Citrix Remote Browser Isolation

Machine translated content

Disclaimer

Contents

Remote Browser Isolation

July 2, 2024

Citrix Remote Browser Isolation サービス（旧称 Secure Browser サービス）は、Web 閲覧アクティビティを分離することにより、ブラウザーベースの攻撃から企業のネットワークを保護します。Remote Browser Isolation サービスは、ユーザーデバイスを構成する必要なく、インターネットでホストされた Web アプリケーションに一貫してセキュアにリモートアクセスすることができます。管理者はすばやくリモート分離ブラウザーを展開して、すぐに価値を生み出すことができます。IT 管理者は、インターネット閲覧を分離することで、企業ネットワークのセキュリティを損なうことなく、エンドユーザーに安全なインターネットアクセスを提供します。

ユーザーは、Citrix Workspace（または Citrix Receiver）を使用してログオンし、構成済みの Web ブラウザーで Web アプリを開くことができます。Web サイトとユーザーデバイスとの間で閲覧データが直接転送されないため、ユーザー操作中のセキュリティが保護されます。

Remote Browser Isolation サービスでは、以下で使用するリモート分離ブラウザーを公開できます:

- 外部 **Web** アプリで共有パスコードを使用。共有パスコード認証を使用したブラウザーを公開する場合、ユーザーはアプリを起動するためにパスコードを入力する必要があります。
- 認証済みの外部 **Web** アプリ。認証済みの外部 Web アプリを公開し、Citrix Workspace を使用してこのアプリを起動する場合、少なくとも 1 つの Cloud Connector を含むリソースの場所が必要です（2 つ以上を推奨）。詳しくは、「Citrix Cloud Connector」を参照してください。認証済みアプリの場合、Citrix Cloud のライブラリを使用してユーザーを追加する必要があります。
- 認証されていない外部 **Web** アプリ。認証されていない外部 Web アプリを公開し、Citrix Workspace を使用してこのアプリを起動する場合、少なくとも 1 つの Cloud Connector を含むリソースの場所が必要です（2 つ以上を推奨）。詳しくは、「Citrix Cloud Connector」を参照してください。

  通常は推奨されませんが、認証されていない外部 Web アプリを単純な概念実証に使用することがあります。

詳しくは、「リモート分離ブラウザーを公開する」を参照してください。

Secure Browser サービスはまた、次の機能を提供します:

- 公開アプリと Citrix Workspace の統合
- 公開アプリとオンプレミス StoreFront の統合
- セキュリティのための簡易 URL 許可リスト機能
- 使用状況の監視
- クリップボードの使用、印刷、キオスクモード、リージョンフェールオーバー、およびクライアントドライブマッピングの管理

Citrix Secure Private Access による **Remote Browser Isolation** サービス

Citrix Secure Private Access コンソールを使用して Remote Browser Isolation サービスの公開ブラウザーを起動し、エンタープライズ Web、TCP、SaaS アプリケーションにアクセスできます。また、Citrix Secure Private Access を使用して、許可されていない Web サイトをリダイレクトして、Remote Browser Isolation サービスの公開ブラウザーで開くこともできます。

Citrix Secure Private Access を使用してリモート分離ブラウザーにアクセスする方法について詳しくは、Citrix Secure Private Access ドキュメントの「複数の規則を含むアクセスポリシーの構成」と「未承認の Web サイト」を参照してください。

参考記事

- Secure Private Access サービスソリューションの概要
- Citrix Cloud
- Remote Browser Isolation のセルフサービス検索（Secure Browser）
- Citrix Enterprise Browser
- セキュリティおよびコンプライアンスの情報
- 開発者用のドキュメント

関連製品の新着情報

- Secure Private Access
- Citrix Enterprise Browser
- Citrix Analytics for Security

新機能

October 19, 2022

2022 年 **7** 月

- **Remote Browser Isolation** は、**Azure Active Directory** を使用するすべてのアプリの認証をサポートします。
  - ユーザーは、Azure Active Directory の資格情報を使用して、Citrix Workspace から Remote Browser Isolation アプリにサインインできるようになりました。
  - Remote Browser Isolation ユーザーがサインインすると、サイト用に構成した Workspace のサインインページが使用されます。詳しくは、「Citrix Workspace との統合」を参照してください

2021 年 **9** 月

- **Remote Browser Isolation** は双方向オーディオをサポートしています。双方向オーディオは Remote Browser Isolation で使用できます。
- **launch.cloud.com** からの **Remote Browser Isolation** の起動は、**Citrix Cloud** 認証によって認証されます。ユーザーが launch.cloud.com の URL を使用して Remote Browser Isolation アプリを起動すると、Citrix Cloud 認証がユーザーの資格情報を処理します。これによりセキュリティが強化されますが、ユーザーエクスペリエンスは変わりません。

2021 年 **3** 月

- **Remote Browser Isolation** は、**Azure Active Directory** を使用する認証をサポートしています。ユーザーは、Azure Active Directory の資格情報を使用して、Citrix Workspace から Remote Browser Isolation アプリにサインインできるようになりました。詳しくは、「Citrix Workspace との統合」を参照してください
- **Remote Browser Isolation** を使用すると、ユーザーのアクティブなセッションを監視してログオフさせることができます。Remote Browser Isolation は、ユーザー名、セッション ID、クライアント IP、認証の種類、アプリケーション名、セッション開始時間、ユーザーのアクティブなセッションに関するセッション期間情報を提供します。アクティブな各セッションに関する基本情報を表示し、必要に応じてセッションを切断できます。詳しくは、「アクティブなセッションを監視」を参照してください。

2020 年のリリース

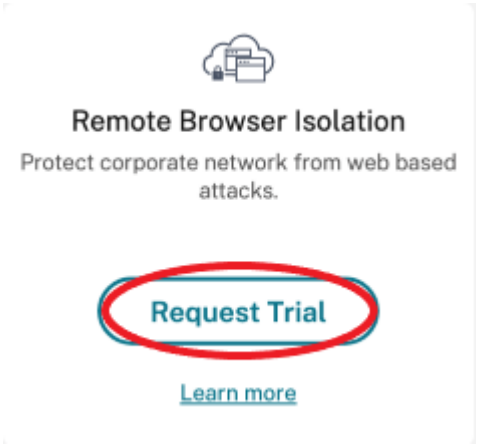
2020 年のすべてのリリースで、全体のパフォーマンスと安定性の向上に役立つ機能強化が行われています。

Remote Browser Isolation の利用を開始する

October 19, 2022

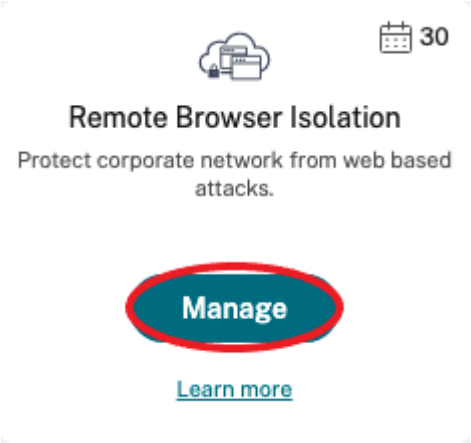
以下のビデオでは、Remote Browser Isolation サービス（旧称 Secure Browser サービス）の使用開始について説明しています。

1. Citrix Cloud にサインインします。アカウントをお持ちでない場合は、「Citrix Cloud へのサインアップ」を参照してください。Citrix Remote Browser Isolation の 30 日間トライアルをリクエストできます。
2. [**Remote Browser Isolation**] タイルで、[トライアルをリクエスト] をクリックします。

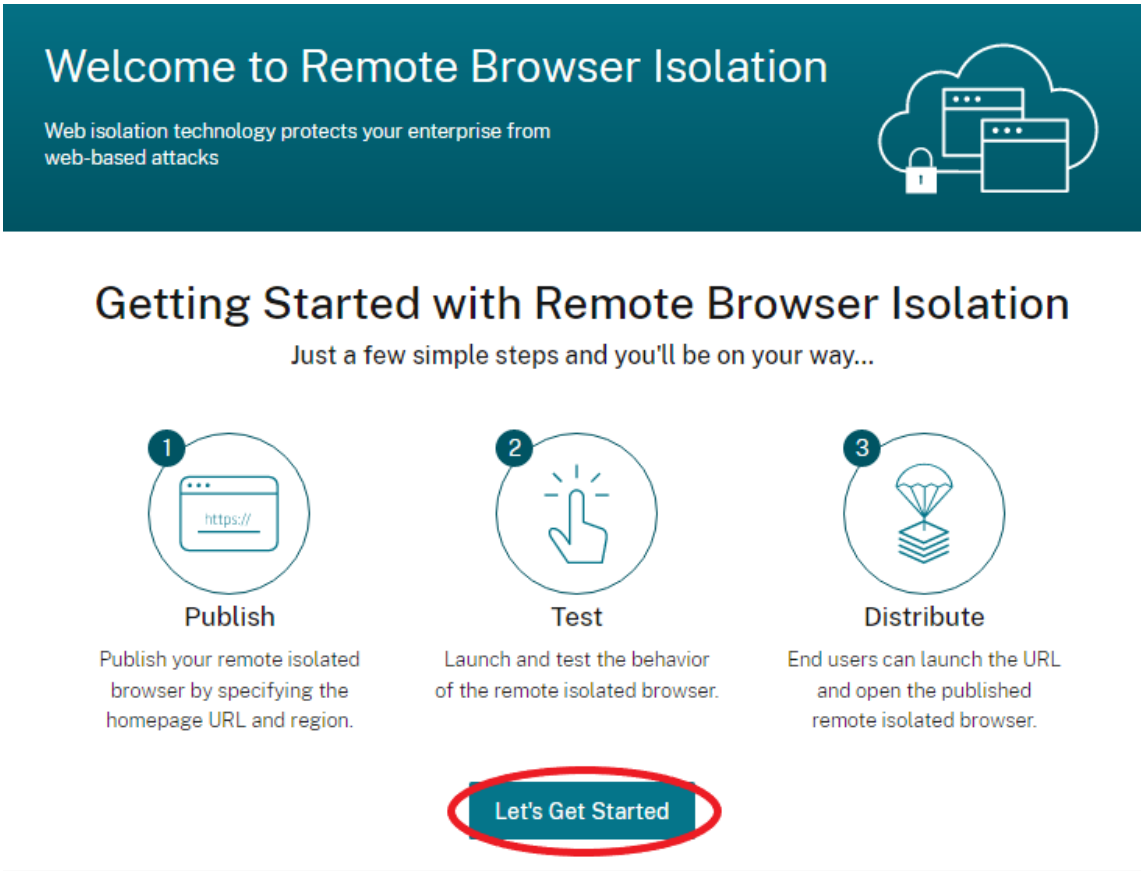


3. 数分後にメールが届きます。このメールは、Citrix Cloud アカウントに関連付けられています。メール内のサインインリンクをクリックします。
4. Citrix Cloud に再度サインインした後、[**Remote Browser Isolation**] タイルで [管理] をクリックしま

す。



5. ［**Remote Browser Isolation** へようこそ］ページで、［使用を開始する］をクリックします。



6. 公開するリモート分離ブラウザーの種類を選択します：共有パスコード、認証済み、または非認証。次に、［続行］をクリックします。

   デフォルトでは、ユーザーは launch.cloud.com を使用して、共有パスコード認証でアプリケーションを起動する必要があります。Citrix Workspace および Citrix Cloud ライブラリは共有パスコード使用のアプリをサポートしません。

Citrix Workspace を使用するには、認証済みアプリを公開して Citrix Cloud ライブラリで利用者（ユーザー）やグループを明示的に割り当てる必要があります。認証されていないアプリは、ユーザー割り当てなしですべての Workspace 利用者が使用できます。

7. 次の設定を構成します：

   - 名前：作成中のアプリの名前を入力します。
   - 開始 **URL**：ユーザーがアプリを起動したときに開く URL を指定します。
   - リージョン：サーバーの場所/リージョンを選択します。利用可能なリージョンは米国西部、米国東部、東南アジア、オーストラリア東部、西ヨーロッパです。

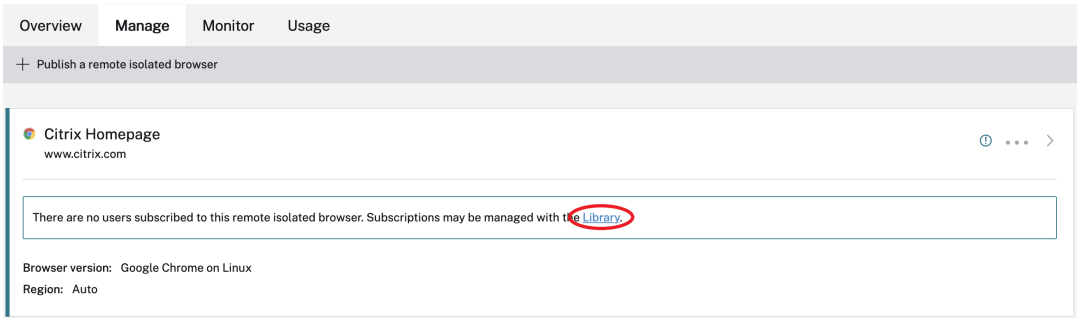
     ［自動］を選択すると、分離ブラウザーが地理位置情報に基づいて最も近いリージョンに接続します。
   - パスコード：共有パスコード認証のブラウザーを選択した場合は、アプリにアクセスするときのセキュリティを強化するために、パスコードを入力します。パスコードは、数字と記号をそれぞれ 1 つ以上含む 10 文字以上にする必要があります。パスコードを保存したことを確認してから、ユーザーと共有します。launch.cloud.com を使用してアプリを起動したときに、ユーザーがパスコードを入力する必要があります。
   - アイコン：デフォルトでは、分離ブラウザーを公開するときに使用される Google Chrome の実行可能ファイルのアイコンです。公開ブラウザーに、独自のアイコンを表示することもできるようになりました。

     ［アイコンの変更］**>** ［アイコンの選択］の順にクリックし、アイコンを選択してアップロードするか、［デフォルトのアイコンを使用］を選択し、既存の Google Chrome のアイコンを使用します。

   ［公開］をクリックします。

8. ［管理］タブには、公開したブラウザーが表示されます。作成したばかりのブラウザーを起動するには、分離ブラウザーを含むタイルの省略記号をクリックし、［公開ブラウザーの起動］をクリックします。

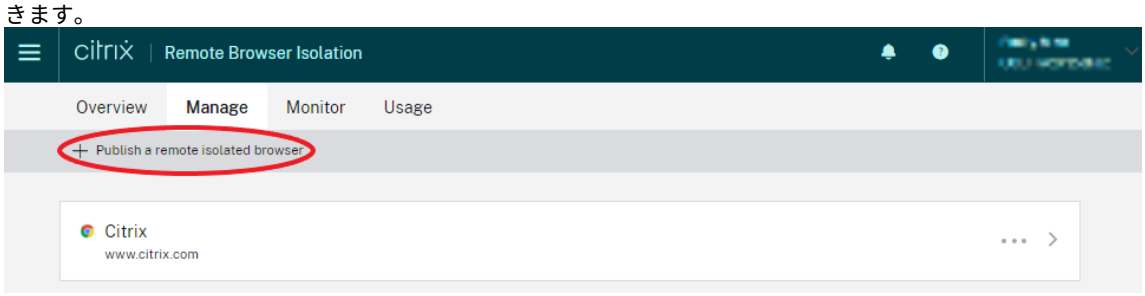
   - 認証済みの分離ブラウザーを公開した場合、Citrix Cloud のライブラリを使用してユーザーやグループを追加する必要があります。行末尾にある右矢印をクリックして、ライブラリへのリンクを含む詳細ペインを展開します。

     このリンクをクリックし、説明に従って、ライブラリ画面で作成したリモート分離ブラウザーを表示します。分離ブラウザーを含むタイルの省略記号（…）をクリックし、［利用者の管理］をクリックします。

利用者の追加について詳しくは、「ライブラリを使用してサービスオファリングにユーザーとグループを割り当てる」を参照してください。

［管理］タブの ［リモート分離ブラウザーを公開する］をクリックして、別のリモート分離ブラウザーを公開できます。



Citrix Remote Browser Isolation サービス（旧称 Citrix Secure Browser サービス）の購入については、https://www.citrix.com/products/citrix-remote-browser-isolation/を参照してください。

Citrix Workspace との統合

Remote Browser Isolation は、Citrix Workspace と統合できます。サービスが統合されていることを確認するには:

1. Citrix Cloudにサインインします。
2. 左上のメニューで、［ワークスペース構成］を選択します。
3. ［サービス統合］タブを選択します。
4. Remote Browser Isolation サービスのエントリが ［有効］になっていることを確認します。無効になっている場合は、省略記号メニューをクリックし、［有効化］を選択します。

まだ統合していない場合は、「ワークスペースへの認証を構成する」の説明に従って、ワークスペースのワークスペース URL、外部接続、およびワークスペース認証を構成します。

Remote Browser Isolation は、Active Directory および Azure Active Directory での認証をサポートします。Active Directory による認証はデフォルトで構成されています。Azure Active Directory を使用した認証の構成について詳しくは、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。

Azure Active Directory を使用して認証を構成した場合、Active Directory ドメインコントローラーを含むオンプレミスのドメインには、少なくとも 1 つ（推奨は 2 つ以上）の Cloud Connector が含まれている必要があります。

オンプレミス **StoreFront** と統合する

オンプレミス StoreFront を使用している Citrix Virtual Apps and Desktops の顧客は、Remote Browser Isolation サービスと簡単に統合することで次の利点が得られます:

- 公開されたリモート分離ブラウザーと既存の Citrix Virtual Apps and Desktops アプリを集約した、統合されたストアエクスペリエンス。

- ネイティブの Citrix Receiver を使用して、エンドユーザーエクスペリエンスを強化できます。
- StoreFront に統合された既存の多要素認証ソリューションを使用して、Remote Browser Isolation 起動時のセキュリティを強化できます。

詳しくは、CTX230272および StoreFront の構成に関するドキュメントを参照してください。

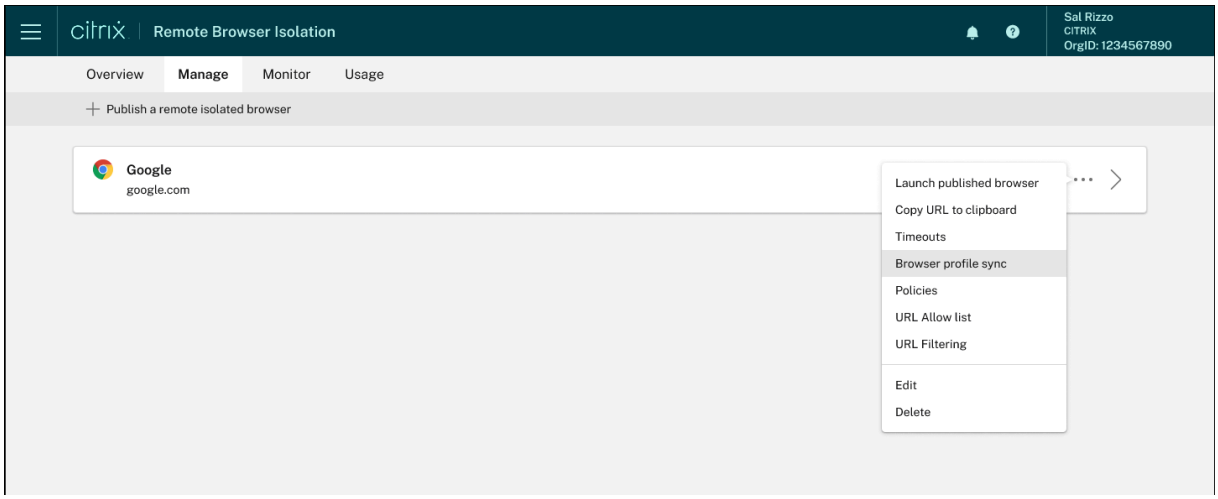
Remote Browser Isolation を管理および監視する

April 5, 2024

Remote Browser Isolation で公開ブラウザーの使用状況を管理、監視、確認できるようになりました。

管理

［管理］タブに、公開ブラウザーが表示されます。管理タスクを利用するには、公開ブラウザーの右端にある省略記号をクリックし、必要なタスクを選択します。



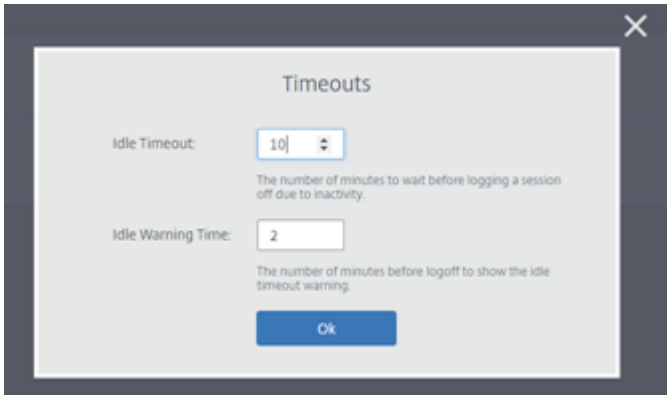
メニュー項目を選択して変更せずに終了する場合は、ダイアログボックスの外側にある ［**X**］をクリックして、選択をキャンセルします。

次のタスクを使用して、公開した分離ブラウザーを管理できます:

- 公開ブラウザーの起動: 公開ブラウザーセッションを開きます。ブラウザーを公開した後、このタスクを選択して、公開されたブラウザーセッションの起動を確認できます。
- **URL** をクリップボードにコピー: 公開ブラウザーの URL をコピーします。この URL をエンドユーザーと共有して、公開ブラウザーにアクセスできます。
- タイムアウト: [タイムアウト] タスクを選択すると、[アイドルタイムアウト] と [アイドル警告の時間] を設定できます。
  - アイドルタイムアウト: 非アクティブのセッションを終了する前にアイドル状態を維持できる時間 (分)。
  - アイドル警告の時間: 警告メッセージがユーザーに送信されてからセッションが終了するまでの時間 (分)。

  たとえば、[アイドルタイムアウト] を「20」、[アイドル警告の時間] を「5」に設定した場合、そのセッションで 15 分間アクティビティがなければ、警告が表示されます。ユーザーが対応しないと、セッションは 5 分後に終了します。

  公開した分離ブラウザーの [アイドル タイムアウト] と [アイドル警告の時間] を設定するには、[タイムアウト] タスクを選択し、[タイムアウト] ダイアログボックスで [アイドルタイムアウト] と [アイドル警告の時間] を設定します。次に、[**OK**] をクリックして変更を保存します。

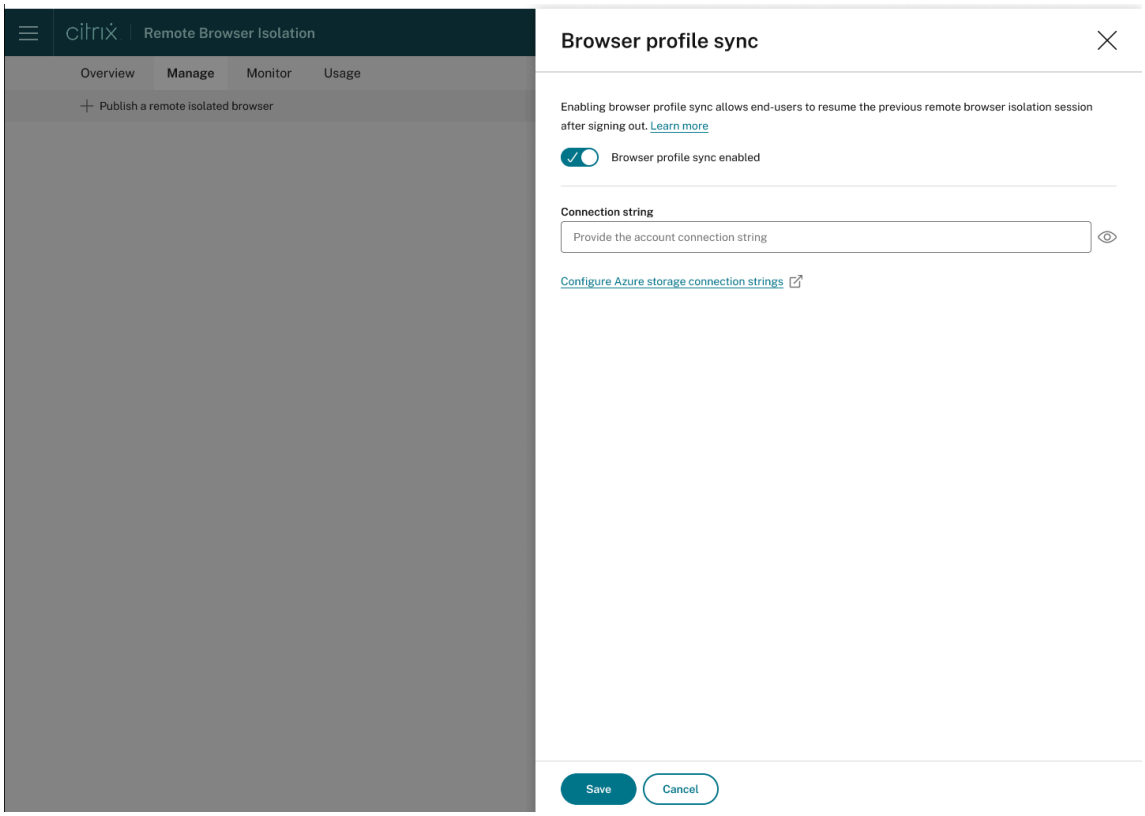
  

- ブラウザープロファイルの同期: エンドユーザーがサインアウトした後に前のブラウザーセッションを再開できるようにします。管理者は、Azure ストレージの接続文字列を指定して、ブラウザーのプロファイルのスト

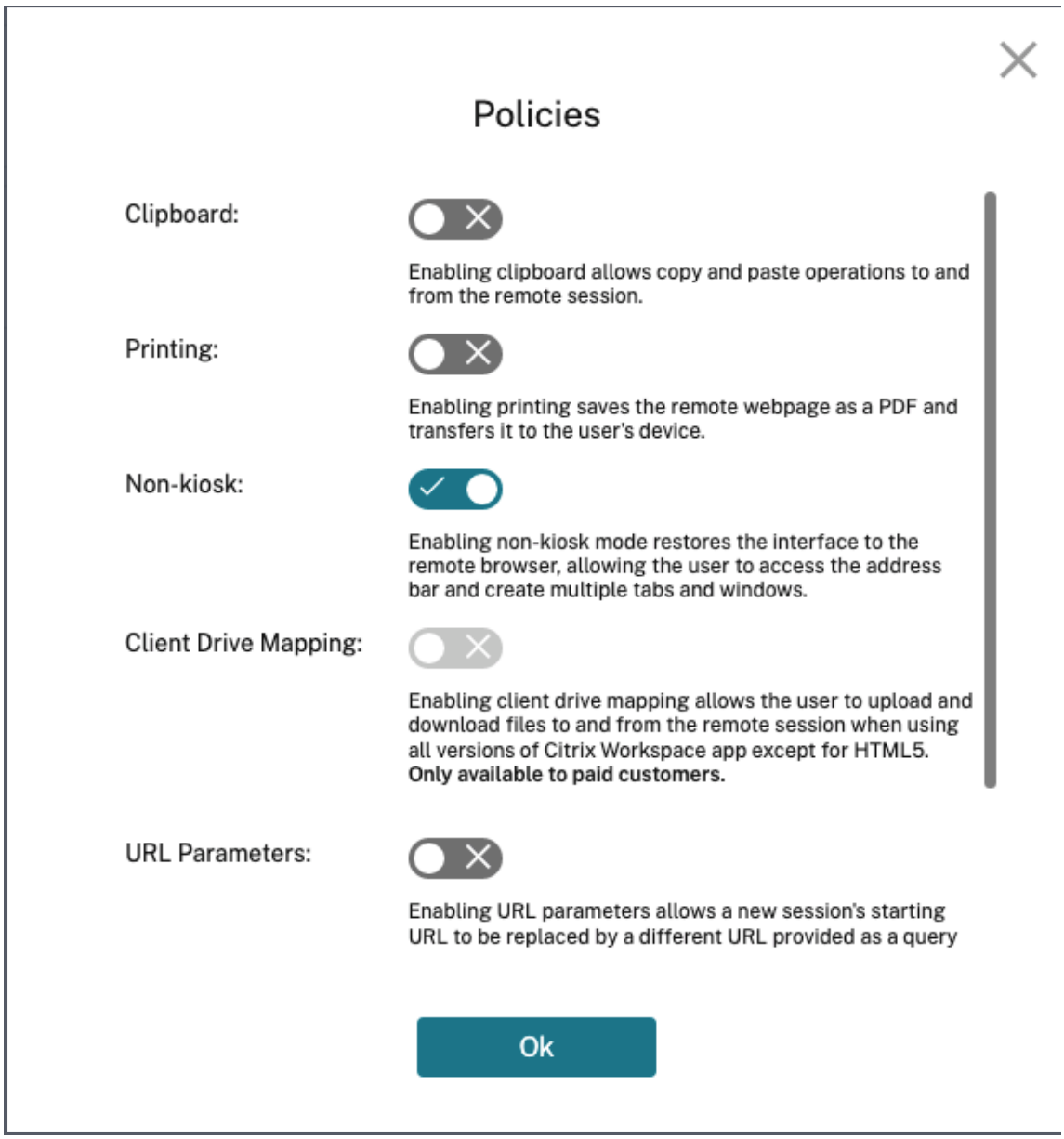
レージを有効にすることができます。ユーザーが同じプロファイルで別のブラウザーセッションを開くと、ユーザーが中断したところから前のブラウザーセッションが復元されます。ユーザーがいずれかの Web サイトにログインした場合、それらの Web サイトが認証を担当します。この機能ではセッション、Cookie、その他の情報を保存できますが、Web サイトではユーザーの再度のサインインが必要な場合があります。現在、この機能はタブの復元のみをサポートしています。

［ブラウザープロファイルの同期］機能を有効にするには、次の手順を実行します：

1. 必要な公開ブラウザーの ［ブラウザープロファイルの同期］タスクを選択します。
2. ［ブラウザー プロファイルの同期］ダイアログ ボックスで、［ブラウザープロファイルの同期］を有効にし、接続文字列を入力します。接続文字列の構成の詳細については、Azure Blob Storage ドキュメントの「Azure Storage の接続文字列を構成する」を参照してください。
3. ［保存］をクリックします。



- ポリシー：公開ブラウザーに対してポリシーを設定できます。



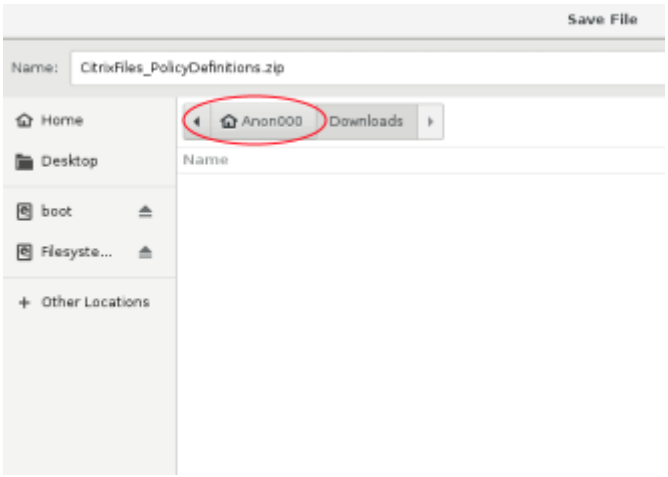
ポリシーページの設定により、次の項目を管理できます：

- クリップボード：クリップボードポリシーを有効にすると、リモートセッションとの間でコピーと貼り付けができるようになります。（クリップボードポリシーを無効にすると、Citrix Workspace アプリのツールバーからクリップボードボタンが削除されます。）デフォルトでは、この設定は無効になっています。
- 印刷：印刷を有効にすると、リモート Web ページが PDF として保存され、ユーザーのデバイスに転送されます。ユーザーは、Ctrl+P キーを押して Citrix PDF プリンターを選択できます。デフォルトでは、この設定は無効になっています。
- 非キオスク：非キオスクモードを有効にすると、インターフェイスがリモートブラウザーに復元されます。ユーザーは、ここでアドレスバーにアクセスして複数のタブとウィンドウを作成できます。（非キオ

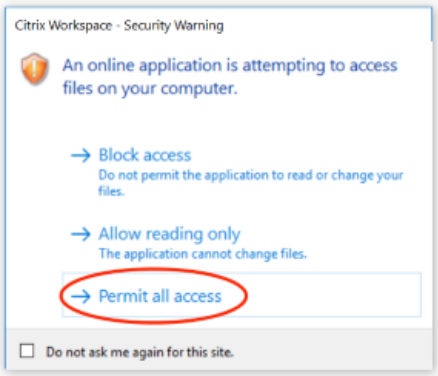
スクモードを無効にすると、リモートブラウザーの各ナビゲーションコントロールとアドレスバーが削除されます。）デフォルトでは、この設定は有効です（非キオスクモードがオンになっている）。

- リージョンフェールオーバー：現在のリージョンで問題が報告されている場合は、リージョンフェールオーバーポリシーにより、公開ブラウザーが自動的に別のリージョンに転送されます。オプトアウトするには、リージョンフェールオーバーポリシーを無効にします。リージョンの選択を ［自動］にしてブラウザーを公開すると、分離ブラウザーはポリシーに登録されたままになります。デフォルトでは、有効になっています。
- クライアントドライブマッピング：クライアントドライブマッピングポリシーを有効にすると、ユーザーは、リモートセッションとの間でファイルをアップロードおよびダウンロードできます。この機能は、Citrix Workspace アプリで開始されたセッションでのみ使用できます。デフォルトでは、この設定は無効になっています。

  * ダウンロードしたファイルは、必ず **Anonxxx**ディレクトリ内の**ctxmnt**ディスクに保存する必要があります。これを行うには、ユーザーはファイルを保存する場所を指定する必要があります。（例：［**Anonxxx**］**>** ［**ctxmnt**］**>** ［**C**］**>** ［ユーザー］**>**「ユーザー名」**>** ［ドキュメント］）



  * ダイアログボックスで、**ctxmnt**フォルダーへのすべてのアクセスを許可するか、読み取り/書き込みアクセスをどのように許可するかを指定します。



- **URL** パラメーター： URL パラメーターを有効にすると、ユーザーがアプリを起動した際に新しいセッ

ションの開始 URL を変更できます。このポリシーを有効にするには、疑わしい Web サイトを特定し、それらを Remote Browser Isolation にリダイレクトするようローカルプロキシサーバーを構成します。デフォルトでは、この設定は無効になっています。詳しくは、「概念実証ガイド：Azure における Citrix ADC を使用した Remote Browser Isolation への URL リダイレクト」を参照してください。

- ホスト名の追跡：ホスト名の追跡を使用して、ユーザーのセッション中に Remote Browser Isolation でホスト名をログに記録する機能を有効にします。このポリシーは、デフォルトでは無効になっています。この情報は、Citrix Analytics と共有されています。詳しくは、「Citrix Analytics」を参照してください。

設定を完了したら、［**OK**］をクリックします。

- **URL** 許可リスト：［ホワイトリスト］タスクでは、公開された Remote Browser Isolation とのセッション内で、ユーザーが許可された URL のみにアクセスできるように制限することができます。この機能は、外部認証済みの Web アプリで使用できます。

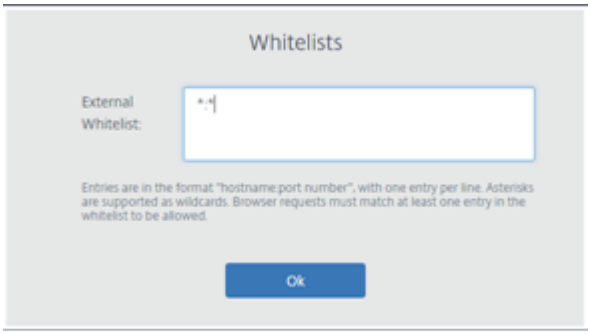
  許可リストのエントリは「`hostname:port number`」の形式で入力します。1 行に 1 つずつ入力します。アスタリスクをワイルドカードとして使用できます。ブラウザーの要求は、許可リストの少なくとも 1 つのエントリと一致する必要があります。

  たとえば、許可された URL として`https://example.com`を設定するには：

  - `example.com:*`と入力すると、任意のポートからこの URL に接続できます。
  - `example.com:80`と入力すると、ポート 80 からのみこの URL への接続を許可します。
  - `*:*`と入力すると、この URL への任意のポートからのアクセスと、ほかの URL やポートへの任意のリンクからのアクセスを許可します。「`*.*`」の形式で入力すると、公開アプリからすべての外部 Web アプリへのアクセスが許可されます。この形式は、Web アプリの外部の許可リストに指定するデフォルト設定です。

  設定を完了したら、［**OK**］をクリックします。

  アクセス制御サービスと統合すると、高度な Web フィルター機能が利用できます。詳しくは、「使用目的：特定のアプリへのアクセスを許可するアクセスポリシーを設定する」を参照してください。



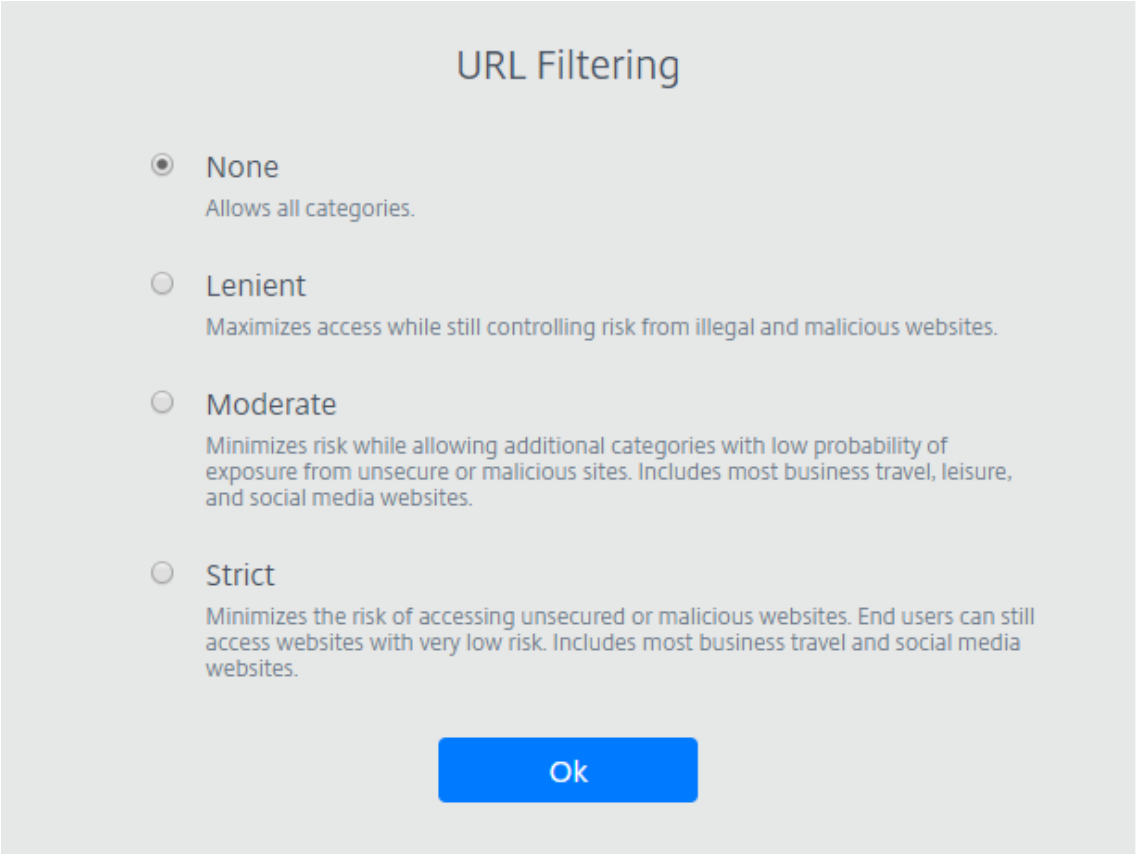
- **URL** フィルタリング：リスクモデルに関連した事前定義のカテゴリごとにアクセス方法を制御するように、URL フィルタリングを構成できます。以下は、URL フィルタリングオプションです：

  - なし - すべてのカテゴリを許可します。

- 低 - 不正または悪意のある Web サイトによるリスクを管理しながら、Web サイトに最大限アクセスできるようにします。次のカテゴリが含まれます:
  - 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
  - コンピューティングとインターネット：リモートプロキシ、プライベート IP アドレス、ピアツーピアのファイル共有、トレント。
  - ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
  - 違法で有害：テロリズム、過激派、誹謗、中傷、武器、暴力、自殺、違法薬物、薬物、違法行為、マリファナ、主義主張全般。
  - マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
- 中 - リスクを最小限に抑えながら、セキュリティ保護されていない Web サイトや悪意のある Web サイトへの露出の可能性が低いカテゴリを許可します。次のカテゴリが含まれます:
  - 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
  - ビジネスと産業：オークション。
  - コンピューティングとインターネット：広告、バナー、リモートプロキシ、プライベート IP アドレス、ピアツーピアファイル共有、トレント。
  - ダウンロード：モバイルアプリストア、ストレージサービス、ダウンロード、プログラムのダウンロード。
  - メール： Web ベースのメールおよびメールサブスクリプション。
  - 金融：暗号通貨。
  - ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
  - マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
  - メッセージング、チャット、電話：インスタントメッセージおよび Web ベースのチャット。
  - ニュース、娯楽、社会： Wordpress（投稿とアップロード）、サポートされていない URL、オカルト、コンテンツなし、その他、ホロスコープ、占星術、運勢判断、飲酒、宗教、個人の Web ページ、ブログ、オンラインゲーム。
  - ソーシャルネットワーク：写真の検索および共有サイト、IT 掲示板、掲示板。
- 高 - セキュリティ保護されていない Web サイトや悪意のある Web サイトにアクセスするリスクを最小限に抑えます。エンドユーザーは、引き続きリスクの低い Web サイトにアクセスできます。次のカテゴリが含まれます:
  - 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
  - ビジネスと産業：オークション。

* コンピューティングとインターネット：広告、バナー、動的 DNS、モバイルアプリ、パブリッシャー、パークドメイン、リモートプロキシ、プライベート IP アドレス、ピアツーピアファイル共有、トレント。
* ダウンロード：モバイルアプリストア、ストレージサービス、ダウンロード、プログラムのダウンロード。
* メール： Web ベースのメールおよびメールサブスクリプション。
* 金融：暗号通貨と金融商品。
* ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
* 違法で有害：テロリズム、過激派、誹謗、中傷、武器、暴力、自殺、違法薬物、薬物、違法行為、マリファナ、主義主張全般。
* 求人と履歴書：雇用、キャリアアップ、LinkedIn（更新、メール、接続、ジョブ）。
* マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
* メッセージング、チャット、電話：インスタントメッセージおよび Web ベースのチャット。
* ニュース、娯楽、社会： Wordpress（投稿とアップロード）、宿泊施設、旅行と観光、サポートされていない URL、政治、ファッションと美容、芸術と文化的イベント、リファレンス、レジャーと趣味、地域社会、その他、飲酒、人気のトピック、特別なイベント、ニュース、社会と文化、オンライン雑誌、オンラインゲーム、ライフイベント、オカルト、コンテンツなし、星占い、占星術、運勢判断、有名人、ストリーミングメディア、娯楽、施設、アクティビティ、個人の Web ページとブログ、宗教。
* ソーシャルネットワーク：ソーシャルネットワーク全般、YikYak（投稿）、Twitter（投稿、メール、フォロー）、Vine（アップロード、コメント、メッセージ）、Google+（写真とビデオのアップロード、投稿、ビデオチャット、コメント）、Instagram （アップロードとコメント）、YouTube（共有とコメント）、Facebook（グループ、ゲーム、質問、ビデオのアップロード、写真のアップロード、イベント、チャット、アプリ、投稿、コメント、友達）、Tumblr（投稿、コメント、写真、ビデオのアップロード）、Pinterest（ピンとコメント）、IT 掲示板、掲示板。

設定を完了したら、［**OK**］をクリックします。



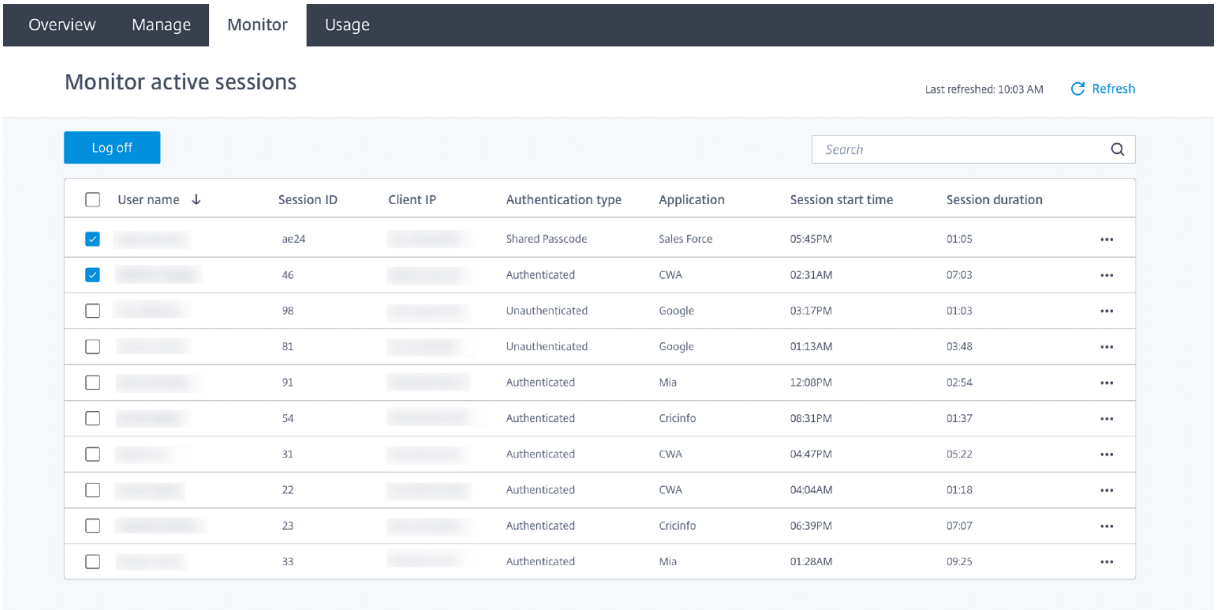
- 編集：［編集］タスクでは、公開されたブラウザーの名前、開始 URL、リージョン、またはパスコードを変更することができます。完了したら、［公開］をクリックします。
- 削除：公開した分離ブラウザーを削除するには、［削除］タスクを使用できます。このタスクを選択すると、削除確認メッセージが表示されます。

監視

［監視］タブには、ユーザーのリアルタイムセッションに関する情報が表示されます。1 つまたは複数のアクティブなセッションを監視および切断できます。

単一のセッションを停止するには、セッションを選択し、エントリの行の最後にある省略記号メニューをクリックします。［セッションのログオフ］をクリックして、変更を確認します。

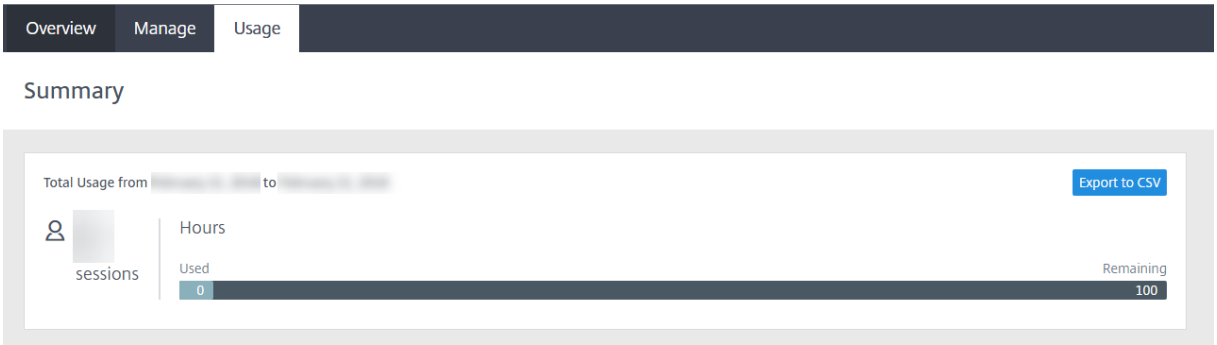
複数のセッションを切断するには、一覧からアクティブなセッションを選択し、ページ上部の ［ログオフ］ボタンをクリックします。変更を確認すると、Remote Browser Isolation は選択したすべてのセッションを直ちに切断します。



使用状況

［使用状況］タブには、開始されたセッションの数と使用された時間数が表示されます。

使用状況の詳細を含むスプレッドシートを作成するには、［**CSV** にエクスポート］をクリックして、確認する期間を選択します。



Remote Browser Isolation のセキュリティの技術概要

October 19, 2022

Remote Browser Isolation（旧称 Secure Browser サービス）は、Citrix が管理および運用する SaaS 製品です。このサービスを使用すると、クラウドでホストされている Web ブラウザーを介して Web アプリケーションにアクセスできます。

クラウドサービス

Citrix Remote Browser Isolation サービスは、Virtual Delivery Agent（VDA）上で実行される Web ブラウザーと、ユーザー管理およびこれらの VDA へのユーザー接続を行う管理コンソールで構成されています。Citrix Cloud は、オペレーティングシステム、Web ブラウザー、および Citrix コンポーネントのセキュリティおよびパッチ適用など、これらのコンポーネントの運用を管理します。

Remote Browser Isolation サービスを使用している間、ホストされている Web ブラウザーはユーザーの閲覧履歴を追跡し、HTTP 要求のキャッシュを実行します。固定プロファイルが使用されているため、閲覧セッションが終了するとこのデータは確実に削除されます。

Remote Browser Isolation サービスには、HTML5 対応の Web ブラウザーでアクセスします。このサービスでは、ダウンロード可能なクライアントは使用しません。使用するブラウザーとクラウドサービスの間のすべてのトラフィックは、業界標準の TLS で暗号化されています。Remote Browser Isolation では、TLS 1.2 のみがサポートされています。

Remote Browser Isolation のエグレストラフィックは、指定の IP アドレスを使用して内部ネットワークを保護します。受け入れる IP アドレスの一覧については、Knowledge Center の記事CTX286379を参照してください。

Web アプリケーション

Citrix Remote Browser Isolation サービスは、顧客またはサードパーティの Web アプリケーションを配信するために使用されます。Web アプリケーションの所有者にはセキュリティを管理する責任があり、Web サーバーとアプリケーションの脆弱性に対するパッチ適用などを行います。

Remote Browser Isolation と Web アプリケーションの間のトラフィックのセキュリティは、Web サーバーの暗号化設定によって異なります。インターネット上でこのトラフィックを保護するため、管理者は HTTPS の URL を公開します。

追加情報

セキュリティ情報について詳しくは、次のリソースを参照してください：

- Citrix Web サイトのセキュリティ関連情報ページ：https://www.citrix.com/security
- Citrix Cloud に関するドキュメント：「セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド」