



# Citrix Secure Private Access-オン プレミス

Machine translated content

## Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

## Contents

製品の技術概要	3
新機能	4
解決された問題	5
既知の問題	5
システム要件	8
サイズガイドライン	12
インストールと構成	15
<b>Secure Private Access</b> インストーラー	16
<b>Secure Private Access</b> のセットアップ	21
コンポーネント	29
<b>NetScaler Gateway</b>	30
コンテキストタグの設定	37
<b>StoreFront</b>	42
<b>Director</b>	44
ライセンスサーバー	45
<b>Web Studio</b>	45
アプリケーションの構成	46
アプリケーションのアクセスポリシーを設定します	49
<b>Secure Private Access</b> をクラスターとして展開	52
<b>Secure Private Access</b> のアンインストール	54
アップグレード	54
<b>Secure Private Access</b> インストーラーのアップグレード	55
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	58

管理	58
インストール後に設定を管理	59
アプリケーションとポリシーの管理	60
エンドユーザーフロー	62
監視とトラブルシューティング	64
ダッシュボードの概要	64
基本的なトラブルシューティング	66
<b>Director</b> を使用したトラブルシューティング	73
ログ保持設定	76
ログとテレメトリのクリーンアップ	77
サードパーティ通知	78

## 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。

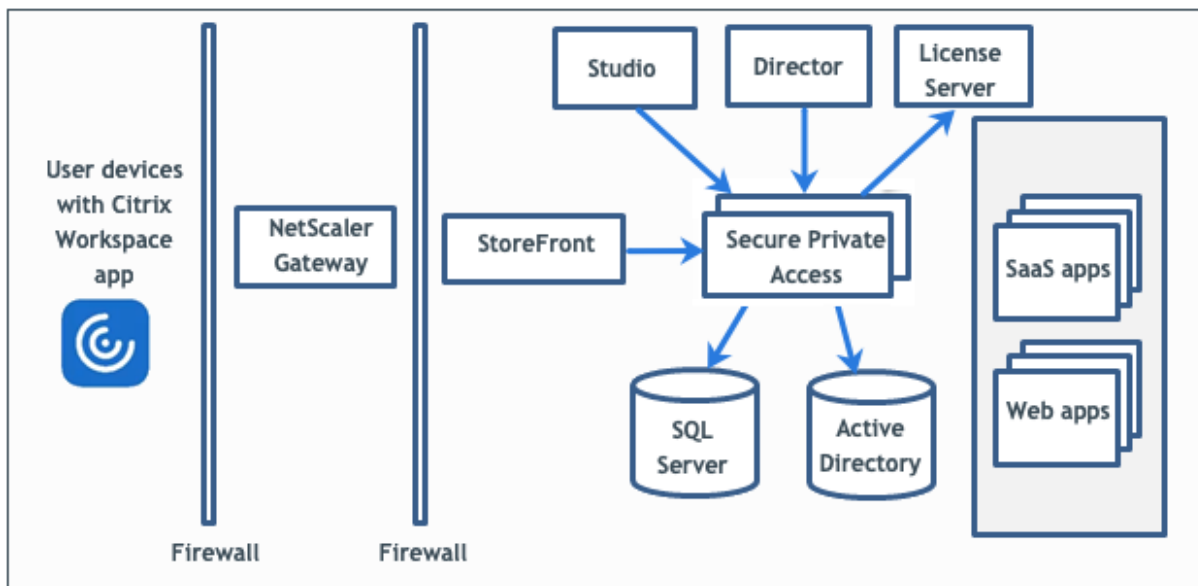
Citrix Secure Private Access オンプレミスソリューションは、Web および SaaS アプリへの統合アクセスポータルとして StoreFront のオンプレミスポータルを使用し、Citrix Workspace の統合部分として仮想アプリとデスクトップを使用することで、ブラウザーベースのアプリ (社内 Web アプリおよび SaaS アプリ) へのゼロトラストアクセスを簡単に提供できるため、組織の全体的なセキュリティとコンプライアンスの体制を強化します。

Citrix Secure Private Access は、NetScaler Gateway と StoreFront の要素を組み合わせ、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

2023年2月

### Citrix Secure Private Access と Director の統合

Citrix Secure Private Access が Director と統合され、パフォーマンス管理とトラブルシューティングの強化が可能になりました。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 Secure Private Access のユーザーセッションを表示できるようになりました。アクティブなセッションと失敗したセッションに関する詳細を表示できます。また、アプリ、ポリシー、および失敗したセッションと成功したセッションの詳細に関連する情報も確認できます。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。

## Citrix Secure Private Access とライセンスサーバーの統合

Citrix Secure Private Access がライセンスサーバーと統合され、ライセンスデータを収集して処理できるようになりました。詳細については、「[Secure Private Access を備えたライセンスサーバー](#)」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。

#### 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。

#### 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。

### 既知の問題

August 26, 2024

リリース 2402 には次の問題があります。

#### ドメインコントローラーの構成

- 異なる AD フォレストにまたがるドメイン間の信頼タイプを「フォレスト」とする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 公開アプリにアクセスできません。

- 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、以下を実行する必要があります：

Secure Private Access 管理サービスとランタイムサービスの両方の IIS アプリケーションプールに 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。

- 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。
- 配布グループは Secure Private Access ではサポートされていません。そのため、ポリシーでは配布グループを検索してユーザーとグループの条件を追加することはできません。
- Secure Private Access は、管理コンソールまたはサービスにドメインの詳細をキャプチャしません。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、そのドメインはサポートされません。

## NetScaler Gateway

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

- お客様は 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` トグルは有効になっています。

回避方法：

SSL プロファイルで構成された 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/Workspace for web

RFWeb/Workspace for Web はサポートされていないため、アプリは列挙されていません。詳しくは、「[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。

アプリケーションアイコン

ICO アイコン形式のみがサポートされています。PNG、JPEG、その他の形式はサポートされていません。

## 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。
- LDAP UPN と SAM アカウント名は異なります。

## アップグレード

- 2308 から 2402 以降へのアップグレードはサポートされていません。
- 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。

## StoreFront

- 「ストア」 > 「統合エクスペリエンスの設定」で、<StoreName>Web サイトのデフォルトトレシーバーを /Citrix/Web に設定する必要があります。以前のバージョンの StoreFront では、Web サイトのデフォルトトレシーバーは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、以前のバージョンの Receiver UI がクライアントに表示されます。StoreFront の構成について詳しくは、「[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] ページには、[Secure Private Access] プラグインの種類が **XenMobile** として表示されます。これは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は削除しないでください。これらのフォルダを削除すると、Secure Private Access は再作成できません。

## 管理コンソール

- 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。



[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ーの表示

ISO ファイルを使用して Secure Private **Access** を **2311** から **2402** 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 **Secure PrivateAccess** インストーラーの最初のエントリが置き換えられずに 2 つのエントリが表示されます。

- **Citrix Virtual Apps and Desktops 7 2402 LTSR**
- **Citrix Virtual Apps and Desktops 7 2311-Secure Private Access**

2311 ビルドインストーラーは、**Citrix Virtual Apps and Desktops 7 2311-Secure Private Access** を選択してアンインストールできます。

注:

Secure Private Access 2311 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、この問題は発生しません。

## システム要件

August 26, 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 –2309 以降
  - macOS –2309 およびそれ以降
- 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、およびそれ以降。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てください。詳細については、「[通信ポート](#)」を参照してください。

注:

オンプレミス向けの Secure Private Access 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

既存の NetScaler Gateway を作成または更新する場合は、次の詳細情報を確認してください:

- SSL/TLS 証明書で構成された IIS が稼働している Windows サーバマシン。このマシンに Secure Private Access プラグインがインストールされます。
- セットアップ中に入力する StoreFront ストアの URL。
- StoreFront のストアが構成されており、ストアサービスの URL が使用可能になっている必要があります。ストアサービス 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・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) の IP アドレスと FQDN。
- NetScaler 上で構成されている認証プロファイル名。
- NetScaler 上で SSL サーバ証明書が設定されています。
- ドメイン名。
- 証明書の設定が完了しました。管理者は証明書の設定が完了していることを確認する必要があります。Secure Private Access インストーラーは、マシンに証明書が見つからない場合に自己署名証明書を設定します。ただし、これが常に機能するとは限りません。

### 注:

ランタイムサービス (IIS デフォルト Web サイトの secureAccess アプリケーション) は Windows 認証をサポートしていないため、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、手動で変更しないでください。

## 管理者アカウント要件

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

- Secure Private Access のインストール: 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。
- Secure Private Access の管理: 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。

## 通信ポート

次の表は、Secure Private Access ・ プラグインが使用する通信ポートの一覧です。

接続元	接続先	種類	ポート	詳細	
管理ワークステーション	Secure Private Access・プラグイン	HTTPS	4443	Secure Private Access プラグイン-管理コンソール時刻同期	
Secure Private Access・プラグイン	NTP サービス	TCP、UDP	123		
	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の Director への連絡	
	ライセンスサーバー		TCP	8083	ライセンスデータを収集および処理するためのライセンスサーバーへの通信
			TCP	389	LDAP オーバープレーンテキスト (LDAP)
			TCP	636	SSL 経由の LDAP (LDAPS)
	Microsoft SQL Server	TCP	1433	Secure Private Access プラグイン-データベース通信	
	StoreFront	HTTPS	443	認証の検証	
	NetScaler Gateway	HTTPS	443	NetScaler Gateway コールバック	
StoreFront	NTP サービス	TCP、UDP	123	時刻同期	
	DNS サービス	TCP、UDP	53	DNS ルックアップ	
	Active Directory	TCP、UDP	88	kerberos	
		TCP	389	LDAP オーバープレーンテキスト (LDAP)	

接続元	接続先	種類	ポート	詳細
		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 Windows 認証プロトコル
	Secure Private Access・プラグイン	HTTPS	443	認証とアプリケーション列挙
	NetScaler Gateway	HTTPS	443	NetScaler Gateway コールバック
NetScaler Gateway	Secure Private Access・プラグイン	HTTPS	443	アプリケーション認証検証
	StoreFront	HTTPS	443	認証とアプリケーション列挙
	Web アプリケーション	HTTP、HTTPS	80, 443	構成済みの Secure Private Access 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の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](#)
- [SSL 証明書を NetScaler 上の仮想サーバー \(SSL\) にバインドします](#)。

## 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100K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

---

構成	詳細
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

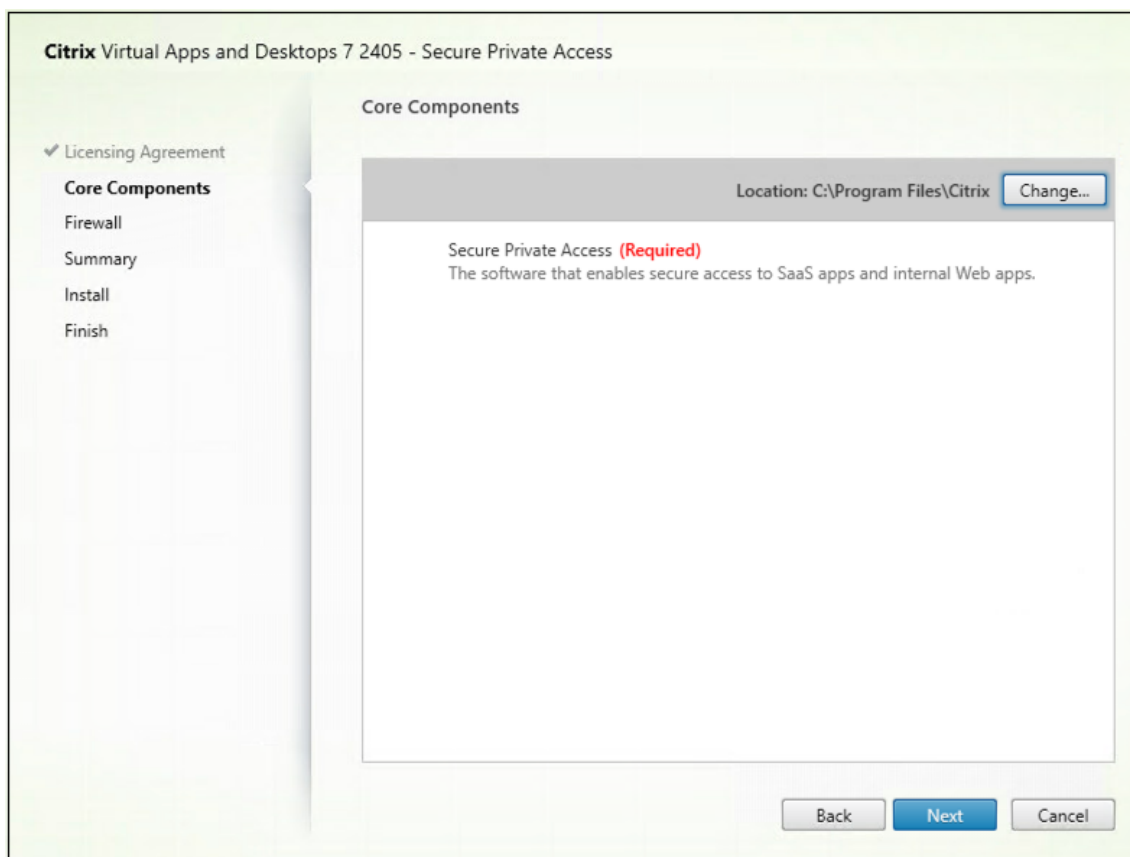
## Secure Private Access インストーラー

August 26, 2024

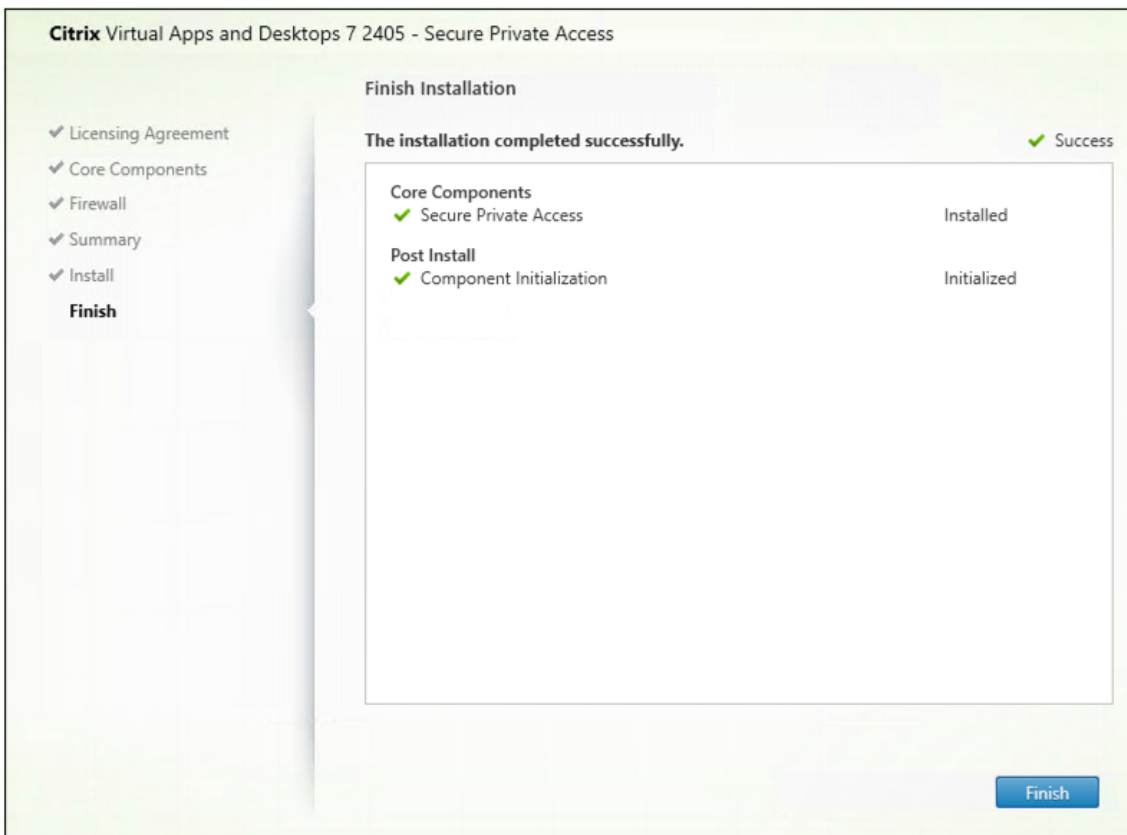
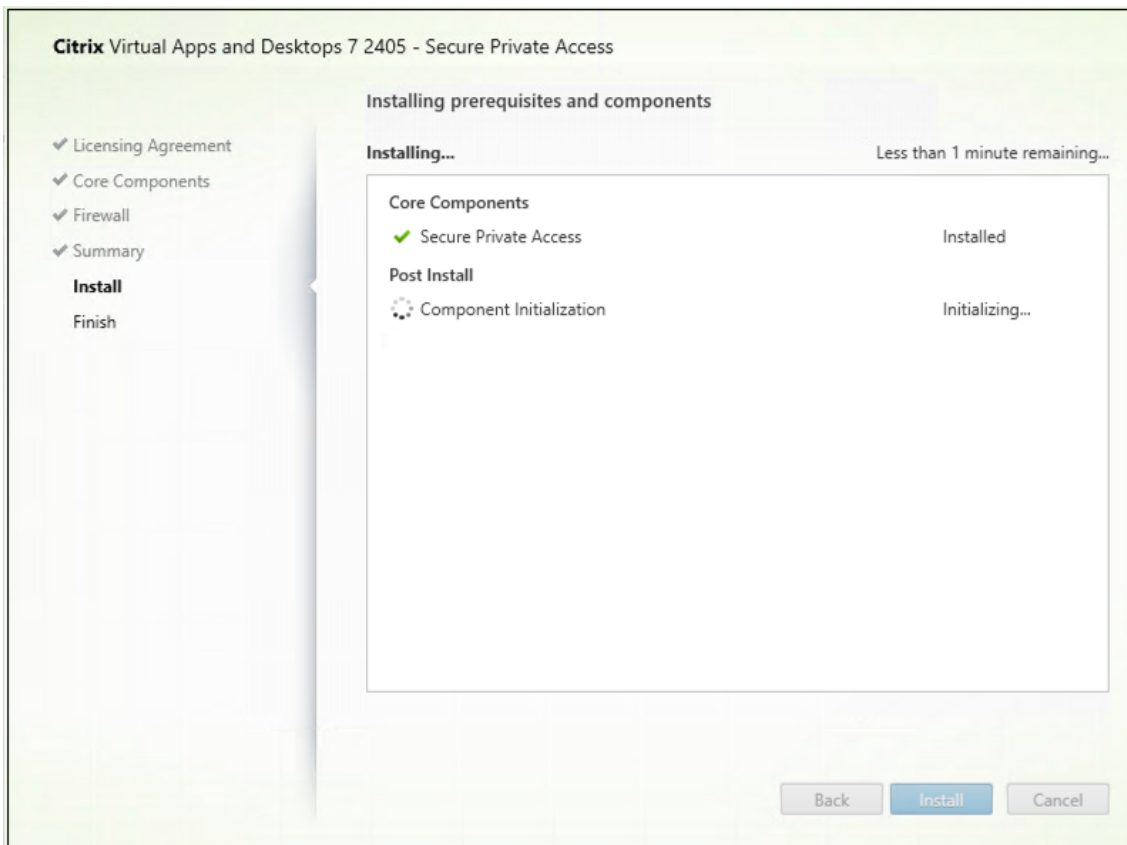
1. Citrix Secure Private Access のインストーラーを<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/>からダウンロードします。
2. .exe をドメインに参加しているマシン上で管理者として実行します。

注：

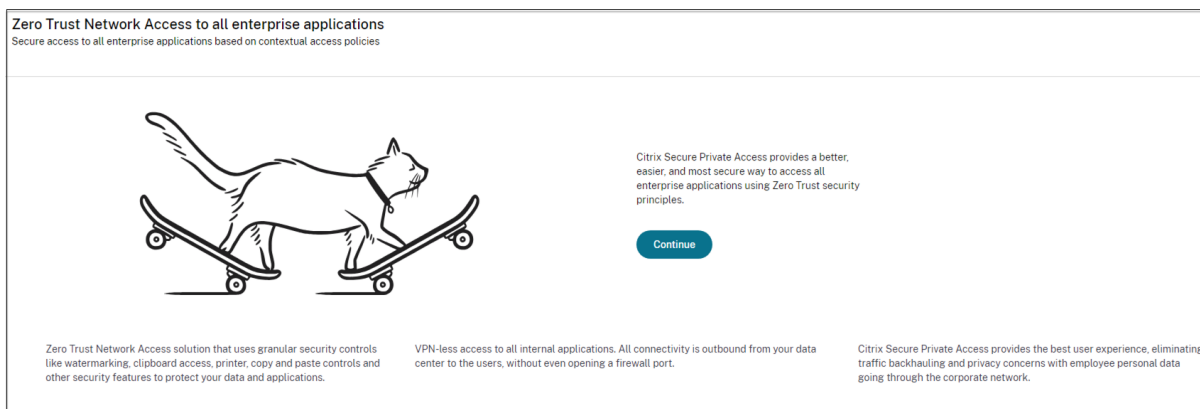
POC の目的で、StoreFront がインストールされているのと同じマシンに Secure Private Access をインストールすることをお勧めします。



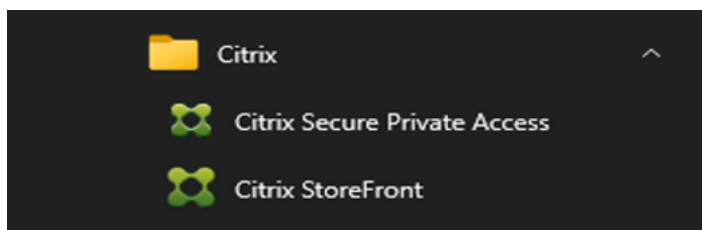
3. 画面の指示に従ってインストールを完了します。



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。

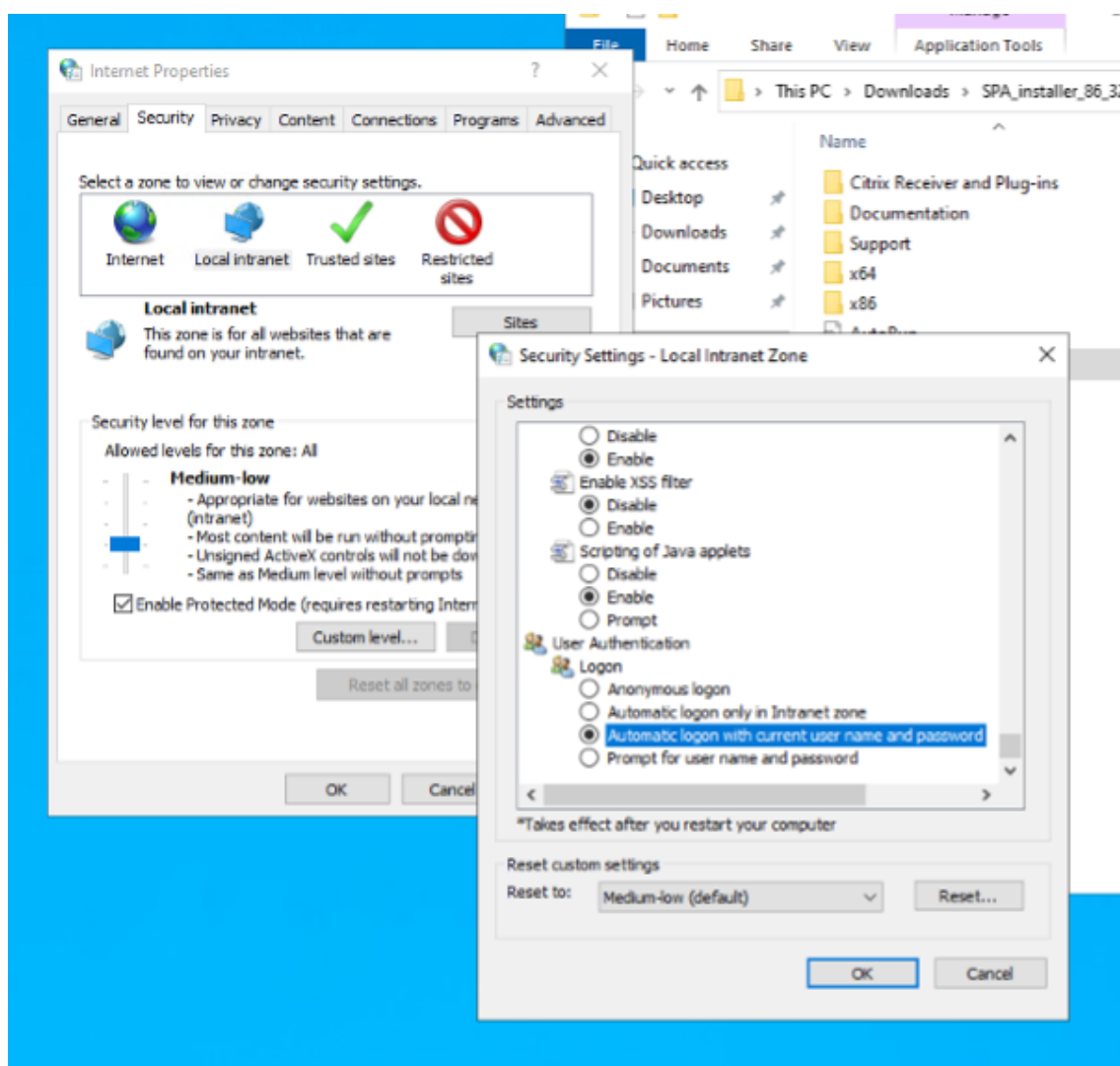
Secure Private Access のセットアップを続行するには、管理コンソールにサインインする必要があります。インストールマシンと同じドメインに属する任意のユーザーに Secure Private Access を設定できます。ただし、そのユーザーがインストールマシンのローカル管理者権限を持っている必要があります。

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](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。
- 他のブラウザについては、Kerberos 認証に関する特定のブラウザ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。

### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- 1 Site
- 2 Database
- 3 Integrations
- 4 Summary

#### Step 1: Creating or joining a site

A Secure Private Access site is a cluster of servers that all share the same configuration.

Create a new Secure Private Access site

Select this option if this is your first time installing Secure Private Access.

Join an existing Secure Private Access site

Select this option to add additional instances to an existing Secure Private Access site.

Next

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。

### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- Site
- Database
- Integrations
- Summary

#### Step 2: Database configuration

Every site requires its own database, which must be created by the database administrator or the machine identity. You can create the database on the same SQL server where you host the Citrix Virtual Apps and Desktops databases.

Enter the SQL Server address that will host the database and enter your desired site name.

SQL Server host\*  Site name\*

Select how you would like to create and/or configure your database:

Automatically

With this option, we'll automatically configure the database for you. If the database doesn't exist, we'll automatically create one. For the automatic creation and configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

Manually

With this option, you must manually create and configure the database yourself. After creating an empty database, download the script and share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

**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 権限がマシンにならない場合、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:** -Secure Private Access を Citrix Director に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。

### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- 3 Integrations
- 4 Summary

#### Step 3: Integrations

Connect with StoreFront and NetScaler Gateway servers so they can route traffic to Secure Private Access servers.

**Secure Private Access address \***  
Enter the address of your Secure Private Access server or the load balancer managing traffic for your Secure Private Access servers. The address doesn't need to be a public address.

 ✓

**StoreFront Store URL \***  
Enter your complete StoreFront Store URL.

 ✓  
[+ Add another Store URL](#)

**Public NetScaler Gateway address \***  
Enter all the addresses of the NetScaler Gateways accessing StoreFront. If you have a Global Server Load Balancing (GSLB) deployment, add the GSLB addresses as well.

 ✓  
[+ Add another public address](#)

**NetScaler Gateway virtual IP address and callback URL \***  
Enter the callback URL and virtual IP (VIP) address from each NetScaler Gateway. Each entry must match the values configured in StoreFront. [Learn more](#)

<b>Virtual IP address *</b> ⓘ <input type="text" value="10.80.174.125"/>	<b>Callback URL *</b> ⓘ <input type="text" value="https://gwgamma.spaopdev.local"/> ✓
---	--

  
[+ Add another virtual IP address and callback URL](#)

**Director URL \***  
Utilize the monitoring capabilities of Director in Secure Private Access. Enter the Director URL to configure Director for use in Secure Private Access. You must also use the configuration tool for Director as described in the [product documentation](#).

 ✓

**License Server URL \***  
A license server is a mandatory component required to collect and process licensing data. Enter the License Server URL to configure this component.

 ✓

[Test all URLs](#)

[Back](#) [Next](#)

#### 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。

### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- ✓ Integrations
- ✓ Summary

#### Step 4: Summary

Review the summary of your Secure Private Access setup.

#### Administration

You are a full administrator on this site and can add other administrators if needed.

#### Configurations

- SQL Server Database has been configured. ✓
- StoreFront has been configured. ✓
- NetScaler Gateway connected. ✓
- Director connected. ✓
- License Server connected. ✓
- Secure Private Access server connected. ✓

Close

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。

### You're almost done setting up

Finish the following tasks to complete the setup. These items are essential for publishing applications and policies.

- Configure Gateway**  
You must configure your Citrix Gateway for use with Secure Private Access by downloading the necessary scripts from the Gateway Downloads page.  
[Get Gateway scripts](#)  
[Mark as done](#)
- Configure StoreFront**  
You must configure StoreFront for use with Secure Private Access by downloading and running the necessary scripts.  
[Download StoreFront scripts](#)
- Director**  
To connect with Director for real-time diagnostics, you must use the configuration tool to configure Director with Secure Private Access as described in the product documentation.  
[Go to Director documentation](#)  
[Mark as done](#)

#### Service overview

<b>Active users</b> 65	<b>Applications</b> 319	<b>Application launch count</b> 316	<b>Access policies</b> 30
---------------------------	----------------------------	--	------------------------------

#### Troubleshooting resources

<b>Troubleshooting and Logs</b> View app access status and information for apps configured within Secure Private Access. <a href="#">Go to Troubleshooting Logs</a>	<b>Director</b> Search by end user in Director to view and triage Secure Private Access session activity. <a href="#">Go to Director</a>	<b>Gateway</b> Log into your Gateway appliance to track sessions and manage single sign-on across all applications. <small>Activate Windows Go to Settings to activate Windows.</small>
---	--	---

**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。

Zero Trust Network Access to all enterprise applications  
Secure access to all enterprise applications based on contextual access policies

Site  
② Database  
③ Summary

### Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host\* ⓘ  
i.e.: sql.example.com,1433

Site name\* ⓘ  
i.e.: Site1

Test connection

Select how you would like to create and/or configure your database:

Automatically  
With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Manually [Download script](#)  
With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Back Next

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。

**Zero Trust Network Access to all enterprise applications**  
Secure access to all enterprise applications based on contextual access policies

1 Site

2 Database

3 Summary

### Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host\* ⓘ  Site name\* ⓘ

[Test connection](#)

Select how you would like to create and/or configure your database:

**Automatically**

With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

**Manually** [Download script](#)

With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

[Back](#) [Next](#)

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:** 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

August 26, 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。例: `*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`。

例: `*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`

注:

- 一時データを保存するには、NetScaler /var/tmp フォルダ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。
- エラー `--bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M : bad interpreter: No such file or directory` 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。スクリプトは、Notepad++ などの任意のリッチテキストエディタを使用して変換できます。

3. NetScaler に SSH 接続し、シェルに切り替えます (NetScaler CLI では「シェル」と入力します)。
4. アップロードしたスクリプトを実行可能にします。そのためには `chmod` コマンドを使用してください。

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

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

```
root@ns32201# ./ns_gateway_secure_access_2405.sh
NetScaler Gateway vsrver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin IP:
SPA Plugin FQDN:
StoreFront Store URL (including protocol http/https):
NetScaler authentication profile name: authnprof
NetScaler SSL server certificate name: ns32205
Domain: cgwsanity.net
Enable TCP/UDP Apptype support (Y/N): Y

***** Gateway configuration *****
NetScaler Gateway name: spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin FQDN: spa.cgwsanity.net
SPA Plugin IP:
StoreFront Store URL:
NetScaler authentication profile name: authnprof
NetScaler Gateway server certificate name: ns32205
Domain: cgwsanity.net
Enable App type TCP/UDP:
*****

Checking SPA Plugin support...
NetScaler supports SPA CLI, skipping nsapimgr commands
Number of PEs running: 3
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
TCP/UDP Apptype support is enabled
Persisting TCP/UDP Apptype support setting: nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3 in /nsconfig/rc.netscaler file.

NetScaler Gateway creation script ns_gateway_secure_access created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output
Check ns_gateway_secure_access_output file for output
```

6. 必須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 証明書については、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。





既存の構成を使用して **NetScaler Gateway** に **Secure Private Access** を構成する

既存の NetScaler Gateway 上のスクリプトを使用して、Secure Private Access をサポートすることもできます。ただし、このスクリプトは以下を更新しません:

- 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ときは、次のパラメーターが定義済みの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:

- tcpProfileName: nstcp\_default\_XA\_XD\_profile
- 展開タイプ:ICA\_STOREFRONT (コマンドでのみ使用可能) `add vpn vserver`
- icaOnly: オフ

仮想サーバーの更新:

- tcpProfileName: nstcp\_default\_XA\_XD\_profile
- icaOnly: 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使用して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、次のパラメーターが定義済みの値に設定されていることを確認してください。

- transparentInterception: オフ
- SSO: オン
- ssoCredential: プライマリ
- useMIP: NS
- useIIP: オフ
- icaProxy: オフ
- wihome: "<https://storefront.mydomain.com/Citrix/MyStoreWeb>" -実際のストア URL に置き換えます。/Citrix/MyStoreWeb ストアへのパスはオプションです。
- ClientChoices: オフ
- ntDomain: mydomain.com-SSO に使用 (オプション)
- defaultAuthorizationAction: 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 固有の認証ポリシーをバインドするために使用されています)
- clientlessVpnMode: オン
- clientlessModeUrlEncoding: 透明
- SecureBrowse: 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
```

セッションアクションパラメータの詳細については、を参照してください <https://developer-docs.netscaler.com/en-us/ad-command-reference-int/13-1/vpn/vpn-sessionaction>。

## ICA アプリとの互換性

Secure Private Access プラグインをサポートするように作成または更新された NetScaler Gateway を使用して、ICA アプリを列挙して起動することもできます。この場合、Secure Ticket Authority (STA) を構成し、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 の DDC 展開の一部です。

詳細については、以下のトピックを参照してください：

- [NetScaler Gateway での Secure Ticket Authority 構成](#)
- [よくある質問:Citrix Secure Gateway/NetScaler Gateway Secure Ticket Authority](#)

## 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 が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 およびそれ以降
- 14.1–4.42 およびそれ以降

スマートアクセスタグは、Secure Private Access プラグインリクエストのヘッダーとして追加されます。

これらの NetScaler バージョンでは、トグル `ns_vpn_enable_spa_onprem` または `ns_vpn_disable_spa_onpre` を使用してこの機能を有効/無効にします。

- 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 コールアウト設定の 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、「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 -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
```

- CDN でホストされている「アクセス制限」 ページを使用してください。

```
nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

- 無効にするには、同じコマンドをもう一度実行します。

- 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

Secure Private Access プラグインの設定を NetScaler に保持するには、次の操作を行います：

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

```
nsapimgr -ys call=ns_vpn_enable_spa_onprem
```

```
nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
```

```
nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
```

```
nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

3. ファイルを保存します。

Secure Private Access プラグインの設定は、NetScaler の再起動時に自動的に適用されます。

### 既知の制限事項

- 既存の NetScaler Gateway はスクリプトで更新できますが、1つのスクリプトでは対応できない NetScaler 構成は無限にあります。
- NetScaler Gateway では ICA プロキシを使用しないでください。この機能は、NetScaler Gateway が構成されている場合は無効になります。
- 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 のプライベート 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

パブリックゲートウェイに 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 /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。

The screenshot shows the Citrix Secure Private Access console interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The main content area is titled 'Create Preauthentication Policy'. It features a 'Name\*' field with the value 'Windows10', a 'Request Action\*' dropdown menu, and an 'Expression\*' field with three 'Select' dropdown menus. Below these fields are 'Add' and 'Edit' buttons. At the bottom of this panel are 'Create' and 'Close' buttons. A secondary panel on the right, titled 'Create Preauthentication Profile', contains a 'Name\*' field with 'win10\_profile', an 'Action\*' dropdown menu set to 'ALLOW', and fields for 'Processes to be cancelled', 'Files to be deleted', and 'Default EPA Group' (set to 'spaopdev'). This panel also has 'Create' and 'Close' buttons at the bottom.

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。

This screenshot shows the 'Create Preauthentication Policy' panel in detail. The 'Name\*' field contains 'Windows10'. The 'Request Action\*' dropdown is empty. The 'Expression\*' field contains the sample expression: `CLIENT.OS(win10).HOTFIX == EXISTS`. Below the expression field are 'Add' and 'Edit' buttons. At the bottom of the panel are 'Create' and 'Close' buttons.

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。

**Add Expression**

Select Expression Type: Client Security ▾

Component  
Operating System ▾

Name\*  
Windows 10 ▾

Qualifier  
Hotfix ▾

Operator  
== ▾

Value\*  
EXISTS|

Frequency (min)  
[Empty text box]

Error Weight  
[Empty text box]

Freshness  
[Empty text box]

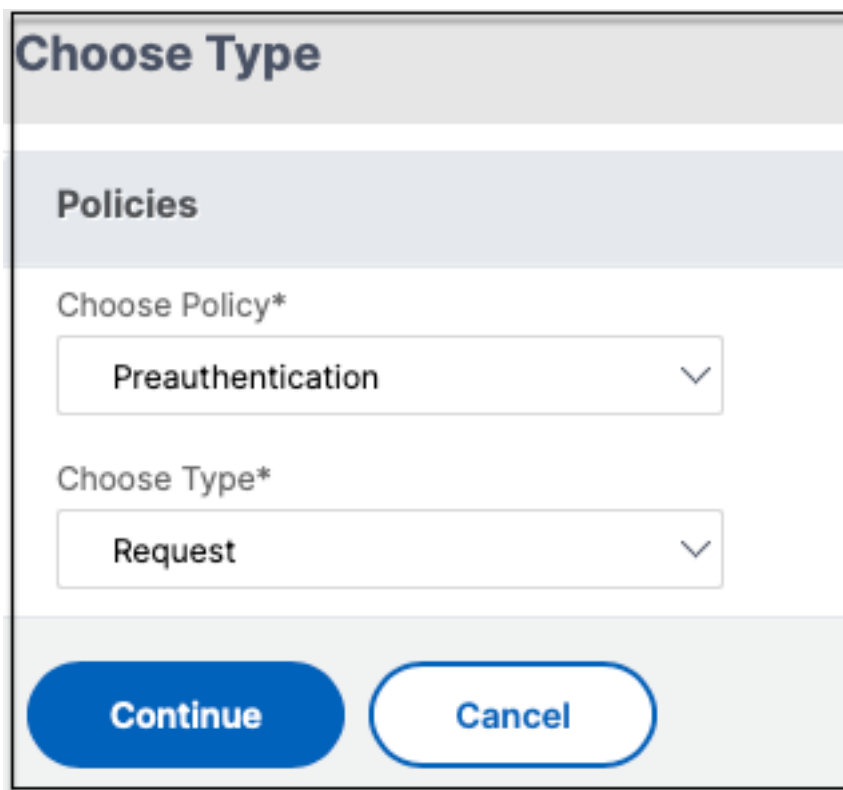
**Done** **Cancel**

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。



The screenshot shows a dialog box titled "Choose Type". Under the "Policies" section, there are two dropdown menus. The first is labeled "Choose Policy\*" and has "Preauthentication" selected. The second is labeled "Choose Type\*" and has "Request" selected. At the bottom of the dialog, there are two buttons: "Continue" (a solid blue button) and "Cancel" (a white button with a blue border).

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。

The screenshot shows a configuration window titled "Choose Type". It has three main sections:

- Policies:** A table with two columns. The first column is "Choose Policy" and the second is "Choose Type". The row "Preauthentication" is selected in the first column, and "Request" is selected in the second column.
- Policy Binding:** A section with a "Select Policy\*" dropdown menu containing "Windows10", an "Add" button, an "Edit" button, and an information icon.
- Binding Details:** A section with a "Priority\*" input field containing the value "100".

At the bottom of the window are two buttons: "Bind" and "Close".

### 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 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 StoreFront 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。

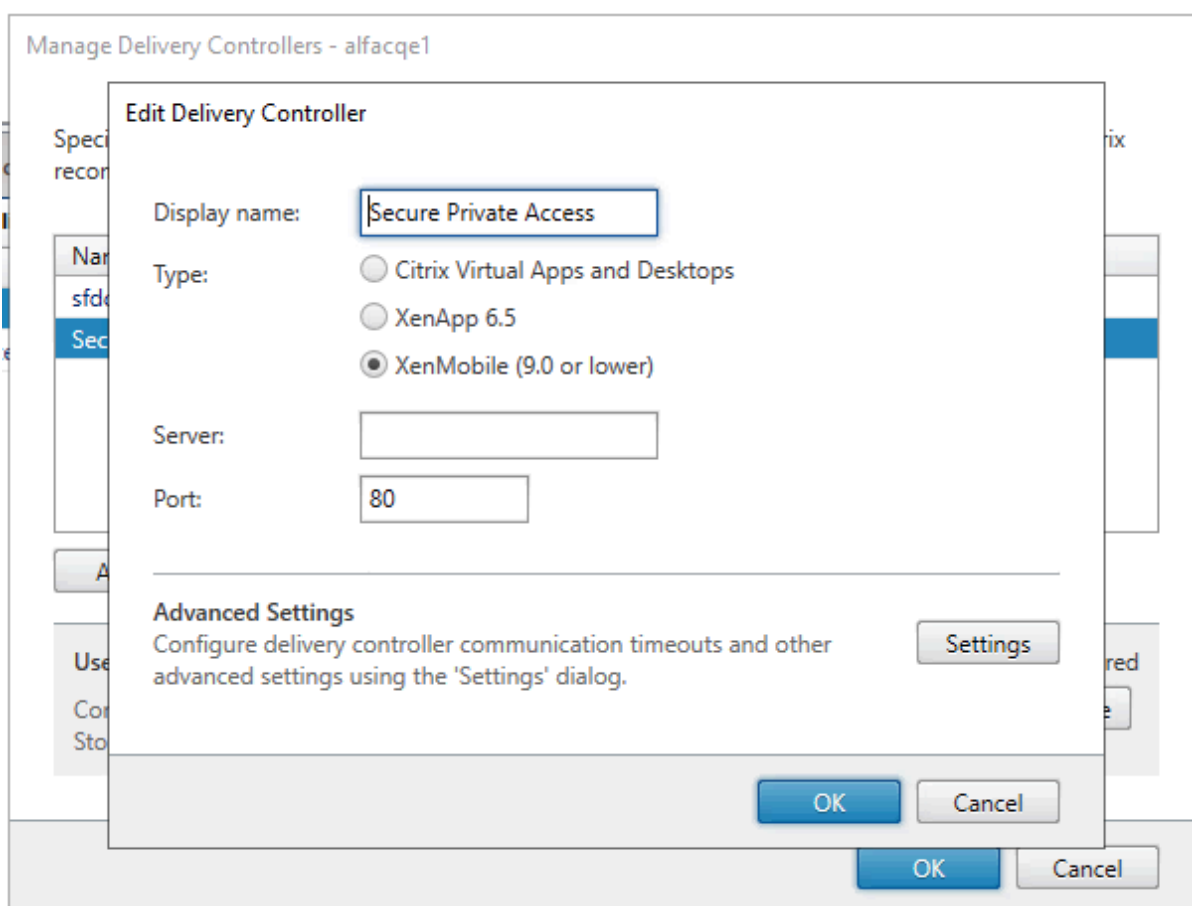
StoreFront は、[設定] > [統合] ページから追加できます。

- Secure Private Access が StoreFront と共存している場合でも、StoreFront 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 プラグインに登録するには、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

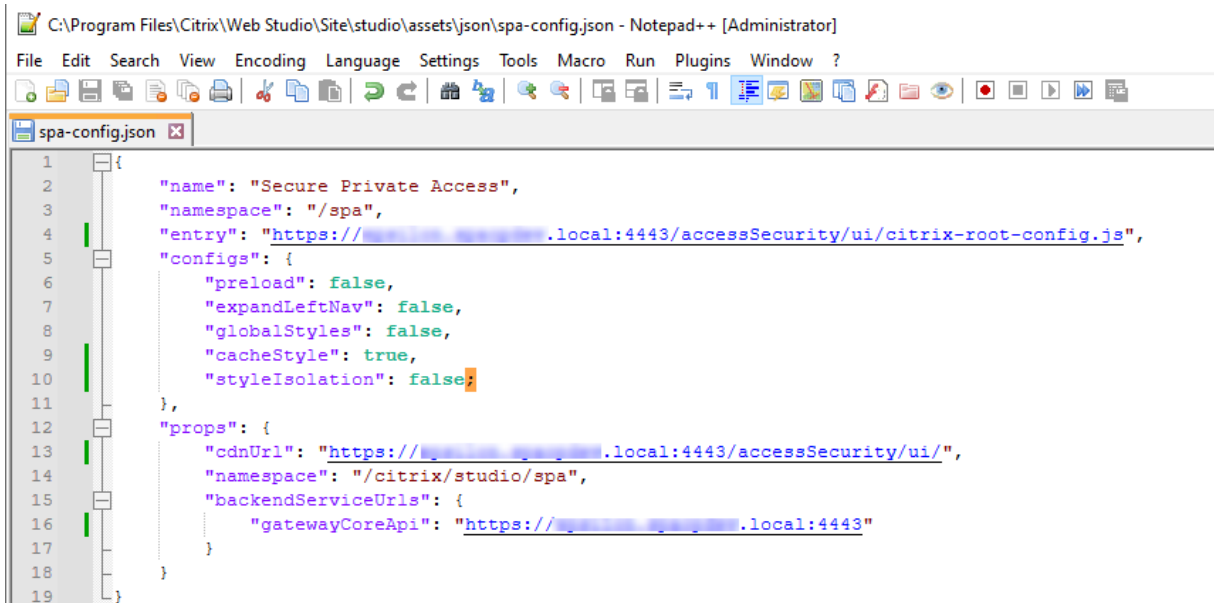
Citrix Secure Private Access も Web Studio コンソールに統合されているため、ユーザーは Web Studio を介してサービスにシームレスにアクセスできます。

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。



```
C:\Program Files\Citrix\Web Studio\Site\studio\assets\json\spa-config.json - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
spa-config.json
1 {
2   "name": "Secure Private Access",
3   "namespace": "/spa",
4   "entry": "https://[redacted].local:4443/accessSecurity/ui/citrix-root-config.js",
5   "configs": {
6     "preload": false,
7     "expandLeftNav": false,
8     "globalStyles": false,
9     "cacheStyle": true,
10    "styleIsolation": false;
11  },
12  "props": {
13    "cdnUrl": "https://[redacted].local:4443/accessSecurity/ui/",
14    "namespace": "/citrix/studio/spa",
15    "backendServiceUrls": {
16      "gatewayCoreApi": "https://[redacted].local:4443"
17    }
18  }
19 }
```

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。

## アプリケーションの構成

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。
- アプリケーションをお気に入り自動的に追加—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設定します

August 26, 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、アプリへのアクセスを制限できます。

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。

The image shows two side-by-side screenshots of the 'Create Access Policy' configuration interface in the Citrix Secure Private Access console.

**Left Screenshot: Policy for Web/SaaS apps**

- Policy name and applications:** Policy name: msn-pol; Applications: msn
- Conditions:** User conditions: Matches any of (selected), spablr1.com, spablr1.com\Administrator
- Actions:** Allow access with restrictions (selected)
- Access Restrictions (0):** Add restrictions button
- Enable policy on save:** Unchecked

**Right Screenshot: Policy for TCP/UDP apps**

- Policy name and applications:** Policy name: rdp; Applications: Go
- Conditions:** User conditions: Matches any of (selected), spaopdev.local, spaopdev.local\SPAOP users; AND; Contextual Tags (selected), Matches all of (selected), allow\_access
- Actions:** Allow access (selected)
- Enable policy on save:** Checked

3. 「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。
4. ユーザー/ユーザーグループで、アプリアクセスを許可または拒否す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。
  - いずれかに一致: フィールドに表示されている名前のいずれかに一致するユーザーまたはグループのみがアクセスを許可されます。

- いずれにも一致しない: フィールドに表示され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がアクセスを許可されます。
5. コンテキストタグに基づいて別の条件を追加するには、「条件を追加」をクリックします。これらのタグは NetScaler Gateway から取得されます。
  6. 「コンディショナルタグ」を選択し、アプリへのアクセスを許可または拒否する条件を選択します。
  7. 「次に以下を実行する」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
    - 制限付きアクセスを許可
    - アクセスを拒否

「制限付きでアクセスを許可」を選択すると、次の制限を選択できます。

### Add/edit restrictions ✕

0 selected  View selected only

	Access Settings	Current Value
> <input type="checkbox"/>	Clipboard	Allowed
> <input type="checkbox"/>	Copy	Allowed
> <input type="checkbox"/>	Download MIME types	Multiple options
> <input type="checkbox"/>	Downloads	Allowed
> <input type="checkbox"/>	Insecure content	Prohibited
> <input type="checkbox"/>	Keylogging protection	Allowed
> <input type="checkbox"/>	Microphone	Ask every time
> <input type="checkbox"/>	Notifications	Ask every time
> <input type="checkbox"/>	Paste	Allowed
> <input type="checkbox"/>	Personal data masking	Multiple options
> <input type="checkbox"/>	Popups	Block
> <input type="checkbox"/>	Printing	Allowed
> <input type="checkbox"/>	Printing options	Multiple options
> <input type="checkbox"/>	Screen capture	Allowed
> <input type="checkbox"/>	Upload MIME types	Multiple options
> <input type="checkbox"/>	Uploads	Allowed
> <input type="checkbox"/>	Watermark	Disabled
> <input type="checkbox"/>	Webcam	Ask every time

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

注:

キーロギングと画面キャプチャの制限は、Citrix Workspace デスクトップクライアントにのみ適用されます。

8. [ポリシー名] に、ポリシーの名前を入力します。
9. [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

アクセスポリシーを作成すると、デフォルトで優先順位番号がアクセスポリシーに割り当てられます。優先順位は、アクセスポリシーのホームページで確認できます。

優先順位の値が小さいほど、優先順位が最も高くなり、最初に評価されます。このポリシーが定義された条件と一致しない場合、優先順位番号の小さい次のポリシーが評価され、それ以降も同様です。

優先順位を変更するには、「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します。

### 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。

#### [サンプル構成検証](#)

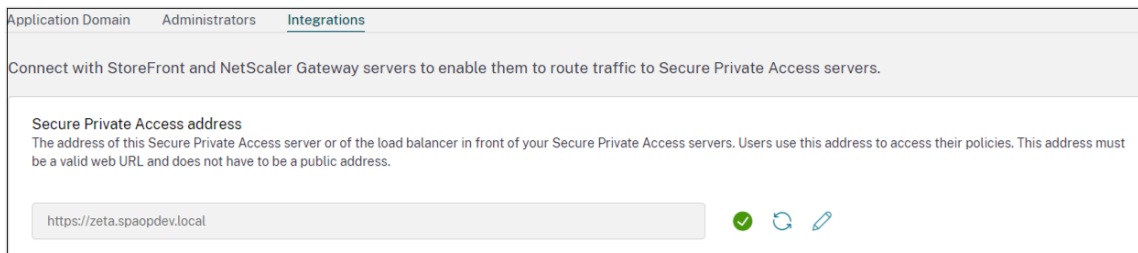
## Secure Private Access をクラスターとして展開

August 26, 2024

Secure Private Access オンプレミスソリューションはクラスターとして展開できるため、高可用性、高スループット、スケーラビリティを実現できます。大規模な展開 (ユーザー数が 5000 人を超える場合など) には、スタンドアロンの Secure Private Access ノードを展開することをお勧めします。

### Secure Private Access ノードの作成

- 新しい Secure Private Access サイトを作成します。詳細については、「[Secure Private Access サイトのセットアップ](#)」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 Secure Private Access 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設定します。証明書のサブジェクトの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 の最初のノードを設定するときは、ロードバランサー名を使用してください。後続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。



Application Domain Administrators Integrations

Connect with StoreFront and NetScaler Gateway servers to enable them to route traffic to Secure Private Access servers.

**Secure Private Access address**  
The address of this Secure Private Access server or of the load balancer in front of your Secure Private Access servers. Users use this address to access their policies. This address must be a valid web URL and does not have to be a public address.

### ロードバランサー構成

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、サブジェクトの別名 (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 の両方を含めてください。これは SSL 証明書に適用されます。Secure Private Access には、ロードバランサーを設定すれば十分です。詳しくは、「[NetScaler による負荷分散](#)」を参照してください。

Secure Private Access 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、ベース URL にロードバランサー名を設定し、HTTPS を使用して安全な通信を行います。詳しくは、「[HTTPS による StoreFront のセキュリティ保護](#)」を参照してください。

- Secure Private Access 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。Secure Private Access サービスは HTTP としても展開できます。
- 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ー設定を使用できます。SSL ブリッジを使用するときは、各 Secure Private Access ノードで同じサーバー証明書を設定してください。また、証明書のサブジェクトの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、ロードバランサーサービスで SAN を設定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。
- Secure Private Access サービス (管理とランタイムの両方) はステートレスなので、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ビルトインモニター (プローブ) があります。Secure Private Access オンプレミスサーバー用にカスタム HTTP ベースのモニター (プローブ) を設定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`

期待される応答:

```
1  Http status code: 200 OK
2
3  Payload:
4
5  {
6    "status":"OK","details":{
7    "duration":"00:00:00.0084206","status":"OK" }
8  }
```

NetScaler ロードバランサーの構成について詳しくは、「[基本的な負荷分散の設定](#)」を参照してください。

### Secure Private Access 用のモニターを作成

次の CLI コマンドを使用して、Secure Private Access 用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について詳しくは、「[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 2402 – 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。

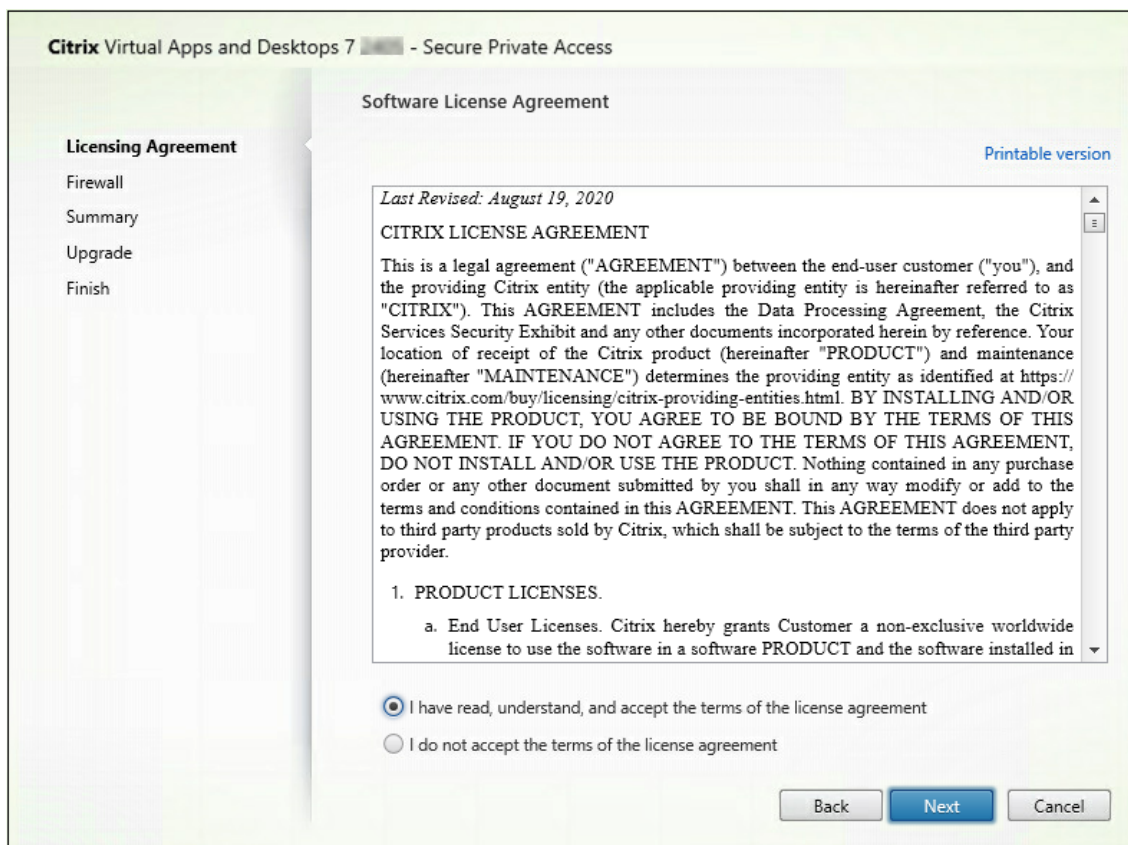
4. (オプション) NetScaler Gateway クリプトを実行します。詳しくは、「[NetScaler Gateway](#)」を参照してください。

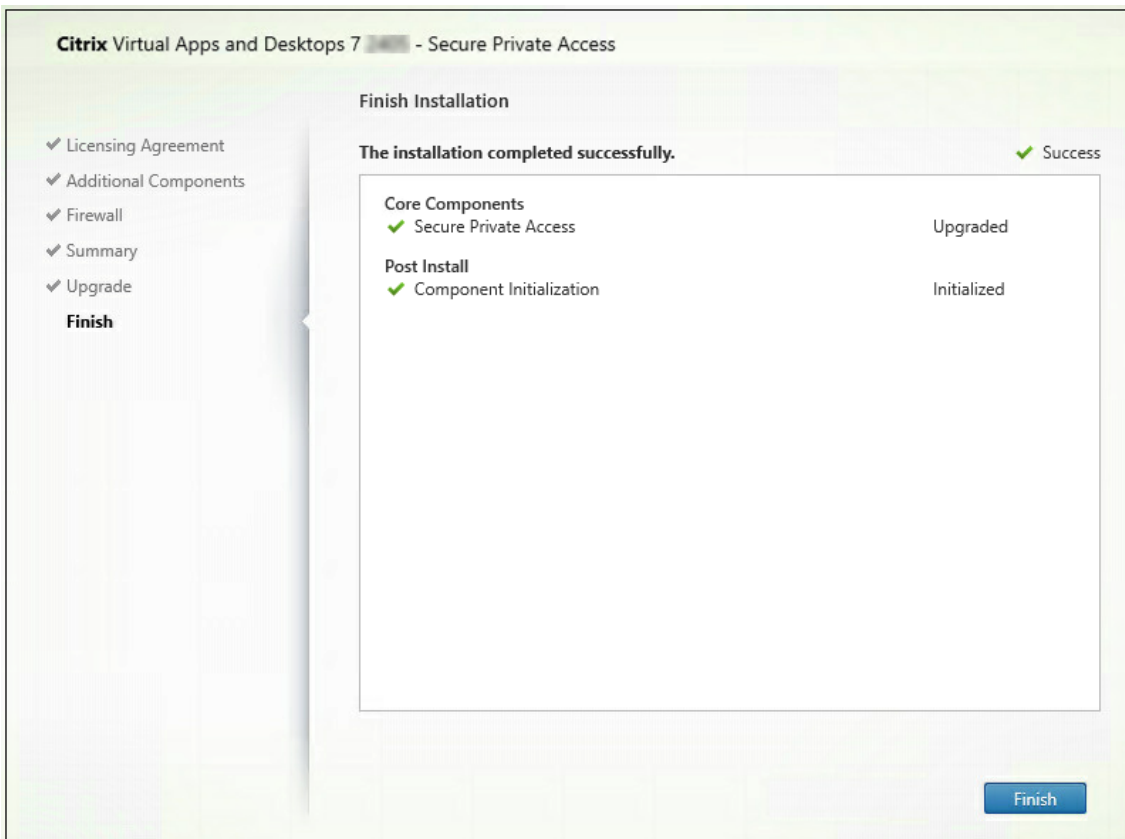
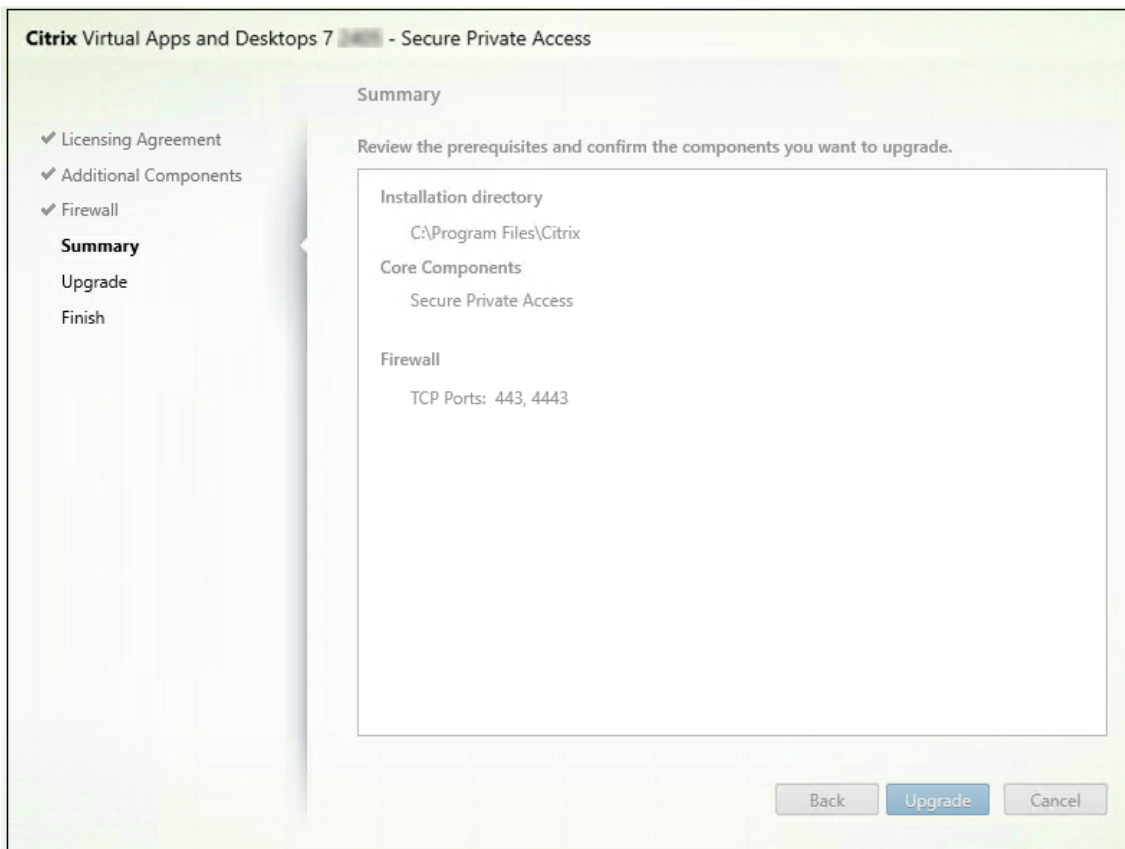
## Secure Private Access インストーラーのアップグレード

August 26, 2024



1. Citrix Secure Private Access 2402 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 2402 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:

- [アプリケーションドメインのルーティングを管理](#)
- [管理者の管理](#)
- [統合設定の変更](#)

## 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。

The screenshot shows the 'Integrations' page in the Citrix Secure Private Access management console. The page is titled 'Connect with StoreFront and NetScaler Gateway servers to enable them to route traffic to Secure Private Access servers.' It contains several configuration sections:

- Secure Private Access address:** A text input field containing 'https://gamma.spaopdev.local'. A green checkmark and a refresh icon are visible to the right.
- StoreFront Store URL:** A text input field containing 'https://gamma.spaopdev.local/Citrix/StoreGamma'. A green checkmark, a refresh icon, and a 'Download Script' button are visible to the right. Below the field is a '+ Add another Store URL' link.
- Public NetScaler Gateway address:** A text input field containing 'https://gwgamma.spaopdev.local'. A green checkmark, a refresh icon, and a 'Refresh Certificate' button are visible to the right. Below the field is a '+ Add another public address' link.
- NetScaler Gateway virtual IP address and callback URL:** Two text input fields. The 'Gateway VIP' field is empty, and the 'Callback URL' field contains 'https://gwgamma.spaopdev.local'. A green checkmark and a refresh icon are visible to the right. Below the fields is a '+ Add another virtual IP address and callback URL' link.
- Director URL:** A text input field containing 'https://gamma.spaopdev.local'. A green checkmark and an edit icon are visible to the right.
- License Server URL:** A text input field containing 'https://ls.spaopdev.local'. A green checkmark, a refresh icon, and an edit icon are visible to the right.

The left sidebar of the console shows navigation options: Overview, Applications, Access Policies, Settings, and Troubleshooting. The top navigation bar shows 'Application Domain', 'Administrators', and 'Integrations'.

## 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。

### Edit App

Click Finish once you're finished editing your app.

**App Details**

Where is the application located? \*

Outside my corporate network


Inside my corporate network

---

**App type \***

HTTP/HTTPS

**App icon**

 [Change icon](#) [Use default icon](#)  
(128 KB max, ICO)

Do not display application icon in Workspace app

Add application to favorites in Workspace app

Allow user to remove from favorites

Do not allow user to remove from favorites

**App name \***

Slack

**App description**

**App category ⓘ**

Verizon

---

**URL \***

https://csg.enterprise.slack.com

**App Connectivity ⓘ**

Internal

**Related Domains \***

\*.csg.enterprise.slack.com

**App Connectivity ⓘ**

Internal

**Related Domains \***

\*.slack.com

**App Connectivity ⓘ**

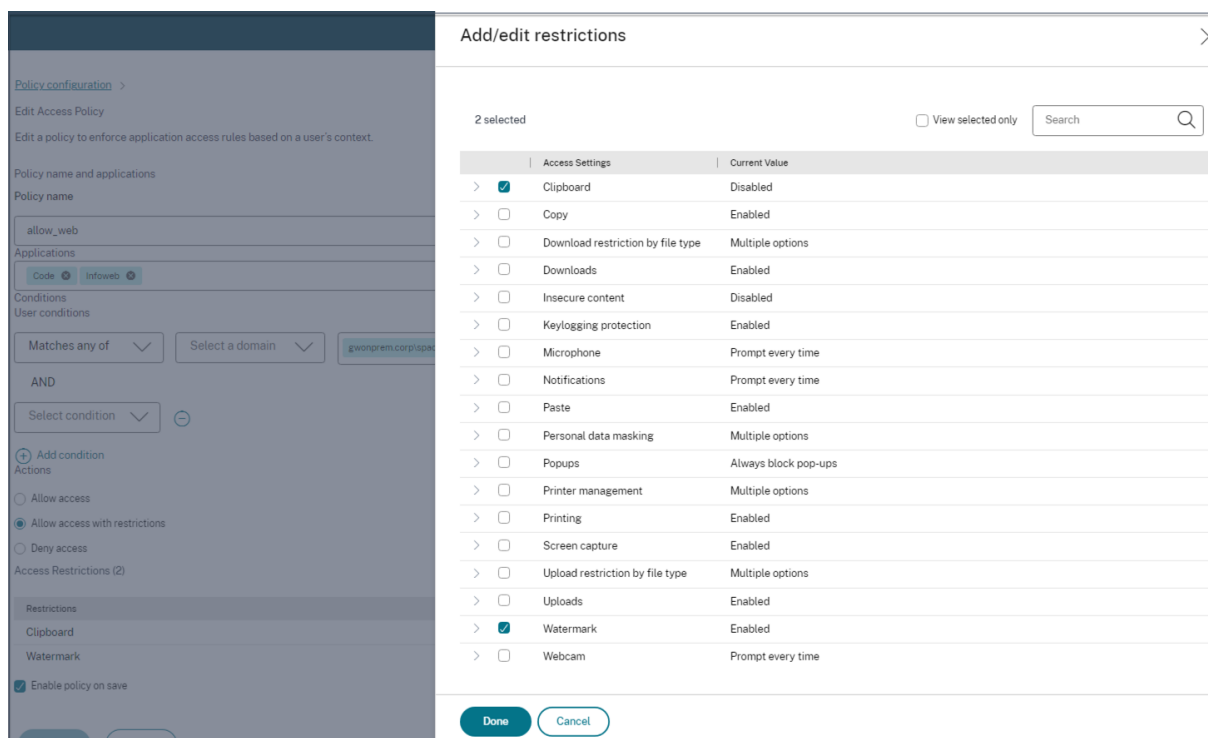
Internal

[+ Add another related domain](#)

**Save** **Cancel**

## 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。



## エンドユーザーフロー

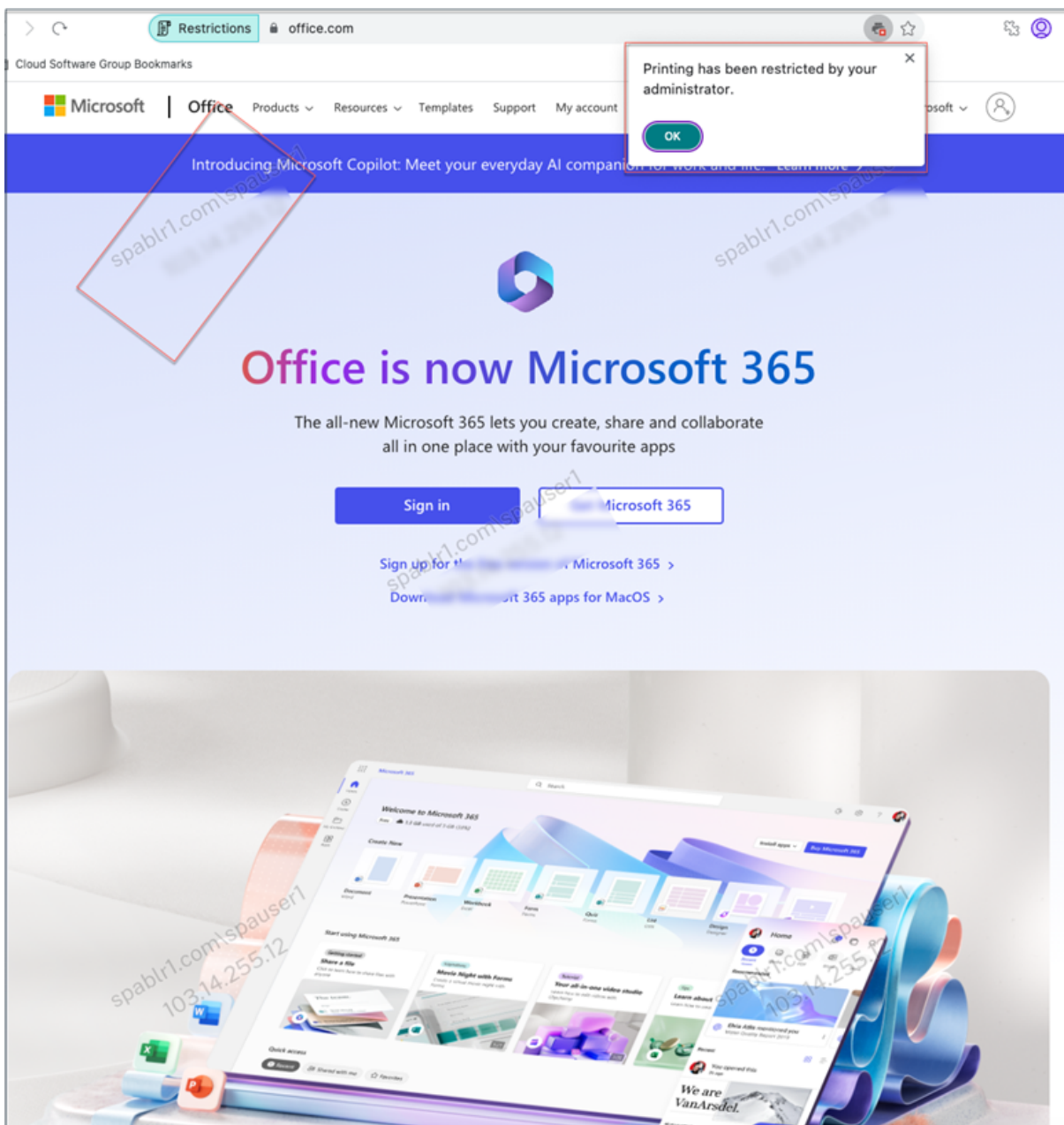
August 26, 2024

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

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。

事前に設定した時間またはカスタムタイムラインのログを表示できます。ダッシュボードに表示したい情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログは CSV 形式にエクスポートできます。

フィルター (CATEGORY と RESULT) を使用して検索結果を絞り込むことができます。

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2024-06-19 13:26:29	spouser@spab1.com	App Enumeration	Success	e4e1460e-0f37-4a25-8f90-a57a936f16a4	Total apps enumerated for user spouser@spab-
2024-06-19 13:26:29	spouser@spab1.com	App Enumeration	Success	e4e1460e-0f37-4a25-8f90-a57a936f16a4	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 13:26:29	spouser@spab1.com	App Enumeration	Success	e4e1460e-0f37-4a25-8f90-a57a936f16a4	Credential validation succeeded for user spous-
2024-06-19 13:26:29	spouser@spab1.com	App Enumeration	Success	e4e1460e-0f37-4a25-8f90-a57a936f16a4	Received Gateway callback response successf-
2024-06-19 12:55:22	spouser@spab1.com	App Access	Success	e278a3c3-7636-41af-8f9f-966168f7015b	Successfully validated the user credentials rec-
2024-06-19 12:55:22	spouser@spab1.com	App Access	Success	e278a3c3-7636-41af-8f9f-966168f7015b	Policy evaluation returned access state as ALL-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	Policy evaluation returned access state as ALL-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	Policy evaluation returned access state as ALL-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	Policy evaluation returned access state as ALL-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	659b39f6-5049-4a8e-9926-da5a56a9098	Policy evaluation returned access state as ALL-
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	688977eb-9f59-4ec7-8ef5-e97ba2a42c97	Successfully generated and sent the policy doc-
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	688977eb-9f59-4ec7-8ef5-e97ba2a42c97	Policy evaluation returned access state as ALL-
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	400088ca-5068-4840-b76a-7b20594a1cc7	SmartAccess tags received PL_OS_SecureAcc-
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	400088ca-5068-4840-b76a-7b20594a1cc7	Policy evaluation returned access state as ALL-
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	688977eb-9f59-4ec7-8ef5-e97ba2a42c97	SmartAccess tags received PL_OS_SecureAcc-

次のパラメータと検索フィールドの演算子に基づいて検索を絞り込むこともできます。

- User-Name
- カテゴリ
- イベントタイプ
- 結果
- トランザクション ID
- 詳細

ユーザーログと上位アクセスポリシー別の適用チャートで検索を絞り込むために使用できる検索演算子は次のとおりです。

- =: 検索条件に完全に一致するログ/ポリシーを検索します。
- !=: 指定された条件が含まれていないログ/ポリシーを検索します。
- ~: 検索条件に部分的に一致するログ/ポリシーを検索します。
- !~: 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 **Event-Type = DSAuth** という文字列を使用すると、イベントタイプ「**DSAuth**」を検索できます。

同様に、「operator」という用語の一部を含むユーザーを検索するには、**User-Name ~ 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」

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 を使用してトラブルシューティングログをフィルタリングし、特定のアプリアクセスリクエストに関連するすべてのログを検索できます。

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。

The screenshot displays the logs management interface. On the left, there are filters for 'CATEGORY' (App Enumeration, App Access) and 'RESULT' (Success, Failure). The main area shows a search bar with 'User-Name = \"User\"' and a 'Last 1 Week' time filter. Below the search bar, a message states 'Results are limited to the first 1000 records. Narrow your search criteria for more relevant results.' and an 'Export to CSV format' link. The table below has columns for TIME, USER NAME, CATEGORY, RESULT, TRANSACTION ID, and DETAILS. A tooltip is shown over a row, displaying 'Applications: Wikipedia is ALLOWED by Wikipedia\_spaop\_win10, Google is ALLOWED by Google\_spaop' and 'ContextualTags: Windows10, PL\_OS\_SecureAccess\_Gateway'.

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-09-07 10:29:13	spaopdev.local/usera	App Access	Failure	9c7c2de9-0351-43b1-8...	ERROR: Error in process...
2023-09-07 10:29:13	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 10:29:12	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 10:29:12	spaopdev.local/usera	App Access			DSAuth validation was s...
2023-09-07 09:48:50	spaopdev.local/usera	App Access			Successfully generated ...
2023-09-07 09:48:50	spaopdev.local/usera	App Access			Show Details
2023-09-07 09:48:49	spaopdev.local/usera	App Access			SmartAccess tags recei...
2023-09-07 09:48:49	spaopdev.local/usera	App Access			DSAuth validation was s...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	Show Details
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	Policy evaluation return...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	SmartAccess tags recei...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	DSAuth validation was s...
2023-09-07 09:46:27	spaopdev.local/usera	App Access	Failure	6e9d1dd1-5bdb-4474-8...	ERROR: Error in process...

## 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.registryKeyNotFoundException 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。

```
1 - Information
2 - Debug
3 - Warning
4 - Error
5
6 "TroubleshootingSql": {
7
8   "restrictedToMinimumLevel": "Error",
9   "batchPostingLimit": 50,
10  "batchPeriod": "00:00:05" // 5 seconds
11 }
```

## 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てしました。

## 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。

## 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:

```
1  "TroubleshootingLogs": {
2
3    "CleanupPeriodInHours": 12,
4    "CleanupDataOlderThanDays": 7,
5    "CleanupOldestDataIfEntriesCountAbove": 0
6  }
```

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

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:

```
1 "CdfFile": {  
2  
3     "fileSizeLimitBytes": 10485760, // 10 MB  
4     "retainedFileCountLimit": 600  
5 }
```

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](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).