Citrix SecurAccess™ ZTNA Hybrid Deployment

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

Contents

Solution overview 13

- Why Use Citrix SecurAccess ZTNA 13
- Key components 14
  - Network diagram 14
- End user access methods 16
- Citrix Endpoint Analysis (EPA) client 16
- Limitations 17

What's new 18

- 27 October 2026 18
- 31 July 2026 18
- 27 April 2026 18
- 07 April 2026 19
- November 2025 19
- September 2025 21
- August 2025 21
- May 2025 22
- April 2025 22
- December 2024 23
- October 2024 23
  - Initial release 23

Known issues 30

System requirements and prerequisites 32

- Software version requirements 32
- Firewall requirements 32
- Prerequisites 35
  - NetScaler prerequisites 35

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

Chrome Enterprise Premium + Citrix SecurAccess™ deployment 35
Citrix SecurAccess only deployment 36
Cloud Connector prerequisites 36
StoreFront prerequisites 37
Citrix SecurAccess ZTNA prerequisites 37
Google prerequisites 37
Chrome Enterprise Premium license 37
Google Workspace Admin console 38
Google Chrome 39
Managed Chrome profiles 39
Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory 39
Bypass TLS inspection 40
Get Started with Citrix SecurAccess™ ZTNA hybrid deployment 41
Before you begin 41
Verify your Citrix SecurAccess ZTNA entitlement 41
Verify prerequisites 42
Choose the deployment mode 42
Next steps 42
Step 1: Set up Google Chrome Enterprise Premium 42
Google Chrome Enterprise Premium configuration 43
Step 2: Set up the first data center 45
Step 3: Configure and analyze 46
Download and run NetScaler and StoreFront scripts 46
NetScaler script 46
StoreFront script 48
Upload reports and analyze configuration 49
Complete onboarding and publish applications 51

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

Post-onboarding tasks 51
Configure applications 51
Configure access policies 51
Update the Chrome Enterprise Premium configuration 52
Synchronize the configuration 53
Access your applications (end users) 53
Accessing Web and SaaS applications 54
Accessing TCP/UDP (client/server) applications 55
Data regionalization 56
Supported deployments 56
Configuration 57
Limitations 57
Hybrid deployment setup components 58
Cloud Connector Configuration 58
Citrix SecurAccess™ ZTNA service 58
Port Configuration for Citrix SecurAccess ZTNA service 59
Citrix SecurAccess ZTNA load balancer 59
Configure TLS/SSL certificates for the Citrix SecurAccess ZTNA service on Cloud Connector 60
NetScaler 62
Configure authentication 62
Sample authentication configurations 63
Multifactor authentication with conditional authentication 63
Third-party integration with multifactor authentication 63
Device posture scans (EPA) 63
Miscellaneous scenarios 64
StoreFront 64
Configuring a new Store 64

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

Component Analyzer 65
Citrix SecurAccess ZTNA Analyzer 66
NetScaler Gateway Analyzer 67
StoreFront Analyzer 67
Integration with Google Chrome Enterprise Premium 69
Chrome Enterprise Premium advanced security features 69
Prerequisites for successful integration 70
Citrix SecurAccess ZTNA - Supported deployment modes 70
Legal 71
Admin roles and privileges 71
Google custom admin role privileges 72
Create and assign roles and privileges 74
Open ID Connect profile to use NetScaler Gateway as the IdP 74
Create a Google OIDC SSO profile 75
Bind the OIDC Profile (To either an OU or group) 77
Configure NetScaler as an OAuth IdP 78
Directory synchronization 78
Microsoft Entra ID using G Suite connector 78
Google Cloud Directory Sync (GCDS) tool 79
Active Directory 79
Google Cloud Directory Sync configuration 80
End user experience 89
Citrix SecurAccess™ extension for Chrome Enterprise Premium 91
Secure Access extension logs 92
Citrix SecurAccess controls for Chrome Enterprise 92
Supported controls 95
Users and groups in policies 95
Search for users or groups 95

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

Use synchronized users and groups 96
Anti-keylogging control 96
Prerequisites 97
Configure the anti-keylogging policy 97
Clipboard container control 98
Prerequisites 98
Enable Clipboard Container control 98
Enable Clipboard Sharing Scope 100
Domain suffix for web applications 102
Prerequisites 102
Configure DNS suffix 103
Session recording control 103
Architecture 104
Prerequisites 104
System requirements 104
Set up the environment 105
Browser session reauthentication control 106
Prerequisites 106
Enable Browser session reauthentication control 107
SSH control 108
Benefits of this integration 109
Use cases 109
System requirements 109
Prerequisites 110
Configure Citrix SecurAccess ZTNA for SSH access 110
Configure the SSH policy 110
Remote Desktop control 111
Benefits of this integration 112

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

Use cases 112
System requirements 112
Prerequisites 112
Configure Citrix SecurAccess ZTNA for RDP access 113
Configure the remote desktop policy 113
Troubleshoot CEP integration issues 114
Diagnostic logs for CEP troubleshooting 115
Confirm that user is logged in to the correct Chrome profile 115
Check Secure Enterprise Browser extension installed 116
Check ExtensionInstallForcelist policy 116
Troubleshoot conflicting extension install list policies 116
Check Secure Enterprise Browser Extension policy 117
Check user extension configuration within Google Admin Console 119
Check if routes are being fetched 119
Validate CEP integration in the Citrix SecurAccess ZTNA admin console 120
Troubleshoot Google Secure Gateway reachability 121
Confirm application inclusion in routes 121
Troubleshoot routed application access 122
Ensure IdP and Google Directory alignment 123
Check access settings for the group in Google Admin Console 123
Known issues with the CEP integration 123
Citrix SecurAccess ZTNA user interface 123
Adaptive access policy configuration 124
Google Chrome browser 124
Apps configuration and management 126
Configure enterprise web or SaaS applications 126
Automatic cleanup of routing entries on application deletion 129
Next steps 129

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

Discover related domains using a HAR file 129
Example 130
Prerequisites 130
Import a HAR file 130
Manage related domains 133
Validation and file requirements 134
Configure TCP/UDP apps 134
Next steps 137
Configure TCP/UDP - server to client apps 138
Edit an application 140
Next steps 140
Access policy configuration and management 141
Configure access policies for the applications 141
Configure access policies 142
Edit an access policy 143
Change access policy priority 144
Next steps 144
Policy conditions 144
User and user groups 144
Verify user and group synchronization 146
Network Location 146
Configure session policies 148
Device certificate enrollment 149
Device Posture service 154
Configure the device posture checks on NetScaler Gateway 154
Device Posture checks on on-premises NetScaler® Gateway 154
Entitlements 155
Enable Device Posture for Citrix SecurAccess ZTNA hybrid solutions 155

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

Manage settings 156
Manage settings 156
Application domains 156
Configuration report 157
Generate a configuration report 157
Manage setup configuration after installation 161
Reset Citrix SecurAccess™ ZTNA configuration 162
Upgrade 162
Advanced Citrix SecurAccess™ ZTNA features 164
Advanced data center configuration 165
Prerequisites 166
GSLB configuration CLI commands 166
References 167
Data centers setup and configuration 169
Global server load balancing connection proxy 169
Prerequisites 170
Configure GSLB connection proxy 170
Configure a global server load balancer domain URL 170
Configuration 171
Edit data center (optional) 172
Configure and analyze 173
Context-based application routing 173
Use case: Context-based routing 174
Steps to change the routing type 175
Use case: Route internal corporate users directly to back-end applications 176
Routing precedence 176
Supported Citrix SecurAccess™ clients 176
Example use case 176

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

Configure direct routing within the hospital network using session policies 177
Discover domains or IP addresses accessed by end users 178
Application Discovery for internal domains in a new environment 179
Create an application from the App discovery page 182
Update an existing application 183
Policy modeling tool 184
Configure Data Loss Prevention (DLP) policies 185
High availability deployments 185
High availability within the data center 186
NetScaler 186
Cloud Connectors (Citrix SecurAccess ZTNA servers) 186
StoreFront servers 188
Reset Citrix SecurAccess™ ZTNA configuration 188
Visibility and monitoring 189
Service entitlements 189
Supported clients 189
How to access Monitor 189
Session definitions 189
Web/SaaS app sessions 190
TCP/UDP app sessions 191
View user sessions 191
Application topology 193
Triage and troubleshoot 195
User/client issues in Citrix SecurAccess mode 195
User unable to log in 195
User unable to launch an app 196
Steps to collect a NetScaler support bundle with debug-level logging 197
Revert verbose logging 198

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

Tools that help to troubleshoot 198
Collect client logs 198
Chrome Enterprise Premium logs 198
Steps to capture logs for the Secure Enterprise Browser extension 198
Steps to capture logs for Citrix SecurAccess Extension 201
Real-time session troubleshooting using Monitor 201
Session codes 202
App enumeration message codes 202
App launch message codes 204
App launch error codes 205
End user experience 208
Accessing web and SaaS applications with Chrome Enterprise Premium 208
Option 1: Create a managed Chrome profile and access apps directly (recommended) 208
Option 2: Access store URL in existing Managed Chrome profile 210
Option 3: Access store URL from a non-managed Chrome profile or a non-Chrome browser (Edge, Firefox) 211
Option 4: Access apps through the Citrix Workspace app 212
Accessing client/server (TCP/UDP) applications 213
index 215
Integration with DaaS monitor 215
Service entitlements 215
Supported clients 215
How to access Monitor 215
Session definitions 215
Web/SaaS app sessions 216
TCP/UDP app sessions 217
View user sessions 217
Application topology 219

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

Contextual tags 221
Configure custom tags using the GUI 221
Configure a classic gateway preauthentication policy 221
Bind the custom tag to NetScaler Gateway 223
Configure custom tags using the CLI 224
Adding a new contextual tag 225
Note on EPA tags sent to Citrix SecurAccess ZTNA provider 225
Citrix SecurAccess™ ZTNA 225
Key capabilities of Citrix SecurAccess ZTNA 226

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

Solution overview

Citrix SecurAccess™ ZTNA for hybrid deployments provides a Zero Trust Network Access (ZTNA) solution that divides functions between your on-premises environment and Citrix Cloud. This architecture allows you to leverage existing investments while gaining cloud-based management. The responsibilities are distributed as follows:

- **On-premises components (data plane):** Your existing NetScaler Gateway, StoreFront, and Windows Cloud Connector installations remain on-premises. These components are responsible for controlling and routing all user access traffic.
- **Citrix Cloud components (control plane):**
  - Centralized management: Use the Citrix Cloud UI for all configuration, administration, and policy management.
  - Monitoring and troubleshooting: Utilize the hosted Citrix Monitor service for all monitoring, analytics, and troubleshooting functions.

Why Use Citrix SecurAccess ZTNA

Citrix SecurAccess ZTNA solution provides end-to-end access control by integrating single sign-on (SSO), remote access, and out-of-band content inspection into a unified platform.

- **Govern app access:** Enforce security policies and provide simplified SSO experience for all approved SaaS and internal applications.
- **Enhance security:** Protect the network and user devices from malware and data leaks by filtering access to specific websites and website categories.
- **Google Chrome Enterprise Premium integration:** Leverage Google Chrome Enterprise Premium, allowing users to natively access authorized corporate web apps with a familiar and secure experience. For details, see Integration with Google Chrome Enterprise Premium.
- **Data loss prevention (DLP):** Enforce granular controls to restrict printing, downloads, and clipboard copy-paste actions.
- **Analyse user activity and protect enterprise network:** Gain deep visibility into user activities, such as malicious website visits or risky file transfers. Use these analytics to take corrective actions and protect the enterprise network.

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

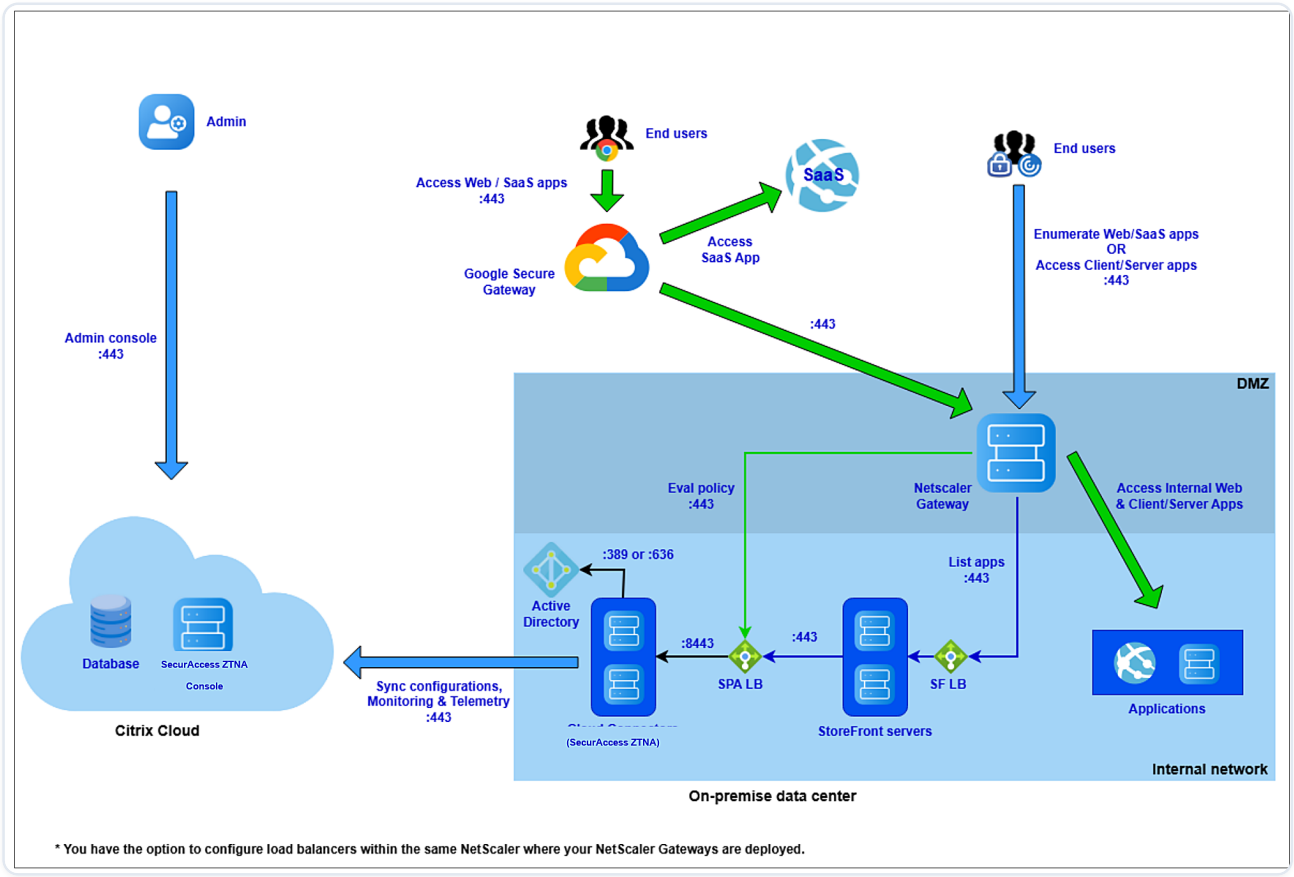
- **Seamless user experience:** Provide secure, seamless access to critical business applications from any device, location, or network.

Key components

The following sections provide more information about the key components of the Citrix SecurAccess ZTNA hybrid solution.

Network diagram

The following figure illustrates the network diagram of the Citrix SecurAccess ZTNA hybrid solution.



The key components of the Citrix SecurAccess ZTNA hybrid solution are:

- **Citrix SecurAccess ZTNA admin console:** Click the Citrix SecurAccess ZTNA tile in Citrix Cloud to access the admin console. Use the admin console to onboard, configure apps, and set policies. Site management is centralized and streamlined. No on-premises infrastructure required.
- **Google Chrome and Chrome Enterprise Premium Secure Gateway:** End users access corporate internal and SaaS applications using the Google Chrome browser.

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

The Chrome Enterprise Premium Secure Gateway functions as a forward proxy to enforce a zero-trust access framework. It provides granular, context-aware control over application access. All traffic from the user's Chrome browser connects to the NetScaler Gateway through the Chrome Enterprise Premium Secure Gateway, ensuring policies are applied before access is granted.

NOTE:

The Google components are required only when using Citrix SecurAccess ZTNA to provide secure access to SaaS and internal Web applications. They are not required if you plan to use Citrix SecurAccess ZTNA only for TCP/UDP (client/server) applications.

- **NetScaler Gateway:** The NetScaler Gateway component provides secure remote access to applications and desktops. It acts as the secure entry point for external users, allowing them to connect to corporate resources from outside the network. For details, see NetScaler.
- **Cloud Connector:** The Cloud Connector is an on-premises component, installed on a Windows server, that acts as a secure communication bridge between your network and Citrix Cloud.

  Cloud Connector is responsible for synchronizing all configurations and policies from the Citrix SecurAccess ZTNA service in the cloud. These policies are then used to enforce access rules for applications. The connector also persistently caches this data, which allows users to continue accessing applications even if Citrix Cloud becomes unavailable. For details, see Cloud Connector.
- **StoreFront:** The on-premises StoreFront is the user facing component that aggregates, enumerates, and delivers all authorized applications and desktops to end-users. It functions as an enterprise app store. This hybrid architecture allows you to leverage your existing StoreFront setup without migrating to the cloud. For details, see StoreFront.

NOTE:

StoreFront is optional if you plan to use Citrix SecurAccess ZTNA only for TCP/UDP (client/server) applications. If you do configure StoreFront, it only enumerates applications that are configured as a web application type. Standard TCP/UDP apps are not displayed in the store.

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

End user access methods

End users can access the Citrix SecurAccess ZTNA apps using any of the following methods:

- **Citrix Workspace App (CWA) and Workspace UI:** These are the two clients end users can use to connect and view Citrix Store.
  - **Citrix Workspace App (native client):** This is the full, native application installed on the user's endpoint (for example, Windows and macOS). It provides the richest user experience and is required for certain advanced features.
  - **Citrix Workspace UI (web client):** This is the browser-based version of the store. Users access it by navigating to the StoreFront URL in a web browser. It allows users to access their applications without installing any client software.
- **Google Chrome:** All web and SaaS applications are launched exclusively through the Google Chrome browser using a managed enterprise profile. When a user launches an application from their Citrix Store, it automatically opens in this managed Chrome Enterprise profile to enforce all security controls.

  NOTE:

  Google Chrome is not mandatory if you plan to use Citrix SecurAccess ZTNA only for TCP/UDP (client/server) applications. Users can use any browser (such as a non-managed Chrome, Edge, or Firefox) to access TCP/UDP applications.
- **Citrix SecurAccess (CSA) client:** This is the client-side agent, installed on the user's endpoint, that is required for ZTNA access to all TCP/UDP (client/server) applications.

  CSA provides secure, per-application connectivity to internal corporate resources without requiring a traditional, full-tunnel VPN.

Citrix Endpoint Analysis (EPA) client

The Citrix EPA client is a lightweight plug-in that runs on the user's endpoint to perform device posture scans (also known as EPA scans). This client is required only if you have configured access policies that check the endpoint's security posture (for example, up-to-date OS, specific antivirus software, or registry keys) before granting access.

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

Limitations

- EPA as a factor is not supported. Instead, you can use the Device Posture service. For more information about the Device Posture service, see Device Posture.
- Enabling device posture checks at virtual server level is not supported with Always On.
- Policy modeling supports only user conditions. Device posture and network location conditions are not supported.
- StoreFront analyzer supports only one Citrix SecurAccess ZTNA type Store in StoreFront.
- The simplified Citrix SecurAccess ZTNA user interface for hybrid deployments supports only one data center (one gateway and one StoreFront) in the current release.
- IPv6 is not supported for Network Locations in the Citrix SecurAccess client.

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

What's new

The following sections capture details about the new features and enhancements.

27 October 2026

- **Product rebranding:**

  Citrix Secure Private Access is now known as Citrix SecurAccess™ ZTNA.

31 July 2026

- **Citrix SecurAccess™ controls for Chrome Enterprise:**

  Citrix SecurAccess™ ZTNA supports security policies that are delivered to and enforced by the Citrix SecurAccess extension for Google Chrome Enterprise Premium (CEP).

  The following policies are supported by Citrix SecurAccess ZTNA.

  - Anti-keylogging
  - Clipboard container
  - Domain suffix for web applications
  - Session recording
  - Browser session reauthentication

27 April 2026

- **Advanced data center configuration**

  Citrix SecurAccess ZTNA hybrid deployment is now supported in a multi-data center with multi-sites configuration using NetScaler GSLB in active-active site deployment with site persistency method for GSLB connection proxy. For details, see Advanced data center configuration.

- **Support to configure a global server load balancer domain URL**

  To set up multi-site redundancy for Citrix SecurAccess ZTNA, you must configure a global server load balancer (GSLB) address. This address acts as a single entry point, routing users

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

to a specific data center's Citrix SecurAccess ZTNA gateway based on your traffic policies, such as static proximity. For details, see Configure a global server load balancer domain URL.

- **Global server load balancing connection proxy support**

  The global server load balancing (GSLB) connection enables NetScaler Gateway to transparently detect misrouted requests and proxy them to the correct site without any user intervention. For details, see Global server load balancing connection proxy.

07 April 2026

- **Context-based application routing**

  When an app is configured, routing types are defined for the application URL and its related domains or app destinations under app configuration. The routing type defined here applies to all users who have access to the app. However, there can be scenarios where admins want to route the same app differently based on user context. For example, an internal app URL or destination must be routed directly instead of via Citrix SecurAccess ZTNA when users are inside the corporate network. The Routing Exceptions configuration in the access policies allows admins to edit the routing type for users or machines that match the conditions defined in the policy. For details, see Context-based application routing.

- **Secure access to SSH and RDP applications within the browser**

  Citrix SecurAccess ZTNA is integrated with Chrome Enterprise Premium to enable secure SSH and RDP sessions directly within the browser. For details, see the following topics:

  - Secure access to SSH apps within the browser
  - Secure access to RDP apps within the browser

November 2025

- **Simplified onboarding journey**

  The Citrix SecurAccess ZTNA for hybrid deployments onboarding interface is now significantly simplified to streamline the configuration process for all components. The enhanced user interface now features an intuitive topology view that displays step-by-step configuration status for each component. This visual approach enables administrators to quickly understand the deployment state, identify the configuration steps are complete, and determine actions that are still pending, thereby reducing setup time and minimizing configuration errors.

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

Also, the SecurePrivateAccessProfile is supported in NetScaler to simplify the NetScaler Gateway configuration for the hybrid deployment.

For details, see Get Started with Citrix SecurAccess ZTNA hybrid deployment.

- **Google Chrome Enterprise Premium support**

  With the integration of Citrix SecurAccess ZTNA service with Google Chrome Enterprise Premium, end users can now securely access private Web/SaaS applications using the Google Chrome browser as their enterprise browser, and achieve per-application access with data loss prevention (DLP) controls, web filtering, and ZTNA policy enforcement.

  For details, see Integration with Google Chrome Enterprise Premium

- **Analyzer to verify and identify configuration issues in components**

  Component Analyzer is a web-based tool that performs the configuration checks required for a Citrix SecurAccess ZTNA hybrid setup. After uploading the necessary reports, the Analyzer identifies issues with detailed error messages and explanations, including examples of detected StoreFront configuration errors. The tool also lists potential remediations to resolve the identified problems.

  For details, see Component Analyzer.

- **Support for launching apps from StoreFront UI using NetScaler Gateway URL**

  End users can now seamlessly launch applications directly from the StoreFront user interface by accessing the NetScaler Gateway URL.

  For details, see Accessing Web and SaaS applications.

- **Network Location Service condition support in access policies**

  The Network Location Service (NLS) is a policy condition that allows you to restrict access based on the user's network location. An admin can configure the access policy based on the location from where the user is accessing the application. The location can be the country from where the user is accessing the application or the user's network location. The network location is defined using an IP address range or subnet addresses.

  For details, see Network Location.

- **Configuration reports**

  Customer administrators can now generate configuration reports to gain insights into the Citrix SecurAccess ZTNA setup.

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

For details, see Configuration report.

September 2025

- **Citrix SecurAccess ZTNA hybrid deployments support for iOS devices**

  Citrix SecurAccess ZTNA hybrid deployments are now supported for mobile devices starting with Secure Access Client version 25.08.1 for iOS. Mobile users can access corporate applications from their iOS devices.

  IMPORTANT:

  For Citrix SecurAccess ZTNA support with Citrix SecurAccess for the iOS platform, you must also add the string "NSGiOSplugin" in the HTTP "User-Agent" header.

  Example: `add vpn sessionPolicy PL_OSspahybrid "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") && (HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NSGiOSplugin\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixSecureAccess\"))" AC_OSspahybrid`
  For details, see the following topics:

  - NetScaler configuration
  - Citrix SecurAccess ZTNA for mobile device.

August 2025

- **Generate Citrix SecurAccess ZTNA site configuration reports**

  Customer administrators can now generate configuration reports to gain insights into the Citrix SecurAccess ZTNA site's setup. The configuration reports can be used in the following scenarios:

  - Identify and resolve configuration issues.
  - Share with the Citrix Support team for investigation and troubleshooting purposes.
  - Use the report as a reference to set up new sites or modify existing site details.
  - **Additional dashboard widgets**

  The Citrix SecurAccess ZTNA dashboard for hybrid deployments is now enhanced to include the following widgets to provide deeper insights and improved monitoring:

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

- Device Posture logs
- Connector status
- Top applications by launch count
- Top discovered applications by total visits
- Top access policies by enforcement

For more information, see Visibility and monitoring.

May 2025

- **Integration of Citrix SecurAccess ZTNA with Google Chrome Enterprise Premium**

  The integration of Citrix SecurAccess ZTNA with Google Chrome Enterprise Premium enables customers to use Google Chrome Enterprise Premium as the enterprise browser solution for secure access to private web apps and SaaS applications along with secure connectivity provided by Citrix SecurAccess ZTNA. For details, see Integration of Citrix SecurAccess ZTNA with Google Chrome Enterprise Premium.

April 2025

- **Device Posture checks on on-premises NetScaler® Gateway**

  Citrix Device Posture checks can now be configured to work with on-premises NetScaler Gateway. This integration allows administrators to evaluate the security posture of devices attempting to access network resources and ensure that only trusted devices can access corporate resources.

  For details, see the following topics:

  - Device Posture
  - Device Posture checks on on-premises NetScaler Gateway
  - Citrix Device Posture service for NetScaler Gateway authentication

- **Key-based authentication for StoreFront™ to Citrix SecurAccess ZTNA communication**

  A security key-based authentication method is introduced for StoreFront to Citrix SecurAccess ZTNA communication. Key based authentication is enabled by default for the new customers whereas it is disabled for the existing customers. Existing customers must enable the security key and run the StoreFront configuration script again. For details, see Configure StoreFront.

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

- **Support for Web/SaaS apps in ICA Proxy mode**

  The ICA Proxy mode now supports enumeration and launching of Web/SaaS applications. This also enables the use of the new StoreFront UI to enumerate apps.

The ICA Proxy mode support is only available in NetScaler Gateway release 14.1 build 43.x and later. For details on configuration, see NetScaler configuration.

- **Enforce application rules based on the machine's context**

  You can now enforce application access rules based on the machine's context in addition to the user's context. You can select the machine or user context when creating an access policy. For details, see Configure access policies for the applications.

- **Exclude domains from being tunneled through NetScaler Gateway**

  You can now configure domains that can be excluded from being intercepted and tunneled through NetScaler Gateway. You can set the application connectivity type as Internal or External to allow or exclude domains from being intercepted and tunneled respectively. For details, see Configure TCP/UDP apps.

- **DNS over TCP support for Citrix SecurAccess ZTNA hybrid deployments**

  DNS over TCP is now supported for Citrix SecurAccess ZTNA hybrid deployments. The application FQDNs can now be resolved using TCP.

December 2024

- **Support for Citrix SecurAccess ZTNA hybrid solution on FIPS platform**

  The Citrix SecurAccess ZTNA hybrid solution is now supported on NetScaler platforms that comply with Federal Information Processing Standards (FIPS) and running the 13.1–37.219 and later FIPS builds. For more information, see Federal Information Processing Standards.

October 2024

The following sections provide more information about October 2024.

Initial release

Citrix SecurAccess ZTNA for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway

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

components and use Citrix Cloud™ for managing the configuration, administration, and monitoring functions.

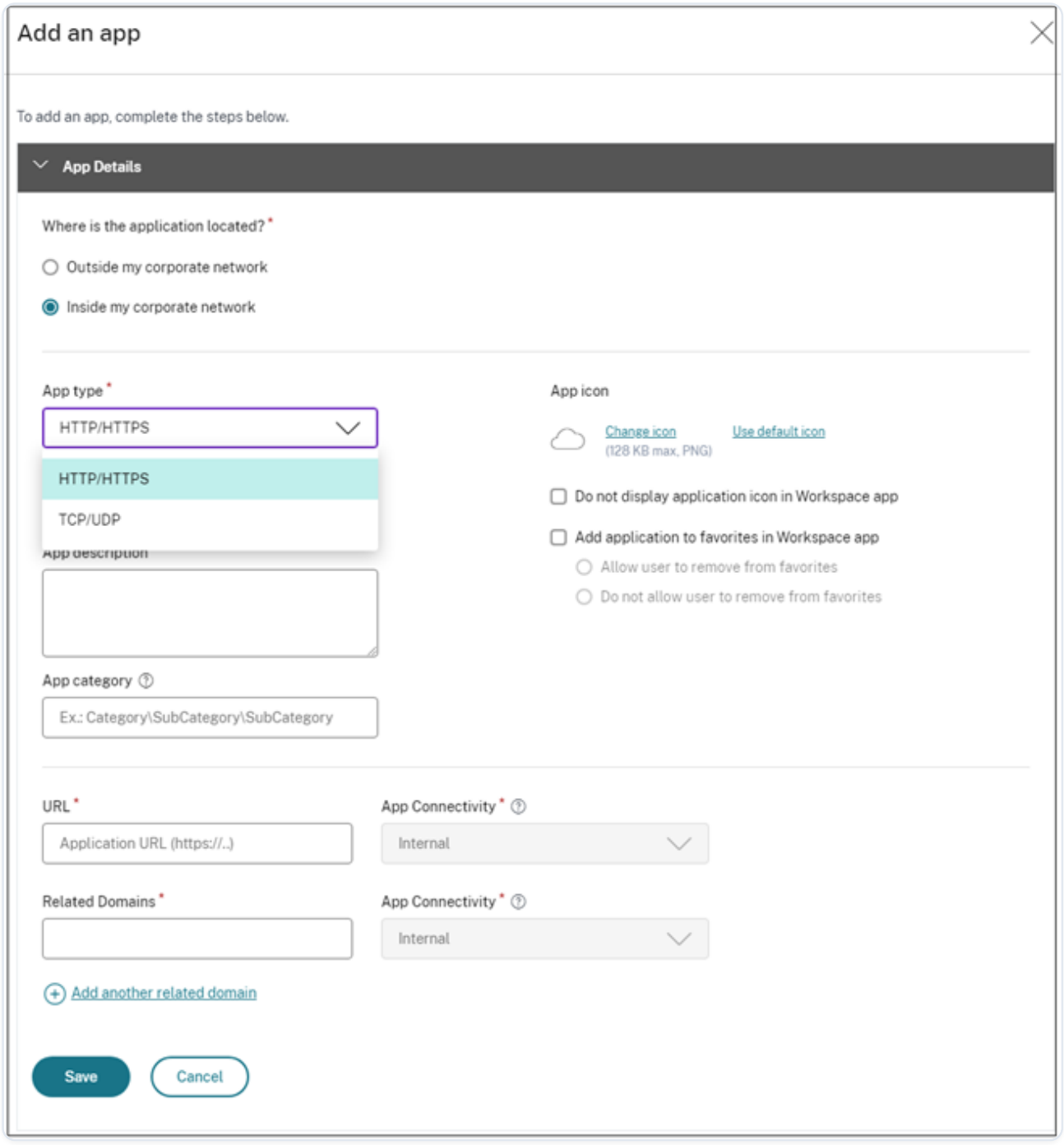
The following are some of the key features of the Citrix SecurAccess ZTNA for hybrid deployment.

- **Web/SaaS and TCP/UDP support:**

  Citrix SecurAccess ZTNA for hybrid deployment supports Web/SaaS and TCP/UDP apps. For details, see the following topics:

  - System requirements and prerequisites.
  - Configure Web/SaaS applications
  - Configure TCP/UDP apps

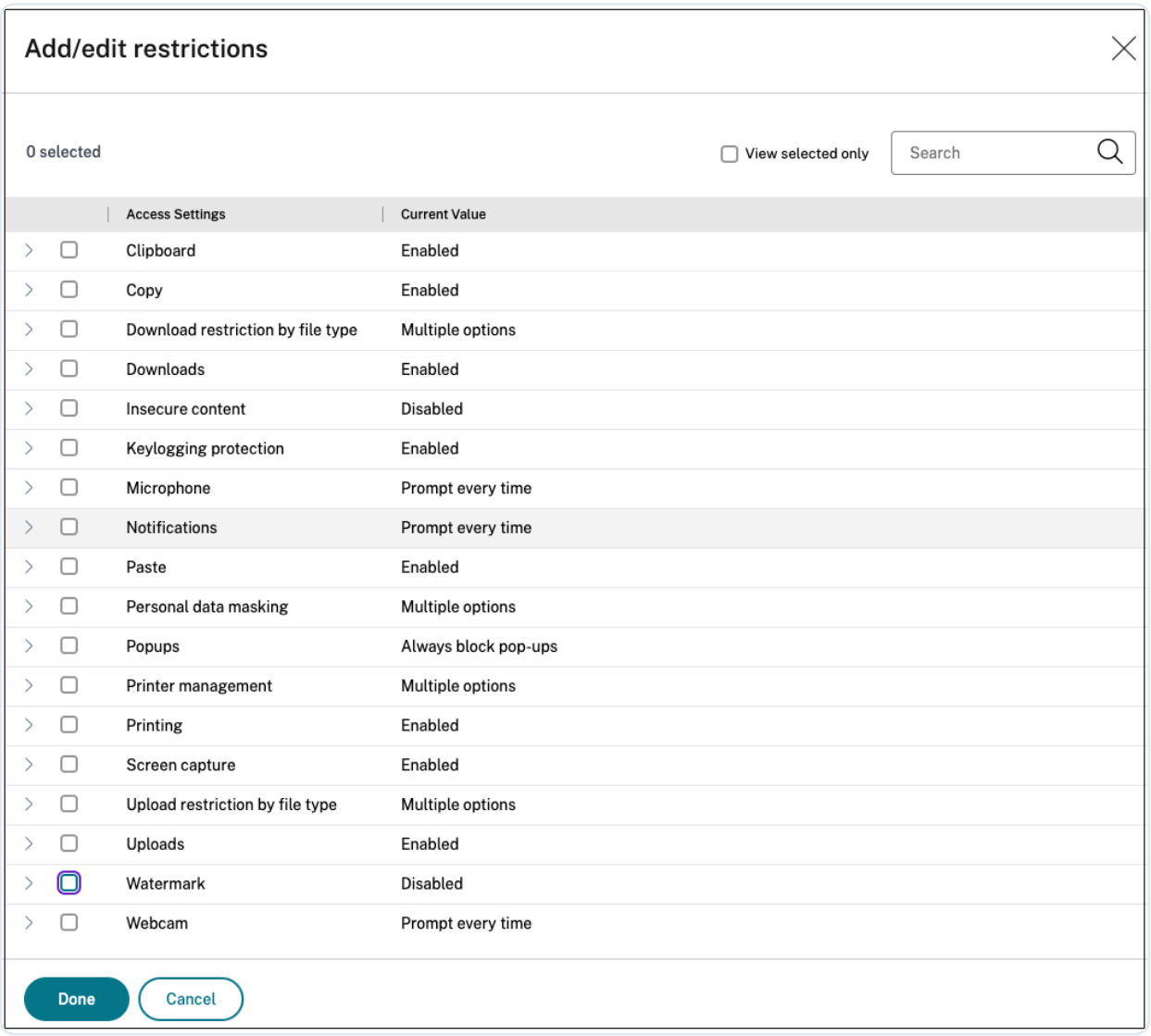
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Enhanced access restriction options:**

  While creating access policies for applications, you can select access restrictions that must be enforced on the applications. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. For details, see Configure access policies.

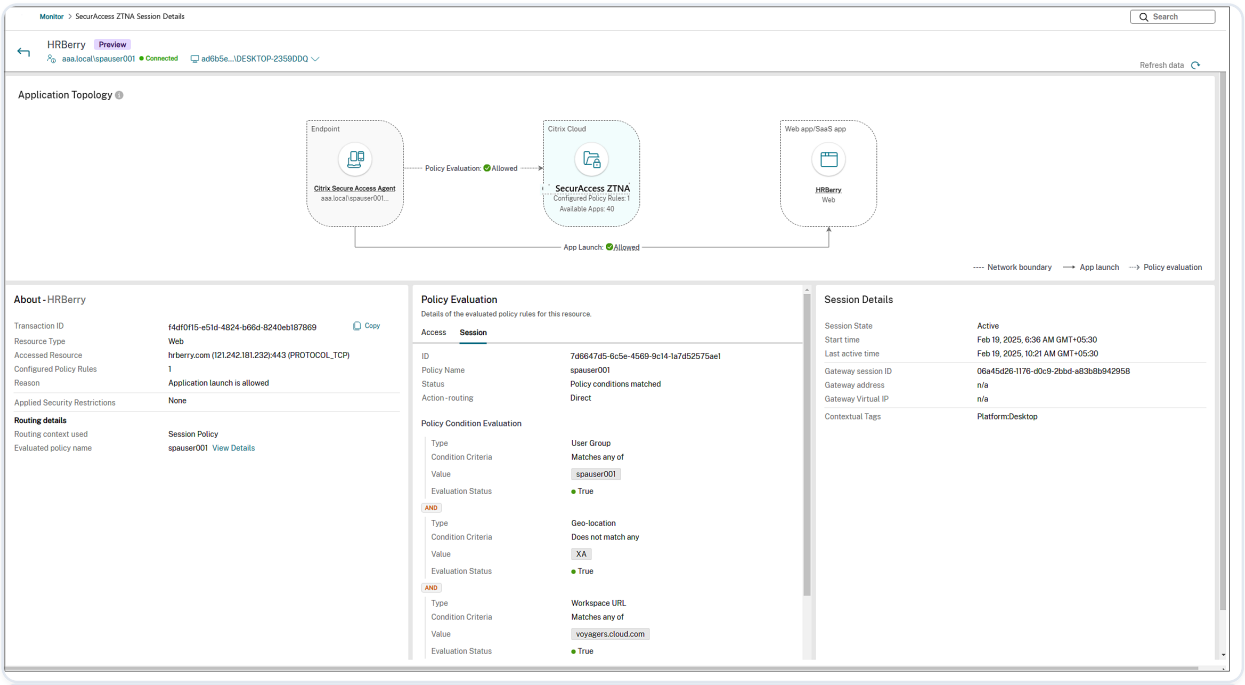
© 1997–2026 Citrix Systems, Inc. All rights reserved.

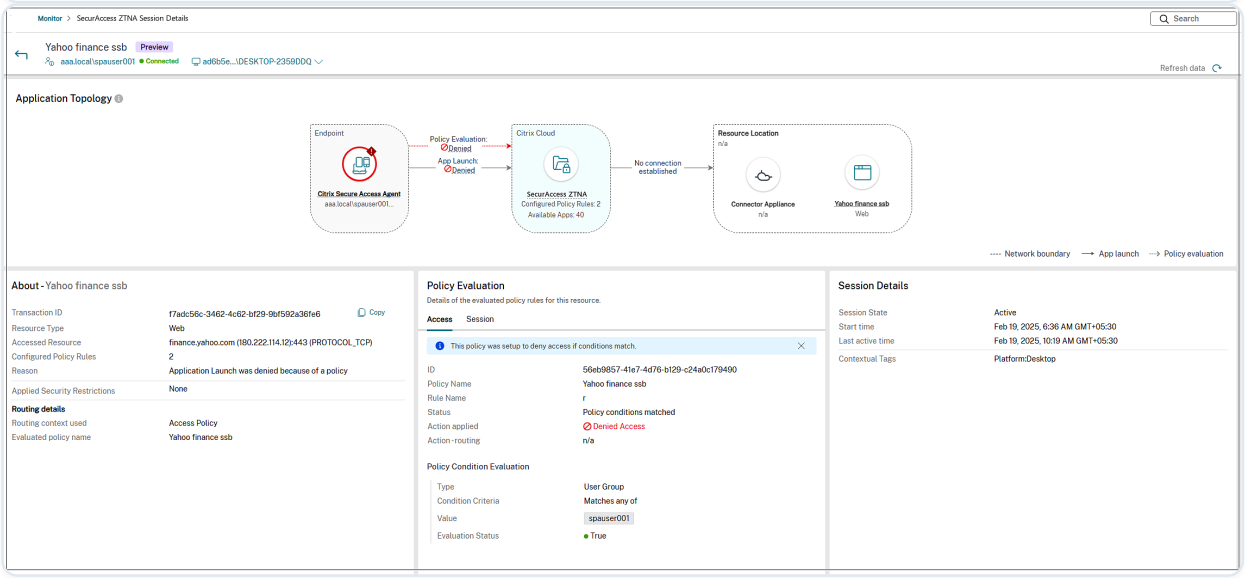


- **Citrix SecurAccess ZTNA integration with DaaS Monitor:**

  Citrix SecurAccess ZTNA is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor. For details, see Citrix SecurAccess ZTNA integration with DaaS monitor.

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

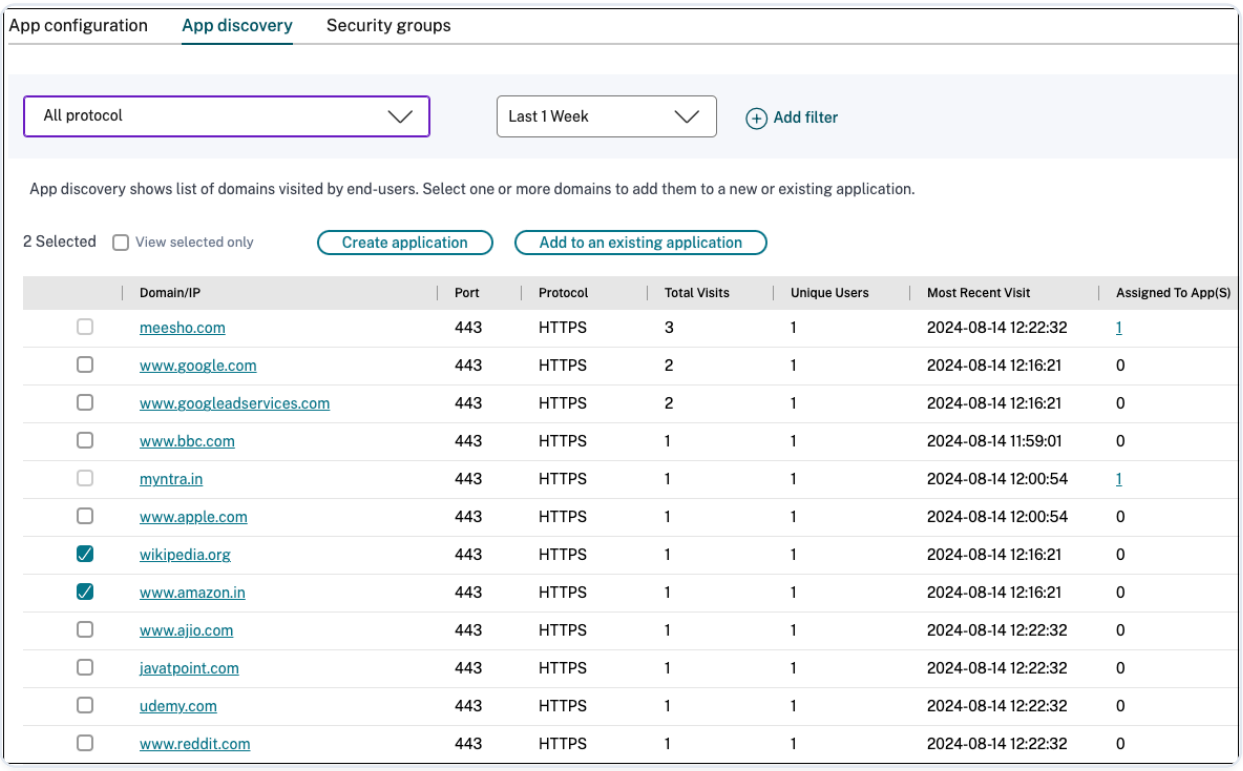




- **Application Discovery:**

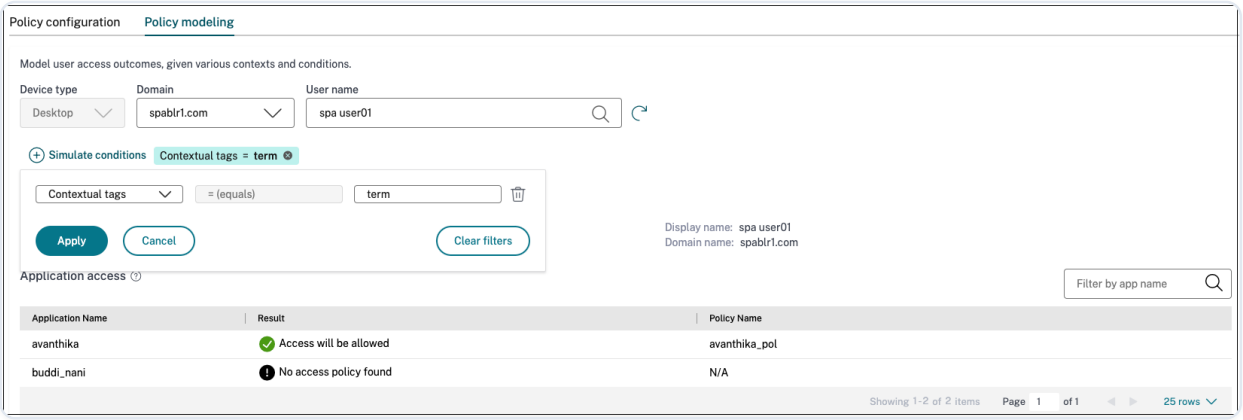
  The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users. For details, see Discover domains or IP addresses accessed by end users.

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



- **Policy modeling tool:**

  The policy modeling tool **(Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.

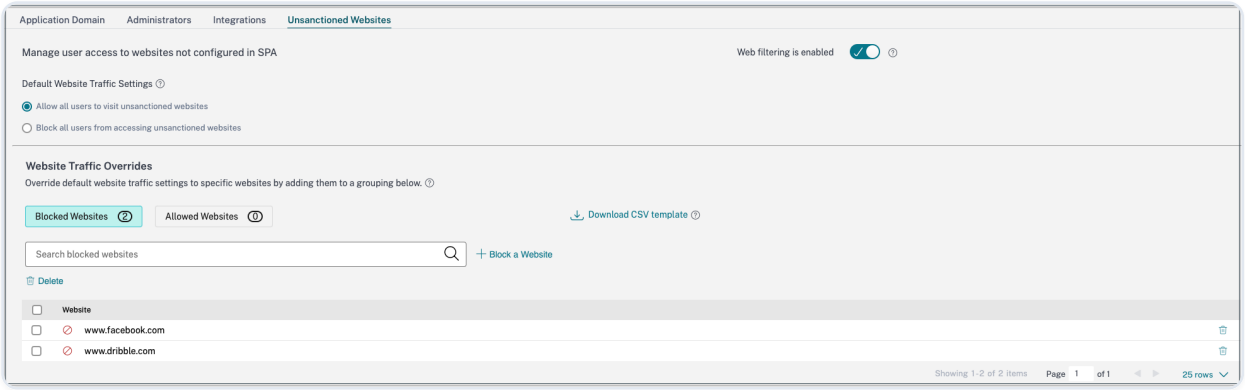


- **Support for Unsanctioned websites:**

  Applications (intranet or internet) that are not configured within Citrix SecurAccess ZTNA are regarded as “Unsanctioned Websites”. By default, Citrix SecurAccess ZTNA denies access to all intranet web applications if there are no applications and access policies configured for those applications. For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin

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

console to allow or deny access via Citrix Enterprise Browser. For details, see Unsanctioned websites.



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

Known issues

The following known issues exist in the Citrix SecurAccess™ ZTNA for hybrid deployments in the 2511 release.

- App launches from Citrix Workspace app or web-based user interface prompts for proxy login.

  Workaround: Cancel the prompt to continue with app launch.

- On the first app launch from Citrix Workspace app or the web-based user interface without a Chrome profile, the app does not open in the Chrome browser after the profile is added.

- If NetScaler is added as an IdP for OIDC under Third Party SSO in Google Cloud Identity, users are unable to sign in to the Chrome profile after signing out either explicitly or due to a session timeout.

  Workaround: The managed profile must be removed and re-added.

- In Citrix SecurAccess ZTNA hybrid CEP deployment, the mTLS handshake between the CEP proxy and Citrix SecurAccess ZTNA proxy fails when SSL default profile or cipher group is enabled.

- Policy changes on Network Location service condition (adding or removing a location tag) fail on update.

- When configuring Citrix Enterprise Premium, if the Google customer changes, incorrect validation and unclear error message is displayed.

- The Policy modeling tool does not display the apps from a disabled policy.

- The Application Launch count chart in the Citrix SecurAccess ZTNA dashboard does not display the SaaS apps launch count.

- The Application Launch count chart in the Citrix SecurAccess ZTNA dashboard does not display all launched apps for a given time frame.

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

- Web app launches from Citrix Receiver for Linux display an AM_ERROR_UNEXPECTED prompt.
- You cannot add conditions for a machine-based policy from the access policy user interface (**Citrix SecurAccess ZTNA > Access Policies)**.
- Device Posture with SAML is not supported in an nFactor authentication flow.
- Special characters (#, @, !, \^, &, %) are not allowed in the Client Secret field while configuring the OAuth IdP profile on NetScaler.
- The Citrix SecurAccess client for Linux doesn’t work if the client certificate authentication is configured in the NetScaler Gateway.
- The Citrix SecurAccess client for Linux cannot tunnel the applications if the app FQDN ends with “.local”.
- First-time app launches intermittently show the error message ‘Service Unavailable...’ in a managed profile.
- If data loss prevention (DLP) is configured, app access is allowed by the Citrix SecurAccess client.

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

System requirements and prerequisites

The following sections provide more information about system requirements and prerequisites.

Software version requirements

The following software versions are required for the Citrix SecurAccess™ ZTNA hybrid configuration:

- **NetScaler:** 14.1–66.54 and later
- **StoreFront:** 2507 LTSR CU1 or 2511 CR and later
- **Cloud Connector:** 6.141.0 / 4.420.200 and later

The following minimum software versions are required on the end user devices:

- **For web/SaaS applications:**
  - Google Chrome: 142
  - Citrix Workspace app for Windows: 2507.1 LTSR or 2508
  - Citrix Workspace app for Mac: 2508.10
- **For TCP/UDP applications:**
  - Citrix SecurAccess for Windows: 25.5.1.15
  - Citrix SecurAccess for Mac: 25.11.1.1
- **For endpoint analysis (EPA):**
  - EPA client for Windows: 25.10.1.7
  - EPA client for Mac: 25.10.3

Firewall requirements

The following firewall requirements assume that the standard HTTPS port 443 is used for StoreFront servers and the StoreFront load balancer. If a non-standard port is used, adjust the port settings accordingly.

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

SOURCE	SOURCE IP	DESTINATION	PROTOCOL	PORT	DESCRIPTION
Internet	Any	NetScaler Gateway	TCP	443	-
StoreFront servers	StoreFront server machine IP address	Citrix SecurAccess ZTNA load balancer	TCP	443	-
Cloud Connector	Cloud Connector machine IP address	Active Directory	TCP	389 or 636	-

If same NetScaler contains gateway and load balancers for StoreFront and Citrix SecurAccess ZTNA configurations:

SOURCE	SOURCE IP	DESTINATION	PROTOCOL	PORT	DESCRIPTION
NetScaler	NetScaler Subnet IP (SNIP) address	StoreFront servers	TCP	443	-
NetScaler	NetScaler Subnet IP (SNIP) address	Cloud Connector	TCP	8443	Assuming the default port is used for Citrix SecurAccess ZTNA
NetScaler	NetScaler Subnet IP (SNIP) address	NetScaler outbound proxy	TCP	Depends on the outbound proxy port	-
NetScaler	NetScaler Subnet IP	Backend applications (Web app or	Depends on the back-end	Depends on the back-end	-

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

SOURCE	SOURCE IP	DESTINATION	PROTOCOL	PORT	DESCRIPTION
	(SNIP) address	client/server apps)	application protocol	application port	

If different NetScalers are used for gateway and load balancers for StoreFront and Citrix SecurAccess ZTNA configurations:

SOURCE	SOURCE IP	DESTINATION	PROTOCOL	PORT	DESCRIPTION
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	StoreFront Load balancer	TCP	443	-
StoreFront load balancer	StoreFront load balancer IP address	StoreFront servers	TCP	443	-
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	Citrix SecurAccess ZTNA load balancer	TCP	443	-
Citrix SecurAccess ZTNA load balancer	Citrix SecurAccess ZTNA load balancer IP	Cloud Connectors	TCP	8443	Assuming the default port is used for Citrix SecurAccess ZTNA
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	NetScaler outbound proxy	TCP	Depends on the outbound proxy port	-
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	Backend applications (Web app or	Depends on the backend application protocol	Depends on the back-end	-

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

SOURCE	SOURCE IP	DESTINATION	PROTOCOL	PORT	DESCRIPTION
		client/server apps)		application port	

Prerequisites

To ensure optimal integration between the Citrix Workspace™ application and Chrome Enterprise Premium, the following prerequisites must be met. Successful completion of these prerequisites results in a more efficient and seamless experience when launching applications from the Citrix Workspace app or the web-based user interface.

NetScaler prerequisites

The following sections provide more information about NetScaler prerequisites.

Chrome Enterprise Premium + Citrix SecurAccess™ deployment

- Ensure that a NetScaler Gateway exists with the required settings for Citrix Desktop as a Service (DaaS). This NetScaler Gateway is used to enumerate Citrix SecurAccess™ ZTNA apps and DaaS apps in Citrix Workspace App/Citrix Receiver for Web.
    - To create Gateway using the wizard, see Setting up NetScaler for Citrix Virtual Apps and Desktops.
    - To set up NetScaler Gateway, see How to configure NetScaler.
- Ensure that a new public IP address and the corresponding private IP address exist for the new fully qualified domain name (FQDN). The public IP must be NATed to the private IP. This information is used to configure a new NetScaler Gateway for Citrix SecurAccess ZTNA apps. This Gateway FQDN is used to access private web apps using a managed Chrome profile. End users can also connect to the gateway using this FQDN from Citrix SecurAccess client to access internal apps. This private IP address must be used in the **Internal IP address** field in the UI. For more information, see Get started with Citrix SecurAccess ZTNA hybrid deployment.
- Ensure that you have an SSL server certificate for the NetScaler Gateway. The certificate must include the necessary Fully Qualified Domain Names (FQDNs), including the FQDN for the new Citrix SecurAccess ZTNA NetScaler Gateway. See NetScaler configuration for the relevant configuration details.

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

- Ensure that an authentication profile is configured on NetScaler. You can use an existing authentication profile and the corresponding authentication virtual server as well. See Configure authentication for details.

NOTE:

For using NetScaler Gateway as an IdP for Google OIDC, see Open ID Connect profile to use NetScaler Gateway as the IdP.

Citrix SecurAccess only deployment

- A new public IP address and the corresponding private IP address must exist for the new fully qualified domain name (FQDN). The public IP must be NATed to the private IP address. This information is used to configure a new NetScaler Gateway for Citrix SecurAccess ZTNA apps. This gateway FQDN is used to access private web apps using a managed Chrome profile. End users can also connect to the gateway using this FQDN from Citrix SecurAccess client to access internal apps. This private IP address must be used in the **Internal IP address** field in the UI. For more information, see Get started with Citrix SecurAccess ZTNA hybrid deployment.
- You must have an SSL server certificate for the NetScaler Gateway. The certificate must include the necessary Fully Qualified Domain Names (FQDNs), including the FQDN for the new Citrix SecurAccess ZTNA NetScaler Gateway. See NetScaler configuration for the relevant configuration details.
- Ensure that an authentication profile is configured on NetScaler.

  Existing authentication profile and the corresponding authentication virtual server can also be used.

  See Configure authentication to create a new authentication profile.

Cloud Connector prerequisites

- Ensure that the Citrix SecurAccess ZTNA service is enabled on the Cloud Connector. Reach out to Citrix Support if you need help.
- Ensure that the outbound calls to Connector Common and Citrix SecurAccess ZTNA FQDNs are allowed from Cloud Connectors on port 443. For more details, see System and Connectivity Requirements for Cloud Connectors.

See Cloud Connector configuration for details.

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

StoreFront prerequisites

- Ensure that a Store is created on StoreFront with enabled remote access (NetScaler Gateway is configured). See StoreFront documentation.
- Add Citrix SecurAccess ZTNA as a site in your StoreFront store:
  - Open your store and select **Manage Sites**.
  - Click **Add Site**, choose **Citrix SecurAccess ZTNA** as the type, and enter the display name and the Citrix SecurAccess ZTNA load balancer FQDN.

NOTE:

StoreFront is optional if you are using Citrix SecurAccess ZTNA only for TCP/UDP (client/server) applications.

See StoreFront Configuration for details.

Citrix SecurAccess ZTNA prerequisites

- Ensure that a Windows Cloud Connector inbound rule allows port 8443 from the data center network. Citrix SecurAccess ZTNA exposes a plain HTTP service at port 8443.
- Ensure that the internal load balancer for Citrix SecurAccess ZTNA targets the Cloud Connector backend on port 8443.
- Ensure that an SSL Bridge or SSL Offload is configured on the internal load balancer for Citrix SecurAccess ZTNA.

See Citrix SecurAccess ZTNA service for details.

Google prerequisites

The following sections provide more information about Google prerequisites.

Chrome Enterprise Premium license

Ensure that you have an active Chrome Enterprise Premium license, available through the Citrix Cloud Platform License (CPL) program.

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

Google Workspace Admin console

- **Google customer ID:** Obtain your Google Customer ID from the Google Admin console. This ID is required to configure Google services and integrations. Your customer ID can be retrieved through **Account > Account Settings** in the Google Admin console.
- **Create a custom role in the Google Admin console:** To onboard customers to Chrome Enterprise Premium (CEP) and enable Google Chrome integration, admins must create a custom role and assign the appropriate privileges in the Google Admin console. For details, see Admin roles and privileges.
- **Proxy mode configuration:** Set the proxy mode to Allow user to configure proxy. Avoid restrictive options such as No proxy, OS proxy, or Use this proxy only.

  NOTE:

  If the Google Admin console is set to use system proxy settings, the managed profile cannot apply the required proxy configuration for Citrix SecurAccess ZTNA, and the integration with Chrome Enterprise Premium fails.

- **Restrict DevTools extensions:** Chrome DevTools for force-installed extensions must be disabled to prevent exposure of sensitive data. This is the default option in the Google Admin console.
- **Access restrictions are now configured in Google Admin console for Chrome Enterprise Premium:** Access restrictions that were previously configured in the Citrix SecurAccess ZTNA console only apply to Citrix Enterprise Browser. When Google Chrome is the enterprise browser, access restrictions must be configured as policies and rules in the Google Admin console.
  - Policies are configured in the **Google Admin console > Devices > Chrome > Settings**. These settings allow you to manage browser settings, such as block JavaScript and allow list of printers.
  - Rules are configured in **Google Admin console > Rules**. These rules are advanced settings related to DLP, such as adding a watermark, blocking the download of files with social security numbers, and URL filtering.

  For details on creating policies and rules in the Google Workspace Admin console, see the following topics:

  - Set Chrome Enterprise connector policies for Chrome Enterprise

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

    - Data protection rules

- **License:** Ensure that you have an active Chrome Enterprise Premium license, available through the Citrix Cloud Platform License (CPL) program.

Google Chrome

The following sections provide more information about Google Chrome prerequisites.

Managed Chrome profiles

All end users must access Chrome using a managed profile. Managed profiles ensure that Chrome policies, extensions, and security settings are enforced on user devices.

Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory

You must synchronize the user directory configured in Citrix Workspace or StoreFront with the Google Cloud user directory. Specifically, the following user directories are supported:

- Active Directory
- Microsoft Entra ID (previously known as Azure Active Directory)

NOTE:

Synchronize the user directory periodically to ensure that application access is appropriately enforced.

Populate Email Address fields (mandatory)

The Google Cloud user directory requires the email address field to be populated. To be synchronized with the Google Cloud user directory, a user or group object in Citrix SecurAccess ZTNA must have an email address. Otherwise, the synchronization fails.

Ensure that all users that require access to the integrated Chrome Enterprise Premium and Citrix SecurAccess ZTNA offering, as well as all groups involved in access security policies, have the email address field populated. The email address domain part must be a domain that is configured and verified in your Google Admin console.

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

Active Directory sync

You must synchronize your AD with the Google Cloud user directory to ensure seamless integration and consistent user management across your enterprise using the Google Cloud Directory Sync.

For details on how to sync your AD with Google Cloud to include custom AD fields under the custom schema “Citrix-schema”, see Connect Google Cloud Identity as an identity provider to Citrix Cloud.

Microsoft Entra ID

You must synchronize your Microsoft Entra ID with the Google Cloud user directory for user and group management across both Google and Microsoft cloud platforms. For details, see Get started with Directory Sync.

For more information, see Google Directory sync.

Bypass TLS inspection

To ensure that Chrome Enterprise Premium endpoints function correctly on networks employing TLS inspection (or SSL inspection), you must exclude the following hostnames from inspection.

- `ingress.cloudproxy.app`
- `securegateway.goog`
- `*.securegateway.goog`

This exclusion is essential because many TLS inspection solutions (such as SSE vendors or proxy servers) do not fully support the HTTP CONNECT method used by Chrome Enterprise Premium, which can result in traffic being abruptly dropped.

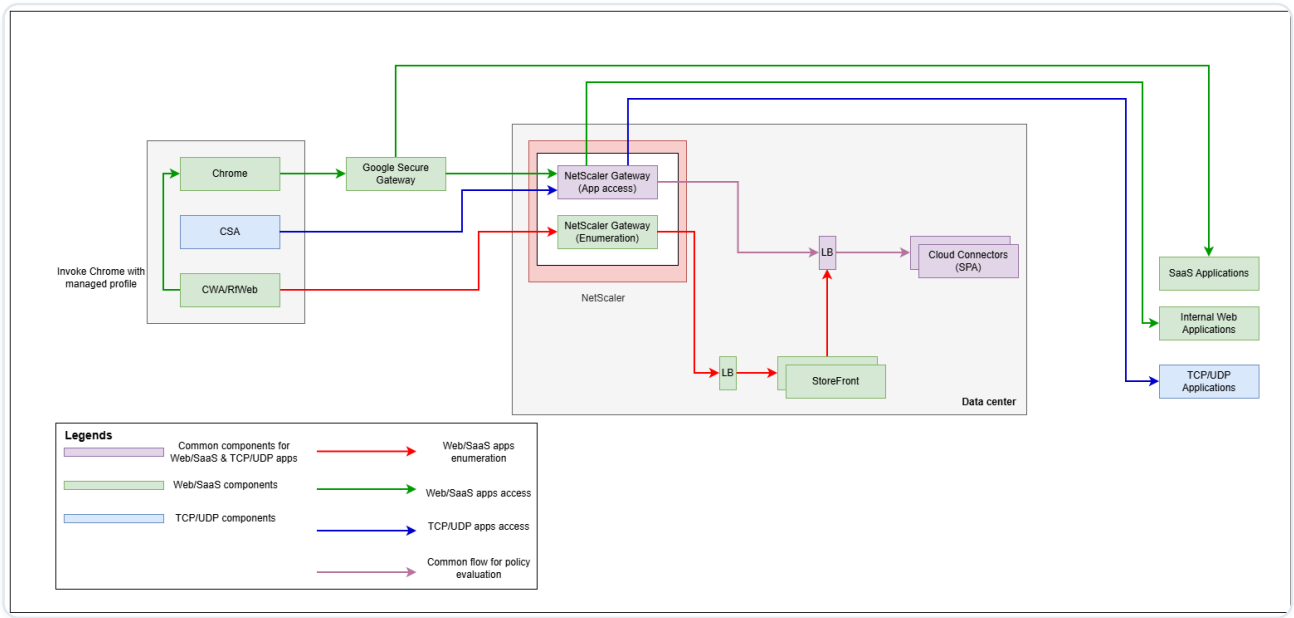
Furthermore, it is recommended to exclude the following hostnames from TLS inspection to avoid potential end-user performance issues and connection delays.

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

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

Get Started with Citrix SecurAccess™ ZTNA hybrid deployment

This topic provides step-by-step instructions for setting up the Citrix SecurAccess ZTNA hybrid environment.



Before you begin

The following sections provide details regarding the checks that you must perform before getting started with Citrix SecurAccess ZTNA hybrid deployment.

Verify your Citrix SecurAccess ZTNA entitlement

You must be entitled to the Citrix SecurAccess ZTNA service in your Citrix Cloud account.

- Log in to the Citrix Cloud console.
- On the dashboard, verify that the **Citrix SecurAccess ZTNA** service tile is visible and available.
- If the service is not visible, you cannot proceed. Contact your Citrix representative to resolve the entitlement issue.

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

Verify prerequisites

Ensure that all prerequisites are met. For details, see Prerequisites.

Verify that all networking prerequisites are met. Refer to the network diagram for complete details of all required ports and communication paths.

Choose the deployment mode

On the welcome screen, select **Set up for hybrid** to begin the configuration.

Next steps

- Step 1: Set up Google Chrome Enterprise Premium
- Step 2: Set up the first data center
- Step 3: Configure and analyze

Step 1: Set up Google Chrome Enterprise Premium

At this step, you are prompted to configure Google Chrome Enterprise Premium.

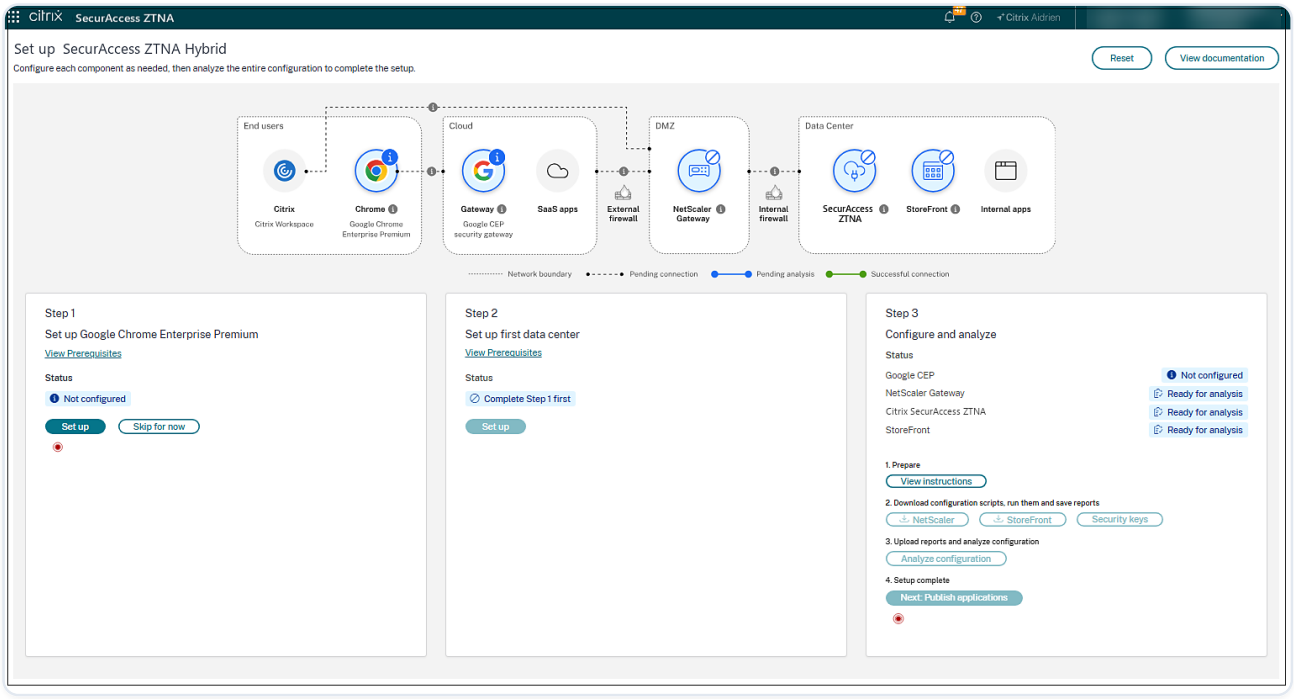
NOTE:

Before setting up Google Chrome Enterprise Premium, consider the following points:

- If you are using Citrix SecurAccess™ ZTNA only for TCP/UDP (client/server) applications, click **Skip for now**. Otherwise, click **Set up** to begin the configuration for Web or SaaS applications.
- If you click **Skip for now**, you cannot enable Chrome Enterprise Premium later without a full reset.
- If you choose to **Set up** Chrome Enterprise Premium, you are enabling support for Web/SaaS applications. This path also allows you to configure TCP/UDP (client/server) applications. If you plan to use Citrix SecurAccess ZTNA for Web or SaaS applications in the future, you must click **Set up** now.

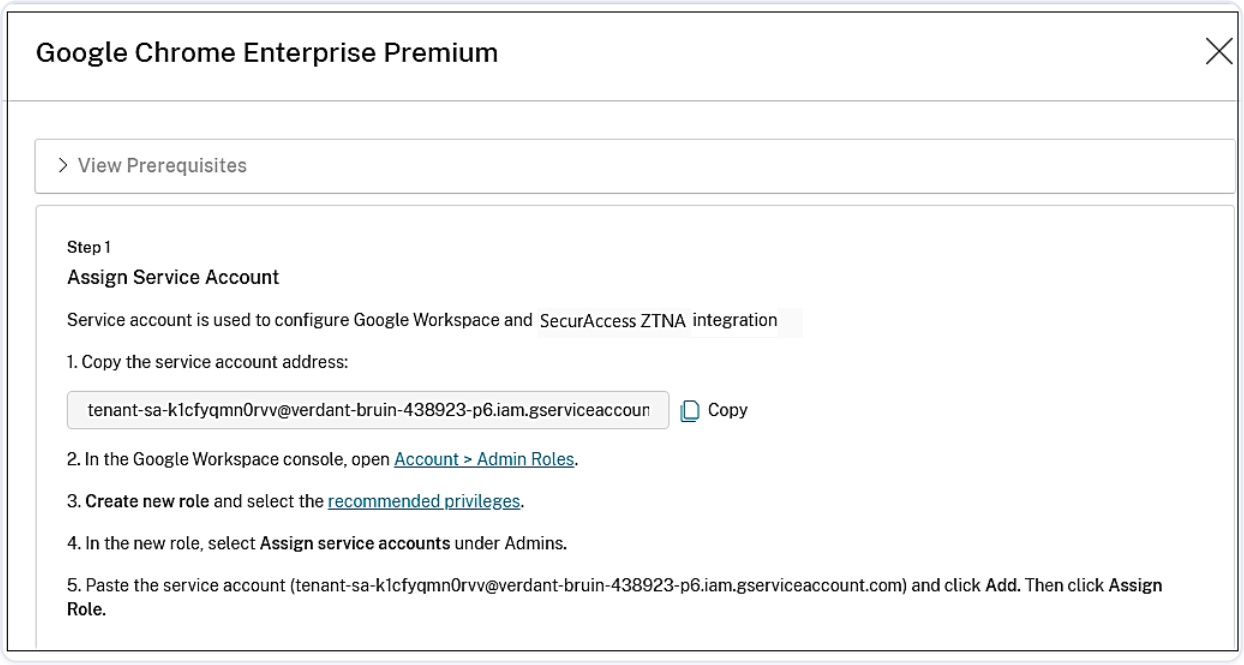
  The only way to enable Web or SaaS features after skipping this step is to reset your entire Citrix SecurAccess ZTNA configuration. To do this, contact Citrix Support.

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



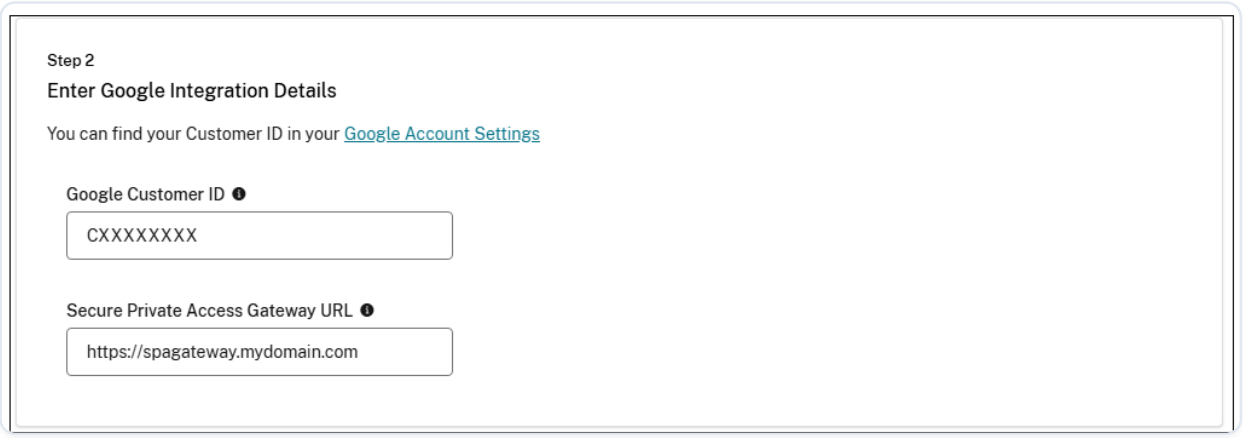
Google Chrome Enterprise Premium configuration

1. Follow the on-screen instructions to create a **Google Admin Role**.
2. Assign the new role created for Citrix SecurAccess ZTNA role to the **Citrix service account** as shown in the instructions. This account is used by Citrix to perform the necessary integration configuration in your Google Workspace Admin console.



3. Follow the on-screen instructions to find your **Google Customer ID** within the Google Workspace Admin console.

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



4. Copy the Google customer ID and paste it into the **Google Customer ID** input field.
5. Ensure that you have already reserved a public IP address and DNS record for your NetScaler Gateway.

   Enter this public URL in the **Citrix SecurAccess ZTNA Gateway URL** field. This URL will be the public address for the NetScaler Gateway you configure in the Step 2 - Set up the first data center. If you are configuring a multi-data center, multi-site setup, this will be the public address of the global server load balancing (GSLB) domain URL.

   Saving this setting automatically configures the **Google Secure Gateway** to use this address, which enables it to connect to your NetScaler Gateway for internal app access.
6. Select the user groups that must be granted access. Only members of these groups can access applications configured in Citrix SecurAccess ZTNA.

   NOTE:

   - The user groups that you select must already exist in Google Workspace.
   - Optionally, apply the configuration to selected Google Directory organizational units, in addition to or instead of user groups. For more information, see Update the Chrome Enterprise Premium configuration.
7. Click **Verify** to ensure that all configurations are correct, and that Citrix SecurAccess ZTNA is ready for Chrome Enterprise Premium integration.
8. Click **Save**.

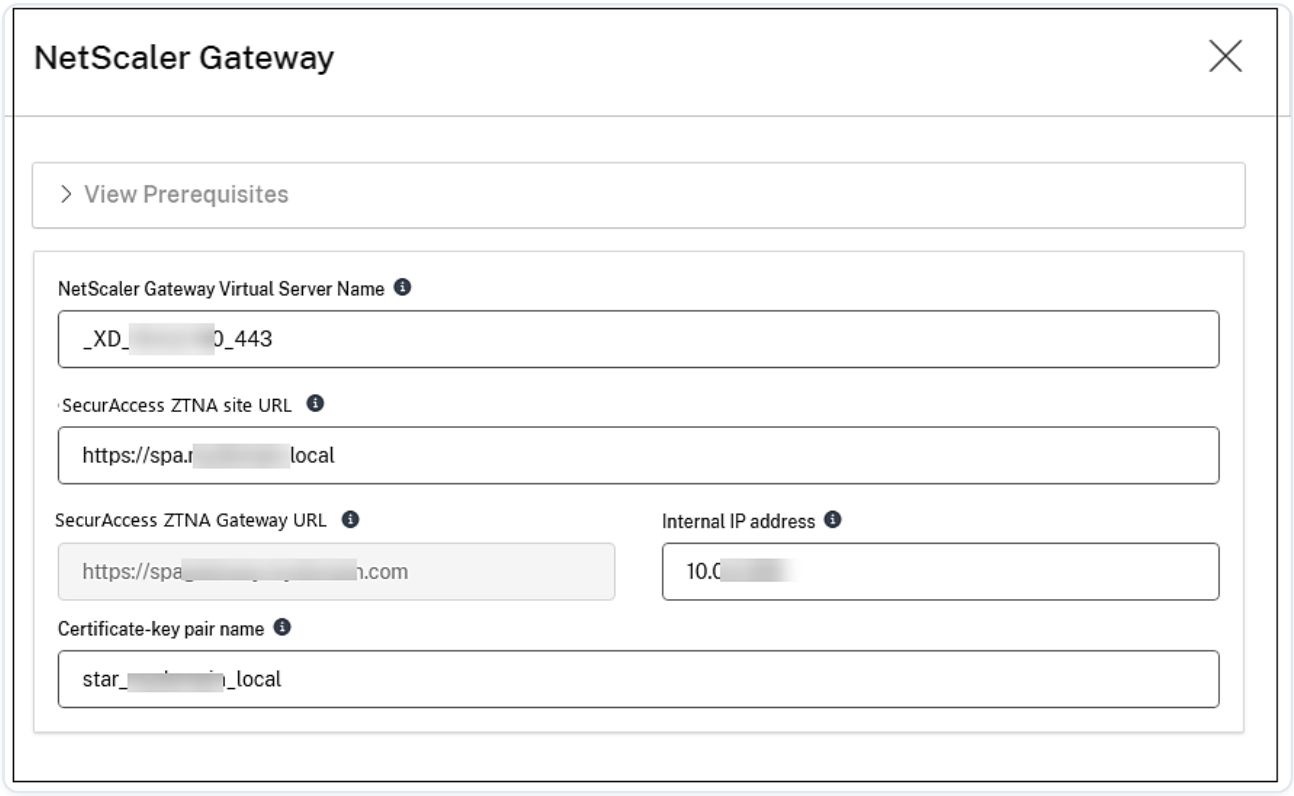
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Set up the first data center

In this step, you are prompted to enter the details required to configure Citrix SecurAccess™ ZTNA on your NetScaler.

NOTE:

Ensure NetScaler meets all prerequisites.



- **NetScaler Gateway virtual server name:** Enter the name of the NetScaler Gateway virtual server that is already configured with your StoreFront deployment. This virtual server is used to enumerate applications configured in Citrix SecurAccess ZTNA within the Citrix Store.

  NOTE:

  This input is not required if you skipped the Chrome Enterprise Premium configuration.

- **Citrix SecurAccess ZTNA site URL:** Enter the load balancer URL that directs traffic to the Citrix SecurAccess ZTNA services running on your Cloud Connectors.

  This load balancer must be configured to use **HTTPS on port 443**. If you have not yet created this load balancer, see Citrix SecurAccess ZTNA load balancer for instructions before proceeding.

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

- **Citrix SecurAccess ZTNA Gateway URL:** This URL is the public address for the NetScaler Gateway that is shared with the users. It is utilized to connect to internal applications.

  If you are configuring a multi-data center, multi-site deployment, this will be the public address of the global server load balancing (GSLB) domain URL. It will be pre-populated if the URL was entered earlier during Step 1: Set up Google Chrome Enterprise Premium.
- **Internal IP address:** Enter the **private IPv4 address** that is used for your Citrix SecurAccess ZTNA gateway. This IP address is assigned to the NetScaler Gateway virtual server during the configuration in Step 3 - Configure and Analyze.
- **Certificate-key pair name:** Enter the name of the **SSL certificate-key pair** that is already configured on your NetScaler.
- Click **Save**. Once saved, a **Shared Secret** is displayed. You need this shared secret value for configuration in Step 3 - Configure and Analyze.

Step 3: Configure and analyze

Configuration can now be applied to the on-premises StoreFront and NetScaler components.

Before proceeding, ensure that all prerequisites for both StoreFront and NetScaler are met.

Download and run NetScaler and StoreFront scripts

The following sections provide more information about the NetScaler and StoreFront scripts.

NetScaler script

NOTE:

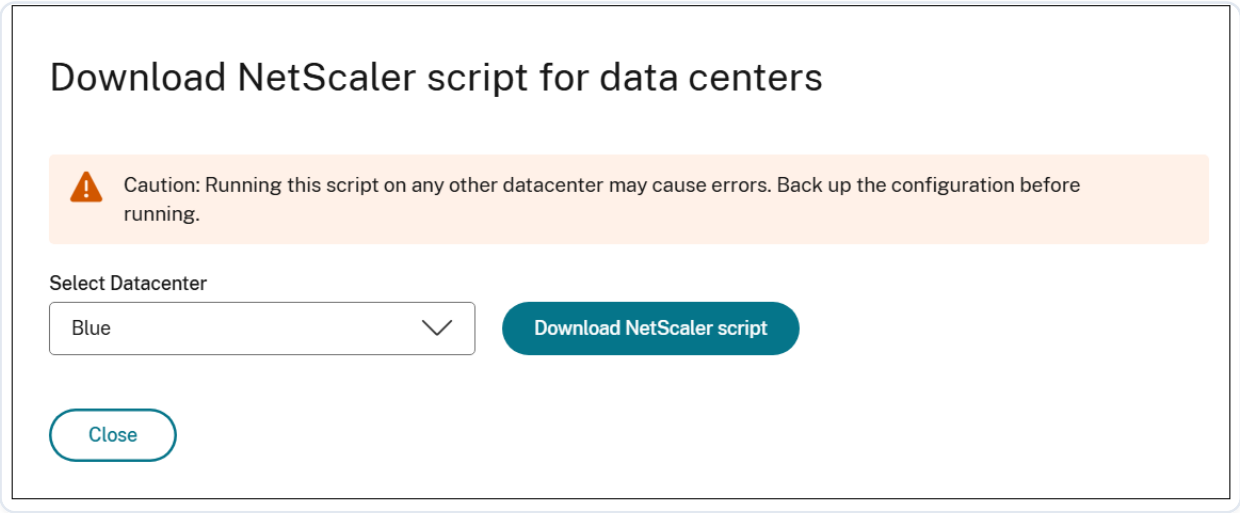
All Citrix SecurAccess™ ZTNA configurations on the **NetScaler** must be performed using the **Command Line Interface (CLI)**.

1. Click **NetScaler** to download the setup script. This script is a diagnostic tool designed to configure and analyze your NetScaler Gateway for the Citrix SecurAccess ZTNA deployment, and collect the required information. For more information, see NetScaler Gateway Analyzer.

   The script file name has the following format:

   `gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz`

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



2. Use an **SCP client** (like `scp` or WinSCP) to copy the downloaded `*.tar.gz` file to your **NetScaler**.
3. Place the file in the `/var/tmp/` directory.
4. Log in to your NetScaler's command-line interface (CLI) using **SSH** (for example with PuTTY) with administrative (`nsroot`) privileges.
5. Type "shell" on the CLI prompt to access the NetScaler shell. Navigate to the temporary directory: `cd /var/tmp/`
6. Extract the archive.

   NOTE:

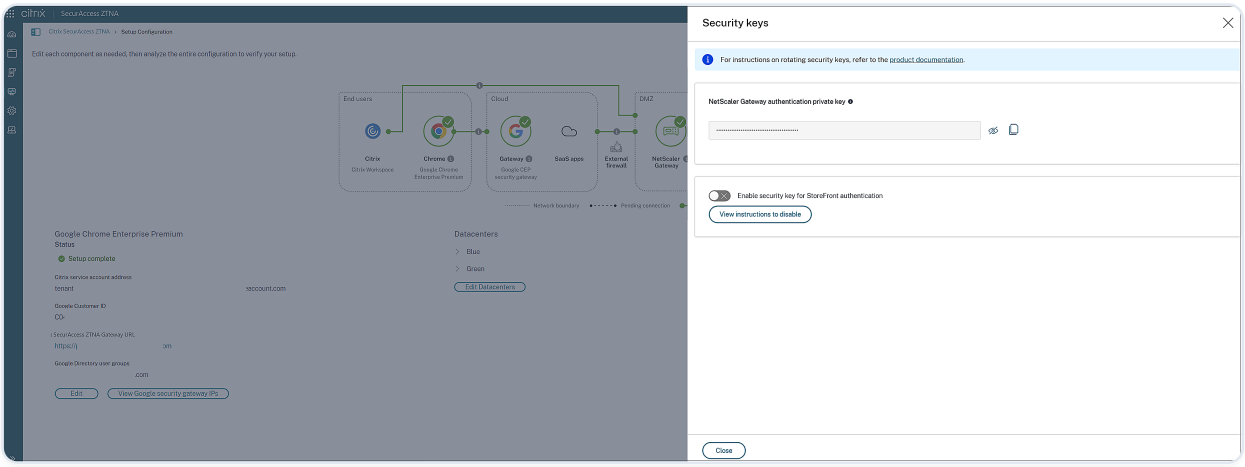
   Your file name is specific to your download.

   ```
   tar -xzf gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz
   ```

7. The `tar` command creates a directory. Use `ls` to see the new folder's name, then navigate into it.
8. Run the analyzer script using python3: `python3 analyzer.py`
9. When the script prompts for the NetScaler Gateway authentication private key:

   a. Return to the Citrix SecurAccess ZTNA setup page in your browser and click **Security keys** on the **Configure and analyze** card.

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



a. Copy the NetScaler Gateway authentication private key.

b. Paste the secret into the NetScaler CLI and press **Enter**.

> **NOTE:**
>
> The key is required to finish the Citrix SecurAccess ZTNA configuration on NetScaler Gateway.

10. After the script is successfully run, it generates an analysis report in the current folder.
11. Download and save this report using scp/winscp. You need it for the Analyzer later.

StoreFront script

> **NOTE:**
>
> This step is optional for CSA-only mode, that is, if CEP configuration is skipped in Step 1 - Set up Google Chrome Enterprise Premium.

1. Click **StoreFront** to download the PowerShell script.
2. This script is a diagnostic tool designed to:

   a. **Analyze** your on-premises StoreFront configuration.

   b. **Collect** the information needed for your deployment.

> **WARNING:**
>
> **Administrator and execution policy required:** You must run this PowerShell script with administrator privileges (example, right-click and "Run as Administrator").

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

Additionally, you might need to adjust the PowerShell execution policy to allow the script to run. If necessary, you can do so by running `Set-ExecutionPolicy Bypass` (or an appropriate policy for your organization) from an elevated PowerShell prompt.

The script file name has the following format:

`storefront_analyzer_<tenant-id>_<timestamp>.zip.`

3. Copy the downloaded .zip file to your **StoreFront server**.
4. On the StoreFront server, **extract** the contents of the .zip file (for example, to a folder like C:\temp\spa-sf-script\).
5. Open a **PowerShell** window with **Administrator privileges** (right-click, "Run as Administrator").
6. In the PowerShell window, navigate (using cd) to the directory where you extracted the script.
7. Execute the script by running the following command:

   `.\CollectAnalyzerStorefrontInfo.ps1`

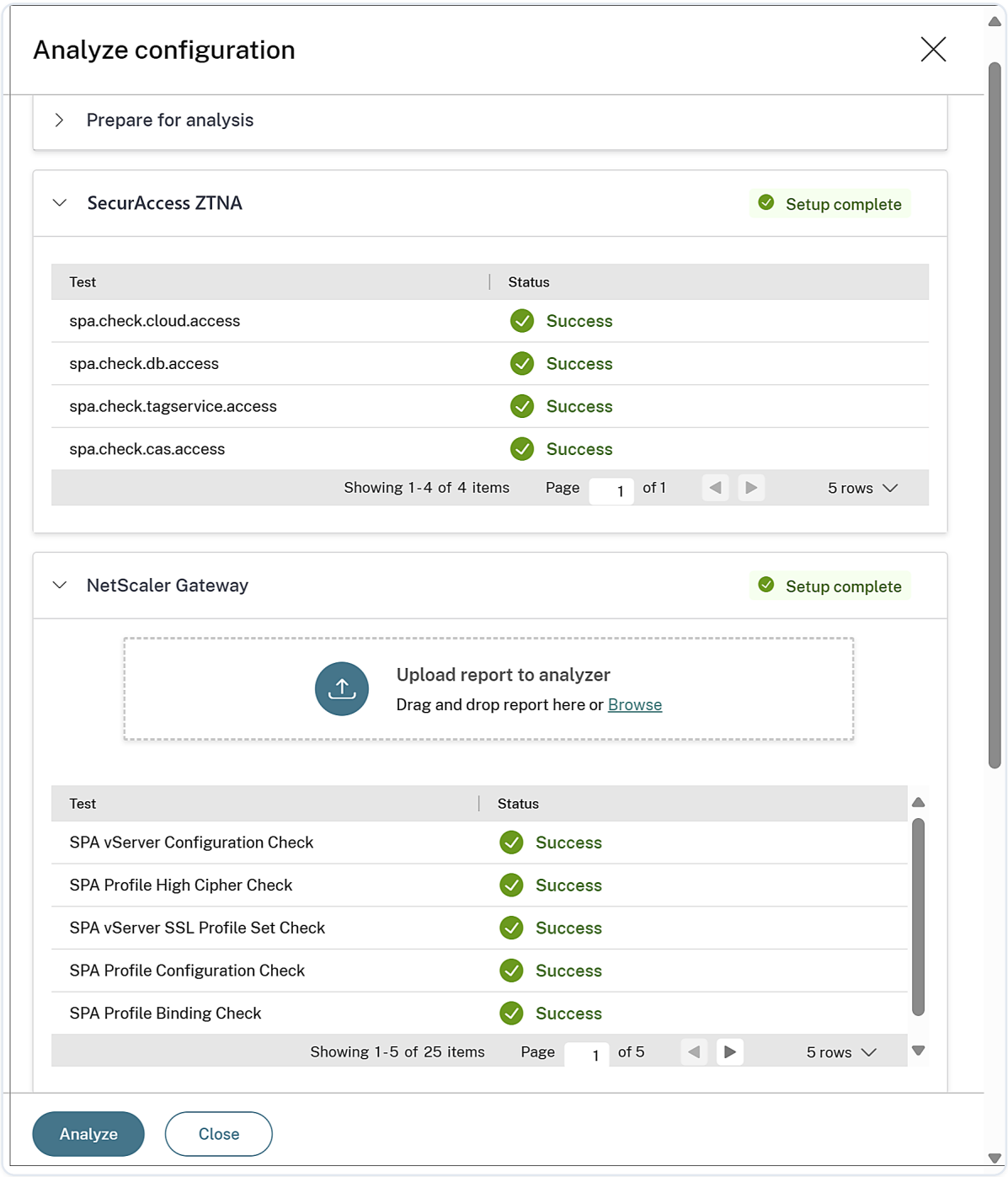
Once the script is successfully run, it generates an analysis report. Download and save it for the next step.

Upload reports and analyze configuration

You can now upload the reports generated by the on-premises scripts to validate your configuration.

1. Click **Analyze**.
2. You are prompted to upload your analysis reports. Upload the two files that you generated:
   - The **NetScaler** analysis report.
   - The **StoreFront** analysis report.
3. Once both files are successfully uploaded, click **Analyze**.
4. Wait for the analysis to complete. The system displays the **Success/Failed** results for all checks.
5. **Review the analysis results:**
   a. **If all analyzer steps have passed:** You have successfully validated your configuration and can proceed to the next step.

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



b. **If any of the steps failed:**

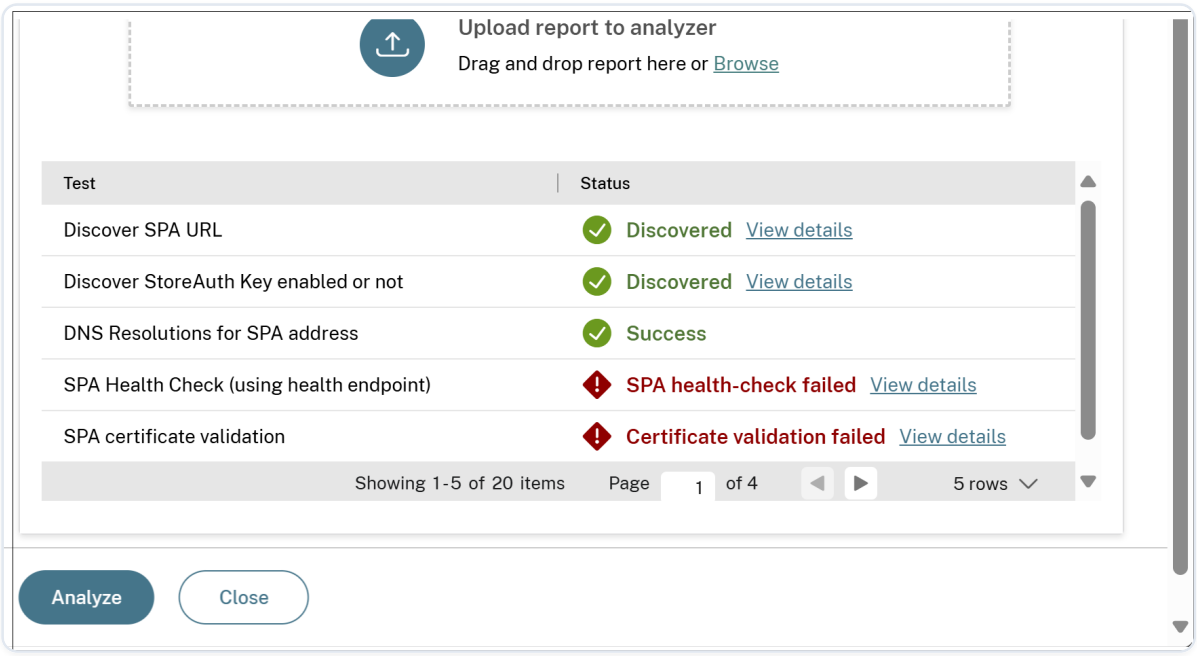
   i. The report suggests **remediation steps**.

   ii. Follow the suggested instructions to fix the error on the failed component (NetScaler or StoreFront).

   iii. After fixing the issues, **re-run the diagnostic script** on that component to generate a new report.

   iv. Return to this step and **re-upload the new analysis report**.

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



Complete onboarding and publish applications

Click **Next: Publish applications** to complete and exit the setup wizard.

This completes your initial hybrid onboarding. If you are configuring a multi-data center, multi-site deployment, proceed to Advanced data center configuration.

Post-onboarding tasks

The following sections provide more information about the post-onboarding tasks.

Configure applications

Your next immediate task is to publish your first application. It is recommended that you test your setup by publishing at least one internal web application or one TCP/UDP application. Follow the detailed instructions in the Apps Configuration and Management.

Configure access policies

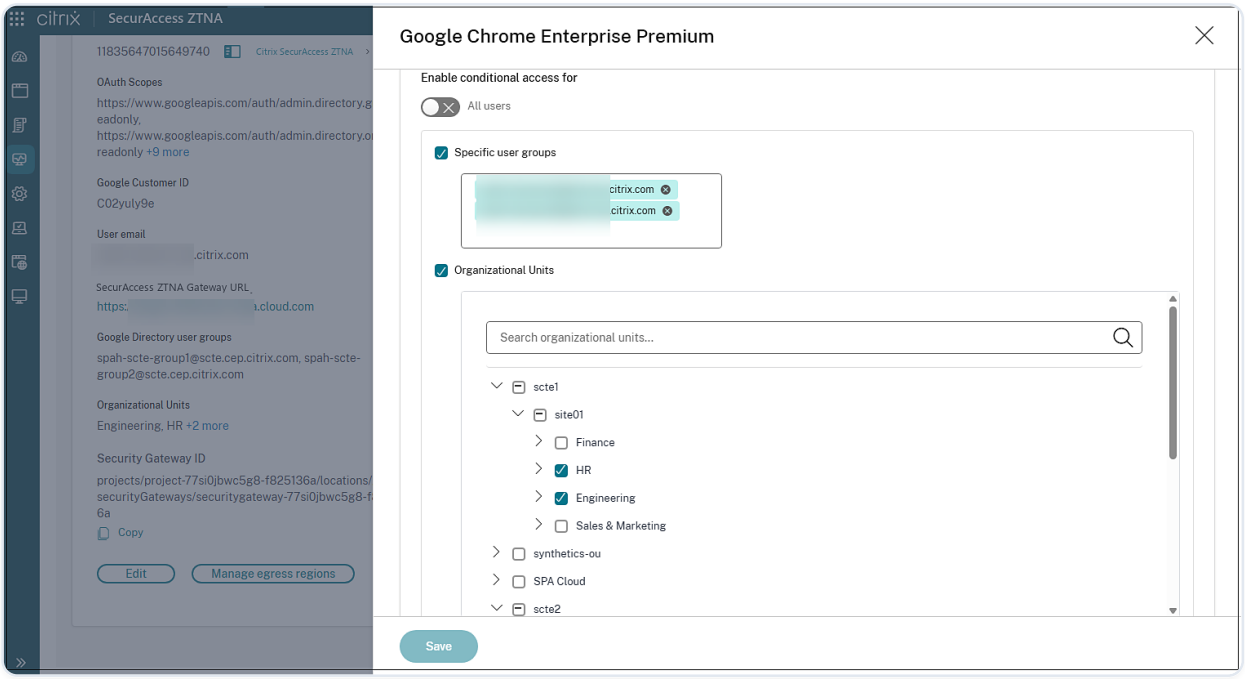
- In the Citrix SecurAccess™ ZTNA admin console, navigate to **Policies > Access Policies**.
- Create an access policy for your application, making sure to define the **User conditions**.
- See the Access policies configuration and management for complete details.

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

Update the Chrome Enterprise Premium configuration

You can update the Chrome Enterprise Premium (CEP) configuration after onboarding to change which users receive it. In addition to all users and Google Directory user groups, you can apply the configuration to selected Google Directory organizational units. User groups and organizational units are not mutually exclusive, so a single configuration can target both.

1. In the Citrix SecurAccess ZTNA console onboarding page, click **Edit** in the Chrome Enterprise Premium setup card.



2. Click **Organizational Units** to display your Google Directory hierarchy as a tree of checkboxes, and then select the organizational units to include.

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

NOTE:

- A selected organizational unit is inherited. The configuration applies to the users in that organizational unit and in all of its child organizational units, including any that are created later. Selecting a parent also selects its child organizational units, which appear selected and grayed out. To include only a subset, clear the parent and select the specific child organizational units.
- The root organizational unit is not shown in the tree. To enable CEP integration for everyone, select **All users** instead.
- The hierarchy is read from your Google Directory using the Citrix service account, which requires the **Organization Units > Read privilege**. For details, see Admin roles and privileges.

3. Click **Verify** to validate the selection, and then click **Save**.

   If you change the selection after a successful verification, run the verification again before you save.

Synchronize the configuration

After saving the changes (new applications or policies), the Citrix SecurAccess ZTNA component inside your on-premises Cloud Connectors must synchronize this new configuration from Citrix Cloud.

This process typically takes up to **10 minutes** to complete.

How to verify: It is recommended to check if the new configuration has been applied by using the **Policy Modeling tool** (under **Policies > Policy Modeling**) to see if your new policies are active.

Access your applications (end users)

This section captures information about how end users access published applications on their devices.

Supported Devices:

- **Web/SaaS applications** (via Google Chrome managed profile) are accessible from any desktop OS.

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

On Linux, iOS, and Android devices, Web/SaaS applications are accessible via the Citrix SecurAccess client.

- **TCP/UDP applications** (via the Citrix SecurAccess client) are supported on **Windows, macOS, Linux, iOS, and Android**.

Accessing Web and SaaS applications

There are three primary ways for users to access their web applications on desktop devices. All these methods will automatically launch the app in the Google Chrome managed profile.

Method A: Using Chrome browser with managed profile (recommended)

This is the most seamless experience for the user.

1. Launch the **Google Chrome** browser.
2. If this is your first time, add a new browser profile using the corporate email address that is configured on the access policy. This creates a managed profile.
3. In the managed profile, navigate to your **NetScaler Gateway URL** (the one configured in Step 2: Set up the first data center).
4. Log in to your store.
5. Click a Web or SaaS application icon to launch it.

The app launches in a new tab in the managed profile.

Method B: Using a non-managed web browser

NOTE:

This method requires a supported version of the Citrix Workspace app to be installed on the desktop device.

1. Launch any browser of your preference (for example, non-managed Chrome, Edge, Firefox).
2. Navigate to your **NetScaler Gateway URL** (the one configured for StoreFront in Step 2: Set up the first data center).
3. Log in to your store.
4. Click a Web or SaaS application icon to launch it.
5. The browser displays a dialogue prompting you to open the **Citrix Workspace App**.
6. Click **Continue** or **Open**.

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

7. Citrix Workspace app takes over and launches the application in the **Google Chrome managed profile**. If a profile is not already created, a setup screen with your email address pre-populated appears for you to complete the profile.

Method C: Using Citrix Workspace app

1. Launch the **Citrix Workspace App** on your device.
2. If not already configured, add your store using the **NetScaler Gateway URL** (the one configured for StoreFront in Step 2: Set up the first data center).
3. Log in to your store.
4. You can see your list of enumerated applications.
5. Click a Web or SaaS application icon to launch it. The application automatically opens in the managed Google Chrome profile.

Accessing TCP/UDP (client/server) applications

Accessing TCP/UDP applications requires the Citrix SecurAccess client.

You must install Citrix SecurAccess with the supported version on the endpoint device.

Connect the Secure Access Client

1. Launch the **Citrix SecurAccess client**.
2. When prompted for a URL, enter the **Citrix SecurAccess ZTNA Gateway URL** (the FQDN configured in Step 2: Set up the first data center).
3. Complete the login and authentication prompts.
4. The client connects and then runs securely in the background.

Launch your published applications

You can now use your native client software directly if allowed by Citrix SecurAccess ZTNA policies. For example:

- Open **Microsoft Remote Desktop** and connect to the internal host name of your RDP server.
- Open an **SSH client** and connect to the internal IP of your Linux server.

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

Data regionalization

Data regionalization in Citrix SecurAccess™ ZTNA enables customers to control where their data is stored by selecting a preferred geographic region. Customers can choose the region where their data is stored, with options including Global, Europe (EU), APAC (Asia Pacific), and North America (NA). All configuration data at rest remains within the selected region, ensuring that it does not leave the designated geography.

The data regionalization feature delivers the following benefits:

- Ensures strong data residency control by keeping all configuration data within the selected region.
- Helps organizations meet regulatory and data sovereignty requirements.
- Reduces risk by preventing data from leaving designated geographies.
- Supports flexible global deployments with region-specific needs, enabling customers to confidently adopt cloud-delivered secure access aligned with their residency policies.

NOTE:

Without data regionalization, organizations operating across regions might face strict data residency and compliance requirements while lacking control over where their service data is stored. Without regional data boundaries, configuration data might be stored outside required geographies, increasing regulatory risk and limiting adoption of cloud-delivered secure access solutions.

Supported deployments

This feature applies to all Citrix SecurAccess ZTNA deployments, including both service and hybrid models, and is especially relevant for organizations with regional data residency, compliance, and regulatory requirements.

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

Configuration

Selecting a region is a one-time setting during onboarding of the Citrix SecurAccess ZTNA service or a hybrid deployment. After it is set, all data remains in the selected region, with no impact on ongoing operations or user workflows.

1. Log in to Citrix Cloud and then click **Citrix SecurAccess ZTNA**.
2. Select **Setup for cloud** or **Hybrid** and then click **Continue**.
3. In **Select deployment region** select the region where your data must be stored, and then click **Continue**.

Limitations

Some of the limitations of data regionalization are:

- Data regionalization applies only to configuration data at rest. Other data types (such as telemetry or in-transit data) might not be restricted to the selected region.
- There are dependencies on other Citrix Cloud services that operate globally, which might not follow the same regional boundaries.
- This is a one-time configuration during onboarding and cannot be changed later.
- The feature is currently available for new customers only.

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

Hybrid deployment setup components

The following components are involved in the SecurAccess™ ZTNA hybrid deployment.

- **Cloud Connector:** SecurAccess ZTNA service runs in Cloud Connectors as Windows service. Ensure that Cloud Connectors are installed in your resource location. Set them up if necessary. For details, see Cloud Connector.
- **SecurAccess™ ZTNA service:** The SecurAccess ZTNA™ service provider for hybrid deployment is installed as part of Citrix Cloud Connector. After Citrix Cloud Connector is installed, the Citrix SecurAccess ZTNA service can be found in the Windows services. For details, see SecurAccess™ ZTNA service.
- **NetScaler:** Ensure that all prerequisites for NetScaler configuration are met. For details, see NetScaler.
- **StoreFront:** To display Citrix SecurAccess™ ZTNA web applications in your on-premises Citrix Store, you must configure the Citrix SecurAccess ZTNA service as a new Delivery Controller on StoreFront. For details, see StoreFront.

Cloud Connector Configuration

Citrix SecurAccess™ ZTNA service runs in Cloud Connectors as Windows service. Ensure that Cloud Connectors are installed in your resource location. Set them up if necessary.

For details, see Cloud Connector installation.

Ensure that your Cloud Connectors (or their configured proxy) can send outbound traffic on port 443 to all FQDNs listed in the Connector Common and SPA FQDNs of the `allowlist.json` file.

Citrix SecurAccess™ ZTNA service

The Citrix SecurAccess ZTNA service provider for hybrid deployment is installed as part of Citrix Cloud Connector. After Citrix Cloud Connector is installed, the Citrix SecurAccess ZTNA service can be found in the Windows services. The Citrix SecurAccess ZTNA service operates under the network service account.

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

IMPORTANT:

- Once the Cloud Connector is updated, the Citrix SecurAccess ZTNA service is disabled. To enable the feature, customers must contact Citrix Support.
- Once enabled, the service status changes to **Running**, and the Citrix SecurAccess ZTNA service automatically starts on the connector machine.

Port Configuration for Citrix SecurAccess ZTNA service

- Citrix SecurAccess ZTNA uses port 8443 as a plain HTTP service.
- Ensure that the inbound rule for port 8443 is added to allow access from the data center network. The port 8443 can be opened by manually configuring the firewall rules or by running the Citrix SecurAccess ZTNA config tool.
  - Navigate to the Citrix SecurAccess ZTNA installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).
  - Run the command .\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443.

After the command is run successfully, the firewall is configured automatically.

- The internal load balancer for Citrix SecurAccess ZTNA adds the Cloud Connector back-end service using port 8443.

Citrix SecurAccess ZTNA load balancer

The load balancer for the Citrix SecurAccess ZTNA service must be configured with TLS enabled using one of two approaches:

- **SSL offload on the load balancer:** The Citrix SecurAccess ZTNA load balancer communicates with the Citrix SecurAccess ZTNA service on Cloud Connector over HTTP on port 8443, and the TLS/SSL certificate is installed on the load balancer. Traffic between the load balancer and the Citrix SecurAccess ZTNA service is plain HTTP and not encrypted. For details, see Configure SSL offloading.
- **SSL bridge:** The load balancer forwards encrypted traffic to the Citrix SecurAccess ZTNA service on Cloud Connector. TLS/SSL certificate must be installed for the Citrix SecurAccess ZTNA service on each Cloud Connector host. For details, see See Configure SSL bridging.

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

Configure TLS/SSL certificates for the Citrix SecurAccess ZTNA service on Cloud Connector

1. Install a valid TLS/SSL certificate on the Cloud Connector's local machine Personal certificate store. Ensure that the certificate is trusted. Add the issuing CA certificates if necessary.

   NOTE:

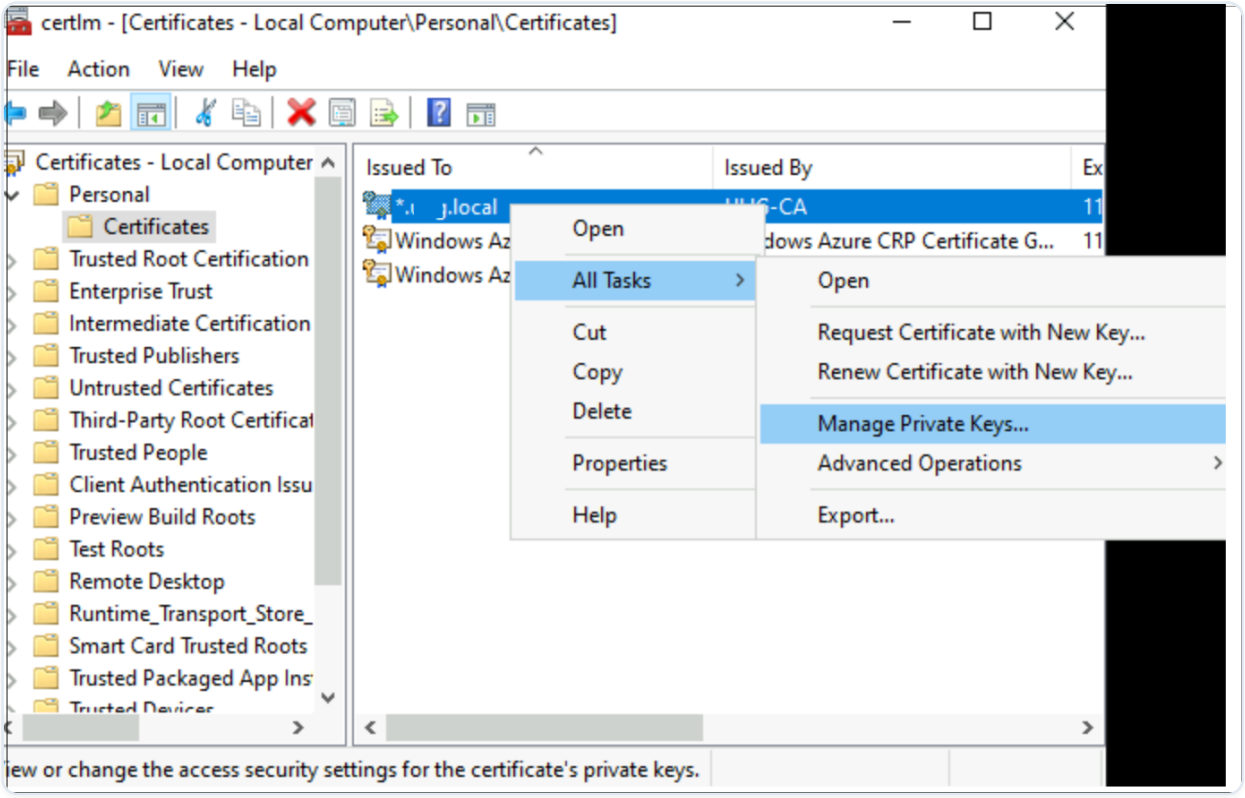
   Ensure that the TLS/SSL certificate contains Cloud Connector FQDN as part of Subject Alternative Name (SAN).

2. Grant Network Service account permission to access the installed certificate.

   a. Open the Microsoft Management console and add certificate snap-in to your local computer account, follow the wizard, and click **OK**.

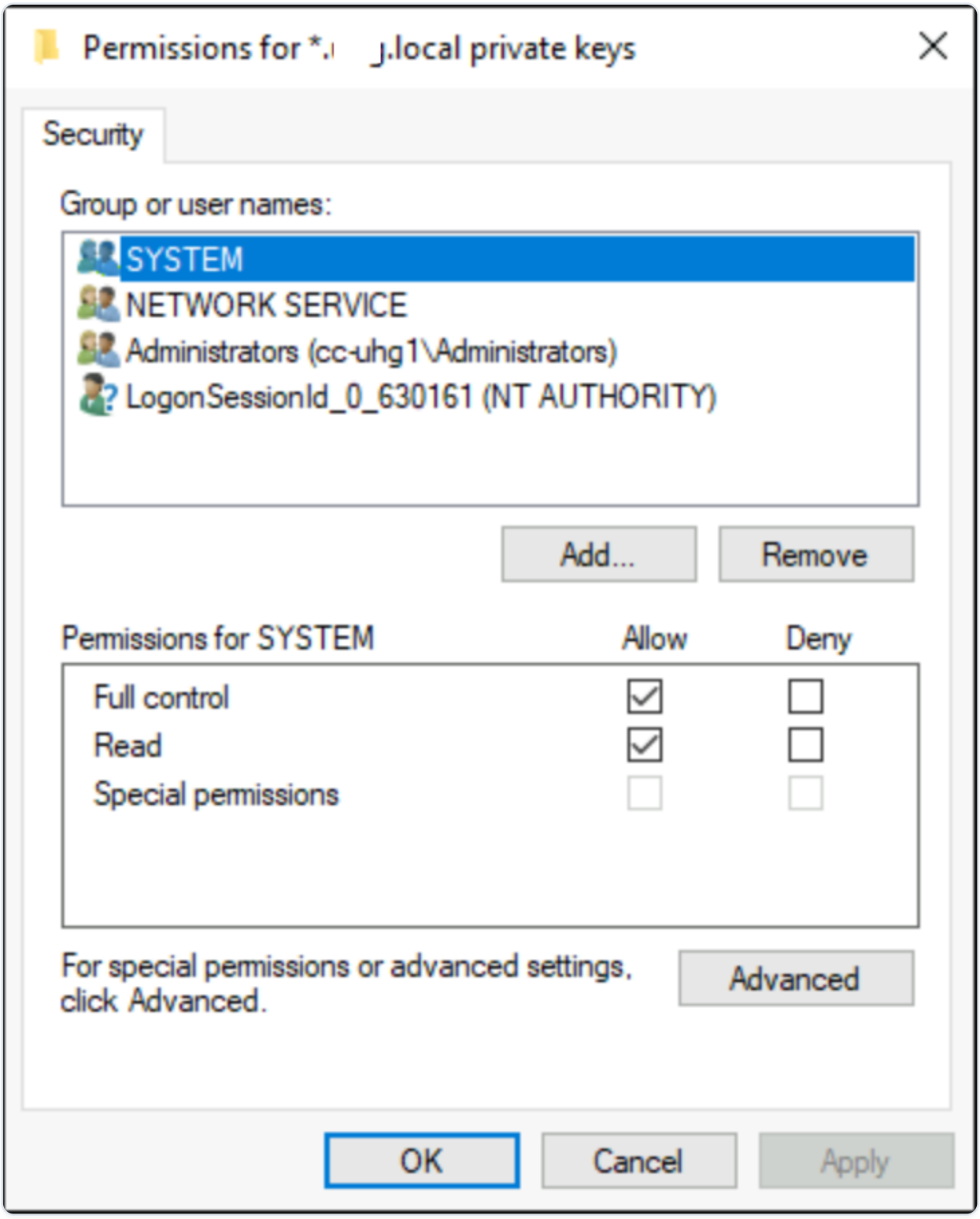
   b. In the Microsoft Management Console, go to **Console Root > Certificates > Personal > Certificates**.

   c. Right-click the certificate that is required to configure Citrix SecurAccess ZTNA and select **All Tasks > Manage Private Keys**.



   a. In the **Permissions** window, click **Add** and then search for the Network Service account, and select **Read only permission**.

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



3. Configure the Citrix SecurAccess ZTNA service with TLS/SSL certificate thumbprint.

   a. Copy the thumbprint from **TLS/SSL Certificate Details**.

   b. Navigate to the Citrix SecurAccess ZTNA installation folder (default path - C:\Program Files\Citrix\AccessSecurityService) and run .\Citrix.AccessSecurityService.exe / CERTIFICATE_THUMBPRINT `<ThumbprintValue>`.

   c. Restart the Citrix SecurAccess ZTNA service.

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

4. Ensure that the Citrix SecurAccess ZTNA service is running as a TLS service (use browser or cURL): `https://<Cloud connector address>:<port>/secureAccess/health`.

   Expected result: `response 200 OK with status “Ok”`.

NetScaler

The topic helps you ensure that all prerequisites for NetScaler configuration are met.

- Set up NetScaler Gateway for Citrix Virtual Apps and Desktops by using one of the following methods:
  - Create a NetScaler Gateway virtual server for remotely accessing StoreFront, for users who are using Citrix Workspace app or a web browser. For details, see Integrate NetScaler Gateway with StoreFront.
  - Configure the settings on NetScaler Gateway. For details, see ConfigureNetScaler Gateway appliance by using wizards.

  NOTE:

  The XenApp and XenDesktop wizard configures the basic authentication. Citrix SecurAccess™ ZTNA requires advanced authentication. Therefore, you can skip the **Authentication step** in XenApp and XenDesktop wizard. You can configure the authentication profile later once NetScaler Gateway is created using the wizard.

- Add SSL certificates to NetScaler. For details, see Install SSL certificates on a NetScaler instance.

Configuring a load balancer for StoreFront. For details, see Load balancing with NetScaler.

Configure authentication

Perform the following steps to configure authentication:

- Configure an authentication virtual server. For details, see Authentication virtual server.
- Configure an authentication profile. For details, see Configuring Authentication Profiles.
- Configure nFactor authentication. For details, see nFactor authentication.

  Commonly used nFactor authentication methods:

  - LDAP authentication

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

- RADIUS authentication
- Microsoft Entra ID

Sample authentication configurations

The following sections provide more information about the sample authentication configurations.

Multifactor authentication with conditional authentication

- Dual factor authentication with LDAP and RADIUS using dual factor schema (taking user input only once)
- Authentication log on method according to user's departments (Employee, Partner, Vendor) in organization with drop-down menu to select the department
- Authentication log on method according to user domains with drop-down menu
- Configure email ID (or user name) input as first factor with conditional access based on group extraction with email ID at first factor and provide different logon type for each group
- Multifactor authentication using Certificate authentication for users with user certificates and Native OTP registration for non-cert users
- Different authentication type with conditional authentication according to user host name inputs
- Dual factor authentication with Native OTP authentication

Third-party integration with multifactor authentication

- Configure Azure AD as SAML IdP (Configure next factor as LDAP policy - NO_AUTH to complete OAuth trust)
- Conditional authentication with First factor as SAML and then custom login to certificate or LDAP based on SAML attributes
- First factor as webauth login followed by LDAP

Device posture scans (EPA)

- Device posture check for version check followed by customized login for compliant (RADIUS) and non-compliant users(LDAP)
- LDAP authentication followed by mandatory device posture scan
- Device posture check before and after AD authentication - Pre and Post-EPA as a factor
- Device Certificate as an EPA factor

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

Miscellaneous scenarios

- Add EULA with authentication
- Customize nFactor policy labels, login schema

StoreFront

To display Citrix SecurAccess™ ZTNA web applications in your on-premises Citrix Store, you must configure the Citrix SecurAccess ZTNA service as a new Delivery Controller on StoreFront.

Follow this procedure, especially if you are integrating with an existing Citrix DaaS environment (as it allows you to use your existing StoreFront).

1. On the StoreFront server, open the StoreFront admin console.
2. Navigate to the section for managing Delivery Controllers (for example, select **Store** and click **Manage sites**).
3. Click **Add** to create a new controller.
4. When prompted for the controller type, select the **Citrix SecurAccess ZTNA** option.
5. In the **Server** field, enter the FQDN of your Citrix SecurAccess ZTNA load balancer.
6. Select Transport type **HTTPS** and Port **443**.
7. Save your changes.

Configuring a new Store

If the Store doesn't already exist, install the supported version of StoreFront, and then follow the **Create Store** wizard. Ensure that the Store is configured with:

- **Remote access:** Remote access configuration requires NetScaler Gateway virtual server address that is used to enumerate web/SaaS applications published in Citrix SecurAccess ZTNA.
- **Authentication methods:** Ensure Pass-through from Citrix Gateway is enabled.

For details, see Create store.

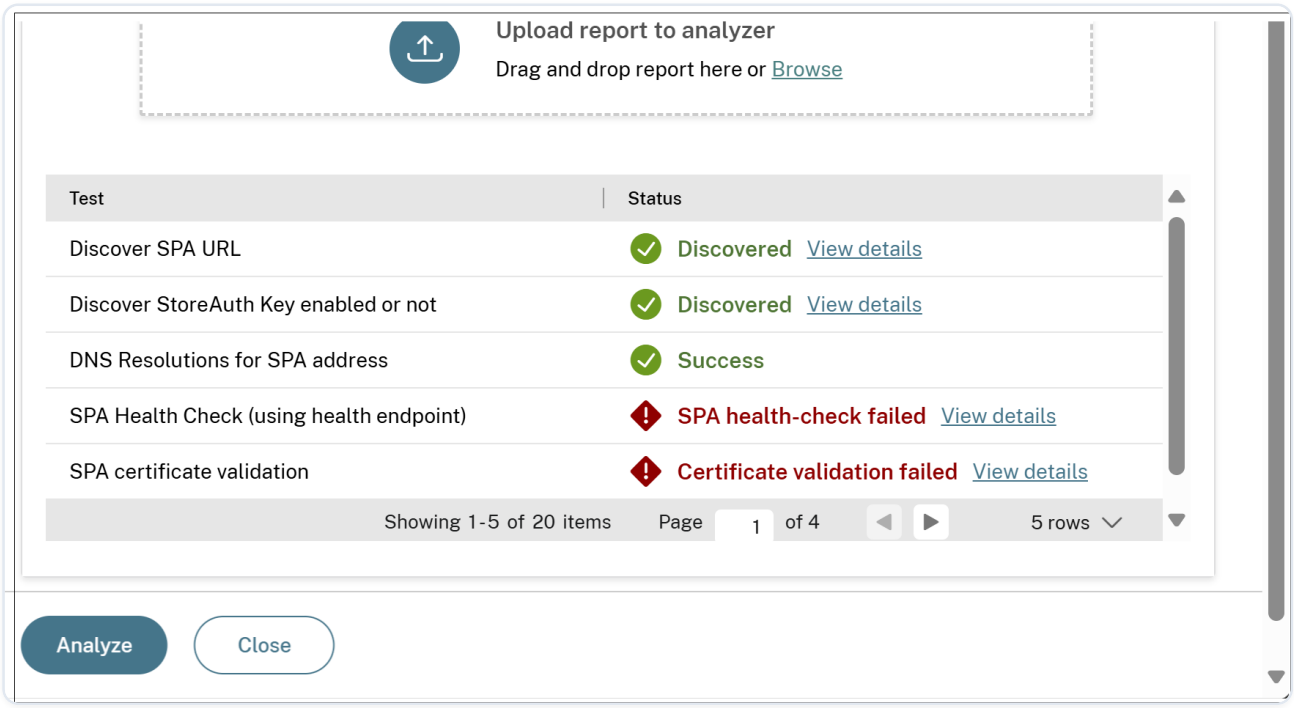
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Component Analyzer

Component Analyzer is a web-based tool that performs the configuration checks required for a Citrix SecurAccess™ ZTNA hybrid setup. After uploading the necessary reports, the Analyzer identifies issues with detailed error messages and explanations, including examples of detected StoreFront configuration errors. The tool also lists potential remediations to resolve the identified problems.

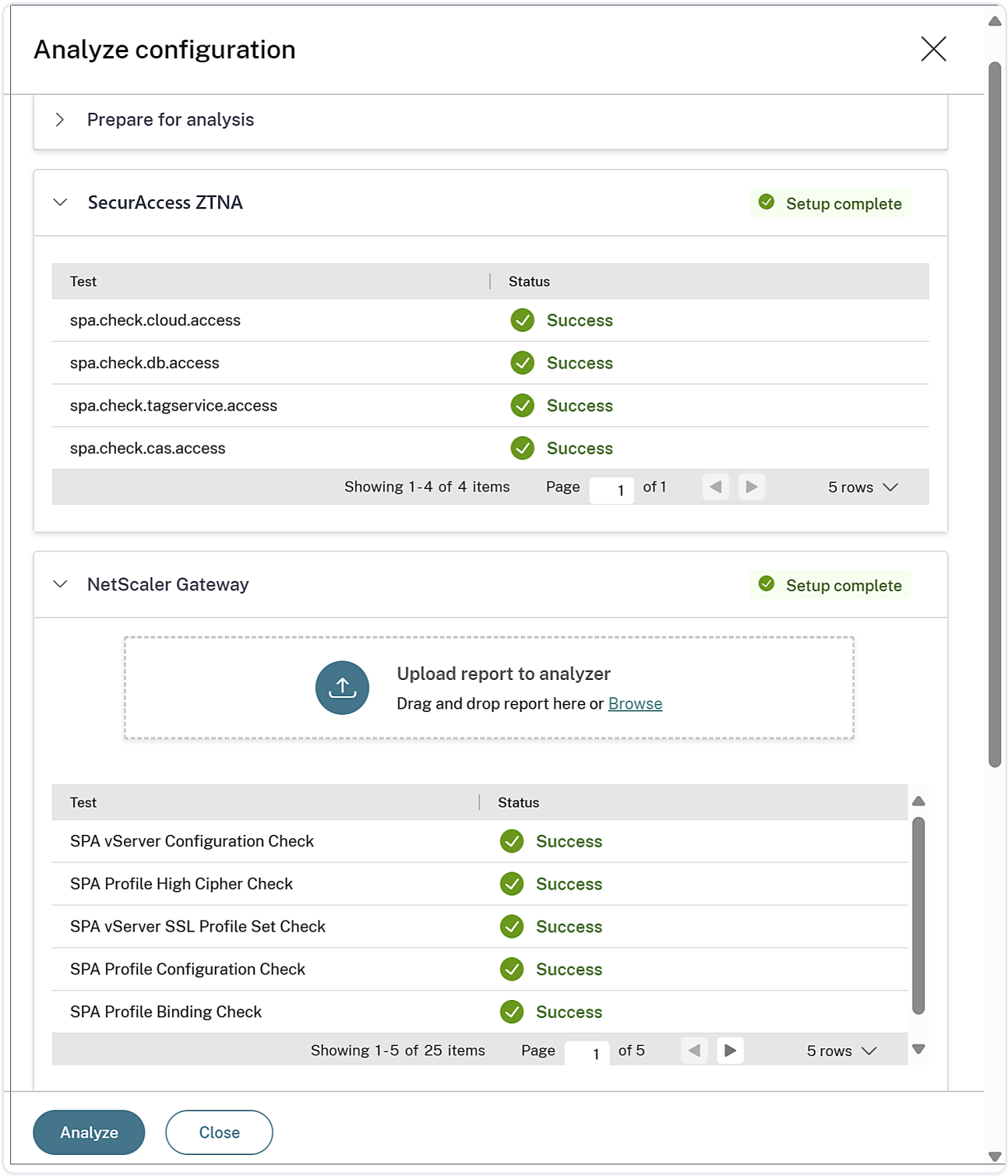
You must re-run the Analyzer after applying remediations to confirm that all configuration checks pass.

Example of a detected StoreFront configuration error.



If there are no errors, the Analyzer displays successful results for all checks.

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



Citrix SecurAccess ZTNA Analyzer

The Citrix SecurAccess ZTNA Analyzer evaluates the readiness and reachability of key Citrix Cloud components required for Citrix SecurAccess ZTNA deployment. Without the need for report uploads, it automatically checks connectivity to essential services such as Cloud Access, database services, and other required internal services.

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

By verifying each component's accessibility and operational status, the tool helps administrators quickly identify network or configuration issues, ensuring that all Citrix Cloud dependencies are available and properly functioning for Citrix SecurAccess ZTNA integration.

NetScaler Gateway Analyzer

NetScaler Gateway Analyzer streamlines Citrix SecurAccess ZTNA deployments by automating key tasks and highlighting configuration issues. It performs targeted checks and validations, producing actionable diagnostics that enhance reliability and performance while reducing manual effort and configuration risk.

The NetScaler Gateway Analyzer capabilities include:

- **Configuration:** Automatic or interactive setup of the NetScaler Gateway component.
- **Analysis:** Assessment of connectivity, compliance, and operational health across Citrix SecurAccess ZTNA components.
- **Cleanup:** Removal of Citrix SecurAccess ZTNA configurations when required.

Each capability is invoked via dedicated command line options (see README.txt), supporting flexible lifecycle management from initial rollout through maintenance to controlled teardown.

The execution generates timestamped artifacts containing structured logs and analysis summaries. Outputs cover configuration state, connectivity test results, discovered component metadata, and identified issues. Cleanup operations provide confirmation of entity removal to ensure a clean state. All results are delivered in a structured JSON format suitable for automation, integration, and audit.

See Step 3: Configure and analyze to download and run the script on NetScaler.

StoreFront Analyzer

StoreFront Analyzer streamlines Citrix SecurAccess ZTNA readiness checks for Citrix StoreFront by automating discovery and validation tasks. It performs targeted assessments of configuration, connectivity, authentication, and certificates, producing actionable diagnostics that improve reliability while reducing manual effort and configuration risk.

The StoreFront Analyzer capabilities include:

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

- **Analysis:** Read-only evaluation of StoreFront configuration, network reachability, authentication settings, remote access parameters, and certificate validity relevant to Citrix SecurAccess ZTNA compatibility.

The execution produces timestamped artifacts with structured logs and analysis summaries. Outputs include Citrix SecurAccess ZTNA URL discovery, StoreAuth key status, DNS resolution results, health endpoint accessibility, SSL certificate validation, and discovered component metadata. All results are delivered in a structured JSON format suitable for automation, integration, and audit.

No configuration changes are made. The analyzer operates in read-only mode.

See Step 3: Configure and analyze to download and run the script on NetScaler.

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

Integration with Google Chrome Enterprise Premium

Citrix customers can leverage the world's most popular and secure web browser, Chrome with a familiar experience to natively access authorized corporate web applications. Citrix SecurAccess™ ZTNA enforces per application least privilege access based on admin-defined policies that are centrally managed through the Citrix SecurAccess ZTNA console. Administrators can easily configure enterprise application domains and zero trust access policies on the Citrix SecurAccess ZTNA console. They can model policies to validate and test security outcomes and deliver the right level of user access and end-user experience.

The integrated solution includes the following components:

- Google Chrome Enterprise Premium (CEP), which includes features such as data loss prevention (DLP), malware and phishing protection, URL filtering, and Google administration console.
    - The Google Chrome browser running locally on the client machine acts as a secure browser with per user level policy enforcement via Chrome managed profiles.
    - The Google Chrome Enterprise Premium console accessed via the Google Cloud portal provides the administration, management, and monitoring console for the Chrome Enterprise Premium security policies.
- Citrix SecurAccess ZTNA, which includes access to the cloud infrastructure, ZTNA policy engine, and Connector Appliances deployed in the customer environment.
- Citrix console including the Citrix SecurAccess ZTNA console for zero-trust access policies to private applications and Citrix Monitor for monitoring and troubleshooting.

The Citrix SecurAccess ZTNA service enforces all the access policies configured by the administrator, ensuring that users are only granted access to specific web applications.

Chrome Enterprise Premium advanced security features

The following are some of the advanced security features offered by Chrome Enterprise Premium:

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

- **Data loss prevention (DLP)**: Implement granular controls and policies to prevent sensitive data from being leaked or accidentally shared.
- **Malware deep scanning**: Use advanced scanning techniques to detect and quarantine unknown or high-risk files, preventing the execution of malicious code and protecting against zero-day attacks.
- **Phishing protection**: Safeguard users from visiting harmful websites by identifying and blocking phishing attempts, preventing the theft of login credentials and personal information.
- **URL categorization and filtering**: Restrict access to websites based on their content category, preventing users from accessing inappropriate or malicious content.
- **Web usage insights and analytics**: Provide detailed reports and analytics on web traffic, allowing administrators to monitor user activity, identify potential security threats, and optimize network bandwidth.

For more information, see Chrome Enterprise Premium overview.

Prerequisites for successful integration

To ensure optimal integration between the Citrix Workspace™ application and Chrome Enterprise Premium, the following prerequisites must be met. Successful completion of these prerequisites results in a more efficient and seamless experience when launching applications from the Citrix Workspace app or the web-based user interface.

The prerequisites are broadly classified into the following categories.

- NetScaler prerequisites
- Cloud Connector prerequisites
- StoreFront prerequisites
- Citrix SecurAccess ZTNA prerequisites
- Google prerequisites
- Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory
- Bypass TLS inspection

Citrix SecurAccess ZTNA - Supported deployment modes

The integrated solution supports the following deployment modes from Citrix SecurAccess ZTNA:

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

- **Citrix SecurAccess ZTNA service**: In this deployment mode, all components, including the control plane and gateway infrastructure, are hosted in Citrix Cloud. For more information, see Citrix SecurAccess ZTNA.
- **Citrix SecurAccess ZTNA hybrid deployment**: This deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use Citrix Cloud for managing the configuration, administration, and monitoring functions. This means customers can leverage existing NetScaler Gateway on-premises to control user traffic routing while using Citrix Cloud hosted UI for management of configurations and policies and also use Citrix Monitor hosted in the Citrix Cloud for monitoring and troubleshooting functions. For more information, see Citrix SecurAccess ZTNA hybrid deployment.

IMPORTANT:

For Chrome Enterprise Premium (CEP), only HTTPS enterprise web and SaaS apps are supported. HTTP enterprise web and SaaS apps are not supported.

Legal

Chrome Enterprise Premium is provided by Google LLC and your use is subject to Google's Acceptable Use Policy and Service Specific Terms.

Admin roles and privileges

The Citrix service account is used by Citrix SecurAccess™ ZTNA to onboard users to Chrome Enterprise Premium (CEP) and enable CEP integration. Therefore, you must assign a role with the required privileges to the service account in the Google Admin console.

Two types of roles are available in the Google Admin console:

System roles: These are the default roles provided by Google. Except for the super admin role, the remainder of the system roles does not include all the necessary privileges required for CEP integration with Citrix SecurAccess ZTNA.

Custom roles: These can include any subset of Admin API privileges. You must create a custom role that includes all privileges required for CEP integration with Citrix SecurAccess ZTNA.

You must be signed into the Google Admin console as a super administrator for this task.

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

NOTE:

Super administrator roles cannot be assigned to service accounts.

Google custom admin role privileges

For CEP and Citrix SecurAccess ZTNA integration, the Citrix service account must have a custom role in the Google Admin console with the following specific privileges:

REQUIRED ADMIN PRIVILEGE	WHY IS THIS PRIVILEGE NEEDED
Manage customer > Read customer	To read the Google customer organization-friendly name.
Organization Units > Read	To verify that the organization units configured are available in Google Directory.
Services > Chrome Management > Settings > Manage User Settings **Note:** Ensure that you select the top-level privilege **Manage User Settings** and the sub-privileges (**Manage Application Settings** and **Manage Web Settings**).	To add the mandatory extensions, and configuration thereof, required for CEP and SPA integration at the user profiles.
Services > Chrome Management > Settings Managed Browsers > Read	To read the managed Chrome profiles and the managed browsers.
License Management > Read	To query the total number of Chrome Enterprise Premium-assigned licenses provisioned for the organization.

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

REQUIRED ADMIN PRIVILEGE	WHY IS THIS PRIVILEGE NEEDED
Reports	To read the users that are actively using their assigned licenses. To read the activity events when the Data Loss Prevention (DLP) rules are triggered. To read the failure events.
Groups > Read	To verify that the integration groups configured are available in Google Directory.
Services > Alert Center > Full access > View access	To read the security alerts for Data Loss Prevention and the login failure events.
Manage Devices and Settings	To read device metadata so as to display them in the Monitor network topology view.
Users > Read	To verify that the integration users configured are available in Google Directory.

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

NOTE:

- It is also required to grant the equivalent OAuth scopes for these admin privileges.
- All administrative privileges are now found in the **Admin privileges** section. This includes privileges previously listed in the **Admin console privileges** and **Admin API privileges** sections. This change does not affect how privileges are assigned, and existing privileges continue to work as they did before.
- Ensure that you select the top-level privilege **Manage User Settings** and the sub-privileges (**Manage Application Settings** and **Manage Web Settings**). Selecting only the sub-privileges is not sufficient.
- Citrix SecurAccess ZTNA deploys configurations to your Google account using the Citrix service account configured. After Citrix SecurAccess ZTNA and Google CEP integration is completed, open the Google Admin console and navigate to **Chrome Browser > Apps & Extensions**. Note that several browser extensions have been configured at the root org level. Those are inherited by the child OUs. When users onboard Google Chrome profiles with this tenant, these extensions are automatically provisioned.

Create and assign roles and privileges

Perform the following steps to create a custom admin role and assign privileges:

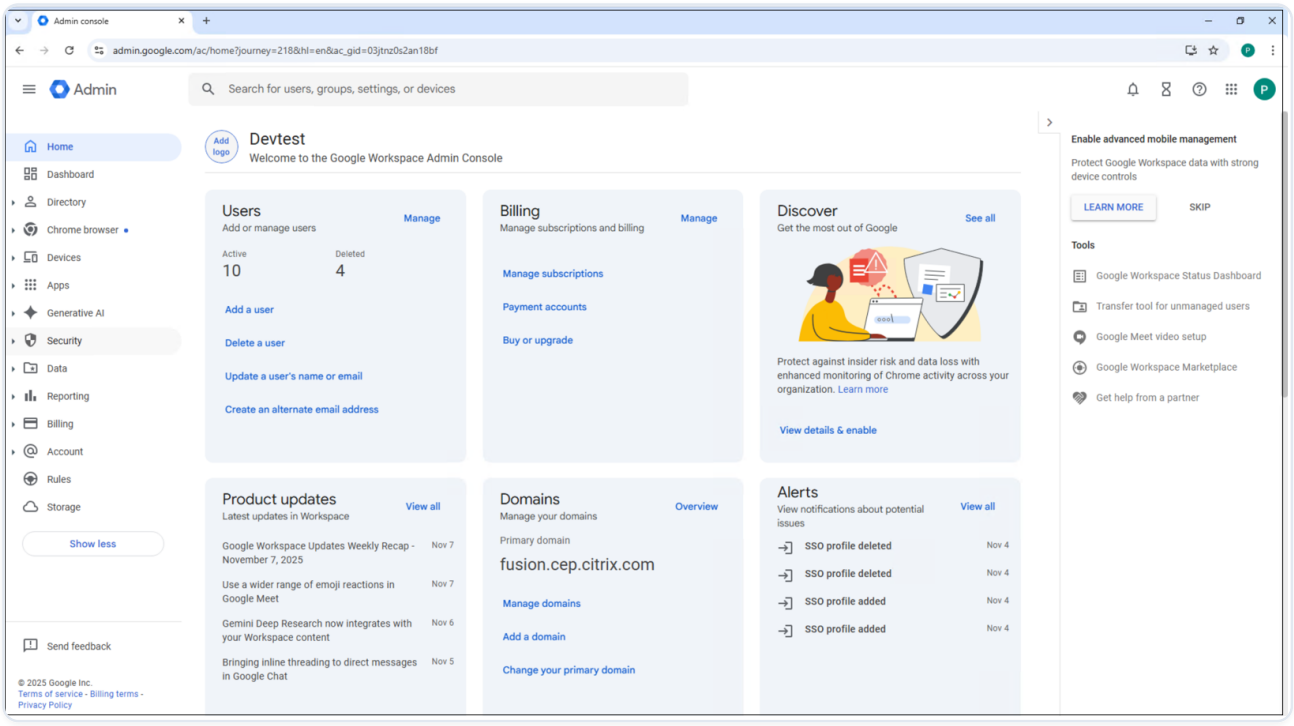
1. In the Google Admin console, go to **Accounts** > **Admin roles**.
2. Click **Create new role** and enter a name and description for the role.
3. Add all the privileges required for Google Chrome integration to this custom role. For the list of required privileges, see Google custom admin role privileges.

   For more information related to roles and privileges, see the Google documentation.
4. Save the custom role.

Open ID Connect profile to use NetScaler Gateway as the IdP

You must create an OIDC profile on the Google Admin console for using NetScaler Gateway as an IdP.

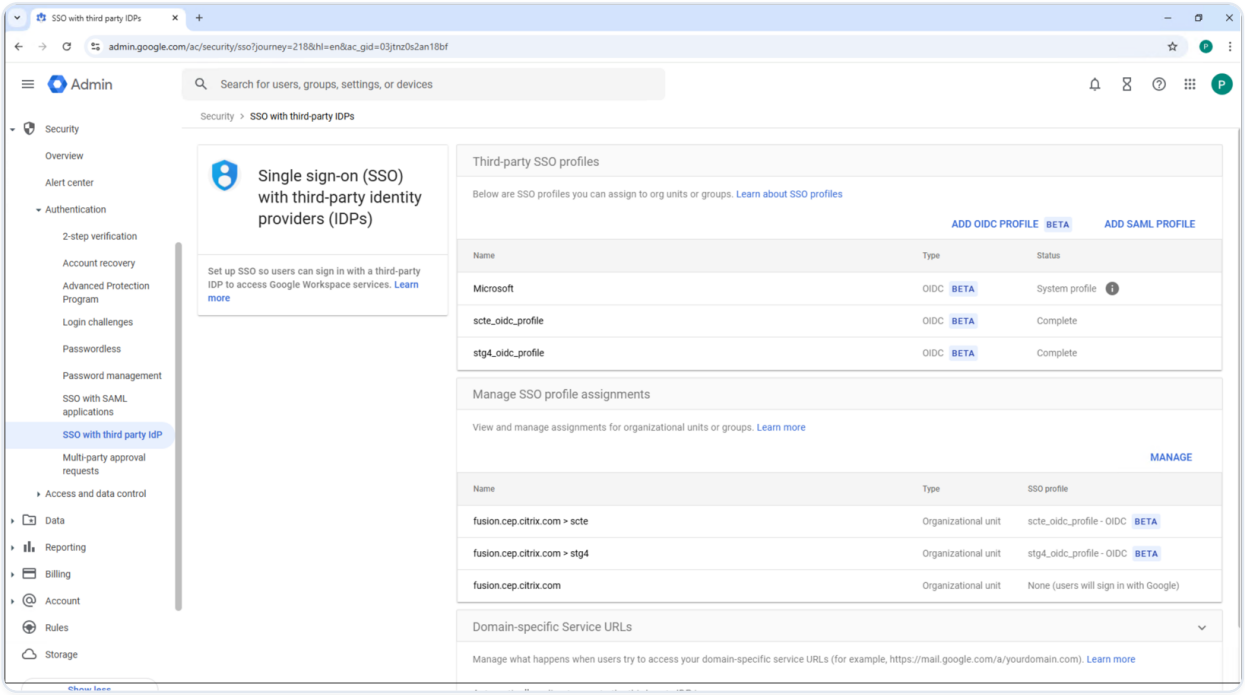
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a Google OIDC SSO profile

Perform the following steps in the Google Admin console.

1. Go to **Security > Authentication > SSO with third party IdP** and then select **Add OIDC Profile**.



2. Enter a name for the profile.
3. Enter the OIDC details.

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

- **Client ID:** Use a random client ID (usually a 22 characters numeric string)
- **Client Secret:** Generate a random string of a minimum of 32 characters. The string must include alphanumeric and special characters.

  Some special characters such as, - #, @, !, \^, &, %, are not allowed in the **Client secret** field while configuring OAuth IdP profile on NetScaler. Therefore, you must not use these special characters in the **Client Secret** field here.

> **NOTE:**
>
> You must manually generate the client ID and client secret in NetScaler Gateway.

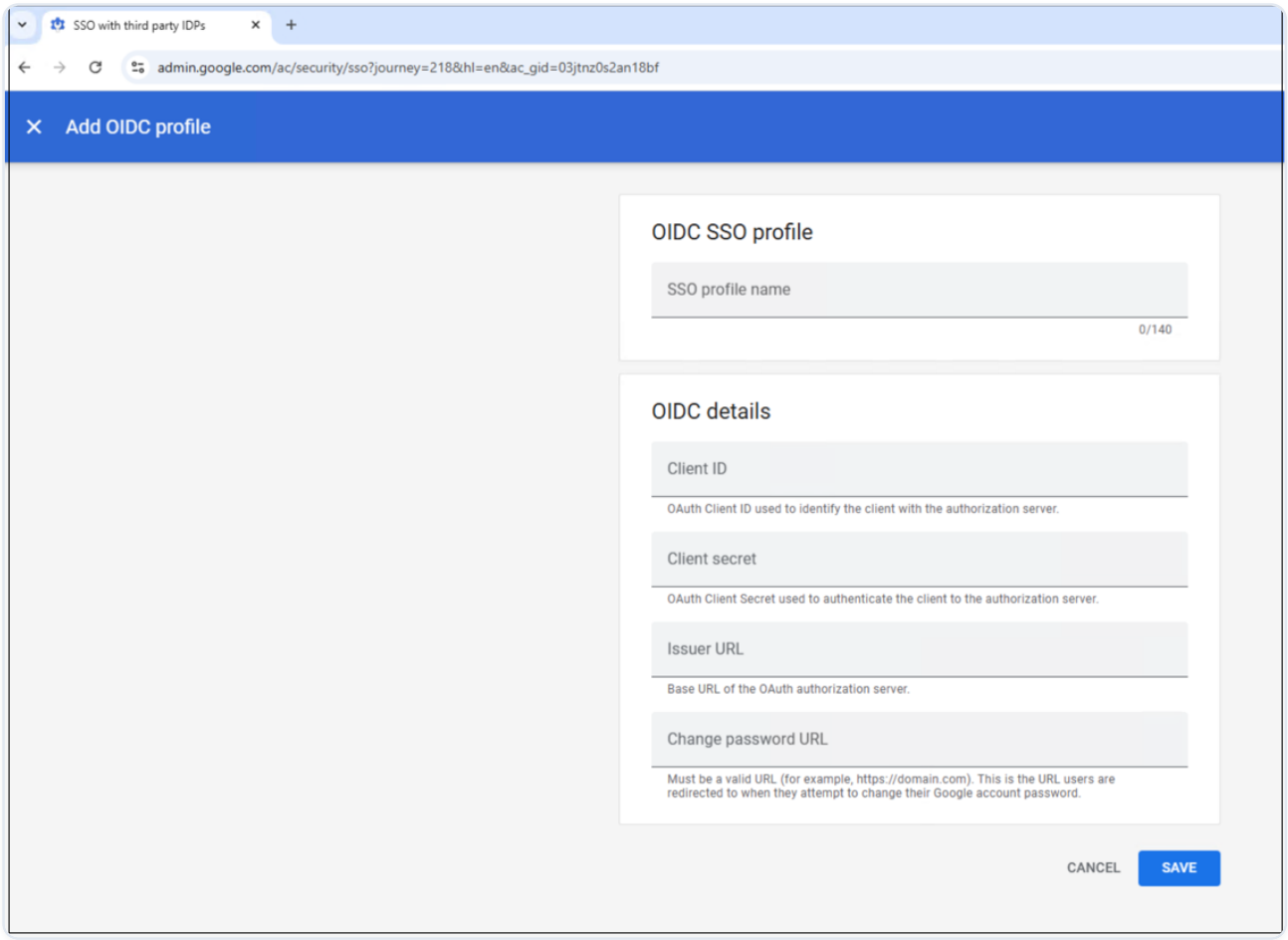
- **Issuer URL:** Set this field to `https://<SPAGatewayFQDN>/oauth/idp/<OAuthIdpProfileName>`, where `SPAGatewayFQDN` is the FQDN corresponding to the Citrix SecurAccess™ ZTNA Gateway URL and `OAuthIdpProfileName` is the name of the OAuth IdP profile, which is created on the NetScaler Gateway.

> **NOTE:**
>
> Do not use spaces in the IdP profile name.

- **Change password URL:** Leave it blank (not needed at this point)

4. Click **Save**.

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



IMPORTANT:

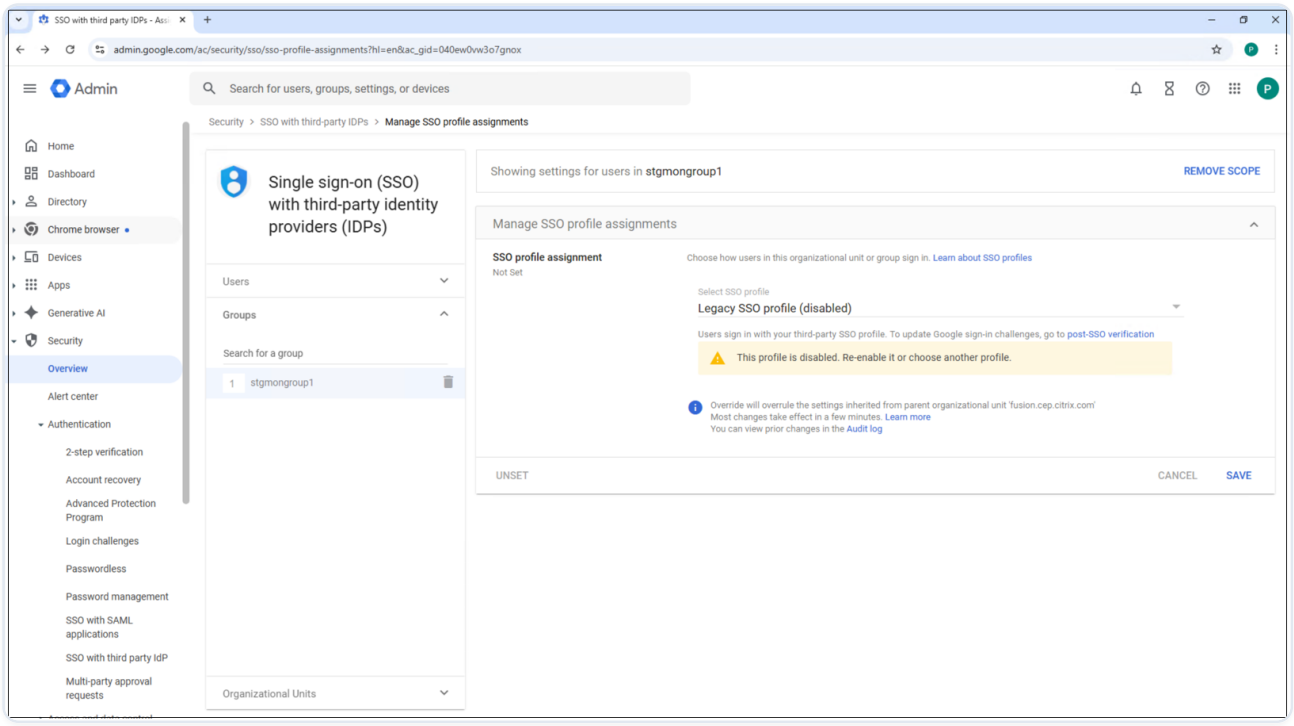
Note down the Client ID, Client secret, and the Redirect URL. These values are required while configuring the OAuth IdP profile on NetScaler Gateway.

Bind the OIDC Profile (To either an OU or group)

To complete the OIDC profile configuration, you must bind it to specific organizational units (OUs) or groups in your Google Workspace. This binding determines which users can authenticate using this OIDC profile with NetScaler Gateway as the IdP.

1. Navigate to **Security > Authentication > SSO with 3rd Party IDPs**.
2. In **Manage SSO profile assignments**, click **Manage**
3. From the left navigation pane, select the root organizational unit (OU) and your SSO profile to enable SSO for all users of your organization. Alternatively, you can assign the SSO profile to specific groups or OUs.
4. Select the SSO profile that you created and click **Save**.

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



Configure NetScaler as an OAuth IdP

See NetScaler as an OAuth IdP for configuring NetScaler as an OAuth IdP.

NOTE:

- The **Audience** field value in the OAuth IdP profile must be same as the client ID value.
- The **Issuer URL** must match with the one configured in the Google Admin console.
- The **Client ID**, **Client Secret** and **Redirect URL** values must be taken from the Google Admin console.

Directory synchronization

The following sections provide more information about the directory synchronization.

Microsoft Entra ID using G Suite connector

You must synchronize your Microsoft Entra ID with the Google Cloud user directory for user and group management across both Google and Microsoft cloud platforms. For details, see the following topics:

- Microsoft Entra ID (formerly Azure AD) user provisioning and single sign-on

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

- Configure Google Cloud / G Suite Connector by Microsoft for Single sign-on with Microsoft Entra ID

The email address field must be populated for all users and groups. The email domain must match the one configured in Google Directory. Implicitly, this means that Security Groups without an email address or groups with an @onmicrosoft.com email domain are currently not supported.

Single sign-on: Single sign-on (SSO) configuration is optional. You might configure a separate password in the Google directory. See To configure SSO with Open ID Connect profile to use NetScaler Gateway as the IdP.

Google Cloud Directory Sync (GCDS) tool

With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.

For details, see About Google Cloud Directory Sync.

Install and prepare GCDS:

- Download
- Installation

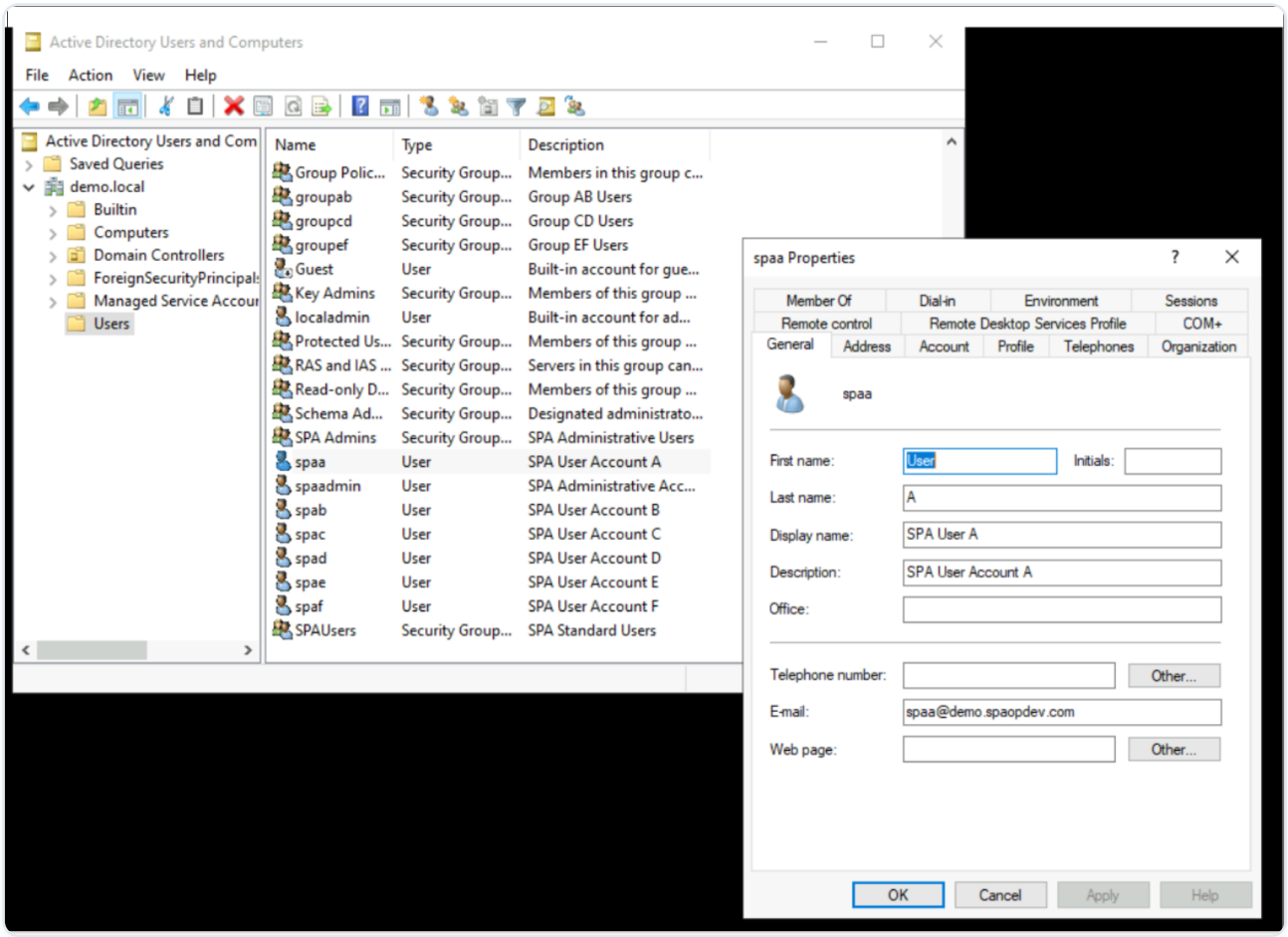
NOTES:

- For POC purposes, the GCDS tool can be installed on an AD machine.
- Run the installer with Administrator permissions.
- Configuration can be saved in a file (File\Save As) and opened next time when you want to synchronize.

Active Directory

As a prerequisite, ensure that you have users and groups created on Active Directory. Users and groups must have the email attribute.

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

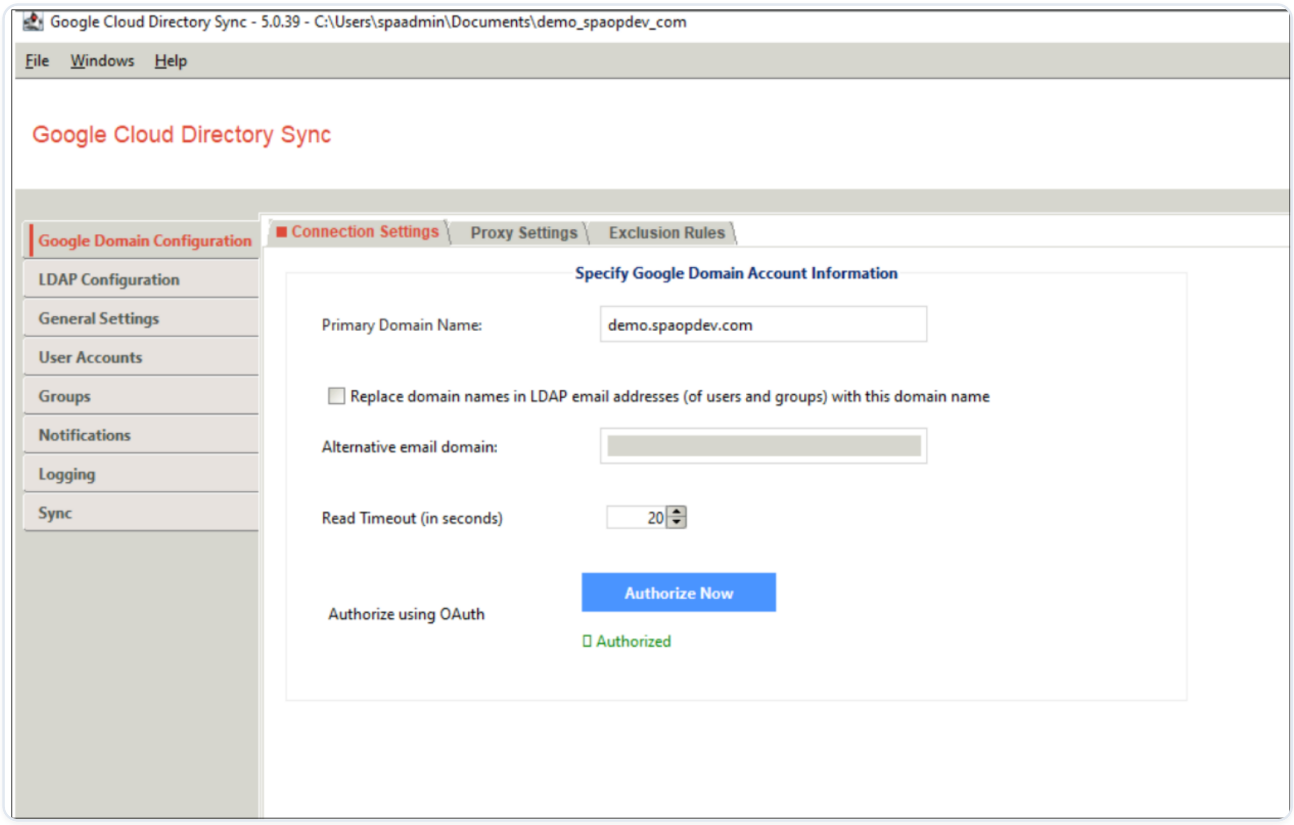


Google Cloud Directory Sync configuration

Google domain configuration:

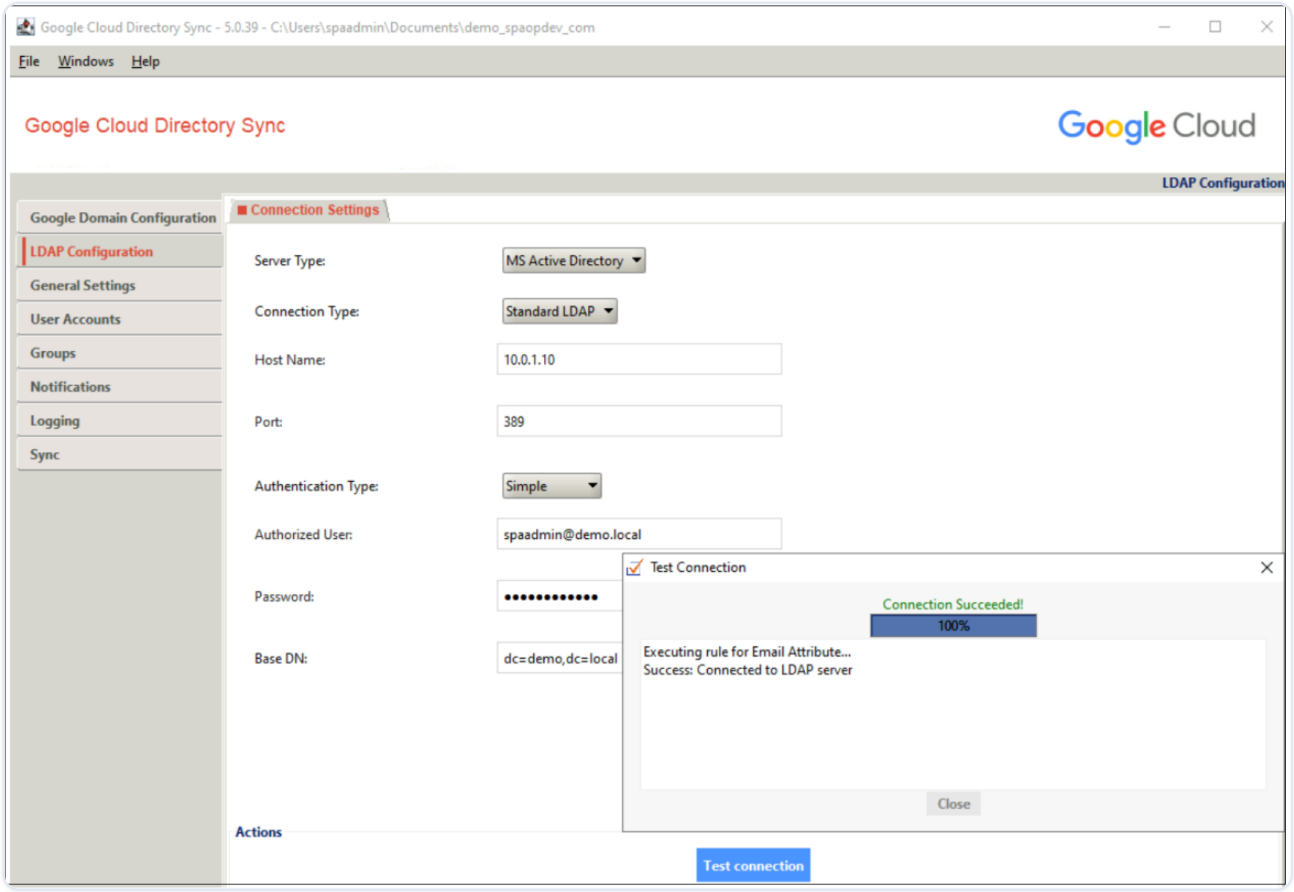
1. Enter the primary domain name.
2. Authorize using OAuth. Click **Authorize Now**. You are prompted to enter your Google Workspace admin credentials and asked to allow access to Google Workspace Directory.

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



LDAP configuration:

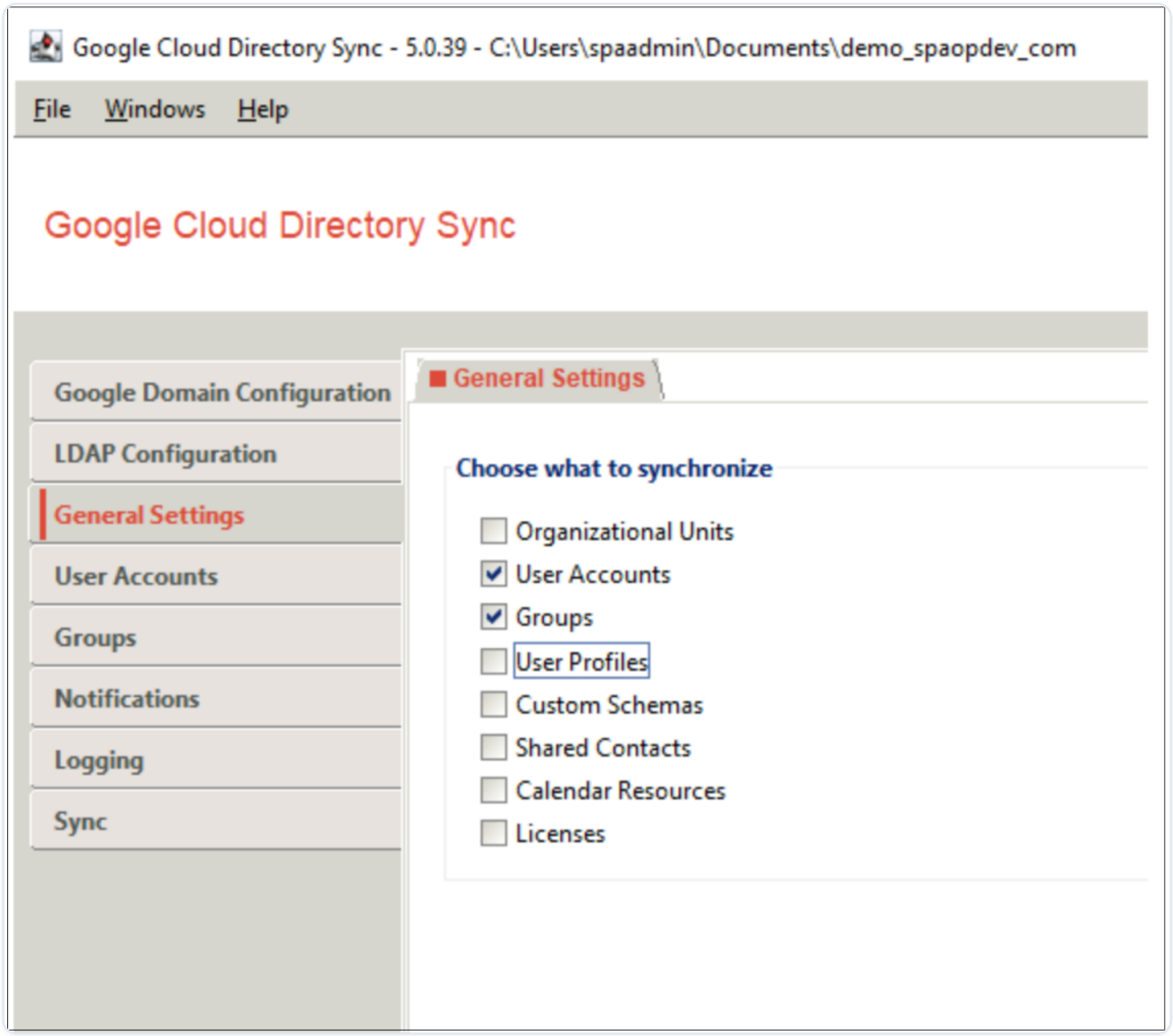
1. Enter the host name, port, authorized user, and password.



General settings:

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

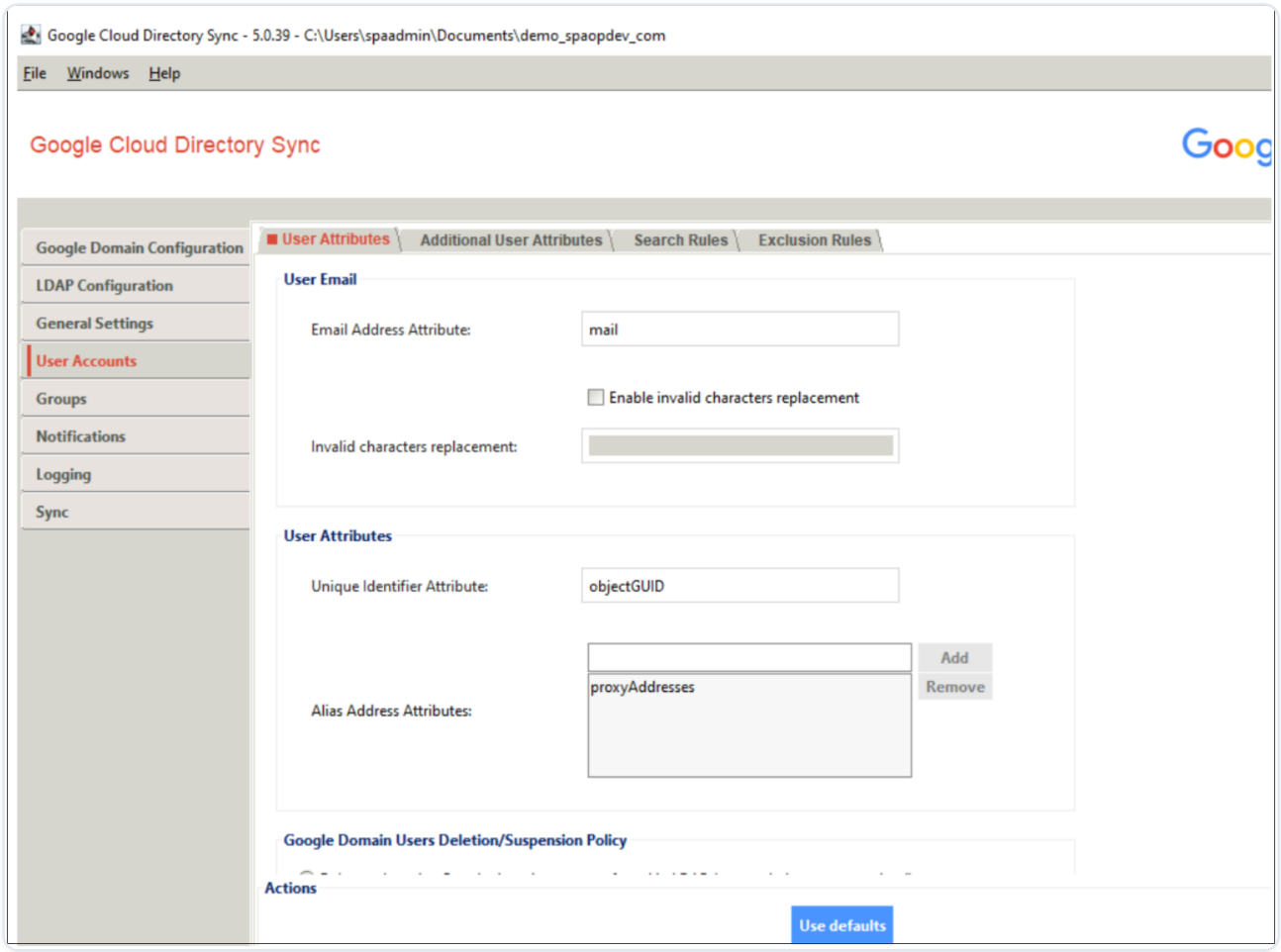
Select the items for the synchronization.

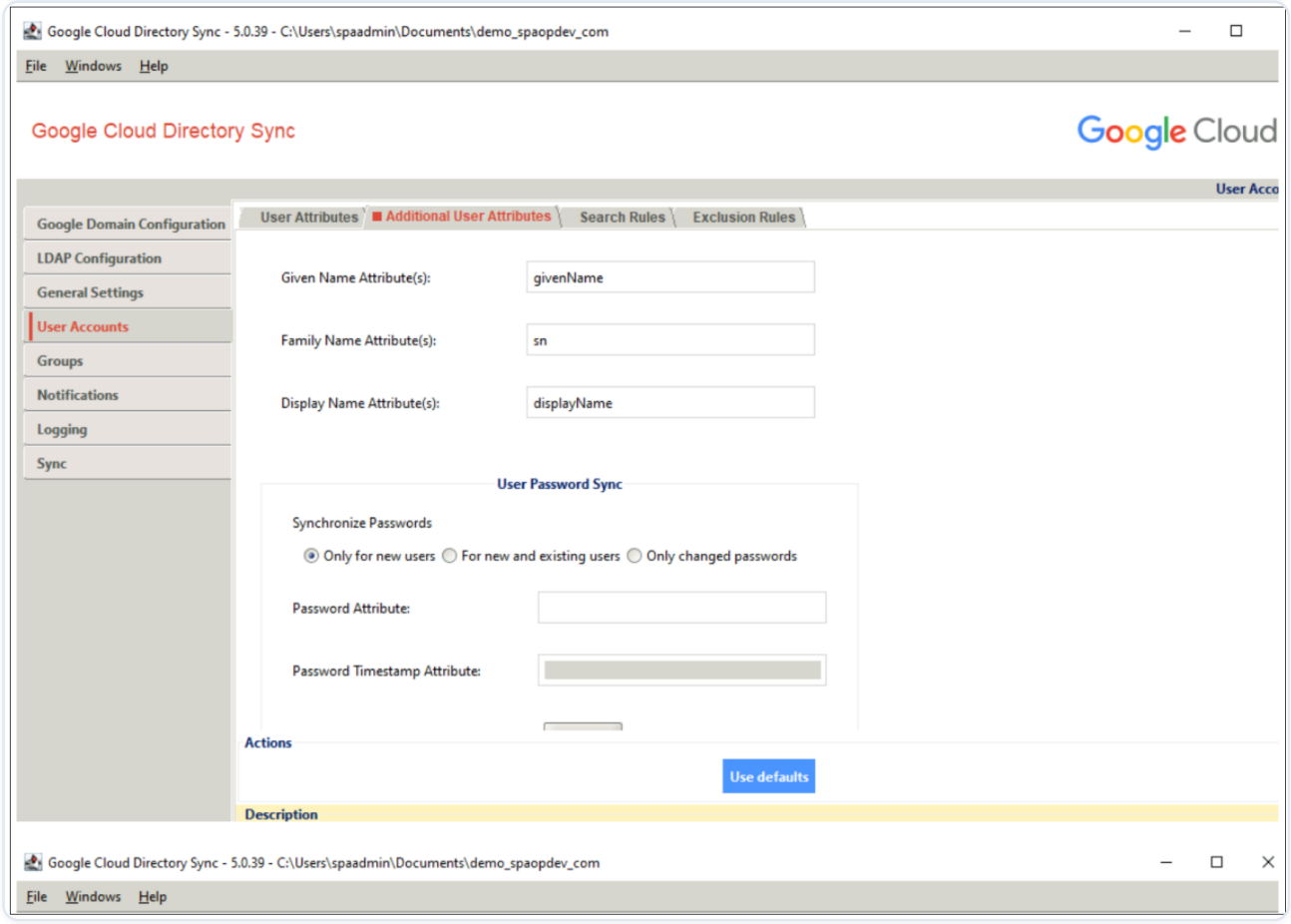


User Accounts:

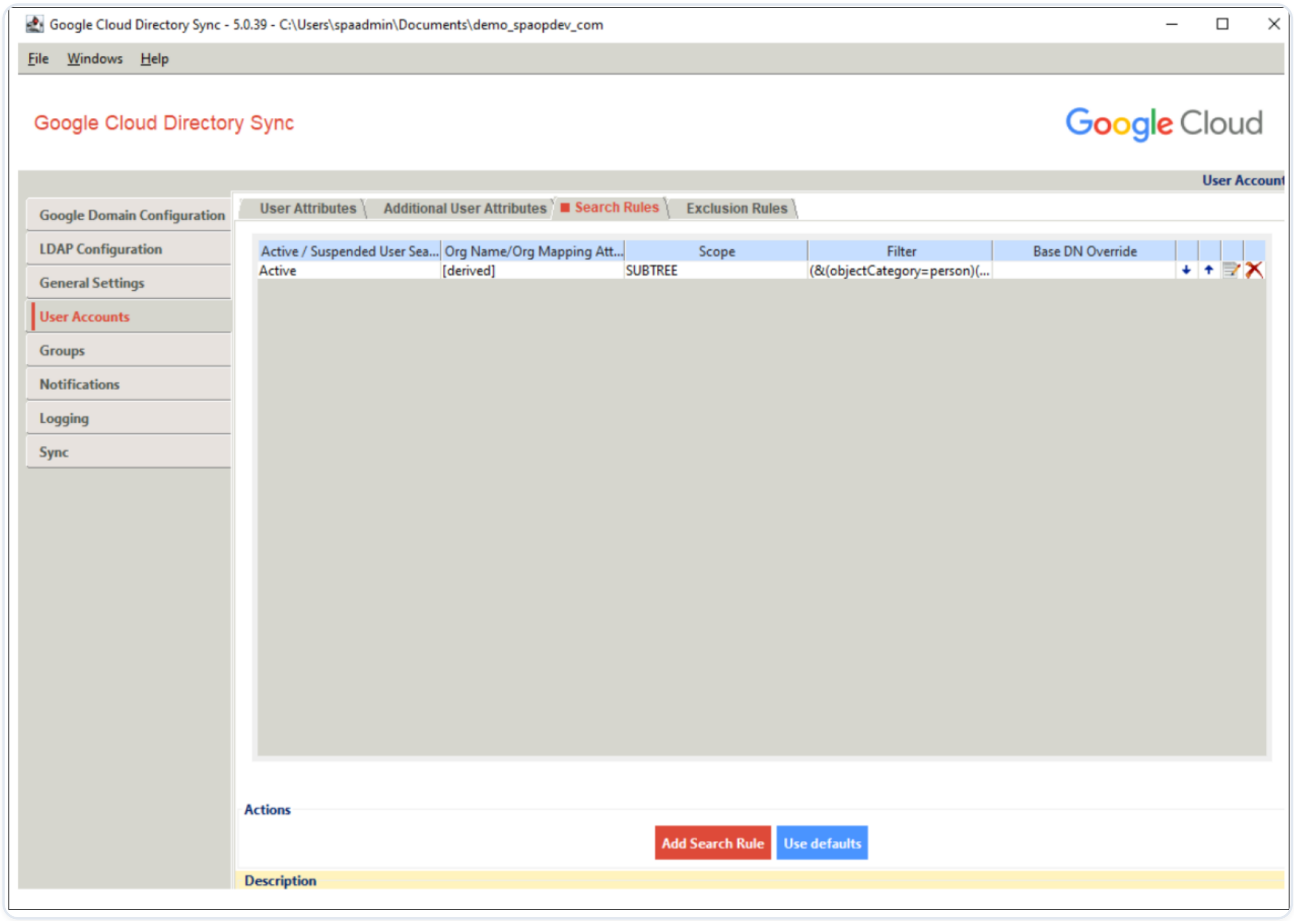
1. Specify which users to import and synchronize.
2. Click **Use defaults** for **User Attributes**, **Additional User Attributes**, and **Search Rules**.

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





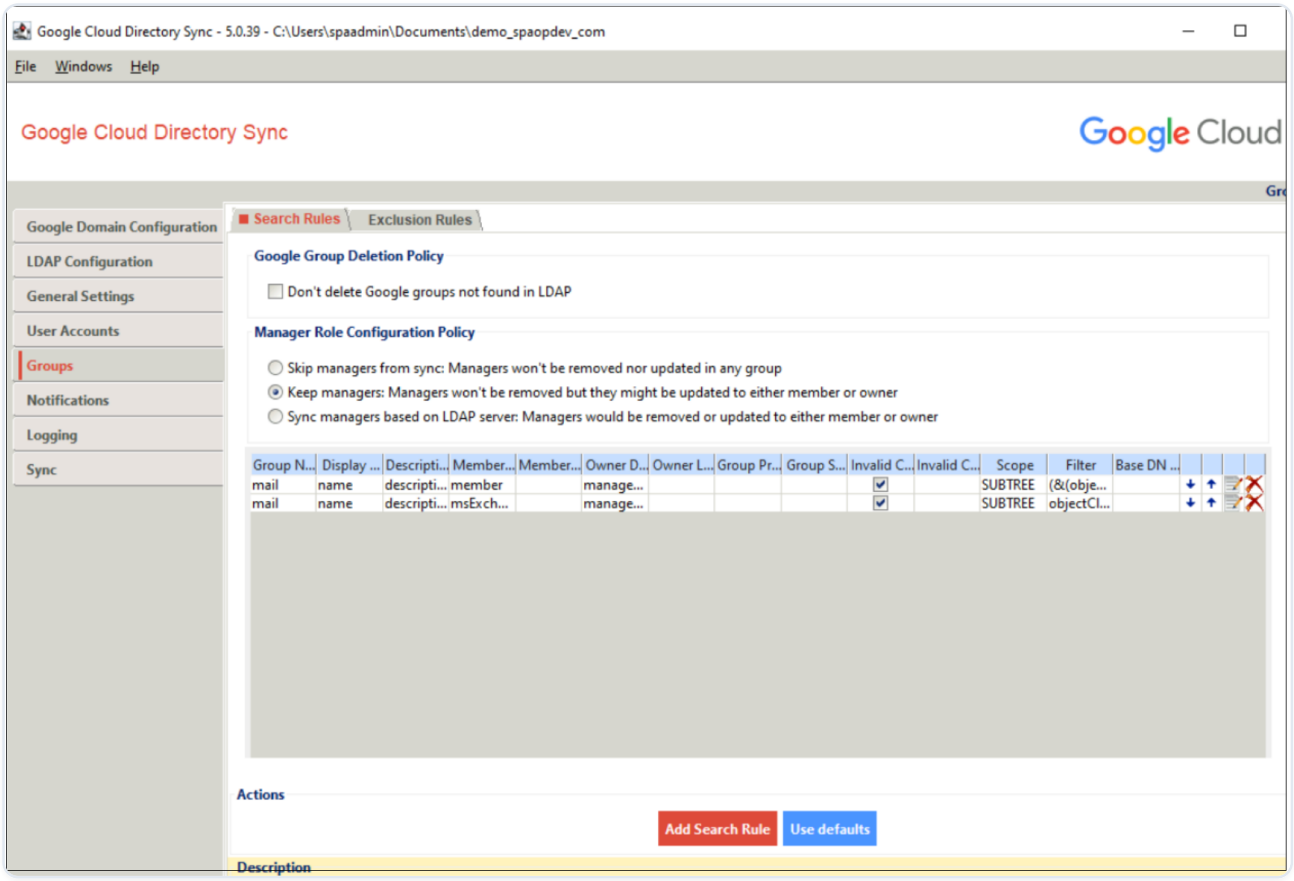
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Groups:

1. Specify which groups to import and synchronize.
2. Click **Use defaults** for groups **Search Rules**.

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



Notifications:

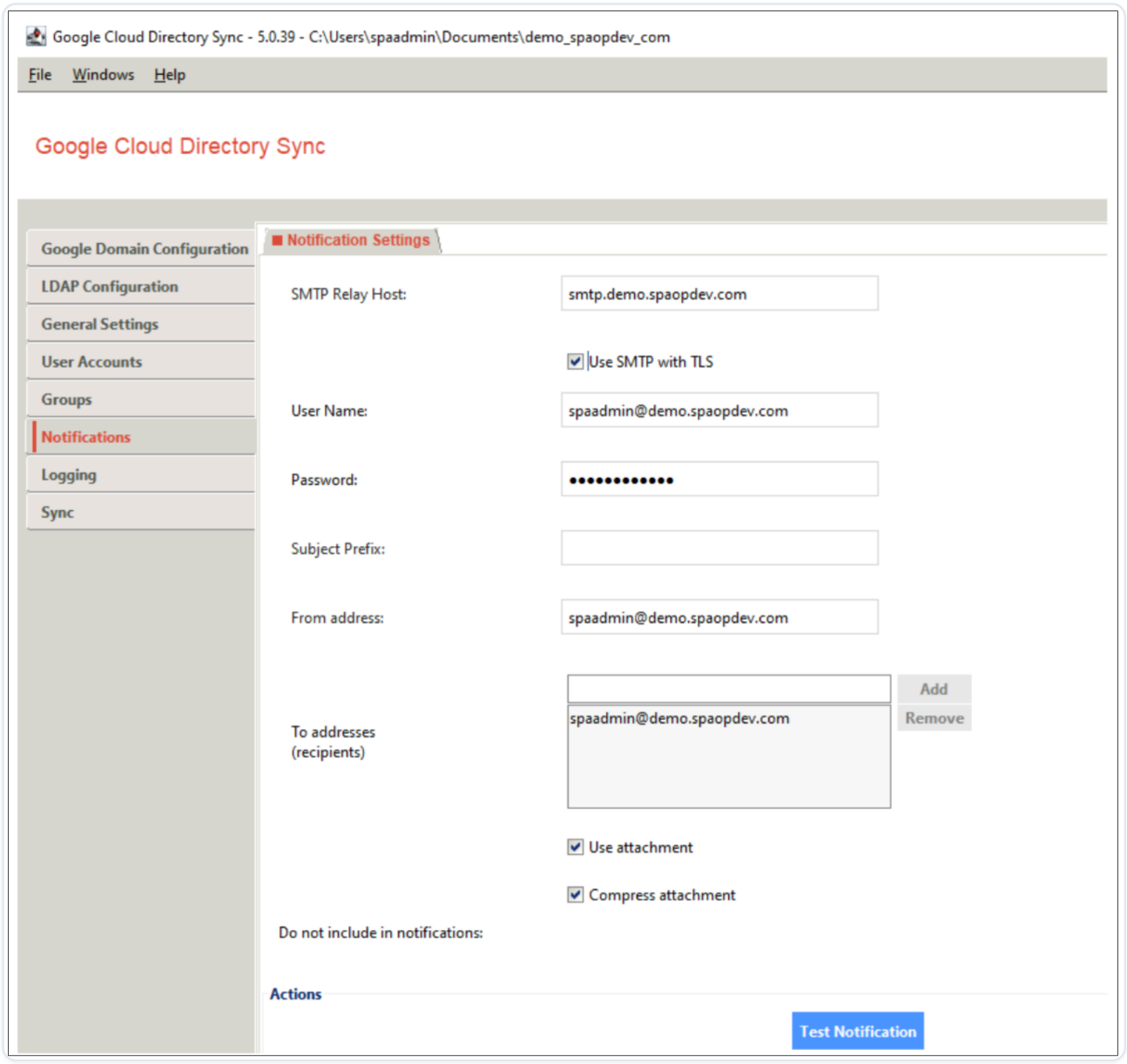
This step is optional.

After synchronization, Google Cloud Directory Sync connects to your SMTP relay host and sends a notification with synchronization details.

- Specify the senders address that you want to appear in the notification header.
- Enter the recipient email addresses one at a time and click the **Add** button for each address.

If the synchronization report exceeds 24 MB, it is compressed and sent as a ZIP attachment.

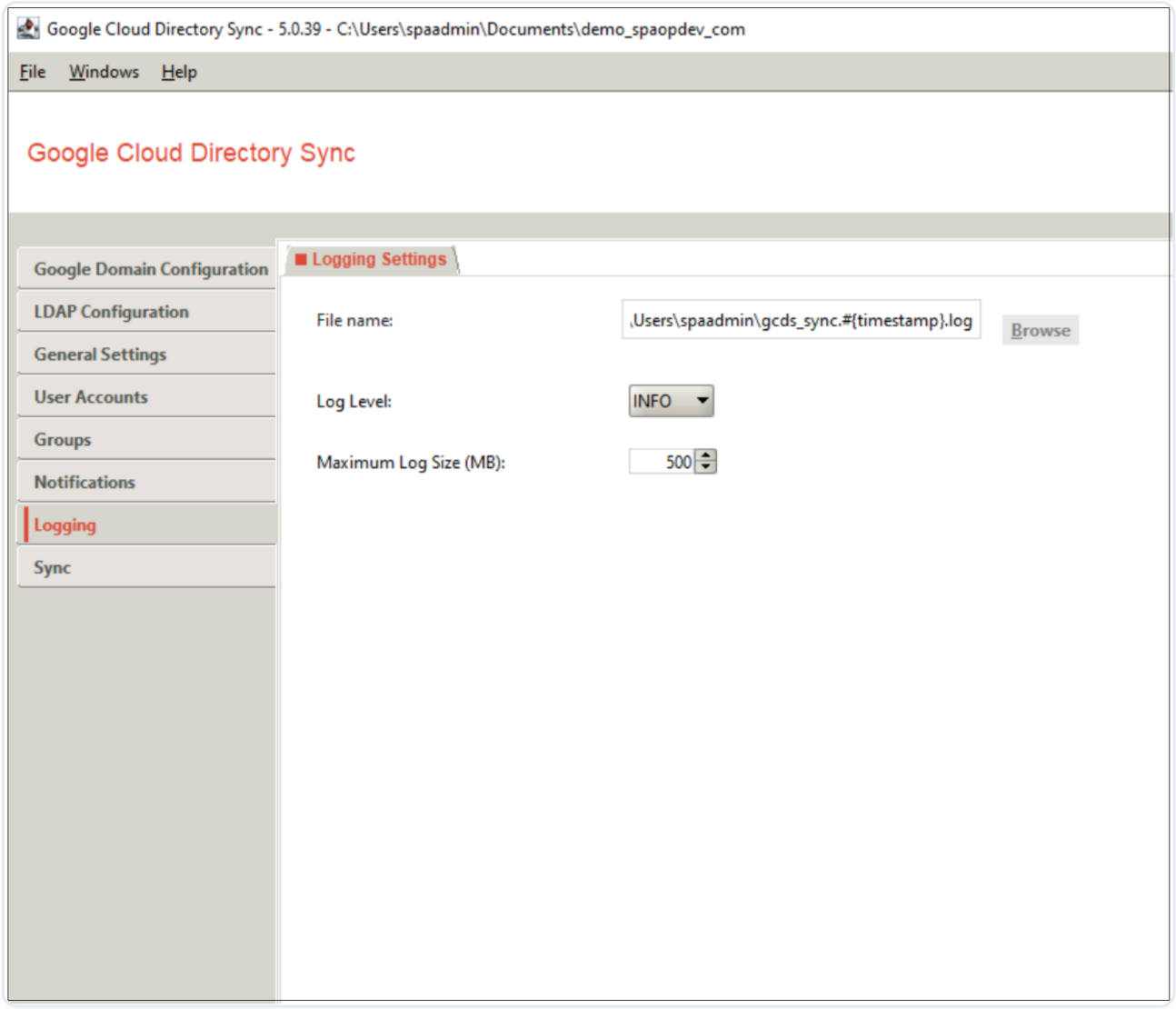
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Logging:

Specify where to write the log file information, the level of detail, and the maximum log file size.

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

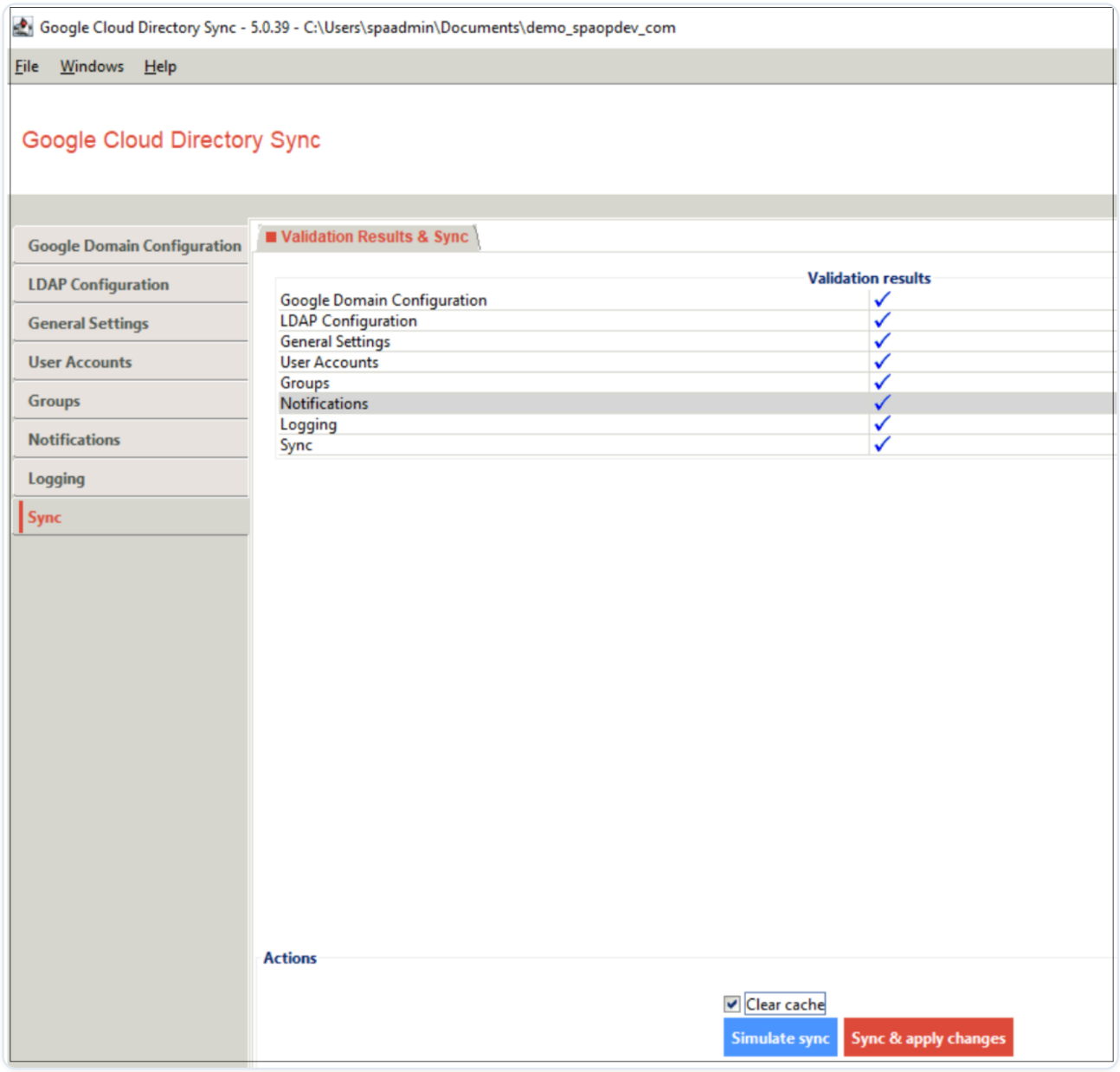


Synchronization:

Review your settings and correct any problems before you synchronize.

- Once your settings are correct, click **Simulate sync** to connect to both servers and generate a list of changes for the simulated synchronization.
- To commit changes, save the configuration file and click **Sync** and apply changes or run `sync-cmd` from the command line.

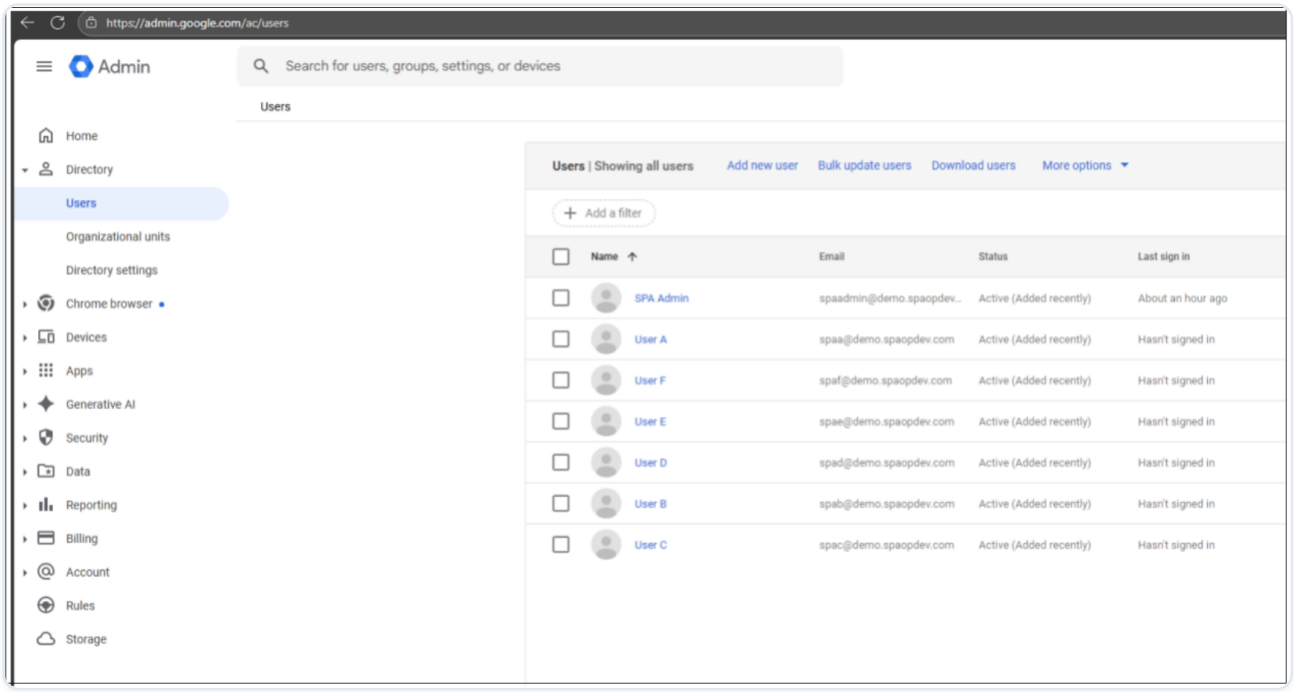
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Google Workspace Directory:

New users are created during the synchronization.

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



Synchronize using CLI:

See Synchronize using the command line.

End user experience

Users can access applications through Citrix SecurAccess™ ZTNA using the following methods. Each access method provides a different user experience allowing organizations to choose the most appropriate approach based on their desired user experience and deployment strategy.

- **Citrix Workspace App** - The native desktop application that provides the most secure and feature-rich access experience with full policy enforcement and single sign-on capabilities.
- **Store URL from a web browser** - A web-based interface that can be accessed through different browser environments:
  - Non-Chrome browsers (such as Firefox, Safari, or Edge)
  - Chrome with non-managed profile (personal Chrome browser without enterprise policies)
  - Chrome with managed profile (enterprise-managed Chrome browser with Chrome Enterprise Premium policies)
- **Chrome managed profile** - Users access applications directly by using bookmarks or manually typing the application URL in the address bar of a Chrome managed profile.

The following table summarizes the end-user experience when the applications are accessed using various methods:

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

	DIRECT	STORE URL FROM A WEB BROWSER	CITRIX WORKSPACE APP
Non-chrome browser	Access denied for SaaS apps (assuming that the SaaS apps have been configured with the appropriate IP address allow list).	Apps are enumerated in the store.	Not-applicable
	Private apps are unreachable.	The applications are launched in the appropriate Chrome managed profile.	
		A profile creation wizard is launched if the respective managed profile has not been created already.	
Chrome (non-managed profile)	Access denied for SaaS apps (assuming that the SaaS apps have been configured with the appropriate IP address allow list).	The applications are launched in the appropriate Chrome managed profile.	Not-applicable
	Private apps are unreachable.	A profile creation wizard is launched if the respective managed profile has not been created already.	
Chrome (managed profile)	Apps are allowed or denied depending on the Citrix SecurAccess ZTNA configuration.	The enumerated app is launched in a new tab.	Not-applicable

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

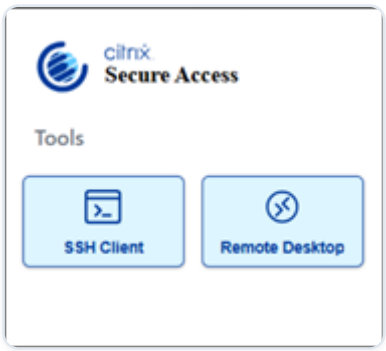
	DIRECT	STORE URL FROM A WEB BROWSER	CITRIX WORKSPACE APP
Citrix Workspace app	Not-applicable	Not-applicable	Apps are enumerated in the store.
			The applications are launched in the appropriate Chrome managed profile.
			A profile creation wizard is launched if the respective managed profile has not been created already.

Citrix SecurAccess™ extension for Chrome Enterprise Premium

The Citrix SecurAccess extension for Chrome Enterprise Premium (CEP) enables secure, clientless access to internal and external applications directly from the Chrome browser. It combines Citrix SecurAccess™ ZTNA and Chrome Enterprise capabilities to deliver enterprise-grade security, Zero Trust access, contextual controls, and a modern user experience.

Organizations can use this extension to provide secure access to SaaS applications, internal web apps, SSH servers, and RDP systems, all without requiring VPNs or native client installations.

The Secure Access browser extension is automatically installed when you integrate Citrix SecurAccess ZTNA with Chrome Enterprise Premium. For setup instructions, see Setup Google Chrome integration. Once installed, you can access the extension from the icon in the upper-right corner of your Chrome browser.



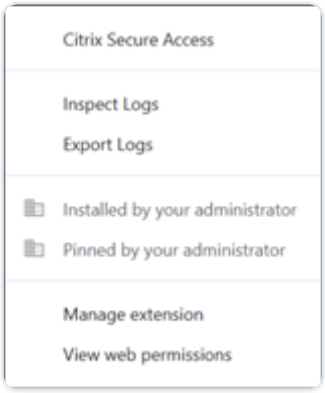
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Access extension logs

The Secure Access browser extension logs are essential for monitoring and troubleshooting. End users can review and download logs to share with administrators or support teams when issues occur.

To review or download logs:

1. Right-click the browser extension icon.
    - Click **Inspect Logs** to review logs.
    - Click **Export Logs** to download logs.



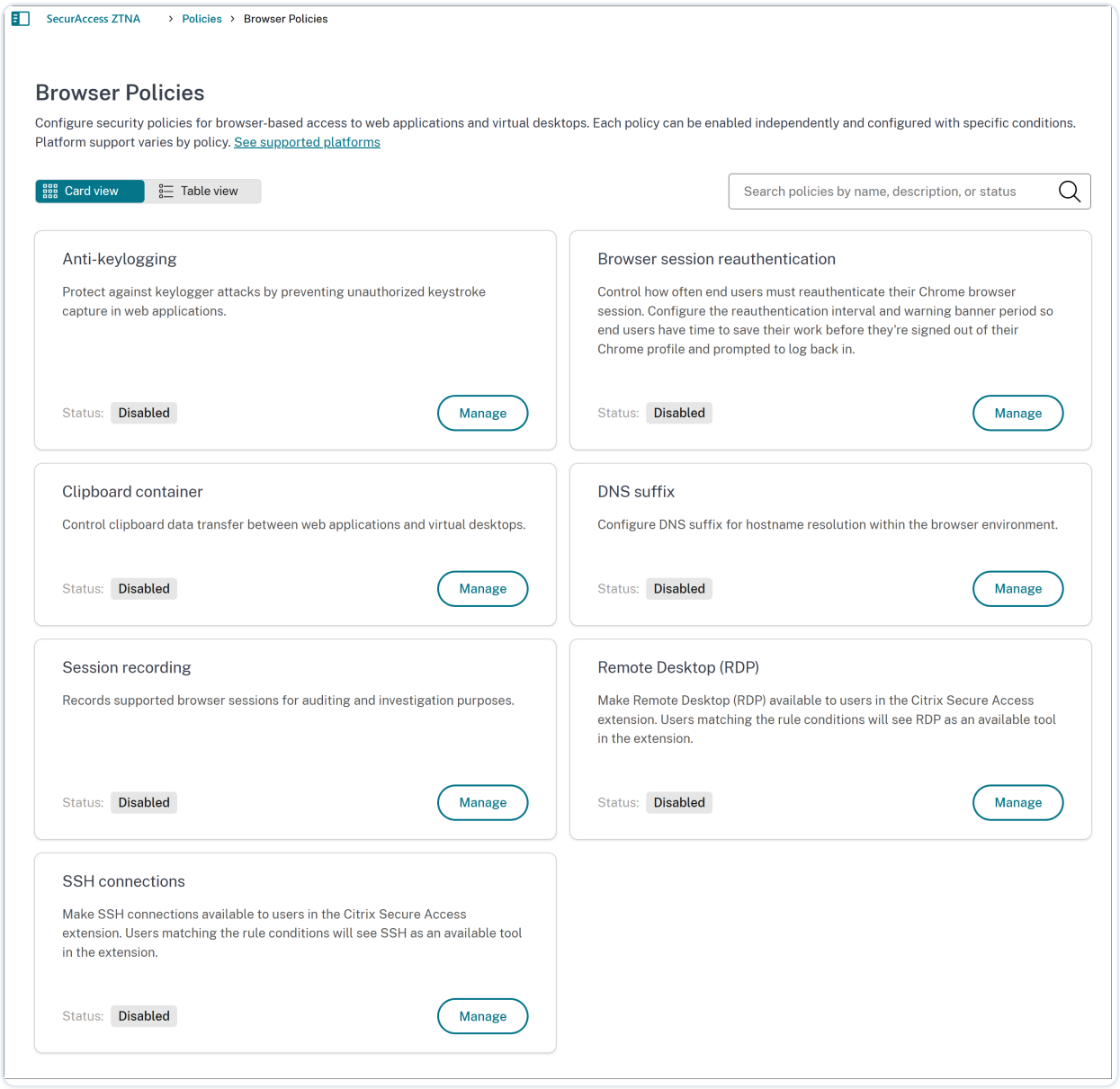
Citrix SecurAccess controls for Chrome Enterprise

Citrix SecurAccess ZTNA supports security policies that are delivered to and enforced by the Citrix SecurAccess extension for Google Chrome Enterprise Premium (CEP). For details, see Supported controls.

You can configure these policies from the Citrix SecurAccess ZTNA admin console.

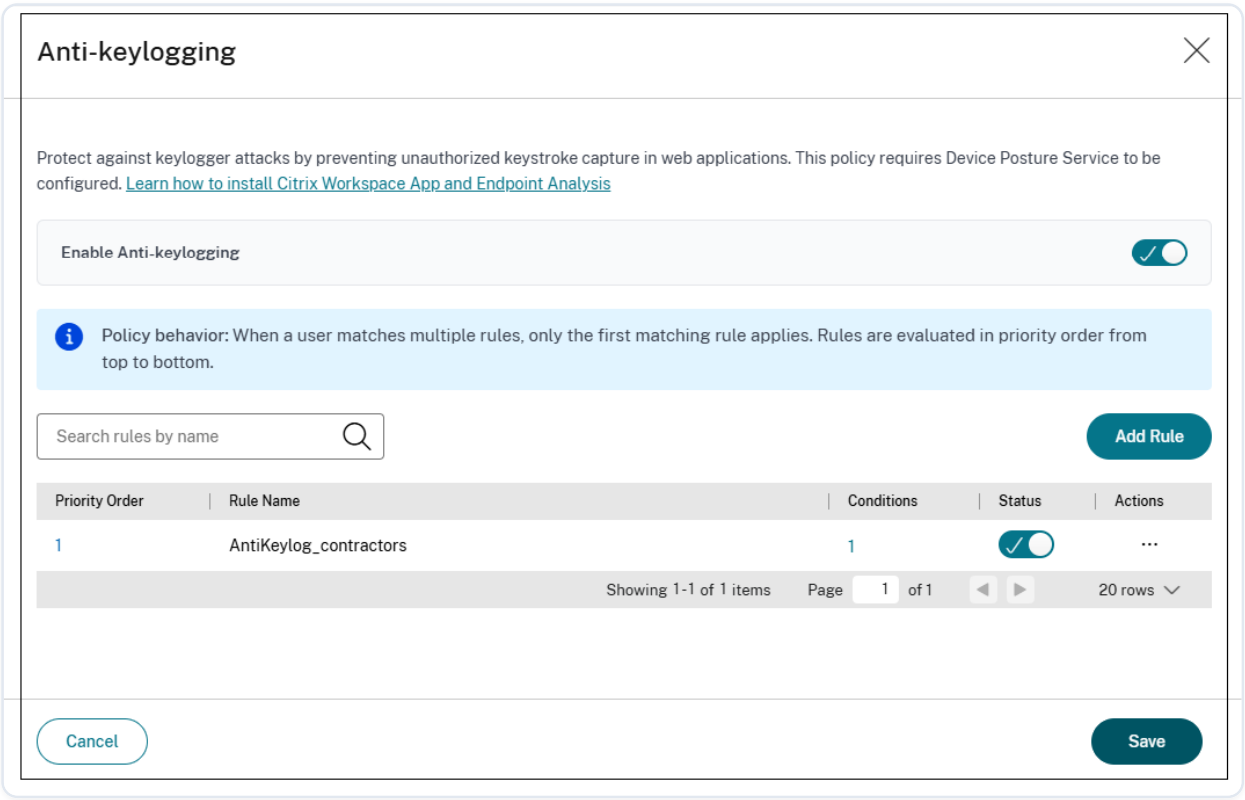
1. Go to **Policies > Browser policies**, and then click **Create browser policy**.
2. Select the policy and then click **Manage**.

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

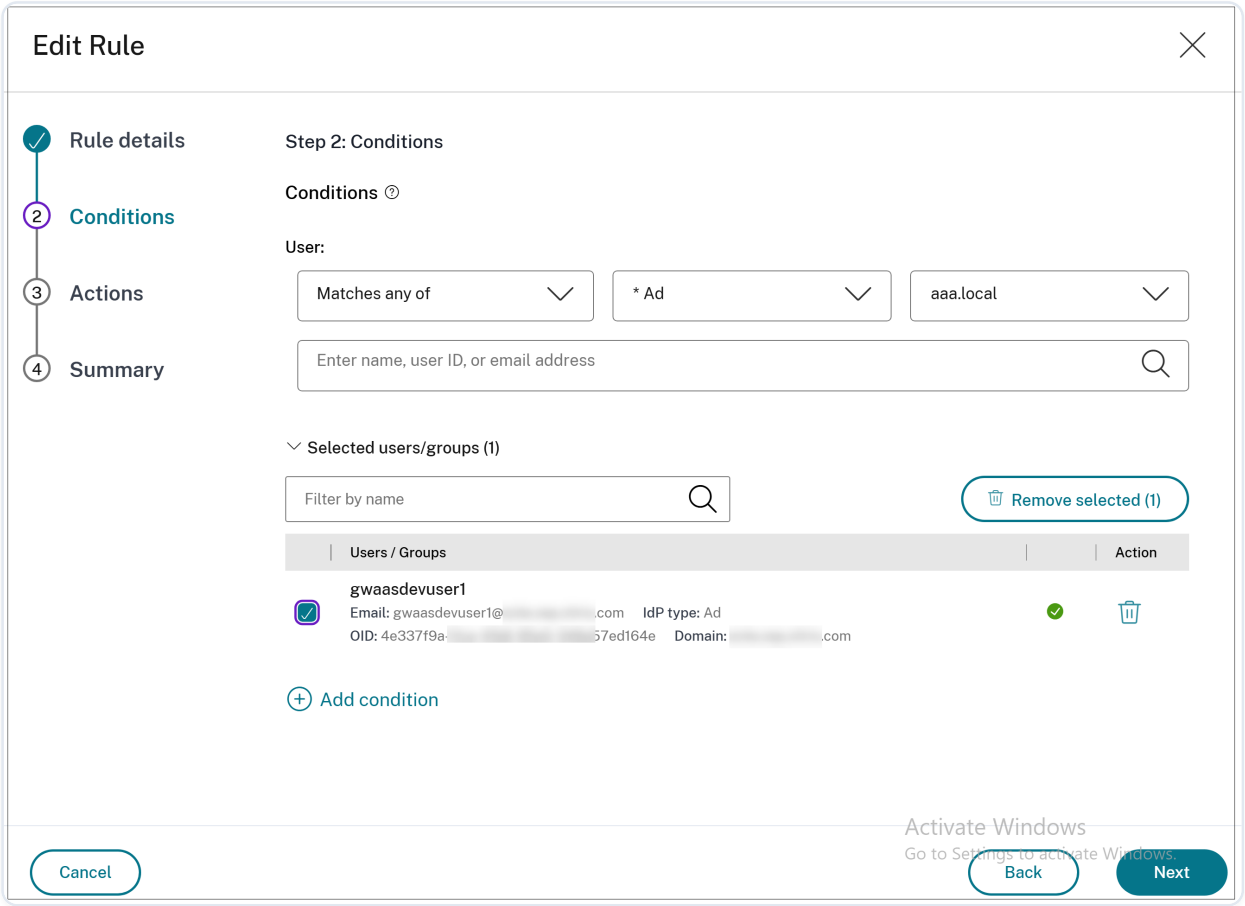


3. Add rules for the policy.

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



4. Select the conditions for which the policy must be evaluated.



Citrix SecurAccess browser policies are supported for both hybrid and service-based Citrix SecurAccess ZTNA deployments with Chrome Enterprise Premium (CEP).

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

For detailed configuration steps, see the documentation for each control.

Supported controls

Citrix supports the following Secure Access controls with the Citrix SecurAccess ZTNA and Chrome Enterprise Premium integration:

CONTROL	WHAT IT DOES
Anti-keylogging	Obfuscates keystrokes to prevent keylogger malware on the endpoint from capturing user input.
Clipboard container	Controls what users can copy and paste between the browser and other apps.
DNS suffix	Automatically completes short internal URLs (like “wiki/”) into full addresses.
Session recording	Records browser session activity for audit and compliance.
Browser session reauthentication	Enforces periodic re-authentication of browser sessions after a configured time interval.
SSH connections	Enables users to establish SSH connections directly within a browser tab, without requiring a terminal client.
Remote Desktop (RDP)	Enables users to launch Remote Desktop sessions directly within a browser tab, without requiring an RDP client.

Users and groups in policies

The following sections provide more information about users and groups:

Search for users or groups

The users and groups that you select appear in a grid. Each row in the grid displays the following identity details so that you can clearly distinguish between identically named users or groups across different domains, forests, or identity providers (IdPs):

- **Name** – The display name of the user or group.

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

- **Email** – The email address associated with the identity.
- **IDP type** – The identity provider, such as Azure AD, Active Directory, Okta, or Google.
- **OID** – The object ID or security identifier of the identity.
- **Domain** – The domain to which the user or group belongs.

You can filter the grid by name, remove individual rows, or select multiple entries and remove them together using **Remove selected**.

Use synchronized users and groups

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Citrix SecurAccess ZTNA policies evaluate correctly only when they use synchronized users and groups. Otherwise, the following warnings might appear:

- **Missing tenant account privileges.**

  Remediation: In the Google Admin console, assign the **Users > Read** and **Groups > Read** privileges to the tenant service account. SPA requires these privileges to verify that a user or group exists.

- **User or group not synchronized.**

  Remediation: The searched or selected user or group is not synchronized with Google Directory. Synchronize the directory entity with Google Directory before using it in an SPA policy.

- **Insufficient group access settings.**

  Remediation: In the Google Admin console, open the access settings for the selected group and make sure the **Who can view members** has at least the **Group members** option selected.

NOTE:

This feature is available only after the Google Chrome integration is successfully completed.

Anti-keylogging control

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

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

The Citrix SecurAccess™ 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 SecurAccess™ ZTNA 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 SecurAccess and Chrome Enterprise Premium (CEP) is complete.

Configure the anti-keylogging policy

1. Log in to the Citrix SecurAccess ZTNA 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

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: Citrix SecurAccess™ ZTNA service and hybrid deployments.

Supported platforms: Windows.

Prerequisites

Ensure that the following prerequisites are met:

- Integration between Citrix SecurAccess 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

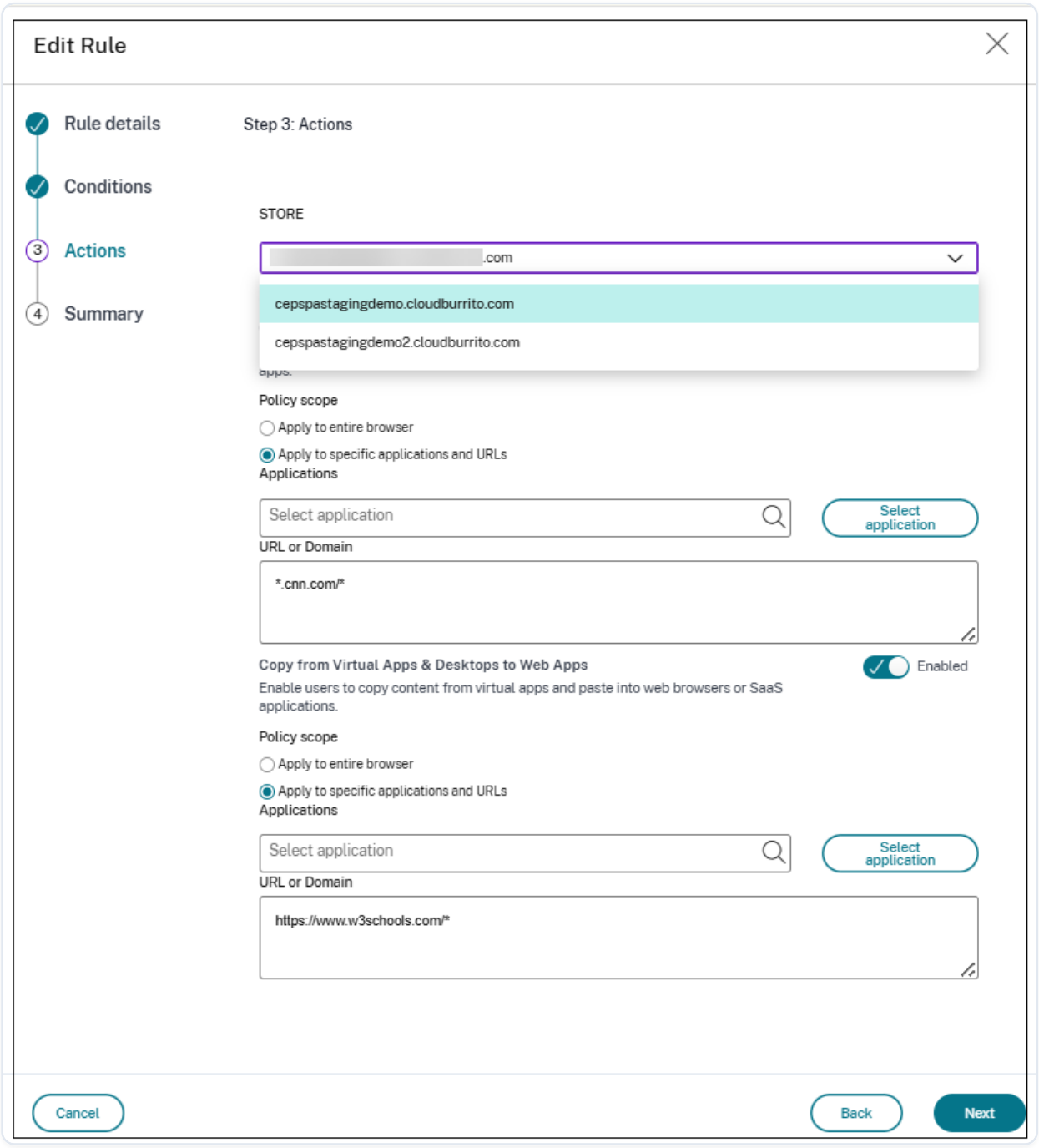
1. Log in to the Citrix SecurAccess ZTNA admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Clipboard container**, and then click **Manage**.
4. Click **Add Rule** to add rules for the clipboard share between VDA and browser.
   a. Enter the 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**.
   c. Click **Next**.

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

d. Define the URL and Citrix SecurAccess ZTNA 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.



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

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

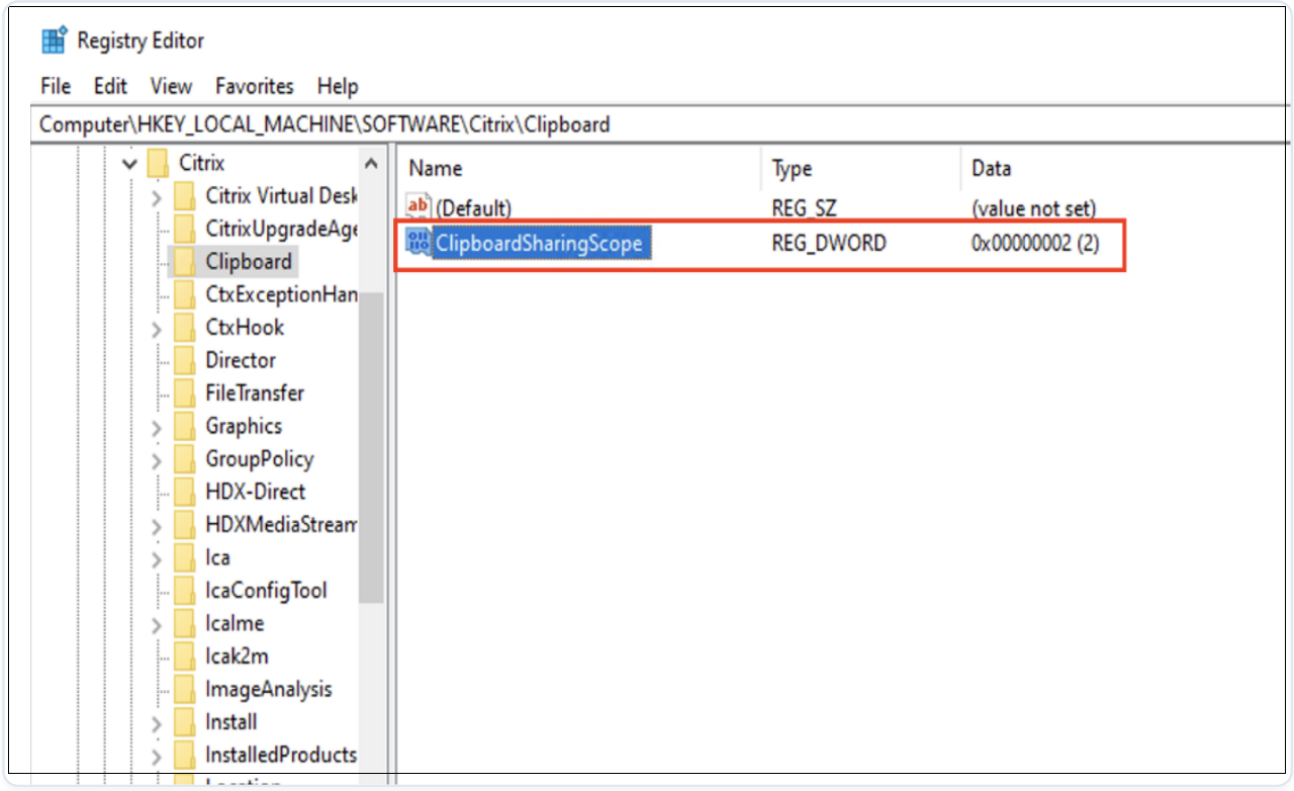
For VDA version 2607:

See How it works.

For VDA version 2507:

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

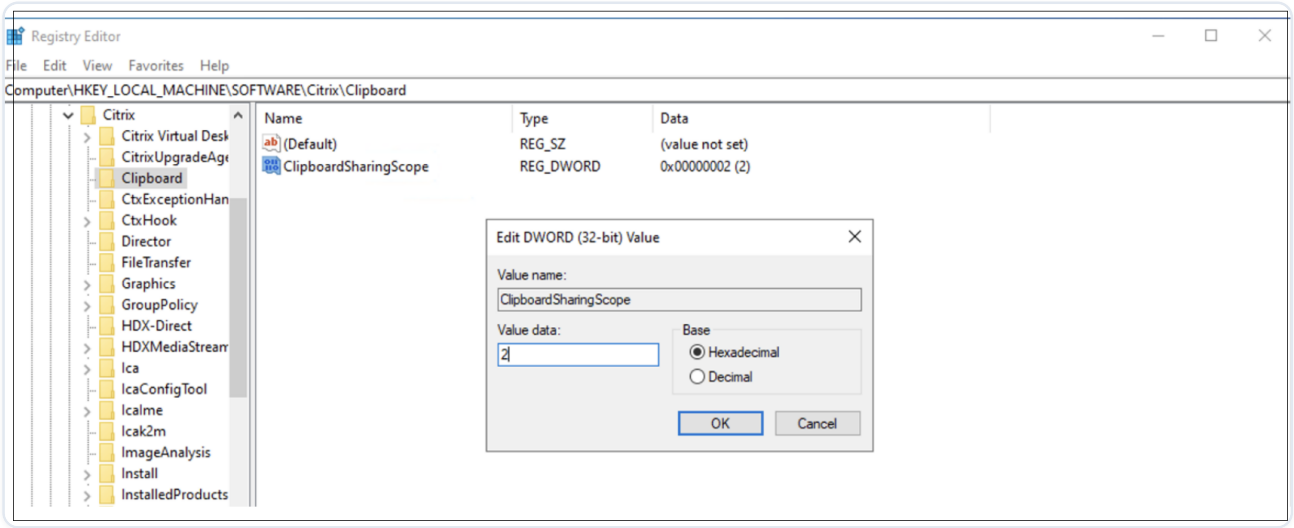
1. Open the Windows Registry Editor using regedit.exe.
2. Navigate to HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\.
3. Create a REG_DWORD value named `ClipboardSharingScope`.



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.

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

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



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

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

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 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: Citrix SecurAccess™ ZTNA service and hybrid deployments.

Supported platforms: Windows and macOS.

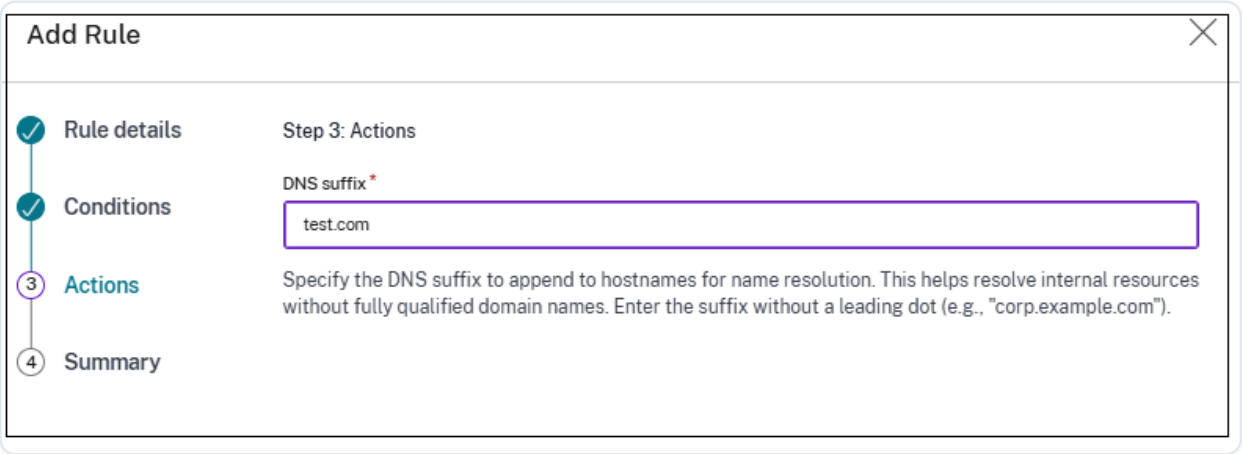
Prerequisites

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

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

Configure DNS suffix

1. Log in to the Citrix SecurAccess ZTNA 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.



5. Click **Save**.

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

Session recording control

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.

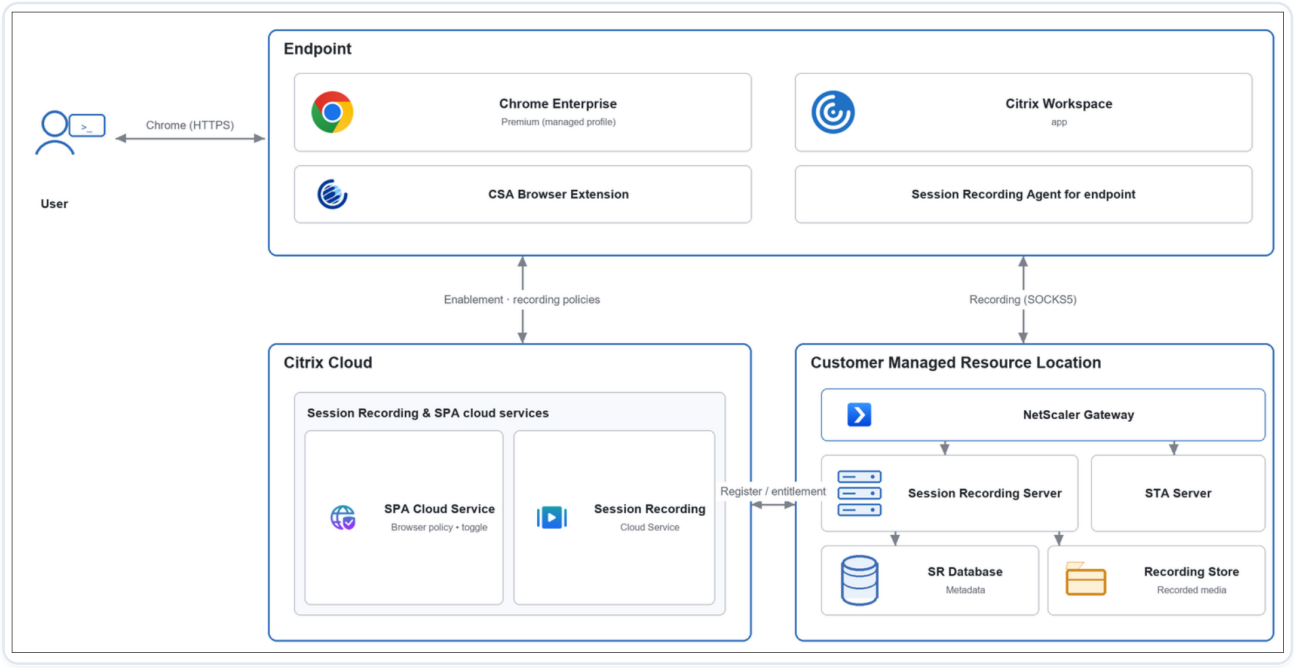
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For details, see Benefits.

Architecture

The session recording solution spans three planes:

- The endpoint with the managed Chrome profile, Citrix SecurAccess™ extension, and Session Recording Agent for endpoints.
- The Citrix Cloud control plane, which houses the Citrix SecurAccess™ ZTNA 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.



Prerequisites

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

System requirements

- Citrix SecurAccess ZTNA, 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:

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

- 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.

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 Citrix SecurAccess ZTNA deployment types. Even with the Citrix SecurAccess ZTNA 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 Citrix SecurAccess ZTNA

1. Log in to the Citrix SecurAccess ZTNA 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.

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

- 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.

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 SecurAccess ZTNA 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

Citrix SecurAccess™ ZTNA 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: Citrix SecurAccess ZTNA service and hybrid deployments.

Supported platforms: Windows, macOS, Linux, ChromeOS.

Prerequisites

Ensure that the following prerequisite is met:

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

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

Enable Browser session reauthentication control

1. Log in to the Citrix SecurAccess ZTNA admin console.
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**.

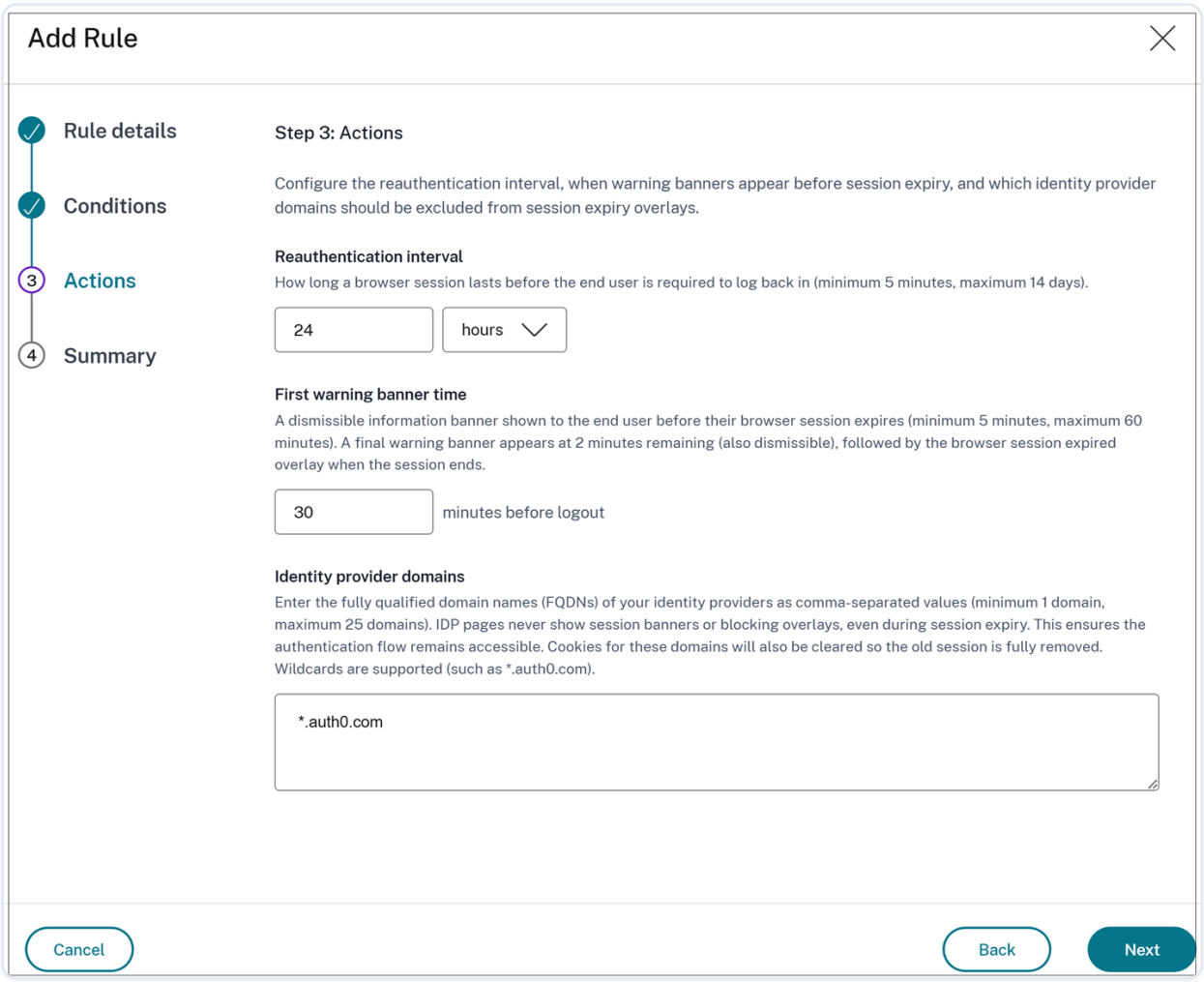
    b. Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.

    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

Citrix SecurAccess™ ZTNA 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.

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

NOTE:

- This feature is applicable for Chrome Enterprise Premium integrated Citrix SecurAccess ZTNA setup for hybrid and cloud deployments. For details, see the following topics:
- You must have admin rights to configure Citrix SecurAccess ZTNA 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 SecurAccess ZTNA is configured for the integration.

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

- Access policies to allow SSH traffic must be created in the Citrix SecurAccess ZTNA admin console.

Prerequisites

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

- Citrix SecurAccess ZTNA 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 SecurAccess browser extension.
- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix SecurAccess ZTNA
  - Hybrid deployment – System requirements and prerequisites

Configure Citrix SecurAccess ZTNA for SSH access

1. Log in to Citrix Cloud and then click **Citrix SecurAccess ZTNA**.
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 Citrix SecurAccess ZTNA.
   - 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 Citrix SecurAccess ZTNA 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**.

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

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 > SSH** tab.

Remote Desktop control

Citrix SecurAccess™ ZTNA 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 Citrix SecurAccess ZTNA setup for hybrid and cloud deployments. For details, see the following topics:
- You must have admin rights to configure Citrix SecurAccess ZTNA 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

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

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 SecurAccess ZTNA is configured for the integration.
- Access policies to allow RDP traffic must be created in the Citrix SecurAccess ZTNA admin console.

Prerequisites

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

- Citrix SecurAccess ZTNA 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 SecurAccess browser extension.

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

- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix SecurAccess ZTNA
  - Hybrid deployment – System requirements and prerequisites

Configure Citrix SecurAccess ZTNA for RDP access

1. Log in to Citrix Cloud and then click **Citrix SecurAccess ZTNA**.
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 Citrix SecurAccess ZTNA.
   - 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 Citrix SecurAccess ZTNA 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.

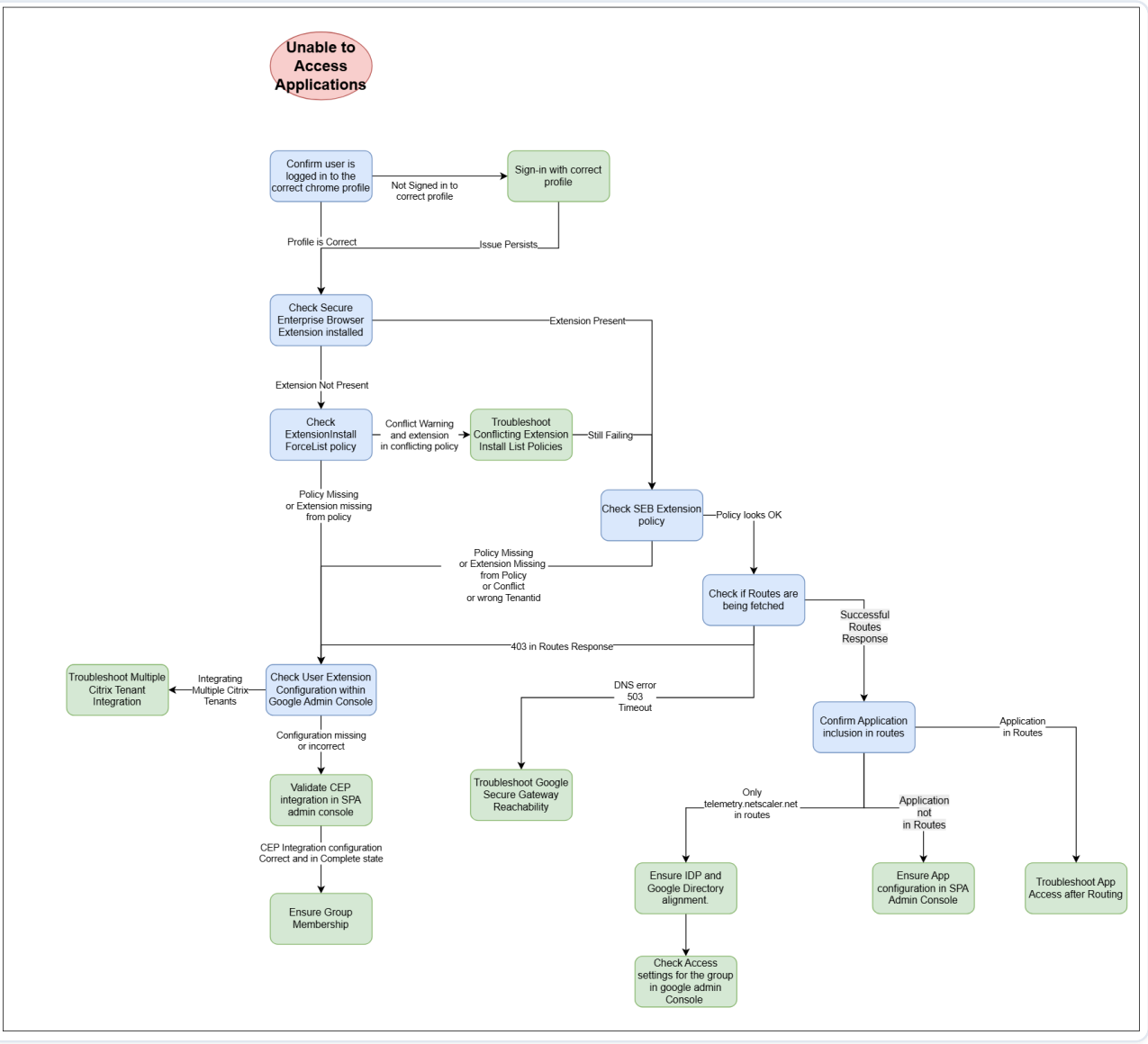
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot CEP integration issues

This article provides a troubleshooting workflow for customer admins who have completed Chrome Enterprise Premium (CEP) integration with Citrix SecurAccess™ ZTNA and are unable to access applications.

Basic assumptions:

- The customer administrator has completed directory synchronization with Google Directory.
- The customer has successfully completed Chrome Enterprise onboarding in Citrix SecurAccess ZTNA.
- Applications and access policies are configured in the Citrix SecurAccess ZTNA admin console to allow access to the relevant applications for the user or a group the user belongs to.
- The user is logging in to the onboarded domain.
- The browser has internet connectivity.



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

Diagnostic logs for CEP troubleshooting

To streamline investigation, collect the following diagnostic information before opening a support case and include it with every submission.

1. Export Chrome policies.
    a. Open Chrome and navigate to chrome://policy/.
    b. Click **More Actions** and then select **Export to JSON**.
    c. Attach the exported file to your support case.
2. Enable Verbose Logging for the Secure Enterprise Browser extension.
    a. Click the ellipsis icon next to the Secure Enterprise Browser extension.
    b. Click the options and then set **Log level** to **All**.
    c. Close and reopen Chrome.
    d. Go back to the extension options (ellipsis icon), and then click **Download the log**.
3. Collect the extension Log.
    a. Close and reopen Chrome.
    b. Repeat step 2 to access the **Extension** options, then click **Download the log**.
    c. Attach the downloaded file to your support case.
4. Capture a network log.
    a. In Chrome, navigate to chrome://net-export/ and click **Start Logging to Disk** (the default file name is chrome-net-export-log.json).
    b. Access a few SaaS and web applications, then return to chrome://net-export/ and click **Stop Logging**.
    c. Attach the resulting file to your support case.

Confirm that user is logged in to the correct Chrome profile

How to check: On the top right corner of the Chrome browser, click the profile icon. It must show the correct user and correct domain for the profile through which you intend to access your applications.

Also, ensure that the profile doesn't show **Paused** or **Click to Sign-in**. If it does, you must re-authenticate.

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

- **Profile is correct and authenticated:** Proceed to Check Secure Enterprise Browser Extension installed.
- **Profile is incorrect or not authenticated:** Log in or re-authenticate with the correct profile. Ensure that the domain suffix of the user's email aligns with the domain of the Google Admin account that is installed with Citrix SecurAccess ZTNA.

Check Secure Enterprise Browser extension installed

How to check: On the top right corner of the Chrome browser, there must be a green shield icon that corresponds to the Secure Enterprise Browser extension. You might need to click the jigsaw puzzle piece to see all the extensions.

- **Extension present:** Proceed to Check Secure Enterprise Browser Extension policy.
- **Extension not present:** Proceed to Check ExtensionInstallForcelist policy.

Check ExtensionInstallForcelist policy

How to check: Navigate to chrome://policy and under **Chrome Policies** look for a policy named **ExtensionInstallForcelist**. Click **show more** at the end of the corresponding row to see the details of the policy.

Within this force list, you expect to see an extension with the ID: `ekajlcmdfcigmdbphhifahdfjbkciflj`. This corresponds to the Secure Enterprise Browser extension.

It is possible that you are presented with a warning suggesting that there are two conflicting policies.

- **Conflict warning and extension in conflicting policy:** Proceed to Troubleshoot conflicting extension install list policies.
- **Policy missing:** Complete absence of the policy suggests that the user is not configured to use Secure Enterprise Browser and you must Check user extension configuration within Google Admin Console.
- **Extension missing from policy:** Proceed to Check user extension configuration within Google Admin Console.

Troubleshoot conflicting extension install list policies

Having conflicting policies isn't necessarily a blocker for supporting CEP with Citrix SecurAccess ZTNA. However, the effective policy must force the installation of the following three extensions:

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

- Secure Enterprise Browser (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- Citrix SecurAccess (`loifegnemklkgbmonigcdkmniboielgl`)
- Endpoint Verification (`callobklhcbilhphinckomhgkigmfocg`)

To resolve extension policy conflicts for Citrix SecurAccess ZTNA, follow these steps based on Chrome Policy Hierarchy Guide.

1. **Identify the conflict:** Navigate to `chrome://policy`. Locate **ExtensionInstallForcelist** and check the **Status** and **Source**.
2. **Analyze precedence:** Note that machine-level policies (GPO) generally supersede cloud/user-level policies.
3. **Harmonize:** Ensure the highest-precedence policy includes all three required extension IDs (it's OK if additional extensions are included). Alternately, if the browser and the profile are managed by the same Google Workspace organization, you can use the Policy Merging feature.
4. **Verify:** Click **Reload policies**. The **Applies to** and **Level** columns must confirm that the required extensions are **Mandatory** and active at the effective level.

If the issue persists even after correcting the extension install list policy, then proceed to Check Secure Enterprise Browser Extension policy.

Check Secure Enterprise Browser Extension policy

How to check: Navigate to chrome://policy and under **Secure Enterprise Browser** look for a policy named **securityGateway**. Click **Show More** to display the full policy configuration. Its value is expected to have the following format:

```
{

  "authentication": {},

  "context": {

    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"

  },

  "externalHelper": {
```

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

```
    "id": "com.citrix.device_posture_context_provider",
    "metadata": {
      "action": "device/metadata",
      "input": [
        {
          "key": "tenantId",
          "stringValue": "<tenant_id>"
        }
      ]
    }
  },
  ...
}
```

Ensure that the `tenant_id` field has a value that corresponds to your Citrix Cloud Tenant ID. If this value is different, it might be that a second tenant is configured to integrate with this Google Account.

- **Policy missing or empty:** Complete absence of the policy suggests that the Secure Enterprise Browser extension is configured not only by Citrix SecurAccess ZTNA but by the customer as well, and the user is picking up the extension empty configuration from a previous or manual configuration. You must Check user extension configuration within Google Admin Console.
- **Policy is populated with wrong Citrix Tenant ID:** If the policy is present but the value doesn't line up with the example, either the tenant ID is different or there are two conflicting policies. Proceed to Check user extension configuration within Google Admin Console.
- **Policy looks correct:** Proceed to Check if routes are being fetched.

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

Check user extension configuration within Google Admin Console

How to check: Navigate to https://admin.google.com. From here, go to **Chrome Browser > Apps & Extensions**. Within this view, you must find all policy configurations that are being applied.

Click the **Overview** tab (assuming it is present) and select the **Secure Enterprise Browser** app. To the left, under **Installation policy** it must read **Force installed and pinned in \<primary domain\>**, where \<primary domain\> corresponds to the top-level Organizational Unit of your Google Admin Console.

When clicking through to see the extension **Deployment Settings**, look for the **Policy for extensions** configuration. This must look like what is described in the Check Secure Enterprise Browser Extension policy section.

- **Single policy that appears correct:** If the policy for the parent OU looks correct, you must ensure the user that you are testing with belongs to the account in question and also that there is no other configuration at a sub-OU or group level that might be overriding the parent OU's policy. If the membership is confirmed but still the issue persists, reach out to Citrix Support.
- **Policy missing:** Complete absence of the policy suggests that this Google account is not configured to use Secure Enterprise Browser and you must Validate CEP integration in the Citrix SecurAccess ZTNA admin console.
- **Multiple policies - Multiple Citrix accounts:** If you see multiple configurations for the Secure Enterprise Browser extension, then this might be a cause for incorrect configuration of the associated policy. Associating multiple Citrix accounts to the same Google account is not prohibited but might cause the integration not to function.
- **Multiple policies - Single Citrix account:** If you are integrating only one Citrix tenant, you must ensure that no other admin functions in your organization might be configuring this extension. If you are confident there is no one else providing policy configuration for this extension, you can proceed to remove those policy configurations that don't correspond to the Citrix tenant against which you have integrated through the Citrix SecurAccess ZTNA Admin Console.

  If you remove the superfluous extension configurations and, after restarting the browser you are still unable to access your applications, reach out to Citrix Support.

Check if routes are being fetched

How to check: Navigate to chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj or right-click the Secure Enterprise Browser extension and select **Options**.

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

Set log level to **ALL** and click **SHOW LOG**. Once the log shows up, close the browser and repeat the process to go to the log page. This ensures that you have retrieved the full set of logs necessary for troubleshooting.

Within the log, search for a log line containing:

```
Calling 'https://api.prod.securegateway.goog/api/v1/routes'
```

This must be followed by a response such as:

```
[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog',...
```

- **Contextual Routes show a 403 status code in the logs:** This 403 might be returned by an intercepting firewall such as Zscaler, Umbrella, and so on.
  - In this case, ensure that the traffic bound for Google Security Gateway is allowed as per Prerequisites for the integrated solution.
  - If not, then it is likely an authentication issue with the user profile and might imply incomplete integration of Citrix SecurAccess ZTNA with CEP. Proceed to Validate CEP integration in the Citrix SecurAccess ZTNA admin console.
- **Contextual Routes show timeout, a DNS error or 503 error:** Proceed to Troubleshoot Google Secure Gateway reachability.
- **Contextual Routes appears successful (200 OK):** Proceed to Confirm Application inclusion in routes.

Validate CEP integration in the Citrix SecurAccess ZTNA admin console

Visit the **Browser Settings** section within Citrix SecurAccess ZTNA of the Citrix Cloud console.

In this section, verify the following:

- **Google Chrome integration status** must read as **Complete**. If you find that it has failed, ensure that you have completed the prerequisite steps for CEP integration per the documentation and retry. If the issue persists, reach out to Citrix Support.
- **Customer ID** must have a value that corresponds to the Google account you are integrating with. You can find the value in your Google Admin Console under **Account > Account settings**.

If all the above values are correct but you are still not getting the correct extension configuration in your Chrome browser, reach out to Citrix Support.

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

Troubleshoot Google Secure Gateway reachability

How to check: Copy the URL `https://api.prod.securegateway.goog/api/v1/routes` and navigate to this URL in the browser location bar. You must get an HTTP 401 error response. This is an expected behavior and indicates that a network connection to the Google Secure Gateway can be successfully established.

- **DNS Resolution error:** This suggests that your company might have some restrictive DNS resolution configuration in place that prevents lookup of the Google Security Gateway FQDN. However, this is a prerequisite for the use of this feature and the respective FQDN must be resolvable.
- **The request hangs or is presented with a timeout error page:** This strongly suggests that a firewall between the browser and the internet is dropping traffic bound for Google's Security Gateway. Follow the Prerequisites for the integrated solution to ensure that the prerequisite internet locations are reachable from your network.

If you are still not receiving the correct routes, reach out to Citrix Support.

Confirm application inclusion in routes

A successful routes response includes FQDNs that correspond to applications configured by your Citrix SecurAccess ZTNA admin. For example:

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog',
endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'},
{hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname:
'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}.
```

Does this line include the application you are trying to access?

- **The inaccessible application is included in the routes response:** Proceed to Troubleshoot routed application access.
- **Only telemetry.netscalergateway.net is included in the routes response:** Try configuring an additional application and inclusive application policy. If you are still not seeing it in the routes, this strongly suggests an issue with group membership or a misalignment of groups between your IdP configured in Citrix and Google Directory. Proceed to Ensure IdP and Google Directory alignment.
- **The inaccessible application is not included in the routes response:** This suggests that the application is not correctly configured in the Citrix SecurAccess ZTNA Admin console. Verify

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

that the application exists and has a policy associated (either to allow or deny access). If you are certain that the application is configured but it is still missing from the preceding routes, contact Citrix Support.

Troubleshoot routed application access

When attempting to access your application (that does show up in the routes list), what is the observed behavior?

- **You are getting a domain resolution error (ERR_NAME_NOT_FOUND)**

  This most likely suggests that the application is not correctly configured or the contextual routes are not received correctly.

- **A cream-yellow page showing "Access Denied"**

  This suggests that the policy configuration in the Citrix SecurAccess ZTNA console is not configured to include the current user.

- **A cream-yellow page showing "Oops! Something went wrong."**

  The most common cause for this error page is the Connector being unable to reach the target application. In this case, troubleshoot connector access to internal applications as per Citrix documentation. Common issues include:

  - Internal DNS reachability
  - Backend service is down
  - Firewall rules

- **A white page showing "Service Unavailable" in a large red font**

  This can be a transient error and might resolve after a few minutes.

  If the issue persists, reach out to Citrix Support.

- **Timeout**

  - First, verify that `via.prod.securegateway.goog` is reachable by entering it in Chrome's address bar. You must receive a 401 response. If it times out, an intermediate firewall or proxy is blocking access and must be resolved before applications can be accessed.
  - Another potential cause for an application timeout is a firewall blocking traffic to the internet and to the Google Security Gateway in particular. This is common in scenarios where a

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

customer requires an explicit proxy to reach the internet. The Citrix SecurAccess ZTNA integration with Chrome Enterprise Premium does not support this proxy configuration.

- **Certificate error**

  Application might be using a private CA certificate and as such the browser might throw an "untrusted certificate error". Through Chrome Enterprise Premium configuration, the customer can push their trusted root CA to the browser. For details, see Use Chrome Enterprise Premium to manage root certificate configurations.

Ensure IdP and Google Directory alignment

For Citrix SecurAccess ZTNA integration with Chrome Enterprise Premium, the synchronization of your directory to Google Directory has to follow some specifications covered in Prerequisites for the integrated solution.

If the user and user group emails are correct and line up with what is configured in your source directory, proceed to Check access settings for the group in Google Admin Console.

Check access settings for the group in Google Admin Console

In Google Admin Console, navigate to **Directory > Groups** and select the group against which you have configured your access policy and against which your application is not loading.

From there, select **Access settings** and ensure that the row **Who can view members** has the option **Group Members** enabled. This configuration must apply to all groups you want to create policies against in Citrix SecurAccess ZTNA.

If this option is already enabled, reach out to Citrix Support.

Known issues with the CEP integration

The following known issues exist in the Citrix SecurAccess™ ZTNA integration with Chrome Enterprise Premium.

Citrix SecurAccess ZTNA user interface

- **Issue:** Session policy configuration currently allows users to add only two simulate conditions, even though three conditions are available. This limits flexibility in policy creation.

  Workaround: Create two separate session policies; one with two of the simulate conditions and another policy with the remaining condition.

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

- **Issue:** The TCP/UDP server-to-client configuration option is currently not available in the application configuration UI across all customer environments. This limits the ability to define server-to-client traffic behavior.

Adaptive access policy configuration

- **Issue:** Access policy creation fails when Okta groups are specified in the rules. This issue only affects groups that are present in the Okta directory.

  Workaround: You can use Okta as an identity provider but not as a directory. To use Okta as an IdP, you must first integrate your on-premises AD with Okta. For details, see Connect Okta as an identity provider to Citrix Cloud.

Google Chrome browser

- **Issue:** If the Google profile picker is open and the user tries to launch an app from CWA or a non-Chrome browser when there is no existing profile, the profile creation workflow is not triggerred.

  Workaround: Close the profile picker and relaunch the app.

- **Issue:** Logging into CWA with a managed Chrome profile and launching an app does not take the user to the original internal app URL after profile creation.

  Workaround: After the profile creation, relaunch app.

- **Issue:** Users part of a group is not auto synced when synced a group from Google Admin console. The `whoCanViewGroupMembership` setting is explicitly overridden to `ALL_MANAGERS_CAN_VIEW` during the sync. So, the restricted visibility is expected.

  Workaround: Manually update the google group permission on the Google Admin console or usomg via API. For details, see [URL}(https://developers.google.com/workspace/admin/groups-settings/manage).

- **Issue:** Users are prompted to authenticate with a user name and password through a proxy pop-up when accessing published SaaS/Web applications through a managed Chrome profile. This typically occurs after a period of inactivity:

  Causes:

  - A proxy token is unavailable or the proxy token is available but has subsequently expired.
  - The SEB extension requires re-initialization due to delayed initialization.

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

Workaround: Relaunch the Chrome session in a new window.

- **Issue:** Users might experience intermittent "Service Unavailable" errors when accessing external SaaS applications through Managed Chrome profiles or Citrix Workspace App. This issue is due to an unresolved backend issue on Google's infrastructure.

  Workaround: Contact the Google team for support.

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

Apps configuration and management

Citrix SecurAccess™ ZTNA provides a user-friendly, centralized platform for configuring and managing access to a diverse range of applications (SaaS/Web and TCP/UDP). The Citrix SecurAccess ZTNA console simplifies administration by providing a single point of control for various configuration tasks. Using the configuration wizard, administrators can easily set up Adaptive Authentication, configure applications, define access policies to control user permissions, and implement security restrictions to protect sensitive data, all within the same console. Additionally, Citrix SecurAccess ZTNA supports agentless access to Enterprise web apps without the need for installing a VPN client.

For details, see the following topics:

- Configure enterprise web or SaaS applications
- Configure TCP/UDP apps
- Configure TCP/UDP - server to client apps

Configure enterprise web or SaaS applications

After you have set up Citrix SecurAccess™ ZTNA, you can configure apps and access policies from the admin console.

1. In the admin console, click **Applications**.
2. Click **Add an app**.
3. Select the location where the app resides.
    - **Outside my corporate network** for external applications.
    - **Inside my corporate network** for internal applications.
4. Enter the following details in the App Details section and click **Next**.
    - **App type** - Select the app type.

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

NOTE:

For Chrome Enterprise Premium (CEP), only HTTPS enterprise web and SaaS apps are supported. HTTP enterprise web and SaaS apps are not supported.

- **App name** – Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in their store. You can also enter keywords for the applications in the format `KEYWORDS: <keyword_name>`. You can use the keywords to filter the applications.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you are publishing must appear in the store UI. You can add a new category for each app or use existing categories from the store UI. Once you specify a category for a web or a SaaS app, the app shows up in the store UI under the specific category.
  - The category/subcategory are admin configurable and administrators can add a new category for every app.
  - The category/subcategory names must be separated by a backslash. For example, Business And Productivity\Engineering. Also, this field is case sensitive. Administrators must ensure that they define the correct category. If there is a mismatch between the name in the store UI and the category name entered in the App category field, the category gets listed as a new category.

    For example, if you enter the Business and Productivity category incorrectly as Business And productivity in the App category field, then a new category named Business and productivity gets listed in the store UI in addition to the Business And Productivity category.
- **App icon** – Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels and only the ICO and PNG format are supported. If you do not change the icon, the default icon is displayed.
- **Do not display application to users** - Select this option if you do not want to display the app to the users.
- **URL** – URL of the application.
- **Related Domains** – The related domain is auto-populated based on the application URL. Administrators can add more related internal or external domains.

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

NOTE:

- Ensure that an app's related domain does not overlap with another app's related domain. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront™ or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.
- Similarly, a published app's URL must not be added as another app's related domain.
- For more details, see Best practices for Web and SaaS application configurations.

- **Add application to favorites automatically** – Click this option to add the app as a favorite app in Citrix Workspace app. When you select this option, a star icon with a padlock appears at the top left-hand corner of the app in Citrix Workspace app.
  - **Allow user to remove from favorites** – Click this option to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app. When you select this option, a yellow star icon appears at the top left-hand corner of the app in Citrix Workspace app.
  - **Do not allow user to remove from favorites** – Click this option to prevent subscribers from removing the app from the favorites apps list in Citrix Workspace app.

  If you remove the apps marked as favorites from the Citrix SecurAccess ZTNA console, then these apps must be removed manually from the favorites list in their store. The apps are not automatically deleted from the store if the apps are removed from the Citrix SecurAccess ZTNA console.
- **App Connectivity** - Select **Internal** for Web apps and **External** for SaaS apps.

5. Click **Save**, and then click **Finish**.

You can view all the application domains that are configured in **Settings > Application Domain**. For more details, see Manage settings after installation.

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

Automatic cleanup of routing entries on application deletion

When you configure an application, its destinations (FQDNs or application domains) are added to the routing table, which Citrix SecurAccess ZTNA uses for routing decisions. When you delete an application, Citrix SecurAccess ZTNA cleans up the routing entries based on the following rules:

- **Unreferenced entries are removed** - If a routing entry (FQDN or application domain) associated with the deleted application is not referenced by any other application, Citrix SecurAccess ZTNA removes it from the routing table automatically.
- **Shared entries are retained** - If a routing entry is used by more than one application, deleting one of those applications does not remove the shared entry. The entry remains in the routing table for as long as at least one active application references it.
- **No retroactive removal** - Routing entries are evaluated and removed only as part of an application deletion. Existing entries are not removed retroactively unless they are confirmed to be unused by any application.

NOTE:

- The cleanup runs automatically when an application is deleted from the Applications page (using the ellipsis (...) menu). No administrator action is required.
- Because shared routing entries are preserved, deleting an application does not disrupt access to other applications that share the same destination.

Next steps

Configure access policies for the applications.

Discover related domains using a HAR file

Citrix SecurAccess™ ZTNA enables you to upload a HTTP Archive (HAR) file to automatically discover the domains accessed by an application. You can review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains.

Previously, administrators had to know all of an application's related domains in advance, or discover them reactively as users hit blocked URLs. Because every URL other than the ones configured is blocked by default, this reactive approach leads to a poor user experience. Citrix SecurAccess ZTNA had no way to identify the internal or embedded URLs within an application.

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

Example

Suppose you are configuring an application whose primary domain is `example.com`. While using the application, the browser also accesses several additional domains. For example:

- `api.example.com` – Handles the application's backend API calls.
- `auth.example.com` – Manages sign-in and authentication.
- `cdn.example.com` – Serves static content such as images, scripts, and stylesheets.
- `login.microsoftonline.com` – Provides third-party identity authentication.
- `player.vimeo.com` – Loads embedded video content.

Instead of identifying each of these domains manually:

1. Capture a HAR file while using the application.
2. Import the HAR file into Citrix SecurAccess ZTNA.
3. Review the domains discovered by Citrix SecurAccess ZTNA. For example, the import might surface `api.example.com`, `auth.example.com`, and `cdn.example.com` as required, along with domains such as `player.vimeo.com` that you can choose to exclude.
4. Select the domains required by the application.
5. Configure routing and resource locations as needed.

This provides a faster way to identify and configure the domains required for application connectivity.

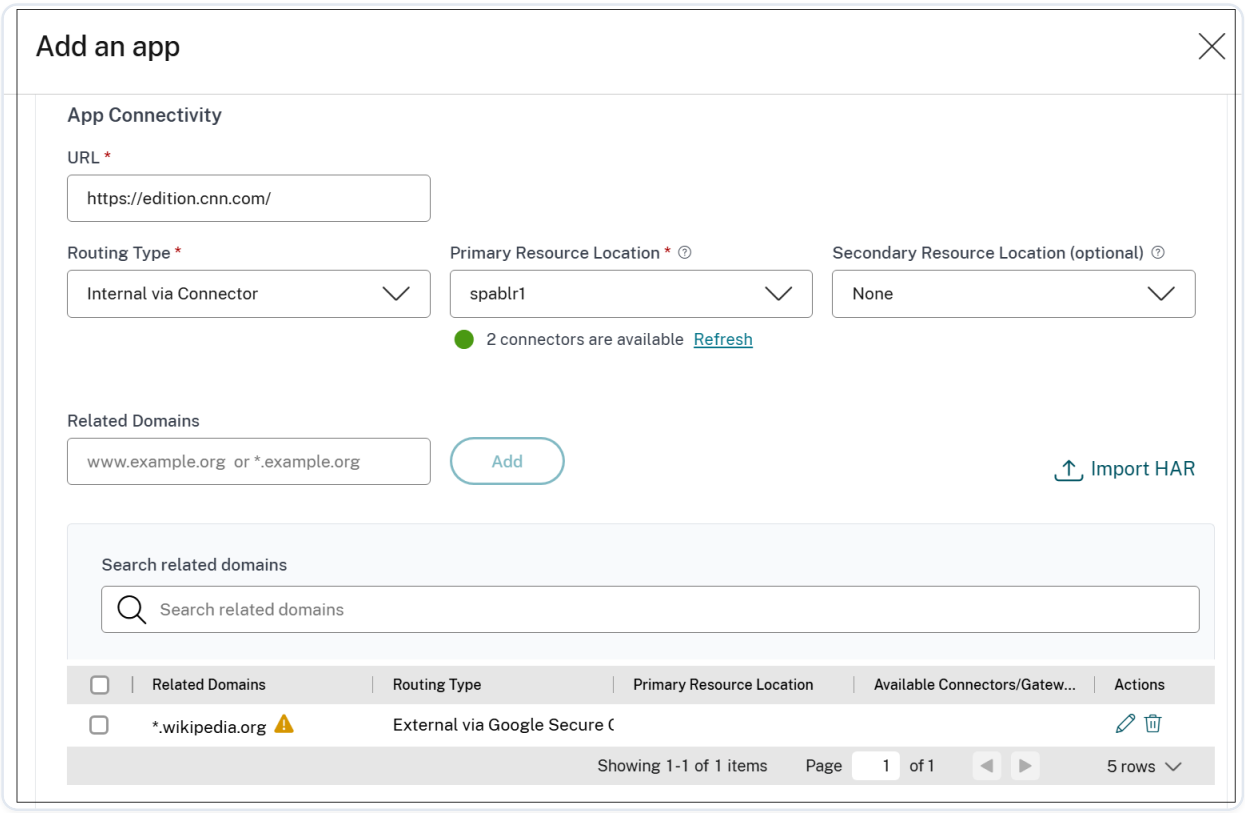
Prerequisites

Ensure that you have captured a HAR file while accessing the Web or SaaS application. The HAR file must contain the network request information and must be 50 MB or smaller.

Import a HAR file

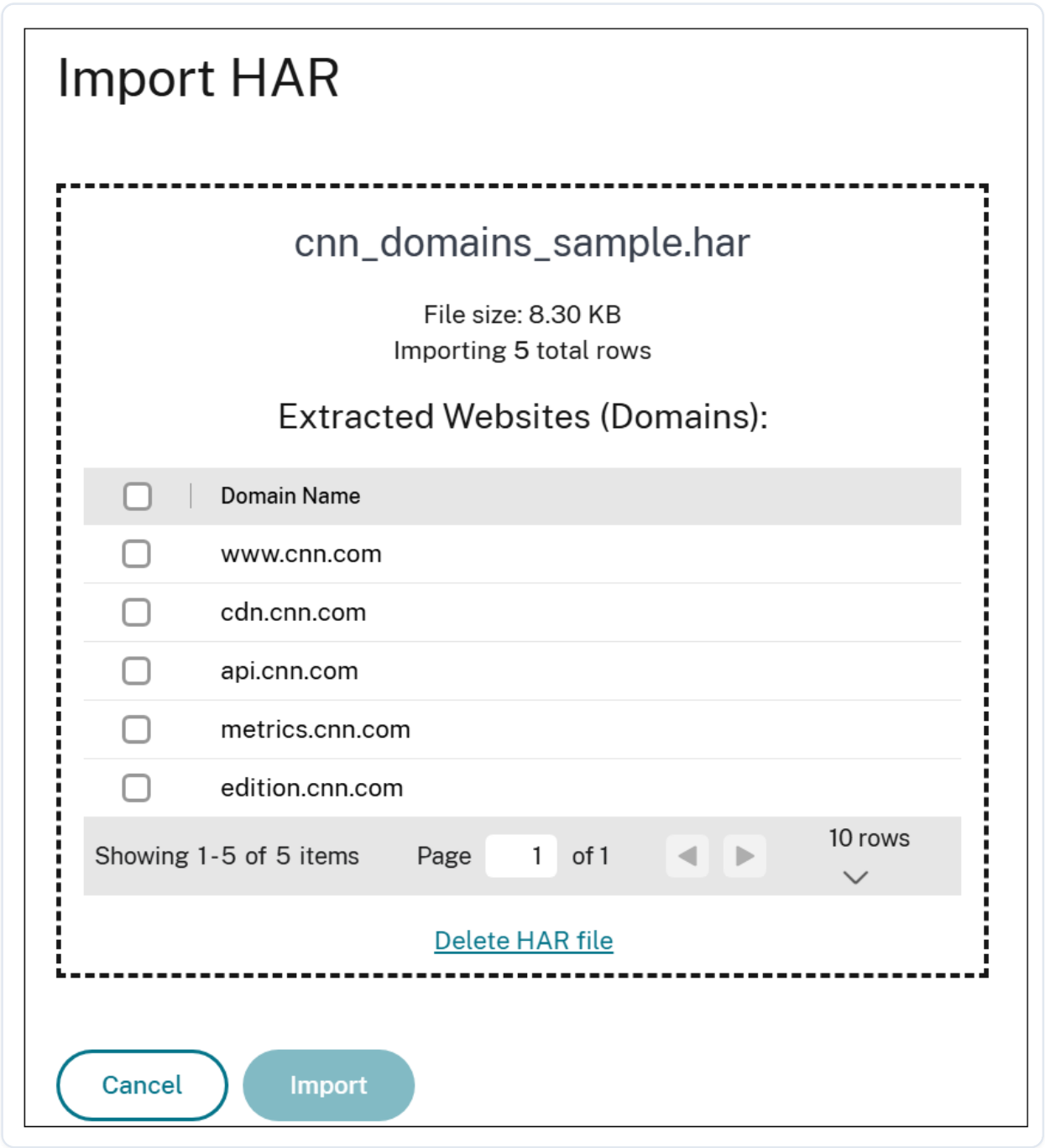
1. In the Citrix SecurAccess ZTNA admin portal, open the Web or SaaS application you want to configure.
2. Go to **App Connectivity** and click **Import HAR**.

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



3. Drag and drop the HAR file into the import window, or select the file from your device.
4. Citrix SecurAccess ZTNA analyzes the HAR file and displays the domains identified from the network requests.

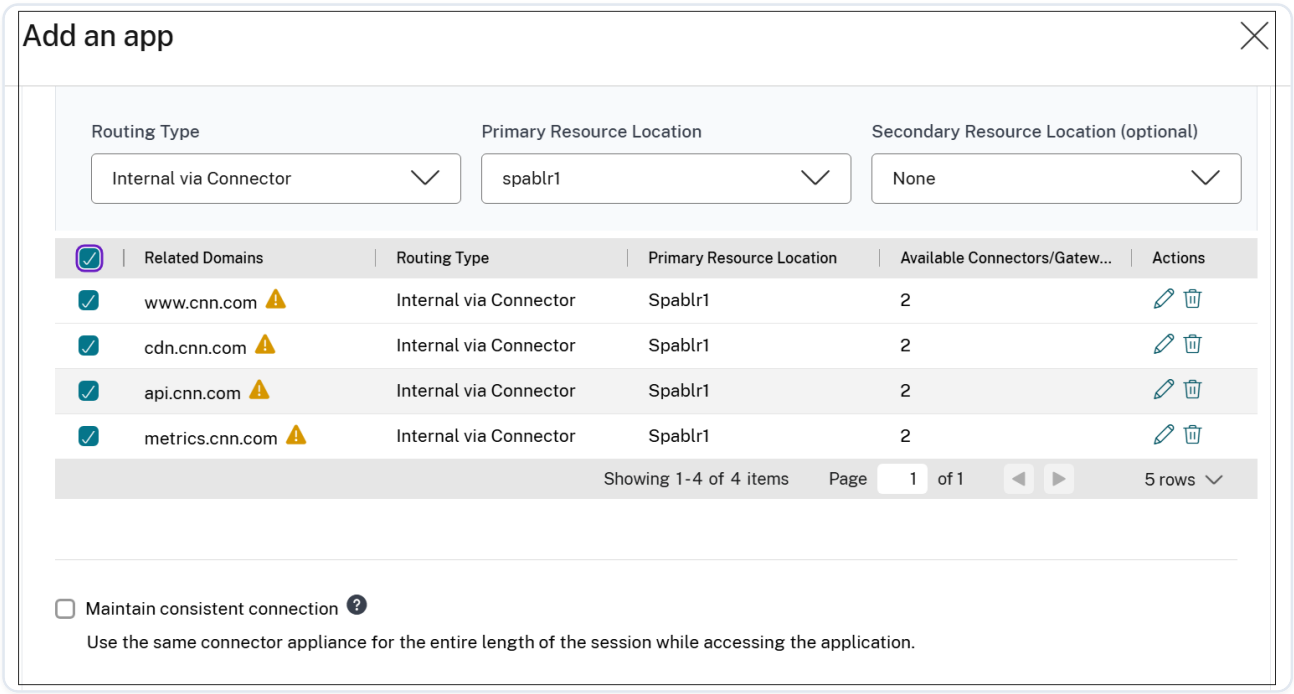
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Review the discovered domains.
6. Select the domains that you want to add to the application.
7. Select **Import**.

The selected domains are added to the application's **Related Domains** configuration.

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



NOTE:

Review the domains discovered before importing them. A HAR file can contain domains that are not required for the application's connectivity.

Manage related domains

After importing the domains, you can manage them from the **Related Domains** table:

- **Search for a domain** – Use the search field to filter the table and quickly find a specific domain.
- **Select domains** – Select individual domains, or use the table header checkbox to select multiple domains. The selection can be used to perform actions on multiple domains at the same time.
- **Edit domain configuration** – Update the configuration of related domains, including the routing type, primary resource location, and secondary resource location.
- **Bulk edit domains** – Select multiple eligible domains and update their routing and resource-location settings at the same time. Bulk editing is available for applicable internal domains. External domains might not support all configuration options.
- **Resource locations** – When configuring a related domain, assign a primary and, where applicable, secondary resource location. Use these settings to define how Citrix SecurAccess ZTNA routes traffic for the related domain and which resource locations are used to provide connectivity.

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

Validation and file requirements

The HAR import feature validates the uploaded file before processing it.

- Only valid HAR files containing network request entries can be imported.
- The maximum supported file size is **50 MB**.
- Domains are automatically extracted from the URLs in the HAR file.
- Duplicate domains are automatically removed.
- Domains are normalized before they are added to the related-domain configuration.

Configure TCP/UDP apps

Before configuring TCP/UDP apps, see System requirements.

Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.
3. Enter the following details:
    - **App type** – Select **TCP/UDP** for initiating connections with the back-end servers residing in the data center.
    - **App name**– Name of the application.
    - **App description** – Description of the app you are adding. This field is optional.
    - **Destinations** – IP Addresses or FQDNs of the back-end machines residing in the data center. One or more destinations can be specified as follows.
        - **IP address v4**
        - **IP address Range** – Example: 10.68.90.10-10.68.90.99
        - **CIDR** – Example: 10.106.90.0/24
        - **FQDN of the machines or Domain name** – Single or wildcard domain. Example: ex.destination.domain.com, *.domain.com

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

NOTE:

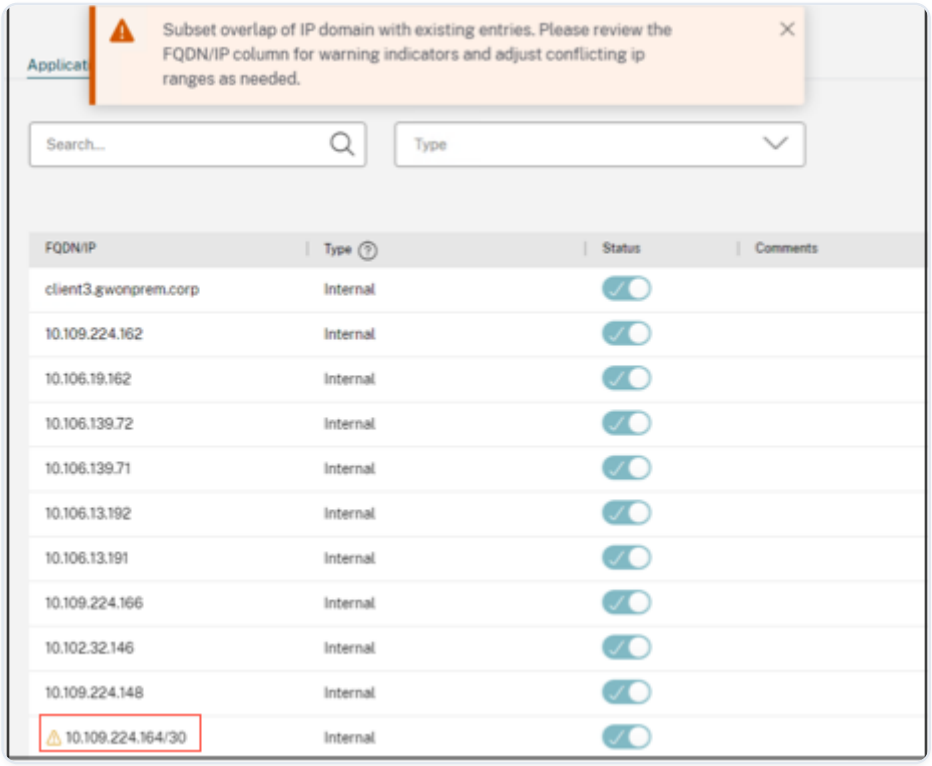
- End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix SecurAccess™ client can resolve an FQDN to the real IP address.

The following table provides examples of various destinations and how to access the apps with these destinations:

DESTINATION INPUT	HOW TO ACCESS THE APP
10.10.10.1-10.10.10.100	The end user is expected to access the app only through IP addresses in this range.
10.10.10.0/24	The end user is expected to access the app only through IP addresses configured in the IP CIDR.
10.10.10.101	the end user is expected to access the app only through 10.10.10.101
`*.info.citrix.com`	The end user is expected to access subdomains of `info.citrix.com` and also `info.citrix.com` (the parent domain). For example, `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Note:** The wildcard must always be the starting character of the domain and only one *. is allowed.
info.citrix.com	The end user is expected to access `info.citrix.com` only and no subdomains. For example, `sub1.info.citrix.com` is not accessible.

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

The destination IP address must be unique across resource locations. If a conflicting configuration exists, a warning symbol is displayed against the specific IP address in the Application Domain table (**Settings > Application Domain**).



- **Port** – The destination port on which the app is running. Admins can configure multiple ports or port ranges per destination.

  The following table provides examples of ports that can be configured for a destination.

PORT INPUT	DESCRIPTION
*	By default, the port field is set to "*" (any port). The port numbers from 1 to 65535 are supported for the destination.
1300–2400	The port numbers from 1300 to 2400 are supported for the destination.
38389	Only the port number 38389 is supported for the destination.
22,345,5678	The ports 22, 345, 5678 are supported for the destination.

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

PORT INPUT	DESCRIPTION
1300–2400, 42000-43000,22,443	The port number range from 1300 to 2400, 42000–43000, and ports 22 and 443 are supported for the destination.

NOTE:

Wildcard port (*) cannot co-exist with port numbers or ranges.

- **Protocol** – TCP/UDP

4. **App Connectivity:** Define how your application traffic must be routed.

   - **Internal:** DNS resolution is done via a remote DNS server.

     By default, all the traffic to the domain marked as **Internal** is intercepted and tunneled through NetScaler Gateway. For example, if the connectivity for `.example.net` is set as **Internal**, all of its related domains/subdomains (for example; `code.example.net`, `test.example.net`, `123.example.net`) are intercepted and tunneled through NetScaler Gateway.

   - **External:** DNS resolution is done via a local DNS server.

     When a related domain/subdomain is marked as **External**, traffic to that domain is not intercepted and tunneled through NetScaler Gateway. For example, if connectivity to code.`example.net` is set as **External**, then traffic to this domain is routed directly through the internet while traffic to subdomains (for example `text.example.net` and `123.example.net`) is tunneled through NetScaler Gateway.

5. Click **Add** to add additional destinations or servers accordingly.
6. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.

   - **Edit Application**
   - **Delete**

Next steps

Configure access policies for the applications.

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

Configure TCP/UDP - server to client apps

The **TCP/UDP - server to client** app type can be used for supporting the following features:

- Software distribution using Microsoft Endpoint Configuration Manager or similar solutions
- Remote policy updates on managed devices using GPO Push
- Remote assistance to troubleshoot and debug user workstations.

Prerequisites:

- Citrix SecurAccess™ ZTNA setup is complete.
- Client versions meet the following requirements:
  - Windows - 24.6.1.18 and later
  - macOS - 24.06.2 and later
- The intranet IP address is configured on NetScaler® Gateway and is bound to the respective VPN virtual server. Use the following sample commands for reference:

  `set vpn sessionAction ns_default_vpn_session_profile_spa_tcp_udp_apps -useMIP NS -useIIP NOSPILLOVER`

  (Optionally users can create a VPN session profile and a session action with `-useMIP NS -useIIP NOSPILLOVER`)

  bind vpn vserver `<spa vserver name>` -intranetIP `<IP address>`

Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.
3. Enter the following details:
   - **App type** – Select **TCP/UDP - server to client**.
   - **App name**– Name of the application.
   - **App description** – Description of the app you are adding. This field is optional.
   - **Server** - Details of the application servers that are authorized to establish connection with the client. You can enter the IP address, IP address range, or the CIDR.
   - **Port** – The client port number.
   - **Protocol** – TCP/UDP.

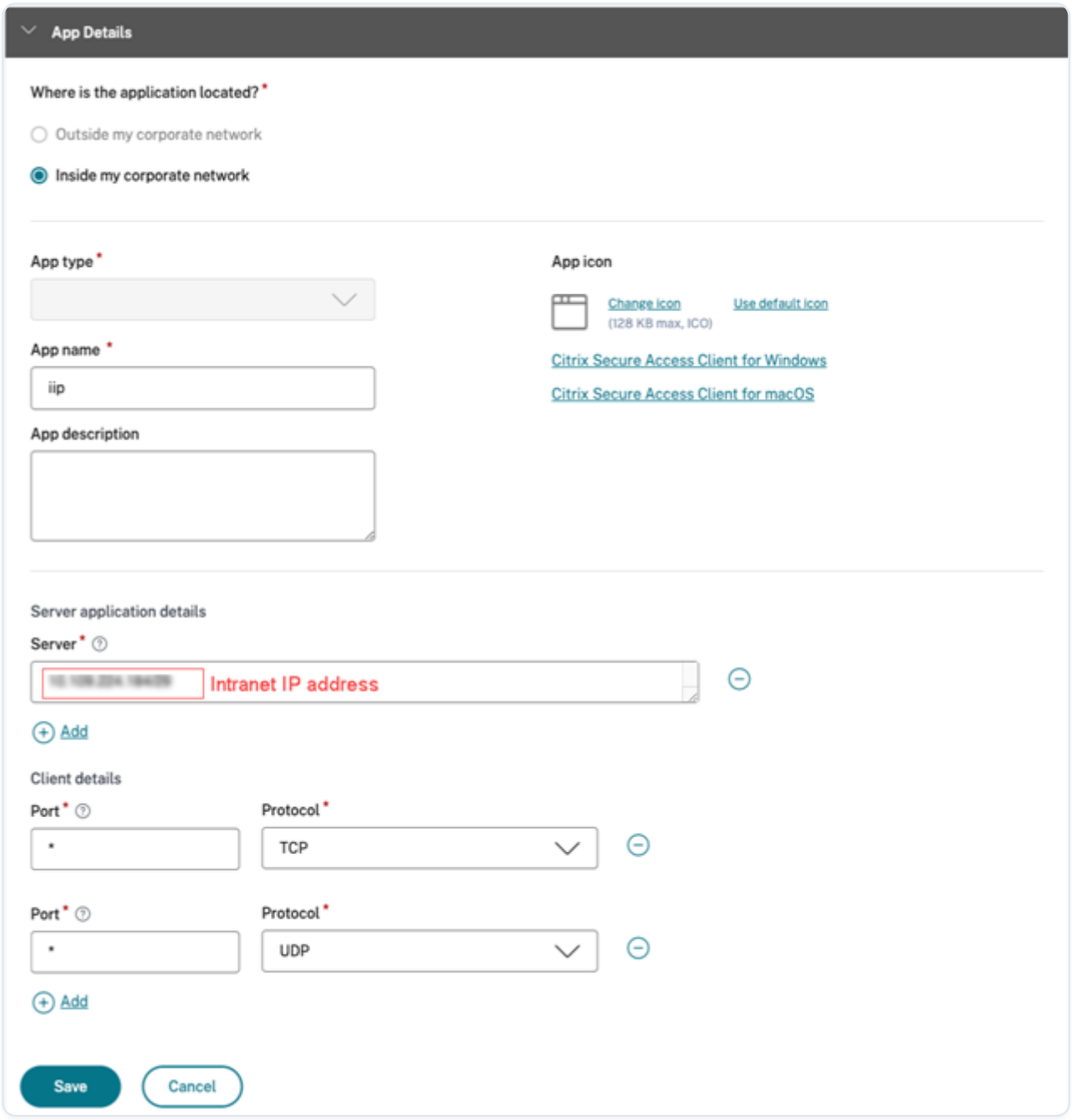
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Add** to add additional servers.
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.
    - **Edit Application**
    - **Delete**

IMPORTANT:

After you add an app for server-client communication, intranet IP address ranges configured on NetScaler Gateway must be added as a TCP/UDP app to enable server-client and client-client communication.

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



Edit an application

1. In the Citrix SecurAccess ZTNA admin console, click **Applications**.
2. Click the ellipsis button in line with the application that you want to modify, and then click **Edit Application**.
3. Edit the application details.
4. Click **Save**.

Next steps

Configure access policies for the applications.

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

Access policy configuration and management

In today's ever changing situations, application security is vital for any business. Making context-aware security decisions and then enabling access to the applications reduces the associated risks while enabling access to users.

The Citrix SecurAccess™ ZTNA adaptive access feature offers a comprehensive zero-trust access approach that delivers secure access to the applications. Adaptive access enables admins to provide granular level access to the apps that users can access based on the context.

Access policies within Citrix SecurAccess ZTNA allow you to enable or disable access to the apps based on the context of the user or user's device.

For more information, see the following topics:

- Configure access policies for the applications
- Policy conditions
- Configure session policies
- Device certificate enrollment

Configure access policies for the applications

Access policies within Citrix SecurAccess™ ZTNA allow you to enable or disable access to the apps based on the context of the user or user's device.

Access restrictions must be configured through the Google Admin console rather than within the Citrix SecurAccess ZTNA interface.

Rules are configured in the **Google Admin console > Rules**. These rules are advanced settings related to DLP, such as adding a watermark, blocking the download of files with social security numbers, and URL filtering.

For details on creating policies and rules for Google Chrome in the Google Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise

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

- Data protection rules

Configure access policies

1. In the admin console, click **Access Policies**.
2. Click **Create Policy**.
3. In the **Create Access Policy** page, select one of the following:

   - **Users/User groups**
   - **Machines/Machine groups**

   Application access rules are enforced based on a user's or machine's context, based on the selection in the access policy.

   You can select **Machine/Machine groups** to enable Always On connectivity. For Always On connectivity, you must have the device certificates enrolled. For details see Device certificate enrollment configuration.

   For more information on the machine tunnel, see Always On VPN before Windows Logon.

4. a. In **Policy name**, enter a name for the policy.
5. In **Applications**, select the apps for which you want to enforce the access policies.
6. In **Users conditions** – Select the conditions and users or user groups based on which app access must be allowed or denied.

   - **Matches any of**: Only the users or groups that match any of the names listed in the field are allowed access.
   - **Does not match any**: All users or groups except those listed in the field are allowed access.

   You can search for users by display name, email ID, or user principal name. This search option allows admins to accurately identify and grant access to the correct user, even if they have multiple accounts. For details, see Policy conditions.

7. (Optional) Click **+** to add multiple conditions based on the context.

   When you add conditions based on a context, an AND operation is applied on the conditions, and the policy is evaluated only if the Users and the optional contextual based conditions are met. You can apply the following conditions based on context.

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

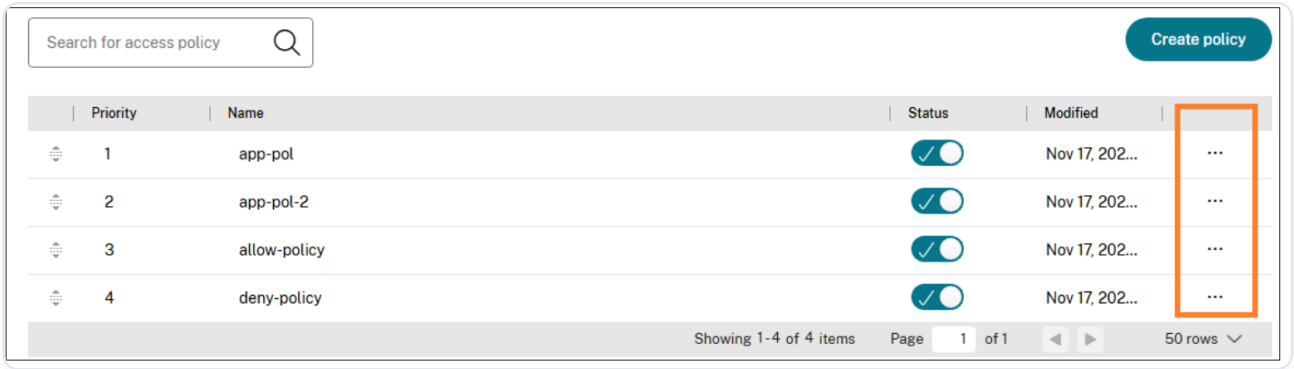
- **Network Location** - Select the condition and the network using which the users access the apps.
  - **Matches any of:** Only users or user groups accessing the apps from any of the network locations listed are enabled for access to the apps.
  - **Does not match any:** All users or user groups other than those from the listed network locations are enabled for access.
- **Device Posture** - Select the conditions that the user device must fulfill to access the apps.

For details, see Policy conditions.

8. In **Actions**, select one of the following actions that must be enforced on the app based on the condition evaluation.
   - **Allow access**
   - **Deny access**
9. Select **Enable policy on save**. If you do not select this option, the policy is only created and not enforced on the applications. Alternatively, you can also enable the policy from the Access Policies page by using the toggle switch.

Edit an access policy

1. In the Citrix SecurAccess ZTNA admin console, click **Access Policies**.
2. Click the ellipsis button in line with the policy that you want to modify, and then click **Edit access policy**.
3. Edit the policy details.
4. Click **Update**.



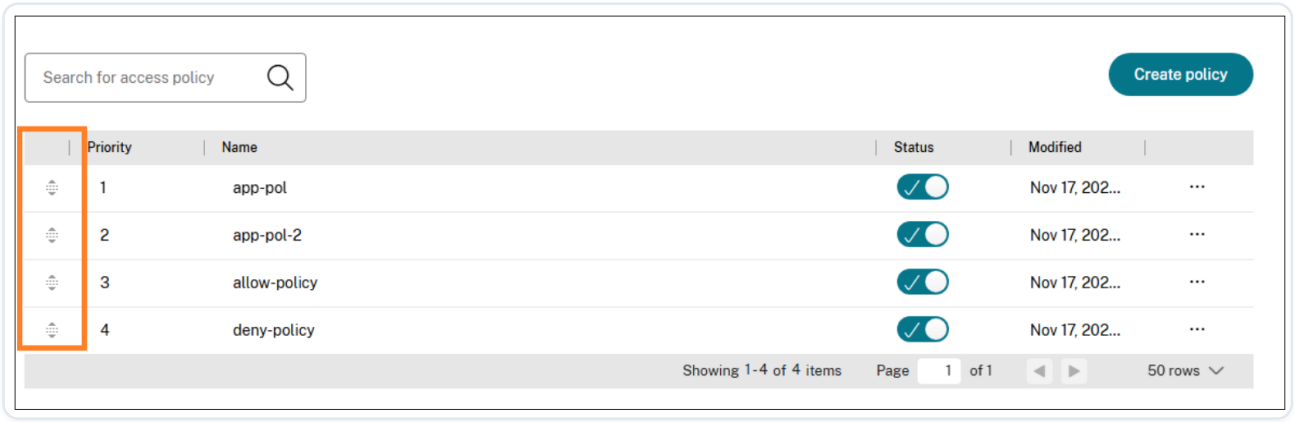
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change access policy priority

After an access policy is created, a priority number is assigned to the access policy, by default. You can view the priority on the Access Policies home page.

A priority with a lower value has the highest preference and is evaluated first. If this policy does not match the conditions defined, the next policy with the lower priority number is evaluated and so on.

You can change the priority order by moving the policies up or down by using the up-down icon in the **Priority** column.



Next steps

- Validate your configuration from the client machines (Windows and macOS).
- For the TCP/UDP apps, validate your configuration from the client machines (Windows and macOS) by logging into the Citrix SecurAccess client.

Sample configuration validation

Policy conditions

The following sections provide more information about the policy conditions.

User and user groups

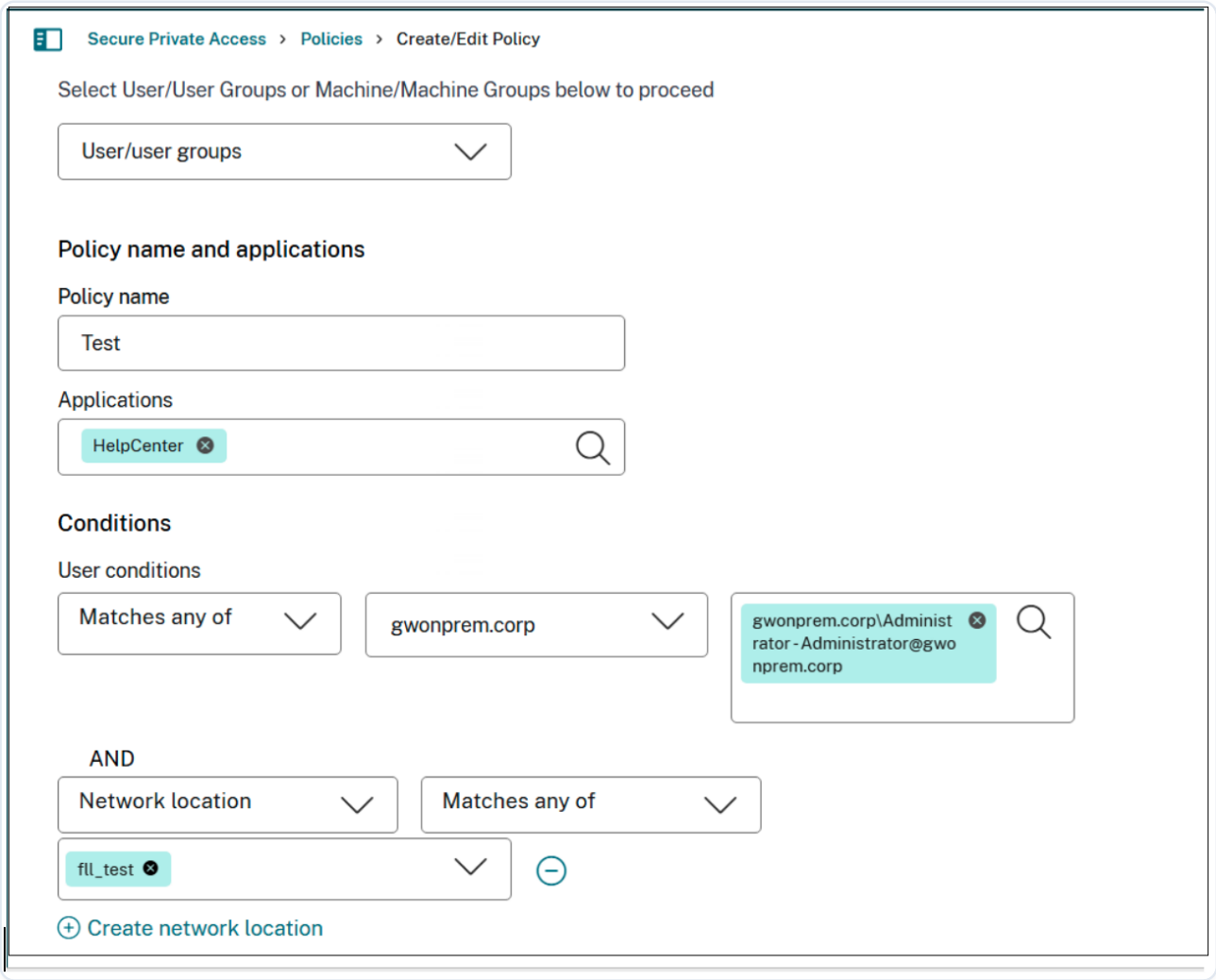
User conditions define which users, groups, or identity attributes the access policy applies to. These rules let administrators include or exclude specific identities when determining access to an application.

User conditions consist of three primary components:

Match Type: This drop-down list controls how the list of selected identities is evaluated.

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

- **Matches any of:**
  - Use this when the policy must apply only to the selected users or groups.
  - The condition is satisfied if at least one identity in your list matches.
  - Works like an IN filter.
- **Does not match any**
  - Use this to apply the policy to everyone except the selected users or groups.
  - The condition is satisfied only if none of your selected identities match.
  - Works like a NOT IN filter.



Domain Selector:

The **Domain** drop-down list filters identities by directory or identity source.

- **Identity Selector (user emails, group emails)** - This field allows selecting one or more identities, including user emails and group emails.

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

Verify user and group synchronization

During user lookup, administrators can verify whether users from the selected directory are synchronized with Google Directory. Citrix SecurAccess™ ZTNA policies evaluate correctly only when the users are synchronized with the Google Directory. Otherwise, the following warnings might appear:

- **Missing tenant account privileges:**

  Workaround:

  In the Google Admin console, assign the **Users > Read** privileges to the tenant service account. Citrix SecurAccess ZTNA requires these privileges to verify that a user exists.

- **User not synchronized:**

  Workaround:

  The searched or selected user is not synchronized with Google Directory. Synchronize the directory entity with Google Directory before using it in the Citrix SecurAccess ZTNA policy.

NOTE:

This feature is available only after the Google Chrome integration is successfully completed.

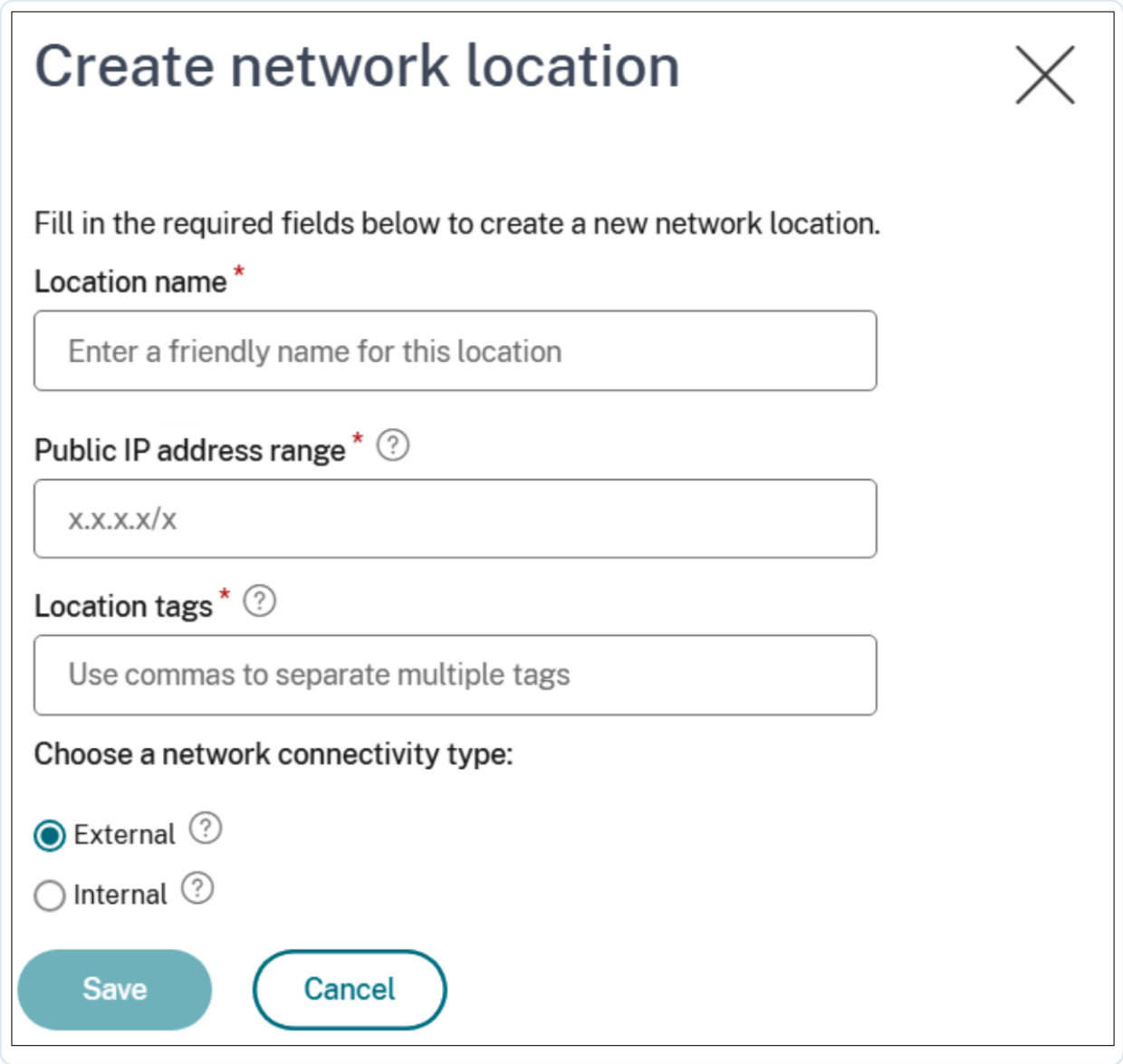
Network Location

The Network Location Service (NLS) is a policy condition that allows you to restrict access based on the user's network location. An admin can configure the access policy based on the location from where the user is accessing the application. The location can be the country from where the user is accessing the application or the user’s network location. The network location is defined using an IP address range or subnet addresses.

To configure an access policy based on the location, do the following:

1. Under **Conditions** section, click **Add condition**.
2. Select **Network location**.

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



If you have configured multiple network locations, then select one of the following as per your requirement.

- **Matches any of** – The network locations match any of the network locations configured in the database.
- **Does not match any** – The network locations do not match with the network locations configured in the database.

NOTE:

For **Network location**, you can select an existing network location or create a network location. To create a new network location, click **Create network location**.

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

- Ensure that you have enabled Adaptive Access from **Citrix Cloud > StoreFront Cloud > Access > Adaptive Access**. If not, you cannot add the location tags. For details, see Enable Adaptive Access.

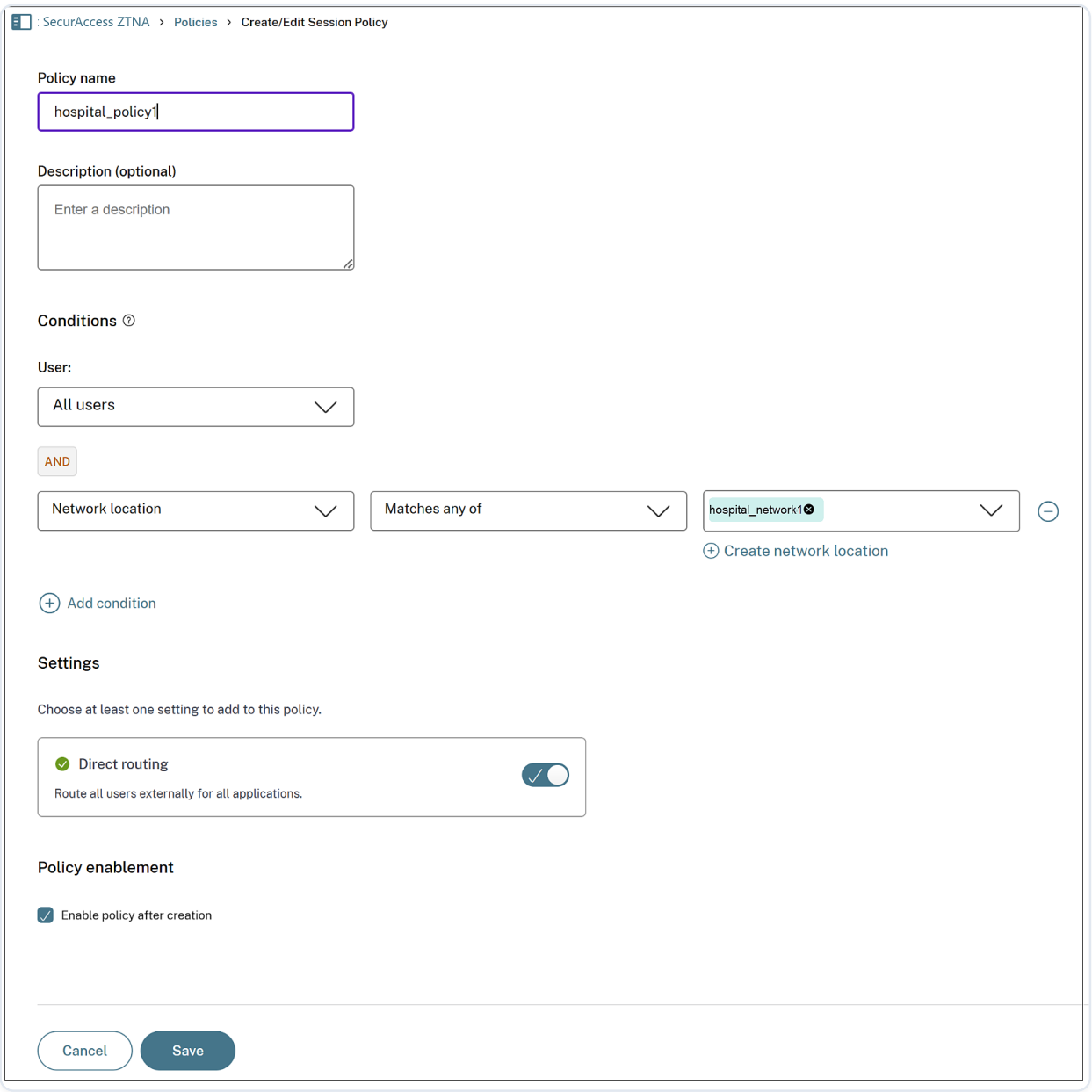
You can also create a network location from the Citrix Cloud console. For details, see Connectivity to DaaS resources.

3. Complete the policy configuration.

Configure session policies

You can use a session policy to allow users to directly access back-end applications by bypassing NetScaler Gateway tunneling.

1. Navigate to **Policies > Session Policies** and click **Create Session Policy**.



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

2. Enter a name and a description of the policy.
3. Select the users and conditions to which you want to apply these settings.

   You can apply the condition to all users or to a subset of users.

   For example, you can define the **Network Location** condition to enable dynamic routing for the entire session. This ensures that direct routing is enabled only when users are inside the company's corporate network.

   When you add additional conditions based on a context, an AND operation is applied on the conditions, and the policy is evaluated only if both the users and the optional contextual-based conditions are met.
4. Select **Direct routing** to send user traffic directly to the back-end applications without NetScaler Gateway tunneling.
5. Select **Enable policy after creation**. If you do not select this option, the policy is only created and not enforced on the applications.

   Alternatively, you can also enable the policy from the Session Policies page by using the toggle switch in the **Status** column.
6. Click **Save**.

NOTE:

Network location changes trigger session policy refreshes and this might impact the end clients as follows:

- **Citrix SecurAccess™ client:** Policy refreshes might alter routing configurations and hence impact application access.
- **Chrome Secure Browse extension:** Policy refreshes occur every 30 minutes. Users must restart the browser or wait for the refresh to access applications.

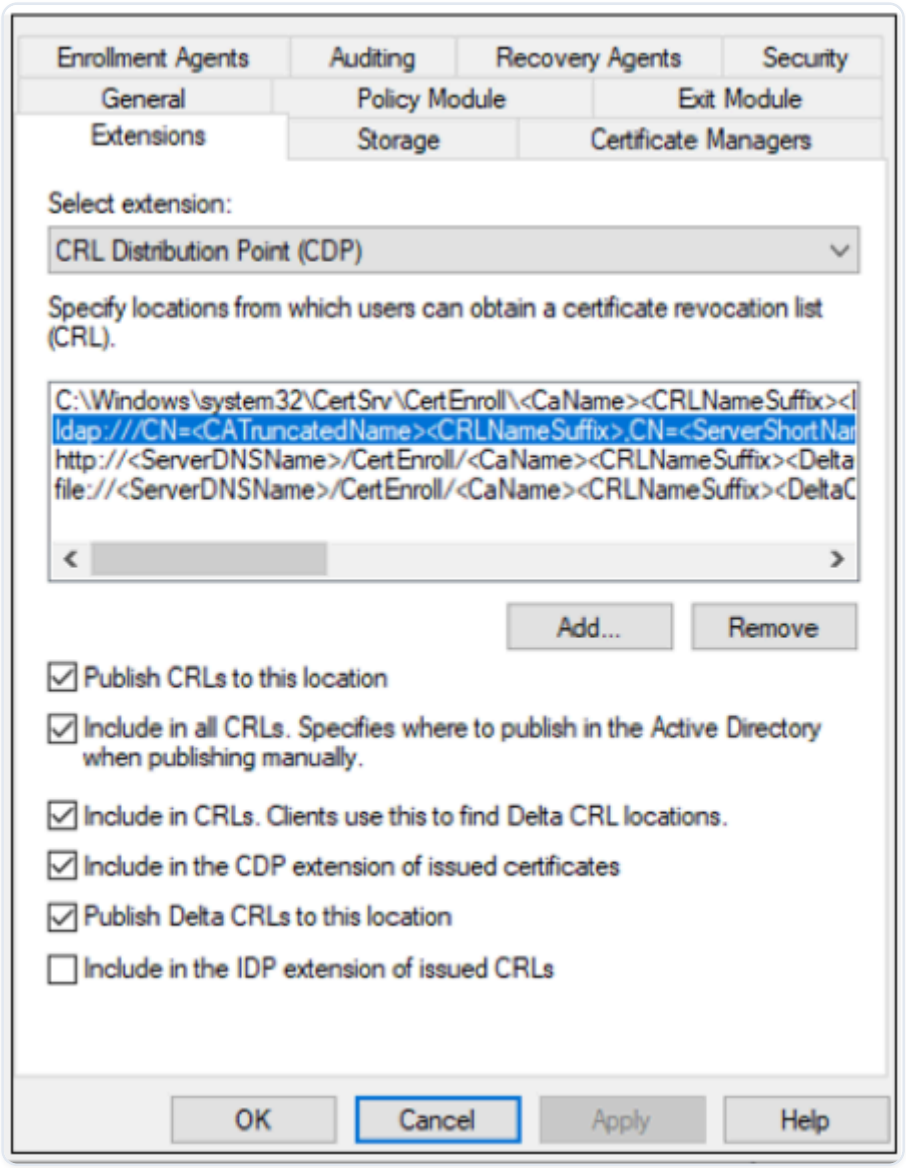
Device certificate enrollment

Device certificates must be enrolled for Always On configurations to ensure that devices can consistently and securely connect to the network.

The following steps are involved in device certificate enrollment:

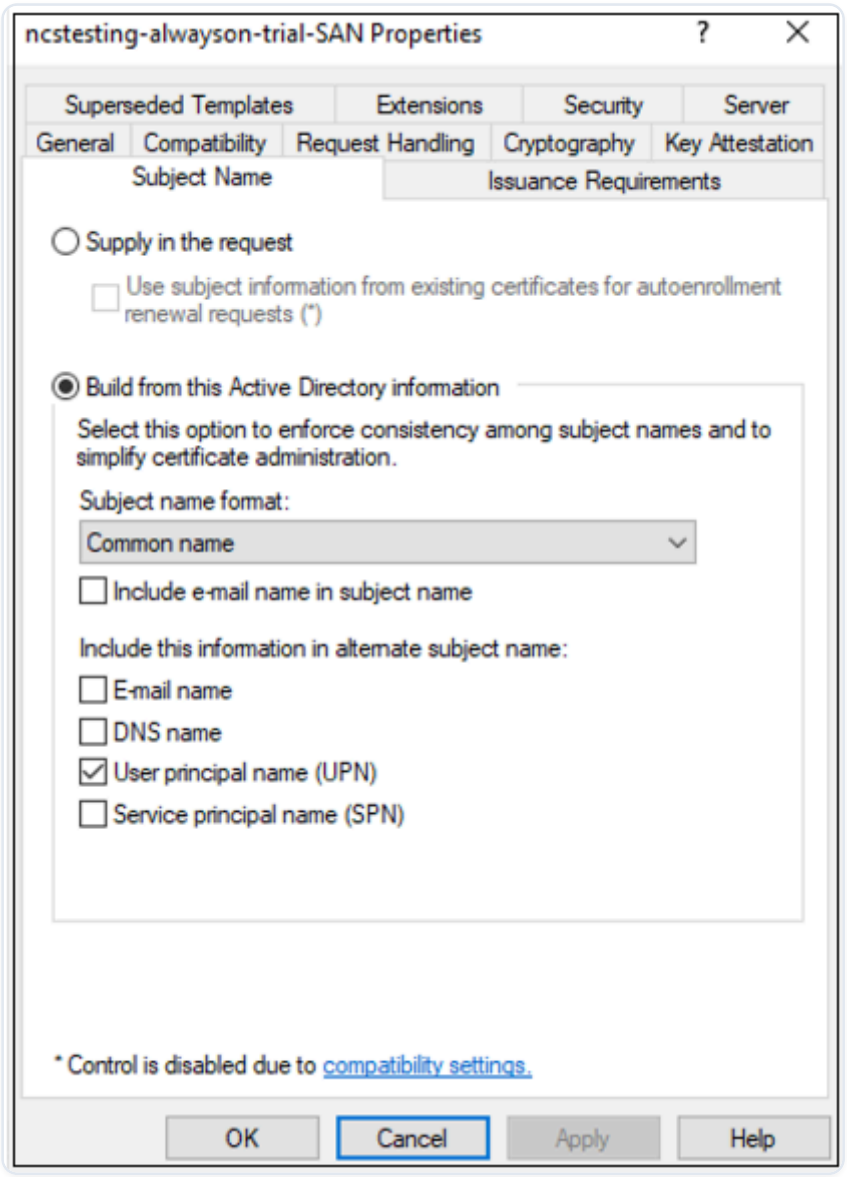
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. The Active Directory Enterprise Certificate Authority issues a Device Certificate for machine authentication.
2. The certificate authority must have the LDAP URL published for the CRL distribution point (CDP) extension.



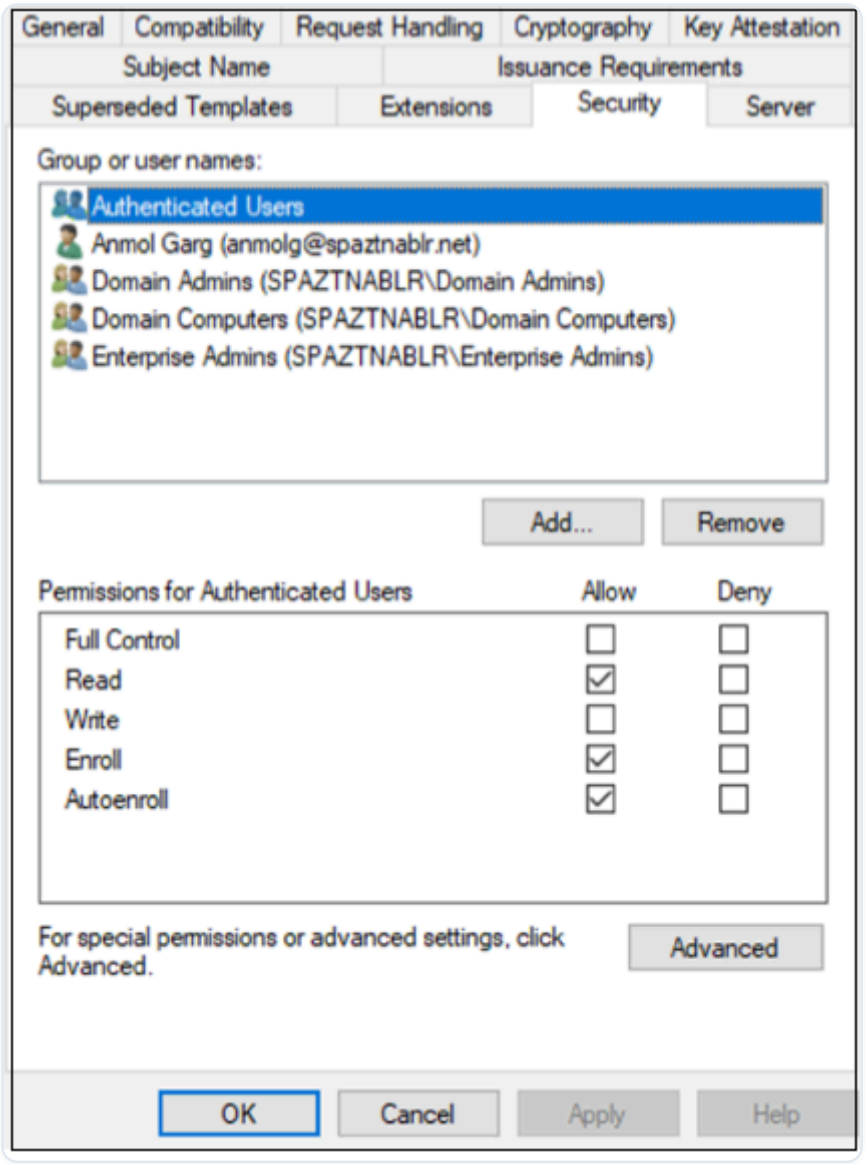
3. A certificate template in this certificate authority must be created to enroll the device certificate with the following details.
    a. Open the certification template snap-in and duplicate either the **Computer** or **Workstation Authentication** (preferred) template.
    b. Provide a new name for the certificate.
    c. Switch to the **Subject Name** tab, change the **Subject name format** setting to **Common name**, and check **User Principal Name (UPN)** to be included in the alternate subject name.

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



d. Switch to the **Security** tab and add a security group (containing only computer accounts) to which you want to autoenroll the new certificate template. Select the added group and select **Allow** for **Autoenroll**.

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

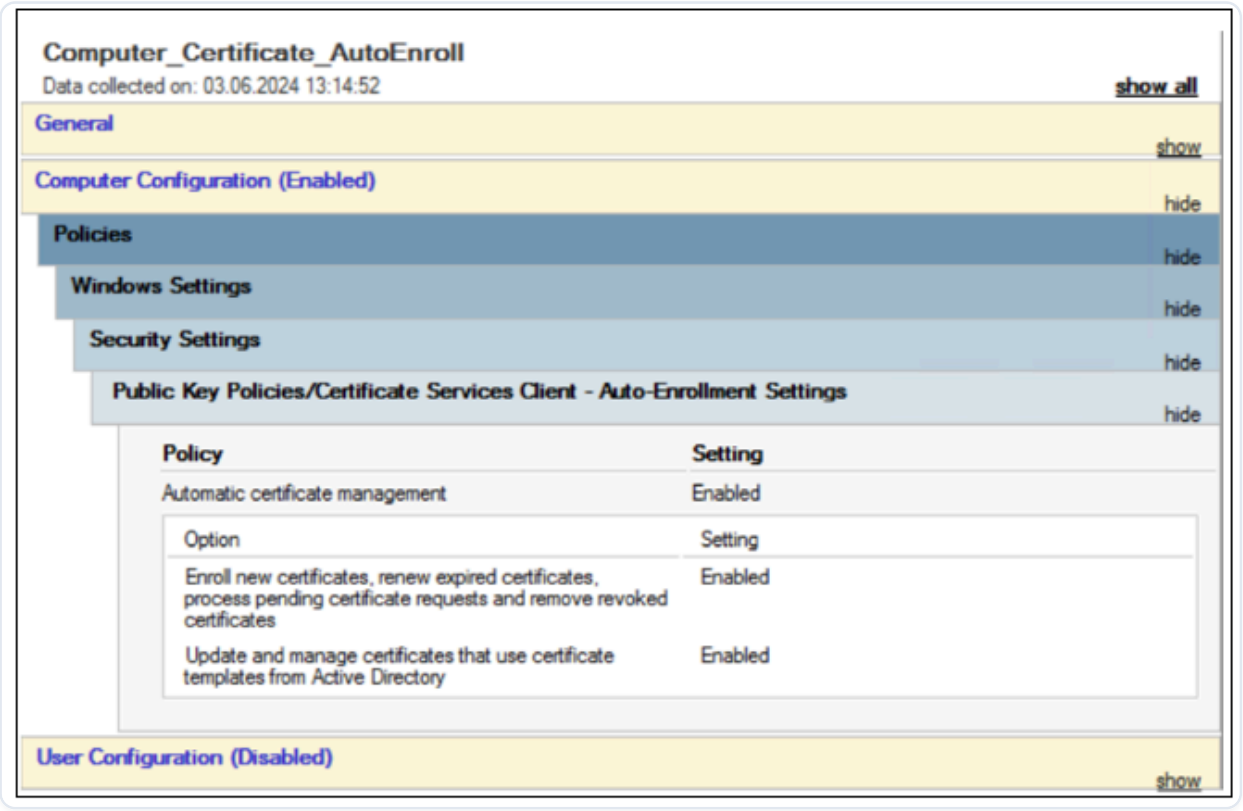


NOTE:

In the preceding image, **Authenticated Users** (all computer objects) are permitted to enroll or autoenroll the new certificate template.

e. (Optional) Create a group policy object (GPO) that allows for auto certificate enrollment and bind it to an organization unit (OU) or at the domain level.

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



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

Device Posture service

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix SecurAccess™ ZTNA resources (SaaS, Web apps, TCP, and UDP apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

For more information about device posture, see Device Posture.

Configure the device posture checks on NetScaler Gateway

The Citrix Device Posture service is integrated with NetScaler Gateway. You can configure the device posture checks on NetScaler Gateway.

For more information, see Device Posture checks on NetScaler® Gateway.

NOTE:

- It is recommended to enable device posture checks at the virtual server level.
- Ensure that the customer ID is set up using the `set dps parameter` that is `set dps parameter -CustomerID <CCID>`. The rest of the parameters are auto populated.

Device Posture checks on on-premises NetScaler® Gateway

Citrix Device Posture service is a cloud-based solution that helps admins enforce certain requirements that the end devices must meet to gain access to Citrix SecurAccess™ ZTNA resources, such as SaaS/ Web and TCP/UDP apps. Establishing device trust by checking the device's posture is critical for implementing zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in. For details on the Device Posture service, see Device Posture.

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

Entitlements

The Device Posture service is available as part of the Universal Hybrid Multi Cloud (UHMC) license and Citrix Platform License (CPL). For more information, see Current offerings.

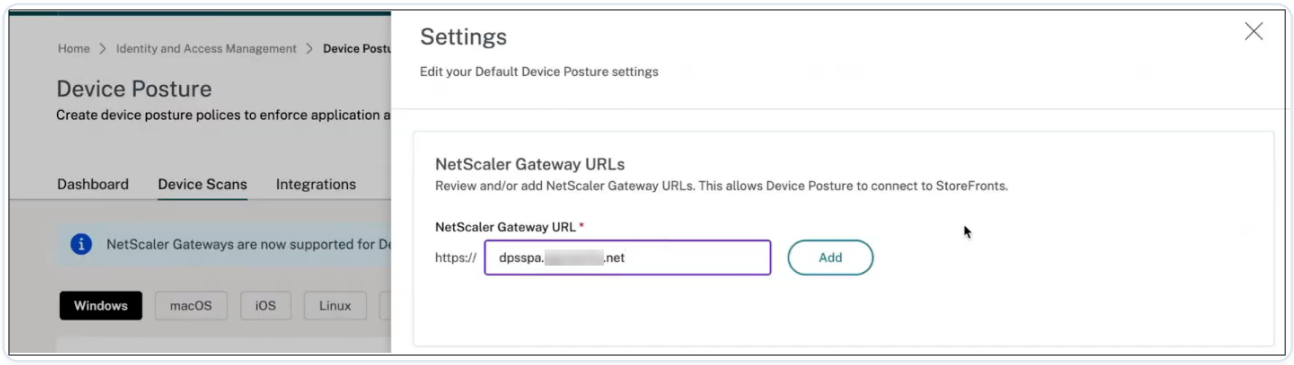
Enable Device Posture for Citrix SecurAccess ZTNA hybrid solutions

Integration of the Device Posture service with Citrix SecurAccess ZTNA for hybrid solutions is supported only from NetScaler Gateway release 14.1 build 43.x. The Device Posture feature must be enabled on NetScaler Gateway for the Device Posture scans to function in the Citrix SecurAccess ZTNA hybrid deployment.

For details on enabling Device Posture checks on NetScaler Gateway, see Device Posture checks on NetScaler Gateway.

In addition to enabling the Device Posture feature on NetScaler Gateway, you must add the URL of NetScaler Gateway accessing StoreFront™ in the Device Posture **Settings** page.

1. In the Citrix SecurAccess ZTNA admin console navigation pane, click **Device Posture**.
2. In the **Device Scans** page, click **Settings**.
3. In **NetScaler Gateway URL**, enter the FQDN of the virtual server for which the Device Posture checks must be enabled. For example, `https://gw.example.net`.



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

Manage settings

You can update and maintain the Citrix SecurAccess™ ZTNA hybrid deployment settings after onboarding.

- Manage application domain routing and generate configuration reports. Reports can include details about access policies, applications, routing domains, resource locations, security groups, cloud connectors, site configurations, and browser settings. For details, see Manage settings after on boarding.
- Manage onboarding configuration inputs. Changes can be disruptive because multiple components depend on these values. Depending on what is changed, required follow-up actions can include reconfiguring and re-analyzing NetScaler, reconfiguring StoreFront, and re-analyzing StoreFront. For details, see Manage setup configuration after installation.
- Reset configuration when switching from Citrix Enterprise Browser integration to Chrome Enterprise Premium. For details, see Reset Citrix SecurAccess ZTNA configuration.
- Cloud Connector updates are installed by default one connector at a time when available, and Citrix SecurAccess ZTNA is upgraded as part of the Cloud Connector upgrade by default. For details, see Components upgrade.

Manage settings

The following sections provide more information about the settings.

Application domains

Citrix SecurAccess™ ZTNA admins can view the list of application domains added to your Citrix SecurAccess ZTNA setup. The application domains table lists all the related domains and how the app traffic is routed (externally or internally).

1. Click **Settings > Application Domain**.
2. Click the edit icon and change the routing type, if necessary.

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

Configuration report

Customer administrators can generate configuration reports to gain insights into the Citrix SecurAccess ZTNA setup. The configuration report includes information for the following categories:

- Access policies governing access to applications and resources.
- Applications configured within Citrix SecurAccess ZTNA.
- Routing domains set up for the applications.
- Resource locations associated with the customer.
- Security Groups.
- Cloud connectors.
- Site configurations.
- Browser settings.

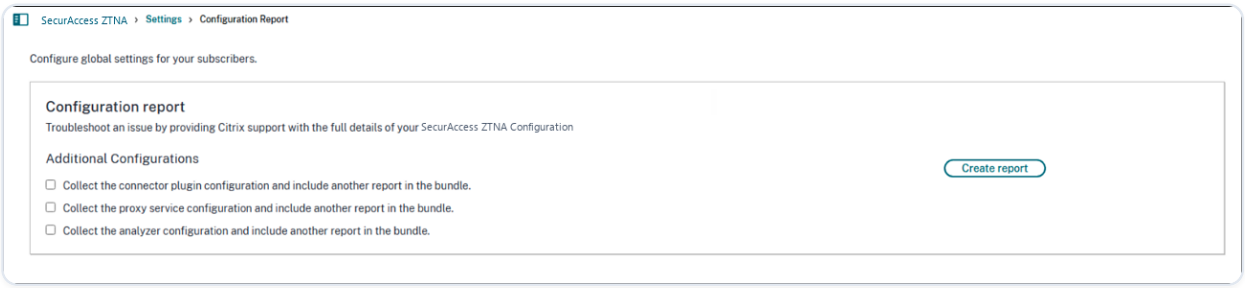
You can also include additional configuration reports in the bundle:

- Details from the connector plug-in database.
- Details from the proxy service.
- Details from the analyzer configuration.

Generate a configuration report

Perform the following steps to generate a configuration report:

1. In the Citrix SecurAccess ZTNA admin console, go to **Settings > Configuration Report**.



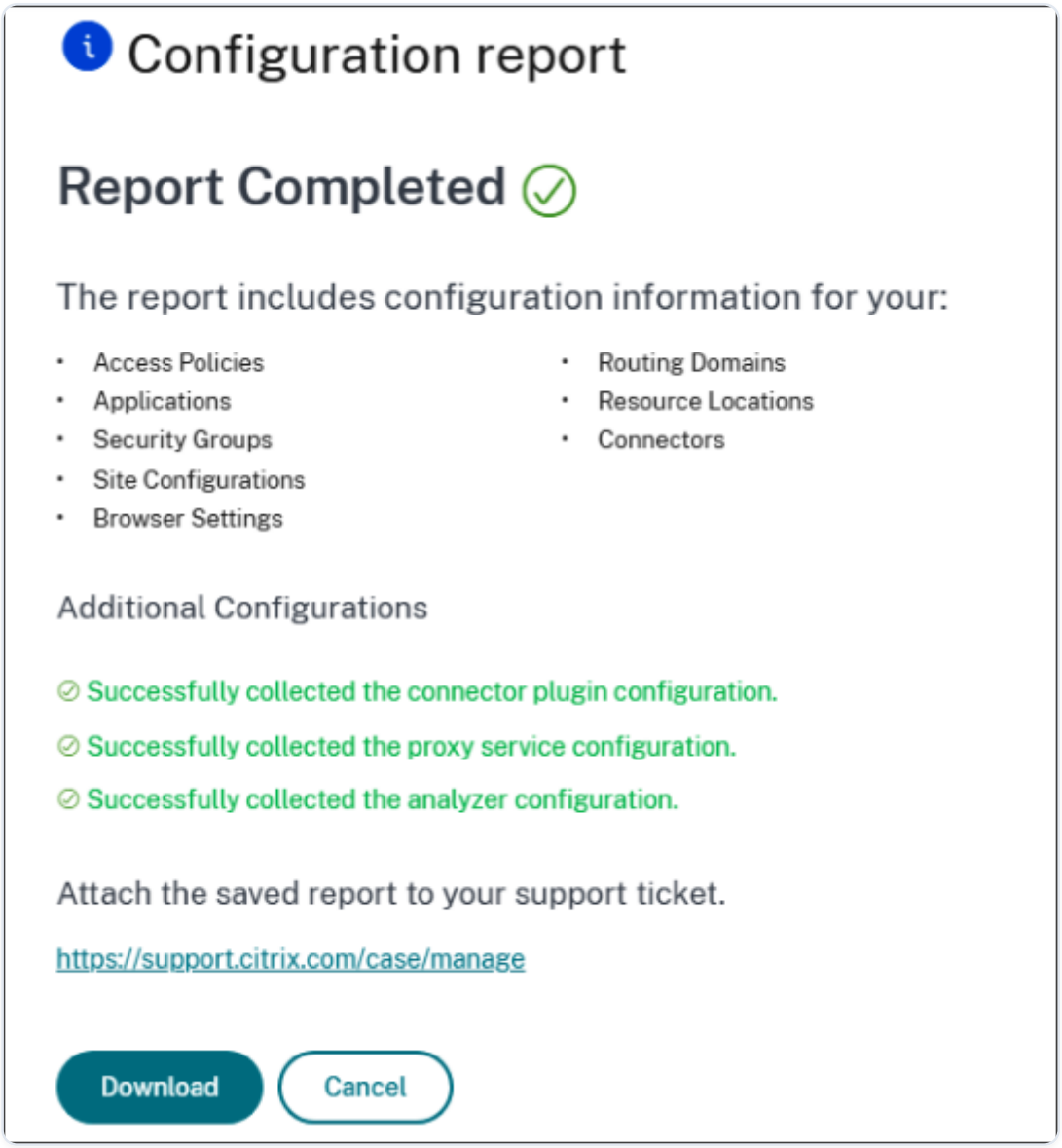
2. To include the additional reports in the bundle by collecting the configuration details stored in the connector plug-in database, the proxy service, or the analyzer configuration, check the appropriate checkboxes under the **Additional Configurations** section.
3. Click **Create report** to initiate the report generation process.

   Once the report is generated, the **Configuration Report** dialog displays the following status:

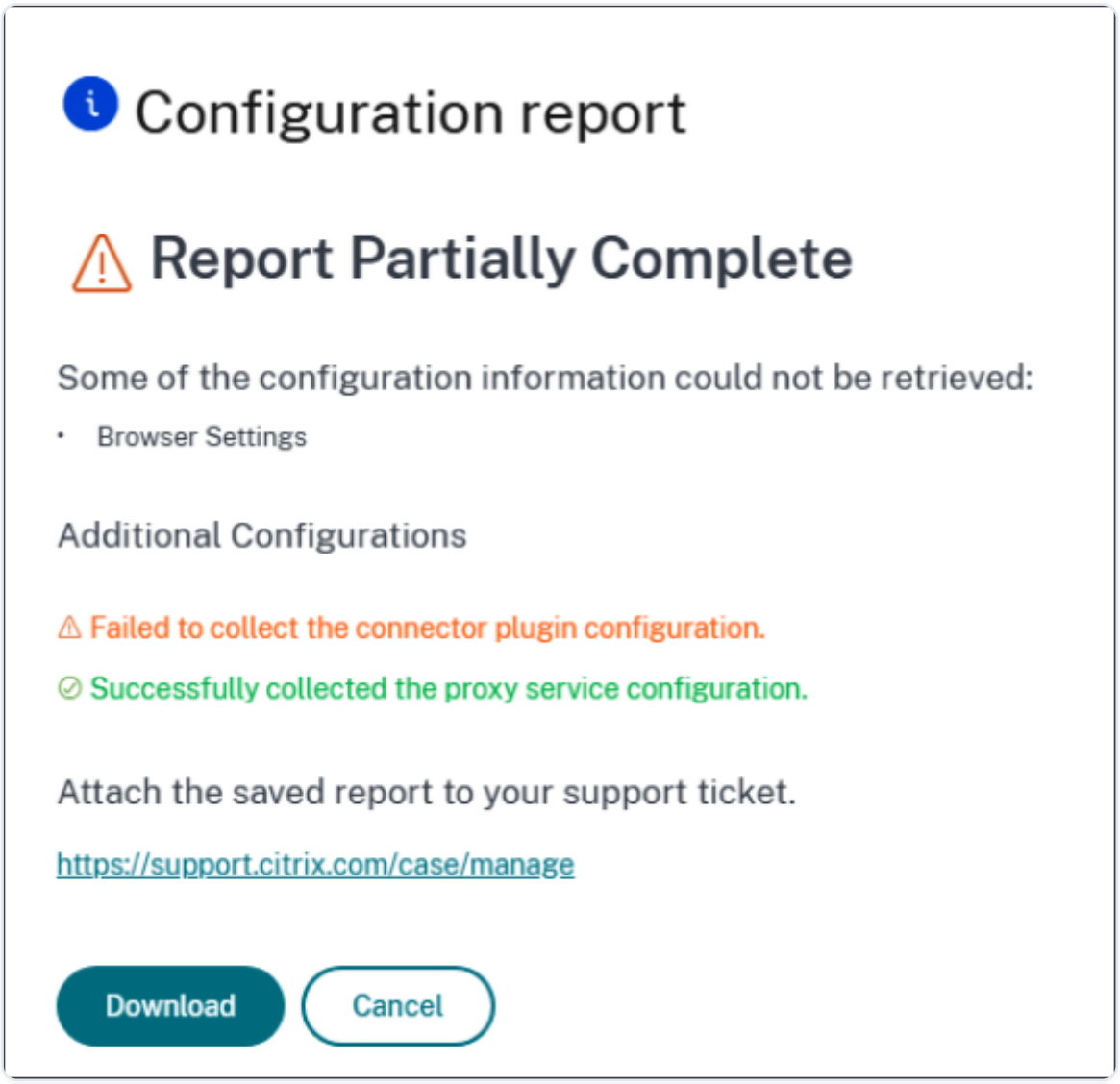
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Report Completed:** Indicates that all required details are successfully included in the report.
- **Report Partially Complete:** Indicates that some details are missing or not generated.
- The dialog also lists the categories for which the report generation was incomplete.

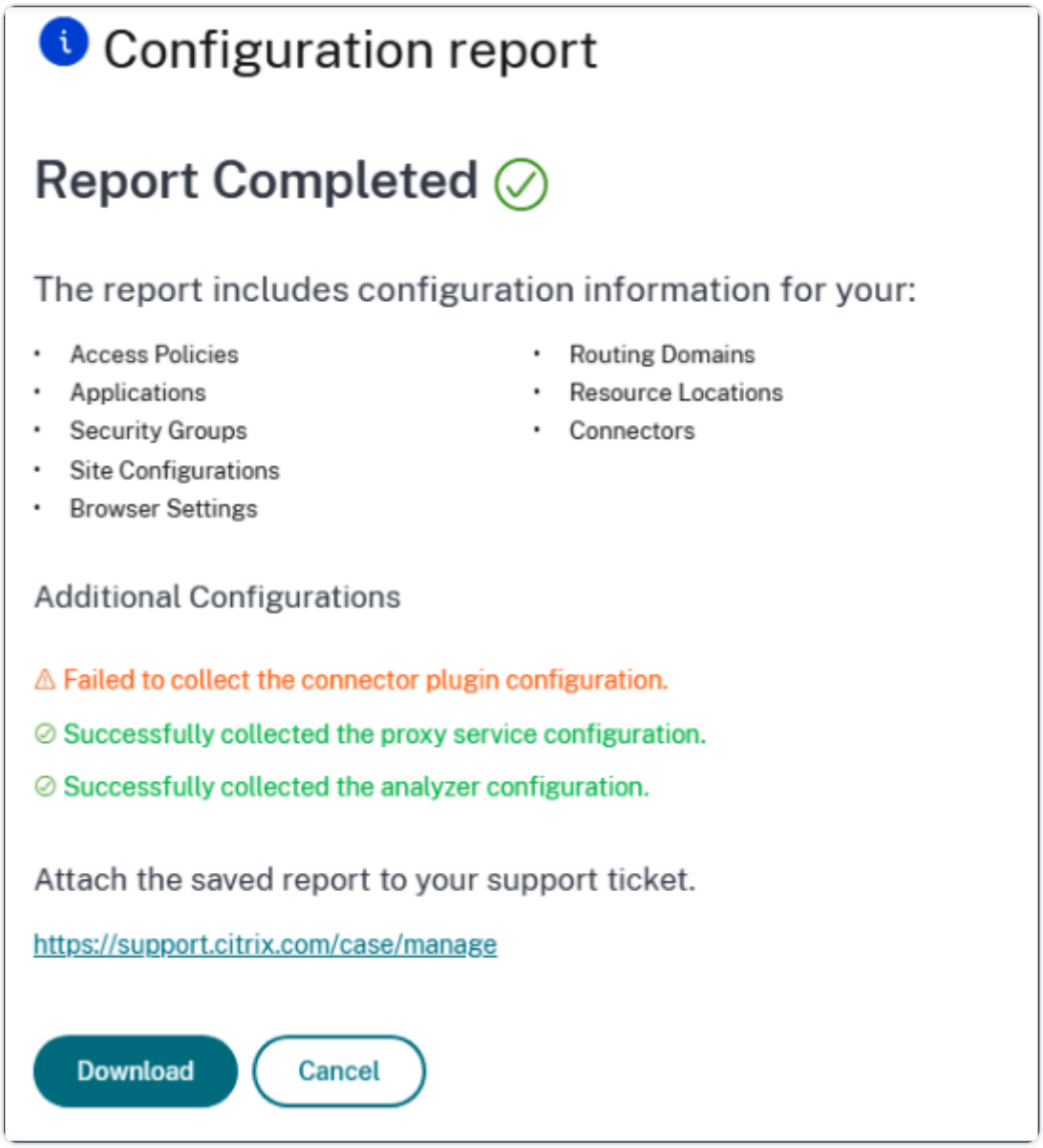
The following figure displays a sample **Configuration Report** dialog with complete and partially complete status.



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



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



4. Click **Download** to manually export the reports to your local drive.

IMPORTANT:

Generating configuration reports is limited to administrators with the following Citrix SecurAccess ZTNA roles:

- Full Access Administrator
- Read Only Administrator
- Full Monitor Administrator

Administrators with the Help Desk Administrator role cannot generate configuration reports.

Note:

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

Reports can contain sensitive data.

Manage setup configuration after installation

The **Setup configuration** menu option can be used to manage various configuration inputs provided during the onboarding.

WARNING:

Changing the configuration values can be disruptive. Since this configuration is referenced by multiple components, changes may necessitate re-configuration in dependent components to avoid service interruptions.

The following table summarizes the additional actions needed if any configuration is changed.

CONFIG NAME	ACTION NEEDED	DESCRIPTION
Step1		
Google Customer ID	Reconfigure and re-analyze NetScaler by downloading the script again.	Google services are automatically reconfigured.
Secure Private Access Gateway URL	Reconfigure and re-analyze NetScaler by downloading the script again.	Google services are automatically reconfigured.
	Note If CEP config is skipped, this setting is part of Step2.	
Google Workspace user groups	No manual action needed	New user groups are auto configured on required Google services when settings are saved.
Step2		
NetScaler Gateway virtual server name	Rerun the NetScaler Analyzer only	Use the analyze option when running the NetScaler script.

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

CONFIG NAME	ACTION NEEDED	DESCRIPTION
Secure Private Access site URL	Reconfigure StoreFront with the new Secure Private Access address.	
	Re-analyze StoreFront by downloading scripts again	
	Reconfigure and re-analyze NetScaler by downloading the script again.	
Internal IP address (for Secure Private Access Gateway URL)	Reconfigure and analyze NetScaler by downloading the script again.	
Certificate-key pair name	Reconfigure and re-analyze NetScaler by downloading the script again.	

Reset Citrix SecurAccess™ ZTNA configuration

If you have a Citrix SecurAccess ZTNA hybrid deployment with Citrix Enterprise Browser integration and you want to switch to Chrome Enterprise Premium, you can reset the Citrix SecurAccess ZTNA configuration. This action deletes the entire configuration, including applications and access policies. The StoreFront and NetScaler configurations require manual cleanup. After configuration reset, you can onboard a Citrix SecurAccess ZTNA hybrid deployment again and select Chrome Enterprise Premium.

Reach out to Citrix Support if you need to reset the configuration.

Upgrade

Periodically, Citrix releases updates to enhance the performance, security, and reliability of the Cloud Connector. By default, Citrix Cloud installs these updates on each connector, one at a time, when they become available. Citrix SecurAccess™ ZTNA is upgraded as part of the Cloud Connector upgrade by default.

For details on Cloud Connector upgrade, see, Connector updates.

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

NOTE:

NetScaler upgrade through the GUI sometimes does not install Python. It is recommended that you upgrade NetScaler through the CLI.

Refer to the following topics for details about the other components upgrade:

- StoreFront
- NetScaler Gateway

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

Advanced Citrix SecurAccess™ ZTNA features

The following are some of the advanced features supported by Citrix SecurAccess ZTNA:

- **Advanced data center configuration**: Citrix SecurAccess ZTNA hybrid deployment is supported in a multi-data center with multi-sites configuration using NetScaler GSLB in active-active site deployment with site persistency method for GSLB connection proxy. For details, see Advanced data center configuration.
- **Global server load balancing connection proxy**: The global server load balancing (GSLB) connection proxy enables NetScaler Gateway to transparently detect misrouted requests and proxy them to the correct site without any user intervention. For details, see Global server load balancing connection proxy.
- **Configure a global server load balancer domain URL**: To set up multi-site redundancy for Citrix SecurAccess ZTNA, you must configure a global server load balancer (GSLB) address. This address acts as a single entry point, routing users to a specific data center's Citrix SecurAccess ZTNA gateway based on your traffic policies, such as static proximity. For details, see Configure a global server load balancer domain URL.
- **Context-based application routing:** When an app is configured, routing types are defined for the application URL and its related domains or app destinations under app configuration. The routing type defined here applies to all users who have access to the app. However, there can be scenarios where admins want to route the same app differently based on user context. For example, an internal app URL or destination must be routed directly instead of via Citrix SecurAccess ZTNA when users are inside the corporate network. For details, seeContext-based application routing.
- **Discover domains or IP addresses accessed by end users:** The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users. For details, see Discover domains or IP addresses accessed by end users.

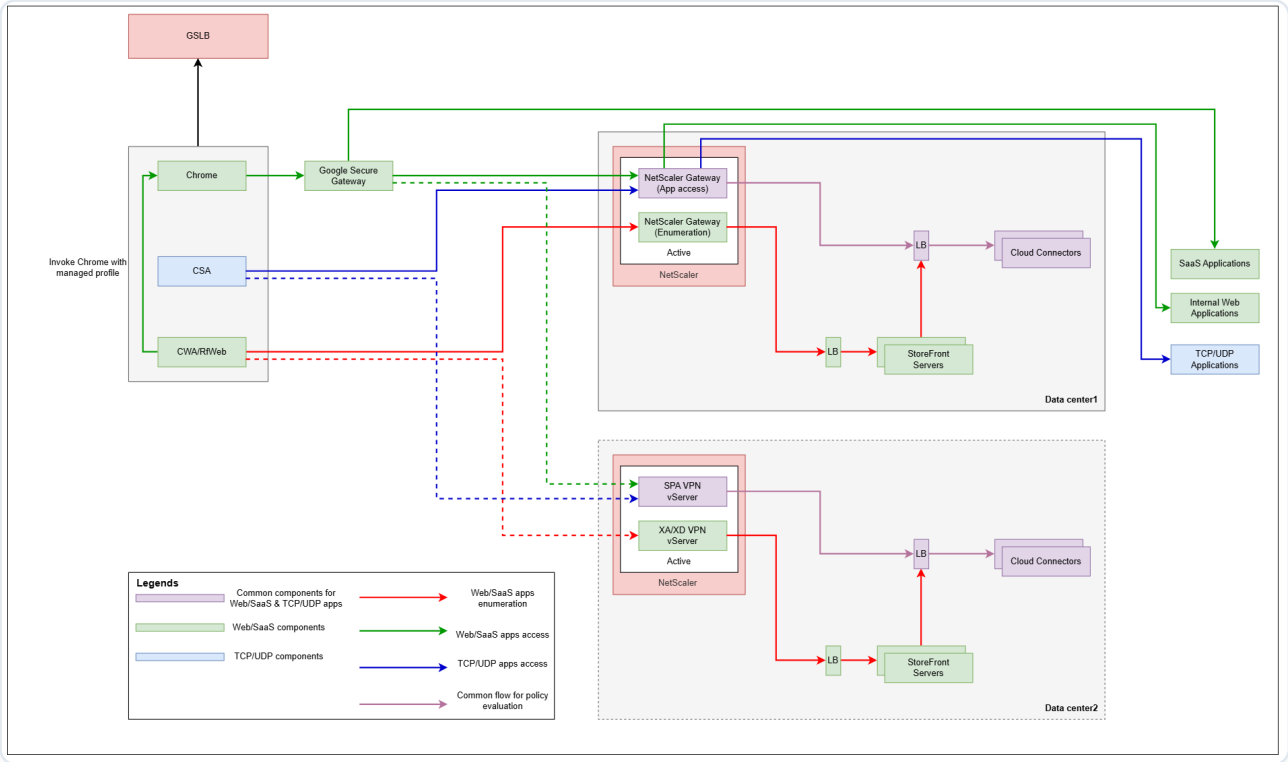
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Policy modeling tool**: Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users. That is, if the end-user is allowed or denied access based on the application and access policy configurations. The policy modeling tool (Access policies > Policy modeling) helps resolve these issues by giving the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). For details, see Policy modeling tool.
- **Configure Data Loss Prevention (DLP) policies**: Access restrictions are configured in the Google Admin console for CEP. Access restrictions that were previously configured in the Citrix SecurAccess ZTNA console only apply to Citrix Enterprise Browser. When Google Chrome is the enterprise browser, access restrictions must be configured as policies and rules in the Google Admin console. For details, see Configure Data Loss Prevention (DLP) policies.
- **High availability deployments**: You can configure high availability for Citrix SecurAccess ZTNA in just a few straightforward steps. For details, see High availability deployments.
- **Reset Citrix SecurAccess ZTNA configuration**: If you have a Citrix SecurAccess ZTNA hybrid deployment with Citrix Enterprise Browser integration and you want to switch to Chrome Enterprise Premium, you can reset the Citrix SecurAccess ZTNA configuration. For details, see Reset Citrix SecurAccess ZTNA configuration.

Advanced data center configuration

Citrix SecurAccess™ ZTNA hybrid deployment is supported in a multi-data center with multi-sites configuration using NetScaler GSLB in active-active site deployment with site persistency method for GSLB connection proxy.

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



This topic provides step-by-step instructions for setting up the Citrix SecurAccess ZTNA hybrid deployment in a multi-data center multi-site configuration.

Prerequisites

Ensure that the following prerequisites are met to deploy Citrix SecurAccess ZTNA hybrid in multi-data centers.

- NetScaler Gateway version 14.1–66.59 and later.
- NetScaler GSLB in active-active site deployment. The GSLB domain must be configured on all sites. If you have not yet configured the GSLB, see Active-active site deployment for instructions.
- Source IP persistence is enabled on GSLB.
- Connection proxy persistence is enabled for CEP session. For details, see Global server load balancing connection proxy.

GSLB configuration CLI commands

We recommend using the NetScaler CLI to configure GSLB. The following are the CLI command templates and an example configuration.

- `add service <ADNS_SERVICE_NAME> <ADNS_IP> ADNS 53`
- `add gslb site <SITE_NAME> <SITE_IP> -sitePassword "<SITE_PASSWORD>"`

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

- `add gslb service <GSLB_SERVICE_NAME> <SERVICE_IP> SSL 443 -publicIP <PUBLIC_IP> -publicPort 443 -siteName <SITE_NAME>`
- `add gslb vserver <VSERVER_NAME> SSL`
- `bind gslb vserver <VSERVER_NAME> -serviceName <GSLB_SERVICE_NAME>`
- `bind gslb vserver <VSERVER_NAME> -domainName <GSLB_DOMAIN_FQDN>`
- `set lb vserver <VSERVER_NAME> -PersistenceType SOURCEIP`
- `set gslb service <GSLB_SERVICE_NAME> -sitePersistence ConnectionProxy`
- `bind ssl service <GSLB_SERVICE_NAME> -certKeyName <SERVICE_CERT_KEY>`
- `bind ssl vserver <VSERVER_NAME> -certKeyName <CA_CERT_KEY> -CA`
- `bind ssl vserver <VSERVER_NAME> -certKeyName <EXTERNAL_CA_CERT_KEY> -CA`
- `bind ssl vserver <VSERVER_NAME> -certKeyName <SERVER_CERT_KEY>`

References

The following table summarizes the placeholders used in the CLI commands and a brief description of the same.

Placeholder	Description
`<ADNS_SERVICE_NAME>`	Name of the ADNS service (for example, adns_`<env>`)
`<ADNS_IP>`	IP address of the ADNS listener on this NetScaler
`<SITE_NAME>`	GSLB site identifier (for example, blue, green)
`<SITE_IP>`	GSLB site IP (SNIP or management IP used for MEP communication)
`<SITE_PASSWORD>`	Shared secret for GSLB site-to-site MEP authentication
`<GSLB_SERVICE_NAME>`	Name of the GSLB service bound to a local/ remote load balancing virtual server
`<SERVICE_IP>`	IP address of the backend load balancing virtual server or service

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

`<PUBLIC_IP>`	Public (NAT) IP address reachable from the internet
`<VSERVER_NAME>`	Name of the GSLB virtual server
`<GSLB_DOMAIN_FQDN>`	FQDN that GSLB resolves for clients
`<SERVICE_CERT_KEY>`	SSL certificate key name bound to the GSLB service
`<CA_CERT_KEY>`	Internal CA certificate key name (bound as -CA)
`<EXTERNAL_CA_CERT_KEY>`	External/public CA certificate key name (bound as -CA)
`<SERVER_CERT_KEY>`	Server certificate key name bound to the virtual server

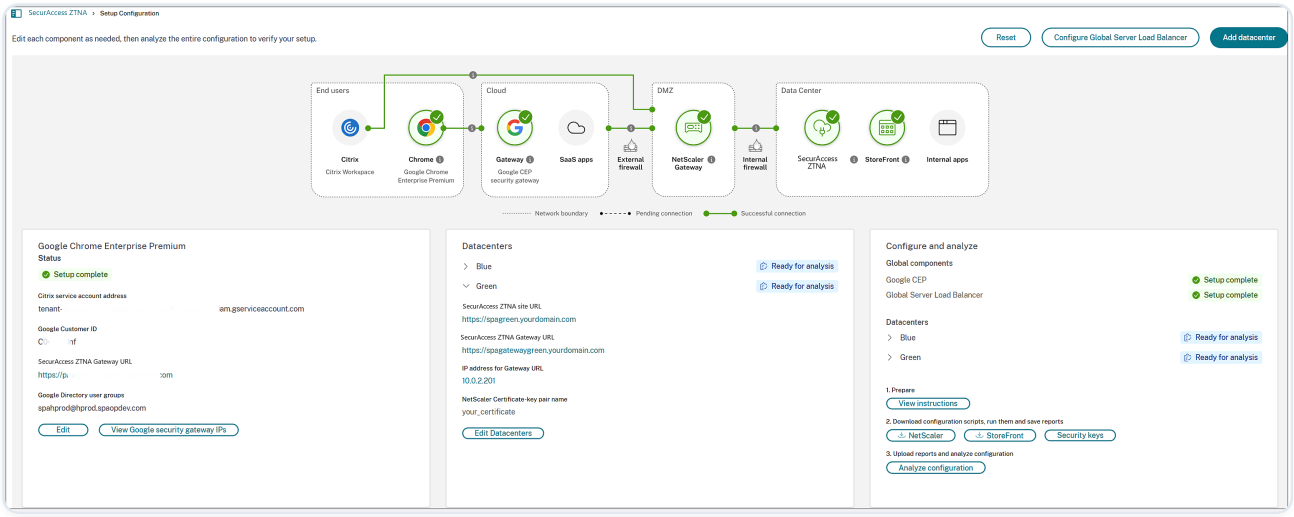
Example configuration:

- `add service adns_staging 10.100.5.50 ADNS 53`
- `add gslb site us-east-dc1 10.100.5.60 -sitePassword "password"`
- `add gslb service us-east-dc1-svc1 10.100.5.80 SSL 443 -publicIP 203.0.113.42 -publicPort 443 -siteName us-east-dc1`
- `add gslb vserver staging_us-east_vs SSL`
- `bind gslb vserver staging_us-east_vs -serviceName us-east-dc1-svc1`
- `bind gslb vserver staging_us-east_vs -domainName proxy-staging.example.com`
- `set lb vserver staging_us-east_vs -PersistenceType SOURCEIP`
- `set gslb service us-east-dc1-svc1 -sitePersistence ConnectionProxy`
- `bind ssl service us-east-dc1-svc1 -certKeyName star_staging_local`
- `bind ssl vserver staging_us-east_vs -certKeyName ca_staging.local -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName CA.csg.proxy.ext.example -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName csg.proxy.ext.example`

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

Data centers setup and configuration

The following figure displays a topology diagram of Citrix SecurAccess ZTNA hybrid deployment in a multi-data center.



1. Add data centers. For details, see Step 2: Set up the first data center.
2. For each data center, download and run the NetScaler and StoreFront scripts. For details, see Download and run NetScaler and StoreFront scripts.
3. For each data center, upload reports and analyze configurations. For details, see Upload reports and analyze configuration.
4. Review the analysis results.

If all analyzer steps have passed for each data center, you have successfully validated your configuration and can proceed with post-onboarding tasks. For details, see Post-onboarding tasks.

Global server load balancing connection proxy

The global server load balancing (GSLB) connection proxy enables NetScaler Gateway to transparently detect misrouted requests and proxy them to the correct site without any user intervention.

In multi-site Citrix SecurAccess™ ZTNA hybrid deployments that use GSLB, DNS resolution might occasionally route a user request to a non-intended site. When this occurs, the user lands on a site where their session was not established, which can prevent access to internal web applications.

The GSLB connection proxy addresses this issue by enabling NetScaler Gateway to transparently detect misrouted requests and proxy them to the correct site without any user intervention. This process is transparent to end users and improves session persistence and eliminates dropped sessions and application access failures caused by non-optimal DNS routing.

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

Prerequisites

Ensure that the following prerequisites are met to support GSLB connection proxy:

- Multi-site Citrix SecurAccess ZTNA hybrid deployment with GSLB configured across all sites.
- Source IP persistency is enabled on GSLB. For details, see Configure persistence based on source IP address.
- Static proximity is configured (IP database managed by the administrator). For details, see Static proximity.
- NetScaler Gateway version is 14.1 or later.

Configure GSLB connection proxy

To enable the GSLB connection proxy, bind a certificate to all GSLB services and the VPN virtual server:

1. Generate a self-signed client certificate with a common name, for example `csg.proxy.ext.goog`.
2. Bind the certificate to all GSLB services across all sites.
3. Bind the issuer certificate to the VPN virtual server as a CA certificate.
4. Repeat the service binding for every GSLB service on every site in the deployment.

CLI commands:

- Bind the certificate to a GSLB service.

  ```
  bind ssl service <gslb-service-name> -certKeyName <certificate-name>
  ```

- Bind the issuer certificate to the VPN virtual server.

  ```
  bind ssl vserver <vpn-vserver-name> -certKeyName <certificate-name> -CA
  ```

Configure a global server load balancer domain URL

To set up multi-site redundancy for Citrix SecurAccess™ ZTNA, you must configure a global server load balancer (GSLB) address. This address acts as a single entry point, routing users to a specific data center's Citrix SecurAccess ZTNA gateway based on your traffic policies, such as static proximity.

When configuring GSLB for a Citrix SecurAccess ZTNA deployment, the GSLB address must be updated within the Google Secure Gateway (in Google Cloud service). If a data center-specific

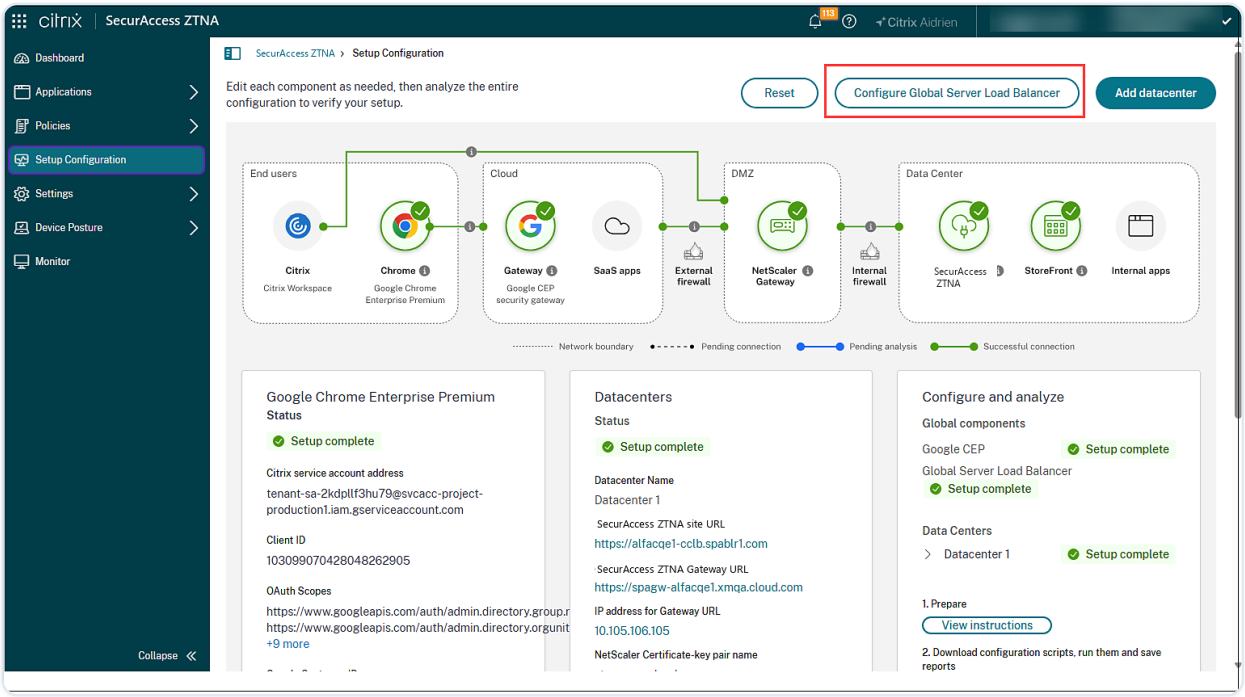
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix SecurAccess ZTNA gateway was previously used, providing the GSLB address automatically overrides the existing configuration to point to the new global address.

Configuration

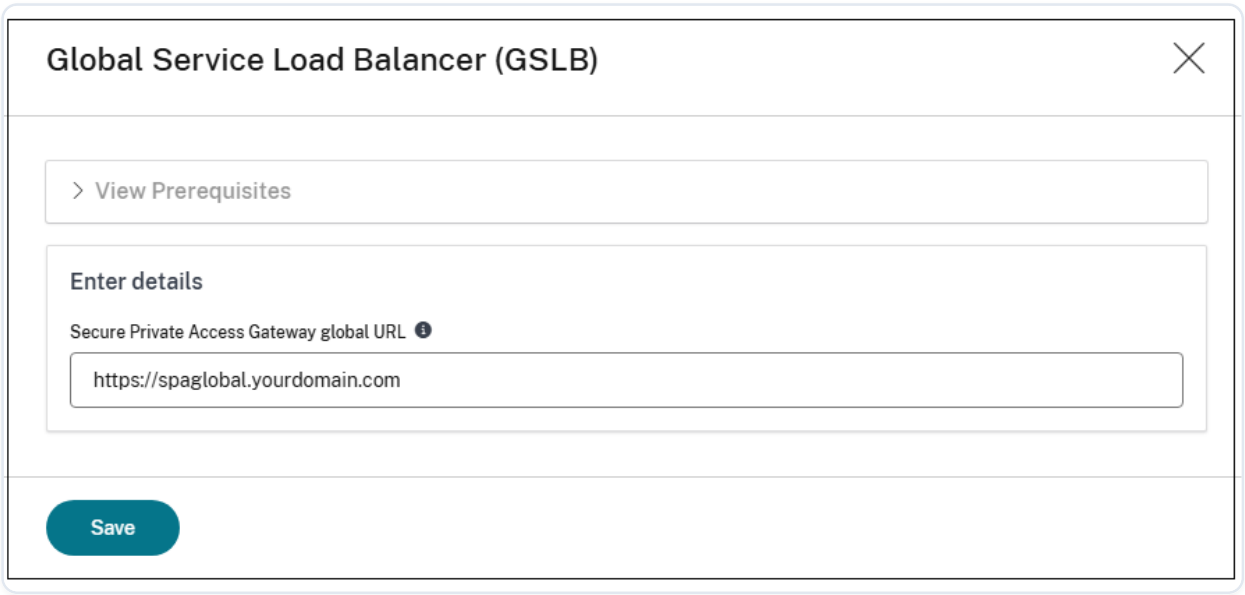
When prompted, enter the global server load balancer (GSLB) domain URL details to update the Chrome Enterprise Premium (CEP) configuration with the GSLB domain. After this update, reconfigure the NetScaler Gateway in the first data center.

1. Log in to **Citrix SecurAccess ZTNA** admin console.
2. Go to **Setup Configuration**.
3. Click **Global Server Load Balancer (GSLB)**.



4. Enter the public address of the GSLB domain URL in the **Citrix SecurAccess ZTNA Gateway URL** field.

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



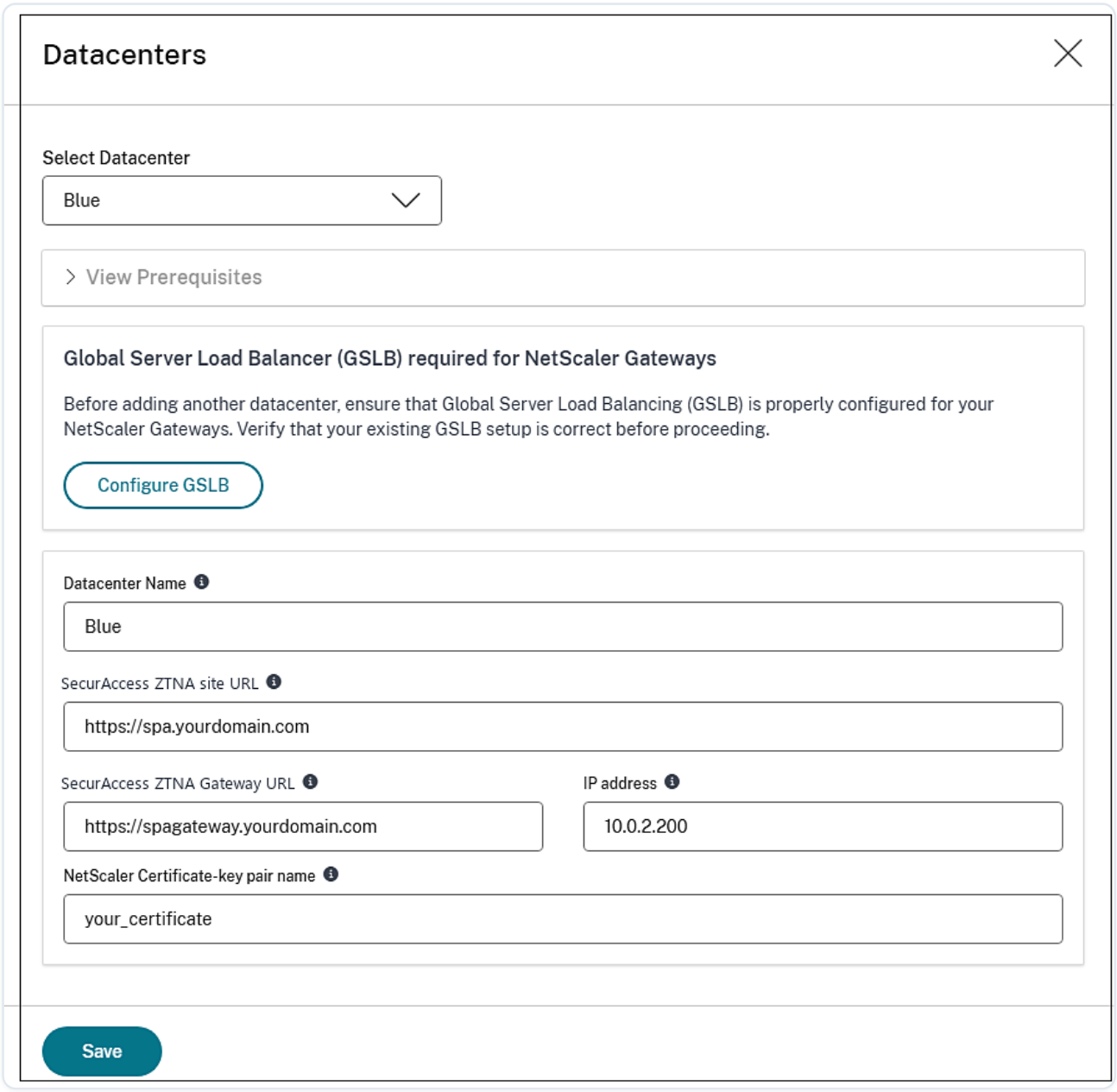
NOTE:

This updates the CEP integration and replaces the Citrix SecurAccess ZTNA Gateway URL with the GSLB domain URL that you entered.

Edit data center (optional)

This step is required only if you need to change a data center.

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



Configure and analyze

After you complete the preceding steps, you can update the configuration for the on-premises StoreFront and NetScaler components in the first data center.

Follow Step 3: Configure and analyze to complete re-configuration of the NetScaler components of the data center and analyze the NetScaler and StoreFront configuration, if necessary.

Context-based application routing

When an app is configured, routing types are defined for the application URL and its related domains or app destinations under app configuration. The routing type defined here applies to all users who have access to the app. However, there can be scenarios where admins want to route

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

the same app differently based on user context. For example, an internal app URL or destination must be routed directly instead of via Citrix SecurAccess™ ZTNA when users are inside the corporate network.

You can configure this using **Routing Exceptions** in access policies (for specific users) or session policies (all users). The Routing Exceptions configuration in the access policies allows admins to edit the routing type for users or machines that match the conditions defined in the policy. Because this setting is part of an access policy, it applies only to the users and machines included in that policy.

> **NOTE:**
>
> If there is a routing configuration within an access policy, then it overrides the app configuration.

The following examples demonstrate the routing exception use cases.

- Context-based routing
- Route internal corporate users directly to back-end applications

Use case: Context-based routing

Scenario:

- Group A users: Employees of company ABC who access the Outlook app and Microsoft Teams app through NetScaler Gateway that is routed internally.
- Group B users: Employees of a third-party company working with ABC. They access certain applications (excluding Outlook) through NetScaler Gateway. They also have their own Outlook application accessed over the internet and do not want to route their Outlook traffic through NetScaler Gateway.

Problem:

- Group B users log in to the Secure Access client to access ABC apps.
- Their requests to access Outlook through their native browser are routed through NetScaler Gateway, resulting in access denial.
- The destination domain for the Outlook application is the same for both Group A and Group B users.

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

- The access policy allows access only for Group A users, causing access denial for Group B users when they try to launch Microsoft Teams or Outlook.
- Group B users cannot access their company Outlook because of this routing issue.

Solution:

The ABC company admin can make the following configuration changes to resolve this issue:

1. Define a new access policy specifically for Group B users accessing the Office 365 app.
2. In the access policy, enable the **Routing exceptions** option.

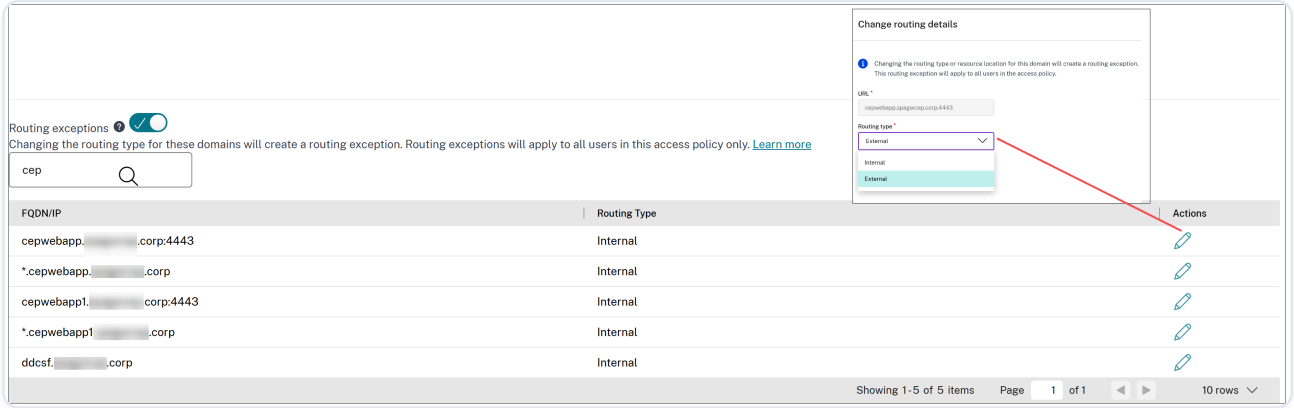
   The admin can view the list of all URLs and related domains of all internal apps associated with the access policy.
3. For all Office 365 app URLs, configure the routing to happen externally.

   This ensures that Group B users' requests to access their Outlook application are routed over the internet, bypassing NetScaler Gateway.

   By implementing these changes, Group B users can access their company Outlook application over the internet without being routed through NetScaler Gateway, while still maintaining access to other ABC applications as needed.

Steps to change the routing type

1. Create or edit an access policy. For detailed instructions, see Configure access policies.
2. In the access policy, enable the **Routing exceptions** toggle to ON.
3. From the list of app URLs and related domains associated with the access policy, locate the domains whose routing type you want to change.
4. Change the routing type (for example, from **Internal** to **External**) for the selected domains based on the user context you want to apply.
5. Save the access policy.



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

Use case: Route internal corporate users directly to back-end applications

Admins can configure session policies to route internal corporate users directly to back-end apps without tunneling traffic through NetScaler Gateway. Session policies offer dynamic routing based on factors, such as network location and device posture.

For details on configuring a session policy, see Configure session policies.

NOTE:

- Session policy settings are applied at the session level to all applications rather than being tied to specific applications.
- Session policies can be assigned to all users or a subset of users.

Routing precedence

Session policies work alongside access policies, with access policies taking precedence if there is a conflict. In such scenarios, access policy routing exceptions override session policies. If neither an access policy nor a session policy is configured, global routing settings (**Settings > Application Domain**) apply.

Supported Citrix SecurAccess™ clients

The following versions of Citrix SecurAccess client support routing of users directly to the back-end applications.

- macOS - 24.11.1 and later.
- Windows - 24.11.1.17 and later. Also, the **EnableContextualAccess** VPN client registry must be enabled. For more information, see NetScaler Gateway Windows VPN client registry keys.

Example use case

Scenario:

In a hospital, when users are connected to the hospital network "hospital_network1", then traffic from apps must flow directly to the back-end apps, as these apps are directly reachable on the hospital network. If the users are outside the hospital network, then the app traffic must be tunneled.

Solution:

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

1. Add app1, app2 with routing set to **Internal**.
2. Add an access policy for the apps (app1, app2) to grant access.
3. Add a session policy to configure conditions to specify the user group and network locations that must be considered when granting access.
4. Select the **User** condition and set it to **All users**.
5. Add a **Network Location** condition. Set it to **Matches any of** and specify the network location "hospital_network1". This ensures that traffic coming from "hospital_network1" flows directly to the back-end apps.

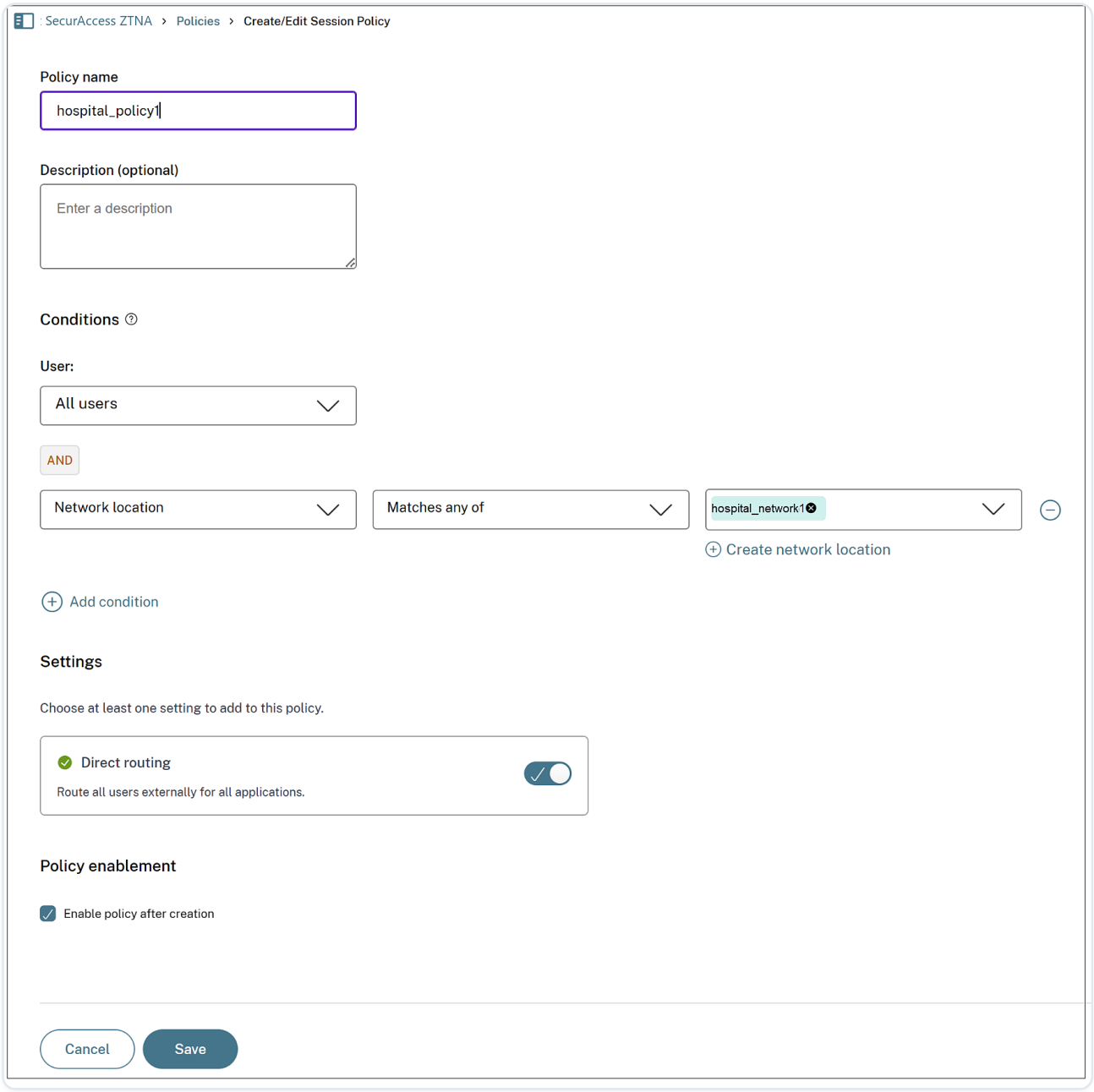
You can also enable routing exceptions for this scenario. For example, if app1 must always be tunneled even on the hospital network, then routing exceptions can be configured for domains of app1 in the access policy. When this is done, the routing exception takes precedence over the session policy.

Configure direct routing within the hospital network using session policies

You can use a session policy to allow users to directly access back-end applications by bypassing the NetScaler Gateway tunneling.

For details on configuring a session policy, see Configure session policies.

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



Discover domains or IP addresses accessed by end users

The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users.

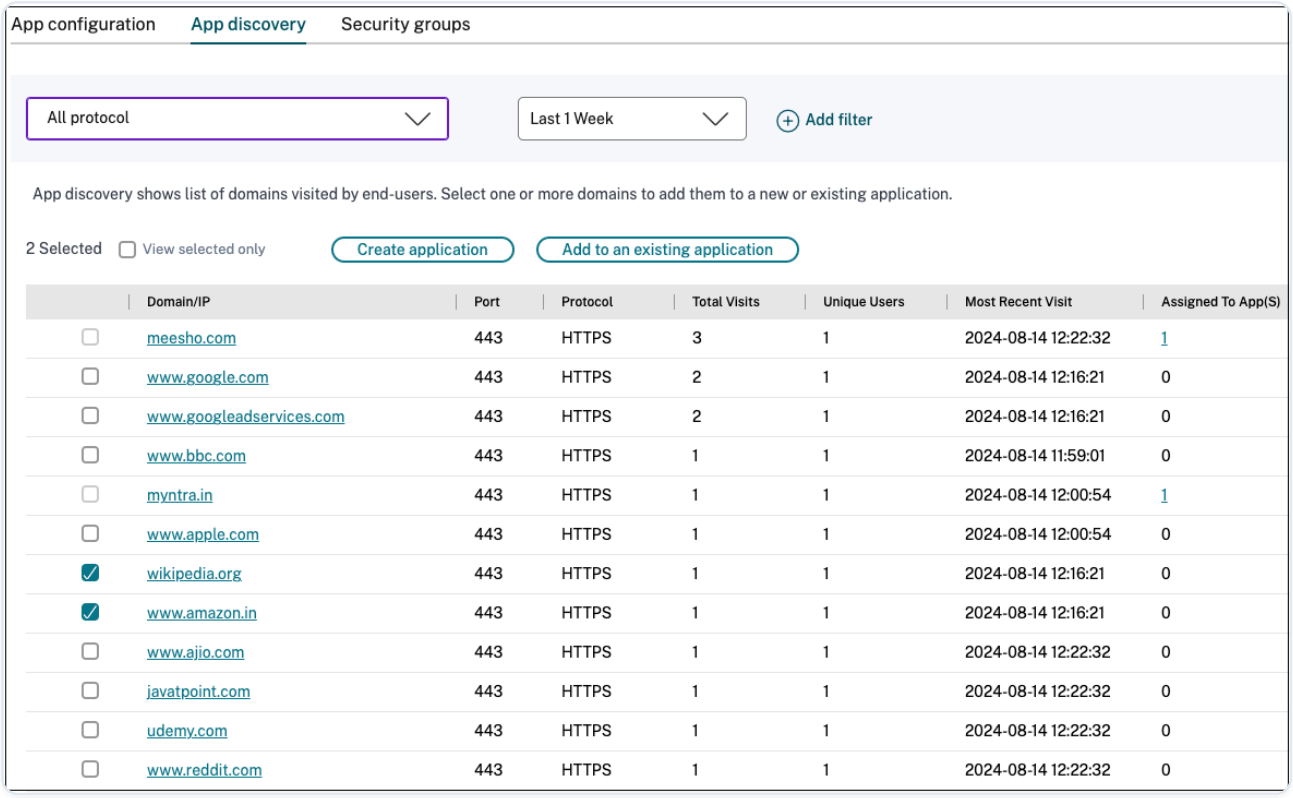
The Application Discovery feature provides the following capabilities to the admins:

- Provides visibility into both internal or external domains/IPs addresses accessed by the end users.

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

- Provides a comprehensive visibility into all types of applications accessed (HTTP, HTTPS, TCP, and UDP). Access Citrix Enterprise Browser™ and Citrix SecurAccess™ agent are supported.
- Displays both published or unpublished domains/IP addresses accessed by the end users.

The following figure displays a sample **App discovery** page. The **App discovery** page allows filtering of domains based on the protocol (HTTP/HTTPS, TCP/UDP) and Domain/IP address and port numbers. It also displays the unpublished (not assigned to any app) domains accessed by the end users.



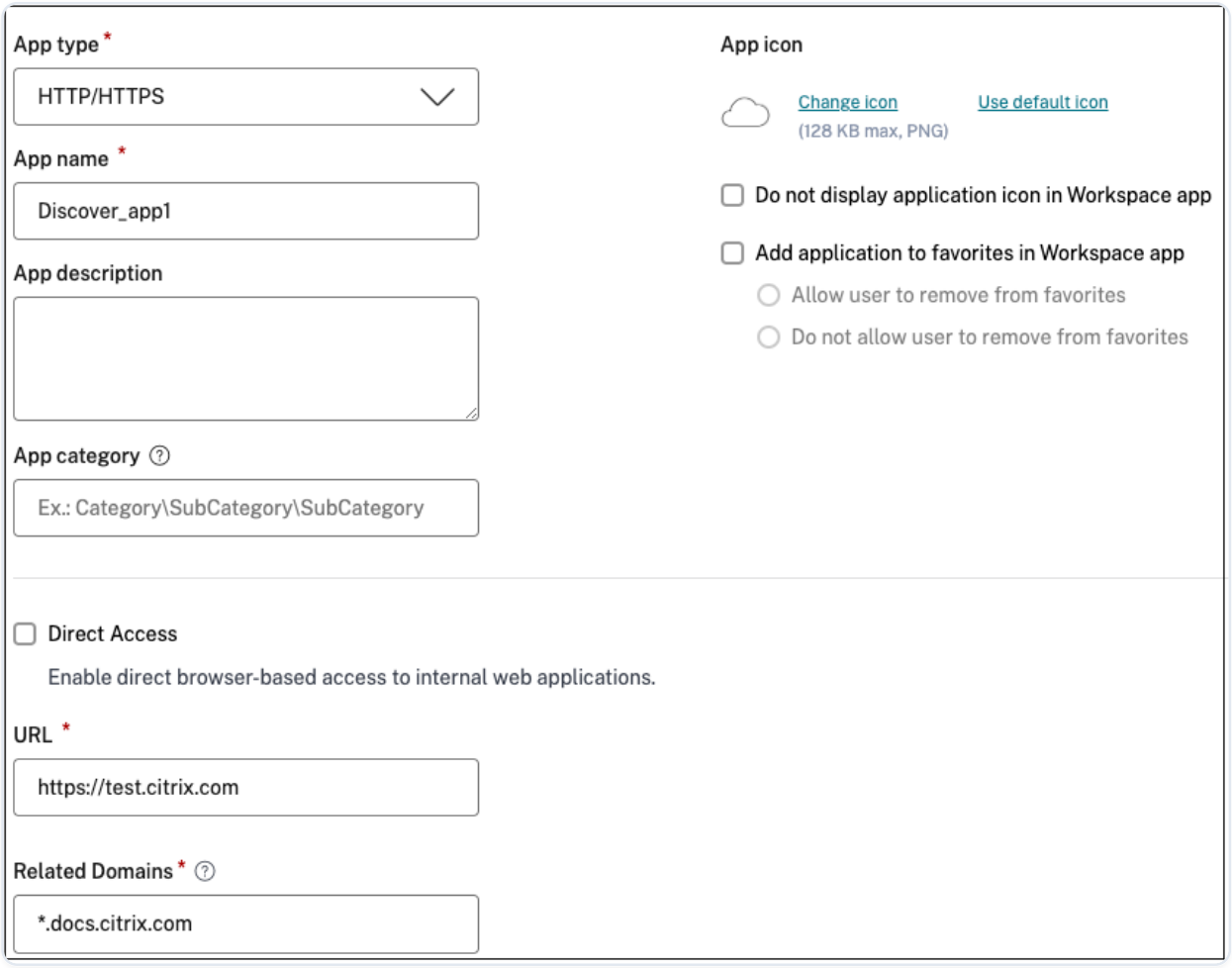
Application Discovery for internal domains in a new environment

The Application Discovery feature can be used if you are setting up a new Citrix SecurAccess™ ZTNA environment and want visibility into the applications that are to be configured. This feature discovers and lists all domains/IPs addresses that are accessed by your end users so you can configure them as applications. Use the following steps to enable the Application Discovery feature when you are setting up your Citrix SecurAccess ZTNA environment:

- To discover internal web applications, configure an application within Citrix SecurAccess ZTNA and specify the wildcard related domain that belongs to the domain/subdomain of the applications that you want to discover.

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

For example, if you want to discover all applications with the domain citrix.com, create an application with a related wildcard domain as `*.citrix.com`. To allow completion of application configuration, add any test URL as the main web app URL section.



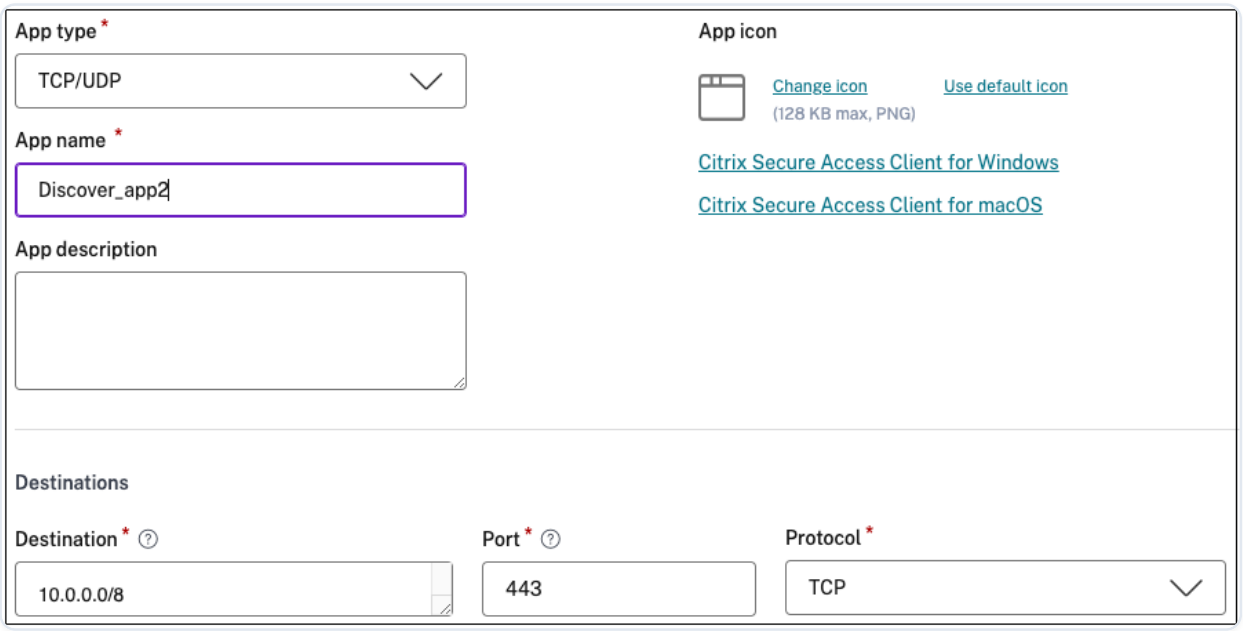
Web app URL: `https://test.citrix.com/` Related domain: `*.citrix.com`

- For internal TCP/UDP apps, configure an application within Citrix SecurAccess ZTNA and specify the subnet along with the TCP/UDP protocol and range of ports (enter `*` to include the entire range). This enables discovering all TCP and UDP apps from the Citrix SecurAccess agent. For example, if you want to discover all applications within subnet 10.0.0.0/8, then configure the app with the following details: Example: 10.0.0.0/8:

  Port: (*)

  Protocol: TCP

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



- Once you have created the applications, you must also define users that are allowed access to apps with the configured domains and IP subnets. Create an access policy and assign users to whom you want to allow access to the FQDNs/IP addresses configured in the applications created. These can be an initial set of test users or a limited number of users you want to give access to initially.
- After creating the applications and corresponding access policies, users can continue to access applications from the Citrix Workspace app and access different domains. All FQDN/IP addresses accessed by the end users start to show up in the Application Discovery page.

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

NOTE:

- Once you have discovered and identified most of the applications over a few days/weeks, we recommend deleting the initially created applications so that the wider access given via the wildcard domains and IP subnets can be closed down, and only specific application URLs and IP addresses that are discovered must be allowed access via new applications.
- Add the prefix `Discover` in the app name to indicate that this is a special app configuration to enable discovery monitoring and reporting. This naming helps you identify to remove the wild card domains or IP subnets or both so you can reduce the overall app access zone to just the specific FQDNs and IP/port combinations later in weeks or a month.
- To access TCP/UDP apps, users must use the Citrix SecurAccess agent. App access from various access methods is monitored based on the apps' domains and subnets configuration and reported within the **App Discovery** page.
- Even after you have removed the discovered applications, this feature keeps on discovering domains/IP addresses accessed by your users. So at any time, you can come back to the **App Discovery** page to see what is being accessed and if there are any new domains/IP addresses discovered that must be configured as applications.

For details on adding the domains, FQDNs, or IP address, see the following topics.

- Configure HTTP/HTTPS applications
- Configure TCP/UDP apps

Create an application from the App discovery page

To create an application for main domains and unpublished domains from the **App discovery** page, do the following steps:

1. Navigate to **Applications > App discovery**.
2. Select a domain from the list.

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

NOTE:

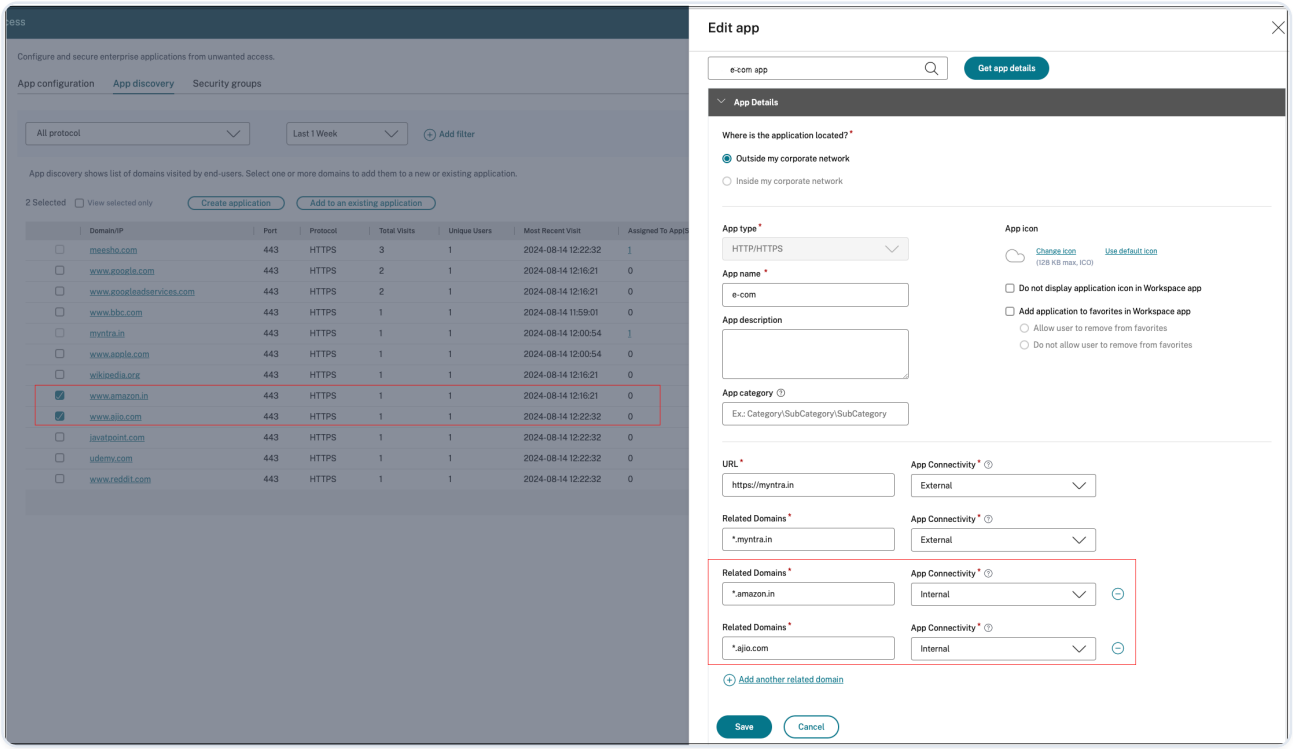
- You cannot select domains belonging to different protocols to create an application. An error message is displayed when you select domains belonging to different protocols.
- If a domain is already associated with an application, you cannot select that domain again to create an application. The checkbox corresponding to that domain appears grayed out and when you hover the mouse over the checkbox, a tooltip appears.

3. Click **Create application**. For details on creating an application, Configure HTTP/HTTPS applications and Configure TCP/UDP apps.

Update an existing application

To add a domain to an existing application, perform the following steps:

1. Select the domain that must be added to an application.
2. Click **Add to an existing application**.
3. In **Applications**, select the application to which you want to add these domains.
4. Click **Get app details**.
5. The **Related Domains** field displays all the domains that you selected earlier in separate rows.
6. Click **Finish**.



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

NOTE:

- You can only add a TCP/UDP destination IP address to an existing TCP/UDP application. The **Applications** field lists only the TCP/UDP apps configured in the system.
- You can select an existing HTTP/HTTPS or TCP/UDP app to add domains (main or single entry) whose protocol is HTTP/HTTPS.
- You cannot select a domain that is already associated with an application.

Policy modeling tool

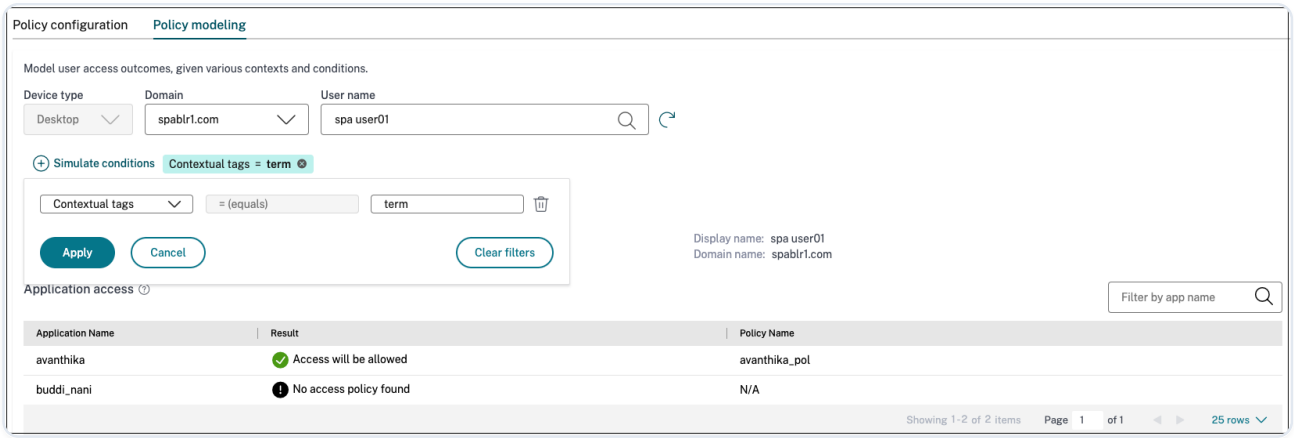
Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users. That is, if the end-user is allowed or denied access based on the application and access policy configurations. The policy modeling tool (**Access policies > Policy modeling**) helps resolve these issues by giving the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. The tool also displays the list of policies associated with the applications.

To analyze the access policy configuration, perform the following steps.

1. In the Citrix SecurAccess™ ZTNA console, click **Access Policies** and then click the **Policy modeling** tab.
2. Add the following details:
   - **Device type**: Desktop is selected by default.
   - **Domain**: Select the domain associated with the user.
   - **User**: Select the user name for which you want to analyze the applications and associated policies.
3. You can also simulate a condition based on contextual tags on the end user and their devices.
   a. Click **Simulate conditions**. The condition **Contextual tags** is selected by default.
   b. Enter the contextual tag in **Value**.
   c. Click the **+** sign to add other conditions.
4. Click **Apply**.

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

The applications and associated policies for the selected user are displayed in a tabular format.



Configure Data Loss Prevention (DLP) policies

Access restrictions are configured in the Google Admin console for CEP. Access restrictions that were previously configured in the Citrix SecurAccess™ ZTNA console only apply to Citrix Enterprise Browser. When Google Chrome is the enterprise browser, access restrictions must be configured as policies and rules in the Google Admin console.

Policies are configured in the **Google Admin console > Devices > Chrome > Settings**. These settings allow you to manage browser settings, such as block JavaScript and allow list of printers.

Rules are configured in **Google Admin console > Rules**. These rules are advanced settings related to DLP, such as adding a watermark, blocking the download of files with social security numbers, and URL filtering.

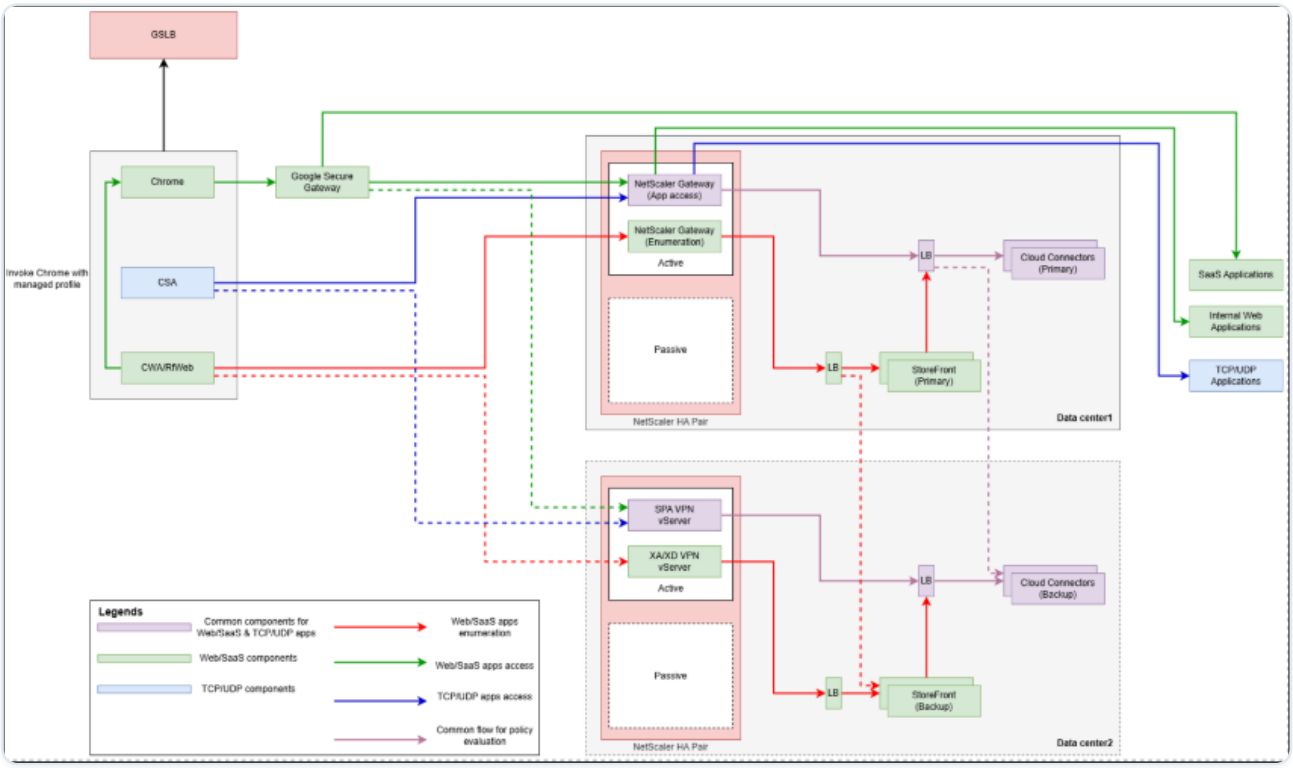
For details on creating policies and rules in the Google Workspace Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

High availability deployments

You can configure high availability for Citrix SecurAccess™ ZTNA in just a few straightforward steps.

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



High availability within the data center

The following sections provide more information about high availability within the data center.

NetScaler

For high availability, it is recommended to Create NetScaler high-availability Pair. This is an active-passive NetScaler pair.

If the active NetScaler is down, the passive NetScaler is automatically promoted as active, and all user traffic is routed to the new active NetScaler. Users are not required to re-authenticate as the sessions are also synchronized across the NetScaler high availability pair.

For more details on NetScaler HA pair, see High Availability.

Cloud Connectors (Citrix SecurAccess ZTNA servers)

Configure a NetScaler load balancer for Citrix SecurAccess ZTNA with service group configuration.

1. **Create a new service group on NetScaler:** Navigate to **Configuration > Traffic Management > Load Balancing > Service Groups**.
2. Click **Add**.
3. Enter a **Name** for the service group, for example, `primary_spa_servers`.
4. Depending upon the type of load balancer (**SSL** or **SSL_BRIDGE**), choose the appropriate **Protocol** for the service group.

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

5. Leave other fields with default values and click **OK** to save the service group.
6. Click **No Service Group Member** to add Cloud Connectors from the current data center.
7. Use the **IP Based** option and add the current data center's Cloud Connectors **IP address** and **Port**. By default, Citrix SecurAccess ZTNA uses port **8443**. Other fields can be retained with default values.
8. Repeat this step if additional Cloud Connectors must be added.
9. Click **Create** to create the load balancer service.
10. Click **OK** to add the service to the service group.

> **NOTE:**
>
> Optionally you can add an HTTP Monitor for the Citrix SecurAccess ZTNA service. The following URL path can be used to do so.

`/secureAccess/health`

It returns **200 OK** if Citrix SecurAccess ZTNA is up and running.

11. Click **Done**.
12. Now create a load balancer. Navigate to **Configuration > Traffic Management > Load Balancing > Virtual Servers**.
13. Click **Add**.
14. Enter a load balancer name.
15. Choose the appropriate **Protocol**, for example, **SSL** or **SSL_BRIDGE**.
16. Set **IP Address Type** as **IP Address** and **Port** as `443`.

> **NOTE:**
>
> The protocol must be SSL or SSL_BRIDGE. HTTP type is not supported for Citrix SecurAccess ZTNA load balancer. The port must be 443. Custom HTTPS ports are not supported.

17. Click **OK**.
18. Click **No Load Balancing Virtual Server ServiceGroup Binding**.
19. Click to select the service group created earlier, then click **Select**.
20. Set **Order** value as **10**. Click **Bind**, then **Continue**.

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

21. If using **SSL** type **Protocol**, click **No Server Certificate** to bind the appropriate server certificate. For SSL_BRIDGE type load balancer, no server certificate is required in the load balancer, but the server certificate must be configured in the Cloud Connector for Citrix SecurAccess ZTNA service. For details, see Configure TLS/SSL certificates for the Citrix SecurAccess ZTNA service on Cloud Connector.

This concludes the load balancer configuration with the service group for Citrix SecurAccess ZTNA.

All the Citrix SecurAccess ZTNA servers in the load balancer are active. If one Citrix SecurAccess ZTNA server goes down, users are not impacted as the other Citrix SecurAccess ZTNA servers continue to serve the traffic. The Citrix SecurAccess ZTNA servers are stateless, so there is no persistency requirement.

StoreFront servers

StoreFront servers also behave the same as Citrix SecurAccess ZTNA servers during failover within the same data center.

Reset Citrix SecurAccess™ ZTNA configuration

If you have a Citrix SecurAccess ZTNA hybrid deployment with Citrix Enterprise Browser integration and you want to switch to Chrome Enterprise Premium, you can reset the Citrix SecurAccess ZTNA configuration. This action deletes the entire configuration, including applications and access policies. The StoreFront and NetScaler configurations require manual cleanup. After configuration reset, you can onboard a Citrix SecurAccess ZTNA hybrid deployment again and select Chrome Enterprise Premium.

Reach out to Citrix Support if you need to reset the configuration.

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

Visibility and monitoring

Citrix SecurAccess™ ZTNA is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Citrix SecurAccess ZTNA dashboard.

Service entitlements

To use the DaaS Monitor feature with Citrix SecurAccess ZTNA, you must have both Citrix SecurAccess ZTNA and DaaS entitlements.

Supported clients

- Citrix Workspace™ app - 2409 and later
- Citrix SecurAccess for Windows - 24.8.1.19 and later
- Citrix SecurAccess for macOS - 24.10.1 and later

How to access Monitor

You can access Monitor from the Citrix SecurAccess ZTNA dashboard (**Go to Monitor**) or from the Citrix DaaS™ service tile.

In the **Monitor** page, search for the user to view the sessions.

Session definitions

A Citrix SecurAccess ZTNA session offers a comprehensive summary of an end-user’s session lifecycle, application activity, and user experience on a specific device. A session serves as a unified record for troubleshooting and analysis by providing visibility into the following aspects:

- Detailed insights into how applications are accessed, including launch hops, network topology, connections, and routing details. These details are crucial for resolving issues related to access policies.
- Tracks all session activity from:

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

    - Browsers accessing web or SaaS applications.
    - The Citrix SecurAccess client for private applications using TCP/UDP protocols.

Some of the key characteristics of a Citrix SecurAccess ZTNA session are:

- Each session is assigned a unique ID for tracking and analysis.
- A single session can include multiple app launches and provides a comprehensive view of the user activity within that specific session.
- For each app, the session tracks:
    - The security controls that apply to the app.
    - The policy display name and ID that triggered the security controls.
    - The condition that resulted in the policy being enforced.
- The session tracks all the internal domains that a user has visited in Citrix Enterprise Browser™ providing insights into the user navigation within the secure environment.

Web/SaaS app sessions

The session start and end for Web/SaaS apps is defined as follows:

- Start: Citrix Enterprise Browser is opened in the Citrix Workspace app and applications are accessed.
- End: A session ends in the following scenarios.
    - You close the Citrix Enterprise Browser.
    - After 30 minutes of inactivity, if no session activity is reported.

      The Citrix Enterprise Browser client sends a session activity to Monitor every 15 minutes to Monitor. If this session activity is not received for 30 minutes, which might occur due to reasons such as:
        - Network failure.
        - Internet connectivity issues.
        - Session is automatically closed after the 30-minute interval without session activity.

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

NOTE:

For apps launched through native browsers (agentless), the session ends after 120 minutes of inactivity.

TCP/UDP app sessions

The session start and end for TCP/UDP apps is defined as follows:

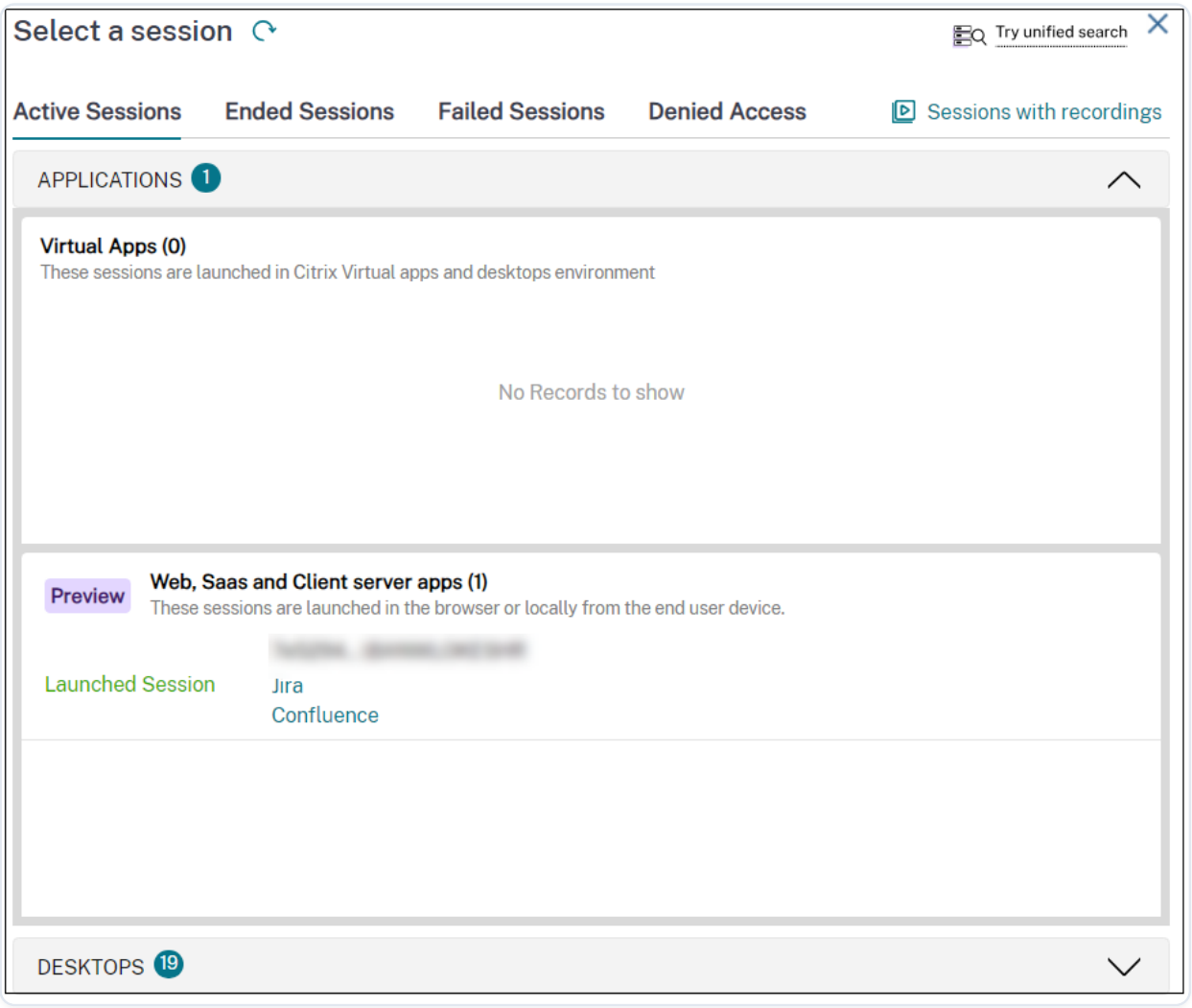
- Start: You log in to the Citrix SecurAccess™ client and access the apps.
- End: A session ends in the following scenarios.
  - You log out of the Citrix SecurAccess client.
  - After 30 minutes of inactivity, if no session activity is reported.

View user sessions

Perform the following steps to view a user session:

1. Search for a user to view the sessions.
   - The **Select a session** page displays all active sessions. If you do not find your session in the **Active Sessions** tab, check in the **Denied Access** tab.
   - The **Ended Sessions** and **Failed Sessions** tabs are not applicable to Citrix SecurAccess ZTNA.

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



2. In the **Active Sessions** tab, click the session ID to view the details of the session.

   The **Activity Manager** page appears.

3. Click one of the following tabs:

   - **Launched apps:** View all applications launched by the user and the results (allow or deny) of the access policy evaluation.

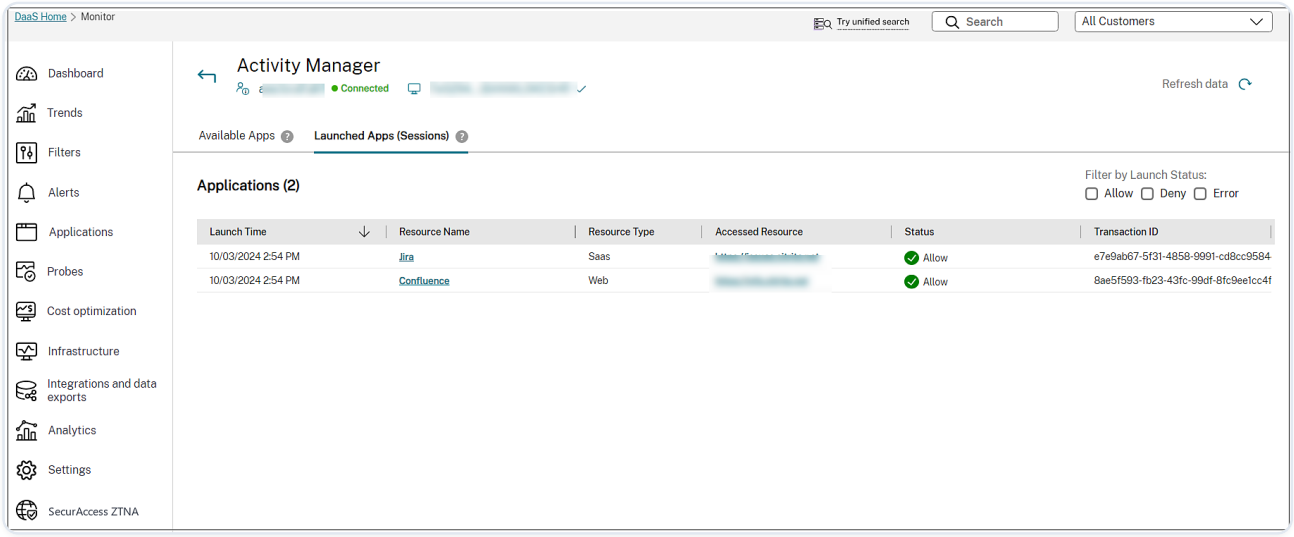
     If an application was accessed multiple times in the same session, only the latest launch details are captured.

   - **Available Apps:** View app enumeration details of all the applications that were launched by this user.

     - If multiple enumeration requests were sent by Citrix Workspace app for a user, only the latest enumeration details are captured.
     - For TCP/UDP apps (web and ZTNA), although there is no concept of app enumeration, all apps configured and associated with the user are listed in the **Available Apps** list.

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

- The **Available Apps** list does not contain external apps that are enumerated through the Citrix SecurAccess client as they are not tunneled by Citrix SecurAccess ZTNA.
- For the Citrix SecurAccess agent, the **Available Apps** list only displays only the internal web and TCP/UDP apps.



Application topology

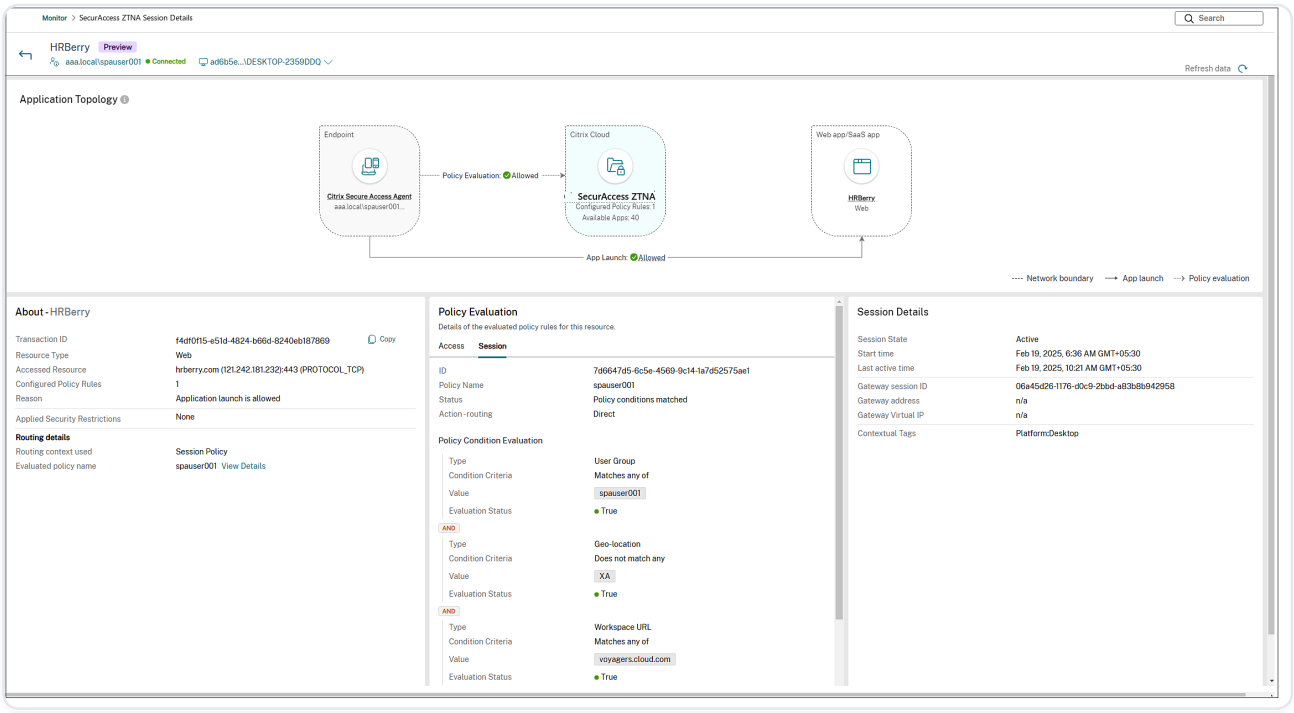
When you click an app from the **Launched Apps** or **Available Apps** tabs, the application topology page appears, displaying complete information about the app.

- **Session Topology:** Displays the app launch flow.
- **About:** Displays app-related information such as app type, number of policy rules, security restrictions, and accessed resources. The data that appears in the **Accessed Resources** section varies depending on the app type.
  - SaaS apps - URL or the app FQDN
  - TCP/UDP – IP address/FQDN, port, and protocol
  - Web app (launched via Citrix SecurAccess client) - FQDN, port, and protocol
  - Web app (launched via Citrix Workspace app) - URL
- **Policy evaluation:** Displays information related to the access policy, such as rules, actions, and conditions.
- **Session Details:** Displays information related to the session, including session start and end time, session state, and contextual tags associated with the policy.

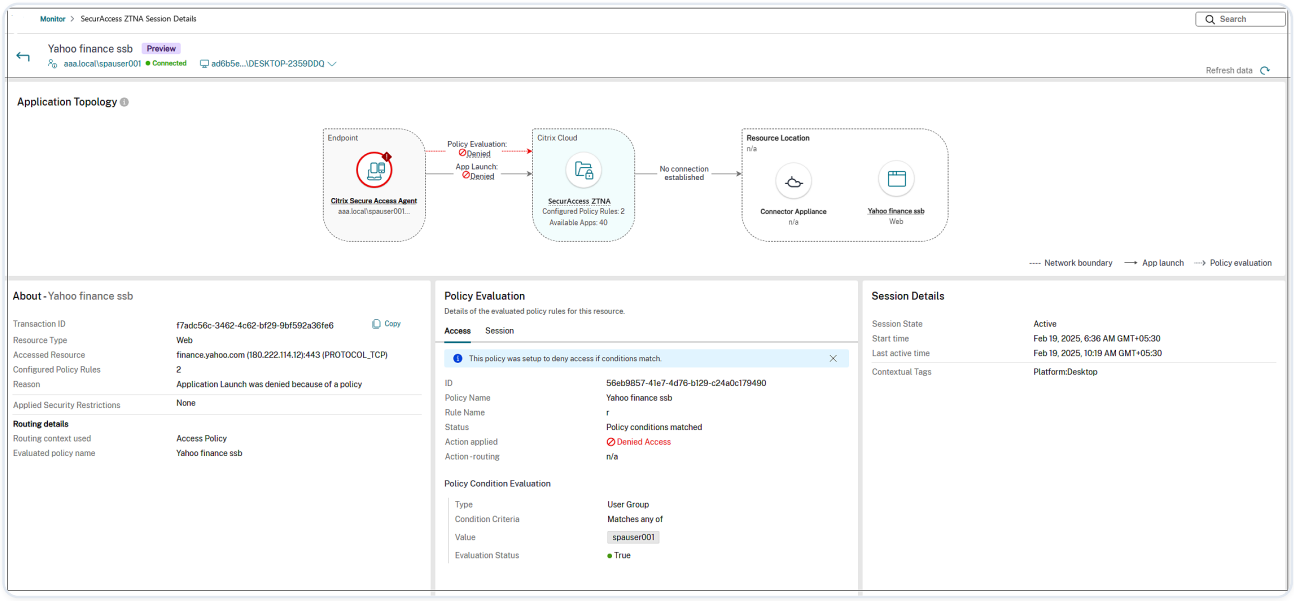
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Domains Visited** field is applicable only for the Web/SaaS apps and is updated only after 15 minutes, as the Citrix Enterprise Browser clients on macOS and Windows send session activity every 15 minutes.
- The **Session Details** column section remains empty for apps clicked from the **Available Apps** tab, as app enumeration is not associated with a session.

The following figure displays a sample topology diagram for a successfully launched app.



The following figure displays a sample topology diagram for an access denied app.



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

Triage and troubleshoot

This topic outlines the essential considerations and procedures for effectively troubleshooting and triaging issues related to Citrix SecurAccess™ ZTNA. Admins can use this document as a guide for identifying, diagnosing, and resolving problems, ensuring seamless and secure access for users.

User/client issues in Citrix SecurAccess mode

The following sections provide more information about user/client issues in Citrix SecurAccess mode.

User unable to log in

Things to check:

- Check if the VPN virtual server and authentication virtual server is UP.

```
> show vpn vserver _spa_cep_csa_vpn_vs_10.8.0.35
        _spa_cep_csa_vpn_vs_10.8.0.35 (10.8.0.35:443) - SSL     Type: CONTENT
        State: UP


 > show authentication vserver authvs
         authvs (0.0.0.0:0) - SSL        IPSet: ???      Type: CONTENT
         State: UP  ARP:DISABLED
```

- Check if the Citrix SecurAccess ZTNA profile URL status is UP.

```
 > show vpn securePrivateAccessProfile _spa_cep_csa_profile
 1)      Name: _spa_cep_csa_profile
                 URL: https://stg4spalb.spagwcep.corp  [Status: UP]
```

- Ensure that the apps and access policies are correctly configured for the user in the Citrix SecurAccess ZTNA admin console. See Apps configuration and management and Configure access policies for the applications.
- Check the load balancer virtual server status to ensure that all connector servers are added and are UP.

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

- To troubleshoot any nFactor authentication issues, see Troubleshoot authentication, authorization, and auditing issues.

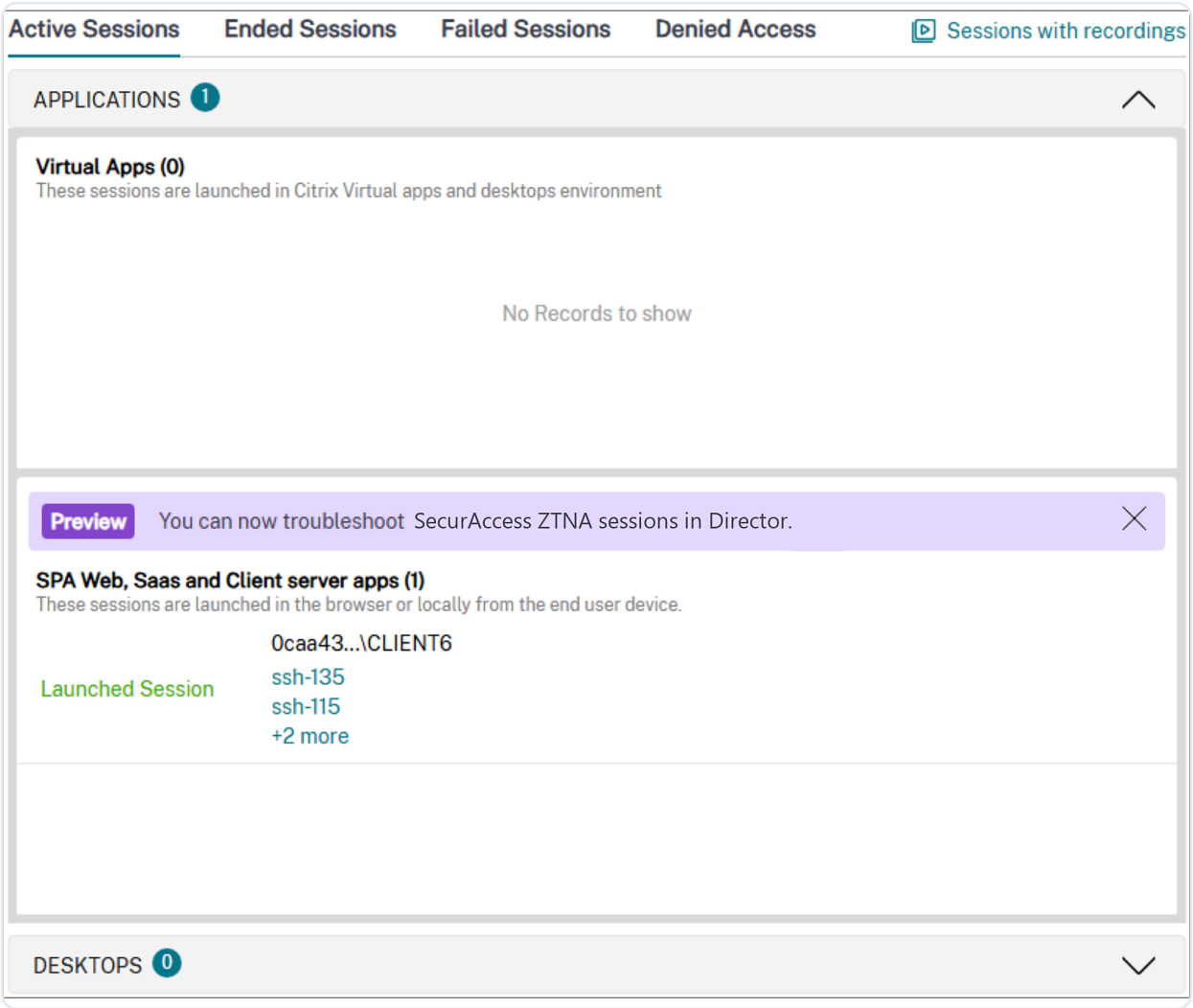
After confirming what was mentioned earlier, do the following:

1. Enable debug level logging and collect a support bundle from NetScaler.
2. Enable verbose logging on the CSA client and collect client logs.
3. Contact Citrix Support and provide the collected diagnostics.

User unable to launch an app

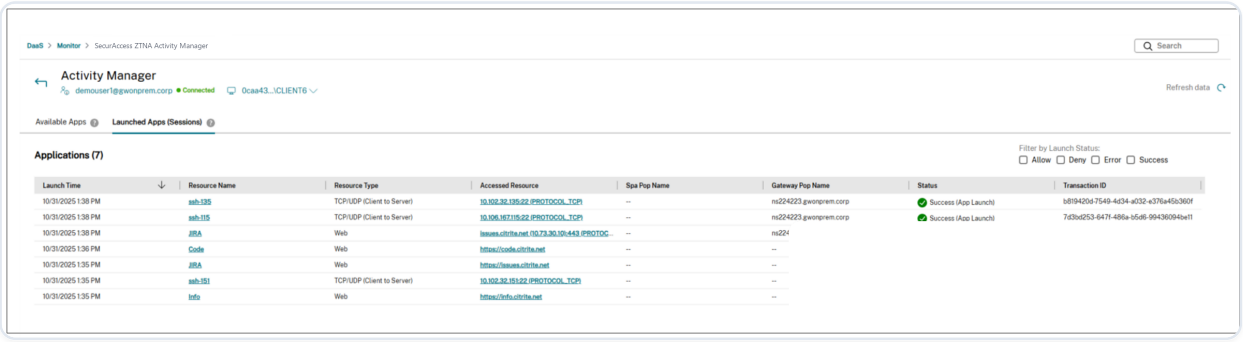
Things to check:

- In Citrix Monitor, search for the user UPN and verify that an active Citrix SecurAccess ZTNA session exists.



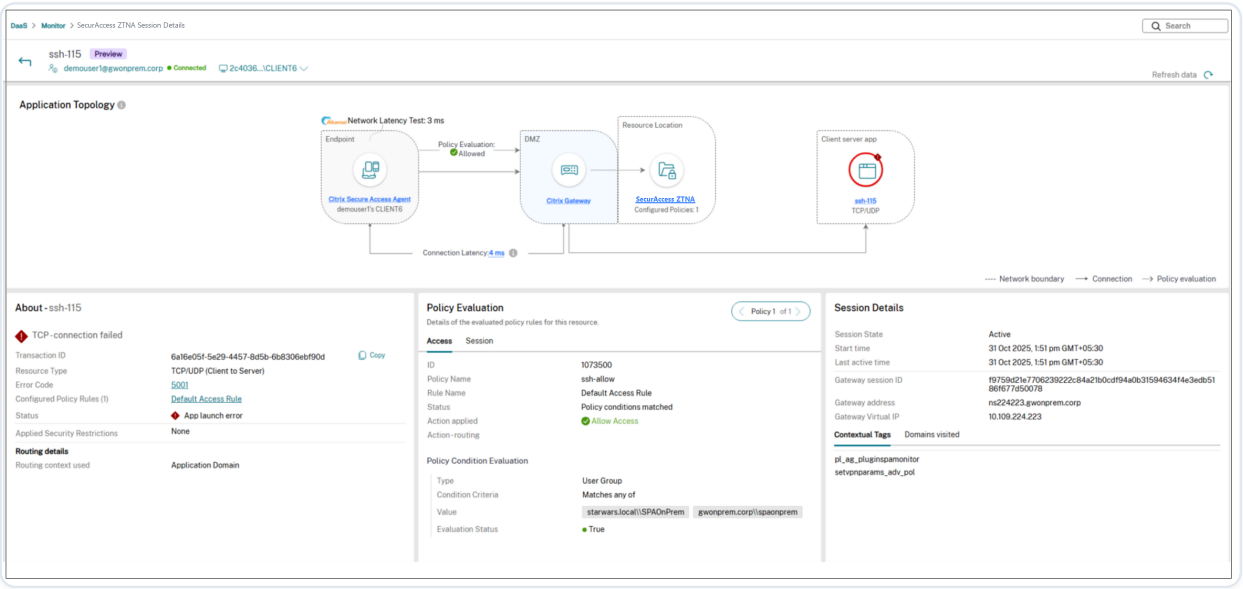
  - The launched app must appear under **Available apps**.
  - An **App Launch Allow** event for the app must be visible under **Launched apps**.

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



- If not present, check that the app and access policies are correctly configured for the user in the Citrix SecurAccess ZTNA admin console.

- In Citrix Monitor, look for any app launch error event for the app under **Launched apps**.



- Common errors: DNS resolution failure/TCP connection failure.
- From the NetScaler CLI, verify connectivity to the app from the appropriate SNIP.

Steps to collect a NetScaler support bundle with debug-level logging

1. Set debug-level syslog from the CLI.

   ```
   set syslogparams loglevel ALL DEBUG
   ```

2. Enable Citrix SecurAccess ZTNA specific verbose logging from Shell.

   ```
   nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=1
   ```

3. Collect the support bundle (and optional traces)
4. Use your standard method to collect the NetScaler support bundle.

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

5. Optionally capture additional traces if requested by support.

IMPORTANT:

Revert verbose logging after collecting the bundle. Leaving verbose logging enabled can generate excessive logs and impact performance. Always revert verbose logging once the collection is complete.

Revert verbose logging

1. Restore syslog level from the CLI.

   ```
   set syslogparams loglevel ALL
   ```

2. Disable Citrix SecurAccess ZTNA specific verbose logging from Shell.

   ```
   nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=0
   ```

Additional References:

- How to generate a technical support bundle for a NetScaler® instance Logs
- How to record a packet trace on NetScaler

Tools that help to troubleshoot

- Configuration reports
- Component Analyzer
- Policy modeling

Collect client logs

The following sections provide more information about collecting client logs.

Chrome Enterprise Premium logs

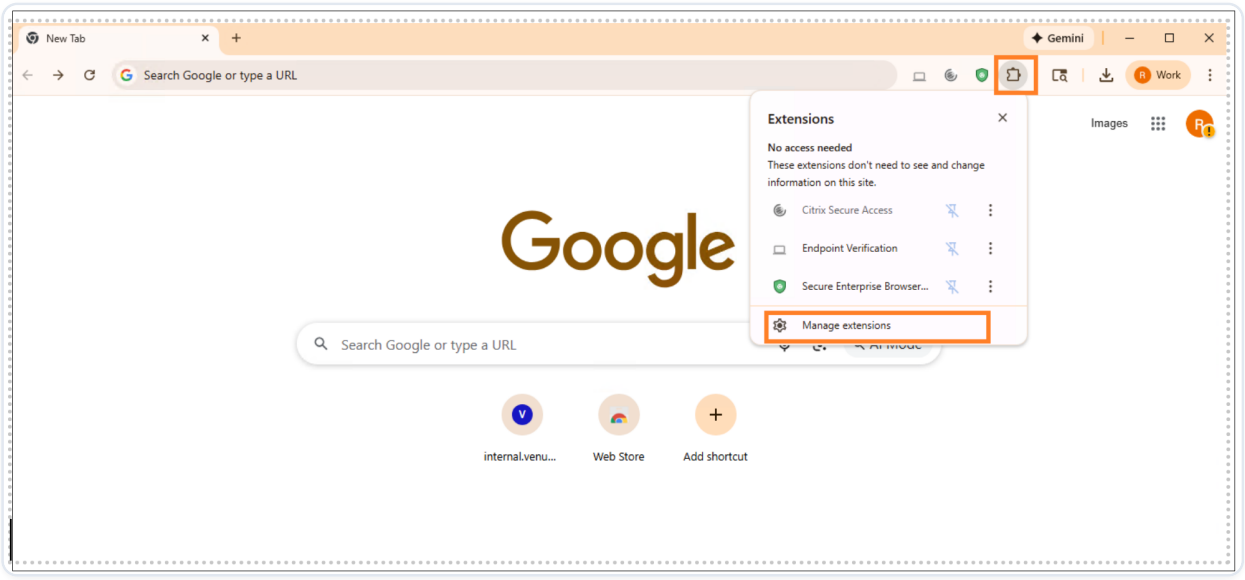
If you experience issues on the client side with Chrome Enterprise Premium, collect the extension logs for both Secure Enterprise Browser and Citrix SecurAccess™.

Steps to capture logs for the Secure Enterprise Browser extension

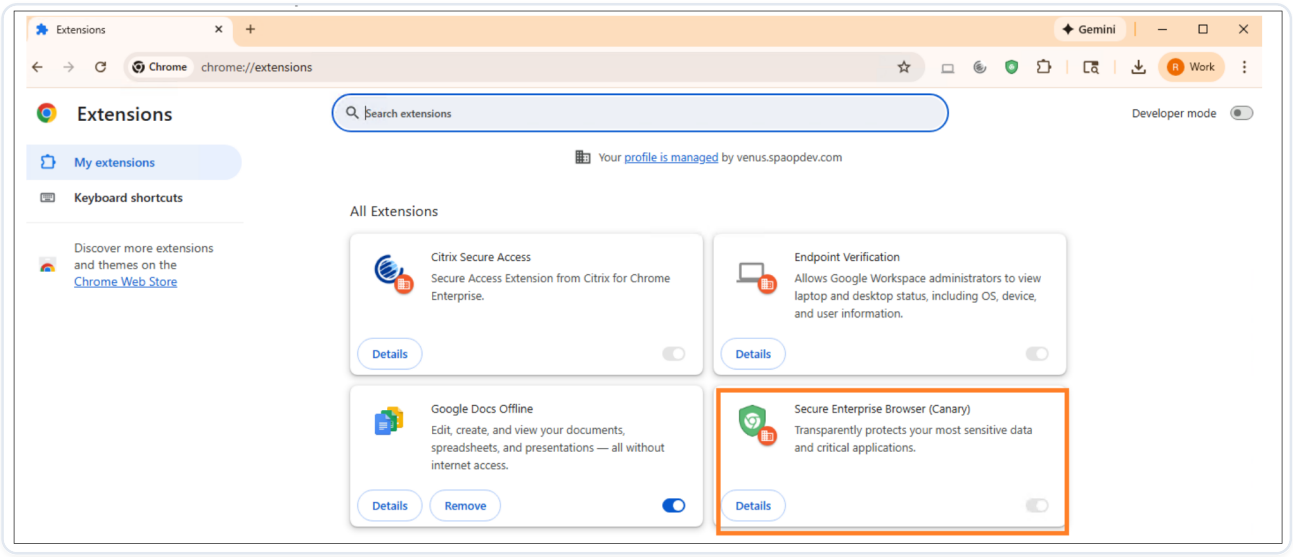
1. Open the Chrome browser.

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

2. Switch to your managed Chrome profile.
3. Click the **Extensions** icon and select **Manage extensions**.

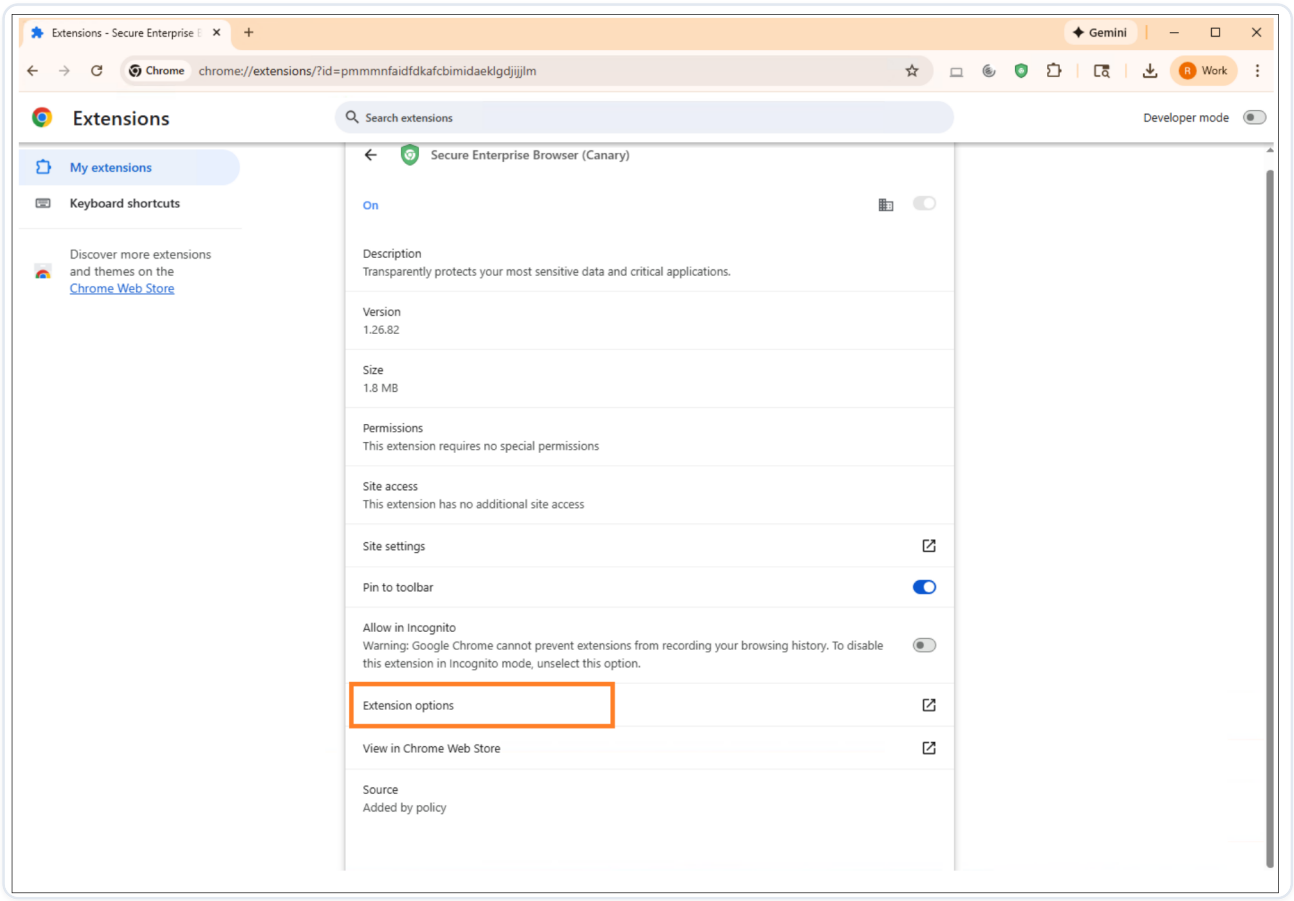


4. Under Secure Enterprise Browser, click **Details**.

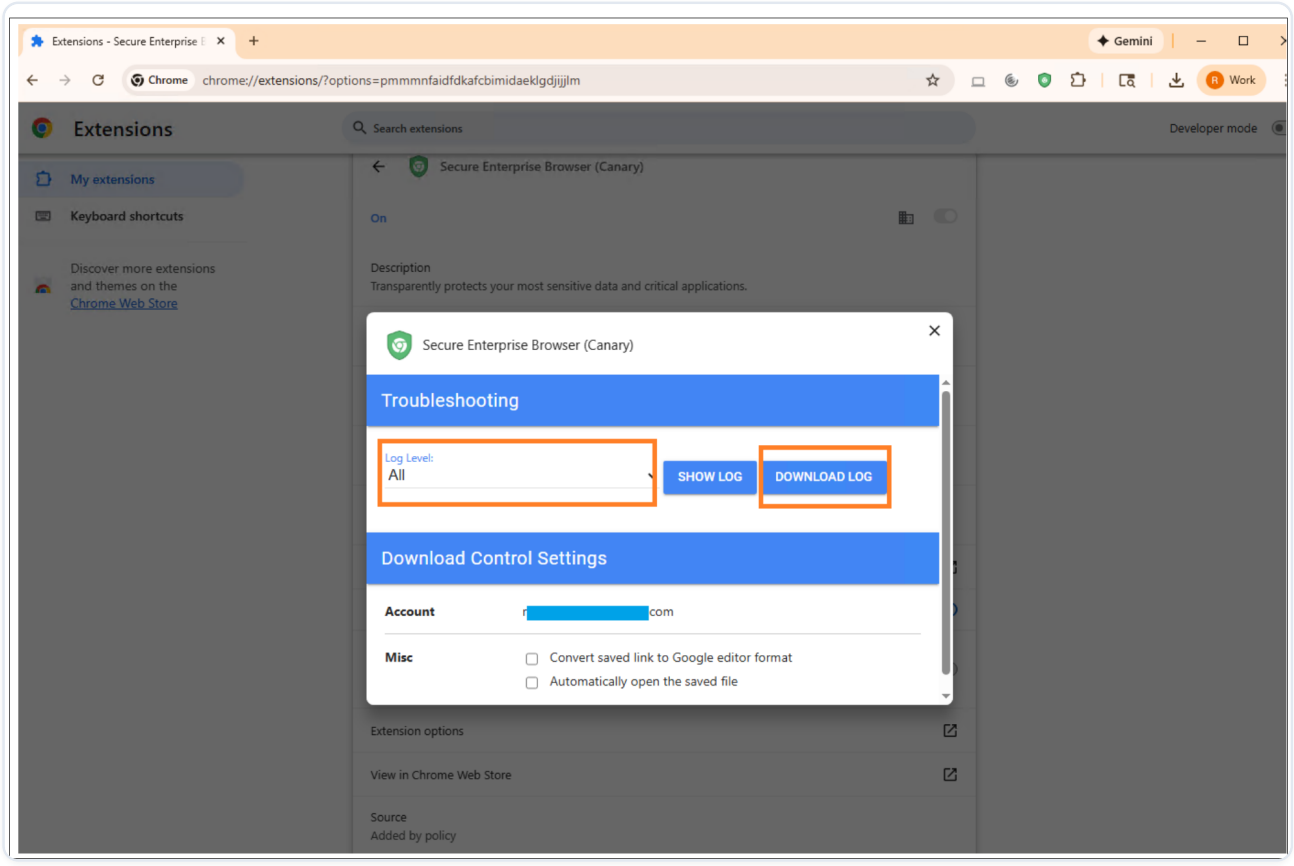


1. Select **Extension options**.

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



1. Click **DOWNLOAD LOG**.

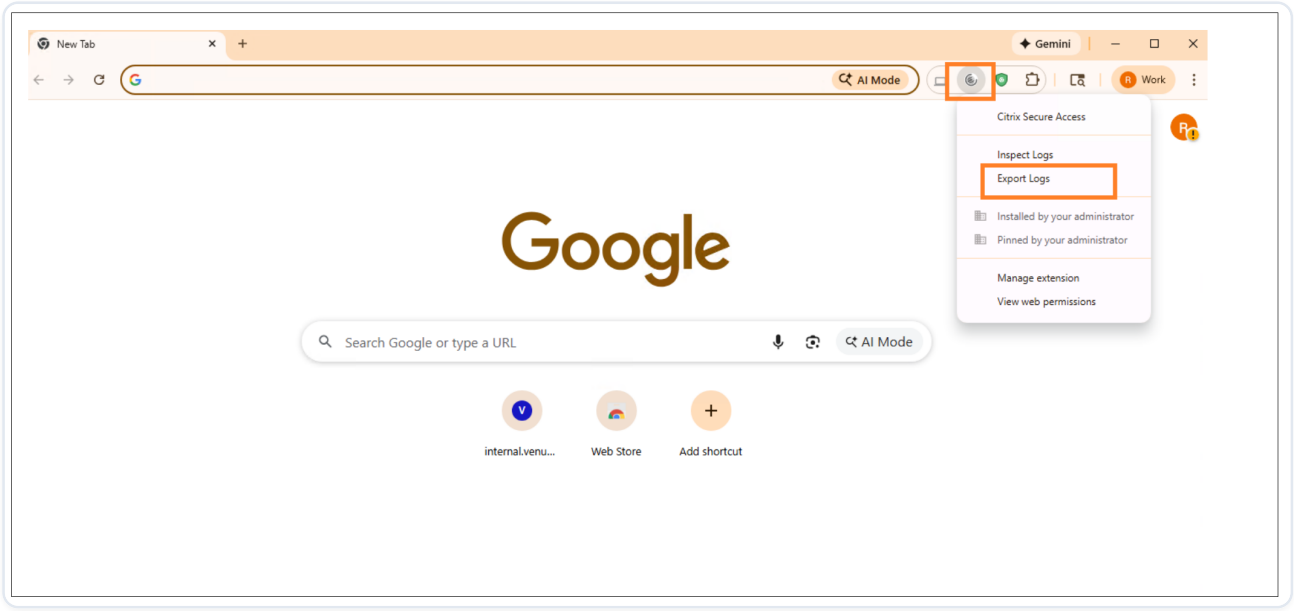


1. Save the downloaded log files to your computer.

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

Steps to capture logs for Citrix SecurAccess Extension

1. Open the Chrome browser.
2. Switch to your managed Chrome profile.
3. Click the **Citrix SecurAccess extension** icon next to the address bar.
4. Select **Export Logs**.



1. Save the exported log files to your computer.

Real-time session troubleshooting using Monitor

Administrators can monitor and troubleshoot Citrix SecurAccess™ ZTNA sessions in real-time using the Monitor console.

For related information, see the following topics:

- For information on integrating Citrix SecurAccess ZTNA with Monitor, see Integration with DaaS monitor.
- You can search for Citrix SecurAccess ZTNA user sessions in Monitor to quickly locate specific sessions for troubleshooting and reporting purposes. For details, see View a Citrix SecurAccess ZTNA session by user.
- For more information on Monitor, see DaaS Monitor.

The following error codes are captured for Citrix SecurAccess ZTNA hybrid deployments:

- Session codes
- App enumeration message codes

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

- App launch message codes
- App launch error codes

Session codes

CODE	STATUS	DESCRIPTION
2101	Failure	Session failure
2102	active/inactive/failure	Session is active or terminated or at least one app launch in the session failed
2000	Active	The session is active
2001	Inactive	Session is terminiated/ inactive

App enumeration message codes

CODE	STATUS	DESCRIPTION
1000	Success	Enumeration was successful. At least one app was enumerated
1001	Success	No applications were enumerated because they were all denied by policies
1002	Success	No applications were enumerated because no policies matched
1003	Success	No applications were enumerated because some were denied and for others, no policies matched

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

CODE	STATUS	DESCRIPTION
1004	Success	No applications were enumerated because no policies to evaluate
1101	failure	An internal error occurred during the enumeration
1102	failure	Some applications were enumerated but at least one app evaluation failed
1103	failure	No applications were enumerated and at least one app evaluation failed
3000	Allow	Application enumeration is allowed
3001	Deny	Application enumeration is denied by policy
3002	Deny	Application was not enumerated because no policies matched
3003	Unknown	Application enumeration status is unknown
3004	Application launch from CEB	Application launch attempt from Citrix Enterprise Browser™
3101	Failure	Application enumeration - An internal error occurred (currently unused)
3102	Failure	Application was not enumerated because there was an exception during policy evaluation

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

CODE	STATUS	DESCRIPTION
3103	Failure	Application enumeration status is null - An internal error occurred during policy evaluation
3104	Allow/deny/failure	Error retrieving policy details for the app

App launch message codes

CODE	STATUS	DESCRIPTION
4000	Allow	Application Launch is allowed
4001	Deny	Application launch was denied because of a policy
4002	Deny	Application launch was denied because no policy matched
4101	Failure	Application launch error - An internal error occurred during application launch
4102	Failure	Application launch error (internal)
4103	Allow/deny/failure	Error retrieving policy details for the app
4104	Failure	Application Launch Error - No application configuration found

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

App launch error codes

CODE	DESCRIPTION	RESOLUTION/WORKAROUD
5001	TCP - connection failed	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway). ^
5003	TCP - probe failed	
5002	TCP - proxy server down	Ensure that the proxy host is UP.
5004	TCP - memory allocation in gateway failed	Enable debug level logging and collect support bundle from NetScaler.
5005	TCP - server down	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway) and check if the server is DOWN.
5006	TCP - proxy connection failed	Ensure that the proxy host is UP and accepting connections.
5007	TCP - proxy probe failed	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway). Enable debug level logging and collect support bundle from NetScaler.
5008	SPA - server down	Verify that the Citrix SecurAccess ZTNA site URL is UP. (Use the `show vpn securePrivateAccessProfile` CLI command on NetScaler CLI to check the URL status).

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

CODE	DESCRIPTION	RESOLUTION/WORKAROUD
5009	SPA - callout request error	Verify that the Citrix SecurAccess ZTNA site URL is UP. Enable debug level logging and collect support bundle from NetScaler. ^
5010	SPA - callout response error	
5011	TCP - session expired	This indicates that the app was accessed when the user session was no longer active. Start a new active user session.
5013	TCP - gateway internal error	Enable debug level logging and collect support bundle from NetScaler.
5014	TCP - DNS server down	Ensure that the DNS server is UP.
5015	TCP - gateway DNS internal error	Ensure that the DNS Server is UP. Enable debug level logging and collect support bundle from NetScaler.
5016	Destination server connection failed	Verify network reachability to the destination (ping -S `<SNIP>` from NetScaler Gateway).
5017	Destination server DNS resolution failed	Make sure the hostname your application uses is resolved by the intended DNS servers (internal vs public).
5018	Gateway internal error	Enable debug level logging and collect support bundle from NetScaler.
0x1300000C	DNS resolution failed for application domain	Ensure that the host name your application uses is

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

CODE	DESCRIPTION	RESOLUTION/WORKAROUD
		resolved by the intended DNS servers (internal vs public).

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

End user experience

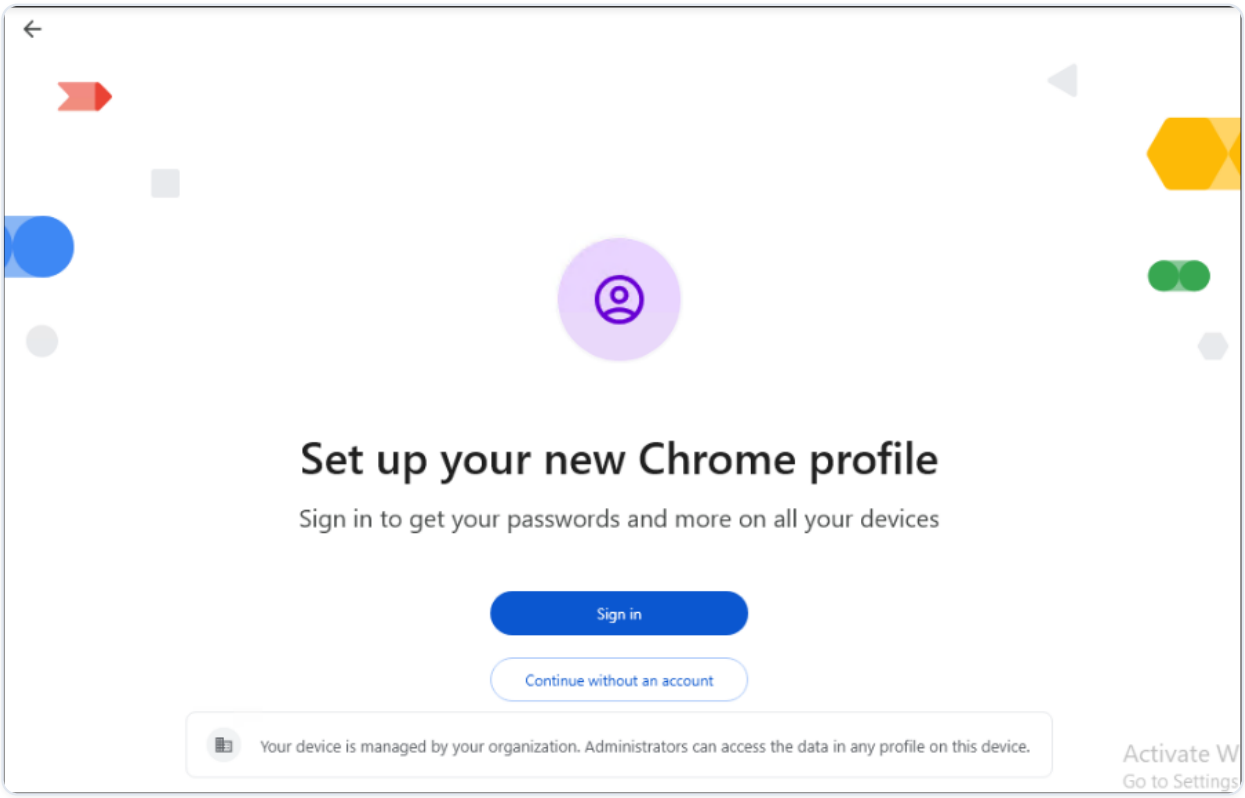
The following sections provide more information about the end user experience.

Accessing web and SaaS applications with Chrome Enterprise Premium

You can access published internal web applications and external SaaS applications using Chrome Enterprise Premium in four different ways. Choose the option that applies to your environment.

Option 1: Create a managed Chrome profile and access apps directly (recommended)

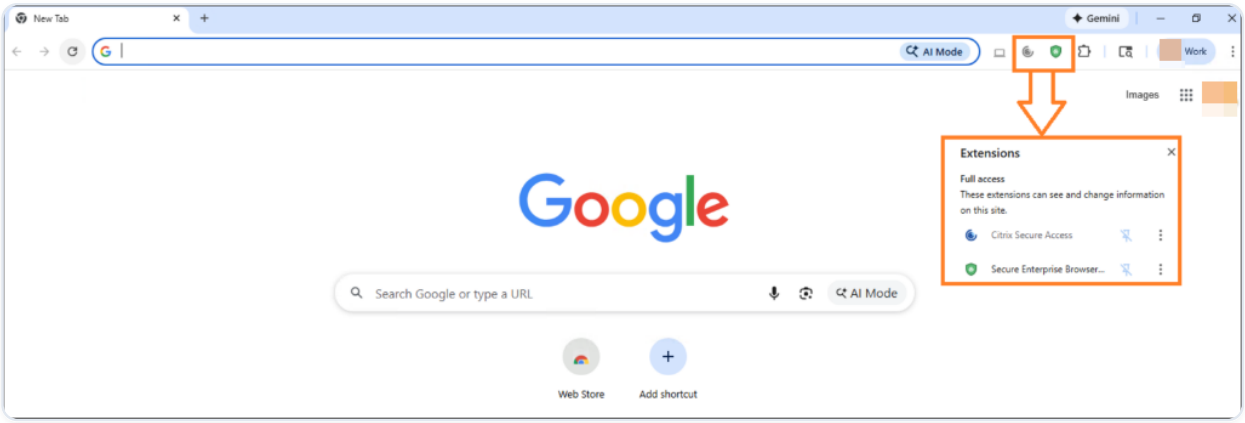
- Open the Chrome browser.
- Add a new Chrome profile using your company's credentials (that is, create a managed Chrome profile).



- After the profile is created, two extensions are automatically installed:

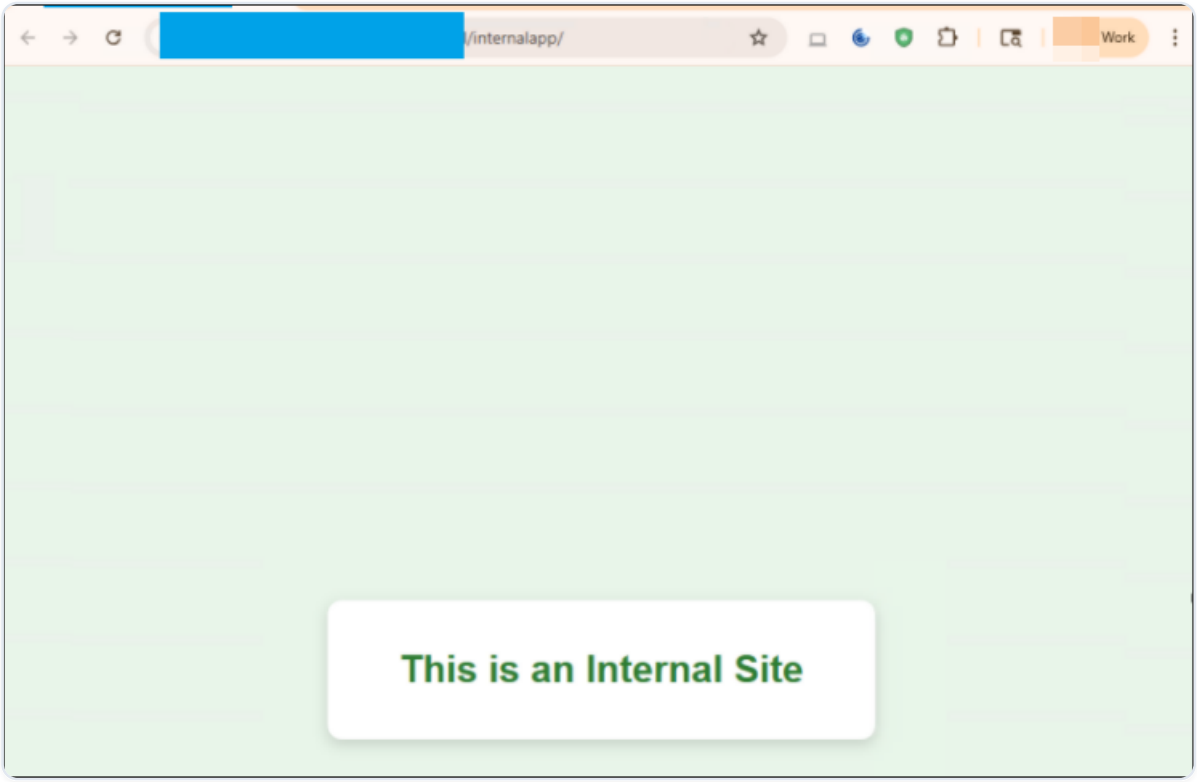
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix SecurAccess™
- Secure Enterprise Browser



- Access internal and external applications by entering the URL in the address bar or by navigating to the published sites.
- Behavior when the URL is entered manually:
  - **Internal web app (allowed):**

    The request is securely tunneled through Citrix SecurAccess™ ZTNA and the site loads.



  - **Internal web app (denied):**

    Citrix SecurAccess ZTNA blocks the request, and an **Access Restricted** page appears.

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



- **External SaaS app (allowed):**

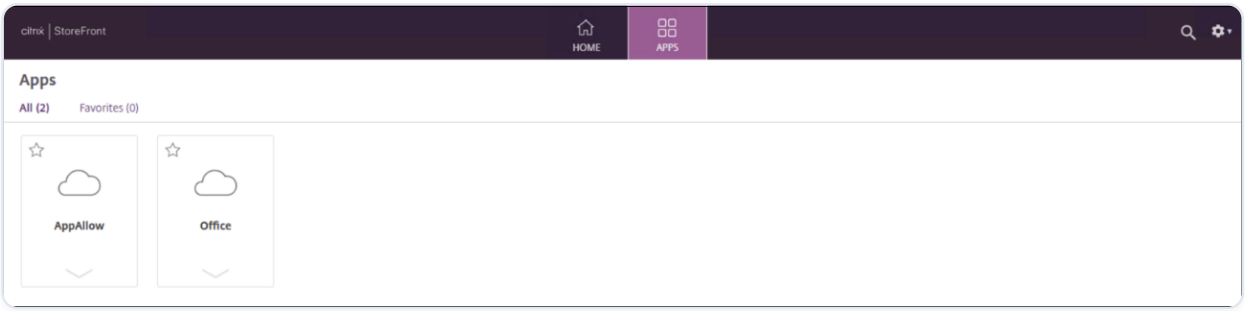
  The request is allowed directly without tunneling.

- **External SaaS app (denied):**

  Citrix SecurAccess ZTNA blocks the request, and an **Access Restricted** page appears.

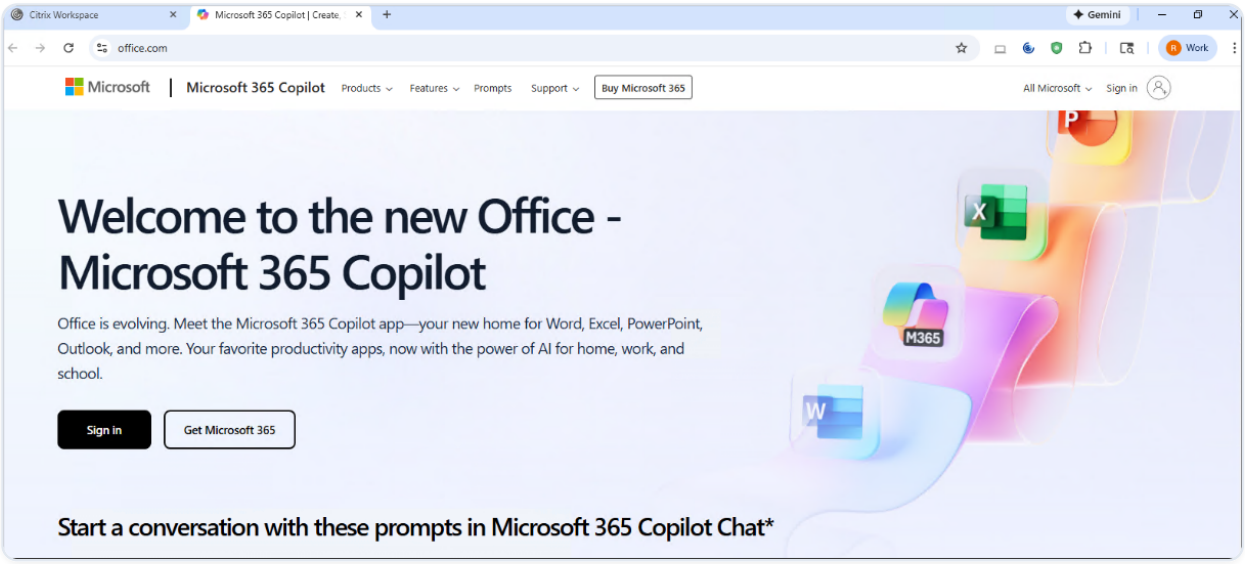
Option 2: Access store URL in existing Managed Chrome profile

- Ensure the managed Chrome profile with company credentials already exists.
- Launch Chrome with the correct company-managed profile.
- Open the store URL in a web browser.
- Log in to the store.
- Go to the **Apps** tab and select the web/saas app published by your company's admin.



- The web/saas app launches seamlessly in a new tab within the same managed Chrome profile.

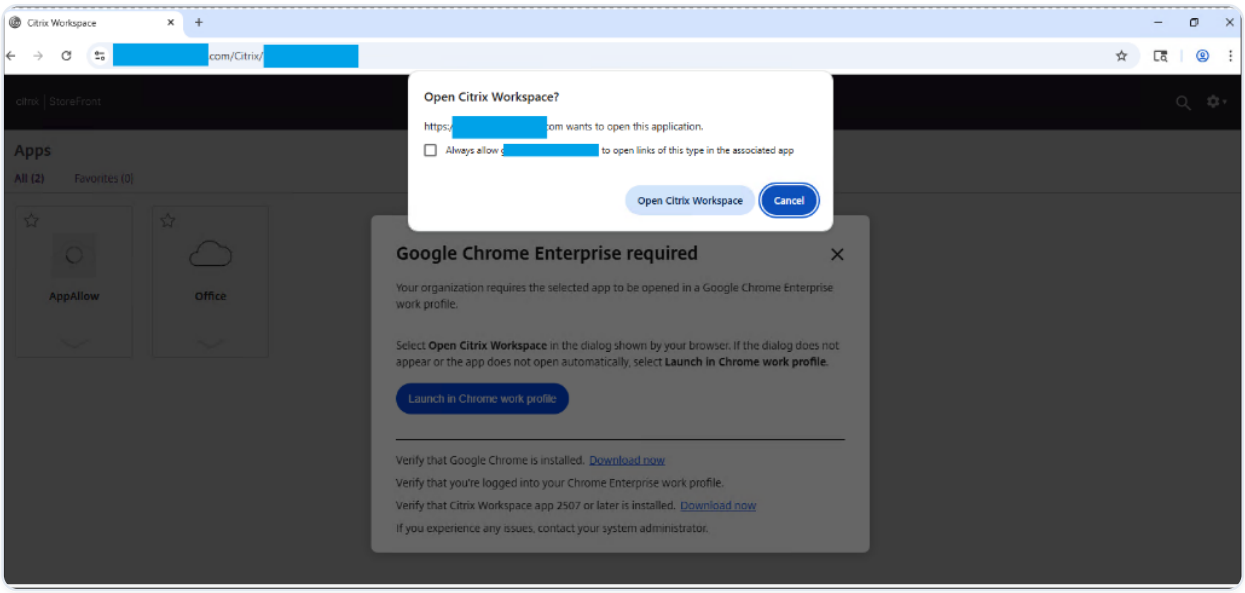
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Allow and deny logic remains the same as Option 1.

Option 3: Access store URL from a non-managed Chrome profile or a non-Chrome browser (Edge, Firefox)

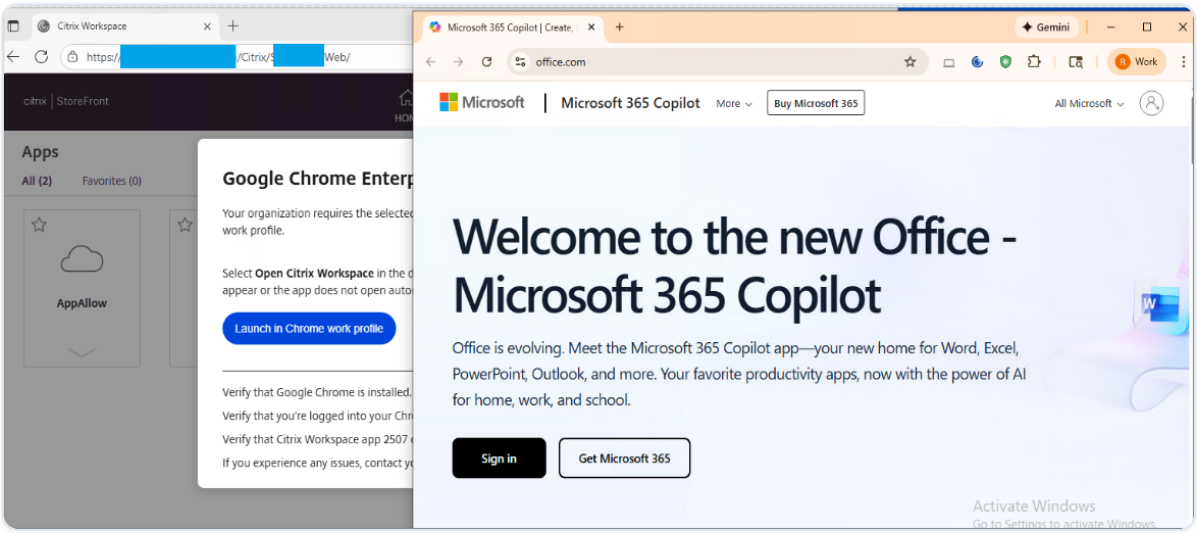
- Launch Edge, Firefox, or a non-managed Chrome profile.
- Open the store URL in the web browser
- Log in to the store.
- Go to the **Apps** tab and select the published web app.
- A popup appears with a dialog showing the button **Open Citrix Workspace**. Click this button to proceed.



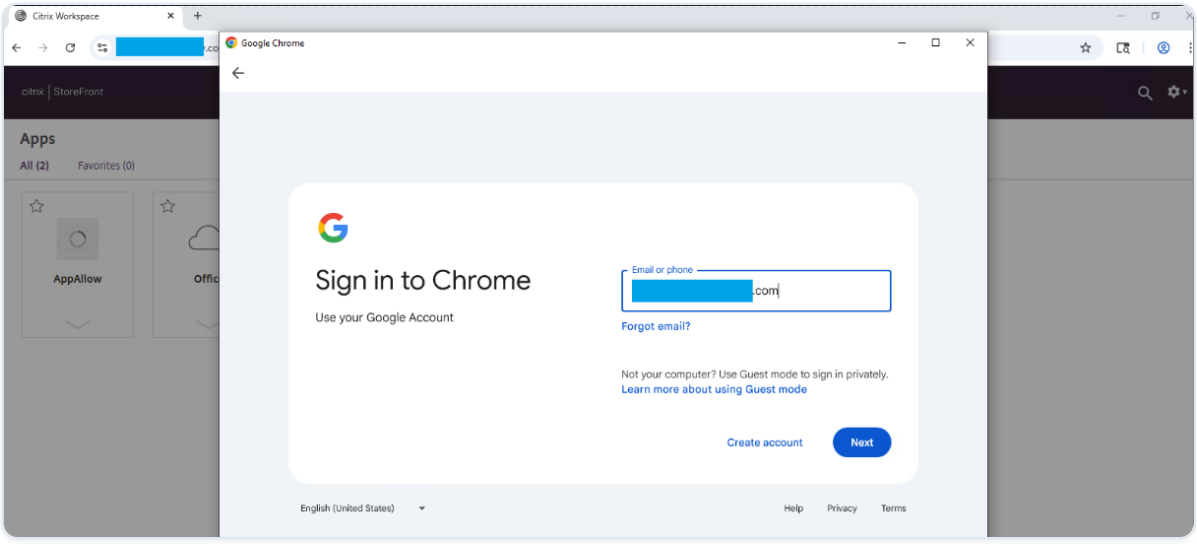
- After clicking the button, one of the following happens:

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

- **Managed Chrome profile already exists:** The app launches directly in the managed profile.



- **Managed Chrome profile does not exist:** You are prompted to create a managed Chrome profile before the app launches.

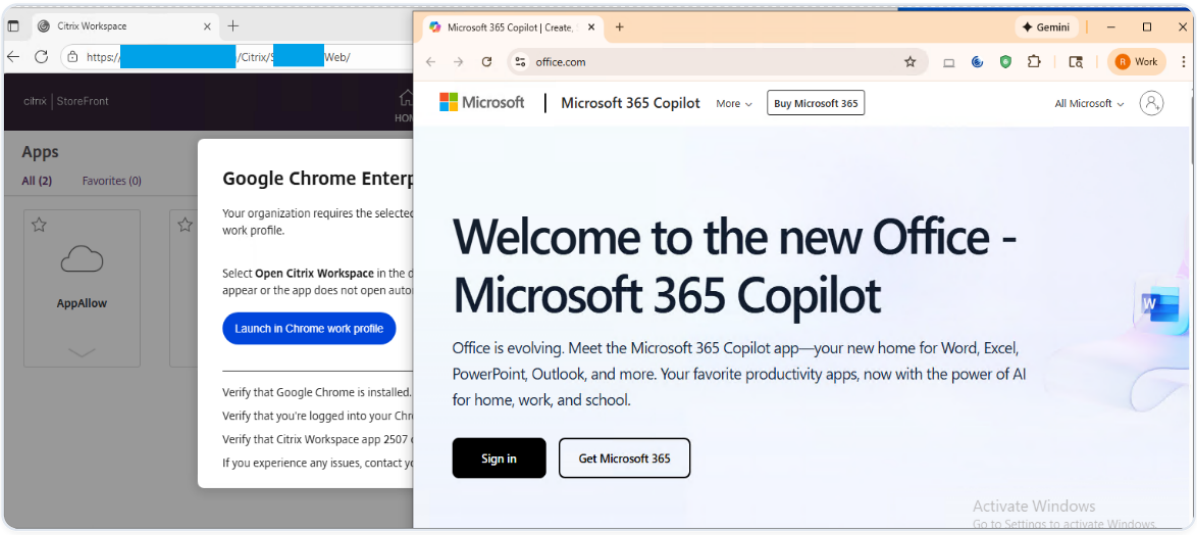


- Allow and deny logic remains the same as Option 1.

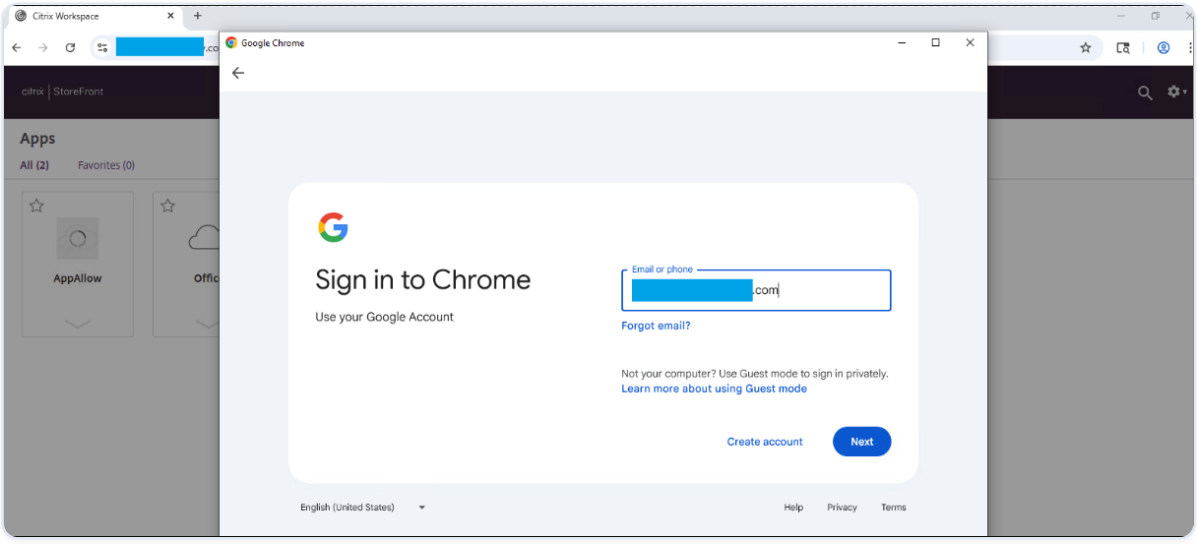
Option 4: Access apps through the Citrix Workspace app

- Open the StoreFront store using the Citrix Workspace app.
- Log in to the store.
- Go to the **Apps** tab and select the published web app.
- The Workspace app launches Chrome automatically. Based on your setup:
  - **Managed Chrome profile exists:** The app opens directly in the managed profile.

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



- **Managed Chrome profile does not exist:** You are prompted to create one before the app opens.



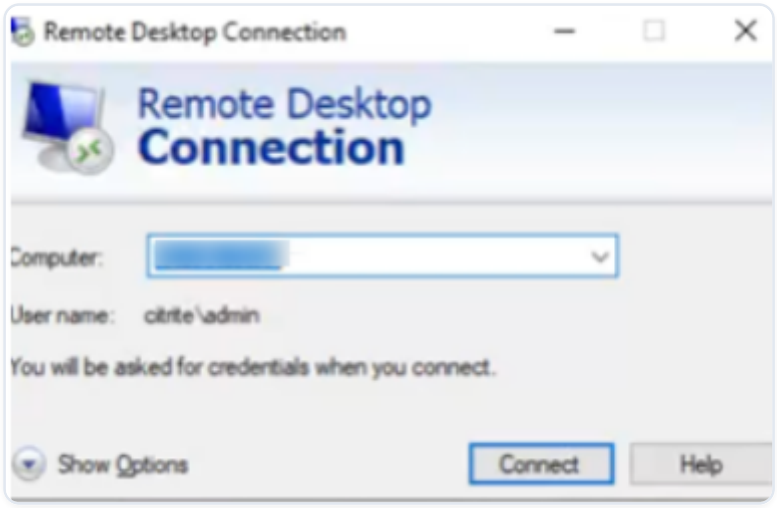
- Allow and deny logic remains the same as Option 1.

Accessing client/server (TCP/UDP) applications

If RDP is configured, end users must perform the following steps to access the TCP/UDP app:

1. Log in to the Citrix SecurAccess client.
2. After the secure access session is established, start a remote desktop connection.

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



a. Press the Windows key, type **Remote Desktop Connection**, and press **Enter**.
b. Enter the IP address or host name of the computer that you are trying to connect to.
c. Click **Connect**. You might be prompted to enter the credentials.
d. Enter the user name and password for the remote computer and then click **OK**.

A remote desktop connection is established now and the end user can interact with the remote computer.

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

index

- Integration with DaaS monitor
- Contextual tags
- Citrix SecurAccess™ ZTNA

Integration with DaaS monitor

Citrix SecurAccess™ ZTNA is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Citrix SecurAccess ZTNA dashboard.

Service entitlements

To use the DaaS Monitor feature with Citrix SecurAccess ZTNA, you must have both Citrix SecurAccess ZTNA and DaaS entitlements.

Supported clients

- Citrix Workspace™ app - 2409 and later
- Citrix SecurAccess for Windows - 24.8.1.19 and later
- Citrix SecurAccess for macOS - 24.10.1 and later

How to access Monitor

You can access Monitor from the Citrix SecurAccess ZTNA dashboard (**Go to Monitor**) or from the Citrix DaaS™ service tile.

In the **Monitor** page, search for the user to view the sessions.

Session definitions

A Citrix SecurAccess ZTNA session offers a comprehensive summary of an end-user’s session lifecycle, application activity, and user experience on a specific device. A session serves as a unified record for troubleshooting and analysis by providing visibility into the following aspects:

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

- Detailed insights into how applications are accessed, including launch hops, network topology, connections, and routing details. These details are crucial for resolving issues related to access policies.
- Tracks all session activity from:
  - Browsers accessing web or SaaS applications.
  - The Citrix SecurAccess client for private applications using TCP/UDP protocols.

Some of the key characteristics of a Citrix SecurAccess ZTNA session are:

- Each session is assigned a unique ID for tracking and analysis.
- A single session can include multiple app launches and provides a comprehensive view of the user activity within that specific session.
- For each app, the session tracks:
  - The security controls that apply to the app.
  - The policy display name and ID that triggered the security controls.
  - The condition that resulted in the policy being enforced.
- The session tracks all the internal domains that a user has visited in Citrix Enterprise Browser™ providing insights into the user navigation within the secure environment.

Web/SaaS app sessions

The session start and end for Web/SaaS apps is defined as follows:

- Start: Citrix Enterprise Browser is opened in the Citrix Workspace app and applications are accessed.
- End: A session ends in the following scenarios.
  - You close the Citrix Enterprise Browser.
  - After 30 minutes of inactivity, if no session activity is reported.

    The Citrix Enterprise Browser client sends a session activity to Monitor every 15 minutes to Monitor. If this session activity is not received for 30 minutes, which might occur due to reasons such as:
    - Network failure.
    - Internet connectivity issues.
    - Session is automatically closed after the 30-minute interval without session activity.

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

NOTE:

For apps launched through native browsers (agentless), the session ends after 120 minutes of inactivity.

TCP/UDP app sessions

The session start and end for TCP/UDP apps is defined as follows:

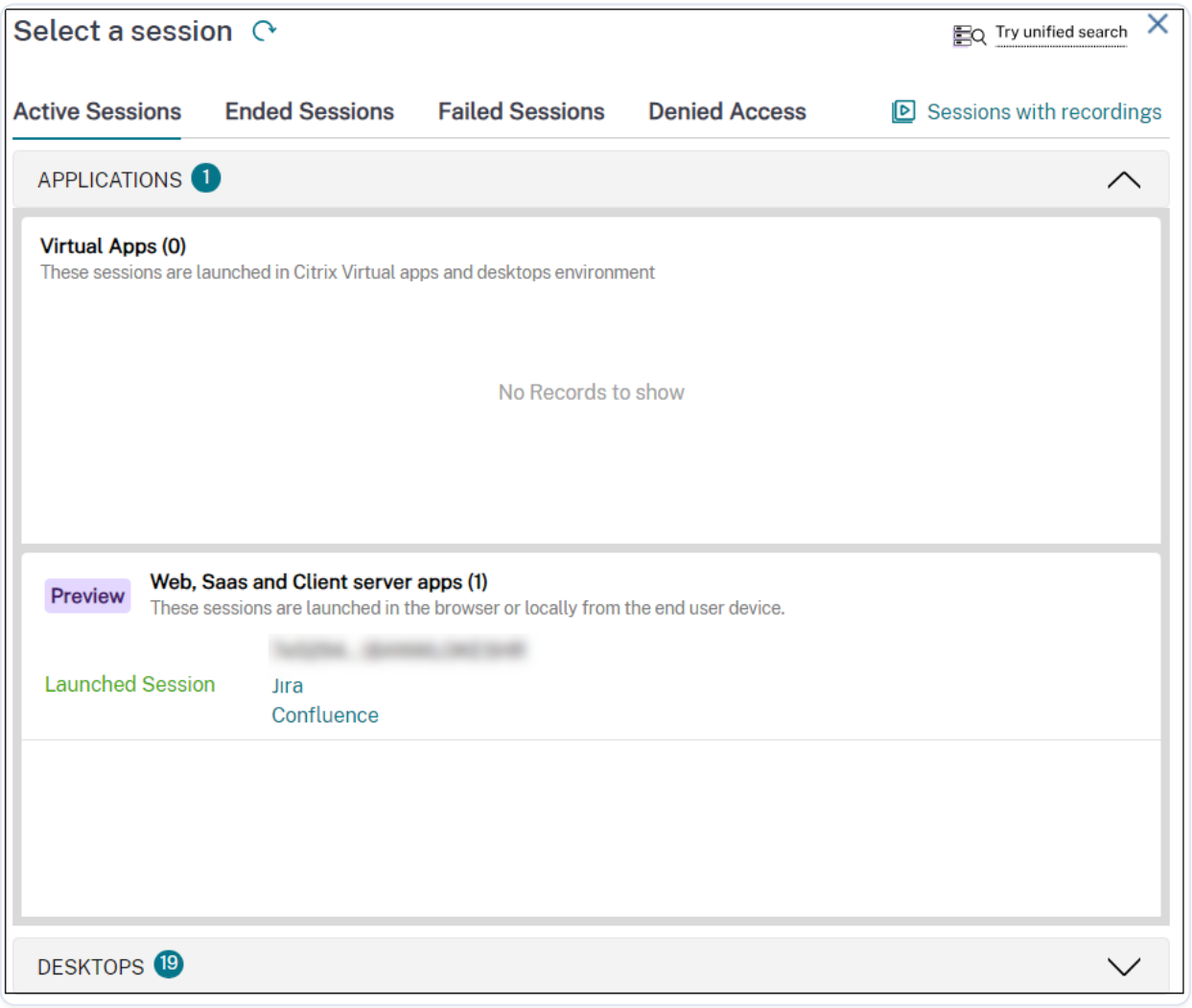
- Start: You log in to the Citrix SecurAccess™ client and access the apps.
- End: A session ends in the following scenarios.
  - You log out of the Citrix SecurAccess client.
  - After 30 minutes of inactivity, if no session activity is reported.

View user sessions

Perform the following steps to view a user session:

1. Search for a user to view the sessions.
   - The **Select a session** page displays all active sessions. If you do not find your session in the **Active Sessions** tab, check in the **Denied Access** tab.
   - The **Ended Sessions** and **Failed Sessions** tabs are not applicable to Citrix SecurAccess ZTNA.

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



2. In the **Active Sessions** tab, click the session ID to view the details of the session.

   The **Activity Manager** page appears.

3. Click one of the following tabs:

   - **Launched apps:** View all applications launched by the user and the results (allow or deny) of the access policy evaluation.

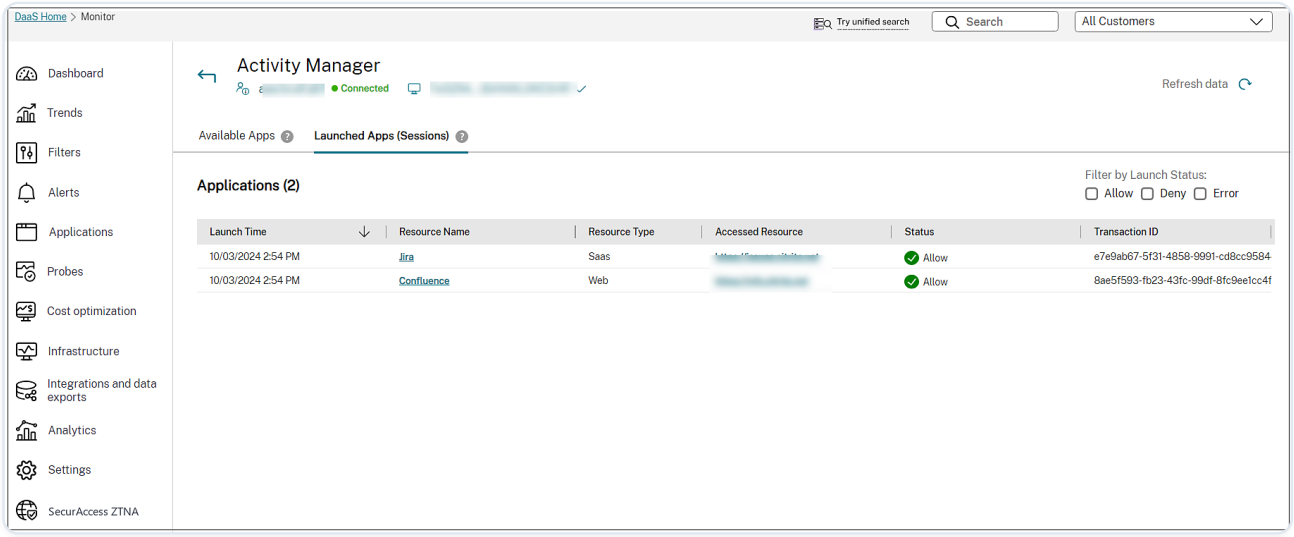
     If an application was accessed multiple times in the same session, only the latest launch details are captured.

   - **Available Apps:** View app enumeration details of all the applications that were launched by this user.

     - If multiple enumeration requests were sent by Citrix Workspace app for a user, only the latest enumeration details are captured.
     - For TCP/UDP apps (web and ZTNA), although there is no concept of app enumeration, all apps configured and associated with the user are listed in the **Available Apps** list.

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

- The **Available Apps** list does not contain external apps that are enumerated through the Citrix SecurAccess client as they are not tunneled by Citrix SecurAccess ZTNA.
- For the Citrix SecurAccess agent, the **Available Apps** list only displays only the internal web and TCP/UDP apps.



Application topology

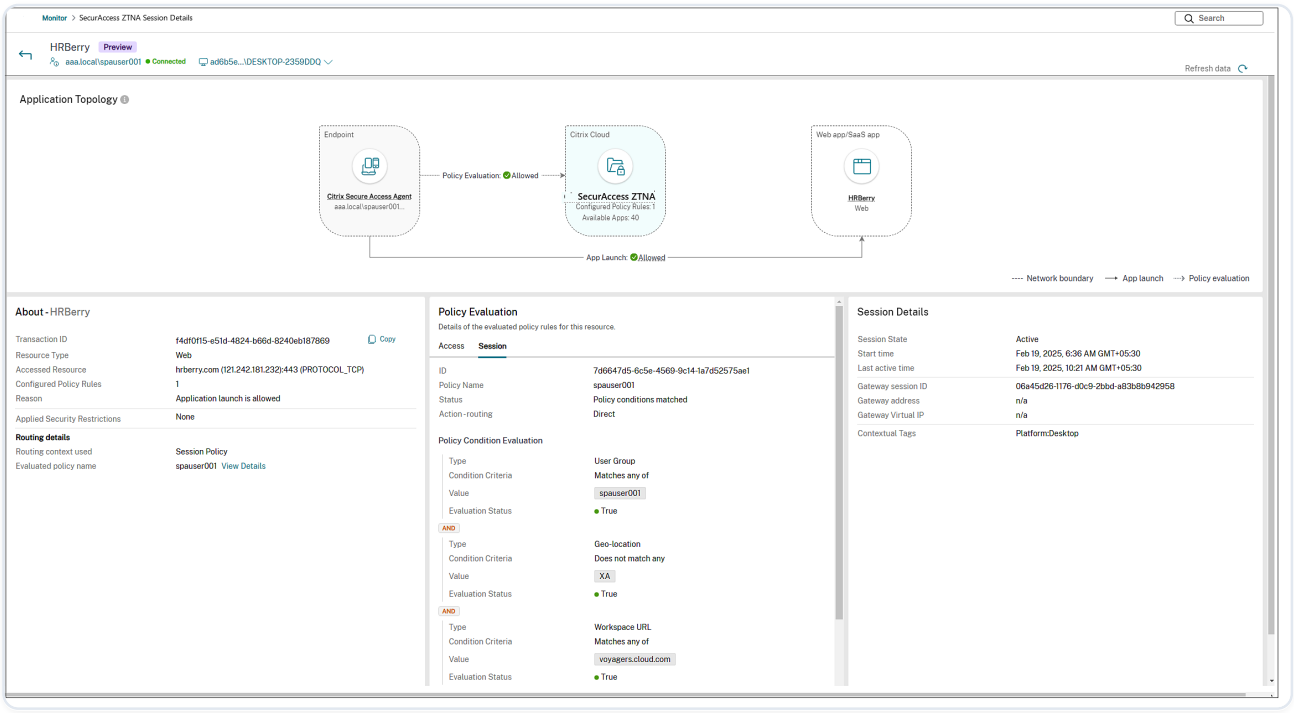
When you click an app from the **Launched Apps** or **Available Apps** tabs, the application topology page appears, displaying complete information about the app.

- **Session Topology:** Displays the app launch flow.
- **About:** Displays app-related information such as app type, number of policy rules, security restrictions, and accessed resources. The data that appears in the **Accessed Resources** section varies depending on the app type.
  - SaaS apps - URL or the app FQDN
  - TCP/UDP – IP address/FQDN, port, and protocol
  - Web app (launched via Citrix SecurAccess client) - FQDN, port, and protocol
  - Web app (launched via Citrix Workspace app) - URL
- **Policy evaluation:** Displays information related to the access policy, such as rules, actions, and conditions.
- **Session Details:** Displays information related to the session, including session start and end time, session state, and contextual tags associated with the policy.

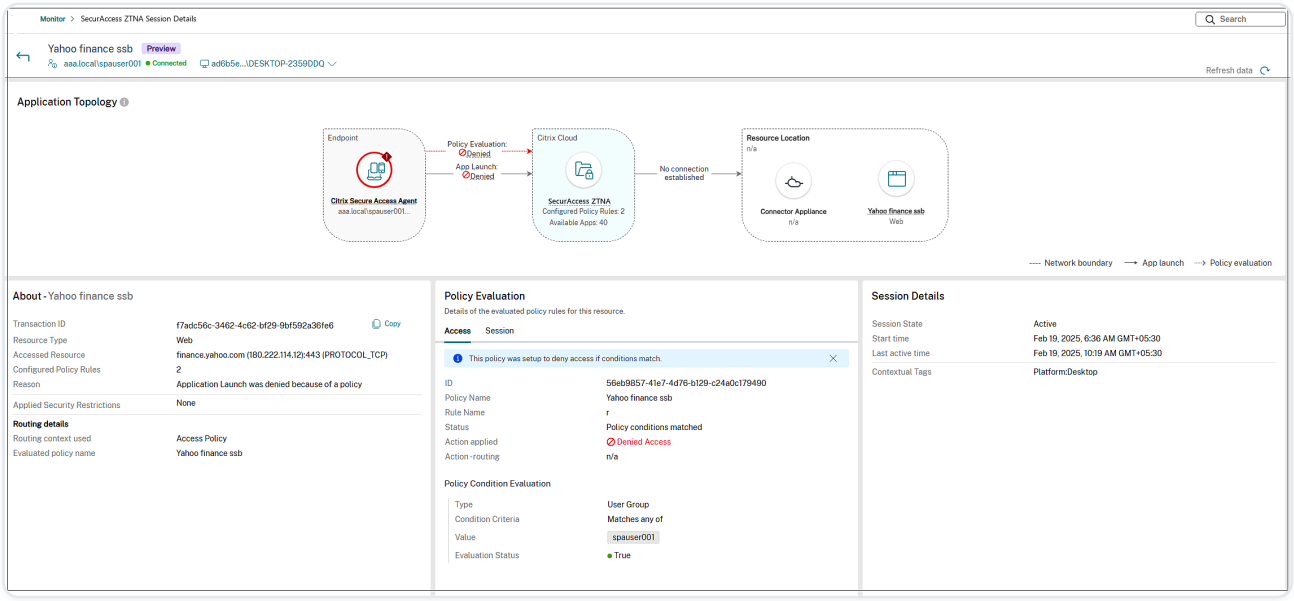
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Domains Visited** field is applicable only for the Web/SaaS apps and is updated only after 15 minutes, as the Citrix Enterprise Browser clients on macOS and Windows send session activity every 15 minutes.
- The **Session Details** column section remains empty for apps clicked from the **Available Apps** tab, as app enumeration is not associated with a session.

The following figure displays a sample topology diagram for a successfully launched app.



The following figure displays a sample topology diagram for an access denied app.



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

Contextual tags

The Citrix SecurAccess™ ZTNA provider enables contextual access (smart access) to Web or SaaS applications based on the user session context such as device platform and OS, installed software, geolocation.

Administrators can add conditions with contextual tags to the access policy. The contextual tag on the Citrix SecurAccess ZTNA provider is the name of a NetScaler® Gateway policy (session, preauthentication, EPA) that is applied to the sessions of the authenticated users.

The Citrix SecurAccess ZTNA provider can receive smart access tags as a header (new logic) or by making callbacks to Gateway. For details, see Adding a new contextual tag.

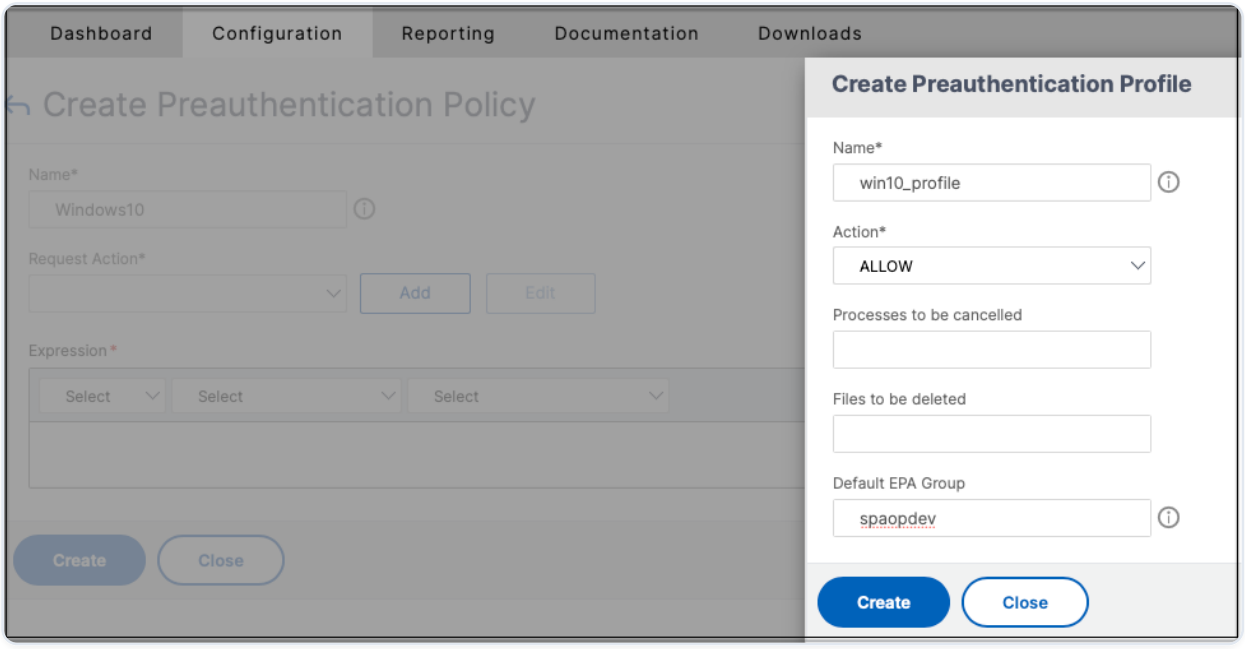
Configure custom tags using the GUI

The following high-level steps are involved in configuring contextual tags.

1. Configure a classic gateway preauthentication policy.
2. Bind the classic preauthentication policy to the gateway virtual server.

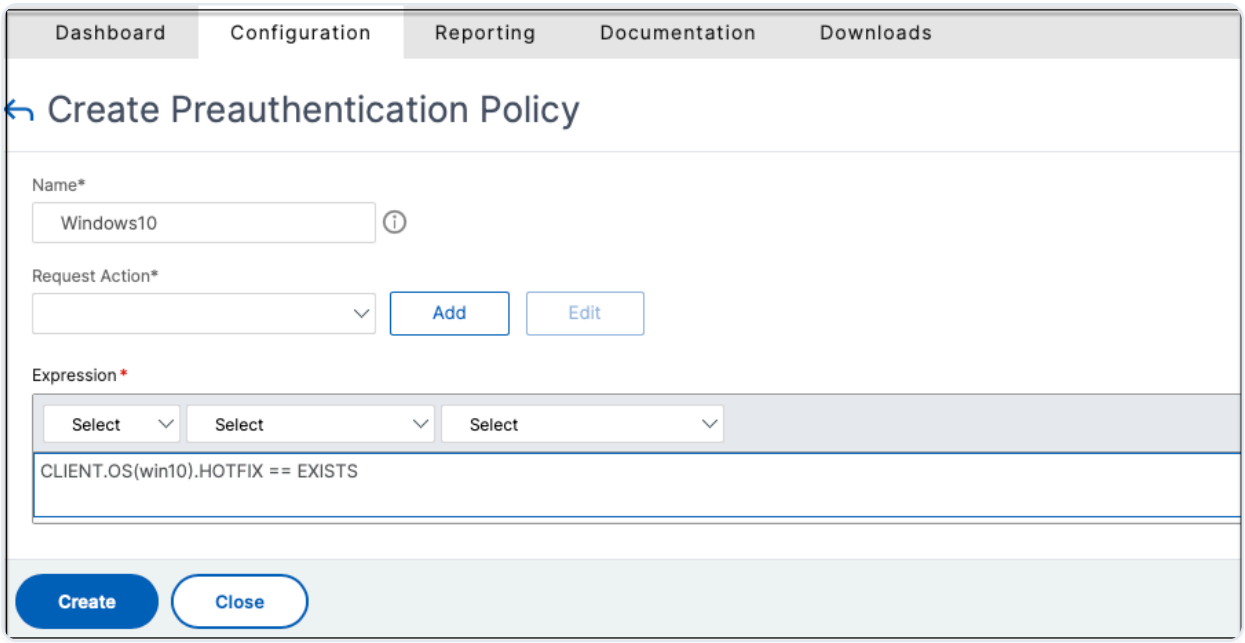
Configure a classic gateway preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.
2. Select an existing policy or add a name for the policy. This policy name is used as the custom tag value.
3. In **Request Action**, click **Add** to create an action. You can reuse this action for multiple policies, for example, use one action to allow access, another to deny access.



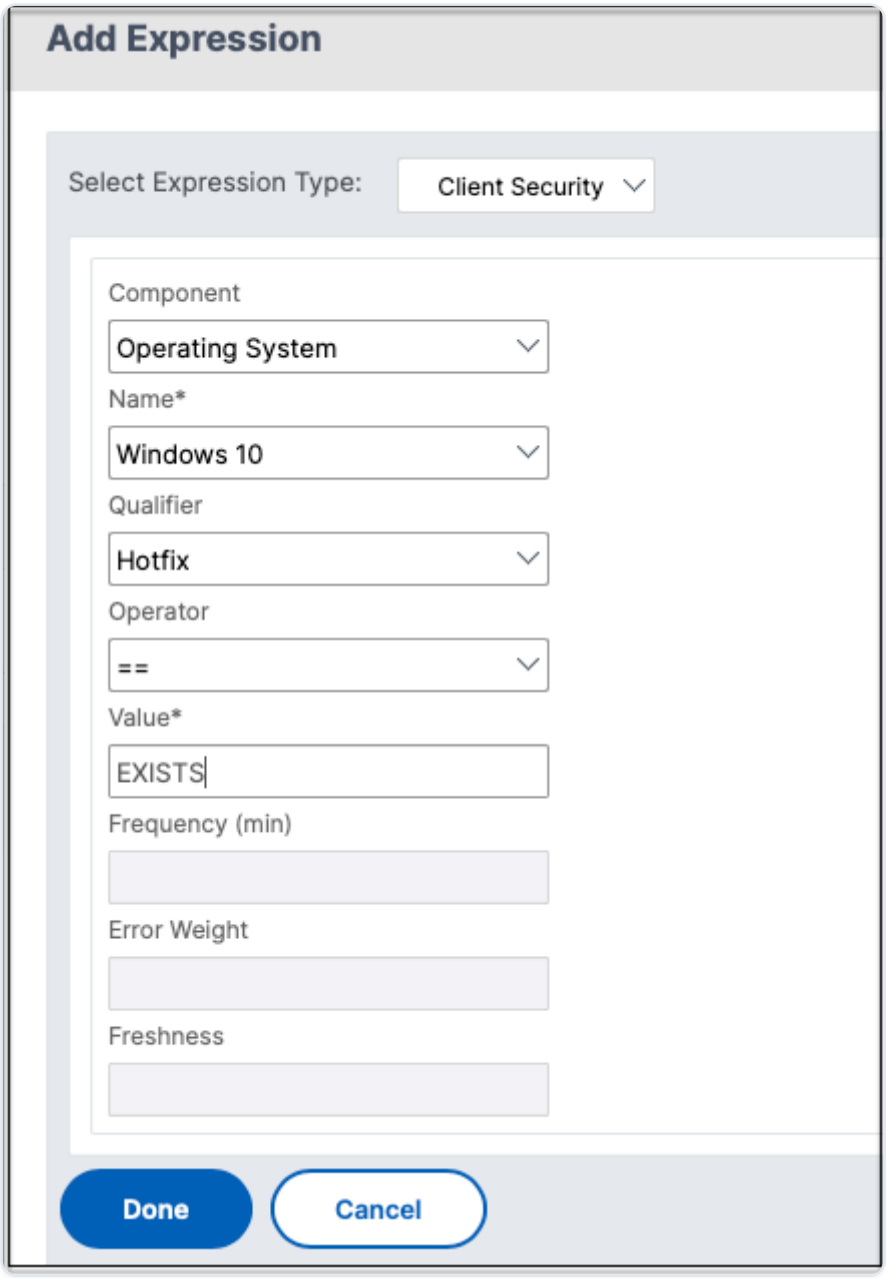
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Fill in the details in the required fields and click **Create**.
5. In **Expression**, enter the expression manually or use the Expression editor to construct an expression for the policy.



The following figure displays a sample expression constructed for checking the Windows 10 OS.

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

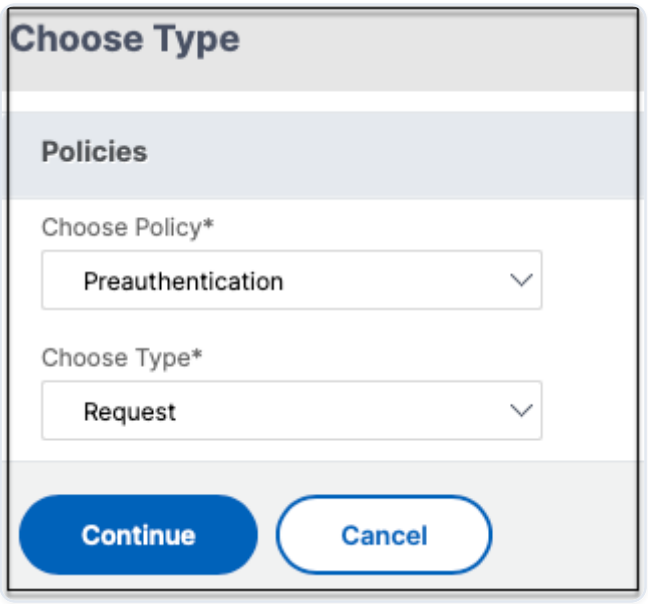


6. Click **Create**.

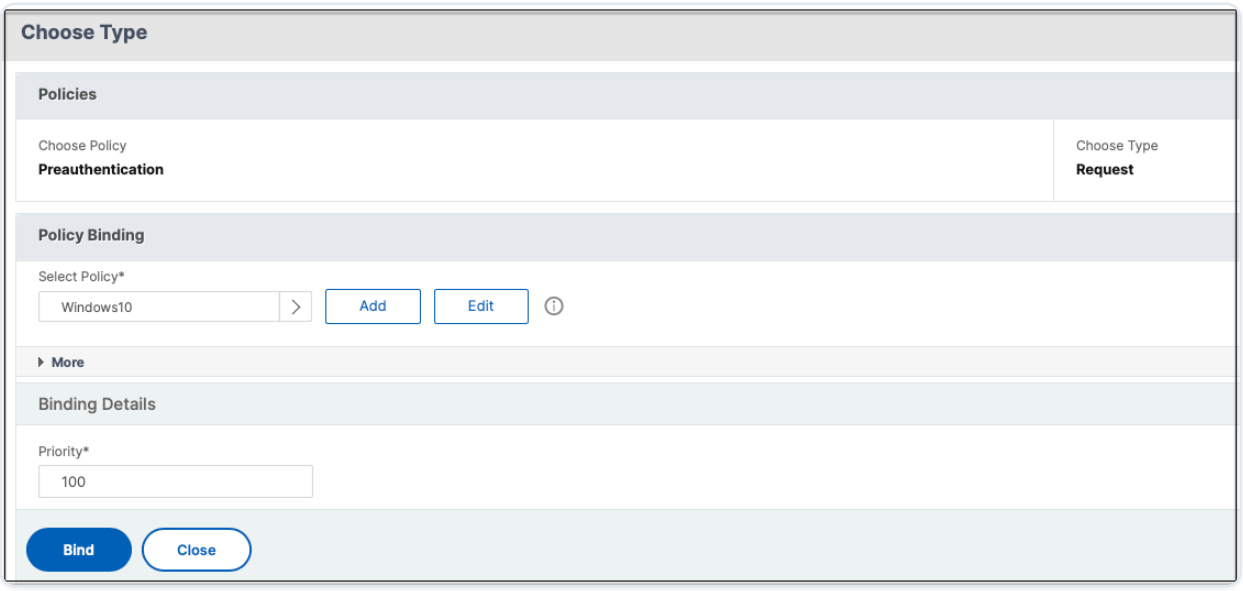
Bind the custom tag to NetScaler Gateway

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Select the virtual server for which the preauthentication policy is to be bound and then click **Edit**.
3. In the **Policies** section, click **+** to bind the policy.
4. In **Choose Policy**, select the preauthentication policy and select **Request** in **Choose Type**.

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



5. Select the policy name and the priority for the policy evaluation.
6. Click **Bind**.



Configure custom tags using the CLI

Run the following sample commands on the NetScaler CLI to create and bind a preauthentication policy:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10) EXISTS" win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Run the following sample command on the NetScaler CLI to configure nFactor EPA policy:

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

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr(\"proc_0_notepad.exe\")" -defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

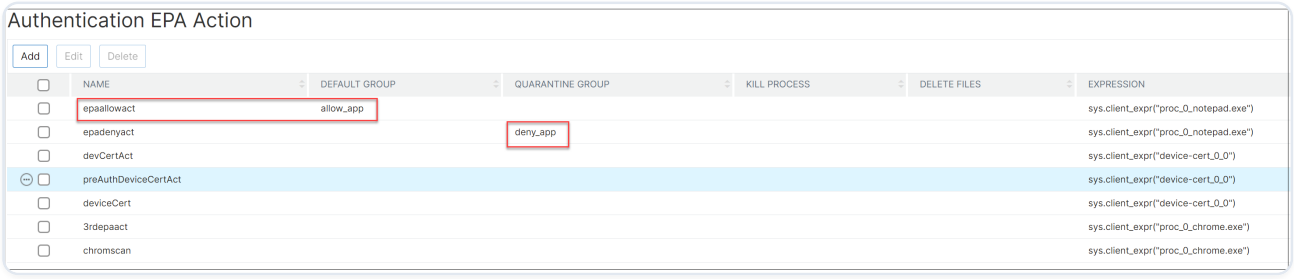
Adding a new contextual tag

1. Open the Citrix SecurAccess ZTNA admin console and click **Access Policies**.
2. Create a new policy or edit an existing policy.
3. In the **Condition** section, click **Add condition** and select **Contextual Tags**, **Matches all of**, and then enter the contextual tag name (for example, `Windows10`).

Note on EPA tags sent to Citrix SecurAccess ZTNA provider

The EPA action name configured in nFactor EPA policy and the associated group name as smart access tags to the Citrix SecurAccess ZTNA provider. However, the tags that are sent are dependent on the outcome of the EPA action evaluation.

- If all EPA actions in an nFactor EPA policy results in action **DENY** and a quarantine group is configured in the last action, the quarantine group name is sent as the smart access.
- If an EPA action in an nFactor EPA policy results in action **ALLOW**, the EPA policy names associated with the action and the default group name (if configured) are sent as the smart access tags.



In this example, when the action is denied, deny_app is sent as the smart access tag to the Citrix SecurAccess ZTNA provider. When the action is allowed, epaallowact and allow_app are sent as the smart access tags to the Citrix SecurAccess ZTNA provider.

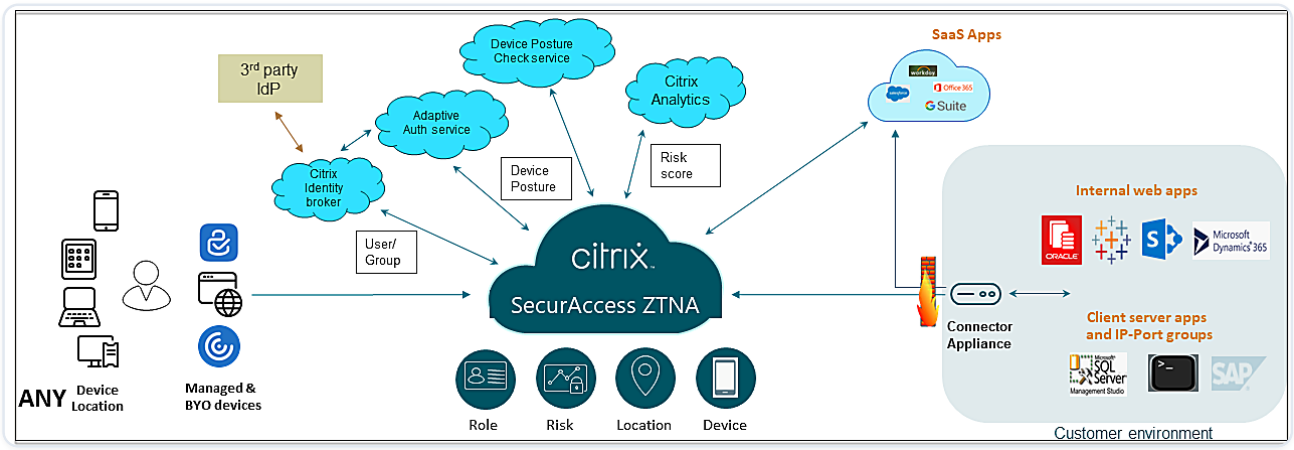
Citrix SecurAccess™ ZTNA

The Citrix SecurAccess ZTNA service enables the administrators to provide a cohesive experience integrating single sign-on, remote access, and out-of-band content inspection into a single solution for end-to-end access control. IT administrators can govern access to approved SaaS apps with a simplified single sign-on experience. With the Citrix SecurAccess ZTNA service, administrators can

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

also protect the organization's network and end user devices from malware and data leaks by filtering access to specific websites and website categories. Administrators can enforce enhanced access security policies for secure access to SaaS applications. Once authenticated, employees have access to all critical business applications from any device irrespective of whether they are in the office premises, at home, or traveling.

Administrators can monitor user activities, such as malicious, dangerous, or unknown websites visited, and the bandwidth consumed, and risky download and upload behaviors. Using the Analytics around websites and website categories accessed, administrators can take corrective action to protect the enterprise network. At the same time, the service provides end users seamless and secure access to all their hosted apps.



Key capabilities of Citrix SecurAccess ZTNA

Some of the key tasks that you can complete with the Citrix SecurAccess ZTNA service are:

- **Publish SaaS apps with single sign-on access** - Once the user is authenticated to Citrix Workspace™ with a primary identity, subsequent authentication challenges to SaaS and web apps are automatically fulfilled by the single sign-on feature in the Citrix Cloud™ using SAML assertions.

By default, the SAML assertion utilizes the email address associated with the user's Active Directory account (identity provider) with the email address associated with the user's SaaS or web app account (service provider).

- **Provide contextual access** - Although an authorized SaaS app is considered safe, content in the SaaS app actually can be dangerous - constituting a security risk. When a user clicks a hyperlink within a SaaS app, the traffic is routed through the web filtering feature, which provides a risk assessment for the hyperlink. Based on the hyperlink's risk assessment, and

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

the customized list of URL categories, the web filtering feature allows, redirects, or denies the hyperlink request from the user as follows:

  - Approved: The hyperlink is considered safe and the Chrome browser within the Workspace app accesses the hyperlink.
  - Denied: The hyperlink is considered dangerous and access is denied.
  - Redirected: The hyperlink request is redirected to the Remote Browser Isolation service, where the user's internet browsing activities are isolated from the endpoint device, the corporate network, and the SaaS app.

- **Security and performance analytics** - Users invariably access SaaS apps that have enhanced security inherent in them. The workspace app, the Citrix SecurAccess ZTNA service, and the Remote Browser Isolation service provide the Security analytics service with information about the following user and application behaviors. These analytics impact the user's overall risk score:

  - App launch time
  - App end time
  - Print action
  - Clipboard access
  - URL Access
  - Data upload
  - Data download

- **Web filtering:** The web filtering feature evaluates the risk of each hyperlink selected within the SaaS application. Accessing these sites and monitoring changes in user behavior increases the user's overall risk score because it signals the endpoint device is compromised and started to infect or encrypt data or the user and device are stealing intellectual property.
- **Integration with Security Information and Event Management (SIEM)** - The Citrix SecurAccess ZTNA logs can be exported via Kafka to SIEM such as Splunk, Sentinel, and Elastic. Exporting logs to SIEM enhances security capabilities and improves incident response effectiveness. For details, see Citrix SecurAccess ZTNA events.

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