**MetaEngage v2 Customer Technical Checklist**

Customer Company: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Software Product: MetaEngage Client v2

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Details** | **Sign off (Yes/No)** |
| **System Requirements** | | | |
| Operating System | To ensure that MetaEngage runs successfully on a user’s machine, we recommend that the following requirements are met: | * Windows 10 * Windows 10 IoT Enterprise LTSC x32 2019 * Windows 10 IoT Enterprise LTSC x64 2019 * Windows 10 IoT Enterprise 21h1 x64 * Windows 10 22h2 * Windows 11 * Windows Server 2022 * Windows Server 2019 * Windows Server 2016 |  |
| Browser specification |  | Microsoft Edge or Later |  |
| Memory (RAM) |  | * **Minimum:** of 4GB and Core i5 * **Recommended**: 8GB RAM and Core i7 |  |
| **Network Requirements** | | | |
| Firewall Configuration |  | * Ports to be opened: 443 * Protocols to be allowed: https * Viewlicense.adobe.io * Use.typekit.net * P13n.adobe.io * Acrobatservices.adobe.com * p.typekit.net |  |
| Network Access | Network access to the following endpoints (Metacompliance technical support can inform you of which ends points are required for your region): | * metaengageire.metacompliance.com * metaengageuk.metacompliance.com * metaengagenl.metacompliance.com * metaengagecan.metacompliance.com * metaengagedach.metacompliance.com * signalrire.metacompliance.com * signalruk.metacompliance.com * signalrcan.metacompliance.com * signalrdach.metacompliance.com * signalrnl.metacompliance.com * cdnmetacompliancelive.metacompliance.com * cdnmetacomplianceuk.metacompliance.com * cdnmetacompliancecan.metacompliance.com * cdnmetacompliancedach.metacompliance.com * Cdnmetacompliancenl.metacompliance.com * globalmetaengagefiles.file.core.windows.net |  |
| Proxy Server / Firewall Configuration |  | Ensure content packet inspection is disabled for MetaEngage traffic. We recommend whitelisting \*.metacompliance.com. |  |
| **Citrix** | | | |
| Recommended Dual Core Support per Citrix Session. |  | **Recommended:** Dual Core Support per Citrix Session. Please inform the MetaCompliance Support Team if you require a Citrix-compatible MetaEngage client. |  |
| **Software Dependencies** | | | |
| .NET 8 Windows Desktop Runtime | <https://dotnet.microsoft.com/en-us/download/dotnet/8.0/runtime?cid=getdotnetcore&os=windows&arch=x86> (216mb) | .Net 8 or above (click on link to left will bring you to the latest version). |  |
| Microsoft Edge WebView2 | <https://developer.microsoft.com/en-gb/microsoft-edge/webview2/?form=MA13LH>  (170mb). | Version 124 or above (click on link to left will bring you to the latest version). Webview 2 included by default with Windows 11. |  |
| ASP.NET Core runtime | <https://dotnet.microsoft.com/en-us/download/dotnet/8.0> | ASP.NET Core runtime 8.0. or above (click on link to left will bring you to the latest version) |  |
| UPN Compatibility | Account logged into device must match account register in MyCompliance. | Username that user logs into their machine with must be the same username that is synced into the MetaCompliance platform database.  **Example:** A user may login to their PC using the net bios domain name, but login to their cloud applications using different credentials.   1. **Primary Connection**- MetaEngage Client will connect to Active Directory by LDAP to gather UPN and deliver content to MetaEngage Client. 2. **Fallback Connection** - If this fails it will build the UPN from the volatile environment registry settings on the users device by combining the username and userDNSdomain values and then delivery content to MetaEngage Client. 3. If points 1 and 2 fail, then no content will get delivered to the MetaEngage client for user. |  |
| VPN Updates | Ensure any VPN clients are all updated to the latest version. | Out of date versions can cause connection issues with the API. |  |
| Whitelisting security PC software | Ensure whitelisting on any security PC software that may restrict connection to the above endpoints. |  |  |
| Updated Client | Ensure MetaEngage Client on user’s devices have updated to the latest version. |  |  |
| Windows Updates | Ensure Windows update settings are all installed to the latest versions on every user's machine. |  |  |

**Further Information**

**Installation Components**

The MetaEngage client is a small MSI that should be rolled out to all required users along with any pre-requisites within your organisation via your preferred delivery method (i.e. SCCM, Group Policy, Intune).

* Single MSI package – only one installation needed
* Requires admin access for installation
* MetaEngage Desktop Client executable
* Worker service executable

**User Identification**

* Client makes an LDAP (port 389) connection to retrieve current user's UPN.
* If unable to make an LDAP connection, i.e. not on corporate network, the UPN will be created using keys from the registry HKEY\_CURRENT\_USER\Volatile Environment.
* The UPN will be stitched together using the username and userdnsdomain keys.

**Important**: If the values of these keys do not match the user's UPN, they cannot receive enforced content when a connection to AD cannot be established.

**Feature Updates**

* **Auto Updates –** For most bug fixes and feature releases, theclient will update automatically (Internet connection is required) when the machine is restarted, or the user logs out and back in again. AV/FW rules may need to be applied to allow the automatic update of functionality.
* **Non-Auto Updates** – In some cases, an updated version of the client may be required to install fixes or apply new features and will need to be deployed Customers will be notified as detailed below in the ‘Delivery of Updates'. MetaCompliance will not be held responsible for a mismatch in client/API version.
* **Delivery of new Fixes and Features for Non- Auto Updates**
* General – Communication sent to customer 1 month prior of release.
* Critical – Communication sent to customer 48 hours prior of release.

**High-Level Architecture Diagram**

