Protect Outbound Mail with DMARC

To protect outbound mail from your domain, you will need to create a DMARC record for your domain. We recommend carefully following an incremental deployment strategy, as outlined in this guide.

What is DMARC and What Does It Do?

DMARC (Domain-based Message Authentication, Reporting & Conformance) defines a scalable mechanism by which a mail sending organization can express domain level preferences for message validation, disposition, and reporting, and a mail receiving organization can use those preferences to improve mail handling.

Why Should You Use DMARC?

DMARC provides an easier way for recipients to validate the sender of the message, easier debugging and troubleshooting, and more consistent results for handling email based on the results of SPF and DKIM lookups.

How Does DMARC Work?

When an inbound message is received, the receiving mail server performs SPF record lookups on the domain in the RFC5322 From field and DKIM lookups on the domain in the d=tag of the DKIM signature (when a message has been signed with DKIM). A message is considered to be in alignment with DMARC when:

- The organizational domain of the SPF authenticated RFC5321 Mail From command and the RFC5322 From field match. The message must pass SPF verification and the domain in the From: header must match the domain used to validate SPF (must exactly match for strict alignment, or must be a sub-domain for relaxed alignment).

  ...and/or

- The organizational domain from the “d=” value of the DKIM record matches the domain taken from the RFC5322 From field (must exactly match for strict alignment, or must be a sub-domain for relaxed alignment), and the DKIM signature has been validated.

If the message is not in alignment, then actions can be taken, such as placing the message in quarantine for review by the administrator. These actions are based on the p= tag in the DMARC record, and therefore, are chosen by the administrator of the sending domain. Additionally, aggregate reports can be sent to the domain administrator or another designated contact for all messages sent to a server claiming to be from your domain, and forensic reports can be sent for those messages that are considered to be unaligned. Aggregate reports are sent daily at midnight UTC. Forensic reports are sent immediately as incidents occur.

Creating DMARC Records

Step 1 - Prerequisites

1. Create SPF or DKIM Records (or both) for your domain. DMARC requires that at least one of these record types be available, however, we recommend using both. In addition to creating these two records, messages should also be signed using DKIM.
2. Designate an email account to receive aggregate reports from servers that receive messages claiming to be from your domain and specify the email address these reports should be sent to.

Step 2 - DMARC Record Format

Here is a sample DMARC record:
v=DMARC1; p=none; rua=mailto:dmarc_aggrepts@example.com; ruf=mailto:dmarc_forensicrepts@example.com; pct=100

There are five parts (tags) to the above DMARC record - V, P, RUA, RUF, and PCT. These tags are defined below:

1. V= The protocol version of DMARC that is being used.
   EXAMPLE: *v=DMARC1*
2. P= The policy that you want to implement, such as p=none, p=quarantine, or p=reject. The p=tag tells receiving servers how you want them to handle mail that is considered unaligned. P=reject is not recommended.
3. RUA= Indicates that you want to receive DMARC aggregate reports from servers that receive messages claiming to be from your domain and specifies the email address these reports should be sent to.
   EXAMPLE: *rua=mailto:dmarc_aggrepts@example.com*
4. RUF= Indicates that you want to receive DMARC forensic reports from servers that receive unaligned messages claiming to be from your domain and specifies the email address these reports should be sent to.
   EXAMPLE: *ruf=mailto:dmarc_forensicrepts@example.com*
5. PCT= The percentage of messages that should be handled based on the p= tag. In other words, if you have a policy of p=quarantine, then this indicates the percentage of emails that will be quarantined when they are not in alignment.
   EXAMPLE: *pct=100*

   The V and P tags are required in every DMARC record.

Step 3 - Domain/Identifier Alignment

You'll want to make sure all messages sent from your domain are in alignment with SPF and DKIM.

1. Look at the domain in the From field of sent messages. If you are using strict alignment anything other than an exact match of the domains for SPF and DKIM will be considered unaligned. If you are using relaxed alignment then subdomains are acceptable. There are many examples of DKIM and SPF records in strict and relaxed alignment under the Video Training section at www.dmarc.org.
2. Compare the "d=" tag in the DKIM signature with the domain in the RFC5322 From field of the message.

   From: user01@example.com
   DKIM-Signature: *v=1; a=rsa-sha256; c=simple/relaxed;* d=example.com*; s=mail1; t=1422368164; x=1422972964; q=dns/txt; h=Received-SPF:VBR-Info:Precedence:Sender:From:To:Subject:Date:Message-ID:MIME-Version:Content-Type:Thread-Index:Content-Language:Reply-To:List-ID:List-Post; bh=kiw5A0UkMcpoKR+R4e9XSuzDrMX5XqTWl8ye/xkmpv*
3. The DKIM signature must be valid, and the domains in the d= tag and the From header must match, depending on whether relaxed or strict alignment is being used, in order for the message to be in alignment. When relaxed alignment is used, subdomains are acceptable.

Deployment Strategy

We recommend starting out in Monitor mode, then switching to Quarantine mode incrementally, as described below.

Step 1 - Start in Monitor Mode

When starting out, it's best to start with a policy of p=none and specify the email address that will receive aggregate reports using the rua=tag. This email address will receive daily aggregate reports of email messages sent using your domain from servers that agree to send them. When you use p=none, no emails claiming to be from your domain that are unaligned with DMARC will be deleted or quarantined. This allows you to monitor the results of your DMARC implementation so that legitimate emails are not accidentally deleted or quarantined due to a misconfigured mail server or for other reasons.

You can also request to receive a copy of the message headers from the actual message that is unaligned with DMARC by listing the ruf tag (if the reporting server provides it. Some servers only send the headers of the message in the report). You can do this now or later when you've had a chance to get comfortable with the RUA (aggregate) reports. Some domains don't send the RUF (forensic) reports. Here is an example of a DMARC record with an RUF tag.

v=DMARC1; p=none; rua=mailto:dmarc_aggrepts@example.com; ruf=mailto:dmarc_forensicrepts@example.com

Forensic reports are sent immediately, rather than on a schedule, and they may or may not include the message body. They should always include the message headers.

Step 2 - Switch to Quarantine Mode

After reviewing your forensic reports and correcting any issues found, you can tell mailbox providers to quarantine any spoofed or phishing emails to the spam/junk email folder.

Use the p=quarantine tag in your DMARC record to tell others to quarantine unaligned mail from your domain.

v=DMARC1; p=quarantine

Step 3 - Increase Quarantine Percentages Incrementally Using the PCT=tag

After you've had time to monitor the aggregate reports, you can use the pct= tag to request that receiving mail servers only quarantine a small percentage of emails from your domain that are unaligned. In the first example, we're requesting that receiving mail servers only quarantine 1% of unaligned messages.

v=DMARC1; p=quarantine*; rua=mailto:dmarc_aggrepts@example.com; ruf=mailto:dmarc_forensicrepts@example.com; rf=afrf;* pct=1

Then, after you've had time to review additional reports and have corrected any issues found, you can gradually increase this percentage until you're comfortable enough to have receiving mail servers quarantine all unaligned messages from your domain.

v=DMARC1; p=quarantine*; rua=mailto:dmarc_aggrepts@example.com; ruf=mailto:dmarc_forensicrepts@example.com; rf=afrf;* pct=80

When you're ready to have receiving servers quarantine all unaligned messages from your domain, you can simply remove the pct=tag from your DMARC record.

CAUTION: *We do not recommend using p=reject mode. Using p=reject would increase the likelihood that legitimate messages sent from your domain are rejected in certain situations. It can also cause problems with mailing lists. Instead, use p=quarantine or p=none and review your DMARC reports so that you can make any changes necessary for messages from your domain to be in alignment with DMARC.*

Verifying DMARC Records for Inbound Mail

The following steps explain how to configure MDaemon to verify DMARC records for inbound mail.

Step 1 - Enabling DMARC Verification in MDaemon

To enable DMARC verification in MDaemon, navigate to **Security | Security Settings | Sender Authentication | DMARC Verification**, and check the first box "**Enable DMARC Verification and Reporting.**" [Figure 1-1]

As part of the DMARC verification process, MDaemon will first use SPF and/or DKIM to validate each message. Each message must pass at least one of these two methods in order to be in alignment for purposes of DMARC. If the message is aligned, then it will proceed normally through the rest of MDaemon's delivery and filtering processes. If the message fails both DKIM and SPF, however, then the fate of the message is determined by a combination of the domain's DMARC policy and how you have configured MDaemon to deal with those messages.

MDaemon then performs a DMARC DNS query on the domain found in the RFC 5322 From: field of each incoming message to determine whether or not the domain uses DMARC. If a DMARC DNS record is found, MDaemon will scan this record for its DMARC policy.

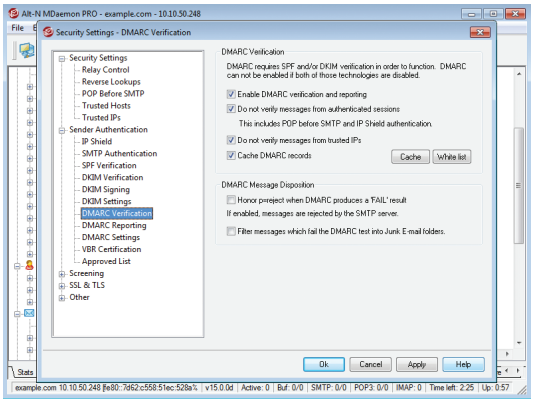

Figure 4-1

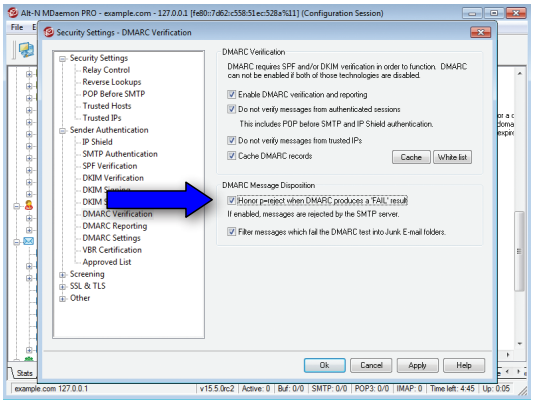

Figure 4-2

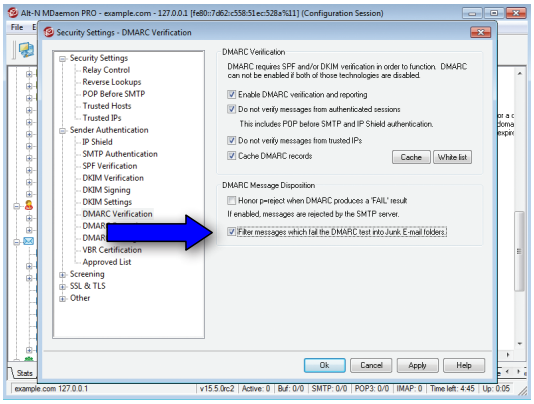

Figure 4-3

Step 2 - If the Message Fails DKIM and/or SPF Verification

1. **Policy p=none** - If a message fails DKIM and SPF verification and the DMARC domain has a policy of "p=none" then no punitive action will be taken and normal message processing will continue.
2. **Policy p=quarantine** - When a domain has a restrictive policy of "p=quarantine" MDaemon can optionally filter unaligned messages automatically to the receiving user's Junk E-mail folder. MDaemon will also insert a fail policy header, such as:
   X-MDDMARC-Fail-policy: quarantine
3. **Policy p=reject** - When a domain has a restrictive policy of "p=reject," and MDaemon has been configured to honor the p=reject tag when DMARC produces a FAIL result, unaligned messages will be rejected and the SMTP session will be terminated. If the option to honor p=reject is disabled, then instead of rejecting the message, MDaemaon can accept the message and insert an "X-MDDMARC-Fail-policy: reject" header into the message. You can then use the Content Filter to perform actions based on the presence of those headers, such as sending the message to a specific folder for further review. [Figure 4-2]

   You can optionally route all unaligned messages to the user's Junk Email folder. [Figure 4-3]

NOTE [for items 2 and 3 above]: *be careful when enabling the option to route unaligned messages to the user's Junk Email folder because if users are using POP, they won't have access to this junk email folder. They would need to be using IMAP (Outlook Connector included), ActiveSync, or WorldClient. When this is enabled, MDaemon will ask if it should create an IMAP filter rule for all users to route DMARC failed messages to the Junk Email folder.*

NOTE: *If you've enabled the option to Honor a policy of p=reject when DMARC produces a 'FAIL' result, messages will not be routed to the junk email folder because the SMTP sessions will be terminated.*

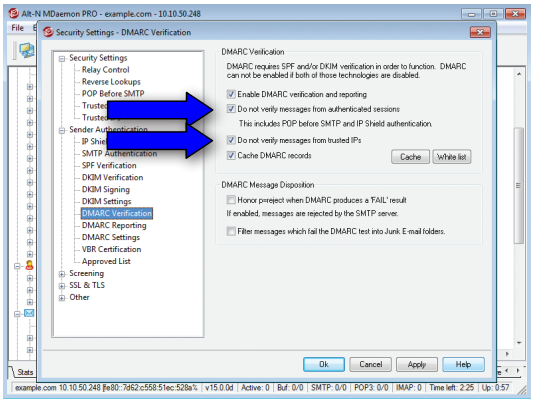

Figure 5-1

Step 3 - Exceptions

You can optionally skip DMARC verification for messages from authenticated sessions or trusted IPs. You can also optionally cache DMARC records for faster processing. [Figure 5-1]

Step 4 - Reporting

1. **Aggregate** - Check the box to allow MDaemon to send DMARC aggregate reports to domains that include an RUA= entry in their DMARC records. If no RUA entry exists, then the domain is not requesting these reports. With this option enabled, MDaemon will send aggregate reports to the address defined in the rua= entry of the public DMARC record of the sending domain. [Figure 5-2]
2. **Forensic/Failure** - Check the box to have MDaemon submit failure reports to domains that contain the ruf= entry in their public DMARC records. [Figure 5-2]

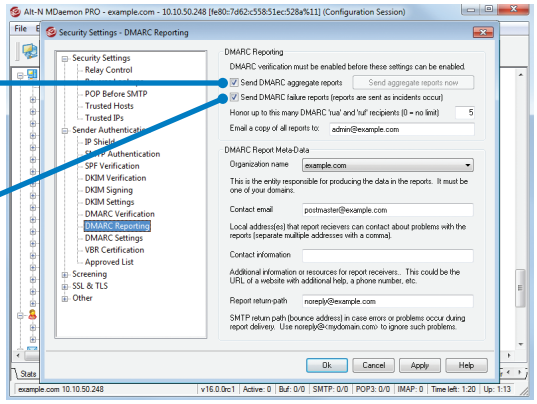

Figure 5-2

DMARC Settings

The DMARC Settings screen contains various options for including certain information in DMARC reports, logging DMARC DNS records, and updating the Public Suffix file used by MDaemon for DMARC.

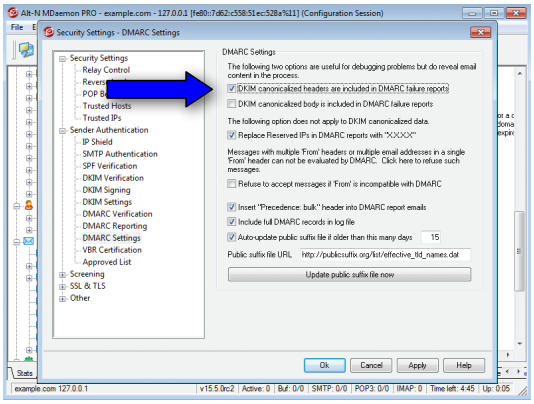

Figure 5-3

Step 1 - DKIM Canonicalized Headers are Included in DMARC Failure Reports

When this option is enabled, DKIM headers of messages that failed DKIM verification will be included in the DMARC failure reports that are sent to the domains that request them. [Figure 5-3]

Use this with caution: *This header information may include the message subject, which may contain sensitive information.*

Step 2 - DKIM Canonicalized Body is Included in DMARC Failure Reports

When this option is enabled, the body of the failed message will be included in the DMARC failure report to the domain that requested it.

NOTE: *The above options are useful for debugging, however, they do reveal email content when sending failure reports.*

Step 3 - Replace Reserved IPs in DMARC Reports with 'X.X.X.X'

This option is enabled by default to conceal reserved IPs in DMARC reports. Reserved IPs may include 127.0.0.*, 192.168.*.*, 10.*.*.*, and 172.16.0.0/12. [Figure 6-1]

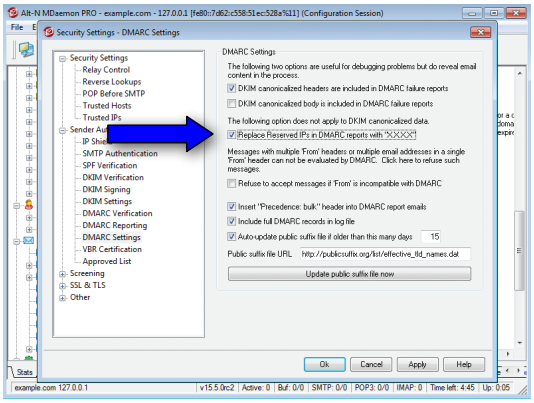

Figure 6-1

Step 4 - Automatically Update Public Suffix File if It's Older Than This Many Days

DMARC uses a public suffix file to reliably determine the proper domains to query for DMARC DNS records. By default, this file is updated when it's more than 15 days old. You can change this setting if you'd like to update this file more or less often. [Figure 6-2]

Click on **Update public suffix file now** to have MDaemon immediately update the suffix file at the URL specified.

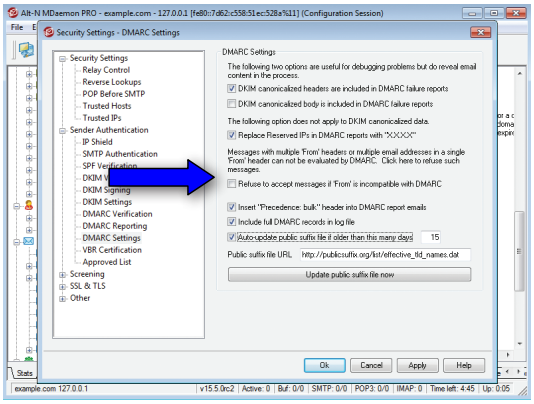

Figure 6-2

Summary

DMARC takes the guesswork out of determining what to do with messages that did not originate from the domain specified in the From field of the message. When a message fails DKIM and SPF lookups, DMARC allows domain administrators to tell receiving mail server administrators or mailbox providers what to do with the message, such as accept, quarantine, or reject the message. Forensic and aggregate reports allow domain administrators to see how, when and where their domain is being abused.

For a more technical, more thorough explanation of DMARC, including many examples of aligned and unaligned messages, you can view the complete lesson at www.dmarc.org.

MDaemon® technologies