



CHECKLIST

Citrix Session Reliability Troubleshooting Checklist

A practical, vendor-neutral checklist for isolating Citrix Session Reliability issues, validating the transport path, and deciding on safe fixes before rollout.

Citrix Session Reliability Troubleshooting Checklist

Use this checklist to isolate where Session Reliability is failing, verify the transport path, and confirm whether a change is safe before wider production rollout.

1) Confirm the symptom pattern

- ☐ Identify whether users report a brief freeze, disconnect, delayed reconnect, or repeated drop.
- ☐ Note whether the session recovers automatically or requires a manual reconnect.
- ☐ Record whether the failure happens immediately, after logon, after idle time, or during network changes.
- ☐ Check whether the issue is intermittent or occurs at a consistent interval.
- ☐ Capture the user's network type: office wired, home broadband, Wi-Fi, VPN, or mobile hotspot.

2) Define the fault domain

- ☐ Determine whether the issue appears on the endpoint, network path, gateway, broker, or session host.
- ☐ Test one affected user against one known-good user path.



- ☐ Compare behavior on a different network or from a different endpoint.
- ☐ Confirm whether the problem follows the user, the device, or the network path.
- ☐ Separate transport issues from application performance or logon slowness.

3) Verify the policy and session settings

- ☐ Confirm that Session Reliability is enabled where expected.
- ☐ Check which policy is actually applied to the affected user or delivery group.
- ☐ Look for higher-priority settings that override the intended configuration.
- ☐ Verify related HDX/session timeout settings for conflicts.
- ☐ Document the current configuration before changing anything.

4) Validate the transport path

- ☐ Confirm whether users connect directly or through a gateway.
- ☐ Verify that all required ports and protocols are allowed end to end.
- ☐ Check for firewall session timeouts or idle tracking limits.
- ☐ Review proxy, inspection, and packet-filtering behavior on the path.
- ☐ Check for asymmetric routing, NAT changes, or load balancer persistence issues.

5) Inspect intermediate devices

- ☐ Review firewall logs for session resets, drops, or idle expirations.
- ☐ Check load balancer persistence and timeout values.
- ☐ Validate gateway timeout behavior against expected session recovery duration.
- ☐ Confirm that no device is closing the connection before recovery can occur.
- ☐ If possible, compare affected and unaffected paths through the same infrastructure.



6) Check endpoint conditions

- ☐ Ask whether the failure correlates with sleep, wake, network roaming, or VPN reconnect.
- ☐ Check whether wireless instability or roaming events coincide with the symptom.
- ☐ Verify whether endpoint security software is inspecting or delaying traffic.
- ☐ Test from a clean or controlled endpoint where possible.
- ☐ Confirm whether managed devices fail while unmanaged devices do not.

7) Compare good and bad cases

- ☐ Reproduce the issue on a known-bad path.
- ☐ Repeat the same test on a known-good path.
- ☐ Compare network latency, packet loss, and disconnect timing.
- ☐ Note whether the symptom disappears on wired connectivity.
- ☐ Document every difference between the two paths.

8) Decide whether the issue is transient or structural

- ☐ If the session pauses briefly and recovers, treat it as a transient transport event.
- ☐ If the disconnect happens at a fixed time, focus on a timeout or policy mismatch.
- ☐ If reconnect is slow or requires retries, inspect routing, gateway, or broker behavior.
- ☐ If only one network fails, treat the remote path as the primary suspect.
- ☐ Avoid changing multiple layers at once.

9) Apply safe fixes in order



- ☐ Start with the smallest change that matches the likely fault domain.
- ☐ Adjust intermediate timeout or persistence settings before broad Citrix changes when the evidence points to the path.
- ☐ Correct routing, firewall, or gateway behavior if the transport is being interrupted.
- ☐ Change Citrix policy only when the configuration is misaligned or confirmed to be the cause.
- ☐ Re-test after each change before moving to the next.

10) Validate before production rollout

- ☐ Test the change with one affected user or a limited pilot group.
- ☐ Confirm that the original symptom no longer occurs.
- ☐ Verify that normal reconnect behavior still works as intended.
- ☐ Watch for side effects such as slower reconnects, lingering sessions, or broader connectivity issues.
- ☐ Roll out broadly only after the fix is stable across the affected path types.

Quick symptom-to-cause guide

Symptom Most likely area to check first
Brief freeze, then recovery Wireless instability, short packet loss, transient path interruption
Disconnect after a consistent interval Idle timeout, firewall session lifetime, gateway timeout, load balancer persistence
Slow reconnect or retry required Gateway path, routing, persistence, broker behavior
Works on one network but not another Environmental difference, VPN, home router, ISP, firewall policy
Fails after sleep or network change Endpoint power state, Wi-Fi roaming, VPN reconnect handling



Minimum evidence to collect

- ☐ Exact time of each failure.
- ☐ User name or session ID.
- ☐ Network type and location.
- ☐ Whether the session was direct or gateway-mediated.
- ☐ Timeout values or relevant policy settings.
- ☐ Any firewall, gateway, or load balancer logs that show resets or expirations.
- ☐ A side-by-side comparison of affected and unaffected paths.

Safe operating rule

- ☐ Treat Session Reliability as a recovery feature, not a substitute for a stable path.
- ☐ Fix the fault domain that is actually interrupting the session.
- ☐ Validate one change at a time.
- ☐ Confirm recovery behavior before broad rollout.

Notes

- ☐ If symptoms include lag as well as disconnects, investigate network latency alongside Session Reliability behavior.
- ☐ If the issue only appears on remote or VPN paths, prioritize intermediate network devices and timeout settings.
- ☐ If users report a pattern that is consistent to the minute, look for a timer first.

Outcome: After completing this checklist, you should be able to identify the most likely fault domain, confirm whether the transport path supports session recovery, and choose a safe remediation path for production.