Citrix Secure Private Access-レガシー

Machine translated content

Disclaimer

Contents

オンプレミスデプロイメント用の **Secure Private Access** の設定-レガシー

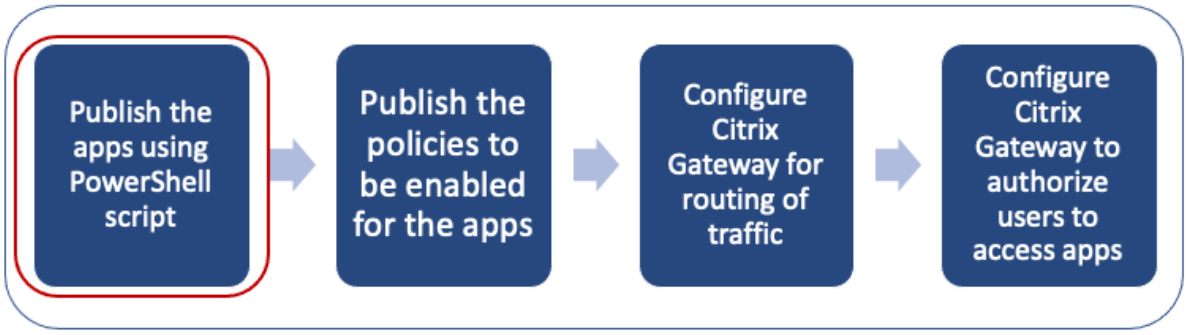
January 9, 2024

オンプレミス向け Secure Private Access ソリューションの設定は、4 段階のプロセスです。

1. アプリを公開
2. アプリのポリシーを公開
3. NetScaler Gateway 経由のトラフィックのルーティングを有効にする
4. 承認ポリシーの設定

> 重要:
>
> 構成ツールを使用すると、アプリやポリシーをすばやくオンボーディングしたり、NetScaler Gateway と StoreFront の設定を構成したりできます。ただし、ツールを使用する前に次の点に注意してください。
>
> - 「アプリを公開する 」セクションと 「アプリのポリシーを公開 」セクションを読んで、オンプレミスソリューション構成の設定要件を完全に理解していることを確認してください。
> - このツールは、このトピックに記載されている既存の手順を補完するものとしてのみ使用でき、手動で行う必要がある構成に代わるものではありません。
>
> ツールの詳細については、「Secure Private Access 設定ツールを使用してアプリとポリシーを構成する」を参照してください。

ステップ **1:** アプリを公開する



URL を公開するには PowerShell スクリプトを使用する必要があります。アプリを公開すると、Citrix Studio コンソールを使用して管理できます。

PowerShell スクリプトは、https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.htmlからダウンロードできます。

1. PowerShell SDK をインストール済みのマシンで PowerShell を開きます。
2. 次のコマンドを実行します:

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

3. Web アプリの変数を定義します。

```
$citrixUrl: "<URL of the app>"
$appName: <app name as it must appear on Workspace>
$DesktopGroupId: 1
$desktopgroupname: <your desktop group name>
$AppIconFilePath: <path of the image file>
<!--NeedCopy-->
```

> 注:
>
> コマンドを実行する前に、角括弧 (< >) でマークされたプレースホルダーを必ず更新してください。

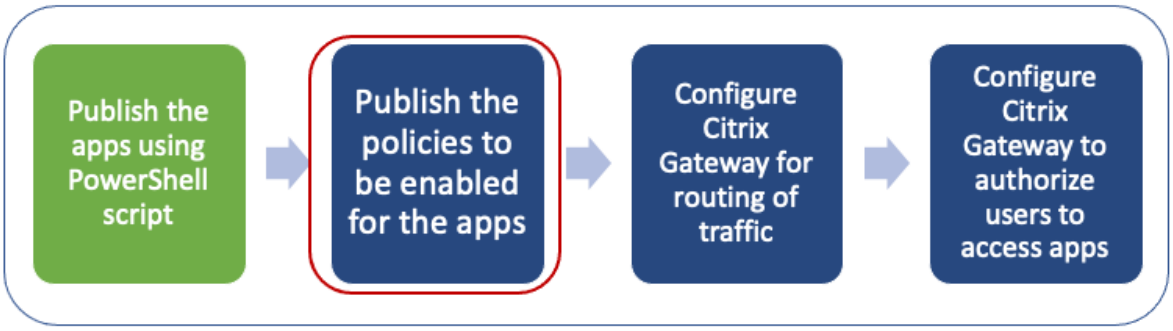
場所とアプリケーション名を割り当てたら、次のコマンドを実行してアプリケーションを公開します。

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

公開されたアプリは、**Citrix Studio** の［アプリケーション］セクションに表示されます。Citrix Studio コンソール自体からアプリの詳細を変更できるようになりました。

アプリの公開と公開済みアプリのデフォルトアイコンの変更について詳しくは、「コンテンツの公開」を参照してください。

ステップ **2:** アプリのポリシーを公開する



ポリシーファイルには、公開された各アプリのルーティングとセキュリティ制御が定義されています。Web または SaaS アプリケーションのルーティング方法 (ゲートウェイ経由またはゲートウェイなし) に関するポリシーファイルを更新する必要があります。

アプリにアクセスポリシーを適用するには、Web アプリまたは SaaS アプリごとにポリシーを公開する必要があります。そのためには、ポリシーの JSON ファイルと Web.config ファイルを更新する必要があります。

- ポリシー **JSON** ファイル**:** ポリシー JSON ファイルをアプリの詳細とアプリのセキュリティポリシーで更新します。次に、ポリシー JSON ファイルを `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`にある StoreFront サーバーに配置する必要があります。

  > 注**:**
  >
  > 「リソース」と「**SecureBrowser**」という名前のフォルダーを作成し、「**SecureBrowser** 」フォルダーにポリシー JSON ファイルを追加する必要があります。
  > さまざまなポリシーアクションとその値の詳細については、「アプリケーションアクセスポリシーの詳細」を参照してください。

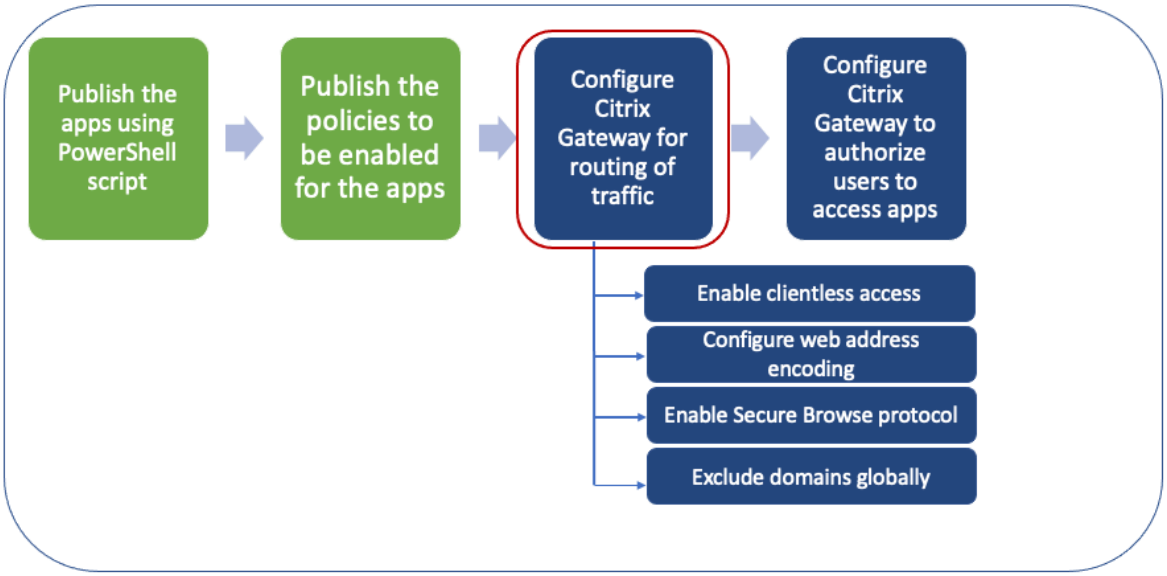
- **Web.config** ファイル: 新しいポリシーの詳細を Citrix Workspace アプリと Citrix Enterprise Browser で使用できるようにするには、StoreFront ストアディレクトリにある web.config ファイルを変更する必要があります。ファイルを編集して、route という名前の新しい XML タグを追加する必要があります。次に、Web.config ファイルを C:\inetpub\wwwroot\Citrix\Store1. という場所に配置する必要があります

  XML ファイルの例については、「エンドツーエンド設定の例 」を参照してください。

  > 注**:**
  >
  > パス内の「store1」は、ストアが作成されたときに指定された名前を指します。別のストア名を使用する場合は、適切なフォルダを作成する必要があります。

  既存のルートの最後に新しいルートを追加することをお勧めします。途中でルートを追加する場合は、後続のすべてのルートの注文番号を手動で更新する必要があります。

手順 **3: NetScaler Gateway** 経由のトラフィックのルーティングを有効にする



NetScaler Gateway を介したトラフィックのルーティングを有効にするには、次の手順が必要です。

- クライアントレスアクセスを有効にする
- URL エンコーディングを有効にする
- Secure Browse を有効にする
- クライアントレスアクセスモードでのドメインの書き換えから除外する

クライアントレスアクセス、URL エンコーディング、およびセキュアブラウズは、グローバルに、またはセッションポリシーごとに有効にできます。

- グローバルに有効な設定は、構成済みのすべての NetScaler Gateway 仮想サーバーに適用されます。
- セッションごとのポリシー設定は、ユーザー、グループ、または Gateway 仮想サーバーに適用されます。

クライアントレスアクセスを有効にする

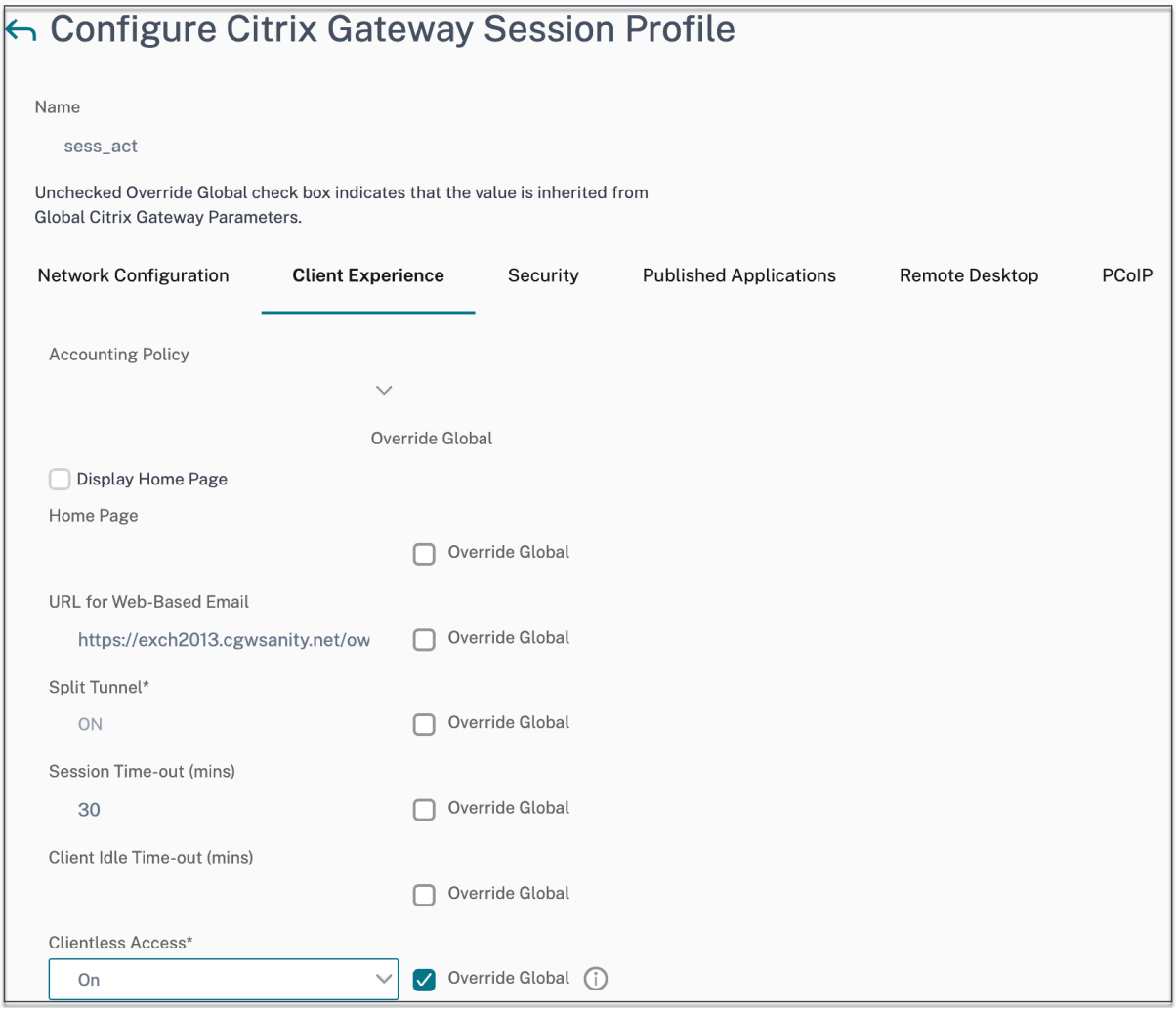
NetScaler Gateway GUI を使用してクライアントレスアクセスをグローバルに有効にするには:

［構成］タブの［**Citrix Gateway** ］を展開し、［グローバル設定］をクリックします。
「グローバル設定」ページで、「グローバル設定の変更」をクリックします。
「クライアントエクスペリエンス」タブの「クライアントレスアクセス」で、「オン」を選択し、「**OK**」をクリックします。

NetScaler Gateway GUI を使用してセッションポリシーを使用してクライアントレスアクセスを有効にするには:

選択したユーザ、グループ、または仮想サーバのグループだけにクライアントレスアクセスを使用する場合は、クライアントレスアクセスをグローバルに無効またはクリアします。次に、セッションポリシーを使用して、クライアントレスアクセスを有効にし、ユーザー、グループ、または仮想サーバーにバインドします。

1. [構成] タブで [**Citrix Gateway**] を展開し、[ポリシー] **>** [セッション] をクリックします。
2. [セッションポリシー] タブをクリックし、[追加] をクリックします。
3. **[**名前] に、ポリシーの名前を入力します。
4. **[**プロフィール**]** の横にある **[**新規**]** をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. **[**クライアントエクスペリエンス**]** タブの [クライアントレスアクセス] の横にある **[**グローバルオーバーライド**]** をクリックし、**[**オン**]** を選択して **[**作成**]** をクリックします。
7. エクスプレッションに、**`true`**と入力します。値**`true`**を入力すると、ポリシーは常にバインドされているレベルに適用されます。
8. [作成] をクリックし、[閉じる] をクリックします。



NetScaler Gateway CLI を使用してクライアントレスアクセスをグローバルに有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

```
set vpn parameter -clientlessVpnMode On -icaProxy OFF
<!--NeedCopy-->
```

NetScaler Gateway CLI を使用してセッションごとのクライアントレスアクセスを有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

```
set vpn sessionAction <session-profile-name> -clientlessVpnMode On -
   icaProxy OFF
<!--NeedCopy-->
```

URL エンコーディングを有効にする

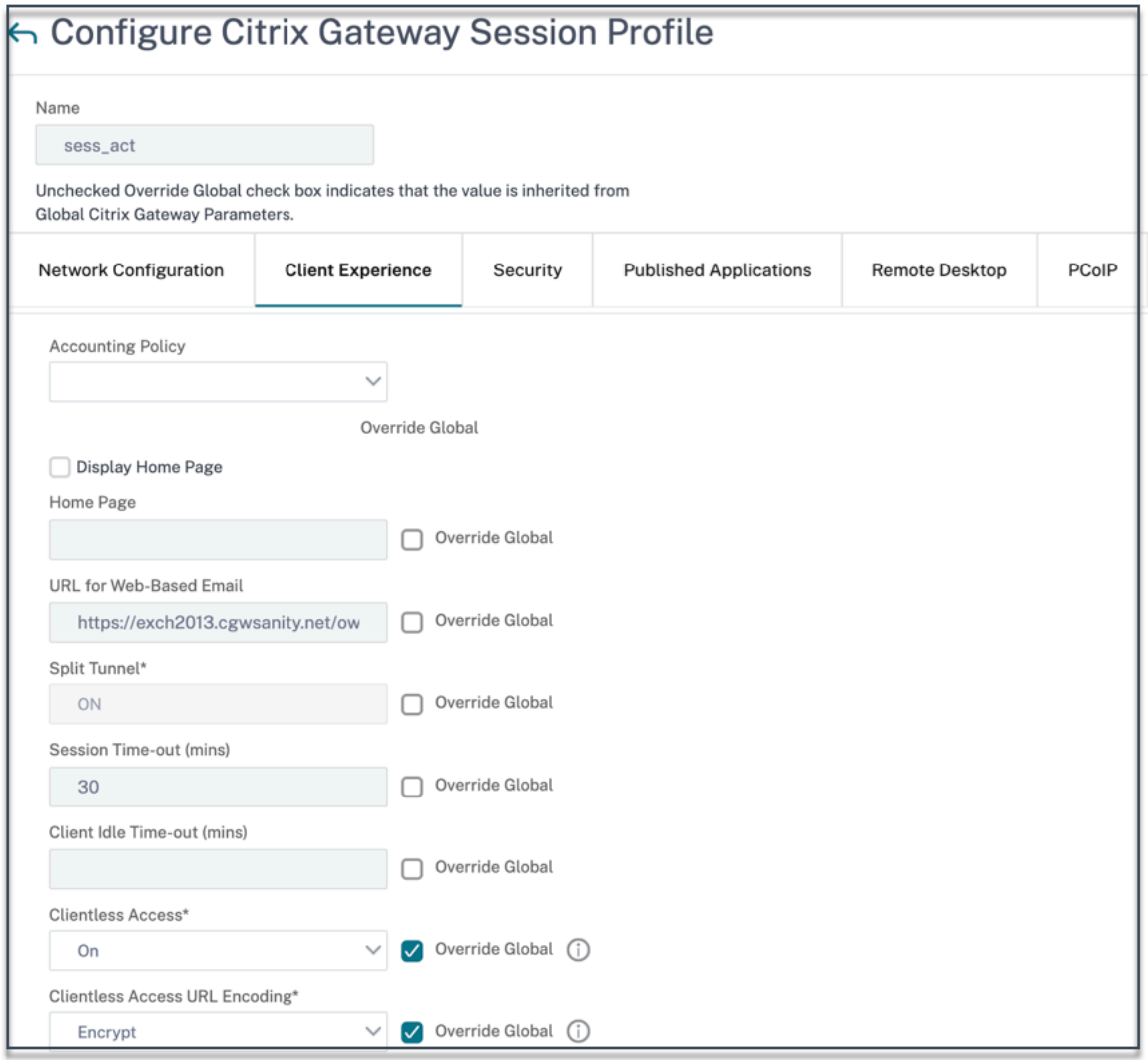
クライアントレスアクセスを有効にすると、内部 Web アプリケーションのアドレスをエンコードするか、アドレスをクリアテキストのままにするかを選択できます。クライアントレスアクセスのため、Web アドレスはクリアテキストのままにしておくことをお勧めします。

NetScaler Gateway GUI を使用して **URL** エンコーディングをグローバルに有効にするには:

1. [構成] タブの [**Citrix Gateway**] を展開し、[グローバル設定] をクリックします。
2. 「グローバル設定」ページで、「グローバル設定の変更」をクリックします。
3. 「クライアントエクスペリエンス」タブの「クライアントレスアクセス **URL** エンコーディング」で、Web URL をエンコードする設定を選択し、「**OK**」をクリックします。

NetScaler Gateway GUI を使用してセッションポリシーレベルで **URL** エンコーディングを有効にするには:

1. [構成] タブで [**Citrix Gateway**] を展開し、[ポリシー] **>** [セッション] をクリックします。
2. [セッションポリシー] タブをクリックし、[追加] をクリックします。
3. **[**名前] に、ポリシーの名前を入力します。
4. **[**プロフィール**]** の横にある **[**新規**]** をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. 「クライアントエクスペリエンス」タブで、「クライアントレスアクセス **URL** エンコーディング」の横にある「グローバルオーバーライド」をクリックし、エンコードレベルを選択して「**OK**」をクリックします。
7. エクスプレッションに、`true`と入力します。値`true`を入力すると、ポリシーは常にバインドされているレベルに適用されます。



NetScaler Gateway CLI を使用して **URL** エンコーディングをグローバルに有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

```
1 set vpn parameter -clientlessModeUrlEncoding TRANSPARENT
2 <!--NeedCopy-->
```

NetScaler Gateway CLI を使用してセッションごとの **URL** エンコーディングポリシーを有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

```
1 set vpn sessionAction <session-profile-name> -clientlessModeUrlEncoding
      TRANSPARENT
2 <!--NeedCopy-->
```


Secure Browse を有効にする

セキュアブラウズとクライアントレスアクセスが連携して、クライアントレス VPN モードを使用した接続が可能になります。Citrix Enterprise Browser がセキュアブラウズモードを使用してレガシー VPN なしでアプリにアクセスできるようにするには、セキュアブラウズモードを有効にする必要があります。

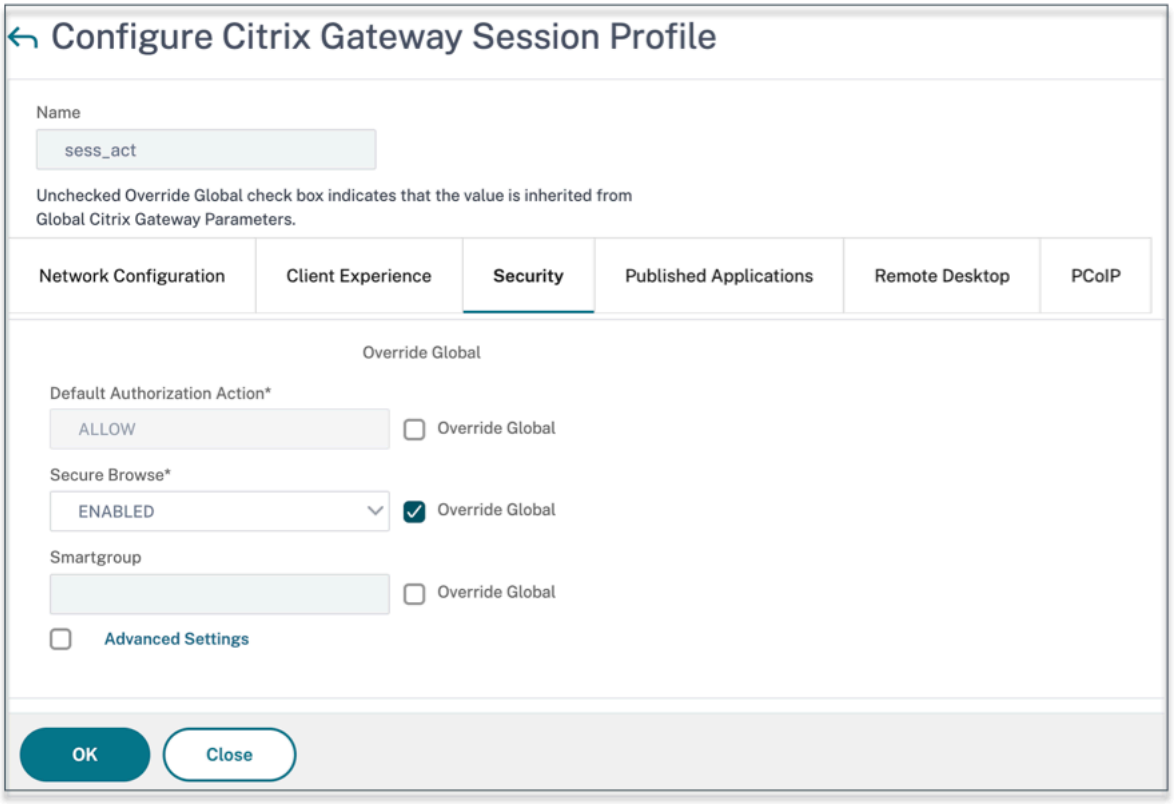
> 注:
>
> エンドユーザーが Citrix Enterprise Browser をインストールしていない場合、**SPAEnabled** タグが付いた公開 **URL** は、Citrix Enterprise Browser ではなくデバイスのデフォルトブラウザーで開きます。このような場合、セキュリティポリシーは適用されません。この問題は、StoreFront 展開環境でのみ発生します。

NetScaler Gateway GUI を使用してセキュアブラウズモードをグローバルに有効にするには:

1. ［構成］タブの［**Citrix Gateway** ］を展開し、［グローバル設定］をクリックします。
2. 「グローバル設定」ページで、「グローバル設定の変更」をクリックします。
3. 「セキュリティ」タブの「Secure Browse」で、「有効」を選択し、「**OK**」をクリックします。

NetScaler Gateway GUI を使用してセッションポリシーレベルでセキュアブラウズモードを有効にするには:

1. ［構成］タブで［**Citrix Gateway** ］を展開し、［ポリシー］**>** ［セッション］をクリックします。
2. [セッションポリシー] タブをクリックし、[追加] をクリックします。
3. **[**名前] に、ポリシーの名前を入力します。
4. **[**プロフィール**]** の横にある **[**新規**]** をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブで [グローバルオーバーライド] をクリックし、[**Secure Browse**] を [有効] に設定します。



NetScaler Gateway CLI を使用してグローバルにセキュアブラウジングを有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

```
set vpn parameter -secureBrowse ENABLED
<!--NeedCopy-->
```

NetScaler Gateway CLI を使用してセッションごとのセキュアブラウズポリシーを有効にするには:

コマンドプロンプトで、次のコマンドを実行します:

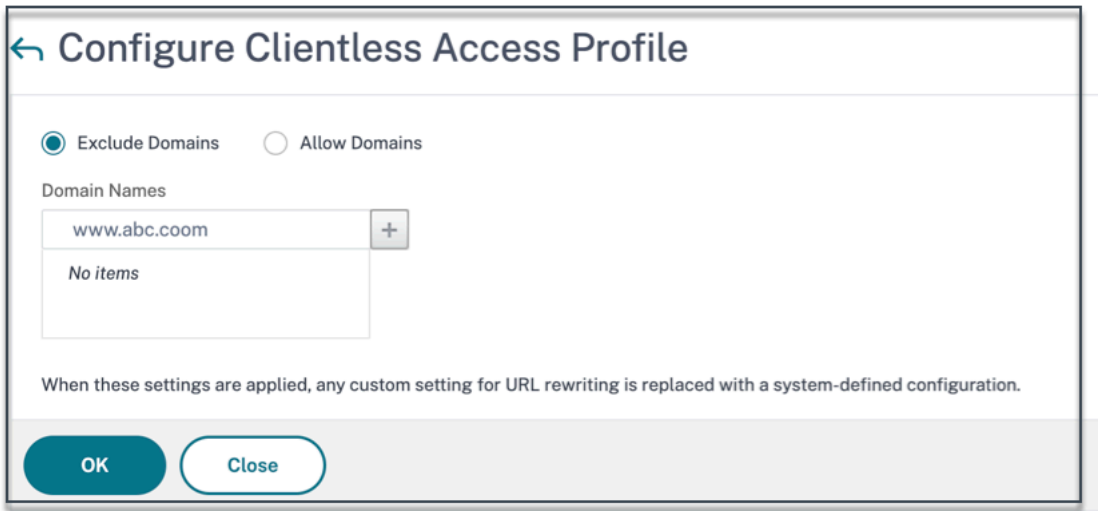
```
set vpn sessionAction <session-profile-name> -secureBrowse ENABLED
<!--NeedCopy-->
```

クライアントレスアクセスモードでのドメインの書き換えから除外する

StoreFront がクライアントレスアクセスモードで URL を書き換えないようにするには、ドメインを指定する必要があります。StoreFStoreFront サーバーの FQDN、または StoreFront ロードバランサーの FQDN、および citrix.com を除外します。この設定はグローバルにのみ適用できます。

1. [**NetScaler Gateway**] **>** [グローバル設定] に移動します。
2. [クライアントレスアクセス] で、[クライアントレスアクセス用のドメインの設定] をクリックします。
3. [ドメインを除外] を選択します。

4. [ドメイン名] に、ドメイン名 (StoreFront サーバーの FQDN、または StoreFront ロードバランサーの FQDN) を入力します。
5. **+** 記号をクリックして`citrix.com`を入力します。
6. [**OK**] をクリックします。

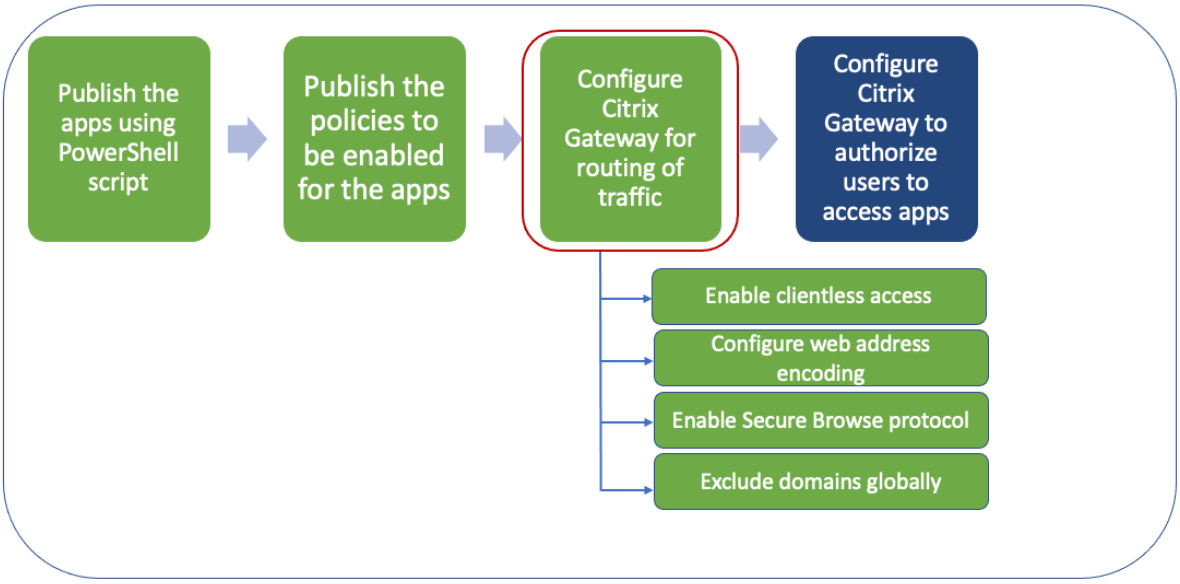


NetScaler Gateway CLI を使用してドメインを除外するには:

コマンドプロンプトで、次のコマンドを実行します:

```
bind policy patset ns_cvpn_default_bypass_domains <StoreFront-FQDN>
bind policy patset ns_cvpn_default_bypass_domains citrix.com
<!--NeedCopy-->
```

ステップ **4:** 承認ポリシーを設定する



承認は、ユーザーが NetScaler Gateway にログオンしたときにアクセスできるネットワークリソースを指定します。承認のデフォルト設定では、すべてのネットワークリソースへのアクセスを拒否します。デフォルトのグローバル設定を使用し、承認ポリシーを作成して、ユーザーがアクセスできるネットワークリソースを定義することをお勧めします。

NetScaler Gateway での承認は、承認ポリシーと式を使用して構成します。承認ポリシーを作成したら、アプライアンスで構成したユーザーまたはグループに承認ポリシーをバインドできます。ユーザーポリシーは、グループバウンドポリシーよりも優先度が高くなります。

デフォルトの承認ポリシー**:** StoreFront サーバーへのアクセスを許可し、公開されているすべての Web アプリへのアクセスを拒否するには、2 つの承認ポリシーを作成する必要があります。

- Allow_StoreFront
- Deny_ALL

Web アプリ承認ポリシー**:** 既定の承認ポリシーを作成したら、公開されている Web アプリごとに承認ポリシーを作成する必要があります。

- `Allow_<app1>`
- `Allow_<app2>`

NetScaler Gateway GUI を使用して承認ポリシーを構成するには:

1. [**Citrix Gateway] > [**ポリシー**] > [**承認] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [アクション] で、**[**許可**]** または **[**拒否**]** を選択します。
5.「エクスプレッション」で、「エクスプレッションエディタ」をクリックします。
6. 式を設定するには、「選択」をクリックして必要な要素を選択します。
7. [完了] をクリックします。
8. [作成] をクリックします。

NetScaler Gateway CLI を使用して承認ポリシーを構成するには:

コマンドプロンプトで、次のコマンドを実行します:

```
1 add authorization policy <policy-name> "HTTP.REQ.HOSTNAME.CONTAINS("<
     StoreFront-FQDN>")" ALLOW
2 <!--NeedCopy-->
```

NetScaler Gateway GUI を使用して承認ポリシーをユーザー**/**グループにバインドするには:

1. [**Citrix Gateway**] **>** [ユーザー管理] に移動します。
2. [**AAA** ユーザ] または [**AAA** グループ] をクリックします。
3. 詳細ペインでユーザー/グループを選択し、[編集] をクリックします。
4. [詳細設定] で、[承認ポリシー] をクリックします。

5.「ポリシーバインディング」ページで、ポリシーを選択するか、ポリシーを作成します。
6. [優先度] で、優先度番号を設定します。
7.「タイプ」でリクエストのタイプを選択し、「**OK**」をクリックします。

NetScaler Gateway CLI を使用して承認ポリシーをバインドするには:

コマンドプロンプトで、次のコマンドを実行します:

```
bind aaa group <group-name> -policy <policy-name> -priority <priority>
    -gotoPriorityExpression END
<!--NeedCopy-->
```

エンドツーエンド構成の例

この例では、URL（https://docs.citrix.com）が指定された「ドキュメント」という名前のアプリが Citrix Workspace に公開されます。

1. PowerShell SDK をインストール済みのマシンで PowerShell を開きます。
2. 次のコマンドを実行します。

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

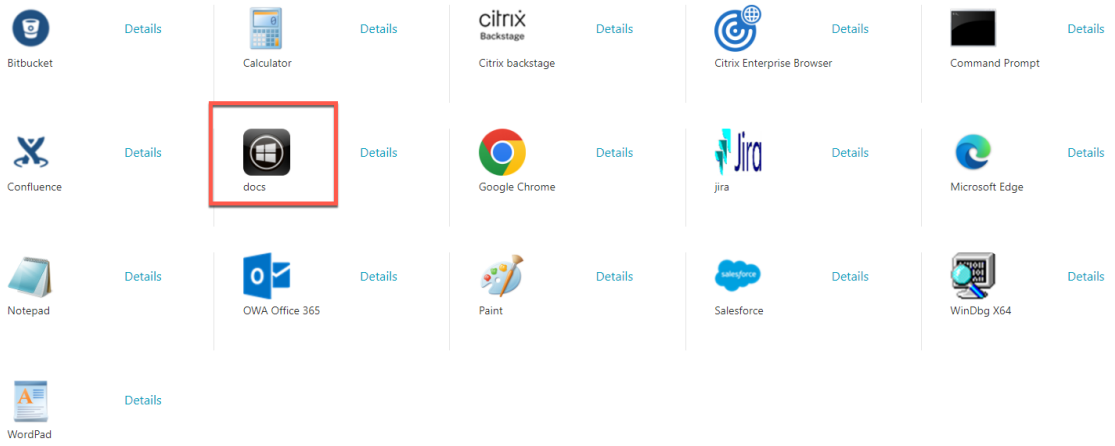
3. コマンドレットに次の詳細を追加します。

```
$citrixUrl: “https://docs.citrix.com”
$appName: docs
$DesktopGroupId: 1
$desktopgroupname: <mydesktop23>
<!--NeedCopy-->
```

4. 次のコマンドを実行します。

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup
     $dg.Uid
<!--NeedCopy-->
```

アプリは現在、Citrix Workspace で公開されています。



5. ポリシーの JSON ファイルをアプリ (「docs」) の詳細で更新します。次の事項に留意してください。

   - `proxytraffic_v1secureBrowse`値は常に以下に設定されます。この設定により、Citrix Enterprise Browser は、セキュアブラウズプロトコルを使用してトラフィックを NetScaler Gateway 経由で Web ページにトンネリングします。
   - `browser_v1embeddedBrowser`値は常に以下に設定されます。この設定は、Citrix Enterprise Browser (CEB) がワークブラウザーとして構成されている場合にのみ適用されます。`embeddedBrowser`に設定すると、構成済みの Secure Private Access ドメインに関連するリンクが CEB で開きます
   - `secureBrowseAddress` 値は NetScaler Gateway の URL です。


```
{
  "policies": [
    {
      "name": "Docs",
      "patterns": ["*.docs.netscaler.com/*"],
      "policy": {
        "watermark_v1": "enabled",
        "clipboard_v1": "disabled",
        "printing_v1": "disabled",
        "download_v1": "disabled",
        "upload_v1": "disabled",
        "keylogging_v1": "disabled",
        "screencapture_v1": "enabled",
        "proxytraffic_v1": "secureBrowse",
        "browser_v1" : "embeddedBrowser"
      }

    }],
  "system": {
    "secureBrowseAddress": "https://yournetscalergateway.com"
  }
}
```

6. ポリシー JSON ファイルを C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser. に配置します。
7. 更新したポリシーファイルを指すように Web.config ファイルを変更します。

```
<route name="webSecurePolicy" order="22" url="Resources/SecureBrowser/policy.json">
        <defaults>
          <add param="controller" value="BrowserPolicy" />
          <add param="action" value="BrowserResources" />
        </defaults>
        <data>
          <add name="endpointId" value="WebSecurePolicy" />
          <add name="endpointCapabilities" value="webSecurePolicy" />
          <add name="CommonData" factory="Citrix.DeliveryServices.Configuration.ObjectCollectionFactory, Citrix.DeliveryServices.Configuration, Version=3.23.0.0, Culture=neutral,
PublicKeyToken=e8b77d454fa2a856" path="citrix.deliveryservices/dazzleResources" property="commonData" />
        </data>
      </route>
```

8. NetScaler Gateway オンプレミスアプライアンスで、次の操作を行います。
   - アプリへのクライアントレスアクセスを有効にします。クライアントレスアクセスは、グローバルに、またはセッションレベルで有効にできます。
   - Web アドレスエンコーディングを有効にする
   - Secure Browse モードを有効にする
   - クライアントレスアクセスモードでのドメインの書き換えから除外する

詳しくは、「手順 3: オンプレミスの NetScaler Gateway を使用して認証と承認を有効にする」を参照してください。

エンドユーザーフロー

- PublishedContentApps デリバリーグループのアプリケーションにアクセスできるユーザーとして StoreFront t にログオンします。
- ログオンしたら、新しいアプリケーションがデフォルトのアイコンで表示される必要があります。アイコンは必要に応じてカスタマイズできます。詳しくは、https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/を参照してください。
- アプリをクリックすると、Citrix Enterprise Browser でアプリが開きます。

アプリケーションアクセスポリシーの詳細

次の表は、使用可能なアクセスポリシーオプションとその値を示しています。

キー名	ポリシーの説明	Value
–	–	–
screencapture_v1	Web ページのアンチスクリーンキャプチャ機能を有効または無効にする	有効または無効
keylogging_v1	Web ページのアンチキーロギングを有効または無効にする	有効または無効
watermark_v1	Web ページにウォーターマークを表示する/表示しない	有効または無効
upload_v1	Web ページのアップロードを有効または無効にする	有効または無効
printing_v1	Web ページからの印刷を有効または無効にする	有効または無効
download_v1	Web ページからのダウンロードを有効または無効にする	有効または無効
clipboard_v1	Web ページのクリップボードを有効または無効にする	有効または無効
proxytraffic_v1	Citrix Enterprise Browser がセキュアブラウズを使用してトラフィックを NetScaler Gateway 経由で Web ページにトンネリングするか、直接アクセスを可能にするかを決定します	ダイレクトブラウズまたはセキュアブラウズ
browser_v1	Citrix Enterprise Browser がワークブラウザーとして構成されている場合にのみ適用されます。embeddedBrowser に設定すると、構成済みの Secure Private Access ドメインに関連するリンクが Citrix Enterprise Browser で開きます	systemBrowser または embeddedBrowser
名前	公開された Web または SaaS アプリの名前	アプリパターンの公開時に入力したものと同じ名前を使用することをお勧めします	このアプリに関連するドメイン名をカンマで区切ったリスト。ワイルドカードも使用できます。これらのドメイン名は、Citrix Enterprise Browser がアプリにポリシーを適用するために使用されます。| 例: “*.office.com/*”，“*.office.net/*”，“*.microsoft.com/* “.sharepoint.com/*”

> 注:
>
> キーロギング対策と画面キャプチャ対策には、Citrix Workspace アプリに付属する App protection 機能をインストールする必要があります。

Secure Private Access 構成ツール-レガシーを使用してアプリとポリシーを構成する

February 20, 2024

Citrix Virtual Apps and Desktops Delivery Controller の Secure Private Access 構成ツールを使用すると、SaaS または Web アプリケーションをすばやく作成できます。さらに、このツールを使用して、アプリケーションの制限やトラフィックルーティングを設定したり、NetScaler Gateway を作成したりできます。ツールはスクリプトファイルを出力として生成し、それをそれぞれのマシンで実行して構成をデプロイできます。

サポート対象製品バージョン

製品が最小バージョン要件を満たしていることを確認してください。

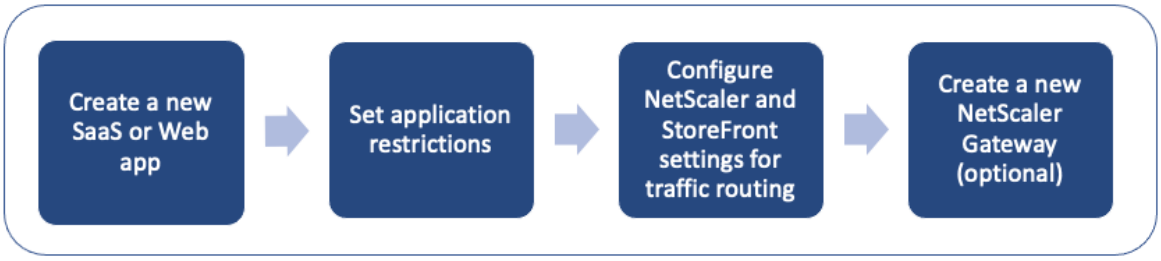
- Citrix Workspace アプリ
  - Windows—2303 以降
  - macOS —2304 およびそれ以降
- Citrix Virtual Apps and Desktops —サポートされている LTSR と現在のバージョン
- StoreFront —LTSR 2203 または非 LTSR 2212 以降
- NetScaler —12.1 以降

設定ツールを使用するための前提条件

- ダウンロードページから設定ツールをダウンロードできます。
- 構成ツールを実行するための Citrix Virtual Apps and Desktops コントローラーの管理者権限。
- Delivery Controller には少なくとも 1 つのデリバリーグループが存在します。

設定ツールを使ってみる

設定ツールを使用して次のタスクを実行できます。

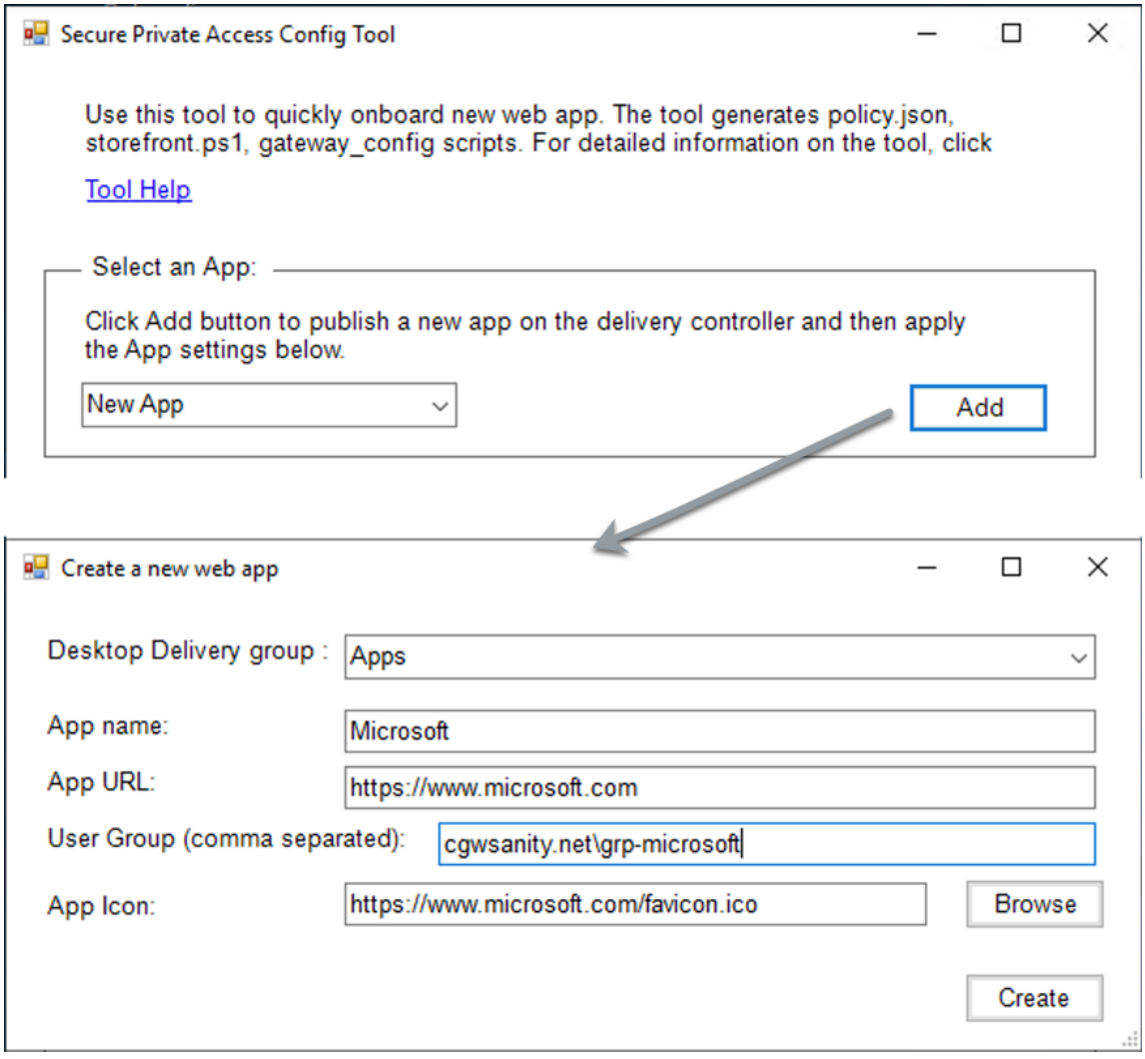


- 新しいアプリケーションを公開する

- アプリケーション制限の設定
- StoreFront と NetScaler Gateway の設定を構成する
- 新しい NetScaler Gateway の設定

新しいアプリケーションを公開する

1. 設定ツールを実行します。
2. 「アプリを選択」セクションで、ドロップダウンリストから「新規アプリ」を選択し、「追加」をクリックします。



3. アプリの設定を完了します。

   - デスクトップデリバリーグループ: このアプリにアクセスできるようにする必要があるデリバリーグループを選択します。
     既存のデリバリーグループはすべてデスクトップデリバリーグループに列挙されます。
   - アプリ名: アプリ名を入力します。

- アプリの **URL**: アプリの URL を指定します。
- ユーザーグループ: ドメイン名とグループ名の両方を「Domain\ Group」の形式で入力します。ユーザーグループにはスペースを含めることができます。たとえば、「cgwsanity.net\ grp-Microsoft」、「cgwsanity.net\ grp Microsoft」などです。
  これらのグループはすでに Active Directory に存在している必要があります。

  > **Note:**
  >
  > - Built-in domain security groups such as “Domain Users” or “Domain Admins” are not supported. Only the manually created user groups must be used.
  > - The user group is only used in NetScaler Gateway authorization policies and not for app assignments in Citrix Virtual Apps and Desktops. Hence, the user group that you enter here is not visible in Studio.

- アプリアイコン:URL が検出された場合、ツールはその URL の favicon.ico を使用します。管理者は必要に応じてアイコンをカスタマイズすることもできます。管理者がアイコンを提供しない場合、デフォルトのアイコンがアプリに割り当てられます。

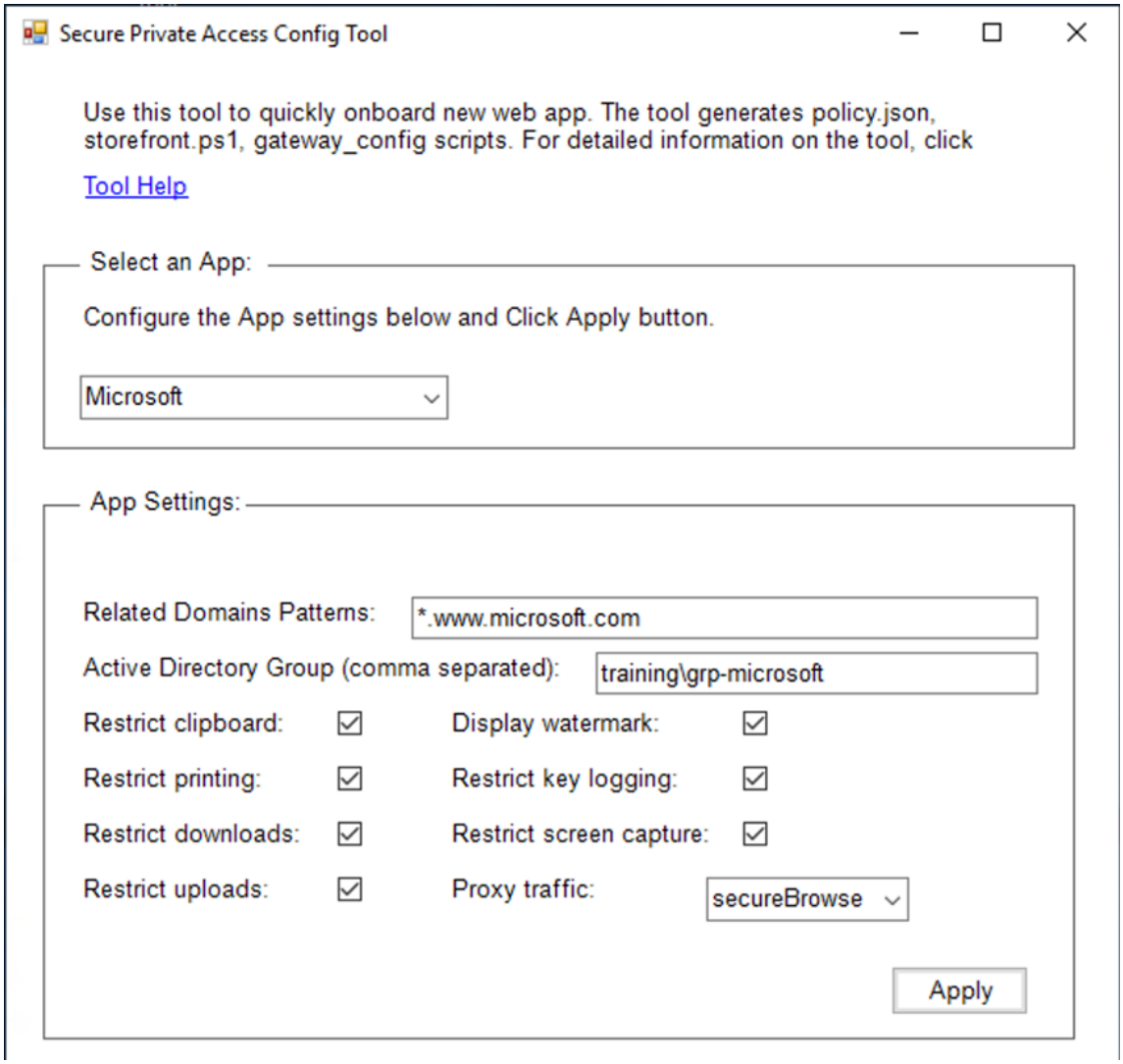
4. ［作成］をクリックします。

アプリケーションは Delivery Controller で公開され、StoreFront のユーザーグループのユーザーが利用できます。

アプリケーション制限の設定

新しいアプリケーションを公開したら、そのアプリの制限を有効または無効にできます。

1. 「アプリを選択」セクションで、設定を適用するアプリをドロップダウンリストから選択します。



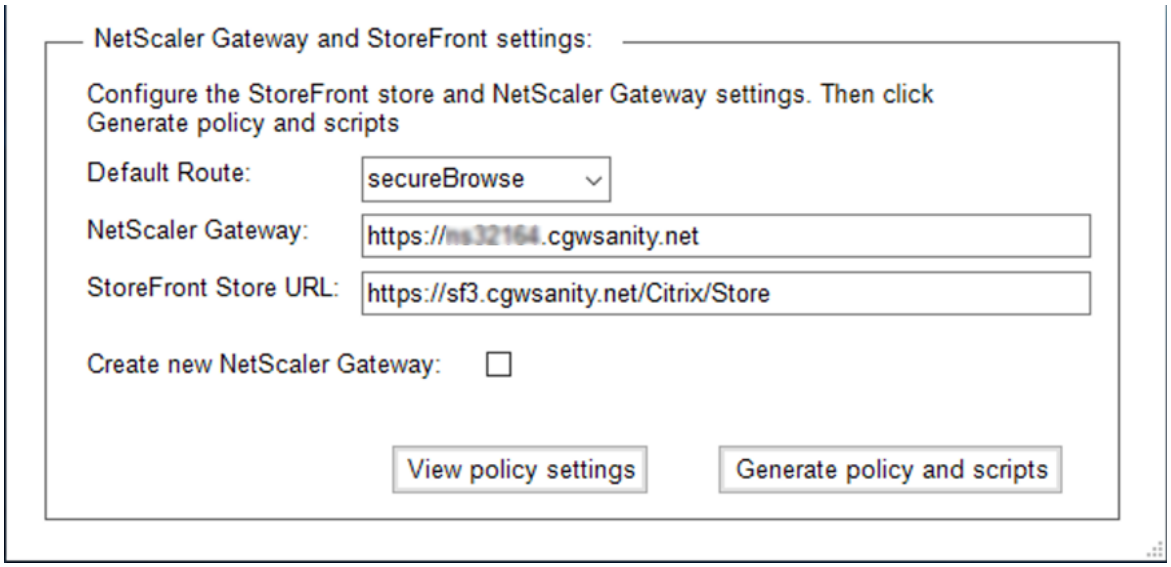
2. アプリ設定セクションでアプリ設定を行います。

   - 関連ドメインパターン: 関連ドメイン URL は、アプリ URL に基づいて自動入力されます。管理者はドメインをカンマで区切って追加できます。
   - **Active Directory** グループ: このアプリケーションにアクセスできる必要があるグループを入力します。これは必須のフィールドです。
     複数のグループをカンマで区切って入力できます。これらのグループは、Active Directory で使用可能なグループと一致する必要があります。ここに入力したグループ名の検証は行われません。そのため、グループ名を Active Directory にあるものと一致するように注意して入力することが重要です。
   - アプリ設定: デフォルトでは、すべてのアプリ設定が制限 (選択) されています。ユーザーグループに必要な適切な設定を選択または選択解除できます。
   - プロキシトラフィック:「セキュアブラウズ」を選択します。この設定により、Citrix Enterprise Browser は NetScaler Gateway 経由でトラフィックをウェブページにトンネリングできるようになります。

3. ［適用］をクリックします。

StoreFront と **NetScaler Gateway** の設定を構成する

NetScaler Gateway を介してトラフィックをルーティングするための設定を構成できます。既存の NetScaler Gateway を構成することも、ゲートウェイと **StoreFront** の設定セクションで新しい NetScaler Gateway を作成することもできます。



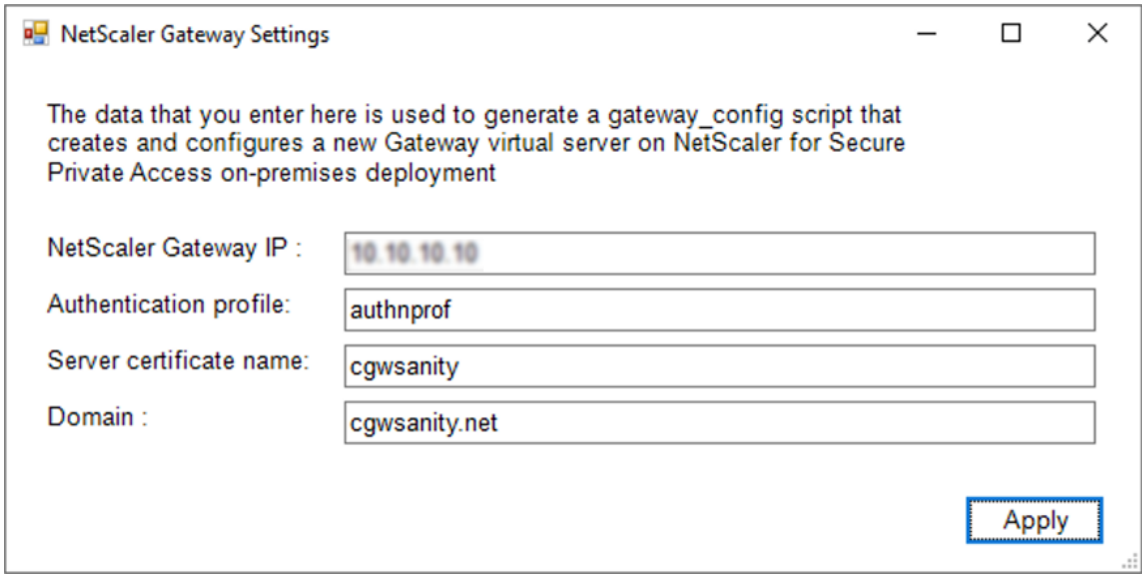
- デフォルトルート: アプリのポリシーが定義されていない場合、デフォルトルートがアプリに適用されます。
  - **SecureBrowse**: Citrix のエンタープライズブラウザは、NetScaler Gateway を介してトラフィックをウェブページにトンネリングします。
  - ダイレクト:Citrix Enterprise Browser を使用すると、アプリに直接アクセスできます。
- **NetScaler Gateway**: NetScaler ゲートウェイ URL を入力します。
- **StoreFront** ストア **URL**: StoreFront ストアの URL をすべて入力します。例: `http://<directory path>/Citrix/<StoreName>`。URL は StoreFront コンソールから取得できます。
- （オプション）新しいゲートウェイの作成: チェックボックスを選択して新しい NetScaler Gateway を作成し、「作成」をクリックします。

新しい **NetScaler Gateway** の作成（オプション）

既存のゲートウェイ設定を変更したくない場合は、新しい NetScaler Gateway を作成できます。

NetScaler Gateway を既にお持ちの場合は、構成ツールを使用してアプリの認証ポリシーとバインディングを構成できます。

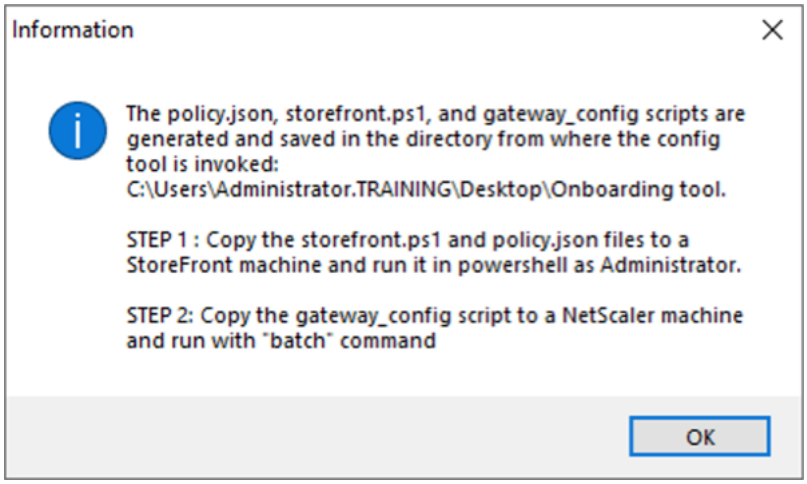
1. 新しい NetScaler Gateway には、次の詳細を入力する必要があります。新しいゲートウェイを作成するときに入力した値については、ツールによる検証は行われません。そのため、正確な値を入力するように注意することが重要です。



   - ゲートウェイ **IP**: NetScaler Gateway の IP アドレス。
   - 認証プロファイル:NetScaler ですでに設定されている認証プロファイル名を入力します。詳細については、認証プロファイルを参照してください。
   - サーバー証明書名:NetScaler ですでに設定されている SSL 証明書名を入力します。詳細については、「SSL 証明書」を参照してください。
   - ドメイン: 内部ネットワークのアプリへの SSO に使用されます。詳細については、「VPN セッションアクション」を参照してください。

2. ［適用］をクリックします。
3. 「ポリシーとスクリプトを生成」をクリックします。

   policy.json、storefront.ps1、および gateway_config ファイルは、設定ツールを実行した場所に生成および保存されます。



サポートされているアプリケーションで gateway_config ファイルを開くと、出力ファイルに 2 つのセクションが表示されます。

- NetScaler Gateway の構成に関連するセクション（新しいゲートウェイが作成された場合にのみ適用）
- 承認ポリシー、ユーザーグループ、およびユーザーグループへのバインディングポリシーに関連するセクション。

次の画像は、新しい NetScaler Gateway 構成の gateway_config ファイルを示しています。


```
#############################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)
#2. Run batch command (e.g. batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_output)
#3. Analyze output (e.g. cat /var/tmp/gateway_config_output)
#############################################################################################################

# Enable NS features
enable ns feature SSL SSLVPN AAA

# Add Gateway
add vpn vserver _XD_SPAGateway_443 SSL [redacted] -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile
-deploymentType ICA_STOREFRONT -vserverFqdn gwalextest.spaopdev.local -authnProfile spaopdev_auth_prof -icaOnly OFF

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains corealextest.spaopdev.local
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

add vpn sessionAction AC_WB_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_OS_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_SPAGateway
add vpn sessionPolicy PL_WB_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" AC_WB_SPAGateway

# Bind policies to vserver
bind vpn vserver _XD_SPAGateway_443 -policy PL_OS_SPAGateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _XD_SPAGateway_443 -policy PL_WB_SPAGateway -priority 110 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to GW
bind ssl vserver _XD_SPAGateway_443 -certkeyName spaopdev

# Add default authorization policies
add authorization policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add authorization policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

次の画像は、更新された NetScaler Gateway 構成の gateway_config ファイルを示しています。


```
#############################################################################################################
#1. Upload file to NetScaler (e.g. to /tmp)
#2. Run batch command (e.g. batch -fileName /tmp/Gateway_config -outfile /tmp/Gateway_config_output)
#3. Analyze output (e.g. cat /tmp/Gateway_config_output)
#############################################################################################################

# Add default authorization policies
add  policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add  policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

新しい **NetScaler Gateway** で **StoreFront** を構成する

- ツールで StoreFront と NetScaler Gateway の設定を行うには、次のものが必要です。
  - NetScaler Gateway の FQDN
  - StoreFront ストア URL
- StoreFront の構成要件:
  - NetScaler Gateway: リモートアクセスが有効になっています。
  - NetScaler Gateway からのパススルー認証が有効になっています。
  - Active Directory: ユーザーまたはグループを追加または更新したり、NetScaler の認証プロファイルやポリシーを設定したりするための管理者アクセス権。

詳しくは、「NetScaler Gateway と StoreFront の統合」を参照してください。

設定ツールの出力ファイルを使用して、アプリとポリシーの設定をデプロイします

設定ツールは次のファイルを生成します。これらのファイルは、ツールがアップロードされて実行される場所/ディレクトリに保存されます。

- policy.json
- storefront.ps1
- gateway_config

1. StoreFront の.ps1 ファイルをストアフロントにコピーします。
2. PowerShell で storefront.ps1 スクリプトを管理者として実行します。

   このスクリプトは、ストア下のパスに Resources\ SecureBrowser フォルダーがまだ使用できない場合、そのフォルダーを作成します。

   このスクリプトは、policy.json ファイルのルートの web.config ファイルも更新します。
3. policy.json ファイルを、ストアフロント.ps1 がストアの下に作成する Resources\ SecureBrowser フォルダーにコピーします。
4. gateway_config を NetScaler にコピーし、NetScaler CLI で次のバッチコマンドを使用してスクリプトを実行します。

   ```
   batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_o
   ```

> 注:
>
> - ツールで設定を変更した場合は、スクリプトとポリシーを再生成する必要があります。policy.json ファイルを StoreFront マシン上の Resources\ SecureBrowser フォルダーに再度コピーする必要があります。また、gateway_config スクリプトを NetScaler で再度実行する必要があります。
> - ストア名/URL が変更されていない場合は、storefront.ps1 を再度実行する必要はありません。

その他の参考資料

詳細については、次のドキュメントを参照してください。

- オンプレミス向けの Secure Private Access
- 導入ガイド: オンプレミスでの Secure Private Access