

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





Table of Contents

Understanding the Barracuda Cloud Control (BCC) as an MSP	1
Overview	1
Email Security Service.....	2
Overview	2
Pre-requisites.....	2
Inbound Scanning Setup	2
Add a Domain to Barracuda Cloud Control	2
Best Practice Recommendations	7
Configure Advanced Threat Protection	7
Enable Email Continuity	7
Enable Inbound Quarantine	8
Update Office 365 SPAM Policies	9
Outbound Scanning (Optional)	10
Send Connector	11
Encryption (Optional)	16
Overview	16
Final Deployment Steps	18
Barracuda Cloud Archiving Service	19
Overview	19
Pre-requisites.....	19
Add archiving domain to BCC	19
Configuring Journal Archiving for Office365	19
Add a Remote Domain.....	19
Add a Send Connector	20
Create a Non-Delivery Report Recipient	25
Configure Office365 to Journal Mail.....	26
Configure Exchange Integration	27
Exchange Database: Historical Import	28
Exchange Non-Email Sync	33
Exchange Folder Structure Sync.....	35
PST Import.....	36
Cloud to Cloud Backup.....	37



Overview	37
Pre-requisites:	37
Exchange Online	37
Create a Global Service Account	37
Configure Application Impersonation for Exchange Online	39
Configure Exchange Online Data Source	40
OneDrive for Business	43
Create a Global Service Account	43
Configure Permissions for OneDrive for Business	44
Configure OneDrive for Business Data Source	48
SharePoint Online	51
Create a Global Service Account	51
Configure Impersonation for SharePoint	53
Configure SharePoint Online Data Source	54
Appendix 1 – How to locate your Office365 domain or mail server.....	58
Appendix 2 – How to configure LDAP for Barracuda Cloud Archiving Service (BCAS) ..	59



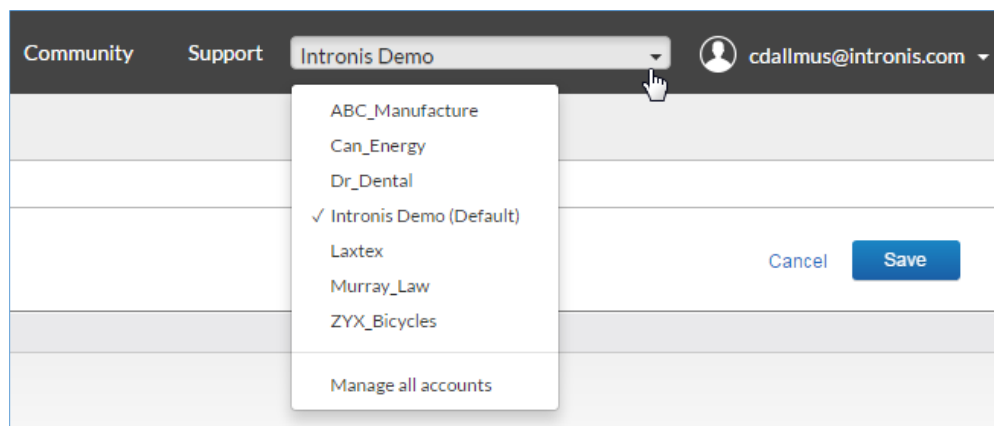
Understanding the Barracuda Cloud Control (BCC) as an MSP

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.

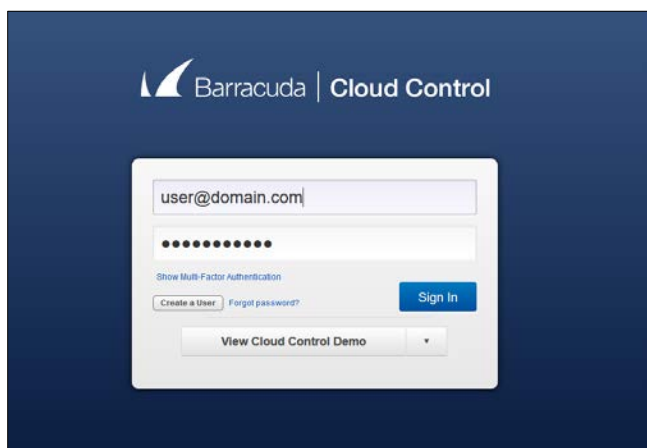
- **Access & Credentials to <https://login.barracuda.com> (Barracuda Cloud Control or BCC)** – The username is contained in the provisioning activation email sent from Intronis. You can manually reset your password directly in the BCC portal using the ‘forgot password’ link.
- **Customer’s domain and 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

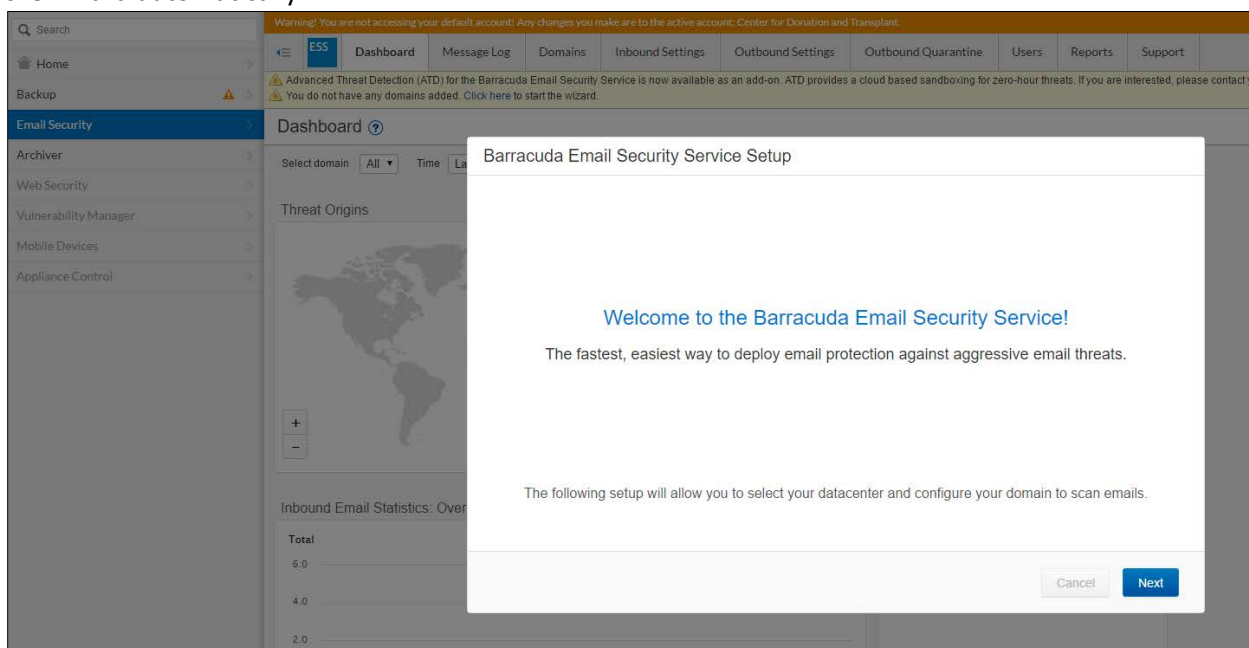
During this step we will configure the customer’s primary domain for BESS. This will be done using the BESS wizard. You will want to have the client’s domain & mail server information for this step.

Add a Domain to Barracuda Cloud Control

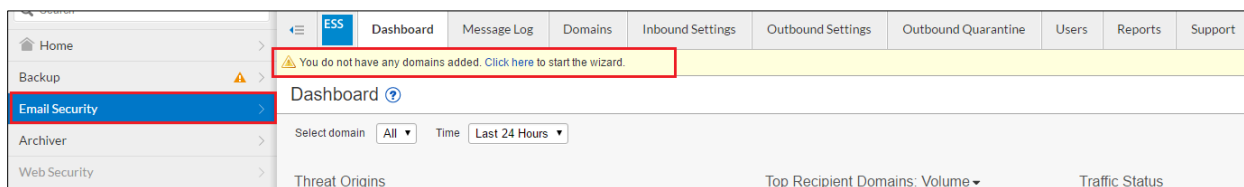
1. **Login** to the BCC (<https://login.barracuda.com>) console. Please note that if you’ve never logged into BCC before, you need to click ‘forgot password’ to create your password.



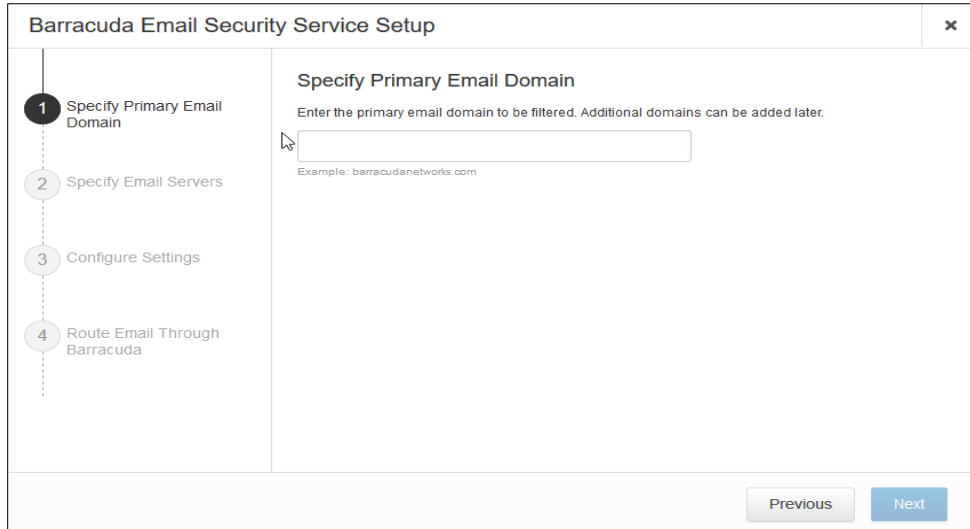
2. Click on **Email Security** from the left hand menu.
3. If this is your first time logging into a customer's Email Security service, you will be prompted with the wizard automatically:



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.



Barracuda Email Security Service Setup

1 Specify Primary Email Domain

Specify Primary Email Domain

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

Example: barracudanetworks.com

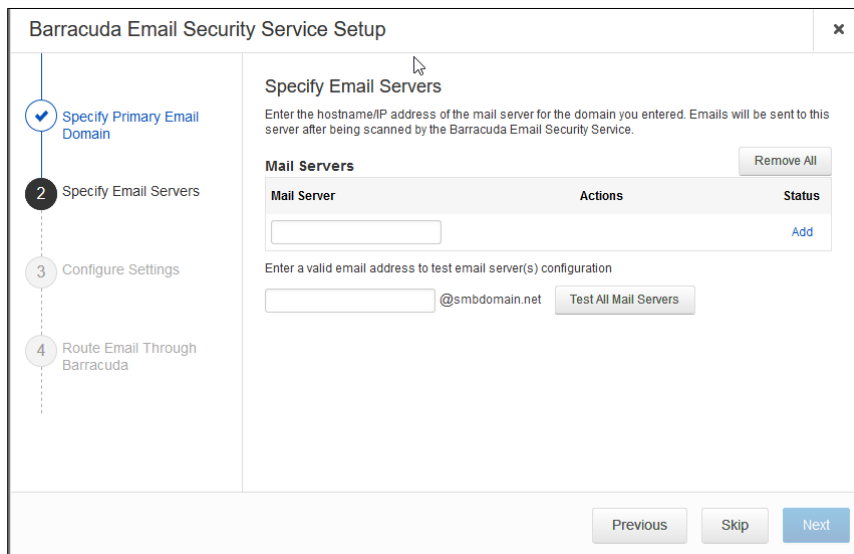
2 Specify Email Servers

3 Configure Settings

4 Route Email Through Barracuda

Previous Next

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**.



Barracuda Email Security Service Setup

Specify Email Servers

Enter the hostname/IP address of the mail server for the domain you entered. Emails will be sent to this server after being scanned by the Barracuda Email Security Service.

Mail Servers Remove All

Mail Server	Actions	Status
<input type="text"/>		Add

Enter a valid email address to test email server(s) configuration

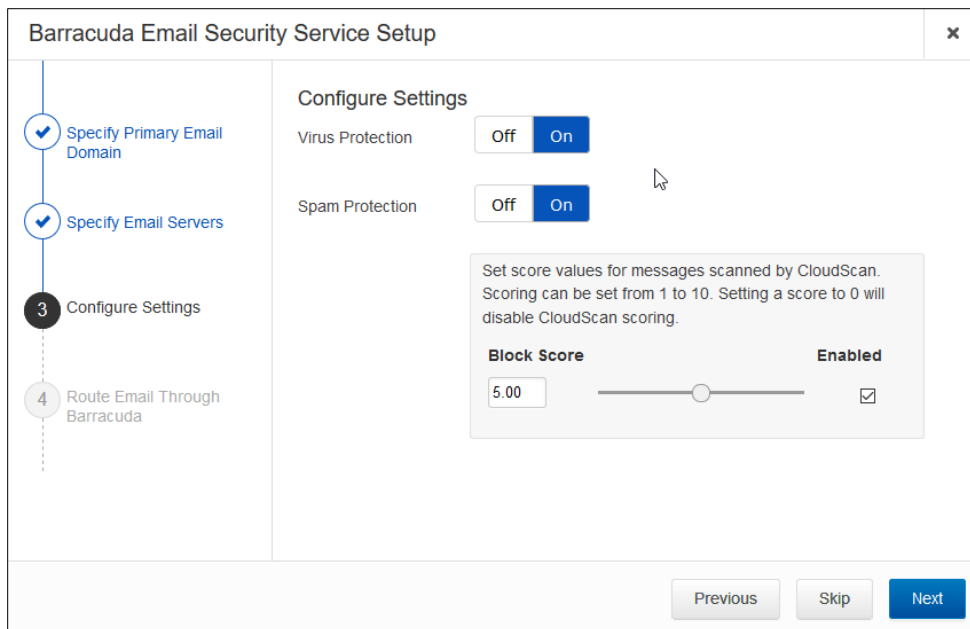
@smbdomain.net Test All Mail Servers

Previous Skip Next

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.



Barracuda Email Security Service Setup

✓ Specify Primary Email Domain

✓ Specify Email Servers

✓ [Configure Settings](#)

4 Route Email Through Barracuda

Route Email Through Barracuda

[\(Click here for more details \)](#)

MX Records

To Verify your domain and begin using the Barracuda Email Security Service, please change your MX records to the following:

Primary: `d110143a.ess.barracudanetworks.com`

Backup: `d110143b.ess.barracudanetworks.com`

[Verify MX Records](#)

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

[Previous](#) [Skip](#) [Next](#)

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

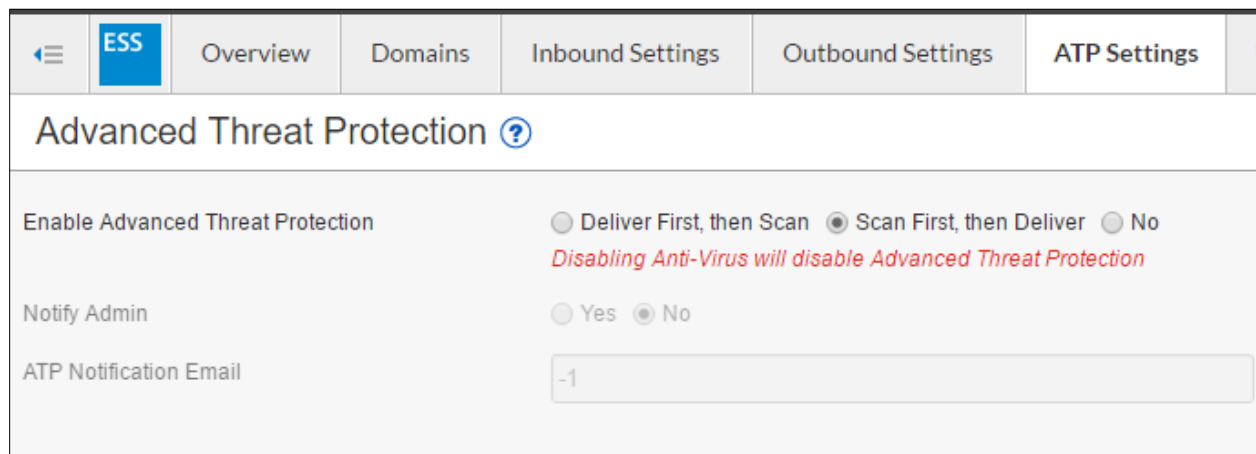
Best Practice Recommendations

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.



ESS		Overview	Domains	Inbound Settings	Outbound Settings	ATP Settings
Advanced Threat Protection ?						
Enable Advanced Threat Protection	<input type="radio"/> Deliver First, then Scan <input checked="" type="radio"/> Scan First, then Deliver <input type="radio"/> No <i>Disabling Anti-Virus will disable Advanced Threat Protection</i>					
Notify Admin	<input type="radio"/> Yes <input checked="" type="radio"/> No					
ATP Notification Email	<input type="text" value="-1"/>					

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.



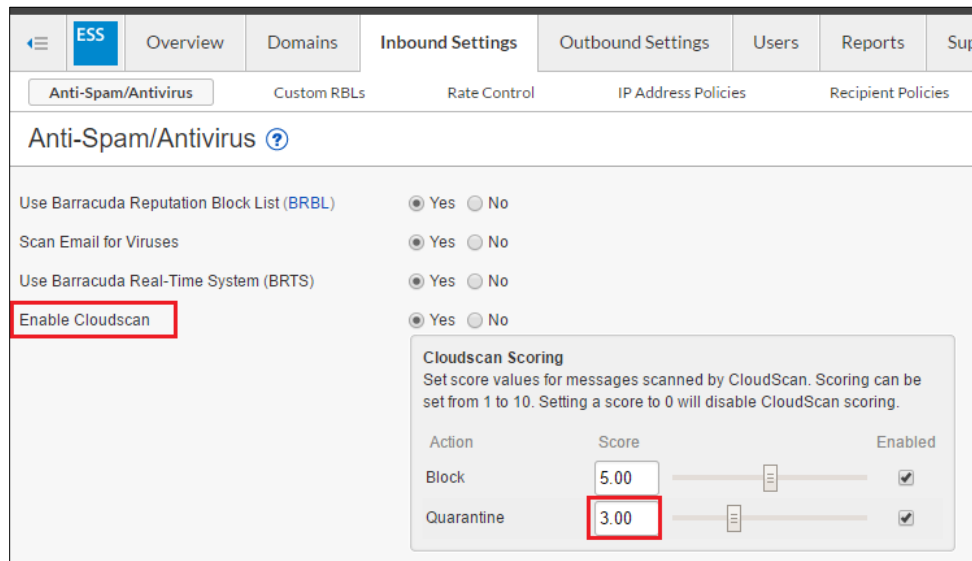
The screenshot shows the Intronis ESS interface. The top navigation bar includes tabs for Overview, Domains, Inbound Settings, Outbound Settings, Users, Reports, and Support. The 'Email Continuity' tab is active. Below the navigation bar, there are links for Users List, Default Policy, Add/Update Users, Quarantine Notification, and Email Continuity. The Email Continuity section contains a description: 'Allows end users the ability to receive and send emails when designated mail servers are unavailable. Email Continuity service will auto-'. Below this, there are two radio buttons: 'Off' and 'Auto-Enable'. The 'Auto-Enable' radio button is selected and highlighted with a red box. Below the radio buttons, a modal dialog titled 'Enable Spooling' is displayed. The dialog contains a warning icon and the text: 'Using the Auto-Enable feature for Email Continuity will enable spooling for all of the domains associated with this account.' At the bottom of the dialog, there are two buttons: 'Cancel' and 'OK'. The 'OK' button is highlighted with a red box.

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.



Anti-Spam/Antivirus ?

Use Barracuda Reputation Block List (BRBL) ☒ Yes ☐ No

Scan Email for Viruses ☒ Yes ☐ No

Use Barracuda Real-Time System (BRTS) ☒ Yes ☐ No

Enable Cloudscan ☒ Yes ☐ No

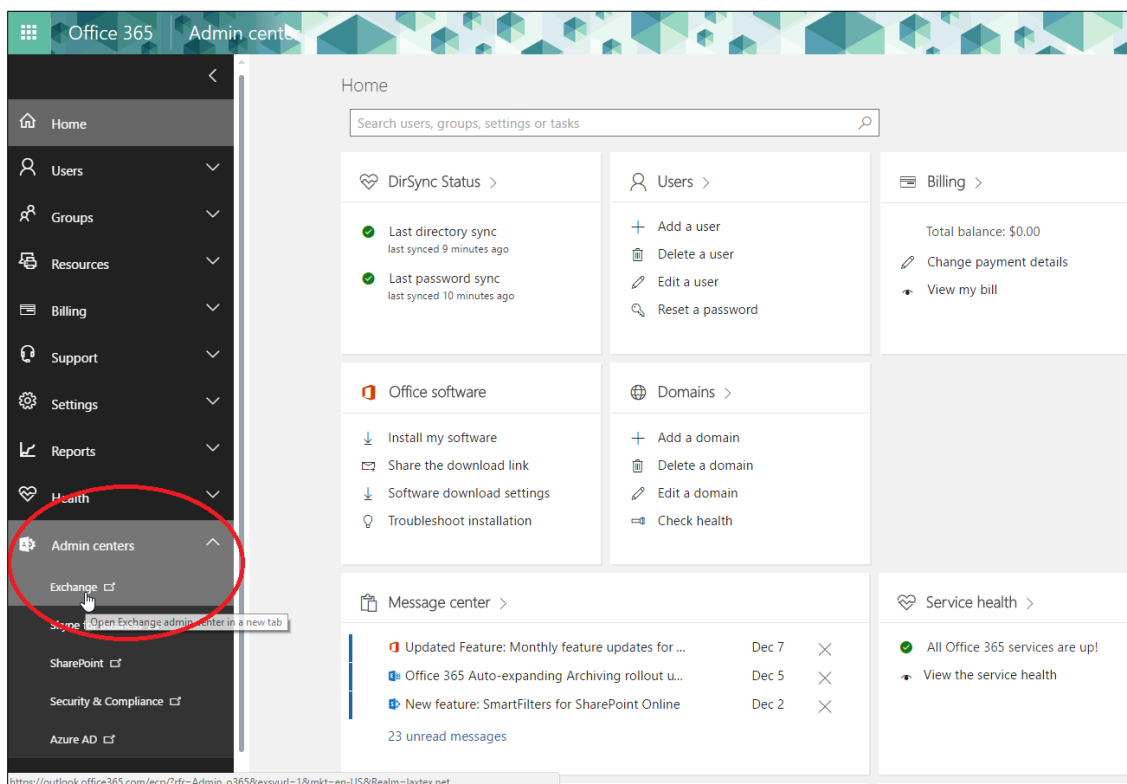
Cloudscan Scoring
Set score values for messages scanned by CloudScan. Scoring can be set from 1 to 10. Setting a score to 0 will disable CloudScan scoring.

Action	Score	Enabled
Block	5.00	<input checked="" type="checkbox"/>
Quarantine	3.00	<input checked="" type="checkbox"/>

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

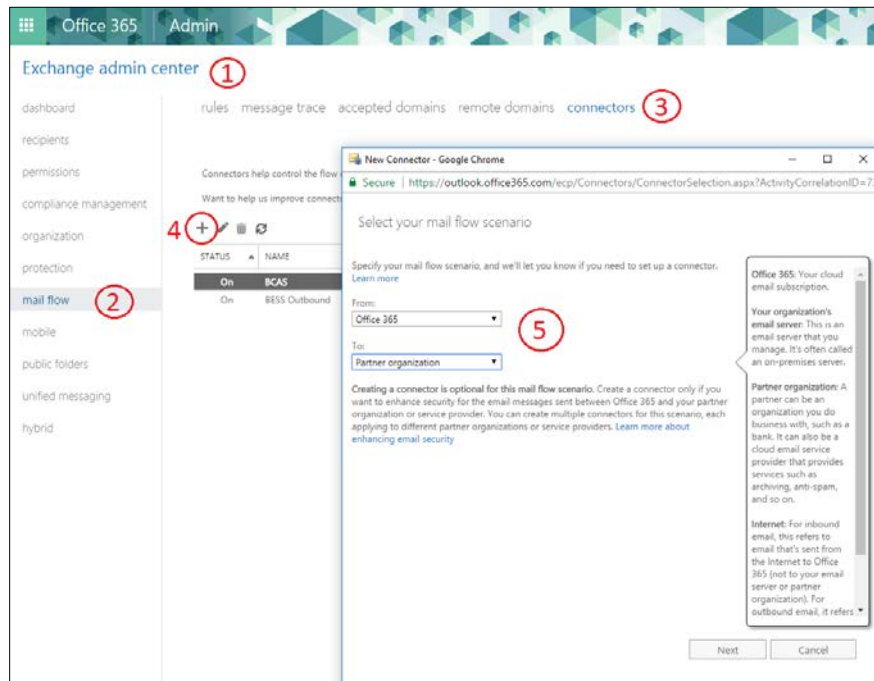
We will add an outbound send connector within Office365 to route outbound mail through a Barracuda smart host.

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.

ESS	Overview	Domains	Inbound Settings	Outbound Settings	ATP Settings	Users	Reports	Support
Domains Manager ? 1								
Domain Name ^	Aliases	Recipients (Last 30 days)	Mail Servers	Settings	Domain Options			
✓ laxtex.net 2	0	3	laxtex-net.mail.protect...	Edit	Manage	Remove		
MX Records Configuration		Aliases	Email Continuity	Domain Specific Policies				
Primary:		None	Disabled	Account Policies				
Backup:								
d118151a.ess.barracudanetworks.com								
d118151b.ess.barracudanetworks.com								
Outbound:								
d118151.o.ess.barracudanetworks.com								

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.



New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partner

New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

*Name:
BESS outbound

Description:

What do you want to do after connector is saved?
☒ Turn it on

Select this check box to start using this connector immediately after it's saved. Don't select it if you want to keep this connector in test mode. You'll be able to turn it on later.

Next Cancel

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

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partne

New connector

When do you want to use this connector?

☐ Only when I have a transport rule set up that redirects messages to this connector

☒ Only when email messages are sent to these domains

+
Add



New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partne

add domain

Specify the domain name, with or without wildcards.
Example: * or *.contoso.com or *.com

Specify the fully qualified domain name. Example: myhost.contoso.com

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.

New connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partne

New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

☐ Use the MX record associated with the partner's domain

☒ Route email through these smart hosts

+ Add

Back Next Cancel



New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partne

add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
Example: myhost.contoso.com or 192.168.3.2

d23092.o.ess.barracudanetworks.com

Save Cancel

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)”.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partne

New connector

How should Office 365 connect to your partner organization's email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☐ Any digital certificate, including self-signed certificates

☒ Issued by a trusted certificate authority (CA)

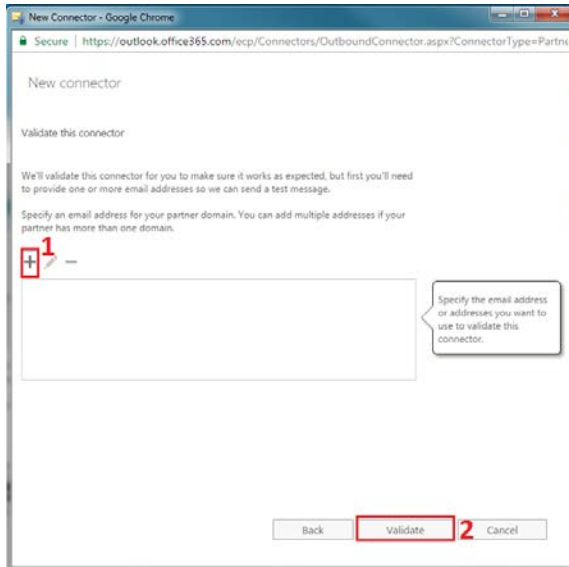
☐ And the subject name or subject alternative name (SAN) matches this domain name:
Example: contoso.com or *.contoso.com

TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.

Back Next Cancel

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.

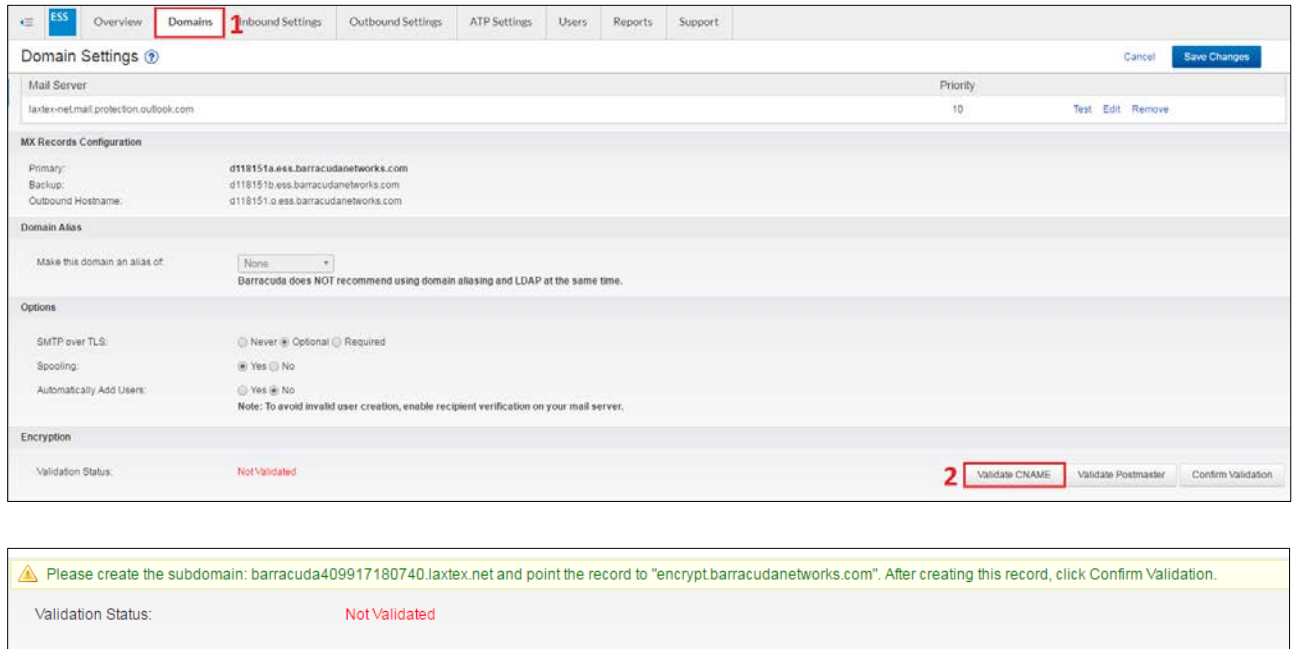
Encryption (Optional)

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**

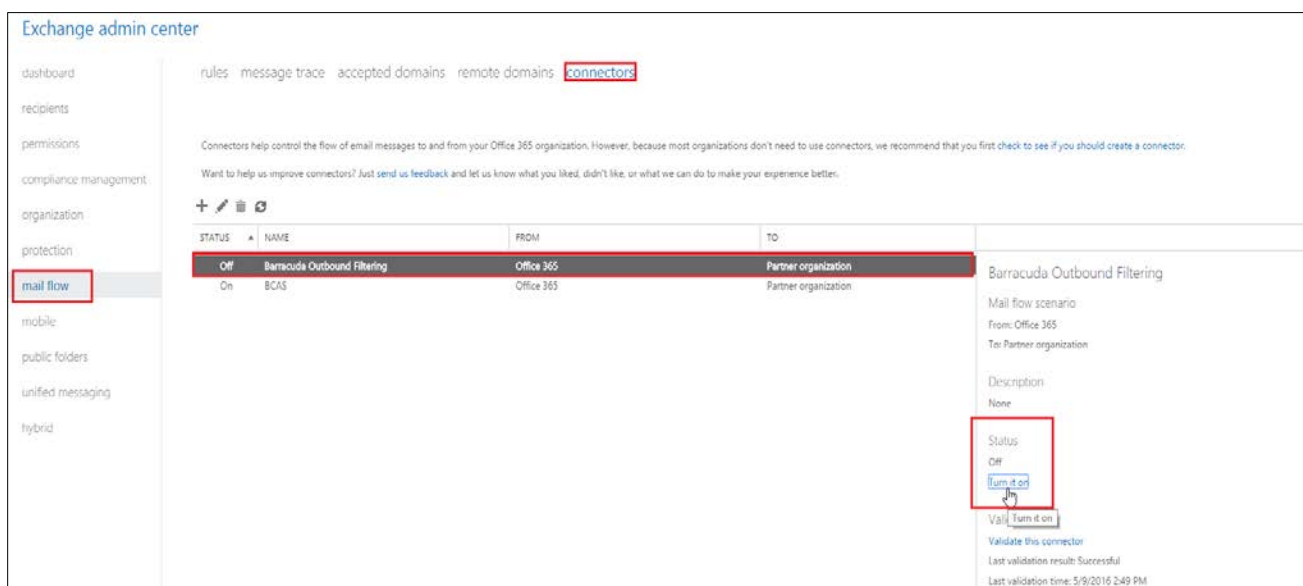
Please Note: Allow the DNS propagation to take effect before proceeding – this can take up to 24 hours for some providers.

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'



Exchange admin center

rules message trace accepted domains remote domains **connectors**

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first check to see if you should create a connector.

Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS	NAME	FROM	TO
Off	Barracuda Outbound Filtering	Office 365	Partner organization
On	BCAS	Office 365	Partner organization

Barracuda Outbound Filtering

Mail flow scenario

From: Office 365

To: Partner organization

Description

None

Status

Off

Turn it on

Validate this connector

Last validation result: Successful

Last validation time: 5/9/2016 2:49 PM



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**

https://outlook.office365.com/ecp/RemoteDomain/NewRemoteDo

new remote domain

Specify a domain that will be considered remote when mail is received.

*Name:
Barracuda Cloud Archiving Service

*Remote Domain:
mas.barracudanetworks.com

Out of Office automatic reply types:
☒ None
☐ Allow only external Out of Office replies
☐ Allow internal Out of Office replies

Automatic replies:
☐ Allow automatic replies
☒ Allow automatic forwarding

Message reporting:
☐ Allow delivery reports
☐ Allow non-delivery reports
☐ Allow meeting forward notifications

Use rich-text format:
☐ Always
☒ Never
☐ Follow user settings

Supported Character Set
MIME character set:
None

Non-MIME character set:
None

Save Cancel

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**:

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:
Office 365 ▼

To:
Partner organization ▼

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

Next Cancel

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:



New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

*Name:
Barracuda Cloud Archiving Service

Description:

What do you want to do after connector is saved?
☒ Turn it on

Next Cancel

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]**



add domain

Specify the domain name, with or without wildcards.
Example: * or *.contoso.com or *.com

mas.barracudanetworks.com

OK Cancel

6. Click **OK**:

New connector

When do you want to use this connector?

☐ Only when I have a transport rule set up that redirects messages to this connector

☒ Only when email messages are sent to these domains

+ -

mas.barracudanetworks.com

Back Next Cancel



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

New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

☒ Use the MX record associated with the partner's domain

☐ Route email through these smart hosts

+ - x

Back Next Cancel

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

New connector

How should Office 365 connect to your partner organization's email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☒ Any digital certificate, including self-signed certificates

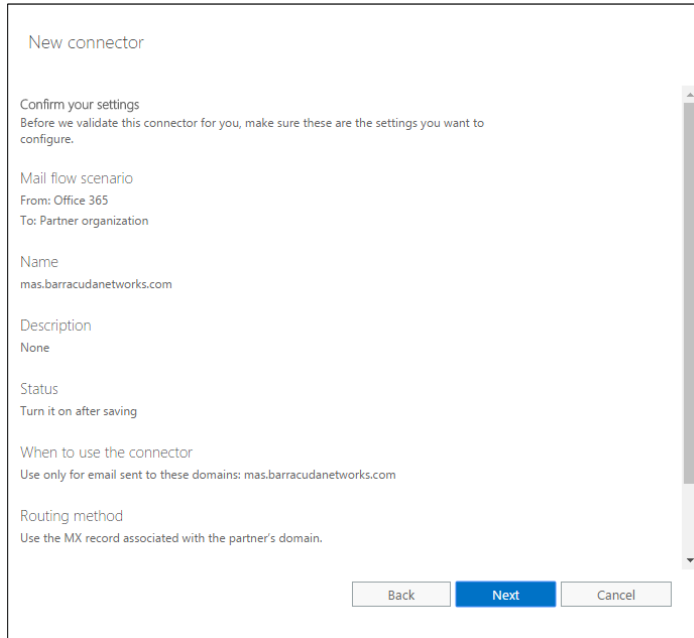
☐ Issued by a trusted certificate authority (CA)

☐ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or *.contoso.com

Back Next Cancel

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



New connector

Confirm your settings
Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario
From: Office 365
To: Partner organization

Name
mas.barracudanetworks.com

Description
None

Status
Turn it on after saving

When to use the connector
Use only for email sent to these domains: mas.barracudanetworks.com

Routing method
Use the MX record associated with the partner's domain.

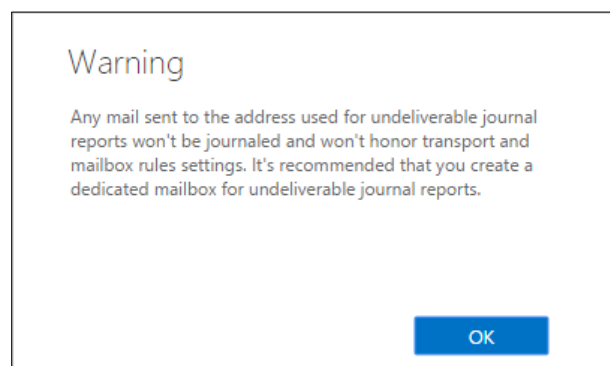
Back Next Cancel

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

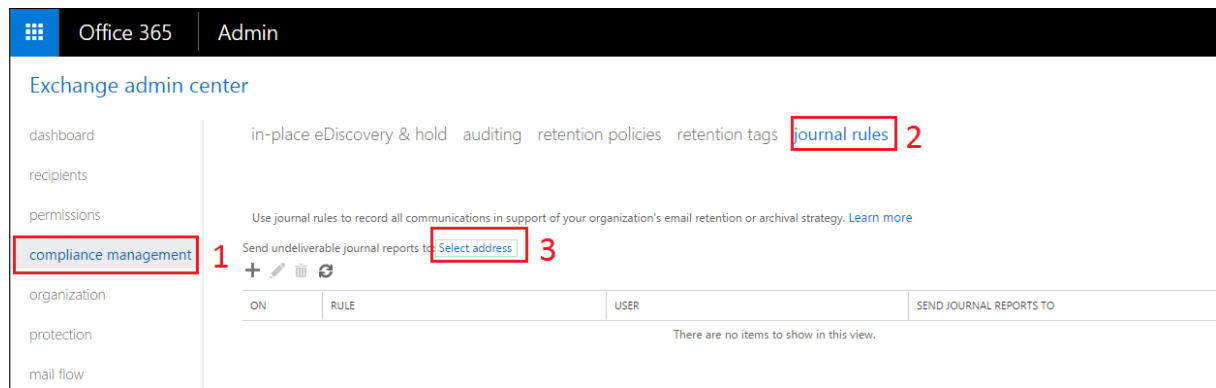
Before creating journal rules, specify a journal recipient for non-delivery reports (NDRs) to reduce the risk of losing journal reports.

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:



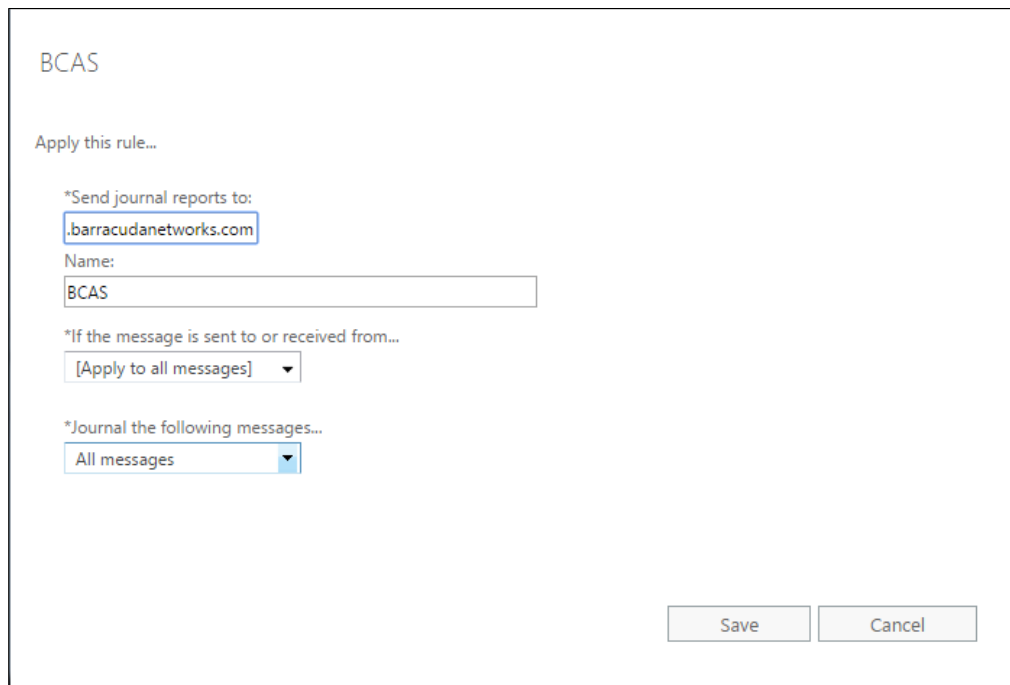
4. Browse to and select a recipient from the address book who should receive undeliverable journal reports. You can search for a recipient by typing all or part of a display name, and then clicking the **Search** icon, or click on either the **Display Name** or **E-Mail Address** heading to sort the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

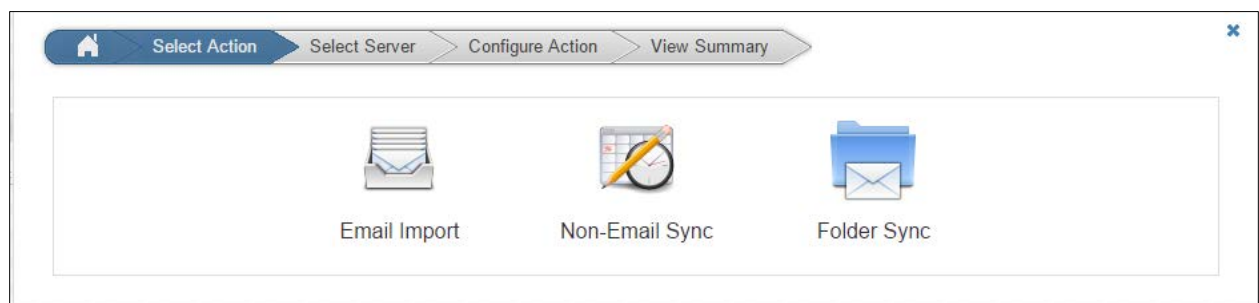
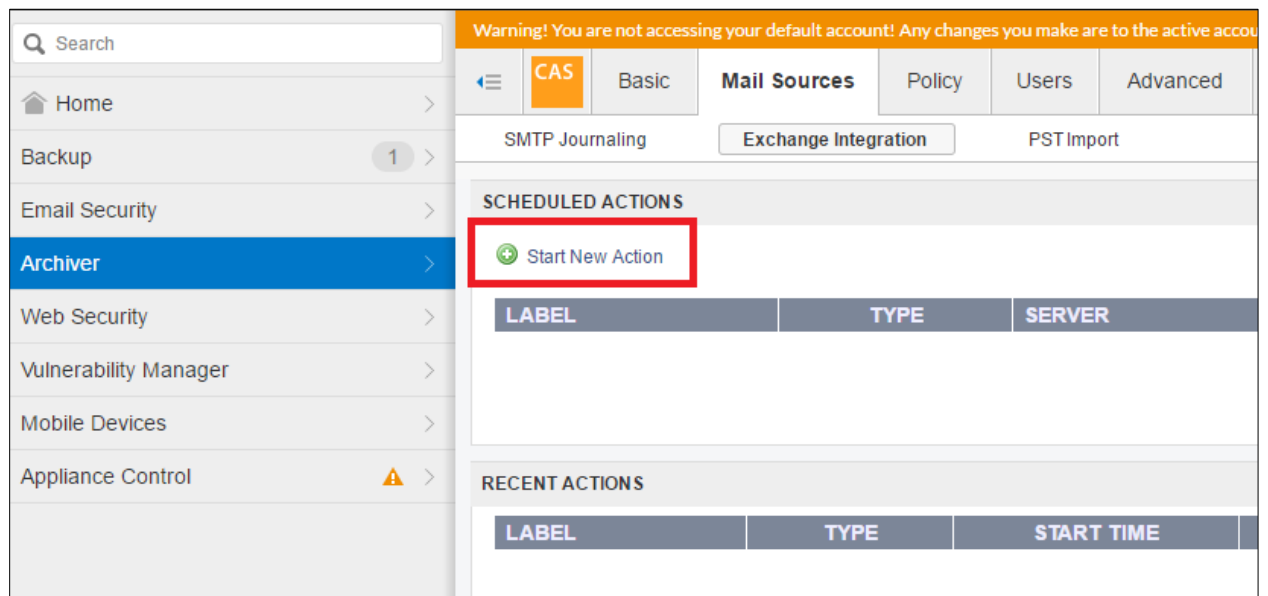
1. Open Windows PowerShell, enter the following command, and then press Enter:
\$UserCredential = Get-Credential
2. In the Windows PowerShell Credential Request dialog box, enter your Exchange Online user name and password, and then click OK.
3. Enter the following command, and then press Enter:
\$Session = 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

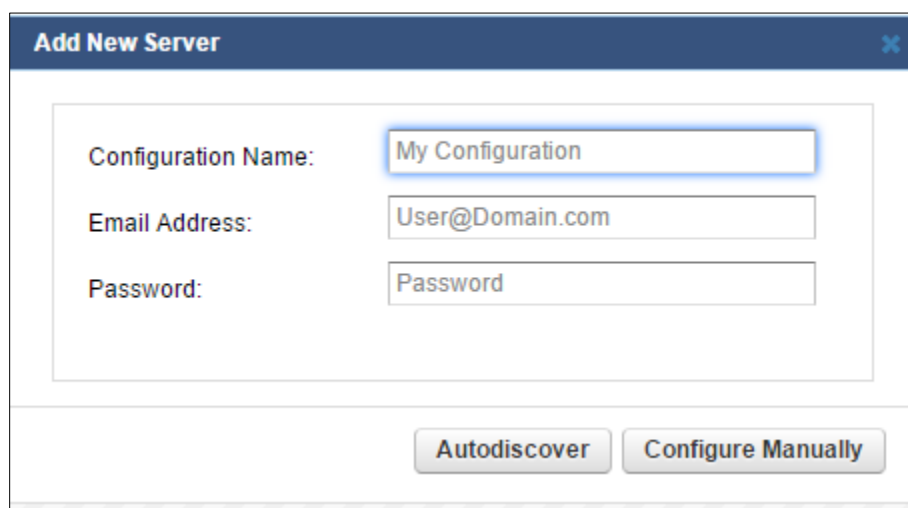
Please note: When setting up the Exchange import job in the web interface: Use the [GUID@domain.com](#) -style hostname available when setting up an Outlook profile *or* use <https://testconnectivity.microsoft.com/>

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.



The screenshot shows the 'Add New Server' dialog box. It has a title bar with a close button. Inside, there are three input fields: 'Configuration Name' with the value 'My Configuration', 'Email Address' with the value 'User@Domain.com', and 'Password' with the value 'Password'. At the bottom, there are two buttons: 'Autodiscover' and 'Configure Manually'.

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



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> $UserCredential = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\windows\system32> $Session = New-PSSession -ConfigurationName Microsoft
-Credential $UserCredential -Authentication Basic -AllowRedirection
PS C:\windows\system32> Import-PSSession $Session
WARNING: The names of some imported commands from the module 'tmp_a0xdij5z.1do
find the commands with unapproved verbs, run the Import-Module command again

ModuleType Name
-----
Script tmp_a0xdij5z.1do
ExportedCommands
{Add-AvailabilityAddressSpace,

PS C:\windows\system32> Get-Mailbox -Identity se@n.a.com | Format-List

ExchangeGuid : 2ee256dd-35d2-44e9-89c9-3
PrimarySmtpAddress : se@n.a.com

PS C:\windows\system32> Remove-PSSession $Session
PS C:\windows\system32> _
```

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:

The 'Add New Server' dialog box contains three input fields: 'Configuration Name' with the value 'My Configuration', 'Email Address' with the value 'User@Domain.com', and 'Password' with the value 'Password'. At the bottom, there are two buttons: 'Autodiscover' and 'Configure Manually'.



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.

Add New Server

Configuration Name: Exchange Online Hist. Import

Exchange Hostname: 0adbf69c-a89d-43c2-a21f-53903c734

Username: cdallmus

Password:

Exchange 2013 or newer: ☒ Yes ☐ No

If you are using Office 365 or Exchange 2013 or newer, select "Yes".

▼ Advanced Options

Proxy Server: outlook.office365.com

Save Cancel

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



Select a server for the action: **Non-Email Sync**

[Add New Server](#)

	NAME	SERVER	USERNAME	
<input checked="" type="radio"/>	cdallmus@laxtex.n...	0adb69c-a89d-43c2-a21f-53903c734f67@...	cdallmus@laxtex.net	Copy Edit Delete

[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**.

Configure settings for the action: **Email Import**

Which will run using configuration: **EOP DB Import (0adb69c-a89d-43c2-a21f-53903c734f67@laxtex.net)**

Source: [Verify](#)

Date: ☒ All Items ☐ By Date ☐ Item Age

Schedule: ☐ Nightly ☒ Now

[Advanced Options](#)

[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.



NAME	SERVER	USERNAME	
cdallmus@laxtex.n...	0adbf69c-a89d-43c2-a21f-53903c734f67@...	cdallmus@laxtex.net	Copy Edit Delete

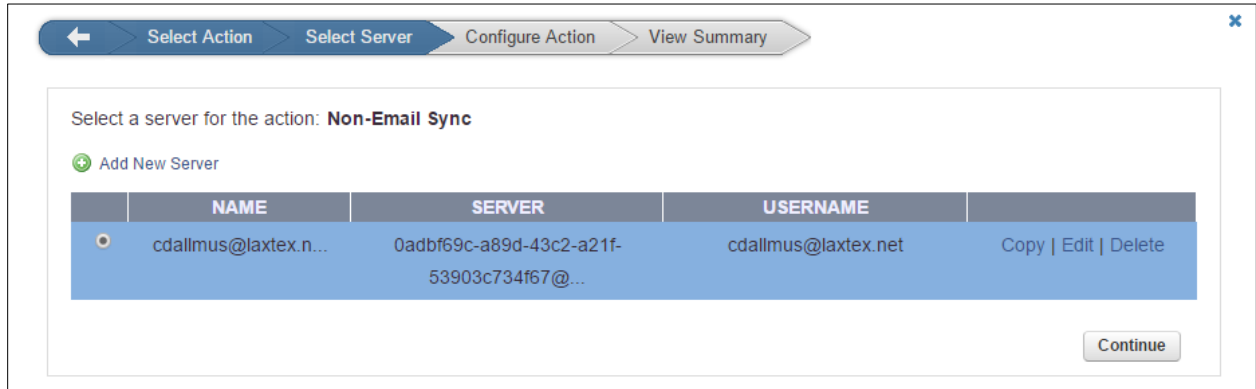
4. In the Configure Action page, Click **Continue**.
5. In the View Summary page, select **All Users** from the Source drop-down menu. For item type, check or de-check any of the items you would like to synchronize. For schedule, select **Nightly**. Then click **Continue**.

TYPE
<input checked="" type="checkbox"/> Appointments
<input checked="" type="checkbox"/> Contacts
<input checked="" type="checkbox"/> Tasks
<input checked="" type="checkbox"/> Notes

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.



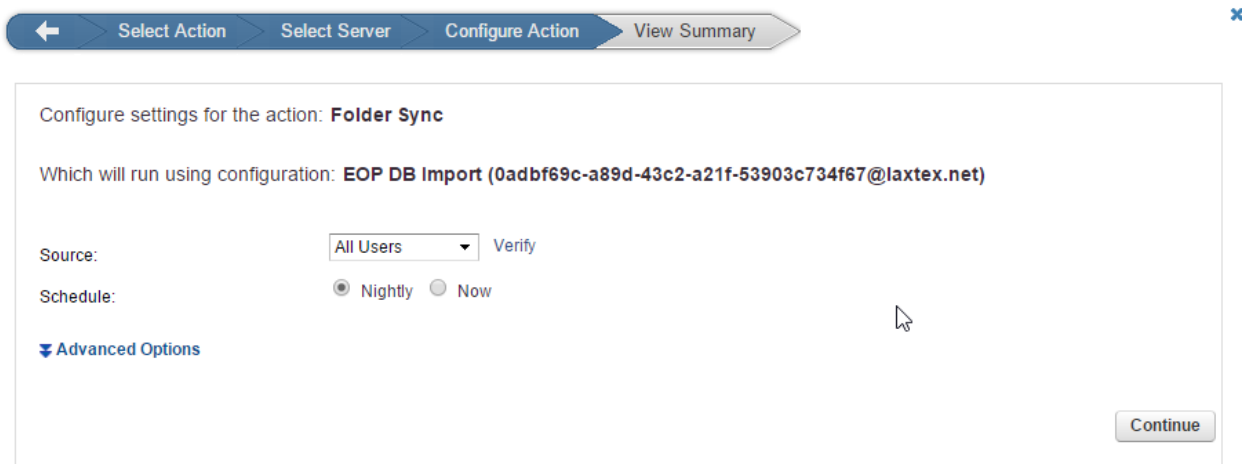
Select a server for the action: **Non-Email Sync**

[+ Add New Server](#)

	NAME	SERVER	USERNAME	
<input checked="" type="radio"/>	cdallmus@laxtex.n...	0adbf69c-a89d-43c2-a21f-53903c734f67@...	cdallmus@laxtex.net	Copy Edit Delete

[Continue](#)

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**.



Configure settings for the action: **Folder Sync**

Which will run using configuration: **EOP DB Import (0adbf69c-a89d-43c2-a21f-53903c734f67@laxtex.net)**

Source: [Verify](#)

Schedule: ☒ Nightly ☐ Now

[Advanced Options](#)

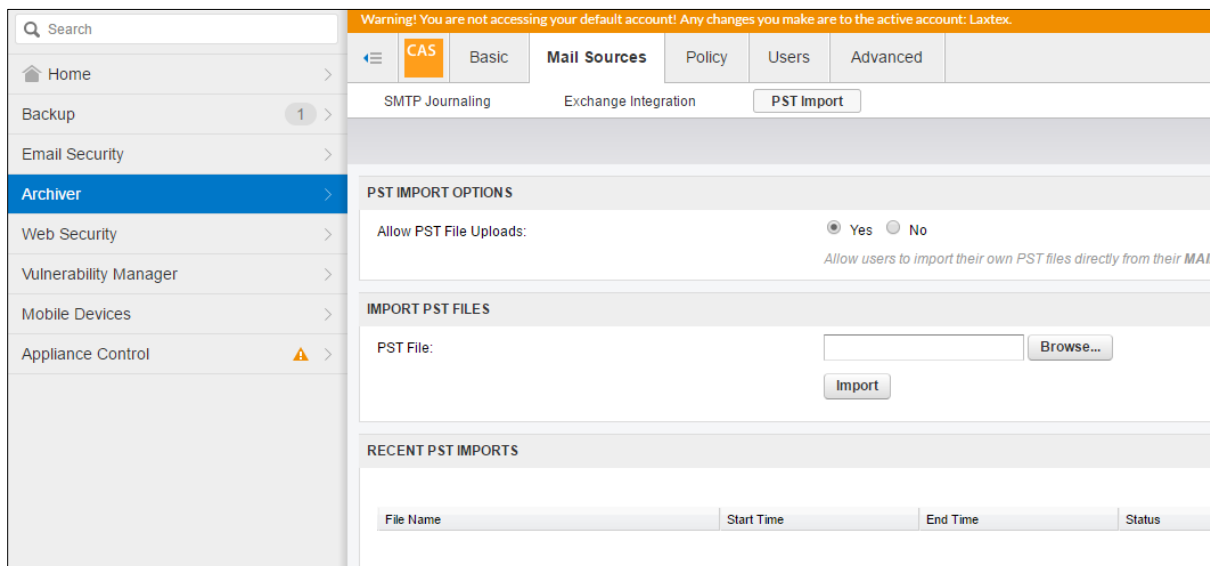
[Continue](#)

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.



The screenshot shows the Barracuda Cloud Archiving Service (CAS) interface. On the left is a navigation menu with options: Home, Backup, Email Security, Archiver (selected), Web Security, Vulnerability Manager, Mobile Devices, and Appliance Control. The main content area has a top warning bar: "Warning! You are not accessing your default account! Any changes you make are to the active account: Laxtex." Below this is a tabbed interface with tabs for CAS, Basic, Mail Sources (selected), Policy, Users, and Advanced. Under the Mail Sources tab, there are sub-tabs for SMTP Journaling, Exchange Integration, and PST Import (selected). The PST Import section contains "PST IMPORT OPTIONS" with a toggle for "Allow PST File Uploads" set to "Yes". Below this is the "IMPORT PST FILES" section with a "PST File:" label, a text input field, a "Browse..." button, and an "Import" button. At the bottom is a "RECENT PST IMPORTS" section with a table header: File Name, Start Time, End Time, and Status.

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****]



Barracuda Exchange Backup
cudaxchange@laxtex.net

First name: Barracuda Exchange
Last name: Backup
Display name: Barracuda Exchange Backup
User name: cudaxchange
Domain: laxtex.net
Location: United States

▼ Contact information

^ Password Admin-created

☐ Auto-generate password
☒ Let me create the password

Password: Weak

☒ Make this user change their password when they first sign in

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**.

^ Roles Global administrator

You can assign different roles to people in your organization. [Learn more about admin roles](#)

☐ User (no administrator access)
This user won't have permissions to the Office 365 admin center or any admin tasks.

☒ Global administrator
This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.

☐ Customized administrator
You can assign this user one or many roles so they can manage specific areas of Office 365.

^ Product licenses

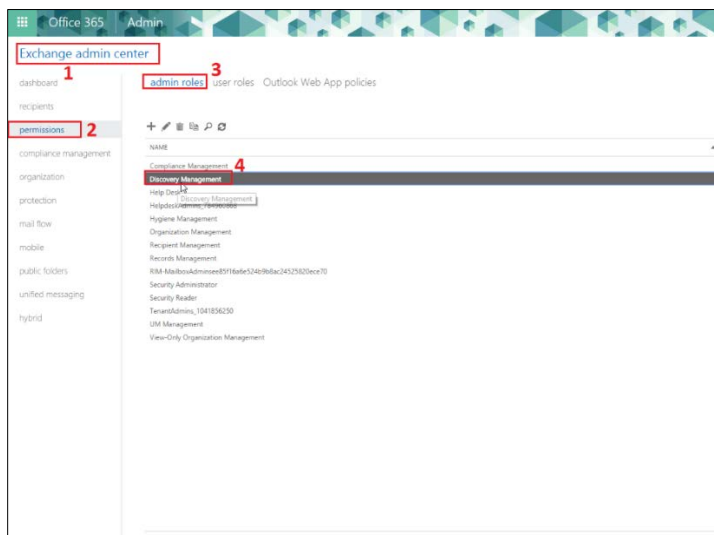
▼ Microsoft Office 365 Developer Off

Create user without product license On

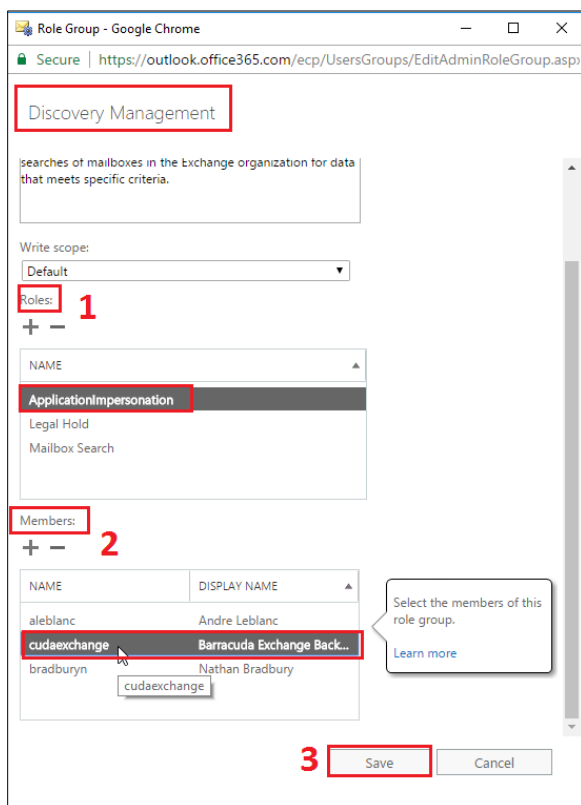
Add Cancel

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**"

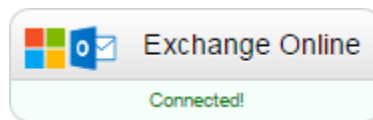


4. Under the **members (2)** section click '+' to add the **Exchange Backup** service account user.

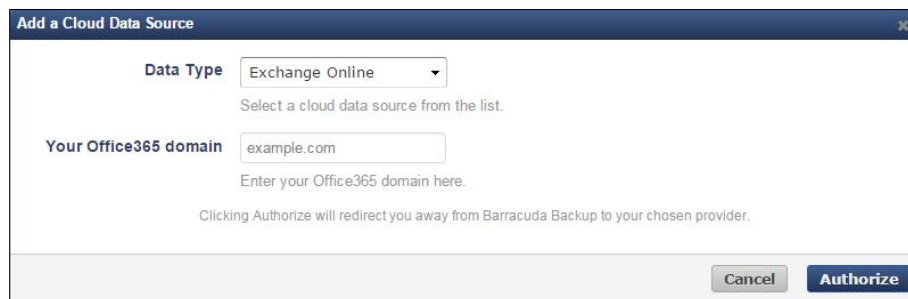
Configure Exchange Online Data Source

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**:



The dialog box titled 'Add a Cloud Data Source' contains the following elements:

- Data Type**: A dropdown menu with 'Exchange Online' selected.
- Select a cloud data source from the list.**: A small text instruction.
- Your Office365 domain**: A text input field containing 'example.com'.
- Enter your Office365 domain here.**: A small text instruction.
- Clicking Authorize will redirect you away from Barracuda Backup to your chosen provider.**: A small text instruction.
- Buttons**: 'Cancel' and 'Authorize' buttons at the bottom right.

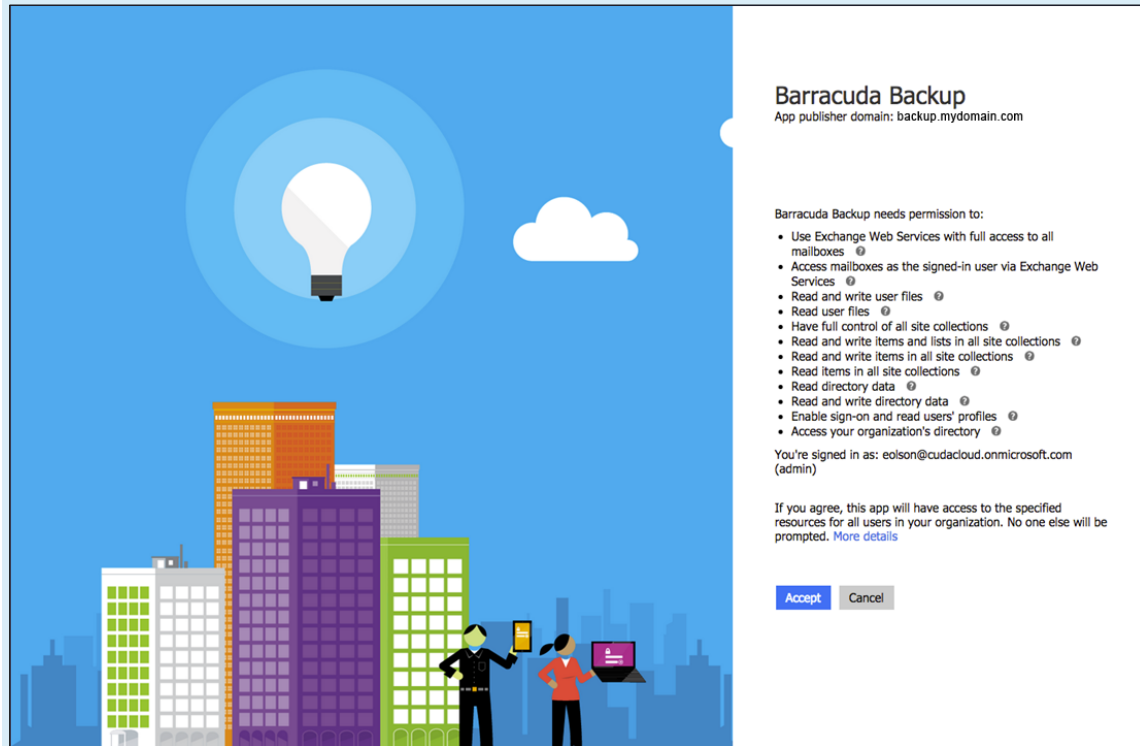
- b. Enter **Your Office365 domain** URL.
 1. The URL is available once you log in to Exchange Online.
5. Click **Authorize**.

[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**:

Edit Exchange Online: Exchange Cancel Save

[Back to Sources](#)

Backup

Data Description Describe the data source you are backing up.

Backup Status

Select to back up this data source on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this data source.

☒ **Enable Backups**

Authorization

[Reauthorize your Office365 account](#)

Add to Schedule

Item selections are done on a per schedule basis. If you would like to add this share to a schedule after you have finished configuring this data source, choose a schedule below.

Schedule ✓ - Select -
OneDrive Daily
- Add New -



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

The 'Add New Schedule' dialog box is shown. It has a title bar with a close button. Inside, there is a label 'Schedule Name' and a text input field containing 'Exchange Online Daily'. At the bottom, there are 'Cancel' and 'OK' buttons.

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:

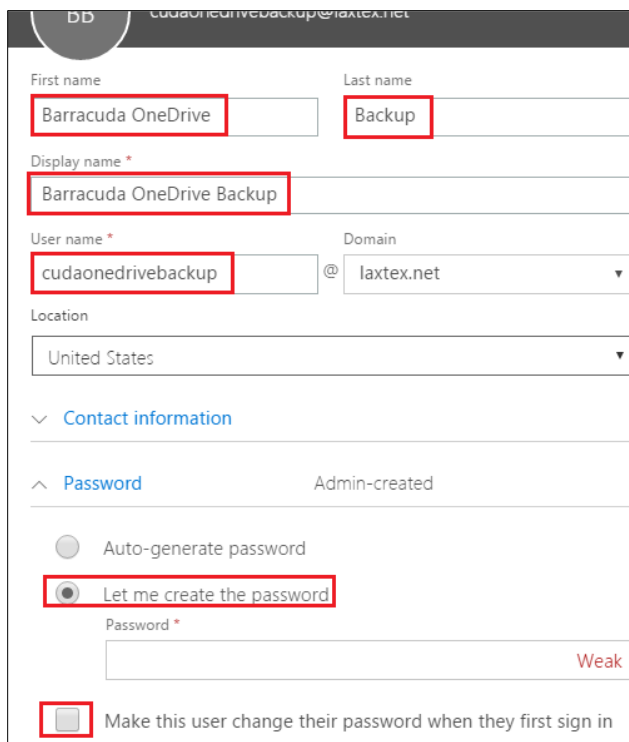
The 'Edit Backup Schedule: Exchange Daily' page is shown. It has a title bar with a 'Save' button. Below the title bar is a 'Back to Schedules' link. The page is divided into several sections: 'Schedule name' with a text input field containing 'Exchange Daily'; 'Items to Back Up' with a checkbox for 'Apply to all computers and data sources for this Barracuda Backup Cloud Service' and a tree view showing 'OneDrive' (with 'OneDrive for Business' and 'Exchange' selected) and 'TwoDrive'; 'Schedule Timeline' with checkboxes for all days of the week (all selected); and 'Daily Backup Timeline' with a 'Start time' field set to '2C : 0C' and a 'Repeat' checkbox.

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**]**



First name: Barracuda OneDrive

Last name: Backup

Display name *: Barracuda OneDrive Backup

User name *: cudaonedrivebackup

Domain: laxtex.net

Location: United States

✓ Contact information

^ Password Admin-created

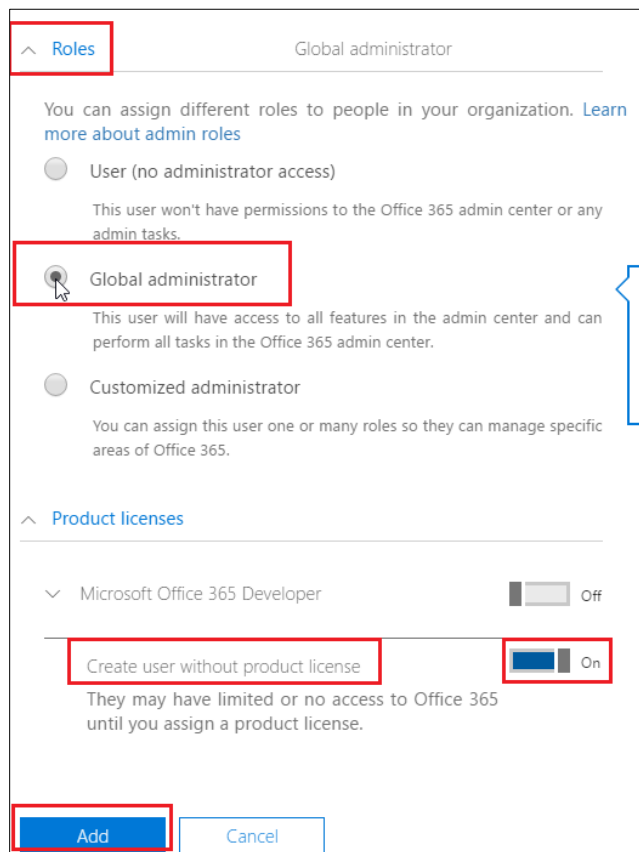
☐ Auto-generate password

☒ Let me create the password

Password *: Weak

☐ Make this user change their password when they first sign in

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**.



Roles Global administrator

You can assign different roles to people in your organization. [Learn more about admin roles](#)

- ☐ User (no administrator access)
This user won't have permissions to the Office 365 admin center or any admin tasks.
- ☒ **Global administrator**
This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.
- ☐ Customized administrator
You can assign this user one or many roles so they can manage specific areas of Office 365.

Product licenses

Microsoft Office 365 Developer ☐ Off

☒ **Create user without product license** ☒ On
They may have limited or no access to Office 365 until you assign a product license.

Add Cancel

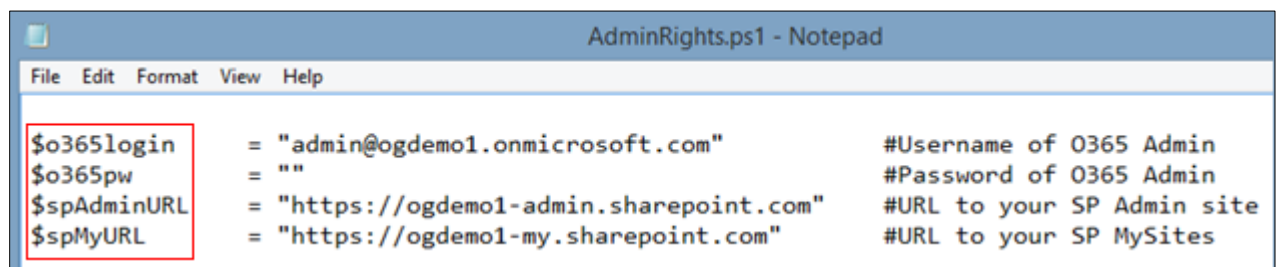
Configure Permissions for OneDrive for Business

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:



```

AdminRights.ps1 - Notepad
File Edit Format View Help

$o365login = "admin@ogdemo1.onmicrosoft.com" #Username of O365 Admin
$o365pw = "" #Password of O365 Admin
$spAdminURL = "https://ogdemo1-admin.sharepoint.com" #URL to your SP Admin site
$spMyURL = "https://ogdemo1-my.sharepoint.com" #URL to your SP MySites
  
```



- **\$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:

```
Administrator: SharePoint Online Management Shell
PS C:\Windows\system32> cd C:\Users\slubahn\Desktop
PS C:\Users\slubahn\Desktop>
```

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

```
Administrator: SharePoint Online Management Shell
PS C:\Windows\system32> cd C:\Users\slubahn\Desktop
PS C:\Users\slubahn\Desktop> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described
in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\slubahn\Desktop>
```

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



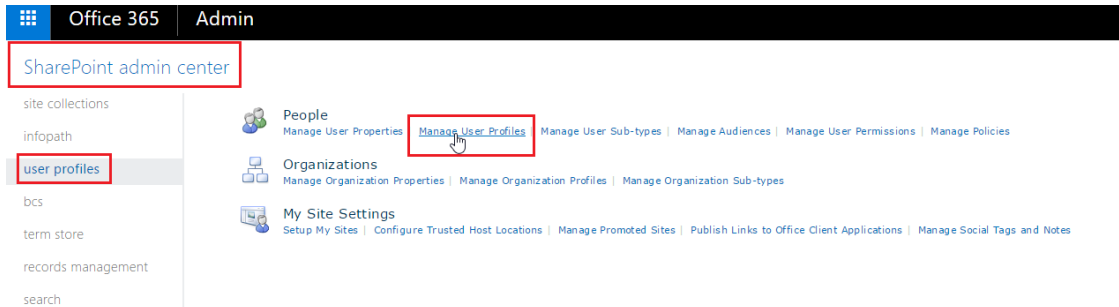
```
PS C:\Users\slobahn\Desktop> .\AdminRights.ps1
WARNING: The names of some imported commands from the module
'Microsoft.Online.SharePoint.PowerShell' include unapproved verbs that might
make them less discoverable. To find the commands with unapproved verbs, run
the Import-Module command again with the Verbose parameter. For a list of
approved verbs, type Get-Verb.
Begin discovery of 15 profiles
Checking profile 1 of 15
Checking profile 2 of 15
Checking profile 3 of 15
Checking profile 4 of 15
Adding /personal/admin_cuda365_com/ to the list
Checking profile 5 of 15
Adding /personal/rwagner_cuda365_com/ to the list
Checking profile 6 of 15
Adding /personal/sbanks_cuda365_com/ to the list
Checking profile 7 of 15
Adding /personal/chayes_cuda365_com/ to the list
Checking profile 8 of 15
Adding /personal/thale_cuda365_com/ to the list
Checking profile 9 of 15
Checking profile 10 of 15
Checking profile 11 of 15
Checking profile 12 of 15
Checking profile 13 of 15
Checking profile 14 of 15
Checking profile 15 of 15
Finished discovery of profiles
Connecting to Sharepoint Online
Start processing profiles
Processing https://barracudademo-my.sharepoint.com/personal/admin_cuda365_com

Display Name          Login Name          Groups
-----
Administrator         admin@cuda365.com   {}
admin@cuda365.com permissions added to https://barracudademo-my.sharepoint.com/p
ersonal/admin_cuda365_com
Processing https://barracudademo-my.sharepoint.com/personal/rwagner_cuda365_com
Administrator         admin@cuda365.com   {}
admin@cuda365.com permissions added to https://barracudademo-my.sharepoint.com/p
ersonal/rwagner_cuda365_com
Processing https://barracudademo-my.sharepoint.com/personal/sbanks_cuda365_com
Administrator         admin@cuda365.com   {}
admin@cuda365.com permissions added to https://barracudademo-my.sharepoint.com/p
ersonal/sbanks_cuda365_com
Processing https://barracudademo-my.sharepoint.com/personal/chayes_cuda365_com
Administrator         admin@cuda365.com   {}
admin@cuda365.com permissions added to https://barracudademo-my.sharepoint.com/p
ersonal/chayes_cuda365_com
Processing https://barracudademo-my.sharepoint.com/personal/thale_cuda365_com
Administrator         admin@cuda365.com   {}
admin@cuda365.com permissions added to https://barracudademo-my.sharepoint.com/p
ersonal/thale_cuda365_com
Job Finished
Press Enter to continue...:
```

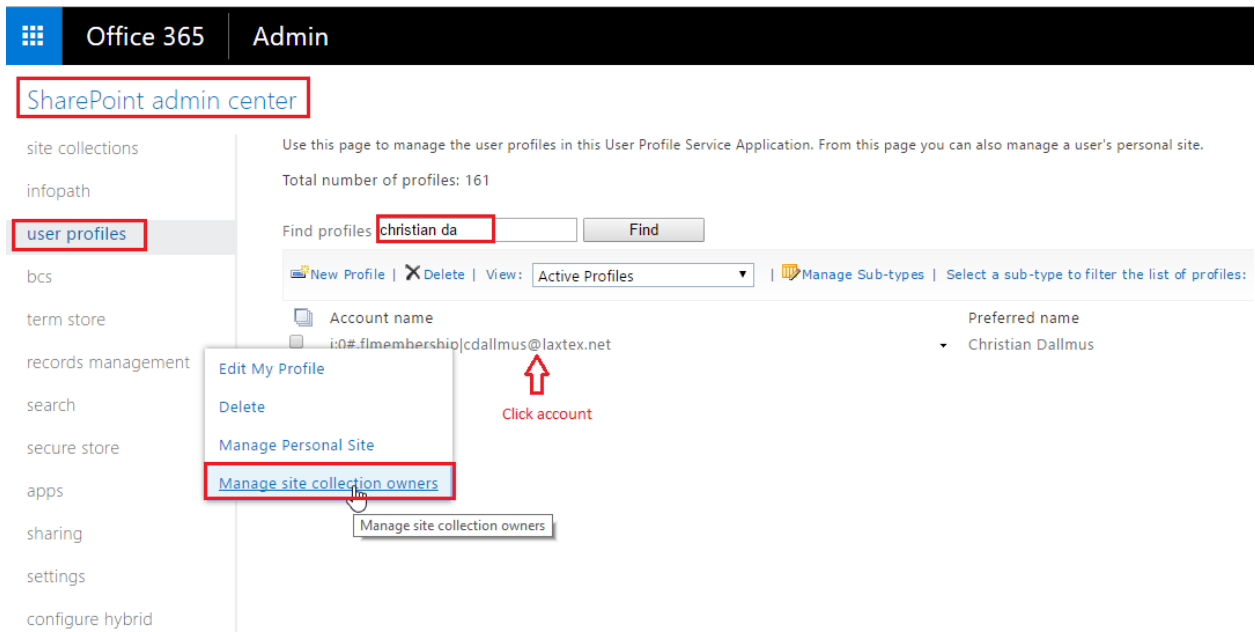
11. Press **Enter** to exit the script.
12. Exit SharePoint Online Management Shell.

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**:



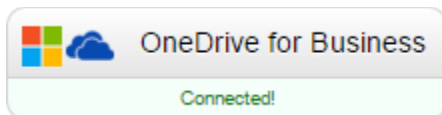
5. The **site collection owners** dialog box displays. In the **Site Collection Administrators** field, add the OneDrive service account we created earlier
6. Type the account name, and then click the **Verify User** (👤) icon, or
7. Click the **Directory** (📁) icon, and navigate to and select the account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



Add a Cloud Data Source

Data Type OneDrive for Business

Select a cloud data source from the list.

Your OneDrive URL https://cudacloud-my.sharepoint.com

Enter the first part of the URL you see once you have signed into your account through onedrive.live.com.

Clicking Authorize will redirect you away from Barracuda Backup to your chosen provider.

Cancel 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.
- Enter a name to identify the data source in the **Data Description** field.
 - 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:



Edit Backup Schedule: OneDrive Daily Save

[Back to Schedules](#)

Schedule name

A label to identify this backup schedule. A useful label may include information such as the type of data being backed up.

Schedule name

Items to Back Up

Identify the computers and data sources to back up with this schedule. Unselect the checkbox to display a list of all available computers and data sources from which individual ones can be selected.

☐ Apply to all computers and data sources for this Barracuda Backup Cloud Service

☒ OneDrive

☒ OneDrive for Business

Schedule Timeline

The days on which this backup schedule is to run. In general, backups should be run on each day when the data may change.

☒ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday

Daily Backup Timeline

When the backup runs begin. Select Repeat to schedule multiple backups in the same day. 24 hour format.

Start time :

Repeat ☐

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**]**



First name: Barracuda SharePoint
Last name: Backup
Display name: Barracuda SharePoint Backup
User name: cudasharepointbackup
Domain: laxtex.net
Location: United States
Contact information
Password: Admin-created
Auto-generate password: ☐
Let me create the password: ☒
Password: Weak
Make this user change their password when they first sign in: ☐

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**.

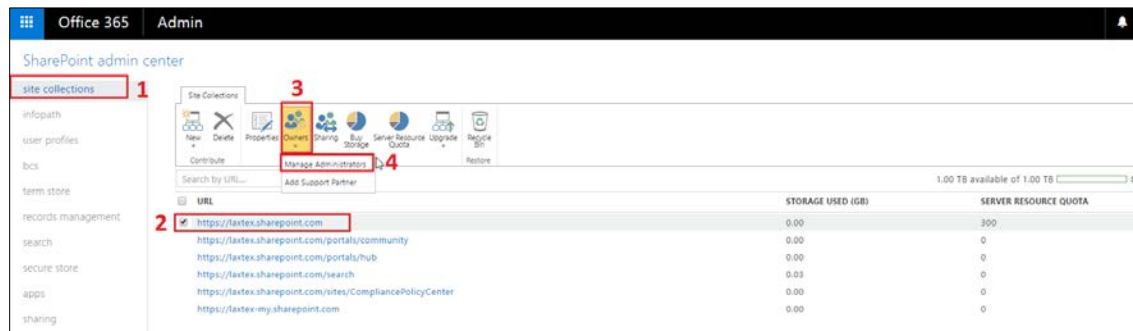
Roles: Global administrator
You can assign different roles to people in your organization. [Learn more about admin roles](#)
User (no administrator access)
This user won't have permissions to the Office 365 admin center or any admin tasks.
Global administrator
This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.
Customized administrator
You can assign this user one or many roles so they can manage specific areas of Office 365.
Product licenses
Microsoft Office 365 Developer: Off
Create user without product license: On
Add Cancel



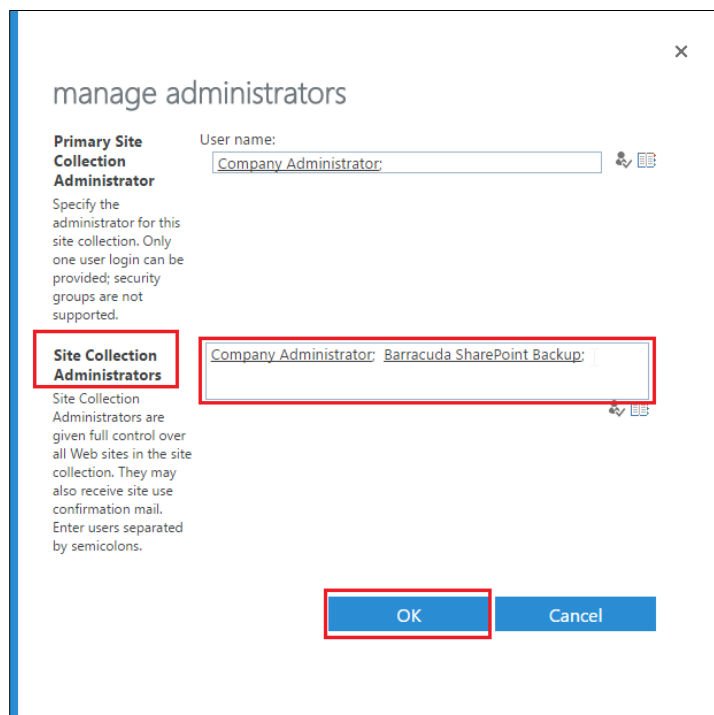
Configure Impersonation for SharePoint

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:

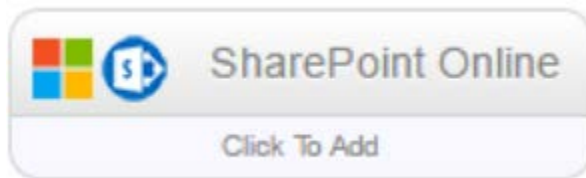


7. Click **OK** to save your changes.

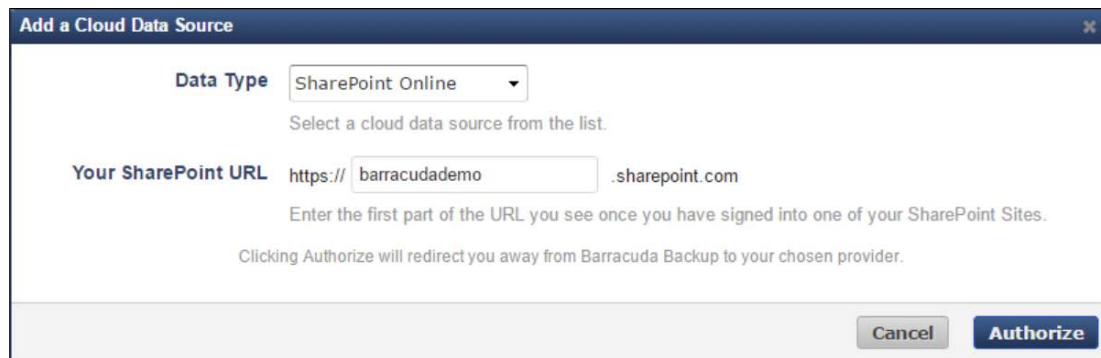
Configure SharePoint Online Data Source

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

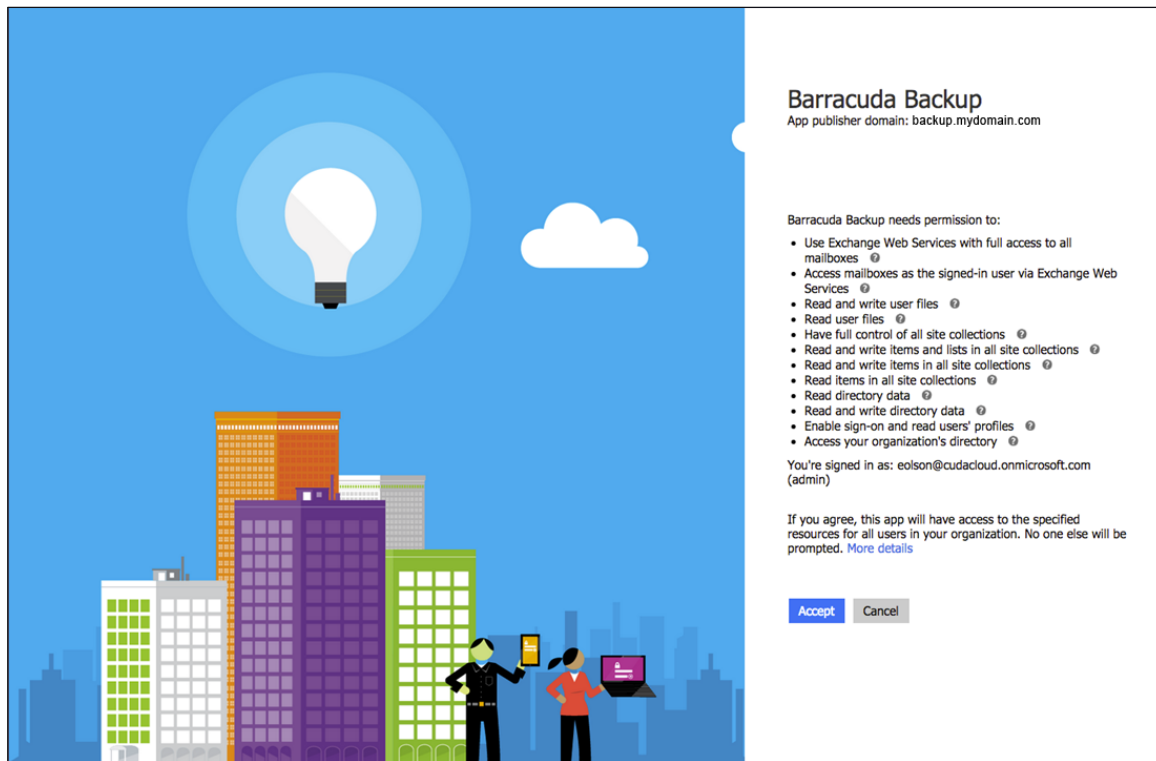
1. Use the following steps to set up SharePoint Online backup:
2. Log in to Barracuda Backup, and select the **Cloud Source** in the left pane.
3. In the **Status** page, click SharePoint Online:



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:

Edit SharePoint Online: Office 365

< Back to Sources Cancel Save

Backup

Data Description SharePoint Online

Describe the data source you are backing up.

Backup Status

Select to back up this data source on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this data source.

☒ Enable Backups

Authorization

Reauthorize your SharePoint Online account

Add to Schedule

Item selections are done on a per schedule basis. If you would like to add this share to a schedule after you have finished configuring this data source, choose a schedule below.

Schedule - Select -

- Select -

- Add New -

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



A dialog box titled "Add New Schedule" with a close button (X) in the top right corner. It contains a text input field labeled "Schedule Name" with the text "SharePoint Backup" entered. Below the input field is the instruction "Save data source to make selections". At the bottom are "Cancel" and "OK" buttons.

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:

The "Edit Backup Schedule: SharePoint Backup" page. It includes a "Save" button in the top right and a "Back to Schedules" link. The "Schedule name" section shows "SharePoint Backup". The "Identify the data sources" section has an information icon and a checkbox for "Apply to all computers and data sources for this Barracuda Cloud to Cloud Backup". Below is a tree view of Office 365 sources, with "SharePoint Online" expanded to show various sites and documents, all of which are selected. The "Schedule Timeline" section shows checkboxes for all days of the week (Sunday through Saturday), all of which are checked. The "Daily Backup Timeline" section has a "Start time" field set to "20:00" and a "Repeat" checkbox.



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

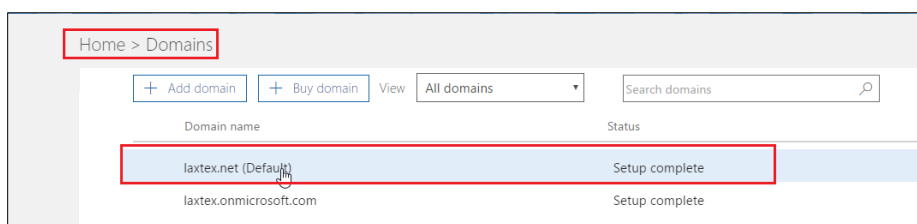


Appendix 1 – How to locate your Office365 domain or mail server

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.

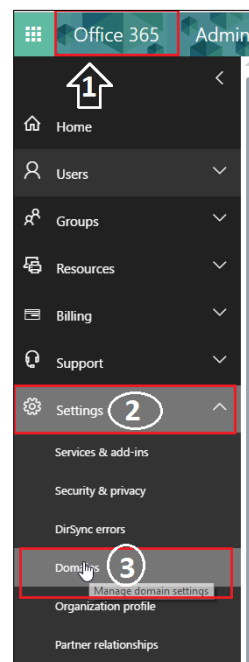
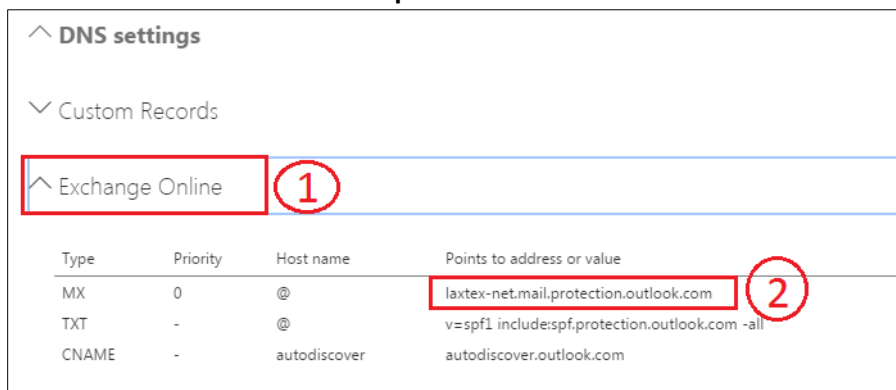
1. Login to your customer's **Office365 Portal**, then going to the **Admin Center (1)** and click on **Settings (2) > Domains (3)**.

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.