Chrome browser extension

Contents

Secure access to SSH apps within the browser

January 23, 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.

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.
- 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
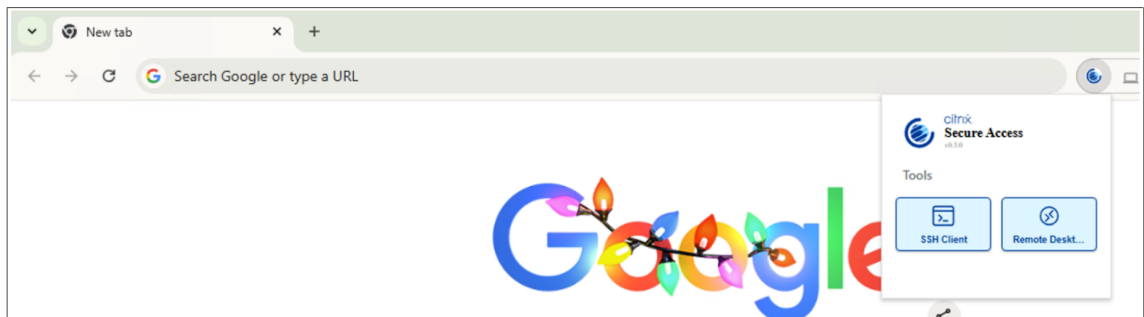- Hybrid deployment —Support for TCP/UDP apps

Access the SSH app

The SSH app access button is visible to the end-user in the extension UI irrespective of whether it is configured or not. If not configured, the user cannot access the SSH-based application.

- Type `CitrixSSH` and hit **tab** in the URL bar, then enter the IP address and hit **enter** to start an SSH session.
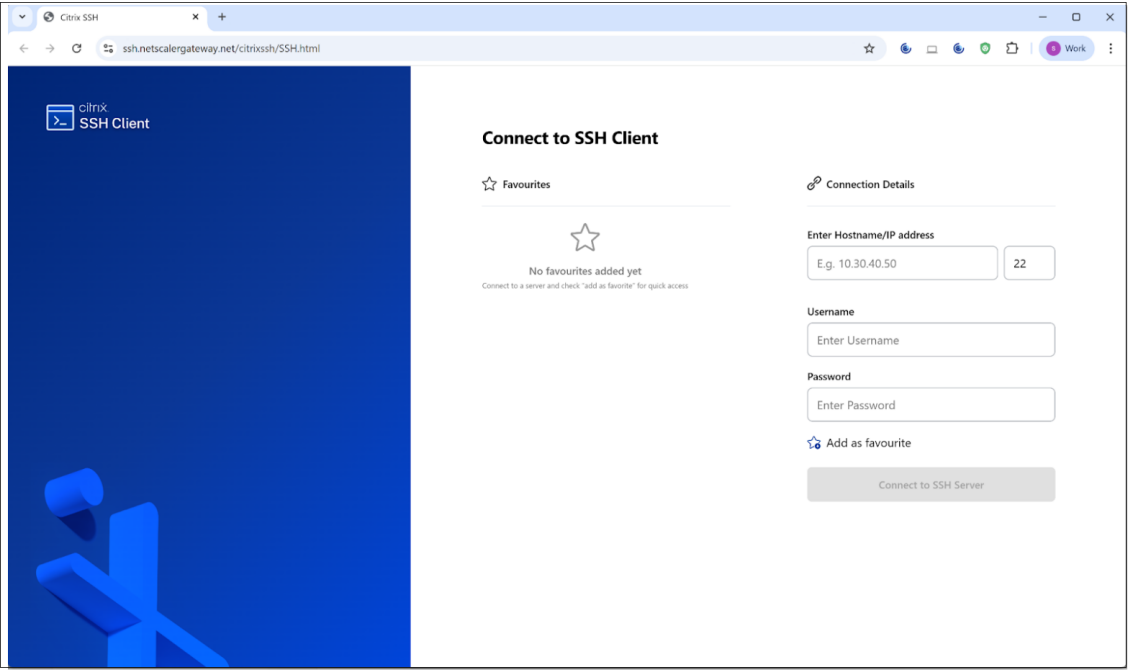

- Alternatively, you can click the extension icon and click **SSH** from the menu.
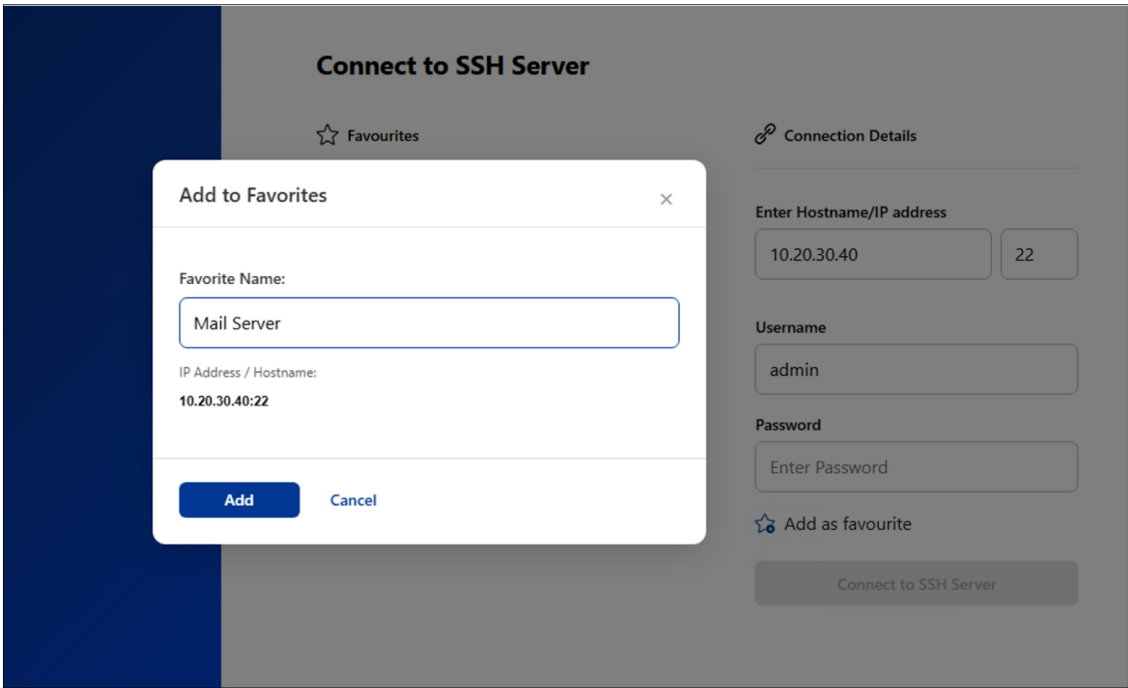

- Port 22 is filled in by default. You can choose to change the port number as required.

  > **Note:**
  >
  > Enter your user name and password. Only the user name and password-based authentication is supported.

- You can also save sessions as favorites.

Secure access to RDP apps within the browser

January 23, 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.
- **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

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

Access the RDP app

The RDP app access button is visible to the end-user in the extension UI irrespective of whether it is configured or not. If not configured, the user cannot access the RDP-based application.
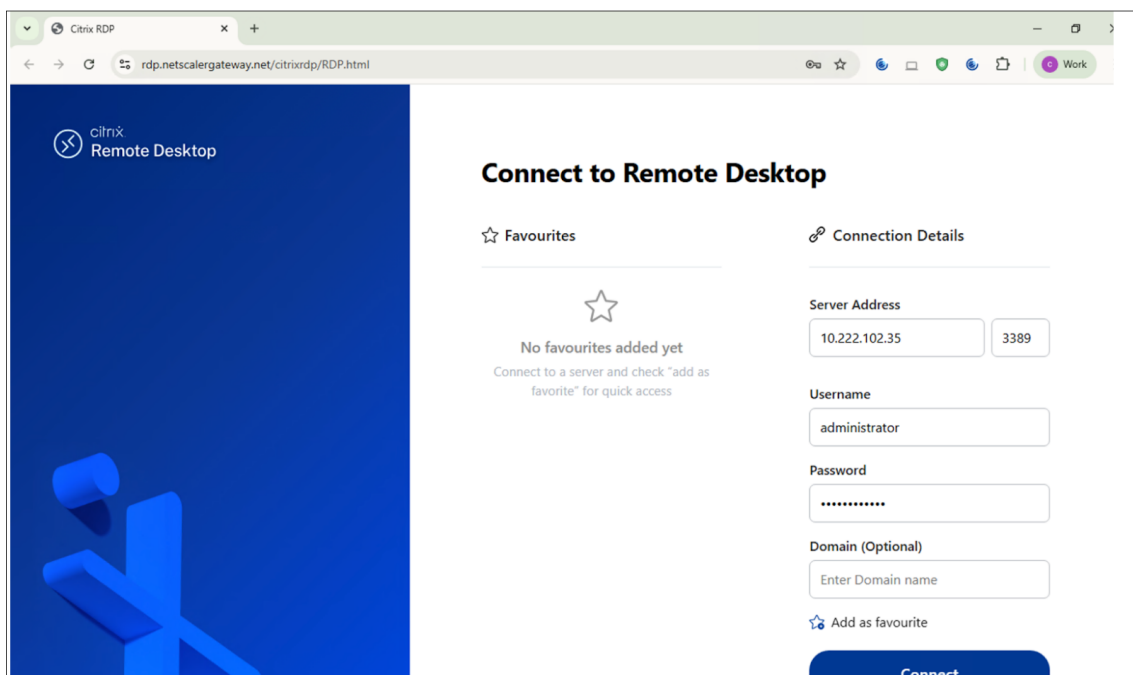
- Users can access the Remote Desktop app directly from the extension UI.

- Users are presented with a login screen to authenticate.

  > **Note:**
  >
  > Only the user name and password-based authentication is supported. You can also enter the domain name for the authentication.

- Users can save the frequently used Remote Desktop connections as favorites for quick access.

---

citrix
Remote Desktop

Connect to Remote Desktop

☆ Favourites

🔗 Connection Details

Add to Favorites   ✕

Favorite Name:

Mail Server 1

Server Address:

10.20.30.40:3389

Add   Cancel

Server Address

| 10.20.30.40 | 3389 |

Username

administrator

Password

••••••••••••••

Domain (Optional)

Enter Domain name

☆ Add as favourite

Connect