



Citrix セキュア プライベート アクセス - オンプレミス

Contents

技術的な概要	7
コンポーネント	8
新機能	9
2024年12月	9
2023年2月	9
シトリックス セキュア プライベート アクセス™とディレクターの統合	9
ディレクターでセキュアプライベートアクセスユーザーセッションを表示	9
シトリックス セキュアプライベートアクセスとライセンスサーバーの統合	9
修正された問題	9
管理者管理	10
管理コンソール	10
既知の問題	10
ドメインコントローラーの構成	10
ネットスケーラー® ゲートウェイ	11
RfWeb / Web版ワークスペース	11
アプリケーションアイコン	11
アプリケーションの起動	11
アップグレード	11
ストアフロント™	12
ログ	12
管理コンソール	12
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	12
システム要件	14
前提条件	14
管理者アカウントの要件	16
通信ポート	16

参考文献	19
サイジングガイドライン	19
データベースストレージ要件	19
サーバー構成	20
トラフィックプロファイル	20
展開ガイドライン	21
その他のコンポーネント構成	22
インストールと構成	23
Secure Private Accessをインストールおよび管理するための管理者アカウント要件	23
セキュアプライベートアクセスのセットアップ	23
アプリケーションとアクセスポリシーの構成	24
セキュア プライベート アクセス インストーラー	24
管理コンソールへのSSO	25
次のステップ	26
セキュアプライベートアクセスを設定する	26
前提条件	26
新しいサイトを作成して Secure Private Access をセットアップする	26
ステップ 1: Secure Private Access サイトをセットアップする	26
ステップ2: データベースの構成	27
ステップ3: サーバーの統合	28
ステップ4: 構成の概要	29
既存のサイトに参加してSecure Private Accessをセットアップする	30
HTTP2設定を無効にする	31
マルチドメイン環境	31
サービスアカウントを構成する	32
次のステップ	32
コンポーネント	32
ネットスケーラー ゲートウェイ	33

既存の構成を持つネットスケーラー ゲートウェイでセキュア プライベート アクセスを構成する	35
ICA®アプリとの互換性	38
スマートアクセスタグのサポート	38
公開ゲートウェイ証明書をアップロードする	40
既知の制限事項	40
コンテキストタグを構成する	41
ストアフロント	43
StoreFrontバージョン2308以前を使用している場合	44
StoreFrontバージョン2311以降を使用している場合	44
ディレクター	44
ディレクター設定ツールを使用して、ディレクターで Secure Private Access を構成する	45
ディレクターで Secure Private Access のユーザーセッションを表示する	45
ライセンスサーバー	46
ウェブスタジオ	46
アプリケーションの構成	47
次のステップ	49
アプリケーションのアクセスポリシーを構成する	49
アクセス ポリシーの優先度	50
次のステップ	50
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	50
セキュア プライベート アクセス ノードを作成する	51
ロードバランサー構成	51
Secure Private Access のヘルスチェックモニターを作成する	52
セキュア プライベート アクセスのアンインストール	53
ストアフロント 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	53
アップグレード	54
アップグレードの順序	54

Secure Private Access インストーラーをアップグレードする	55
次のステップ	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	56
管理	57
インストール後の設定を管理する	57
アプリケーションドメインのルーティングを管理する	57
管理者を管理する	57
統合設定を変更する	58
アプリケーションとポリシーの管理	58
アプリケーションの編集	58
アクセスポリシーの編集	58
エンドユーザーフロー	60
監視とトラブルシューティング	61
トラブルシューティング	61
Directorでのセッション関連コード	61
関連情報	61
ダッシュボードの概要	62
ログからコンテキストタグを表示する	63
基本的なトラブルシューティング	63
証明書エラー	63
データベース作成エラー	63
StoreFront™ における障害について	64
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	66
セキュア プライベート アクセス サーバーに接続できません	67
データベース接続チェックの失敗	67
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	67
アプリケーション列挙の失敗	68
その他の項目	68

初回セットアップを完了できません	68
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	68
セキュアプライベートアクセス の SQL データベース権限	69
トラブルシューティングログのログレベルを変更する	70
ディレクターにおけるセキュアプライベートアクセスセッションコード	71
セッションコード	71
アプリ列挙関連コード	72
アプリ起動メッセージコード	74
ログ保持設定	74
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	74
ログとテレメトリのクリーンアップ	76
テレメトリデータのクリーンアップ	76
CDFログのクリーンアップ	76
CDFログのカスタムクリーンアップ	76
サードパーティ通知	78

技術的な概要

Citrix Secure Private Access™ オンプレミスは、顧客が管理するゼロトラストネットワークアクセス (ZTNA) ソリューションであり、VPNなしで社内WebアプリケーションおよびSaaSアプリケーションへのアクセスを提供し、以下の機能とシームレスなエンドユーザーエクスペリエンスを提供します。

- 最小特権の原則
- シングルサインオン (SSO)
- 多要素認証方式
- デバイスの姿勢評価
- アプリケーションレベルのセキュリティ制御
- アプリ保護機能

このソリューションは、StoreFront オンプレミスとCitrix Workspace™ アプリを活用して、Citrix Enterprise Browser内でWebおよび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エクスペリエンスを実現します。このソリューションは、NetScaler Gatewayも活用して、認証および認可制御を適用します。

Citrix Secure Private Access オンプレミスソリューションは、StoreFront™ オンプレミス ポータルをWeb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統合されたCitrix Workspaceの一部として、ブラウザベースのアプリ（社内WebおよびSaaSアプリ）へのゼロトラストアクセスを容易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。

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向けに統合されたエクスペリエンスを提供します。

機能概要	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	ストアフロント オンプレミス/シトリックス ワークスペース アプリ
SaaSおよびWebアプリへのSSO	ネットスケーラー ゲートウェイ

機能概要	機能を提供するサービス/コンポーネント
多要素認証 (MFA) およびデバイスポスチャ (別名エンドポイント分析)	ネットスケーラー ゲートウェイ
WebおよびSaaSアプリのセキュリティ制御とアプリ保護制御	シトリックス エンタープライズ ブラウザ
承認ポリシー	セキュアプライベートアクセス
アクセス強制	ネットスケーラー ゲートウェイおよびCitrix Secure Access™クライアント
構成と管理について	セキュア プライベート アクセス
可視性、監視、トラブルシューティング	セキュア プライベート アクセス、ネットスケーラー コンソール (旧ADM)、およびシトリックス ディレクター

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

2024年12月

- FIPSプラットフォームでのSecure Private Accessオンプレミスソリューションのサポート

Secure Private Accessオンプレミスソリューションは、連邦情報処理標準 (FIPS) に準拠し、13.1-37.219以降のFIPSビルドを実行しているNetScalerプラットフォームでサポートされるようになりました。詳細については、[Federal Information Processing Standards](#)を参照してください。

2023年2月

シトリックス セキュア プライベート アクセス™とディレクターの統合

Citrix Secure Private Accessは、パフォーマンス管理とトラブルシューティングの強化のためにDirectorと統合されました。詳細については、「[Secure Private Access integration with Director](#)」を参照してください。

ディレクターでセキュアプライベートアクセスユーザーセッションを表示

DirectorでSecure Private Access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、失敗したセッションと成功したセッションのアプリ、ポリシー、セッションの詳細に関する情報も表示できます。詳細については、「[View a Secure Private Access session by user](#)」を参照してください。

シトリックス セキュアプライベートアクセスとライセンスサーバーの統合

Citrix Secure Private Accessは、ライセンスデータを収集および処理するためにライセンスサーバーと統合されました。詳細については、「[License server with Secure Private Access](#)」を参照してください。

修正された問題

リリース2402では、以下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切れによる) にのみ反映されます。

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**) で関連ドメインエントリが変更された後も、そのページは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。アプリが公開された後、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

リリース2402には以下の問題があります。

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、SPAがa.com/b.comにドメイン参加しているマシンに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。

- オンプレミス用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、以下を実行する必要があります。

Secure Private Access管理者サービスとランタイムサービスの両方について、IISアプリケーションプールに異なる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) アプリの列挙において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、ポリシーは配布グループを検索してユーザーおよびグループの条件を追加することはできません。
- Secure Private Access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、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。

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る。

回避策:

SSLプロファイルで構成されたSSLパラメーターを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、「[Support for smart access tags](#)」を参照してください。

RfWeb / Web版ワークスペース

RfWeb / Workspace for web はサポートされていないため、アプリは列挙されません。詳細については、「[When using StoreFront version 2311 or later](#)」を参照してください。

[SPAOP-2487]

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。

アプリケーションの起動

以下のすべての条件が満たされている場合、アプリケーションの起動は失敗します。

- 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が使用されている。
- LDAP UPNが実際のドメインとは異なるサフィックスで構成されている。
- LDAP UPN and sAMAccountName are different.

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証明書が使用されている場合、その証明書は、Internet Information Service (IIS)上の「Citrix Access Security Admin」サイトに再度バインドされる必要があります。

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が空白値に設定されており、これはSecure Private Accessでは機能しません。また、クライアントには以前のバージョンのReceiver UIが表示されます。StoreFrontの構成については、[StoreFront](#)を参照してください。
- StoreFrontバージョン2308以前を使用している場合、「ストア > 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。
- 管理サービスとランタイムサービスのログフォルダーは削除しないでください。これらのフォルダーが削除されると、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、アプリ名にコンマが含まれている場合、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 Private Accessインストーラーのエントリが最初のを置き換えるのではなく、2つ表示されます。

- 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™ 7 2402 LTSR
- 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 7 2311 - セキュアプライベートアクセス

You can uninstall the 2311 build installer by selecting **Citrix Virtual Apps and Desktops 7 2311 - Secure private access**.

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する場合、この問題は発生しません。

システム要件

お使いの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。

- シトリックス ワークスペース™ アプリ
 - ウィンドウズ – 2309 以降
 - macOS - バージョン 2309 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は、Windows Server 2019 以降です。
- StoreFront™ – LTSR 2203 or CR 2212 and later.
- NetScaler – 13.0、13.1、14.1以降。パフォーマンスを最適化するために、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 以降のバージョン。
- NetScaler FIPS - 13.1-37.219 and later FIPS builds.
- 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:

オンプレミス環境向けのSecure Private Accessは、iOSおよびAndroid版の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には、以下の詳細情報があることを確認してください。

- IISが稼働し、SSL/TLS証明書が構成されているWindowsサーバーマシン。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。
- セットアップ時に入力するStoreFrontストアのURL。

- StoreFront上のストアが構成されており、ストアサービスURLが利用可能である必要があります。ストアサービスURLの形式は `https://store.domain.com/Citrix/StoreSecureAccess` です。
- ネットスケラー ゲートウェイのIPアドレス、FQDN、およびネットスケラー ゲートウェイのコールバック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ー）のIPアドレスとFQDN。
- NetScalerで構成された認証プロファイル名。
- NetScalerで構成されたSSLサーバー証明書。
- ドメイン名。
- 証明書構成が完了していること。管理者は、証明書構成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、自己署名証明書を構成します。ただし、これは常に機能するとは限りません。
- データベース: サイト構成、構成ログ、および監視データベースでサポートされている Microsoft SQL Serverのバージョンは次のとおりです。
 - SQL Server 2022、エクスプレス、スタンダード、およびエンタープライズ エディション。
 - SQL Server 2019、エクスプレス、スタンダード、およびエンタープライズ エディション。
 - SQL Server 2017、エクスプレス、スタンダード、およびエンタープライズ エディション。

新規インストールの場合: 既存のサポートされているSQL Serverインストールが検出されない場合、デフォルトで累積更新プログラム16を含むSQL Server Express 2017がControllerのインストール時にインストールされます。

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

以下のデータベース高可用性ソリューションがサポートされています（SQL Server Expressはスタンドアロンモードのみをサポートするため、例外です）。

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

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

データベースの詳細については、[データベース](#)を参照してください。

注:

ランタイムサービス（IISデフォルトWebサイト内のsecureAccessアプリケーション）はWindows認証をサポートしないため、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ており、手動で変更してはなりません。

管理者アカウントの要件

Secure Private Accessのセットアップ中に、以下の管理者アカウントが必要です。

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

通信ポート

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

ソース	接続先	タイプ	ポート	詳細
管理ワークステーション	セキュア プライベート アクセス プラグイン	エイチティーティーピーエス	4443	セキュア プライベート アクセス プラグイン - 管理コンソール
セキュア プライベート アクセス プラグイン	NTPサービス	TCP, UDP	123	時間の同期
	DNSサービス	TCP, UDP	53	DNSルックアップ

ソース	接続先	タイプ	ポート	詳細
	アクティブディレクトリ	TCP, UDP	88	ケルベロス
	ディレクター	HTTP, HTTPS	80、443	パフォーマンス管理と高度なトラブルシューティングのためのDirectorへの通信
	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	プレーンテキスト経由のLDAP (LDAP)
		TCP	636	SSL経由のエルダップ (エルダップス)
	マイクロソフト SQL Server	TCP	1433	セキュア プライベート アクセス プラグイン - データベース通信
	ストアフロント	エイチティーティーピーエス	443	認証の有効性確認
	ネットスケーラー ゲートウェイ	エイチティーティーピーエス	443	ネットスケーラー ゲートウェイ コールバック
ストアフロント	NTP サービス	TCP, UDP	123	時刻の同期

ソース	接続先	タイプ	ポート	詳細
	DNS サービス	TCP、UDPプロトコル	53	DNS ルックアップ
	アクティブ ディレクトリ	TCP、UDPプロトコル	88	ケルベロス
		TCP	389	プレーンテキスト経由のLDAP (LDAP)
		TCP	636	エスエスエル経由のエラダップ (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
	セキュア プライベート アクセス プラグイン	エイチティーティーピーエス	443	認証とアプリケーションの列挙
	ネットスケーラー ゲートウェイ	エイチティーティーピーエス	443	ネットスケーラー ゲートウェイ コールバック
ネットスケーラー ゲートウェイ	セキュア プライベート アクセス プラグイン	HTTPS (エイチティーティーピーエス)	443	アプリケーション認証の検証
	ストアフロント	HTTPS (エイチティーティーピーエス)	443	認証とアプリケーションの列挙
	Webアプリケーション	HTTP, HTTPS	80, 443	構成された Secure Private Accessアプリケーションへの

ソース	接続先	タイプ	ポート	詳細
				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	ネットスケーラー ゲートウェイ	エイチティーティーピーエス	443	エンドユーザーデバイスとNetScaler Gateway間の通信

参考文献

- 認証プロファイル(<https://docs.netScaler.com/ja-jp/citrix-adc/current-release/aaa-tm/entities-of-authentication-authorization-auditing/authentication-profiles.html>)。
- [認証ポリシーの仕組み](#)
- [NetScaler上の仮想サーバー（SSL）にSSL証明書をバインドする](#)

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。

次の図は、サーバーのストレージ要件を示しています。



注:

- このメトリックは、ログイベントのクリーンアップが無効になっており、ログの保持期間が7日に設定されているという前提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、または構成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。

サーバー構成

次の表に、サーバー構成の詳細を示します。

構成内容	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構成	ユーザーは20のグループに属し、最大20レベルのネスト
トラブルシューティングログの保持期間	7日間 (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)
セキュア プライベート アクセス サーバー ログの保持	90日間または600ファイル

トラフィックプロファイル

次の表は、ユーザーあたりの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。

プロファイル	詳細
列挙項目	10
エンタープライズブラウザポリシーの同期	20

プロファイル	詳細
Citrix Workspace™ アプリからのアプリ起動	4
シトリックス エンタープライズ ブラウザ™ からのアプリアクセス	500
Citrix Directorを介したヘルプデスクのトラブルシューティングリクエスト（1日あたり）	1000

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などのパラメータに基づいたデータベースサイジング要件を示しています。

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	セキュア プライベート アクセスのメモリ容量 (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、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SPAを展開できます。
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	より良いパフォーマンスのために、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目的でローカルVMにSQL Expressを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と共存させるのではなく、Secure Private Accessを専用サーバーにデプロイすることをお勧めします。
- ******* 既知のパフォーマンス問題があるため、このような負荷に対しては少なくとも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	仮想CPU	メモリ
セキュア プライベート アクセス プラグイン	8	16 GB
セキュアプライベートアクセス SQLサーバー	8	16 GB
ストアフロント	16	8 GB
ゲートウェイ	4	8 GB
アクティブディレクトリ	8	14 GB
クライアント	4	8 GB

インストールと構成

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利用できます。詳細については、「[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用したインストール](#)」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Secure Private Accessのショートカットが表示されます。

Secure Private Accessをインストールおよび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。

セキュアプライベートアクセスのセットアップ

次の手順を完了することで、Secure Private Access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](#) または [既存のサイトに参加してSecure Private Accessをセットアップする](#)
- [データベースの構成](#)
- [ストアフロント、ネットスケーラーゲートウェイ、ディレクター、およびライセンスサーバーの統合](#)

アプリケーションとアクセスポリシーの構成

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

- 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

セキュア プライベート アクセス インストーラー

セキュア プライベート アクセス インストーラーは、統合されたシトリックス バーチャル アプリケーションズ アンド デスクトップス™ インストーラーの一部です。

Secure Private Access をインストールするには、次の手順を実行します。

1. <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/> から Citrix Virtual Apps and Desktops 製品ソフトウェアをダウンロードし、ウィザードを起動します。
2. 「仮想アプリまたは仮想アプリおよびデスクトップ」の横にある「スタート」をクリックします。
3. **Secure Private Access** を選択し、画面の指示に従ってインストールを完了します。



詳細な手順については、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。

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。**Continue** 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 **セキュアプライベートアクセス** のショートカットも表示されます。



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、Secure Private Accessを設定できます。

Google ChromeおよびMicrosoft Edgeブラウザで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/2402/spa-onprem-configure-apps.html)
- 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/2402/spa-onprem-configure-access-policies.html)

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。どちらの場合も、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として、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。
- マルチドメイン環境を使用している場合は、異なるフォレストにある Active Directory ドメイン間でドメイン信頼を確立してください。詳細については、「[マルチドメイン環境](#)」を参照してください。

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 Web 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、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行うことができます。

1. 「**SQL Serverホスト**」に、サーバーホスト名を入力します。例：

`sql1.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。

注：

入力したサイト名はデータベース名に接尾辞として追加されます。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サーバーが利用できない場合、接続チェックは失敗します。
- SQLサーバー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。

- Secure Private Accessは、マシンIDを使用したWindows認証を利用してSQLサーバーに認証します。

自動構成:

- **自動構成オプション**は、マシンIDが必要なデータベース権限を持ってい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：サーバーの統合

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。この接続は、StoreFrontおよびNetScaler® GatewayがSecure Private Access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。また、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。

- **セキュアプライベートアクセスサーバーのアドレス**。例えば、`https://secureaccess.domain.com`。

- **ストアフロント ストアのURL。**例えば、 `https://storefront.domain.com/Citrix/StoreMain`。
- **パブリック ネットスケーラー 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。例えば、 `https://gateway.domain.com`。
- **仮想IPアドレス** – 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。
- **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`。
- **ディレクター URL:** - セキュア プライベート アクセス を Citrix ディレクター 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URL:** - 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、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[トラブルシューティングエラー](#)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。



セットアップが完了すると、**概要**ページで**閉じる**をクリックした後に次のページが表示されます。

「セットアップ完了」 (/ja-jp/citrix-secure-private-access/media/setup-done.png)

注：

- 環境をセットアップした後、Web管理コンソールで **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。

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**ホストで、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**で、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サーバーインスタンスが有効であり、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)

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行われます。

HTTP2設定を無効にする

オンプレミス版Secure Private Accessは、Internet Information Services (IIS) 環境内で動作します。そのため、IIS内のHTTP/2に影響を与える可能性のある一般的な脆弱性は、Microsoftによって直接対処され、パッチが適用されます。それまでの間、お客様はIIS内でHTTP/2設定を手動で変更することでこの脆弱性を軽減でき、公式パッチがリリースされる前でもオンプレミス版Secure Private Accessソリューションが保護された状態を維持できます。

サイトごとにHTTP2を無効にするには、次の手順を実行します。

1. インターネット インフォメーション サービス (IIS) マネージャーを開きます。
2. ナビゲーションペインで「サイト」を展開し、「Default Web Site」を選択します。
3. 「操作」ペインで「バインド」をクリックし、「HTTP/2を無効にする」チェックボックスをオンにして、HTTPSバインドを変更します。
4. 保存してIISマネージャーを再起動します。

HTTP2を無効にする(/ja-jp/citrix-secure-private-access/media/disable-http2.png)

マルチドメイン環境

オンプレミス版Secure Private Accessの展開は、マシンサーバーとユーザーアカウントサーバーが異なるActive Directoryドメインに存在するマルチドメイン環境をサポートします。このクロスドメイン展開機能により、インフラストラクチャとユーザーIDの管理に柔軟性がもたらされます。ただし、この環境を成功させるには、異なるフォレストにあるActive Directoryドメイン間で少なくとも一方向の信頼関係を確立する必要があります。

信頼を確立する(/ja-jp/citrix-secure-private-access/media/spaop-multidomain-overview.png)

マルチドメイン環境でSecure Private Accessオンプレミス展開のドメインの信頼を確立するには、以下の前提条件を満たす必要があります。

- 初期構成に使用されるマシンドメイン（例：ドメインB）のサービスアカウントは、ユーザーアカウントドメイン（例：ドメインA）にプロビジョニングされている必要があります。

注：

サービスアカウントは、Citrix Access Security Runtime Service PoolのIISに追加する必要があります。サービスアカウントに管理者権限は必要ありません。詳細については、「[サービスアカウントを構成する手順](#)」を参照してください。

- インストールサーバー（ドメインAにあり、「サーバー ドメインA」と表記）もドメインAにある場合、サービスアカウントは、関連するデータベースインスタンス内で「db owner」権限を持つデータベースユーザーとして作成する必要があります。

サービスアカウントを構成する

サービスアカウントを構成するには、次の手順を実行します。

1. インターネット インフォメーション サービス (IIS) マネージャーを起動します。
2. サイトサーバーの下で、>>を選択します。

IISマネージャー(/ja-jp/citrix-secure-private-access/media/spaop-multidomain-iis-manager.png)

3. **ID > アプリケーションプールID** の編集アイコンをクリックします。

IDプール(/ja-jp/citrix-secure-private-access/media/spaop-multidomain-application-pool.png)

4. で、 をクリックします。

カスタム資格情報を設定(/ja-jp/citrix-secure-private-access/media/spaop-multidomain-set-service-account.png)

5. ユーザーの資格情報を設定します。
6. **OK**をクリックします。

資格情報を入力します(/ja-jp/citrix-secure-private-access/media/spaop-multidomain-service-credentials.png)

次のステップ

- NetScaler 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

コンポーネント

オンプレミス展開におけるSecure Private Accessの主要コンポーネントは以下のとおりです。

- **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。エンタープライズアプリケーションストアをホストでき、ユーザーは利用可能なデスクトップとアプリケーションにセルフサービスでアクセスできます。また、ユーザーのアプリケーションサブスクリプション、ショートカット名、その他のデータを追跡します。これにより、ユーザーは複数のデバイスで一貫したエクスペリエンスを

享受できます。StoreFrontとSecure Private Accessの統合の詳細については、[StoreFront](#)を参照してください。

- **NetScaler Gateway:** NetScaler Gatewayは、企業ファイアウォールを介して、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の統合に関する詳細については、[NetScaler Gateway](#)をご参照ください。
- **Director:** Directorは、効果的なパフォーマンス監視とトラブルシューティングを可能にします。DirectorをSecure Private Accessと統合するには、Secure Private Accessに登録する必要があります。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の統合の詳細については、「Secure Private AccessとDirectorの統合」([/ja-jp/citrix-virtual-apps-desktops/director/spa-integration-with-director.html](#))を参照してください。
- **License Server:** ライセンスサーバーは、ライセンスデータを収集および処理します。ライセンスサーバーとSecure Private Accessの統合の詳細については、[License Server integration with Secure Private Access](#)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おり、これにより、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することが可能になります。Web StudioとのSecure Private Accessの統合に関する詳細については、「Web StudioとのSecure Private Accessの統合」([/ja-jp/citrix-secure-private-access/2402/spaop-integration-with-studio.html](#))をご参照ください。

注:

ディレクターとライセンスサーバーは、リリース2402以降、セキュアプライベートアクセスと統合されています。

ネットスケーラー ゲートウェイ

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. スクリプトを <https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html> から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`。

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上の既存のリソース名を提供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。

注:

スクリプトの実行中に、NetScalerとSecure Private Accessプラグインの互換性がチェックされます。NetScalerがSecure Private Accessプラグインをサポートしている場合、スクリプトはNetScalerの機能を有効にし、スマートアクセスタグの送信改善と、リソースへのアクセスが制限された場合の新しい拒否ページへのリダイレクトをサポートします。スマートタグの詳細については、[スマートアクセスタグのサポート](#)を参照してください。

/nsconfig/rc.netscalerファイルに保持されているSecure Private Accessプラグインの機能により、NetScalerの再起動後もそれらを有効に保つことができます。



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:

```
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、次のコマンドの実行を続行します。

リソースが存在する場合、または手順6で入力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、パラメーター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。

既存の構成を持つネットスケーラー ゲートウェイでセキュア 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。

ネットスケラー ゲートウェイ仮想サーバーでの設定

既存の NetScaler Gateway 仮想サーバーを追加または更新する際は、次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。

仮想サーバーを追加:

- tcpProfileName: nstcp_default_XA_XD_profile
- デプロイメントタイプ: ICA_STOREFRONT (`add vpn vsrver` コマンドでのみ利用可能)
- ICAのみ: オフ
- ディーティーエルエス: オフ

仮想サーバーを更新:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: 無効にする

例示:

仮想サーバーを追加するには:

```
add vpn vsrver _SecureAccess_Gateway SSL 999.999.999.999 443 -Listenpolicy NONE  
-tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT  
-vsrverFqdn gateway.mydomain.com -authnProfile auth_prof_name -icaOnly OFF -  
dtls: OFF
```

仮想サーバーを更新するには:

```
set vpn vsrver _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。ストアへのパス `/Citrix/MyStoreWeb` はオプションです。
- `ClientChoices` : オフ
- `ntDomain` : mydomain.com - SSOに使用されます (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

使用例:

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
```

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

Secure Private AccessプラグインをVPN仮想サーバーにバインドするには。

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

ICA®アプリとの互換性

Secure Private Accessプラグインをサポートするために作成または更新されたNetScaler Gatewayは、ICAアプリ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。

- NetScaler Gatewayでのセキュアチケットオーソリティの構成(<https://docs.netscaler.com/ja-jp/citrix-gateway/current-release/integrate-citrix-gateway-with-citrix-products/integrate-web-interface-apps/ng-wi-comm-wrapper-con/ng-wi-comm-sta-config-tsk.html>)
- 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。

セキュアプライベートアクセス トグルの構成

次の表に、オンプレミス展開でスマートアクセスタグをサポートするために使用する必要があるトグルを示します。

トグル名	説明文
<pre>nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem</pre>	オンプレミス展開向けにSecure Private Accessを有効にする
<pre>nsapimgr_wr.sh -ys call=ns_vpn_disable_spa_onprem</pre>	オンプレミス展開向けにSecure Private Accessを無効にする
<pre>nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3</pre>	TCP/UDPアプリを有効にする
<pre>nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=0</pre>	TCP/UDPアプリを無効にする
<pre>nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode</pre>	HTTPコールアウト構成でSecureBrowseクライアントモードを有効にする
<pre>nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny</pre>	アクセスが拒否された場合に「アクセス制限」ページへのリダイレクトを有効にする。
<pre>nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page</pre>	CDNでホストされている「アクセス制限」ページを使用します。

注:

- 個別の無効化コマンドがないトグルを無効にするには、同じコマンドを再度実行します。これは、コマンドに「toggle」が含まれるコマンドにのみ適用されます。
- 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設定するには、「[コンテキストタグの設定](#)」を参照してください。

NetScaler 上で Secure Private Access プラグインの設定を永続的に保持するようにする

NetScaler で Secure Private Access プラグイン設定を永続化するには、次の手順を実行します。

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

```
nsapimgr -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。

NetScaler の再起動時に、Secure Private Access プラグイン設定が自動的に適用されます。

公開ゲートウェイ証明書をアップロードする

公開ゲートウェイがSecure Private Accessマシンから到達できない場合、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必要があります。

公開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>
```

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数のNetScaler構成が存在する可能性があります。
- Secure Private Accessが有効なVPN仮想サーバーで、**ICAプロキシ**をOFFに設定することをお勧めします。
- 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。ポートの詳細については、[通信ポート](#)を参照してください。
- NetScaler GatewayでSSOを有効にする場合、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。

コンテキストタグを構成する

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の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（新しいロジック）として、またはGatewayへのコールバックを行うことによって、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：

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ています。

GUIを使用してカスタムタグを構成する

コンテキストタグの構成には、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、**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できます。



4. 必須フィールドに詳細を入力し、**作成**をクリックします。
5. **式**に、式を手動で入力するか、式エディタ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し、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、コンテキストタグ名を入力します（例: `Windows10`）。

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 タグのサポート。](#)

ストアフロント

Secure Private AccessがStoreFrontと共同ホストされている場合、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と共同ホストされていない場合は、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、以下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. 構成変更を行う必要がある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. PowerShell 64ビットインスタンスで、コマンド `./ConfigureStorefront.ps1` を使用してスクリプトを管理者として実行します。

- 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、StoreFront管理UI (**デリバリーコントローラーの管理画面**) でSecure Private Accessプラグインの構成を確認できます。

Citrix Virtual Apps and Desktops™デリバリーコントローラーにも同じ設定がされている場合、StoreFrontスクリプトは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用に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）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、**設定 > 統合**ページからのStoreFrontの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XenMobile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アドレスは表示されません。
- 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**

ストアフロントバージョン2311以降では、シトリックスワークスペース™ for Webクライアントはセキュアプライベートアクセスアプリを列挙しません。これは、セキュアプライベートアクセスがワークスペース for Webプラットフォームでのセキュアプライベートアクセスアプリの起動をサポートしていないためです。

ディレクター

DirectorとSecure Private Accessの統合により、効果的なパフォーマンス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、オンプレミス版2402のお客様向けのSecure Private Accessにとって必須の構成です。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。すでにDirectorが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。Directorを登録しないと、Secure Private Accessのセットアップを完了できません。また、次の場合には検証が失敗します。

- ディレクターは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が存在しません。

DirectorをSecure Private Accessに登録する方法の詳細については、「[StoreFrontおよびNetScaler Gatewayサーバーの統合](#)」と「[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コンソールにログオンした場合、Director登録の資格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、その詳細がDirectorサーバーへの認証に利用されます。それが成功しない場合、管理者は資格情報を入力するよう求められます。
- セットアップ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の詳細を更新する際、管理者は変更を行うために資格情報を入力する必要があります。Director URL IPv6、SSLv3の編集にはシングルサインオンはサポートされていません。

ディレクター設定ツールを使用して、ディレクターで Secure Private Access を構成する
構成ツールを使用してDirectorをSecure Private Accessと構成することは、統合を完了するための必須の手順です。詳細については、「[DirectorとのSecure Private Access統合](#)」を参照してください。

ディレクターで Secure Private Access のユーザーセッションを表示する

DirectorでSecure Private Accessユーザーセッションを表示できます。詳細については、「[ユーザー別の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

Secure Private Accessプラグイン用のライセンスサーバーは、ライセンスデータを収集および処理するため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、初期設定時にSecure Private Accessに登録することも、設定完了後に構成または更新することもできます。Secure Private Accessへのライセンスサーバーの登録の詳細については、「[StoreFrontおよび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、ライセンスサーバーに自動的に登録されます。

注:

- Secure Private Accessプラグインをライセンスサーバーに登録するには、ライセンスサーバーにCitrix Virtual Apps and Desktops™ブローカーライセンスを少なくとも1つインストールする必要があります。
- Secure Private Accessプラグイン用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。すでにライセンスサーバーをお持ちの場合は、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。

ウェブスタジオ

Citrix Secure Private Access™ は、Web Studio コンソールにも統合されており、ユーザーが Web Studio を通じてサービスにシームレスにアクセスできるようにします。

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 の統合を有効にするには、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後、C:\Program Files\Citrix\Web Studio\Site\studio\assets\json に格納されているフォルダーへ移動し、spa-config.json ファイルの内容を修正してください。

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。
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

Secure Private Access をセットアップしたら、管理コンソールからアプリとアクセスポリシーを構成できます。

1. 管理コンソールで、 をクリックします。
2. 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。
 - 外部アプリケーションの場合は、。
 - 内部アプリケーションの場合は、。
4. セクションに次の詳細を入力し、 をクリックします。

アプリの構成(/ja-jp/citrix-secure-private-access/media/spaop-add-app.png)

- – アプリケーションの名前。
- - 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。
- - 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に 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。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 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、アプリケーションカテゴリフィールドで、「ビジネスと生産性」というカテゴリを誤って「ビジネス アンド プロダクティビティ」と入力した場合、Citrix Workspace UI には、「ビジネスと生産性」というカテゴリに加えて、「ビジネス アンド プロダクティビティ」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ピクセルである必要があります。サポートされているのはIco形式のみです。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たくない場合は、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。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。
 - 。 **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。

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、アプリはStoreFront™から自動的に削除されません。

- **アプリの接続** - Webアプリの場合は「**内部**」を、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、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. 管理コンソールで、 をクリックします。
2.  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>)

3.  で、アクセスポリシーを適用するアプリを選択します。
4.  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。

5.  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。
6.  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.  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。
 - 「制限付きアクセスを許可」を選択すると、制限を選択するために「制限の追加」をクリックする必要があります。各制限の詳細については、「[利用可能なアクセス制限](#)」を参照してください。

制限を選択し、「完了」をクリックします。

「

注:

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



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、アクセスポリシーページで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。アクセス ポリシーのホーム ページで優先度を表示できます。

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）から構成を検証します。

[「構成検証の例」](#)

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

Secure Private Access オンプレミスソリューションは、高可用性、高スループット、およびスケーラビリティのためにクラスターとして展開できます。大規模な展開（例えば、5000人以上のユーザー）の場合、ワークロードを分散し、スケーラビリティを向上させるために、複数の個別の Secure Private Access ノードを展開できます。

セキュア プライベート アクセス ノードを作成する

- 新しい Secure Private Access サイトを作成します。詳細については、[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。
- Secure Private Access で最初のノードを構成する際は、ロードバランサー名を使用します。後続のノードを追加するには、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たデータベースのアップグレード](#)を参照してください。



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、以下に注意してください。

- StoreFront へのアクセスに使用される FQDN は、サブジェクト代替名 (SAN) として DNS フィールドに含まれます。ロードバランサーを使用している場合は、個々のサーバーの FQDN とロードバランサーの FQDN の両方を含めます。これは SSL 証明書に適用されます。Secure Private Access の場合、ロードバランサーの構成で十分です。詳細については、[NetScaler を使用したロードバランシング](#)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している場合は、ベース URL をロードバランサー名で構成し、安全な通信のために HTTPS を使用します。詳細については、[HTTPS を使用した StoreFront の保護](#)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構成を使用できます。SSL ブリッジを使用する場合は、各 Secure Private Access ノードで同じサーバー証明書を構成するようにしてください。また、証明書のサブジェクト共通名またはサブジェクト代替名 (SAN) は、ロードバランサーの FQDN と一致する必要があります。また、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。

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

Secure Private Access のヘルスチェックモニターを作成する

Secure Private Accessのモニターを作成するには、次のCLIコマンドを使用します。

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

モニターを作成したら、証明書をモニターにバインドします。

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

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. シトリックス バーチャルアプリとデスクトップ™ 7 2402 – 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、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 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 ファイルをダウンロードする必要があります。
3. StoreFrontScripts.zip を任意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
```

アップグレード

新しいマシンやサイトを最初にセットアップすることなく、Secure Private Accessの展開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、構成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、新しいバージョンの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. セキュア プライベート アクセス を最初にインストールした方法に応じて、デリバリー コントローラー™ を介して、またはインストーラーUIの専用セキュア プライベート アクセス タイルを介して、セキュア プライベート アクセス をアップグレードできます。
 - Secure Private AccessをDelivery Controller経由でインストールした場合、Secure Private Accessコンポーネントのみ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。詳細については、[展開のアップグレード](#)を参照してください。
 - 専用のSecure Private Accessタイルを介してSecure Private Accessをインストールした場合、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を介してSecure Private Accessをインストールすることをお勧めしますが、本番環境では、新しい機能や機能に適応できるように、専用の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たデータベースのアップグレード](#)を参照してください。

3. StoreFront構成を再度実行します。設定 > 構成からStoreFrontスクリプトをダウンロードし、対応するStoreFrontマシン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スクリプトを実行します。詳細については、[NetScaler Gateway](#)を参照してください。

Secure Private Access インストーラーをアップグレードする

1. <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/> から Citrix セキュアプライベートアクセス 2402 インストーラーを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。
3. 画面の指示に従ってインストールを完了します。

インストーラーのアップグレード 1(/ja-jp/citrix-secure-private-access/media/spaop-upgrade-2402-1.png)

インストーラーのアップグレード 2(/ja-jp/citrix-secure-private-access/media/spaop-upgrade-2402-2.png)

インストーラーのアップグレード 3(/ja-jp/citrix-secure-private-access/media/spaop-upgrade-2402-3.png)

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後、新しいエンドポイントの詳細が利用可能になるように、StoreFront™ スクリプトを再実行する必要があります。

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

管理設定ツールを使用して、Secure Private Accessプラグイン用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>
```

管理

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](#)

インストール後の設定を管理する

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。

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。

統合設定を変更する

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. > 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)

アプリケーションとポリシーの管理

アプリケーションとアクセスポリシーを設定した後、必要に応じて編集できます。

アプリケーションの編集

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と同じ行にある省略記号ボタンをクリックし、 をクリックします。
3. アプリの詳細を編集します。
4. をクリックします。

アプリを編集する (/ja-jp/citrix-secure-private-access/media/spaop-edit-app.png)

アクセスポリシーの編集

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. 変更するポリシーと同じ行にある省略記号ボタンをクリックし、 をクリックします。
3. ポリシーの詳細を編集します。
4. をクリックします。

アクセスポリシーを編集する(/ja-jp/citrix-secure-private-access/media/spaop-edit-policy.png)

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アプリに透かし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、透かし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™ アプリケーションから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。

エンドユーザーは、Office365アプリケーションが起動され、透かし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 アプリにストアURLを追加する](#)」を参照してください。

監視とトラブルシューティング

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」([/ja-jp/citrix-secure-private-access/2402/spa-onprem-dashboard](https://ja-jp.citrix-secure-private-access/2402/spa-onprem-dashboard))を参照してください。

トラブルシューティング

Secure Private Accessのセットアップ中またはセットアップ後に、次のような問題が発生する可能性があります。

- 証明書エラー
- データベース作成エラー
- StoreFront™ に問題が発生した場合
- 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 が到達不能

これらの問題の修正の詳細については、「基本的なトラブルシューティング」([/ja-jp/citrix-secure-private-access/2402/spa-onprem-troubleshooting.html](https://ja-jp.citrix-secure-private-access/2402/spa-onprem-troubleshooting.html))を参照してください。

Directorでのセッション関連コード

DirectorとSecure Private Accessの統合により、Secure Private Accessのセットアップ内のすべてのコンポーネントからの問題がDirectorにキャプチャされるため、効果的なパフォーマンス監視とトラブルシューティングが可能になります。ログを調べて、障害または例外の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、サポートにお問い合わせください。

関連情報

- [ディレクターでセキュアプライベートアクセスを構成する](#)
- [ディレクターでセキュアプライベートアクセスセッションを表示する](#)
- [ディレクターのセキュアプライベートアクセスセッションコード。](#)
- [ディレクター。](#)

ダッシュボードの概要

Secure Private Access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チャート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。



検索フィールドの演算子とともに、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

以下は、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/ポリシーを検索する場合。
- !~: 指定された条件の一部を含まないログ/ポリシーを検索する場合。

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」

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、アクセス要求に対するすべての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)

基本的なトラブルシューティング

このトピックでは、Secure Private Access のセットアップ中またはセットアップ後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

データベース作成エラー

ストアフロントの障害

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

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、パブリック 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 のセットアップ時、またはセットアップ完了後の設定更新時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 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。

- 。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、スクリプトを再度実行する必要があります。

- 。そのマシンには、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: マシンに適切な権限を付与してください。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サーバー（インストーラーからではない）を使用している場合、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。

StoreFront™ における障害について

- **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をセットアップした後、**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エントリの設定に失敗しました: `<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 > 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。Settings > Integrations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をセットアップした後、Settings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をメモしておいてください。

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. **Settings**をクリックし、次に**Integrations**タブをクリックします。
- b. **StoreFront Store URL**で、エラーが発生したURLエントリを特定します。
- c. このストアURLの横にある「Download Script」 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、管理者権限でWindows x64互換のPowerShellウィンドウを開き、ConfigureStorefront.ps1を実行します。このスクリプトは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、 `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。

セキュア プライベート アクセス サーバーに接続できません

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:

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

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: 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([/ja-jp/citrix-secure-private-access/2402/spa-onprem-troubleshooting#sql-database-permissions-for-secure-private-access](#))。

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でした。」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。
- 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。

その他の項目

初回セットアップを完了できません

初回セットアップ中にDirectorの構成が失敗した場合、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ます。

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。
- Secure Private Access のインストールフォルダーの直下にある 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てください (例えば、Windows のコマンドプロンプトや PowerShell などのターミナルアプリケーションで、"cd "C:\Program

Files\Citrix\Citrix Access Security\Admin\AdminConfigTool"" とコマンドを入力し、実行してください)。

- 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の 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用の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. Assign the db_owner role to the “NT AUTHORITY\SYSTEM” user.

```
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ログレベルを変更する

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。

To change the log level for the troubleshooting logs, in the runtime service appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) update

`restrictedToMinimumLevel` for `TroubleshootingSql` to one of the following values:

- Information
- Debug
- Warning
- Error

```
"TroubleshootingSql": {
```

```
  "restrictedToMinimumLevel": "Error",
```

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

ディレクターにおけるセキュアプライベートアクセスセッションコード

DirectorとSecure Private Accessの統合により、Secure Private Accessセットアップ内のすべてのコンポーネントからの問題がDirectorにキャプチャされるため、効果的なパフォーマンス監視とトラブルシューティングが可能になります。以下の表は、Directorに表示されるさまざまなエラーコードと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。

- [ディレクターとセキュアプライベートアクセスの構成](#)
- [Directorでセキュアプライベートアクセス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、失敗または例外を表します。たとえば、2101はセッションの失敗を表します。失敗または例外の場合、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。

セッションコード

コード	ステータス	説明文
2101	失敗	セッションの失敗。
2102	アクティブ/非アクティブ/失敗	セッションはアクティブであるか、終了しているか、またはセッション内の少なくとも

コード	ステータス	説明文
		1つのアプリ起動が失敗しました。
2000	アクティブ	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。

アプリ列挙関連コード

コード	ステータス	項目説明
1101	失敗	列挙中に内部エラーが発生しました。
1102	失敗	いくつか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	すべてのアプリがポリシーによって拒否されたため、アプリは列挙されませんでした。
1002	成功	ポリシーが一致しなかったため、アプリは列挙されませんでした。
1003	成功	一部のアプリが拒否され、他のアプリには一致するポリシーがなかったため、アプリは列挙されませんでした。

コード	ステータス	項目説明
1004	成功	評価するポリシーがなかったため、アプリは列挙されませんでした。
3101	失敗	アプリの列挙 - 内部エラーが発生しました（現在未使用）。
3102	失敗	ポリシー評価中に例外が発生したため、アプリは列挙されませんでした。
3103	失敗	アプリケーション列挙ステータスがnullです - 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の取得中にエラーが発生しました。
3000	許可	アプリケーションの列挙は許可されています。
3001	拒否	アプリケーションの列挙はポリシーによって拒否されました。
3002	拒否	一致するポリシーがなかったため、アプリケーションは列挙されませんでした。
3003	不明	アプリ列挙ステータスは不明です。
3004	CEBからのアプリ起動	シトリックス エンタープライズ ブラウザからのアプリ起動試行。

アプリ起動メッセージコード

コード	ステータス	説明内容
4101	失敗	アプリケーション起動エラー - アプリケーション起動中に 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の取得 中にエラーが発生しました。
4104	失敗	アプリケーション起動エラー - アプリケーション構成が見 つかりません。
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かった ため、アプリケーションの起 動が拒否されました。

ログ保持設定

ログはSecure Private Accessデータベースに7日間保存されます。ログの総数が多すぎる場合（たとえば100,000を超える場合）、90日より古いログを早期に削除できます。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 ファイルを介して構成できます。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 ファイルのサンプル記述例:

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

クリーンアップを無効にするには、必要に応じて次の設定を構成します。

- 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に設定するか、`CleanupPeriodInHours` を0に設定することは、ディスク使用率が100%になる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。クリーンアップ対象のテレメトリデータを識別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、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。ランタイムサービスはAdminサービスと同じように機能しますが、一度に最大600個という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および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ファイルを介して構成できます。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ファイルの次のエントリを更新します。

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

注：

サイト用にSecure Private Accessの複数のインスタンスが設定されている場合は、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ファイルを更新してください。

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 オンプレミス版