

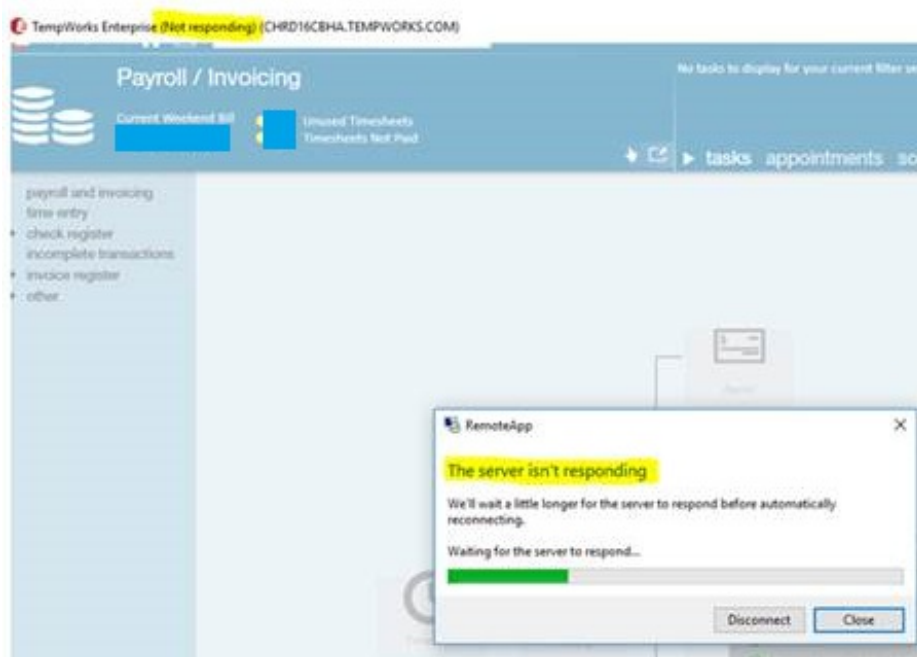
# “Not Responding” lockup when using TempWorks Enterprise RemoteApp

Last Modified on 06/06/2018 2:49 pm CDT

Updated for latest information after Windows Version 1803 release

In the months surrounding January 2018 several users of TempWorks Software’s “Apps.TempWorks.com” hosted software model have reported frequent and persistent issues with the software appearing to “lock up”.

An example of this particular condition is shown below, characterized by the appearance of a title bar on top of the window with the “(Not responding)” indication, as well as the pop-up message titled “RemoteApp” containing the “The server isn’t responding” error. The condition will not resolve unless the Remote Desktop process is manually ended by the user.



This condition has been found to be caused by a specific form of network connectivity failure where the conversation between the client computer and TempWorks’ datacenter

is interrupted suddenly and with no notification to either the client or TempWorks. This interruption could potentially be caused by network devices at the client, or by devices on the client's internet service provider. Technical details of the connectivity failure can be found in appendix below. At this time all confirmed examples of this condition are occurring at locations serviced by Comcast Cable internet.

At this time the condition has only been found to occur on clients running the Windows 10 operating system "Fall creators update" also known as version 1709. While the underlying cause is network connection failure, other versions of the Microsoft Operating system resolve the situation with an automatic reconnection attempt that is usually not noticed by the end user. However, this version of Microsoft software appears to suffer from a defect in the reconnection mechanism.

There is some indication from the Microsoft community that this issue may be resolved in the next release of Windows 10 codenamed "Redstone 4", it is currently available on an Opt-In basis via the Windows 10 Insider Preview program.

<https://blogs.windows.com/windowsexperience/tag/windows-insider-program/>

However, use of this is cautioned as these preview versions of windows have historically proven problematic for production environments at times.

At this time it is our recommendation that clients experiencing this issue seek to either

A. Improve network connection stability with the assistance of local IT and ISP resources.

B. move off of Windows version 1709 either by rolling back updates or upgrading to version 1803

Warning, 1803 has a new RDP performance issue described in <http://kb.tempworks.com/help/popup-windows-freeze-or-do-not-appear-in-enterprise-remote-app>

C. apply a manual update to RDP components referenced in

<http://kb.tempworks.com/help/popup-windows-freeze-or-do-not-appear-in-enterprise-remote-app>

Either should reduce or eliminate the occurrence of this condition.

If you would like further assistance or have additional information on this matter please reach out to TempWorks Support.

#### Appendix:

The network disconnection presents as a sudden halt of data flow on the underlying primary TCP session between TempWorks' RDP Gateway server and the RDP client. No TCP RST packets are received by either side of the connection.

Exhaustive diagnostics on TempWorks' infrastructure has ruled out this session loss occurring on any of TempWorks' systems or direct ISP systems.

Further the only ISP in common in the routes to all examples of this condition is Comcast Cable.

The only technical explanation is that some network device between the client computer and the internet that is capable of differentiating traffic on a TCP (layer 4) basis is disposing of the session which allows such traffic for a specific conversation or is discriminating against a specific conversation. This could include NAT gateways, Network Firewalls, or other L4 security or traffic management systems. It could also include such systems operated by the client's ISP (in all examples, Comcast)

Packet capture/analysis of disconnect event.

## Server Side, captured at TempWorks network edge

Seq	Time	Source	Destination	Length	Protocol	Details	Notes
5388	2018-02-09T10:10:03.10153270	68.142.156.75	96.84.100.100	3033998803	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5390	2018-02-09T10:10:04.04703256	68.142.156.75	96.84.100.100	532765794	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
5392	2018-02-09T10:10:04.05366560	68.142.156.75	96.84.100.100	333333333	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5394	2018-02-09T10:10:06.20071880	68.142.156.75	96.84.100.100	3033998987	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5396	2018-02-09T10:10:08.20180790	68.142.156.75	96.84.100.100	3033999070	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5397	2018-02-09T10:10:09.03093358	68.142.156.75	96.84.100.100	3033999072	HTTPS (443)	51564	Retransmitted #5396
5398	2018-02-09T10:10:09.03123928	68.142.156.75	96.84.100.100	3033999070	HTTPS (443)	51564	Retransmitted #5398
5399	2018-02-09T10:10:09.03892290	68.142.156.75	96.84.100.100	3033999171	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5400	2018-02-09T10:10:10.01120880	68.142.156.75	96.84.100.100	3033999070	HTTPS (443)	51564	Retransmitted #5398
5401	2018-02-09T10:10:10.07895440	68.142.156.75	96.84.100.100	3033999263	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5402	2018-02-09T10:10:11.04893728	68.142.156.75	96.84.100.100	3033999071	HTTPS (443)	51564	Retransmitted #5396
5403	2018-02-09T10:10:12.16150480	68.142.156.75	96.84.100.100	3033999355	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5404	2018-02-09T10:10:13.07948718	68.142.156.75	96.84.100.100	3033999070	HTTPS (443)	51564	Retransmitted #5398
5405	2018-02-09T10:10:13.08161740	68.142.156.75	96.84.100.100	3033999447	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5406	2018-02-09T10:10:15.20093408	68.142.156.75	96.84.100.100	3033999339	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5407	2018-02-09T10:10:17.20093358	68.142.156.75	96.84.100.100	3033999631	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5408	2018-02-09T10:10:18.05781218	68.142.156.75	96.84.100.100	3033999070	HTTPS (443)	51564	Retransmitted #5398
5409	2018-02-09T10:10:18.04373880	68.142.156.75	96.84.100.100	3033999723	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5410	2018-02-09T10:10:19.10157940	68.142.156.75	96.84.100.100	3033999015	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5411	2018-02-09T10:10:21.20080880	68.142.156.75	96.84.100.100	3033999907	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5412	2018-02-09T10:10:22.10182970	68.142.156.75	96.84.100.100	3033999999	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5413	2018-02-09T10:10:24.20192250	68.142.156.75	96.84.100.100	3034000091	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5414	2018-02-09T10:10:26.20059440	68.142.156.75	96.84.100.100	3034000183	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5415	2018-02-09T10:10:28.10113120	68.142.156.75	96.84.100.100	3034000275	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
5416	2018-02-09T10:10:28.01837450	68.142.156.75	96.84.100.100	3034000367	HTTPS (443)	51564	Records: [ApplicationData(Encrypted)]
						Flags: ...A.R... SrcPort: HTTPS (443), DestPort: 51564	after 20 seconds of no communication a reset is sent to hangup this reset is never received

## Client Side, captured by Microsoft packet filter on client

Seq	Time	Source	Destination	Length	Protocol	Details	Notes	
25810	2018-02-09T10:10:03.8371935	96.84.100.100	68.142.156.75	532765994	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]	
25812	2018-02-09T10:10:04.6460868	96.84.100.100	68.142.156.75	333333333	HTTPS (443)	51564	Segment_Lost	
25823	2018-02-09T10:10:06.4061304	2.8521259	68.142.156.75	10.1.10.54	3033998987	HTTPS (443)	Incomplete_ApplicationData	
25825	2018-02-09T10:10:16.0640881	9.5679577	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25826	2018-02-09T10:10:16.3643977	9.3083986	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25827	2018-02-09T10:10:16.6645138	9.3083218	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25826
25828	2018-02-09T10:10:17.2649336	9.6803151	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25829	2018-02-09T10:10:18.4644887	1.1395581	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25830	2018-02-09T10:10:20.8649592	2.4805105	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25831	2018-02-09T10:10:24.0540254	2.1209262	10.1.10.54	68.142.156.75	532766144	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25832	2018-02-09T10:10:25.0510974	1.6118728	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25833	2018-02-09T10:10:25.2656747	0.5997723	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25834	2018-02-09T10:10:54.0551732	18.7894985	10.1.10.54	68.142.156.75	532766191	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25835	2018-02-09T10:10:56.6916438	8.4124267	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25836	2018-02-09T10:11:03.8457931	9.3780592	10.1.10.54	68.142.156.75	532766226	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25837	2018-02-09T10:11:13.8728661	29.0211608	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25838	2018-02-09T10:11:33.8459594	0.9788013	10.1.10.54	68.142.156.75	532766269	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25839	2018-02-09T10:12:03.8460488	30.0008894	10.1.10.54	68.142.156.75	532766304	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25840	2018-02-09T10:13:03.8610463	28.0322979	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25841	2018-02-09T10:13:03.8418604	30.9737231	10.1.10.54	68.142.156.75	532766417	51564	HTTPS (443)	Segment_Lost
25842	2018-02-09T10:13:33.8601433	29.0272739	10.1.10.54	68.142.156.75	532766037	51564	HTTPS (443)	Retransmitted #25825
25843	2018-02-09T10:13:33.8422894	0.9734661	10.1.10.54	68.142.156.75	532766408	51564	HTTPS (443)	Records: [ApplicationData(Encrypted)]
25844	2018-02-09T10:14:32.8090426	59.0264332	10.1.10.54	68.142.156.75	532766538	51564	HTTPS (443)	Flags: ...A.R... SrcPort: 51564, DstPort: 51564

# Related Articles