



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	8
コンポーネント	9
新機能	10
2024年12月	10
2024年6月	10
SaaSおよび社内Webアプリに対する追加のアクセス制限	10
未承認Webサイトのサポート	10
シトリックス セキュア プライベート アクセス™ プラグインとSIEMサービスとの統合	10
トラブルシューティングログレベルが「情報」から「エラー」に変更されました	11
修正された問題	11
ドメインコントローラーの構成	11
管理者管理	11
アプリケーションの起動	11
管理コンソール	11
アップグレード	12
既知の問題	12
ドメインコントローラーの構成	12
ネットスケーラー® ゲートウェイ	13
アールエフウェブ / ウェブ向けワークスペース	13
アプリケーションの起動	13
ストアフロント™	13
ログ	13
プログラムのアンインストールまたは変更ページでのインストーラの表示	14
アップグレード	14
システム要件	15
前提条件	15

管理者アカウントの要件	17
通信ポート	17
リファレンス	20
サイジングガイドライン	20
データベースストレージ要件	20
サーバー構成	21
トラフィックプロファイル	21
展開ガイドライン	22
その他のコンポーネント構成	23
インストールと構成	24
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の要件	24
セキュアプライベートアクセスの設定	24
アプリケーションとアクセスポリシーを構成する	25
セキュア プライベート アクセス インストーラー	25
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の要件	25
管理コンソールへの SSO	26
次のステップ	27
セキュア プライベート アクセスを設定する	28
前提条件	28
新しいサイトを作成して Secure Private Access をセットアップする	28
ステップ 1: Secure Private Access サイトをセットアップする	28
ステップ2: データベースの構成	29
ステップ3: サーバーを統合する	30
ステップ4: 構成の概要	31
既存のサイトに参加して Secure Private Access をセットアップする	31
HTTP2設定を無効にする	32
マルチドメイン環境	33
サービス アカウントを構成する	33

次のステップ	34
コンポーネント	34
ネットスケーラー ゲートウェイ	35
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	37
ICA®アプリとの互換性	39
スマートアクセスタグのサポート	39
パブリックゲートウェイ証明書のアップロード	41
既知の制限事項	42
コンテキストタグを設定する	42
ストアフロント	44
StoreFrontバージョン2308以前を使用している場合	45
StoreFrontバージョン2311以降を使用している場合	45
ディレクター (オプション)	46
ディレクター構成ツールを使用して、セキュアプライベートアクセスでディレクターを構成する	47
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する	47
ライセンスサーバー	47
ウェブスタジオ (オプション)	47
HTTP/HTTPSアプリケーションを構成する	48
次のステップ	51
アプリケーションのアクセスポリシーを構成する	51
アクセス ポリシーの優先順位	52
次のステップ	52
アクセス制限オプション	52
クリップボード	53
コピー	53
ファイルタイプによるダウンロード制限	53

ダウンロード	54
安全でないコンテンツ	54
キーロギング保護	55
マイク	55
通知設定	56
貼り付け	57
個人データマスキング	57
ポップアップ	58
印刷	59
プリンター管理	59
画面キャプチャ	61
ファイルタイプによるアップロード制限	61
アップロード	62
透かし	62
Webカメラ	62
セキュリティグループのクリップボード制限	63
Secure Private Accessをクラスターとして展開する（オプション）	67
セキュアプライベートアクセス ノードを作成する	67
ロードバランサーの構成	67
セキュアプライベートアクセス のモニターを作成する	69
セキュアプライベートアクセスのアンインストール	69
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	70
アップグレード	71
アップグレードシーケンス	71
Secure Private Access インストーラーをアップグレードする	72
次のステップ	72
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	73
管理	74

インストール後の設定を管理する	74
アプリケーションドメインのルーティングを管理する	74
管理者の管理	74
統合設定の変更	75
アプリケーションとポリシーの管理	75
アプリケーションを編集する	75
アクセスポリシーを編集する	75
承認されていないWebサイト	76
承認されていないWebサイトの仕組み	76
未承認ウェブサイトのルールを構成する	77
エンドユーザーフロー	78
監視とトラブルシューティング	79
トラブルシューティング	79
Director のセッション関連コード	79
参考資料	79
ダッシュボードの概要	80
ログからコンテキストタグを表示する	80
基本的なトラブルシューティング	81
証明書エラー	81
データベース作成エラー	81
ストアフロント™ の障害	82
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	84
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	85
データベース接続チェックの失敗	85
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	85
アプリケーション列挙の失敗	86
その他の項目	86
初回セットアップを完了できません	86

Secure Private Access診断サポートバンドルを作成する	86
セキュアプライベートアクセスのSQLデータベース権限	87
トラブルシューティングログのログレベルを変更する	88
アプリケーション起動 / Citrix Secure Access ログイン失敗	89
Directorでのセキュアプライベートアクセスセッションコード	89
セッションコード	90
アプリ列挙関連コード	90
アプリ起動メッセージコード	92
SIEM統合	93
参照ドキュメント	94
ログ保持設定	95
トラブルシューティングログの保持設定をカスタマイズする	95
ログとテレメトリのクリーンアップ	96
テレメトリデータのクリーンアップ	96
CDFログのクリーンアップ	96
CDFログのカスタムクリーンアップ	96
サードパーティ通知	98

技術的な概要

Citrix Secure Private Access™ on-premises 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、シームレスなエンドユーザーエクスペリエンスとともに、以下の機能で内部WebアプリケーションおよびSaaSアプリケーションへのVPN不要のアクセスを提供します。

- 最小権限の原則
- シングルサインオン (SSO)
- 多要素認証機能
- デバイスポスチャ評価
- 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 on-premises 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可能にします。また、このソリューションはNetScaler Gatewayを活用して、認証および認可制御を適用します。

Citrix Secure Private Access on-premises ソリューションは、StoreFront™ on-premises 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、Citrix Workspace の統合された一部として仮想アプリとデスクトップとともに、ブラウザベースのアプリ（内部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。

機能一覧	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統一された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

機能一覧	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アプリ向け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シトリックス セキュア アクセス™ クライアント
構成および管理	セキュア プライベート アクセス
可視性、監視、および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、[連邦情報処理標準](#)を参照してください。

2024年6月

SaaSおよび社内Webアプリに対する追加のアクセス制限

SaaSおよび社内Webアプリに対して、追加のアクセス制限が利用可能になりました。管理者は、アクセスポリシーを通じてこれらの制限を適用できます。詳細については、「利用可能なアクセス制限」([/ja-jp/citrix-secure-private-access/2405/spaop-security-controls.html](#))を参照してください。

未承認Webサイトのサポート

Secure Private Accessプラグインにより、未承認Webサイトへのアクセスがサポートされるようになりました。Secure Private Access内で構成されていないアプリケーション（イントラネットまたはインターネット）は、「未承認Webサイト」と見なされます。デフォルトでは、Secure Private Accessは、アプリケーションおよびそれらのアプリケーション用に構成されたアクセスポリシーがない場合、すべてのイントラネットWebアプリケーションへのアクセスを拒否します。詳細については、「未承認Webサイト」([/ja-jp/citrix-secure-private-access/2405/unsanctioned-websites.html](#))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™ プラグインとSIEMサービスとの統合

Citrix Secure Private Accessは、セキュリティ情報およびイベント管理 (SIEM) と統合されました。詳細については、「SIEM統合」([/ja-jp/citrix-secure-private-access/2405/spa-opprem-siem-integration.html](#))を参照してください。

トラブルシューティングログレベルが「情報」から「エラー」に変更されました

データベースの負荷を軽減するため、トラブルシューティングログレベルが「情報」から「エラー」に変更されました。ログレベルの変更方法の詳細については、「トラブルシューティングログのログレベルの変更」([/ja-jp/citrix-secure-private-access/2405/spa-onprem-troubleshooting#change-log-level-for-troubleshooting-logs](https://ja-jp.citrix-secure-private-access/2405/spa-onprem-troubleshooting#change-log-level-for-troubleshooting-logs))を参照してください。

修正された問題

以下の問題はリリース 2402 で対処されています。

ドメインコントローラーの構成

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

管理者管理

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

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。

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ても、「**アプリの編集**」ページが自動的に閉じません。

例えば、アプリの作成時に入力した関連ドメインが `www.example.com` だったとします。アプリが公開された後、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。

- 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。

- アプリの URL に `www` が含まれている場合、その URL はルーティングドメインテーブル (設定 > アプリケーションドメイン) にプレフィックス `www` なしで保存されます。

アップグレード

セキュアプライベートアクセス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する必要があります。

既知の問題

リリース2405には以下の問題があります。

注:

一部の問題には内部参照のみを目的とした追跡IDが割り当てられており、これらはお客様には影響しません。

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で、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。

例えば、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。

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

Secure Private Accessの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。

- Secure Private Accessでは配布グループはサポートされていません。そのため、ポリシーはユーザーおよびグループ条件を追加するために配布グループを検索できません。
- Secure Private Accessは、管理コンソールまたはサービスでドメインの詳細をキャプチャしません。そのため、ユーザーが提供したドメインに完全に依存します。したがって、対応するドメインにアクセスできない場合や、ドメイン名が有効な名前でない場合、そのドメインはサポートされません。

ネットスケーラー® ゲートウェイ

- 以下のシナリオでは、SSLプロファイル構成を持つSSL仮想サーバーはサポートされていません。
 - お客様がNetScaler Gateway 13.1–48.47以降または14.1–4.42以降を使用している場合。
 - 「`ns_vpn_enable_spa_onprem`」 トグルが有効になっています。

回避策:

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

トグルの詳細については、[スマートアクセスタグのサポート](#) を参照してください。

アールエフウェブ / ウェブ向けワークスペース

- RfWeb / Workspace for web はサポートされていないため、アプリは列挙されません。詳細については、「StoreFront バージョン 2311 以降を使用する場合」 ([/ja-jp/citrix-secure-private-access/2405/spa-onprem-storefront-config#when-using-storefront-version-2311-or-later](#)) を参照してください。

アプリケーションの起動

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

ストアフロント™

- ストア > **Unified Experience の構成** で、Webサイトのデフォルトレシーバーは `/Citrix/<StoreName> Web` に設定する必要があります。以前のバージョンのStoreFrontでは、Webサイトのデフォルトレシーバーは空白に設定されており、Secure Private Access では機能しません。また、クライアントには以前のバージョンのReceiver UIが表示されます。StoreFront の構成については、「StoreFront」 ([/ja-jp/citrix-secure-private-access/2405/spa-onprem-storefront-config.html](#)) 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 プラグインの種類が **XenMobile®** と表示されます。これは機能には影響しません。

ログ

- クラスターのサポートバンドル生成はサポートされていません。

- 管理サービスとランタイムサービスのログフォルダは削除しないでください。これらのフォルダが削除されると、Secure Private Access は再作成できません。

プログラムのアンインストールまたは変更ページでのインストーラの表示

- ISOファイルを使用してSecure Private Accessを以前のバージョンから2405にアップグレードすると、「プログラムのアンインストールまたは変更」ページ（コントロールパネル > プログラム > プログラムと機能）に、最初の項目を置き換える代わりに、Secure Private Accessインストーラのエントリが2つ表示されます。

回避策: 古いビルドのインストーラをアンインストールします。

注:

この問題は、Secure Private Accessスタンドアロンインストーラが2402スタンドアロンインストーラを使用してアップグレードされた場合には発生しません。

アップグレード

- 2405にアップグレードした後、URLが **www** で始まる既存のアプリを編集すると、「アプリ接続」フィールドに以前の状態が入力されません。アプリ接続タイプを再度選択する必要があります。これはアップグレード後の一度限りのアクションであり、その後設定は保存され、永続的に維持されます。
- 2405にアップグレードした後、管理コンソールにログオンすることはできますが、アプリケーションとポリシーを管理できません。エラーメッセージが表示されます。

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

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

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

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

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™ アプリケーション
 - ウィンドウズ – 2403以降
 - macOS 2402以降のバージョン
- Secure Private Accessプラグインサーバーのオペレーティングシステム - Windows Server 2019以降のバージョン。
- 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には、NetScaler Gateway バージョン13.1または14.1の最新ビルドを使用することをお勧めします。
- NetScaler FIPS - 13.1-37.219 and later FIPS builds.
- ディレクター 2402 以降。
- 通信ポート: Secure Private Accessプラグインに必要なポートが開いていることを確認してください。詳細については、「[通信ポート](#)」を参照してください。

注:

オンプレミス版のセキュアプライベートアクセスは、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。
- セットアップ中に入力するStoreFrontストアのURL。

- StoreFront上のストアが構成されており、ストアサービス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。
- NetScaler Gateway IP address, FQDN, and NetScaler Gateway Callback 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。
- 証明書の設定が完了していること。管理者は、証明書の設定が完了していることを確認する必要があります。Secure Private Accessインストーラーは、マシン内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, Express, Standard, and Enterprise Editions.
 - 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の各エディション。
 - 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の各エディション。

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が適用された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はスタンダードオンモードのみをサポートします）。

- 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。

送信元	目的地	種類	ポート	詳細
管理者ワークステーション	セキュアプライベートアクセスプラグイン	HTTPSプロトコル	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	時刻の同期
	DNSサービス	TCP, UDP	53	DNSルックアップ
	アクティブディレクトリ	TCP, UDP	88	ケルベロス

送信元	目的地	種類	ポート	詳細
	ディレクター	HTTP, HTTPS	80、443	パフォーマンス 管理と強化され たトラブル 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 タの収集と処理 のためのライセ ンスサーバーへ の通信
		TCP	389	プレーンテキス ト経由のLDAP (LDAP)
		TCP	636	SSLプロトコル を利用した LDAP (LDAPS)
	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	HTTPSプロト コル	443	認証情報の検証
	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	時間の同期
	DNSサービス	TCP, UDP	53	DNSルックアッ プ

送信元	目的地	種類	ポート	詳細
	アクティブ ディレクトリ	TCP, UDP	88	ケルベロス
		TCP	389	平文でのエルディーイーピー (LDAP)
		TCP	636	エスエスエル経由のエルディーイーピー (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	エイチティーティーピーエス	443	アプリケーション認証検証
	ストアフロント	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 NetScaler Gateway通信

送信元	目的地	種類	ポート	詳細
				(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	ネットスケール 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

リファレンス

- [認証プロファイル](#)。
- [認証ポリシーの仕組み](#)。
- [NetScalerでSSL証明書を仮想サーバー \(SSL\) にバインドする](#)。

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。

サーバーのストレージ(/ja-jp/citrix-secure-private-access/media/spaop-sizing-guidelines.png)

注:

- メトリックは、ログイベントのクリーンアップが無効になっており、ログ保持期間が7日に設定されているという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

次の表は、サーバー構成の詳細を示しています。

構成設定	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レベルのネストがあります
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で使用するCPUなどのパラメータに基づいたデータベースのサイジング要件を示しています。

同時アプリ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 (GB)	セキュアプライベートアクセス CPU	ストレージ (GB)	注記
20未満 (PoC目的)	2	4 GB	2	40 GB*	PoC目的の場合、SPAは既存のVM仕様を変更することなく、StoreFront™ と同じマシンに展開できます。
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	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のサイズのロールオーバーログファイルを600個保持します。したがって、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との共存ではなく、専用サーバーにSecure Private Accessをデプロイすることをお勧めします。
- *** このような負荷に対しては、既知のパフォーマンス問題があるため、少なくとも2つのSecure Private Accessノードクラスターを使用することをお勧めします。これらの問題は、今後のリリースで対処される予定です。

その他のコンポーネント構成

コンポーネント	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、(</ja-jp/citrix-virtual-apps-desktops/install-configure/install-core-components.html>)または(</ja-jp/citrix-virtual-apps-desktops/install-configure/install-core/install-command.html>)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Secure Private Accessのショートカットも表示されます。

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の要件

- 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設定

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(</ja-jp/citrix-secure-private-access/2405/spa-onprem-setup-spa#set-up-secure-private-access-by-creating-a-new-site>) 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(</ja-jp/citrix-secure-private-access/2405/spa-onprem-setup-spa#set-up-secure-private-access-by-joining-an-existing-site>)

secure-private-access/2405/spa-onprem-setup-spa#set-up-secure-private-access-by-joining-an-existing-site)

- データベースを構成する(/ja-jp/citrix-secure-private-access/2405/spa-onprem-setup-spa#step-2-configure-databases)
- 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を統合する(/ja-jp/citrix-secure-private-access/2405/spa-onprem-setup-spa#step-3-integrate-storefront-and-netscaler-gateway-servers)

アプリケーションとアクセスポリシーを構成する

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

Secure Private Access 2405 インストーラーは、Secure Private Access コンポーネントのみをインストール/アップグレードするスタンドアロンインストーラーとして利用可能です。

注：

Secure Private Access 2405 は、MSI を使用してメタインストーラー経由でインストールすることもできます。詳細については、<https://www.citrix.com/downloads/citrix-secure-private-access/spa-onprem-standalone/spa-2405.html> を参照してください。

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の要件

- Secure Private Access をインストールするには、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 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、その後、他の管理者を追加できます。
- セットアップ後に Secure Private Access を管理するには、Secure Private Access 管理者アカウントで Secure Private Access 管理コンソールにサインインする必要があります。

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

1. Secure Private Access 2405 インストーラーを [<https://www.citrix.com/downloads/citrix-secure-private-access/spa-onprem-standalone/>](https://www.citrix.com/downloads/citrix-secure-private-access/spa-onprem-standalone/) からダウンロードします。
2. ドメイン参加済みマシンで .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。

注：

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

「インストーラー 1」 (/ja-jp/citrix-secure-private-access/media/spaop-install1.png)

4. 画面の指示に従ってインストールを完了してください。

「インストーラー 3」 (/ja-jp/citrix-secure-private-access/media/spaop-install3.png)

「インストーラー 2」 (/ja-jp/citrix-secure-private-access/media/spaop-install2.png)

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。

「初回セットアップ」 (/ja-jp/citrix-secure-private-access/media/first-time-setup.png)

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

「インストーラーのショートカット」 (/ja-jp/citrix-secure-private-access/media/spaop-installer-shortcut.png)

管理コンソールへの SSO

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

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

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

Secure Private Access のセットアップを続行するには、管理コンソールにサインインする必要があります。インストールマシンと同じドメインに属するユーザーで、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、そのユーザーで 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、特定のブラウザのKerberos認証に関するドキュメントを確認してください。

次のステップ

- セキュアプライベートアクセスをセットアップする
- ネットスケーラー ゲートウェイを構成する

- アプリケーションを構成する
- アプリケーションのアクセスポリシーを構成する

セキュア プライベート アクセスを設定する

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

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

前提条件

- Secure Private Access がインストールされているマシンのローカルマシン管理者でもあるドメインユーザーとして、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 Host**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サーバー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、ただし必要なデータベース権限を持っ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:

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

手動構成では、まずスクリプトをダウンロードし、次に**SQL Server Host**フィールドで指定したデータベースサーバーでスクリプトを実行する必要があります。

注

マシンが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権限を持っていない場合、データベースの作成が失敗する可能性があります。マシンで適切な権限を有効にする必要があります。詳細については、「[データベースのセットアップに必要な権限](#)」を参照してください。

ステップ3: サーバーを統合する

Secure Private AccessをStoreFrontおよびNetScaler® Gatewayサーバーに接続するには、StoreFrontおよびNetScaler Gatewayサーバーの詳細を指定する必要があります。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。

- **安全なプライベートアクセス サーバーの所在地。**例: `https://secureaccess.domain.com`。
- **StoreFront ストアのURL。**例えば、`https://storefront.domain.com/Citrix/StoreMain` のようになります。
- **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`。
- **Director URL:** - (Optional) The Director server IP address or FQDN to connect Secure Private Access with Citrix Director.
- **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、**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実行されます。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[エラーのトラブルシューティング](#)を参照してください。これにより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。



注:

- 環境をセットアップした後、Web管理コンソールの > 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。管理者のリストは、> 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許可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. ページで、**を**選択し、**を**クリックします。



2. に、サーバーホスト名を入力します。入力したサイト名に対応するデータベースが、選択した SQL Server にすでに存在することを確認してください。データベースアドレスは、次のいずれかの形式で指定できます。

- サーバー名
- サーバー名\インスタンス名
- サーバー名,ポート番号

詳細については、「[データベース](#)」を参照してください。

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

4. SQLサーバーインスタンスが有効であること、および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するには、**接続テスト**をクリックします。

データベース構成(/ja-jp/citrix-secure-private-access/media/spaop-database-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。

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、これにより公式パッチがリリースされる前であってもオンプレミス版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. IISマネージャーを保存して再起動します。

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存在する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。



マルチドメイン環境でオンプレミス展開のSecure Private Accessのドメイン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 アカウントには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 内、「サーバー ドメイン A」と呼ぶ) 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、**アプリケーション プール > Citrix Access Security Runtime Pool > 詳細設定**を選択します。



3. **Identity > ApplicationPoolIdentity** の項目にある編集アイコンをクリックしてください。



4. **カスタム アカウント:** で、**設定**をクリックします。



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。



次のステップ

- [ネットスケラー 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](#)

コンポーネント

以下は、一般的な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、これにより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、その他のデータも追跡します。これにより、ユーザーは複数のデバイス間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 provides a single secure point of access through the corporate firewall. For details about the integration of NetScaler Gateway with Secure Private Access, see [NetScaler Gateway](#).
- **Director:** (オプション) Directorを使用すると、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。DirectorとSecure Private Accessの統合の詳細については、[Secure Private Access integration with Director](#)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、[Secure Private Accessとのライセンスサーバー統合](#)を参照してください。
- **Web Studio:** (Optional) Citrix Secure Private Access is integrated into the Web Studio console to enable users seamlessly access the service through Web Studio. For details about the Secure Private Access integration with Web Studio, see [Secure Private Access integration with Web Studio](#).

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の設定を保存することをお勧めします。

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

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

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

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

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

注:

- 一時データを保存するには、NetScalerの/var/tmpフォルダーを使用することをお勧めします。
- ファイルがLF改行で保存されていることを確認してください。FreeBSDはCRLFをサポートしていません。
- `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M: bad interpreter: No such file or directory` というエラーが表示される場合、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. アップロードされたスクリプトを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機能を有効にし、スマートアクセスタグ送信の改善と、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ファイルに永続化されたSecure Private Accessプラグイン機能により、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、バッチコマンドを使用して新しいファイルから結果の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、またはステップ6で入力されたパラメータのいずれかが正しくない場合、コマンドは失敗する可能性があります。

8. すべてのコマンドが正常に完了したことを確認してください。

注:

エラーが発生した場合でも、NetScaler は残りのコマンドを実行し、リソースを部分的に作成/更新/バインドします。したがって、いずれかのパラメーター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、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。

仮想サーバーを追加する:

- tcpProfileName: nstcp_default_XA_XD_profile
- デプロイメントタイプ: ICA_STOREFRONT (`add vpn vserver` コマンドでのみ利用可能)
- ICAのみ: オフ
- dtls: 無効です

仮想サーバーを更新する:

- tcpProfileName: nstcp_default_XA_XD_profile
- ICAのみ: オフ

使用例:

仮想サーバーを追加するには:

```
add vpn vserver _SecureAccess_Gateway SSL 999.999.999.999 443 -Listenpolicy NONE  
-tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT
```

```
-vserverFqdn gateway.mydomain.com -authnProfile auth_prof_name -icaOnly OFF  
dtls: OFF
```

仮想サーバーを更新するには:

```
set vpn vsriver _SecureAccess_Gateway -icaOnly OFF
```

仮想サーバーの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。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` : オン
- `clientlessModeUrlEncoding` : 透過
- `SecureBrowse` : 有効
- `Storefronturl` : "https://storefront.mydomain.com"
- `sfGatewayAuthType` : ドメイン

例を次に示します:

セッションアクションを追加するには:

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

セッションアクションを更新するには:

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

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

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

```
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](#)
- [よくある質問: シトリックス セキュア ゲートウェイ/NetScaler Gateway 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はタグを自動的に送信します。スマートアクセスタグを取得するためにゲートウェイコールバックアドレスを使用する必要はありません。

- 13.1–48.47以降

- 14.1–4.42以降

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

Secure Private Access の切り替え設定を構成する方法

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	項目説明
<code>nsapimgr_wr.sh -ys</code> <code>call=ns_vpn_enable_spa_onprem</code>	オンプレミス展開でSecure Private Accessを有効にする
<code>nsapimgr_wr.sh -ys</code> <code>call=ns_vpn_disable_spa_onprem</code>	オンプレミス展開でSecure Private Accessを無効にする
<code>nsapimgr_wr.sh -ys</code> <code>ns_vpn_enable_spa_tcp_udp_apps=3</code>	TCP/UDPアプリを有効にする
<code>nsapimgr_wr.sh -ys</code> <code>ns_vpn_enable_spa_tcp_udp_apps=0</code>	TCP/UDPアプリを無効にする
<code>nsapimgr_wr.sh -ys</code> <code>call=toggle_vpn_enable_securebrowse_client_mode</code>	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
<code>nsapimgr -ys</code> <code>call=toggle_vpn_redirect_to_access_restricted_page_on_deny</code>	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。
<code>nsapimgr -ys</code> <code>call=toggle_vpn_use_cdn_for_access_restricted_page</code>	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 上でセキュア プライベート アクセス プラグイン設定を永続化する

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

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

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

```
nsapimgr_wr.sh -ys
```

```
call=toggle_vpn_redirect_to_access_restricted_page_on_deny
```

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

3. ファイルを保存します。

NetScalerが再起動されると、Secure Private Accessプラグイン設定が自動的に適用されます。

パブリックゲートウェイ証明書のアップロード

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

パブリックゲートウェイ証明書をアップロードするには、次の手順を実行します。

1. 管理者権限でPowerShellまたはコマンドプロンプトウィンドウを開きます。
2. 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NetScaler構成が無限に存在する可能性があります。
- Secure Private Accessが有効なVPN仮想サーバーでは、**ICA Proxy**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、ネットワークでいくつかの変更を行う必要があります。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を有効にする場合は、NetScalerがプライベートIPアドレスを使用してStoreFront™と通信することを確認してください。StoreFrontのプライベートIPアドレスを使用して、新しいStoreFront DNSレコードをNetScalerに追加する必要がある場合があります。

コンテキストタグを設定する

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

管理者は、アクセスポリシーにコンテキストタグ付きの条件を追加できます。Secure Private Accessプラグインのコンテキストタグは、認証済み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設定する

コンテキストタグの設定には、以下の大まかな手順が含まれます。

1. 従来のゲートウェイ事前認証ポリシーを設定する

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設定する

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、別のポリシーでアクセスを拒否するといった使い方ができます。



4. 必要なフィールドに詳細を入力し、**作成**をクリックします。
5. **式**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。



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。



6. **作成**をクリックします。

カスタムタグをNETSCALER GATEWAYにバインドする

1. **ネットスケーラー ゲートウェイ > 仮想サーバー**に移動します。
2. プリ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**でプリ認証ポリシーを選択し、**種類の選択**で**要求**を選択します。



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



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（例： `Windows10` ）を入力します。

参考文献

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

ストアフロント

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

ただし、Secure Private AccessがStoreFrontと共存していない場合は、特定の設定変更を手動で行う必要があります。

StoreFrontを手動で構成するには、次の手順を実行します。

1. Secure Private Access管理コンソール（**設定 > 統合**）からスクリプトをダウンロードします。
2. 設定変更を行うStoreFrontエントリに対応する**スクリプトのダウンロード**をクリックします。

ダウンロードしたzipファイルには、構成スクリプト、READMEファイル、および構成クリーンアップスクリプトが含まれています。クリーンアップスクリプトは、StoreFrontとSecure Private Access間の統合を削除する場合に使用できます。

3. PowerShell 64ビットインスタンスで、管理者として `./ConfigureStorefront.ps1` コマンドを使用してスクリプトを実行します。
 - 他のパラメーターは必要ありません。
 - 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**無制限**または**バイパス**に設定する必要があります。
 - StoreFrontがクラスターとして構成されている場合、スクリプトは構成を他のStoreFrontサーバーにも伝播します。

StoreFrontがSecure Private Access設定で構成されると、Secure Private Accessプラグインの構成はStoreFront管理UI（**デリバリーコントローラーの管理画面**）で確認できます。

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

重要:

- Secure Private AccessのStoreFrontを構成するには、Secure Private Access管理UIからダウンロードしたStoreFrontスクリプトのみを使用することをお勧めします。UIではStoreFrontに必要なすべての構成が網羅されていないため、StoreFront管理UIからSecure Private Accessを構成しないでください。必要なすべての構成を完了するには、スクリプトを実行する必要があります。
- 1つのSecure Private Accessサイトを、複数のStoreFront展開（同じStoreFront上の別のストア、または別のStoreFront展開のいずれか）にも構成できます。StoreFrontは、**設定 > 統合**ページから追加できます。
- Secure Private AccessがStoreFrontと共存している場合でも、StoreFrontの自動構成は**設定 > 統合**ページからは機能しません。自動構成は、初回セットアップ時にのみ実行されます。**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のURLは表示されません。
- Secure Private Accessポートは常に80として表示されます。

**StoreFrontバージョン2311以降を使用している場合**

StoreFrontバージョン2311以降では、Citrix Workspace™ for Webクライアントは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・フォー・ウェブ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 (オプション)

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の必須構成です。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、次の場合にも検証が失敗します。

- ディレクターはセキュア プライベート アクセス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が存在しない。

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、Integrated Windows Authentication (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、管理者は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、その詳細は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別のDirectorを追加する必要がある場合、**Manage Settings**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。

ディレクター構成ツールを使用して、セキュアプライベートアクセスでディレクターを構成する

Configツールを使用してDirectorをSecure Private Accessで構成することは、統合を完了するための必須手順です。詳細については、「[DirectorとSecure Private Accessの統合](#)」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 (オプション)

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 を介し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 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、シトリックス 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. After successful installation, navigate to the folder C:\Program Files\Citrix\Web Studio\Site\studio\assets\json and modify the content of the spa-config.json file.

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、ご使用のセキュアプライベートアクセスプラグインのFQDNに置き換えてください。
2. Web Studio にログインします。
3. 左側のナビゲーションメニューで、**Secure Private Access** をクリックして、Web Studio から Secure Private Access 管理コンソールにアクセスします。

HTTP/HTTPSアプリケーションを構成する

Secure Private Access をセットアップした後、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、ワークスペースのユーザーに表示されます。アプリケーションのキーワードを `KEYWORDS: <keyword_name>` の形式で入力することもできます。キーワードを使用してアプリケーションをフィルタリングできます。詳細については、「[含まれるキーワードでリソースをフィルタリングする](#)」を参照してください。
- - 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せん。管理者は正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UI の名前と 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、フィールドに「ビジネス・アンド・プロダクティビティ」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・アンド・プロダクティビティ」カテゴリに加えて、「ビジネス・アンド・プロダクティビティ」という新しいカテゴリがリストされます。
- **アプリのアイコン – アイコンの変更**をクリックして、アプリのアイコンを変更します。アイコンファイルのサイズは128x128ピクセルで、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。
- **ユーザーにアプリケーションを表示しない** - ユーザーにアプリを表示したくない場合は、このオプションを選択します。
- **URL** – アプリケーションのURL。
- **関連ドメイン** – 関連ドメインは、アプリケーションの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。

注：

- 。あるアプリの関連ドメインが、別のアプリの関連ドメインと重複しないようにしてください。重複が発生した場合は、すべてのアプリから関連ドメインを削除し、このドメインで新しいアプリを作成してから、アクセスポリシーでそれに応じてアクセスを設定します。このアプリをStoreFront™に表示するか、非表示にするかを検討することもできます。アプリを公開する際に、**ユーザーにアプリケーションを表示しないオプション**を使用して、StoreFrontでアプリを非表示にできます。
- 。同様に、公開されたアプリのURLを別のアプリの関連ドメインとして追加してはなりません。
- 。詳細については、[WebおよびSaaSアプリケーション構成のベストプラクティス](#)を参照してください。

- **アプリケーションをお気に入りへ自動追加** – 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、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** - 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。

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（HTTP/HTTPS）へのアクセスを制限することもできます。

1. 管理コンソールで、[ポリシー](#) をクリックします。
2. [ポリシー](#) をクリックします。



3. a. に、ポリシーの名前を入力します。
4. で、アクセスポリシーを適用するアプリを選択します。
5. – 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。
6. 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。
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。
 - **アクセスを許可**
 - **制限付きアクセスを許可**
 - **アクセスを拒否**

「制限付きアクセスを許可」を選択した場合、制限を選択するには「制限を追加」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. 「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 ポリシーの優先順位

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

値が小さい優先順位ほど優先度が高く、最初に評価されます。このポリシーが定義された条件と一致しない場合、次に優先順位番号が小さいポリシーが評価されます。

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

構成検証の例

アクセス制限オプション

アクション制限付きアクセスを許可を選択すると、要件に応じてセキュリティ制限を選択できます。これらのセキュリティ制限はシステムに事前定義されています。管理者は他の組み合わせを変更または追加することはできません。

アクセス制限(/ja-jp/citrix-secure-private-access/media/secure-private-access-multirule-access-restrictions-onprem.png)

クリップボード

Citrix Enterprise Browser経由でアクセスする場合、このアクセスポリシーを使用して、SaaSまたは社内Webアプリでの切り取り/コピー/貼り付け操作を有効/無効にします。デフォルト値: 有効。

コピー

Citrix Enterprise Browser経由でアクセスする場合、このアクセスポリシーを使用して、SaaSまたは社内Webアプリからのデータコピーを有効/無効にします。デフォルト値: 有効。

注:

- ポリシーでクリップボードとコピーの両方の制限が有効になっている場合、クリップボードの制限がコピーの制限よりも優先されます。
- エンドユーザーは、この制限が有効になっているアプリケーションにアクセスするために、Citrix Enterprise Browser™バージョン126以降を使用する必要があります。そうでない場合、アプリケーションアクセスは制限されます。
- アプリ内でのコピー操作をきめ細かく制御するには、管理者はセキュリティグループ制限を使用できます。詳細については、「[セキュリティグループのクリップボード制限](#)」を参照してください。

ファイルタイプによるダウンロード制限

Citrix Enterprise Browser経由でアクセスする場合、このポリシーを使用して、SaaSまたは社内Webアプリ内から特定のMIME（ファイル）タイプのダウンロード機能を有効/無効にします。

注:

- ファイルタイプによるダウンロード制限は、ダウンロード制限に加えて利用できます。
- 「ダウンロード」と「ファイルタイプによるダウンロード制限」の両方の制限がポリシーで有効になっている場合、「ダウンロード」制限は「ファイルタイプによるダウンロード制限」制限よりも優先されます。
- エンドユーザーは、この制限が有効になっているアプリケーションにアクセスするために、Citrix Enterprise Browserバージョン126以降を使用する必要があります。そうしないと、アプリケーションへのアクセスが制限されます。

MIMEタイプのダウンロードを有効にするには、次の手順を実行します。

1. アクセスポリシーを作成または編集します。アクセスポリシーの作成の詳細については、「[アクセスポリシーの構成](#)」を参照してください。
2. 「アクション」で、「制限付きで許可」を選択します。
3. 「ファイルタイプによるダウンロード制限」をクリックし、「編集」をクリックします。
4. 「ファイルタイプによるダウンロード制限設定」ページで、次のいずれかを選択します。
 - 「例外付きですべてのダウンロードを許可」 – ブロックする必要があるタイプを選択し、他のすべてのタイプを許可します。
 - 「例外付きですべてのダウンロードをブロック」 – アップロードできるタイプのみを選択し、他のすべてのタイプをブロックします。
5. ファイルタイプがリストにない場合は、次の操作を行います。
 - a. 「カスタムMIMEタイプを追加」をクリックします。
 - b. 「MIMEタイプの追加」で、`category/subcategory<extension>` の形式でMIMEタイプを入力します。例: `image/png`。
 - c. 「完了」をクリックします。

MIMEタイプが例外リストに表示されます。

エンドユーザーが制限されたファイルタイプをダウンロードしようとする、Citrix Enterprise Browserは次の警告メッセージを表示します。

ダウンロード (/ja-jp/citrix-secure-private-access/media/spa-download-restricted-file.png)

ダウンロード

Citrix Enterprise Browser経由でアクセスする場合、このポリシーを使用してSaaSまたは内部Webアプリ内からダウンロードするユーザーの機能を有効/無効にします。デフォルト値: 有効。

注:

ポリシーでダウンロードとファイルタイプによるダウンロード制限の両方の制限が有効になっている場合、ダウンロード制限はファイルタイプによるダウンロード制限よりも優先されます。

安全でないコンテンツ

Citrix Enterprise Browser経由でアクセスする場合、このポリシーで構成されたSaaSまたは内部Webアプリ内の安全でないコンテンツへのエンドユーザーのアクセスを有効/無効にします。安全

でないコンテンツとは、HTTPSリンクではなくHTTPリンクを使用してWebページからリンクされているファイルのことです。デフォルト値: 無効。

安全でないコンテンツの表示を有効にするには、次の手順を実行します。

1. **アクセスポリシーを作成または編集します。**アクセスポリシーの作成について詳しくは、「[アクセス**ポリシーの構成](#)」を参照してください。
2. **アクションで、制限付きで許可**を選択します。
3. **安全でないコンテンツをクリック**します。
4. **保存**をクリックし、**完了**をクリックします。

次の図は、安全でないコンテンツにアクセスしたときの通知の例を示しています。

ダウンロード (/ja-jp/citrix-secure-private-access/media/spaop-insecure-content.png)

キーロギング保護

Citrix Enterprise Browser経由でアクセスする場合、このアクセスポリシーを使用してSaaSまたは内部Webアプリからのキーストロークをキャプチャするキーロガーを有効/無効にします。デフォルト値: 有効。

マイク

Citrix Enterprise Browser経由でアクセスする場合、このポリシーで構成されたSaaSまたは内部Webアプリ内でマイクにアクセスするたびに、ユーザーにプロンプトを表示するかどうかを設定します。デフォルト値: 毎回プロンプトを表示。

マイク制限が有効になっているアプリケーションにアクセスするには、エンドユーザーはCitrix Enterprise Browserバージョン126以降を使用する必要があります。

プロンプトなしで常にマイクを許可するには、次の手順を実行します。

1. **アクセスポリシーを作成または編集します。**詳細については、「[アクセスポリシーの構成](#)」を参照してください。
2. **アクションで、制限付きで許可**を選択します。
3. **マイクをクリックし、編集**をクリックします。
4. **マイク設定ページで、常にアクセスを許可**をクリックします。
5. **保存**をクリックし、**完了**をクリックします。

注:

- Secure Private Accessポリシーで**マイク**制限が有効になっている場合、Citrix Enterprise Browserには**許可**の設定が表示されます。
- Secure Private Accessポリシーで**毎回プロンプトを表示**オプションが設定されている場合、Citrix Enterprise Browserに適用される設定は、Global App Configuration service (GACS) を使用してCitrix Enterprise Browserを管理しているかどうかによって異なります。
- GACSを使用している場合、GACS設定がCitrix Enterprise Browserに適用されます。
- GACSを使用していない場合、Citrix Enterprise Browserには**尋ねる**の設定が表示されます。
- 現在、Secure Private Accessはマイクのブロックをサポートしていません。マイクをブロックする必要がある場合は、GACSを介して行う必要があります。

GACS の詳細については、[グローバルアプリ構成サービスを介した Citrix Enterprise Browser の管理](#) を参照してください。

通知設定

Citrix Enterprise Browser経由でアクセスする場合、このポリシーで構成されたSaaSまたは社内Webアプリ内で通知を表示するたびに、ユーザーに許可/プロンプトを表示します。デフォルト値: 毎回プロンプトを表示する。

この制限が有効になっているアプリケーションにアクセスするには、エンドユーザーはCitrix Enterprise Browserバージョン126以降を使用する必要があります。

プロンプトなしで通知の表示をブロックするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。詳細については、「[アクセス ポリシーの構成](#)」を参照してください。
2. **アクション**で、**制限付きで許可**を選択します。
3. **通知**をクリックし、次に**編集**をクリックします。
4. **通知設定**ページで、**常に通知をブロック**をクリックします。
5. **保存**をクリックし、次に**完了**をクリックします。

貼り付け

Citrix Enterprise Browser経由でアクセスする場合、このアクセス ポリシーでSaaSまたは社内Web アプリへのコピーしたデータの貼り付けを有効/無効にします。デフォルト値: 有効。

注:

- ポリシーでクリップボードと貼り付けの両方の制限が有効になっている場合、**クリップボード**の制限が**貼り付け**の制限よりも優先されます。
- この制限が有効になっているアプリケーションにアクセスするには、エンドユーザーは Citrix Enterprise Browserバージョン126以降を使用する必要があります。そうでない場合、アプリケーションへのアクセスは制限されます。
- アプリ内での貼り付け操作をきめ細かく制御するには、管理者は**セキュリティグループ**の制限を使用できます。詳細については、「[セキュリティグループのクリップボード制限](#)」を参照してください。

個人データマスキング

Citrix Enterprise Browser経由でアクセスする場合、このポリシーを使用してSaaSまたは社内Web アプリ上の個人を特定できる情報 (PII) の編集またはマスキングを有効/無効にします。

注:

エンドユーザーは、この制限が有効になっているアプリケーションにアクセスするには、Citrix Enterprise Browserバージョン126以降を使用する必要があります。そうしないと、アプリケーションへのアクセスが制限されます。

個人を特定できる情報を編集またはマスキングするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。詳細については、「[アクセス ポリシーの構成](#)」を参照してください。
2. **アクション**で、**制限付きで許可**を選択します。
3. **個人データマスキング**をクリックし、**編集**をクリックします。
4. 隠蔽またはマスキングする情報タイプを選択し、**追加**をクリックします。

情報タイプが事前定義されたリストに表示されない場合は、カスタム情報タイプを追加できます。詳細については、「[カスタム情報タイプの追加](#)」を参照してください。

5. マスキングタイプを選択します。

- **完全マスキング** – 機密情報を完全に覆い、読み取れないようにします。
- **部分マスキング** – 機密情報を部分的に覆います。関連するセクションのみが覆われ、残りはそのまま残ります。

部分マスキングを選択すると、ドキュメントの先頭または末尾から始まる文字を選択する必要があります。**最初のマスキング文字フィールドと最後のマスキング文字フィールド**に数値を入力する必要があります。

プレビューフィールドにマスキング形式が表示されます。このプレビューはカスタムポリシーでは利用できません。

6. 保存をクリックし、次に完了をクリックします。

カスタム情報タイプを追加

情報タイプの正規表現を追加することで、カスタム情報タイプを追加できます。

1. **情報タイプの選択**で**カスタム**を選択し、次に**追加**をクリックします。
2. **フィールド名**に、マスクする情報タイプの名前を入力します。
3. **文字数**に、情報タイプの文字数を入力します。
4. ****正規表現 (RE2 ライブラリ)****に、カスタム情報タイプの式を入力します。例: `\^[0-9]{12}(?:[0-9]{3})?$`。
5. 情報全体、または最初または最後の数文字をマスクする場合は、マスキングタイプを選択します。
6. **保存**をクリックし、次に**完了**をクリックします。



次の図は、PII がマスクされているサンプルアプリを示しています。この図は、PII のマスキングに関連する通知も表示しています。



ポップアップ

Citrix Enterprise Browser 経由でアクセスされた場合、このポリシーで構成された SaaS または内部 Web アプリ内でのポップアップの表示を有効/無効にします。デフォルトでは、Web ページ内のポップアップは無効になっています。デフォルト値: 常にポップアップをブロックします。

この制限が有効になっているアプリケーションにアクセスするには、エンドユーザーは Citrix Enterprise Browser バージョン 126 以降を使用する必要があります。

ポップアップの表示を有効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。詳細については、「[アクセス ポリシーの構成](#)」を参照してください。
2. で、を選択します。
3. をクリックし、をクリックします。
4. ページで、をクリックします。
5. をクリックし、をクリックします。

印刷

Citrix Enterprise Browser 経由でアクセスする場合、このポリシーを使用して、構成済みの SaaS または内部 Web アプリからデータを印刷することを有効/無効にします。既定値: 有効。

印刷制限が有効になっているアプリケーションからエンドユーザーがコンテンツを印刷しようとすると、次のメッセージが表示されます。



注:

ポリシーで と の両方の制限が有効になっている場合、制限が 制限よりも優先されます。

プリンター管理

Citrix Enterprise Browser 経由でアクセスする場合、このポリシーを使用して、構成済みの SaaS または内部 Web アプリから管理者によって構成されたプリンターを使用してデータを印刷することを有効/無効にします。

注:

- 「**プリンター管理**」制限は、印刷が有効または無効になっている「**印刷**」制限に加えて利用できます。アクセス ポリシーで「**印刷**」制限と「**プリンター管理**」制限の両方が有効になっている場合、「**印刷**」制限が「**プリンター管理**」制限よりも優先されます。
- エンドユーザーは、この制限が有効になっているアプリケーションにアクセスするには、Citrix Enterprise Browser バージョン126以降を使用する必要があります。そうでない場合、アプリケーションへのアクセスは制限されます。

印刷制限を有効/無効にするには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。アクセス ポリシーの作成の詳細については、「[アクセス ポリシーの構成](#)」を参照してください。
2. アクションで、**制限付きで許可**を選択します。
3. **プリンター管理**をクリックし、次に**編集**をクリックします。



1. 要件に応じて例外を選択します。

- **ネットワークプリンター** - ネットワークプリンターとは、ネットワークに接続して複数のユーザーが使用できるプリンターです。
 - **無効**: ネットワーク内のすべてのプリンターからの印刷が無効になります。
 - **有効**: すべてのネットワークプリンターからの印刷が有効になります。プリンターのホスト名が指定されている場合、指定されたもの以外のすべてのネットワークプリンターはブロックされます。

注: ネットワークプリンターはホスト名で識別されます。

- **ローカルプリンター** - ローカルプリンターとは、有線接続を介して個々のコンピューターに直接接続されたデバイスです。この接続は通常、USB、パラレルポート、またはその他の直接インターフェイスを介して行われます。
 - **無効**: すべてのローカルプリンターからの印刷が無効になります。
 - **有効**: すべてのローカルプリンターからの印刷が有効になります。
- **PDFとして保存して印刷**
 - **無効**: アプリケーションのコンテンツをPDF形式で保存することは無効になっています。
 - **有効**: アプリケーションのコンテンツをPDF形式で保存することは有効になっています。

2. **保存**をクリックします。

ネットワークプリンターが無効になっている場合、**宛先**フィールドでプリンターを選択しようとすると、その特定のプリンター名がグレー表示されます。

また、**PDFとして保存して印刷**が無効になっている場合、**宛先**フィールドの**詳細を表示**リンクをクリックすると、**PDFとして保存**オプションがグレー表示されます。

印刷 3(/ja-jp/citrix-secure-private-access/media/spa-print-restriction-pdf.png)

画面キャプチャ

Citrix Enterprise Browser経由でアクセスするSaaSまたは内部Webアプリから、このポリシーを使用して、任意の画面キャプチャプログラムまたはアプリで画面をキャプチャする機能を有効/無効にします。ユーザーが画面をキャプチャしようとする、空白の画面がキャプチャされます。デフォルト値: 有効。

ファイルタイプによるアップロード制限

Citrix Enterprise Browser経由でアクセスするSaaSまたは内部Webアプリから、このポリシーを使用して、特定のMIME（ファイル）タイプのダウンロードをユーザーが実行できる機能を有効/無効にします。

注:

- ファイルタイプによるアップロード制限は、アップロード制限に加えて利用可能です。
- ポリシーでアップロードとファイルタイプによるアップロード制限の両方が有効になっている場合、アップロード制限がファイルタイプによるアップロード制限よりも優先されます。
- この制限が有効になっているアプリケーションにアクセスするには、エンドユーザーはCitrix Enterprise Browserバージョン126以降を使用する必要があります。そうでない場合、アプリケーションへのアクセスは制限されます。

MIMEタイプのアップロードを有効/無効にするには、次の手順を実行します。

1. アクセスポリシーを作成または編集します。詳細については、[アクセスポリシーの作成](#)を参照してください。
2. で、を選択します。
3. をクリックし、をクリックします。
4. ページで、次のいずれかを選択します。

– 選択した種類を除くすべてのファイルをアップロードします。 – 選択した種類を除くすべてのファイルタイプのアップロードをブロックします。

5. ファイルの種類がリストにない場合は、次の手順を実行します。
 - a. をクリックします。
 - b. で、`category/subcategory<extension>` の形式でMIMEタイプを入力します。例:
`image/png`。

c. をクリックします。

MIMEタイプが例外のリストに表示されます。

エンドユーザーが制限されたファイルタイプのアップロードを試みると、Citrix Enterprise Browserに警告メッセージが表示されます。



アップロード

Citrix Enterprise Browser経由でアクセスする場合、このポリシーで構成されたSaaSまたは内部Webアプリ内でのユーザーのアップロード機能を有効/無効にします。デフォルト値: 有効。

注記:

ポリシーで「アップロード」と「ファイルタイプによるアップロード制限」の両方の制限が有効になっている場合、「アップロード」制限が「ファイルタイプによるアップロード制限」制限よりも優先されます。

透かし

ユーザーの画面に、ユーザー名とユーザーのマシンのIPアドレスを表示する透かしを有効/無効にします。デフォルト値: 無効。

Webカメラ

Citrix Enterprise Browser経由でアクセスする場合、このポリシーで構成されたSaaSまたは内部Webアプリ内でWebカメラにアクセスするたびに、ユーザーにプロンプトを表示するかどうかを設定します。デフォルト値: 毎回プロンプトを表示。

「**Webカメラ**」制限が有効になっているアプリケーションにアクセスする場合、エンドユーザーはCitrix Enterprise Browserバージョン126以降を使用する必要があります。

プロンプトなしで常にWebカメラを許可するには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。詳細については、「[アクセス ポリシーの構成](#)」を参照してください。
2. 「アクション」で、「制限付きで許可」を選択します。
3. 「Webカメラ」をクリックし、「編集」をクリックします。
4. 「Webカメラ設定」ページで、「常にアクセスを許可」をクリックします。
5. 「保存」をクリックし、「完了」をクリックします。

注記:

- Secure Private AccessポリシーでWebカメラ制限が有効になっている場合、Citrix Enterprise Browserは「許可」の設定を表示します。
- Secure Private Accessポリシーで**毎回プロンプトを表示**オプションが選択されている場合、Citrix Enterprise Browserに適用される設定は、Global App Configuration service (GACS) を使用してCitrix Enterprise Browserを管理しているかどうかによって異なります。
- GACSを使用している場合、GACS設定がCitrix Enterprise Browserに適用されます。
- GACSを使用していない場合、Citrix Enterprise Browserは**尋ねる**設定を表示します。
- 現在、Secure Private Accessはウェブカメラのブロックをサポートしていません。ウェブカメラをブロックする必要がある場合は、GACSを通じて行う必要があります。

GACS の詳細については、「[グローバルアプリ構成サービスを介した Citrix Enterprise Browser の管理](#)」を参照してください。

セキュリティグループのクリップボード制限

セキュリティグループ制限（アプリケーション > セキュリティグループ）を使用して、指定されたアプリのグループに対してクリップボードアクセスを有効にできます。セキュリティグループには、コピー & ペースト操作を実行できる一連のアプリが割り当てられます。セキュリティグループ内のアプリでクリップボードアクセスを有効にするには、アクセス設定を選択せずに、アクションが許可または制限付きで許可に設定されたアクセスポリシーを構成するだけで済みます。

- セキュリティグループ制限が有効になっている場合、異なるセキュリティグループ内のアプリケーション間でデータをコピー/ペーストすることはできません。たとえば、アプリ「ProdDocs」がセキュリティグループ「SG1」に属し、アプリ「Edocs」がセキュリティグループ「SG2」に属している場合、両方のグループでコピー/ペースト制限が有効になっていても、「Edocs」から「ProdDocs」にコンテンツをコピー/ペーストすることはできません。
- セキュリティグループの一部ではないアプリの場合、アクションが**制限付きで許可**に設定され、制限（コピー、ペースト、またはクリップボード）が選択されたアクセスポリシーを作成できます。この場合、アプリはセキュリティグループの一部ではないため、そのアプリにコピー/ペースト制限を適用できます。

注：

Global App Configuration service (GACS) を介してCitrix Enterprise Browser経由でアクセスされるアプリのクリップボードアクセスを制限することもできます。GACSを使用してCitrix Enterprise Browserを管理している場合は、**サンドボックス化されたクリップボードを有効にする**オプションを使用してクリップボードアクセスを管理します。GACSを通じてクリップボードアクセスを制限すると、Citrix Enterprise Browser経由でアクセスされるすべてのアプリに適用されます。GACSの詳細については、「[Global App Configuration service を介した Citrix Enterprise Browser の管理](#)」を参照してください。

セキュリティグループを作成するには、次の手順を実行します。

1. Secure Private Accessコンソールで、**アプリケーション**をクリックし、次に**セキュリティグループ**をクリックします。
2. **新しいセキュリティグループを追加**をクリックします。



1. セキュリティグループの名前を入力します。
2. **WebまたはSaaSアプリケーションを追加**で、コピー＆ペースト制御を有効にするためにグループ化したいアプリケーションを選択します。例えば、Wikipedia、Pinterest、Dribbleなどです。
3. 「**保存**」をクリックします。

高度なクリップボード設定の詳細については、「[ネイティブアプリケーションおよび未公開アプリケーションのコピー/貼り付けコントロールを有効にする](#)」を参照してください。

エンドユーザーがCitrix Workspaceからこれらのアプリケーション（Wikipedia、Pinterest、Dribble）を起動する場合、セキュリティグループ内のアプリケーション間でデータを共有（コピー/貼り付け）できる必要があります。コピー/貼り付けは、アプリケーションに対してすでに有効になっている他のセキュリティ制限とは関係なく行われます。

ただし、エンドユーザーは、自分のマシン上のローカルアプリケーションや未公開アプリケーションから、これらの指定されたアプリケーションにコンテンツをコピーして貼り付けることはできません。また、その逆もできません。指定されたアプリケーションから別のアプリケーションにコンテンツがコピーされると、次の通知が表示されます。



注:

ユーザーマシン上のローカルアプリケーションまたは未公開アプリケーションからのコンテンツのコピー/貼り付けコントロールは、「**高度なクリップボード設定**」セクションのオプションを使用して有効にできます。詳細については、「[ネイティブアプリケーションおよび未公開アプリケーションのコピー/貼り付けコントロールを有効にする](#)」を参照してください。

詳細なレベルのコピー/貼り付けを有効にする

指定されたグループ内のアプリケーションに対して、詳細なレベルのクリップボードアクセスを有効にできます。これは、アプリケーションのアクセスポリシーを作成し、要件に応じて「**コピー**」/「**貼り付け**」制限を有効にすることで実現できます。

「

注:

詳細なレベルのクリップボードアクセス用に作成した特定のアクセスポリシーが、セキュリティグループ用に作成したポリシーよりも高い優先順位を持つようにしてください。

「例:」

Wikipedia、Pinterest、Dribbbleという3つのアプリケーションを含むセキュリティグループを作成したとします。

ここで、WikipediaまたはDribbbleからPinterestへのコンテンツの貼り付けを制限したいとします。そのためには、次の手順を実行します。

1. アプリケーションに割り当てられたアクセスポリシーを作成または編集します **Pinterest**。
アクセスポリシーの作成の詳細については、「[アクセスポリシーを構成する](#)」を参照してください。
2. 「**アクション**」で、「**制限付きで許可**」を選択します。
3. 「**貼り付け**」を選択します。

PinterestはWikipediaとDribbbleも含むセキュリティグループの一部ですが、Pinterestに関連付けられているアクセスポリシーで「**貼り付け**」制限が有効になっているため、ユーザーはWikipediaまたはDribbbleからPinterestにコンテンツをコピーできません。

貼り付けエラー2(/ja-jp/citrix-secure-private-access/media/spa-printing-block-example.png)

ネイティブアプリケーションおよび未公開アプリのコピー/貼り付けコントロールを有効にする

1. セキュリティグループを作成します。詳細については、「[コピーと貼り付けの制限のためのクリップボードセキュリティグループ](#)」を参照してください。
2. 「高度なクリップボード設定」を展開します。

詳細オプション(/ja-jp/citrix-secure-private-access/media/spa-security-group-advanced-settings.png)

3. 要件に応じて、次のオプションを選択します。
 - **セキュリティグループから未公開ドメインへのデータコピーを許可する** – セキュリティグループ内のアプリケーションから、Secure Private Accessで公開されていないアプリへのデータコピーを有効にします。
 - **セキュリティグループからネイティブアプリへのデータコピーを許可する** – セキュリティグループ内のアプリケーションから、お使いのマシンのローカルアプリケーションへのデータコピーを有効にします。
 - **未公開ドメインからセキュリティグループへのデータコピーを許可する** – Secure Private Accessを介して公開されていないアプリから、セキュリティグループ内のアプリケーションへのデータコピーを有効にします。
 - **ネイティブアプリのオペレーティングシステムからセキュリティグループへのデータコピーを許可する** – マシン上のローカルアプリケーションからアプリケーションへのデータコピーを有効にします。

既知の問題

- (設定 > アプリケーションドメイン) のルーティングテーブルは、削除されたアプリケーションのドメインを保持します。そのため、これらのアプリケーションもSecure Private Accessで公開されたアプリケーションと見なされます。これらのドメインがCitrix Enterprise Browserから直接アクセスされた場合、「高度なクリップボード設定」で選択したオプションに関係なく、これらのアプリケーションからのコピー/貼り付けは無効になります。

例えば、次のシナリオを想定してください。

- セキュリティグループの一部であったJira2 (<https://test.citrite.net>) という名前のアプリケーションを削除しました。
- オプション「セキュリティグループから未公開ドメインへのデータコピーを許可する」を有効にしました。

このシナリオでは、ユーザーがこのアプリケーションから同じセキュリティグループ内の別のアプリケーションにデータをコピーしようとする、貼り付けコントロールが無効になります。その旨の通知がユーザーに表示されます。

- SaaSアプリの場合、アプリケーションがアクション「**アクセス拒否**」のアクセスポリシーで構成されていると、アプリへのアクセスが拒否されることがあります。エンドユーザーは、アプリのトラフィックがSecure Private Accessを介してトンネルされないため、引き続きアプリにアクセスできます。また、アプリケーションがセキュリティグループの一部である場合、セキュリティグループの設定は尊重されず、そのためアプリケーションからコンテンツをコピー/貼り付けすることはできません。

Secure Private Accessをクラスターとして展開する（オプション）

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（たとえば、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。
- Secure Private Accessサイトに必要な数のクラスターノードを追加します。詳細については、「[既存のサイトに参加してSecure Private Accessをセットアップする](#)」を参照してください。
- 各Secure Private Accessノードで、同じサーバー証明書を構成します。証明書のサブジェクト共通名またはサブジェクト代替名は、ロードバランサーのFQDNと一致する必要があります。
- 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、** [Integrations] **タブでデータベースアドレスを指定し、データベーススクリプトを手動で実行します。スクリプトを使用してデータベースをアップグレードする方法の詳細については、「[スクリプトを使用してデータベースをアップグレードする](#)」を参照してください。



ロードバランサーの構成

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

- StoreFrontへのアクセスに使用されるFQDNは、サブジェクト代替名（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による負荷分散](#)」を参照してください。Secure Private Accessを構成する前に、StoreFrontストアを構成する必要があります。ロードバランサーを使用する場合は、ベースURL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でStoreFrontを保護する](#)」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。さらに、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る。
- セキュアな暗号が使用されている。
- 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のHTTPベースのモニター（プローブ）を構成する必要がある場合は、次のエンドポイントを使用できます。

```
/secureAccess/health
```

期待される応答:

```
Http status code: 200 OK
```

```
Payload:
```

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

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

セキュアプライベートアクセスのモニターを作成する

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. Citrix バーチャルアプリとデスクトップ™ 7 2405 – 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オンします。
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 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 マシンにログオンします。
2. StoreFrontScripts.zip という名前のファイルをダウンロードします。
3. StoreFrontScripts.zip を任意のフォルダーに展開してください。
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されたSecure Private Accessプラグインをアップグレードします。

アップグレードシーケンス

アップグレードシーケンスは次のとおりです。

1. Secure Private Accessを最初にインストールした方法に基づいて、Delivery Controller™を介して、またはインストーラーUIの専用のSecure Private Accessタイルを介してSecure Private Accessをアップグレードできます。
 - Delivery Controllerを介してSecure Private Accessを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。ただし、本番環境では、新しい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-secure-private-access/spa-onprem-standalone/>` からシトリックス セキュア プライベート アクセス 2405 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。

**重要:**

インストーラーをリリース 2405 にアップグレードした後、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プラグインのデータベースアップグレードスクリプトをダウンロードできます。

1. PowerShellまたはコマンドプロンプトウィンドウを管理者権限で開きます。
2. 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. **設定 > アプリケーションドメイン**をクリックします。
2. 必要に応じて、編集アイコンをクリックしてルーティングタイプを変更できます。

管理者の管理

設定 > 管理者ページから、管理者のリストを表示したり、管理者を追加したりできます。Secure Private Accessを初めてインストールした管理者には、完全な権限が付与されます。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許可することもできます。

1. **管理者**ページで、**追加**をクリックします。
2. **ドメイン**で、この管理者を追加するドメインを選択します。

3. **ユーザーまたはユーザーグループ**で、このユーザーが属するユーザーまたはグループを選択します。
4. **管理者タイプ**で、このユーザーに割り当てる権限タイプを選択します。

統合設定の変更

Secure Private Accessをセットアップした後、**統合**タブからStoreFront™およびNetScaler Gatewayのエントリを変更または更新できます。

1. **設定 > 統合**をクリックします。
2. 変更したい設定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、必要に応じてそれらを編集できます。

アプリケーションを編集する

1. Secure Private Access 管理コンソールで、**アプリケーション**をクリックします。
2. 変更したいアプリケーションの行にある省略記号ボタンをクリックし、**アプリケーションの編集**をクリックします。
3. アプリの詳細を編集します。
4. **保存**をクリックします。

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

アクセスポリシーを編集する

1. Secure Private Access 管理コンソールで、**アクセスポリシー**をクリックします。
2. 変更したいポリシーの行にある省略記号ボタンをクリックし、**アクセスポリシーの編集**をクリックします。

3. ポリシーの詳細を編集します。
4. **更新**をクリックします。

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

承認されていないWebサイト

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

アプリが構成されていない他のすべてのインターネットURLまたはSaaSアプリケーションについては、管理者は管理コンソールの**設定 > 承認されていないWebサイト**タブを使用して、Citrix Enterprise Browser経由でのアクセスを許可または拒否できます。

注：

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

承認されていないWebサイトの仕組み

1. URL分析チェックが実行され、そのURLがCitrix®サービスURLであるかどうか判断されます。
2. 次に、URLがチェックされ、それがエンタープライズWebまたはSaaSアプリのURLであるかどうか判断されます。
3. 次に、URLがチェックされ、それがブロックされたURLとして識別されるか、またはアクセスが許可されるURLであるかどうか判断されます。

次の図は、エンドユーザーのトラフィックフローを示しています。

エンドユーザーのトラフィックフロー(/ja-jp/citrix-secure-private-access/media/website-filtering-onprem.png)

リクエストが到着すると、次のチェックが実行され、対応するアクションが実行されます。

1. リクエストはグローバル許可リストと一致しますか？
 - a. 一致する場合、ユーザーは要求されたWebサイトにアクセスできます。

- b. 一致しない場合、Webサイトリストがチェックされます。
2. リクエストは設定されたウェブサイトリストと一致しますか？
- a. 一致する場合、次のシーケンスによってアクションが決定されます。
- ブロック
 - 許可
- b. 一致しない場合、デフォルトのアクション (許可) が適用されます。デフォルトのアクションは変更できません。

未承認ウェブサイトのルールを構成する

1. Secure Private Access 管理コンソールで、> をクリックします。

注:

- Webフィルタリング機能はデフォルトで有効になっており、すべての未承認インターネットURLへのアクセスが許可されています。
- 設定を**すべてのユーザーが未承認ウェブサイトアクセスするのをブロックする**に変更することで、Citrix Enterprise Browserを介したすべてのユーザーによる任意のインターネットURLへのアクセスをブロックできます。



特定のURLの設定は、ブロックされたウェブサイトまたは許可されたウェブサイトを追加することで変更することもできます。

たとえば、デフォルトですべての未承認URLへのアクセスをブロックしているが、特定のいくつかのインターネットURLへのアクセスのみを許可したい場合は、次の手順を実行することで可能です。

- タブをクリックし、をクリックします。
- アクセスを許可する必要があるウェブサイトアドレスを追加します。ウェブサイトアドレスを手動で追加するか、ウェブサイトアドレスを含むCSVファイルをドラッグアンドドロップすることができます。
- 「URLを追加」をクリックし、次に「保存」をクリックします。

URLが許可されたWebサイトのリストに追加されます。

エンドユーザーフロー

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™ アプリケーションを使用して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、**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を確認する必要があります。また、エンドユーザーがOffice365アプリケーションからデータを印刷しようとする、印刷制限メッセージがユーザーに表示される必要があります。



注:

管理者は、仮想デスクトップおよびアプリケーションにアクセスするために必要なアカウント情報をユーザーに提供する必要があります。詳細については、[Citrix Workspace アプリにストア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](#)」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、以下の問題に遭遇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
- 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接続できません

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](#)」を参照してください。

Director 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 のセットアップにおけるすべてのコンポーネントからの問題が Director に取り込まれるため、効果的なパフォーマンス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。

参考資料

- [ディレクターとセキュアプライベートアクセスの構成](#)
- [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

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でログを表示できます。**フィルターの追加オプション**を使用して、アプリカテゴリ、ユーザー名、トランザクションIDなどのさまざまな条件に基づいて検索を絞り込むことができます。たとえば、検索フィールドで「Transaction-ID」、「= (特定の値に等しい)」、および「7456c0fb-a60d-4bb9-a2a2-edab8340bb15」をこの順序で選択して入力すると、このトランザクションIDに関連するすべてのログを検索できます。

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



フィルターの追加オプションを使用して、検索を絞り込むには、次の検索演算子を使用できます。

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

たとえば、検索フィールドで文字列 **Event-Type > = (特定の値に等しい) > Enumeration** を使用して、イベントタイプ「Enumeration」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 > ~ (特定の値を含む) > operator** を使用します。この検索では、「operator」という用語を含むすべてのユーザー名が一覧表示されます。たとえば、「local operator」、「admin operator」などです。

トランザクションIDを使用して、単一のイベントに関連するすべてのログを検索できます。トランザクションIDは、アクセス要求のすべてのSecure Private Accessログに関連付けます。1つのアプリアクセス要求に対して、認証から始まり、アプリの列挙、そしてアプリアクセス自体に至るまで、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に関連付けるために使用されます。トランザクションIDを使用して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。



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(/ja-jp/citrix-secure-private-access/2405/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

セキュアプライベートアクセスサーバーに到達不能(/ja-jp/citrix-secure-private-access/2405/spa-onprem-troubleshooting#secure-private-access-server-not-reachable)

その他

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に設定を更新する際に発生する可能性があります。

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

データベース作成エラー

- **エラーメッセージ:** データベース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。

- スクリプトを使用してデータベースを手動でセットアップすることを選択し（「データベースの構成」ページで「手動構成」を選択）、その後「自動構成」オプションに変更したが、同じサイト名を使用した場合。この場合、スクリプトの実行中に同じ名前のデータベースが既に作成されています。

解決策: サイトの名前を変更し、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:

- マシンからのデータベースネットワーク接続を確認します。ファイアウォールで SQL Server ポートが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 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サーバーを使用している場合は、マシンIDに正しいロール（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。

ストアフロント™ の障害

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

StoreFrontエントリが表示されない場合は、**設定**タブから更新してください。ウィザードを使用してSecure Private Accessを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、統合タブをクリックします。
 - b. **StoreFrontストアURL**で、StoreFrontエントリが表示されない場合は追加します。
- エラーメッセージ: StoreFrontエントリの構成に失敗しました: `<Store URL>`

解決策:

- a. PowerShellの実行ポリシーに制限がある可能性があります。詳細については、PowerShell スクリプトコマンド `Get-ExecutionPolicy` を実行してください。
- b. 制限されている場合は、これをバイパスして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、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を使用してこの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。

注記:

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をセットアップした後、設定タブからゲートウェイエントリを編集できます。このエラーが発生したStoreFront Store URLをメモしておきます。

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、統合タブをクリックします。

- b. ストアフロント ストア URL で、エラーが発生したストアフロント URL エントリを特定します。
- c. このStore URLの横にある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。

注記:

ストアフロントの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。ストアフロントスクリプトはWindows PowerShell (x86)と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、Windows x64互換のPowerShellウィンドウを管理者権限で開き、`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: `<Gateway URL>` のゲートウェイエントリの作成に失敗しました。または、`<Callback Gateway URL>` の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。

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をメモしてください。ウィザードを使用してSecure Private Accessを設定した後、**設定**タブから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. 障害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と仮想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:

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

また、デフォルトのIISサイト `"Default Web Site"` が稼働していることを確認します。

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ます。

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

解決策: 「[Secure Private AccessのSQLデータベース権限](#)」を参照してください。

ゲートウェイ接続チェックに失敗しました。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:

- 構成ツールを使用して、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 のインストールフォルダー内に格納されている Admin\AdminConfigTool フォルダーへと、現在の作業ディレクトリを移動または変更してください（例: cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool"）
- 次のコマンドを実行します。

```
.\AdminConfigTool.exe /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は中断されます。

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場合があります。

解決策:

license_serverテーブルを手動でクリーンアップします。

Secure Private Access診断サポートバンドルを作成する

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 のインストールフォルダー内に格納されている Admin\AdminConfigTool フォルダーへと、現在の作業ディレクトリを移動または変更してください（例: cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool"）。
- 次のコマンドを実行します。

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

セキュアプライベートアクセスの SQL データベース権限

データベースの自動作成の場合、Secure Private Access プラグインホストマシンは、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ためのアクセス許可が必要です。

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、以下の手順を実行します。

1. 名前構文 `CitrixAccessSecurity<Site Name>` で空のデータベースを作成します。ここで、`<Site Name>` はセキュアプライベートアクセス 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、以下の手順を実行します。

1. 名前構文 `CitrixAccessSecurity<Site Name>` を使用して空のデータベースを作成します。ここで、`<Site Name>` は Secure Private Access のサイト名です。(例: `CitrixAccessSecuritySPA`)。

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

2. `NT AUTHORITY\SYSTEM` ユーザー用に SQL Server ログインを作成します。ログインがすでに作成されている場合は、この手順を無視できます。

```
USE CitrixAccessSecurity<SiteName>
```

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

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

```
USE CitrixAccessSecurity<SiteName>
```

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

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

データベースを手動で作成すると、ダウンロードされたデータベーススクリプトがマシンIDに権限を追加します。

トラブルシューティングログの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。

トラブルシューティングログのログレベルを変更するには、ランタイムサービスの appsettings.json ファイル（C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService）内で、`TroubleshootingSql` の `restrictedToMinimumLevel` を以下のいずれかの値に更新してください。

- Information
- Debug
- Warning
- Error

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

}

アプリケーション起動 / Citrix Secure Access ログイン失敗

Netscaler Gateway 証明書がローテーションされると、アプリケーションの起動または Citrix Secure Access ログインが失敗します。

解決策: Secure Private Access管理コンソールで証明書を更新します。

1. **設定 > 統合**に移動します。
2. **Public NetScaler Gateway address**セクションで、**証明書の更新**をクリックします。

更新が完了するまでに数分かかる場合があります。

詳細については、統合設定の変更を参照してください。

Directorでの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で捕捉されるため、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。以下の表に、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](#)

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	項目の説明
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	セッションが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	項目の説明
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。

コード	ステータス	項目の説明
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	一部のアプリは拒否され、その他は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。
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	アプリケーションのポリシー詳細の取得エラー。
3000	許可	アプリケーション列挙は許可されています。
3001	拒否	アプリケーション列挙はポリシーによって拒否されています。
3002	拒否	ポリシーが一致しなかったため、アプリケーションは列挙されませんでした。

コード	ステータス	項目の説明
3003	不明	アプリケーション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	説明文
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	アプリの起動が許可されています。
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。

SIEM統合

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

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

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

イベントID	まとめ	説明	接続元
4738	ユーザーアカウント が変更されました	新しいSecure Private Access管理 者が更新したときに 作成されたイベント	Citrix Access Security Adminサー ビス
4726	ユーザーアカウント が削除されました	新しいSecure Private Access管理 者が削除されたとき に作成されたイベン ト	Citrix Access Security Adminサー ビス
8001	ユーザーのセキュ ア・アクセス・セッ ション	エンドポイントで ユーザーセッション が開始または終了し たときに作成される イベント。ユー ザー、セッション、 デバイスの詳細、 セッション中にアク セスした内部ドメイ ンと外部ドメインが 含まれます	Citrix Access Security Adminサー ビス
8002	ユーザーアクセス承 認リクエスト	Secure Private Access プラグイン がリソースへのアク セスを承認したとき に作成されるイベン ト。リソースの FQDN と承認決定が 含まれます	Citrix Access Security Adminサー ビス

参照ドキュメント

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

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。合計ログ数が多すぎる場合（たとえば100,000を超える場合）、90日より前の最も古いログを削除できます。クリーンアップジョブは、デフォルトで12時間ごとに実行されます。ランタイムサービスが再起動するたびに、このジョブも実行されます。

トラブルシューティングログの保持設定をカスタマイズする

ログのクリーンアップは、ランタイムサービスのインストールフォルダーにあるappsettings.json ファイルを通じて設定できます。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てください。

appsettings.jsonファイルに関するサンプル：

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

クリーンアップを無効にするには、必要に応じて次の設定を構成します。

- 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、管理者サービスとランタイムサービスのインストールフォルダ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。管理者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管理者サービスと同じように機能しますが、一度に最大600個のより多くのファイルを保持できます。

CDFログのカスタムクリーンアップ

CDFログのクリーンアップは、管理者サービスとランタイムサービスのインストールフォルダーにある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ファイルで次のエントリを更新します。

```
"CdfFile": {  
  
    "fileSizeLimitBytes": 10485760, // 10 MB
```

```
"retainedFileCountLimit": 600  
  
}
```

注：

サイトにSecure Private Accessの複数のインスタンスが設定されている場合は、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 (オンプレミス向け)