Technical Prerequisites

Cegid Retail Store Excellence

September 2022

cegid

Introduction

This document describes the Technical Prerequisites associated with Cegid Retail Store Excellence, a SaaS (Software as a Service) solution hosted by Cegid.

Cegid Retail Store Excellence is a web application which can be accessed via the internet on any device.

1. Browsers

Cegid Retail Store Excellence supports modern browsers, specifically Chrome (recommended), Edge, Firefox (with auto-updates) and Safari. Note that the browser must include a PDF viewer.

2. Devices

Cegid Retail Store Excellence is available on any device with an internet connection and the recommended hardware standards are outlined below.

Hardware	Recommended
Processor	Celeron/i3 or higher Intel Xeon AMD Athlon
Memory	2GB

A smartphone or tablet with a camera is recommended for stores to enable them to upload photos directly.

3. Whitelisting

3.1 Network Access Whitelisting (Firewall)

Cegid Retail Store Excellence is accessed via the internet, and if network access is restricted for store users (e.g. by setting Access Control Lists – ACLs – on a proxy server), it may be necessary to whitelist the one domain URL (http://<client>.storiq.net) and all of the following domains must be whitelisted with wildcards:

*.storiq.net
*.storiq.knowledgeowl.com

*.amazonaws.com
*.newrelic.com
*.nr-data.net
*.google-analytics.com
*.googleapis.com
*.gstatic.com
*.googleusercontent.com
And either: *.google.com or: *.docs.google.com/forms

The google URLs are used to support the Forms and Surveys features in Cegid Retail Store Excellence, but we appreciate some clients may not want to whitelist *.google.com.

3.2 Email Whitelisting

Cegid Retail Store Excellence generates email notifications and so the storiq.net and em2.storiq.net domain names must be whitelisted in your company email system to ensure that system generated email notifications are received.

The appropriate MX, DNS SPF and TXT records have been put in place for both storiq.net and em2.storiq.net. If you are using Mimecast, this is particularly important - see https://community.mimecast.com/docs/DOC-1419-anti-spoofing-policies. If your mail servers have an IP whitelist, you will need to add the following IPs: 54.240.90.165 54.240.90.166

4. User access

Unless you wish to authenticate user access via single sign-on, then all users require an email address to sign into the platform and manage their passwords.