Citrix Secure Private Access-オンプレミス

Machine translated content

Disclaimer

Contents

新機能

June 19, 2024

2023 年 **12** 月

オンプレミス向け **Citrix Secure Private Access** —一般提供

オンプレミス向け Citrix Secure Private Access は、Citrix Virtual Apps and Desktops 2311 リリースの一部として一般提供されるようになりました。Citrix Secure Private Access オンプレミスソリューションは、StoreFront を Web アプリや SaaS アプリへの統合アクセスポータルとして、また Citrix Workspace の統合部分としての仮想アプリやデスクトップを使用して、ブラウザベースのアプリ（社内 Web アプリと SaaS アプリ）にゼロトラストネットワークアクセスを簡単に提供できるようにすることで、組織の全体的なセキュリティとコンプライアンス体制を強化します。このソリューションは、NetScaler および StoreFront の既存リリースと互換性があり、バージョンを変更する必要はありません。詳細については、「オンプレミスの Secure Private Access」を参照してください。

Citrix Virtual Apps and Desktops 搭載の統合 **Secure Private Access** インストーラー

Secure Private Access インストーラーは Desktop Delivery Controller (DDC) と統合され、コマンドラインと GUI を使用してインストールできるようになりました。詳細については、「コアコンポーネントのインストール」を参照してください。

既知の問題

June 19, 2024

オンプレミス向け Citrix Secure Private Access ソリューションには、次の既知の問題があり、将来のリリースで対処される予定です。

ドメインコントローラーの構成

- 異なる AD フォレストにまたがるドメイン間の信頼タイプを「フォレスト」とする一方向または双方向の信頼はサポートされていません。

  たとえば、a.com ドメインと b.com ドメインが 2 つの異なる AD フォレストにあり、ドメインが a.com/b.com に参加しているマシンに SPA がインストールされている場合、他のドメインユーザーは SPA 公開アプリにアクセスできません。

- オンプレミスの Secure Private Access がインストールされているマシンのドメインが、Secure Private Access にログインしている管理者のドメインと異なる場合は、以下を実行する必要があります。
  - Secure Private Access Admin と Runtime サービスの両方の IIS アプリケーションプールに、ID として別のドメインサービスアカウントを追加します。
- 代替 UPN サフィックスは、イントラネット（StoreFront）ログインおよびインターネット/エクストラネット（ゲートウェイ）アプリ列挙用の Secure Private Access ではサポートされていません。
- 分散グループは Secure Private Access ではサポートされていません。そのため、ポリシーでは分散グループを検索してユーザーとグループの条件を追加することはできません。
- Secure Private Access は、管理コンソールまたはサービスにドメインの詳細をキャプチャしません。したがって、ユーザーが提供したドメインに完全に依存します。したがって、対応するドメインにアクセスできない場合、またはドメイン名が有効な名前でない場合、そのドメインはサポートされません。

NetScaler Gateway

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

- お客様は NetScaler Gateway 13.1–48.47 以降または 14.1–4.42 以降を使用しています。
- `ns_vpn_enable_spa_onprem` トグルは有効になっています。

回避方法:

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

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

RFWeb/Workspace for web

RFWeb/ウェブ用ワークスペースはサポートされていません。アプリは列挙されていますが、アプリの起動が失敗する可能性があります。

アプリケーションアイコン

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

管理者管理

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

アップグレード

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

StoreFront

- 「ストア」**>**「統合エクスペリエンスの設定」で、<StoreName>Web サイトのデフォルトレシーバーを/Citrix/Web に設定する必要があります。以前のバージョンの StoreFront では、Web サイトのデフォルトレシーバーは空白の値に設定されており、Secure Private Access では機能しません。また、以前のバージョンの Receiver UI がクライアントに表示されます。
- StoreFront バージョン 2308 以前を使用している場合、［ストア］**>**［**Delivery Controller** の管理］ページには、［Secure Private Access］プラグインの種類が **XenMobile** として表示されます。これは機能には影響しません。

ログ

- クラスターのサポートバンドルの生成はサポートされていません。
- 管理サービスとランタイムサービスのログフォルダは削除しないでください。これらのフォルダを削除すると、Secure Private Access は再作成できません。

Secure Private Access をインストールするための管理者アカウント要件

- Secure Private Access をインストールするには、ローカルマシンの管理者アカウントでログインする必要があります。
- Secure Private Access を設定するには、Secure Private Access がインストールされているマシンのローカルマシン管理者でもあるドメインユーザーで Secure Private Access 管理コンソールにサインインする必要があります。
- セットアップが完了すると、そのユーザーは最初の Secure Private Access 管理者になり、他の管理者を追加できます。
- セットアップ後に Secure Private Access を管理するには、Secure Private Access 管理者アカウントで Secure Private Access 管理コンソールにサインインする必要があります。

セキュリティ制限

最初に公開された関連ドメインを別のドメインに置き換えると、アプリに関連するセキュリティ制限が機能しなくなります。

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

管理コンソール

関連するドメインエントリが変更された後に公開アプリケーションの [アプリの編集] ページ (****[Secure Private Access] > [アプリケーション] > [アプリケーションの ** 編集]) が閉じないと、[アプリケーションの編集] ページが自動的に閉じません。

たとえば、アプリの作成時に入力した関連ドメインが`www.example.com`だったとします。アプリが公開されたら、関連ドメイン`www.example.com`を`abc.com`に置き換えて、[保存] をクリックします。アプリは正常に更新されますが、**[**アプリの編集] ページは閉じません。

[プログラムのアンインストールまたは変更**]** ページでのインストーラーの表示

ISO ファイルを使用して Secure Private Access を 2308 から 2311 にアップグレードすると、プログラムのアンインストールまたは変更ページ ([コントロールパネル**] > [**プログラム**] > [**プログラムと機能]) に Secure PrivateAccess インストーラーの最初のエントリが置き換えられずに 2 つのエントリが表示されます。

- **Citrix** 仮想アプリおよびデスクトップ **7 2311**
- **Citrix** 仮想アプリおよびデスクトップ **7 2308-Secure Private Access**

プレビュービルドインストーラーは、**Citrix** 仮想アプリおよびデスクトップ **7 2308-Secure Private Access** を選択してアンインストールできます。

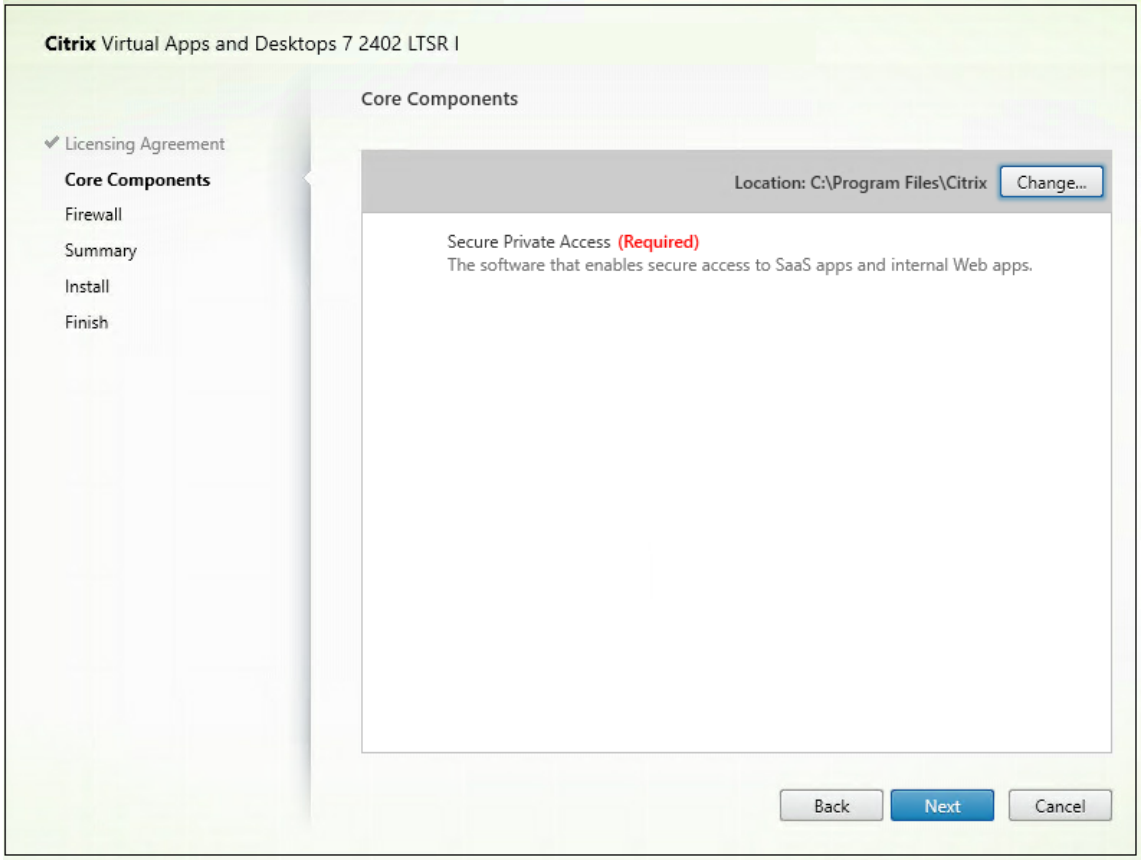
> 注**:**
>
> この問題は、Secure Private Access 2308 スタンドアロンインストーラーを 2311 スタンドアロンインストーラーを使用してアップグレードした場合には発生しません。

Secure Private Access インストーラー

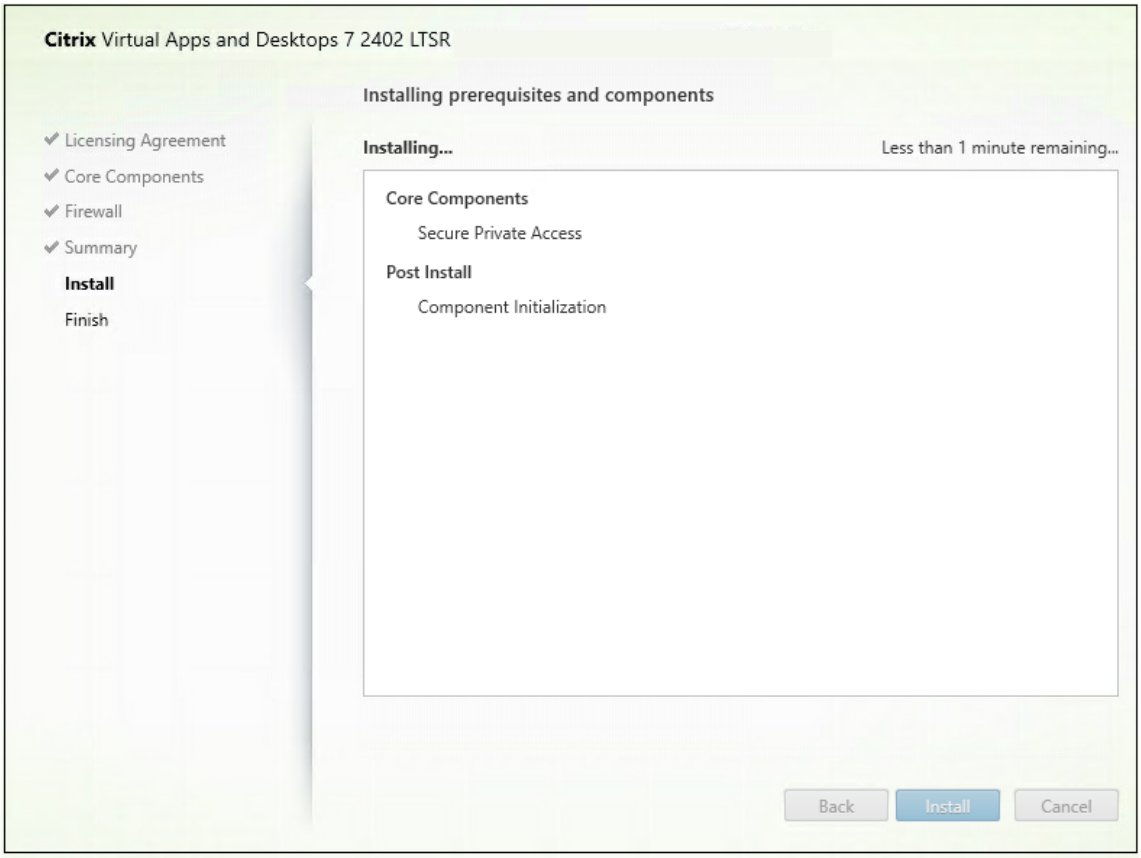
June 19, 2024

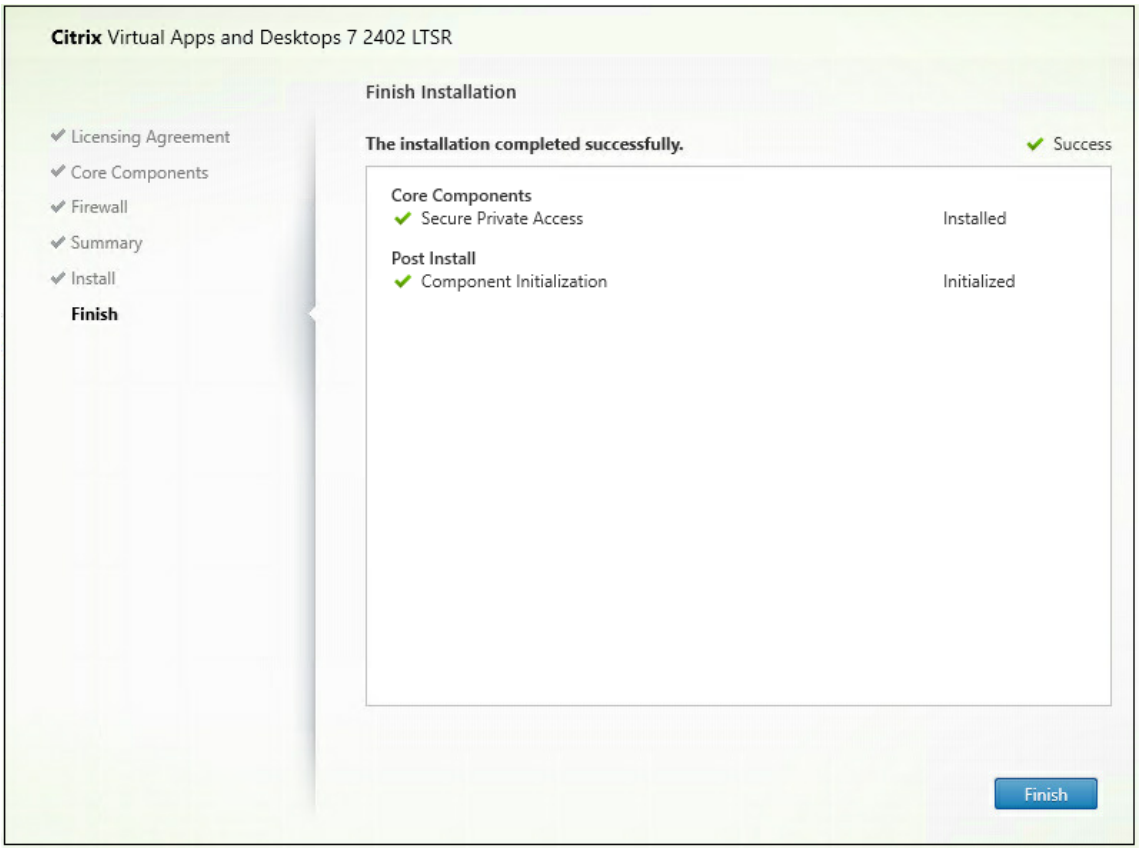
1. Citrix Secure Private Access のインストーラーをhttps://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/からダウンロードします。
2. .exe をドメインに参加しているマシン上で管理者として実行します。

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

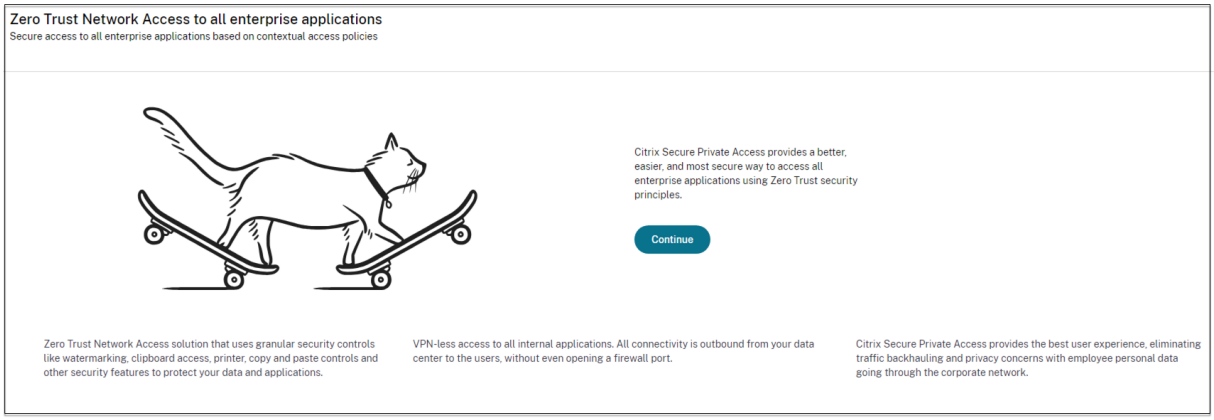


3. 画面の指示に従ってインストールを完了します。

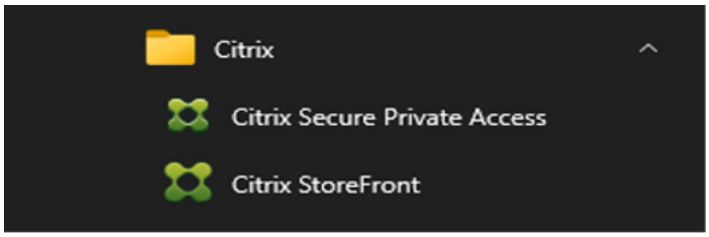




インストールが完了すると、初回セットアップの管理コンソールがデフォルトのブラウザウィンドウで自動的に開きます。「続行」をクリックして、Secure Private Access を設定できます。



また、デスクトップの［スタート］メニュー（[**Citrix**] **>** [**Citrix Secure Private Access**]）に［**Secure Private Access**］ショートカットが表示されます。



詳しくは、次のトピックを参照してください:

- コアコンポーネントのインストール
- コマンドラインを使用したインストール

管理コンソールへの **SSO**

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

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

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

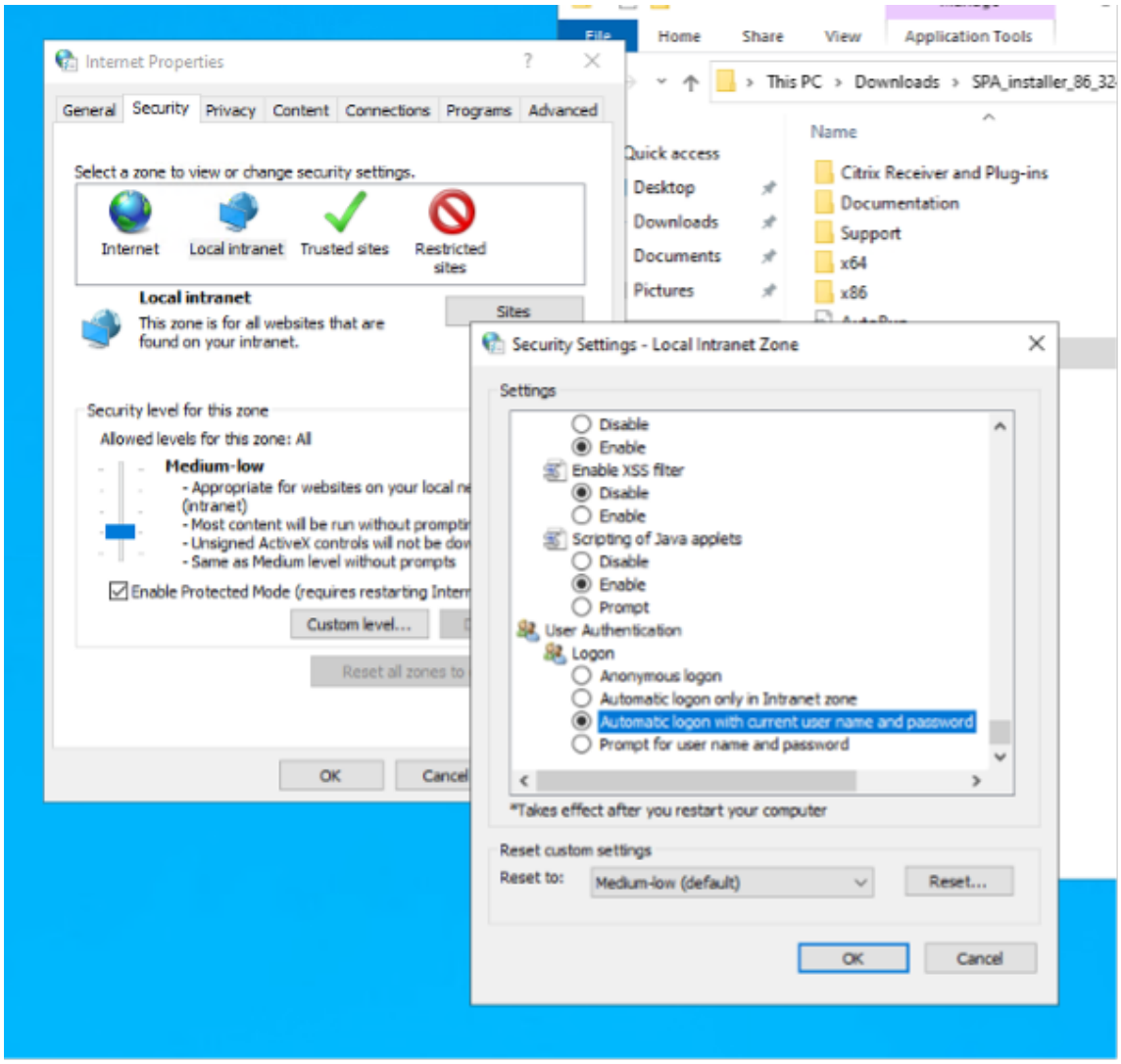
Secure Private Access のセットアップを続行するには、管理コンソールにサインインする必要があります。インストールマシンと同じドメインに属する任意のユーザーに Secure Private Access を設定できます。ただし、そのユーザーがインストールマシンのローカル管理者権限を持っている必要があります。

Google Chrome および Microsoft Edge ブラウザの場合は、次の手順を実行して Kerberos を有効にします。

1. [インターネットオプション] を開きます。
2. [セキュリティ] タブを選択し、[ローカルイントラネットゾーン] をクリックします。
3. 「サイト」をクリックし、Secure Private Access の URL を追加します。

   Secure Private Access を複数のマシンにインストールする予定がある場合は、ワイルドカードを使用することもできます。例: `"https://*.fabrikam.local"`。

4. 「カスタムレベル」をクリックし、「ユーザー認証」**>**「ログオン」で、「現在のユーザー名とパスワードで自動ログオン」を選択します。



> 注記:

- Chrome シークレットセッションを使用している場合は、DWORD レジストリキー Computer\ HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Google\ Chrome\ AmbientAuthenticationInPrivateModesEnabled を作成し、値 1 に設定します。

- Kerberos をシークレットモードで有効にする前に、すべての Chrome ウィンドウ (非シークレットウィンドウを含む) を再起動する必要があります。
- 他のブラウザーについては、Kerberos 認証に関する特定のブラウザーのドキュメントを確認してください。

次の手順

- Secure Private Access のセットアップ
- NetScaler Gateway の構成
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

スクリプトを使用してデータベースをアップグレードする

June 19, 2024

管理者設定ツールを使用して、Secure Private Access プラグインのデータベースアップグレードスクリプトをダウンロードできます。

1. PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
2. ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)。
3. 次のコマンドを実行します:

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

サイズガイドライン

June 19, 2024

データベースストレージ要件

データベースストレージのほとんどはログによって消費されます。アプリケーションとポリシー設定によるストレージ容量の消費は、ログと比較するとごくわずかです。

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

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

> 注記:
>
> - メトリクスは、ログイベントのクリーンアップが無効で、ログの保持期間が 7 日間に設定されていることを前提として算出されます。
> - デフォルトでは、構成された設定に応じて、ログは 90 日間保持されるか、最大 100 K のログイベントが保持されます。これらの設定は、Secure Private Access ランタイム・サービスの appsettings.json ファイルで使用でき、必要に応じて変更できます。詳しくは、イベントログを保持するための設定を参照してください。

導入ガイドライン

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数、Secure Private Access が使用する CPU などのパラメーターに基づくデータベースサイズ要件を示しています。

アプリケーションへの同時アクセスユーザーセッション	1 分あたりのアプリ列挙	Secure Private Access メモリ (GB)	Secure Private Access CPU	GB 単位のストレージ	メモ
< 20 (実証実測の目的)	2	4 GB	2	40 GB*	PoC の目的では、既存の仮想マシンの仕様を変更することなく、SPA を StoreFront と同じマシンに展開できます。
20	5	8 GB	4	60 GB	-

アプリケーションへの同時アクセスユーザーセッション	1 分あたりのアプリ列挙	Secure Private Access メモリ (GB)	Secure Private Access CPU	GB 単位のストレージ	メモ
160**	18	16 GB	4***	60 GB	2 つ以上の SPA ノードを導入してパフォーマンスを向上させることができます。

> 注記:
>
> - * ストレージは主に CDF ログによって消費されます。デフォルトでは、Secure Private Access は、各ファイルのサイズが 10 MB の 600 個のロールオーバーログファイルを保持します。そのため、Secure Private Access 管理サービスとランタイムサービスの両方が同じマシンで実行されている場合、ログによる最大ストレージ使用率は 12 GB になります。また、PoC の目的で SQL Express をローカル VM にインストールすることもできます。
> - ** この負荷プロファイル以上では、NetScaler Gateway のバージョンが 13.0 未満または 13.1～48.47 未満でない限り、StoreFront との共同ホスティングではなく、専用サーバーに Secure Private Access を展開することをお勧めします。
> - *** パフォーマンス上の問題がいくつかあることがわかっているため、このような負荷には少なくとも 2 つの Secure Private Access ノードクラスターを使用することをお勧めします。これらの問題は、今後のリリースで対処される予定です。

その他のコンポーネント構成

コンポーネント	vCPU	メモリ
SQL Server	4	16 GB
ストアフロント	4	8 GB
Active Directory	8	16GB

Secure Private Access のセットアップ

June 19, 2024

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

- 新しいサイトを作成して Secure Private Access を設定する
- 既存のサイトに参加して Secure Private Access を設定する

前提条件

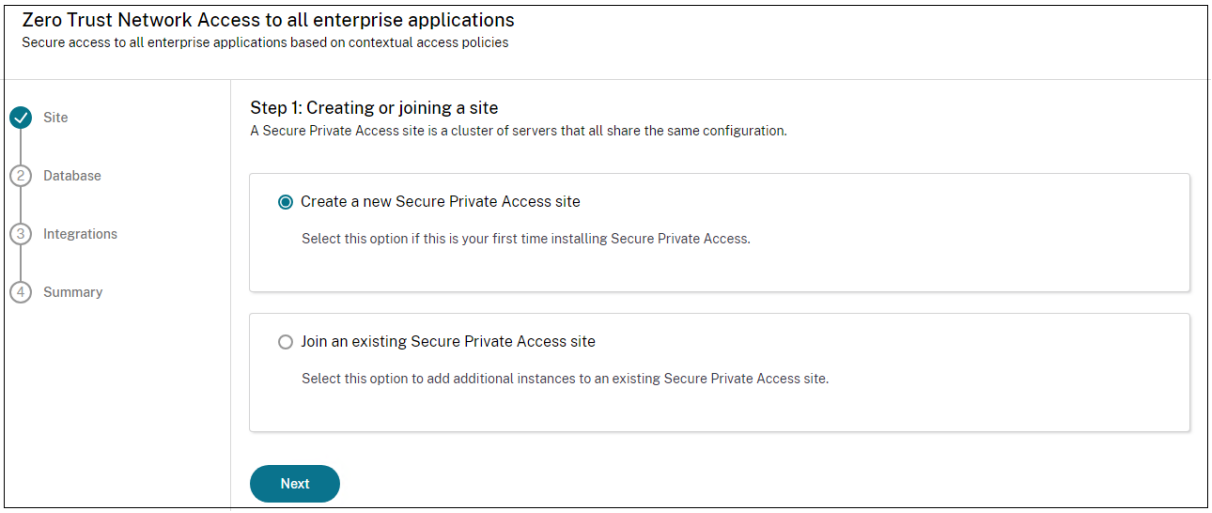
- Secure Private Access がインストールされているマシンのローカルマシン管理者でもあるドメインユーザーで Secure Private Access 管理コンソールにサインインする必要があります。
- サイトを作成する前に SQL データベースサーバーをインストールする必要があります。

新しいサイトを作成して **Secure Private Access** を設定する

ステップ **1: Secure Private Access** サイトのセットアップ

サイトとは、Secure Private Access 環境の名前です。サイトを作成するか、既存のサイトに参加することができます。

1. Secure Private Access Web 管理コンソールを起動します。
2.「サイトの作成」または「サイトへの参加」ページでは、「新しい **Secure Private Access** サイトを作成する」がデフォルトで選択されています。
3.［次へ］をクリックします。



サイトを作成する場合、サイト名に対応するデータベースがセットアップで使用できない場合があるため、新しいサイトのデータベースを自動または手動で構成する必要があります。

ステップ **2:** データベースを設定する

新しい Secure Private Access サイト用のデータベースを作成する必要があります。これは手動または自動で行うことができます。

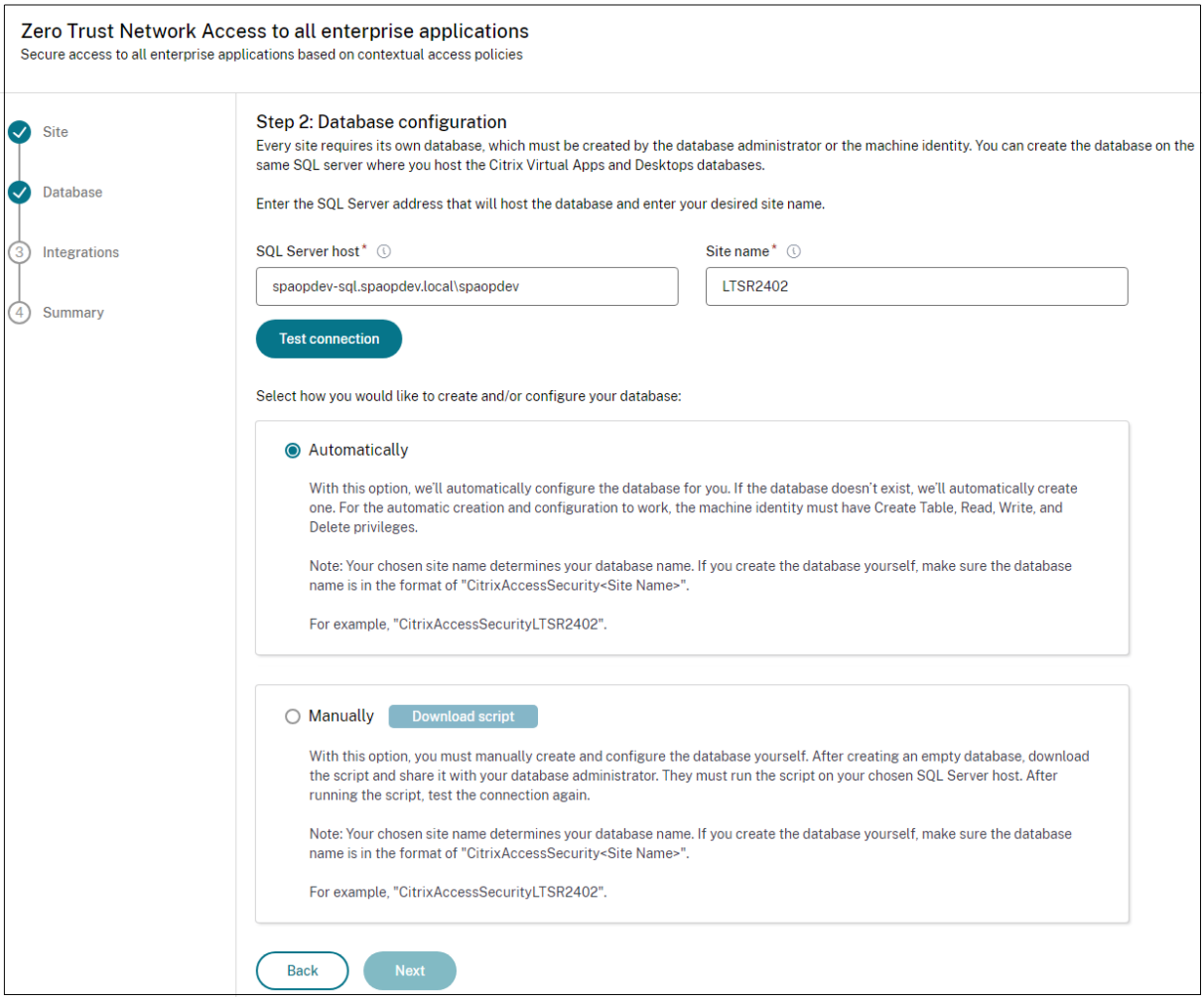
1. 「**SQL Server** ホスト」に、サーバーのホスト名を入力します。例: `sql1.fabrikam.local\citrix`。

   データベースのアドレスは、以下の形式のいずれかで指定できます:

   - サーバー名
   - ServerName\InstanceName
   - サーバー名、ポート番号

   詳しくは、「データベース」を参照してください。

2. [サイト] に、Secure Private Access サイトの名前を入力します。
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、および指定したデータベースがサイトに存在することを確認します。



> 注記:

- サイトで SQL Server が使用できない場合、接続チェックは失敗します。
- SQL Server は利用できるが、データベースが存在しない場合、接続チェックは成功します。ただし、警告メッセージが表示されます。

- Secure Private Access は、マシン ID を使用した Windows 認証を使用して SQL Server を認証します。

自動構成:

- 自動構成オプションは、マシン ID に必要なデータベース権限がある場合にのみ使用できます。
- 指定したアドレスにデータベースが存在しない場合、データベースが自動的に作成されます。
- データベースを作成するときは、そのデータベースが空で、必要なデータベース権限があることを確認してください。権限の詳細については、「データベースの設定に必要な権限」を参照してください。

手動設定:

手動構成オプションを使用してデータベースをセットアップできます。

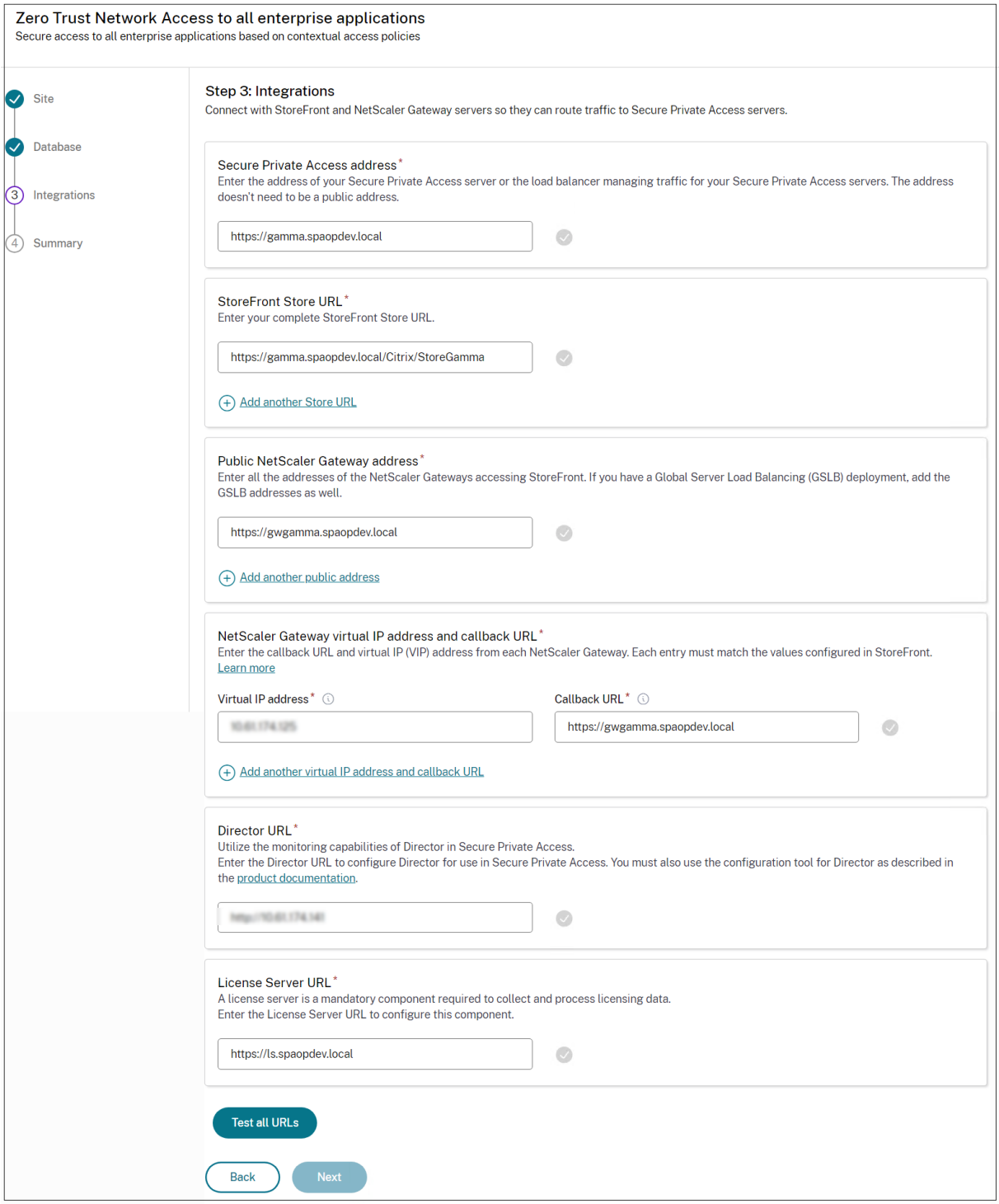
手動構成では、最初にスクリプトをダウンロードしてから、[**SQL Server Host]** フィールドで指定したデータベースサーバー上でスクリプトを実行する必要があります。

> 注記:
>
> SQL Server 上のデータベース内にテーブルを作成するための READ、WRITE、UPDATE 権限がマシンにない場合、データベースの作成が失敗することがあります。マシン上で適切な権限を有効にする必要があります。詳細については、「データベースの設定に必要な権限」を参照してください。

ステップ **3: StoreFront** サーバーと **NetScaler Gateway** サーバーを統合する

Secure Private Access を StoreFront および NetScaler Gateway サーバーに接続するには、StoreFront および NetScaler Gateway サーバーの詳細を指定する必要があります。StoreFront と NetScaler Gateway がトラフィックを Secure Private Access にルーティングできるようにするには、この接続を確立する必要があります。

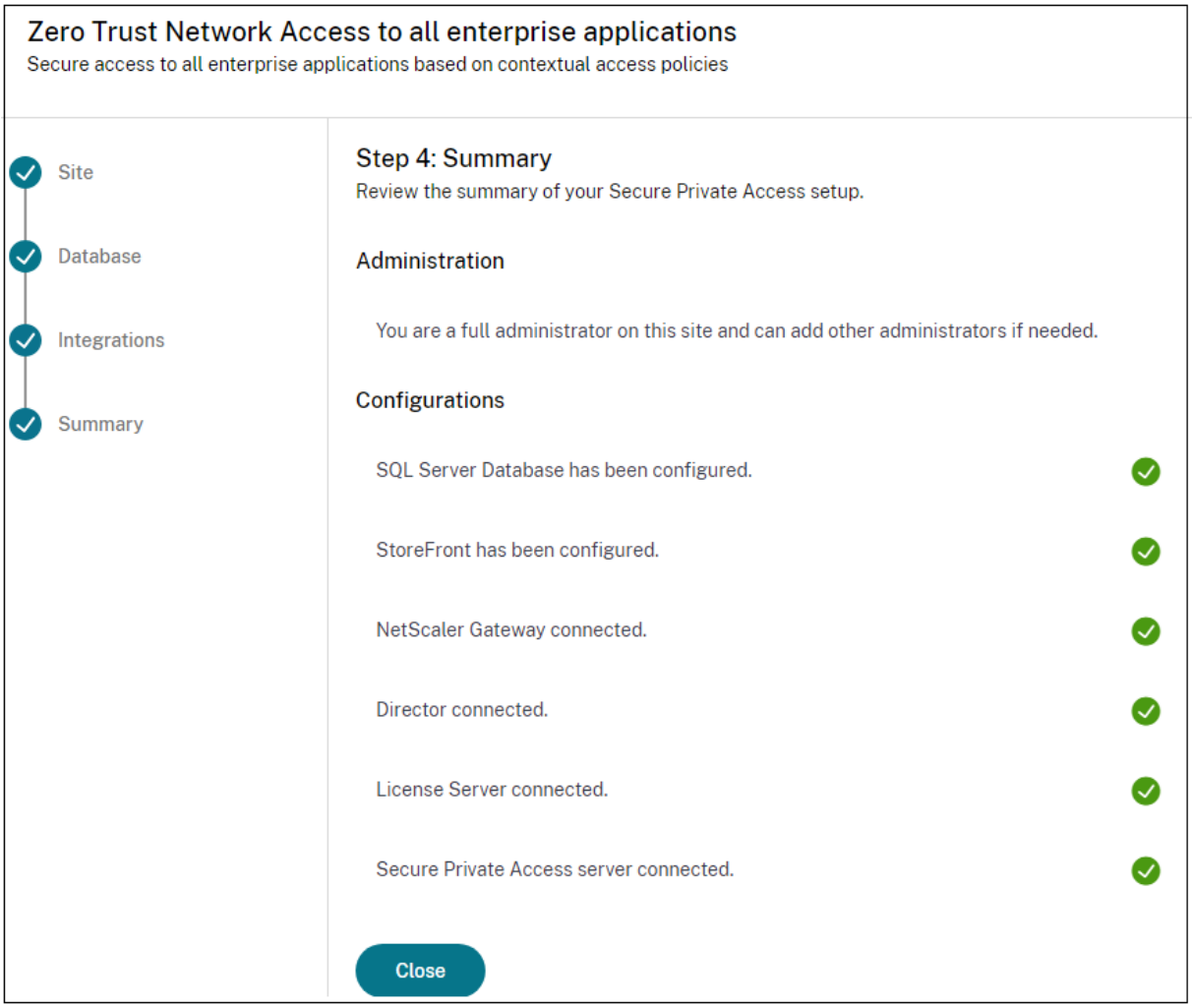
1. 次の詳細を入力します。
    - **Secure Private Access** サーバーのアドレス。例: `https://secureaccess.domain.com`。
    - **StoreFront** ストア **URL**。例: `https://storefront.domain.com/Citrix/StoreMain`。
    - パブリックゲートウェイアドレス—NetScaler Gateway の URL。例: `https://gateway.domain.com`。
    - ゲートウェイコールバックアドレス—この URL は、StoreFront で構成された URL と同じである必要があります。例: `https://gateway.domain.com`。
    - ゲートウェイ **VIP** —この仮想 IP アドレスは、StoreFront でコールバック用に構成されたものと同じである必要があります。
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、検証が行われ、構成されたサーバーにアクセスできることが確認されます。また、Secure Private Access サーバーにアクセス可能であることを確認するためのチェックも行われます。

構成の概要ページにエラーが表示される場合は、「エラーのトラブルシューティング 」で詳細を確認してください。それでも問題が解決しない場合は、Citrix サポートにお問い合わせください。

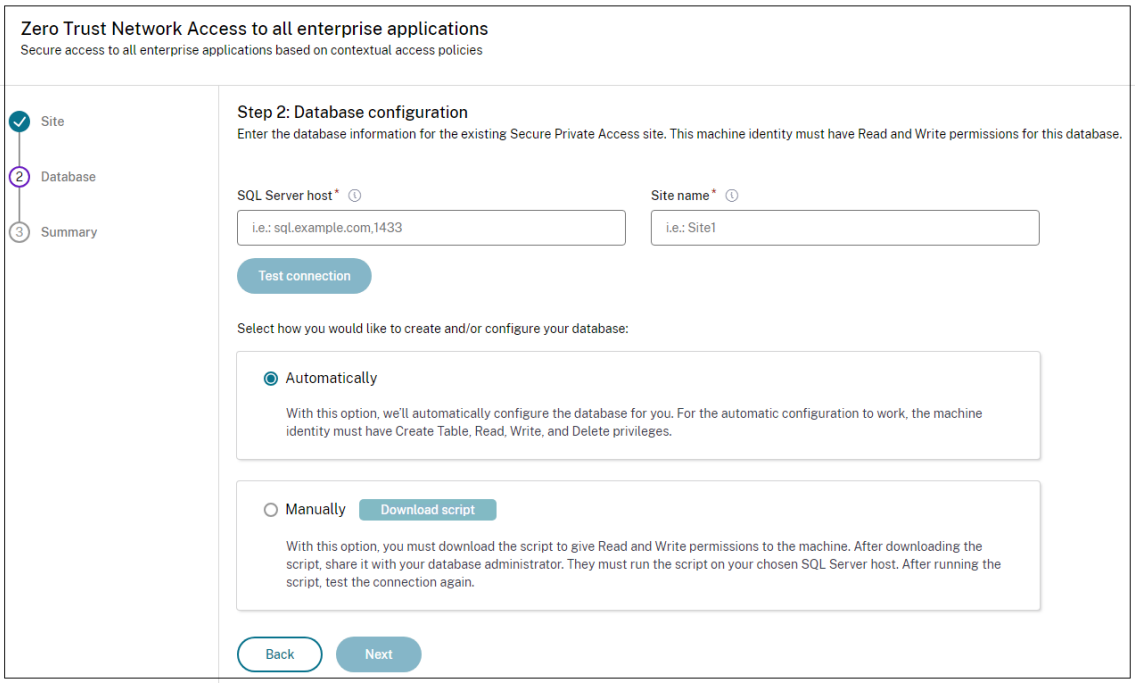


> 注記:
>
> - 環境を設定したら、Web 管理コンソールの [設定] > [統合] から設定を変更できます。
> - Secure Private Access を初めてインストールした管理者には、完全な権限が付与されます。その後、この管理者は他の管理者をセットアップに追加できます。管理者のリストは、**[設定] > [管理者]** から表示できます。
> - また、管理者グループを追加して、そのグループのすべての管理者がアクセスできるようにすることもできます。

詳細については、「インストール後の設定の管理」を参照してください。

既存のサイトに参加して **Secure Private Access** を設定する

1. [サイトの作成または参加] ページで、**[** 既存のサイトに参加する] を選択し、**[** 次へ] をクリックします。

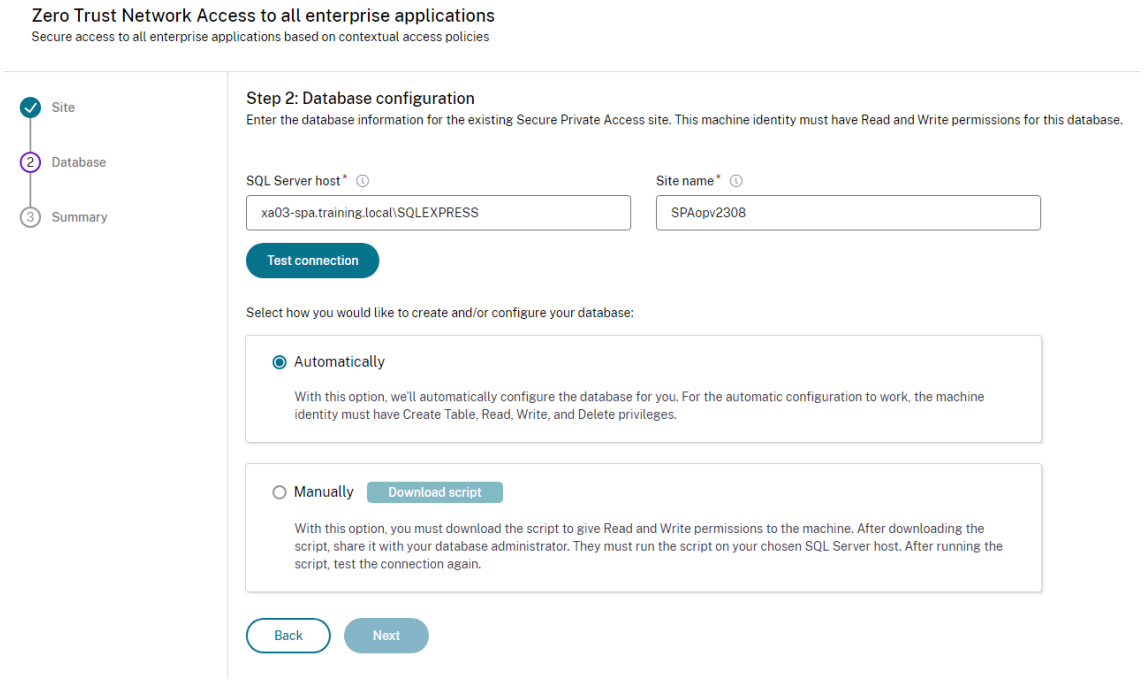


2. 「**SQL Server** ホスト」に、サーバーのホスト名を入力します。入力したサイト名に対応するデータベースが、選択した SQL Server に既に存在していることを確認してください。データベースのアドレスは、以下の形式のいずれかで指定できます:

   - サーバー名
   - ServerName\InstanceName
   - サーバー名、ポート番号

   詳しくは、「データベース」を参照してください。

3. [サイト] に、Secure Private Access サイトの名前を入力します。
4. 「接続テスト」をクリックして、SQL Server インスタンスが有効であること、および指定したサイトがデータベースに存在することを確認します。



サイトに対応するデータベースがない場合、接続チェックは失敗します。

5. [**Save**] をクリックします。

構成の検証チェックは、SQL データベースサーバーが構成されていることを確認し、Secure Private Access サーバーにアクセス可能であることを確認するために行われます。

次の手順

- NetScaler Gateway の構成
- アプリケーションの構成
- アプリケーションのアクセスポリシーを設定します

NetScaler Gateway Gateway の構成

June 19, 2024

> 重要：これらの変更を適用する前に
>
> 、NetScaler スナップショットを作成するか、NetScaler 構成を保存することをお勧めします。

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

新しい *NetScaler Gateway* を作成するには、*ns_gateway_secure_access.sh* を使用します。
既存の *NetScaler Gateway* を更新するには、*ns_gateway_secure_access_update.sh* を使用します。

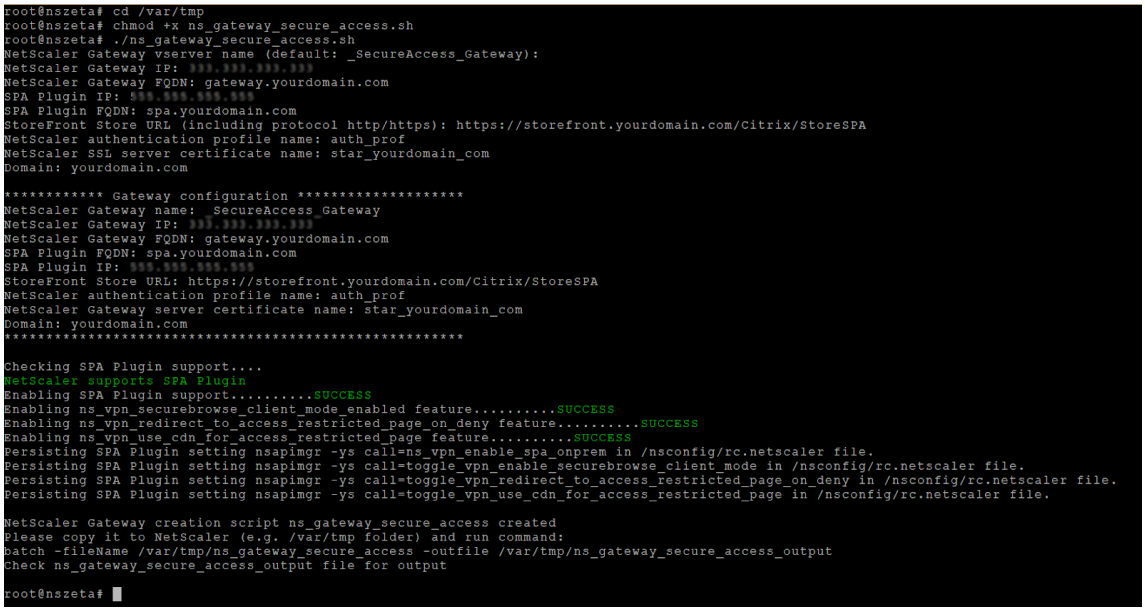
2. これらのスクリプトを NetScaler マシンにアップロードします。WinSCP アプリまたは SCP コマンドを使用できます。例: *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*。

   > 注記:
   >
   > - 一時データを保存するには、NetScaler /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 行末で保存されていることを確認してください。FreeBSD は CRLF をサポートしていません。
   > - エラー`-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M: bad interpreter: No such file or directory`が表示される場合は、行末が正しくないことを意味します。スクリプトは、Notepad++ などの任意のリッチテキストエディタを使用して変換できます。

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

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

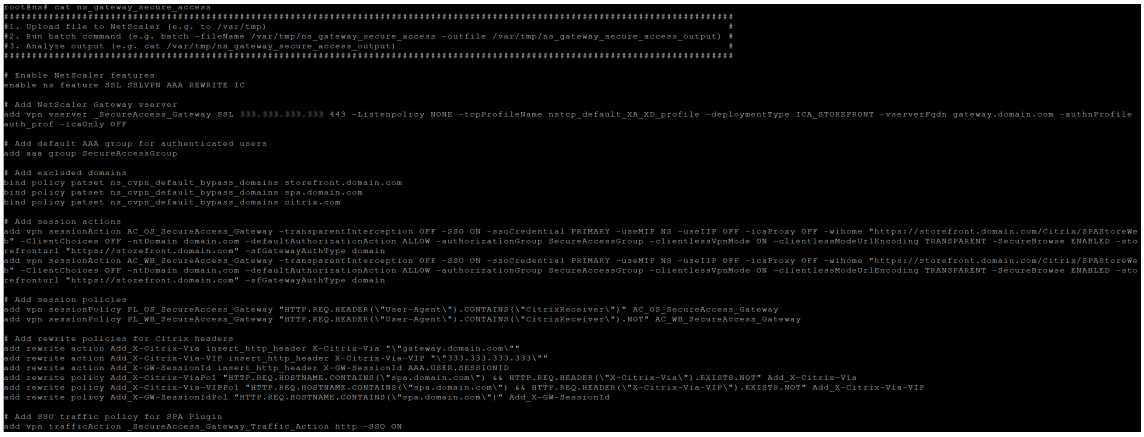
5. アップロードしたスクリプトを NetScaler シェルで実行します。



6. 必須パラメータを入力します。パラメータのリストについては、「前提条件」を参照してください。

   認証プロファイルと SSL 証明書については、NetScaler で名前を指定する必要があります。

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



7. NetScaler CLI に切り替え、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、ファイルからコマンドを 1 つずつ実行します。コマンドが失敗すると、次のコマンドに進みます。

   リソースが存在するか、ステップ 6 で入力し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ます。

> 注:
>
> エラーが発生しても、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。

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

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

- 既存の NetScaler Gateway 仮想サーバー
- NetScaler Gateway にバインドされた既存のセッションアクションとセッションポリシー

実行前に各コマンドを確認し、ゲートウェイ構成のバックアップを作成してください。

NetScaler Gateway 仮想サーバーの設定

既存の NetScaler Gateway 仮想サーバーを追加または更新するときは、次のパラメーターが定義済みの値に設定されていることを確認してください。

tcpProfileName: nstcp_default_XA_XD_profile
deploymentType: ICA_STOREFRONT
icaOnly: OFF

例:

仮想サーバーを追加するには:

```
`add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443 -
   Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
   deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
   authnProfile auth_prof_name -icaOnly OFF`
```

仮想サーバーを更新するには:

```
`set vpn vserver  _SecureAccess_Gateway -icaOnly OFF`
```

仮想サーバーのパラメータの詳細については、vpn-sessionActionを参照してください。

NetScaler Gateway セッションアクション

セッションアクションは、セッションポリシーを使用してゲートウェイ仮想サーバーにバインドされます。セッションアクションを作成するときは、次のパラメータが定義済みの値に設定されていることを確認してください。

- transparentInterception: オフ
- SSO: オン
- ssoCredential: プライマリ
- useMIP: NS
- useIIP: オフ
- icaProxy: オフ
- wihome: "https://storefront.mydomain.com/Citrix/MyStoreWeb" -実際のストア URL に置き換える
- ClientChoices: オフ
- ntDomain: mydomain.com-SSO に使用
- defaultAuthorizationAction: 許可
- authorizationGroup: SecureAccessGroup (このグループが作成されていることを確認してください。このグループは Secure Private Access 固有の認証ポリシーをバインドするために使用されています)
- clientlessVpnMode: オン
- clientlessModeUrlEncoding: 透明
- SecureBrowse: 有効
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: ドメイン

例:

セッションアクションを追加するには:

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

セッションアクションを更新するには:

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

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

ICA アプリとの互換性

Secure Private Access プラグインをサポートするように作成または更新された NetScaler Gateway を使用して、ICA アプリを列挙して起動することもできます。この場合、Secure Ticket Authority（STA）を構成し、NetScaler Gateway にバインドする必要があります。
注：STA サーバーは通常、Citrix Virtual Apps and Desktops の DDC 展開の一部です。

詳細については、以下のトピックを参照してください:

- NetScaler Gateway での Secure Ticket Authority 構成
- よくある質問:Citrix Secure Gateway/NetScaler Gateway Secure Ticket Authority

スマートアクセスタグのサポート

次のバージョンでは、NetScaler Gateway がタグを自動的に送信します。スマートアクセスタグを取得するためにゲートウェイコールバックアドレスを使用する必要はありません。

- 13.1.48.47 およびそれ以降
- 14.1–4.42 およびそれ以降

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

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

- コマンド (FreeBSD シェル) で切り替えることができます:

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

- 次のコマンド (FreeBSD シェル) を実行して、HTTP コールアウト設定の SecureBrowse クライアントモードを有効にします。

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

- 無効にするには、同じコマンドをもう一度実行します。
- トグルがオンかオフかを確認するには、`nsconmsg` コマンドを実行します。
- NetScaler Gateway でスマートアクセスタグを構成するには、「NetScaler Gateway でのカスタムタグ (SmartAccess タグ) の設定」を参照してください。

既知の制限事項

- 既存の NetScaler Gateway はスクリプトで更新できますが、1 つのスクリプトでは対応できない NetScaler 構成は無限にあります。
- NetScaler Gateway では ICA プロキシを使用しないでください。この機能は、NetScaler Gateway が構成されている場合は無効になります。
- クラウドに展開された NetScaler を使用する場合は、ネットワークにいくつかの変更を加える必要があります。たとえば、特定のポートで NetScaler と他のコンポーネント間の通信を許可します。
- NetScaler Gateway で SSO を有効にする場合は、NetScaler がプライベート IP アドレスを使用して StoreFront と通信することを確認してください。StoreFront のプライベート IP アドレスを使用して、新しい StoreFront DNS レコードを NetScaler に追加する必要がある場合があります。

パブリックゲートウェイ証明書をアップロード

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

パブリックゲートウェイ証明書をアップロードするには、次の手順を実行します。

1. 管理者権限で PowerShell またはコマンドプロンプトウィンドウを開きます。
2. ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)
3. 次のコマンドを実行します:

   ```
   \AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
   > <PublicGatewayCertificatePath>
   ```


コンテキストタグの設定

June 19, 2024

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

管理者はコンテキストタグ付きの条件をアクセスポリシーに追加できます。Secure Private Access プラグインのコンテキストタグは、認証されたユーザーのセッションに適用される NetScaler Gateway ポリシー（セッション、事前認証、EPA）の名前です。

Secure Private Access プラグインは、スマートアクセスタグをヘッダー (新しいロジック) として受け取るか、Gateway にコールバックすることで受け取ることができます。詳細については、「スマートアクセスタグ」を参照してください。

> 注:
>
> Secure Private Access プラグインは、NetScaler Gateway で構成できるクラシックゲートウェイ事前認証ポリシーのみをサポートします。

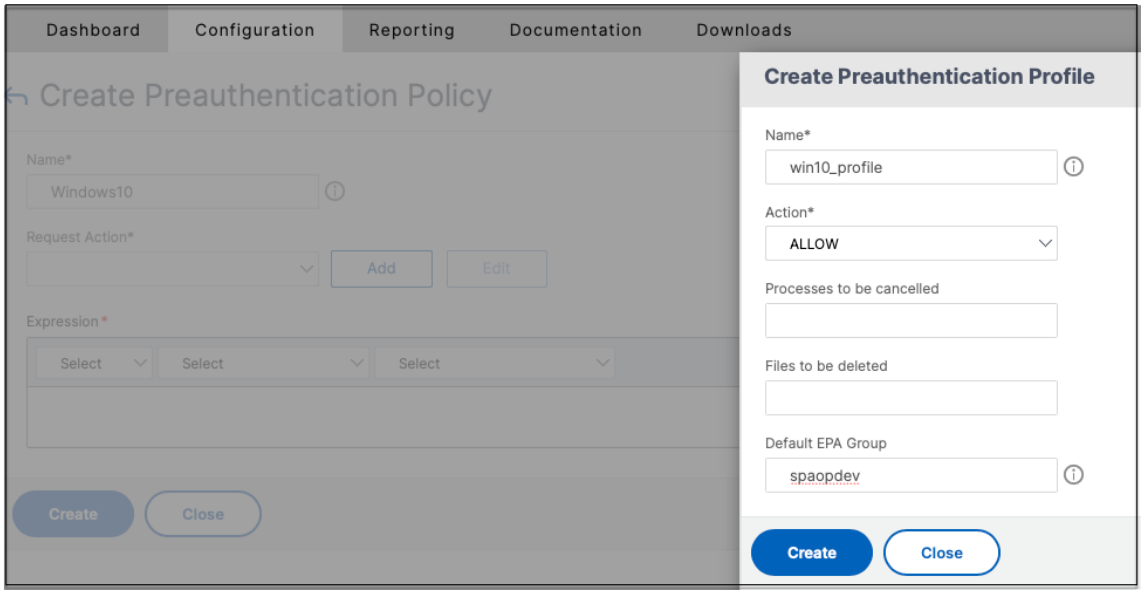
GUI を使用してカスタムタグを設定する

コンテキストタグの設定には、以下の大まかな手順が含まれます。

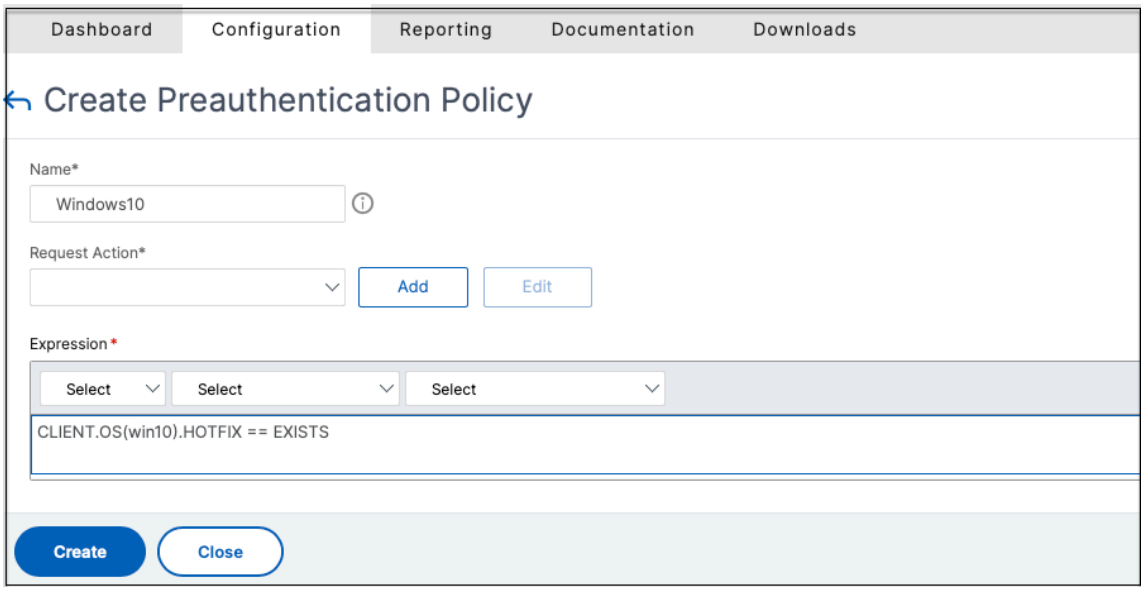
1. クラシックゲートウェイ事前認証ポリシーの設定
2. 従来の事前認証ポリシーをゲートウェイ仮想サーバーにバインドする

クラシックゲートウェイ事前認証ポリシーの設定

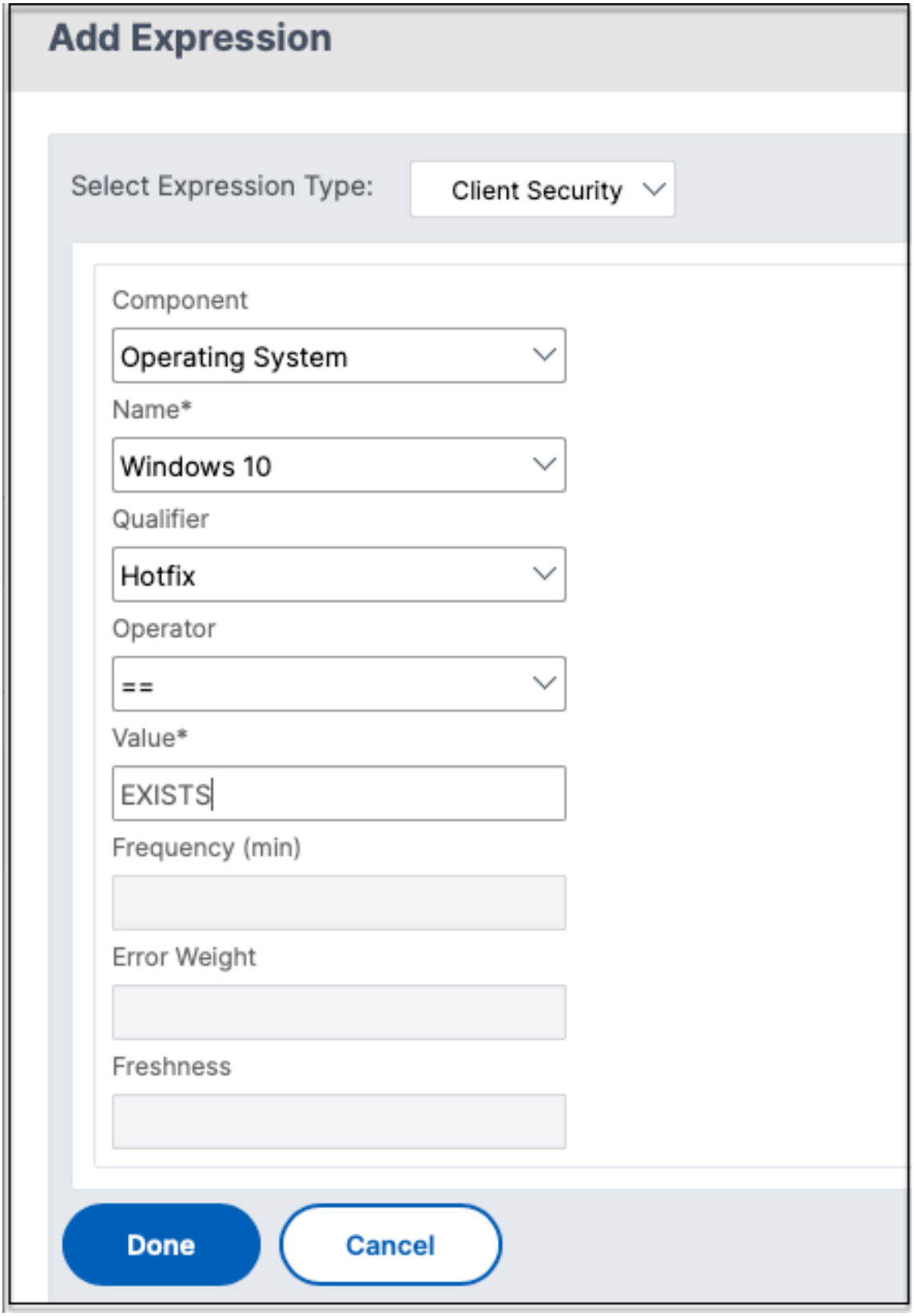
1. ［**NetScaler Gateway**］**>** ［ポリシー］**>** ［事前認証］に移動し、［追加］をクリックします。
2. 既存のポリシーを選択するか、ポリシーの名前を追加します。このポリシー名はカスタムタグ値として使用されます。
3. 「リクエストアクション」で、「追加」をクリックしてアクションを作成します。このアクションは複数のポリシーで再利用できます。たとえば、あるアクションを使用してアクセスを許可し、別のアクションを使用してアクセスを拒否できます。



4. 必須フィールドに詳細を入力し、「作成」をクリックします。
5. [式] に、式を手動で入力するか、式エディタを使用してポリシーの式を作成します。



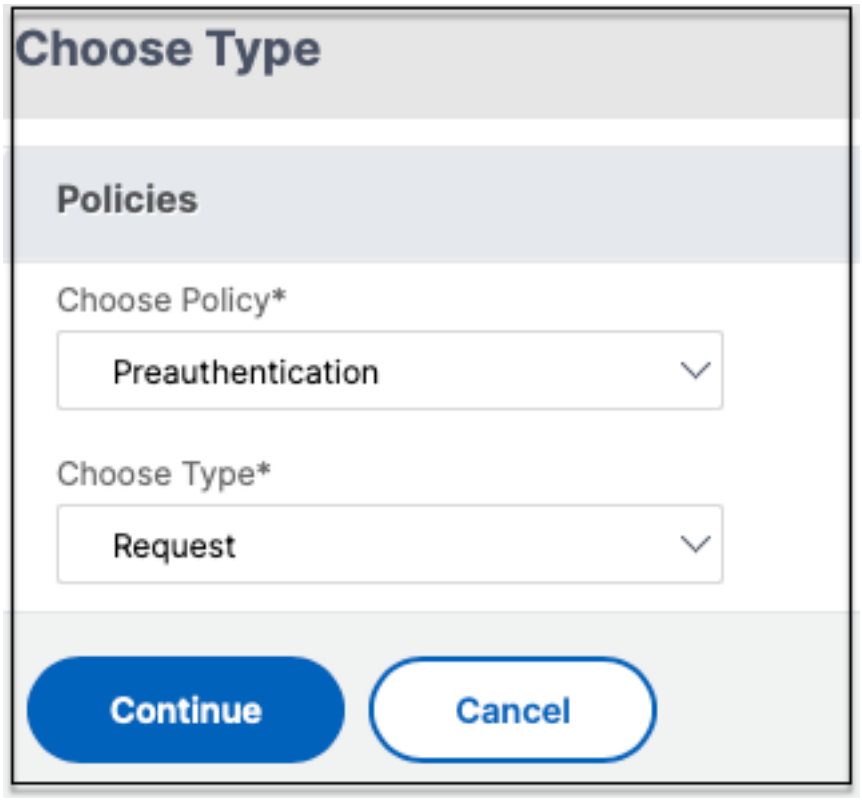
次の図は、Windows 10 OS をチェックするために作成されたサンプル式を示しています。



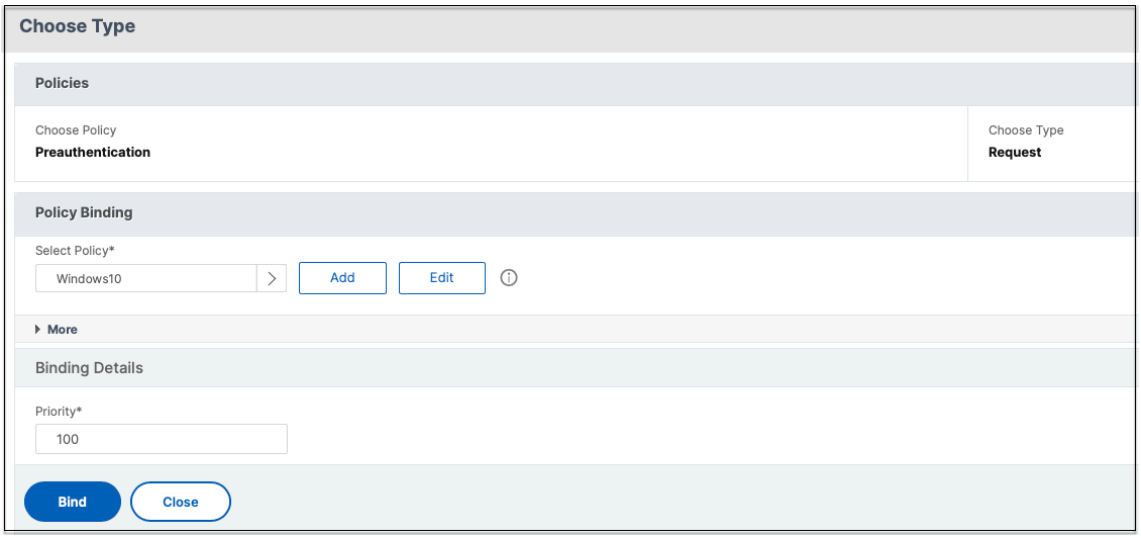
6. [**Create**] をクリックします。

カスタムタグを **NetScaler Gateway** にバインドする

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. 事前認証ポリシーをバインドする仮想サーバーを選択し、[編集] をクリックします。
3. 「ポリシー」セクションで、「**+** 」をクリックしてポリシーをバインドします。
4. 「ポリシーの選択」で事前認証ポリシーを選択し、「タイプの選択」で「要求」を選択します。



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



CLI を使用してカスタムタグを設定する

NetScaler CLI で次のコマンドを実行して、事前認証ポリシーを作成してバインドします。

例:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

新しいコンテキストタグの追加

1. Secure Private Access 管理コンソールを開き、「アクセスポリシー」をクリックします。
2. 新しいポリシーを作成するか、既存のポリシーを選択します。
3. 「次の条件が満たされている場合」セクションで、「条件を追加」をクリックし、「コンテキストタグ」、「すべてに一致」を選択し、コンテキストタグ名 (例:`Windows10`) を入力します。

参照ドキュメント

- アプリケーションのアクセスポリシーを設定します。
- スマートアクセスタグのサポート。

StoreFront の構成

June 19, 2024

Secure Private Access が StoreFront と共存している場合、StoreFront の Secure Private Access 構成は初回セットアップウィザードで自動的に行われます。

ただし、Secure Private Access を StoreFront と共存させていない場合は、特定の構成変更を手動で行う必要があります。

StoreFront を手動で構成するには、次の手順を実行します。

1. Secure Private Access 管理コンソール ([設定] **>** [統合]) からスクリプトをダウンロードします。
2. 構成を変更する必要がある StoreFront エントリに対応するスクリプトのダウンロードをクリックします。

   ダウンロードされた zip ファイルには、構成スクリプト、README ファイル、および構成クリーンアップスクリプトが含まれています。クリーンアップスクリプトは、StoreFront と Secure Private Access 間の統合を削除する場合に使用できます。
3. 次のコマンドを使用して、PowerShell 64 ビットインスタンスの管理者としてスクリプトを実行します。`./ConfigureStorefront.ps1`.

   - 他のパラメータは必要ありません。
   - StoreFront スクリプトを実行するには、PowerShell スクリプト実行ポリシーを［制限なし］または［バイパス］に設定する必要があります。
   - StoreFront reFront がクラスターとして構成されている場合、このスクリプトは構成を他の StoreFront サーバーにも伝播します。

StoreFront を Secure Private Access 設定で構成すると、Secure Private Access プラグインの構成が StoreFront 管理 UI（**Delivery Controller** の管理画面）に表示されます。

Citrix Virtual Apps and Desktops Delivery Controller で同じアグリゲーショングループ設定が構成されている場合、StoreFront スクリプトは Secure Private Access のアグリゲーショングループ設定を自動的に構成します。デフォルトでは、このスクリプトはすべてのユーザーに Secure Private Access を設定します（ユーザーマッピングとマルチサイトアグリゲーションの設定 **>** 設定済み）。

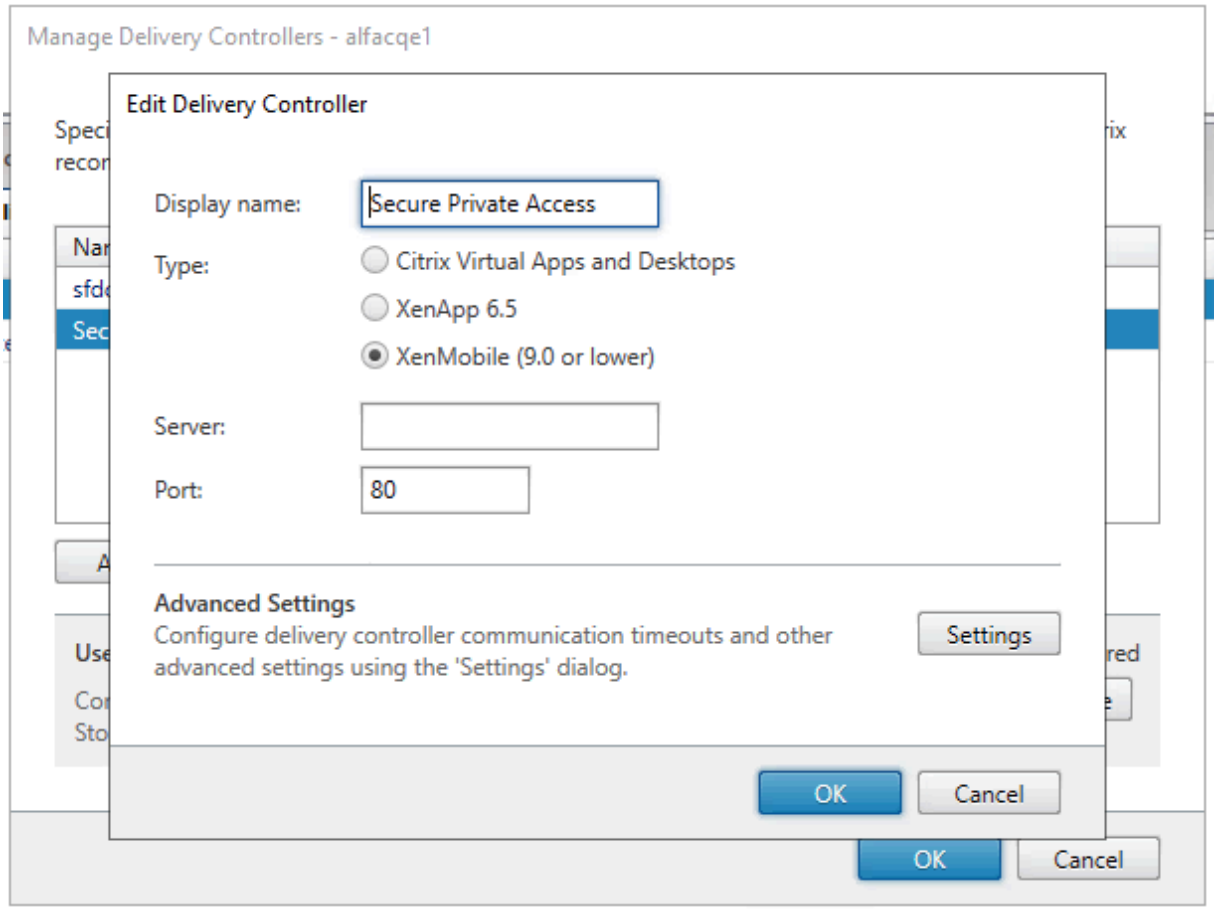
> 重要:
>
> - Secure Private Access 管理 UI からダウンロードした StoreFront スクリプトを使用して、Secure Private Access 専用に StoreFront を構成することをお勧めします。StoreFront 管理 UI から Secure Private Access を構成しないでください。UI には StoreFront で必要な構成がすべて含まれていないためです。必要な設定をすべて完了するには、スクリプトを実行する必要があります。
> - 1 つの Secure Private Access サイトを、複数の StoreFront 展開（同じ StoStoreFront 上の別のストアまたは別の StoreFront 展開環境）で構成することもできます。

> StoreFront は、［設定］**>**［統合］ページから追加できます。
>
> - Secure Private Access が StoreFront と共存している場合でも、StoreStoreFront の自動構成は [設定] **>** [統合] ページでは機能しません。自動構成は、初回セットアップ時にのみ行われます。設定ページから新しいストア構成を追加する場合 、StoreFront スクリプトをダウンロードして対応する StoreFront マシンで実行する必要があります。

StoreFront バージョン **2.308** 以前のバージョンを使用している場合

StoreFront バージョン 2308 以前を使用している場合、StoreFront 管理 UI には次の既知の問題があります。

- Secure Private Access プラグインタイプは XenMobile として表示されます。
- Secure Private Access サーバーの URL は表示されません。
- Secure Private Access ポートは常に 80 と表示されます。



StoreFront バージョン **2.3.11** 以降を使用している場合

StoreFront バージョン 2311 以降では、Web 向け Citrix Workspace クライアントは Secure Private Access アプリを列挙しません。これは、Secure Private Access が Workspace for Web プラットフォームでの Secure

Private Access アプリの起動をサポートしていないためです。

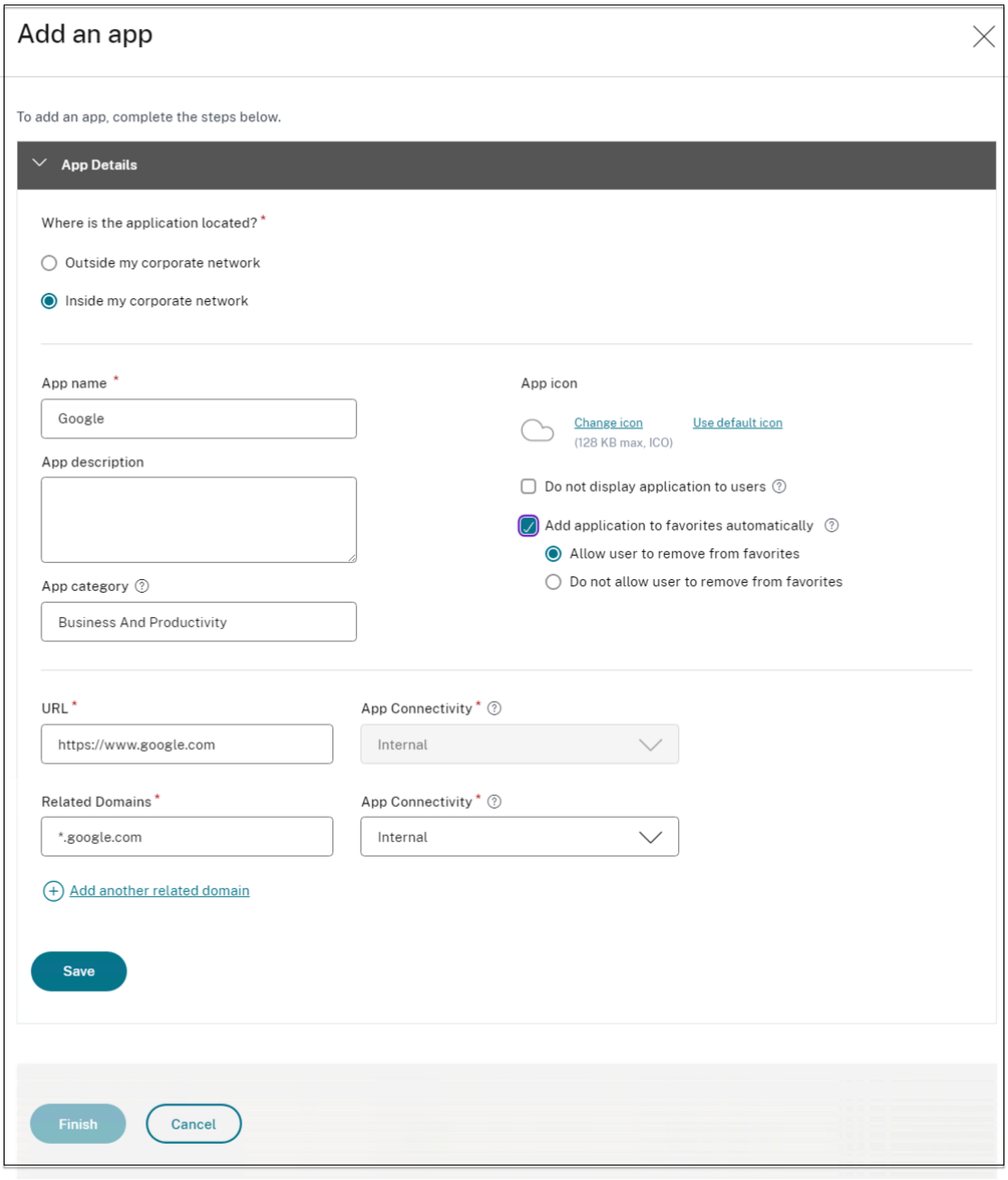
アプリケーションの構成

June 19, 2024

1. アプリが存在する場所を選択します。

    - 社内ネットワーク外の外部アプリケーション用
    - 社内ネットワークの内部アプリケーション用

2. [アプリの詳細] セクションに次の詳細を入力し、[次へ] をクリックします。



- アプリ名—アプリケーションの名前。
- アプリの説明 -アプリの簡単な説明。この説明は、ワークスペースのユーザーに表示されます。アプリケーションのキーワードをフォーマットKEYWORDS： <keyword_name>で入力することもできます。キーワードを使用してアプリケーションをフィルタリングできます。詳細については、「含まれているキーワードによるリソースのフィルタリング」を参照してください。
- アプリカテゴリ -公開するアプリが Citrix Workspace UI に表示される必要があるカテゴリとサブカテゴリ名（該当する場合）を追加します。アプリごとに新しいカテゴリを追加するか、Citrix Workspace UI から既存のカテゴリを使用できます。Web アプリまたは SaaS アプリのカテゴリを指定すると、そ

のアプリは Workspace UI の特定のカテゴリの下に表示されます。

- カテゴリ/サブカテゴリは管理者が設定可能で、管理者はアプリごとに新しいカテゴリを追加できます。
- カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。たとえば、「ビジネスと生産性\ エンジニアリング」などです。また、このフィールドは大文字と小文字が区別されます。管理者は、正しいカテゴリを定義していることを確認する必要があります。Citrix Workspace UI の名前と［アプリカテゴリ］フィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとして表示されます。

  たとえば、「ビジネスと生産性」カテゴリを「アプリカテゴリ」フィールドに「ビジネスと生産性」として誤って入力すると、「ビジネスと生産性」カテゴリに加えて、Citrix Workspace UI に「ビジネスと生産性」という名前の新しいカテゴリが表示されます。

- アプリアイコン—[アイコンの変更] をクリックして、アプリアイコンを変更します。アイコンファイルのサイズは 128x128 ピクセルでなければならず、Ico 形式のみがサポートされています。アイコンを変更しない場合、デフォルトのアイコンが表示されます。
- アプリケーションをユーザーに表示しない**-**ユーザーにアプリを表示したくない場合は、このオプションを選択してください。
- **URL** —アプリケーションの URL。
- 関連ドメイン—関連ドメインは、アプリケーション URL に基づいて自動入力されます。管理者は、関連する内部ドメインまたは外部ドメインをさらに追加できます。
  アプリケーションをお気に入りに自動的に追加—このオプションをクリックすると、このアプリが Citrix Workspace アプリのお気に入りアプリとして追加されます。
- ユーザーにお気に入りからの削除を許可—アプリ利用者が Citrix Workspace アプリのお気に入りアプリリストからアプリを削除できるようにするには、このオプションをクリックします。
  このオプションを選択すると、Citrix Workspace アプリの左上隅に黄色の星のアイコンが表示されます。
- ユーザーにお気に入りからの削除を許可しない—このオプションをクリックすると、利用者が Citrix Workspace アプリのお気に入りアプリリストからアプリを削除できなくなります。

このオプションを選択すると、Citrix Workspace アプリの左上隅に南京錠の付いた星のアイコンが表示されます。

Secure Private Access コンソールからお気に入りとしてマークされたアプリを削除する場合、それらのアプリは Citrix Workspace のお気に入りリストから手動で削除する必要があります。Secure Private Access コンソールからアプリを削除しても、アプリは StoreFront から自動的に削除されません。
アプリ接続:Web アプリの場合は [内部]、SaaS アプリの場合は [外部] を選択します。

3. [保存] をクリックし、[完了] をクリックします。

[設定] **>** **[**アプリケーションドメイン**]** で設定されているすべてのアプリケーションドメインを表示できます。詳細については、「インストール後の設定の管理」を参照してください。

次の手順

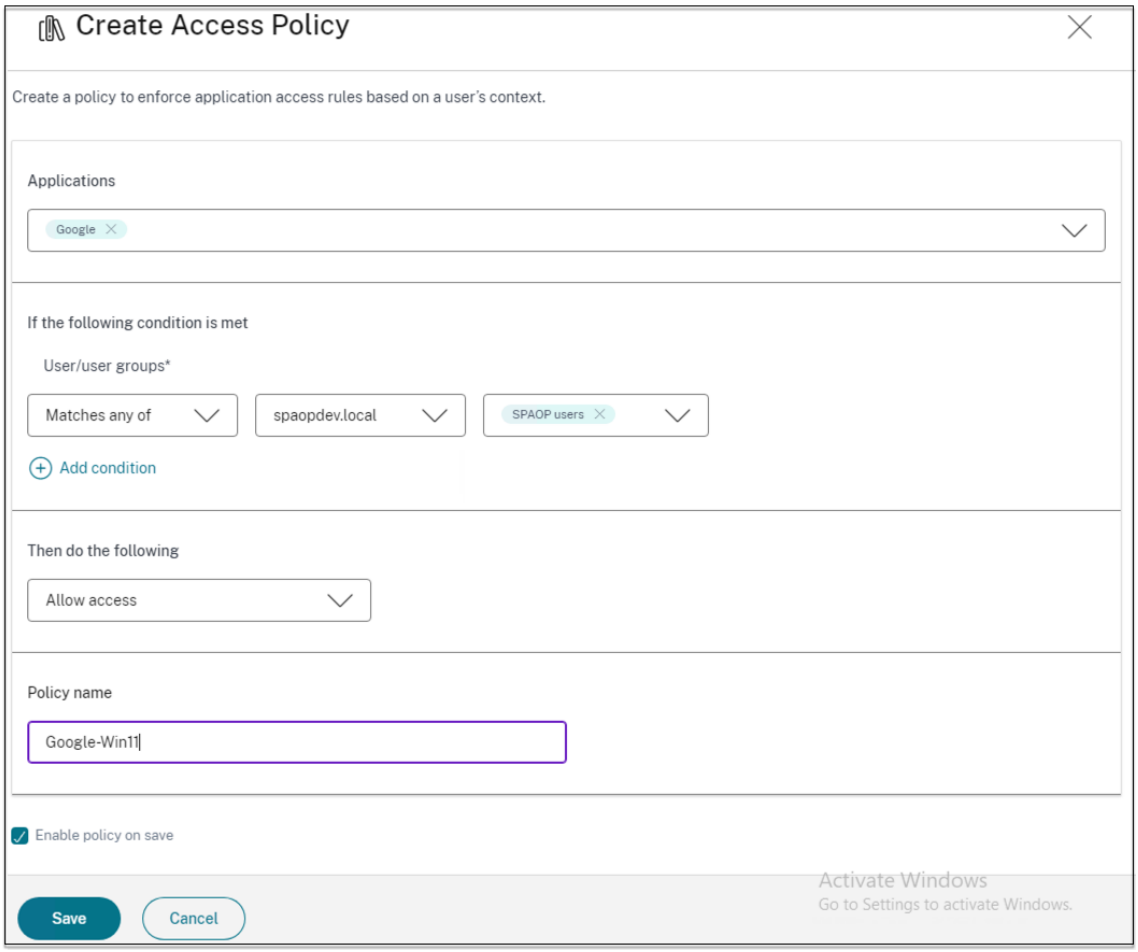
アプリケーションのアクセスポリシーを設定します

アプリケーションのアクセスポリシーを設定します

June 19, 2024

アクセスポリシーを使用すると、ユーザーまたはユーザーグループに基づいてアプリへのアクセスを有効または無効にできます。さらに、セキュリティ制限を追加することで、アプリへのアクセスを制限できます。

1. ［ポリシーの作成］をクリックします。



2.「アプリケーション」で、アクセスポリシーを適用するアプリを選択します。

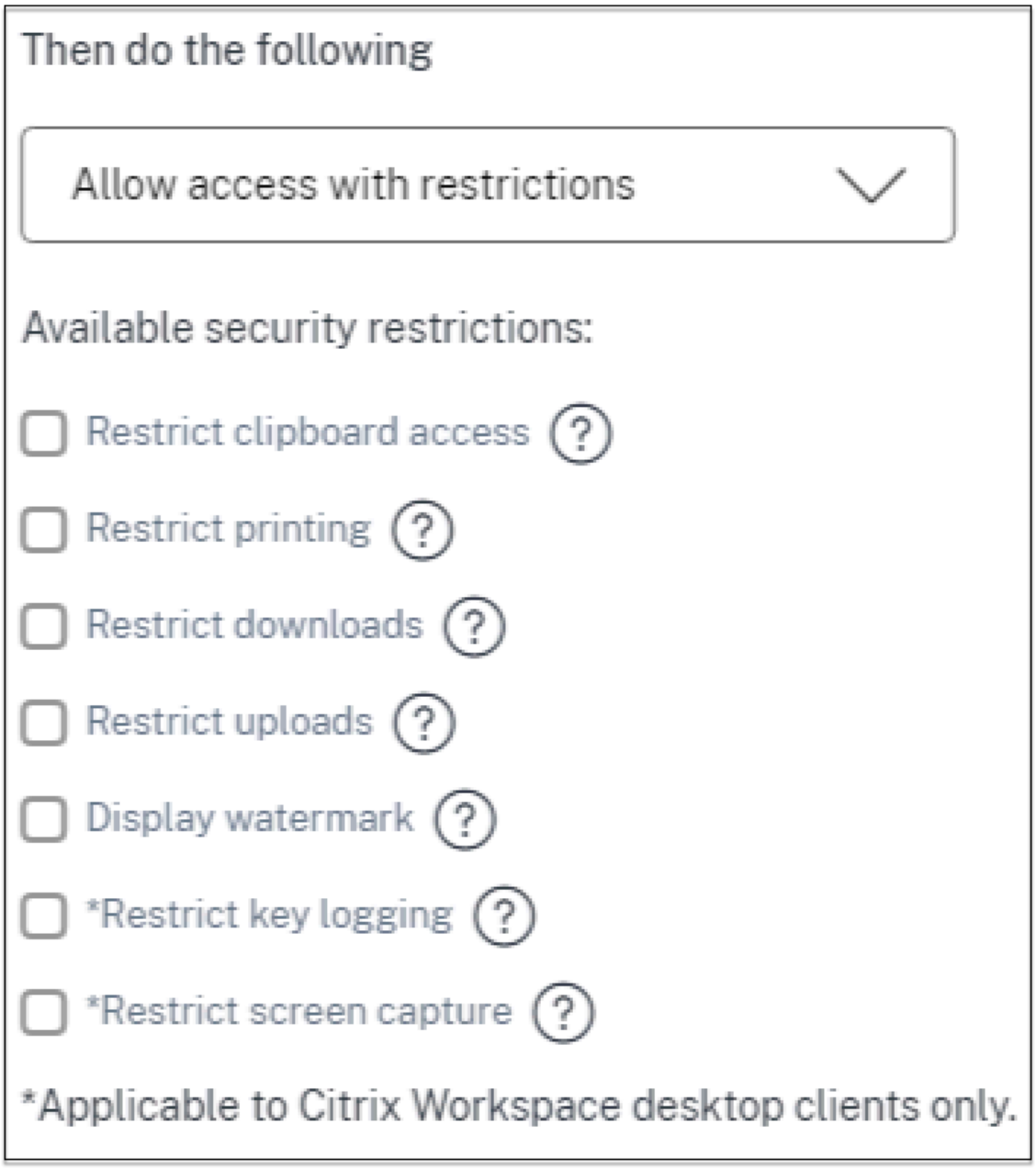
3. ユーザー/ユーザーグループで、アプリアクセスを許可または拒否する条件とユーザーまたはユーザーグループを選択します。

    - いずれかに一致: フィールドに表示されている名前のいずれかに一致するユーザーまたはグループのみがアクセスを許可されます。
    - いずれにも一致しない: フィールドに表示されているユーザーまたはグループを除くすべてのユーザーまたはグループがアクセスを許可されます。

4. コンテキストタグに基づいて別の条件を追加するには、「条件を追加」をクリックします。これらのタグは NetScaler Gateway から取得されます。
5. 「コンディショナルタグ」を選択し、アプリへのアクセスを許可または拒否する条件を選択します。
6. 「次に以下を実行する」で、条件評価に基づいてアプリに適用する必要がある次のアクションのいずれかを選択します。

    - アクセスを許可
    - 制限付きアクセスを許可
    - アクセスを拒否

    「制限付きでアクセスを許可」を選択すると、次の制限を選択できます。



- クリップボードへのアクセスを制限**:** アプリとシステムクリップボード間の切り取り**/**コピー**/**貼り付け操作を無効にします。
- 印刷の制限: Citrix Enterprise Browser 内からの印刷機能を無効にします。
- ダウンロードを制限する: ユーザーがアプリ内からダウンロードできないようにします。
- アップロードを制限する: ユーザーがアプリ内でアップロードできないようにします。
- ウォーターマークを表示: ユーザーの画面にウォーターマークを表示し、ユーザーのマシンのユーザー名と IP アドレスを表示します。
- キーロギングの制限: キーロガーから保護します。ユーザーがユーザー名とパスワードを使用してアプリにログオンしようとすると、すべてのキーがキーロガーで暗号化されます。また、ユーザーがアプリで

実行するすべてのアクティビティは、キーロギングから保護されます。
たとえば、Office 365 のアプリ保護ポリシーが有効になっていて、ユーザーが Office 365 の Word 文書を編集した場合、すべてのキーストロークはキーロガーで暗号化されます。

- 画面キャプチャを制限する: 画面キャプチャプログラムまたはアプリのいずれかを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとすると、空白の画面がキャプチャされます。

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

7. [ポリシー名] に、ポリシーの名前を入力します。
8. [保存時にポリシーを有効にする] を選択します。このオプションを選択しない場合、ポリシーは作成されるだけで、アプリケーションには適用されません。または、トグルスイッチを使用してアクセスポリシーページからポリシーを有効にすることもできます。

アクセスポリシーの優先順位

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

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

優先順位を変更するには、「優先度」列の上下アイコンを使用してポリシーを上下に移動します。

次の手順

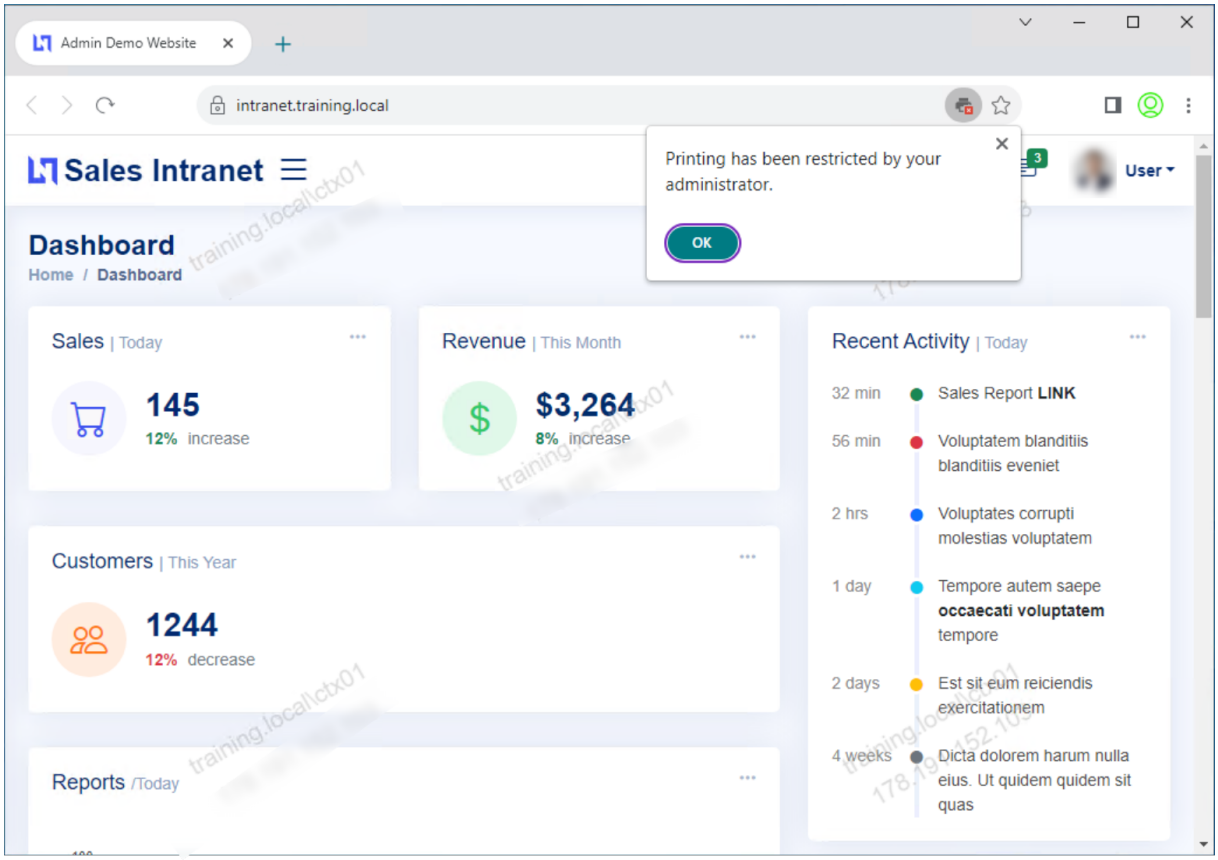
クライアントマシン (Windows および macOS) から構成を検証します。

Example

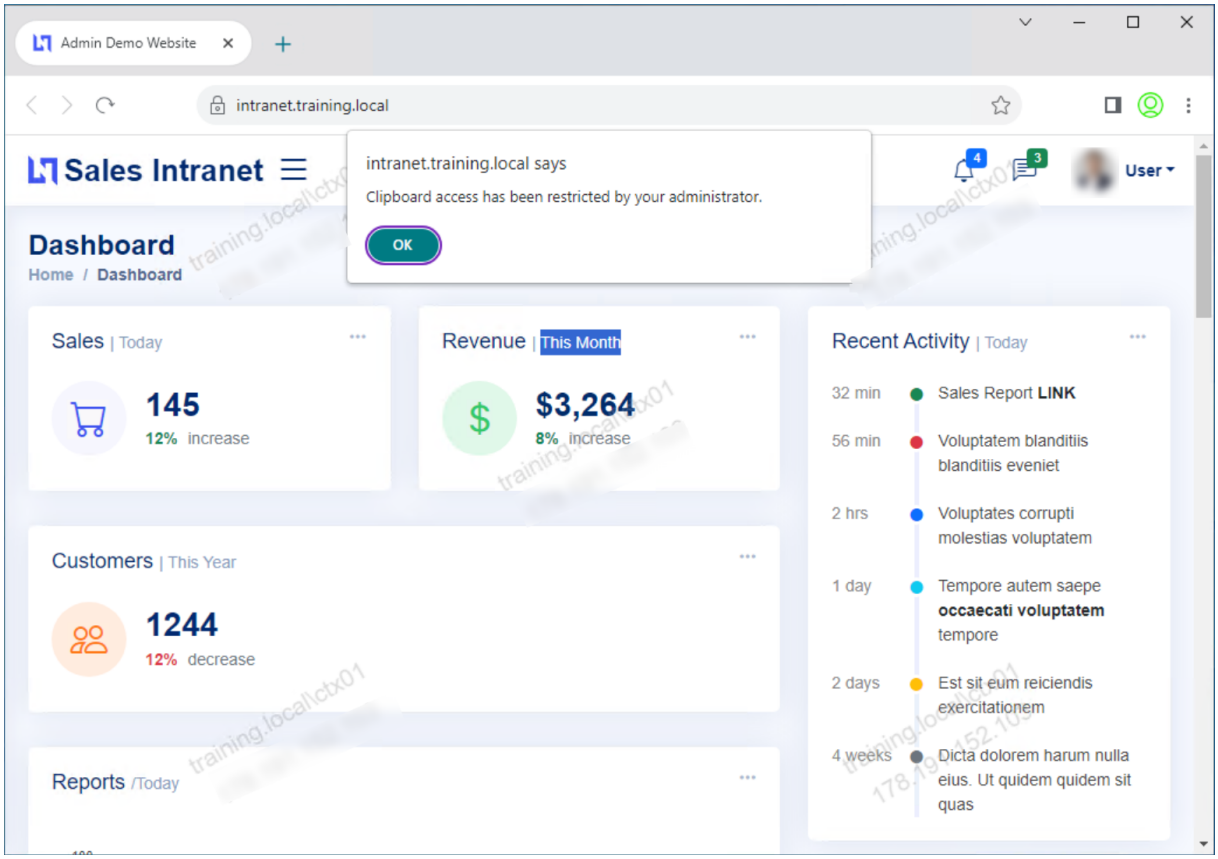
エンドユーザーフロー

June 19, 2024

クリップボードアクセスと印刷制限のあるアプリのアクセスポリシーを作成したと仮定します。これで、エンドユーザーが StoreFront からアプリにアクセスすると、Citrix Enterprise Browser でアプリが開き、ユーザーはアプリを使用できるようになります。ただし、ユーザーがアプリから印刷しようとすると、次のメッセージが表示されます。



同様に、ユーザーがクリップボードにアクセスしようとすると、次のメッセージが表示されます。



> 注:
>
> 管理者は、仮想デスクトップとアプリケーションにアクセスするために必要なアカウント情報をユーザーに提供する必要があります。詳しくは、「Citrix Workspace アプリへのストア URL の追加」を参照してください。

Secure Private Access と Web Studio の統合

June 19, 2024

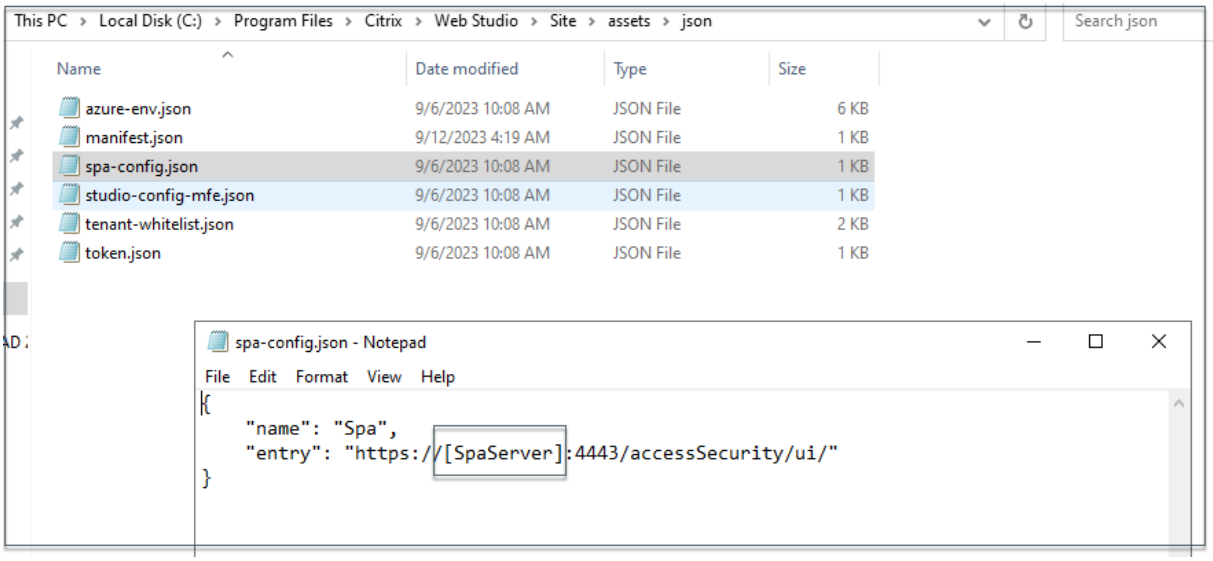
Citrix Secure Private Access も Web Studio コンソールに統合されているため、ユーザーは Web Studio を介してサービスにシームレスにアクセスできます。

Web Studio バージョン 2308 以降をインストールする必要があります。

Web Studio 統合を有効にするには、次の手順を実行します:

1. Citrix 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 Web Studio をインストールします。
2. 画面上の指示に従い、インストールを完了します。コントローラアドレスの入力を求められたら、コントローラアドレスとして DDC FQDN を入力します。

3. インストールが成功したら、C:\Program Files\ Citrix\ Web Studio\ Site\ assets\ json フォルダーに移動し、spa-config.json ファイルの内容を変更します。
   Web Studio のインストールにデフォルト以外の場所が使用された場合は、C:\Program Files\ Citrix のデフォルトのインストール場所を正しい場所に置き換えてください。



1. 「SPAServer」を Secure Private Access プラグインの FQDN に置き換えてください。
2. Web Studio にログインします。
3. 左側のナビゲーションメニューで [**Secure Private Access **] をクリックして、Web Studio から Secure Private Access 管理コンソールにアクセスします。

Secure Private Access をクラスターとして展開

June 19, 2024

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

NetScaler Gateway のバージョン 13.0 または 13.1 ビルド 48.47 以前を使用している場合は、Secure Private Access を StoreFront と共同ホストすることをお勧めします。

Secure Private Access ノードの作成

- 新しい Secure Private Access サイトを作成します。詳細については、「Secure Private Access サイトのセットアップ」を参照してください。

- 必要な数のクラスターノードを Secure Private Access サイトに追加します。詳細については、「既存のサイトに参加して Secure Private Access を設定する」を参照してください。
- 各 Secure Private Access ノードで、同じサーバー証明書を設定します。証明書のサブジェクトの共通名またはサブジェクト代替名は、ロードバランサーの FQDN と一致する必要があります。

ロードバランサー構成

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

- Secure Private Access サービス (管理とランタイムの両方) はステートレスなので、永続性は必要ありません。
- Secure Private Access サービスは HTTPS として実行することをお勧めしますが、これは必須要件ではありません。Secure Private Access サービスは HTTP としても展開できます。
- SSL オフロードまたは SSL ブリッジがサポートされているため、任意のロードバランサー設定を使用できます。SSL ブリッジを使用するときは、各 Secure Private Access ノードで同じサーバー証明書を設定してください。また、証明書のサブジェクトの共通名またはサブジェクト代替名 (SAN) は、ロードバランサーの FQDN と一致する必要があります。また、ロードバランサーサービスで SAN を設定する必要があります。
- ロードバランサー（NetScaler など）には、バックエンドサーバー用のデフォルトのビルトインモニター（プローブ）があります。Secure Private Access オンプレミスサーバー用にカスタム HTTP ベースのモニター (プローブ) を設定する必要がある場合は、次のエンドポイントを使用できます。

  `/secureAccess/health`

  期待される応答:

```
Http status code: 200 OK

Payload:

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

<!--NeedCopy-->
```

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

インストール後に設定を管理

June 19, 2024

Secure Private Access をインストールしたら、設定ページから設定を変更できます。

設定を変更するには、Secure Private Access 管理者アカウントで Secure Private Access 管理コンソールにサインインする必要があります。

アプリケーションドメインのルーティングを管理

Secure Private Access の設定に追加されたアプリケーションドメインのリストを表示できます。アプリケーションドメインテーブルには、すべての関連ドメインと、アプリケーショントラフィックのルーティング方法（外部または内部）が一覧表示されます。

1. [設定**] > [**アプリケーションドメイン] をクリックします。
2. 必要に応じて、編集アイコンをクリックしてルーティングタイプを変更できます。

Secure Private Access のための管理者の管理

[設定**] > [**管理者**]** ページから、管理者のリストを表示したり、管理者を追加したりできます。Secure Private Access を初めてインストールした管理者には、完全な権限が付与されます。その後、この管理者は他の管理者をセットアップに追加できます。

管理者グループを追加して、そのグループのすべての管理者がアクセスできるようにすることもできます。

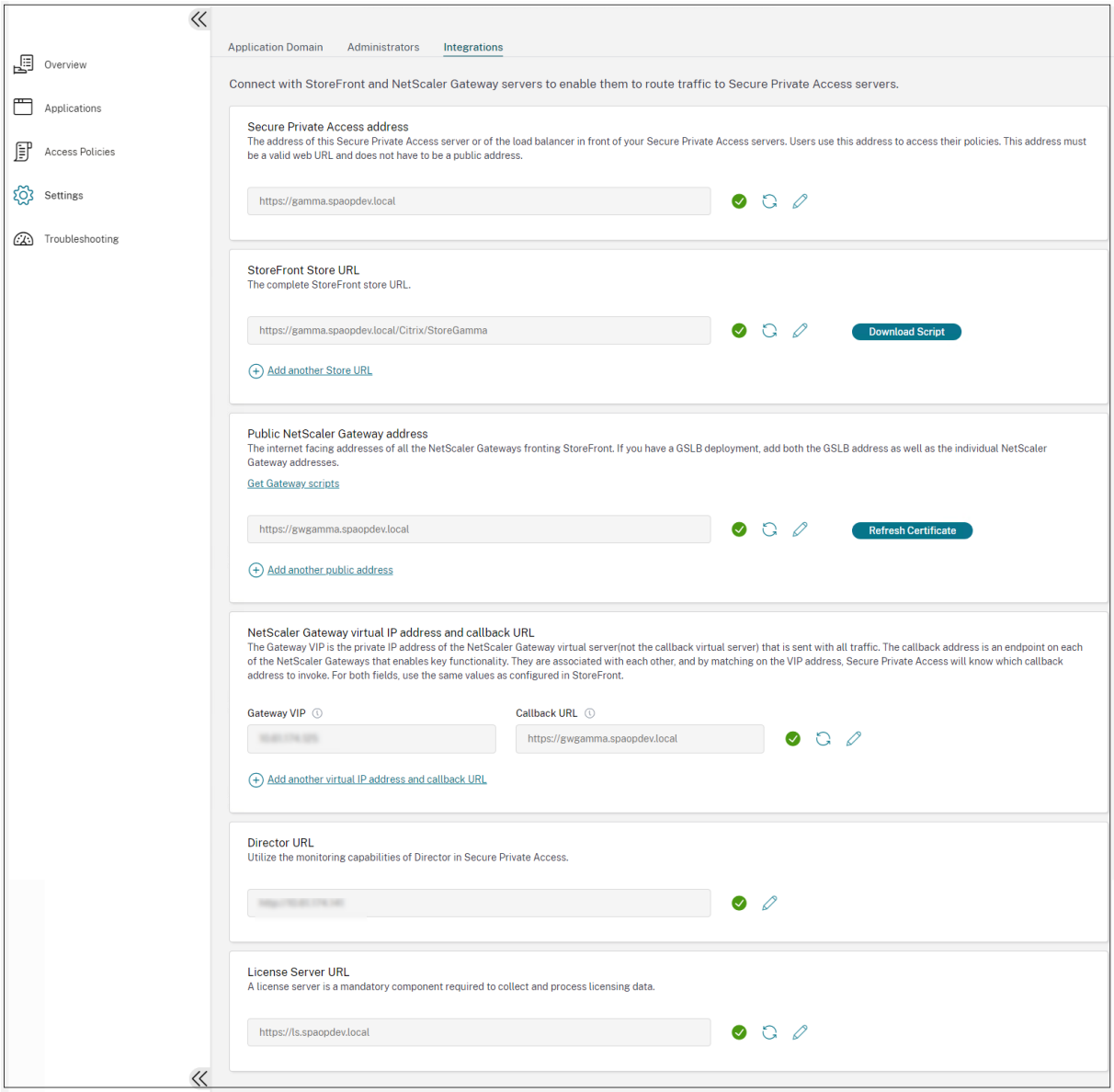
1. 管理者ページで、「追加」をクリックします。
2. 「ドメイン」で、この管理者を追加する必要があるドメインを選択します。
3. 「ユーザーまたはユーザー・グループ」で、このユーザーが属するユーザーまたはグループを選択します。
4. 「管理者タイプ」で、このユーザーに割り当てる必要がある権限タイプを選択します。

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

Secure Private Access を設定したら、［統合］タブから **StoreFront** と **NetScaler Gateway** のエントリを変更または更新できます。

1. [設定**] > [**インテグレーション] をクリックします。
2. 変更する設定の横にある編集アイコンをクリックし、エントリを更新します。
3. 更新アイコンをクリックして、設定が有効であることを確認します。

> 注:
>
> Secure Private Access が StoreFront と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 で実行してください。



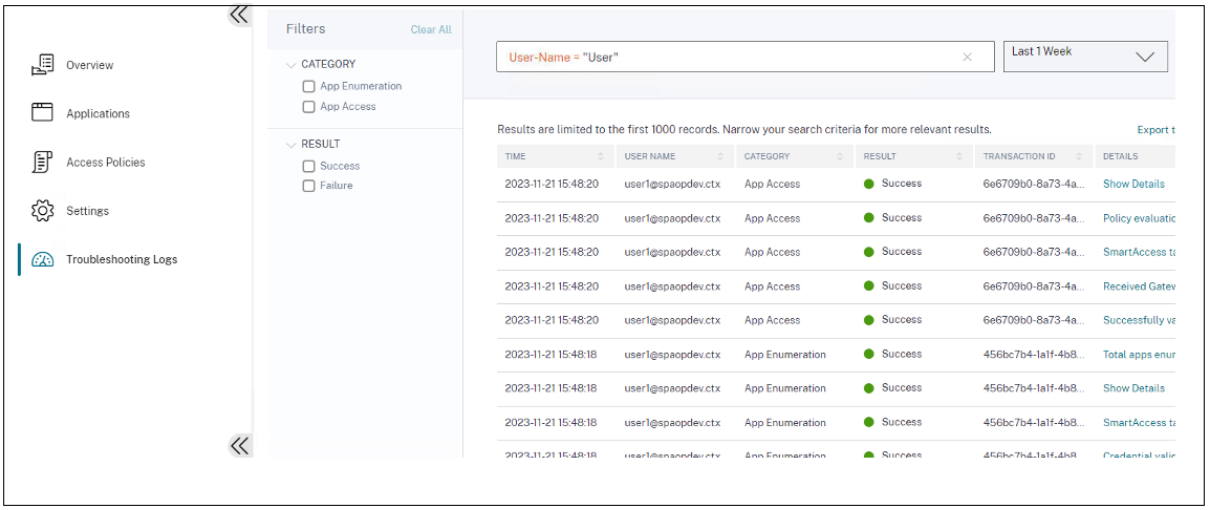
ダッシュボードの概要

June 19, 2024

Secure Private Access トラブルシューティングログダッシュボードには、アプリケーションの起動、アプリケーションの列挙、およびそれらのステータスに関連するログが表示されます。

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

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



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

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

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

- =: 検索条件に完全に一致するログ/ポリシーを検索します。
- !=: 指定された条件が含まれていないログ/ポリシーを検索します。
- ~: 検索条件に部分的に一致するログ/ポリシーを検索します。
- !~: 指定された条件の一部を含まないログ/ポリシーを検索します。

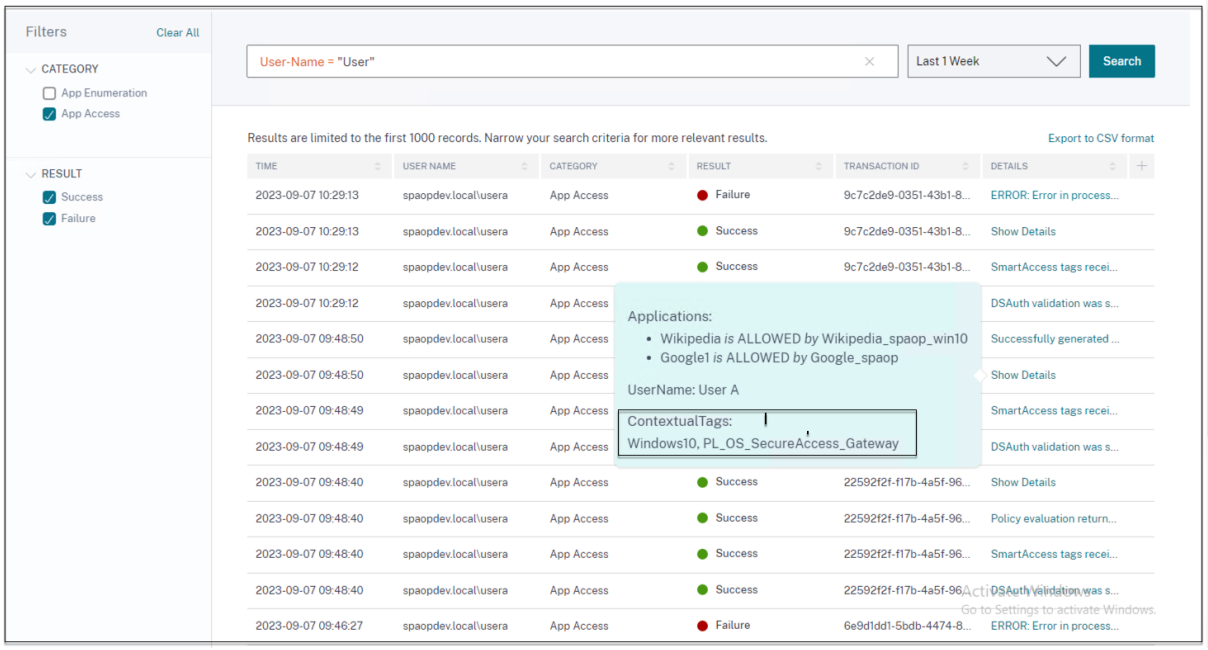
たとえば、検索フィールドに **Event-Type = DSAuth** という文字列を使用すると、イベントタイプ「**DSAuth** 」を検索できます。

同様に、「operator」という用語の一部を含むユーザーを検索するには、**User-Name ~ operator** という文字列を使用します。この検索では、「operator」という用語を含むすべてのユーザー名が一覧表示されます。たとえば、「ローカルオペレータ」、「管理者オペレータ」

トランザクション ID を使用して、1 つのイベントに関連するすべてのログを検索できます。トランザクション ID は、アクセス要求のすべての Secure Private Access ログを関連付けます。1 つのアプリアクセスリクエストで、認証、アプリ列挙、アプリアクセス自体など、複数のログを生成できます。これらのイベントはすべて独自のログを生成します。トランザクション ID は、これらすべてのログを関連付けるために使用されます。トランザクション ID を使用してトラブルシューティングログをフィルタリングし、特定のアプリアクセスリクエストに関連するすべてのログを検索できます。

ログからコンテキストタグを表示

[**Details]** 列の **[ShowDetails**] リンクには、特定のアクセスポリシーに関連付けられているアプリケーションのリストと、そのポリシーに関連付けられているコンテキストタグが表示されます。



よくあるエラーのトラブルシューティング

June 19, 2024

このトピックでは、Secure Private Access の設定中に発生する可能性のあるエラーの一部を示します。

証明書のエラー

データベース作成エラー

StoreFront 障害

パブリックゲートウェイ/コールバックゲートウェイの障害

Secure Private Access サーバーにアクセスできない

証明書のエラー

エラーメッセージ:1 つ以上の Gateway サーバーから証明書を自動的に取得できません。

このエラーメッセージは、NetScaler Gateway のパブリックアドレスを追加しようとして、証明書の取得に問題がある場合に表示されます。この問題は、Secure Private Access をセットアップするとき、またはセットアップが完了した後に設定を更新するときに発生する可能性があります。

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

データベース作成エラー

- エラーメッセージ: データベースを作成できませんでした

  解決策: 自動の場合-SQL Server 上のデータベース内にテーブルを作成するには、マシンに READ、WRITE、UPDATE 権限が必要です。

- エラーメッセージ: データベースを作成できませんでした: データベースは既に存在します。

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

  - データベースの構成時に「自動構成」オプションを選択した場合。
  - 管理者がデータベースを作成する場合、そのデータベースは空のデータベースでなければなりません。このエラーメッセージは、データベースが空でないデータベースである場合に表示されることがあります。

    解決策: 空のデータベースを作成する必要があります。
  - Secure Private Access をアンインストールし、同じサイト名でセットアップを再試行します。この場合、以前のインストールのデータベースは削除されなかったでしょう。

    解決策: データベースを手動で削除する必要があります。
  - スクリプトを使用してデータベースを手動で設定し ([データベースの構成] ページで [手動構成] を選択)、次に [自動構成] オプションに変更しますが、サイト名は同じです。この場合、スクリプトの実行中に同じ名前のデータベースがすでに作成されています。

    解決策: サイトの名前を変更してから、スクリプトを再実行する必要があります。
  - マシンには、SQL Server 上のデータベース内にテーブルを作成するための READ、WRITE、UPDATE 権限がありません。

    解決策: マシン上で適切な権限を有効にします。詳細については、「データベースの設定に必要な権限」を参照してください。

- エラーメッセージ: データベースを作成できませんでした: 接続に失敗しました

  解決策:

  - マシンからのデータベースネットワーク接続を確認してください。SQL Server ポートがファイアウォールで開いていることを確認します。

- リモート SQL Server を使用している場合は、SQL Server に Secure Private Access のマシン ID である Domain\ hostname$ を使用して作成されたログインがあるかどうかを確認してください。
- リモート SQL Server を使用している場合は、マシン ID に正しいロール、つまりシステム管理者ロールが割り当てられていることを確認してください。
- ローカル SQL Server (インストーラからではない) を使用している場合は、NT AUTHORITY\ SYSTEM ユーザにログインを作成する必要があるかどうかを確認してください。

StoreFront 障害

- エラーメッセージ: 次の StoreFront エントリを作成できませんでした: <Store URL>

  表示されていない場合は、［設定］タブから StoreFront のエントリを更新します。ウィザードを使用して Secure Private Access を設定したら、［設定］タブから StoreFront のエントリを編集できます。このエラーが発生した StoreFront ストアの URL を書き留めてください。

  解決策:

  1. [設定] をクリックし、[インテグレーション] タブをクリックします。
  2. **StoreFront** ストア **URL** に、StoreFront エントリが表示されていない場合は、そのエントリを追加します。

- エラーメッセージ: 次の StoreFront エントリを構成できませんでした: <Store URL>

  解決策:

  1. PowerShell の実行ポリシーによる制限が設定されている可能性があります。詳細については、PowerShell スクリプトコマンド `Get-ExecutionPolicy`を実行してください。
  2. 制限されている場合は、これを回避して StoreFront 構成スクリプトを手動で実行する必要があります。
  3. [設定] をクリックし、[インテグレーション] タブをクリックします。
  4.「**StoreFront** ストア **URL**」で、エラーが発生した StoreFront URL のエントリを特定します。
  5. このストア URL の横にある［スクリプトのダウンロード］ボタンをクリックし、対応する StoreFront がインストールされているマシン上で管理者権限でこの PowerShell スクリプトを実行します。このスクリプトはすべての StoreFront マシンで実行する必要があります。

  > 注:
  >
  > アンインストール後にインストールを再試行する場合は、StoreFront 構成（StoreFront > ストア **> Delivery Controller-**Secure Private Access）に「Secure Private Access」という名前のエントリがないことを確認してください。Secure Private Access が存在する場合は、このエントリを削除してください。設定 > インテグレーションページからスクリプトを手動でダウンロードして実行します。

- エラーメッセージ: 次の StoreFront 構成はローカルではありません: <Store URL>

ウィザードを使用して Secure Private Access を設定したら、[設定] タブからゲートウェイエントリを編集できます。このエラーが発生した StoreFront ストアの URL を書き留めてください。

解決策:

この問題は、StoreFront が Secure Private Access と同じマシンにインストールされていない場合に発生します。StoreFront をインストールしたマシンで StoreFront 構成を手動で実行する必要があります。

1. [設定] をクリックし、[インテグレーション] タブをクリックします。
2.「**StoreFront** ストア **URL**」で、エラーが発生した StoreFront URL のエントリを特定します。
3. このストア URL の横にある［スクリプトのダウンロード］ボタンをクリックし、対応する StoreFront がインストールされているマシン上で管理者権限でこの PowerShell スクリプトを実行します。このスクリプトはすべての StoreFront マシンで実行する必要があります。

> 注:
>
> StoreFront PowerShell スクリプトを実行するには、管理者権限で Windows x64 互換の PowerShell ウィンドウを開き、ConfigureStoreFront.ps1 を実行します。StoreFront スクリプトは Windows PowerShell (x86) と互換性がありません。

- エラーメッセージ: PowerShell を使用して StoreFront スクリプトを実行しているときに「Get-STFStoreService: タイプ'Citrix.DeliveryServices.framework.feature.exceptions.registryKeyNotFoundExceptio の例外が発生しました。」。

  このエラーは、StoreFront スクリプトを x86 互換の PowerShell ウィンドウで実行した場合に発生します。

  解決策:

  StoreFront PowerShell スクリプトを実行するには、管理者権限で Windows x64 互換の PowerShell ウィンドウを開いてから`ConfigureStorefront.ps1`を実行します。

パブリックゲートウェイ/コールバックゲートウェイの障害

エラーメッセージ:: のゲートウェイエントリを作成できませんでした。<`Gateway URL`> または、次のコールバックゲートウェイエントリを作成できませんでした: <`Callback Gateway URL`>

解決策:

障害が発生したパブリックゲートウェイまたはコールバックゲートウェイの URL を書き留めておきます。ウィザードを使用して Secure Private Access を設定したら、[設定] タブからゲートウェイエントリを編集できます。

1. [設定] をクリックし、[インテグレーション] タブをクリックします。
2. パブリックゲートウェイアドレスまたはコールバックゲートウェイアドレスと、障害が発生した仮想 IP アドレスを更新します。

Secure Private Access サーバーにアクセスできない

エラーメッセージ:IIS プールを更新できませんでした。IIS プールを再起動できませんでした

解決策:

インターネットインフォメーションサービス (IIS) の [アプリケーションプール] に移動し、次のアプリケーションプールが起動して実行されていることを確認します。

- Secure Private Access ランタイム・プール
- Secure Private Access 管理者プール

また、デフォルトの IIS サイト`"Default Web Site"`が稼働していることも確認してください。

データベース接続チェックの失敗

エラーメッセージ**:** 接続チェックが失敗しました

データベース接続チェックは、複数の理由で失敗する可能性があります:

- ファイアウォールのため、Secure Private Access プラグインのホストマシンからデータベースサーバーにアクセスできません。

  解決策**:** データベースポート (デフォルトポート 1433) がファイアウォールで開いているかどうかを確認します。

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

  解決策**:**Secure Private Access の SQL データベース権限を参照してください。

ゲートウェイ接続チェックが失敗しました。公開証明書を取得できません

エラーメッセージ**:** インストール後の構成が次のエラーで失敗します。「ゲートウェイ接続チェックに失敗しました。公開証明書を取得できません…」

解決策:

- 構成ツールを使用して、ゲートウェイのパブリック証明書を Secure Private Access データベースに手動でアップロードします。
- PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
- ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)

- 次のコマンドを実行します:

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

アプリケーション列挙失敗

StoreFront の URL または NetScaler Gateway の URL の末尾にスラッシュ（/）が含まれていると、アプリケーションの列挙が中断されます。

解決策:

StoreFront ストア URL または NetScaler Gateway URL の末尾のスラッシュを削除します。詳しくは、「セットアップ後の StoreFront または NetScaler Gateway サーバーの詳細の更新」を参照してください。

その他

Secure Private Access 診断サポートバンドルの作成

次の手順を実行して、Secure Private Access 診断サポート・バンドルを作成します:

- PowerShell またはコマンドプロンプトウィンドウを管理者権限で開きます。
- ディレクトリを Secure Private Access インストールフォルダの下の Admin\ AdminConfigTool フォルダに変更します (たとえば、cd「C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ Admin\ AdminConfigTool」など)。
- 次のコマンドを実行します:

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

Secure Private Access の **SQL** データベース権限

データベースを自動作成するには、Secure Private Access プラグインホストマシンに、データベースに接続してデータベーススキーマを作成する権限が必要です。

リモートデータベース**:**

次の手順を実行して、リモートデータベースの権限を設定します。

1. 名前の構文CitrixAccessSecurity<Site Name>で空のデータベースを作成します。<Site Name>は、Secure Private Access のサイト名です。(例えば。CitrixAccessSecuritySPA)。

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


2. Secure Private Access 仮想マシンのマシン ID 用の SQL Server ログインを作成します。たとえば、Secure Private Access ブローカーのマシン名が HOST1 で、マシンドメインが DOMAIN1 の場合、マシン ID は「DOMAIN1\ HOST1$」になります。ログインが既に作成されている場合は、このステップは無視できます。

   ```
   USE CitrixAccessSecurity<SiteName>
   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   ドメイン名は次のクエリを使用して検索できます:

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. db_owner ロールをマシン ID に割り当てます。

   ```
   USE CitrixAccessSecurity<SiteName>
   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'
   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

ローカルデータベース**:**

ローカルデータベースの権限を設定するには、次の手順を実行します。

1. 名前の構文`CitrixAccessSecurity<Site Name>`で空のデータベースを作成します。`<Site Name>`は Secure Private Access のサイト名です。(たとえば、CitrixAccessSecuritySPA)。

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

2. `NT AUTHORITY\SYSTEM` ユーザーの SQL Server ログインを作成します。ログインが既に作成されている場合は、このステップは無視できます。

   ```
   USE CitrixAccessSecurity<SiteName>
   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. db_owner ロールを「NT AUTHORITY\SYSTEM」ユーザーに割り当てます。

   ```
   USE CitrixAccessSecurity<SiteName>
   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'
   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

データベースを手動で作成すると、ダウンロードしたデータベーススクリプトによってマシン ID に権限が追加されます。

トラブルシューティングログを保持

June 19, 2024

トラブルシューティングログページのログは、Secure Private Access データベースに 90 日間保存されます。ログの合計数が大きくなりすぎると (たとえば、100,000 を超えるなど)、90 日より前に最も古いログを削除できます。クリーンアップジョブは、デフォルトで 12 時間ごとに実行されます。このジョブは、ランタイムサービスが再起動するたびにも実行されます。

トラブルシューティングログの保持設定のカスタマイズ

ログのクリーンアップは、ランタイムサービスのインストールフォルダーにある appsettings.json ファイルを使用して設定できます。ログの保存期間とデータベースに保存できるログの数に基づいてクリーンアップを設定できます。必要に応じて、appsettings.json ファイル内の以下のエントリを変更します。

サンプルアプリ設定**.json** ファイル**:**

```
  "TroubleshootingLogs": {

    "CleanupPeriodInHours": 12,
    "CleanupDataOlderThanDays": 90,
    "CleanupOldestDataIfEntriesCountAbove": 100000
   }

<!--NeedCopy-->
```

クリーンアップを無効にするには、必要に応じて次の設定を行います。

- ログを 7 日間だけ保持するには、`CleanupDataOlderThanDays`を 7 に設定します。
- 日単位のクリーンアップを無効にするには、`CleanupDataOlderThanDays`を 0 に設定します。
- カウントベースのクリーンアップを無効にするには、`CleanupOldestDataIfEntriesCountAbove`を 0 に設定します。
- これらの設定が両方とも 0 に設定されている場合、または`CleanupPeriodInHours`が 0 に設定されている場合、ログは永久に保持されます。
  - ディスク使用率が 100% 低下する可能性があるため、`CleanupDataOlderThanDays`または`CleanupOldestDataIfEntriesCountAbove`の両方を 0 に、または`CleanupPeriodInHours`を 0 に設定することはお勧めしません。
  - ログのクリーンアップ頻度は、`CleanupPeriodInHours`エントリを変更して変更することもできます。

> 注**:**
>
> Secure Private Access をクラスターとして展開する場合、これらの設定は各クラスターノードで変更する必要があります。ノード設定に不一致がある場合は、最も頻繁にクリーンアップされるインスタンスが優先されます。

ログとテレメトリのクリーンアップ

June 19, 2024

テレメトリデータのクリーンアップ

テレメトリデータは、Secure Private Access データベースに 3 か月間保存されます。クリーンアップが必要なテレメトリデータを特定するためのチェックは、30 秒ごとに行われます。

> 注記:
>
> テレメトリデータのクリーンアップを開始するには、Runtime サービスが実行されている必要があります。

CDF ログのクリーンアップ

CDF ログは、Secure Private Access インストールマシンの Admin および Runtime サービスのインストールフォルダー内に保存されます。CDF ログは.csv ファイルに保存され、各ファイルには 10MB のサイズ制限が適用されます。
Admin サービスは一度に最大 90 個の CDF ログファイルを保持できます。その後、最も古いファイルを削除して、新しい CDF ログファイルを作成するためのスペースを空けます。
Runtime サービスは Admin サービスと同じように機能しますが、一度に保持できるファイル数は最大 600 個です。

CDF ログのカスタムクリーンアップ

CDF ログのクリーンアップは、管理サービスとランタイムサービスのインストールフォルダにある appsettings.json ファイルを使用して設定できます。ファイルのファイルサイズとカウント制限を変更するには、appsettings.json ファイルの次のエントリを更新します。

```
"CdfFile": {

       "fileSizeLimitBytes": 10485760, // 10 MB
       "retainedFileCountLimit": 600
      }

<!--NeedCopy-->
```

> 注:
>
> サイトに Secure Private Access の複数のインスタンスが設定されている場合は、Secure Private Access の各インストールマシンで appsettings.json ファイルを更新して CDF クリーンアップを行います。

Secure Private Access のアンインストール

June 19, 2024

Secure Private Access は、**[**コントロールパネル**] > [**プログラム**] > [**プログラムと機能] からアンインストールできます。

1.「**Citrix Virtual Apps and Desktops 7 2308 –Secure Private Access**」を選択します。
2.［アンインストール］をクリックします。
3. 画面の指示に従い、アンインストールを完了します。

> 注:
>
> Secure Private Access のインストール後のセットアップが完了したら、Secure Private Access をアンインストールする前に、管理コンソールから StoreFrontScripts.zip ファイルをダウンロードして、StoreFront ストア構成から Secure Private Access プラグインを削除してください。

StoreFrontScript の zip ファイルをダウンロードするには、次の手順に従ってください:

1. Secure Private Access 管理コンソールにログインします。
2. [設定] をクリックし、[インテグレーション] タブをクリックします。
3. StoreFront ストア URL セクションの「スクリプトのダウンロード」をクリックします。

StoreFront ストア構成から **Secure Private Access** プラグインを削除します

Secure Private Access をアンインストールしたら、StoreFront ストア構成から Secure Private Access プラグインを削除する必要があります。

1. StoreFront マシンにログインします。
2. StoreFrontScripts.zip ファイルをダウンロードします。
3. StoreFrontScripts.zip をフォルダに解凍します。
4. 管理者権限で PowerShell ウィンドウを開きます。
5. 次のコマンドを実行します:

```
cd <unzipped folder>
.\RemoveStorefrontConfiguration.ps1
```

Secure Private Access 2311 とレガシーバージョンとの互換性

June 19, 2024

Secure Private Access 2311 はレガシーバージョンと互換性がありません。NetScaler Gateway は、「NetScaler Gateway の構成」で前述したように、新しいスクリプトを使用して構成する必要があります。Secure Private Access のレガシーバージョンでは、Citrix Virtual Apps and Desktops Delivery Controller を構成する必要はありません。

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

- Web/SaaS アプリからの Citrix Virtual Apps and Desktops Delivery Controller
- Citrix StoreFront をデフォルト構成に更新するか、StoreFront に新しいストアを作成します
- NetScaler Gateway

Citrix Virtual Apps and Desktops Delivery Controller クリーンアップ

Citrix Virtual Apps and Desktops Delivery Controller で作成された Secure Private Access アプリケーションは、手動で削除することも、PowerShell スクリプトを使用して削除することもできます。

マニュアル:

1. Citrix Studio または Citrix ウェブスタジオを開きます。
2. 「アプリケーション」をクリックします。
3. アプリを選択し、右クリックして [削除] を選択します。

スクリプトの使用:

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

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

   詳細については、「Remove-Broker アプリケーション」を参照してください。

2. アプリを確認したら、次のコマンドを実行してアプリを削除します:

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

Citrix StoreFront クリーンアップ

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

- 新しい StoreFront ストアの作成: レガシーバージョン用に作成された既存の StoreFront ストアは 2311 と互換性がないため、Secure Private Access2311 用に新しい StoreFront toreFront ストアを作成する必要があります。これは、構成関連の問題を回避するための推奨オプションです。
- 既存の StoreFront ストアのクリーンアップ: StoreFront 上の既存のストアは、手動またはスクリプトを使用してクリーンアップできます。ただし、オンプレミスの Secure Private Access を 2311 に移行する最適なオプションは、StoreFront に新しいストアを作成することです。

マニュアル:

1. policy.json (例:C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json) を見つけて削除します。
2. SecureBrowser (例:C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser) とリソース (例:C:\inetpub\wwwroot\Citrix\Store\Resources) のフォルダを検索して削除します。
3. web.config (C:\inetpub\wwwroot\Citrix\Store にあります) から「WebSecurePolicy」という名前の「ルート」ノードを削除し、URL「Resources\ SecureBrowser\ policy.json」にルーティングします。
4. インターネットインフォメーションサービス **(IIS)** マネージャーコンソールで既定の **Web** サイトを再起動して変更を適用します。

スクリプトの使用:

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

   スクリプトは C:\inetpub\wwwroot\Citrix\Store\Resources フォルダー、サブフォルダー、およびファイルを削除し、web.config ファイルを更新します。
5. インターネットインフォメーションサービス **(IIS)** マネージャーコンソールで既定の **Web** サイトを再起動して変更を適用します。

NetScaler Gateway のクリーンアップ

NetScaler Gateway 仮想サーバー

レガシーバージョン用に作成された NetScaler Gateway 仮想サーバーは、Secure Private Access2311 に再利用できます。

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

セッションポリシーとアクション

レガシーバージョン用に作成されたセッションポリシーとアクションは、Secure Private Access2311 で再利用できます。

- 既存の NetScaler Gateway セッションポリシー/アクションを更新するには、「NetScaler Gateway セッションアクション」を参照してください。

- 新しい NetScaler ゲートウェイを構成するには、「NetScaler Gateway の構成」を参照してください。

このスクリプトは、完全に構成されたセッションポリシー/アクションも作成します。

承認ポリシー

NetScaler Gateway でレガシーバージョン用に作成された承認ポリシーは、Secure Private Access2311 ポリシーに干渉し、フローを中断する可能性があります。

認証ポリシーをクリーンアップするには、次の操作を行います。

- NetScaler Gateway でデフォルトグループとして使用されている認証グループと承認グループから、承認ポリシーを手動でバインド解除します。この場合、ポリシーを再利用できます。
- 承認ポリシーを削除します。

サードパーティ通知

June 19, 2024

Citrix Secure Private Access オンプレミス向け）