MTA-STS Set Up Guide

1. Set up DNS records on your domain(s)

In order to set up MTA-STS for your domain(s), you need to set up two DNS records for each domain. The first record is either an A or CNAME record at mta-sts.<domain> that points to the web server (described below) that will serve your MTA-STS policy file.

You will then need to set up either a TXT or CNAME record at _mta-sts.<domain> that indicates that you use MTA-STS. This should be updated when you update your policy in order for it to take effect. Example content would be:

```
v=STSv1; id=20250929;
```

ID must be alphanumeric. We recommend to use the current date of which the policy has been set up.

2. MTA-STS Policy

The content of this policy file determines how a sending MTA attempts to deliver email to SMX before we send it on to you. You must ensure that:

- The policy file is a plain text file
- The web server has a valid certificate for the domain it is being hosted at (which is TLS 1.2 compliant)
- The web server listens on HTTPS
- The web server responds with a 200 OK, and not a redirect

The MTA-STS policy needs to be hosted on a web host at `https://mta-sts.<domain>/.well-known/mta-sts.txt`. Example content would be:

```
version: STSv1
mode: none
mx: mx1.nz.smxemail.com
max_age: 86400
```

To identify the correct MX records to use, use a DNS lookup. The potential options for SMX Customers are shown on the right banner of this guide.

3. TLS Reporting

TLS reporting is intended to provide recipient domains statistics and information from senders about their success/failure to negotiate a secure channel between the sender and the receiver. This is a companion piece to MTA-STS. We recommend using a dedicated reporting tool like OnDMARC to simplify the capture and visualisation of this information.

In order to set up TLS reporting you must add a TXT record at _smtp._tls.<domain>, that matches the following:

```
v=TLSRPTv1; rua=mailto:tlsreports@<domain>
```

Technically challenged or resource-constraint?

We understand MTA-STS implementation is complex, yet beneficial for businesses. Start using MTA-STS and DMARC with our expert-led managed services, Domain Protection Service and Red Sift's OnDMARC reporting and analysis tool.

Request a free consultation with SMX →

Our recommendations

We recommend that customers intending to introduce MTA-STS to their domains, do so as follows:

1. Check your MX records; these are what you would put into your policy.

2. Start with your policy being in the `testing` mode, this provides both the ability for senders to attempt delivery in a more secure way, while also falling back if necessary. Depending on your MX records, you'll need to select the two that apply to your business:

```
version: STSv1
mode: testing
mx: mx1.au.smxemail.com
mx: mx2.au.smxemail.com
mx: mx1.nz.smxemail.com
mx: mx2.nz.smxemail.com
mx: mx1.securemx.biz
mx: mx2.securemx.biz

max_age: 86400
```

3. Implement TLS Reporting. Along with the `testing` mode, this ensures that you are notified of any potential issues.

4. Eventually, after you are satisfied that you are receiving all mail, you can upgrade to the `enforce` mode.

Note: Remember to publish the `enforce` mode policy, and then update your DNS TXT entry for MTA-STS with a new ID