Barracuda Essentials for Office365

Services Configuration

Abstract
The following is the walkthrough procedure for configuring Barracuda Essentials & its underlying services to protect your Office365 environment

Intronis

Table of Contents

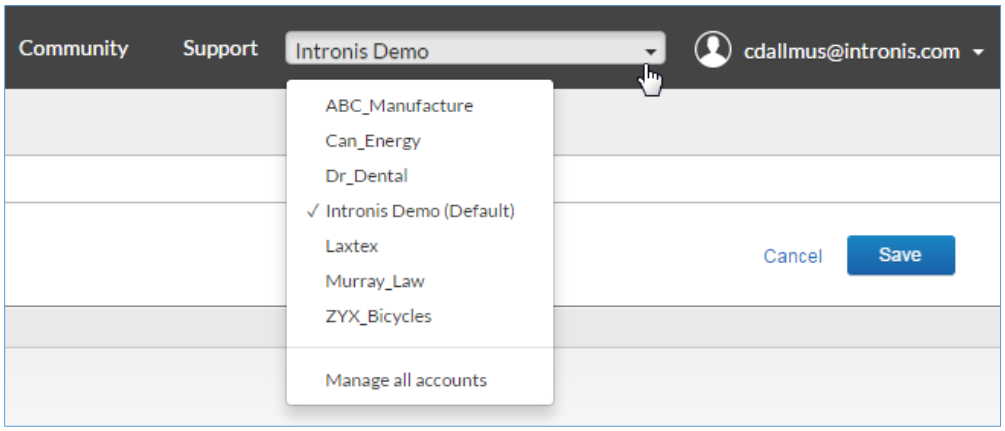
Understanding the Barracuda Cloud Control (BCC) as an MSP

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.

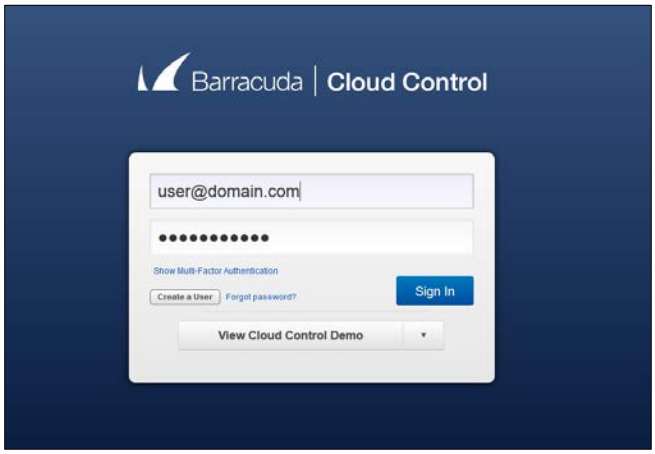
- **Access & Credentials to** https://login.barracuda.com **(Barracuda Cloud Control or BCC)** – The username is contained in the provisioning activation email sent from Intronis. You can manually reset your password directly in the BCC portal using the 'forgot password' link.
- **Customer's domain and Office365 mail server**
    - **Please note**: if you do not know your customers domain or mail server you can find it by referencing Appendix 1.
- **Access & Credentials to customer's DNS Management Console –**You will need the customer's credentials to access your customer's domain settings. [Please note changes to DNS may take up to 24 hours to propagation].
- **Access & Credentials to Office365 Admin Center –** You will need the customer's credentials to access their Office365 Admin Center https://portal.office365.com
- Any **email address** on customer's domain.

Inbound Scanning Setup

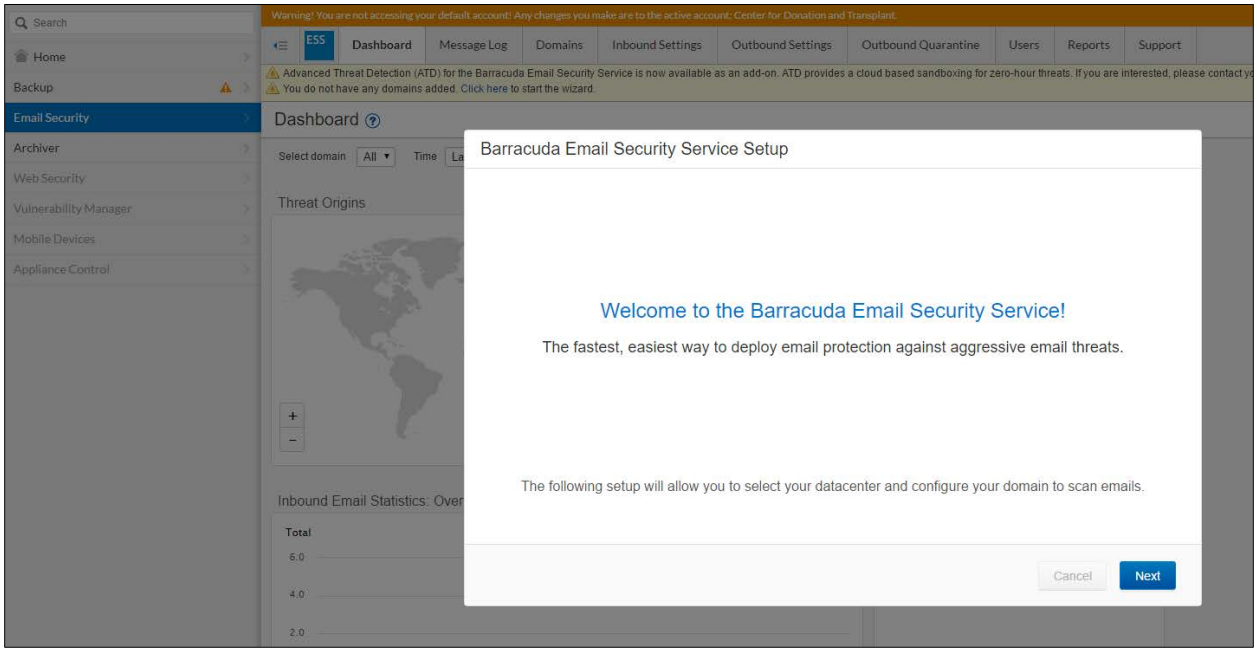
During this step we will configure the customer's primary domain for BESS. This will be done using the BESS wizard. You will want to have the client's domain & mail server information for this step.

Add a Domain to Barracuda Cloud Control

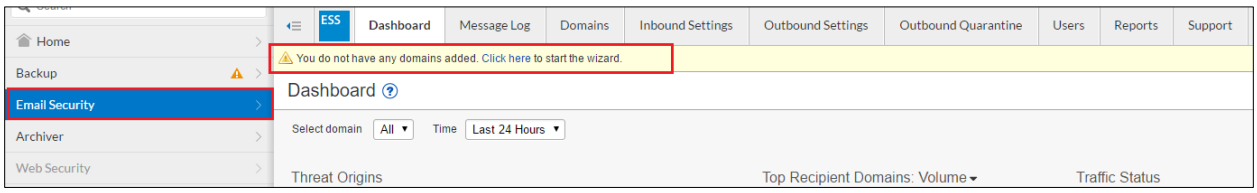
1. **Login** to the BCC (https://login.barracuda.com) console. Please note that if you've never logged into BCC before, you need to click 'forgot password' to create your password.



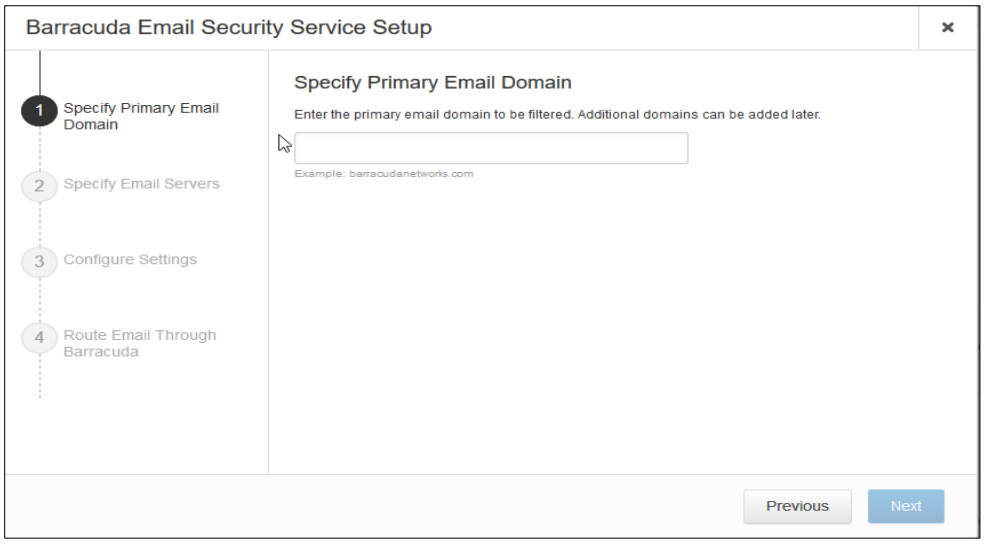
2. Click on **Email Security** from the left hand menu.
3. If this is your first time logging into a customer's Email Security service, you will be prompted with the wizard automatically:



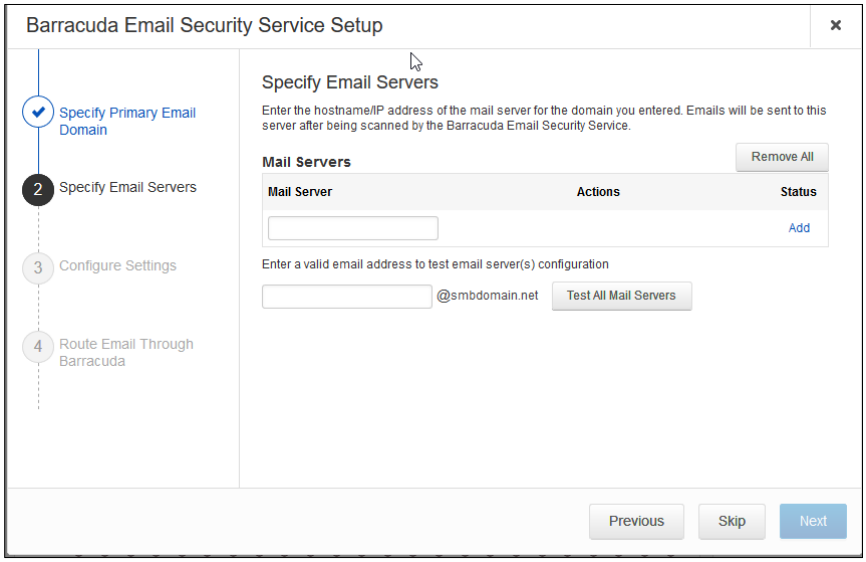
4. If you've already logged into their service before, but you have not yet started the configuration, **click here** to start the wizard:



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



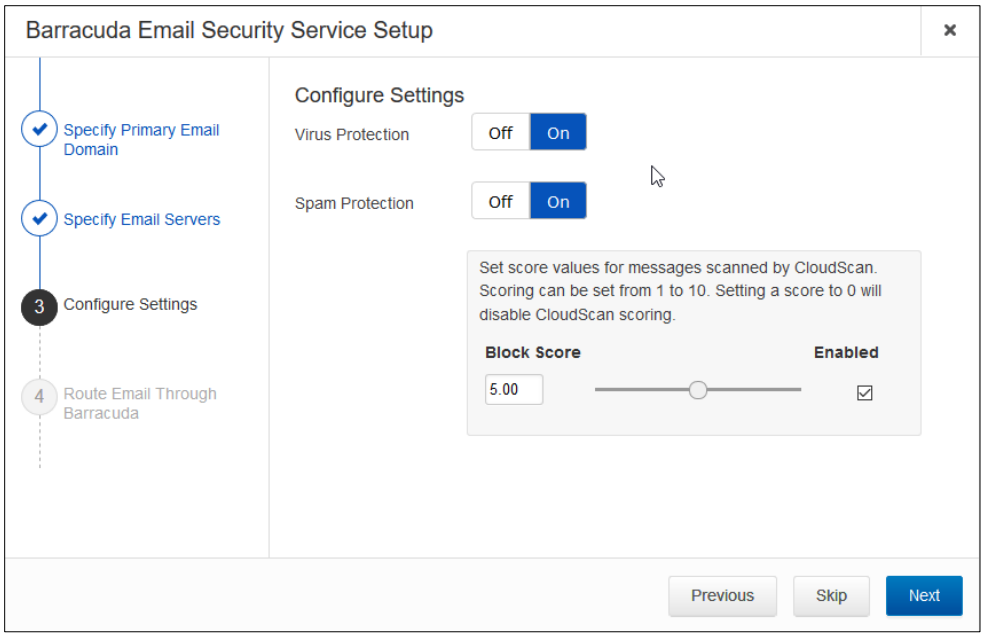
7. Enter the mail server in the space provided, this will be the MX record value from O365 **[<domain>-com.mail.protection.outlook.com**] and click **add**.



8. Enter any email address on the domain, then click **Test All Mail Servers**.
9. Click **Next** to continue with the defaults.

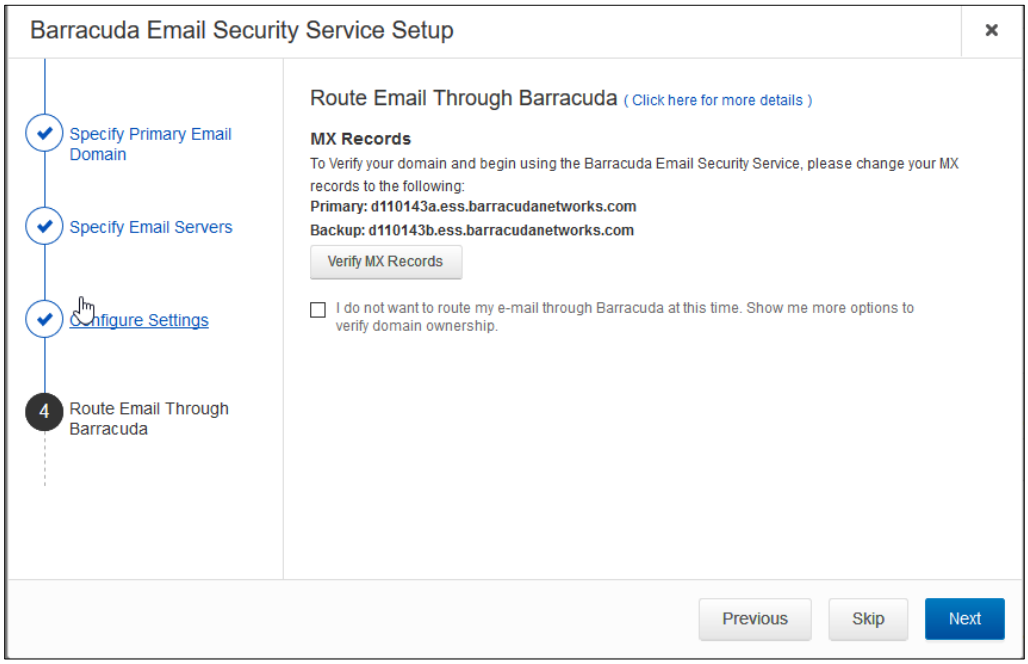
By default Virus & Spam Protection are enabled and the CloudScan Spam Scoring system's block threshold is set to 5. This can be modified later in the **Inbound Settings > Anti-Spam/Antivirus** settings. Leaving Virus Protection enabled directs

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.



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

Add the 2 MX records generated below. Ensure you check with your DNS provider for 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. When you have verified that mail flow is operational through the Barracuda service, please remove the old Office 365 MX record.



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

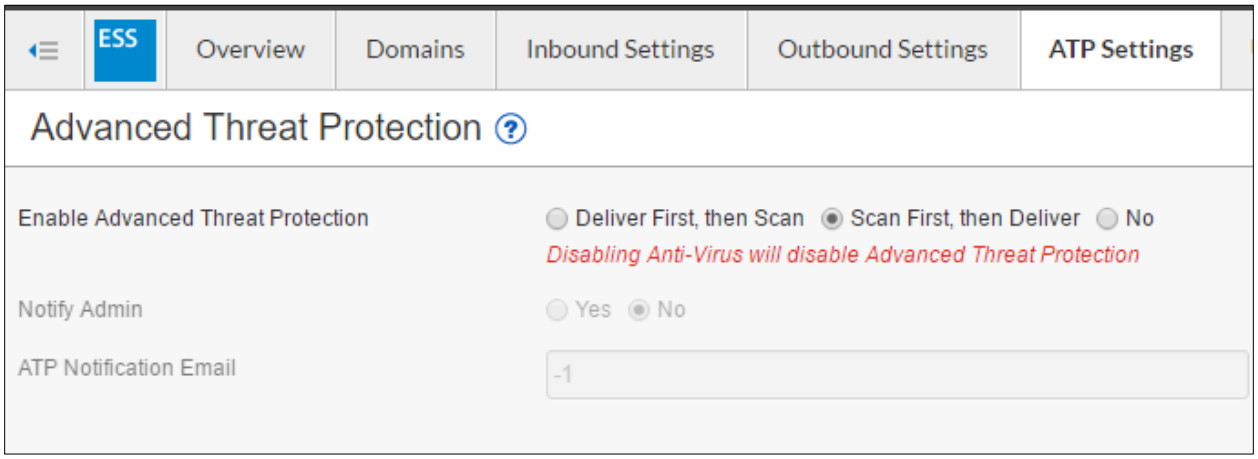
Best Practice Recommendations

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

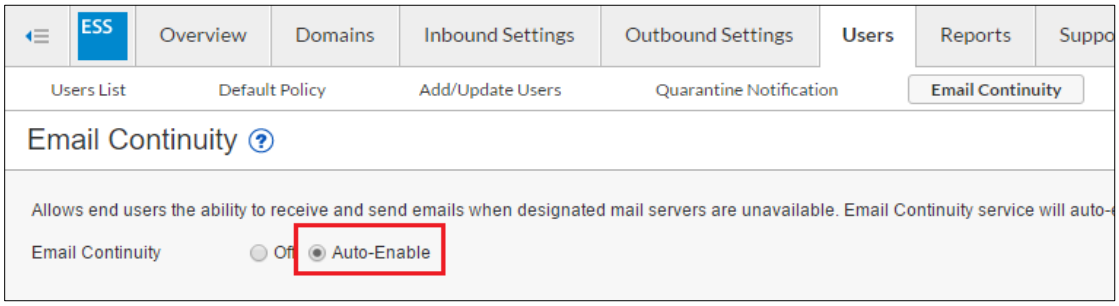
1. Log in to BCC and go to the **Email Security Service.**
2. Navigate to the top menu bar for the **ATP Settings** tab.
3. Set ATP to Scan first, then Deliver.

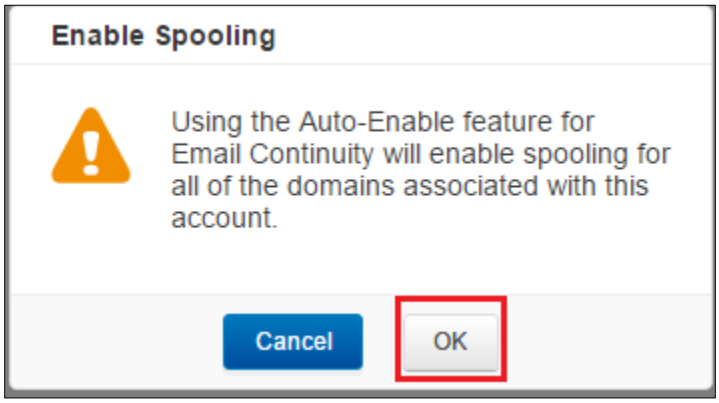


Enable Email Continuity

With this feature enabled, your end users will be able to continue business communications even in the event that Office 365 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.



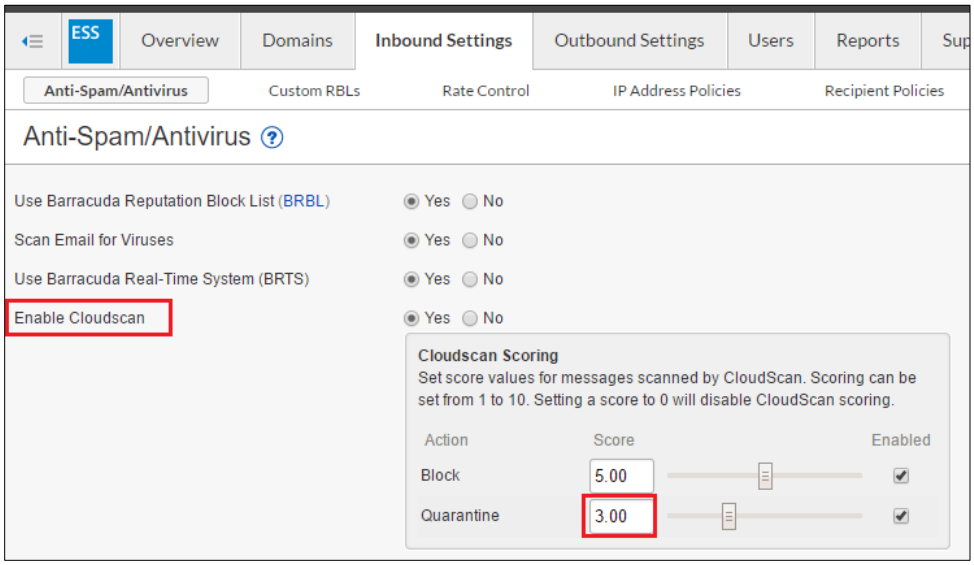


Enable Inbound Quarantine

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.

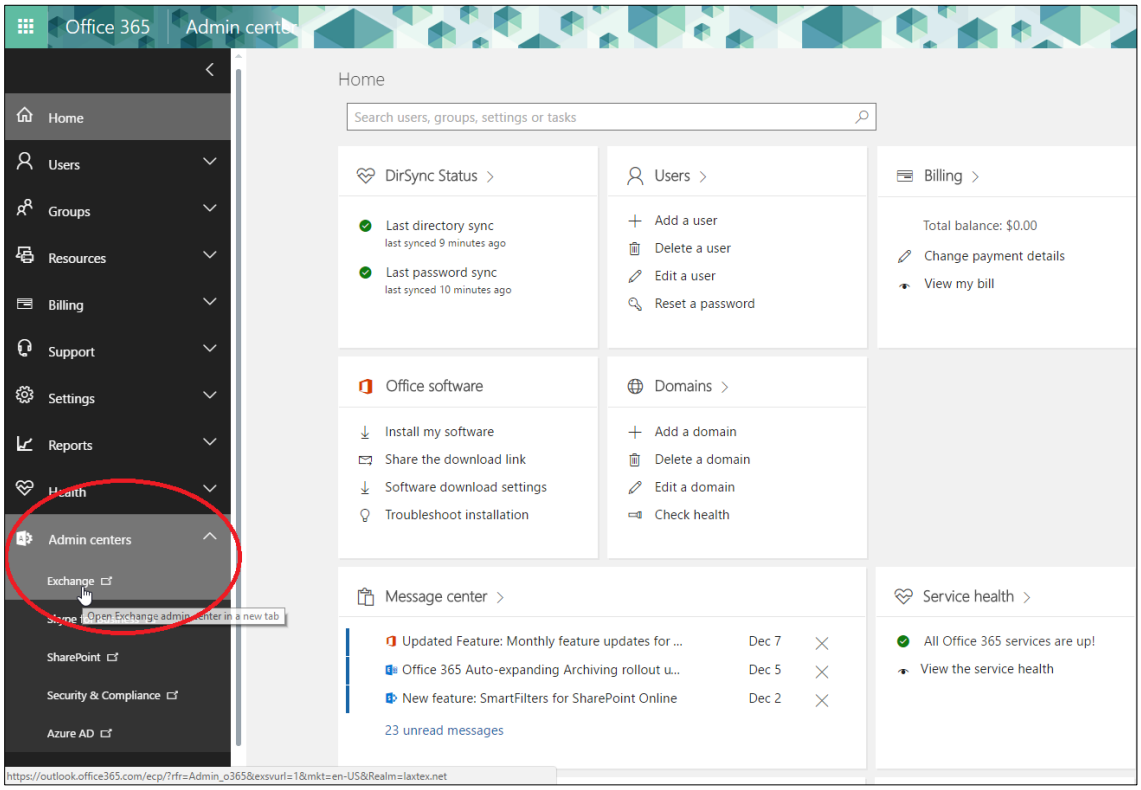
Please note: This is a good starting point as most malicious spam attacks are graded 3 or higher, but may need to be modified later if the policy is too strict or too lenient.



Update Office 365 SPAM Policies

While not required, we recommend defining a rule to bypass the Exchange Online Protection filtering. This will allow messages related to the Barracuda Email Security Service to properly pass through unfiltered, as well as prevent against duplicate quarantine logs.

1. **Log in** to your Office365 portal, or your customer's Office365 portal.
2. Expand **Admin Centers** in the left pane, then click **Exchange**.



3. Click on **Mail flow**, then **Rules**, then click the '**+**' to create a new **Bypass Spam Filtering rule**.
4. Name the rule **BESS Inbound** (1)
5. ***Apply this rule if…** > **The sender** > **IP address is in any of these ranges or exactly matches**
6. Enter **64.235.144.0/20** (click **+** button), then enter **209.222.80.0/21** (click **+** button) then click **OK**.
7. Leave the rest at defaults and click **save**.

Please note: Once the rule is created, click the pencil or edit symbol within the Exchange admin center in order to change the priority to 0 – this ensures that this rule is processed first.

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

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.

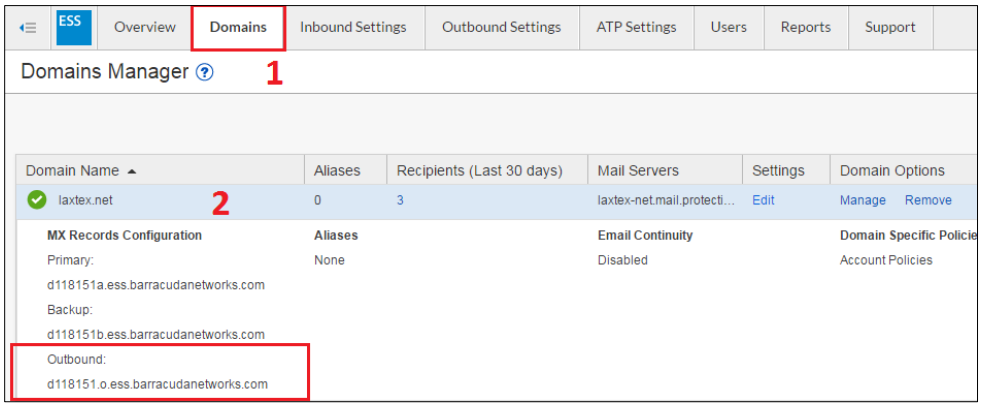
Please Note: To configure Encryption, Outbound Scanning must also be configured.

Send Connector

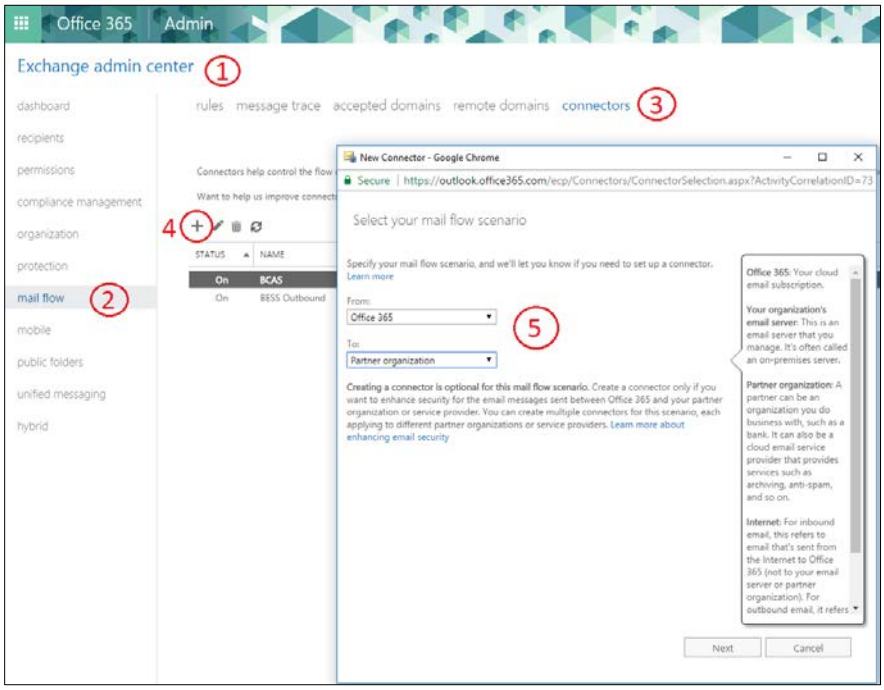
We will add an outbound send connector within Office365 to route outbound mail through a Barracuda smart host.

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)**, click anywhere on the domain **(2)** to expand more details and copy the outbound hostname under the MX records configuration.

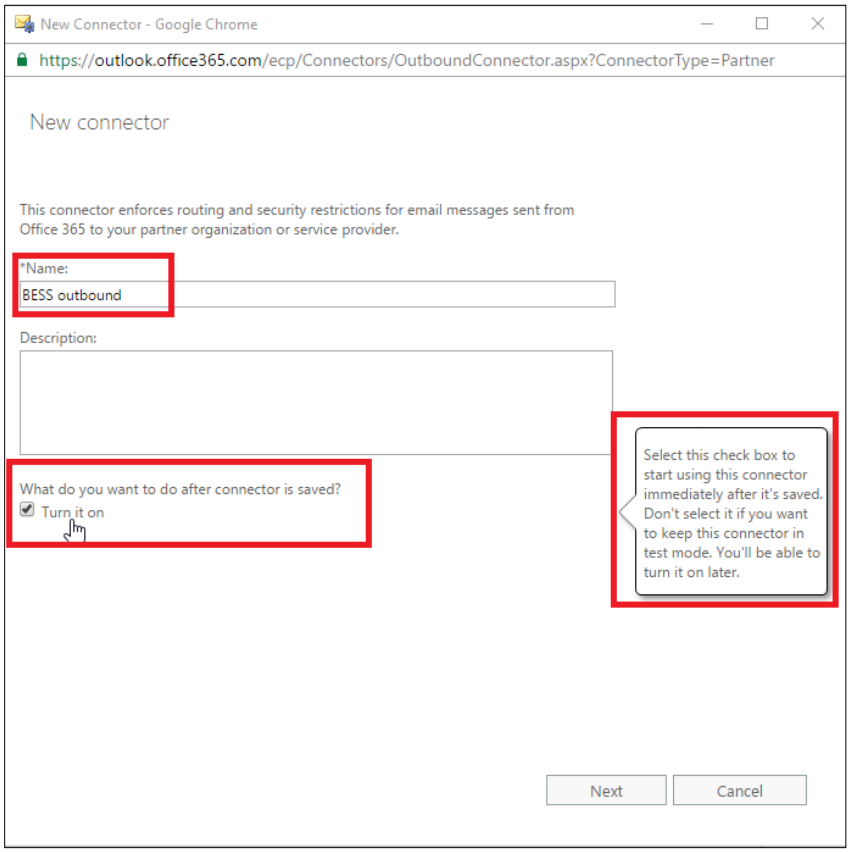


2. Within **Office365** go to **Admin Center for Exchange (1) > Mail flow (2)**, click *Connectors* **(3)**, then click '+' **(4)** to add a new connector.
3. Select from **Office365** to **Partner organization (5).** Click **next**.

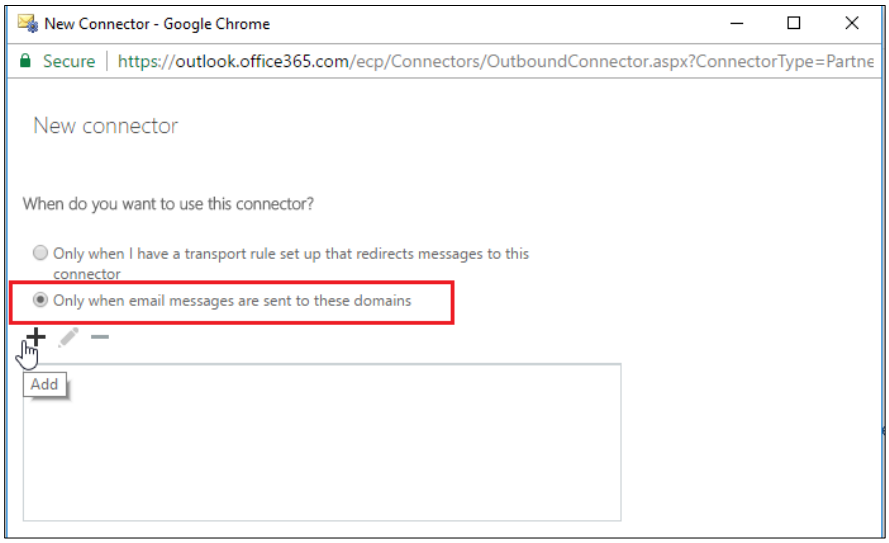


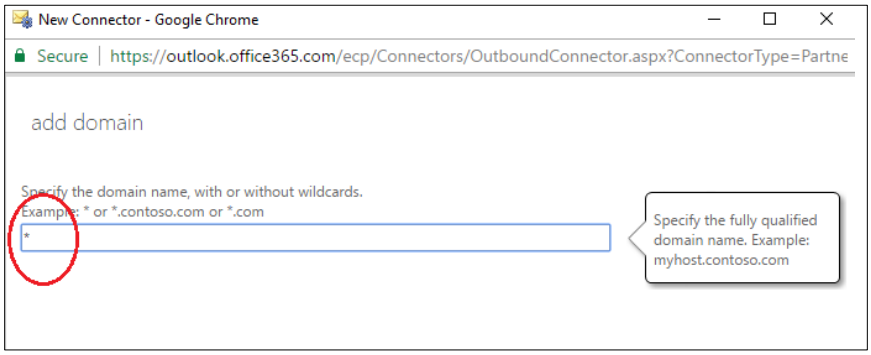
4. Enter the Name, *BESS Outbound*, and optionally enter a description. Click **next**.

   Please note: If you do not wish to route outbound mail through Barracuda at this time, de-check the **Turn it on** box below. This can be enabled later when you are ready to finalize this deployment.

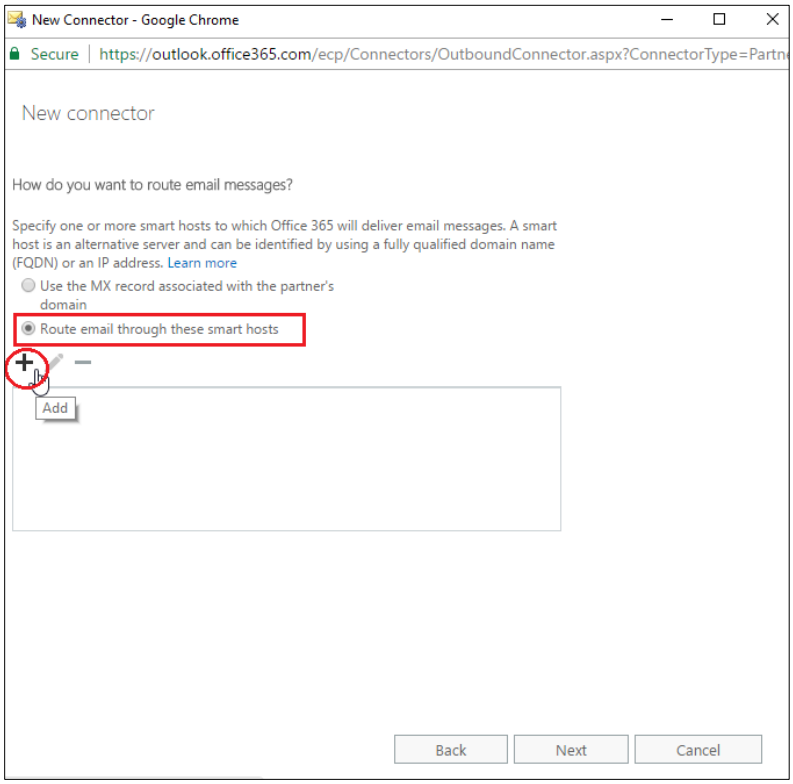


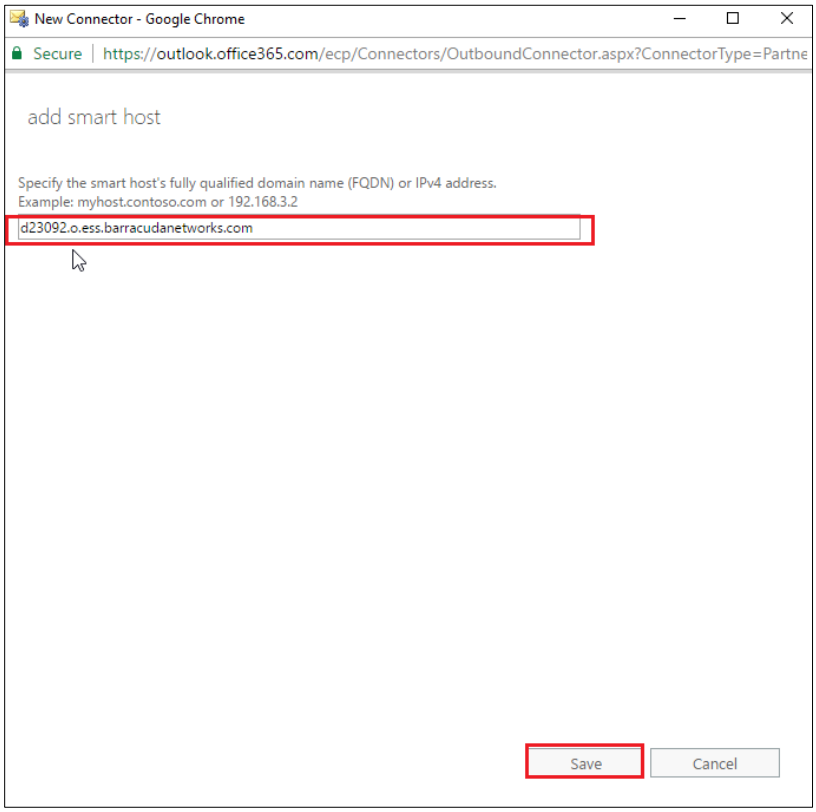
5. **Select** Only when email messages are sent to these domains.
6. Click '**+**' and enter '*'. Click **OK**. Click **next**.



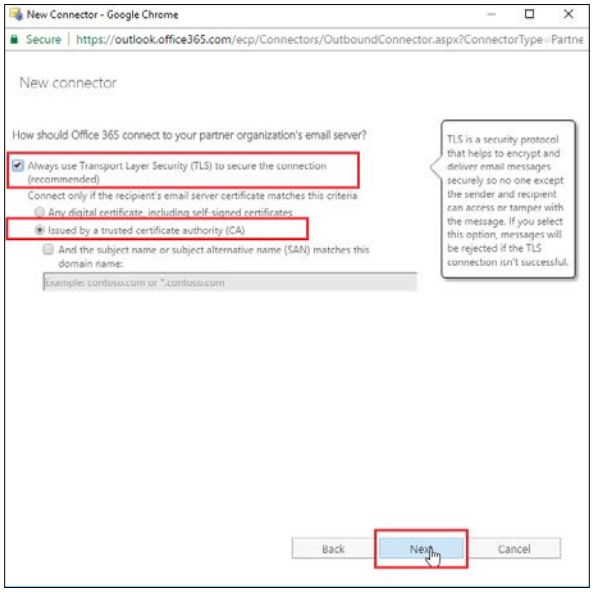


7. **Select** Route email through these smart hosts.
8. Click '+', then **Enter** the **outbound hostname** previously recorded from within the BCC Email Security domain settings.



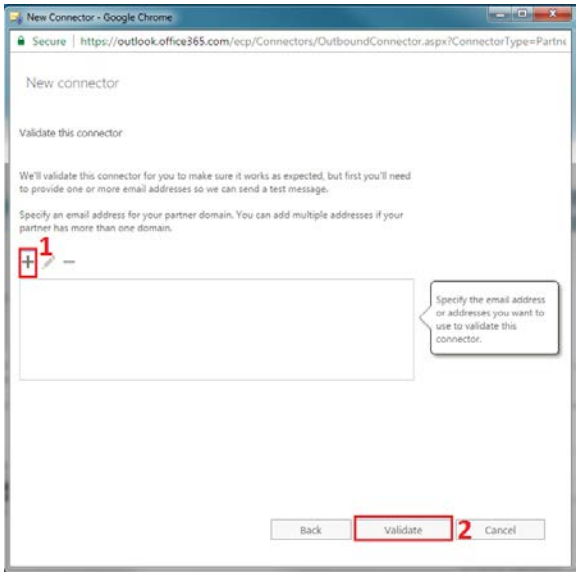


9. Click **Save.** Click **Next**.
10. For connection security, leave "Always use Transport Layer Security (TLS)" **enabled** and **select** "Issued by a trusted certificate authority (CA)".



11. **Click Next.**

12. After reviewing the summary click **Next**.
13. **Click** the '+' button **(1)** to specify an email address used to validate the send connector, enter an email address, then **click** validate **(2)** to test the connector's functionality.



14. After the validation step finishes, click **Save**.

    If you disabled this send connector during the first step of this process, connectivity to the Barracuda outbound host name will succeed, but the validation result of **Sending test email** will fail.

15. 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.

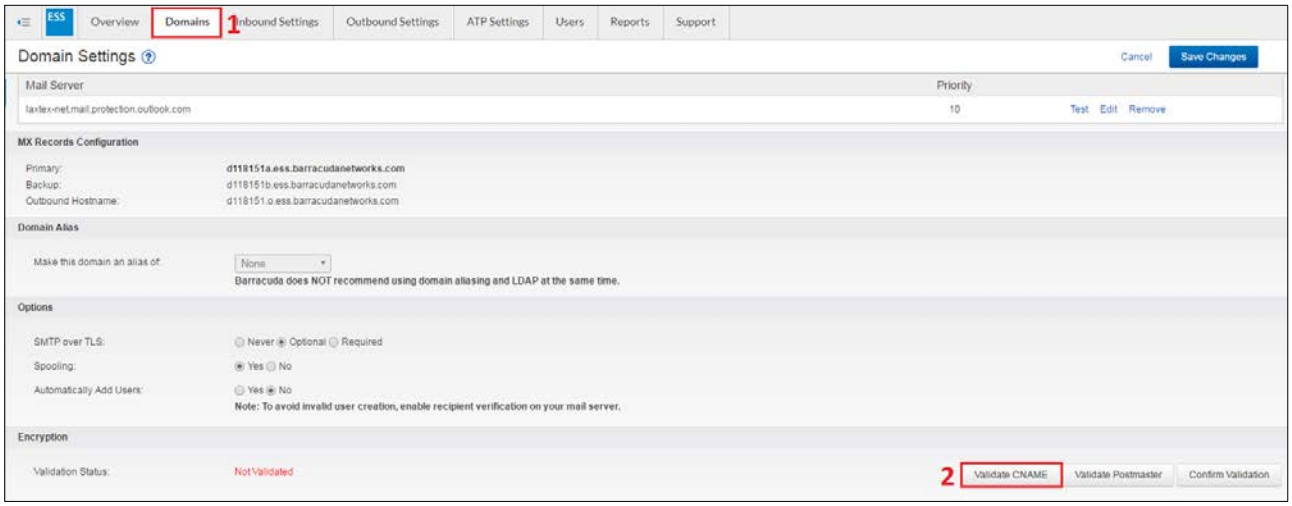
Encryption (Optional)

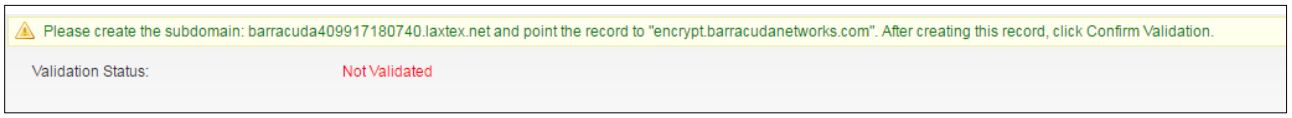
Overview

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**

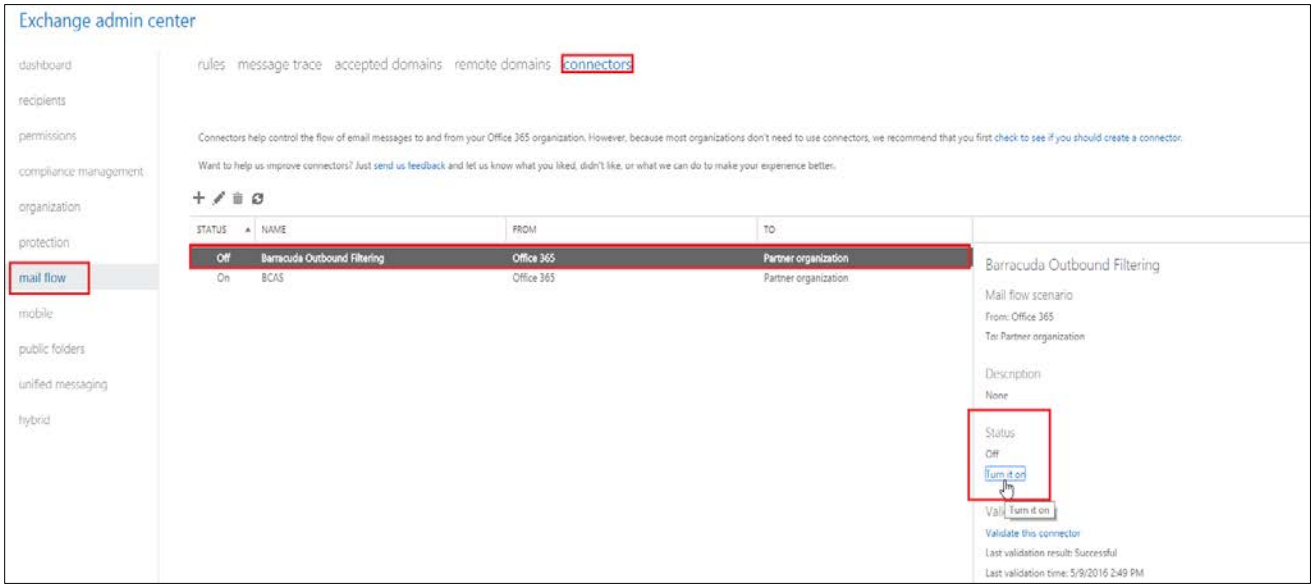
   Please Note: Allow the DNS propagation to take effect before proceeding – this can take up to 24 hours for some providers.

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. **Office365** - Enable the Outbound Send Connector in Office365 to allow outbound mail to flow through the BESS. Go to the **Admin Center for Exchange > Mail flow > 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 Office365 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 Office365 Admin Center –** portal.office365.com

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**.

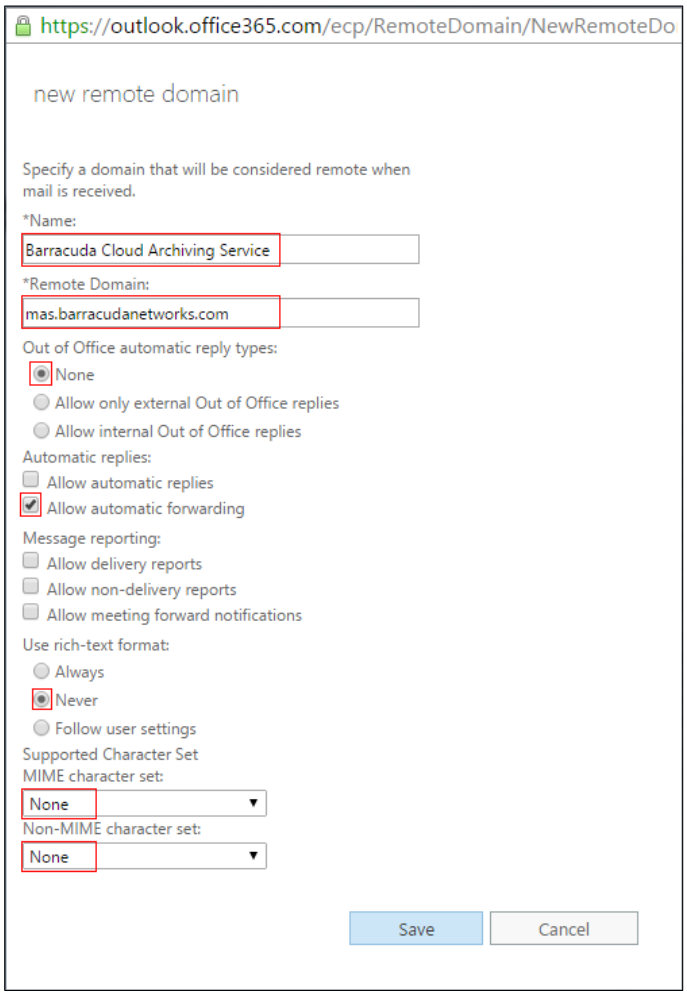
   The page will refresh, click **Mail Sources > SMTP Journaling** where a **journaling address** will be generated. Copy this address to clipboard, we will use this when we create a journaling rule within Office 365 in the journal rule step.

Configuring Journal Archiving for Office365

Add a Remote Domain

1. Log in to Office365 Exchange Admin Center.
2. Select **mail flow > remote domains**.

3. Click the **+** symbol. In the **new remote domain**, complete the following:
   a. **Name** – Type **Barracuda Cloud Archiving Service**
   b. Remote Domain – Enter your region-specific MAS hostname, for example:
      -mas.barracudanetworks.com [US]
      -mas.ca.barracudanetworks.com [Canada]
      -mas.uk.barracudanetworks.com [UK]
   c. **Out of Office automatic reply types** – Select **None**
   d. **Automatic replies** – Select **Allow automatic forwarding**
   e. **Message reporting** – Clear all options
   f. **Use rich-text format** – Select **Never**
   g. **Supported Character Set** – Set both options to **None**

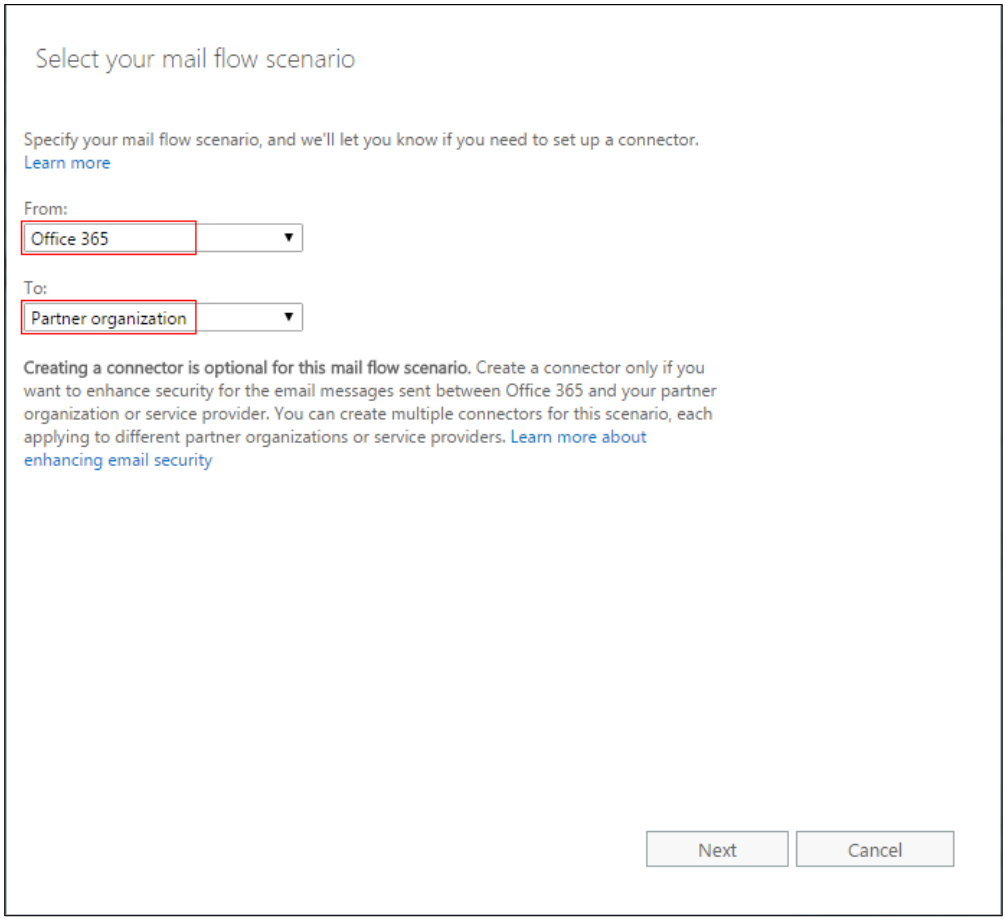


4. Click **Save**.

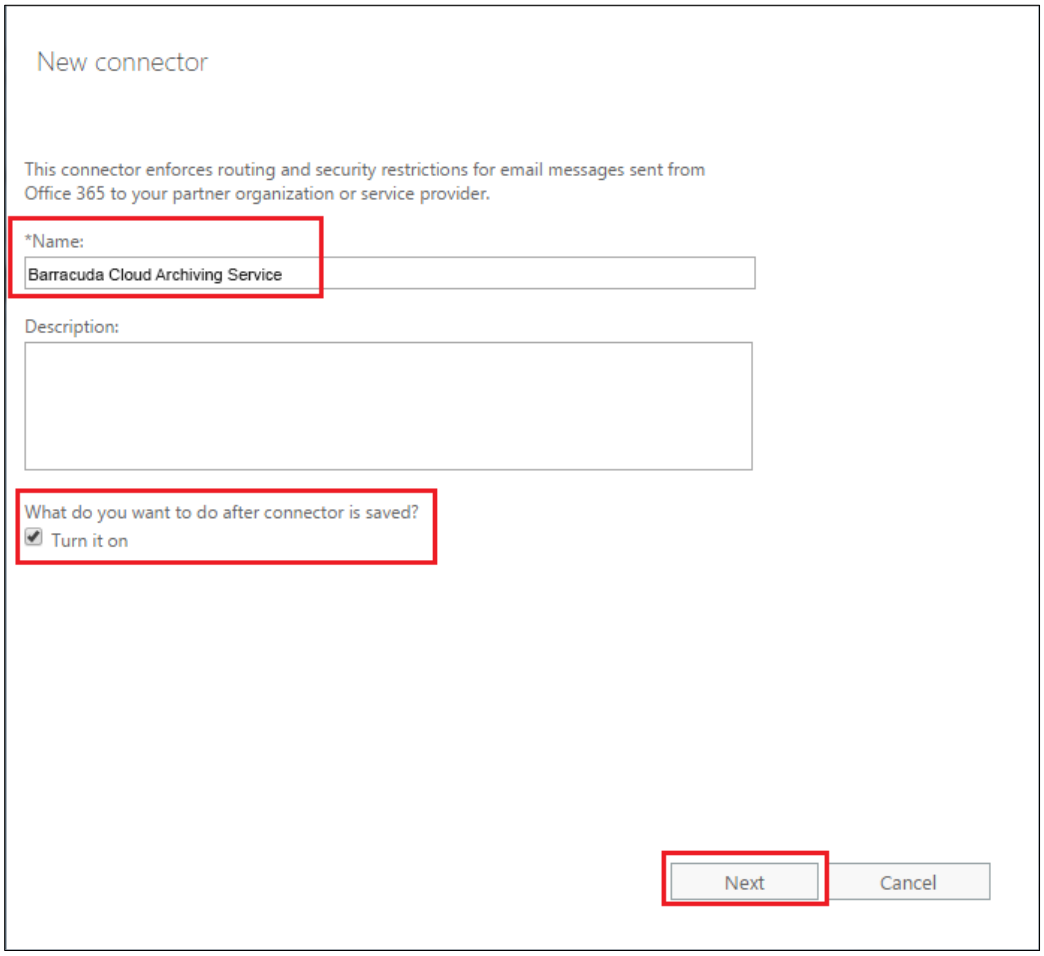
Add a Send Connector

1. Click **Mail flow > connectors**, and click the **+** symbol.

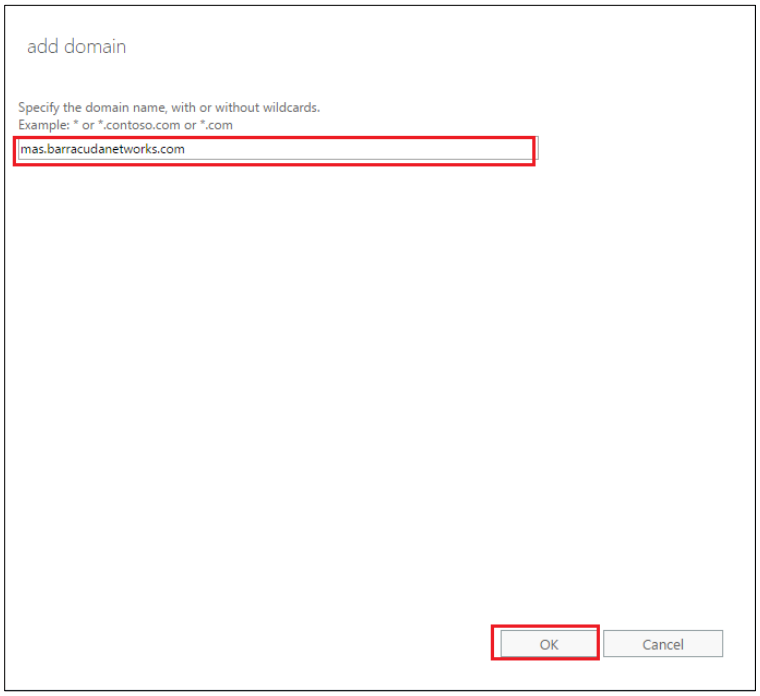
2. The **Select your mail flow scenario** page displays.
3. From the **From** drop-down menu, select **Office365**, and from the **To** drop-down menu, select **Partner organization**:



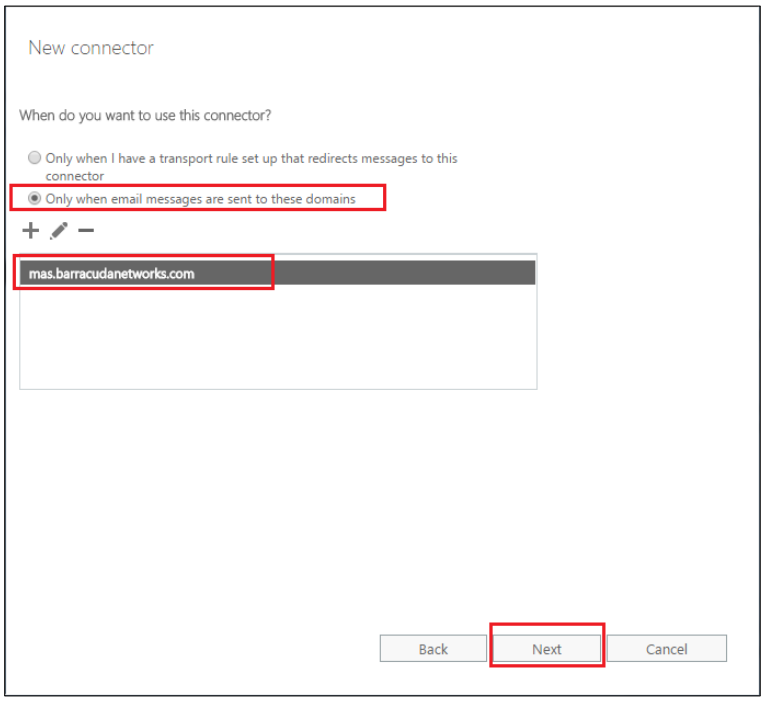
4. Enter a **Name** and (optional) **Description** to identify the connector. Turning it on will archive all mail from this point in time forward, or you can disable it until a later date:



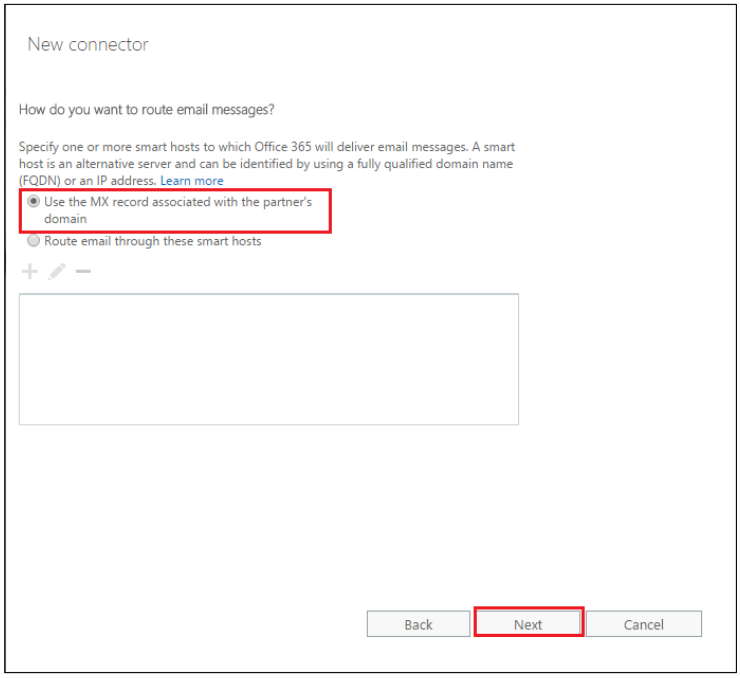
5. Click **Next**. Select **Only when email messages are sent to these domains**, click the **+** symbol, and in the **add domain** field, type **mas.barracudanetworks.com[US] mas.ca.barracudanetworks.com [Canada] or mas.uk.barracudanetworks.com [UK]**



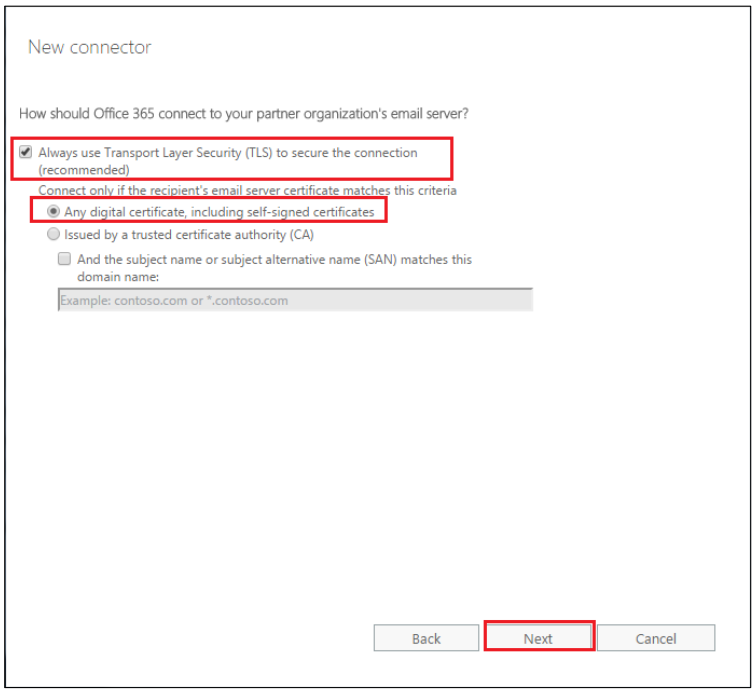
6. Click **OK**:



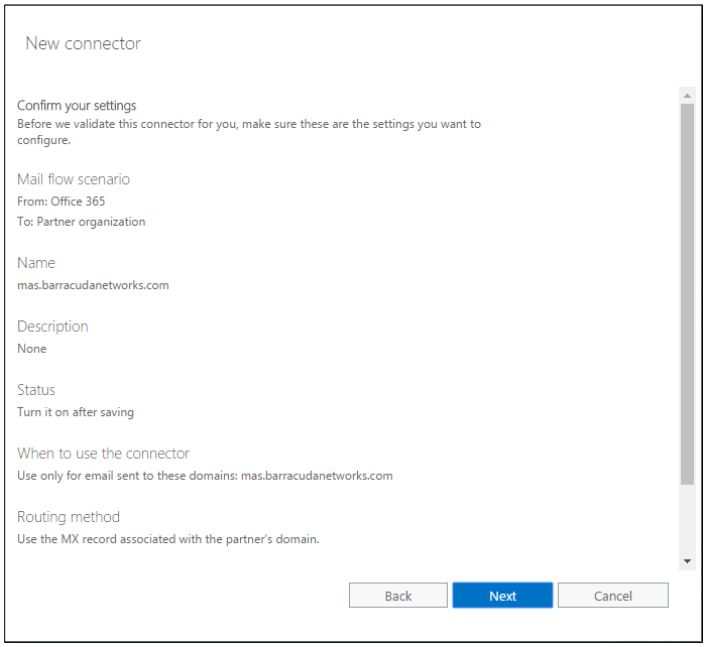
7. Click **Next**. Select **Use the MX record associated with the partner's domain**:



8. Select **Always use Transport Layer Security (TLS) to secure the connection (recommended) > Any digital certificate, including self-signed certificates**:



9. Click **Next**. In the confirmation page, verify your settings:

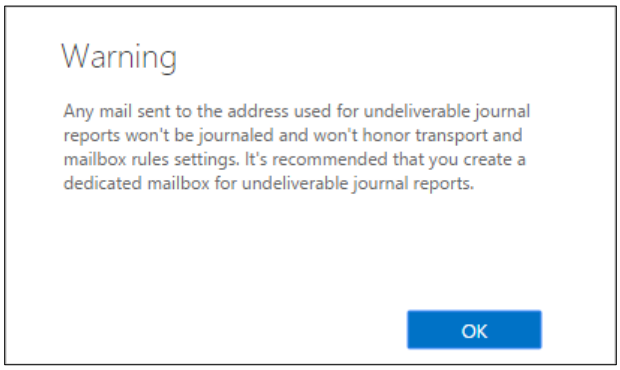


10. Click **Next**. Office365 runs a test to verify your settings. When the verification page displays, enter a test email address (non-O365 account), and click **Validate**. Once the verification is complete, your mail flow settings are added.

Create a Non-Delivery Report Recipient

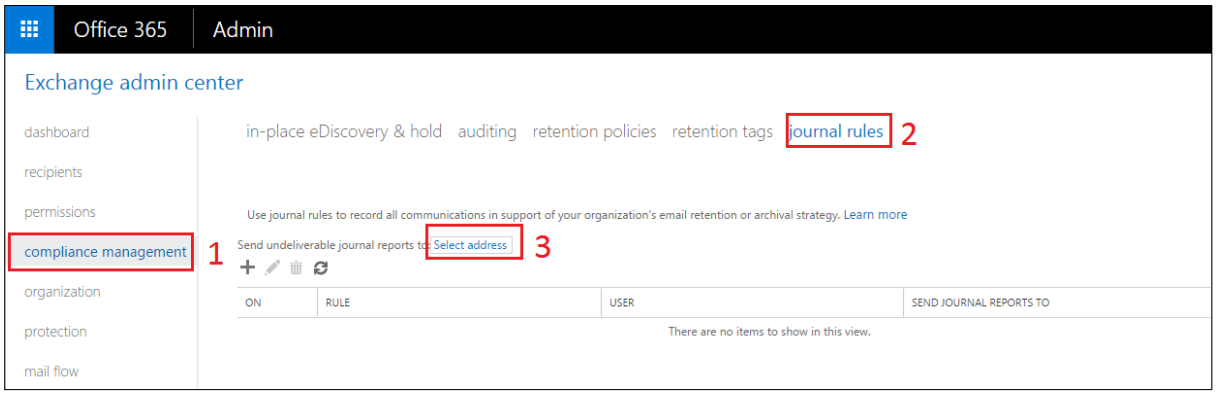
Before creating journal rules, specify a journal recipient for non-delivery reports (NDRs) to reduce the risk of losing journal reports.

Please note: Microsoft recommends that you create a dedicated mailbox for NDR reports. Whichever mailbox you configure as the NDR will lose all of its Outlook client rules, so our recommendation is to create a licensed shared mailbox dedicated for NDR's. [This will not require an extra Essentials license].



To create an NDR recipient:

1. Log in to your Office365 Exchange admin center.
2. Select **compliance management (1)** > **journal rules (2)**.
3. If an NDR email recipient is not already specified, click **Select address (3)** to the right of **Send undeliverable journal reports to** field:



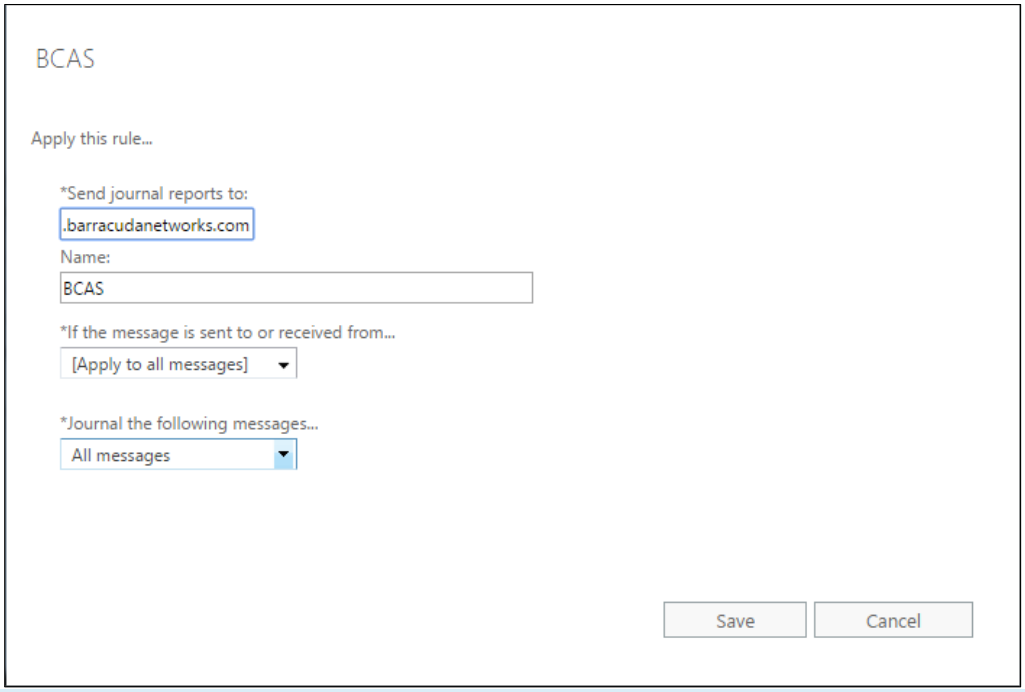
4. Browse to and select a recipient from the address book who should receive undeliverable journal reports. You can search for a recipient by typing all or part of a display name, and then clicking the **Search** icon, or click on either the **Display Name** or **E-Mail Address** heading to sort the list.
5. Click **OK** once you select a recipient, and in the **NDRs for undeliverable journal reports** window, click **Save**.

When creating the journaling rule, depending on your Office365 configuration, you may be required to send the journaling report to an external email address. For more information, refer to the Microsoft Office365 community discussion board: http://community.office365.com/en-us/f/158/t/162118.aspx[2]

Configure Office365 to Journal Mail

1. Log in to Office365 Exchange Admin Center.
2. Select **Compliance management** > **Journal rules**.
3. Click the **+** symbol. In the **new journal rule** dialog box, complete the following:
   a. **Send journal reports to** – Enter the journaling address from the **MAIL SOURCES > SMTP** page in the Barracuda Cloud Archiving web interface. This is called the journaling mailbox.
   b. **Name** – By default, the name of the journal rule is automatically generated from the journal recipients. If there are existing journal rules that contain the same journal recipients, numbers are automatically appended to the journal rule name to avoid duplicates. If you choose to override the automatically-generated name by typing in a custom name, verify the name is unique and descriptive.
   c. **If the message is sent to or received from** – Select **Apply to all messages** to journal all recipients.
   d. **Journal the following messages** – Enter the **journaling address** you copied to clipboard from step 1 into ***Send Journal Report to***

e. Then under ***If the message is sent to or received from***: select ***Apply to all messages*** & under ***Journal the following messages***: select ***All messages*** to journal all messages regardless of source or destination:



Because the journaling mailbox may contain sensitive information, it is recommended that you create organization-wide policies that govern who can access the journaling mailboxes in your organization.

4. Click **Save**. Then click **Yes**. The rule is added to the **journal rules** table.

Once you complete this configuration, mail begins forwarding to the Barracuda Cloud Archiving Service. Log in to the web interface as the administrator, and go to the **BASIC > Dashboard** page. Processed mail displays in the **Message Statistics** table. Statistics are cached and may take up to 30 minutes to appear.

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** Office 365 service account with global admin rights to the client's domain in order to synchronize data.

Requirements

- Windows 8 or 8.1
- Windows Server 2012 or Windows Server 2012 R2

- Windows 7 Service Pack 1 (SP1)*
- Windows Server 2008 R2 SP1*
- Microsoft .NET Framework 4.5 or 4.5.1 and either the Windows Management Framework 3.0[1] or the Windows Management Framework 4.0[2]
- Verify the service account has a mailbox, and *is not* hidden in the **Global Address** list

Exchange Database: Historical Import

Step 1. Connect to Office 365 Exchange Online

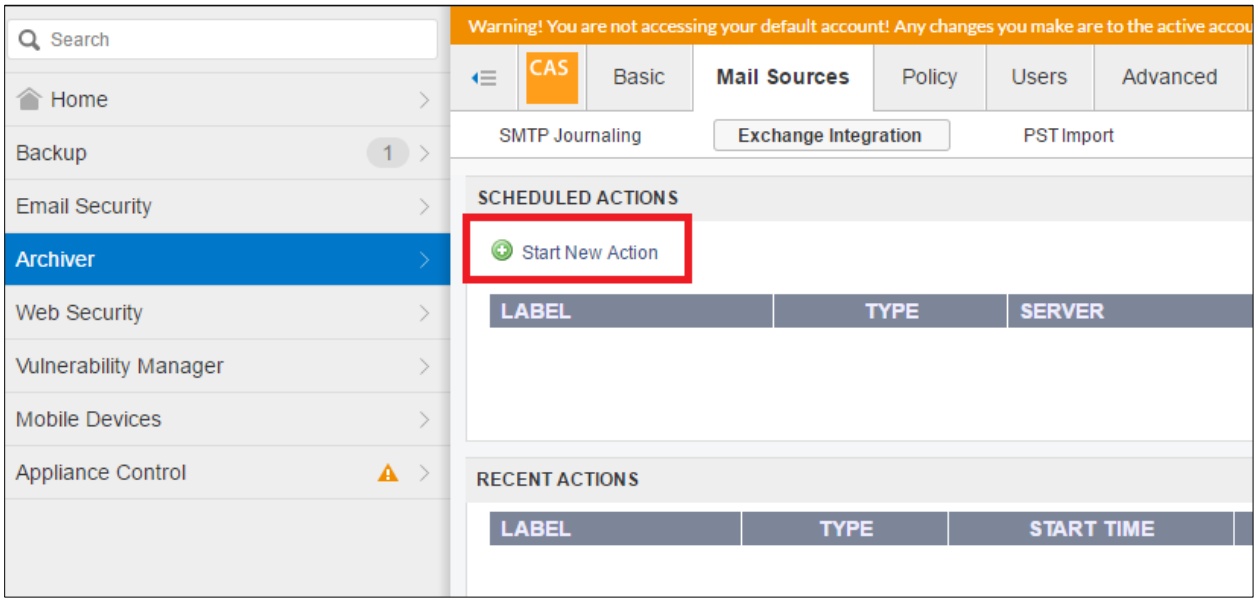
1. Open Windows PowerShell, enter the following command, and then press Enter:
   $UserCredential = Get-Credential
2. In the Windows PowerShell Credential Request dialog box, enter your Exchange Online user name and password, and then click OK.
3. Enter the following command, and then press Enter:
   $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
4. For more information, refer to the Microsoft TechNet article Connect to Exchange Online using remote PowerShell.
5. Enter the following command, and then press Enter:
   Import-PSSession $Session
6. Enter the following command, and then press Enter (make sure to update the **ServiceAccount@domain.com** user to your licensed O365 service account):
   Get-Mailbox -ResultSize unlimited | Add-MailboxPermission -User ServiceAccount@domain.com -AccessRights fullaccess -InheritanceType all -Automapping $false
   a. Permissions are assigned on existing mailboxes only; if additional mailboxes are added to your organization, you must rerun this command.
   b. For more information on adding mailbox permissions, see Add-MailboxPermission in the Microsoft TechNet. For information on testing mailbox rights, see Get-MailboxPermission in the Microsoft TechNet.

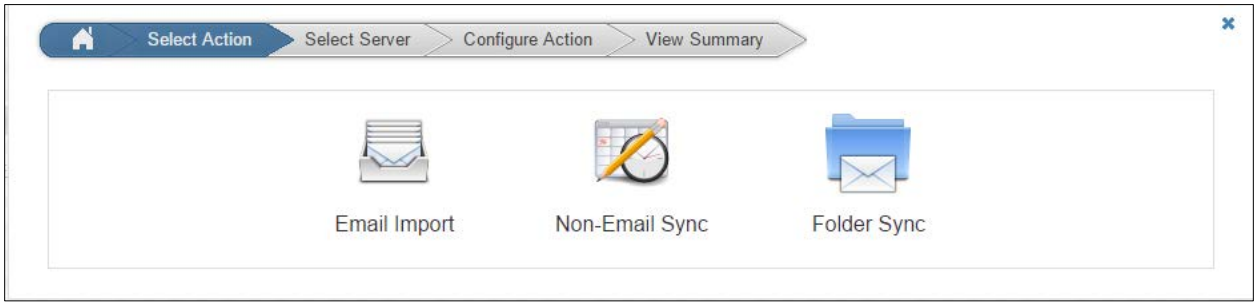
Step 2. Import from Office 365 Exchange Online

Please note: When setting up the Exchange import job in the web interface: Use the GUID@domain.com -style hostname available when setting up an Outlook profile *or* use https://testconnectivity.microsoft.com/

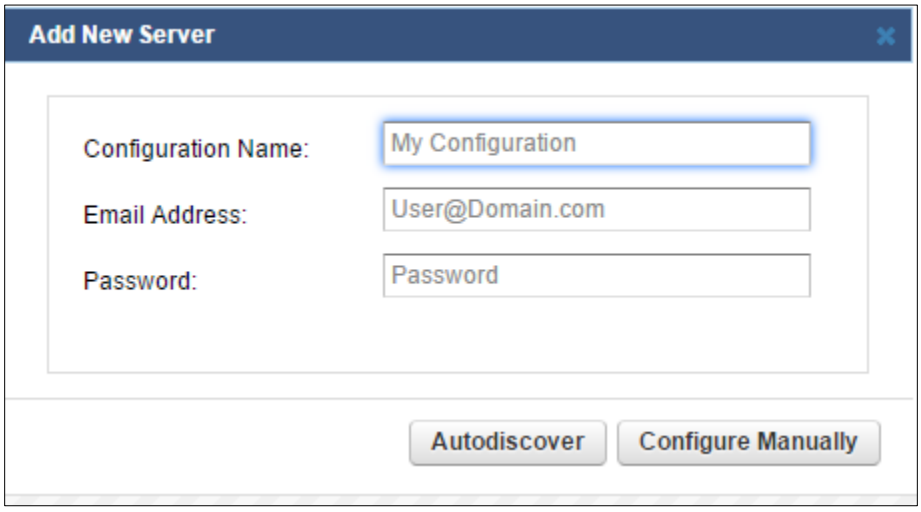
Option 1 - Automatically Discover Settings

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





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



4. In the **Add New Server** dialog box, enter a Configuration Name, the email address for the service account and the service account password.

5. Click **Autodiscover**.

Please note: If autodiscover is unable to identify your settings, use the steps below.

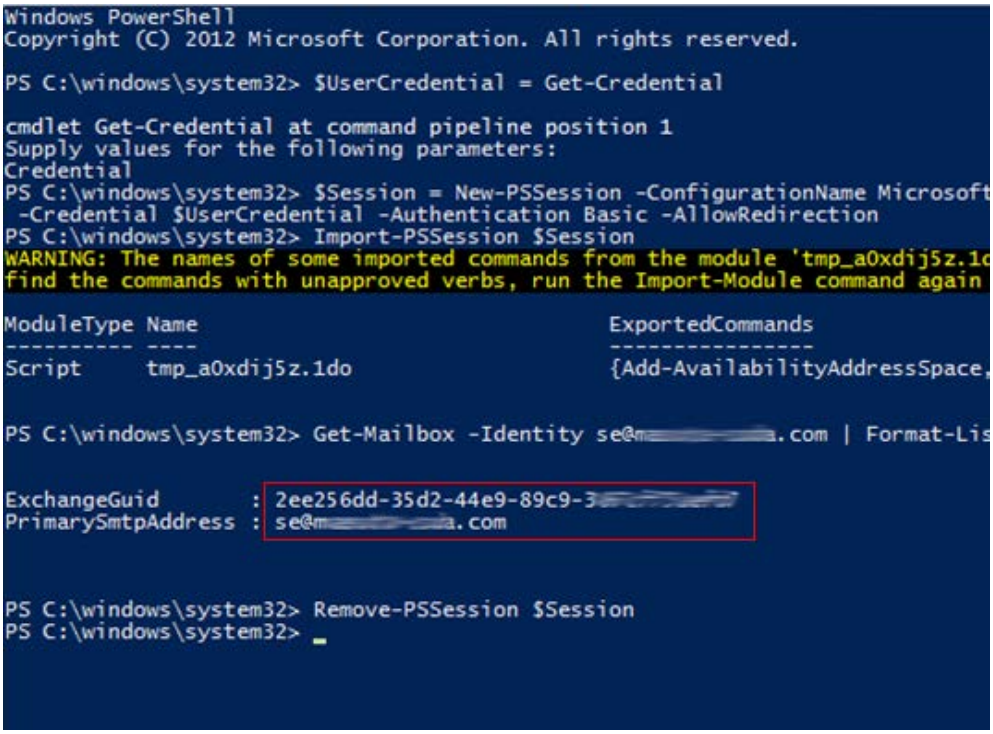
Option 2 - Manually Configure Settings

Please note: Use the steps in this section only if autodiscover is unable to identify your settings as described above in the section Automatically Discover Settings.

Step 1. Manually Obtain Exchange Hostname Using PowerShell

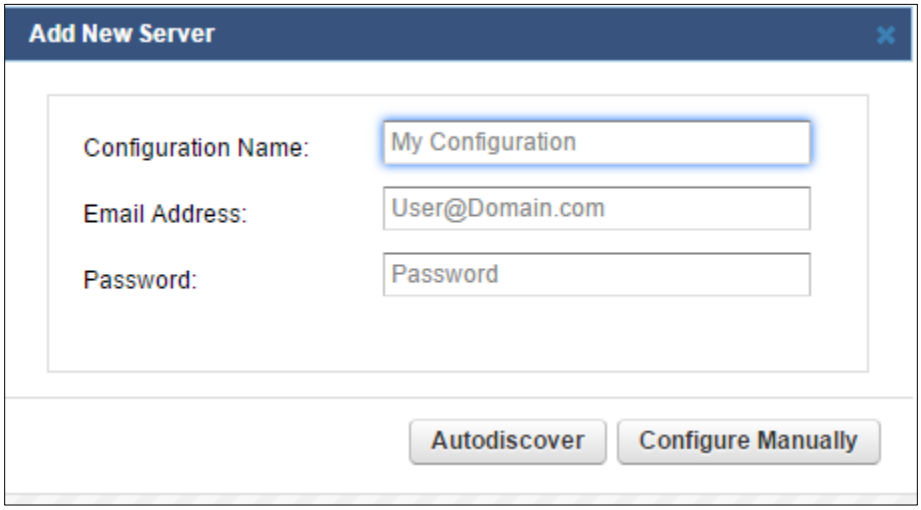
Please note: if you still have your connection to O365 Exchange online $Session, please skip to step 7.

1. Open Windows PowerShell, and connect to Office 365 Exchange Online.
2. Enter the following command, and then press Enter:
   $UserCredential = Get-Credential
3. In the Windows PowerShell Credential Request dialog box, enter your Exchange Online admin username and password, and then click OK.
4. Enter the following command, and then press Enter:
   $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
5. For more information, refer to the Microsoft TechNet article Connect to Exchange Online using remote PowerShell.
6. Enter the following command, and then press Enter:
   Import-PSSession $Session
7. Enter the following command, and then press Enter (make sure to update the **ServiceAccount@domain.com** user to your licensed O365 service account):
   Get-Mailbox -Identity ServiceAccount@domain.com | Format-List ExchangeGuid, PrimarySMTPAddress
8. To determine the **Exchange Hostname**, combine the **ExchangeGuid** with the **domain** portion of the PrimarySMTPAddress in the form ExchangeGuid@domain.com

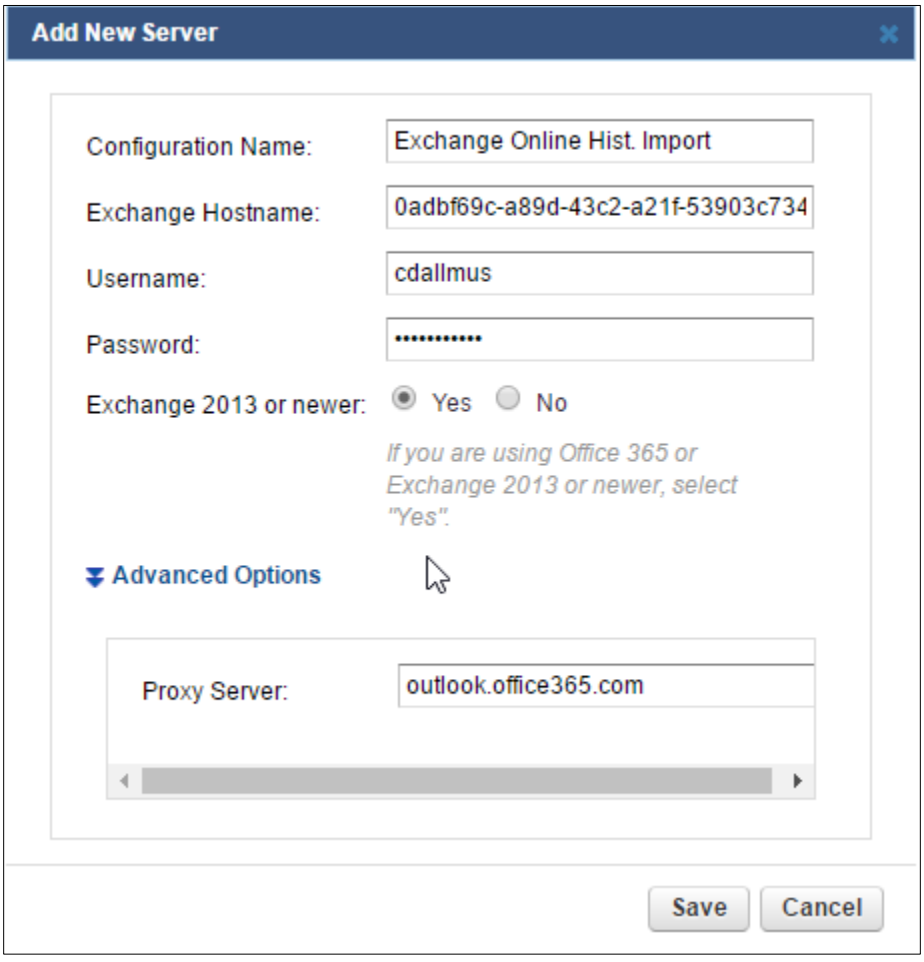


Step 2. Manually Configure Server Settings for Email Import

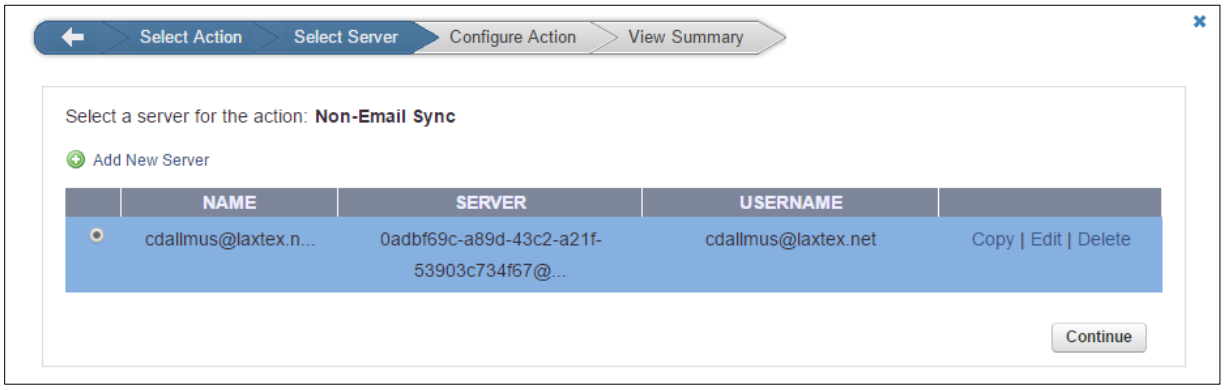
1. Log in to the Barracuda Cloud Archiving Service as the admin, and go to Mail Sources > Exchange Integration.
2. Click **Start New Action**. In the Select Action page, click **Email Import**.
3. In the Select Server page, click **Add New Server**.
4. In the Add New Server dialog, click **Configure Manually**; enter the Exchange details:



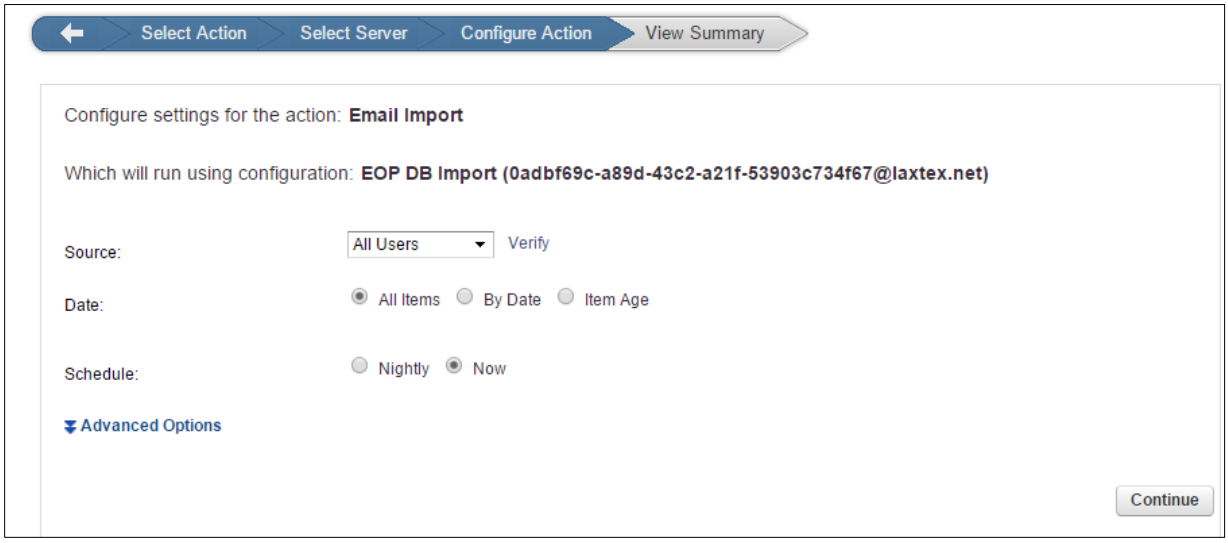
5. Configuration Name – Enter a name to identify the configuration. For example, type: Exch DB Historical Import
6. Exchange Hostname – Enter the **ExchangeGUID@Domain** from Step 1.8 Manually Obtain Exchange Hostname Using PowerShell. For example, type: **2ee256dd-35d2-44e9-89c9-3df7987f93@domain.com**
7. Username – Enter the service account username. For example, type: **ServiceAccount@testdomain.com**
8. Password – Enter the password associated with the username.
9. Exchange 2013 or newer – Select **Yes**.
10. Advanced Options – In the **Proxy Server** field type **outlook.office365.com** and leave the Global Catalog Server field blank.



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



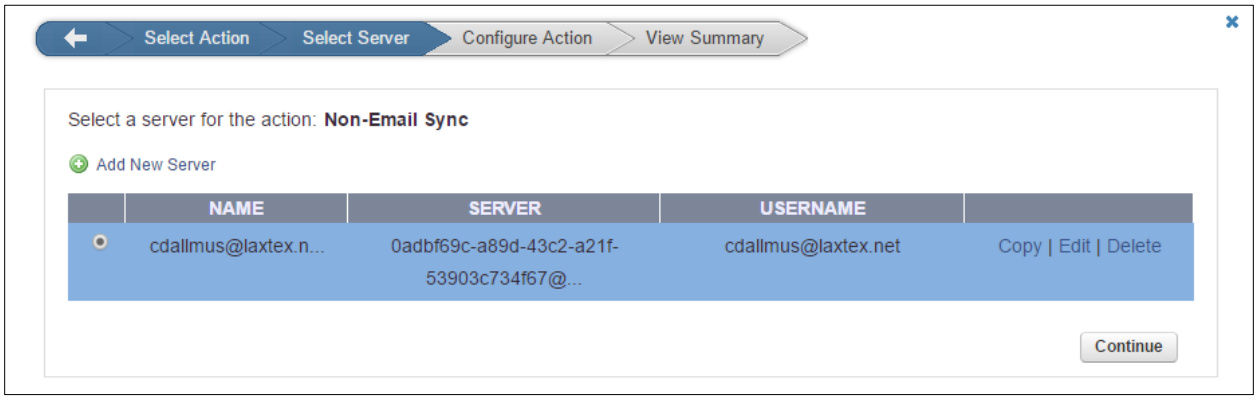
13. In the View Summary page, select **All Users** from the Source drop-down menu.
14. In the schedule section, enter the desired Date and Select **Now**. Click **Continue**.



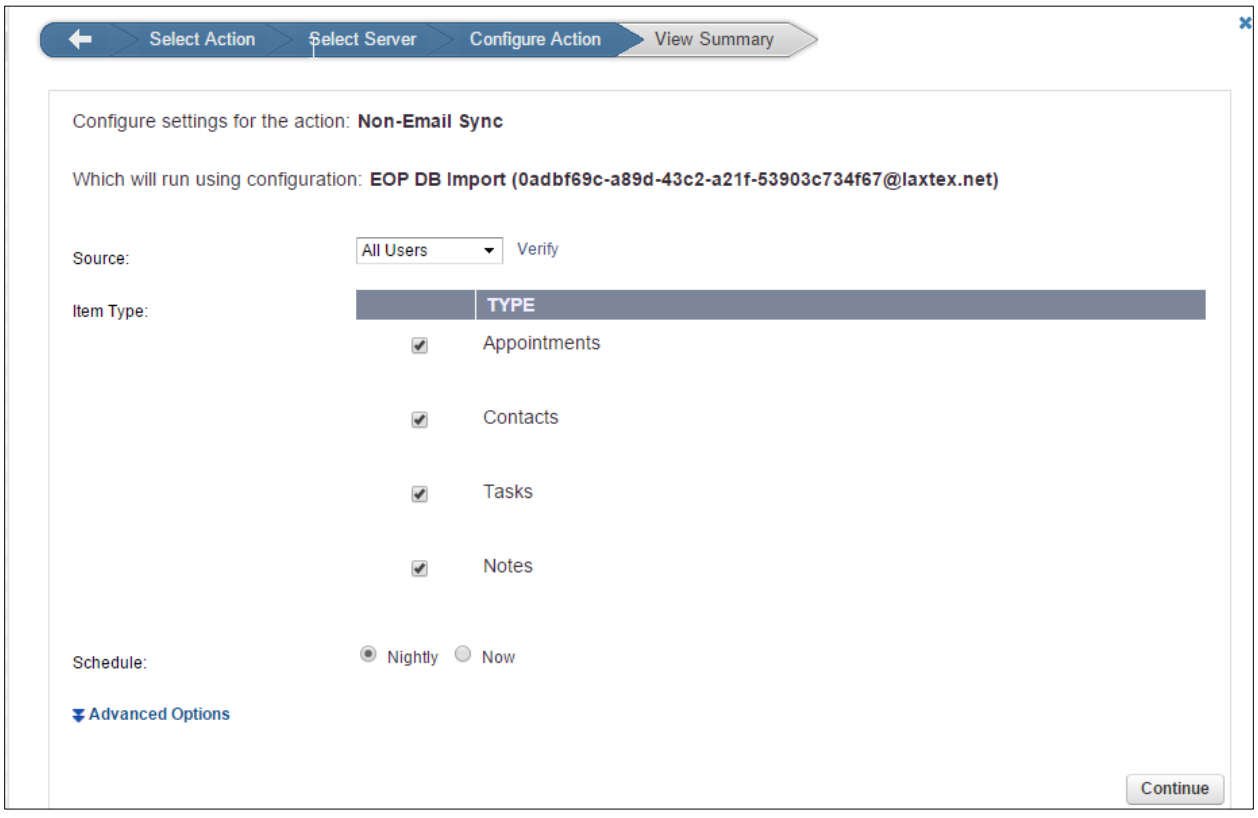
15. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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 O365 server will be saved. If not, please reference this section for connecting your O365 server.



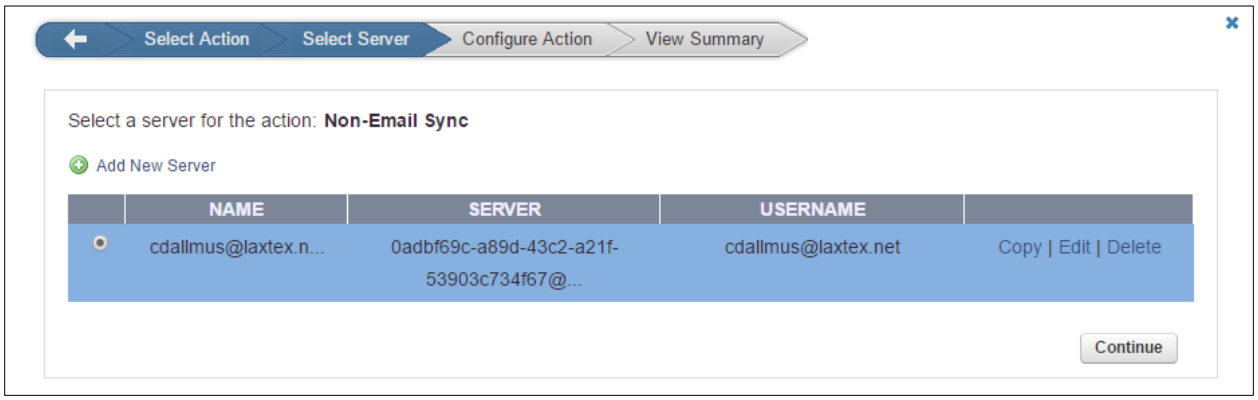
4. In the Configure Action page, Click **Continue**.
5. In the View Summary page, select **All Users** from the Source drop-down menu. For item type, check or de-check any of the items you would like to synchronize. For schedule, select **Nightly**. Then click **Continue**.



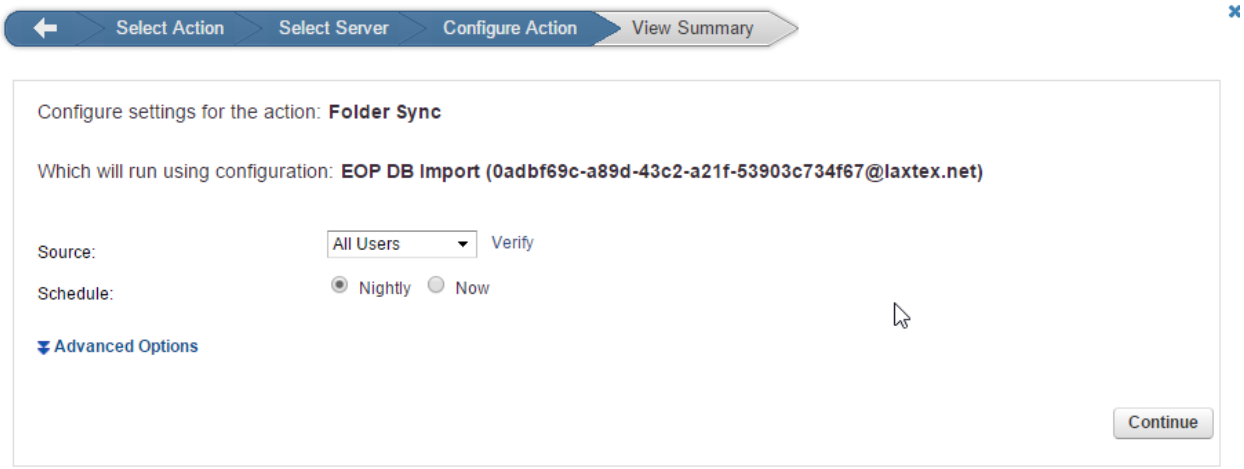
6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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 O365 server will be saved. If not, please reference this section for connecting your O365 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**.

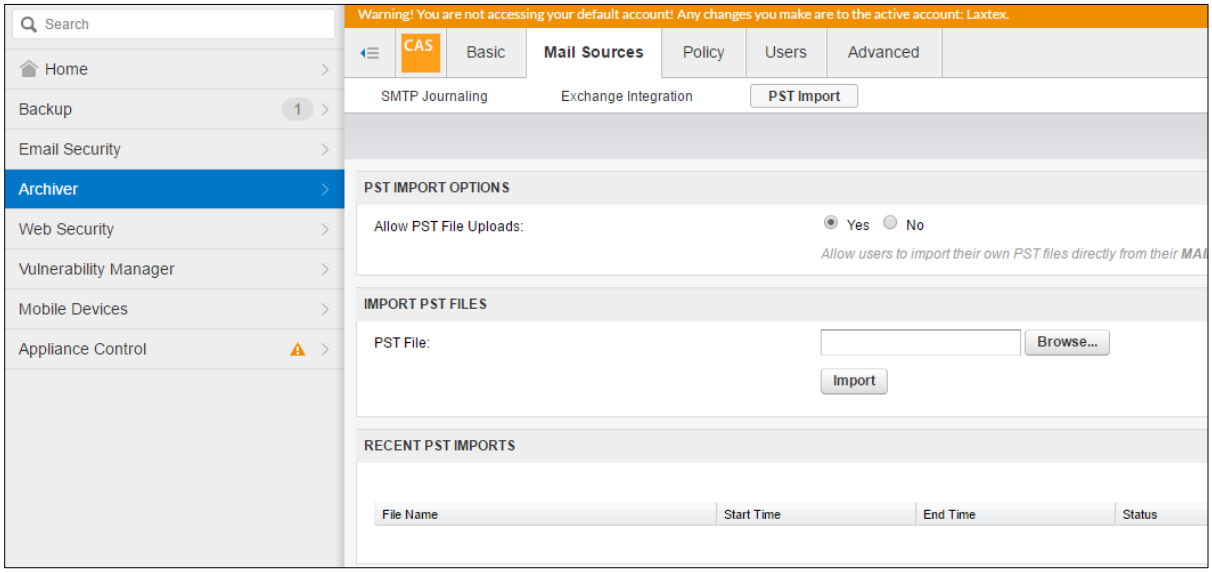


6. Verify the configuration settings in the View Summary page, and then click **Submit** to add the Email Import to the Scheduled Actions table.

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.

Cloud to Cloud Backup

Overview

Hosting production data in the cloud does not mitigate the need for backup and recovery. Emails and important documents are susceptible to corruption and risk being unrecoverable due to malicious attacks or even accidental deletion. Barracuda Essentials for Office365 protects Exchange Online, SharePoint Online, and OneDrive for Business data by backing it up directly to Barracuda Cloud Storage. The steps below walk you through the configuration for backing up all 3 Office365 services: Exchange Online, OneDrive for Business & SharePoint Online.

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. If you don't have the email, check your spam or "clutter" folder. Otherwise, you can manually reset your password directly in the BCC portal using the 'forgot password' link.
- **Access & Credentials to Office365 Admin Center –** portal.office365.com

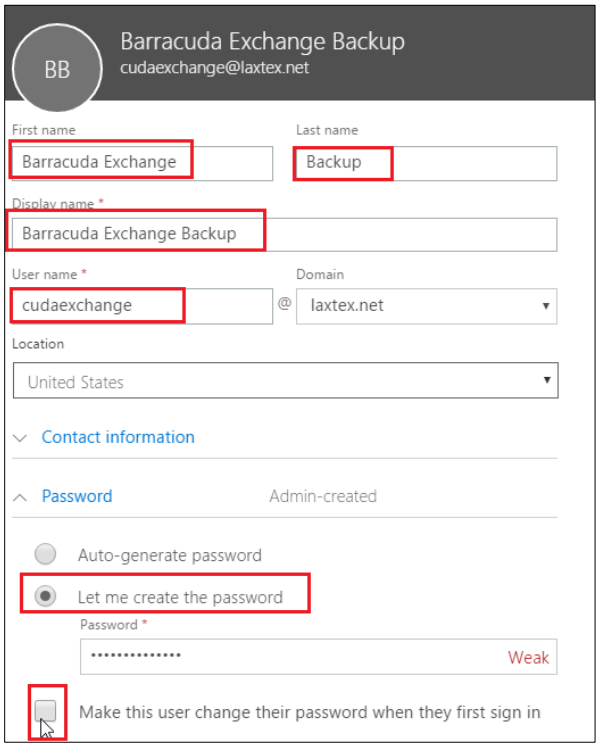
Like the Archiving service, Cloud to Cloud Backup can be configured and brought online without affecting the customer's production systems. The steps below walk you through the configuration for backing up all 3 Office365 services, Exchange, OneDrive & SharePoint.

> **Please Note:** If you plan to back up multiple services, we recommend creating 3 Global Service Accounts for each service due to Office365 rate limits on maximum bandwidth utilization per mailbox – by separating out Global Service accounts, we optimize your Cloud-to-Cloud backups' performance.

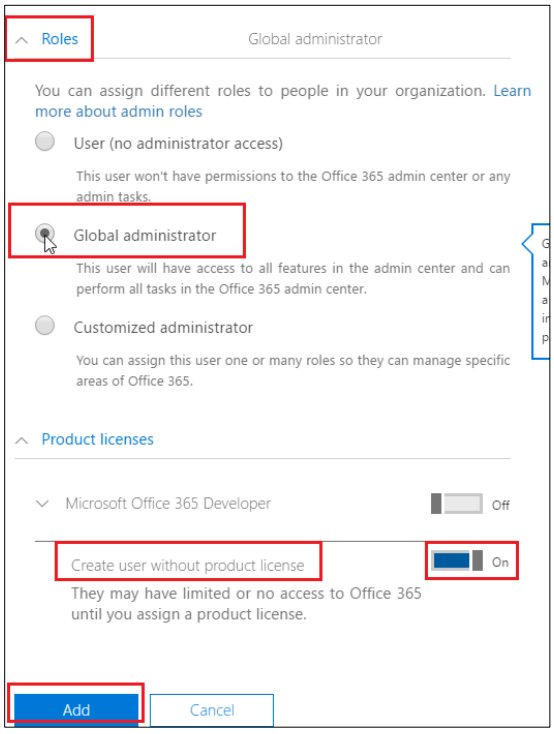
Exchange Online

Create a Global Service Account

1. Log in to your Office365 Management Panel using an account with administrative privileges, and click **users and groups** in the left pane.
2. Click the + symbol to create a new account.
3. Enter the name for the new service account **[**take note of these details**]**
    1. **First name:** Barracuda Exchange
    2. **Last name:** Backup
    3. **Username:** cudaexchangebackup
4. Drill into the password section, click **'Let me create the password'**, uncheck **'Make this user change their password when they first sign in'** and define a password that you will remember. **[**take note of password**]**

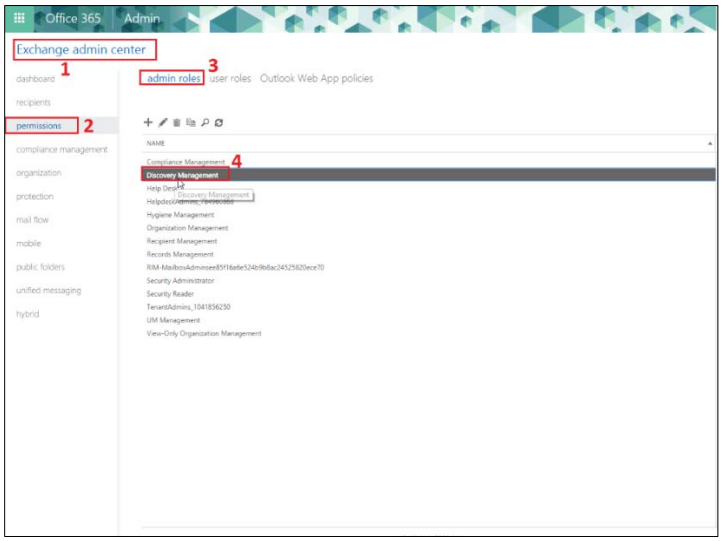


5. Drill into the **roles** section and select **global administrator**.
6. In the **product licenses** section, enabled the toggle for **'Create user without product license'**. Click **Add.**

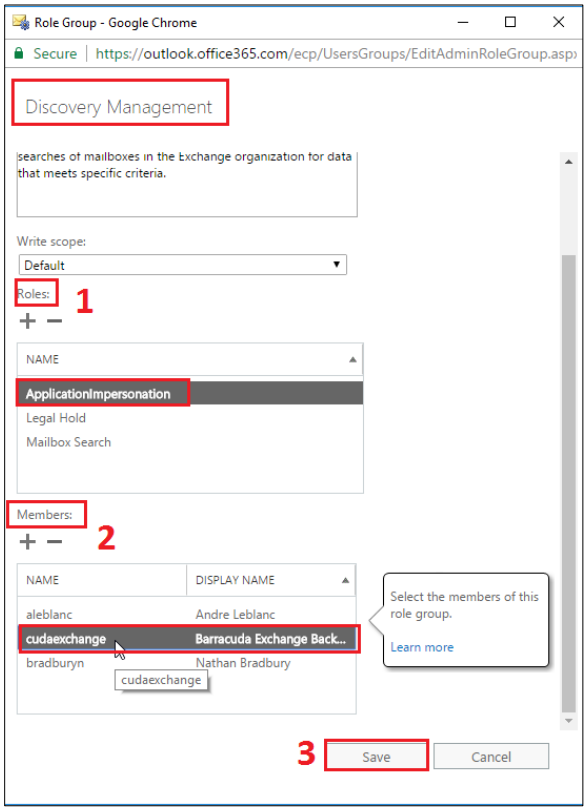


Configure Application Impersonation for Exchange Online

1. Within Office365 go to **Admin Center Exchange (1)**:
2. Click on **Permissions (2)** > **Admin roles (3)** > Double click on **Discovery Management (4)**



3. Under the **Roles (1)** section, click the **'+'** button and add "**Application Impersonation**"

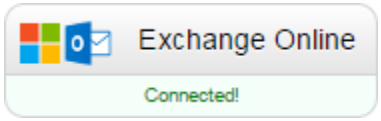


4. Under the **members (2)** section click '+' to add the **Exchange Backup** service account user.

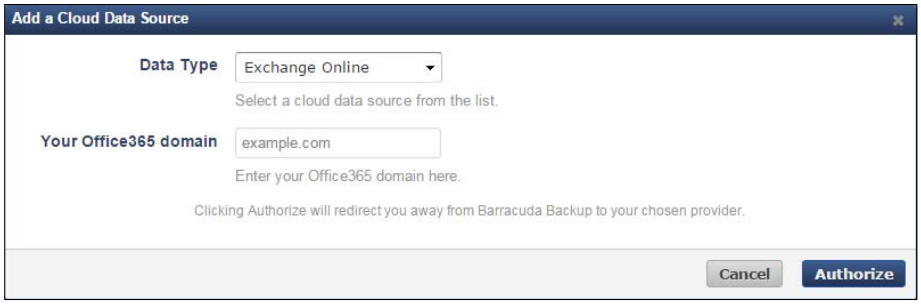
Configure Exchange Online Data Source

Use the following steps to set up Exchange Online backup within BCC. Open a private browsing window in order to prevent cache from trying to authenticate with your admin user account.

1. Log in to **BCC** then click the Backup tab, and select the Cloud Source in the left pane.
2. In the **Status** page, click **Exchange Online**:



3. The **Data Sources** page displays. Click **Add a Cloud Provider**, and enter the following details:
   a. In the **Cloud Provider description** field, enter a name to represent the data source.
   b. From the **Cloud Provider type** drop-down menu, select **Microsoft Office365**.
   c. Click **Save**.
4. The **Add a Cloud Data Source** dialog box displays:
   a. From the **Data Type** drop-down menu, select **Exchange Online**:

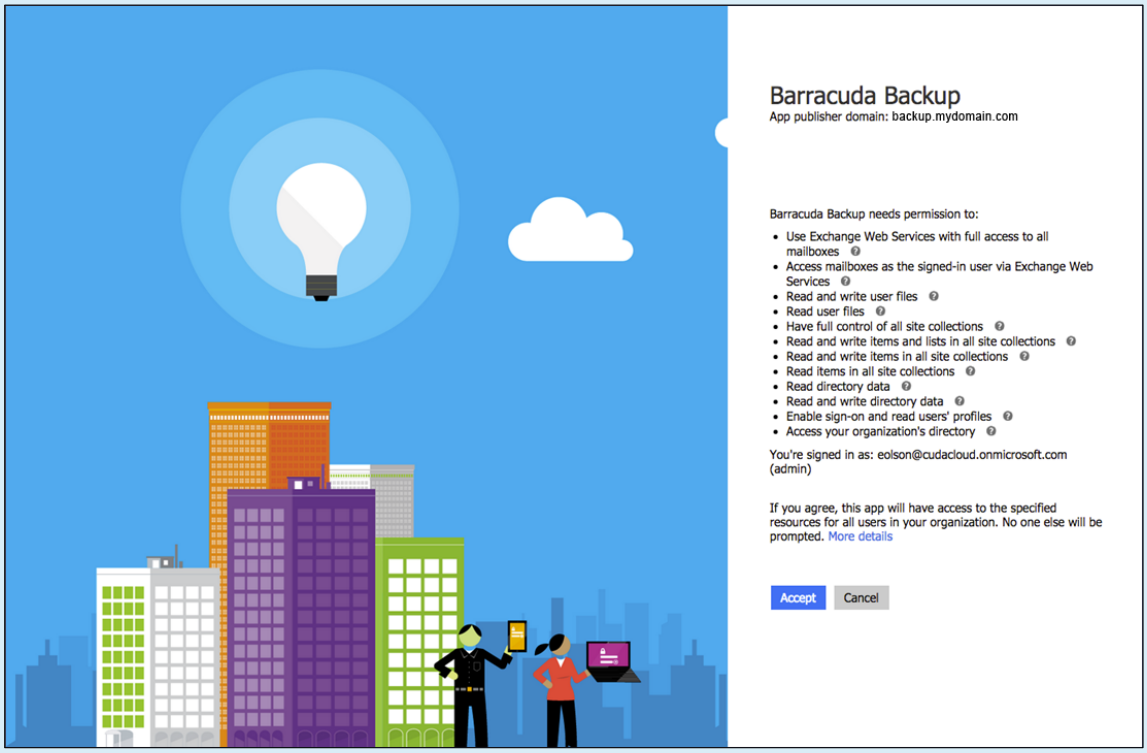


   b. Enter **Your Office365 domain** URL.
      1. The URL is available once you log in to Exchange Online.
5. Click **Authorize**.

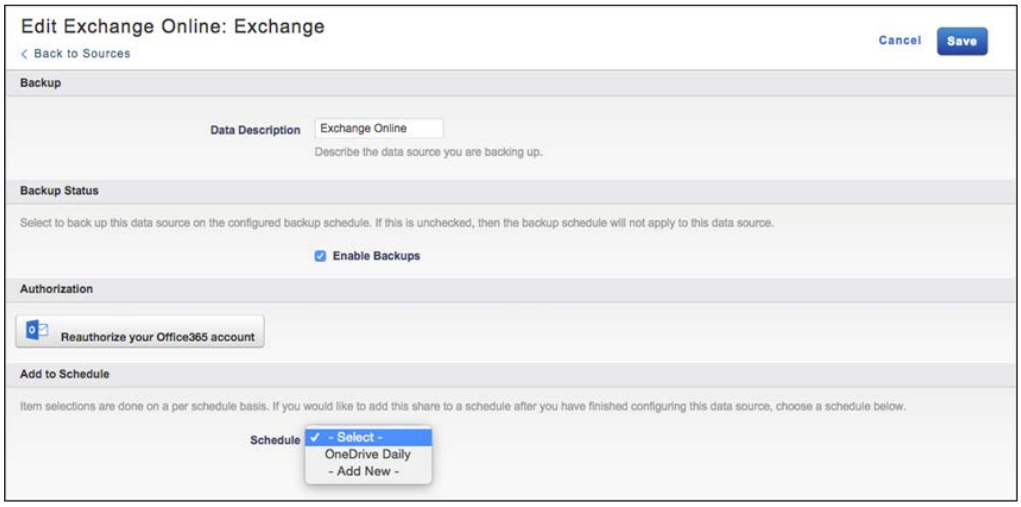
[**Note**: Be careful during this step. You need to authorize with the Global Service Account for Exchange Backup we just created. Click **Add another account** & enter the credentials for the **Exchange Backup account** we created in step one]

In the Exchange Online page, click **Accept** to authorize Barracuda to back up data from Exchange Online: Then make sure to click the **Exchange Backup account** once again to complete the

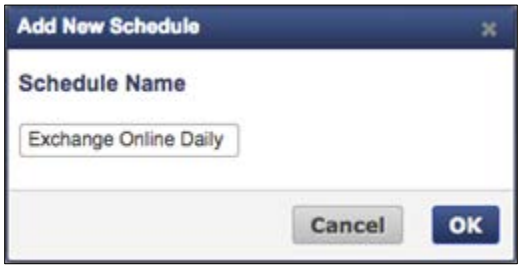
authorization and redirect you back into the BCC portal.



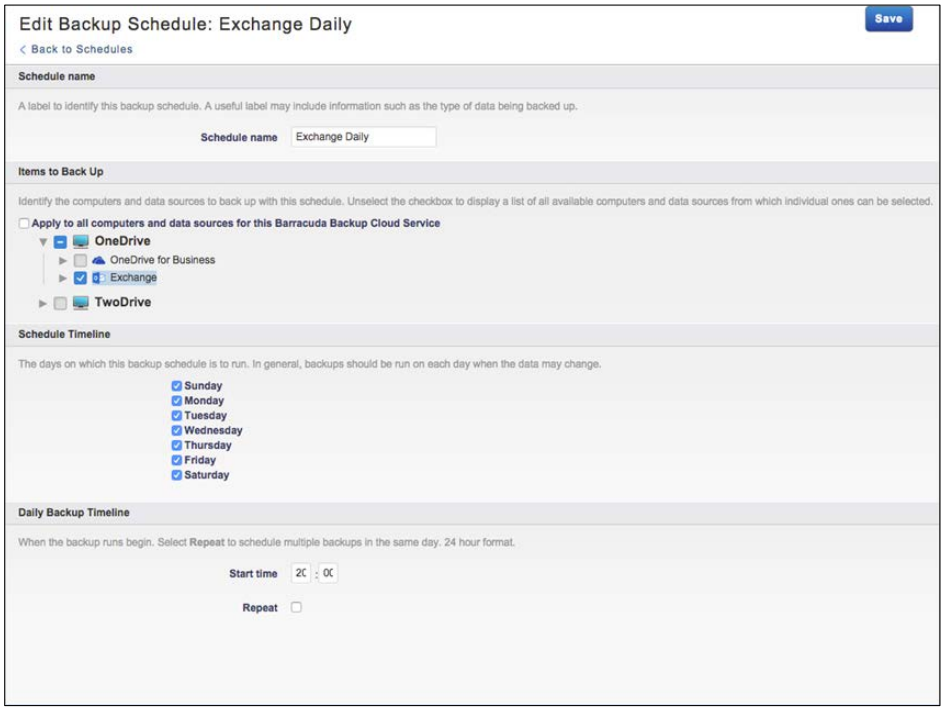
1. The **Edit Exchange Online** page displays.
   a. Enter a name to identify the data source in the **Data Description** field.
2. In the **Add to schedule** section, click the drop-down menu, and then click **Add New**:



3. The **Add New Schedule** dialog box displays. Enter a name to represent the schedule:



4. Click **OK**. The **Edit Exchange Online** page is updated with the new schedule name.
5. Click **Save**. The **Edit Backup Schedule** page displays.
6. In the **Items to Back Up** section, select individual items to back up, or click **Apply to all computers and data sources for this Barracuda Backup Cloud Service** to back up everything in Exchange Online.
7. In the **Schedule Timeline** section, select the day you want the schedule to run.
8. In the **Daily Backup Timeline**, specify the time of day the schedule is to run:

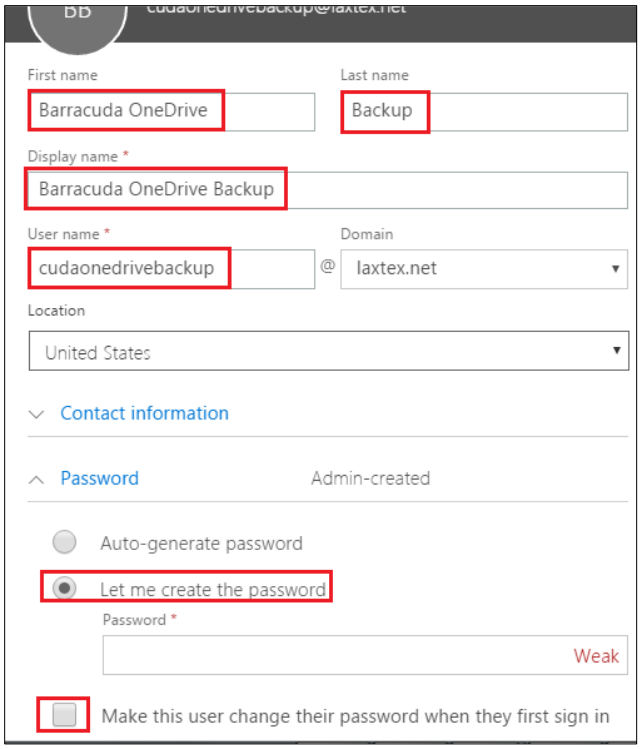


9. Click **Save**. Exchange Online is backed up based on your data source and schedule settings.

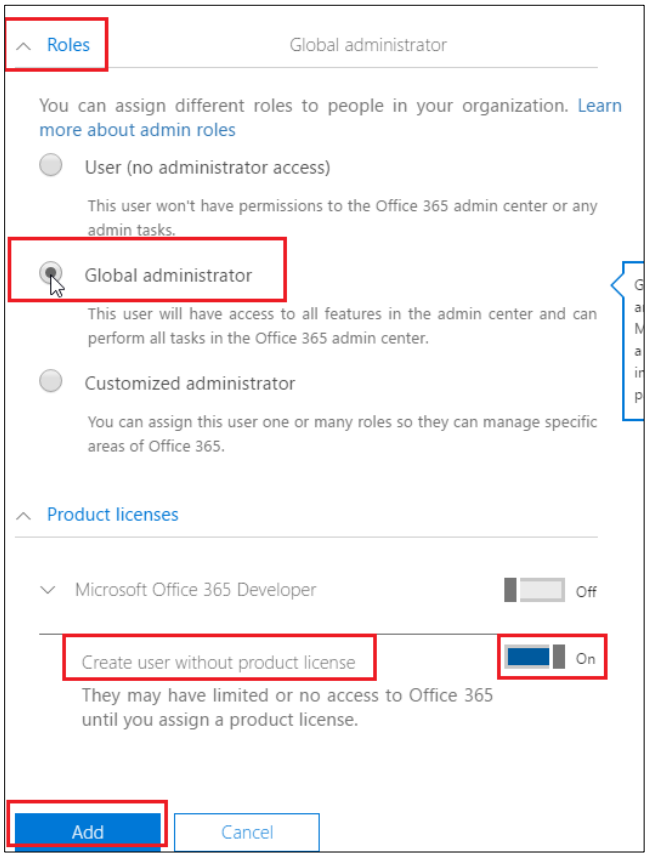
OneDrive for Business

Create a Global Service Account

1. Log in to your Office365 Management Panel using an account with administrative privileges, and click **users and groups** in the left pane.
2. Click the + symbol to create a new account.
3. Enter the name for the new service account **[**take note of these details**]**
    1. **First name:** Barracuda OneDrive
    2. **Last name:** Backup
    3. **Username:** cudaonedrivebackup
4. Drill into the password section, click **'Let me create the password'**, uncheck **'Make this user change their password when they first sign in'** and define a password that you will remember. **[**take note of password**]**



5. Drill into the **roles** section and select **global administrator**.
6. In the **product licenses** section, enabled the toggle for **'Create user without product license'**. Click **Add.**



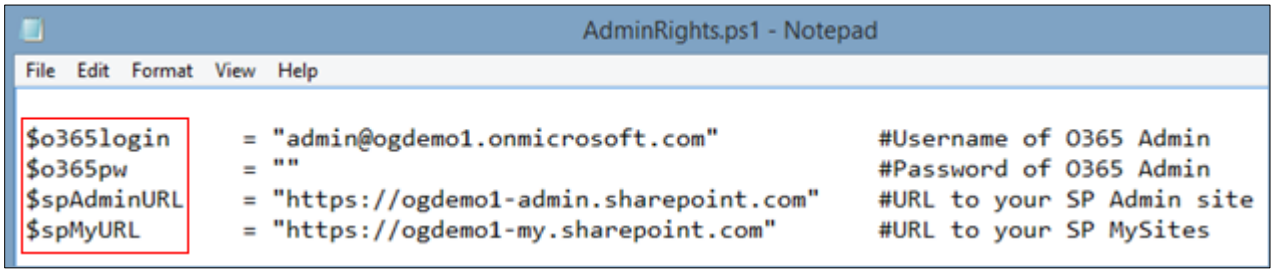
Configure Permissions for OneDrive for Business

There are two options you can use to give the service account created in the prior Step:

- **Option 1 –** Run a SharePoint Online Management Shell script to automatically apply the proper permissions to each user account; this is the preferred and fastest. If you have multiple users, this is also the easiest method.
  or
- **Option 2 –** Manually configure each user account from within the Microsoft SharePoint Admin Center. If you have only a few users, this is the easiest method.

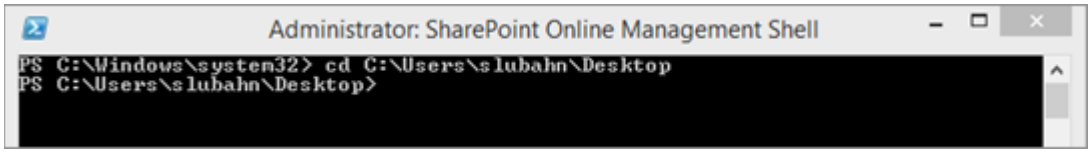
Option 1. - Configure Permissions Using a SharePoint Online Management Shell Script

1. Download and open the **AdminRights.ps1** script using a text editor such as Notepad.
2. Navigate to and edit the following four variables:

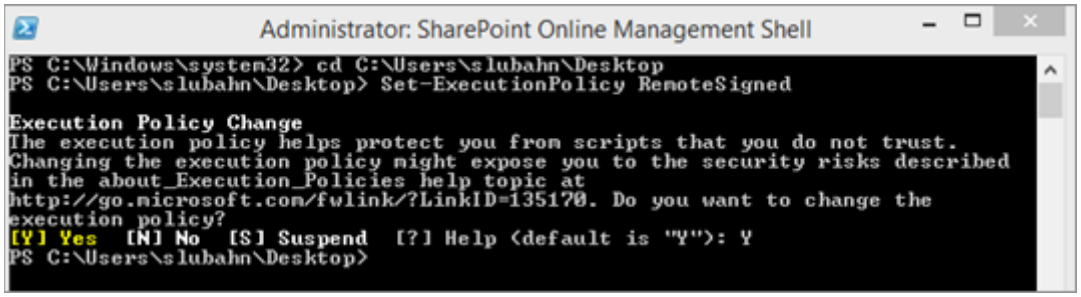


- **$o365login** – Replace with the Office365 global service account for OneDrive we previously created
- **$o365pw** – Replace with the Office365 global service account for OneDrive we previously created
- **$spAdminURL** – Replace with the same URL used in your organization's OneDrive URL, but suffixed with **-admin**
- **$spMyURL** – Replace with the same URL used in your organizations' OneDrive URL, but suffixed with **–my**

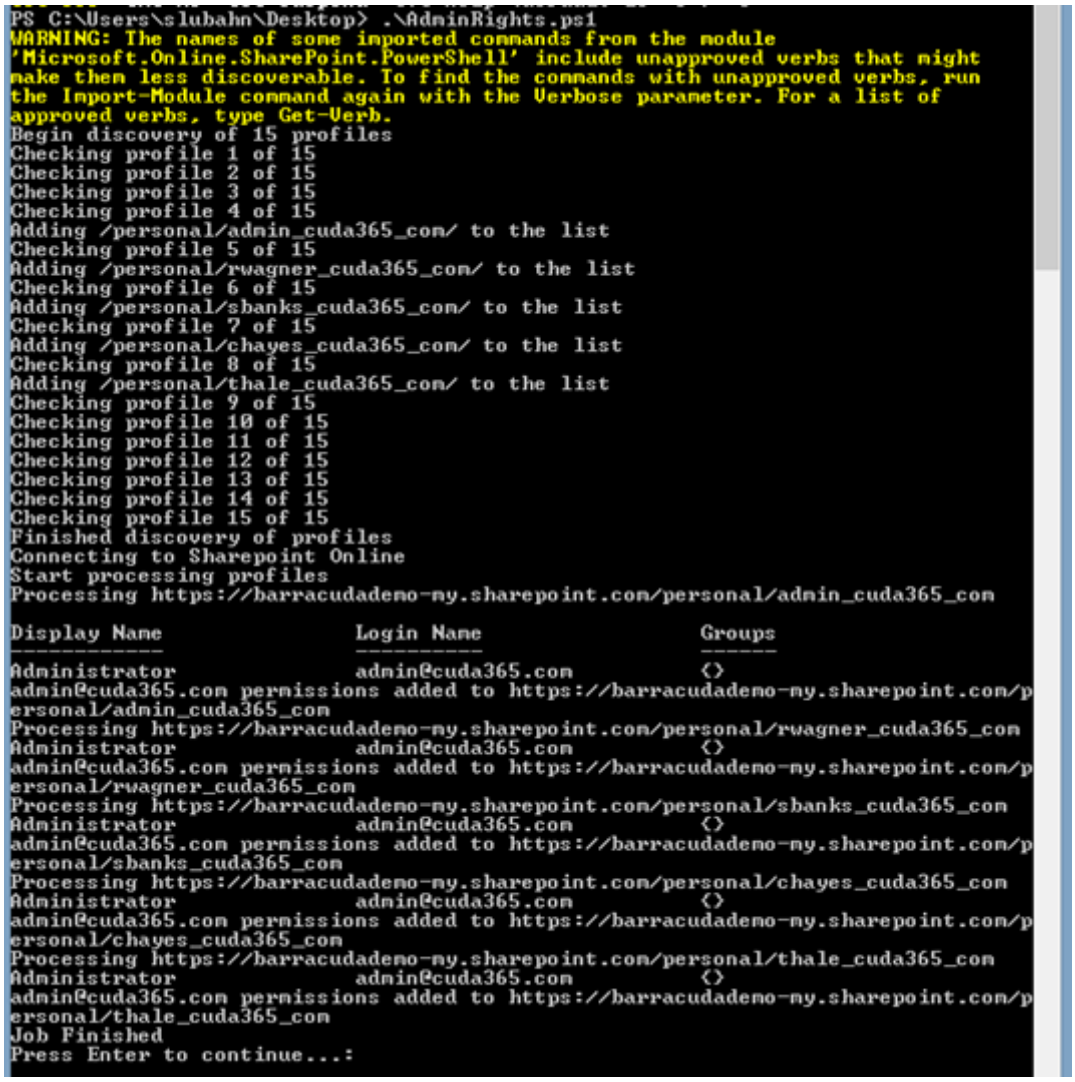
3. Save and close the script.
4. Locate the SharePoint Online Management Shell installed in *Step 1*, then right-click and click **Run as administrator**.
5. Change your working directory within the SharePoint Online Management Shell to the location where you saved the **AdminRights.ps1** script:



6. Run the following command: **Set-ExecutionPolicy RemoteSigned**
   Then enter '**Y**' for yes.



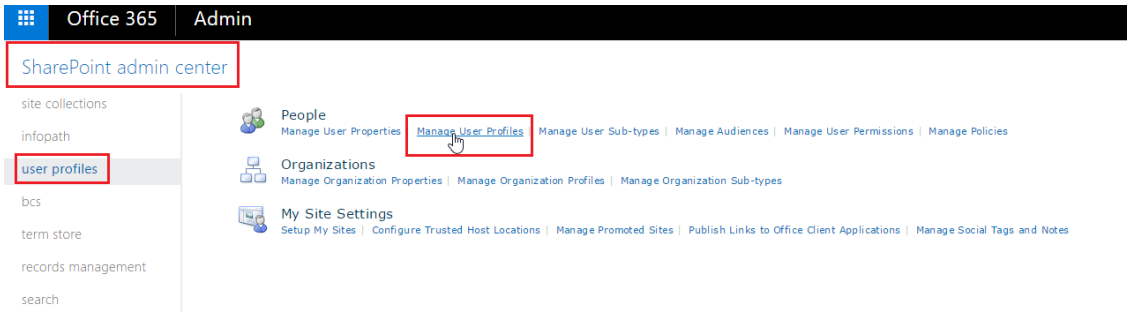
7. Run the following command to run the **AdminRights.ps1** script:
   .\AdminRights.ps1



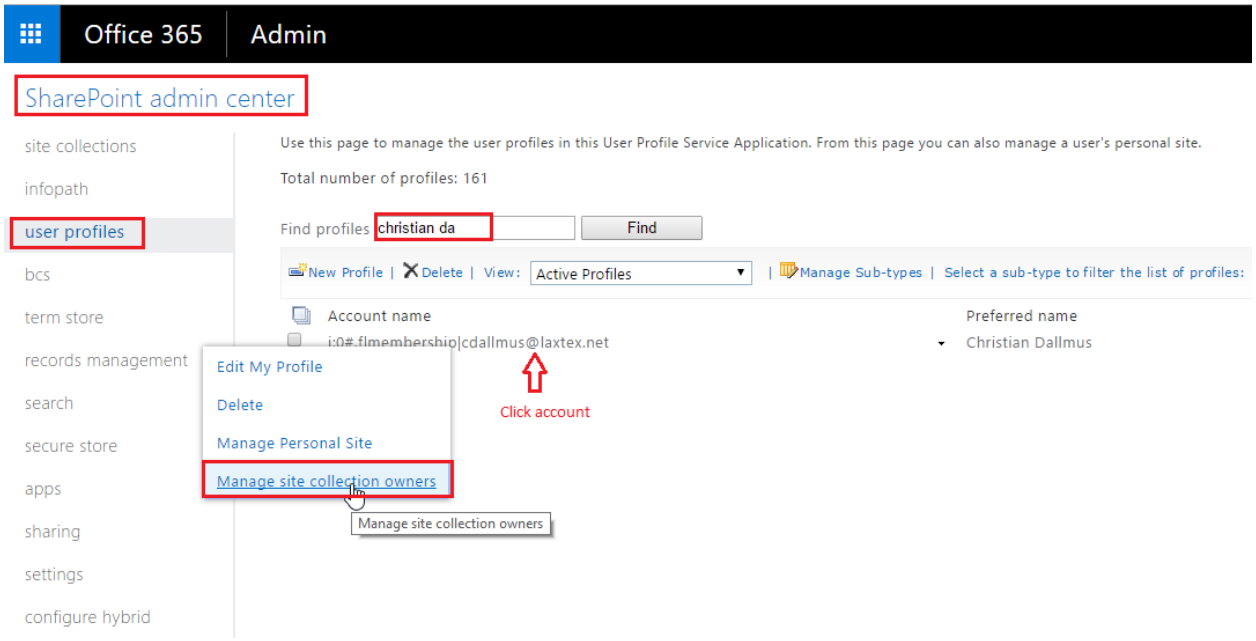
11. Press **Enter** to exit the script.
12. Exit SharePoint Online Management Shell.

Option 2 - Configure OneDrive Impersonation Manually from the SharePoint Admin Center

1. In the left pane click **Admin centers > SharePoint, and click User profiles**.
2. Click **Manage User Profiles**:



3. In the **Find profiles** field, type the name of a user who's OneDrive for Business data is to be backed up, and then click **Find:**
4. Click the user's **Account** name, and then click **Manage site collection owners**:



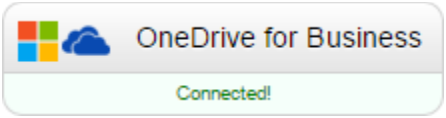
5. The **site collection owners** dialog box displays. In the **Site Collection Administrators** field, add the OneDrive service account we created earlier
6. Type the account name, and then click the **Verify User** ( ) icon, *or*
7. Click the **Directory** ( ) icon, and navigate to and select the account from the directory:

8. Click **OK**. The service account or administrative account added as the user's Site Collection Administrator can now view the user's entire OneDrive account.
9. Repeat *Steps 3 through 7* for each user who's OneDrive for Business data is to be backed up with Barracuda Cloud-to-Cloud Backup.

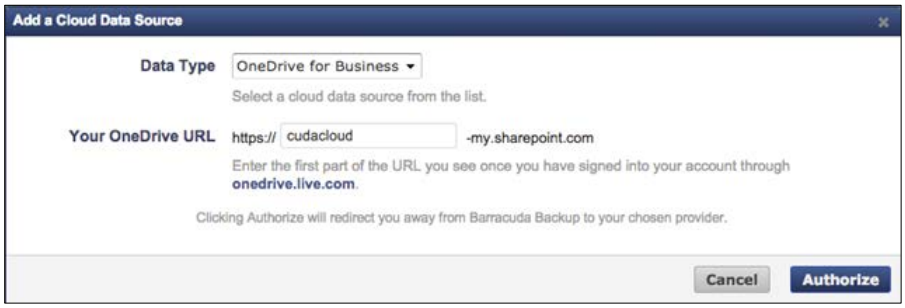
Configure OneDrive for Business Data Source

1. Log in to **BCC** > **Backup**, and select the **Cloud-to-Cloud** Backup Source in the left pane. Open a private browsing window in order to prevent cache from trying to authenticate with your admin user account.

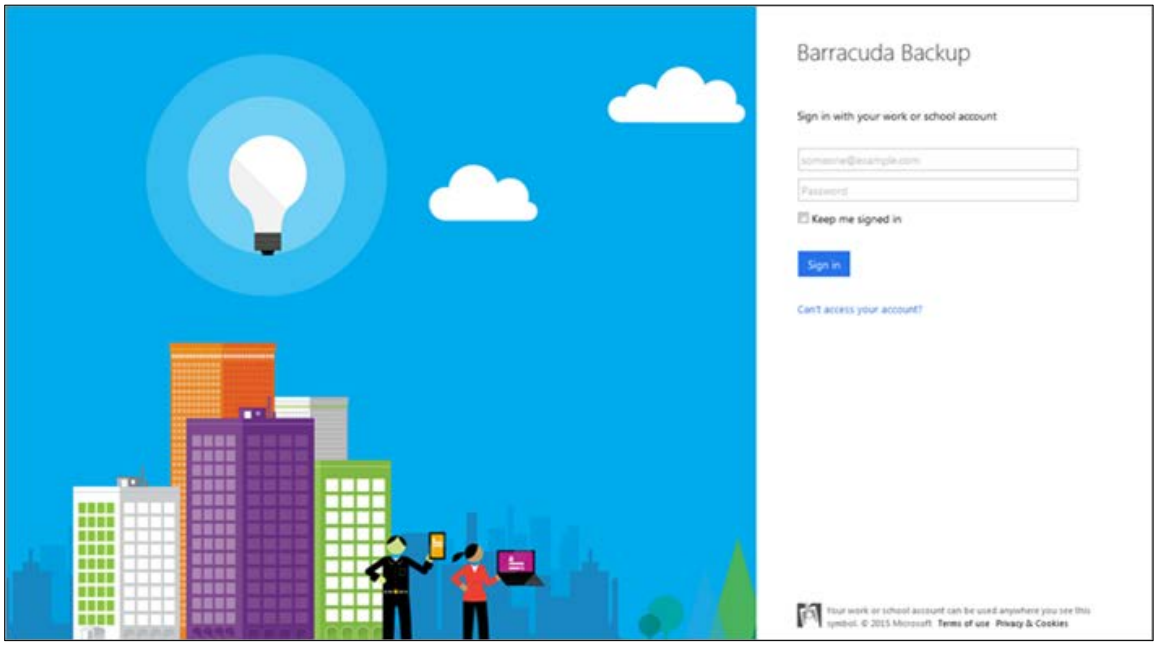
2. In the **Status** page, click **OneDrive for Business**:



3. The **Data Sources** page displays. Click **Add a data source** within the Microsoft Office365 Cloud Provider section.
4. The **Add a Cloud Data Source** page displays:
   a. From the **Data Type** drop-down menu, select **OneDrive for Business**.
   b. Enter the OneDrive URL in the associated field; the URL is available once you log in to OneDrive.
   c. Click **Authorize**:

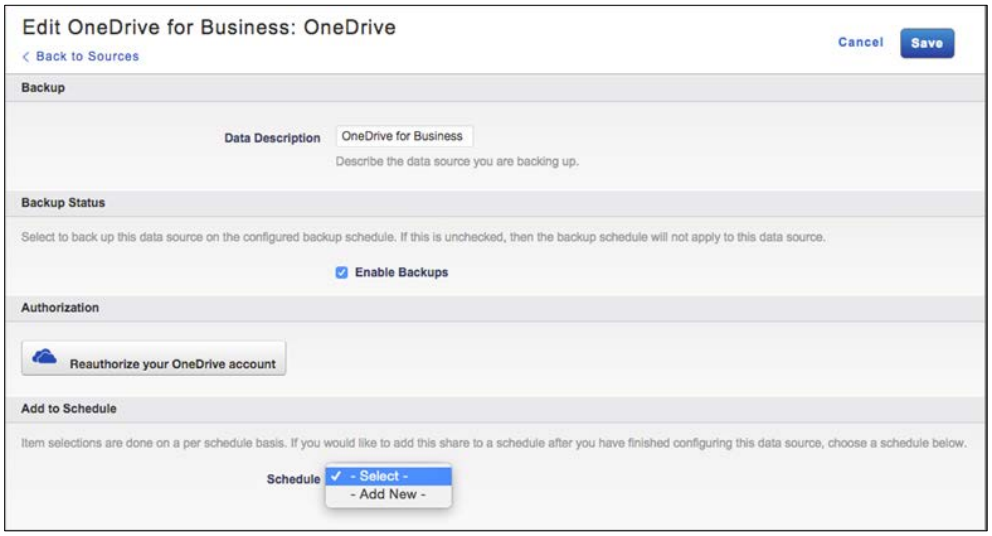


d. If you are not currently logged into the **OneDrive for Business** account, the Microsoft login page displays [****Note**:** Be careful during this step. You need to authorize with the Global Service Account for **OneDrive Backup** we just created. Click **Add another account** & enter the credentials for the **OneDrive Backup account** we created in step one]

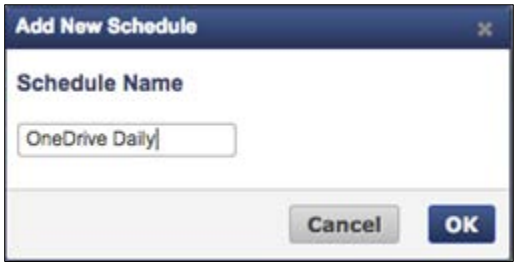


e. Enter your OneDrive for Business Global Service account login information, and then click **Sign in**. Then make sure to click the **OneDrive Backup account** once again to complete the authorization and redirect you back into the BCC portal.

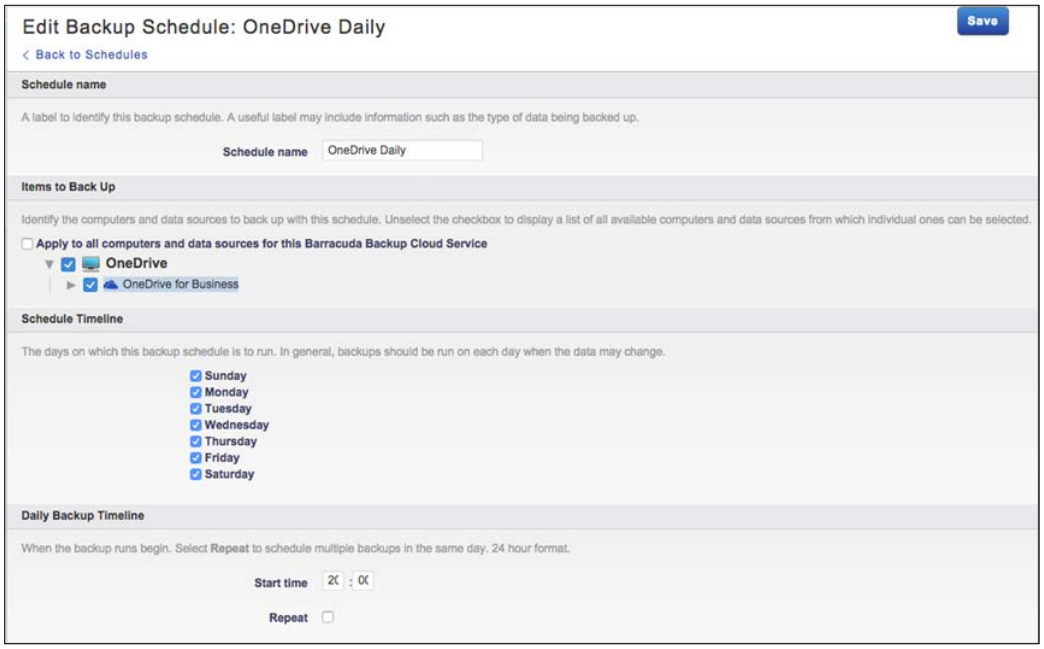
5. The **Edit OneDrive for Business** page displays.
   a. Enter a name to identify the data source in the **Data Description** field.
   b. In the **Add to schedule** section, click the drop-down menu, and then click **Add New**:



6. The **Add New Schedule** dialog box displays. Enter a name to represent the schedule:



7. Click **OK**. The **Edit OneDrive for Business** page is updated with the new schedule name.
8. Click **Save**. The **Edit Backup Schedule** page displays.
9. In the **Items to Back Up** section:
   a. Select individual items to back up, or
   b. To back up everything on OneDrive, click **Apply to all computers and data sources for this Barracuda Backup Cloud Service**.
10. In the **Schedule Timeline** section, select the day you want the schedule to run.
11. In the **Daily Backup Timeline**, specify the time of day the schedule is to run:

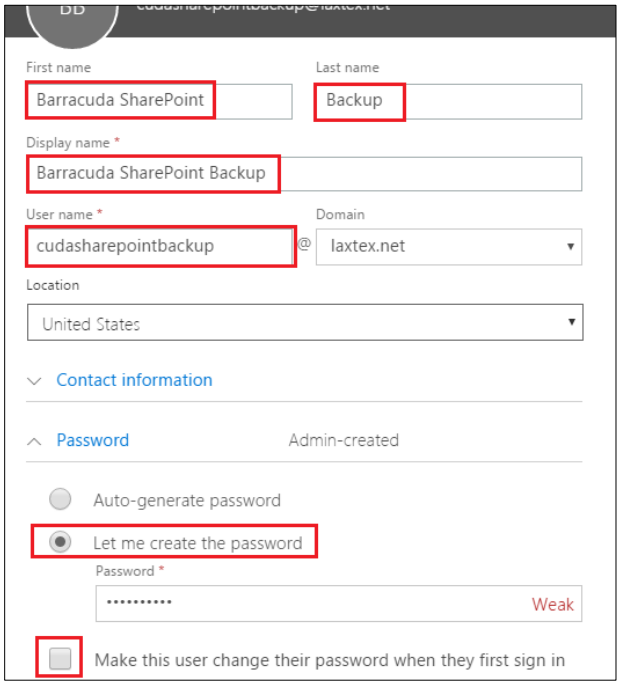


12. Click **Save.** OneDrive is backed up based on your data source and schedule settings.

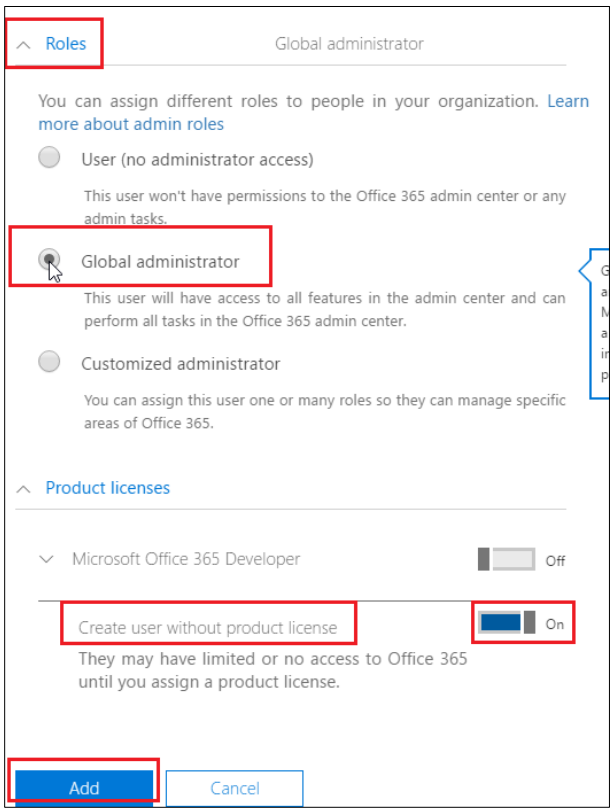
SharePoint Online

Create a Global Service Account

1. Log in to your Office365 Management Panel using an account with administrative privileges, and click **users and groups** in the left pane.
2. Click the + symbol to create a new account.
3. Enter the name for the new service account **[**take note of these details**]**
    1. **First name:** Barracuda SharePoint
    2. **Last name:** Backup
    3. **Username:** cudasharepointbackup
4. Drill into the password section, click **'Let me create the password'**, uncheck **'Make this user change their password when they first sign in'** and define a password that you will remember. **[**take note of password**]**



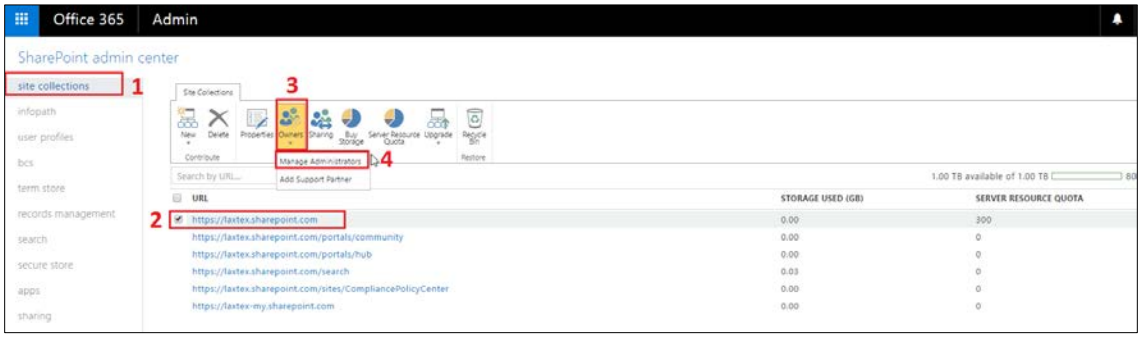
5. Drill into the **roles** section and select **global administrator**.
6. In the **product licenses** section, enabled the toggle for **'Create user without product license'**. Click **Add.**



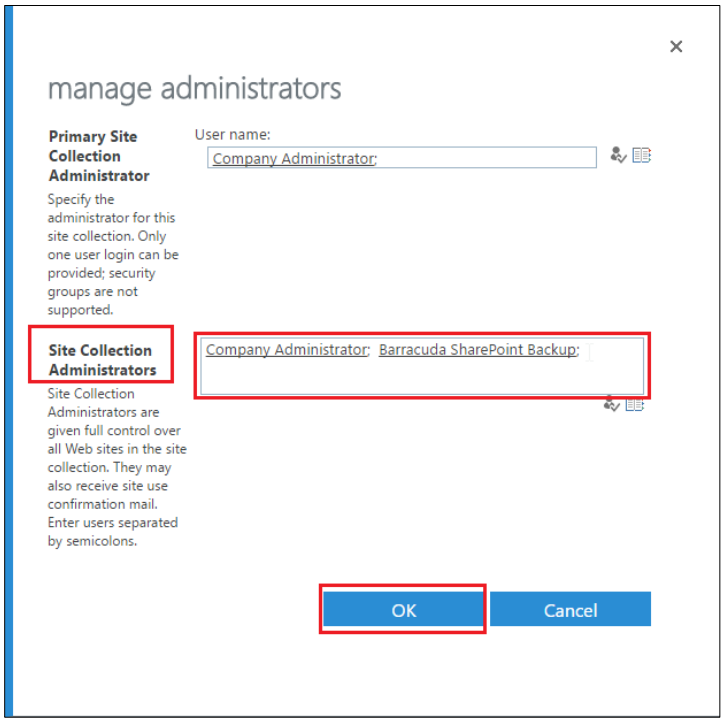
Configure Impersonation for SharePoint

Please Note: You must complete the following steps for each SharePoint Site Collection you want to back up.

1. To configure the site collection administrator for SharePoint Online:
2. Log in to your Office365 Management Panel and go to the Office365 admin center.
3. In the left pane click **Admin center for SharePoint > Site collections (1)**.
4. **Check the box (2)** next to the the site collection you want to backup.
5. Click **Owners (3) > Manage Administrators (4)**:



6. The manage administrators page displays. In the **Site Collection Administrator** section, enter the SharePoint Backup global service account we previously created in the text field, and click the Check Names ( ) icon to verify the user name is valid:

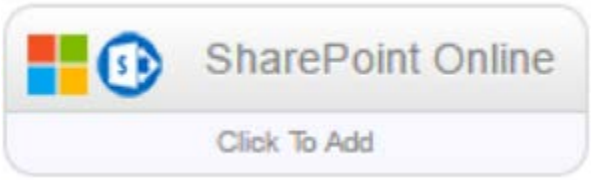


7. Click **OK** to save your changes.

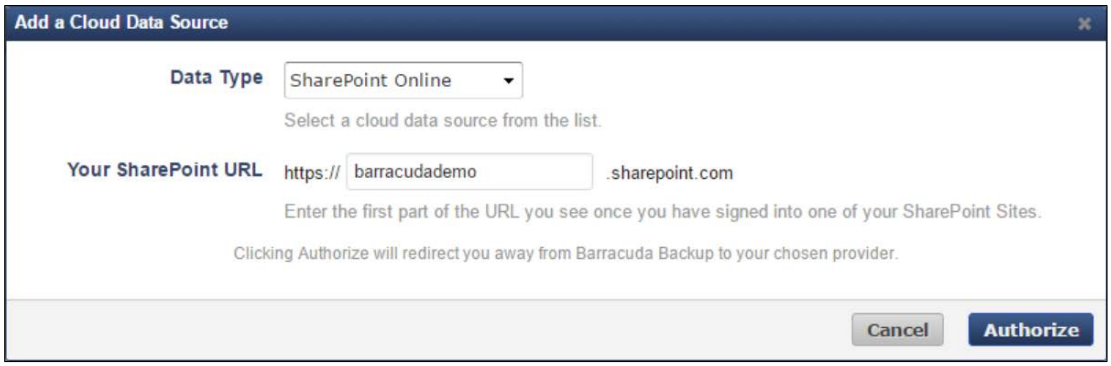
Configure SharePoint Online Data Source

Log in to **BCC** > **Backup**, and select the **Cloud-to-Cloud** Backup Source in the left pane. Open a private browsing window in order to prevent cache from trying to authenticate with your admin user account

1. Use the following steps to set up SharePoint Online backup:
2. Log in to Barracuda Backup, and select the **Cloud Source** in the left pane.
3. In the **Status** page, click SharePoint Online:

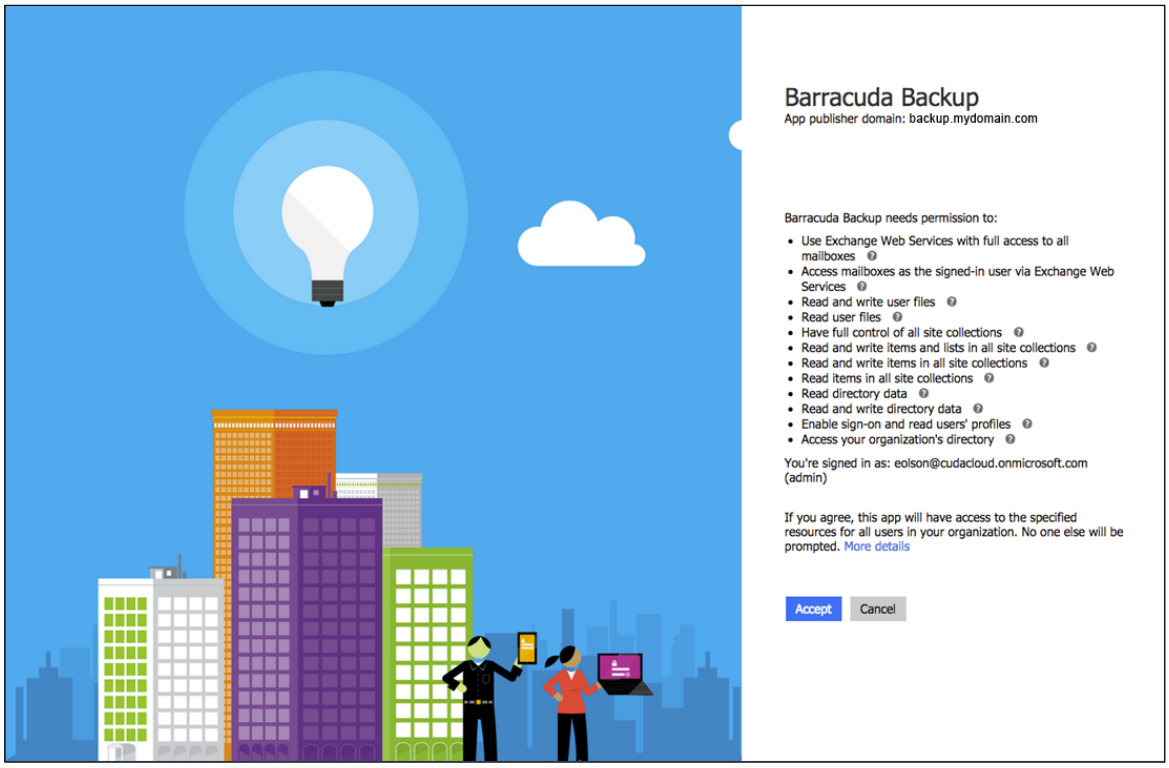


4. The **Data Sources** page displays. Click **Add a data source** within the Microsoft Office365 Cloud Provider section.
5. The **Add a Cloud Data Source** dialog box displays:
6. From the **Data Type** drop-down menu, select **SharePoint Online**.
7. Enter Your **Office365 domain** URL.
8. The URL is available once you log in to SharePoint Online.
9. Click **Authorize**.

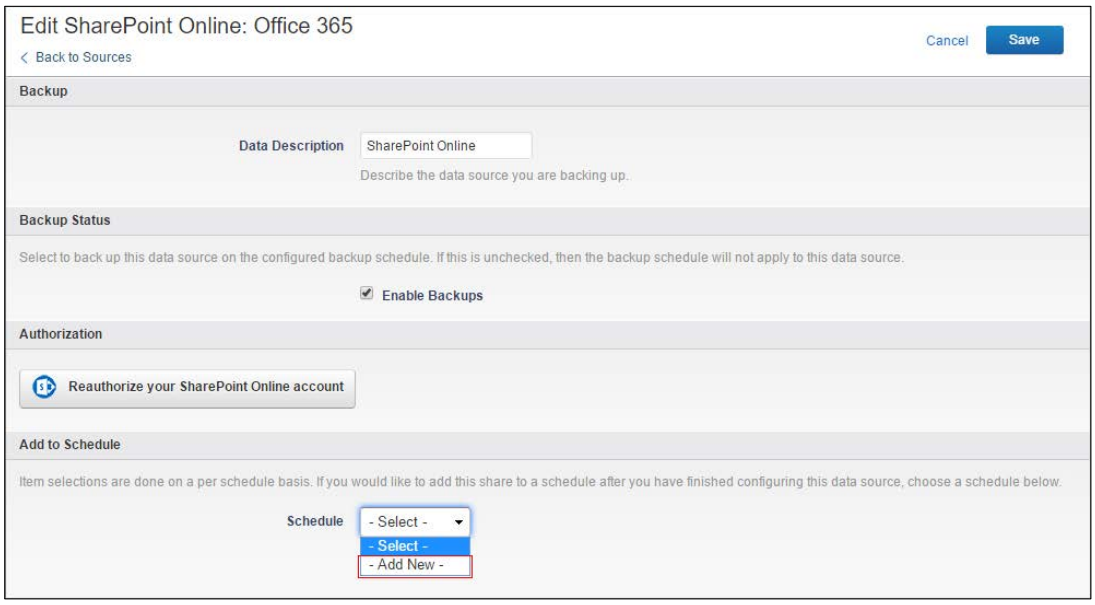


10. If you are not currently logged in to the SharePoint Online Global Service account, the Microsoft login page displays. Enter your SharePoint Online Global Service account login information, and then click Sign in. [****Note**:** Be careful during this step. You need to authorize with the Global Service Account for Sharepoint Backup we just created. Click **Add another account** & enter the credentials for the **SharePoint Backup account** we created in step one]

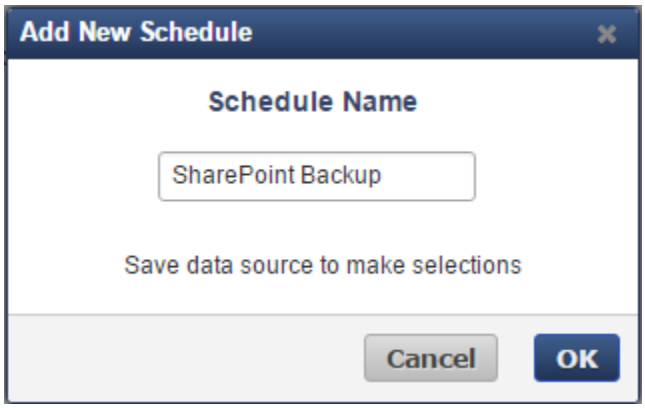
11. In the SharePoint Online page, click Accept to authorize Barracuda to back up data from SharePoint Online.
    a. Then make sure to click the **SharePoint Backup account** once again to complete the authorization and redirect you back into the BCC portal.



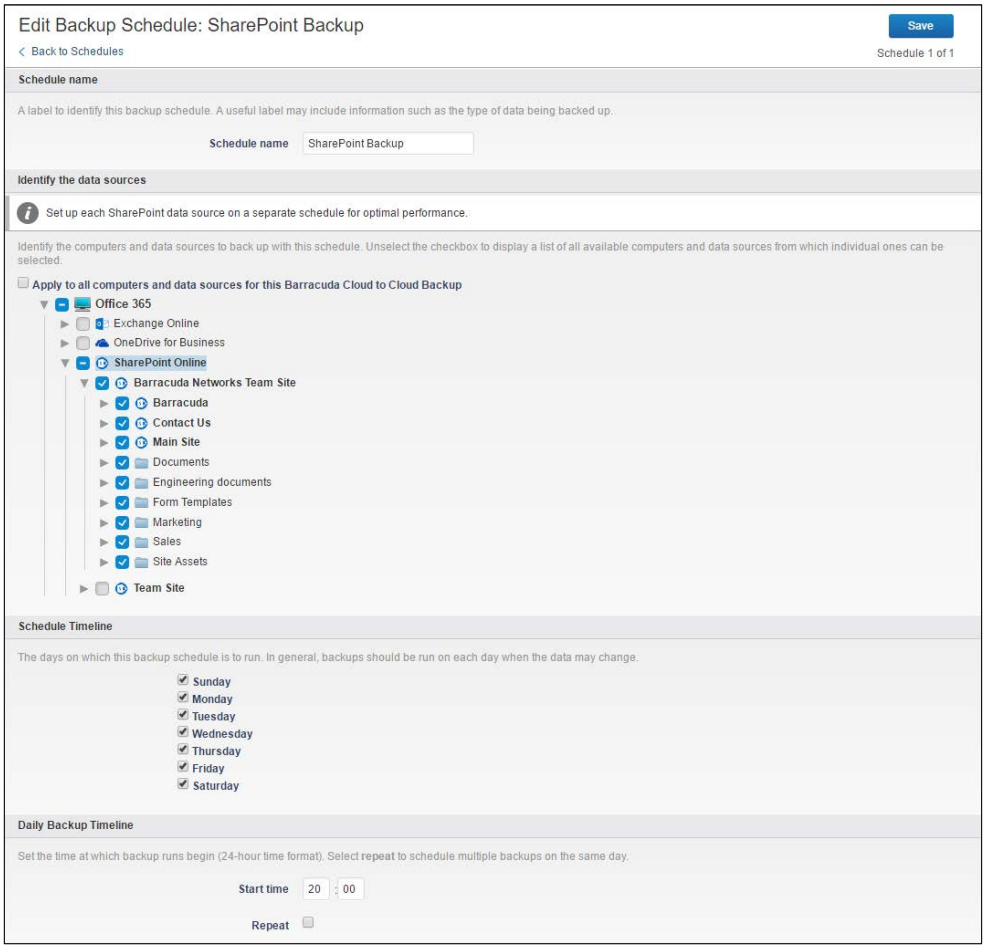
12. The Edit SharePoint Online page displays. Complete the following:
13. Enter a name to identify the data source in the Data Description field.
14. In the Add to schedule section, click the drop-down menu, and then click Add New:



15. The Add New Schedule dialog box displays. Enter a name to represent the schedule:



16. Click **OK**. The Edit SharePoint Online page is updated with the new schedule name.
17. Click **Save.** The Edit Backup Schedule page displays.
18. In **the Items to Back Up** section, select individual items to back up, or click **Apply to all computers and data sources** for this Barracuda Backup Cloud Service to back up everything in SharePoint Online.
19. In the **Schedule Timeline** section, select the day you want the schedule to run.In the **Daily Backup Timeline**, specify the time of day the schedule is to run:

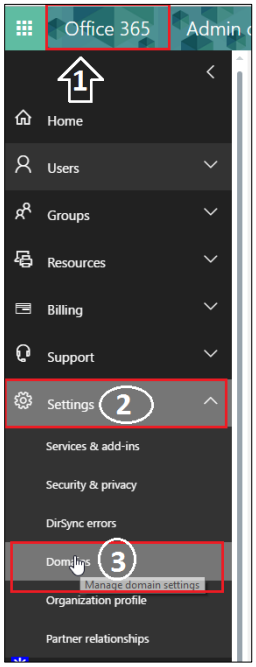


20. Click **Save**. SharePoint Online is backed up based on your data source and schedule settings.

Appendix 1 – How to locate your Office365 domain or mail server

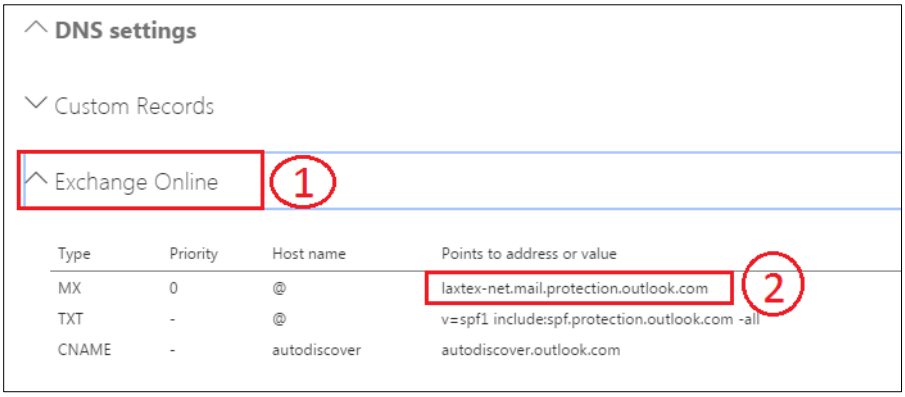
The steps below will show you how to locate your customer's Office365 domain & mail server in order to help facilitate the deployment for Email Security.

1. Login to your customer's **Office365 Portal**, then going to the **Admin Center (1)** and click on **Settings (2) > Domains (3)**.



2. Once loaded click on the customer's domain. Make sure to select "customerdomain.com" & not the 'customerdomain.onmicrosoft.com'.

3. Drill into the **DNS settings**, then drill into the **Exchange Online** section. Copy the MX record 'Points to address of value' to clipboard, this is their mail server:
   a. i.e. **<domain>-com.mail.protection.outlook.com**



Appendix 2 – How to configure LDAP for Barracuda Cloud Archiving Service (BCAS)

The steps below walk you through the configuration for LDAP AD integration using the Initials Setup wizard.

1. The **Directory Services** page displays. Use this page to set up LDAP authentication to store and administer Barracuda Cloud Archiving Service user accounts via your organization's LDAP servers.
2. Click **Verify** to add your LDAP servers to your Barracuda Cloud Control account.
   a. *If you do not wish to set up LDAP authentication at this time, click Skip. You can continue setting up the Barracuda Cloud Archiving Service without setting up LDAP authentication. [Skip ahead to step 19]*
3. If you are adding your LDAP servers, the **ADMIN > Options** page displays in Barracuda Cloud Control.
4. In the **Your Domains** section, click **Add a Domain** to open the setup dialog, and enter your **Domain** name.
5. Click **Add Domain**; the domain is added to the **Domains** field. Click **Verify**.
6. In the **Verify a Domain** dialog, select the manner in which to verify the domain:
   a. **Option 1** – Copy the META tag to your site header, *or*
   b. **Option 2** – Add the TXT record to your domain host's DNS management settings
7. Scroll to the **LDAP Settings** section, and click **Add a BaseDN**; the **Edit LDAP Settings** dialog displays.
8. Enter your LDAP details, and select the **Connection Security** setting: **STARTTLS**, **LDAPS**, or **None**. Click **Save** to add your LDAP settings.
9. Scroll to the **LDAP Hosts** section, and click **Add an LDAP Host**. The **Add an LDAP Host** dialog box displays. Enter the **Server Hostname** and associated **Port** number, and click **Save** to add your LDAP Host settings.
10. Scroll to the **Administrator Contact** section, and click **Add Contact Information**; the **Add Administrative Contacts** dialog box displays.
11. Enter the administrator name and contact email address to which users can send requests for help with LDAP issues, and click **Save**. The contact is added to the **Administrator Contact** section.
12. At the top of the page, toggle LDAP Authentication to **ON**, and click **Test LDAP Connection**. If the connection is successful, the **Successfully connected to LDAP host** message displays.
13. Click **Continue**. LDAP Groups are now enabled and Barracuda Cloud Control begins synchronizing with your LDAP environment.
14. Scroll to the LDAP Groups section, and click **Enable LDAP Groups**; the **Enable LDAP Groups** dialog box displays.
15. In the left pane, click **Archiver** to return to the **Setup Wizard**. Click **Next** in the **Directory Services** page.