

Increasing Windows TCP socket limits

Uptime Infrastructure Monitor is a heavily network-dependent application and requires many short-lived socket connections to be running simultaneously. At times this socket load can reach or exceed the default Windows monitoring station socket limit. Symptoms of socket limits within Uptime Infrastructure Monitor include:

- Random service outages stating connection errors.
- Random connection errors appearing in the Apache error_log file.
- Errors such as Monitor failed: Software caused connection abort: recv failed.

To increase the Windows socket limits and allow sockets to be freed up more quickly, create 2 keys in the Windows registry using regedit.

Within `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`, create these 2 DWORD values:

- `MaxUserPort`: this value will increase the number of ephemeral ports that can be dynamically allocated to clients. Set the value to any decimal between 5000 and 65534. Higher counts will allow more concurrent sockets to be available to Uptime Infrastructure Monitor.
- `TcpTimedWaitDelay`: this value will reduce the length of time that a connection stays in the `TIME_WAIT` state when the connection is being closed. While a connection is in the `TIME_WAIT` state, the socket pair cannot be re-used. Lower values allow sockets to be released more quickly for re-use by Uptime Infrastructure Monitor. Set the value to a decimal number between 30 and 240. Note that you will need to restart the computer for the system changes to take effect. For more information, please refer to [Avoiding TCP/IP Port Exhaustion](#) on the Microsoft website.

Related KB - [monitor failed: software caused connection abort: recv failed](#)