

Managed Email Authentication Service

Helps businesses **implement and manage DMARC and DKIM** protocols for their **email domains**

What is a Managed Email Authentication Service

The Managed Email Authentication Service helps businesses implement and manage DMARC (Domain-based Message Authentication, Reporting & Conformance) and DKIM (DomainKeys Identified Mail) protocols for their email domains. This ensures that only authorised senders can use the domain, protecting against email spoofing and phishing attacks. It also improves email deliverability by ensuring that legitimate emails are recognised and not flagged as spam by recipient servers. Apex manages the ongoing monitoring, adjustments, and reporting, ensuring continuous protection and compliance.

How Does a Managed Email Authentication Service Work

Businesses face a significant risk of email spoofing and phishing attacks, where bad actors impersonate legitimate domains to send fraudulent emails. These attacks can lead to data breaches, financial fraud, and loss of trust. Additionally, many organisations struggle with email deliverability issues because emails sent from their domains are often flagged as spam or not delivered at all if proper authentication protocols like DMARC and DKIM are not in place.

The Importance of a Managed Email Authentication Service

With email being the backbone of business communication, failing to secure your domain can result in phishing attacks, loss of sensitive data, and reputational damage. Additionally, many businesses find that their emails aren't delivered if DMARC and DKIM are not correctly configured. Implementing these protocols ensures that legitimate emails reach their recipients, while fraudulent emails are blocked, thus improving security and communication reliability.

The Outcome

Customers benefit from enhanced protection against email-based attacks such as phishing and spoofing, and improved email deliverability. With Apex managing the service, businesses can focus on their core operations while enjoying peace of mind that their domain is secure and emails are consistently reaching their intended recipients. This also builds trust with customers and partners by ensuring secure and reliable email communications.



What This Product Does:

Prevents Email Spoofing and Phishing: Ensures only authorised users can send emails from your domain, protecting against fraudulent activities.

Managed Service: Apex handles the setup, monitoring, and adjustments of DMARC and DKIM protocols, so businesses don't need to manage this internally.

Improves Email Deliverability: Increases the likelihood that legitimate emails are delivered and not flagged as spam by ensuring proper authentication.

Comprehensive Reporting: Provides real-time insights and reports on who is trying to misuse your domain and how effective the protection is.

If used as part of the Apex Cyber Security Sphere: Integrates with Apex's broader security offering for a holistic approach to protecting your IT infrastructure.

What This Product Doesn't Do:

Not a Full Email Security Solution: This service manages DMARC and DKIM but doesn't cover encryption, malware detection, or full email threat protection. Additional tools are necessary for full email security.

Doesn't Guarantee Complete Deliverability: While it significantly improves deliverability, other factors such as email content and sending reputation also influence whether emails are delivered successfully.

No Protection Against Internal Misuse: This service doesn't protect against internal email misuse or insider threats. Separate internal policies and monitoring are required.