MHFA England Online Learning Hub – system requirements and security

Contents

MHFA England

System requirements

In order to ensure a high-quality experience, your computer/phone/tablet and internet connection speed should meet the following recommended system requirements.

Overview

- Internet connection - broadband wired or wireless (3G or 4G/LTE)
- Speakers and microphone* – built-in, USB plug-in, or wireless Bluetooth
- Webcam* - built-in, USB plug-in

*Webcam and microphone are only required for those speaking and broadcasting video.

Operating systems / browsers

Windows

To use the web platform, you'll need:

- Windows 10, Windows 8 or 8.1, Windows 7
- Chrome, Firefox, *Edge*, *IE11 (with client)*
- Computer or laptop with Intel Pentium 4 processor or later that is SSE2 capable and 512 MB of RAM, or a Surface PRO 2 or Surface PRO 3

Mac

To use on Mac, you'll need:

- Mac OS X, macOS 10.9 or later
- Chrome, Firefox, Edge, *Safari (coming soon)*
- Intel processor 64-bit and 512 MB of RAM

Linux

To use on Linux, you'll need:

- Ubuntu 12.04, Mint 17.1, Red Hat Enterprise Linux 6.4, Oracle Linux 6.4, CentOS 6.4, Fedora 21, OpenSUSE 13.2, ArchLinux (64-bit only)
- Chrome, Firefox
- Intel Pentium 4 processor

Chrome OS

Chrome OS works directly through the Chrome browser on laptops and tablets utilising Chrome OS (Chromebooks).

- Chrome

- 2GB Ram

iOS (iPhones and iPads)

To use on iPhone, you'll need:

- iPhone 5S or later
- Safari
- iOS 11 or later

To use on iPad, you'll need:

- iPad Mini 3, iPad Air, iPad Pro, iPad (2017) or later
- Safari
- iOS 11 or later

Android (phones and tablets)

To use on Android phones or tablets, you'll need:

- Android 4.0 or later
- Chrome

Bandwidth recommendations

The bandwidth is optimized to deliver the best experience based on your network:

- Participate with webcam and microphone: 2 Mbps upload, 2 Mbps download
- Participate with microphone: 1.5Mbps upload, 2 Mbps download
- Participate without webcam or microphone: 1 Mbps upload, 2 Mbps download

Firewall

To participate in a real time session, please ensure that the location you are connecting from allows for the streaming and downloading of real time video.

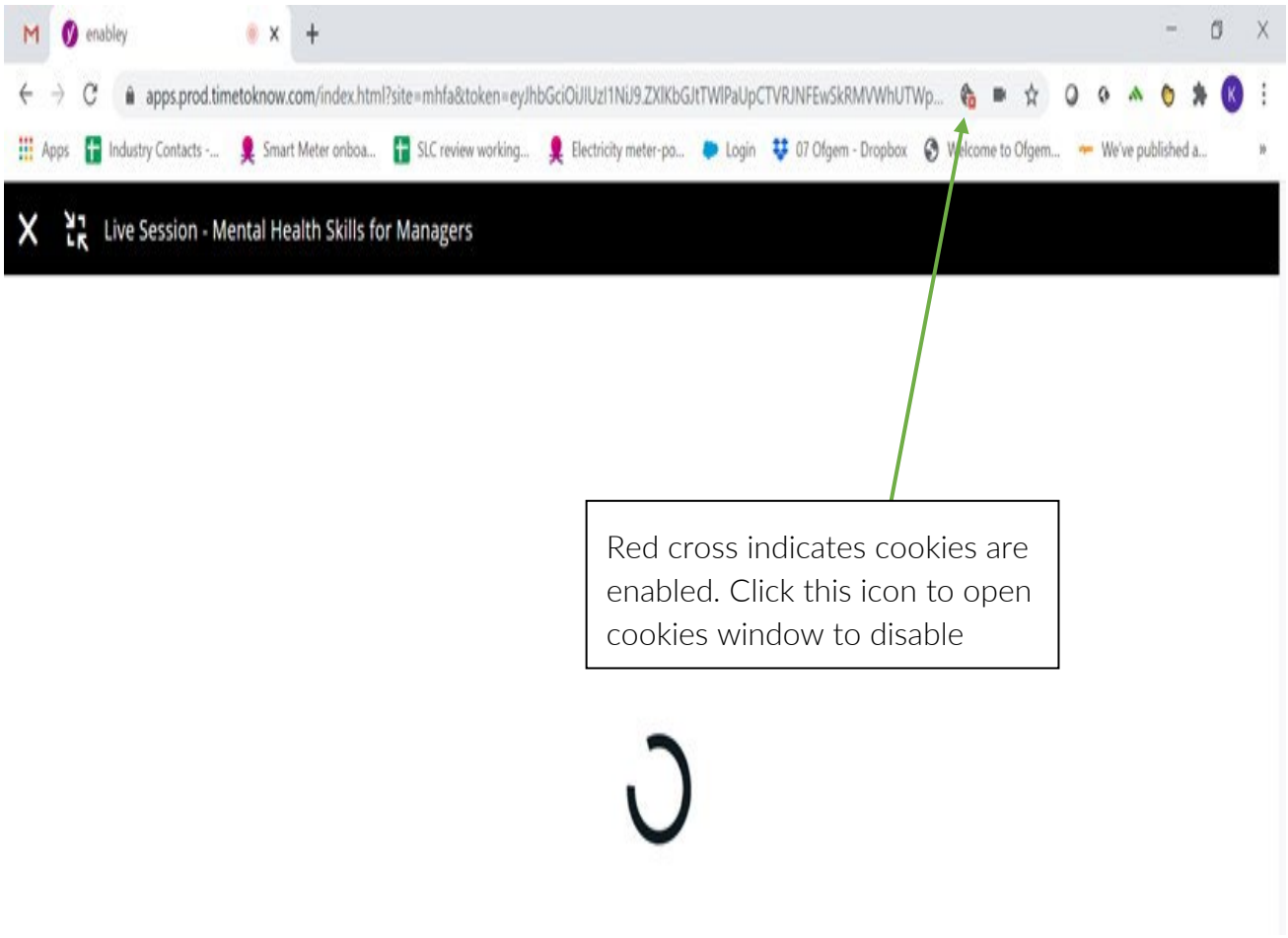
- UDP
- TCP: 80, 443
- HTTP: 80, 443

Cookies

Cookies must be enabled in order to use the web platform.

Extensions or browser configurations that block or disable cookies may prevent participants from joining a live session.

MHFA England



For further information on how to enable cookies:
https://help.enabley.io/en/article/live-session-enabling-third-party-cookies-on-your-browser

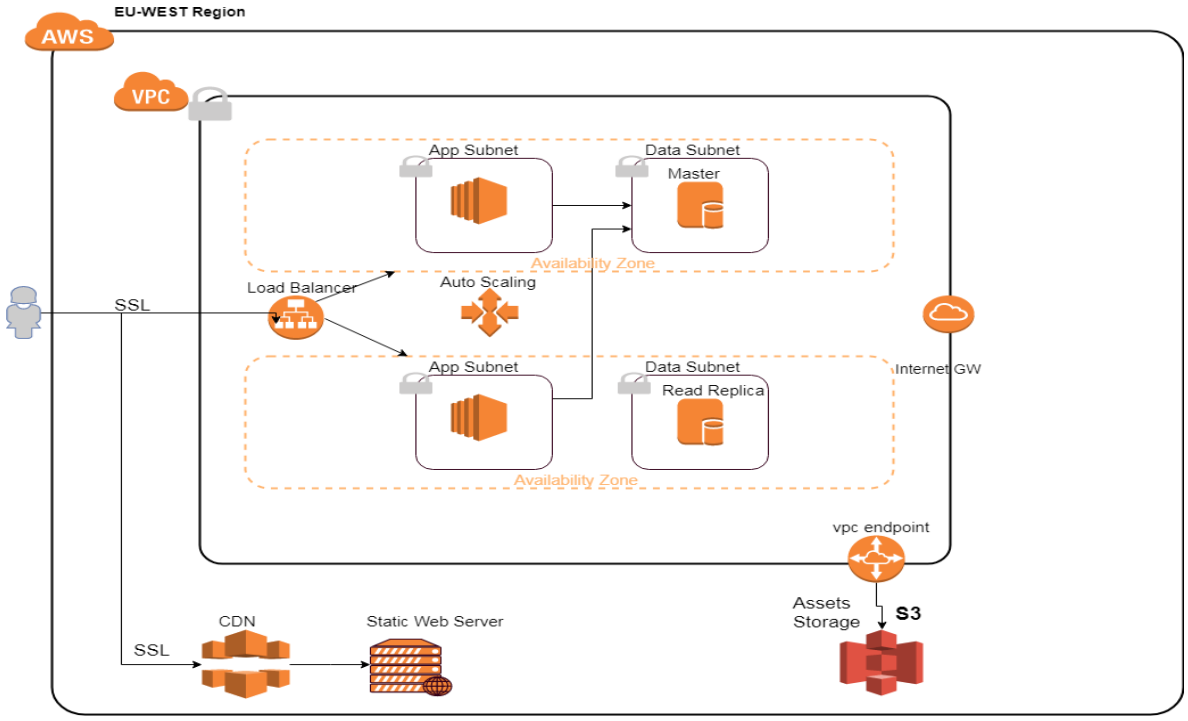
MHFA England

Security architecture and protocols

We have put this information together to describe the architecture and connection security for the MHFA England Online Learning Hub. The following information will be useful to share with your internal IT departments as they will want to ensure our platform meets their security standards. Hopefully this information will help get our Online Learning Hub added to approved site list, allowing any internal blocks accessing our platform to be removed.

Main architecture schema

The following schema displays the architecture and protocols.



The Online Learning Hub platform is hosted and managed on Amazon AWS and leverages the AWS security, provided by Security Group's (FW) Services and Internal Network Isolations.

MHFA England

Access control and authentication

Unique usernames

Unique usernames and passwords are required to access the Online Learning Hub.

Authentication

The Online Learning Hub supports Auth2 JWT protocol, which requires clients to be authenticated for any protected action. Other authentication methods, like LTI SSO (auth1), can be used as well.

Password protection

The Online Learning Hub supports strong passwords that match industry standards and requirements, as per client request. Passwords are not stored as clear text.

Separate authorisation and authentication

The Online Learning Hub ensures that user data and permission validations are separate from authentication. Roles and permissions are controlled through The Online Learning Hub administration centre.

Data storage access

Data can be accessed only from authorised network clients. The data-tier subnet can be accessed only from the app-tier subnet through dedicated FW.

Tenant isolation

Data storage is logically secured for customer access from one account to another. The application layer validates and protects each client request for data scope boundaries.

MHFA England

Data transmission and network security

Access through a secured Connection (TLS/SSL)

Access to the Online Learning Hub is allowed only by connecting through a secured connection (TLS) to ensure that all data exchanged between the servers and user devices are securely encrypted.

Network security

The Online Learning Hub on Amazon AWS is protected by a strong firewall layer. The default state is closed rather than open. This means that a port/service must be actively opened to receive internet traffic.

OS patches

Server OS's are regularly updated to ensure that the most recent security patches are implemented to combat the latest threats.

SSH access

For IT/DevOps operations – the Online Learning Hub utilises AWS SSH key management. SSH ports are accessible behind FW to an authorised set of assigned IPs.

Malicious files scanning

The Online Learning Hub includes a built-in antivirus service that scans user uploaded files, and blocks uploads with malicious behaviour.