

DKIM Settings

DomainKeys Identified Mail (DKIM) is a protocol that allows verifiable email transmission through the use of cryptographic authentication. This is accomplished through the use of private and public keys. The private key is stored on the sending email server so that hash strings can be generated out of email message using that private key and a public key which is stored in DNS so that recipients can verify those hashes using that public key.

DKIM Enabled

Setting this setting to **YES** will enable DKIM verification of all incoming email and if **DKIM Sign** is enabled for any domains, it will also enable the generation of DKIM keys for all outgoing email for those domains. If DKIM Sign is not enabled for any domains it will **ONLY** enable DKIM verification of all incoming email.

Disabling DKIM will also automatically disable DKIM if enabled.

Body Canonicalization

The canonicalization method for the message body used when DKIM signing messages. The recommended setting is **Relaxed**.

Headers Canonicalization

The canonicalization method for the message headers used when DKIM signing messages. The recommended setting is **Relaxed**.

Default Message Action

This is the default action to take when an incoming message DKIM signature fails to validate. The recommended setting is **Accept**. This action is processed before all the other actions below so it's best to be set to Accept and then set any overrides below.

Bad Signature Action

This is the default action to take when an incoming message DKIM signature fails to validate. The recommended setting is **Accept**.

DNS Error Action

This is the default action to take when a DNS error occurs during the DKIM validation of an incoming message . The recommended setting is **Temp Fail**.

Internal Error Action

This is the default action to take when a system internal occurs during the DKIM validation of an incoming message . The recommended setting is **Quarantine**.

No Signature Action

This is the default action to take when an incoming message has no DKIM signature . The recommended setting is **Accept**.

Security Concern Action

This is the default action to take when an incoming message contains properties that maybe of a security concern . The recommended setting is **Quarantine**.

Signature Algorithm

This settings sets the DKIM signature algorithm used when signing outgoing DKIM messages . The recommended setting is **RSA-SHA-256**. (**Figure 1**).

Figure 1

⚠ Disabling **DKIM** will also disable **DMARC**

DKIM Enabled

YES

Body Canonicalization

Relaxed (Recommended)

Headers Canonicalization

Relaxed (Recommended)

Default Message Action

Accept (Recommended)

Bad Signature Action

Quarantine

DNS Error Action

Temp Fail

Internal Error Action

Temp Fail

No Signature Action

Accept (Recommended)

Security Concern Action

Temp Fail

Signature Algorithm

RSA-SHA256 (Recommended)

Submit

Add Whitelisted Domain(s)

Adding entries in the Whitelisted Domain(s) will allow Hermes SEG to skip DKIM checks for those entries.

Click the **Add Whitelisted Domain(s)** button and in the resultant menu enter the entries the **Domain(s)** field (You can add multiple entries each in its own line), enter an optional note in the **Note** field and click the **Submit** button (**Figure 2**).

Figure 2

Add Whitelisted Domain(s)

Domain(s)

domain.tld

someotherdomain.tld

yetanotherdomain.tld

Note

This is a test note

Submit

Cancel

Add Trusted Host(s)

Adding entries in Trusted Host(s) enables those hosts to send DKIM signed e-mail through Hermes SEG. Trusted Host(s) can be IPs, Network Address(es) and FQDNs.

Click the **Add Trusted Host(s)** button and in the resultant menu enter the entries the **Trusted Host(s)** field (You can add multiple entries each in its own line), enter an optional note in the **Note** field and click the **Submit** button (**Figure 3**).

Figure 3

Add Trusted Host(s)

Trusted Host(s)

192.168.100.0/24

192.168.50.25

host.domain.tld

Note

This is a test note





Submit

Cancel

Delete Whitelisted Domain(s) or Trusted Host(s) Entries

Select the entries you wish to delete by checking their checkboxes and click the **Delete** button on top of the page (**Figure 4**).

Figure 4

<input type="checkbox"/>	Edit	Entry	Type	Note
<input checked="" type="checkbox"/>		192.168.100.0/24	TRUSTED HOST	LAN
<input type="checkbox"/>		192.168.100.0/24	TRUSTED HOST	LAN
<input checked="" type="checkbox"/>		192.168.50.25	TRUSTED HOST	E LAN
<input checked="" type="checkbox"/>		192.168.100.0/24	TRUSTED HOST	LAN

Edit Whitelisted Domain or Trusted Host Entry


Click the  icon next to the entry you wish to edit. In the resultant window, make changes as necessary and click the **Submit** button (**Figure 5**).

Figure 5

Edit Entry

Entry

Note

Revision #7

Created 2 January 2021 14:15:38 by Dino Edwards

Updated 20 May 2023 22:22:35 by Dino Edwards