HOW TO SET UP DMARC FOR YOUR ORGANIZATION

Before any organization can be issued a Verified Mark Certificate (VMC), that organization must first be compliant with DMARC (Domain-based Message Authentication, Reporting & Conformance). This guide will take you through the steps you need to take to ensure your organization has correctly implemented DMARC.

digicert®

digicert®

WHAT IS DMARC?

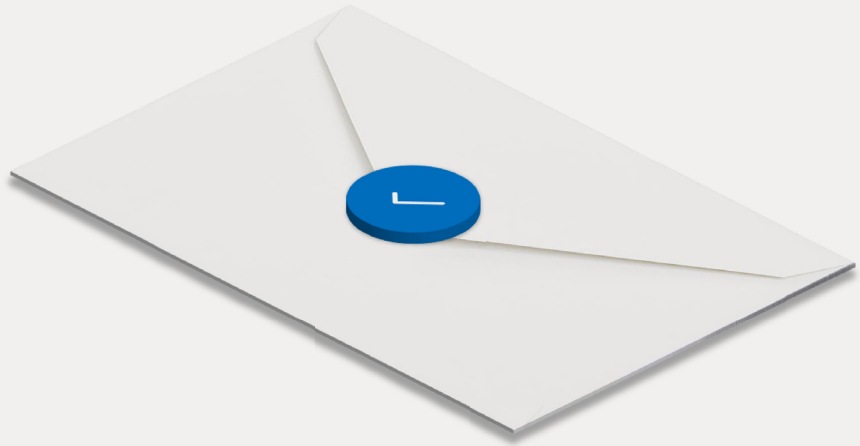
DMARC is an email authentication, policy, and reporting protocol that allows organizations to protect their domain from unauthorized use—including impersonation and phishing attacks.

Here's a basic summary:

- DMARC is a TXT record stored in DNS that gives email receivers the ability to check the authenticity of received mail.
- It is designed to fit into an organization's existing inbound authentication process, and helps email recipients determine if a message "aligns" with what the receiver knows about the sender.
- Organizations have three policy options to handle "non-aligned" messages:

- "p = none" (no enforcement)
- "p = quarantine"
- "p = reject"

- For DMARC to work properly, Sender Policy Framework (SPF) and DomainKeysIdentified Mail (DKIM) protocols must be set up beforehand.
- An organization's DMARC record can be checked through existing Internet-based "tools."



BETTER MAIL AUTHENTICATION STARTS WITH DMARC

The goal of DMARC is to build a system of senders and receivers that will mutually collaborate to improve mail authentication practices of senders and enable receivers to reject unauthenticated messages.

digicert®

WHY DMARC?

By implementing DMARC, organizations can enjoy four key benefits:

1. **Security**

   Protect people from spam, fraud and phishing by blocking the unauthorized use of your email domain.

2. **Visibility**

   Get detailed reports about who (and/or what) across the internet is sending email using your domain.

Deliverability

Increase deliverability by 5-10% and prevent emails from being flagged as SPAM.

4. **Brand protection**

   Defend your brand against identity-targeted attacks.

of customers are less likely to engage with a brand after being phished by an attacker posing as that organization.

digicert®

HOW TO SET UP SPF:

1. Gather IP Addresses that are used to send email from your domain, including:
    - Web server
    - In-office mail server
    - ISP's mail server
    - Any third-party mail servers
2. Make a list of both your sending and your non-sending domains.
3. Create an SPF record in .txt for each domain using a text-editing program (i.e.Notepad ++, Vim, Nano, etc.)

    Example 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all
    Example 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all
4. Publish your SPF to DNS.

    If you manage your DNS, just add a new TXT Record containing the SPF text.If you do not manage your DNS, contact your server administrator to add the record.
5. Once the record is added to DNS, check it using an SPF Check Tool.

WHAT IS SPF?

Don't get burned by unauthorized senders. Womp womp.

SPF is the standard that pioneered the concept of domain-based email authentication. It prevents spoofing by enabling domain owners to automatically approve IP addresses of servers that are authorized to send email on the domain's behalf. If a mail server with an IP address that's not on the list tries to send email using that domain, it won't pass SPF authentication

digicert®

HOW TO SET UP DKIM:

1. Choose a DKIM selector.

It should be a simple, user-defined text string that will be appended to the domain name to help identify the DKIM public key (e.g. “standard”).

Example: “standard._domain.example.com” = host name

2. Generate a public-private key pair for your domain.

- Windows end-users can use PUTTYGen
- Linux and Mac end-users can use ssh-keygen

3. Create and publish a new TXT Record

Create a new record through your DNS management console using the public key from the pair above.

Example: v=DKIM1; p=YourPublicKey

WHAT IS DKIM?

Prevent emails from being tampered with in transit

DKIM is an email authentication standard that uses public/private key cryptography to sign email messages.

DKIM is used to verify that the email came from the domain that the DKIM key is associated with, and that the email had not been modified in transit.

digicert®

SETTING UP DMARC MONITORING MODE

1. Ensure you’ve correctly set up SPF and DKIM
2. Create a DNS record

   The “txt” DMARC record should be named similar to “_dmarc.your_domain.com.”

   Example: “v=DMARC1;p=none; rua=mailto:dmarcreports@your_domain.com”

   If you manage the DNS for your domain, create a “p=none” (monitoring mode) DMARC record in the same manner as the SPF and DKIM records.

   If you don’t manage the DNS, ask your DNS provider to create the DMARC record for you.

3. Test your DMARC record through a DMARC check tool

   Note: You usually have to wait 24-48 hrs. for replication

   DMARC check tool

WHAT IS DMARC MONITORING MODE?

Gain visibility into what’s being sent from your domain

The monitoring mode enables domain owners to review DMARC reports containing the email traffic for the domain.

The reports identify potential failing messages that would be either quarantined or rejected once DMARC is set to full enforcement. Furthermore, DMARC reports show info about all systems and services sending emails from the monitored domain.

NOTE: Monitoring mode does not provide any level of enforcement. Mail that fails authentication is delivered normally, allowing you to avoid potential disruptions while implementing DMARC.

digicert®

COMMON TAGS USED IN DMARC .TXT RECORDS

TAG NAME	REQUIRED	PURPOSE
V	REQUIRED	PROTOCOL VERSION
P	REQUIRED	PROTOCOL VERSION
PCT	OPTIONAL	% OF MESSAGE SUBJECTED TO FILTERING
RUA	OPTIONAL	REPORTING UTI OF AGGREGATE REPORT
SP	OPTIONAL	POLICY FOR SUBDOMAINS OF THE DOMAIN

digicert®

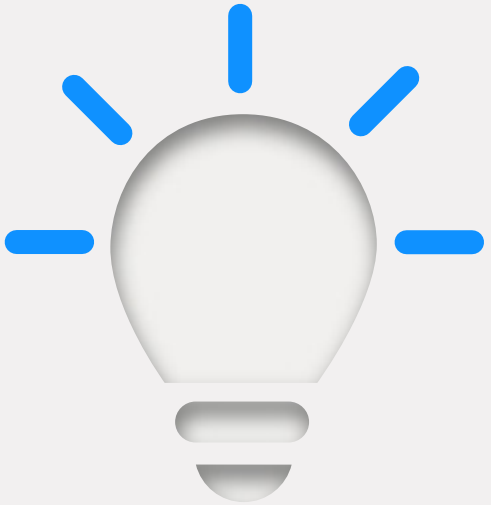
WHAT INFORMATION DOES THE DMARC REPORT PROVIDE?

The report shows domain owners how many fraudulent messages are using their domain, where they're coming from, and whether they would be stopped by a DMARC "quarantine" or "reject" policy.

The report from each receiver is an XML file that includes the following fields:

- A count of messages from each of those IP addresses
- What was done with these messages per the DMARC policy shown
- SPF results for these messages
- DKIM results for these messages

While readable, the XML report is not convenient. Domain owners may wish to use a DMARC report processor.



4 WAYS TO USE THE DMARC REPORT

Get a good baseline before you begin enforcement

1. Identify traffic that is marked as non-legitimate.

2. Look for legitimate emails that are flagged as non-legitimate by DMARC. Those emails, depending on the policy, would be either "rejected" or "quarantined" once you begin enforcement.

3. Reach out to potential systems/application owners to clarify the legitimacy of emails being flagged as non-legitimate.

4. If necessary, update your SPF record by whitelisting the IP addresses that are legitimate but were not previously included.

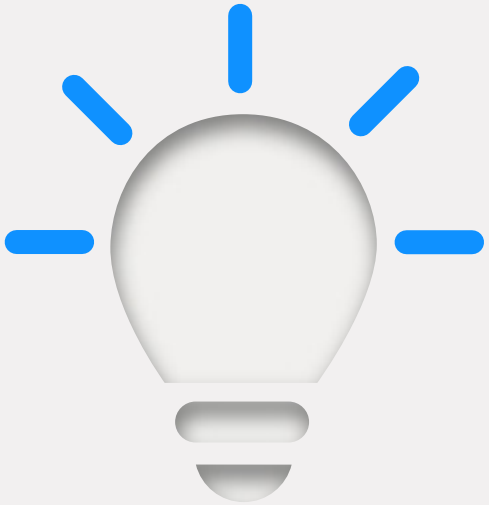
digicert®

USE DMARC REPORTING TO GET YOUR HOUSE IN ORDER BEFORE TURNING ON ENFORCEMENT

Analysis of DMARC reports can be time-consuming. However, if domain owners overlook or misidentify senders, they can end up blocking "good" emails when the DMARC policy is set to enforcement ("quarantine" or "reject"), which can cause even more time-consuming problems that may derail your progress.

Instead, here are a few suggested internal tasks before you begin DMARC enforcement:

- Inventory all email senders identified from the DMARC report and all others mentioned by the stakeholders
- Identify owners for each service/email sender
- Categorize the sending services as authorized, unauthorized or malicious
- Identify, with the support of stakeholders, any other sender that might not have shown up in the DMARC report
- Reach out to stakeholders for every new sender identified
- Update your SPF record with any newly discovered legitimate email sender's IP address



RECOMMENDATIONS FOR PRE-ENFORCEMENT COMMUNICATION

5 tips to improve adoption

- Document an implementation policy that you can share with stake holders
- Get help with DMARC support if tasks are too overwhelming or if assistance is needed.
- Communicate new findings from DMARC reports as soon as they are available.
- Start the DMARC deployment as an internal project.
- Have your executive team act as the main project sponsors.

digicert®

HOW LONG SHOULD DMARC BE LEFT IN MONITORING MODE?

The time will vary from organization to organization, with Enterprises generally spending more time than smaller organizations. Plan for weeks to months.

Once you're confident that your inventory is complete, all authorized senders have been mapped and your organization is sufficiently well-informed, you're ready to move to the quarantine phase.

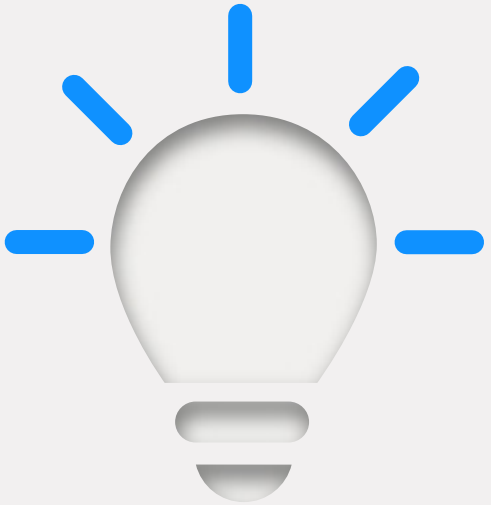
When the quarantine mode is on, messages that fail authentication will be quarantined. Usually this means that the messages are delivered to a user's spam folder.

HOW TO SET UP DMARC QUARANTINE ENFORCEMENT

1. Log in to your DNS server and search for the DMARC record
2. Open the DMARC record for the specified domain and update the policy from "p=none' to "p=quarantine"
   Example: "v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@you_domain.com"
3. Add the flag "pct" (% of messages subject to filtering). We suggest starting with 10%.
4. Incrementally increase the percentage of filtered messages to "pct=100" (100%) as you become more comfortable.

   NOTE: You must be at "pct=100" to meet BIMI and VMC standards, but your policy can be either "quarantine" or "reject."

digicert®



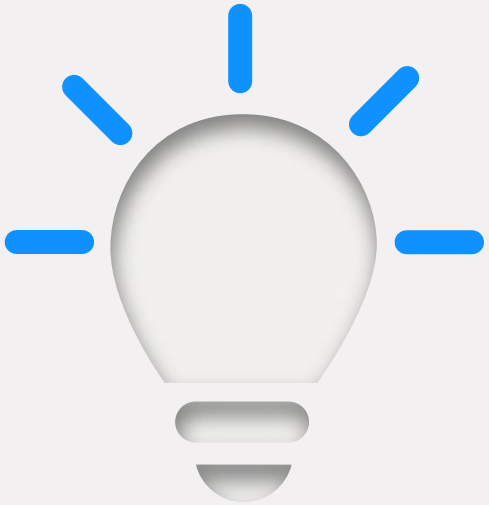
HOW FLAGGING WORKS:

- If a policy other than "p=none" is specified, that policy will be applied to the percentage in the "pct" flag
- The next less-restrictive policy will be applied to the remainder (e.g. for a DMARC record where "p=quarantine" and "pct=10," 10% of failing traffic would be quarantined and the other 90% would be delivered normally)

digicert®

ONCE YOU'VE REACHED 100% FILTERING, YOU'RE READY TO MOVE TO "P=REJECT," THE HIGHEST ENFORCEMENT LEVEL.

digicert®



HOW TO SET UP DMARC REJECT POLICY

1. Open your DMARC record through your DNS console
2. Change "p=quarantine" to "p=reject"
   Example: "v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports @ you_domain.com
3. Save the record

TIP: It's especially important to continue monitoring in this stage to ensure that legitimate emails are not being rejected and deleted.

WHAT DOES THE REJECT POLICY DO TO EMAILS?

All messages that fail the DMARC check (unauthorized emails) will be blocked/deleted and the email receiver will never get a copy of it or will be aware of its deletion.