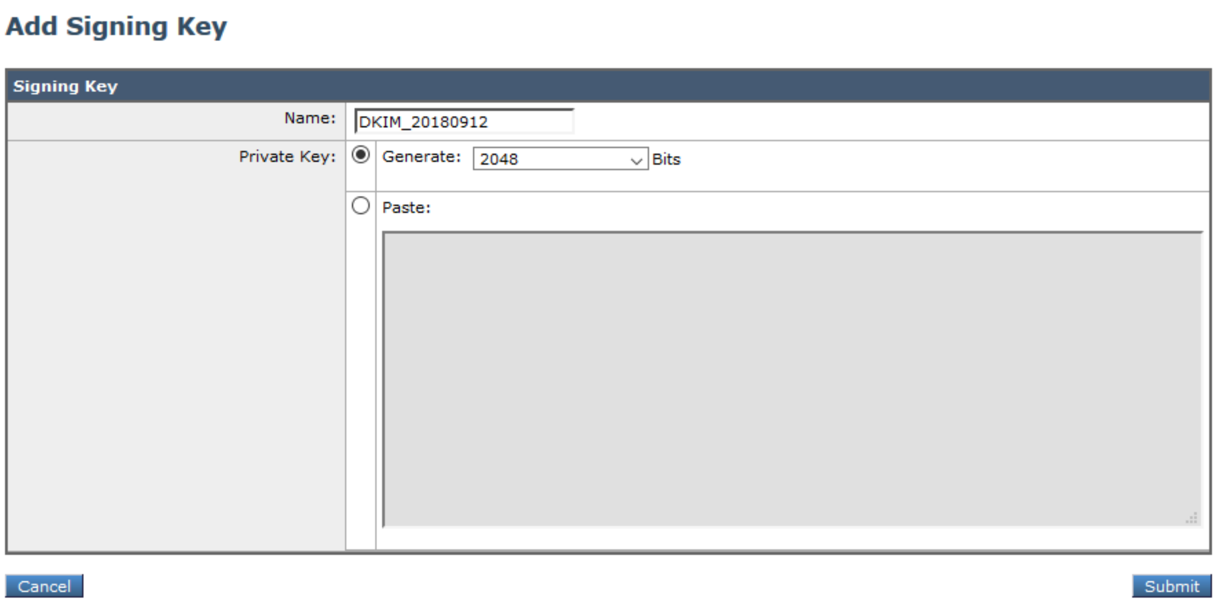
Best practices for configuring DKIM and DMARC on Cisco AsyncOS

Configure DKIM signing

DKIM signing should be enabled for all outgoing email on all domains. These domains can share the same DKIM public-private key pair using CNAME DNS records.

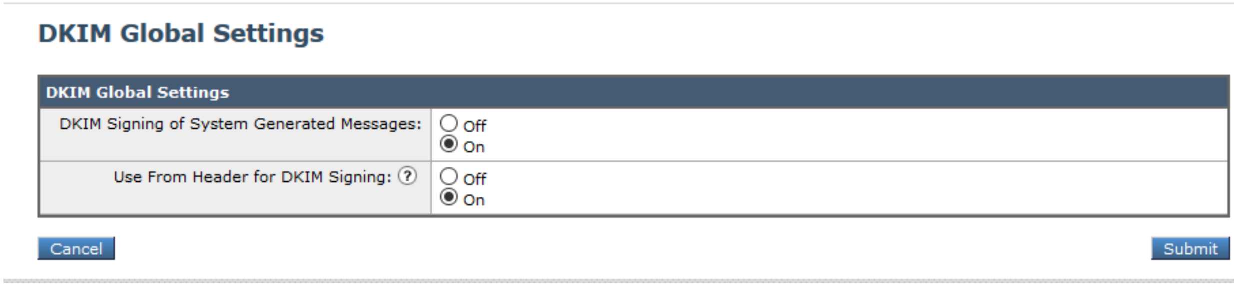
Create a new signing key pair

1. Go to Mail Policies > Signing Keys
2. Click Add Key
3. Use DKIM_YYYYMMDD as the format for the key name
4. Use a 2048-bit key length
5. Click submit



Configure global DKIM settings

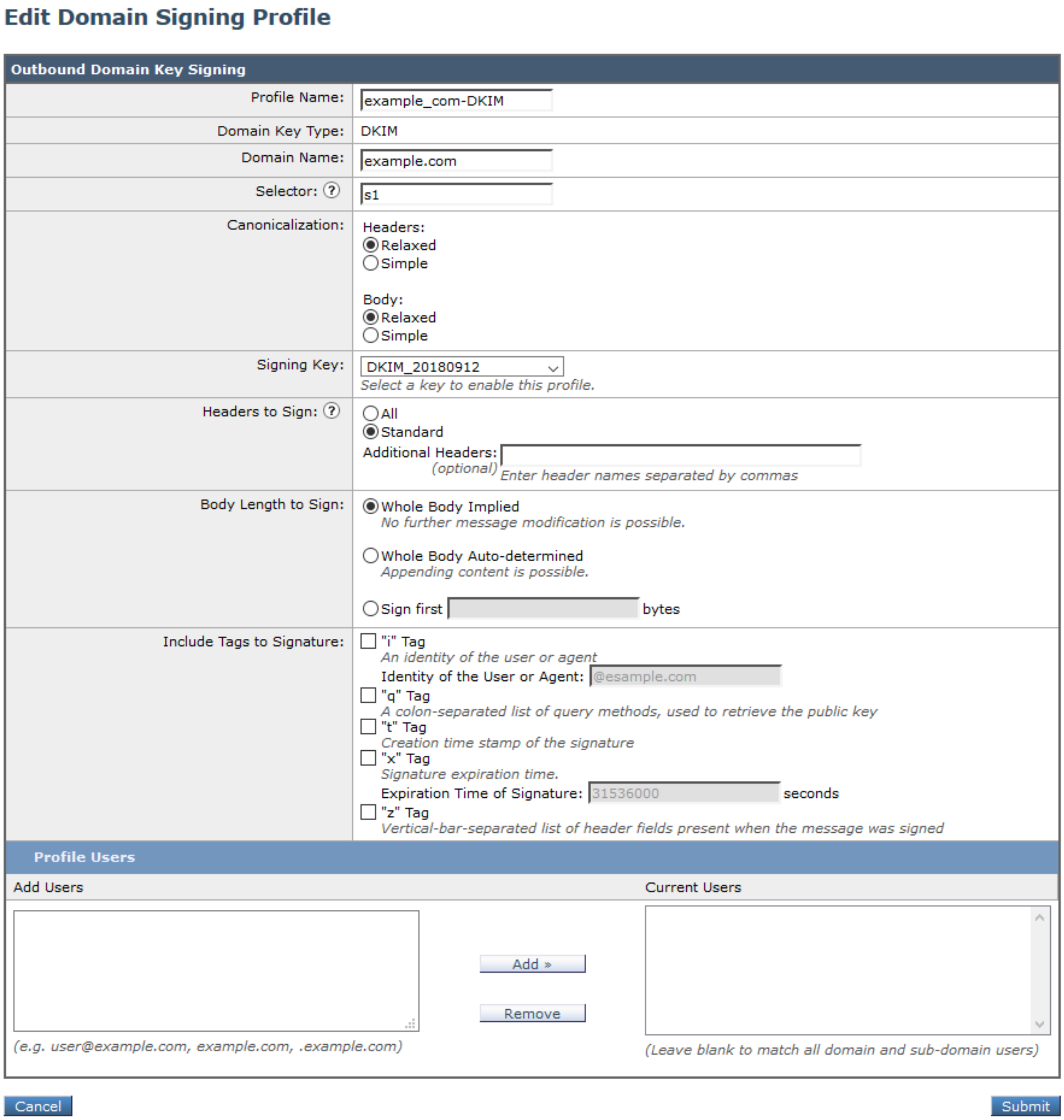
1. Go to Mail Policies> Signing Profiles
2. Under DKIM Global Settings, click Edit Settings
3. Set DKIM Signing of System Generated Messages to **Yes**
4. Set use From Header for DKIM signing to **Yes**
5. Click submit



Create a separate signing profile for each mail domain/subdomain

1. Go to mail Policies> Singing Profiles
2. In the Domain Signing Profiles section, click Add Profile
3. Enter a name for the signing profile (e.g. example_com-DKIM)
4. Select **DKIM** as the Domain Key Type
5. Enter the domain name
6. Use **s1** as the selector (or another arbitrary name if another service already uses s1)
7. Select **relaxed** for the header canonicalization (This allows for variations in whitespace)
8. Select **relaxed** for the body canonicalization (This allows for variations in whitespace)
9. Select the signing key
10. Configure the profile to sign the **Standard** headers. This configures the gateway to only sign the following headers, so that DKIM will still pass when other mail systems add other, non-standard headers in transit (e.g. debugging headers):
    - From
    - Sender, Reply To-
    - Subject
    - Date, Message-ID
    - To, Cc
    - MIME-Version
    - Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description
    - Resent-Date, Resent-From, Resent-Sender, Resent-To, Resent-cc, Resent-Message-ID
    - In-Reply-To, References
    - List-Id, List-Help, List-Unsubscribe, List-Subscribe, List-Post, List-Owner, List-Archive
11. Specify **Whole Body Implied** for body signing
12. **Uncheck** all tags to include in the signature

13. Leave the users field blank
14. Click Submit



Add the public key for the DKIM to the primary domain

To generate the needed DNS record, go to Mail Policies> Signing Profiles. Then, in the Domain Signing Profiles Section, locate the row for the signing profile of your primary domain, then click on the Generate link in the DNS TXT Records column. The record will look like this:

```
s1._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=<public key>"
```

Lines in DNS TXT records are truncated at 256 characters. The key must be split into separate lines in the same record to be valid.

Create CAME records on the other domains

The allows these domains to the same key and selectors as the primary domain

```
s1._domainkey.example.net CNAME s1._domainkey.example.com
s2._domainkey.example.net CNAME s2._domainkey.example.com
```

Always add a s2 CNAME record, even though s2 selector or key has not been created on the primary domain yet. It makes any key rotation that may need to be done in the future much easier.

DKIM key rotation

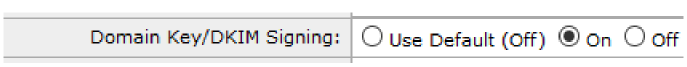
If you ever need to rotate the keys, use this ping-pong key rotation scheme to ensure that email is always signed with a valid, secure key.

Unless a key is known to have been compromised, it is important to wait a week (i.e. 7 days) before replacing it, as some receiving mail servers will cache the public key at a given selector for up to a week.

1. Start exclusively signing with the other selector
2. Wait 7 days
3. Replace the key at the old selector so it is ready for the next rotation
4. Go to step 1

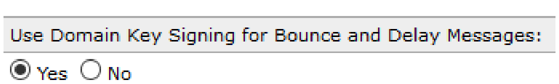
Enable signing for outgoing mail

1. Go to Mail Policies> Mail Flow Policies
2. Click on the RELAYED (i.e. outgoing) mail flow policy (or create it if it does not exist)
3. In the Security Features section, set DomainKeys/DKIM Signing to **On**
4. Click Submit



Enable signing for bounce and delay messages

1. Go to Network> Bounce Profiles
2. Edit the bounce profile associated with the public listener where you will send signed outbound messages (e.g. Default)
3. Set Enable Use Domain Key Signing for Bounce and Delay Messages to **Yes**
4. Click Submit



Exporting and importing signing keys and domain profiles

If you have multiple email gateways, you must copy the same signing keys and domain profiles to each gateway.

Exporting signing keys

1. Go to Mail Policies > Signing Keys
2. Click Export Keys

Importing an existing key export file

All existing keys will be replaced by this process

1. Go to Mail Policies > Signing Keys
2. Click Import Keys
3. Select the file that contains the keys to be imported
4. Click Submit - A warning is displayed
5. Click Import

Exporting domain profiles

1. Go to Mail Policies > Signing Profiles
2. Click Export Domain Profiles

Importing an existing domain profiles export file

All existing domain profiles will be replaced by this process

1. Go to Mail Policies > Signing Profiles
2. Click Import Domain Profiles
3. Select the file that contains the domain profiles to be imported
4. Click Submit - A warning is displayed
5. Click Import

Configure DMARC verification

Edit the default DMARC verification profile

Go to Mail Policies> DMARC

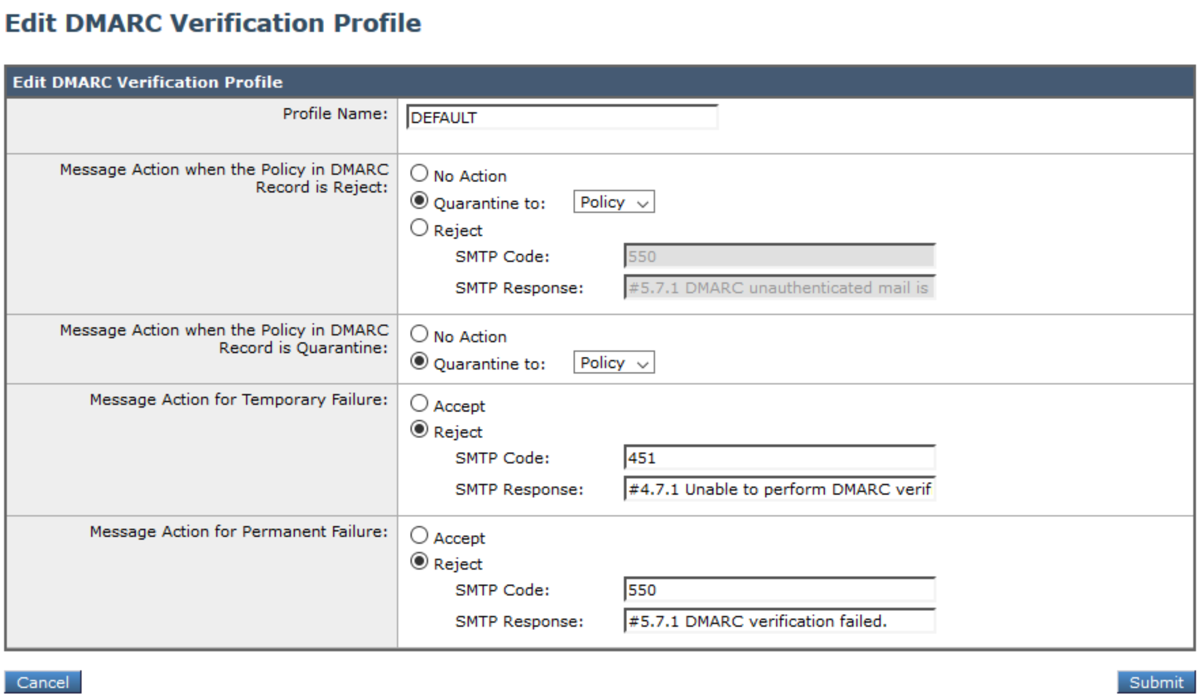
Then click Edit on the Default profile

1. Configure the profile to override a reject policy, and send the message to a quarantine that only the incident response team can access
2. Configure the quarantine action to send the message to a quarantine that only the incident response team can access

3. Configure the profile to **reject** messages that have a temporary failure during DMARC verification

4. Configure the profile to **reject** messages that have a permanent failure during DMARC verification (This **does not** affect domains that do not have a DMARC record)

5. Click Submit



Exporting and importing DMARC verification profiles

If you have more than one email gateway, you should copy the DMARC verification profiles for consistency.

Exporting DMARC verification profiles

1. Go to Mail Policies> DMARC

2. Click Export Profiles

3. Enter a name for the file

4. Click submit

Importing DMARC verification profiles

1. Go to Mail Policies> DMARC

2. Click Import Profiles

3. Select the file to import

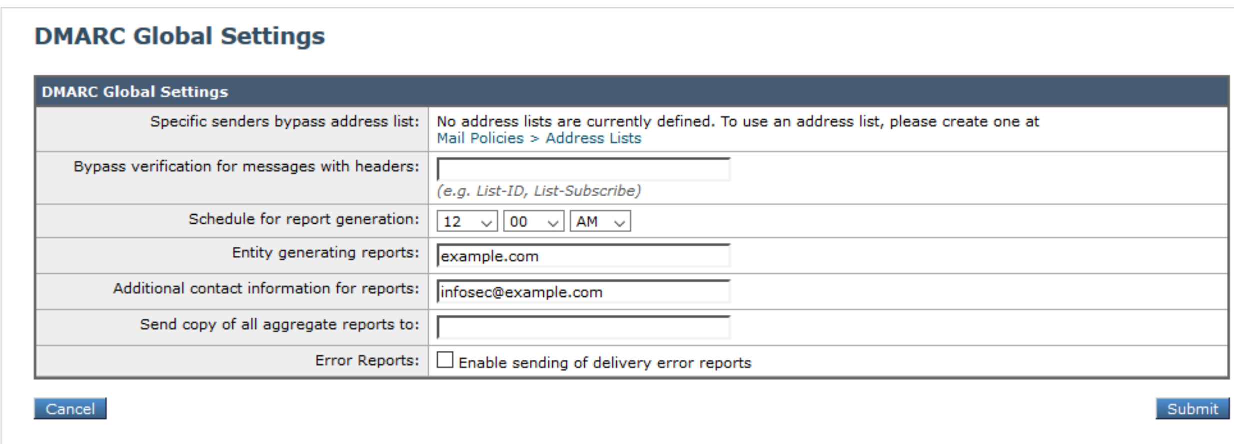
4. Click Submit – A warning message is displayed

5. Click import

Configure global DMARC settings

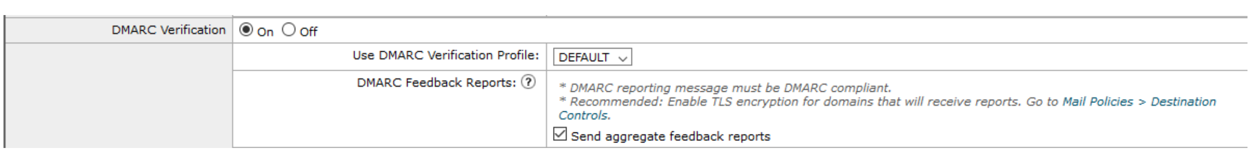
DMARC Aggregate reports are generated once per day

1. Go to Mail Policies> DMARC
2. **DO NOT set bypasses for senders or headers – this would make DMARC trivial to bypass**
3. Choose non-peak hours for generating aggregate reports to avoid impact on mail flow
4. Enter your primary domain name in the **Entity generating reports** field
5. Optionally, provide additional contact information in case organizations receiving your reports have questions
6. **DO NOT** enable sending of delivery error reports
7. Click Submit



Enable DMARC verification on the mail flow policy

1. Go to Mail Policies> Mail Flow Policies
2. **Click Default Policy Parameters**
3. In the Security Features section of the mail flow policy, enable DMARC Verification by choosing **On**
4. Enable sending DMARC Aggregate (RUA) reports
5. Click submit



Publish SPF records

If your email domains do not already have a SPF record, add a basic SPF TXT DNS record to the root of each domain

```
"v=spf1 mx ~all"
```

If mail should never be sent from a domain, use this SPF record:

Publish DMARC records

DMARC policy records are placed at a TXT record at the _dmarc subdomain. Subdomains of the TLD/base domain automatically inherit this DMARC policy record, or they can have their own record at their own _dmarc subdomain.

Here is an example DMARC policy record:

```
_dmarc.example.com TXT "v=DMARC1; p=none; rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com"
```

Set the rua and ruf addresses to the address of the mailbox that will process incoming DMARC reports.

Authorization records

If an email address in rua or ruf has a different base domain than the domain of the policy record, an authorization record must be added to the base domain of the email address to indicate that it accepts reports about that domain. For example, if dmarc@example.com also needed to accept reports for example.net, the poly record for example.net would look like this:

```
_dmarc.example.net TXT "v=DMARC1; p=none; rua=mailto:dmarc@example.com;
ruf=mailto:dmarc@example.com"
```

Because example.net is a different base domain than example.com, the following record needs to be added to example.com to indicate that it accepts reports about example.com:

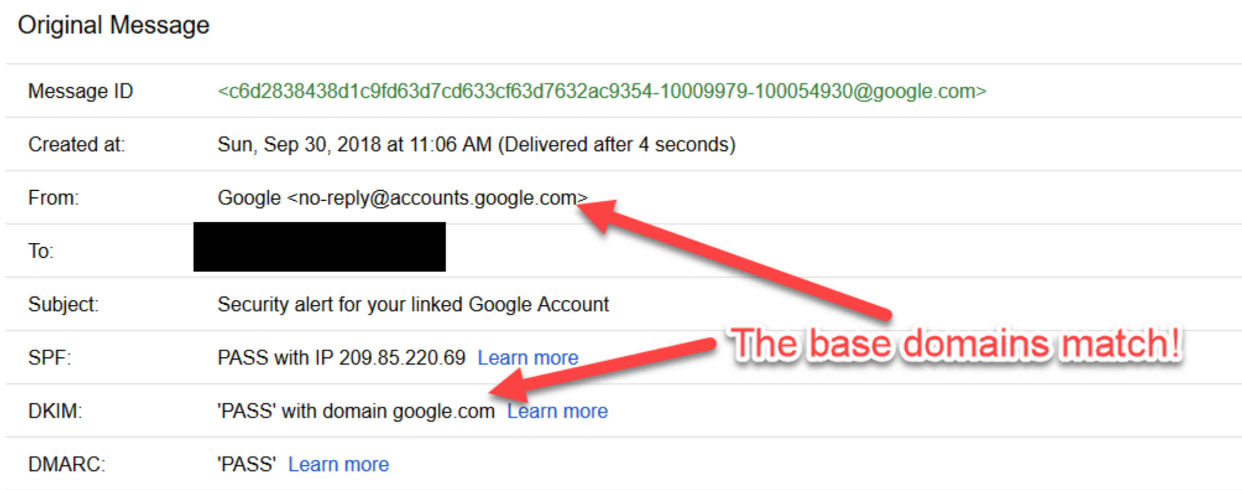
```
example.net._report._dmarc_example.com TXT "v=DMARC1"
```

Testing domain profiles

Don't forget to commit the changes first, after all the above steps are completed

1. Go to Mail Policies> Signing Profiles
2. In the Test Profile column, click on the Test link

After the above test is successful, conduct a more complete test by sending an email to a Gmail/G-Suite account. Then, open the message in Gmail, and click on the three vertical dot menu button, and click show original. This will display a page showing if DKIM and/or DMARC passed.



Original Message

Message ID	<c6d2838438d1c9fd63d7cd633cf63d7632ac9354-10009979-100054930@google.com>
Created at:	Sun, Sep 30, 2018 at 11:06 AM (Delivered after 4 seconds)
From:	Google <no-reply@accounts.google.com>
To:	[redacted]
Subject:	Security alert for your linked Google Account
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

References

- [Demystifying DMARC: A guide to preventing email spoofing]
- [DomainKeys and DKIM Signing in AsyncOS]
- [DMARC Verification in AsyncOS]