Secure Access extension

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

Contents

Anti-keylogging control 2

Clipboard container control 3

Domain suffix for web applications 6

Session recording control 8

Browser session reauthentication control 11

SSH control 13

Remote Desktop control 16

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

Anti-keylogging control

October 1, 2026

Cybercriminals use malicious software such as keyloggers to steal sensitive information, such as passwords, credit card numbers, and confidential company data.

The Citrix Secure Access browser extension for Chrome Enterprise Premium (CEP) supports anti-keylogging to help protect your data. This feature scrambles keystrokes so that if a malicious program attempts to capture typed input, it records only unreadable characters while the actual text is securely delivered to your work applications.

Supported deployments: Citrix Secure Private Access service and hybrid deployments.

Supported platforms: Windows 11 and later.

> **Note:**
>
> Anti-keylogging is not supported for native RDP sessions.

Prerequisites

Ensure that the following prerequisites are met before enabling anti-keylogging:

- CWA version 2603 and later is installed.
- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.

Configure the anti-keylogging policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Anti-keylogging**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable anti-keylogging.
    a) Enter the name for the rule and click **Next**.
    b) Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.
    c) Click **Next**.
5. Click **Save**.

    The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > Anti-keylogging** tab.

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

Clipboard container control

October 1, 2026

Deployments that use Chrome for web access and VDI for native applications can use the Clipboard container feature to control data sharing between the browser and VDI sessions. Clipboard data is transferred directly between Citrix sessions without being written to the local endpoint clipboard. This improves security while still giving users flexibility to work across both environments.

Supported deployments: Secure Private Access service and hybrid deployments.

Supported platforms: Windows.

Prerequisites

Ensure that the following prerequisites are met:

- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.
- Citrix Workspace app 2603.10 or later.
- Windows VDA running 2607 LTSR or later (GA version for Clipboard Sharing Scope). For details, see Clipboard Sharing Scope.
- Windows VDA running 2507 LTSR (Preview version for Clipboard Sharing Scope), enable the following:
  - **Cross clipboard container with DaaS** feature. For details, see Cross clipboard container with DaaS. This feature is currently available as a preview in DaaS.
  - **Clipboard Sharing Scope** registry. For details, see Enable the Clipboard Sharing Scope registry.

Enable Clipboard Container control

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Clipboard container**, and then click **Manage**.
4. Click **Add Rule** to add rules for the clipboard share between VDA and browser.
   a) Enter the name for the rule and click **Next**.
   b) Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.

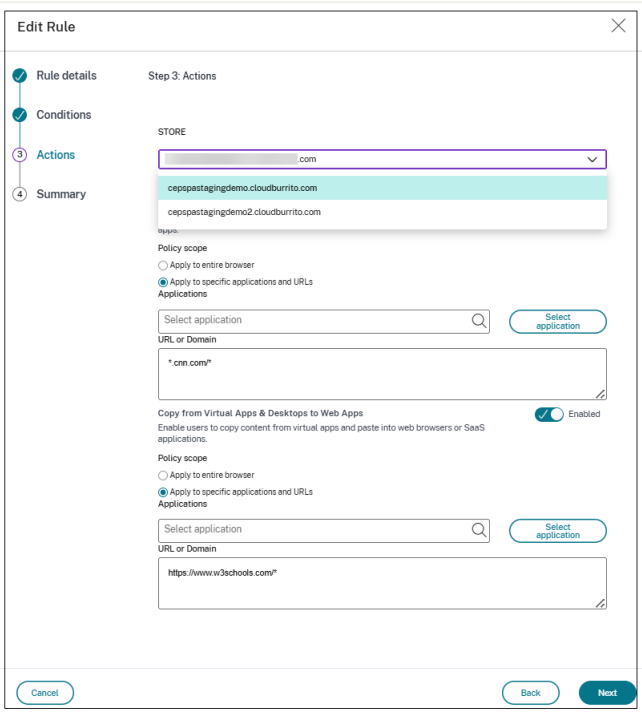
© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) Click **Next**.

d) Define the URL and Secure Private Access applications to allow clipboard sharing.

e) Select the policy scope.

- **Apply to entire browser** —The policy governs all clipboard activity in the managed profile.
- **Apply to specific applications and URLs** —The policy is limited to selected applications and the URL/domain patterns entered.
  - **Select Application** —Select the specific published applications using the application picker.
  - **URL or Domain** - Enter the URL or the domains of the specific application.



5. Click **Save**.

   The number of rules configured for the clipboard container policy appears in the **Browser Policies > Clipboard container** tab.

Enable Clipboard Sharing Scope

For VDA version 2607:

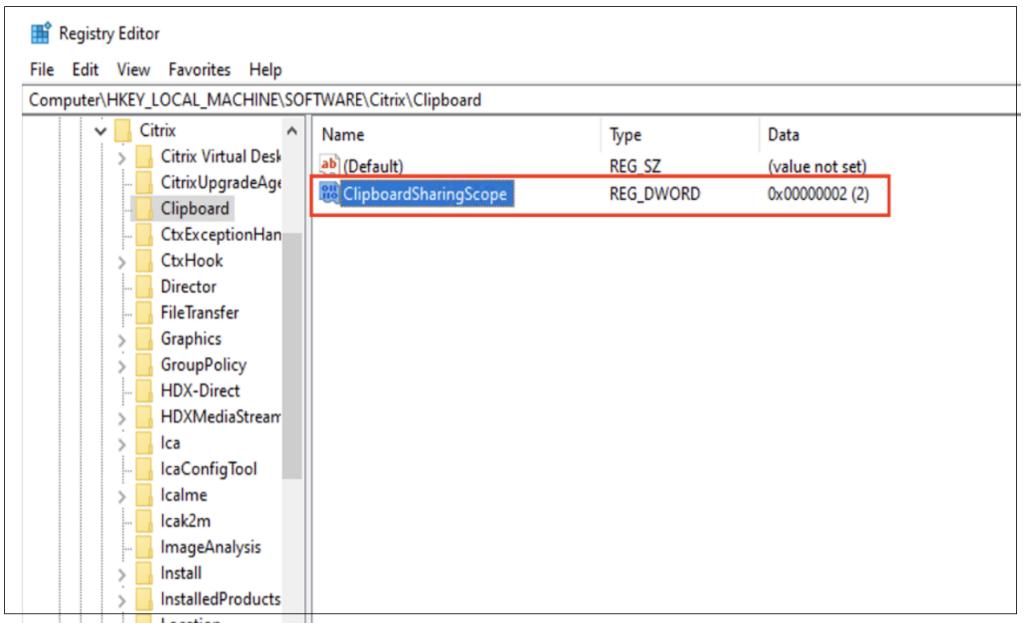
See How it works.

For VDA version 2507:

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

Enable this registry **Clipboard Sharing Scope** registry.

1. Open the Windows Registry Editor using regedit.exe.
2. Navigate to HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard.
3. Create a REG_DWORD [DWORD (32 bit)] value named `ClipboardSharingScope`.

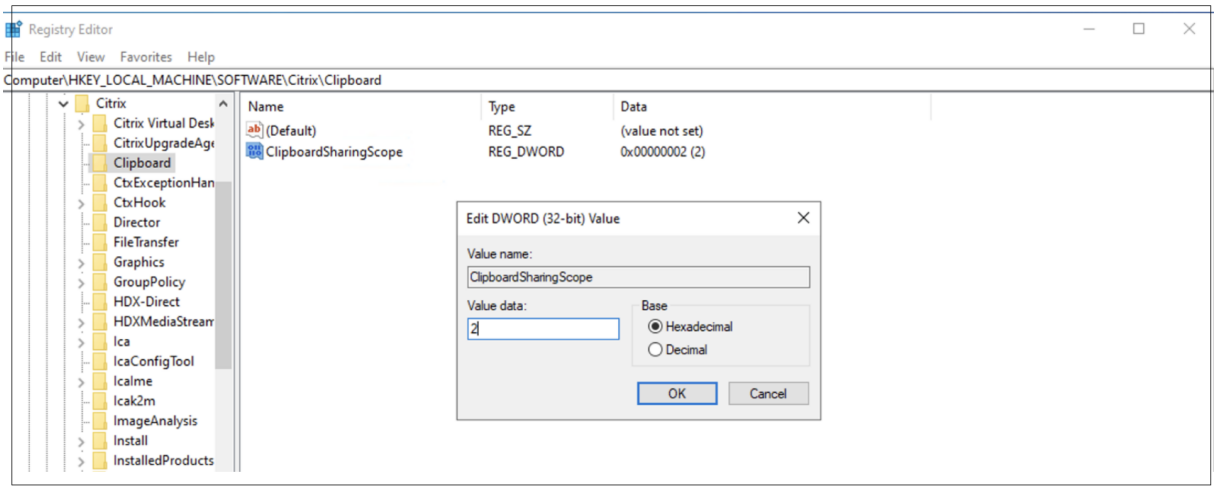


The `ClipboardSharingScope` policy controls where VDA clipboard data can be shared. Until the new DDC policy is available, this setting can be configured using the preceding registry key.

Supported value	Scope	Description
0	Unlimited	Clipboard data is copied to the client system clipboard and can be accessed by the Client, VDA, and CEP.
1	VDA only	Clipboard data is accessible only to the VDA. The client system clipboard and CEP cannot access the clipboard content.
2	CEP only	Clipboard data is accessible only to CEP. The client system clipboard and VDA cannot access the clipboard content.

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

Supported value	Scope	Description
3	VDA and CEP	Clipboard data is accessible to both the VDA and CEP. The client system clipboard cannot access the clipboard content.



Note:

- The CEP only (2) and VDA and CEP (3) modes are designed to work with the Clipboard Container feature in the CEP extension.
- When the Clipboard Container policy is enabled, only administrator-configured URLs are allowed to exchange clipboard data with the VDI.
  - Content copied from the approved web applications can be pasted into the VDI.
  - Content copied from the VDI can be pasted only into administrator-configured, paste-allowed URLs.
  - If a user attempts to paste VDI clipboard content into a website that is not included in the policy, the paste operation is blocked and an error message appears.

Domain suffix for web applications

October 1, 2026

In scenarios where users enter short, internal host names in the browser (for example, `sw` or `server001`), the domain suffix feature automatically appends the DNS suffix and converts them

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

into Fully Qualified Domain Names (FQDNs) using browser-managed DNS suffix policies instead of relying on the operating system's DNS suffix configuration.

The DNS suffix feature is supported on both **Windows** and **macOS** platforms, and consistently applies across common URL entry formats, including:

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

Supported deployments: Secure Private Access service and hybrid deployments.

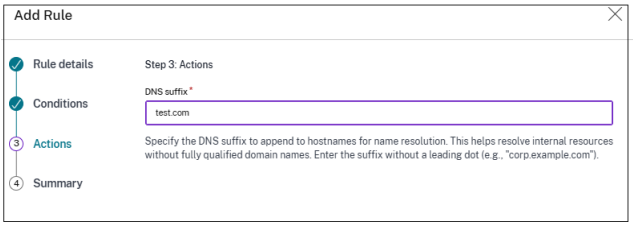
Supported platforms: Windows and macOS.

Prerequisites

Ensure that the integration of Citrix Secure Access with Chrome Enterprise is configured. For details, see Integration with Google Chrome Enterprise Premium.

Configure DNS suffix

1. Log in to the Secure Private Access admin console.
2. a) Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **DNS suffix**, and then click **Manage**.
4. Click **Add Rule** to add rules for the domain to be added to your URL.
   a) Enter the name for the rule and click **Next**.
   b) Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location** and **Device posture check**.
   c) Click **Next**.
   d) Define the domain that you want to append for access.



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

5. Click **Save**.

   The number of rules configured for the DNS suffix policy appears in the **Browser Policies > DNS suffix** tab.

Session recording control

October 1, 2026

Session recording records, catalogs, and archives sessions for retrieval and playback.

Session recording offers the following key benefits:

- Provides flexible policies to trigger recordings of application and desktop sessions automatically.
- Enables IT personnel to monitor and examine user activity, and supports internal controls for regulatory compliance and security monitoring.
- Aids technical support by speeding up problem identification and reducing time-to-resolution.

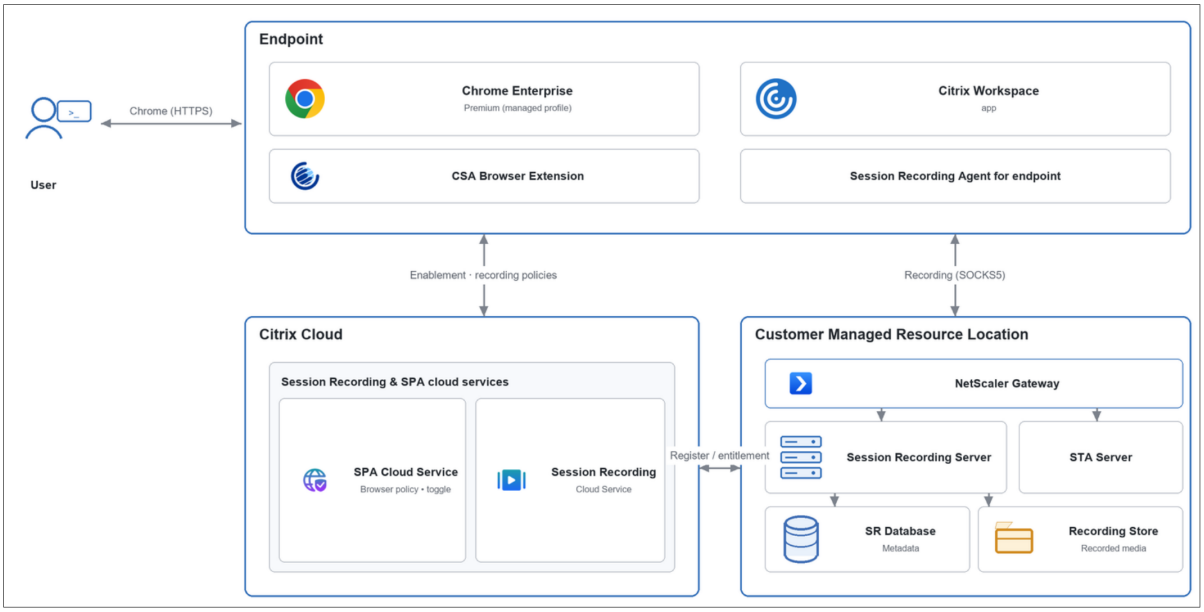
For details, see Benefits.

Architecture

The session recording solution spans three planes:

- The endpoint with the managed Chrome profile, Citrix Secure Access extension, and Session Recording Agent for endpoints.
- The Citrix Cloud control plane, which houses the Secure Private Access and Session Recording cloud services.
- The customer-managed resource location, which encompasses NetScaler Gateway, the STA server, the Session Recording server, and its database and recording stores.

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



Prerequisites

- Citrix Workspace app for Windows 2603.10 or later
- Endpoint analysis (EPA) version: 26.5.1.7 and later

System requirements

- Citrix Secure Private Access, deployed in either service or hybrid mode combined with Chrome Enterprise Premium (with managed profile).
- Session Recording Cloud service with Session Recording server 2511 or later. For details, see Get started.
- Windows 64-bit or 32-bit endpoints with the following components:
  - Citrix Endpoint Analysis (EPA) plug-in 26.5.1.7 or later.
  - Citrix Workspace app for Windows, version 2603.10 or later, with the Session Recording Endpoint Agent installed

Set up the environment

Complete the following steps to enable and validate endpoint recording for Chrome Enterprise sessions.

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

Configure the Session Recording site

Follow the steps documented in Configure endpoint recording policies.

> **Note:**
>
> NetScaler Gateway is required for endpoint recording. It routes recording traffic to the Session Recording Server through the STA in both Secure Private Access deployment types. Even with the Secure Private Access service, where NetScaler does not manage user-to-application access, you must provide a gateway URL for recording traffic.

Configure the Session Recording browser policy in Secure Private Access

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Session recording**, and then click **Manage**.
4. Click **Add Rule**, enter a name for the rule, and then click **Next**.
5. Set the conditions (users and groups). (Optional) Add **Geo-location**, **Network location** and **Device posture check**, and then click **Next**.
6. Click **Save**. The rule count appears on the **Browser Policies > Session recording** tab.

Install the Workspace App with Session Recording Agent for endpoints

Follow the steps documented in Session Recording add-on support.

Replay recorded sessions

Recordings are viewable in the Session Recording console.

- All windows associated with the user's Chrome work profile are recorded.
- Multiple windows across one or more monitors are recorded.
- Windows that are out of focus or obscured by another application are still recorded in their entirety.
- Minimized windows and windows with anti-screen capture enabled appear as black rectangles during playback.

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

Best practices

- **Keep one global site**. Use a single global endpoint-recording site and document the configuration. Changing it can unintentionally disable the other sites' configured policies.
- **Align regions**. Keep the Session Recording cloud service URL, cloud client, and back end in the same Citrix Cloud region to avoid latency and data-residency issues.
- **Plan storage**. Full-screen web/SaaS recording can be storage-intensive. Size the server, Session Recording database, and recording storage accordingly, and monitor storage consumption closely.
- **Validate entitlement and roles first**. Mismatched Citrix DaaS and Citrix Secure Private Access entitlements are the most common cause of deployment failure. Confirm that a single active customer record exists and that the required administrative roles are assigned before enabling policies.

Browser session reauthentication control

October 1, 2026

Citrix Secure Private Access allows administrators to enforce session timeout policies for Chrome Enterprise Premium (CEP) browser sessions. Users are required to re-authenticate after a configured session duration, regardless of browser activity. This strengthens Zero Trust access controls for applications accessed through the Google Chrome work profile.

Once a session expires, users must re-authenticate with enterprise credentials and multifactor authentication (MFA). Successful reauthentication restores their last active page and restarts the session timer.

Supported deployments: Secure Private Access service and hybrid deployments.

Supported platforms: Windows, macOS, Linux, ChromeOS.

Prerequisites

Ensure that the following prerequisite is met:

- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.

Enable Browser session reauthentication control

1. Log in to the Secure Private Access admin console.

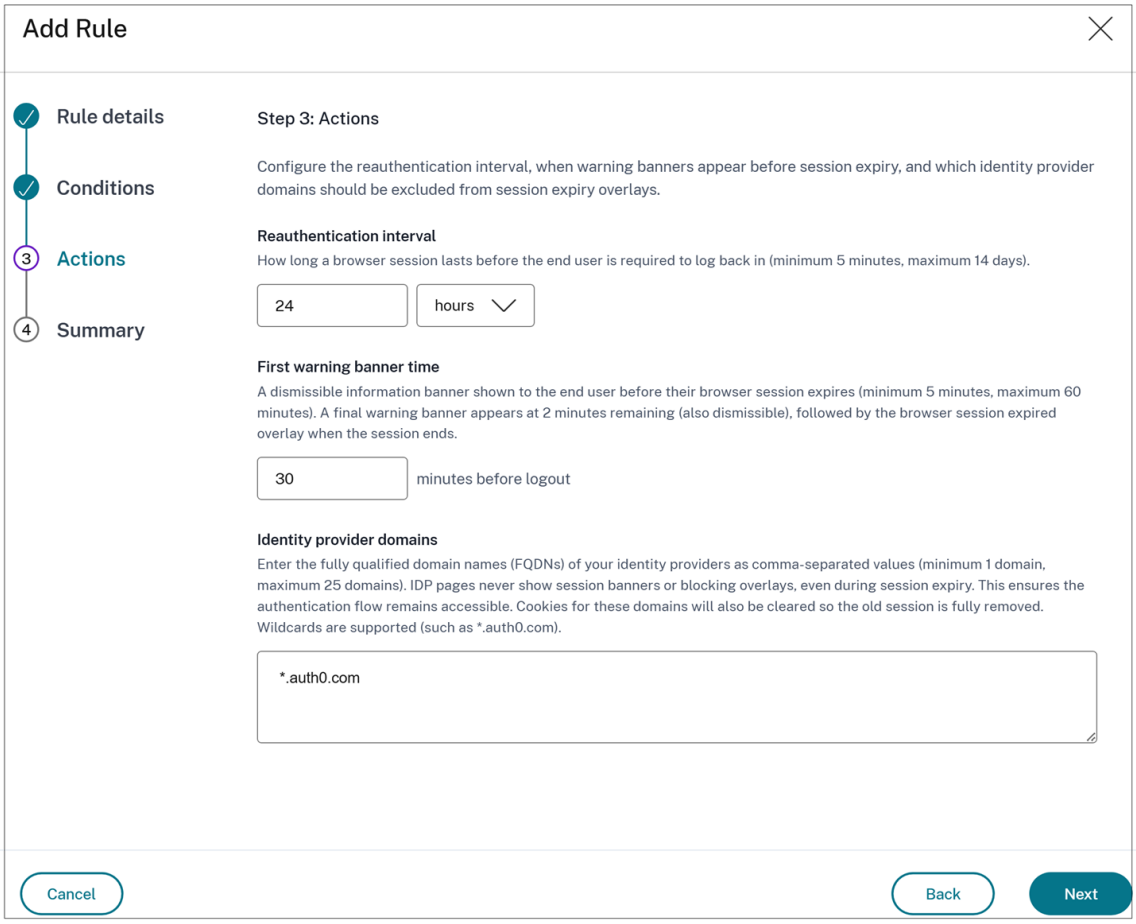
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Browser session reauthentication**, and then click **Manage**.
4. Click **Add Rule** to add rules to enable browser session reauthentication.

    a) Enter the name for the rule and click **Next**.
    b) Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.
    c) Click **Next**.
    d) Configure the following:

    - **Reauthentication interval**: The duration of a browser session before the user is required to re-authenticate. The interval can be set between 5 minutes and 14 days, and configured in minutes, hours, or days.
    - **First warning banner time**: A dismissible warning banner to be displayed to the user before their browser session expires. The value can be set between 5 and 60 minutes before expiry. A second warning banner appears when 2 minutes are left, followed by a session-expired overlay when the session ends.
    - **Identity provider domains**: The fully qualified domain names (FQDNs) of your identity providers as comma-separated values. You can specify between 1 and 25 domains. Session banners and blocking overlays are suppressed on IdP pages to ensure that the authentication flow remains uninterrupted. Cookies for these domains are cleared when the session expires to ensure that the old session is fully removed. Wildcards are supported (for example, *.auth0.com).

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



5. Click **Next** and then click **Save**.

   The number of rules configured for the clipboard container policy appears in the **Browser Policies > Browser session reauthentication** tab.

SSH control

October 1, 2026

Citrix Secure Private Access is integrated with Chrome Enterprise Premium to enable secure SSH sessions directly within the browser. This integration enhances security and streamlines access for administrators and users.

Organizations require secure remote administration of SSH-based systems. Traditional methods using standalone SSH clients pose risks by exposing endpoints to unmanaged environments and lacking robust Data Loss Prevention (DLP) enforcement, making compliance challenging.

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

The SSH sessions are now launched within the Chrome browser instead of standalone SSH clients, reducing dependency on local installations and improving compliance.

> **Note:**
>
> - This feature is applicable for Chrome Enterprise Premium integrated Secure Private Access setup for hybrid and cloud deployments. For details, see the following topics:
> - You must have admin rights to configure Secure Private Access and Chrome Enterprise Premium policies.
> - Connections to FreeBSD servers are not supported.

Benefits of this integration

This integration offers the following key benefits:

- **Enhanced security:** Eliminates reliance on unmanaged SSH clients, reducing exposure to security risks.
- **Simplified access:** Provides browser-native access, removing the need for additional software installations.
- **Compliance:** Enforces corporate DLP policies directly within the browser, helping meet regulatory requirements.
- **Operational efficiency:** Reduces IT overhead associated with endpoint management and client deployment.

Use cases

This feature supports various use cases such as:

- **Healthcare kiosks:** Enables secure SSH access for device troubleshooting without installing native clients.
- **IT administration:** Allows administrators to securely access Linux servers from managed Chrome browsers with enforced DLP policies.
- **Contractor access:** Provides temporary SSH access for third-party vendors without compromising the organization's security posture.

System requirements

Ensure that your environment meets the following requirements:

- Latest version of Chrome Enterprise Premium.

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

- Citrix Secure Private Access is configured for the integration.
- Access policies to allow SSH traffic must be created in the Secure Private Access admin console.

Prerequisites

Ensure that the following prerequisites are met for enabling secure access to SSH applications:

- Citrix Secure Private Access is configured with Google Chrome Enterprise Premium integration. For details, see Integration with Google Chrome Enterprise Premium.
- The end user has installed the latest Google Chrome browser with the Citrix Secure Access browser extension.
- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix Secure Private Access
  - Hybrid deployment –System requirements and prerequisites

Configure Secure Private Access for SSH access

1. Log in to Citrix Cloud and then click **Secure Private Access**.
2. In the admin console, Click **Applications > App Configuration**, and then click **Add an app**.
3. Configure the SSH app as a TCP/UDP app within Secure Private Access.
   - The app can have an exact IP address or a range, FQDN, or host name of the server.
   - SSH is supported over default and non-default ports.
4. Assign access to relevant user groups.

For detailed information on creating a TCP/UDP app, see the following topics.

- Cloud deployment - Support for TCP/UDP apps
- Hybrid deployment –Support for TCP/UDP apps

Configure the SSH policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **SSH**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable SSH.
5. Enter the name for the rule and click **Next**.
6. Select conditions based on your requirement such as user or group. 1. You can also add conditions such as **Geo-location, Network location**, and **Device posture check**.

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

7. Click **Next**.
8. Click **Save**.

The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > SSH** tab.

Remote Desktop control

October 1, 2026

Citrix Secure Private Access is integrated with Chrome Enterprise Premium to enable secure RDP sessions directly within the browser. This integration enhances security and streamlines access for administrators and users.

Traditional remote desktop access often relies on native RDP clients, which typically lack browser-based DLP enforcement. This deficiency can increase security risks, especially in unmanaged environments, and make compliance challenging. Organizations require a secure, compliant, and simplified solution for remote access that addresses these concerns.

This integration enables admins to enforce enterprise-grade DLP controls such as clipboard control and screenshot prevention.

> **Note:**
>
> - This feature is applicable for Chrome Enterprise Premium integrated Secure Private Access setup for hybrid and cloud deployments. For details, see the following topics:
> - You must have admin rights to configure Secure Private Access and Chrome Enterprise Premium policies.

Unsupported features:

The following features are not supported:

- Clipboard sharing
- Audio/WebCam/SmartCard/USB redirection
- Two-factor and biometric authentication

Benefits of this integration

This integration offers the following key benefits:

- **Security:** Prevents data leakage during remote sessions by enforcing granular DLP policies.

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

- **Compliance:** Helps meet regulatory requirements for sensitive environments through robust security controls.
- **Ease of use:** Eliminates the need for installing separate RDP clients, simplifying user access and deployment.
- **Flexibility:** Supports secure RDP access from managed Chrome browsers, providing a consistent and secure experience.

Use cases

This feature supports various use cases such as:

- **Enterprise contractors:** Provides secure remote desktop access for third-party vendors without compromising internal security.
- **Healthcare staff:** Enables secure access to Windows systems from kiosks or shared workstations in healthcare settings.
- **IT support:** Allows IT personnel to troubleshoot remote desktops without requiring additional software installations.

System requirements

Ensure that your environment meets the following requirements:

- Latest version of Chrome Enterprise Premium.
- Citrix Secure Private Access is configured for the integration.
- Access policies to allow RDP traffic must be created in the Secure Private Access admin console.

Prerequisites

Ensure that the following prerequisites are met for enabling secure access to RDP applications:

- Citrix Secure Private Access is configured with Google Chrome Enterprise Premium integration. For details, see Integration with Google Chrome Enterprise Premium.
- The end user has installed the latest Google Chrome browser with the Citrix Secure Access browser extension.
- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix Secure Private Access
  - Hybrid deployment –System requirements and prerequisites

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

Configure Secure Private Access for RDP access

1. Log in to Citrix Cloud and then click **Secure Private Access**.
2. In the admin console, Click **Applications > App Configuration**, and then click **Add an app**.
3. Configure the RDP app as a TCP/UDP app within Secure Private Access.
    - The app can have an exact IP address or a range, FQDN, or host name of the server.
    - RDP is supported over default and non-default ports.
4. Assign access to relevant user groups.

For detailed information on creating a TCP/UDP app, see the following topics.

- Cloud deployment - Support for TCP/UDP apps
- Hybrid deployment –Support for TCP/UDP apps

Configure the remote desktop policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Remote Desktop**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable remote desktop.
5. Enter the name for the rule and click **Next**.
6. Select conditions based on your requirement such as user or group. 1. You can also add conditions such as **Geo-location, Network location**, and **Device posture check**.
7. Click **Next**.
8. Click **Save**.

The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > Remote desktop** tab.

© 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.