Adding video call access to your services

Technical Guide
Technical Guide

Copyright ©2021
All rights reserved.
Publication date: October 2021
Build: NHS211012.1001

**Audience** - People who: ensure that network environments are Attend Anywhere-ready; set up video calling equipment; provide Attend Anywhere troubleshooting advice.

If you need assistance relating to the content of this book, contact nhsenglandsupport@attendanywhere.com

**Note: PDF note:** For best results when printing this document, use your printer's double-sided setting if available.
# Table of contents

## Overview
- Introduction .......................................................... 5
- Online resources ..................................................... 5

## How does Attend Anywhere support your organisation?
- Designed for health and care ........................................ 6
- Robust client-side component integration .......................... 6
- Sandboxed application .................................................. 6
- WebRTC implementation ............................................. 6
- Network security ....................................................... 6
- Web proxy services .................................................... 8
- Call quality profiles ................................................... 8

## Privacy and security strategy
- Management console privacy and security ......................... 9
- Security ....................................................................... 10
- Privacy ....................................................................... 10
- Hosting practices ........................................................ 11
- Attend Anywhere's hosting practices ............................... 11

## Configure patient administration systems
- Your network ................................................................ 13

## Your network
- WebRTC and Attend Anywhere ........................................ 16
- Testing WebRTC network readiness ................................ 18
  - Understanding the test results .................................... 18
  - Running the test ....................................................... 18
  - Examples .................................................................... 19
- Network access ............................................................. 21
- Web access .................................................................... 21
- Signalling access .......................................................... 21
- Attend Anywhere relay servers ...................................... 21
- Network readiness ....................................................... 22

## Media pathways
- Achieving the best-quality connection .............................. 23

## Call Quality and Bandwidth
- Bandwidth per remote party in a call .............................. 26

## Troubleshoot Network
- Check WebRTC network readiness .................................. 27
- Resolve web proxy-based WebRTC connection issues ......... 27

## Equipment ..................................................................... 29
Overview

Introduction

The Technical Guide contains information and advice for both Attend Anywhere and IT administrators, who oversee the successful operation of consultations and meetings via video.

This book includes topics on:

- Preparing networks for WebRTC-based video calling
- Hardware, web browser, and internet requirements
- Integrating video calling into websites and third-party application software
- Improving the user experience for people making video calls, and users of the Attend Anywhere Management Console
- Troubleshooting

Online resources

- **Making Video Calls poster set**: https://england.nhs.attendanywhere.com/makingcalls
- **Technical implementation guide**: https://england.nhs.attendanywhere.com/techguide
- **Management Console help topics**: https://england.nhs.attendanywhere.com/help
How does Attend Anywhere support your organisation?

Designed for health and care

Attend Anywhere maintains a controlled and regularly-reviewed environment, and application design optimised for health purposes. This limits the exposure to vulnerabilities and inappropriate configurations present in general-purpose communications products and services.

Robust client-side component integration

As the service is hosted and managed by Attend Anywhere, only the client-side components (Google Chrome, Apple Safari, and/or Microsoft Edge web browsers), need to be verified for operation on your LAN/WAN. The Attend Anywhere platform is periodically updated to work with the latest versions of Chrome, Safari, and Edge for best video calling performance.

Note: Both browsers deploy feature and security updates on regular cycles. You do not have to wait for Attend Anywhere application updates to deploy these.

Sandboxed application

Being a web application, the Attend Anywhere Management Console's code is run securely within the web browser, and is limited in its ability to impact your computer's desktop environment.

WebRTC implementation

WebRTC is a dual standard track of IETF and W3C, under the guidance and review of many web and telecommunications industry security experts. The implementations of WebRTC components in Google Chrome, Apple Safari, Microsoft Edge, and the Attend Anywhere web apps, are from Open Source projects; they are therefore open to community review, offering timely discovery of any potential vulnerabilities.

Learn more in the the WebRTC and Attend Anywhere topic in the Resource Centre.

Network security

To minimise exposure of your network to external threats, the system is designed to only require access to a few standard HTTPS and Secure Media ports on trusted Attend Anywhere servers from your desktop, laptop, or mobile device. These are detailed in the Networks topic in the Resource Centre.
How does Attend Anywhere support your organisation?
Web proxy services

Secure web traffic for the Attend Anywhere Management Console can use your existing web proxy services and security policies.

Call quality profiles

You can set a range of video call quality profiles to constrain video media demands on network links to stay within known limits.
Privacy and security strategy

Health-grade privacy, security, and data protection are fundamental to Attend Anywhere’s design.
Management console privacy and security

Health-grade privacy, security, and data protection are fundamental to Attend Anywhere’s design. The Management Console and its network architecture are covered by design assurance processes to ensure that new features and capabilities continue to meet the required standards.

Security

While WebRTC video call media traffic is protected with AES 256-bit encryption between web browsers, expecting this to be adequate protection in a health-care setting would be naive. For example, call encryption does not help if someone is able to highjack the signalling and listen in on the call.

As the volume of video consultations grow, there is a heightened public awareness around privacy and security, and the measures taken to protect against:

- Someone impersonating a clinician. Example: *Gaining access to the video room.*
- Unauthorised observation of a consultation. Example: *Gaining unauthorised access (‘hacking’) the video call signalling.*
- Third parties accessing the history of a consultation. Example: *Observing the call logs on the patient device.)*

Unlike provider-centric meetings, video chat, or conferencing based architectures (which are inherently less private and secure), Attend Anywhere has a **three-tier privacy and security model** that involves:

- Ensuring access is via a single point on the clinic's website.
- Creating private video rooms for each consultation.
- Ensuring that the media signalling cannot be hacked in order to impersonate a clinician, or observe a consult. (Not simply protecting the call content.)
- Ensuring only authorised clinicians from the clinic can join patients’ rooms.
- Ensuring the media content is secure.

Privacy

The Management Console is compliant with government privacy policies in Australia and the UK.

The Management Console is implemented and run according to a System Security Policy approved by NHS National Services Scotland. This incorporates GDPR- and UK Data Protection Act 2018-compliant controls and policies.
Patients enter online Waiting Areas via a trusted service website and wait in their own private video room. It doesn't matter if a clinician is running overtime with another patient, as there is no chance of people running into each other. The room is deleted after the consultation.

Patients can be seen by any clinician authorised to access the Waiting Area. Authorisation is defined by a unique login and assigned roles in the platform. Organisation Administrators are responsible for assigning this access to their staff.

The Management Console does not retain patient-identifiable information which means patients using the Attend Anywhere service leave no digital footprint.

Hosting practices

Attend Anywhere's hosting practices

Attend Anywhere's hosting is operated under an extensive range of security measures, components, and controls, which deliver a robust and secure environment for digital services.

The Attend Anywhere Management Console and its network architecture are covered by design assurance processes, to ensure that new features and capabilities continue to meet the required standards.

Data Sovereignty

All call records and related clinic data within the Attend Anywhere Management Console, stay within sovereign territorial boundaries as required by Privacy Legislation in the UK and Australia.

Infrastructure and application protection

The Attend Anywhere Management Console hosting and web application has multiple layers of protection from web attacks and exploits.

- Web Application Firewall (WAF) with comprehensive Open Web Application Security Project (OWASP) Top 10 coverage
- Distributed Denial-of-Service (DDoS) protection
- Application server systems protection covering:
  - Malware and virus protection
  - Automated system vulnerability assessment
  - On host intrusion protection and detection system
- Virtual patching providing automatic update of protection modules for newly discovered vulnerabilities even before operating system or vendor patches are available.
Infrastructure and application testing

- Attend Anywhere, as part of infrastructure and application assurance, maintains a suite of standard security testing tools
- Regular external-facing testing is performed to ensure infrastructure attack surface-area complies with the design and deployment specifications
- Server configuration and software versions are audited against currently-known vulnerabilities
- The application hosting environment is audited for any inadvertent misconfiguration
- Third-party-contracted testing is performed in concert with key stakeholders

Hosting

- The system is provided as resilient, high availability, hosted service
- Underlying infrastructure is provided by accredited cloud providers, with redundant and resilient internet connections and local utilities
- All systems are hardened according to recognised standards
- All data transported between users and all system components is encrypted
- All data at rest is encrypted

High availability

The system is designed for continuity with resilience to site and component failures.

- Redundant sets of components are deployed into geographically-separated sites. These redundant components are configured for cross-communication, so that if a component fails in a given zone, its functions will be fulfilled by surviving components in the alternate site.
- The design is scalable with additional component units able to be added for resiliency, and capacity.
Configure patient administration systems

Configure patient administration system (PAS) with the option of attending consultations via a video call.

For example:

- Ensure clinic staff can select a *video consultation* appointment type when making a booking
- Ensure the system indicates when a patient will be attending via a video call
- Create reminders to offer video consultations as part of the booking process
- Create a shortcut to the clinic's online Waiting Area from the PAS and other, commonly-used administration or applications
- Create an appointment confirmation template letter with directions (link) to the clinic's online Waiting Area. Include the *Patient Information Leaflet* with appointment confirmations.
- Ensure video consultations are flagged in clinic reports
- Establish a build process for clinic templates (defining whether there will be *ad-hoc* / mixed clinics, or all-video clinics)
Your network

The Attend Anywhere system is designed to work in as many different corporate or institutional networks as possible, with little to no special network configuration required.

After Attend Anywhere is up and running, there are a number of things you can do to improve the user experience. To ensure that the people in an organisation are able to hold video consultations or meetings in the most effective way, make sure that their equipment, web browser, and internet/network environment are all suitable for the task.
WebRTC and Attend Anywhere

The Attend Anywhere Management Console uses WebRTC in-browser technology for the video call itself.

What is WebRTC?

WebRTC 1.0 is a joint W3C and IETF standards candidate web browser technology that enables secure, high-quality video calls between modern web browsers.

How does Attend Anywhere use WebRTC?

Attend Anywhere uses WebRTC for secure video calling between patients and clinicians. Users access Attend Anywhere's calling features without having to download and install special software or plug-ins.

Attend Anywhere supports Google Chrome, Apple Safari, and Microsoft Edge, the most popular web browsers with the most complete support for WebRTC on desktop and mobile.

The platform can support four-to-six sites in the same WebRTC call, depending on the bandwidth and processing power of the equipment at each location.

Call setup

- Attend Anywhere Relay Server
- Consumer's PC & web browser
- Provider's PC & web browser
- Web Application Server
Network

- Web Application Server
- Signalling Data
- Relay Server
- Media Data
- NAT
- Peer
- Peer
Testing WebRTC network readiness

The Attend Anywhere WebRTC Network Readiness Test evaluates how the network setup connects to the outside world, and whether the available bandwidth is sufficient to make video calls.

Although this test is targeted at IT administrators, anyone can use it. It takes less than a minute, and can be run from a Google Chrome or Microsoft Edge web browser. **Important:** This test only evaluates the network connection from the device on which it is run. It does not test the device’s equipment setup.

Understanding the test results

There are five possible connection results. In decreasing order of quality, they are:

- **Excellent**
- **Great**
- **Good**
- **Adequate**
- **No connection**

When the test is complete, the page displays information about the best connection type currently available between your organisation’s network, and an Attend Anywhere Relay Server.

- Any result except for No Connection means that you can make successful video calls. However, the better the result, the more reliable and higher quality the connections will be.
- If the result is other than Excellent, the page also displays information to help you improve it.
- The page also displays a Send Test Results button that makes it easy to email the results to your network administrator.

Running the test

The WebRTC Network Readiness Test is located at:
https://england.nhs.attendanywhere.com/webrtctest

**Technical note:** To provide a known location, the test uses an Attend Anywhere relay server to determine how well you will be able to make successful peer-to-peer video calls. Under normal circumstances, a relay server is not required when making calls, unless specific restrictions have been applied to your network.
Examples

Good connection

The test returns results that indicate good connection to the Attend Anywhere relay server, with suggestions for improving connection quality.

No connection

The test cannot find any possible connection to the Attend Anywhere relay server. The results list the various connection methods and the resulting quality of those connections.
Good connection; low bandwidth

The test returns results that indicate good connection to the Attend Anywhere relay server, with suggestions for improving connection quality. However, the test also determines that the available bandwidth for making calls is low, so the results also indicate the type and quality of call that users can realistically participate in from this connection.
Network access

Web access

Each Attend Anywhere Management Console user’s desktop or laptop computer must have access to Hypertext Transfer Protocol Secure (HTTPS). This is the same access requirement as for other secure internet websites.

For whitelisting site address information, see whitelisting site addresses in the Knowledge Base.

Signalling access

The Attend Anywhere Management Console's background real-time signalling uses HTTPS in Long-Polling mode. This holds web connections open for up to a minute, to allow messages to be sent to the user side as they occur.

Attend Anywhere relay servers

Attend Anywhere relay servers - technically, Traversal Using Relays around NAT (TURN) servers - have several important functions:

- Provide a common, well-known internet address that web browsers can connect to if they are unable to establish a valid peer-to-peer connection
- Act as a protocol converter from TCP to UDP, should a web browser not be able to obtain network egress via UDP
- Act as an endpoint for a web proxy tunnelling connection, should a web browser not be able to route to the relay server on the required UDP or TCP port

The relay process cannot inspect the encrypted media data; it only forwards the data to the negotiated endpoint.

Is latency an issue with Attend Anywhere relay servers?

Relay servers are deployed in several regions, and the closest to participants is automatically used. Variable latency can occur, depending on the location of call participants in relation to the relay server being used for that call.
Network readiness

The Attend Anywhere **WebRTC Network Readiness Test** evaluates how the network setup connects to the outside world, and whether the available bandwidth is sufficient to make video calls.

Although this test is targeted at IT administrators, anyone can use it. It takes less than a minute, and can be run from a Google Chrome or Microsoft Edge web browser. **Important**: This test only evaluates the network connection from the device on which it is run. It does not test the device's equipment setup.

For more information, see *Testing WebRTC network readiness* on page 18.
Media pathways

Attend Anywhere will attempt to use the best network path that it can find.

The following table lists the network paths that the browser attempts to use. These attempts are made in order of preference (1 through 5). The first successful connection will be used.

<table>
<thead>
<tr>
<th>Network path</th>
<th>STUN/Relay server port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1: Direct peer-to-peer UDP, with STUN server-assisted NAT traversal</strong></td>
<td>3478 (UDP)</td>
</tr>
<tr>
<td>Each endpoint will discover its external Internet address using the provided STUN Server. This address is provided to the other endpoint and used to set up the connection through Network Address Translation. Media flows over randomly selected ports over large range of UDP ports <strong>49152 - 65535</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>2: Via (Recommended) Attend Anywhere relay server, using UDP-NAT egress</strong></td>
<td>3478 (UDP)</td>
</tr>
<tr>
<td>Connection is established via UDP port <strong>3478</strong>. This relay address is provided to the other endpoint and used to set up the connection through the relay, back through the local endpoint's connection to the TURN server.</td>
<td></td>
</tr>
</tbody>
</table>
### Network path

<table>
<thead>
<tr>
<th>Network path</th>
<th>STUN/Relay server port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media flows to UDP Port <strong>3478</strong> on the TURN server.</td>
<td></td>
</tr>
<tr>
<td><strong>3: Via Attend Anywhere relay server, using TCP-NAT egress</strong></td>
<td>3478 (TCP)</td>
</tr>
<tr>
<td>Connection is established via TCP <strong>3478</strong>.</td>
<td></td>
</tr>
<tr>
<td>Media flows outwards to TCP <strong>3478</strong> on the TURN Server.</td>
<td></td>
</tr>
<tr>
<td><strong>4: Via Attend Anywhere relay server, using TCP-NAT egress</strong></td>
<td>443 (TCP/TLS)</td>
</tr>
<tr>
<td>Connection is established via TCP/TLS <strong>443</strong>.</td>
<td></td>
</tr>
<tr>
<td>Media flows outwards to TCP/TLS <strong>443</strong> on the TURN Server.</td>
<td></td>
</tr>
<tr>
<td><strong>5: Via Attend Anywhere relay server, using TCP tunnelling through local Web Proxy Server</strong></td>
<td>443 (TCP/TLS)</td>
</tr>
<tr>
<td>As per 4, but the connections are established via a tunnelling connection through your proxy server.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, see *Attend Anywhere relay servers* in **Network Basics**.

**Attend Anywhere relay server addresses** (Pilot DNS):

- turn.attendanywhere.com *(the closest global IP address)*
- turnlon.attendanywhere.com *(a London-based IP address)*

Access is via:

- Port 3478 UDP and TCP
- Port 443 TCP and TCP/TLS

To one of the following IP addresses:

- 52.49.123.201
- 52.213.35.238
- 35.177.237.5
- 35.179.41.66
- 52.56.101.249

**Note:** Only one address will be used per session, but all should be allowed.
Achieving the best-quality connection

For most network paths, the negotiation will likely result in a valid media connection.

- **Direct peer-to-peer via UDP provides the best connection**, but will often be unavailable across institutional networks, due to the security constraints of their network policies.

- **A secure tunnelled TCP connection is the least-desirable option** for media transfer, but most likely to be supported with no network security changes. Overuse of proxies may impact other general use and video signalling and/or latency. Call stability will likely be impacted if the proxy is so busy transferring video that the signalling traffic is delayed or dropped.

**Recommended option**: For many networks, allowing NAT egress to UDP port 3478 on the relay server (network path 2, above) will provide low latency with little overhead. This should require only a minor, low-risk change to your network configuration.
Call Quality and Bandwidth

WebRTC video connections can be configured, per Waiting Area or Meeting Room, for a variety of resolutions and bandwidth caps. The default is **Standard Wide** resolution (640 x 360) at 30 fps.

In all cases, the specified quality level will degrade gracefully based on each participant's available CPU and network capacity. Video calls can be sustained with bandwidth as low as 300 Kbps per remote party, but with a reduced quality experience.

**Bandwidth per remote party in a call**

- **Minimum**: 384 Kbps
- **Recommended**: 768 Kbps
- **Optimal**: 1 Mbps and above

WebRTC Peer connections can use up to 4 Mbps under unrestricted conditions. If necessary, constraints can be configured to reduce this maximum.

**Quality target presets**

Quality is dynamically balanced in temporal (frames-per-second) and spatial (resolution) domains. This is reduced when device has insufficient power to encode or limited bandwidth

- **Ultra** (1080p, bandwidth per connection 6 Mbps)
- **High** (720p, bandwidth per connection 4 Mbps)
- **Standard** (480p, bandwidth per connection 2 Mbps)
- **(Default) Standard Wide** (360p, bandwidth per connection 2 Mbps)
- **Moderate** (360p, bandwidth per connection 1 Mbps)
- **Low** (240p, bandwidth per connection 0.5 Mbps)

**How does the peer-to-peer model impact bandwidth for multi-party calls?**

As Attend Anywhere is a peer-to-peer system, bandwidth is specified per remote party. Multiple parties in the call will increase the bandwidth required at each endpoint.

If the bandwidth is not available for a particular endpoint, the video to or from each party will degrade to fit within that endpoint's available bandwidth. As connections are established independently, this may only impact a particular party and possibly only in one direction.
Troubleshoot Network

The following network-related troubleshooting can assist with the diagnosis of call or connection issues.

Check WebRTC network readiness

The **Attend Anywhere WebRTC Network Readiness Test** evaluates how your network setup connects to the outside world, and whether your available bandwidth is sufficient to make video calls.

See *Testing WebRTC network readiness* on page 18 for details.

Resolve web proxy-based WebRTC connection issues

In some network environments, unusual web proxy configuration can result in the long polling connections used for real-time signalling to either close prematurely, or not be processed at all. This interferes with the successful operation of Attend Anywhere by not allowing messages about, and status of, calls to be conveyed from the application to its associated web pages in real time.

**Possible symptoms**

- Call setup does not complete (after confirming that media connections are possible with the network test)
- Video call starts as expected, but disconnects after approximately 10 seconds
- First connection always has no audio/video from other participants, but refreshing the call results in a good connection
- Call status does not get updated in the Attend Anywhere Management Console, on the **Quick View, Waiting Areas**, specific Waiting Area, and **Reports** pages

**Solution**

To allow WebRTC communication to work as intended, you may need to either reconfigure or bypass your web proxy.

To ensure that the web proxy bypass is effective, you must ensure that the network path to the server via NAT is also available. This will require coordination between network administration and desktop administration teams to ensure that the configuration is valid.
For device proxy bypass

Ensure that the site england.nhs.attendanywhere.com will not be requested via the web proxy, by updating system or user options for internet connections.

On Windows, Google Chrome shares the same settings as the Microsoft Edge browser.

For firewalls

Ensure that your firewall allows traffic to england.nhs.attendanywhere.com for port 443 TCP.

NHS England Attend Anywhere recommends using the symbolic name england.nhs.attendanywhere.com if supported in the firewall settings, as dynamic changes in hosting infrastructure may cause the IPs to be changed in future.

What if I cannot bypass the web proxy?

Investigate the configuration that is causing the real-time signalling to fail.

This could be due to a range things, but is likely to include the following:

- Timeout settings on data flowing in open connections
- Packet inspection that does not allow the request body to be empty
Equipment

Ensure that all users have the minimum requirements for using, from devices and operating systems, to web browsers, as well as additional equipment and data use. Find out about what peripherals are needed for the best user experience, as well as testing your devices and creating desktop shortcuts.
What do people need to make calls?

Make sure any equipment can make browser-based video calls.

- A web camera (built-in or USB)
- A microphone (usually built in to most laptop computers and external webcams)
- Speakers and headsets, if required (speakers are usually built into most laptop computers, but not necessarily into external webcams)
- (Recommended for clinicians) A second monitor (allows clinicians to display the video consultation on one monitor and patient information on the other)
<table>
<thead>
<tr>
<th>Everyone will also need</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A <strong>reliable connection to the internet</strong> <em>(if you can watch a video online, you can make a video call)</em></td>
</tr>
<tr>
<td>• A <strong>private, well-lit area</strong> where you will not be disturbed during the consultation</td>
</tr>
</tbody>
</table>
User requirements

Ensure that all users have the minimum requirements for using Attend Anywhere, from device and operating systems, to additional equipment and data use.

Hardware requirements

Device and operating system

When making calls with Attend Anywhere, user devices must meet the following requirements:

<table>
<thead>
<tr>
<th>Device type</th>
<th>Minimum requirement</th>
<th>Operating system*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows computer</strong></td>
<td>2GHz dual-core, i5 processor 3GB of RAM See also Additional equipment, below.</td>
<td>Microsoft Windows 7 or later</td>
</tr>
<tr>
<td><strong>Apple computer</strong> (iMac, Mac Pro, Mac Mini, MacBook, MacBook Air, or MacBook Pro)</td>
<td>Intel 2GHz dual-core, i5 processor 3GB of RAM See also Additional equipment, below.</td>
<td>(Using Chrome) MacOS version 10.11 or later (Using Safari) MacOS version 10.12 (Sierra) or later</td>
</tr>
<tr>
<td><strong>Android tablet or smartphone</strong></td>
<td>Less than two years old, with a front-facing camera</td>
<td>Android 5.1 or later</td>
</tr>
<tr>
<td><strong>Apple iPhone</strong></td>
<td>iPhone 5s or later</td>
<td>iOS 12.4 or later</td>
</tr>
<tr>
<td><strong>Apple iPad</strong></td>
<td>iPad Air or later, iPad (2017) or later, iPad Mini 2 or later, iPad Pro</td>
<td>13 or later</td>
</tr>
</tbody>
</table>

*Please note that use of "Beta", unofficial or non-genuine copies of the operating systems above may cause NHS England to not perform as expected.

WebRTC video calling in a Virtual Desktop (VDI) environment

WebRTC Calling can work well within Virtual Desktop Infrastructure (VDI) environments if appropriate vendor-supported configurations can be applied and the Thin Client hardware has sufficient capacity.
Browser Content Redirection modules are available for both Citrix and VMware Horizon to allow offloading elements of browser processing to the Thin Clients, while still maintaining centralised management of desktop and applications.

Because the client needs to be able to process and/or render video locally, capable clients must be deployed to the clinicians' locations. i5 processors, 4GB RAM and local GPU are recommended. More recently, higher-powered System on a Chip (SoC) units have been used.

As almost all VDI environments are different, contact us through your support channels so that we can arrange for the relevant information exchange and guidance on testing.

For information on contacting your local support representative, see the Troubleshooting & Support > Support > Support contacts section of the Resource Centre.

Additional equipment

Desktop and laptop computers

Speakers/headphones

Attend Anywhere's Call Screen uses the device's default audio output (such as its speakers, or headphone port/jack)

Plugging in a headset (which combines a microphone and headphones) can help reduce background noise, and prevent others from overhearing your conversation.

For conference room or group meetings, use a USB echo-cancelling microphone/speaker unit wherever possible. This will provide better sound for all participants.

For a range of example speaker units and headsets, see Peripherals on page 46.

Microphone

- On tablets, smartphones, and laptop PCs, Attend Anywhere's Call Screen uses the built-in microphone
- For PCs without a microphone, any currently-available USB microphone is suitable.

Note: Many USB web cameras also have built-in microphones. Depending on the level of ambient noise where users make video calls, this may prove sufficient.

- Microphones integrated into combined USB speaker/microphone devices
• A headset (combines headphones and microphone - includes earbud/microphone sets used with smartphones and tablets).

**Note:** A headset is especially useful where background noise may be a problem.

For a range of example speaker units and headsets, see *Peripherals* on page 46.
Web camera

- On tablets, smartphones, and laptop PCs, Attend Anywhere's Call Screen uses the built-in camera.
- For PCs without a camera, any currently available USB web camera is suitable.

For a range of example web cameras, see Peripherals on page 46.

- Where more than one participant will be in the same room during the video call, use a web camera with a wide-angle lens.

- Make sure that users have the most current software drivers installed for their web cameras.

Web browser requirements

Users require one of the following web browsers to use Attend Anywhere:

- Chrome
- Safari
- Edge

Attend Anywhere always recommends using the latest version of Chrome, Safari, or Edge for best video calling performance.
Bandwidth and data requirements

Download speed, upload speed, and latency

When making video calls with Attend Anywhere, make sure that users' internet connections meet the following requirements:

- **Minimum download speed:** 0.3 Megabits per second (Mbps) - provides lower-quality video
  
  **Recommended:** 1.1 Mbps or better

- **Minimum upload speed:** 0.15 Mbps - provides lower-quality video to other participants
  
  **Recommended:** 0.7 Mbps or better

- **Recommended latency:** Less than 150 milliseconds (ms)

Testing speed and latency

You can test a device's speed and latency at http://www.speedtest.net.

When the test completes, the results will look something like this:

![Speed test results](image)

Compare the results to the minimum and recommended values above.

A wired internet connection will provide best video quality, but you can also use a fixed-wireless or mobile (3.5/4G) data service.

How much data does a call use?

- Patients don't use any data while waiting for a clinician to join them.

- A 20 minute video consultation uses about 230 MB on a mobile device, and 450 MB on a PC.

- Data use is less on lower-speed internet connections, or on a less powerful computer, tablet, or smartphone. These factors can also reduce the overall quality of the call.

- Data use increases when there are more than two participants in the call.

**Smartphone & tablet users**
Attend Anywhere recommends connecting to a Wi-Fi network to avoid using the device's mobile data allowance.
Desktop shortcuts

Desktop and laptop computers

Shortcut types

- For Management Console users: Desktop shortcut to the Attend Anywhere Management Console (Windows and MacOS computers)
- For patients: Desktop shortcut to make a video call to a specific Waiting Area (Windows computers)

Attend Anywhere Management Console

Windows computers

Google Chrome shortcut

This method opens the specified page in Chrome, even if the user has a different browser set as the default. The shortcut also picks up the page's favicon as the art for the shortcut's icon.

This shortcut only works on the device for which it is created.

To create a desktop shortcut from the Chrome web browser

1. In the Google Chrome web browser, sign in to the Attend Anywhere Management Console, and open the page to which you want to direct people.
2. Click the menu button in the web browser's top right corner.
3. From the menu, select More tools > Create shortcut.
4. Enter a suitable name for the shortcut.
   Example: Attend Anywhere Waiting Areas
5. Do one of the following:
   - To have Chrome open the Management Console in its own window, select "Open as window".
   - To open the Management Console in a browser tab, clear the "Open as window" check-box.
6. Click Add.
Windows shortcut

This method opens the specified page in Chrome or Edge, even if the user has a different browser set as the default.

You can email a copy of this shortcut to other people for their use, as long as they have Chrome or Edge installed in the same location.

The following steps assume that the browser is installed in its default location.

To create a Windows shortcut

Windows desktop

1. Right-click the desktop, and from the menu, select **New > Shortcut**.
   The Create Shortcut wizard opens.

2. Click **Browse**.

3. In the **Browse for Files or Folders** dialog, navigate to the location of your browser's program file.
   For Chrome, this is typically `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`
   For Edge, this is typically `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`

4. Click **OK**.
   The wizard’s location field now contains the following:
   For Chrome, this is typically "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
   For Edge, this is typically "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"

5. Add the following URL to the end of the location field, after the double-quote mark:
   If wanting to create a link to the Waiting Area, you could use
   https://england.nhs.attendanywhere.com/waiting-area/view-all
   If wanting to create a link to the Organisational Units Area, you could use
   https://england.nhs.attendanywhere.com/entity-admin/view-all
   **Important**: Make sure that you insert a space between the double-quote mark, and the start of the URL.
To create a Windows shortcut

6. Click **Next**.

7. Enter a suitable name for the shortcut.
   - Example: *Attend Anywhere Waiting Areas*
   - Example: *Attend Anywhere Organisational Units*

8. Click **Finish**.

The new shortcut icon is added to the desktop. It will use the Google Chrome or Microsoft Edge icon, and have the name you chose in step 7.

**Note:** After you create the shortcut, you can edit the icon, the URL, and the location of Chrome or Edge that it uses. To do so, right-click the shortcut, and from the menu, select **Properties**. Make the desired changes in the **Shortcut** tab, and then click **OK**.

(Optional) To customise the desktop shortcut's icon

**Windows desktop**

1. Right-click the desktop shortcut, and select **Properties**.
   
The shortcut's property sheet opens.

2. In the **Shortcut** tab, click **Change Icon**.
   
The **Change Icon** dialog opens.

3. In the **Change Icon** dialog, click **Browse**.

4. Navigate to the location of the icon that you want to use, and click **Open**.

5. In the **Change Icon** dialog, click **OK**.

6. In the property sheet, click **OK**.
MacOS computers

To create a MacOS Desktop/Dock shortcut

Attend Anywhere Management Console

1. In either the Google Chrome or Safari web browser, sign in to the Attend Anywhere Management Console, and navigate to the page you want to open on launch.
2. In the browser window, click once in the address bar to highlight the URL.
3. With the URL highlighted, click and drag the address from the browser to either the Desktop, or the right-hand side of the Dock.

   Note: On the Desktop, this creates a shortcut with a Safari icon, even if Chrome is the default browser.

   Optional: To customise the shortcut's icon, find your preferred image, open it in Preview, and copy it. Then continue from the next step.

4. Open the shortcut's context menu, and select Get Info.
5. Click the icon image at the top-left of the Get Info window.
6. Type ⌘-V to paste the copied image onto the icon.
7. Close the Get Info window.

Call Screen to a specific Waiting Area

Windows computers

The computer on which the shortcut is to be used must have Google Chrome installed.

To create a Windows shortcut

Windows desktop

1. Right-click the desktop, and from the menu, select New > Shortcut.

   The Create Shortcut wizard opens.

2. Click Browse.

3. In the Browse for Files or Folders dialog, navigate to the location of Chrome's program file (chrome.exe)

   This is typically C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
To create a Windows shortcut

4. Click **OK**.
   
The wizard's location field now contains the following:
   
   "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"

5. Add the direct-access URL to the end of the location field, after the double-quote mark:
   
   **Important**: Make sure that you insert a space between the double-quote mark, and the start of the URL.

6. Click **Next**.

7. Enter a suitable name for the shortcut.
   
   Example: **Acme Health Waiting Area (Attend Anywhere)**

8. Click **Finish**.
   
The new shortcut icon is added to the desktop. It will use the Google Chrome icon, and have the name you chose in step 7.

**Note**: After you create the shortcut, you can edit the icon, the URL, and the location of Chrome that it uses. To do so, right-click the shortcut, and from the menu, select **Properties**. Make the desired changes in the **Shortcut** tab, and then click **OK**.
Testing video calling devices

Desktop/laptop computers  Android tablets/smartphones

The microphone, camera, and connection tests are automated while you will be prompted to perform the speaker test manually.

The Video call setup test checks the device’s microphone, camera, internet connection, and speakers are working as expected. The microphone, camera, and connection tests are automated while you will be prompted to perform the speaker test manually.

Users can run this test from the Attend Anywhere Management Console, or from any web page that displays the Test Call link:

https://england.nhs.attendanywhere.com/ce/?testonly=true

or the Test call button (legacy option):

If all four stages of the test are successful, then users should be able to make a successful call with Attend Anywhere.

If the test results indicate issues with the device’s current setup, see Troubleshooting on page 55.
Audiovisual tips

Based on the image and video you are receiving from others, you may assume that the quality of the video call is good. However, people on the other end of the call may be receiving bad quality video and/or sound from your end.

⚠️ **Remember:** If you’re sending poor quality video, you may not realise it!

The following tips will help you optimise the experience for others in the video call.

**Achieve a natural face-to-face interaction**

Position the camera at eye level where feasible. This makes it easier to maintain eye contact and a natural, human interaction.

Ensure that you, and anyone else in the room with you, are within view of the camera. Try and keep the camera centred on the person talking.

Remember that the other participants can see you. Act like you would if they were in the room with you.

**Ensure the best possible experience for other participants**

Good quality laptops or mobile devices can provide a decent experience however, these are typically designed for individuals (a maximum of two people).

When using audio devices built-in to laptops, mobile devices, and computer monitors/displays, bear in mind that:

- Microphones are directional. You need to be positioned directly in-front of the screen for them to work efficiently.
- Cameras of (some) monitors and laptops have a narrow field of view.
- The quality of built-in cameras can be poor and not transmit good quality video, especially in poor light.
- Speakers can be poor quality and not designed for rich audio communication or whole rooms.

**Recommendations**

Use an external USB camera/mic or a microphone/speaker. This will increase the overall quality transmitted to other participants.

Use a headset/microphone in a noisy environment. This will also increase the quality of the audio transmitted, compared to many in-built microphones.
Present yourself in the best light

Cameras perform better with optimal lighting, however 'normal' room lighting is typically sufficient. Some things to consider:

- Avoid pointing the camera into a bright light or a window (this can cause the aperture of the camera to close and your image will appear dark to the other people in the call).
- Avoid sitting directly beneath a light source if possible (this can create shadows beneath your eyes or and chin). Side-lighting works well.
- Bear in mind that the in-built camera of (some) monitors, or lower end web cameras do not perform well in low light conditions. This can adversely affect the frame rate and picture quality transmitted.
Peripherals

Desktop and laptop computers

Disclaimer
The presence of any particular product on this page should not be considered as an endorsement of that product by Attend Anywhere. The items described here are provided solely as a guide to the current range of suitable equipment to successfully hold video calls; there are many alternatives to those listed. Always evaluate products for suitability in your own environment before purchasing.

Cameras

For personal or small group use

Auto-focus USB camera and microphone for small groups (one to six people). (£50)
HD 720p; noise reduction

You can select this device as both camera and microphone.

Auto-focus USB camera and microphone for small groups (one to six people). (£95)
HD 1080p or HD 720p

You can select this device as both camera and microphone.
Premium auto-focus, USB, pan/tilt/zoom, video conferencing camera for **ten to fifteen people** (£749).

Full HD 1080p; superior optics; pan, tilt, and zoom controls

⚠️ **Important:** Using this camera will require a separate microphone, or microphone/speaker (or speakerphone) combination.

---

**Microphones & Speakers**

**Microphone/speaker combinations (speakerphones)**

USB speakerphone for **small groups (two to six people)** sitting in front of the speaker. (£185)

http://www.clearone.com/chat-50

If you already have a camera, the Chat 50 is good for small groups sitting up to 2.5 metres away from, and in front of, the speaker. This model's microphone's only has a 120 degree arc to the front of the unit, which will not clearly pick up people sitting to the side of, or behind, the speaker.

Make sure that you select the Chat 50 as both your microphone and speaker to ensure the best quality audio.

---

USB speakerphone for **larger groups (six to eight people)** sitting around the speaker. (£410)

http://www.clearone.com/chat%C2%AE-150-chatattach%C2%AE-150

If you already have a camera, the Chat 150 is good for slightly larger groups sitting up to 2.5 metres away from the speaker. The microphone's 360 degree arc ensures that people can be heard regardless of their position around the unit.

Make sure that you select the Chat 150 as both your microphone and speaker to ensure the best quality audio.
USB speakerphone array for larger groups (ten to fifteen people) sitting around a large conference table. (approx. £770)

http://www.clearone.com/chat%C2%AE-150-chatattach%C2%AE-150

The ChatAttach 150 is two Chat 150 speakerphones daisy-chained together for wider reach.

Make sure that you select the Chat 150 as both your microphone and speaker to ensure the best quality audio.

Headsets

Headsets typically provide an better desktop alternative to built-in microphones and speakers. They provide increased privacy for the call, and in open-plan environments, reduce both distractions for others in the area, and ambient feedback heard by call participants.

If you already use headsets that connect to a computer in your existing work environment, you should be able to continue using them, regardless of the video calling technology adopted.

Microphone noise-cancelling or noise-reduction features can be very useful, especially in busy surroundings.

Wireless headsets can help to reduce cable clutter, although they are more expensive - make sure that they have a recharging cradle.

Microsoft's LifeChat range of USB headsets provide good quality audio, and range between £20 and £25.

https://www.microsoft.com/accessories/en-gb/headsets

Logitech make a range of quality headsets that vary in price from £15 for simple USB models to £90 for high-end wireless/Bluetooth sets.

https://www.logitech.com/en-gb/headsets
Camera/microphone/speaker all-in-one units

Powered, USB, pan/tilt/zoom ‘stalk’ camera with in-built speaker and microphone for **four to six people** sitting in-front of the device. (£219)


Great all-in-one pan, tilt zoom camera, noise-cancelling microphone and speaker for small groups. Requires power.

USB camera and speakerphone bundle for **medium size conference rooms** (£1099)

Monitors

**Video consultations**

Attend Anywhere strongly recommends that clinicians have two monitors when conducting video consultations. This allows them to display the patient and other call participants on one monitor, while using the other to display notes and data.

Monitors range considerably in size, price, and quality.

When using a second monitor, it's a good idea to use the better monitor to display video.

**Alternatives as a second monitor**

If you have an Android or iOS tablet/smartphone, you can use the Splashtop Wired XDisplay app to turn that device into a second monitor for your Windows or MacOS computer. This is potentially a great option for providers who use laptop computers and don’t necessarily have the desk space for a permanent second monitor.

- Splashtop Wired XDisplay: [https://www.splashtop.com/wiredxdisplay](https://www.splashtop.com/wiredxdisplay)

If you have an iOS device (iPhone or iPad running iOS7 or later) you can alternatively use the Duet Display app (approx £10) to connect it to your Windows or MacOS computer.

- Duet display: [https://www.duetdisplay.com/](https://www.duetdisplay.com/)
Group meetings

When holding video meetings with medium to large groups of people sharing a conference room, it's a good idea to use a larger monitor (27" to 30" widescreen works well) or digital projector to display the video participants.

A good quality monitor costs between £125 and £300, while projectors typically range in price between £200 and £1000. Projectors also require a screen or suitable wall space on which to display the image.

Types of video port

Make sure that you have compatible ports on the PC and the monitor/TV that you intend to use, as well as the correct cables of suitable length for the room in which you set up the conference.
Set up a new organisation in Attend Anywhere

Set up a new organisation in Attend Anywhere by using the following broad stages as a guide.

Note: Many of these tasks are performed by the local project team in your region, on request.
New provider request

Email nhsenglandsupport@attendanywhere.com to determine whether you are eligible to participate in NHS England Attend Anywhere’s video consultation support offer.

If you are eligible, the national video team will provide you with a set up form for completion.

Set up process

Send completed set up form to nhsenglandsupport@attendanywhere.com to initiate deployment of Attend Anywhere to your organisation.

Begin setup tasks

Provision a new Waiting Area and Organisational Unit

NHS England Attend Anywhere send the organisation a link to provision a new Waiting Area (and associated Organisational Unit).

Schedule an orientation session

Arrange a time to meet via video call for an orientation session with the organisation staff (for example, implementation project managers/clinicians/Technical Leads).

Schedule training and design sessions

Schedule ‘train the trainer’ sessions

NHS England Attend Anywhere provides training and materials to support the adoption of video consulting.

Note: NHS England Attend Anywhere is not resourced to provide end-user training or support.

Train-the-trainer sessions cover the following areas:

- How to provide technical support. (Audience: IT support teams.)
- Troubleshooting (Audience: IT support teams and departmental ‘super-users’.)
- Administering the Attend Anywhere Management Console (Audience: Local Administrators of the Attend Anywhere Management Console, such as departmental administrators.)
- Attend Anywhere resources to support adoption (Audience: Local Adoption Leads, Educators, and departmental ‘super-users’.)

Note: NHS England Attend Anywhere is not resourced to provide end-user training or support.
Set up a new organisation in Attend Anywhere

Schedule a video call access design workshop for the clinic

Arrange a service-specific video call access design workshop with a video consulting subject matter expert (SME).

**Note:** It is important that key people are available for this session. For example, you may include and executive leads, (patient representatives, if appropriate), clinicians, clinic staff, finance, communications, and technical leads.

**Workshop objectives**

- Discuss the objectives of video call access throughout the organisation.
- Fill any knowledge gaps regarding the Attend Anywhere offering, including the video consulting resources available, the Attend Anywhere Management Console and the video technology used.
- Discuss the end-to-end video call access workflow and systems integration design, in terms of the initial services that are to be enabled and the longer term vision, if applicable.
- Agree on initial configurations of the Attend Anywhere Management Console.
- Discuss key project steps and next actions.

**Confirm primary contacts**

Primary Adoption and Support contacts provide the communications link between the organisation and NHS England Attend Anywhere.

Primary contacts can:

- Submit service requests and third-level support requests to NHS England Attend Anywhere
- Have access to regular training sessions
- Receive Attend Anywhere information bulletins
Add the Waiting Area links

Prerequisite:
The approach for adding the Start video call button to your website has been decided. (Either a single Waiting Area, or all Waiting Areas under a single Organisational Unit.)

1. To add the Waiting Area link to the web page, do one of the following:
   - (Recommended) From the About your Waiting Area email, copy the link or button script
   - From the Attend Anywhere Management Console, copy the link or applicable button script

2. Place the link or button on the clinic's web page and test to ensure everything works.

If required, you can send the link or button script to the Local IT administrators or webmaster for placement.

How do I customise Waiting Areas?
After the Waiting Area is set up in the Attend Anywhere Management Console, you can customise the Waiting Area's logo, patient messages, hours of availability, and more...

From the specific Waiting Area's page, click the configure button.

All customisable actions are performed from here.

- General information
- Support Contact for Staff
- Information for Callers
- Logo and pause screen images
- Video call access hours (Providers)
- Waiting Area Links
- Before calls (Patient Details)
- Before calls (Please Read!)
- During calls
- After calls
Troubleshooting

From network setup to video calling, Attend Anywhere provides various materials, resources, tools — as well as training for IT departments — for you to diagnose and rectify common problems and technical difficulties that may occur.
Troubleshoot Network

The following network-related troubleshooting can assist with the diagnosis of call or connection issues.

Check WebRTC network readiness

The Attend Anywhere WebRTC Network Readiness Test evaluates how your network setup connects to the outside world, and whether your available bandwidth is sufficient to make video calls.

See Testing WebRTC network readiness on page 18 for details.

Resolve web proxy-based webRTC connection issues

In some network environments, unusual web proxy configuration can result in the long polling connections used for real-time signalling to either close prematurely, or not be processed at all. This interferes with the successful operation of Attend Anywhere by not allowing messages about, and status of, calls to be conveyed from the application to its associated web pages in real time.

Possible symptoms

- Call setup does not complete (after confirming that media connections are possible with the network test)
- Video call starts as expected, but disconnects after approximately 10 seconds
- First connection always has no audio/video from other participants, but refreshing the call results in a good connection
- Call status does not get updated in the Attend Anywhere Management Console, on the Quick View, Waiting Areas, specific Waiting Area, and Reports pages

Solution

To allow WebRTC communication to work as intended, you may need to either reconfigure or bypass your web proxy.

To ensure that the web proxy bypass is effective, you must ensure that the network path to the server via NAT is also available. This will require coordination between network administration and desktop administration teams to ensure that the configuration is valid.
For device proxy bypass

Ensure that the site england.nhs.attendanywhere.com will not be requested via the web proxy, by updating system or user options for internet connections.

On Windows, Google Chrome shares the same settings as the Microsoft Edge browser.

For firewalls

Ensure that your firewall allows traffic to england.nhs.attendanywhere.com for port 443 TCP.

NHS England Attend Anywhere recommends using the symbolic name england.nhs.attendanywhere.com if supported in the firewall settings, as dynamic changes in hosting infrastructure may cause the IPs to be changed in future.

What if I cannot bypass the web proxy?

Investigate the configuration that is causing the real-time signalling to fail.

This could be due to a range things, but is likely to include the following:

- Timeout settings on data flowing in open connections
- Packet inspection that does not allow the request body to be empty
Troubleshoot video calling

To make a successful video call, you need an internet connection that receives and transmits data quickly enough to allow for an acceptable level of video quality between you and the other participants in the call. This topic describes the most likely problems, and suggests what should be checked, if users are having issues during a video call.

These troubleshooting suggestions are also available as a single-page, downloadable PDF.

Download the troubleshooting poster from https://england.nhs.attendanywhere.com/usertroubleshooting

Note: When patients or Management Console users make a video call, or use the Test my equipment button (available from each Waiting Area's page in the Attend Anywhere Management Console), Attend Anywhere runs a short series of tests to make sure that they have what they need to make a successful call.

Should any of these tests fail, patients will be taken to their own troubleshooting documentation.

General issues

Minimum requirements for my computer, tablet, or smartphone to make a video call

- **Windows PC** with an i5 processor and 3GB of RAM (Windows 7 or later)
- **Apple Mac** with an i5 processor and 3GB of RAM:
  - (Using Chrome) MacOS version 10.11 or later
  - (Using Safari) MacOS version 10.12 (Sierra) or later
- **Android-based smartphone or tablet** (Android 5.1 or later)
- **iPhone** (iOS 12.4 or later)
- **iPad** (iOS 12.4 or later, 13 or later)

More information:

- **Hardware requirements** on page 32
**Compatible web browser**

Attend Anywhere requires one of the following web browsers:

- **Google Chrome** version 80 or later
- **Apple Safari** version 12.4 or later
- **Microsoft Edge** version 83 or later

**Connection/stability issues**

**My connection speed test failed**

To make a successful video call, you need an internet connection that receives and transmits data quickly enough to allow for an acceptable level of video quality between you and the other participants in the call.

*How can I improve the quality of my existing connection for video calling?*

- *(Wireless home or office network)* Move closer to - or at least in line-of-sight of - the Wi-Fi base station.
- *(Mobile internet connection)* Move to an area with better reception.
- Make sure that no one else in your home is streaming video or downloading large files from the same connection. This substantially reduces the bandwidth available to make a good quality video call.
- Avoid having more than one active connection to the internet (for example, a wired and a wireless connection running at the same time).
- Make sure that you have not used all of your internet plan’s data allocation for the month. This often results in your internet provider reducing the speed of your service.
- When you first switch on your computer after not using it for a while, it may automatically download updates. This will reduce available bandwidth. Either wait for the updates to finish, or postpone the downloads until after you have made your video call.

**My video and audio are very 'choppy' during the call**

*Are there too many sites/participants in the call?*

NHS England Attend Anywhere recommends you have a maximum of **four to six** separate sites in a call. (A site is the video stream to and from a single device.) Shared screens do not count as a site.

**Examples**
• Four separate participants, plus one shared screen in a call, counts as *four* sites.
• One location with five people sharing a call screen, plus two separate participants, plus two shared screens, counts as *three* sites

*(Desktop computers) Do you have other software/apps running while you're making the call?*

If other apps are open on your computer while you are making a call, they may be using a significant percentage of your computer's available processing power (CPU). This will affect the quality of your call experience.

When making a video call, make sure that CPU-heavy apps are either minimised, or closed.

**Speaker issues (desktop/laptop computers)**

I can't hear any sound from my speakers/headset

*Are your speakers separate to your device? (Also applies to earphones/headphones)*

• *(Speakers only)* If your speakers are powered separately, make sure that the power adapter is plugged in and switched on.
• Make sure that the speakers are correctly plugged into the relevant USB port or audio output jack.
• If your speakers or headphones have a separate volume control, make sure that it is set to an audible level.

*Have you checked the device's volume?*

• Make sure that the audio volume on your device is not on mute.
• Make sure that the device's volume is turned up to an audible level.
• Check if your audio is working by playing something else on your device. If you can't hear anything, make sure that the speakers are not disabled.

Microphone issues

Desktop/laptop computers

During setup, I can't hear anything when I hold the microphone test button and speak

Is your microphone separate to your device? (Can also apply to earphones or a headset)

• Is it plugged in?
• If it is plugged in, is it plugged in firmly?

⚠️ If your microphone uses a USB plug, unplug it, and plug it in again. This forces your computer to try and detect it again.

• Can the computer detect the microphone?
  Check the computer's audio settings.
• Can the browser detect the microphone?
Click the **camera** icon in the Call Screen's address bar, and make sure that the correct microphone is selected.

**Have you checked the microphone settings?**

- Check that the volume on your device, headset microphone, or external camera is turned up and not muted.
  
  **Note:** On smartphones, the microphone will always be active, as it is also accessed by the telephone.

- Check that the microphone is enabled in your device’s Sound or Audio settings.

- Make sure that the Call Screen is using the correct microphone.
  
  *(If the microphone is external)* Is the microphone plugged in securely?

- Is the microphone muted?
  
  Check the **Mute Mic** control in the Call Screen, the audio controls on the computer, tablet, or smartphone, and (if you're using an external microphone) the mute button on the microphone or headset itself.

- Is other software using the microphone at the same time? *(Example: *Skype* also running.)*
  
  If another program (such as *Skype*) is trying to use the microphone as well, close that program, and try again. If they still can't use the microphone, they may wish to restart the computer and then try again.

**Mobile devices**

*(iPhones and iPads)* People can't hear me

First, try refreshing the call. If this does not fix the issue, restart the Safari app by swiping up or double-clicking the home button to view all open apps, and then close the Safari app. Restart Safari, and re-join the call.

**My browser cannot access the microphone**

Your tablet or smartphone's microphone settings may have been set to prevent the browser or apps from accessing the microphone. This may have happened when a website or web app asked for access to your device's microphone, and you said no.
To re-enable microphone access, do the following:

**iPhone or iPad**

1. Open the **Settings** app.
2. Swipe to the **Safari** entry, and tap it.
3. In the **Safari** section, swipe down to the **Microphone** entry (located in the **Settings for websites** group) and tap it.
4. If **Microphone access on all websites** is set to **Deny**, tap either **Allow** or **Ask**.
   (As a general rule, it's a good idea to set this option to **Ask**, to prevent websites from unexpectedly accessing your microphone.)

   ![Microphone access settings](image)

5. Tap < **Safari** to return to the previous screen.
6. (iPhone only) Tap < **Settings** to return to the main **Settings** screen.
7. Close the **Settings** app.

You may need to refresh the call screen to regain audio.

**Android smartphone or tablet**

1. Open the **Settings** app.
2. Tap the **Apps** section.
3. Swipe to the **Chrome** entry, and tap it.
4. In the **Chrome** section, swipe down to **Permissions**, and tap it.
5. In the **App permissions** page, make sure that the **Microphone** option is selected.
6. Close the **Settings** app.

You may need to refresh the call screen to regain audio.

---

**Video issues**

**Desktop/laptop computers**

I can't see myself in the video test window

Make sure that the Call Screen is using the correct camera.

*Is your web camera a separate peripheral?*

- Is it plugged in?
- If it is plugged in, is it plugged in **firmly**?

  **Tip:** Unplug the camera, and plug it in again. This forces your computer to try and detect it again.

- You may need to update your web camera's software. Check the web camera manufacturer's website for updates to supporting software or drivers.

*Is your camera built in to the device (such as on laptop PCs, tablets, and smartphones)?
Can other people see anything from your side?

- **No:** Make sure that your camera has not been disabled in the device's settings.
- **Yes:** Make sure that your device is using its front camera (the one on the same side as the screen).

Is the browser accessing the correct camera?

- Click the camera icon in the Call Screen's address bar, and make sure that the correct camera is selected.

### Is other software using the camera?

Example: Skype is also in use, and already has access to the camera.

- If so, close the other software, and try again. If you still can't see yourself in the test window, you may have to restart your device before trying again.

### Do the firewall settings allow video streams through?

If necessary, reconfigure the firewall to allow video streams.

I think I'm using the wrong camera

- If the video is showing the room in front of you, and not you, the device's front-facing camera may have been selected by default.
- Make sure that the Call Screen is using the correct camera.
  
  **Tip:** If you have an external USB web camera, it may provide better quality video than a built-in one.

My image in the test/call is very dark

Bright light behind you will cause the camera to darken. If possible, have the light to one side, or in front of you, behind the camera. This will allow the person at the other end to see you better.

- Make sure that there are no bright lights or windows that the camera can see.
  
  Remember that web cameras with a wide field-of-view may also see light sources your left and right.

I see a black rectangle in the Call Screen where another participant should be

First, make sure that they are using the latest version of the Google Chrome, Apple Safari, or Microsoft Edge web browser.
If they are, and the problem persists, it is possible that the computer's firewall may be blocking the incoming video signal. Check the firewall settings, and make sure that it allows communications from the web browser.

For instructions on how to do this, consult the computer's help documentation.

I see the 'may not be able to see all participants' message in the Call Screen, but refreshing the call doesn't fix the problem

First, make sure that they are using the latest version of the Google Chrome, Apple Safari, or Microsoft Edge web browser.

If they are, and the problem persists, it is possible that the computer's firewall may be blocking the incoming video signal. Check the firewall settings, and make sure that it allows communications from the web browser.

For instructions on how to do this, consult the computer's help documentation.

Mobile devices

My browser cannot access the camera

Your tablet or smartphone's camera settings may have been set to prevent the browser or apps from accessing the camera. This may have happened when a website or web app asked for access to your device's camera, and you said no.

To re-enable camera access, do the following:

**iPhone or iPad**

1. Open the **Settings** app.
2. Swipe to the **Safari** entry, and tap it.
3. In the **Safari** section, swipe down to the **Camera** entry (located in the **Settings for websites** group) and tap it.
4. If **Camera access on all websites** is set to **Deny**, tap either **Allow** or **Ask**.
   
   (As a general rule, it's a good idea to set this option to **Ask**, to prevent websites from unexpectedly accessing your camera.)
5. Tap <Safari> to return to the previous screen.
6. (iPhone only) Tap <Settings> to return to the main Settings screen.
7. Close the Settings app.

You may need to refresh the call screen to regain camera access.

**Android smartphone or tablet**

1. Open the Settings app.
2. Tap the Apps section.
3. Swipe to the Chrome entry, and tap it.
4. In the Chrome section, swipe down to Permissions, and tap it.
5. In the App permissions page, make sure that the Camera option is selected.

6. Close the Settings app.

You may need to refresh the call screen to regain camera access.
Video calls and call quality

The actual amount of bandwidth and data used during a video call depends upon factors such as the resolution and quality of the user's web camera, and the quality of their internet service.

Each link between two participants in a video call is a connection. Each connection uses some of the available internet bandwidth and data allocation, as each participant sends and receives video and audio.

If the connections try to use more of these resources than the device can easily provide, the quality of the call experience may be affected.

Each new participant in a video call creates an additional connection for each participant:

Upload speed determines the overall quality of the video and audio that people send to other participants. As most internet plans provide slower upload speeds than download speeds, this is the limiting factor in overall call quality for most people.

For most people, a two-participant video call provides the best experience, even using modest internet connections.
Create a diagnostic report for connection issues

Introduction

On rare occasions, a video call will appear to connect successfully, but the participants in the call cannot see or hear each other.

The reasons why this problem arises are often not simple; to help the Attend Anywhere support team diagnose the cause of the problem, they may need additional diagnostic information from the Chrome or Edge web browser on the computer from which the problems occur.

Use the following steps to create this diagnostic information, and send it to Attend Anywhere support.

⚠️ Before you begin

Make sure that you **DO NOT end the call or close the Call Screen before you proceed.**

After you complete Task A below, you can end the call.

Instructions

Complete all three of the following tasks:

Task A: Create a logfile

1. In the Call Screen, right-click anywhere on the video image; from the displayed menu, select **Inspect element.**

   ![Inspect element](image)

   The browser's **Developer Tools** window opens.
2. From the window’s menu bar, click Console.

3. Right-click anywhere on the console page and from the displayed menu, select **Save as**.

4. From the **Save As** dialog, select the location to which you want to save the logfile.

5. Accept the default name for the file, and click **Save**.

6. Proceed to **Task B**.
Task B: Record your IP and if relevant, IPV6 address

1. In the Chrome or Edge web browser, open a new window or tab.
2. In the address bar, type `whatsmyip.net` and press the Enter key.
3. The What's My IP website opens, displaying your current IP address, and (if relevant) your current IPV6 address.

   ![IP address example]

4. Make a note of both the IP address, and the IPV6 address.
5. Proceed to Task C.

Task C: Email the file and information to Attend Anywhere

1. Open your email software, and create a new message.
2. In the To field, enter `support@attendanywhere.com`
3. In the Subject field, enter `Attend Anywhere Connection Diagnostics`
4. In the Message area, enter the IP address information you gathered in Task B.
5. Attach the file you created in Task A to the message.
6. Click Send.
Resolve web proxy-based webRTC connection issues

In some network environments, unusual web proxy configuration can result in the long polling connections used for real-time signalling to either close prematurely, or not be processed at all. This interferes with the successful operation of Attend Anywhere by not allowing messages about, and status of, calls to be conveyed from the application to its associated web pages in real time.

Possible symptoms

- Call setup does not complete (after confirming that media connections are possible with the network test)
- Video call starts as expected, but disconnects after approximately 10 seconds
- First connection always has no audio/video from other participants, but refreshing the call results in a good connection
- Call status does not get updated in the Attend Anywhere Management Console, on the Quick View, Waiting Areas, specific Waiting Area, and Reports pages

Solution

To allow WebRTC communication to work as intended, you may need to either reconfigure or bypass your web proxy.

To ensure that the web proxy bypass is effective, you must ensure that the network path to the server via NAT is also available. This will require coordination between network administration and desktop administration teams to ensure that the configuration is valid.
For device proxy bypass

Ensure that the site england.nhs.attendanywhere.com will not be requested via the web proxy, by updating system or user options for internet connections.

On Windows, Google Chrome shares the same settings as the Microsoft Edge browser.

For firewalls

Ensure that your firewall allows traffic to england.nhs.attendanywhere.com for port 443 TCP.

NHS England Attend Anywhere recommends using the symbolic name england.nhs.attendanywhere.com if supported in the firewall settings, as dynamic changes in hosting infrastructure may cause the IPs to be changed in future.

What if I cannot bypass the web proxy?

Investigate the configuration that is causing the real-time signalling to fail.

This could be due to a range things, but is likely to include the following:

- Timeout settings on data flowing in open connections
- Packet inspection that does not allow the request body to be empty
Troubleshoot screen sharing

Desktop and laptop computers

In many cases, the Call Screen will be able to identify any problems and either resolve them automatically, or walk you through the process of fixing them. However, should you need to take further action, consult the following troubleshooting issues.

Issues - General

My Call Screen doesn't have a Share Screen button

The screen sharing feature is only available to participants on desktop and laptop PCs. If you are using a mobile device (smartphone or tablet) to make a video call, you cannot share your screen with other participants. You can, however, view other participants' shared screens.
Issues - Apple Safari browser

My screen sharing permissions are denied

This may have happened when a website or web app asked for access to Attend Anywhere's screen sharing function, and you said no. This changed the screen sharing preference for Attend Anywhere from **Ask** to **Deny**. To allow screen sharing on the Safari browser, do the following:

1. In the Safari app on your Mac, choose **Safari > Preferences**.
2. Click **Websites**.
   The **Websites** pane of Safari preferences opens.
3. Click **Screen Sharing**.
4. Locate the **Attend Anywhere** website and change **Deny** to **Ask**.

Issues - Google Chrome browser extension

⚠️ For **Google Chrome** browsers that are **older than** version 74, the Call Screen uses a web browser extension to provide screen sharing features during video calls. Occasionally, problems may arise that are a result of issues with this extension.

I clicked the Share Screen button, but nothing happened
One of the following may be true; try to resolve the issue in the following order:

**Screen Sharing extension is installed, but disabled**

**Solution: Enable the Screen Sharing extension**

1. Open the Extensions page.
   a. In Google Chrome's address bar, type `chrome://extensions`
   b. Press Enter.
      The Extension page opens.
2. Scroll down the page and look for an item called **Screen sharing for Video Call**.

![Screen sharing for Video Call](image)

3. Make sure that the **Enabled** slider is selected.
4. Close the browser extension tab and return to the Call Screen.
5. Click the **Share Screen** button again.

**Screen Sharing extension is installed, but out of date**

**Solution: Update the Screen Sharing extension**

The Call Screen should automatically update the extension whenever an updated version is released. However, if this doesn't occur, and you see an 'extension out of date' message, then you can update the extension manually:

1. Open the Extensions page.
   a. In Google Chrome's address bar, type `chrome://extensions`
   b. Press Enter.
      The Extension page opens.
Troubleshooting

Solution: Update the Screen Sharing extension

2. In the Extensions page, select the Developer mode slider and then click Update.
3. Close the page.

I installed the Screen Sharing extension, but it didn't appear to install correctly

Solution: Repeat the installation

The simplest solution to this problem is to try installing the extension again: click the Call Screen's Share Screen button and repeat the installation steps.

If this doesn't work, you may wish to try one or more of the following:

- Click the Call Screen's Refresh button, rejoin the call, and click Share Screen
- Leave the call, close and restart your web browser, then rejoin the call, and click Share Screen
- (If neither of the above work) Leave the call, restart your PC, and then rejoin the call, and click Share Screen

If none of these are successful, talk to your IT support team.

If for some reason you cannot click the Refresh button, or the page has frozen, press Ctrl+R instead (On Mac PCs, this is Cmd+R)

The Call Screen tells me that the Screen sharing extension is out of date

Solution: Manually update your copy of the Screen Sharing extension

The Call Screen should automatically update the extension whenever an updated version is released. However, if this doesn't occur, and you see an 'extension out of date' message, then you can update the extension manually:

1. Open the Extensions page.
Solution: Manually update your copy of the Screen Sharing extension

1. In Google Chrome's address bar, type `chrome://extensions` and press Enter.

2. The Extension page opens.

3. In the Extensions page, select the Developer mode check box and then click Update.

4. Close the page.

The Call Screen asked me to Refresh the call

The Screen Sharing extension is installed and enabled, but not working.

Solution: Refresh the Call Screen

If the Call Screen cannot determine why screen sharing is not working, it will prompt you to refresh the page.

Call Screen

1. Click the Refresh button.

2. Wait for the Call Screen to reload.

3. Click Share Screen again.

If for some reason you cannot click the Refresh button, or the page has frozen, press Ctrl+R instead (On Mac PCs, this is Cmd+R)

I'm making a call from a private browser window, and Screen Sharing doesn't work

Solution: Configure Screen Sharing to work in Incognito mode

By default, Google Chrome does not allow extensions to work when they are run in a private window. However, you can configure extensions to work in private windows.
Solution: Configure Screen Sharing to work in Incognito mode

A private browser window is called an **Incognito** window in Chrome.

1. Open the **Extensions** page.
   a. In Google Chrome’s address bar, type `chrome://extensions` and press **Enter**. The Chrome Extension page opens.

2. Scroll down the page and look for an item called **Screen sharing for Video Call**.

3. Click **Details**. The details panel opens.

4. Scroll down the **Allow in incognito** section.

5. Make sure that the **Allow in incognito** check box is selected.

6. Close the browser extension tab and return to the Call Screen.

7. Click the **Share Screen** button again.
Index

bandwidth 26, 68
call quality 68
Call Screen
  screen sharing 74
camera 64
Citrix 32
connection 59, 69
connection issues See troubleshooting
connection speed 36, 59
data use 36
desktop shortcut 38
devices 58
diagnostics 69
equipment 46
Google Chrome 18, 35, 59, See also web browser
headset 48
log file 69
logfile 69
Management Console 38
microphone 47, 49
microphone test 61
Microsoft Edge 18, 35, 59
minimum 32
monitor 49
network 15, 18, 21, 23, 26-27, 56
network readiness 22, 27, 56
peripherals 46
port access 21
relay server 21, 23
requirements 32
  internet 36
  web browser 35
Safari 18, 35, 59
screen sharing 74
  extension 76-78
signalling access 21
speaker test 60
speakers 47, 49
specifications 32
testing 27, 56
Thin Client 32
training 52
troubleshooting 27, 56, 72
  connection issues 69
  network 27, 56
  screen sharing 74
  video calling 58
  web proxy 27, 56, 72
TURN server 21, 23
VDI 32
video test 64
virtual desktop 32
VMware 32
VMware Horizon 32
web browser 35, 59
web camera 46, 49
web proxy 27, 56, 72
WebRTC 15, 18, 22, 27, 56, 72