How to Migrate Your MailFoundry Account

https://campus.barracuda.com/doc/96022994/

This article lists the steps needed to finish the migration of your mailfoundry email account to Email Gateway Defense.

The following steps have already been completed for your account migration:

1. Barracuda Networks has migrated configuration information from your mailfoundry account.
2. Barracuda Networks has created an administrator account for your organization in Email Gateway Defense. You will have a chance to reset the password for this account.

You should have received an email from Barracuda Networks outlining the high level steps. Follow the steps below to finish migrating your account to Email Gateway Defense.

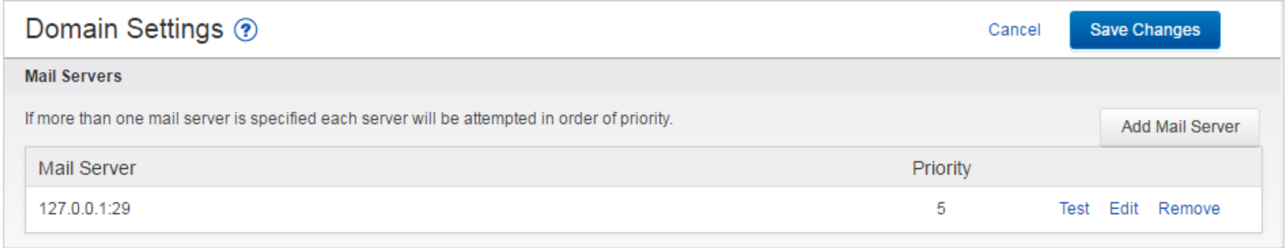
Step 1. Log in as Administrator

This step ensures you have administrator level access to your account.

1. Click the link sent to you in an email from Barracuda Networks. The login page displays.
2. Click **Request Password**. A new password is sent to the email address on file.
3. When you receive the email, click on the link in the email to reset the password.
4. Enter a new secure password. Remember that this is the password for your administrator account. For security, do not share this password with anyone.
5. Once you are logged in with the new password, click **Email Gateway Defense** in the left navigation pane; the **Overview > Dashboard** page displays and you are logged into Email Gateway Defense as *administrator:*

Step 2. Verify Domains and Configuration

1. Click the **Domains** tab. The **Domains Manager** page displays. Confirm each of your domains is listed here.
2. Double check that the IP address of the Mail Server for each host is correct. If it is not correct for a domain, click **Edit** in the **Settings** column for that domain to make modifications:



Domain Settings ?

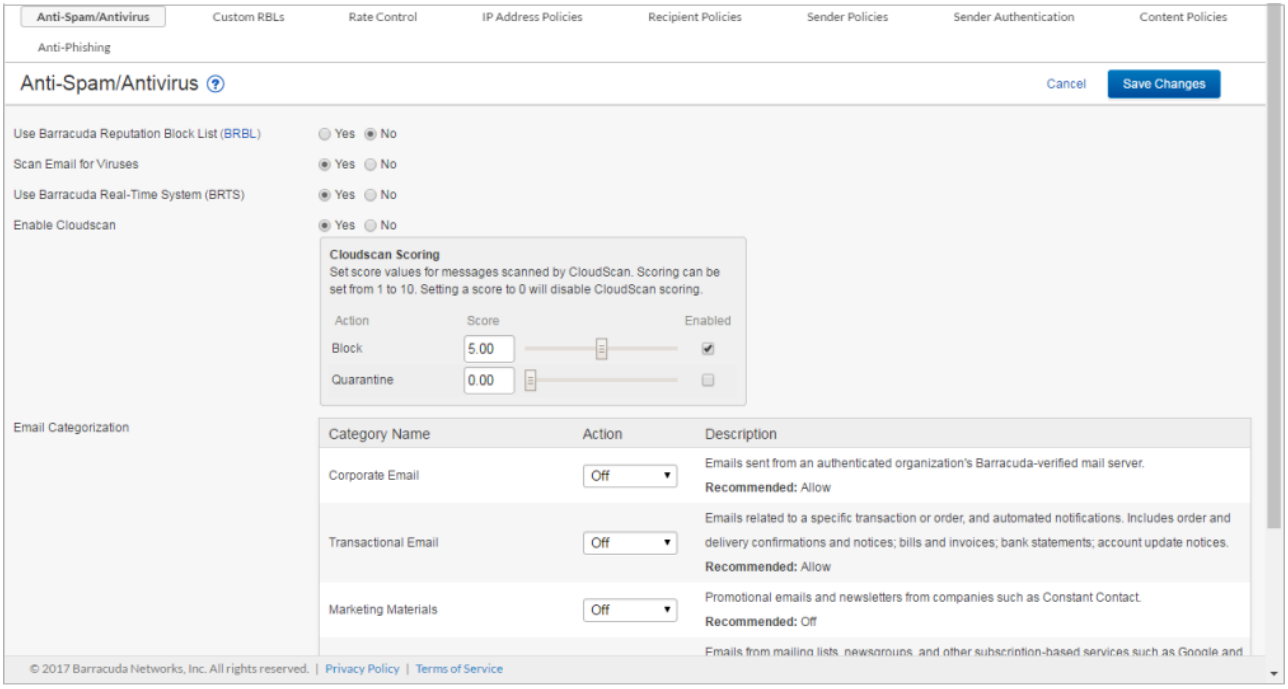
Mail Servers

If more than one mail server is specified each server will be attempted in order of priority.

Mail Server	Priority	
127.0.0.1:29	5	Test Edit Remove

3. Verify the IP address for the mail server for the domain, and click **Save Changes**.

   Connectivity from Email Gateway Defense to the mail server is verified in a separate step.
4. In the **Domains** page, for each of the domains, click **Manage** in the **Domain Options** section, one domain at a time.
5. For each domain, verify all settings on the **Inbound Settings** pages are correct for each sub-tab: Anti-**Spam/Antivirus**, **Custom RBLs**, **Rate Control**, **IP Address Policies**, **Recipient Policies**, **Sender Policies**, **Sender Authentication**, **Content Policies**, and **Anti-Phishing**. Use these pages to create policies for inbound mail.



Anti-Spam/Antivirus ?

Use Barracuda Reputation Block List (BRBL) ○ Yes ● No

Scan Email for Viruses ● Yes ○ No

Use Barracuda Real-Time System (BRTS) ● Yes ○ No

Enable Cloudscan ● Yes ○ No

Cloudscan Scoring
Set score values for messages scanned by CloudScan. Scoring can be set from 1 to 10. Setting a score to 0 will disable CloudScan scoring.

Action	Score	Enabled
Block	5.00	☑
Quarantine	0.00	□

Email Categorization

Category Name	Action	Description
Corporate Email	Off	Emails sent from an authenticated organization's Barracuda-verified mail server. **Recommended:** Allow
Transactional Email	Off	Emails related to a specific transaction or order, and automated notifications. Includes order and delivery confirmations and notices; bills and invoices; bank statements; account update notices. **Recommended:** Allow
Marketing Materials	Off	Promotional emails and newsletters from companies such as Constant Contact. **Recommended:** Off
		Emails from mailing lists, newsgroups, and other subscription-based services such as Google and

© 2017 Barracuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

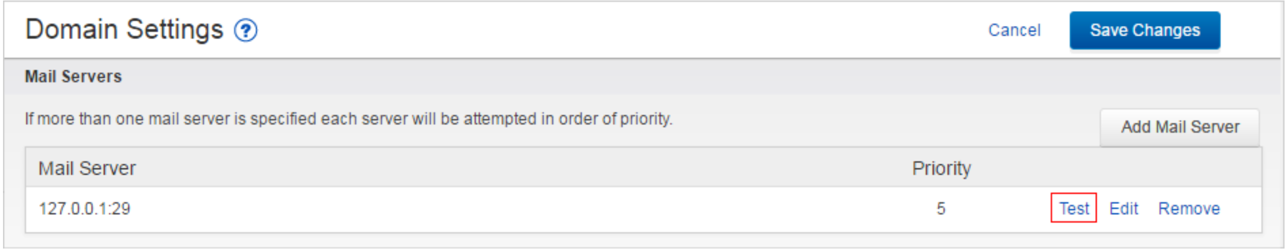
Step 3. Ensure Connectivity

1. If you have trouble routing email traffic through the service, make sure that your firewall allows traffic originating from Email Gateway Defense. To allow mail traffic from the service, open your firewall ports to allow the IP address ranges such that your LDAP and Microsoft Exchange servers can communicate with Email Gateway Defense based on your instance; see Email Gateway Defense IP Ranges for a list of ranges based on your instance.
2. Additionally, open these ports in your corporate firewall to allow communication between Email Gateway Defense and remote servers:

Port	Direction	Used for

25	In/Out	SMTP
389	In/Out	LDAP
636	In/Out	LDAP

3. To ensure that the service can send traffic to the mail servers listed for each of your domains, click **Domains Manager**.
4. Click **Edit** in the **Settings** column for the first domain in the list; t he **Domains > Domain Settings** page for this domain displays. click **Test**:



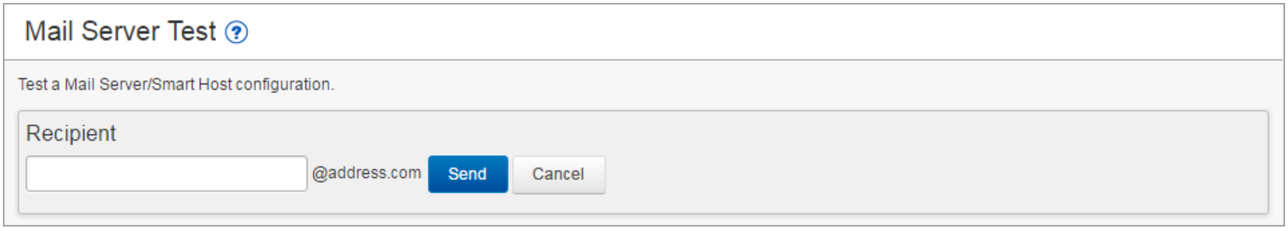
Domain Settings

Mail Servers

If more than one mail server is specified each server will be attempted in order of priority.

Mail Server	Priority	
127.0.0.1:29	5	Test Edit Remove

5. The **Mail Server Test** page displays:



Mail Server Test

Test a Mail Server/Smart Host configuration.

Recipient

@address.com

6. Enter the username of a mailbox on the server that you can readily test, and click **Send**. If the email is routed correctly, a **Success** message displays. If the **Success** message does not display and the recipient does not receive the test email, double check the steps above. If a problem persists, see the troubleshooting section below.
7. Verify that Email Gateway Defense is able to reach your configured LDAP server. Go to **Domains > Domain Manager > Settings**, configure your LDAP host and click **Test Settings**. If you have problems connecting, open your firewall ports as described below.

Troubleshooting

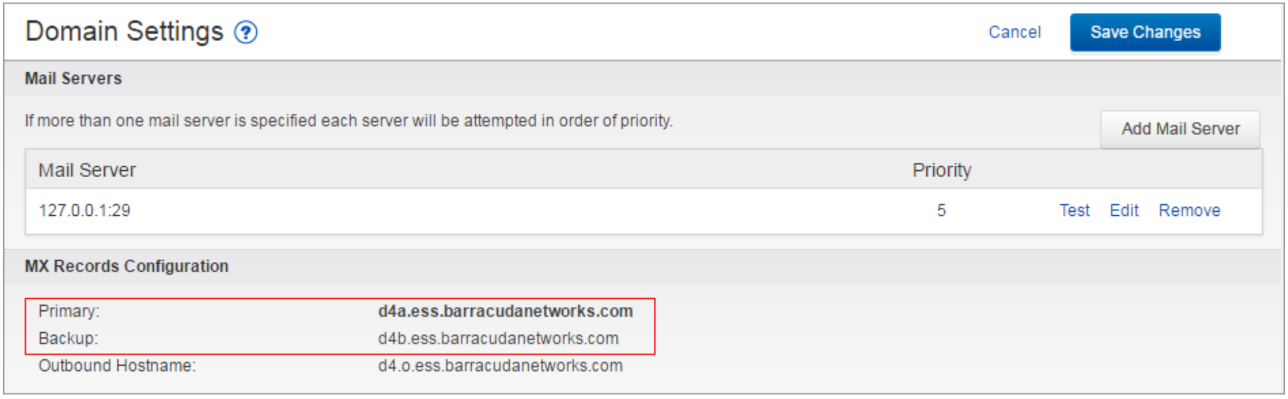
Verify that your firewall allows traffic originating from Email Gateway Defense. To allow mail traffic from the service, open your firewall ports to allow the IP address ranges based on Barracuda Networks instance such that your LDAP and Microsoft Exchange servers can communicate with Email Gateway Defense .

Additionally, open these ports in your corporate firewall to allow communication between Email Gateway Defense and remote servers.

Port	Direction	Used for
25	In/Out	SMTP
389	In/Out	LDAP
636	In/Out	LDAP

Step 4. Route Email through Email Gateway Defense

1. Go to the **Settings** page for this domain.
2. Make note of the two MX records listed under the **MX Records Configuration** section. They are listed as **Primary** and **Backup**:



Mail Servers

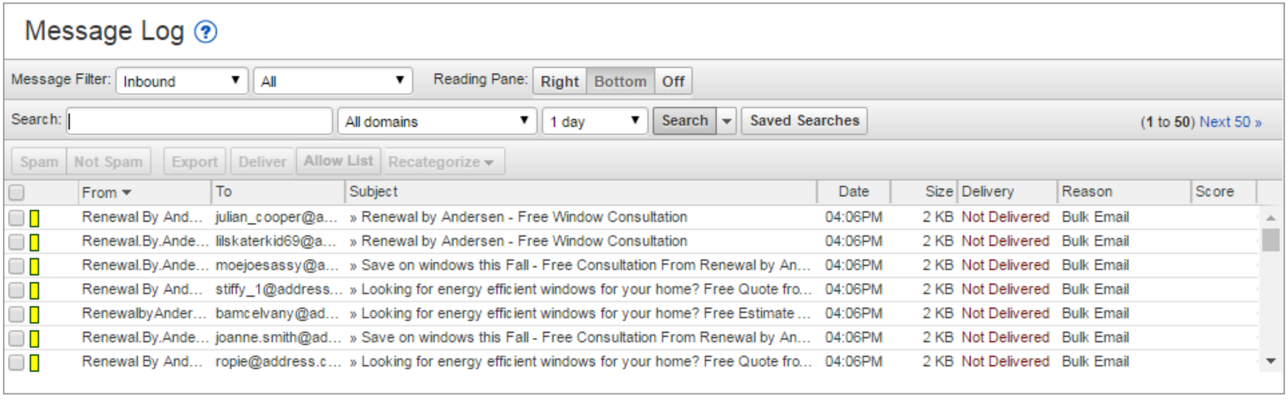
If more than one mail server is specified each server will be attempted in order of priority.

Mail Server	Priority	
127.0.0.1:29	5	Test Edit Remove

MX Records Configuration

Primary:	**d4a.ess.barracudanetworks.com**
Backup:	d4b.ess.barracudanetworks.com
Outbound Hostname:	d4.o.ess.barracudanetworks.com

3. Log in to your ISP or hosting provider and change the MX records to the records listed above.
4. Depending on your ISP settings, this change can take a few minutes to a few hours to complete. Once complete, email begins flowing through Email Gateway Defense.
5. Go to the **Overview > Message Log** page to look for incoming email. Your email is now being filtered by Barracuda Networks:



Message Filter: Inbound ▾ All ▾ Reading Pane: Right Bottom Off

Search: | All domains ▾ | 1 day ▾ | (1 to 50) Next 50 »

☐		From ▾	To	Subject	Date	Size	Delivery	Reason	Score
☐	▯	Renewal By And...	julian_cooper@a...	» Renewal by Andersen - Free Window Consultation	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	Renewal.By.Ande...	lilskaterkid69@a...	» Renewal by Andersen - Free Window Consultation	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	Renewal.By.Ande...	moejoesassy@a...	» Save on windows this Fall - Free Consultation From Renewal by An...	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	Renewal By And...	stiffy_1@address...	» Looking for energy efficient windows for your home? Free Quote fro...	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	RenewalbyAnder...	bamcelvany@ad...	» Looking for energy efficient windows for your home? Free Estimate ...	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	Renewal.By.Ande...	joanne.smith@ad...	» Save on windows this Fall - Free Consultation From Renewal by An...	04:06PM	2 KB	Not Delivered	Bulk Email	
☐	▯	Renewal By And...	ropie@address.c...	» Looking for energy efficient windows for your home? Free Quote fro...	04:06PM	2 KB	Not Delivered	Bulk Email	

Repeat this process for each additional domain.

Important
If you have **Sender Policy Framework** (SPF) checking enabled on your mail server or network, it is critical when using Email Gateway Defense that you either disable SPF checking in the service or add the Email Gateway Defense IP ranges based on your instance to your SPF exemptions. Otherwise, your SPF checker blocks mail from domains with an SPF record set to **Block** because mail is coming from an Email Gateway Defense IP address not in the sender's SPF record.

See Also

Outbound policy and encryption settings:

- How to Use DLP and Outbound Mail Encryption
- Outbound Filtering Policy

Advanced topics:

- Advanced Configuration (Sender Authentication, SPF, Recipient Verification)
- Managing User Accounts
- Reporting

Figures

1. domainSettings.png
2. antiSpamAntivirus.png
3. clickTest.png
4. MailServerTest.png
5. MXRecords.png
6. Message_Log.png