Contents

Introduction .......................................................................................................................... 1
  Multi-domain environments .............................................................................................. 1
  Multiple Domains without a Uniform Addressing Scheme .............................................. 1
  Multiple Domains with a Uniform Addressing Scheme .................................................. 2
  Public and Primary Domains with Intelligent Routing .................................................. 2
  How Employees Get Public Domain Email with Intelligent Routing ............................ 3
Detailed Example of Intelligent Routing ........................................................................... 4
  Detailed Example of Pulling Addresses from Active Directory ..................................... 4
  Detailed Example of Routing Messages to Primary and Public Domains ..................... 5
Prerequisites for Using Intelligent Routing ................................................................. 7
Users with Multiple Email Addresses in the Public Domain .............................................. 7
Domain Aliases .............................................................................................................. 7
Issues with Changing a Primary Domain to a Public Domain ......................................... 8
  The Risk of Removing a Primary Domain to
  Use Its Name for a Public Domain .............................................................................. 8
  Components You Must Configure for Intelligent Routing to Work ........................... 8

Administering Intelligent Routing ................................................................................... 9
  Associate a Public Domain with a Primary Domain ...................................................... 9
    Where the Public Domain Appears in the Control Console After It Has Been
    Assigned ...................................................................................................................... 10
  Turn on Explicit User Creation ..................................................................................... 10
  Add a Public Domain Address to Test ........................................................................ 10
  Check the Availability of the Test Public Domain Address ......................................... 11
  View the Public Domain in the Domains List ............................................................. 12
  Add the Public Domain Email Addresses for Users ....................................................... 13
    Add Public Domain Email Addresses with Directory Integration ........................... 14
    Directory Services Connector .................................................................................... 15
    .............................................................................................................................. 16
  Add Public Domain Email Addresses Manually ........................................................... 16
  Add Batches of Public Domain Email
  Addresses, Without Directory Integration ................................................................... 17
  How the Public Domain Affects Reports ..................................................................... 20
This page intentionally left blank.
Introduction

The Intelligent Routing feature of Email Protection allows you to route filtered email destined for employee addresses to your organization's distributed email systems based on the company's configuration. With this benefit, you can:

- Accept mail for a single domain and route the mail to different mail environments (for example, different geographic locations or business units), which can use different policies, if necessary.
- Create email address uniformity for corporate branding purposes.
- Easily add new local domains to the existing public domain as your company expands its workforce or locations.
- Reduce the need for the purchase, administration and maintenance of internal email routing equipment and save bandwidth.
- Leverage disaster recovery when one of your mail sites goes down without interrupting mail service for other sites that are still up and running.

Multi-domain environments

Multiple Domains without a Uniform Addressing Scheme

With a multi-domain environment, a company might have several locations and/or functional organizations, each with a domain supported by one or more SMTP mail servers. For example, say that Acme Company has acme-denver.com as one domain for employees in Denver and acme-uk.com as a second domain for employees in London. In this case, Joe Q. Smith in Denver has an email address of joesmith@acme-denver.com. Joe K. Smith in London has an email address of joesmith@acme-uk.com.

In this case, the high-level configuration of the network for Email Protection might appear as follows:

**Figure 1: Multi-domain environment without uniform addressing**

Because the domains for Denver and London are different, there is no uniform addressing scheme.
Multiple Domains with a Uniform Addressing Scheme

The company might also have a domain acme.com that is pointed to the site- or function-specific domains for delivery of email. As an umbrella domain, acme.com creates a uniform email addressing scheme for all employees. In this case, acme.com is a registered domain with a public mail exchange (MX) record. Thus, to expand the previous example, the two Joe Smiths in Denver and London would each need to have additional email addresses using the umbrella domain. In this case, the recipient names in their email addresses would have to be unique. Thus, Joe Q. Smith of Denver would have an additional email address of joesmith@acme.com, but Joe K. Smith in London would have an additional email address of jsmith@acme.com.

Without Intelligent Routing, an umbrella domain for a uniform addressing scheme, as in our example, would be implemented with an internal email router that could map addresses using the umbrella domain to the addresses using the local mail servers’ domains.

In this case, the high-level configuration of the network for Email Protection might appear as follows:

Figure 2: Multi-domain environment with uniform addressing

For this example, the internal email router receives incoming mail on the umbrella domain and routes the email to the appropriate mail servers for acme-denver.com and acme-uk.com.

NOTE: acme-denver.com and acme-uk.com could also be registered domains with public MX records. In this case, Joe Smith in Denver could receive email via either the address on umbrella domain acme.com or the address on acme-denver.com.

Public and Primary Domains with Intelligent Routing

Within Email Protection, domains that are supported by an SMTP Mail Server are considered primary domains. For Intelligent Routing on Email Protection, the umbrella domain from the previous example is called a public domain. Thus, a public domain is a registered domain with a public MX record that is used for uniform email addresses across multiple primary domains. And within Email Protection, the public domain is assigned to each primary domain.
Note: A primary domain can also be a registered domain with a public MX record. In this case, a user with both a public and a primary domain address can receive external email at either address.

With Intelligent Routing enabled in Email Protection, Email Protection can receive and filter an email sent to a public domain address and then route the email directly to the appropriate mail server hosting the recipient’s mailbox. In this way, Email Protection can fulfill the role of an internal routing solution. In the meantime, Email Protection also filters the recipient’s email in the standard way, which is according to the recipient’s assigned group or primary domain policy.

In this case, the high-level configuration of the network for Email Protection might appear as follows:

**Figure 3: Multi-domain environment with Intelligent Routing public domain**

Note: A customer can have up to 10 public domains.

**How Employees Get Public Domain Email with Intelligent Routing**

To modify the previous example, employee Joe Smith, who works in Denver, has an email address on the public domain called **joesmith@acme.com**. Joe Smith also has an email address on the Denver primary domain called **joesmith@acme-denver.com**. When an email is sent to **joesmith@acme.com**, Email Protection filters the email according to the policy for Joe Smith and then sends the email to the server hosting his mailbox.

Another employee also named Joe Smith, who works in London, has an email address on the public domain called **jsmith@acme.com**. This employee cannot use **joesmith@acme.com** because this address is already used by Joe Smith in Denver and each email address in the public domain must be unique. Londoner Joe Smith also has an email address on the London primary domain called **joesmith@acme-uk.com**. When an email is sent to **jsmith@acme.com**, Email Protection filters the email according to the policy for this Joe Smith and then sends the email to the server hosting his mailbox.

If a single email is sent to both **joesmith@acme.com** and **jsmith@acme.com**, the email is filtered for each Joe’s assigned policy and sent to each Joe’s mailbox.

The following diagram illustrates a sample network with public and primary domains:
Figure 4: Email flow through Email Protection for a public domain

Detailed Example of Intelligent Routing

The following two figures detail how addressing works in a customer environment that uses a public domain, as well as domain aliases.

Detailed Example of Pulling Addresses from Active Directory

In the example in the following figure, the Acme Company has two Active Directories, in Denver and London, with public and primary domain addresses, including aliases. The figure shows how AD addresses are processed by Email Protection and Intelligent Routing to create addresses within Email Protection.

Important: If the same public domain email address is administered in the Active Directories of different company domains, the first instance of the address pulled into Intelligent Routing, regardless of the Active Directory it came from, becomes the valid address. Any other duplicates of this address that Intelligent Routing finds will be rejected.
**Detailed Example of Routing Messages to Primary and Public Domains**

In the example in the following figure, Email Protection filters and routes messages to employees of the Acme Company according to public domain addresses, as well as primary domain and domain alias addresses.

**Note:** Joe Smith in London cannot have the same public domain address as Joe Smith in Denver. In this example, Email Protection found the public domain address, *joesmith@acme.com*, through synchronization with the Denver Active Directory. As a result, the Active Directory for Joe Smith in London must use *jsmith@acme.com* for the public domain address.
To: joesmith@acme-uk.com
1. Domain is a primary domain.
2. Resolve recipient to primary address joesmith@acme-uk.com.
3. Filter mail per policies and route to destination inbound server for acme-uk.com.

To: joesmith@acme.com
1. Domain is a public domain for primary domains: acme-uk.com, acme-denver.com
2. Resolve recipient to primary address: joesmith@acme.com is found as an alias for primary address joesmith@acme-denver.com.
3. Filter mail per policies and route to destination inbound server for acme-denver.com.

To: jsmith@uk.acme.com
1. Domain is an alias domain for primary domain acme-uk.com.
2. Resolve recipient to primary address: joesmith@acme-uk.com is found.
3. Filter mail per policies and route to destination inbound server for acme-uk.com.

To: jsmith@acme.com
1. Domain is a public domain for primary domains: acme-uk.com, acme-denver.com
2. Resolve recipient to primary address: jsmith@acme.com is found as an alias for primary address joesmith@acme-uk.com.
3. Filter mail per policies and route to destination inbound server for acme-uk.com.

To: jsmith@denver.acme.com
1. Domain is an alias domain for primary domain acme-denver.com.
2. Resolve recipient to primary address: joesmith@acme-denver.com is found.
3. Filter mail per policies and route to destination inbound server for acme-denver.com.

To: joesmith@acme-denver.com
1. Domain is a primary domain.
2. Resolve recipient to primary address joesmith@acme-denver.com.
3. Filter mail per policies and route to destination inbound server for acme-denver.com.

1. Domain is an alias domain for primary domain acme-denver.com.
2. Resolve recipient to primary address: joesmith@acme-denver.com is found.
3. Filter mail per policies and route to destination inbound server for acme-denver.com.

Exchange - acme-uk.com
Exchange mailbox: joesmith@acme-uk.com

Company Mail Servers

Exchange - acme-denver.com
Exchange mailbox: joesmith@acme-denver.com
Prerequisites for Using Intelligent Routing

To setup and use Intelligent Routing, the following prerequisites must be met:

• Each destination mail server must have a unique primary domain and be accessible to Email Protection for delivery of email.
• Each user mailbox must have an email address in the primary and the public domain. Also, these primary and public domain addresses must be administered on both the mail server and the Email Protection Control Console.

**NOTE:** A public MX record is not required for primary domains. Therefore, a primary domain can be kept private and used only by Email Protection and the customer’s network. However, if desired, for example as a replacement for a published domain, a public domain can have an MX record.

Users with Multiple Email Addresses in the Public Domain

An employee might have multiple email addresses on the public domain. These addresses are treated the same way. For example, Joe Smith in Denver might have a second address of cowboy@acme.com. As with the other address joesmith@acme.com, Email Protection matches the cowboy address with Joe Smith’s primary domain address and routes the email from the public domain to server hosting Joe’s mailbox.

**Caution:** Depending on your service configuration, Email Protection supports up to 10 aliases for each user with a primary domain email address. This limit includes any public domain addresses for a user. However, if you use Directory Integration to add public domain addresses, all aliases and public domain addresses for a user will be added, even if they exceed 10.

Note also that, with Directory Integration, your Active Directory is the authoritative source for user addresses. However, a protected user doesn’t get updated by Directory Integration, but is administered manually in the Edit User Account screen in the Control Console. A protected user is kept on record no matter what the Active Directory records are for that user. If you don’t protect any users and are using Directory Integration, it is suggested that you disable the ability for users to manage user aliases. This parameter is set on the User Aliases screen under User Management.

Domain Aliases

Though you can continue to administer and use domain aliases for primary domains, you cannot administer domain aliases for a public domain.
Issues with Changing a Primary Domain to a Public Domain

The Risk of Removing a Primary Domain to Use Its Name for a Public Domain

If the domain that the customer wants to use as the public domain already exists as a primary domain within Email Protection, the primary domain must be replaced with a new primary domain first, the old primary domain deleted, and then the public domain assigned. For example, if company.com is currently listed as a primary domain, and the customer wishes to use it as the public domain, a new primary domain must first be created and configured (example, company-hq.com) and then company.com deleted from the system. At that time, your service provider can assign company.com as the public domain.

Warning: Deleting an existing primary domain also deletes all configuration data related to that domain. An administrator should configure the new primary domain before deleting the old primary domain. Also, the new primary domain must be configured before the public domain is assigned. Failure to heed this warning can result in loss of your primary domain and all data associated with it, including:

- Quarantine messages
- Domain policies
- Domain allow/deny lists
- All users
- User policies
- User passwords
- User preferences
- User allow/deny lists
- Groups/Group policy actions
- Any other non-default settings such as Spam Quarantine Report settings, Notifications, User Creation settings, etc.

Components You Must Configure for Intelligent Routing to Work

Service components that must be configured include:

- **Administrative Users:** Set up new Administrator accounts under the new primary domain prior to domain deletion.
- **Users:** Create all users under the new primary domain. Then contact your service provider to delete the old primary domain and create the public domain with the old primary domain name. Finally, as quickly as possible, define, for each user mailbox, an email address in the public domain and any applicable email aliases. Since your
MX record points to the name of the old primary domain, mail will be rejected after you delete the old primary domain until the public domain that uses that name is created and users are added to the public domain.

If your mail servers use Active Directory, it is strongly recommended that you use Directory Integration within Email Protection to add users. If you do not use Active Directory, it is strongly recommended that you use the batch file process for adding users to the public domain.

- **Spam Quarantine Reports:** Quarantined messages associated with the domain you are deleting will also be deleted. Therefore, before you delete the domain, you should notify all users who receive Spam Quarantine Reports for that domain to release any quarantined mail that they would like to retain.

- **Policies and Inbound/Outbound Servers:** Configure all policies and servers, both inbound and outbound, for the new primary domain before deleting the old primary domain and before assigning the public domain. Public domains do not have policies assigned to them. All policies and inbound/outbound server settings associated with the old primary domain are deleted along with the domain itself.

**Caution:** Rejection of mail is possible during the transition time after the current primary domain is deleted, during which the public domain is provisioned, and then user accounts are created in the public domain. To minimize lost email, coordinate the timing of event with your Email Protection service provider and schedule most work during off-hours.

---

### Administering Intelligent Routing

**Important:** If you are a new Email Protection customer and are implementing Intelligent Routing, do not redirect your MX record until you have administered Intelligent Routing and tested a public domain email address for each mail server in your network.

### Associate a Public Domain with a Primary Domain

After your primary domains are set up in Email Protection, contact your service provider to assign the public domain.

**Note:** Only your service provider operations personnel have permission to perform this task.

**Warning:** If the domain you want to use as the public domain already exists within Email Protection as a primary domain, the primary domain must be replaced with a new primary domain before the public domain can be assigned. Failure to do so can result in loss deletion of your primary domain and all data, including policies and users associated with it.
Where the Public Domain Appears in the Control Console After It Has Been Assigned

After the public domain has been assigned to a domain, the public domain name is displayed for reference on a number of Control Console administration pages, such as the User Management pages, the Setup pages, Reports, and the Domain Management page. In addition, the user Alias Addresses page allows the manual addition of a public domain alias.

Turn on Explicit User Creation

Explicit user creation means that you must add public email addresses using one of the methods that are described later. You must not use SMTP Discovery.

To turn on Explicit User Creation, perform the following steps:

1. Click Email Protection > Setup.
2. Click User Creation Settings.
3. Under the User Creation Mode heading, select Explicit.
4. Click Save.

Add a Public Domain Address to Test

To test the connection to public domain email addresses, you should first manually add, in both your mail server and the Control Console, a public domain address for a user. See Add Public Domain Email Addresses Manually.
Check the Availability of the Test Public Domain Address

After you add a public domain address for test user, and before you add the rest of your users, test the availability of the user’s public domain address.

**Note:** The following procedure might vary slightly depending on the specific Telnet application you use.

1. Install a Telnet application such as PuTTY on your computer.
2. Open your Telnet application.
3. Connect to your domain on the Email Protection application over port 25. If you type the Telnet command, the format of the command would be
   ```plaintext
telnet <primarydomain.com>.<EDS_Service_Domain_Name> 25
   ``
   where:
   - `<primarydomain.com>` is your company’s primary domain as administered in the Control Console
   - `<EDS_Service_Domain_Name>` is the domain name of your Email Protection service.

   For more information on these domain names, see your Service Activation Guide or your account representative.

   The application responds with a message such as: Connected to <primarydomain.com>.<EDS_Service_Domain_Name> <IP_Address>

4. Type `HELO <your_domain_name>`, for example, `denver.acme.com`. Press Enter.

   The application responds with: 250 <primarydomain.com>.<EDS_Service_Domain_Name> <IP_Address>.

5. Type `MAIL FROM:<your_email_address>`, for example, `joesmith@denver.acme.com`. Press Enter.

6. Type `RCPT TO:<test_public_domain_address>`, for example, `joesmith@acme.com`. Press Enter.

   The application responds with the message: 250 <user_public_domain_address> ok (RCPTMode: normal/deferred).

   Note: At this point, the user’s public domain address is recognized.

7. Type `DATA`, and press Enter.

   The application responds with: 354 Start mail input; end with <CRLF> . <CRLF>

8. Type a test message, then press `CTRL + f`.

9. Type a period (.), then press `CTRL + f` again.

10. Press Enter.

11. Type `QUIT`.

See the following sample inputs.
12 Log into the mailbox of the test public domain address you sent mail to.

13 Check that the message appears in the mailbox.

**View the Public Domain in the Domains List**

You can view public domains in the Domains List window to verify that they have been added. To view the public domains, perform the following steps:

1. Click **Account Management > Domains**.

   The Domains List is displayed.

2. Click the **Show Public Domains** checkbox.

   The public domains are listed along with the primary domains. The associated primary domain for a public domain is listed in brackets. The Type column displays **Public Domain** for a public domain.
3 To see the details of the primary domain associated with the public domain, click the name of the public domain.

**Add the Public Domain Email Addresses for Users**

You must add public domain email addresses for users so that Email Protection can then associate those addresses with users’ primary domain email addresses. You can add users’ public domain email addresses in three ways:

- Automatically, pulling the addresses from an Active Directory server using Directory Integration on the Control Console (the recommended approach) See Add Public Domain Email Addresses with Directory Integration.
- Automatically, pushing the addresses from an Active Directory server using Directory Services Connector, which is an add-on package to McAfee ePolicy Orchestrator (ePO). See Directory Services Connector.
- Manually using the User Aliases screen under User Management on the Control Console.
- Batch creation, which would include primary addresses, public domain addresses, and aliases.

**IMPORTANT:** It is required that you turn off SMTP Discovery on the User Creation Settings page and turn on Explicit.

**Caution:** Depending on your service configuration, Email Protection supports up to 10 aliases for each user with a primary domain email address. This limit includes any public domain addresses for a user. However, if you use Directory Integration to add public domain addresses, all aliases and public domain addresses for a user will be added, even if they exceed 10.

Note also that, with Directory Integration, your Active Directory is the authoritative source for user addresses. However, a protected user doesn’t get updated by Directory Integration, but is administered manually in the Edit User Account screen in the Control Console. A protected user is kept on record no matter what the Active Directory records are for that user. If you don’t protect any users and are using Directory Integration, it is suggested that you disable the ability for users to manage user aliases. This parameter is set on the User Aliases screen for each user listed under Account Management>Users.
Add Public Domain Email Addresses with Directory Integration

Set up Directory Integration

Directory Integration must be set up with the Sync Setup page before you can use this method of adding email addresses.

1. Click Account Management.
2. Click Configuration.

   The Directory Integration page is displayed.

3. Complete the Directory Settings section, if necessary. See the online help for more information.

4. Complete the Enable Automatic Synchronization and Approval fields, if necessary. See the online help for more information.
5 Scroll to the bottom of the page, and click the Exception Notification box. This box enables synchronization notifications and allows you to turn on the specific notifications you want. These notifications are a good way to help manage duplicate addresses in your public domain.

6 In the Exception Notification Distribution drop-down list, select the distribution list to which you want to send notifications. The lists that appear are those that you set up on the Customer Distribution Lists page.

7 In the Exception Notification Content, check the checkbox for each type of notification content you want. See the online help for more information on these fields.

**Manually run User Synchronization**

Run the User Synchronization to capture public domain email addresses from your domains’ Active Directories.

1 Click Users.

2 Click Sync.

3 Click Request Sync.

4 When the synchronization is complete, click Review to check the results.

5 If the list is satisfactory, click Approve.

6 Return to the Directory Integration screen and schedule automatic synchronization, if necessary. See “Set up Directory Integration” on page 14.

**Directory Services Connector**

As an alternative to using Directory Integration from the Control Console, you can synchronize your Active Directory (AD) using the Directory Services Connector, which is an add-on package to McAfee ePolicy Orchestrator (ePO). The Directory Services
Connector, because it is on your company premises, initiates a connection from your ePO and AD and "pushes" data to the Control Console. In contrast, when you set up and run Directory Integration from the Control Console, the Control Console initiates a connection to your Active Directory and "pulls" data from it. Unlike synchronizations run from the Control Console, Directory Services Connector also allows you to synchronize all email addresses identified in the Active Directory domain, including those that are in different email domains. From the Control Console, you must synchronize the addresses in one email domain at a time.

To configure the Control Console so that it will accept and add users sent from the Directory Services Connector, select “AD Domain” in the Logical Structure field on the Directory Integration window.

Note: Even though you run a synchronization with the Directory Services Connector, you can still review and approve the results of that synchronization in the Control Console.

For more information and to download and install the Directory Services Connector, contact your sales representative or go to http://download.mcafeesaas.com/directoryservicesconnector/.

Add Public Domain Email Addresses Manually

1. Click Account Management.
2. Click Users.
3. Select a user from the list, and click Edit.
4. Click Aliases.
5 In the Alias Address box for the public domain, type the recipient portion of the user’s email address.

6 Click the drop-down box for domain names and select the public domain name if there is more than one.

7 Click New.

The new public domain address is added and appears under the Public Domain Addresses list.

### Add Batches of Public Domain Email Addresses, Without Directory Integration

You can add multiple user accounts at one time using the batch method. Following are the rules for creating multiple user accounts in this window:

- All user accounts and alias email addresses must be unique within the system.
- All new user accounts will be added with the role of User.
- All the user accounts added in the same batch will use the same user-level policy configurations that are defined in this window.

**Note:** For security reasons, all new user accounts added using this method will not have passwords assigned (passwords will be set to a null value). However, you can also add multiple passwords at one time using a batch file. For more information, access the User Authentication screen at Account Management > Users > Configuration > User Authentication. Then click Help.
1. Open a text editor, for example Notepad, to create your file of addresses. On the first line of the file, type the primary domain address for a user, followed by a username, if any, then followed by the public domain address or any other alias addresses for the user, all separated by a comma. Alias addresses must also be fully-qualified addresses and can include different domain names than that of the primary address.

For example, Joe Smith in Denver has the following addresses administered in the Active Directory:

- A primary domain address of joesmith@denver-acme.com
- A username of joesmith
- A public domain address of joesmith@acme.com
- An alias address of jsmith@denver-acme.com

On a single line, you would type the following in the Email Address box for Joe Smith:

joesmith@acme-denver.com, joesmith, joesmith@acme.com, jsmith@acme-denver.com

Note: User account names cannot contain any of the following special characters:

- Spaces at the beginning, middle, or end of the user account name
- Comma (, )
- Double quotes (" )
- Left arrow (<)
- Right arrow (>)
- Semi-colon (;)

See the following example:

- The username can include a domain name with the format `<domain>/<username>`, for example:
  jsmith@denver.acme.com, acme\joesmith, joesmith@acme.com. The domain portion can contain 1-15 alphanumeric characters as well as the following symbols (no spaces): ! @ # $ % ^ & ( ) - _ ' { } . ~

- If the local name, or handle, portion of an email address contains commas, you must enclose that portion of the address in double-double quotes (" "). Example: ""smith,j""@denver.acme.com, joesmith@acme.com, jsmith@denver.acme.com, joemith@denver.acme.com

- If you do not include a username for a user, you must still include the commas to specify that there is no username.
Example: joesmith@denver.acme.com, , joesmith@acme.com
• Up to five aliases can be created per user, depending on your company’s configuration.

2 Press the Enter key or an equivalent key to create a hard return and start a new line in the file.

3 Repeat Steps 1 and 2 for each user you want to enter.

4 Save the file to your computer’s hard drive with a filename of your choice. The file size can be up to 100 KB.

5 Click **Account Management**.

6 Click **Users**.

7 Click **New**.

8 From the Creation Mode drop-down list under Create Users, select **Batch**.

   The New User screen changes to show batch creation fields.

9 Click the **Browse** button and search for the file you just created.

10 Click **Upload**.

11 In the **Type** drop-down menu, select **User**.

12 In the **Group Membership** drop-down menu, do one of the following:

   • Select **Ungrouped**.
• If all users are in the same group and a group has been defined, select the group to which the users should be assigned.

13 In the **Time Zone** drop-down menu, select the time zone used to timestamp incoming email. The time zone represents the offset from Greenwich Mean Time (GMT).

14 Click **Save**.

## How the Public Domain Affects Reports

If a primary domain has a public domain assigned, then messages sent to the public domain addresses are in reports that are separate from those of the primary domain. In addition, primary domain reports do **not** include messages sent to public domain addresses.

**NOTE:** To see a report that includes both public domain and primary domain messages, you must select **All Domains** for a particular report. This report includes all primary domains and the public domain.

To generate a report for the public domain, perform the following steps:

1. Click **Email Protection**.
2. Click **Reports**.
3. Click the **Domain** drop-down box.

   The list of primary, alias, and public domains is displayed. Alias names have “[alias]” appended to the name. Public domains have the primary domain in brackets “[primary domain]” appended to the name.

4. Select the domain name for which you want to view report data.
Report data for the associated primary domain’s portion of the public domain is displayed.