MTA-STS, TLS-RPT, and BIMI

EXPERT ADVICE ON GETTING STARTED, BEST PRACTICES, AND PIT FALLS TO AVOID

This is the third episode in a Zimbra webinar series that aims to demystify modern email authentication and email encryption for practical, everyday use.

A Brief Introduction

Randy Leiker

President and CEO of Skyway Networks

- 26 Years Of IT industry experience
- 23 Of Those Years at Skyway Networks
- Long history with Zimbra, dating back to Zimbra 5.0

Skyway Networks℠

Overview Of Today's Webinar

- MTA-STS
  - What Is MTA-STS?
  - Opportunistic Encryption Of Email
  - How To Setup MTA-STS By Example
- TLS-RPT
  - What Is TLS-RPT?
  - How To Setup TLS-RPT By Example
  - What Is In A Report?
- MTA-STS and TLS-RPT Best Practices
- MTA-STS and TLS-RPT Questions & Answers
- BIMI
  - What Is BIMI?
  - How To Setup BIMI By Example
  - BIMI Best Practices
  - BIMI Questions & Answers
- Wrap Up & Key Takeaways

This webinar is being recorded and will be posted on the Zimbra YouTube Channel at https://www.youtube.com/c/zimbra

Email Security Webinar Series

- **Earlier Topics (Available at https://www.youtube.com/c/zimbra):**
  - SPF & DKIM: these form the foundation on which modern email authentication operates and are the first key steps to protecting your outbound email and domain name's reputation.
  - DMARC: supercharges SPF & DKIM by providing enforcement of your email policies, with a powerful feedback mechanism.
- **Upcoming Topics**
  - DNSSEC: prevent your DNS infrastructure from being the weakest link in the security chain and defend yourself from a variety of spoofing and man-in-the-middle attacks.
  - TLS & DANE: an overview of how email encryption works, and how to overcome inherent weaknesses with the Certificate Authorities that issue SSL certificates by using certificate pinning.

What Is MTA-STS and Why Do You Need It?

- MTA-STS: Mail Transfer Agent Strict Transport Security
- Introduced in 2018 by Google, Oath, Microsoft and Comcast.
- Purpose:
  - Addresses vulnerabilities in the STARTTLS standard
  - Declares to email senders what should happen when email encryption fails
  - Defeats man-in-the-middle and email eavesdropping attacks

Opportunistic Encryption Of Email

- Used by 90% of email servers today
- The Essential Steps:
    1. Two mail servers connect using a plain-text, non-encrypted connection.
    2. Negotiate the features each server supports, including encryption.
    3. If encryption is available, use it to deliver an email, otherwise send as plain-text.

Source: https://transparencyreport.google.com/safer-email/overview

Opportunistic Encryption Illustrated

Jill: (Connects to mail.company.example with no encryption)

mail.zimbra.tech

mail.company.example

Opportunistic Encryption Illustrated

Jill: (Connects to mail.company.example with no encryption)

Chris: 220 mail.company.example welcomes you
Jill: EHLO mail.zimbra.tech
Chris: 250-STARTTLS

mail.zimbra.tech

mail.company.example

Opportunistic Encryption Illustrated

Jill: (Connects to mail.company.example with no encryption)

Chris: 220 mail.company.example welcomes you
Jill: EHLO mail.zimbra.tech
Chris: 250-STARTTLS

Jill: STARTTLS
Chris: 220 Ready to start TLS
... Upgrades to an encrypted connection …

mail.zimbra.tech

mail.company.example

Opportunistic Encryption Illustrated

mail.zimbra.tech

Jill: (Connects to mail.company.example with no encryption)

Chris: 220 mail.company.example welcomes you
Jill: EHLO mail.zimbra.tech
Chris: 250-STARTTLS

Jill: STARTTLS
Chris: 220 Ready to start TLS
... Upgrades to an encrypted connection …

Jill: EHLO mail.zimbra.tech
Chris: 250 mail.company.example loves encryption
Jill: MAIL FROM:<jill@zimbra.tech>
Chris: 250 OK
Jill: RCPT TO:<chris@company.example>
Chris: 250 Accepted
Jill: DATA (sends email)
Jill: QUIT

mail.company.example

Opportunistic Encryption Illustrated

mail.zimbra.tech

Jill: (Connects to mail.company.example with no encryption)

Chris: 220 mail.company.example welcomes you
Jill: EHLO mail.zimbra.tech
Chris: 250-STARTTLS

... Plain-text (non-encrypted) connection continues …

Jill: MAIL FROM:<jill@zimbra.tech>
Chris: 250 OK
Jill: RCPT TO:<chris@company.example>
Chris: 250 Accepted
Jill: DATA (sends email)
Jill: QUIT

mail.company.example

Opportunistic Encryption Under Attack

- Adversaries that eavesdrop on email are not always typical or expected

Source: http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/mobile-isp-thwarted-customers-attempts-to-send-encrypted-e-mails-research-finds

Opportunistic Encryption Under Attack

- Adversaries that eavesdrop on email are not always typical or expected
  - Cricket Wireless (owned by AT&T)

Source: http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/mobile-isp-thwarted-customers-attempts-to-send-encrypted-e-mails-research-finds

Opportunistic Encryption Under Attack

- Adversaries that eavesdrop on email are not always typical or expected
  - Cricket Wireless (owned by AT&T)
  - Employer Snooping

Source: http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/mobile-isp-thwarted-customers-attempts-to-send-encrypted-e-mails-research-finds

Mitigating Attacks Against STARTTLS

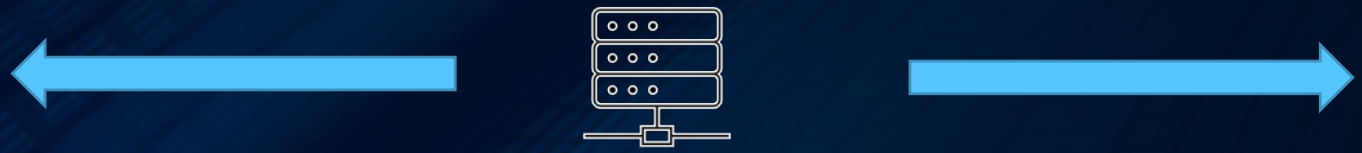
- SMTP was not built with security in mind.

Mitigating Attacks Against STARTTLS

- SMTP was not built with security in mind.
- STARTTLS introduced in 2002 and took 11 years to reach at least 30% usage on the Internet. Jumped to 60-70% in 2013, then to 90% today.

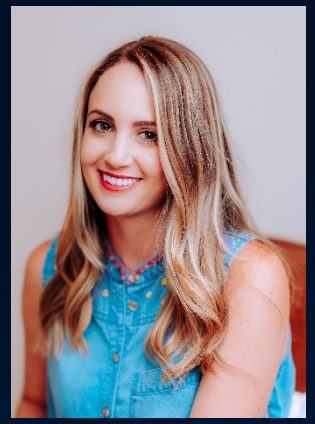
Mitigating Attacks Against STARTTLS

- SMTP was not built with security in mind.
- STARTTLS introduced in 2002 and took 11 years to reach at least 30% usage on the Internet. Jumped to 60-70% in 2013, then to 90% today.
- STARTTLS attacks are preventable: DANE and MTA-STS



Attacker (man-in-the-middle)
Blocking STARTTLS Commands

How To Setup MTA-STS By Example

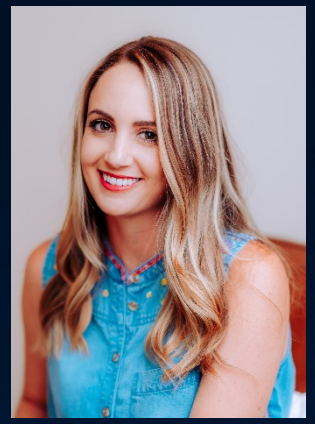


katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

How To Setup MTA-STS By Example

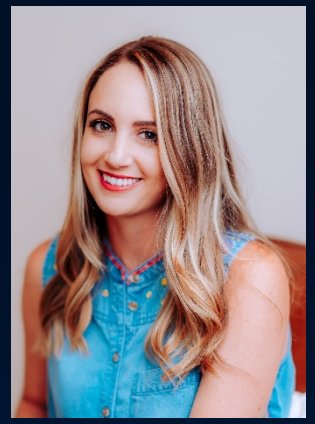


- MTA-STS Prerequisites:
  - Each email server requires a valid SSL certificate from a Certificate Authority.

mail1.zimbra.example

mail2.zimbra.example

How To Setup MTA-STS By Example



mail1.zimbra.example

mail2.zimbra.example

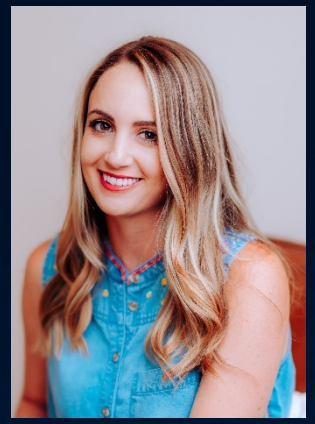
- MTA-STS Prerequisites:
  - Each email server requires a valid SSL certificate from a Certificate Authority.
  - STARTTLS (Opportunistic Encryption) must be available on each email server.

Ubuntu: sudo su - zimbra
Or for Red Hat: su - zimbra

zmprov gs `zmhostname` zimbraMtaTlsSecurityLevel
zmprov gs `zmhostname` zimbraMtaSmtpTlsSecurityLevel

zmprov ms `zmhostname` zimbraMtaTlsSecurityLevel may
zmprov ms `zmhostname` zimbraMtaSmtpTlsSecurityLevel may
zmmtactl restart

How To Setup MTA-STS By Example



mail1.zimbra.example

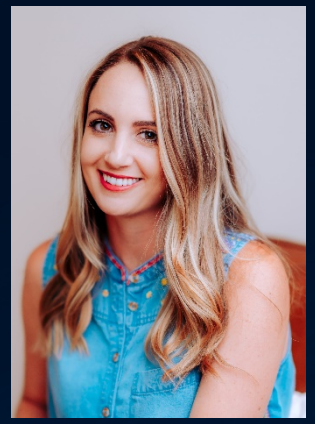
mail2.zimbra.example

- MTA-STS Prerequisites:
  - Each email server requires a valid SSL certificate from a Certificate Authority.
  - STARTTLS (Opportunistic Encryption) must be available on each email server.
  - TLS 1.2 or higher must be used on each email server.

zmprov gcf zimbraMtaSmtpdTlsProtocols

If zimbraMtaSmtpdTlsProtocols does not show >=TLSv1.2 then refer to:
https://wiki.zimbra.com/wiki/Cipher_suites#Configuring_Zimbra_MTA_Postfix

How To Setup MTA-STS By Example



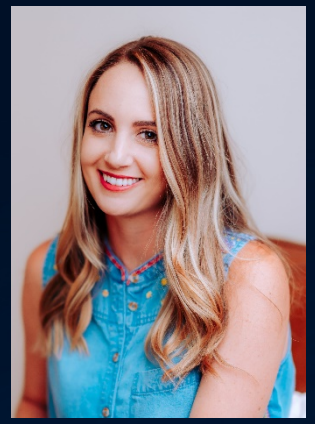
katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

- Publishing An MTA-STS Policy
  - Create a web site called https://mta-sts.zimbra.example
    - Required format: https://mta-sts.[email-domain-name]
  - Sub-domain example: katie@mail.zimbra.example:
    - https://mta-sts.mail.zimbra.example

How To Setup MTA-STS By Example



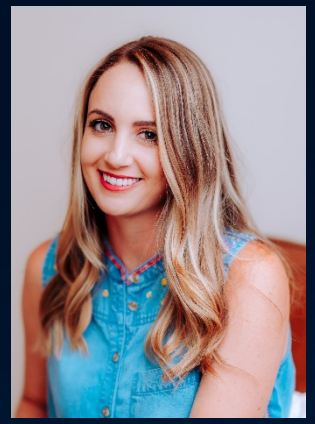
katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt

How To Setup MTA-STS By Example



katie@zimbra.example

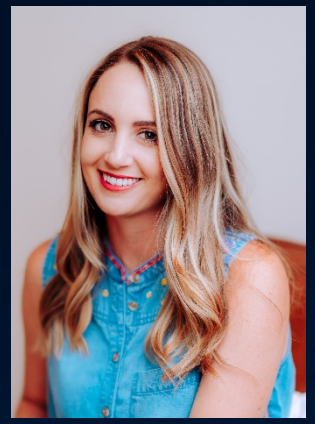
mail1.zimbra.example

mail2.zimbra.example

- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt
  - With this content:

    version: STSv1

How To Setup MTA-STS By Example



katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

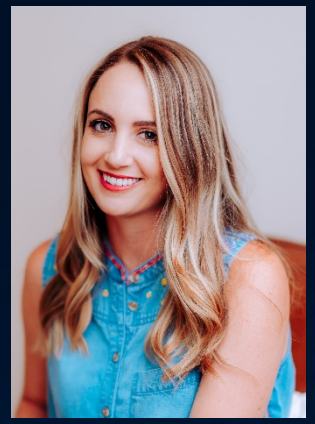
- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt
  - With this content:

    version: STSv1
    mode: testing

Available Mode Options:

- **None:** ignore this MTA-STS policy.
- **Testing:** senders should report how this policy would be applied to email, but the policy is otherwise ignored.
- **Enforce:** senders should enforce the requirement for email sent to Katie's email server to always use encryption.

How To Setup MTA-STS By Example



katie@zimbra.example

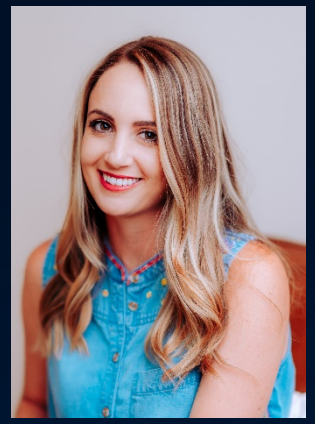
mail1.zimbra.example

mail2.zimbra.example

- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt
  - With this content:

```
version: STSv1
mode: testing
mx: mail1.zimbra.example
mx: mail2.zimbra.example
```

How To Setup MTA-STS By Example



katie@zimbra.example

- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt
  - With this content:

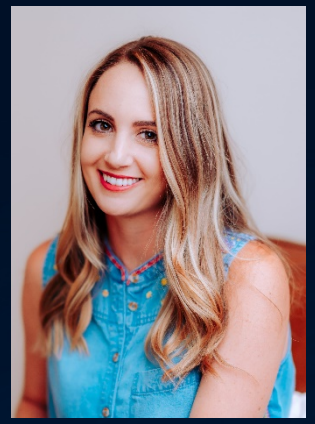
mail1.zimbra.example

mail2.zimbra.example

version: STSv1
mode: testing
~~mx: mail1.zimbra.example~~
~~mx: mail2.zimbra.example~~
mx: *.zimbra.example

The *.zimbra.example wildcard does not include sub-domains like: west.mail1.zimbra.example

How To Setup MTA-STS By Example



katie@zimbra.example

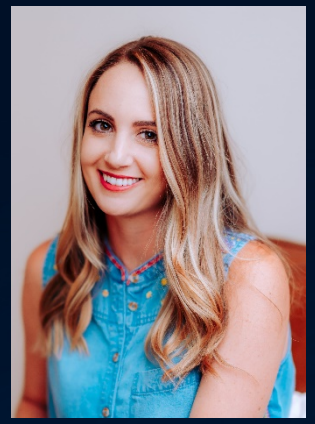
mail1.zimbra.example

mail2.zimbra.example

- Publishing An MTA-STS Policy
  - Create a text file at:
    - https://mta-sts.zimbra.example/.well-known/mta-sts.txt
  - With this content:

```
version: STSv1
mode: testing
mx: mail1.zimbra.example
mx: mail2.zimbra.example
max_age: 31557600
```

How To Setup MTA-STS By Example



katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

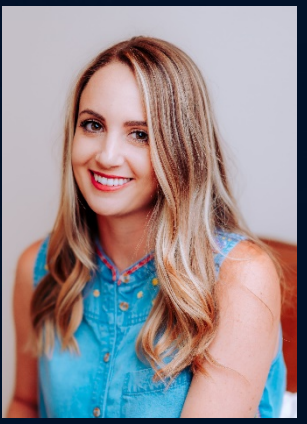
- Publishing An MTA-STS DNS Record
  - Record Type: DNS TXT
  - Host name: _mta-sts.zimbra.example
  - Content
    v=STSv1; id=2022051001;

The id value can be any alphanumeric string, but consider using a format of: YYYYMMDDNN where:

- YYYY: calendar year
- MM: calendar month
- DD: calendar day
- NN: revision number

Re-Visited: Attacks Against STARTTLS With MTA-STS

mail.company.example



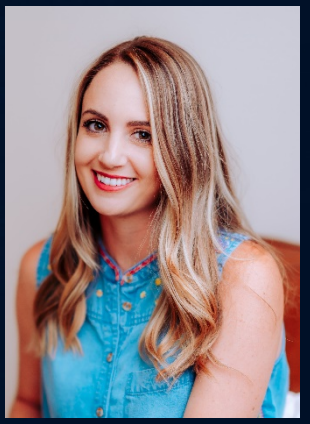
mail1.zimbra.example

version: STSv1
mode: enforce
mx: mail1.zimbra.example
mx: mail2.zimbra.example
max_age: 31557600

Re-Visited: Attacks Against STARTTLS With MTA-STS

mail.company.example

Chris: (requests Katie's DNS record for _mta-sts.zimbra.example)
Katie: v=STSv1; id=2022051001; (no change from cached copy)



mail1.zimbra.example

version: STSv1
mode: enforce
mx: mail1.zimbra.example
mx: mail2.zimbra.example
max_age: 31557600

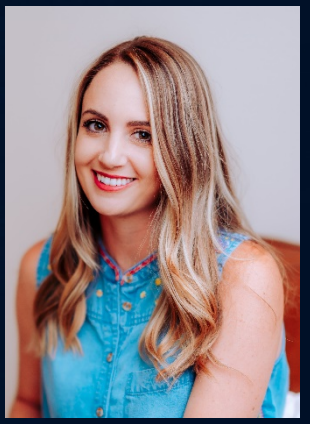
Re-Visited: Attacks Against STARTTLS With MTA-STS

mail.company.example

Chris: (requests Katie's DNS record for _mta-sts.zimbra.example)
Katie: v=STSv1; id=2022051001; (no change from cached copy)

Chris: (Connects to mail1.zimbra.example with no encryption)

Katie: 220 mail1.zimbra.example says how are you
Chris: EHLO mail.company.example
Katie: 250-STARTTLS



mail1.zimbra.example

version: STSv1
mode: enforce
mx: mail1.zimbra.example
mx: mail2.zimbra.example
max_age: 31557600

Re-Visited: Attacks Against STARTTLS With MTA-STS

mail.company.example

Chris: (requests Katie's DNS record for _mta-sts.zimbra.example)
Katie: v=STSv1; id=2022051001; (no change from cached copy)

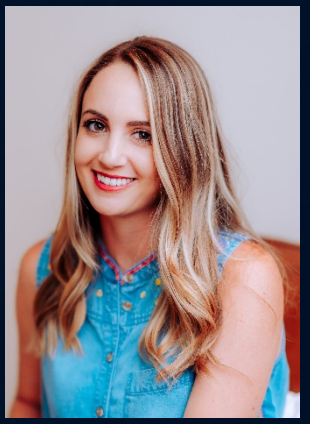
Chris: (Connects to mail1.zimbra.example with no encryption)

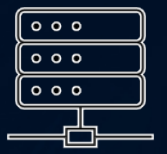
Katie: 220 mail1.zimbra.example says how are you
Chris: EHLO mail.company.example
Katie: 250-STARTTLS

Chris: STARTTLS
~~**Katie:** 220 Ready to start TLS~~ (blocked by hacker)
Hacker: 454 TLS not available due to temporary reason

Response is non-compliant with Katie's MTA-STS policy, so Chris immediately drops the connection instead of continuing with a plain-text email delivery.

Chris: QUIT





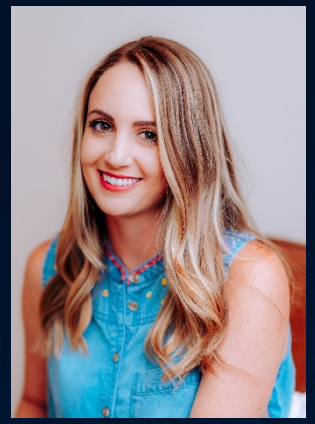
mail1.zimbra.example

version: STSv1
mode: enforce
mx: mail1.zimbra.example
mx: mail2.zimbra.example
max_age: 31557600

What Is TLS-RPT and Why Do You Need It?

- TLS-RPT: Transport Layer Security Reporting
- Introduced in 2018 by same authors of the MTA-STS standard
- Purpose:
  - Provides feedback loop of sender’s successful & failed email deliveries.
  - An early warning system of configuration errors on your email server, or attacks that are underway.

How To Setup TLS-RPT By Example



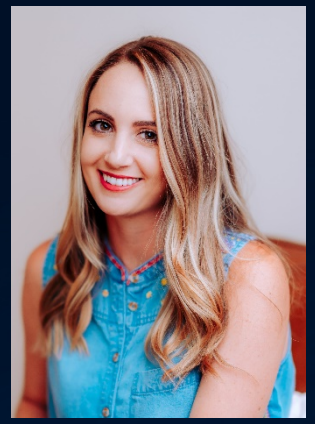
katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

- Publishing An TLS-RPT DNS Record
  - Record Type: DNS TXT
  - Host name: _smtp._tls.zimbra.example
  - Content
    v=TLSRPTv1; rua=mailto:tlsreports@zimbra.example

How To Setup TLS-RPT By Example



katie@zimbra.example

mail1.zimbra.example

mail2.zimbra.example

- Publishing An TLS-RPT DNS Record
  - Record Type: DNS TXT
  - Host name: _smtp._tls.zimbra.example
  - Content
    v=TLSRPTv1; rua=mailto:tlsreports@zimbra.example

The rua keyword can be configured to send to any domain, for example: reports@somewhere.company. Unlike DMARC, no additional DNS TXT record is needed on the somewhere.company domain to enable this reporting.

What Do The Reports Contain?

- Reports are sent every 24 hours as gzipped text files attached to emails.
  - Free tools like 7-Zip (https://www.7-zip.org) can be useful for opening the compressed files on Windows.
- Reports will be formatted in JSON
  - Search online for “JSON parser” where many tools are available to help re-format the reports into a human readable form.

What Do The Reports Contain?


```
{
    "organization-name": "Google Inc.",
    "date-range": {
        "start-datetime": "2022-05-10T00:00:00Z",
        "end-datetime": "2022-05-10T23:59:59Z"
    },
    "contact-info": "smtp-tls-reporting@google.com",
    "report-id": "2022-05-08T00:00:00Z_zimbra.example",
    "policies": [
        {
            "policy": {
                "policy-type": "sts",
                "policy-string": [
                    "version: STSv1",
                    "mode: enforce",
                    "mx: mail1.zimbra.example",
                    "mx: mail2.zimbra.example",
                    "max_age: 31557600"
                ],
                "policy-domain": "zimbra.example"
            },
            "summary": {
                "total-successful-session-count": 15,
                "total-failure-session-count": 0
            }
        }
    ]
}
```

What Do The Reports Contain?


```
{
    "organization-name": "Google Inc.",
    "date-range": {
        "start-datetime": "2022-05-10T00:00:00Z",
        "end-datetime": "2022-05-10T23:59:59Z"
    },
    "contact-info": "smtp-tls-reporting@google.com",
    "report-id": "2022-05-10T00:00:00Z_zimbra.example",
    "policies": [
        {
            "policy": {
                "policy-type": "sts",
                "policy-string": [
                    "version: STSv1",
                    "mode: enforce",
                    "mx: mail1.zimbra.example",
                    "mx: mail2.zimbra.example",
                    "max_age: 31557600"
                ],
                "policy-domain": "zimbra.example"
            },
            "summary": {
                "total-successful-session-count": 11,
                "total-failure-session-count": 4
            },
            "failure-details": [
                {
                    "result-type": "certificate-expired",
                    "sending-mta-ip": "209.136.73.254",
                    "receiving-mx-hostname": "mta2.zimbra.example",
                    "receiving-mx-helo": "mta2.zimbra.example",
                    "receiving-ip": "64.200.180.2",
                    "failed-session-count": 4
                }
            ]
        }
    ]
}
```


Report documentation: https://datatracker.ietf.org/doc/html/rfc8460#section-4.4

MTA-STS and TLS-RPT Best Practices

- **Best Practice # 1:** Before publishing an MTA-STS policy, ensure these prerequisites are met. All mail servers included in your DNS MX records must:

  1. Have valid SSL certificates issued by a Certificate Authority.

  2. Have SSL certificates that exactly match both the server's host name and DNS MX record names.

  3. Support an encryption protocol of at least TLSv1.2 or higher. MTA-STS does not have a minimum encryption cipher requirement, but consider using only strong ciphers, as described here: https://wiki.zimbra.com/wiki/Cipher_suites#Configuring_Zimbra_MTA_Postfix

  4. Have Opportunistic Encryption (STARTTLS) support enabled. Preferably this should apply to both inbound & outbound email servers. The Zimbra commands to check this were included earlier in the webinar.

MTA-STS and TLS-RPT Best Practices

- **Best Practice # 2:** When publishing your MTA-STS policy, ensure that your web server has:

    1. A valid SSL certificate issued by a Certificate Authority for mta-sts.[your-domain]. For example: mta-sts.zimbra.example. For a sub-domain, this would be mta-sts.[your-sub-domain].

    2. An encryption protocol configured of at least TLSv1.2 or higher. This Mozilla site: https://ssl-config.mozilla.org can help you select strong encryption ciphers too for your web server too.

MTA-STS and TLS-RPT Best Practices

- **Best Practice # 3:** Choose the mode and max_age values for your MTA-STS policy carefully.
  - When first getting started with MTA-STS, always start with a mode setting of “testing” in your MTA-STS policy. The “none” mode can safely be skipped.
  - Immediately follow this up by configuring TLS-RPT to begin monitoring the results of how email senders will apply your MTA-STS policy.
  - Consider collecting a minimum of 1 week of monitoring data via TLS-RPT before progressing from testing to enforce mode. Larger email sending domains may need a minimum of several weeks of monitoring data.
  - Set the max_age keyword in your MTA-STS policy to a minimum of at least a few weeks, if not several months. Should email senders be unable to access your MTA-STS DNS record for some period of time, this ensures consistent application of your MTA-STS policy as email senders will cache this information.

MTA-STS and TLS-RPT Best Practices

- **Best Practice # 4:** Use a report summarization tool for automatically parsing TLS-RPTs.
    - Similar to DMARC aggregate reports, you may find that the number of TLS-RPTs received over time steadily increases as more email senders adopt MTA-STS.

MTA-STS and TLS-RPT Best Practices

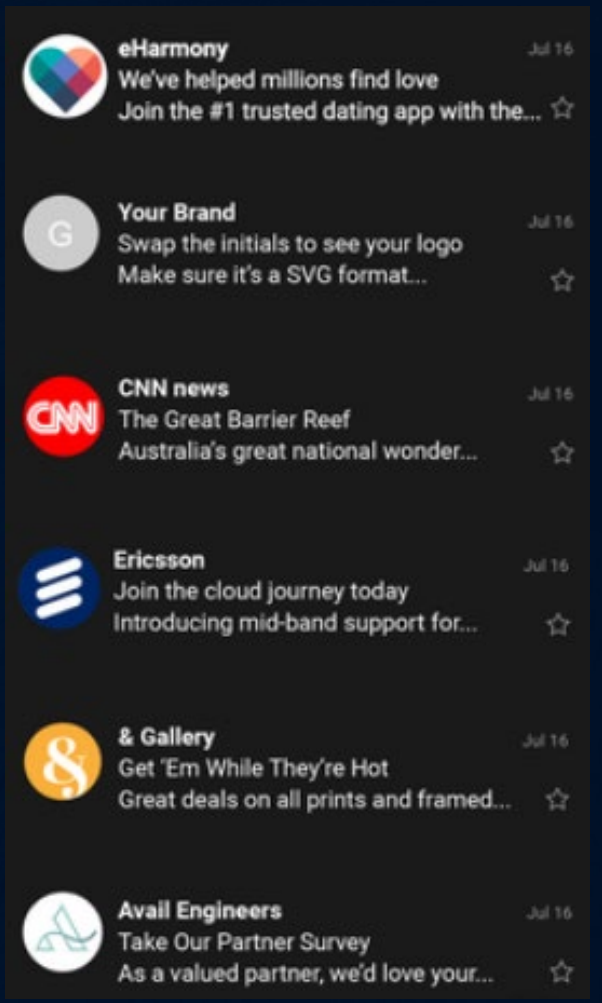
- **Best Practice # 5:** Avoid duplicate MTA-STS and TLS-RPT records in your DNS zone.
  - Consider this example:
    - Host name: _mta-sts.zimbra.example
    - Content: v=STSv1; id=2022022401;
    - Host name: _mta-sts.zimbra.example
    - Content: v=STSv1; id=2022051701;
  - Email senders will treat this duplication as if you have no MTA-STS policy published at all.

MTA-STS and TLS-RPT Questions

Up Next: BIMI

What Is BIMI and When Should You Use It?

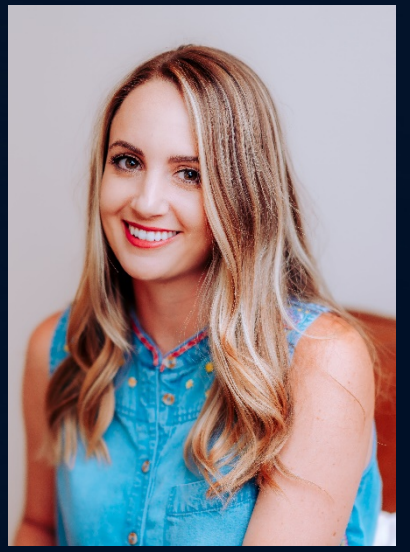
- BIMI: Brand Indicators for Message Identification
- Introduced in 2021 by Valimail, Skye Logicworks, and Fastmail.
- Purpose:
  - Provides a standardized means for organizations to request that email providers display their brand logo next to emails the organization sends to recipients.
  - Provides trademark owners with a means to attest that they have the rights to use a logo.



What Is BIMI and When Should You Use It?

- BIMI: Brand Indicators for Message Identification
- Introduced in 2021 by Valimail, Skye Logicworks, and Fastmail.
- Purpose:
  - Provides a standardized means for organizations to request that email providers display the organization's brand logo next to emails the organization sends to recipients.
  - Provides trademark owners with a means to attest that they have the rights o use a logo.

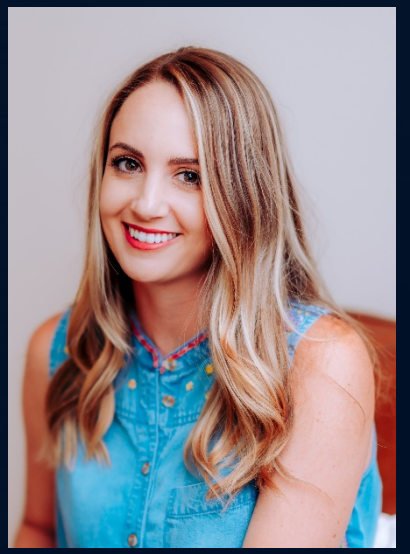
How To Setup BIMI By Example



- Step 1.) Katie imports her company logo into Adobe Illustrator.
- Step 2.) With assistance from a graphic designer, her logo is cropped so that it fits within a perfect square & is less than 32 KB in size.

- Step 3.) Katie will need to work with her graphic design to make a few additional manual tweaks to her logo, as described on this page: https://bimigroup.org/creating-bimi-svg-logo-files/

How To Setup BIMI By Example

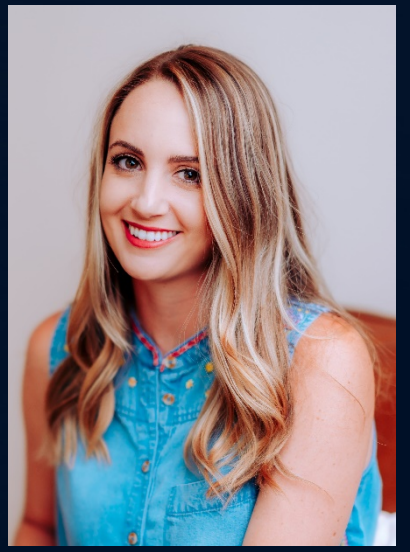


- Step 4.) Katie uploads the SVG file containing her company's logo to her web server. BIMI requires the logo to be served with HTTPS only, but it may be served from any web site domain.

- Step 5.) Katie next creates a new DNS TXT record of:

- Host name: default._bimi.zimbra.example
- Content: v=BIMI1; l=https://zimbra.example/logo.svg;

How To Setup BIMI By Example



- Step 6.) If Katie has trademarked her company logo, as an optional step, she can also obtain a digital certificate where a Certificate Authority verifies that she owns the trademark. Presently this service is provided by 2 CAs: Digicert and Entrust DataCard.

- Once she has her digital certificate, she would modify her DNS record with:

- Host name: default._bimi.zimbra.example
- Content: v=BIMI1; l=https://zimbra.example/logo.svg; a=https://zimbra.example/mark.pem;

BIMI Questions

Up Next: Key Take Aways

Key Take Aways

- Before publishing your first MTA-STS policy, carefully check that all of the prerequisites described earlier in this webinar have been met. If any are skipped, this will often result in your MTA-STS policy being ignored by email senders.

- Use a large max_age value in your MTA-STS policy to limit exposure to short term DNS outages that could cause email senders to ignore the published policy. You can always override this at anytime by changing the id value in the MTA-STS DNS TXT record.

- Before attempting to setup BIMI, ensure that you have DMARC setup with a policy of at least quarantine or reject. If DMARC policy of none is in use, them your BIMI DNS record will be ignored.

Thank You For Attending Today's Webinar!

Speaker's Contact Information

Randy Leiker
Skyway Networks
randy@skywaynetworks.com
https://skywaynetworks.com