Step 2 - Deploy Security Edition for Exchange 2013 and Newer

https://campus.barracuda.com/doc/74550040/

Use this article to deploy the Barracuda Email Security Service and Advanced Threat Protection (ATP) for Exchange 2013 and Newer in your environment.

Evaluate Barracuda Email Security for Exchange 2013 and Newer for 14 days, after which you can purchase and link the services to your account.

> **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 Email Security Service instance; see Barracuda Email Security Service IP Ranges for a list of ranges based on your Barracuda Email Security Service 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 the Barracuda Email Security Service IP address ranges based on your Barracuda Email Security Service instance

Step 2. Launch the Barracuda Email Security Service Setup Wizard

Alternatively, you can manually set up the Barracuda Email Security Service using the web interface.

Configure Domain

1. Log into Barracuda Email Security Service, 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 Barracuda Email Security Service, and click **Enter Linking Code and Serial Number** to activate your subscription:

Activate Subscription	Enter Linking Code and Serial Number

2. Enter the **Serial Number** and **Linking Code**, and click **Activate Subscription**.
3. In the setup page, click **Set up** to the right of **Email Security**:

Email Security	Set up ›

4. In the setup wizard, click **Get Started**. The **Specify Primary Email Domain** page displays.
5. Enter the primary Exchange domain you want to filter, for example: `cudaware.com`

6. 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 Barracuda Email Security Service Setup wizard has already identified your mail server IP based on the MX record, the **Mail Servers** field pre-populates.

7. Click **Add**. Enter an email address to test the server configuration, and click **Test All Mail Servers**.
8. 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.
9. Click **Next**. The **Configure Settings** page displays. Select from the following options:
   1. **Virus Protection** – Set to **On** to direct the Barracuda Email Security Service to detect and block viruses on inbound email.

2. **Spam Protection** – Set to **On** to direct the Barracuda Email Security Service 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 the Barracuda Email Security Service 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).

10. Click **Next**. The **Route Email Through Barracuda** page displays.

11. To verify your domain, replace your current MX records with the Barracuda Email Security Service Primary and Backup MX records displayed on the page:

Edit Zone Record

CUDAWARE.COM

Record type:
MX (Mail Exchanger)

View current

Host: * ⓘ

@

Points to: * ⓘ

d91262a.ess.barracudanetworks.com

Priority: * ⓘ

10

TTL: * ⓘ

1 Hour ▼

Finish   Cancel

Barracuda Essentials

Barracuda.
Your journey, secured.

Barracuda Email Security Service Setup ✕

- ✔ Specify Primary Email Domain
- ✔ Specify Email Servers
- ✔ Configure Settings
- ✔ Configure Outbound Settings for Office365
- **5** Route Email Through Barracuda

Route Email Through Barracuda (Click here for more details)

MX Records

To Verify your domain and begin using the Barracuda Email Security Service, please change your MX records to the following:
Primary: d91262a.ess.barracudanetworks.com
Backup: d91262b.ess.barracudanetworks.com

[Verify MX Records]

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

[Previous] [Skip] [Next]

Barracuda Email Security Service Setup ✕

- ✔ Specify Primary Email Domain
- ✔ Specify Email Servers
- ✔ Configure Settings
- ✔ Configure Outbound Settings for Office365
- **5** Route Email Through Barracuda

Route Email Through Barracuda (Click here for more details)

MX Records

To Verify your domain and begin using the Barracuda Email Security Service, please change your MX records to the following:
Primary: d91262a.ess.barracudanetworks.com
Backup: d91262b.ess.barracudanetworks.com

[Verify MX Records]

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

[Previous] [Skip] [Next]

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**. The Barracuda Email Security Service 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:
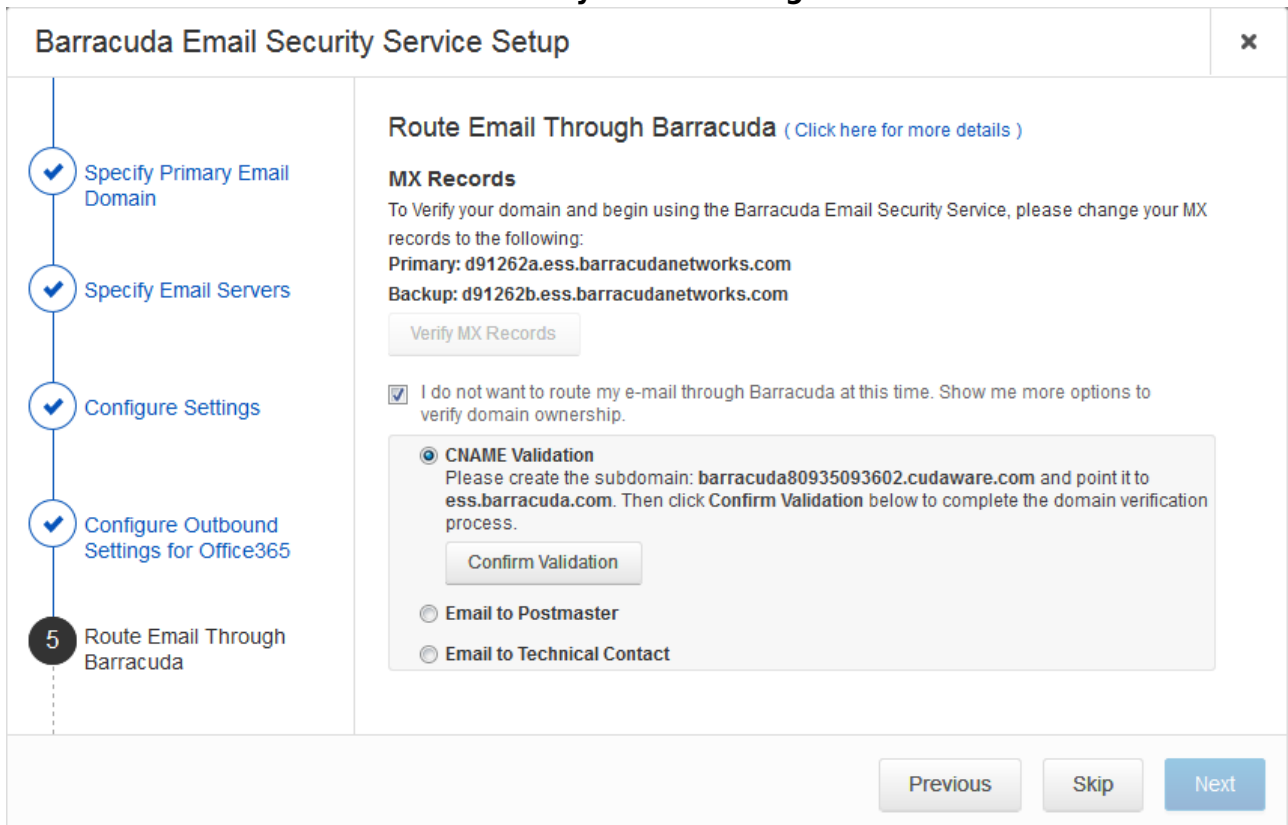>
> http://mxtoolbox.com/
>
> https://toolbox.googleapps.com/apps/dig/ (select the MX option)
>
> If your domain's MX records do not display in the Barracuda Email Security Service MX records, you must wait until they display before your domain can be verified.
>
> Note that after verifying your domain, any mail sent to your domain from another Barracuda ESS customer will be processed normally by your ESS account and not delivered via MX records.

12. 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**:

13. 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 the Barracuda Email Security Service 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 the Barracuda Email Security Service 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.

14. Click **Next**, and click **Next** again.
15. On the **Select Data Center Region** page, select the data center for your locale, and click **Get Started**.
16. Complete the wizard pages.
17. The **Confirmation** page displays. Confirm domain ownership, and then click **Done**.
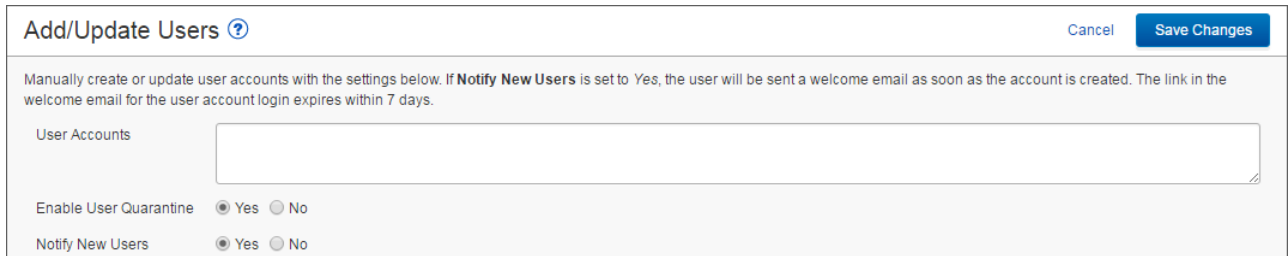
Step 3. Set Up User Accounts

You can add users manually, or use your organization's LDAP server or Azure AD service to automatically synchronize the Barracuda Email Security Service 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 the Barracuda Email Security Service 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**:

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 the Barracuda Email Security Service 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 the Barracuda Email Security Service 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 Azure AD service. For complete setup details, see the following articles:

- How to Configure User Authentication with Azure AD
- How to Configure User Authentication Using LDAP

Step 4. Configure Outbound Mail Scanning

1. Log into the Barracuda Email Security Service, 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 each mail server must contain a reverse DNS PTR record.
3. Add all IP addresses from which outgoing mail is allowed to flow through the Barracuda Email Security Service. The **Logging Domain** is the domain name that appears in the **Message Log** as the sending domain for the associated IP address.

Step 5. Configure Sender Policy Framework for Outbound Mail

To assure Barracuda Networks is the authorized sending mail service of outbound mail from your Barracuda Email Security Service, 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 Email Security Service:

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
```

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 Email Security Service 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 Email Security Service 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 Barracuda Email Security Service. Be sure to add all of your accepted domains into Barracuda Email Security Service before configuring outgoing email in this section.

Before you begin, log into the Barracuda Email Security Service, 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

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 Barracuda Email Security Service.

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 the Barracuda Email Security Service.

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

1. ClickLinkingCode.png
2. BESS_Setup.png
3. PrimaryDomain.png
4. verified_icon.png
5. MxRecord.png
6. VerifyMX.png
7. VerifyMX.png
8. RouteEmail.png
9. AddUpdateUser.png
10. newSendConnectorA.png
11. smartHost.png
12. SMTPasterisk.png
13. NewSendConnectorB.png