



# Citrix Secure Private Access-オンプレミ ス

# Contents

|                                             |    |
|---------------------------------------------|----|
| 新機能                                         | 5  |
| 2023年10月                                    | 5  |
| シトリックス セキュア プライベート アクセス™ オンプレミス版 – プレビュー    | 5  |
| 既知の問題                                       | 6  |
| ドメインコントローラーの構成                              | 6  |
| ネットスケーラー® ゲートウェイ                            | 6  |
| RfWeb / Web用ワークスペース                         | 6  |
| アプリケーションアイコン                                | 7  |
| 管理者管理                                       | 7  |
| アップグレード                                     | 7  |
| ストアフロント™                                    | 7  |
| ログ                                          | 7  |
| セキュア プライベート アクセス インストーラー                    | 8  |
| 管理コンソールへの SSO                               | 8  |
| 次のステップ                                      | 9  |
| 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                  | 10 |
| セキュアプライベートアクセスの設定                           | 11 |
| 前提条件                                        | 11 |
| 新しいサイトを作成して Secure Private Access をセットアップする | 11 |
| ステップ 1: Secure Private Access サイトをセットアップする  | 11 |
| ステップ 2: データベースの構成                           | 12 |
| ステップ3: ストアフロントとネットスケーラー ゲートウェイ サーバーを統合する    | 13 |
| ステップ4: 構成の概要                                | 14 |
| 既存のサイトに参加してSecure Private Accessをセットアップする   | 14 |
| 次のステップ                                      | 15 |
| ネットスケーラー ゲートウェイ を構成する                       | 16 |

|                                                     |    |
|-----------------------------------------------------|----|
| 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       | 17 |
| ネットスケラー ゲートウェイ仮想サーバーの設定                             | 18 |
| ネットスケラー ゲートウェイ セッションアクション                           | 18 |
| ICA®アプリとの互換性                                        | 19 |
| スマートアクセスタグのサポート                                     | 20 |
| 既知の制限事項                                             | 20 |
| 公開ゲートウェイ証明書のアップロード                                  | 21 |
| アプリケーションの構成                                         | 22 |
| 次のステップ                                              | 23 |
| アプリケーションのアクセス ポリシーを構成する                             | 24 |
| アクセスポリシーの優先度                                        | 25 |
| 次のステップ                                              | 25 |
| エンドユーザーフロー                                          | 26 |
| セキュアプライベートアクセス統合とウェブスタジオ統合                          | 27 |
| インストール後の設定管理                                        | 28 |
| アプリケーションドメインのルーティングを管理する                            | 28 |
| セキュア プライベート アクセス の管理者の管理                            | 28 |
| 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 | 28 |
| ダッシュボードの概要                                          | 30 |
| ログからコンテキストタグを表示                                     | 31 |
| エラーのトラブルシューティング                                     | 32 |
| 証明書エラー                                              | 32 |
| データベース作成エラー                                         | 32 |
| StoreFront™ で発生する問題                                 | 33 |
| 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                         | 35 |
| 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                          | 35 |
| データベース接続チェックの失敗                                     | 36 |
| 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                   | 36 |

|                                                        |    |
|--------------------------------------------------------|----|
| 認証に関する問題                                               | 36 |
| その他の項目                                                 | 37 |
| 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                            | 37 |
| セキュアプライベートアクセス用SQLデータベース権限                             | 37 |
| セキュア プライベート アクセスのアンインストール                              | 39 |
| ストアフロントの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                | 39 |
| セキュア プライベート アクセス 2308 とレガシーバージョンの互換性                   | 41 |
| 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<br>リーンアップ | 41 |
| シトリックス ストアフロントのクリーンアップ                                 | 42 |
| ネットスケーラー ゲートウェイ のクリーンアップ                               | 43 |
| ネットスケーラー ゲートウェイ 仮想サーバー                                 | 43 |
| セッションポリシーとアクション                                        | 43 |
| 承認ポリシー                                                 | 43 |
| サードパーティ通知                                              | 44 |

# 新機能

---

## 2023年10月

### シトリックス セキュア プライベート アクセス™ オンプレミス版 – プレビュー

Citrix Secure Private Access for オンプレミスがプレビュー版として利用可能になりました。

Secure Private Access オンプレミスソリューションには、Secure Private Access サービスと同様のロックアンドフィールドを持つフルサービスの管理コンソールUIが含まれています。詳細については、Secure Private Access for オンプレミス – プレビューを参照してください。

# 既知の問題

---

Citrix Secure Private Access™ オンプレミスソリューションには、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

- 同じフォレスト内または異なるフォレスト間の片方向信頼はサポートされていません。Secure Private Access オンプレミスソリューションは、以下の両方の条件が満たされている場合、機能しません。
  - Secure Private Access オンプレミス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。
  - マシンのドメインからユーザーのドメインへの信頼が構成されていない。
- sAMAccountName と UPN が異なる場合、列挙は失敗します。

## ネットスケラー® 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。
- `ns_vpn_enable_spa_onprem` トグルが有効になっている。

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 / Workspace for web 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って）にのみ反映されます。
- 認証が失敗するため、管理者ユーザーはデフォルトの「Domain Users」AD グループに属してはいけません。

## アップグレード

ビルド間のアップグレードはサポートされていません。オンプレミス版 Secure Private Access は、ビルド間のアップグレード時に既存のインストールを削除して再インストールするよう促します。

## 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 プラグインタイプが 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生成はサポートされていません。
- 管理者サービスとランタイムサービスのログフォルダーは削除してはいけません。これらのフォルダーが削除されると、Secure Private Access は再作成できません。

# セキュア プライベート アクセス インストーラー

SecurePrivateAccessSetup\_2308.exe を使用してセキュア プライベート アクセスをインストールできます。

1. [<https://www.citrix.com/downloads/citrix-early-access-release/>](https://www.citrix.com/downloads/citrix-early-access-release/) から Citrix Secure Private Access のインストーラーをダウンロードしてください。
2. ドメインに参加しているマシンで、できれば StoreFront™ がインストールされているのと同じマシンで、.exe を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。



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™**) には、Secure Private Access のショートカットも表示されていることを確認できます。



## 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は、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に限り、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。

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(/ja-jp/citrix-secure-private-access/2308/spa-onprem-configure-apps)
- アプリケーションのアクセスポリシーを構成する(/ja-jp/citrix-secure-private-access/2308/spa-onprem-configure-access-policies)

# 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. 「セキュアプライベートアクセス」のインストールフォルダーの配下にあります  
「Admin\AdminConfigTool」という名前のフォルダーへ、現在の作業ディレクトリを移動させるようにしてください。(例: cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool")。
3. 次のコマンドを実行します。

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

# セキュアプライベートアクセスの設定

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。どちらの場合でも、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(/ja-jp/citrix-secure-private-access/2308/spa-onprem-setup-spa#set-up-secure-private-access-by-creating-a-new-site)
- 既存のサイトに参加して Secure Private Access をセットアップする(/ja-jp/citrix-secure-private-access/2308/spa-onprem-setup-spa#set-up-secure-private-access-by-joining-an-existing-site)

## 前提条件

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

## 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。

サイトの選択(/ja-jp/citrix-secure-private-access/media/spaop-firsttime-select-site1.png)

サイトを作成することを選択した場合、セットアップでサイト名に対応するデータベースが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実行できます。

1. 「**SQL Server Host**」に、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**」に、Secure Private Accessサイトの名前を入力します。
3. 「**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、接続テストは失敗します。
- SQL Serverが利用可能でもデータベースが存在しない場合、接続テストは成功します。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に対して認証を行います。

### 自動構成:

- マシンIDに必要なデータベース権限がある場合にのみ、**自動構成**オプションを使用できます。
- 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、空であることを確認し、必要なデータベース権限が付与されてい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:

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、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。マシンに適切な権限を付与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：ストアフロントとネットスケーラー 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 – ネットスケーラー ゲートウェイ の URL**。例：  
`https://gateway.domain.com`。
- **Gateway Callback Address** – 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`。
- **Gateway 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. 「**Next**」をクリックし、次に「**Save**」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サーバー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、「[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も確認します。

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

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(/ja-jp/citrix-secure-private-access/2308/spa-onprem-configure-apps)
- アプリケーションのアクセスポリシーを構成する(/ja-jp/citrix-secure-private-access/2308/spa-onprem-configure-access-policies)

# ネットスケーラー ゲートウェイ を構成する

## 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 の構成を保存することをお勧めします。

1. `<https://www.citrix.com/downloads/citrix-early-access-release/>` 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 改行コード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` が表示された場合、それは改行コード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 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。そのためには `chmod` コマンドを使用します。

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

5. NetScaler シェルでアップロードしたスクリプトを実行します。

ネットスケーラーの構成 1(/ja-jp/citrix-secure-private-access/media/spaop-configure-netscaler1.png)

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。

ネットスケーラーの構成 2(/ja-jp/citrix-secure-private-access/media/spaop-configure-netscaler2.png)

7. NetScaler CLIに切り替えて、バッチコマンドを使用して新しいファイルから生成されたNetScalerコマンドを実行します。例: `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、または手順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

例示：

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に置き換えてください

- `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

例示:

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/adsc-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](#)
- [よくある質問: 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` を切り替えます。

- 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NetScaler構成が無限に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。

## 公開ゲートウェイ証明書のアップロード

公開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. 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>
```

# アプリケーションの構成

1. アプリが配置されてい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. アプリケーション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、ワークスペースで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。詳しくは、「[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。
- **アプリのカテゴリ** - 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、**アプリのカテゴリ**フィールドに入力されたカテゴリ名との間に不一致がある場合、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、正しいカテゴリ名である「Business and Productivity」を誤って「Business And productivity」と入力した場合、Citrix Workspace UIには、既存の「Business And Productivity」カテゴリに加えて、

「Business and productivity」という名称の新しいカテゴリが一覧表示されることになります。

- **アプリのアイコン** – アプリのアイコンを変更するには、**アイコンの変更**をクリックします。アイコンファイルのサイズは128x128ピクセルで、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さらに追加できます。**アプリケーションをお気に入りへ自動的に追加** – このオプションをクリックすると、Citrix Workspaceアプリでこのアプリが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の付いた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、次に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-add-policy.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:** 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:** 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:** 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:** 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:** 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:** 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:** 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た画面のキャプチャ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、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度

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度番号が割り当てられます。優先度は、アクセスポリシーのホームページで確認できます。

値が小さい優先度ほど優先順位が高く、最初に評価されます。このポリシーが定義された条件と一致しない場合、次に優先度番号が小さいポリシーが評価され、以下同様に続きます。

「**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) から設定を検証します。

例

# エンドユーザーフロー

管理者がエンドユーザー向けにOffice365アプリにウォーターマークと印刷制限を設定していると仮定します。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以下の手順を実行する必要があります。

1. Citrix Workspace™ アプリを使用してStoreFront™ ストアにアクセスします。
2. ストアにログインします。
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。

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づくはずですが、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はずですが。

エンドユーザーフロー1(/ja-jp/citrix-secure-private-access/media/spaop-enduser-flow-restrict-printing.png)

## 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統合とウェブスタジオ統合

---

Citrix Secure Private Access™はWeb Studioコンソールにも統合されており、ユーザーはWeb Studioを通じ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. シトリックスバーチャルアプリとデスクトップ™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、シトリックスWeb Studio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てください。



1. 「SpaServer」を、あなたのセキュアプライベートアクセスプラグインのFQDNに置き換えます。
2. Web Studioにログインします。

ウェブスタジオ (/ja-jp/citrix-secure-private-access/media/spaop-cvad-integration.png)

1. 左側のナビゲーションメニューで、**Secure Private Access** **<Preview>** 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。

# インストール後の設定管理

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。

## 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、アプリの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 の管理者の管理

> 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。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、そのグループ内のすべての管理者にアクセスを有効に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、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. 変更したい設定の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. 設定が有効であることを確認するために、更新アイコンをクリックします。

**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。

インストール後の設定(/ja-jp/citrix-secure-private-access/media/spaop-manage-settings-dayn.png)

# 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（CATEGORYとRESULT）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ともに、以下のパラメータ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上位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。

例えば、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。例えば、「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ログを関連付けます。1つのアプリケーションアクセス要求に対して、認証から始まり、アプリの列挙、そしてアプリケーションアクセス自体に至るまで、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、特定のアプリケーション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

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た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たコンテキストタグも表示します。

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

# 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 のセットアップ中に発生する可能性のあるエラーの一部をリストします。

「証明書エラー」 (/ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#certificate-errors) 「データベース作成エラー」 (/ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#database-creation-errors) 「StoreFront の障害」 (/ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#storefront-failures) 「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」 (/ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#public-gateway-callback-gateway-failures) 「Secure Private Access Server に到達できません」 (/ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#secure-private-access-server-not-reachable)

## 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。 **回避策:** Citrix Virtual Apps and Desktops の場合と同様に、Gateway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:** 自動の場合 - マシンは、SQL Server 上のデータベース内にテーブルを作成するための読み取り、書き込み、更新のアクセス許可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: データベースはすでに存在します。

このエラーメッセージは、次のいずれかのシナリオで発生する可能性があります。

- 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。このエラーメッセージは、データベースが空でない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。

- 。データベースを手動でセットアップすることを選択し（ ページで を選択）、スクリプトを使用してから、オプションに変更したが、同じサイト名を使用している場合。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 権限がありません。

**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:**

- 。お使いのマシンからデータベースのネットワーク接続を確認してください。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てください。
- 。リモート SQL Server を使用している場合は、マシンの ID に適切なロール (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 (インストーラーからではない) を使用している場合は、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。

## StoreFront™ で発生する問題

- **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、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 をセットアップした後、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. をクリックし、次に タブをクリックします。
- b. 「**StoreFront Store URL**」に、StoreFrontエントリが表示されてい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の実行ポリシー制限が適用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。
- b. 制限されている場合は、これをバイパスして、StoreFront構成スクリプトを手動で実行する必要があります。
- 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 Store URL」において、エラーが発生したStoreFront URLの項目を特定してください。
- 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。

「

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ます。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」: 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 Store 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 Store URL** にて、エラーが発生したストアフロントのURLを特定してください。
- c. このStore 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。

**注:**

ストアフロント パワーシェル スクリプトを実行するには、管理者権限でウィンドウズ x64互換のパワーシェル ウィンドウを開き、ConfigureStorefront.ps1を実行します。ストアフロント スクリプトはウィンドウズ パワーシェル (x86) と互換性がありません。

## 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: Gatewayエントリの作成に失敗しました: `<Gateway URL>` または Callback Gatewayエントリの作成に失敗しました: `<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をメモします。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. 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、および障害が発生した仮想IPアドレスを更新します。

## 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

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:**

1. 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、実行中であることを確認します。
  - セキュアプライベートアクセスランタイムプール
  - セキュアプライベートアクセス 管理プール

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。

- ファイアウォールにより、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:** 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](#) 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、ゲートウェイの公開証明書を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。
- 「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下にある「アドミン\アドミン コンフィグツール」フォルダーにディレクトリを変更します (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 /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl>  
<PublicGatewayCertificatePath>
```

## 認証に関する問題

Secure Private AccessランタイムサービスのIIS認証構成は、統合Windows認証 (IWA) がサポートされていないため、機能しない可能性があります。

## その他の項目

### 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下にある「アドミン\アドミン コンフィグツール」 フォルダーにディレクトリを変更します（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>
```

### セキュアプライベートアクセス用SQLデータベース権限

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. マシンIDにdb\_ownerロールを割り当てます。

```
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サーバー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”というユーザーに、`db_owner`という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はマシンIDに権限を追加します。

# セキュア プライベート アクセスのアンインストール

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. **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。

## ストアフロントの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. StoreFrontScripts.zip という名前のファイルをダウンロードしてください。
3. StoreFrontScripts.zip ファイルを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 2308 と レガシーバージョンの互換性

Secure Private Access 2308 は、レガシーバージョン (オンプレミス用 Secure Private Access V1.0 および V1.5) と互換性がありません。NetScaler Gateway の構成 で前述したように、NetScaler Gateway は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 2308 の Citrix Virtual Apps and Desktops デリバリーコントローラーでは、構成は不要です。

Secure Private Access オンプレミスレガシーバージョン (1.0 および 1.5) から 2308 への移行の最良の方法は、以下をクリーンアップすることです。

- Web/SaaS アプリからのシトリックス バーチャルアプリおよびデスクトップ 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 上に新しいストアを作成します
- ネットスケーラー® 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、手動で、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。

スクリプトを使用：

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2308と互換性がないため、Secure Private Access 2308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されるオプションです。
- 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2308に移行するための最良のオプションは、StoreFront上に新しいストアを作成することです。

### 手動:

1. policy.json という名前のファイルを検索し、見つかった場合は削除してください。例えば、C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json のような場所に存在することがあります。
2. 「セキュアブラウザ」フォルダー (例えば、C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser のようなパスにあります) および「リソース」フォルダー (例えば、C:\inetpub\wwwroot\Citrix\Store\Resources のようなパスにあります) を見つけて削除してください。
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** コンソール上の **既定の Web サイト** 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で管理者としてスクリプトを実行します。
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) Manager** 上のデフォルト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 (1.0 および 1.5) 向けに作成されたNetScaler Gateway仮想サーバーは、Secure Private Access 2308で再利用できます。

- 既存のNetScaler Gatewayを更新するには、[こちら](#)を参照してください。
- 新しいNetScaler Gatewayを構成するには、[こちら](#)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 (1.0 および 1.5) 向け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 2308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 session actions](#)を参照してください。
- 新しいネットスケーラー ゲートウェイを構成するには、[ネットスケーラー ゲートウェイの構成](#)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 (1.0 および 1.5) 用に NetScaler Gateway で作成された承認ポリシーは、Secure Private Access 2308 ポリシーと干渉し、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。

- NetScaler Gateway でデフォルトグループとして使用されている認証グループおよび承認グループから、承認ポリシーを手動でアンバインドします。この場合、ポリシーは再利用できません。
- 承認ポリシーを削除します。

# サードパーティ通知

---

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