SECURITY IN THE CLOUD

A comprehensive look at the technical specifications and security measures employed by Exclaimer for Microsoft 365

exclaimer

exclaimer.com

TABLE OF CONTENTS

WHAT DOES EXCLAIMER OFFER

Exclaimer offers the premier cloud service for centrally managing Microsoft 365 email signatures. It provides the same benefits as on-premises server-based email signature solutions, but within Microsoft's cloud environment.

Exclaimer Cloud adds signatures to all sent emails via Microsoft Azure. That means signatures are added to email sent from any device, including smartphones and tablets. It 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 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.

With an intuitive editor that lets you customize key elements and choose what information to include, you can create beautiful signatures with your own brand including logo, imagery, and color scheme.

Users' contact details are taken from Azure Active 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 Outlook 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. Since its incorporation, Exclaimer has been providing a market-leading portfolio of email signature software that works directly with Microsoft and Google email technology, specifically Microsoft 365, Google Workspace, and Microsoft Exchange.

Exclaimer has over 50,000 customers 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.

Exclaimer is a Microsoft Gold Partner. This demonstrates its technical expertise in the development of solutions and services for Microsoft 365 and Microsoft Exchange. The accreditation also showcases Exclaimer's skill in building solutions that work using the Microsoft Azure cloud platform.

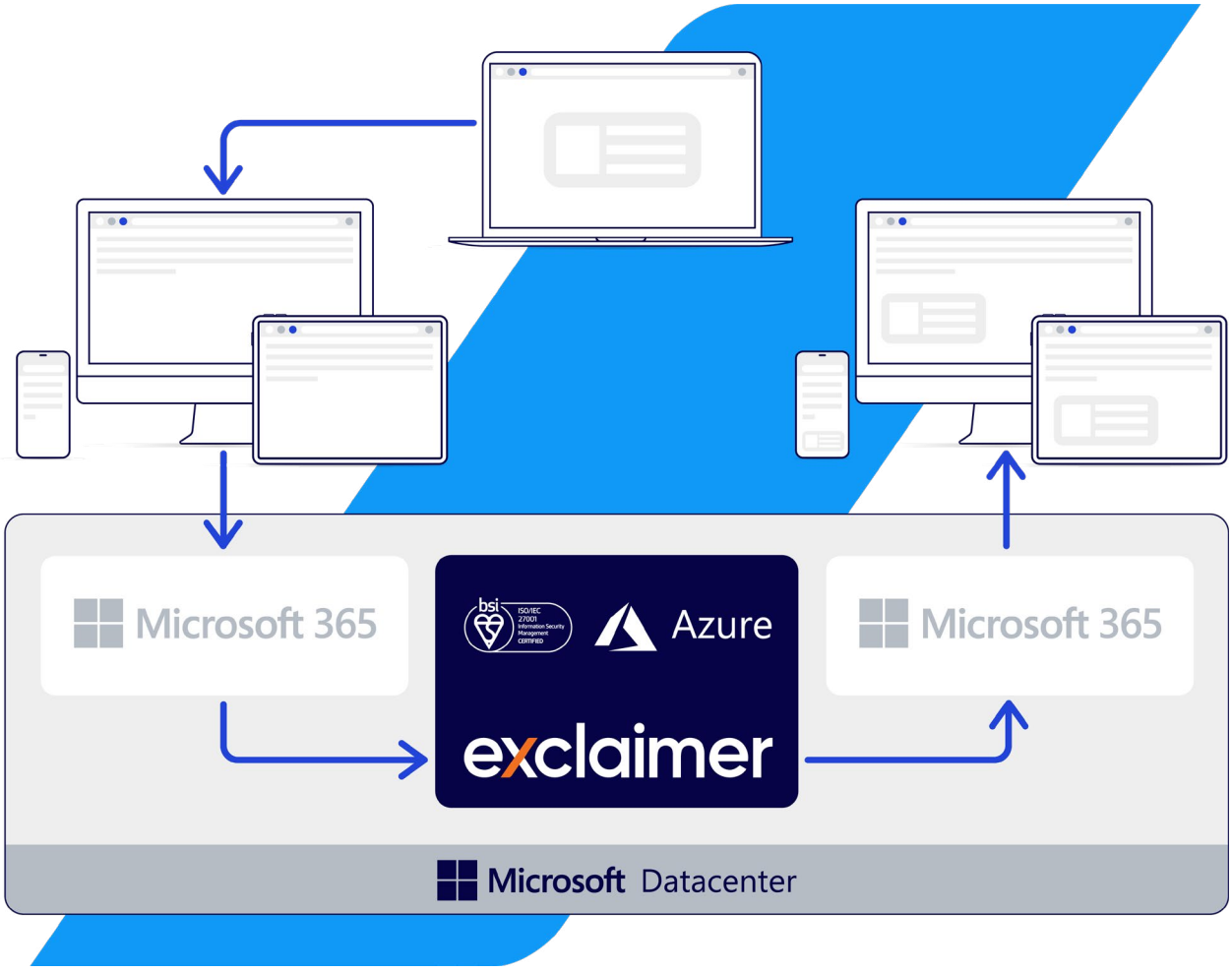
TECHNICAL OVERVIEW

Exclaimer is hosted within Microsoft datacenters, so your Microsoft 365 emails never leave the Microsoft Cloud infrastructure.

When users send emails from any device, messages are passed from Microsoft 365 and routed to one of Exclaimer's regional datacenters. Exclaimer sees the emails and applies a professional email signature to every message. These emails then pass back to Microsoft 365 and are sent out as normal.

It's as simple as that! All emails are guaranteed to have the correct email signature while staying within the Microsoft Cloud.

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 Azure Active 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 Microsoft 365 from any web-enabled device.

3. Each email sent passes from Microsoft 365 and is routed to one of Exclaimer's regional Azure datacenters using a start point (Send) connector set up in Microsoft 365. Exclaimer is a high-availability, load balanced service hosted within the Microsoft datacenters local to you. This guarantees that no email ever leaves the Microsoft Cloud environment.

4. Exclaimer 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 Microsoft 365, but with a high-quality signature added to them.

5. With the signature/s added, emails are passed back to Microsoft 365 via an end point (Receive) connector, also set up in Microsoft 365. Signatures are only added to an email once due to a secured closed loop process between Microsoft 365 and the Microsoft Azure infrastructure. Emails are also authenticated using Microsoft 365 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.

MICROSOFT 365 CONNECTORS

A standard Microsoft 365 protocol, connectors let you customize the way your email flows to and from an organization using Microsoft 365.

Connectors can be configured to:

- Enable mail flow between Microsoft 365 and your on-premises email servers (hybrid environment).

- **Apply security restrictions to mail exchanges with a business partner or service provider, e.g. a cloud provider that provides a service** - this is the purpose of this document.

- Enable email notifications from a printer or other non-mailbox entity.

To enable Exclaimer to interact with Microsoft 365 and our Azure datacenters, you must configure the mail flow using connectors. Connectors allow for emails to be rerouted to Exclaimer's Azure datacenters, authenticated by Microsoft 365 security and sent back to Microsoft 365 once a signature has been added.

As you are sharing your Azure Active Directory details with Exclaimer, connectors protect the integrity of the mail flow. The SMTP connectors to/from Microsoft 365 use negotiated Transport Level Security (TLS) encryption to enable a secure channel for communicating with Exclaimer.

When an email has a signature added and is passed back to Microsoft 365, the 'Receive' connector checks the message to see if it meets security conditions you have specified. As the email never leaves the Microsoft Cloud, it continues to meet Microsoft's strict security standards.

Exclaimer does not send any emails out on your behalf. All emails are still sent through Microsoft 365. The email signature is authenticated by standard Microsoft 365 protocols with all data encrypted.

OUR AZURE SERVICE OVERVIEW

Why we use Azure

Exclaimer has been designed to work exclusively with Microsoft Azure, which is highly trusted by IT professionals worldwide. By utilizing the Azure platform, no email you send to us requiring a signature ever leaves the Microsoft Cloud environment. Azure provides ultimate scalability and flexibility, using the same technologies as other Window platforms. 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's certificate and configuration. It also lets you know that our domains are highly trusted.

Any updates to the Exclaimer 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 servers.

The ISO/IEC 27001 Certification

Exclaimer Cloud has achieved the ISO/IEC 27001 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 Certification means a third party accredited independent auditor has performed a thorough assessment of Exclaimer and has confirmed it is operating in alignment with ISO cloud standards.

Data handling

To use Exclaimer, a customer has to setup an Exclaimer 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 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 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 to read user data from your Azure Active 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's user interface (UI).

The AD attributes aggregated by Exclaimer are shown below:

Attr LDAP Name	Attr Display Name
City	l
Country	co
Department	department
DisplayName	displayName
EmailAddress	mail
FaxNumber	facsimileTelephoneNumber
FirstName	givenName
LastName	sn
MobileNumber	mobile
Office	physicalDeliveryOfficeName
State	st
StreetAddress	streetAddress
TelephoneNumber	telephoneNumber
JobTitle	title
PostalCode	postalcode

Data in transit between Exclaimer's cloud platform and Microsoft 365 is encrypted using a combination of RSA-2048-bit asymmetric encryption and a one-time use Rijndael symmetric session key. Rijndael is an algorithm selected by the U.S. National Institute of Standards and Technology (NIST) as the Advanced Encryption Standard (AES). Keys issued are managed through certificates, with several of these being used for encipherment (converting a message into a cipher for encryption and decryption) purposes.

When Exclaimer processes an email, it examines the message to decipher the sender's and intended recipient's details so it can apply the relevant signature as configured within the UI. It also scans the mail for common strings that represent a reply separator, so the signature can be inserted in the correct location.

Exclaimer does not actually 'read' the message in the traditional sense, and the email content is not available to Exclaimer personnel or retained on our platform for any longer than is required to process and pass back to Microsoft 365.

The cached, read-only Azure Active Directory data that is stored by Exclaimer is hosted within your assigned regional datacenters. The data is never stored or processed outside of your regional datacenter.

For more information on Azure SQL Database security, visit msdn.microsoft.com/en-us/library/azure/ff394108.aspx.

The Exclaimer portal

Exclaimer can only be accessed with a web browser on any web-enabled device using HTTPS for transport encryption. The Exclaimer portal, the only access point to the service, 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.

The portal incorporates 2-factor authorization to prove the identification of Exclaimer 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 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

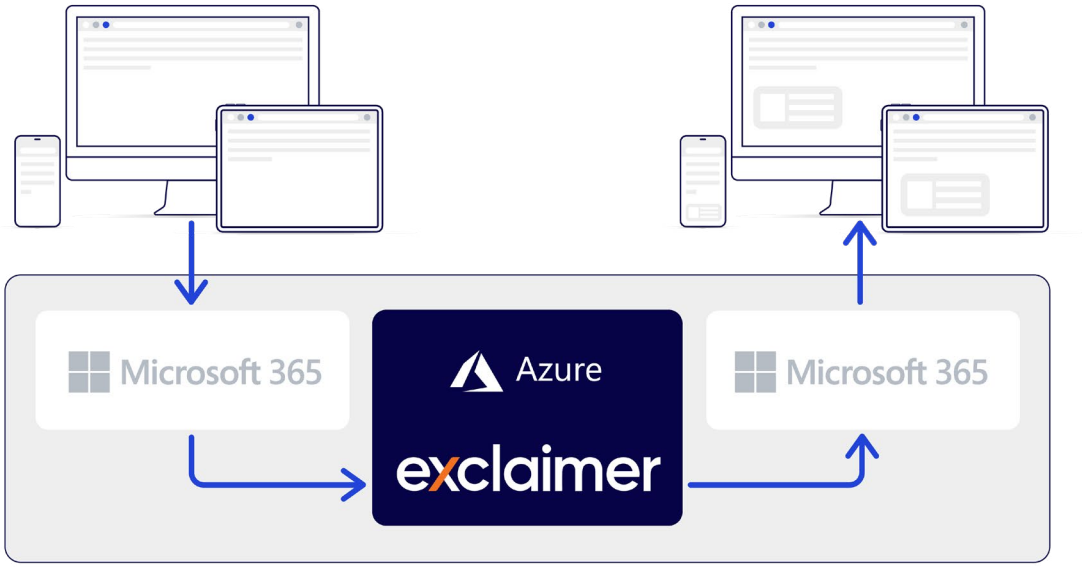
When a user sends an email via Microsoft 365, it passes through the Send connector and is rerouted to an Exclaimer regional Azure datacenter, as mentioned previously.

When the email reaches the Azure datacenter, Exclaimer 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 Azure AD data, which is used to populate the selected signature, e.g. name, job title, phone number etc. Exclaimer then ascertains where the signature is to be inserted. It decodes the MIME (Multipurpose Internet Mail Extensions)/TNEF (Transport Neutral Encapsulation Format) carrier to do this.

The signature is then inserted in the appropriate location and this new email is sent back to Microsoft 365. It passes through the Receive connector, which forwards the email onto its original recipient/s.

Exclaimer does not save any email content to an external location. This is due to the SMTP mode of integration with Microsoft 365 not requiring emails to be stored prior to being forwarded back to Microsoft 365. 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.



The local Exclaimer Exchange agent, used by organizations with a hybrid environment, utilizes HTTPS over TLS 1.2 (secured using a certificate from a trusted certificate authority) to communicate with the Exclaimer service in Azure.

That service, in turn, uses the API key provided by the agent in the 'Authorization' header over HTTPS to confirm the agent, and the Exclaimer customer using that agent, are legitimate. This API key can only be generated from within the Exclaimer UI by a logged-in administrator and expires after one year, when it must be replaced.

The agent will parse the headers of the message to determine the sender (along with other metadata) to confirm whether Exclaimer needs to process the message, e.g. the message has a blank sender address or is from an external sender to a recipient in the customer's organization (and doesn't need a signature).

The message is then passed to the Azure service (via HTTPS as described above, authorized with a unique API key), where a signature is added via the imprinting service. If it encounters a problem processing the message, a retry will be attempted after 2 seconds, 4 seconds, 8 seconds, and 20 seconds have elapsed. After this time period, if the issue still occurs, the message is sent without an email signature. If this is a major concern, transport rules can be configured to prevent an email leaving the organization without a signature.

On the agent itself, if a minute elapses without the message being imprinted successfully, or if a 'Back Off' response from the Azure infrastructure, it will give up on imprinting the message and it will be sent without an email signature. This ensures that mail flow is not disrupted.

FAULT HANDLING AND FAILURE

Exclaimer uses state-of-the-art tools and technologies to ensure 99.99% service availability. The Exclaimer 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 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
Australia	Australia East - NSW	Australia South East - Victoria
UK	UK South - London	UK West - Cardiff
India	Central India - Pune	South India - Chennai
Canada	Canada Central - Quebec City	Canada East - Toronto

Sent Items Update

Exclaimer Sent Items Update requires the following permissions:

- User Exchange Web Services with full access to all mailboxes
- Read and write mail in mailboxes

Exclaimer uses Exchange Web Services (EWS) to update the sent item in the user's mailbox; this requires read and write access to the user's mailbox to locate and update the email. Access to the user's mailbox through EWS is authorized using a certificate securely stored in the Exclaimer infrastructure and the Azure application that required consent during the configuration of Sent Items Update. Consent for Exclaimer's Sent Items Update can be revoked by deleting the Sent Items application in the Azure Portal.

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 occur as normal through an alternate datacenter automatically. The primary goal is to maintain mail flow for all Exclaimer customers using multiple locations, high availability, and load balancing.

What is Exclaimer's datacenter load balancing policy?

If an incident occurs at one of Exclaimer's two regional datacenters, 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 Azure Active 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.

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 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 https://portal.exclaimer.com/support/raise-a-ticket/, give a description of the technical issue, and one of our Support Engineers will contact you within a matter of 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.