IPSWITCH

IMail Server™

DomainKeys / DKIM

Getting Started Guide

Ipswitch, Inc.
753 Broad Street
Suite 200
Augusta, GA 30901-5518

Web: www.imailserver.com
Phone: 706-312-3535
Fax: 706-868-8655

Copyrights

IMail Server – DomainKeys / DKIM Getting Started Guide

Update History

November 2009 First Edition v11.01

CHAPTER 1

DomainKeys / DKIM

In This Chapter

About DomainKeys / DKIM

DomainKeys and **DomainKeys Identified Mail (DKIM)** are e-mail authentication methodologies designed to verify digitally signed e-mail on a per-domain basis. Both methods were designed for protection of e-mail identity and have assisted in the control of "spam" and "phishing". DomainKeys and DKIM use asymmetric key cryptography to sign messages with a private key and use DNS to distribute the public key for signature verification.

DomainKeys (*RFC4870* (http://tools.ietf.org/html/rfc4870)) is a precursor to DKIM (*RFC4871* (http://tools.ietf.org/html/rfc4871)), though both are currently in use, DomainKeys is considered deprecated by DKIM.

DomainKeys

DomainKeys is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove the legitimacy and contents of an e-mail message, and also verifies that the domain used in the "from" or "sender" header of a message has not been modified while in transit.

Public Key / Private Key

A public key/private key-pair is created for the sending domain. The private key is stored securely on the mail server and is used to sign all outgoing messages. The public key is stored and published in DNS as a TXT record of the domain.

When an e-mail is sent, the mail server will use the private key to digitally sign it, which is part of the message header. When the e-mail message is received, the DomainKeys signature can be verified against the public key on the domain's DNS.

For detail specifications on **DomainKeys** see *RFC4870* (http://tools.ietf.org/html/rfc4870).

DKIM

DKIM is very similar in functionality to DomainKeys, with an enhanced standard that provides more flexibility and security. Although DKIM does not filter or identify spam, widespread use of DKIM can prevent spammers from forging the source address of their messages. If spammers are forced to show a correct source domain, then the other spam filtering techniques will work more effectively.

Some of the improvements provided by DKIM are as follows:

- Multiple hashing algorithms (as opposed to just one available with DomainKeys).
- Capability for one DNS text record to handle multiple domains.
- Improved option for canonicalization that validates header and body separately.
- Capability to delegate signing to third parties.
- Capability to self-sign additional headers.
- More advanced options for customization using DKIM. (e.g. Hash Algorithms, Body Settings, Expiration)

For detail specifications on **DKIM** see *RFC4871* (http://tools.ietf.org/html/rfc4871).

How DomainKeys / DKIM Works

How it works:

1. The sending server has to first generate a public and private key-pair.
2. This public and private key pair must be assigned to a Selector. A Selector is just the name given to a set of signing options.
3. The public key must be published in a TXT DNS record with the Selector Name on the public facing DNS server for that mail domain.

Once these steps are completed, the sending server can now sign outgoing mail. Once the message is received, the message is parsed and the signature is identified. Then a DNS lookup attempts to retrieve the public key for that Selector. If the TXT record is found, the public key is then used to verify the signature. If everything is correct, the message passes, if not, the receiver must decide what to do with the failed signature.

DomainKeys / DKIM FAQs

Which one should I use?

DKIM should be preferred as DomainKeys is considered deprecated. However, there may be older servers which require DomainKeys but do not implement DKIM. You may also choose to sign with both. However, be aware that the RFC gives fairly broad leeway to verifiers in determining what constitutes a failed signature, so you need to have some idea what the receiving server is expecting. Also DomainKeys settings must be applied on a domain-by-domain basis and requires DNS records to be set for each host alias of each domain that is signing. DKIM can use a single selector for all domains on the server.

Is DomainKeys another anti-spam method?

DomainKeys and DKIM should not be considered an anti-spam solution. In addition to other anti-spam checks, they can be helpful in identifying spam, but DomainKeys alone is not a very effective anti-spam method.

Can I setup message signing without verification?

DomainKeys / DKIM signature signing and message verification are setup in your IMail Server to allow as much flexibility as possible.

- DomainKeys / DKIM signing is setup on a per-domain basis, allowing the IMail Administrator to only have one domain or all domains (including both IP'd and Virtual domains) to sign outgoing messages.
- Verification of in-coming messages can be turned off for one domain or all domains without affecting the signing of outbound messages.

Note: Verification is controlled only for domains with IP addresses. Virtual domains use the settings for the host assigned to the IP address on which the message arrived. To determine which IP address is being used by a virtual domain, check the domains MX records.

CHAPTER 2

DomainKeys / DKIM Signing Setup

In This Chapter

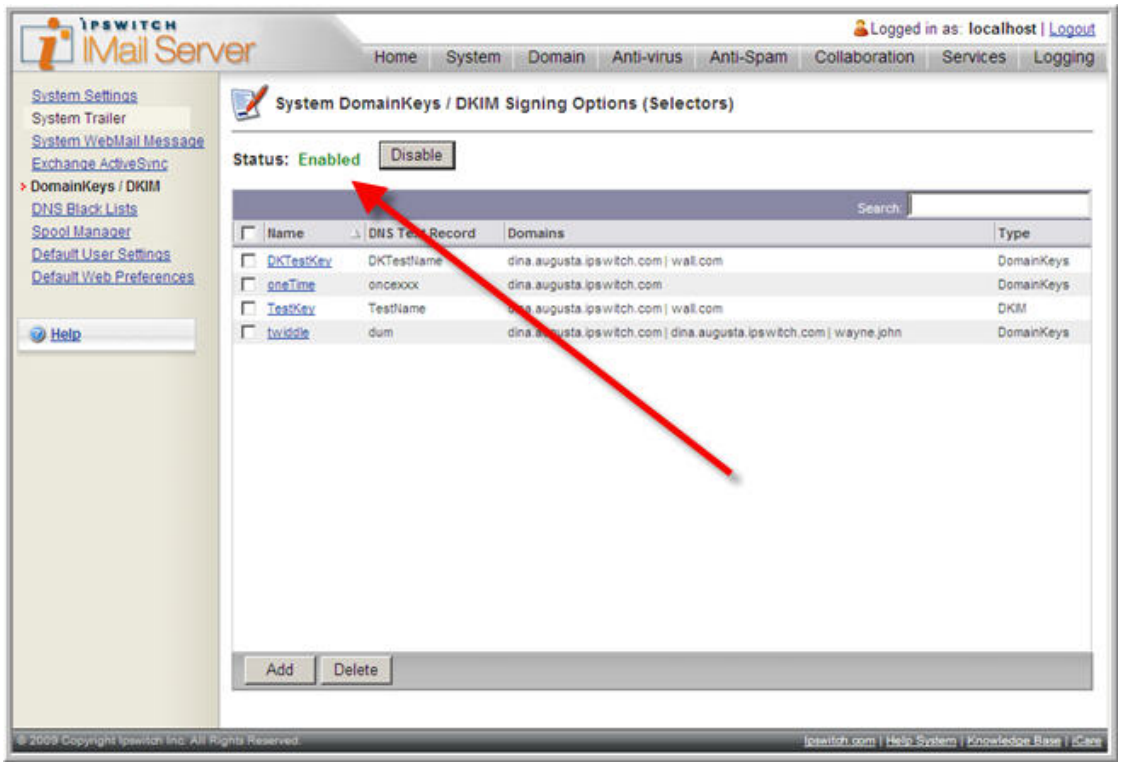
DomainKeys / DKIM setup is fully functional in both the Web Administration and the Console Administration. For purposes of this document only the Web Administration will be used to demonstrate DomainKeys / DKIM functionality.

 **Important for Windows 2003 Servers** using DKIM selectors with SHA256 hash algorithm.

- The .NET Framework 3.5 SP1 is also required which can be downloaded from *Microsoft Update* (http://www.microsoft.com/downloads/details.aspx?familyid=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en).
- "`RegisterSHA2.exe`" a .NET Framework 3.5 utility located under your /IMail directory must be invoked to correct a potential problem with .NET Cryptography classes that may prevent DomainKeys from processing signatures.

Step 1 - Enabling DomainKeys / DKIM

- **DomainKeys / DKIM** must be enabled at the **System** level. **Go to System > DomainKeys / DKIM** in your IMail Administrator. (For **Console Administrator** go to **System** and click tab **DomainKeys / DKIM**.)



Step 2 - Creating a DKIM Selector

- To create a DKIM selector, go to the **System > DomainKeys / DKIM** in your IMail Administrator. (For **Console Administrator** go to **System** and click tab **DomainKeys / DKIM**.)
- Click **"Add"** and a pop-up window will appear asking to either use the **"Wizard"** or the **"Advanced"** option. The wizard is recommended for IMail Administrators unfamiliar with DomainKeys / DKIM, and will be used in this guide.

Note: The **"Advanced"** option requires full understanding of all DomainKeys / DKIM options and how to create the DNS records.

- Click the **"Wizard"** button to continue.

Signing Options

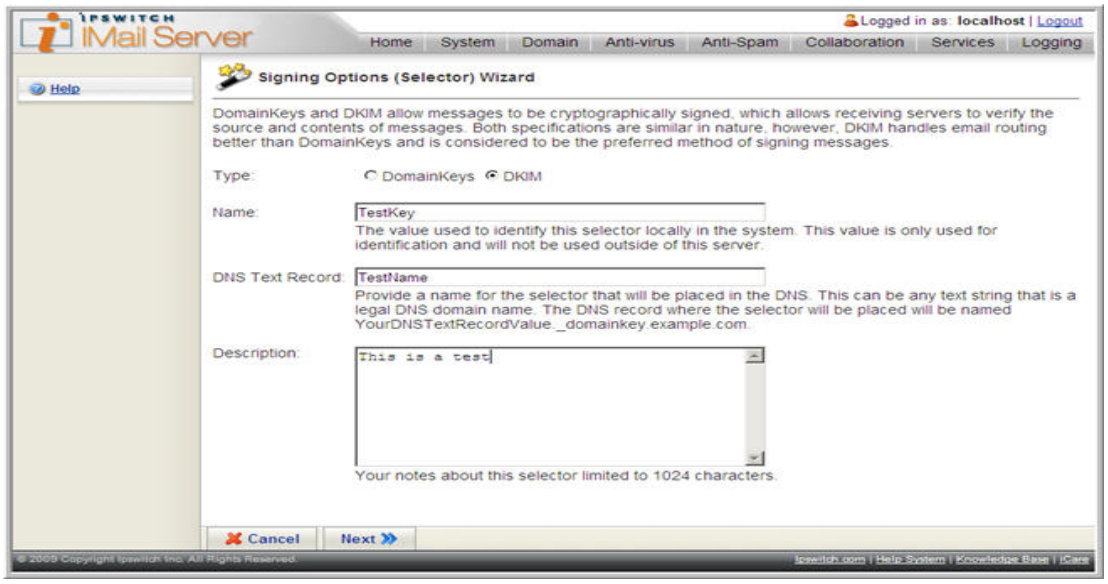
- Choose the **DKIM** selector type, set by default.
- Enter the **Name** for the selector. The selector Name is your IMail reference for selector updating.
- Enter the **DNS Text Record name** to be associated with this selector. The DNS Text Record is used for naming the TXT record in DNS.

Example: If the DNS Text Record is "DKTestName" with a domain name of "test.domain.com", the full name of the TXT record in DNS containing the public-key will be named "DKTestName_domainkey.test.domain.com".

The DNS Text Record name comes before "_domainkey" from the full name of the DNS Text Record.

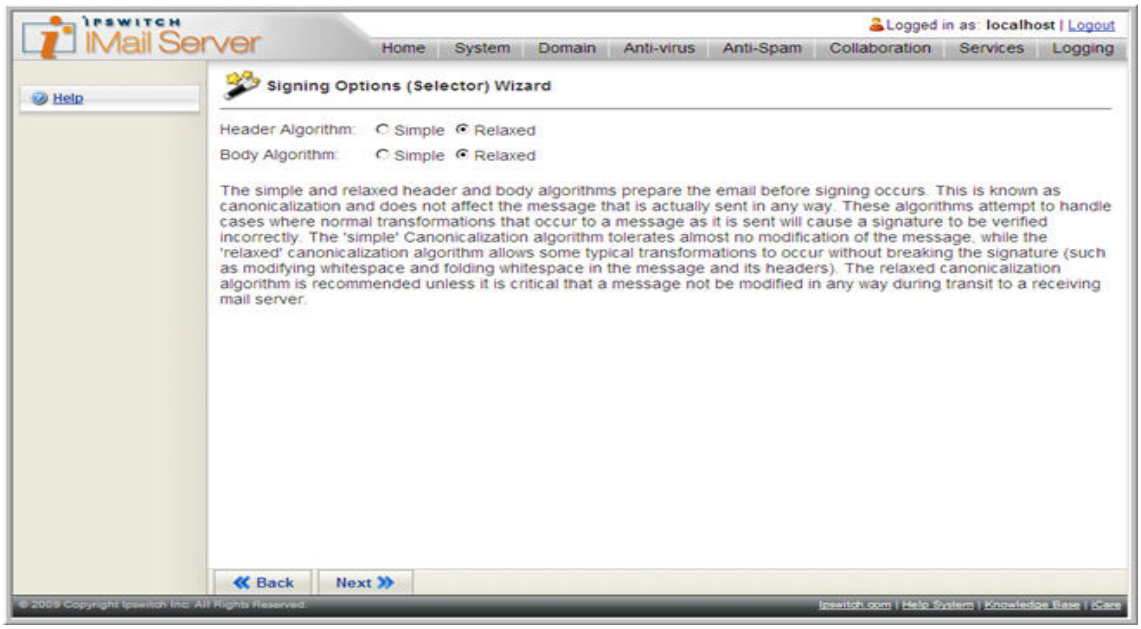
Note: Keep in mind the DNS Text Record must follow all DNS naming rules.

- **Description** is optional.



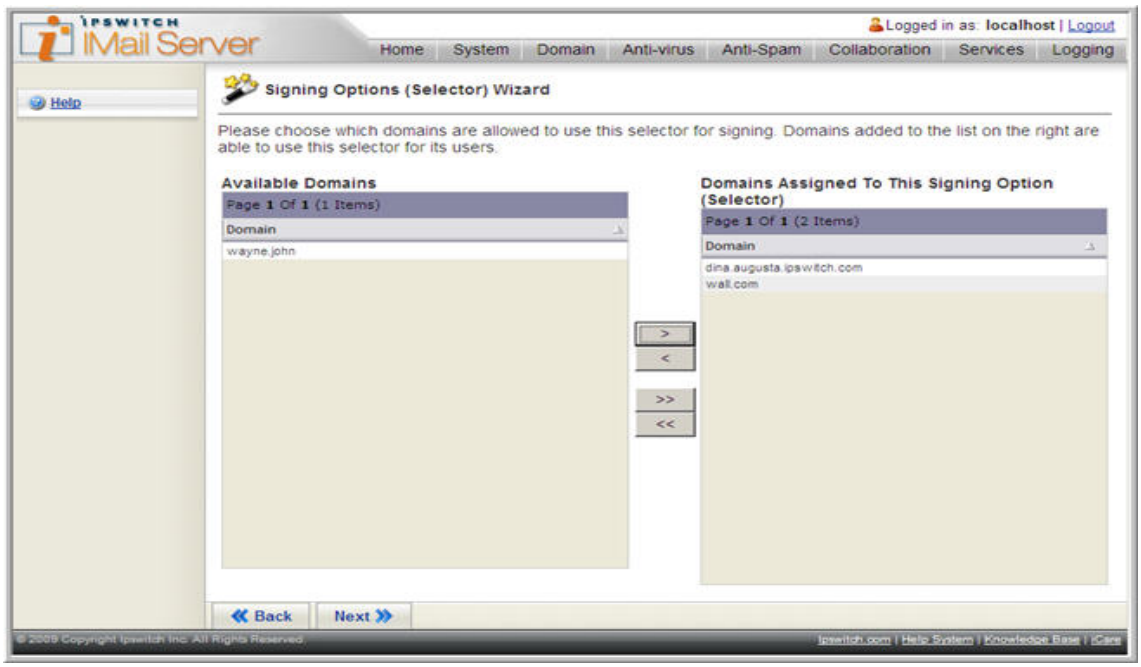
Canonicalization Algorithm Settings

- This page is setting the **Header and Body Algorithms**. The default setting **"Relaxed"** is recommended to allow whitespace and folding whitespace modifications in a message to be tolerated.



Domain Selection

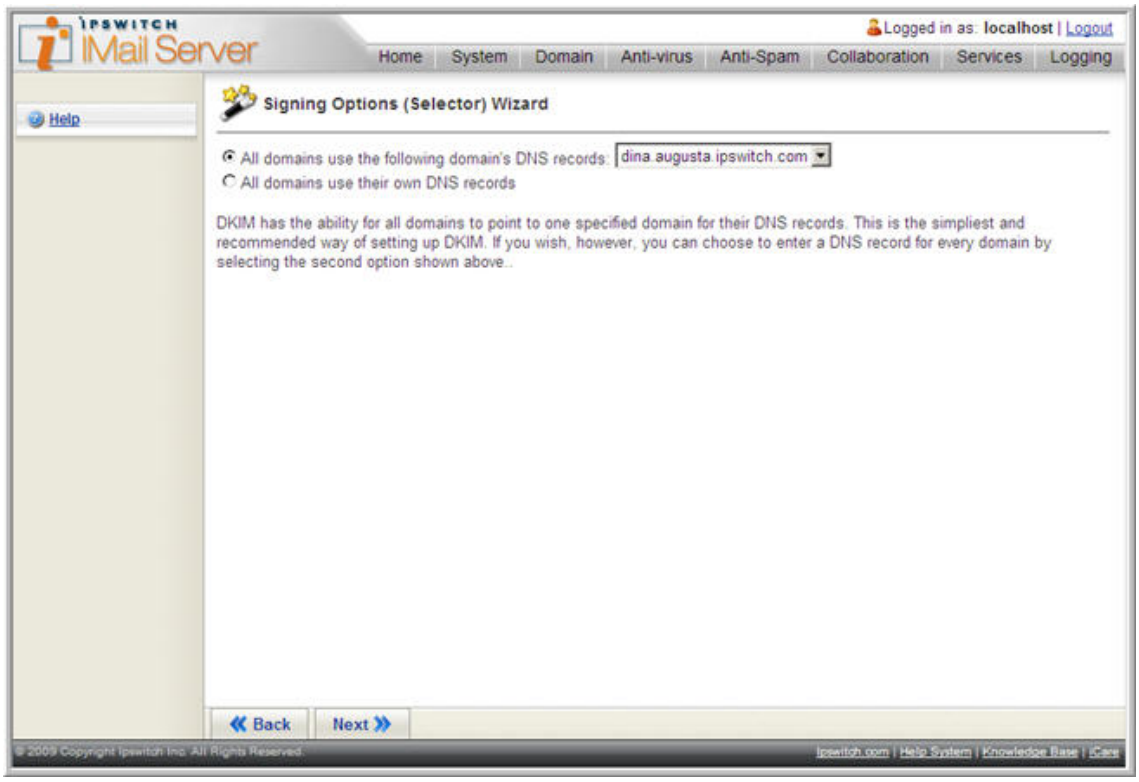
- The Available Domains displays all domains that exist on the IMail Server.
- Select the domain(s) you wish to be applied to this selector.



Multiple Domain Selection

Note: This step only appears when multiple domains have been assigned to a selector.

- **DNS Text Record** Options:
  - A single domain to sign for all the selected domains. This is the simplest and the recommended method.
  - Each domain sign for itself, requiring a separate DNS Text Record for each domain.



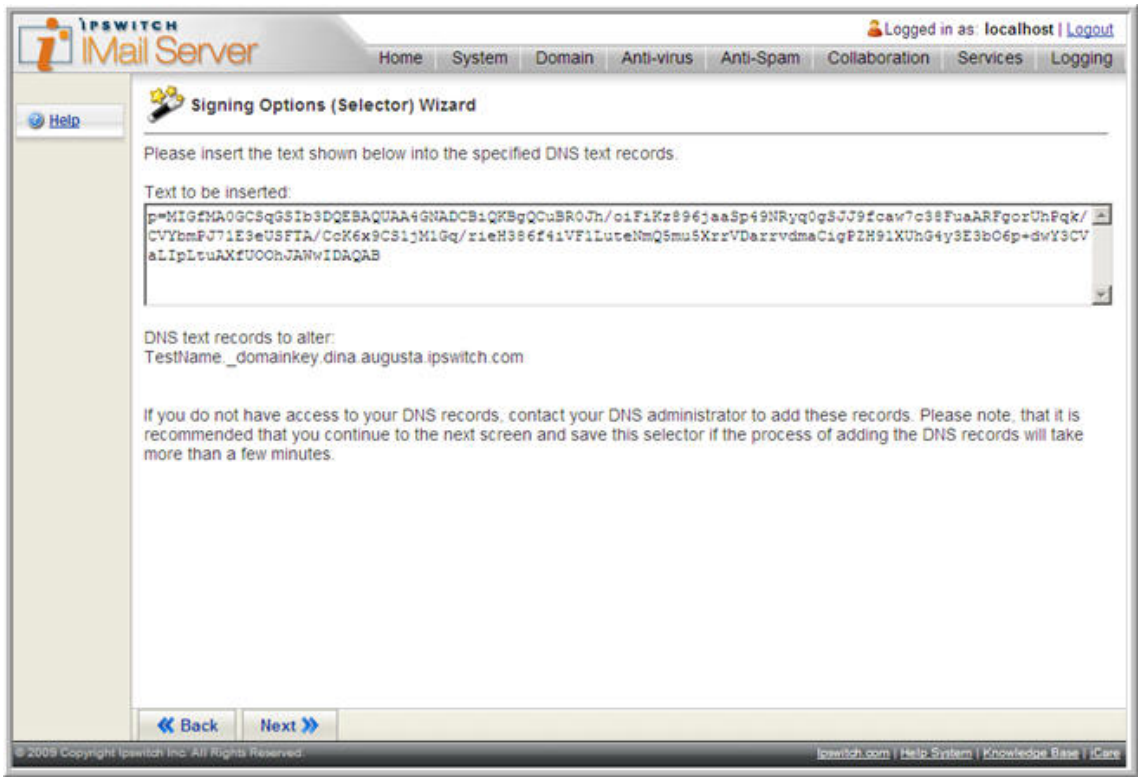
DNS Text Record Setup

Note: Please contact your DNS Administrator or ISP for assistance in setting up TXT records on your DNS Server. Detail assistance with DNS TXT records is beyond the scope of Ipswitch support.

- This page displays the information needed for setting up your DNS text record.
- Create a TXT record in DNS with the name given on the displayed page.
- If multiple DNS text records are displayed, then be sure to create a DNS text record name for each.
- Copy and paste the public key displayed into the DNS text record.

Note: To avoid time-out issues, click next, as this information is displayed on the Selector edit page.

Tip: Remember to check for the "p=" in front of the key



DNS Test

- This last screen allows you to test your DNS setup once all the DNS text records have been created.

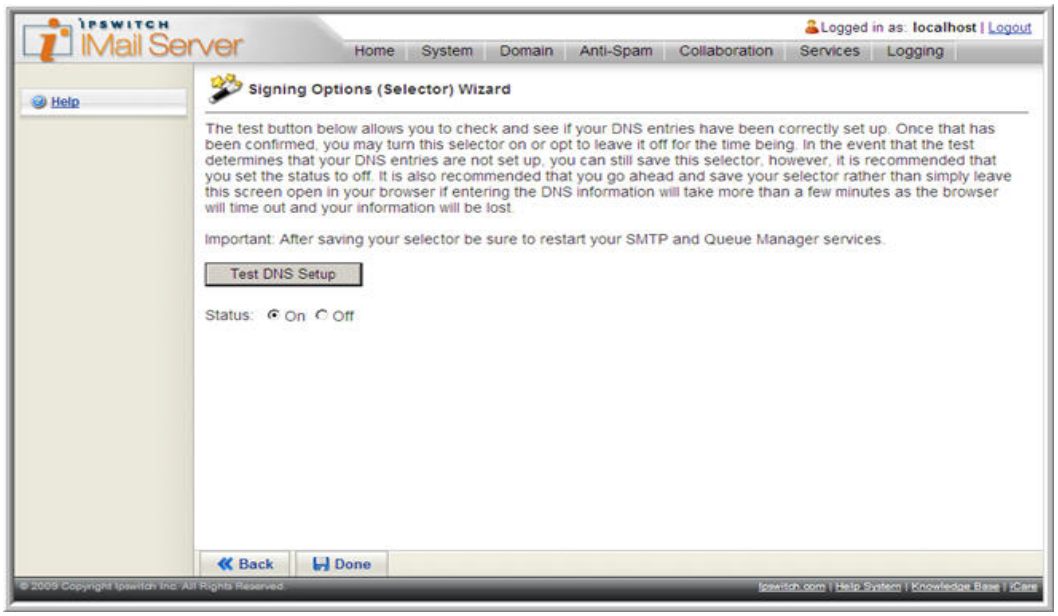
Note: This **"DNS Test"** button also exists on the Selector edit page.

- The status displayed is for the selector. The Status is set to "On" by default.

Tip: Although the **Status** for the selector is **"On"**, the signing will not begin until the selector is **"Enabled"** for a domain.

- Click **"Done"**. The selector is now saved.

Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.



Updating Your DNS TXT Records

For active existing DNS TXT records you need to be aware that it will take some time for records to expire from your DNS server, as TXT records are cached when they are first accessed.

The time it will take a DNS record to expire from cache is the TTL value (Time To Live, in seconds) for your TXT record minus the time elapsed since the record was cached. You will need to wait, probably several hours, possibly a couple of days before the old record expires and the new one is obtained. This is the normal behavior of DNS.

To Prevent This

- Change the TTL value for your TXT records to meet your needs.
- Create a new selector / TXT record.

Step 3 - Creating a DomainKeys Selector

- To create a DomainKeys selector, go to **System > DomainKeys / DKIM** in your IMail Administrator.
- Click **"Add"** and a pop-up window will appear asking to either use the **"Wizard"** or the **"Advanced"** option. The wizard is recommended for IMail Administrators unfamiliar with DomainKeys / DKIM, and will be used is this guide.

Note: The **"Advanced"** option requires full understanding of all DomainKeys / DKIM options and how to create the DNS records.

- Click the **"Wizard"** button to continue.

Signing Options

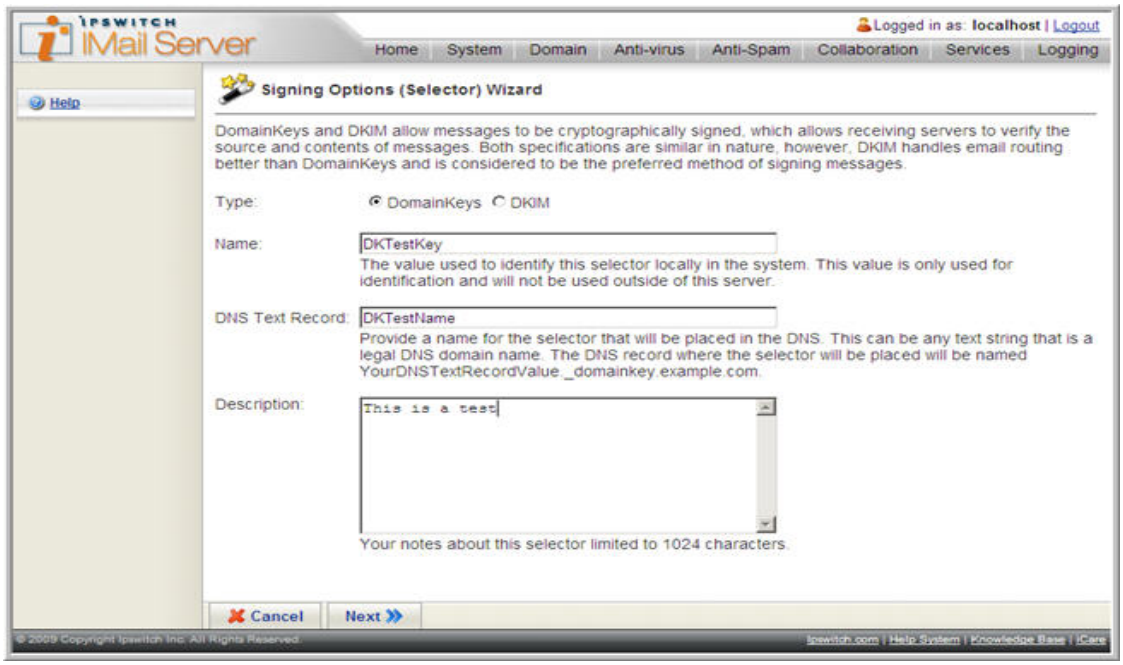
- Choose the selector type: **DomainKeys**.
- Enter the **Name** for the selector. The selector Name is your IMail reference for selector updating.
- Enter the **DNS Text Record name** to be associated with this selector. The DNS Text Record is used for naming the TXT record in DNS.

  Example: If the DNS Text Record is "DKTestName" with a domain name of "test.domain.com", the full name of the TXT record in DNS containing the public-key will be named "DKTestName_domainkey.test.domain.com".

  The DNS Text Record name comes before "_domainkey" from the full name of the DNS Text Record.

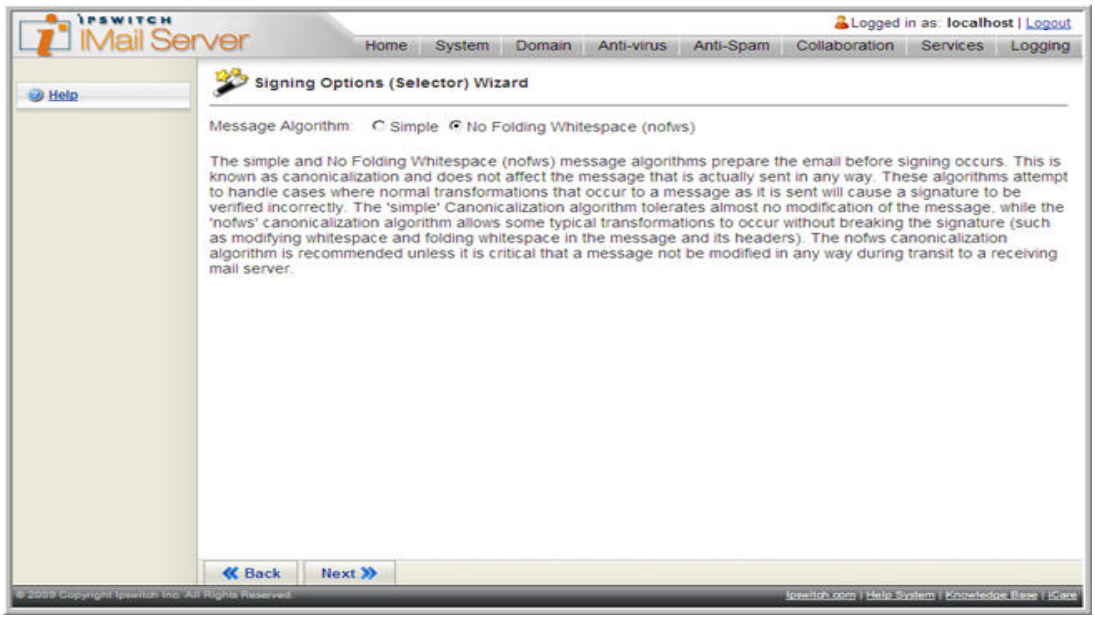
Note: Keep in mind the DNS Text Record must follow all DNS naming rules.

- **Description** is optional.



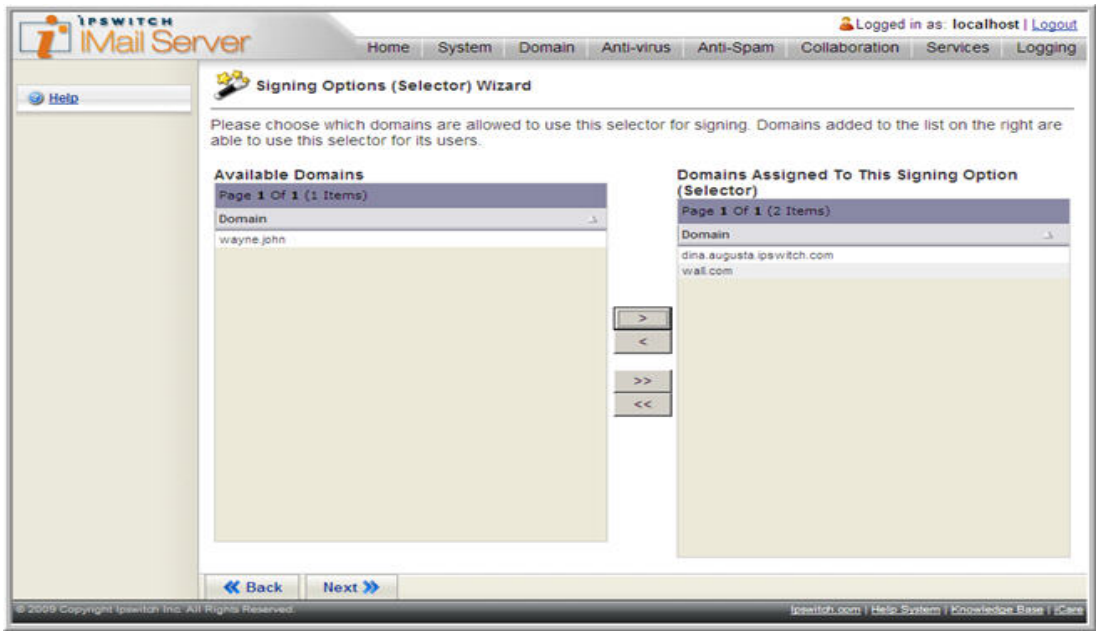
Canonicalization Algorithm Settings

- This page is setting the **Message Algorithms**. The default setting **"No Folding Whitespace"** is recommended to allow whitespace and folding whitespace modification in a message to be tolerated.
- Click **"Next"**.



Domain Selection

- The Available Domains displays all domains that exist on the IMail Server.
- Select the domain(s) you wish to be applied to this selector.



DNS Text Record Setup

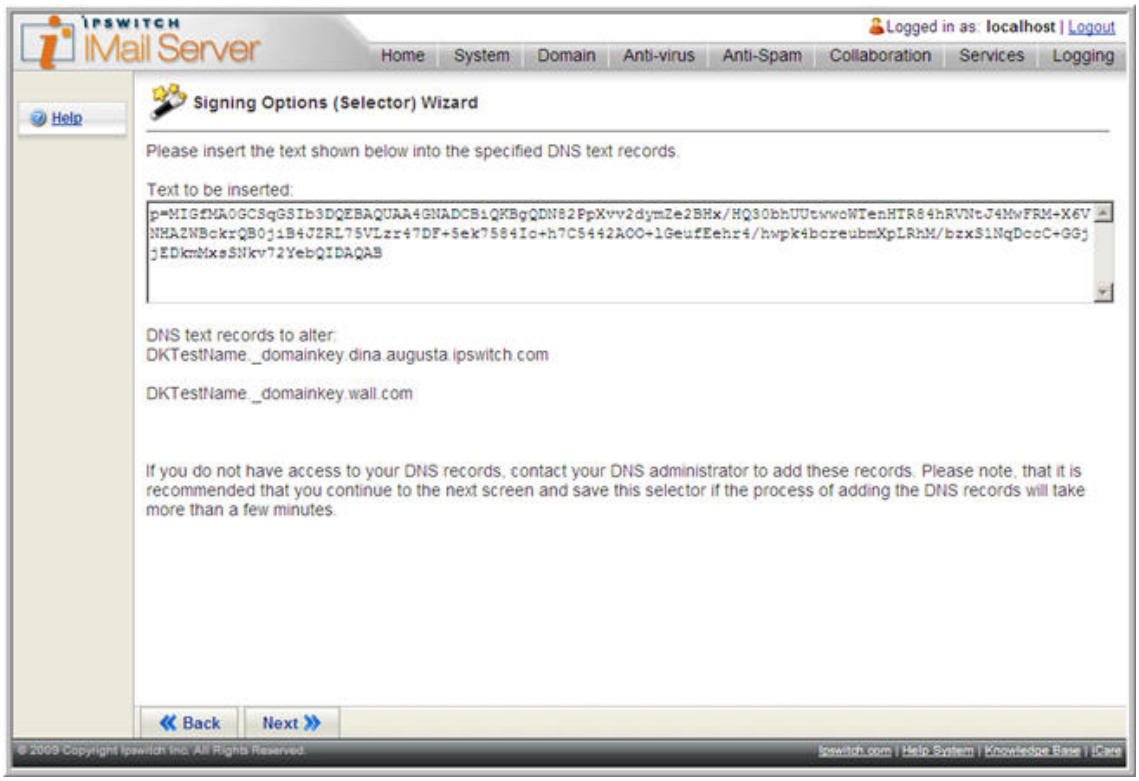
DomainKeys does not have the option of a single DNS record to sign for all the domains (as DKIM). All domains assigned to this selector **MUST** have its own DNS Text Record, as shown in the wizard.

Note: Please contact your DNS Administrator or ISP for assistance in setting up TXT records on your DNS Server. Detail assistance with DNS TXT records is beyond the scope of Ipswitch support.

- This page displays the information needed for setting up your DNS text record.
- Create a TXT record in DNS with the name given on the displayed page.
- If multiple DNS text records are displayed, then be sure to create a DNS text record name for each.
- Copy and paste the public key displayed into the DNS text record.

Note: To avoid time-out issues, click next, as this information is displayed on the Selector edit page.

Tip: Remember to check for the "p=" in front of the key



DNS Test

- This last screen allows you to test your DNS setup once all the DNS text records have been created.

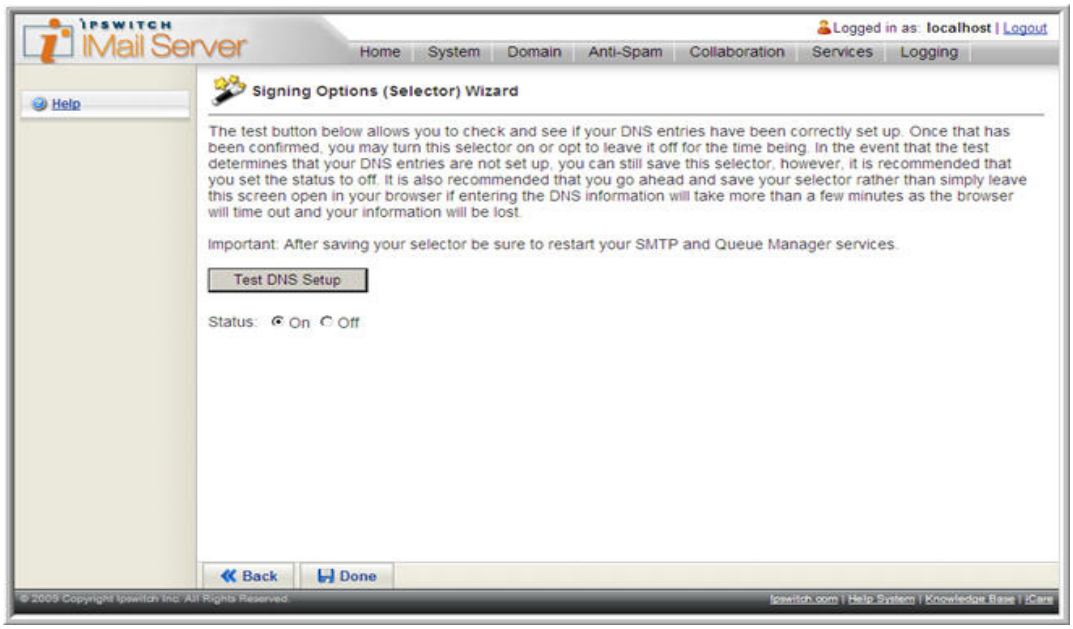
Note: This **"DNS Test"** button also exists on the Selector edit page.

- The status displayed is for the selector. The Status is set to "On" by default.

Tip: Although the **Status** for the selector is **"On"**, the signing will not begin until the selector is **"Enabled"** for a domain.

- Click **"Done"**. The selector is now saved.

Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.



Updating Your DNS TXT Records

For active existing DNS TXT records you need to be aware that it will take some time for records to expire from your DNS server, as TXT records are cached when they are first accessed.

The time it will take a DNS record to expire from cache is the TTL value (Time To Live, in seconds) for your TXT record minus the time elapsed since the record was cached. You will need to wait, probably several hours, possibly a couple of days before the old record expires and the new one is obtained. This is the normal behavior of DNS.

To Prevent This

- Change the TTL value for your TXT records to meet your needs.
- Create a new selector / TXT record.

Step 4 - Enabling Your New Selector

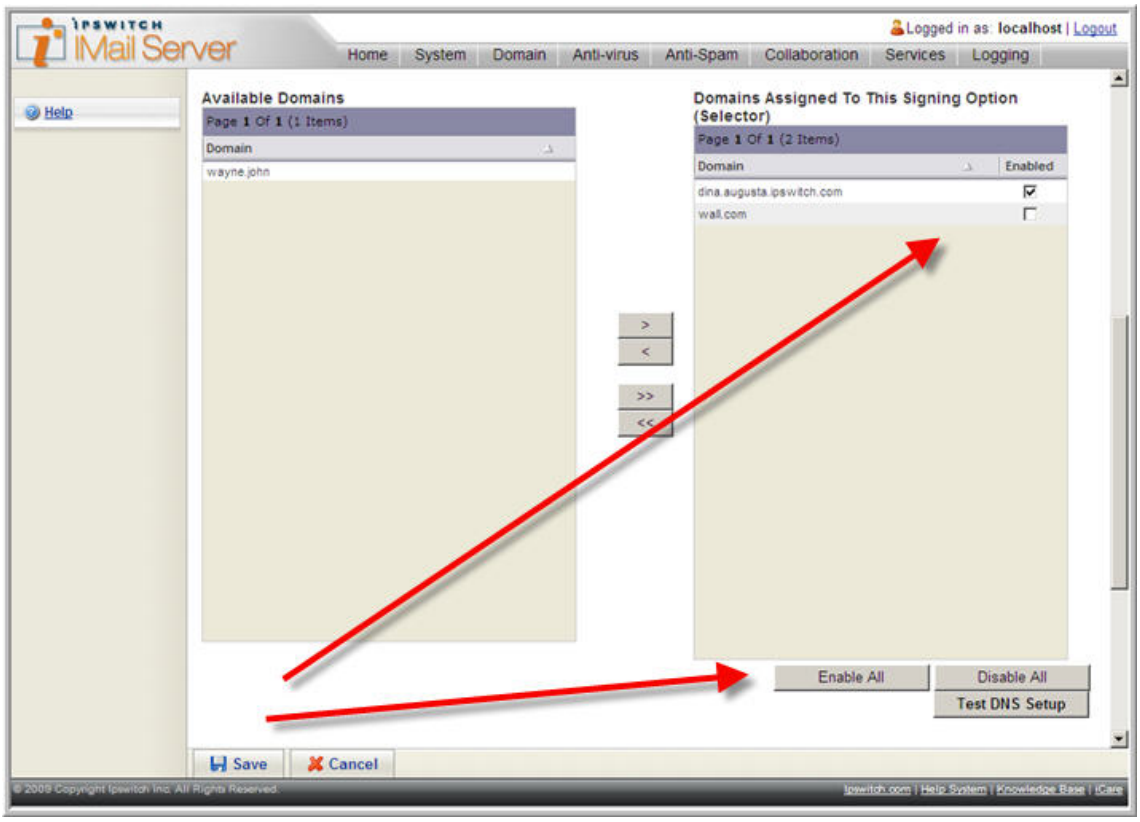
Once DNS testing is successful, the IMail Administrator will need to edit the selector and "Enable" the selector for each domain.

Important: Only **one DomainKey selector** and **one DKIM selector** can be enabled at **one time for a domain**. **Example:** A DKIM selector "selector1" is enabled for domain1.com. The IMail Administrator decides to enable "selector2" for domain1.com. "selector1" will automatically be disabled for domain1.com.

Enabling a Selector

- From your IMail Web Administrator menu selection go to System > DomainKeys / DKIM.
- Click on the selector to edit.
- Scroll down to Available Domains.
- You will see the domains that have been assigned for the selector.
- Click either the "Enable All" button, or check the boxes manually.

Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.



CHAPTER 3

DomainKeys Verification

Verification Settings

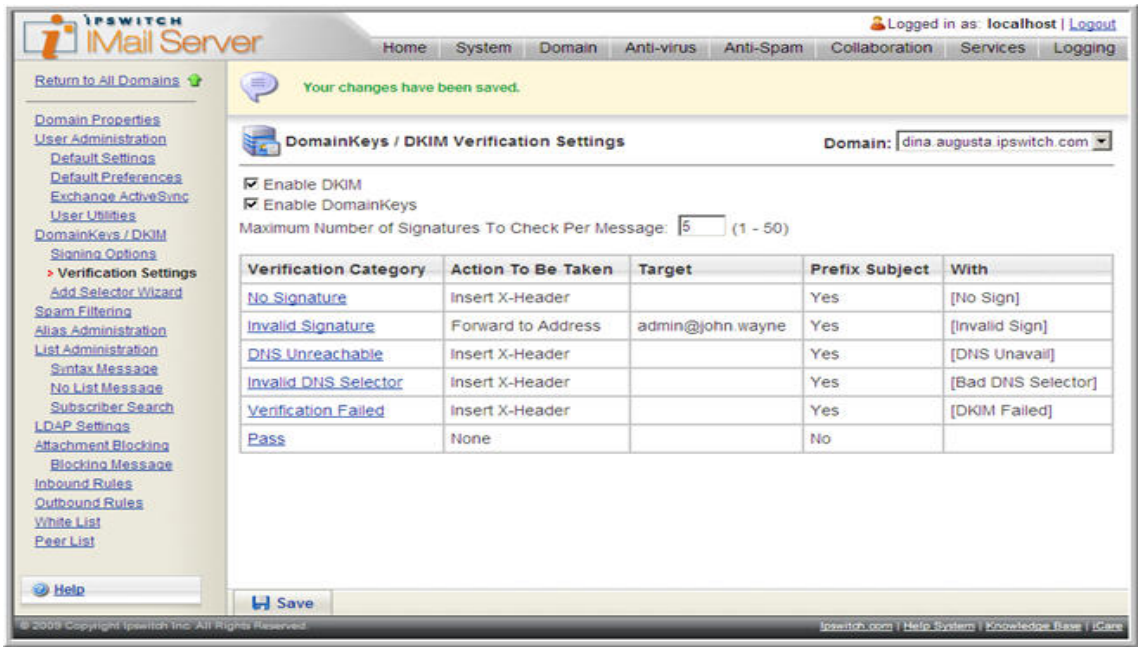
Only domains with IP addresses can be assigned unique verification settings. Virtual domains will default to the IP'd domain settings that the message used when it arrived.

Important: DomainKeys / DKIM Signature Verification will **not** be processed when an address exists in the **"Relay Mail for Addresses"**.

To view the DomainKeys / DKIM Verification Settings page

- From IMail Administration home page, click **Domain > DomainKeys / DKIM**, and the DomainKeys / DKIM Menu page appears. (For **Console Administrator** go to **Domains > DomainKeys / DKIM Signature > DomainKeys / DKIM Verification**.)
- Click on the second link **DomainKeys / DKIM Verification Settings.**
- To display the verification settings, **"Enable"** DomainKeys and/or DKIM.
- The **Verification Settings** should now display.

Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.



Verification Categories

- **No Signature**. The message is not signed using a recognized algorithm. If you are only checking for DKIM, and a DomainKeys signed message is received, it will be treated as unsigned.
- **Invalid Signature**. The syntax or formatting of the signature is incorrect. As a result, verification cannot be performed.
- **DNS Unreachable**. The DNS server for the signing domain can not be reached.
- **Invalid DNS Selector.** The DNS Text Record for the selector exists, but is not properly formatted, or has a syntax error.
- **Verification Failure**. The message is signed and the DNS records are correct and properly formatted, but the signature verification failed. This can be caused by a number of reasons, including modification to the message body, headers, or key (the private key used to sign does not match the public key in DNS).

Verification Options

- **None.** No action is performed**.**
- **Delete.** Immediately deletes the message.
- **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
- **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was verified and identified.
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.
- **Reject Connection**. Immediately ends the message connection, and the message will not be accepted with a 550 error.

Note: DNS Unreachable will return a 452 error, and a 550 error for the following failed results: Invalid Signature, Invalid DNS Selector, and Verification Failure.

CHAPTER 4

For More Assistance

Ipswitch Support

The Ipswitch Support Center provides a multitude of product related resources such as Knowledge Base articles, peer support forums, patches and documentation downloads. It also lists Ipswitch's Technical Support staff's contact information, hours of operation, and information about service agreements.

You can access the support center at:

http://www.imailserver.com/support/ (http://www.imailserver.com/Support/)