Step 2 - Configure Email Gateway Defense for Exchange 2013 and Other On-Premise Mail Servers

https://campus.barracuda.com/doc/96022760/

Use this article to deploy Email Gateway Defense for Exchange 2013 and other on-premise mail servers in your environment.

Important

Exchange user interfaces can change; refer to Microsoft documentation for configuration details.

Step 1. Ensure Connectivity and Redundancy

- Open your firewall ports to allow the IP address ranges based on your Barracuda Networks instance; see Email Gateway Defense IP Ranges Used for Configuration for a list of ranges based on your Barracuda Networks instance
- Where relevant, verify your network subnet is granted access to your mail server ACL and LDAP server
- Block all port 25 traffic except for that originating from Email Gateway Defense IP Ranges Used for Configuration based on your Barracuda Networks instance

Step 2. Launch the Email Gateway Defense Setup Wizard

Alternatively, you can manually set up Email Gateway Defense using the web interface.

Configure Domain

1. Log into Email Gateway Defense, and go to the **Domains** page.
2. Click **Add Domain**, and enter the following in the dialog box:
    1. Enter the primary Exchange domain name you want to filter, for example: corpdomain.com
    2. Enter the mail server hostname (FQDN) or IP address for the entered domain, for example: corpdomain-com.mail.protection.outlook.com
3. Click **Add**; the **Domains > Domain Settings** page displays. If you are adding multiple mail servers, assign a priority level, and click **Add**.

1. Log into Email Gateway Defense, and click the link to launch the Email Gateway Defense Setup

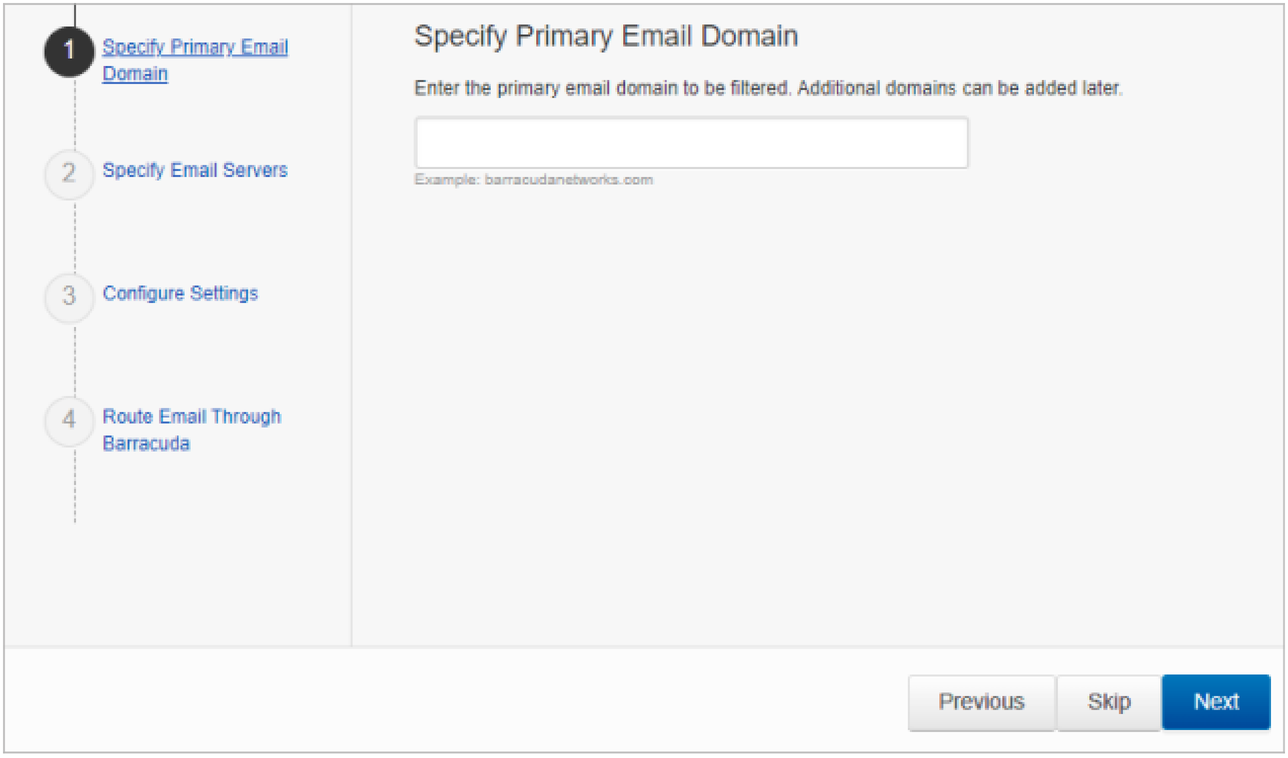
wizard.

2. Select the **Region** for your Data Center. Then click **Get Started** .

   After you select your region, you cannot change it.

   The **Specify Primary Email Domain** page displays.

3. Enter the primary Exchange domain you want to filter, for example: `cudaware.com`



Specify Primary Email Domain

Enter the primary email domain to be filtered. Additional domains can be added later.

Example: barracudanetworks.com

1 Specify Primary Email Domain
2 Specify Email Servers
3 Configure Settings
4 Route Email Through Barracuda
Previous
Skip
Next

4. Click **Next**. The **Specify Email Servers** page displays. Enter the mail server hostname (FQDN) or IP address for the domain entered in the previous step,

   If the Email Gateway Defense Setup wizard has already identified your mail server IP based on the MX record, the **Mail Servers** field pre-populates.

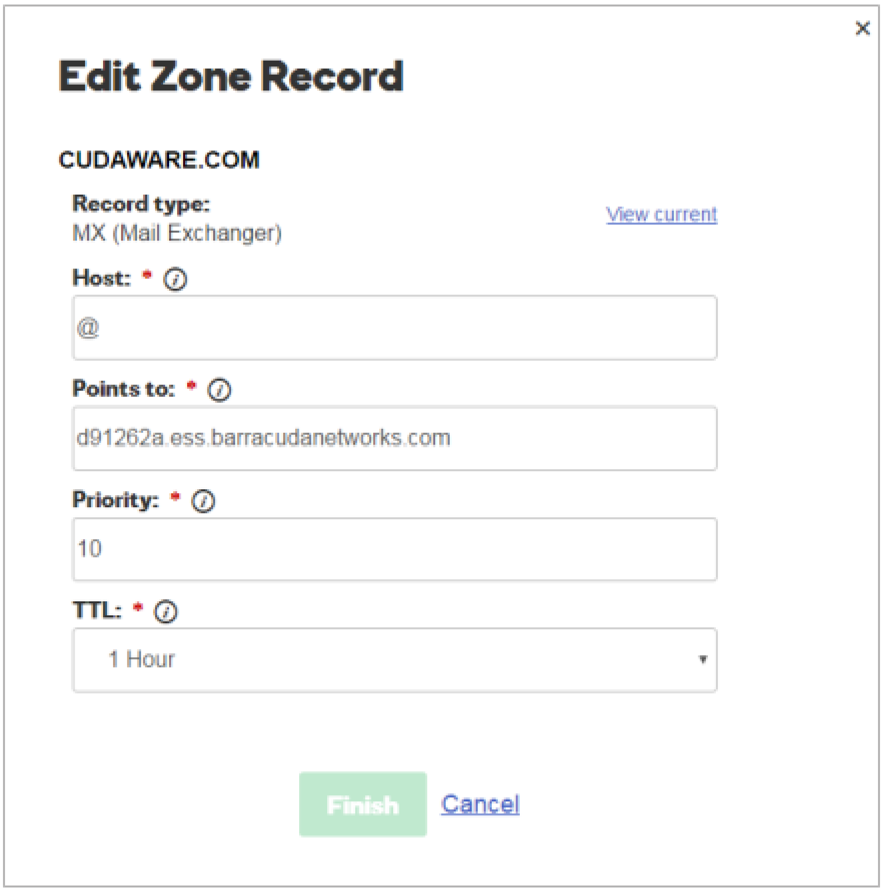
5. Click **Add**. Enter an email address to test the server configuration, and click **Test All Mail Servers**.
6. Once the mail server is verified, the **Verified** (✓) icon displays in the status column and a confirmation message displays at the top of the page.
7. Click **Next**. The **Configure Settings** page displays. Select from the following options:
   1. **Virus Protection** – Set to **On** to direct Email Gateway Defense to detect and block viruses on inbound email.
   2. **Spam Protection** – Set to **On** to direct Email Gateway Defense to evaluate inbound mail for spam based on a score assigned to each processed message. When set to **Off** inbound mail is not scanned for spam.
   3. **Spam Scoring** – Set **Spam Protection** to **On** to enable **Spam Scoring**. Scoring ranges from 1 (definitely not spam) to 10 (definitely spam). Setting a score of '1' will likely block legitimate messages while setting a score of '10' will allow more messages through the system. Based on this score, Email Gateway Defense blocks messages that appear to be spam and logs these messages in the user's Message Log with **Score** as the reason for the block.

      The following features, configured on the **Inbound Settings > Anti-**

Spam/Antivirus page, are enabled when **Spam Protection** is set to **On**:

- **Barracuda Reputation Block List (BRBL)** – Database of IP addresses manually verified to be a noted source of spam.
- **Barracuda Real-Time System (BRTS)** – Advanced service to detect zero-hour spam and virus outbreaks even where traditional heuristics and signatures to detect such messages do not yet exist. Each quarantined message has a reason of **BRTS** in the Message Log.
- **Sender Policy Framework (SPF)** – Block Fail is disabled.
- **Barracuda Anti-Fraud Intelligence** – Barracuda Networks anti-phishing detection which uses a special Bayesian database for detecting Phishing scams.
- **Intent Analysis** – Blocking based on intent analysis.
- **CloudScan Scoring** – A cloud-based spam scanning engine which assigns a score to each message processed ranging from 0 (definitely not spam) to 10 (definitely spam).

8. Click **Next**. The **Route Email Through Barracuda** page displays.
9. To verify your domain, replace your current MX records with the Email Gateway Defense Primary and Backup MX records displayed on the page:



Edit Zone Record

CUDAWARE.COM

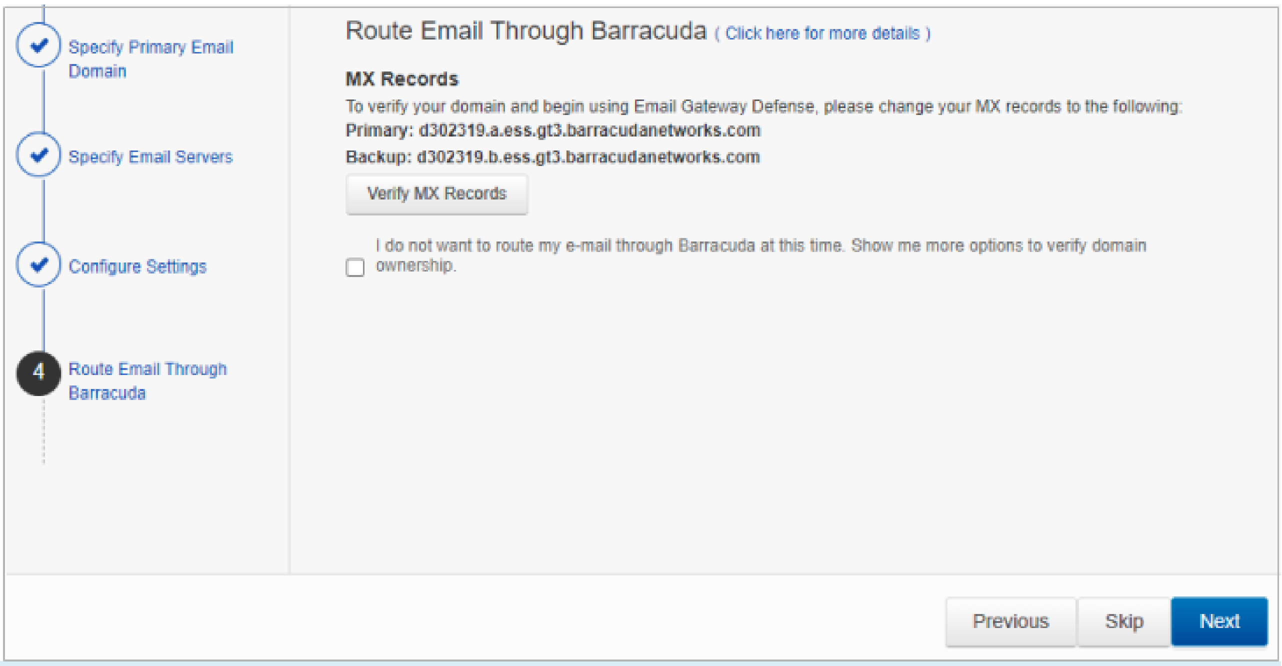
Record type: MX (Mail Exchanger)

Host: * @

Points to: * d91262a.ess.barracudanetworks.com

Priority: * 10

TTL: * 1 Hour



Route Email Through Barracuda (Click here for more details)

MX Records

To verify your domain and begin using Email Gateway Defense, please change your MX records to the following:

Primary: d302319.a.ess.gt3.barracudanetworks.com

Backup: d302319.b.ess.gt3.barracudanetworks.com

□ I do not want to route my e-mail through Barracuda at this time. Show me more options to verify domain ownership.

During the evaluation period, to complete the verification process but allow your legitimate mail to continue using your current mail server, you can add the MX records with a low priority, for example, *99*.

Some mail may appear in the Message Log after making this MX record change as spammers routinely send mail to all MX records for a domain.

Once you have made the change to your MX records, return to the **Route Email Through Barracuda** page and click **Verify MX Records**. Email Gateway Defense should see the changes made and verify your domain. If the domain does not verify correctly, verify that your MX changes are live. You can do this by using the following sites that return your MX information:

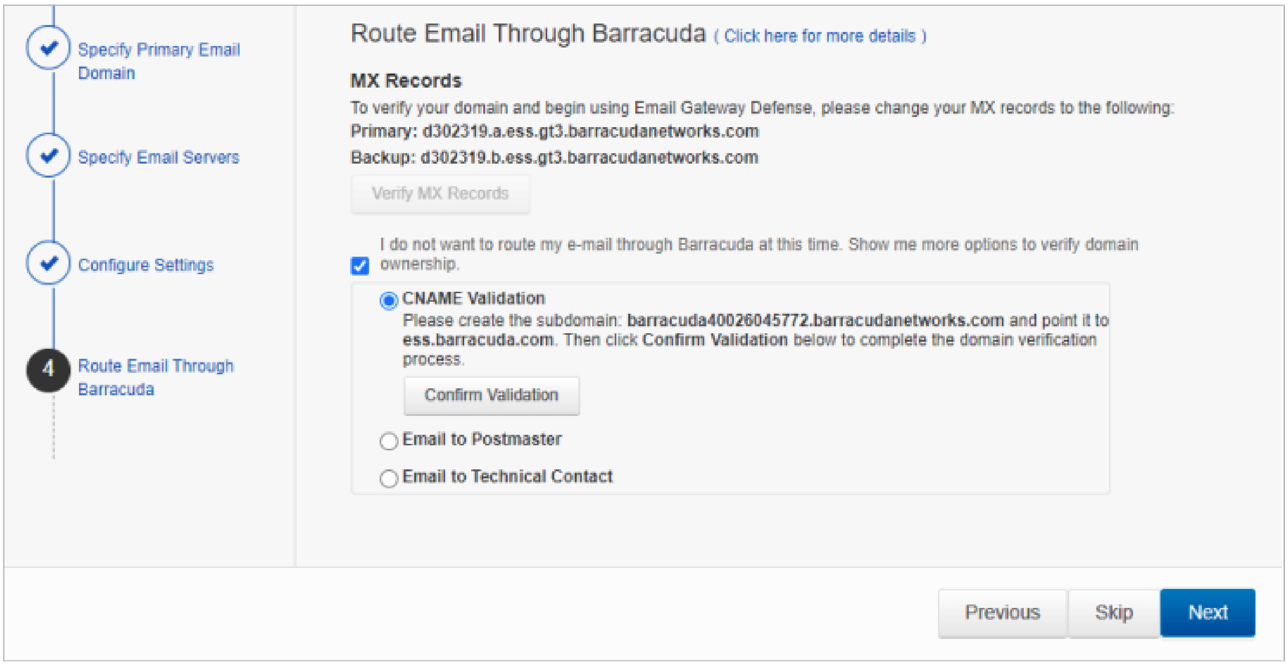
http://mxtoolbox.com/

https://toolbox.googleapps.com/apps/dig/ (select the MX option)

If your domain's MX records do not display in the Email Gateway Defense MX records, you must wait until they display before your domain can be verified.

Note that after verifying your domain, any mail sent to your domain from another Barracuda Email Gateway Defense customer will be processed normally by your Email Gateway Defense account and not delivered via MX records.

10. If you choose not to change your MX records, you can use another method to verify your domain. Select **I do not want to route my e-mail through Barracuda at this time**:



Route Email Through Barracuda (Click here for more details)

MX Records

To verify your domain and begin using Email Gateway Defense, please change your MX records to the following:

Primary: d302319.a.ess.gt3.barracudanetworks.com

Backup: d302319.b.ess.gt3.barracudanetworks.com

☑ I do not want to route my e-mail through Barracuda at this time. Show me more options to verify domain ownership.

● CNAME Validation

Please create the subdomain: **barracuda40026045772.barracudanetworks.com** and point it to **ess.barracuda.com**. Then click **Confirm Validation** below to complete the domain verification process.

○ Email to Postmaster

○ Email to Technical Contact

11. Select the verification option:
    1. **CNAME Records** – To use the CNAME records method to verify the domain ownership:
        1. Log into your DNS Server and, under this domain, create a subdomain whose name is created by concatenating 'barracuda' and the CNAME token shown in the **Route Email Through Barracuda** page. For example: barracuda30929916985.corpdomain.com
        2. Point the CNAME record of that subdomain to **ess.barracuda.com**

           Allow the DNS propagation to take effect before proceeding.
        3. Click **Confirm Validation** in the **Route Email Through Barracuda** page.
    2. **Email to Technical Contact** – This method sends a verification email to the technical contact email address, if it exists, listed on your domain's WHOIS entry.

       This verification option is not available if Email Gateway Defense cannot find your domain's WHOIS entry. If there is not a technical contact, then only the **MX Records**, **CNAME**, and **Email to the Postmaster** options displays on this page.
    3. **Email to the postmaster** – This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.

       This option is available if Email Gateway Defense can find your postmaster in your domain’s WHOIS records. This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.
12. Click **Next**, and click **Next** again.
13. On the **Select Data Center Region** page, select the data center for your locale, and click **Get Started**.
14. Complete the wizard pages.
15. The **Confirmation** page displays. Confirm domain ownership, and then click **Done**.

Step 3. Set Up User Accounts

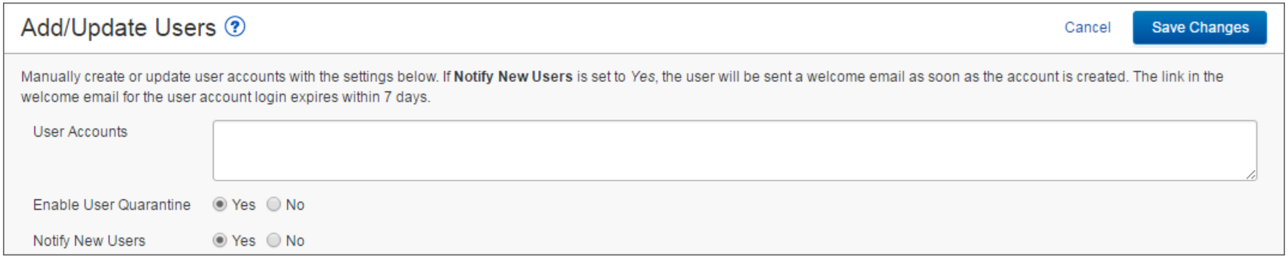
You can add users manually, or use your organization's LDAP server or Microsoft Entra ID service to automatically synchronize Email Gateway Defense with your active directory server. To create a few test accounts during the evaluation period, use the **Manually Add Users** steps below.

Decide whether or not you want to enable user quarantine. When enabled, users have quarantine accounts and can decide whether or not mail is spam. Users can also create their own sender allow list and block list. Manually add a few test accounts on the **Users > Add/Update Users** page, and set **Enable User Quarantine** to **Yes**. The first time Email Gateway Defense receives an email for that user and the message is quarantined, the user receives a quarantine notification email at the scheduled quarantine notification interval.

> Depending on how you have configured the quarantine notification interval on the **Users > Quarantine Notification** page, the user receives a quarantine digest at a specified time. From the **Users > Quarantine Notification** page you can also allow the user to set their own quarantine notification interval.

Manually Add Users

1. Go to **Users > Add/Update Users**:



Manually create or update user accounts with the settings below. If **Notify New Users** is set to *Yes*, the user will be sent a welcome email as soon as the account is created. The link in the welcome email for the user account login expires within 7 days.

User Accounts

Enable User Quarantine ● Yes ○ No

Notify New Users ● Yes ○ No

2. In the **User Accounts** field, enter each user email address for the domain on a separate line, and then select from the following options:
   1. **Enable User Quarantine** – All emails for the user which meet the configured block policy go to the user's quarantine account.

      > Depending on how you have configured the quarantine notification interval on the **Users > Quarantine Notification** page, the user receives a quarantine digest at a specified time. From the **Users > Quarantine Notification** page you can also allow the user to set their own quarantine notification interval.

   2. **Notify New Users** – When set to **Yes**, users receive a welcome email when the account is created.
3. Click **Save Changes**. The users are added to the **Users > Users List** table where you can select from the following actions:

   1. **Edit** – Click to specify domains this user can manage.
   2. **Reset** – Click to send the user an email with instructions on how to reset their account password.
   3. **Log in as this user** – Click to view or change the user's settings (for example, quarantine notifications), v iew/manage the domains this user manages, and v iew/search/manage the user's Message Log.
   4. **Delete** – Click to remove the user account.
4. Click **Save Changes**; the **Users List** displays.

The first time Email Gateway Defense receives an **Allowed** email for a non-existent user at a domain configured for the service, if that same recipient receives a second email 1-6 days later, a new user account is created. This method of new account creation does not use LDAP lookup, and the user receives an email from Email Gateway Defense with their login information so they can access their quarantine account.

Automatically Add Users

You can configure user authentication via your organization's LDAP server or Microsoft Entra ID service. For complete setup details, see the following articles:

- How to Configure User Authentication with Microsoft Entra ID
- How to Configure User Authentication Using LDAP

Step 4. Configure Outbound Mail Scanning

1. Log into Email Gateway Defense, and go to **Outbound Settings > Sender IP Address Ranges**.
2. Enter the IP Address and Domain Name (logging domain) and optional **Comment** for IP address ranges allowed to send outgoing email from your domains. Click **Add**.
   Note that Barracuda Networks policy requires all outbound IP addresses to have a rDNS (PTR) record.
   This requirement is for the security of our service and your email. This policy stops spammers from signing up to our service, adding hundreds of outbound IP addresses, and using our service to send out massive spam attacks. For security reasons, there are no exceptions to this policy.
   If you are using an IP or ISP that does not provide a rDNS (PTR) record for your IP, Barracuda Networks recommends either moving to a different ISP, or routing your mail through another ISP/Service that does provide an rDNS (PTR) record. For example, Microsoft 365.
3. Add all IP addresses from which outgoing mail is allowed to flow through Email Gateway Defense. The **Logging Domain** is the domain name that appears in the **Message Log** as the sending domain for the associated IP address.

Note that if there are multiple domains sending from a single IP address through Email Gateway Defense, you only need to configure one Logging and Policy Domain entry.

Step 5. Configure Sender Policy Framework for Outbound Mail

To ensure Barracuda Networks is the authorized sending mail service of outbound mail from Email Gateway Defense, add the following to the Sender Policy Framework (SPF) record INCLUDE line of the SPF record for your sending mail server for each domain sending outbound mail. Select the relevant SPF INCLUDE based on the region you selected for your Barracuda Networks instance:

AU (Australia)

```
include:spf.ess.au.barracudanetworks.com -all
```

CA (Canada)

```
include:spf.ess.ca.barracudanetworks.com -all
```

DE (Germany)

```
include:spf.ess.de.barracudanetworks.com -all
```

IN (India)

```
include:spf.ess.in.barracudanetworks.com -all
```

UK (United Kingdom)

```
include:spf.ess.uk.barracudanetworks.com -all
```

US (United States)

```
include:spf.ess.barracudanetworks.com -all
```

See Sender Authentication for more information.

- If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Networks instance. For example: `include:spf.ess.barracudanetworks.com -all`
- If you do not have an SPF record set up for your domain, use the following value to create a TXT record that creates a HARDFail SPF for your domain based on your Barracuda Networks instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

For additional configuration options and features, log into the web interface, and click **Help**.

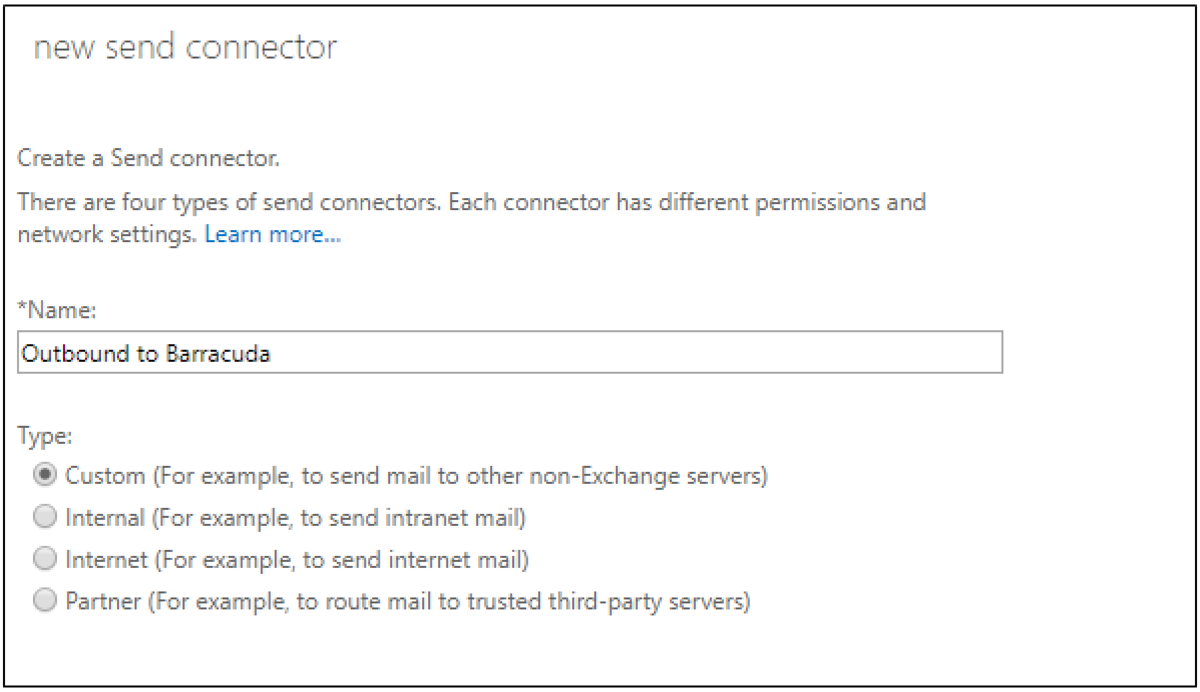
Step 6. Configure Your Exchange Mail Server

If you have multiple domains configured on Exchange, you only need to create one send connector. You can use any one of the outbound smarthosts to make the send connector.

Each of the domains that you want to be able to send email *must* be added to Email Gateway Defense. Be sure to add all of your accepted domains into Email Gateway Defense before configuring outgoing email in this section.

*Before you begin, log into Email Gateway Defense, and go to **Domains > Domain Manager**. Note the **Outbound Hostname** for the domain that is to relay outbound mail. You will use this information in Step 4c below.*

1. Log into your Exchange Admin Center.
2. In the left navigation panel, select **Mail Flow**, then **Send Connectors**.
3. Click the Plus icon to create a new send connector. Enter the following information:
   1. **Name**: Outbound to Barracuda
   2. **Type**: Custom



new send connector

Create a Send connector.

There are four types of send connectors. Each connector has different permissions and network settings. Learn more...

*Name:

Outbound to Barracuda

Type:

● Custom (For example, to send mail to other non-Exchange servers)

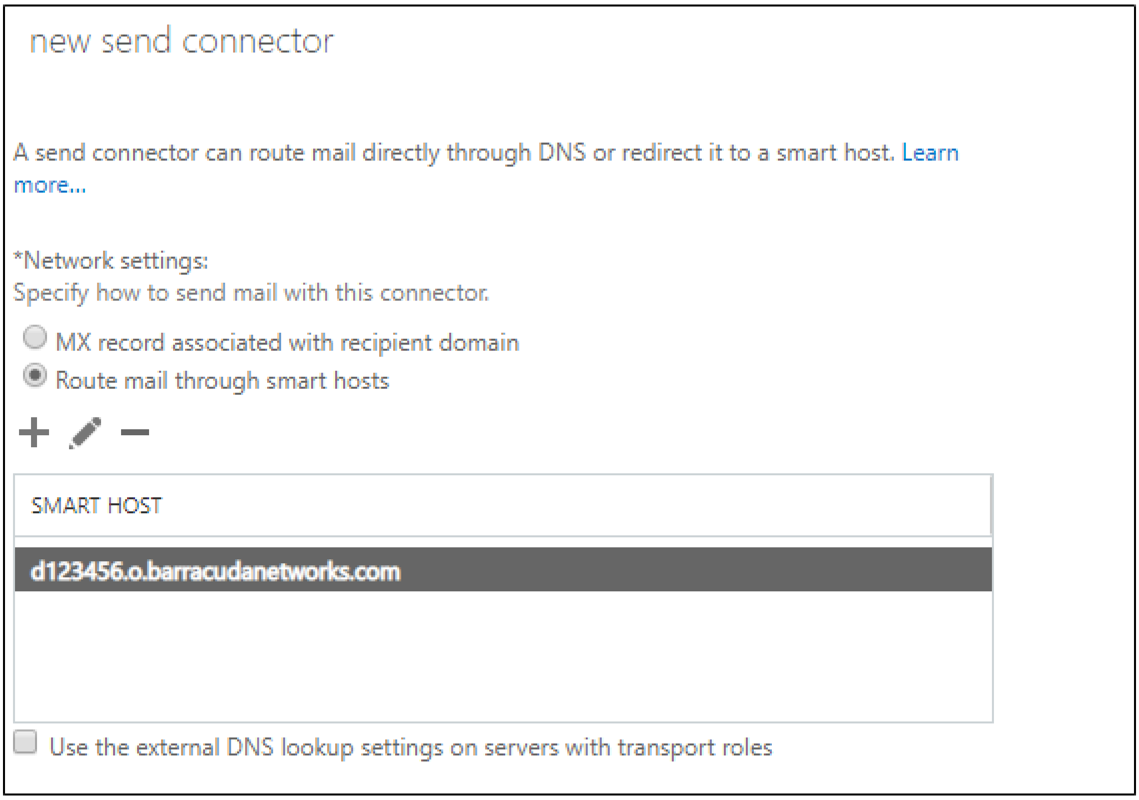
○ Internal (For example, to send intranet mail)

○ Internet (For example, to send internet mail)

○ Partner (For example, to route mail to trusted third-party servers)

4. Click **Next**.
   1. Select **Route mail through smart hosts**.
   2. Click the Plus icon.

3. Enter the Outbound Smart Host for the domain that is to relay outbound mail. This is the Outbound Hostname you noted earlier from the Domain Manager in Email Gateway Defense.



new send connector

A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...

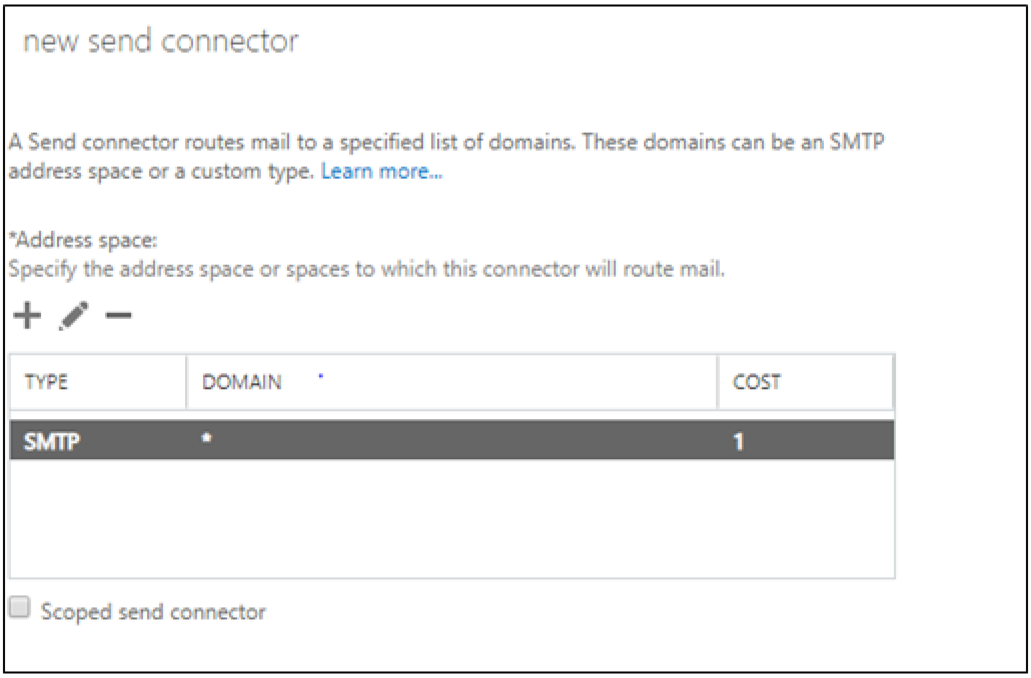
*Network settings:
Specify how to send mail with this connector.

○ MX record associated with recipient domain
● Route mail through smart hosts

SMART HOST
d123456.o.barracudanetworks.com

□ Use the external DNS lookup settings on servers with transport roles

5. Click **Next**. Ensure that the Authentication is set to **None**. Click **Next** again.
6. Click the Plus icon and type an asterisk for the FQDN. Click **Save**, then click **Next**.



new send connector

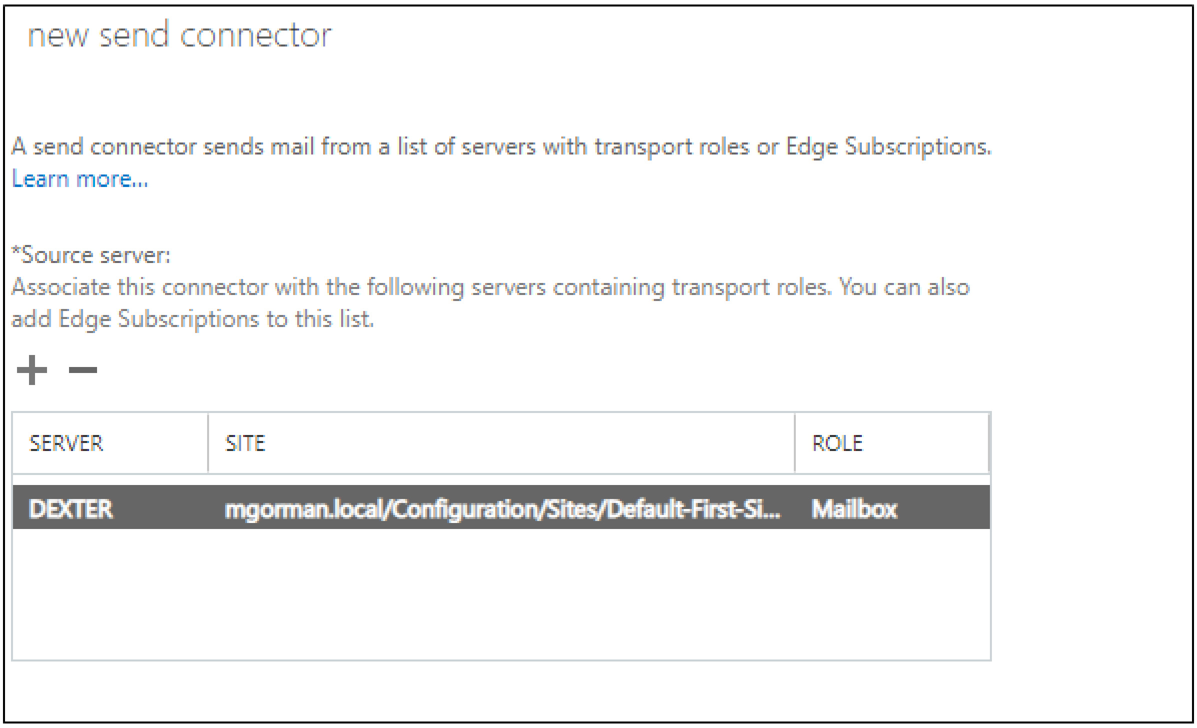
A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. Learn more...

*Address space:
Specify the address space or spaces to which this connector will route mail.

TYPE	DOMAIN	COST
SMTP	*	1

□ Scoped send connector

7. Click the Plus icon and add your source servers. These are any servers that will be sending email.



new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions.
Learn more...

*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

SERVER	SITE	ROLE
DEXTER	mgorman.local/Configuration/Sites/Default-First-Si...	Mailbox

8. Click **Finish**.

Step 7. Verify Mail is Flowing

1. Log into Email Gateway Defense.
2. In the **Dashboard** page, verify inbound and outbound messages are being logged for the selected domain.

   You can also click **Message Log** to view inbound and outbound email traffic. Use the filters to refine your search.

Step 8. Enable Advanced Threat Protection

Files blocked by ATP display on the **Dashboard**.

1. Go to **ATP Settings**, and select the desired option:
   - **Deliver First, then Scan** – Attachments are delivered with the message to the recipient and then scanned by the ATP service; if a virus is detected, an email notification is sent to the email recipient. Additionally, if **Notify Admin** is set to **Yes**, and a virus is detected in the scanned attachment, an email is sent to the administrator.
   - **Scan First, then Deliver** – Attachments are scanned by the ATP service before delivery. If a virus is detected in the attachment the message is blocked, otherwise it is delivered to the recipient.
2. Select whether to **Notify Admin** if a virus is detected in a scanned attachment. When set

to **Yes**, enter the **ATP Notification Email** address in the associated field.

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning in the **ATP Exemptions** section on the **ATP Settings** page.

Figures