは、Citrix Connector Appliance を介してドメインを外部または内部でルーティングする必要がある場合に、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。

   - 内部–プロキシをバイパス - ドメイン トラフィックは、コネクタ アプライアンスで構成された顧客の Web プロキシをバイパスして、Citrix Cloud Connector を介してルーティングされます。
   - コネクタ経由の内部 - アプリは外部にあってもかまいませんが、トラフィックはコネクタ アプライアンスを経由して外部ネットワークに流れる必要があります。
   - 外部–トラフィックは直接インターネットに流れます。

   詳細については、「SaaS アプリと Web アプリの両方で関連ドメインが同じ場合に競合を解決するためのルート テーブル」を参照してください。

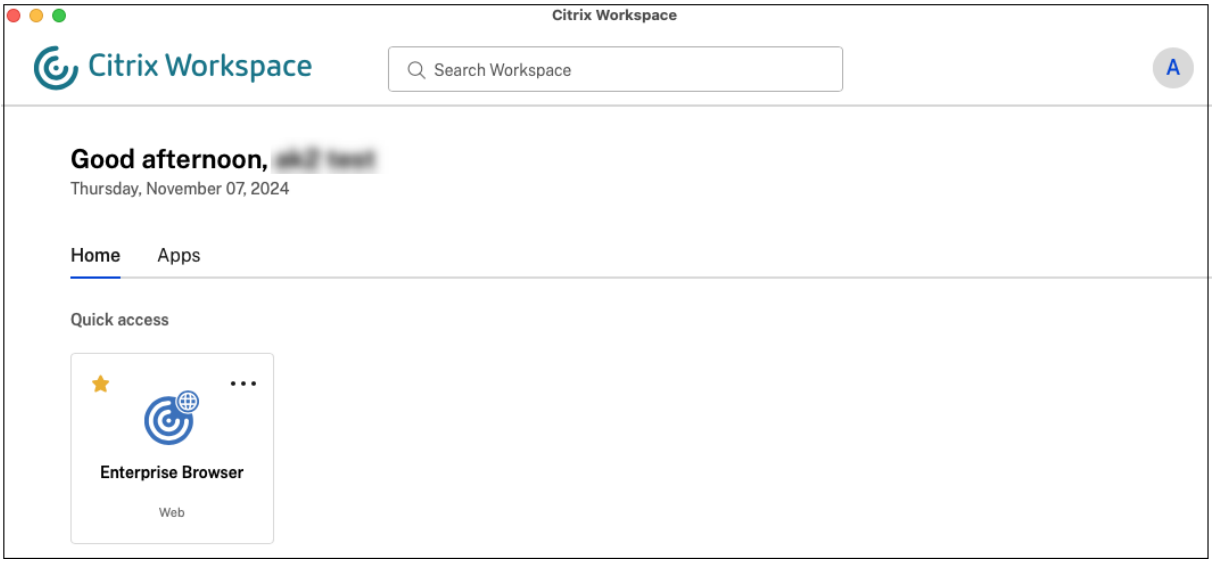


2. **[完了]** をクリックします。

   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。これを行うには、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 Citrix Workspace UI に自動的に表示されます。さらに、Citrix Enterprise Browser も、デフォルトでお気に入りの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内部 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、管理者はアプリ サブスクライバーを追加し、セキュリティ制御を構成します。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。

エンタープライズウェブアプリへの直接アクセス

October 21, 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 ブラウザー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。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 アプリにアクセスすることもできます。これにより、顧客に真のゼロフットプリントソリューションが提供されます。

機能

- 構成されたエンタープライズ 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、構成されたエンタープライズ Web アプリ FQDN の新しいパブリック DNS レコードを追加するか、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されたエンタープライズ Web アプリへのアクセスを開始すると、アプリ トラフィックは Citrix Secure Private Access サービスに誘導され、アプリへのアクセスがプロキシされます。
- リクエストが Citrix Secure Private Access サービスに到達すると、コンテキスト アクセス ポリシーのチェックを含む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、顧客の環境 (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、構成されたエンタープライズ Web アプリへのアクセスを有効にします。

Citrix Secure Private Access を構成してエンタープライズ **Web** アプリに直接アクセスする

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–設定するアプリの公開証明書
- 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、アプリの構成中に Citrix によって提供された正規名 (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構成する手順**:**

> 重要**:**
>
> アプリの完全なエンドツーエンドの構成については、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。

> 注意**:**
>
> 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。以降の使用では、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できます。

1. ID と認証を設定します。詳細については、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参照してください。
2. アプリの追加に進みます。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。
3. 追加したいアプリを選択し、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にありますか**?** 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 (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。ここで入力した説明は、ワークスペース内のユーザーに表示されます。
- アプリアイコン–アプリアイコンを変更するには、アイコンの変更 をクリックします。アイコン ファイルのサイズは 128 x 128 ピクセルである必要があります。アイコンを変更しない場合は、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。

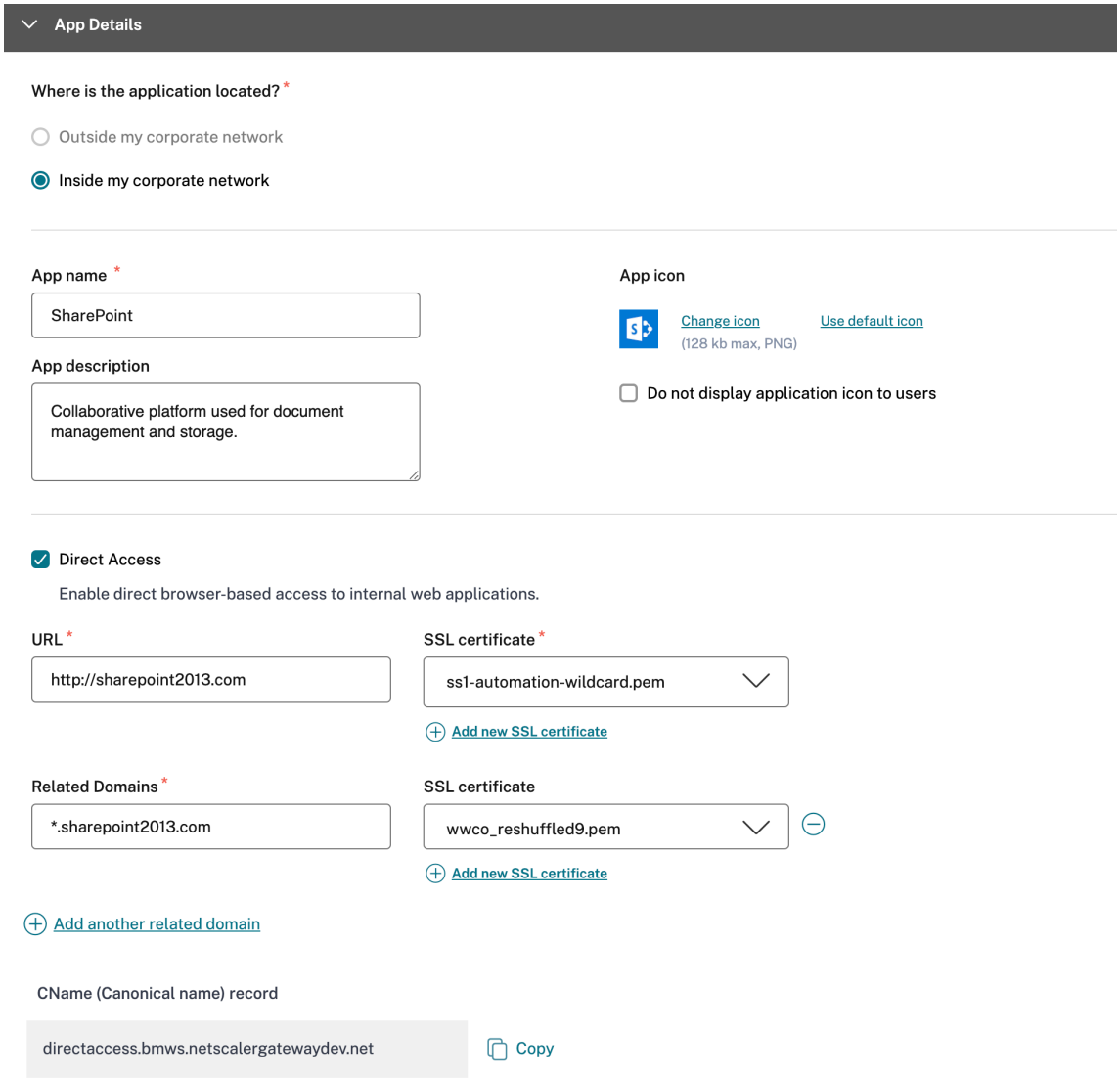
6. ユーザーがクライアント ブラウザーから直接アプリにアクセスできるようにするには、直接アクセス を選択します。次の詳細を入力します。

   - **URL** –バックエンドアプリケーションの URL。URL は HTTPS 形式である必要があり、対応する DNS エントリが管理者によって追加される必要があります。
   - **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。

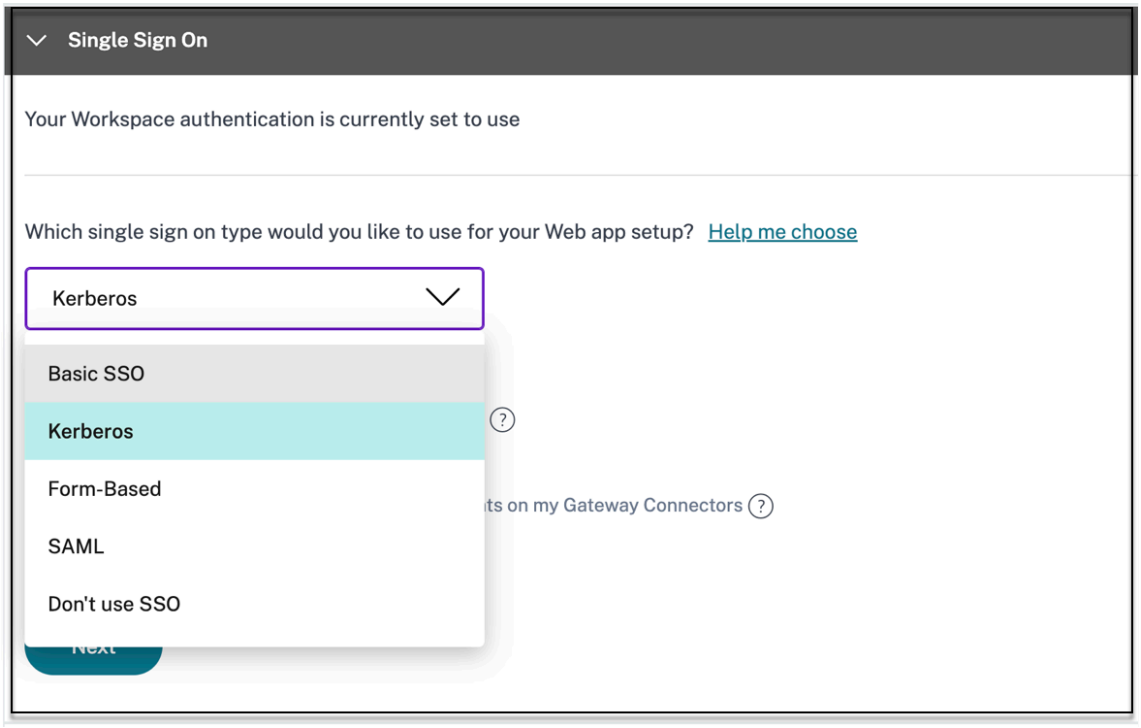
     注意事項:

     – パブリック証明書または信頼された 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。
     – 証明書の完全なチェーンをアップロードする必要があります。

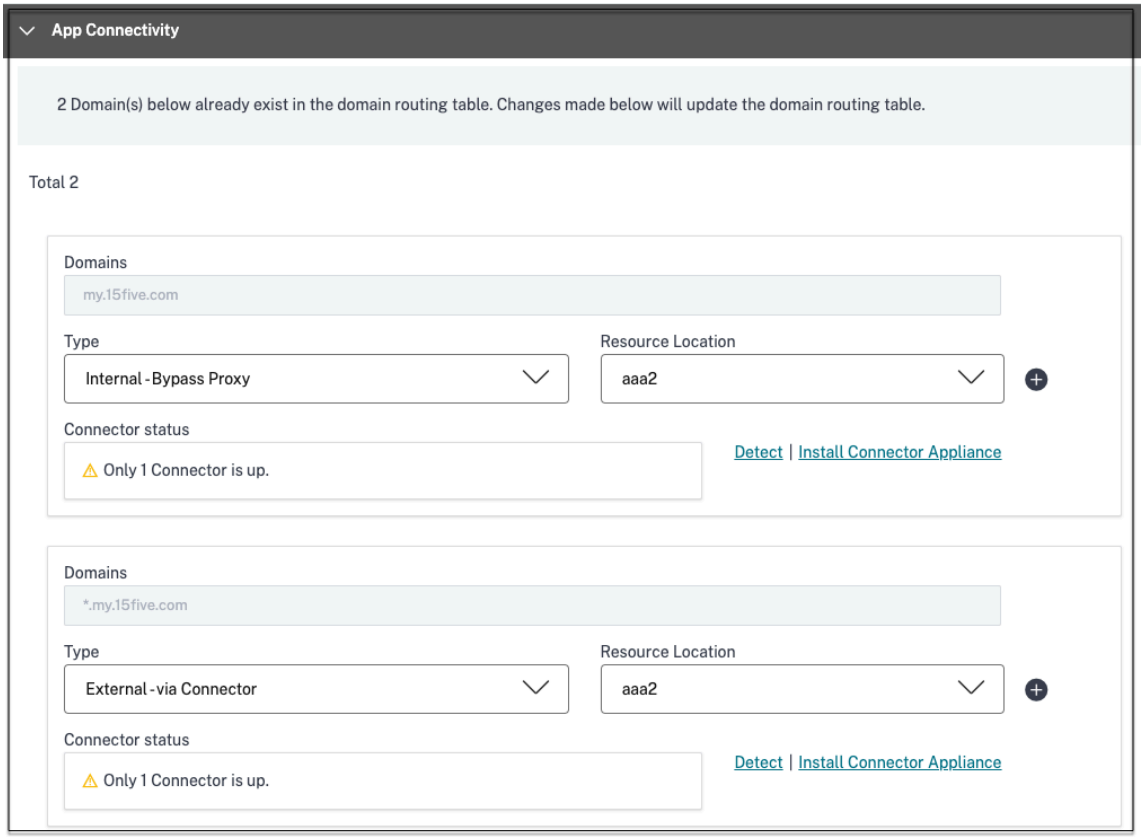
   - 関連ドメイン–関連ドメインは、指定した URL に基づいて自動的に入力されます。関連ドメインは、サービスが URL をアプリの一部として識別し、それに応じてトラフィックをルーティングするのに役立ちます。関連するドメインを複数追加できます。関連する各ドメインに SSL 証明書をバインドできますが、これはオプションです。
   - **CName** レコード–Secure Private Access によって自動生成されます。これは、アプリケーションへの直接アクセスを有効にするために DNS に入力する必要がある値です。



7. 次へをクリックします。
8. 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優先シングル サインオン タイプを選択し、次へをクリックします。



9. アプリ接続 セクションでは、既存のリソースの場所を選択するか、リソースの場所を作成して新しいコネクタアプライアンスをデプロイすることができます。既存のリソースの場所を選択するには、リソースの場所のリストからリソースの場所の 1 つ (たとえば、[My Resource Location]) をクリックし、[**Next**] をクリックします。詳細については、「SaaS アプリと Web アプリの両方で関連ドメインが同じ場合に競合を解決するためのルート テーブル」を参照してください。



10. [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、「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。これを行うには、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。アプリケーションにアクセス ポリシーが関連付けられている場合にのみ、アプリへのアクセスが有効になります。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。

直接アクセス アプリを備えたデバイス ポスチャ サービス

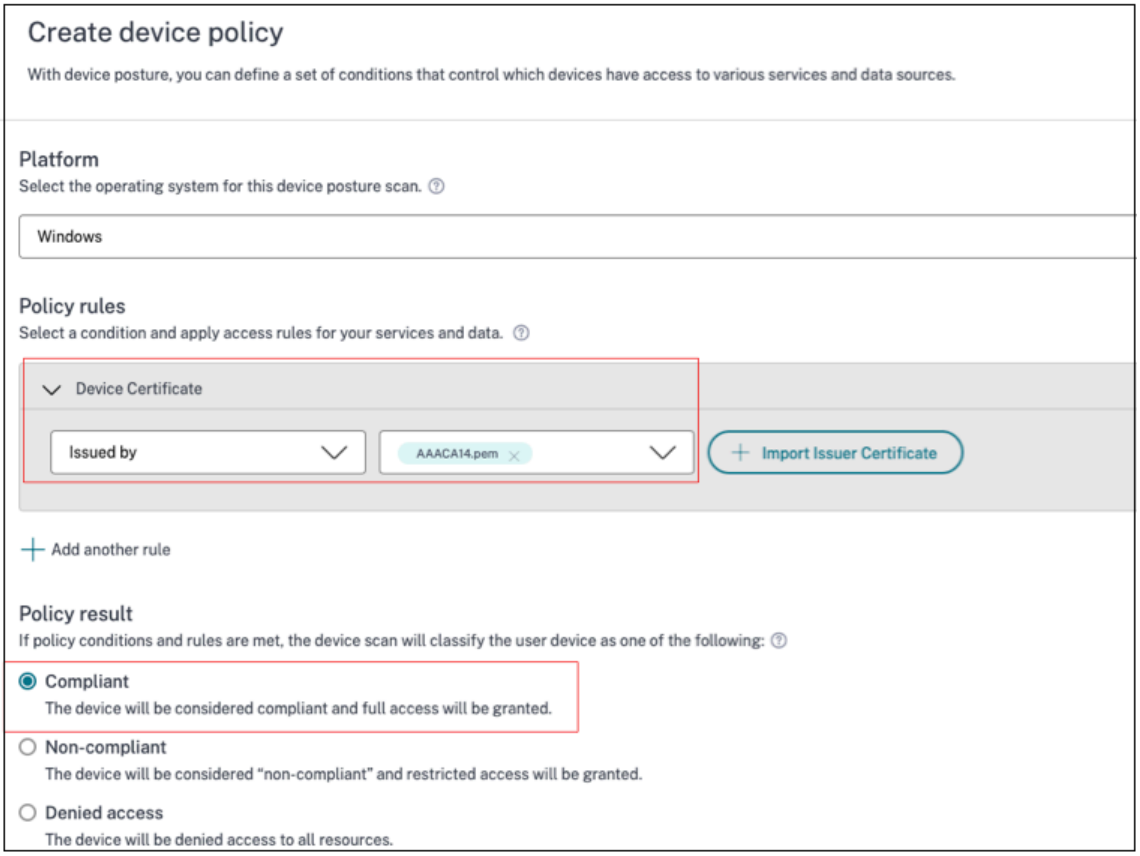
Citrix Secure Private Access と直接アクセス アプリを Device Posture サービスと組み合わせると、準拠しているデバイスのみが直接アクセスを通じて機密アプリケーションにアクセスできるようになります。管理者は、デバイ

ス ポスチャ サービスのスキャン結果に基づいて、非準拠デバイスまたは管理対象外デバイスへのアクセスをブロックできます。

準拠デバイスのみに直接アクセスを有効にする手順

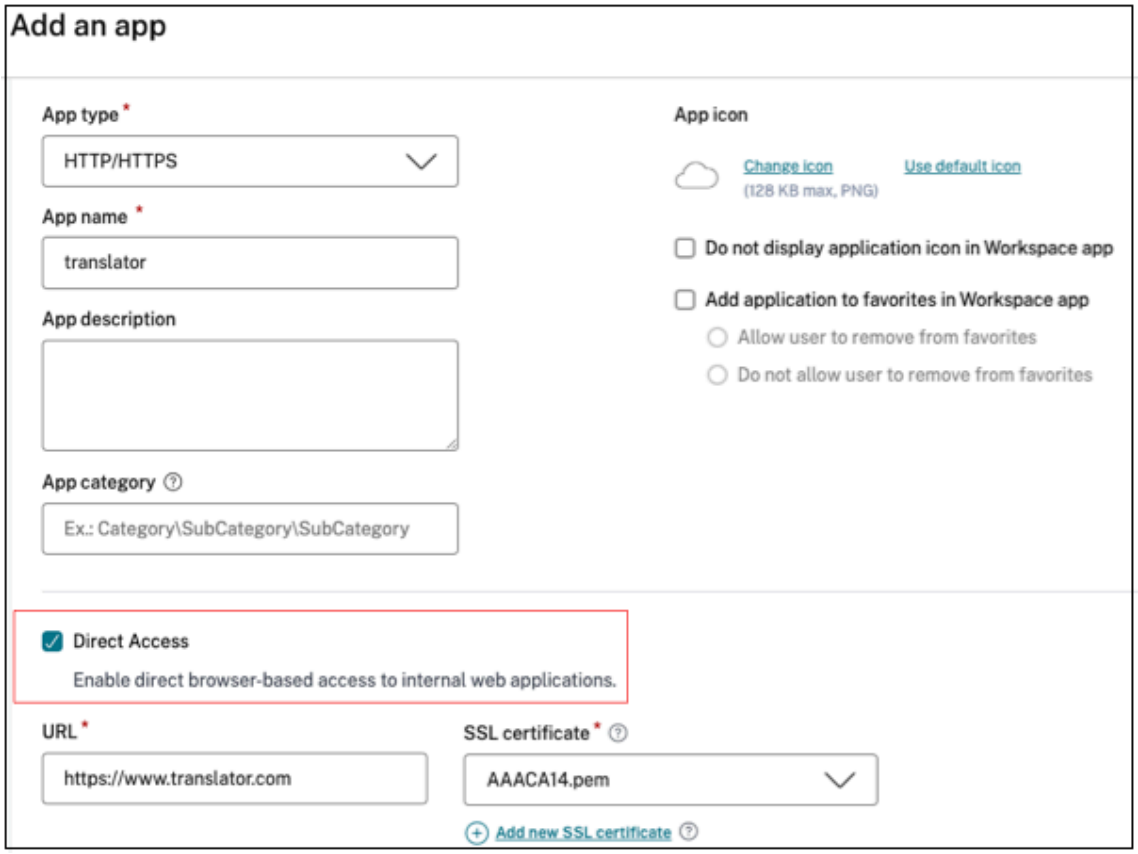
準拠デバイスのみへの直接アクセスを有効にするには、管理者は次の手順を実行する必要があります。

1. デバイス ポスチャ サービス管理コンソールから、デバイス ポスチャ ポリシーを作成し、デバイス証明書、ウイルス対策、ブラウザーなどのデバイス ポスチャ スキャン条件をチェックし、ポリシー結果アクションとして 準拠 を選択します。詳細については、「デバイスの状態を構成する」を参照してください。



2. Secure Private Access 管理コンソールから、次の操作を実行します。

   - 直接アクセスを有効にするアプリケーションを作成します。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。



- デバイス ポスチャを使用して安全なプライベート アクセスを構成します。ルールのスコープで、デバイス ポスチャ チェック > いずれかに一致 を選択し、タグ 準拠を入力します。このタグは、デバイス ポスチャ サービスから送信されます。

> 注意:
>
> タグは、先頭を大文字にして、先ほどキャプチャしたとおりに正確に入力する必要があります (準拠)。そうしないと、デバイス ポスチャ ポリシーは意図したとおりに機能しません。詳細については、「Device Posture を使用した Citrix Secure Private Access の構成」を参照してください。

```
1 ![直接アクセスのためのデバイス姿勢3](/en-us/citrix-secure-private-
    access/media/spa-direct-access-device-posture-3.png)
```

この構成を実行すると、デバイスのポスチャ スキャン結果に基づいて、デバイスは準拠、非準拠、またはログイン拒否としてタグ付けされ、それに応じてアプリ アクセスが有効になります。

例:

エンドポイント デバイスにデバイス証明書が存在するかどうかを確認し、ログイン ステータスを判断するためのデバイス ポスチャ ポリシーを作成したとします。デバイス ポスチャ ポリシーが設定され、デバイス ポスチャが有効になると、エンド ユーザーが Citrix Workspace にログインしたときに次のアクションが実行されます。

1. デバイス ポスチャ スキャンは、エンドポイント デバイスにデバイス証明書が存在するかどうかを確認します。

- デバイス証明書がデバイス上に存在する場合、デバイスは 準拠としてタグ付けされます。
- デバイス証明書がデバイスに存在しない場合、デバイスは 非準拠としてタグ付けされます。

2. この情報はタグとして Citrix Secure Private Access サービスに渡されます。
3. アクセス ポリシーは、デバイスの分類に基づいて評価されます。

    - デバイスが準拠している場合は、アプリへの直接アクセスが許可されます。
    - デバイスが準拠していない場合、アプリへの直接アクセスは無効になります。

エンドユーザーエクスペリエンス

エンド ユーザー エクスペリエンスは、デバイスが準拠しているか非準拠であるかの分類に基づいて決まります。

- 対応デバイス**:**

  ユーザーは、Citrix Workspace から、またはアプリ URL を使用してブラウザーから直接アクセス アプリを起動できます。

- 非準拠デバイス**:**

  - アプリは Citrix Workspace に列挙されません。
  - ユーザーはアプリの URL を使用してブラウザからアプリを起動できません。
  - アクセスがブロックされたページがユーザーに表示されます。

サービスとしてのソフトウェア アプリのサポート

October 21, 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ソフトウェア配布モデルです。一般的に使用される SaaS アプリには、Salesforce、Workday、Concur、GoToMeeting などがあります。

SaaS アプリには、Citrix Workspace の Secure Private Access サービスを使用してアクセスできます。Citrix Workspace と連携した Secure Private Access サービスは、構成された SaaS アプリ、構成された仮想アプリ、またはその他のワークスペース リソースに対して統一されたユーザー エクスペリエンスを提供します。

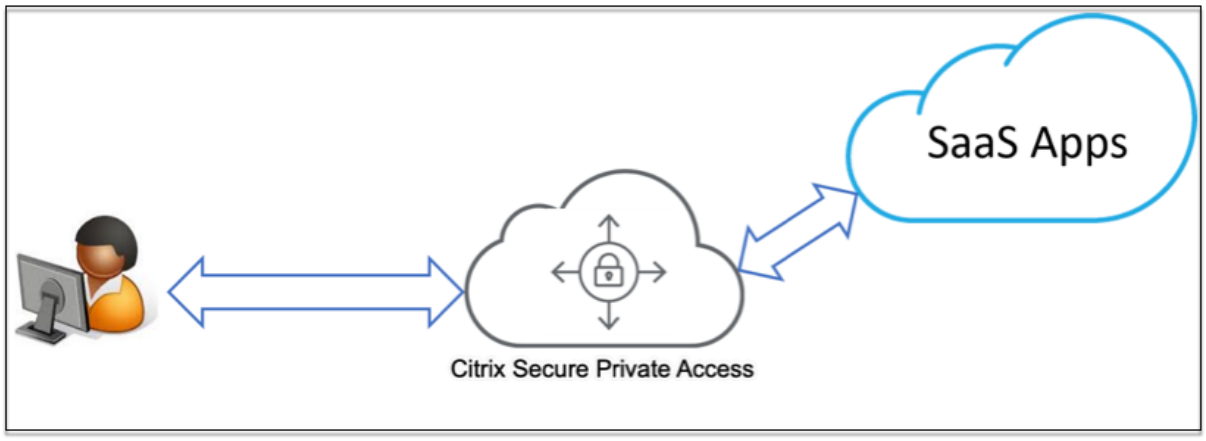
Secure Private Access サービスを使用した SaaS アプリ配信により、アプリを管理するための簡単、安全、堅牢、かつスケーラブルなソリューションが提供されます。クラウド上で配信される SaaS アプリには、次のような利点があります。

- 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 サインオンで簡単にログオンできます。
- さまざまなアプリ用の標準テンプレート–人気のあるアプリのテンプレートベースの構成。

SaaS アプリが **Secure Private Access** サービスでサポートされる方法

1. 顧客管理者は、Secure Private Access サービス 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、ユーザーは列挙された 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、アプリが起動します。

> 注意:
>
> - 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、管理者はアプリ サブスクライバーを追加し、セキュリティ制御を構成します。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。
> - 構成された SaaS アプリは、Citrix Workspace 内の仮想アプリやその他のリソースとともに集約され、統一されたユーザー エクスペリエンスを実現します。



SaaS アプリを構成する

SaaS アプリを構成するには、次の大まかな手順を実行します。

1. アプリケーションの詳細を設定する
2. 優先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を定義する

アプリケーションの詳細を構成する

1. セキュア プライベート アクセス タイルで、管理をクリックします。
2. 続行 をクリックし、次に アプリの追加 をクリックします。

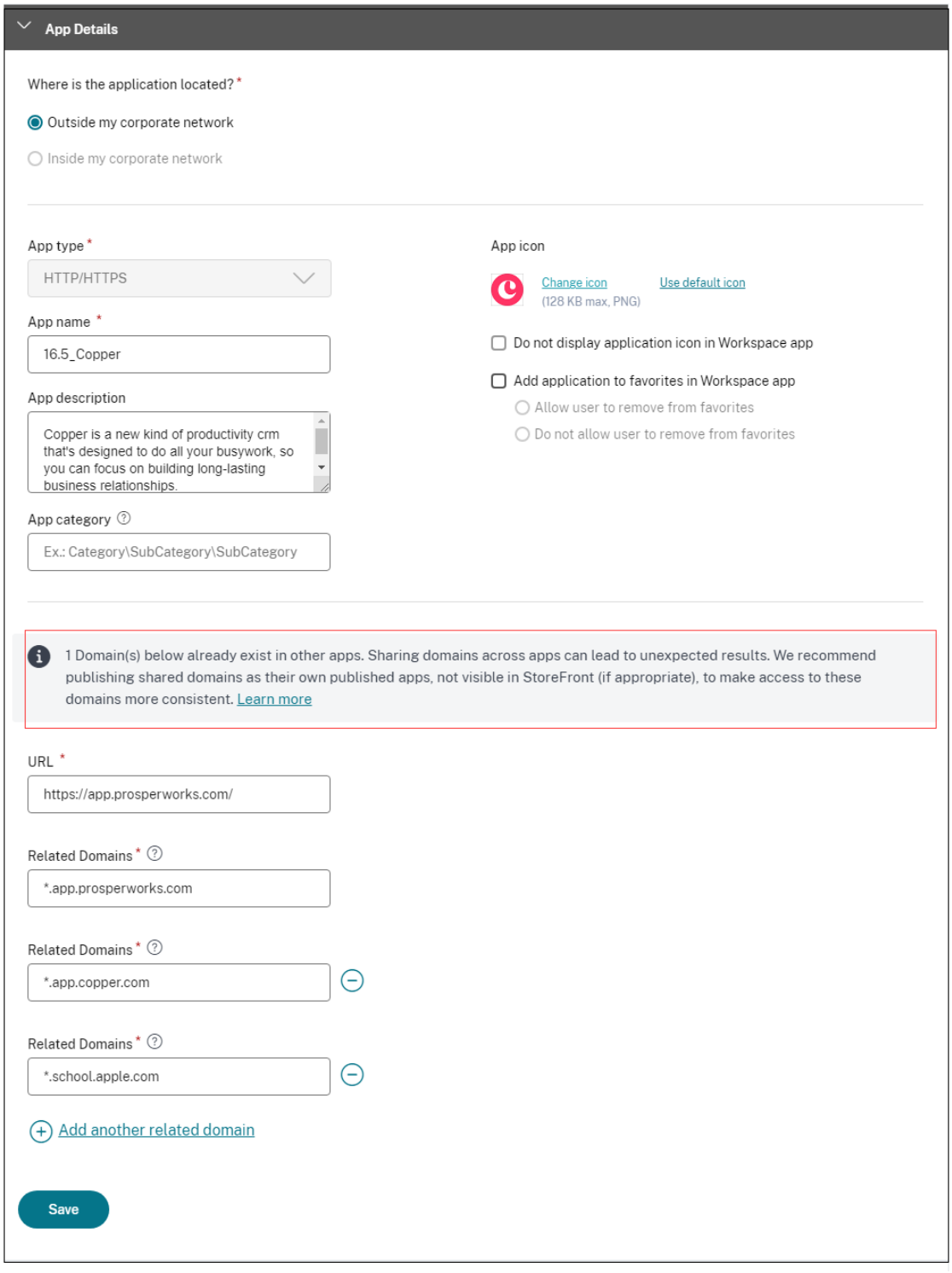
> 注意:
>
> - 続行 ボタンは、ウィザードを初めて使用するときにのみ表示されます。以降の使用では、アプリケーション ページに直接移動し、アプリの追加 をクリックします。
> - アプリの詳細を入力して SaaS アプリを手動で追加することも、人気のある SaaS アプリのリストで使用できるアプリ テンプレートを選択することもできます。テンプレートには、アプリケーションの構成に必要な情報の多くが事前に入力されています。ただし、顧客固有の情報は提供する必要があります。SaaS アプリ構成テンプレートの詳細については、SaaS アプリ サーバー固有の構成を参照してください。

1. アプリを設定します。

   - 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、企業ネットワークの外部 がデフォルトで有効になっています。

2. 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。

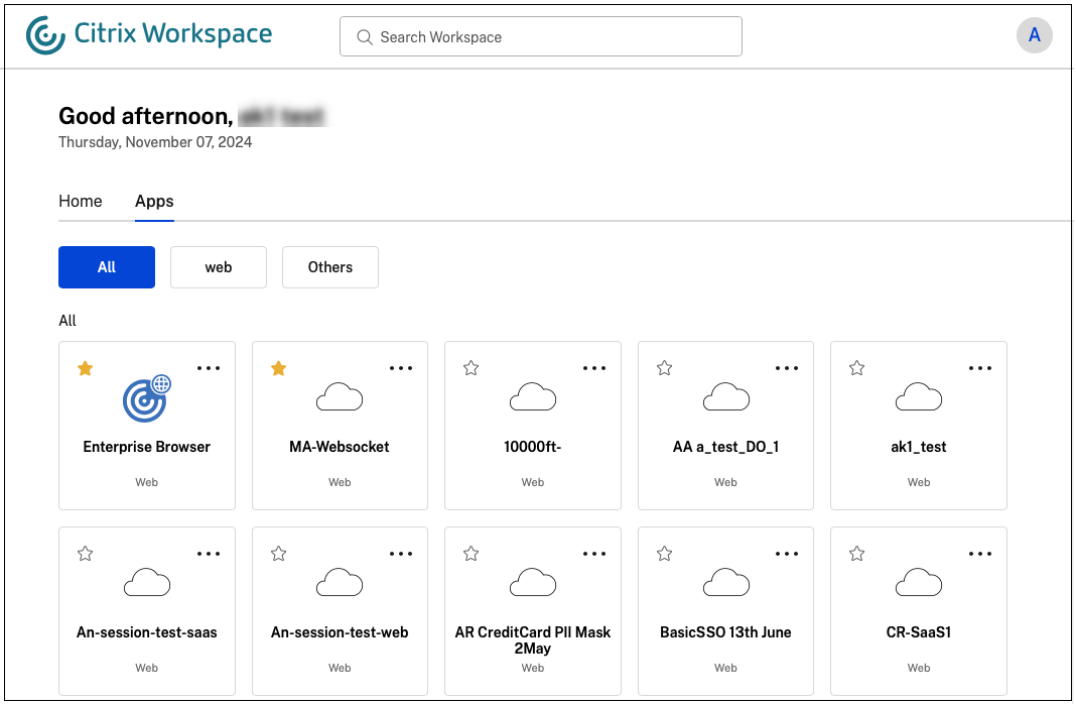


- アプリ名–アプリケーションの名前。
- アプリの説明 - アプリの簡単な説明。ここで入力した説明は、ワークスペース内のユーザーに表示されます。
- アプリ カテゴリ - 公開するアプリが Citrix Workspace UI に表示されるカテゴリとサブカテゴリ名（該

当する場合）を追加します。各アプリ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、管理者はアプリごと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 アプリでは非表示になります。
- カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。たとえば、**Business And Productivity\Engineering** などです。また、このフィールドで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 内の名前と「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リストされます。

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



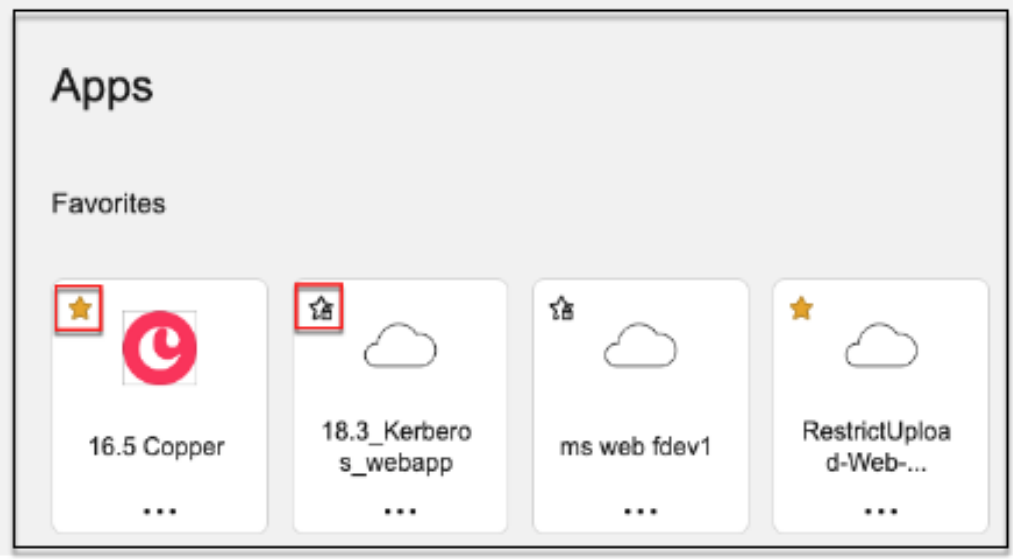
- アプリアイコン–アプリアイコンを変更するには、アイコンの変更 をクリックします。アイコン ファイルのサイズは 128 x 128 ピクセルである必要があります。アイコンを変更しない場合は、デフォルトのアイコンが表示されます。

```
1  If you do not want to display the app icon, select **Do not
       display application icon to users**.
```


- **URL** –顧客 ID を含む URL。URL には顧客 ID (Citrix Cloud 顧客 ID) が含まれている必要があります。顧客 ID を取得するには、「Citrix Cloud へのサインアップ」を参照してください。SSO が失敗した場合、または SSO を使用しない場合は、ユーザーはこの URL にリダイレクトされます。
- 顧客ドメイン名 および 顧客ドメイン **ID** - 顧客ドメイン名と ID は、SAML SSO ページでアプリ URL とその他の後続の URL を作成するために使用されます。

```
For example, if you' re adding a Salesforce app, your domain name is `salesforceformyorg` and ID is 123754, then the app URL is `https://salesforceformyorg.my.salesforce.com/?so=123754.`

Customer domain name and Customer ID fields are specific to certain apps.
```

- 関連ドメイン–関連ドメインは、指定した URL に基づいて自動的に入力されます。関連ドメインは、サービスが URL をアプリの一部として識別し、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。関連するドメインを複数追加できます。
- このアプリを Citrix Workspace アプリのお気に入りアプリとして追加するには、「アプリケーションを自動的にお気に入りに追加」をクリックします。
  - アプリの利用者が 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るようにするには、［ユーザーがお気に入りから削除できるようにする］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、［ユーザーがお気に入りから削除することを許可しない］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。



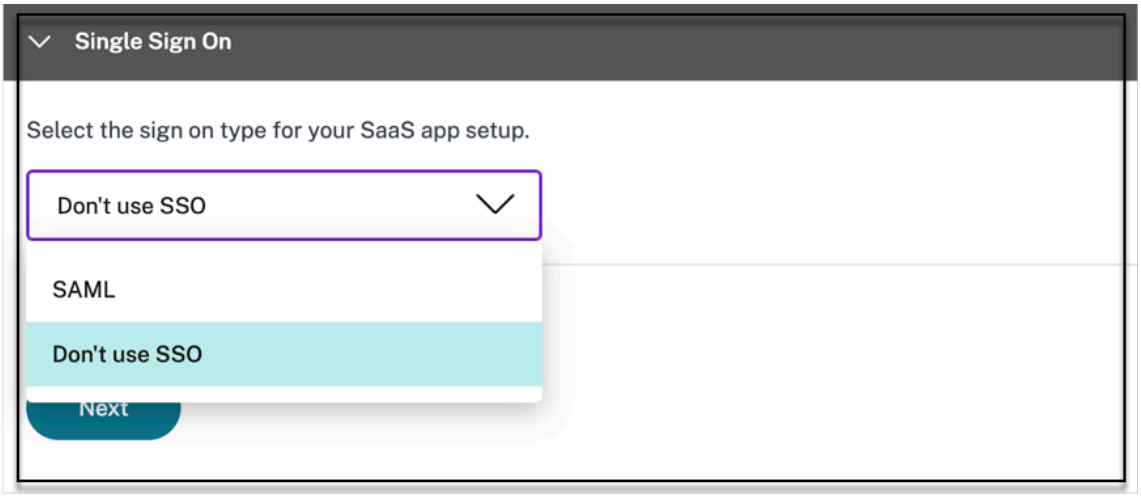
Secure Private Access サービス コンソールからお気に入りとしてマークされたアプリを削除する場合、これらのアプリは Citrix Workspace のお気に入りリストから手動で削除する必要があります。Secure Private Access サービス コンソールから削除された場合でも、アプリは Workspace アプリから自動的に削除されません。

3. 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。アプリケーションにアクセス ポリシーが関連付けられている場合にのみ、アプリへのアクセスが有効になります。詳細については、「デフォルトでアプリへのアクセスが拒否されます」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。詳細については、「アプリのアクセスの問題を引き起こす可能性のある競合する構成」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、アプリケーションで使用する優先シングル サインオン タイプを選択し、保存をクリックします。利用可能なシングル サインオンの種類は次のとおりです。

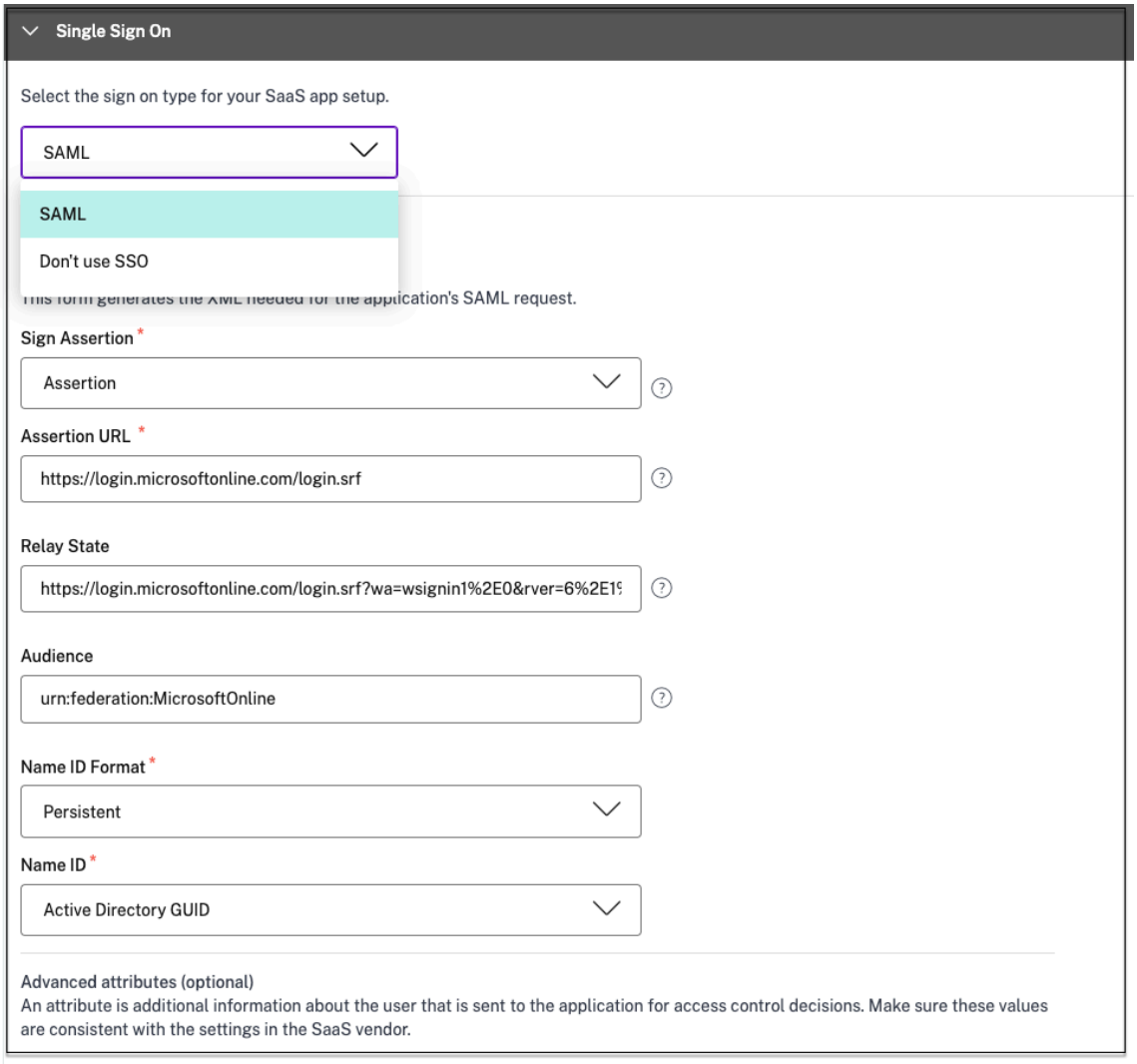


   - **SSO** を使用しない–バックエンド サーバーでユーザーを認証する必要がない場合は、**SSO** を使用しない オプションを使用します。**SSO** を使用しない オプションが選択されている場合、ユーザーは アプリの詳細 セクションで構成された URL にリダイレクトされます。
   - **SAML** - Web アプリケーションへの SAML ベースの SSO の場合は、**SAML** を選択します。**SAML** SSO タイプの設定詳細を入力します。

     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。

- アサーションの署名 - アサーションまたは応答に署名すると、応答またはアサーションが依存パーティ (SP) に配信されたときにメッセージの整合性が保証されます。アサーション、レスポンス、両方、または 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。
- リレー状態–リレー状態パラメーターは、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 ステートは、ユーザーに対して単一の URL を生成します。ユーザーはこの URL をクリックして、対象アプリケーションにログオンできます。
- 対象者–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たことを確認します。
- 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** が開始**)** を選択します。

2. 詳細属性 **(**オプション**)** で、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。

> 注意:
>
> - ログイン **URL** の下の SSO ログイン URL をコピーし、SaaS アプリ サーバーで SSO を構成するときにこの URL を使用できます。
> - また、証明書 リストから証明書をダウンロードし、SaaS アプリ サーバーで SSO を構成するときにその証明書を使用することもできます。

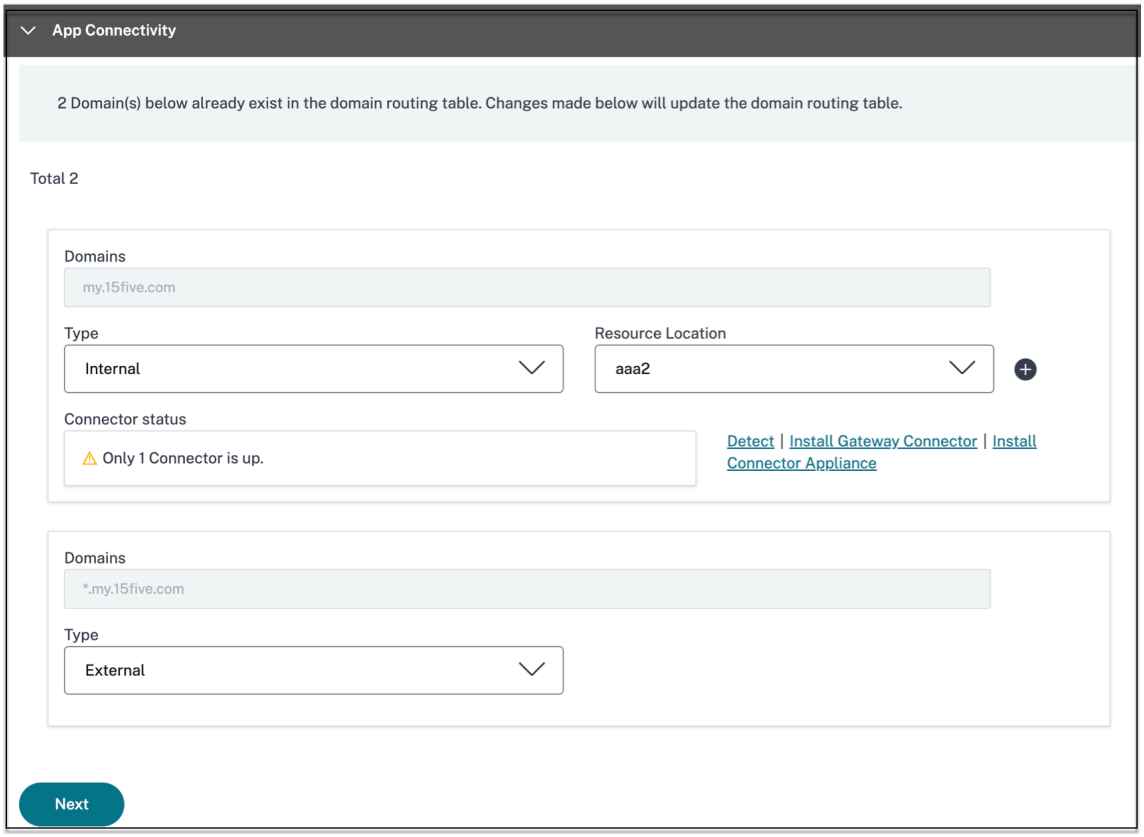
1. 次へをクリックします。

アプリケーションルーティングを定義する

1. **App Connectivity** セクションで、ドメインを Citrix Connector Appliances 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、アプリケーションの関連ドメインのルーティングを定義します。

- 内部–プロキシをバイパス - ドメイン トラフィックは、コネクタ アプライアンスで構成された顧客の Web プロキシをバイパスして、Citrix Cloud Connector を介してルーティングされます。
- コネクタ経由の内部 - アプリは外部にあってもかまいませんが、トラフィックはコネクタ アプライアンスを経由して外部ネットワークに流れる必要があります。

詳細については、「SaaS アプリと Web アプリの両方で関連ドメインが同じ場合に競合を解決するためのルート テーブル」を参照してください。

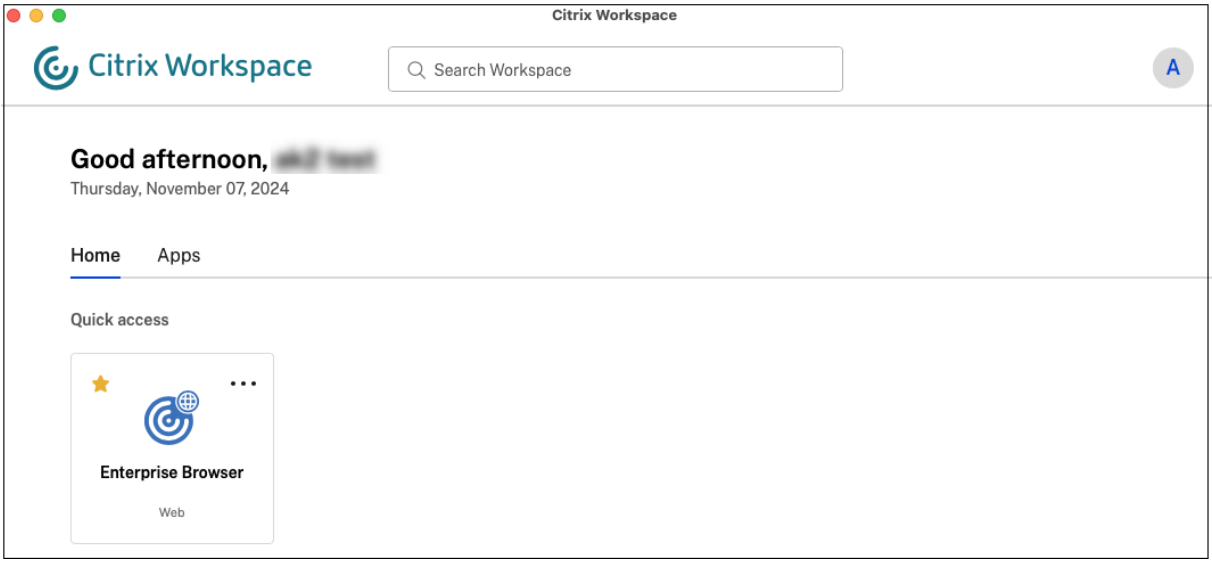


2. **[完了]** をクリックします。

   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。これを行うには、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 Citrix Workspace UI に自動的に表示されます。さらに、Citrix Enterprise Browser も、デフォルトでお気に入りの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内部 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の構成については、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参照してください。

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、

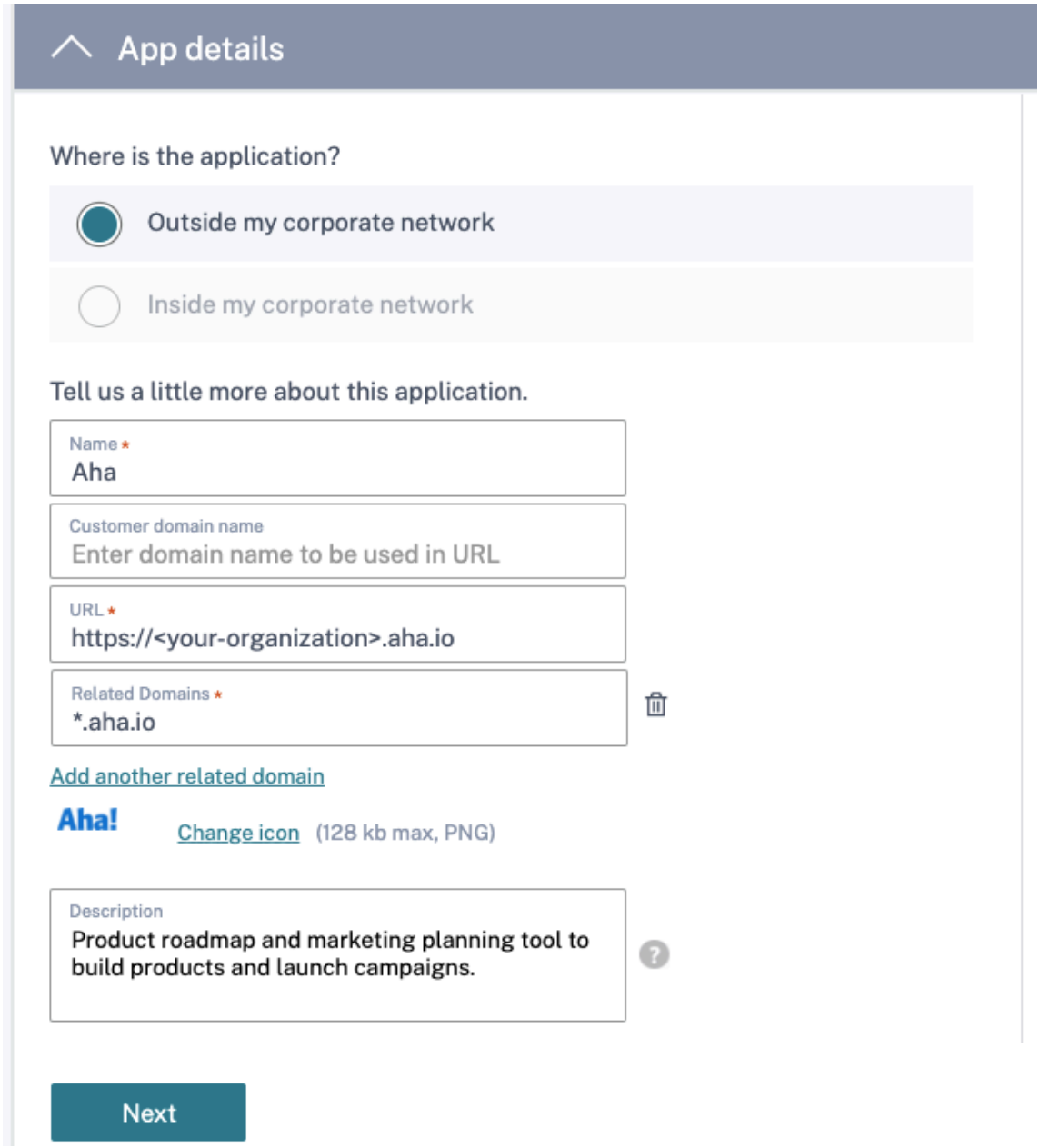
   顧客のドメイン名とカスタマードメイン **ID** -顧客のドメイン名と ID は、SAML SSO ページでアプリの URL とその他の後続の URL を作成するために使用されます。

   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。

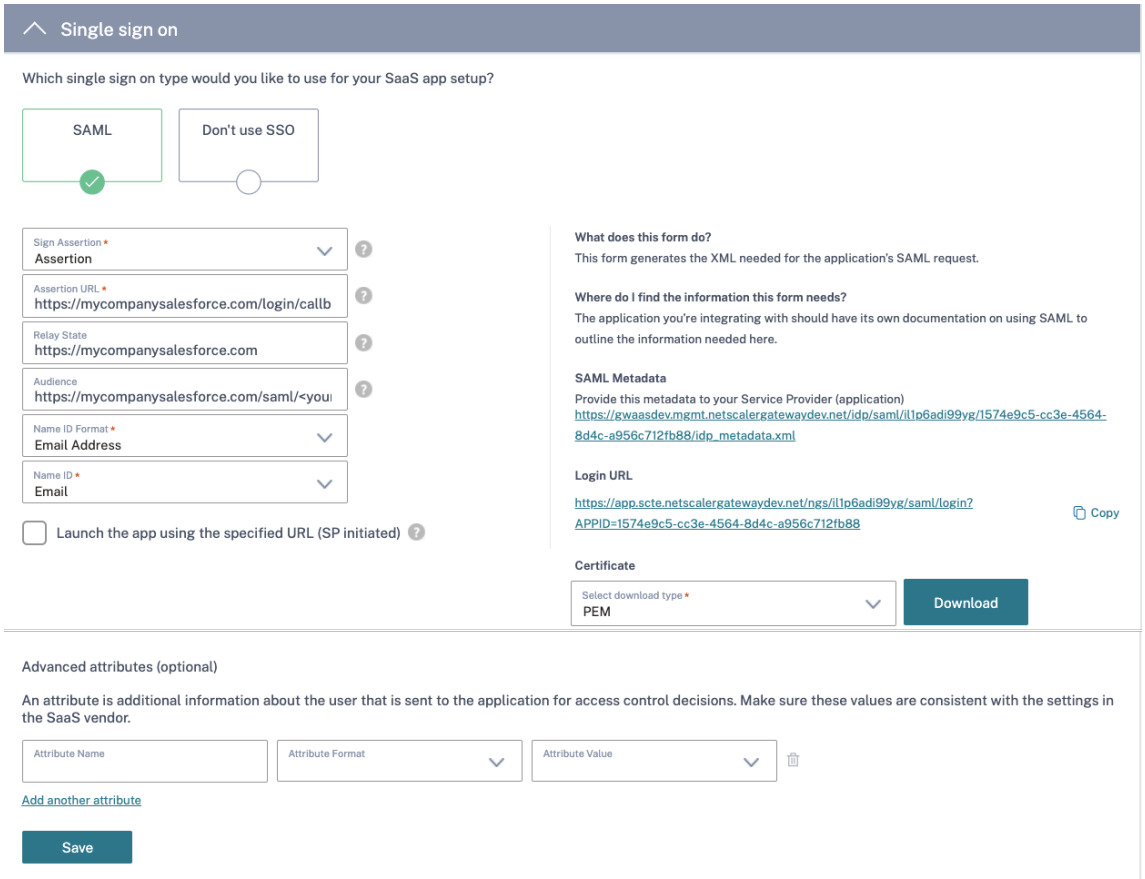
   アサーション **URL** —アプリケーションベンダーが提供する SaaS アプリケーションの SAML アサーション URL。SAML アサーションは、この URL に送信されます。

   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。

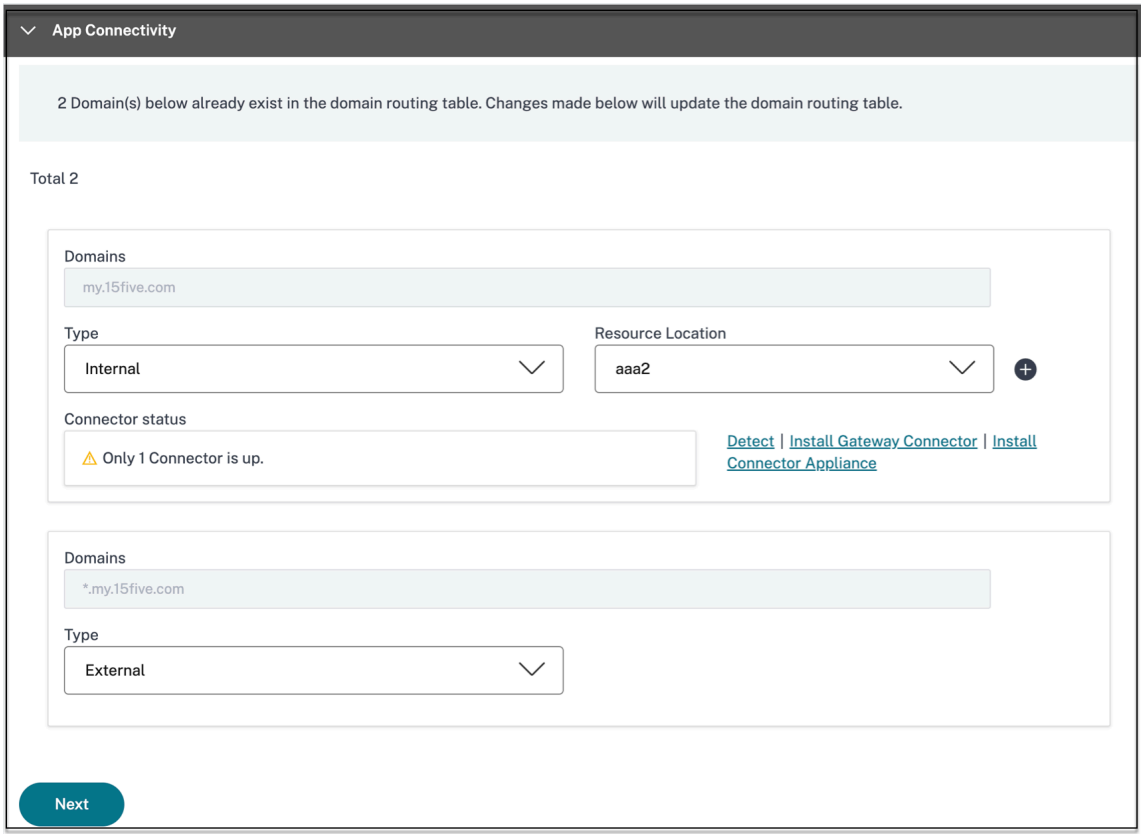
5. [**SAML** メタデータ**]** の下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaS アプリサーバーで SSO を構成します。

   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。

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。

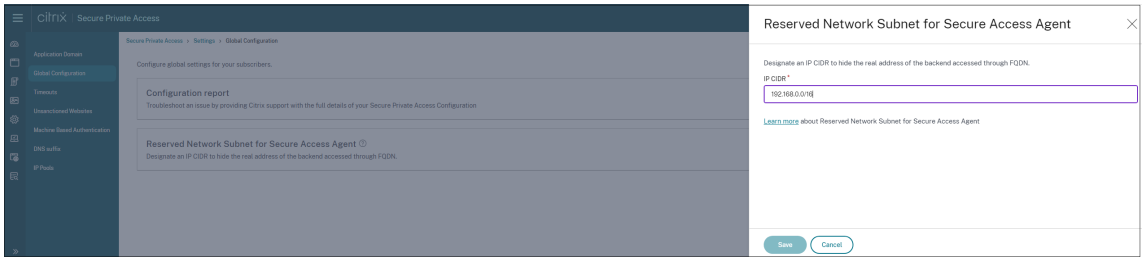
許可されている予約済み CIDR IP アドレスの範囲は次のとおりです。

- 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。

		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
	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。 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。

		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」を使用して Workday にアクセスできます。
	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。	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「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。

	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
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。

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。

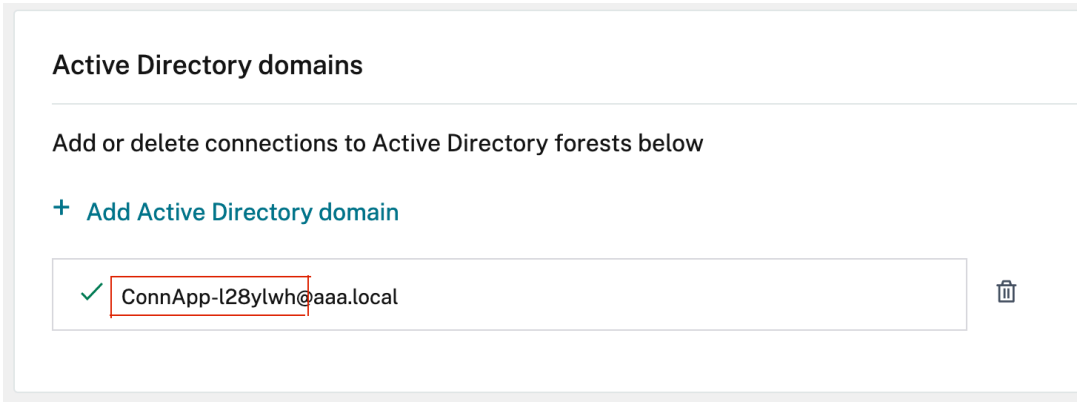
        管理ページに［**Active Directory** ドメイン］セクションがない場合は、Citrix に連絡してプレビューへの登録を依頼してください。

      - ［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。

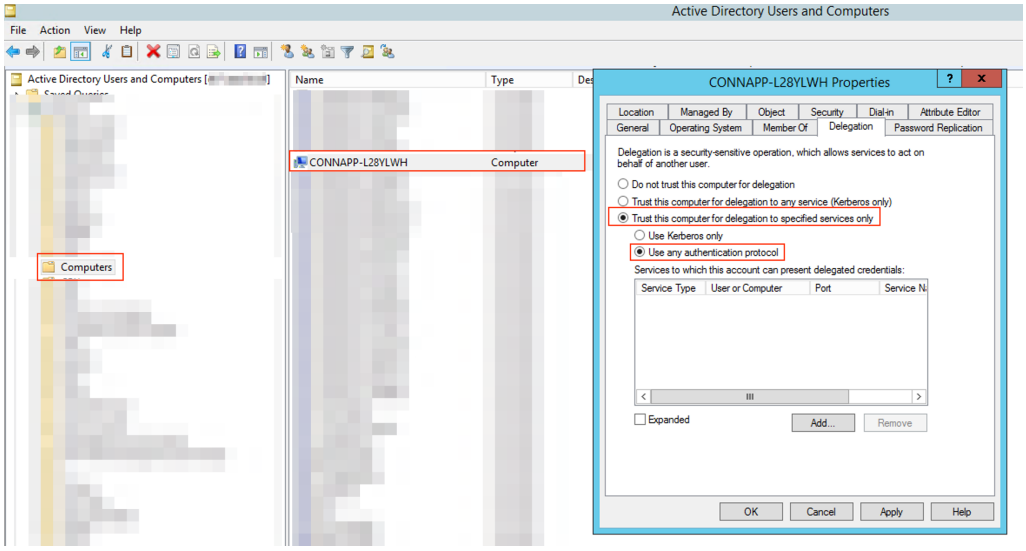
        このマシン名は、Connector Appliance が参加したときに Active Directory ドメインに作成されます。

      - ［参加］をクリックします。

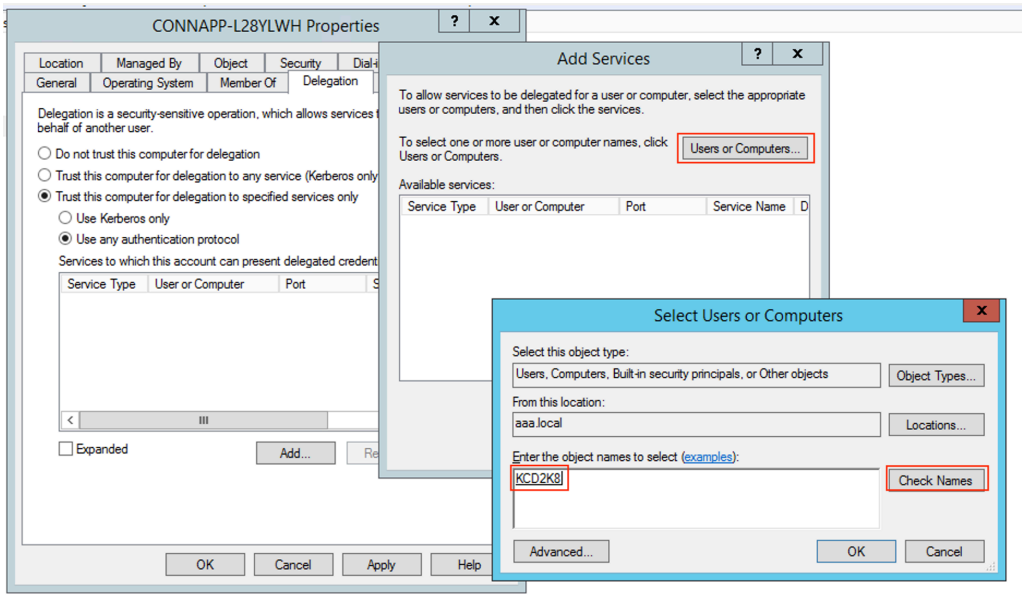
   b) ロードバランサを使用しない Web サーバの Kerberos 制約委任を設定します。



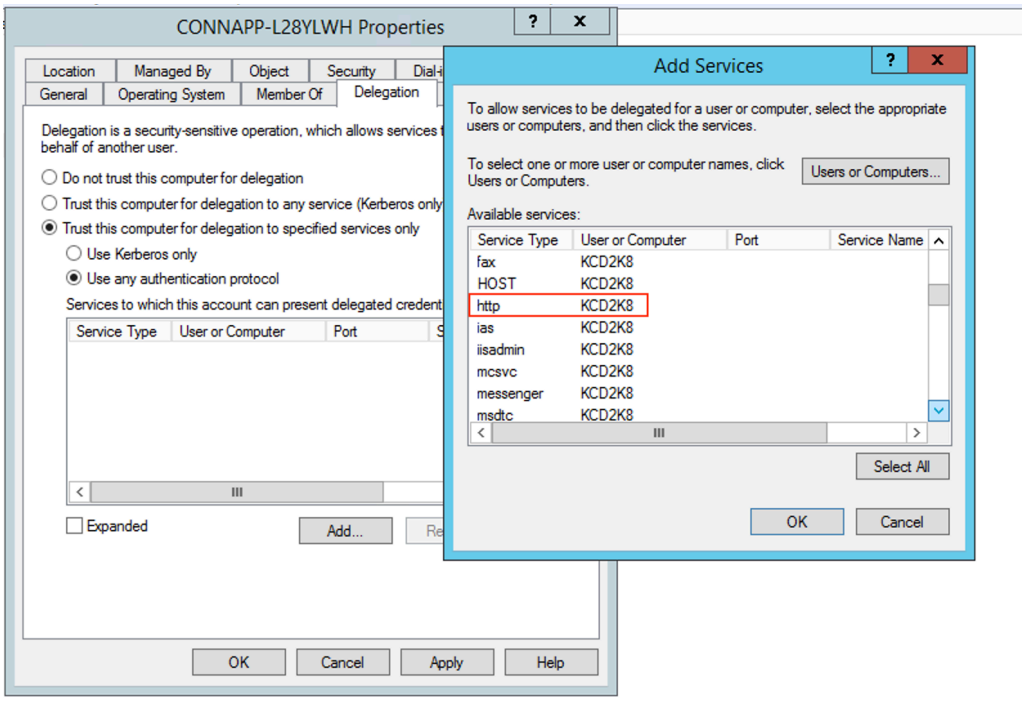
- Connector Appliance のコンピュータ名を識別します。この名前は、ホストした場所、または単にコネクタ UI から取得できます。
- Active Directory コントローラで、Connector Appliance コンピュータを探します。
- Connector Appliance コンピュータアカウントのプロパティに移動し、[委任] タブに移動します。
- [指定したサービスへの委任のみにコンピュータを信頼する] を選択します。次に、[任意の認証プロトコルを使用する] を選択します。



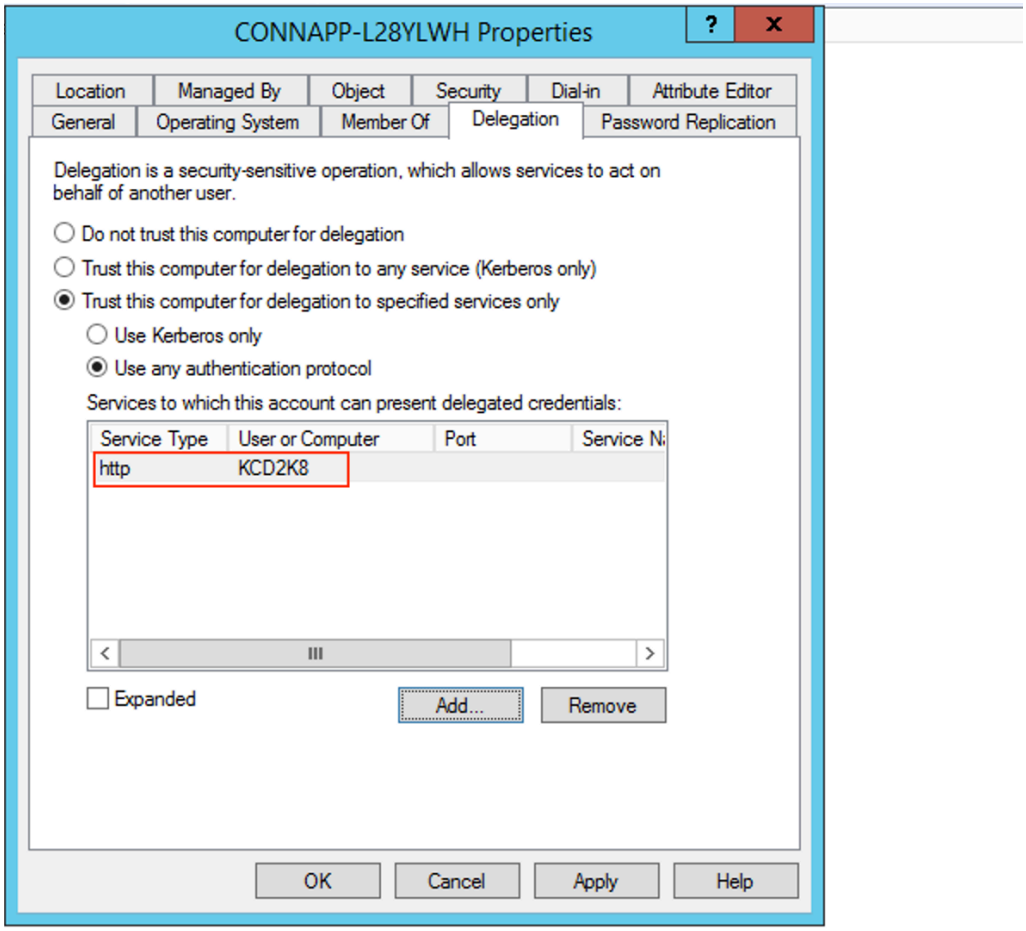
- 「追加」をクリックします。
- [ユーザー] または [コンピュータ] をクリックします
- ターゲット Web サーバーのコンピューター名を入力し、[名前の確認] をクリックします。上の画像では、**KCD2K8** が Web サーバーです。



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



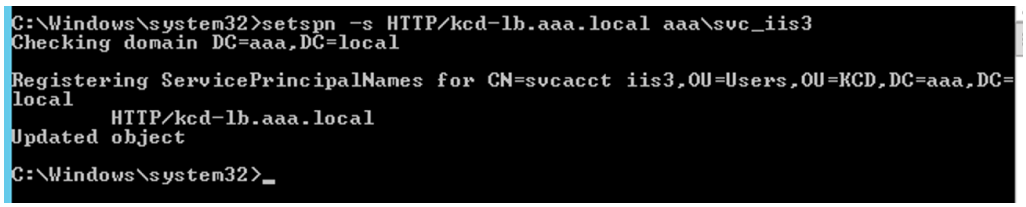
- [**OK**] をクリックします。
- 「適用」をクリックし、「**OK**」をクリックします。



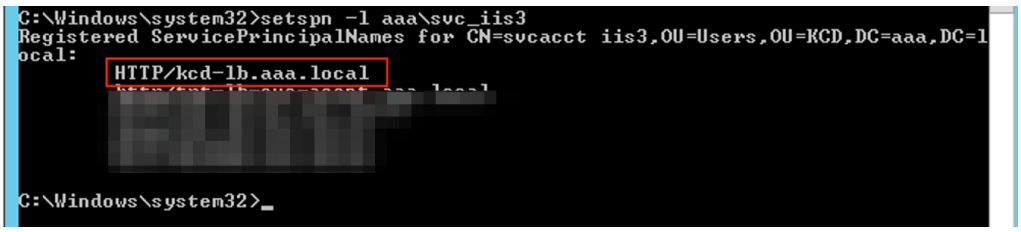
これで、Web サーバーの委任を追加する手順は完了です。

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。

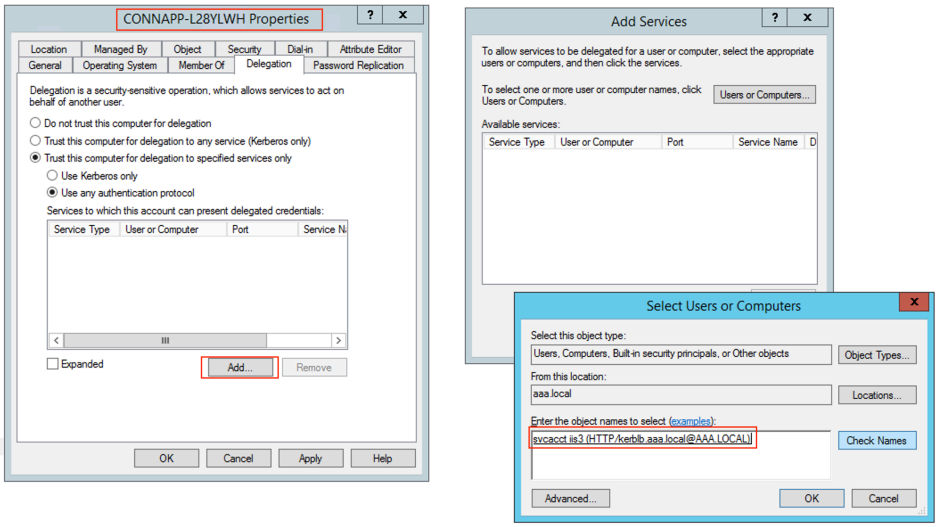
- `setspn`コマンドを使用して、ロードバランサー SPN をサービスアカウントに追加します。
  `setspn -S HTTP/<web_server_fqdn> <service_account>`



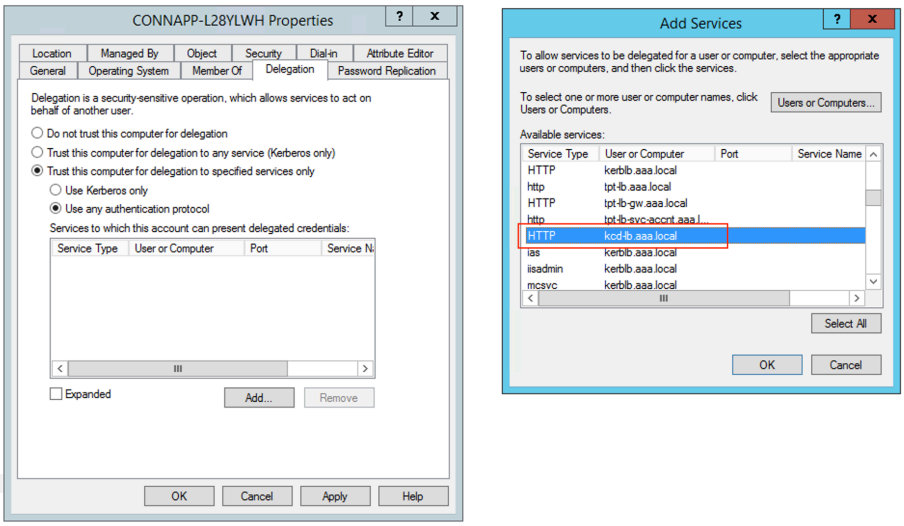
- 次のコマンドを使用して、サービスアカウントの SPN を確認します。
  `setspn -l <service_account>`



- 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。

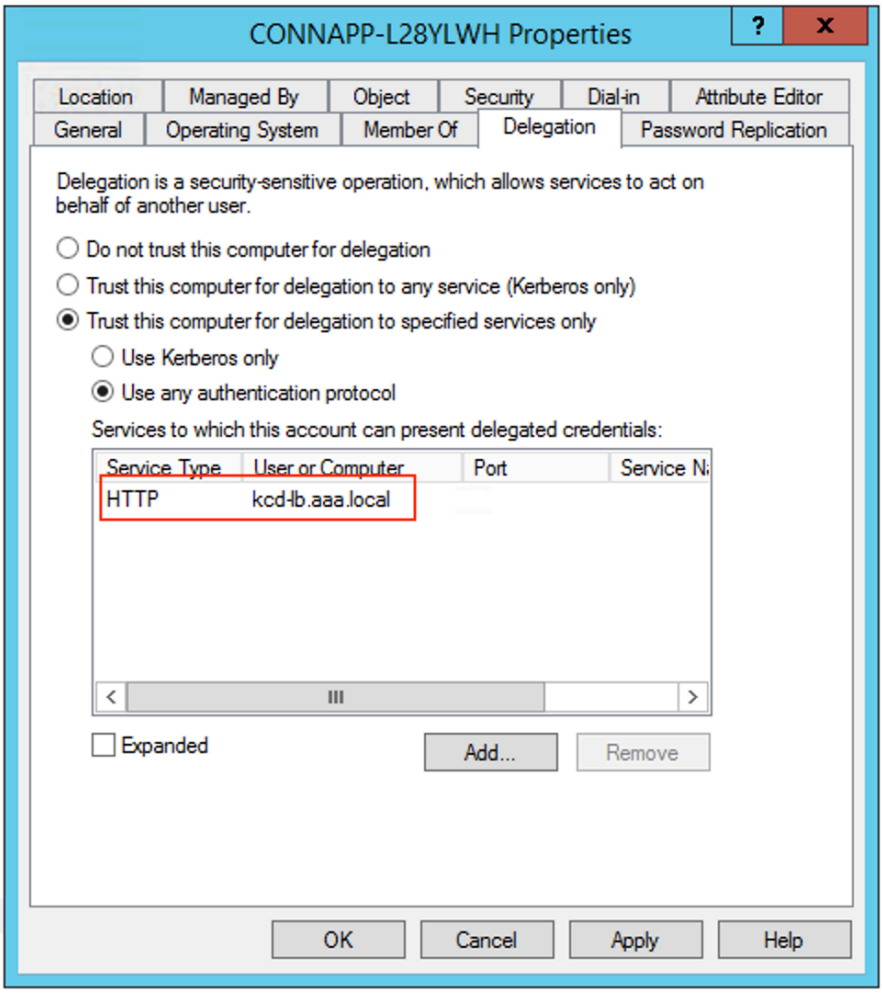


  - サービスで、**ServiceType: HTTP** とユーザーまたはコンピューター:Web サーバー (例: `kcd-lb.aaa.local`)



。

  - [**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。

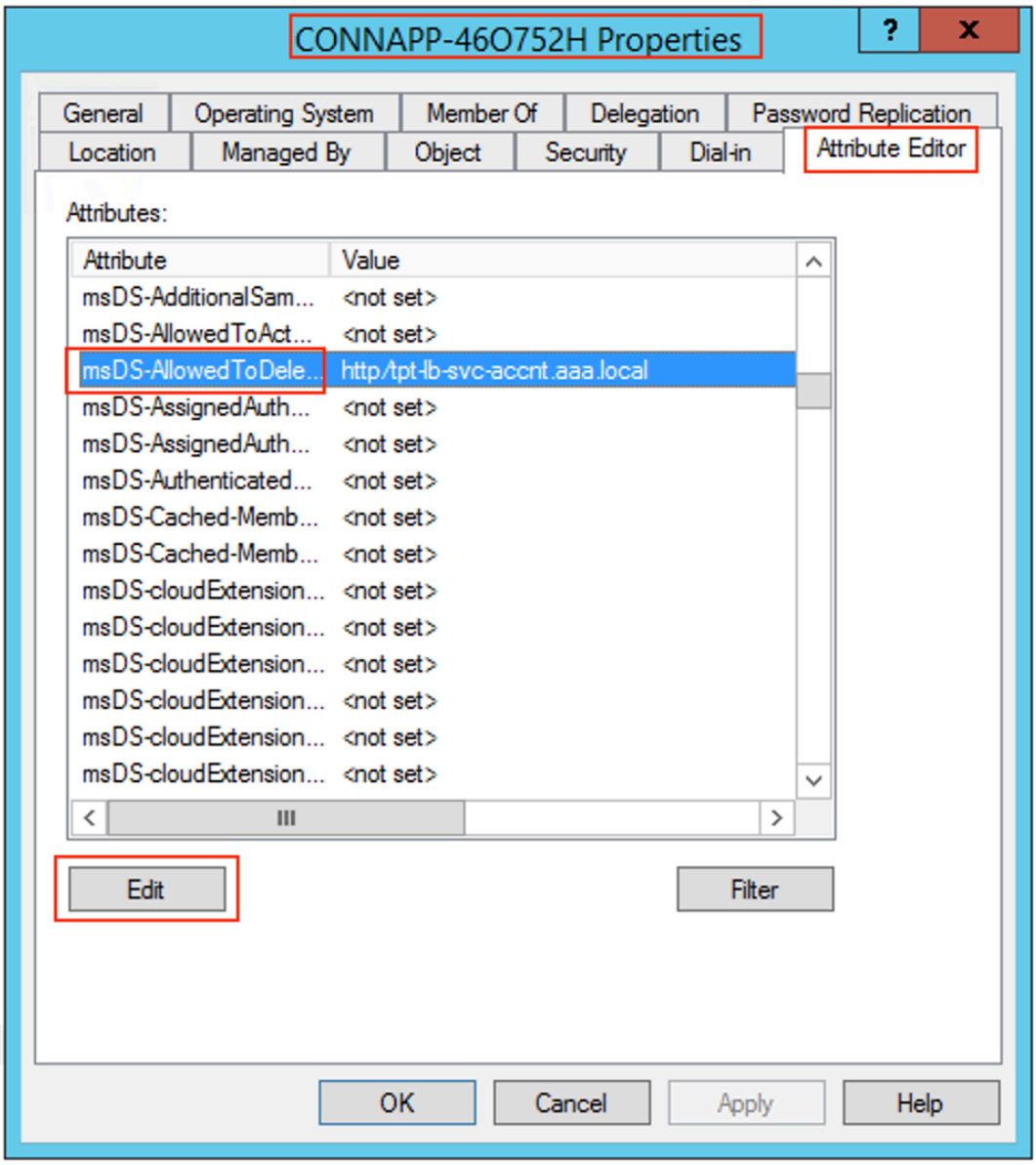


d) グループ管理サービスアカウントの Kerberos 制約付き委任 (KCD) を構成します。

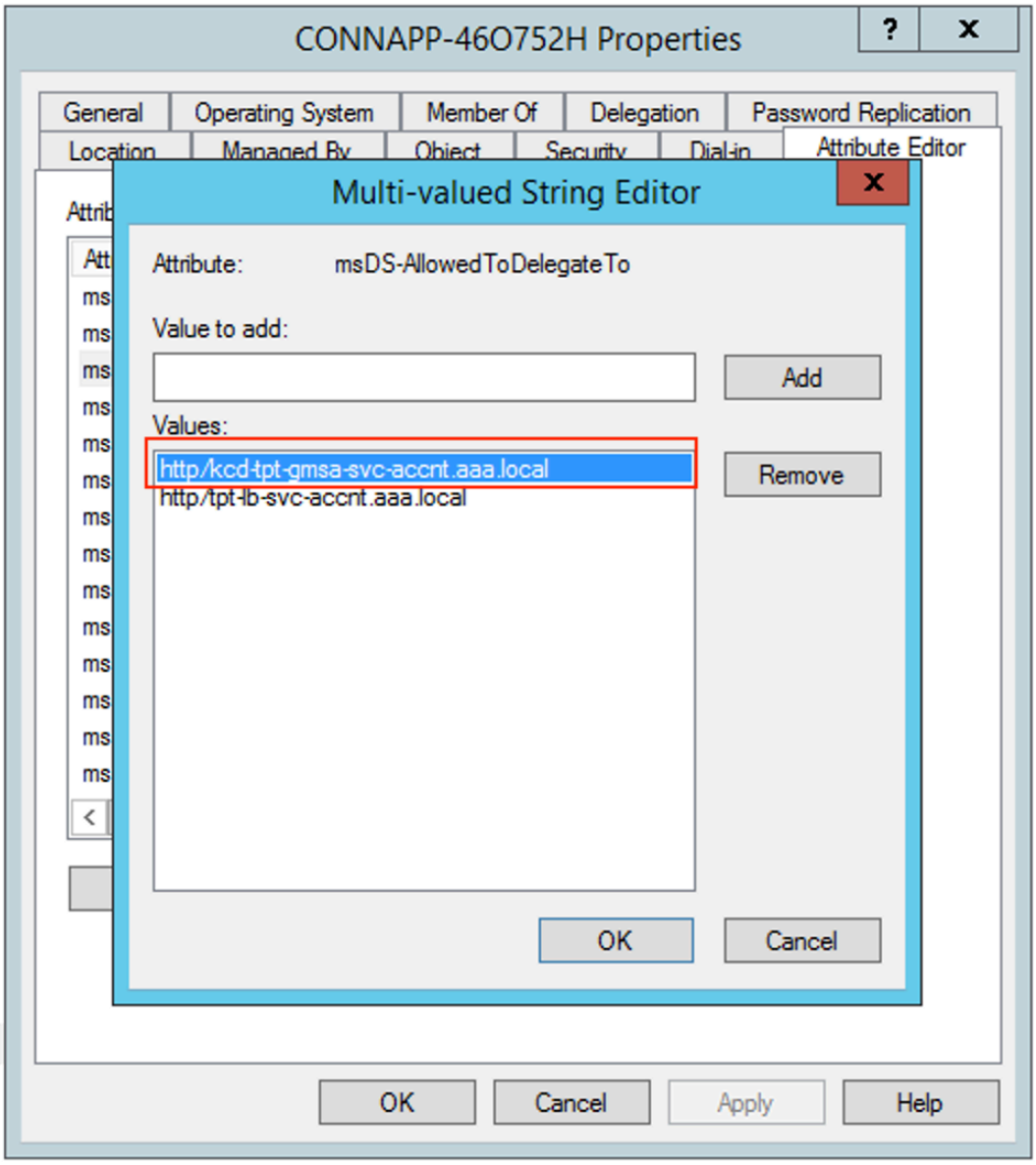
- まだ行っていない場合は、SPN をグループ管理サービスアカウントに追加します。
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- 以下のコマンドで SPN を確認します。
  `setspn -l <group_manged_service_account>`

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。



)

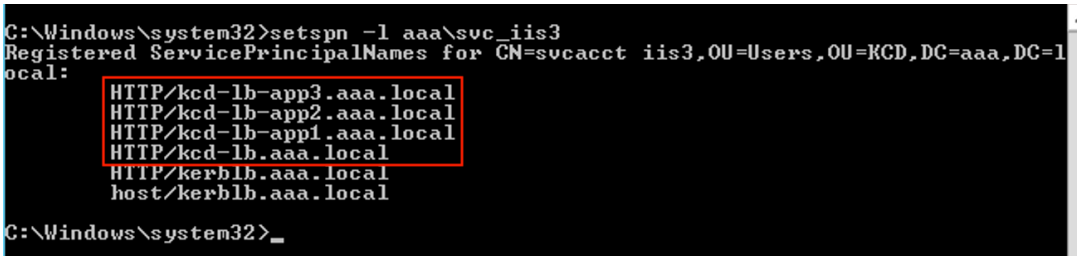


)

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

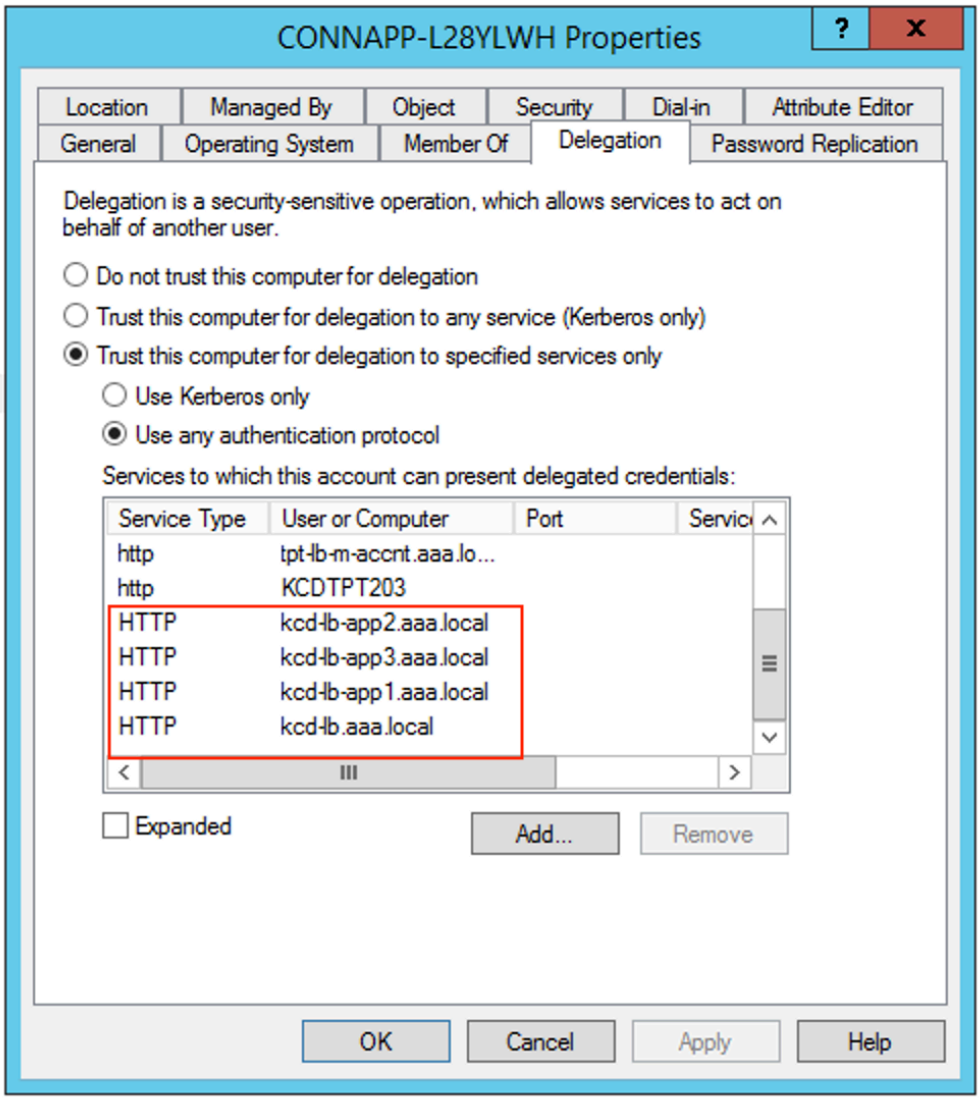
- SPNs はゲートウェイコネクタの構成時にサービスアカウントにすでに設定されているため、新しい kerberos アプリが構成されていない場合は、サービスアカウントに SPN を追加する必要はありません。次のコマンドを実行して、サービスアカウントに割り当てられているすべての SPN の一覧を表示し、それらを CA コンピューターアカウントの委任されたエントリとして割り当てることができます。

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

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

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。

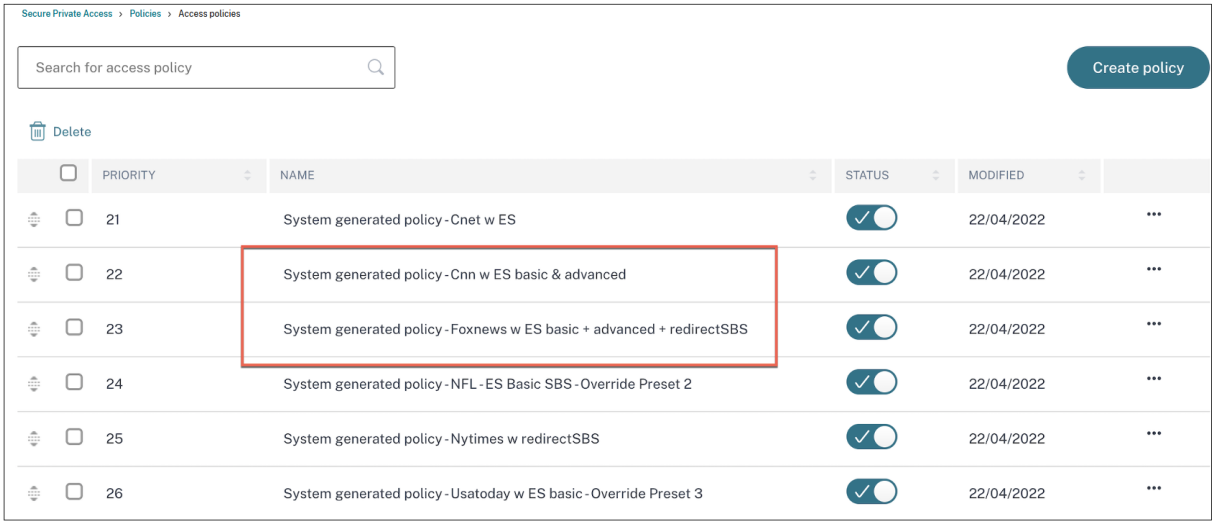
- 新しいポリシーが作成されました
- 1 つのポリシーが複数のポリシーに分割される
- プレフィックス<System generated policy - App name>が付いたポリシー名

> 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。

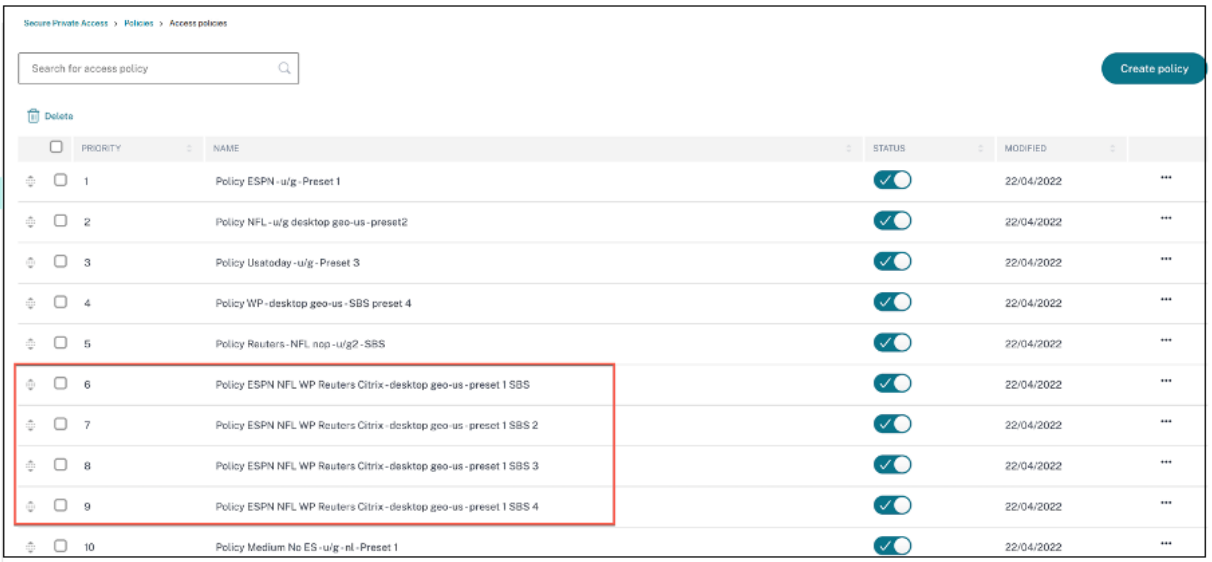
次の表に、変更の概要を示します。

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。



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

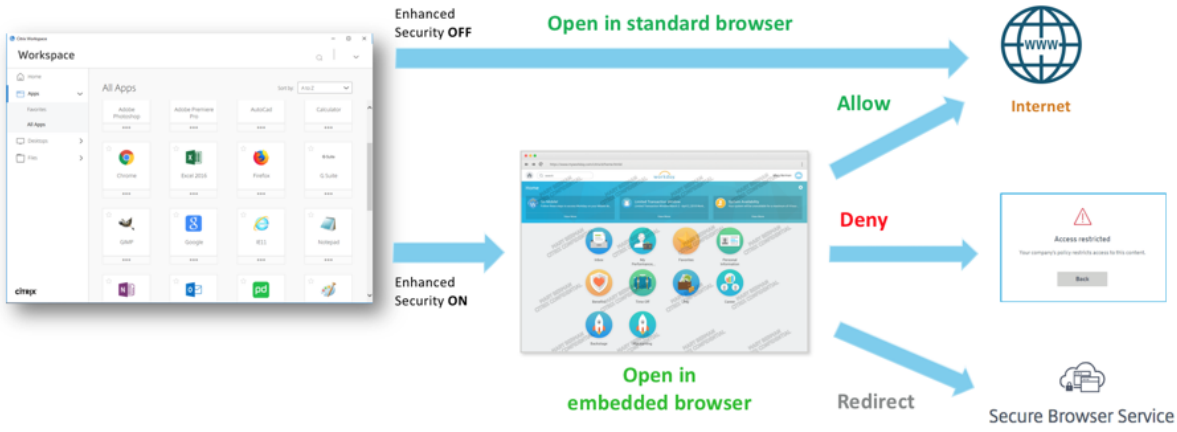
エンドユーザーは、次の操作を行う必要があります:

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。

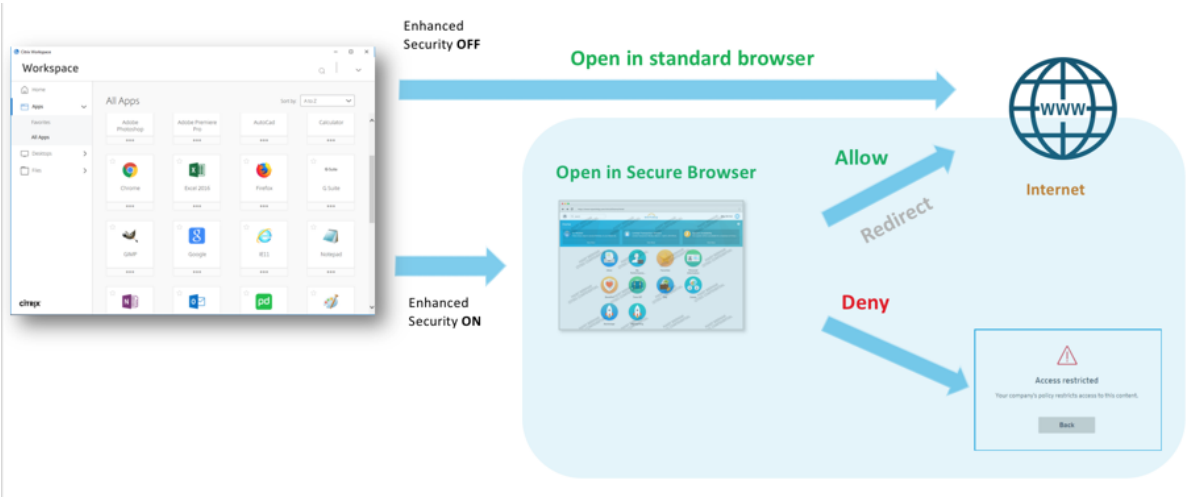
Citrix Workspace アプリ内または Citrix Workspace Web ポータルから SaaS アプリを使用できるようになりました。

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。



エンドユーザーがアクセスしたドメインまたは IP アドレスを検出する

October 21, 2024

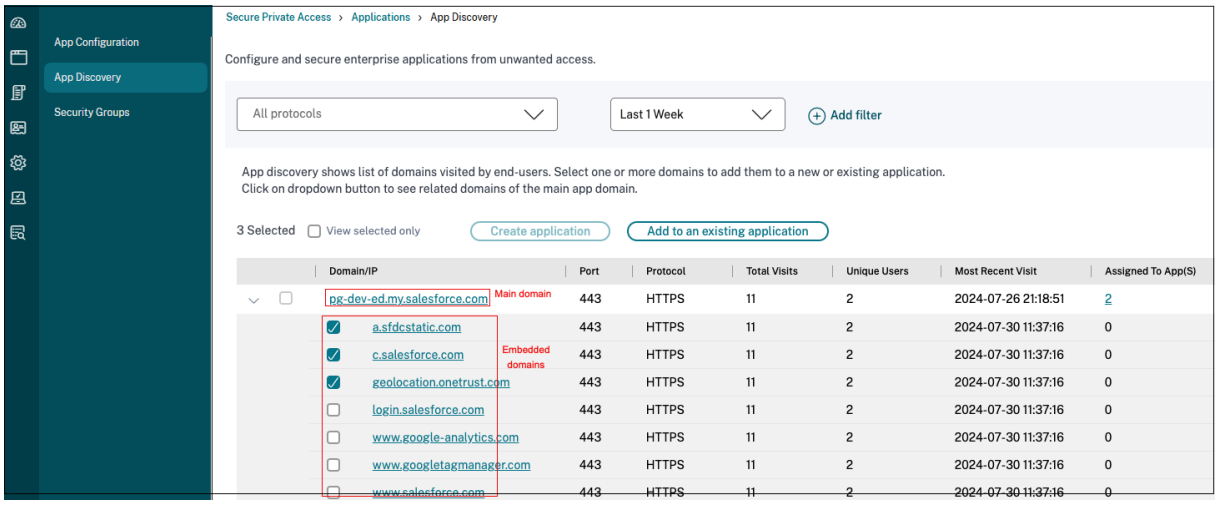
アプリケーション検出機能を使用すると、管理者は組織内でアクセスされている外部および内部アプリケーション (HTTP/HTTPS および TCP/UDP アプリ) を可視化できます。この機能は、公開されているか未公開であるかにかかわらず、すべてのドメイン/IP アドレスを検出して一覧表示します。したがって、管理者はどのドメイン/IP アドレス

が誰によってアクセスされているかを確認し、それらをアプリケーションとして公開してそれらのユーザーにアクセスを提供するかどうかを決定できます。

アプリケーション検出機能は、管理者に次の機能を提供します。

- エンドユーザーがアクセスする内部または外部のドメイン/IP アドレスの両方に対する可視性を提供します。
- アクセスされるすべてのタイプのアプリケーション (HTTP、HTTPS、TCP、UDP) に対する包括的な可視性を提供します。すべてのアクセス方法、つまり Citrix Enterprise Browser、Secure Access Agent、Direct Access、または Workspace for Web 経由のアクセスがサポートされています。
- エンドユーザーがアクセスした公開済みまたは未公開のドメイン/IP アドレスの両方を表示します。
- Citrix Enterprise Browser 経由でアクセスするアプリケーションを公開する際に関連ドメインとして構成する必要があるメイン ドメインとその基盤となる埋め込みドメインの両方を表示します。
- 埋め込まれたドメインをツリー構造で表示します。管理者は、メイン ドメインに沿って展開記号 (**>**) をクリックして、埋め込まれたドメインを表示できます。
- メイン ドメインまたは埋め込みドメイン (HTTP/HTTPS) または宛先 IP アドレス (TCP/UDP) がアプリケーションに関連付けられていない場合、管理者は新しいアプリケーションを作成したり、既存のアプリケーションにそれらのドメインを追加したりできます。

次の図は、アプリ検出 ページのサンプルを示しています。アプリ検出 ページでは、プロトコル (HTTP/HTTPS、TCP/UDP) およびドメイン/IP アドレスとポート番号に基づいてドメインをフィルタリングできます。また、エンドユーザーがアクセスした未公開の（どのアプリにも割り当てられていない）ドメインも表示されます。メイン ドメインとその下に埋め込まれたドメインのドロップダウン リストが表示されます。これらのドメインは、アプリケーションを公開するときに関連ドメインとして構成する必要があります。



> 注意:
>
> - 埋め込みドメインは、Citrix Enterprise Browser 経由でアクセスされる HTTP/HTTPS アプリの場合のみ、メイン ドメインの下にグループ化されます。TCP/UDP ドメインは 1 つのメイン ドメインにグループ化されません。
> - 埋め込みドメインのグループ化は、Citrix Enterprise Browser (v119 以降) からアクセスされるアプリ

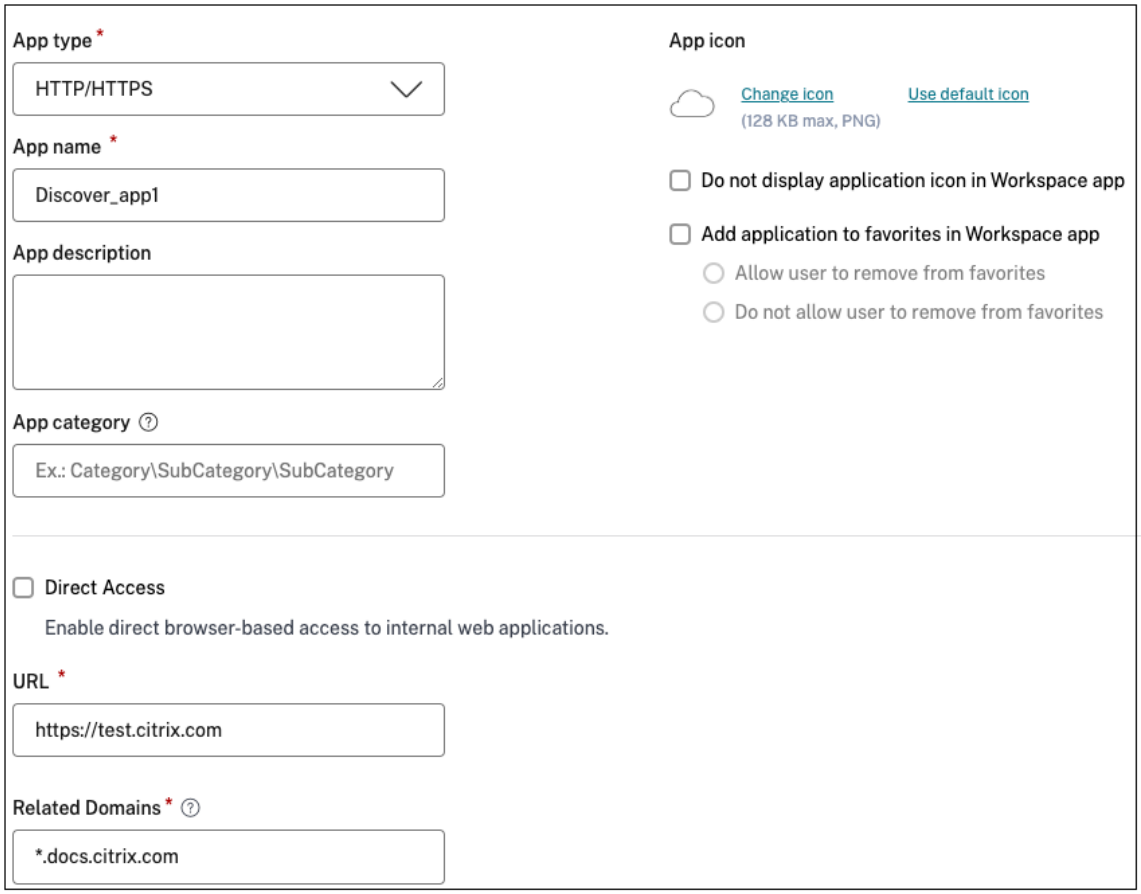
> でのみ使用できます。

新しい環境における内部ドメインのアプリケーション検出

新しいセキュア プライベート アクセス環境をセットアップし、構成するアプリケーションを可視化する必要がある場合は、アプリケーション検出機能を使用できます。この機能は、エンドユーザーがアクセスするすべてのドメイン/IP アドレスを検出して一覧表示し、アプリケーションとして構成できるようにします。Secure Private Access 環境を設定するときに、アプリケーション検出機能を有効にするには、次の手順に従います。

- 内部 Web アプリケーションを検出するには、Secure Private Access 内でアプリケーションを構成し、検出するアプリケーションのドメイン/サブドメインに属するワイルドカード関連のドメインを指定します。

  たとえば、ドメイン citrix.com を持つすべてのアプリケーションを検出する場合は、関連するワイルドカード ドメインを `*.citrix.com`としてアプリケーションを作成します。アプリケーション構成を完了できるようにするには、メインの Web アプリ URL セクションとして任意のテスト URL を追加します。



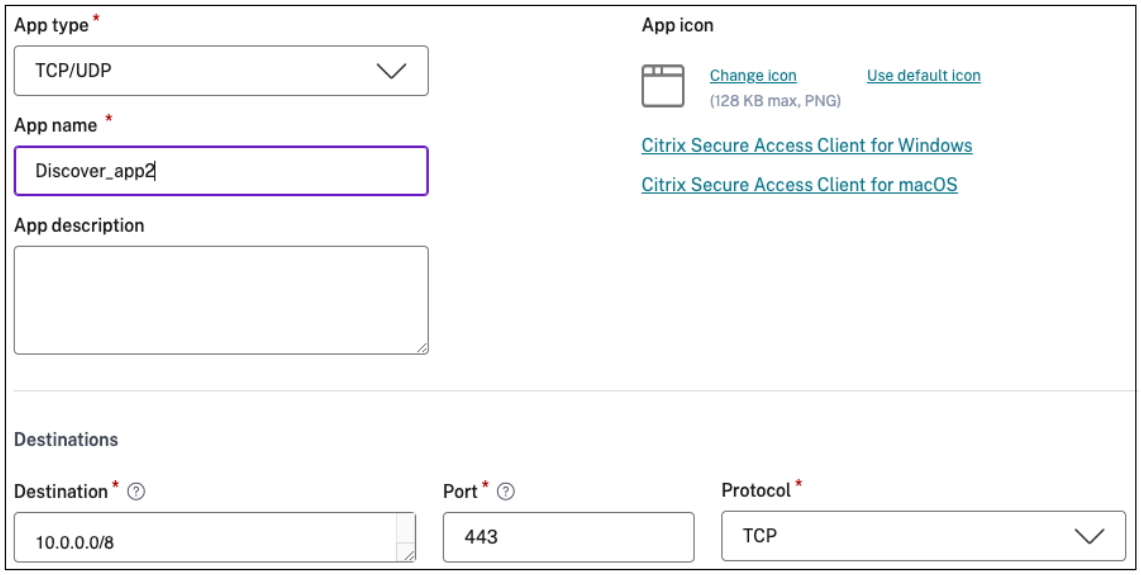
  Web アプリの URL: `https://test.citrix.com/` 関連ドメイン: `*.citrix.com`

- 内部 TCP/UDP アプリの場合は、Secure Private Access 内でアプリケーションを構成し、TCP/UDP プロトコルとポートの範囲とともにサブネットを指定します (範囲全体を含めるには、* と入力します)。これにより、Citrix Secure Access エージェントからすべての TCP および UDP アプリを検出できるようになります。

たとえば、サブネット 10.0.0.0/8 内のすべてのアプリケーションを検出する場合は、次の詳細を使用してアプリを構成します。例: 10.0.0.0/8:

ポート: (*)

プロトコル:TCP



- アプリケーションを作成したら、構成されたドメインと 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。アクセス ポリシーを作成し、作成されたアプリケーションで構成された FQDN/IP アドレスへのアクセスを許可するユーザーを割り当てます。これらは、テスト ユーザーの初期セット、または最初にアクセス権を付与する限られた数のユーザーになります。
- 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、ユーザーは 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引き続きアクセスできます。エンドユーザーがアクセスしたすべての FQDN/IP アドレスが、アプリケーション検出ページに表示されるようになります。

> 注意:
>
> - 数日/数週間かけてほとんどのアプリケーションを検出して特定したら、最初に作成したアプリケーションを削除して、ワイルドカード ドメインと IP サブネット経由で提供される広範なアクセスを閉鎖し、検出された特定のアプリケーション URL と IP アドレスのみに新しいアプリケーション経由でのアクセスを許可することをお勧めします。
> - アプリ名にプレフィックス `Discover` を追加して、これが検出監視とレポートを有効にする特別なアプリ構成であることを示します。この命名により、ワイルド カード ドメインまたは IP サブネット、あるいはその両方を削除する必要があることがわかり、数週間後または 1 か月後に、全体的なアプリ アクセス ゾーンを特定の FQDN と IP/ポートの組み合わせだけに縮小できるようになります。
> - TCP/UDP アプリにアクセスするには、ユーザーは Citrix Secure Access エージェント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構成に基づいて監視され、アプリ検出 ページ内で報告されます。

> - 検出されたアプリケーションを削除した後でも、この機能はユーザーがアクセスしたドメイン/IP アドレスの検出を継続します。したがって、いつでも **App Discovery** ページに戻って、アクセスされている内容や、アプリケーションとして構成する必要がある新しいドメイン/IP アドレスが検出されたかどうかを確認できます。

ドメイン、FQDN、または IP アドレスの追加の詳細については、次のトピックを参照してください。

- エンタープライズウェブアプリのサポート
- サービスとしてのソフトウェア アプリのサポート
- クライアントサーバーアプリのサポート

アプリ検出ページからアプリケーションを作成する

アプリ検出 ページから埋め込みドメインまたは未公開ドメインのアプリケーションを作成するには、次の手順を実行します。

1. アプリケーション **>** アプリの検出に移動します。
2. リストからドメインを選択します。ドメインに埋め込みドメインがある場合は、メインドメインに沿って展開記号 (**>**) をクリックし、埋め込みドメインを選択します。

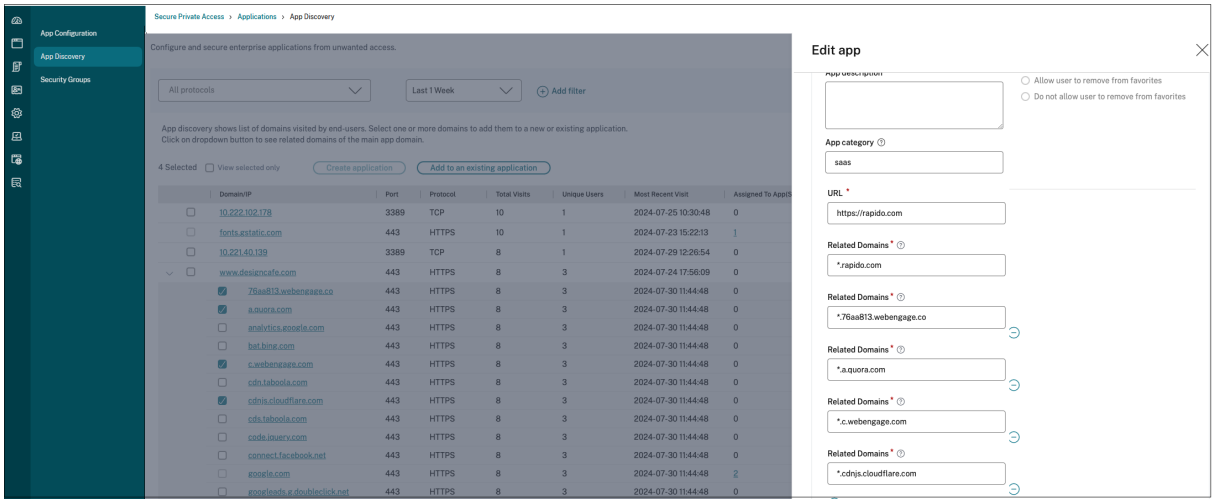
> 注意**:**
>
> - 異なるプロトコルに属するドメインを選択してアプリケーションを作成することはできません。異なるプロトコルに属するドメインを選択すると、エラー メッセージが表示されます。
> - ドメインがすでにアプリケーションに関連付けられている場合は、そのドメインを再度選択してアプリケーションを作成することはできません。そのドメインに対応するチェックボックスはグレー表示され、チェックボックスの上にマウスを置くとツールヒントが表示されます。
> - 異なるメイン ドメインの下にグループ化された埋め込みドメインを選択してアプリケーションに追加することはできません。アプリケーション検出機能では、単一のメイン ドメインの下にグループ化された埋め込みドメインのみをアプリに追加できます。異なるメイン ドメインからの埋め込みドメインを選択して同じアプリに追加すると、エラー メッセージが表示されます。

1. アプリケーションの作成をクリックします。アプリケーション作成の詳細については、「エンタープライズ Web アプリのサポート」、「Software as a Service アプリのサポート」、および「クライアント サーバー アプリのサポート」(/en-us/citrix-secure-private-access/service/spa-support-for-client-server-apps) を参照してください。

既存のアプリケーションを更新する

既存のアプリケーションにドメインを追加するには、リストからドメインを選択します。ドメインに埋め込みドメインがある場合は、メインドメインに沿って展開記号 (**>**) をクリックし、埋め込みドメインを選択します。

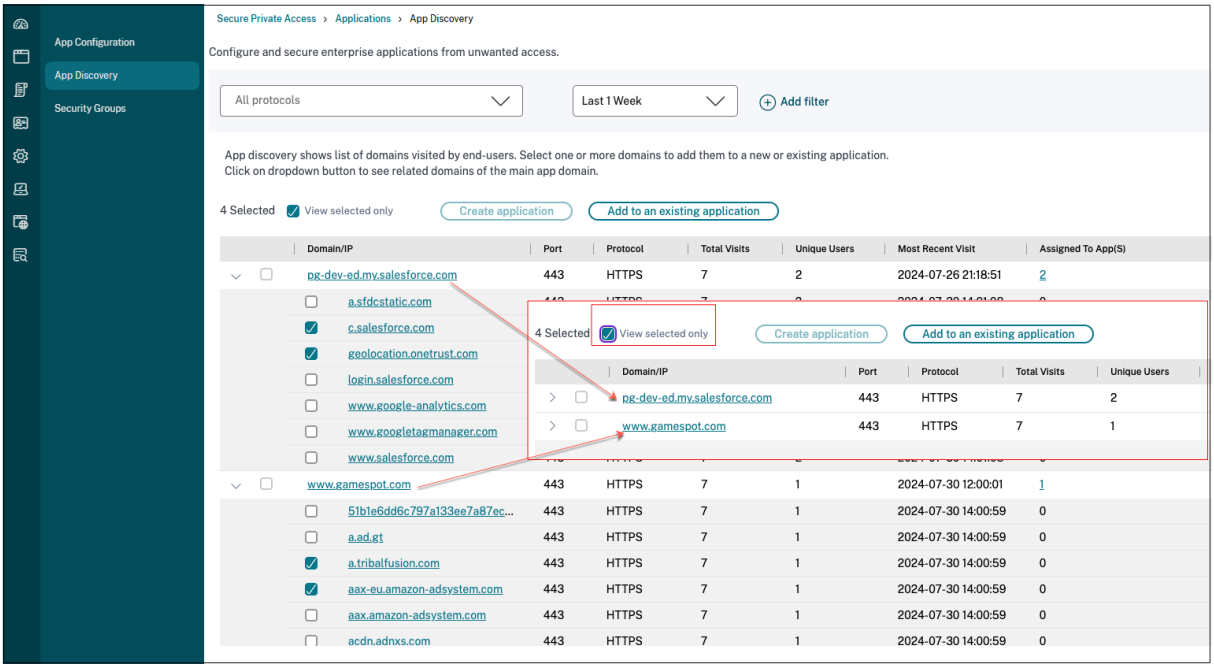
1. アプリケーションに追加する必要がある埋め込みドメインを選択します。
2. 既存のアプリケーションに追加をクリックします。
3. アプリケーションで、これらのドメインを追加するアプリケーションを選択します。
4. アプリの詳細を取得をクリックします。
5. 関連ドメイン フィールドには、先ほど選択したすべての埋め込みドメインが別々の行に表示されます。
6. [完了] をクリックします。



> 注意:
>
> - 既存の TCP/UDP アプリケーションにのみ TCP/UDP 宛先 IP アドレスを追加できます。アプリケーション フィールドには、システムで構成されている TCP/UDP アプリケーションのみがリストされます。
> - 既存の HTTP/HTTPS または TCP/UDP アプリを選択して、プロトコルが HTTP/HTTPS であるドメイン (メイン、単一エントリ、または埋め込み) を追加できます。
> - すでにアプリケーションに関連付けられているドメインを選択することはできません。

選択した埋め込みドメインをすべて表示

ドメインを選択したら、[選択したドメインのみを表示] チェックボックスをクリックして、アプリケーションの作成または更新を続行できます。また、アプリ検出ページの FQDN/IP アドレスのリストが複数のページにまたがる場合は、[選択したもののみを表示] チェックボックスを使用して、アプリケーションの作成または更新のために選択したすべてのメイン ドメインと埋め込みドメインを表示できます。このチェックボックスをオンにすると、選択した埋め込みドメインのすべてのメインドメインが表示されます。



既知の制限事項

- アプリケーションの作成 および 既存のアプリケーションへの追加 オプションは Secure Private Access ダッシュボード (合計訪問数による上位の検出されたアプリケーション グラフ) で使用できますが、アプリの検出 タブ (アプリケーション **>** アプリの検出) からアプリケーションを作成または更新することをお勧めします。これは、ダッシュボードからアプリケーションを追加または更新しているときに操作をキャンセルすると、ページが再読み込みされ、結果としてすべての設定がリセットされるためです。
- メイン ドメインに対して展開記号 (>) が表示されることがありますが、その特定の FQDN に対しては埋め込まれたドメインが取得されません。この問題は、次の場合に発生する可能性があります。
  - ユーザーのアクセス制限により、メイン Web ページの読み込み中にエラーが発生しました。
  - ウェブページの読み込みを妨げるエラーです。
  - Citrix Enterprise Browser によって埋め込みドメイン リソースがキャッシュされるため、埋め込みドメインがソースから取得されません。

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。

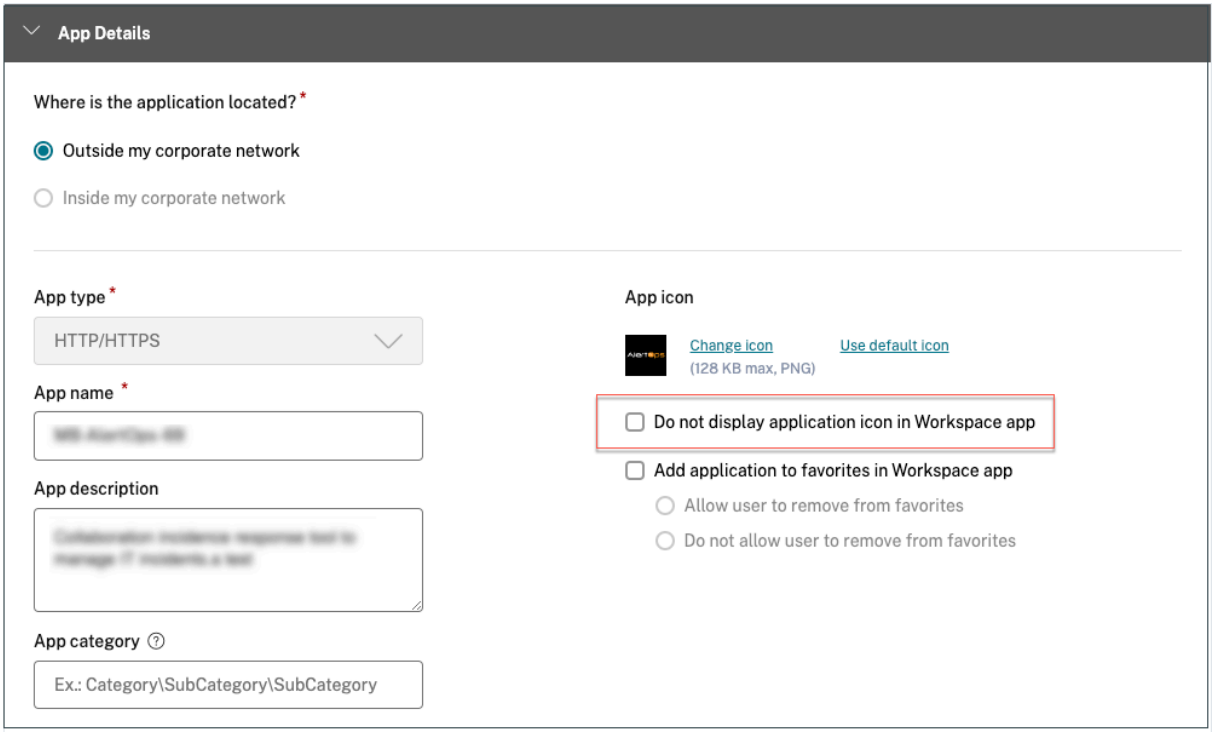
ただし、App1 に代わりに関連ドメインとして`*.intranet.local`がある場合、`app.intranet.local`が`PolicyB`に完全に一致することになるため、ユーザー`Eng-User5`にはアクセスできないため、`Eng-User5`へのアクセスは拒否されます。

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。

アクティブなユーザーセッションを終了し、ユーザーをユーザーブロックリストに追加する

October 21, 2024

管理者は、すべてのアクティブなエンドユーザー セッションを直ちに終了し、ユーザーをユーザー ブロック リストに追加できます。このユーザー ブロック リストにユーザーを追加すると、アクティブな Secure Private Access アプリケーション セッションがすべて終了し、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、直接アクセス、HTML5 用 CWA、および Secure Access エージェント経由のすべてのアクティブなアプリケーション セッションが終了し、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た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、ブロックされたユーザー 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。

> 注意:
>
> - ユーザー ブロック リストにユーザーを追加しても、構成された 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 ポリシーがどのような構成であっても、アクセスの終了とブロックが行われます。ユーザーがリストから削除されると、そのユーザーの既存の Secure Private Access アクセス ポリシーが復元されます。
> - 公開された 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 経由のインターネット アクセスは、Web フィルタリング構成に基づいて、ユーザーがブロック リストに追加された後でも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。状況が制御された後、ユーザーをユーザー ブロック リストから削除できます。
- ユーザーがアプリのアクセスを悪用します。この場合、ユーザーのアクセスは直ちに取り消されます。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。

ユーザーをユーザーブロックリストに追加する

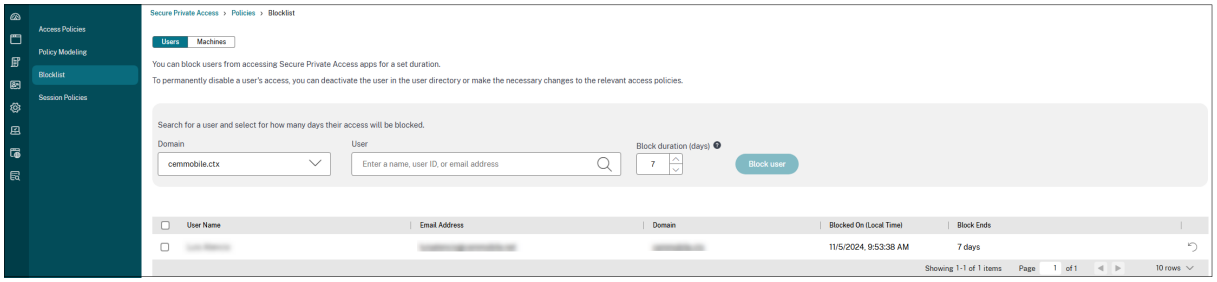
1. セキュア プライベート アクセス > アクセス ポリシー に移動し、ユーザー ブロックリスト タブをクリックします。
2. ドメインで、アクセスを無効にする必要があるドメインを選択します。
3. ユーザーで、ユーザー ブロック リストに追加する必要があるユーザー名を検索します。検索条件に一致するすべてのユーザー名が表示されます。ユーザーがディレクトリ サービスから削除されると、そのユーザー名はユーザー リストに表示されなくなります。
4. ブロック期間 (日数) に、このユーザーをブロックする必要がある日数を入力します。ユーザーをブロックリストに追加すると、デフォルトで 7 日間ブロックされます。ただし、期間は 1 日から 99 日までの間で変更できます。期間が終了すると、ユーザー ディレクトリとポリシー構成に基づいてユーザー アクセスが復元されま

す。また、この値は、将来の追加のためにユーザーに対して永続的に保持されます。たとえば、管理者がユーザーのブロック期間を 30 日に設定した場合、この設定は将来の追加時にもユーザーに対して保持されます。

5. ユーザーをブロックをクリックします。

   ユーザーはユーザー ブロック リストに追加されます。ユーザーがユーザー ブロック 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セキュア プライベート アクセス セッションは直ちに終了します。
   - 今後、すべての Secure Private Access 公開アプリケーションへのアクセスがブロックされます。
   - ユーザーがユーザー ブロック リストに追加された後でも、Citrix Enterprise Browser 経由のインターネット アクセスは許可されます。公開された 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。



ブロック期間が終了する前でも、次のいずれかの手順を実行することでアクセスを復元できます。

- アクセスを復元する必要があるアクセスを選択し、[アクセスの復元] をクリックします。
- アクセスを復元するユーザーの復元アイコンをクリックします。

どちらの場合も、確認ダイアログが表示されます。

> 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、ユーザー ブロック 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、今後のアプリへのアクセスがブロックされます。ユーザーが Workspace からログアウトすると、ディレクトリの資格情報が非アクティブになるため、再度ログインできなくなります。

ユーザーセッションのタイムアウト

January 9, 2024

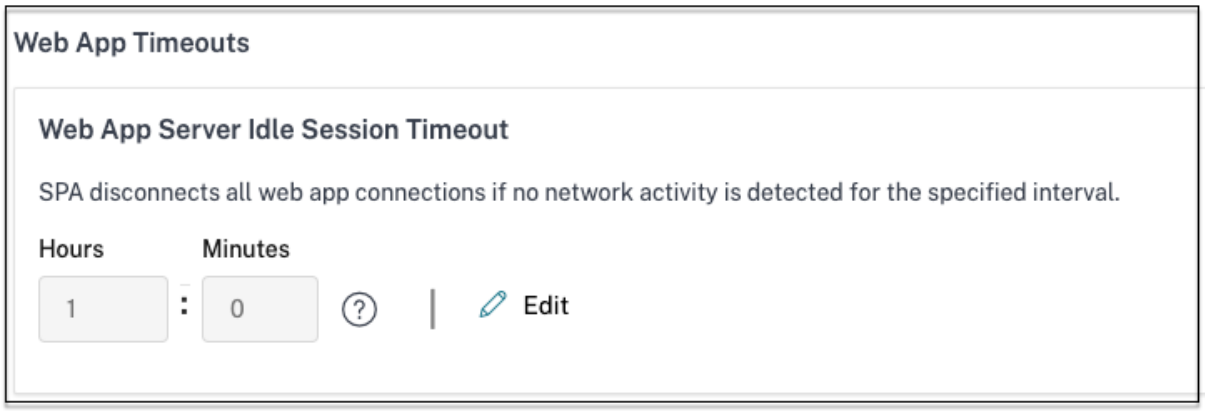
指定した期間にネットワークアクティビティがない場合に、Web アプリと Citrix Secure Access クライアントがユーザーセッションを終了するためのタイムアウト期間を設定できます。

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。

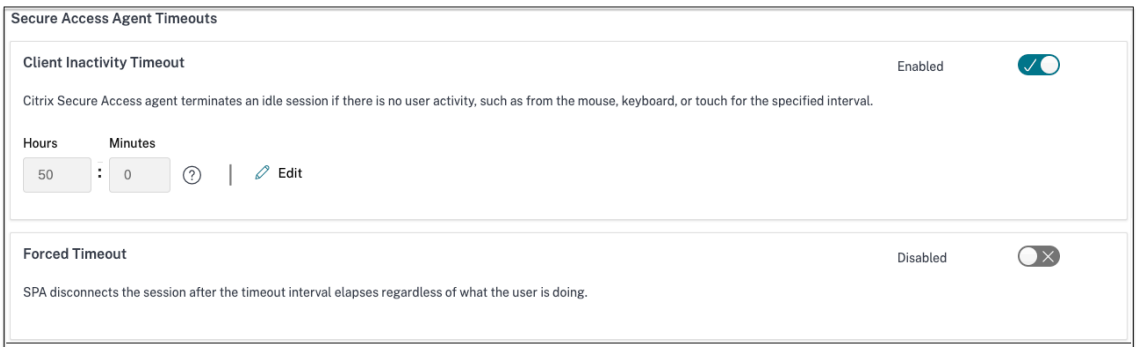


Citrix Secure Access クライアントのタイムアウト

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。

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。

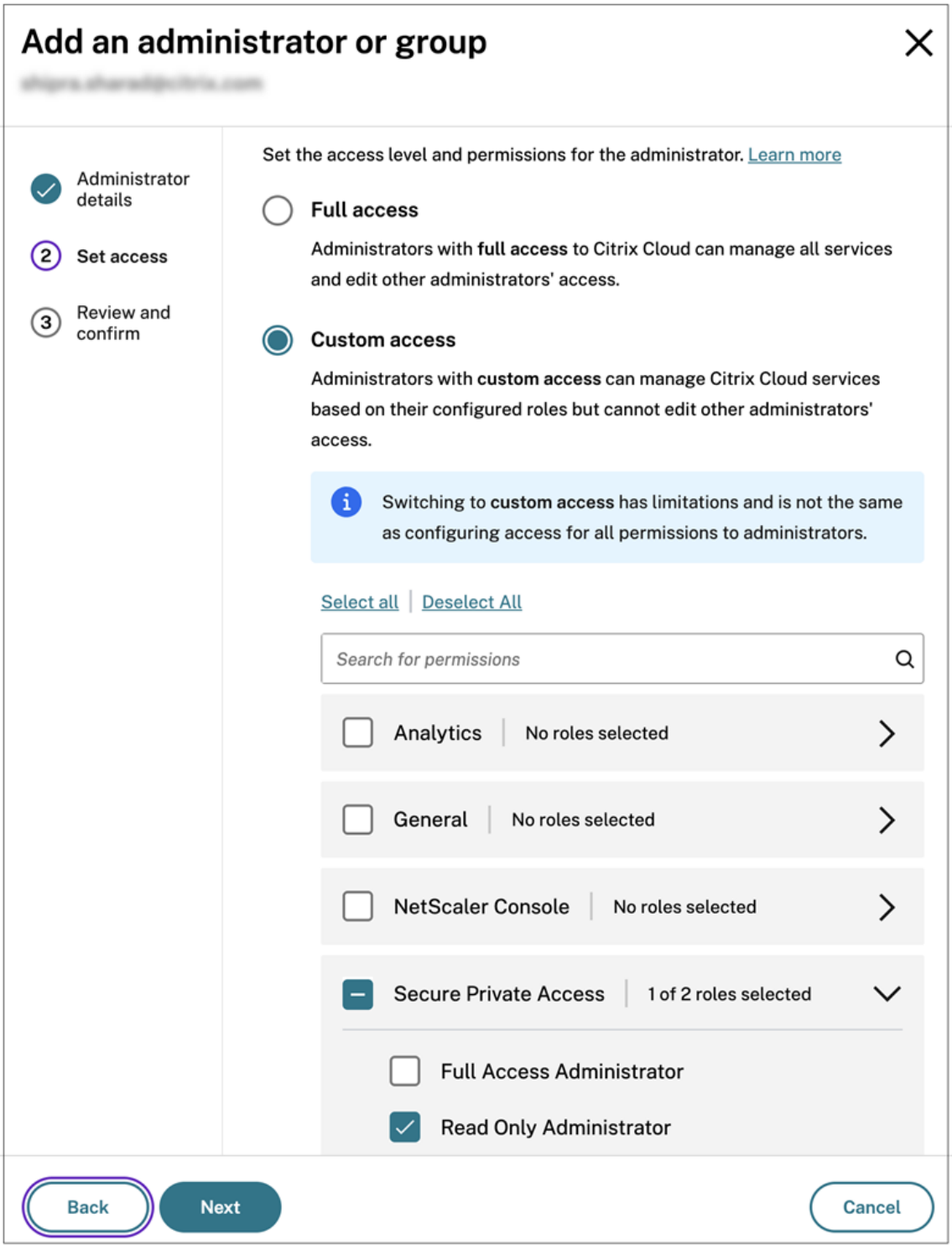
- エンタープライズ Web アプリまたは SaaS アプリを追加します。
- 既存または新規のリソースロケーションに新しいコネクタアプライアンスを追加します。

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。



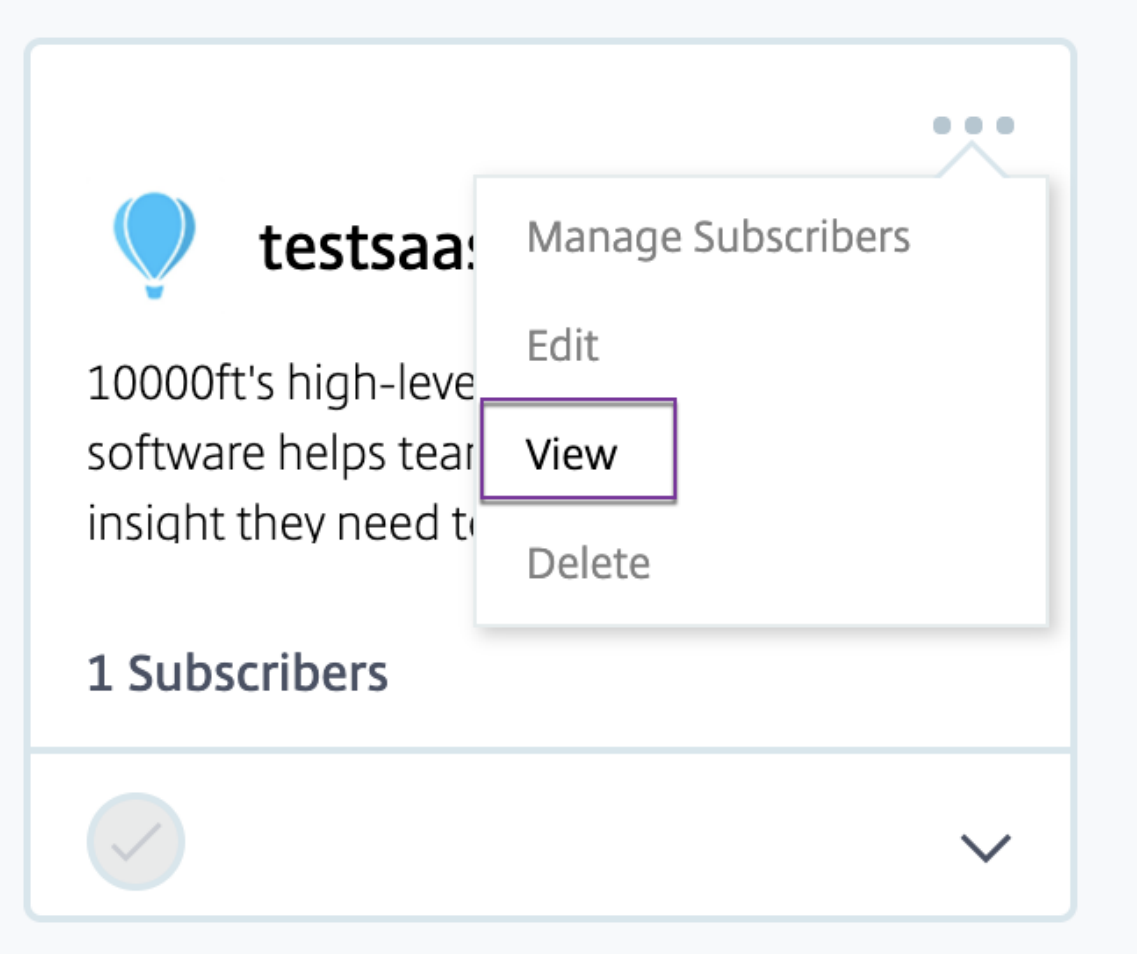
6. [招待を送信する] をクリックします。

> 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

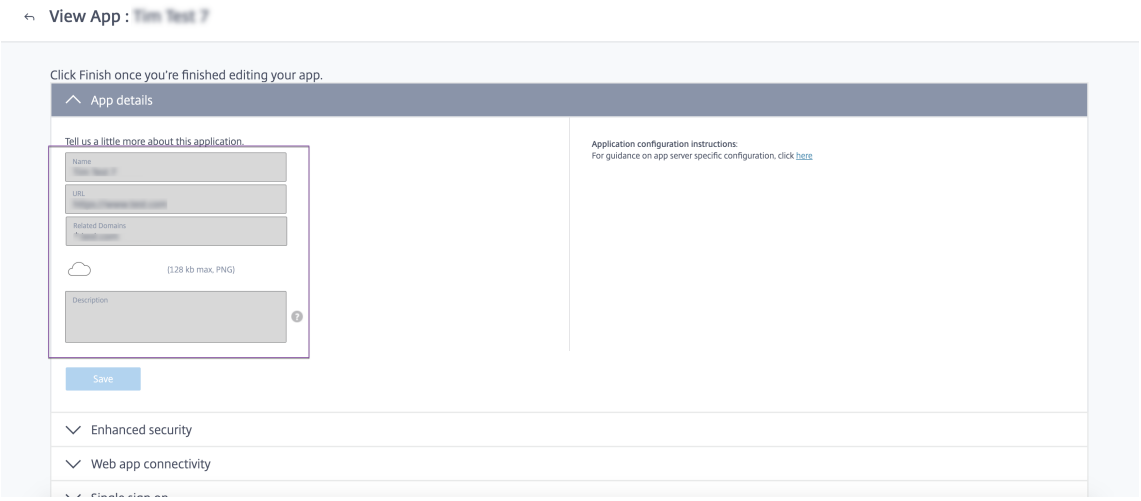
> ［全般管理］リストから［ライブラリ］を有効にする必要があります。管理者に対してのみ、アプリの [表示] オプションが有効になります。
> - 読み取り専用管理者アクセス権を持つユーザーの場合、**[Web/SaaS** アプリケーションの追加] ボタンは無効になります。

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。



ダッシュボードの概要

October 21, 2024

Secure Private Access サービスのダッシュボードには、SaaS、Web、TCP、UDP アプリの診断データと使用状況データが表示されます。ダッシュボードを使用すると、管理者はアプリ、ユーザー、コネクタの正常性状態、帯域幅の使用状況を 1 か所で完全に把握できます。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、事前に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については、ドリルダウンして詳細を表示できます。

メトリックは、大きく分けて次のカテゴリに分類されます。

- ログ記録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、アプリの列挙、デバイスの状態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) にアクセスした一意のユーザーの合計数。
  - アップロード: 選択した時間間隔で Secure Private Access サービスを通じてアップロードされたデータの合計量。
  - ダウンロード: 選択した時間間隔で Secure Private Access サービスを通じてダウンロードされたデータの合計量。
- アプリケーション:
  - アプリケーション: 現在構成されているアプリケーションの合計数 (時間間隔とは無関係)。

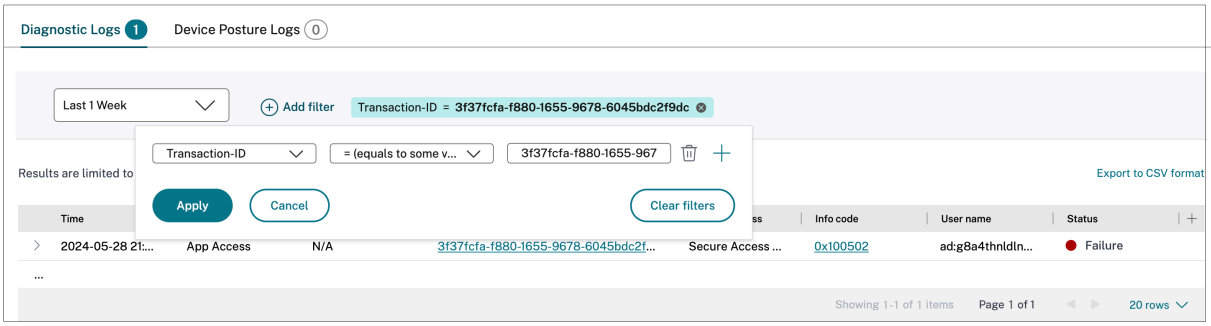
  - アプリケーションの起動数: 選択した時間間隔で各ユーザーが起動したアプリケーション (アプリ セッション) の合計数。
  - 構成されたドメイン: 選択した時間間隔に構成されたドメインの合計数。
  - 検出されたアプリケーション: アクセスされたが、どのアプリにも関連付けられていない固有の個別ドメインの合計数

- アクセスポリシー
  - アクセス ポリシー: 現在構成されているアクセス ポリシーの合計数 (時間間隔とは無関係)。

診断ログ

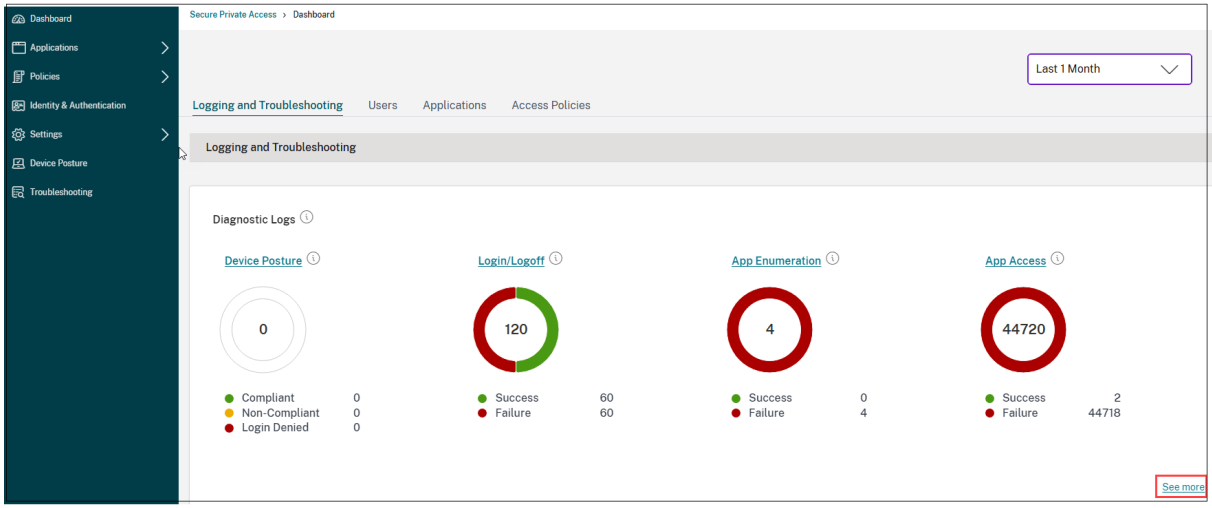
診断ログ チャートを使用して、認証、アプリケーションの起動、アプリの列挙に関連するログ、およびデバイスの状態に関連するログを表示します。ログの詳細を表示するには、「もっと見る」リンクをクリックします。詳細は表形式で表示されます。事前に設定した時間またはカスタム タイムラインのログを表示できます。ダッシュボードに表示する情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログを CSV 形式でエクスポートできます。

- フィルターの追加 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基準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、トランザクションID、= (ある値に等しい) を選択し、この順序で 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。

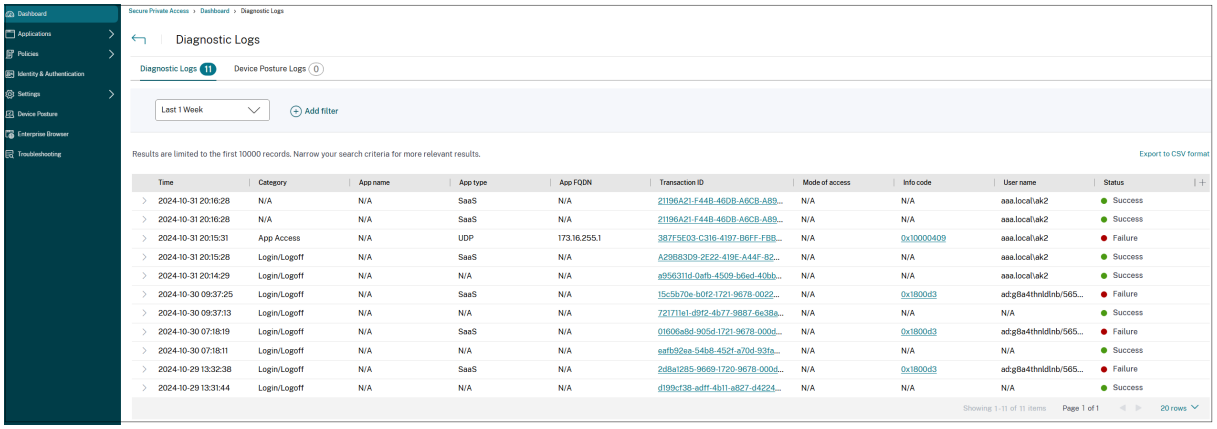


- デバイス ポスチャ ログ**:** ポリシー結果 (準拠、非準拠、ログイン拒否) に基づいて検索を絞り込むことができます。デバイスの姿勢の詳細については、「デバイスの姿勢」を参照してください。

> 注意**:**
>
> - 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、関連付けられた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、アクセス要求のすべての 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。



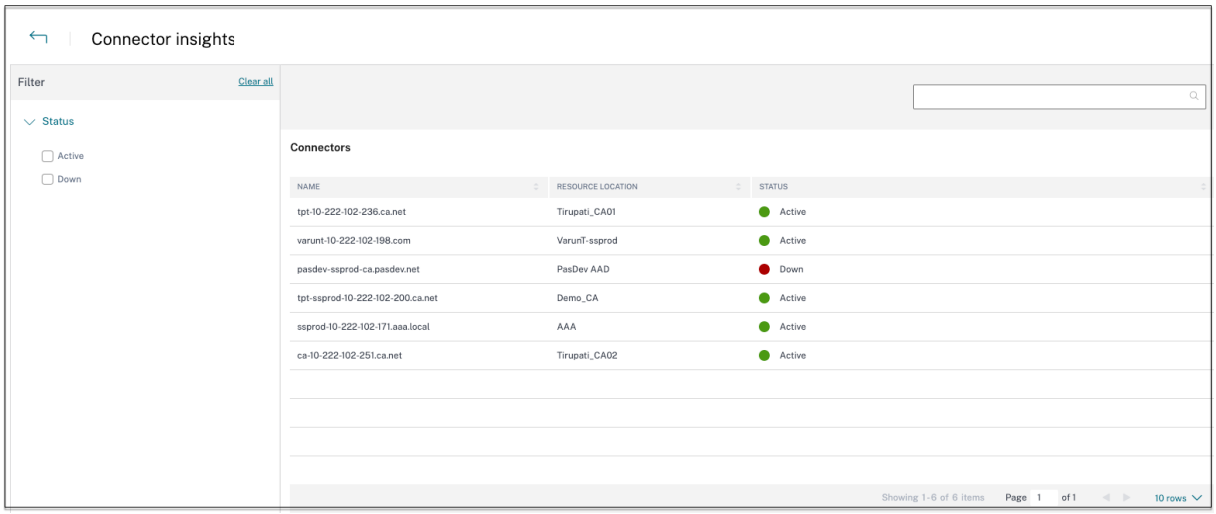
- 展開アイコン (>) をクリックすると、ログの完全な詳細を表示できます。
- 診断ログ ページには、アクセスされる各メイン URL の埋め込みドメインが表示されます。管理者は、メイン URL から展開アイコン (>) をクリックして、埋め込まれたドメインを表示できます。管理者は埋め込みドメイン リストを使用して、アプリのアクセスやアプリのレンダリングに関連する問題に対処できます。たとえば、アプリケーション構成でドメインが欠落していると、エンドユーザーは特定のアプリにアクセスできません。この場合、管理者は埋め込まれたドメインのリストを表示し、不足しているドメインを特定し、不足しているドメインでアプリの構成を更新できます。



> 注意:
>
> - デフォルトでは、診断ログ ページには、現在の週のデータと最近の 10000 件の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。

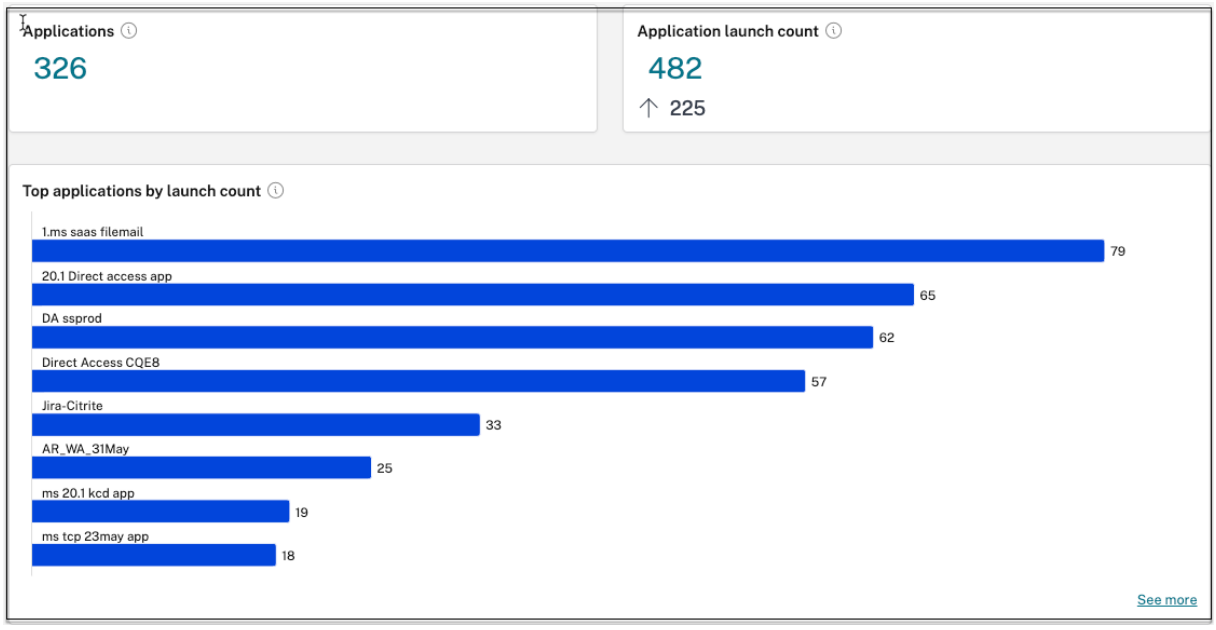
コネクタのステータス

コネクタ 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、コネクタがデプロイ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、フィルター アクティブ または 非アクティブ を使用して、コネクタをステータスに基づいてフィルター処理できます。



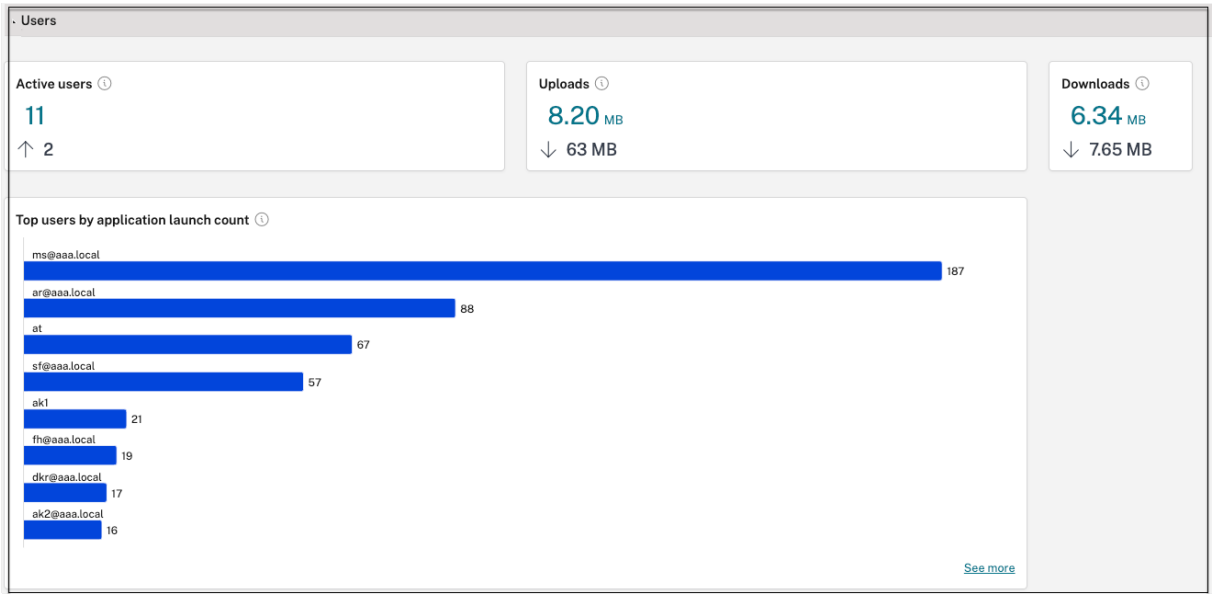
起動回数による上位アプリケーション

起動回数による上位アプリケーション チャートを使用して、アプリが起動された回数、アプリ サーバーにアップロードされたデータの合計量、アプリ サーバーからダウンロードされたデータの合計量に基づいて上位アプリケーションのリストを表示します。フィルター **SaaS** アプリ、**Web** アプリ、または **TCP/UDP** アプリ を適用して、検索を特定のアプリに絞り込むことができます。事前に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ーできます。



アプリケーション起動回数による上位ユーザー

ユーザーごとのデータを表示するには、「アプリケーションの起動回数による上位ユーザー」グラフを使用します。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合計量、アプリ サーバーからダウンロードされたデータの合計量などです。事前に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ーできます。

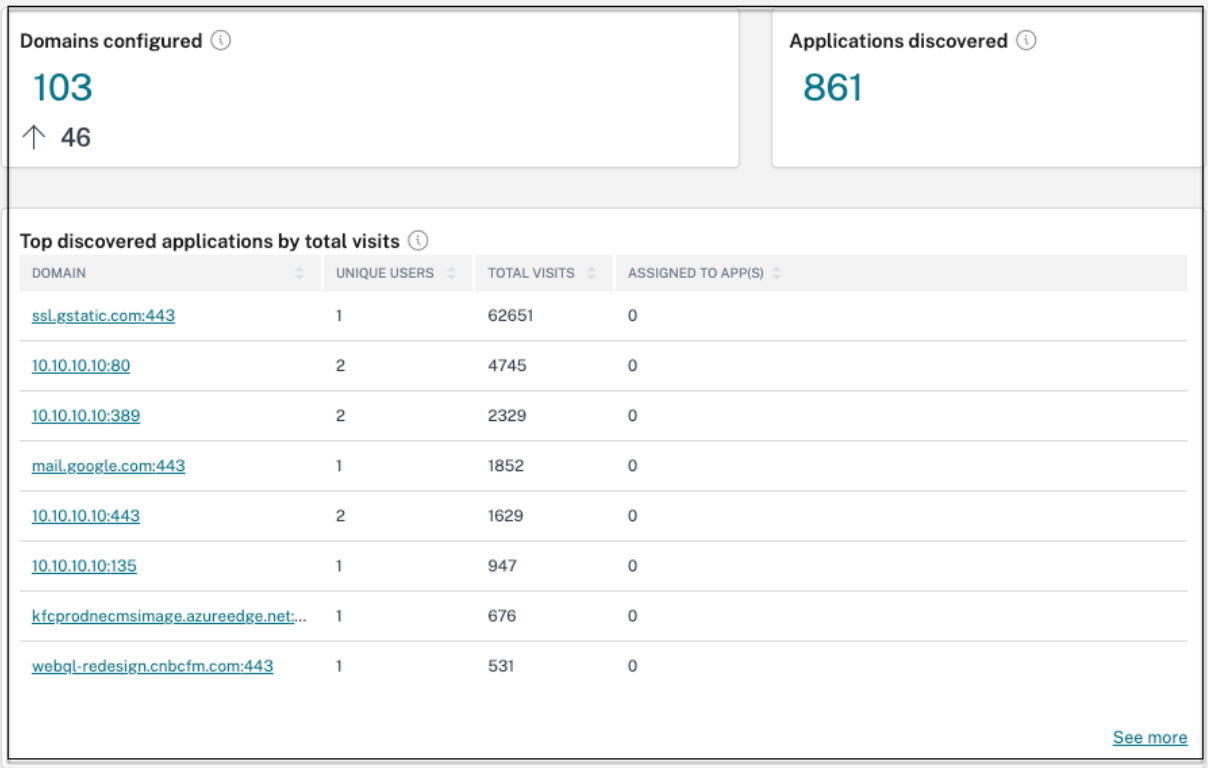


施行による上位のアクセス ポリシー

アプリに適用されているアクセス ポリシーの一覧を表示するには、「適用別の上位アクセス ポリシー」グラフを使用します。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た回数を表示するには、[詳細を表示] リンクをクリックします。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ー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。

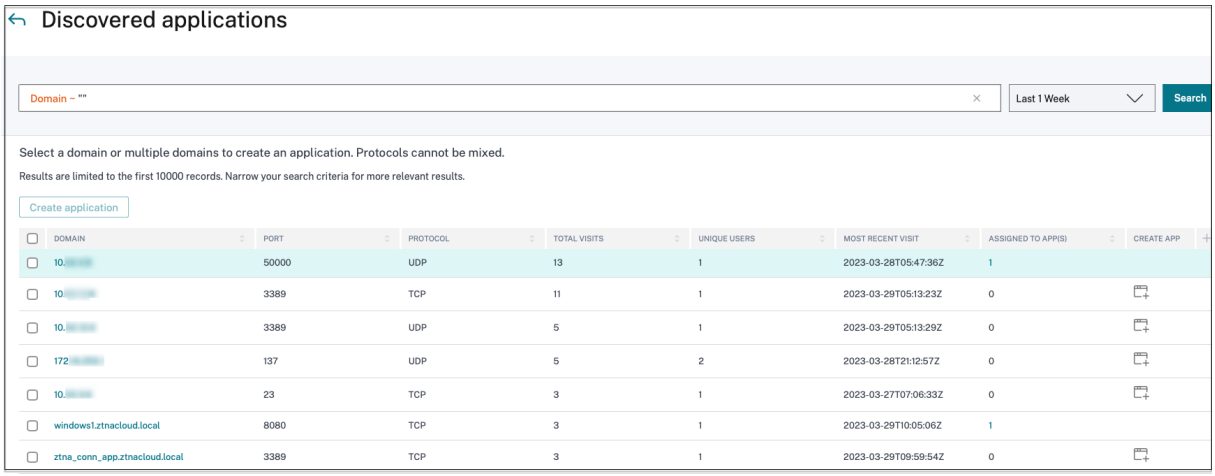
最も多く発見されたアプリケーション

合計訪問数による上位の検出されたアプリケーションのグラフ を使用して、ある時点でアクセスされたが、どのアプリにも関連付けられていない一意の個別のドメインのリストを表示します。これらのドメインは、そのドメインへの総訪問数に基づいてリストされます。管理者はこのグラフを使用して、特に関心のあるドメインが多くのユーザーによってアクセスされ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合計数が表示されます。数字をクリックすると、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。

すべてのドメインの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。



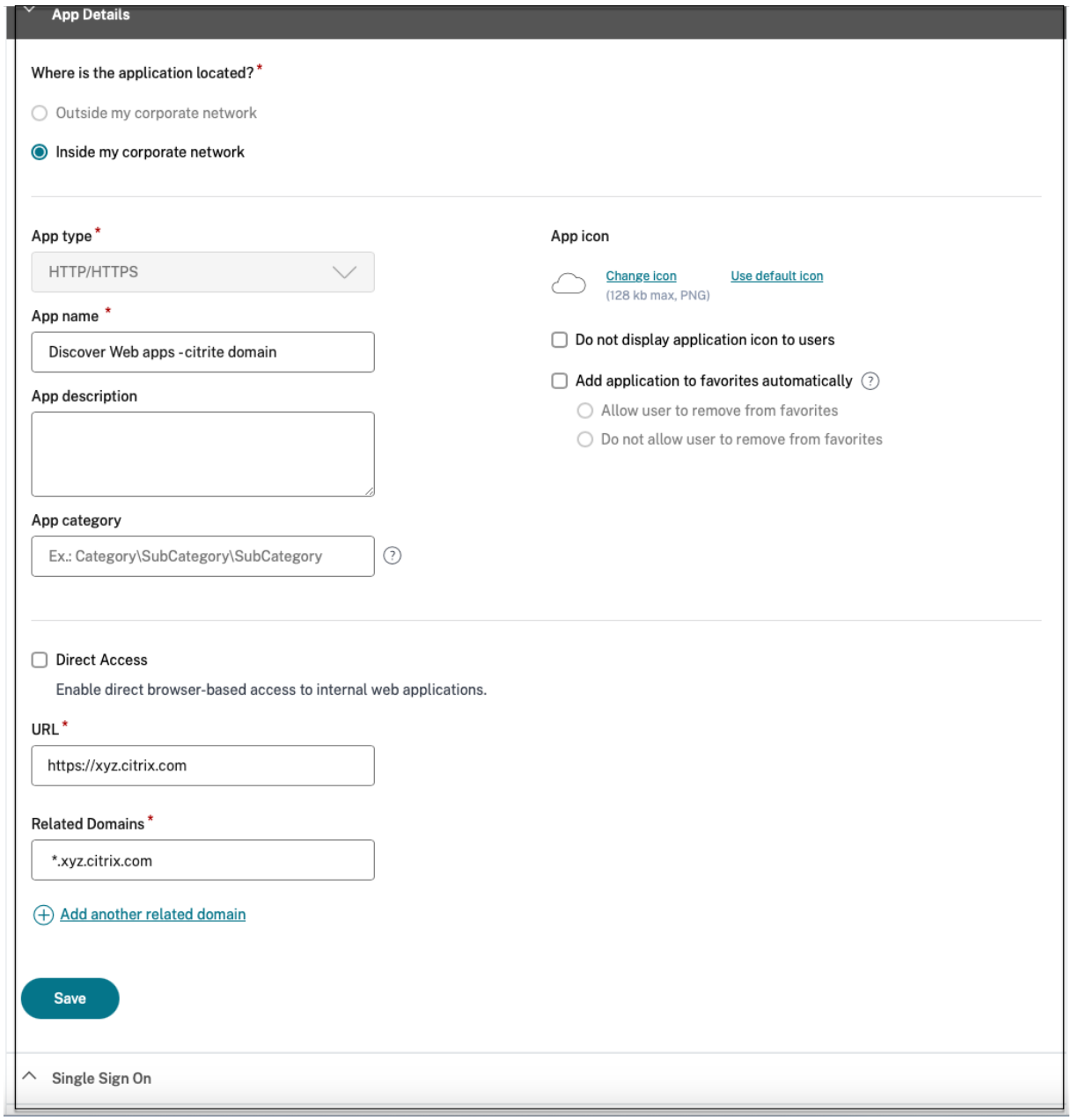
検出されたアプリケーション ページには、ドメイン名、ポート、プロトコル、合計訪問数、ユニーク ユーザー数、最新の訪問日などのドメインの詳細が表示されます。グラフ内のすべての列は並べ替え可能です。検索バーを使用してドメインに基づいて検索できます。

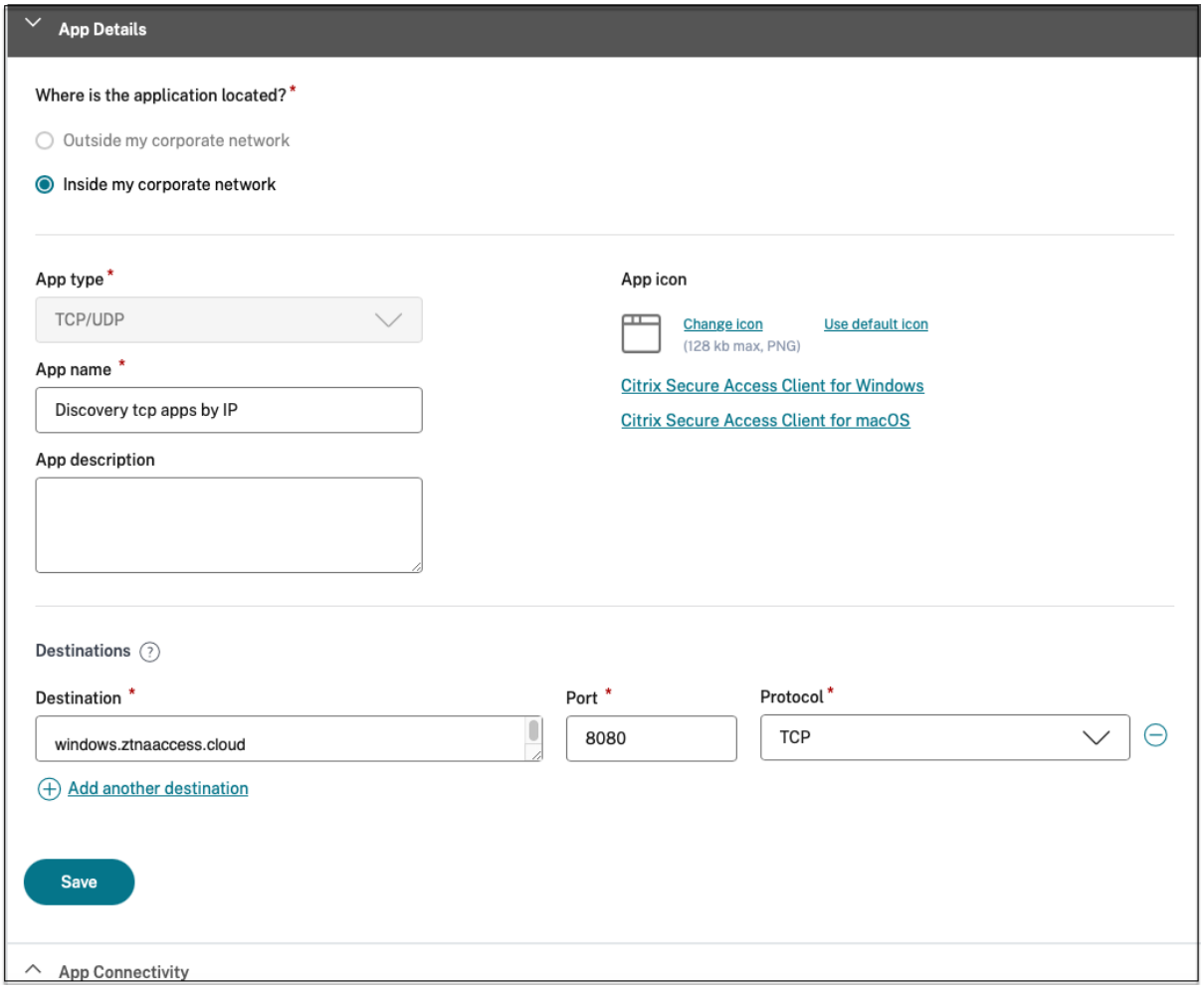
> 注意:
>
> - プロトコルは、顧客が使用する標準ポートに基づいて派生されます。
> - 検出されたドメインのリストは 10000 件のレコードに制限されます。

チャートからアプリを作成する

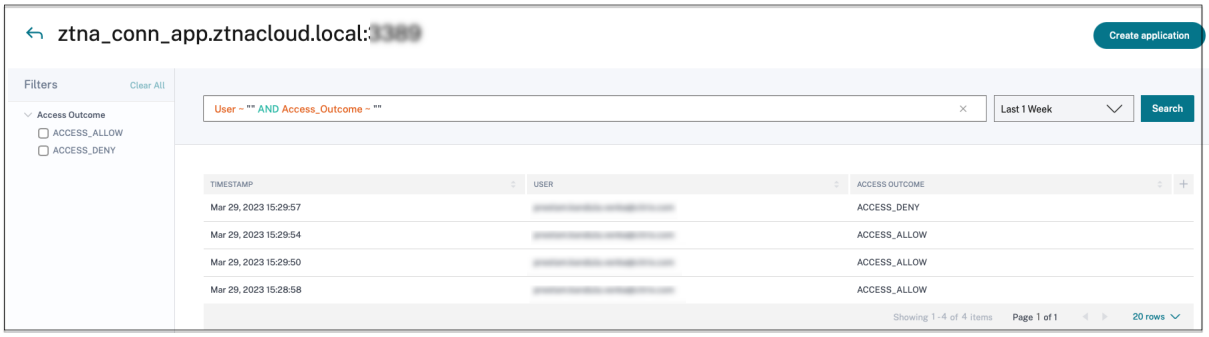
それぞれのドメインに沿って **+** アイコンをクリックしてアプリを作成します。アプリ構成ウィザードがポップアップ表示されます。同じドメイン、ポート、プロトコルの組み合わせでアプリがすでに作成されていて、完了状態になっている行には、アプリ作成アイコンは表示されません。

- アプリの種類は、選択したアプリのプロトコルに基づいて自動的に入力されます。ただし、必要に応じてタイプを変更することもできます。
- **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的に入力されます。アプリを追加するための手順を完了します。詳細については、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参照してください。





固有のドメイン 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。アプリを追加するための手順を完了します。



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。

- **= (**ある値に等しい**)**: 検索条件に完全に一致するログ/ポリシーを検索します。

- **!= (**ある値と等しくない**)**: 指定された条件を含まないログ/ポリシーを検索します。
- **~ (**何らかの値が含まれています**)**: 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。

ログ記録とトラブルシューティング

October 21, 2024

このトピックを使用して、アプリの構成、認証と SSO、またはアプリのアクセス関連の問題をトラブルシューティングします。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ます。このトピックをより有効に活用するために役立つよくある質問を次に示します。

よくある質問?

Secure Private Access 診断ログとは何ですか?

セキュア プライベート アクセス ログはどこにありますか?

Secure Private Access 診断ログを表示するウィジェットはどれですか?

Secure Private Access 診断ログにはどのような詳細が記載されていますか?

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

診断ログをフィルタリングするにはどうすればよいですか?

発生した障害を解決するために、Secure Private Access のトラブルシューティング トピックをどのように使用すればよいですか?

情報コードとは何ですか? 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? どうやって使うんですか?

セキュア プライベート アクセス PoP の場所とは何ですか?

情報コードとエラー参照テーブルを使用しても障害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

次のエラー参照表は、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	説明	解像度
0x180006、0x1800B7、0x1800B7 のエラー	アプリの FQDN の長さが超過したため、アプリの起動に失敗しました	アプリの FQDN の長さが超過したため、アプリの起動に失敗しました
0x180022	認証サービスがダウンしているため、アプリの起動に失敗しました	認証サービスがダウンしているため、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 の 0x1800B1、0x1800B2、0x1800B3、0x180048 の 0x1800EF	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、無効なアプリ FQDN	アプリへのアクセスが拒否されました
	コネクタアプライアンスへの接続に問題があります	コネクタアプライアンスへの接続に問題があります
0x18009D	DNS ルックアップ/接続に失敗しました	セキュア ブラウザ サービス - DNS ルックアップ/接続エラー
0x1800A0、0x1800A2、0x1800A3、0x1800A5 0x1800A6、0x1800A7 の	バックエンドの 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	バックエンドの 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 の	ユーザーは Web/SaaS アプリにアクセスする権限がありません	ユーザーは Web/SaaS アプリにアクセスする権限がありません
0x1800BD	ユーザーには DirectAccess の 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 DirectAccess の Web/SaaS アプリ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の取得中に Citrix Secure Access エージェントセッションの起動に失敗しました	アプリケーション構成の取得中に Citrix Secure Access エージェントセッションの起動に失敗しました
0x1800CD、0x1800CE、0x1800D6、0x1800EA	アプリケーション構成の取得中に Citrix Secure Access エージェント セッションの起動に失敗しました。ポリシー評価中に Citrix Secure Access エージェント アプリの起動に失敗しました。Citrix Secure Access エージェント アプリの起動に失敗しました。	不正なクライアントリクエスト

情報コード	説明	解像度
0x1800DE	ポリシー評価中に Citrix Secure Access エージェントアプリの起動に失敗しました	ポリシー評価中に Citrix Secure Access エージェントアプリの起動に失敗しました
0x180055、0x1800DF、0x1800E3	コンテキスト ポリシーによってアプリが制限され、ポリシー構成によりアクセスが拒否されました	ユーザーダッシュボードにリストされていないアプリが 1 つ以上あります
0x1800EB	IPv6 がサポートされていないため、Citrix Secure Access エージェント アプリ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 エージェント アプリの起動に失敗しました
0x1800EC、0x1800ED	Citrix Secure Access エージェント アプリの起動が無効な IP アドレスのため失敗しました	Citrix Secure Access エージェント アプリの起動が無効な IP アドレスのため失敗しました
0x10000001、0x10000002、0x10000003、0x10000004	ネットワークの問題により Citrix Secure Access クライアントのログインに失敗する	Citrix Secure Access クライアントのネットワーク接続到達可能性の問題
0x10000006	中間のプロキシによる Citrix Secure Access クライアントのログイン失敗	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	信頼できない証明機関による 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観察されました
0x10000008	無効な証明書による Citrix Secure Access クライアントのログイン失敗	無効なサーバー証明書の問題が観察されました
0x1000000A	構成の問題により Citrix Secure Access クライアントのログインに失敗する	ユーザーの設定が空のためログインに失敗しました
0x1000000B	接続失敗による Citrix Secure Access クライアントのログイン失敗	ネットワークまたはエンドユーザーによって接続が終了されました
0x10000010	セッションの期限切れにより Citrix Secure Access クライアントのログインに失敗する	セッションの有効期限が切れたため、構成のダウンロードに失敗しました
0x10000013	構成リストが巨大であるため、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

情報コード	説明	解像度
0x11000003	制御チャネルの作成失敗による Citrix Secure Access クライアントのログイン失敗	セッションの有効期限が切れたため、制御チャネルの確立に失敗しました
0x11000004	制御チャネルの作成に失敗したため、Citrix Secure Access クライアントのログインに失敗しました	制御チャネルの確立に失敗しました
0x11000005	制御チャネルの作成に失敗したため、Citrix Secure Access クライアントのログインに失敗しました	制御チャネルの確立に失敗しました
0x11000006	制御チャネルの作成に失敗したため、Citrix Secure Access クライアントのログインに失敗しました	ネットワークの問題により制御チャネルの確立に失敗しました
0x12000001	セッションがすでに期限切れのため、Citrix Secure Access クライアントのログアウトに失敗しました	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に失敗しました	セッションは強制的に終了しました
0x13000001	セッションの有効期限が切れたため、アプリへのアクセスに失敗しました	セッションの有効期限が切れたため、アプリケーションの起動に失敗しました
0x13000002	ライセンスが不十分なためアプリへのアクセスに失敗しました	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に失敗しました。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、アプリケーションの起動に失敗しました
0x13000004、0x13000005	サーバーが利用できないため、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、アプリケーションの起動に失敗しました
0x13000007	アクセス ポリシーが無効になっているか、ユーザーがサブスクライブしていないため、アプリへのアクセスに失敗しました	ポリシー評価と構成検証に失敗したため、アプリケーションの起動に失敗しました

情報コード	説明	解像度
0x13000009	ルーティングエントリが見つからないため、アプリへのアクセスに失敗しました	アプリケーション ドメイン テーブルの問題のため、アプリケーションの起動に失敗しました
0x1300000B	クライアントが接続を閉じました	クライアントはセキュアプライベートアクセスサービスとの接続を閉じました
0x1300000C	ZTNA 経由の FQDN 解決に失敗しました	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のダウンロードに失敗しました	設定されたアプリケーションの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 アプリの起動に失敗しました。ポリシー評価中に無効な結果で TCP/UDP アプリの起動に失敗しました。	アプリケーション構成の問題
0x001800DB	無効なリソース ロケーション構成により、TCP/UDP アプリの起動に失敗しました	リソースの場所に関する問題
0x13000006、0x001800DC、0x001800DD	TCP アプリの起動は、アプリにサポートされていない拡張セキュリティポリシーが設定されているため失敗しました。TCP アプリの起動は、TCP アプリにサポートされていないセキュア ブラウザ サービス リダイレクトが設定されているために失敗しました。	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ています
0x001800DE	宛先のアプリケーション構成が見つからないため、TCP/UDP アプリの起動に失敗しました	アプリケーションが見つかりません
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 アプリの起動に失敗しました	無効な IP アドレス
0x001800EF	プライベート TCP サーバーへの接続確立中に TCP アプリの起動に失敗しました	エンドツーエンド接続を確立できません

情報コード	説明	解像度
0x001800F5	IPV6 アドレスのため UDP アプリ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 トラフィックの配信に失敗しました	UDP トラフィックが配信に失敗した
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に失敗しました	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	コネクタアプライアンスを登録できません。UDP ネットワーク接続の初期化に失敗しました	コネクタアプライアンスがセキュアプライベートアクセスサービスに登録できませんでした
0x10000403、0x10000404、0x10000407、0x1000040A、0x1000040A のエラー 0x1000040B、0x1000040F、0x10000410	接続エラー、制御パケットの送信失敗、ゲートウェイ サービスの読み取りエラー、制御パケットの解析失敗、ゲートウェイ サービスの書き込みエラー	コネクタアプライアンスとの接続の問題
0x10000405、0x10000408、0x10000409、0x1000040D、0x1000040E … 0x1000040E、0x10000412	バックエンドに到達できません、UDP パケットの送信に失敗しました、UDP パケットの受信に失敗しました、バックエンドへの書き込み中にエラーが発生しました、バックエンドが接続を閉じました	コネクタアプライアンスと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
0x10000406	DNS 解決に失敗しました	コネクタアプライアンスが 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閉じました	プライベートサーバーの接続が終了しました
0x10000413	接続切断理由の判定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 への接続またはデータの送信に失敗しました
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ません	一致するポリシー条件がありません
0x100509	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	アプリケーションにアクセスポリシーが関連付けられていません
0x10050C	ユーザーが権利を有す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	アプリの列挙情報

情報コード	説明	解像度
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	コネクタに到達できないため、UDP/DNS 要求が失敗しました	コネクタに到達できないため、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 ポリシーの取得に失敗しました	JSON Web トークンの解析中にアクセス ポリシーの取得に失敗しました
0x20580004	アクセス ポリシーの詳細を取得するためのネットワーク障害	アクセス ポリシーの詳細を取得するためのネットワーク障害
0x20580005	公開証明書の取得中にポリシーの取得に失敗しました	公開証明書の取得中にポリシーの取得に失敗しました
0x20580007	JWT の署名の検証中にポリシーの取得に失敗しました	JWT の署名の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 を形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 を形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 認証トークンの有効期限が切れたため、アクセス ポリシーの取得に失敗しました	セカンダリ DS 認証トークンの有効期限が切れたため、アクセス ポリシーの取得に失敗しました

情報コード	説明	解像度
0x10200002	コネクタアプライアンスが登録されていません	コネクタアプライアンスが登録されていません
0x10200003	コネクタアプライアンスに接続できません	コネクタアプライアンスに接続できません
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 です。	プロキシサーバーにアクセスできません	プロキシサーバーにアクセスできません
0x10000305	プロキシサーバーの認証に失敗しました	プロキシサーバーの認証に失敗しました
0x10000306	設定されたプロキシサーバーにアクセスできません	設定されたプロキシサーバーにアクセスできません
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 の処理に失敗しました	SSO の処理に失敗しました
0x10000108、0x1000010B、0x1000010C、0x1000010D、0x1000010E …	SSO の処理に失敗しました。SSO 設定を判別できません	SSO の処理に失敗しました。SSO 設定を判別できません
0x10000101、0x10000102、0x10000103、0x10000104 の	FormFill SSO に失敗しました。フォーム アプリの構成が正しくありません。	FormFill SSO に失敗しました。フォーム アプリの構成が正しくありません。
0x1000010A	FormFill SSO に失敗しました。フォーム アプリの構成が正しくありません。	FormFill SSO に失敗しました。フォーム アプリの構成が正しくありません。
0x10000202	Kerberos SSO に失敗しました	Kerberos SSO に失敗しました
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

情報コード	説明	解像度
0x14000001	Citrix Workspace アプリケーションで構成された複数の ZTNA 権限アカウント	Citrix Workspace アプリケーションで構成された複数の ZTNA 権限アカウント

解決手順

次のセクションでは、ほとんどの情報コードの解決手順を示します。解決手順が記録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アプリが **1** つ以上あります

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。信頼要因 (デバイスの状態やリスク 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 `理由` 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` 列フィルターを変更して、`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。このフィルターは、ポリシー評価に関連するログのみを表示します。
3. `理由` 列で評価されたポリシー ペイロードを検索します。このペイロードには、ユーザーがサブスクライブしているすべてのアプリのユーザーのコンテキストに対して評価されたポリシーが表示されます。
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た場合、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
    - ポリシー内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
    - ポリシー内の一致するデフォルト ルールが正しくありません。これはフォールスルー ケースです。それに応じて条件を調整します。

ユーザーは **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をサブスクリプション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. 対象ユーザーがサブスクリプション リストにエントリされていることを確認します。

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

リソースの場所にあるコネクタがダウンしたり、バックエンド サーバー自体が応答しなくなったりして、顧客ネットワークが不安定になる場合があります。

1. ネットワーク遅延を排除するために、コネクタ アプライアンスがバックエンド 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ます。
2. バックエンド サーバーのファイアウォールがコネクタ アプライアンス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、クライアントで `nslookup nssvc.dnsdiag.net` を実行すると、応答の正規名は `aws-us-wgnssvc.net` などの地域固有のサーバーを示します。

アプリの **FQDN** の長さが超過したため、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 の長さは 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が超過しました

情報コード**:** 0x18000E

アプリのアクセスがブロックされているかどうか、ポリシー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. アプリに権限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。

アプリへの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に対してアプリが拒否されます。

アプリのアクセスをブロックしているポリシー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. アプリに権限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。

列挙されていないアプリケーション

ポリシーの拒否や Secure Private Access 統合が有効になっていない場合、列挙リストからアプリケーションが欠落する可能性があります。

- 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 1 つも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ます。

コネクタアプライアンスへの接続に問題があります

情報コード**:** 0x1800EF

オンプレミスのコネクタとの TCP 接続が利用できないため、アプリ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. 診断ログの csv ファイルで、エラー コード `0x1800EF` の `トランザクションID` を検索します。
2. csv ファイル内のトランザクション ID に一致するすべてのイベントをフィルターします。
3. また、csv ファイル内の `prod` 列のうち `SWA.GOCTRL`に一致するもの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ましたか? 結果;

   - 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 `リソースの場所` が正しいかどうかを確認します。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リソースの場所を修正します。
   - ログ メッセージ内の `VDA Ip とポート` が正しいかどうかを確認します。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 イベント の確認に進みます。

connectType メッセージ connect::failure または multiconnect::successのイベントが表示される場合は、次のようになります。

- このログ メッセージの推奨修正内容を確認します - コネクタがまだ同じポップに接続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ている可能性があることを示しています。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 サポートにお問い合わせください。

connectType メッセージ IntraAll::failureのイベントが表示される場合は、Citrix カスタマー サポートにお問い合わせください。

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 トランザクションID を検索します。
2. csv ファイル内のトランザクション ID に一致するすべてのイベントをフィルターします。
3. また、csv ファイル内の prod 列のうち SWA.ConnectorAppliance.WebAppsと一致する列をフィルターします。
4. ステータス のイベントが 失敗として表示される場合、
   - これらの各障害イベントの 理由 メッセージを確認します。
   - 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 サポートにお問い合わせください。
   - IsProxyRequiredCheckError または ProxyDialFailed または ProxyConnectionFailed または ProxyAuthenticationFailure または ProxiesUnReachable は、コネクタがプロキシ構成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。プロキシ設定が正しいかどうかを確認してください。
   - さらなる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、アプリ構成からさまざまな SSO 属性が抽出され、アプリの起動時に適用されます。特定のユーザーに属性がない場合、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。構成が正しいことを確認します。

1. アクセス ポリシーに移動します。
2. アプリに権限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 方式は、オンプレミス コネクタによって実行されます。コネクタからの次の診断ログを確認します。

コネクタコンポーネントからの **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 コンポーネント名 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ていますか?

    - 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 または ProxyConnectionFailed または ProxyAuthenticationFailure または ProxiesUnReachable は、コネクタがプロキシ構成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。プロキシ設定が正しいかどうかを確認してください。
    - 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 サポートにお問い合わせください。
    - UnableToConnectTargetServer は、コネクタからバックエンド サーバーにアクセスできないことを示します。バックエンドの構成を再度確認してください。
    - IncorrectFormAppConfiguration または NoLoginFormFound または FailedToConstructForLoginActionURL 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フォーム SSO 構成セクションを確認します。
    - NTLMAuthNotFound は、NTLM ベースの認証が失敗したことを示します。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。
    - さらにデバッグするには、コネクタ イベントを参照してください。

認証サービスがダウンしているため、アプリの起動に失敗しました

情報コード**:** 0x180022

セキュア プライベート アクセスを使用すると、管理者は従来の Active Directory、AAD、Okta、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の停止により、この問題が発生する可能性があります。

サードパーティのサーバーが稼働していてアクセス可能かどうかを確認します。

SAML SSO 失敗

情報コード**:** 0x18008A、0x1800A9、0x1800AA、0x1800AB、0x1800AC、0x1800AD、0x1800AE、0x1800AF、0x1800B0、0x1800B1、0x1800B2、0x1800B3

IdP によって開始されたアプリの起動時に、ユーザーは認証に失敗したり、SP によって開始されたアプリの起動時にアクセスできないリンクが表示されることがあります。Secure Private Access サービス側の SAML アプリ構成とサービス プロバイダー構成も確認してください。

セキュアプライベートアクセス構成**:**

1. アプリケーション タブに移動します。
2. 問題のある SAML アプリを探します。
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. 次のフィールドをチェックしてください。

    - アサーション URL
    - リレー状態
    - オーディエンス
    - 名前 ID の形式、名前 ID、およびその他の属性

サービスプロバイダーの構成**:**

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、対象者、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 サポートにお問い合わせください。

無効なアプリ **FQDN**

情報コード**:** 0x180048

顧客管理者が無効な FQDN またはバックエンド サーバーで DNS 解決が失敗する FQDN を指定した可能性があります。

この場合、エンドユーザーの Web ページにエラーが表示されます。アプリケーションの設定を確認してください。

SaaS アプリの検証　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 アプリの検証

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 を確認してください。URL はイントラネットまたはインターネットのいずれからもアクセスできる必要があります。

セキュア ブラウザ サービス **- DNS** ルックアップ**/**接続に失敗しました

情報コード**:** 0x18009D

リモート ブラウザ分離サービスによるブラウジング エクスペリエンスが損なわれます。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 サーバーにアクセスし、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。
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。

> 注意**:**
>
> Citrix リモート ブラウザ分離サービスは、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壊れます。

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 サーバーに到達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ようにブロックされていないかどうかを確認します。

ダイレクト アクセス **- Web** アプリとして誤って構成されています

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、それらに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 テーブルとアプリ構成の間で競合する構成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、直接アクセスが有効になっているかどうかを確認します。
3. ルーティング ドメイン テーブル内のアプリ 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

アプリの構成により、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をサブスクリプション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、エージェントレス アクセス構成を確認します。

強化されたセキュリティ ポリシー **-** セキュア ブラウザ サービスの構成ミス

情報コード**:** 0x1800C3

ポリシー ルールで意図されたものとは異なる誤った動作が見られます。コンテキスト 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付けられているポリシーを確認します。
3. そ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 **-** ポリシーの誤った構成

ポリシー ルールで意図されたものとは異なる誤った動作が見られます。強化されたセキュリティ設定を確認してください。

1. アプリケーションに進みます。
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** エージェントセッションの起動に失敗しました

情報コード**:** 0x1800D0

Citrix Secure Access アプリは、Citrix Cloud への完全なトンネルを正常に確立できません。

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. エントリの最大数が 16k の制限内に十分収まっていることを確認します。

TCP/UDP アプリ **-** 不正なクライアント要求

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. リクエストが中間のプロキシによって偽造または再構築されていないことを確認します。
2. 中間者攻撃の疑い。

TCP/UDP アプリ **-** セキュア ブラウザ サービスのリダイレクト構成ミス

情報コード**:** 0x1800DD

リモート ブラウザ分離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 でアプリの構成を確認します。

> 注意**:**
>
> Citrix リモート ブラウザ分離サービスは、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** エージェント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 に、ルーティング ドメイン テーブル内に対応するエントリがあることを確認します。

IPv6 がサポートされていないため、**Citrix Secure Access** エージェント アプリ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。

Citrix Secure Access エージェント アプリの起動は、**IP** アドレスが無効であるため失敗しました

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 アドレスが有効であり、正しいバックエンドを指していることを確認します。

Citrix Secure Access クライアントのネットワーク接続到達可能性の問題

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ます。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 サポートにお問い合わせください。
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どうかを確認します。

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ます。
2. クライアントでプロキシが正しく設定されているかどうかを確認します。
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 サポートにお問い合わせください。

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観察されました

情報コード**:** 0x10000007

Citrix サポートに問い合わせて、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観察されました

情報コード**:** 0x10000008

Citrix サポートに問い合わせて、サーバー証明書が自己署名されているか、期限切れか、信頼できないソースからのものであるかを確認してください。

ユーザーの設定が空のためログインに失敗しました

情報コード**:** 0x1000000A

1. 少なくとも 1 つの TCP/UDP/HTTP アプリが構成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 (セキュア プライベート アクセス **>** 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。

ネットワークまたはエンドユーザーによって接続が終了されました

情報コード**:** 0x1000000B

ZTNA セッション接続中にネットワークが中断されたか、エンドユーザーが接続をキャンセルしたかどうかを確認します。

セッションの有効期限が切れたため、構成のダウンロードに失敗しました

情報コード**:** 0x10000010

ZTNA セッション構成のダウンロード要求中に VPN セッションの有効期限が切れた可能性があります。Citrix Secure Access クライアントに再度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たため、Citrix Secure Access クライアントはログインに失敗しました。

1. セキュア プライベート アクセス **>** 設定 **>** アプリケーション ドメインで 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. エントリの数が多すぎないことを確認してください。エントリ リストが非常に大きい場合は、使用されていない宛先を無効にするか削除します。

   宛先リストが 1000 を超えると予想される場合は、ConfigSize レジストリ キーを更新して、最大構成ダウンロード サイズを増やしてみてください。詳細については、「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、制御チャネルの確立に失敗しました

情報コード**:** 0x11000003

セッションの有効期限が切れたため、DNS 要求の確立のための制御チャネルが失敗しました。

制御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 クライアントに再度ログインしてみてください。

制御チャネルの確立に失敗しました

情報コード**:** 0x11000004

DNS 要求の確立のための制御チャネルに失敗しました。

- 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にあるコネクタ アプライアンスのヘルス チェックを実行します。
4. それでも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** コネクタ アプライアンスのメンテナンス**:**

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. 予想されるリソースの場所に少なくとも 2 つのコネクタ アプライアンスがあることを確認します。

次のことを確認してください。

- リソース ロケーション LAN は動作状態です。
- コネクタ アプライアンスからサービスまたはバックエンド サーバーへのアクセスをブロックするファイアウォールやプロキシは中間に存在しません。
- 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、次の操作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 ダッシュボードでトランザクション ID に一致するすべてのイベントをフィルターします。
3. トランザクション ID と一致するエラーがクライアントまたはコネクタ アプライアンスまたはサービスの診断ログで発生したかどうかを確認します。その後、それに応じて適切な措置を講じてください。
4. アプリケーション ドメイン テーブル (セキュア プライベート アクセス **>** 設定 **>** アプリケーション ドメイン) で、宛先のリソースの場所が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どうかを確認します。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。

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 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。

制御チャネルの確立に失敗しました

情報コード**:** 0x11000005

制御チャネル (DNS 要求用) の確立に失敗しました。

1. Secure Private Access サービスのライセンス資格を確認します。
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制御チャネルの確立に失敗しました

情報コード**:** 0x11000006

ネットワークの問題により、制御チャネル (DNS 要求用) の確立に失敗しました。

1. Secure Private Access サービスにアクセスできるかどうかを確認します。
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 サポートにお問い合わせください。

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 が不足しているため制御チャネルの確立に失敗しました

情報コード**:** 0x11000007

IIP が不十分なため、制御チャネル (DNS 要求用) の確立に失敗しました。

エラー コードとクライアント ログを 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であ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 クライアントに再度ログインしてみてください。

セッションは強制的に終了しました

設定された強制タイムアウトに達すると、セッションは強制的に終了します。

情報コード**:** 0x12000002

Citrix Secure Access クライアントに再度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. アプリの起動中に ZTNA セッションが期限切れになりました。
2. Citrix Secure Access クライアントに再度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付与されているかどうかを確認します。
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、アプリケーションの起動に失敗しました

情報コード**:** 0x13000003、0x13000008、0x001800DF

ユーザーとアプリケーションのポリシー構成に従って、アプリケーションの起動は拒否されます。

以下の点を確認してください。

- 複数のアプリケーションで同じ宛先が使用されていない (HTTP、HTTPS、TCP、UDP)
- 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対して設定された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、アプリケーションの起動に失敗しました

情報コード**:** 0x13000004, 0x13000005

1. セキュア プライベート アクセス サービスにアクセスできるかどうかを確認します。
2. アプリを再度起動します。
3. アプリに長時間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 サポートにお問い合わせください。

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。

ポリシー評価と構成検証に失敗したため、アプリケーションの起動に失敗しました

情報コード**:** 0x13000007

セキュア プライベート アクセス サービスによるポリシー評価と構成検証に失敗したため、アプリケーションの起動に失敗しました。

アクセスした宛先のアプリケーションを検出できません。

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 テーブルの問題のため、アプリケーションの起動に失敗しました

情報コード**:** 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。

セキュア プライベート アクセス **>** 設定 **>** アプリケーション ドメインで、アプリケーションのルート エントリが正しく構成されていることを確認します。

クライアントはセキュアプライベートアクセスサービスとの接続を閉じました

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ます。
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 サポートにお問い合わせください。

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、コネクタ アプライアンスが FQDN の DNS を解決できない場合に発生します。

1. DNS サーバーでそれぞれのアプリ FQDN の DNS エントリを確認します。
2. コネクタ アプライアンスに適切な 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、「コネクタ アプライアンス管理ページでのネットワーク設定の構成」を参照してください。

アプリケーションが見つかりません

情報コード**:** 0x001800DE

ユーザーがアクセスした先のアプリケーションが見つからない可能性があります。これは、アプリケーション ドメイン テーブルに宛先とリソースの場所のマッピングがない場合に発生する可能性があります。

- アクセス先の宛先に対して 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サブスクリプション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. 対象ユーザーがサブスクリプション リストにエントリされていることを確認します。
4. アプリケーション ドメイン 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ます。

設定されたアプリケーションの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 アプリが構成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 (セキュア プライベート アクセス **>** 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。

アプリケーション構成の問題

アプリケーション構成に特殊文字が含まれているか、ポリシー構成に問題があります。

情報コード**:** 0x001800D9, 0x001800DA

次のことを確認してください。

- アプリ構成にサポートされていない文字が含まれていません。
- 宛先 IP アドレスまたは IP アドレス範囲、または IP CIDR が有効です。
- 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 (セキュア プライベート アクセス **>** 設定 **>** アプリケーション ドメイン) で有効になっています。
- ポリシーはそれぞれのアプリケーションに設定され、バインドされます。
- アクセス ポリシーの構成は正しいです。

リソースの場所に関する問題

情報コード**:** 0x001800DB

- リソースの場所が構成されていることを確認します。
  1. Citrix Cloud 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. 予想されるリソースの場所が構成され、リソースの場所がアクティブな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 (セキュア プライベート アクセス **>** 設定 **>** アプリケーション ドメイン) で、宛先に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ています

情報コード**:** 0x001800DC、0x001800DD、0x13000006

強化されたセキュリティ ポリシーがバインドされている 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します。

- 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ます。
- HTTP/HTTPS アプリケーションに対して強化されたセキュリティ 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 リモート ブラウザー分離サービス経由でのみアプリにアクセスすることをお勧めします。
- Citrix Secure Access クライアントを介してアプリにアクセスするために、HTTP/HTTPS アプリケーションの拡張セキュリティ制御を無効にします。
  - Secure Private Access 管理ポータルに移動します。
  - 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、前に特定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。

設定の詳細については、「アプリケーションの追加と管理」を参照してください。

> 注意**:**
>
> Citrix リモート ブラウザ分離サービスは、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要求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。

無効な **IP** アドレス

情報コード**:** 0x001800ED

アプリケーション起動要求で受信した IP アドレスが無効です。

クライアントからは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

リソースの場所で構成されたクライアントと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な状態であることを確認します。
  - Citrix Cloud 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。
  - 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。
- 高可用性コネクタアプライアンスを維持する
  - Citrix Cloud 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 つのコネクタ アプライアンスがあることを確認します。
- 次のことを確認してください。
  - リソース ロケーション LAN は動作状態です。
  - コネクタ アプライアンスからサービスまたはバックエンド サーバーへの接続をブロックする中間の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。

これらに問題がなければ、次の操作を行ってください。

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 サービス ダッシュボードでトランザクション ID に一致するすべてのイベントをフィルターします。
3. Secure Private Access サービス 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 (セキュア プライベート アクセス **>** 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 を使用して構成されているかどうかを確認します (セキュア プライベート アクセス **>** アプリケーション)。

これらの手順のいずれで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 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

アプリ要求でサポートされていない IPv6 が受信されました。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 管理ポータルに移動します。
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。

詳細については、「アプリの追加と管理」を参照してください。

UDP トラフィックが配信に失敗した

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ます。
2. ログアウトしてから再度ログインしてください。

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

- エラー コードのトランザクション ID を検索し、Secure Private Access サービス ダッシュボードでトランザクション ID に一致するすべてのイベントをフィルターします。
- トランザクション ID に一致する他のコンポーネントでエラーが発生したかどうかを確認します。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 サポートにお問い合わせください。

ネットワーク接続の問題によりアプリケーションの起動に失敗しました

情報コード**:** 0x10000401

コネクタアプライアンスとセキュアプライベートアクセスサービス間の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

1. コネクタ アプライアンスのパブリック 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どうかを確認します。
3. プロキシが問題の原因となっている場合は、プロキシをバイパスしてアプリの起動を再度試してください。

4. コネクタアプライアンスの正常性ステータスを確認します (**Citrix Cloud >** リソースの場所)。

ネットワーク設定の詳細については、コネクタ アプライアンスのネットワーク設定を参照してください。

コネクタアプライアンスがセキュアプライベートアクセスサービスに登録できませんでした

情報コード**:** 0x10000402, 0x1000040C

1. コネクタ アプライアンスの管理ページに移動し、コネクタの概要を確認します。
2. コネクタの状態が良好でない場合は、管理ポータルのリソースの場所へ移動します。
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. 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、ヘルスチェックを再度実行します。

ネットワーク設定の詳細については、コネクタ アプライアンスのネットワーク設定を参照してください。

コネクタアプライアンスとの接続の問題

情報コード**:** 0x10000403、0x10000404、0x10000407、0x1000040A、0x1000040B、0x1000040F、0x10000410

- エラー コードのトランザクション ID を検索します。
- Secure Private Access ダッシュボードでトランザクション ID に一致するすべてのイベントをフィルターします。
- トランザクション ID に一致する他のコンポーネントでエラーが発生したかどうかを確認し、見つかった場合は、そのエラー コードに一致するそれぞれの回避策を実行します。
- 他のコンポーネントにエラーが見つからない場合は、次の操作を実行します。
  - コネクタ アプライアンス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てください。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、「ネットワーク接続を確認する」を参照してください。
- この診断レポートとパケット トレースをエラー コードとトランザクション ID とともに Citrix サポートに問い合わせてください。

コネクタアプライアンスと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

コネクタ アプライアンスには、バックエンドのプライベート TCP/UDP サーバーとの接続の問題があります。

- 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おり、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 サーバーの到達可能性を確認します。
- 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ようにブロックされていないかどうかを確認します。
- FQDN ベースのアプリを要求している場合は、DNS サーバー内のそれぞれのアプリの DNS エントリを確認します。

コネクタアプライアンスが **FQDN** の **DNS** を解決できない

情報コード**:** 0x10000406

- DNS サーバーでそれぞれのアプリ FQDN の DNS エントリを確認します。
- コネクタ アプライアンスに適切な 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、「コネクタ アプライアンス管理ページでのネットワーク設定の構成」を参照してください。

プライベートサーバーの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ます。
2. このログのトランザクション ID に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 サポートに連絡してください。

プライベート サービス **IP** または **FQDN** への接続またはデータの送信に失敗しました

情報コード**:** 0x10000413

- プライベートサーバーの接続が終了しました
- [コネクタ アプライアンスと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](/en-us/citrix-secure-private-access/service/secure-private-access-troubleshooting。html#connectivity-issues-with-connector-appliance-and-backend-private-tcpudp-servers を参照してください。ルーティング ドメイン エントリを確認します。IP アドレスが有効であり、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。

一致するポリシー条件がありません

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たアクセス 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構成を更新します。

アプリケーションに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 サービスの 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ます。
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 サポートにお問い合わせください。

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

着信 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ケーションとして分類されます。これが予想外の場合は、次の操作を行ってください。

1. Secure Private Access サービスの管理ポータルに移動します。
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. アプリケーションに FQDN または IP アドレスを追加します。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。

   注意**:** セキュア プライベート アクセス **>** 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。

アプリの列挙情報

情報コード**:** 0x10050C

このコードは、ユーザーが権限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をキャプチャします。次の理由によりアプリへのアクセスが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、「一致するポリシー条件がありません」を参照してください。
- アプリケーションにアクセス ポリシーが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アクセス ポリシーが関連付けられていません」を参照してください。
- アプリケーションに関連付けられたポリシーはアクセスを拒否するように構成されています。この場合、意図されたとおりにアクションは必要ありません。
- 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 エントリが見つからないか、以前に削除されている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 (セキュア プライベート アクセス **>** 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、どのコネクタも起動しておらず、新しい接続に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。

コネクタに到達できないため、**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。

NGS クッキー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 サポートにお問い合わせください。

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 サポートにお問い合わせください。

JSON Web トークンの解析中にアクセス ポリシーの取得に失敗しました

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 サポートにお問い合わせください。

アクセス ポリシーの詳細を取得するためのネットワーク障害

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どうかを確認します。
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 サポートにお問い合わせください。

公開証明書の取得中にポリシーの取得に失敗しました

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 サポートにお問い合わせください。

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. ネットワーク時間とユーザーデバイスの時間が同期されているかどうかを確認します。
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 サポートにお問い合わせください。

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 サポートにお問い合わせください。

ポリシー **URL** を形成するためのストア環境を判別できませんでした

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 サポートにお問い合わせください。

アクセス ポリシー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 サポートにお問い合わせください。

セカンダリ **DS** 認証トークンの有効期限が切れたため、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 サポートにお問い合わせください。

コネクタアプライアンスが登録されていません

情報コード**:** 0x10200002

コネクタアプライアンスの登録を確認します。

詳細については、「コネクタアプライアンスを Citrix Cloud に登録する」を参照してください。

コネクタアプライアンスに接続できません

情報コード**:** 0x10200003

コネクタアプライアンスは、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。

詳細については、「コネクタアプライアンスを Citrix Cloud に登録する」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

コネクタアプライアンスのネットワーク設定を確認します。詳細については、コネクタ アプライアンスのネットワーク設定 を参照してください。

プロキシサーバーにアクセスできません

情報コード**:** 0x10000303, 0x10000304

プロキシ サーバーの設定を確認し、コネクタ アプライアンスに到達可能であることを確認します。詳細については、「コネクタアプライアンスを Citrix Cloud に登録する」を参照してください。

プロキシサーバーの認証に失敗しました

情報コード**:** 0x10000305

プロキシ サーバーの資格情報を確認し、コネクタ アプライアンス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、コネクタ アプライアンスを登録した後の を参照してください。

設定されたプロキシサーバーにアクセスできません

情報コード**:** 0x10000306

コネクタ アプライアンスのネットワーク設定、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、次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 コードが予期されるコードでない場合は、それを確認します。

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、コネクタ アプライアンスのネットワーク設定を確認してください。詳細については、コネクタ アプライアンスのネットワーク設定 を参照してください。

SSO の処理に失敗しました

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でした。

コネクタ アプライアンスのネットワーク設定を確認し、NTP サーバーが構成されており、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、コネクタ アプライアンスのネットワーク設定 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

コネクタアプライアンスのネットワーク設定を確認します。詳細については、コネクタ アプライアンスのネットワーク設定 を参照してください。

SSO の処理に失敗しました。**SSO** 設定を判別できません

情報コード**:** 0x1000010A

SSO 構成を確認し、サーバーがコネクタ アプライアンスに到達可能であることを確認します。

FormFill SSO に失敗しました。フォーム アプリの構成が正しくありません

情報コード**:** 0x10000101、0x10000102、0x10000103、0x10000104

SSO フォーム アプリの構成を確認し、ユーザー名、パスワード、アクション、およびログイン URL フィールドがアプリ設定で正しく構成されていることを確認します。

Kerberos SSO に失敗しました

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を設定する」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 コントローラからの Kerberos チケットの取得に失敗しました。セカンダリ認証として、コネクタ アプライアンスはフォールバック NTLM 認証を試みました。

Kerberos 認証を正常に行うには、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** 権限アカウント

情報コード**:** 0x14000001

Citrix Workspace アプリケーションで、ZTNA 資格を持つアカウントを 1 つだけ構成します。

クライアントログを収集する方法

- **Windows** クライアント:
  1. アプリを開き、ログ記録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、直面している問題を再現します。
  3. アプリで、ログ記録 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. アプリを開き、ログ **>** 詳細に移動します。
  2. ログをクリアして、問題の再現を続行します。
  3. ログ **>** エクスポート ログに戻ります。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**?**

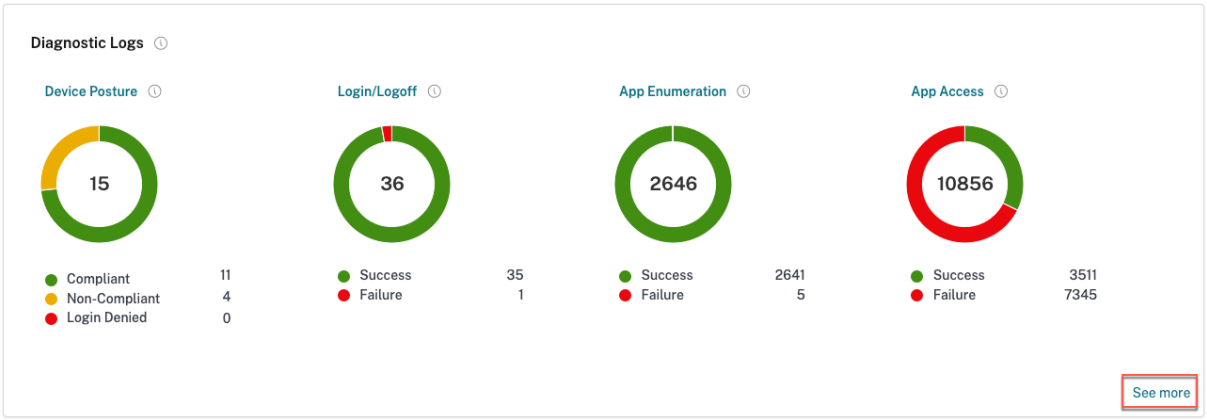
Secure Private Access 診断ログは、ユーザーが任意のアプリケーション (Web/SaaS/TCP/UDP) にアクセスしたときに発生するすべてのイベントをキャプチャします。これらのログには、デバイスの状態、アプリの認証、アプリの列挙、アプリのアクセス ログが記録されます。詳細は表形式で表示されます。事前に設定した時間またはカスタム タイムラインのログを表示できます。ダッシュボードに表示する情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログを CSV 形式でエクスポートできます。

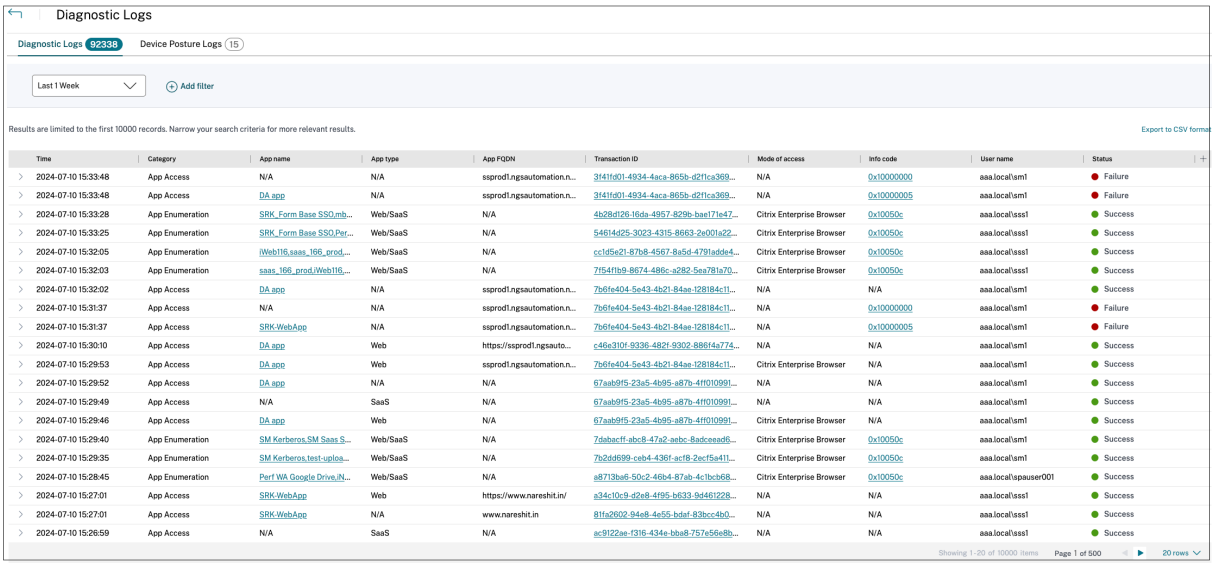
セキュア プライベート アクセス ログはどこにありますか**?**

1. Citrix Cloud にログオンします。
2. Secure Private Access サービス 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で、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 診断ログを表示するウィジェットはどれですか**?**

ログ記録とトラブルシューティング セクションの 診断ログ ウィジェットには、認証、アプリケーションの起動、アプリの列挙に関連するすべての Secure Private Access イベントと、デバイスの状態に関連するログの円グラフ ビューが表示されます。Secure Private Access 診断ログは、エンドユーザーがアプリケーションにアクセスしたときに各コンポーネントからイベントを送信する複数の内部コンポーネントからイベントを取得します。これらのイベントは、ログイン/ログオフ、アプリ列挙、および アプリアクセスのカテゴリに分かれています。円グラフには、各カテゴリの全体的な成功/失敗の比率が表示されます。任意のグラフ上の色付きの円グラフをクリックすると、適切なイベントを見つけることができる診断ログが表示されます。デバイス ポスチャ サービスが有効になっている場合は、デバイス ポスチャ ログもあります。完全な診断ログを表示するには、[詳細を表示] リンクをクリックすることもできます。





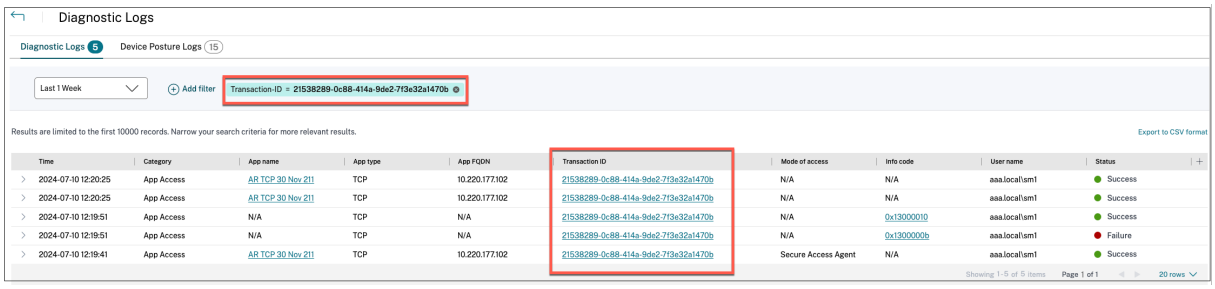
Secure Private Access 診断ログにはどのような詳細が記載されていますか**?**

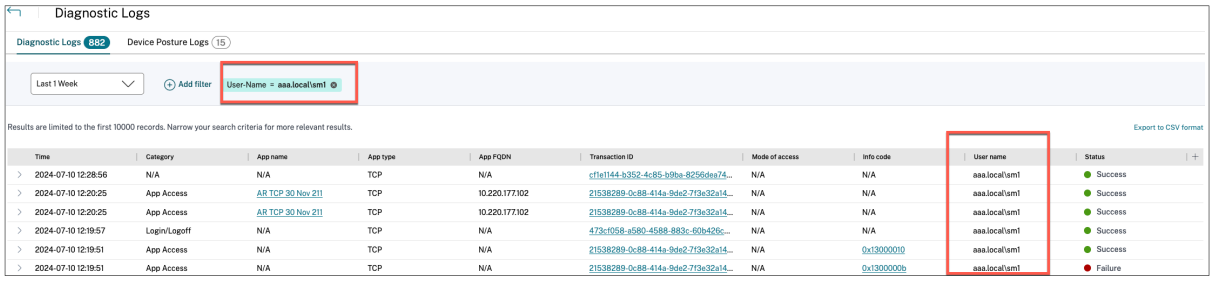
Secure Private Access ユーザー ログ ダッシュボードには、デフォルトで次の詳細が表示されます。

- 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アクセス ポリシーの名前を表示します。
- ステータス - イベントのステータス（成功、失敗）を表示します。
- 情報コード - 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、関連付けられた情報コードがあります。情報コードで詳細をご覧ください。
- 説明 - 失敗の理由またはイベントの詳細を表示します。
- **APP FQDN**: アクセスし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付けられたイベント タイプを表示します。
- 操作タイプ - ログが生成される操作を表示します。
- カテゴリー - イベントの種類に応じて 3 つのカテゴリーが利用できます。つまり、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すると、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 は、アクセス要求のすべての Secure Private Access ログを関連付けます。トランザクション ID の使用方法を学びます。ダッシュボードの右端にある + ボタンをクリックすると、次の詳細を取得できます。
- **SPA PoP** ロケーション - アプリ アクセス中に使用された Secure Private Access サービス PoP ロケーションの名前/ID を表示します。セキュアプライベートアクセス PoP の場所を参照してください。

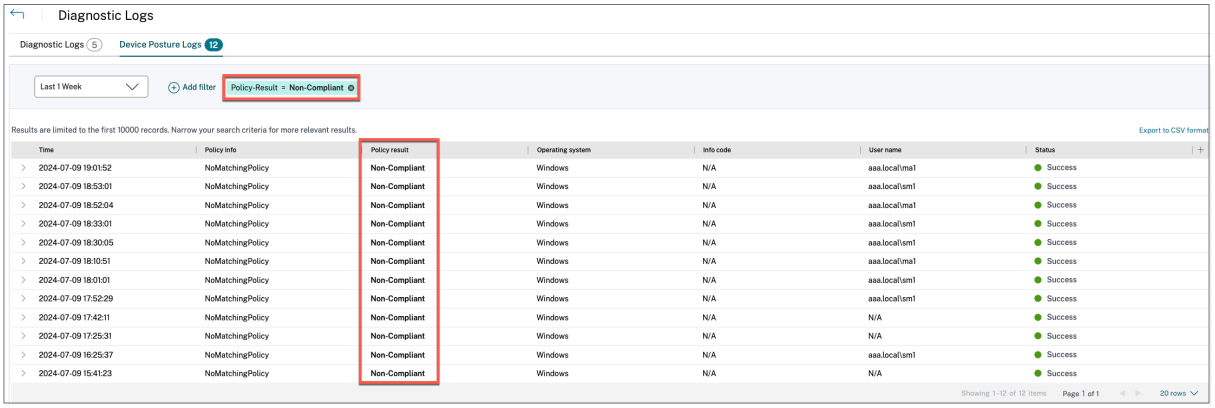
診断ログをフィルタリングするにはどうすればよいですか**?**

フィルターの追加 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基準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、トランザクション ID、= (ある値に等しい) をクリックし、21538289-0c88-414a-9de2-7f3e32a1470b 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。





さまざまなフィルター オプションを使用して、デバイス ポスチャ ログの検索を絞り込むこともできます。



Secure Private Access 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 診断ログには、次のイベントが記録されます。

- デバイスの状態**:** エンドユーザーのデバイスのステータス。これらのログには、デバイスの姿勢結果に関する情報が記録されます。デバイス ポスチャ ポリシーに基づいて、デバイスが準拠、非準拠、またはアクセス拒否と判断されたかどうか。

- 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状態、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。
- アプリの列挙: Secure Private Access サービスでは、管理者が構成したアクセス 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 App 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 サービス内で構成されたアクセス ポリシーに基づいて、ユーザーへのアクセスが許可または拒否されたアプリケーションを知るのに役立ちます。
- アプリ アクセス: 選択した時間間隔で構成されたアクセス ポリシーに従って、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、および接続ステータスのイベント。

発生した障害を解決するために、**Secure Private Access** のトラブルシューティング トピックをどのように使用すればよいですか**?**

1. 解決しようとしている障害の 情報コード を取得します。
2. エラー検索テーブルで情報コードを見つけます。
3. その情報コードに提供されている解決手順に従ってください。

情報コードとは何ですか**?** 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、関連付けられた情報コードがあります。解決手順やそのイベントに関する詳細情報を見つけるには、エラー検索テーブル 内でこの情報コードを検索してください。

トランザクション **ID** とは何ですか**?** どうやって使うんですか

Citrix Enterprise Browser 経由のアクセス失敗/問題が発生すると、エンド ユーザーにトランザクション ID が表示されます。管理者は、エンドユーザーからこのトランザクション ID を取得し、このトランザクション ID を使用して問題の原因となった正確なログを フィルタリング することで、正確な問題を特定することができます。管理者がトランザクション ID を使用してイベントをフィルタリングすると、問題に関連するイベントのみが表示され、失敗や問題が発生した理由に関するすべての詳細が管理者に提供されます。管理者は、これらのログの エラー コード を使用して、問題をさらに解決できます。

セキュア プライベート アクセス **PoP** の場所とは何ですか**?**

以下は、セキュア プライベート アクセス PoP の場所の一覧です。

PoP 名	ゾーン	リージョン
az-us-e	Azure イースト	バージニア州
az-us-w	アズールウェストス	California
az-us-sc	アズール サウスセントララス	テキサス
az-aus-e	アズールオーストラリアイースト	ニューサウスウェールズ州
アズ・エウ・ン	アズール 北ヨーロッパ	アイルランド
az-eu-w	アズール 西ヨーロッパ	オランダ
az-jp-e	アズールジャパン	東京、埼玉
az-bz-s	アズールブラジルサウス	サンパウロ州
アジア	アズール東南アジア	シンガポール
アラブ首長国連邦	アズールアラブ首長国連邦	ドバイ
az-in-s	アズール 南インド	チェンナイ
アジア香港	アズールイースタシア	香港

情報コードとエラー参照テーブルを使用しても障害を解決できない場合はどうすればよいですか**?**

Citrix サポートにお問い合わせください。

参照ドキュメント

- **Web** アプリを追加する
  - エンタープライズウェブアプリのサポート
  - 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 サーバー固有の構成
- 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
- アクセスポリシーを作成する
  - アクセスポリシーを作成する
- ルートテーブル

- ルートテーブル

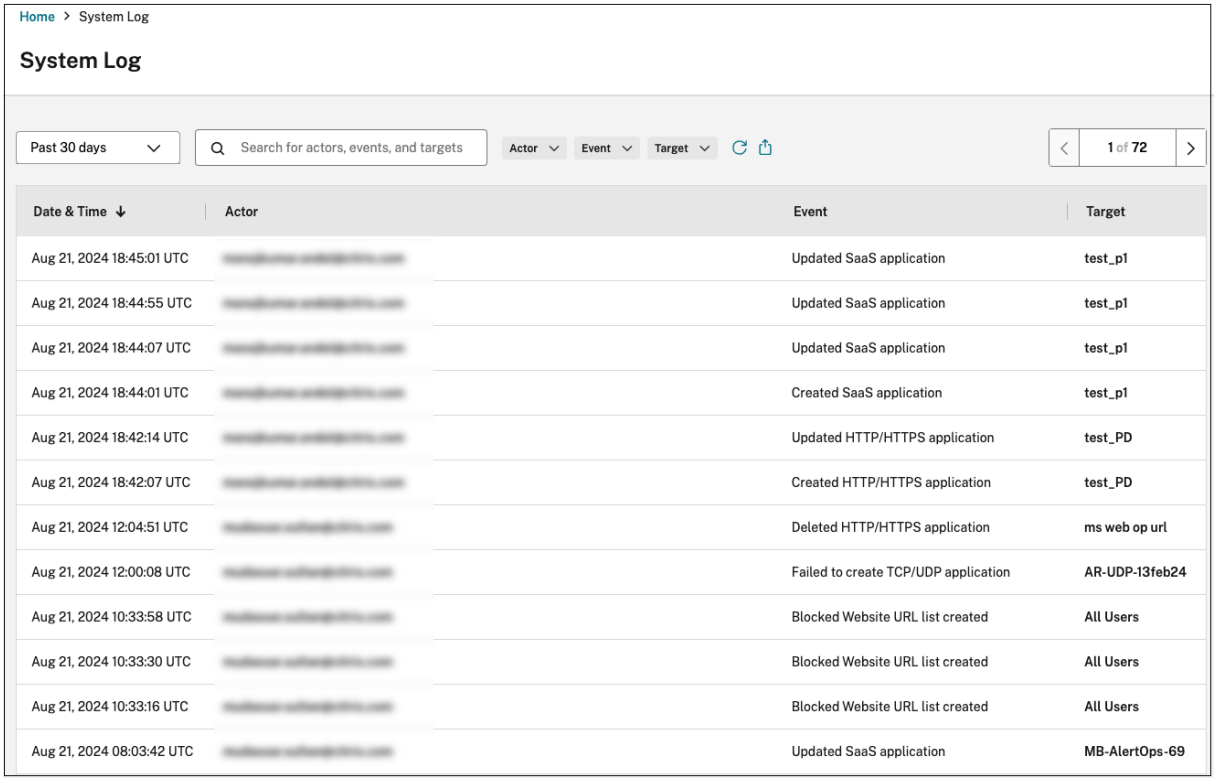
監査ログ

October 21, 2024

Secure Private Access サービス関連のイベントは、**Citrix Cloud >** システムログにキャプチャされます。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。管理者イベントには次のようなものがあります (ただし、これらに限定されません)。

- アプリの作成または更新
- アプリを削除する
- 適応型アクセスポリシーの設定または削除
- コネクタのアップグレード
- 許可またはブロックされたウェブサイトの作成

次の図は、システム ログ内のセキュア プライベート アクセス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、データの保持などの詳細については、「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

August 26, 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。

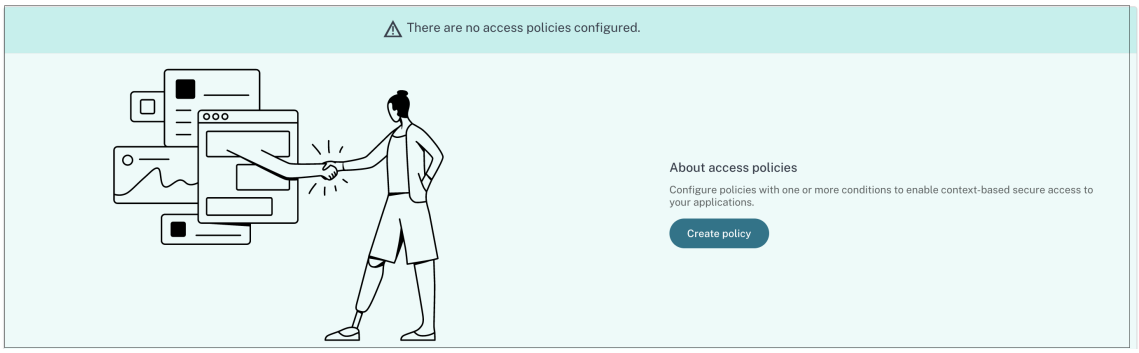
- クリップボードへのアクセスを制限する
- 印刷を制限
- ダウンロードを制限
- アップロードを制限する
- ウォーターマークを表示
- キーロギングを制限する
- 画面キャプチャを制限する

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」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。

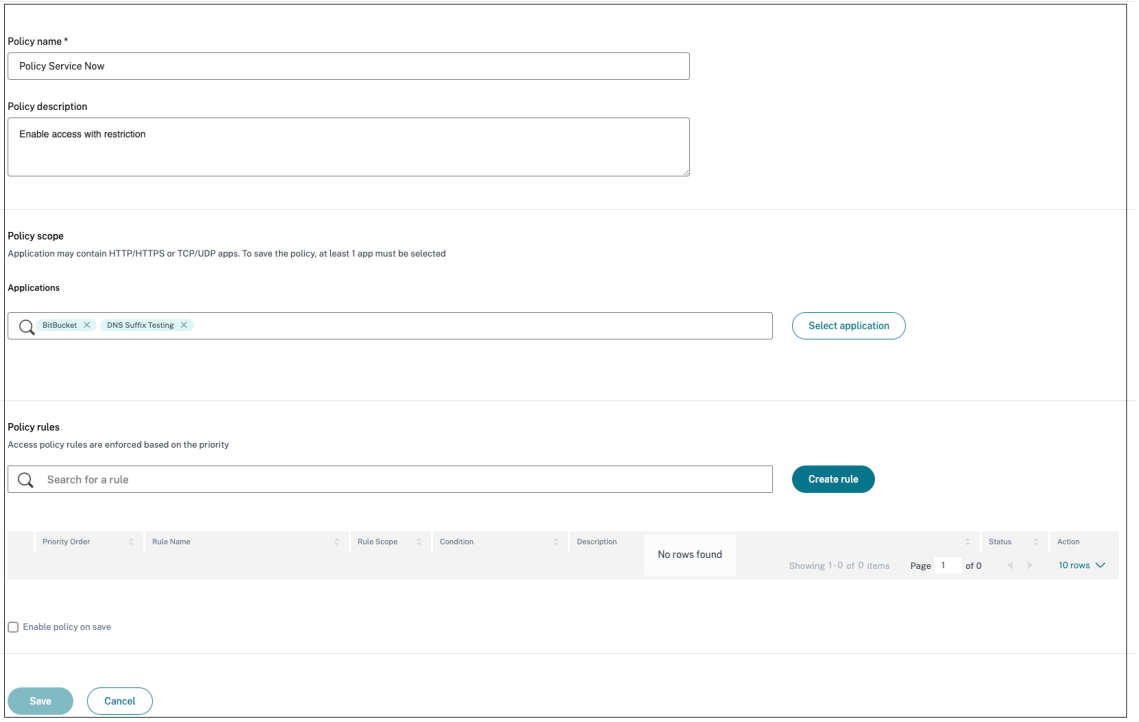
- ID と認証の設定
- 設定済みアプリケーション

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。

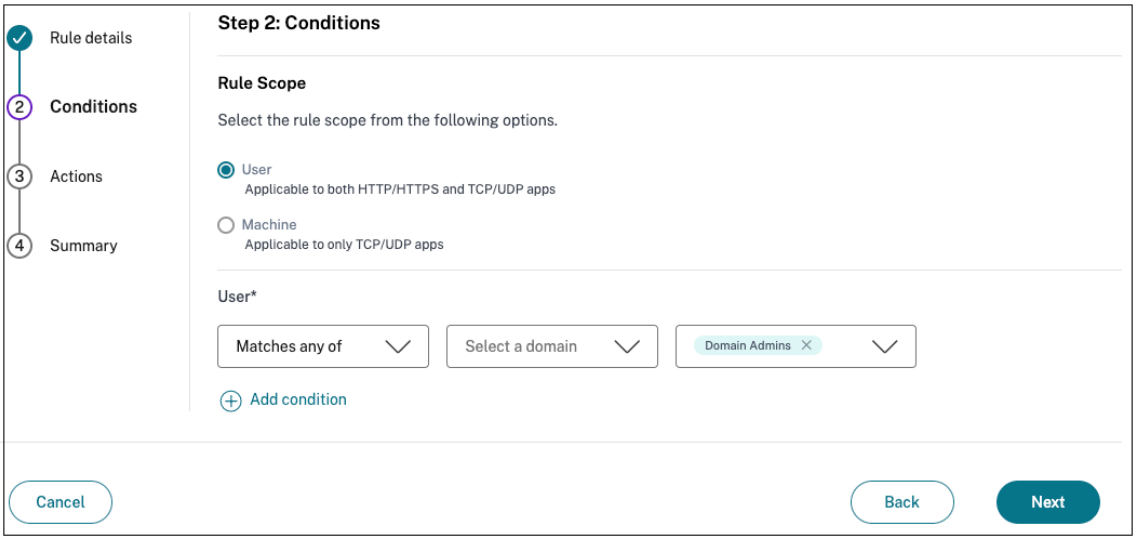


5. ルール名とルールの簡単な説明を入力して、[次へ] をクリックします。

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。

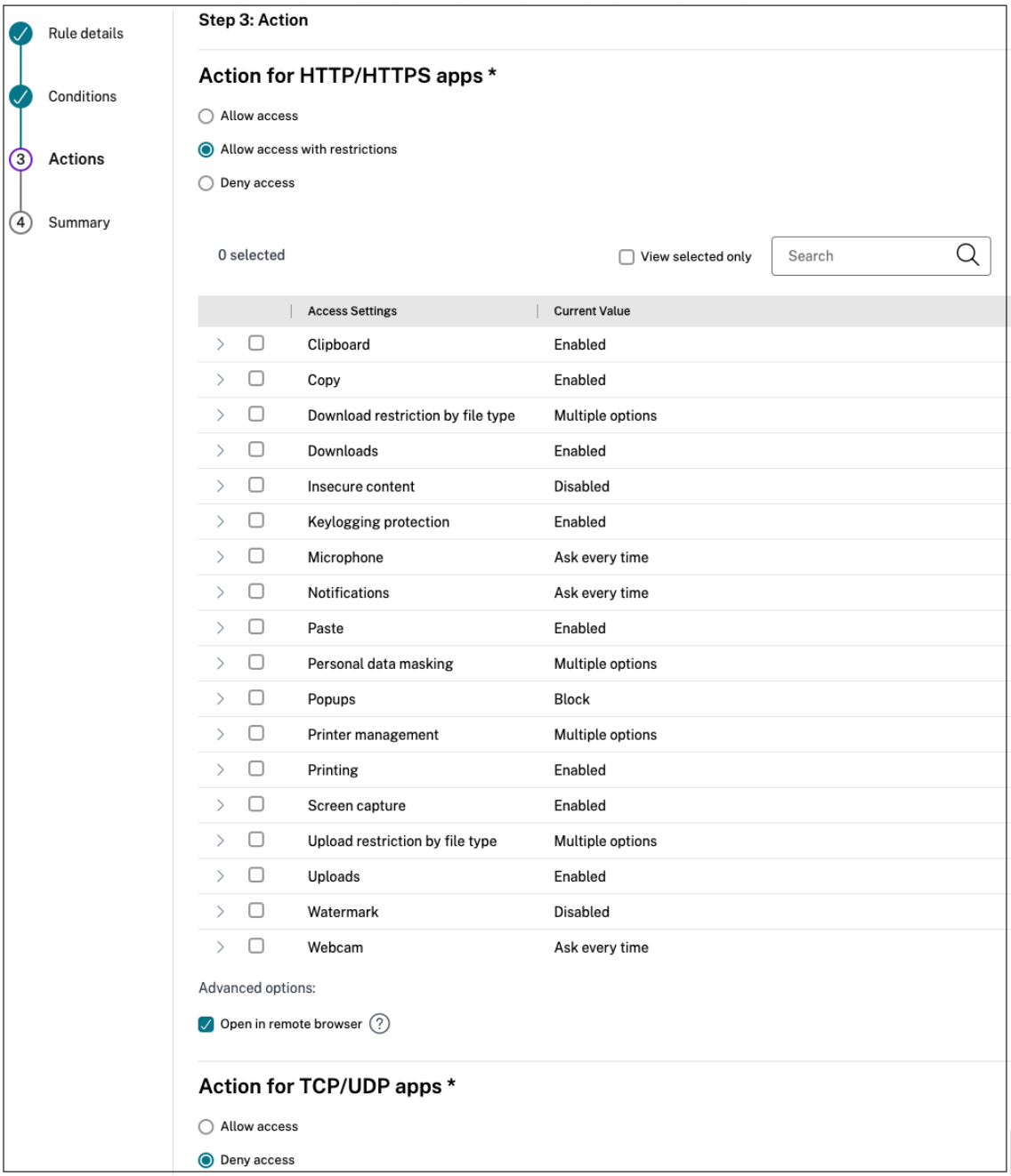
8. [次へ] をクリックします。

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。

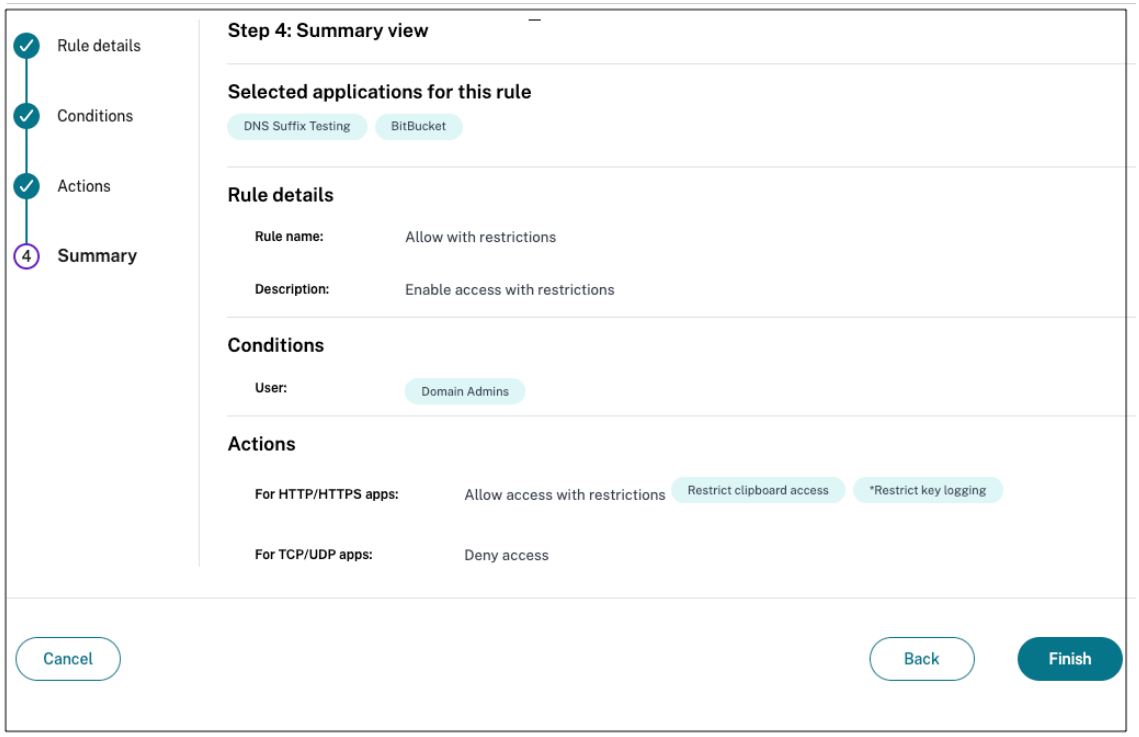
   - HTTP/HTTPS アプリの場合、以下を選択できます。
     - アクセスを許可
     - 制限付きでアクセスを許可
     - アクセスを拒否

   > 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

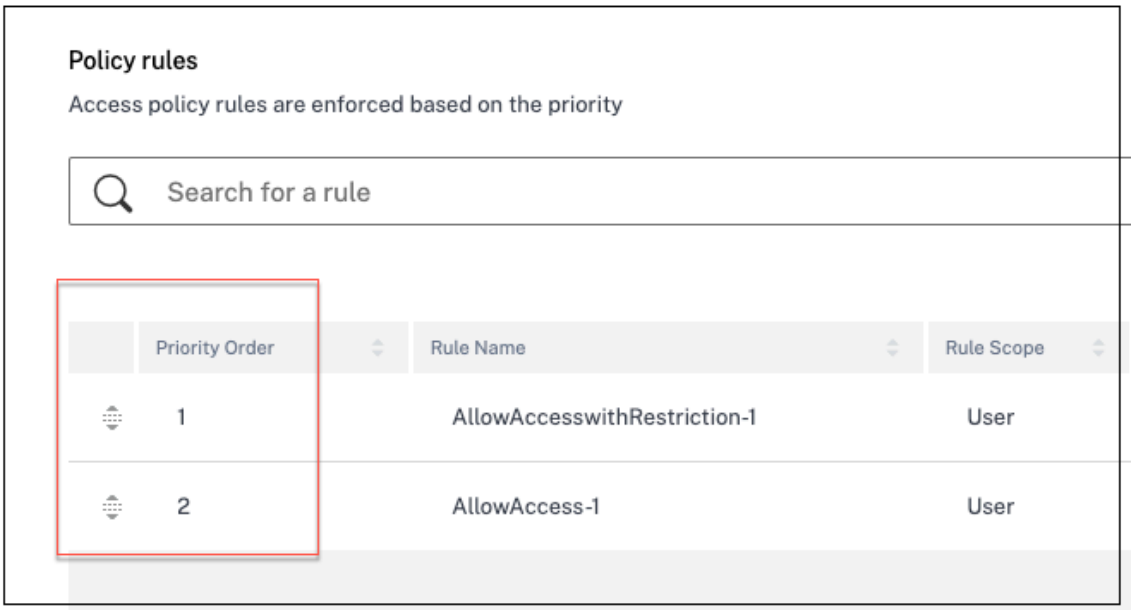


10. ［次へ］をクリックします。「概要」ページには、ポリシーの詳細が表示されます。
11. 詳細を確認して [完了] をクリックします。



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:
>
> 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

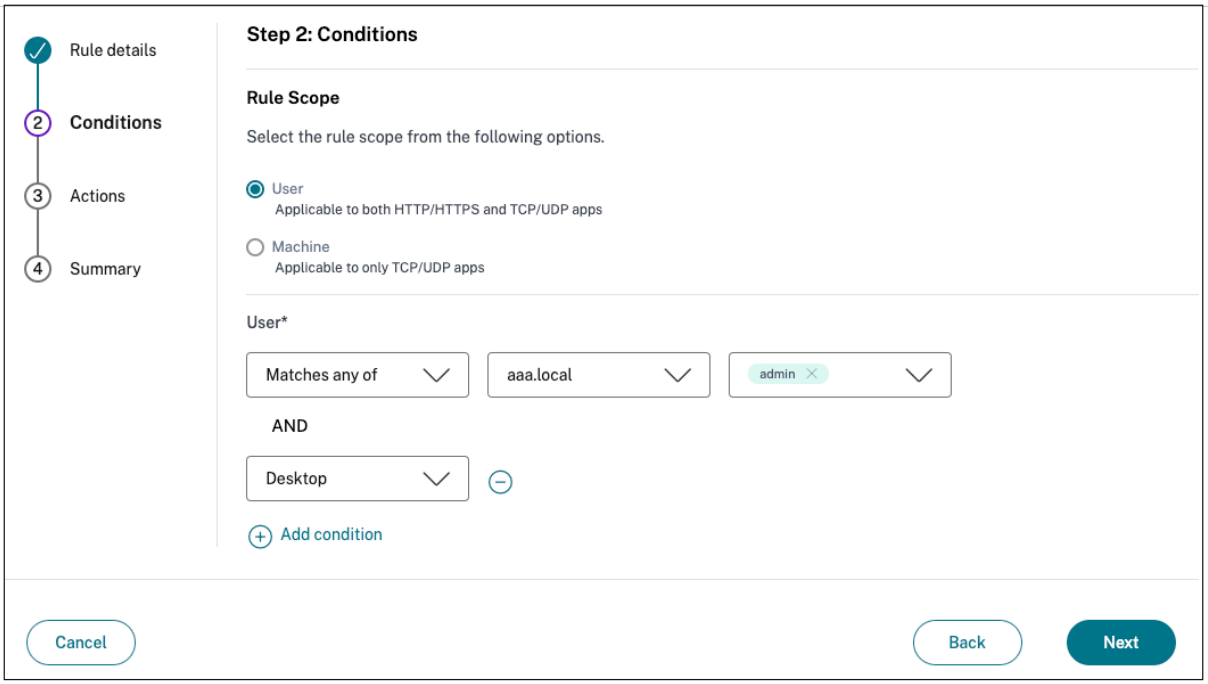
「制限付きアクセスを許可する」アクションを選択するときは、セキュリティ制限を少なくとも 1 つ選択する必要があります。これらのセキュリティ制限は、システムであらかじめ定義されています。管理者は、他の組み合わせを変更したり追加したりすることはできません。詳細については、「利用可能なアクセス制限オプション」を参照してください

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

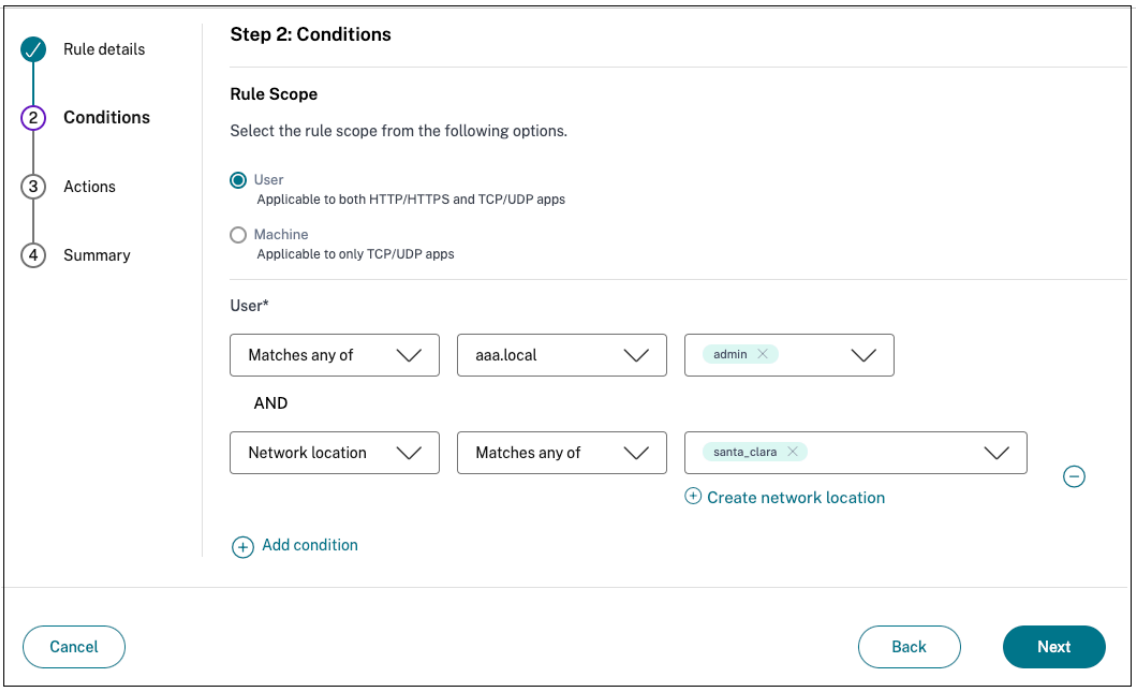
管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいて、アダプティブアクセスポリシーを設定できます。ロケーションは、ユーザーがアプリケーションにアクセスしている国またはユーザーのネットワークロケーションです。ネットワークの場所は、IP アドレス範囲またはサブネットアドレスを使用して定義されます。

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:

- **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

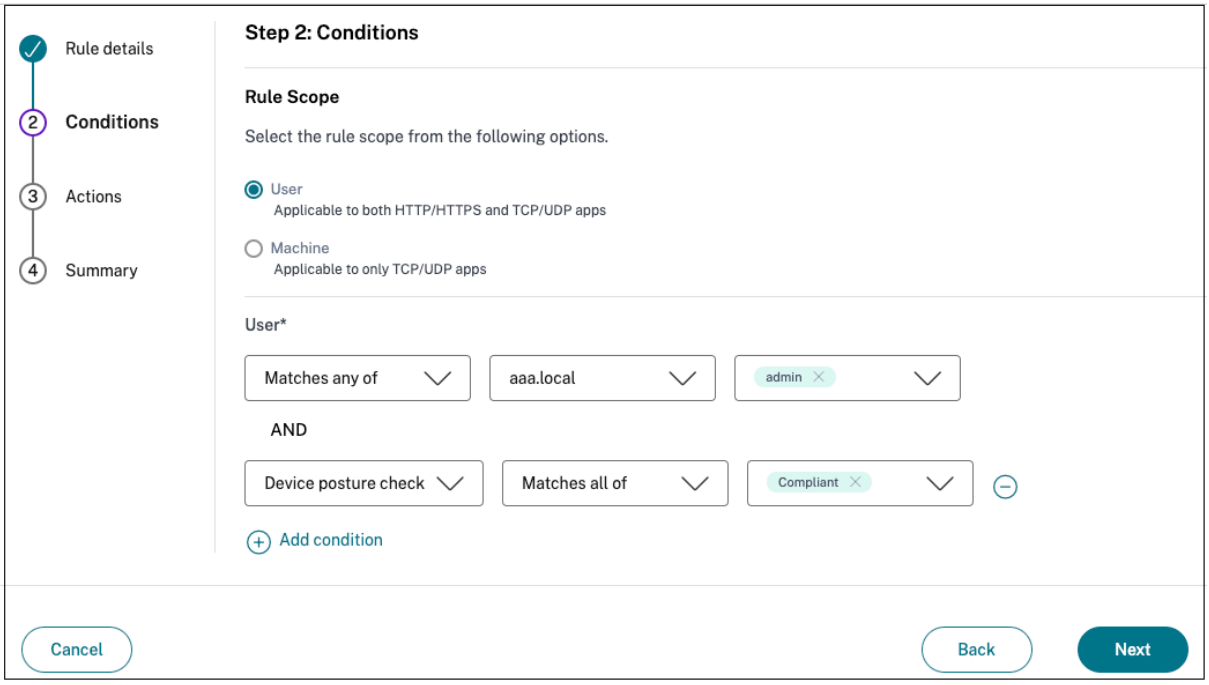
デバイスポスチャタグを使用してアクセス制御を強制するように Secure Private Access サービスを設定できます。デバイスポスチャ検証後にデバイスのログインが許可されると、そのデバイスは準拠または非準拠として分類できます。この情報は、Citrix DaaS サービスおよび Citrix Secure Private Access サービスにタグとして提供され、デバイスの状態に基づいてコンテキストアクセスを提供するために使用されます。

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。

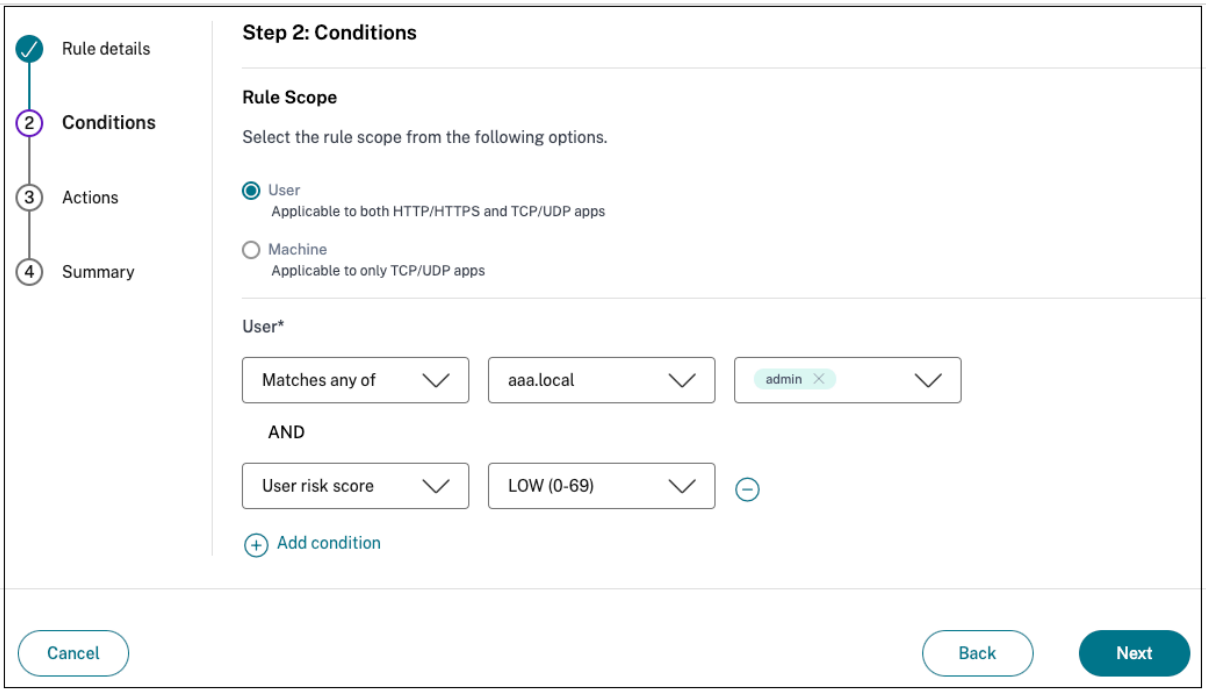
ユーザーリスクスコアは、企業内のユーザーアクティビティに関連するリスクを判断するためのスコアリングシステムです。リスク指標は、疑わしいと思われるユーザーアクティビティや、組織にセキュリティ上の脅威を与える可能性のあるユーザーアクティビティに割り当てられます。リスク指標は、ユーザーの行動が正常から逸脱したときにト

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:
    >
    > 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



同じ関連ドメインから生じる競合を解決するためのルートテーブル

October 21, 2024

Citrix Secure Private Access サービスのアプリケーション ドメイン機能を使用すると、顧客は、アプリケーションの関連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にルーティングできるようにするルーティング決定を行うことができます。

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構成しているとします。たとえば、Okta が Salesforce (SaaS アプリ) と Jira (内部 Web アプリ) の両方の SAML IdP である場合、管理者は両方のアプリの構成で関連ドメインとして `*.okta.com` を構成することがあります。これにより競合が発生し、エンド ユーザーは一貫性のない動作を経験することになります。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ためのルールを定義できます。

ルートテーブルの仕組み

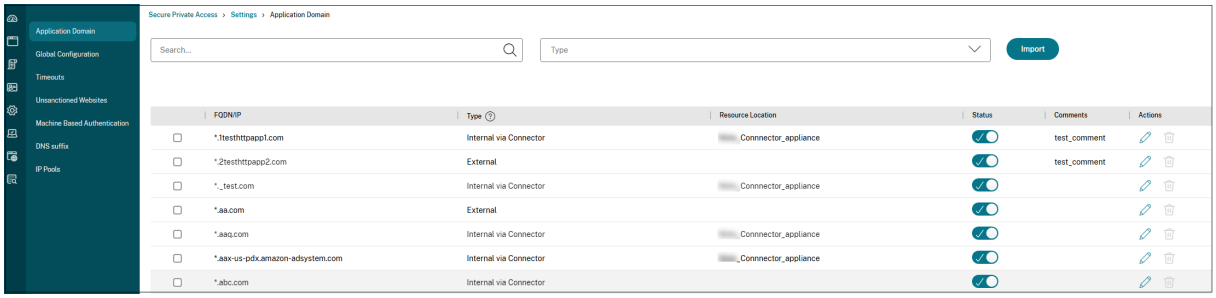
管理者は、トラフィック フローを定義する方法に応じて、アプリに対して次のルート タイプを定義できます。

- 内部–プロキシをバイパス - ドメイン トラフィックは、コネクタ アプライアンスで構成された顧客の Web プロキシをバイパスして、Citrix Cloud Connector を介してルーティングされます。
- コネクタ経由の内部 - アプリは外部にありますが、トラフィックはコネクタ アプライアンスを経由して外部ネットワークに流れる必要があります。
- 外部–トラフィックは直接インターネットに流れます。

> 注意:
>
> - 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 ポリシーに影響を与えません。
> - 管理者がルート テーブル内のエントリを使用するつもりがない場合、または対応するアプリが意図したとおりに動作していない場合は、管理者はエントリを削除するのではなく、単に無効にすることができます。
> - アプリの種類に関係なく、特定の顧客のすべてのコネクタ アプライアンスは SSO 設定を取得します。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。

メインルート表

Secure Private Access コンソールのメイン ルーティング テーブル (設定 **>** アプリケーション ドメイン) は、すべてのアプリケーションで構成されたドメインに関するすべての詳細を提供する表示専用のダッシュボードです。これを使用して、任意のドメインの次の情報を表示できます。



メイン ルート テーブルを使用すると、任意のドメインの次の情報を確認できます。

- **FQDN/IP:** トラフィック ルーティングの種類を構成する 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、内部–プロキシをバイパス、または 外部。

> 重要:
>
> 競合がある場合は、テーブル内のそれぞれの行に警告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。

- リソースの場所**:** タイプ 内部のルーティングのリソースの場所です。リソースの場所が割り当てられていない場合は、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。アイコンにマウスを合わせると、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**:** ステータス 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することができます。トグルスイッチをオフにすると、ルート入力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**:** コメントがある場合は表示します。
- 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 エントリの種類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。

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、アプリの構成中にルーティングの決定を行うことができます。Citrix Secure Private Access サービスのユーザー インターフェイスの **App Connectivity** セクションで使用できるミニ ルート テーブル。

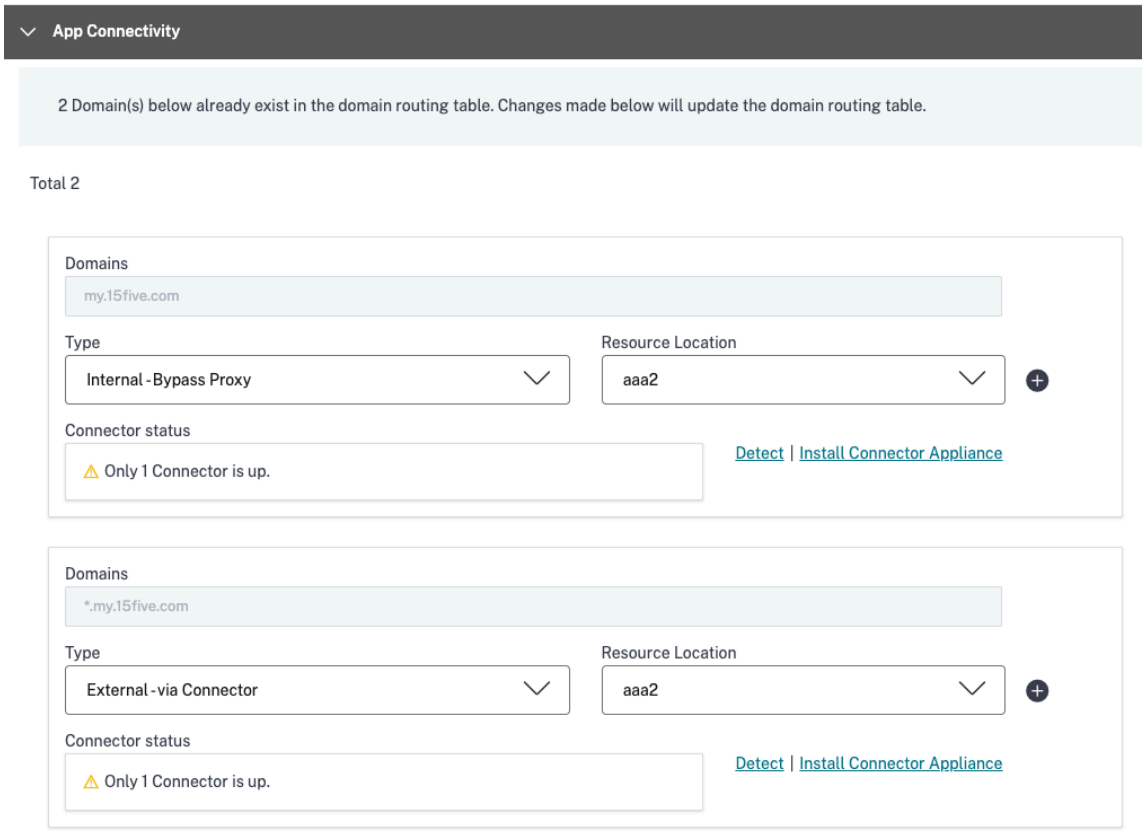
ミニルートテーブルにルートを追加するには

Citrix Secure Private Access サービスにアプリを追加する手順は、次の 2 つの変更を除いて、トピック 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 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、強化されたセキュリティの詳細を選択します。
   - 必要に応じて、シングル サインオンの方法を選択します。

2. アプリ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、アプリの構成中にルーティングの決定を行うことができます。



   - 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ときに入力した実際のアプリ URL が表示されます。他の行はすべて、アプリの詳細を追加するときに入力される関連ドメインです。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、1 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。
     - 内部–プロキシをバイパス - ドメイン トラフィックは、コネクタ アプライアンスで構成された顧客の Web プロキシをバイパスして、Citrix Cloud Connector を介してルーティングされます。
     - コネクタ経由の内部 - アプリは外部にありますが、トラフィックはコネクタ アプライアンスを経由して外部ネットワークに流れる必要があります。

  - 外部–トラフィックは直接インターネットに流れます。
- リソースの場所**:** アプリの種類として「内部」を選択すると自動的に入力されます。別のリソースの場所が必要な場合は変更してください。
- コネクタアプライアンスのステータス**:** アプリのタイプとして「内部」を選択すると、リソースの場所とともに自動的に入力されます。

非認可ウェブサイト

October 21, 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、「非承認 Web サイト」と見なされます。デフォルトでは、アプリケーションとアクセス ポリシーがアプリケーションに対して構成されていない場合、Secure Private Access は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。

アプリが構成されていないその他のすべてのインターネット URL または SaaS アプリケーションの場合、管理者は管理コンソールの 設定 **>** 未承認の **Web** サイト タブを使用して、Citrix Enterprise Browser 経由のアクセスを許可または拒否できます。管理者は、ブラウザベースの攻撃を防ぐために、アクセスをリモート ブラウザ分離 (RBI) 環境にリダイレクトすることもできます。管理者が URL を RBI にリダイレクトするように設定している場合は、次のアクションが発生します。

1. Secure Private Access はドメインを変換します。
2. 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。

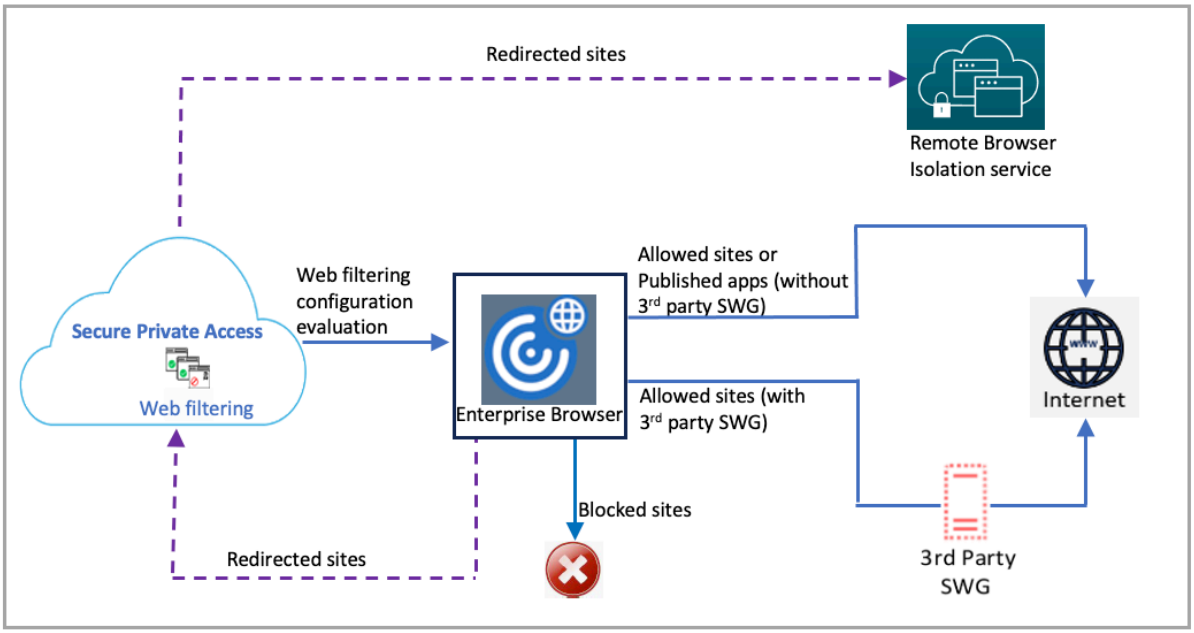
`*.example.com`などのワイルドカードを使用して、その Web サイト内のすべてのドメインとそのドメイン内のすべてのページへのアクセスを制御できます。

> 注意**:**
>
> 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。

非認可ウェブサイトの仕組み

1. URL が Citrix サービス URL であるかどうかを判断するために、URL 分析チェックが実行されます。
2. 次に、URL がチェックされ、エンタープライズ Web または SaaS アプリの URL であるかどうかが判断されます。
3. 次に、URL がチェックされ、ブロックされた URL として識別されるか、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、または URL へのアクセスを許可できるかが判断されます。

次の図は、エンド ユーザーのトラフィックのフローを説明しています。

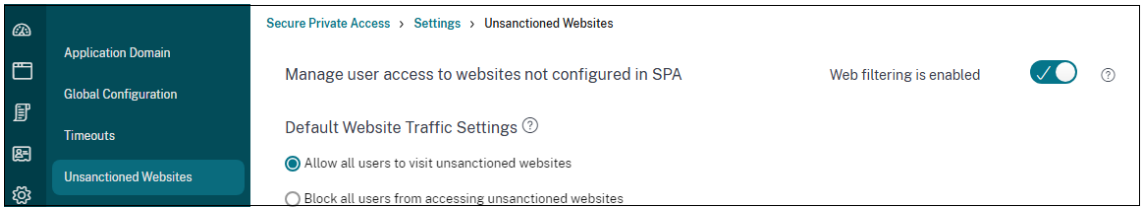


リクエストが到着すると、次のチェックが実行され、対応するアクションが実行されます。

1. リクエストはグローバル許可リストと一致していますか?
   a) 一致する場合、ユーザーは要求された Web サイトにアクセスできます。
   b) 一致しない場合は、Web サイトのリストがチェックされます。
2. リクエストは構成された Web サイト リストと一致しますか?
   a) 一致した場合、次のシーケンスによってアクションが決定されます。
      i. 禁止
      ii. リダイレクト
      iii. 許可
   b) 一致しない場合は、デフォルトのアクション (ALLOW) 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。

許可されていないウェブサイトのルールを設定する

1. Secure Private Access コンソールで、設定 **>** 未承認の **Web** サイトをクリックします。



注意:

- 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許可されていない **Web** サイトにアクセスするのをブロック に変更すると、すべてのユーザーに対して Citrix Enterprise Browser 経由のインターネット URL へのアクセスがブロックされます。

```
1  ![ルールの構成](/en-us/citrix-secure-private-access/media/spa-enable-
       website-list-filtering.png)
2
3  特定の URL をブロックされた Web サイト、許可された Web サイトに追加したり、リモート ブラウザ分離リストにリダイレクトしたりすることで、特定の URL の設定を変更することもできます。
4
5  たとえば、すべての未承認 URL へのアクセスをデフォルトでブロックしていて、特定のインターネット URL へのアクセスのみを許可する場合は、次の手順に従います。
6
7  1.  **許可された Web サイト** タブをクリックし、 **Web サイトの許可**をクリックします。
8  1.  アクセスを許可する Web サイトのアドレスを追加します。 ウェブサイトのアドレスを手動で追加するか、ウェブサイトのアドレスを含む CSV ファイルをドラッグ アンド ドロップすることができます。
9  1.  **URL の追加** をクリックし、 **保存**をクリックします。
10
11     URL が許可された Web サイトのリストに追加されます。
```

注意:

有料の Remote Browser Isolation Standard サービスの顧客 (組織) は、デフォルトで年間 5,000 時間の使用が許可されます。さらに長い時間使用するには、セキュア ブラウザ 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 アイソレーション 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。

注意事項

ユーザーが SaaS アプリにアクセスできない場合、Citrix Enterprise Browser からアプリケーションを起動することはできません。ただし、Citrix Enterprise Browser に URL を直接入力することで、アプリにアクセスできる可能性があります。

- ポリシーによってアプリへのアクセスが拒否された場合、**Web** フィルタリング 機能が有効になっていると、アプリケーションの URL がブロック リストに追加されます。これにより、Citrix Enterprise Browser 経由か URL 経由かを問わず、アプリにアクセスしようとする試みがすべてブロックされます。
- 未公開のアプリの場合、ルーティングが構成されている場合でも、これらのアプリへのアクセスは拒否されます。**Web** フィルタリング 機能が有効になっている場合、未公開アプリの URL はブロック リストに追加され、アクセス試行が防止されます。

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。

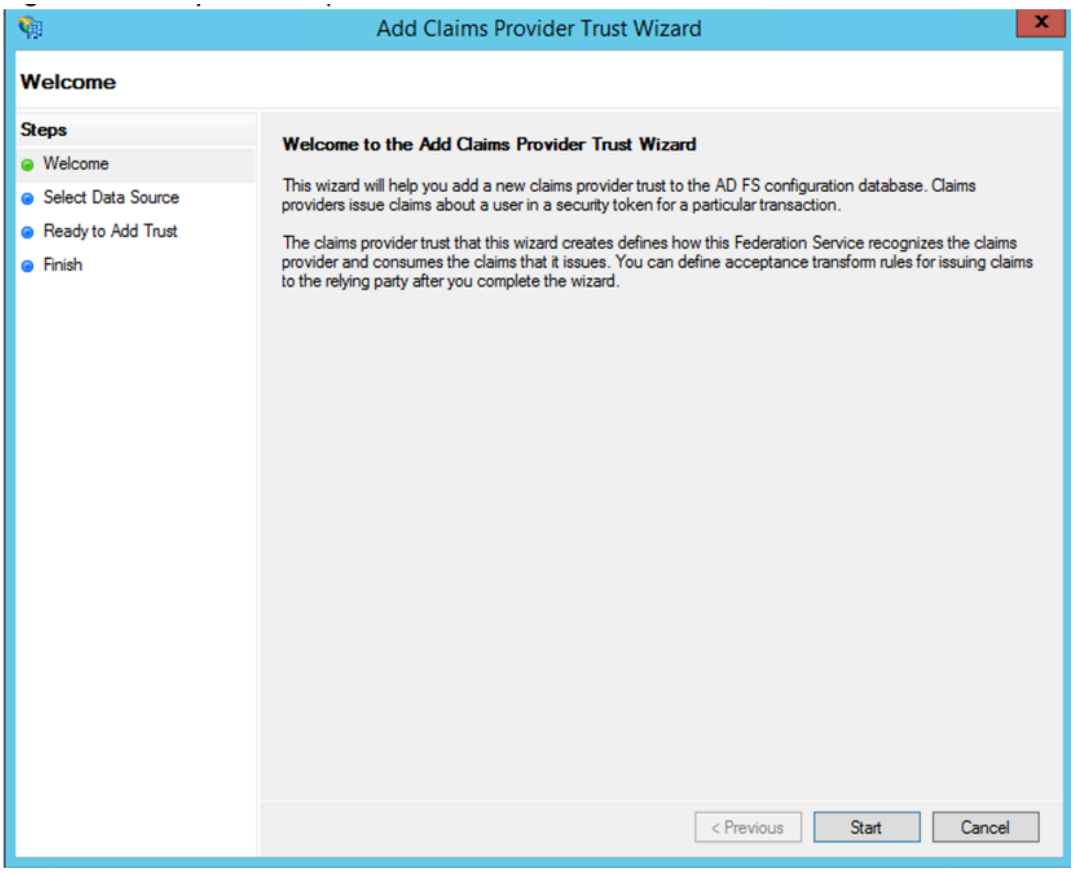
Citrix Secure Private Access からの要求を受け入れるように ADFS を設定するには、次の手順を実行する必要があります。

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

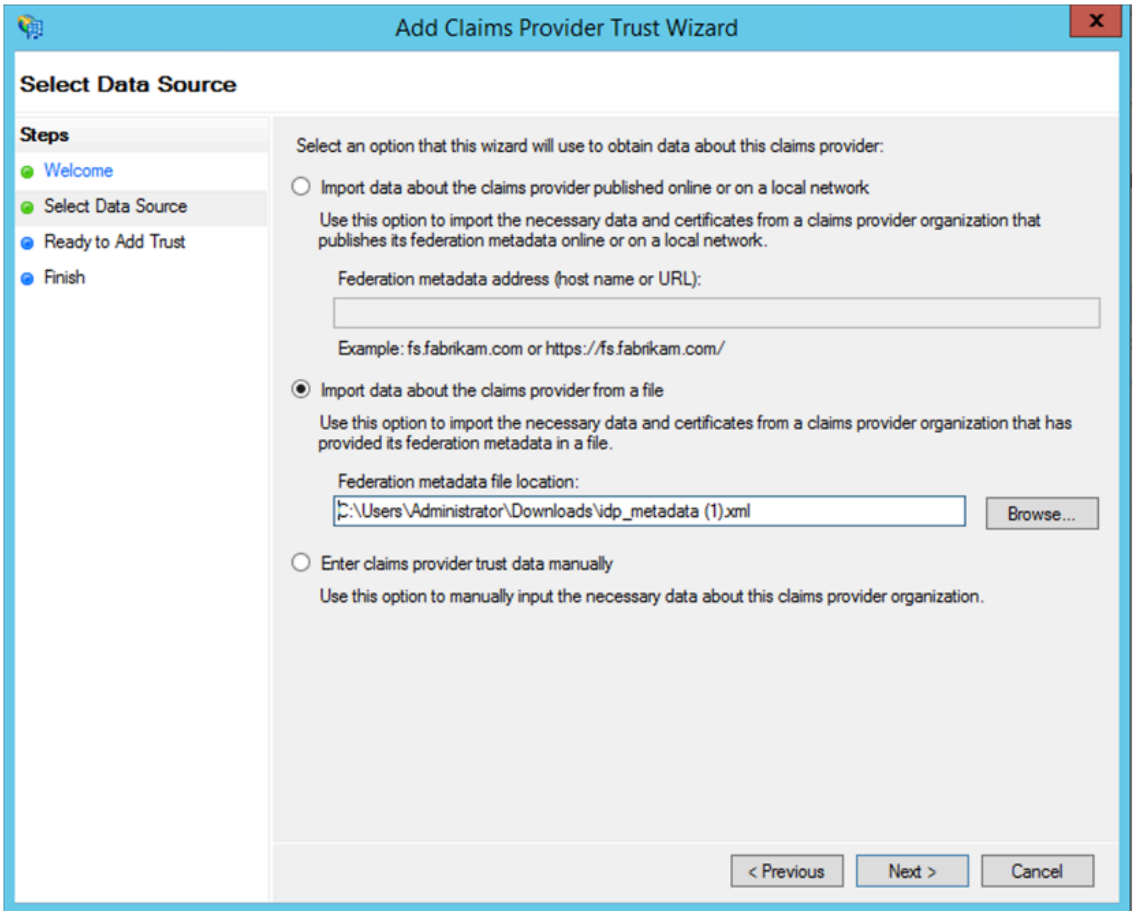
1. ADFS 管理コンソールを開きます。[**ADFS] > [**信頼関係**] > [**クレームプロバイダの信頼] に移動します。

    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。

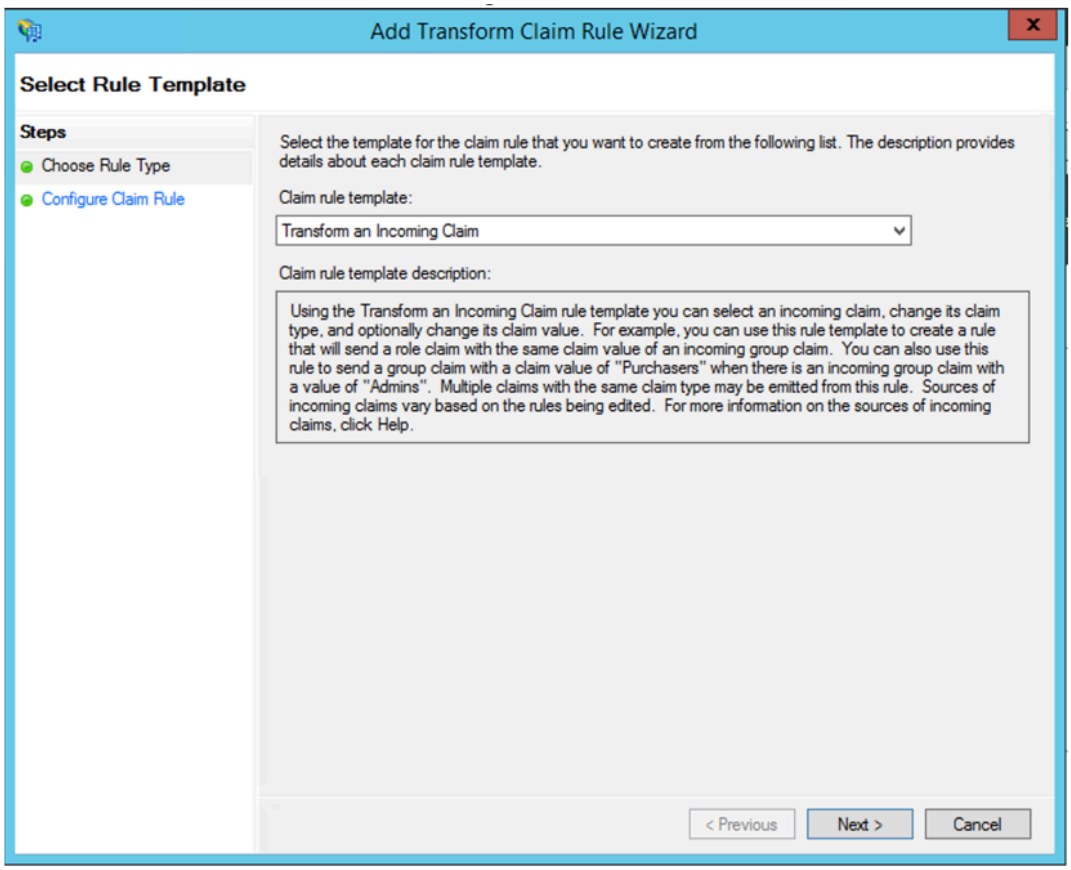


b) ADFS へのフェデレーションに使用されるアプリケーションを Secure Private Access に追加します。
詳しくは、「Citrix Secure Private Access でのアプリ構成」を参照してください。

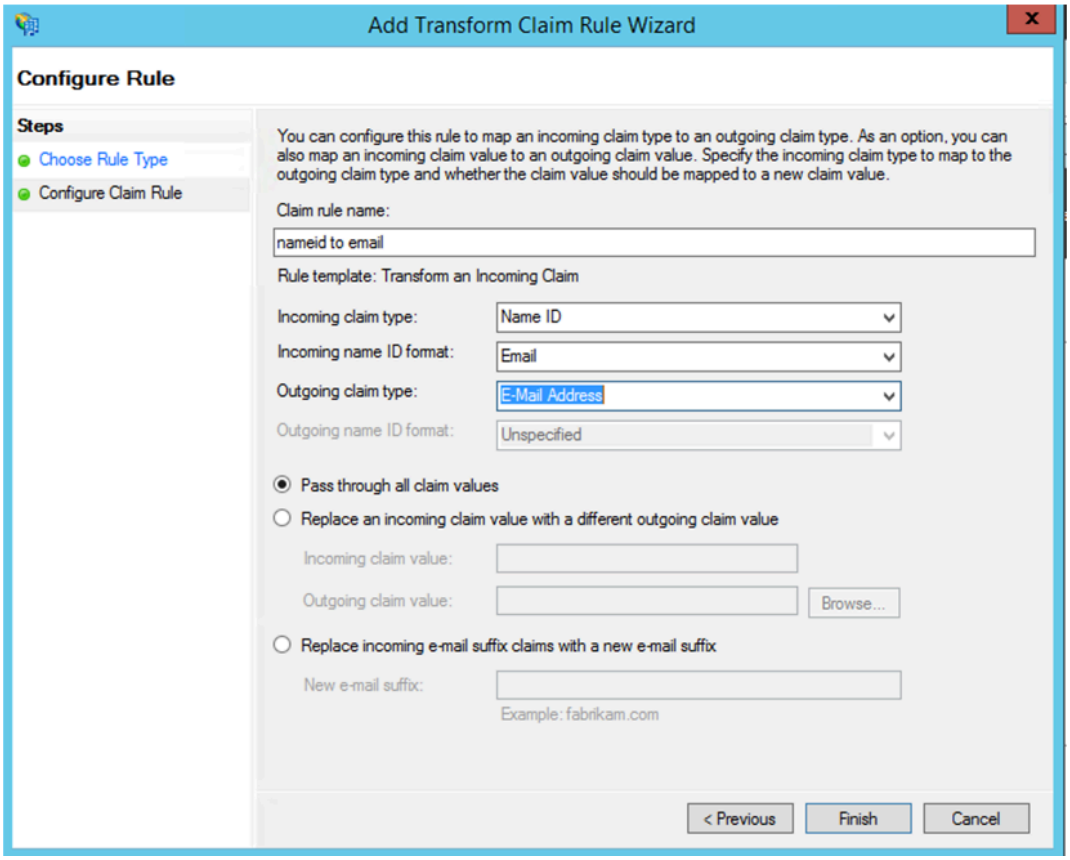
> 注:
>
> まずアプリを追加し、アプリケーションの SSO 設定セクションから SAML メタデータファイルをダウンロードし、メタデータファイルを ADFS にインポートします。



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。



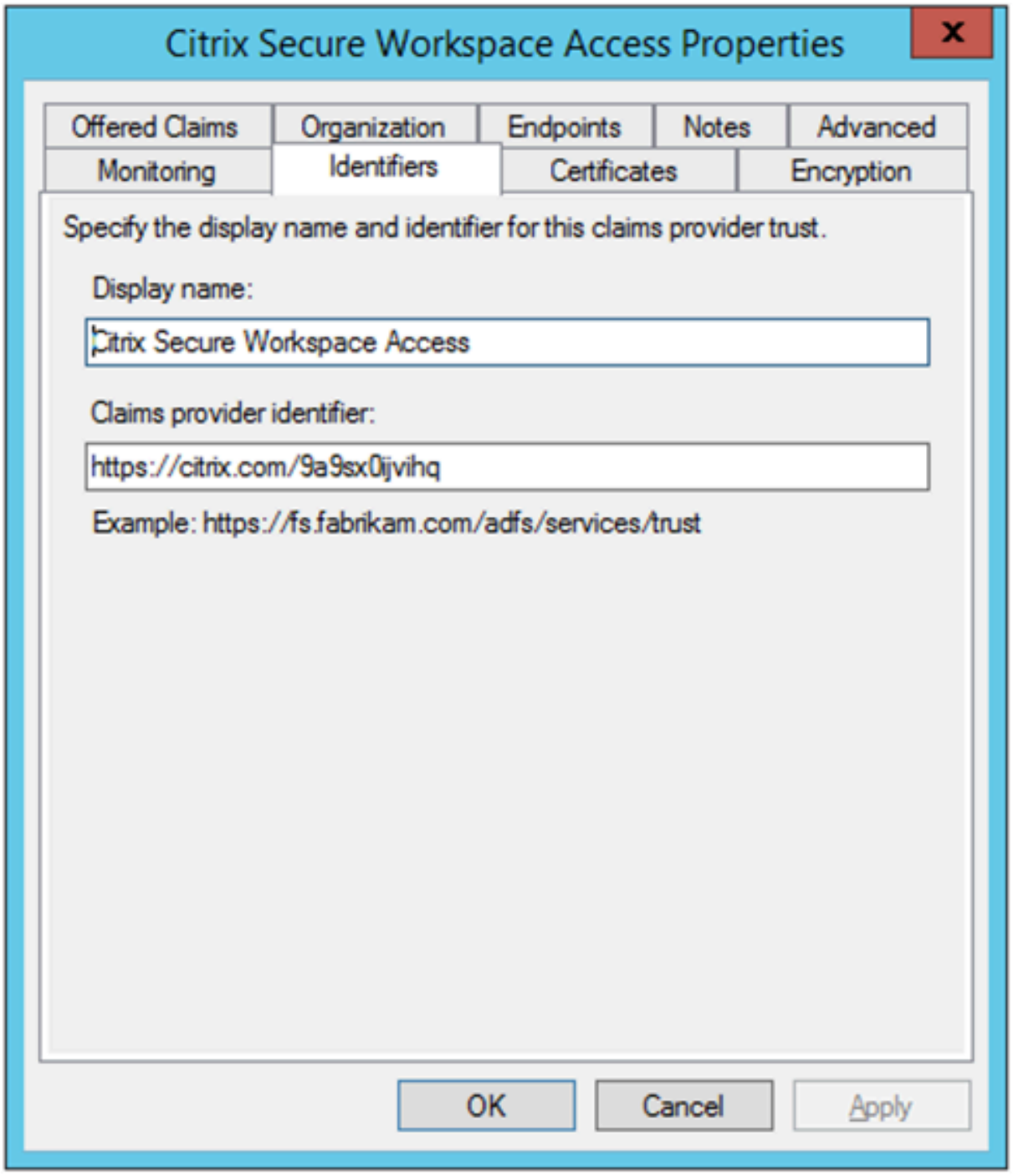
c) 次の図に示すように、設定を完了します。ADFS が他のクレームを受け入れる場合は、それらのクレームを使用し、それに応じて Secure Private Access で SSO も設定します。



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。

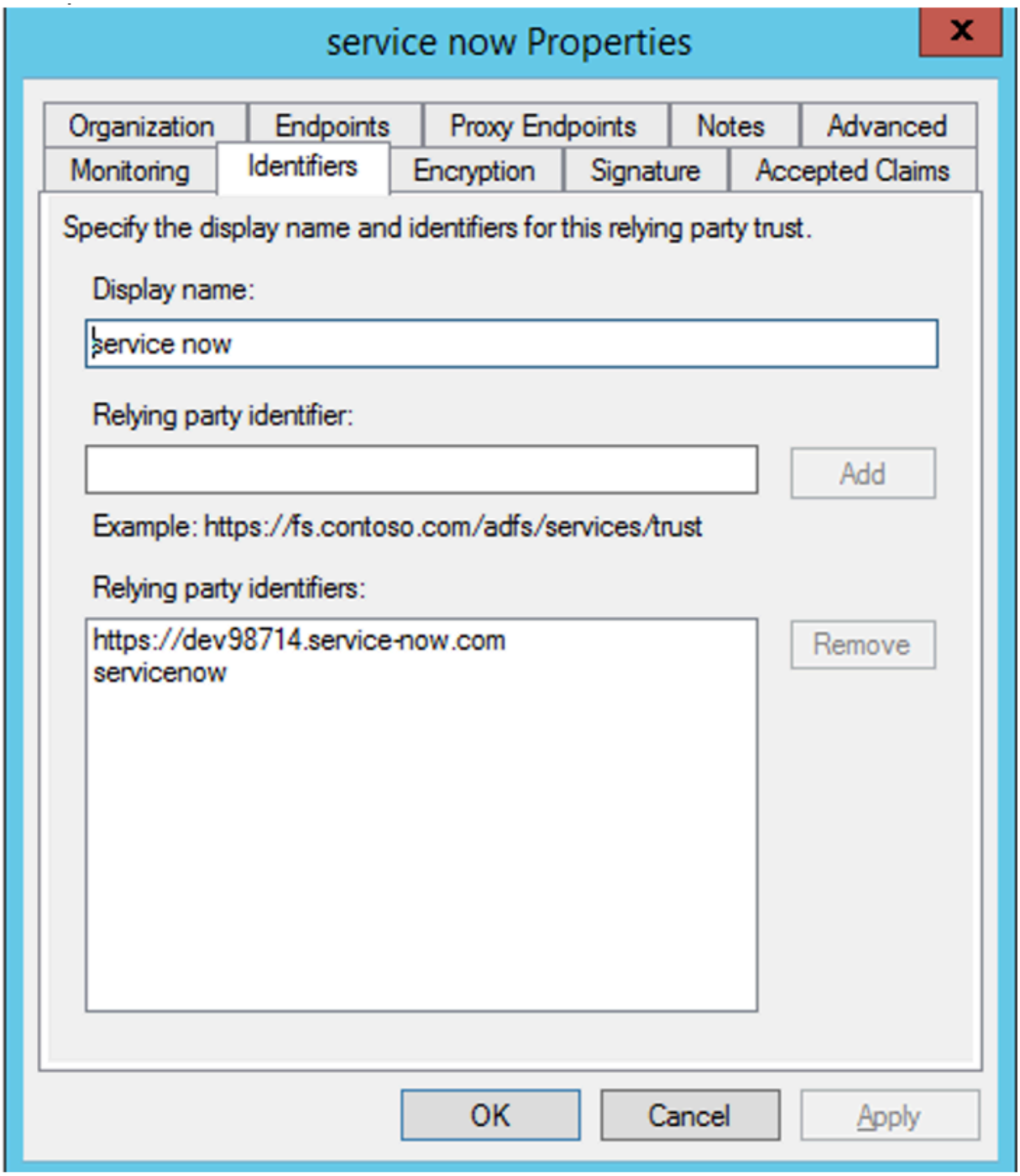
クレームプロバイダの信頼 **ID**

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。

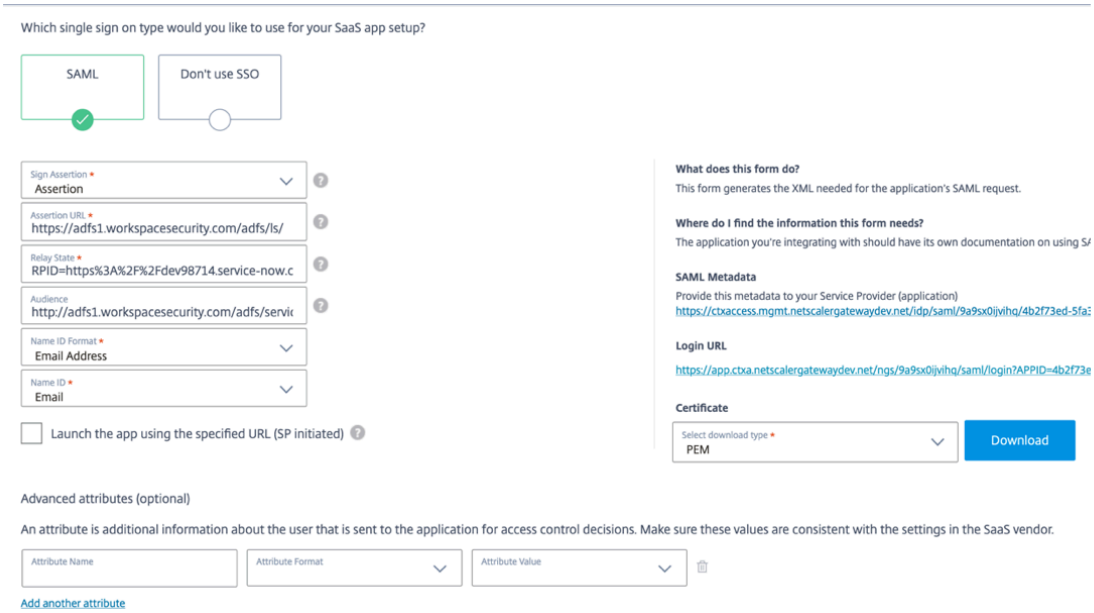
  例**:** https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

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。

機能の非推奨

August 26, 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	-
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。

