Step 2 - Configure Office 365 for Inbound and Outbound Mail

You can configure Microsoft Office 365 with the Barracuda Email Security Service as your inbound and/or outbound mail gateway.

If you make changes to the settings, allow a few minutes for the changes to take effect.

Office 365 IP addresses and user interfaces can change; refer to Microsoft documentation for configuration details.

Time Requirement

After you update your MX records, you must wait at least 24-48 hours before starting work on Step 4 below so that your emails are not rejected. Plan accordingly.

You can specify the Barracuda Email Security Service as an inbound mail gateway through which all incoming mail for your domain is filtered before reaching your Office 365 account. The Barracuda Email Security Service filters out spam and viruses, then passes the mail on to the Office 365 mail servers. Use the Configure Inbound Mail Flow instructions below to configure.

You can also specify the Barracuda Email Security Service as the outbound mail gateway through which all mail is sent from your domain via your Office 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Service processes the mail by filtering out spam and viruses before final delivery. By configuring Office 365 as described in Configure Outbound Mail Flow below, you instruct the Office 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Service (the gateway server).

Step 1. Launch the Barracuda Email Security Service Setup Wizard

Before you launch the wizard, verify you have the following:

- Office 365 admin credentials
- Credentials to run a PowerShell script or terminal to manually execute PowerShell scripts

Note that you cannot reopen the wizard after you close or complete the wizard.
1. Log into Barracuda Cloud Control. On the left side, select Email Security.

The Email Security wizard launches. Click Next.

2. Select the Region for your Data Center. Then click Get Started. After you select your region, you cannot change it.

3. Enter the primary email domain you want to protect with Barracuda Email Security Service. Then click Next.
4. The system automatically retrieves your current MX records and auto-fills that information as your Destination Server. If this is not the correct Destination Server, click **Remove** and add the Destination Server with the correct data.

If you want to add additional servers, enter data for those servers now.

After you properly configure the Destination Server, enter a valid User Name to test the mail server connection.

After you have determined that the settings are correct, click **Next**.
5. Select your settings, accepting the default values or making changes if needed, then click Next.

6. Barracuda recommends waiting to configure outbound filtering until your inbound mail is fully cut over.
   You will set up your Outbound Settings later.
   Select the second option on this screen, then click Next to continue.
7. Barracuda recommends verifying your domain via MX records with Priority 99. If you do not want to update MX records now, check the box and select a different method. In the first case, click **Verify MX Records.** Otherwise, click **Confirm Validation.**

When the verification is successful, click **Next.**
If the verification is not successful, a message appears, letting you know that the domain could not be verified.

If you are having DNS issues that you want to address, click Skip to exit the wizard. Behind the wizard, click the Domains tab to retry the validation.

8. Click Finish to finalize the setup and close the wizard.

### Step 2. Add Additional Email Domains (Optional)

You configured your primary email domain in Step 3 of the wizard, above. Use the steps in the following section if you want to protect additional domains with Barracuda Email Security Service. If you are only protecting one domain, continue below with Step 3.

#### Obtain the hostname:

1. Log into the Office 365 admin center.
2. In the left pane, click Settings > Domains.
3. In the Domains table, click on your domain.
4. Take note of the hostname. This is the address of your destination mail server, for example, cudaware-com.mail.protection.outlook.com

#### Enter the hostname:

Barracuda recommends using a hostname rather than an IP address so that you can move the
destination mail server and update DNS records without making changes to the Barracuda Email Security Service configuration. This address indicates where the Barracuda Email Security Service should direct inbound mail from the Internet to your Office 365 Exchange server. For example, your domain displays to the Internet as: *bess-domain.mail.protection.outlook.com*

1. Log into the Barracuda Cloud Control as administrator. In the left panel, click **Email Security**. Select the **Domains** tab, then click **Add Domain**.
2. Enter the domain name and destination mail server hostname obtained from your Office 365 account:
   ![Add Domain](image)
   
   Click **Add Domain**; the **Domain Settings** page displays, listing the new domain.

3. Click **Add Domain**; the **Domain Settings** page displays, listing the new domain.
4. Verify that the domain is yours. Follow the instructions in [How to Set Up MX Records for Domain Verification](#). Make sure that you see that the domain is successfully verified, then return to this page.

Repeat these steps, as needed, for additional Office 365 domains before continuing with Step 3 below.

**Step 3. Create Transport Rule to Bypass Spam Filtering**

1. Log into the Office 365 admin center, and go to **Admin centers > Exchange**.
2. In the left pane, click **mail flow**, and click **rules**.
3. Click the + symbol, and click **Bypass spam filtering**:
4. In the **new rule** page, enter a **Name** to represent the rule.
5. From the **Apply this rule** drop-down menu, select **The sender > IP address is in any of these ranges or exactly matches:**
6. In the **specify IP address ranges** page, enter the IP address/range for the Sender (Barracuda Email Security Service). For example, if you are in the US region, type 64.235.144.0/20. For other regions, refer to the IP addresses listed in [Barracuda Email Security Service IP Ranges](#). If your region has only one IP address range, you can skip ahead to Step 8 below.

7. If there is more than one IP address or range, click the + symbol, then type the next IP address or range. For example, for the US region, type 209.222.80.0/21, and click the + symbol:
8. Click OK, and click Save to create the transport rule.
9. Click the Edit icon for the rule, scroll to the Properties of this rule section, and in the Priority field, type 0.
10. Click Save.

Step 4. Restrict Inbound Mail to the Barracuda Email Security Service IP Range

Time Requirement

It is essential that you wait at least 24-48 hours after you update your MX records before you begin working on the steps in this section. That time is needed for the records to propagate so your email will not be rejected.

The steps in this section enhance the security of the connection between Barracuda Email Security Service and Office 365. It will only allow inbound email to come from the Barracuda system.

1. Connect to Exchange Online Powershell using one of the options:
   - If you are using Basic Authentication, see Connect to Exchange Online PowerShell.
   - If you are using Modern Authentication such as multi-factor authentication (MFA), see Connect to Exchange Online PowerShell using multi-factor authentication.
2. Find the correct IP range based on the region selected when setting up your Barracuda Email Security Service instance. Refer to the Barracuda Email Security Service IP Ranges for the IP ranges corresponding to your region.
3. After you connect to Exchange Online PowerShell, expand and run the appropriate script based
on the connection setup you chose:

**PowerShell Script for the Australia Region**

```powershell
Set-ExecutionPolicy unrestricted
$userCredential = Get-Credential
Import-PSSession $Session
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 3.24.133.128/25 -RestrictDomainstoIPAddresses $true
```

**PowerShell Script for the Canada Region**

```powershell
Set-ExecutionPolicy unrestricted
$userCredential = Get-Credential
Import-PSSession $Session
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 15.222.16.128/25 -RestrictDomainstoIPAddresses $true
```

**PowerShell Script for the German Region**

```powershell
Set-ExecutionPolicy unrestricted
$userCredential = Get-Credential
Import-PSSession $Session
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.157.190.224/27 -RestrictDomainstoIPAddresses $true
```

**PowerShell Script for the UK Region**

```powershell
Set-ExecutionPolicy unrestricted
$userCredential = Get-Credential
Import-PSSession $Session
```
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.176.92.96/27 -RestrictDomainstoIPAddresses $true

**PowerShell Script for the US Region**

Set-ExecutionPolicy unrestricted
$UserCredential = Get-Credential
Import-PSSession $Session
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 64.235.144.0/24,64.235.145.0/24,64.235.146.0/24,64.235.147.0/24,64.235.148.0/24,64.235.149.0/24,64.235.150.0/24,64.235.151.0/24,64.235.152.0/24,64.235.153.0/24,64.235.154.0/24,64.235.155.0/24,64.235.156.0/24,64.235.157.0/24,64.235.158.0/24,64.235.159.0/24,209.222.80.0/24,209.222.81.0/24,209.222.82.0/24,209.222.83.0/24,209.222.84.0/24,209.222.85.0/24,209.222.86.0/24,209.222.87.0/24 -RestrictDomainstoIPAddresses $true

**Note:** Replace `<your-UPN>` with your Office 365 account.

**PowerShell Script for the Australia Region**

Connect-EXPOSSession -UserPrincipalName <your-UPN>
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 3.24.133.128/25 -RestrictDomainstoIPAddresses $true

**PowerShell Script for the Canada Region**

Connect-EXPOSSession -UserPrincipalName <your-UPN>
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 15.222.16.128/25 -RestrictDomainstoIPAddresses $true

**PowerShell Script for the German Region**

Connect-EXPOSSession -UserPrincipalName <your-UPN>
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.157.190.224/27 -RestrictDomainstoIPAddresses $true
PowerShell Script for the UK Region

Connect-EXPOSSession -UserPrincipalName <your-UPN>
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.176.92.96/27 - RestrictDomainstoIPAddresses $true

PowerShell Script for the US Region

Connect-EXPOSSession -UserPrincipalName <your-UPN>
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 64.235.144.0/24,64.235.145.0/24,64.235.146.0/24,64.235.147.0/24,64.235.148.0/24,64.235.149.0/24,64.235.150.0/24,64.235.151.0/24,64.235.152.0/24,64.235.153.0/24,64.235.154.0/24,64.235.155.0/24,64.235.156.0/24,64.235.157.0/24,64.235.158.0/24,64.235.159.0/24,64.235.160.0/24,64.235.161.0/24,64.235.162.0/24,64.235.163.0/24,64.235.164.0/24,64.235.165.0/24,64.235.166.0/24,64.235.167.0/24,64.235.168.0/24,64.235.169.0/24,64.235.170.0/24,64.235.171.0/24,64.235.172.0/24,64.235.173.0/24,64.235.174.0/24,64.235.175.0/24,64.235.176.0/24,64.235.177.0/24,64.235.178.0/24,64.235.179.0/24,64.235.180.0/24,64.235.181.0/24,64.235.182.0/24,64.235.183.0/24,64.235.184.0/24,64.235.185.0/24,64.235.186.0/24,64.235.187.0/24,64.235.188.0/24,64.235.189.0/24,64.235.190.0/24,64.235.191.0/24,64.235.192.0/24,64.235.193.0/24,64.235.194.0/24,64.235.195.0/24,64.235.196.0/24 -RestrictDomainstoIPAddresses $true

Step 5. Configure Sender Policy Framework for Outbound Mail

To assure Barracuda Networks is the authorized sending mail service of outbound mail from your Barracuda Email Security Service, add the following to the Sender Policy Framework (SPF) record INCLUDE line of the SPF record for your sending mail server for each domain sending outbound mail. Select the relevant SPF INCLUDE based on the region you selected for your Barracuda Email Security Service:

AU (Australia)

include:spf.ess.au.barracudanetworks.com -all

CA (Canada)

include:spf.ess.ca.barracudanetworks.com -all

DE (Germany)

include:spf.ess.de.barracudanetworks.com -all

UK (United Kingdom)

include:spf.ess.uk.barracudanetworks.com -all
If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Email Security Service instance. For example:

```
include:spf.ess.barracudanetworks.com -all
```

If you do not have an SPF record set up for your domain, use the following value to create a TXT record that creates a HARD Fail SPF for your domain based on your Barracuda Email Security Service instance. For example:

```
v=spf1 include:spf.ess.barracudanetworks.com -all
```

### Step 6. Configure User Accounts and User Lists

Expand and complete the steps in the appropriate section, based on your organization's setup.

If you make setting changes, allow a few minutes for the changes to take effect.

Sender authentication and recipient verification are a critical part of maintaining security of email flowing into and out of your organization. By identifying known trusted senders and recipients of email, you can block a large percentage of spam, viruses and malware from your network. Once you have entered information about your LDAP server, click **Test Settings** on the **Domain Settings** page to ensure that the Barracuda Email Security Service can communicate with the server. LDAP server types supported include Active Directory, Novell eDirectory, Domino Directory and OpenLDAP.

### LDAP Lookup

You can synchronize the Barracuda Email Security Service with your existing LDAP server to automatically create accounts for all users in the domain. For more information about user accounts, see **Managing User Accounts**.
LDAP lookup configuration and LDAP authentication of user logins is done by domain on the **Domains > Domain Settings** page. On the **Domains** page, click **Edit** in the **Settings** column to the right of the domain name. Once you configure your LDAP settings on the **Domains > Domain Settings** page, click **Synchronize Now** to create user accounts for all users in your LDAP server.

**Important**

The Barracuda Email Security Service connects with your network from various IP addresses, including performing LDAP lookups. To ensure that the service can connect with your network, allow traffic originating from the range of network addresses based on your Barracuda Email Security Service instance; see [Barracuda Email Security Service IP Ranges](#) for a list of ranges based on your Barracuda Email Security Service instance.

1. Log into [https://login.barracudanetworks.com/](https://login.barracudanetworks.com/) using your account credentials, and click **Email Security** in the left pane.
2. Go to the **Domains** page, and click **Edit** in the **Settings** column to the right of the domain.
3. In the **Domains > Domain Settings** page, scroll to the **Directory Services** section, select **LDAP**, and click **Save Changes** at the top of the page.
4. In the **LDAP Configuration** section, configure the following variables:
   1. **LDAP Host** – The server utilized for LDAP lookups. If this setting is a hostname, and is contained in multiple A records, then fail-over capabilities are available if the Barracuda Email Security Service is unable to connect to one of the machines listed here.
   2. **Port** – Port used to connect to the LDAP service on the specified LDAP Server. Typically port 389 is used for regular LDAP and LDAP using the STARTTLS mode for privacy. Port 636 is assigned to the LDAPS service (LDAP over SSL/TLS).
   3. **Use SSL (LDAPS)** – By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) technology by selecting **Yes** for this option.
   4. **Bind DN (Username)** – Username used to connect to the LDAP service on the specified LDAP Server. If in the form `accountname@domain.com`, the username is transformed into a proper LDAP bind DN, for example, `CN=accountname,CN=users,DC=domain,DC=com`, when accessing the LDAP server. Sometimes the default transformation does not generate a proper bind DN. In such cases, a fully formed and valid bind DN must be entered.
   5. **Bind Password** – Password used to connect to the LDAP service on the specified LDAP Server.
   6. **Base DN** – Base DN for your directory. This is the starting search point in the LDAP tree. The default value looks up the defaultNamingContext top-level attribute and use it as the search base. For example, if your domain is `test.com`, your Base DN might be `dc=test,dc=com`.
   7. **Mail Attributes** – Attribute in your LDAP directory that contains the user's email addresses.

The attributes listed in this field determine which user address is primary versus
5. The Barracuda Email Security Service will sync to your LDAP server from certain IP addresses. Ensure that your network and LDAP server accept connections from the IP ranges listed in Barracuda Email Security Service IP Ranges.

Use the **Test LDAP Configuration Settings** section, enter a valid email address in the **Testing Email Address** field to test your LDAP settings; if left blank, LDAP settings are only tested for connection.

6. Click **Test Settings**.

7. Optionally, expand the **Advanced LDAP Configuration** section, and set the following options:
   1. **User Filter** – Set to **Yes** to limit newly synchronized email users and linked email users strictly to this one domain.
   2. **Custom User Filter** – Filter used to limit the accounts that the Barracuda Email Security Service creates when an LDAP query is made. For example, you could limit the LDAP synchronization to just users in certain sub-domains using the \textit{mail=} parameter, or only synchronize user-objects in a certain organizational unit (OU) using the \textit{ou=} parameter. Each type of LDAP server has specific query syntax, so consult the documentation for your LDAP server. For Microsoft Exchange syntax and examples, see the TechNet article [LDAP Query Basics](#).

   Example: Your list of valid users on your directory server includes 'User1', 'User2', 'User3', 'BJones', 'RWong', and 'JDoe', and you create the User Filter (name=*User*). In this case, the service only creates accounts for 'User1', 'User2', and 'User3'.

8. In the **Directory Options** section, specify the following options:
   1. **Synchronize Automatically** – Set to **Yes** if you are using LDAP and want the Barracuda Email Security Service to automatically synchronize your LDAP users to its database on a regular basis for recipient verification. With Microsoft Exchange server, the synchronization is incremental. Select **No** if you want to synchronize manually in case your LDAP server is not always available. To synchronize manually, click **Synchronize Now**.
   2. **Use LDAP for Authentication** – Set to **Yes** to enable LDAP for user login authentication. You can disable this setting if your LDAP server is unavailable for a period of time.
   3. **Authentication Filter** – Filter used to look up an email address and determine if it is valid for this domain. The filter consists of a series of attributes that might contain the email address. If the email address is found in any of those attributes, then the account is valid and is allowed by the Barracuda Email Security Service.

The first time the Barracuda Email Security Service receives a **Not Allowed** email for a valid user, the service does the following:

- Uses the email address of the recipient as the username of the account and auto-generates a password. If **Use LDAP for Authentication** is set to **No** on the **Domains > Domain Settings** page, the user receives an email with the login information so they can
access their quarantine account, otherwise, the user can use single sign-on via LDAP lookup.

- Places the quarantined message in the account holder’s quarantine inbox.
- Sends a quarantine summary report to the account holder at the specified notification interval, as set on the Users > Quarantine Notification page. If Allow users to specify interval is set to Yes on this page, then the quarantine summary report is sent to the user on the schedule specified on the Settings > Quarantine Notification page once they log into their account. The default is Daily.

If you make setting changes, allow a few minutes for the changes to take effect.

See also: How to Restore LDAP or Azure AD Directory Services

---

**Azure Active Directory**

Configure recipient verification with Azure Active Directory (AD) to allow end-users to sign in to the Barracuda Email Security Service using their Azure AD credentials. Once logged in, users can view their quarantine messages.

Note: If when setting up your Office 365 Enterprise applications you set Users can consent to apps accessing company data on their behalf to No, users might not be able to log into the Barracuda Email Security Service without administrator consent. To resolve this issue, reauthorize Azure AD from the Domain Settings page in the web interface. See the Azure Active Directory Authentication section of How to Restore LDAP or Azure AD Directory Services for step-by-step instructions on Azure AD reauthorization.

**Single Sign-On**

You can configure Single Sign-On (SSO) for a domain so that authenticated users can access all or a subset of the restricted resources by authenticating just once using their Azure AD credentials. SSO is
a mechanism where a single set of user credentials is used for authentication and authorization to access multiple applications across different web servers and platforms, without having to re-authenticate.

The SSO environment protects defined resources (websites and applications) by requiring the following steps before granting access:

- **Authentication**: Authentication verifies the identity of a user using login credentials.
- **Authorization**: Authorization applies permissions to determine if this user may access the requested resource.

### Set Up Azure AD Authorization

Complete the steps in this section for each domain you want to synchronize with your Azure AD directory.

1. Log into [https://login.barracudanetworks.com/](https://login.barracudanetworks.com/) using your account credentials, and click **Email Security** in the left pane.
2. Click **Domains**, and click **Edit** in the **Settings** column for the desired domain.
3. In the **Domains > Domain Settings** page, scroll to the **Directory Services** section, and select **Azure AD**, and click **Save Changes** at the top of the page.
4. Scroll down to the **Status** section, and click **Authorize**.
5. The **Authorize Azure AD** dialog box displays. Click **Continue**.
6. When prompted, log into your Microsoft Office 365 account using your administrator credentials.
7. In the **Authorization** page, click **Accept** to authorize the Barracuda Email Security Service to connect to your Azure AD directory.
8. In the Barracuda Email Security Service **Domain Settings** page, the **Status** field displays as **Active**; the **Authorized Account** and **Authorization Date** display below the status:

```
Directory Services
You can use either Azure AD or LDAP directory services to enable single sign on and synchronization of users lists.

<table>
<thead>
<tr>
<th>Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://login.barracudanetworks.com/" alt="LDAP" /></td>
<td>Azure AD</td>
</tr>
<tr>
<td><img src="https://login.barracudanetworks.com/" alt="None" /></td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>(Revoke Authorization)</td>
<td></td>
</tr>
</tbody>
</table>

Authorized Account: organizationname.info
Authorization Date: 3/28/2018, 11:44:24 AM
```

9. Click **Sync Now** to add your Azure AD users to the Barracuda Email Security Service. This will do a full synchronization with your Azure AD directory.
10. The synchronization progress displays; allow the process to complete.
11. In the **Synchronization Options** section, select **Synchronize Automatically**. When selected, the Barracuda Email Security Service automatically synchronizes with your Azure AD directory every 15 minutes and adds/updates your users. If you encounter sync issues, such as new users...
not being properly synced between your Azure AD directory and the Barracuda Email Security Service user list, click **Sync Now** to manually synchronize the Barracuda Email Security Service with your Azure AD directory.

If you select **Manual**, you must click **Sync Now** to synchronize the Barracuda Email Security Service with your Azure AD directory and add/update users.

12. To use SSO, click **Yes** for **Enable Single Sign On**. Once enabled, users are prompted to log in to their Microsoft Office 365 account when accessing their messages in the Barracuda Email Security Service.

13. To use the **Test Azure AD Configuration Settings** section, enter a valid email address in the **Testing Email Address** field to test your Azure AD settings.

14. Click **Test Settings**.

15. Click **Save** at the top of the page to save your settings and return to the **Domains** page.

If you previously set up LDAP authentication with your Barracuda Email Security Service account, your settings are not lost when you select **Azure AD** for a selected domain. Note, however, turning off Azure AD disables SSO and new users are not synchronized but recipient verification continues to function. For more information, see [How to Restore LDAP or Azure AD Directory Services](#).

### Step 7. Configure Outbound Mail

If you have more than one domain on your tenant (e.g., x.com and y.com) and you only want to filter one of the domains (like x.com), refer to [How to Configure Office 365 to Scan Only Selected Domains Outbound](#). The instructions in this section below describe how to filter for all domains for outbound mail.
If you have multiple outgoing account domains for Office 365, you only need to make one send connector in Office 365. You can use any one of the outbound smarthosts to make the send connector.

Each of your domains that you want to be able to send email must be added to Barracuda Email Security Service. Be sure to add all of your accepted Office 365 domains into Barracuda Email Security Service before configuring outgoing email in this section.

Outbound Groups must be enabled on your Barracuda Email Security Service account. Contact Barracuda Technical Support to request that Outbound Groups be enabled on your Barracuda Email Security Service account.

1. Log into your Barracuda Cloud Control account. On the left side, select Email Security. Select the Domains tab. For the appropriate domain, click Edit.
2. On the Domain Settings page, locate the Outbound Smarthost Configuration section and make note of the Hostname:

3. Log into the Office 365 admin center, and go to Admin centers > Exchange.
4. In the left pane, click mail flow, and click connectors.
5. Click the + symbol, and use the wizard to create a new connector.
6. From the From drop-down menu, select Office 365, and from the To drop-down menu, select Partner organization:
7. Enter a **Name** and (optional) **Description** to identify the connector:
8. Click **Next**. Select **Only when email messages are sent to these domains**, click the + symbol, and enter an asterisk ( * ) in the **add domain** field:

9. Click **OK**, and click **Next**. Select **Route email through these smart hosts**, and click the + symbol.

10. Go to the Barracuda Email Security Service, and click the **Domains** tab. Copy your outbound hostname from the MX records, and enter it in the **add smart host** page:
11. Click **Save**, and click **Next**. Use the default setting, **Always use Transport Layer Security (TLS) to secure the connection (recommended)** > Issued by Trusted certificate authority (CA):
12. Click **Next**. In the confirmation page, verify your settings and click **Next**. Office 365 runs a test to verify your settings:
13. When the verification page displays, enter a test email address, and click **Validate**. For this test, it is important to use an email address from outside your organization, like a gmail or yahoo email address.

There are two parts of the validation:

1. **Test Connectivity** – If this test fails, Outbound Groups is not enabled. Contact Barracuda Technical Support and request that Outbound Groups be enabled on your Barracuda Email Security Service account.

2. **Send Test Email** – If the test fails, there is no cause for concern. The test email comes from a Microsoft domain, not from your domain, so it is rejected. If you changed your domain away from onmicrosoft.com, the test should work.

14. Click **Save**. Your mail flow settings are added.

Barracuda Email Security Service now accepts outbound traffic from Outlook 365.

For additional configuration options and features, log into the Barracuda Email Security Service
Continue with [Step 3 - Complete Service Configuration](#).
Figures

1. BCC_ESS.png
2. dataRegion1.png
3. primaryDomain.png
4. specifyEmailServers2.png
5. spamProtection.png
6. confOutbound.png
7. verifyMX.png
8. verifySuccess.png
9. AddDomain.png
10. BypassSpamFiltering.png
11. SenderIPAddress.png
12. SpecifyIPranges.png
13. authorization.png
14. testAzureAD.png
15. outboundHost.png
16. MailFlowScenario.png
17. NewConnector2.png
18. AddSmartHost_Updated.png
19. TLS.png
20. confirmationUpdated.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.