TAX SYSTEMS

T: 01784 777 700
E: enquiries@taxsystems.com
W: www.taxsystems.com

HMRC Anti-Fraud Headers

AlphaBridge V1.3

The Delivery of Tax Information through Software (Ancillary Metadata) Regulations, SI 2019/360, which came into effect on 1 April 2019, introduced the requirement for MTD software vendors to include additional 'relevant ancillary metadata' when transmitting tax information to HMRC, which they call 'Header information'.

This information contains details about how you are communicating with the HMRC servers, e.g. via an installed desktop application or a web application. It also includes information such as the IP address of the device you are using and characteristics such as screen size.

In asking for this information HMRC are looking to protect taxpayers by detecting and preventing fraud by identifying any suspicious activity through monitoring how you connect to their systems and what you do whilst you are on them.

If more than one of the characteristics monitored in the heading changes this could indicate suspicious activity.

Further information can be found here.

AlphaBridge complies with the requirements of the Instrument by collecting and sending the required header information, where the originating device require it, the information is available and operating system permissions or security controls permit.

HMRC state that they use this information to help improve the safety and security of their services. Including detecting, preventing and responding to fraud, abuse, security risks and technical issues that could harm HMRC, or our customers.

Please see the table below for details of the different headers for which HMRC require software vendors to return the ancillary metadata.

Please note: *HMRC state that where you cannot collect a value for any particular header then you can either omit the header completely or leave the value empty. Therefore, AlphaBridge will omit any particular header where it didn't collect any data.*

Header	Description	Included
Gov-Client-Connection-Method	This header tells HMRC how the application is connecting with the HMRC server. In our MTD for VAT solutions, AlphaBridge and AlphaVAT, this is always of the value: WEB-APP-VIA-SERVER for our connection type because this is a cloud solution.	Always
Gov-Client-Public-IP	This is the public IP address from which the device makes the request to HMRC, only required for connections via intermediary servers.	If available
Gov-Client-Public-Port	This is the public TCP port that the originiating device uses when initiating the request, only required for connections via intermediary server.	If available
Gov-Client-Device-ID	This is the unique identifier that some applications generate and store on the device, it persists and does not expire. We don't deploy any code on the originating device, consequently we cannot generate a unique device ID.	Never
Gov-Client-User-IDs	This is the user identifier as constructed based on details of connection method and vendor service handling the request.	If available
Gov-Client-Timezone	This is the local timezone of the originating device, expressed in relation to Coordinated Universal Time (UTC).	If available
Gov-Client-Local-IPs	This is a list of all local IP addresses available to the originating device.	If available
Gov-Client-Screens	Contains information relating to the originating device's screens including: • pixel width • pixel height • scaling • colour-depth.	If available
Gov-Client-Window-Size	The number of pixels of the window on the originating device in which the **user** initiated the API call to HMRC, width and height.	If available
Gov-Client-User-Agent	These are the originating device details such as operating system (OS) family, OS version, manufacturer and model. This is not required for our connection method: WEB-APP-VIA-SERVER.	Not applicable

Header	Description	Included
Gov-Client-Browser-Plugins	A list of browser plugins on the originating device.	If available
Gov-Client-Browser-JS-User-Agent	Required for web applications, the java script reports the user agent from the originating device, identifying browser, device, OS family etc.	If available
Gov-Client-Browser-Do-Not-Track	Required for web applications, this identifies whether or not the “do not track” option is enabled for the browser.	If available
Gov-Client-Multi-Factor	This provides HMRC with details of how multi-factor-authentication (MFA) is performed, the time and a unique reference.	If available
Gov-Vendor-Version	This is the software name and version involved in handling the request.	If available
Gov-Vendor-License-IDs	This is the hashed license key relating to the vendor software on the originating device.	If available
Gov-Vendor-Public-IP	Public IP address of the servers to which the originating device sent the requests.	If available
Gov-Client-MAC-Address	This is the list of MAC addresses available on the originating device. This is not required for our connection method: WEB-APP-VIA-SERVER.	Not applicable
Gov-Vendor-Forwarded	A list that details hops over the internet between services that terminate TLS – showing all “handshakes” between services.	If available