



Citrix Secure Private Access™ ハイブリッド展開

Contents

ソリューションの概要	13
Secure Private Accessを使用する理由	13
主要コンポーネント	14
ネットワーク図	14
エンドユーザーのアクセス方法	16
Citrix Endpoint Analysis (EPA) クライアント	17
制限事項	17
新機能	18
31 July 2026	18
27 April 2026	18
07 April 2026	19
2025年11月	19
2025年9月	21
2025年8月	21
2025年5月	22
2025年4月	22
2024年12月	23
2024年10月	23
初回リリース	24
既知の問題	30
システム要件と前提条件	32
ソフトウェアバージョンの要件	32
ファイアウォールの要件	32
前提条件	35
NetScaler の前提条件	35
クローム エンタープライズ プレミアム + シトリックス セキュア アクセス の展開	35

Citrix Secure Access のみの展開	36
Cloud Connector の前提条件	37
StoreFront の前提条件	37
Secure Private Access の前提条件	37
Google の前提条件	38
Chrome Enterprise Premium ライセンス	38
Google Workspace 管理コンソール	38
Google Chrome	39
管理対象Chromeプロファイル	39
Citrix Workspaceで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと同期する	39
TLS インспекションのバイパス	40
Secure Private Access ハイブリッド展開の開始	42
開始する前に	42
Secure Private Access の資格を確認する	42
前提条件を確認する	43
展開モードを選択する	43
次のステップ	43
ステップ 1: Google Chrome Enterprise Premium をセットアップする	43
グーグル クローム エンタープライズ プレミアム の設定手順	44
ステップ2: 最初のデータセンターをセットアップする	46
ステップ 3: 構成と分析	47
NetScaler および StoreFront スクリプトのダウンロードと実行	47
NetScaler スクリプト	47
StoreFrontスクリプト	49
レポートをアップロードして構成を分析する	50
オンボーディングを完了し、アプリケーションを公開する	52
オンボーディング後のタスク	52

アプリケーションの構成	52
アクセス ポリシーの構成	52
Chrome Enterprise Premium構成の更新	53
構成を同期する	54
アプリケーションへのアクセス（エンドユーザー）	54
WebおよびSaaSアプリケーションへのアクセス	55
TCP/UDP（クライアント/サーバー）アプリケーションへのアクセス	56
データ地域化	57
サポートされる展開	57
構成	58
制限事項	58
コンポーネントのセットアップ	59
Cloud Connector の構成	59
セキュアプライベートアクセス サービス	59
Citrix Secure Private Access サービスのポート構成	59
Secure Private Access ロードバランサー	60
クラウドコネクタ上のセキュアプライベートアクセスサービス用のTLS/SSL証明書を構成する	60
NetScaler	63
認証の構成	63
認証構成の例	64
条件付き認証による多要素認証	64
多要素認証によるサードパーティ統合	64
デバイスポスチャスキャン (EPA)	65
その他のシナリオ	65
StoreFront	65
新しいStoreの構成	65
コンポーネントアナライザー	67

Secure Private Accessアナライザー	68
NetScaler Gatewayアナライザー	69
StoreFrontアナライザー	69
グーグル クローム エンタープライズ プレミアム との統合	71
Chrome Enterprise Premium の高度なセキュリティ機能	72
統合を成功させるための前提条件	72
Citrix Secure Private Access - サポートされている展開モード	73
法的情報	73
管理者の役割と権限	73
Googleカスタム管理者ロールの権限	74
ロールと権限の作成と割り当て	76
NetScaler Gateway を IdP として使用するための Open ID Connect プロファイル	76
Google OIDC SSO プロファイルの作成	77
OIDCプロファイルのバインド（OUまたはグループのいずれかに）	78
NetScalerをOAuth IdPとして構成する	79
ディレクトリ同期	79
G Suiteコネクタを使用したMicrosoft Entra ID	80
グーグル クラウド ディレクトリ シンク (GCDS) ツール	80
アクティブディレクトリ	81
グーグル クラウド ディレクトリ シンク の構成	81
エンドユーザーエクスペリエンス	89
Chrome エンタープライズ プレミアム 用 シトリックス セキュア アクセス 拡張機能	91
Secure Access 拡張機能ログ	92
Chrome Enterprise 用 Citrix Secure Access コントロール	92
サポートされているコントロール	93
ポリシー内のユーザーとグループ	94
ユーザーまたはグループの検索	94
同期されたユーザーとグループを使用する	94

キーロギング対策制御	95
前提条件	95
キーロギング対策ポリシーを構成する	95
クリップボードコンテナ制御	96
前提条件	96
クリップボードコンテナ制御を有効にする	97
クリップボード共有スコープを有効にする	98
Webアプリケーションのドメインサフィックス	100
前提条件	101
DNSサフィックスの構成	101
セッション記録制御	101
アーキテクチャ	102
前提条件	102
システム要件	102
環境をセットアップする	103
ブラウザセッションの再認証制御	104
前提条件	104
ブラウザセッションの再認証制御を有効にする	105
SSH制御	106
この統合の利点	107
ユースケース	107
システム要件	107
前提条件	108
SSHアクセス用にSecure Private Accessを構成する	108
SSHポリシーを構成する	108
リモートデスクトップ制御	109
この統合の利点	110
ユースケース	110

システム要件	110
前提条件	111
RDP アクセス用に Secure Private Access を構成する	111
リモートデスクトップポリシーを構成する	111
CEP統合の問題のトラブルシューティング	112
CEPトラブルシューティング用の診断ログ	113
ユーザーが正しいChromeプロファイルにログインしていることを確認します	114
Secure Enterprise Browser拡張機能がインストールされているか確認する	115
ExtensionInstallForcelistポリシーを確認する	115
競合する拡張機能インストールリストポリシーのトラブルシューティング	115
Secure Enterprise Browser拡張機能ポリシーの確認	116
Google 管理コンソール内でユーザー拡張機能の設定を確認する	117
ルートがフェッチされているか確認する	118
Secure Private Access管理コンソールでCEP統合を検証する	119
Google Secure Gatewayの到達可能性のトラブルシューティング	120
ルートへのアプリケーションの組み込みを確認する	120
ルーティングされたアプリケーションアクセスのトラブルシューティング	121
IdPとGoogleディレクトリの整合性を確保する	122
Google 管理コンソールでグループのアクセス設定を確認する	122
CEP統合に関する既知の問題	122
Secure Private Accessユーザーインターフェイス	123
適応型アクセス ポリシーの構成	123
Google Chromeブラウザ	123
アプリの構成と管理	125
エンタープライズWebアプリケーションまたはSaaSアプリケーションを構成する	125
アプリケーション削除時のルーティングエントリの自動クリーンアップ	128
次のステップ	128
HARファイルを使用して関連ドメインを検出する	129

例	129
前提条件	130
HARファイルのインポート	130
関連ドメインの管理	130
検証とファイルの要件	131
TCP/UDPアプリを構成する	131
次のステップ	135
TCP/UDP の構成 - サーバーからクライアントアプリへ	135
アプリケーションを編集する	137
次のステップ	137
アクセス ポリシーの構成と管理	138
アプリケーションのアクセスポリシーを構成する	138
アクセスポリシーを構成する	139
アクセスポリシーを編集する	140
アクセスポリシーの優先度を変更する	140
次のステップ	141
ポリシー条件	141
ユーザーとユーザーグループ	141
ユーザーとグループの同期を確認する	142
ネットワークロケーション	143
セッションポリシーを構成する	145
デバイス証明書の登録	146
デバイスポスチャサービス	148
NetScaler Gateway でデバイスポスチャチェックを構成する	148
オンプレミスNetScaler® Gatewayでのデバイスポスチャチェック	148
エンタイトルメント	149
Secure Private Accessハイブリッドソリューション向けにDevice Postureを有効にする	149
設定の管理	150

設定を管理する	150
アプリケーションドメイン	150
構成レポート	151
構成レポートを生成する	151
インストール後のセットアップ構成を管理する	155
Secure Private Access 構成をリセットする	156
アップグレード	156
高度なSecure Private Access機能	158
高度なデータセンター構成	159
前提条件	159
GSLB 構成 CLI コマンド	160
参照	160
データセンターのセットアップと構成	162
グローバルサーバー負荷分散接続プロキシ	162
前提条件	163
GSLB 接続プロキシの構成	163
グローバルサーバーロードバランサードメインURLを構成する	164
構成	164
データセンターの編集 (オプション)	165
構成と分析	165
コンテキストベースのアプリケーションルーティング	166
ユースケース: コンテキストベースのルーティング	166
ルーティングの種類を変更する手順	167
ユースケース: 社内ユーザーをバックエンドアプリケーションに直接ルーティングする	168
ルーティングの優先順位	168
サポートされているCitrix Secure Access™クライアント	168
使用例	168
セッションポリシーを使用して病院ネットワーク内で直接ルーティングを構成する	169

エンドユーザーがアクセスするドメインまたはIPアドレスを検出する	170
新しい環境における内部ドメインのアプリケーション検出	171
アプリ検出ページからアプリケーションを作成する	174
既存のアプリケーションを更新する	174
ポリシーモデリングツール	175
データ損失防止 (DLP) ポリシーを構成する	176
高可用性展開	176
データセンター内の高可用性	177
NetScaler	177
クラウドコネクタ (Secure Private Access サーバー)	177
StoreFrontサーバー	179
Secure Private Access 構成をリセットする	179
可視性と監視	180
サービスエンタイトルメント	180
サポートされるクライアント	180
Monitor へのアクセス方法	180
セッションの定義	180
Web/SaaSアプリセッション	181
TCP/UDPアプリセッション	182
ユーザーセッションの表示	182
アプリケーションのトポロジ	184
トリアージとトラブルシューティング	187
シトリックス セキュア アクセス モードにおけるユーザー/クライアントの問題	187
ユーザーがログインできない	187
ユーザーがアプリを起動できない	188
デバッグレベルのログを含むNetScalerサポートバンドルを収集する手順	189
詳細ログを元に戻す	190
トラブルシューティングに役立つツール	190

クライアントログを収集する	190
クローム エンタープライズ プレミアム ログ	191
Secure Enterprise Browser 拡張機能のログをキャプチャする手順	191
Citrix Secure Access Extension のログをキャプチャする手順	191
Monitorを使用したリアルタイムセッションのトラブルシューティング	192
セッションコード	193
アプリ列挙メッセージコード	193
アプリ起動メッセージコード	195
アプリケーション起動エラーコード	195
エンドユーザーエクスペリエンス	199
Chrome Enterprise Premium を使用した Web および SaaS アプリケーションへのアクセス	199
オプション 1: 管理対象の Chrome プロファイルを作成し、アプリに直接アクセスする (推奨)	199
オプション2: 既存の管理対象ChromeプロファイルでストアURLにアクセスする	200
オプション3: 管理対象外のChromeプロファイルまたはChrome以外のブラウザ (Edge、Firefox) からストアURLにアクセスする	200
オプション 4: Citrix Workspace アプリを介してアプリにアクセスする	201
クライアント/サーバー (TCP/UDP) アプリケーションへのアクセス	202
index	204
DaaSモニターとの統合	204
サービスエンタイトルメント	204
サポートされているクライアント	204
Monitorへのアクセス方法	204
セッションの定義	204
Web/SaaSアプリセッション	205
TCP/UDPアプリセッション	206
ユーザーセッションの表示	206
アプリケーションのトポロジ	207

コンテキストタグ	208
GUIを使用してカスタムタグを構成する	208
クラシックゲートウェイの事前認証ポリシーを構成する	208
カスタムタグをNetScaler Gatewayにバインドする	209
CLIを使用してカスタムタグを構成する	210
新しいコンテキストタグの追加	210
Secure Private Accessプロバイダーに送信されるEPAタグに関する注意	210

ソリューションの概要

ハイブリッド展開向けのCitrix Secure Private Access™は、オンプレミス環境とCitrix Cloudの間で機能を分割するゼロトラストネットワークアクセス (ZTNA) ソリューションを提供します。このアーキテクチャにより、既存の投資を活用しながら、クラウドベースの管理を実現できます。責任は次のように分担されます。

- **オンプレミスコンポーネント (データプレーン):** 既存のNetScaler Gateway、StoreFront、およびWindows Cloud Connectorのインストールはオンプレミスに残ります。これらのコンポーネントは、すべてのユーザーアクセスを制御し、ルーティングする役割を担います。
- **Citrix Cloudコンポーネント (コントロールプレーン):**
 - 一元管理: すべての構成、管理、およびポリシー管理にはCitrix Cloud UIを使用します。
 - 監視とトラブルシューティング: すべての監視、分析、およびトラブルシューティング機能には、ホストされているCitrix Monitorサービスを利用します。

Secure Private Accessを使用する理由

Citrix Secure Private Accessソリューションは、シングルサインオン (SSO)、リモートアクセス、および帯域外コンテンツ検査を統合プラットフォームに統合することで、エンドツーエンドのアクセス制御を提供します。

- **アプリへのアクセスを管理:** 承認されたすべてのSaaSおよび社内アプリケーションに対して、セキュリティポリシーを適用し、簡素化されたSSOエクスペリエンスを提供します。
- **セキュリティの強化:** 特定のWebサイトやWebサイトカテゴリへのアクセスをフィルタリングすることで、マルウェアやデータ漏洩からネットワークとユーザーデバイスを保護します。
- **Google Chrome Enterprise Premiumとの統合:** Google Chrome Enterprise Premiumを活用し、ユーザーが慣れ親しんだ安全なエクスペリエンスで、承認された企業Webアプリにネイティブにアクセスできるようにします。詳細については、「[Google Chrome Enterprise Premiumとの統合](#)」を参照してください。
- **データ損失防止 (DLP):** 印刷、ダウンロード、クリップボードのコピー/貼り付け操作を制限するためのきめ細かな制御を適用します。

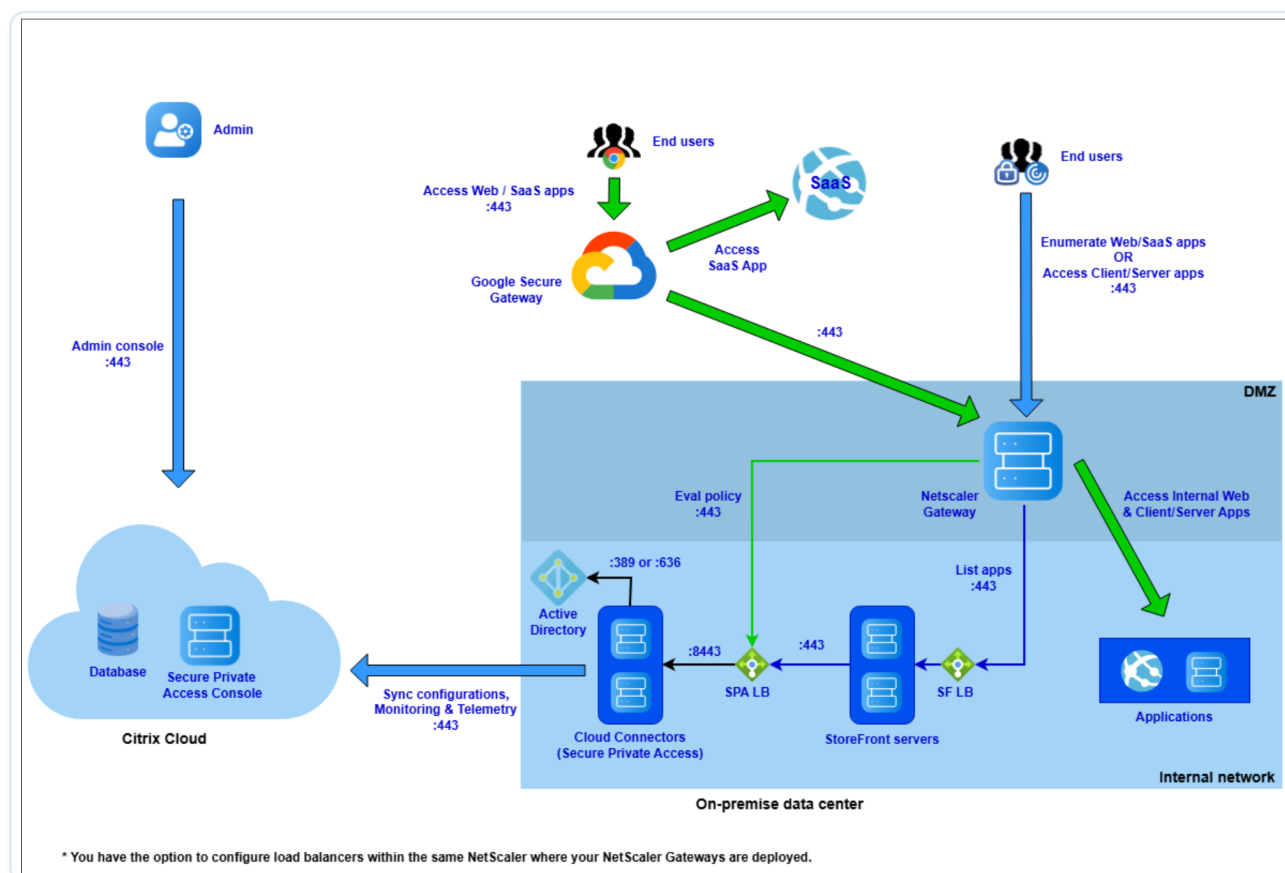
- **ユーザーアクティビティの分析と企業ネットワークの保護:** 悪意のあるWebサイトへのアクセスや危険なファイル転送など、ユーザーアクティビティを詳細に可視化します。これらの分析を使用して、是正措置を講じ、企業ネットワークを保護します。
- **シームレスなユーザーエクスペリエンス:** あらゆるデバイス、場所、またはネットワークから、重要なビジネスアプリケーションへの安全でシームレスなアクセスを提供します。

主要コンポーネント

以下のセクションでは、Secure Private Accessハイブリッドソリューションの主要コンポーネントに関する詳細情報を提供します。

ネットワーク図

次の図は、Secure Private Accessハイブリッドソリューションのネットワーク図を示しています。



Secure Private Accessハイブリッドソリューションの主要コンポーネントは次のとおりです。

- **Secure Private Access管理コンソール:** Citrix CloudのSecure Private Accessタイルをクリックして、管理コンソールにアクセスします。管理コンソールを使用して、オンボーディング、アプリの構成、ポリシーの設定を行います。サイト管理は一元化され、効率化されています。オンプレミスインフラストラクチャは不要です。

- **Google ChromeおよびChrome Enterprise Premium Secure Gateway:** エンドユーザーは、Google Chromeブラウザを使用して企業の内部アプリケーションおよびSaaSアプリケーションにアクセスします。

Chrome Enterprise Premium Secure Gatewayは、ゼロトラストアクセスフレームワークを適用するためのフォワードプロキシとして機能します。これにより、アプリケーションアクセスに対するきめ細かくコンテキストを認識した制御が提供されます。ユーザーのChromeブラウザからのすべてのトラフィックは、Chrome Enterprise Premium Secure Gatewayを介してNetScaler Gatewayに接続され、アクセスが許可される前にポリシーが適用されることを保証します。

注:

Googleコンポーネントは、Secure Private Accessを使用してSaaSおよび内部Webアプリケーションへのセキュアなアクセスを提供する場合にのみ必要です。Secure Private AccessをTCP/UDP（クライアント/サーバー）アプリケーションにのみ使用する予定の場合は、これらは必要ありません。

- **NetScaler Gateway:** NetScaler Gatewayコンポーネントは、アプリケーションおよびデスクトップへのセキュアなリモートアクセスを提供します。外部ユーザーのセキュアなエントリポイントとして機能し、ネットワーク外から企業リソースに接続できるようにします。詳細については、[NetScaler](#)を参照してください。
- **Cloud Connector:** Cloud Connectorは、Windowsサーバーにインストールされるオンプレミスコンポーネントであり、お客様のネットワークとCitrix Cloud間のセキュアな通信ブリッジとして機能します。

Cloud Connectorは、クラウド内のSecure Private Accessサービスからすべての構成とポリシーを同期する役割を担います。これらのポリシーは、アプリケーションのアクセスルールを適用するために使用されます。コネクタはまた、このデータを永続的にキャッシュするため、Citrix Cloudが利用できなくなった場合でも、ユーザーは引き続きアプリケーションにアクセスできます。詳細については、[Cloud Connector](#)を参照してください。

- **StoreFront:** オンプレミスのStoreFrontは、すべての承認済みアプリケーションとデスクトップを集約、列挙し、エンドユーザーに配信するユーザー向けコンポーネントです。エンタープライズアプリストアとして機能します。このハイブリッドアーキテクチャにより、既存のStoreFront設定をクラウドに移行することなく活用できます。詳細については、[StoreFront](#)を参照してください。

注:

TCP/UDP (クライアント/サーバー) アプリケーションにのみSecure Private Accessを使用する予定の場合、StoreFrontはオプションです。StoreFrontを構成した場合、Webアプリケーションタイプとして構成されているアプリケーションのみが列挙されます。標準のTCP/UDPアプリはストアに表示されません。

エンドユーザーのアクセス方法

エンドユーザーは、以下のいずれかの方法でSecure Private Accessアプリにアクセスできます。

- **Citrix Workspaceアプリ (CWA) とWorkspace UI:** これらは、エンドユーザーがCitrix Storeに接続して表示するために使用できる2つのクライアントです。
 - **Citrix Workspaceアプリ (ネイティブクライアント) :** これは、ユーザーのエンドポイント (WindowsやmacOSなど) にインストールされる完全なネイティブアプリケーションです。最もリッチなユーザーエクスペリエンスを提供し、特定の高度な機能には必須です。
 - **Citrix Workspace UI (Webクライアント) :** これは、ストアのブラウザベースバージョンです。ユーザーはWebブラウザでStoreFrontのURLにアクセスして使用します。これにより、ユーザーはクライアントソフトウェアをインストールすることなくアプリケーションにアクセスできます。
- **Google Chrome :** すべてのWebおよびSaaSアプリケーションは、管理されたエンタープライズプロファイルを使用して、Google Chromeブラウザを介してのみ起動されます。ユーザーがCitrix Storeからアプリケーションを起動すると、すべてのセキュリティ制御を適用するために、この管理されたChrome Enterpriseプロファイルで自動的に開きます。

注:

TCP/UDP (クライアント/サーバー) アプリケーションにのみSecure Private Accessを使用する予定の場合、Google Chromeは必須ではありません。ユーザーは、TCP/UDPアプリケーションにアクセスするために、任意のブラウザ (管理されていないChrome、Edge、Firefoxなど) を使用できます。

- **Citrix Secure Access (CSA) クライアント:** これは、すべてのTCP/UDP (クライアント/サーバー) アプリケーションへのZTNAアクセスに必要な、ユーザーのエンドポイントにインストールされるクライアント側エージェントです。

CSAは、従来のフルトンネルVPNを必要とせずに、社内リソースへのセキュアなアプリケーションごとの接続を提供します。

Citrix Endpoint Analysis (EPA) クライアント

Citrix EPAクライアントは、デバイスのポスチャスキャン（EPAスキャンとも呼ばれる）を実行するためにユーザーのエンドポイントで実行される軽量プラグインです。このクライアントは、アクセスを許可する前にエンドポイントのセキュリティポスチャ（最新のOS、特定のウイルス対策ソフトウェア、レジストリキーなど）をチェックするアクセスポリシーを構成している場合にのみ必要です。

制限事項

- 要素としてのEPAはサポートされていません。代わりに、デバイスポスチャサービスを使用できます。デバイスポスチャサービスの詳細については、「[Device Posture](#)」を参照してください。
- 仮想サーバーレベルでのデバイスポスチャチェックの有効化は、Always Onではサポートされていません。
- ポリシーモデリングはユーザー条件のみをサポートします。デバイスポスチャとネットワークロケーションの条件はサポートされていません。
- StoreFrontアナライザーは、StoreFrontでSecure Private Accessタイプのストアを1つのみサポートします。
- ハイブリッド展開用の簡素化されたSecure Private Accessユーザーインターフェイスは、現在のリリースではデータセンターを1つのみ（ゲートウェイ1つとStoreFront1つ）サポートします。
- Citrix Secure Accessクライアントでは、ネットワークロケーションでIPv6はサポートされていません。

新機能

以下のセクションでは、新機能と機能強化の詳細を説明します。

31 July 2026

- **Chrome Enterprise向けCitrix Secure Accessコントロール:**

Citrix Secure Private Accessは、Google Chrome Enterprise Premium (CEP) 用のCitrix Secure Access拡張機能によって配信および適用されるセキュリティポリシーをサポートします。

Secure Private Accessでは、以下のポリシーがサポートされています。

- [アンチキーロギング](#)
- [クリップボードコンテナ](#)
- [Webアプリケーションのドメインサフィックス](#)
- [セッション記録](#)
- [ブラウザセッションの再認証](#)

27 April 2026

- **高度なデータセンター構成**

Secure Private Accessハイブリッド展開は、GSLB接続プロキシのサイト永続性メソッドを使用したアクティブ-アクティブサイト展開でNetScaler GSLBを使用する、マルチサイト構成のマルチデータセンターでサポートされるようになりました。詳細については、「[高度なデータセンター構成](#)」を参照してください。

- **グローバルサーバーロードバランサーのドメインURLを構成するためのサポート**

Secure Private Access のマルチサイト冗長性を設定するには、グローバルサーバーロードバランサー (GSLB) アドレスを構成する必要があります。このアドレスは単一のエントリポイントとして機能し、静的近接性などのトラフィックポリシーに基づいて、ユーザーを特定のデータセンターの Secure Private Access ゲートウェイにルーティングします。詳細については、「[グローバルサーバーロードバランサーのドメイン URL を構成する](#)」を参照してください。

- **グローバルサーバーロードバランシング接続プロキシのサポート**

グローバルサーバーロードバランシング (GSLB) 接続により、NetScaler Gateway は誤ってルーティングされたリクエストを透過的に検出し、ユーザーの介入なしに正しいサイトにプロキシできます。詳細については、「[グローバルサーバーロードバランシング接続プロキシ](#)」を参照してください。

07 April 2026

- **コンテキストベースのアプリケーションルーティング**

アプリが構成されると、アプリ構成の下で、アプリケーション URL および関連ドメインまたはアプリの宛先に対してルーティングタイプが定義されます。ここで定義されたルーティングタイプは、アプリにアクセスできるすべてのユーザーに適用されます。ただし、管理者がユーザーコンテキストに基づいて同じアプリを異なる方法でルーティングしたいシナリオもあります。たとえば、ユーザーが社内ネットワーク内にいる場合、内部アプリの URL または宛先は Secure Private Access 経由ではなく直接ルーティングする必要があります。アクセスポリシーのルーティング例外構成により、管理者はポリシーで定義された条件に一致するユーザーまたはマシンのルーティングタイプを編集できます。詳細については、「[コンテキストベースのアプリケーションルーティング](#)」を参照してください。

- **ブラウザ内での SSH および RDP アプリケーションへのセキュアなアクセス**

Citrix Secure Private Access は Chrome Enterprise Premium と統合されており、ブラウザ内で直接セキュアな SSH および RDP セッションを有効にします。詳細については、次のトピックを参照してください。

- [ブラウザ内での SSH アプリへのセキュアなアクセス](#)
- [ブラウザ内での RDP アプリへのセキュアなアクセス](#)

2025年11月

- **オンボーディングジャーニーの簡素化**

ハイブリッド展開向けの Secure Private Access のオンボーディングインターフェイスが大幅に簡素化され、すべてのコンポーネントの構成プロセスが合理化されました。強化されたユーザーインターフェイスには、各コンポーネントの構成ステータスを段階的に表示する直感的なトポロジビューが搭載されています。この視覚的なアプローチにより、管理者は展開の状態を迅速に理解し、完了した構成手順を特定し、まだ保留中のアクションを判断できるため、セットアップ時間を短縮し、構成エラーを最小限に抑えることができます。

また、ハイブリッド展開における NetScaler Gateway の構成を簡素化するために、NetScaler で SecurePrivateAccessProfile がサポートされています。

詳細については、「[Secure Private Access ハイブリッド展開の開始](#)」を参照してください。

- **Google Chrome Enterprise Premium のサポート機能**

Citrix Secure Private Access サービスと Google Chrome Enterprise Premium の統合により、エンドユーザーは Google Chrome ブラウザをエンタープライズブラウザとして使用して、プライベートな Web/SaaS アプリケーションに安全にアクセスできるようになり、データ損失防止 (DLP) コントロール、Web フィルタリング、ZTNA ポリシーの適用によるアプリケーションごとのアクセスを実現できます。

詳細については、「[Google Chrome Enterprise Premium との統合](#)」を参照してください。

- **コンポーネントの構成の問題を検証および特定するためのアナライザー**

コンポーネントアナライザーは、Secure Private Access ハイブリッドセットアップに必要な構成チェックを実行する Web ベースのツールです。必要なレポートをアップロードすると、アナライザーは、検出された StoreFront 構成エラーの例を含む詳細なエラーメッセージと説明で問題を特定します。このツールは、特定された問題を解決するための潜在的な修復策も一覧表示します。

詳細については、「[コンポーネントアナライザー](#)」を参照してください。

- **NetScaler Gateway URL を使用して StoreFront UI からアプリを起動するサポート**

エンドユーザーは、NetScaler Gateway URL にアクセスすることで、StoreFront ユーザーインターフェイスから直接アプリケーションをシームレスに起動できるようになりました。

詳細については、「[Web および SaaS アプリケーションへのアクセス](#)」を参照してください。

- **アクセスポリシーにおけるネットワークロケーションサービス条件のサポート**

ネットワークロケーションサービス (NLS) は、ユーザーのネットワークロケーションに基づいてアクセスを制限できるポリシー条件です。管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいてアクセスポリシーを構成できます。ロケーションは、ユーザーがアプリケーションにアクセスしている国、またはユーザーのネットワークロケーションのいずれかです。ネットワークロケーションは、IP アドレス範囲またはサブネットアドレスを使用して定義されます。

詳細については、「[ネットワークロケーション](#)」を参照してください。

- **構成レポート**

顧客管理者は、Secure Private Access のセットアップに関する洞察を得るために、構成レポートを生成できるようになりました。

詳細については、「[構成レポート](#)」を参照してください。

2025年9月

• iOSデバイス向けSecure Private Accessハイブリッド展開のサポート

Secure Access Clientバージョン25.08.1 for iOS以降、Secure Private Accessハイブリッド展開がモバイルデバイスでサポートされるようになりました。モバイルユーザーはiOSデバイスから企業アプリケーションにアクセスできます。

重要:

iOSプラットフォーム向けCitrix Secure AccessでのSecure Private Accessサポートには、HTTP「User-Agent」ヘッダーに文字列「NSGiOSplugin」も追加する必要があります。

例: `add vpn sessionPolicy PL_OSspahybrid "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") && (HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NSGiOSplugin\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixSecureAccess\"))" AC_OSspahybrid`

詳細については、以下のトピックを参照してください。

- [NetScalerの構成](#)
- [モバイルデバイス向けCitrix Secure Private Access。](#)

2025年8月

• Secure Private Accessサイト構成レポートの生成

顧客管理者は、Secure Private Accessサイトのセットアップに関する洞察を得るために、構成レポートを生成できるようになりました。構成レポートは、以下のシナリオで使用できます。

- 構成の問題を特定し、解決する。
- 調査およびトラブルシューティングの目的でCitrixサポートチームと共有する。
- 新しいサイトをセットアップしたり、既存のサイトの詳細を変更したりするための参照としてレポートを使用する。
- [追加のダッシュボードウィジェット](#)

ハイブリッド展開用のSecure Private Accessダッシュボードが強化され、より深い洞察と改善された監視を提供するために、以下のウィジェットが含まれるようになりました。

- デバイスポスチャログ
- コネクタステータス
- 起動数別上位アプリケーション
- 総訪問数別上位検出アプリケーション
- 適用別上位アクセスポリシー

詳細については、「[可視性と監視](#)」を参照してください。

2025年5月

- シトリックス セキュア プライベート アクセス™ と グーグル クローム エンタープライズ プレミアムの連携

Citrix Secure Private AccessとGoogle Chrome Enterprise Premiumの統合により、お客様はGoogle Chrome Enterprise Premiumをエンタープライズブラウザソリューションとして使用し、Citrix Secure Private Accessが提供するセキュアな接続とともに、プライベートWebアプリやSaaSアプリケーションへのセキュアなアクセスを実現できます。詳細については、「[Citrix Secure Private AccessとGoogle Chrome Enterprise Premiumの統合](#)」を参照してください。

2025年4月

- オンプレミスNetScaler® Gatewayでのデバイスポスチャチェック

Citrix Device Postureチェックは、オンプレミスNetScaler Gatewayと連携するように構成できるようになりました。この統合により、管理者はネットワークリソースへのアクセスを試みるデバイスのセキュリティポスチャを評価し、信頼できるデバイスのみが企業リソースにアクセスできるようにすることができます。

詳細については、以下のトピックを参照してください。

- [デバイスポスチャ](#)
- [オンプレミスNetScaler Gatewayでのデバイスポスチャチェック](#)
- [NetScaler Gateway認証用Citrix Device Postureサービス](#)

- **StoreFront™ と Secure Private Access間の通信におけるキーベース認証**

StoreFrontとSecure Private Access間の通信に、セキュリティキーベースの認証方法が導入されました。キーベース認証は、新規顧客にはデフォルトで有効になっていますが、既存顧客に

は無効になっています。既存顧客は、セキュリティキーを有効にして、StoreFront構成スクリプトを再度実行する必要があります。詳細については、「[StoreFrontの構成](#)」を参照してください。

- **ICAプロキシモードでのWeb/SaaSアプリのサポート**

ICAプロキシモードで、Web/SaaSアプリケーションの列挙と起動がサポートされるようになりました。これにより、新しいStoreFront UIを使用してアプリを列挙することも可能になります。

ICAプロキシモードのサポートは、NetScaler Gatewayリリース14.1ビルド43.x以降でのみ利用可能です。構成の詳細については、「[NetScalerの構成](#)」を参照してください。

- **マシンのコンテキストに基づいたアプリケーションルールの適用**

ユーザーのコンテキストに加えて、マシンのコンテキストに基づいてアプリケーションアクセスルールを適用できるようになりました。アクセスポリシーを作成する際に、マシンまたはユーザーのコンテキストを選択できます。詳細については、「[アプリケーションのアクセスポリシーの構成](#)」を参照してください。

- **NetScaler Gatewayを介したトンネリングからドメインを除外する**

NetScaler Gatewayを介した傍受およびトンネリングから除外できるドメインを構成できるようになりました。アプリケーションの接続タイプを「内部」または「外部」に設定することで、ドメインの傍受とトンネリングをそれぞれ許可または除外できます。詳細については、「[TCP/UDPアプリの構成](#)」を参照してください。

- **Secure Private Accessハイブリッド展開におけるDNS over TCPのサポート**

Secure Private Accessハイブリッド展開でDNS over TCPがサポートされるようになりました。アプリケーションのFQDNはTCPを使用して解決できるようになりました。

2024年12月

- **FIPSプラットフォームでのSecure Private Accessハイブリッドソリューションのサポート**

Secure Private Accessハイブリッドソリューションは、連邦情報処理標準 (FIPS) に準拠し、13.1–37.219以降のFIPSビルドを実行しているNetScalerプラットフォームでサポートされるようになりました。詳細については、「[連邦情報処理標準](#)」を参照してください。

2024年10月

以下のセクションでは、2024年10月に関する詳細情報を提供します。

初回リリース

ハイブリッド展開用のCitrix Secure Private Accessを使用すると、オンプレミスのStoreFrontおよびNetScaler Gatewayコンポーネントを使用してゼロトラストネットワークアクセス (ZTNA) ソリューションを実装し、Citrix Cloud™を使用して構成、管理、および監視機能を管理できます。

以下は、ハイブリッド展開用のCitrix Secure Private Accessの主な機能の一部です。

- **Web/SaaSおよびTCP/UDPのサポート:**

ハイブリッド展開用のCitrix Secure Private Accessは、Web/SaaSおよびTCP/UDPアプリをサポートしています。詳細については、次のトピックを参照してください。

- [システム要件と前提条件。](#)
- [Web/SaaSアプリケーションの構成](#)
- [TCP/UDPアプリの構成](#)

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 type *

HTTP/HTTPS

HTTP/HTTPS

TCP/UDP

App icon

 [Change icon](#)
(128 KB max, PNG)

[Use default icon](#)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

☐ Allow user to remove from favorites

☐ Do not allow user to remove from favorites

App description

App category ⓘ

Ex.: Category\SubCategory\SubCategory

URL *

Application URL (https://...)

App Connectivity * ⓘ

Internal

Related Domains *

App Connectivity * ⓘ

Internal

[+ Add another related domain](#)

Save

Cancel

- 強化されたアクセス制限オプション:

アプリケーションのアクセスポリシーを作成する際に、アプリケーションに適用する必要があるアクセス制限を選択できます。これらのセキュリティ制限はシステムに事前定義されています。管理者は、他の組み合わせを変更または追加することはできません。詳細については、「[アクセスポリシーの構成](#)」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

25

Add/edit restrictions

0 selected
☐ View selected only

	Access Settings	Current Value
> ☐	Clipboard	Enabled
> ☐	Copy	Enabled
> ☐	Download restriction by file type	Multiple options
> ☐	Downloads	Enabled
> ☐	Insecure content	Disabled
> ☐	Keylogging protection	Enabled
> ☐	Microphone	Prompt every time
> ☐	Notifications	Prompt every time
> ☐	Paste	Enabled
> ☐	Personal data masking	Multiple options
> ☐	Popups	Always block pop-ups
> ☐	Printer management	Multiple options
> ☐	Printing	Enabled
> ☐	Screen capture	Enabled
> ☐	Upload restriction by file type	Multiple options
> ☐	Uploads	Enabled
> ☒	Watermark	Disabled
> ☐	Webcam	Prompt every time

• DaaS モニター との セキュア プライベート アクセス 連携:

Secure Private Accessは、Citrix DaaSの監視およびトラブルシューティングコンソールであるMonitorと統合されています。管理者とヘルプデスク担当者は、DaaS MonitorからWeb/SaaSおよびTCP/UDPアプリのセッションとイベントを監視およびトラブルシューティングできます。詳細については、[Secure Private Access integration with DaaS monitor](#)を参照してください。

The image displays two screenshots of the Citrix Secure Private Access Monitor interface, showing session details and application topology for two different resources: HRBerry and Yahoo finance ssb.

Top Screenshot: HRBerry

- Application Topology:** Shows a flow from the Endpoint (Citrix Secure Access Agent) through Policy Evaluation (Allowed) to Citrix Cloud (Secure Private Access), and then to the Web app/SaaS app (HRBerry).
- About - HRBerry:**
 - Transaction ID: f4df0f15-e51d-4824-b66d-8240eb187869
 - Resource Type: Web
 - Accessed Resource: hrberry.com (121.242.181.232):443 (PROTOCOL_TCP)
 - Configured Policy Rules: 1
 - Reason: Application launch is allowed
 - Applied Security Restrictions: None
- Policy Evaluation:**
 - Access: Session
 - ID: 7d6647d5-6c5e-4569-9c14-1a7d52575ae1
 - Policy Name: spause001
 - Status: Policy conditions matched
 - Action-routing: Direct
 - Policy Condition Evaluation:
 - Type: User Group
 - Condition Criteria: Matches any of
 - Value: spause001
 - Evaluation Status: True
- Session Details:**
 - Session State: Active
 - Start time: Feb 19, 2025, 6:36 AM GMT+05:30
 - Last active time: Feb 19, 2025, 10:21 AM GMT+05:30
 - Gateway session ID: 06a45d26-1176-d0c9-2bbd-a83b8b942958
 - Gateway address: n/a
 - Gateway Virtual IP: n/a
 - Contextual Tags: PlatformDesktop

Bottom Screenshot: Yahoo finance ssb

- Application Topology:** Shows a flow from the Endpoint (Citrix Secure Access Agent) through Policy Evaluation (Denied) to Citrix Cloud (Secure Private Access), and then to the Resource Location (Connector Appliance) and the Web app/SaaS app (Yahoo finance ssb). A message indicates "No connection established".
- About - Yahoo finance ssb:**
 - Transaction ID: f7adc56c-3462-4c62-b129-9b1592a361e6
 - Resource Type: Web
 - Accessed Resource: finance.yahoo.com (180.222.114.12):443 (PROTOCOL_TCP)
 - Configured Policy Rules: 2
 - Reason: Application Launch was denied because of a policy
 - Applied Security Restrictions: None
- Policy Evaluation:**
 - Access: Session
 - ID: 56eb9857-41e7-4d76-b129-c24a0c179490
 - Policy Name: Yahoo finance ssb
 - Rule Name: r
 - Status: Policy conditions matched
 - Action applied: Denied Access
 - Action-routing: n/a
 - Policy Condition Evaluation:
 - Type: User Group
 - Condition Criteria: Matches any of
 - Value: spause001
 - Evaluation Status: True
- Session Details:**
 - Session State: Active
 - Start time: Feb 19, 2025, 6:36 AM GMT+05:30
 - Last active time: Feb 19, 2025, 10:19 AM GMT+05:30
 - Contextual Tags: PlatformDesktop

• アプリケーション検出:

アプリケーション検出機能は、管理者が組織内でアクセスされている外部および内部アプリケーション（HTTP/HTTPSおよびTCP/UDPアプリ）を可視化するのに役立ちます。この機能は、公開済みまたは未公開のすべてのドメイン/IPアドレスを検出し、一覧表示します。これにより、管理者はどのドメイン/IPアドレスが誰によってアクセスされているかを確認し、それらをアプリケーションとして公開して、それらのユーザーにアクセスを提供するかどうかを決定できます。詳細については、[Discover domains or IP addresses accessed by end users](#)を参照してください。

App configuration **App discovery** Security groups

All protocol Last 1 Week [+ Add filter](#)

App discovery shows list of domains visited by end-users. Select one or more domains to add them to a new or existing application.

2 Selected ☐ View selected only [Create application](#) [Add to an existing application](#)

	Domain/IP	Port	Protocol	Total Visits	Unique Users	Most Recent Visit	Assigned To App(S)
☐	meesho.com	443	HTTPS	3	1	2024-08-14 12:22:32	1
☐	www.google.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.googleadservices.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.bbc.com	443	HTTPS	1	1	2024-08-14 11:59:01	0
☐	myntna.in	443	HTTPS	1	1	2024-08-14 12:00:54	1
☐	www.apple.com	443	HTTPS	1	1	2024-08-14 12:00:54	0
☒	wikipedia.org	443	HTTPS	1	1	2024-08-14 12:16:21	0
☒	www.amazon.in	443	HTTPS	1	1	2024-08-14 12:16:21	0
☐	www.ajio.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	javatpoint.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	udemy.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	www.reddit.com	443	HTTPS	1	1	2024-08-14 12:22:32	0

• ポリシーモデリングツール:

ポリシーモデリングツール (**Access policies > Policy modeling**) は、管理者に予期されるアプリケーションアクセス結果（許可/制限付き許可/拒否）を完全に可視化します。管理者は特定のユーザーのアクセス結果を確認し、コンテキストタグのユーザー条件を追加します。詳細については、[Policy modeling tool](#)を参照してください。

Policy configuration **Policy modeling**

Model user access outcomes, given various contexts and conditions.

Device type: Desktop Domain: spablr1.com User name: spa user01

[+ Simulate conditions](#) Contextual tags = term

Contextual tags: [dropdown] = (equals) term [trash icon]

[Apply](#) [Cancel](#) [Clear filters](#)

Display name: spa user01
Domain name: spablr1.com

Application access ⓘ [Filter by app name](#) [search icon]

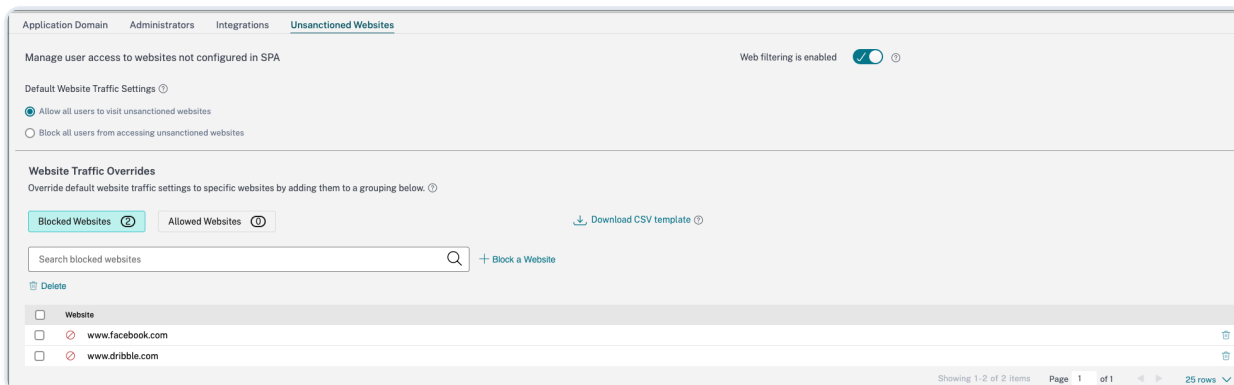
Application Name	Result	Policy Name
avanthika	✓ Access will be allowed	avanthika_pol
buddi_nani	! No access policy found	N/A

Showing 1-2 of 2 items Page 1 of 1 25 rows

• 未承認Webサイトのサポート:

Secure Private Access内で構成されていないアプリケーション（イントラネットまたはインターネット）は、「未承認Webサイト」と見なされます。デフォルトでは、Secure Private Accessは、アプリケーションおよびアクセスポリシーが構成されていない場合、すべてのイントラネットWebアプリケーションへのアクセスを拒否します。アプリが構成されていない他のすべてのインターネットURLまたはSaaSアプリケーションの場合、管理者は管理コンソールの **Settings > Unsanctioned Websites** タブを使用して、Citrix Enterprise Browser経由でのア

アクセスを許可または拒否できます。詳細については、Unsanctioned websitesを参照してください。



既知の問題

2511リリースにおけるハイブリッド展開用のSecure Private Accessには、以下の既知の問題があります。

- Citrix WorkspaceアプリまたはWebベースのユーザーインターフェイスからのアプリ起動時に、プロキシログインが要求されます。

回避策: アプリの起動を続行するには、プロンプトをキャンセルしてください。

- Chromeプロファイルがない状態でCitrix WorkspaceアプリまたはWebベースのユーザーインターフェイスから初めてアプリを起動すると、プロファイルが追加された後もアプリがChromeブラウザで開きません。
- NetScalerがGoogle Cloud IdentityのサードパーティSSOでOIDCのIdPとして追加されている場合、明示的にサインアウトした後、またはセッションタイムアウトにより、ユーザーはChromeプロファイルにサインインできません。

回避策: 管理対象プロファイルを削除して再追加する必要があります。

- Secure Private AccessハイブリッドCEP展開において、SSLデフォルトプロファイルまたは暗号グループが有効になっている場合、CEPプロキシとSecure Private Accessプロキシ間のmTLSハンドシェイクが失敗します。
- ネットワークロケーションサービス条件に対するポリシー変更（ロケーションタグの追加または削除）は、更新時に失敗します。
- Citrix Enterprise Premiumを構成する際、Google顧客が変更されると、不正確な検証と不明瞭なエラーメッセージが表示されます。
- ポリシーモデリングツールは、無効なポリシーのアプリを表示しません。
- Secure Private Accessダッシュボードのアプリケーション起動回数グラフには、SaaSアプリの起動回数が表示されません。

- Secure Private Accessダッシュボードのアプリケーション起動回数グラフには、特定の期間に起動されたすべてのアプリが表示されません。
- Linux向けCitrix ReceiverからWebアプリケーションを起動すると、AM_ERROR_UNEXPECTEDの警告が表示されます。
- アクセスポリシーユーザーインターフェイス（**Secure Private Access > Access Policies**）から、マシンベースのポリシーの条件を追加することはできません。
- SAMLを使用したデバイスポスチャは、nFactor認証フローではサポートされていません。
- NetScalerでOAuth IdPプロファイルを構成する際、クライアントシークレットフィールドでは特殊文字（#、@、!、\、&、%）は使用できません。
- NetScaler Gateway でクライアント証明書認証が構成されている場合、Linux 用 Citrix Secure Access クライアントは動作しません。
- アプリの FQDN が「.local」で終わる場合、Linux 用 Citrix Secure Access クライアントはアプリケーションをトンネルできません。
- 管理プロファイルでアプリを初めて起動すると、断続的に「Service Unavailable...」というエラーメッセージが表示されます。
- データ損失防止 (DLP) が構成されている場合、アプリへのアクセスは Citrix Secure Access クライアントによって許可されます。

システム要件と前提条件

以下のセクションでは、システム要件と前提条件に関する詳細情報を提供します。

ソフトウェアバージョンの要件

Secure Private Accessハイブリッド構成には、以下のソフトウェアバージョンが必要です。

- **NetScaler:** 14.1–66.54以降
- **StoreFront:** 2507 LTSR CU1または2511 CR以降
- **クラウドコネクタ:** 6.141.0 / 4.420.200 以降

エンドユーザーデバイスには、以下の最小ソフトウェアバージョンが必要です。

- **Web/SaaSアプリケーションの場合:**
 - グーグルクローム: 142
 - Windows用Citrix Workspaceアプリ: 2507.1 LTSRまたは2508
 - Mac用Citrix Workspaceアプリ: 2508.10
- **TCP/UDPアプリケーションの場合:**
 - Windows用シトリックス セキュアアクセス: 25.5.1.15
 - Mac用シトリックス セキュアアクセス: 25.11.1.1
- **エンドポイント分析 (EPA) の場合:**
 - Windows 用 EPA クライアント: 25.10.1.7
 - Mac 用 EPA クライアント: 25.10.3

ファイアウォールの要件

以下のファイアウォール要件は、StoreFrontサーバーおよびStoreFrontロードバランサーに標準のHTTPSポート443が使用されることを前提としています。標準以外のポートが使用されている場合は、それに応じてポート設定を調整してください。

送信元	送信元 IP	宛先	プロトコル	ポート	説明
インター ネット	任意	ネットス ケーラー ゲートウェ イ	TCP	443	-
StoreFront サーバー	StoreFront サーバーマ シンのIPア ドレス	Secure Private Accessロー ドバラン サー	TCP	443	-
クラウドコ ネクタ	Cloud Connectorマ シンのIPア ドレス	アクティブ ディレクト リ	TCP	389または 636	-

同じNetScalerにStoreFrontおよびSecure Private Access構成用のゲートウェイとロードバランサーが含まれている場合:

ソース	ソースIP	宛先	プロトコル	ポート	説明
NetScaler	NetScaler サブネット IP (SNIP) ア ドレス	StoreFront サーバー	TCP	443	-
NetScaler	NetScaler サブネット IP (SNIP) ア ドレス	クラウドコ ネクタ	TCP	8443	Secure Private Access にデ フォルト ポートが使 用されてい ると仮定し た場合
NetScaler	NetScaler サブネット IP (SNIP) ア ドレス	NetScaler アウトバウ ンドプロキ シ	TCP	アウトバウ ンドプロキ シポートに よって異な ります	-

ソース	ソースIP	宛先	プロトコル	ポート	説明
NetScaler	NetScaler サブネット IP (SNIP) ア ドレス	バックエン ドアプリ ケーション (Web アプ リまたはク ライアント/ サーバーア プリ)	バックエン ドアプリ ケーション プロトコル によって異 なります	バックエン ドアプリ ケーション ポートに よって異な ります	-

ゲートウェイとStoreFrontおよびSecure Private Access構成のロードバランサーに異なる
NetScalerを使用する場合：

ソース	ソースIP	宛先	プロトコル	ポート	説明
NetScaler Gateway (ネットス ケーラー ゲートウェ イ)	NetScaler Subnet IP (SNIP) アド レス	StoreFront ロードバラ ンサー	TCP	443	-
StoreFront ロードバラ ンサー	StoreFront ロードバラ ンサー IP ア ドレス	StoreFront サーバー	TCP	443	-
ネットス ケーラー ゲートウェ イ	NetScalerサ ブネットIP (SNIP) アド レス	Secure Private Accessロー ドバラ ンサー	TCP	443	-
Secure Private Accessロー ドバラ ンサー	Secure Private Accessロー ドバラ ンサーIP	クラウドコ ネクタ	TCP	8443	Secure Private Access にデ フォルト ポートが使 用されてい ると仮定し た場合

ソース	ソースIP	宛先	プロトコル	ポート	説明
ネットスケーラーゲートウェイ	NetScalerサブネットIP (SNIP) アドレス	NetScalerアウトバウンドプロキシ	TCP	アウトバウンドプロキシポートによって異なります	-
ネットスケーラーゲートウェイ	NetScalerサブネットIP (SNIP) アドレス	バックエンドアプリケーション (Web アプリまたはクライアント/サーバーアプリ)	バックエンドアプリケーションプロトコルによって異なります	バックエンドアプリケーションポートによって異なります	-

前提条件

Citrix Workspace™ アプリケーションと Chrome Enterprise Premium の最適な統合を確保するには、以下の前提条件を満たす必要があります。これらの前提条件を正常に完了すると、Citrix Workspace アプリまたはWebベースのユーザーインターフェイスからアプリケーションを起動する際に、より効率的でシームレスなエクスペリエンスが得られます。

NetScaler の前提条件

以下のセクションでは、NetScaler の前提条件に関する詳細情報を提供します。

クローム エンタープライズ プレミアム + シトリックス セキュア アクセス の展開

- Citrix Desktop as a Service (DaaS) に必要な設定で NetScaler Gateway が存在することを確認してください。この NetScaler Gateway は、Citrix Workspace アプリ/Citrix Receiver for Web で Secure Private Access アプリと DaaS アプリを列挙するために使用されます。
 - ウィザードを使用してGatewayを作成するには、「[Setting up NetScaler for Citrix Virtual Apps and Desktops](#)」を参照してください。
 - NetScaler Gateway をセットアップするには、「[How to configure NetScaler](#)」を参照してください。
- 新しい完全修飾ドメイン名 (FQDN) に対して、新しいパブリック IP アドレスと対応するプライベート IP アドレスが存在することを確認してください。パブリック IP はプライベート IP

に NAT される必要があります。この情報は、Secure Private Access アプリ用の新しい NetScaler Gateway を構成するために使用されます。この Gateway FQDN は、管理された Chrome プロファイルを使用してプライベート Web アプリにアクセスするために使用されます。エンドユーザーは、Citrix Secure Access クライアントからこの FQDN を使用してゲートウェイに接続し、内部アプリにアクセスすることもできます。このプライベート IP アドレスは、UI の **内部 IP アドレス** フィールドで使用する必要があります。詳細については、「[Get started with Secure Private Access hybrid deployment](#)」を参照してください。

- NetScaler Gateway 用の SSL サーバー証明書があることを確認してください。証明書には、新しい Secure Private Access NetScaler Gateway の FQDN を含む、必要な完全修飾ドメイン名 (FQDN) が含まれている必要があります。関連する構成の詳細については、「[NetScaler configuration](#)」を参照してください。
- NetScaler で認証プロファイルが構成されていることを確認してください。既存の認証プロファイルと、対応する認証仮想サーバーも使用できます。詳細については、「[Configure authentication](#)」を参照してください。

注：

Google OIDC の IdP として NetScaler Gateway を使用する場合は、「[Open ID Connect profile to use NetScaler Gateway as the IdP](#)」を参照してください。

Citrix Secure Access のみの展開

- 新しい完全修飾ドメイン名 (FQDN) に対して、新しいパブリック IP アドレスと対応するプライベート IP アドレスが存在する必要があります。パブリック IP はプライベート IP アドレスに NAT される必要があります。この情報は、Secure Private Access アプリ用の新しい NetScaler Gateway を構成するために使用されます。このゲートウェイ FQDN は、管理された Chrome プロファイルを使用してプライベート Web アプリにアクセスするために使用されます。エンドユーザーは、Citrix Secure Access クライアントからこの FQDN を使用してゲートウェイに接続し、内部アプリにアクセスすることもできます。このプライベート IP アドレスは、UI の **内部 IP アドレス** フィールドで使用する必要があります。詳細については、「[Get started with Secure Private Access hybrid deployment](#)」を参照してください。
- NetScaler Gateway 用の SSL サーバー証明書が必要です。証明書には、新しい Secure Private Access NetScaler Gateway の FQDN を含む、必要な完全修飾ドメイン名 (FQDN) が含まれている必要があります。関連する構成の詳細については、[NetScaler configuration](#) を参照してください。
- NetScaler で認証プロファイルが構成されていることを確認してください。

既存の認証プロファイルと、対応する認証仮想サーバーも使用できます。

新しい認証プロファイルを作成するには、[Configure authentication](#) を参照してください。

Cloud Connector の前提条件

- Cloud Connector で Secure Private Access サービスが有効になっていることを確認してください。サポートが必要な場合は、Citrix Support にお問い合わせください。
- Cloud Connector からポート 443 で [Connector Common and Secure Private Access FQDNs](#) へのアウトバウンド呼び出しが許可されていることを確認してください。詳細については、[System and Connectivity Requirements for Cloud Connectors](#) を参照してください。

詳細については、[Cloud Connector configuration](#) を参照してください。

StoreFront の前提条件

- StoreFront にリモートアクセスが有効なストアが作成されていることを確認してください (NetScaler Gateway が構成されていること)。[StoreFront documentation](#) を参照してください。
- Secure Private Access を StoreFront ストアのサイトとして追加します。
 - ストアを開き、**Manage Sites** を選択します。
 - **Add Site** をクリックし、タイプとして **Secure Private Access** を選択し、表示名と Secure Private Access ロードバランサーの FQDN を入力します。

注:

Secure Private Access を TCP/UDP (クライアント/サーバー) アプリケーションのみに使用している場合、StoreFront はオプションです。

詳細については、[StoreFront Configuration](#) を参照してください。

Secure Private Access の前提条件

- Windows Cloud Connector の受信ルールが、データセンターネットワークからのポート 8443 を許可していることを確認します。Citrix Secure Private Access は、ポート 8443 でプレーン HTTP サービスを公開します。
- Citrix Secure Private Access の内部ロードバランサーが、ポート 8443 で Cloud Connector バックエンドをターゲットにしていることを確認します。

- Citrix Secure Private Access の内部ロードバランサーで、SSL ブリッジまたは SSL オフロードが構成されていることを確認します。

詳細については、[Secure Private Access サービス](#) を参照してください。

Google の前提条件

以下のセクションでは、Google の前提条件に関する詳細情報を提供します。

Chrome Enterprise Premium ライセンス

Citrix Cloud Platform License (CPL) プログラムを通じて利用可能な、アクティブな Chrome Enterprise Premium ライセンスがあることを確認してください。

Google Workspace 管理コンソール

- **Google 顧客 ID:** Google 管理コンソールから Google 顧客 ID を取得します。この ID は、Google サービスと統合を構成するために必要です。顧客 ID は、Google 管理コンソールの **アカウント > アカウント設定** から取得できます。
- **Google 管理コンソールでカスタムロールを作成する:** 顧客を Chrome Enterprise Premium (CEP) にオンボーディングし、Google Chrome 統合を有効にするには、管理者は Google 管理コンソールでカスタムロールを作成し、適切な権限を割り当てる必要があります。詳細については、[管理者ロールと権限](#) を参照してください。
- **プロキシモードの構成:** プロキシモードを「ユーザーがプロキシを構成することを許可する」に設定します。「プロキシなし」、「OS プロキシ」、または「このプロキシのみを使用する」などの制限的なオプションは避けてください。

注:

Google 管理コンソールがシステムプロキシ設定を使用するように設定されている場合、管理プロファイルは Citrix Secure Private Access に必要なプロキシ構成を適用できず、Chrome Enterprise Premium との統合は失敗します。

- **DevTools 拡張機能を制限する:** 機密データの漏洩を防ぐため、強制インストールされた拡張機能の Chrome DevTools は無効にする必要があります。これは Google 管理コンソールのデフォルトオプションです。
- **Chrome Enterprise Premium の Google 管理コンソールでアクセス制限が構成されるようになりました:** 以前 Secure Private Access コンソールで構成されていたアクセス制限は、Citrix Enterprise Browser にのみ適用されます。Google Chrome がエンタープライズブラウザである

場合、アクセス制限はGoogle管理コンソールでポリシーおよびルールとして構成する必要があります。

- ポリシーは**Google管理コンソール > デバイス > Chrome > 設定**で構成されます。これらの設定により、JavaScriptのブロックやプリンターの許可リストなど、ブラウザ設定を管理できます。
- ルールは**Google管理コンソール > ルール**で構成されます。これらのルールは、透かしの追加、社会保障番号を含むファイルのダウンロードのブロック、URLフィルタリングなど、DLPに関連する高度な設定です。

Google Workspace管理コンソールでのポリシーとルールの作成の詳細については、以下のトピックを参照してください。

- [Chrome EnterpriseのChrome Enterpriseコネクタポリシーを設定する](#)
- [データ保護ルール](#)
- **ライセンス:** Citrix Cloud Platform License (CPL) プログラムを通じて利用可能な、アクティブなChrome Enterprise Premiumライセンスがあることを確認してください。

Google Chrome

以下のセクションでは、Google Chromeの前提条件に関する詳細情報を提供します。

管理対象Chromeプロファイル

すべてのエンドユーザーは、管理対象プロファイルを使用してChromeにアクセスする必要があります。管理対象プロファイルは、Chromeのポリシー、拡張機能、およびセキュリティ設定がユーザーデバイスに適用されることを保証します。

Citrix Workspaceで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと同期する

Citrix WorkspaceまたはStoreFrontで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと同期する必要があります。具体的には、以下のユーザーディレクトリがサポートされています。

- Active Directory
- マイクロソフト エントラ ID (旧称 アジュール アクティブ ディレクトリ)

注:

アプリケーションへのアクセスが適切に適用されるように、ユーザーディレクトリを定期的に同期してください。

メールアドレスフィールドへの入力 (必須)

Google Cloud ユーザーディレクトリでは、メールアドレスフィールドへの入力が必要です。

Google Cloud ユーザーディレクトリと同期するには、Secure Private Access のユーザーまたはグループオブジェクトにメールアドレスが必要です。そうでない場合、同期は失敗します。

統合された Chrome Enterprise Premium および Secure Private Access オファリングへのアクセスを必要とするすべてのユーザー、およびアクセスセキュリティポリシーに関与するすべてのグループについて、メールアドレスフィールドが入力されていることを確認してください。メールアドレスのドメイン部分は、Google 管理コンソールで設定および検証されているドメインである必要があります。

Active Directory の同期

Google Cloud Directory Sync を使用して、企業全体でシームレスな統合と一貫したユーザー管理を確保するために、AD を Google Cloud ユーザーディレクトリと同期する必要があります。

カスタムスキーマ「Citrix-schema」の下にカスタム AD フィールドを含めるように AD を Google Cloud と同期する方法の詳細については、「[Citrix Cloud に ID プロバイダーとして Google Cloud Identity を接続する](#)」を参照してください。

マイクロソフト エントラ ID

Google と Microsoft の両方のクラウドプラットフォームでユーザーとグループを管理するために、Microsoft Entra ID を Google Cloud ユーザーディレクトリと同期する必要があります。詳細については、「[ディレクトリ同期の開始](#)」を参照してください。

詳細については、「[Google Directory sync](#)」を参照してください。

TLS インспекションのバイパス

TLS インспекション (または SSL インспекション) を使用するネットワークで Chrome Enterprise Premium エンドポイントが正しく機能するようにするには、以下のホスト名をインспекションから除外する必要があります。

- `ingress.cloudproxy.app`
- `securegateway.goog`

- *.securegateway.goog

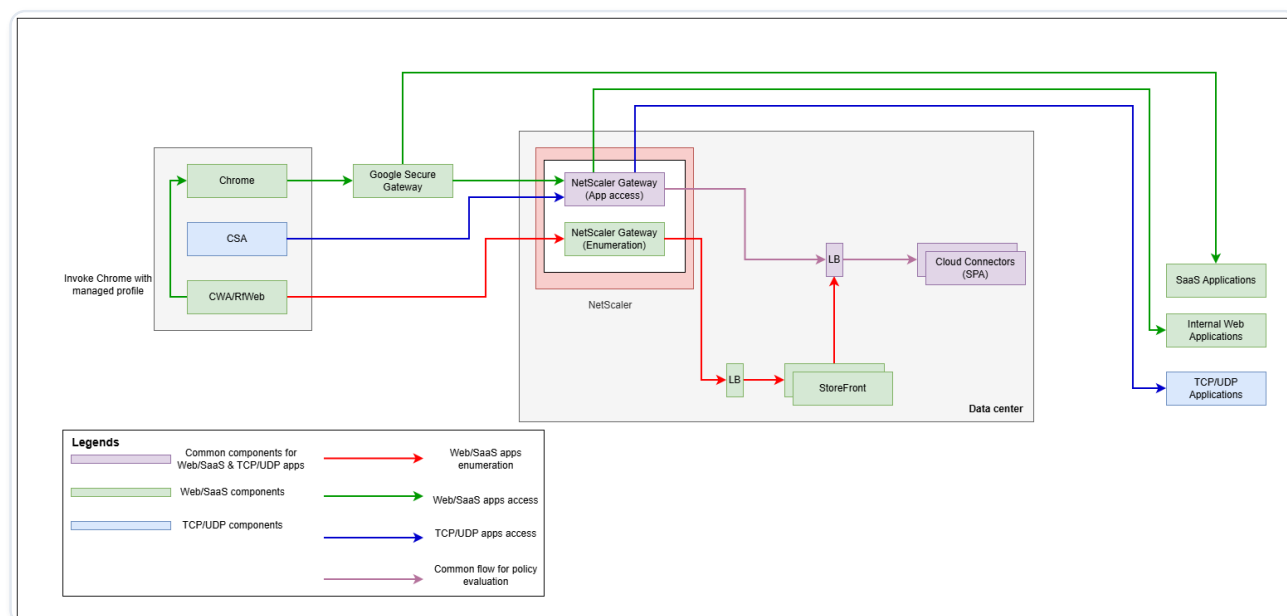
この除外は不可欠です。多くのTLSインスペクションソリューション（SSEベンダーやプロキシサーバーなど）は、Chrome Enterprise Premiumで使用されるHTTP CONNECTメソッドを完全にサポートしていないため、トラフィックが突然切断される可能性があります。

さらに、潜在的なエンドユーザーのパフォーマンス問題や接続遅延を回避するために、以下のホスト名をTLSインスペクションから除外することをお勧めします。

- safebrowsingrealtime.googleapis.com
- secureconnect-pa.clients6.google.com
- secureconnect-pa.mtls.clients6.google.com
- secureconnect-pa.googleapis.com
- chromereporting-pa.googleapis.com

Secure Private Access ハイブリッド展開の開始

このトピックでは、Secure Private Access ハイブリッド環境をセットアップするための段階的な手順を説明します。



開始する前に

以下のセクションでは、Secure Private Access ハイブリッド展開を開始する前に実行する必要があるチェックの詳細について説明します。

Secure Private Access の資格を確認する

Citrix Cloud アカウントで Secure Private Access サービスを利用できる資格が必要です。

- Citrix Cloud コンソールにログインします。
- ダッシュボードで、**Secure Private Access** サービススタイルが表示され、利用可能であることを確認します。
- サービスが表示されない場合、続行できません。資格の問題を解決するには、Citrix の担当者にお問い合わせください。

前提条件を確認する

すべての前提条件が満たされていることを確認します。詳細については、「[前提条件](#)」を参照してください。

すべてのネットワーク前提条件が満たされていることを確認します。必要なすべてのポートと通信パスの詳細については、[ネットワーク図](#)を参照してください。

展開モードを選択する

ようこそ画面で、**Set up for hybrid** を選択して構成を開始します。

次のステップ

- ステップ1: Google Chrome Enterprise Premium をセットアップする
- ステップ2: 最初のデータセンターをセットアップする
- ステップ3: 構成と分析

ステップ 1: Google Chrome Enterprise Premium をセットアップする

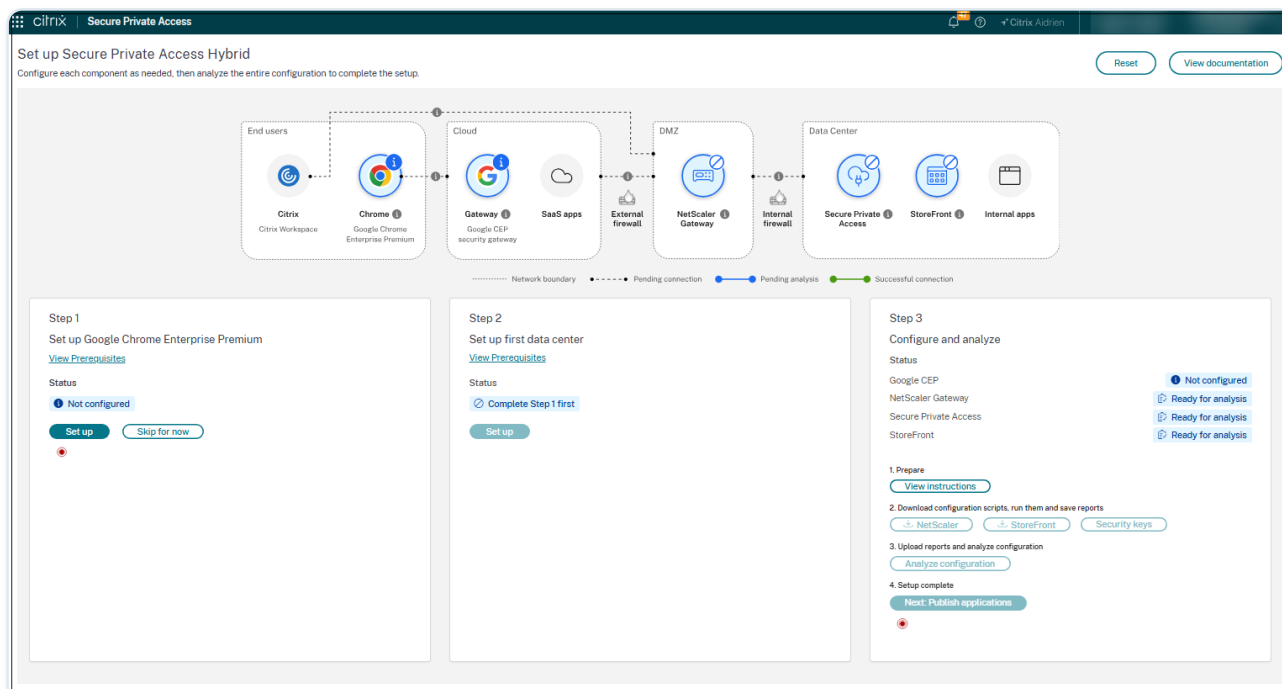
このステップでは、Google Chrome Enterprise Premium の設定を求められます。

注:

Google Chrome Enterprise Premium をセットアップする前に、次の点に注意してください。

- TCP/UDP (クライアント/サーバー) アプリケーションのみに Secure Private Access を使用している場合は、**今はスキップ** をクリックします。それ以外の場合は、Web または SaaS アプリケーションの設定を開始するには、**セットアップ** をクリックします。
- **今はスキップ** をクリックすると、完全なリセットなしでは後で Chrome Enterprise Premium を有効にすることはできません。
- Chrome Enterprise Premium を**セットアップ**することを選択した場合、Web/SaaS アプリケーションのサポートを有効にすることになります。このパスでは、TCP/UDP (クライアント/サーバー) アプリケーションも構成できます。将来的に Web または SaaS アプリケーションに Secure Private Access を使用する予定がある場合は、今すぐ**セットアップ**をクリックする必要があります。

このステップをスキップした後に Web または SaaS 機能を有効にする唯一の方法は、Secure Private Access の構成全体をリセットすることです。これを行うには、Citrix サポートにお問い合わせください。



グーグル クローム エンタープライズ プレミアム の設定手順

1. 画面の指示に従って、**Google 管理者ロール**を作成します。
2. 指示に従って、Secure Private Access ロール用に作成された新しいロールを**Citrix サービスアカウント**に割り当てます。このアカウントは、Citrix が Google Workspace 管理コンソールで必要な統合構成を実行するために使用されます。

Google Chrome Enterprise Premium

> View Prerequisites

Step 1
Assign Service Account

Service account is used to configure Google Workspace and Secure Private Access integration

1. Copy the service account address:

tenant-sa-k1cfyqmn0rvv@verdant-bruin-438923-p6.iam.gserviceaccount
Copy

2. In the Google Workspace console, open [Account > Admin Roles](#).

3. **Create new role** and select the [recommended privileges](#).

4. In the new role, select **Assign service accounts** under Admins.

5. Paste the service account (tenant-sa-k1cfyqmn0rvv@verdant-bruin-438923-p6.iam.gserviceaccount.com) and click **Add**. Then click **Assign Role**.

3. 画面の指示に従って、Google Workspace 管理コンソール内で**Google 顧客 ID** を見つけます。

Step 2
Enter Google Integration Details

You can find your Customer ID in your [Google Account Settings](#)

Google Customer ID ⓘ

CXXXXXXXX

Secure Private Access Gateway URL ⓘ

https://spagateway.mydomain.com

4. GoogleカスタマーIDをコピーし、**Google Customer ID**入力フィールドに貼り付けます。
5. NetScaler Gateway用にパブリックIPアドレスとDNSレコードをすでに予約していることを確認してください。

このパブリックURLを**Secure Private Access Gateway URL**フィールドに入力します。このURLは、[手順2 - 最初のデータセンターをセットアップする](#)で構成するNetScaler Gatewayのパブリックアドレスになります。マルチデータセンター、マルチサイト設定を構成している場合、これはグローバルサーバー負荷分散 (GSLB) ドメインURLのパブリックアドレスになります。

この設定を保存すると、**Google Secure Gateway**がこのアドレスを使用するように自動的に構成され、内部アプリへのアクセスでNetScaler Gatewayに接続できるようになります。

6. アクセスを許可する必要があるユーザーグループを選択します。これらのグループのメンバーのみが、Secure Private Accessで構成されたアプリケーションにアクセスできます。

注:

- 選択したユーザーグループは、Google Workspaceにすでに存在している必要があります。
- オプションで、ユーザーグループに加えて、またはユーザーグループの代わりに、選択したGoogle Directory組織単位に構成を適用します。詳細については、[Chrome Enterprise Premium構成を更新する](#)を参照してください。

7. **検証**をクリックして、すべての構成が正しいこと、およびSecure Private AccessがChrome Enterprise Premiumとの統合の準備ができていることを確認します。
8. **保存**をクリックします。

ステップ2: 最初のデータセンターをセットアップする

このステップでは、NetScalerでSecure Private Accessを構成するために必要な詳細を入力するよう求められます。

注:

NetScalerがすべての前提条件を満たしていることを確認してください。

NetScaler Gateway

> View Prerequisites

NetScaler Gateway Virtual Server Name ⓘ
_XD_443

Secure Private Access site URL ⓘ
https://spa.local

Secure Private Access Gateway URL ⓘ
https://spa.com

Internal IP address ⓘ
10.0

Certificate-key pair name ⓘ
star_local

- **NetScaler Gateway仮想サーバー名:** StoreFront展開で既に構成されているNetScaler Gateway仮想サーバーの名前を入力します。この仮想サーバーは、Citrix Store内でSecure Private Accessに構成されたアプリケーションを列挙するために使用されます。

注:

[Chrome Enterprise Premiumの構成](#)をスキップした場合、この入力是不要です。

- **Secure Private AccessサイトURL:** Cloud Connectorで実行されているSecure Private Accessサービスにトラフィックを誘導するロードバランサーのURLを入力します。

このロードバランサーは、**ポート443でHTTPS**を使用するように構成する必要があります。このロードバランサーをまだ作成していない場合は、続行する前に[Secure Private Accessロードバランサー](#)で手順を参照してください。

- **Secure Private Access Gateway URL:** このURLは、ユーザーと共有されるNetScaler Gatewayの公開アドレスです。内部アプリケーションへの接続に利用されます。

マルチデータセンター、マルチサイト展開を構成している場合、これはグローバルサーバー負荷分散 (GSLB) ドメインURLの公開アドレスになります。URLが[ステップ1: Google Chrome Enterprise Premiumのセットアップ](#)で以前に入力されている場合、事前に設定されます。

- **内部IPアドレス:** Secure Private Accessゲートウェイに使用される**プライベートIPv4アドレス**を入力します。このIPアドレスは、[ステップ3 - 構成と分析](#)での構成中にNetScaler Gateway仮想サーバーに割り当てられます。
- **証明書-キーペア名:** NetScalerに既に構成されている**SSL証明書-キーペア**の名前を入力します。
- **保存をクリックします。**保存すると、**共有シークレット**が表示されます。[ステップ3 - 構成と分析](#)での構成には、この共有シークレット値が必要です。

ステップ 3: 構成と分析

オンプレミスの StoreFront および NetScaler コンポーネントに構成を適用できるようになりました。

続行する前に、StoreFront と NetScaler の両方のすべての前提条件が満たされていることを確認してください。

NetScaler および StoreFront スクリプトのダウンロードと実行

以下のセクションでは、NetScaler および StoreFront スクリプトに関する詳細情報を提供します。

NetScaler スクリプト

注:

NetScaler 上のすべての Secure Private Access 構成は、**コマンドラインインターフェイス (CLI)** を使用して実行する必要があります。

1. **NetScaler** をクリックしてセットアップスクリプトをダウンロードします。このスクリプトは、Secure Private Access 展開用に NetScaler Gateway を構成および分析し、必要な情報を収集するように設計された診断ツールです。詳細については、[NetScaler Gateway Analyzer](#) を参照してください。

スクリプトファイル名は次の形式です。

```
gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz
```

Download NetScaler script for data centers

 Caution: Running this script on any other datacenter may cause errors. Back up the configuration before running.

Select Datacenter

Blue

Download NetScaler script

Close

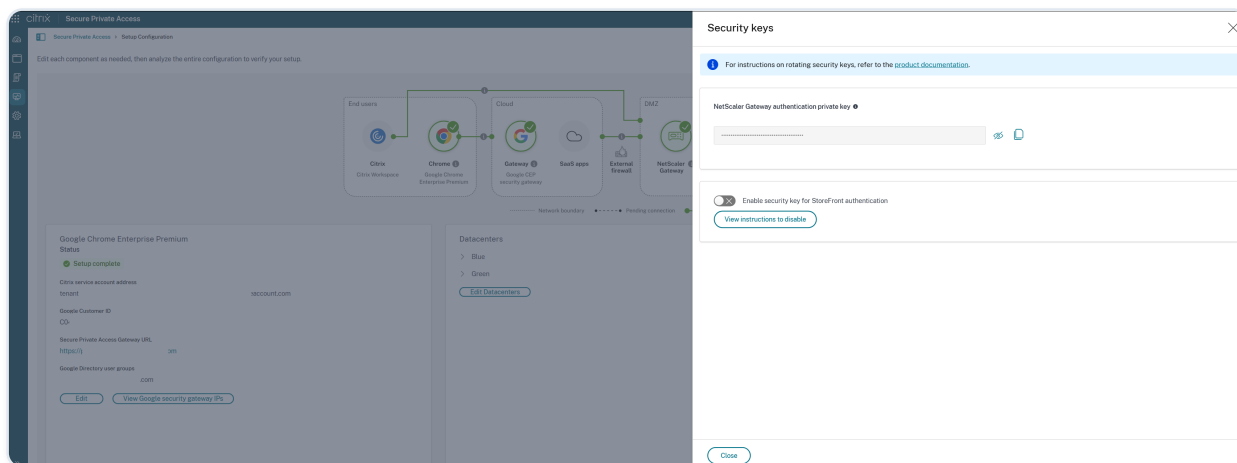
2. **SCP クライアント** (`scp` や WinSCP など) を使用して、ダウンロードした `*.tar.gz` ファイルを **NetScaler** にコピーします。
3. ファイルを `/var/tmp/` ディレクトリに配置します。
4. **SSH** (PuTTY など) を使用して、管理者 (`nsroot`) 権限で NetScaler のコマンドラインインターフェイス (CLI) にログインします。
5. CLIプロンプトで「shell」と入力してNetScalerシェルにアクセスします。一時ディレクトリに移動します: `cd /var/tmp/`
6. アーカイブを解凍します。

注:

ファイル名はダウンロードによって異なります。

```
tar -xzf gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz
```

7. `tar` コマンドはディレクトリを作成します。新しいフォルダーの名前を確認するには `ls` を使用し、そのフォルダーに移動します。
8. `python3`を使用してアナライザースクリプトを実行します: `python3 analyzer.py`
9. スクリプトがNetScaler Gateway認証秘密鍵の入力を求めるとき:
 - a. ブラウザでSecure Private Accessセットアップページに戻り、**Configure and analyze** カードの**Security keys**をクリックします。



- a. NetScaler Gateway認証秘密鍵をコピーします。
- b. 秘密鍵をNetScaler CLIに貼り付け、**Enter**を押します。

注:

このキーは、NetScaler GatewayでSecure Private Accessの構成を完了するために必要です。

10. スクリプトが正常に実行されると、現在のフォルダーに分析レポートが生成されます。
11. scp/winscpを使用してこのレポートをダウンロードして保存します。後でアナライザーに必要になります。

StoreFrontスクリプト

注:

この手順は、CSA専用モードの場合、つまり、[ステップ1 - Google Chrome Enterprise Premiumのセットアップ](#)でCEP構成がスキップされた場合にオプションです。

1. PowerShellスクリプトをダウンロードするには、**StoreFront**をクリックします。
2. このスクリプトは、以下の目的で設計された診断ツールです。
 - a. オンプレミスのStoreFront構成を分析します。
 - b. 展開に必要な情報を収集します。

警告:

管理者権限と実行ポリシーが必要です: このPowerShellスクリプトは、管理者権限で実行する必要があります（例: 右クリックして「管理者として実行」）。

さらに、スクリプトの実行を許可するためにPowerShellの実行ポリシーを調整する必要がある場合があります。必要に応じて、昇格されたPowerShellプロンプトから **Set-ExecutionPolicy Bypass**（または組織に適したポリシー）を実行することでこれを行うことができます。

スクリプトファイル名は次の形式です。

```
storefront_analyzer_<tenant-id>_<timestamp>.zip.
```

3. ダウンロードした.zipファイルを**StoreFrontサーバー**にコピーします。
4. StoreFrontサーバーで、.zipファイルの内容を展開します (例: C:\\temp\\spa-sf-script のようなフォルダーに\\))。
5. **管理者権限**で**PowerShell**ウィンドウを開きます（右クリックし、「管理者として実行」を選択）。
6. PowerShellウィンドウで、スクリプトを抽出したディレクトリに（cdを使用して）移動します。
7. 次のコマンドを実行してスクリプトを実行します。

```
.\CollectAnalyzerStorefrontInfo.ps1
```

スクリプトが正常に実行されると、分析レポートが生成されます。次のステップのためにダウンロードして保存してください。

レポートをアップロードして構成を分析する

オンプレミススクリプトによって生成されたレポートをアップロードして、構成を検証できるようになりました。

1. **分析**をクリックします。
2. 分析レポートのアップロードを求められます。生成した2つのファイルをアップロードします。

- **NetScaler**分析レポート。
- **StoreFront**分析レポート。

3. 両方のファイルが正常にアップロードされたら、**分析**をクリックします。
4. 分析が完了するまで待ちます。システムはすべてのチェックの**成功/失敗**結果を表示します。
5. **分析結果を確認**します。
 - a. **すべてのアナライズステップが合格した場合:** 構成が正常に検証され、次のステップに進むことができます。

Analyze configuration

> Prepare for analysis

Secure Private Access

✓ Setup complete

Test	Status
spa.check.cloud.access	✓ Success
spa.check.db.access	✓ Success
spa.check.tagsservice.access	✓ Success
spa.check.cas.access	✓ Success

Showing 1-4 of 4 items Page 1 of 1 5 rows

NetScaler Gateway

✓ Setup complete

Upload report to analyzer

Drag and drop report here or [Browse](#)

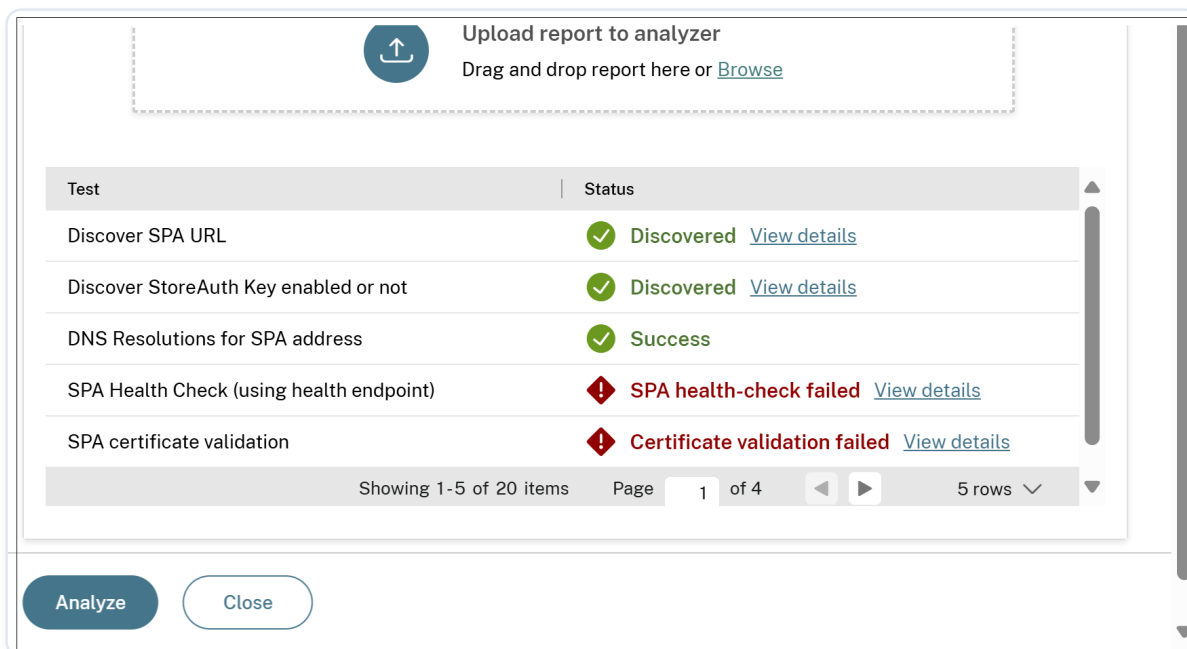
Test	Status
SPA vServer Configuration Check	✓ Success
SPA Profile High Cipher Check	✓ Success
SPA vServer SSL Profile Set Check	✓ Success
SPA Profile Configuration Check	✓ Success
SPA Profile Binding Check	✓ Success

Showing 1-5 of 25 items Page 1 of 5 5 rows

Analyze Close

- b. **いずれかの手順が失敗した場合:**
 - i. レポートには**修復手順**が示されています。

- ii. 提案された指示に従って、失敗したコンポーネント (NetScaler または StoreFront) のエラーを修正してください。
- iii. 問題を修正した後、そのコンポーネントで診断スクリプトを再実行して、新しいレポートを生成します。
- iv. この手順に戻り、新しい分析レポートを再アップロードします。



オンボーディングを完了し、アプリケーションを公開する

次へ: アプリケーションを公開をクリックして、セットアップウィザードを完了し、終了します。

これで、最初のハイブリッドオンボーディングが完了しました。マルチデータセンター、マルチサイト展開を構成する場合は、[高度なデータセンター構成](#)に進んでください。

オンボーディング後のタスク

以下のセクションでは、オンボーディング後のタスクに関する詳細情報を提供します。

アプリケーションの構成

次の緊急のタスクは、最初のアプリケーションを公開することです。少なくとも1つの内部Webアプリケーションまたは1つのTCP/UDPアプリケーションを公開して、セットアップをテストすることをお勧めします。[アプリの構成と管理](#)の詳細な手順に従ってください。

アクセス ポリシーの構成

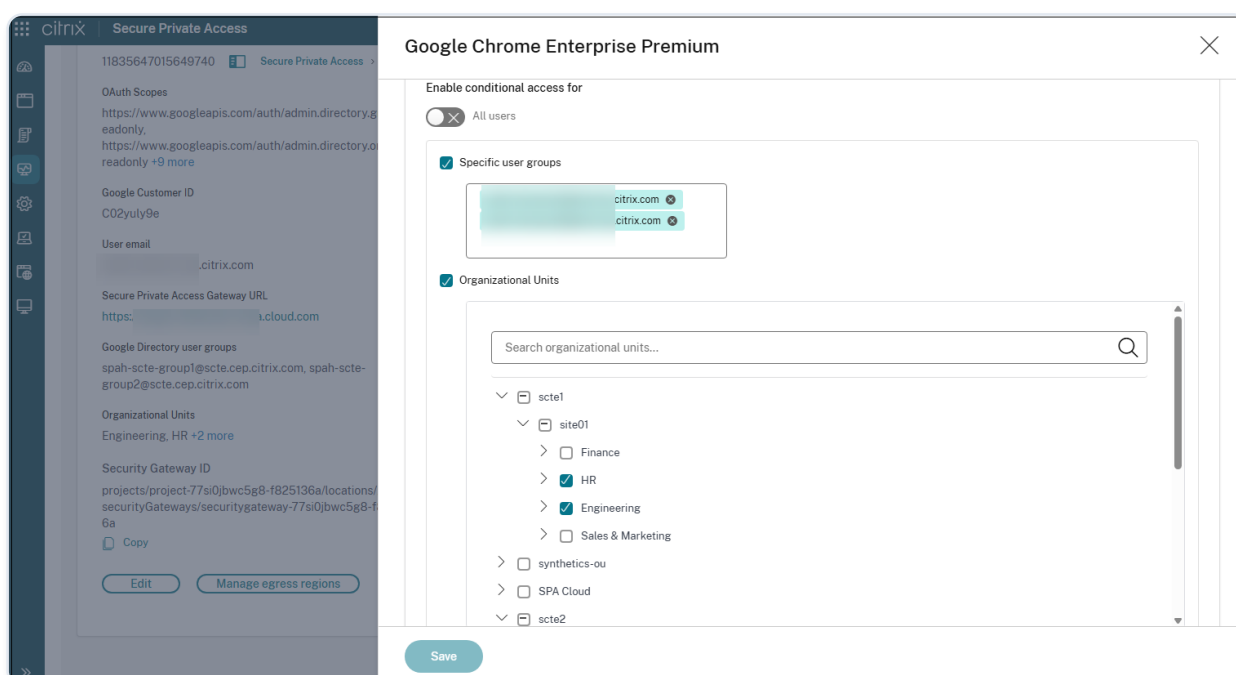
- Secure Private Access管理コンソールで、> の順に移動します。

- アプリケーションのアクセス ポリシーを作成し、を必ず定義してください。
- 詳細については、[アクセス ポリシーの構成と管理](#) を参照してください。

Chrome Enterprise Premium構成の更新

オンボーディング後にChrome Enterprise Premium (CEP) 構成を更新して、どのユーザーがそれを受け取るかを変更できます。すべてのユーザーとGoogleディレクトリのユーザーグループに加えて、選択したGoogleディレクトリの組織部門に構成を適用できます。ユーザーグループと組織部門は相互に排他的ではないため、単一の構成で両方をターゲットにできます。

1. Secure Private Accessコンソールのオンボーディングページで、Chrome Enterprise Premium セットアップカードの をクリックします。



2. をクリックして、Googleディレクトリの階層をチェックボックスのツリーとして表示し、含める組織部門を選択します。

注:

- 選択された組織部門は継承されます。構成は、その組織部門およびそのすべての子組織部門（後で作成されるものも含む）のユーザーに適用されます。親を選択すると、その子組織部門も選択され、選択済みでグレー表示されます。一部のみを含めるには、親の選択を解除し、特定の子組織部門を選択します。
- ルート組織単位はツリーに表示されません。すべてのユーザーに対してCEP統合を有効にするには、代わりに**すべてのユーザー**を選択します。
- 階層は、Citrixサービスアカウントを使用してGoogleディレクトリから読み取られます。これには**組織単位 > 読み取り権限**が必要です。詳細については、[管理者ロールと権限](#)を参照してください。

3. 選択を検証するには、**検証**をクリックし、次に**保存**をクリックします。

検証が成功した後に選択を変更した場合は、保存する前にもう一度検証を実行してください。

構成を同期する

変更（新しいアプリケーションまたはポリシー）を保存した後、オンプレミスのCloud Connector内のSecure Private Accessコンポーネントは、Citrix Cloudからこの新しい構成を同期する必要があります。

このプロセスは通常、完了までに**10分**かかります。

確認方法: 新しいポリシーがアクティブになっているかを確認するには、**ポリシーモデリングツール**（ポリシー > ポリシーモデリング内）を使用して、新しい構成が適用されたかどうかを確認することをお勧めします。

アプリケーションへのアクセス（エンドユーザー）

このセクションでは、エンドユーザーがデバイス上の公開アプリケーションにアクセスする方法に関する情報について説明します。

サポートされているデバイス:

- **Web/SaaSアプリケーション**（Google Chrome管理プロファイル経由）は、任意のデスクトップOSからアクセスできます。

Linux、iOS、およびAndroidデバイスでは、Web/SaaSアプリケーションはCitrix Secure Accessクライアントを介してアクセスできます。

- **TCP/UDPアプリケーション**（Citrix Secure Accessクライアント経由）は、**Windows、macOS、Linux、iOS、およびAndroid**でサポートされています。

WebおよびSaaSアプリケーションへのアクセス

ユーザーがデスクトップデバイスでWebアプリケーションにアクセスするには、主に3つの方法があります。これらの方法はすべて、Google Chromeの管理対象プロファイルでアプリを自動的に起動します。

方法A：管理対象プロファイルでChromeブラウザを使用する（推奨）

これはユーザーにとって最もシームレスなエクスペリエンスです。

1. **Google Chrome** ブラウザを起動します。
2. 初めての場合は、アクセスポリシーで構成されている会社のメールアドレスを使用して、新しいブラウザプロファイルを追加します。これにより、管理対象プロファイルが作成されます。
3. 管理対象プロファイルで、**NetScaler Gateway URL**（[手順2：最初のデータセンターをセットアップする](#)で構成したもの）に移動します。
4. ストアにログインします。
5. WebまたはSaaSアプリケーションアイコンをクリックして起動します。

アプリは管理対象プロファイルの新しいタブで起動します。

方法B：非管理対象Webブラウザを使用する

注：

この方法では、サポートされているバージョンのCitrix Workspaceアプリがデスクトップデバイスにインストールされている必要があります。

1. お好みのブラウザ（例：非管理対象のChrome、Edge、Firefox）を起動します。
2. **NetScaler Gateway URL**（[手順2：最初のデータセンターをセットアップする](#)でStoreFront用に構成したもの）に移動します。
3. ストアにログインします。
4. WebまたはSaaSアプリケーションのアイコンをクリックして起動します。
5. ブラウザに、**Citrix Workspaceアプリ**を開くよう促すダイアログが表示されます。
6. **続行**または**開く**をクリックします。

7. Citrix Workspaceアプリが引き継ぎ、**Google Chrome管理プロファイル**でアプリケーションを起動します。プロファイルがまだ作成されていない場合は、メールアドレスが事前に入力されたセットアップ画面が表示され、プロファイルを完了できます。

方法C：Citrix Workspaceアプリを使用する

1. デバイスで**Citrix Workspaceアプリ**を起動します。
2. まだ構成されていない場合は、**NetScaler Gateway URL** ((/ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-setup-netscaler-gateway.html)のStoreFront用に構成されたもの) を使用してストアを追加します。
3. ストアにログインします。
4. 列挙されたアプリケーションのリストが表示されます。
5. WebまたはSaaSアプリケーションのアイコンをクリックして起動します。アプリケーションは、管理されたGoogle Chromeプロファイルで自動的に開きます。

TCP/UDP（クライアント/サーバー）アプリケーションへのアクセス

TCP/UDPアプリケーションにアクセスするには、Citrix Secure Accessクライアントが必要です。

エンドポイントデバイスに、サポートされているバージョンのCitrix Secure Accessをインストールする必要があります。

Secure Accessクライアントを接続する

1. **Citrix Secure Accessクライアント**を起動します。
2. URLの入力を求められたら、**Secure Private Access Gateway URL** ((/ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-setup-netscaler-gateway.html)で構成されたFQDN) を入力します。
3. ログインと認証のプロンプトを完了します。
4. クライアントが接続し、バックグラウンドで安全に実行されます。

公開されたアプリケーションを起動する

Secure Private Accessポリシーで許可されている場合、ネイティブクライアントソフトウェアを直接使用できます。例：

- **Microsoft Remote Desktop**を開き、RDPサーバーの内部ホスト名に接続します。
- **SSHクライアント**を開き、Linuxサーバーの内部IPに接続します。

データ地域化

Citrix Secure Private Accessにおけるデータ地域化により、お客様は優先する地理的地域を選択することで、データの保存場所を制御できます。お客様は、グローバル、ヨーロッパ (EU)、APAC (アジア太平洋)、北米 (NA) などのオプションから、データの保存場所となる地域を選択できます。すべての保存済み構成データは選択された地域内に留まり、指定された地理的範囲外に出ることはありません。

データ地域化機能には、以下の利点があります。

- すべての構成データを選択された地域内に保持することで、強力なデータレジデンシー制御を保証します。
- 組織が規制およびデータ主権の要件を満たすのに役立ちます。
- データが指定された地理的範囲外に出るのを防ぐことで、リスクを軽減します。
- 地域固有のニーズを持つ柔軟なグローバル展開をサポートし、お客様がレジデンシーポリシーに沿ったクラウド提供のセキュアアクセスを安心して導入できるようにします。

注:

データ地域化がない場合、複数の地域で事業を展開する組織は、サービスデータの保存場所を制御できないまま、厳格なデータレジデンシーおよびコンプライアンス要件に直面する可能性があります。地域的なデータ境界がない場合、構成データが必要な地理的範囲外に保存される可能性があり、規制リスクが増大し、クラウド提供のセキュアアクセスソリューションの導入が制限されます。

サポートされる展開

この機能は、サービスモデルとハイブリッドモデルの両方を含むすべてのCitrix Secure Private Access展開に適用され、特に地域的なデータレジデンシー、コンプライアンス、および規制要件を持つ組織にとって重要です。

構成

地域の選択は、Secure Private Accessサービスまたはハイブリッド展開のオンボーディング時における1回限りの設定です。設定後は、すべてのデータが選択された地域に残り、継続的な運用やユーザーワークフローに影響はありません。

1. Citrix Cloudにログインし、**Secure Private Access**をクリックします。
2. **Setup for cloud**または**Hybrid**を選択し、**Continue**をクリックします。
3. 「**展開リージョンを選択**」で、データを保存する必要があるリージョンを選択し、「**続行**」をクリックします。

制限事項

データリージョン化の制限事項は次のとおりです。

- データリージョン化は、保存されている構成データにのみ適用されます。その他のデータタイプ（テレメトリや転送中のデータなど）は、選択されたリージョンに制限されない場合があります。
- グローバルに動作する他のCitrix Cloudサービスに依存関係があり、それらが同じリージョン境界に従わない場合があります。
- これはオンボーディング時の一度限りの構成であり、後で変更することはできません。
- この機能は現在、新規顧客のみが利用できます。

コンポーネントのセットアップ

Cloud Connector の構成

Secure Private Access サービスは、Cloud Connector で Windows サービスとして実行されます。Cloud Connector がリソースの場所にインストールされていることを確認してください。必要に応じてセットアップしてください。

詳細については、「[Cloud Connector のインストール](#)」を参照してください。

Cloud Connector (または構成済みのプロキシ) が、`allowlist.json` ファイルの **Connector Common and SPA FQDNs** にリストされているすべての FQDN に、ポート 443 でアウトバウンドトラフィックを送信できることを確認してください。

セキュアプライベートアクセス サービス

ハイブリッド展開用の Secure Private Access™ サービスプロバイダーは、Citrix Cloud Connector の一部としてインストールされます。Citrix Cloud Connector がインストールされると、Citrix Secure Private Access サービスは Windows サービスに表示されます。Secure Private Access サービスは、ネットワークサービスアカウントで動作します。

重要:

- Cloud Connector が更新されると、Secure Private Access サービスは無効になります。この機能を有効にするには、お客様は Citrix サポートに連絡する必要があります。
- 有効にすると、サービスステータスは**実行中**に変わり、Secure Private Access サービスはコネクタマシンで自動的に起動します。

Citrix Secure Private Access サービスのポート構成

- Citrix Secure Private Access は、プレーン HTTP サービスとしてポート 8443 を使用します。
- データセンターネットワークからのアクセスを許可するために、ポート 8443 の受信ルールが追加されていることを確認してください。ポート 8443 は、ファイアウォールルールを手動で構成するか、Citrix Secure Private Access 構成ツールを実行することで開くことができます。

- Citrix Secure Private Accessのインストールフォルダー（デフォルトパス - C:\Program Files\Citrix\AccessSecurityService）に移動します。
- コマンド `.\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443` を実行します。

コマンドが正常に実行されると、ファイアウォールは自動的に構成されます。

- Citrix Secure Private Accessの内部ロードバランサーは、ポート8443を使用してCloud Connectorバックエンドサービスを追加します。

Secure Private Access ロードバランサー

Secure Private Accessサービスのロードバランサーは、次の2つのアプローチのいずれかを使用してTLSを有効にして構成する必要があります。

- **ロードバランサーでのSSLオフロード:** Secure Private Accessロードバランサーは、ポート8443でHTTP経由でCloud Connector上のSecure Private Accessサービスと通信し、TLS/SSL証明書はロードバランサーにインストールされます。ロードバランサーとSecure Private Accessサービス間のトラフィックはプレーンHTTPであり、暗号化されません。詳細については、「[SSLオフロードの構成](#)」を参照してください。
- **SSLブリッジ:** ロードバランサーは、暗号化されたトラフィックをCloud Connector上のSecure Private Accessサービスに転送します。各Cloud ConnectorホストのSecure Private AccessサービスにTLS/SSL証明書をインストールする必要があります。詳細については、[SSLブリッジの構成](#)を参照してください。

クラウドコネクタ上のセキュアプライベートアクセスサービス用のTLS/SSL証明書を構成する

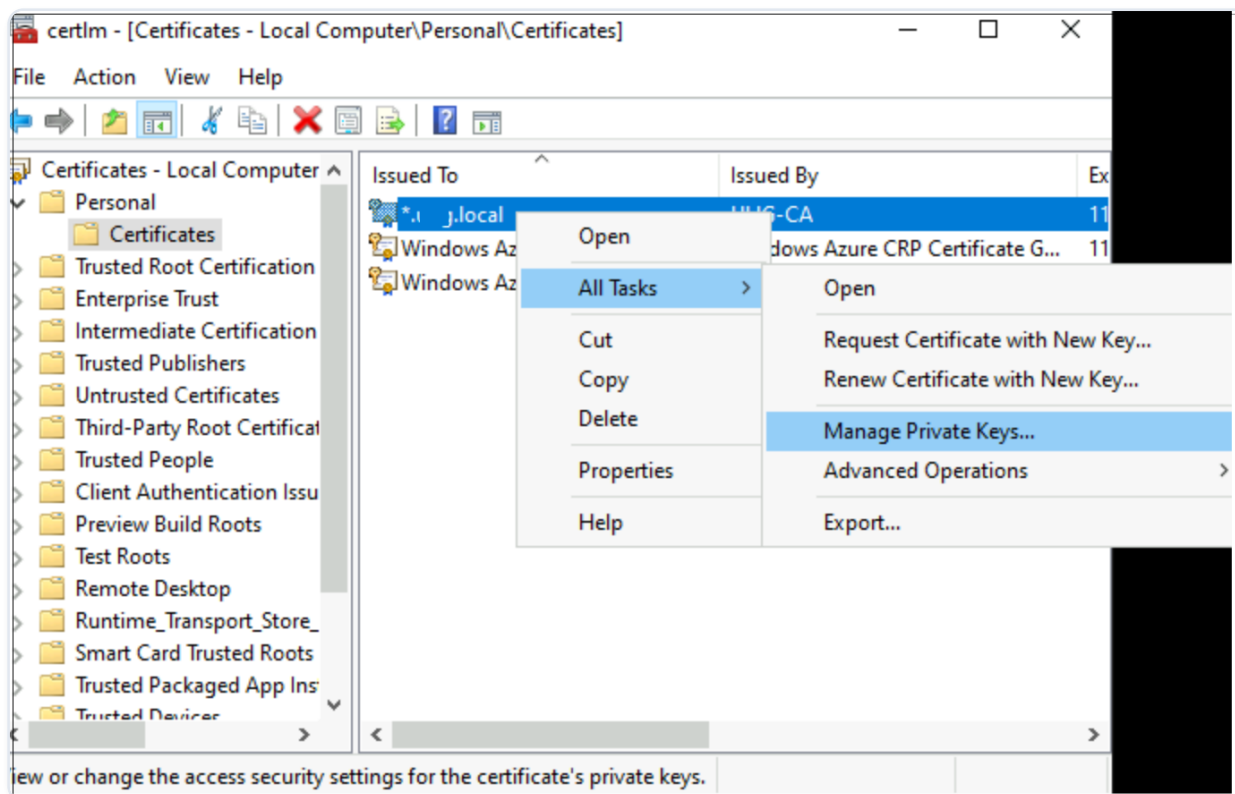
1. クラウドコネクタのローカルマシンの個人証明書ストアに有効なTLS/SSL証明書をインストールします。証明書が信頼されていることを確認してください。必要に応じて、発行元のCA証明書を追加します。

注:

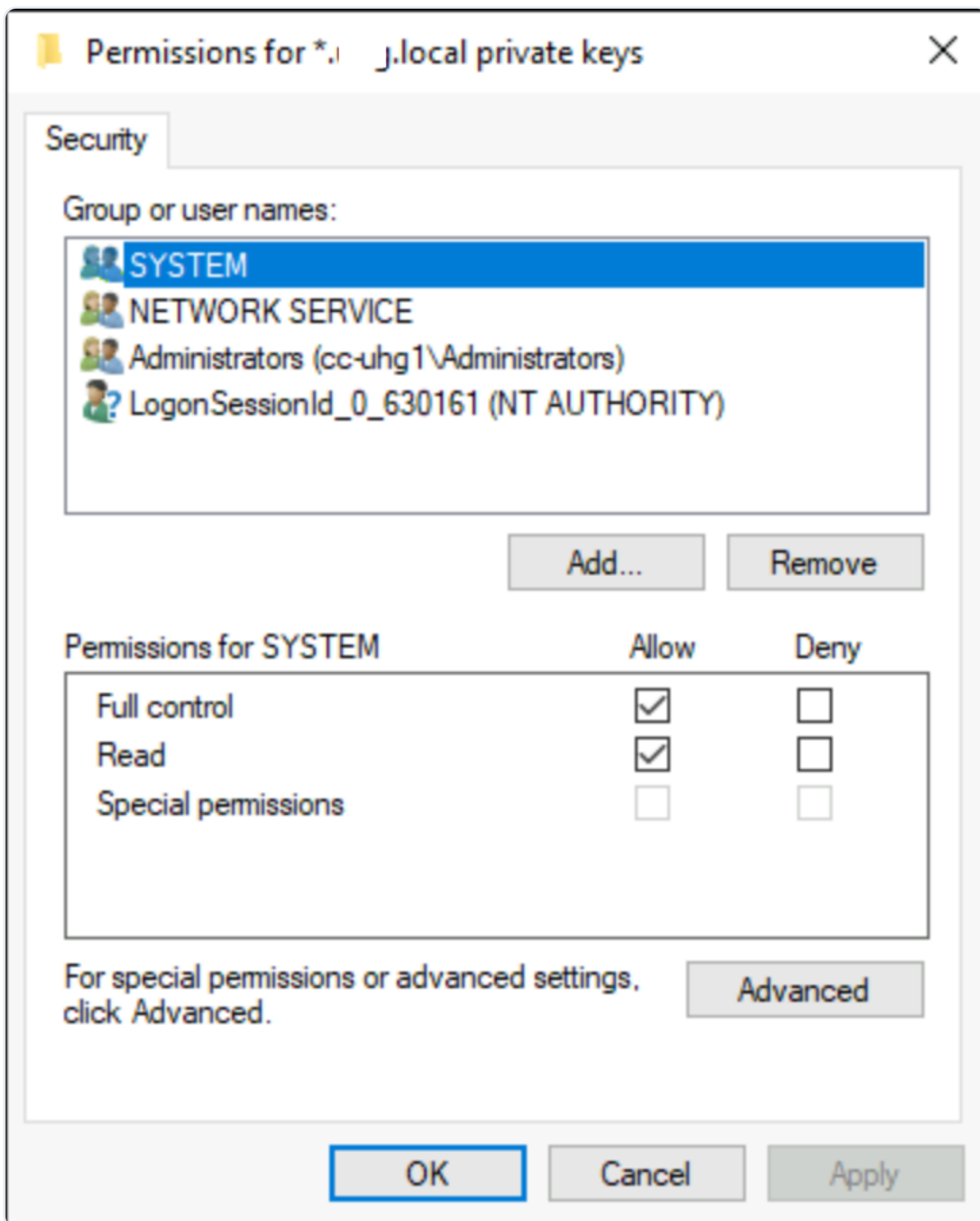
TLS/SSL証明書に、サブジェクトの別名 (SAN) の一部としてCloud ConnectorのFQDNが含まれていることを確認してください。

2. インストールされた証明書にアクセスするためのネットワークサービスアカウントのアクセス許可を付与します。

- a. Microsoft管理コンソールを開き、証明書スナップインをローカルコンピューターアカウントに追加し、ウィザードに従ってOKをクリックします。
- b. Microsoft管理コンソールで、コンソールルート > 証明書 > 個人 > 証明書に移動します。
- c. Secure Private Accessの構成に必要な証明書を右クリックし、すべてのタスク > プライベートキーの管理を選択します。



- a. アクセス許可ウィンドウで、追加をクリックし、ネットワークサービスアカウントを検索して、読み取り専用アクセス許可を選択します。



3. TLS/SSL証明書のサムプリントを使用してSecure Private Accessサービスを構成します。
 - a. **TLS/SSL証明書**の詳細からサムプリントをコピーします。
 - b. Citrix Secure Private Accessのインストールフォルダー（デフォルトパス - C:\Program Files\Citrix\AccessSecurityService）に移動し、.\Citrix.AccessSecurityService.exe / CERTIFICATE_THUMBPRINT <ThumbprintValue> を実行します。
 - c. Citrix Secure Private Accessサービスを再起動します。

- Secure Private AccessサービスがTLSサービスとして実行されていることを確認します (ブラウザまたはcURLを使用): `https://<Cloud connector address>:<port>/secureAccess/health`。

期待される結果: `response 200 OK with status "Ok"`。

NetScaler

このトピックは、NetScaler の構成に必要なすべての前提条件が満たされていることを確認するのに役立ちます。

- 以下のいずれかの方法を使用して、Citrix Virtual Apps and Desktops 用の NetScaler Gateway をセットアップします。
 - Citrix Workspace アプリまたは Web ブラウザを使用しているユーザー向けに、StoreFront にリモートでアクセスするための NetScaler Gateway 仮想サーバーを作成します。詳細については、「[NetScaler Gateway と StoreFront の統合](#)」を参照してください。
 - NetScaler Gateway の設定を構成します。詳細については、「[ウィザードを使用して NetScaler Gateway アプライアンスを構成する](#)」を参照してください。

注:

XenApp および XenDesktop ウィザードは、基本認証を構成します。Secure Private Access には高度な認証が必要です。そのため、XenApp および XenDesktop ウィザードの認証ステップをスキップできます。NetScaler Gateway がウィザードを使用して作成された後で、認証プロファイルを構成できます。

- NetScaler に SSL 証明書を追加します。詳細については、「[NetScaler インスタンスに SSL 証明書をインストールする](#)」を参照してください。

StoreFront のロードバランサーを構成します。詳細については、「[NetScaler を使用したロードバランシング](#)」を参照してください。

認証の構成

認証を構成するには、次の手順を実行します。

- 認証仮想サーバーを構成します。詳細については、「[認証仮想サーバー](#)」を参照してください。

- 認証プロファイルを構成します。詳細については、「[認証プロファイルの構成](#)」を参照してください。
- nFactor 認証を構成します。詳細については、「[nFactor 認証](#)」を参照してください。

一般的に使用される nFactor 認証方法:

- [LDAP認証](#)
- [RADIUS認証](#)
- [マイクロソフト Entra ID](#)

認証構成の例

以下のセクションでは、認証構成の例に関する詳細情報を提供します。

条件付き認証による多要素認証

- LDAPとRADIUSを使用した二要素スキーマによる二要素認証（ユーザー入力は1回のみ）
- 組織内のユーザーの部署（従業員、パートナー、ベンダー）に応じた認証ログオン方法（部署を選択するためのドロップダウンメニュー付き）
- ドロップダウンメニュー付きのユーザーのドメインに応じた認証ログオン方法
- メールID（またはユーザー名）入力を第一要素として構成し、第一要素でメールIDを使用したグループ抽出に基づく条件付きアクセスで、各グループに異なるログオンタイプを提供する
- ユーザー証明書を持つユーザー向けの証明書認証と、非証明書ユーザー向けのネイティブOTP登録を使用した多要素認証
- ユーザーのホスト名入力に応じた条件付き認証による異なる認証タイプ
- ネイティブOTP認証による二要素認証

多要素認証によるサードパーティ統合

- Azure ADをSAML IdPとして構成する（OAuth信頼を完了するために、次の要素をLDAPポリシー - NO_AUTHとして構成する）
- SAMLを第一要素とする条件付き認証、その後SAML属性に基づいて証明書またはLDAPへのカスタムログイン
- Web認証ログインを第一要素とし、その後にLDAP

デバイスポスチャスキャン (EPA)

- バージョンチェックのためのデバイスポスチャチェック、その後に準拠ユーザー（RADIUS）と非準拠ユーザー（LDAP）向けのカスタマイズされたログイン
- LDAP認証、その後に必須のデバイスポスチャスキャン
- AD認証の前後にデバイスポスチャチェック - 要素としての事前および事後EPA
- EPA要素としてのデバイス証明書

その他のシナリオ

- 認証付きEULAの追加
- nFactorポリシーラベル、ログインスキーマのカスタマイズ

StoreFront

オンプレミスのCitrix StoreでSecure Private Access Webアプリケーションを表示するには、StoreFront上でSecure Private Accessサービスを新しいDelivery Controllerとして構成する必要があります。

この手順に従ってください。特に、既存のCitrix DaaS環境と統合する場合（既存のStoreFrontを使用できるため）に役立ちます。

1. StoreFrontサーバーで、StoreFront管理コンソールを開きます。
2. Delivery Controllerを管理するセクションに移動します（例: **Store**を選択し、**Manage sites**をクリックします）。
3. 新しいコントローラーを作成するには、**追加**をクリックします。
4. コントローラーの種類を求められたら、**Secure Private Access**オプションを選択します。
5. サーバーフィールドに、Secure Private AccessロードバランサーのFQDNを入力します。
6. トランスポートの種類として**HTTPS**、ポートとして**443**を選択します。
7. 変更を保存します。

新しいStoreの構成

Storeがまだ存在しない場合は、サポートされているバージョンのStoreFrontをインストールし、**Storeの作成**ウィザードに従ってください。Storeが以下のように構成されていることを確認してください:

- **リモートアクセス:** リモートアクセス構成には、Secure Private Accessで公開されているWeb/SaaSアプリケーションを列挙するために使用されるNetScaler Gateway仮想サーバーアドレスが必要です。
- **認証方法:** Citrix Gatewayからのパススルーが有効になっていることを確認します。

詳細については、[Storeの作成](#)を参照してください。

コンポーネントアナライザー

コンポーネントアナライザーは、Secure Private Access ハイブリッドセットアップに必要な構成チェックを実行するWebベースのツールです。必要なレポートをアップロードすると、アナライザーは、検出されたStoreFront構成エラーの例を含む、詳細なエラーメッセージと説明で問題を特定します。このツールは、特定された問題を解決するための潜在的な修復策もリストします。

すべての構成チェックが合格したことを確認するには、修復を適用した後、アナライザーを再実行する必要があります。

検出されたStoreFront構成エラーの例。



Upload report to analyzer
Drag and drop report here or [Browse](#)

Test	Status
Discover SPA URL	✓ Discovered View details
Discover StoreAuth Key enabled or not	✓ Discovered View details
DNS Resolutions for SPA address	✓ Success
SPA Health Check (using health endpoint)	✗ SPA health-check failed View details
SPA certificate validation	✗ Certificate validation failed View details

Showing 1-5 of 20 items Page 1 of 4 5 rows ▾

Analyze Close

エラーがない場合、アナライザーはすべてのチェックで成功した結果を表示します。

Analyze configuration

> Prepare for analysis

Secure Private Access

Setup complete

Test	Status
spa.check.cloud.access	Success
spa.check.db.access	Success
spa.check.tag.service.access	Success
spa.check.cas.access	Success

Showing 1-4 of 4 items Page 1 of 1 5 rows

NetScaler Gateway

Setup complete

Upload report to analyzer

Drag and drop report here or [Browse](#)

Test	Status
SPA vServer Configuration Check	Success
SPA Profile High Cipher Check	Success
SPA vServer SSL Profile Set Check	Success
SPA Profile Configuration Check	Success
SPA Profile Binding Check	Success

Showing 1-5 of 25 items Page 1 of 5 5 rows

Analyze

Close

Secure Private Accessアナライザー

Secure Private Accessアナライザーは、Secure Private Accessの展開に必要な主要なCitrix Cloudコンポーネントの準備状況と到達可能性を評価します。レポートのアップロードは不要で、Cloud Access、データベースサービス、その他の必要な内部サービスなどの必須サービスへの接続を自動的にチェックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

68

各コンポーネントのアクセシビリティと稼働状況を確認することで、このツールは管理者がネットワークまたは構成の問題を迅速に特定するのに役立ち、Secure Private Accessの統合のためにすべてのCitrix Cloud依存関係が利用可能で適切に機能していることを保証します。

NetScaler Gatewayアナライザー

NetScaler Gatewayアナライザーは、主要なタスクを自動化し、構成の問題を強調表示することで、Secure Private Accessの展開を効率化します。ターゲットを絞ったチェックと検証を実行し、信頼性とパフォーマンスを向上させ、手作業と構成リスクを削減する実用的な診断を生成します。

NetScaler Gatewayアナライザーの機能は次のとおりです。

- **構成:** NetScaler Gatewayコンポーネントの自動または対話型セットアップ。
- **分析:** Secure Private Accessコンポーネント全体の接続性、コンプライアンス、および運用健全性の評価。
- **クリーンアップ:** 必要に応じてSecure Private Access構成を削除します。

各機能は、専用のコマンドラインオプション（README.txtを参照）を介して呼び出され、初期展開からメンテナンス、制御されたシャットダウンまで、柔軟なライフサイクル管理をサポートします。

実行により、構造化されたログと分析の概要を含むタイムスタンプ付きの成果物が生成されます。出力には、構成状態、接続テスト結果、検出されたコンポーネントメタデータ、および特定された問題が含まれます。クリーンアップ操作は、クリーンな状態を確保するためにエンティティ削除の確認を提供します。すべての結果は、自動化、統合、監査に適した構造化されたJSON形式で提供されます。

NetScalerでスクリプトをダウンロードして実行するには、[ステップ3: 構成と分析](#)を参照してください。

StoreFrontアナライザー

StoreFrontアナライザーは、検出および検証タスクを自動化することで、Citrix StoreFrontのSecure Private Accessの準備状況チェックを効率化します。構成、接続、認証、および証明書のターゲット評価を実行し、信頼性を向上させ、手動での作業と構成リスクを軽減する実用的な診断を生成します。

StoreFrontアナライザーの機能は次のとおりです。

- **分析:** Secure Private Accessの互換性に関連するStoreFront構成、ネットワーク到達可能性、認証設定、リモートアクセスパラメーター、および証明書の有効性の読み取り専用評価。

実行により、構造化されたログと分析の概要を含むタイムスタンプ付きの成果物が生成されます。出力には、Secure Private Access URLの検出、StoreAuthキーのステータス、DNS解決結果、ヘルスエンドポイントのアクセシビリティ、SSL証明書の検証、および検出されたコンポーネントメタデータが含まれます。すべての結果は、自動化、統合、監査に適した構造化されたJSON形式で提供されます。

構成の変更は行われません。アナライザーは読み取り専用モードで動作します。

NetScalerでスクリプトをダウンロードして実行するには、[ステップ3: 構成と分析](#)を参照してください。

グーグル クローム エンタープライズ プレミアム との統合

Citrix のお客様は、世界で最も人気があり安全なウェブブラウザである Chrome を使い慣れた操作感で活用し、承認された企業ウェブアプリケーションにネイティブにアクセスできます。Citrix Secure Private Access は、Secure Private Access コンソールを通じて一元的に管理される管理者定義のポリシーに基づいて、アプリケーションごとの最小特権アクセスを適用します。管理者は、Secure Private Access コンソールでエンタープライズアプリケーションドメインとゼロトラストアクセスポリシーを簡単に構成できます。ポリシーをモデル化してセキュリティの結果を検証およびテストし、適切なレベルのユーザーアクセスとエンドユーザーエクスペリエンスを提供できます。

統合ソリューションには、次のコンポーネントが含まれています。

- Google Chrome Enterprise Premium (CEP) には、データ損失防止 (DLP)、マルウェアおよびフィッシング対策、URL フィルタリング、Google 管理コンソールなどの機能が含まれています。
 - クライアントマシンでローカルに実行されている Google Chrome ブラウザは、Chrome 管理プロファイルを介したユーザーレベルごとのポリシー適用により、セキュアブラウザとして機能します。
 - Google Cloud ポータル経由でアクセスされる Google Chrome Enterprise Premium コンソールは、Chrome Enterprise Premium のセキュリティポリシー向けに管理、運用、監視コンソールを提供します。
- Citrix Secure Private Access には、クラウドインフラストラクチャへのアクセス、ZTNA ポリシーエンジン、および顧客環境に展開されたコネクタアプライアンスが含まれます。
- Citrix コンソールには、プライベートアプリケーションへのゼロトラストアクセスポリシー用の Secure Private Access コンソールと、監視とトラブルシューティング用の Citrix Monitor が含まれます。

Citrix Secure Private Access サービスは、管理者が構成したすべてのアクセスポリシーを適用し、ユーザーが特定のウェブアプリケーションにのみアクセスを許可されるようにします。

Chrome Enterprise Premium の高度なセキュリティ機能

以下は、Chrome Enterprise Premium が提供する高度なセキュリティ機能の一部です。

- **データ損失防止 (DLP):** 機密データが漏洩したり誤って共有されたりするのを防ぐために、きめ細かな制御とポリシーを実装します。
- **マルウェアの詳細スキャン:** 高度なスキャン技術を使用して、未知または高リスクのファイルを検出して隔離し、悪意のあるコードの実行を防ぎ、ゼロデイ攻撃から保護します。
- **フィッシング対策:** フィッシングの試みを特定してブロックすることで、有害なウェブサイトへのアクセスからユーザーを保護し、ログイン資格情報や個人情報の盗難を防ぎます。
- **URL の分類とフィルタリング:** コンテンツカテゴリに基づいてウェブサイトへのアクセスを制限し、ユーザーが不適切または悪意のあるコンテンツにアクセスするのを防ぎます。
- **ウェブ利用状況のインサイトと分析:** ウェブトラフィックに関する詳細なレポートと分析を提供し、管理者がユーザーアクティビティを監視し、潜在的なセキュリティ脅威を特定し、ネットワーク帯域幅を最適化できるようにします。

詳細については、「[Chrome Enterprise Premium の概要](#)」を参照してください。

統合を成功させるための前提条件

Citrix Workspace™ アプリケーションとChrome Enterprise Premium間の最適な統合を確保するには、以下の前提条件を満たす必要があります。これらの前提条件を正常に完了すると、Citrix Workspaceアプリまたはウェブベースのユーザーインターフェイスからアプリケーションを起動する際に、より効率的でシームレスなエクスペリエンスが得られます。

前提条件は、以下のカテゴリに大別されます。

- [NetScaler の前提条件](#)
- [Cloud Connector の前提条件](#)
- [StoreFront の前提条件](#)
- [Secure Private Access の前提条件](#)
- [Google の前提条件](#)
- Citrix Workspaceで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと同期する
- [TLSインスペクションのバイパス](#)

Citrix Secure Private Access - サポートされている展開モード

統合ソリューションは、Citrix Secure Private Accessからの以下の展開モードをサポートしていません。

- **Citrix Secure Private Accessサービス:** この展開モードでは、コントロールプレーンとゲートウェイインフラストラクチャを含むすべてのコンポーネントがCitrix Cloudでホストされます。詳細については、[Citrix Secure Private Access](#)を参照してください。
- **Citrix Secure Private Access ハイブリッド展開:** この展開により、お客様はオンプレミスのStoreFrontおよびNetScaler Gatewayコンポーネントを使用してゼロトラストネットワークアクセス（ZTNA）ソリューションを実装し、Citrix Cloudを構成、管理、および監視機能の管理に使用できます。これは、お客様が既存のオンプレミスNetScaler Gatewayを活用してユーザーのトラフィックルーティングを制御しつつ、Citrix CloudでホストされているUIを構成とポリシーの管理に使用し、さらにCitrix CloudでホストされているCitrix Monitorを監視およびトラブルシューティング機能に使用できることを意味します。詳細については、「Citrix Secure Private Access ハイブリッド展開」([/ja-jp/citrix-secure-private-access/hybrid.html](#))を参照してください。

重要:

Chrome Enterprise Premium (CEP) では、HTTPSエンタープライズWebアプリとSaaSアプリのみがサポートされます。HTTPエンタープライズWebアプリとSaaSアプリはサポートされません。

法的情報

Chrome Enterprise PremiumはGoogle LLCによって提供され、その使用は、[Googleの許容される使用ポリシー](#)および[サービス固有の利用規約](#)に従うものとします。

管理者の役割と権限

Citrixサービスアカウントは、Secure Private Accessによって、ユーザーをChrome Enterprise Premium (CEP) にオンボーディングし、CEP統合を有効にするために使用されます。したがって、Google管理コンソールで、必要な権限を持つ役割をサービスアカウントに割り当てる必要があります。

Google管理コンソールでは、2種類の役割が利用可能です。

システムロール: これらはGoogleが提供するデフォルトの役割です。スーパー管理者ロールを除き、残りのシステムロールには、Secure Private AccessとのCEP統合に必要なすべての権限が含まれていません。

カスタムロール: これらはAdmin API権限の任意のサブセットを含むことができます。Secure Private AccessとのCEP統合に必要なすべての権限を含むカスタムロールを作成する必要があります。

このタスクを実行するには、スーパー管理者としてGoogle管理コンソールにサインインしている必要があります。

注:

スーパー管理者ロールはサービスアカウントに割り当てることはできません。

Googleカスタム管理者ロールの権限

CEPとSecure Private Accessの統合には、CitrixサービスアカウントがGoogle管理コンソールで以下の特定の権限を持つカスタムロールを持っている必要があります。

必要な管理者権限	この権限が必要な理由
顧客の管理 > 顧客の読み取り	Google顧客組織のフレンドリー名（表示名）を読み取るため。
組織部門 > 読み取り	構成された組織部門がGoogleディレクトリで利用可能であることを確認するため。
サービス > Chrome管理 > 設定 > ユーザー設定の管理 注: トップレベルの権限であるユーザー設定の管理と、サブ権限（アプリケーション設定の管理およびウェブ設定の管理）を選択していることを確認してください。	ユーザープロファイルでCEPおよびSPA統合に必要な必須の拡張機能とその構成を追加するため。

必要な管理者権限	この権限が必要な理由
サービス > Chrome管理 > 設定 管理対象ブラウザ > 読み取り	管理対象のChromeプロフィールと管理対象のブラウザを読み取るため。
ライセンス管理 > 読み取り	組織にプロビジョニングされたChrome Enterprise Premium割り当てライセンスの総数を照会するため。
レポート	割り当てられたライセンスを積極的に使用しているユーザーを読み取るため。 データ損失防止（DLP）ルールがトリガーされたときの活動イベントを読み取るため。 失敗イベントを読み取るため。
グループ > 読み取り	構成された統合グループがGoogleディレクトリで利用可能であることを確認するため。
サービス > アラートセンター > フルアクセス > アクセスの表示	データ損失防止のセキュリティアラートとログイン失敗イベントを読み取るため。
デバイスと設定の管理	デバイスのメタデータを読み取り、モニターネットワークトポロジビューに表示するため。
ユーザー > 読み取り	構成された統合ユーザーがGoogleディレクトリで利用可能であることを確認するため。

注:

- これらの管理者権限に対して、同等のOAuthスコープを付与することも必要です。
- すべての管理権限は、現在「**管理者権限**」セクションにあります。これには、以前「**管理コンソール権限**」および「**管理API権限**」セクションに記載されていた権限が含まれます。この変更は権限の割り当て方法には影響せず、既存の権限は以前と同様に機能し続けます。
- 最上位の権限「**ユーザー設定の管理**」と、サブ権限（「**アプリケーション設定の管理**」および「**Web設定の管理**」）を選択していることを確認してください。サブ権限のみを選択するだけでは不十分です。
- Citrix Secure Private Accessは、構成されたCitrixサービスアカウントを使用して、Googleアカウントに構成を展開します。Citrix Secure Private AccessとGoogle CEPの統合が完了したら、Google管理コンソールを開き、「**Chromeブラウザ > アプリと拡張機能**」に移動します。いくつかのブラウザ拡張機能がルート組織レベルで構成されていることに注意してください。これらは子OUに継承されます。ユーザーがこのテナントでGoogle Chromeプロファイルをオンボードすると、これらの拡張機能は自動的にプロビジョニングされます。

ロールと権限の作成と割り当て

カスタム管理者ロールを作成し、権限を割り当てるには、次の手順を実行します。

1. Google 管理コンソールで、**アカウント > 管理者ロール** に移動します。
2. **新しいロールを作成** をクリックし、ロールの名前と説明を入力します。
3. Google Chrome 統合に必要なすべての権限をこのカスタムロールに追加します。必要な権限のリストについては、[Google カスタム管理者ロールの権限](#) を参照してください。

ロールと権限に関する詳細については、[Google ドキュメント](#) を参照してください。

4. カスタムロールを保存します。

NetScaler Gateway を IdP として使用するための Open ID Connect プロファイル

NetScaler Gateway を IdP として使用するには、Google 管理コンソールで OIDC プロファイルを作成する必要があります。

Google 管理コンソール(/en-us/citrix-secure-private-access/media/spa-hybrid-oidc-google-console.png)

Google OIDC SSO プロファイルの作成

Google 管理コンソールで次の手順を実行します。

1. >> に移動し、 を選択します。

OIDC プロファイルの詳細(/en-us/citrix-secure-private-access/media/spa-hybrid-oidc-google-console-ssso.png)

2. プロファイルの名前を入力します。
3. OIDC の詳細を入力します。

- **クライアント ID:** ランダムなクライアント ID (通常は 22 文字の数字文字列) を使用します。
- **クライアントシークレット:** 32 文字以上のランダムな文字列を生成します。文字列には、英数字と特殊文字を含める必要があります。

NetScaler で OAuth IdP プロファイルを構成する際、クライアントシークレットフィールドでは、-#、@、!、\、&、% などの一部の特殊文字は使用できません。したがって、ここではクライアントシークレットフィールドでこれらの特殊文字を使用しないでください。

注:

NetScaler Gateway でクライアント ID とクライアントシークレットを手動で生成する必要があります。

- **発行者 URL:** このフィールドを `https://<SPAGatewayFQDN>/oauth/idp/<OAuthIdpProfileName>` に設定します。ここで、`SPAGatewayFQDN` は Secure Private Access Gateway URL に対応する FQDN であり、`OAuthIdpProfileName` は NetScaler Gateway で作成された OAuth IdP プロファイルの名前です。

注:

IdP プロファイル名にスペースを使用しないでください。

- **パスワード変更URL:** 空白のままにする（現時点では不要）

4. 保存をクリックします。

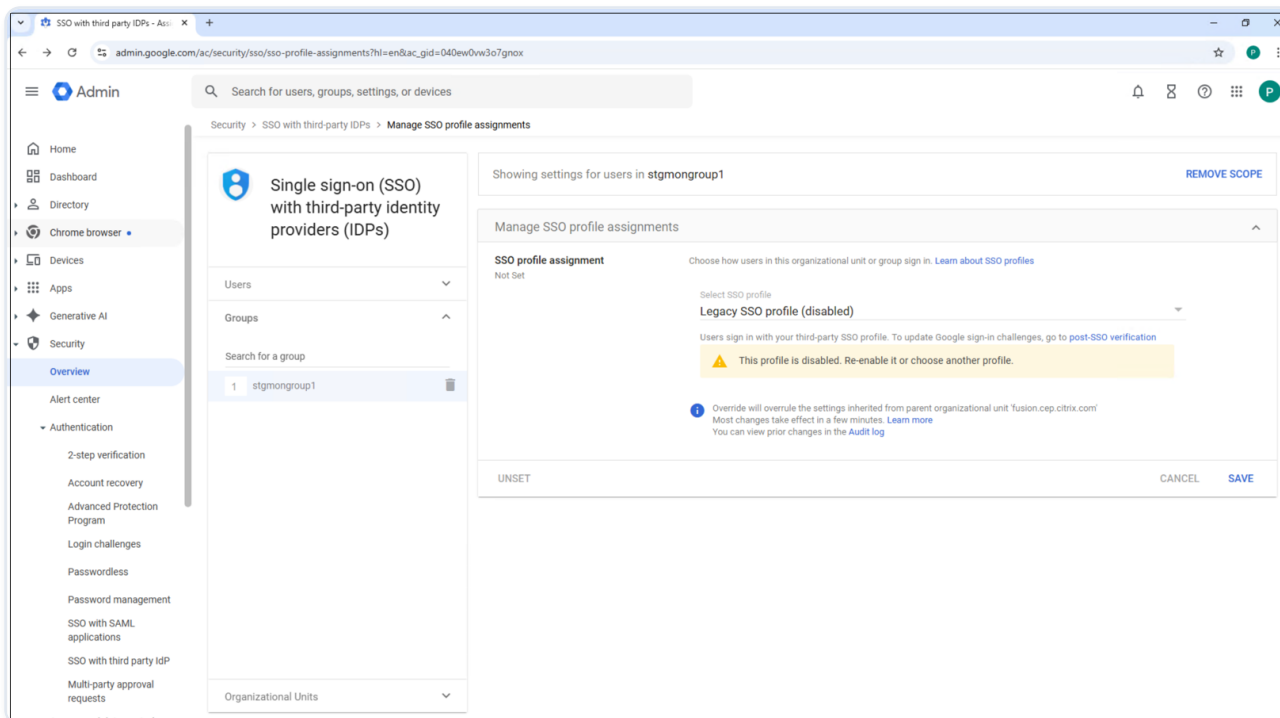
重要:

クライアントID、クライアントシークレット、およびリダイレクトURLをメモしておきます。これらの値は、NetScaler GatewayでOAuth IdPプロファイルを構成する際に必要です。

OIDCプロファイルのバインド（OUまたはグループのいずれかに）

OIDCプロファイルの設定を完了するには、Google Workspaceの特定の組織部門（OU）またはグループにバインドする必要があります。このバインドにより、NetScaler GatewayをIdPとして使用して、どのユーザーがこのOIDCプロファイルで認証できるかが決まります。

1. **セキュリティ > 認証 > サードパーティIdPとのSSO**に移動します。
2. **SSOプロファイル割り当ての管理**で、**管理**をクリックします。
3. 左側のナビゲーションペインから、ルート組織部門（OU）とSSOプロファイルを選択して、組織のすべてのユーザーに対してSSOを有効にします。または、SSOプロファイルを特定のグループまたはOUに割り当てることもできます。
4. 作成したSSOプロファイルを選択し、**保存**をクリックします。



NetScalerをOAuth IdPとして構成する

NetScalerをOAuth IdPとして構成する方法については、[OAuth IdPとしてのNetScaler](#)を参照してください。

注:

- OAuth IdPプロファイル内の**Audience**フィールドの値は、クライアントIDの値と同じである必要があります。
- **Issuer URL**は、Google管理コンソールで構成されているものと一致する必要があります。
- **Client ID**、**Client Secret**、および**Redirect URL**の値は、Google管理コンソールから取得する必要があります。

ディレクトリ同期

以下のセクションでは、ディレクトリ同期に関する詳細情報を提供します。

G Suiteコネクタを使用したMicrosoft Entra ID

GoogleとMicrosoftの両方のクラウドプラットフォームでユーザーとグループを管理するには、Microsoft Entra IDをGoogle Cloudユーザーディレクトリと同期する必要があります。詳細については、以下のトピックを参照してください。

- [Microsoft Entra ID \(旧Azure AD\) のユーザープロビジョニングとシングルサインオン](#)
- [Microsoft Entra IDでのシングルサインオンのためにMicrosoftによるGoogle Cloud / G Suiteコネクタを構成する](#)

すべてのユーザーとグループについて、メールアドレスフィールドに入力する必要があります。メールのドメインは、Google Directoryで構成されているものと一致する必要があります。これは、メールアドレスを持たないセキュリティグループや、@onmicrosoft.comのメールアドレスを持つグループは現在サポートされていないことを暗黙的に意味します。

シングルサインオン: シングルサインオン (SSO) の構成はオプションです。Googleディレクトリで別のパスワードを構成することもできます。[NetScaler GatewayをIdPとして使用するためのOpen ID ConnectプロファイルによるSSOの構成](#)を参照してください。

グーグル クラウド ディレクトリ シンク (GCDS) ツール

Google Cloud Directory Sync (GCDS) を使用すると、GoogleアカウントのデータをMicrosoft Active DirectoryまたはLDAPサーバーと同期できます。GCDSは、コンテンツ (メールメッセージ、カレンダーイベント、ファイルなど) をGoogleアカウントに移行しません。GCDSは、Googleユーザー、グループ、共有連絡先をLDAPサーバーの情報と一致させるために使用します。

詳細については、[Google Cloud Directory Syncについて](#)を参照してください。

GCDSのインストールと準備:

- [ダウンロード](#)
- [インストール](#)

注:

- POC目的で、GCDSツールはADマシンにインストールできます。
- インストーラーを管理者権限で実行します。
- 設定はファイルに保存でき (ファイル名前を付けて保存)、次回同期したいときに開くことができます。

アクティブディレクトリ

前提条件として、Active Directoryにユーザーとグループが作成されていることを確認してください。ユーザーとグループにはメール属性が必要です。

メール属性(/en-us/citrix-secure-private-access/media/spa-hybrid-gcds-email-attribute.png)

グーグルクラウド ディレクトリ シンク の構成

Google ドメインの構成:

1. プライマリドメイン名を入力します。
2. OAuth を使用して承認します。 **今すぐ承認** をクリックします。Google Workspace の管理者認証情報を入力するよう求められ、Google Workspace Directory へのアクセスを許可するよう求められます。

プライマリドメイン(/en-us/citrix-secure-private-access/media/spa-hybrid-gcds-primary-domain.png)

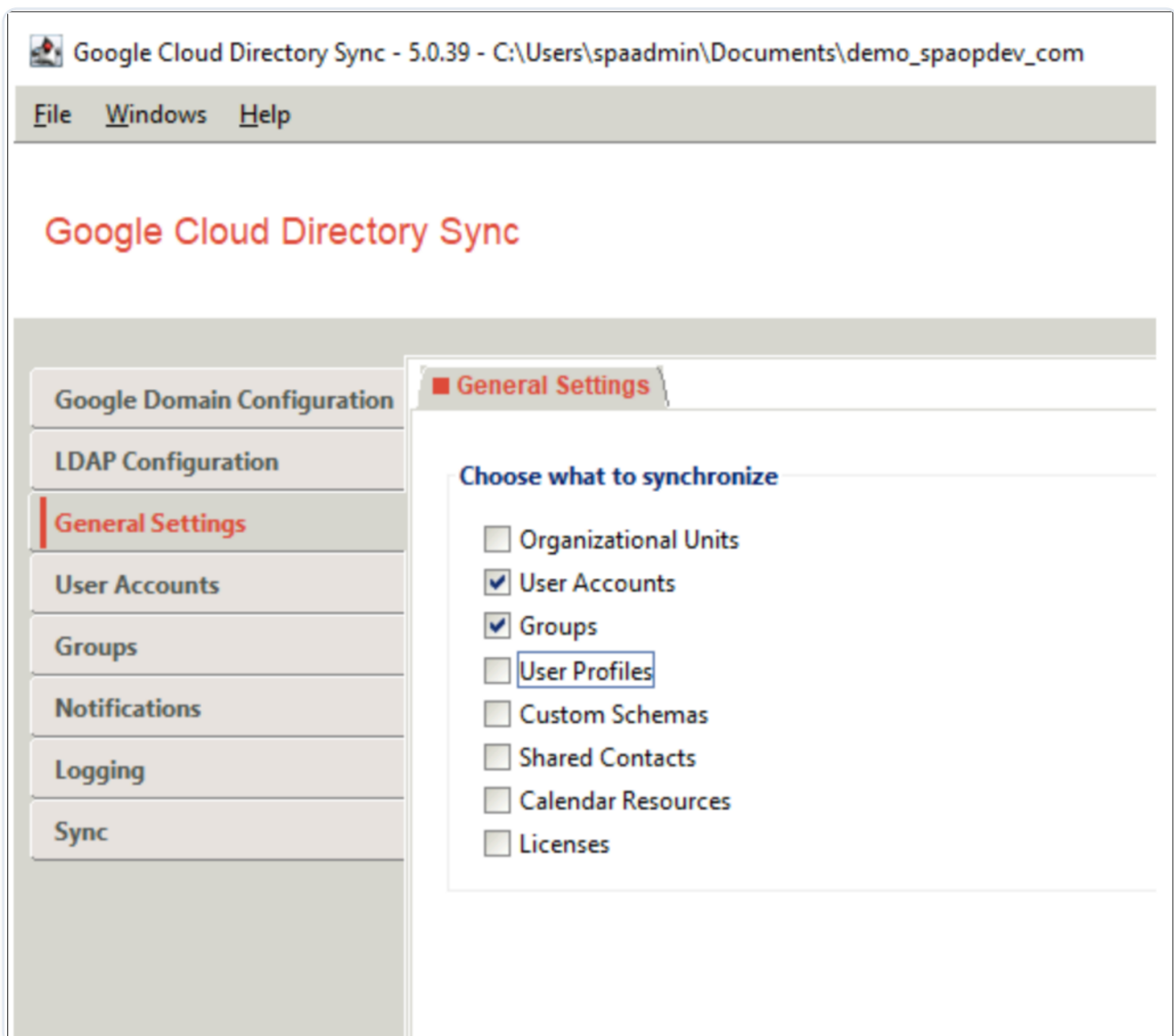
LDAP の構成:

1. ホスト名、ポート、承認済みユーザー、およびパスワードを入力します。

LDAP の構成(/en-us/citrix-secure-private-access/media/spa-hybrid-gcds-ldap-configuration.png)

一般設定:

同期する項目を選択します。



ユーザーアカウント:

1. インポートおよび同期するユーザーを指定します。
2. ユーザー属性、追加ユーザー属性、および検索ルールについては、デフォルトを使用をクリックします。

Google Cloud Directory Sync - 5.0.39 - C:\Users\spadmin\Documents\demo_spaopdev_com

File Windows Help

Google Cloud Directory Sync

Google Domain Configuration

LDAP Configuration

General Settings

User Accounts

Groups

Notifications

Logging

Sync

User Attributes Additional User Attributes Search Rules Exclusion Rules

User Email

Email Address Attribute:

☐ Enable invalid characters replacement

Invalid characters replacement:

User Attributes

Unique Identifier Attribute:

Alias Address Attributes:

Add Remove

Google Domain Users Deletion/Suspension Policy

Actions

Use defaults

Google Cloud Directory Sync - 5.0.39 - C:\Users\spadmin\Documents\demo_spaopdev_com

File Windows Help

Google Cloud Directory Sync

User Accounts

Google Domain Configuration

LDAP Configuration

General Settings

User Accounts

Groups

Notifications

Logging

Sync

User Attributes **Additional User Attributes** Search Rules Exclusion Rules

Given Name Attribute(s):

Family Name Attribute(s):

Display Name Attribute(s):

User Password Sync

Synchronize Passwords

☒ Only for new users ☐ For new and existing users ☐ Only changed passwords

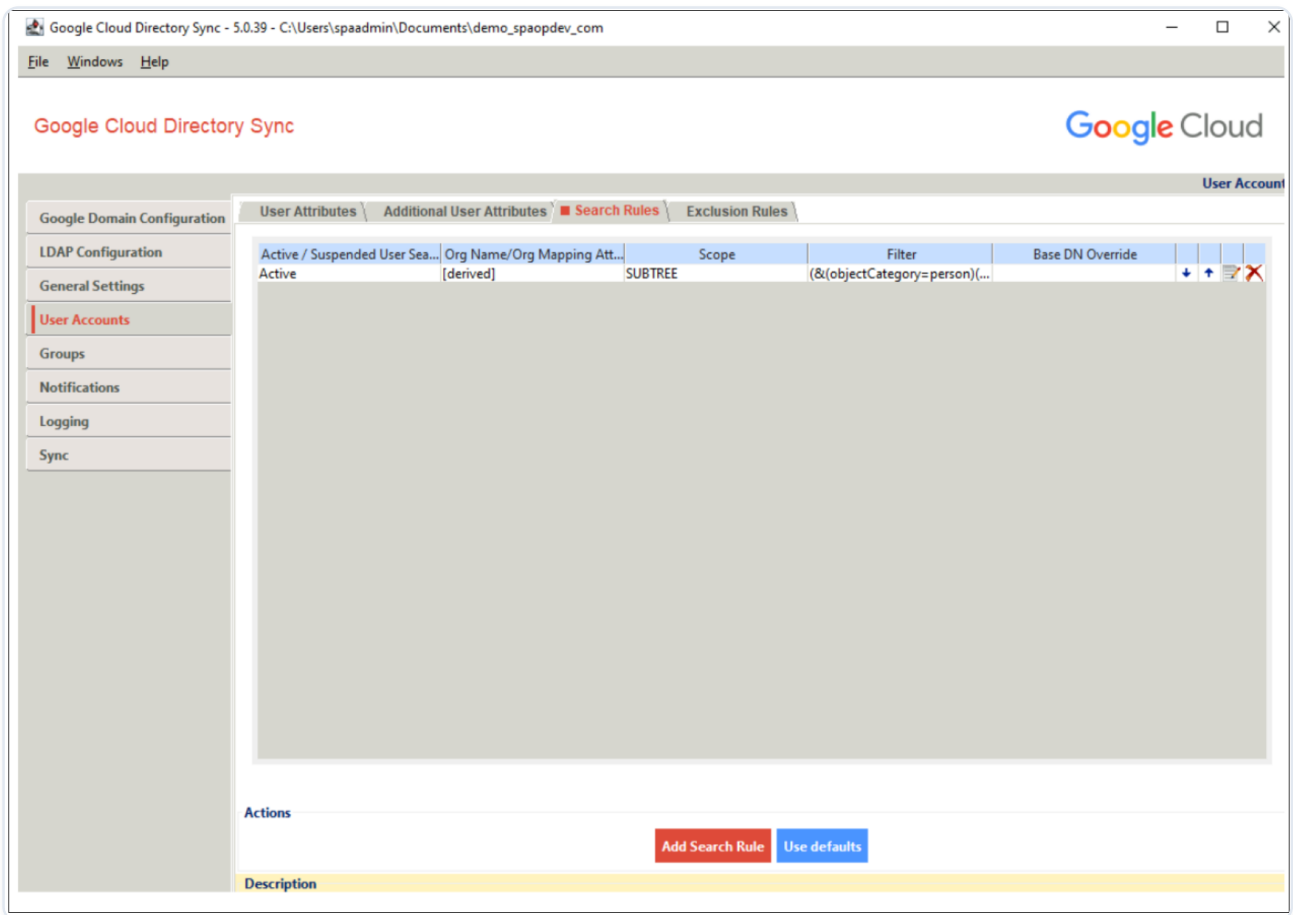
Password Attribute:

Password Timestamp Attribute:

Actions

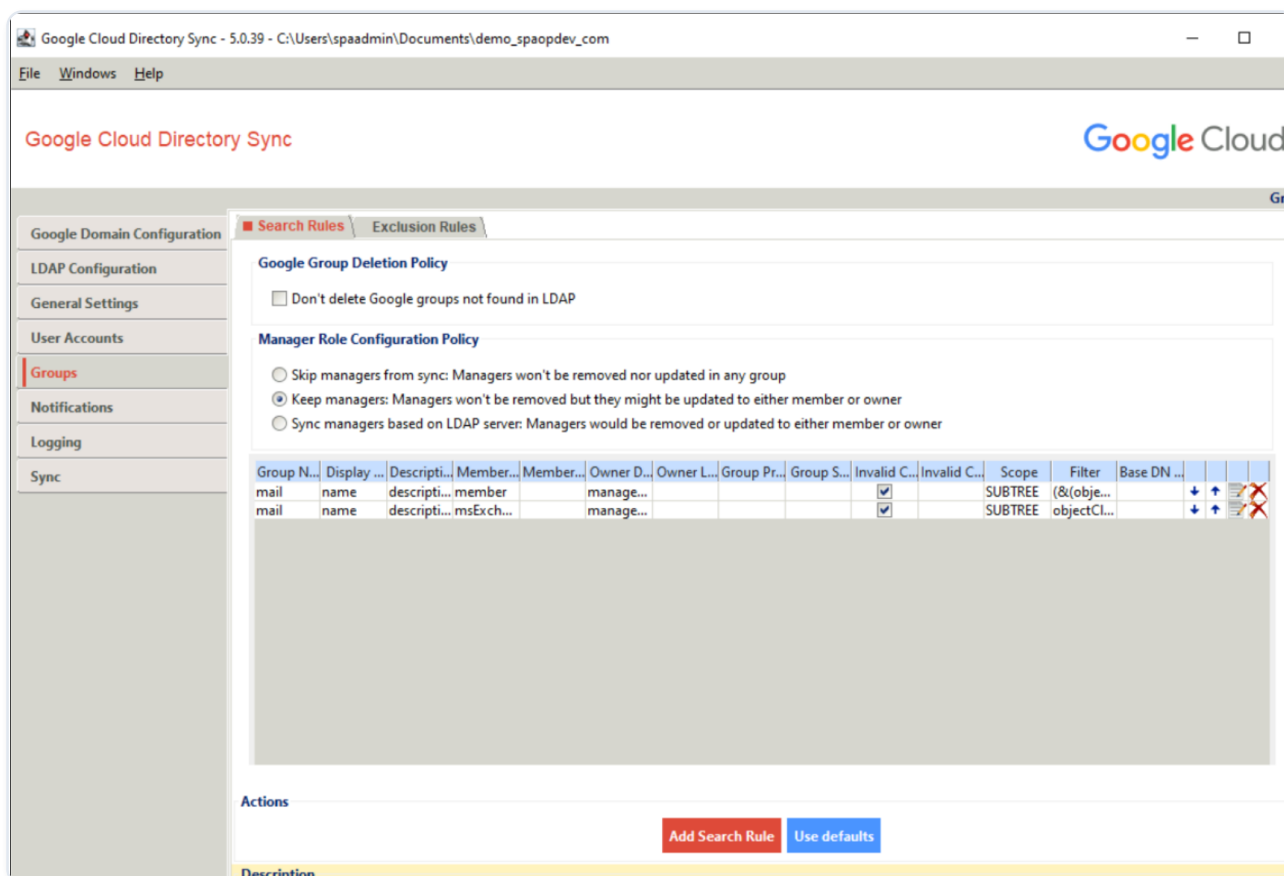
Use defaults

Description



グループ:

1. インポートおよび同期するグループを指定します。
2. グループの検索ルールについては、デフォルトを使用をクリックします。



通知:

この手順はオプションです。

同期後、Google Cloud Directory Sync は SMTP リレーホストに接続し、同期の詳細を含む通知を送信します。

- 通知ヘッダーに表示する送信元アドレスを指定します。
- 受信者のメールアドレスを1つずつ入力し、各アドレスに対して**追加**ボタンをクリックします。

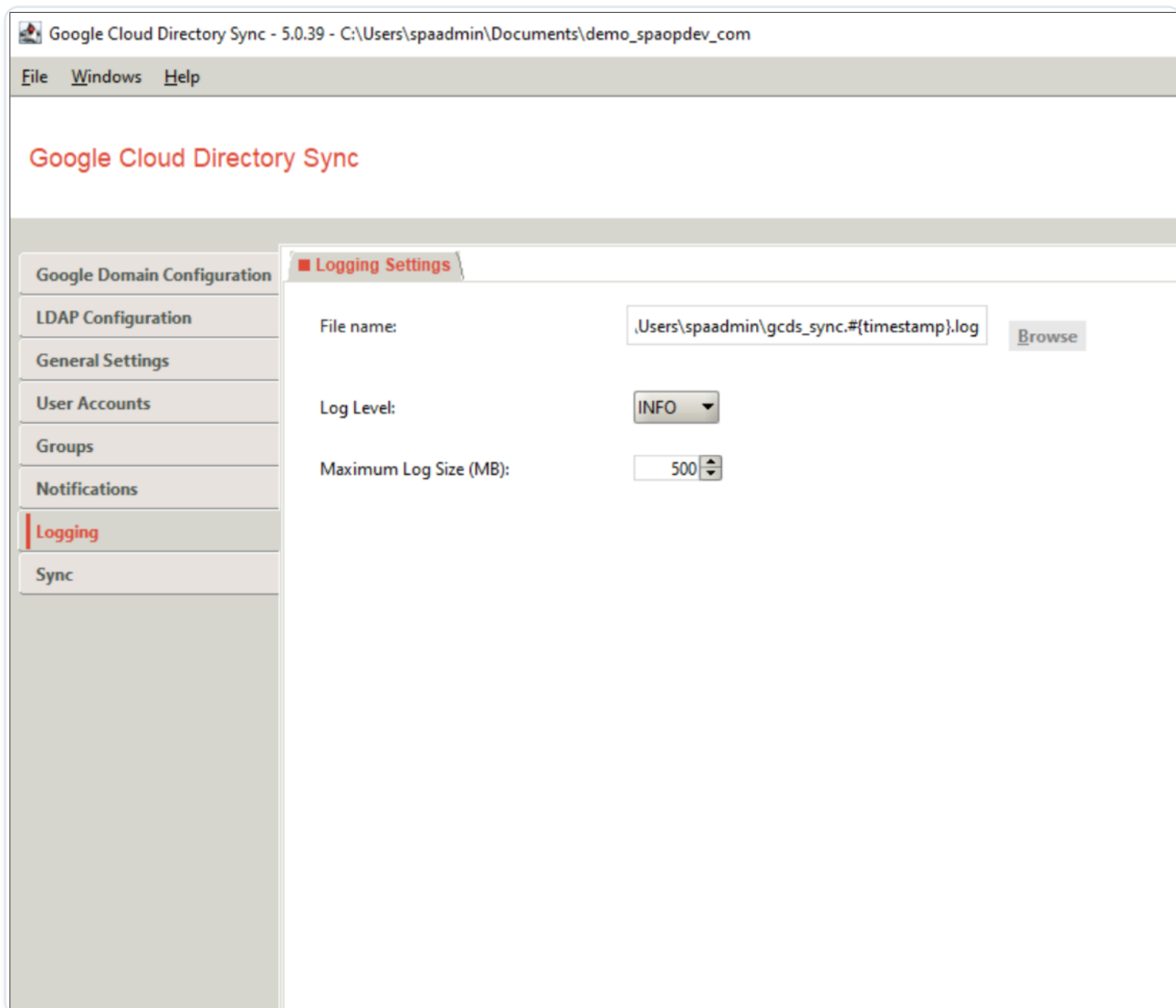
同期レポートが24 MBを超える場合、圧縮されてZIP添付ファイルとして送信されます。

The screenshot shows the 'Google Cloud Directory Sync - 5.0.39' application window. The title bar indicates the file path: 'C:\Users\spadmin\Documents\demo_spaopdev_com'. The menu bar includes 'File', 'Windows', and 'Help'. The main window has a sidebar with the following options: 'Google Domain Configuration', 'LDAP Configuration', 'General Settings', 'User Accounts', 'Groups', 'Notifications' (highlighted in red), 'Logging', and 'Sync'. The 'Notifications' tab is active, displaying the following settings:

- SMTP Relay Host:** smtp.demo.spaopdev.com
- ☒ **Use SMTP with TLS**
- User Name:** spaadmin@demo.spaopdev.com
- Password:** [Masked with dots]
- Subject Prefix:** [Empty field]
- From address:** spaadmin@demo.spaopdev.com
- To addresses (recipients):** A list containing 'spaadmin@demo.spaopdev.com'. To the right of the list are 'Add' and 'Remove' buttons.
- ☒ **Use attachment**
- ☒ **Compress attachment**
- Do not include in notifications:** [Empty field]
- Actions:** A section at the bottom with a 'Test Notification' button.

ログ:

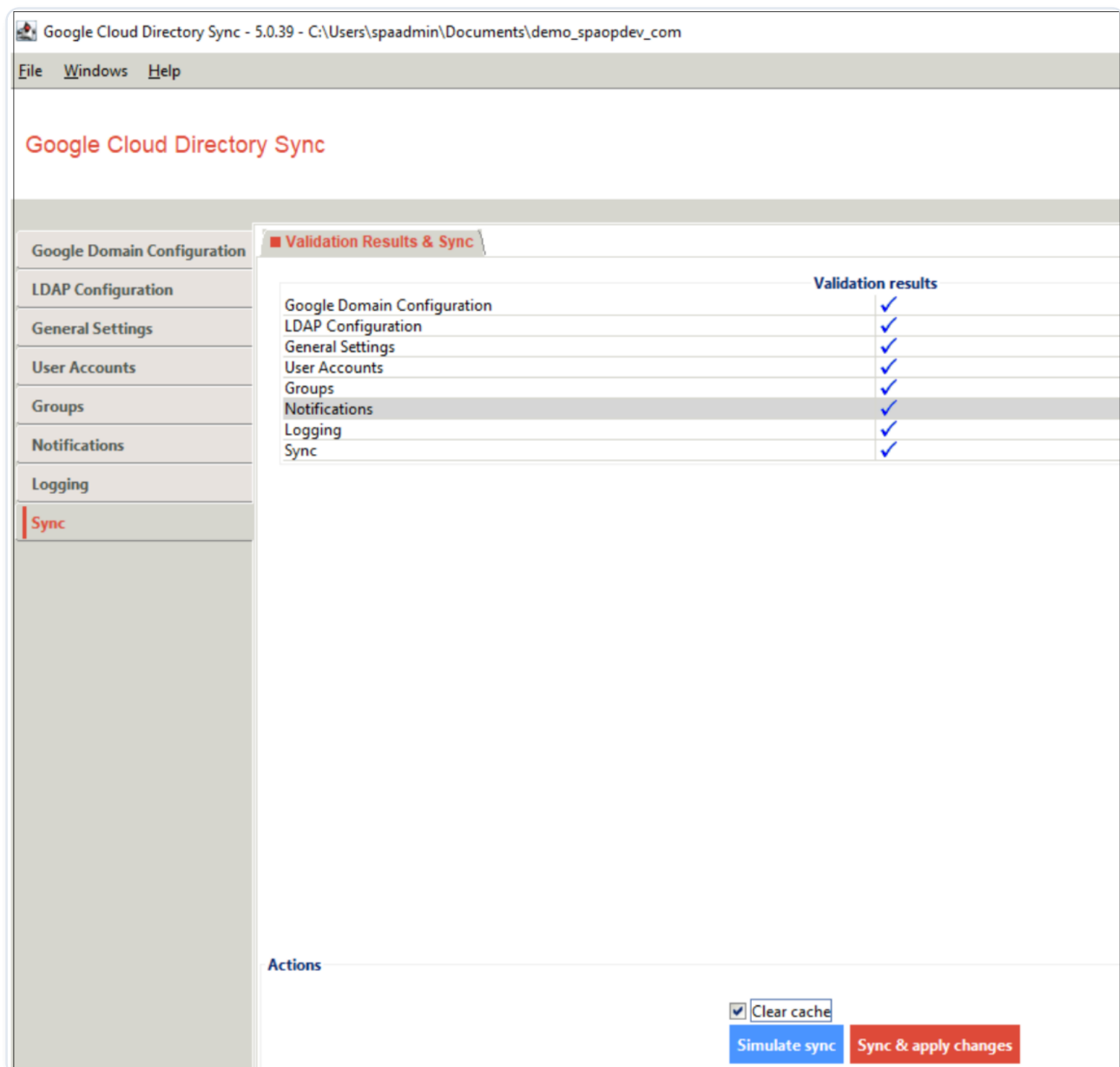
ログファイルの情報の書き込み先、詳細レベル、およびログファイルの最大サイズを指定します。



同期:

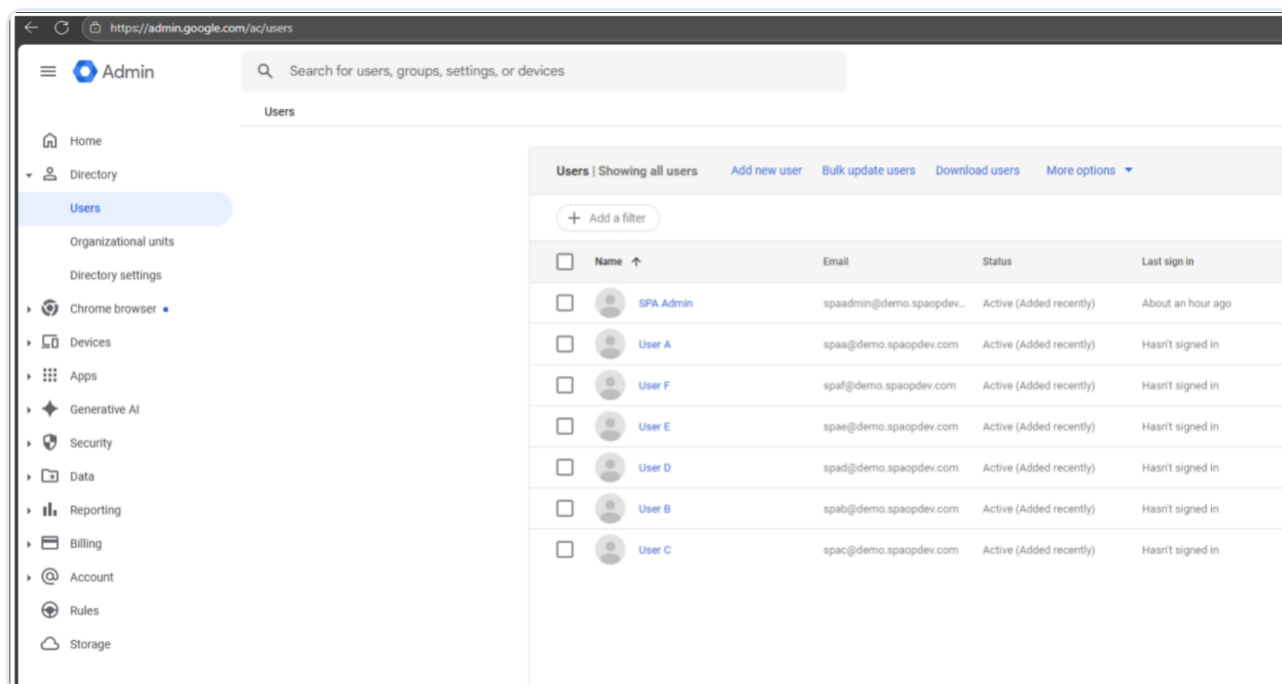
同期する前に、設定を確認し、問題があれば修正してください。

- 設定が正しいことを確認したら、**同期シミュレーション**をクリックして両方のサーバーに接続し、シミュレートされた同期の変更リストを生成します。
- 変更をコミットするには、構成ファイルを保存し、**同期**をクリックして変更を適用するか、コマンドラインから `sync-cmd` を実行します。



Google Workspace ディレクトリ:

新しいユーザーは同期中に作成されます。



CLI を使用して同期する:

「コマンドラインを使用した同期」を参照してください。

エンドユーザーエクスペリエンス

ユーザーは、以下の方法でSecure Private Accessを介してアプリケーションにアクセスできます。各アクセス方法は異なるユーザーエクスペリエンスを提供するため、組織は希望するユーザーエクスペリエンスと展開戦略に基づいて最適なアプローチを選択できます。

- **Citrix Workspace App** - 完全なポリシー適用とシングルサインオン機能を備え、最も安全で機能豊富なアクセスエクスペリエンスを提供するネイティブデスクトップアプリケーションです。
- **WebブラウザからのストアURL** - さまざまなブラウザ環境からアクセスできるWebベースのインターフェイスです。
 - Chrome以外のブラウザ（Firefox、Safari、Edgeなど）
 - 管理されていないプロファイルのChrome（エンタープライズポリシーのない個人のChromeブラウザ）
 - 管理されているプロファイルのChrome（Chrome Enterprise Premiumポリシーが適用されたエンタープライズ管理のChromeブラウザ）
- **Chrome管理プロファイル** - ユーザーは、ブックマークを使用するか、Chrome管理プロファイルのアドレスバーにアプリケーションURLを手動で入力することで、アプリケーションに直接アクセスします。

次の表は、さまざまな方法でアプリケーションにアクセスした場合のエンドユーザーエクスペリエンスをまとめたものです。

	直接	WEBブラウザからのストアURL	CITRIX WORKSPACEアプリ
Chrome以外のブラウザ	SaaSアプリへのアクセスは拒否されます（SaaSアプリが適切なIPアドレス許可リストで構成されていると仮定した場合）。	アプリはストアに列挙されます。	該当なし
	プライベートアプリに到達できません。	アプリケーションは、適切なChrome管理プロファイルで起動されます。	
		該当する管理プロファイルがまだ作成されていない場合、プロファイル作成ウィザードが起動されます。	
Chrome（非管理プロファイル）	SaaSアプリへのアクセスは拒否されました（SaaSアプリが適切なIPアドレス許可リストで構成されていると仮定した場合）。	アプリケーションは、適切なChrome管理プロファイルで起動されます。	該当なし
	プライベートアプリに到達できません。	対応する管理プロファイルがまだ作成されていない場合、プロファイル作成ウィザードが起動します。	

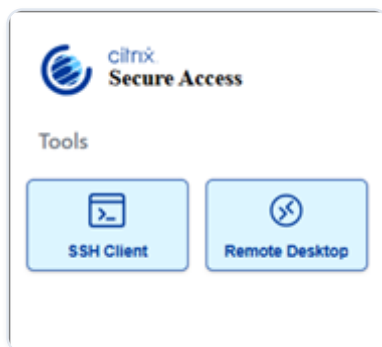
	直接	WEBブラウザからのストアURL	CITRIX WORKSPACEアプリ
Chrome (管理プロファイル)	アプリはSecure Private Accessの設定に応じて許可または拒否されます。	列挙されたアプリは新しいタブで起動されます。	該当なし
Citrix Workspaceアプリ	該当なし	該当なし	アプリはストアに列挙されます。
			アプリケーションは適切なChrome管理プロファイルで起動されます。
			該当する管理プロファイルがまだ作成されていない場合は、プロファイル作成ウィザードが起動します。

Chrome エンタープライズ プレミアム 用 シトリックス セキュア アクセス 拡張機能

Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能は、Chrome ブラウザから直接、内部および外部アプリケーションへの安全なクライアントレスアクセスを可能にします。これは、Citrix Secure Private Access と Chrome Enterprise の機能を組み合わせることで、エンタープライズグレードのセキュリティ、ゼロトラストアクセス、コンテキスト制御、および最新のユーザーエクスペリエンスを提供します。

組織は、この拡張機能を使用して、VPN やネイティブクライアントのインストールを必要とせずに、SaaS アプリケーション、内部 Web アプリ、SSH サーバー、および RDP システムへの安全なアクセスを提供できます。

Secure Access ブラウザ拡張機能は、Secure Private Access を Chrome Enterprise Premium と統合すると自動的にインストールされます。設定手順については、「[Google Chrome 統合のセットアップ](#)」を参照してください。インストール後、Chrome ブラウザの右上隅にあるアイコンから拡張機能にアクセスできます。

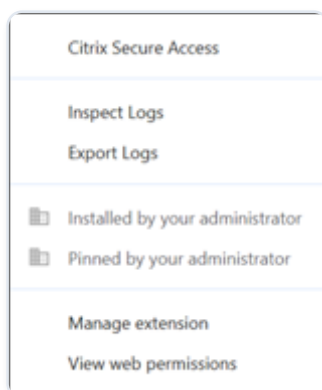


Secure Access 拡張機能ログ

Secure Access ブラウザ拡張機能のログは、監視とトラブルシューティングに不可欠です。エンドユーザーは、問題が発生したときに管理者やサポートチームと共有するために、ログを確認およびダウンロードできます。

ログを確認またはダウンロードするには：

1. ブラウザ拡張機能アイコンを右クリックします。
 - ログを確認するには、**ログの検査**をクリックします。
 - ログをダウンロードするには、**ログのエクスポート**をクリックします。



Chrome Enterprise 用 Citrix Secure Access コントロール

Citrix Secure Private Access は、Google Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能によって配信および適用されるセキュリティポリシーをサポートしています。詳細については、「サポートされているコントロール」を参照してください。

これらのポリシーは、Secure Private Access 管理コンソールから構成できます。

1. **ポリシー > ブラウザポリシー** に移動し、**ブラウザポリシーの作成** をクリックします。
2. ポリシーを選択し、**管理** をクリックします。

利用可能なコントロール(/en-us/citrix-secure-private-access/media/secure-access-controls.png)

3. ポリシーのルールを追加します。

キーロギング対策ルール(/en-us/citrix-secure-private-access/media/spa-browser-add-aki-rule.png)

4. ポリシーを評価する必要がある条件を選択します。

キーロギング対策ポリシーの条件(/en-us/citrix-secure-private-access/media/spa-browser-policy-condition.png)

Citrix Secure Accessブラウザポリシーは、Chrome Enterprise Premium (CEP) を使用したハイブリッドおよびサービススペースのSecure Private Access展開の両方でサポートされています。

詳細な設定手順については、各コントロールのドキュメントを参照してください。

サポートされているコントロール

Citrixは、Secure Private AccessとChrome Enterprise Premiumの統合により、以下のSecure Accessコントロールをサポートしています。

コントロール	機能
キーロギング対策(/ja-jp/citrix-secure-private-access/secure-access-extension/spa-cep-anti-keylogging.html)	キーストロークを難読化して、エンドポイント上のキーロガーマルウェアによるユーザー入力のキャプチャを防ぎます。
クリップボードコンテナ	ユーザーがブラウザと他のアプリ間でコピー＆ペーストできる内容を制御します。
DNSサフィックス	短い内部URL（「wiki/」など）を完全なアドレスに自動的に補完します。
セッション記録	監査およびコンプライアンスのためにブラウザセッションアクティビティを記録します。
ブラウザセッションの再認証	設定された時間間隔の後、ブラウザセッションの定期的な再認証を強制します。
SSH接続	ユーザーがターミナルクライアントを必要とせずに、ブラウザタブ内で直接SSH接続を確立できるようにします。

コントロール	機能
リモートデスクトップ (RDP)	ユーザーがRDPクライアントを必要とせずに、ブラウザタブ内で直接リモートデスクトップセッションを起動できるようにします。

ポリシー内のユーザーとグループ

以下のセクションでは、ユーザーとグループに関する詳細情報を提供します。

ユーザーまたはグループの検索

選択したユーザーとグループはグリッドに表示されます。グリッドの各行には、異なるドメイン、フォレスト、またはIDプロバイダー (IdP) 間で同じ名前のユーザーまたはグループを明確に区別できるように、次のID詳細が表示されます。

- **名前** – ユーザーまたはグループの表示名。
- **メール** – IDに関連付けられているメールアドレス。
- **IDPタイプ** – Azure AD、Active Directory、Okta、GoogleなどのIDプロバイダー。
- **OID** – IDのオブジェクトIDまたはセキュリティ識別子。
- **ドメイン** – ユーザーまたはグループが属するドメイン。

グリッドを名前でフィルタリングしたり、個々の行を削除したり、複数のエントリを選択して**選択を削除**を使用してまとめて削除したりできます。

同期されたユーザーとグループを使用する

ユーザーまたはグループを選択する際、管理者は、選択したユーザーディレクトリのエントリがGoogleディレクトリと同期され、正しく構成されているかを確認できます。Secure Private Accessポリシーは、同期されたユーザーとグループを使用している場合にのみ正しく評価されます。そうでない場合、次の警告が表示されることがあります。

- **テナントアカウントの権限がありません。**

修正: Google管理コンソールで、**ユーザー > 読み取り**および**グループ > 読み取り**の権限をテナントサービスアカウントに割り当てます。SPAは、ユーザーまたはグループが存在することを確認するためにこれらの権限を必要とします。

- **ユーザーまたはグループが同期されていません。**

修正: 検索または選択されたユーザーまたはグループは、Googleディレクトリと同期されていません。SPAポリシーで使用する前に、ディレクトリエンティティをGoogleディレクトリと同期してください。

- グループアクセス設定が不十分です。

修正: Google管理コンソールで、選択したグループのアクセス設定を開き、**メンバーを表示できるユーザー**が少なくとも**グループメンバーオプション**を選択していることを確認してください。

注:

この機能は、Google Chromeの統合が正常に完了した後にのみ利用可能です。

キーロギング対策制御

サイバー犯罪者は、キーロガーなどの悪意のあるソフトウェアを使用して、パスワード、クレジットカード番号、機密性の高い企業データなどの機密情報を盗みます。

Chrome Enterprise Premium (CEP) 用のCitrix Secure Accessブラウザ拡張機能は、データの保護に役立つキーロギング対策をサポートしています。この機能はキーストロークをスクランブル化するため、悪意のあるプログラムが入力された入力をキャプチャしようとしても、判読不能な文字のみが記録され、実際のテキストは安全に作業アプリケーションに配信されます。

サポートされている展開: Citrix Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows 11以降。

注:

ネイティブRDPセッションでは、キーロギング対策はサポートされていません。

前提条件

キーロギング対策を有効にする前に、次の前提条件が満たされていることを確認してください。

- CWAバージョン2603以降がインストールされていること。
- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。

キーロギング対策ポリシーを構成する

1. Secure Private Access管理コンソールにログインします。

2. **【ポリシー】 > 【ブラウザポリシー】** の順に選択し、**【ブラウザポリシーの作成】** をクリックします。
3. **【キーロギング対策】** を選択し、**【管理】** をクリックします。
4. **「ルールを追加」** をクリックして、ユーザーがアンチキーロギングを有効にするためのルールを追加します。
 - a. ルールの名前を入力し、**「次へ」** をクリックします。
 - b. ユーザーまたはグループなど、要件に基づいて条件を選択します。また、**「地理的位置」**、**「ネットワークの場所」**、**「デバイスの姿勢チェック」**などの条件を追加することもできます。
 - c. **「次へ」** をクリックします。
5. **「保存」** をクリックします。

アンチキーロギングポリシー用に構成されたルールのは、**「ブラウザポリシー > アンチキーロギング」** タブに表示されます。

クリップボードコンテナ制御

WebアクセスにChromeを、ネイティブアプリケーションにVDIを使用する展開では、クリップボードコンテナ機能を使用して、ブラウザとVDIセッション間のデータ共有を制御できます。クリップボードデータは、ローカルエンドポイントのクリップボードに書き込まれることなく、Citrixセッション間で直接転送されます。これにより、セキュリティが向上し、ユーザーは両方の環境で柔軟に作業できるようになります。

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows。

前提条件

以下の前提条件が満たされていることを確認してください。

- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。
- Citrix Workspaceアプリ 2603.10以降。
- 2607 LTSR以降を実行しているWindows VDA (Clipboard Sharing ScopeのGAバージョン)。詳細については、**「Clipboard Sharing Scope」** を参照してください。
- 2507 LTSRを実行しているWindows VDA (Clipboard Sharing Scopeのプレビューバージョン) では、以下を有効にします。

- **DaaSとのクロス・クリップボード・コンテナ機能**。詳細については、「[DaaSとのクロス・クリップボード・コンテナ](#)」を参照してください。この機能は現在、DaaSでプレビューとして利用可能です。
- **Clipboard Sharing Scope** レジストリ。詳細については、「[Clipboard Sharing Scope レジストリを有効にする](#)」を参照してください。

クリップボードコンテナ制御を有効にする

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. 「**Clipboard container**」を選択し、「**Manage**」をクリックします。
4. 「**Add Rule**」をクリックして、VDAとブラウザ間のクリップボード共有のルールを追加します。
 - a. ルールの名前を入力し、「**Next**」をクリックします。
 - b. ユーザーやグループなど、要件に基づいて条件を選択します。また、「**Geo-location**」、「**Network location**」、「**Device posture check**」などの条件を追加することもできます。
 - c. 「**Next**」をクリックします。
 - d. クリップボード共有を許可するURLとSecure Private Accessアプリケーションを定義します。
 - e. ポリシーのスコープを選択します。
 - **Apply to entire browser** — このポリシーは、管理対象プロファイル内のすべてのクリップボードアクティビティを管理します。
 - **特定のアプリケーションとURLに適用** — このポリシーは、選択されたアプリケーションと入力されたURL/ドメインパターンに限定されます。
 - **Select Application** — アプリケーションピッカーを使用して、特定の公開アプリケーションを選択します。
 - **URL or Domain** - 特定のアプリケーションのURLまたはドメインを入力します。

クリップボードコンテナアクション(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-action.png)

5. 「**Save**」をクリックします。

クリップボードコンテナポリシー用に構成されたルールのは数は、「**Browser Policies > Clipboard container**」タブに表示されます。

クリップボード共有スコープを有効にする

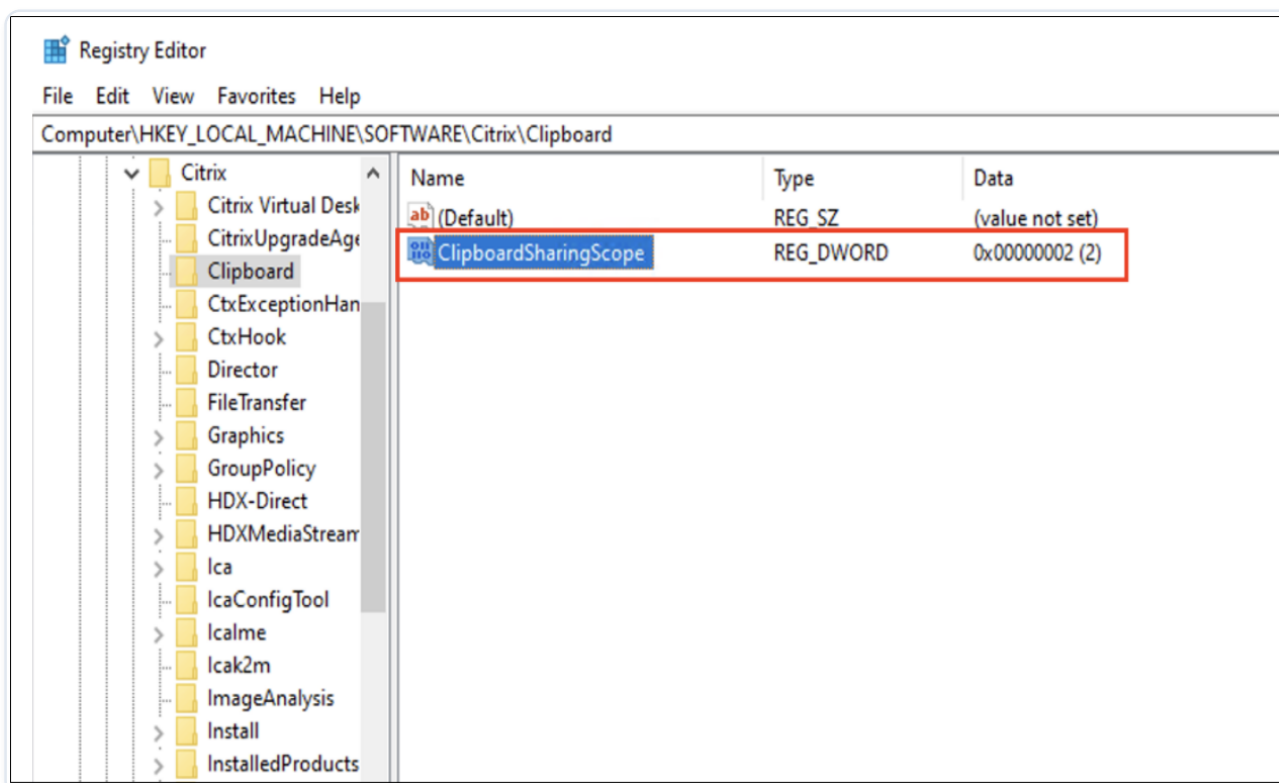
VDA バージョン 2607 の場合:

[仕組み](#)を参照してください。

VDA バージョン 2507 の場合:

この **Clipboard Sharing Scope** レジストリを有効にします。

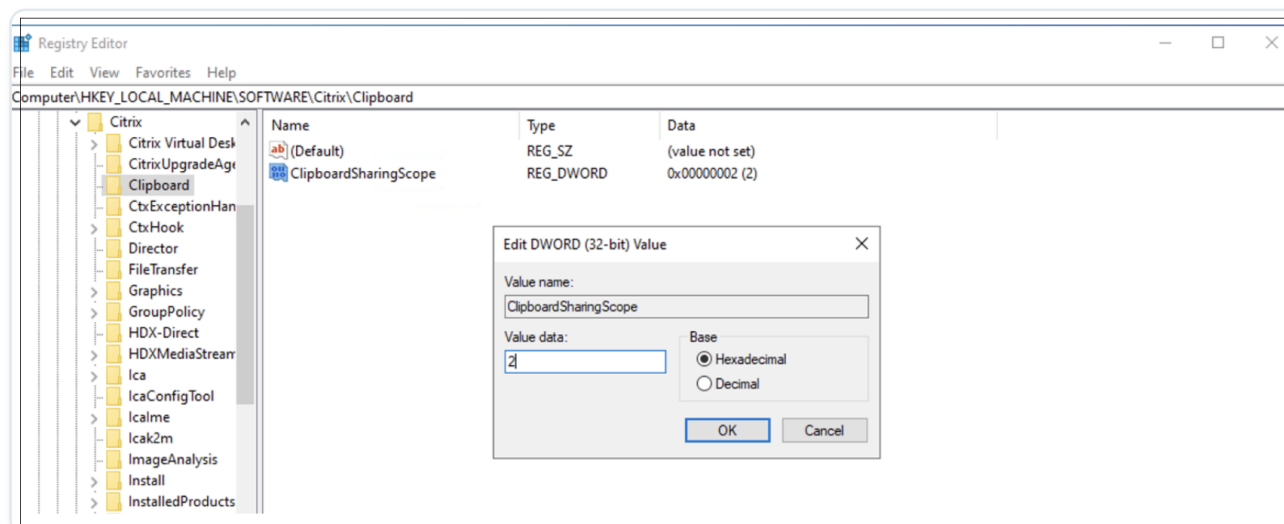
1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\ に移動します。
3. REG_DWORD 値を `ClipboardSharingScope` という名前で作成します。



`ClipboardSharingScope` ポリシーは、VDA クリップボードデータを共有できる場所を制御します。新しい DDC ポリシーが利用可能になるまで、この設定は上記のレジストリキーを使用して構成できます。

サポートされている値	スコープ	説明
0	無制限	クリップボードデータはクライアントシステムのクリップボードにコピーされ、クライアント、VDA、および CEP からアクセスできます。

サポートされている値	スコープ	説明
1	VDAのみ	クリップボードデータはVDAのみがアクセスできます。クライアントシステムのクリップボードとCEPはクリップボードコンテンツにアクセスできません。
2	CEPのみ	クリップボードデータはCEPのみがアクセスできます。クライアントシステムのクリップボードとVDAはクリップボードコンテンツにアクセスできません。
3	VDA と CEP	クリップボードデータはVDAとCEPの両方からアクセスできます。クライアントシステムのクリップボードはクリップボードコンテンツにアクセスできません。



注記：

- CEPのみ（2）およびVDAとCEP（3）モードは、CEP拡張機能のクリップボードコンテナ機能と連携するように設計されています。
- クリップボードコンテナポリシーが有効な場合、管理者によって構成されたURLのみがVDIとクリップボードデータを交換することを許可されます。

>- Content copied from the approved web applications can be pasted into the VDI.

>- Content copied from the VDI can be pasted only into administrator-configured, paste-allowed URLs.

>- If a user attempts to paste VDI clipboard content into a website that is not included in the policy, the paste operation is blocked and an error message appears.

Webアプリケーションのドメインサフィックス

ユーザーがブラウザに短い内部ホスト名（例: `sw` または `server001`）を入力するシナリオでは、ドメインサフィックス機能は、オペレーティングシステムのDNSサフィックス設定に依存するのではなく、ブラウザ管理のDNSサフィックスポリシーを使用して、DNSサフィックスを自動的に追加し、それらを完全修飾ドメイン名（FQDN）に変換します。

DNSサフィックス機能は、**Windows** と **macOS** の両プラットフォームでサポートされており、以下を含む一般的なURL入力形式全体に一貫して適用されます。

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

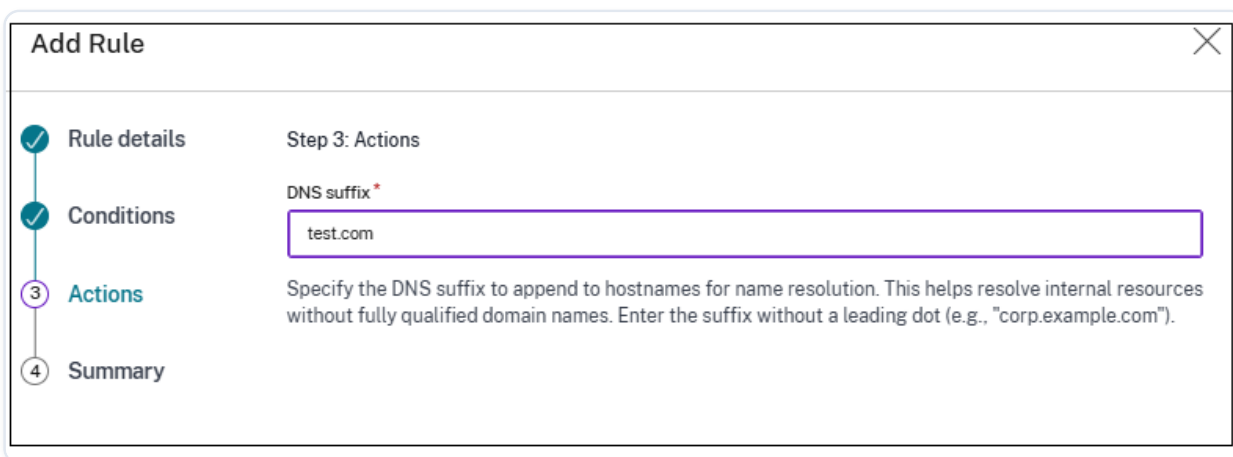
サポートされているプラットフォーム: WindowsおよびmacOS。

前提条件

Citrix Secure AccessとChrome Enterpriseの統合が構成されていることを確認してください。詳細については、「[Google Chrome Enterprise Premiumとの統合](#)」を参照してください。

DNSサフィックスの構成

1. Secure Private Access管理コンソールにログインします。
2. a. 「ポリシー > ブラウザポリシー」に移動し、「ブラウザポリシーの作成」をクリックします。
3. 「DNSサフィックス」を選択し、「管理」をクリックします。
4. 「ルールを追加」をクリックして、URLに追加するドメインのルールを追加します。
 - a. ルールの名前を入力し、「次へ」をクリックします。
 - b. ユーザーやグループなど、要件に基づいて条件を選択します。地理的位置、ネットワークの場所、デバイスの姿勢チェックなどの条件を追加することもできます。
 - c. 「次へ」をクリックします。
 - d. アクセス用に付加するドメインを定義します。



5. 「保存」をクリックします。

DNSサフィックスポリシーに設定されているルールのは数は、「ブラウザポリシー > DNSサフィックス」タブに表示されます。

セッション記録制御

セッション記録は、取得と再生のためにセッションを記録、カタログ化、アーカイブします。

セッション記録には、次の主要な利点があります。

- アプリケーションおよびデスクトップセッションの記録を自動的にトリガーするための柔軟なポリシーを提供します。
- IT担当者がユーザーアクティビティを監視および調査できるようにし、規制遵守およびセキュリティ監視のための内部統制をサポートします。
- 問題の特定を迅速化し、解決までの時間を短縮することで、テクニカルサポートを支援します。

詳細については、「メリット」(</ja-jp/session-recording/current-release.html#benefits>)を参照してください。

アーキテクチャ

セッション記録ソリューションは、次の3つのプレーンにまたがっています。

- 管理対象のChromeプロファイル、Citrix Secure Access拡張機能、およびエンドポイント用 Session Recording Agentを備えたエンドポイント。
- Secure Private AccessおよびSession Recordingクラウドサービスを収容するCitrix Cloudコントロールプレーン。
- NetScaler Gateway、STAサーバー、Session Recordingサーバー、およびそのデータベースと記録ストアを含む、顧客管理のリソースロケーション。

セッション記録アーキテクチャ(</en-us/citrix-secure-private-access/media/spa-cep-session-recording-architecture.png>)

前提条件

- Windows版 Citrix Workspaceアプリ 2603.10以降
- Endpoint analysis (EPA) バージョン: 26.5.1.7 以降

システム要件

- Citrix Secure Private Access（サービスモードまたはハイブリッドモードで展開され、Chrome Enterprise Premium（管理プロファイル付き）と組み合わせたもの）。
- Session Recording Cloud サービス（Session Recording サーバー 2511 以降を使用）。詳細については、[はじめに](#)を参照してください。
- 以下のコンポーネントを備えた Windows 64 ビットまたは 32 ビットのエンドポイント:
 - Citrix Endpoint Analysis (EPA) プラグイン 26.5.1.7 以降。
 - Session Recording Endpoint Agent がインストールされた Citrix Workspace app for Windows バージョン 2603.10 以降

環境をセットアップする

Chrome Enterprise セッションのエンドポイント記録を有効にして検証するには、次の手順を完了します。

Session Recording サイトを構成する

[エンドポイント記録ポリシーの構成](#)に記載されている手順に従ってください。

注:

エンドポイント記録には NetScaler Gateway が必要です。これは、Secure Private Access の両方の展開タイプで、STA を介して記録トラフィックを Session Recording Server にルーティングします。NetScaler がユーザーからアプリケーションへのアクセスを管理しない Secure Private Access サービスを使用している場合でも、記録トラフィック用のゲートウェイ URL を指定する必要があります。

Secure Private Access で Session Recording ブラウザポリシーを構成する

1. Secure Private Access 管理コンソールにログインします。
2. 「ポリシー > ブラウザポリシー」に移動し、「[ブラウザポリシーの作成](#)」をクリックします。
3. 「セッションレコーディング」を選択し、「管理」をクリックします。
4. 「ルールの追加」をクリックし、ルールの名前を入力して、「次へ」をクリックします。
5. 条件（ユーザーとグループ）を設定します。（オプション）「[地理的位置](#)」、「[ネットワークロケーション](#)」、「[デバイスポスチャチェック](#)」を追加し、「次へ」をクリックします。
6. 「保存」をクリックします。ルール数は「ブラウザポリシー > セッションレコーディング」タブに表示されます。

エンドポイント用のセッションレコーディングエージェント付きWorkspaceアプリをインストールする

[セッションレコーディングアドオンのサポート](#)に記載されている手順に従ってください。

記録されたセッションを再生する

記録はセッションレコーディングコンソールで表示できます。

- ユーザーのChromeワークプロファイルに関連付けられているすべてのウィンドウが記録されます。
- 1つまたは複数のモニターにまたがる複数のウィンドウが記録されます。

- フォーカスが外れているウィンドウや、他のアプリケーションによって隠されているウィンドウも、全体が記録されます。
- 最小化されたウィンドウや、画面キャプチャ防止が有効になっているウィンドウは、再生中に黒い四角として表示されます。

ベストプラクティス

- **グローバルサイトを1つ維持する。** 単一のグローバルエンドポイント記録サイトを使用し、その構成を文書化します。これを変更すると、他のサイトで構成されているポリシーが意図せず無効になる可能性があります。
- **リージョンを揃える。** 遅延やデータレジデンシーの問題を避けるため、セッションレコーディングクラウドサービスURL、クラウドクライアント、およびバックエンドを同じCitrix Cloudリージョンに保持します。
- **ストレージを計画する。** 全画面のWeb/SaaSレコーディングはストレージを大量に消費する可能性があります。それに応じてサーバー、セッションレコーディングデータベース、およびレコーディングストレージのサイズを決定し、ストレージ消費量を綿密に監視してください。
- **最初にエンタイトルメントとロールを検証する。** Citrix DaaSとCitrix Secure Private Accessのエンタイトルメントの不一致は、展開失敗の最も一般的な原因です。ポリシーを有効にする前に、単一のアクティブな顧客レコードが存在し、必要な管理ロールが割り当てられていることを確認してください。

ブラウザセッションの再認証制御

Citrix Secure Private Access を使用すると、管理者は Chrome Enterprise Premium (CEP) ブラウザセッションのセッションタイムアウトポリシーを適用できます。ユーザーは、ブラウザのアクティビティに関係なく、設定されたセッション期間が経過すると再認証を求められます。これにより、Google Chrome の仕事用プロファイルを介してアクセスされるアプリケーションのゼロトラストアクセス制御が強化されます。

セッションの有効期限が切れると、ユーザーはエンタープライズ資格情報と多要素認証 (MFA) を使用して再認証する必要があります。再認証が成功すると、最後にアクティブだったページが復元され、セッションタイマーが再開されます。

サポートされている展開: Secure Private Access サービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows、macOS、Linux、ChromeOS。

前提条件

次の前提条件が満たされていることを確認してください。

- Citrix Secure Access と Chrome Enterprise Premium (CEP) の統合が完了していること。

ブラウザセッションの再認証制御を有効にする

1. Secure Private Access 管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー** に移動し、**ブラウザポリシーの作成** をクリックします。
3. **ブラウザセッションの再認証** を選択し、**管理** をクリックします。
4. **ルールの追加** をクリックして、ブラウザセッションの再認証を有効にするルールを追加します。
 - a. ルールの名前を入力し、**次へ** をクリックします。
 - b. ユーザーやグループなど、要件に基づいて条件を選択します。**地理的位置、ネットワークの場所、デバイスの姿勢チェック**などの条件を追加することもできます。
 - c. **次へ** をクリックします。
 - d. 以下を構成します。
 - **再認証間隔**: ユーザーが再認証を求められるまでのブラウザセッションの期間。間隔は5分から14日の間で設定でき、分、時間、または日で構成できます。
 - **最初の警告バナー表示時間**: ブラウザセッションの有効期限が切れる前にユーザーに表示される、閉じることができる警告バナー。値は有効期限の5分から60分前に設定できます。残り2分になると2番目の警告バナーが表示され、セッション終了時にはセッション期限切れのオーバーレイが表示されます。
 - **IDプロバイダーのドメイン**: コンマ区切りの値として、IDプロバイダーの完全修飾ドメイン名 (FQDN)。1～25個のドメインを指定できます。認証フローが中断されないように、IdP ページではセッションバナーとブロックオーバーレイは非表示になります。古いセッションが完全に削除されるように、セッションの有効期限が切れるとこれらのドメインの Cookie はクリアされます。ワイルドカードがサポートされています (例: *.auth0.com)。

Add Rule

✓ Rule details

✓ Conditions

3 Actions

4 Summary

Step 3: Actions

Configure the reauthentication interval, when warning banners appear before session expiry, and which identity provider domains should be excluded from session expiry overlays.

Reauthentication interval

How long a browser session lasts before the end user is required to log back in (minimum 5 minutes, maximum 14 days).

24

hours

First warning banner time

A dismissible information banner shown to the end user before their browser session expires (minimum 5 minutes, maximum 60 minutes). A final warning banner appears at 2 minutes remaining (also dismissible), followed by the browser session expired overlay when the session ends.

30

minutes before logout

Identity provider domains

Enter the fully qualified domain names (FQDNs) of your identity providers as comma-separated values (minimum 1 domain, maximum 25 domains). IDP pages never show session banners or blocking overlays, even during session expiry. This ensures the authentication flow remains accessible. Cookies for these domains will also be cleared so the old session is fully removed. Wildcards are supported (such as *.auth0.com).

*.auth0.com

Cancel

Back

Next

5. **次へ**をクリックし、**保存**をクリックします。

クリップボードコンテナポリシー用に構成されたルール数は、**ブラウザポリシー > ブラウザセッションの再認証タブ**に表示されます。

SSH制御

Citrix Secure Private AccessはChrome Enterprise Premiumと統合されており、ブラウザ内で直接安全なSSHセッションを可能にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが効率化されます。

組織はSSHベースのシステムの安全なリモート管理を必要としています。スタンドアロンのSSHクライアントを使用する従来の方法では、エンドポイントを管理されていない環境に公開し、堅牢なデータ損失防止 (DLP) の実施が不足しているため、コンプライアンスが困難になるというリスクがあります。

SSHセッションは、スタンドアロンのSSHクライアントではなく、Chromeブラウザ内で起動されるようになりました。これにより、ローカルインストールへの依存が減り、コンプライアンスが向上します。

注:

- この機能は、ハイブリッドおよびクラウド展開向けのChrome Enterprise Premium統合 Secure Private Accessセットアップに適用されます。詳細については、以下のトピックを参照してください。
- Secure Private AccessおよびChrome Enterprise Premiumポリシーを構成するには、管理者権限が必要です。
- FreeBSDサーバーへの接続はサポートされていません。

この統合の利点

この統合には、次の主要な利点があります。

- **セキュリティの強化:** 管理されていないSSHクライアントへの依存を排除し、セキュリティリスクへの露出を減らします。
- **アクセスの簡素化:** ブラウザネイティブのアクセスを提供し、追加のソフトウェアインストールの必要性をなくします。
- **コンプライアンス:** ブラウザ内で直接企業のDLPポリシーを適用し、規制要件への準拠を支援します。
- **運用効率:** エンドポイント管理とクライアント展開に関連するITオーバーヘッドを削減します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **ヘルスケアキオスク:** ネイティブクライアントをインストールすることなく、デバイスのトラブルシューティングのために安全なSSHアクセスを可能にします。
- **IT管理:** 管理者は、DLPポリシーが適用された管理対象ChromeブラウザからLinuxサーバーに安全にアクセスできます。
- **請負業者アクセス:** 組織のセキュリティ体制を損なうことなく、サードパーティベンダーに一時的なSSHアクセスを提供します。

システム要件

お使いの環境が以下の要件を満たしていることを確認してください。

- Chrome Enterprise Premiumの最新バージョン。

- Citrix Secure Private Accessが統合用に構成されていること。
- SSHトラフィックを許可するためのアクセスポリシーは、Secure Private Access管理コンソールで作成する必要があります。

前提条件

SSHアプリケーションへのセキュアなアクセスを有効にするには、以下の前提条件が満たされていることを確認してください。

- Citrix Secure Private AccessがGoogle Chrome Enterprise Premium統合で構成されていること。詳細については、「[Google Chrome Enterprise Premiumとの統合](#)」を参照してください。
- エンドユーザーが、Citrix Secure Accessブラウザ拡張機能を備えた最新のGoogle Chromeブラウザをインストールしていること。
- 展開固有の前提条件については、以下のトピックを参照してください。
 - クラウド展開 - [Citrix Secure Private Accessの概要](#)
 - ハイブリッド展開 - [システム要件と前提条件](#)

SSHアクセス用にSecure Private Accessを構成する

1. Citrix Cloudにログインし、**Secure Private Access**をクリックします。
2. 管理コンソールで、**Applications > App Configuration**をクリックし、**Add an app**をクリックします。
3. Configure the SSH app as a TCP/UDP app within Secure Private Access.
 - アプリは、サーバーの正確なIPアドレス、範囲、FQDN、またはホスト名を持つことができます。
 - SSHは、デフォルトポートおよび非デフォルトポートでサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDPアプリの作成の詳細については、次のトピックを参照してください。

- クラウド展開 - [TCP/UDPアプリのサポート](#)
- ハイブリッド展開 - [TCP/UDPアプリのサポート](#)

SSHポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **Policies > Browser Policies**に移動し、**Create browser policy**をクリックします。

3. **SSH**を選択し、**Manage**をクリックします。
4. 「**ルールを追加**」をクリックして、ユーザーがSSHを有効にするためのルールを追加します。
5. ルールの名前を入力し、「**次へ**」をクリックします。
6. ユーザーやグループなど、要件に基づいて条件を選択します。1. **地理的位置、ネットワークロケーション、デバイスの姿勢チェック**などの条件も追加できます。
7. 「**次へ**」をクリックします。
8. 「**保存**」をクリックします。

アンチキーロギングポリシー用に構成されたルールのは、**「ブラウザポリシー > SSH」** タブに表示されます。

リモートデスクトップ制御

Citrix Secure Private AccessはChrome Enterprise Premiumと統合されており、ブラウザ内で直接セキュアなRDPセッションを可能にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが効率化されます。

従来のリモートデスクトップアクセスは、多くの場合、ネイティブのRDPクライアントに依存していますが、これらは通常、ブラウザベースのDLP適用機能が不足しています。この欠点は、特に管理されていない環境においてセキュリティリスクを高め、コンプライアンスを困難にする可能性があります。組織は、これらの懸念に対処する、セキュアで準拠した簡素化されたリモートアクセスソリューションを必要としています。

この統合により、管理者はクリップボード制御やスクリーンショット防止などのエンタープライズグレードのDLP制御を適用できます。

注:

- この機能は、ハイブリッドおよびクラウド展開向けのChrome Enterprise Premium統合 Secure Private Accessセットアップに適用されます。詳細については、以下のトピックを参照してください。
- Secure Private AccessおよびChrome Enterprise Premiumポリシーを構成するには、管理者権限が必要です。

サポートされていない機能:

以下の機能はサポートされていません。

- クリップボード共有
- オーディオ/Webカメラ/スマートカード/USBリダイレクト
- 2要素認証および生体認証

この統合の利点

この統合には、以下の主要な利点があります。

- **セキュリティ:** きめ細かなDLPポリシーを適用することで、リモートセッション中のデータ漏洩を防ぎます。
- **コンプライアンス:** 堅牢なセキュリティ制御により、機密性の高い環境における規制要件への対応を支援します。
- **使いやすさ:** 個別のRDPクライアントをインストールする必要がなくなり、ユーザーアクセスと展開が簡素化されます。
- **柔軟性:** 管理対象のChromeブラウザからのセキュアなRDPアクセスをサポートし、一貫性のあるセキュアなエクスペリエンスを提供します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **企業請負業者:** 内部セキュリティを損なうことなく、サードパーティベンダーにセキュアなリモートデスクトップアクセスを提供します。
- **医療スタッフ:** 医療現場のキオスクや共有ワークステーションからWindowsシステムへのセキュアなアクセスを可能にします。
- **ITサポート:** IT担当者が追加のソフトウェアインストールを必要とせずにリモートデスクトップのトラブルシューティングを行うことができます。

システム要件

お使いの環境が以下の要件を満たしていることを確認してください。

- Chrome Enterprise Premiumの最新バージョン。
- Citrix Secure Private Accessが統合用に構成されていること。
- RDPトラフィックを許可するアクセスポリシーは、Secure Private Access管理コンソールで作成する必要があります。

前提条件

RDPアプリケーションへのセキュアなアクセスを有効にするために、以下の前提条件が満たされていることを確認してください。

- Citrix Secure Private Access は Google Chrome Enterprise Premium と統合するように構成されています。詳細については、「[Google Chrome Enterprise Premium との統合](#)」を参照してください。
- エンドユーザーは、Citrix Secure Access ブラウザ拡張機能を備えた最新の Google Chrome ブラウザをインストールしています。
- 展開固有の前提条件については、次のトピックを参照してください。
 - クラウド展開 - [Citrix Secure Private Access の概要](#)
 - ハイブリッド展開 – [システム要件と前提条件](#)

RDP アクセス用に Secure Private Access を構成する

1. Citrix Cloud にログインし、**Secure Private Access** をクリックします。
2. 管理コンソールで、**アプリケーション > アプリ構成** をクリックし、**アプリの追加** をクリックします。
3. RDP アプリを Secure Private Access 内の TCP/UDP アプリとして構成します。
 - アプリは、正確な IP アドレスまたは範囲、FQDN、またはサーバーのホスト名を持つことができます。
 - RDP は、デフォルトポートと非デフォルトポートの両方でサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDP アプリの作成に関する詳細については、次のトピックを参照してください。

- クラウド展開 - [TCP/UDP アプリのサポート](#)
- ハイブリッド展開 – [TCP/UDP アプリのサポート](#)

リモートデスクトップポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー** に移動し、**ブラウザポリシーの作成** をクリックします。
3. **リモートデスクトップ** を選択し、**管理** をクリックします。
4. **ルールの追加** をクリックして、ユーザーがリモートデスクトップを有効にするためのルールを追加します。

5. ルールの名前を入力し、**次へ** をクリックします。
6. ユーザーやグループなど、要件に基づいて条件を選択します。1. **地理的位置、ネットワークロケーション、デバイスポスチャチェック** などの条件を追加することもできます。
7. **次へ** をクリックします。
8. **保存** をクリックします。

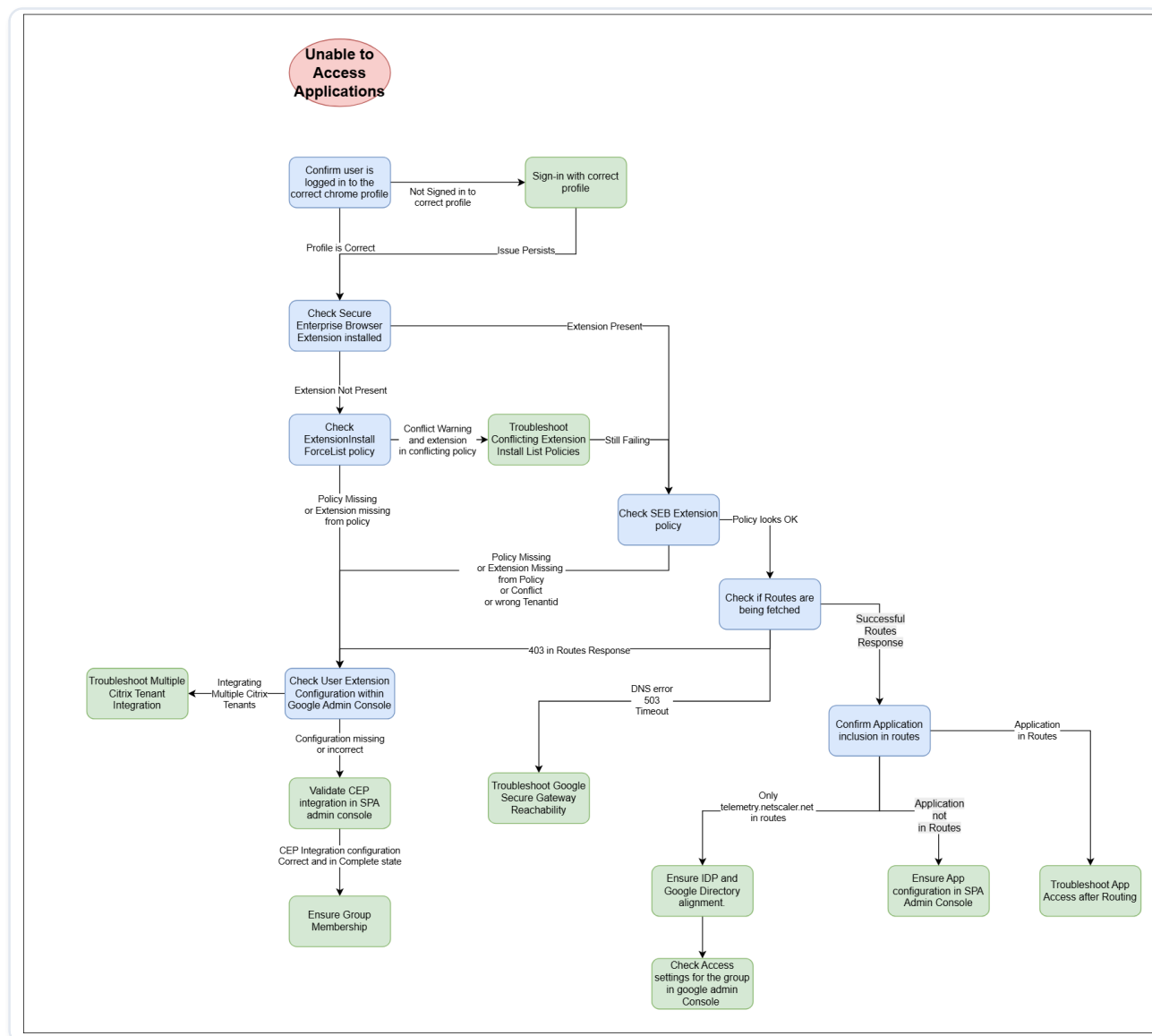
アンチキーロギングポリシー用に構成されたルールのは数は、**ブラウザポリシー > リモートデスクトップ** タブに表示されます。

CEP統合の問題のトラブルシューティング

この記事では、Citrix Secure Private Access と Chrome Enterprise Premium (CEP) の統合を完了したがアプリケーションにアクセスできない顧客管理者向けのトラブルシューティングワークフローを提供します。

基本的な前提条件:

- 顧客管理者は、Google Directory とのディレクトリ同期を完了していること。
- 顧客は、Secure Private Access で Chrome Enterprise のオンボーディングを正常に完了していること。
- Secure Private Access 管理コンソールで、ユーザーまたはユーザーが属するグループに対して関連するアプリケーションへのアクセスを許可するように、アプリケーションとアクセスポリシーが構成されていること。
- ユーザーがオンボーディングされたドメインにログインしていること。
- ブラウザがインターネットに接続されていること。



CEPトラブルシューティング用の診断ログ

調査を効率化するために、サポートケースを開く前に以下の診断情報を収集し、すべての提出物に含めてください。

1. Chromeポリシーをエクスポートします。
 - a. Chromeを開き、chrome://policy/ に移動します。
 - b. その他の操作をクリックし、次に**JSON**にエクスポートを選択します。
 - c. エクスポートされたファイルをサポートケースに添付します。
2. Secure Enterprise Browser 拡張機能の詳細ログを有効にします。
 - a. Secure Enterprise Browser 拡張機能の横にある省略記号アイコンをクリックします。
 - b. オプションをクリックし、**ログレベル**を**すべて**に設定します。

- c. Chrome を閉じて再度開きます。
 - d. 拡張機能のオプション（省略記号アイコン）に戻り、**ログをダウンロード**をクリックします。
3. 拡張機能のログを収集します。
- a. Chrome を閉じて再度開きます。
 - b. 手順2を繰り返して**拡張機能**オプションにアクセスし、**ログをダウンロード**をクリックします。
 - c. ダウンロードしたファイルをサポートケースに添付します。
4. ネットワークログをキャプチャします。
- a. Chrome で `chrome://net-export/` に移動し、**ディスクへのログ記録を開始**をクリックします（デフォルトのファイル名は `chrome-net-export-log.json` です）。
 - b. いくつかのSaaSおよびWebアプリケーションにアクセスし、`chrome://net-export/` に戻って**ログ記録を停止**をクリックします。
 - c. 結果のファイルをサポートケースに添付します。

ユーザーが正しいChromeプロファイルにログインしていることを確認します

確認方法: Chromeブラウザの右上隅にあるプロフィールアイコンをクリックします。アプリケーションにアクセスしようとしているプロファイルの正しいユーザーと正しいドメインが表示されている必要があります。

また、プロファイルが**一時停止**または**サインインするにはクリック**と表示されていないことを確認してください。表示されている場合は、再認証する必要があります。

- **プロファイルが正しく認証されている場合:** [Secure Enterprise Browser拡張機能がインストールされているか確認する](#)に進みます。
- **プロファイルが正しくないか、認証されていない場合:** 正しいプロファイルでログインまたは再認証してください。ユーザーのメールのドメインサフィックスが、Secure Private AccessがインストールされているGoogle管理アカウントのドメインと一致していることを確認してください。

Secure Enterprise Browser拡張機能がインストールされているか確認する

確認方法: Chromeブラウザの右上隅に、Secure Enterprise Browser拡張機能に対応する緑色の盾のアイコンがあるはずです。すべての拡張機能を表示するには、ジグソーパズルのピースをクリックする必要があるかもしれません。

- 拡張機能が存在する場合: [Secure Enterprise Browser拡張機能ポリシー](#)を確認するに進みます。
- 拡張機能が存在しない場合: [ExtensionInstallForcelist](#)ポリシーを確認するに進みます。

ExtensionInstallForcelistポリシーを確認する

確認方法: <chrome://policy>に移動し、**Chrome**ポリシーの下で**ExtensionInstallForcelist**という名前のポリシーを探します。対応する行の末尾にある[詳細を表示](#)をクリックして、ポリシーの詳細を確認します。

この強制リスト内に、ID: `ekajlcmdfcigmdbphhifahdfjbkciflj` の拡張機能が表示されるはずです。これはSecure Enterprise Browser拡張機能に対応します。

2つの競合するポリシーがあることを示唆する警告が表示される可能性があります。

- 競合の警告があり、競合するポリシーに拡張機能がある場合: [競合する拡張機能インストールリストポリシーのトラブルシューティング](#)に進みます。
- ポリシーがない場合: ポリシーが完全に存在しない場合、ユーザーがSecure Enterprise Browserを使用するように構成されていないことを示唆しており、[Google管理コンソール](#)内で[ユーザー拡張機能の構成を確認](#)する必要があります。
- ポリシーから拡張機能が欠落している場合: [Google管理コンソール](#)内で[ユーザー拡張機能の構成を確認](#)に進みます。

競合する拡張機能インストールリストポリシーのトラブルシューティング

競合するポリシーがあることは、必ずしもSecure Private AccessでCEPをサポートする上での障害となるわけではありません。ただし、有効なポリシーは以下の3つの拡張機能のインストールを強制する必要があります。

- セキュアエンタープライズブラウザ (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- Citrix セキュアアクセス (`loifegnemklkgbmonigcdkmniboiegl`)
- エンドポイント検証 (`callobklhcbilhphincmohgkigmfocg`)

Secure Private Accessの拡張機能ポリシーの競合を解決するには、[Chrome Policy Hierarchy Guide](#)に基づいて以下の手順に従ってください。

1. **競合の特定:** `chrome://policy` に移動します。 **ExtensionInstallForcelist** を見つけて、**Status** と **Source** を確認します。
2. **優先順位の分析:** マシンレベルのポリシー (GPO) は、通常、クラウド/ユーザーレベルのポリシーよりも優先されることに注意してください。
3. **調和:** 最も優先順位の高いポリシーに、必要な3つの拡張機能IDすべてが含まれていることを確認します（追加の拡張機能が含まれていても問題ありません）。あるいは、ブラウザとプロファイルが同じGoogle Workspace組織によって管理されている場合は、ポリシーマージ機能を使用できます。
4. **確認:** **Reload policies** をクリックします。 **Applies to** と **Level** の列で、必要な拡張機能が **Mandatory** であり、有効なレベルでアクティブであることを確認する必要があります。

拡張機能のインストールリストポリシーを修正しても問題が解決しない場合は、[Secure Enterprise Browser拡張機能ポリシーの確認](#)に進んでください。

Secure Enterprise Browser拡張機能ポリシーの確認

確認方法: `chrome://policy` に移動し、**Secure Enterprise Browser** の下にある **securityGateway** という名前のポリシーを探します。 **Show More** をクリックして、完全なポリシー構成を表示します。その値は次の形式であると予想されます。

```
{
  "authentication": {},
  "context": {
    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"
  },
  "externalHelper": {
    "id": "com.citrix.device_posture_context_provider",
    "metadata": {
```

```
    "action": "device/metadata",  
  
    "input": [  
  
        {  
  
            "key": "tenantId",  
  
            "stringValue": "<tenant_id>"  
  
        }  
  
    ]  
  
    }  
  
    },  
  
    ...  
  
}
```

`tenant_id` フィールドに、Citrix CloudテナントIDに対応する値があることを確認してください。この値が異なる場合、2番目のテナントがこのGoogleアカウントと統合するように構成されている可能性があります。

- **ポリシーがないか空の場合:** ポリシーが完全に存在しない場合、Secure Enterprise Browser拡張機能がSecure Private Accessだけでなく顧客によっても構成されており、ユーザーが以前または手動の構成から空の拡張機能構成を取得していることを示唆しています。[Google管理コンソール内でユーザー拡張機能構成を確認](#)する必要があります。
- **ポリシーに誤ったCitrixテナントIDが入力されている場合:** ポリシーは存在するが、その値が例と一致しない場合、テナントIDが異なるか、2つの競合するポリシーが存在します。[Google管理コンソール内でユーザー拡張機能構成を確認](#)に進んでください。
- **ポリシーが正しい場合:** ルートがフェッチされているか確認するに進みます。

Google 管理コンソール内でユーザー拡張機能の設定を確認する

確認方法: <https://admin.google.com>に移動します。ここから、**Chrome ブラウザ > アプリと拡張機能**に移動します。このビュー内で、適用されているすべてのポリシー構成を見つける必要があります。

「概要」タブ（存在する場合）をクリックし、「Secure Enterprise Browser」アプリを選択します。左側の「インストールポリシー」の下には、「\<primary domain\>に強制インストールされ、固定されています」と表示されている必要があります。ここで、\<primary domain\>は Google 管理コンソールの最上位組織部門に対応します。

拡張機能の展開設定を確認するためにクリックすると、拡張機能のポリシー構成を探します。これは、Secure Enterprise Browser 拡張機能のポリシーを確認するセクションで説明されている内容と一致している必要があります。

- **単一のポリシーが正しいように見える場合:** 親 OU のポリシーが正しいように見える場合、テストしているユーザーが該当するアカウントに属していること、およびサブ OU またはグループレベルで親 OU のポリシーを上書きする可能性のある他の構成がないことを確認する必要があります。メンバーシップが確認されて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。
- **ポリシーが見つからない場合:** ポリシーが完全に存在しない場合、この Google アカウントは Secure Enterprise Browser を使用するように構成されていないことを示唆しており、Secure Private Access 管理コンソールで CEP 統合を検証する必要があります。
- **複数のポリシー - 複数の Citrix アカウント:** Secure Enterprise Browser 拡張機能に複数の構成が表示される場合、これは関連するポリシーの構成が正しくない原因である可能性があります。複数の Citrix アカウントを同じ Google アカウントに関連付けることは禁止されていますが、統合が機能しない原因となる可能性があります。
- **複数のポリシー - 単一の Citrix アカウント:** Citrix テナントを 1 つだけ統合している場合、組織内の他の管理機能がこの拡張機能を構成していないことを確認する必要があります。この拡張機能のポリシー構成を提供している人が他にいないと確信している場合は、Secure Private Access 管理コンソールを通じて統合した Citrix テナントに対応しないポリシー構成を削除することができます。

不要な拡張機能の構成を削除し、ブラウザを再起動してもアプリケーションにアクセスできない場合は、Citrix サポートにお問い合わせください。

ルートがフェッチされているか確認する

確認方法: chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj に移動するか、Secure Enterprise Browser 拡張機能を右クリックしてオプションを選択します。

ログレベルを**ALL**に設定し、**SHOW LOG**をクリックします。ログが表示されたら、ブラウザを閉じて、ログページに移動するプロセスを繰り返します。これにより、トラブルシューティングに必要なすべてのログが取得されていることを確認できます。

ログ内で、次の内容を含むログ行を検索します。

```
Calling 'https://api.prod.securegateway.goog/api/v1/routes'
```

これに続いて、次のような応答があるはずです。

```
[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime:  
'2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog', ...}
```

- **コンテキストルートがログに403ステータスコードを表示する:** この403は、Zscaler、Umbrellaなどの傍受ファイアウォールによって返される可能性があります。
 - この場合、Google Security Gateway宛てのトラフィックが、[統合ソリューションの前提条件](#)に従って許可されていることを確認してください。
 - そうでない場合、ユーザープロファイルに認証の問題がある可能性があります、Secure Private AccessとCEPの統合が不完全であることを示唆している可能性があります。[Secure Private Access管理コンソール](#)でCEP統合を検証するに進んでください。
- **コンテキストルートがタイムアウト、DNSエラー、または503エラーを表示する:** [Google Secure Gatewayの到達可能性のトラブルシューティング](#)に進んでください。
- **コンテキストルートが成功したと表示される (200 OK):** [ルートへのアプリケーションの組み込みを確認する](#)に進んでください。

Secure Private Access管理コンソールでCEP統合を検証する

Citrix CloudコンソールのSecure Private Access内にある「**ブラウザ設定**」セクションにアクセスします。

このセクションで、以下を確認します。

- **Google Chrome統合ステータス**が「完了」と表示されている必要があります。失敗している場合は、[ドキュメント](#)に従ってCEP統合の前提条件を完了していることを確認し、再試行してください。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。
- **顧客ID**は、統合しているGoogleアカウントに対応する値である必要があります。この値は、Google管理コンソールの「**アカウント > アカウント設定**」で確認できます。

上記のすべての値が正しいにもかかわらず、Chromeブラウザで正しい拡張機能構成が取得できない場合は、Citrixサポートにお問い合わせください。

Google Secure Gatewayの到達可能性のトラブルシューティング

確認方法: URL `https://api.prod.securegateway.goog/api/v1/routes` をコピーし、ブラウザのアドレスバーでこのURLにアクセスします。HTTP 401エラー応答が表示されるはずですが、これは予期される動作であり、Google Secure Gatewayへのネットワーク接続が正常に確立できることを示しています。

- **DNS解決エラー:** これは、貴社がGoogle Security Gateway FQDNのルックアップを妨げるような、制限的なDNS解決設定を導入している可能性があることを示唆しています。しかし、これはこの機能を使用するための前提条件であり、該当するFQDNは解決可能である必要があります。
- **リクエストがハングするか、タイムアウトエラーページが表示される:** これは、ブラウザとインターネット間のファイアウォールが、Google Security Gateway宛てのトラフィックを破棄している可能性が高いことを強く示唆しています。ネットワークから前提条件となるインターネットロケーションに到達できることを確認するには、[統合ソリューションの前提条件](#)に従ってください。

正しいルートがまだ受信されない場合は、Citrixサポートにお問い合わせください。

ルートへのアプリケーションの組み込みを確認する

正常なルート応答には、Secure Private Access管理者によって構成されたアプリケーションに対応するFQDNが含まれます。例:

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime: '2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog', endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'}, {hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname: 'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}
```

この行に、アクセスしようとしているアプリケーションが含まれていますか？

- **アクセスできないアプリケーションがルート応答に含まれている:** [ルーティングされたアプリケーションアクセスをトラブルシューティングする](#)に進んでください。
- **ルート応答にtelemetry.netscalergateway.netのみが含まれている:** 追加のアプリケーションと包括的なアプリケーションポリシーを構成してみてください。ルートにまだ表示されない場合は、グループメンバーシップの問題、またはCitrixで構成されたIdPとGoogle Directory間のグループの不一致が強く示唆されます。[IdPとGoogle Directoryの整合性を確保する](#)に進んでください。

- **アクセスできないアプリケーションがルート応答に含まれていない:** これは、Secure Private Access管理コンソールでアプリケーションが正しく構成されていないことを示唆しています。アプリケーションが存在し、ポリシー（アクセスを許可または拒否するいずれか）が関連付けられていることを確認してください。アプリケーションが構成されていると確信しているにもかかわらず、以前のルートにまだ表示されない場合は、Citrixサポートにお問い合わせください。

ルーティングされたアプリケーションアクセスのトラブルシューティング

（ルートリストに表示される）アプリケーションにアクセスしようとする、どのような動作が観察されますか？

- **ドメイン解決エラー (ERR_NAME_NOT_FOUND) が発生する**

これは、アプリケーションが正しく構成されていないか、コンテキストルートが正しく受信されていない可能性が高いことを示唆しています。

- **「アクセス拒否」と表示されたクリーム色のページ**

これは、Secure Private Accessコンソールでのポリシー構成が、現在のユーザーを含めるように構成されていないことを示唆しています。

- **「おっと！何か問題が発生しました。」と表示されるクリーム色のページ**

このエラーページが表示される最も一般的な原因は、コネクタがターゲットアプリケーションに到達できないことです。この場合、Citrixのドキュメントに従って、内部アプリケーションへのコネクタアクセスをトラブルシューティングしてください。一般的な問題は次のとおりです。

- 内部DNSの到達可能性
- バックエンドサービスが停止している
- ファイアウォールルール

- **大きな赤いフォントで「Service Unavailable」と表示される白いページ**

これは一時的なエラーである可能性があり、数分後に解決する場合があります。

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。

- **タイムアウト**

- まず、Chromeのアドレスバーに `via.prod.securegateway.goog` を入力して、到達可能であることを確認します。401応答を受信する必要があります。タイムアウトする場合は、

中間ファイアウォールまたはプロキシがアクセスをブロックしており、アプリケーションにアクセスする前に解決する必要があります。

- 。アプリケーションのタイムアウトのもう1つの潜在的な原因は、インターネット、特に Google Security Gatewayへのトラフィックをブロックするファイアウォールです。これは、顧客がインターネットに到達するために明示的なプロキシを必要とするシナリオで一般的です。Chrome Enterprise PremiumとのSecure Private Access統合は、このプロキシ構成をサポートしていません。

• 証明書エラー

アプリケーションがプライベートCA証明書を使用している可能性があり、そのためブラウザが「信頼されていない証明書エラー」をスローする場合があります。Chrome Enterprise Premiumの設定を通じて、顧客は信頼されたルートCAをブラウザにプッシュできます。詳細については、「[Chrome Enterprise Premiumを使用してルート証明書構成を管理する](#)」を参照してください。

IdPとGoogleディレクトリの整合性を確保する

Chrome Enterprise PremiumとのSecure Private Access統合の場合、ディレクトリをGoogleディレクトリに同期するには、[統合ソリューションの前提条件](#)で説明されているいくつかの仕様に従う必要があります。

ユーザーとユーザーグループのメールが正しく、ソースディレクトリで構成されている内容と一致している場合は、[Google 管理コンソールでグループのアクセス設定を確認する](#)に進みます。

Google 管理コンソールでグループのアクセス設定を確認する

Google 管理コンソールで、ディレクトリ > グループに移動し、アクセス ポリシーを構成したグループ、およびアプリケーションがロードされないグループを選択します。

そこから、[アクセス設定](#)を選択し、メンバーを表示できるユーザーの行でグループメンバーオプションが有効になっていることを確認します。この構成は、Secure Private Access でポリシーを作成するすべてのグループに適用する必要があります。

このオプションがすでに有効になっている場合は、Citrix サポートにお問い合わせください。

CEP統合に関する既知の問題

Secure Private AccessとChrome Enterprise Premiumの統合には、以下の既知の問題があります。

Secure Private Accessユーザーインターフェイス

- **問題:** セッションポリシーの設定では、3つの条件が利用可能であるにもかかわらず、現在、ユーザーは2つのシミュレート条件しか追加できません。これにより、ポリシー作成の柔軟性が制限されます。

回避策: 2つの個別のセッションポリシーを作成します。1つは2つのシミュレート条件を含むもの、もう1つは残りの条件を含むポリシーです。

- **問題:** TCP/UDPのサーバーからクライアントへの構成オプションは、現在、すべての顧客環境のアプリケーション構成UIでは利用できません。これにより、サーバーからクライアントへのトラフィック動作を定義する機能が制限されます。

適応型アクセス ポリシーの構成

- **問題:** ルールでOktaグループが指定されている場合、アクセスポリシーの作成に失敗します。この問題は、Oktaディレクトリに存在するグループにのみ影響します。

回避策: OktaをIDプロバイダーとして使用できますが、ディレクトリとしては使用できません。OktaをIdPとして使用するには、まずオンプレミスのADをOktaと統合する必要があります。詳細については、「[OktaをCitrix CloudへのIDプロバイダーとして接続する](#)」を参照してください。

Google Chromeブラウザ

- **問題:** Googleプロフィールピッカーが開いていて、既存のプロファイルがない状態でユーザーがCWAまたはChrome以外のブラウザからアプリを起動しようとすると、プロフィール作成ワークフローがトリガーされません。

回避策: プロファイルピッカーを閉じて、アプリを再起動します。

- **問題:** 管理対象のChromeプロファイルでCWAにログインし、アプリを起動しても、プロフィール作成後にユーザーが元の内部アプリURLに移動しない。

回避策: プロファイル作成後、アプリを再起動する。

- **問題:** Google管理コンソールからグループを同期しても、グループに属するユーザーは自動的に同期されない。同期中に `whoCanViewGroupMembership` 設定が明示的に `ALL_MANAGERS_CAN_VIEW` に上書きされるため、表示が制限されるのは想定内である。

回避策: Google管理コンソールでGoogleグループの権限を手動で更新するか、API経由で更新する。詳細については、[URL](https://developers.google.com/workspace/admin/groups-settings/manage)を参照してください。

- **問題:** 管理対象のChromeプロファイルを通じて公開されたSaaS/Webアプリケーションにアクセスする際、プロキシのポップアップを介してユーザー名とパスワードによる認証を求められる。これは通常、一定期間の非アクティブ状態の後に発生する。

原因:

- プロキシトークンが利用できないか、プロキシトークンは利用可能だがその後期限切れになった。
- 遅延初期化のため、SEB拡張機能の再初期化が必要である。

回避策: 新しいウィンドウでChromeセッションを再起動する。

- **問題:** 管理対象のChromeプロファイルまたはCitrix Workspaceアプリを介して外部SaaSアプリケーションにアクセスする際、ユーザーは断続的に「Service Unavailable」エラーを経験する可能性がある。この問題は、Googleのインフラストラクチャにおける未解決のバックエンドの問題が原因である。

回避策: サポートについてはGoogleチームに問い合わせる。

アプリの構成と管理

Citrix Secure Private Access は、さまざまなアプリケーション (SaaS/Web および TCP/UDP) へのアクセスを構成および管理するための、ユーザーフレンドリーな集中型プラットフォームを提供します。Secure Private Access コンソールは、さまざまな構成タスクを単一の制御ポイントで提供することで、管理を簡素化します。構成ウィザードを使用すると、管理者は同じコンソール内で、アダプティブ認証のセットアップ、アプリケーションの構成、ユーザー権限を制御するアクセスポリシーの定義、機密データを保護するためのセキュリティ制限の実装を簡単に行うことができます。さらに、Secure Private Access は、VPN クライアントをインストールすることなく、エンタープライズ Web アプリへのエージェントレス アクセスをサポートします。

詳細については、以下のトピックを参照してください。

- [エンタープライズ Web アプリケーションまたは SaaS アプリケーションを構成する](#)
- [TCP/UDP アプリを構成する](#)
- [TCP/UDP - サーバーからクライアントへのアプリを構成する](#)

エンタープライズ Web アプリケーションまたは SaaS アプリケーションを構成する

Secure Private Access を設定した後、管理コンソールからアプリとアクセスポリシーを構成できます。

1. 管理コンソールで、[アプリ](#) をクリックします。
2. [アプリ](#) をクリックします。
3. アプリケーションが配置されている場所を選択します。
 - 外部アプリケーションの場合は、[外部アプリケーション](#)。
 - 内部アプリケーションの場合は、[内部アプリケーション](#)。
4. セクションに以下の詳細を入力し、[アプリ](#) をクリックします。
 - [アプリの種類](#) - アプリケーションの種類を選択します。

注:

Chrome Enterprise Premium (CEP) では、HTTPSエンタープライズWebアプリケーションとSaaSアプリケーションのみがサポートされています。HTTPエンタープライズWebアプリケーションとSaaSアプリケーションはサポートされていません。

- – アプリケーションの名前。
- - アプリケーションの簡単な説明。この説明は、ユーザーのストアに表示されます。アプリケーションのキーワードを `KEYWORDS: <keyword_name>` の形式で入力することもできます。キーワードを使用してアプリケーションをフィルタリングできます。
- - 公開するアプリケーションがストアUIに表示されるカテゴリとサブカテゴリ名 (該当する場合) を追加します。各アプリケーションに新しいカテゴリを追加することも、ストアUIの既存のカテゴリを使用することもできます。WebアプリケーションまたはSaaSアプリケーションのカテゴリを指定すると、そのアプリケーションはストアUIの特定のカテゴリの下に表示されます。
 - カテゴリ/サブカテゴリは管理者によって構成可能であり、管理者はすべてのアプリケーションに新しいカテゴリを追加できます。
 - カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。例えば、ビジネスと生産性\エンジニアリングのように指定します。また、このフィールドは大文字と小文字を区別します。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。ストア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リストされます。

例えば、「アプリカテゴリ」フィールドに「Business and Productivity」カテゴリを誤って「Business And productivity」と入力した場合、「Business And Productivity」カテゴリに加えて、「Business and productivity」という新しいカテゴリがストアUIに表示されます。
- **アプリのアイコン** – アプリのアイコンを変更するには、**アイコンの変更**をクリックします。アイコンファイルのサイズは128x128ピクセルである必要があり、ICOおよびPNG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** - アプリをユーザーに表示したくない場合は、このオプションを選択します。
- **URL** – アプリケーションのURL。

- **関連ドメイン** – 関連ドメインは、アプリケーションのURLに基づいて自動入力されます。管理者は、関連する内部または外部ドメインを追加できます。

注：

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

- **アプリケーションをお気に入りに追加（自動）** – このオプションをクリックすると、Citrix Workspaceアプリでお気に入りアプリとして追加されます。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に南京錠付きの星アイコンが表示されます。
 - **ユーザーがお気に入りにから削除することを許可** – このオプションをクリックすると、アプリのサブスクライバーがCitrix Workspaceアプリのお気に入りにアプリリストからアプリを削除できるようになります。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に黄色の星アイコンが表示されます。
 - **ユーザーがお気に入りにから削除することを許可しない** – このオプションをクリックすると、サブスクライバーがCitrix Workspaceアプリのお気に入りにアプリリストからアプリを削除できなくなります。

Secure Private Accessコンソールからお気に入りにしてマークされたアプリを削除した場合、これらのアプリは、ストアのお気に入りにリストから手動で削除する必要があります。Secure Private Accessコンソールからアプリが削除されても、ストアからアプリが自動的に削除されることはありません。

- **アプリの接続** - Webアプリの場合は**内部**を、SaaSアプリの場合は**外部**を選択します。

5. 保存をクリックし、次に完了をクリックします。

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

アプリケーション削除時のルーティングエントリの自動クリーンアップ

アプリケーションを構成すると、その宛先（FQDNまたはアプリケーションドメイン）がルーティングテーブルに追加され、Secure Private Accessはルーティングの決定にそれを使用します。アプリケーションを削除すると、Secure Private Accessは次のルールに基づいてルーティングエントリをクリーンアップします。

- **参照されていないエントリは削除されます** - 削除されたアプリケーションに関連付けられているルーティングエントリ（FQDNまたはアプリケーションドメイン）が他のどのアプリケーションからも参照されていない場合、Secure Private Accessはルーティングテーブルから自動的に削除します。
- **共有エントリは保持されます** - ルーティングエントリが複数のアプリケーションで使用されている場合、それらのアプリケーションの1つを削除しても、共有エントリは削除されません。エントリは、少なくとも1つのアクティブなアプリケーションがそれを参照している限り、ルーティングテーブルに残ります。
- **遡及的な削除はありません** - ルーティングエントリは、アプリケーションの削除の一部としてのみ評価および削除されます。既存のエントリは、どのアプリケーションにも使用されていないことが確認されない限り、遡及的に削除されることはありません。

注:

- アプリケーションがアプリケーションページから削除されると（省略記号 (...) メニューを使用して）、クリーンアップは自動的に実行されます。管理者の操作は必要ありません。
- 共有ルーティングエントリは保持されるため、アプリケーションを削除しても、同じ宛先を共有する他のアプリケーションへのアクセスが中断されることはありません。

次のステップ

アプリケーションのアクセスポリシーを構成する。

HARファイルを使用して関連ドメインを検出する

Secure Private Accessを使用すると、HTTPアーカイブ (HAR) ファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できます。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加するドメインを選択できます。これにより、関連ドメインを手動で特定して構成する必要がなくなるため、アプリケーションのオンボーディングが簡素化されます。

以前は、管理者はアプリケーションの関連ドメインをすべて事前に把握しているか、ユーザーがブロックされたURLにアクセスしたときに事後的に検出する必要がありました。構成されていないURLはすべてデフォルトでブロックされるため、この事後的なアプローチはユーザーエクスペリエンスの低下につながります。Secure Private Accessには、アプリケーション内の内部URLまたは埋め込みURLを識別する方法がありませんでした。

例

プライマリドメインが `example.com` であるアプリケーションを構成しているとします。アプリケーションの使用、ブラウザはいくつかの追加ドメインにもアクセスします。例:

- `api.example.com` – アプリケーションのバックエンドAPIコールを処理します。
- `auth.example.com` – サインインと認証を管理します。
- `cdn.example.com` – 画像、スクリプト、スタイルシートなどの静的コンテンツを提供します。
- `login.microsoftonline.com` – サードパーティのID認証を提供します。
- `player.vimeo.com` – 埋め込みビデオコンテンツをロードします。

これらの各ドメインを手動で識別する代わりに:

1. アプリケーションの使用中にHARファイルをキャプチャします。
2. HARファイルをSecure Private Accessにインポートします。
3. Secure Private Accessによって検出されたドメインを確認します。たとえば、インポートによって、必要な `api.example.com`、`auth.example.com`、および `cdn.example.com` が、除外を選択できる `player.vimeo.com` などのドメインとともに表示される場合があります。
4. アプリケーションに必要なドメインを選択します。
5. 必要に応じてルーティングとリソースの場所を構成します。

これにより、アプリケーション接続に必要なドメインをより迅速に特定し、構成できます。

前提条件

WebまたはSaaSアプリケーションにアクセスしている間にHARファイルをキャプチャしたことを確認してください。HARファイルにはネットワーク要求情報が含まれている必要があり、サイズは50 MB以下である必要があります。

HARファイルのインポート

1. Secure Private Access管理ポータルで、構成するWebまたはSaaSアプリケーションを開きます。
2. **アプリ接続**に移動し、**HARのインポート**をクリックします。

アプリ接続セクションのHARインポートオプション(/en-us/citrix-secure-private-access/media/har-import-button.png)

3. HARファイルをインポートウィンドウにドラッグアンドドロップするか、デバイスからファイルを選択します。
4. Secure Private AccessはHARファイルを分析し、ネットワーク要求から識別されたドメインを表示します。

インポートされたHARファイルから検出されたドメイン(/en-us/citrix-secure-private-access/media/har-discovered-domains.png)

5. 検出されたドメインを確認します。
6. アプリケーションに追加するドメインを選択します。
7. **インポート**を選択します。

選択したドメインは、アプリケーションの**関連ドメイン**構成に追加されます。

「関連ドメイン」テーブルに表示されるインポート済みドメイン(/en-us/citrix-secure-private-access/media/har-related-domains-table.png)

注:

インポートする前に、検出されたドメインを確認してください。HARファイルには、アプリケーションの接続に必要なドメインが含まれている場合があります。

関連ドメインの管理

ドメインをインポートした後、**関連ドメイン**テーブルから管理できます。

- **ドメインの検索** – 検索フィールドを使用してテーブルをフィルタリングし、特定のドメインをすばやく見つけます。
- **ドメインの選択** – 個々のドメインを選択するか、テーブルヘッダーのチェックボックスを使用して複数のドメインを選択します。この選択により、複数のドメインに対して同時にアクションを実行できます。
- **ドメイン構成の編集** – ルーティングタイプ、プライマリリソースロケーション、セカンダリリソースロケーションなど、関連ドメインの構成を更新します。
- **ドメインの一括編集** – 複数の対象ドメインを選択し、ルーティングとリソースロケーションの設定を同時に更新します。一括編集は、該当する内部ドメインで利用できます。外部ドメインでは、すべての構成オプションがサポートされていない場合があります。
- **リソースロケーション** – 関連ドメインを構成する際、プライマリリソースロケーションと、該当する場合はセカンダリリソースロケーションを割り当てます。これらの設定を使用して、Secure Private Accessが関連ドメインのトラフィックをどのようにルーティングするか、および接続を提供するためにどのリソースロケーションが使用されるかを定義します。

検証とファイルの要件

HARインポート機能は、アップロードされたファイルを処理する前に検証します。

- ネットワーク要求エントリを含む有効なHARファイルのみをインポートできます。
- サポートされる最大ファイルサイズは**50 MB**です。
- ドメインは、HARファイル内のURLから自動的に抽出されます。
- 重複するドメインは自動的に削除されます。
- ドメインは、関連ドメイン構成に追加される前に正規化されます。

TCP/UDPアプリを構成する

TCP/UDPアプリを構成する前に、[システム要件](#)を参照してください。

管理コンソールからTCP/UDPアプリを構成するには、次の手順を実行します。

1. 管理コンソールで、[TCP/UDPアプリ](#) をクリックし、次に [新規TCP/UDPアプリ](#) をクリックします。
2. 場所として [データセンター](#) を選択します。
3. 次の詳細を入力します。
 - – データセンターにあるバックエンドサーバーとの接続を開始するには、[データセンター](#) を選択します。
 - – アプリケーションの名前。

- – 追加するアプリの説明。このフィールドはオプションです。
- – データセンターにあるバックエンドマシンのIPアドレスまたはFQDN。1つ以上の宛先を次のように指定できます。
 - **IPv4アドレス**
 - **IPアドレス範囲** – 例: 10.68.90.10-10.68.90.99
 - – 例: 10.106.90.0/24
 - – 単一またはワイルドカードドメイン。例: ex.destination.domain.com, *.domain.com

注:

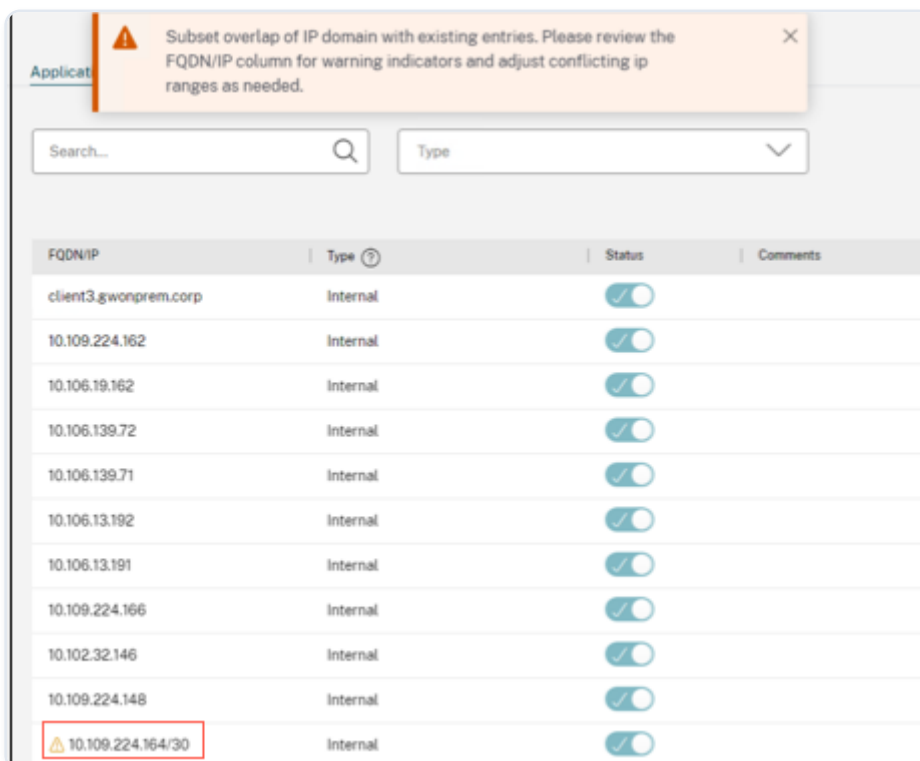
- エンドユーザーは、管理者がIPアドレスを使用してアプリを設定した場合でも、FQDNを使用してアプリにアクセスできます。これは、Citrix Secure Access™クライアントがFQDNを実際のIPアドレスに解決できるためです。

次の表は、さまざまな宛先の例と、これらの宛先でアプリにアクセスする方法を示しています。

宛先入力	アプリへのアクセス方法
10.10.10.1-10.10.10.100	エンドユーザーは、この範囲内のIPアドレスを介してのみアプリにアクセスすることが想定されています。
10.10.10.0/24	エンドユーザーは、IP CIDRで構成されたIPアドレスを介してのみアプリにアクセスすることが想定されています。
10.10.10.101	エンドユーザーは、10.10.10.101を介してのみアプリにアクセスすることが想定されています。
*.info.citrix.com	エンドユーザーは、info.citrix.comのサブドメイン、およびinfo.citrix.com (親ドメイン) にもアクセスすることが想定されています。例: info.citrix.com, sub1.info.citrix.com, level1.sub1.info.citrix.com 注: ワイ

宛先入力	アプリへのアクセス方法
	ルドカードは常にドメインの先頭文字である必要があります、* は1つのみ許可されます。
info.citrix.com	エンドユーザーは <code>info.citrix.com</code> のみにアクセスすることが想定されており、サブドメインにはアクセスできません。例えば、 <code>sub1.info.citrix.com</code> にはアクセスできません。

宛先IPアドレスは、リソースロケーション全体で一意である必要があります。競合する構成が存在する場合、アプリケーションドメインテーブル（設定 > アプリケーションドメイン）の特定のIPアドレスの横に警告記号が表示されます。



- **ポート** – アプリが実行されている宛先ポート。管理者は、宛先ごとに複数のポートまたはポート範囲を構成できます。

次の表に、宛先に構成できるポートの例を示します。

ポート入力	説明
*	デフォルトでは、ポートフィールドは <code>"*"</code> (任意のポート) に設定されています。宛先

ポート入力	説明
	では、1から65535までのポート番号がサポートされています。
1300–2400	宛先では、1300から2400までのポート番号がサポートされています。
38389	宛先では、ポート番号38389のみがサポートされています。
22,345,5678	宛先では、ポート22、345、5678がサポートされています。
1300–2400, 42000-43000,22,443	宛先では、ポート番号の範囲1300から2400、42000から43000、およびポート22と443がサポートされています。

注記:

ワイルドカードポート (*) は、ポート番号または範囲と共存できません。

- **プロトコル** – TCP/UDP

4. アプリ接続: アプリケーションのトラフィックをどのようにルーティングするかを定義します。

- **内部:** DNS解決はリモートDNSサーバー経由で行われます。

デフォルトでは、**内部**としてマークされたドメインへのすべてのトラフィックは、NetScaler Gatewayを介して傍受され、トンネルされます。たとえば、`.example.net` の接続が**内部**に設定されている場合、その関連ドメイン/サブドメイン（例: `code.example.net`、`test.example.net`、`123.example.net`）のすべてがNetScaler Gatewayを介して傍受され、トンネルされます。

- **外部:** DNS解決はローカルDNSサーバー経由で行われます。

関連ドメイン/サブドメインが**外部**としてマークされている場合、そのドメインへのトラフィックはNetScaler Gatewayを介して傍受されず、トンネルされません。たとえば、`code.example.net` への接続が**外部**に設定されている場合、このドメインへのトラフィックはインターネット経由で直接ルーティングされ、サブドメイン（例:

`text.example.net` および `123.example.net`) へのトラフィックはNetScaler Gatewayを介してトンネルされます。

5. 必要に応じて追加の宛先またはサーバーを追加するには、**追加**をクリックします。
6. **保存**をクリックします。アプリは**アプリ構成**ページに追加されます。アプリケーションを構成した後、**アプリケーション**ページからアプリを編集または削除できます。そのためには、アプリと同じ行にある省略記号ボタンをクリックし、必要に応じてアクションを選択します。

- アプリケーションの編集
- 削除

次のステップ

アプリケーションのアクセスポリシーを構成する。

TCP/UDP の構成 - サーバーからクライアントアプリへ

「TCP/UDP - サーバーからクライアントへ」アプリタイプは、以下の機能をサポートするために使用できます。

- Microsoft Endpoint Configuration Manager または類似のソリューションを使用したソフトウェア配布
- GPO Push を使用した管理対象デバイスのリモートポリシー更新
- ユーザーワークステーションのトラブルシューティングとデバッグのためのリモートアシスタンス。

前提条件:

- Secure Private Access のセットアップが完了していること。
- クライアントバージョンが以下の要件を満たしていること。
 - Windows - 24.6.1.18 以降
 - macOS - 24.06.2 以降
- イン트라ネット IP アドレスが NetScaler® Gateway で構成され、対応する VPN 仮想サーバーにバインドされていること。以下のサンプルコマンドを参照してください。

```
set vpn sessionAction ns_default_vpn_session_profile_spa_tcp_udp_apps -useMIP  
NS -useIIP NOSPILOVER
```

(オプションで、ユーザーは `-useMIP NS -useIIP NOSPILLOVER` を使用して VPN セッションプロファイルとセッションアクションを作成できます)

VPN仮想サーバー `<spa vserver name>` をイントラネットIP `<IP address>` にバインドします。

管理コンソールから TCP/UDP アプリを構成するには、以下の手順を実行します。

1. 管理コンソールで、アプリケーションをクリックし、アプリの追加をクリックします。
2. 場所として社内ネットワーク内を選択します。
3. 次の詳細を入力します。

- **アプリの種類** – TCP/UDP - サーバーからクライアントを選択します。
- **アプリ名** – アプリケーションの名前。
- **アプリの説明** – 追加するアプリの説明。このフィールドはオプションです。
- **サーバー** - クライアントとの接続を確立することを許可されているアプリケーションサーバーの詳細。IPアドレス、IPアドレス範囲、またはCIDRを入力できます。
- **ポート** – クライアントのポート番号。
- **プロトコル** – TCP/UDP。

4. **追加**をクリックして、追加のサーバーを追加します。
5. **保存**をクリックします。アプリが**アプリ構成**ページに追加されます。アプリケーションを構成した後、**アプリケーション**ページからアプリを編集または削除できます。そのためには、アプリと同じ行にある省略記号ボタンをクリックし、それに応じてアクションを選択します。

- **アプリケーションの編集**
- **削除**

重要:

サーバーとクライアント間の通信用にアプリを追加した後、NetScaler Gatewayで構成されたイントラネットIPアドレス範囲をTCP/UDPアプリとして追加して、サーバーとクライアント間およびクライアントとクライアント間の通信を有効にする必要があります。

イントラネットIPアドレス(/en-us/citrix-secure-private-access/media/spaop-tcp-upd-intranet-ip-app.png)

アプリケーションを編集する

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

次のステップ

アプリケーションのアクセスポリシーを構成する(/ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-configure-access-policies.html)。

アクセス ポリシーの構成と管理

今日の絶えず変化する状況において、アプリケーションセキュリティはあらゆるビジネスにとって不可欠です。コンテキストを認識したセキュリティ決定を行い、アプリケーションへのアクセスを有効にすることで、関連するリスクを軽減しつつ、ユーザーへのアクセスを可能にします。

Citrix Secure Private Access™ のアダプティブアクセス機能は、アプリケーションへのセキュアなアクセスを提供する包括的なゼロトラストアクセスアプローチを提供します。アダプティブアクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリに対して、きめ細かなレベルのアクセスを提供できます。

Secure Private Access 内のアクセス ポリシーを使用すると、ユーザーまたはユーザーのデバイスのコンテキストに基づいて、アプリへのアクセスを有効または無効にできます。

詳細については、以下のトピックを参照してください。

- [アプリケーションのアクセス ポリシーを構成する](#)
- [ポリシー条件](#)
- [セッション ポリシーを構成する](#)
- [デバイス証明書の登録](#)

アプリケーションのアクセスポリシーを構成する

Secure Private Access の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のデバイスのコンテキストに基づいて、アプリへのアクセスを有効または無効にできます。

アクセス制限は、Secure Private Access インターフェイス内ではなく、Google 管理コンソールを通じて構成する必要があります。

ルールは、**Google 管理コンソール > ルール** で構成されます。これらのルールは、透かしの追加、社会保障番号を含むファイルのダウンロードのブロック、URL フィルタリングなど、DLP に関連する高度な設定です。

Google 管理コンソールで Google Chrome のポリシーとルールを作成する方法の詳細については、次のトピックを参照してください。

- [Chrome Enterprise の Chrome Enterprise コネクタポリシーを設定する](#)

- [データ保護ルール](#)

アクセスポリシーを構成する

1. 管理コンソールで、 をクリックします。
2. をクリックします。
3. ページで、次のいずれかを選択します。

アプリケーションアクセスルールは、アクセスポリシーでの選択に基づいて、ユーザーまたはマシンのコンテキストに基づいて適用されます。

Always On 接続を有効にするには、 を選択できます。Always On 接続の場合、デバイス証明書が登録されている必要があります。詳細については、[デバイス証明書の登録構成](#) を参照してください。

マシン トンネルの詳細については、「[Always On VPN before Windows Logon](#)」を参照してください。

4. a. に、ポリシーの名前を入力します。
5. で、アクセス ポリシーを適用するアプリを選択します。
6. – アプリへのアクセスを許可または拒否する条件とユーザーまたはユーザーグループを選択します。
 - : フィールドにリストされている名前のいずれかに一致するユーザーまたはグループのみがアクセスを許可されます。
 - : フィールドにリストされているユーザーまたはグループを除くすべてのユーザーまたはグループがアクセスを許可されます。

表示名、メール ID、またはユーザープリンシパル名でユーザーを検索できます。この検索オプションを使用すると、管理者は、複数のアカウントを持っている場合でも、正しいユーザーを正確に識別してアクセスを許可できます。詳細については、「[Policy conditions](#)」を参照してください。

7. (オプション) + をクリックして、コンテキストに基づいて複数の条件を追加します。

コンテキストに基づいて条件を追加すると、条件に AND 演算が適用され、ユーザーとオプションのコンテキストベースの条件が満たされた場合にのみポリシーが評価されます。コンテキストに基づいて、次の条件を適用できます。

- - ユーザーがアプリにアクセスする条件とネットワークを選択します。

- : リストされているネットワークロケーションのいずれかからアプリにアクセスしているユーザーまたはユーザーグループのみが、アプリへのアクセスを有効にされます。
- : リストされているネットワークロケーション以外のすべてのユーザーまたはユーザーグループが、アクセスを有効にされます。

- - ユーザーデバイスがアプリにアクセスするために満たす必要がある条件を選択します。

詳細については、「[Policy conditions](#)」を参照してください。

8. で、条件評価に基づいてアプリに適用する必要がある次のいずれかのアクションを選択します。

- アクセスを許可
- アクセスを拒否

9. 「保存時にポリシーを有効にする」を選択します。このオプションを選択しない場合、ポリシーは作成されるだけで、アプリケーションには適用されません。または、「アクセスポリシー」ページでトグルスイッチを使用してポリシーを有効にすることもできます。

アクセスポリシーを編集する

1. Secure Private Access管理コンソールで、「アクセスポリシー」をクリックします。
2. 変更するポリシーと同じ行にある省略記号ボタンをクリックし、「アクセスポリシーの編集」をクリックします。
3. ポリシーの詳細を編集します。
4. 「更新」をクリックします。

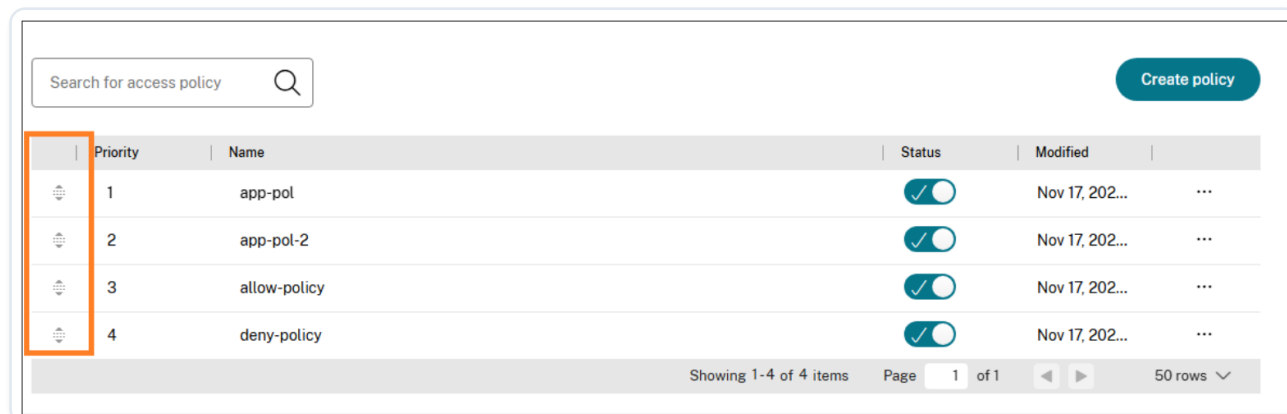
Search for access policy					Create policy
	Priority	Name	Status	Modified	
	1	app-pol	☒	Nov 17, 202...	...
	2	app-pol-2	☒	Nov 17, 202...	...
	3	allow-policy	☒	Nov 17, 202...	...
	4	deny-policy	☒	Nov 17, 202...	...
Showing 1-4 of 4 items					Page 1 of 1
					50 rows

アクセスポリシーの優先度を変更する

アクセスポリシーが作成されると、デフォルトで優先度番号が割り当てられます。優先度は「アクセスポリシー」ホームページで確認できます。

値が小さい優先度ほど優先順位が高く、最初に評価されます。このポリシーが定義された条件と一致しない場合、次に優先度番号が低いポリシーが評価され、以降同様に処理されます。

「優先度」列の上下アイコンを使用してポリシーを上下に移動することで、優先順位を変更できます。



	Priority	Name	Status	Modified	
↑ ↓	1	app-pol	✓	Nov 17, 202...	...
↑ ↓	2	app-pol-2	✓	Nov 17, 202...	...
↑ ↓	3	allow-policy	✓	Nov 17, 202...	...
↑ ↓	4	deny-policy	✓	Nov 17, 202...	...

Showing 1-4 of 4 items Page 1 of 1 50 rows ▾

次のステップ

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

構成検証の例

ポリシー条件

以下のセクションでは、ポリシー条件に関する詳細情報を提供します。

ユーザーとユーザーグループ

ユーザー条件は、アクセスポリシーが適用されるユーザー、グループ、またはID属性を定義します。これらのルールにより、管理者はアプリケーションへのアクセスを決定する際に、特定のIDを含めたり除外したりできます。

ユーザー条件は、主に次の3つのコンポーネントで構成されています。

一致タイプ: このドロップダウンリストは、選択されたIDのリストがどのように評価されるかを制御します。

- **いずれかに一致:**
 - ポリシーが選択されたユーザーまたはグループにのみ適用される必要がある場合に使用します。

- 。リスト内の少なくとも1つのIDが一致する場合、条件は満たされます。
- 。INフィルターのよう機能します。

- **いずれにも一致しない**

- 。選択されたユーザーまたはグループを除く全員にポリシーを適用する場合に使用します。
- 。選択されたIDのいずれにも一致しない場合にのみ、条件は満たされます。
- 。NOT INフィルターのよう機能します。

ポリシー条件(/en-us/citrix-secure-private-access/media/spa-hybrid-create-network-location.png)

ドメインセクター:

「ドメイン」ドロップダウンリストは、ディレクトリまたはIDソースによってIDをフィルタリングします。

- **IDセクター (ユーザーメール、グループメール)** - このフィールドでは、ユーザーメールやグループメールを含む1つ以上のIDを選択できます。

ユーザーとグループの同期を確認する

ユーザー検索中に、管理者は選択したディレクトリのユーザーがGoogle Directoryと同期されているかどうかを確認できます。Secure Private Accessポリシーは、ユーザーがGoogle Directoryと同期されている場合にのみ正しく評価されます。そうでない場合、次の警告が表示されることがあります。

- **テナントアカウントの権限がありません:**

回避策:

Google管理コンソールで、テナントサービスアカウントに「**ユーザー > 読み取り**」権限を割り当てます。Secure Private Accessは、ユーザーが存在することを確認するためにこれらの権限を必要とします。

- **ユーザーが同期されていません:**

回避策:

検索または選択されたユーザーはGoogle Directoryと同期されていません。Secure Private Accessポリシーで使用する前に、ディレクトリエンティティをGoogle Directoryと同期してください。

注:

この機能は、Google Chromeとの統合が正常に完了した後にのみ利用可能です。

ネットワークロケーション

ネットワークロケーションサービス (NLS) は、ユーザーのネットワークロケーションに基づいてアクセスを制限できるポリシー条件です。管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいてアクセスポリシーを構成できます。場所は、ユーザーがアプリケーションにアクセスしている国、またはユーザーのネットワークロケーションである場合があります。ネットワークロケーションは、IPアドレス範囲またはサブネットアドレスを使用して定義されます。

場所に基づいてアクセスポリシーを構成するには、次の手順を実行します。

1. **条件セクションで、条件の追加をクリックします。**
2. **ネットワークロケーションを選択します。**

Create network location ✕

Fill in the required fields below to create a new network location.

Location name *

Public IP address range * (?)

Location tags * (?)

Choose a network connectivity type:

☒ External (?)

☐ Internal (?)

複数のネットワークロケーションを構成している場合は、要件に応じて次のいずれかを選択します。

- **いずれかに一致** – ネットワークロケーションは、データベースで構成されているネットワークロケーションのいずれかに一致します。
- **いずれにも一致しない** – ネットワークロケーションは、データベースで構成されているネットワークロケーションのいずれにも一致しません。

注:

ネットワークロケーションでは、既存のネットワークロケーションを選択するか、新しいネットワークロケーションを作成できます。新しいネットワークロケーションを作成するには、**ネットワークロケーションの作成**をクリックします。

- **Citrix Cloud > StoreFront Cloud > アクセス > アダプティブアクセス**からアダプティブアクセスを有効にしていることを確認してください。有効にしていない場合、ロケーションタグを追加できません。詳細については、「[アダプティブアクセスの有効化](#)」を参照してください。

Citrix Cloudコンソールからネットワークロケーションを作成することもできます。詳細については、「[DaaSリソースへの接続](#)」を参照してください。

3. ポリシー構成を完了します。

セッションポリシーを構成する

セッションポリシーを使用すると、NetScaler Gatewayのトンネリングをバイパスして、ユーザーがバックエンドアプリケーションに直接アクセスできるようになります。

1. **ポリシー > セッションポリシー**に移動し、**セッションポリシーの作成**をクリックします。

セッションポリシー(/en-us/citrix-secure-private-access/media/spa-hybrid-session-policy.png)

2. ポリシーの名前と説明を入力します。
3. これらの設定を適用するユーザーと条件を選択します。

条件をすべてのユーザーに適用することも、ユーザーのサブセットに適用することもできます。

たとえば、**ネットワークロケーション**条件を定義して、セッション全体の動的ルーティングを有効にできます。これにより、ユーザーが会社の企業ネットワーク内にいる場合にのみ、直接ルーティングが有効になります。

コンテキストに基づいて追加の条件を追加すると、条件にAND演算が適用され、ユーザーとオプションのコンテキストベースの条件の両方が満たされた場合にのみポリシーが評価されます。

4. **直接ルーティング**を選択すると、NetScaler Gatewayのトンネリングなしでユーザーのトラフィックがバックエンドアプリケーションに直接送信されます。
5. **作成後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、**ステータス列**のトグルスイッチを使用して、セッション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。

6. **保存**をクリックします。

注：

ネットワークロケーションの変更はセッションポリシーの更新をトリガーし、これはエンドクライアントに次のように影響する可能性があります。

- **Citrix Secure Accessクライアント:** ポリシーの更新はルーティング構成を変更する可能性があります、その結果、アプリケーションアクセスに影響を与える可能性があります。
- **Chrome Secure Browse拡張機能:** ポリシーの更新は30分ごとに発生します。ユーザーはブラウザを再起動するか、更新を待ってからアプリケーションにアクセスする必要があります。

デバイス証明書の登録

デバイスがネットワークに一貫して安全に接続できるように、Always On構成のためにデバイス証明書を登録する必要があります。

デバイス証明書の登録には、以下の手順が含まれます。

1. Active Directoryエンタープライズ証明機関は、マシン認証のためにデバイス証明書を発行します。
2. 証明機関は、CRL配布ポイント (CDP) 拡張機能のためにLDAP URLを公開している必要があります。

常時オン CRL CDP(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-crl-cdp.png)

3. デバイス証明書を登録するには、この証明機関で以下の詳細を持つ証明書テンプレートを作成する必要があります。
 - a. 証明書テンプレートスナップインを開き、**Computer** または **Workstation Authentication** (推奨) テンプレートのいずれかを複製します。
 - b. 証明書に新しい名前を指定します。
 - c. **サブジェクト名**タブに切り替え、**サブジェクト名形式**の設定を**共通名**に変更し、代替サブジェクト名に****ユーザープリンシパル名 (UPN)****を含めるようにチェックします。

常時オン サブジェクト名(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-common-name-upn.png)

- d. **セキュリティ**タブに切り替え、新しい証明書テンプレートを自動登録したいセキュリティグループ (コンピューターアカウントのみを含む) を追加します。追加したグループを選択し、**自動登録**に対して**許可**を選択します。

常時オン 認証済みユーザー (/en-us/citrix-secure-private-access/media/spa-ztna-always-on-auto-enroll.png)

注：

上の画像では、**認証済みユーザー** (すべてのコンピューターオブジェクト) が新しい証明書テンプレートを登録または自動登録することが許可されています。

- e. (オプション) 自動証明書登録を許可するグループポリシーオブジェクト (GPO) を作成し、それを組織単位 (OU) またはドメインレベルにバインドします。

常に自動登録証明書 (/en-us/citrix-secure-private-access/media/spa-ztna-always-on-autoenroll-certificate.png)

デバイスポスチャサービス

Citrix デバイスポスチャサービスは、エンドデバイスが Citrix DaaS (仮想アプリおよびデスクトップ) または Citrix Secure Private Access リソース (SaaS、Web アプリ、TCP、UDP アプリ) にアクセスするために満たす必要のある特定の要件を管理者が適用するのに役立つクラウドベースのソリューションです。デバイスのポスチャを確認してデバイスの信頼を確立することは、ゼロトラストベースのアクセスを実装するために不可欠です。デバイスポスチャサービスは、エンドユーザーがログインする前に、エンドデバイスのコンプライアンス (管理対象/BYOD およびセキュリティポスチャ) を確認することで、ネットワークにゼロトラスト原則を適用します。

デバイスポスチャの詳細については、「[デバイスポスチャ](#)」を参照してください。

NetScaler Gateway でデバイスポスチャチェックを構成する

Citrix デバイスポスチャサービスは NetScaler Gateway と統合されています。NetScaler Gateway でデバイスポスチャチェックを構成できます。

詳細については、「[NetScaler® Gateway でのデバイスポスチャチェック](#)」を参照してください。

注:

- 仮想サーバーレベルでデバイスポスチャチェックを有効にすることをお勧めします。
- 顧客 ID が `set dps parameter -CustomerID <CCID>` である `set dps parameter` を使用して設定されていることを確認してください。残りのパラメーターは自動入力されます。

オンプレミスNetScaler® Gatewayでのデバイスポスチャチェック

Citrix Device Postureサービスは、クラウドベースのソリューションです。これにより、管理者は、SaaS/WebおよびTCP/UDPアプリなどのCitrix Secure Private Accessリソースにアクセスするためにエンドデバイスが満たす必要のある特定の要件を適用できます。デバイスのポスチャをチェックしてデバイスの信頼を確立することは、ゼロトラストベースのアクセスを実装するために不可欠です。Device Postureサービスは、エンドユーザーがログインする前に、エンドデバイスの

コンプライアンス（管理対象/BYODおよびセキュリティポスチャ）をチェックすることで、ネットワークにゼロトラスト原則を適用します。Device Postureサービスの詳細については、「[Device Posture](#)」を参照してください。

エンタイトルメント

Device Postureサービスは、Universal Hybrid Multi Cloud (UHMC) ライセンスおよびCitrix Platform License (CPL) の一部として利用できます。詳細については、<https://www.citrix.com/buy/licensing/product.html>を参照してください。

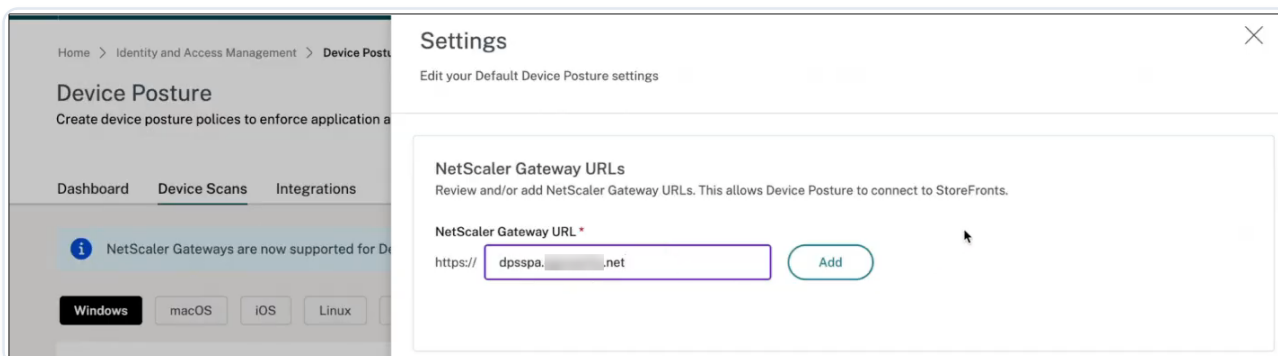
Secure Private Accessハイブリッドソリューション向けにDevice Postureを有効にする

ハイブリッドソリューション向けのSecure Private AccessとDevice Postureサービスの統合は、NetScaler Gatewayリリース14.1ビルド43.x以降でのみサポートされています。Secure Private Accessハイブリッド展開でDevice Postureスキャンが機能するには、NetScaler GatewayでDevice Posture機能を有効にする必要があります。

NetScaler GatewayでDevice Postureチェックを有効にする方法の詳細については、「[NetScaler GatewayでのDevice Postureチェック](#)」を参照してください。

NetScaler GatewayでDevice Posture機能を有効にするだけでなく、Device Postureの**設定**ページで、StoreFront™にアクセスするNetScaler GatewayのURLを追加する必要があります。

1. Secure Private Access管理コンソールのナビゲーションペインで、**Device Posture**をクリックします。
2. デバイススキャンページで、**設定**をクリックします。
3. **NetScaler Gateway URL**に、Device Postureチェックを有効にする仮想サーバーのFQDNを入力します。例: <https://gw.example.net>。



設定の管理

オンボーディング後、Secure Private Access ハイブリッド展開設定を更新および維持できます。

- アプリケーションドメインルーティングを管理し、構成レポートを生成します。レポートには、アクセスポリシー、アプリケーション、ルーティングドメイン、リソースの場所、セキュリティグループ、Cloud Connector、サイト構成、ブラウザ設定に関する詳細が含まれます。詳細については、「オンボーディング後の設定の管理」(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-manage-settings-post-onboarding.html>)を参照してください。
- オンボーディング構成入力を管理します。複数のコンポーネントがこれらの値に依存しているため、変更は中断を引き起こす可能性があります。変更内容によっては、NetScaler の再構成と再分析、StoreFront の再構成、StoreFront の再分析などの必要なフォローアップアクションが含まれる場合があります。詳細については、「インストール後のセットアップ構成の管理」(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-manage-configuration-after-installation.html>)を参照してください。
- Citrix Enterprise Browser 統合から Chrome Enterprise Premium に切り替える際に構成をリセットします。詳細については、「Secure Private Access 構成のリセット」(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-reset-spa-configuration.html>)を参照してください。
- Cloud Connector の更新は、利用可能になったときにデフォルトで一度に1つのコネクタにインストールされ、Secure Private Access はデフォルトで Cloud Connector のアップグレードの一部としてアップグレードされます。詳細については、「コンポーネントのアップグレード」(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-components-upgrade.html>)を参照してください。

設定を管理する

以下のセクションでは、設定に関する詳細情報を提供します。

アプリケーションドメイン

Secure Private Access 管理者は、Secure Private Access セットアップに追加されたアプリケーションドメインのリストを表示できます。アプリケーションドメインテーブルには、関連するすべてのドメインと、アプリトラフィックがどのようにルーティングされるか（外部または内部）が一覧表示されます。

1. **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します。

構成レポート

顧客管理者は、Secure Private Access セットアップに関する洞察を得るために構成レポートを生成できます。構成レポートには、以下のカテゴリの情報が含まれます。

- アプリケーションとリソースへのアクセスを管理するアクセスポリシー。
- Secure Private Access 内で構成されたアプリケーション。
- アプリケーション用に設定されたルーティングドメイン。
- 顧客に関連付けられたリソースロケーション。
- セキュリティグループ。
- クラウドコネクタ。
- サイト構成。
- ブラウザ設定。

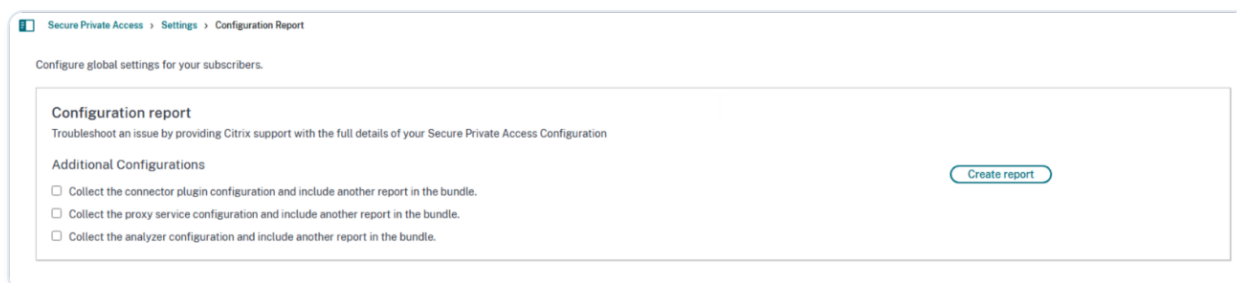
バンドルには、追加の構成レポートを含めることもできます。

- コネクタプラグインデータベースからの詳細。
- プロキシサービスからの詳細。
- アナライザー構成からの詳細。

構成レポートを生成する

構成レポートを生成するには、次の手順を実行します。

1. Secure Private Access 管理コンソールで、**設定 > 構成レポート**に移動します。

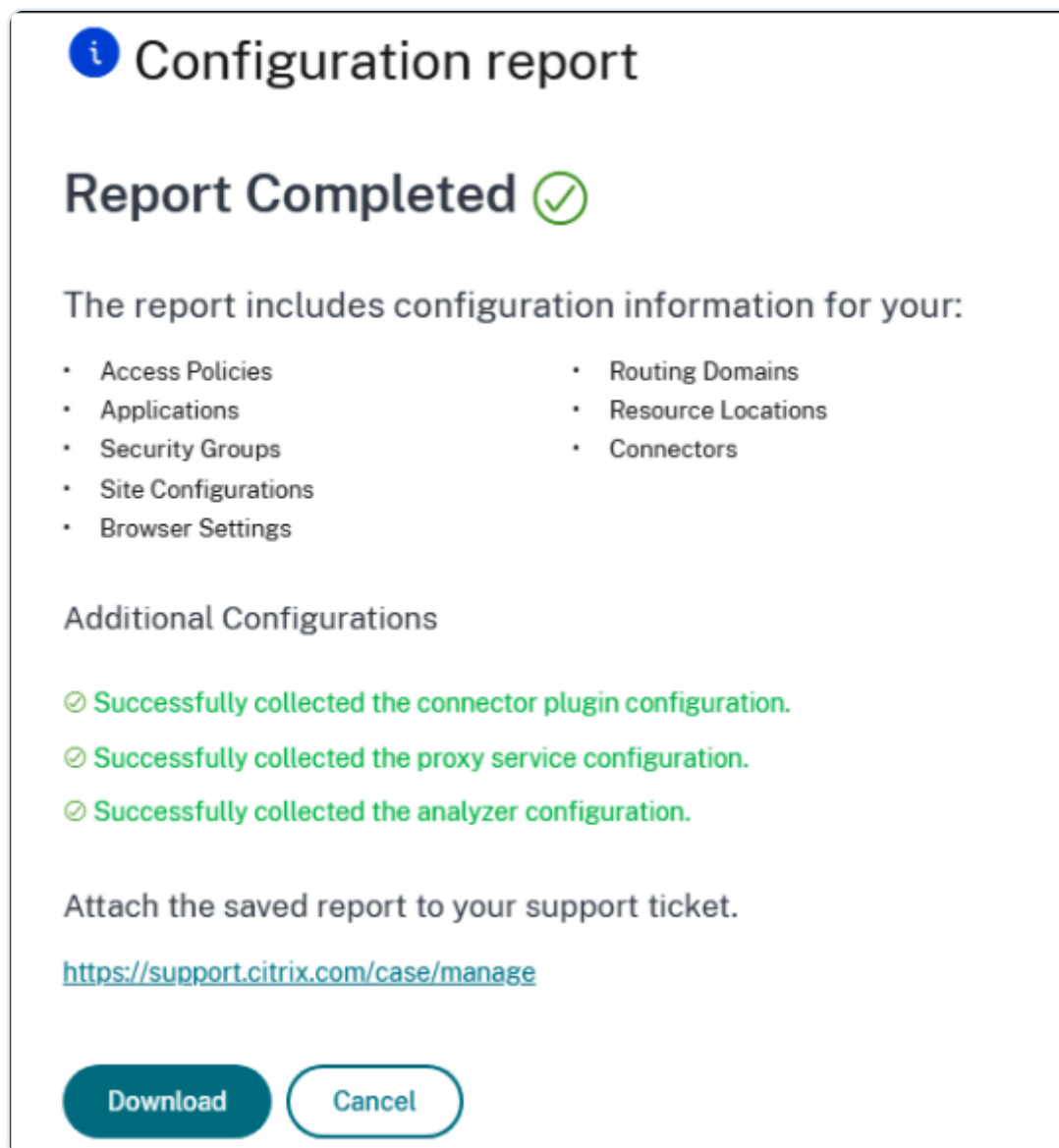


2. コネクタプラグインデータベース、プロキシサービス、またはアナライザー構成に保存されている構成の詳細を収集して、追加レポートをバンドルに含めるには、**追加構成**セクションの下にある適切なチェックボックスをオンにします。
3. **レポートの作成**をクリックして、レポート生成プロセスを開始します。

レポートが生成されると、**構成レポート**ダイアログに次のステータスが表示されます。

- **レポート完了:** 必要なすべての詳細がレポートに正常に含まれていることを示します。
- **レポート一部完了:** 一部の詳細が不足しているか、生成されていないことを示します。
- ダイアログには、レポート生成が不完全だったカテゴリも表示されます。

次の図は、完了および部分的に完了したステータスを持つ**構成レポート**ダイアログのサンプルを示しています。



Configuration report

Report Partially Complete

Some of the configuration information could not be retrieved:

- Browser Settings

Additional Configurations

 Failed to collect the connector plugin configuration.

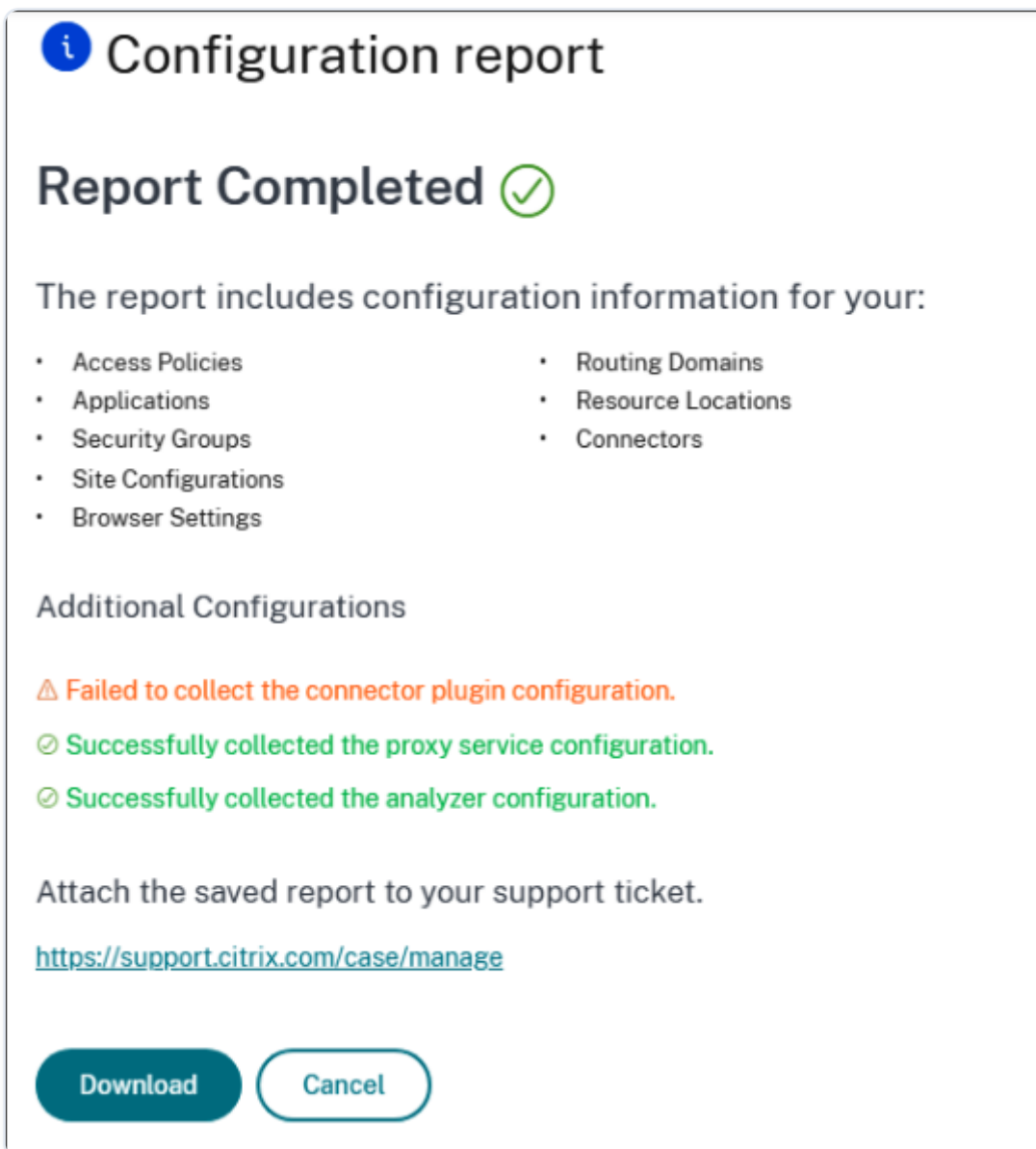
 Successfully collected the proxy service configuration.

Attach the saved report to your support ticket.

<https://support.citrix.com/case/manage>

Download

Cancel



4. ダウンロードをクリックして、レポートをローカルドライブに手動でエクスポートします。

重要:

構成レポートの生成は、次のSecure Private Accessの役割を持つ管理者に限定されます。

- フルアクセス管理者
- 読み取り専用管理者
- フルモニター管理者

ヘルプデスク管理者ロールを持つ管理者は、構成レポートを生成できません。

注:

レポートには機密データが含まれる場合があります。

インストール後のセットアップ構成を管理する

「セットアップ構成」メニューオプションを使用して、オンボーディング中に提供されたさまざまな構成入力を管理できます。

警告:

構成値を変更すると、中断が発生する可能性があります。この構成は複数のコンポーネントによって参照されるため、変更によってサービス中断を避けるために、依存するコンポーネントで再構成が必要になる場合があります。

以下の表は、構成が変更された場合に必要となる追加のアクションをまとめたものです。

構成名	必要なアクション	説明
ステップ1		
GoogleカスタマーID	スクリプトを再度ダウンロードして、NetScalerを再構成し、再分析します。	Googleサービスは自動的に再構成されます。
セキュア プライベート アクセス ゲートウェイ URL	スクリプトを再度ダウンロードして、NetScalerを再構成し、再分析します。	Googleサービスは自動的に再構成されます。 注 CEP構成がスキップされた場合、この設定はStep2の一部です。
Google Workspace ユーザーグループ	手動での操作は不要です	設定が保存されると、新しいユーザーグループは必要なGoogleサービスに自動的に構成されます。
ステップ2		
NetScaler Gateway 仮想サーバー名	NetScaler Analyzer のみを再実行します	NetScaler スクリプトの実行時に分析オプションを使用します。
セキュア プライベート アクセス サイトURL	新しいSecure Private Access アドレスでStoreFrontを再構成します。	

構成名	必要なアクション	説明
	スクリプトを再度ダウンロードしてStoreFrontを再分析します	
	スクリプトを再度ダウンロードしてNetScalerを再構成し、再分析します。	
内部IPアドレス (Secure Private Access Gateway URL 用)	スクリプトを再度ダウンロードしてNetScalerを再構成し、分析します。	
証明書キーペア名	スクリプトを再度ダウンロードしてNetScalerを再構成し、再分析します。	

Secure Private Access 構成をリセットする

Citrix Enterprise Browser と統合された Citrix Secure Private Access ハイブリッド展開があり、Chrome Enterprise Premium に切り替えたい場合は、Secure Private Access 構成をリセットできます。この操作により、アプリケーションとアクセスポリシーを含む構成全体が削除されます。StoreFront と NetScaler の構成は手動でクリーンアップする必要があります。構成リセット後、Secure Private Access ハイブリッド展開を再度オンボーディングし、Chrome Enterprise Premium を選択できます。

構成をリセットする必要がある場合は、Citrix サポートにお問い合わせください。

アップグレード

定期的に、Citrix は Cloud Connector のパフォーマンス、セキュリティ、信頼性を向上させるためのアップデートをリリースしています。デフォルトでは、Citrix Cloud はこれらのアップデートが利用可能になったときに、各コネクタに一度に1つずつインストールします。Secure Private Access は、デフォルトで Cloud Connector のアップグレードの一部としてアップグレードされません。

Cloud Connector のアップグレードの詳細については、[コネクタの更新](#)を参照してください。

注:

GUI を介した NetScaler のアップグレードでは、Python がインストールされない場合があります。CLI を介して NetScaler をアップグレードすることをお勧めします。

その他のコンポーネントのアップグレードの詳細については、以下のトピックを参照してください。

- [StoreFront](#)
- [ネットスケラー ゲートウェイ](#)

高度なSecure Private Access機能

Secure Private Accessでサポートされている高度な機能の一部を以下に示します。

- **高度なデータセンター構成:** Secure Private Accessハイブリッド展開は、GSLB接続プロキシのサイト永続性メソッドを使用したアクティブ-アクティブサイト展開でNetScaler GSLBを使用する、マルチサイト構成のマルチデータセンターでサポートされています。詳細については、「[高度なデータセンター構成](#)」を参照してください。
- **グローバルサーバー負荷分散接続プロキシ:** グローバルサーバー負荷分散（GSLB）接続プロキシを使用すると、NetScaler Gatewayは誤ってルーティングされた要求を透過的に検出し、ユーザーの介入なしに正しいサイトにプロキシできます。詳細については、「[グローバルサーバー負荷分散接続プロキシ](#)」を参照してください。
- **グローバルサーバー負荷分散ドメインURLの構成:** Secure Private Accessのマルチサイト冗長性を設定するには、グローバルサーバー負荷分散（GSLB）アドレスを構成する必要があります。このアドレスは単一のエントリポイントとして機能し、静的近接性などのトラフィックポリシーに基づいて、ユーザーを特定のデータセンターのSecure Private Accessゲートウェイにルーティングします。詳細については、「[グローバルサーバー負荷分散ドメインURLの構成](#)」を参照してください。
- **コンテキストベースのアプリケーションルーティング:** アプリが構成されると、アプリケーションURLとその関連ドメインまたはアプリの宛先に対して、アプリ構成の下でルーティングタイプが定義されます。ここで定義されたルーティングタイプは、アプリにアクセスできるすべてのユーザーに適用されます。ただし、管理者がユーザーコンテキストに基づいて同じアプリを異なる方法でルーティングしたいシナリオもあります。たとえば、ユーザーが企業ネットワーク内にいる場合、内部アプリのURLまたは宛先はSecure Private Access経由ではなく直接ルーティングする必要があります。詳細については、「[コンテキストベースのアプリケーションルーティング](#)」を参照してください。
- **エンドユーザーがアクセスしたドメインまたはIPアドレスの検出:** アプリケーション検出機能は、管理者が組織内でアクセスされている外部および内部アプリケーション（HTTP/HTTPSおよびTCP/UDPアプリ）を可視化するのに役立ちます。この機能は、公開済みまたは未公開のすべてのドメイン/IPアドレスを検出し、一覧表示します。これにより、管理者はどのドメイン/IPアドレスが誰によってアクセスされているかを確認し、それらをアプリケーションとして公開して、それらのユーザーにアクセスを提供するかどうかを決定できます。詳細について

は、「[エンドユーザーがアクセスしたドメインまたはIPアドレスの検出](#)」を参照してください。

- **ポリシーモデリングツール:** 管理者は複数のポリシーを作成し、これらのポリシーを複数のアプリケーションに割り当てることができます。その結果、管理者はエンドユーザーのアプリケーションアクセス結果を理解することが困難になる場合があります。つまり、アプリケーションとアクセスポリシーの構成に基づいて、エンドユーザーがアクセスを許可されているか拒否されているかです。ポリシーモデリングツール（アクセスポリシー > ポリシーモデリング）は、管理者に期待されるアプリケーションアクセス結果（許可/制限付きで許可/拒否）を完全に可視化することで、これらの問題を解決するのに役立ちます。詳細については、「[ポリシーモデリングツール](#)」を参照してください。
- **データ損失防止（DLP）ポリシーの構成:** CEPのアクセス制限は、Google管理コンソールで構成されます。以前Secure Private Accessコンソールで構成されていたアクセス制限は、Citrix Enterprise Browserにのみ適用されます。Google Chromeがエンタープライズブラウザである場合、アクセス制限はGoogle管理コンソールでポリシーおよびルールとして構成する必要があります。詳細については、「[データ損失防止（DLP）ポリシーの構成](#)」を参照してください。
- **高可用性展開:** Secure Private Accessの高可用性は、いくつかの簡単な手順で構成できます。詳細については、「[高可用性展開](#)」を参照してください。
- **Secure Private Access構成のリセット:** Citrix Enterprise Browser統合を備えたCitrix Secure Private Accessハイブリッド展開があり、Chrome Enterprise Premiumに切り替えたい場合は、Secure Private Access構成をリセットできます。詳細については、「[Secure Private Access構成のリセット](#)」を参照してください。

高度なデータセンター構成

Secure Private Access ハイブリッド展開は、GSLB 接続プロキシのサイト永続性メソッドを使用したアクティブ/アクティブサイト展開で NetScaler GSLB を使用する、マルチデータセンターとマルチサイト構成でサポートされています。

マルチデータセンター展開(</en-us/citrix-secure-private-access/media/spa-hybrid-multi-datacenter.png>)

このトピックでは、マルチデータセンターマルチサイト構成で Secure Private Access ハイブリッド展開を設定するための段階的な手順を説明します。

前提条件

マルチデータセンターに Secure Private Access ハイブリッドを展開するには、次の前提条件が満たされていることを確認してください。

- NetScaler Gateway バージョン 14.1–66.59 以降。
- アクティブ/アクティブサイト展開の NetScaler GSLB。GSLB ドメインはすべてのサイトで構成する必要があります。GSLB をまだ構成していない場合は、手順について [アクティブ/アクティブサイト展開](#) を参照してください。
- GSLB で送信元 IP 永続性が有効になっています。
- CEP セッションで接続プロキシ永続性が有効になっています。詳細については、[グローバルサーバー負荷分散接続プロキシ](#) を参照してください。

GSLB 構成 CLI コマンド

GSLB の構成には NetScaler CLI を使用することをお勧めします。以下に CLI コマンドテンプレートと構成例を示します。

- `add service <ADNS_SERVICE_NAME> <ADNS_IP> ADNS 53`
- `add gslb site <SITE_NAME> <SITE_IP> -sitePassword "<SITE_PASSWORD>"`
- `add gslb service <GSLB_SERVICE_NAME> <SERVICE_IP> SSL 443 -publicIP <PUBLIC_IP> -publicPort 443 -siteName <SITE_NAME>`
- `add gslb vsrver <VSERVER_NAME> SSL`
- `bind gslb vsrver <VSERVER_NAME> -serviceName <GSLB_SERVICE_NAME>`
- `bind gslb vsrver <VSERVER_NAME> -domainName <GSLB_DOMAIN_FQDN>`
- `set lb vsrver <VSERVER_NAME> -PersistenceType SOURCEIP`
- `set gslb service <GSLB_SERVICE_NAME> -sitePersistence ConnectionProxy`
- `bind ssl service <GSLB_SERVICE_NAME> -certKeyName <SERVICE_CERT_KEY>`
- `bind ssl vsrver <VSERVER_NAME> -certKeyName <CA_CERT_KEY> -CA`
- `bind ssl vsrver <VSERVER_NAME> -certKeyName <EXTERNAL_CA_CERT_KEY> -CA`
- `bind ssl vsrver <VSERVER_NAME> -certKeyName <SERVER_CERT_KEY>`

参照

以下の表は、CLIコマンドで使用されるプレースホルダーとその簡単な説明をまとめたものです。

プレースホルダー	説明
<code><ADNS_SERVICE_NAME></code>	ADNSサービスの名前（例: adns_ <code><env></code> ）

<ADNS_IP>	このNetScaler上のADNSリスナーのIPアドレス
<SITE_NAME>	GSLBサイト識別子（例：blue、green）
<SITE_IP>	GSLBサイトIP（MEP通信に使用されるSNIPまたは管理IP）
<SITE_PASSWORD>	GSLBサイト間MEP認証用の共有シークレット
<GSLB_SERVICE_NAME>	ローカル/リモートの負荷分散仮想サーバーにバインドされたGSLBサービスの名前
<SERVICE_IP>	バックエンドの負荷分散仮想サーバーまたはサービスのIPアドレス
<PUBLIC_IP>	インターネットから到達可能なパブリック（NAT）IPアドレス
<VSERVER_NAME>	GSLB仮想サーバーの名前
<GSLB_DOMAIN_FQDN>	GSLBがクライアントのために解決するFQDN
<SERVICE_CERT_KEY>	GSLBサービスにバインドされているSSL証明書キー名
<CA_CERT_KEY>	内部CA証明書キー名 (-CAとしてバインド)
<EXTERNAL_CA_CERT_KEY>	外部/公開CA証明書キー名 (-CAとしてバインド)
<SERVER_CERT_KEY>	仮想サーバーにバインドされているサーバー証明書キー名

構成例:

- `add service adns_staging 10.100.5.50 ADNS 53`
- `add gslb site us-east-dc1 10.100.5.60 -sitePassword "password"`
- `add gslb service us-east-dc1-svc1 10.100.5.80 SSL 443 -publicIP 203.0.113.42 -publicPort 443 -siteName us-east-dc1`
- `add gslb vserver staging_us-east_vs SSL`

- `bind gslb vserver staging_us-east_vs -serviceName us-east-dc1-svc1`
- `bind gslb vserver staging_us-east_vs -domainName proxy-staging.example.com`
- `set lb vserver staging_us-east_vs -PersistenceType SOURCEIP`
- `set gslb service us-east-dc1-svc1 -sitePersistence ConnectionProxy`
- `bind ssl service us-east-dc1-svc1 -certKeyName star_staging_local`
- `bind ssl vserver staging_us-east_vs -certKeyName ca_staging.local -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName CA.csg.proxy.ext.example -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName csg.proxy.ext.example`

データセンターのセットアップと構成

次の図は、マルチデータセンターにおけるSecure Private Accessハイブリッド展開のトポロジ図を示しています。

マルチデータセンター展開(/en-us/citrix-secure-private-access/media/spa-hybrid-multidata-center-topology.png)

1. データセンターを追加します。詳細については、「[ステップ2: 最初のデータセンターをセットアップする](#)」を参照してください。
2. 各データセンターで、NetScalerおよびStoreFrontスクリプトをダウンロードして実行します。詳細については、「[NetScalerおよびStoreFrontスクリプトをダウンロードして実行する](#)」を参照してください。
3. 各データセンターで、レポートをアップロードし、構成を分析します。詳細については、「[レポートをアップロードして構成を分析する](#)」を参照してください。
4. 分析結果を確認します。

すべてのアナライザーの手順が各データセンターで合格した場合、構成の検証に成功し、オンボーディング後のタスクに進むことができます。詳細については、[オンボーディング後のタスク](#)を参照してください。

グローバルサーバー負荷分散接続プロキシ

グローバルサーバー負荷分散 (GSLB) 接続プロキシを使用すると、NetScaler Gateway は、誤ってルーティングされたリクエストを透過的に検出し、ユーザーの介入なしにそれらを正しいサイトにプロキシできます。

GSLB を使用するマルチサイトの Citrix Secure Private Access ハイブリッド展開では、DNS 解決によって、ユーザーリクエストが意図しないサイトにルーティングされることがあります。このような場合、ユーザーはセッションが確立されていないサイトにアクセスすることになり、これにより、内部 Web アプリケーションへのアクセスが妨げられる可能性があります。

GSLB 接続プロキシは、NetScaler Gateway が、誤ってルーティングされたリクエストを透過的に検出し、ユーザーの介入なしにそれらを正しいサイトにプロキシできるようにすることで、この問題を解決します。このプロセスはエンドユーザーには透過的であり、セッションの永続性を向上させ、最適ではない DNS ルーティングによって発生するセッションの中断やアプリケーションアクセス障害を排除します。

前提条件

GSLB 接続プロキシをサポートするには、以下の前提条件が満たされていることを確認してください。

- すべてのサイトで GSLB が構成されているマルチサイトの Secure Private Access ハイブリッド展開。
- GSLB で送信元 IP 永続性が有効になっていること。詳細については、「[送信元 IP アドレスに基づく永続性の構成](#)」を参照してください。
- 静的近接が構成されていること (管理者によって管理される IP データベース)。詳細については、「[静的近接](#)」を参照してください。
- NetScaler Gateway のバージョンが 14.1 以降であること。

GSLB 接続プロキシの構成

GSLB 接続プロキシを有効にするには、すべての GSLB サービスと VPN 仮想サーバーに証明書をバインドします。

1. 共通名を持つ自己署名クライアント証明書を生成します (例: `csg.proxy.ext.goog`)。
2. すべてのサイトのすべての GSLB サービスに証明書をバインドします。
3. 発行者証明書を CA 証明書として VPN 仮想サーバーにバインドします。
4. デプロイ内のすべてのサイトのすべてのGSLBサービスに対して、サービスバインディングを繰り返します。

CLIコマンド:

- 証明書をGSLBサービスにバインドします。

```
bind ssl service <gslb-service-name> -certKeyName <certificate-name>
```

- 発行者証明書をVPN仮想サーバーにバインドします。

```
bind ssl vsrver <vpn-vserver-name> -certKeyName <certificate-name> -CA
```

グローバルサーバーロードバランサードメインURLを構成する

Secure Private Access のマルチサイト冗長性を設定するには、グローバルサーバーロードバランサー (GSLB) アドレスを構成する必要があります。このアドレスは単一のエントリポイントとして機能し、静的近接性などのトラフィックポリシーに基づいて、ユーザーを特定のデータセンターの Secure Private Access ゲートウェイにルーティングします。

Secure Private Access 展開用に GSLB を構成する場合、GSLB アドレスは Google Secure Gateway (Google Cloud サービス内) 内で更新する必要があります。データセンター固有の Secure Private Access ゲートウェイが以前に使用されていた場合、GSLB アドレスを提供すると、既存の構成が自動的に上書きされ、新しいグローバルアドレスを指すようになります。

構成

プロンプトが表示されたら、グローバルサーバーロードバランサー (GSLB) ドメインURLの詳細を入力して、Chrome Enterprise Premium (CEP) 構成をGSLBドメインで更新します。この更新後、最初のデータセンターでNetScaler Gatewayを再構成します。

1. **Secure Private Access** 管理コンソールにログインします。
2. **セットアップ構成**に移動します。
3. **グローバルサーバーロードバランサー (GSLB)** をクリックします。

GSLBドメインURLのセットアップ(/en-us/citrix-secure-private-access/media/spa-hybrid-gslb-domain-setup.png)

4. **Secure Private Access Gateway URL** フィールドに、GSLB ドメイン URL のパブリックアドレスを入力します。

GSLBドメインURL(/en-us/citrix-secure-private-access/media/spa-hybrid-gslb-domain.png)

注:

これにより、CEP 統合が更新され、Secure Private Access Gateway URL が入力した GSLB ドメイン URL に置き換えられます。

データセンターの編集 (オプション)

この手順は、データセンターを変更する必要がある場合にのみ必要です。

Datacenters

×

Select Datacenter

Blue

▼

> View Prerequisites

Global Server Load Balancer (GSLB) required for NetScaler Gateways

Before adding another datacenter, ensure that Global Server Load Balancing (GSLB) is properly configured for your NetScaler Gateways. Verify that your existing GSLB setup is correct before proceeding.

Configure GSLB

Datacenter Name ⓘ

Blue

Secure Private Access site URL ⓘ

https://spa.yourdomain.com

Secure Private Access Gateway URL ⓘ

https://spagateway.yourdomain.com

IP address ⓘ

10.0.2.200

NetScaler Certificate-key pair name ⓘ

your_certificate

Save

構成と分析

前述の手順を完了したら、最初のデータセンターにあるオンプレミスのStoreFrontおよびNetScalerコンポーネントの構成を更新できます。

必要に応じて、データセンターのNetScalerコンポーネントの再構成を完了し、NetScalerおよびStoreFrontの構成を分析するには、[ステップ3：構成と分析](#)に従ってください。

コンテキストベースのアプリケーションルーティング

アプリが構成されると、アプリケーションURLとその関連ドメインまたはアプリの宛先に対して、アプリ構成の下でルーティングタイプが定義されます。ここで定義されたルーティングタイプは、アプリにアクセスできるすべてのユーザーに適用されます。ただし、管理者がユーザーコンテキストに基づいて同じアプリを異なる方法でルーティングしたいシナリオも考えられます。たとえば、ユーザーが社内ネットワーク内にいる場合、内部アプリのURLまたは宛先は、Secure Private Accessを介するのではなく、直接ルーティングされる必要があります。

これは、**アクセスポリシー (特定のユーザー向け)** または **セッションポリシー (すべてのユーザー向け)** の **ルーティング例外** を使用して構成できます。アクセスポリシーのルーティング例外構成により、管理者はポリシーで定義された条件に一致するユーザーまたはマシンのルーティングタイプを編集できます。この設定はアクセスポリシーの一部であるため、そのポリシーに含まれるユーザーとマシンにのみ適用されます。

注:

アクセスポリシー内にルーティング構成がある場合、それはアプリ構成を上書きします。

次の例は、ルーティング例外のユースケースを示しています。

- **コンテキストベースのルーティング**
- **社内ユーザーをバックエンドアプリケーションに直接ルーティングする**

ユースケース: コンテキストベースのルーティング

シナリオ:

- **グループAユーザー:** 会社ABCの従業員で、NetScaler Gatewayを介してOutlookアプリとMicrosoft Teamsアプリにアクセスし、内部的にルーティングされます。
- **グループBユーザー:** ABCと協力しているサードパーティ企業の従業員。彼らはNetScaler Gatewayを介して特定のアプリケーション（Outlookを除く）にアクセスします。また、インターネット経由でアクセスする独自のOutlookアプリケーションを持っており、OutlookトラフィックをNetScaler Gateway経由でルーティングしたくありません。

問題:

- **グループBユーザーは、ABCアプリにアクセスするためにSecure Accessクライアントにログインします。**

- 彼らがネイティブブラウザを介してOutlookにアクセスしようとする、そのリクエストはNetScaler Gateway経由でルーティングされ、アクセス拒否につながります。
- Outlookアプリケーションの宛先ドメインは、グループAとグループBのユーザーの両方で同じです。
- アクセス ポリシーはグループAのユーザーのみにアクセスを許可しているため、グループBのユーザーがMicrosoft TeamsまたはOutlookを起動しようとする、アクセスが拒否されます。
- このルーティングの問題により、グループBのユーザーは会社のOutlookにアクセスできません。

解決策:

ABC社の管理者は、この問題を解決するために以下の構成変更を行うことができます。

1. Office 365アプリにアクセスするグループBのユーザー専用の新しいアクセス ポリシーを定義します。
2. アクセス ポリシーで、**ルーティング例外**オプションを有効にします。

管理者は、アクセス ポリシーに関連付けられているすべての内部アプリのすべてのURLと関連ドメインのリストを表示できます。

3. すべてのOffice 365アプリのURLについて、ルーティングが外部で行われるように構成します。

これにより、グループBのユーザーがOutlookアプリケーションにアクセスするためのリクエストがインターネット経由でルーティングされ、NetScaler Gatewayをバイパスすることが保証されます。

これらの変更を実装することで、グループBのユーザーはNetScaler Gatewayを経由せずにインターネット経由で会社のOutlookアプリケーションにアクセスでき、必要に応じて他のABCアプリケーションへのアクセスも維持できます。

ルーティングの種類を変更する手順

1. アクセス ポリシーを作成または編集します。詳細な手順については、「[アクセス ポリシーの構成](#)」を参照してください。
2. アクセス ポリシーで、**ルーティング例外**トグルをオンに設定します。
3. アクセス ポリシーに関連付けられているアプリのURLと関連ドメインのリストから、ルーティングの種類を変更したいドメインを見つけます。
4. 適用したいユーザーコンテキストに基づいて、選択したドメインのルーティングタイプを変更します（例：**Internal**から**External**へ）。
5. アクセス ポリシーを保存します。

ルーティング例外(/en-us/citrix-secure-private-access/media/spa-hybrid-routing-exceptions.png)

ユースケース: 社内ユーザーをバックエンドアプリケーションに直接ルーティングする

管理者は、NetScaler Gateway を介してトラフィックをトンネリングすることなく、社内ユーザーをバックエンドアプリに直接ルーティングするようにセッションポリシーを設定できます。セッションポリシーは、ネットワークロケーションやデバイスのポスチャなどの要因に基づいて動的なルーティングを提供します。

セッションポリシーの設定の詳細については、「[セッションポリシーの設定](#)」を参照してください。

注:

- セッションポリシー設定は、特定のアプリケーションに紐付けられるのではなく、すべてのアプリケーションにセッションレベルで適用されます。
- セッションポリシーは、すべてのユーザーまたはユーザーのサブセットに割り当てることができます。

ルーティングの優先順位

セッションポリシーはアクセスポリシーと連携して機能し、競合がある場合はアクセスポリシーが優先されます。このようなシナリオでは、アクセスポリシーのルーティング例外がセッションポリシーを上書きします。アクセスポリシーもセッションポリシーも設定されていない場合は、グローバルルーティング設定 (**Settings > Application Domain**) が適用されます。

サポートされているCitrix Secure Access™クライアント

以下のバージョンのCitrix Secure Accessクライアントは、ユーザーをバックエンドアプリケーションに直接ルーティングすることをサポートしています。

- macOS - 24.11.1以降。
- Windows - 24.11.1.17以降。また、**EnableContextualAccess** VPNクライアントレジストリを有効にする必要があります。詳細については、「[NetScaler Gateway Windows VPNクライアントレジストリキー](#)」を参照してください。

使用例

シナリオ:

病院では、ユーザーが病院ネットワーク「hospital_network1」に接続されている場合、これらのアプリは病院ネットワーク上で直接到達可能であるため、アプリからのトラフィックはバックエンドアプリに直接流れる必要があります。ユーザーが病院ネットワークの外部にいる場合、アプリのトラフィックはトンネル経由で送信される必要があります。

解決策:

1. ルーティングを**内部**に設定して、app1、app2を追加します。
2. アプリ (app1、app2) のアクセス権を付与するためのアクセスポリシーを追加します。
3. アクセスを許可する際に考慮する必要があるユーザーグループとネットワークロケーションを指定する条件を設定するために、セッションポリシーを追加します。
4. **ユーザー条件**を選択し、**すべてのユーザー**に設定します。
5. **ネットワークロケーション**条件を追加します。これを**いずれかに一致**に設定し、ネットワークロケーション「hospital_network1」を指定します。これにより、「hospital_network1」からのトラフィックがバックエンドアプリに直接流れるようになります。

このシナリオでは、ルーティング例外を有効にすることもできます。たとえば、app1が病院ネットワーク上でも常にトンネル経由で送信される必要がある場合、アクセスポリシーでapp1のドメインに対してルーティング例外を設定できます。これが完了すると、ルーティング例外がセッションポリシーよりも優先されます。

セッションポリシーを使用して病院ネットワーク内で直接ルーティングを構成する

セッションポリシーを使用して、NetScaler Gatewayのトンネリングをバイパスして、ユーザーがバックエンドアプリケーションに直接アクセスできるようにすることができます。

セッションポリシーの設定の詳細については、「[セッションポリシーの構成](#)」を参照してください。

Secure Private Access > Policies > Create/Edit Session Policy

Policy name

hospital_policy1

Description (optional)

Enter a description

Conditions ⓘ

User:

All users

AND

Network location

Matches any of

hospital_network1

+ Create network location

+ Add condition

Settings

Choose at least one setting to add to this policy.

✓ Direct routing

Route all users externally for all applications.

✓

Policy enablement

✓ Enable policy after creation

Cancel

Save

エンドユーザーがアクセスするドメインまたはIPアドレスを検出する

アプリケーション検出機能は、管理者が組織内でアクセスされている外部および内部アプリケーション（HTTP/HTTPSおよびTCP/UDPアプリ）を可視化するのに役立ちます。この機能は、公開されているかどうかにかかわらず、すべてのドメイン/IPアドレスを検出し、一覧表示します。これにより、管理者はどのドメイン/IPアドレスが誰によってアクセスされているかを確認し、それらをアプリケーションとして公開して、それらのユーザーにアクセスを提供するかどうかを決定できます。

アプリケーション検出機能は、管理者に以下の機能を提供します。

- エンドユーザーがアクセスする内部または外部のドメイン/IPアドレスの両方を可視化します。
- アクセスされるすべての種類のアプリケーション（HTTP、HTTPS、TCP、UDP）を包括的に可視化します。Citrix Enterprise Browser™およびCitrix Secure Accessエージェントがサポートされています。
- エンドユーザーがアクセスする、公開済みまたは未公開のドメイン/IPアドレスの両方を表示します。

次の図は、**アプリ検出**ページの例を示しています。**アプリ検出**ページでは、プロトコル（HTTP/HTTPS、TCP/UDP）およびドメイン/IPアドレスとポート番号に基づいてドメインをフィルタリングできます。また、エンドユーザーがアクセスした未公開（どのアプリにも割り当てられていない）ドメインも表示されます。

App configuration <u>App discovery</u> Security groups							
All protocol ▼ Last 1 Week ▼ + Add filter App discovery shows list of domains visited by end-users. Select one or more domains to add them to a new or existing application. 2 Selected ☐ View selected only Create application Add to an existing application							
	Domain/IP	Port	Protocol	Total Visits	Unique Users	Most Recent Visit	Assigned To App(S)
☐	meesho.com	443	HTTPS	3	1	2024-08-14 12:22:32	1
☐	www.google.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.googleadservices.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.bbc.com	443	HTTPS	1	1	2024-08-14 11:59:01	0
☐	myntra.in	443	HTTPS	1	1	2024-08-14 12:00:54	1
☐	www.apple.com	443	HTTPS	1	1	2024-08-14 12:00:54	0
☒	wikipedia.org	443	HTTPS	1	1	2024-08-14 12:16:21	0
☒	www.amazon.in	443	HTTPS	1	1	2024-08-14 12:16:21	0
☐	www.ajio.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	javatpoint.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	udemy.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	www.reddit.com	443	HTTPS	1	1	2024-08-14 12:22:32	0

新しい環境における内部ドメインのアプリケーション検出

新しいSecure Private Access環境をセットアップしていて、構成するアプリケーションを可視化したい場合に、アプリケーション検出機能を使用できます。この機能は、エンドユーザーがアクセスするすべてのドメイン/IPアドレスを検出し、一覧表示するため、それらをアプリケーションとして構成できます。Secure Private Access環境をセットアップする際に、アプリケーション検出機能を有効にするには、次の手順を使用します。

- 内部Webアプリケーションを検出するには、Secure Private Access内でアプリケーションを構成し、検出したいアプリケーションのドメイン/サブドメインに属するワイルドカード関連ドメインを指定します。

たとえば、ドメインcitrix.comを持つすべてのアプリケーションを検出したい場合、関連するワイルドカードドメインとして *.citrix.com を持つアプリケーションを作成します。アプリケーション構成を完了させるために、メインのWebアプリURLセクションに任意のテストURLを追加します。

App type * HTTP/HTTPS	App icon  Change icon (128 KB max, PNG)
App name * Discover_app1	☐ Do not display application icon in Workspace app
App description 	☐ Add application to favorites in Workspace app ☐ Allow user to remove from favorites ☐ Do not allow user to remove from favorites
App category ? Ex.: Category\SubCategory\SubCategory	
☐ Direct Access Enable direct browser-based access to internal web applications.	
URL * https://test.citrix.com	
Related Domains * ? *.docs.citrix.com	

WebアプリURL: 関連ドメイン:

- 内部TCP/UDPアプリの場合、Secure Private Access内でアプリケーションを構成し、サブネットとTCP/UDPプロトコルおよびポート範囲（全範囲を含めるには * を入力）を指定します。これにより、Citrix Secure AccessエージェントからすべてのTCPおよびUDPアプリを検出できます。たとえば、サブネット10.0.0.0/8内のすべてのアプリケーションを検出したい場合、次の詳細でアプリを構成します。例: 10.0.0.0/8:

ポート: (*)

プロトコル: TCP

アプリ検出2の構成(/en-us/citrix-secure-private-access/media/spa-app-discovery-2.png)

- アプリケーションを作成したら、構成済みのドメインとIPサブネットを持つアプリへのアクセスを許可するユーザーも定義する必要があります。アクセス ポリシーを作成し、作成したアプリケーションで構成されているFQDN/IPアドレスへのアクセスを許可するユーザーを割り当てます。これらは、最初のテストユーザーのセット、または最初にアクセスを許可したい限られた数のユーザーにすることができます。
- アプリケーションと対応するアクセス ポリシーを作成した後、ユーザーはCitrix Workspaceアプリから引き続きアプリケーションにアクセスし、さまざまなドメインにアクセスできます。エンドユーザーがアクセスしたすべてのFQDN/IPアドレスは、アプリケーション検出ページに表示され始めます。

注:

- 数日/数週間にわたってほとんどのアプリケーションを発見し特定したら、最初に作成したアプリケーションを削除することをお勧めします。これにより、ワイルドカードドメインとIPサブネットを介して付与された広範なアクセスを閉じることができ、検出された特定のアプリケーションURLとIPアドレスのみが新しいアプリケーションを介してアクセスを許可されるようにします。
- アプリ名にプレフィックス **Discover** を追加して、これが検出監視とレポートを有効にするための特別なアプリ構成であることを示します。この命名により、ワイルドカードドメインまたはIPサブネット、あるいはその両方を削除することを特定し、数週間または1か月後にアプリ全体のアクセスゾーンを特定のFQDNとIP/ポートの組み合わせのみに減らすことができます。
- TCP/UDPアプリにアクセスするには、ユーザーはCitrix Secure Accessエージェントを使用する必要があります。さまざまなアクセス方法からのアプリアクセスは、アプリのドメインとサブネット構成に基づいて監視され、**アプリ検出**ページ内で報告されます。
- 検出されたアプリケーションを削除した後でも、この機能はユーザーがアクセスしたドメイン/IPアドレスを検出し続けます。そのため、いつでも**アプリ検出**ページに戻って、何がアクセスされているか、およびアプリケーションとして構成する必要がある新しいドメイン/IPアドレスが検出されたかどうかを確認できます。

ドメイン、FQDN、またはIPアドレスの追加の詳細については、次のトピックを参照してください。

- [HTTP/HTTPSアプリケーションの構成](#)

- [TCP/UDPアプリの構成](#)

アプリ検出ページからアプリケーションを作成する

アプリ検出ページからメインドメインおよび未公開ドメインのアプリケーションを作成するには、次の手順を実行します。

1. 「**アプリケーション > アプリ検出**」に移動します。
2. リストからドメインを選択します。

注:

- 異なるプロトコルに属するドメインを選択してアプリケーションを作成することはできません。異なるプロトコルに属するドメインを選択すると、エラーメッセージが表示されます。
- ドメインがすでにアプリケーションに関連付けられている場合、そのドメインを再度選択してアプリケーションを作成することはできません。そのドメインに対応するチェックボックスはグレー表示され、チェックボックスにマウスを合わせるとツールヒントが表示されます。

3. 「**アプリケーションの作成**」をクリックします。アプリケーションの作成の詳細については、「[HTTP/HTTPSアプリケーションの構成](#)」および「[TCP/UDPアプリの構成](#)」を参照してください。

既存のアプリケーションを更新する

既存のアプリケーションにドメインを追加するには、次の手順を実行します。

1. アプリケーションに追加する必要があるドメインを選択します。
2. 「**既存のアプリケーションに追加**」をクリックします。
3. 「**アプリケーション**」で、これらのドメインを追加するアプリケーションを選択します。
4. 「**アプリの詳細を取得**」をクリックします。
5. 「**関連ドメイン**」フィールドには、以前に選択したすべてのドメインが別々の行に表示されます。
6. 「**完了**」をクリックします。

「アプリを更新」 (/en-us/citrix-secure-private-access/media/spaop-application-discovery2.png)

注：

- 既存のTCP/UDPアプリケーションにのみ、TCP/UDP宛先IPアドレスを追加できます。アプリケーションフィールドには、システムで構成されているTCP/UDPアプリのみが表示されます。
- 既存のHTTP/HTTPSまたはTCP/UDPアプリを選択して、プロトコルがHTTP/HTTPSであるドメイン（メインまたは単一エントリ）を追加できます。
- すでにアプリケーションに関連付けられているドメインを選択することはできません。

ポリシーモデリングツール

管理者は複数のポリシーを作成し、それらのポリシーを複数のアプリケーションに割り当てることができます。その結果、管理者がエンドユーザーのアプリケーションアクセス結果を理解することが困難になる場合があります。つまり、アプリケーションとアクセスポリシーの構成に基づいて、エンドユーザーがアクセスを許可されるか拒否されるかです。ポリシーモデリングツール（**アクセスポリシー > ポリシーモデリング**）は、管理者に予想されるアプリケーションアクセス結果（許可/制限付きで許可/拒否）を完全に可視化することで、これらの問題の解決に役立ちます。管理者は特定のユーザーのアクセス結果を確認し、コンテキストタグのユーザー条件を追加できます。このツールは、アプリケーションに関連付けられているポリシーのリストも表示します。

アクセスポリシーの構成を分析するには、次の手順を実行します。

1. Secure Private Accessコンソールで、**アクセスポリシー**をクリックし、**ポリシーモデリング**タブをクリックします。
2. 次の詳細を追加します。
 - **デバイスの種類**: デスクトップがデフォルトで選択されています。
 - **ドメイン**: ユーザーに関連付けられているドメインを選択します。
 - **ユーザー**: アプリケーションと関連ポリシーを分析するユーザー名を選択します。
3. エンドユーザーとそのデバイスのコンテキストタグに基づいて条件をシミュレートすることもできます。
 - a. **条件をシミュレート**をクリックします。コンテキストタグの条件がデフォルトで選択されています。
 - b. **値**にコンテキストタグを入力します。
 - c. ****+****記号をクリックして、他の条件を追加します。

4. 適用をクリックします。

選択したユーザーのアプリケーションと関連ポリシーが表形式で表示されます。

Policy configuration | Policy modeling

Model user access outcomes, given various contexts and conditions.

Device type: Desktop | Domain: spablr1.com | User name: spa user01

+ Simulate conditions | Contextual tags = term

Contextual tags: [dropdown] = (equals) term [trash icon]

Apply | Cancel | Clear filters

Display name: spa user01
Domain name: spablr1.com

Application access [filter icon]

Application Name	Result	Policy Name
avanthika	✓ Access will be allowed	avanthika_pol
buddi_nani	❌ No access policy found	N/A

Showing 1-2 of 2 items | Page 1 of 1 | 25 rows

データ損失防止 (DLP) ポリシーを構成する

アクセス制限は、CEP の Google 管理コンソールで構成されます。以前に Secure Private Access コンソールで構成されたアクセス制限は、Citrix Enterprise Browser にのみ適用されます。Google Chrome がエンタープライズブラウザである場合、アクセス制限は Google 管理コンソールでポリシーおよびルールとして構成する必要があります。

ポリシーは、**Google 管理コンソール > デバイス > Chrome > 設定** で構成されます。これらの設定により、JavaScript のブロックやプリンターの許可リストなど、ブラウザ設定を管理できます。

ルールは、**Google 管理コンソール > ルール** で構成されます。これらのルールは、透かしの追加、社会保障番号を含むファイルのダウンロードのブロック、URL フィルタリングなど、DLP に関連する高度な設定です。

Google Workspace 管理コンソールでのポリシーとルールの作成の詳細については、以下のトピックを参照してください。

- [Chrome Enterprise の Chrome Enterprise コネクタ ポリシーを設定する](#)
- [データ保護ルール](#)

高可用性展開

Secure Private Access の高可用性は、いくつかの簡単な手順で構成できます。

高可用性展開(/en-us/citrix-secure-private-access/media/spa-hybrid-ha-deployment.png)

データセンター内の高可用性

以下のセクションでは、データセンター内の高可用性について詳しく説明します。

NetScaler

高可用性を実現するには、[NetScaler 高可用性ペアを作成する](#) ことをお勧めします。これはアクティブ/パッシブの NetScaler ペアです。

アクティブな NetScaler がダウンした場合、パッシブな NetScaler は自動的にアクティブとして昇格され、すべてのユーザー トラフィックは新しいアクティブな NetScaler にルーティングされます。セッションも NetScaler 高可用性ペア間で同期されるため、ユーザーは再認証する必要はありません。

NetScaler HA ペアの詳細については、[高可用性](#) を参照してください。

クラウドコネクタ (Secure Private Access サーバー)

サービスグループ構成を使用して、Secure Private Access 用の NetScaler ロードバランサーを構成します。

1. **NetScaler で新しいサービスグループを作成する:** **構成 > トラフィック管理 > ロードバランシング > サービスグループ** に移動します。
2. **追加** をクリックします。
3. サービスグループの**名前**を入力します。例: `primary_spa_servers`。
4. ロードバランサーの種類 (**SSL** または **SSL_BRIDGE**) に応じて、サービスグループの適切な**プロトコル**を選択します。
5. 他のフィールドはデフォルト値のままにし、**OK** をクリックしてサービスグループを保存します。
6. **No Service Group Member** をクリックして、現在のデータセンターから Cloud Connector を追加します。
7. **IP Based** オプションを使用し、現在のデータセンターの Cloud Connector の **IP アドレスとポート**を追加します。デフォルトでは、Secure Private Access はポート **8443** を使用します。他のフィールドはデフォルト値のままにできます。
8. 追加の Cloud Connector を追加する必要がある場合は、この手順を繰り返します。
9. **Create** をクリックしてロードバランサーサービスを作成します。
10. **OK** をクリックしてサービスをサービスグループに追加します。

注:

オプションで、Secure Private Access サービスに HTTP モニターを追加できます。そのために、次の URL パスを使用できます。

`/secureAccess/health`

Secure Private Access が稼働している場合、**200 OK** が返されます。

11. **Done** をクリックします。
12. ロードバランサーを作成します。**Configuration > Traffic Management > Load Balancing > Virtual Servers** に移動します。
13. **Add** をクリックします。
14. ロードバランサー名を入力します。
15. 適切なプロトコル（例: **SSL** または **SSL_BRIDGE**）を選択します。
16. 「IPアドレスタイプ」を「IPアドレス」に、「ポート」を **443** に設定します。

「

注:

プロトコルはSSLまたはSSL_BRIDGEである必要があります。Secure Private Access ロードバランサーではHTTPタイプはサポートされていません。ポートは443である必要があります。カスタムHTTPSポートはサポートされていません。

17. 「**OK**」をクリックします。
18. 「ロードバランシング仮想サーバサービスグループバインディングなし」をクリックします。
19. 以前に作成したサービスグループを選択するにはクリックし、その後「**選択**」をクリックします。
20. 「**順序**」の値を「**10**」に設定します。「**バインド**」をクリックし、その後「**続行**」をクリックします。
21. **SSL**タイプのプロトコルを使用している場合は、「**サーバー証明書なし**」をクリックして、適切なサーバー証明書をバインドします。SSL_BRIDGEタイプのロードバランサーの場合、ロードバランサーにサーバー証明書は必要ありませんが、Secure Private Accessサービス用のCloud Connectorでサーバー証明書を構成する必要があります。詳細については、「Cloud ConnectorでのSecure Private Accessサービス用のTLS/SSL証明書の構成」([/ja-jp/citrix-secure-](#)

[private-access/hybrid/spa-hybrid-spa-service-configuration.html#configure-tlsssl-certificates-for-the-secure-private-access-service-on-cloud-connector](https://docs.citrix.com/en-us/private-access/hybrid/spa-hybrid-spa-service-configuration.html#configure-tlsssl-certificates-for-the-secure-private-access-service-on-cloud-connector))を参照してください。

これで、Secure Private Accessのサービスグループを使用したロードバランサーの構成は完了です。

ロードバランサー内のすべてのSecure Private Accessサーバーはアクティブです。1つのSecure Private Accessサーバーがダウンしても、他のSecure Private Accessサーバーがトラフィックを処理し続けるため、ユーザーには影響がありません。Secure Private Accessサーバーはステートレスであるため、永続性の要件はありません。

StoreFrontサーバー

StoreFrontサーバーも、同じデータセンター内でのフェイルオーバー中にSecure Private Accessサーバーと同様に動作します。

Secure Private Access 構成をリセットする

Citrix Enterprise Browser と統合された Citrix Secure Private Access ハイブリッド展開があり、Chrome Enterprise Premium に切り替えたい場合は、Secure Private Access 構成をリセットできます。この操作により、アプリケーションとアクセスポリシーを含む構成全体が削除されます。StoreFront と NetScaler の構成は手動でクリーンアップする必要があります。構成リセット後、Secure Private Access ハイブリッド展開を再度オンボーディングし、Chrome Enterprise Premium を選択できます。

構成をリセットする必要がある場合は、Citrix サポートにお問い合わせください。

可視性と監視

Secure Private Access は、Citrix DaaS の監視およびトラブルシューティングコンソールである Monitor と統合されています。管理者とヘルプデスク担当者は、Secure Private Access ダッシュボードに加えて、DaaS Monitor から Web/SaaS および TCP/UDP アプリのセッションとイベントを監視およびトラブルシューティングできます。

サービスエンタイトルメント

Secure Private Access で DaaS Monitor 機能を使用するには、Secure Private Access と DaaS の両方のエンタイトルメントが必要です。

サポートされるクライアント

- Citrix Workspace™ アプリ - 2409 以降
- シトリックス セキュア アクセス for Windows - 24.8.1.19 以降
- シトリックス セキュア アクセス for macOS - 24.10.1 以降

Monitor へのアクセス方法

Secure Private Access ダッシュボード (**Monitor に移動**) または Citrix DaaS™ サービスタイルから Monitor にアクセスできます。

Monitor ページで、ユーザーを検索してセッションを表示します。

セッションの定義

Secure Private Access セッションは、特定のデバイスにおけるエンドユーザーのセッションライフサイクル、アプリケーションアクティビティ、およびユーザーエクスペリエンスの包括的な概要を提供します。セッションは、次の側面への可視性を提供することで、トラブルシューティングと分析のための統合された記録として機能します。

- 起動ホップ、ネットワークトポロジ、接続、ルーティングの詳細など、アプリケーションへのアクセス方法に関する詳細なインサイト。これらの詳細は、アクセスポリシーに関連する問題を解決するために不可欠です。

- すべてのセッションアクティビティを追跡します。
 - WebまたはSaaSアプリケーションにアクセスするブラウザ。
 - TCP/UDPプロトコルを使用するプライベートアプリケーション向けのCitrix Secure Accessクライアント。

Secure Private Accessセッションの主な特徴は次のとおりです。

- 各セッションには、追跡と分析のための一意のIDが割り当てられます。
- 単一のセッションには複数のアプリ起動を含めることができ、その特定のセッション内のユーザーアクティビティの包括的なビューを提供します。
- 各アプリについて、セッションは以下を追跡します。
 - アプリに適用されるセキュリティ制御。
 - セキュリティ制御をトリガーしたポリシーの表示名とID。
 - ポリシーが適用された条件。
- セッションは、ユーザーがCitrix Enterprise Browser™でアクセスしたすべての内部ドメインを追跡し、セキュアな環境内でのユーザーナビゲーションに関する洞察を提供します。

Web/SaaSアプリセッション

Web/SaaSアプリのセッションの開始と終了は、次のように定義されます。

- 開始: Citrix WorkspaceアプリでCitrix Enterprise Browserが開き、アプリケーションにアクセスされます。
- 終了: セッションは次のシナリオで終了します。
 - Citrix Enterprise Browserを閉じます。
 - セッションアクティビティが報告されず、30分間非アクティブ状態が続いた場合。

Citrix Enterprise Browserクライアントは、15分ごとにセッションアクティビティをMonitorに送信します。このセッションアクティビティが30分間受信されない場合、次のような理由が考えられます。

- ネットワーク障害。
- インターネット接続の問題。
- セッションアクティビティがないまま30分が経過すると、セッションは自動的に閉じられます。

注:

ネイティブブラウザ（エージェントレス）を介して起動されたアプリの場合、セッションは120分間非アクティブ状態が続くと終了します。

TCP/UDPアプリセッション

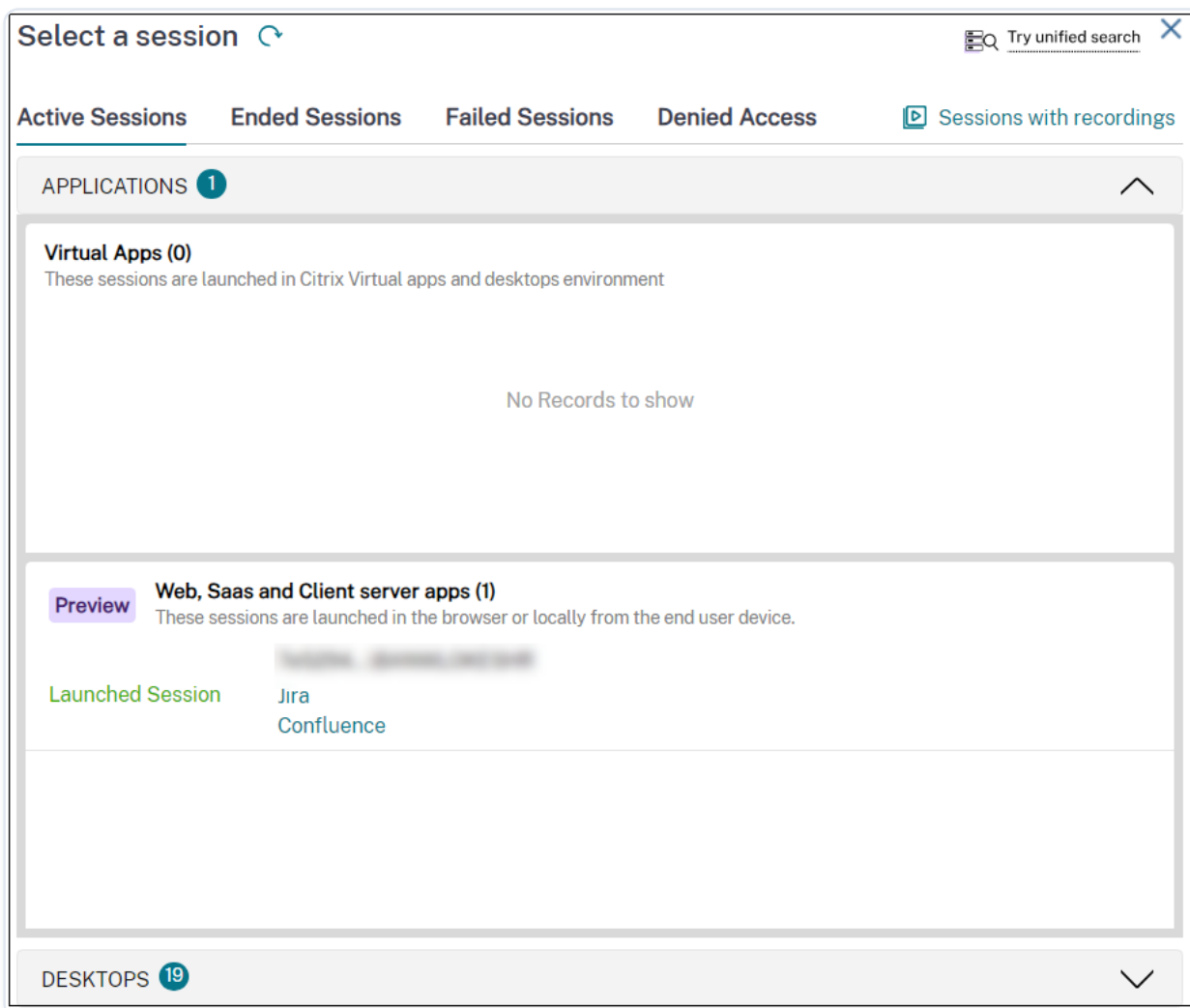
TCP/UDPアプリのセッションの開始と終了は、次のように定義されます。

- 開始: Citrix Secure Access™ クライアントにログインし、アプリにアクセスします。
- 終了: セッションは次のシナリオで終了します。
 - Citrix Secure Access クライアントからログアウトします。
 - セッションアクティビティが報告されず、30分間非アクティブ状態が続いた場合。

ユーザーセッションの表示

ユーザーセッションを表示するには、次の手順を実行します。

1. セッションを表示するには、ユーザーを検索します。
 - **セッションの選択**ページには、すべてのアクティブなセッションが表示されます。セッションが**アクティブなセッション**タブに見つからない場合は、**アクセス拒否**タブを確認してください。
 - **終了したセッション**タブと**失敗したセッション**タブは、Secure Private Accessには適用されません。



2. アクティブなセッションタブで、セッションIDをクリックしてセッションの詳細を表示します。

アクティビティマネージャーページが表示されます。

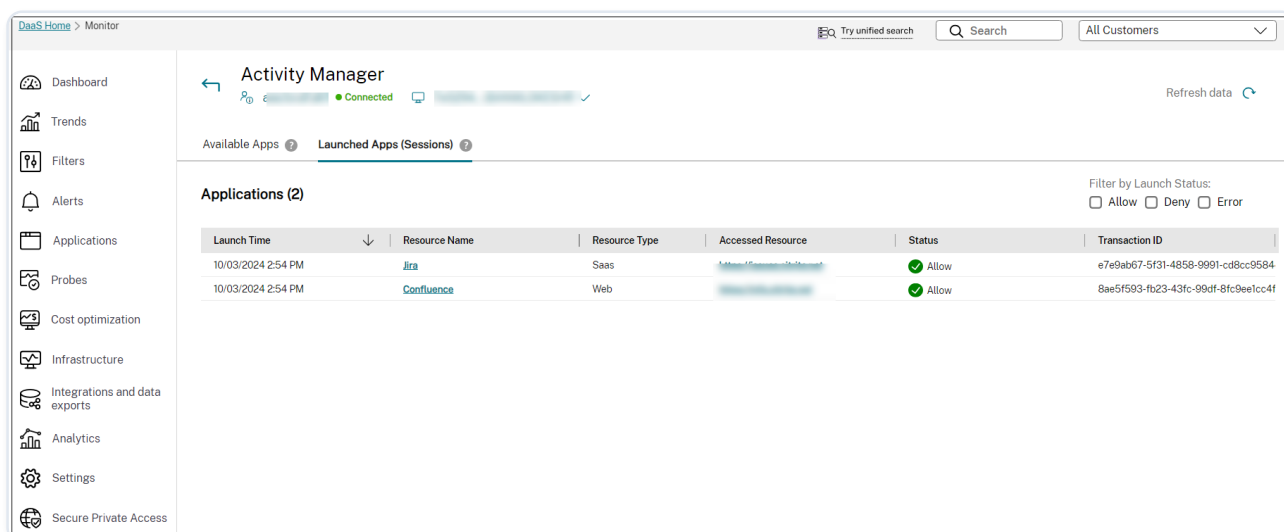
3. 次のいずれかのタブをクリックします。

- **起動されたアプリ:** ユーザーによって起動されたすべてのアプリケーションと、アクセスポリシー評価の結果（許可または拒否）を表示します。

同じセッションでアプリケーションが複数回アクセスされた場合、最新の起動詳細のみがキャプチャされます。

- **利用可能なアプリ:** このユーザーによって起動されたすべてのアプリケーションのアプリ列挙の詳細を表示します。
 - ユーザーに対してCitrix Workspaceアプリから複数の列挙要求が送信された場合、最新の列挙詳細のみがキャプチャされます。

- TCP/UDPアプリ（WebおよびZTNA）の場合、アプリ列挙の概念はありませんが、ユーザーに構成され関連付けられているすべてのアプリが**利用可能なアプリリスト**に表示されます。
- **利用可能なアプリリスト**には、Citrix Secure Accessクライアントを介して列挙される外部アプリは含まれません。これは、それらがSecure Private Accessによってトンネルされないためです。
- Citrix Secure Accessエージェントの場合、「**利用可能なアプリ**」リストには、内部WebおよびTCP/UDPアプリのみが表示されます。



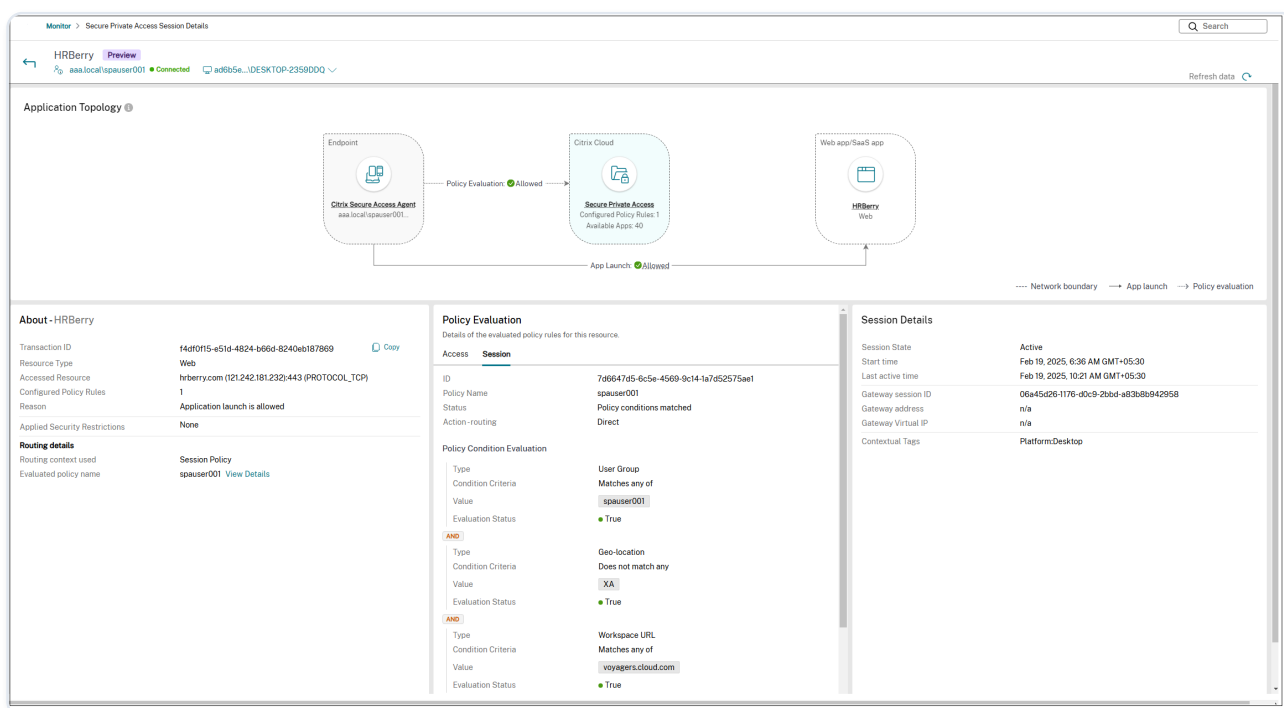
アプリケーションのトポロジ

起動済みアプリタブまたは利用可能なアプリタブからアプリをクリックすると、アプリケーションのトポロジページが表示され、アプリに関する完全な情報が表示されます。

- **セッショントポロジ:** アプリの起動フローを表示します。
- **概要:** アプリの種類、ポリシー規則の数、セキュリティ制限、アクセスされたリソースなど、アプリ関連の情報を表示します。**アクセスされたリソース** セクションに表示されるデータは、アプリの種類によって異なります。
 - SaaSアプリ - URLまたはアプリのFQDN
 - TCP/UDP – IPアドレス/FQDN、ポート、プロトコル
 - Webアプリ（Citrix Secure Accessクライアント経由で起動） - FQDN、ポート、プロトコル
 - Webアプリ（Citrix Workspaceアプリ経由で起動） - URL

- **ポリシー評価:** アクセスポリシーに関連する情報（ルール、アクション、条件など）を表示します。
- **セッションの詳細:** セッションの開始時刻と終了時刻、セッションの状態、ポリシーに関連付けられたコンテキストタグなど、セッションに関連する情報を表示します。
 - **アクセス済みドメインフィールド**はWeb/SaaSアプリにのみ適用され、Citrix Enterprise Browserクライアント（macOSおよびWindows）がセッションアクティビティを15分ごとに送信するため、15分後にのみ更新されます。
 - **利用可能なアプリタブ**からクリックされたアプリの場合、アプリの列挙はセッションに関連付けられていないため、**セッションの詳細列セクション**は空のままになります。

次の図は、正常に起動されたアプリのトポロジ図の例を示しています。



次の図は、アクセスが拒否されたアプリのトポロジ図の例を示しています。

Monitor > Secure Private Access Session Details

Search

← Yahoo finance ssb Preview

% aaa.local\spauser001 Connected adbb5e...DESKTOP-23580DQ ▾

Refresh data ↺

Application Topology ⓘ

Endpoint

Citrix Secure Access Agent
aaa.local\spauser001...

Policy Evaluation

○ Denied
App Launch: Denied

Citrix Cloud

Secure Private Access
Configured Policy Rules: 2
Available Apps: 40

No connection established

Resource Location

n/a

Connector Appliance

n/a

Yahoo finance ssb

Web

--- Network boundary → App launch → Policy evaluation

About - Yahoo finance ssb

Transaction ID f7adc56c-3462-4c62-bf29-9bf592a36fe6 Copy

Resource Type Web

Accessed Resource finance.yahoo.com (180.222.114.12):443 (PROTOCOL_TCP)

Configured Policy Rules 2

Reason Application Launch was denied because of a policy

Applied Security Restrictions None

Routing details

Routing context used Access Policy

Evaluated policy name Yahoo finance ssb

Policy Evaluation

Details of the evaluated policy rules for this resource.

Access Session

This policy was setup to deny access if conditions match.

ID 50eb9857-41e7-4d76-bf29-c24a0c179490

Policy Name Yahoo finance ssb

Rule Name r

Status Policy conditions matched

Action applied Denied Access

Action-routing n/a

Policy Condition Evaluation

Type User Group

Condition Criteria Matches any of

Value spauser001

Evaluation Status True

Session Details

Session State Active

Start time Feb 19, 2025, 6:36 AM GMT+05:30

Last active time Feb 19, 2025, 10:19 AM GMT+05:30

Contextual Tags PlatformDesktop

トリアージとトラブルシューティング

このトピックでは、Citrix Secure Private Accessに関連する問題を効果的にトラブルシューティングおよびトリアージするための重要な考慮事項と手順について概説します。管理者はこのドキュメントを、問題の特定、診断、解決、およびユーザーへのシームレスで安全なアクセスの確保のためのガイドとして使用できます。

シトリックス セキュア アクセス モードにおけるユーザー/クライアントの問題

以下のセクションでは、Citrix Secure Accessモードでのユーザー/クライアントの問題に関する詳細情報を提供します。

ユーザーがログインできない

確認事項:

- VPN仮想サーバーと認証仮想サーバーがUPしていることを確認します。

```
> show vpn vsriver _spa_cep_csa_vpn_vs_10.8.0.35
 spa_cep_csa_vpn_vs_10.8.0.35 (10.8.0.35:443) - SSL      Type: CONTENT
 State: UP

> show authentication vsriver authvs
 authvs (0.0.0.0:0) - SSL      IPSet: ???      Type: CONTENT
 State: UP  ARP:DISABLED
```

- Secure Private AccessプロファイルのURLステータスがUPしていることを確認します。

```
> show vpn securePrivateAccessProfile _spa_cep_csa_profile
1)      Name: _spa_cep_csa_profile
        URL: https://stg4spalb.spagwcep.corp [Status: UP]
```

- Secure Private Access管理コンソールで、アプリとアクセスポリシーがユーザーに対して正しく構成されていることを確認します。「[アプリの構成と管理](#)」および「[アプリケーションのアクセスポリシーの構成](#)」を参照してください。
- ロードバランサー仮想サーバーのステータスを確認し、すべてのコネクタサーバーが追加され、UPしていることを確認します。

- nFactor認証の問題をトラブルシューティングするには、「[認証、承認、および監査の問題のトラブルシューティング](#)」を参照してください。

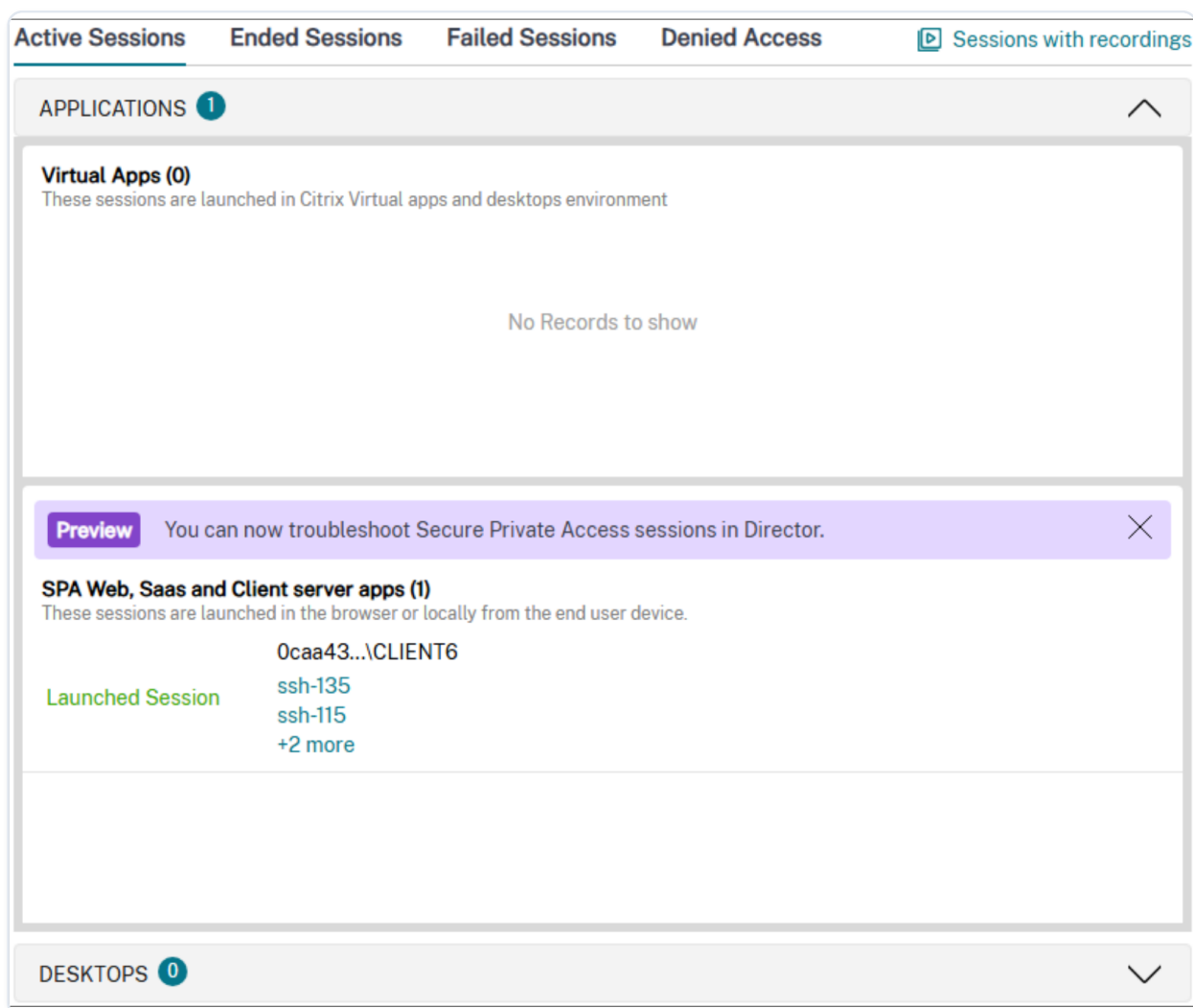
前述の内容を確認した後、以下を実行します。

1. デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集します。
2. CSAクライアントで詳細ログを有効にし、クライアントログを収集します。
3. Citrixサポートに連絡し、収集した診断情報を提供してください。

ユーザーがアプリを起動できない

確認事項:

- In Citrix Monitor, search for the user UPN and verify that an active Secure Private Access session exists.



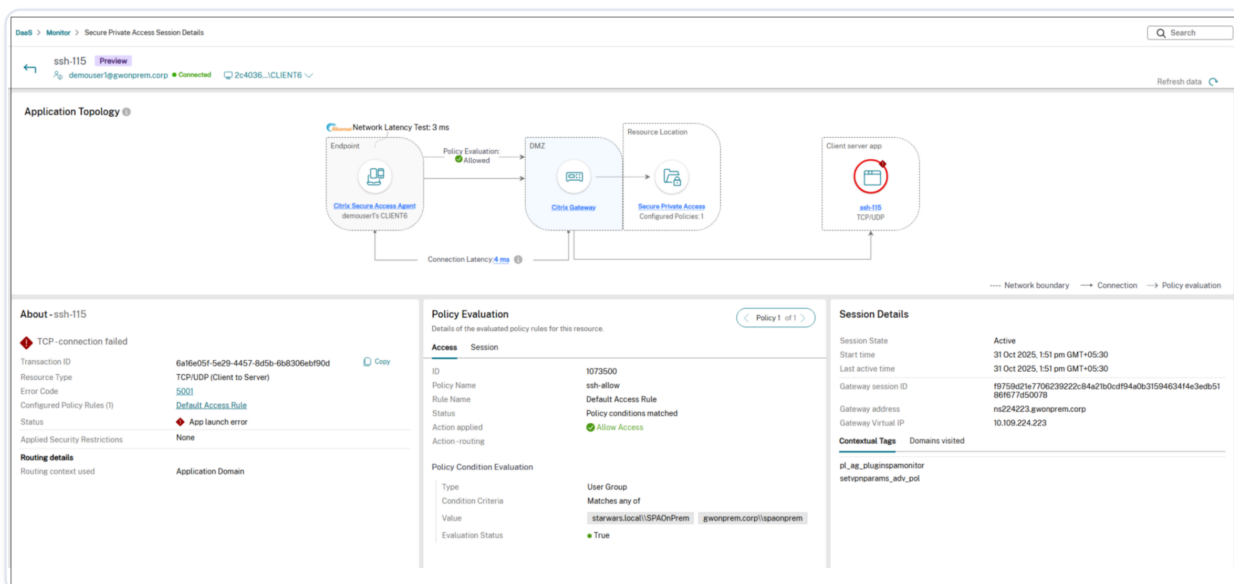
- 起動されたアプリは、**Available apps**の下に表示される必要があります。

- 。アプリの**App Launch Allow**イベントが**Launched apps**の下に表示されている必要があります。

The screenshot shows the 'Activity Manager' interface with a table of 'Launched Apps (Sessions)'. The table has columns for Launch Time, Resource Name, Resource Type, Accessed Resource, Spa Pop Name, Gateway Pop Name, Status, and Transaction ID. The status for the first two rows is 'Success (App Launch)'.

Launch Time	Resource Name	Resource Type	Accessed Resource	Spa Pop Name	Gateway Pop Name	Status	Transaction ID
10/31/2025 1:38 PM	ssh-115	TCP/UDP (Client to Server)	10.102.32.101:22 / 192.168.1.101:22	ns224223.gwoprem corp	ns224223.gwoprem corp	Success (App Launch)	18f94304-7549-4d34-e033-e376a45a360f
10/31/2025 1:38 PM	ssh-115	TCP/UDP (Client to Server)	10.102.32.101:22 / 192.168.1.101:22	ns224223.gwoprem corp	ns224223.gwoprem corp	Success (App Launch)	768b253-847f-489a-b5d6-99436094ac1f
10/31/2025 1:38 PM	JIRA	Web	https://jira.itsm.net	ns224	ns224		
10/31/2025 1:38 PM	Code	Web	https://code.itsm.net				
10/31/2025 1:38 PM	JIRA	Web	https://jira.itsm.net				
10/31/2025 1:38 PM	ssh-115	TCP/UDP (Client to Server)	10.102.32.101:22 / 192.168.1.101:22				
10/31/2025 1:38 PM	Info	Web	https://info.itsm.net				

- 。存在しない場合は、Secure Private Access管理コンソールで、アプリとアクセスポリシーがユーザーに対して正しく構成されていることを確認してください。
- Citrix Monitorで、**Launched apps**の下にあるアプリのアプリ起動エラーイベントを探します。



- 。一般的なエラー: DNS解決の失敗/TCP接続の失敗。
- 。NetScaler CLIから、適切なSNIPからのアプリへの接続を確認します。

デバッグレベルのログを含むNetScalerサポートバンドルを収集する手順

1. CLIからデバッグレベルのsyslogを設定します。

```
set syslogparams loglevel ALL DEBUG
```

2. ShellからSecure Private Access固有の詳細ログを有効にします。

```
nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=1
```

3. サポートバンドル（およびオプションのトレース）を収集します。
4. 標準的な方法を使用してNetScalerサポートバンドルを収集します。
5. サポートから要求された場合は、オプションで追加のトレースをキャプチャします。

重要:

バンドルを収集した後、詳細ログを元に戻します。詳細ログを有効にしたままにすると、過剰なログが生成され、パフォーマンスに影響を与える可能性があります。収集が完了したら、必ず詳細ログを元に戻してください。

詳細ログを元に戻す

1. CLIからsyslogレベルを復元します。

```
set syslogparams loglevel ALL
```

2. ShellからSecure Private Access固有の詳細ログを無効にします。

```
nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=0
```

追加の参照:

- NetScaler®インスタンスログのテクニカルサポートバンドルを生成する方法(<https://docs.netscaler.com/ja-jp/netscaler-console-service/networks/instance-management/generate-techsupport-bundle.html>)
- NetScalerでパケットトレースを記録する方法(<https://docs.netscaler.com/ja-jp/citrix-adc/current-release/system/troubleshooting-citrix-adc/how-to-record-a-packet-trace-on-citrix-adc.html>)

トラブルシューティングに役立つツール

- 構成レポート(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-manage-settings-post-onboarding.html#configuration-report>)
- コンポーネントアナライザー(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-component-analyzer.html>)
- ポリシーモデリング(</ja-jp/citrix-secure-private-access/hybrid/spa-policy-modeling-tool.html>)

クライアントログを収集する

以下のセクションでは、クライアントログの収集に関する詳細情報を提供します。

クローム エンタープライズ プレミアム ログ

Chrome Enterprise Premium でクライアント側の問題が発生した場合は、Secure Enterprise Browser と Citrix Secure Access の両方の拡張機能ログを収集してください。

Secure Enterprise Browser 拡張機能のログをキャプチャする手順

1. Chrome ブラウザを開きます。
2. 管理対象の Chrome プロファイルに切り替えます。
3. **拡張機能**アイコンをクリックし、**拡張機能を管理**を選択します。

拡張機能を管理(/en-us/citrix-secure-private-access/media/spa-hybrid-manage-extensions.png)

4. Secure Enterprise Browser の下で、**詳細**をクリックします。

詳細(/en-us/citrix-secure-private-access/media/spa-hybrid-secure-browser.png)

1. **拡張機能オプション**を選択します。

拡張機能オプション(/en-us/citrix-secure-private-access/media/spa-hybrid-extension-option.png)

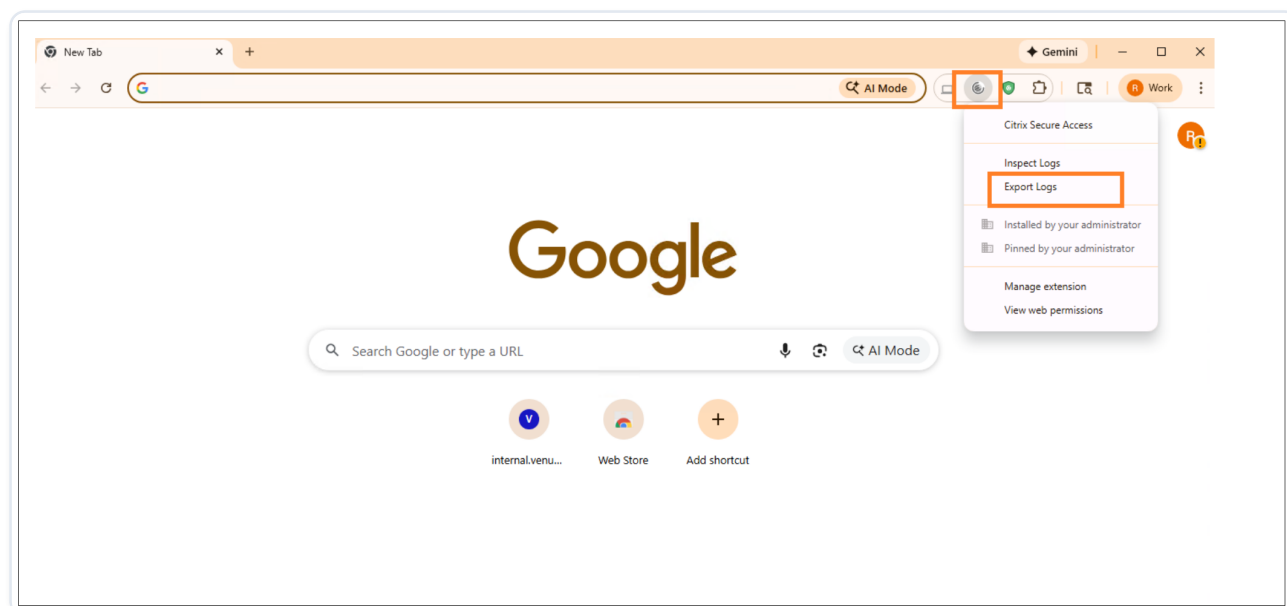
1. **ログをダウンロード**をクリックします。

ログをダウンロード(/en-us/citrix-secure-private-access/media/spa-hybrid-download-logs.png)

1. ダウンロードしたログファイルをコンピューターに保存します。

Citrix Secure Access Extension のログをキャプチャする手順

1. Chrome ブラウザを開きます。
2. 管理対象の Chrome プロファイルに切り替えます。
3. アドレスバーの横にある **Citrix Secure Access extension** アイコンをクリックします。
4. **ログのエクスポート**を選択します。



1. エクスポートしたログファイルをコンピューターに保存します。

Monitorを使用したリアルタイムセッションのトラブルシューティング

管理者は、Monitorコンソールを使用して、Secure Private Accessセッションをリアルタイムで監視し、トラブルシューティングできます。

関連情報については、次のトピックを参照してください。

- Secure Private AccessとMonitorの統合については、「[DaaS Monitorとの統合](#)」を参照してください。
- MonitorでSecure Private Accessユーザーセッションを検索して、トラブルシューティングとレポート作成のために特定のセッションをすばやく見つけることができます。詳しくは、「[ユーザー別のSecure Private Accessセッションの表示](#)」を参照してください。
- Monitorの詳細については、「[DaaS Monitor](#)」を参照してください。

Secure Private Accessハイブリッド展開では、次のエラーコードがキャプチャされます。

- セッションコード
- アプリ列挙メッセージコード
- アプリ起動メッセージコード
- アプリ起動エラーコード

セッションコード

コード	ステータス	説明
2101	失敗	セッションの失敗
2102	アクティブ/非アクティブ/失敗	セッションがアクティブであるか、終了しているか、またはセッション内の少なくとも1つのアプリ起動が失敗しました
2000	アクティブ	セッションはアクティブです
2001	非アクティブ	セッションは終了/非アクティブです

アプリ列挙メッセージコード

コード	ステータス	説明
1000	成功	列挙は成功しました。少なくとも1つのアプリが列挙されました。
1001	成功	すべてのアプリケーションがポリシーによって拒否されたため、列挙されませんでした。
1002	成功	一致するポリシーがなかったため、アプリケーションは列挙されませんでした。
1003	成功	一部のアプリケーションは拒否され、その他は一致するポリシーがなかったため、アプリケーションは列挙されませんでした。
1004	成功	評価するポリシーがないため、アプリケーションは列挙されませんでした。

コード	ステータス	説明
1101	失敗	列挙中に内部エラーが発生しました。
1102	失敗	いくつかのアプリケーションは列挙されましたが、少なくとも1つのアプリ評価が失敗しました。
1103	失敗	アプリケーションは列挙されず、少なくとも1つのアプリ評価が失敗しました。
3000	許可	アプリケーションの列挙は許可されています。
3001	拒否	ポリシーによりアプリケーションの列挙が拒否されました
3002	拒否	一致するポリシーがなかったため、アプリケーションは列挙されませんでした
3003	不明	アプリケーションの列挙ステータスが不明です
3004	CEBからのアプリケーション起動	Citrix Enterprise Browser™からのアプリケーション起動試行
3101	失敗	アプリケーションの列挙 - 内部エラーが発生しました（現在未使用）
3102	失敗	ポリシー評価中に例外が発生したため、アプリケーションは列挙されませんでした
3103	失敗	アプリケーションの列挙ステータスがnullです - ポリ

コード	ステータス	説明
		シー評価中に内部エラーが発生しました
3104	許可/拒否/失敗	アプリのポリシー詳細の取得中にエラーが発生しました

アプリ起動メッセージコード

コード	ステータス	説明
4000	許可	アプリケーションの起動が許可されています
4001	拒否	ポリシーによりアプリケーションの起動が拒否されました
4002	拒否	一致するポリシーがなかったため、アプリケーションの起動が拒否されました
4101	失敗	アプリケーション起動エラー - アプリケーション起動中に内部エラーが発生しました
4102	失敗	アプリケーション起動エラー (内部)
4103	許可/拒否/失敗	アプリのポリシー詳細の取得中にエラーが発生しました
4104	失敗	アプリケーション起動エラー - アプリケーション構成が見つかりません

アプリケーション起動エラーコード

コード	説明	解決策/回避策
5001	TCP - 接続に失敗しました	宛先へのネットワーク到達可能性を確認します (NetScaler

コード	説明	解決策/回避策
5003	TCP - プロープに失敗しました	Gateway から <code>-S <SNIP></code> を ping します。 ^
5002	TCP - プロキシサーバーがダウンしています	プロキシホストが稼働していることを確認してください。
5004	TCP - ゲートウェイでのメモリ割り当てに失敗しました	デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集します。
5005	TCP - サーバーがダウンしています	宛先へのネットワーク到達可能性を確認し (NetScaler Gatewayから <code>-S <SNIP></code> を ping します)、サーバーがダウンしているか確認します。
5006	TCP - プロキシ接続に失敗しました	プロキシホストが稼働しており、接続を受け入れていることを確認します。
5007	TCP - プロキシプロープに失敗しました	宛先へのネットワーク到達可能性を確認し (NetScaler Gatewayから <code>-S <SNIP></code> を ping します)。デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集します。
5008	SPA - サーバーがダウンしています	Secure Private AccessサイトのURLが稼働していることを確認します。(NetScaler CLI で <code>show vpn securePrivateAccessProfile</code> CLI コマンドを使用して URL ステータスを確認します)。
5009	SPA - コールアウト要求エラー	Secure Private AccessサイトのURLが稼働していることを確認してください。デバッグ

コード	説明	解決策/回避策
5010	SPA - コールアウト応答エラー	レベルのログを有効にし、NetScalerからサポートバンドルを収集してください。 ^
5011	TCP - セッションの有効期限切れ	これは、ユーザーセッションがアクティブでなくなったときにアプリにアクセスされたことを示します。新しいアクティブなユーザーセッションを開始してください。
5013	TCP - ゲートウェイ内部エラー	デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集してください。
5014	TCP - DNSサーバーがダウンしています	DNSサーバーが稼働していることを確認してください。
5015	TCP - ゲートウェイ DNS 内部エラー	DNSサーバーが稼働していることを確認してください。デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集してください。
5016	宛先サーバーへの接続に失敗しました	宛先へのネットワーク到達性を確認してください (NetScaler Gatewayからping -S <SNIP> を実行)。
5017	宛先サーバーのDNS解決に失敗しました	アプリケーションが使用するホスト名が、意図したDNSサーバー (内部DNSかパブリックDNSか) によって解決されることを確認してください。
5018	ゲートウェイ内部エラー	デバッグレベルのログを有効にし、NetScalerからサポー

コード	説明	解決策/回避策
		トバンドルを収集してください。
0x1300000C	アプリケーションドメインのDNS解決に失敗しました	アプリケーションが使用するホスト名が、意図したDNSサーバー (内部DNSかパブリックDNSか) によって解決されることを確認してください。

エンドユーザーエクスペリエンス

以下のセクションでは、エンドユーザーエクスペリエンスに関する詳細情報を提供します。

Chrome Enterprise Premium を使用した Web および SaaS アプリケーションへのアクセス

Chrome Enterprise Premium を使用して、公開されている社内 Web アプリケーションおよび外部 SaaS アプリケーションに 4 つの異なる方法でアクセスできます。お使いの環境に適用されるオプションを選択してください。

オプション 1: 管理対象の Chrome プロファイルを作成し、アプリに直接アクセスする (推奨)

- Chrome ブラウザを開きます。
- 会社の資格情報を使用して新しい Chrome プロファイルを追加します (つまり、管理対象の Chrome プロファイルを作成します)。

新しい Chrome プロファイル(/en-us/citrix-secure-private-access/media/spa-hybrid-new-chrome-profile.png)

- プロファイルが作成されると、2 つの拡張機能が自動的にインストールされます。
 - シトリックス セキュアアクセス
 - セキュア エンタープライズ ブラウザ

インストールされた拡張機能(/en-us/citrix-secure-private-access/media/spa-hybrid-extensions.png)

- アドレスバーに URL を入力するか、公開されているサイトに移動して、社内および外部アプリケーションにアクセスします。
- URL を手動で入力した場合の動作:
 - **社内 Web アプリ (許可):**

リクエストは Secure Private Access を介して安全にトンネルされ、サイトがロードされます。

内部Webアプリへのアクセス(/en-us/citrix-secure-private-access/media/spa-hybrid-internal-app-access.png)

◦ **内部Webアプリ（拒否）：**

Secure Private Access はリクエストをブロックし、「アクセス制限」ページが表示されます。

拒否された内部Webアプリへのアクセス(/en-us/citrix-secure-private-access/media/spa-hybrid-internal-app-access-denied.png)

◦ **外部SaaSアプリ（許可）：**

リクエストはトンネリングなしで直接許可されます。

◦ **外部SaaSアプリ（拒否）：**

Secure Private Access はリクエストをブロックし、「アクセス制限」ページが表示されます。

オプション2：既存の管理対象ChromeプロファイルでストアURLにアクセスする

- 会社の資格情報を持つ管理対象Chromeプロファイルが既に存在することを確認してください。
- 正しい会社管理プロファイルでChromeを起動します。
- WebブラウザでストアURLを開きます。
- ストアにログインします。
- 「アプリ」タブに移動し、会社の管理者が公開したWeb/SaaSアプリを選択します。

公開済みアプリ(/en-us/citrix-secure-private-access/media/spa-hybrid-published-apps.png)

- Web/SaaSアプリは、同じ管理対象Chromeプロファイル内の新しいタブでシームレスに起動します。

アプリの起動(/en-us/citrix-secure-private-access/media/spa-hybrid-app-launch.png)

- 許可および拒否ロジックは、[オプション1](#)と同じです。

オプション3：管理対象外のChromeプロファイルまたはChrome以外のブラウザ（Edge、Firefox）からストアURLにアクセスする

- Edge、Firefox、または管理対象外のChromeプロファイルを起動します。
- WebブラウザでストアURLを開きます

- ストアにログインします。
- アプリタブに移動し、公開されているWebアプリを選択します。
- ポップアップが表示され、**Citrix Workspaceを開く**ボタンが表示されたダイアログが表示されます。続行するには、このボタンをクリックします。

Workspaceポップアップ(/en-us/citrix-secure-private-access/media/spa-hybrid-workspace-popup.png)

- ボタンをクリックすると、次のいずれかが発生します。
 - **管理対象Chromeプロファイルが既に存在する場合**：アプリは管理対象プロファイルで直接起動します。

既存のChromeプロファイル(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-exist.png)

- **管理対象Chromeプロファイルが存在しない場合**：アプリの起動前に、管理対象Chromeプロファイルを作成するよう求められます。

Chrome プロファイルを作成(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-create.png)

- 許可および拒否ロジックは、[Option 1](#) と同じです。

オプション 4: Citrix Workspace アプリを介してアプリにアクセスする

- Citrix Workspace アプリを使用して StoreFront ストアを開きます。
- ストアにログインします。
- アプリタブに移動し、公開されている Web アプリを選択します。
- Workspace アプリは Chrome を自動的に起動します。設定に応じて、次のようになります。
 - **管理対象の Chrome プロファイルが存在する場合**：アプリは管理対象プロファイルで直接開きます。

既存の Chrome プロファイル(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-exist.png)

- **管理対象の Chrome プロファイルが存在しない場合**：アプリが開く前に、プロファイルの作成を求められます。

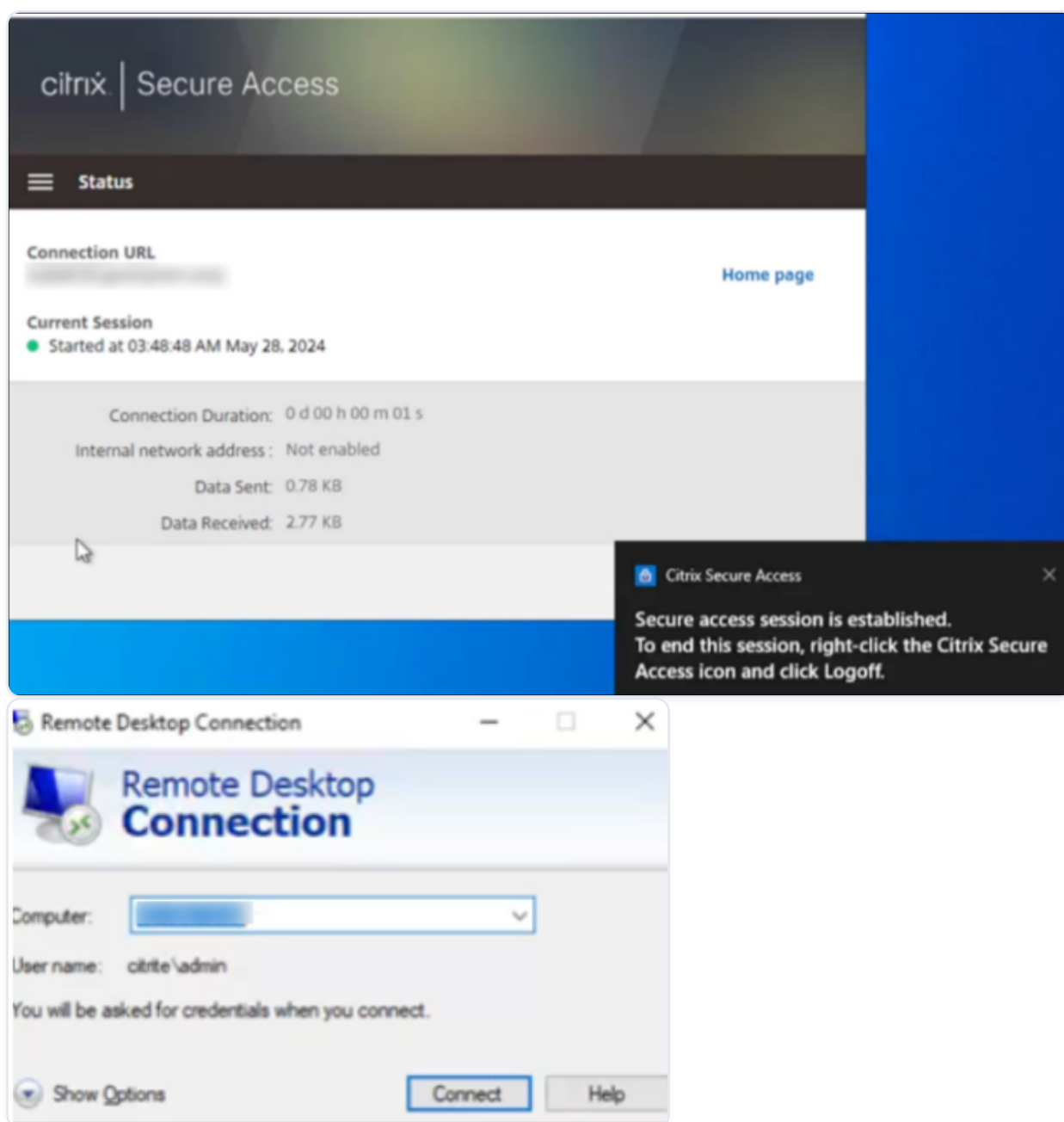
Chrome プロファイルを作成(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-create.png)

- 許可および拒否ロジックは、Option 1 と同じです。

クライアント/サーバー (TCP/UDP) アプリケーションへのアクセス

RDP が構成されている場合、エンドユーザーは TCP/UDP アプリにアクセスするために次の手順を実行する必要があります。

1. Citrix Secure Access クライアントにログインします。
2. セキュアアクセスセッションが確立されたら、リモートデスクトップ接続を開始します。



- a. Windowsキーを押し、「リモートデスクトップ接続」と入力してEnterキーを押します。

- b. 接続しようとしているコンピューターのIPアドレスまたはホスト名を入力します。
- c. 「**接続**」をクリックします。資格情報の入力を求められる場合があります。
- d. リモートコンピューターのユーザー名とパスワードを入力し、「**OK**」をクリックします。

これでリモートデスクトップ接続が確立され、エンドユーザーはリモートコンピューターと対話できます。

index

- [DaaSモニターとの統合](#)
- [コンテキストタグ](#)

DaaSモニターとの統合

Secure Private Accessは、Citrix DaaSの監視およびトラブルシューティングコンソールであるMonitorと統合されています。管理者とヘルプデスク担当者は、Secure Private Accessダッシュボードに加えて、DaaS MonitorからWeb/SaaSおよびTCP/UDPアプリのセッションとイベントを監視およびトラブルシューティングできます。

サービスエンタイトルメント

Secure Private AccessでDaaS Monitor機能を使用するには、Secure Private AccessとDaaSの両方のエンタイトルメントが必要です。

サポートされているクライアント

- Citrix Workspace™ アプリ - 2409以降
- Citrix セキュアアクセス (Windows版) - 24.8.1.19以降
- Citrix セキュアアクセス (macOS版) - 24.10.1以降

Monitorへのアクセス方法

Monitorには、Secure Private Accessダッシュボード（**Monitorに移動**）またはCitrix DaaS™ サービススタイルからアクセスできます。

Monitorページで、ユーザーを検索してセッションを表示します。

セッションの定義

Secure Private Accessセッションは、エンドユーザーのセッションライフサイクル、アプリケーションアクティビティ、および特定のデバイスでのユーザーエクスペリエンスの包括的な概要を提供します。セッションは、次の側面を可視化することで、トラブルシューティングと分析のための統合された記録として機能します。

- アプリケーションへのアクセス方法に関する詳細な洞察。これには、起動ホップ、ネットワークポロジ、接続、ルーティングの詳細が含まれます。これらの詳細は、アクセスポリシーに関連する問題を解決するために不可欠です。
- すべてのセッションアクティビティを追跡します。
 - WebまたはSaaSアプリケーションにアクセスするブラウザ。
 - TCP/UDPプロトコルを使用するプライベートアプリケーション用のCitrix Secure Accessクライアント。

Secure Private Accessセッションの主な特徴は次のとおりです。

- 各セッションには、追跡と分析のために一意のIDが割り当てられます。
- 1つのセッションには複数のアプリ起動を含めることができ、その特定のセッション内でのユーザーアクティビティの包括的なビューを提供します。
- 各アプリについて、セッションは以下を追跡します。
 - アプリに適用されるセキュリティ制御。
 - セキュリティ制御をトリガーしたポリシーの表示名とID。
 - ポリシーが適用される原因となった条件。
- セッションは、ユーザーがCitrix Enterprise Browser™でアクセスしたすべての内部ドメインを追跡し、セキュアな環境内でのユーザーナビゲーションに関する洞察を提供します。

Web/SaaSアプリセッション

Web/SaaSアプリのセッションの開始と終了は、次のように定義されます。

- 開始: Citrix WorkspaceアプリでCitrix Enterprise Browserが開き、アプリケーションにアクセスされます。
- 終了: セッションは次のシナリオで終了します。
 - Citrix Enterprise Browserを閉じます。
 - 30分間アクティビティがなく、セッションアクティビティが報告されない場合。

Citrix Enterprise Browserクライアントは、15分ごとにセッションアクティビティをMonitorに送信します。このセッションアクティビティが30分間受信されない場合、次のような理由が考えられます。

- ネットワーク障害。
- インターネット接続の問題。

- 。セッションアクティビティがないまま30分が経過すると、セッションは自動的に閉じられます。

注：

ネイティブブラウザ（エージェントレス）を介して起動されたアプリの場合、120分間アクティビティがないとセッションは終了します。

TCP/UDPアプリセッション

TCP/UDPアプリのセッションの開始と終了は、次のように定義されます。

- 開始：Citrix Secure Access™ クライアントにログインし、アプリにアクセスします。
- 終了：セッションは次のシナリオで終了します。
 - Citrix Secure Accessクライアントからログアウトします。
 - 30分間アクティビティがなく、セッションアクティビティが報告されない場合。

ユーザーセッションの表示

ユーザーセッションを表示するには、次の手順を実行します。

1. ユーザーを検索してセッションを表示します。
 - 「**セッションの選択**」ページには、すべてのアクティブなセッションが表示されます。「**アクティブなセッション**」タブでセッションが見つからない場合は、「**アクセス拒否**」タブを確認してください。
 - 「**終了したセッション**」タブと「**失敗したセッション**」タブは、Secure Private Accessには適用されません。

セッションの選択(/en-us/citrix-secure-private-access/media/spa-select-a-session-success.png)

2. 「**アクティブなセッション**」タブで、セッションIDをクリックしてセッションの詳細を表示します。

「**アクティビティマネージャー**」ページが表示されます。

3. 次のいずれかのタブをクリックします。
 - **起動されたアプリ**: ユーザーが起動したすべてのアプリケーションと、アクセスポリシー評価の結果（許可または拒否）を表示します。

同じセッションでアプリケーションが複数回アクセスされた場合、最新の起動詳細のみがキャプチャされます。

- **利用可能なアプリ:** このユーザーによって起動されたすべてのアプリケーションのアプリ列挙の詳細を表示します。
 - ユーザーに対してCitrix Workspaceアプリから複数の列挙リクエストが送信された場合、最新の列挙詳細のみがキャプチャされます。
 - TCP/UDPアプリ（WebおよびZTNA）の場合、アプリ列挙の概念はありませんが、ユーザーに構成され関連付けられているすべてのアプリが「**利用可能なアプリ**」リストに表示されます。
 - 「**利用可能なアプリ**」リストには、Citrix Secure Accessクライアントを介して列挙される外部アプリは含まれません。これは、それらがSecure Private Accessによってトンネルされないためです。
 - Citrix Secure Accessエージェントの場合、**利用可能なアプリ**リストには、内部WebアプリとTCP/UDPアプリのみが表示されます。

アクティビティマネージャー(/en-us/citrix-secure-private-access/media/spa-monitor-activity-manager.png)

アプリケーションのトポロジ

「**起動済みアプリ**」または「**利用可能なアプリ**」タブからアプリをクリックすると、アプリケーションのトポロジページが表示され、アプリに関する完全な情報が表示されます。

- 「**セッショントポロジ:**」 アプリの起動フローを表示します。
- **概要:** アプリの種類、ポリシー規則の数、セキュリティ制限、アクセスされたリソースなど、アプリ関連の情報を表示します。「**アクセスされたリソース**」セクションに表示されるデータは、アプリの種類によって異なります。
 - SaaSアプリ - URLまたはアプリのFQDN
 - TCP/UDP – IPアドレス/FQDN、ポート、プロトコル
 - Webアプリ (Citrix Secure Accessクライアント経由で起動) - FQDN、ポート、プロトコル
 - Webアプリ (Citrix Workspaceアプリ経由で起動) - URL
- 「**ポリシー評価:**」 規則、アクション、条件など、アクセスポリシーに関連する情報を表示します。
- 「**セッションの詳細:**」 セッションの開始時刻と終了時刻、セッションの状態、ポリシーに関連付けられたコンテキストタグなど、セッションに関連する情報を表示します。

- 。「アクセス済みドメイン」フィールドは、Web/SaaSアプリにのみ適用され、macOSおよびWindows上のCitrix Enterprise Browserクライアントが15分ごとにセッションアクティビティを送信するため、15分後にのみ更新されます。
- 。「利用可能なアプリ」タブからクリックされたアプリの場合、「セッションの詳細」列セッションは空のままになります。これは、アプリの列挙がセッションに関連付けられていないためです。

次の図は、正常に起動されたアプリのトポロジ図の例を示しています。

起動されたアプリのアプリケーションのトポロジ(/en-us/citrix-secure-private-access/media/spa-monitor-application-topology-allow-access.png)

次の図は、アクセスが拒否されたアプリのトポロジ図の例を示しています。

アクセス拒否されたアプリのアプリケーション トポロジ(/en-us/citrix-secure-private-access/media/spa-monitor-application-topology-denied-access.png)

コンテキストタグ

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

管理者は、アクセスポリシーにコンテキストタグ付きの条件を追加できます。Secure Private Accessプロバイダー上のコンテキストタグは、認証済みユーザーのセッションに適用されるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。

Secure Private Accessプロバイダーは、ヘッダー（新しいロジック）として、またはGatewayへのコールバックを行うことによって、スマートアクセスタグを受信できます。詳細については、「[新しいコンテキストタグの追加](#)」を参照してください。

GUIを使用してカスタムタグを構成する

コンテキストタグの構成には、次の大まかな手順が含まれます。

1. クラシックゲートウェイの事前認証ポリシーを構成します。
2. クラシック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します。

クラシックゲートウェイの事前認証ポリシーを構成する

1. **NetScaler Gateway > ポリシー > 事前認証**に移動し、**追加**をクリックします。

2. 既存のポリシーを選択するか、ポリシーの名前を追加します。このポリシー名は、カスタムタグ値として使用されます。
3. **要求アクション**で、**追加**をクリックしてアクションを作成します。このアクションは複数のポリシーで再利用できます。たとえば、1つのアクションでアクセスを許可し、別のポリシーでアクセスを拒否します。

4. 必須フィールドに詳細を入力し、**作成**をクリックします。
5. **式**に式を手動で入力するか、式エディターを使用してポリシーの式を構築します。

式のサンプル(/en-us/citrix-secure-private-access/media/spaop-expression-sample.png)

次の図は、Windows 10 OSをチェックするために構築された式のサンプルを示しています。

式エディター(/en-us/citrix-secure-private-access/media/spaop-polcy-exp-editor.png)

6. **作成**をクリックします。

カスタムタグをNetScaler Gatewayにバインドする

1. **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、**種類の選択**で**要求**を選択します。

ポリシーの種類(/en-us/citrix-secure-private-access/media/spaop-request-type.png)

5. ポリシー名とポリシー評価の優先度を選択します。

6. バインドをクリックします。

ポリシーのバインド(/en-us/citrix-secure-private-access/media/spaop-preauth-policy-binding.png)

CLIを使用してカスタムタグを構成する

NetScaler CLIで次のサンプルコマンドを実行して、事前認証ポリシーを作成およびバインドします。

- `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`

NetScaler CLIでnFactor EPAポリシーを設定するには、以下のサンプルコマンドを実行します。

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr(\"proc_0_notepad.exe\")" -defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

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、既存のポリシーを編集します。
3. 「条件」セクションで、「条件の追加」をクリックし、「コンテキストタグ」、「すべてに一致」を選択して、コンテキストタグ名（例: `Windows10`）を入力します。

Secure Private Accessプロバイダーに送信されるEPAタグに関する注意

nFactor EPAポリシーで構成されたEPAアクション名と関連付けられたグループ名は、スマートアクセスタグとしてSecure Private Accessプロバイダーに送信されます。ただし、送信されるタグはEPAアクション評価の結果によって異なります。

- nFactor EPAポリシー内のすべてのEPAアクションが**DENY**アクションになり、最後のEPAアクションで隔離グループが構成されている場合、隔離グループ名がスマートアクセスとして送信されます。

- nFactor EPAポリシー内のEPAアクションが**ALLOW**アクションになった場合、そのアクションに関連付けられたEPAポリシー名とデフォルトグループ名（構成されている場合）がスマートアクセスタグとして送信されます。

スマートアクセスタグ(/en-us/citrix-secure-private-access/media/epa-smart-access-tags.png)

この例では、アクションが拒否された場合、deny_app がスマートアクセスタグとして Secure Private Access プロバイダーに送信されます。アクションが許可された場合、epaallowact と allow_app がスマートアクセスタグとして Secure Private Access プロバイダーに送信されます。