FortiMail Email Authentication: SPF, DKIM and DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) performs email authentication with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) checking.

SPF compares the client IP address to the IP address of the authorized senders in the DNS record. If the test fails, the email is treated as spam.

DKIM allows FortiMail to check for DKIM signatures for incoming email or sign outgoing email with the domain keys for the protected domains.

This recipe covers how to enable DMARC, SPF, and DKIM.

If you require more information on DMARC, SPF, or DKIM, consult the FortiMail Administrator Guide.

Enabling SPF Checking

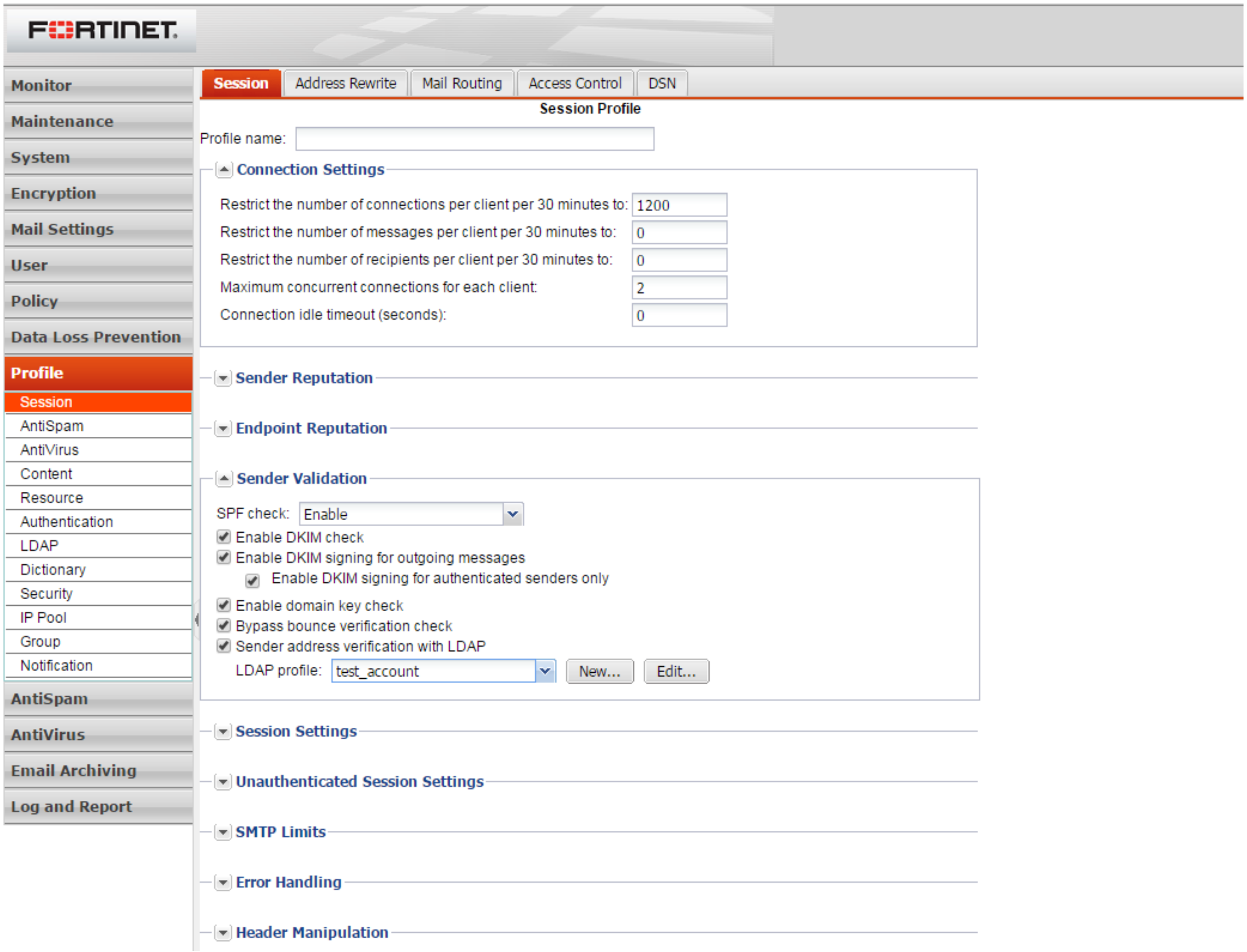
You can enable SPF in the antispam profile and in the session profile settings. If you select to *Bypass SPF checking* in the session profile, however, SPF checking will be bypassed even though you enable it in the antispam profile.

To enable SPF in an antispam profile

1. Go to **Profile > Antispam**.
2. Select **New** or double click an existing profile.
3. Enable **SPF check.**

To enable SPF in a session profile

1. Go to **Profile > Session.**



Session Profile

Profile name:

Connection Settings

Restrict the number of connections per client per 30 minutes to: 1200
Restrict the number of messages per client per 30 minutes to: 0
Restrict the number of recipients per client per 30 minutes to: 0
Maximum concurrent connections for each client: 2
Connection idle timeout (seconds): 0

Sender Validation

SPF check: Enable
☑ Enable DKIM check
☑ Enable DKIM signing for outgoing messages
☑ Enable DKIM signing for authenticated senders only
☑ Enable domain key check
☑ Bypass bounce verification check
☑ Sender address verification with LDAP
LDAP profile: test_account

2. Select **New** or double click an existing profile.
3. Select the arrow beside the **Sender Validation** section to expand it.
4. Enable or disable SPF by selecting the appropriate option from the dropdown menu.

   If the sender domain DNS record lists SPF authorized IP addresses, use SPF check to compare the client IP address to the IP addresses of authorized senders in the DNS record. An unauthorized client IP address increases the client sender reputation score, while an authorized client IP address decreases the client sender reputation score

Enabling DKIM Checking

FortiMail can perform DKIM checking for the incoming mail by query the DNS server that hosts the DNS record for the sender’s domain name to retrieve its public key to decrypt and verify the DKIM signature.

To enable DKIM checking

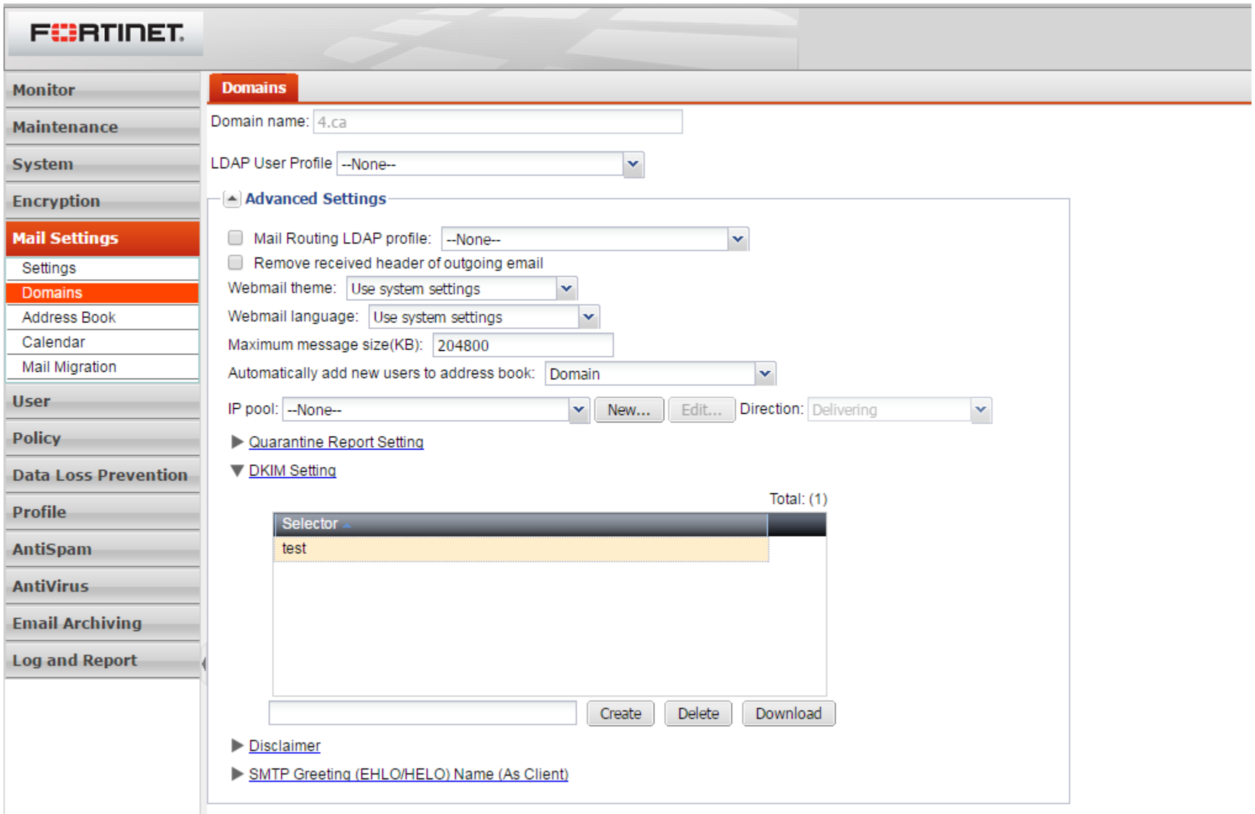
1. Go to **Profile > Session.**
2. Select New or double click an existing profile.
3. Select the arrow beside the *Sender Validation* section to expand it.
4. Enable **DKIM check.**

Configuring DKIM Signing

If you want to sign the outgoing mail with DKIM signatures so that the remote receiving server can verify the signatures, you can do so after you create the protected domains. Note that the DKIM signing settings only appear when configuring an existing protected domain.

To configure DKIM signing

1. Go to **Mail Settings > Domains >Domains**.



Domain name: 4.ca

LDAP User Profile --None--

Advanced Settings

□ Mail Routing LDAP profile: --None--

□ Remove received header of outgoing email

Webmail theme: Use system settings

Webmail language: Use system settings

Maximum message size(KB): 204800

Automatically add new users to address book: Domain

IP pool: --None-- Direction: Delivering

▶ Quarantine Report Setting

▼ DKIM Setting

Total: (1)

Selector
test

▶ Disclaimer

▶ SMTP Greeting (EHLO/HELO) Name (As Client)

2. Double click an existing protected domain.
3. Expand the *Advanced Settings* and then expand the *DKIM setting*.
4. Enter a selector to use for the DKIM key in the entry field and select **Create.** The selector name for the key pair appears in the list of domain key selectors.

The key pair is generated and public key exported for publication on a DNS server.

5. Click to select the domain key and then select **Download**.
6. Publish the public key by inserting the exported DNS record into the DNS zone file of the DNS server that resolves this domain name.
7. Select **OK.**

To enable DKIM signing

1. Go to **Profile > Session.**
2. Select **New** or double click an existing profile.
3. Select the arrow beside the **Sender Validation** section to expand it.
4. Enable **DKIM signing for outgoing messages**.

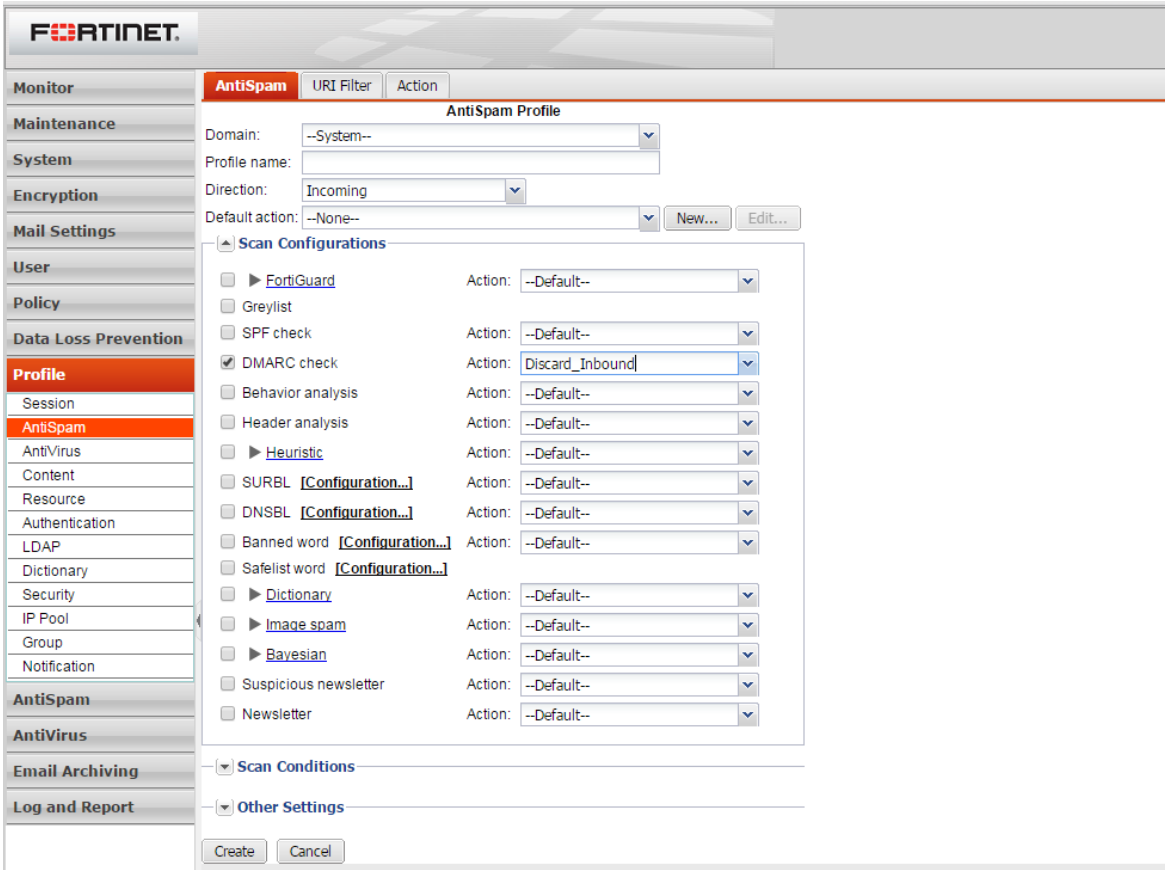
Enabling DMARC

DMARC performs email authentication with SPF and DKIM checking. If either SPF or DKIM check passes, DMARC check will pass. If both of them fails, DMARC check will fail.

Enabling DMARC will enable both SPF and DKIM.

To enable DMARC

1. Go to **Profile > AntiSpam > AntiSpam.**



AntiSpam Profile

Domain: --System--

Profile name:

Direction: Incoming

Default action: --None--

Scan Configurations

□ ▶ FortiGuard	Action:	--Default--
□ Greylist		
□ SPF check	Action:	--Default--
☑ DMARC check	Action:	Discard_Inbound
□ Behavior analysis	Action:	--Default--
□ Header analysis	Action:	--Default--
□ ▶ Heuristic	Action:	--Default--
□ SURBL [Configuration...]	Action:	--Default--
□ DNSBL [Configuration...]	Action:	--Default--
□ Banned word [Configuration...]	Action:	--Default--
□ Safelist word [Configuration...]		
□ ▶ Dictionary	Action:	--Default--
□ ▶ Image spam	Action:	--Default--
□ ▶ Bayesian	Action:	--Default--
□ Suspicious newsletter	Action:	--Default--
□ Newsletter	Action:	--Default--

Scan Conditions

Other Settings

2. Select **New** or modify an existing profile.
3. Enable **DMARC check.**