Citrix Remote Browser Isolation™

Contents

Remote Browser Isolation

September 6, 2025

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 through Citrix Workspace™ (or Citrix Receiver™) 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 using Citrix Workspace, 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 using Citrix Workspace, 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 Workspace
- 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

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

September 6, 2025

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.

Prerequisites:

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

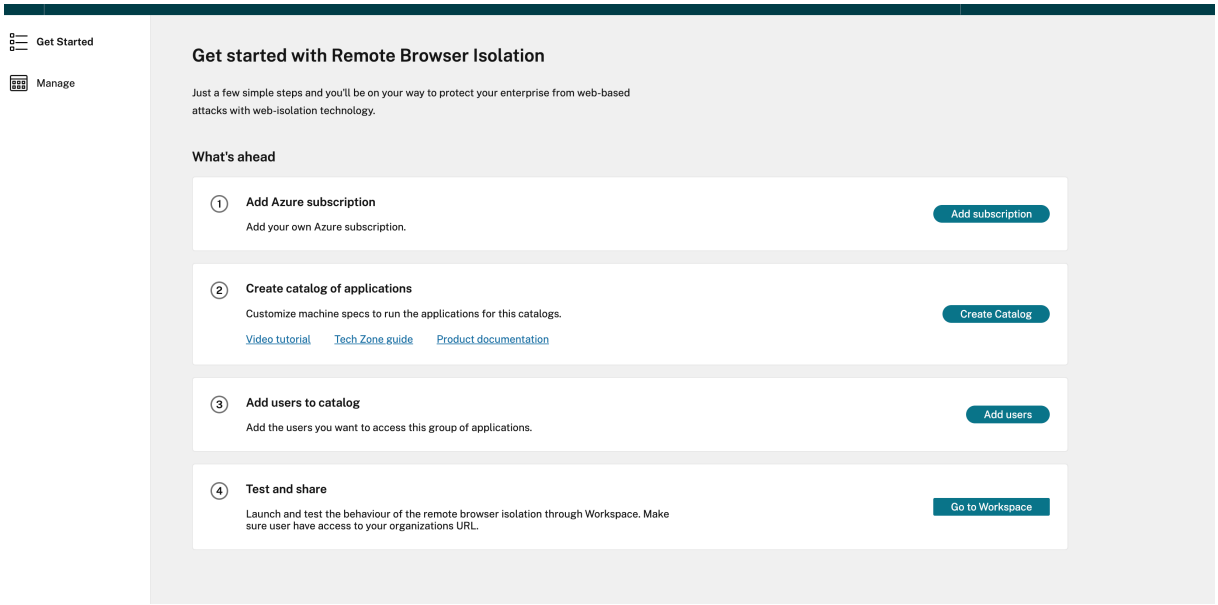
  > **Note:**
  >
  > This step is possible only if the customer tenant has the necessary entitlements.

- 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.

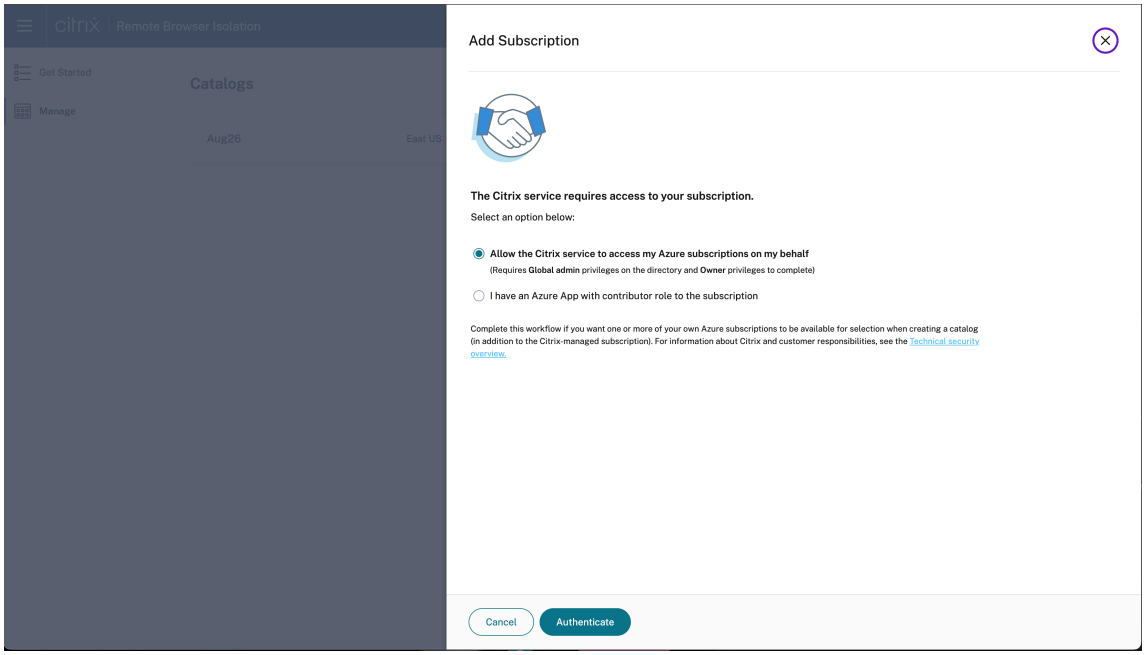
Onboarding Process for RBI On the Citrix Cloud page, click **Manage RBI Service** to access the Remote Browser Isolation landing page.



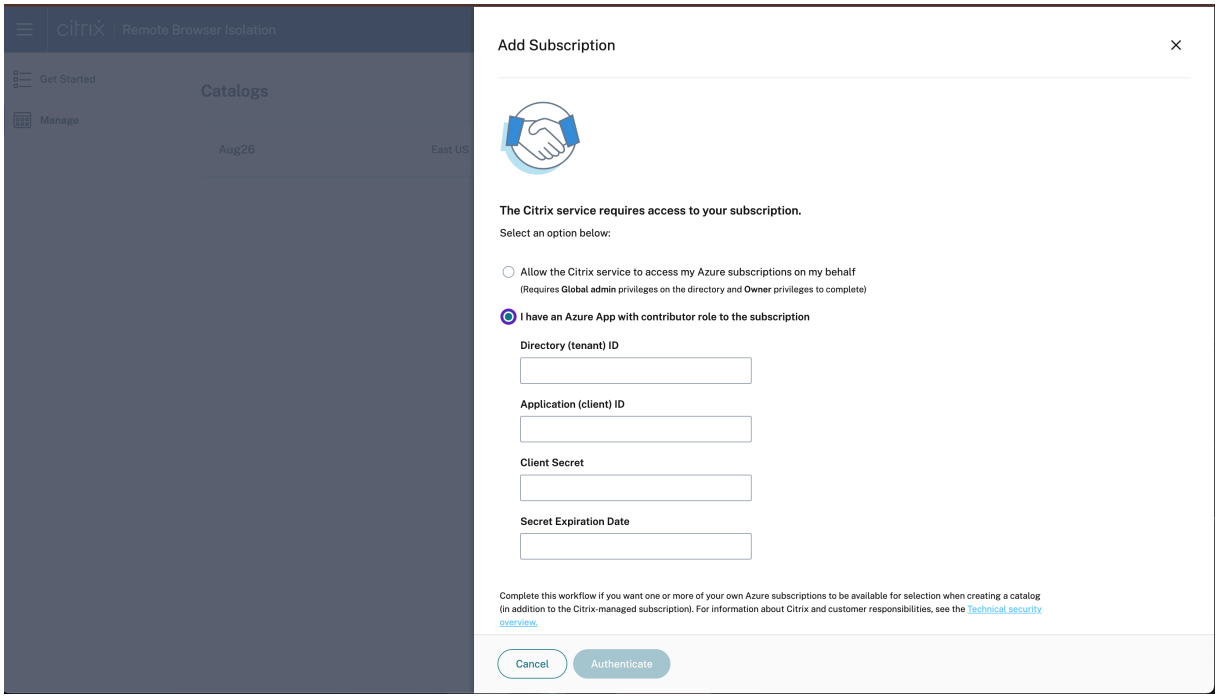
Step 1: Add Azure Subscription

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**.
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**.

   > **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

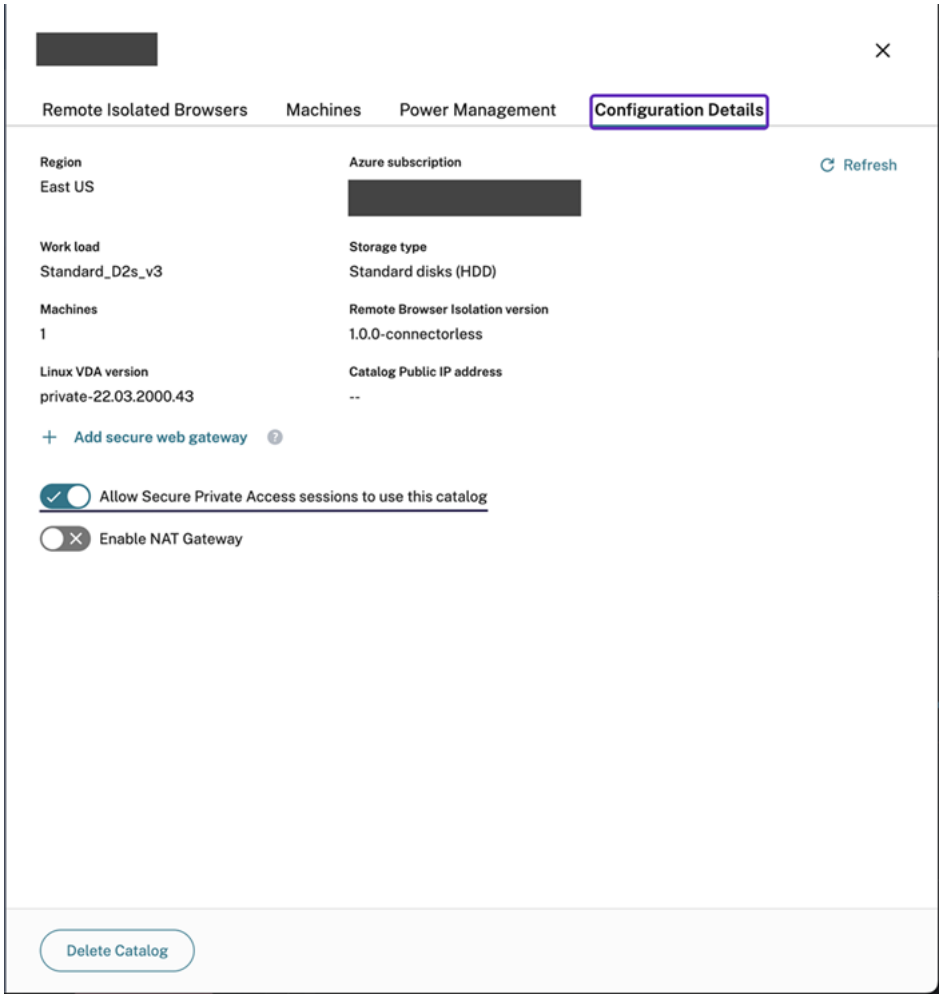
Customer admins can select which catalog to use for SPA sessions, allowing them to dedicate a specific catalog for this purpose.

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**.



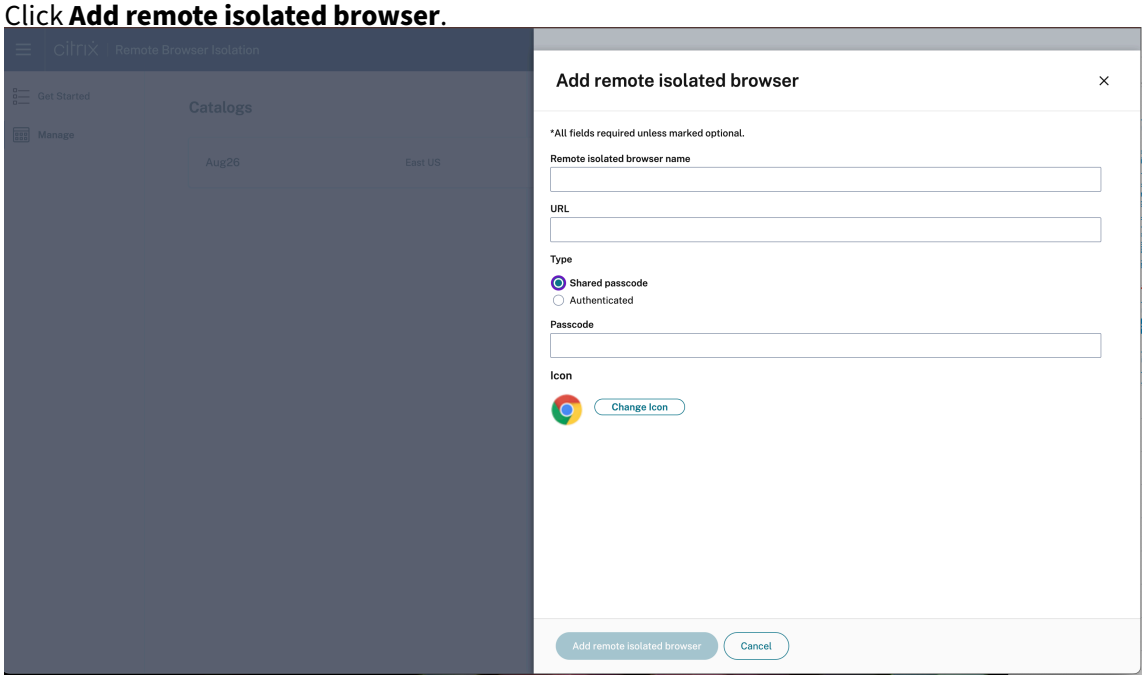
> **Note:**
>
> You can select more than one catalog with this option. If multiple catalogs are selected, SPA launches goes to the catalog in the nearest region from where the launch request is made.

Step 3: Publish Browser Application Create a Browser Application

Follow these steps to add a remote isolated browser:

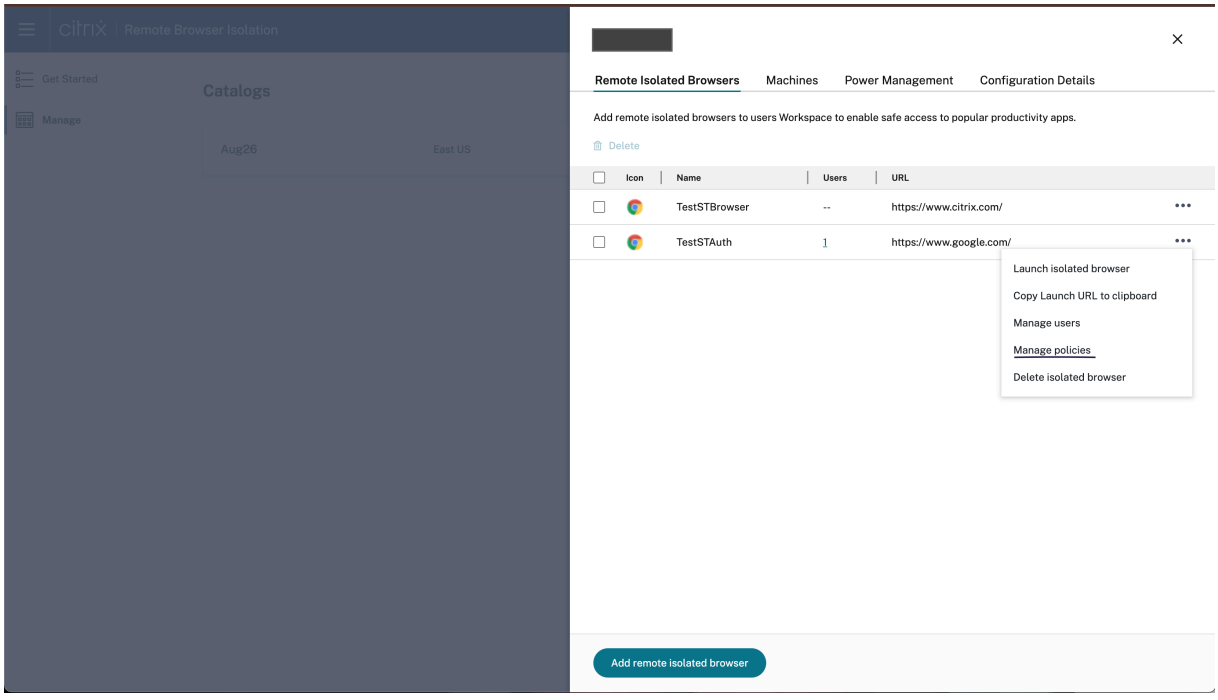
1. Click the catalog on the **Manage** tab of the RBI Self-hosted workloads console.
2. Click **Add remote isolated browser** and provide the following configuration details:
    - **Name of the Browser:** Enter any name that you prefer.
    - **URL:** Specify the target application URL.
    - **Type:** 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**.

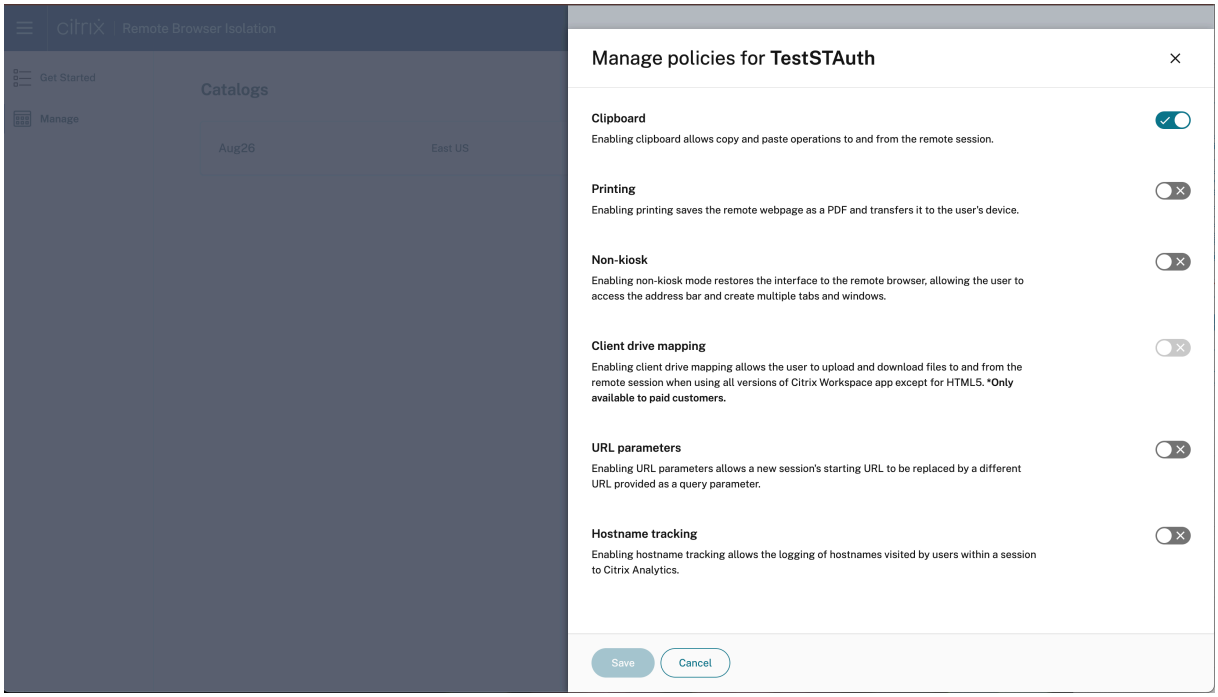


Assign Policies to the Browser Application

Once a browser is created, you can configure the necessary policies on the browser.

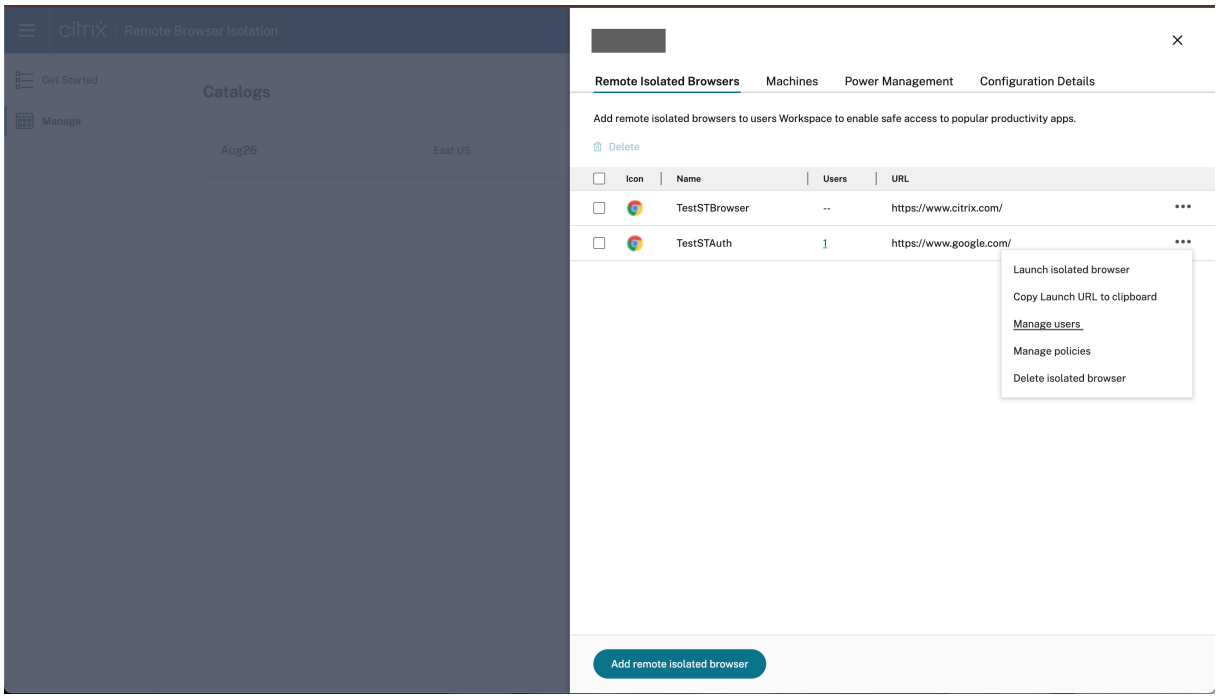


1. Click the ellipses and then click **Manage policies**.
2. Enable the desired policies and click **Save**.

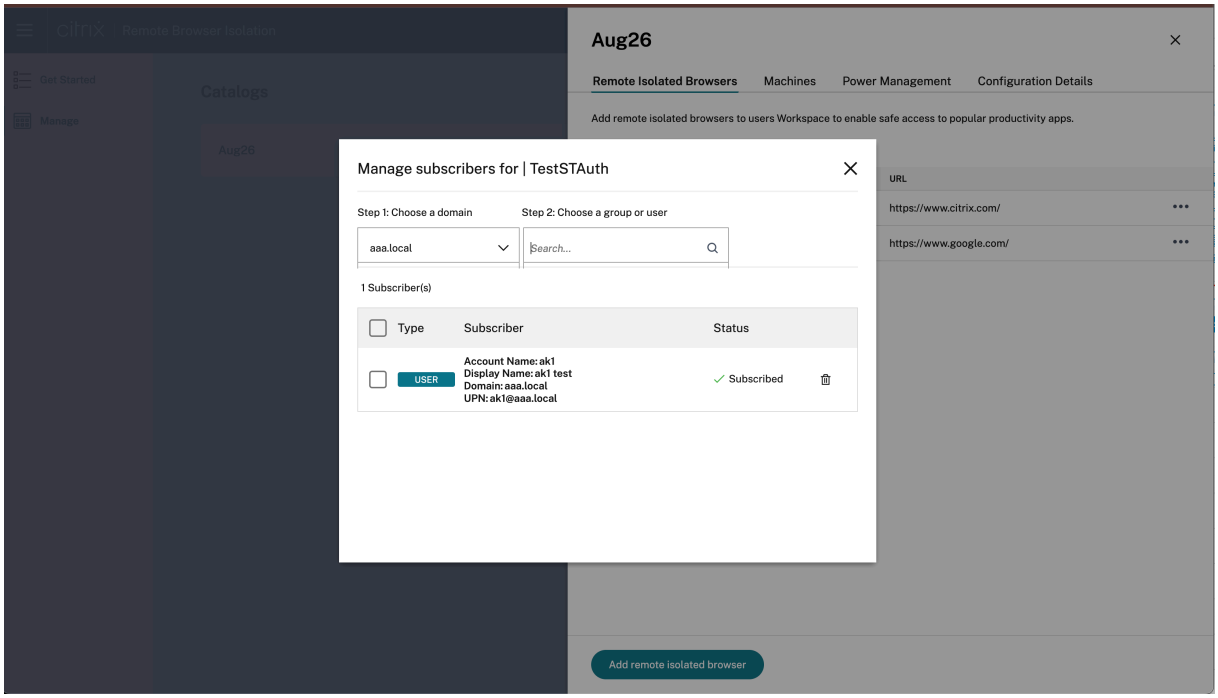


Add Users to a Browser Application

Customers need to bring in their domains and the Identity provider to assign users and groups to the published browser in the catalog.



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 the workspace or direct URLs. Launch requests are directed to the machines in the assigned catalogs in your account.

> **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

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 (e.g., 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**.

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 (e.g., 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 (e.g., 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`:
   - **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.

Enable Network Address Translation (NAT) (Secure Web) Gateway On the **Configuration Details** page, you have the option to add a Secure Web Gateway for specific catalogs.

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.

July 2022

- **Remote Browser Isolation supports authentications for all apps with Azure Active Directory.**
  - Users can now sign in to any Remote Browser Isolation app from Citrix Workspace™ using Azure Active Directory 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 authenicated 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 Azure Active Directory**. Users can now sign in to Remote Browser Isolation apps from Citrix Workspace using Azure Active Directory 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.

Features in Technical Preview

September 6, 2025

Features in Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

Technical Preview to General Availability (GA)

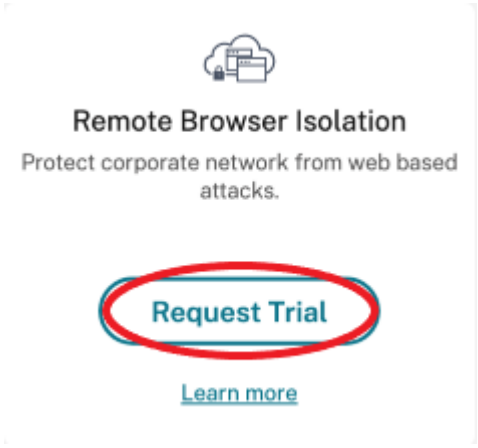
Service or feature	General availability version
Configuring Azure Firewall for Customer-Managed RBI Catalog Virtual Network	2505.5
Remote Browser Isolation - Self-hosted workloads	2505.5
Enable Network Address Translation (NAT) (Secure Web) Gateway	2505.5
Software Upgrades and Patch Management	2505.5

Get started with Remote Browser Isolation

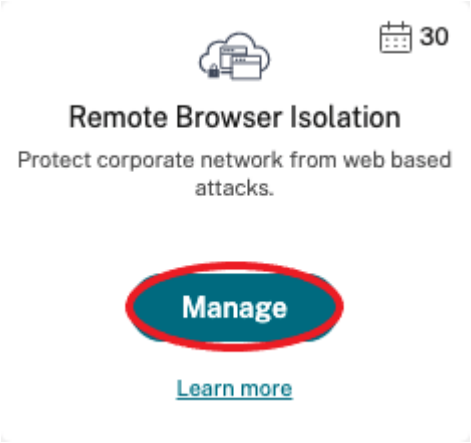
September 13, 2025

Here's a video about getting started with Remote Browser Isolation service (formerly Secure Browser service).

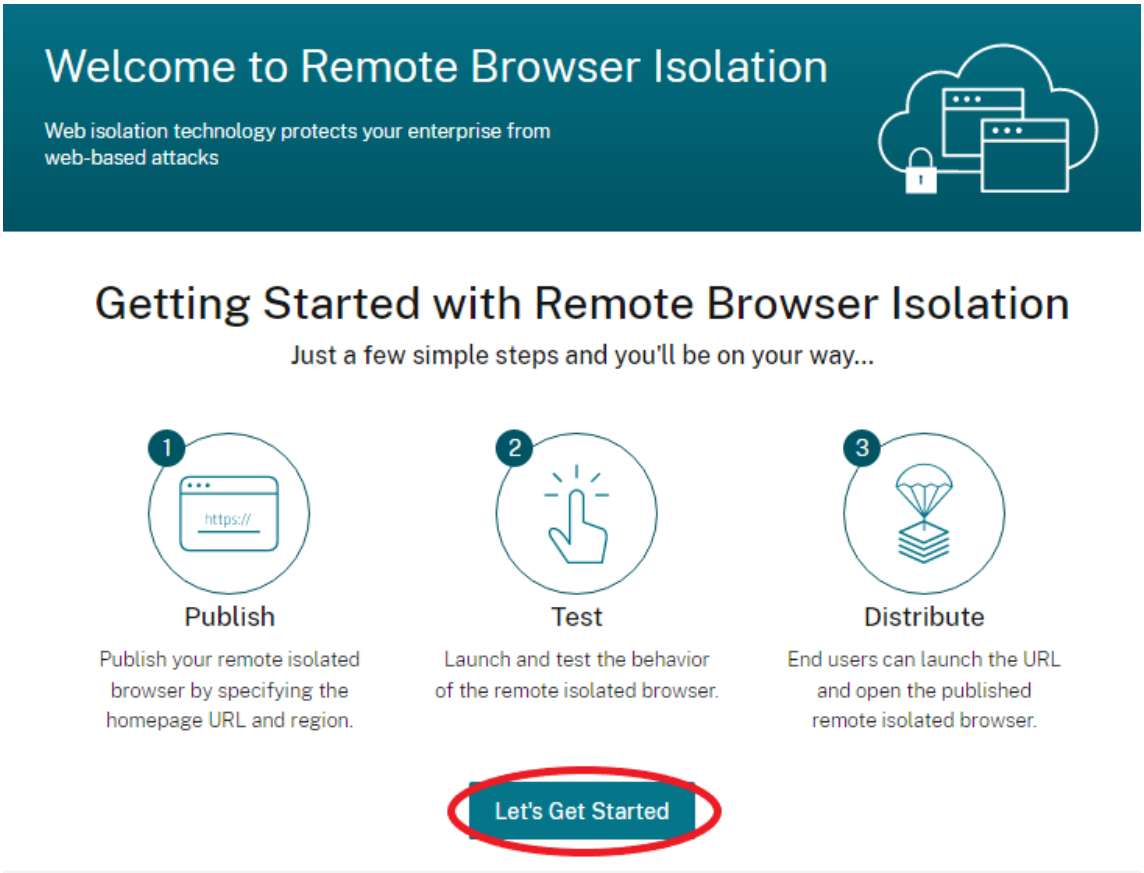
1. Sign in to Citrix Cloud. If you don't have an account, see Sign up for Citrix Cloud. You can request a 30-day trial of the Citrix Remote Browser Isolation.
2. In the **Remote Browser Isolation** tile, click **Request Trial**.



3. In a few moments, you will receive an email (the email associated with your Citrix Cloud™ account). Click the **Sign-in** link in the email.
4. After you're in Citrix Cloud again, click **Manage** on the **Remote Browser Isolation** tile.



5. On the **Welcome to Remote Browser Isolation** page, click **Let's Get Started**.



6. Select the type of remote isolated browser to publish: shared passcode, authenticated, or unauthenticated. Then click **Continue**.

   By default, users must launch apps with shared passcode authentication using launch.cloud.com. Citrix Workspace and the Citrix Cloud Library do not support apps with shared passcode.

   To use Citrix Workspace™, you must publish authenticated apps and explicitly assign subscribers (users) or groups in the Citrix Cloud Library. The unauthenticated apps are available

to all Workspace subscribers without user assignment.

7. Configure the following settings:

   - **Name:** Type a name for the app you are creating.
   - **Start URL:** Specify the URL that opens when users start an app.
   - **Region:** Choose the location/region for the server. Available regions are West US, East US, Southeast Asia, Australia East, and West Europe.

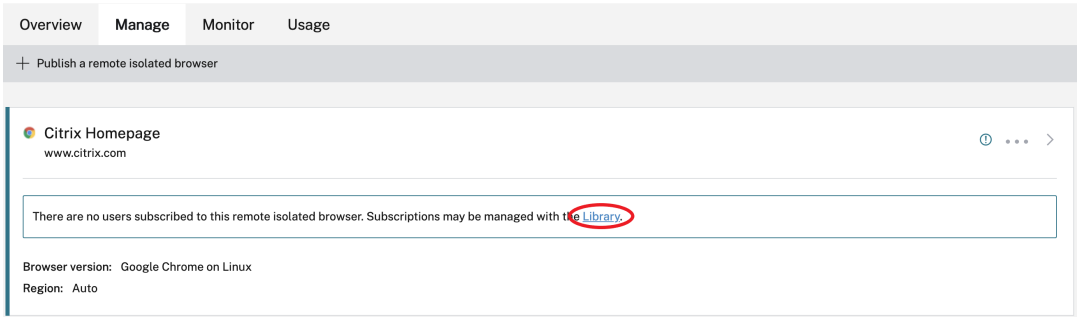
     If you select **Auto**, your isolated browser connects you to the closest region based on your geolocation.
   - **Passcode:** If you selected a browser with shared passcode authentication, enter the passcode to provide an enhanced secure access to your app. The passcode must be at least 10 characters long with at least 1 numeral and 1 symbol. Ensure that you save the passcode and share it with your users. Users must enter the passcode when they launch an app using launch.cloud.com.
   - **Icon:** By default, the icon of the Google Chrome executable is used when you publish an isolated browser. You can now choose your own icon to represent a published browser.

     Click **Change icon > Select icon** to upload the icon of your choice, or choose **Use default icon** to use the existing Google Chrome icon.

   Click **Publish**.

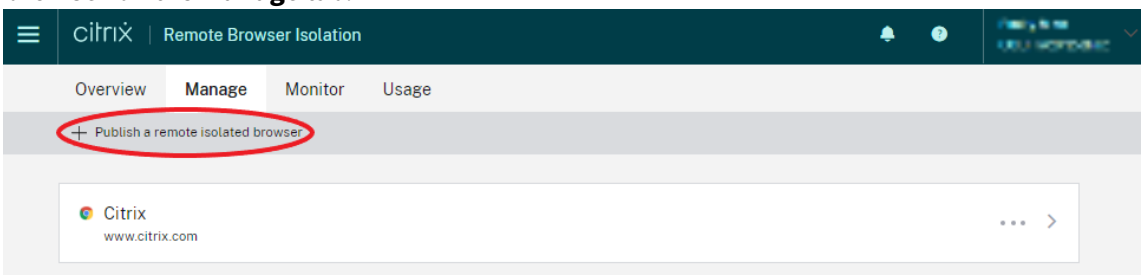
8. The **Manage** tab lists the browser you published. To launch the browser you just created, click the ellipsis on the tile containing the isolated browser and click **Launch Published Browser**.

   - If you published an authenticated isolated browser, you must use the Citrix Cloud Library to add users or groups. Click the right arrow at the end of the row to expand the details pane containing a link to the Library.

     When you click the link provided, you are guided to the Library display containing your remote isolated browser. Click the ellipsis on the tile containing the isolated browser and click **Manage Subscribers**. For information about adding subscribers, see Assigning users and groups to service offerings using Library.

You can publish another remote isolated browser by clicking **Publish a remote isolated browser** on the **Manage** tab.



For information about purchasing the Citrix Remote Browser Isolation service (formerly Citrix Secure Browser service), visit https://www.citrix.com/products/citrix-remote-browser-isolation/.

Integration with Citrix Workspace

Remote Browser Isolation can be integrated with Citrix Workspace. To ensure that it's integrated:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **Workspace Configuration**.
3. Select the **Service Integrations** tab.
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 Workspace URL, external connectivity, and workspace authentication for your Workspace, as described in Configure authentication to workspaces.

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

If you configure authentication using Azure Active Directory, 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.

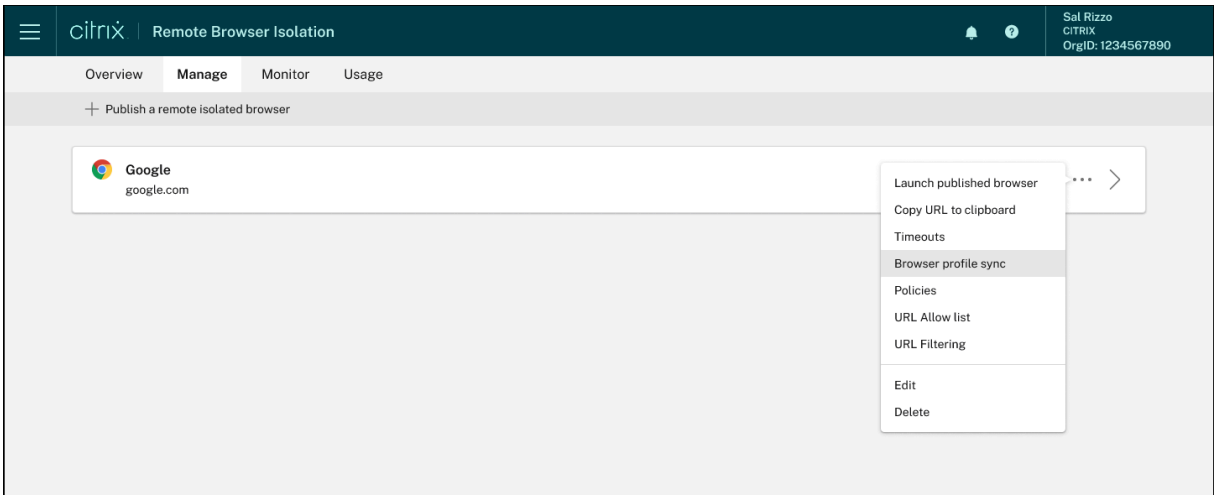
Manage and monitor remote isolated browsers

September 6, 2025

You can now manage, monitor, and check usage of the published browsers in Remote Browser Isolation.

Manage

The **Manage** tab lists the published browsers. To access management tasks, click the ellipsis at the right-end of the published browser, and then select the required task.



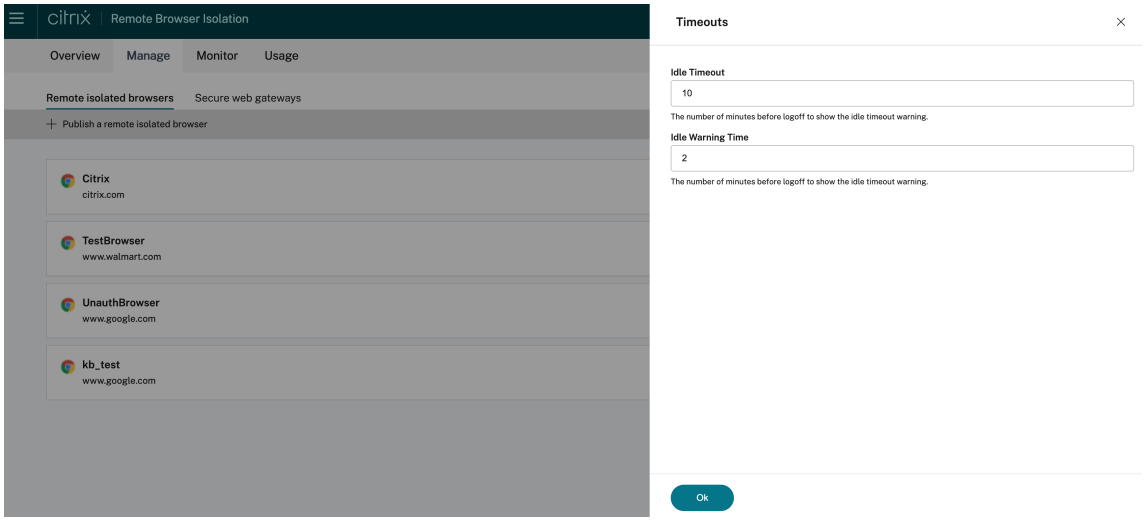
If you select a menu entry, and then decide not to change anything, cancel the selection by clicking the **X** outside the dialog box.

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

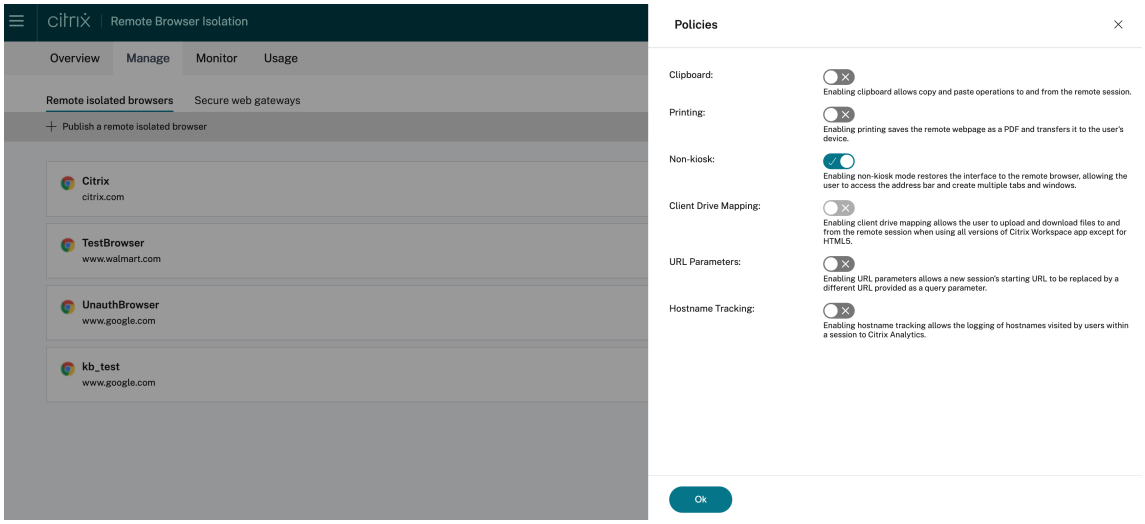
- **Launch published browser:** Opens the published browser session. After publishing the browser, you can select this task to verify the launch of the published browser session.
- **Copy URL to clipboard:** Copies the URL of the published browser. You can share this URL with end users to access the published browsers.
- **Timeouts:** You can set the **Idle timeout** and **Idle Warning time** by selecting the **Timeouts** task.
  - **Idle Timeout:** The number of minutes a session can stay idle before it's ended due to inactivity.
  - **Idle Warning Time:** The number of minutes before ending a session that a warning message is sent to the user.

  For example, if you set Idle Timeout to 20 and Idle Warning Time to 5, the system will display a warning message if there is no activity in the session for 15 minutes. If the user does not respond, the session ends five minutes later.

  To set **Idle timeout** and **Idle Warning time** of the published isolated browser, select the **Timeouts** task and set the time for **Idle Timeout** and **Idle Warning time** in the **Timeouts** dialog box. Then, click **OK** to save the changes.

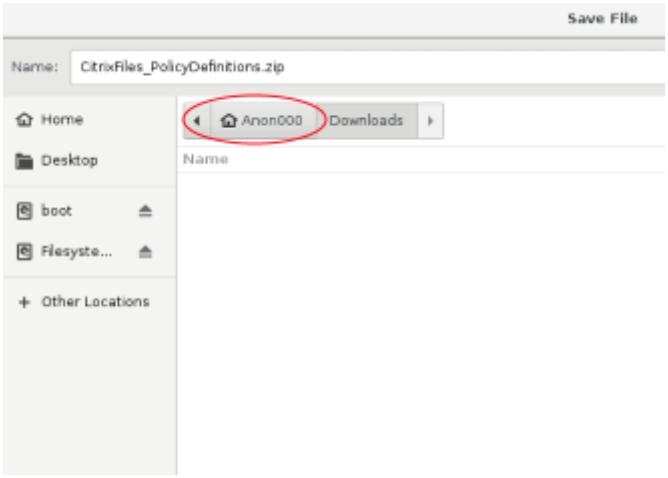


- **Policies:** You can set policies for the published browsers.

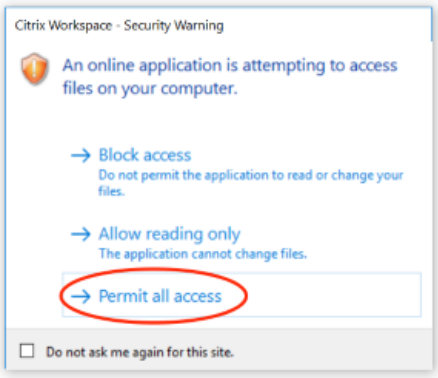


Settings on the policies page control the following:

- **Clipboard:** Enabling the Clipboard policy allows copy and paste operations to and from the remote session. (Disabling the Clipboard policy removes the Clipboard button from the Citrix Workspace™ app toolbar.) By default, this setting is disabled.
- **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**.



- 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.

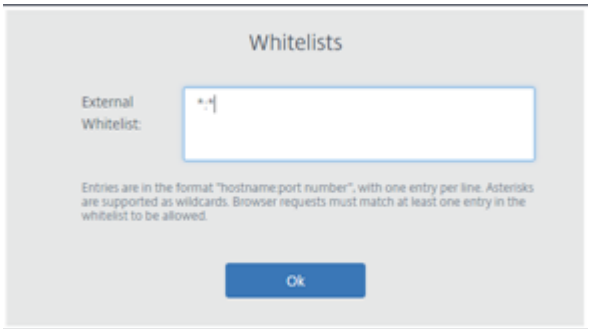
  Enter allow list entries in the form `hostname:port number`. Specify each entry on a new line. Asterisks are supported as wildcards. Browser requests must match at least one entry in the allow list.

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.



- **URL filtering:** You can configure URL filtering to control access methods based on pre-defined categories associated with risk models. URL filtering options include:
  - **None** - Allows all categories.
  - **Lenient** - Maximizes access while still controlling risk from illegal and malicious websites. Includes the following categories:
    - **Adult:** Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
    - **Computing and Internet:** remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
    - **Gambling:** Sweepstakes, prizes, lotteries, and gambling in general.
    - **Illegal and harmful:** Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
    - **Malware and spam:** Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
  - **Moderate** - Minimizes risk while allowing more categories with low probability of exposure from unsecure or malicious sites. Includes the following categories:

- **Adult:** Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
- **Business and industry:** Auctions.
- **Computing and Internet:** Advertisements, banners, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
- **Downloads:** Mobile app stores, storage services, downloads, and program downloads.
- **Email:** Web-based mail and email subscriptions.
- **Finance:** Cryptocurrency.
- **Gambling:** Sweepstakes, prizes, lotteries, and gambling in general.
- **Malware and spam:** Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
- **Messaging, chat, and telephony:** Instant messages and web-based chat.
- **News, entertainment, and society:** Wordpress (posts and uploads), unsupported URLs, occult, no content, miscellaneous, horoscope, astrology, fortune telling, drinking, religions, personal webpages, blogs, and online games.
- **Social networking:** Photo search and sharing sites, IT bulletin boards, and bulletin boards.

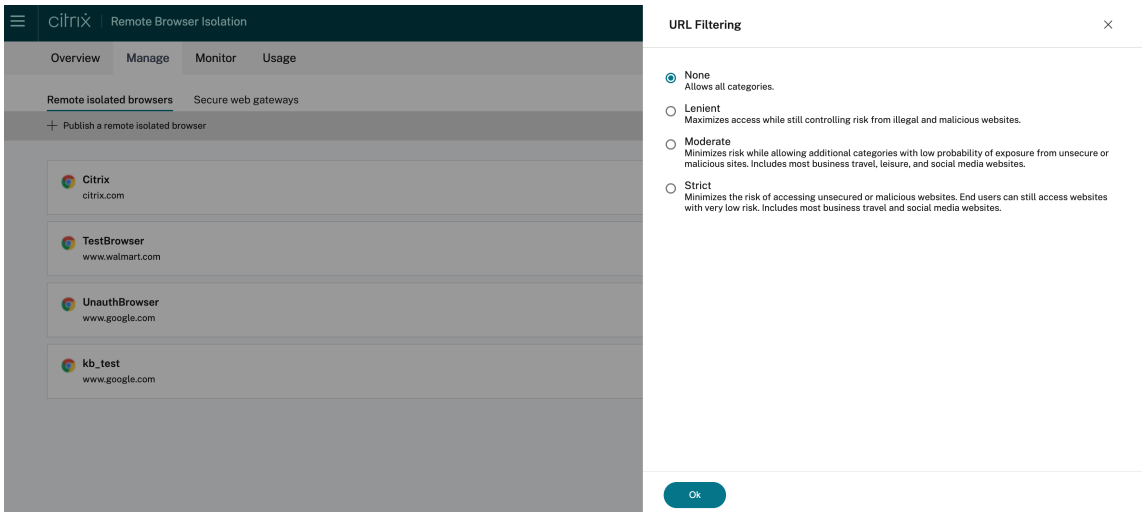
- **Strict** - Minimizes the risk of accessing unsecured or malicious websites. End users can still access websites with low risk. Includes the following categories:

  - **Adult:** Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Business and industry:** Auctions.
  - **Computing and Internet:** Advertisements, banners, dynamic DNS, mobile apps, publishers, parked domains, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Downloads:** Mobile app stores, storage services, downloads, and program downloads.
  - **Email:** Web-based mail and email subscriptions.
  - **Finance:** Cryptocurrency and financial products.
  - **Gambling:** Sweepstakes, prizes, lotteries, and gambling in general.
  - **Illegal and harmful:** Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
  - **Jobs and resumes:** Employment, career advancement, and LinkedIn (updates, mail, connections, and jobs).
  - **Malware and spam:** Hacking, malware, spam, spyware, botnets, infected sites, phish-

ing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.

- **Messaging, chat, and telephony:** Instant messages and web-based chat.
- **News, entertainment, and society:** Wordpress (posts and uploads), accommodations, travel and tourism, unsupported URLs, politics, fashion and beauty, arts and cultural events, reference, recreation and hobbies, local communities, miscellaneous, drinking, popular topics, special events, news, society and culture, online magazines, online games, life events, occult, no content, horoscope, astrology, fortune telling, celebrity, streaming media, entertainment, venues, activities, personal webpages and blogs, and religions.
- **Social networking:** Social networks in general, YikYak (posts), Twitter (posts, mail, and follows), Vine (uploads, comments, and messages), Google+ (photo and video uploads, posts, video chat, and comments), Instagram (uploads and comments), YouTube (shares and comments), Facebook (groups, games, questions, video upload, photo uploads, events, chat, apps, posts, comments, and friends), Tumblr (posts, comments, photo, and video uploads), Pinterest (pins and comments), IT bulletin boards, and bulletin boards.

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



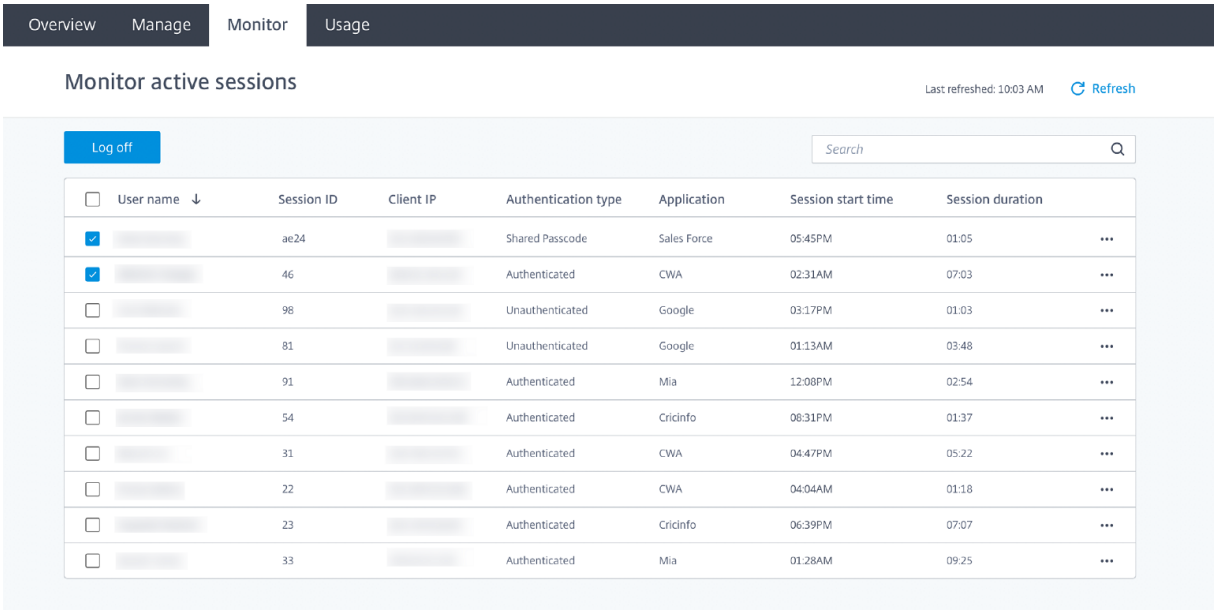
- **Edit:** You can use the **Edit** task to change the name, start URL, region of a published browser, or the passcode. When you're done, click **Publish**.
- **Delete:** You can use the **Delete** task to remove a published isolated browser. When you select this task, you're prompted to confirm the deletion.

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.

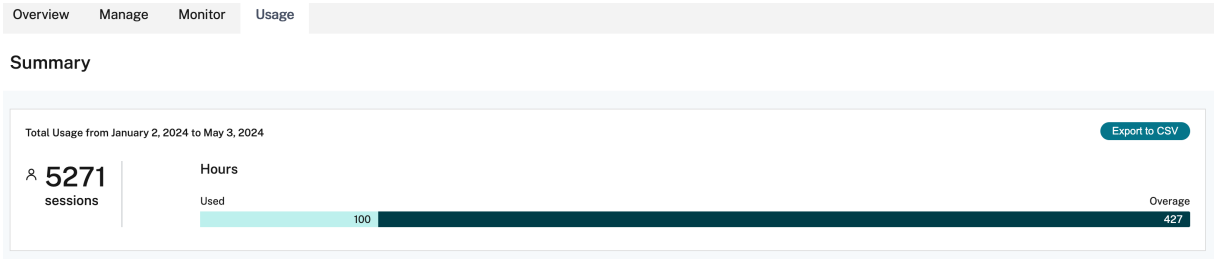
To disconnect multiple sessions, select the active sessions in the list and click the **Log off** button on the top of the page. After you confirm your changes, Remote Browser Isolation immediately disconnects all selected sessions.



Usage

The **Usage** tab shows the number of initiated sessions and the number of hours used.

To create a spreadsheet containing usage details, click **Export to CSV** and select a timeframe.



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.

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