BARRACUDA ESSENTALS FOR EXCHANGE SERVER 2010/2007

Services Configuration

Abstract
The following is the walkthrough procedure for configuring Barracuda Essentials & its underlying services to protect your Exchange environment

Intronis
MSP Solutions by Barracuda

Table of Contents

Understanding the Barracuda Cloud Control (BCC) as an MSP 1
Overview 1
Email Security Service 2
Overview 2
Pre-requisites 2
Ensure Connectivity and Redundancy 2
Inbound Scanning Setup 2
Add a Domain to Barracuda Cloud Control 2
Best Practice Recommendations 6
Configure Advanced Threat Protection 6
Enable Email Continuity 7
Enable Inbound Quarantine 8
Add a receive connector in the Exchange Management Console 8
Define an Accepted Domain within Exchange 10
Outbound Scanning (Optional) 11
Outbound Sender IP Address 11
Send Connector 11
Update SPF record in DNS 13
Encryption (Optional) 13
Overview 13
Final Deployment Steps 14
Barracuda Cloud Archiving Service 15
Overview 15
Pre-requisites 15
Add archiving domain to BCC 15
Configuring Journal Archiving for Exchange 2010/2007 16
Add a Remote Domain 16
Create Mail Contact 18
Create Send Connector 22
Create Journaling Rule 25

Configure Exchange Integration 26
Create an Email Service Account for Exchange Server 2007/2010 27
Historical Import of Exchange Server Database 28
Exchange Non-Email Sync 32
Exchange Folder Structure Sync 33
PST Import 34
Appendix 1 – How to exempt or disable SPF checking for the Barracuda ESS service 36
Appendix 2 – How to Disable Throttling in MS Exchange Server 2007 37
Appendix 3 – How to Disable Throttling in MS Exchange Server 2010 38
Create and Assign Throttling Policy 38

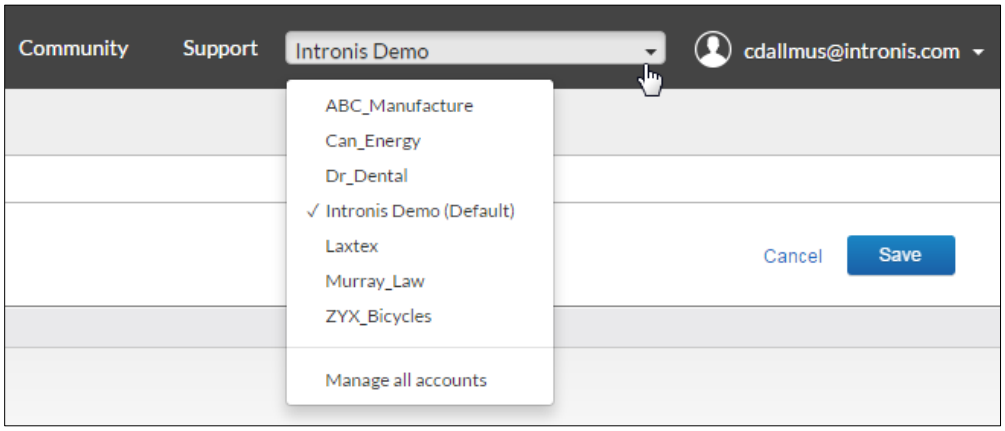
Understanding the Barracuda Cloud Control (BCC) as an MSP

Overview

As a partner, we want to provide you with as much clarity as possible to make your job easier. One of the more attractive features of the Barracuda Cloud Control interface is its central management design; all of your customer's Essentials Services can be managed from one login! Below is a brief explanation of the layout and navigation tips for your MSP account.

Whenever you log into your BCC account, your default page will bring you to your MSP "parent" account. Think of this as the root that contains all of your underlying "child" customer accounts. The only configuration you will apply to this account is adding in admin users and managing their permissions to products and customer accounts.

1. In the top right hand corner of the BCC (https://login.barracudanetworks.com) portal is your customer account switcher.



In this example, your MSP "parent account" would be "Intronis Demo (Default)". As you move forward with this configuration walkthrough, ensure that you select the appropriate customer account from the account dropdown.

Email Security Service

Overview

Barracuda Essentials Email Security is a, scalable, cloud based email security solution that comprehensively protects organizations against advanced email based attacks, data loss and minimizes business disruptions. Essentials Email Security protects against spam, viruses and known malware, and also provides granular policy management and monitoring controls for customized rules. In this section, we will walk through the setup for Inbound & Outbound Scanning as well Encryption

Pre-requisites

You will need access to the following items in order to configure Barracuda Email Security Service (BESS). This process does not automatically go live after configuration, you will set it up so that you can cut over to our service when you and your customer are ready.

- **Access & Credentials to** https://login.barracuda.com **(Barracuda Cloud Control or BCC)** – The username is contained in the provisioning activation email sent from Barracuda/Intronis. Otherwise, you can manually reset your password directly in the BCC portal using the 'forgot password' link.
- **Customer's domain and Exchange [2010/2007] Server hostname and external IP address**
    - [These are included in the pre-deployment guide]
- **Access & Credentials to customer's DNS Management Console –**You will need the customer's credentials to access your customer's domain settings. [Keep in mind that some DNS providers take significantly longer to propagate changes to records than others, up to 24 hours].
- **Access & Credentials to Exchange Management Console [2010/2007] –** You will need the customer's credentials to access their Exchange Admin Center.

Ensure Connectivity and Redundancy

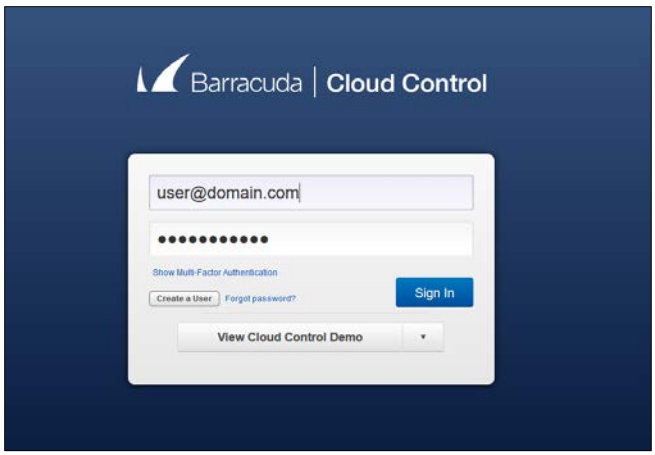
1. Open your firewall ports to allow the IP address ranges 64.235.144.0/20 [/20=255.255.240.0] & 209.222.80.0/21 [/21=255.255.248.0]
2. Where relevant, verify your network subnet is granted access in the ACL on your mail server (and LDAP server where applicable)
3. Block all port 25 traffic except for that originating from the Barracuda Email Security Service IP address ranges 64.235.144.0/20 [/20=255.255.240.0] & 209.222.80.0/21 [/21=255.255.248.0]

Inbound Scanning Setup

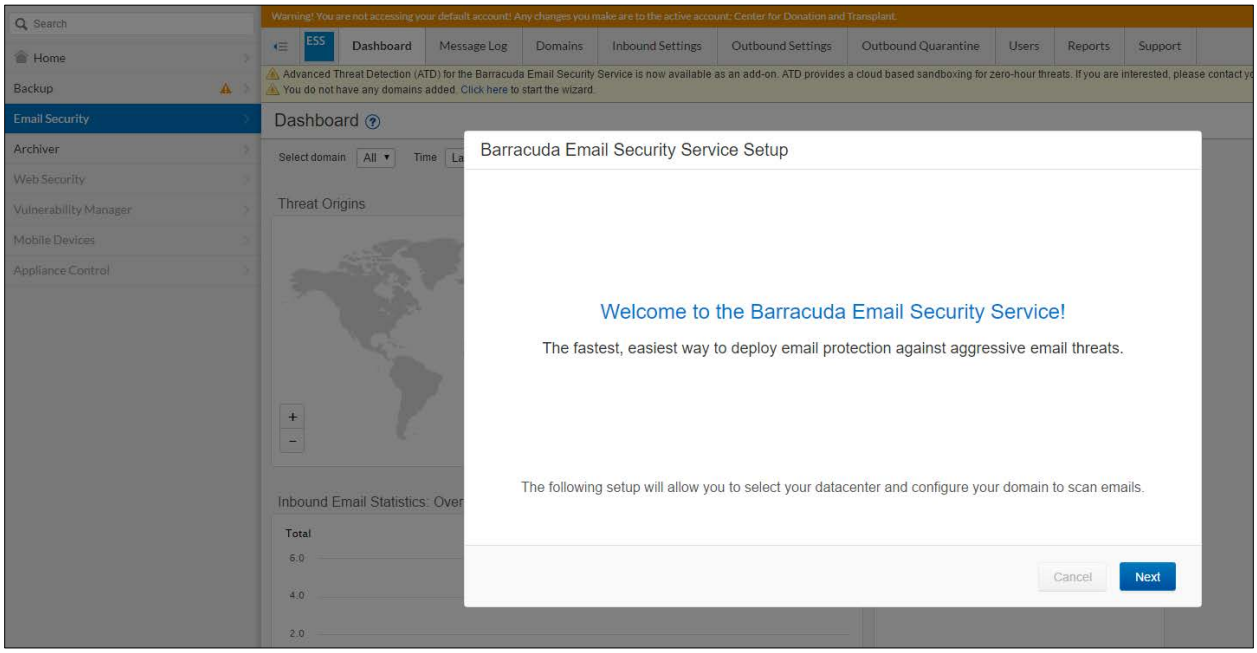
During this step we will configure the customer's domain for BESS. This will be done using the BESS wizard. You will want to have the domain & mail server IP information for this step.

Add a Domain to Barracuda Cloud Control

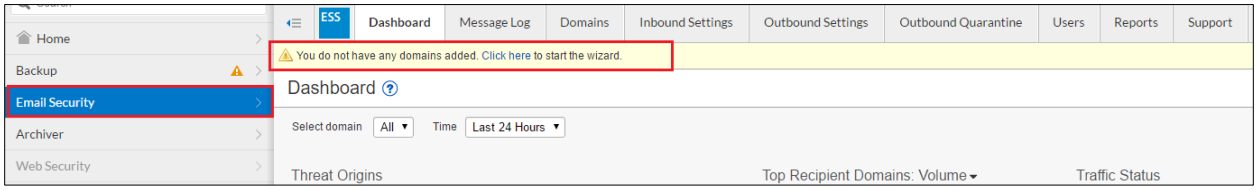
1. **Login** to the BCC (https://login.barracuda.com) console.



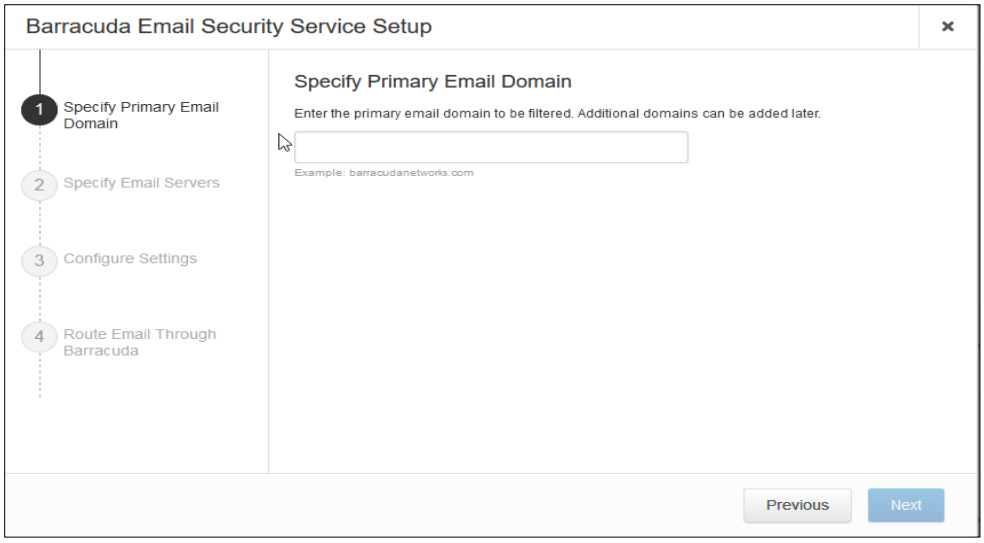
2. If this is your first time logging into a customer's Email Security service, you will be prompted with the wizard automatically:



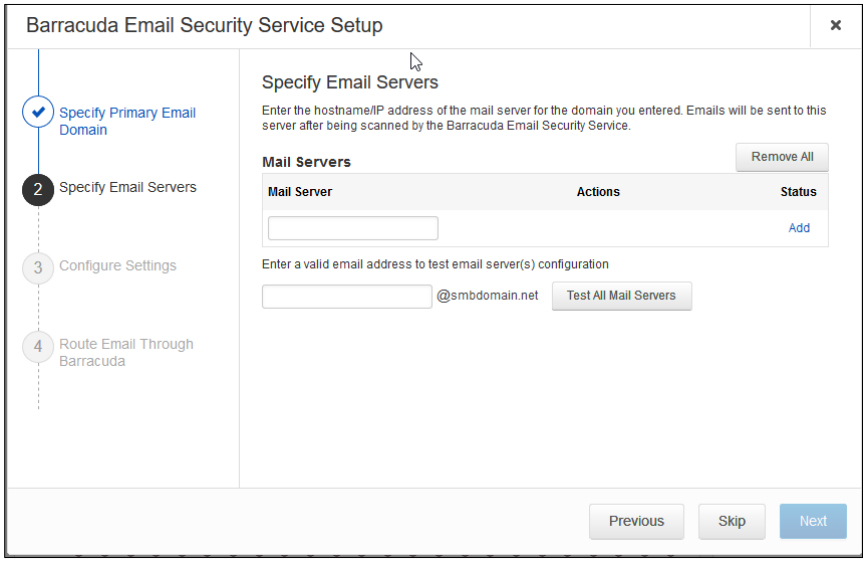
3. If you've already logged into their service before, but you have not yet started the configuration, **click here** to start the wizard:



4. **Select the region** where the mail will be scanned. If in the US/Canada, select *United States*. If in the UK, select *United Kingdom*.
5. **Enter** the customer primary **domain** in the space provided.



6. Enter the mail server in the space provided, this will be either the hostname or the public IP of the customer's Exchange 2013 server and click **add**.

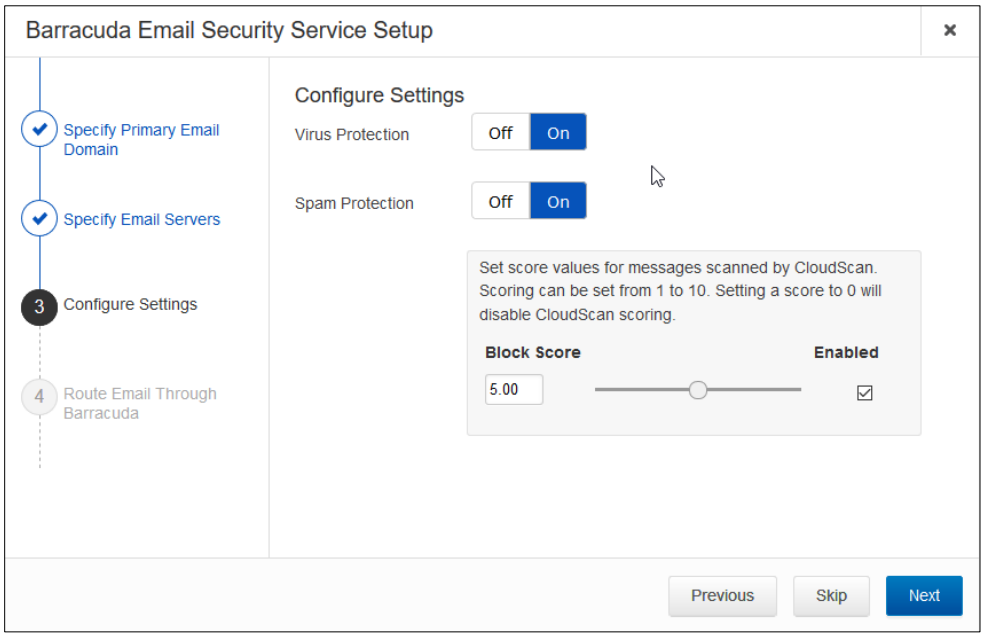


7. Click **Test All Mail Servers**.

   Please note: If you get an error at this step, please double check that the new firewall rules were implemented properly.

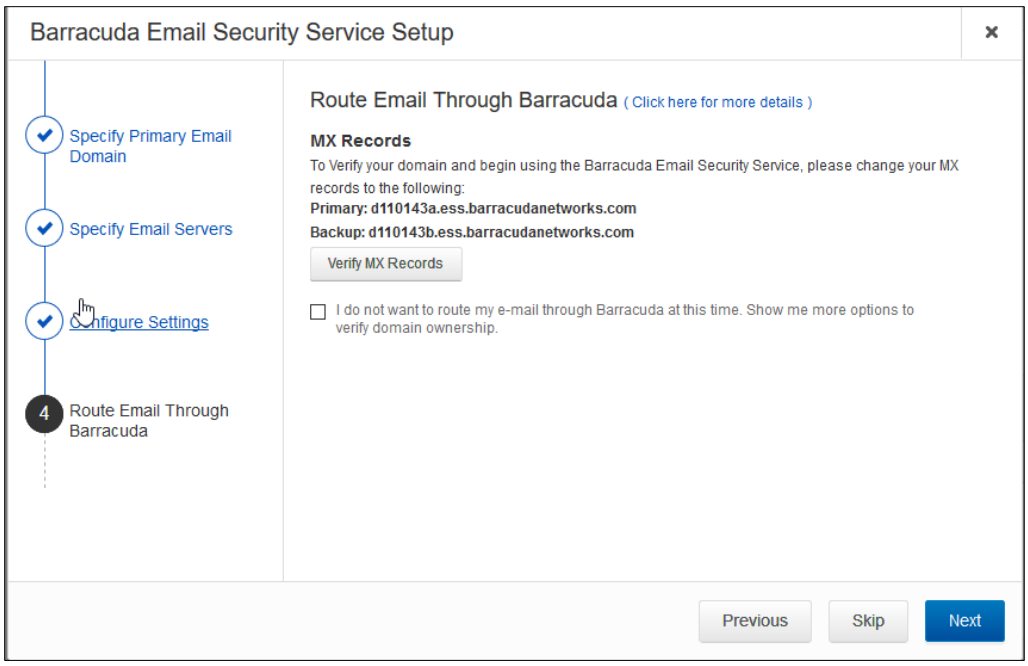
8. Click **Next** to continue with the defaults.

   By default Virus & Spam Protection are enabled and the CloudScan Spam Scoring system's block threshold is set to 5. This can be modified later in the **Inbound Settings > Anti-Spam/Antivirus** settings. Leaving Virus Protection enabled directs the BESS to detect and block viruses on inbound mail. Leaving Spam Protection enabled directs the BESS to evaluate inbound mail for spam based on a score assigned to each processed message. CloudScan Spam Scoring grades each inbound message, Scoring ranges from 1 (definitely not spam) to 10 (definitely spam). For more details, please read this Barracuda Campus KB article.



9. **Update** customer **MX records** with records provided

   Add the 2 MX records generated below. Ensure you check with your DNS provider on the appropriate syntax. If you are not currently ready to cut over to the BESS service and plan to at a later date, **use a priority of 99**. Otherwise ensure the priority is 10(a) / 20(b) and no other records exist with a higher priority. This will allow us to validate the domain ownership and provides authorization to route mail.



10. Click **Next** to finalize the domain creation.

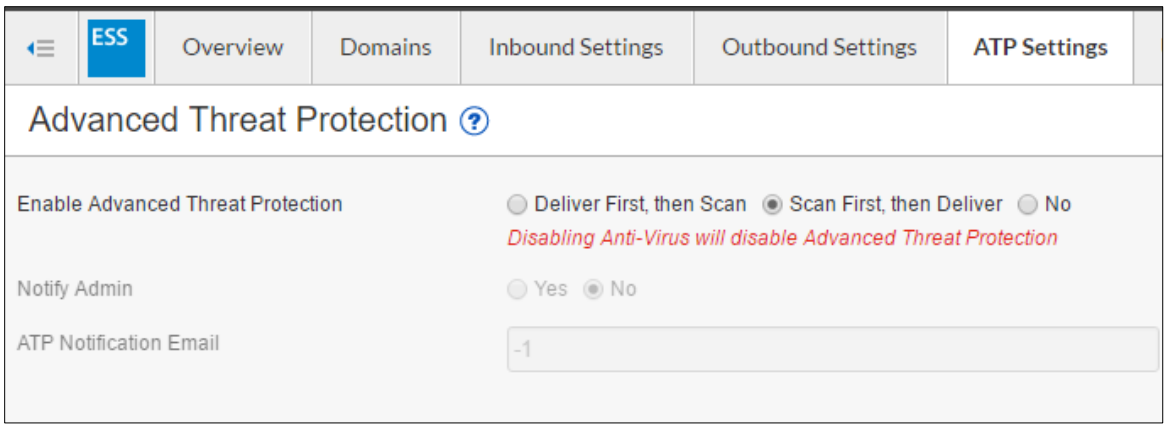
Best Practice Recommendations

The following sections are not required, but, if configured, will add more layers to your security & business continuity measures to further protect your client's environment.

Configure Advanced Threat Protection

We recommend that you configure your ATP to scan first then deliver in order to defend your client's network against advanced cyber threats. This service analyzes inbound email attachments with most MIME types in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Service virus scanning features.

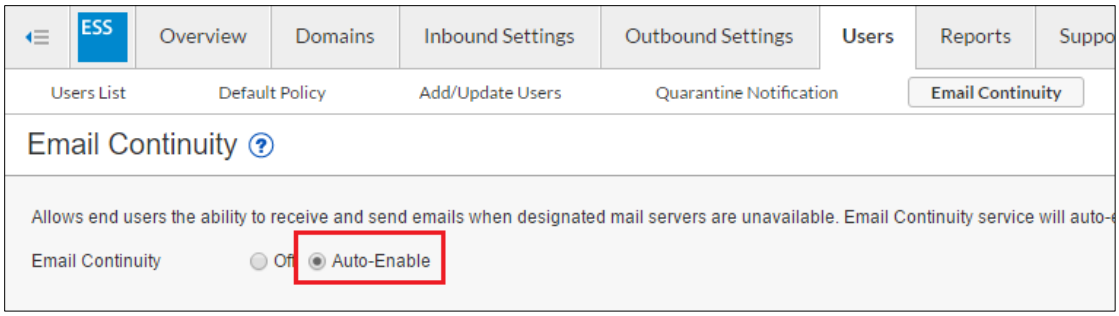
1. Log in to BCC and go to the **Email Security Service.**
2. Navigate to the top menu bar for the **ATP Settings** tab.
3. Set ATP to Scan first, then Deliver.

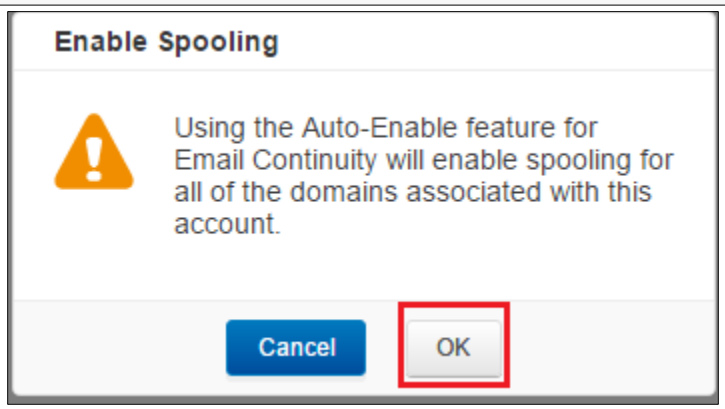


Enable Email Continuity

With this feature enabled, your end users will be able to continue business communications even in the event that their mail server goes offline. Our Email Continuity service for Business Continuity works by keeping a "heartbeat" with your client's mail server & if it goes offline, we will automatically failover mail server responsibilities for up to 96 hours.

1. Log in to BCC and go to the **Email Security Service**.
2. Navigate to the **Users** tab across the top menu bar, then click **Email Continuity**.
3. Click the radio button for **Auto-Enable**, then click **OK** to enable spooling.



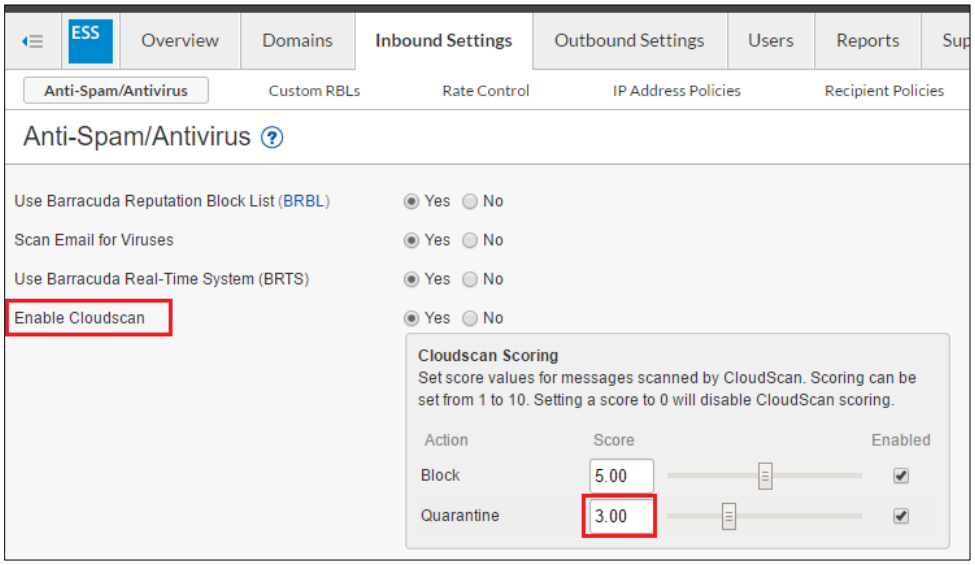


Enable Inbound Quarantine

In order to enable quarantine globally for all domains associated with the account, you must raise the CloudScan scoring value for quarantine to a value greater than 0. Enabling quarantine creates a buffer layer between email that is allowed into the environment and mail that is blocked.

1. Log in to BCC and go to the **Email Security Service**
2. Navigate to the **Inbound Settings > Anti-Spam/Antivirus**.
3. Under CloudScan Scoring > Quarantine: Set the Quarantine threshold to 3.

Please note: This is a good starting point as most malicious spam attacks are graded 3 or higher, but may need to be modified later if the policy is too strict or too lenient.

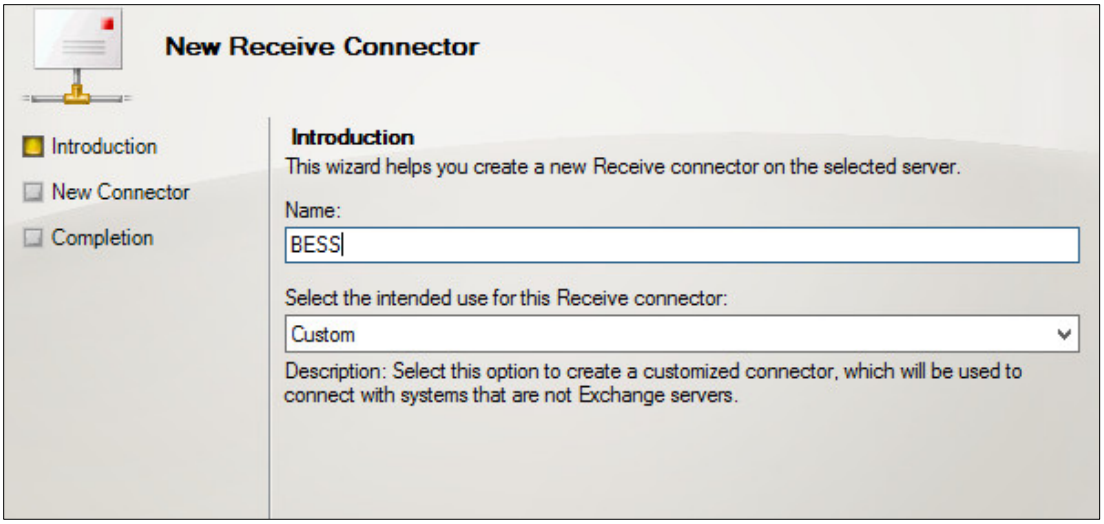


CONGRATULATIONS YOU ARE NOW CONFIGURED FOR COMPREHENSIVE PROTECTION AGAINST SPAM, VIRUSES & MALWARE, ADVANCED PHISHING ATTACKS AND SOPHISTICATED, ZERO-DAY THREATS LIKE RANSOMWARE & WANNACRY!

Add a receive connector in the Exchange Management Console

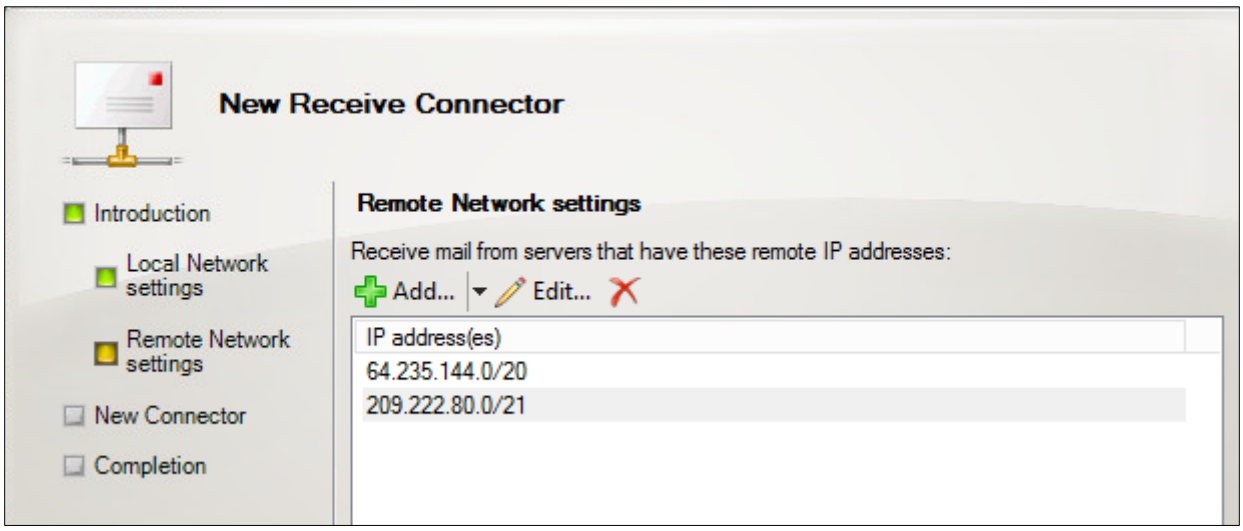
Since all inbound mail will now be scanned by the Barracuda ESS then relayed to your Exchange server, we want to secure your server by only allow incoming mail that is sourced from our service's IP address ranges.

1. In the EAC, navigate to **Server Configuration** > **Hub Transport**: Select the Exchange server under the Hub Transport section. Click **New Receive Connector** in the Action pane to the right to create a new receive connector.
2. On the **New receive connector** page, specify the name as "**BESS**" for the Receive connector and then select **Custom** from the intended use drop down.



Please note: Since you are receiving mail from the Barracuda ESS in this case, we recommend that you route mail to your front end server to simplify and consolidate your mail flow.

3. For the **Local Network Settings**, observe that **All available IPV4** is listed in the **IP addresses** list and the **Port** is 25. (Simple Mail Transfer Protocol uses port 25.) This indicates that the connector listens for connections on all IP addresses assigned to network adapters on the local server. Click **Next**.
4. In the **Remote network settings** page lists 0.0.0.0-255.255.255.255, which means that the Receive connector receives connections from all IP addresses. Delete the default entry, then click **Add** + and enter the primary Barracuda ESS IP range **64.235.144.0/20** [/20=255.255.240.0], then click Click **Add** +, & add the second Barracuda ESS IP range: **209.222.80.0/21** [/21=255.255.248.0] and click **Next**.

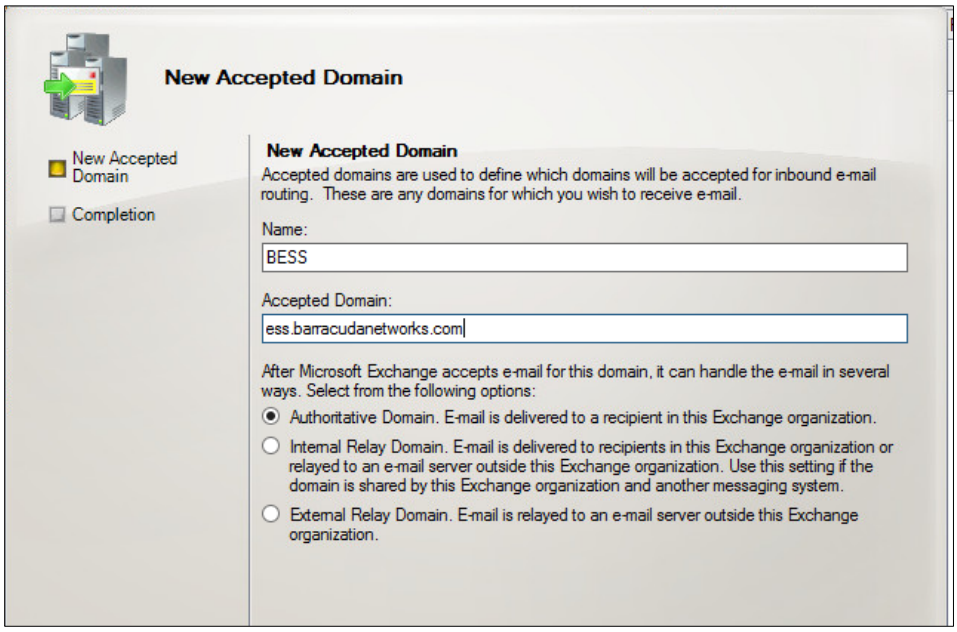


5. You will see the configuration summary page, verify the settings, then click **New**.
6. Click **Finish** to create the connector.

Define an Accepted Domain within Exchange

Now that we added a receive connector that corresponds to the IP address space of the Barracuda ESS, we will add another layer of security by defining an accepted domain that resolves to the IP address space defined in the previous step. If you are using Exchange 2010, please refer to Appendix 3.

1. In the EAC, navigate to **Organization Configuration** > **Hub Transport > Accepted Domains**. Right click and select **New Accepted Domain** to create a new Accepted Domain.
2. In the **Name** field, enter **BESS.**
3. In the **Accepted domain** field, enter **ess.barracudanetworks.com**
4. Select **Authoritative**
5. Click **Save.**



Outbound Scanning (Optional)

If you wish to scan outbound mail for spam and viruses, as well as scan outbound mail for material that should remain internal (for Data Loss Prevention [**DLP**]), follow the steps below to route outbound mail through our service.

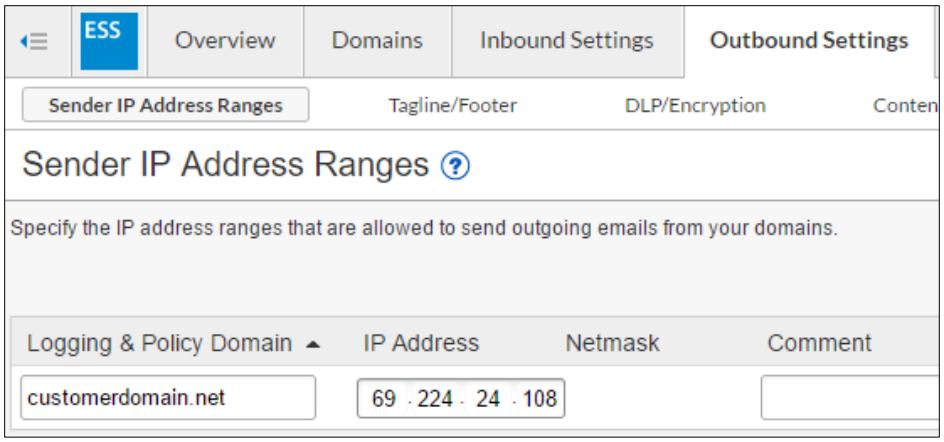
> **Please Note**: To configure Encryption, Outbound Scanning must also be configured.

Outbound Sender IP Address

To route outbound mail through the BESS, we will need to enter the public IP address on the network where your client's Exchange server resides.

1. In BCC, go to **Email Security** > **Outbound Settings** > **Sender IP Address Ranges.**
2. Enter the sending domain name & enter the public IP of the network that will be sourcing the mail traffic.

Please note: BCC can only accept a specific public IP one time, so if you are entering 2+ domains that share the same public IP, select the primary or longest tenured domain as the "Logging & Policy Domain"

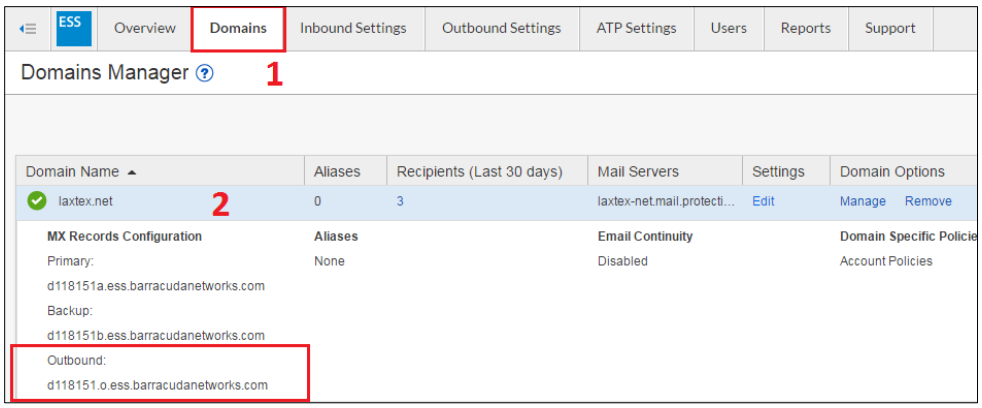


Send Connector

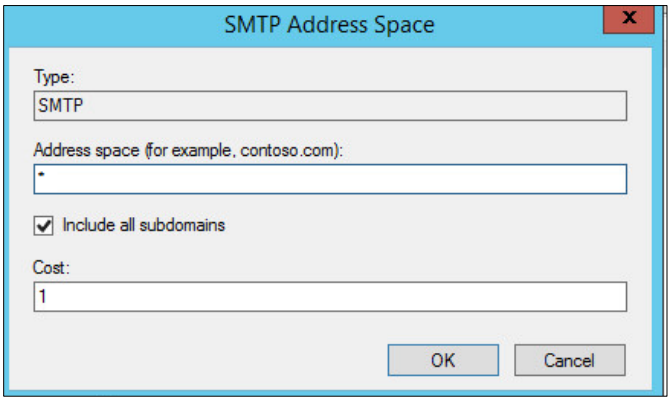
We will add an outbound send connector within Exchange Management Console to route outbound mail through a Barracuda smart host.

1. Ensure you have a copy of the **BESS outbound hostname** for your domain.

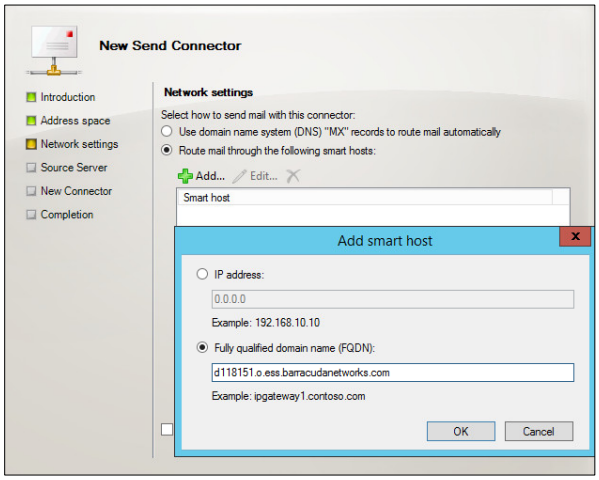
   If you have forgotten, login to **BCC** [select the appropriate customer from the account switcher] > **Email Security** go to **Domains (1) > Settings (2)** and copy the outbound hostname under the MX records configuration.



2. Within Exchange Management Console, go to **Organization Configuration > Hub Transport > Send Connectors**, then in the actions pane to the right, click **New Send Connector**.
3. Enter the name "**BESS Outbound**" & select **Custom** from the intended use drop down. Click **next**.
4. In the Address Space section, click **Add+,** leave the type as SMTP, enter an **asterisk *** for the address space (wildcard all destination domains), then click **OK**. Click **Next**.



5. In the Network Settings section, select **Route email through the following smart hosts**: then click **Add+.** Enter the FQDN copied from step 1 above into the FQDN Space. Click **Ok**, then Click **Next**.



6. In the Smart Host authentication settings, select **None**. Click **Next**.
7. In the Source Server page, select your Exchange server. Click **Next**.
8. Review the summary page, then click **New**. Then click **Finish**.

Please note: This send connector will go live upon completion- if you would like to wait until a change window or after business hours, please disable the connector in the action pane to the right.

Update SPF record in DNS

1. Login to the customer's **DNS management panel** then update their SPF record to include the Barracuda ESS FQDN: **include:spf.ess.barracudanetworks.com.** If they do not have an SPF record in place, please create a new TXT record against their domain: **"v=spf1 include:spf.ess.barracudanetworks.com –all"**

For more details about updating your customers SPF record please contact your DNS provider. If your DNS provider is unable to leverage host names please use the IP ranges 64.235.144.0/20 & 209.222.80.0/21.

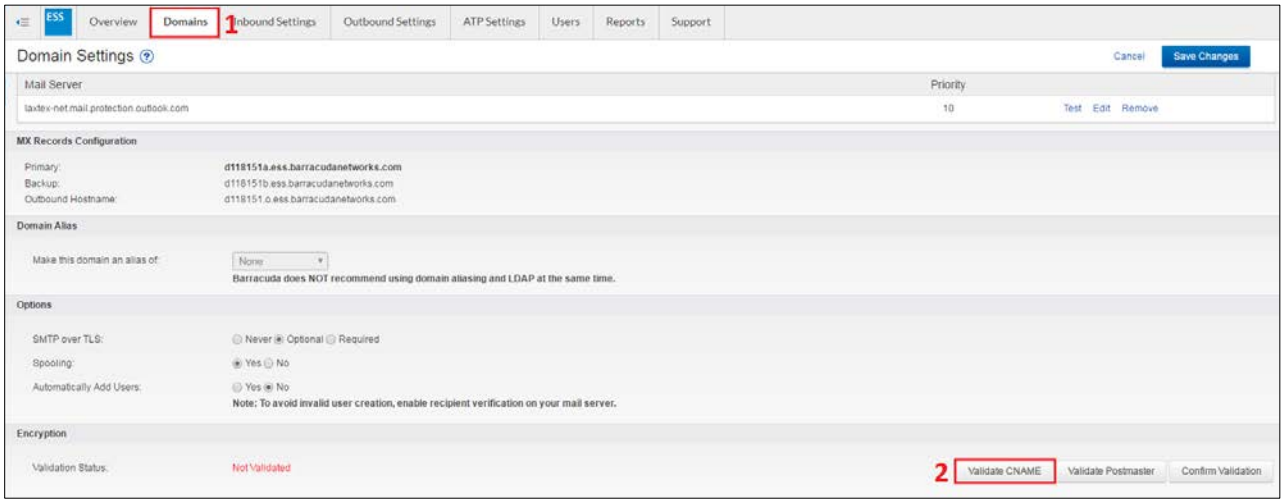
Encryption (Optional)

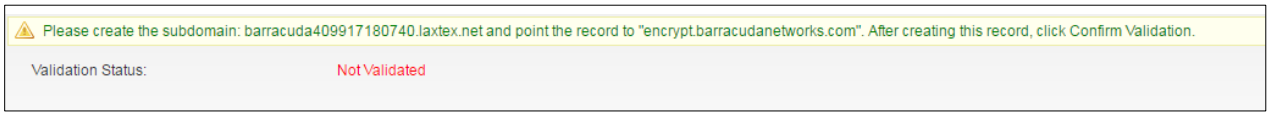
Overview

The BESS can perform encryption on outbound mail in order to secure transmission of sensitive mail. This encryption service is triggered by keyword content policies scanned on outbound messages, and the recipient is sent a link to the Barracuda Message Center where they can retrieve the decrypted message. For more information about how our encryption service works, please read the following Barracuda Campus KB article.

1. **Login to BCC** then navigate to **Email Security** > **Domains (1)** tab.
2. Click **Settings** next to the domain you want to enable encryption for.
3. Under the encryption sub-header, click **Validate CNAME (2)** to generate a new record.

Please note: each time you click the 'Validate CNAME' button, it will generate a new record. You will need to update your CNAME record to reflect the newly generated CNAME record.





4. Log in to your **DNS management portal** for this domain, and create a **CNAME record** using the prefix before the <**.customerdomain.com**> that was generated in the prior step next to Validation status. For example: barracuda30929916985
5. Point the CNAME record of that domain to **encrypt.barracudanetworks.com**

   Please Note: Allow the DNS propagation to take effect before proceeding – this can take up to 24 hours for some providers.

6. Within the Domain settings in BCC, next to encryption, click **Confirm Validation** to query DNS and resolve the CNAME. If DNS propagation takes longer than you would like, you can validate via Postmaster instead.
7. Once it's validated, a new subset of options will appear under the Encryption section for customer or MSP branding: logo image upload & custom text/HTML fields to make the encrypted message portal personalized for your customer's recipients.

Final Deployment Steps

Certain Steps shouldn't be completed until the customer is ready to go live with the Barracuda Email Security Service (BESS) solution.

1. **DNS** - Change MX records for the Barracuda ESS to priority of 10(a) & 20(b)
   a. Raise the priority of their existing MX records (to 99) until you verify mail flow through BESS. This can be done by going into the Message Log tab within the Barracuda Cloud Control portal

> Email Security > Overview – Then once confident cutting over to BESS, delete their old MX records altogether.

2. **Exchange Management Console**- Enable the Outbound Send Connector in EMC to allow outbound mail to flow through the BESS. Go to the **EMC > Organization Configuration > Hub Transport > Send Connectors**. Select the 'BESS Outbound' send connector and in the actions pane to the right click 'Enable'

Barracuda Cloud Archiving Service

Overview

In this section we will configure your customer's domain to archive all messages, adhering to compliance regulations and ensuring the facilitation of eDiscovery requests. Barracuda Cloud Archiving can be configured and put into production without interrupting the flow of mail or anything related to the company's email. The service works by journaling replicated, immutable copies of each inbound and outbound message sent by or received for a given domain. For more information about the Barracuda Cloud Archiving Service, please read the following Barracuda Campus KB article.

Pre-requisites

- **Access & Credentials to "login.barracudanetworks.com" (Barracuda Cloud Control or BCC)** – You should have this from the provisioning activation email. It's sent directly from Barracuda/Intronis. Otherwise, you can manually reset your password directly in the BCC portal using the 'forgot password' link.
- **Access & Credentials to Exchange Management Console**

Add archiving domain to BCC

1. Log in to Barracuda Cloud Control using your login credentials, click **Archiver** in the left pane, and click the **Archiver** tab.
2. Click **Run setup wizard**.
3. The **Welcome** page displays. Click **Get Started**.
4. If you wish to setup LDAP AD integration, please see Appendix 2. [At this time the Archiving AD integration is only compatible with on premise AD servers]. If not, click **skip,** then **yes skip** to continue without configuring LDAP.
5. The **Local Domains** page displays. Enter email domains and fully-qualified domain names (FQDNs) to be archived. Messages sent to any recipient in the listed domains are added to the archive. Enter a domain and click **Add**, or add multiple domains separated with commas, and then click **Add**. The added domains display in the **Domains** list.
6. Click **Next**.
7. The **Retention** page displays. Specify how long you want email archived to the Barracuda Cloud. [By default, email will be archived forever, with no storage limitations.]
8. Click **Next**. The **Apply Changes** page displays. Confirm your settings. Once you are satisfied, click **Apply Changes and Finish**.

The page will refresh, click **Mail Sources > SMTP Journaling** where a **journaling address** will be generated. Copy this address to clipboard, we will use this when we create a journaling rule within Exchange Management Console in the journal rule step.

Configuring Journal Archiving for Exchange 2010/2007

Once the Barracuda Cloud Archiving Service is configured to receive SMTP traffic, you must complete the following from the Exchange Management Console (EMC) of each Exchange Server that will be journaling directly into the Barracuda Cloud Archiving Service:

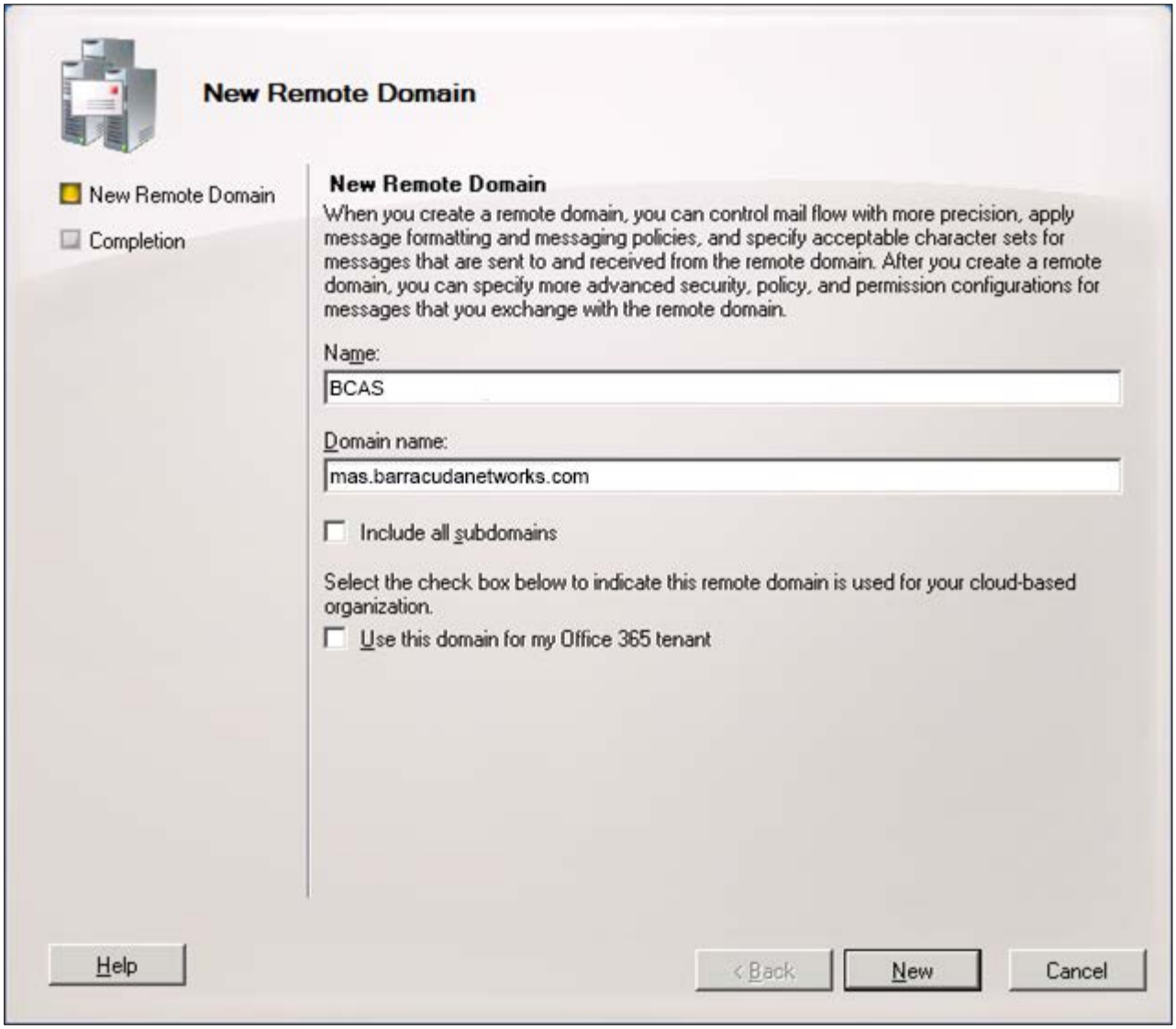
1. *From* Recipient Configuration **– Create a Mail Contact that is to act as the recipient of all journaled messages**.
2. *From* Organization Configuration > Hub Transport – **Create the following items**:
    a. **(non-routable)** Remote Domain**, to act as the recipient domain for journaled traffic**
    b. Send Connector, **for routing journaled messages**
    c. Journaling Rule **to actually enable journaling on your Exchange Server**

Add a Remote Domain

The Remote Domain must match the Mail Contact that is the recipient of journaled messages as it is used by the Exchange Server for routing all SMTP Journal traffic. Use the following steps to create a remote domain:

1. Open the **EMC** > **Organization Configuration** > **Hub Transport** > **Remote Domains** tab in the center pane.
2. In the **Actions** panel in the right pane, click **New Remote Domain.** The **New Remote Domain** dialog displays.
3. In the **Name** field, type BCAS, and in the **Domain name** field, type your region-specific MAS hostname, for example:

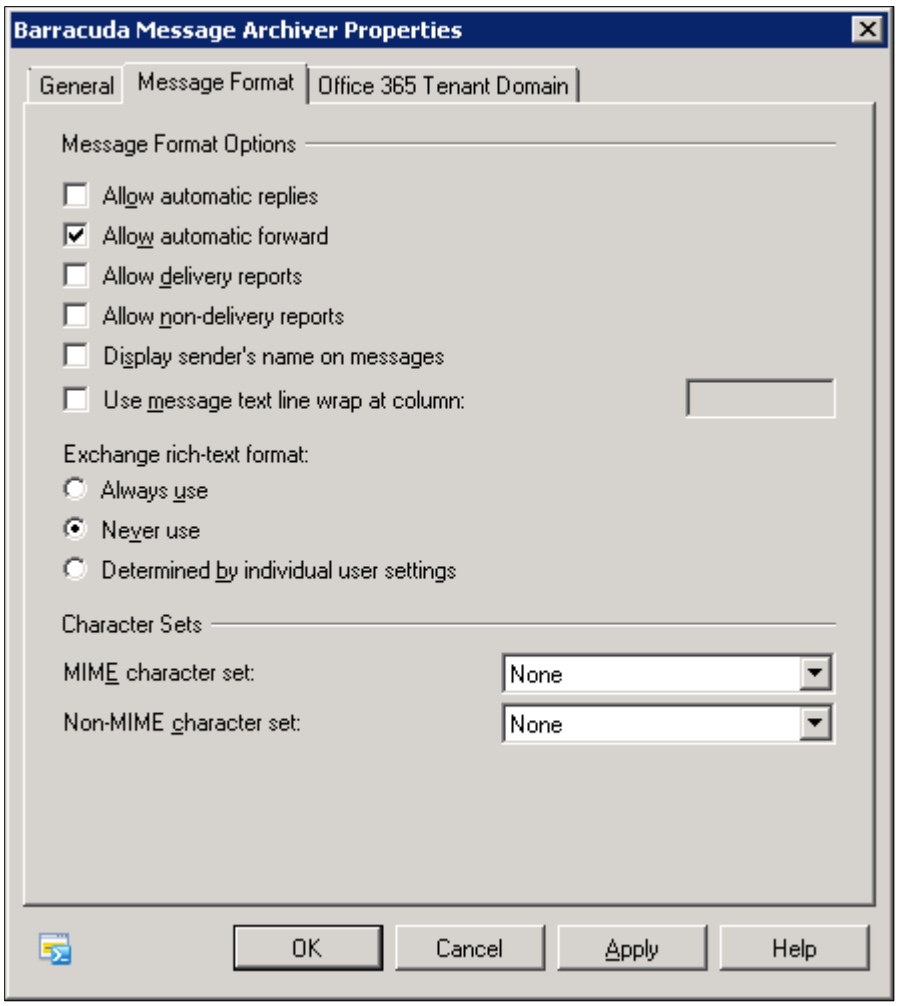
    mas.barracudanetworks.com (US)
    mas.ca.barracudanetworks.com (Canada)
    mas.uk.barracudanetworks.com (UK)



4. Click **New** to verify the domain settings, and click **Finish** to save your settings. The newly created domain displays in the **Remote Domains** list.
5. Double-click on the newly created domain to open the **Properties** dialog for the newly created domain, and:

6. In Exchange 2007, select **Format of original message sent as attachment to the journal report**.
7. In Exchange 2010, select the **Message Format** tab in the **Properties** dialog box.
8. Select the following options to ensure journal messages sent to this domain are *MIME Plain Text* format (rather than the unsupported *Exchange Rich Text* format):

9. In the **Message Format Options** section, turn on **Allow automatic forward**.
10. In the **Exchange rich-text format** section, select **Never Use**:

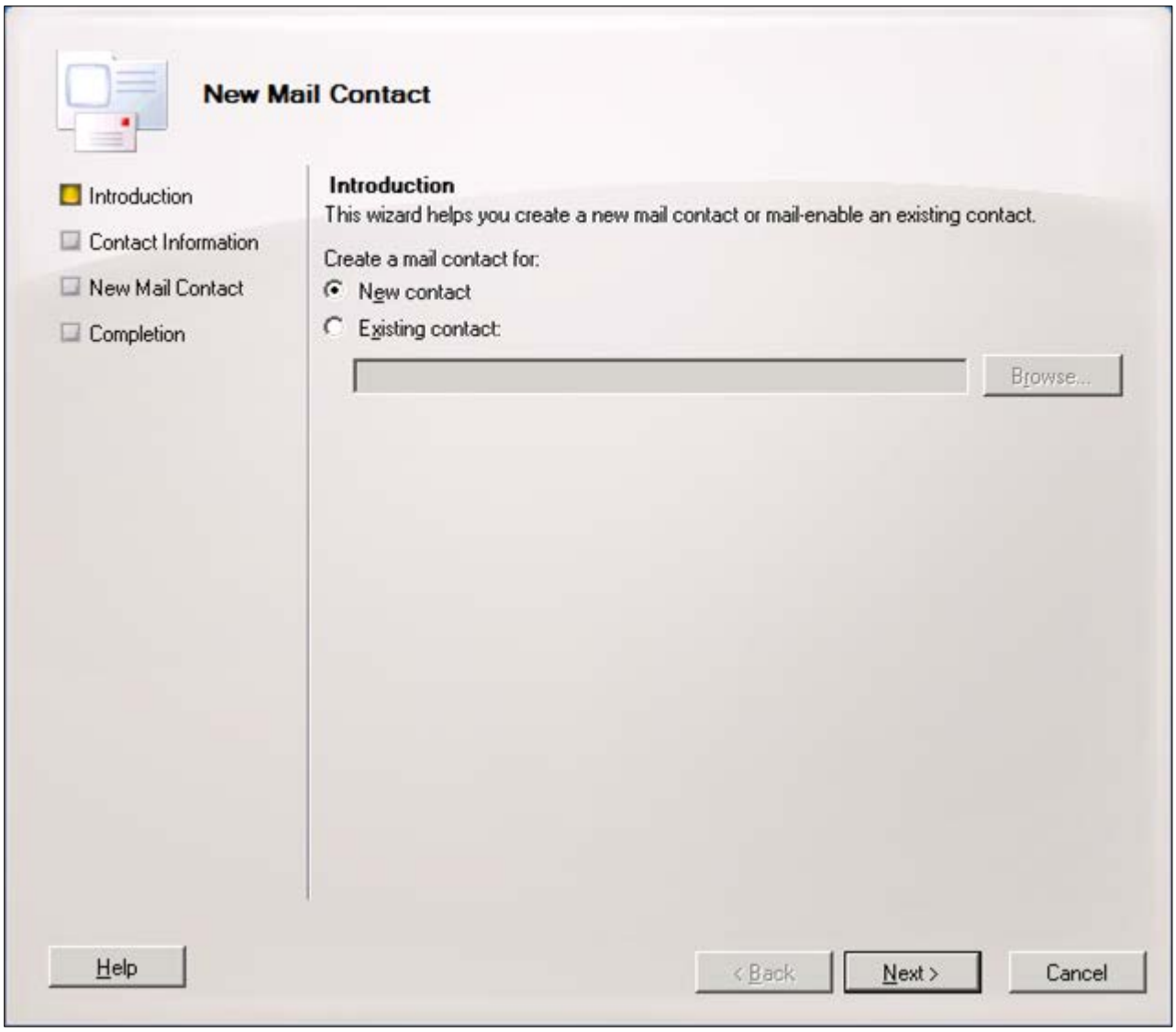


11. Verify that only **Never use** and **Allow automatic forward** are selected in the dialog box.
12. Click **Apply** to save your settings, and click **OK** to close the **Properties** dialog.

Create Mail Contact

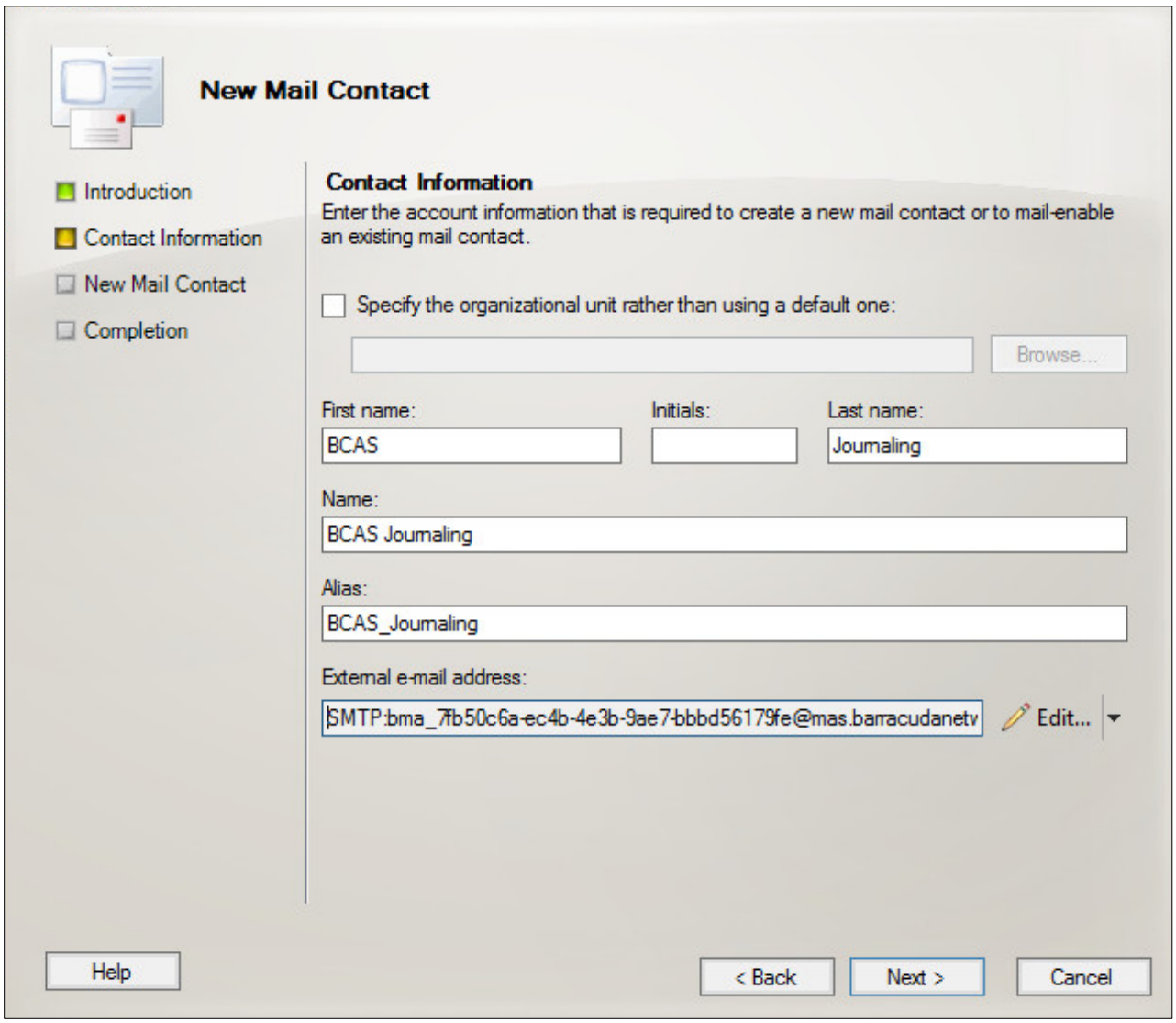
The Mail Contact is the account that is to act as a "holding location" for journaled messages. The email address associated with this account is the designated recipient. Use the following steps to create a Mail Contact:

1. In the **EMC**, expand **Recipient Configuration**, select **Mail Contact**, and in the **Actions** panel, click **New Mail Contact**:

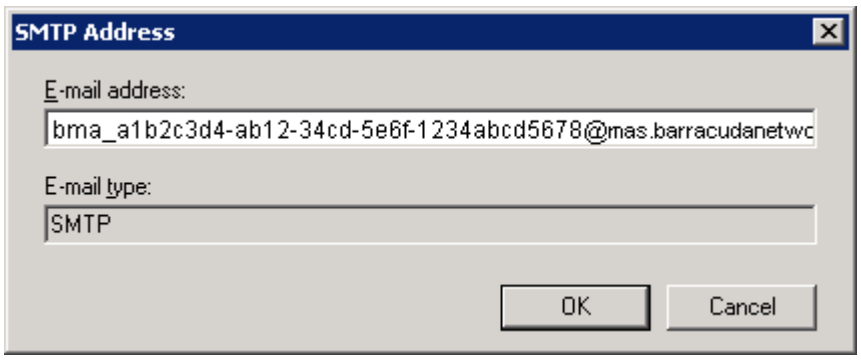


2. In the dialog, select **New Contact**, and click **Next**.

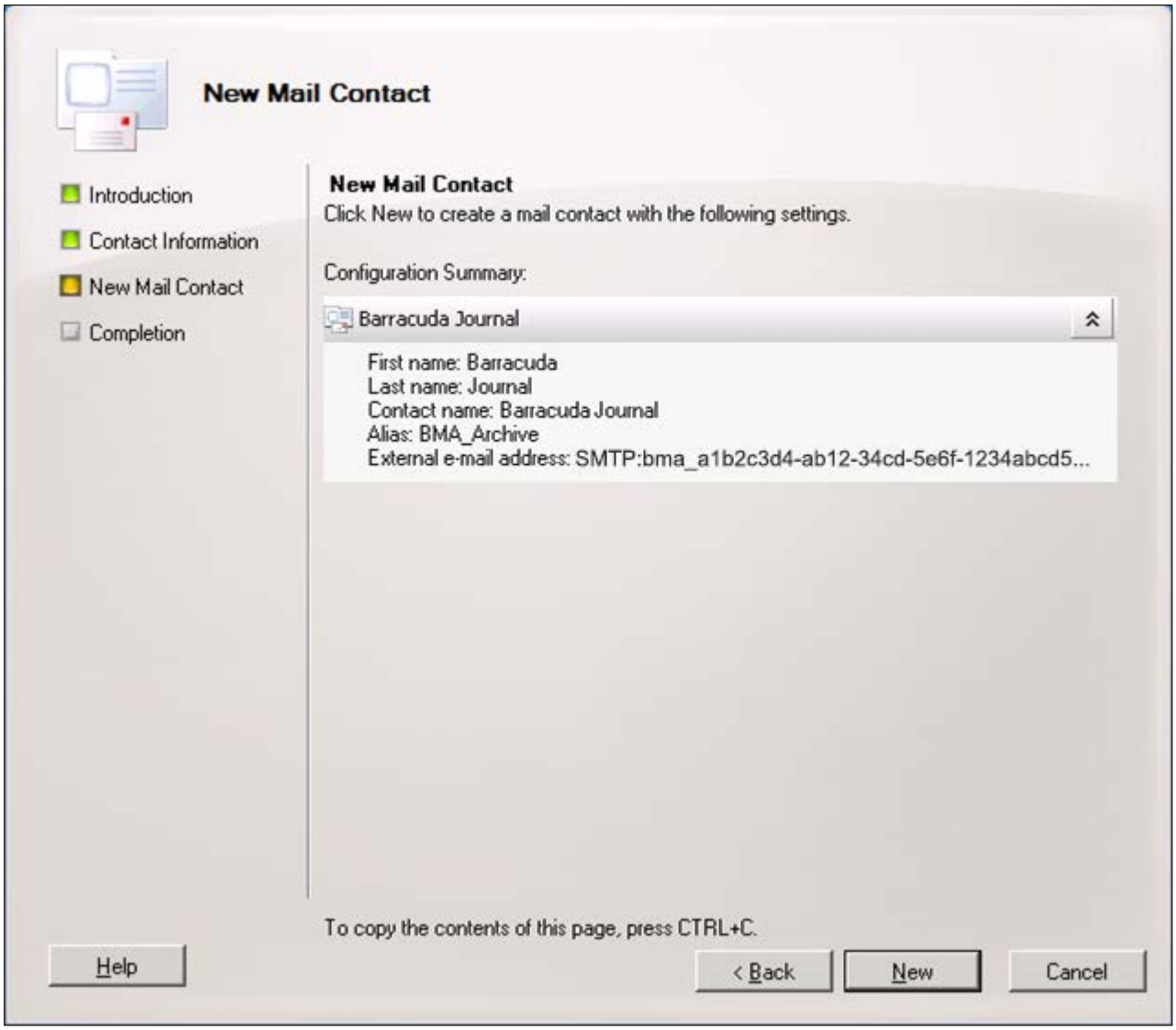
3. Enter a **First name** and **Last name**; the **Name** field automatically populates based on the entered values. Enter an **Alias**:



4. Click **Edit** to the right of the **External e-mail address** field, and in the **SMTP Address** dialog, enter the journaling address:



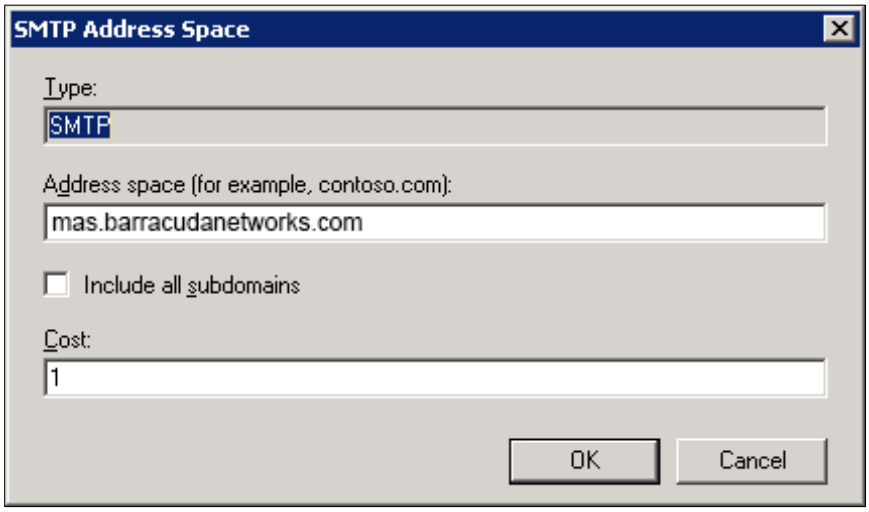
5. Click **OK** to close the dialog box. In the Wizard, click **Next** to verify the information:



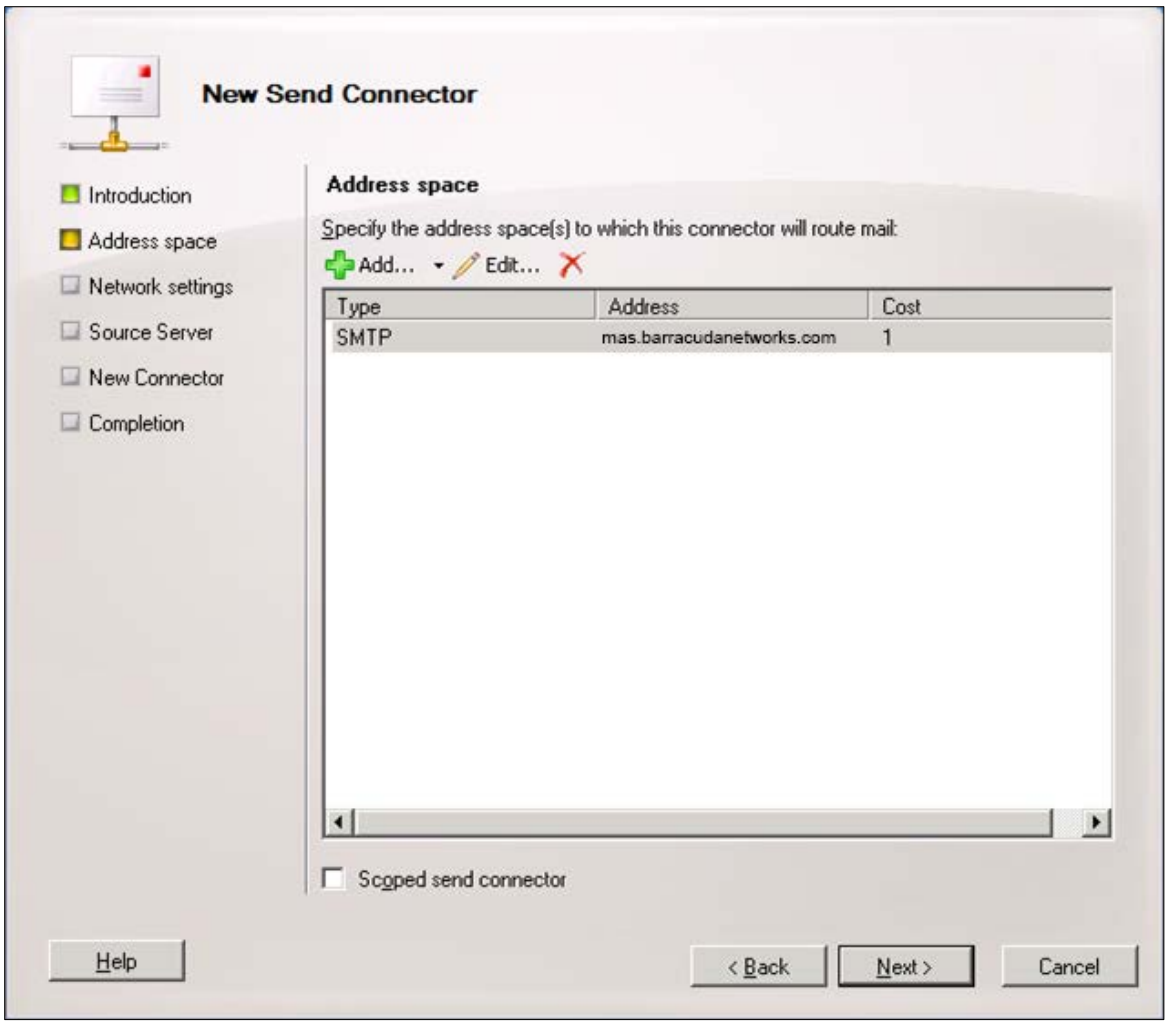
6. Click **New** to create the Mail Contact. The newly-created contact appears in the **Mail Contact** list. Click **Finish** to close the Wizard.

Create Send Connector

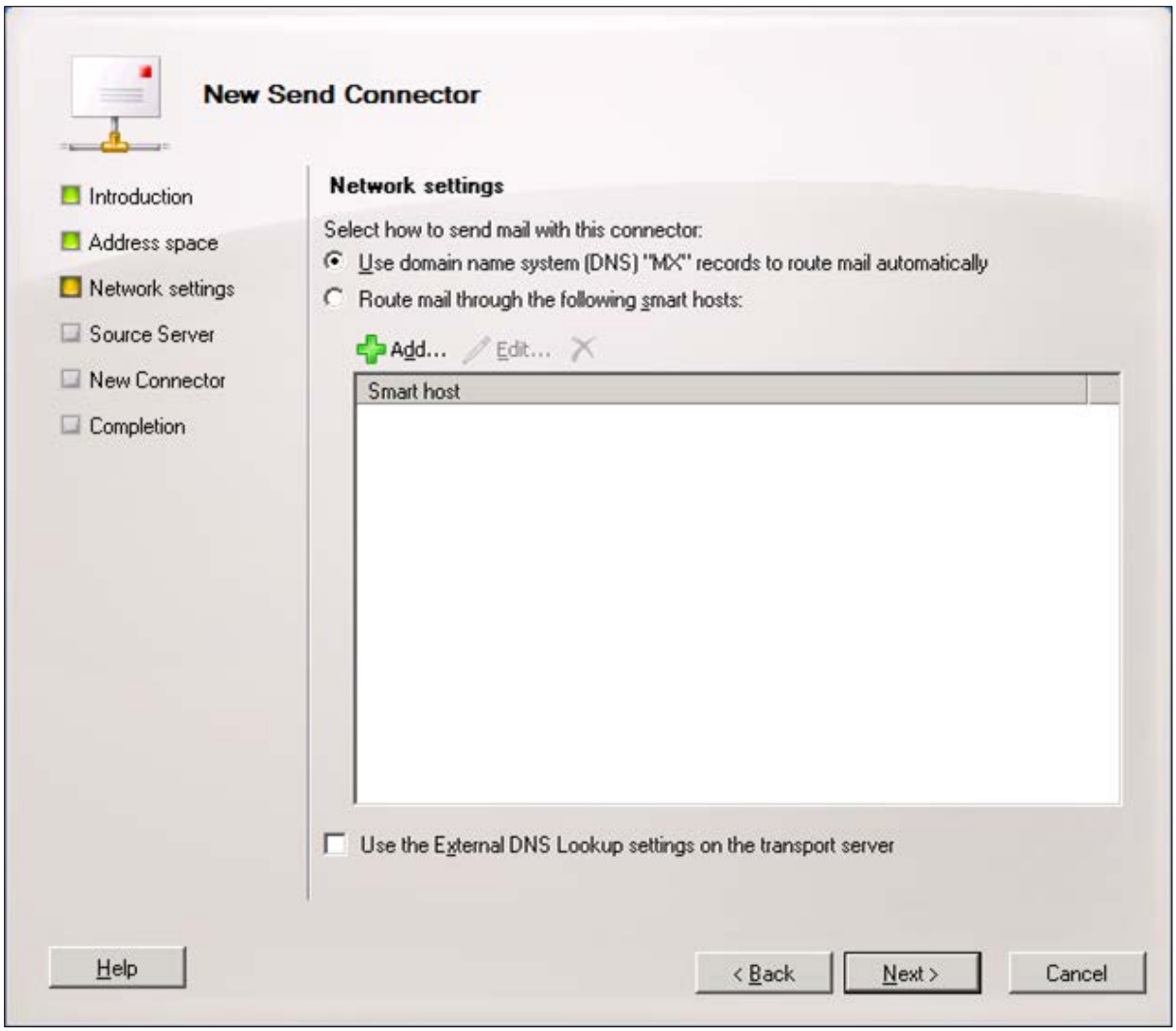
1. In the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and select the **Send Connector** tab. In the **Actions** panel, and click **New Send Connector**. The **New Send Connector** dialog displays. Enter a **Name** to identify this send connector.
2. From the **Select the intended use for this Send connector** menu, select **Custom**, and click **Next**.
3. In the **Address Space** section, click **Add**; the **SMTP Address Space** dialog box displays.
4. In the **Address space** field, type your region-specific MAS hostname, for example:
   mas.barracudanetworks.com
   mas.ca.barracudanetworks.com
   mas.uk.barracudanetworks.com



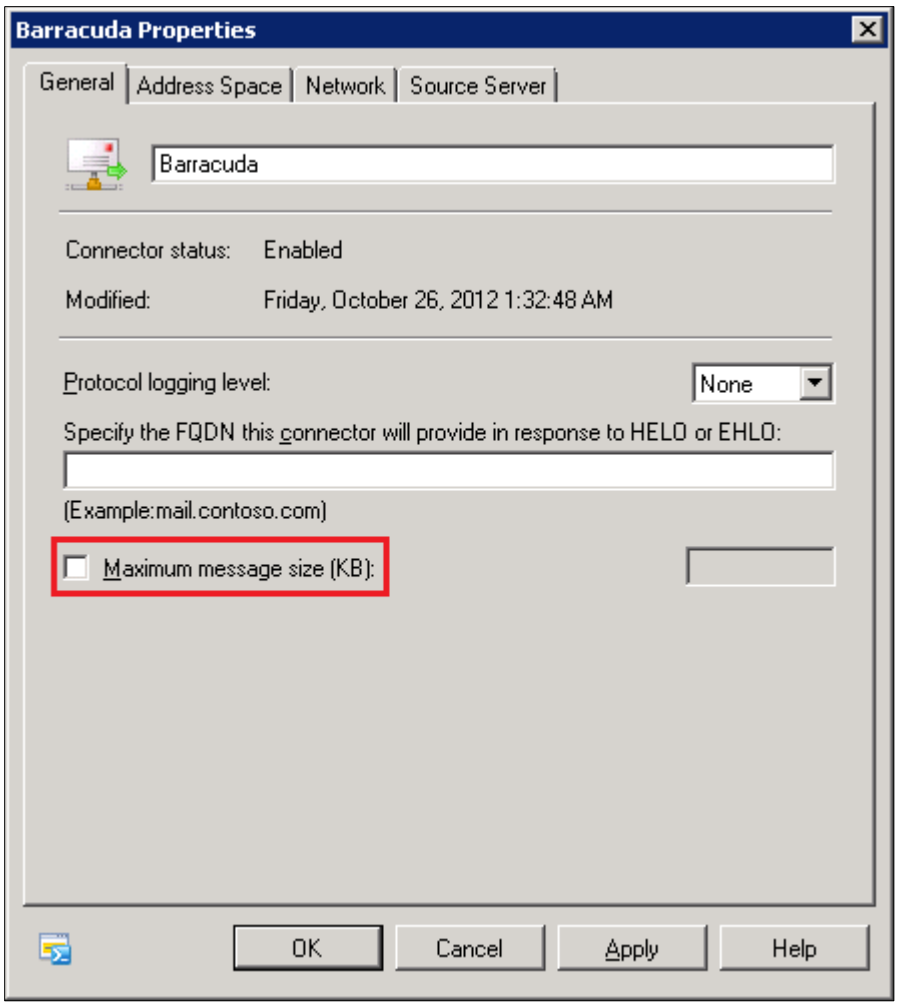
5. Click **OK**. The SMTP connector is added:



6. Click **Next**. Select the default setting **Use domain name system (DNS) "MX" records to route mail automatically**:



7. Click **Next**. In the **Source Server** page, if your Exchange server is not already listed, click **Add** to search for and add the server to this list. Click **Next** to verify your configuration, and click **New** to create the Send Connector. Click **Finish** to return to the **Send Connectors** tab; the newly-created Send Connector displays in the list.
8. Right-click on the new Send Connector, and click **Properties**.
9. In the **Properties** dialog box, clear **Maximum message size (KB)**:

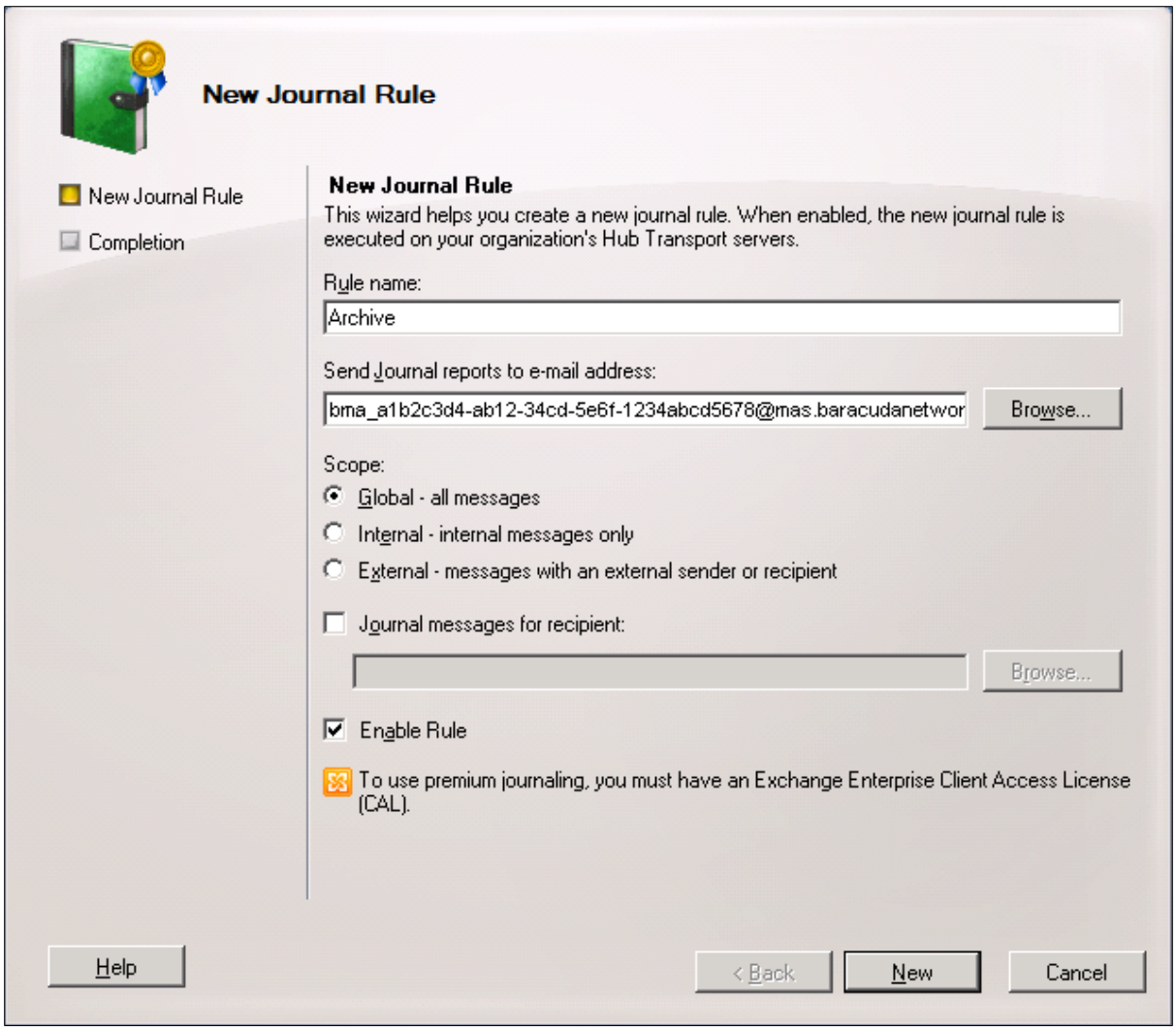


10. Click **Apply**, and then click **OK** to save your changes and close the dialog box.

Create Journaling Rule

Both the Standard and Enterprise versions of Microsoft Exchange Server 2007 and 2010 support Standard and Premium Journaling. Open the EMC, and complete the following steps to add a journaling rule:

1. In the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and select the **Journal Rules** tab.
2. In the **Actions** panel, click **New Journal Rule**; the **New Journal Rule** dialog displays.
3. Enter a Rule name, and for the **Send Journal reports to e-mail address**, click **Browse** and navigate to and select the mail contact you created in Step 2:



4. Select the Scope for archiving; the recommended setting is **Global - all messages** for the most complete coverage.
5. Turn on **Enable Rule**, click **New** to create the Journaling rule, and click **Finish** to return to the **Journal Rules** tab where the newly-created rule displays in the list.

Configure Exchange Integration

In addition to journaling mail, we offer the ability to integrate your Exchange database with the archiver service. The steps below will show you how to configure 3 actions: a historical import of your Exchange DB, synchronize non-email items (calendar, contacts, notes & tasks), and synchronize mailbox folder structure.

Please note: the steps outlined below required a **licensed** Exchange service account with global admin rights to the client's domain in order to synchronize data.

Create an Email Service Account for Exchange Server 2007/2010

An email service account provides Exchange Server directory permissions to grant the Barracuda Cloud Archiving Service unrestricted access to all mailboxes. Create an email service account for Exchange import integration.

Recommended

Microsoft Exchange Server 2007 & 2010 set bandwidth limits and restrict the number of processed messages by default which can impact job performance. Barracuda recommends disabling throttling for the service account after following the steps in this article. For details, see:

- How to Disable Throttling in Microsoft Exchange Server 2007 and 2010

Service Account Password Setting

When configuring the service account, you must set the password to never expire. To set this option in Active Directory (AD), go to the Properties dialog box for the service account, click the Account tab, and in the Account options section, select Password never expires. Click OK to save your settings.

To create an email service account, you will need to:

- Verify the service account has a mailbox, and is not hidden in the Global Address list.
- (Optional but highly recommended) Establish a user account through OWA or other source before setting up the email service account.

Microsoft Exchange 2007

1. Use the following steps to set the permissions on Exchange 2007:
2. Log in to the Exchange Server as the administrator.
3. From the Start menu, go to Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Shell.
4. At the command prompt, enter the following command where Exchange2007 is the name of the Microsoft Exchange 2007 Server and CUDASVC is the name of the Barracuda service account, and then press Enter:

   get-mailboxserver *Exchange2007* | add-adpermission -user *CUDASVC* -accessrights GenericRead, GenericWrite -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin

5. In the Exchange Management Shell, enter the following command to add View-Only Administrator permissions, replacing CUDASVC with the name of the Barracuda service account:

   add-exchangeadministrator *CUDASVC* -role ViewOnlyAdmin

Important:
If inheritance to the individual mail stores is not enabled on a custom mailbox database, to set the Send As, Receive As, and Administer Information Store permissions at the store level, you must enter the following command in the Exchange Management Shell:

```
Add-ADPermission -identity "custom database name" -user "CUDASVC" -accessrights GenericRead, GenericWrite -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin
```

To verify the Send As, Receive As, and Administer Information Store permissions, enter the following command in the Exchange Management Shell, where *Exchange2007* is the name of the Microsoft Exchange 2007 Server, *dbname* is the name of the Exchange mail database, and *CUDASVC* is the name of the Barracuda service account:

```
get-mailboxdatabase Exchange2007\dbname | get-ADpermission -user CUDASVC | Format-List
```

Microsoft Exchange 2010

Use the following steps to set the permissions on Exchange 2010, 2013, or 2016 where *database name* is the name of the Microsoft Exchange Server and *CUDASVC* is the name of the Barracuda service account:

1. Open your **Exchange Management Shell**.
2. At the command prompt, enter the following command, and then press **Enter**:
   Get-MailboxDatabase | Add-ADPermission -User *"CUDASVC"* -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin
3. Next, enter the following command, and then press **Enter**:
   Add-RoleGroupMember "Organization Management" -Member "*CUDASVC*"

Use the following steps to apply permissions for the service account to a specific MailStore database rather than all databases:

1. Open your **Exchange Management Shell**.
2. At the command prompt, enter the following command, and then press **Enter**:
   Get-MailboxDatabase -Identity *database name* | Add-ADPermission -User "*CUDASVC*" -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin

Historical Import of Exchange Server Database

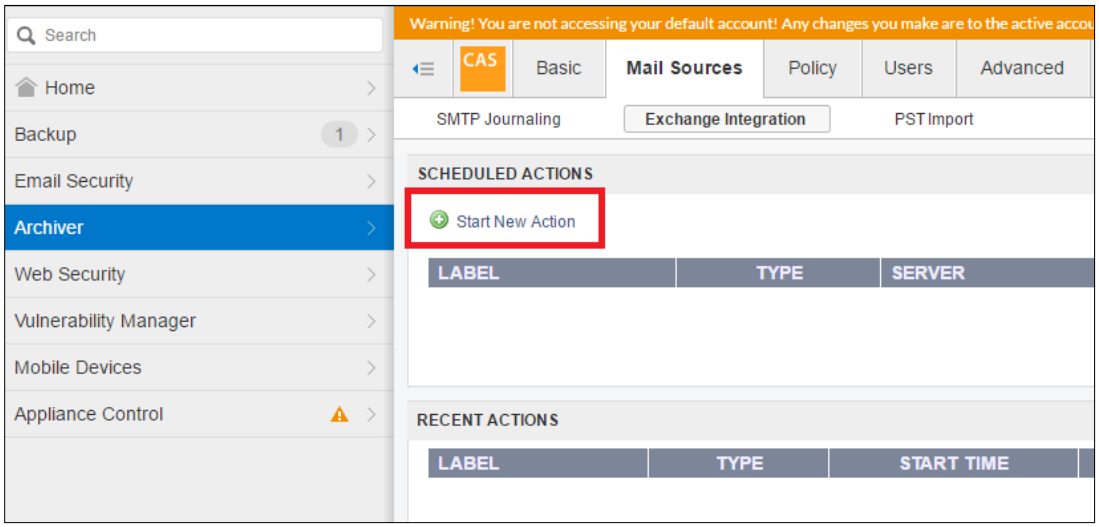
Add New Server

Configure a new Exchange Server:

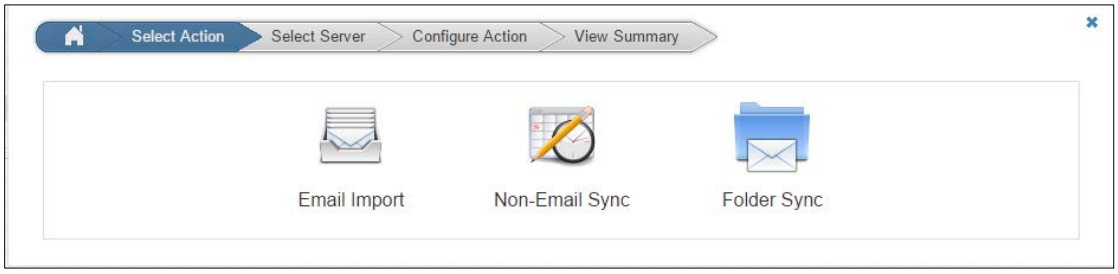
Automatically Discover Server Settings for Email Import

Use autodiscover to automatically populate your server settings using the steps in this section. If, however, autodiscover is unable to identify your server settings, you can manually enter the details as described in the section *Manually Configure Server Settings for Email Import.*

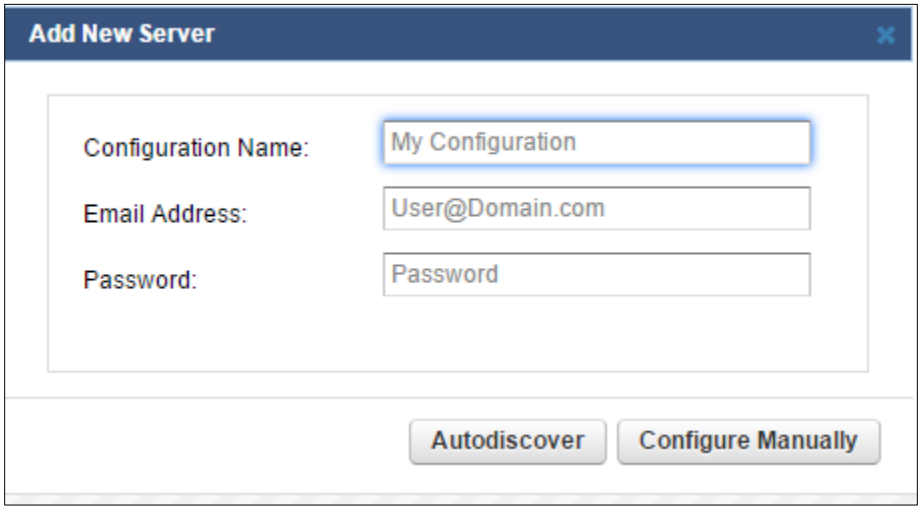
1. Log in to the Barracuda Cloud Archiving Service as the admin, and go to **MAIL SOURCES > Exchange Integration.**
2. **Click** Start New Action**.**



3. **In the** Select Action **page, click** Email Import**.**



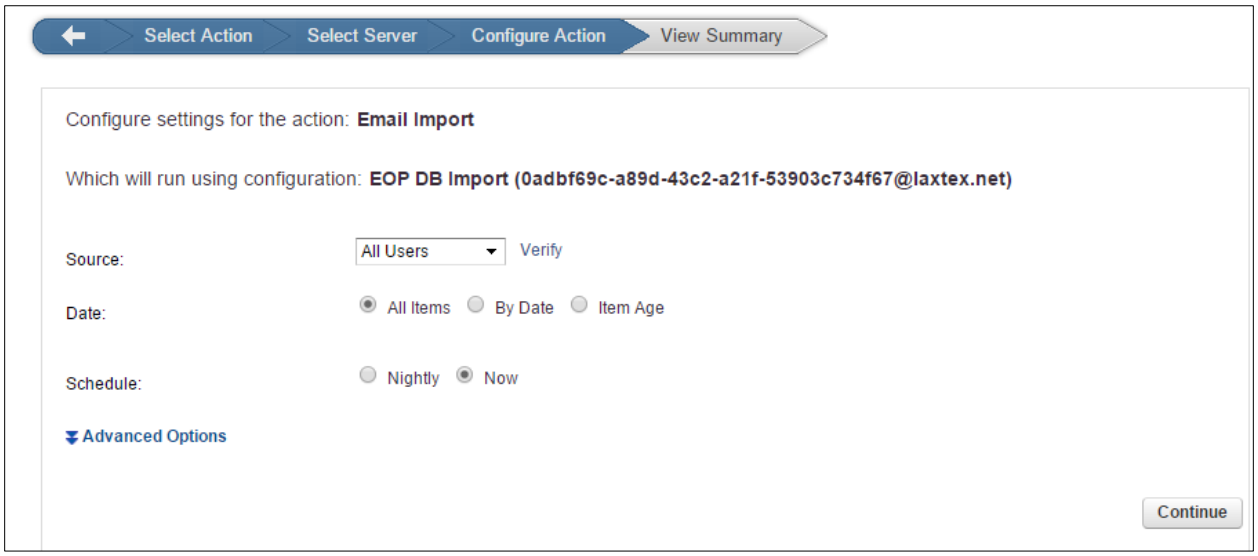
4. **In the** Select Server **page, click** Add New Server**.**



5. **In the** Add New Server **dialog, enter a name to identify the configuration as well as the service account** Username/Password**. Click** Autodiscover

Please note: If autodiscovery fails please skip ahead to the manual configuration section below.

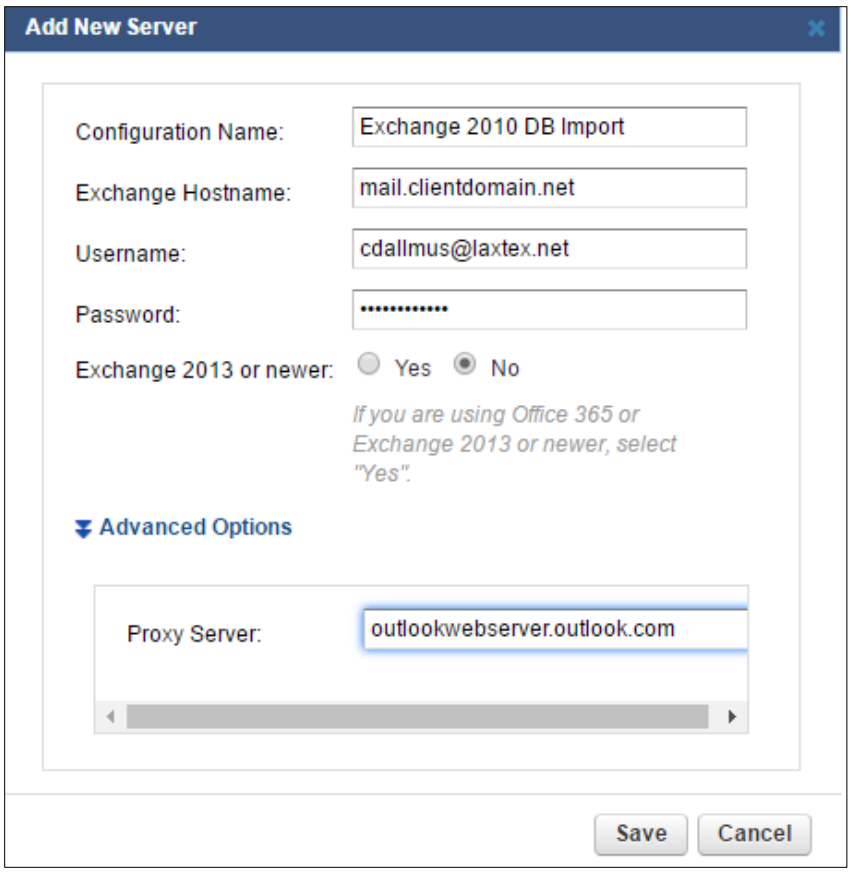
6. When the server details display**, click** Save**.**
7. The server is added to the Server table**. Click** Continue**.**
8. In the Configure Action page**,** select **All Users** from the drop-down menu, and specify the desired Date and Schedule settings**. Click** Continue**.**
9. Verify the configuration settings in the **View Summary** page, and then click Submit **to** add the Email Import to the **Scheduled Actions** table.



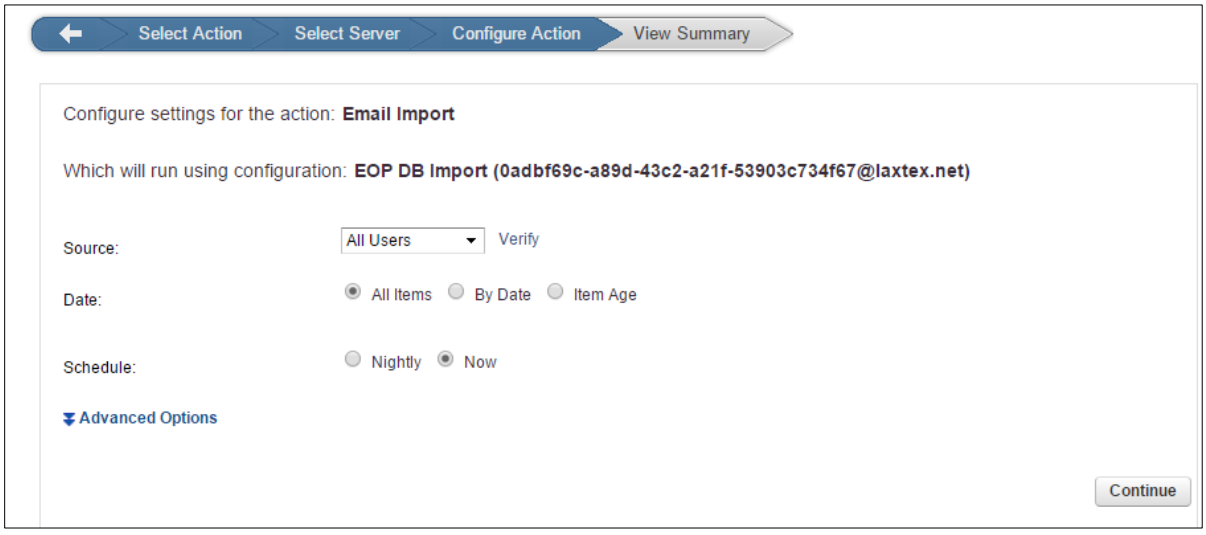
Manually Configure Server Settings for Email Import

1. **Click** Configure Manually**,** and enter the following details**:**
   a. **Configuration Name** – Name to identify the Exchange Server.
   b. **Exchange Hostname** – Fully qualified domain name (FQDN) or IP address of the Exchange Server where the action is to be performed.
   c. **Username/Password** – Username and password associated with the service account.
   d. **Advanced Options**:

      i. Proxy Server **–** enter the Outlook Anywhere/Outlook Web Access (OWA) address, for example *mail.domain.com* or *webmail.domain.com*



2. Click **Save** to add your configuration and close the dialog box.
3. In the Configure Action page, click **Continue.**

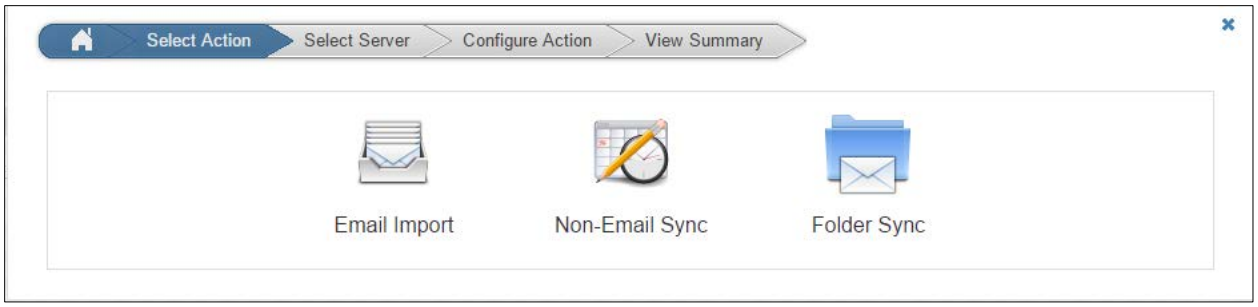


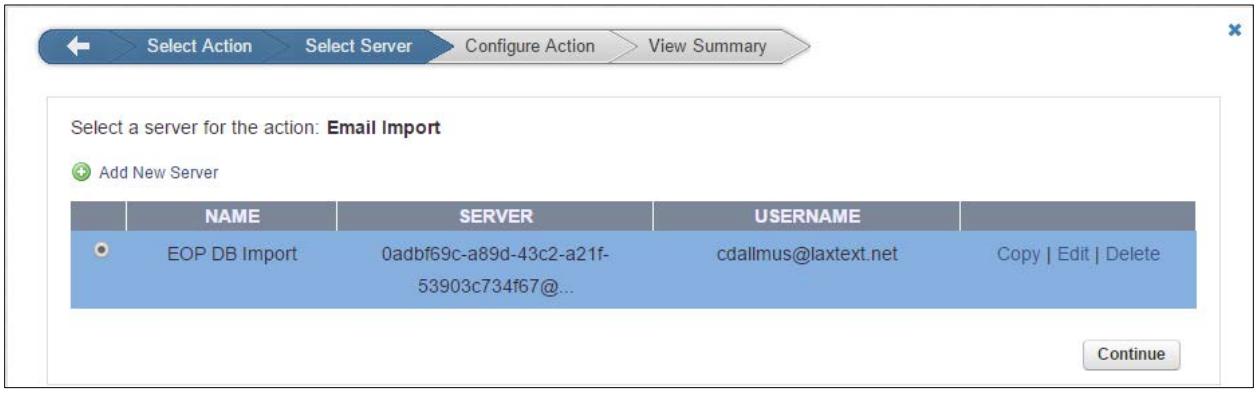
4. In the View Summary page, select **All Users** from the Source drop-down menu.
5. In the schedule section, enter the desired Date and Select **Now**. Click **Continue**.

6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

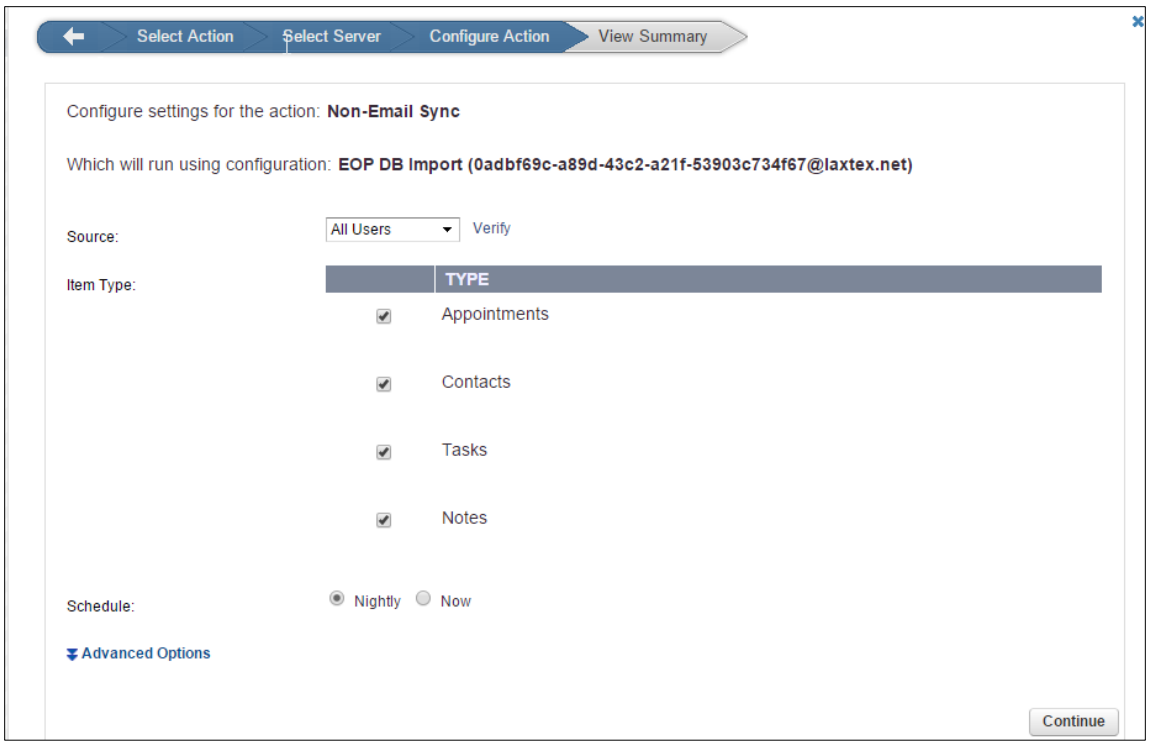
Exchange Non-Email Sync

1. Log in to the Barracuda Cloud Archiving Service as the admin, and go to Mail Sources > Exchange Integration.
2. Click **Start New Action**. In the Select Action page, click **Non-Email.**
   a. If you previously imported your Exchange DB, the Exchange server will be saved. If not, please reference this section for connecting your Exchange server.





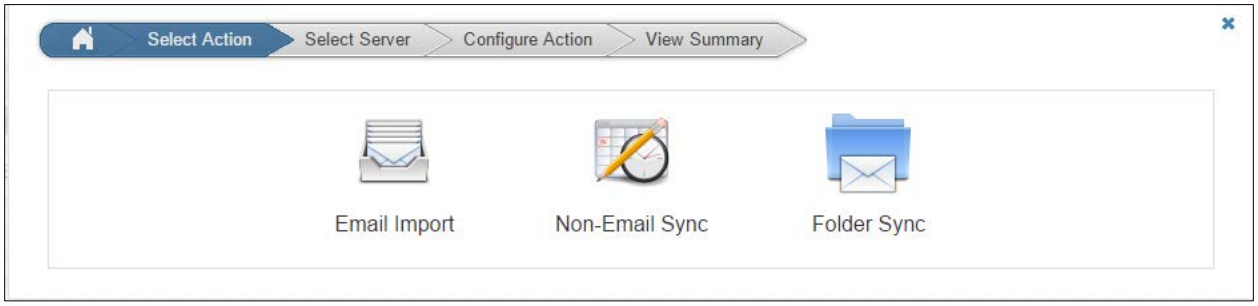
3. In the Configure Action page, Click **Continue**.
4. In the View Summary page, select **All Users** from the Source drop-down menu. For item type, check or de-check any of the items you would like to synchronize. For schedule, select **Nightly**. Then click **Continue**.



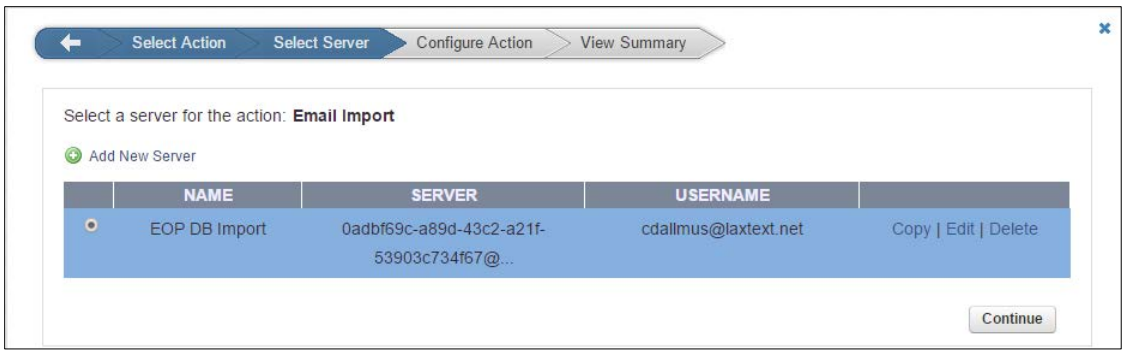
5. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

Exchange Folder Structure Sync

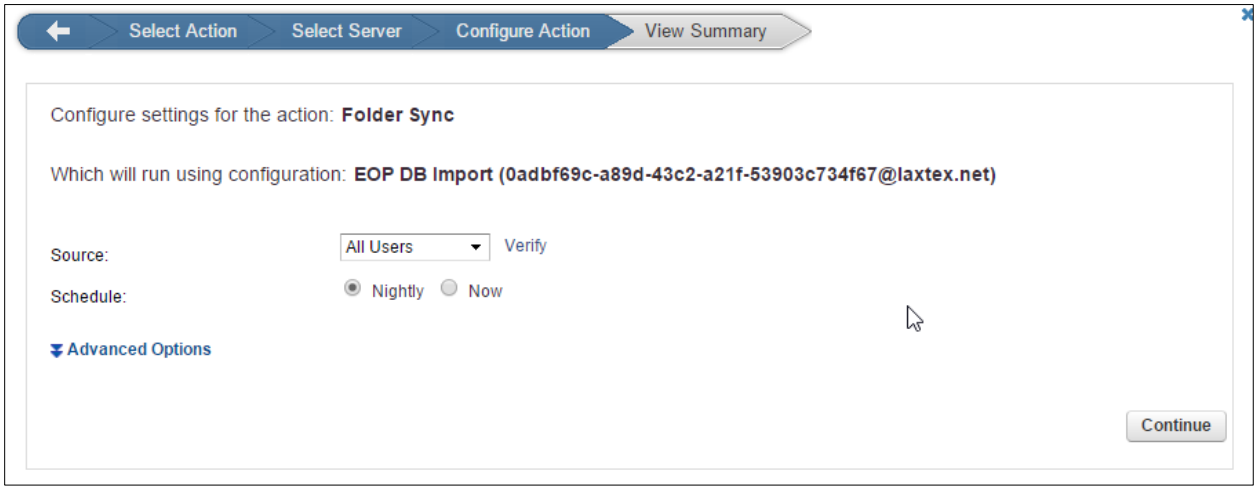
1. Log in to the Barracuda Cloud Archiving Service as the admin, and go to Mail Sources > Exchange Integration.
2. Click **Start New Action**. In the Select Action page, click **Folder Sync.**



3. If you previously imported your Exchange DB, the Exchange server will be saved. If not, please reference this section for connecting your Exchange server.



4. In the Configure Action page, Click **Continue**.
5. In the View Summary page, select **All Users** from the Source drop-down menu. For item type, check or de-check any of the items you would like to synchronize. For schedule, select **Nightly**. Then click **Continue**.

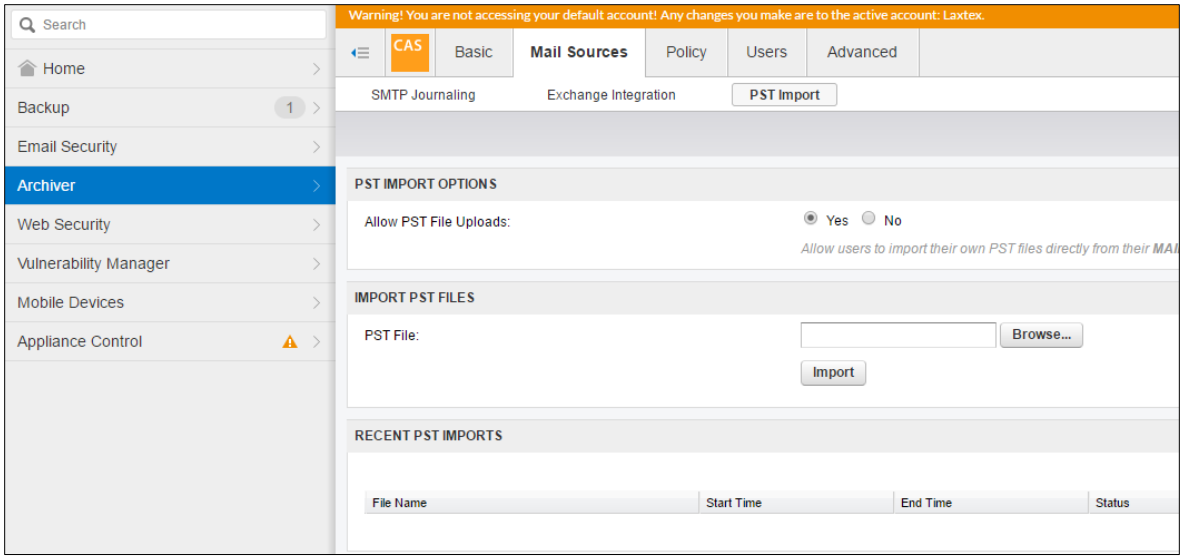


6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

PST Import

For any of your end users/clients who have local only PST files, we can ingest those into your archive in order to adhere to your client's compliance regulations.

1. Log in to the Barracuda Cloud Archiving Service as the admin, and go to Mail Sources > PST Import.
2. Under the Import PST files section, click **Browse** to navigate to the local only PST file.



Please note: The manual process for importing PSTs has a threshold of 250MB PST files. If you have larger PST files and would like to ingest those, please call into Barracuda Support and they will send you an SFTP link to securely upload your PSTs on Barracuda bandwidth.

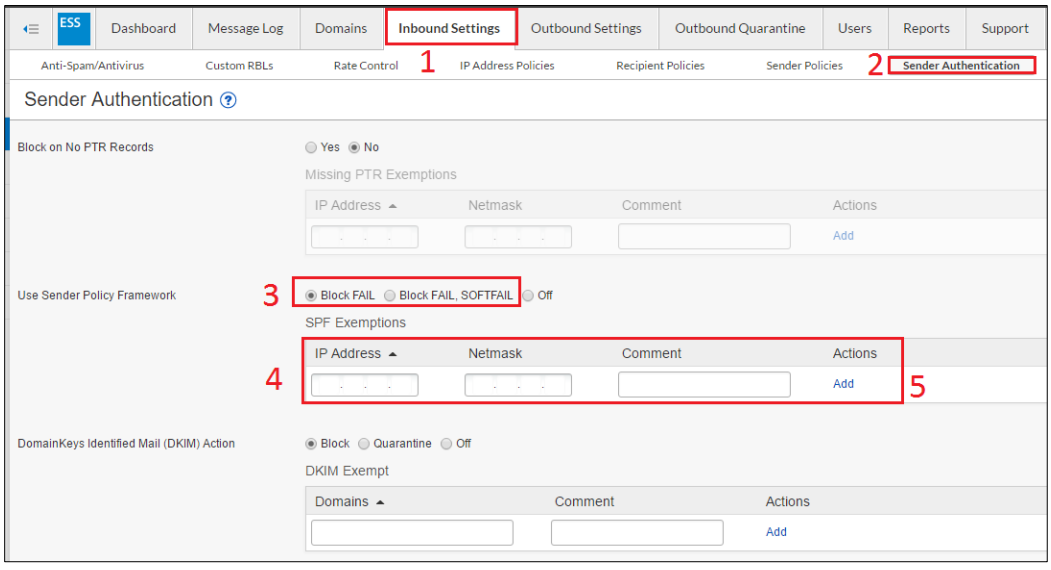
Appendix 1 – How to exempt or disable SPF checking for the Barracuda ESS service

The steps below will show you how to exempt the BESS from SPF checking or to disable SPF checking within our service.

1. Go to **BCC** > **Email Security** > **Inbound Settings (1)** > **Sender Authentication (2)**
2. To exempt our service from SPF checking, set the Use Sender Policy Framework to either **Block FAIL** or **Block FAIL, SOFTFAIL (3).**

   Please note:
   Block FAIL option - The SPF FAIL (also referred to as Hard Fail) response indicates that the IP address of the message sender does not match the IP address or range of IP addresses specified in the sending domain name's SPF record, and that the real owner of the domain has specifically indicated that such messages should be rejected (blocked) as spoofed.
   Block FAIL, SOFTFAIL option- The SPF SOFTFAIL response indicates that the message sender's IP address does not match the IP address or range of IP addresses specified in the sending domain name's SPF record. A SOFTFAIL means that the domain owner did not specify how such messages should be handled. If quarantine is enabled, messages in either the SPF SOFTFAIL or FAIL state are sent to the user's quarantine. If quarantine is disabled, messages in either the SPF SOFTFAIL or FAIL state are blocked.

3. Then add our IP address ranges to the SPF exemptions **(4)**:
   IP Address: **64.235.144.0** Netmask: **255.255.240.0** Comment: **Barracuda ESS Exempt**
   IP Address: **209.222.80.0** Netmask: **255.255.248.0** Comment: **Barracuda ESS Exempt**
4. Click **Add (5)**.



Appendix 2 – How to Disable Throttling in MS Exchange Server 2007

Microsoft Exchange Server 2007 RPC client throttling is enabled by default and allows Exchange to restrict the number of processed messages. If you wish to disable throttling, you can do so through the RPC Throttling Factor Registry. For more information, see the Microsoft TechNet Article Understanding Client Throttling.

Use the following steps to disable throttling in Exchange Server 2007:

1. Log in to the Exchange Server as the administrator, and run regedit to open the Registry Editor.
2. Browse to the following location: **HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem**
3. Double-click the **DWORD** key **RPC Throttling Factor**, and change the value to **0**; if the key is not present, right-click and create a new **DWORD** called **RPC Throttling Factor**.
4. Close the Registry Editor.

Appendix 3 – How to Disable Throttling in MS Exchange Server 2010

Use the following steps to assign the Microsoft Exchange Server service account to the Application Impersonation Management role:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
3. At the command prompt, type the following command replacing *serviceAccount* with the account created in **Step 1: Create Service Account**:
   New-ManagementRoleAssignment -Name:exchangeImpersonation -Role:ApplicationImpersonation -User:serviceAccount

Create and Assign Throttling Policy

Use the following steps to create and assign a new throttling policy, replacing *PolicyName* with the new policy name, and replacing *PolicyAdmin* with the Exchange Server 2010 service account.

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
3. At the command prompt, type the following command:
   New-ThrottlingPolicy *PolicyName*
4. Press **Enter**. At the command prompt, type the following command:
   Set-ThrottlingPolicy *PolicyName* -RCAMaxConcurrency $null -RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null -EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
5. Press **Enter**. At the command prompt, type the following command:
   Set-Mailbox "P*olicyAdmin*" -ThrottlingPolicy *PolicyName*
6. Press **Enter**.