



シトリックス リモートブラウザ分離™

Contents

リモートブラウザ分離	5
Citrix Secure Private Access™ を使用したリモートブラウザ分離サービス	6
参照記事	6
関連製品の新機能	6
新機能	7
2026年8月	7
2026年7月	7
2026年2月	7
2025年6月	8
2022年7月	8
2021年9月	8
2021年3月	9
2020年のリリース	9
Remote Browser Isolation の使用を開始する	10
Remote Browser Isolation - セルフホスト型ワークロード	10
DaaS サービスを有効にする方法	10
RBI のオンボーディングプロセス	11
ステップ1: Azureサブスクリプションの追加	11
ステップ2: アプリケーションカタログの作成	13
ステップ 3: ブラウザアプリケーションを公開する	15
ステップ4: ブラウザアプリケーションをテストして共有する	17
その他の機能	18
ユーザーアクティビティログ	18
主な利点	18
前提条件	18
設定手順	19

ステップ1：Azure Storage接続文字列の取得	19
ステップ2：アプリケーションのユーザーアクティビティログを構成する	20
ステップ3：機能が動作していることを確認する	20
ブラウジングアクティビティの表示と分析	21
データストレージ構造	21
ファイル命名規則	21
データ形式の説明	22
フィールドの説明	22
データを表示する方法	23
主な機能と考慮事項	23
機能のハイライト	23
制限事項	24
トラブルシューティング	24
問題1: Azure Storageにデータがない	24
問題2: 接続文字列の構成時に検証が失敗する	24
問題3: データアップロード後にユーザーセッションが中断されるか、遅くなる	25
問題4: アクティブなユーザーセッションに構成はすぐに適用されますか？	25
問題5: 複数のアプリケーションで同じストレージアカウントを使用できますか？	25
クローム エンタープライズ プレミアム (CEP) との統合	25
はじめに	25
この機能でできること	26
使用方法	26
準備	26
Citrix Cloudポータルでの構成	26
管理者タスク	27
制限事項と既知の動作	27
ユーザープロファイルの同期はサポートされていません	27
構成変更ごとに再起動が必要です	27

許可リストポリシーの動作	27
Google管理に重複するデバイスが表示される場合があります	27
カタログ下のマシンを再起動します	28
顧客管理RBIカタログ仮想ネットワーク用のAzure Firewallの構成	28
Azure仮想ネットワークを特定する	28
Azure Firewallを作成する	28
ルーティングの構成	29
ファイアウォール規則を構成する	29
構成のテスト	30
トラブルシューティング	30
制限事項	30
ソフトウェアのアップグレードとパッチ管理	30
Citrix® StoreFront Cloudとの統合	30
オンプレミスのStoreFrontとの統合	31
リモート分離ブラウザの管理と監視	32
管理	32
監視	37
Remote Browser Isolationの技術的セキュリティ概要	38
クラウドサービス	38
Webアプリケーション	38
詳細情報	39
Citrix Remote Browser Isolationのドキュメント履歴	40

リモートブラウザ分離

Citrix Remote Browser Isolation™ サービス（旧 Secure Browser サービス）は、Webブラウジングを分離し、ブラウザベースの攻撃から企業ネットワークを保護します。Remote Browser Isolationサービスは、ユーザーデバイスの設定を必要とせずに、インターネットでホストされているWebアプリケーションへの一貫した安全なリモートアクセスを提供します。管理者は、リモート分離ブラウザを迅速に展開し、即座に価値を提供できます。インターネットブラウジングを分離することで、IT管理者は、企業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できます。

ユーザーはストアにログオンし、構成済みのWebブラウザでWebアプリを開くことができます。Webサイトは、ブラウジングデータをユーザーデバイスに直接転送したり、ユーザーデバイスから直接転送したりしないため、エクスペリエンスは安全です。

Remote Browser Isolationサービスは、リモート分離ブラウザを公開して次の用途に使用できます。

- **共有パスコード外部Webアプリ:** 共有パスコード認証でブラウザを公開する場合、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。
- **認証済み外部Webアプリ:** 認証済み外部Webアプリを公開し、ストアからアプリを起動する場合、Remote Browser Isolationサービスには、少なくとも1つのCloud Connector（2つ以上を推奨）を含むリソースの場所が必要です。認証済みアプリのユーザーを追加する必要があります。詳細については、「[Citrix Cloud Connector](#)」を参照してください。
- **未認証外部Webアプリ:** 未認証外部Webアプリを公開し、ストアからアプリを起動する場合、Remote Browser Isolationサービスには、少なくとも1つのCloud Connector（2つ以上を推奨）を含むリソースの場所が必要です。詳細については、「[Citrix Cloud Connector](#)」を参照してください。

通常は推奨されませんが、未認証外部Webアプリは、簡単な概念実証に使用される場合があります。

詳細については、「[リモート分離ブラウザの公開](#)」を参照してください。

このサービスは、次の機能も提供します。

- **公開アプリとCitrix® StoreFront Cloud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シンプルな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制御

Citrix Secure Private Access™ を使用したリモートブラウザ分離サービス

Citrix Secure Private Access コンソールを使用して、エンタープライズWeb、TCP、SaaSアプリケーションにアクセスするために、リモートブラウザ分離サービスの公開されたブラウザを起動できます。また、Citrix Secure Private Access を介して、未承認のWebサイトをリモートブラウザ分離サービスの公開されたブラウザで開くようにリダイレクトすることもできます。

Citrix Secure Private Access を介した分離されたリモートブラウザへのアクセスに関する詳細については、Citrix Secure Private Access ドキュメントの [Configure an access policy with multiple rules](#) および [Unsanctioned websites](#) を参照してください。

参照記事

- [Secure Private Access サービスソリューションの概要](#)
- [Citrix Cloud \(シトリックス クラウド\)](#)
- [リモートブラウザ分離 \(Secure Browser\) のセルフサービス検索](#)
- [シトリックス エンタープライズ ブラウザ\(/ja-jp/citrix-enterprise-browser\)](#)
- [セキュリティとコンプライアンス情報](#)
- [開発者向けドキュメント](#)

関連製品の新機能

- [Secure Private Access \(セキュア プライベート アクセス\)](#)
- [シトリックス エンタープライズ ブラウザ\(/ja-jp/citrix-enterprise-browser/whats-new\)](#)
- [シトリックス アナリティクス for セキュリティ](#)

新機能

2026年8月

- **カタログ作成にNAT Gatewayを組み込み**: ネットワークアドレス変換 (NAT) Gateway がカタログ作成フローに組み込まれるようになりました。個別のスイッチは不要になりました。

2026年7月

- **詳細なコピー＆ペーストクリップボードポリシー**: 管理者は、公開されたりリモートブラウザに対して、コピーとペーストのポリシーを個別に構成できるようになりました。以前は、**クリップボードポリシー**がコピーとペーストの両方の操作を単一のトグルとして制御していました。この更新により、単一のクリップボードポリシーは2つの詳細な制御に置き換えられます。
 - **コピー** — 有効にすると、ユーザーはリモートブラウザセッションからローカルクリップボードにコンテンツをコピーできます。
 - **ペースト** — 有効にすると、ユーザーはローカルクリップボードからリモートブラウザセッションにコンテンツをペーストできます。

この分離により、管理者はリモートセッションとユーザーエンドポイント間のデータフローをきめ細かく制御できます。詳細については、「[ポリシー](#)」を参照してください。

2026年2月

- **リモートブラウザアイソレーションの更新**
 - Citrix Remote Browser Isolation™ (RBI) をGoogle Chrome Enterprise Premium (CEP) と統合できるようになりました。Googleトークンを使用してカタログを登録し、カタログレベルでChromeエンタープライズポリシーを適用できます。管理者は、Google管理コンソールからこれらのポリシーを一元的に管理できます。詳細については、「[Chrome Enterprise Premium \(CEP\) との統合](#)」を参照してください。
 - 管理者は、RBIセッション中のユーザーのブラウジングアクティビティを追跡および監査できるようになりました。ログには、アクセスしたWebサイト、アクセス時刻、ユーザー識別子、および許可リストの適用状況が記録されます。収集されたすべてのデータは、完全

なデータ所有権と制御を確保するために、顧客が管理するAzureストレージアカウントに保存されます。詳細については、「[ユーザーアクティビティログ](#)」を参照してください。

2025年6月

- **Remote Browser Isolation - セルフホスト型ワークロード**
 - Remote Browser Isolation (RBI) セルフホスト型ワークロードにより、顧客は自身のAzureサブスクリプション内でリモートブラウザワークロードを運用できます。RBIセルフホスト型ワークロードのデータプレーンコンポーネント (Virtual Desktop Agent) は、顧客が提供するAzureサブスクリプションで実行されます。これにより、顧客は必要に応じてマシンとカタログを水平方向に拡張し、より適切なワークロード分類のために複数のカタログをプロビジョニングできます。

2022年7月

- **Remote Browser Isolationは、Microsoft Entra IDによるすべてのアプリの認証をサポートします**
 - ユーザーは、Microsoft Entra IDの資格情報を使用して、Citrix Workspace™から任意の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サインインページが使用されます。詳細については、「[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ます**
 - Remote Browser Isolationで双方向オーディオが利用可能です。
- **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 URLを使用してRemote Browser Isolationアプリを起動すると、Citrix Cloud認証が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Microsoft Entra IDによる認証をサポートします**
 - ユーザーは、Microsoft Entra ID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。詳細については、「[Citrix Workspaceとの統合](#)」を参照してください。
- **Remote Browser Isolationでは、ユーザーのアクティブなセッションを監視およびログオフできます**
 - Remote Browser Isolationは、ユーザーのアクティブなセッションに関するユーザー名、セッションID、クライアントIP、認証タイプ、アプリケーション名、セッション開始時刻、セッション期間の情報を提供します。各アクティブセッションの基本情報を表示し、必要に応じてセッションを切断できます。詳細については、「[アクティブなセッションの監視](#)」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には、全体的なパフォーマンスと安定性の向上に役立つ機能強化が含まれています。

Remote Browser Isolation の使用を開始する

Remote Browser Isolation - セルフホスト型ワークロード

Remote Browser Isolation (RBI) セルフホスト型ワークロードを使用すると、顧客は独自の Azure サブスクリプション内でリモートブラウザワークロードを運用できます。RBI セルフホスト型ワークロードのデータプレーンコンポーネント (Virtual Desktop Agent) は、顧客が提供する Azure サブスクリプションで実行されます。これにより、顧客は必要に応じてマシンとカタログを水平方向に拡張し、ワークロードの分類を改善するために複数のカタログをプロビジョニングできます。

前提条件:

- Citrix Platform Licenses (CPL) ライセンスまたは RBI 専用エンタイトルメント、および DaaS Premium エンタイトルメント。
- DaaS サービスが有効になっている必要があります。

注:

この手順は、顧客テナントが必要なエンタイトルメントを持っている場合にのみ可能です。

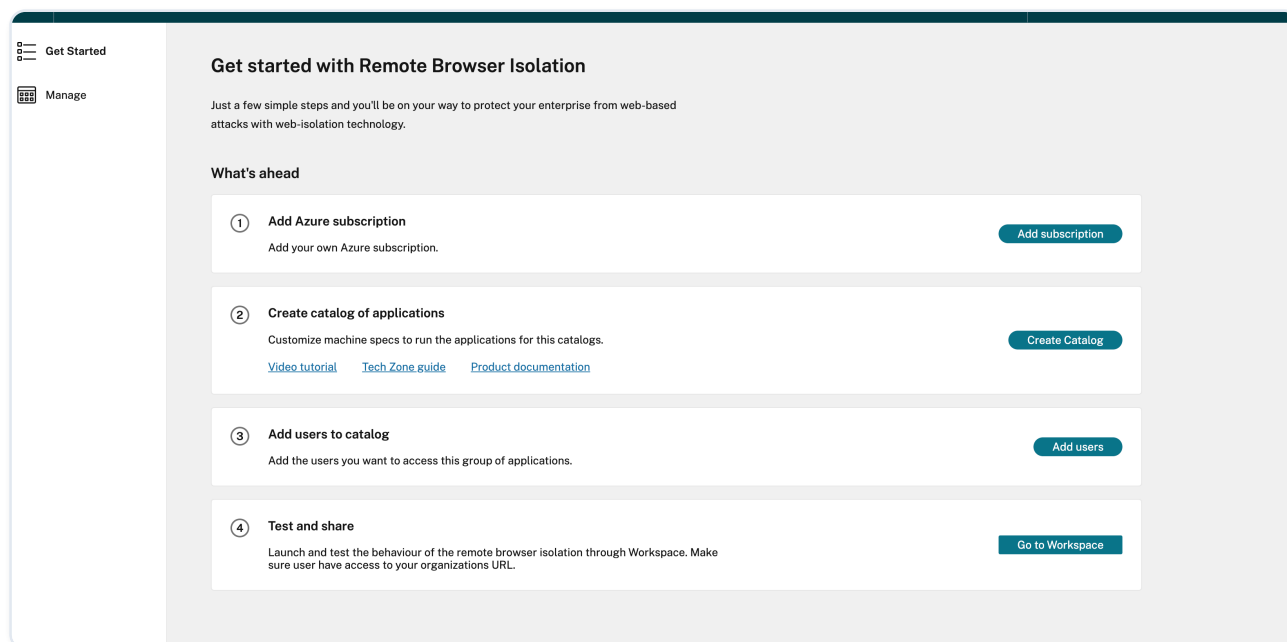
- DaaS で Rendezvous プロトコルを有効にします。

DaaS サービスを有効にする方法

1. [Citrix Cloud](#) にサインインします。
2. DaaS サービスに移動します。
3. **DaaS を有効にする** を見つけてクリックします。この手順では、RBI セルフホスト型ワークロードに必要な DaaS インフラストラクチャを準備し、約 45 分かかります。

RBI のオンボーディングプロセス

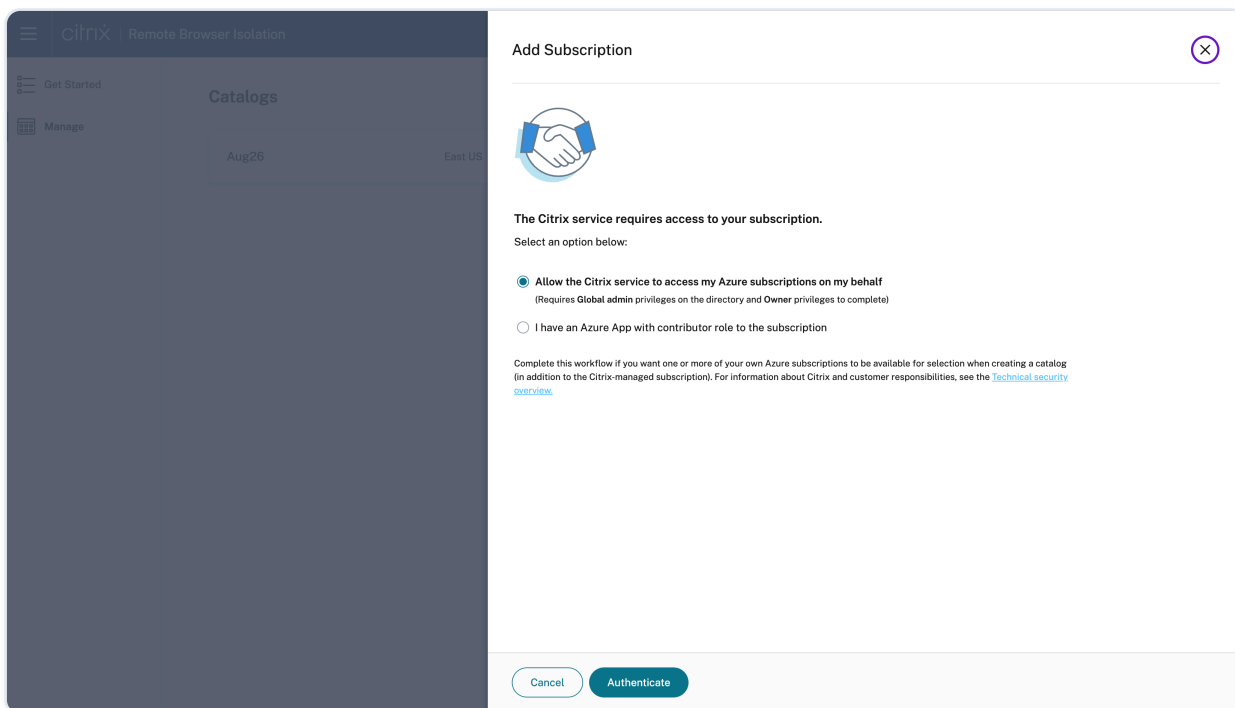
Citrix Cloud ページで、**RBI サービスを管理** をクリックして **Remote Browser Isolation** ランディングページにアクセスします。



ステップ1：Azureサブスクリプションの追加

1. リモート分離の開始ページで、**サブスクリプションの追加**をクリックします。Azureサブスクリプションは、RBIセルフホスト型ワークロードに2つの方法で追加できます。

- グローバル管理者資格情報を使用する: Citrixサービスが私の代わりにAzureサブスクリプションにアクセスすることを許可する。
- サブスクリプション全体に対する共同作成者ロールを持つエンタープライズアプリ登録を使用する。



Add Subscription

The Citrix service requires access to your subscription.
Select an option below:

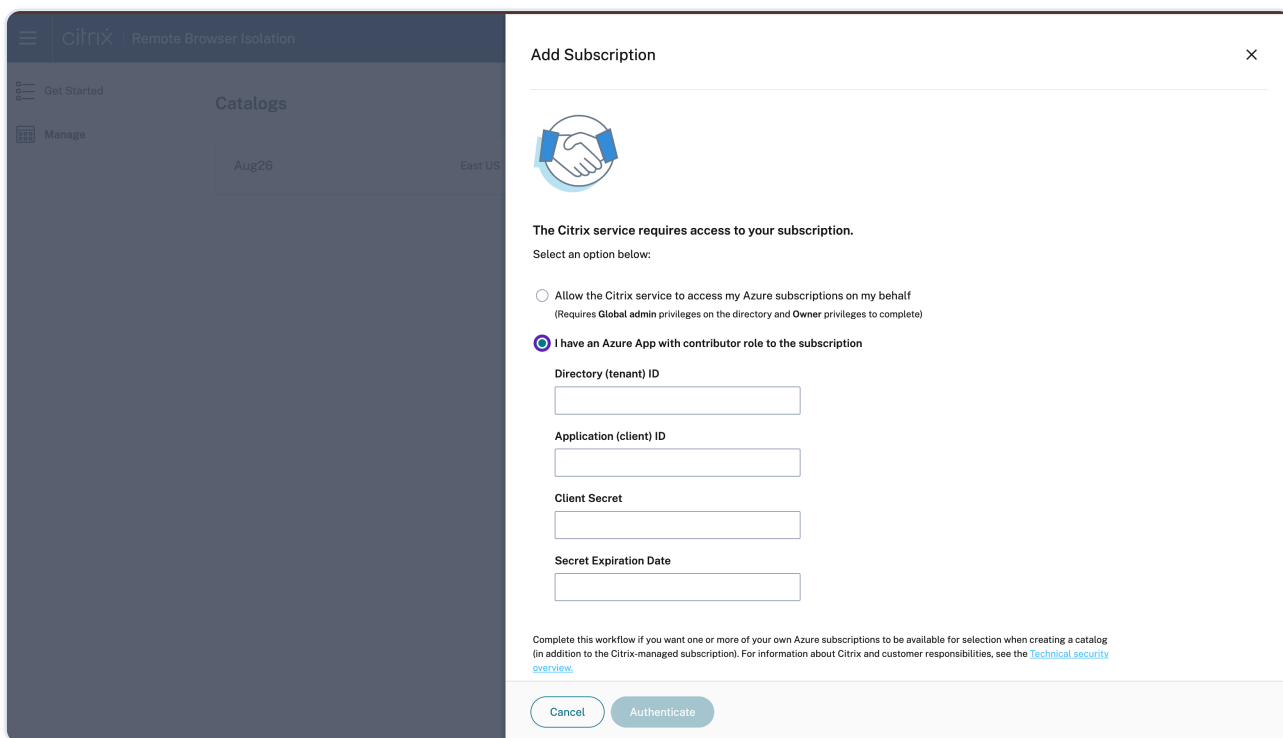
☒ Allow the Citrix service to access my Azure subscriptions on my behalf
(Requires Global admin privileges on the directory and Owner privileges to complete)

☐ I have an Azure App with contributor role to the subscription

Complete this workflow if you want one or more of your own Azure subscriptions to be available for selection when creating a catalog (in addition to the Citrix-managed subscription). For information about Citrix and customer responsibilities, see the [Technical security overview](#).

Cancel Authenticate

2. サブスクリプションに対する共同作成者ロールを持つAzureアプリを持っていますをクリックします。
3. このオプションを有効にするには、ディレクトリID、アプリケーションID、クライアントシークレット、およびシークレット有効期限を入力し、**認証**をクリックします。
4. サブスクリプションの詳細を検証した後、**サブスクリプションの追加**をクリックします。



Add Subscription

The Citrix service requires access to your subscription.
Select an option below:

☐ Allow the Citrix service to access my Azure subscriptions on my behalf
(Requires Global admin privileges on the directory and Owner privileges to complete)

☒ I have an Azure App with contributor role to the subscription

Directory (tenant) ID

Application (client) ID

Client Secret

Secret Expiration Date

Complete this workflow if you want one or more of your own Azure subscriptions to be available for selection when creating a catalog (in addition to the Citrix-managed subscription). For information about Citrix and customer responsibilities, see the [Technical security overview](#).

Cancel Authenticate

注:

複数のAzureサブスクリプションをRBIセルフホスト型ワークロードにリンクできます。Azureサブスクリプションは新規でも再利用でも構いません。RBIセルフホスト型ワークロードは、仮想ネットワーク（VNet）を作成し、その境界内にマシンを展開します。

ステップ2：アプリケーションカタログの作成

カタログはブラウザアプリのコンテナです。グループごとに異なるカタログを作成することで、ブラウザアプリを整理できます。カタログ内のマシンはサイズと設定が同じですが、異なるカタログのマシンはサイズと設定が異なる場合があります。さらに、カタログ間でリージョンも異なる場合があります、これはエンドユーザーの起動パフォーマンスを最適化するのに役立ちます。

新しくリンクされたサブスクリプションでカタログを作成するには、約90分かかります。このプロセスでは、マシンの管理に必要なリソースグループを含め、Azureに必要なリソースが展開されます。

1. Citrix Cloud™ ページで、**Manage RBI Service > Create Catalog** をクリックします。
2. **Create Remote Browser Isolation Catalog** ページで、カタログの名前を入力し、**Add remote isolated browser** をクリックします。

注:

カタログ作成を選択すると、迅速な展開のためにデフォルト設定が適用されます。

3. **Next: Machine Settings** をクリックし、以下の詳細を入力します。

- サブスクリプション
- マシン設定
- リージョン

注:

電源スケジュール設定はデフォルトで無効になっていますが、ユーザーはこれを構成するオプションがあります。

4. **Next: Summary > Create Catalog** をクリックします。
5. カatalogが作成されたら、**View Details** をクリックします。

カタログ構成のハイライト:

- カタログ作成により、顧客のワークロードに必要なすべてが設定され、ワンクリックで完了します。
- 顧客は、マシンに対する独自の電源管理サイクルを選択し、カタログ内でブラウザを公開できます。
- 顧客が複数のサブスクリプションを持っている場合、カタログをどこに展開するかを選択できます。
- Citrix Catalog Service はワークロードを管理します。
- ソフトウェアパッチとアップデートは、顧客が構成したマシンの電源管理設定に基づいて自動的に展開されます。
- カタログ内のマシンはコネクタレスモード (DaaS 用 Rendezvous V2 ポリシー) で動作します。これは、顧客のリソースグループにコネクタの展開が不要であることを意味します。

ステップ 2.1: Secure Private Access (SPA) アプリセッションにカタログを割り当てる

顧客管理者は、SPA セッションに使用するカタログを選択でき、この目的のために特定のカタログを割り当てることができます。

前提条件:

このオプションで SPA RBI アプリを正常に起動するには、少なくとも1つのカタログが有効になっている必要があります。

Secure Private Access セッションを有効にする方法:

1. Citrix Cloud ページで、**Manage RBI Service** をクリックします。
2. **Manage** をクリックし、作成したカタログに移動して、**View Details** をクリックします。
3. **Configuration Details** ページで、**Allow Secure Private Access sessions to use this catalog** のトグルオプションを有効にします。

×

Remote Isolated BrowsersMachinesPower ManagementConfiguration Details

Region
East US

Azure subscription

Refresh

Work load
Standard_D2s_v3

Storage type
Standard disks (HDD)

Machines
1

Remote Browser Isolation version
1.0.0-connectorless

Linux VDA version
private-22.03.2000.43

Catalog Public IP address
--

+ Add secure web gateway ?

☒ Allow Secure Private Access sessions to use this catalog

☐ Enable NAT Gateway

Delete Catalog

注:

このオプションで複数のカタログを選択できます。複数のカタログが選択されている場合、SPA の起動は、起動リクエストが行われた場所から最も近いリージョンのカタログに移動します。

ステップ 3: ブラウザアプリケーションを公開する

ブラウザアプリケーションを作成する

以下の手順に従って、リモート分離ブラウザを追加します。

1. RBIセルフホスト型ワークロードコンソールの**管理**タブでカタログをクリックします。
2. **リモート分離ブラウザの追加**をクリックし、以下の構成詳細を指定します。

- **ブラウザ名:** 任意の名前を入力します。
- **URL:** ターゲットアプリケーションのURLを指定します。

注:

リモートブラウザは、安全な分離環境でホストされます。URLはインターネット経由でアクセス可能である必要があります。

- **タイプ:** 共有パスコードまたは**認証済み**を選択します。これはエンドユーザーに表示されます。
- **パスコード** パスコードを入力します。
- **アイコン:** アプリアイコンをアップロードします。

3. **リモート分離ブラウザの追加**をクリックします。

The screenshot shows the Citrix Remote Browser Isolation console interface. On the left, there's a sidebar with 'Get Started' and 'Manage' options. The main area displays 'Catalogs' with a table containing columns for 'Aug26' and 'East US'. Overlaid on the right is a modal window titled 'Add remote isolated browser'. This modal has a close button (X) in the top right corner. Below the title, it states '*All fields required unless marked optional.' The form includes:

- A text input field for 'Remote isolated browser name'.
- A text input field for 'URL'.
- A 'Type' section with two radio buttons: 'Shared passcode' (which is selected) and 'Authenticated'.
- A text input field for 'Passcode'.
- An 'Icon' section showing a Chrome icon and a 'Change Icon' button.

 At the bottom of the modal, there are two buttons: 'Add remote isolated browser' and 'Cancel'.

ブラウザアプリケーションにポリシーを割り当てる

ブラウザが作成されたら、ブラウザに必要なポリシーを構成できます。

「ポリシーの管理」 (/en-us/citrix-remote-browser-isolation/media/rbi-shw-manage-policies.png)

1. 省略記号をクリックし、「**ポリシーの管理**」をクリックします。

2. 目的のポリシーを有効にし、「**保存**」をクリックします。

「ポリシーの管理2」 (/en-us/citrix-remote-browser-isolation/media/rbi-shw-manage-policies2.png)

ブラウザアプリケーションにユーザーを追加する

お客様は、カタログ内の公開されたブラウザにユーザーとグループを割り当てるために、自身のドメインとIDプロバイダーを導入する必要があります。

「ユーザーの管理」 (/en-us/citrix-remote-browser-isolation/media/rbi-shw-manage-users.png)

1. ユーザーをサブスクライブするには、省略記号をクリックし、「**ユーザーの管理**」を選択します。
2. 次に、ドメインを選択し、ドロップダウンメニューからグループまたはユーザーを選択します。

「ユーザーの管理2」 (/en-us/citrix-remote-browser-isolation/media/rbi-shw-manage-users2.png)

ステップ4: ブラウザアプリケーションをテストして共有する

ストアを介して、またはWebブラウザでURLを直接開くことによって、公開されたブラウザにアクセスできるようになりました。起動リクエストは、アカウント内の割り当てられたカタログ内のマシンに送られます。

注:

カタログのマシンの電源管理が設定されておらず、実行中のマシンがない場合、セッションを起動するとマシンの起動がトリガーされ、その後、セッションを受け入れる準備が整うまで待機します。

ブラウザを削除する:

削除したいブラウザを選択し、**削除**アイコンをクリックします。

マシンの再起動または強制再起動:

マシン名の横にある省略記号をクリックし、目的のオプションをクリックします。

その他の機能

ユーザーアクティビティログ

ユーザーアクティビティログ機能を使用すると、顧客はCitrix Remote Browser Isolation (RBI) セッション中のユーザーのブラウジングアクティビティを追跡および監査できます。この機能は、アクセスしたホスト名、アクセス時刻、ユーザー識別子、および許可リストの適用状況をキャプチャします。収集されたすべてのデータは、顧客のAzureストレージアカウントに保存され、データの完全な所有権と制御が提供されます。

重要:

この機能は、顧客レベルとアプリケーションレベルの両方で有効にする必要があります。ブラウジングアクティビティデータは1時間ごとにアップロードされ、リアルタイムではありません。

主な利点

- **コンプライアンスと監査:** 企業の監査要件を満たし、規制コンプライアンス基準に準拠します。
- **セキュリティ分析:** 異常なブラウジングパターンを特定し、潜在的なセキュリティ脅威を検出します。
- **ポリシーの最適化:** ユーザーの行動を分析して、許可リストの構成を改善します。
- **データ主権:** Azure環境でデータを管理下に置きます。

前提条件

ユーザーアクティビティログを設定する前に、以下があることを確認してください。

- 有効なAzureサブスクリプション。
- ブラウジングアクティビティデータ用のAzureストレージアカウント。
- Remote Browser Isolationサービスの下に作成されたカタログ。

設定手順

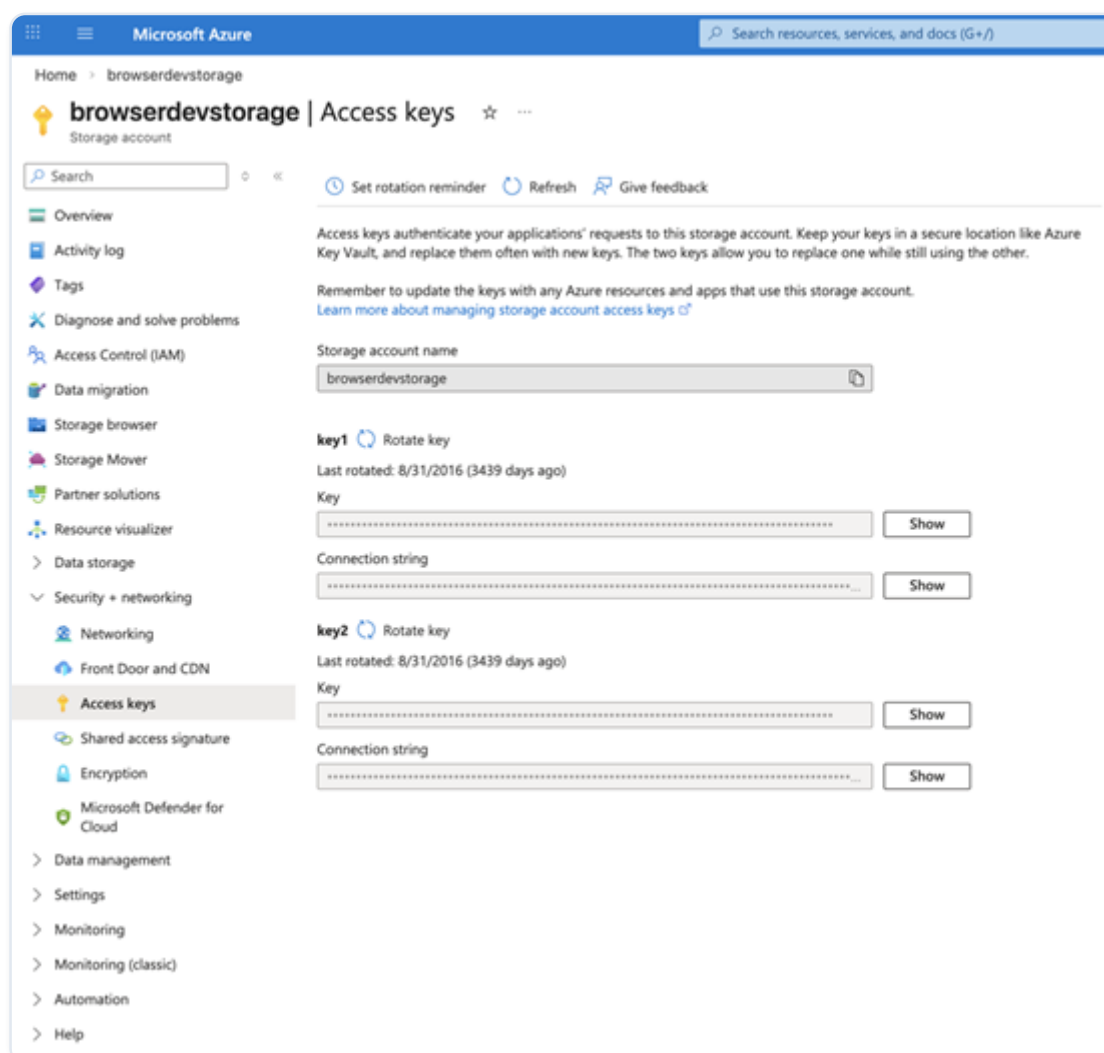
ステップ1：Azure Storage接続文字列の取得

このガイドでは、Azure Storageアカウントが既に存在することを前提としています。作成方法については、[Azure Storageドキュメント](#)を参照してください。

1. [Azure portal](#)にサインインし、ストレージアカウントを開きます。
2. 左側のメニューで、**セキュリティ + ネットワーク**に移動し、**アクセスキー**を選択します。
3. key1またはkey2から**接続文字列**をコピーします。
4. ステップ3（機能が動作していることを確認する）で使用するために、接続文字列を安全に保管してください。

注：

Citrix RBIは、構成を保存すると `user-activity` という名前のコンテナを自動的に作成します。手動でのコンテナ作成は不要です。



ステップ2：アプリケーションのユーザーアクティビティログを構成する

Azure Storage接続は、アプリケーションごとに構成できます。

構成の作成または更新

1. 管理コンソールで、**管理**ページに移動します。
2. ユーザーアクティビティログを有効にするカタログとアプリケーションを選択します。
3. 「ユーザーアクティビティログ」設定を見つけます。
4. 「ユーザーアクティビティログ」を有効にします。
5. ステップ1のAzure Storage接続文字列を貼り付けます。
6. 「**保存**」をクリックします。

セッションモニターテスト(/en-us/citrix-remote-browser-isolation/media/session-monitor-test.png)

ユーザーアクティビティログ(/en-us/citrix-remote-browser-isolation/media/user-activity-logging.png)

構成が保存されると、システムは次の処理を行います。

- 接続文字列を検証します。
- Azure Storageへの接続を確認します。
- `user-activity` という名前のコンテナが存在しない場合は作成します。
- 接続権限を確認します。

構成の削除

特定のアプリケーションの閲覧アクティビティの追跡を停止するには：

1. そのアプリケーションの設定ページに移動します。
2. 「ユーザーアクティビティログ」設定を見つけます。
3. 「ユーザーアクティビティログ」を無効にします。
4. 「**保存**」をクリックします。

設定を削除すると、新しく起動されたユーザーセッションはブラウジングアクティビティを記録しなくなります。すでにAzure Storageにアップロードされている履歴データは削除されません。

ステップ3：機能が動作していることを確認する

設定が完了したら、機能を検証します。

1. ユーザーアクティビティログが設定されたアプリケーションを使用して、新しいブラウザセッションを起動します。
2. たとえば、`www.google.com` や `www.microsoft.com` など、いくつかのWebサイトにアクセスします。
3. アップロードを待ちます。ブラウジングアクティビティはまずローカルに保存され、1時間ごとにアップロードされます。
4. 初回確認の場合は、少なくとも1～2時間待ちます。
5. Azureポータルで、ストレージアカウントを開き、次に `user-activity` コンテナを開きます。
6. 新しいJSONファイルが表示されることを確認します。
7. JSONファイルをダウンロードし、アクセスしたWebサイトのホスト名が含まれていることを確認します。

ブラウジングアクティビティの表示と分析

データストレージ構造

ブラウジングアクティビティデータは、Azure Blob Storageに日付とファイル名で整理されています。

```
Container: user-activity
```

```
| - YYYY-MM-DD/
```

```
|   | - {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json
```

```
|   | - {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json
```

```
|   ` - {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json
```

```
` - YYYY-MM-DD/
```

```
    ` - ...
```

ファイル命名規則

- フォルダー構造: `{YYYY-MM-DD}/` (日付別に整理されています)。
- ファイル名のパターン: `{VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json`

- `{VDAHostname}` : VDAマシンのホスト名。
- `{GUID}` : 各アップロードバッチの一意的識別子。
- `{AppName}` : Secure Browserアプリケーションの名前。
- `{YYYY-MM-DD-HH}` : 24時間形式のアップロードタイムスタンプ。

アクティブなVDAごとに、1時間ごとに新しいファイルが生成されます。

データ形式の説明

各JSONファイルには、NDJSON形式（改行区切りJSON）で複数のレコードが含まれています。各行は1つのアクセスイベントを表します。

```
{"accessHostEvent":  
{"hostname":"www.google.com","acceptHost":true},"accessTime":"2026-01-29T14:23:45.123Z","sessionId":"abc123-def456-ghi789","userName":"user@example.com","appName":"MySecureBrowser"}  
  
{"accessHostEvent":  
{"hostname":"www.microsoft.com","acceptHost":true},"accessTime":"2026-01-29T14:25:10.456Z","sessionId":"abc123-def456-ghi789","userName":"user@example.com","appName":"MySecureBrowser"}  
  
{"accessHostEvent":  
{"hostname":"malicious.site","acceptHost":false},"accessTime":"2026-01-29T14:30:22.789Z","sessionId":"abc123-def456-ghi789","userName":"user@example.com","appName":"MySecureBrowser"}
```

フィールドの説明

フィールド	説明	例
<code>accessHostEvent.hostname</code>	ユーザーがアクセスしたWebサイトのホスト名。	<code>www.google.com</code>
<code>accessHostEvent.acceptHost</code>	アクセスが許可リストによって許可されているかどうか (<code>true</code> は許可、 <code>false</code> はブロックを意味します)。	<code>true</code>
<code>accessTime</code>	アクセス時刻 (UTC)。	<code>2026-01-29T14:23:45.123Z</code>

フィールド	説明	例
sessionId	一意のセッション識別子。	abc123-def456-ghi789
userName	ユーザー識別子。	user@example.com
appName	アプリケーション名。	MySecureBrowser

プライバシー保護: システムは `www.example.com` のようなホスト名のみを記録します。完全な URL パス、クエリパラメータ、またはユーザーが入力したコンテンツは記録しません。

データを表示する方法

閲覧アクティビティの記録を表示するには、以下の方法を使用します。

Azure Storage エクスプローラー

1. [Azure Storage Explorer](#) をダウンロードしてインストールします。
2. ストレージアカウントに接続します。
3. `user-activity` コンテナを参照します。
4. `JSON` ファイルをダウンロードし、その内容を確認します。

Azure ポータル

1. **Azure** ポータルにサインインします。
2. ストレージアカウントに移動します。
3. コンテナ > `user-activity` を選択します。
4. ファイルをダウンロードして内容を表示します。

ヒント: より詳細な分析を行うには、データを Excel、Power BI、または別の分析ツールにインポートしてください。

主な機能と考慮事項

機能のハイライト

- **自動記録:** 手動操作なしでウェブサイトアクセスイベントをキャプチャします。
- **ブロックされた試行も含む:** ブロックされたアクセス試行 (`acceptHost: false`) をキャプチャし、許可リスト分析に利用します。

- **1時間ごとのアップロード:** ネットワークオーバーヘッドを削減するため、データを1時間ごとのバッチでアップロードします。
- **データ主権:** すべてのデータを顧客のAzure環境に保存します。
- **マルチアプリケーション対応:** アプリケーション間で個別の、または共有のストレージアカウント構成をサポートします。

制限事項

- **リアルタイムではない:** データがAzure Storageに表示されるまでに最大1時間かかる場合があります。
- **Dedicated Editionのみ:** Dedicated Editionアプリケーションでのみ利用可能です。
- **固定コンテナ名:** コンテナ名は `user-activity` であり、カスタマイズできません。
- **VDA再起動の影響:** アップロード前にVDAが再起動すると、まだアップロードされていないデータが失われる可能性があります。

トラブルシューティング

問題1: Azure Storageにデータがない

考えられる原因:

- 機能トグルが有効になっていません。
- 接続文字列が正しくないか、期限切れです。
- 待機時間が不十分です (少なくとも1時間が必要です)。
- アプリケーションがDedicated Editionではありません。

解決策:

1. 機能トグルのステータスを確認します。
2. 接続文字列を再構成して保存します。
3. 新しいセッションを開始し、Webサイトにアクセスして、1～2時間待ちます。
4. アプリケーションがDedicated Editionであることを確認します。
5. `user-activity` コンテナが作成されたことを確認します。

問題2: 接続文字列の構成時に検証が失敗する

考えられる原因:

- 接続文字列の形式が正しくありません。

- ストレージアカウントのネットワーク制限によりアクセスがブロックされています。
- コンテナを作成するための権限が不足しています。

解決策:

1. Azure ポータルから完全な接続文字列を再度コピーします。
2. ストレージアカウントのファイアウォール設定を確認します。テストのために、一時的に広範なネットワークアクセスを許可します。
3. 接続文字列がコンテナ作成権限を付与していることを確認します。
4. ストレージアカウントがロックされていないか、その他の制限を受けていないことを確認します。

問題3: データアップロード後にユーザーセッションが中断されるか、遅くなる

いいえ、データアップロードはバックグラウンドで実行され、通常のブラウザ使用を中断することはありません。アップロードは、最小限のリソース消費で非同期I/Oを使用します。

問題4: アクティブなユーザーセッションに構成はすぐに適用されますか?

いいえ、更新された設定を適用するには、ユーザーは現在のセッションを閉じて新しいセッションを開始する必要があります。アクティブなセッションは、起動時に存在していた構成を引き続き使用します。

問題5: 複数のアプリケーションで同じストレージアカウントを使用できますか?

はい、複数のアプリケーションで同じストレージアカウントと `user-activity` コンテナを共有できます。ファイル命名と `appName` フィールドは、アプリケーション間のデータを区別するのに役立ちます。

クローム エンタープライズ プレミアム (CEP) との統合

このトピックでは、Linux VDA 向けの Citrix Remote Browser Isolation (RBI) と Google Chrome Enterprise Premium (CEP) の統合について説明します。この機能で何が可能になるか、どのように機能するか、および管理者が有効にする前に知っておくべきことについて説明します。

はじめに

Google Chrome Enterprise Premium (CEP) は、エンタープライズ環境向けに高度なセキュリティ、ブラウザ管理、およびポリシー適用を提供します。この機能により、Citrix RBI ブラウザは Google 登録トークンを使用して Chrome Enterprise ポリシーに登録できます。管理者は、Google 管理コンソールから組織および部門のセキュアブラウザポリシーを一元的に管理できます。

この統合により、EDR エージェントを必要とせずに、信頼されていないエンドポイントデバイスにセキュリティとコンプライアンスを適用するための、スケーラブルでクラウド管理されたアプローチが提供されます。

この機能でできること

CEP 統合により:

管理者は次のことができます:

- 同じカタログ内のすべての Citrix RBI ブラウザユーザーに Chrome Enterprise ポリシーを適用します。
- Google 管理コンソールを通じてこれらのポリシーを一元的に管理します。

ユーザーは次のことができます:

- 登録後に管理対象ブラウザとなる RBI ブラウザを使用します。
- コピー＆ペースト制御や URL ブロックリストなど、一貫したエンタープライズポリシーを受け取ります。
- Google Cloud から自動ポリシー更新を受け取ります。

使用方法

準備

CEP 統合を有効にする前に:

1. Google Workspace が Chrome Enterprise Premium をサポートしていることを確認します。
2. 少なくとも1つのCitrix RBIカタログが存在することを確認します。存在しない場合は、作成します。
3. どのRBIカタログがChromeポリシーによって管理される必要があるかを特定します。
4. 必要に応じて、Google管理コンソールで組織単位 (OU) ごとに登録トークンを1つ生成します。

Citrix Cloudポータルでの構成

CEPでは、各カタログに登録トークンが必要です。Citrixは、そのカタログから起動されたユーザーセッションにトークンを自動的に配布します。

登録フロー

1. Google管理コンソールから登録トークンを取得します。

2. Citrix Cloudにサインインし、Remote Browser Isolationに移動します。
3. 左側のメニューで**管理**を選択します。
4. ターゲットカタログを選択し、**構成の詳細**を開きます。
5. **Googleトークン登録を有効にする**を有効にし、登録トークンを入力します。
6. **トークンを適用**を選択します。

CEP統合(/en-us/citrix-remote-browser-isolation/media/cep-integration.png)

ユーザーがそのカタログの下でセキュアブラウザアプリケーションを起動すると、トークン登録が自動的に行われ、CEPに登録されたブラウザでブラウジングが続行されます。

管理者タスク

- 「**Googleトークン登録を有効にする**」を無効にするか再度有効にするか、または登録トークンを更新します。
- `chrome://policy` を使用してChromeポリシーの適用を監視します。
- Google管理デバイスリストを定期的に確認し、古いレコードを削除します。

制限事項と既知の動作

ユーザープロファイルの同期はサポートされていません

Chromeユーザープロファイルのクラウド同期は、CEPトークン登録済みのRBIブラウザ内では機能しません。

構成変更ごとに再起動が必要です

RBIは一時的なファイルシステムを使用するため、管理者がCEP統合を有効または無効にする場合、またはCEPトークンを更新する場合には再起動が必要です。

許可リストポリシーの動作

カタログ下のRBIブラウザアプリケーション用に構成された許可リストがデフォルトの `*:*` から変更された場合、CEP登録を完了するために `*.google.com:*` を含めます。CEPが起動された後、RBI許可リストポリシーは適用されません。

Google管理に重複するデバイスが表示される場合があります

イメージアップグレード後、マシンは新しいIDを受け取ることがあります。これにより、Google管理コンソールに追加のデバイスレコードが作成される可能性があります。

カタログ下のマシンを再起動します

カタログにリストされている各マシンについて：

1. 右側のメニューを選択します。
2. 「再起動」を選択します。

マシンの再起動(/en-us/citrix-remote-browser-isolation/media/reboot-machine.png)

顧客管理RBIカタログ仮想ネットワーク用のAzure Firewallの構成

Azure Firewallを使用すると、Remote Browser Isolationサービス内のカタログマシンからの送信Webリクエストをフィルタリングできます。既存のAzure仮想ネットワークにAzure Firewallをデプロイすることで、送信トラフィックを制御および監視できます。これにより、ネットワークセキュリティを強化し、ワークロードの送信接続を管理できます。

前提条件:

- AzureサブスクリプションのRemote Browser Isolationサービスで作成されたカタログ。
- Azureリソースを作成および管理するための十分な権限。

Azure仮想ネットワークを特定する

1. **Citrix Cloud DaaS**コンソールで、保護するマシンカタログを特定します。
2. カタログからマシンを選択し、その名前の最初の部分をコピーします (例: RBI3BLR6-O80001)。
3. Azureポータルで、この名前を使用してVMを検索します。
4. VMの概要で、「リンクされた仮想ネットワーク」を選択します。

Azure Firewallを作成する

1. 仮想ネットワークのメニューで、「設定」の下にある「サブネット」を選択します。
2. 用途を「**Azure Firewall**」に設定して新しいサブネットを追加します (既定の設定を使用)。
3. 仮想ネットワークの概要に戻り、**Capabilities** の下にある **Azure Firewall** を選択します。
4. **Add a new firewall** をクリックします。
5. 次のフィールドに入力します。

- **Subscription** と **Resource group**: 適切に選択します。

- **Name:** ファイアウォールの名前を入力します。
- **Region:** 仮想ネットワークのリージョンと一致させます。
- **Firewall tier:** **Standard** を選択します。
- **Virtual Network:** ステップ1で特定したネットワークを選択します。
- **ファイアウォールポリシー:** このファイアウォールを管理するファイアウォールポリシーを使用する を選択します。
- **Policy Name:** **Add new** をクリックし、名前を入力します (例: Test-policy)。
- **Firewall Management NIC:** この設定を無効にします。

6. 設定を確認し、ファイアウォールを作成します。

ルーティングの構成

1. デプロイ後、Azure Firewall リソースを開き、そのプライベートIPアドレスをメモします。
2. Azure portal で、仮想ネットワークに移動し、**Subnets** を選択します。
3. カタログVMが配置されているサブネットを特定します（通常はdefaultという名前です）。
4. 新しいルートテーブルを作成するか、このサブネットに関連付けられている既存のルートテーブルを選択します。
5. 新しいルートを追加します。

- **宛先:** 0.0.0.0/0
- **ネクストホップの種類:** Virtual appliance
- **ネクストホップアドレス:** Azure FirewallのプライベートIPアドレスを入力します。

6. ルートを保存します。

ファイアウォール規則を構成する

1. Azureポータルで、**Firewall Manager > Azure Firewall Policies**に移動します。
2. 作成したポリシー（例：Test-policy）を選択します。
3. **規則**に移動します。
4. 新しい**アプリケーション規則コレクション**を追加します（Webフィルタリングに推奨）。
5. 特定のFQDNまたはURLカテゴリを許可または拒否する規則を定義します。たとえば、`www.example.com` へのアクセスを拒否するには、次のようにします。

- **名前:** DenyExampleWebsite

- 送信元IPアドレス: カタログVMのサブネット範囲。
- 宛先FQDN: `www.example.com`
- プロトコル: `http:80` , `https`
- アクション: `Deny`

6. ルールコレクションを保存します。

7. 必要に応じて、追加の許可または拒否ルールを追加し、それに応じて優先順位を調整します。
(オプション)

構成のテスト

1. 構成済みのカタログ内のマシンからブラウザセッションを起動します。
2. 許可されたWebサイトとブロックされたWebサイトの両方にアクセスしてみて、アクセスコントロールが正しく機能していることを確認します。
3. 定義されたルールに従って、ファイアウォールがネットワークトラフィックを正しくフィルタリングしていることを確認します。

トラブルシューティング

問題が発生した場合は、[Azure Firewall ドキュメント](#) を参照してください。

制限事項

同じカタログ内のすべてのブラウザは、同じファイアウォール、ポリシー、およびルールを使用します。

ソフトウェアのアップグレードとパッチ管理

Citrix は、ソフトウェア管理を含むマシンイメージとカタログを作成および管理します。新しいバージョンのカタログが利用可能になると、Citrix はこれらのアップグレードを顧客カタログにプッシュし、マシンが次回再起動されたときに最新の修正とパッチを受け取るようにします。RBI は、DaaS Catalog サービスを使用して、顧客のサブスクリプションでこれらのアップグレードを容易にします。

Citrix® StoreFront Cloudとの統合

Remote Browser IsolationはStoreFront Cloudと統合できます。統合されていることを確認するには、次の手順を実行します。

1. [Citrix Cloud](#)にサインインします。
2. 左上のメニューで、**StoreFront Cloud**を選択します。
3. **Service Integrations**タブを選択します。
4. Remote Browser Isolationサービスのエントリが**Enabled**と表示されていることを確認します。表示されていない場合は、省略記号メニューをクリックして**Enable**を選択します。

まだ設定していない場合は、[ストアへの認証を構成する](#)で説明されているように、ストアのストアURL、外部接続、およびストア認証を構成します。

Remote Browser Isolationは、Active DirectoryおよびMicrosoft Entra IDによる認証をサポートしています。Active Directoryによる認証はデフォルトで構成されています。Microsoft Entra IDを使用した認証の構成については、[Microsoft Entra IDをCitrix Cloudに接続する](#)を参照してください。

Microsoft Entra IDを使用して認証を構成する場合、Active Directoryドメインコントローラーを含むオンプレミスドメインには、1つ（できれば2つ）のCloud Connectorが含まれている必要があります。

オンプレミスのStoreFrontとの統合

オンプレミスのStoreFrontを使用しているCitrix Virtual Apps and Desktops™のお客様は、Remote Browser Isolationサービスと簡単に統合して、次の利点を得ることができます。

- 公開されているリモート分離ブラウザーを既存のCitrix Virtual Apps™およびDesktopsアプリと集約し、統合されたストアエクスペリエンスを実現します。
- 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向上させます。
- StoreFrontと統合された既存の多要素認証ソリューションを使用することで、Remote Browser Isolationの起動のセキュリティを強化します。

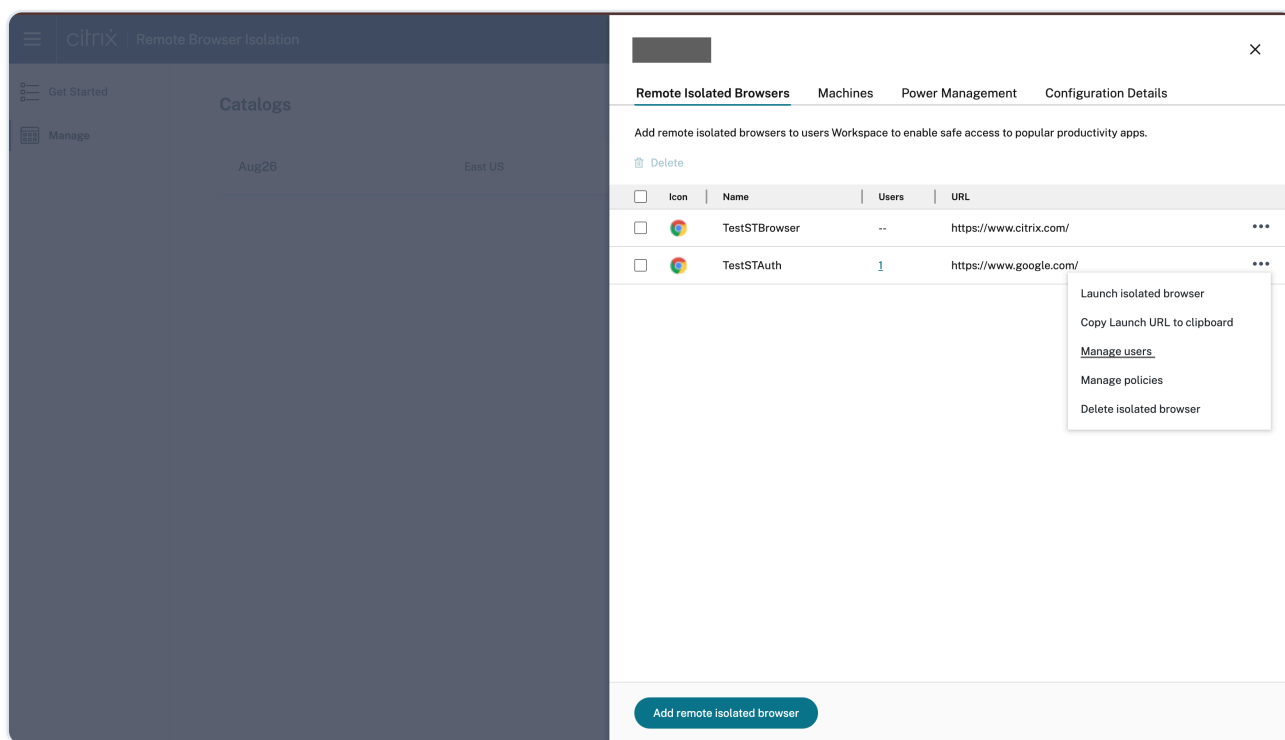
詳細については、[CTX230272](#)およびStoreFront構成ドキュメントを参照してください。

リモート分離ブラウザの管理と監視

公開されたブラウザのポリシーやその他の構成を管理し、Remote Browser Isolation でアクティブなユーザーセッションを監視できます。

管理

「管理」タブには、既存のRemote Browser Isolation (RBI) カタログが一覧表示されます。既存のカタログを選択して、公開されたブラウザの構成を更新できます。公開されたブラウザ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た後、何も変更しないと決めた場合は、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。



以下のタスクを使用して、公開された分離ブラウザを管理できます。

- **公開されたブラウザを起動:** 公開されたブラウザセッションを開きます。ブラウザを公開した後、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:** 公開されたブラウザのURLをコピーします。このURLをエンドユーザーと共有して、公開されたブラウザにアクセスできます。
- **ポリシー:** 公開されたブラウザのポリシーを設定できます。

✕

Manage policies for [REDACTED]

Clipboard

☒

Enabling clipboard allows copy and paste operations to and from the remote session.

☐ Copy out only
 ☐ Paste in only
 ☒ Copy and paste

Printing

☐ ✕

Enabling printing saves the remote webpage as a PDF and transfers it to the user's device.

Non-kiosk

☐ ✕

Enabling non-kiosk mode restores the interface to the remote browser, allowing the user to access the address bar and create multiple tabs and windows.

Client drive mapping

☐ ✕

Enabling client drive mapping allows the user to upload and download files to and from the remote session when using all versions of Citrix Workspace app except for HTML5. *Only available to paid customers.

URL parameters

☐ ✕

Enabling URL parameters allows a new session's starting URL to be replaced by a different URL provided as a query parameter.

Hostname tracking

☐ ✕

Enabling hostname tracking allows the logging of hostnames visited by users within a session to Citrix Analytics.

Save

Cancel

ポリシーページの次の設定を制御します。

- 。 **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、コピー＆ペースト操作に3つのオプションが利用可能になります。
 - 。 **コピーのみ許可:** ユーザーはRBIセッションからローカルデバイスにコンテンツをコピーできますが、RBIへの貼り付けはブロックされます。
 - 。 **貼り付けのみ:** ユーザーはRBIセッションにコンテンツを貼り付けることができますが、コピーして外部に出すことはブロックされます。

- 。 **コピーと貼り付け:** 完全な双方向クリップボードアクセス。

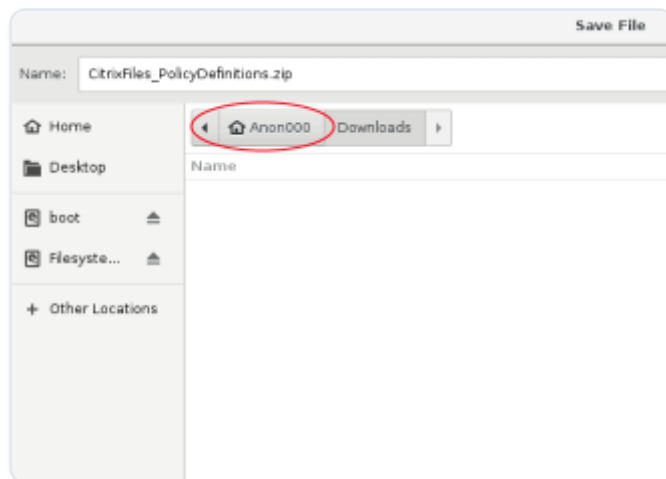
クリップボードポリシーのトグルを無効にすると、Citrix Workspace™ アプリのツールバーからクリップボードボタンが削除されます。

これらのきめ細かいポリシーオプションにより、管理者はリモートセッションとユーザーエンドポイント間のデータフローを詳細に制御できます。たとえば、組織はユーザーがリモートブラウザからテキストをコピーして参照することを許可しつつ、データインジェクションのリスクを減らすためにセッションへの貼り付け操作を防止できます。

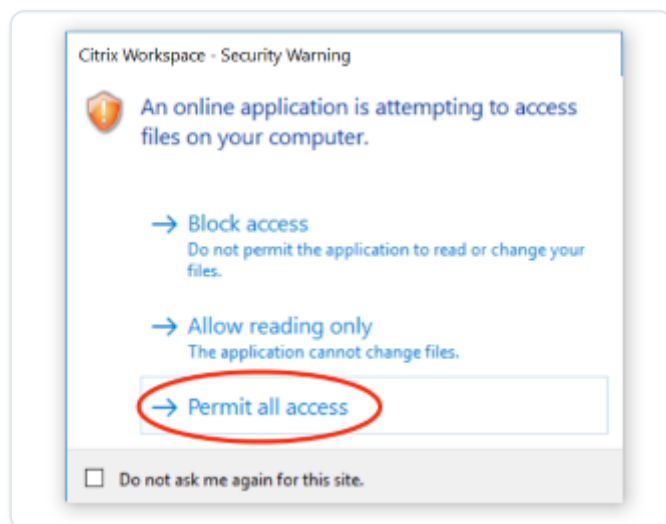
注:

クリップボードポリシーが有効になっていた既存の公開済みブラウザの場合、以前の動作を維持するために、移行中にコピーと貼り付けの両方が自動的に有効になります。管理者の操作は不要です。

- 。 **印刷:** 印刷を有効にすると、リモートのウェブページが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に復元されます。ユーザーはアドレスバーにアクセスし、複数のタブや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、リモートブラウザの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、この設定は有効になっていません（非キオスクモードがオン）。
- 。 **リージョンフェイルオーバー:** リージョンフェイルオーバーポリシーは、現在のリージョンで問題が報告された場合、公開済みブラウザを自動的に別のリージョンに転送します。オプトアウトするには、リージョンフェイルオーバーポリシーを無効にします。**自動リージョン選択**を使用してブラウザを公開した場合、分離されたブラウザ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、この設定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アプリで起動されたセッションでのみ利用可能です。デフォルトでは、この設定は無効になっています。
- 。 ユーザーはダウンロードしたファイルを、**ctxmnt** ディスクの **Anonxxx** ディレクトリにのみ保存する必要があります。そのためには、ファイルを保存する希望の場所に移動する必要があります。例: **Anonxxx > ctxmnt > C > Users > User Name > Documents**。



- 。ダイアログボックスは、**ctxmnt** フォルダーにアクセスするために、ユーザーにすべてのアクセスを許可または読み取りと書き込みの権限を承認するよう促す場合があります。



- 。 **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とき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、疑わしいウェブサイトを特定し、それらをリモートブラウザ分離にリダイレクトするように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。詳細については、[Proof of Concept Guide: URL Redirection to Remote Browser Isolation with Citrix ADC in Azure](#) を参照してください。
- 。 **ホスト名追跡**: ホスト名追跡を使用して、ユーザーセッション中にRemote Browser Isolationがホスト名をログに記録できるようにします。このポリシーはデフォルトで無効になっています。この情報はCitrix Analyticsと共有されます。詳細については、[Citrix Analytics](#)を参照してください。

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を使用して、公開されたRemote Browser Isolation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します。この機能は、外部認証済みWebアプリで利用できます。

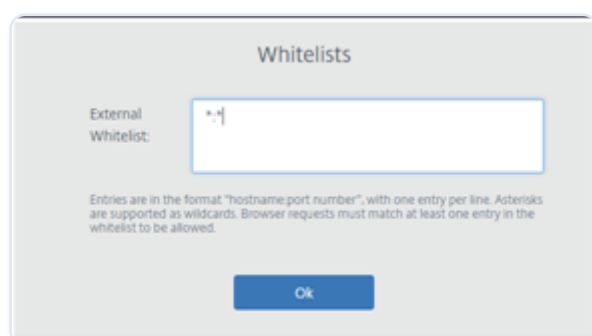
許可リストのエントリを `hostname:port number` の形式で入力します。各エントリを新しい行に指定します。アスタリスクはワイルドカードとしてサポートされています。ブラウザのリクエストは、許可リスト内の少なくとも1つのエントリと一致する必要があります。

例えば、`https://example.com` を許可されたURLとして設定するには:

- `example.com:*` は、任意のポートからこのURLへの接続を許可します。
- `example.com:80` は、ポート80からのみこのURLへの接続を許可します。
- `*:*` は、任意のポートから、および他のURLやポートへの任意のリンクからこのURLへのアクセスを許可します。`*.*` 形式は、公開されたアプリからすべての外部Webアプリへのアクセスを許可します。この形式は、Webアプリの外部ホワイトリストフィールドのデフォルト設定です。

完了したら、**OK**をクリックします。

高度なWebフィルタリング機能は、アクセス制御サービスとの統合を通じて利用できます。詳細については、[ユースケース: アプリへの選択的アクセス](#)を参照してください。



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、エントリの行の末尾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、変更を確定します。

複数のセッションを切断するには、リスト内の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。変更を確定すると、Remote Browser Isolationは選択されたすべてのセッションを直ちに切断します。

Remote Browser Isolationの技術的セキュリティ概要

Remote Browser Isolation（旧Secure Browserサービス）は、Citrixが管理・運用するSaaS製品です。クラウドでホストされる中間Webブラウザを介して、Webアプリケーションへのアクセスを可能にします。

クラウドサービス

Citrix Remote Browser Isolation™サービスは、Virtual Delivery Agent (VDA) 上で動作するWebブラウザと、これらのVDAへのユーザーの管理および接続に使用される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、Citrixコンポーネントのセキュリティとパッチ適用を含む、これらのコンポーネントの運用を管理します。

Remote Browser Isolationサービスの使用中、ホストされているWebブラウザはユーザーの閲覧履歴を追跡し、HTTPリクエストのキャッシュを実行します。Citrixは強制プロファイルを使用し、閲覧セッションが終了するとこのデータが削除されるようにします。

Remote Browser Isolationサービスには、HTML5互換のWebブラウザでアクセスします。このサービスは、ダウンロード可能なクライアントを提供しません。使用中のブラウザとクラウドサービス間のすべてのトラフィックは、業界標準のTLS暗号化を使用して暗号化されます。Remote Browser IsolationはTLS 1.2のみをサポートします。

Remote Browser Isolationの送信トラフィックは、内部ネットワークを保護するために特定のIPアドレスを使用します。許可されているIPアドレスのリストについては、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は、顧客またはサードパーティが所有する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は、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を含め、そのセキュリティに責任を負います。

Remote Browser IsolationとWebアプリケーション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依存します。インターネット上を流れるこのトラフィックを保護するために、管理者はHTTPS URLを公開します。

詳細情報

セキュリティに関する詳細については、以下のリソースを参照してください。

- Citrixセキュリティサイト：<https://www.citrix.com/security>
- Citrix Cloud ドキュメント：[Citrix Cloud Platform 用セキュア展開ガイド](#)

Citrix Remote Browser Isolationのドキュメント履歴

次の表は、Citrix Remote Browser Isolationサービス（旧称Secure Browserサービス）製品のドキュメントに対する重要な変更点です。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

2022年7月より前のRemote Browser Isolationサービスドキュメントの変更については、「[Citrix Cloudのドキュメント履歴](#)」を参照してください。

日付	変更	説明
30 Jun 2025	ソフトウェアアップグレードとパッチ管理.	Citrixは、ソフトウェア管理を含めて、マシンイメージとカタログを作成および管理します。新しいバージョンのカタログが利用可能になると、Citrixはこれらのアップグレードをお客様のカタログにプッシュし、次回の再起動時にマシンに最新の修正とパッチが確実に届くようにします。詳しくは、「 ソフトウェアアップグレードとパッチ管理 」を参照してください。
30 Jun 2025	ネットワークアドレス変換（NAT）（Secure Web）Gatewayを有効にする.	〔構成の詳細〕 ページには、特定のカテゴリ用にSecure Web Gatewayを追加するオプションがあります。詳しくは、「 ネットワークアドレス変換（NAT）（Secure Web）Gatewayを有効にする 」を参照してください。

日付	変更	説明
30 Jun 2025	顧客管理のRBIカタログ仮想ネットワークでAzure Firewallを構成する。	Azure Firewallを使用すると、Remote Browser Isolationサービスでカタログマシンからの送信Web要求をフィルタリングできます。既存のAzure仮想ネットワークにAzure Firewallを展開することで、送信トラフィックを制御および監視できます。詳しくは、「 顧客管理のRBIカタログ仮想ネットワークでのAzure Firewallの構成 」を参照してください。
30 Jun 2025	Remote Browser Isolationの自己ホストワークロード。	Remote Browser Isolationの自己ホストワークロードにより、お客様は自社のAzureサブスクリプション内でリモートブラウザのワークロードを操作できます。詳しくは、「 Remote Browser Isolation - 自己ホストワークロード 」を参照してください。
05 Oct 2022	Secure BrowserはRemote Browser Isolationになります。	Secure Browserという名称がRemote Browser Isolationに変更されます。
27 Jul 2022	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。	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、ユーザーがCitrix Workspaceのサインインページでサインインできるようにします。詳しくは、「 新機能 」を参照してください。