BARRACUDA ESSENTIALS FOR EXCHANGE SERVER 2013

Services Configuration

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

Intronis

Table of Contents

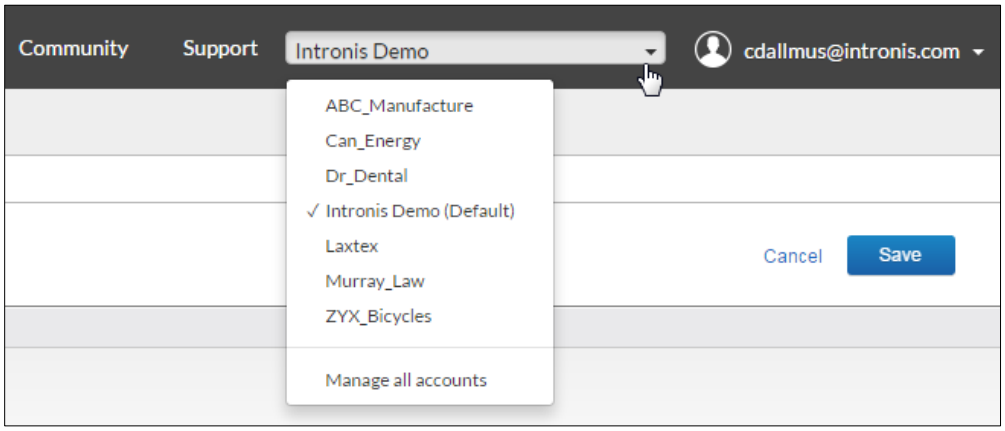
Understanding the Barracuda Cloud Control (BCC) as an MSP

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 [2013] 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 [2013] Admin Center –** You will need the customer's credentials to access their Exchange Admin Center.
- Any **email address** on customer's domain.

Ensure Connectivity and Redundancy

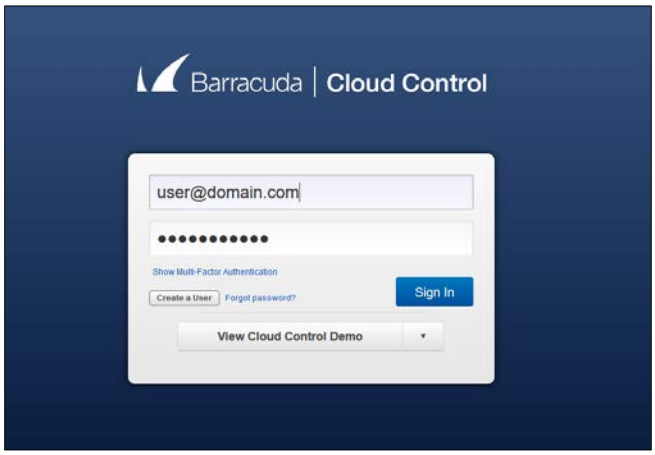
1. Open your firewall ports to allow the IP address ranges 64.235.144.0/20 [/20=255.255.240.0] & 209.222.80.0/21 [/21=255.255.248.0]
2. Where relevant, verify your network subnet is granted access in the ACL on your mail server (and LDAP server where applicable)
3. Block all port 25 traffic except for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

Inbound Scanning Setup

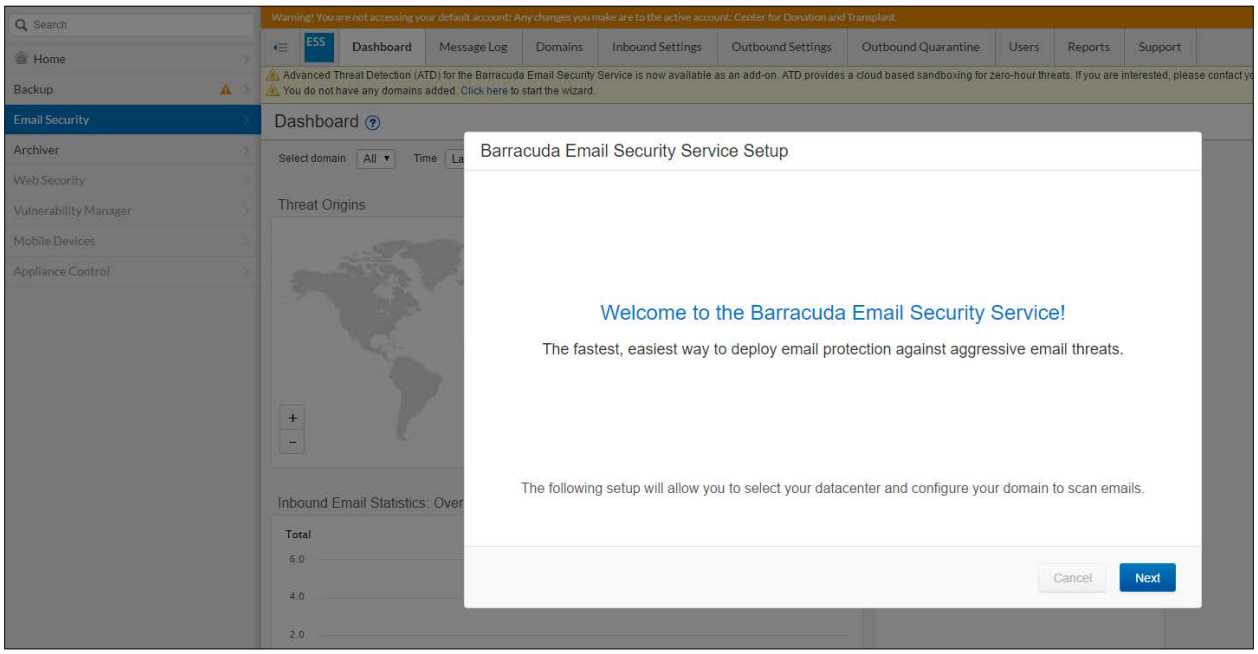
During this step we will configure the customer's domain for BESS. This will be done using the BESS wizard. You will want to have the domain & mail server IP information for this step.

Add a Domain to Barracuda Cloud Control

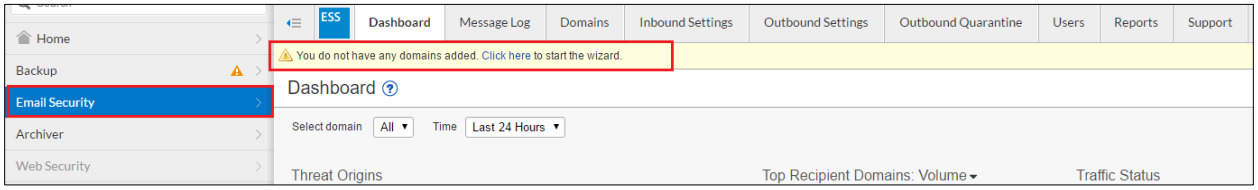
1. **Login** to the BCC (https://login.barracuda.com) console.



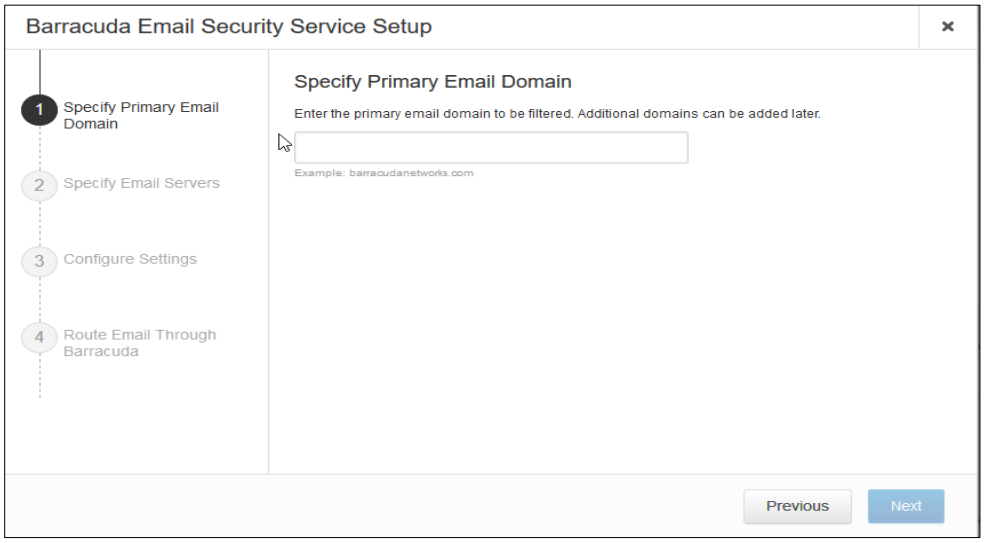
2. If this is your first time logging into a customer's Email Security service, you will be prompted with the wizard automatically:



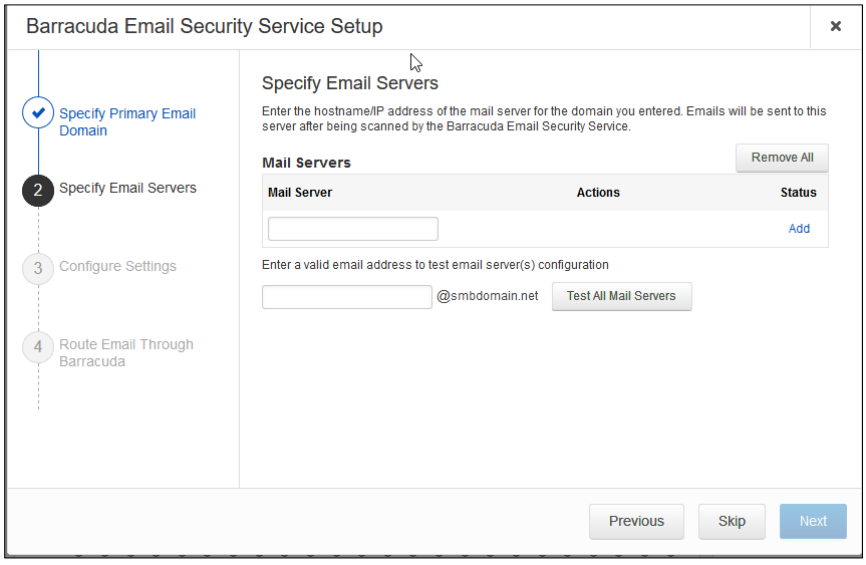
3. If you've already logged into their service before, but you have not yet started the configuration, **click here** to start the wizard:



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**.

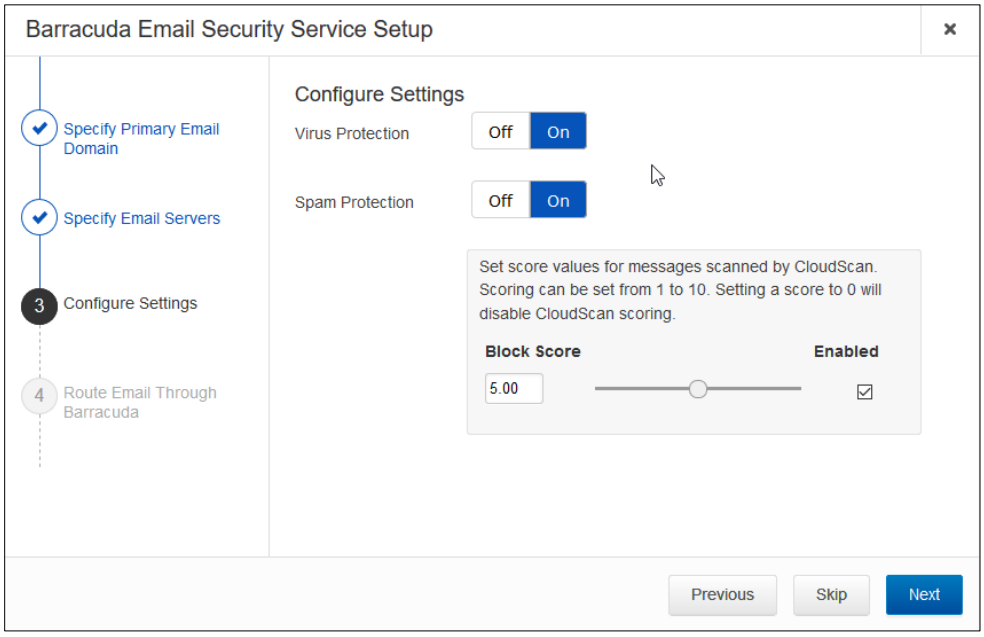


7. Click **Test All Mail Servers**.

   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.

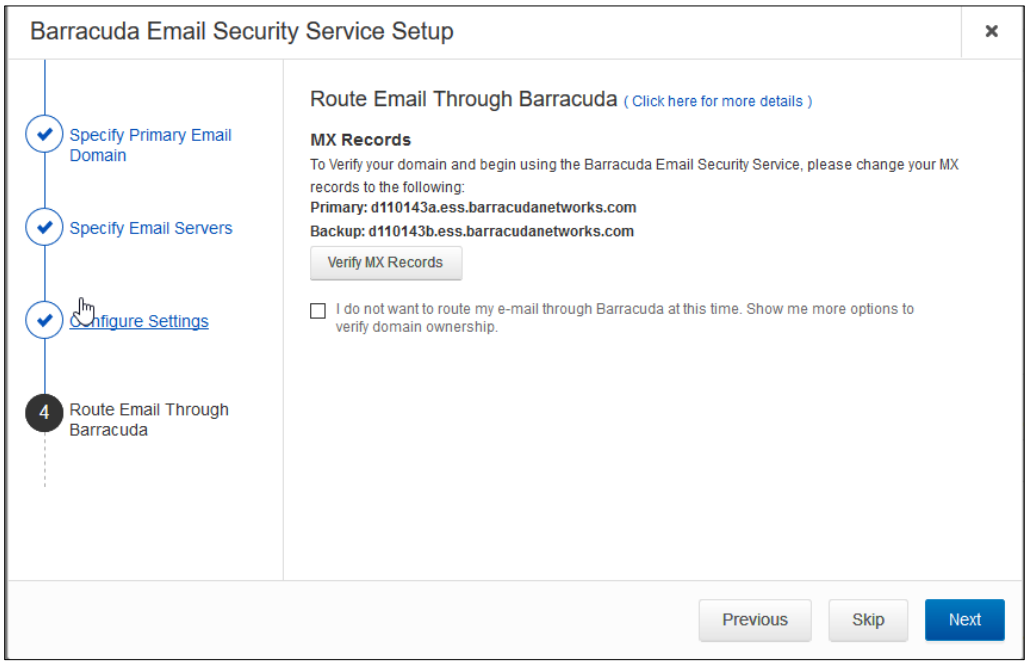
   By default Virus & Spam Protection are enabled and the CloudScan Spam Scoring system's block threshold is set to 5. This can be modified later in the **Inbound**

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.

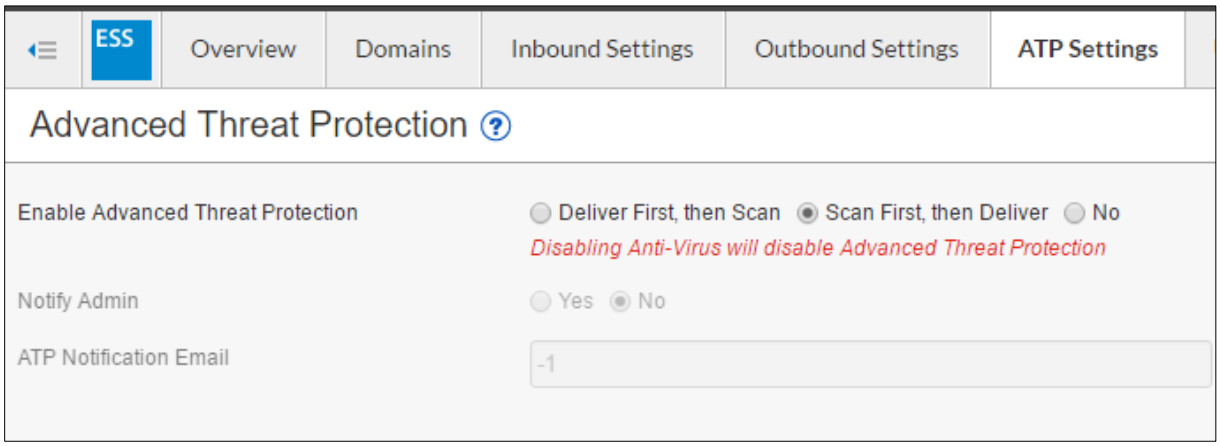
Best Practice Recommendations

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.

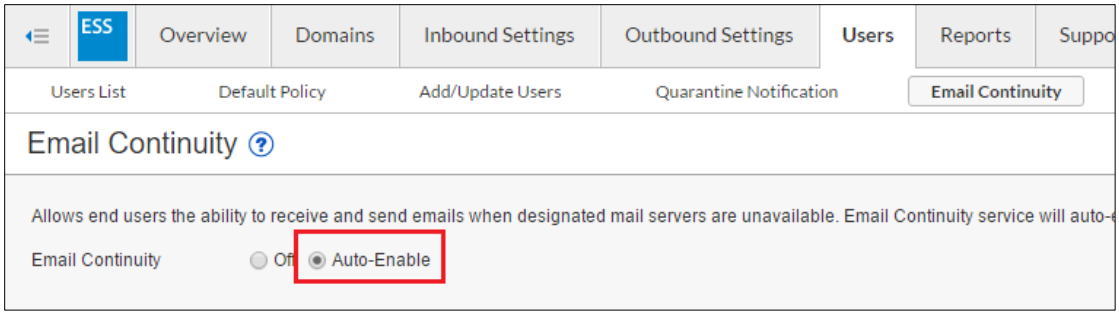
1. Log in to BCC and go to the **Email Security Service.**
2. Navigate to the top menu bar for the **ATP Settings** tab.
3. Set ATP to Scan first, then Deliver.

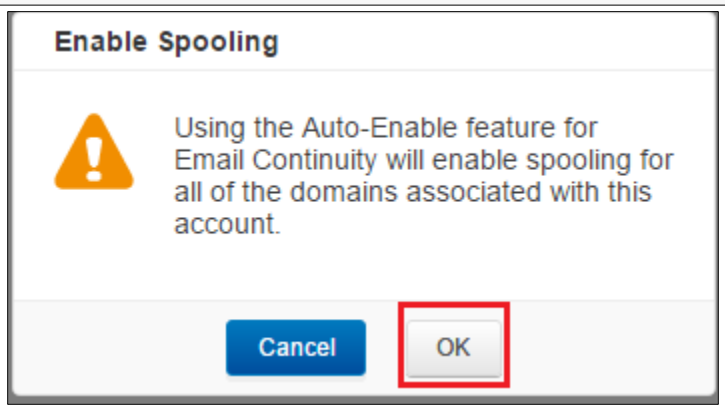


Enable Email Continuity

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.



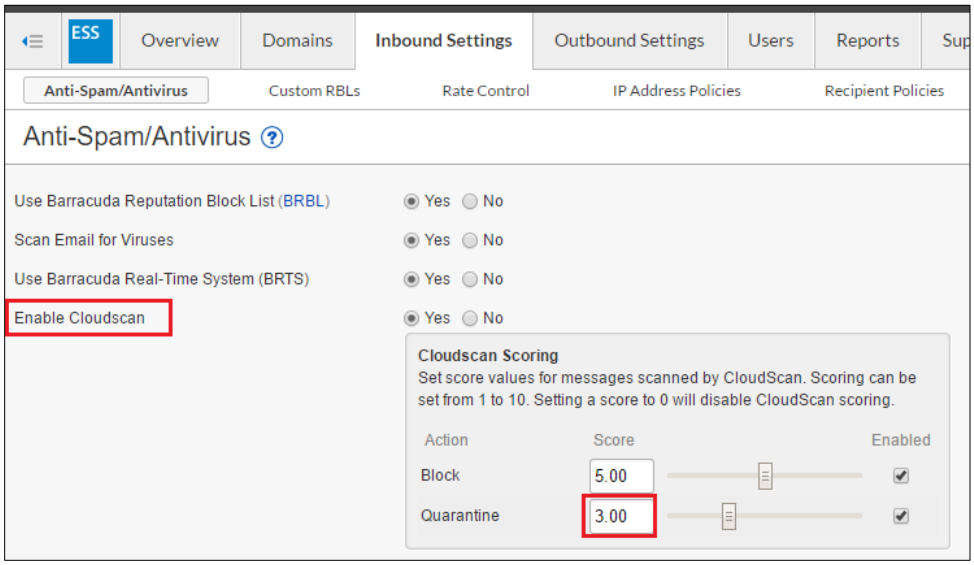


Enable Inbound Quarantine

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 to receive inbound mail from the Barracuda ESS

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 range. If you are using Exchange 2010, please refer to Appendix 2.

1. In the EAC, navigate to **Mail flow** > **Receive connectors**. Click **Add** + to create a new Receive connector.
2. On the **New receive connector** page, specify the name as "**BESS Inbound**" for the Receive connector and then select **Frontend Transport** for the **Role**.
   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. Choose **Partner** for the type.
4. For the **Network adapter bindings**, 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**.
5. If 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, click **Edit** − to edit it. Click **Add** +, add the Barracuda ESS IP address ranges: **64.235.144.0/20** [/20=255.255.240.0], & **209.222.80.0/21** [/21=255.255.248.0 and click **Save**.
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 **Mail flow** > **Accepted Domains**. Click **Add** + 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.

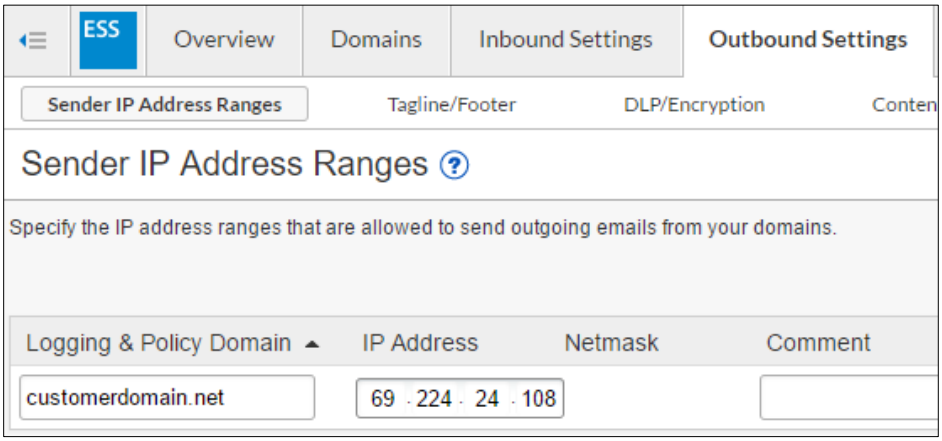
> **Please Note**: To configure Encryption, Outbound Scanning must also be configured.

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"

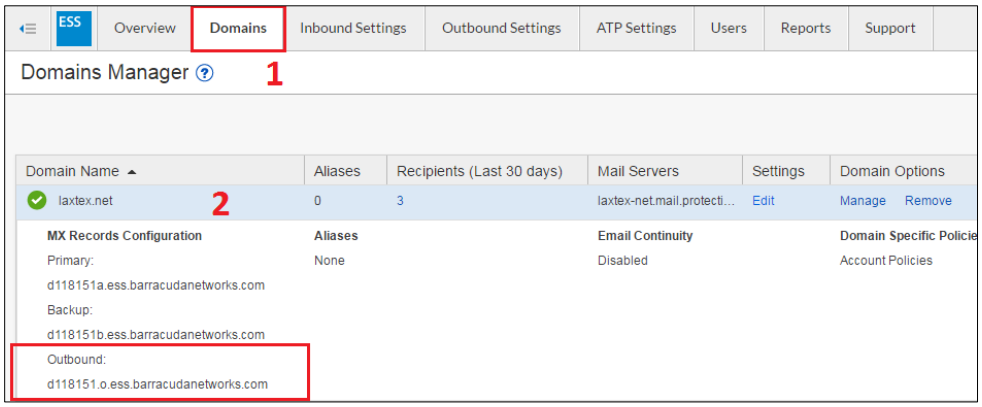


Send Connector

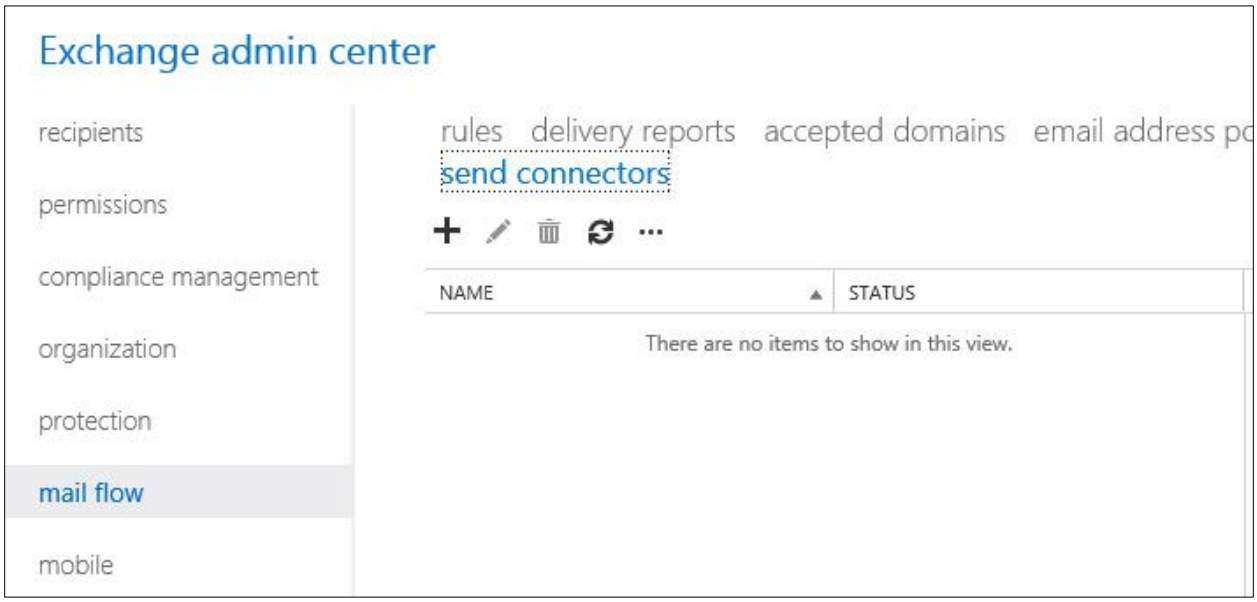
We will add an outbound send connector within Exchange Admin Center to route outbound mail through a Barracuda smart host.

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

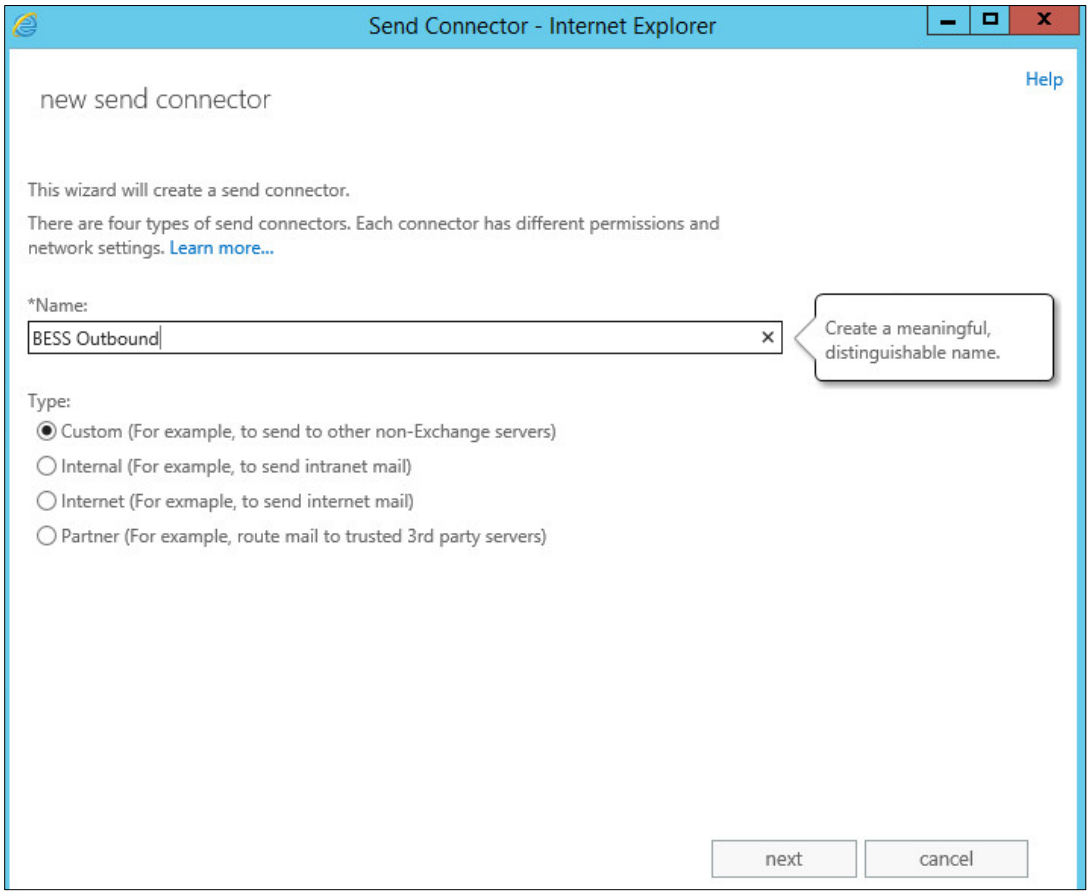
   If you have forgotten, login to **BCC** [select the appropriate customer from the account switcher] > **Email Security** go to **Domains (1) > Settings (2)** and copy the outbound hostname under the MX records configuration.



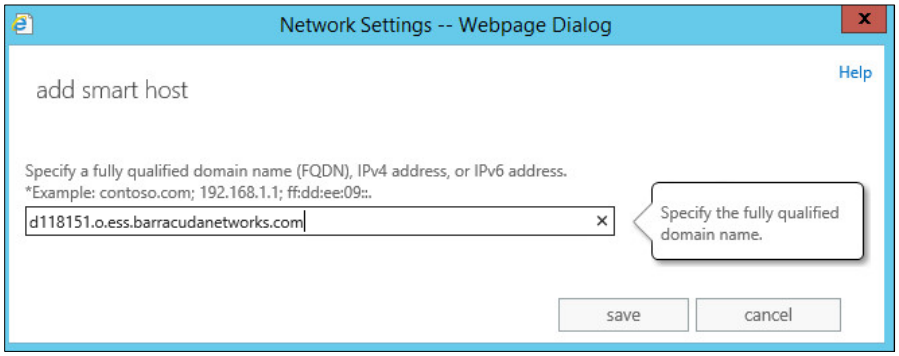
2. Within Exchange Admin Center go to **Mail flow > Send Connectors > click +** to add a new connector.



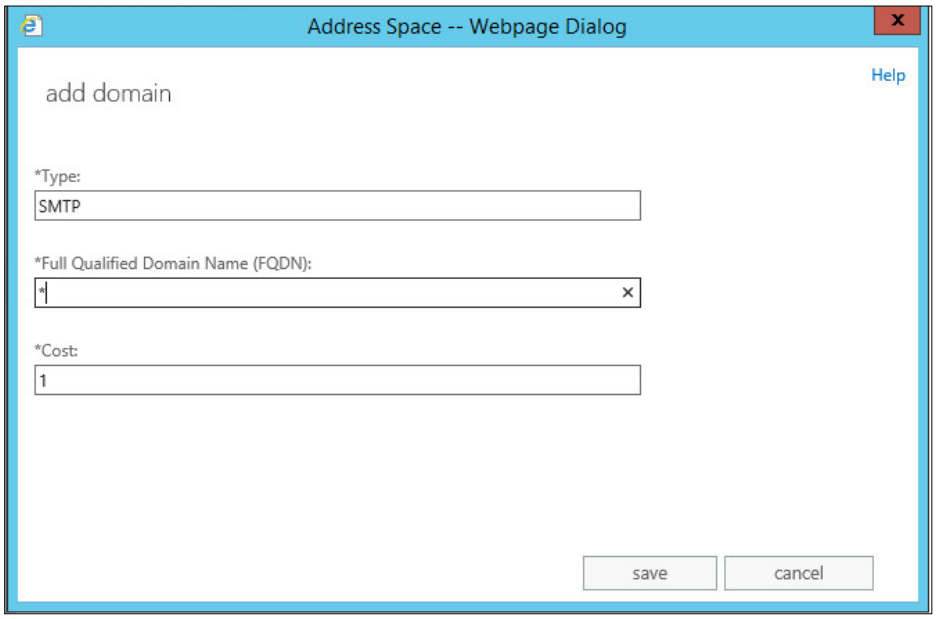
3. Enter the Name**, BESS Outbound** & for type select **Custom:**



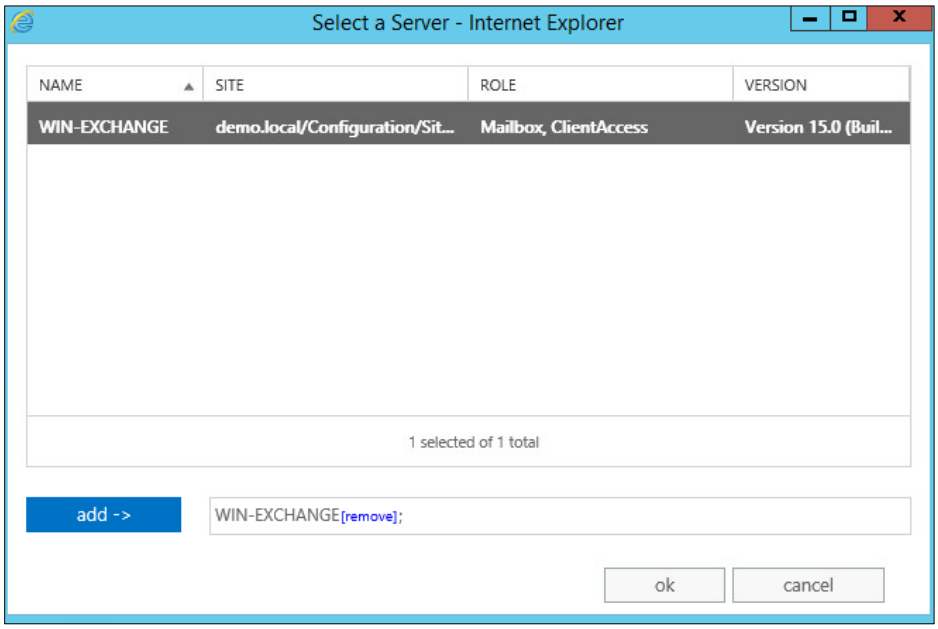
4. For the network settings sections, select the radio button for **Route mail through smart hosts/**
5. Click '**+**' and enter the outbound hostname from step 1. Click **Save.** Then click **next.**



6. For Smart Host authentication**,** leave **None** selected. Click **next**.
7. For the address space section, click + then enter '*' in the FQDN field for wildcard all external domains, type & cost can be left at default. Click **Save**, then click **next**.

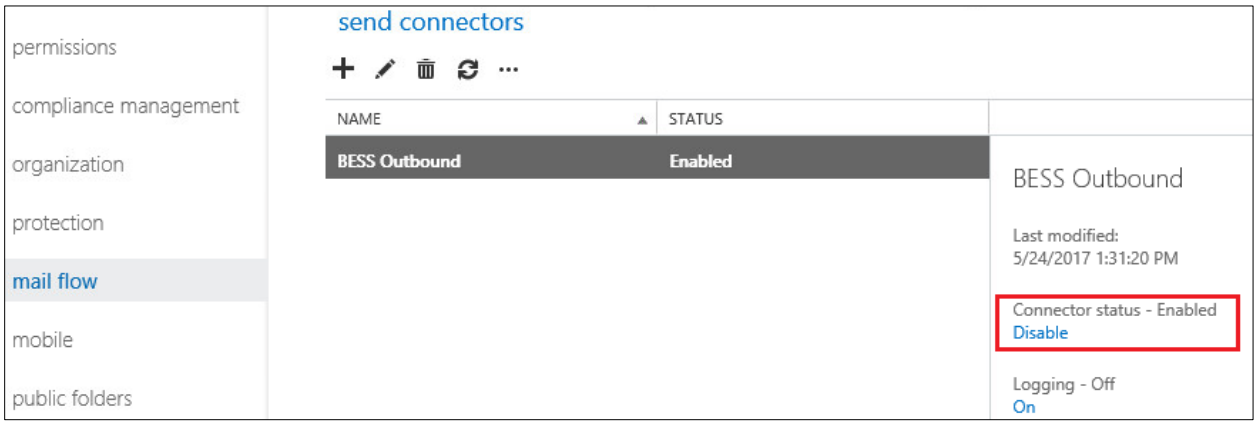


8. For the source server section, click the **+**, select the **Exchange server** that will be sourcing the outbound mail, then click **add** & **ok**.



9. **Click Finish** to finalize the connector.

Please Note: If you do not wish to enable this send connector at this time, navigate to the action panel to the right of the highlighted connector and click **disable**.



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

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.

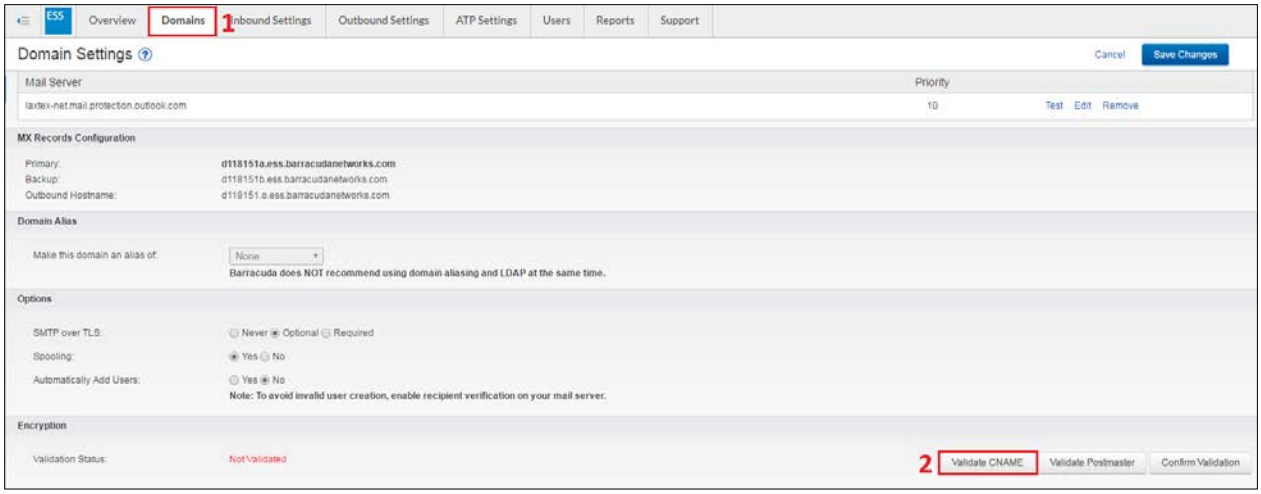
Encryption (Optional)

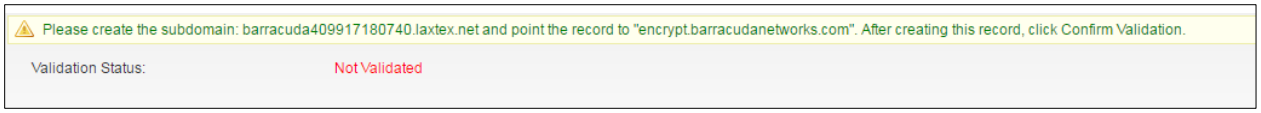
Overview

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**

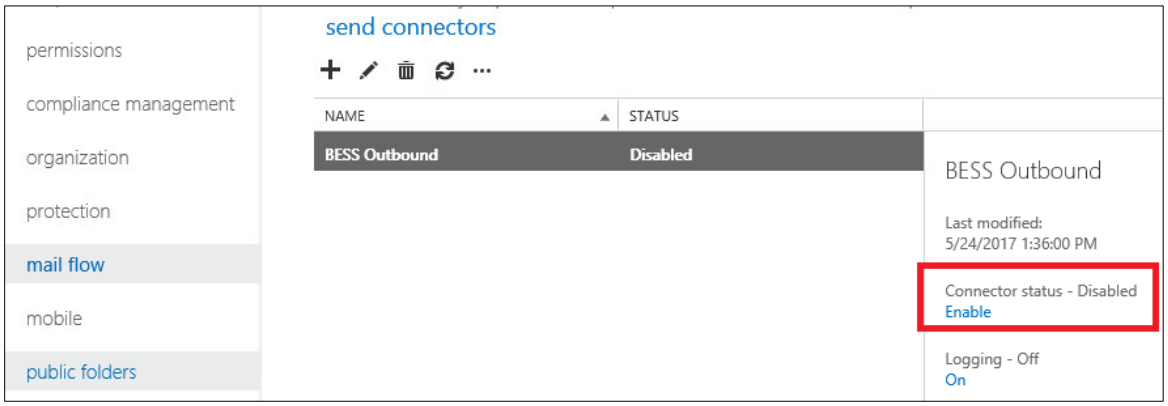
Please Note: Allow the DNS propagation to take effect before proceeding – this can take up to 24 hours for some providers.

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 Admin Center** - Enable the Outbound Send Connector in the Exchange Admin Center to allow outbound mail to flow through the BESS. Go to the **Exchange Admin Center > Mail flow > Send Connectors**. Select the 'BESS Outbound' send connector and in the status pane to the right click 'Turn it on'



Barracuda Cloud Archiving Service

Overview

In this section we will configure your customer's Exchange 2013 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 the Exchange Admin Center**

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. 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**.

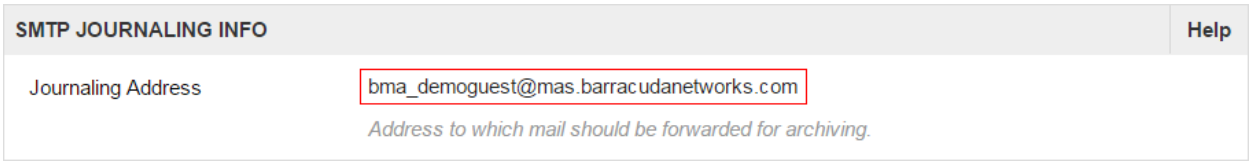
   The page will refresh, click **Mail Sources > SMTP Journaling** where a **journaling address** will be generated. Copy this address to clipboard, we will use this when we create a journaling rule within Exchange in the journal rule step.

Configuring Journal Archiving for Exchange

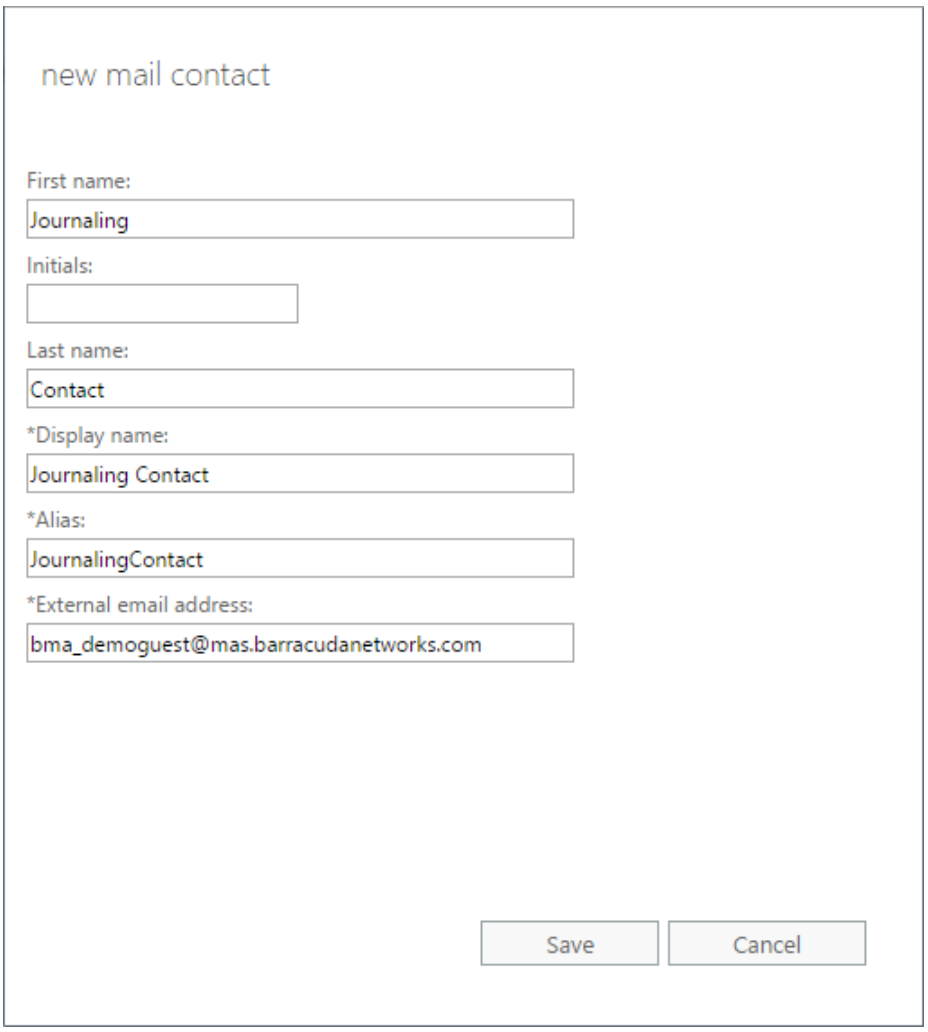
Create Mail Contact

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.

1. Log in to the Barracuda Cloud Archiving Service, and copy your journaling address from the **Mail Sources > SMTP Journaling** page:



2. Log in to the Exchange Admin Center (EAC), and in the left pane, click **recipients > contacts**.
3. Click the **+** symbol, and click **Mail contact**.
4. In the **new mail contact** window, enter **Journaling** in the **First name** field, and **Contact** in the **Last name** field. The **Display name** field automatically populates.
5. Enter **JournalingContact** in the **Alias** field (no spaces), and paste the journaling address copied from the **Mail Sources > SMTP** page into the **External email address** field:



6. Click **Save**.

Configure Journaling

Option 1. Configure Journaling via Script

1. Go to the **Mail Sources > SMTP Journaling** page.
2. Go to **Journaling Setup Scripts** > **Exchange 2013 or newer - Standard Journaling**.
3. Click **Show Script** to copy the script to your clipboard, or click **Download** to save the PowerShell script to your local system.
4. Open Windows PowerShell, and run the script to configure Microsoft Exchange Server 2013+ to journal mail to the Barracuda Cloud Archiving Service.

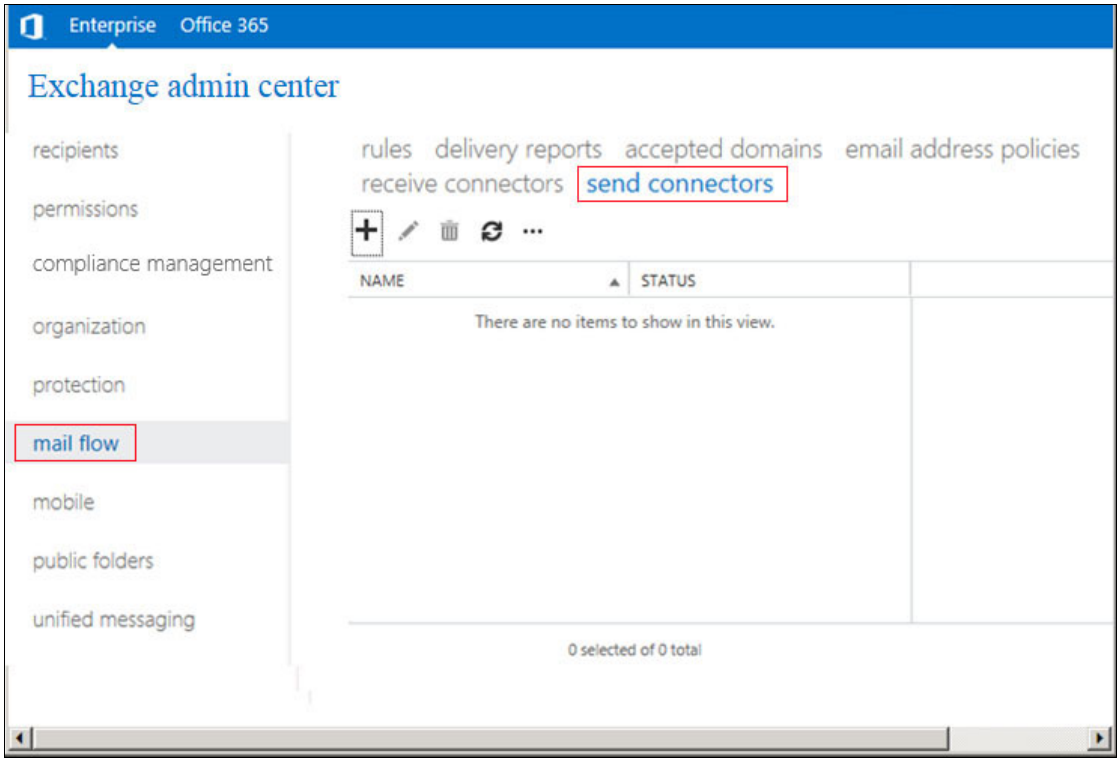
Option 2. Manually Configure Journaling

Remote Domain

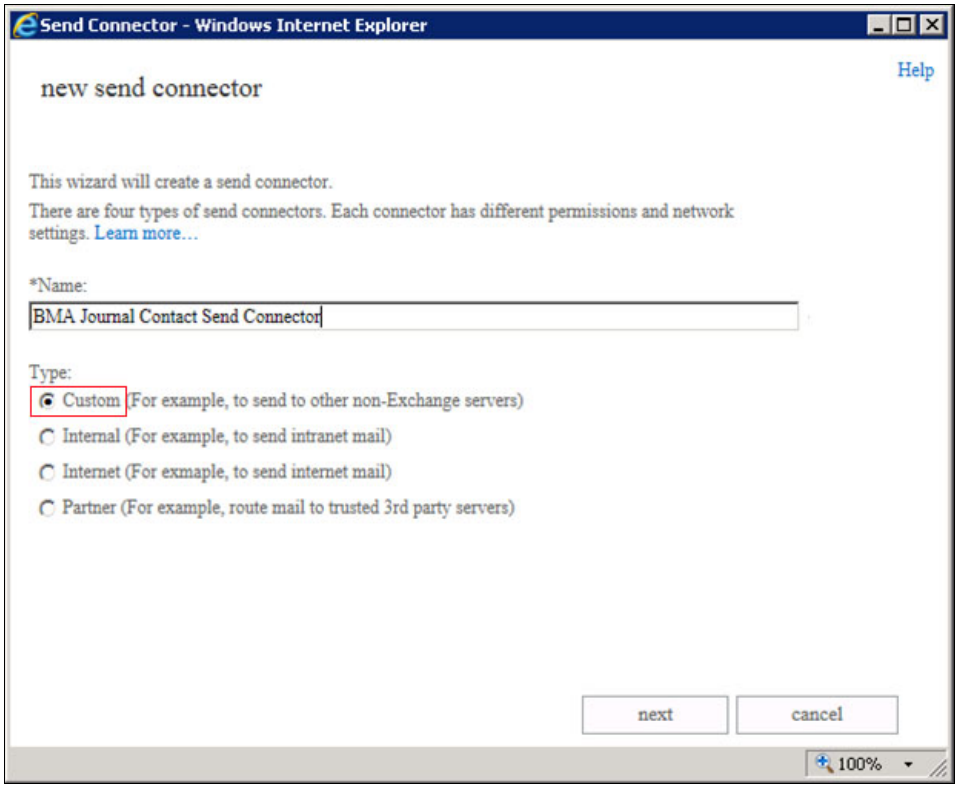
In previous versions of Exchange Server, the Exchange Management Console was used to create a Remote Domain; in Exchange Server 2013+ the ECP/EAC has no analogous functionality so you must use PowerShell to create the Remote Domain.

Use your region-specific MAS hostname, for example:
mas.barracudanetworks.com (US)
mas.ca.barracudanetworks.com (Canada)
mas.uk.barracudanetworks.com (UK)

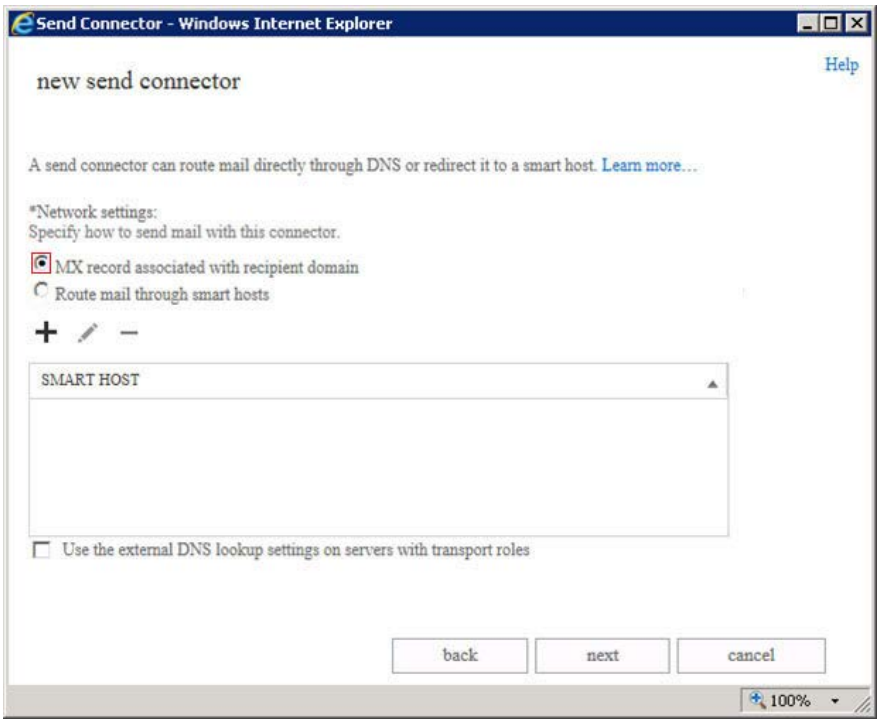
1. Log into your Exchange Server and open the **Exchange Management Shell**.
2. Execute the following command to create the remote domain; this command ensures TNEF encoding is disabled, where *mas.barracudanetworks.com* represents the domain in your journaling address, for example:
   New-RemoteDomain -DomainName *mas.barracudanetworks.com* -Name "Cloud Archiver Domain"
3. Next, execute the following command to enable auto-forwarding:
   Get-RemoteDomain | Where {$_.DomainName -eq "*mas.barracudanetworks.com*"} | Set-RemoteDomain -TNEFEnabled $false -AutoForwardEnabled $true
4. Enter the following command to verify the settings:
   Get-RemoteDomain | Where {$_.DomainName -eq "*mas.barracudanetworks.com*"} |Format-table Name, DomainName, TNEFEnabled, AutoForwardEnabled
5. To route journaled mail that is sent to the contact to the Barracuda Cloud Archiving Service, use the following steps to create a Send Connector for the Remote Domain:
6. Log into the EAC and click **mail flow** in the left pane, select **send connectors** at the top of the page, and then click the **+** symbol to create a new send connector:



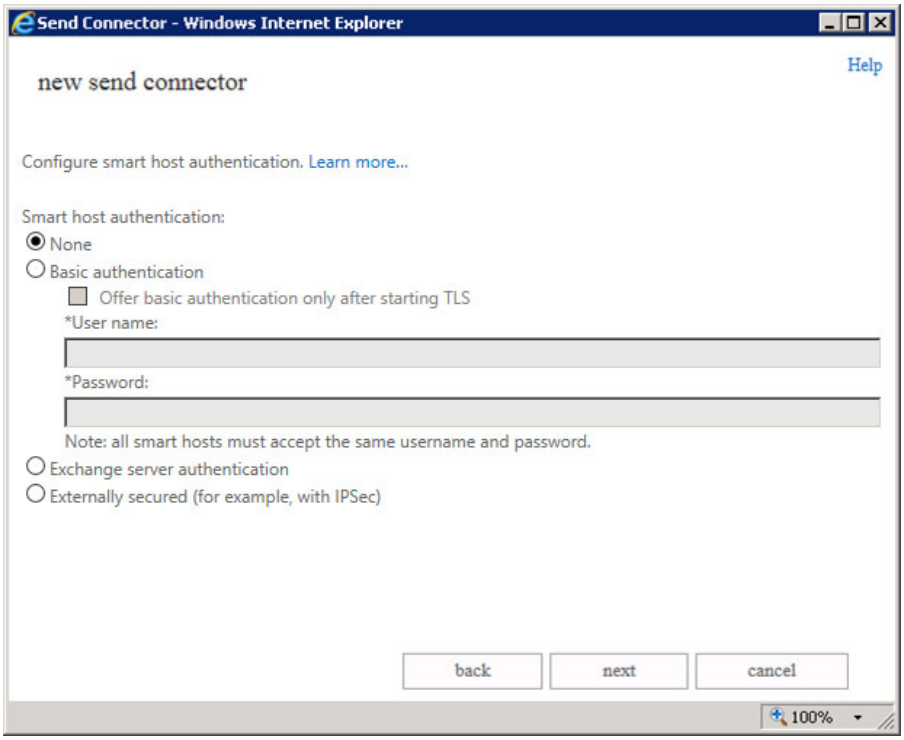
7. In the **Name** field, enter a name for the connector, and in the **Type** section, select **Custom**:



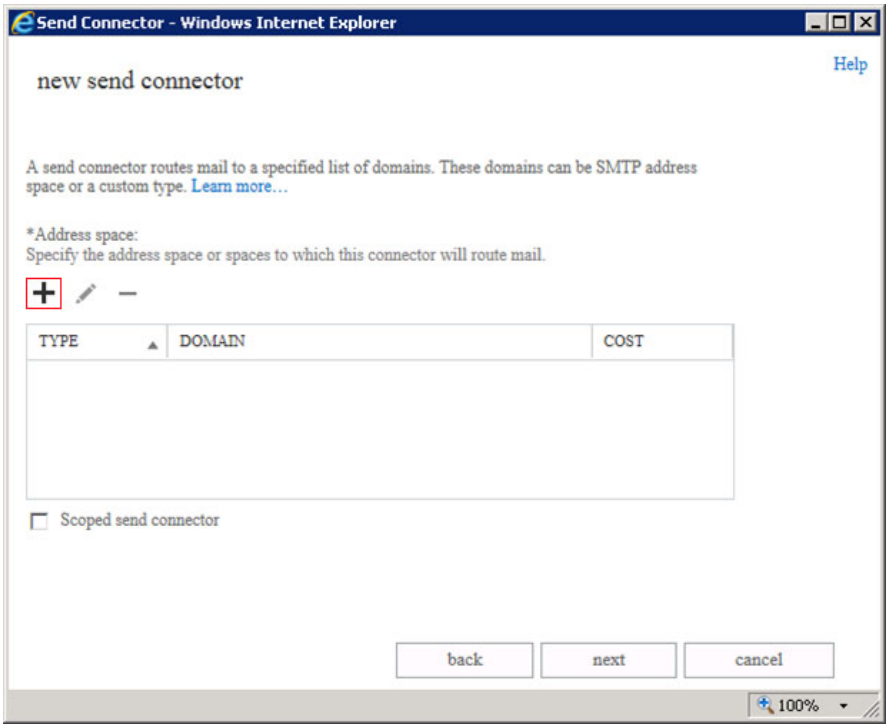
8. Click **next**. In the **Network settings** page, select **MX record associated with recipient domain**:



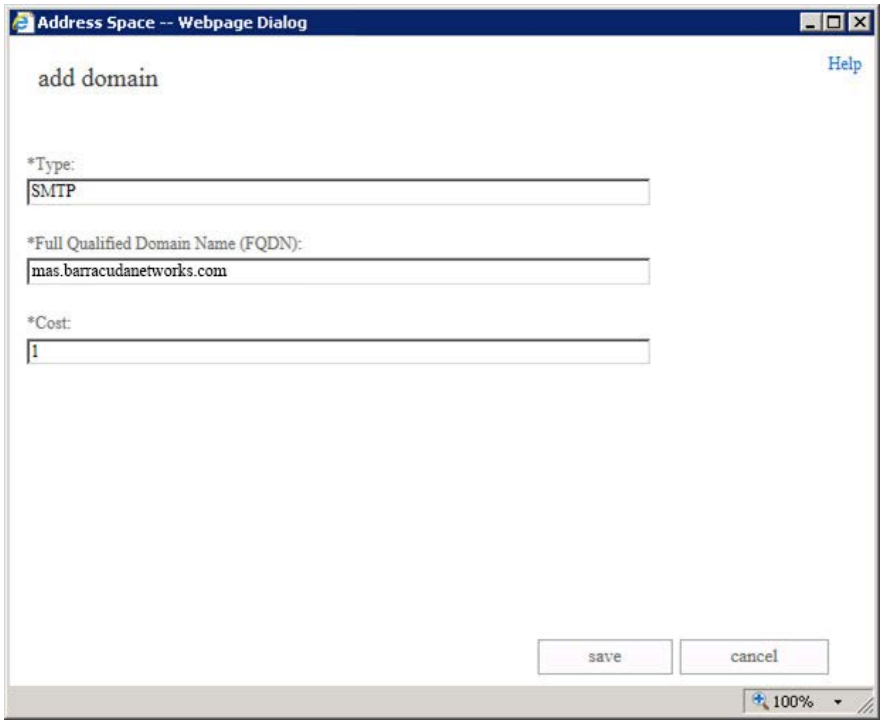
9. Click **next**. In the **Smart host authentication** page, because authentication is not used on the smart host connection to the Barracuda Cloud Archiving Service, no changes are necessary; click **next**:



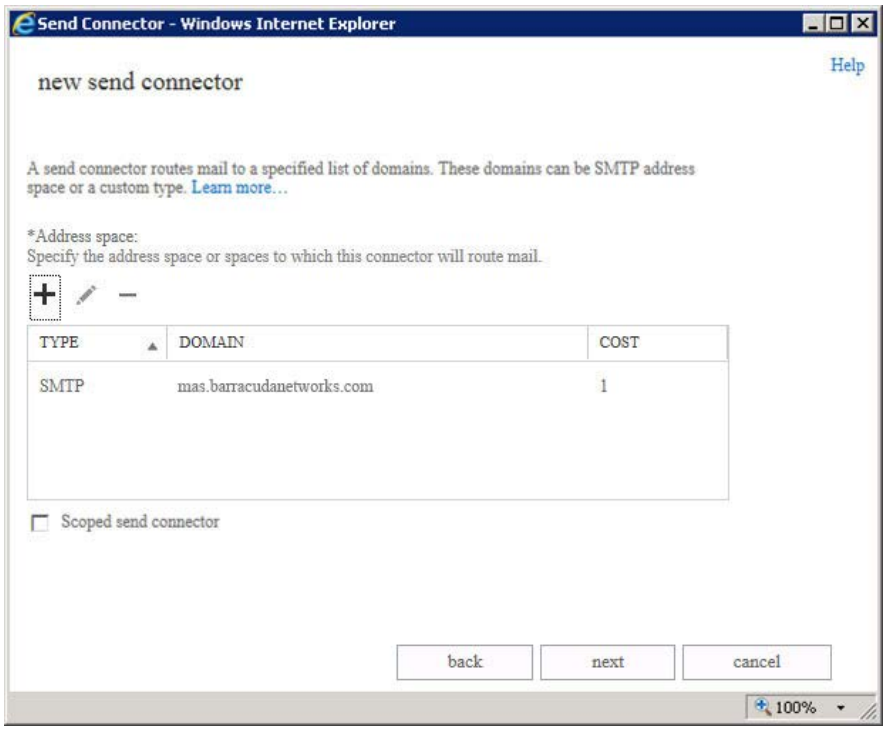
10. In the **Address space** section, click the **+** symbol:



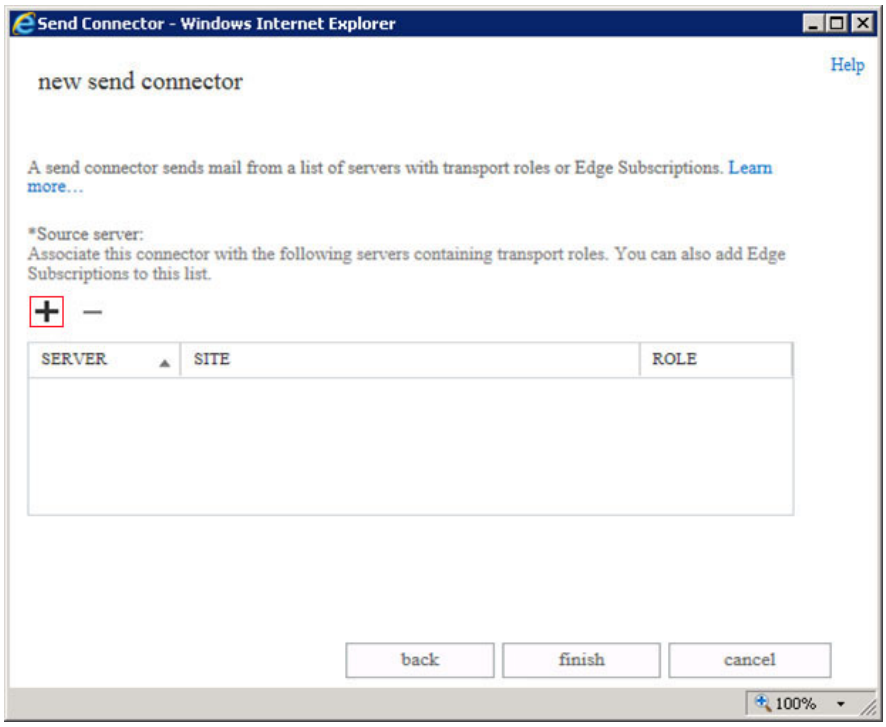
11. In the **Address Space** page, enter the domain portion (region specific) of your journaling address in the **FQDN** text field. Leave **Type SMTP & Cost 1** as is:



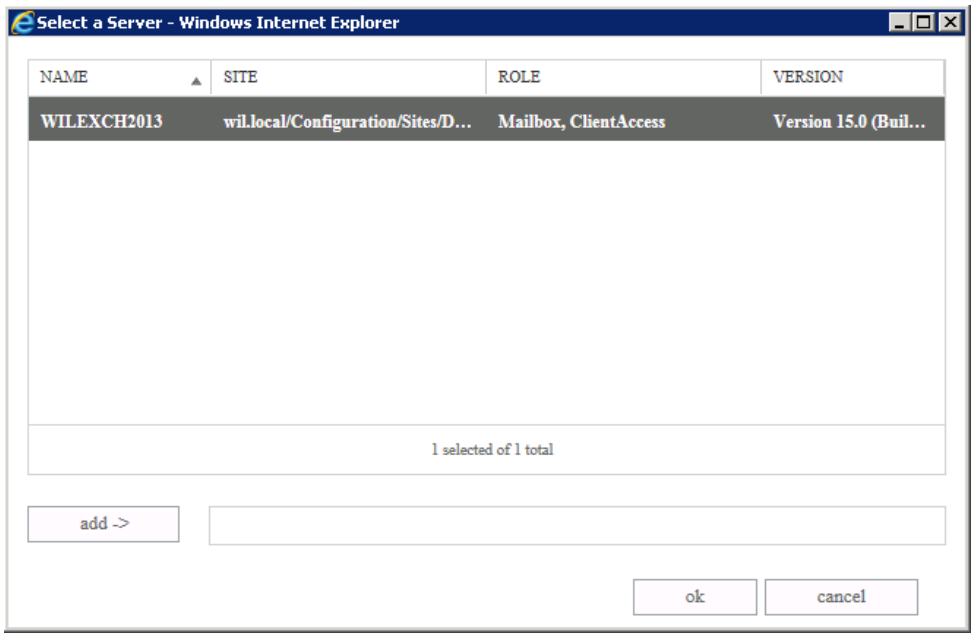
12. The domain is added to the **Address space** list:



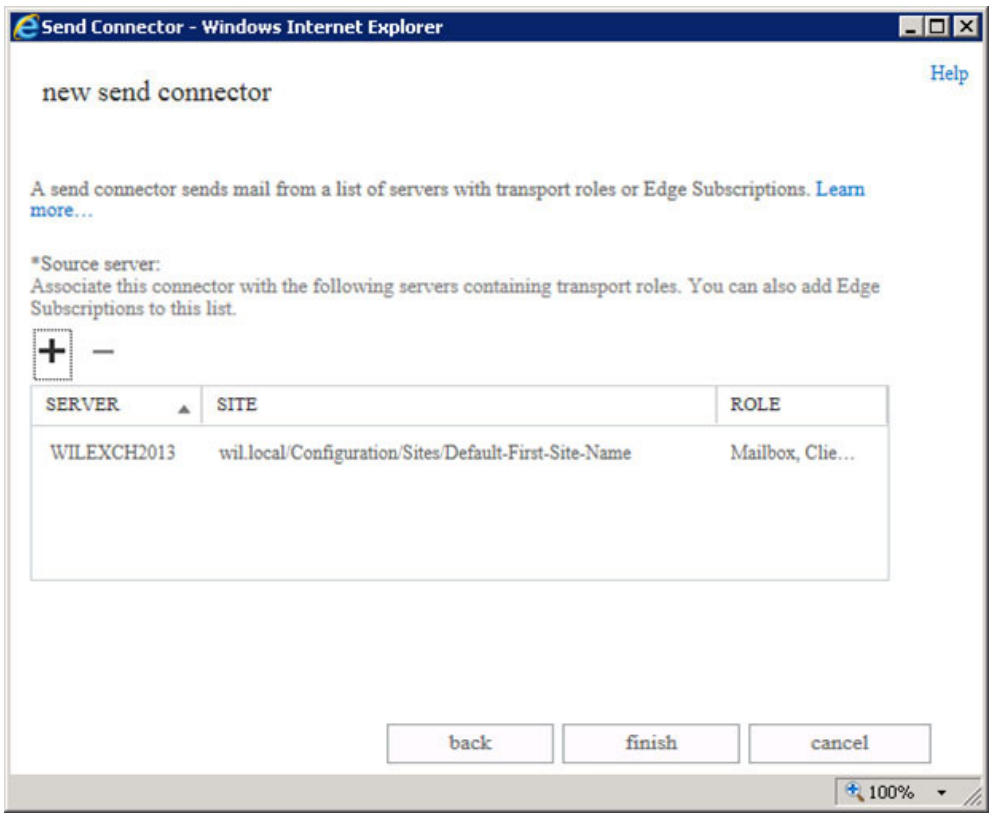
13. Click **next**. In the **Source server** section, click the **+** symbol:



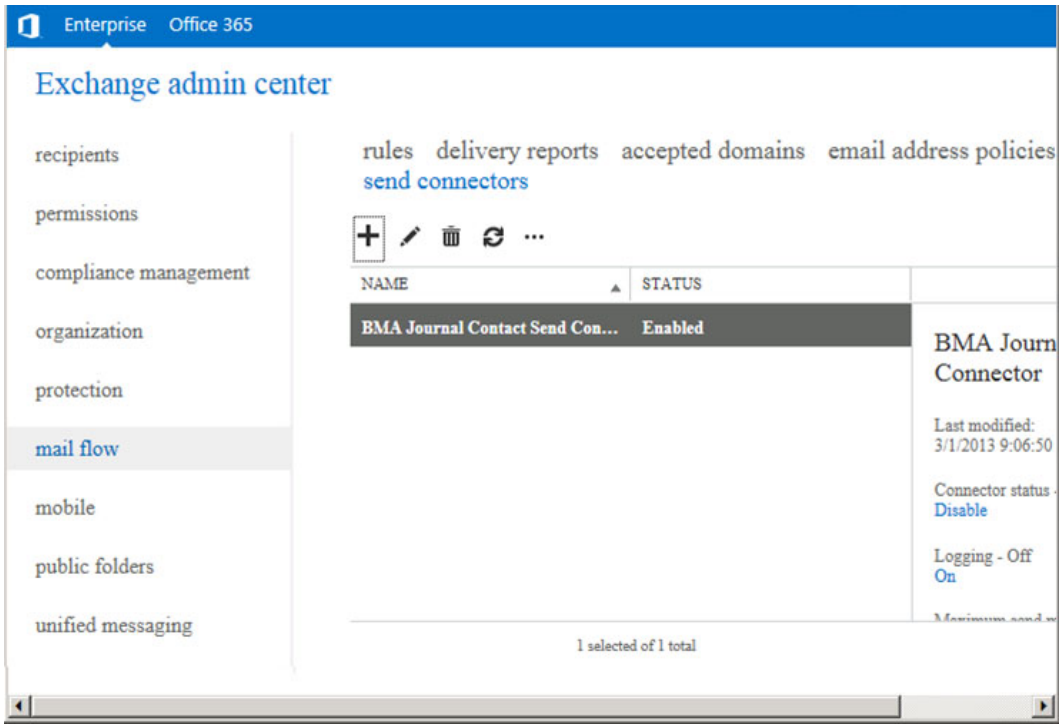
14. Verify all of the appropriate Exchange Servers are listed; click **add** to add additional servers:



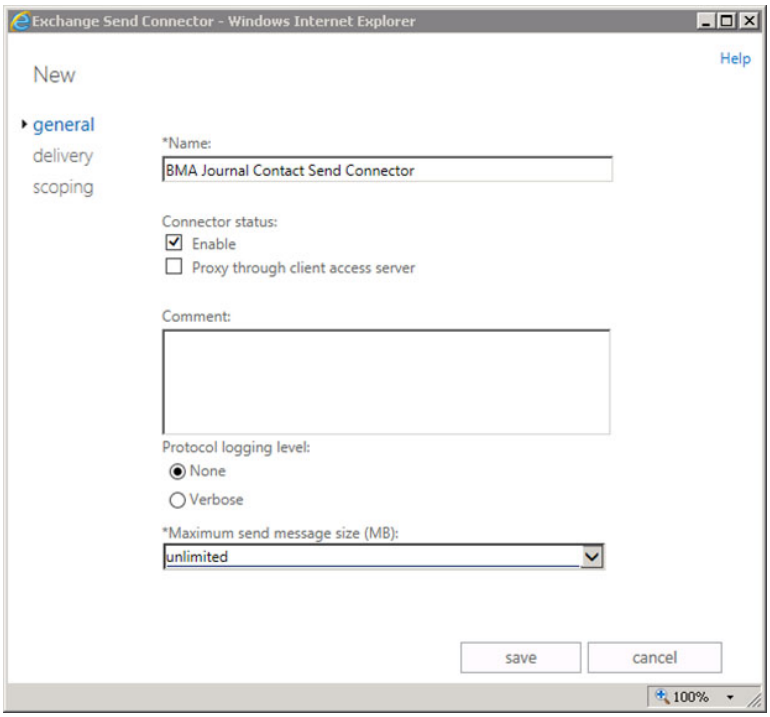
15. Click **OK**. In the **Source server** page, the selected servers display:



16. Click **finish**. The new send connector displays as **Enabled** in the **send connectors** list:



17. Click the **Edit** icon to edit the Send Connector properties. From the **Maximum send message size (MB)** drop-down list, select **unlimited**, and then click **save**:



Once you complete Option 1 or Option 2, the configuration is now complete and journaled mail is forwarded to the Barracuda Cloud Archiving Service. Log in and go to the **Basic > Search** page in the web interface to verify that new mail is being processed. Note that it may take up to 30 minutes before journaled mail is available in the search results.

Barracuda Networks recommends hiding the Journal Contact–as well as any mailbox set up for undeliverable journal reports–from the GAL so that mail is not sent directly to these accounts.

Configure Exchange Integration

In addition to journaling mail, we offer the ability to integrate your Exchange Online DB with the archiver service. The steps below will show you how to configure 3 actions: a historical import of your Exchange Online 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 a Service New Account

Use the following steps to set the permissions on Exchange 2013 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

Continue with Microsoft Exchange Server Operations based on your Exchange Server:

Assign Permissions

Use the following steps to assign permissions to the new service account:

1. Log in to the Exchange Server as the administrator, and open the **Exchange Management Shell**.
2. At the command prompt, type the following command:
   New-ManagementRoleAssignment -Name:BarracudaMessageArchiver -

Role:ApplicationImpersonation -User: *PolicyAdmin*
Where *PolicyAdmin* represents the new service account name.

Disable Throttling Policy Enforcement

Use the following steps to disable throttling policy enforcement on the new account, replacing *PolicyAdmin* with the new account name:

1. Log in to the Exchange Server as the administrator, and open the **Exchange Management Shell**.
2. At the command prompt, type the following command to create a new throttling policy:
   New-ThrottlingPolicy *PolicyAdmin*
3. Press **Enter**. Type the following command to set the throttling policy:
   Set-ThrottlingPolicy *PolicyAdmin* -RCAMaxConcurrency Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
4. Press **Enter**. type the following command to disable policy enforcement:
   Set-Mailbox "*PolicyAdmin*" -ThrottlingPolicy *PolicyAdmin*
5. Press **Enter**.

Historical Import of Exchange Server Database

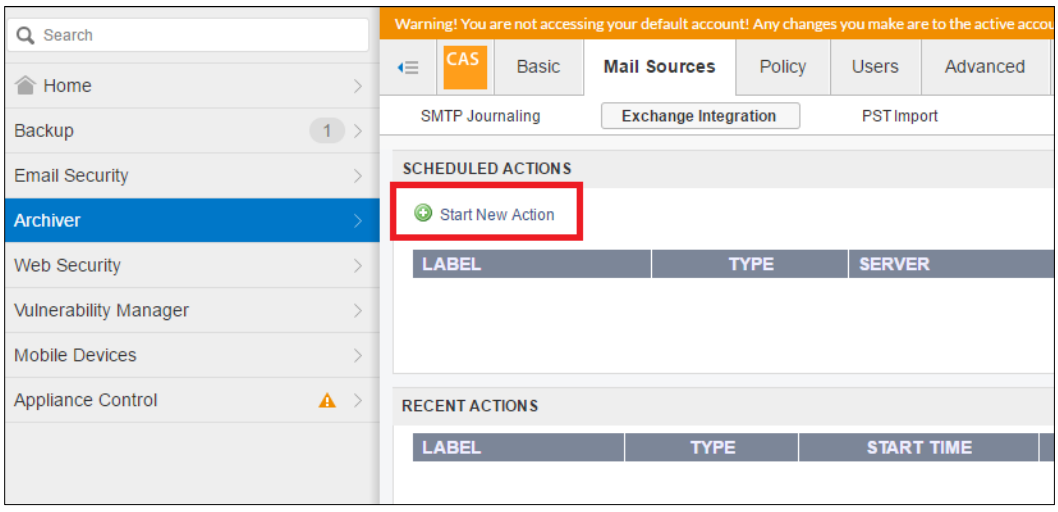
Add New Server

Configure a new Exchange Server:

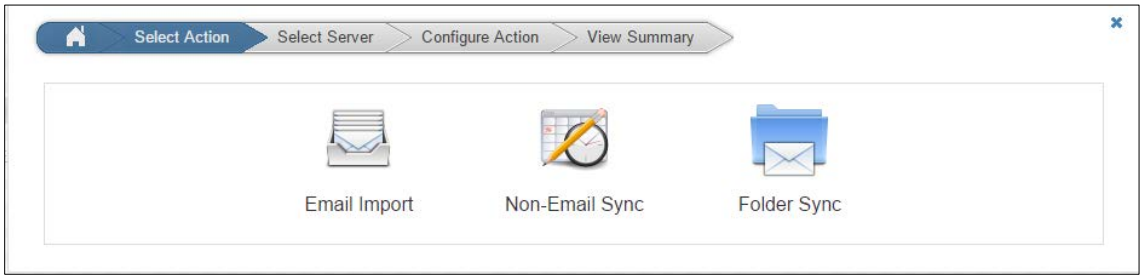
Automatically Discover Server Settings for Email Import

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.*

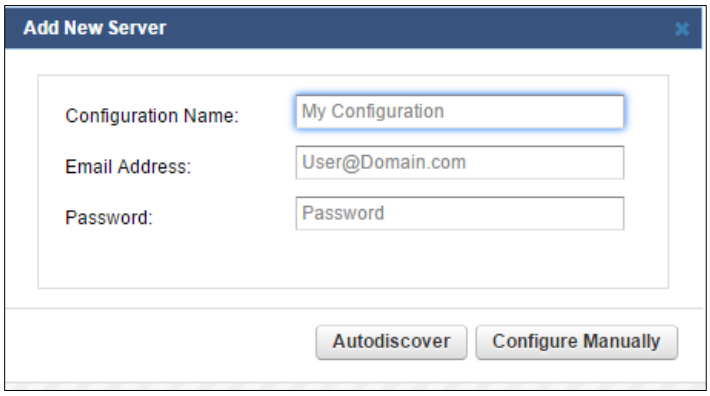
1. Log in to the Barracuda Cloud Archiving Service as the admin**,** and go to **MAIL SOURCES > Exchange Integration.**
2. Click **Start New Action.**



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



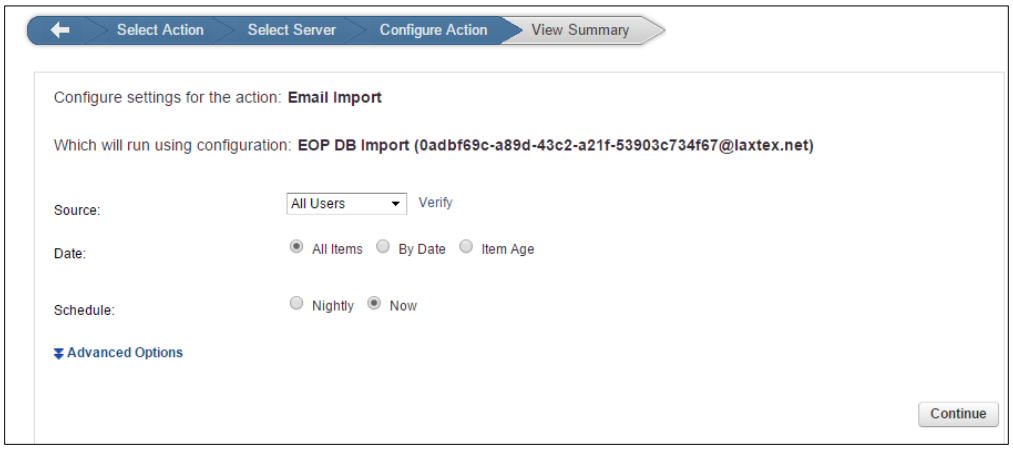
4. In the **Select Server** page, click **Add New Server.**



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.

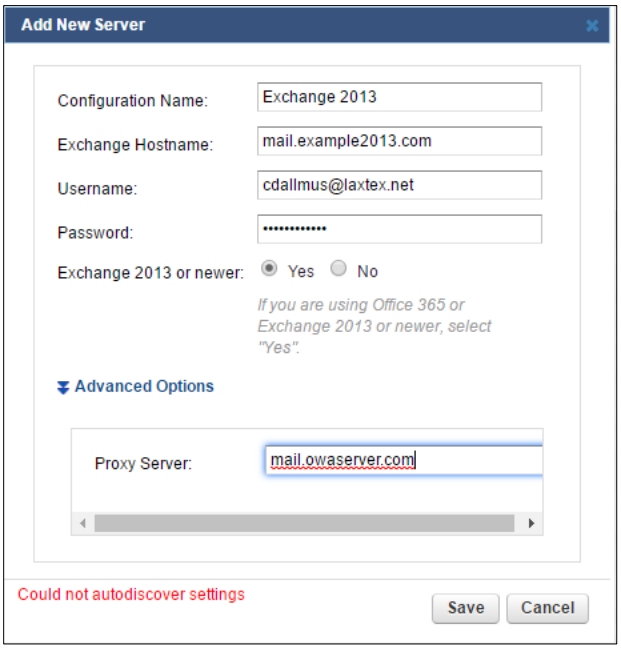
6. When the server details display**, click** Save**.**
7. The server is added to the Server table**. Click** Continue**.**
8. In the Configure Action page**,** select **All Users** from the drop-down menu, and specify the desired Date and Schedule settings**. Click** Continue**.**



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

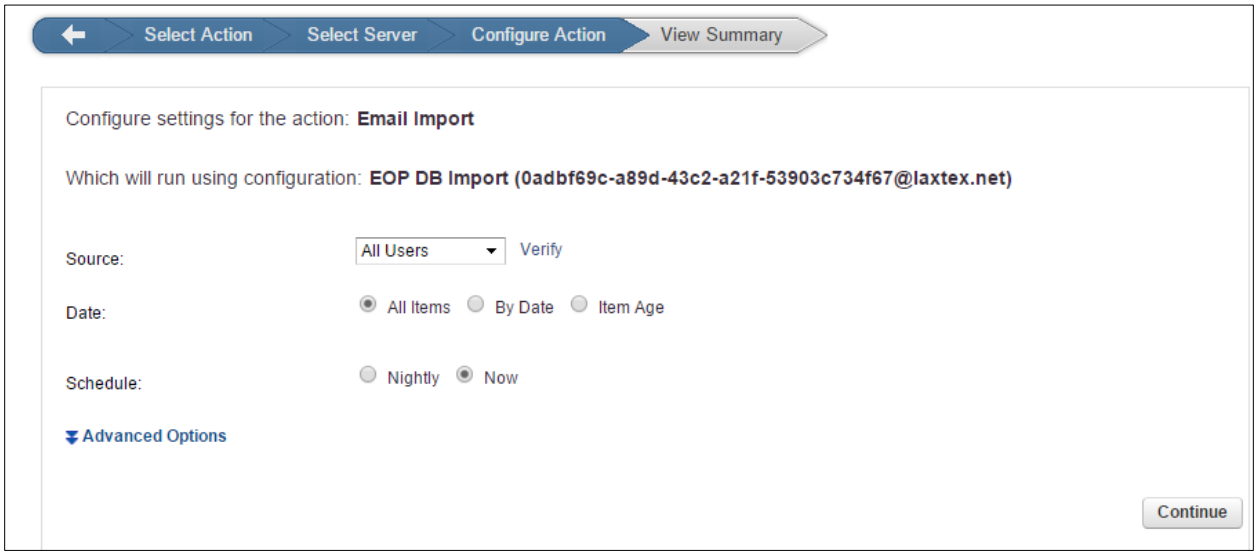
Manually Configure Server Settings for Email Import

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



1. In the View Summary page, select **All Users** from the Source drop-down menu.

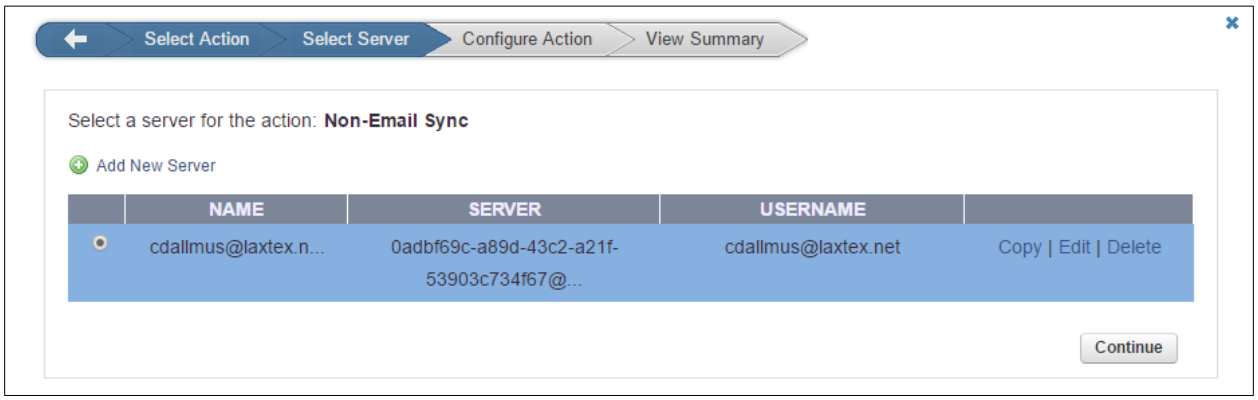
2. In the schedule section, enter the desired Date and Select **Now**. Click **Continue**.



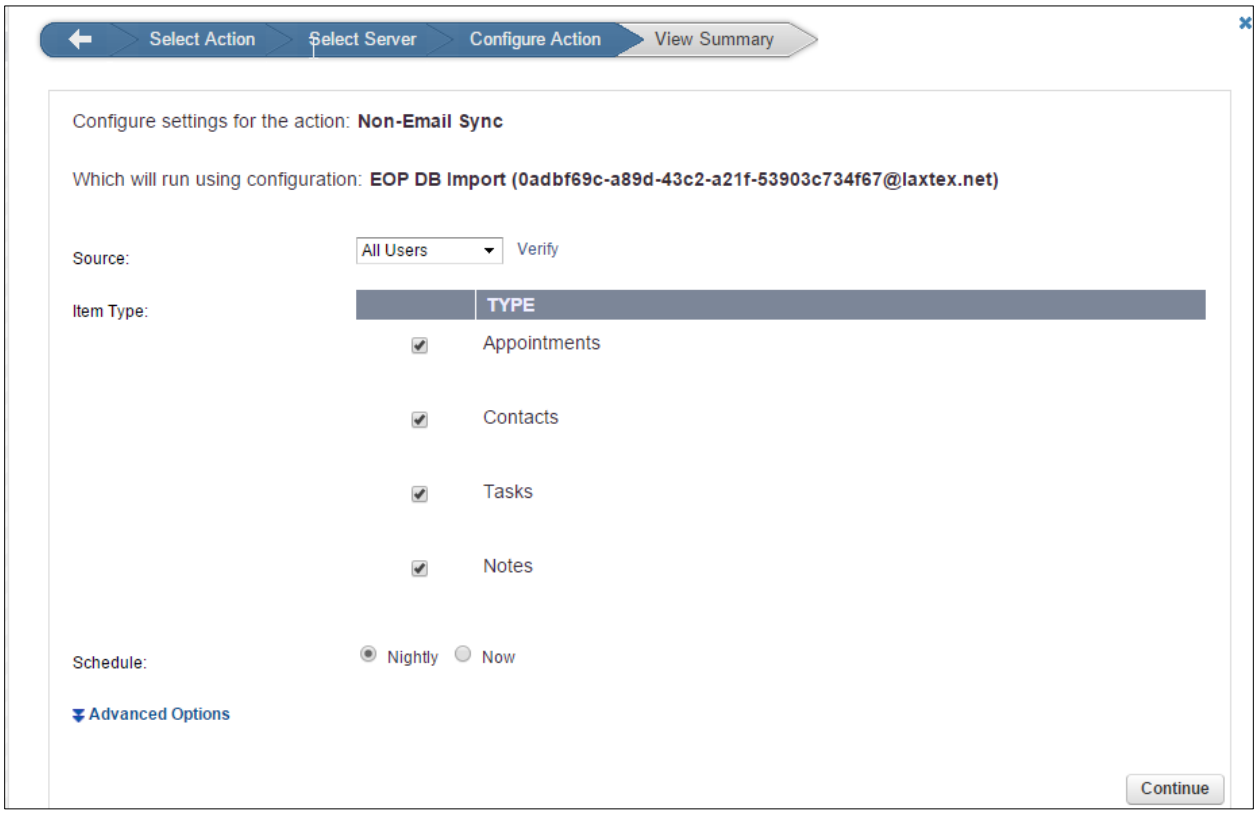
3. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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.**
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.



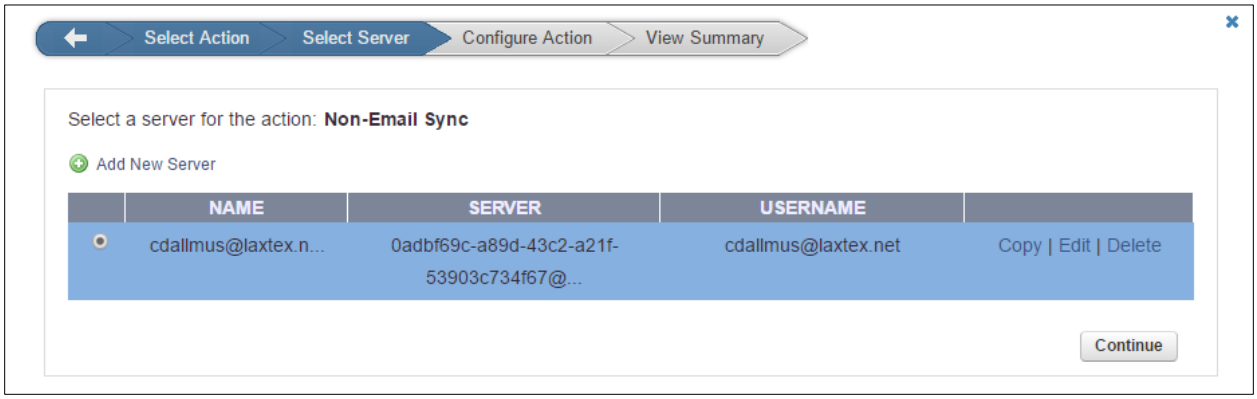
4. In the Configure Action page, Click **Continue**.
5. In the View Summary page, select **All Users** from the Source drop-down menu. For item type, check or de-check any of the items you would like to synchronize. For schedule, select **Nightly**. Then click **Continue**.



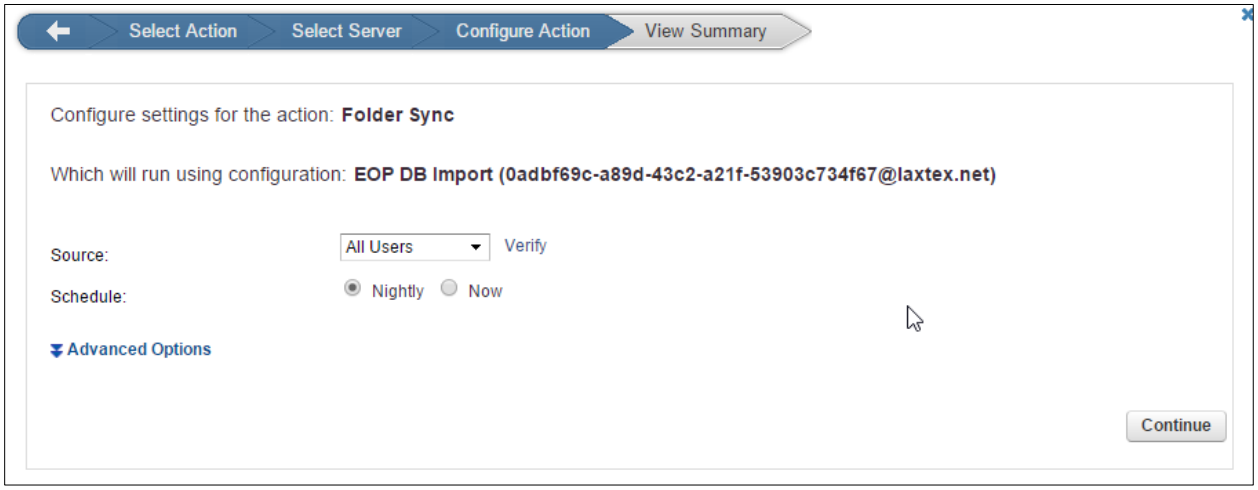
6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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**.

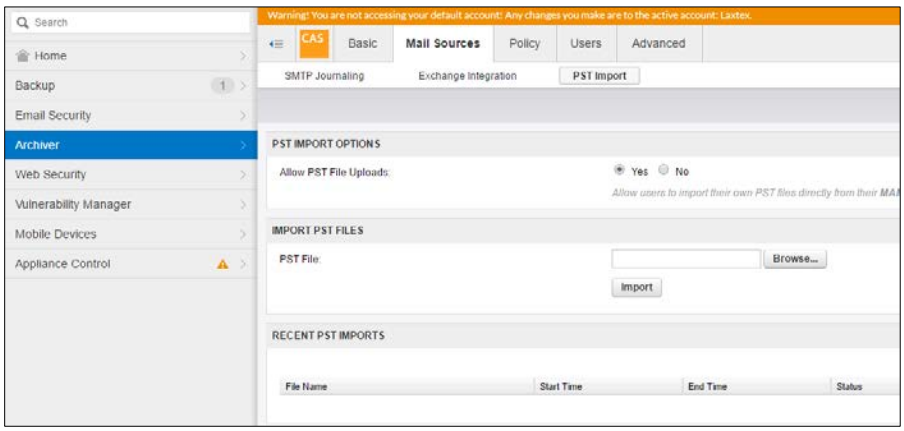


6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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.

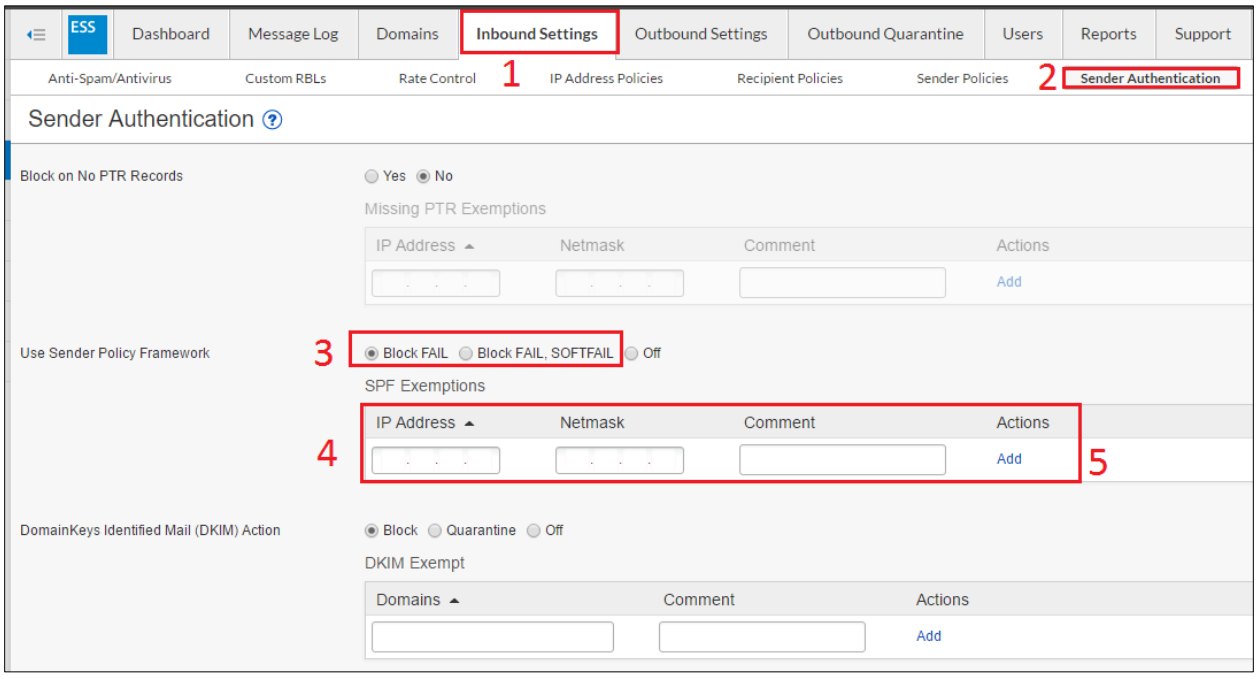
Appendix 1 – How to exempt or disable SPF checking for the Barracuda ESS service

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 range 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 – Adding a receive connector in Exchange 2010

1. Open the Exchange Management Console.
2. Expand **Server Configuration**.
3. Click on **Hub Transport**.
4. Select the server name on the right hand side.
5. In the Toolbox Actions. Click on **New Receive Connector**.
6. Enter "**BESS Inbound Connector**" in the **Name field.**
7. For the intended use of this send connector select **Custom.**
8. On the **Local network settings** page, do the following:
   - Specify the IP addresses and port numbers on which this Receive connector listens for incoming mail. The **Local network settings** page appears only if you selected a usage type of **Custom**, **Partner**, or **Internet** in step 3. By default, all available local IP addresses are listed.
9. On the **Remote network settings** page, Click **Add IP and Mask** to add the Barracuda Email Security Service IP range [**64.235.144.0/20** {/20= 255.255.240.0}] & [**209.222.80.0/21** {/21= 255.255.248.0}]from which the connector accepts incoming connections. Then click **Next.**
10. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Receive connector by using the settings in the configuration summary, click **New**.
11. On the **Completion** page, click **Finish**.

Appendix 3 – Define an accepted domain in Exchange 2010

1. Open the Exchange Management Console. Perform one of the following steps:
   - To create an accepted domain on a computer that has the Edge Transport server role installed, on that computer, in the console tree, select **Edge Transport**, and then in the work pane, click the **Accepted Domains** tab.
   - To create an accepted domain on a computer that has the Hub Transport server role installed, on that computer, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Accepted Domains** tab.
2. In the action pane, click **New Accepted Domain**. The New Accepted Domain wizard appears.
3. On the **New Accepted Domain** page, complete the following fields:
   - Enter "**Barracuda Email Security Service**" in the **Name** field:
   - Enter "ess.barracudanetworks.com" in the **Accepted Domain** field
4. After you complete these fields on the **New Accepted Domain** page, select **External Relay Domain** to set the accepted domain type
   - This option is for relaying e-mail messages to an e-mail server outside the Exchange organization
5. Click **New** to create the new accepted domain.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.