



Citrix Secure Private Access-オンプレミ ス

Contents

新機能	6
2023年12月	6
シトリックス セキュア プライベート アクセス™ オンプレミス向け – 一般提供開始	6
Citrix Virtual Apps and Desktops™ と統合された セキュアプライベートアクセス インストーラー	6
既知の問題	7
ドメインコントローラーの構成	7
ネットスケーラー® ゲートウェイ	7
RfWeb / Web用ワークスペース	8
アプリケーションアイコン	8
管理者管理	8
アップグレード	8
ストアフロント™	8
ログ	9
Secure Private Accessをインストールするための管理者アカウント要件	9
セキュリティ制限	9
管理コンソール	9
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	10
セキュア プライベート アクセス インストーラー	11
管理コンソールへのSSO	12
次のステップ	13
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	14
サイジングガイドライン	15
データベースストレージ要件	15
展開ガイドライン	15
その他のコンポーネント構成	17

セキュア プライベート アクセスを設定する	18
前提条件	18
新しいサイトを作成して Secure Private Access をセットアップする	18
ステップ 1: Secure Private Access サイトをセットアップする	18
ステップ2: データベースの構成	19
ステップ3: ストアフロントおよびネットスケーラー® ゲートウェイサーバーを統合する	20
ステップ4: 構成の概要	21
既存のサイトに参加してSecure Private Accessをセットアップする	21
次のステップ	22
ネットスケーラー ゲートウェイ の設定	23
既存の構成を持つNetScaler Gatewayでセキュアプライベートアクセスを構成する	24
ネットスケーラー ゲートウェイ仮想サーバーの設定	25
ネットスケーラー ゲートウェイ セッションアクション	25
ICA®アプリとの互換性	26
スマートアクセスタグのサポート	27
既知の制限事項	27
パブリックゲートウェイ証明書のアップロード	28
コンテキストタグを設定する	28
GUIを使用してカスタムタグを設定する	29
従来のゲートウェイ事前認証ポリシーを構成する	29
カスタムタグをNetScaler Gatewayにバインドする	29
CLIを使用してカスタムタグを構成する	30
新しいコンテキストタグの追加	30
参考文献	30
ストアフロントを構成する	31
StoreFrontバージョン2308以前を使用している場合	32
StoreFrontバージョン2311以降を使用している場合	32
アプリケーションを構成する	33

次のステップ	34
アプリケーションのアクセスポリシーを構成する	35
アクセスポリシーの優先順位	36
次のステップ	36
エンドユーザーフロー	37
セキュアプライベートアクセスとWeb Studioの統合	38
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	39
セキュア プライベート アクセス ノードを作成する	39
ロードバランサーの構成	39
インストール後の設定を管理する	41
アプリケーションドメインのルーティングを管理する	41
セキュア プライベート アクセス の 管理者を管理する	41
セットアップ後にStoreFront™またはNetScaler Gatewayサーバーの詳細を更新する	41
ダッシュボードの概要	43
ログからコンテキストタグを表示する	44
一般的なエラーのトラブルシューティング	45
証明書エラー	45
データベース作成エラー	45
ストアフロント™ の障害	46
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	48
Secure Private Accessサーバーへの接続に失敗しました	49
データベース接続チェックの失敗	49
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	49
アプリケーション列挙の失敗	50
その他の問題	50
セキュア プライベート アクセス診断サポートバンドルの作成	50
Secure Private Access の SQL データベースに対するアクセス権限	51
トラブルシューティングログの保持	53

トラブルシューティングログの保持設定をカスタマイズする	53
ログとテレメトリのクリーンアップ	55
テレメトリデータのクリーンアップ	55
CDFログのクリーンアップ	55
CDFログのカスタムクリーンアップ	55
セキュアプライベートアクセスをアンインストール	57
StoreFront ストア構成からセキュアプライベートアクセスプラグインを削除する	57
セキュア プライベート アクセス 2311 と旧バージョンの互換性	59
シトリックス バーチャルアップス アンド デスクトップス™ デリバリーコントローラーのク リーンアップ	59
シトリックス ストアフロントのクリーンアップ	60
ネットスケーラー ゲートウェイ のクリーンアップ	61
ネットスケーラー ゲートウェイ 仮想サーバー	61
セッションポリシーとアクション	61
承認ポリシー	61
サードパーティ通知	62

新機能

2023年12月

シトリックス セキュア プライベート アクセス™ オンプレミス向け – 一般提供開始

Citrix Secure Private Access for on-premisesは、Citrix Virtual Apps and Desktops 2311リリースの一部として一般提供が開始されました。Citrix Secure Private Accessオンプレミスソリューションは、StoreFrontをWebアプリおよびSaaSアプリへの統合アクセス ポータルとして使用し、仮想アプリおよびデスクトップとともにCitrix Workspaceの統合された一部として、ブラウザベースのアプリ（社内WebアプリおよびSaaSアプリ）にZero Trust Network Accessを簡単に提供する機能により、組織全体のセキュリティとコンプライアンス体制を強化します。このソリューションは、NetScalerおよびStoreFrontの既存リリースとバージョンを変更することなく互換性があります。詳細については、「Secure Private Access for on-premises」([/ja-jp/citrix-secure-private-access/current-release](https://ja-jp.citrix-secure-private-access/current-release))を参照してください。

Citrix Virtual Apps and Desktops™ と統合された セキュアプライベート アクセス インストーラー

Secure Private AccessインストーラーはDesktop Delivery Controller (DDC)と統合されており、コマンドラインとGUIを使用してインストールできるようになりました。詳細については、「コアコンポーネントのインストール」([/ja-jp/citrix-virtual-apps-desktops/install-configure/install-core-components](https://ja-jp/citrix-virtual-apps-desktops/install-configure/install-core-components))を参照してください。

既知の問題

オンプレミスソリューション向けのCitrix Secure Private Access™には、今後のリリースで対処される予定の以下の既知の問題があります。

ドメインコントローラーの構成

- 異なるADフォレスト間のドメインにおける、信頼の種類が「フォレスト」であ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またはb.comに結合されているマシンに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。
- オンプレミス向け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、以下の操作を行う必要があります。
 - Secure Private Access AdminサービスとRuntimeサービスの両方について、IISアプリケーションプールで別のドメインサービスアカウントをIDとして追加します。
- 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）アプリ列挙のSecure Private Accessではサポートされていません。
- 分散グループはSecure Private Accessではサポートされていません。そのため、ポリシーはユーザーおよびグループ条件を追加するために分散グループを検索できません。
- Secure Private Accessは、管理コンソールまたはサービスでドメインの詳細をキャプチャしません。そのため、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や、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。

ネットスケーラー® ゲートウェイ

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

- お客様がNetScaler Gateway 13.1–48.47以降、または14.1–4.42以降を使用している場合。

- `ns_vpn_enable_spa_onprem` トグルが有効になっています。

回避策:

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 / Web用ワークスペース

RfWeb / Web用ワークスペースはサポートされていません。アプリは列挙されますが、アプリの起動に失敗する可能性があります。

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。

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になった後（サインアウトまたはトークンの有効期限切れによる）にのみ反映されます。

アップグレード

2308から2311以降へのアップグレードはサポートされていません。2308をアンインストールし、必要なバージョン（2311以降）を再インストールする必要があります。

ストアフロント™

- **ストア > 統合エクスペリエンスの構成**で、Webサイトのデフォルトレシーバーを/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レシーバーは空白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バージョン2308以前を使用している場合、**ストア > デリバリーコントローラーの管理**ページには、Secure Private Accessプラグインの種類が**XenMobile®**と表示されます。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てはいけません。これらのフォルダが削除されると、Secure Private Accessは再作成できません。

Secure Private Accessをインストール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をセットアップするには、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、そのユーザーが最初のSecure Private Access管理者となり、他の管理者を追加できるようになります。
- 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。

セキュリティ制限

最初に公開された関連ドメインが別のドメインに置き換えられた場合、アプリに関連付けられたセキュリティ制限は機能しません。

例えば、関連ドメインを `edition.test.com` としてアプリを作成し、アプリケーションに印刷制限とウォーターマークを適用します。アプリケーションURLにアクセスすると、セキュリティ制限が適用されます。しかし、同じアプリケーションを編集し、関連ドメイン `edition.test.com` を `*.1800flowers.com` に置き換えると、新しいアプリケーションURLにアクセスしてもセキュリティ制限は適用されません。

管理コンソール

公開された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) は、関連ドメインエントリが変更されても自動的に閉じません。

例えば、アプリ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。アプリ公開後、関連ドメイン `www.example.com` を `abc.com` に置き換え、**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。

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2308から2311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、最初のエントリを置き換えるのではなく、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。

- Citrix 仮想アプリおよびデスクトップ™ 7 2311
- シトリックス バーチャルアプリ アンド デスクトップ 7 2308 - セキュア プライベート アクセス

プレビュービルドインストーラーは、**Citrix Virtual Apps and Desktops 7 2308 - セキュアプライベートアクセス** を選択してアンインストールできます。

注:

セキュアプライベートアクセス 2308スタンドアロンインストーラーを2311スタンドアロンインストーラーでアップグレードする場合、この問題は発生しません。

セキュア プライベート アクセス インストーラー

1. シトリックス セキュア プライベート アクセス 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. ドメインに参加しているマシンで、.exeを管理者として実行します。

注：

POCの目的では、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をセットアップできます。



デスクトップのスタートメニュー（**Citrix > Citrix Secure Private Access™**）にもセキュアプライベートアクセスのショートカットが表示されます。



詳しくは、以下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てインストールする」 (</ja-jp/citrix-virtual-apps-desktops/install-configure/install-core/install-command>)

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) を使用するためです。

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際に、ブラウザから資格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。
- 資格情報を入力しない場合、Secure Private Access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ユーザーであれば、そのユーザーがインストールマシンに対するローカル管理者権限を持っている場合、Secure Private Accessをセットアップできます。

Google ChromeおよびMicrosoft Edgeブラウザの場合、Kerberosを有効にするには、次の手順を実行します。

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」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。

複数のマシンにSecure Private Accessを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. 「レベルのカスタマイズ」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的にログオンする」を選択します。



注:

- If using Chrome Incognito sessions, create a DWORD registry key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AmbientAuthenticationInPrivate` and set to value 1.
- シークレットモードでKerberosが有効になる前に、すべてのChromeウィンドウ（シークレットモード以外のウィンドウを含む）を再起動する必要があります。
- その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。

次のステップ

- セキュアプライベートアクセスをセットアップする
- ネットスケーラー ゲートウェイを構成する
- アプリケーションを構成する
- アプリケーションのアクセスポリシーを構成する

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

管理構成ツールを使用して、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. 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. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, 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 /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder>
```

サイジングガイドライン

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構成によるストレージスペースの消費は、ログと比較するとごくわずかです。

次の表は、ユーザーセッション、ログ、ユーザーあたりの1日あたりのアプリ列挙などのパラメーターに基づいたサーバーのストレージ要件を示しています。

ユーザーセッション	ユーザーあたりの1日あたりのアプリ列挙	ユーザーあたりの1日あたりのアプリアクセス	1日あたりの総アプリアクセス数	1日あたりのストレージ消費量	ログ保持期間（日数）	ログ保持期間中の総ストレージ使用量（7日間）
1000	20	100	100000	2.5 GB	7	17.5 GB
1000	10	50	50000	1.27 GB	7	9 GB

注記:

- メトリックは、ログイベントのクリーンアップが無効になっており、ログ保持期間が7日に設定されているという仮定に基づいて導き出されています。
- デフォルトでは、ログは90日間、または設定された設定に応じて最大10万件のログイベントが保持されます。これらの設定は、Secure Private Access Runtimeサービスのappsettings.jsonファイルで利用でき、必要に応じて変更できます。詳細については、「[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。

展開ガイドライン

次の表は、同時アプリ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が使用するCPUなどのパラメーターに基づいたデータベースのサイジング要件を示しています。

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 アプリ列挙	セキュアプライベートアクセスメモリ (GB)	セキュアプライベートアクセスCPU	ストレージ (GB)	注記
20未満 (PoC目的)	2	4 GB	2	40 GB*	PoC目的の場合、SPAは既存のVMスペックを変更することなく、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	パフォーマンス向上のため、2つ以上のSPAノードをデプロイできます

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10 MBのサイズのロールオーバーログファイルを600個保持します。そのため、Secure Private Accessの管理者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量は12 GBです。また、PoC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の場合、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をデプロイすることをお勧めします。
- *** このような負荷に対しては、既知のパフォーマンス問題があるため、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
SQLサーバー	4	16 GB
ストアフロント	4	8 GB
アクティブディレクトリ	8	16 GB

セキュア プライベート アクセスを設定する

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 をセットアップできます。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 環境をセットアップできます。

- 新しいサイトを作成して Secure Private Access をセットアップする
- 既存のサイトに参加して Secure Private Access をセットアップする

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がインストールされている必要があります。

新しいサイトを作成して Secure Private Access をセットアップする

ステップ 1: Secure Private Access サイトをセットアップする

サイトとは、Secure Private Access 展開の名前です。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. セキュア プライベート アクセス ウェブ管理コンソールを起動します。
2. 「サイトの作成または参加」ページで、デフォルトで「新しい Secure Private Access サイトを作成」が選択されています。
3. 「次へ」をクリックします。



サイトを作成することを選択した場合、サイト名に対応するデータベースがセットアップで利用できない可能性があるため、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: データベースの構成

新しいSecure Private Accessサイト用に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 Host**で、サーバーホスト名を入力します。例: `sql11.fabrikam.local\citrix`。

データベースアドレスは、次のいずれかの形式で指定できます。

- サーバー名
- サーバー名\インスタンス名
- サーバー名、ポート番号

詳細については、[データベース](#)を参照してください。

2. **サイト**で、Secure Private Accessサイトの名前を入力します。
3. **Test Connectivity**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、指定され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が利用できない場合、接続チェックは失敗します。
- SQL Serverが利用可能でも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。
- セキュアプライベートアクセスは、マシンIDによるWindows認証を使用して、SQL Serverへの認証を行います。

自動構成:

- 「**Automatic Configuration**」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。
- 指定されたアドレスにデータベースが存在しない場合、データベースは自動的に作成されます。
- データベースを作成する際は、空であること、および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、「[データベースのセットアップに必要な権限](#)」を参照してください。

手動構成:

データベースをセットアップするには、「**Manual Configuration**」オプションを使用できます。

手動構成では、まずスクリプトをダウンロードし、次に「**SQL Server Host**」フィールドで指定したデータベースサーバー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可能性があります。マシン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、「[データベースのセットアップに必要な権限](#)」を参照してください。

ステップ3：ストアフロントおよびネットスケーラー® ゲートウェイサーバーを統合する

セキュアプライベートアクセスをストアフロントおよびネットスケーラーゲートウェイサーバーに接続するには、ストアフロントおよびネットスケーラーゲートウェイサーバーの詳細を指定する必要があります。この接続は、ストアフロントおよびネットスケーラーゲートウェイがセキュアプライベートアクセスにトラフィックをルーティングできるようにするために確立する必要があります。

1. 次の詳細を入力します。

- セキュアプライベートアクセスサーバーアドレス。例: `https://secureaccess.domain.com`。
- ストアフロント ストアURL。例: `https://storefront.domain.com/Citrix/StoreMain`。
- パブリックゲートウェイアドレス – NetScaler GatewayのURL。例: `https://gateway.domain.com`。
- ゲートウェイコールバックアドレス – 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`。
- ゲートウェイVIP – この仮想IPアドレスは、コールバック用にStoreFrontで構成されているものと同じである必要があります。

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、次に「**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、構成されたサーバーに到達可能であることを確認するための検証が行われます。また、Secure Private Accessサーバーに到達可能であることも確認されます。

構成の概要ページにエラーが表示された場合は、詳細については、[エラーのトラブルシューティング](#)を参照してください。これで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。



注:

- 環境をセットアップした後、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する管理者は、完全な権限を付与されます。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。管理者の一覧は、[設定 > 管理者](#)から表示できます。
- 管理者グループを追加することもできます。これにより、そのグループ内のすべての管理者にアクセスが有効になります。

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をセットアップする

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」を選択し、「次へ」をクリックします。

「データベース構成」([/ja-jp/citrix-secure-private-access/media/spaop-firsttime-select-site1a.png](#))

2. 「**SQL Server ホスト**」に、サーバー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 にすでに存在することを確認してください。データベースアドレスは、次のいずれかの形式で指定できます。

- サーバー名
- サーバー名\インスタンス名
- サーバー名,ポート番号

詳細については、「」([/ja-jp/citrix-virtual-apps-desktops/technical-overview/databases.html](https://ja-jp.citrix-virtual-apps-desktops/technical-overview/databases.html))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、指定されたサイトがデータベースに存在することを確認します。

「データベース構成」([/ja-jp/citrix-secure-private-access/media/spaop-databse-config-1a.png](https://ja-jp/citrix-secure-private-access/media/spaop-databse-config-1a.png))

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. 「**保存**」をクリックします。

構成検証チェックは、SQL データベースサーバーが構成されていること、および Secure Private Access サーバーに到達可能であることを確認するために実行されます。

次のステップ

- [ネットスケーラー ゲートウェイを構成する](#)
- [アプリケーションを構成する](#)
- [アプリケーションのアクセスポリシーを構成する](#)

ネットスケーラー ゲートウェイ の設定

重要:

これらの変更を適用する前に、NetScaler のスナップショットを作成するか、NetScaler の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。

新しいネットスケーラー ゲートウェイ を作成するには、`ns_gateway_secure_access.sh` を使用します。既存のネットスケーラー ゲートウェイ 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*`。

注:

- 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改行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、それは改行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。

3. 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)。
4. アップロードしたスクリプトを実行可能にします。これには `chmod` コマンドを使用します。

```
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。



6. 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証明書については、NetScalerで名前を指定する必要があります。

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



7. NetScaler CLIに切り替えて、新しいファイルから生成されたNetScalerコマンドをバッチコマンドで実行します。例えば、`batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output`

NetScalerはファイル内のコマンドを1つずつ実行します。コマンドが失敗した場合でも、次のコマンドに進みます。

リソースが存在する場合、またはステップ6で入力されたパラメータのいずれかが正しくない場合、コマンドは失敗する可能性があります。

8. すべてのコマンドが正常に完了したことを確認してください。

注:

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、パラメータのいずれか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、最初から構成をやり直すことをお勧めします。

既存の構成を持つ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Secure Private Accessをサポートすることもできます。ただし、スクリプトは以下を更新しません。

- 既存のネットスケーラー ゲートウェイ仮想サーバー
- NetScaler Gatewayにバインドされている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。

ネットスケーラー ゲートウェイ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際は、以下のパラメーター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。

tcpProfileName: nstcp_default_XA_XD_profile deploymentType: ICA_STOREFRONT icaOnly: OFF

例を挙げます:

仮想サーバーを追加するには:

```
`add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443  
-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`
```

仮想サーバーパラメーターの詳細については、[vpn-sessionAction](#)を参照してください。

ネットスケーラー ゲートウェイ 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際は、以下のパラメーター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。

- `transparentInterception`: オフ
- `SSO`: ON
- `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に置き換える
- `ClientChoices`: オフ

- `ntDomain` : mydomain.com - シングルサインオンに使用されます
- `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。これは、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)
- `clientlessVpnMode` : ON
- `clientlessModeUrlEncoding` : 透過
- `SecureBrowse` : 有効
- `Storefronturl` : "https://storefront.mydomain.com"
- `sfGatewayAuthType` : ドメイン

例を挙げます:

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、<https://developer-docs.netscaler.com/ja-jp/adc-command-reference-int/13-1/vpn/vpn-sessionaction>を参照してください。

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アプリを列挙して起動するためにも使用できます。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™ 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。

- ネットスケーラー ゲートウェイでのセキュア チケット オーソリティの構成
- FAQ: シトリックス セキュア ゲートウェイ / ネットスケーラー ゲートウェイ セキュア チケット オーソリティ

スマートアクセスタグのサポート

以下のバージョンでは、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バージョンでこの機能を有効/無効にするには、

`ns_vpn_enable_spa_onprem` または `ns_vpn_disable_spa_onprem` のトグルを使用します。

- 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
```

- 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、「NetScaler Gateway でカスタムタグ (SmartAccess タグ) を構成する」を参照してください。

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、単一のスクリプトではカバーできない無限のNetScaler構成が存在する可能性があります。

- NetScaler Gateway で 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、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 アドレスを持つ新しい 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のアップロード

パブリックゲートウェイがSecure Private Accessマシンから到達できない場合、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. 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. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, 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>
```

コンテキストタグを設定する

Secure Private Accessプラグインは、デバイスプラットフォームとOS、インストールされているソフトウェア、地理的位置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、アクセスポリシーにコンテキストタグ付きの条件を追加できます。Secure Private Accessプラグイン上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、ヘッダーとして（新しいロジック）、またはGatewayへのコールバックによってスマートアクセスタグを受信できます。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。

注記:

Secure Private Accessプラグインは、NetScaler Gatewayで構成できる従来の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、次の大まかな手順が含まれます。

1. 従来のゲートウェイ事前認証ポリシーを構成する
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

従来のゲートウェイ事前認証ポリシーを構成する

1. **NetScaler Gateway > ポリシー > 事前認証**に移動し、次に**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. **要求アクション**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、1つのアクションでアクセスを許可し、別の1つのアクションでアクセスを拒否します。



4. 必要なフィールドに詳細を入力し、**作成**をクリックします。
5. **式**で、式を手動で入力するか、式エディターを使用してポリシーの式を構築します。

式の例(/ja-jp/citrix-secure-private-access/media/spaop-expression-sample.png)

次の図は、Windows 10 OSをチェックするために構築された式の例を示しています。

式エディター(/ja-jp/citrix-secure-private-access/media/spaop-policy-exp-editor.png)

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. **ネットスケーラー ゲートウェイ > 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、**種類の選択**で**要求**を選択します。

ポリシーの種類(/ja-jp/citrix-secure-private-access/media/spaop-request-type.png)

5. ポリシー名とポリシー評価の優先度を選択します。
6. バインドをクリックします。

ポリシーのバインド (/ja-jp/citrix-secure-private-access/media/spaop-preauth-policy-binding.png)

CLIを使用してカスタムタグを構成する

NetScaler CLIで以下のコマンドを実行して、事前認証ポリシーを作成およびバインドします。

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た場合」セクションで、「**条件の追加**」をクリックし、「**コンテキストタグ**」、「**すべてに一致**」を選択してから、コンテキストタグ名（例: `Windows10`）を入力します。

参考文献

- [アプリケーションのアクセスポリシーを構成する。](#)
- [スマートアクセス用タグのサポート。](#)

ストアフロントを構成する

Secure Private AccessがStoreFrontと共存している場合、StoreFrontでのSecure Private Accessの構成は、初回セットアップウィザードによって自動的に行われます。

ただし、Secure Private AccessがStoreFrontと共存していない場合は、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管理コンソールからスクリプトをダウンロードします (設定 > 統合)。
2. 構成変更を行う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。

ダウンロードした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. コマンド `./ConfigureStorefront.ps1` を使用して、PowerShell 64ビットインスタンスで管理者としてスクリプトを実行します。

- その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スクリプトの実行ポリシーをUnrestrictedまたはBypassに設定する必要があります。
- StoreFrontがクラスターとして構成されている場合、スクリプトは構成を他のStoreFrontサーバーにも伝播します。

StoreFrontがSecure Private Access設定で構成されると、Secure Private Accessプラグインの構成がStoreFront管理UI (デリバリーコントローラーの管理画面) に表示されます。

StoreFrontスクリプトは、Citrix Virtual Apps and Desktops™デリバリーコントローラーに同じものが構成されている場合、Secure Private Accessの集約グループ設定を自動的に構成します。デフォルトでは、スクリプトはSecure Private Accessをすべてのユーザーに対して構成します (ユーザーマッピングとマルチサイト集約構成 > 構成済み)。

重要:

- Secure Private AccessのStoreFrontを構成するには、Secure Private Access管理UIからダウンロードしたStoreFrontスクリプトのみを使用することをお勧めします。UIではStoreFrontに必要なすべての構成が網羅されていないため、StoreFront管理UIからSecure Private Accessを構成しないでください。必要なすべての構成を完了するには、スクリプトを実行する必要があります。
- 1つのSecure Private Accessサイトは、複数のStoreFront展開（同じStoreFront上の別のストア、または異なるStoreFront展開）でも構成できます。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、**設定 > 統合** ページからのStoreFront自動構成は機能しません。自動構成は初回セットアップ時のみ行われます。**設定** ページから新しいストア構成が追加された場合、StoreFrontスクリプトをダウンロードし、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2308以前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には以下の既知の問題があります。

- セキュアプライベートアクセスプラグインの種類はゼンモバイルとして表示されます。
- セキュア プライベート アクセス サーバーのURLは表示されません。
- セキュア プライベート アクセス ポートは常に80と表示されます。



StoreFrontバージョン2311以降を使用している場合

StoreFrontバージョン2311以降では、Citrix Workspace™ for Web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そのアプリの起動をサポートしていないためです。

アプリケーションを構成する

1. アプリが常駐する場所を選択します。

- 外部アプリケーションの場合は、社内ネットワーク外。
- 内部アプリケーションの場合は、社内ネットワーク内。

2. アプリの詳細セクションに次の詳細を入力し、次へをクリックします。



- **アプリ名** – アプリケーションの名前。
- **アプリの説明** - アプリの簡単な説明。この説明は、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 `KEYWORDS: <keyword_name>` の形式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、「[含まれるキーワードでリソースをフィルタリングする](#)」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ことも、Citrix Workspace UIの既存のカテゴリを使用することもできます。WebアプリまたはSaaSアプリのカテゴリを指定すると、そのアプリは特定のカテゴリの下でWorkspace UIに表示されます。
 - カテゴリ/サブカテゴリは管理者によって構成可能であり、管理者はすべてのアプリに新しいカテゴリを追加できます。
 - 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。例: Business And Productivity\Engineering。また、このフィールドでは大文字と小文字が区別されません。管理者は正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UIの名前とアプリカテゴリフィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとしてリストされます。例えば、アプリカテゴリフィールドに「ビジネスおよび生産性」カテゴリを誤って「Business And productivity」と入力した場合、Citrix Workspace UIには「Business And productivity」という新しいカテゴリが、「Business And Productivity」カテゴリに加えてリストされます。

- **アプリのアイコン – アイコンの変更**をクリックして、アプリのアイコンを変更します。アイコンファイルのサイズは128x128ピクセルである必要があり、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** - アプリをユーザーに表示しない場合は、このオプションを選択します。
- **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追加できます。 **アプリケーションをお気に入りへ自動追加** – 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。
- **ユーザーがお気に入りから削除することを許可** – このオプションをクリックすると、アプリのサブスクライバーが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なります。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に黄色の星アイコンが表示されます。
- **ユーザーがお気に入りから削除することを許可しない** – このオプションをクリックすると、サブスクライバーが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。

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付きの星アイコンが表示されます。

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した場合、これらのアプリはCitrix Workspaceのお気に入りリストから手動で削除する必要があります。Secure Private Accessコンソールからアプリが削除されても、StoreFront™からアプリが自動的に削除されることはありません。アプリの接続性: Webアプリの場合は「Internal」を、SaaSアプリの場合は「External」を選択します。

3. 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構成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。

次のステップ

[アプリケーションのアクセスポリシーを構成する](#)

アプリケーションのアクセスポリシーを構成する

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を有効にできます。

1. をクリックします。

ポリシーの作成(/ja-jp/citrix-secure-private-access/media/spaop-tcp-udp-policy-old.png)

2. で、アクセスポリシーを適用するアプリを選択します。
3. で、アプリへの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。
 - : 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。
 - : 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がアクセスを許可されます。
4. をクリックして、コンテキストタグに基づいて別の条件を追加します。これらのタグは NetScaler® Gateway から派生しています。
5. 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。
6. 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いずれかのアクションを選択します。

を選択すると、次の制限を選択できます。

制限(/ja-jp/citrix-secure-private-access/media/spaop-add-policy-restrictions.png)

- **クリップボードアクセスを制限する:** アプリとシステムクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- **印刷を制限する:** Citrix Enterprise Browser 内からの印刷機能を無効にします。
- **ダウンロードを制限する:** アプリ内からのユーザーのダウンロード機能を無効にします。
- **アップロードを制限する:** アプリ内でのユーザーのアップロード機能を無効にします。

- **透かしを表示する:** 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表示します。
- **キーロギングを制限する:** 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上で暗号化されます。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でアプリ保護ポリシーが有効になっており、ユーザーがOffice 365のWordドキュメントを編集した場合、すべてのキーストロークはキーロガー上で暗号化されます。
- **画面キャプチャを制限する:** 任意の画面キャプチャプログラムまたはアプリを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとする、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。

7. **ポリシー名に、ポリシーの名前を入力します。**
8. **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、アクセスポリシーページからトグルスイッチを使用して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順位番号が割り当てられます。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。

値が小さい優先順位が最も高く、最初に評価されます。このポリシーが定義された条件と一致しない場合、次に優先順位番号が小さい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。

次のステップ

クライアントマシン (Windows および macOS) から構成を検証します。

例

エンドユーザーフロー

管理者がOffice365アプリをウォーターマークと印刷制限でエンドユーザー向けに構成したと仮定します。このとき、エンドユーザーがOffice365アプリにアクセスすると、ウォーターマークと印刷制限がアプリに適用される必要があります。

エンドユーザーは、Office365アプリにアクセスするために次の手順を実行する必要があります。

1. シトリックス ワークスペース™ アプリからストアフロント™ ストアにアクセスします。
2. ストアにログオンします。
3. **Apps**タブをクリックし、**Office365**アプリケーションをクリックします。

エンドユーザーは、Office365アプリケーションが起動し、ウォーターマークが含まれていることを確認する必要があります。また、エンドユーザーがOffice365アプリケーションからデータを印刷しようとする、印刷制限メッセージがユーザーに表示される必要があります。



注：

管理者は、仮想デスクトップおよび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。詳細については、「[Citrix WorkspaceアプリへのストアURLの追加](#)」を参照してください。

セキュアプライベートアクセスとWeb Studioの統合

Citrix Secure Private Access™ は、ユーザーが Web Studio を介してサービスにシームレスにアクセスできるように、Web Studio コンソールにも統合されています。

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 連携を有効にするには、次の手順を実行します。

1. 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、Citrix ウェブスタジオ をインストールします。
2. 画面の指示に従ってインストールを完了します。コントローラーアドレスの入力を求められたら、DDC FQDN をコントローラーアドレスとして入力します。
3. インストールが正常に完了したら、C:\Program Files\Citrix\Web Studio\Site\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を使用した場合は、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ます。

JSON ファイル(/ja-jp/citrix-secure-private-access/media/spaop-spa-jason-file.png)

1. 「SpaServer」を、お客様の Secure Private Access プラグインの完全修飾ドメイン名に置き換えます。
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。

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

オンプレミス版の Secure Private Access 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提供するために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。

NetScaler Gateway バージョン 13.0 または 13.1 ビルド 48.47 以前を使用している場合は、Secure Private Access を StoreFront と共存させることをお勧めします。

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、「[Secure Private Access サイトのセットアップ](#)」を参照してください。
- Secure Private Access サイトに必要な数のクラスターノードを追加します。詳細については、「[既存のサイトに参加して Secure Private Access をセットアップする](#)」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。

ロードバランサーの構成

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

- Secure Private Access サービス (管理者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。
- Secure Private Access サービスは HTTPS で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、SAN はロードバランサーサービスで構成する必要があります。
- 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用にカスタムの 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`

期待される応答:

```
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設定の詳細については、[基本的な負荷分散のセットアップ](#)を参照してください。

インストール後の設定を管理する

Secure Private Access をインストールした後、ページから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。

アプリケーションドメインのルーティングを管理する

Secure Private Access のセットアップ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、関連するすべてのドメインと、アプリトラフィックがどのようにルーティングされるか（外部または内部）が一覧表示されます。

1. > 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。

セキュア プライベート アクセス の 管理者を管理する

> ページから、管理者の一覧を表示したり、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。この管理者は、その後、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、そのグループ内のすべての管理者にアクセスを許可することもできます。

1. ページで、 をクリックします。
2. で、この管理者を追加するドメインを選択します。
3. 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. で、このユーザーに割り当てる権限タイプを選択します。

セットアップ後にStoreFront™またはNetScaler Gatewayサーバーの詳細を更新する

Secure Private Access をセットアップした後、「統合」タブから StoreFront および 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. 変更したい設定と同じ行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 で実行します。



ダッシュボードの概要

Secure Private Accessトラブルシューティングログダッシュボードには、アプリケーションの起動、アプリの列挙、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。

事前設定され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。ユーザーログをCSV形式でエクスポートできます。

フィルター（カテゴリと結果）を使用して、検索結果を絞り込むことができます。

ログ(/ja-jp/citrix-secure-private-access/media/spaop-logs.png)

検索フィールドの演算子と合わせて、次のパラメーターに基づいて検索を絞り込むこともできます。

- ユーザー名
- カテゴリ
- イベントタイプ
- 結果
- トランザクションID
- 詳細

ユーザーログおよび適用によるトップアクセスポリシーのグラフ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。
- !=: 指定された条件を含まないログ/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、検索フィールドで文字列 **Event-Type = DSAuth** を使用して、イベントタイプ「DSAuth」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、文字列 **User-Name ~ operator** 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、「local operator」、「admin operator」などです。

トランザクションIDを使用して、単一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ログに関連付けます。1つのアプリアクセス要求に対して、認証から始まり、アプリの列挙、そしてアプリアクセス自体へと、複数のログが生成されることがあります。これらすべてのイベントは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に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要求に関連するすべてのログを見つけることができます。

ログからコンテキストタグを表示する

詳細列の詳細を表示リンクは、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、ポリシーに関連付けられているコンテキストタグを表示します。

コンテキストタグ(/ja-jp/citrix-secure-private-access/media/spaop-context-tags.png)

一般的なエラーのトラブルシューティング

このトピックでは、Secure Private Access の設定中に発生する可能性のあるいくつかのエラーをリストします。

証明書エラー

データベース作成エラー

ストアフロントのエラー

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

セキュアプライベートアクセスサーバーに到達できません

証明書エラー

エラーメッセージ: 1つ以上のGateway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、パブリックなNetScaler® Gatewayアドレスを追加しようとしたときに、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 の設定時、または設定完了後に設定を更新する際に発生する可能性があります。

回避策: Citrix Virtual Apps and Desktops の場合と同様に、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:** データベースの作成に失敗しました

解決策: 自動ケースの場合 - マシンは、SQLサーバー上のデータベース内にテーブルを作成するために、READ、WRITE、UPDATE の権限を持っている必要があります。

- **エラーメッセージ:** データベースの作成に失敗しました: データベースが既に存在します。

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

- データベースの構成中に**自動構成**オプションが選択されている場合。

- 。管理者がデータベースを作成する場合、それは空のデータベースである必要があります。データベースが空でない場合、このエラーメッセージが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た場合。この場合、以前のインストールからのデータベースは削除されていません。

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セットアップすることを選択し（「データベースの構成」ページで「手動構成」を選択）、その後「自動構成」オプションに変更したが、同じサイト名を使用した場合。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既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、スクリプトを再度実行する必要があります。

- 。マシンに、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 権限がない。

解決策: マシンで適切な権限を有効にします。詳細については、「[データベースのセットアップに必要な権限](#)」を参照してください。

- **エラーメッセージ:** データベースの作成に失敗しました: 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ます。SQL Server のポートがファイアウォールで開いていること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、SQL Server に Secure Private Access マシンの ID (Domain\hostname\$) でログインが作成されているか確認します。
- 。リモート SQL Server を使用している場合は、マシン ID に適切な役割（システム管理者役割）が割り当てられていることを確認します。
- 。ローカルSQLサーバーを使用している場合（インストーラーからではない場合）、NT AUTHORITY\SYSTEMユーザーにログインが作成されている必要があるか確認してください。

ストアフロント™ の障害

- **エラーメッセージ:** StoreFront エントリの作成に失敗しました: <Store URL>

StoreFrontエントリが表示されない場合は、**設定**タブから更新してください。ウィザードを使用してSecure Private Accessを設定した後、**設定**タブからStoreFront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URLをメモしてください。

解決策:

- a. **設定**をクリックし、次に**統合**タブをクリックします。
 - b. **StoreFrontストアURL**で、StoreFrontエントリが表示されない場合は追加します。
- **エラーメッセージ:** StoreFront エントリの構成に失敗しました: `<Store URL>`

解決策:

- a. PowerShellの実行ポリシーに制限があ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。
- b. 制限されている場合は、これをバイパスし、StoreFront構成スクリプトを手動で実行する必要があります。
- c. **設定**をクリックし、次に**統合**タブをクリックします。
- d. **StoreFrontストアURL**で、エラーが発生したStoreFront URLエントリを特定します。
- e. 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インストールが存在するマシンで、このPowerShellスクリプトを管理者権限で実行します。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 > store > 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てください。

- **エラーメッセージ:** 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をセットアップした後、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URLをメモしてください。

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。

- a. **設定**をクリックし、次に**統合タブ**をクリックします。
- b. **StoreFrontストアURL**で、エラーが発生したStoreFront URLエントリを特定します。
- c. 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インストールが存在するマシンで、このPowerShellスクリプトを管理者権限で実行します。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、管理者権限を持つWindows x64互換のPowerShellウィンドウを開き、その後ConfigureStorefront.ps1を実行してください。StoreFrontスクリプトは、Windows PowerShell (x86)とは互換性がありません。

- **Error message:** "Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Exceptions.RegistryKeyNotFoundException' was thrown." while running StoreFront script using PowerShell.

このエラーは、StoreFrontスクリプトがx86互換のPowerShellウィンドウで実行され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ウィンドウを開き、次に `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: ゲートウェイエントリの作成に失敗しました: `<Gateway URL>` または コールバックゲートウェイエントリの作成に失敗しました: `<Callback Gateway URL>`

解決策:

失敗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をメモしてください。ウィザードを使用してSecure Private Accessをセットアップした後、**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、次に**統合タブ**をクリックします。

2. 失敗が発生した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、および仮想IPアドレスを更新します。

Secure Private Accessサーバーへの接続に失敗しました

エラーメッセージ: IISプールの更新に失敗しました。IISプールの再起動に失敗しました

解決策:

Internet Information Services (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開始され、実行されていることを確認します。

- セキュア プライベート アクセス 実行時プール
- セキュアプライベートアクセス 管理プール

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: 接続チェックに失敗しました

データベース接続チェックは、複数の理由により失敗する可能性があります。

- ファイアウォールが原因で、Secure Private Accessプラグインホストマシンからデータベースサーバーに到達できません。

解決策: ファイアウォールでデータベースポート（デフォルトポート1433）が開いているか確認してください。

- 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」([/ja-jp/citrix-secure-private-access/2311/spa-onprem-troubleshooting#sql-database-permissions-for-secure-private-access](https://ja-jp.citrix-secure-private-access/2311/spa-onprem-troubleshooting#sql-database-permissions-for-secure-private-access))を参照してください。

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

エラーメッセージ: インストール後の構成が「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...」というエラーで失敗します。

解決策:

- 設定ツールを使用して、ゲートウェイ公開証明書をSecure Private Accessデータベースに手動でアップロードします。
- 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。
- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool")
- 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の失敗

StoreFront URLまたはNetScaler Gateway URLに末尾のスラッシュ (/) が含まれている場合、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。詳細については、[セットアップ後にStoreFrontまたはNetScaler Gatewayサーバーの詳細を更新する](#)を参照してください。

その他の問題

セキュア プライベート アクセス診断サポートバンドルの作成

Secure Private Access診断サポートバンドルを作成するには、次の手順を実行します。

- 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。
- セキュアプライベートアクセス インストールフォルダーの配下にある Admin\AdminConfigTool という名前のフォルダーヘディレクトリを移動してください (例: cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool")。
- 次のコマンドを実行します。

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

Secure Private Access の SQL データベースに対するアクセス権限

データベースを自動的に作成するには、Secure Private Accessプラグインホストマシンがデータベースに接続し、データベーススキーマを作成する権限を持っている必要があります。

リモートデータベース:

リモート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. `CitrixAccessSecurity<Site Name>` という名前の構文で空のデータベースを作成します。ここで、`<Site Name>` は Secure Private Access サイト名です。(例: `CitrixAccessSecuritySPA`)。

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

2. Secure Private Access仮想マシンのマシンIDのSQLサーバーログインを作成します。たとえば、Secure Private Accessブローカーマシン名がHOST1で、マシンドメインがDOMAIN1の場合、マシンIDは「DOMAIN1\HOST1\$」です。ログインがすでに作成されている場合は、この手順を無視できます。

```
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見つけることができます。

```
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. `CitrixAccessSecurity<Site Name>` という名前の構文で空のデータベースを作成します。ここで、`<Site Name>` はSecure Private Accessサイト名です (例: `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。ログインがすでに作成されている場合は、この手順を無視できます。

```
USE CitrixAccessSecurity<SiteName>
```

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

3. 「NT AUTHORITY\SYSTEM」という名前のユーザーに db_owner ロールを割り当てます。

```
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、ダウンロードされたデータベーススクリプトがマシンIDに権限を追加します。

トラブルシューティングログの保持

「トラブルシューティングログ」ページのログは、Secure Private Accessデータベースに90日間保存されます。ログの総数が多すぎる場合（たとえば100,000件を超える場合）、90日より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。また、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をカスタマイズする

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ファイルで構成できます。ログの経過日数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ファイルの次のエントリを変更します。

appsettings.jsonファイルの例 (サンプル):

```
"TroubleshootingLogs": {  
  
  "CleanupPeriodInHours": 12,  
  
  "CleanupDataOlderThanDays": 90,  
  
  "CleanupOldestDataIfEntriesCountAbove": 100000  
  
}
```

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構成します。

- ログを7日間のみ保持するには、`CleanupDataOlderThanDays` を7に設定します。
- 日数ベース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。

- これらの設定の両方が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、ログは永続的に保持されます。
 - `CleanupDataOlderThanDays` または `CleanupOldestDataIfEntriesCountAbove` の両方を0に設定すること、あるいは `CleanupPeriodInHours` を0に設定することは、100%のディスク使用率の問題を引き起こす可能性があるため、推奨されません。
 - ログのクリーンアップ頻度は、`CleanupPeriodInHours` エントリを変更することでも変更できます。

注:

Secure Private Accessがクラスターとして展開されている場合、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、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

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秒ごとに実行されます。

注:

テレメトリデータのクリーンアップをトリガーするには、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 のインストールマシン上の、AdminサービスとRuntimeサービスのインストールフォルダ内に保存されます。CDFログは、各ファイルに10MBのサイズ制限が適用された.csvファイルに配置されます。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、その後、新しいCDFログファイルを作成するためのスペースを確保するために最も古いファイルを削除します。RuntimeサービスはAdminサービスと同じように動作しますが、一度に最大600個のより多くのファイルを保持できます。

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、AdminサービスとRuntimeサービスのインストールフォルダにあるappsettings.jsonファイルを通じて構成できます。ファイルのサイズとカウントの制限を変更するには、appsettings.jsonファイルで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、各Secure Private AccessインストールマシンでCDFクリーンアップ用のappsettings.jsonファイルを更新します。

セキュアプライベートアクセスをアンインストール

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. Select **Citrix Virtual Apps and Desktops™ 7 2308 – Secure Private Access**.
2. アンインストールをクリックします。
3. 画面の指示に従って、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ている場合は、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。

StoreFrontScripts zip ファイルをダウンロードするには、次の手順に従います。

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、次に**統合タブ**をクリックします。
3. StoreFront ストア URL セクションで、**スクリプトのダウンロード**をクリックします。

StoreFront ストア構成からセキュアプライベートアクセスプラグインを削除する

Secure Private Access をアンインストールした後、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. Download the StoreFrontScripts.zip file.
3. StoreFrontScripts.zip を指定のフォルダーに解凍します。
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
```

セキュア プライベート アクセス 2311 と旧バージョンの互換性

Secure Private Access 2311 はレガシーバージョンと互換性がありません。NetScaler Gateway は、以前に説明した「[NetScaler Gateway の構成](#)」に従って、新しいスクリプトを使用して構成する必要があります。Secure Private Access のレガシーバージョンでは、Citrix Virtual Apps and Desktops デリバリーコントローラーでの構成は不要です。

レガシーバージョンから 2311 に移行する最善の方法は、次のものをクリーンアップすることです。

- ウェブ/ソース アプリからのシトリックス バーチャル アプリケーションズ アンド デスクトップ デリバリー コントローラー
- Citrix StoreFront™ をデフォルト構成に更新するか、StoreFront に新しいストアを作成します
- ネットスケaler® ゲートウェイ

シトリックス バーチャルアップス アンド デスクトップス™ デリバリーコントローラーのクリーンアップ

Citrix Virtual Apps and Desktops デリバリーコントローラーで作成された Secure Private Access アプリケーションは、手動または PowerShell スクリプトを使用して削除できます。

手動:

1. シトリックス スタジオ または シトリックス ウェブスタジオ を開きます。
2. **アプリケーション**をクリックします。
3. アプリを選択し、右クリックして、**削除**を選択します。

スクリプトの使用:

1. 次のコマンドを実行して、現在の Secure Private Access アプリを取得します。

```
Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"
```

詳細については、[Remove-BrokerApplication](#)を参照してください。

2. アプリケーションを確認したら、次のコマンドを実行して削除します。

```
Get-BrokerApplication -Description "KEYWORDS:SPAENABLED" | Remove-BrokerApplication
```

シトリックス ストアフロントのクリーンアップ

新しいStoreFrontストアを作成するか、既存のストアをクリーンアップすることができます。

- 新しいStoreFrontストアを作成する: レガシーバージョン用に作成された既存のStoreFrontストアは2311と互換性がないため、Secure Private Access 2311用に新しいStoreFrontストアを作成する必要があります。これは、構成関連の問題を回避するための推奨オプションです。
- 既存のStoreFrontストアをクリーンアップする: StoreFront上の既存のストアは、手動またはスクリプトを使用してクリーンアップできます。ただし、オンプレミスのSecure Private Accessを2311に移行するための最良のオプションは、StoreFrontに新しいストアを作成することです。

手動:

1. Find and remove policy.json (e.g C:
\\inetpub\\wwwroot\\Citrix\\Store\\Resources\\SecureBrowser\\policy.json).
2. SecureBrowser という名前のフォルダー（例えば、C:
\\inetpub\\wwwroot\\Citrix\\Store\\Resources\\SecureBrowser のような場所にあるもの）と、Resources という名前のフォルダー（例えば、C:\\inetpub\\wwwroot\\Citrix\\Store\\Resources のような場所にあるもの）をシステム内で探し出し、それらを完全に削除してください。
3. Remove the "route" node from web.config (you can find it in C:\\inetpub\\wwwroot\\Citrix\\Store\\ with the name "webSecurePolicy" routing to the URL "Resources\\SecureBrowser\\policy.json").
4. 変更を適用するには、インターネットインフォメーションサービス (IIS) マネージャー上の既定のWebサイト コンソールを再起動します。

スクリプトを使用する:

1. <<https://www.citrix.com/downloads/citrix-secure-private-access/>> からスクリプトをダウンロードします。
2. スクリプトをStoreFrontマシンにアップロードします。
3. PowerShellでスクリプトを管理者として実行します。
4. ストア名を入力します。

スクリプトは、C:\inetpub\wwwroot\Citrix\Store\Resources フォルダー、サブフォルダー、およびファイルを削除し、web.config ファイルを更新します。

5. 変更を適用するには、**Internet Information Service (IIS) マネージャー上の既定のWebサイト** コンソールを再起動します。

ネットスケーラー ゲートウェイ のクリーンアップ

ネットスケーラー ゲートウェイ 仮想サーバー

レガシーバージョン用に作成されたNetScaler Gateway仮想サーバーは、Secure Private Access 2311で再利用できます。

- 既存のNetScaler Gatewayを更新するには、「既存のNetScaler Gatewayを更新する」を参照してください。
- 新しいNetScaler Gatewayを構成するには、「NetScaler Gatewayを構成する」を参照してください。

セッションポリシーとアクション

レガシーバージョン用に作成されたセッションポリシーとアクションは、Secure Private Access 2311で再利用できます。

- 既存のNetScaler Gatewayセッションポリシー/アクションを更新するには、「[NetScaler Gatewayセッションアクション](#)」を参照してください。
- 新しいNetScaler Gatewayを構成するには、「[NetScaler Gatewayを構成する](#)」を参照してください。

スクリプトは、完全に構成されたセッションポリシー/アクションも作成します。

承認ポリシー

レガシーバージョン向けにNetScaler Gatewayで作成された承認ポリシーは、Secure Private Access 2311ポリシーと競合し、フローを中断させる可能性があります。

承認ポリシーをクリーンアップするには、次の操作を実行できます。

- ネットスケーラー ゲートウェイでデフォルトグループとして使用されている認証および承認グループから、承認ポリシーを手動でバインド解除します。この場合、ポリシーは再利用できます。
- 承認ポリシーを削除します。

サードパーティ通知

オンプレミス向け シトリックス セキュア プライベート アクセス