Citrix Secure Private Access-オンプレミス

Machine translated content

Disclaimer

Contents

製品の技術概要

August 26, 2024

Citrix Secure Private Access オンプレミスは、シームレスなエンドユーザーエクスペリエンスとともに、VPN なしで内部 Web および SaaS アプリケーションにアクセスできるようにする、顧客管理のゼロトラストネットワークアクセス（ZTNA）ソリューションです:

- 最小特権の原則
- シングルサインオン（SSO）
- 多要素認証
- デバイス ポスチャの評価
- アプリケーションレベルのセキュリティ制御
- App Protection 機能

このソリューションでは、オンプレミスの StoreFront アプリと Citrix Workspace アプリを活用して、Citrix Enterprise Browser 内の Web アプリや SaaS アプリにアクセスするためのシームレスで安全なアクセスを実現します。また、このソリューションでは、NetScaler Gateway を活用して認証と承認の制御を実施します。

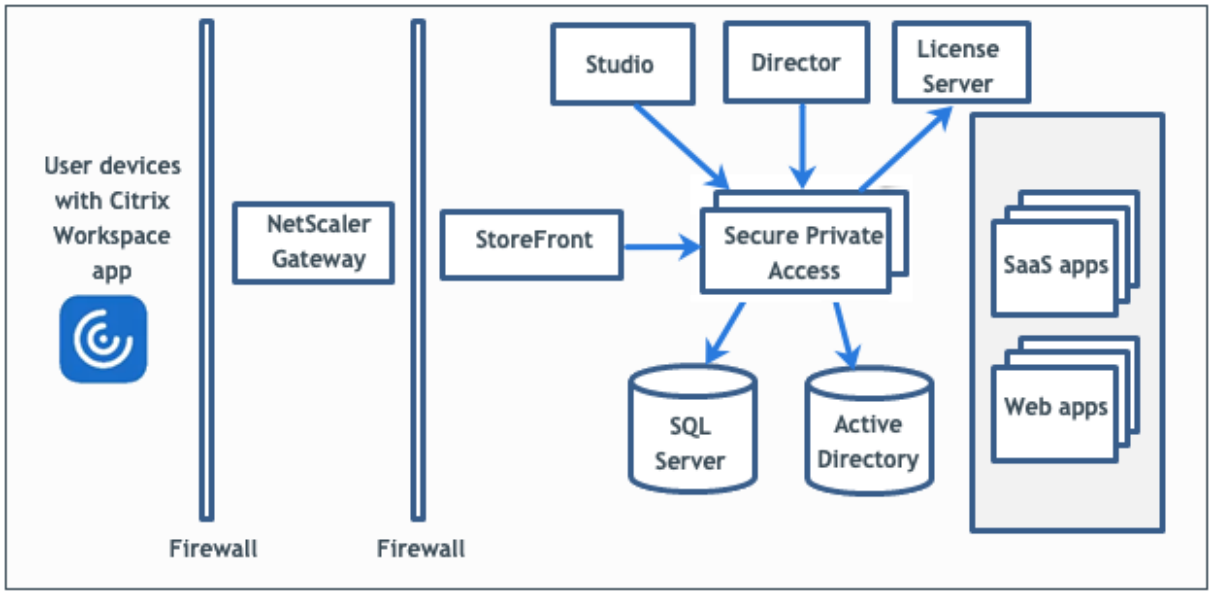
Citrix Secure Private Access オンプレミスソリューションは、Web および SaaS アプリへの統合アクセスポータルとして StoreFront のオンプレミスポータルを使用し、Citrix Workspace の統合部分として仮想アプリとデスクトップを使用することで、ブラウザーベースのアプリ（社内 Web アプリおよび SaaS アプリ）へのゼロトラストアクセスを簡単に提供できるため、組織の全体的なセキュリティとコンプライアンスの体制を強化します。

Citrix Secure Private Access は、NetScaler Gateway と StoreFront 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 UI	StoreFront オンプレミス/Citrix Workspace アプリ
SaaS および Web アプリへの SSO	NetScaler Gateway
多要素認証 (MFA) とデバイスポスチャ (別名エンドポイント分析)	NetScaler Gateway
Web アプリと SaaS アプリのセキュリティ制御とアプリ保護制御	Citrix Enterprise Browser
承認ポリシー	Secure Private Access
アクセス強制	NetScaler Gateway と Citrix Secure Access クライアント
構成と管理	Secure Private Access
可視性、監視、トラブルシューティング	Secure Private Access 、NetScaler コンソール（旧 ADM）、および Citrix Director

コンポーネント

この図は、一般的な Secure Private Access 展開のコンポーネントを示しています。



各コンポーネントの詳細については、「主要コンポーネント」を参照してください。

新機能

August 26, 2024

2024 年 **6** 月

SaaS および内部 **Web** アプリに対するその他のアクセス制限

SaaS と内部 Web アプリに追加のアクセス制限が適用されるようになりました。管理者はアクセスポリシーを通じてこれらの制限を適用できます。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。

認可されていない **Web** サイトのサポート

認可されていない Web サイトへのアクセスは、Secure Private Access Plug-in でサポートされるようになりました。Secure Private Access 内で構成されていないアプリケーション（イントラネットまたはインターネット）は、「認可されていない Web サイト」とみなされます。デフォルトでは、Secure Private Access は、アプリケーションとアクセスポリシーが構成されていない限り、すべてのイントラネット Web アプリケーションへのアクセスを拒否します。詳細については、「認可されていないウェブサイト」を参照してください。

Citrix Secure Private Access プラグインと **SIEM** サービスの統合

Citrix Secure Private Access は、セキュリティ情報およびイベント管理（SIEM）と統合されました。詳細については、SIEM 統合を参照してください。

トラブルシューティングログレベルが「情報」から「エラー」に変更されました

データベースの負荷を軽減するために、トラブルシューティングログレベルが「情報」から「エラー」に変更されました。ログレベルの変更方法の詳細については、「トラブルシューティングログのログレベルの変更」を参照してください。

解決された問題

August 26, 2024

リリース 2402 では、次の問題が解決されています。

ドメインコントローラーの構成

代替 UPN サフィックスは、イントラネット（StoreFront）ログインおよびインターネット/エクストラネット（ゲートウェイ）アプリ列挙用の Secure Private Access ではサポートされていません。

管理者管理

管理者の RBAC ロールの変更は、現在のセッションが無効化された後 (サインアウトまたはトークンの有効期限が切れた後) にのみ反映されます。

アプリケーション起動

次の条件をすべて満たすと、アプリケーションを起動できません：

- Netscaler バージョン 13.0.x、13.1-48.47 より前の 13.1、14.1—4.42 より前の 14.1 が使用されています。
- LDAP UPN は、実際のドメインとは異なるサフィックスで設定されます。

管理コンソール

- 関連するドメインエントリが変更された後に公開アプリケーションの **[**アプリの編集**]** ページ (**[Secure Private Access] > [**アプリケーション**] > [**アプリケーションの編集**]**) が閉じないと、**[**アプリケーションの編集**]** ページが自動的に閉じません。

  たとえば、アプリの作成時に入力した関連ドメインが`www.example.com`だったとします。アプリが公開されたら、関連ドメイン`www.example.com`を`abc.com`に置き換えて、[保存] をクリックします。アプリは正常に更新されますが、**[**アプリの編集] ページは閉じません。

- アプリを追加する際に、アプリ名にカンマが含まれていると、警告が表示されます。ただし、アプリは作成されます。
- アプリの URL に`www`が含まれている場合、URL はプレフィックス`www`なしでルーティングドメインテーブル (**[**設定**] > [**アプリケーションドメイン]) に保存されます。

アップグレード

Secure Private Access 管理サービスにカスタム SSL 証明書を使用する場合、証明書をインターネットインフォメーションサービス（IIS）の「Citrix Access Security Admin」サイトに再度バインドする必要があります。

既知の問題

October 21, 2024

リリース 2405 には次の問題があります。

> 注意**:**
>
> 一部の問題には内部参照専用の追跡 ID が割り当てられており、顧客には影響がありません。

ドメイン コントローラの構成

- 異なる AD フォレスト間のドメイン間の信頼タイプが「フォレスト」の一方向または双方向の信頼はサポートされていません。

  たとえば、a.com ドメインと b.com ドメインが 2 つの異なる AD フォレストにあり、ドメインが a.com / b.com に参加しているマシンに SPA がインストールされている場合、他のドメイン ユーザーは SPA で公開されたアプリにアクセスできません。

  [SPAOP-2031]

- オンプレミスの Secure Private Access がインストールされているマシンのドメインが、Secure Private Access にログインしている管理者のドメインと異なる場合は、次の操作を行う必要があります。

  Secure Private Access 管理サービスとランタイム サービスの両方に対して、IIS アプリケーション プールの ID として別のドメイン サービス アカウントを追加します。

- 配布グループは、Secure Private Access ではサポートされていません。したがって、ポリシーでは配布グループを検索してユーザーおよびグループの条件を追加することはできません。

- Secure Private Access では、管理コンソールまたはサービスでドメインの詳細が取得されません。したがって、ユーザーが提供したドメインに完全に依存します。したがって、対応するドメインにアクセスできない場合、またはドメイン名が有効な名前でない場合は、そのドメインはサポートされません。

NetScaler Gateway

- 次のシナリオでは、SSL プロファイル構成の SSL 仮想サーバーはサポートされません。

  - 顧客は NetScaler Gateway 13.1–48.47 以降または 14.1–4.42 以降を使用しています。
  - `ns_vpn_enable_spa_onprem` トグルが有効になっています。

  回避方法:

  SSL プロファイルで設定された SSL パラメータを SSL 仮想サーバーに直接バインドするか、`ns_vpn_enable_spa_onprem` トグルを無効にします。

  トグルの詳細については、「スマート アクセス タグのサポート」を参照してください。

RfWeb / ウェブ用ワークスペース

- RfWeb / Workspace for web はサポートされていないため、アプリは列挙されません。詳細については、「StoreFront バージョン 2311 以降を使用する場合」を参照してください。

  [SPAOP-2487]

アプリケーションの起動

- LDAP UPN と sAMAccountName が異なる場合、アプリケーションの起動は失敗します。

  [SPAOP-1412]

StoreFront

- ストア > 統合エクスペリエンスの構成では、Web サイトのデフォルトのレシーバーを /Citrix/<`StoreName`>Web に構成する必要があります。StoreFront の以前のバージョンでは、Web サイト

のデフォルトのレシーバーが空白の値に設定されており、Secure Private Access では機能しません。また、クライアントには以前のバージョンの Receiver UI が表示されます。StoreFront の構成については、「StoreFront」を参照してください。

- StoreFront バージョン 2308 以前を使用している場合、ストア **> Delivery Controller** の管理 ページに、Secure Private Access プラグインの種類が **XenMobile** として表示されます。機能には影響しません。

ログ

- クラスターのサポート バンドルの生成はサポートされていません。
- 管理サービスとランタイム サービスのログ フォルダーは削除しないでください。これらのフォルダーが削除された場合、Secure Private Access は再作成できません。

プログラムのアンインストールまたは変更ページでのインストーラの表示

- ISO ファイルを使用して Secure Private Access を以前のバージョンから 2405 にアップグレードすると、[プログラムのアンインストールまたは変更] ページ ([コントロール パネル **>** プログラム **>** プログラムと機能]) に、最初のエントリが置き換えられるのではなく、Secure Private Access インストーラーの 2 つのエントリが表示されます。

  回避策: 古いビルド インストーラーをアンインストールします。

> 注意**:**
>
> この問題は、Secure Private Access スタンドアロン インストーラーを 2402 スタンドアロン インストーラーを使用してアップグレードした場合には発生しません。

アップグレード

- 2405 にアップグレードした後、URL が wwwで始まる既存のアプリを編集すると、アプリ接続 フィールドに以前の状態が入力されません。アプリの接続タイプを再度選択する必要があります。これはアップグレード後の 1 回限りのアクションであり、その後は構成が保存され、引き続き保持されます。

  [SPAOP-4216]

- 2405 にアップグレードすると、管理コンソールにログオンすることはできますが、アプリケーションとポリシーを管理することはできません。エラーメッセージが表示されます。

  回避策: スクリプトを使用してデータベースをアップグレードする必要があります。詳細については、「スクリプトを使用してデータベースをアップグレードする」を参照してください。

  [SPAOP-5255]

- 2405 にアップグレードすると、アプリケーションの列挙とアプリケーションの起動が失敗します。

  回避策: スクリプトを使用してデータベースをアップグレードする必要があります。詳細については、「スクリプトを使用してデータベースをアップグレードする」を参照してください。

  [SPAOP-5255]

- Delivery Controller を使用して 2402 プラグインがインストールされている場合、Secure Private Access プラグインをバージョン 2402 から 2405 にアップグレードすることはできません。

  [SPAOP-4505]

システム要件

October 21, 2024

製品が最小バージョン要件を満たしていることを確認してください。

- Citrix Workspace アプリ
  - Windows –2403 以降
  - macOS –2402 以降
- Secure Private Access プラグイン サーバーのオペレーティング システム - Windows Server 2019 以降
- StoreFront –LTSR 2203 または CR 2212 以降
- NetScaler –13.0、13.1、14.1 以降。パフォーマンスを最適化するには、NetScaler Gateway バージョン 13.1 または 14.1 の最新ビルドを使用することをお勧めします。
- Director 2402 以降
- 通信ポート: Secure Private Access プラグインに必要なポートが開いていることを確認します。詳細については、通信ポートを参照してください。

> 注意:
>
> オンプレミスのセキュアプライベートアクセスは、iOS および Android 向け Citrix Workspace アプリではサポートされていません。

前提条件

NetScaler Gateway を作成または既存の NetScaler Gateway を更新する場合は、次の詳細を確認してください。

- IIS が実行され、SSL/TLS 証明書が構成され、Secure Private Access プラグインがインストールされる Windows サーバー マシン。

- セットアップ中に入力する StoreFront ストアの URL。
- StoreFront 上のストアが構成されており、ストア サービスの URL が利用可能である必要があります。ストア サービスの URL の形式は、`https://store.domain.com/Citrix/StoreSecureAccess` です。
- NetScaler Gateway の IP アドレス、FQDN、および NetScaler Gateway コールバック URL。
- Secure Private Access プラグインのホスト マシン (または、Secure Private Access プラグインがクラスターとして展開されている場合はロード バランサー) の IP アドレスと FQDN。
- NetScaler で設定された認証プロファイル名。
- NetScaler で構成された SSL サーバー証明書。
- ドメイン名.
- 証明書の構成が完了しました。管理者は証明書の構成が完了していることを確認する必要があります。マシン内に証明書が見つからない場合、Secure Private Access インストーラーは自己署名証明書を構成します。ただし、これが常に機能するとは限りません。
- データベース: サイト構成、構成ログ、および監視データベースでサポートされている Microsoft SQL Server バージョンの一覧は次のとおりです。

  - SQL Server 2022 の Express、Standard、および Enterprise Edition。
  - SQL Server 2019 の Express、Standard、および Enterprise Edition。
  - SQL Server 2017 の Express、Standard、および Enterprise Edition。

  新規インストール：デフォルトでは、Controller のインストール時に適切なバージョンの SQL Server が検出されない場合、SQL Server Express 2017 と累積更新プログラム（CU）16 がインストールされます。

  アップグレードの場合、既存の SQL Server Express バージョンはアップグレードされません。

  以下のデータベース高可用性ソリューションがサポートされます（スタンドアロンモードのみをサポートする SQL Server Express を除く）。

  - SQL Server Always On フェールオーバー クラスター インスタンス
  - SQL Server の AlwaysOn 可用性グループ（基本的な可用性グループを含む）
  - SQL Server データベースミラーリング

  Controller と SQL Server サイトデータベース間の接続には Windows 認証が必要です。

  データベースの詳細については、「データベース」を参照してください。

> 注意:
>
> ランタイム サービス (IIS の既定の Web サイトの secureAccess アプリケーション) では、Windows 認証がサポートされていないため、匿名認証を有効にする必要があります。これらの設定は、Secure Private Access インストーラーによってデフォルトで設定され、手動で変更することはできません。

管理者アカウントの要件

Secure Private Access を設定する際には、次の管理者アカウントが必要です。

- Secure Private Access をインストールする: ローカル マシンの管理者アカウントでログインする必要があります。
- Secure Private Access のセットアップ: Secure Private Access がインストールされているマシンのローカル マシン管理者でもあるドメイン ユーザーで、Secure Private Access 管理コンソールにサインインする必要があります。
- セキュア プライベート アクセスの管理: セキュア プライベート アクセス管理者アカウントを使用して、セキュア プライベート アクセス管理コンソールにサインインする必要があります。

通信ポート

次の表は、Secure Private Access プラグインで使用される通信ポートを示しています。

接続元	接続先	種類	ポート	詳細
管理ワークステーション	セキュアプライベートアクセスプラグイン	HTTPS	4443	セキュア プライベート アクセス プラグイン - 管理コンソール
セキュアプライベートアクセスプラグイン	NTP サービス	TCP、UDP	123	時間同期
	DNS サービス	TCP、UDP	53	DNS ルックアップ
	Active Directory	TCP、UDP	88	kerberos
	Director	HTTP、HTTPS	80、443	パフォーマンス管理とトラブルシューティングの強化のためにディレクターとコミュニケーションをとる
	ライセンスサーバー	TCP	8083	ライセンスデータの収集と処理のためのライセンスサーバーへの通信
		TCP	389	プレーンテキスト経由の LDAP (LDAP)

接続元	接続先	種類	ポート	詳細
		TCP	636	SSL 経由の LDAP (LDAPS)
	Microsoft SQL Server	TCP	1433	セキュアプライベートアクセスプラグイン - データベース通信
	StoreFront	HTTPS	443	認証検証
	NetScaler Gateway	HTTPS	443	NetScaler ゲートウェイ コールバック
StoreFront	NTP サービス	TCP、UDP	123	時間同期
	DNS サービス	TCP、UDP	53	DNS ルックアップ
	Active Directory	TCP、UDP	88	kerberos
		TCP	389	プレーンテキスト経由の LDAP (LDAP)
		TCP	636	SSL 経由の LDAP (LDAPS)
		TCP、UDP	464	ユーザーが期限切れのパスワードを変更できるようにするネイティブの Windows 認証プロトコル
	セキュアプライベートアクセスプラグイン	HTTPS	443	認証とアプリケーションの列挙
	NetScaler Gateway	HTTPS	443	NetScaler ゲートウェイ コールバック
NetScaler Gateway	セキュアプライベートアクセスプラグイン	HTTPS	443	アプリケーション認証の検証
	StoreFront	HTTPS	443	認証とアプリケーションの列挙

接続元	接続先	種類	ポート	詳細
	Web アプリケーション	HTTP、HTTPS	80、443	構成されたセキュアプライベート アクセス アプリケーションへの NetScaler Gateway 通信 (ポートはアプリケーション要件によって異なる場合があります)
ユーザーデバイス	NetScaler Gateway	HTTPS	443	エンドユーザーデバイスと NetScaler Gateway 間の通信

参照ドキュメント

- 認証プロファイル。
- 認証ポリシーの仕組み.
- NetScaler 上の仮想サーバー (SSL) に SSL 証明書をバインドします。

サイズガイドライン

August 26, 2024

データベースストレージ要件

データベースストレージのほとんどはログによって消費されます。アプリケーションとポリシー設定によるストレージ容量の消費は、ログと比較するとごくわずかです。

次の図は、サーバーのストレージ要件を示しています:

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

> 注:
>
> - メトリクスは、ログイベントのクリーンアップが無効で、ログ保持期間が 7 日間に設定されていることを前提として算出されます。
> - デフォルトでは、構成された設定に応じて、ログは 90 日間保持されるか、最大 100 K のログイベントが保持されます。これらの設定は、Secure Private Access ランタイム・サービスの appsettings.json ファイルで使用でき、必要に応じて変更できます。詳しくは、イベントログを保持するための設定を参照してください。

サーバー構成

次の表は、サーバー構成の詳細を示しています:

構成	詳細
アプリケーションの総数	250
ポリシーの総数	50
ユーザーあたりのアプリ数	15
AD コンフィギュレーション	ユーザーは 20 のグループに属し、最大 20 レベルのネスティングが可能です
トラブルシューティングログの保存期間	7 日 (デフォルト)
トラブルシューティングログレベル	エラー (デフォルト)
Secure Private Access サーバーのログ保持	90 日または 600 ファイル

トラフィックプロファイル

次の表は、ユーザーごとの 1 日あたりのトラフィックプロファイルの詳細を示しています。

Profile	詳細
列挙	10
エンタープライズブラウザポリシー同期	20
Citrix Workspace アプリからのアプリケーションの起動	4
Citrix Enterprise Browser からのアプリケーションアクセス	500
Citrix Director によるヘルプデスクのトラブルシューティング要求（1 日あたり）	1000

導入ガイドライン

次の表は、同時アプリケーションアクセスユーザーセッション、1 分あたりのアプリケーション列挙数、Secure Private Access で使用される CPU などのパラメーターに基づくデータベースサイジング要件を示しています:

アプリケーションへの同時アクセスユーザーセッション	1 分あたりのアプリ列挙	Secure Private Access メモリ (GB)	Secure Private Access CPU	GB 単位のストレージ	メモ
< 20 (実証実測の目的)	2	4 GB	2	40 GB*	PoC の目的では、既存の仮想マシンの仕様を変更することなく、SPA を StoreFront と同じマシンに展開できます。
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	2 つ以上の SPA ノードを導入してパフォーマンスを向上させることができます。

> 注:
>
> - * ストレージは主に CDF ログによって消費されます。デフォルトでは、Secure Private Access は、各ファイルのサイズが 10 MB の 600 個のロールオーバーログファイルを保持します。そのため、Secure Private Access 管理サービスとランタイムサービスの両方が同じマシンで実行されている場合、ログによる最大ストレージ使用率は 12 GB になります。また、PoC の目的で SQL Express をローカル VM にインストールすることもできます。
> - ** この負荷プロファイル以上では、NetScaler Gateway のバージョンが 13.0 未満または 13.1〜48.47 未満でない限り、StoreFront との共同ホスティングではなく、専用サーバーに Secure Private Access を展開することをお勧めします。
> - *** パフォーマンス上の問題がいくつかあることがわかっているため、このような負荷には少なくとも 2 つの Secure Private Access ノードクラスターを使用することをお勧めします。これらの問題は、今後のリリースで対処される予定です。

その他のコンポーネント構成

コンポーネント	vCPU	メモリ
Secure Private Access・プラグイン	8	16 GB
Secure Private Access SQL サーバー	8	16 GB
StoreFront	16	8 GB
Gateway	4	8 GB
Active Directory	8	14 GB
クライアント	4	8 GB

インストールと構成

August 26, 2024

Secure Private Access インストーラーは、スタンドアロンインストーラーとして、または統合された Citrix Virtual Apps and Desktops インストーラーの一部として使用できます。詳しくは、「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

インストールが完了すると、初回セットアップの管理コンソールがデフォルトのブラウザウィンドウで自動的に開きます。「続行」をクリックして、Secure Private Access を設定できます。デスクトップの［スタート］メニュー（［**Citrix**］**>**［**Citrix Secure Private Access** ］）にも **Citrix Secure Private Access** ショートカットが表示されます。

Secure Private Access をインストールして管理するための管理者アカウント要件

- Secure Private Access をインストールするには、ローカルマシンの管理者アカウントでログインする必要があります。
- Secure Private Access を設定するには、Secure Private Access がインストールされているマシンのローカルマシン管理者でもあるドメインユーザーで Secure Private Access 管理コンソールにサインインする必要があります。
- セットアップが完了すると、そのユーザーは最初の Secure Private Access 管理者になり、他の管理者を追加できます。
- セットアップ後に Secure Private Access を管理するには、Secure Private Access 管理者アカウントで Secure Private Access 管理コンソールにサインインする必要があります。

Secure Private Access のセットアップ

次の手順を実行して、Secure Private Access を設定できます:

- 新しいサイトを作成して Secure Private Access を設定するか、既存のサイトに参加して Secure Private Access をセットアップします
- データベースを設定
- StoreFront、NetScaler Gateway、Director、ライセンスサーバーを統合

アプリケーションとアクセスポリシーの設定

Secure Private Access 環境をセットアップしたら、アプリケーションとアプリケーションのアクセスポリシーを設定する必要があります。

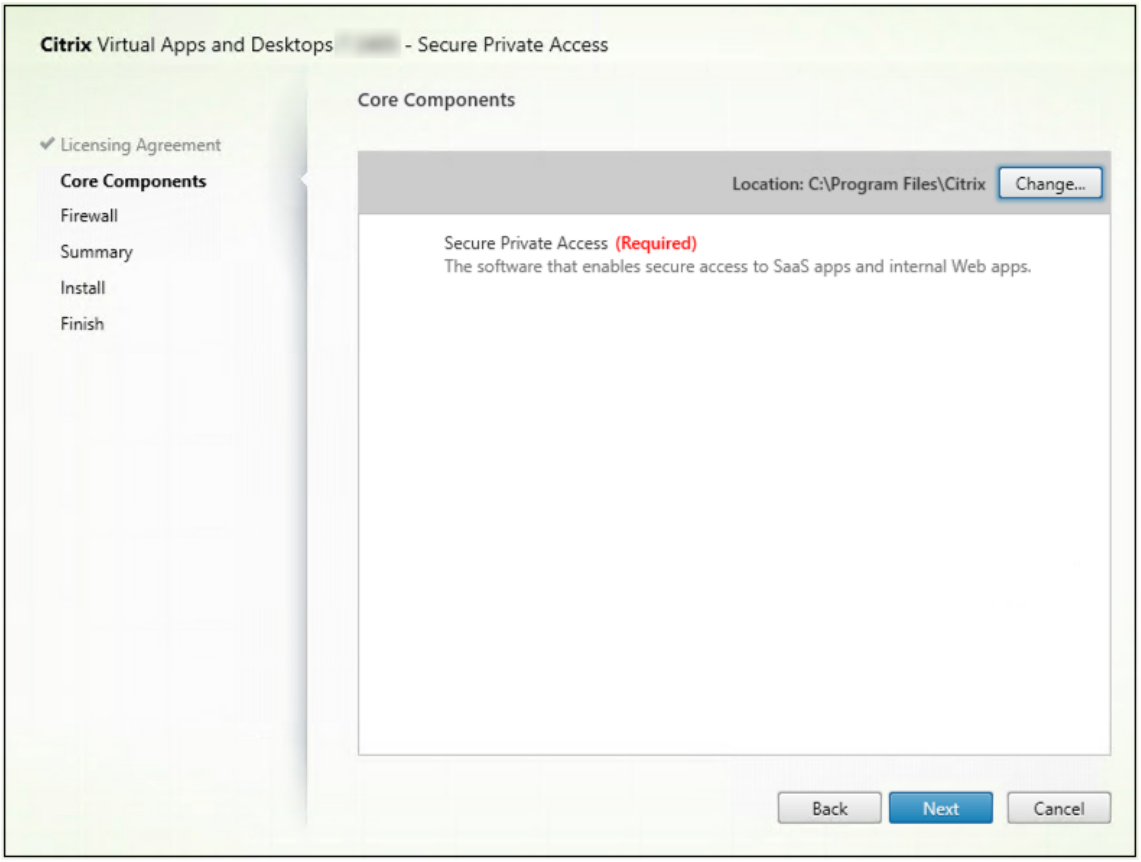
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

Secure Private Access インストーラー

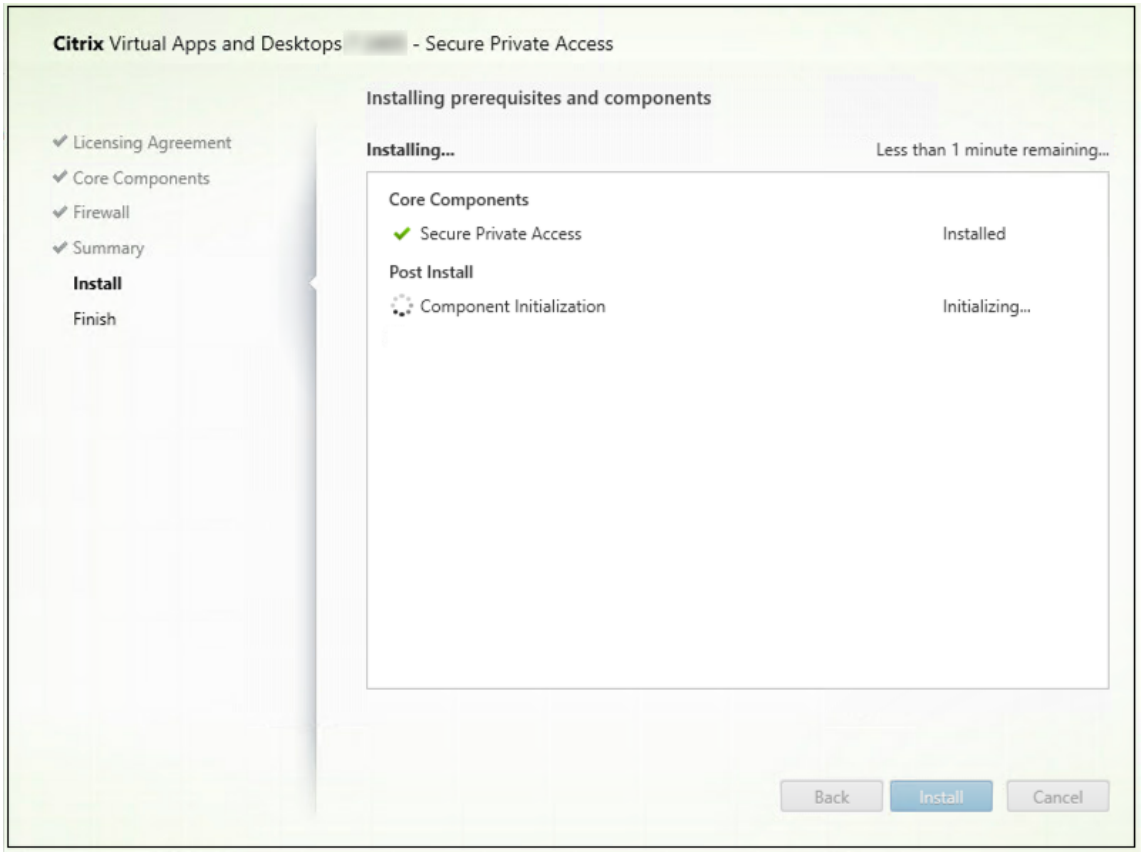
August 26, 2024

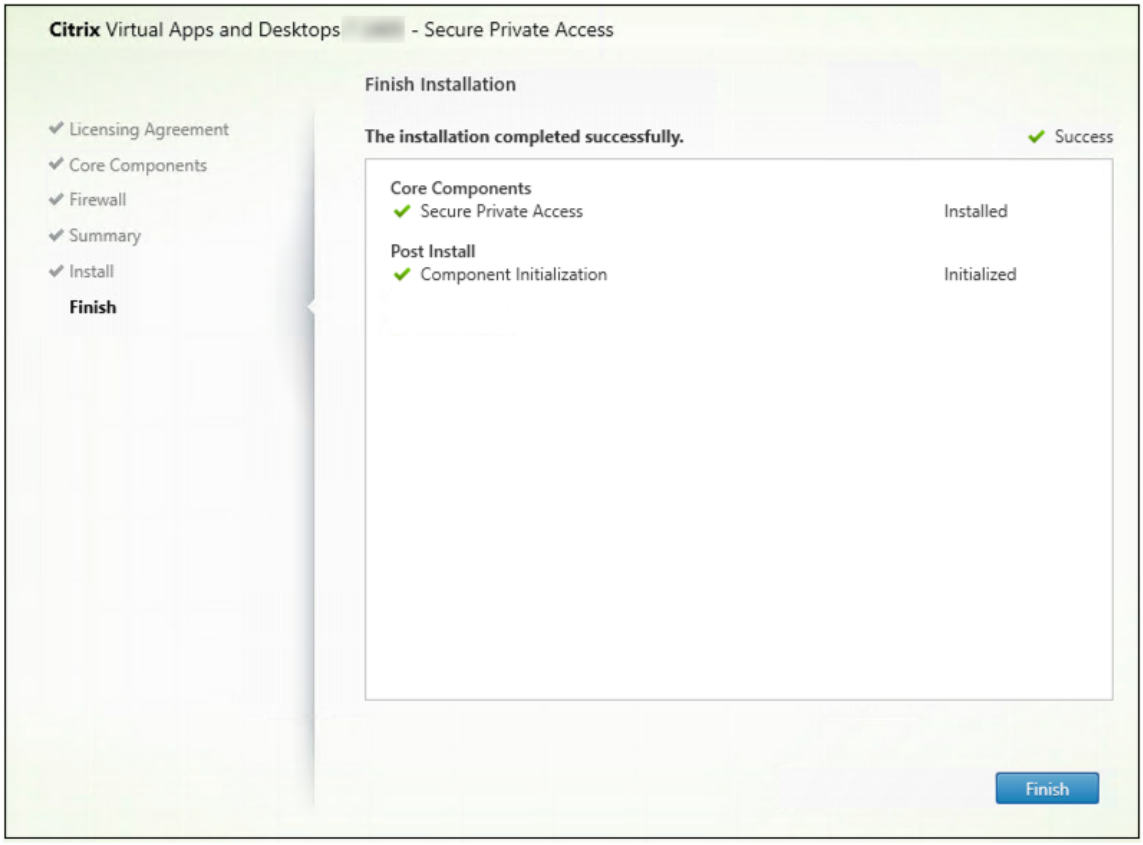
1. Citrix Secure Private Access のインストーラーをhttps://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/からダウンロードします。
2. .exe をドメインに参加しているマシン上で管理者として実行します。

> 注:
>
> POC の目的で、StoreFront がインストールされているのと同じマシンに Secure Private Access をインストールすることをお勧めします。

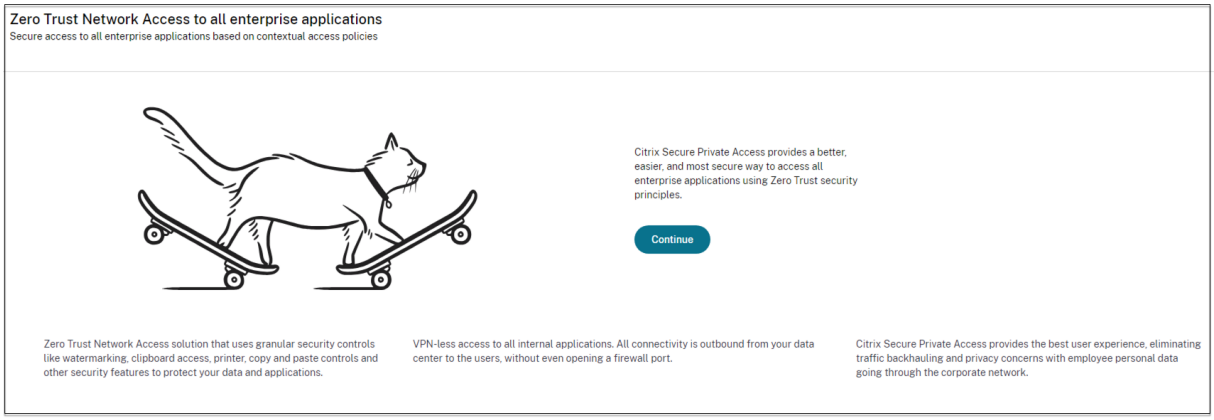


3. 画面の指示に従ってインストールを完了します。

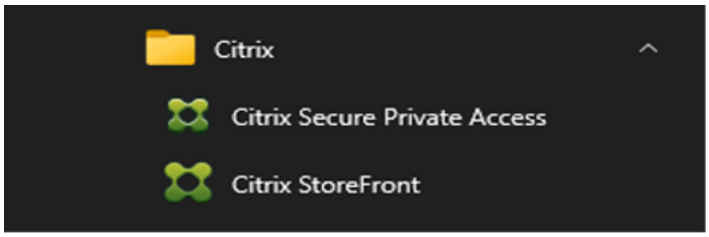




インストールが完了すると、初回セットアップの管理コンソールがデフォルトのブラウザウィンドウで自動的に開きます。「続行」をクリックして、Secure Private Access を設定できます。



デスクトップの［スタート］メニュー（［**Citrix**］**>**［**Citrix Secure Private Access**］）にも **Citrix Secure Private Access** ショートカットが表示されます。



詳しくは、次のトピックを参照してください:

- コアコンポーネントのインストール
- コマンドラインを使用したインストール

管理コンソールへの **SSO**

Secure Private Access 管理コンソールに使用するブラウザに Kerberos 認証を設定することをお勧めします。これは、Secure Private Access が管理者認証に統合 Windows 認証 (IWA) を使用しているためです。

Kerberos 認証が設定されていない場合、Secure Private Access 管理コンソールにアクセスするときに、ブラウザから認証情報の入力を求められます。

- 資格情報を入力すると、統合 Windows 認証 (IWA) サインオンが有効になります。
- 認証情報を入力しない場合、Secure Private Access のサインオンページが表示されます。

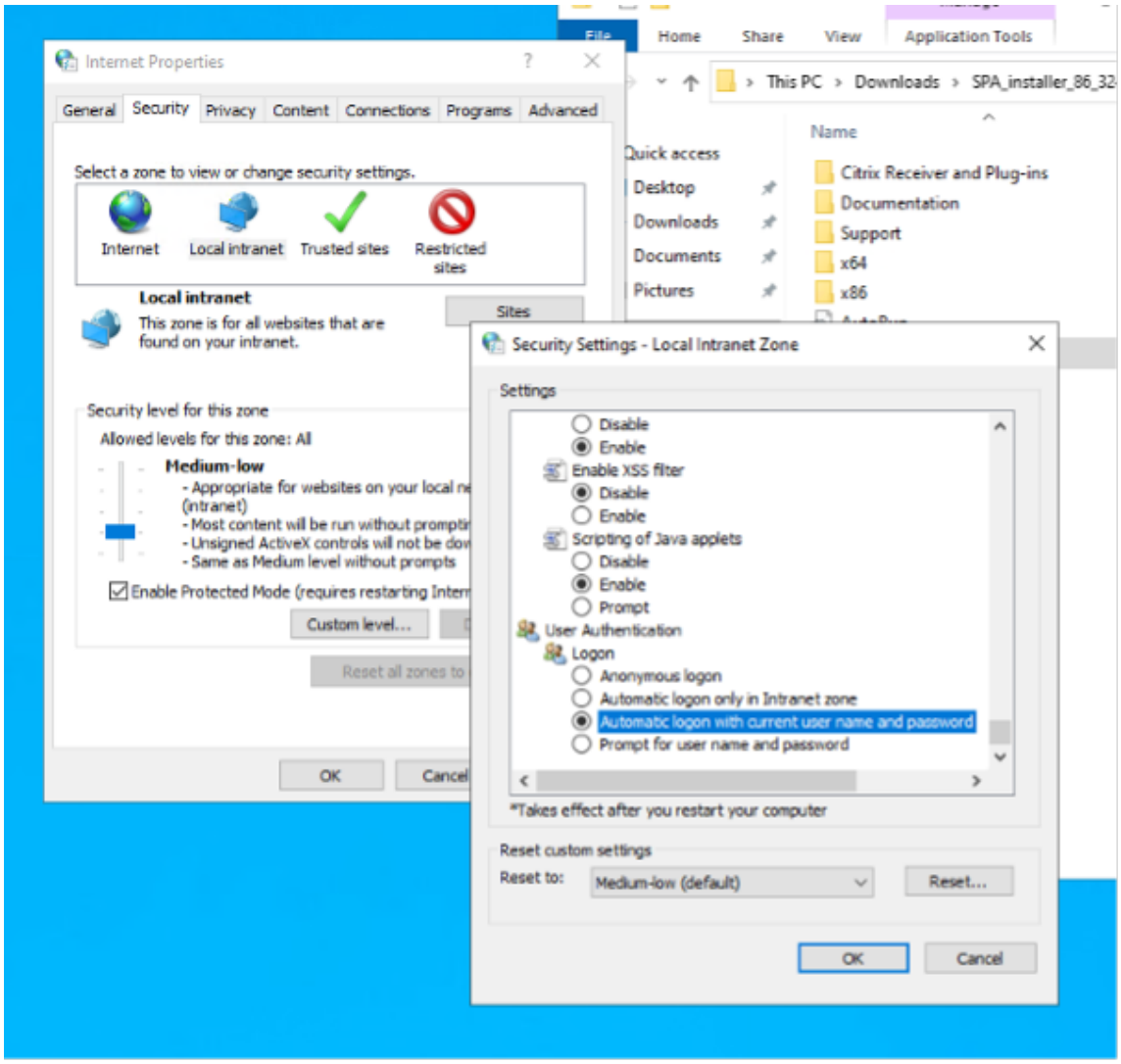
Secure Private Access のセットアップを続行するには、管理コンソールにサインインする必要があります。インストールマシンと同じドメインに属する任意のユーザーに Secure Private Access を設定できます。ただし、そのユーザーがインストールマシンのローカル管理者権限を持っている必要があります。

Google Chrome および Microsoft Edge ブラウザの場合は、次の手順を実行して Kerberos を有効にします。

1. [インターネットオプション] を開きます。
2. [セキュリティ] タブを選択し、[ローカルイントラネットゾーン] をクリックします。
3. 「サイト」をクリックし、Secure Private Access の URL を追加します。

   Secure Private Access を複数のマシンにインストールする予定がある場合は、ワイルドカードを使用することもできます。例: `"https://*.fabrikam.local"`。

4. 「カスタムレベル」をクリックし、「ユーザー認証」>「ログオン」で、「現在のユーザー名とパスワードで自動ログオン」を選択します。



注:

- Chrome シークレットセッションを使用している場合は、DWORD レジストリキー Computer\ HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Google\ Chrome\ AmbientAuthenticationInPrivateModesEnabled を作成し、値 1 に設定します。

- Kerberos をシークレットモードで有効にする前に、すべての Chrome ウィンドウ (非シークレットウィンドウを含む) を再起動する必要があります。
- 他のブラウザーについては、Kerberos 認証に関する特定のブラウザーのドキュメントを確認してください。

次の手順

- Secure Private Access のセットアップ
- NetScaler Gateway Gateway の構成
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

Secure Private Access のセットアップ

August 26, 2024

新しいサイトを作成するか、既存のサイトに参加することで、Secure Private Access を設定できます。どちらのシナリオでも、Web 管理コンソールを使用して Secure Private Access 環境を設定できます。

- 新しいサイトを作成して Secure Private Access を設定する
- 既存のサイトに参加して Secure Private Access を設定する

前提条件

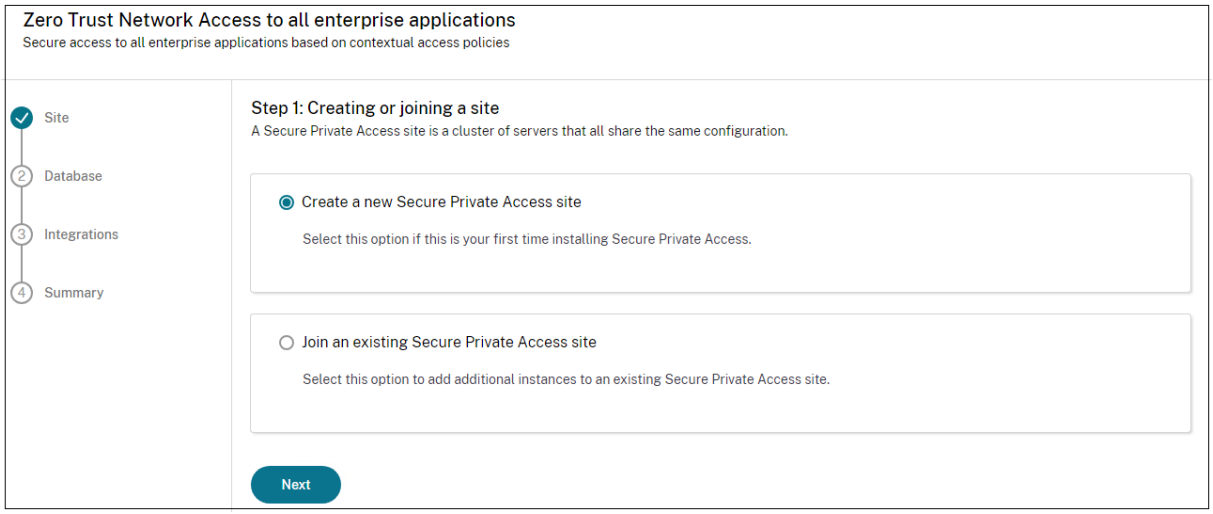
- Secure Private Access がインストールされているマシンのローカルマシン管理者でもあるドメインユーザーで Secure Private Access 管理コンソールにサインインする必要があります。
- サイトを作成する前に SQL データベースサーバーをインストールする必要があります。

新しいサイトを作成して **Secure Private Access** を設定する

ステップ **1: Secure Private Access** サイトのセットアップ

サイトとは、Secure Private Access 環境の名前です。サイトを作成するか、既存のサイトに参加することができます。

1. Secure Private Access Web 管理コンソールを起動します。
2.「サイトの作成」または「サイトへの参加」ページでは、「新しい **Secure Private Access** サイトを作成する」がデフォルトで選択されています。
3.［次へ］をクリックします。



サイトを作成する場合、サイト名に対応するデータベースがセットアップで使用できない場合があるため、新しいサイトのデータベースを自動または手動で構成する必要があります。

ステップ **2:** データベースを設定する

新しい Secure Private Access サイト用のデータベースを作成する必要があります。これは手動または自動で行うことができます。

1. 「**SQL Server** ホスト」に、サーバーのホスト名を入力します。例: `sql1.fabrikam.local\citrix`。

   データベースのアドレスは、以下の形式のいずれかで指定できます:

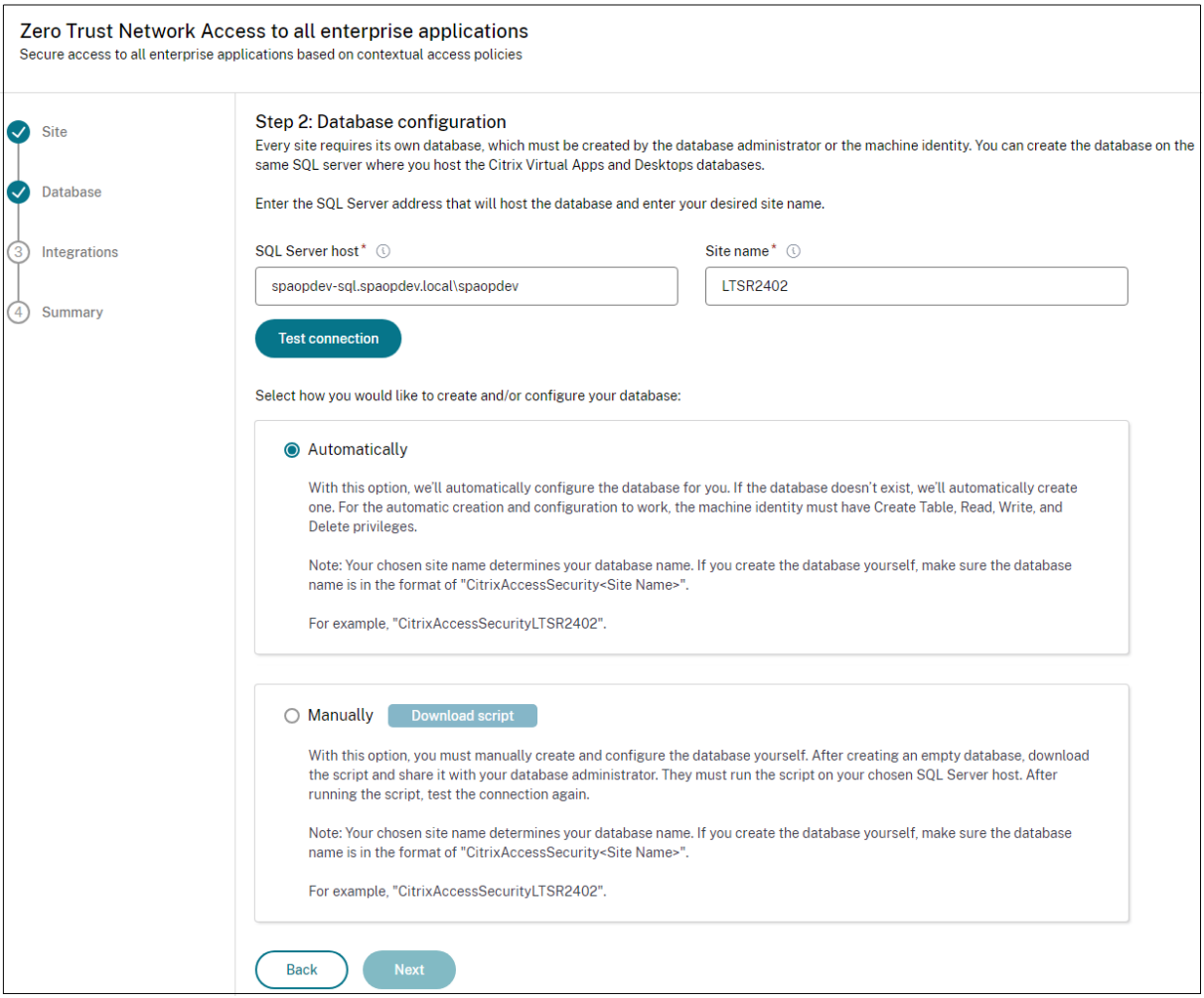
   - サーバー名
   - ServerName\InstanceName
   - サーバー名、ポート番号

   詳しくは、「データベース」を参照してください。

2. [サイト] に、Secure Private Access サイトの名前を入力します。

   > 注:
   >
   > 入力するサイト名の末尾には、データベース名の末尾が付きます。データベース名の形式は`CitrixAccessSecurity<sitename>`であり、変更できません。データベース名をカスタマイズする必要がある場合は、Citrix サポートにお問い合わせください。

3. [接続をテスト] をクリックして、SQL Server インスタンスが有効であることを確認し、指定したデータベースがサイトに存在することを確認します。



> 注:
>
> - サイトで SQL Server が使用できない場合、接続チェックは失敗します。
> - SQL Server は利用できるが、データベースが存在しない場合、接続チェックは成功します。ただし、警告メッセージが表示されます。
> - Secure Private Access は、マシン ID を使用した Windows 認証を使用して SQL Server を認証します。

自動構成:

- 自動構成オプションは、マシン ID に必要なデータベース権限がある場合にのみ使用できます。
- 指定したアドレスにデータベースが存在しない場合、データベースが自動的に作成されます。
- データベースを作成するときは、そのデータベースが空で、必要なデータベース権限があることを確認してください。権限の詳細については、「データベースの設定に必要な権限」を参照してください。

手動設定:

手動構成オプションを使用してデータベースをセットアップできます。

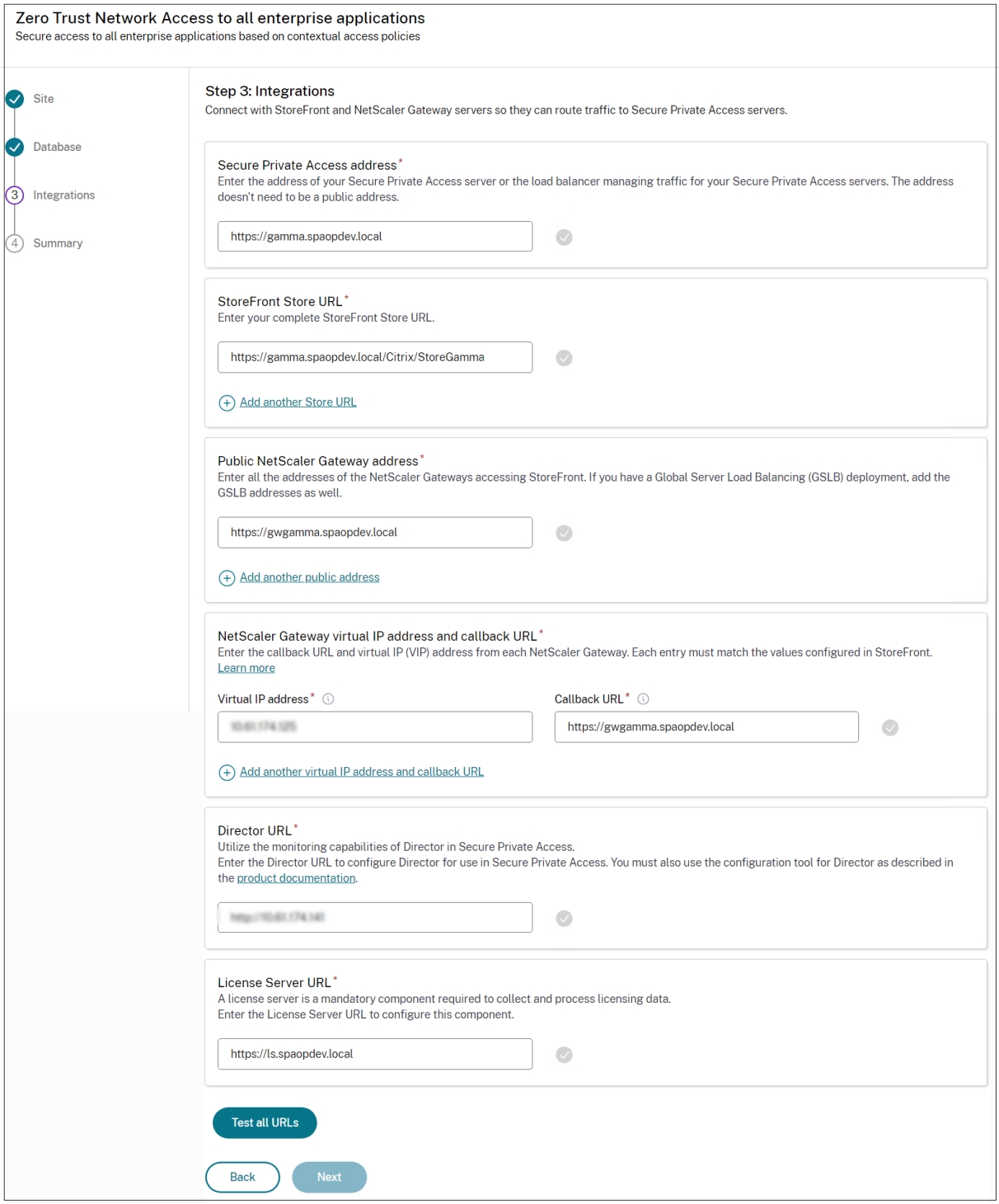
手動構成では、最初にスクリプトをダウンロードしてから、[**SQL Server Host]** フィールドで指定したデータベースサーバー上でスクリプトを実行する必要があります。

> 注:
>
> SQL Server 上のデータベース内にテーブルを作成するための READ、WRITE、UPDATE 権限がマシンにない場合、データベースの作成が失敗することがあります。マシン上で適切な権限を有効にする必要があります。詳細については、「データベースの設定に必要な権限」を参照してください。

ステップ **3:** サーバーを統合する

Secure Private Access を StoreFront および NetScaler Gateway サーバーに接続するには、StoreFront および NetScaler Gateway サーバーの詳細を指定する必要があります。StoreFront と NetScaler Gateway がトラフィックを Secure Private Access にルーティングできるようにするには、この接続を確立する必要があります。Director サーバーとライセンスサーバーの詳細も指定する必要があります。

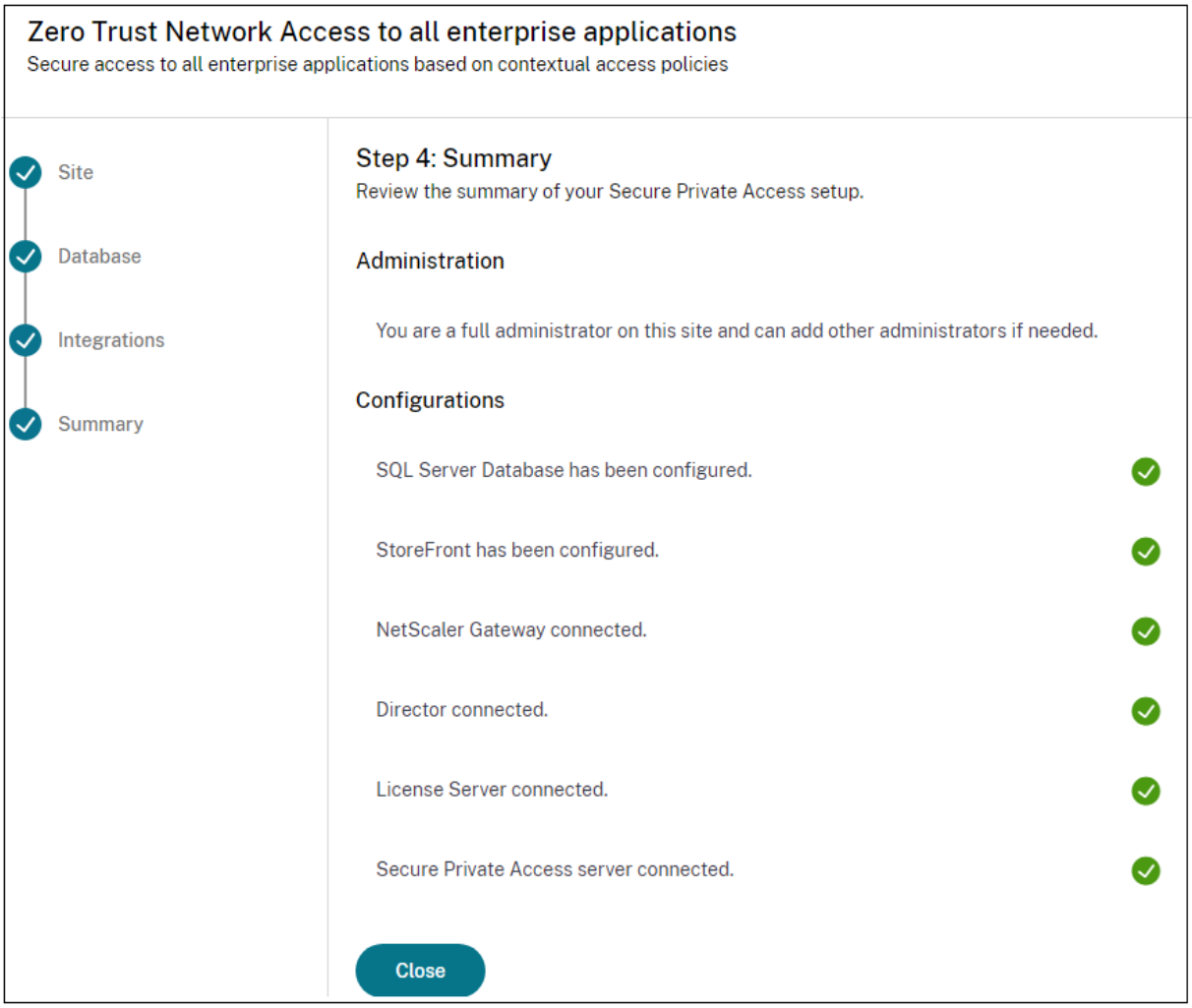
1. 次の詳細を入力します。
    - **Secure Private Access** サーバーのアドレス。例: `https://secureaccess.domain.com`。
    - **StoreFront** ストア **URL**。例: `https://storefront.domain.com/Citrix/StoreMain`。
    - パブリック **NetScaler Gateway** アドレス—NetScaler Gateway の URL。例: `https://gateway.domain.com`。
    - 仮想 **IP** アドレス—この仮想 IP アドレスは、StoreFront でコールバック用に構成されたものと同じである必要があります。
    - コールバック **URL** —この URL は、StoreFront で構成されているものと同じである必要があります。例: `https://gateway.domain.com`。
    - **Director URL:** -(オプション) Citrix Director に Secure Private Access を接続するためのディレクターサーバーの IP アドレスまたは FQDN。
    - ライセンスサーバーの **URL:** -ライセンスデータを収集して処理するためのライセンスサーバーの IP アドレス。
2. 「すべての **URL** を検証」をクリックします
3. [次へ] をクリックし、[保存] をクリックします。



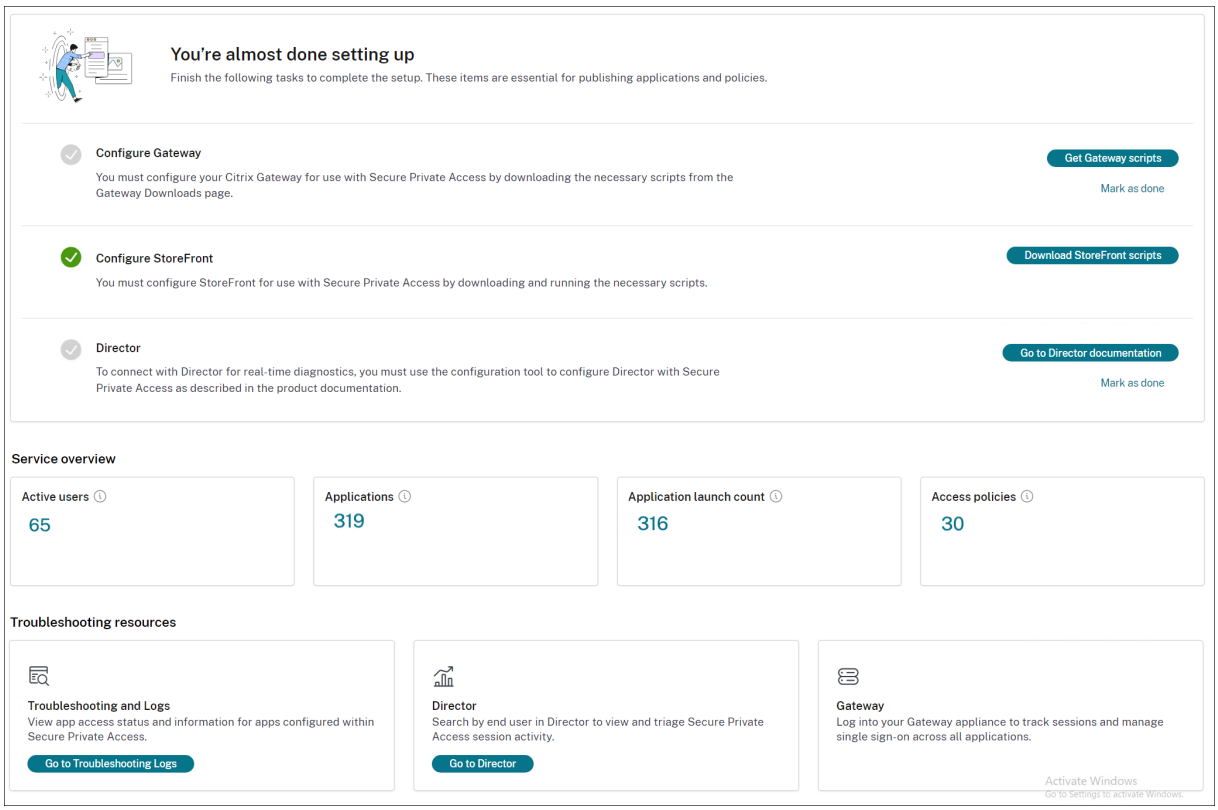
ステップ **4:** 構成の概要

構成が完了すると、検証が行われ、構成されたサーバーにアクセスできることが確認されます。また、Secure Private Access サーバーにアクセス可能であることを確認するためのチェックも行われます。

構成の概要ページにエラーが表示される場合は、「エラーのトラブルシューティング 」で詳細を確認してください。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。



セットアップが完了したら、「概要」ページの「閉じる」をクリックすると、次のページが表示されます。

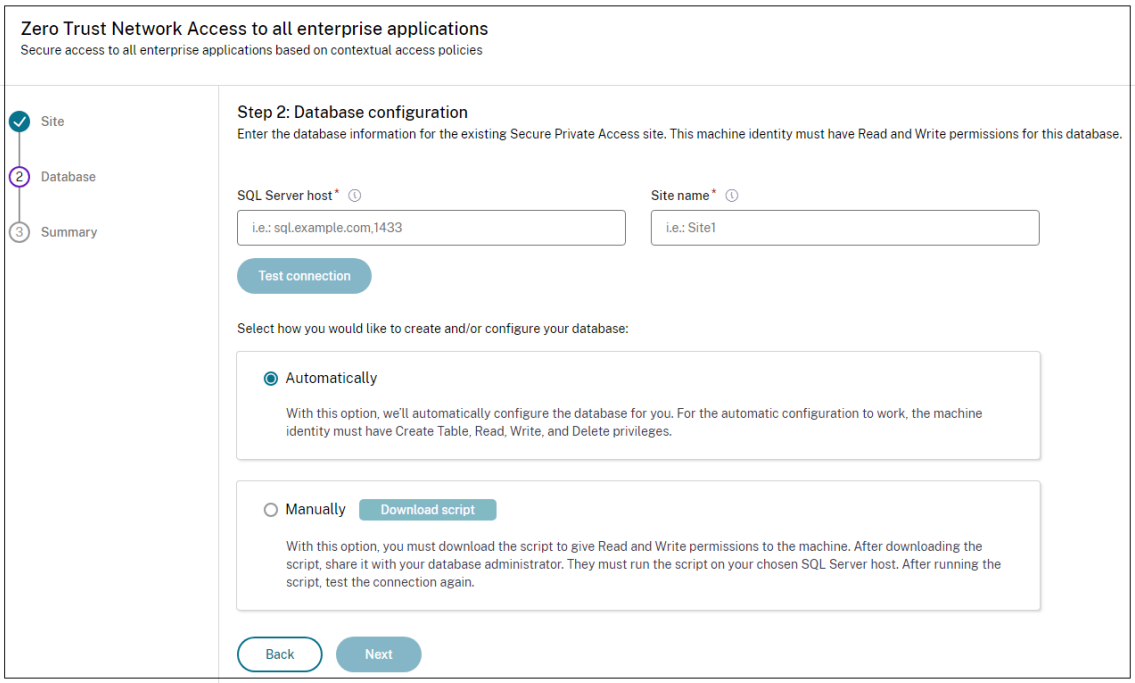


> 注:
>
> - 環境を設定したら、Web 管理コンソールの [設定] **>** **[**統合**]** から設定を変更できます。
> - Secure Private Access を初めてインストールした管理者には、完全な権限が付与されます。その後、この管理者は他の管理者をセットアップに追加できます。管理者のリストは、**[**設定**]** **>** **[**管理者**]** から表示できます。
> - また、管理者グループを追加して、そのグループのすべての管理者がアクセスできるようにすることもできます。

詳細については、「インストール後の設定の管理」を参照してください。

既存のサイトに参加して **Secure Private Access** を設定する

1. [サイトの作成または参加**]** ページで、**[**** 既存のサイトに参加する**]** を選択し、**[**** 次へ] をクリックします。

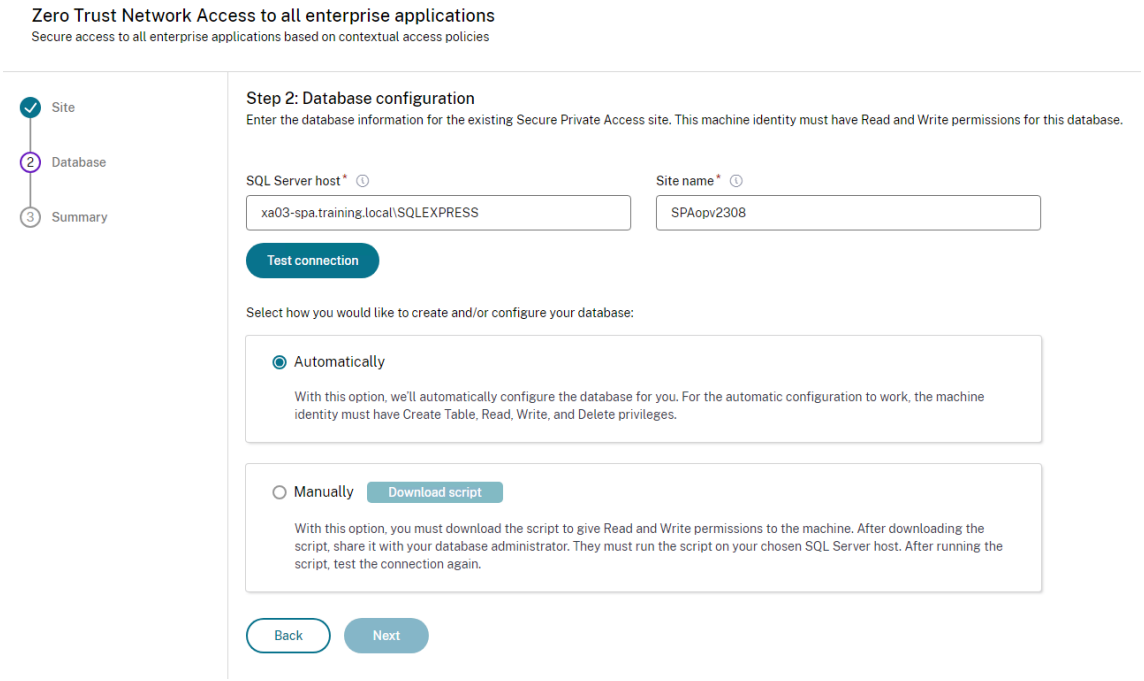


2. 「**SQL Server** ホスト」に、サーバーのホスト名を入力します。入力したサイト名に対応するデータベースが、選択した SQL Server に既に存在していることを確認してください。データベースのアドレスは、以下の形式のいずれかで指定できます:

   - サーバー名
   - ServerName\InstanceName
   - サーバー名、ポート番号

   詳しくは、「データベース」を参照してください。

3. [サイト] に、Secure Private Access サイトの名前を入力します。
4. [接続をテスト] をクリックして、SQL Server インスタンスが有効であることを確認し、指定したサイトがデータベースに存在することを確認します。



サイトに対応するデータベースがない場合、接続チェックは失敗します。

5. [**Save**] をクリックします。

構成の検証チェックは、SQL データベースサーバーが構成されていることを確認し、Secure Private Access サーバーにアクセス可能であることを確認するために行われます。

次の手順

- NetScaler Gateway Gateway の構成
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

コンポーネント

August 26, 2024

以下は、オンプレミス展開の一般的な Secure Private Access の主要コンポーネントです。

- **StoreFront:** -StoreFront はユーザーを認証し、ユーザーがアクセスするデスクトップとアプリケーションのストアを管理します。StoreFront により、デスクトップやアプリケーションへのセルフサービスアクセスをユーザーに提供する「エンタープライズアプリケーションストア」がホストされます。また、ユーザーのアプリケーションのサブスクリプション、ショートカット名、およびその他のデータを追跡します。これにより、

ユーザーが複数のデバイス間で一貫性のある操作を行えるようになります。StoreFront と Secure Private Access の統合について詳しくは、「StoreFront」を参照してください。

- **NetScaler** ゲートウェイ**:** -NetScaler Gateway は、企業のファイアウォールを介した単一の安全なアクセスポイントを提供します。NetScaler Gateway と Secure Private Access の統合について詳しくは、「NetScalerGateway」を参照してください。
- **Director:** (オプション) Director を使用すると、効果的なパフォーマンスの監視とトラブルシューティングが可能になります。Director を Secure Private Access と統合するには、Secure Private Access に登録する必要がある Director サーバーの FQDN の IP アドレスを入力する必要があります。Director と Secure Private Access の統合について詳しくは、「Director との Secure Private Access の統合」を参照してください。
- ライセンスサーバー**:** ライセンスサーバーはライセンスデータを収集して処理します。ライセンスサーバーと Secure Private Access の統合の詳細については、「ライセンスサーバーと Secure Private Access の統合」を参照してください。
- **Web Studio**: Citrix Secure Private Access は Web Studio コンソールに統合されているため、ユーザーは Web Studio からサービスにシームレスにアクセスできます。Web Studio との Secure Private Access の統合について詳しくは、「Web Studio との Secure Private Access の統合」を参照してください。

> 注**:**
>
> Director とライセンスサーバーは、リリース 2402 から Secure Private Access に統合されています。

NetScaler Gateway

October 21, 2024

> 重要**:**
>
> これらの変更を適用する前に、NetScaler スナップショットを作成するか、NetScaler 構成を保存することをお勧めします。

1. https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.htmlからスクリプトをダウンロードします。

   新しい NetScaler Gateway を作成するには、*ns_gateway_secure_access.sh* を使用します。

   既存の NetScaler Gateway を更新するには、*ns_gateway_secure_access_update.sh* を使用します。

2. これらのスクリプトを NetScaler マシンにアップロードします。WinSCP アプリまたは SCP コマンドを使用できます。たとえば、*`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*です。

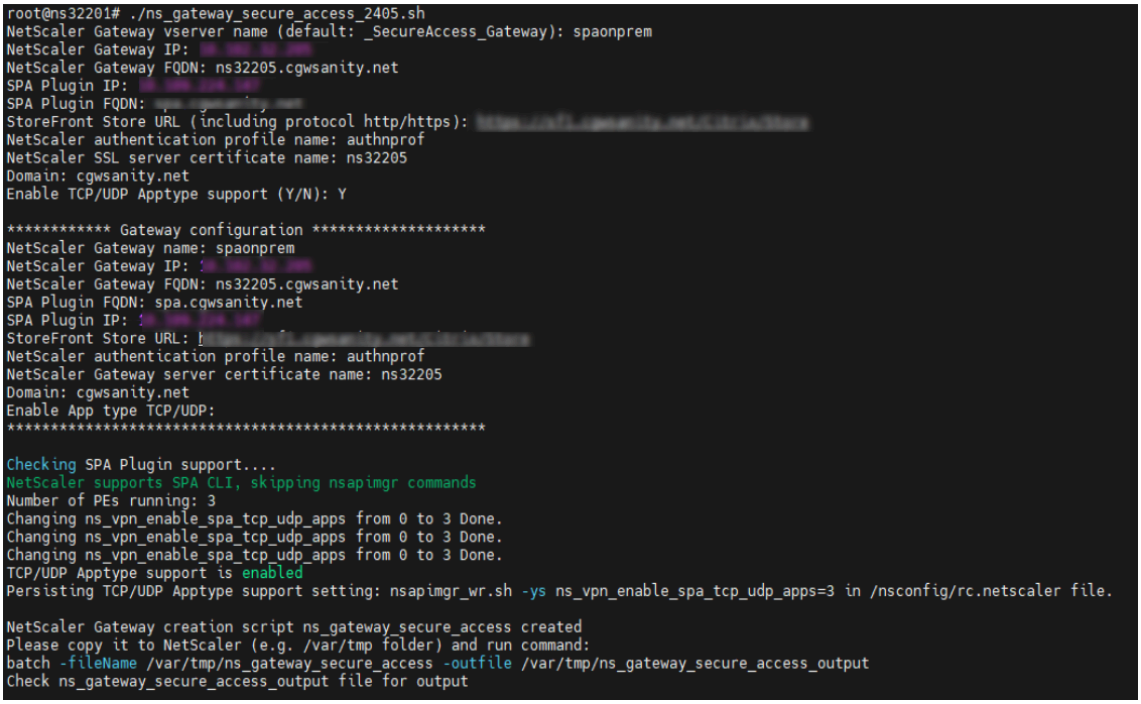
   たとえば、*`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*

> 注意:
>
> - 一時データを保存するには、NetScaler の /var/tmp フォルダーを使用することをお勧めします。
> - ファイルが LF 行末で保存されていることを確認してください。FreeBSD は CRLF をサポートしていません。
> - `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M: bad interpretation: No such file or directory`というエラーが表示される場合は、行末が正しくないことを意味します。Notepad++ などのリッチ テキスト エディターを使用してスクリプトを変換できます。

1. NetScaler に SSH で接続し、シェルに切り替えます (NetScaler CLI で「shell」と入力します)。
2. アップロードしたスクリプトを実行可能にします。これを行うには、chmod コマンドを使用します。

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

3. アップロードしたスクリプトを NetScaler シェルで実行します。



4. 必要なパラメータを入力します。パラメータのリストについては、「前提条件」を参照してください。

   認証プロファイルと SSL 証明書の場合は、NetScaler 上の既存のリソースの名前を指定する必要があります。

   複数の NetScaler コマンド (デフォルトは var/tmp/ns_gateway_secure_access) を含む新しいファイルが生成されます。

> 注意:
>
> スクリプトの実行中に、NetScaler と Secure Private Access プラグインの互換性がチェックされます。NetScaler が Secure Private Access プラグインをサポートしている場合、スクリプトにより、NetScaler

> の機能が、リソースへのアクセスが制限されているときにスマートアクセス タグの送信の改善と新しい拒否ページへのリダイレクトをサポートするようになります。スマート タグの詳細については、「スマート アクセス タグのサポート」を参照してください。
>
> /nsconfig/rc.netscaler ファイルに保持される Secure Private Access プラグイン機能により、NetScaler の再起動後も有効に保つことができます。

```
1 ![NetScaler 構成 2](/en-us/citrix-secure-private-access/media/spaop-
     configure-netscaler2.png)
```

1. NetScaler CLI に切り替えて、バッチ コマンドを使用して、新しいファイルから生成された NetScaler コマンドを実行します。たとえば、

   ```
   batch -fileName /var/tmp/ns_gateway_secure_access -outfile
   /var/tmp/ns_gateway_secure_access_output
   ```

   NetScaler はファイルからのコマンドを 1 つずつ実行します。コマンドが失敗した場合は、次のコマンドを続行します。

   リソースが存在する場合、または手順 6 で入力したパラメータの 1 つが正しくない場合、コマンドは失敗する可能性があります。

2. すべてのコマンドが正常に完了したことを確認します。

> 注意**:**
>
> エラーが発生した場合でも、NetScaler は残りのコマンドを実行し、リソースを部分的に作成/更新/バインドします。したがって、パラメータの 1 つが正しくないために予期しないエラーが発生した場合は、最初から設定をやり直すことをお勧めします。

既存の構成を使用して **NetScaler Gateway** でセキュア プライベート アクセスを構成する

既存の NetScaler Gateway でスクリプトを使用して、セキュア プライベート アクセスをサポートすることもできます。ただし、スクリプトでは次のものは更新されません。

- 既存の NetScaler Gateway 仮想サーバー
- NetScaler Gateway にバインドされた既存のセッションアクションとセッションポリシー

実行前に各コマンドを確認し、ゲートウェイ構成のバックアップを作成してください。

NetScaler Gateway 仮想サーバーの設定

既存の NetScaler Gateway 仮想サーバーを追加または更新する場合は、次のパラメータが定義された値に設定されていることを確認してください。

仮想サーバーの追加**:**

- tcp プロファイル名: nstcp_default_XA_XD_profile
- デプロイメントタイプ: ICA_STOREFRONT (`add vpn vserver` コマンドでのみ使用可能)
- ica のみ: オフ

仮想サーバーを更新します。

- tcp プロファイル名: nstcp_default_XA_XD_profile
- ica のみ: オフ

例:

仮想サーバーを追加するには:

```
add vpn vserver _SecureAccess_Gateway SSL 999.999.999.999 443 -
Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
authnProfile auth_prof_name -icaOnly OFF
```

仮想サーバーを更新するには:

```
set vpn vserver _SecureAccess_Gateway -icaOnly OFF
```

仮想サーバーのパラメータの詳細については、vpn-sessionActionを参照してください。

NetScaler Gateway セッションアクション

セッション アクションは、セッション ポリシーを持つゲートウェイ仮想サーバーにバインドされます。セッション アクションを作成するときは、次のパラメータが定義された値に設定されていることを確認します。

- 透過インターセプション: オフ
- SSO: オン
- ssoCredential: プライマリ
- MIP を使用: NS
- IIP を使用: オフ
- icaProxy: オフ
- wihome: "https://storefront.mydomain.com/Citrix/MyStoreWeb" - 実際のストアの URL に置き換えます。ストアへのパス /Citrix/MyStoreWeb はオプションです。
- クライアントの選択: オフ
- ntDomain: mydomain.com - SSO に使用 (オプション)
- デフォルト認証アクション: 許可
- authorizationGroup: SecureAccessGroup (このグループが作成されていることを確認してください。このグループは、Secure Private Access 固有の承認ポリシーをバインドするために使用されます)
- クライアントレスVPNモード: オン
- クライアントレスモードURL エンコーディング: 透過的

- セキュアブラウズ: 有効
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: ドメイン

例:

セッションアクションを追加するには:

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

セッションアクションを更新するには:

```
set vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON
```

```
1    For details on session action parameters, see <https://developer-docs
        .netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-
        sessionaction>.
```

Secure Private Access プラグインを VPN 仮想サーバーにバインドします。

```
bind vpn vserver spaonprem -appController "https://spa.example.corp"
```

ICA アプリとの互換性

Secure Private Access プラグインをサポートするために作成または更新された NetScaler Gateway は、ICA アプリの列挙と起動にも使用できます。この場合、Secure Ticket Authority (STA) を構成し、それを NetScaler Gateway にバインドする必要があります。注: STA サーバーは通常、Citrix Virtual Apps and Desktops DDC 展開の一部です。

詳細については、次のトピックを参照してください。

- NetScaler Gateway での Secure Ticket Authority の構成
- FAQ: Citrix Secure Gateway/NetScaler Gateway セキュア チケット認証局

スマートアクセスタグのサポート

次のバージョンでは、NetScaler Gateway はタグを自動的に送信します。スマート アクセス タグを取得するためにゲートウェイ コールバック アドレスを使用する必要はありません。

- 13.1-48.47 以降
- 14.1～4.42 以降

スマート アクセス タグは、Secure Private Access プラグイン要求のヘッダーとして追加されます。

これらの NetScaler バージョンでこの機能を有効/無効にするには、トグル `ns_vpn_enable_spa_onprem` または `ns_vpn_disable_spa_onprem` を使用します。

- コマンド (FreeBSD シェル) で切り替えることができます:

  ```
  nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
  ```

- 次のコマンド (FreeBSD シェル) を実行して、HTTP コールアウト構成の SecureBrowse クライアント モードを有効にします。

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode
  ```

- アクセスが拒否された場合に「アクセス制限」ページへのリダイレクトを有効にします。

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_d
  ```

- CDN でホストされている「アクセス制限」ページを使用します。

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page
  ```

- 無効にするには、同じコマンドを再度実行します。
- トグルがオンかオフかを確認するには、`nsconmsg` コマンドを実行します。
- NetScaler Gateway でスマート アクセス タグを構成するには、「コンテキスト タグの構成」を参照してください。

NetScaler で **Secure Private Access** プラグインの設定を保持する

NetScaler で Secure Private Access プラグインの設定を保持するには、次の手順を実行します。

1. ファイル /nsconfig/rc.netscaler を作成または更新します。
2. ファイルに次のコマンドを追加します。

   ```
   nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
   ```



```
nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode

nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_d

nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

3. ファイルを保存します。

NetScaler を再起動すると、Secure Private Access プラグインの設定が自動的に適用されます。

既知の制限事項

- 既存の NetScaler Gateway はスクリプトを使用して更新できますが、1 つのスクリプトではカバーできない NetScaler 構成が無数に存在する可能性があります。
- NetScaler Gateway では ICA プロキシを使用しないでください。NetScaler Gateway が構成されている場合、この機能は無効になります。
- クラウドに展開された NetScaler を使用する場合は、ネットワークにいくつかの変更を加える必要があります。たとえば、特定のポートで NetScaler と他のコンポーネント間の通信を許可します。
- NetScaler Gateway で SSO を有効にする場合は、NetScaler がプライベート IP アドレスを使用して StoreFront と通信することを確認してください。StoreFront プライベート IP アドレスを使用して、新しい StoreFront DNS レコードを NetScaler に追加する必要がある場合があります。

パブリックゲートウェイ証明書をアップロードする

パブリック ゲートウェイが Secure Private Access マシンからアクセスできない場合は、パブリック ゲートウェイ証明書を Secure Private Access データベースにアップロードする必要があります。

パブリック ゲートウェイ証明書をアップロードするには、次の手順を実行します。

1. 管理者権限で PowerShell またはコマンド プロンプト ウィンドウを開きます。
2. ディレクトリを、Secure Private Access インストール フォルダーの下の Admin\AdminConfigTool フォルダーに変更します (例: cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”)
3. 次のコマンドを実行します:

```
\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```


コンテキストタグの設定

August 26, 2024

Secure Private Access プラグインは、デバイスプラットフォームや OS、インストールされているソフトウェア、位置情報などのユーザーセッションコンテキストに基づいて、Web または SaaS アプリケーションへのコンテキストアクセス（スマートアクセス）を提供します。

管理者はコンテキストタグ付きの条件をアクセスポリシーに追加できます。Secure Private Access プラグインのコンテキストタグは、認証されたユーザーのセッションに適用される NetScaler Gateway ポリシー（セッション、事前認証、EPA）の名前です。

Secure Private Access プラグインは、スマートアクセスタグをヘッダー (新しいロジック) として受け取るか、Gateway にコールバックすることで受け取ることができます。詳細については、「スマートアクセスタグ」を参照してください。

> 注:
>
> Secure Private Access プラグインは、NetScaler Gateway で構成できるクラシックゲートウェイ事前認証ポリシーのみをサポートします。

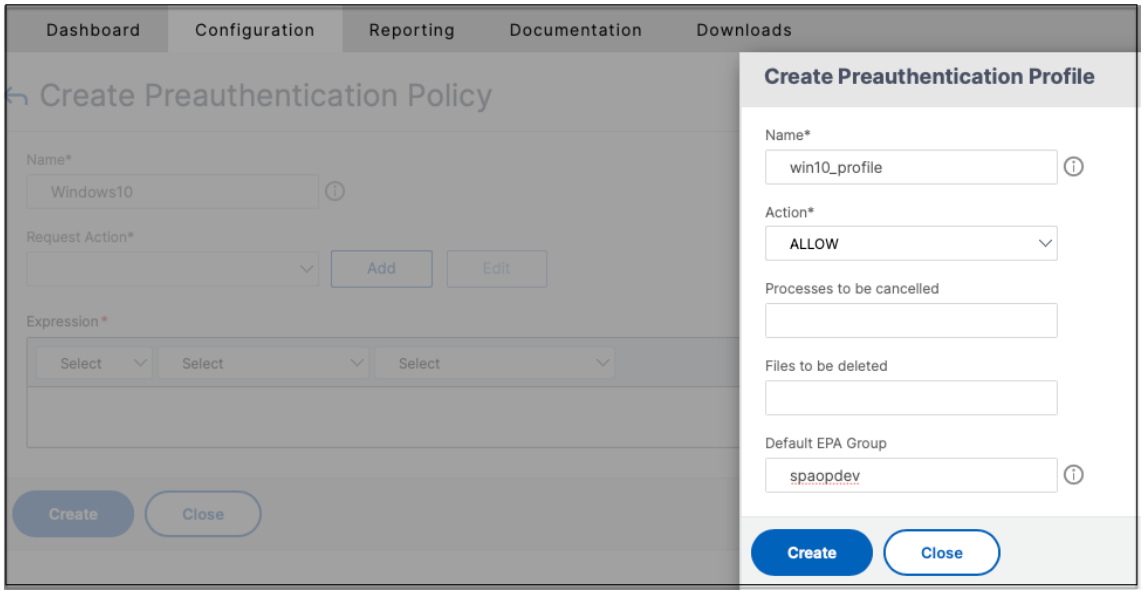
GUI を使用してカスタムタグを設定する

コンテキストタグの設定には、以下の大まかな手順が含まれます。

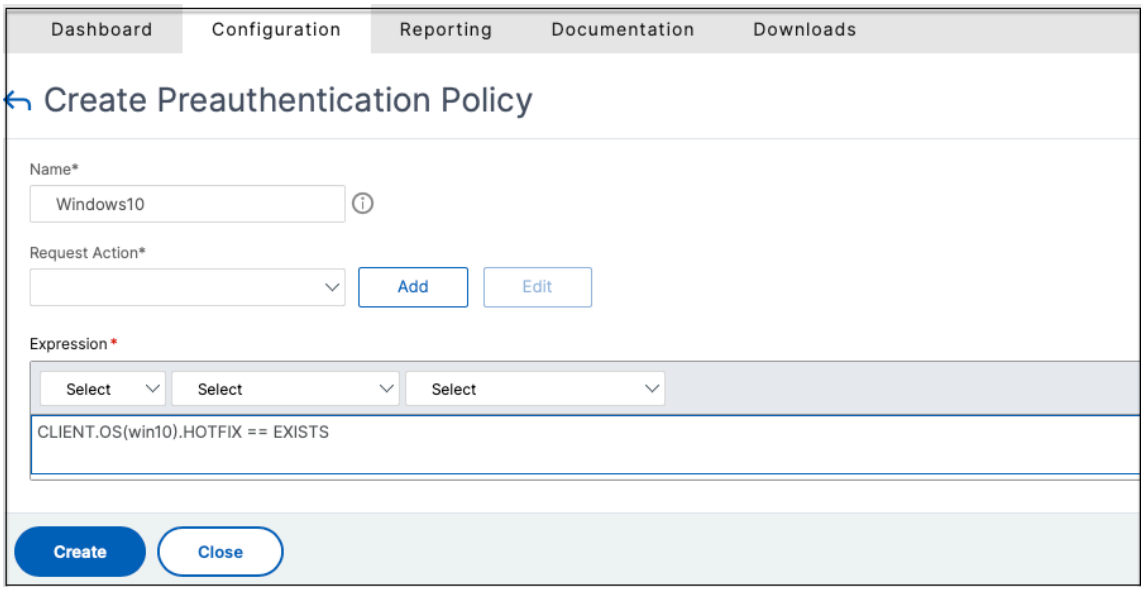
1. クラシックゲートウェイ事前認証ポリシーの設定
2. 従来の事前認証ポリシーをゲートウェイ仮想サーバーにバインドする

クラシックゲートウェイ事前認証ポリシーの設定

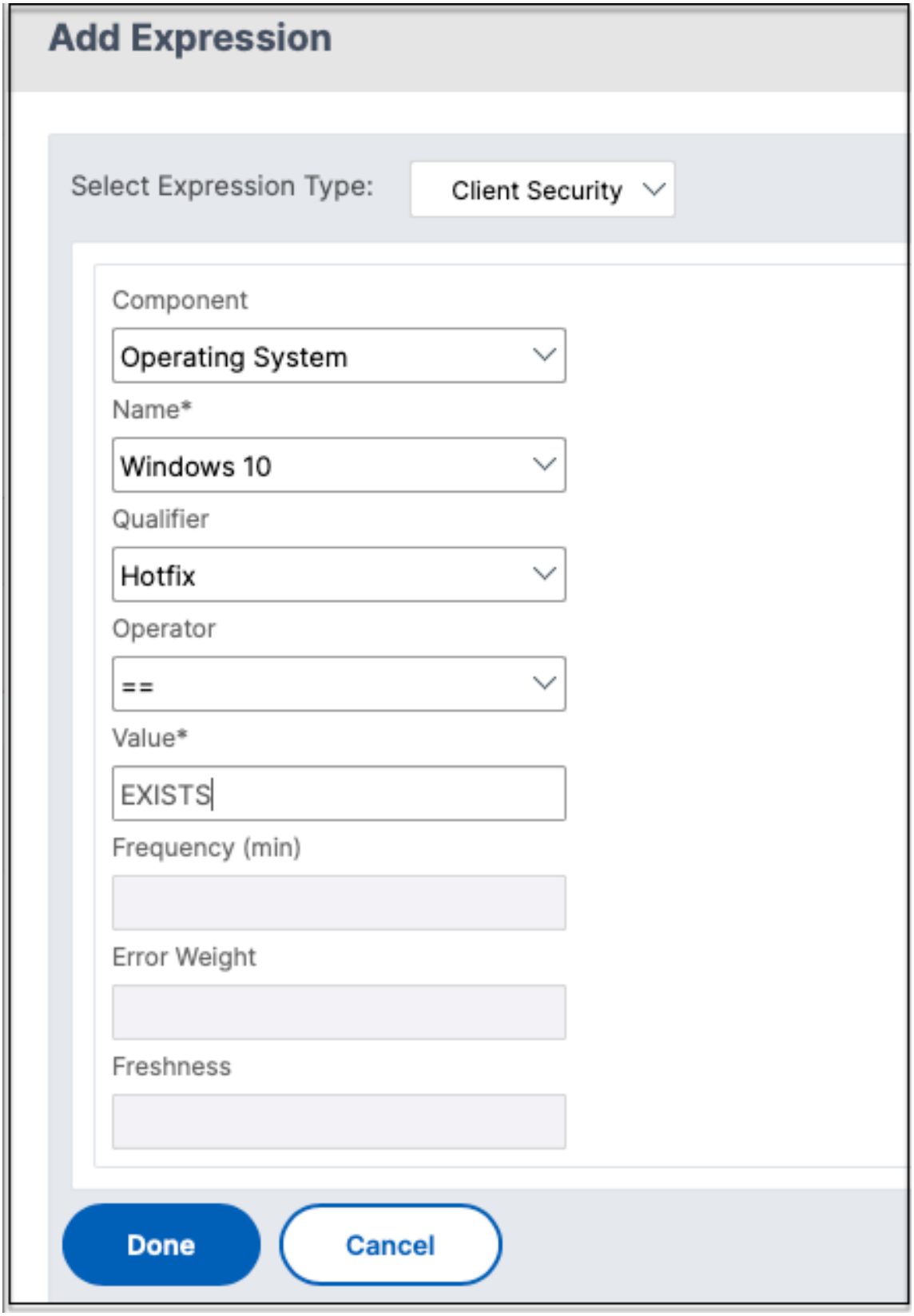
1. ［**NetScaler Gateway**］**>**［ポリシー］**>**［事前認証］に移動し、［追加］をクリックします。
2. 既存のポリシーを選択するか、ポリシーの名前を追加します。このポリシー名はカスタムタグ値として使用されます。
3. 「リクエストアクション」で、「追加」をクリックしてアクションを作成します。このアクションは複数のポリシーで再利用できます。たとえば、あるアクションを使用してアクセスを許可し、別のアクションを使用してアクセスを拒否できます。



4. 必須フィールドに詳細を入力し、「作成」をクリックします。
5. [式] に、式を手動で入力するか、式エディタを使用してポリシーの式を作成します。



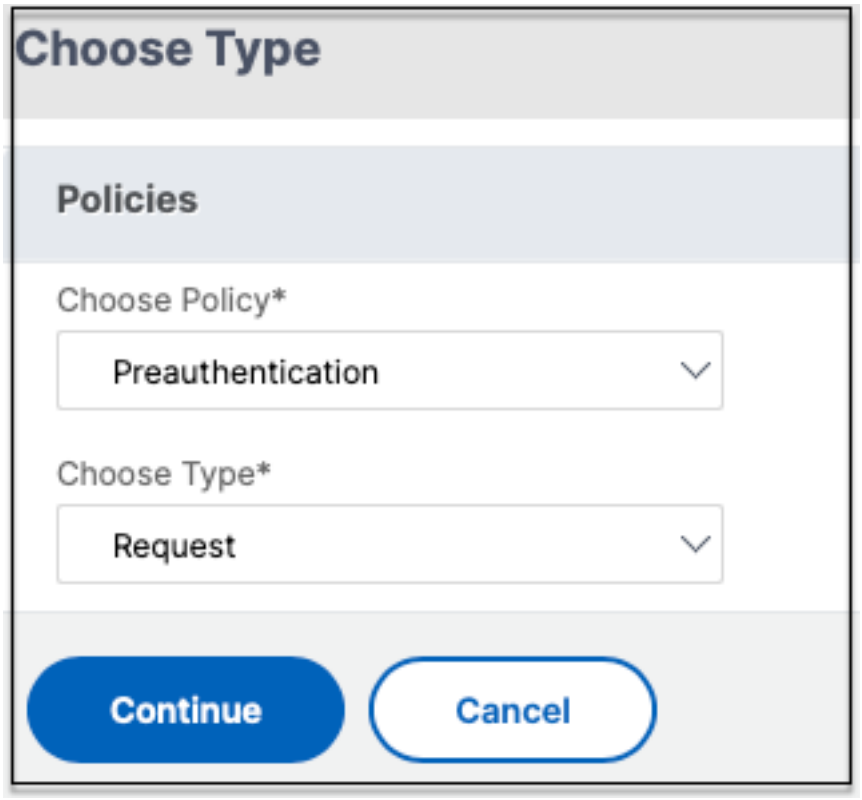
次の図は、Windows 10 OS をチェックするために作成されたサンプル式を示しています。



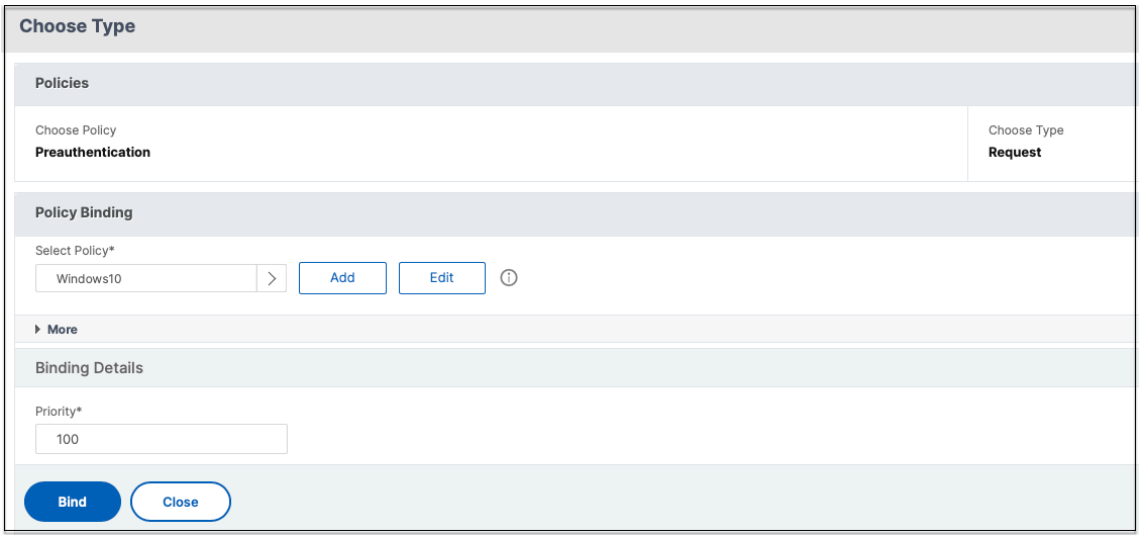
6.［作成］をクリックします。

カスタムタグを **NetScaler Gateway** にバインドする

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. 事前認証ポリシーをバインドする仮想サーバーを選択し、[編集] をクリックします。
3. 「ポリシー」セクションで、「**+** 」をクリックしてポリシーをバインドします。
4. 「ポリシーの選択」で事前認証ポリシーを選択し、「タイプの選択」で「要求」を選択します。



5. ポリシー名とポリシー評価の優先度を選択します。
6. [**Bind**] をクリックします。



CLI を使用してカスタムタグを設定する

NetScaler CLI で次のコマンドを実行して、事前認証ポリシーを作成してバインドします。

例:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

新しいコンテキストタグの追加

1. Secure Private Access 管理コンソールを開き、「アクセスポリシー」をクリックします。
2. 新しいポリシーを作成するか、既存のポリシーを選択します。
3. 「次の条件が満たされている場合」セクションで、「条件を追加」をクリックし、「コンテキストタグ」、「すべてに一致」を選択し、コンテキストタグ名 (例:`Windows10`) を入力します。

参照ドキュメント

- アプリケーションのアクセスポリシーを設定します。
- スマートアクセスタグのサポート。

StoreFront

August 26, 2024

Secure Private Access が StoreFront と共存している場合、StoreFront の Secure Private Access 構成は初回セットアップウィザードで自動的に行われます。

ただし、Secure Private Access を StoreFront と共存させていない場合は、特定の構成変更を手動で行う必要があります。

StoreFront を手動で構成するには、次の手順を実行します。

1. Secure Private Access 管理コンソール ([設定] **>** [統合]) からスクリプトをダウンロードします。
2. 構成を変更する必要がある StoreFront エントリに対応するスクリプトのダウンロードをクリックします。

   ダウンロードされた zip ファイルには、構成スクリプト、README ファイル、および構成クリーンアップスクリプトが含まれています。クリーンアップスクリプトは、StoreFront と Secure Private Access 間の統合を削除する場合に使用できます。
3. 次のコマンドを使用して、PowerShell 64 ビットインスタンスの管理者としてスクリプトを実行します。`./ConfigureStorefront.ps1`.

   - 他のパラメータは必要ありません。
   - StoreFront スクリプトを実行するには、PowerShell スクリプト実行ポリシーを［制限なし］または［バイパス］に設定する必要があります。
   - StoreFront reFront がクラスターとして構成されている場合、このスクリプトは構成を他の StoreFront サーバーにも伝播します。

StoreFront を Secure Private Access 設定で構成すると、Secure Private Access プラグインの構成が StoreFront 管理 UI（**Delivery Controller** の管理画面）に表示されます。

Citrix Virtual Apps and Desktops Delivery Controller で同じアグリゲーショングループ設定が構成されている場合、StoreFront スクリプトは Secure Private Access のアグリゲーショングループ設定を自動的に構成します。デフォルトでは、このスクリプトはすべてのユーザーに Secure Private Access を設定します（ユーザーマッピングとマルチサイトアグリゲーションの設定 **>** 設定済み）。

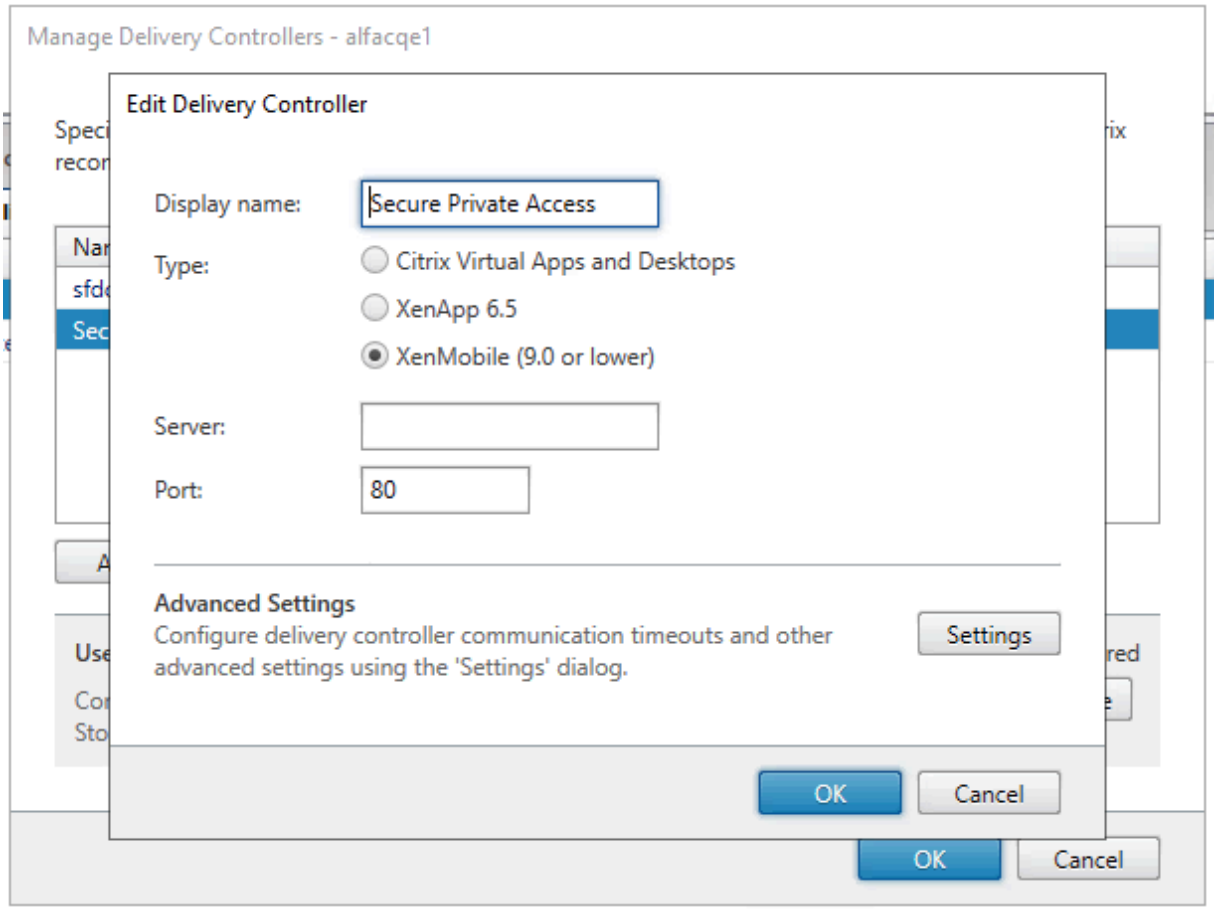
> 重要:
>
> - Secure Private Access 管理 UI からダウンロードした StoreFront スクリプトを使用して、Secure Private Access 専用に StoreFront を構成することをお勧めします。StoreFront 管理 UI から Secure Private Access を構成しないでください。UI には StoreFront で必要な構成がすべて含まれていないためです。必要な設定をすべて完了するには、スクリプトを実行する必要があります。
> - 1 つの Secure Private Access サイトを、複数の StoreFront 展開（同じ StoStoreFront 上の別のストアまたは別の StoreFront 展開環境）で構成することもできます。

> StoreFront は、［設定］**>**［統合］ページから追加できます。
>
> - Secure Private Access が StoreFront と共存している場合でも、StoreStoreFront の自動構成は [設定] **>** [統合] ページでは機能しません。自動構成は、初回セットアップ時にのみ行われます。設定ページから新しいストア構成を追加する場合 、StoreFront スクリプトをダウンロードして対応する StoreFront マシンで実行する必要があります。

StoreFront バージョン **2.308** 以前のバージョンを使用している場合

StoreFront バージョン 2308 以前を使用している場合、StoreFront 管理 UI には次の既知の問題があります。

- Secure Private Access プラグインタイプは XenMobile として表示されます。
- Secure Private Access サーバーの URL は表示されません。
- Secure Private Access ポートは常に 80 と表示されます。



StoreFront バージョン **2.3.11** 以降を使用している場合

StoreFront バージョン 2311 以降では、Web 向け Citrix Workspace クライアントは Secure Private Access アプリを列挙しません。これは、Secure Private Access が Workspace for Web プラットフォームでの Secure

Private Access アプリの起動をサポートしていないためです。

Director

August 26, 2024

Director を Secure Private Access と統合することで、効果的なパフォーマンスの監視とトラブルシューティングが可能になります。Director を Secure Private Access と統合するには、Secure Private Access に登録する必要がある Director サーバーの FQDN の IP アドレスを入力する必要があります。詳細については、「サーバーの統合」を参照してください。

Director を Secure Private Access に登録することは、オンプレミスバージョン 2402 のお客様向けの Secure Private Access の必須設定です。Director が構成されていない場合は、Director の最新バージョンである LTSR 2402 以降をインストールする必要があります。Director がすでに構成されている場合は、最新バージョンである LTSR 2402 以降にアップグレードする必要があります。Secure Private Access の設定は、Director を登録しないと完了できません。検証は次の場合にも失敗します。

- Director は Secure Private Access に登録されていません。
- 入力した Director の IP アドレスまたは FQDN は存在しません。

Director を Secure Private Access に登録する方法について詳しくは、「StoreFront サーバーと NetScaler Gateway サーバーの統合」および 「インストール後の設定の管理」を参照してください。

> 注:
>
> - Director の登録またはログオンは、統合 Windows 認証 (IWA) をサポートしていません。管理者が IWA を使用して Secure Private Access コンソールにログインした場合、管理者は Director 登録の認証情報を入力するよう求められます。
> - 管理者が Secure Private Access コンソールに手動でサインオンした場合、それらの情報は Director サーバーへの認証に利用されます。それでも成功しない場合、管理者は認証情報の入力を求められます。
> - セットアップの完了後に管理者が別の Director を追加する必要がある場合は、「設定の管理」ページから新しい Director を登録します。セットアップ後に Director の詳細を更新する場合、管理者は変更を行うために認証情報を入力する必要があります。Director URL IPv6、SSLv3 の編集では、シングルサインオンはサポートされていません。

Director 設定ツールを使用して **Director** を **Secure Private Access** で設定する

Config ツールを使用して Director を Secure Private Access に設定することは、統合を完了するための必須ステップです。詳しくは、「Director との Secure Private Access の統合」を参照してください。

Director での **Secure Private Access** のユーザーセッションの表示

Director では、Secure Private Access のユーザーセッションを表示できます。詳細については、「ユーザーごとの Secure Private Access セッションの表示」を参照してください。

ライセンスサーバー

August 26, 2024

Secure Private Access プラグインのライセンスサーバーは、ライセンスデータの収集と処理に必要な必須コンポーネントです。ライセンスサーバーは、初期セットアップ時に Secure Private Access に登録することも、セットアップの完了後に構成または更新することもできます。ライセンスサーバーを Secure Private Access に登録する方法について詳しくは、「StoreFront サーバーと NetScaler Gateway サーバーの統合」および 「インストール後の設定の管理」を参照してください。

Secure Private Access をライセンスサーバーに接続するには、ライセンスサーバーの URL を指定する必要があります。Secure Private Access プラグインは、自動的にライセンスサーバーに登録されます。

> 注:
>
> - ライセンスサーバーに Secure Private Access プラグインを登録するには、ライセンスサーバーに少なくとも 1 つの Citrix Virtual Apps and Desktops ブローカーライセンスをインストールする必要があります。
> - Secure Private Access プラグインのライセンスサーバーは、バージョン 11.17.2 ビルド 45000 以降でサポートされています。ライセンスサーバーをすでにお持ちの場合は、ライセンスサーバーをバージョン 11.17.2 ビルド 45000 以降のバージョンにアップグレードする必要があります。

ライセンスサーバーの詳細については、「ライセンスサーバー」を参照してください。

Web Studio

August 26, 2024

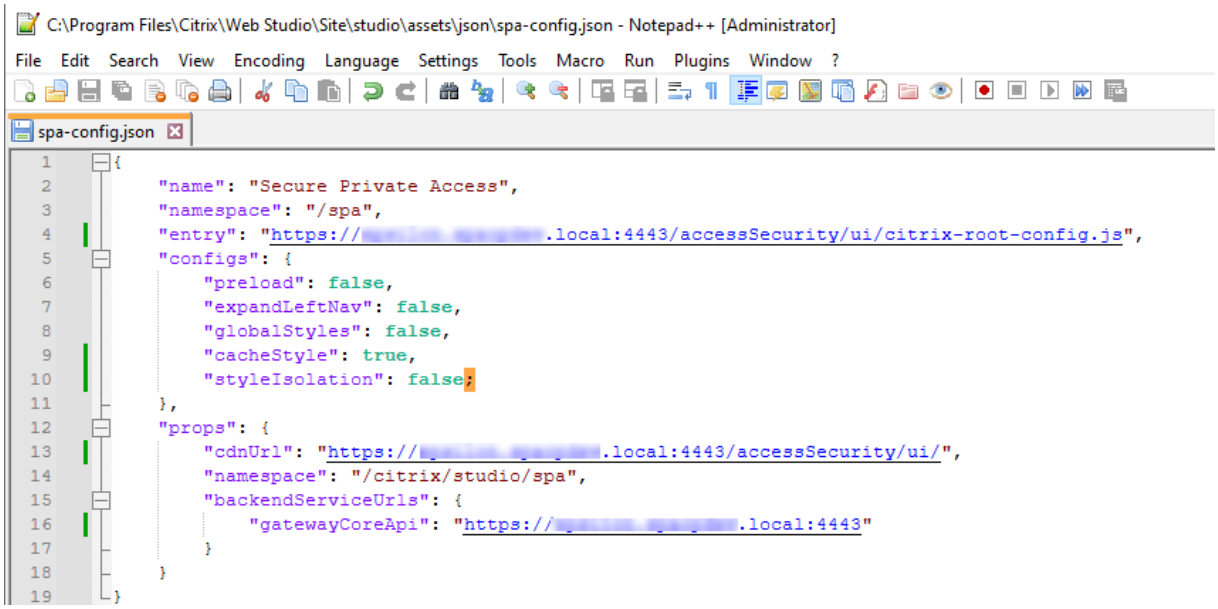
Citrix Secure Private Access も Web Studio コンソールに統合されているため、ユーザーは Web Studio を介してサービスにシームレスにアクセスできます。

Web Studio バージョン 2308 以降をインストールする必要があります。

Web Studio 統合を有効にするには、次の手順を実行します:

1. Citrix Web Studio は、Citrix Virtual Apps and Desktops インストーラーまたは統合 DDC インストーラーを使用してインストールします。
2. 画面上の指示に従い、インストールを完了します。コントローラアドレスの入力を求められたら、コントローラアドレスとして DDC FQDN を入力します。
3. インストールが成功したら、C:\Program Files\ Citrix\ Web Studio\ Site\ studio\ assets\ json フォルダーに移動し、spa-config.json ファイルの内容を変更します。

   Web Studio のインストールにデフォルト以外の場所が使用された場合は、C:\Program Files\ Citrix のデフォルトのインストール場所を正しい場所に置き換えてください。



1.「SPAServer」を Secure Private Access プラグインの FQDN に置き換えてください。
2. Web Studio にログインします。
3. 左側のナビゲーションメニューで [**Secure Private Access **] をクリックして、Web Studio から Secure Private Access 管理コンソールにアクセスします。

HTTP/HTTPS アプリケーションの設定

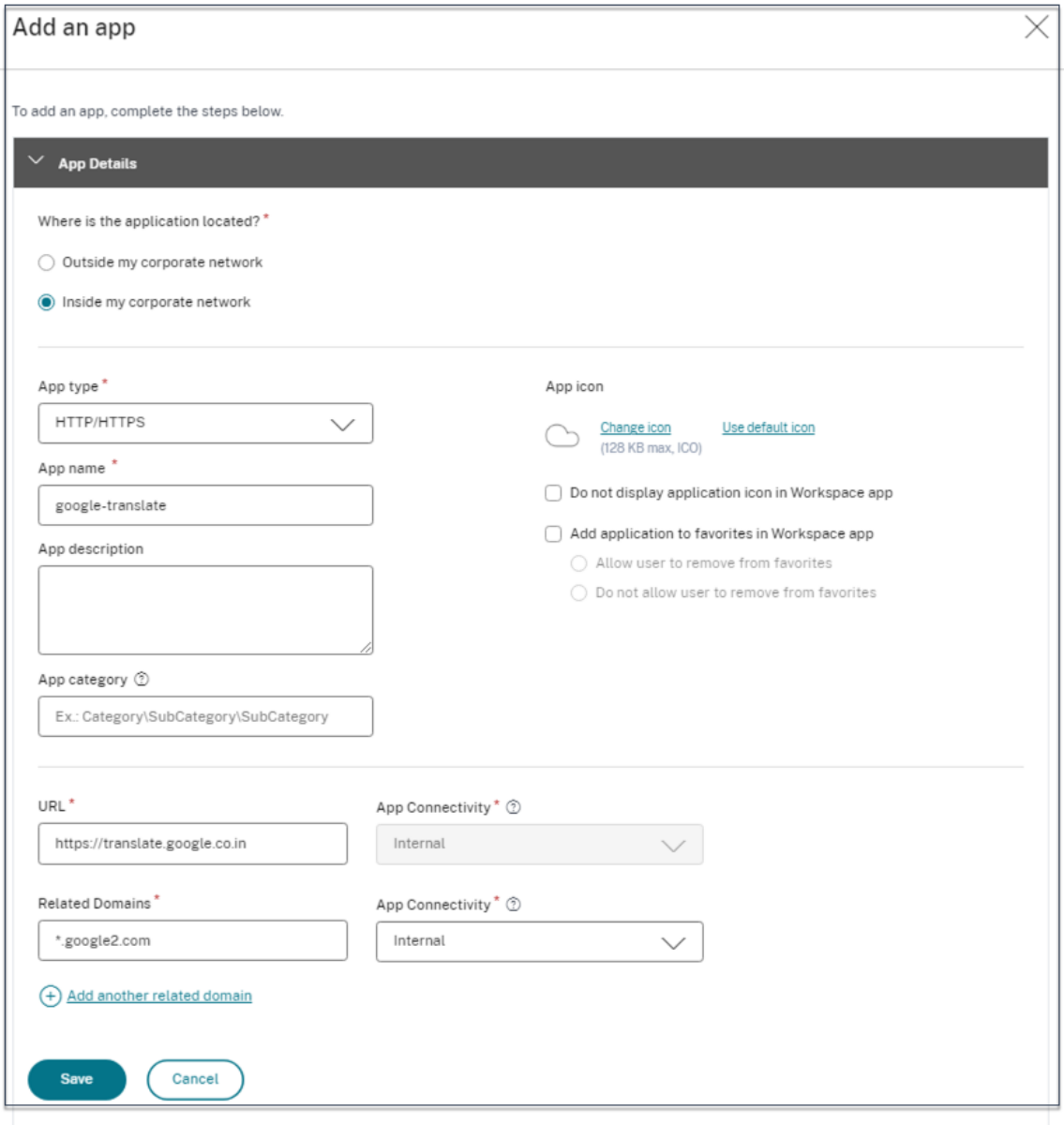
August 26, 2024

Secure Private Access を設定したら、管理コンソールからアプリとアクセスポリシーを設定できます。

1. 管理コンソールで、「アプリケーション」をクリックします。
2. [アプリの追加] をクリックします。
3. アプリが存在する場所を選択します。

- 社内ネットワーク外の外部アプリケーション用
- 社内ネットワークの内部アプリケーション用

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



- アプリ名—アプリケーションの名前。
- アプリの説明 -アプリの簡単な説明。この説明は、ワークスペースのユーザーに表示されます。アプリケーションのキーワードをフォーマットKEYWORDS: <keyword_name>で入力することもできます。キーワードを使用してアプリケーションをフィルタリングできます。詳細については、「含まれているキーワードによるリソースのフィルタリング」を参照してください。
- アプリカテゴリ -公開するアプリが Citrix Workspace UI に表示される必要があるカテゴリとサブカテゴリ名（該当する場合）を追加します。アプリごとに新しいカテゴリを追加するか、Citrix Workspace

UI から既存のカテゴリを使用できます。Web アプリまたは SaaS アプリのカテゴリを指定すると、そのアプリは Workspace UI の特定のカテゴリの下に表示されます。

  - カテゴリ/サブカテゴリは管理者が設定可能で、管理者はアプリごとに新しいカテゴリを追加できます。
  - 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、「ビジネスと生産性\ エンジニアリング」などです。また、このフィールドは大文字と小文字が区別されます。管理者は、正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UI の名前と［アプリカテゴリ］フィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとして表示されます。

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

- アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128x128 ピクセルでなければならず、Ico 形式のみがサポートされています。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。
- アプリケーションをユーザーに表示しない-ユーザーにアプリを表示したくない場合は、このオプションを選択してください。
- **URL** —アプリケーションの URL。
- 関連ドメイン—関連ドメインは、アプリケーション URL に基づいて自動入力されます。管理者は、関連する内部ドメインまたは外部ドメインをさらに追加できます。

  > 注:
  >
  > - アプリの関連ドメインが別のアプリの関連ドメインと重複していないことを確認します。このような場合は、すべてのアプリから関連ドメインを削除し、このドメインを使用して新しいアプリを作成してから、アクセスポリシーでそれに応じてアクセスを設定してください。このアプリを StoreFront に表示するか非表示にするかを検討することもできます。StoreFront でアプリを非表示にするには、［アプリの公開中にユーザーにアプリケーションを表示しない］オプションを使用します。
  > - 同様に、公開アプリの URL を別のアプリの関連ドメインとして追加してはなりません。
  > - 詳細については、「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。

- アプリケーションをお気に入りに自動的に追加—このオプションをクリックすると、このアプリが Citrix Workspace アプリのお気に入りアプリとして追加されます。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。
  - ユーザーにお気に入りからの削除を許可—アプリ利用者が 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、このオプションをクリックします。

このオプションを選択すると、Citrix Workspace アプリの左上隅に黄色の星のアイコンが表示されます。

- ユーザーにお気に入りからの削除を許可しない—このオプションをクリックすると、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くなります。

Secure Private Access 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、それらのアプリは 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 コンソールからアプリを削除しても、アプリは StoreFront から自動的に削除されません。

- アプリ接続 -Web アプリの場合は [内部]、SaaS アプリの場合は [外部] を選択します。

5. [保存] をクリックし、[完了] をクリックします。

[設定] **>** [アプリケーションドメイン] で設定されているすべてのアプリケーションドメインを表示できます。詳細については、「インストール後の設定の管理」を参照してください。

次の手順

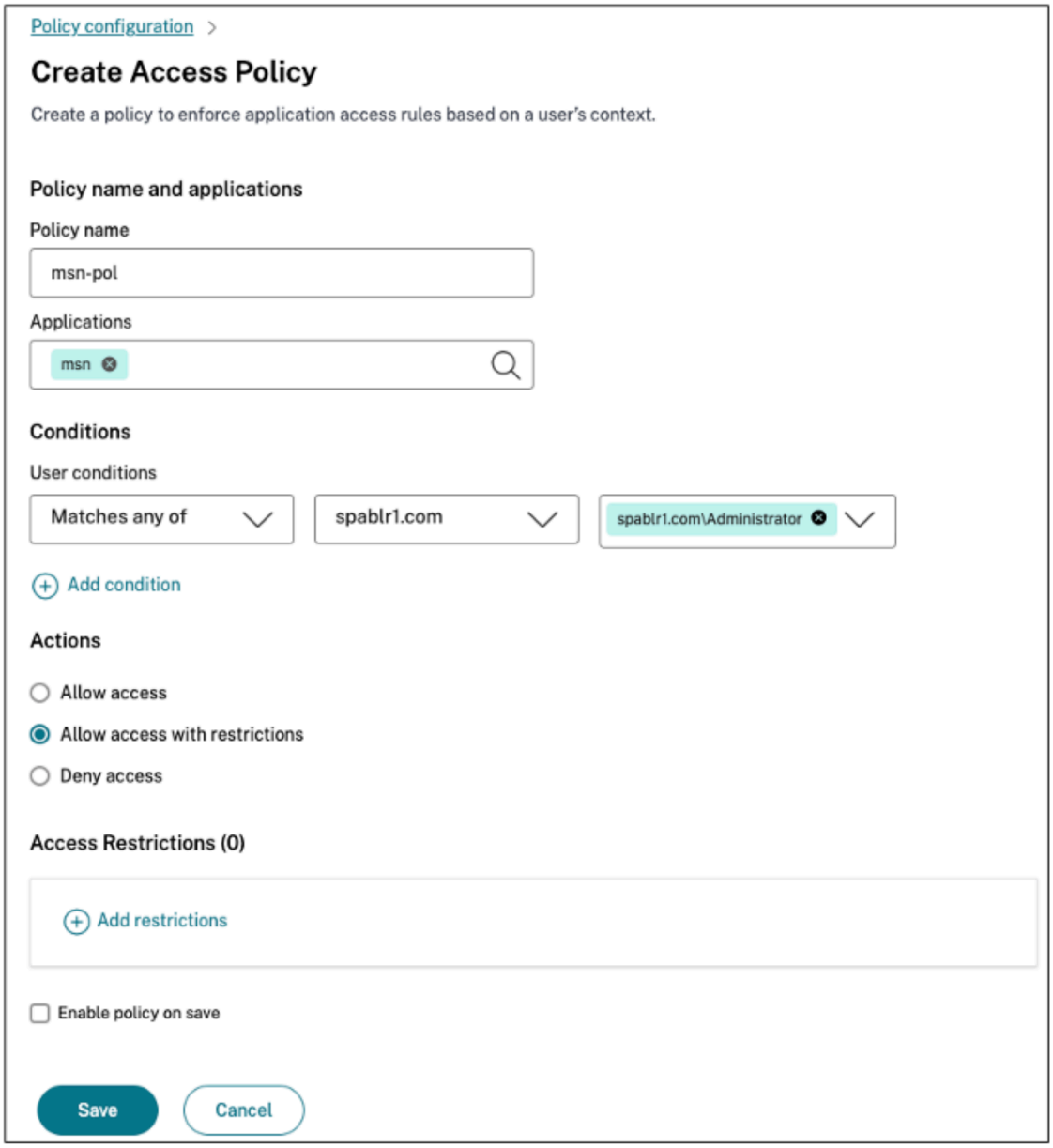
アプリケーションのアクセスポリシーを設定します

アプリケーションのアクセスポリシーを構成する

October 21, 2024

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 グループ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、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 (HTTP/HTTPS) を有効にすることもできます。

1. 管理コンソールで、[アクセス ポリシー] をクリックします。
2. [ポリシーの作成] をクリックします。



3. a)「ポリシー名」に、ポリシーの名前を入力します。
4. アプリケーションで、アクセス ポリシーを適用するアプリを選択します。
5. ユーザー条件–アプリ アクセスを許可または拒否する必要がある条件とユーザーまたはユーザー グループを選択します。
   - 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。
   - いずれにも一致しません: フィールドにリストされてい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。
6. コンテキスト タグに基づいて別の条件を追加するには、[条件の追加] をクリックします。これらのタグは

NetScaler Gateway から派生したものです。

7. アクションで、条件評価に基づいてアプリに適用する必要がある次のアクションのいずれかを選択します。

   - 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

   制限付きアクセスを許可するを選択した場合は、制限を追加 をクリックして制限を選択する必要があります。各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。

   制限を選択して、[完了] をクリックします。

> 注意:
>
> アクション 制限付きアクセスを許可する は、TCP/UDP アプリには適用されません。

```
1 ![アクセス制限](/en-us/citrix-secure-private-access/media/secure-
    private-access-multirule-access-restrictions-onprem.png)
```

1. 保存時にポリシーを有効にするを選択します。このオプションを選択しない場合、ポリシーは作成されるだけで、アプリケーションには適用されません。または、トグル スイッチを使用して、[アクセス ポリシー] ページからポリシーを有効にすることもできます。

アクセスポリシーの優先順位

アクセス ポリシーが作成されると、デフォルトでアクセス ポリシーに優先番号が割り当てられます。アクセス ポリシーのホームページで優先順位を確認できます。

値の低い優先度は最も優先度が高く、最初に評価されます。このポリシーが定義された条件に一致しない場合は、優先順位番号が低い次のポリシーが評価されます。

優先度 列の上下アイコンを使用してポリシーを上下に移動することで、優先順位を変更できます。

次の手順

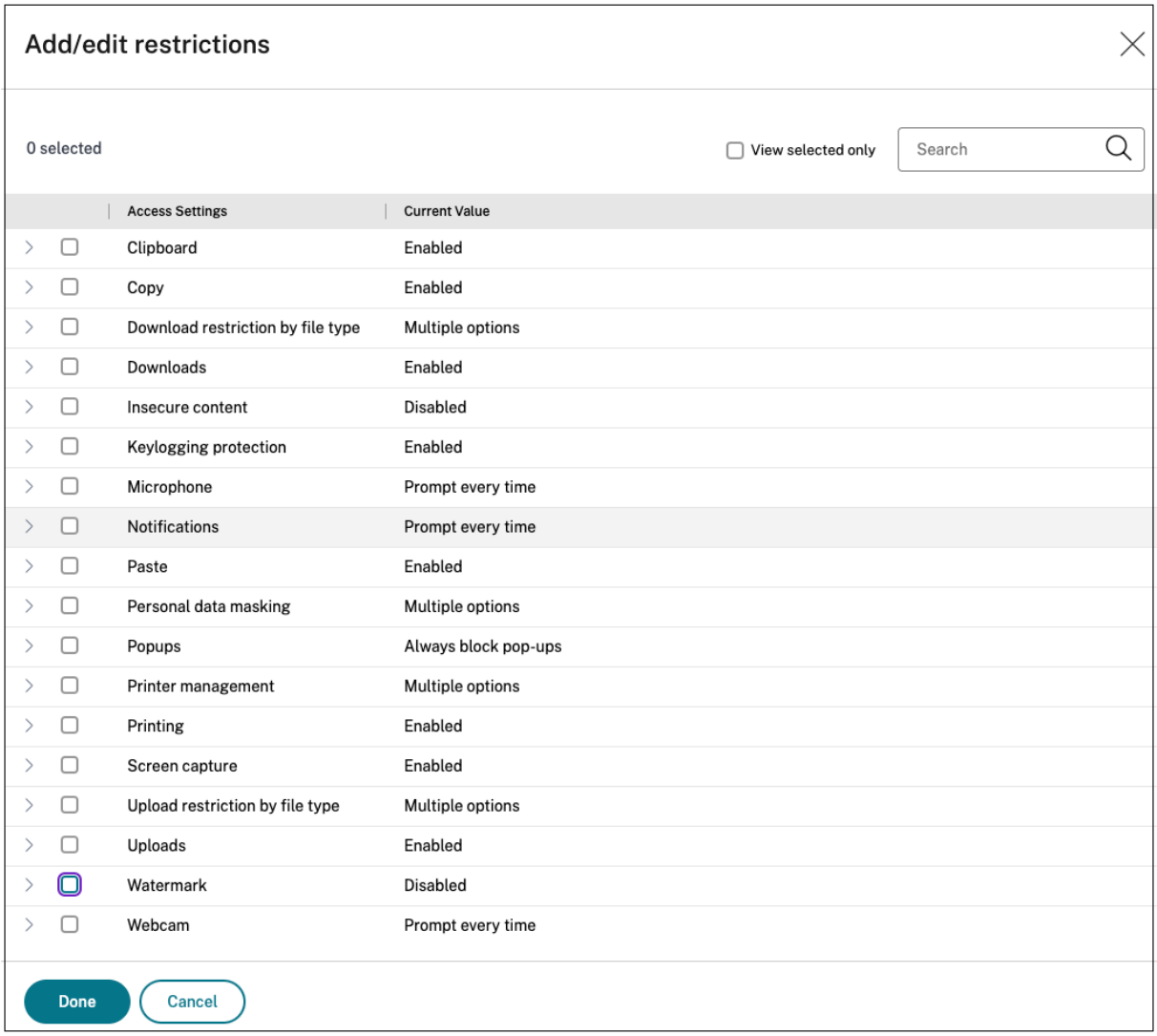
- クライアント マシン (Windows および macOS) から構成を検証します。
- TCP/UDP アプリの場合、Citrix Secure Access クライアントにログインして、クライアント マシン (Windows および macOS) から構成を検証します。

サンプル構成の検証

アクセス制限オプション

October 21, 2024

アクション 制限付きアクセスを許可するを選択すると、要件に応じてセキュリティ制限を選択できます。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。



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 ブラウザ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 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 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。

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。

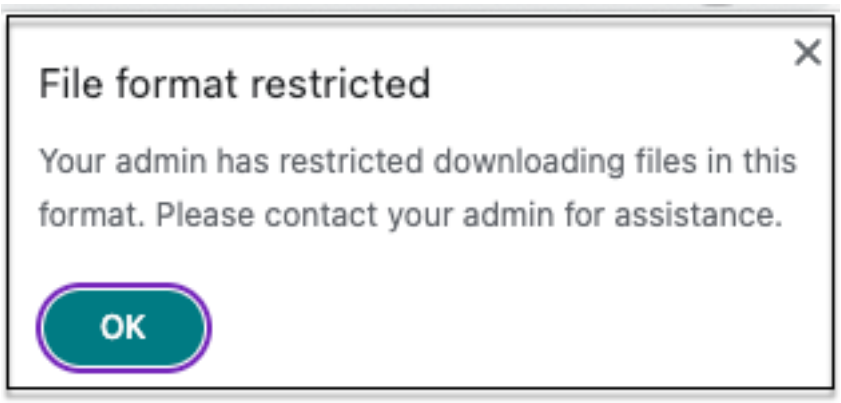
1. アクセス ポリシーを作成または編集します。アクセス ポリシーの作成の詳細については、「アクセス ポリシーの構成」を参照してください。
2. アクションで、制限付きで許可を選択します。
3. ファイルタイプによるダウンロード制限 をクリックし、次に 編集をクリックします。
4. ファイルタイプ別のダウンロード制限設定 ページで、次のいずれかを選択します。
   - 例外を除いてすべてのダウンロードを許可します–ブロックする必要があるタイプを選択し、他のすべてのタイプを許可します。
   - 例外を除いてすべてのダウンロードをブロックします–アップロードできるタイプのみを選択し、他のすべての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

   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 は次の警告メッセージを表示します。



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

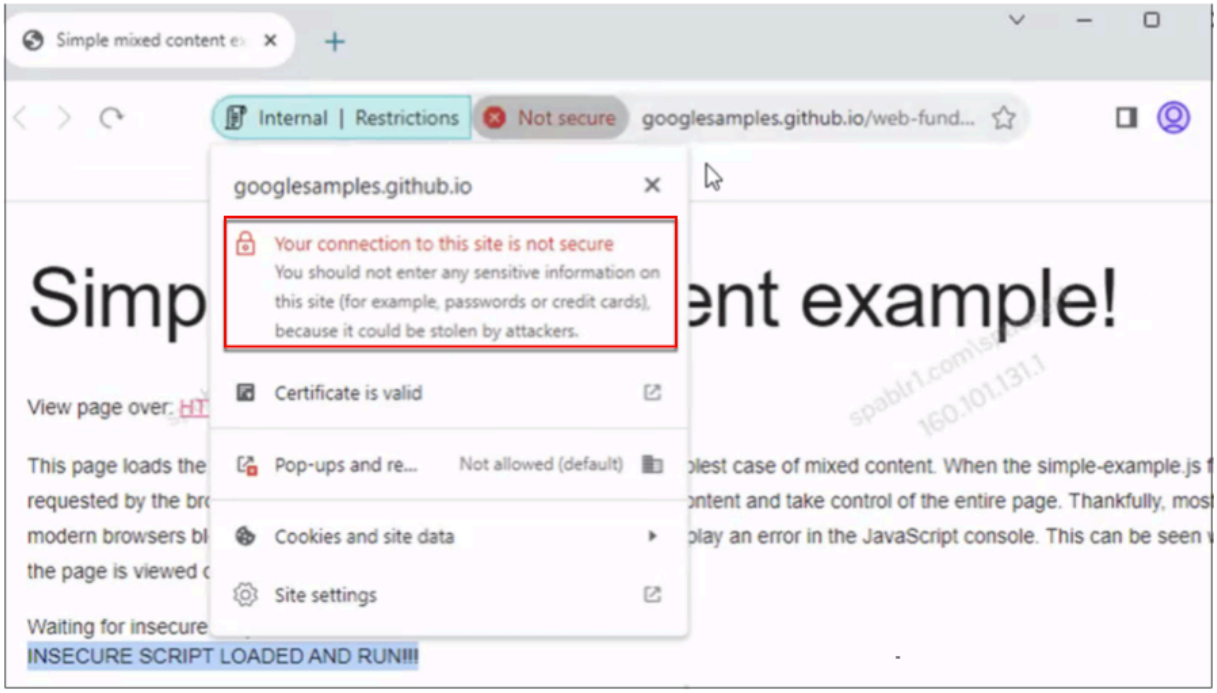
Citrix Enterprise Browser 経由でアクセスする場合、このポリシーで構成された SaaS または内部 Web アプリ内の安全でないコンテンツへのエンドユーザーによるアクセスを有効/無効にします。安全でないコンテンツとは、HTTPS リンクではなく HTTP リンクを使用して Web ページからリンクされているファイルのことです。デフォルト値：無効.

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。アクセス ポリシーの作成の詳細については、「アクセス ポリシーの構成」を参照してください。

2. アクションで、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クリックします。
4. 保存をクリックし、次に 完了をクリックします。

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 ポリシーの構成」を参照してください。
2. アクションで、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、次に 完了をクリックします。

> 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。
> - 現在、Secure Private Access はマイクのブロックをサポートしていません。マイクをブロックする必要がある場合は、GACS を通じて行う必要があります。

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の表示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 ポリシーの構成」を参照してください。
2. アクションで、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、次に 完了をクリックします。

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。

> 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 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。

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 ポリシーの構成」を参照してください。
2. アクションで、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。

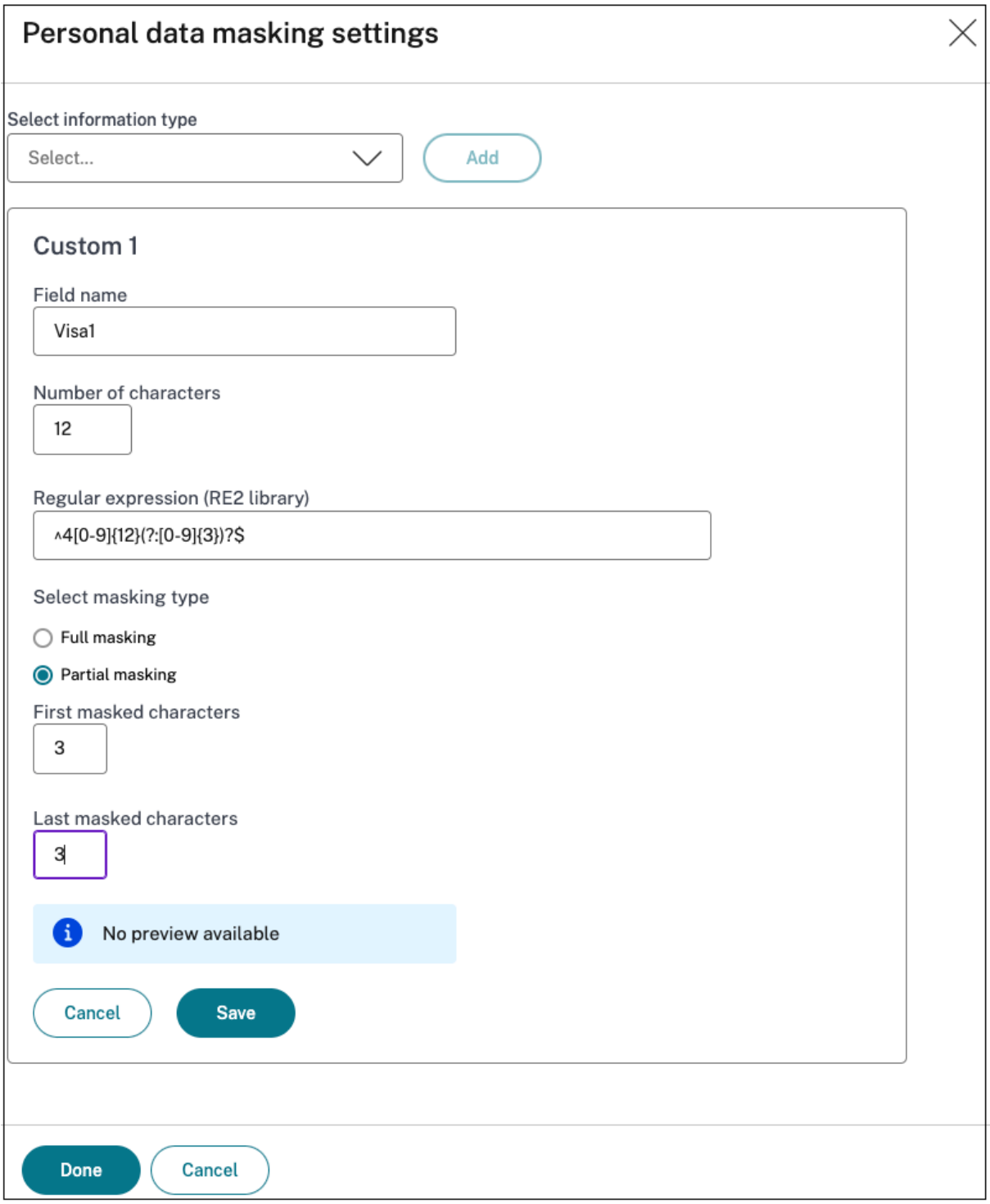
     部分マーキングを選択した場合は、文書の先頭または末尾から文字を選択する必要があります。最初のマスク文字 と 最後のマスク文字 フィールドに数字を入力する必要があります。

     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。

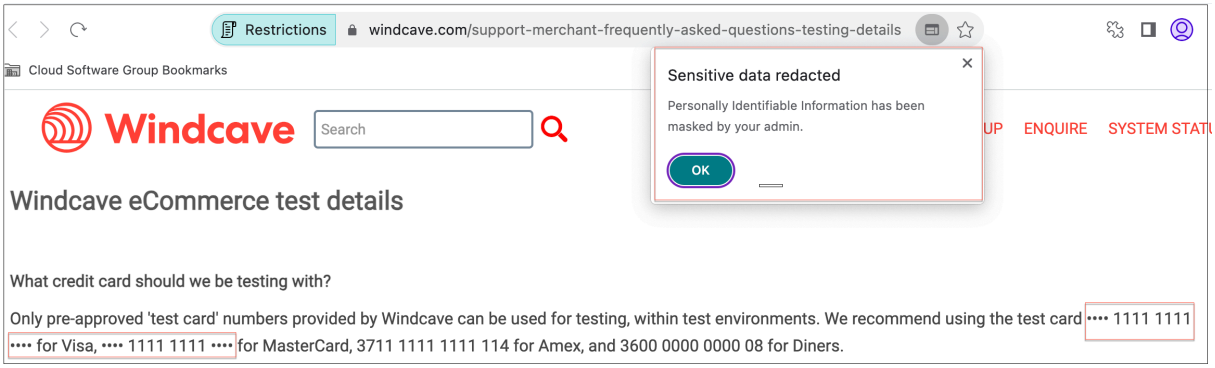
カスタム情報タイプを追加する

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。



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 ポリシーの構成」を参照してください。
2. アクションで、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、次に 完了をクリックします。

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。

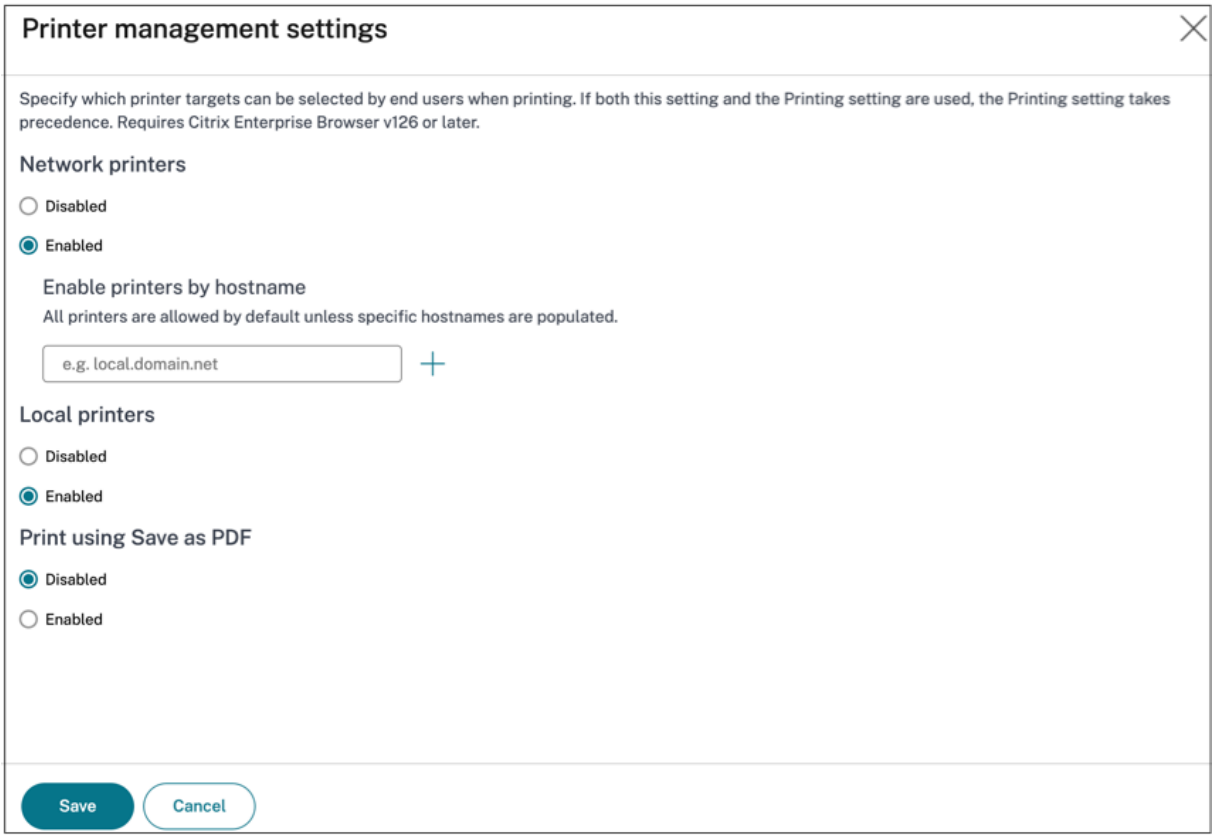
プリンター管理

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 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。

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。アクセス ポリシーの作成の詳細については、「アクセス ポリシーの構成」を参照してください。
2. アクションで、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。

     - 無効**:** ネットワーク内のすべての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。

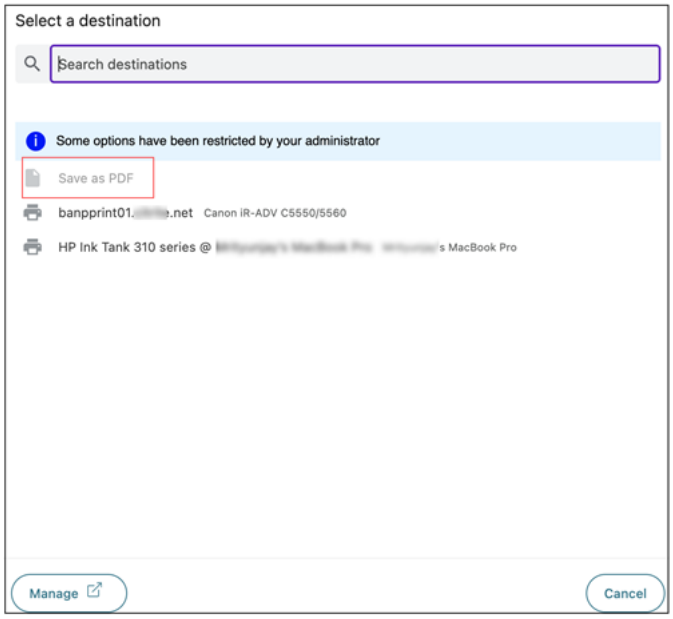
   - **Print using Save as PDF**

     - 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。

ネットワーク プリンターが無効になっている場合、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**]** を使用して印刷 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。



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 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。

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。

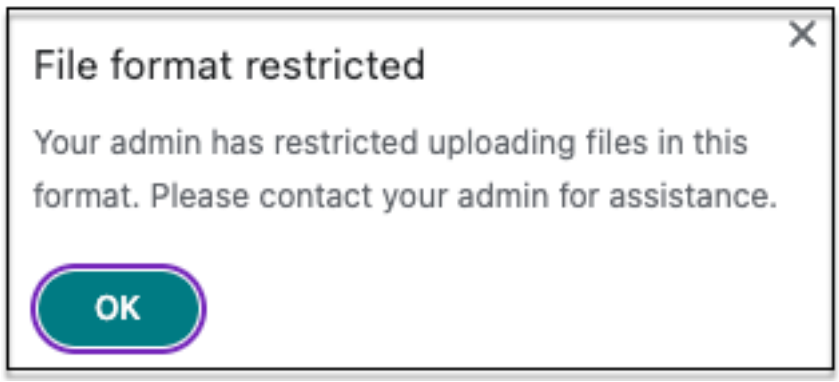
1. アクセス ポリシーを作成または編集します。詳細については、「アクセス ポリシーの作成」を参照してください。
2. アクションで、制限付きで許可を選択します。
3. ファイルタイプによるアップロード制限 をクリックし、次に 編集をクリックします。
4. ファイルタイプ別のアップロード制限設定 ページで、次のいずれかを選択します。

   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。

   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」の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 ポリシーの構成」を参照してください。
2. アクションで、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、次に 完了をクリックします。

> 注意:
>
> - セキュアプライベートアクセスポリシーで Web カメラの制限が有効になっている場合、Citrix Enterprise Browser には設定 許可が表示されます。
> - 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。
> - 現在、Secure Private Access はウェブカメラのブロックをサポートしていません。ウェブカメラをブロックする必要がある場合は、GACS を通じて行う必要があります。

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

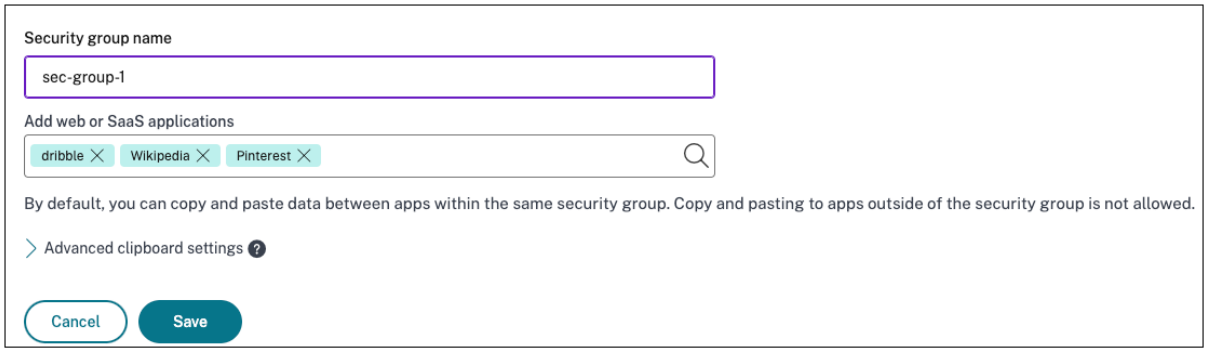
セキュリティ グループ 制限 **(**アプリケーション **>** セキュリティ グループ**)** を使用して、指定したアプリ グループのクリップボード アクセスを有効にすることができます。セキュリティ グループには、コピー アンド ペースト操作を実行できる一連のアプリが割り当てられます。セキュリティ グループ内のアプリ内でクリップボード アクセスを有効にするには、アクセス設定を選択せずに、アクション 許可 または 制限付きで許可 でアクセス ポリシーを構成する必要があります。

- 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、そのアプリには 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。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。



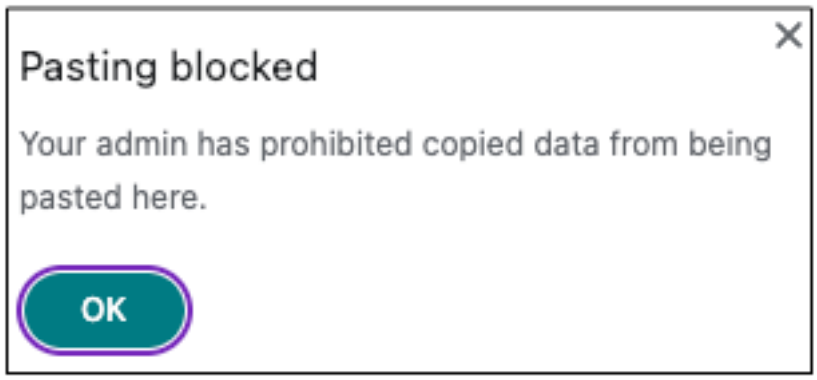
1. セキュリティ グループの名前を入力します。

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 アンド ペースト 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。

詳細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:
>
> 高度なクリップボード設定 セクションのオプションを使用して、ユーザー 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 コントロールからコンテンツのコピー/貼り付けを有効にすることができます。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。

詳細なレベルのコピー/貼り付けを有効にする

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。

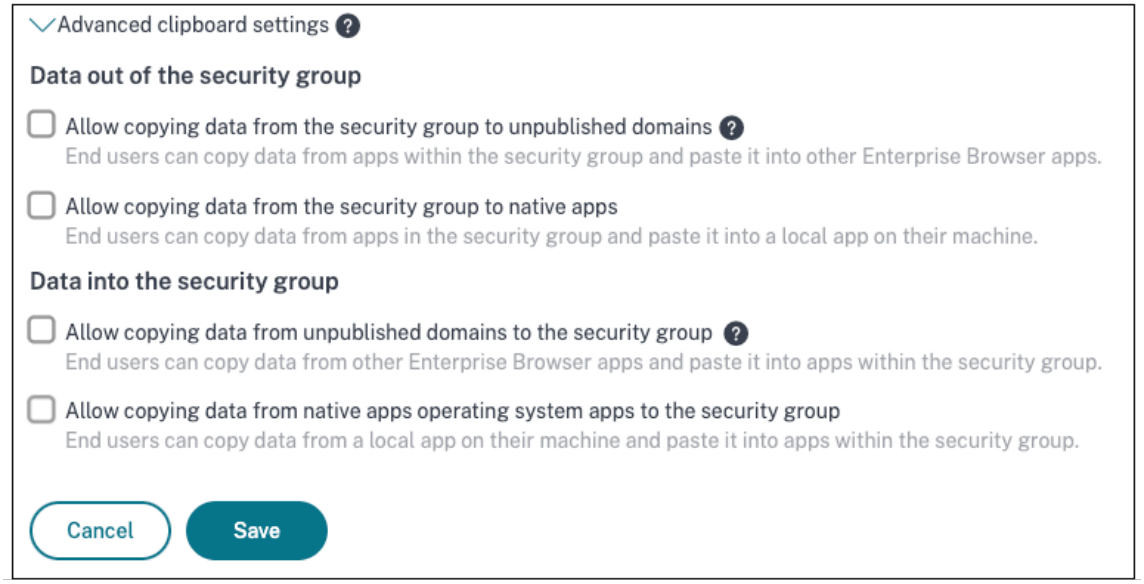
ここで、Wikipedia または Dribble からのコンテンツの Pinterest への貼り付けを制限します。そのためには、次の手順に従います。

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 ポリシーの構成」を参照してください。
2. アクションで、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 制限が有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

1. セキュリティ グループを作成します。詳細については、コピーと貼り付けの制限に関するクリップボード セキュリティ グループ 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ず、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。

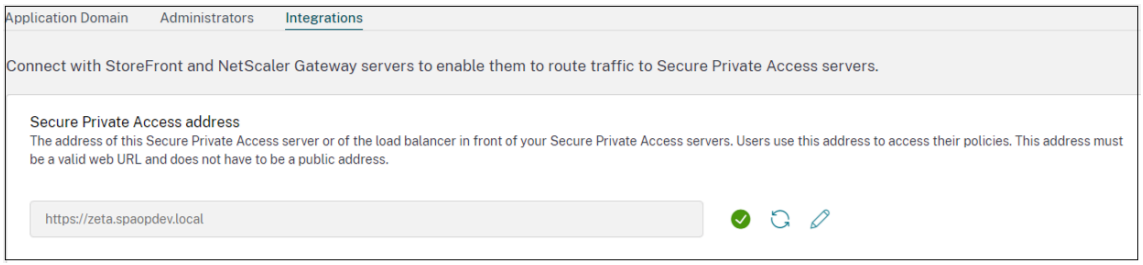
セキュアプライベートアクセスをクラスターとして展開する

October 21, 2024

Secure Private Access オンプレミス ソリューションは、高可用性、高スループット、およびスケーラビリティを実現するクラスターとして展開できます。大規模な展開（たとえば、5000 人以上のユーザー）の場合、複数の個別の Secure Private Access ノードを展開してワークロードを分散し、スケーラビリティを強化できます。

セキュアプライベートアクセスノードを作成する

- 新しい Secure Private Access サイトを作成します。詳細については、「セキュア プライベート アクセス サイトの設定」を参照してください。
- 必要な数のクラスター ノードを Secure Private Access サイトに追加します。詳細については、「既存のサイトに参加して安全なプライベート アクセスを設定する」を参照してください。
- 各 Secure Private Access ノードで、同じサーバー証明書を構成します。証明書のサブジェクト共通名またはサブジェクト代替名は、ロード バランサーの FQDN と一致する必要があります。
- Secure Private Access で最初のノードを構成するときに、ロード バランサー名を使用します。後続のノードを追加するには、[統合] タブでデータベース アドレスを指定し、データベース スクリプトを手動で実行します。スクリプトを使用してデータベースをアップグレードする方法の詳細については、「スクリプトを使用してデータベースをアップグレードする」を参照してください。



ロードバランサの構成

Secure Private Access クラスターのセットアップには、特定の負荷分散構成要件はありません。NetScaler をロードバランサーとして使用している場合は、次の点に注意してください。

- StoreFront へのアクセスに使用される FQDN は、サブジェクト別名 (SAN) として DNS フィールドに含まれます。ロード バランサーを使用している場合は、個々のサーバーの FQDN とロード バランサーの FQDN の両方を含めます。これは SSL 証明書に適用されます。セキュア プライベート アクセスの場合、ロード バランサーを構成するだけで十分です。詳細については、「NetScaler による負荷分散」を参照してください。セキュア プライベート アクセスを構成する前に、StoreFront ストアを構成する必要があります。ロード バラン

サーを使用する場合は、ロード バランサー名を使用してベース URL を構成し、安全な通信のために HTTPS を使用します。詳細については、「HTTPS による StoreFront のセキュリティ保護」を参照してください。

- セキュア プライベート アクセス サービスは HTTPS として実行することをお勧めしますが、これは必須要件ではありません。セキュア プライベート アクセス サービスも HTTP として展開できます。
- SSL オフロードまたは SSL ブリッジがサポートされているため、任意のロード バランサ構成を使用できます。SSL ブリッジを使用する場合は、各 Secure Private Access ノードで同じサーバー証明書を構成するようにしてください。また、証明書のサブジェクト共通名またはサブジェクト代替名 (SAN) は、ロード バランサーの FQDN と一致する必要があります。また、ロード バランサ サービスで SAN を構成する必要があります。
- 正しい SSL 証明書が IIS サーバーと NetScaler にバインドされています。
- 安全な暗号が使用されます。
- セキュア プライベート アクセス サービス (管理とランタイムの両方) はステートレスであるため、永続性は必要ありません。
- ロード バランサー (NetScaler など) には、バックエンド サーバー用のデフォルトの組み込みモニター (プローブ) があります。Secure Private Access オンプレミス サーバーにカスタム HTTP ベースのモニター (プローブ) を構成する必要がある場合は、次のエンドポイントを使用できます。

  `/secureAccess/health`

  予想される応答:

```
    Http status code: 200 OK

    Payload:

    {
"status":"OK","details":{
"duration":"00:00:00.0084206","status":"OK" }
 }
```

  NetScaler ロードバランサーの構成の詳細については、「基本的なロードバランシングのセットアップ」を参照してください。

セキュアプライベートアクセスのモニターを作成する

次の CLI コマンドを使用して、Secure Private Access のモニターを作成します。

```
add lb monitor SPAHealth HTTP -respCode 200 -httpRequest "GET /
secureAccess/health"-secure YES
```

モニターを作成したら、証明書をモニターにバインドします。

NetScaler UI を使用してモニターを作成する方法の詳細については、「モニターの作成」を参照してください。

Secure Private Access のアンインストール

August 26, 2024

Secure Private Access は、**[**コントロールパネル**] > [**プログラム**] > [**プログラムと機能] からアンインストールできます。

1.「**Citrix Virtual Apps and Desktops 7 2405 –Secure Private Access**」を選択します。
2.［アンインストール］をクリックします。
3. 画面の指示に従い、アンインストールを完了します。

> 注:
>
> Secure Private Access のインストール後のセットアップが完了したら、Secure Private Access をアンインストールする前に、管理コンソールから StoreFrontScripts.zip ファイルをダウンロードして、StoreFront ストア構成から Secure Private Access プラグインを削除してください。

StoreFrontScript の zip ファイルをダウンロードするには、次の手順に従ってください:

1. Secure Private Access 管理コンソールにログインします。
2. [設定] をクリックし、[統合] タブをクリックします。
3. StoreFront ストア URL セクションの「スクリプトのダウンロード」をクリックします。

StoreFront ストア構成から **Secure Private Access** プラグインを削除します

Secure Private Access をアンインストールしたら、StoreFront ストア構成から Secure Private Access プラグインを削除する必要があります。

1. StoreFront マシンにログインします。
2. StoreFrontScripts.zip ファイルをダウンロードします。
3. StoreFrontScripts.zip をフォルダに解凍します。
4. 管理者権限で PowerShell ウィンドウを開きます。
5. 次のコマンドを実行します:

```
cd <unzipped folder>
.\RemoveStorefrontConfiguration.ps1
```

アップグレード

August 26, 2024

最初に新しいマシンやサイトをセットアップしなくても、Secure Private Access 展開メントを新しいバージョンにアップグレードできます。アップグレードする前に、スナップショットを作成するか、設定を保存することをお勧めします。アップグレードを開始するには、新しいバージョンからインストーラーを実行して、以前にインストールした Secure Private Access プラグインをアップグレードします。

アップグレードの順序

アップグレードの順序は次のとおりです:

1. Secure Private Access は、最初に Secure Private Access をインストールした方法に応じて、Delivery Controller またはインストーラー UI の専用 Secure Private Access タイルを使用してアップグレードできます。
    - Delivery Controller 経由で Secure Private Access をインストールした場合、Secure Private Access コンポーネントだけをアップグレードすることはできません。代わりに、すべてのコンポーネントをアップグレードする必要があります。詳しくは、「環境のアップグレード」を参照してください。
    - 専用の Secure Private Access タイルを使用して Secure Private Access をインストールした場合は、個別にアップグレードできます。詳細については、「Secure Private Access インストーラーのアップグレード」を参照してください。

    > 注:
    >
    > POC 環境では、Delivery Controller を使用して Secure Private Access をインストールすることをお勧めしますが、実稼働環境では、新しい機能を導入できるように専用インストーラーを使用することをお勧めします。

2. データベーススクリプトを実行します。詳細については、「スクリプトを使用してデータベースをアップグレードする」を参照してください。
3. StoreFront 構成を再実行してください。StoreFront スクリプトを ［設定］>［構成］からダウンロードし、対応する StoreFront マシン上でスクリプトを実行します。詳細については、「統合設定の変更」を参照してください。

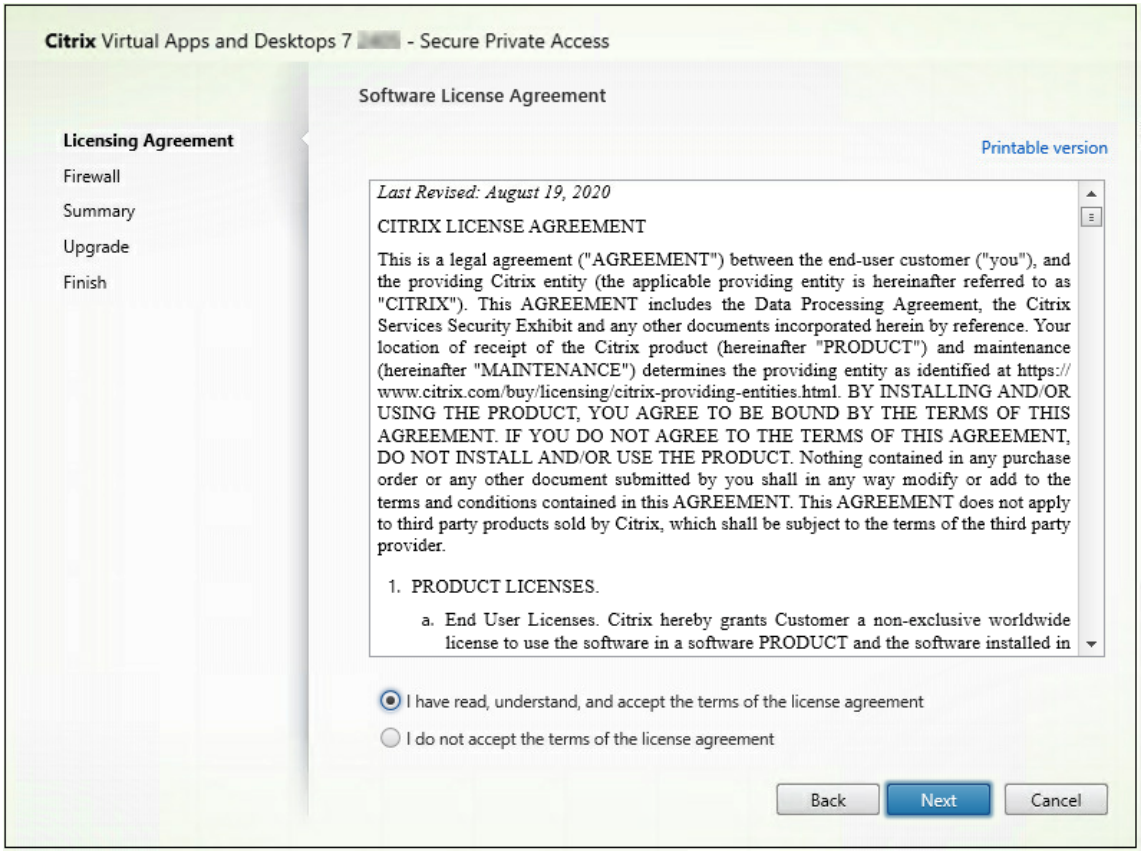
    > 注:
    >
    > スクリプトを実行しない場合、エンドポイントはトリガーされません。

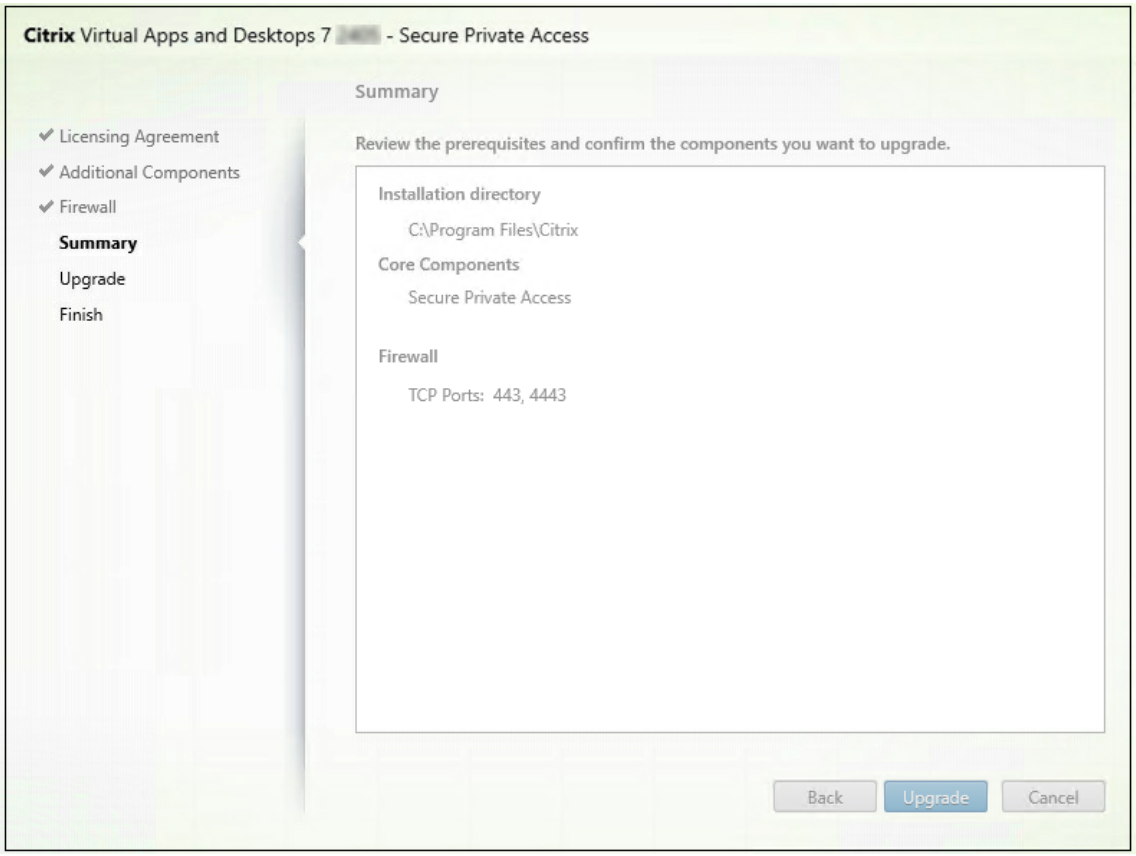
4. (オプション) NetScaler Gateway クリプトを実行します。詳しくは、「NetScaler Gateway」を参照してください。

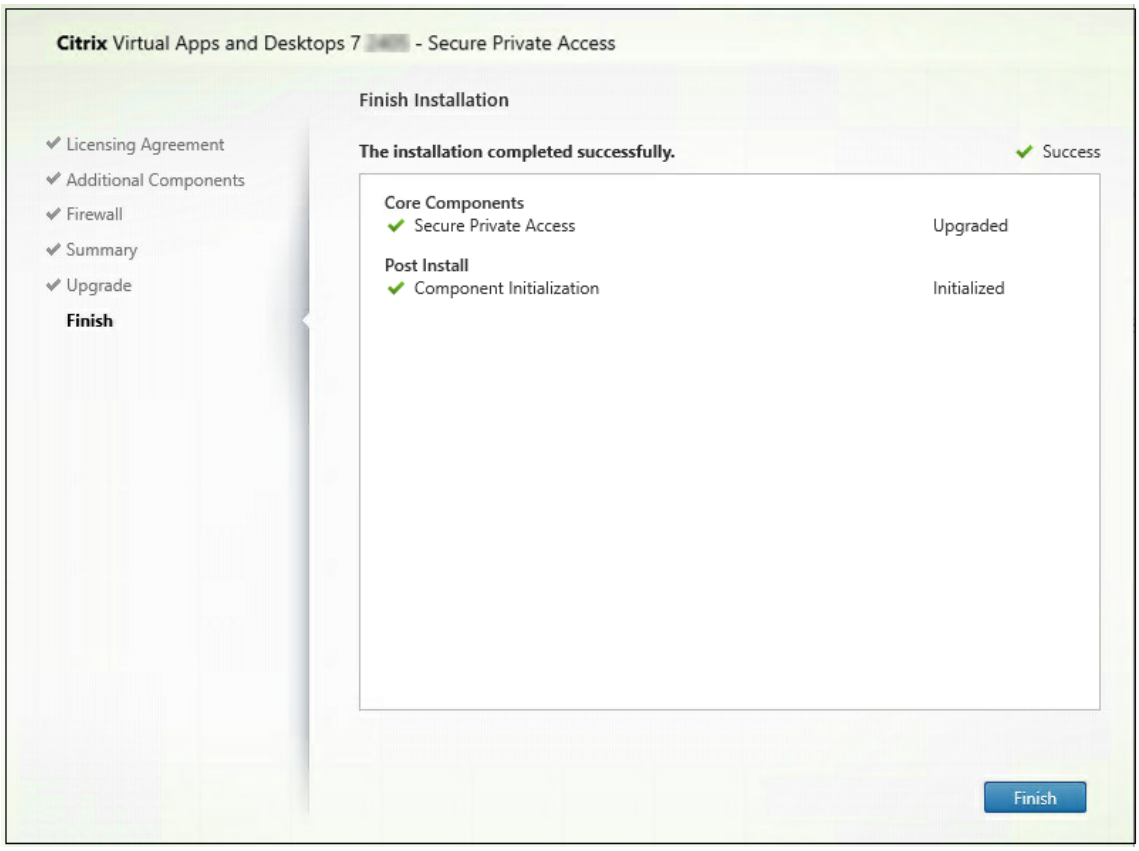
Secure Private Access インストーラーのアップグレード

August 26, 2024

1. Citrix Secure Private Access 2405 インストーラーをhttps://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/からダウンロードします。
2. .exe をドメインに参加しているマシン上で管理者として実行します。
3. 画面の指示に従ってインストールを完了します。







> 重要:
>
> インストーラーをリリース 2405 にアップグレードしたら、StoreFront スクリプトを再実行して、新しいエンドポイントの詳細を使用できるようにする必要があります。

次の手順

- Secure Private Access のセットアップ
- NetScaler Gateway Gateway の構成
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

スクリプトを使用してデータベースをアップグレードする

August 26, 2024

管理者設定ツールを使用して、Secure Private Access プラグインのデータベースアップグレードスクリプトをダウンロードできます。

1. PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
2. ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)。
3. 次のコマンドを実行します:

   ```
   .\AdminConfigTool.exe /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder>
   ```

管理

August 26, 2024

Secure Private Access をインストールしたら、設定ページから設定を変更できます。アプリケーションドメイン、管理者のルーティングを管理し、統合設定を変更できます。

設定を変更するには、Secure Private Access 管理者アカウントで Secure Private Access 管理コンソールにサインインする必要があります。

設定を更新または変更する方法の詳細については、以下のトピックを参照してください:

インストール後に設定を管理

August 26, 2024

アプリケーションドメインのルーティングを管理

Secure Private Access の設定に追加されたアプリケーションドメインのリストを表示できます。アプリケーションドメインテーブルには、すべての関連ドメインと、アプリケーショントラフィックのルーティング方法（外部または内部）が一覧表示されます。

1. [設定] **>** [アプリケーションドメイン] をクリックします。
2. 必要に応じて、編集アイコンをクリックしてルーティングタイプを変更できます。

管理者の管理

[設定] **>** [管理者] ページから、管理者のリストを表示したり、管理者を追加したりできます。Secure Private Access を初めてインストールした管理者には、完全な権限が付与されます。その後、この管理者は他の管理者をセットアップに追加できます。

管理者グループを追加して、そのグループのすべての管理者がアクセスできるようにすることもできます。

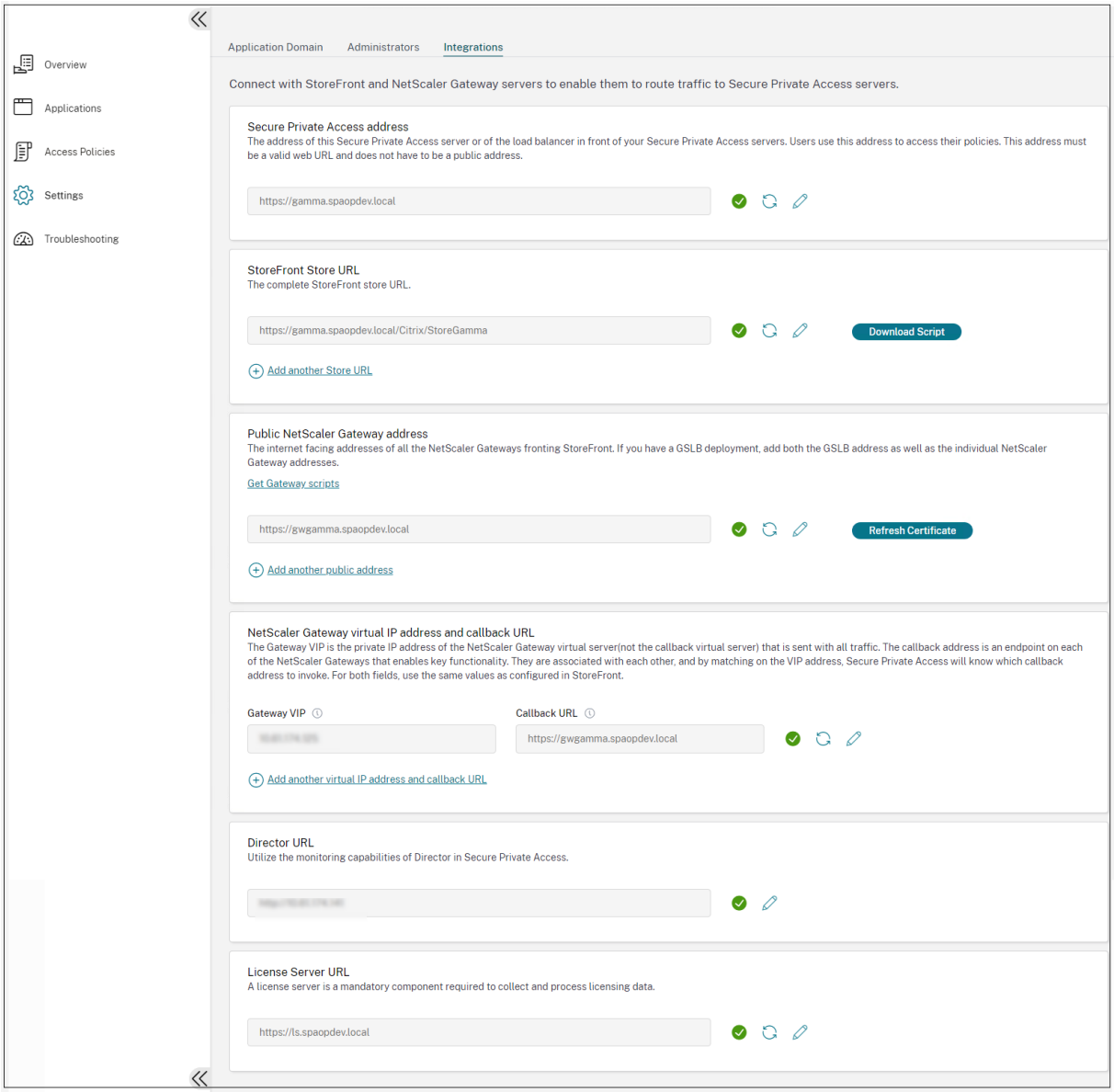
1. 管理者ページで、「追加」をクリックします。
2. 「ドメイン」で、この管理者を追加する必要があるドメインを選択します。
3. 「ユーザーまたはユーザー・グループ」で、このユーザーが属するユーザーまたはグループを選択します。
4. 「管理者タイプ」で、このユーザーに割り当てる必要がある権限タイプを選択します。

統合設定の変更

Secure Private Access を設定したら、［統合］タブから StoreFront と NetScaler Gateway のエントリを変更または更新できます。

1. [設定] **>** [統合] をクリックします。
2. 変更する設定の横にある編集アイコンをクリックし、エントリを更新します。
3. 更新アイコンをクリックして、設定が有効であることを確認します。

> 注:
>
> Secure Private Access が StoreFront とは異なるマシンにインストールされている場合は、StoreFront スクリプトをダウンロードして StoreFront で実行してください。



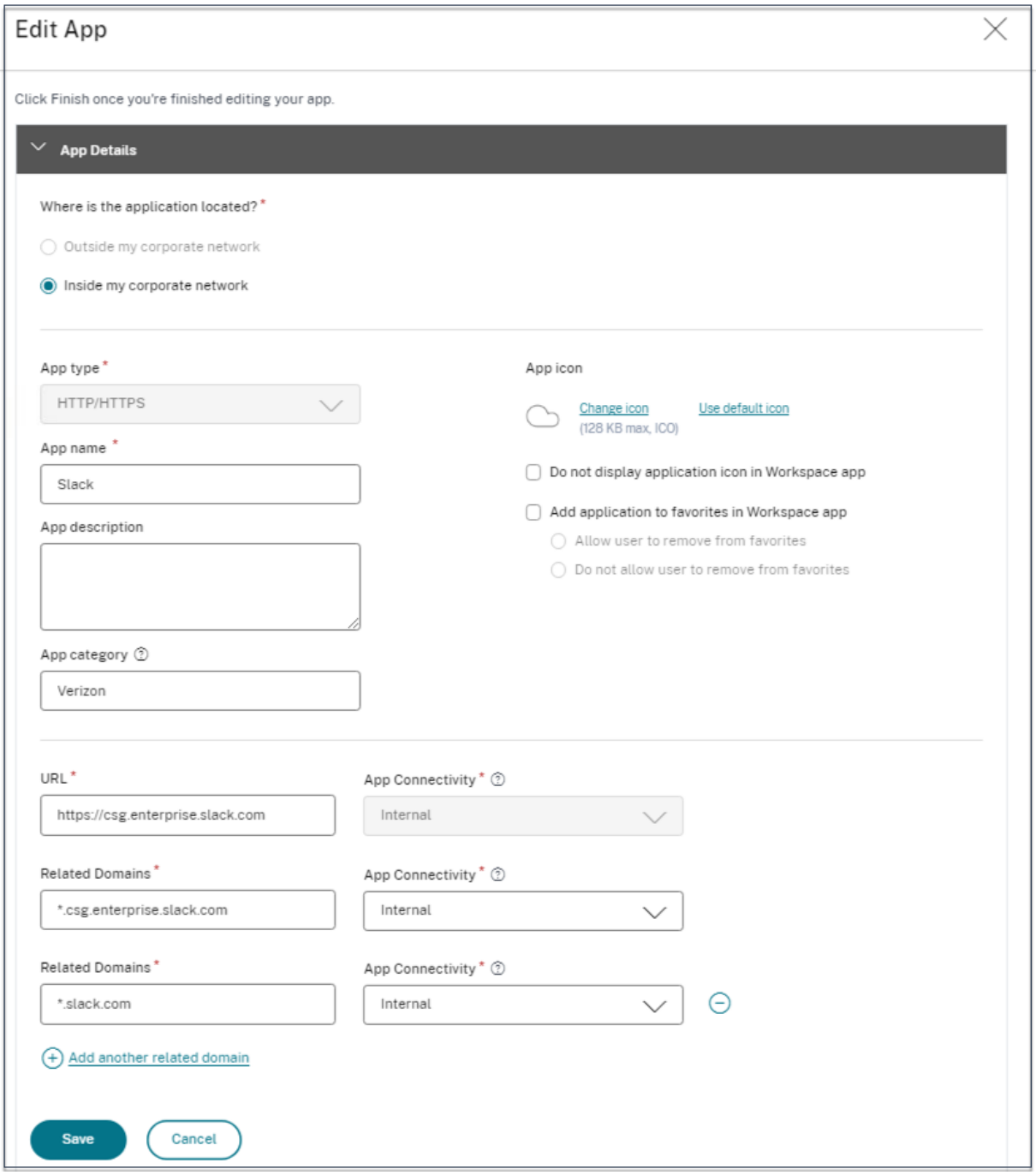
アプリケーションとポリシーの管理

August 26, 2024

アプリケーションとアクセスポリシーを設定したら、必要に応じて編集できます。

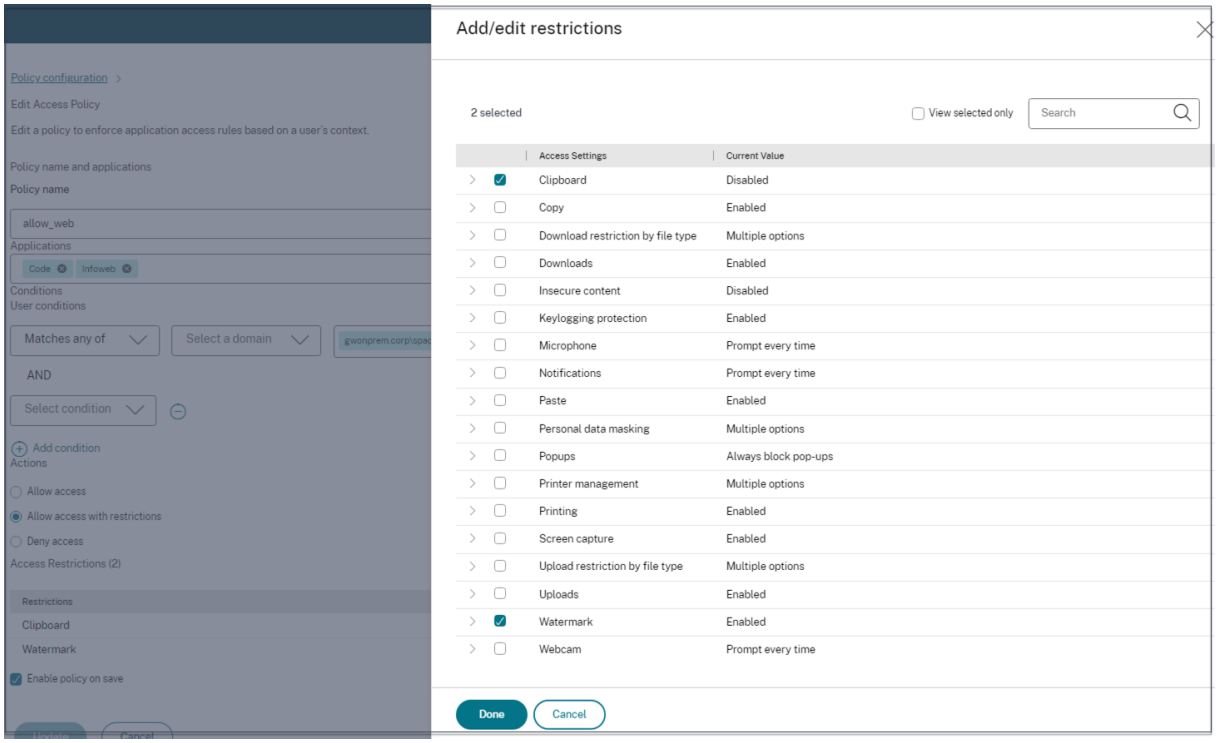
アプリケーションを編集する

1. Secure Private Access 管理コンソールで、「アプリケーション」をクリックします。
2. 変更するアプリケーションの省略記号ボタンをクリックし、**[**アプリケーションの編集**]** をクリックします。
3. アプリの詳細を編集します。
4. [**Save**] をクリックします。



アクセスポリシーを編集する

1. Secure Private Access 管理コンソールで、「アクセスポリシー」をクリックします。
2. 変更するポリシーの省略記号ボタンをクリックし、「アクセスポリシーの編集」をクリックします。
3. ポリシーの詳細を編集します。
4. [**Update**] をクリックします。



認可されていないウェブサイト

August 26, 2024

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

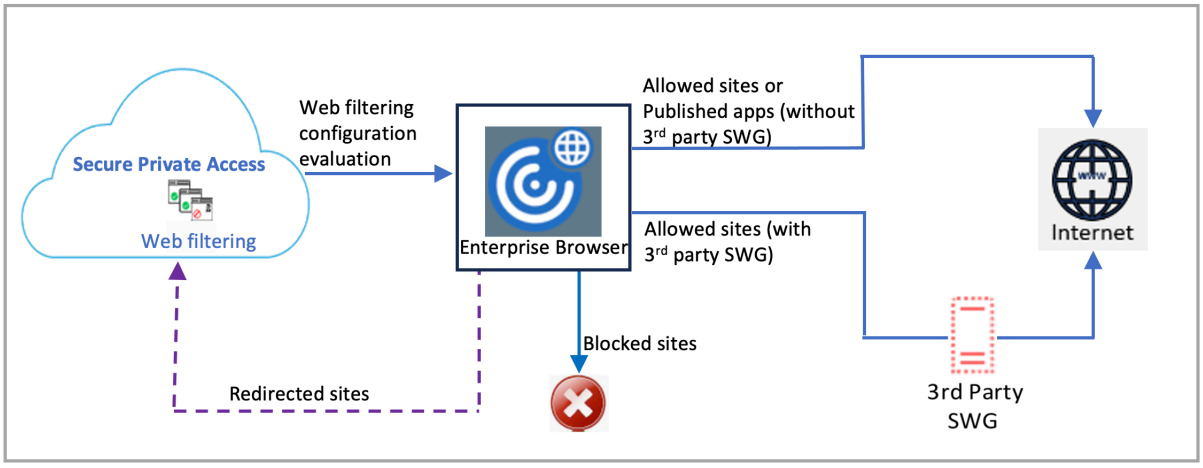
アプリが設定されていない他のすべてのインターネット URL または SaaS アプリケーションでは、管理者は管理コンソールから［設定］**>**［許可されていない **Web** サイト］タブを使用して、Citrix Enterprise Browser によるアクセスを許可または拒否できます。

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

認可されていない **Web** サイトの仕組み

1. URL 分析チェックは、その URL が Citrix サービス URL であるかどうかを判断するために行われます。
2. その後、URL がエンタープライズ Web または SaaS アプリ URL であるかどうかが確認されます。
3. 次に、その URL がブロックされた URL として識別されるかどうか、または URL へのアクセスを許可できるかどうかが確認されます。

次の図は、エンドユーザーのトラフィックフローを示しています。



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

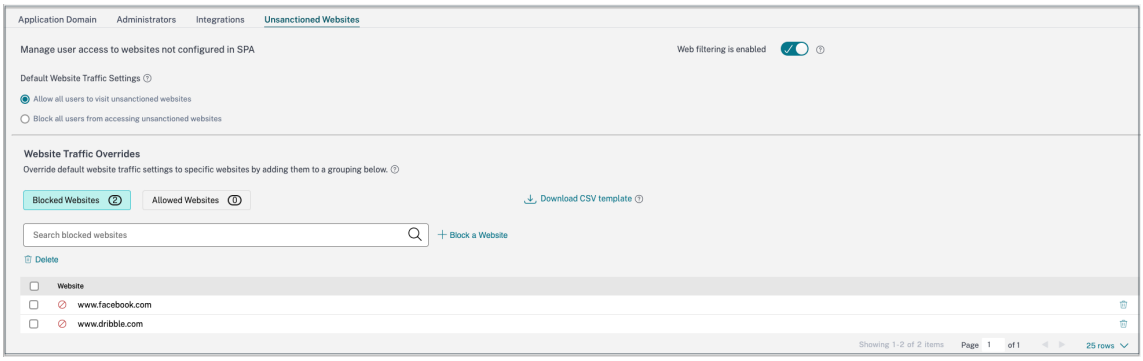
1. 要求はグローバル許可リストに一致していますか?
   a) 一致した場合、ユーザーは要求された Web サイトにアクセスできます。
   b) 一致しない場合、Web サイトリストがチェックされます。
2. 要求は顧客が構成した Web サイトリストに一致していますか?
   a) 一致する場合は、次の順序でアクションが決定されます。
      i. ブロック
      ii. 許可
   b) 一致しない場合、デフォルトのアクション（許可）が適用されます。デフォルトのアクションは変更できません。

認可されていない **Web** サイトのルールを設定

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

   注:

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

   特定の URL を、ブロックされた Web サイトまたは許可された Web サイトに追加して、その設定を変更することもできます。

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

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

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

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

      URL が許可された Web サイトのリストに追加されます。

エンドユーザーフロー

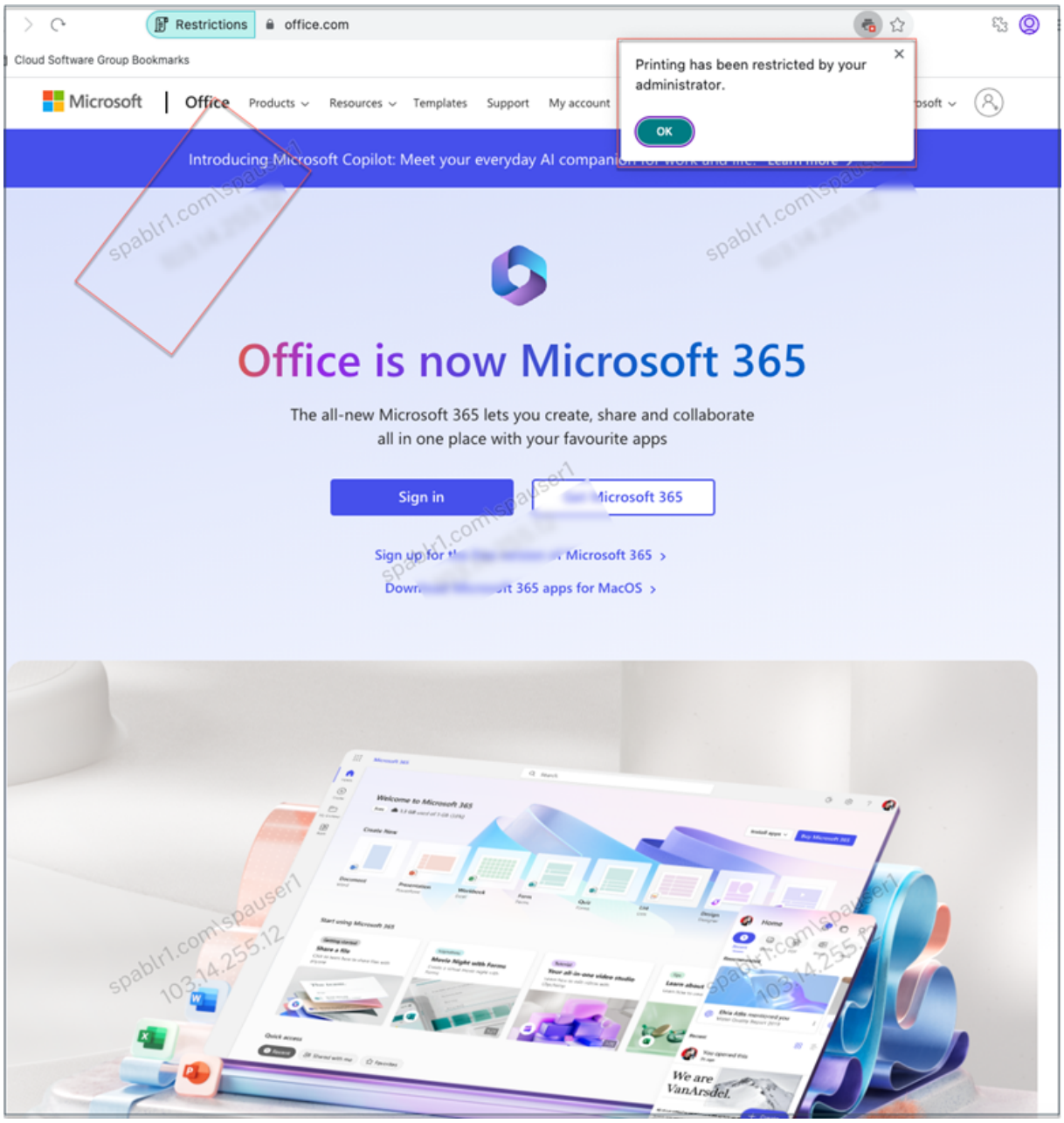
August 26, 2024

管理者がエンドユーザー用のウォーターマークと印刷制限を使用して Office365 アプリを構成したと仮定します。これで、エンドユーザーが Office 365 アプリにアクセスするときに、ウォーターマークと印刷の制限をアプリに適用する必要があります。

エンドユーザーは Office 365 アプリにアクセスするには、次の手順を実行する必要があります:

1. Citrix Workspace アプリから StoreFront ストアにアクセスします。
2. ストアにログオンします。
3. [アプリ] タブをクリックし、次に **Office365** アプリケーションをクリックします。

   これで、エンドユーザーは、Office365 アプリケーションが起動され、ウォーターマークが含まれていることに気付く必要があります。また、エンドユーザーが Office 365 アプリケーションからデータを印刷しようとした場合、印刷制限メッセージをユーザーに表示する必要があります。



> 注:
>
> 管理者は、仮想デスクトップとアプリケーションにアクセスするために必要なアカウント情報をユーザーに提供する必要があります。詳しくは、「Citrix Workspace アプリへのストア URL の追加」を参照してください。

監視とトラブルシューティング

August 26, 2024

Secure Private Access のトラブルシューティングダッシュボードには、アプリケーションの起動、アプリケーションの列挙、およびそれらのステータスに関連するログが表示されます。詳細については、「ダッシュボードの概要」を参照してください。

トラブルシューティング

Secure Private Access の設定中または設定後に、以下に関連する問題が発生する可能性があります:

- 証明書のエラー
- データベース作成エラー
- StoreFront 障害
- パブリックゲートウェイ/コールバックゲートウェイの障害
- Secure Private Access サーバーにアクセスできない

これらの問題の修正について詳しくは、「基本的なトラブルシューティング」を参照してください。

Director のセッション関連コード

Director を Secure Private Access と統合すると、Secure Private Access セットアップのすべてのコンポーネントの問題が Director に取り込まれるため、効果的なパフォーマンスの監視とトラブルシューティングが可能になります。障害または例外の問題は、ログを調べて解決することをお勧めします。それでも問題が解決しない場合は、サポートに連絡してください。

参照ドキュメント

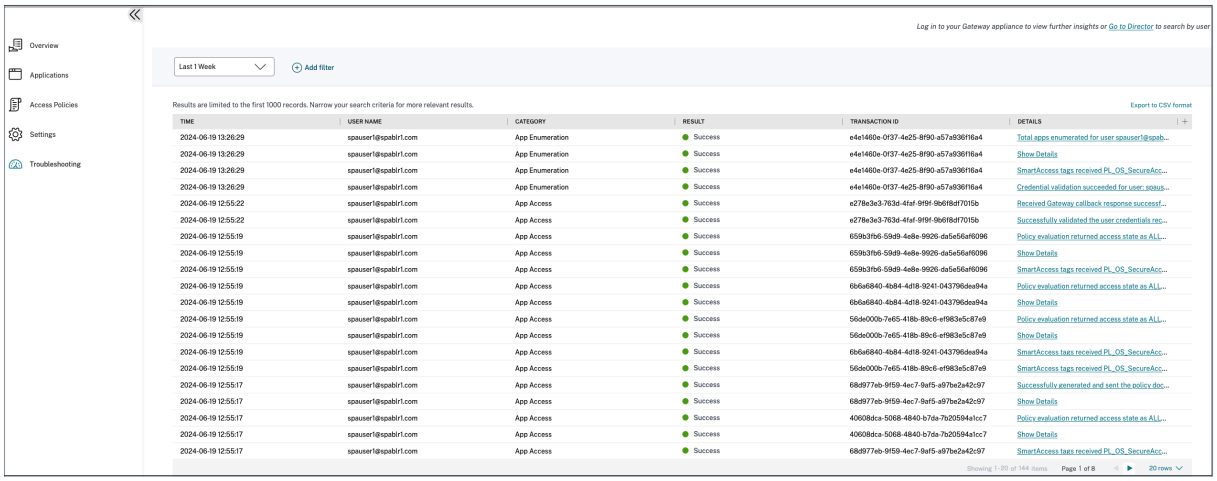
- Secure Private Access で Director を構成する
- Director で Secure Private Access セッションを表示する
- Director の Secure Private Access セッションコードのリスト。
- Director。

ダッシュボードの概要

August 26, 2024

トラブルシューティングダッシュボードには、アプリケーションの起動、アプリケーションの列挙、およびステータスに関連するログが表示されます。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。[フィルターの追加] オプションを使用すると、アプリカテゴリ、ユーザー名、トランザクション ID などのさまざまな条件に基づいて検索を絞り込むことができます。たとえば、検索フィールドでトランザクション ID = (ある値と等しい) 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。

ダッシュボードに表示したい情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログは CSV 形式にエクスポートできます。



[フィルタを追加] オプションを使用すると、次の検索演算子を使用して検索を絞り込むことができます:

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

たとえば、検索フィールドに「イベントタイプ **> = (**ある値と等しい**) >** 列挙」という文字列を使用すると、「列挙」というイベントタイプを検索できます。

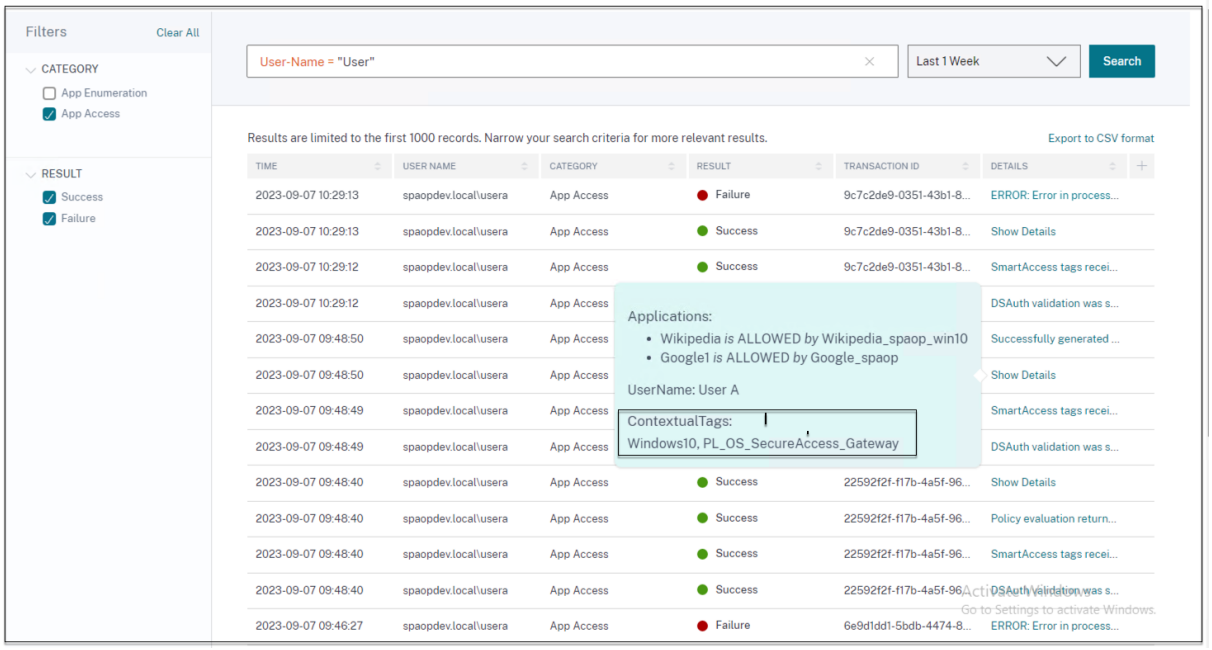
同様に、「operator」という用語を部分的に含むユーザーを検索するには、**User-Name > ~ (**何らかの値を含む**) > operator** という文字列を使用します。この検索では、「operator」という用語を含むすべてのユーザー名が一覧表示されます。たとえば、「ローカルオペレータ」、「管理者オペレータ」などです。

トランザクション ID を使用して、1 つのイベントに関連するすべてのログを検索できます。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。1 つのアプリアクセスリクエストで、認証、アプリ列挙、アプリアクセス自体など、複数のログを生成できます。これらのイベントはすべて独自のログを生成し

ます。トランザクション ID は、これらすべてのログを関連付けるために使用されます。トランザクション ID を使用してログをフィルタリングすると、特定のアプリアクセスリクエストに関連するすべてのログを検索できます。

ログからコンテキストタグを表示

[**Details]** 列の **[ShowDetails**] リンクには、特定のアクセスポリシーに関連付けられているアプリケーションのリストと、そのポリシーに関連付けられているコンテキストタグが表示されます。



基本的なトラブルシューティング

August 26, 2024

このトピックでは、Secure Private Access の設定中または設定後に発生する可能性のあるエラーの一部を示します。

証明書のエラー

データベース作成エラー

StoreFront 障害

パブリックゲートウェイ/コールバックゲートウェイの障害

Secure Private Access サーバーにアクセスできない

証明書のエラー

エラーメッセージ:1 つ以上のゲートウェイサーバーから証明書を自動的に取得できません。

このエラーメッセージは、NetScaler Gateway のパブリックアドレスを追加しようとして、証明書の取得に問題がある場合に表示されます。この問題は、Secure Private Access をセットアップするとき、またはセットアップが完了した後に設定を更新するときに発生する可能性があります。

回避策: Citrix Virtual Apps and Desktops の場合と同じ方法でゲートウェイ証明書を更新します。

データベース作成エラー

- エラーメッセージ: データベースを作成できませんでした

  解決策: 自動の場合-SQL Server 上のデータベース内にテーブルを作成するには、マシンに READ、WRITE、UPDATE 権限が必要です。

- エラーメッセージ: データベースを作成できませんでした: データベースは既に存在します。

  このエラーメッセージは、次のシナリオのいずれかで表示されることがあります。

  - データベースの構成時に「自動構成」オプションを選択した場合。
  - 管理者がデータベースを作成する場合、そのデータベースは空のデータベースでなければなりません。このエラーメッセージは、データベースが空でないデータベースである場合に表示されることがあります。

    解決策: 空のデータベースを作成する必要があります。
  - Secure Private Access をアンインストールし、同じサイト名でセットアップを再試行します。この場合、以前のインストールのデータベースは削除されなかったでしょう。

    解決策: データベースを手動で削除する必要があります。
  - スクリプトを使用してデータベースを手動で設定し ([データベースの構成] ページで [手動構成] を選択)、次に [自動構成] オプションに変更しますが、サイト名は同じです。この場合、スクリプトの実行中に同じ名前のデータベースがすでに作成されています。

    解決策: サイトの名前を変更してから、スクリプトを再実行する必要があります。
  - マシンには、SQL Server 上のデータベース内にテーブルを作成するための READ、WRITE、UPDATE 権限がありません。

    解決策: マシン上で適切な権限を有効にします。詳細については、「データベースの設定に必要な権限」を参照してください。

- エラーメッセージ: データベースを作成できませんでした: 接続に失敗しました

  解決策:

- マシンからのデータベースネットワーク接続を確認してください。SQL Server ポートがファイアウォールで開いていることを確認します。
- リモート SQL Server を使用している場合は、SQL Server に Secure Private Access のマシン ID である Domain\ hostname$ を使用して作成されたログインがあるかどうかを確認してください。
- リモート SQL Server を使用している場合は、マシン ID に正しいロール、つまりシステム管理者ロールが割り当てられていることを確認してください。
- ローカル SQL Server (インストーラからではない) を使用している場合は、NT AUTHORITY\ SYSTEM ユーザにログインを作成する必要があるかどうかを確認してください。

StoreFront 障害

- エラーメッセージ: 次の StoreFront エントリを作成できませんでした: <Store URL>

  表示されていない場合は、［設定］タブから StoreFront のエントリを更新します。ウィザードを使用して Secure Private Access を設定したら、［設定］タブから StoreFront のエントリを編集できます。このエラーが発生した StoreFront ストアの URL を書き留めてください。

  解決策:

  1. [設定] をクリックし、[統合] タブをクリックします。
  2. **StoreFront** ストア **URL** に、StoreFront エントリが表示されていない場合は、そのエントリを追加します。

- エラーメッセージ: 次の StoreFront エントリを構成できませんでした: <Store URL>

  解決策:

  1. PowerShell の実行ポリシーによる制限が設定されている可能性があります。詳細については、PowerShell スクリプトコマンド `Get-ExecutionPolicy`を実行してください。
  2. 制限されている場合は、これを回避して StoreFront 構成スクリプトを手動で実行する必要があります。
  3. [設定] をクリックし、[統合] タブをクリックします。
  4.「**StoreFront** ストア **URL**」で、エラーが発生した StoreFront URL のエントリを特定します。
  5. このストア URL の横にある［スクリプトのダウンロード］ボタンをクリックし、対応する StoreFront がインストールされているマシン上で管理者権限でこの PowerShell スクリプトを実行します。このスクリプトはすべての StoreFront マシンで実行する必要があります。

  > 注:
  >
  > アンインストール後にインストールを再試行する場合は、StoreFront 構成（StoreFront > ストア **> Delivery Controller-**Secure Private Access）に「Secure Private Access」という名前のエントリがないことを確認してください。Secure Private Access が存在する場合は、このエントリを削除してください。設定 > 統合ページからスクリプトを手動でダウンロードして実行します。

- エラーメッセージ：次の StoreFront 構成はローカルではありません：<Store URL>

  ウィザードを使用して Secure Private Access を設定したら、[設定] タブからゲートウェイエントリを編集できます。このエラーが発生した StoreFront ストアの URL を書き留めてください。

  解決策：

  この問題は、StoreFront が Secure Private Access と同じマシンにインストールされていない場合に発生します。StoreFront をインストールしたマシンで StoreFront 構成を手動で実行する必要があります。

  1. [設定] をクリックし、[統合] タブをクリックします。
  2.「**StoreFront** ストア **URL**」で、エラーが発生した StoreFront URL のエントリを特定します。
  3. このストア URL の横にある［スクリプトのダウンロード］ボタンをクリックし、対応する StoreFront がインストールされているマシン上で管理者権限でこの PowerShell スクリプトを実行します。このスクリプトはすべての StoreFront マシンで実行する必要があります。

  > 注**:**
  >
  > StoreFront PowerShell スクリプトを実行するには、管理者権限で Windows x64 互換の PowerShell ウィンドウを開き、ConfigureStoreFront.ps1 を実行します。StoreFront スクリプトは Windows PowerShell (x86) と互換性がありません。

- エラーメッセージ：PowerShell を使用して StoreFront スクリプトを実行しているときに「Get-STFStoreService: タイプ'Citrix.DeliveryServices.framework.feature.exceptions.registryKeyNotFoundExceptio の例外が発生しました。」。

  このエラーは、StoreFront スクリプトを x86 互換の PowerShell ウィンドウで実行した場合に発生します。

  解決策：

  StoreFront PowerShell スクリプトを実行するには、管理者権限で Windows x64 互換の PowerShell ウィンドウを開いてから`ConfigureStorefront.ps1`を実行します。

パブリックゲートウェイ/コールバックゲートウェイの障害

エラーメッセージ:: のゲートウェイエントリを作成できませんでした。<Gateway URL> または、次のコールバックゲートウェイエントリを作成できませんでした: <Callback Gateway URL>

解決策：

障害が発生したパブリックゲートウェイまたはコールバックゲートウェイの URL を書き留めておきます。ウィザードを使用して Secure Private Access を設定したら、[設定] タブからゲートウェイエントリを編集できます。

1. [設定] をクリックし、[統合] タブをクリックします。
2. パブリックゲートウェイアドレスまたはコールバックゲートウェイアドレスと、障害が発生した仮想 IP アドレスを更新します。

Secure Private Access サーバーにアクセスできない

エラーメッセージ:IIS プールを更新できませんでした。IIS プールを再起動できませんでした

解決策:

インターネットインフォメーションサービス (IIS) の [アプリケーションプール] に移動し、次のアプリケーションプールが起動して実行されていることを確認します。

- Secure Private Access ランタイム・プール
- Secure Private Access 管理者プール

また、デフォルトの IIS サイト`"Default Web Site"`が稼働していることも確認してください。

データベース接続チェックの失敗

エラーメッセージ**:** 接続チェックが失敗しました

データベース接続チェックは、複数の理由で失敗する可能性があります:

- ファイアウォールのため、Secure Private Access プラグインのホストマシンからデータベースサーバーにアクセスできません。

  解決策**:** データベースポート (デフォルトポート 1433) がファイアウォールで開いているかどうかを確認します。

- Secure Private Access プラグインホストマシンには、データベースに接続する権限がありません。

  解決策**:**Secure Private Access の SQL データベース権限を参照してください。

ゲートウェイ接続チェックが失敗しました。公開証明書を取得できません

エラーメッセージ**:** インストール後の構成が次のエラーで失敗します。「ゲートウェイ接続チェックに失敗しました。公開証明書を取得できません…」

解決策:

- 構成ツールを使用して、ゲートウェイのパブリック証明書を Secure Private Access データベースに手動でアップロードします。
- PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
- ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)

- 次のコマンドを実行します:

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

アプリケーション列挙失敗

StoreFront の URL または NetScaler Gateway の URL の末尾にスラッシュ（/）が含まれていると、アプリケーションの列挙が中断されます。

解決策:

StoreFront ストア URL または NetScaler Gateway URL の末尾のスラッシュを削除します。詳しくは、「セットアップ後の StoreFront または NetScaler Gateway サーバーの詳細の更新」を参照してください。

その他

初回のセットアップを完了できない

初回セットアップ時に Director の構成が失敗した場合は、ライセンスサーバーを再構成できないことがあります。

解決策:

license_server テーブルを手動でクリーンアップしてください。

Secure Private Access 診断サポートバンドルの作成

次の手順を実行して、Secure Private Access 診断サポート・バンドルを作成します:

- PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
- ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)。
- 次のコマンドを実行します:

```
.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>
```

Secure Private Access の **SQL** データベース権限

データベースを自動作成するには、Secure Private Access プラグインホストマシンに、データベースに接続してデータベーススキーマを作成する権限が必要です。

リモートデータベース**:**

次の手順を実行して、リモートデータベースの権限を設定します。

1. 名前の構文CitrixAccessSecurity<Site Name>で空のデータベースを作成します。<Site Name>は、Secure Private Access のサイト名です。(例えば。CitrixAccessSecuritySPA)。

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Secure Private Access 仮想マシンのマシン ID 用の SQL Server ログインを作成します。たとえば、Secure Private Access ブローカーのマシン名が HOST1 で、マシンドメインが DOMAIN1 の場合、マシン ID は「DOMAIN1\ HOST1$」になります。ログインが既に作成されている場合は、このステップは無視できます。

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   ドメイン名は次のクエリを使用して検索できます:

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. db_owner ロールをマシン ID に割り当てます。

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'

   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

ローカルデータベース**:**

ローカルデータベースの権限を設定するには、次の手順を実行します。

1. 名前の構文CitrixAccessSecurity<Site Name>で空のデータベースを作成します。<Site Name>は Secure Private Access のサイト名です。(たとえば、CitrixAccessSecuritySPA)。

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. NT AUTHORITY\SYSTEM ユーザーの SQL Server ログインを作成します。ログインが既に作成されている場合は、このステップは無視できます。

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. db_owner ロールを「NT AUTHORITY\SYSTEM」ユーザーに割り当てます。

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'

   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

データベースを手動で作成すると、ダウンロードしたデータベーススクリプトによってマシン ID に権限が追加されます。

トラブルシューティングログのログレベルを変更

トラブルシューティングログはデフォルトのエラーログレベルです。

トラブルシューティングログのログレベルを変更するには、ランタイムサービス appsettings.json（C:\Program Files\ Citrix\ Citrix Access Security\ Runtime\ RuntimeService） で、`TroubleshootingSql` の`restrictedToMinimumLevel`を次のいずれかの値に更新します。

```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

Director を使用したトラブルシューティング

August 26, 2024

Director を Secure Private Access と統合すると、Secure Private Access セットアップのすべてのコンポーネントの問題が Director に取り込まれるため、効果的なパフォーマンスの監視とトラブルシューティングが可能になります。次の表は、Director に表示されるさまざまなエラーコードおよび関連する条件を示しています。

詳細については、以下のトピックを参照してください。

- Secure Private Access で Director を構成する
- Director で Secure Private Access セッションを表示する

> 注:
>
> - 2 桁目に「0」を含むコードは通常の実行フローを表します。たとえば、1000 はアプリの列挙が成功したことを表します。
> - 2 桁目に「1」を含むコードは、障害または例外を表します。たとえば、2101 はセッション障害を表します。障害や例外が発生した場合は、ログを調べて問題を解決することをお勧めします。それでも問題が解決しない場合は、サポートに連絡してください。

列挙関連コード

コード	状態	説明
1101	失敗	列挙中に内部エラーが発生しました。
1102	失敗	一部のアプリは列挙されましたが、少なくとも 1 つのアプリ評価が失敗しました。
1103	失敗	アプリは列挙されず、少なくとも 1 つのアプリ評価が失敗しました。
1000	成功	列挙は成功しました。少なくとも 1 つのアプリが列挙されました。
1001	成功	アプリはすべてポリシーによって拒否されたため、列挙されませんでした。
1002	成功	一致するポリシーがないため、アプリは列挙されませんでした。
1003	成功	一部のアプリは拒否され、他のアプリは一致するポリシーがなかったため、列挙されませんでした。
1004	成功	評価するポリシーがないため、アプリは列挙されませんでした。

セッション関連コード

コード	状態	説明
2101	失敗	セッション失敗。
2102	アクティブ/非アクティブ/障害	セッションがアクティブまたは終了しているか、セッションで少なくとも 1 つのアプリの起動が失敗しました。
2000	Active	セッションはアクティブです。
2001	非アクティブ	セッションは終了/非アクティブです。

アプリ列挙メッセージコード

コード	状態	説明
3101	失敗	アプリ列挙- 内部エラーが発生しました (現在は使用されていません)。
3102	失敗	ポリシー評価中に例外が発生したため、アプリが列挙されませんでした。
3103	失敗	アプリ列挙ステータスが null-ポリシー評価中に内部エラーが発生しました。
3104	許可/拒否/失敗	アプリのポリシー詳細を取得中にエラーが発生しました。
3000	許可	アプリの列挙は許可されています。
3001	拒否	アプリの列挙はポリシーにより拒否されます。
3002	拒否	一致するポリシーがないため、アプリが列挙されませんでした。
3003	不明	アプリの列挙状態は不明です。
3004	CEB からのアプリの起動	Citrix Enterprise Browser からアプリを起動しようとしました。

アプリ起動メッセージコード

コード	状態	説明
4101	失敗	アプリケーション起動エラー-アプリケーションの起動中に内部エラーが発生しました
4102	失敗	アプリケーション起動エラー (内部)
4103	許可/拒否/失敗	アプリのポリシー詳細を取得中にエラーが発生しました
4000	許可	アプリの起動は許可されています。
4001	拒否	ポリシーにより、アプリケーションの起動が拒否されました。
4002	拒否	一致するポリシーがないため、アプリケーションの起動は拒否されました。

SIEM 統合

August 26, 2024

Secure Private Access プラグインは、セキュリティ情報およびイベント管理 (SIEM) サービスとの統合をサポートします。セキュリティイベントは Windows イベントログ（イベントビューア\ アプリケーションとサービスログ\ Citrix Access Security）にリアルタイムで保存され、サードパーティツールで収集および分析できます。

次の表は、Secure Private Access プラグインのセキュリティ・イベントの一覧です:

イベント ID	まとめ	説明	接続元
4624	アカウントは正常にログオンされました	Secure Private Access 管理者が Secure Private Access 管理コンソールにログインしたときに作成されるイベント	Citrix Access Security Admin サービス
4625	アカウントがログオンできませんでした	Secure Private Access 管理者が Secure Private Access 管理コンソールへのログインに失敗したときに作成されたイベント	Citrix Access Security Admin サービス
4634	アカウントがログオフされました	Secure Private Access 管理者が Secure Private Access 管理コンソールからログオフしたときに作成されたイベント	Citrix Access Security Admin サービス
4720	ユーザーアカウントが作成されました	新しい Secure Private Access 管理者が追加されたときに作成されたイベント	Citrix Access Security Admin サービス
4738	ユーザーアカウントが変更されました	新しい Secure Private Access 管理者が更新したときに作成されたイベント	Citrix Access Security Admin サービス
4726	ユーザーアカウントが削除されました	新しい Secure Private Access 管理者が削除されたときに作成されたイベント	Citrix Access Security Admin サービス

イベント ID	まとめ	説明	接続元
8001	ユーザーのセキュア・アクセス・セッション	エンドポイントでユーザーセッションが開始または終了したときに作成されるイベント。ユーザー、セッション、デバイスの詳細、セッション中にアクセスした内部ドメインと外部ドメインが含まれます	Citrix Access Security Admin サービス
8002	ユーザーアクセス承認リクエスト	Secure Private Access プラグインがリソースへのアクセスを承認したときに作成されるイベント。リソースの FQDN と承認決定が含まれます	Citrix Access Security Admin サービス

参照ドキュメント

- セキュリティ情報およびイベント管理 (SIEM) の統合
- SIEM ソリューションへのログの共有について SIEM ソリューションへのログの共有について

ログ保持設定

August 26, 2024

ログは Secure Private Access データベースに 7 日間保存されます。ログの合計数が大きくなりすぎると (たとえば、100,000 を超えるなど)、90 日より前に最も古いログを削除できます。クリーンアップジョブは、デフォルトで 12 時間ごとに実行されます。このジョブは、ランタイムサービスが再起動するたびにも実行されます。

トラブルシューティングログの保持設定のカスタマイズ

ログのクリーンアップは、ランタイムサービスのインストールフォルダーにある appsettings.json ファイルを使用して設定できます。ログの保存期間とデータベースに保存できるログの数に基づいてクリーンアップを設定できます。必要に応じて、appsettings.json ファイル内の以下のエントリを変更します。

サンプルアプリ設定**.json** ファイル**:**


```
"TroubleshootingLogs": {

  "CleanupPeriodInHours": 12,
  "CleanupDataOlderThanDays": 7,
  "CleanupOldestDataIfEntriesCountAbove": 0
 }
```

クリーンアップを無効にするには、必要に応じて次の設定を行います。

- ログを 7 日間だけ保持するには、CleanupDataOlderThanDaysを 7 に設定します。
- 日単位のクリーンアップを無効にするには、CleanupDataOlderThanDaysを 0 に設定します。
- カウントベースのクリーンアップを無効にするには、CleanupOldestDataIfEntriesCountAbove を 0 に設定します。
- これらの設定が両方とも 0 に設定されている場合、またはCleanupPeriodInHoursが 0 に設定されている場合、ログは永久に保持されます。
  - ディスク使用率が 100% 低下する可能性があるため、CleanupDataOlderThanDaysまたはCleanupOldestDataIfEntriesCountAboveの両方を 0 に、またはCleanupPeriodInHours を 0 に設定することはお勧めしません。
  - ログのクリーンアップ頻度は、CleanupPeriodInHoursエントリを変更して変更することもできます。

> 注:
>
> Secure Private Access をクラスターとして展開する場合、これらの設定は各クラスターノードで変更する必要があります。ノード設定に不一致がある場合は、最も頻繁にクリーンアップされるインスタンスが優先されます。

ログとテレメトリのクリーンアップ

August 26, 2024

テレメトリデータのクリーンアップ

テレメトリデータは、Secure Private Access データベースに 3 か月間保存されます。クリーンアップが必要なテレメトリデータを特定するためのチェックは、30 秒ごとに行われます。

> 注:
>
> テレメトリデータのクリーンアップを開始するには、ランタイムサービスが実行されている必要があります。

CDF ログのクリーンアップ

CDF ログは、Secure Private Access インストールマシンの Admin およびランタイムサービスのインストールフォルダー内に保存されます。CDF ログは.csv ファイルに保存され、各ファイルには 10MB のサイズ制限が適用されます。
Admin サービスは一度に最大 90 個の CDF ログファイルを保持できます。その後、最も古いファイルを削除して、新しい CDF ログファイルを作成するためのスペースを空けます。
Runtime サービスは Admin サービスと同じように機能しますが、一度に保持できるファイル数は最大 600 個です。

CDF ログのカスタムクリーンアップ

CDF ログのクリーンアップは、管理サービスとランタイムサービスのインストールフォルダにある appsettings.json ファイルを使用して設定できます。ファイルのファイルサイズとカウント制限を変更するには、appsettings.json ファイルの次のエントリを更新します:

```
"CdfFile": {

       "fileSizeLimitBytes": 10485760, // 10 MB
       "retainedFileCountLimit": 600
      }
```

> 注:
>
> サイトに Secure Private Access の複数のインスタンスが設定されている場合は、Secure Private Access の各インストールマシンで appsettings.json ファイルを更新して CDF クリーンアップを行います。

サードパーティ通知

August 26, 2024

Citrix Secure Private Access オンプレミス向け）