Citrix Remote Browser Isolation™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Remote Browser Isolation 2

What's new 3

Get started with Remote Browser Isolation 5

Additional Features 14

Manage and monitor remote isolated browsers 29

Remote Browser Isolation technical security overview 34

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

Remote Browser Isolation

June 22, 2026

The Citrix Remote Browser Isolation™ service (formerly Secure Browser service) isolates web browsing to protect the corporate network from browser-based attacks. Remote Browser Isolation service delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration. Administrators can rapidly roll out remote isolated browsers, providing instant time-to-value. By isolating internet browsing, IT administrators can offer end users safe internet access without compromising enterprise security.

Users log on to their store and can open web apps in the configured web browser. The website does not directly transfer any browsing data to or from the user device, so the experience is secure.

The Remote Browser Isolation service can publish remote isolated browsers for use with:

- **Shared Passcode external web apps:** If you publish a browser with shared passcode authentication, users must enter the passcode to launch an app.
- **Authenticated external web apps:** When you publish authenticated external web apps and launch the apps from their store, the Remote Browser Isolation service requires a resource location containing at least one Cloud Connector (two or more are recommended). You must add users for the authenticated apps. For details, see Citrix Cloud Connector.
- **Unauthenticated external web apps:** When you publish unauthenticated external web apps and launch the apps from their store, the Remote Browser Isolation service requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector.

  Although typically not recommended, unauthenticated external web apps might be used for a simple proof of concept.

For more information, see Publish a remote isolated browser.

The service also offers:

- Integration of published apps with Citrix® StoreFront Cloud
- Integration of published apps with on-premises StoreFront
- Simple URL allow list function for security
- Usage monitoring
- Controls for clipboard use, printing, kiosk mode, region failover, and client drive mapping

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

Remote Browser Isolation service with Citrix Secure Private Access™

You can launch the published browsers of the Remote Browser Isolation Service by using the Citrix Secure Private Access console for accessing the Enterprise Web, TCP, and SaaS applications. You can also redirect the unsanctioned websites to open in the published browsers of the Remote Browser Isolation service through Citrix Secure Private Access.

For more information about accessing the isolated remote browsers through Citrix Secure Private Access, see the Configure an access policy with multiple rules and Unsanctioned websites in the Citrix Secure Private Access documentation.

Reference articles

- Secure Private Access service solution overview
- Citrix Cloud
- Self-service search for Remote Browser Isolation (Secure Browser)
- Citrix Enterprise Browser
- Security and Compliance Information
- Developer documentation

What's new in related products

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

What's new

August 25, 2026

August 2026

- **NAT Gateway built into catalog creation**: Network Address Translation (NAT) Gateway is now built into the catalog creation flow, the separate switch is no longer needed.

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

July 2026

- **Granular Copy and Paste clipboard policies**: Administrators can now configure copy and paste policies independently for published remote browsers. Previously, the **Clipboard** policy controlled both copy and paste operations as a single toggle. With this update, the single Clipboard policy is replaced by two granular controls:
  - **Copy** —When enabled, allows users to copy content from the remote browser session to the local clipboard.
  - **Paste** —When enabled, allows users to paste content from the local clipboard into the remote browser session.

  This separation gives administrators fine-grained control over data flow between the remote session and user endpoints. For more information, see Policies.

February 2026

- **Remote Browser Isolation updates**
  - You can now integrate Citrix Remote Browser Isolation™ (RBI) with Google Chrome Enterprise Premium (CEP). Enroll a catalog by using a Google token to apply Chrome enterprise policies at the catalog level. Administrators can centrally manage these policies from the Google Admin Console. For more information see, Integration with Chrome Enterprise Premium (CEP).
  - Administrators can now track and audit user browsing activity during RBI sessions. The logs capture visited websites, access timestamps, user identifiers, and allowlist enforcement status. All collected data is stored in the customer-managed Azure Storage account to ensure full data ownership and control. For more information see, User Activity Logging.

June 2025

- **Remote Browser Isolation - Self-hosted workloads**
  - Remote Browser Isolation (RBI) Self-hosted workloads enable customers to operate remote browser workloads within their own Azure subscriptions. The data plane component (Virtual Desktop Agent) in RBI Self-hosted workloads runs in a customer-provided Azure subscription. This allows customers to scale machines and Catalogs horizontally as needed and to provision multiple Catalogs for better workload categorization.

July 2022

- **Remote Browser Isolation supports authentications for all apps with Microsoft Entra ID**

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

- Users can now sign in to any Remote Browser Isolation app from Citrix Workspace™ using Microsoft Entra ID credentials.
- When Remote Browser Isolation users sign in, they use the Workspace sign-in page that you configured for your site. For more information, see Integration with Citrix Workspace.

September 2021

- **Remote Browser Isolation supports bidirectional audio**
  - Bidirectional audio is available in Remote Browser Isolation.
- **Remote Browser Isolation launches from launch.cloud.com are authenticated by Citrix Cloud authentication**
  - When users launch Remote Browser Isolation apps using the launch.cloud.com URL, Citrix Cloud authentication handles their credentials. This enhances security but does not change the user experience.

March 2021

- **Remote Browser Isolation supports authentication with Microsoft Entra ID**
  - Users can now sign in to Remote Browser Isolation apps from Citrix Workspace using Microsoft Entra ID credentials. For more information, see Integration with Citrix Workspace.
- **Remote Browser Isolation lets you monitor and log off users'active sessions**
  - Remote Browser Isolation provides user name, session ID, client IP, authentication type, application name, session start time, and session duration information about users'active sessions. You can view basic information about each active session and disconnect the session if needed. For more information, see Monitor active sessions.

Releases in 2020

All releases of 2020 contain enhancements that help improve overall performance and stability.

Get started with Remote Browser Isolation

June 22, 2026

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

Remote Browser Isolation - Self-hosted workloads

Remote Browser Isolation (RBI) Self-hosted workloads enable customers to operate remote browser workloads within their own Azure subscriptions. The data plane component (Virtual Desktop Agent) in RBI Self-hosted workloads runs in a customer-provided Azure subscription. This allows customers to scale machines and Catalogs horizontally as needed and to provision multiple Catalogs for better workload categorization.

Prerequisites:

- Citrix Platform Licenses (CPL) license or an RBI Dedicated Entitlement, and a DaaS Premium Entitlement.
- DaaS service must be enabled.

  > **Note:**
  >
  > This step is possible only if the customer tenant has the necessary entitlements.

- Enable the Rendezvous protocol in DaaS.

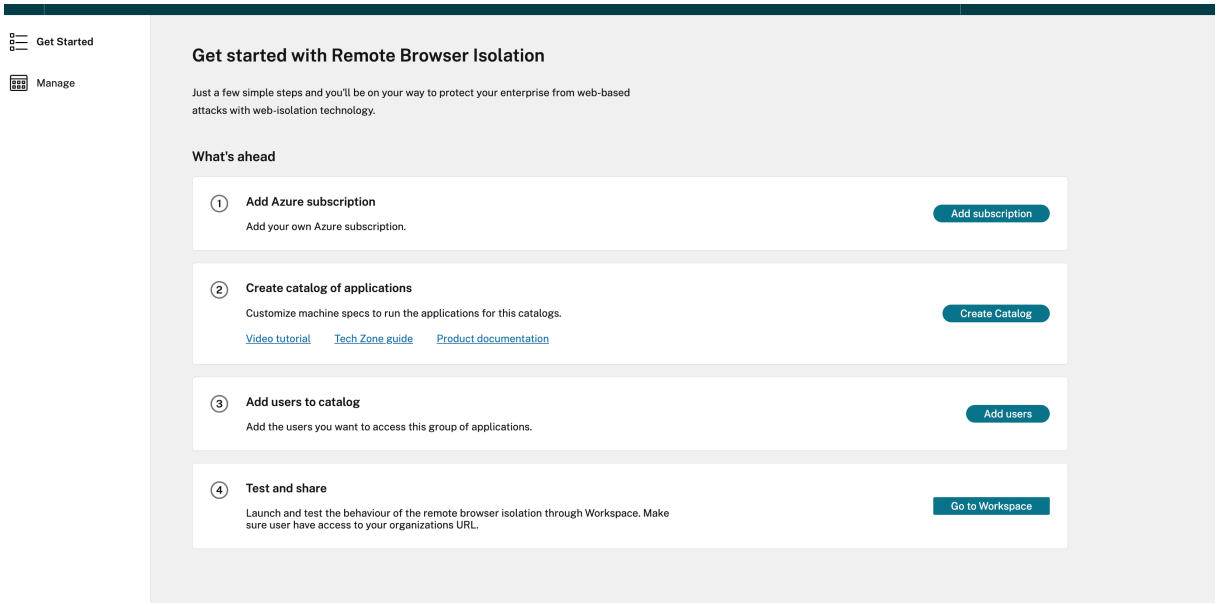
How to Enable DaaS Service

1. Sign in to Citrix Cloud.
2. Navigate to the DaaS service.
3. Locate and click the **Enable DaaS**.
   This step prepares the necessary DaaS infrastructure for RBI Self-hosted workloads and takes approximately 45 minutes.

Onboarding Process for RBI

On the Citrix Cloud page, click **Manage RBI Service** to access the Remote Browser Isolation landing page.

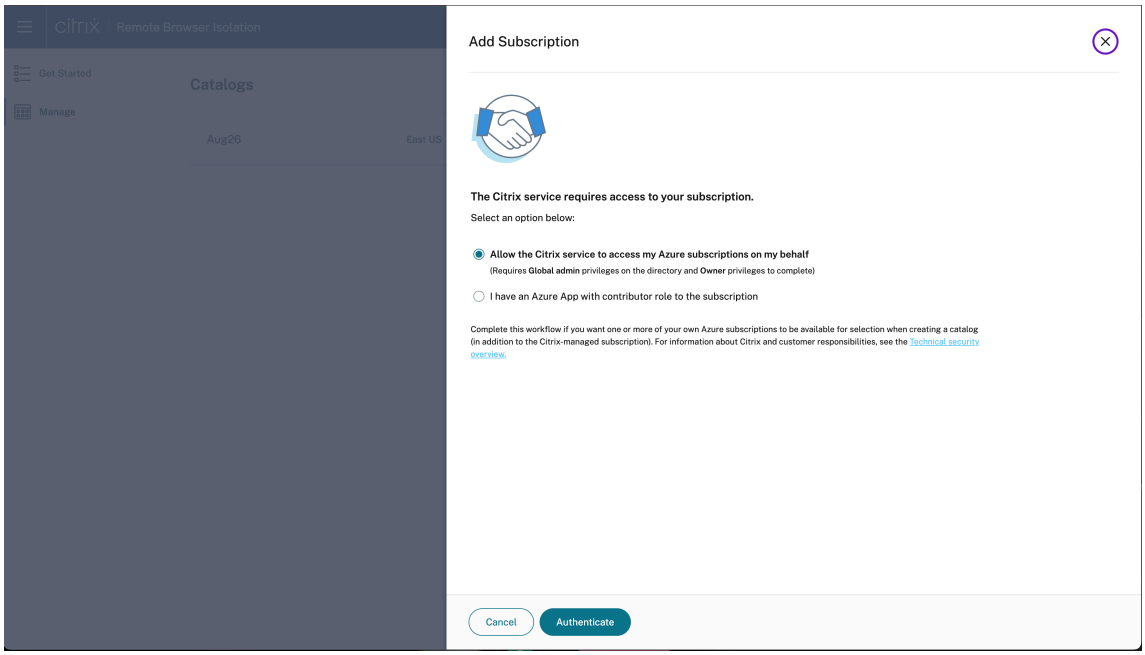
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 1: Add Azure Subscription

1. On the **Get started with Remote Isolation** page, click **Add subscription**. Azure subscriptions can be added to RBI Self-hosted workloads in two ways:

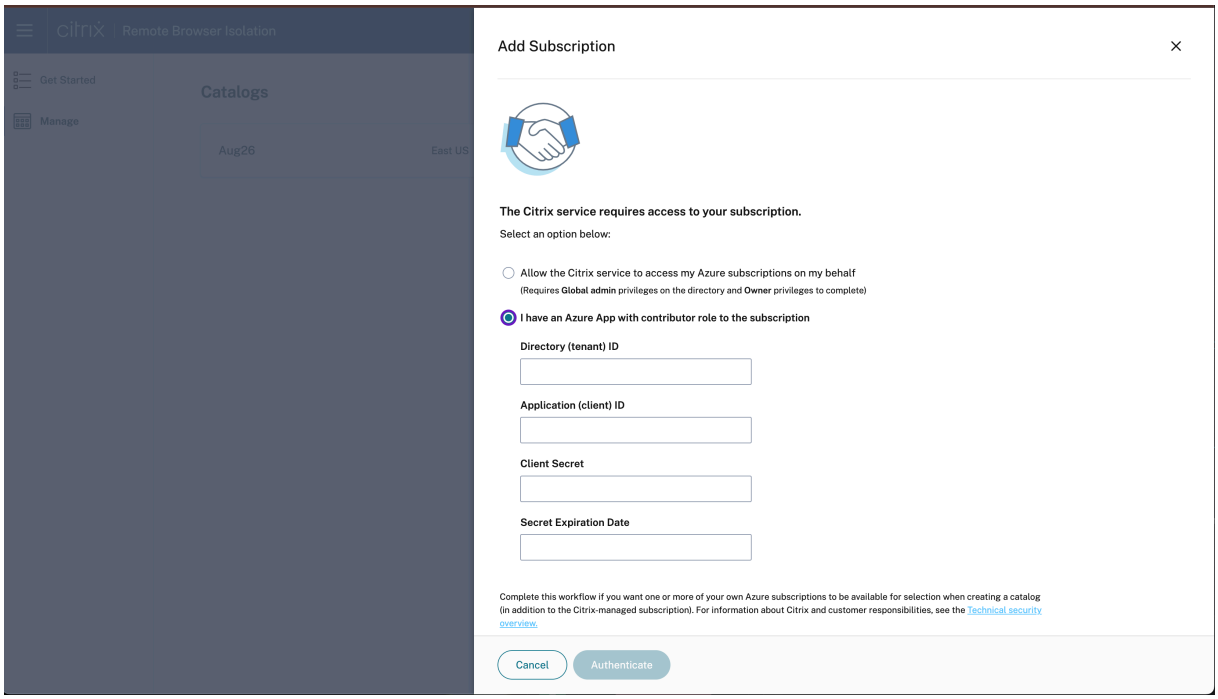
    - Using global admin credentials: **Allow the Citrix service to access my Azure subscription on my behalf**.
    - Using Enterprise App Registrations with Contributor Role on the entire subscription.



2. Click **I have an Azure App with contributor role to the subscription**.

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

3. Provide the **Directory ID**, **Application ID**, **Client Secret**, and **Secret Expiration Date** to enable this option and click **Authenticate**.
4. After validating the subscription details, click **Add subscription**.



> **Note:**
>
> Multiple Azure subscriptions can be linked to RBI Self-hosted workloads. The Azure subscription can be either new or repurposed. RBI Self-hosted workloads create a virtual network (VNet) and deploy the machines within that boundary.

Step 2: Create a catalog of applications Catalogs are containers for browser apps. You can organize browser apps by creating different catalogs for each group.
The machines within a catalog are identical in size and settings, but machines in different catalogs can vary in size and settings. Additionally, the region can also vary between catalogs, which can be useful for optimizing end-user launch performance.

Creating a catalog takes about 90 minutes in a newly linked subscription. This process deploys the necessary resources in Azure, including a Resource Group for managing the machines.

1. In the Citrix Cloud™ page, click **Manage RBI Service** > **Create Catalog**.
2. On the **Create Remote Browser Isolation Catalog** page, give a name for the Catalog and click **Add remote isolated browser**.

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

> **Note:**
>
> If you select create catalog, it takes the default settings for a quick deployment.

3. Click **Next: Machine Settings** and provide the following details:
   - **Subscription**
   - **Machine settings**
   - **Region**

> **Note:**
>
> Set a power schedule is disabled by default but the user has the option to configure this.

4. Click **Next: Summary** > **Create Catalog**.
5. After the catalog is created, click **View Details**.

Catalog Configuration Highlights:

- Catalog creation sets up everything needed for customer workloads with just one click.
- Customers can select their own power management cycles for the machines and publish browsers within the catalogs.
- If a customer has multiple subscriptions, they can choose where to deploy the catalog.
- Citrix Catalog Service manages the workloads.
- Software patches and updates are automatically deployed based on the customer-configured machine power management settings.
- The machine in the catalog operates in connectorless mode (Rendezvous V2 Policy for DaaS). This means that no connector deployment is required in the customer's resource group.

Step 2.1: Assign Catalog for Secure Private Access (SPA) app sessions Customer admins can select which catalog to use for SPA sessions, allowing them to dedicate a specific catalog for this purpose.

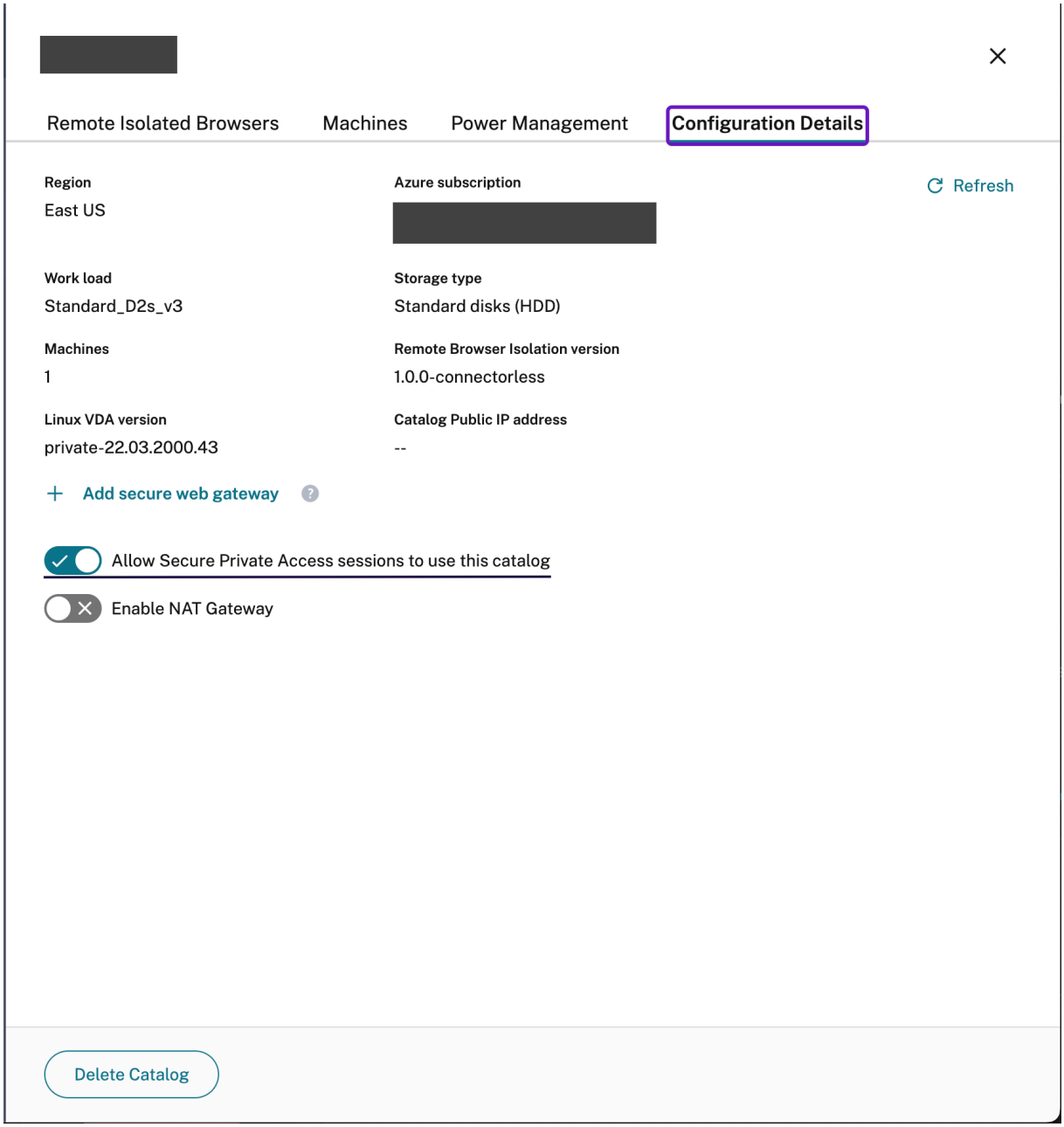
Prerequisites:

At least one catalog must be enabled for this option to successfully launch a SPA RBI app.

How to Enable Secure Private Access session:

1. On the Citrix Cloud page, click **Manage RBI Service**.
2. Click **Manage** and navigate to the created catalog and click **View Details**.
3. On the **Configuration Details** page, enable the toggle option for **Allow Secure Private Access sessions to use this catalog**.

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



> **Note:**
>
> You can select more than one catalog with this option. If multiple catalogs are selected, SPA launches goes to the catalog in the nearest region from where the launch request is made.

Step 3: Publish Browser Application

Create a Browser Application Follow these steps to add a remote isolated browser:

1. Click the catalog on the **Manage** tab of the RBI Self-hosted workloads console.

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

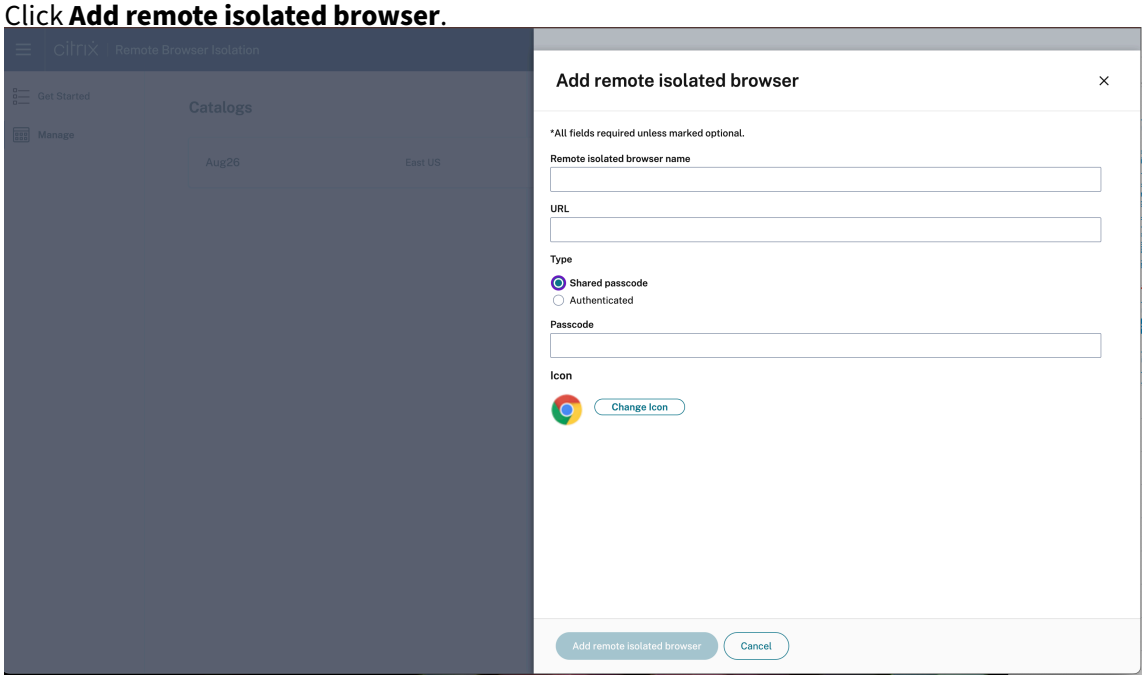
2. Click **Add remote isolated browser** and provide the following configuration details:

   - **Name of the Browser:** Enter any name that you prefer.
   - **URL:** Specify the target application URL.

     > **Note:**
     >
     > The remote browser is hosted in a secure isolated environment. The URL must be accessible through the internet.

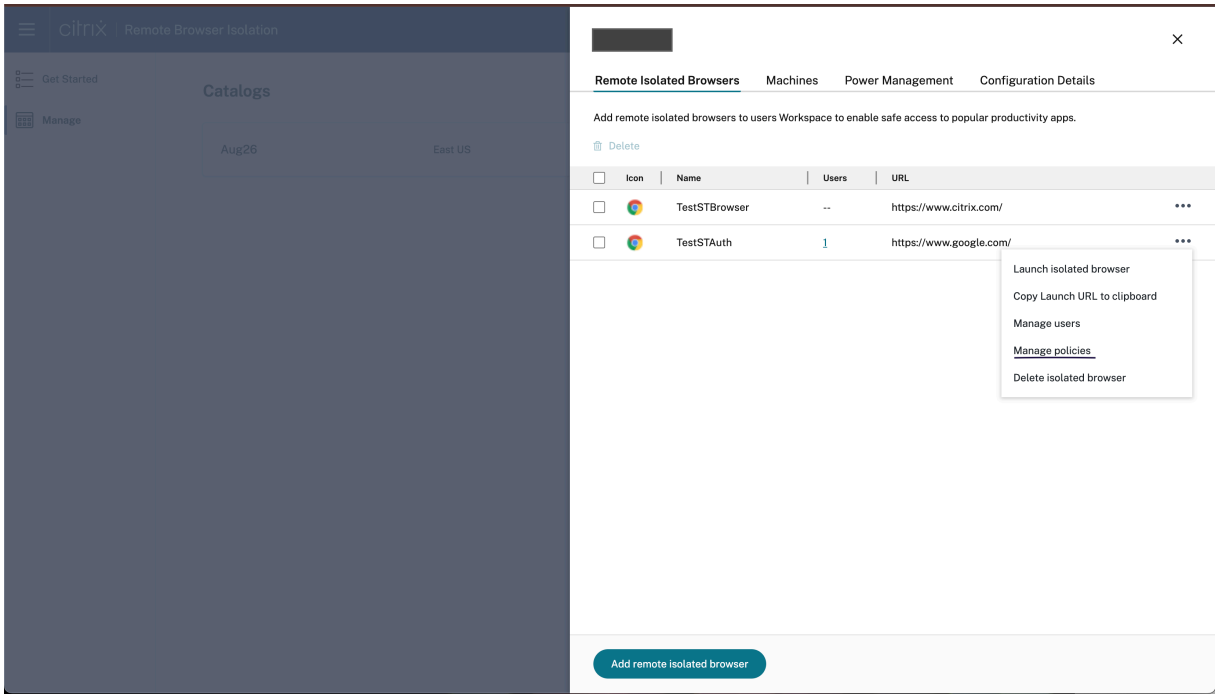
   - **Type:** Choose **Shared passcode** or **Authenticated**, which is visible to end users.
   - **Passcode** Enter the passcode.
   - **Icon:** Upload an app icon.

3. Click **Add remote isolated browser**.

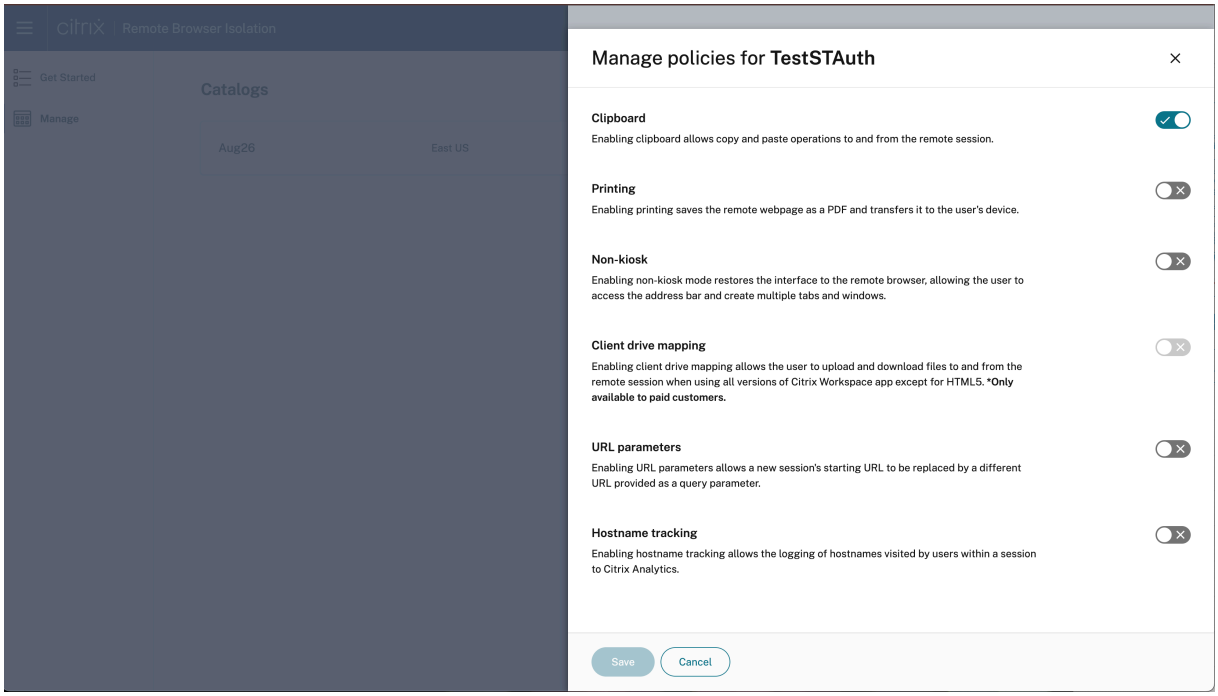


Assign Policies to the Browser Application Once a browser is created, you can configure the necessary policies on the browser.

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

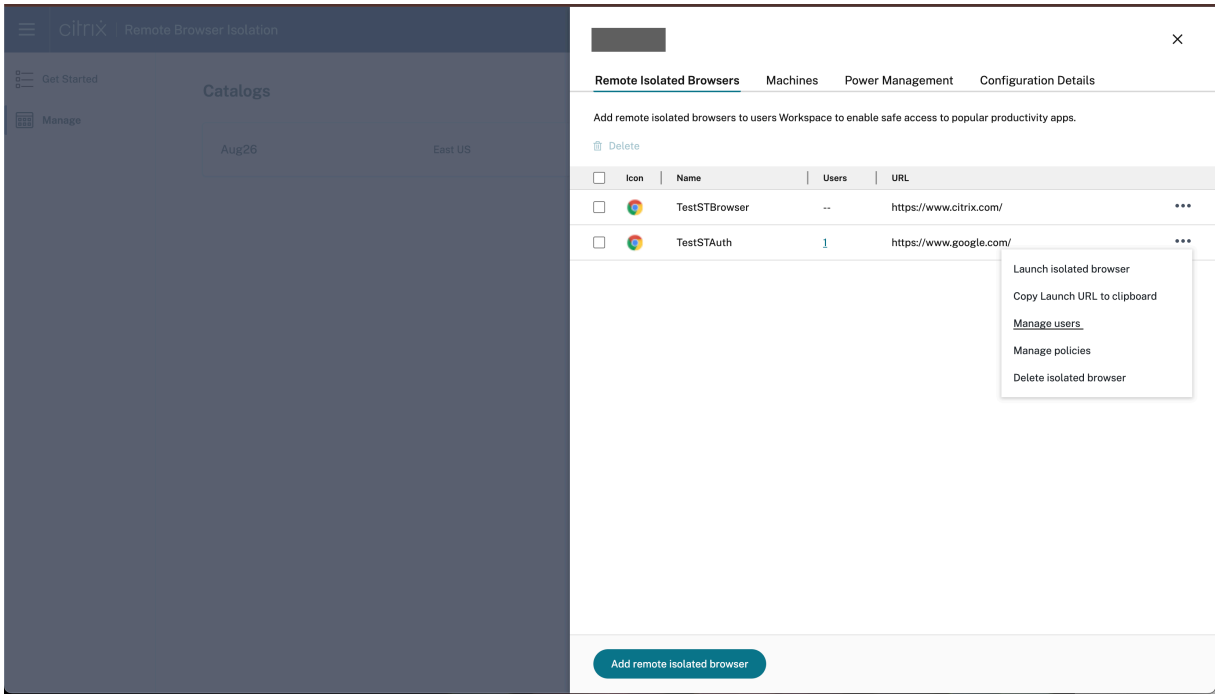


1. Click the ellipses and then click **Manage policies**.
2. Enable the desired policies and click **Save**.

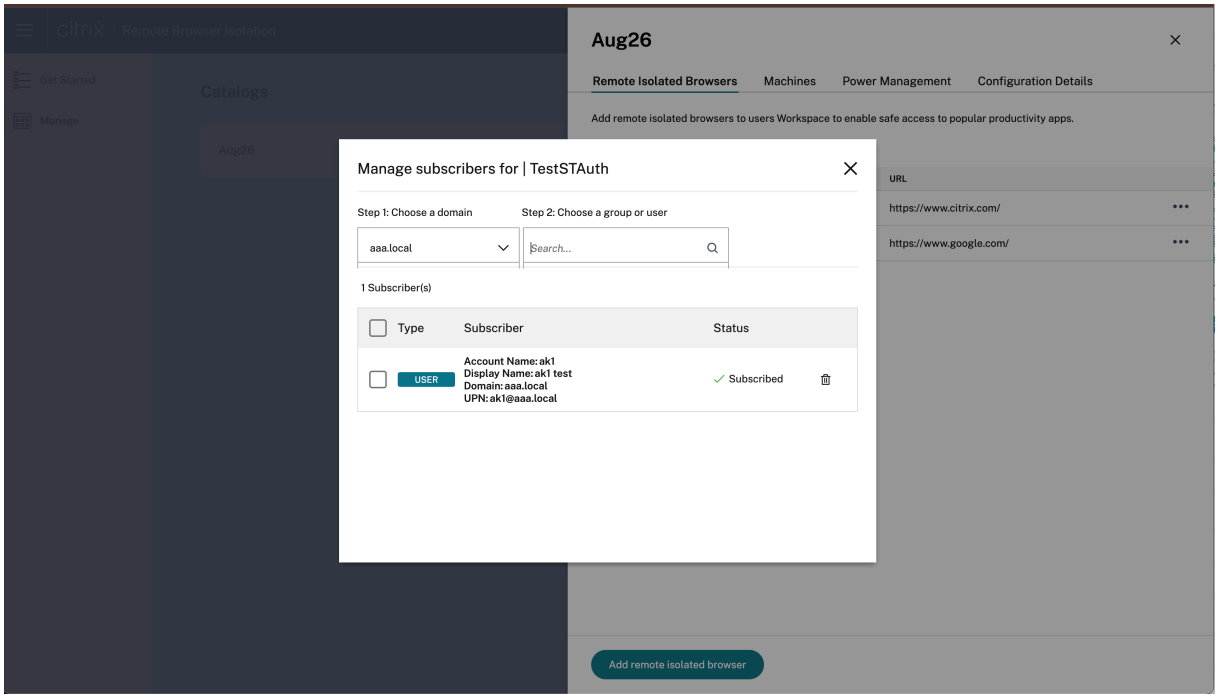


Add Users to a Browser Application Customers need to bring in their domains and the Identity provider to assign users and groups to the published browser in the catalog.

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



1. To subscribe a user, click the ellipsis and select **Manage Users**.
2. Then, choose the domain and select a group or user from the drop-down menu.



Step 4: Test Browser Application and Share You can now access published browsers through your store or by opening their URLs directly in a web browser.

Launch requests are directed to the machines in the assigned catalogs in your account.

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

> **Note:**
>
> If power management for the machines hasn't been set up for the catalog and there are no running machines, launching a session triggers the startup of a machine, which then waits to be ready to accept the session.

Delete a browser:

Select the browser that you want to delete and click the **Delete** icon.

Restart or Force Restart a machine:

Next to the machine name, click the ellipses and click the desired option.

Additional Features

August 25, 2026

User Activity Logging

The User Activity Logging feature lets customers track and audit user browsing activity during Citrix Remote Browser Isolation (RBI) sessions. The feature captures visited host names, access timestamps, user identifiers, and allowlist enforcement status. All collected data is stored in the customer's Azure Storage Account, which provides full data ownership and control.

> **Important:**
>
> This feature must be enabled at both the customer level and the application level. Browsing activity data is uploaded hourly and is not real-time.

Key Benefits

- **Compliance and auditing:** Meet enterprise audit requirements and regulatory compliance standards.
- **Security analysis:** Identify abnormal browsing patterns and potential security threats.
- **Policy optimization:** Analyze user behavior to refine allowlist configurations.
- **Data sovereignty:** Keep data under your control in your Azure environment.

Prerequisites

Before configuring User Activity Logging, ensure that you have the following:

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

- A valid Azure subscription.
- An Azure Storage Account for browsing activity data.
- A catalog created under the Remote Browser Isolation service.

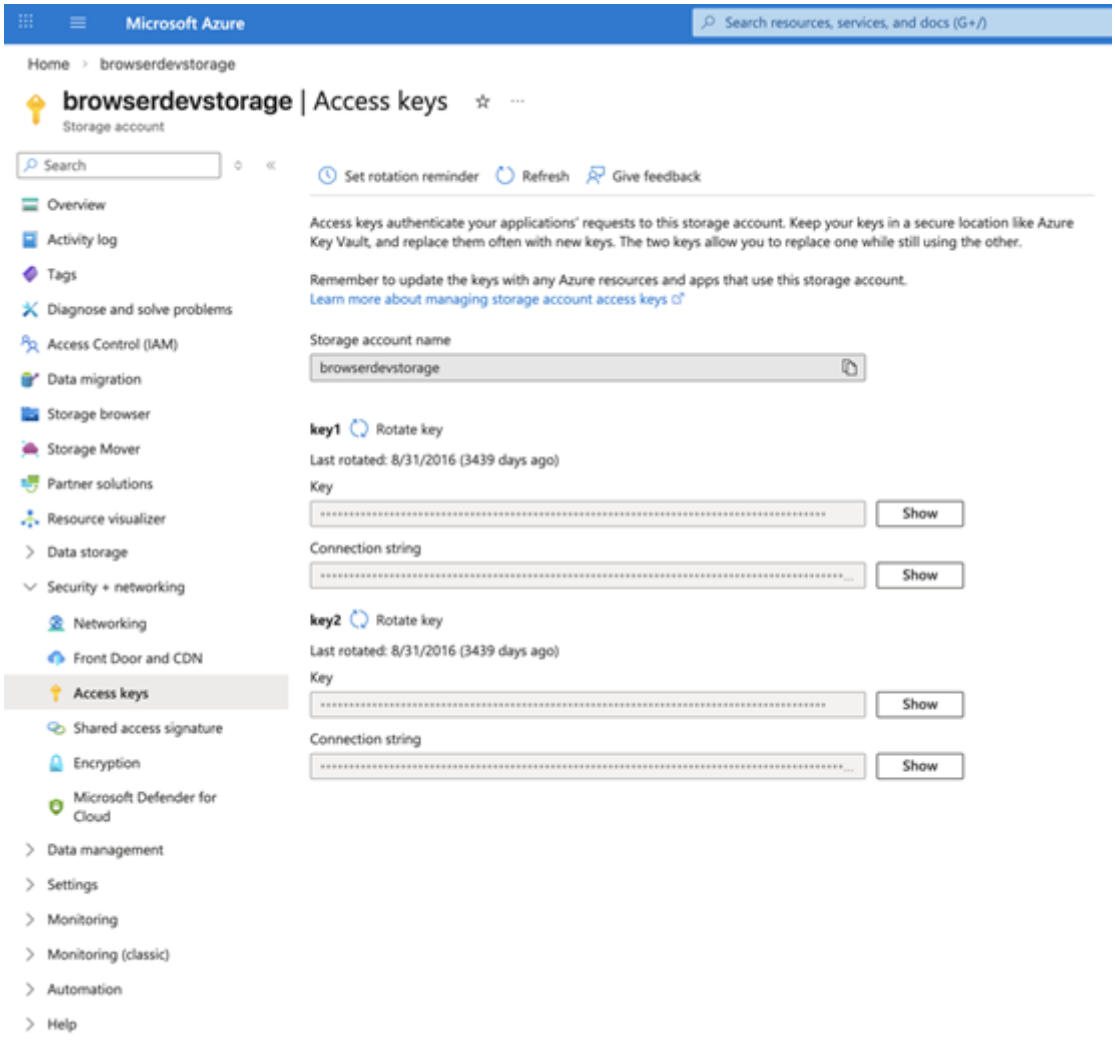
Configuration steps

Step 1: Retrieve Azure Storage connection string This guide assumes that an Azure Storage Account exists. To create one, see Azure Storage documentation.

1. Sign in to Azure portal and open the Storage Account.
2. In the left menu, go to **Security + networking** and select **Access keys**.
3. Copy the **Connection string** from either key1 or key2.
4. Store the connection string securely for use in the step 3 (Verify the feature is working).

> **Note:**
>
> Citrix RBI automatically creates a container named `user-activity` when you save the configuration. Manual container creation is not required.

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

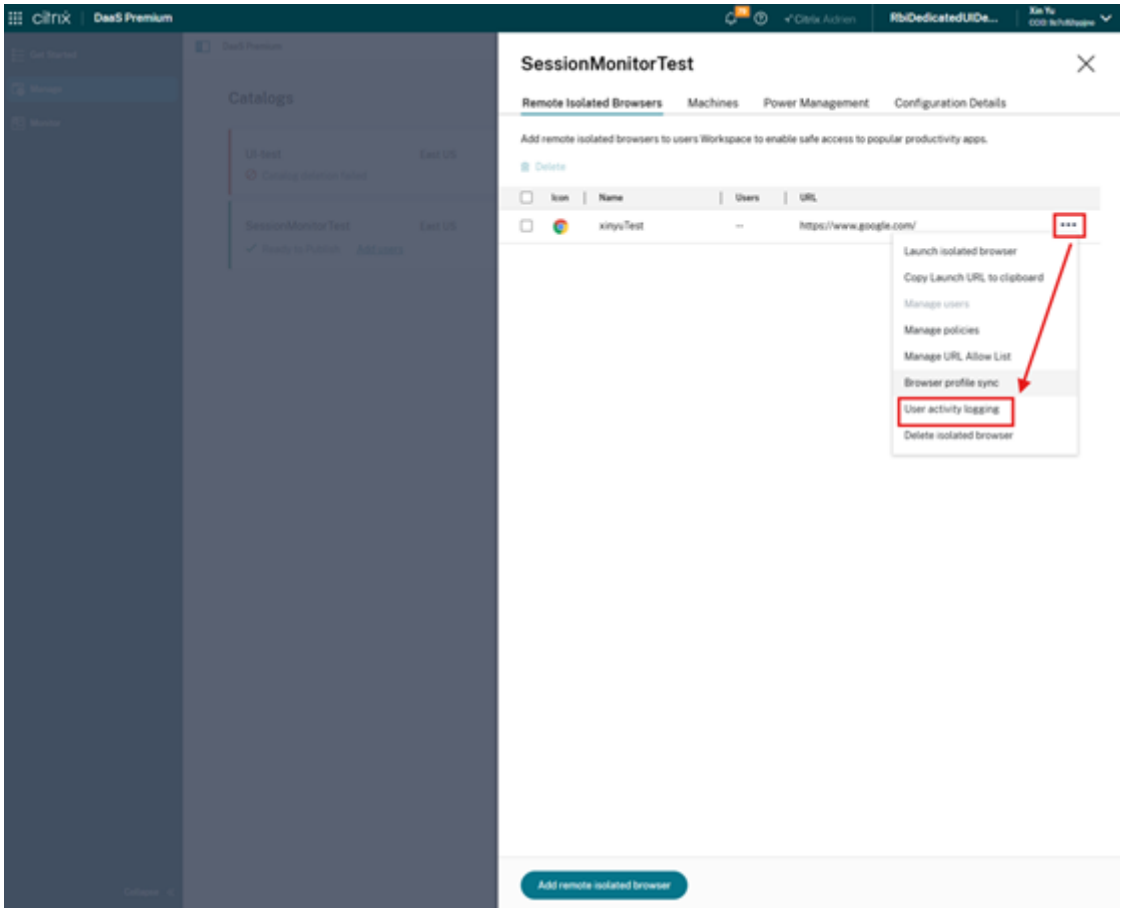


Step 2: Configure User Activity Logging for applications Azure Storage connections can be configured per application.

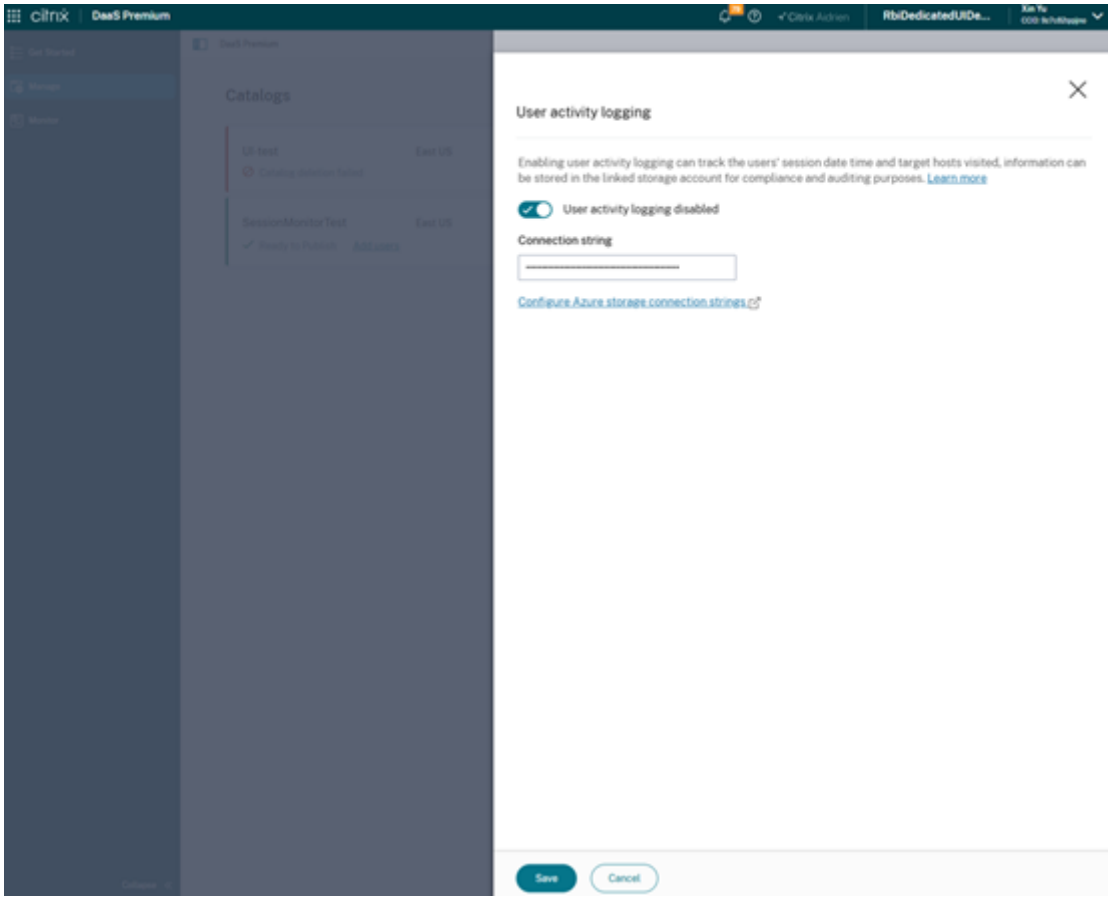
Create or update configuration

1. In the Admin Console, navigate to the **Manage** page.
2. Select the catalog and application for which User Activity Logging must be enabled.
3. Find the **User activity logging** setting.
4. Enable **User activity logging**.
5. Paste the Azure Storage connection string from Step 1.
6. Click **Save**.

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



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



When the configuration is saved, the system:

- Validates the connection string.
- Checks connectivity to Azure Storage.
- Creates a container named `user-activity` if it does not exist.
- Confirms connection permissions.

Delete configuration To stop tracking browsing activity for a specific application:

1. Navigate to the settings page for that application.
2. Find the **User activity logging** setting.
3. Disable **User activity logging**.
4. Click **Save**.

After deleting the configuration, newly launched user sessions no longer record browsing activity. Historical data already uploaded to Azure Storage is not deleted.

Step 3: Verify the feature is working After configuration is complete, verify the feature:

1. Launch a new browser session using the application configured with User Activity Logging.

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

2. Visit several websites, for example `www.google.com` and `www.microsoft.com`.
3. Wait for upload. Browsing activity is saved locally first and uploaded hourly.
4. For initial verification, wait at least 1-2 hours.
5. In Azure portal, open the Storage Account and then the `user-activity` container.
6. Verify that new JSON files appear.
7. Download a JSON file and confirm it contains hostnames of visited websites.

Viewing and analyzing browsing activity

Data Storage Structure Browsing activity data is organized in Azure Blob Storage by date and file name:

```
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/
    `- ...
```

File naming convention

- Folder structure: `{ YYYY-MM-DD }` / (organized by date).

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

- File name pattern: `{ VDAHostname } _{ GUID } _{ AppName } _{ YYYY-MM-DD-HH } .json`
- `{ VDAHostname }`: Hostname of the VDA machine.
- `{ GUID }`: Unique identifier for each upload batch.
- `{ AppName }`: Name of the Secure Browser application.
- `{ YYYY-MM-DD-HH }`: Upload timestamp in 24-hour format.

New files are generated every hour for each active VDA.

Data format description Each JSON file contains multiple records in NDJSON format (newline-delimited JSON). Each line represents one access event.

```
{
 "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" }
```

Field descriptions

Field	Description	Example
`accessHostEvent.hostName`	Hostname of the website accessed by the user.	`www.google.com`
`accessHostEvent.acceptHost`	Whether access is allowed by the allowlist (**`true`** means allowed and **`false`** means blocked).	**`true`**
`accessTime`	Access timestamp (UTC).	`2026-01-29T14:23:45.123Z`
`sessionId`	Unique session identifier.	`abc123-def456-ghi789`

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

Field	Description	Example
`userName`	User identifier.	`user@example.com`
`appName`	Application name.	`MySecureBrowser`

Privacy protection: The system records only hostnames such as `www.example.com`. It does not record full URL paths, query parameters, or user-entered content.

Methods for viewing data Use the following methods to view browsing activity records:

Azure Storage Explorer

1. Download and install Azure Storage Explorer.
2. Connect to the **Storage Account**.
3. Browse the `user-activity` container.
4. Download `JSON` files and review their content.

Azure portal

1. Sign in to **Azure** portal.
2. Navigate to the **Storage Account**.
3. Select **Containers** > `user-activity`.
4. Download files to view their contents.

Tip: For deeper analysis, import the data into Excel, Power BI, or another analytics tool.

Key features and considerations

Feature highlights

- **Automatic recording:** Captures website access events without manual intervention.
- **Blocked attempts included:** Captures blocked access attempts (`acceptHost: false`) for allowlist analysis.
- **Hourly uploads:** Uploads data in hourly batches to reduce network overhead.
- **Data sovereignty:** Stores all data in the customer's Azure environment.
- **Multi-application support:** Supports separate or shared Storage Account configuration across applications.

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

Limitations

- **Not real-time:** Data can take up to one hour to appear in Azure Storage.
- **Dedicated Edition only:** Available only for Dedicated Edition applications.
- **Fixed container name:** The container name is `user-activity` and cannot be customized.
- **VDA restart impact:** Data not uploaded yet can be lost if a VDA restarts before upload.

Troubleshooting

Issue 1: No Data in Azure Storage Possible causes:

- The feature toggle is not enabled.
- The connection string is incorrect or expired.
- Insufficient wait time (at least one hour is required).
- The application is not Dedicated Edition.

Resolutions:

1. Check feature toggle status.
2. Reconfigure the connection string and save.
3. Start a new session, visit websites, and wait 1-2 hours.
4. Confirm the application is Dedicated Edition.
5. Verify that the `user-activity` container was created.

Issue 2: Validation fails when configuring connection string Possible causes:

- Connection string format is incorrect.
- Storage Account network restrictions block access.
- Insufficient permissions to create containers.

Resolutions:

1. Copy the complete connection string again from Azure portal.
2. Check Storage Account firewall settings. For testing, temporarily allow broader network access.
3. Verify that the connection string grants container creation permissions.
4. Ensure that the Storage Account is not locked or otherwise restricted.

Issue 3: User sessions are interrupted or slow after data upload No, data uploads run in the background and do not interrupt normal browser usage. Upload uses asynchronous I/O with minimal resource consumption.

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

Issue 4: Does configuration take effect immediately for active user sessions? No, users must close the current session and start a new one for updated settings to apply. Active sessions continue using the configuration present at launch time.

Issue 5: Can multiple applications use the same Storage Account? Yes, multiple applications can share the same Storage Account and `user-activity` container. File naming and the `appName` field help distinguish data between applications.

Integration with Chrome Enterprise Premium (CEP)

This topic introduces the integration between Citrix Remote Browser Isolation (RBI) and Google Chrome Enterprise Premium (CEP) for Linux VDAs. It explains what the feature enables, how it works, and what administrators must know before enabling it.

Introduction

Google Chrome Enterprise Premium (CEP) provides advanced security, browser management, and policy enforcement for enterprise environments. With this feature, the Citrix RBI browser can enroll into Chrome Enterprise policies by using a Google enrollment token. Administrators can then centrally manage organizational and departmental secure browser policies from Google Admin console.

This integration provides a scalable, cloud-managed approach to enforce security and compliance on untrusted endpoint devices without requiring an EDR agent.

What this feature enables

With CEP integration:

Administrators can:

- Apply Chrome Enterprise policies to all Citrix RBI browser users in the same catalog.
- Centrally manage those policies through Google Admin console.

Users can:

- Use an RBI browser that becomes a managed browser after enrollment.
- Receive consistent enterprise policies, for example copy and paste controls and URL blocklists.
- Receive automatic policy updates from Google Cloud.

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

How to use it

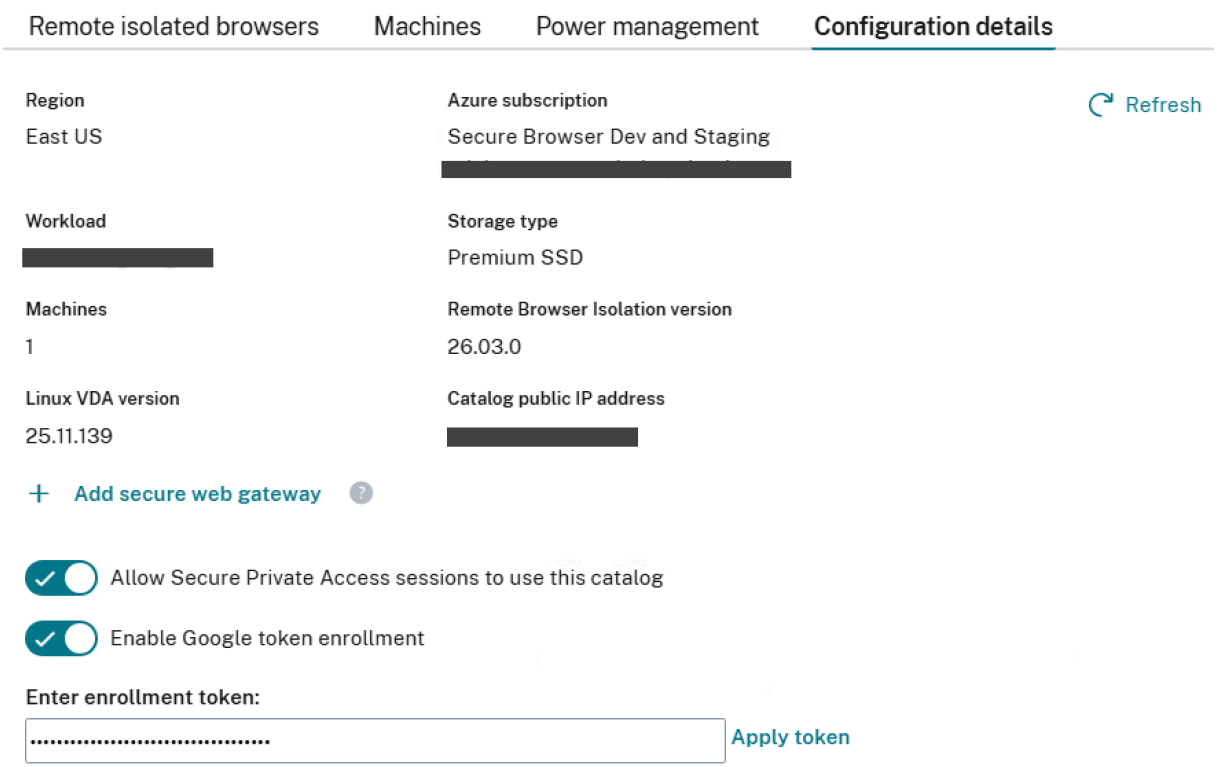
Preparation Before enabling CEP integration:

1. Confirm that Google Workspace supports Chrome Enterprise Premium.
2. Make sure at least one Citrix RBI catalog exists. If not, create one.
3. Identify which RBI catalogs must be governed by Chrome policies.
4. Generate one enrollment token per organizational unit (OU) in Google Admin console, if needed.

Configuration on Citrix Cloud portal CEP requires an enrollment token for each catalog. Citrix automatically distributes the token to user sessions launched from that catalog.

Enrollment flow

1. Obtain an enrollment token from Google Admin console.
2. Sign in to Citrix Cloud and navigate to Remote Browser Isolation.
3. Select **Manage** in the left menu.
4. Select the target catalog, then open **Configuration Details**.
5. Enable **Enable Google Token Enrollment** and enter the enrollment token.
6. Select **Apply token**.



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

When a user launches a secure browser application under that catalog, token enrollment happens automatically and browsing continues in the CEP-enrolled browser.

Administrator tasks

- Disable or re-enable **Enable Google Token Enrollment**, or update the enrollment token.
- Monitor Chrome policy enforcement using `chrome://policy`.
- Review the Google Admin device list periodically and remove stale records.

Limitations and known behaviors

User profile sync is not supported Chrome user profile cloud sync does not function inside a CEP token-enrolled RBI browser.

Reboot is required for each configuration change Because RBI uses ephemeral file systems, a reboot is required if administrators enable or disable CEP integration, or update the CEP token.

Allow list policy behavior If the allow list configured for an RBI browser application under the catalog is modified from the default `*:*`, include `*.google.com:*` to complete CEP enrollment. After CEP is launched, the RBI allow list policy is not honored.

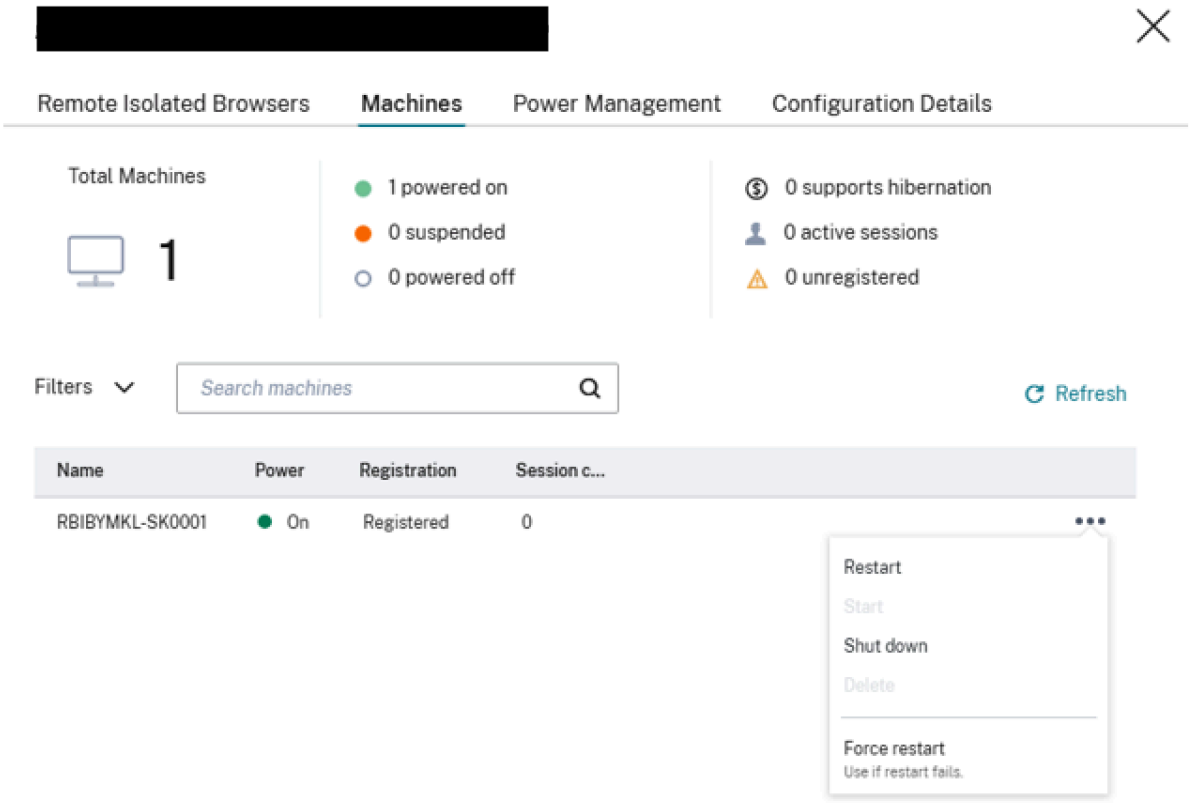
Google admin may show duplicate devices After an image upgrade, a machine can receive a new ID. This can create an additional device record in Google Admin console.

Reboot machines under a catalog

For each machine listed in the catalog:

1. Select the menu on the right.
2. Select **Restart**.

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



Configuring Azure Firewall for Customer-Managed RBI Catalog Virtual Network

Azure Firewall enables you to filter outgoing web requests from your catalog machines in your Remote Browser Isolation service. By deploying Azure Firewall in your existing Azure Virtual Network, you can control and monitor outbound traffic. This helps you enhance network security and manage outbound connections for your workloads.

Prerequisites:

- A catalog created under the Remote Browser Isolation service in your Azure subscription.
- Sufficient permissions to create and manage Azure resources.

Locate the Azure Virtual Network

1. In the **Citrix Cloud DaaS** console, identify the machine catalog you want to secure.
2. Select a machine from the catalog and copy the first part of its name (for example, RBI3BLR6-O80001).
3. In the Azure portal, search for the VM using this name.
4. In the VM's overview, select the **linked virtual network**.

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

Create an Azure Firewall

1. In the virtual network's menu, select **Subnets** under **Settings**.
2. Add a new subnet with the purpose set to **Azure Firewall** (use default settings).
3. Return to the virtual network overview and select **Azure Firewall** under **Capabilities**.
4. Click **Add a new firewall**.
5. Complete the following fields:
    - **Subscription** and **Resource group**: Select as appropriate.
    - **Name**: Enter a name for your firewall.
    - **Region**: Match the region of your virtual network.
    - **Firewall tier**: Select **Standard**.
    - **Virtual Network**: Choose the network identified in Step 1.
    - **Firewall Policy**: Select **Use a Firewall Policy to manage this firewall**.
    - **Policy Name**: Click **Add new** and enter a name (for example, Test-policy).
    - **Firewall Management NIC**: Disable this setting.
6. Review your settings and create the firewall.

Configure Routing

1. After deployment, open the Azure Firewall resource and note its private IP address.
2. In the Azure portal, navigate to your virtual network and select **Subnets**.
3. Identify the subnet where your catalog VMs reside (typically named default).
4. Create a new route table or select an existing one associated with this subnet.
5. Add a new route:
    - **Destination**: `0.0.0.0/0`
    - **Next hop type**: `Virtual appliance`
    - **Next hop address**: Enter the Azure Firewall's private IP address.
6. Save the route.

Configure Firewall Rules

1. In the Azure portal, go to **Firewall Manager > Azure Firewall Policies**.
2. Select the policy that you created (for example, Test-policy).
3. Go to **Rules**.
4. Add a new **Application rule collection** (recommended for web filtering).
5. Define rules to allow or deny specific FQDNs or URL categories. For example, to deny access to `www.example.com`:

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

- **Name**: `DenyExampleWebsite`
- **Source IP address**: The subnet range of your catalog VMs.
- **Destination FQDNs**: `www.example.com`
- **Protocols**: `http:80`, `https`
- **Action**: `Deny`

6. Save the rule collection.
7. Add additional Allow or Deny rules as needed, adjusting priorities accordingly. (Optional)

Test the Configuration

1. Launch a browser session from a machine in the configured catalog.
2. Try accessing both allowed and blocked websites to confirm that access controls are working correctly.
3. Verify that the firewall is correctly filtering network traffic according to the defined rules.

Troubleshooting

If you encounter issues, refer to the Azure Firewall Documentation.

Limitations

All browsers within the same catalog use the same firewall, policies, and rules.

Software Upgrades and Patch Management

Citrix creates and manages the machine images and catalogs, including software management. When new versions of catalogs are available, Citrix pushes these upgrades to customer catalogs, ensuring that their machines receive the latest fixes and patches next time they get restarted. RBI uses the DaaS Catalog service to facilitate these upgrades in the customer's subscription.

Integration with Citrix® StoreFront Cloud

Remote Browser Isolation can be integrated with StoreFront Cloud. To ensure that it's integrated:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **StoreFront Cloud**.
3. Select the **Service Integrations** tab.

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

4. Confirm that the Remote Browser Isolation service entry indicates **Enabled**. If it does not, click the ellipsis menu and select **Enable**.

If you haven't already done so, configure the store URL, external connectivity, and store authentication for your store, as described in Configure authentication to stores.

Remote Browser Isolation supports authentication with Active Directory and Microsoft Entra ID. Authentication with Active Directory is configured by default. For information about configuring authentication using Microsoft Entra ID, see Connect Microsoft Entra ID to Citrix Cloud.

If you configure authentication using Microsoft Entra ID, the on-premises domain containing your Active Directory domain controllers must contain one (preferably two) Cloud Connectors.

Integrate with your on-premises StoreFront

Citrix Virtual Apps and Desktops™ customers with an on-premises StoreFront can easily integrate with the Remote Browser Isolation service to provide the following benefits:

- Aggregate your published remote isolated browsers with your existing Citrix Virtual Apps™ and Desktops apps for a unified store experience.
- Use native Citrix Receivers for enhanced end user experience.
- Strengthen security for Remote Browser Isolation launches by using your existing multifactor authentication solution integrated with your StoreFront.

For details, see CTX230272 and the StoreFront configuration documentation.

Manage and monitor remote isolated browsers

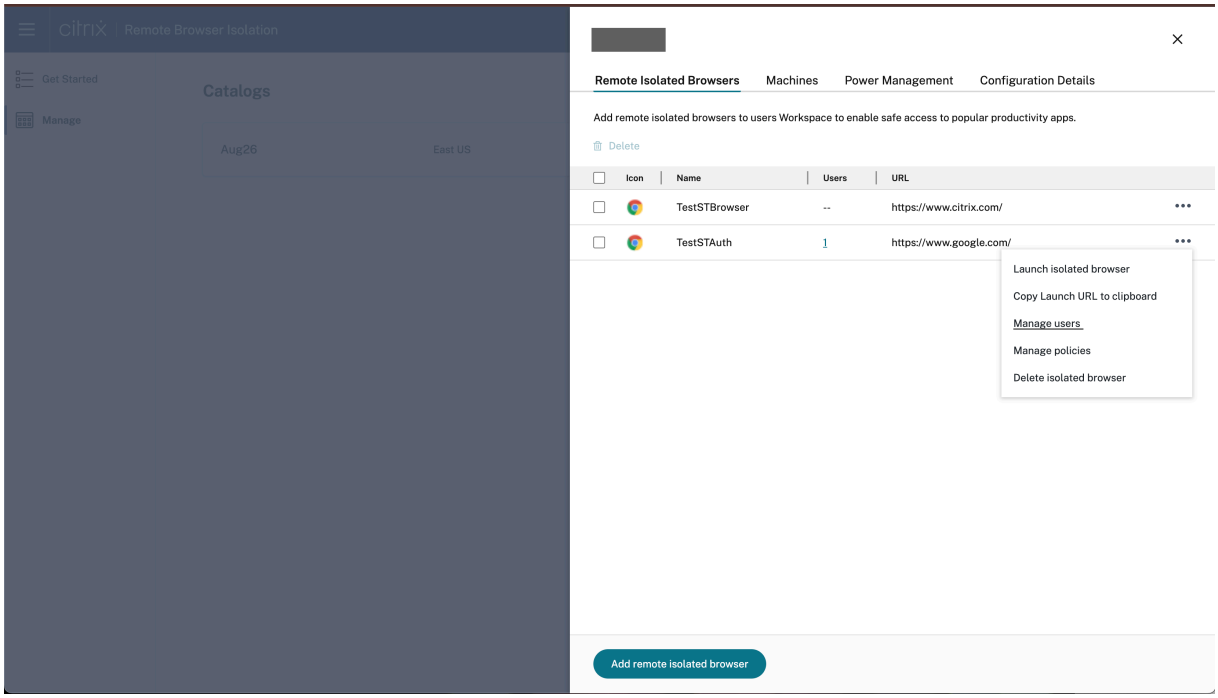
July 28, 2026

You can manage policies and other configurations of the published browsers, and also monitor active user sessions in Remote Browser Isolation.

Manage

The **Manage** tab lists the existing Remote Browser Isolation (RBI) catalogs. You can select an existing catalog to update the configurations of the published browsers. Click **ellipsis** at the right-end of the published browser, and then select the required task.

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



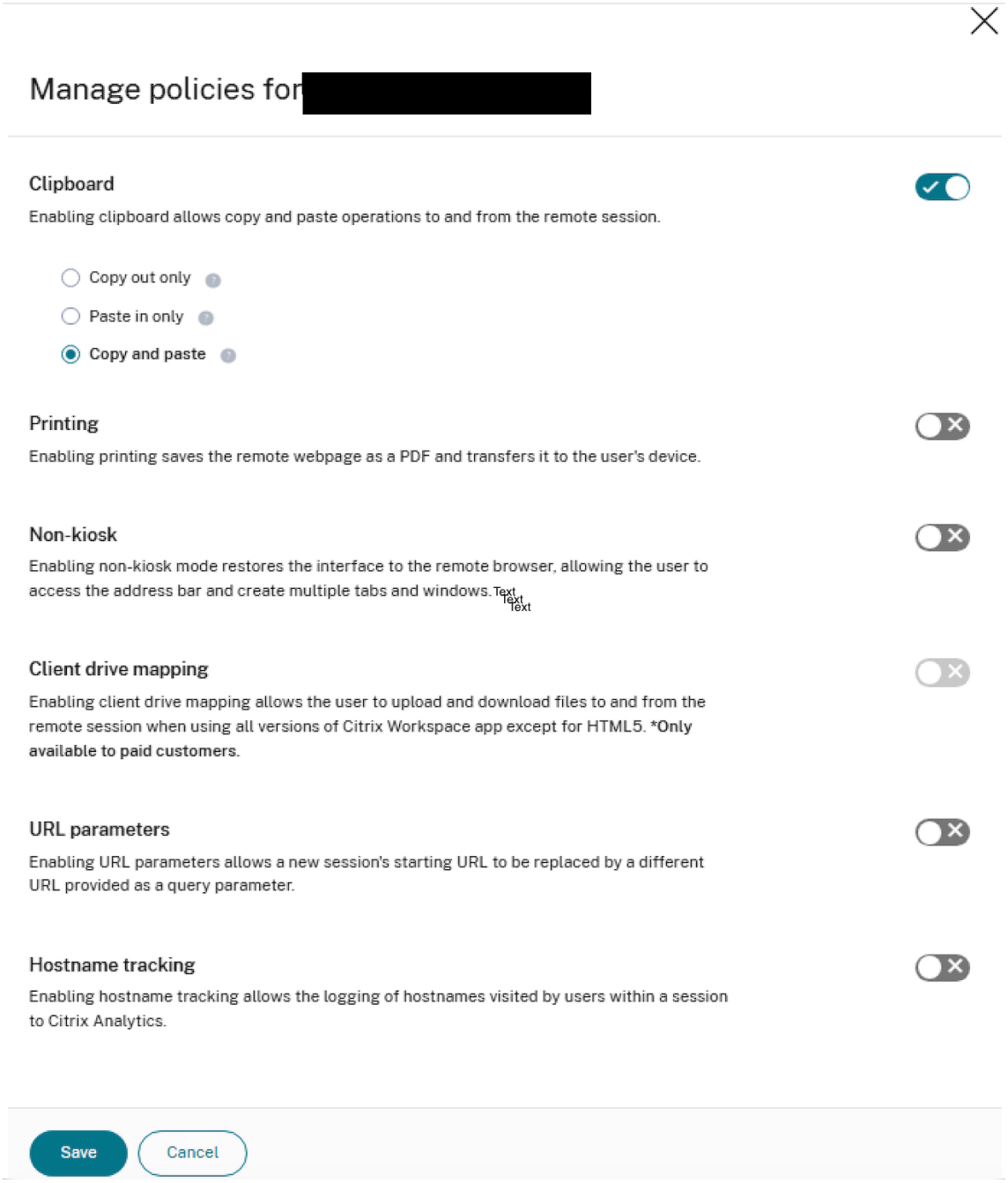
If you select a menu entry, and then decide not to change anything, cancel the selection by clicking the **X** outside the dialog box.



You can manage the published isolated browser using the following tasks:

- **Launch published browser:** Opens the published browser session. After publishing the browser, you can select this task to verify the launch of the published browser session.
- **Copy URL to clipboard:** Copies the URL of the published browser. You can share this URL with end users to access the published browsers.
- **Policies:** You can set policies for the published browsers.

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



Settings on the policies page control the following:

- **Clipboard:** Enabling the Clipboard policy allows three options for copy and paste operations:
  - **Copy out only:** Users can copy content from the RBI session to the local device, pasting into RBI is blocked.
  - **Paste in only:** Users can paste content into the RBI session, copying out is blocked.
  - **Copy and paste:** Full bidirectional clipboard access.

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

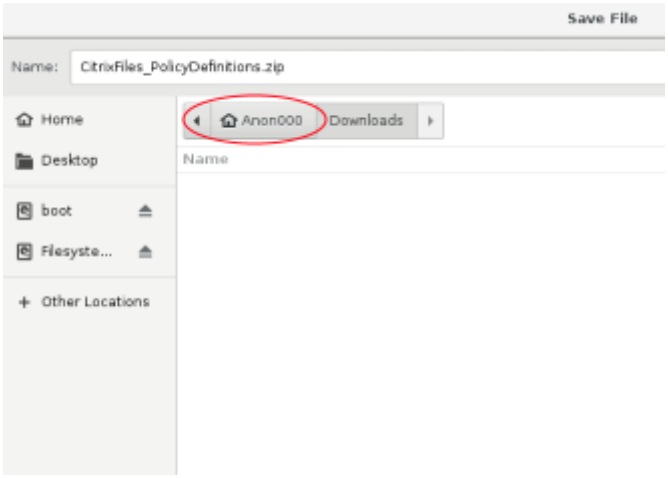
Disabling the Clipboard policy toggle removes the Clipboard button from the Citrix Workspace™ app toolbar.

These granular policy options give administrators fine-grained control over data flow between the remote session and user endpoints. For example, an organization can allow users to copy text out of a remote browser for reference while preventing paste operations into the session to reduce the risk of data injection.

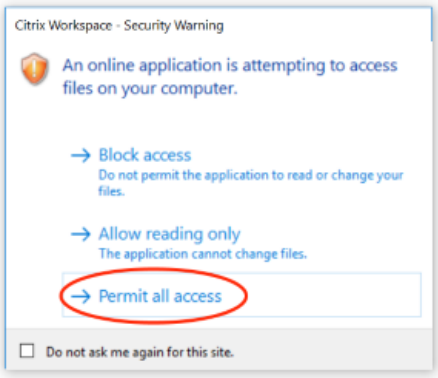
> **Note:**
>
> For existing published browsers that had the Clipboard policy enabled, both Copy and Paste are enabled automatically during migration to preserve the previous behavior. No administrator action is required.

- **Printing:** Enabling printing saves the remote webpage as a PDF and transfers it to the user's device. The user can then press Ctrl-P and select the Citrix PDF printer. By default, this setting is disabled.
- **Non-kiosk:** Enabling non-kiosk mode restores the interface to the remote browser. The user can then access the address bar and create multiple tabs and windows. (Disabling non-kiosk mode removes the remote browser's navigation controls and address bar.) By default, this setting is enabled (non-kiosk mode is on).
- **Region failover:** The Region failover policy automatically transfers your published browser to a different region if your current region is reporting an issue. To opt out, disable the Region failover policy. If you published the browser using the **Auto** region selection, your isolated browser remains enrolled in the policy. By default, this setting is enabled.
- **Client drive mapping:** Enabling the Client drive mapping policy allows the user to upload and download files to and from the remote session. This feature is available only for sessions launched with the Citrix Workspace app. By default, this setting is disabled.
  - Users must save downloaded files only on the `ctxmnt` disk in the `Anonxxx` directory. To do that, users must navigate to the desired location for storing the file. For example, **Anonxxx > ctxmnt > C > Users > User Name > Documents**.

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



- The dialog box might prompt the user to accept the **Permit all access** or **Read and Write** permissions to access the `ctxmnt` folder.



- **URL parameters:** Enabling URL parameters allows you to change a new session's starting URL when users launch an app. For this policy to take effect, configure a local proxy server to identify suspicious websites and redirect them to Remote Browser Isolation. By default, this setting is disabled. For more information, see Proof of Concept Guide: URL Redirection to Remote Browser Isolation with Citrix ADC in Azure.
- **Hostname tracking:** Use host name tracking to enable Remote Browser Isolation to log host names during a user's session. This policy is disabled by default. This information is shared with Citrix Analytics. For more information, see Citrix Analytics.

When you're done, click **OK**.

- **URL Allow lists:** Use the **Whitelists** task to restrict users to visiting only allowed URLs within their published Remote Browser Isolation session. This feature is available for external authenticated web apps.

  Enter allow list entries in the form `hostname:port number`. Specify each entry on a new line. Asterisks are supported as wildcards. Browser requests must match at least one entry in the allow list.

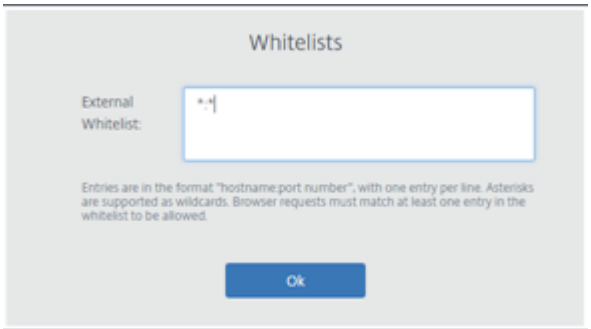
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, to set `https://example.com` as an allowed URL:

- `example.com:*` allows connection to this URL from any port.
- `example.com:80` allows connection to this URL only from port 80.
- `*:*` allows access to this URL from any port and from any links to other URLs and ports. The `*.*` format allows access to all external web apps from the published app. This format is the default setting for the web apps **External Whitelist** field.

When you're done, click **OK**.

Advanced web filtering capabilities are available through integration with the Access Control service. Learn more at Use case: Selective access to apps.



Monitor

The **Monitor** tab provides information about users' real-time sessions. You can monitor and disconnect one or several active sessions.

To stop a single session, select the session and click the ellipsis menu at the end of an entry's row. Click **Log off session** and confirm your changes.

To disconnect multiple sessions, select the active sessions in the list and click the **Log off** button on the top of the page. After you confirm your changes, Remote Browser Isolation immediately disconnects all selected sessions.

Remote Browser Isolation technical security overview

September 6, 2025

Remote Browser Isolation (formerly Secure Browser service) is a SaaS product managed and operated by Citrix. It allows access to web applications via an intermediate web browser hosted in the cloud.

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

Cloud service

The Citrix Remote Browser Isolation™ service consists of web browsers running on Virtual Delivery Agents (VDAs) along with the management console used to manage and connect users to these VDAs. Citrix Cloud manages the operation of these components, including the security and patching of operating systems, web browsers, and Citrix components.

While using Remote Browser Isolation service, hosted web browsers track the user's browsing history and perform caching of HTTP requests. Citrix uses mandatory profiles and ensures that this data is deleted when the browsing session ends.

Remote Browser Isolation service is accessed with a HTML5-compatible web browser. The service does not provide any downloadable clients. All traffic between the browser being used and the cloud service is encrypted using industry-standard TLS encryption. Remote Browser Isolation supports TLS 1.2 only.

Egress traffic for Remote Browser Isolation uses specific IP addresses to protect the internal network. For the list of accepted IP addresses, see Knowledge Center article CTX286379.

Web applications

Citrix Remote Browser Isolation is used to deliver web applications owned by the customer or a third party. The owner of the web application is responsible for its security, including patching the web server and application against vulnerabilities.

Security of the traffic between Remote Browser Isolation and the web application depends on the encryption settings of the web server. To protect this traffic as it flows over the Internet, administrators publish HTTPS URLs.

More information

See the following resources for more security information:

- Citrix Security site: https://www.citrix.com/security
- Citrix Cloud documentation: Secure Deployment Guide for the Citrix Cloud Platform

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.