Security in the Cloud

A comprehensive look at the technical specifications and security measures employed by Exclaimer Cloud for Google Workspace

exclaimer™

Table of Contents

What is Exclaimer Cloud?

Exclaimer Cloud is the premier cloud service for centrally managing Google Workspace users' Gmail signatures. It provides the same benefits as Exclaimer's on-premises server-based email signature solutions, but within a cloud environment.

Exclaimer Cloud adds signatures to all sent emails via Google Workspace. That means signatures are added to email sent from any device, including smartphones and tablets, and all mail clients. The service also allows for easy management of specific email signature elements including social media icons, promotional banners, and legal disclaimers from one intuitive web portal.

As Exclaimer Cloud is hosted outside of your organization, no upfront investment in server hardware is required, meaning no additional IT administration or ongoing maintenance. It also does not require any client installations to operate.

You design signatures using the drag-and-drop signature editor, which is within a user interface that is controlled via a web browser. It is built to be intuitive and easy to navigate, you can either choose a pre-built signature template from the template library, or build your own signature from scratch, just by dragging elements onto a template.

Users' contact details are taken from the Google Directory and merged into an email signature that you create via the service's signature editor. You don't need to depend on specific email clients like Gmail or your end users to update company signatures.

When messages are sent, all enabled signatures are processed and applied as appropriate. If more than one signature applies for a user, the first one processed will be used.

Why choose Exclaimer?

Responsible for creating the first ever email signature solution in 2001, Exclaimer is the undisputed global leader in this field, with Exclaimer Cloud marking a significant evolution in signature management technology. Since its incorporation, Exclaimer has been providing a market-leading portfolio of email signature management solutions that work work with Microsoft and Google email technology.

Exclaimer has over 75 million users worldwide including renowned international organizations such as Lloyds Bank PLC, Sony, Mattel, Morgan Stanley, the Council of the City of Sydney, NBC, the Government of Canada, the BBC, and many more organizations of all sectors and sizes.

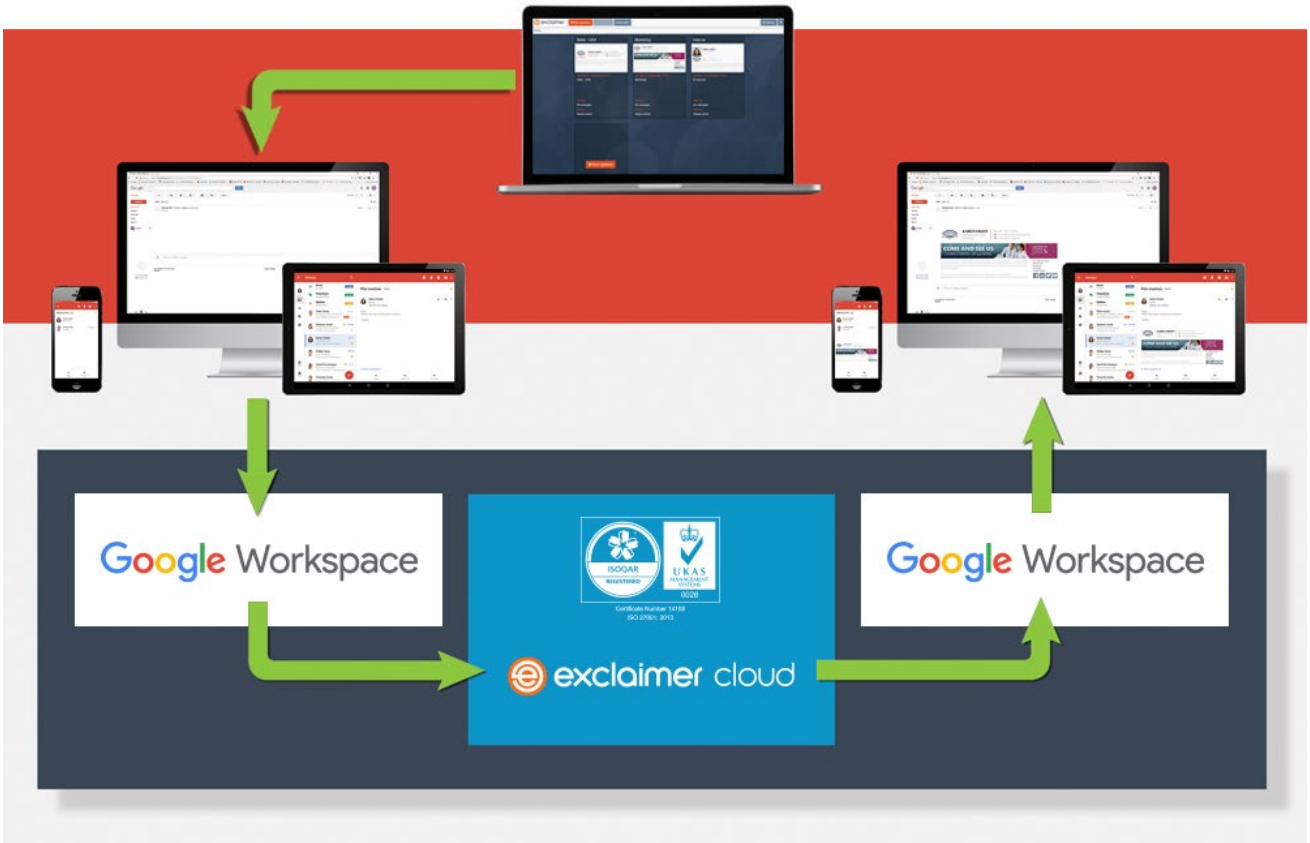
Technical overview

Exclaimer Cloud is hosted within Microsoft datacenters.

When users send emails from any device, messages are passed from Google Workspace and routed to one of Exclaimer's regional Azure datacenters. Exclaimer Cloud sees the emails and applies a professional email signature to every message. These emails then pass back to Google Workspace and are sent out as normal.

It's as simple as that! All emails are guaranteed to have the correct email signature.

How it works



1. Email signatures are designed using a drag-and-drop signature editor, and given to different users and groups. All contact data is taken from the Google Directory and additional email signature elements such as social media icons, promotional banners and legal disclaimers are easily managed. Any signature element can be updated and changes are applied in real time.

2. Users send emails via Google Workspace from any web-enabled device like a PC, Mac, or mobile device.

3. Each email sent passes from Google Workspace and is routed to one of Exclaimer's regional Azure datacenters using a mail route set up in Google Workspace. Exclaimer Cloud is a high-availability, geographically diverse, load balanced service.

4. Exclaimer Cloud sees the incoming messages and imprints the appropriate signature on every email. It **does not** send any emails out on your behalf. All messages are still sent through Google Workspace, but with a high-quality signature added to them.

5. With the signature/s added, emails are passed back to Google Workspace via a smart host. Signatures are only added to an email once due to a secured closed loop process between Google Workspace and the Microsoft Azure infrastructure. Emails are also authenticated using Google Workspace security protocols.

6. The emails are sent out as normal, but now have a high-quality signature appended to them. Signatures are essentially 'stamped' onto every email, meaning users have no control over how they look and cannot modify them.

Google Workspace Mail Routes

Mail routes are created in Google Workspace if you need a more advanced delivery option - say to route mail for Microsoft Exchange users. Exclaimer Cloud utilizes mail routes to send your mail via the Exclaimer Cloud platform.

The route to/from Google Workspace use negotiated Transport Level Security (TLS) encryption to enable a secure channel for communicating with Exclaimer Cloud. When an email has a signature added and is passed back, Google Workspace checks the message to see if it meets security conditions you have specified.

Exclaimer Cloud does not send any emails out on your behalf. All emails are still sent through Google Workspace. The email signature is authenticated by standard Google Workspace protocols with all data encrypted.

Our Azure service overview

Why we use Azure

Exclaimer Cloud has been designed to work exclusively with Microsoft Azure, which is highly trusted by IT professionals worldwide.

Azure provides ultimate scalability and flexibility. Knowing that online security is one of the biggest concerns for companies migrating to the cloud, Microsoft has designed Azure with security in mind, creating a compliance framework to meet regulatory requirements.

The Exclaimer Azure setup uses load balancing to provide a single network service from Exclaimer's regional Azure datacenters around the world. If one of Microsoft's Azure datacenters were to cease operating, our high-availability service ensures uptime and reliability.

Measures are in place to ensure that the service scales with increased number of tenants, maintaining reliability and uptime. All inbound connections are secured through SSL Certificates and TLS, which are constantly checked to meet current cloud standards. For an example, go to the Qualys SSL Labs website (www.ssllabs.com), go to the 'Test your server' link and type in portal.exclaimer.com. This will provide you with a detailed review of Exclaimer Cloud's certificate and configuration. It also lets you know that our domains are highly trusted.

Any updates to the Exclaimer Cloud service are scheduled to occur 'out-of-hours' for each region, minimizing any disruption. Updates are built and tested by Exclaimer's head office based Development and Quality Assurance teams before going into production. This intensive process includes stress testing beyond normal usage and no code is ever deployed to Azure until it has passed rigorous anti-virus checks, in addition to being scanned by native antimalware on all Azure virtual machines (VM).

The ISO/IEC 27001:2013 Certification

Exclaimer Cloud has achieved the ISO/IEC 27001:2013 Certification for Information Security Management, which was awarded by the BSI (British Standards Institution). This is specifically for the development and supply of a cloud-hosted email signature management system. The ISO/IEC 27001:2013 Certification means a third party accredited independent auditor has performed a thorough assessment of Exclaimer Cloud and has confirmed it is operating in alignment with ISO cloud standards.

Data handling

To use Exclaimer Cloud, a customer has to setup an Exclaimer Cloud account online. The data taken during this process is secured within a hosted Microsoft SQL Server. The data stored is shown below:

- First name
- Last name
- Full name
- Company
- Telephone number
- Email address
- Address Line 1
- Address Line 2
- Town/City
- Postcode/Zip Code
- Country

All user passwords are protected using salted password hashing. When you create an Exclaimer Cloud account, your password is 'hashed' and stored within a secure SQL database. At no point is an unencrypted password ever stored and Exclaimer cannot read these password 'hashes'. Exclaimer Cloud does not store any credit/debit card details.

When you add a new payment card to your account, you are redirected to the Global Iris payment portal, powered by RealEx Payments. This is secured using a 128-bit SSL Certificate and is one of the most secure ecommerce platforms for online payments.

After subscribing, you grant permission for Exclaimer Cloud to read user data from your Google Directory. This data is cached using Azure Storage so it can be used continuously in the signature templates and configurations you set up. In addition, we store your template designs and signature rules within Exclaimer Cloud's user interface (UI).

The attributes aggregated by Exclaimer Cloud are shown below:

Attr Name
Address.Company.CountryCode
Address.Company.Line<N>
Address.Company.City
Address.Company.State
Address.Company.PostalCode
Address.Home<N>
Address.Work<N>
Department
Email<N>
FamilyName
FullName
GivenName
JobTitle
OrganizationName
Phone.Home<N>
Phone.Mobile<N>
Domain
Custom.<Category Name>.<AttributeName>

The Exclaimer Cloud portal

Exclaimer Cloud can only be accessed with a web browser on any web-enabled device using HTTPS for transport encryption. The Exclaimer Cloud portal is verified by COMODO RSA Extended Validation Secure Server CA. The connection to the portal uses TLS 1.2 and is encrypted using 256-bit encryption (AES_256_CBC with SHA384 for message authentication and ECDHE_RSA as the key exchange mechanism). This ensures that data is completely secure within the Exclaimer Cloud.

The portal incorporates 2-factor authorization to prove the identification of Exclaimer Cloud users. This adds an extra level of security to the login procedure. The second level of authentication comes in the form of a unique authorization code. Each code is only valid for a maximum of 4 hours. When you login to your account for the first time or from a different device/computer, you will be sent an email with an authorization code to confirm that it is actually you trying to access your account.

All you need to do is enter the unique authorization code once and you're good to go. You won't have to go through this process every time you login.

Exclaimer will never ask for any personal information in an email. This includes:

- Payment information (credit card number, debit card number etc.)
- VAT number

- Your account password

In the end, as with any online service, the weakest link in the security chain is often the implementation of weak passwords. An Exclaimer Cloud account password must be a minimum of 6 characters containing the following:

- Uppercase letter
- Lowercase letter
- Digit (number)

For extra security purposes, we recommend using a password that is:

- Unique to Exclaimer Cloud and not used anywhere else within your organization
- At least 8 characters long
- A mix of uppercase and lowercase letters, digits and symbols e.g. +, @, #, $, £
- Not a birthday, date, name or address

We also recommend that you change your password periodically e.g. every 90 days.

Message processing

When a user sends an email via Google Workspace, it passes through Google Workspace's Content Compliance and is routed to an Exclaimer regional Azure datacenter.

When the email reaches the Azure datacenter, Exclaimer Cloud examines the message 'envelope', which includes the sender's details and intended recipients, determining which signature is applied to the email.

The sender's attributes are pulled from the cached Google Directory data, which is used to populate the selected signature, e.g. name, job title, phone number etc. Exclaimer Cloud then ascertains where the signature will be inserted. It decodes the MIME (Multipurpose Internet Mail Extensions) carrier to do this.
The signature is then inserted in the appropriate location and this new email is sent back to Google Workspace via the SMTP relay service which forwards the email onto its original recipient/s.

Exclaimer Cloud does not save any email content to an external location. This is due to the SMTP mode of integration with Google Workspace not requiring emails to be stored prior to being forwarded back to Google Workspace. All it does is look for a reply separator in order to apply the signature correctly. It also scans the message body for any unique strings to determine if a signature is already present i.e. during email conversations.

Fault handling and failure

Exclaimer Cloud uses state-of-the-art tools and technologies to ensure 99.99% service availability. The Exclaimer Cloud service is situated in load balanced groups for reliability and scalability purposes. Network and application traffic is therefore distributed across a number of different servers.

Our 24/7/365 monitoring services automatically detect any service alerts, which are configured with escalation chains. This means that Exclaimer's senior technical management is notified of any problems immediately.
If an issue occurs that stops the signature imprinting service at one regional datacenter, a highly unlikely scenario, you can be assured that emails sent from your organization will not be lost.

As soon as the issue is resolved, all email continues to be sent as normal. Our Development and Quality Assurance teams are continually evolving and developing the Exclaimer Cloud service in line with changes made to Microsoft Azure in order to prevent any technical matters occurring.

Each region has a secondary datacenter for use as a failover in the case of an infrastructure issue:

Region	Primary datacenter	Secondary datacenter
Europe	West Europe - Netherlands	North Europe - Ireland
USA	East US - Virginia	West US - California

Datacenter Load Balancing Policy

During normal service running, mail is routed intelligently to one of the two Microsoft Azure datacenters in your assigned region, this ensures reliability, resiliency and high performance of the service.

In the rare event of an issue occurring that stops the signature imprinting service at one of Exclaimer's Microsoft Azure datacenters, Exclaimer has a comprehensive method in place that ensures mail flow continues to flow as normal through an alternate datacenter automatically. The primary goal is to maintain mail flow for all Exclaimer Cloud customers using multi-location high availability and load balancing.

What is Exclaimer's datacenter load balancing policy?

If an incident occurs at one of Exclaimer's two datacenters in a region, a comprehensive cross-datacenter system is in place to ensure mail flow for all tenants is maintained. Tenant data is continuously synchronized in both datacenters simultaneously.

Load balancing is fully automated and is controlled intelligently by Microsoft Azure services. Should an incident occur, one of Exclaimer's regional Azure datacenters can be independently removed from the load balancer. This is a fully automated process, but can also be controlled manually if required.

Exclaimer acknowledges mail flow as mission critical, and currently only mail flow is load balanced in this way. In the rare event that we see an issue in the primary regional Azure datacenter, customers will not be able to access the UI; including settings, configuration and the template editor. The ability for new customers to sign up will also not be available.

If you were to update any contact details in your Google Directory, these will update in line with Exclaimer's automatic data synchronization that occurs once every 24 hours. However, you will not be able to start a manual aggregation in Exclaimer Cloud.

The type of incidents that this policy protects against are:

- IP reputation issues
- Azure infrastructure issues
- SaaS issues

Mail routing is dependent on Microsoft's DNS service being active. The DNS service is not datacenter or region specific.

Technical support

Every Exclaimer Cloud customer is automatically entitled to extended technical support that covers all global territories. The Exclaimer Technical Support team is comprised of Microsoft Certified Professionals that are able to assist by phone, email, and remote desktop sessions via TeamViewer.

To raise a Support Ticket, simply visit www.exclaimer.com/support/raise-ticket, give a description of the technical issue and one of our Support Engineers will contact you within 24 working hours. In the event of an outage, your case will be escalated to ensure that your service resumes operation with little downtime. For any urgent technical faults, it is recommended that you contact Exclaimer Technical Support by phone as soon as possible.