Preparing to Implement Cyber Warden Mail Aegis

The implementation process for Mail Aegis is straightforward, but for it to be as seamless as possible, we need to prepare to make the cut over as quick and easy as possible.

The migration will be in a couple of phases – first, we need to make a few minor changes (that won't impact your users at all). We will gather other information in the background.

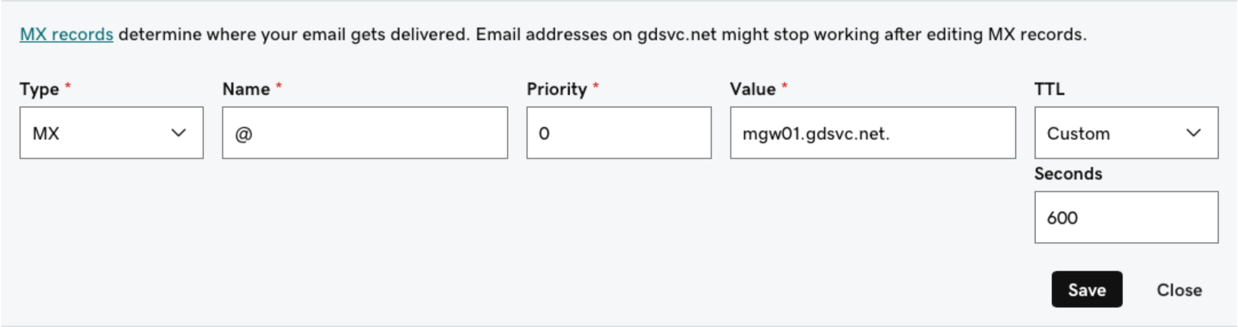
The screenshots in this document are for illustrative purposes only. Your DNS control panel likely looks different but will have similar functionality. If in doubt, don't change anything and ask for help from someone familiar with DNS. We can also provide guidance.

Dmarcian Account

If Advanced DMARC monitoring has been selected, an invitation will have been sent to you to setup an account at Dmarcian. Please complete the sign-up process.

MX Records

On your DNS control panel, change the Time to Live (TTL) for each MX record (you will likely have 2 or 3 of these) to a short time like 10 minutes/600 seconds. Don't change anything else in the MX records.



MX records determine where your email gets delivered. Email addresses on gdsvc.net might stop working after editing MX records.

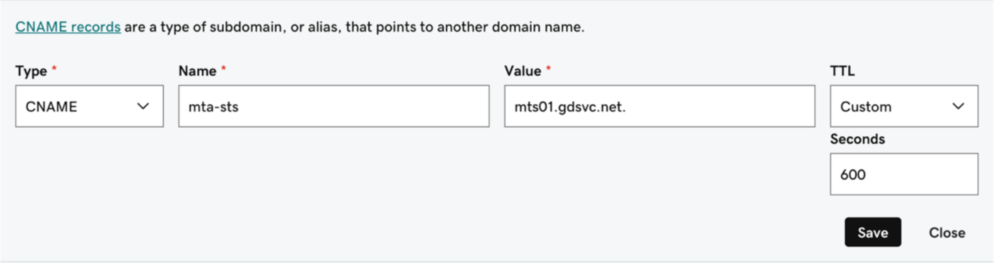
Type *	Name *	Priority *	Value *	TTL
MX	@	0	mgw01.gdsvc.net.	Custom

Seconds: 600

MTA-STS Record

Again, in the DNS control panel, create a CNAME record as below. The TTL doesn't really matter for this one at this stage – just use the default. This record needs to be created before we can proceed with the next step.

The relevant data is:
Type: CNAME
Name: mta-sts
Value: mts01.gdsvc.net



CNAME records are a type of subdomain, or alias, that points to another domain name.

Type *	Name *	Value *	TTL
CNAME	mta-sts	mts01.gdsvc.net.	Custom

Seconds: 600

Google Workspace DKIM setup

If your mail is hosted on Google Workspace, then follow the instructions below.
https://support.google.com/a/answer/180504?hl=en&ref_topic=2752442&sjid=8893866233010802736-EU

Microsoft M365 DKIM setup

If your mail is hosted on Microsoft M365/O360 then follow the instructions below.

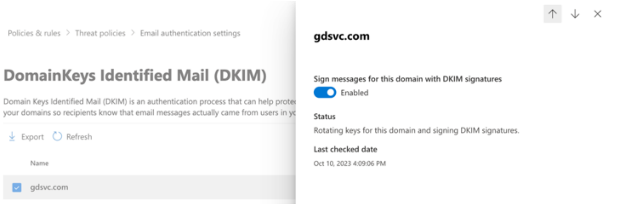
Create DKIM Records

1. Login at security.microsoft.com/dkimv2
2. **Select the domain** that you are sending mail from.
3. Click **Create DKIM Keys.**
4. Take note of the values displayed (copy/paste them into a text document)
5. In your **DNS console**, create a CNAME record for each of the values displayed in the previous step

You will now need to wait a few minutes or a few hours depending on how quickly your DNS provider publishes updates.

Enable DKIM Signing

1. Login at security.microsoft.com/dkimv2
2. **Select the domain** that you are sending mail from.
3. Enable "Sign messages for this domain with DKIM signatures"


Policies & rules > Threat policies > Email authentication settings
Export
Refresh
Name

DomainKeys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is an authentication process that can help prote your domains so recipients know that email messages actually came from users in yo

☑ gdsvc.com

gdsvc.com

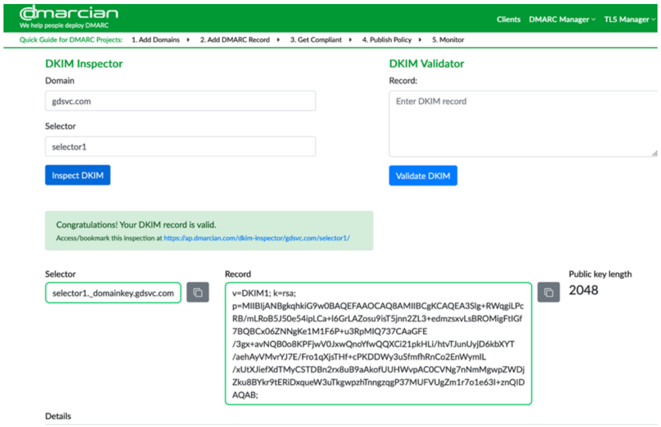
Sign messages for this domain with DKIM signatures
● Enabled

Status
Rotating keys for this domain and signing DKIM signatures.

Last checked date
Oct 10, 2023 4:09:06 PM

Validate DKIM

Validate your DKIM config at https://ap.dmarcian.com/dkim-inspector/
For Microsoft Customers, the selector is selctor1 or selector 2 (check both)
For Google customers, the selector is google.



DKIM Inspector

Domain: gdsvc.com

Selector: selector1

DKIM Validator

Record: Enter DKIM record

Congratulations! Your DKIM record is valid.
Access/bookmark this inspection at https://ap.dmarcian.com/dkim-inspector/gdsvc.com/selector1/

Selector: selector1._domainkey.gdsvc.com

Record:

```
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Slg+RWqgiLPc
RB/mLRoB5J50e54ipLCa+l6GrLAZosu9isT5jnn2ZL3+edmzsxvLsBROMigFtIGf
7BQBCx06ZNNgKe1M1F6P+u3RpMIQ737CAaGFE
/3gx+avNQB0o8KPFjwV0JxwQnoYfwQQXCi21pkHLi/htvTJunUyjD6kbXYT
/aehAyVMvrYJ7E/Fro1qXjsTHf+cPKDDWy3uSfmfhRnCo2EnWymlL
/xUtXJiefXdTMyCSTDBn2rx8uB9aAkofUUHWvpAC0CVNg7nNmMgwpZWDj
Zku8BYkr9tERiDxqueW3uTkgwpzhTnngzqgP37MUFVUgZm1r7o1e63I+znQID
AQAB;
```

Public key length: 2048

Next Steps

Now you’re ready for us to provision everything on our end – That will happen soon after you notify us that you’ve completed these steps. We will confirm that everything looks OK from our end, and then proceed with the next step on our end, then we will ask you to make some more changes in DNS.

MultiFactor Authentication (MFA)

In the meantime, you should make a start on enabling MFA on everything, starting with your email platform (because email is the key to everything else).
We recommend the use of security keys and Authenticator Apps. We strongly discourage prompt based authentication (unless a number needs to be input), email, call, or text based options, and we also discourage the use of backup codes.

Our preferred Authenticator app is Microsoft Authenticator.
Our preferred physical security key is the Yubikey from Yubico

Enable MFA on Microsoft M365 https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/multi-factor-authentication-microsoft-365?view=o365-worldwide
Enable MFA on Google Workspace
https://support.google.com/a/answer/175197?hl=en&ref_topic=2759193&sjid=1474563880529334508-EU

Once MFA is configured on your Microsoft / Google platforms, you should implement it on all other platforms, especially bank accounts, Accounting/finance applications, etc.

On PCs, laptops, tablets, phones, etc, we recommend implementing biometric authentication (finger print or face recognition). We do not recommend pin or pattern based authentication.

If you need any help implementing MFA or obtaining security keys, we can help.

Thanks again,
The Cyber Warden team.

Glossary

DNS: Domain Name System. This is what translates names (like cyberwarden.io) into IP addresses (e.g. 76.223.105.230).

CNAME Record: A Canonical Name record is an alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.

A Record: An A record (or AAAA record for IPv6) is the record that translates a name into an IP address.

MX Record: Mail Exchanger. These records are prioritized – when one MX forwards mail from one domain to another, it will try the destination domain's MX record with the lowest priority number first. If that is not available, then it will try the next highest, and so on. If it can't get a successful connection to any destination MX, it will wait a few minutes before trying again.

MTA-STS: MTA-STS is short for SMTP MTA-STS, which is short for Simple Mail Transfer Protocol (SMTP) Mail Transfer Agent (MTA) Strict Transport Security (STS). The purpose of MTA-STS is to encrypt and secure communications between SMTP servers via TLS (Transport Layer Security) preventing man-in-the-middle attackers from viewing and manipulating in-transit emails.
Read more on this at https://dmarcian.com/mta-sts/