



Citrix Secure Private Access-オン プレミス

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使用の Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

新機能	2
既知の問題	2
Secure Private Access インストーラー	4
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	8
Secure Private Access のセットアップ	8
NetScaler Gateway の構成	15
アプリケーションの構成	21
アプリケーションのアクセスポリシーを設定します	24
エンドユーザーフロー	27
Secure Private Access と Web Studio の統合	29
インストール後に設定を管理	31
ダッシュボードの概要	32
エラーのトラブルシューティング	34
Secure Private Access のアンインストール	40
Secure Private Access 2308 とレガシーバージョンとの互換性	41
サードパーティ通知	43

新機能

January 9, 2024

2023 年 10 月

オンプレミス向け **Citrix Secure Private Access** –プレビュー

オンプレミス向け Citrix Secure Private Access は、現在プレビュー段階にあります。Secure Private Access オンプレミスソリューションには、Secure Private Access サービスと同様の外観を持つフルサービスの管理コンソール UI が含まれています。詳細については、「[オンプレミス向けの Secure Private Access –プレビュー](#)」を参照してください。

既知の問題

February 20, 2024

オンプレミス向け Citrix Secure Private Access ソリューションには、以下の既知の問題があります：

ドメインコントローラーの構成

- 同じフォレスト内または異なるフォレスト間のドメイン間の一方方向の信頼はサポートされていません。オンプレミス向け Secure Private Access ソリューションは、次の両方の条件が満たされている場合は機能しません。
 - オンプレミス用 Secure Private Access がインストールされているマシンのドメインは、Secure Private Access にログインしている管理者のドメインとは異なります。
 - マシンのドメインからユーザーのドメインへの信頼は設定されていません。
- sAMAccountName と UPN が異なる場合、列挙は失敗します。

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/ウェブ用ワークスペース

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。
- 管理者ユーザーは認証に失敗するため、デフォルトの「Domain Users」AD グループに属してはいけません。

アップグレード

ビルド間アップグレードはサポートされていません。オンプレミス用 Secure Private Access では、既存のインストールを削除してビルド間アップグレードで再インストールするよう求められます。

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

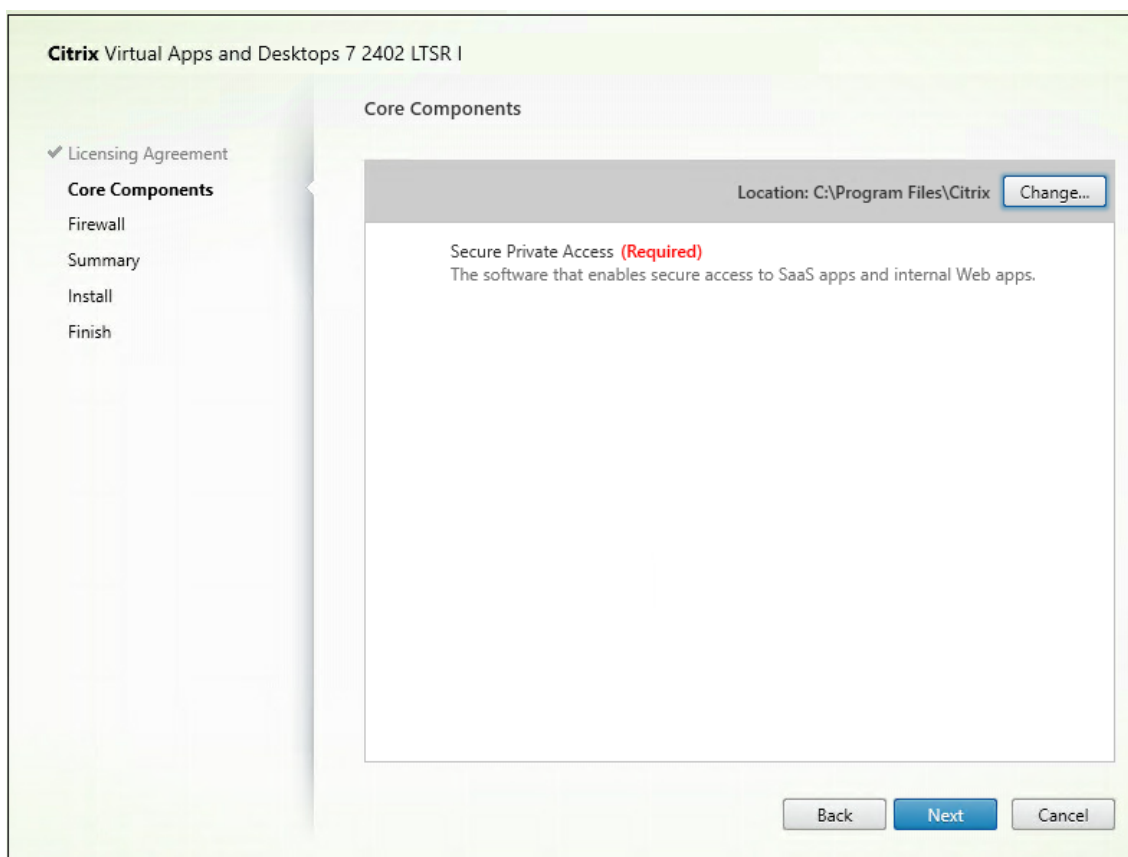
- クラスターのサポートバンドルの生成はサポートされていません。
- 管理サービスとランタイムサービスのログフォルダは削除しないでください。これらのフォルダを削除すると、Secure Private Access は再作成できません。

Secure Private Access インストーラー

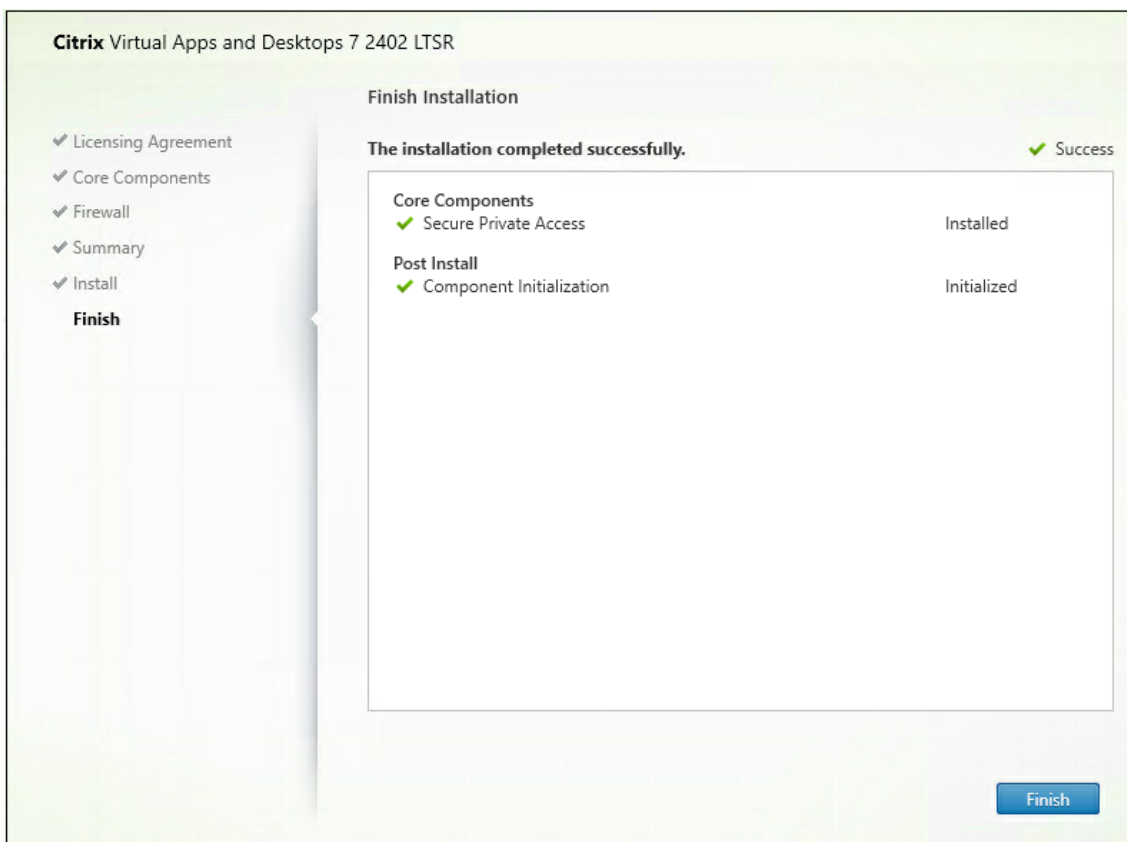
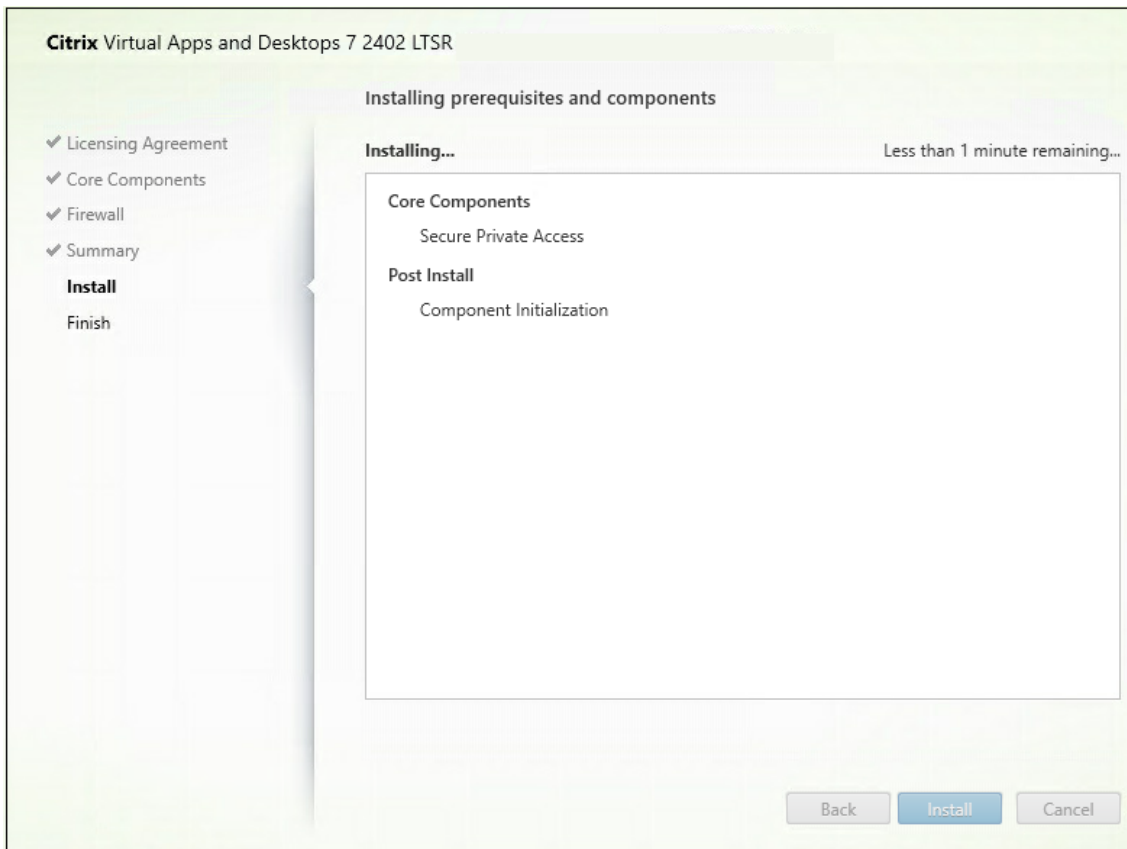
February 20, 2024

SecurePrivateAccessSetup_2308.exe を使用して Secure Private Access をインストールできます。

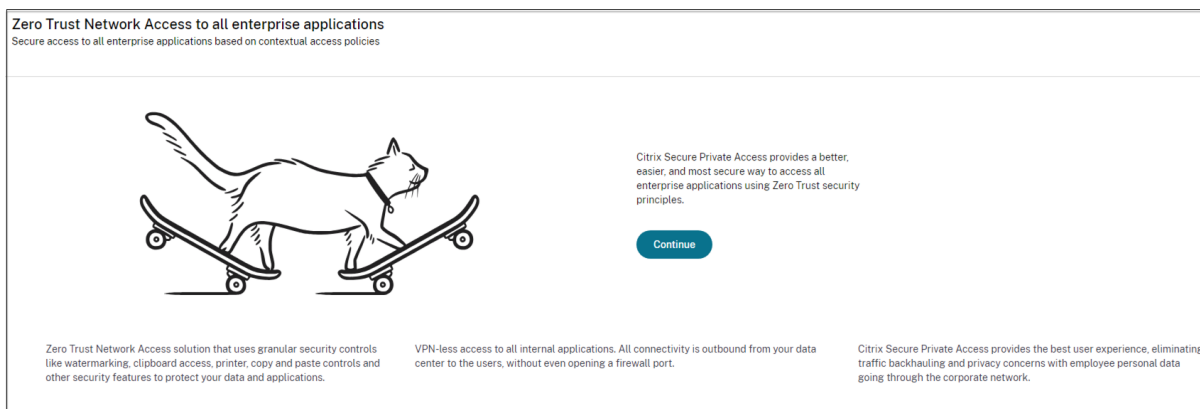
1. Citrix Secure Private Access のインストーラーを<https://www.citrix.com/downloads/citrix-early-access-release/>からダウンロードします。
2. ドメインに参加しているマシン（できれば StoreFront がインストールされているのと同じマシン）で、管理者として.exe を実行します。



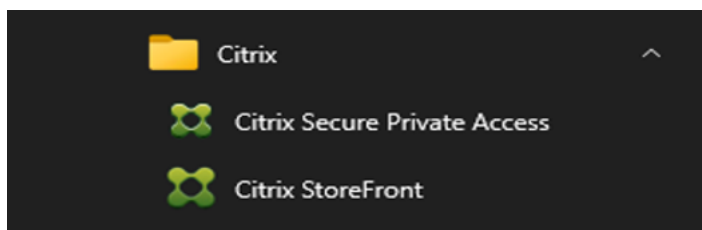
3. 画面の指示に従ってインストールを完了します。



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



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。



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。Secure Private Access は、インストールマシンと同じドメインに属するユーザーであれば誰でも Secure Private Access をセットアップできます。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場合に限ります。

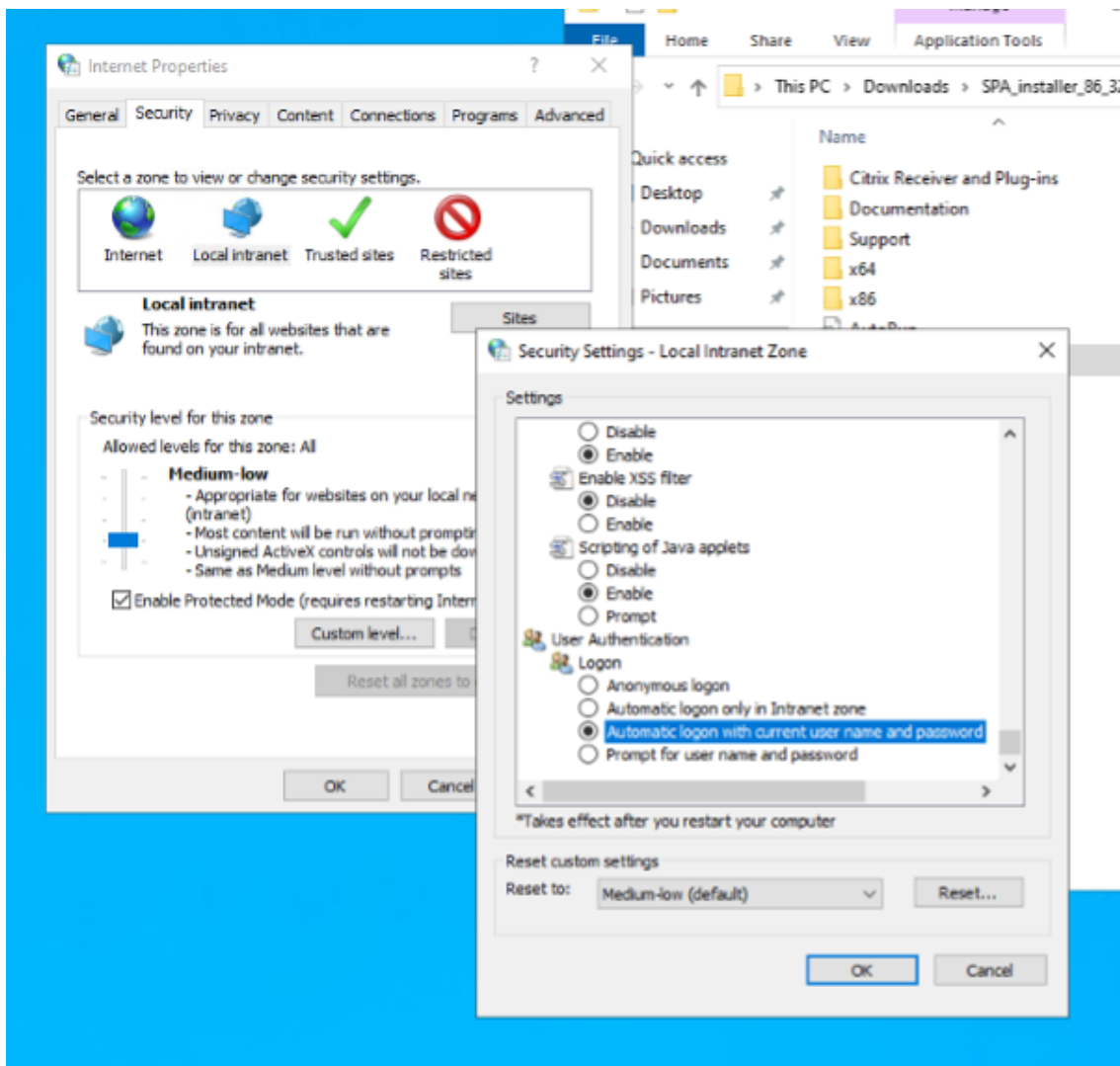
Google Chrome および Microsoft Edge ブラウザの場合は、次の手順を実行して Kerberos を有効にします。

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。たとえば、「https://*.fabrikam.local」などです。

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:

- 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。
- 他のブラウザについては、Kerberos 認証に関する特定のブラウザのドキュメントを確認してください。

次の手順

- [Secure Private Access のセットアップ](#)
- [NetScaler Gateway を構成します](#)
- [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

January 9, 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>
```

Secure Private Access のセットアップ

February 20, 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

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

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。

Zero Trust Network Access to all enterprise applications
Secure access to all enterprise applications based on contextual access policies

Step 1: Creating or joining a site
A Secure Private Access site is a cluster of servers that all share the same configuration.

Create a new Secure Private Access site
Select this option if this is your first time installing Secure Private Access.

Join an existing Secure Private Access site
Select this option to add additional instances to an existing Secure Private Access site.

Next

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。

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- Site
- Database
- Integrations
- Summary

Step 2: Database configuration

Every site requires its own database, which must be created by the database administrator or the machine identity. You can create the database on the same SQL server where you host the Citrix Virtual Apps and Desktops databases.

Enter the SQL Server address that will host the database and enter your desired site name.

SQL Server host* Site name*

Select how you would like to create and/or configure your database:

Automatically

With this option, we'll automatically configure the database for you. If the database doesn't exist, we'll automatically create one. For the automatic creation and configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

Manually

With this option, you must manually create and configure the database yourself. After creating an empty database, download the script and share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

注:

- 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:

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 権限がマシンにならない場合、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。

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- Site
- Database
- 3 Integrations**
- 4 Summary

Step 3: Integrations

Connect with StoreFront and NetScaler Gateway servers so they can route traffic to Secure Private Access servers.

Secure Private Access address *
Enter the address of your Secure Private Access server or the load balancer managing traffic for your Secure Private Access servers. The address doesn't need to be a public address.

 ✓

StoreFront Store URL *
Enter your complete StoreFront Store URL.

 ✓
[+ Add another Store URL](#)

Public NetScaler Gateway address *
Enter all the addresses of the NetScaler Gateways accessing StoreFront. If you have a Global Server Load Balancing (GSLB) deployment, add the GSLB addresses as well.

 ✓
[+ Add another public address](#)

NetScaler Gateway virtual IP address and callback URL *
Enter the callback URL and virtual IP (VIP) address from each NetScaler Gateway. Each entry must match the values configured in StoreFront. [Learn more](#)

Virtual IP address * ⓘ <input type="text" value="10.80.174.125"/>	Callback URL * ⓘ <input type="text" value="https://gwgamma.spaopdev.local"/> ✓
---	--

[+ Add another virtual IP address and callback URL](#)

Director URL *
Utilize the monitoring capabilities of Director in Secure Private Access. Enter the Director URL to configure Director for use in Secure Private Access. You must also use the configuration tool for Director as described in the [product documentation](#).

 ✓

License Server URL *
A license server is a mandatory component required to collect and process licensing data. Enter the License Server URL to configure this component.

 ✓

[Test all URLs](#)

[Back](#) [Next](#)

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。

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- ✓ Integrations
- ✓ Summary

Step 4: Summary

Review the summary of your Secure Private Access setup.

Administration

You are a full administrator on this site and can add other administrators if needed.

Configurations

- SQL Server Database has been configured. ✓
- StoreFront has been configured. ✓
- NetScaler Gateway connected. ✓
- Director connected. ✓
- License Server connected. ✓
- Secure Private Access server connected. ✓

Close

注:

- 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。

Zero Trust Network Access to all enterprise applications
Secure access to all enterprise applications based on contextual access policies

Site
② Database
③ Summary

Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host* ⓘ
ie.: sql.example.com,1433

Site name* ⓘ
ie.: Site1

Test connection

Select how you would like to create and/or configure your database:

Automatically
With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Manually [Download script](#)
With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Back Next

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。

Zero Trust Network Access to all enterprise applications
Secure access to all enterprise applications based on contextual access policies

1 Site

2 Database

3 Summary

Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host* ⓘ Site name* ⓘ

Select how you would like to create and/or configure your database:

Automatically

With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Manually

With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

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 を構成します](#)
- [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 の構成

February 20, 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-early-access-release/>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。

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

注:

- 一時データを保存するには、NetScaler /var/tmp フォルダを使用することをお勧めします。
- ファイルが LF 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。

- 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)。
- 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
```

- アップロードしたスクリプトを NetScaler シェルで実行します。

```
root@nszeta# cd /var/tmp
root@nszeta# chmod +x ns_gateway_secure_access.sh
root@nszeta# ./ns_gateway_secure_access.sh
NetScaler Gateway vsrver name (default: _SecureAccess_Gateway):
NetScaler Gateway IP: 192.168.1.100
NetScaler Gateway FQDN: gateway.yourdomain.com
SPA Plugin IP: 192.168.1.100
SPA Plugin FQDN: spa.yourdomain.com
StoreFront Store URL (including protocol http/https): https://storefront.yourdomain.com/Citrix/StoreSPA
NetScaler authentication profile name: auth_prof
NetScaler SSL server certificate name: star_yourdomain_com
Domain: yourdomain.com

***** Gateway configuration *****
NetScaler Gateway name: SecureAccess Gateway
NetScaler Gateway IP: 192.168.1.100
NetScaler Gateway FQDN: gateway.yourdomain.com
SPA Plugin FQDN: spa.yourdomain.com
SPA Plugin IP: 192.168.1.100
StoreFront Store URL: https://storefront.yourdomain.com/Citrix/StoreSPA
NetScaler authentication profile name: auth_prof
NetScaler Gateway server certificate name: star_yourdomain_com
Domain: yourdomain.com
*****

Checking SPA Plugin support...
NetScaler supports SPA Plugin
Enabling SPA Plugin support.....SUCCESS
Enabling ns_vpn_securebrowse_client_mode_enabled feature.....SUCCESS
Enabling ns_vpn_redirect_to_access_restricted_page_on_deny feature.....SUCCESS
Enabling ns_vpn_use_cdn_for_access_restricted_page feature.....SUCCESS
Persisting SPA Plugin setting nsapimgr -ys call=ns_vpn_enable_spa_onprem in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page in /nsconfig/rc.netscaler file.

NetScaler Gateway creation script ns_gateway_secure_access created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
patch -filename /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output
Check ns_gateway_secure_access_output file for output

root@nszeta#
```

- 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。

```

root@nsd# cat ns_gateway_secure_access
#####
#1. Upload file to NetScaler (e.g. /var/tmp)
#2. Run Batch command (e.g. batch fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output #
#3. Analyze output (e.g. cat /var/tmp/ns_gateway_secure_access_output)
#####
# Enable NetScaler features
enable ns feature SSL SOLVPN AAA RERWRITE IC

# Add NetScaler Gateway vserver
add vpn vserver _SecureAccess_Gateway SSL 333.333.333.443 -listenpolicy NONE -tcpProfileName netcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.domain.com -authProfile
auth_prof -icaOnly OFF

# Add default AAA group for authenticated users
add aaa group SecureAccessGroup

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains storefront.domain.com
bind policy patset ns_cvpn_default_bypass_domains spa.domain.com
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIP OFF -icaProxy OFF -whome "https://storefront.domain.com/Citrix/SPAStoreW
-ClientChoices OFF -nDomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sta
refronturl "https://storefront.domain.com" -isGatewayallType domain

add vpn sessionAction AC_WS_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIP OFF -icaProxy OFF -whome "https://storefront.domain.com/Citrix/SPAStoreW
-ClientChoices OFF -nDomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sta
refronturl "https://storefront.domain.com" -isGatewayallType domain

# Add session policies
add vpn sessionPolicy PL_OS_SecureAccess_Gateway "HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")" AC_OS_SecureAccess_Gateway
add vpn sessionPolicy PL_WS_SecureAccess_Gateway "HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT" AC_WS_SecureAccess_Gateway

# Add rewrite policies for Citrix headers
add rewrite action Add_X-Citrix-Via insert_http_header X-Citrix-Via "*"gateway.domain.com""
add rewrite action Add_X-Citrix-Via-VIP insert_http_header X-Citrix-Via-VIP "*"333.333.333.443""
add rewrite action Add_X-OW-SessionId insert_http_header X-OW-SessionId AAA.USER.SESSIONID
add rewrite policy Add_X-Citrix-Via0 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com") && HTTP.REQ.HEADER("X-Citrix-Via").EXISTS.NOT" Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VIP01 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com") && HTTP.REQ.HEADER("X-Citrix-Via-VIP").EXISTS.NOT" Add_X-Citrix-Via-VIP
add rewrite policy Add_X-OW-SessionId01 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com")" Add_X-OW-SessionId

# Add SSO traffic policy for SPA Plugin
add vpn trafficPolicy _SecureAccess_Gateway_Traffic Action http -SSO ON

```

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。たとえば、

```
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:

```
1 `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:

```
1 `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_onpre` 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・ゲートウェイ証明書を Secure Private Access データベースにアップロードするには、次の手順を実行します:

1. 管理者権限で PowerShell またはコマンドプロンプトウィンドウを開きます。
2. 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>
```

アプリケーションの構成

February 20, 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。

Add an app ✕

To add an app, complete the steps below.

▼ App Details

Where is the application located? *

Outside my corporate network

Inside my corporate network

App name *

App description

App category ?

App icon [Change icon](#) [Use default icon](#)
(128 KB max, ICO)

Do not display application to users ?

Add application to favorites automatically ?

Allow user to remove from favorites

Do not allow user to remove from favorites

URL *

App Connectivity * ?

Related Domains *

App Connectivity * ?

[+ Add another related domain](#)

- 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

January 9, 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。


The screenshot shows the 'Create Access Policy' dialog box. The title bar says 'Create Access Policy' with a close button. Below the title bar, it says 'Create a policy to enforce application access rules based on a user's context.' The dialog is divided into several sections: 'Applications' with a dropdown menu showing 'Google'; 'If the following condition is met' with 'User/user groups*' selected, 'Matches any of' chosen, and two conditions listed: 'spaopdev.local' and 'SPAOP users'; 'Then do the following' with 'Allow access' selected; 'Policy name' with 'Google-Win11' entered; and a checked checkbox for 'Enable policy on save'. At the bottom, there are 'Save' and 'Cancel' buttons. A watermark for 'Activate Windows' is visible in the bottom right corner.

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。

Then do the following

Allow access with restrictions 

Available security restrictions:

- Restrict clipboard access 
- Restrict printing 
- Restrict downloads 
- Restrict uploads 
- Display watermark 
- *Restrict key logging 
- *Restrict screen capture 

*Applicable to Citrix Workspace desktop clients only.

- クリップボードへのアクセスを制限する: アプリとシステムクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- 印刷制限: 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: 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。
- ウォーターマークの表示: 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、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: 任意の画面キャプチャプログラムまたはアプリを使用して画面をキャプチャする機能を無効にします。ユーザーが画面をキャプチャしようとする、空白の画面がキャプチャされます。

注:

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

7. [ポリシー名] に、ポリシーの名前を入力します。
8. [保存時にポリシーを有効にする] を選択します。このオプションを選択しない場合、ポリシーは作成されるだけで、アプリケーションには適用されません。または、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

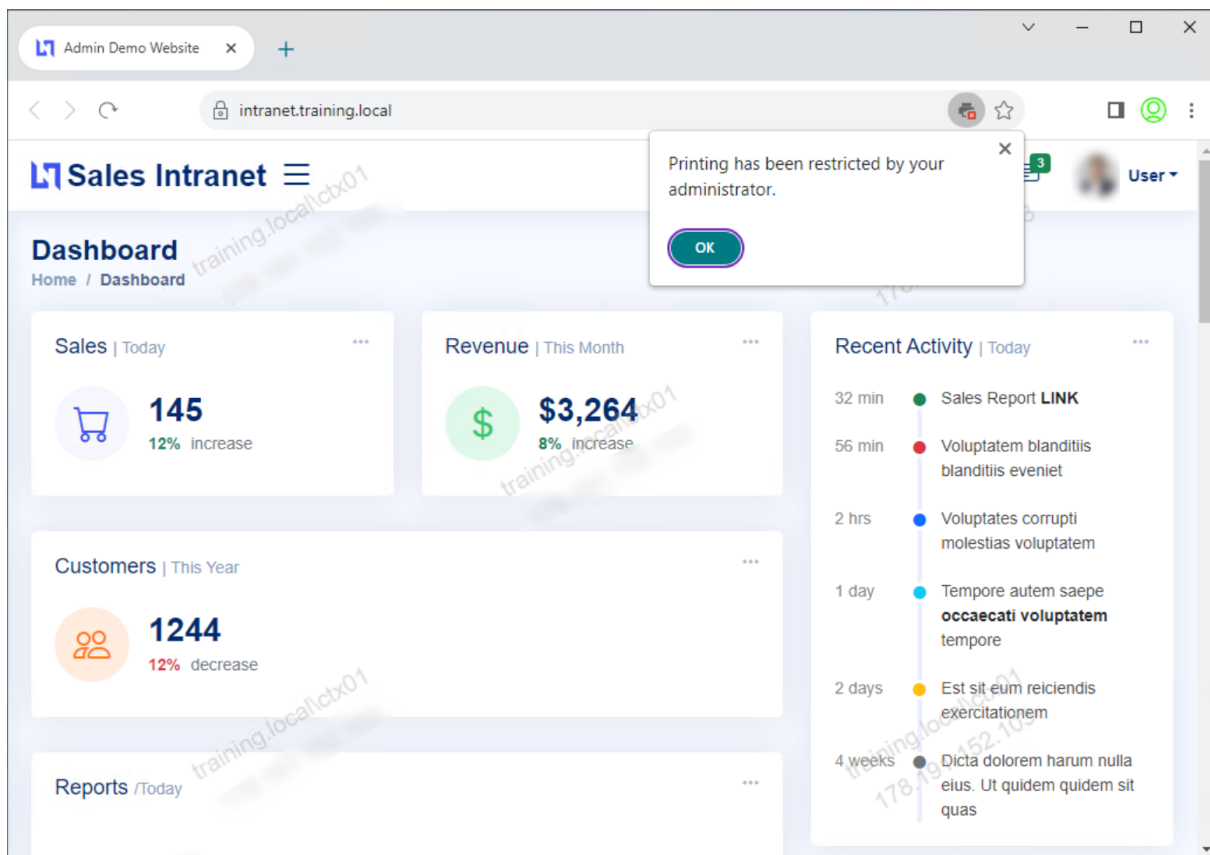
クライアントマシン (Windows および macOS) から構成を検証します。

Example

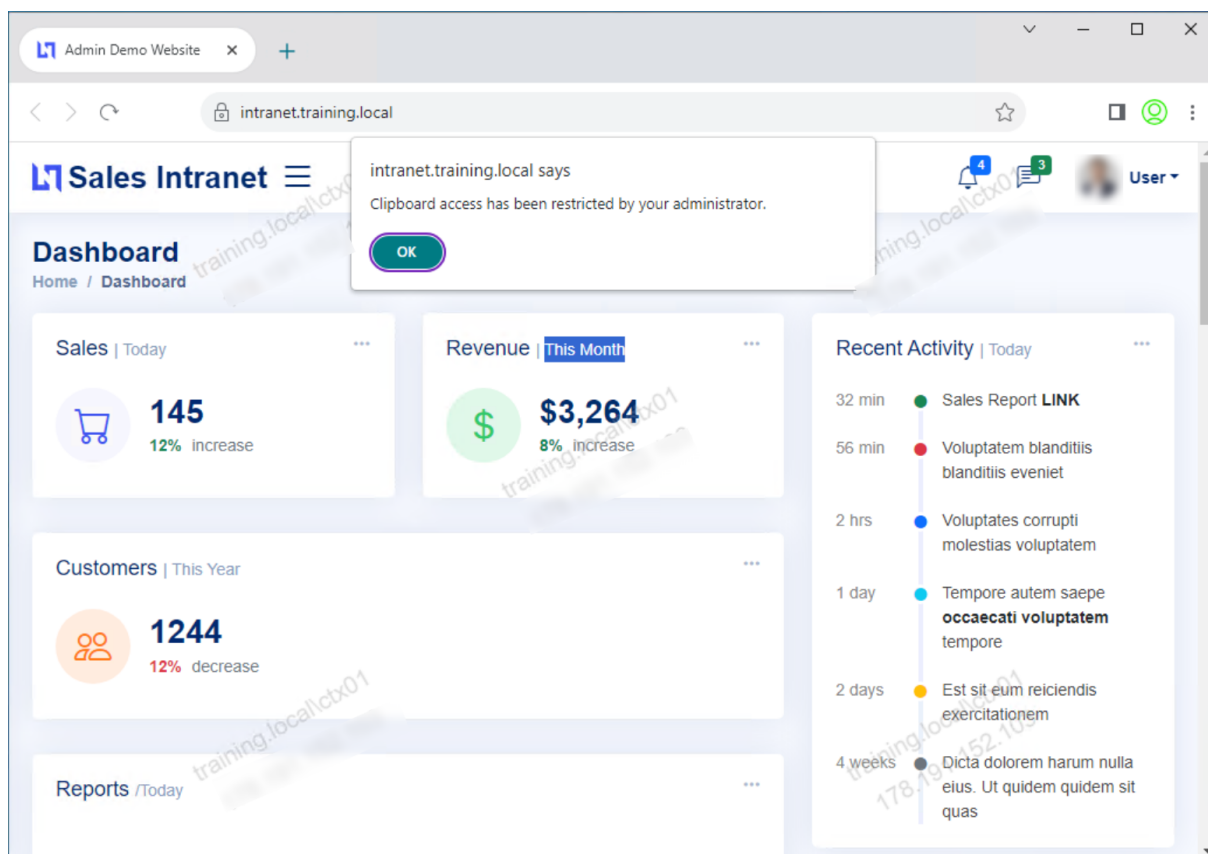
エンドユーザーフロー

January 9, 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時、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。

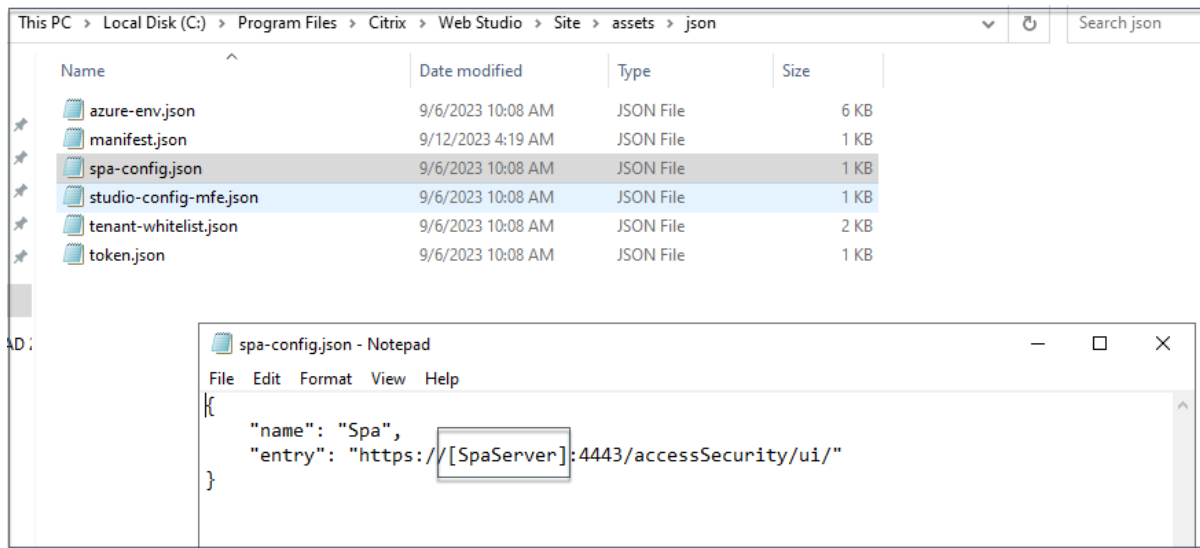
Web Studio バージョン 2308 以降をインストールする必要があります。

Web Studio 統合を有効にするには、次の手順を実行します：

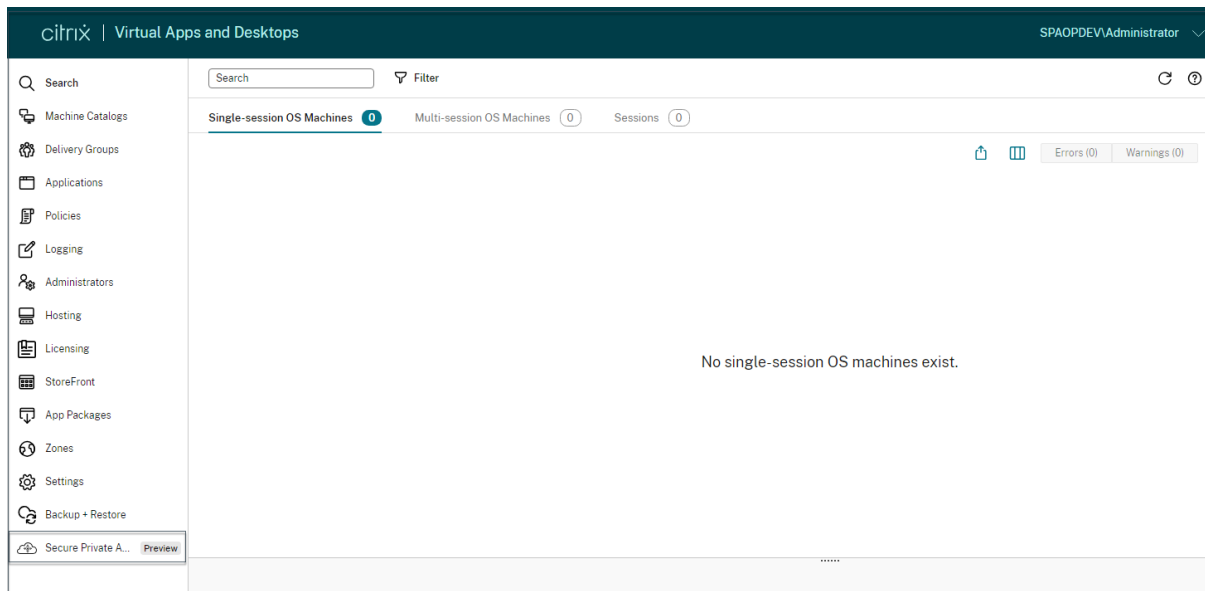
1. Citrix Virtual Apps and Desktops インストーラーまたは統合 DDC インストーラーを使用して Citrix Web Studio をインストールします。
2. 画面上の指示に従い、インストールを完了します。コントローラアドレスの入力を求められたら、コントローラアドレスとして DDC FQDN を入力します。

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。



1. 左側のナビゲーションメニューで、「**Secure Private Access <Preview>**」をクリックして、Web Studio から Secure Private Access 管理コンソールにアクセスします。

インストール後に設定を管理

January 9, 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。

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。

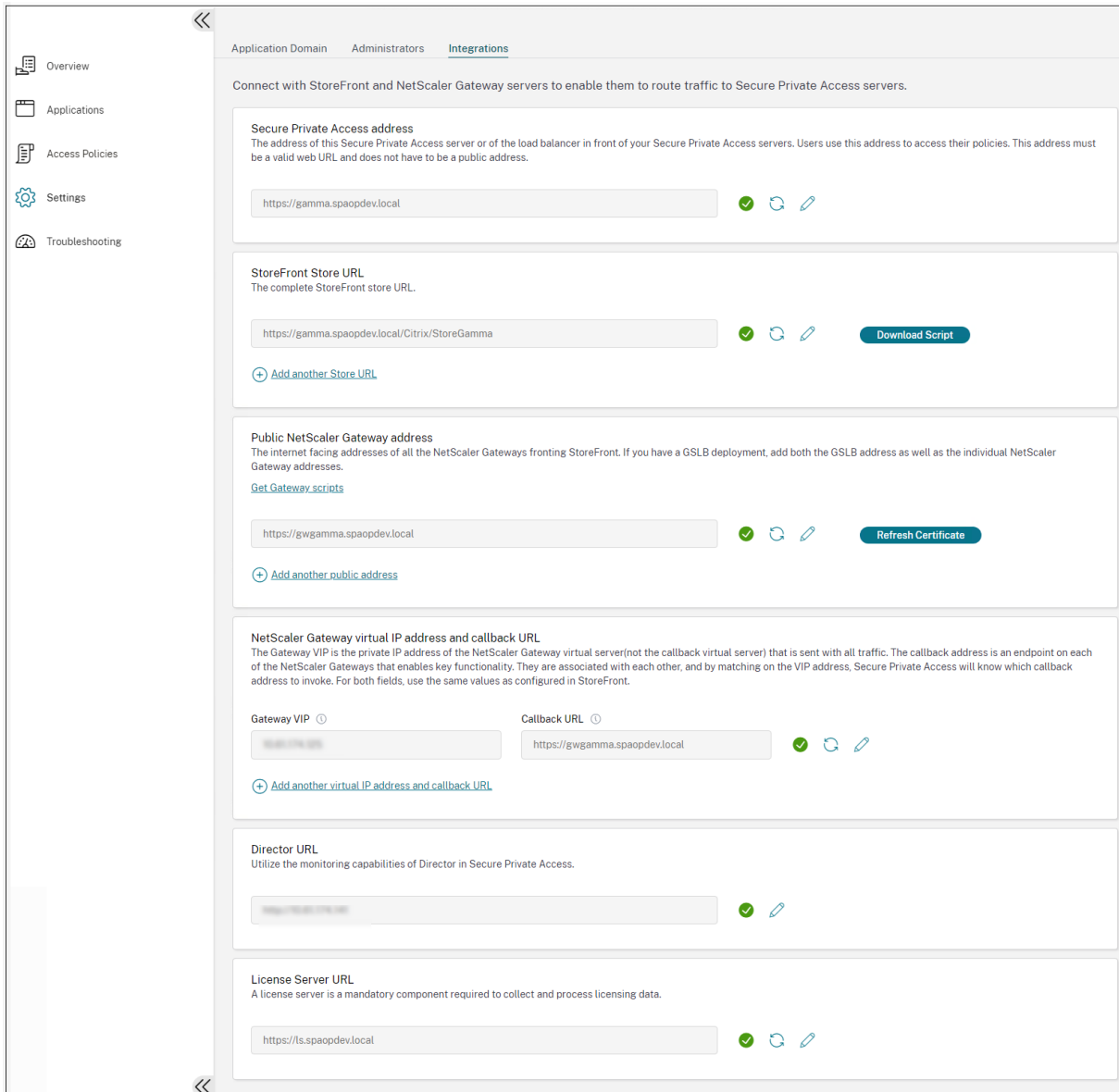
セットアップ後に **StoreFront** または **NetScaler Gateway** サーバーの詳細を更新する

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

January 9, 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。

The screenshot displays the search interface with a filter set to 'User-Name = "User"'. The search results table is as follows:

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Show Details
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Policy evaluatic
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	SmartAccess tr
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Received Gatev
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Successfully ve
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Total apps enur
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Show Details
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	SmartAccess tr
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Credential valir

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の適用チャートでの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が含まれていないログ/ポリシーを検索します。

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

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-09-07 10:29:13	spaopdev.local/usera	App Access	Failure	9c7c2de9-0351-43b1-8...	ERROR: Error in process...
2023-09-07 10:29:13	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 10:29:12	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 10:29:12	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	DSAuth validation was s...
2023-09-07 09:48:50	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	Successfully generated ...
2023-09-07 09:48:50	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 09:48:49	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 09:48:49	spaopdev.local/usera	App Access	Success	9c7c2de9-0351-43b1-8...	DSAuth validation was s...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	Show Details
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	Policy evaluation return...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	SmartAccess tags recei...
2023-09-07 09:48:40	spaopdev.local/usera	App Access	Success	22592f2f-f17b-4a5f-96...	DSAuth validation was s...
2023-09-07 09:46:27	spaopdev.local/usera	App Access	Failure	6e9d1dd1-5bdb-4474-8...	ERROR: Error in process...

エラーのトラブルシューティング

February 20, 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。

[\[証明書エラーデータベース作成エラー\]/\[ja-jp/citrix-secure-private-access/2308/spa-onprem-troubleshooting#database-creation-errors\]](#)

[StoreFront 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。

回避策: Citrix Virtual Apps and Desktops と同じ方法で Gateway 証明書を更新します。

データベース作成エラー

- エラーメッセージ: データベース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、次のいずれかのシナリオで発生する可能性があります。

- データベースの構成時に「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実行します。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

解像度:

- 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。

解像度:

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>

解像度:

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。

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。

解像度:

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。

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。

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>

解像度:

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

解像度:

1. 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>
```

認証に関する問題

統合 Windows 認証 (IWA) がサポートされていないため、Secure Private Access ランタイム・サービスの IIS 認証構成が機能しない場合があります。

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的に作成するには、Secure Private Access プラグインのホストマシンに、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。

Secure Private Access のアンインストール

January 9, 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 2308 とレガシーバージョンとの互換性

February 20, 2024

Secure Private Access 2308 は、レガシーバージョン (オンプレミス V1.0 および V1.5 の Secure Private Access) 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 2308 では、Citrix Virtual Apps and Desktops Delivery Controller を構成する必要はありません。

Secure Private Access オンプレミスのレガシーバージョン (1.0 および 1.5) から 2308 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: 従来のバージョン用に作成された既存の StoreFront ストアは 2308 と互換性がないため、Secure Private Access 2308 用に新しい StoreFront ストアを作成する必要があります。これは、構成関連の問題を回避するための推奨オプションです。
- 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 2308 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 を検索して削除します (例 C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json)
2. SecureBrowser (C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser など) フォルダとリソース (C:\inetpub\wwwroot\Citrix\Store\Resources など) フォルダを検索して削除する
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、「Resources\SecureBrowser\policy.json」の URL 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、サブフォルダ、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（1.0 および 1.5）用に作成された NetScaler Gateway 仮想サーバーは、Secure Private Access 2308 で再利用できます。

- 既存の NetScaler Gateway を更新するには、「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（1.0 と 1.5）用に作成されたセッションポリシーとアクションは、Secure Private Access 2308 で再利用できます。

- 既存の NetScaler Gateway セッションポリシー/アクションを更新するには、「NetScaler Gateway 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（1.0 および 1.5）用に作成された承認ポリシーは、Secure Private Access 2308 ポリシーを妨害し、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

January 9, 2024

[Citrix Secure Private Access オンプレミス向け](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).