

THE STEPS TO ENFORCEMENT WITH VALIMAIL ENFORCE®

With Valimail Enforce, you can achieve DMARC enforcement quickly and painlessly. Follow this streamlined onboarding process — once these tasks are complete, Valimail's automation takes over and your domain is ready for DMARC enforcement.

VALIMAIL (WHAT WE DO)

1 Identify sending services

With your baseline assessment complete, we have visibility of all third-party sending services using your domain(s) and can determine if each service is authenticating or not.



5 Authenticate authorized services

Provided sender-specific instructions for the service owner to follow, ensuring authorized sending services are aligned for DMARC.

6 Review and suggest enforcement

Verify that all authorized sending services are sending correctly. Provide recommendations on any services that do not support authentication. Recommend the customer to move to enforcement.

CUSTOMER (WHAT YOU DO)

2 Confirm emailing and non-emailing domains

With your baseline assessment complete, you have visibility of all third-party sending services using your domain(s). Now decide if each sending service is authorized to send as you.

3 Point records to Valimail

In your DNS, point your SPF and DKIM records to Valimail. If you haven't already done so, also point your DMARC record to Valimail.

4 Identify service owners

Identify the owner of each service and work with your Valimail Product Support Engineer to configure the service with authentication.



7 Move to enforcement

Valimail recommended best practice: Set your DMARC policy to **quarantine** first and then move to a policy of **reject** after 30 days.

CONTINUOUS SUPPORT

Once your domain is at enforcement, Valimail Enforce will continue to monitor your email authentication activity and notify you of items that need your attention, such as a new service attempting to send emails using your domain. You will receive monthly reports and continuous access to, and support from, the Valimail Product Support team.