itracks Realtime Network Requirements

This article is intended for IT teams that need additional details to troubleshoot connection and firewall issues with people accessing the itracks Realtime software.

Basic Requirements

Realtime is a WebRTC application. As such the network requirements are the same as defined for that standard. For the “Azure” destination, see the Azure Public IP Address Ranges section.

Port(s)	Protocol	Destination
443	TCP	*.itracks.com
3478	UDP	Azure
49152-65535	UDP	Azure

These rules should be applied to outbound traffic. Realtime will communicate to the destination port received when the client makes its connection. The firewall should be configured to allow these return connections.

VPN

See itracks Realtime and VPN Connections – itracks (zendesk.com)

In those scenarios where a VPN must be used, we recommend that you provide an alternate path for Realtime traffic that bypasses the virtual private network (VPN), commonly known as split-tunnel VPN. Split tunnelling means that traffic for Realtime doesn't go through the VPN but instead goes directly to Realtime. Bypassing your VPN will have a positive impact on Realtime quality, and it reduces the load from the VPN devices and the network. To implement a split-tunnel VPN, work with your VPN vendor.

Azure Public IP Address Ranges

Itracks Realtime is primarily hosted in the Azure Cloud. Therefore, management of rules for Realtime should be approached similarly as with any other resource hosted within Azure, as the list of IP Addresses can be extensive and may change. There are many online articles explaining how this may be done.

To get started with a static list of ranges, we recommend leveraging the Azure IP Ranges online tool found at https://azureipranges.azurewebsites.net/. To use this tool:

1. Ensure that the Cloud Environment selection is set to “Public”

2. In the input box, for each region below, enter a value in the format “azurecloud.region”
    - Centralus
    - southcentralus
    - australiaeast
    - westus
    - canadacentral
    - ukwest
    - northeurope
    - eastasia
    - japanwest
    - germanywc

3. Download the result in the format that best suits your environment.

This tool works with the list of IP Address ranges published weekly by Microsoft at https://www.microsoft.com/en-us/download/details.aspx?id=56519. This link is to a page where a JSON document listing all ranges for all Azure services may be downloaded. From this document, the Public Cloud values with a name starting with “AzureCloud” list the address prefixes that encompass the ranges that might be used by Realtime servers.

Ideally, scripts should be developed that leverage this resource to ensure ranges are up to date. To get started on this, we recommend looking at Get-AzNetworkServiceTag (Az.Network) | Microsoft Learn

Itracks Public IP Addresses

In some cases, Realtime may require access to resources that hosted by itracks rather than the Azure Cloud. The IP Addresses for these resources are:

- 50.57.24.241 to 50.57.24.254
- 162.209.25.140
- 162.209.25.141
- 162.209.25.208 to 162.209.25.215
- 198.61.139.168 to 198.61.139.171
- 166.78.226.113
- 166.78.226.114

Port Ranges

Realtime may use these ports:

- TCP/80
- TCP/443
- TCP/3478
- UDP/3478

- TCP/8443
- UDP/8443
- UDP/49152-65535

Realtime Domain Considerations

All requests are directed towards *.itracks.com. If your firewall device supports domain-based rules, please add *.itracks.com to the whitelist.

If advanced technologies, such as deep packet inspection (DPI), are employed to inspect encrypted traffic and/or enforce data loss prevention policies, it is recommended to exclude *.itracks.com from the inspection list. These technologies may prevent WebRTC traffic from functioning properly, resulting in unexpected errors.