Citrix Remote Browser Isolation

Machine translated content

Disclaimer

Contents

Remote Browser Isolation

July 2, 2024

Citrix Remote Browser Isolation (zuvor "Secure Browser") isoliert das Webbrowsing und schützt so das Unternehmensnetzwerk vor browserbasierten Angriffen. Remote Browser Isolation bietet konsistenten, sicheren Remotezugriff auf im Internet gehostete Webanwendungen, ohne dass eine Benutzergerätekonfiguration erforderlich ist. Administratoren können isolierte Remotebrowser schnell bereitstellen und so eine sofortige Amortisation erzielen. Durch die Isolierung des Internetbrowsings können IT-Administratoren Endbenutzern einen sicheren Internetzugang bieten, ohne die Sicherheit des Unternehmens zu gefährden.

Benutzer melden sich über Citrix Workspace (oder Citrix Receiver) an und können Web-Apps im konfigurierten Webbrowser öffnen. Die Website überträgt keine Browserdaten direkt zum oder vom Benutzergerät, sodass die Benutzererfahrung sicher ist.

Remote Browser Isolation kann isolierte Remotebrowser für folgende Zwecke veröffentlichen:

- **Freigegebener Passcode für externe Web-Apps.** Wenn Sie einen Browser mit Authentifizierung per freigegebenem Passcode veröffentlichen, müssen Benutzer den Passcode eingeben, um eine App zu starten.
- **Authentifizierte externe Web-Apps.** Wenn Sie authentifizierte externe Web-Apps veröffentlichen und die Apps mit Citrix Workspace starten, erfordert der Remote Browser Isolation-Dienst einen Ressourcenstandort mit mindestens einem Cloud Connector (zwei oder mehr werden empfohlen). Weitere Informationen finden Sie unter Citrix Cloud Connector. Bei authentifizierten Apps müssen Sie Benutzer mit der Citrix Cloud-Bibliothek hinzufügen.
- **Nicht authentifizierte externe Web-Apps.** Wenn Sie nicht authentifizierte externe Web-Apps veröffentlichen und die Apps mit Citrix Workspace starten, erfordert der Remote Browser Isolation-Dienst einen Ressourcenstandort mit mindestens einem Cloud Connector (zwei oder mehr werden empfohlen). Weitere Informationen finden Sie unter Citrix Cloud Connector.

  Die Verwendung nicht authentifizierter externer Web-Apps wird normalerweise nicht empfohlen, jedoch können sie für eine einfache Machbarkeitsstudie verwendet werden.

Weitere Informationen finden Sie unter Isolierte Remotebrowser veröffentlichen.

Der Service bietet zudem Folgendes:

- Integration veröffentlichter Apps in Citrix Workspace
- Integration veröffentlichter Apps mit dem lokalen StoreFront
- Einfache URL-Zulassungslistenfunktion für mehr Sicherheit
- Überwachen der Verwendung

- Steuerelemente für die Zwischenablage, zum Drucken, den Kioskmodus, das Regionsfailover und die Clientlaufwerkzuordnung

Remote Browser Isolation-Dienst mit Citrix Secure Private Access

Sie können die veröffentlichten Browser des Remote Browser Isolation-Diensts starten, indem Sie die Citrix Secure Private Access-Konsole für den Zugriff auf die Enterprise Web-, TCP- und SaaS-Anwendungen verwenden. Sie können die unsanktionierten Websites auch so umleiten, dass sie in den veröffentlichten Browsern des Remote Browser Isolation-Diensts über Citrix Secure Private Access geöffnet werden.

Weitere Informationen zum Zugriff auf die isolierten Remote-Browser über Citrix Secure Private Access finden Sie unter Konfigurieren einer Zugriffsrichtlinie mit mehreren Regeln und Unsanktionierte Websites in der Dokumentation zu Citrix Secure Private Access.

Referenz

- Überblick über die Secure Private Access-Servicelösung
- Citrix Cloud
- Self-Service-Suche nach Remote Browser Isolation (Secure Browser)
- Citrix Enterprise Browser
- Security and Compliance Information
- Developer Documentation

Neue Features in verwandten Produkten

- Secure Private Access
- Citrix Enterprise Browser
- Citrix Analytics für Sicherheit

Was ist neu

October 16, 2022

Juli 2022

- **Remote Browser Isolation unterstützt die Authentifizierung für alle Apps mit Azure Active Directory.**

  - Die Benutzer können sich jetzt mit Azure Active Directory-Anmeldeinformationen von Citrix Workspace aus bei beliebigen Remote Browser Isolation-Apps anmelden.
  - Wenn sich Remote Browser Isolation-Benutzer anmelden, verwenden sie die Workspace-Anmeldeseite, die Sie für Ihre Site konfiguriert haben. Weitere Informationen finden Sie unter Integration in Citrix Workspace.

September 2021

- **Remote Browser Isolation unterstützt bidirektionales Audio**. Bidirektionales Audio ist in Remote Browser Isolation verfügbar.
- **Remote Browser Isolation-Starts von launch.cloud.com werden per Citrix Cloud-Authentifizierung authentifiziert**. Wenn Benutzer Remote Browser Isolation-Apps mit der launch.cloud.com-URL starten, verarbeitet die Citrix Cloud-Authentifizierung ihre Anmeldeinformationen. Dies erhöht die Sicherheit, ändert jedoch nichts an der Benutzererfahrung.

März 2021

- **Remote Browser Isolation unterstützt die Authentifizierung mit Azure Active Directory.** Die Benutzer können sich jetzt mit Azure Active Directory-Anmeldeinformationen von Citrix Workspace aus bei Remote Browser Isolation-Apps anmelden. Weitere Informationen finden Sie unter Integration in Citrix Workspace.
- **Remote Browser Isolation ermöglicht das Überwachen und Abmelden aktiver Benutzersitzungen**. Remote Browser Isolation liefert zu aktiven Benutzersitzungen Daten zu Benutzernamen, Sitzungs-ID, Client-IP, Authentifizierungstyp, Anwendungsname, Startzeit der Sitzung und Sitzungsdauer. Sie können allgemeine Informationen zu jeder aktiven Sitzung anzeigen und die Sitzung bei Bedarf trennen. Weitere Informationen finden Sie unter Überwachen von Sitzungen.

Releases im Jahr 2020

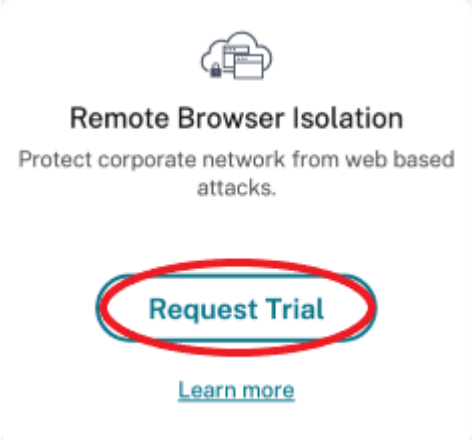
Jedes Release von 2020 enthält Erweiterungen zur Verbesserung der Gesamtleistung und Stabilität.

Erste Schritte mit Remote Browser Isolation

October 16, 2022

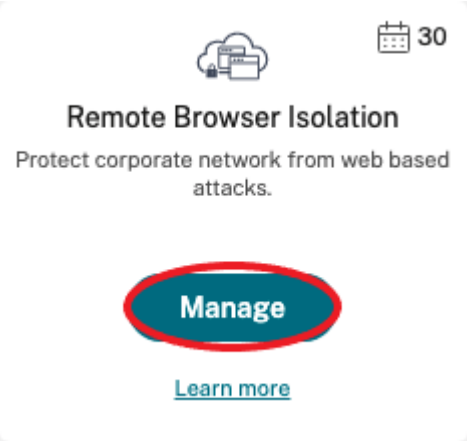
Das folgende Video zeigt die Grundlagen der Verwendung von Remote Browser Isolation (zuvor “Secure Browser”).

1. Melden Sie sich bei Citrix Cloud an. Wenn Sie kein Konto haben, finden Sie Informationen unter Registrierung bei Citrix Cloud. Sie können eine auf 30 Tage beschränkte Testversion von Citrix Remote Browser Isolation anfordern.
2. Klicken Sie auf der Kachel **Remote Browser Isolation** auf **Testversion anfordern**.

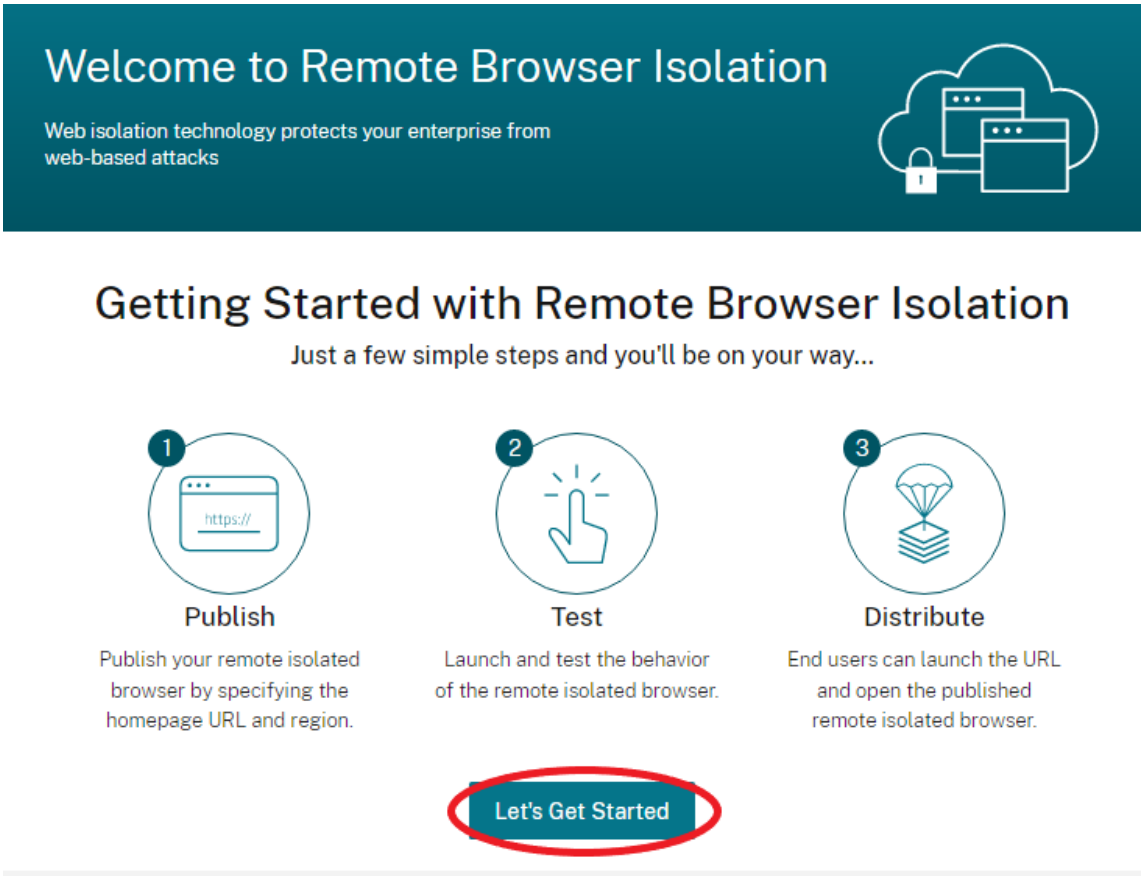


3. Nach kurzer Zeit erhalten Sie eine E-Mail (unter der mit Ihrem Citrix Cloud-Konto verknüpften E-Mail-Adresse). Klicken Sie in der E-Mail auf den Link **Anmelden**.

4. Wenn Sie wieder in Citrix Cloud sind, klicken Sie auf der Kachel **Remote Browser Isolation** auf **Verwalten**.



5. Auf der Seite **Willkommen bei Remote Browser Isolation** klicken Sie auf **Fangen wir an**.



6. Wählen Sie die Art des isolierten Remotebrowsers, der veröffentlicht werden soll: freigegebener Passcode, authentifiziert, oder nicht authentifiziert. Klicken Sie dann auf **Weiter**.

   Standardmäßig müssen Benutzer Apps mit Authentifizierung per freigegebenem Passcode über launch.cloud.com starten. Citrix Workspace und die Citrix Cloud-Bibliothek unterstützen keine

Apps mit freigegebenem Passcode.

Um Citrix Workspace verwenden zu können, müssen Sie authentifizierte Apps veröffentlichen und Abonnenten (Benutzer) oder Gruppen in der Citrix Cloud-Bibliothek explizit zuweisen. Nicht authentifizierte Apps sind ohne Benutzerzuweisung für alle Workspace-Abonnenten verfügbar.

7. Konfigurieren Sie die folgenden Einstellungen:

   - **Name:** Geben Sie einen Namen für die App ein, die Sie erstellen.
   - **Start-URL:** Geben Sie die URL an, die beim Starten einer App geöffnet wird.
   - **Region:** Wählen Sie den Standort/die Region für den Server aus. Verfügbare Regionen sind West-USA, Ost-USA, Südostasien, Ostaustralien und Westeuropa.

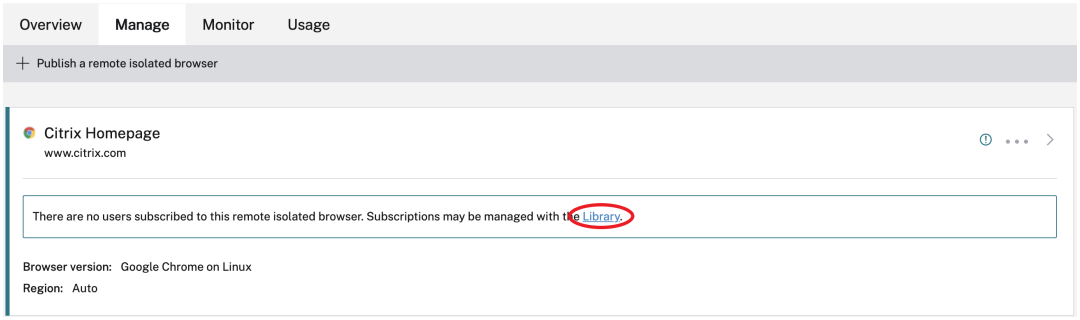
     Wenn Sie **Automatisch** wählen, stellt der isolierte Remotebrowser eine Verbindung mit der Ihrem geografischen Standort nächstgelegenen Region her.
   - **Passcode:** Wenn Sie einen Browser mit Authentifizierung per freigegebenem Passcode ausgewählt haben, geben Sie den Passcode ein, um einen besseren sicheren Zugriff auf Ihre App zu ermöglichen. Der Code muss mindestens zehn Zeichen enthalten, darunter mindestens eine Zahl und ein Symbol. Speichern Sie den Passcode und teilen sie ihn mit den Benutzern. Benutzer müssen den Passcode eingeben, wenn sie eine App mit launch.cloud.com starten.
   - **Symbol:** Standardmäßig wird das Symbol von Google Chrome beim Veröffentlichen eines isolierten Browsers verwendet. Sie können jetzt Ihr eigenes Symbol für einen veröffentlichten Browser auswählen.

     Klicken Sie auf **Symbol ändern > Symbol auswählen**, um das Symbol Ihrer Wahl hochzuladen, oder wählen Sie **Standardsymbol verwenden**, um das vorhandene Google Chrome zu verwenden.

   Klicken Sie auf **Veröffentlichen**.

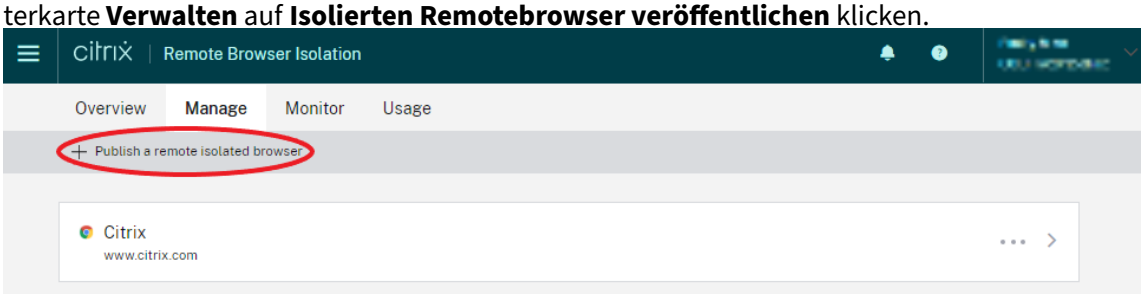
8. Auf der Registerkarte **Verwalten** sind die veröffentlichten Browser aufgelistet. Um den neu erstellten Browser zu starten, klicken Sie auf der Kachel des isolierten Browsers auf die Auslassungspunkte und dann auf **Veröffentlichten Browser starten**

   - Wenn Sie einen authentifizierten isolierten Browser veröffentlicht haben, müssen Sie die Citrix Cloud-Bibliothek verwenden, um Benutzer oder Gruppen hinzuzufügen. Klicken Sie auf den nach rechts weisenden Pfeil am Ende der Zeile, um den Detailbereich mit einem Link zur Bibliothek zu sehen.



Wenn Sie auf den bereitgestellten Link klicken, werden Sie zur Bibliothek geleitet, die den isolierten Remotebrowser enthält. Klicken Sie auf der Kachel mit dem isolierten Browser auf die Ellipse und klicken Sie auf **Abonnenten verwalten**. Informationen zum Hinzufügen von Abonnenten finden Sie unter Zuweisen von Benutzern und Gruppen zu Serviceangeboten über die Bibliothek.

Sie können einen anderen isolierten Remotebrowser veröffentlichen, indem Sie auf der Registerkarte **Verwalten** auf **Isolierten Remotebrowser veröffentlichen** klicken.



Informationen zum Erwerb von Citrix Remote Browser Isolation (zuvor "Citrix Secure Browser") finden Sie auf https://www.citrix.com/products/citrix-remote-browser-isolation/.

Integration in Citrix Workspace

Remote Browser Isolation kann in Citrix Workspace integriert werden. Sicherstellen der Integration:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü links oben die Option **Workspacekonfiguration**.
3. Wählen Sie die Registerkarte **Serviceintegrationen**.
4. Vergewissern Sie sich, dass für Remote Browser Isolation **Aktiviert** angezeigt wird. Wenn dies nicht der Fall ist, klicken Sie auf das Ellipsenmenü und wählen Sie **Aktivieren**.

Falls noch nicht geschehen, konfigurieren Sie die Workspace-URL, die externe Konnektivität und die Workspace-Authentifizierung für Ihren Workspace, wie unter Konfigurieren der Authentifizierung für Workspaces.

Remote Browser Isolation unterstützt die Authentifizierung mit Active Directory und Azure Active Directory. Die Authentifizierung mit Active Directory ist standardmäßig konfiguriert. Informationen

zum Konfigurieren der Azure Active Directory-Authentifizierung finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud.

Wenn Sie die Authentifizierung mit Azure Active Directory konfigurieren, muss die lokale Domäne, die Ihre Active Directory-Domänencontroller enthält, einen (vorzugsweise zwei) Cloud Connector enthalten.

Integrieren eines On-Premises-StoreFront

Benutzer von Citrix Virtual Apps and Desktops mit einem On-Premises-StoreFront können Remote Browser Isolation problemlos integrieren und folgende Vorteile genießen:

- Aggregieren der veröffentlichten isolierten Remotebrowser mit den über Citrix Virtual Apps and Desktops verfügbaren Apps für eine einheitliche Store-Erfahrung.
- Verwenden nativer Citrix Receiver für eine bessere Endbenutzererfahrung.
- Erhöhen der Sicherheit bei Remote Browser Isolation-Starts durch Verwendung der vorhandenen Multifaktorauthentifizierungslösung, die in StoreFront integriert ist.

Weitere Informationen finden Sie in CTX230272 und in der StoreFront-Konfigurationsdokumentation.

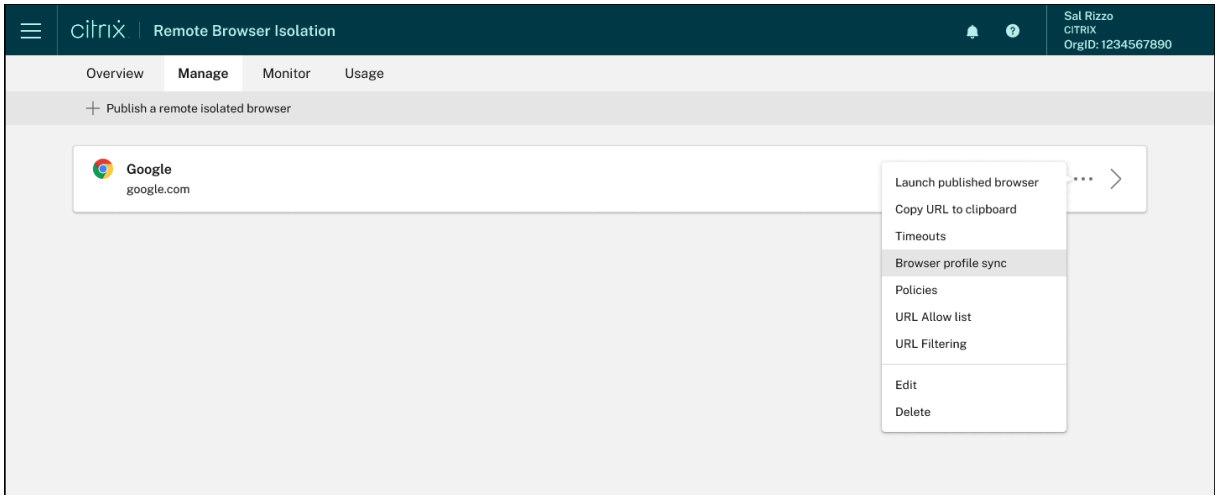
Isolierte Remotebrowser verwalten und überwachen

April 5, 2024

Sie können jetzt die Verwendung der veröffentlichten Browser in Remote Browser Isolation verwalten, überwachen und überprüfen.

Verwalten

Auf der Registerkarte **Verwalten** sind die veröffentlichten Browser aufgelistet. Um auf Verwaltungsaufgaben zuzugreifen, klicken Sie auf das Dreipunktmenü am rechten Ende des veröffentlichten Browsers und wählen Sie dann die erforderliche Aufgabe aus.



Wenn Sie einen Menüeintrag auswählen und dann doch nichts ändern möchten, brechen Sie die Auswahl ab, indem Sie außerhalb des Dialogfelds auf das **X** klicken.

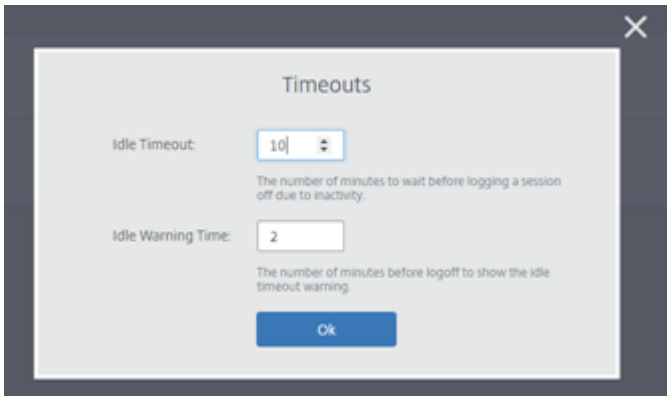
Sie können den veröffentlichten isolierten Browser über die folgenden Aufgaben verwalten:

- **Veröffentlichten Browser starten:** Öffnet die Sitzung des veröffentlichten Browsers. Nach der Veröffentlichung des Browsers können Sie diese Aufgabe auswählen, um den Start der Sitzung des veröffentlichten Browsers zu überprüfen.
- **URL in Zwischenablage kopieren:** Kopiert die URL des veröffentlichten Browsers. Sie können diese URL mit Endbenutzern teilen, damit diese auf die veröffentlichten Browser zugreifen.
- **Timeouts:** Sie können das **Leerlauftimeout** und die **Leerlaufwarnungszeit** festlegen, indem Sie die Aufgabe **Timeouts** auswählen.
  - **Leerlauftimeout:** Die Zeit in Minuten, die eine Sitzung inaktiv sein darf, bevor sie wegen Inaktivität beendet wird.
  - **Leerlaufwarnungszeit:** Die Zeit in Minuten vor dem Timeout einer Sitzung, wenn eine Warnmeldung an den Benutzer gesendet wird.

  Wenn Sie z. B. ein Leerlauftimeout von 20 Minuten und eine Leerlaufwarnungszeit von 5 Minuten festlegen, wird eine Meldung angezeigt, wenn 15 Minuten lang keine Aktivität in der Sitzung

stattfindet. Wenn der Benutzer nicht reagiert, wird die Sitzung fünf Minuten später beendet.

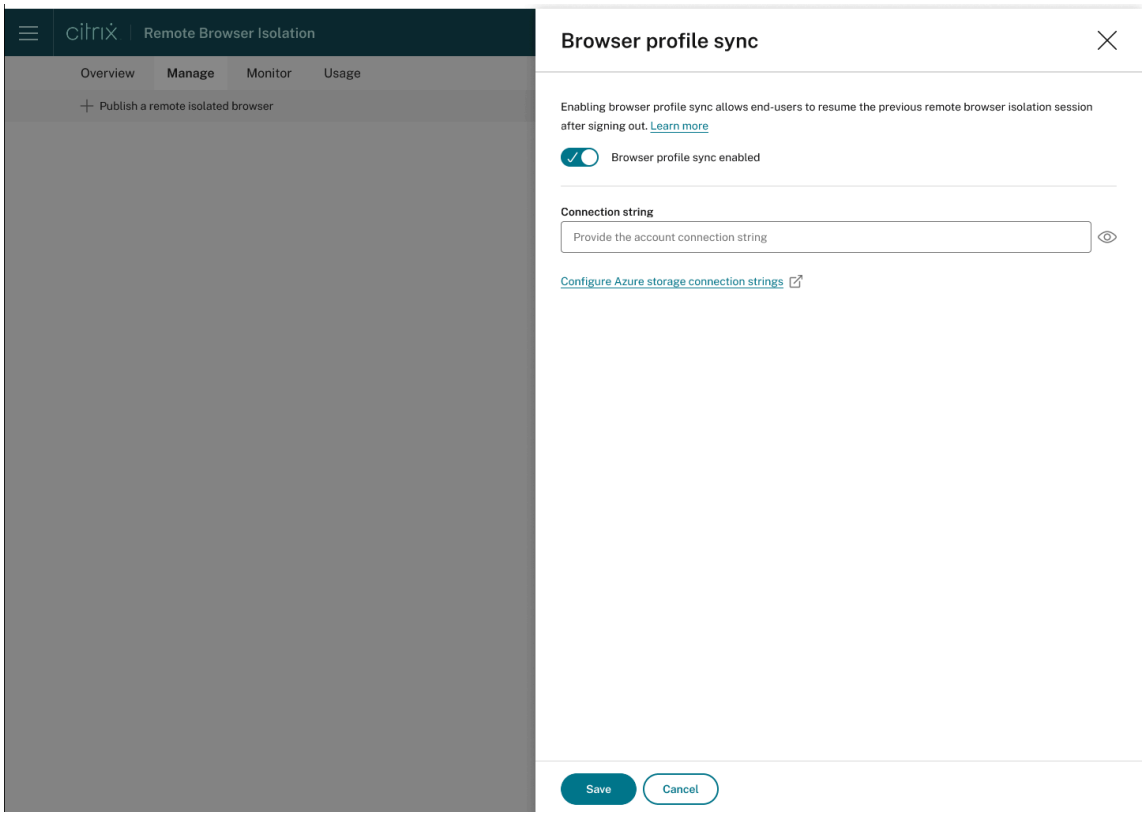
Um das **Leerlauftimeout** und die **Leerlaufwarnzeit** des veröffentlichten isolierten Browsers festzulegen, wählen Sie die Aufgabe **Timeouts** aus und legen Sie die Zeit für **Leerlauftimeout** und **Leerlaufwarnzeit** im Dialogfeld **Timeouts** fest. Klicken Sie dann auf **OK**, um die Änderungen zu speichern.



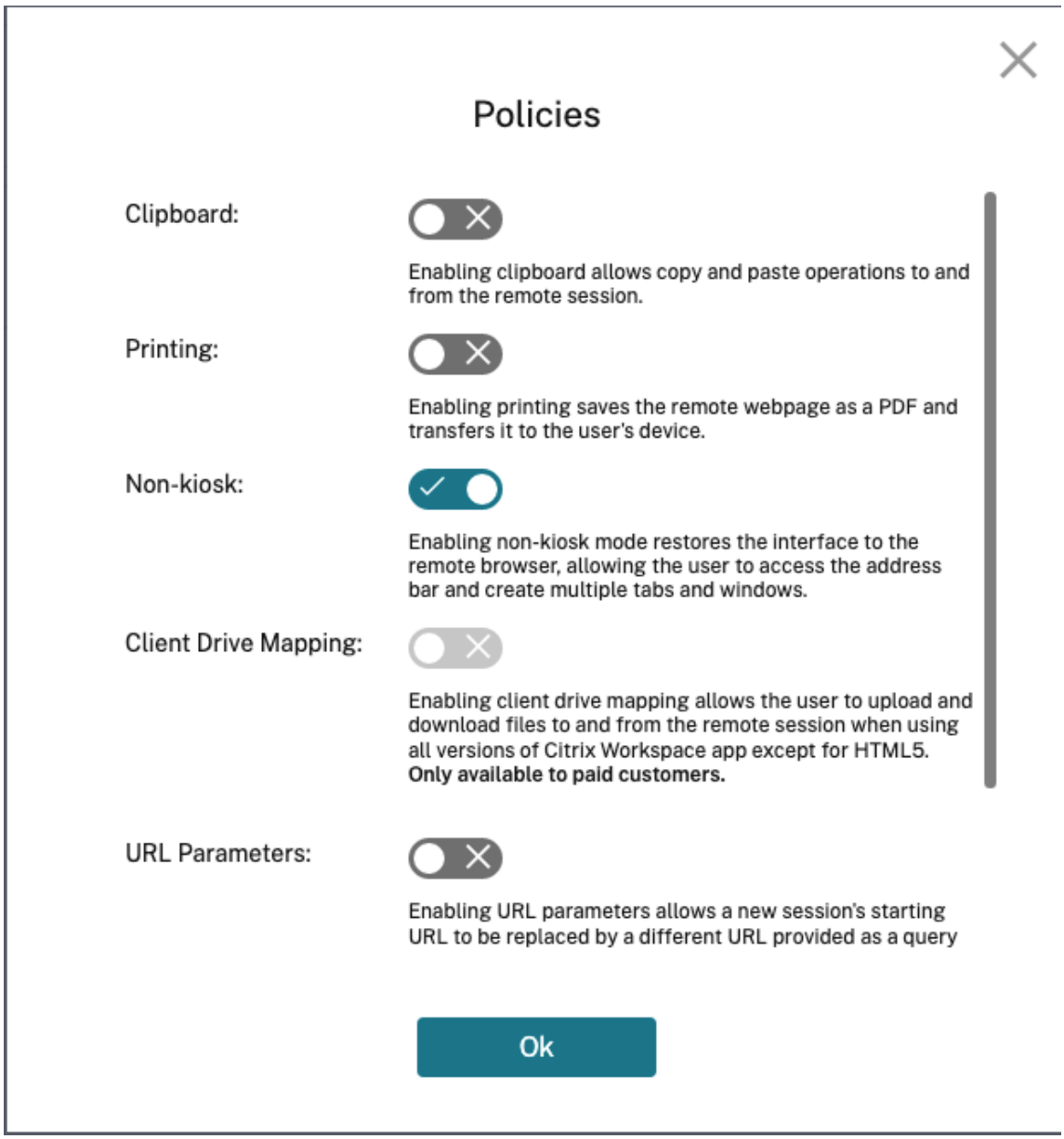
- **Browserprofilsynchronisierung**: Ermöglicht Endbenutzern, ihre vorherige Browsersitzung fortzusetzen, nachdem sie sich abgemeldet haben. Administratoren können eine Verbindungszeichenfolge für ihren Azure-Speicher angeben, um das Speichern des Browserprofils zu ermöglichen. Wenn der Benutzer eine weitere Browsersitzung mit demselben Profil öffnet, wird die vorherige Browsersitzung an der Stelle wiederhergestellt, an der der Benutzer aufgehört hat. Wenn sich der Benutzer auf Websites angemeldet hat, sind diese Websites für die Authentifizierung verantwortlich. Obwohl dieses Feature Sitzungen, Cookies und andere Informationen speichern kann, erfordert die Website möglicherweise, dass der Benutzer sich erneut anmeldet. Derzeit unterstützt dieses Feature nur die Wiederherstellung von Registerkarten.

  Gehen Sie wie folgt vor, um die Funktion zur **Browserprofilsynchronisierung** zu aktivieren:

  1. Wählen Sie die Aufgabe **Browserprofilsynchronisierung** für den erforderlichen veröffentlichten Browser aus.
  2. Aktivieren Sie im Dialogfeld **Browserprofilsynchronisierung** die **Browserprofilsynchronisierung** und geben Sie die **Verbindungszeichenfolge** ein. Weitere Informationen zur Konfiguration der Verbindungszeichenfolge finden Sie unter Azure Storage-Verbindungszeichenfolgen konfigurieren in der Azure Blob Storage-Dokumentation.
  3. Klicken Sie auf **Speichern**.



- **Richtlinien:** Sie können Richtlinien für die veröffentlichten Browser festlegen.



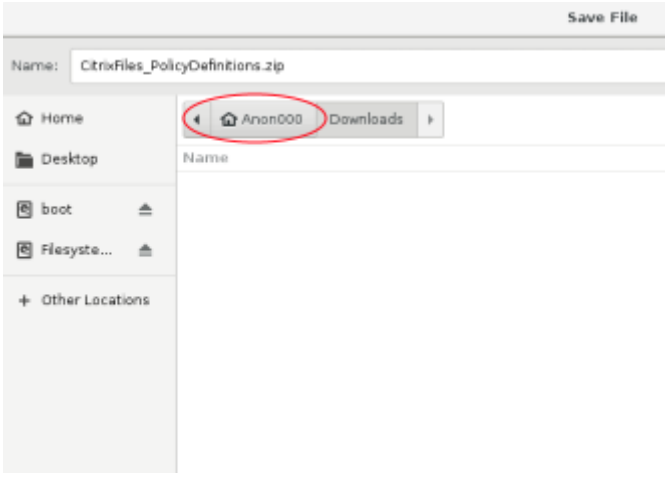
Die Einstellungen auf der Seite "Richtlinien"steuern Folgendes:

- **Zwischenablage:** Durch das Aktivieren der Richtlinie "Zwischenablage"werden Kopier- und Einfügevorgänge in die und aus der Remotesitzung gestattet. (Durch Deaktivieren der Richtlinie "Zwischenablage"wird die Schaltfläche für die Zwischenablage aus der Symbolleiste der Citrix Workspace-App entfernt.) Standardmäßig ist diese Einstellung deaktiviert.
- **Drucken:** Bei Aktivierung des Druckens, wird die Remotewebseite als PDF gespeichert und an das Gerät des Benutzers übertragen. Der Benutzer kann dann Strg+P drücken und den Citrix PDF-Drucker auswählen. Diese Einstellung ist standardmäßig deaktiviert.
- **Nicht-Kiosk:** Wenn der Nicht-Kioskmodus aktiviert wird, wird die Benutzeroberfläche auf den Remotebrowser zurückgesetzt. Der Benutzer kann dann auf die Adressleiste

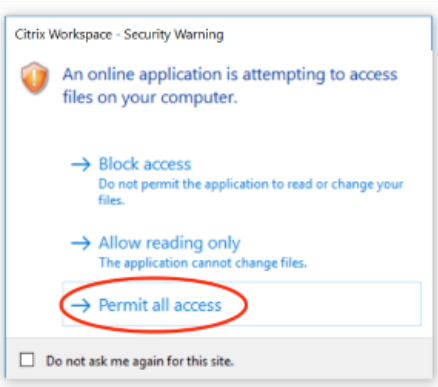
zugreifen und mehrere Registerkarten und Fenster erstellen. (Durch Deaktivieren des Nicht-Kioskmodus werden die Navigationssteuerelemente und die Adressleiste des Remotebrowsers entfernt.) Standardmäßig ist diese Einstellung aktiviert, d. h. der Nicht-Kioskmodus ist aktiviert.

- **Regionsfailover:** Die Richtlinie "Regionsfailover"überträgt Ihren veröffentlichten Browser automatisch in eine andere Region, wenn Ihre aktuelle Region ein Problem meldet. Wenn Sie dies nicht möchten, deaktivieren Sie die Richtlinie "Regionsfailover". Wenn Sie den isolierten Browser mit der Region **Auto** veröffentlicht haben, bleibt er für die Richtlinie registriert. Standardmäßig ist diese Einstellung aktiviert.
- **Clienlaufwerkzuordnung:** Bei aktivierter Clientlaufwerkzuordnungsrichtlinie können Benutzer Dateien in oder aus der Remotesitzung hoch- bzw. herunterladen. Dieses Feature ist nur für Sitzungen verfügbar, die mit der Citrix Workspace-App gestartet wurden. Die Einstellung ist standardmäßig deaktiviert.

  * Benutzer müssen heruntergeladene Dateien auf dem Datenträger `ctxmnt` im Verzeichnis `Anonxxx` speichern. Dafür müssen Benutzer zum gewünschten Speicherort für die Datei gehen. Beispiel: **Anonxxx > ctxmnt > C > Benutzer > Benutzername > Dokumente**.



  * Der Benutzer wird möglicherweise aufgefordert, die Berechtigungen für **uneingeschränkten Zugriff** oder **Lese- und Schreibzugriff** zu akzeptieren, um auf den Ordner `ctxmnt` zuzugreifen.



  - **URL-Parameter:** Durch Aktivieren von URL-Parametern können Sie die Start-URL einer neuen Sitzung ändern, wenn Benutzer eine App starten. Damit diese Richtlinie wirksam wird, konfigurieren Sie einen lokalen Proxyserver, um verdächtige Websites zu identifizieren und sie an Remote Browser Isolation umzuleiten. Diese Einstellung ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Proof of Concept Guide: URL Redirection to Remote Browser Isolation with Citrix ADC in Azure.
  - **Hostnamentracking:** Über das Hostnamentracking können Sie festlegen, dass Remote Browser Isolation Hostnamen während Benutzersitzungen protokollieren kann. Diese Richtlinie ist standardmäßig deaktiviert. Diese Informationen werden an Citrix Analytics weitergegeben. Weitere Informationen finden Sie unter Citrix Analytics.

  Wenn Sie fertig sind, klicken Sie auf **OK**.

- **URL-Positivlisten:** Verwenden Sie **Positivlisten**, um Benutzern in der veröffentlichten Remote Browser Isolation-Sitzung nur Zugriff auf zugelassene URLs zu gewähren. Diese Funktion ist für externe authentifizierte Web-Apps verfügbar.

  Einträge in der Positivliste müssen das Format `hostname:port number` haben. Jeder Eintrag muss in einer neuen Zeile erfolgen. Sternchen werden als Platzhalter unterstützt. Browseranforderungen müssen mit mindestens einem Eintrag in der Positivliste übereinstimmen.

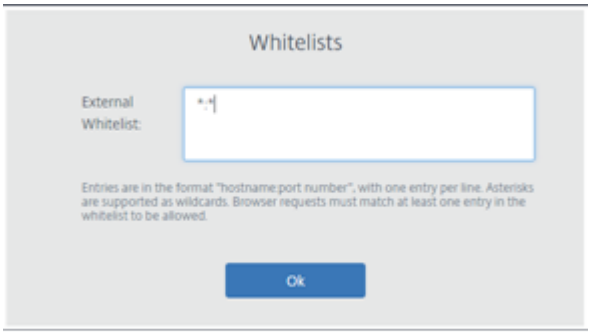
  Um zum Beispiel `https://example.com` als zulässige URL festzulegen:

  - `example.com:*` ermöglicht die Verbindung zu dieser URL von jedem Port aus.
  - `example.com:80` ermöglicht die Verbindung zu dieser URL nur von Port 80 aus.
  - `*:*` ermöglicht den Zugriff auf diese URL von jedem Port aus und über beliebige Links zu anderen URLs und Ports. Das Format mit `*.*` ermöglicht den Zugriff auf alle externen Web-Apps aus der veröffentlichten App. Dieses Format ist die Standardeinstellung für das Feld **Externe Positivliste** für Web-Apps.

  Wenn Sie fertig sind, klicken Sie auf **OK**.

  Erweiterte Webfilterfunktionen sind durch die Integration mit dem Zugriffssteuerungsservice

verfügbar. Weitere Informationen finden Sie unter Konfigurieren einer Zugriffsrichtlinie für den selektiven Zugriff auf Apps.



- **URL-Filterung:** Sie können die URL-Filterung zur Steuerung von Zugriffsmethoden basierend auf vordefinierten Kategorien konfigurieren, die mit Risikomodellen verknüpft sind. URL-Filteroptionen:
  - **Keine:** Erlaubt alle Kategorien.
  - **Nachsichtig:** Maximiert den Zugriff und begrenzt gleichzeitig das Risiko auf illegale und schädliche Websites. Umfasst die folgenden Kategorien:
    - **Erwachseneninhalte:** Grotesk, sexuelle Aufklärung, Pornografie, Nacktbilder, sexuelle Dienste, Erwachseneninhalte (Suche/Links), Bademode und Dessous, Erwachseneninhalte (Magazine/Nachrichten), sexueller Ausdruck (Text), Fetisch und Dating/Singlebörsen.
    - **Computer und Internet:** Remote-Proxyserver, private IP-Adressen, Peer-to-Peer-Dateifreigabe und Torrents.
    - **Glücksspiel:** Gewinnspiele, Preise, Lotterien und Glücksspiel allgemein.
    - **Illegal und schädlich:** Terrorismus, Extremismus, Hass, Verleumdung, Waffen, Gewalt, Selbstmord, illegale Drogen, Medikamente, illegale Aktivitäten, Marihuana und Rechtsfragen allgemein.
    - **Malware und Spam:** Hacking, Malware, Spam, Spyware, Botnets, infizierte Websites, Phishing-Sites, Keylogger, mobile Malware, Telefon-Bots, bösartige und gefährliche Websites.
  - **Moderat:** Minimiert das Risiko und lässt weitere Kategorien mit geringem Risiko auf unsichere oder schädliche Websites zu. Umfasst die folgenden Kategorien:
    - **Erwachseneninhalte:** Grotesk, sexuelle Aufklärung, Pornografie, Nacktbilder, sexuelle Dienste, Erwachseneninhalte (Suche/Links), Bademode und Dessous, Erwachseneninhalte (Magazine/Nachrichten), sexueller Ausdruck (Text), Fetisch und Dating/Singlebörsen.
    - **Industrie und Business:** Auktionen.

    * **Computer und Internet:** Werbung, Banner, Remote-Proxyserver, private IP-Adressen, Peer-to-Peer-Dateifreigabe und Torrents.
    * **Downloads:** Mobile App Stores, Speicherdienste, Downloads und Programm-Downloads.
    * **E-Mail:** Webbasierte E-Mail und E-Mail-Abonnements.
    * **Finanzen:** Kryptowährung.
    * **Glücksspiel:** Gewinnspiele, Preise, Lotterien und Glücksspiel allgemein.
    * **Malware und Spam:** Hacking, Malware, Spam, Spyware, Botnets, infizierte Websites, Phishing-Sites, Keylogger, mobile Malware, Telefon-Bots, bösartige und gefährliche Websites.
    * **Messaging, Chat und Telefonie:** Instant Messaging/Sofortnachrichten und webbasierter Chat.
    * **Nachrichten, Unterhaltung und Gesellschaft:** Wordpress (Posts und Uploads), nicht unterstützte URLs, Okkultes, keine Inhalte, Sonstiges, Horoskop, Astrologie, Wahrsagerei, Trinken, Religionen, persönliche Webseiten, Blogs und Onlinespiele.
    * **Soziale Netzwerke:** Websites für die Suche und Freigabe von Fotos, IT-Foren und Bulletin Boards.

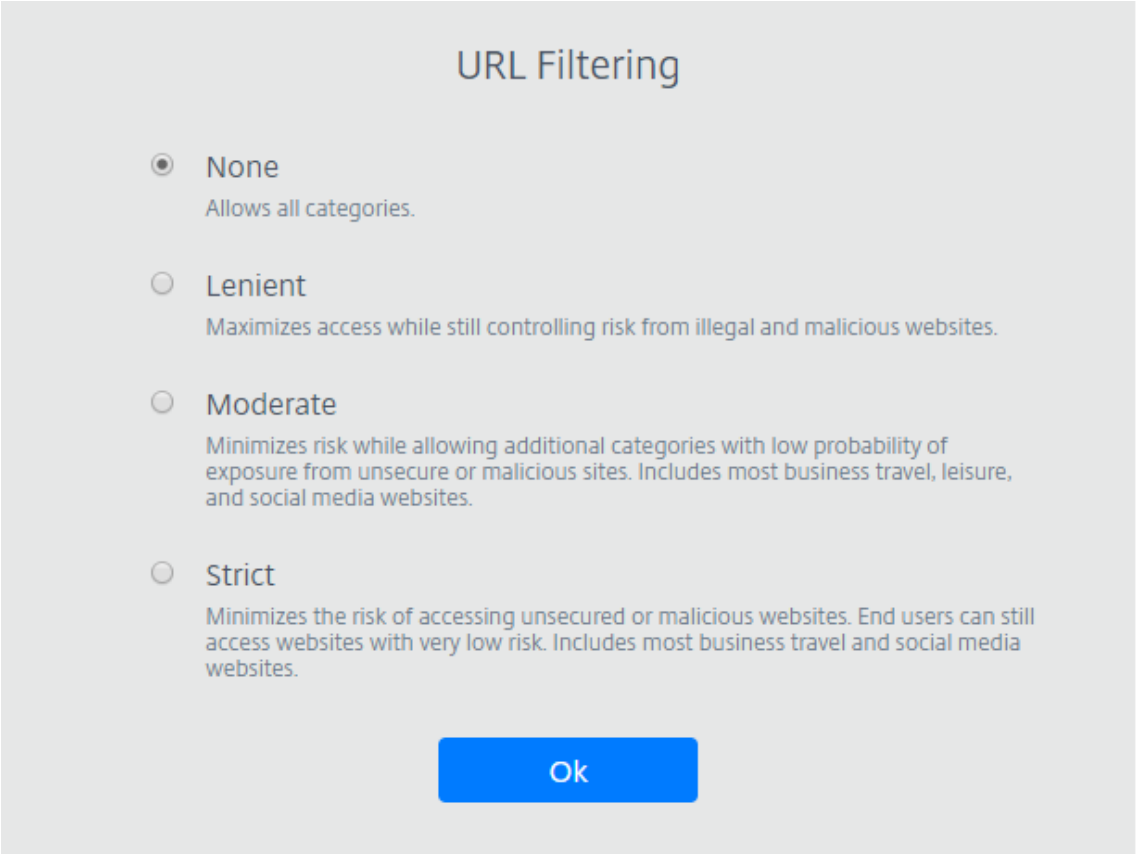
– **Streng:** Minimiert das Risiko, dass Benutzer auf unsichere oder schädliche Websites zugreifen. Endbenutzer können weiterhin auf Websites mit geringem Risiko zugreifen. Umfasst die folgenden Kategorien:

    * **Erwachseneninhalte:** Grotesk, sexuelle Aufklärung, Pornografie, Nacktbilder, sexuelle Dienste, Erwachseneninhalte (Suche/Links), Bademode und Dessous, Erwachseneninhalte (Magazine/Nachrichten), sexueller Ausdruck (Text), Fetisch und Dating/Singlebörsen.
    * **Industrie und Business:** Auktionen.
    * **Computer und Internet:** Werbung, Banner, dynamische DNS, mobile Apps, Herausgeber, Domainparking, Remote-Proxyserver, private IP-Adressen, Peer-to-Peer-Dateifreigabe und Torrents.
    * **Downloads:** Mobile App Stores, Speicherdienste, Downloads und Programm-Downloads.
    * **E-Mail:** Webbasierte E-Mail und E-Mail-Abonnements.
    * **Finanzen:** Kryptowährung und Finanzprodukte.
    * **Glücksspiel:** Gewinnspiele, Preise, Lotterien und Glücksspiel allgemein.
    * **Illegal und schädlich:** Terrorismus, Extremismus, Hass, Verleumdung, Waffen, Gewalt, Selbstmord, illegale Drogen, Medikamente, illegale Aktivitäten, Marihuana und Rechtsfragen allgemein.
    * **Stellenangebote und Lebensläufe:** Arbeitsmarkt, Karrieretipps und LinkedIn (Updates, E-Mail, Verbindungen und Jobangebote).
    * **Malware und Spam:** Hacking, Malware, Spam, Spyware, Botnets, infizierte Websites,

Phishing-Sites, Keylogger, mobile Malware, Telefon-Bots, bösartige und gefährliche Websites.

* **Messaging, Chat und Telefonie:** Instant Messaging/Sofortnachrichten und webbasierter Chat.
* **Nachrichten, Unterhaltung und Gesellschaft:** Wordpress (Beiträge und Uploads), Unterkünfte, Reisen und Tourismus, nicht unterstützte URLs, Politik, Mode und Schönheit, Kunst- und Kulturveranstaltungen, Referenz, Hobbys und Freizeit, Lokales/Nachbarschaft, Sonstiges, Trinken, populäre Themen, Veranstaltungen, News, Kultur und Gesellschaft, Onlinemagazine, Onlinespiele, Lebensereignisse, Okkultes, keine Inhalte, Horoskop, Astrologie, Wahrsagerei, Prominente, Streamingmedien, Unterhaltung, Veranstaltungsorte, Aktivitäten, persönliche Webseiten und Blogs, Religionen.
* **Soziale Netzwerke:** Soziale Netzwerke allgemein, YikYak (Beiträge), Twitter (Beiträge, E-Mail und Follower), Vine (Uploads, Kommentare und Nachrichten), Google+ (Foto- und Video-Uploads, Beiträge, Video-Chat und Kommentare), Instagram (Uploads und Kommentare), YouTube (geteilte Videos, und Kommentare), Facebook (Gruppen, Spiele, Fragen, Video-Uploads, Foto-Uploads, Events, Chat, Apps, Beiträge, Kommentare und Freunde), Tumblr (Beiträge, Kommentare, Fotos und Video-Uploads), Pinterest (Pins und Kommentare), IT-Foren und Bulletin-Boards.

Wenn Sie fertig sind, klicken Sie auf **OK**.



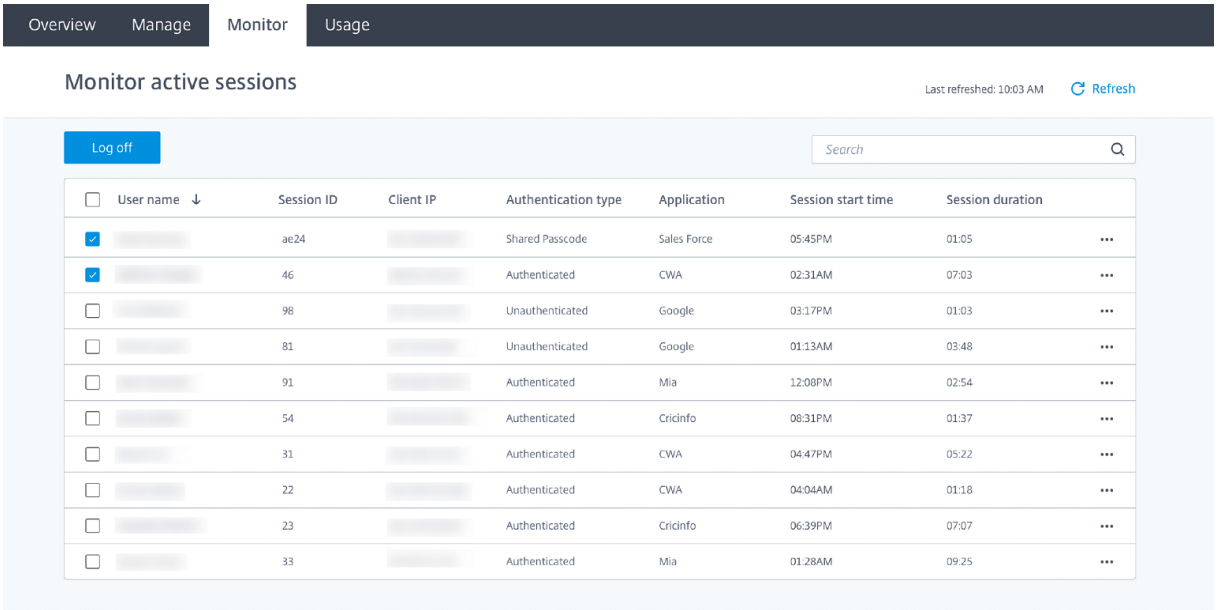
- **Bearbeiten:** Sie können mit der Aufgabe **Bearbeiten** den Namen, die Start-URL oder die Region eines veröffentlichten Browsers oder den Passcode ändern. Wenn Sie fertig sind, klicken Sie auf **Veröffentlichen**.
- **Löschen:** Sie können mit der Aufgabe **Löschen** einen veröffentlichten isolierten Browser entfernen. Bei Auswahl dieser Option werden Sie aufgefordert, das Löschen zu bestätigen.

Überwachung

Die Registerkarte **Überwachen** bietet Daten zu aktiven Sitzungen von Benutzern. Sie können eine oder mehrere aktive Sitzungen überwachen und trennen.

Um eine einzelne Sitzung zu beenden, wählen Sie die Sitzung aus und klicken Sie am Zeilenende des Eintrags auf die Auslassungspunkte (…). Klicken Sie auf **Sitzung abmelden** und bestätigen Sie Ihre Änderungen.

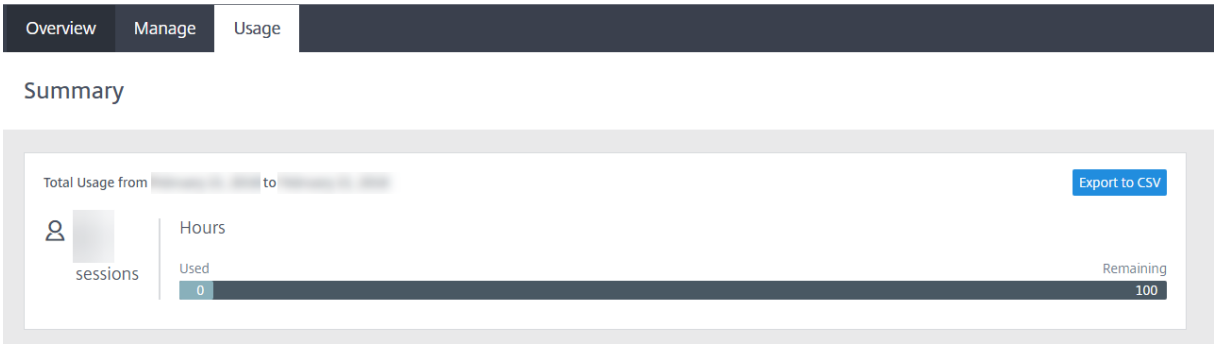
Um mehrere Sitzungen zu trennen, wählen Sie die aktiven Sitzungen in der Liste aus und klicken Sie oben auf der Seite auf die Schaltfläche **Abmelden**. Nachdem Sie Ihre Änderungen bestätigt haben, werden sämtliche ausgewählten Sitzungen sofort getrennt.



Verwendung

Auf der Registerkarte **Nutzung** werden die Anzahl der initiierten Sitzungen und die Anzahl der verwendeten Stunden angezeigt.

Klicken Sie auf **Als CSV-Datei exportieren** und wählen Sie einen Zeitrahmen, um eine Tabelle mit Verwendungsdetails zu erstellen.



Remote Browser Isolation –Technische Sicherheit

October 16, 2022

Remote Browser Isolation (zuvor "Secure Browser") ist ein SaaS-Produkt, das von Citrix verwaltet und betrieben wird. Er ermöglicht den Zugriff auf Webanwendungen über einen zwischengeschalteten Webbrowser in der Cloud.

Cloudservice

Citrix Remote Browser Isolation besteht aus Webbrowsern, die auf Virtual Delivery Agents (VDAs) zusammen mit der Verwaltungskonsole ausgeführt werden. Die Verwaltungskonsole dient zum Verwalten und Verbinden von Benutzern mit den VDAs. Citrix Cloud verwaltet den Betrieb dieser Komponenten, einschließlich der Sicherheit und des Patchens von Betriebssystemen, Webbrowsern und Citrix-Komponenten.

Bei Verwendung des Remote Browser Isolation-Diensts verfolgen gehostete Webbrowser den Browserverlauf des Benutzers und speichern HTTP-Anforderungen zwischen. Citrix verwendet obligatorische Profile und stellt sicher, dass diese Daten gelöscht werden, wenn die Browsersitzung beendet wird.

Der Zugriff auf Remote Browser Isolation erfolgt mit einem HTML5-kompatiblen Webbrowser. Der Service bietet keine herunterladbaren Clients. Der gesamte Datenverkehr zwischen dem verwendeten Browser und dem Cloudservice wird mit der branchenüblichen TLS-Verschlüsselung verschlüsselt. Remote Browser Isolation unterstützt nur TLS 1.2.

Ausgehender Datenverkehr für Remote Browser Isolation verwendet bestimmte IP-Adressen zum Schutz des internen Netzwerks. Eine Liste der akzeptierten IP-Adressen finden Sie im Knowledge Center-Artikel CTX286379.

Webanwendungen

Mit Citrix Remote Browser Isolation werden Webanwendungen von Kunden oder Dritten bereitgestellt. Der Eigentümer der Webanwendung ist für die Sicherheit verantwortlich, einschließlich des Patchens des Webservers und der Anwendung gegen Schwachstellen.

Die Sicherheit des Datenverkehrs zwischen Remote Browser Isolation und der Webanwendung hängt von den Verschlüsselungseinstellungen des Webservers ab. Um diesen Datenverkehr über das Internet zu schützen, veröffentlichen Administratoren HTTPS-URLs.

Weitere Informationen

Weitere Informationen zur Sicherheit finden Sie in den folgenden Ressourcen:

- Citrix Security Site: https://www.citrix.com/security
- Citrix Cloud-Dokumentation: Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform