Step 3 - Deploy Compliance Edition for Exchange Server

https://campus.barracuda.com/doc/74550085/

Use this article to deploy the Barracuda Cloud Archiving Service component for Exchange Server 2007 and 2010 in your environment. You must set up Barracuda Email Security Service *before* Barracuda Cloud Archiving Service.

> Barracuda Cloud Archiving Service is integrated with Barracuda Cloud Control LDAP. Barracuda Email Security Service has a separate LDAP configuration setup to support multiple user roles across configured domains.

Step 1. Activate the Service

1. Log into Barracuda Cloud Archiving Service, and click **Set up** to the right of **Cloud Archiving Service**:

Cloud Archiving Service	Set up ›

2. Select your geographic location from the **Country** drop-down menu, and click **Activate**.

Step 2. Add Users to Your Barracuda Cloud Control Account

Add users through AD authentication and associate a role and whose mail can be viewed with an AD user or group, or manually configure and assign roles to local accounts in the web interface.

Understanding Roles

- **User** – Able only to view messages accessible to the account, either because the username for the account is also that of the sender or recipient of a message, or because it has been given explicit access to view an email address via Alias Linking.
- **Auditor** – Able to create and activate policies, and view, search, and export any messages to/from the domains to which they have access. Additionally, Auditors can save and name an Advanced search for re-execution at a later time from the Saved Searches tab. To create a "Domain Auditor" (an auditor with access to only a subset of the domains on your Barracuda Cloud Archiving Service), set the role to Auditor and specify at least one domain. If no domains are specified, then all messages in the entire Barracuda Cloud Archiving Service are accessible. No auditor account has access to any system or network configuration information on the Barracuda Cloud Archiving Service.
- **Admin** – Able to view all items from any user, not just those listed for the account. Also able to

create and activate policies, and can make other system or network changes.

Active Directory Configuration

Use AD authentication to store and administer Barracuda Cloud Archiving Service user accounts via your organization's LDAP or Azure AD.

Add LDAP Active Directory

Use the following steps to set up Barracuda Cloud Control LDAP authentication:

1. Log into https://login.barracudanetworks.com/ as the account administrator, and go to **Admin > Directories**.
2. Click **Add Directory > LDAP Active Directory** ; the **Create Directory** wizard displays. In the **Info** page, specify the following details:
    1. Enter a name to represent the directory in the **Directory Name** field.
    2. Toggle **User / Group Sync** to **On** to synchronize with AD.
    3. Toggle **Authenticate** to **On** to allow users to authenticate using their LDAP AD credentials. When toggled **Off**, users must authenticate using their Barracuda Cloud Control credentials.
    4. Optionally, enter the administrator contact email address.
3. Click **Save & Continue**.
4. In the **Host** page, enter the following details for your LDAP host:
    1. **LDAP Host IP address**
    2. **LDAP Host Port**
    3. **Base domain name**
    4. **Username**
    5. **Password**
    6. Select the **Connection Security** as **STARTTLS**, **LDAPS**, or **None**.
5. Click **Add Domain**; the domain is added to the **Domains** field. Click **Verify**.
6. Click **Test** to verify connectivity. If the connection is successful, **Connected** displays. If the connection fails, verify the entered LDAP host details. Click **Continue.**
7. In the **Domains** page, click **Add domain** to add the domain to the AD configuration. Complete this step for each domain you want to add.
8. To verify you own the domains you plan to include in your AD configuration, select the manner in which to verify the domains:
    ○ Copy a META tag to your domain header, *or*
    ○ Add a TXT record to your host's DNS management settings

Verify domain: ldap.domain ✕

This domain is not yet verified. Domains must be verified to create an Active Directory. Select a verification method.

Meta Tag

Add the following META tag to the header of ldap.domain.

```
<!--barracuda site verification -->
<meta name="barracuda-site-verification"
content="b4d6fe289bae81fb36a3b588bc2f442f" />
```

COPY TAG TO CLIPBOARD

TXT Records

Add this in your domain host's DNS management settings.

Name/Alias	TTL	Record Type	Value/Answer
@	3600	TXT	b4d6fe289bae81fb36a3b588bc2f442f

COPY VALUE TO CLIPBOARD

CLOSE   **VERIFY**

9. Click **Verify**. Once the domain is verified, it is added to the **Directories** table in the **Admin > Directories** page in Barracuda Cloud Control.

Add Azure Active Directory

See also: [Azure AD with Active Directory Federation Services](#)

Use the following steps to set up Barracuda Cloud Control Azure AD authentication:

1. Log in to https://login.barracudanetworks.com/ as the account administrator, and go to **Admin > Directories**.

2. Click **Add Directory > Azure Active Directory**; the **Create Directory** wizard displays. In the **Info** page, enter a name to represent the directory in the **Directory Name** field.
3. Click **Connect to Microsoft** to sign in to Microsoft and authorize Barracuda Cloud Control to connect to your Azure AD account.
4. Once authorization is complete, toggle **User / Group Sync** to **On** to synchronize with Azure AD.
5. Toggle **Authenticate** to **On** to allow users to authenticate using their Azure AD credentials. When toggled **Off**, users must authenticate using their Barracuda Cloud Control credentials.
6. Optionally, enter the administrator contact email address. Click **Save & Continue**.
7. Once verification is complete, your Azure AD domains display in the wizard. Click **Done**.

Associate a Role

1. Go to the **Users > LDAP User Add/Update** page.
2. In the **LDAP User/Group** field, enter the User or Group name to which the permissions apply.
3. Select the **Role** for the specified user or group account:
    1. **User Role** – Specify mailbox addresses to include or exclude from the account:
        - **Include these Addresses** – Enter a mailbox address that you wish to make available to the specified account, and then click **Add**.
        - **Exclude these Addresses** – Enter a mailbox address that you wish to hide from the specified account, and then click **Add**.
    2. **Auditor Role** – Configure the desired permissions:
        - **Domains** – Enter a domain for which the auditor can view mail, and then click **Add**.
        - **Saved Search** – Define Saved Searches on the **Basic > Search** page, and then select the desired Saved Search from the drop-down menu to filter the auditor's search results.
        - **Exclude these addresses** – Enter a mailbox address that you want to hide from the specified account, and then click **Add**.
    3. **Admin Role** – Specify mailbox addresses that you want to hide from the specified account, and then click **Add**.
4. Click **Save**.

Manually Add Local Accounts

Local accounts reside only on the Barracuda Cloud Archiving Service.

1. Go to the **Users > User Add/Update** page, and enter the user's **Email Address** and the **User Display Name**.
2. Enter all aliases associated with the entered email address, one entry per line.
3. Enter the account password and select the user role for the account.
4. If you select the user role **Auditor** enter the following additional details:

○ Enter a domain for which the auditor can view messages and other Outlook items, and click **Add**. Any messages that includes an email address in the listed domains in either the **From**, **To**, or **CC/Bcc** areas, or any items that belong to a user in the specified domains, display in search results. To allow the auditor to view all items from all domains, leave this field blank.

○ In the **Saved Search** drop-down menu, select a defined Saved-Search to automatically apply to all searches performed by this auditor. Note that the parameters in the Saved Search take precedence over any domain limitations that may be specified above, as well as over any attempts by the auditor to *Search As* any other account.

Step 3. Set Up Journaling

Depending on your Client Access Licenses (CALs), you may need to apply these rules at the mail server level rather than the hub transport level. For more information, see the Microsoft TechNet article [Overview of Compliance Features](#).

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

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

Step 1. Create Remote Domain

Before Proceeding, verify you have your journaling address from the **Mail Sources > SMTP Journaling** page in the Barracuda Cloud Archiving Service web interface.
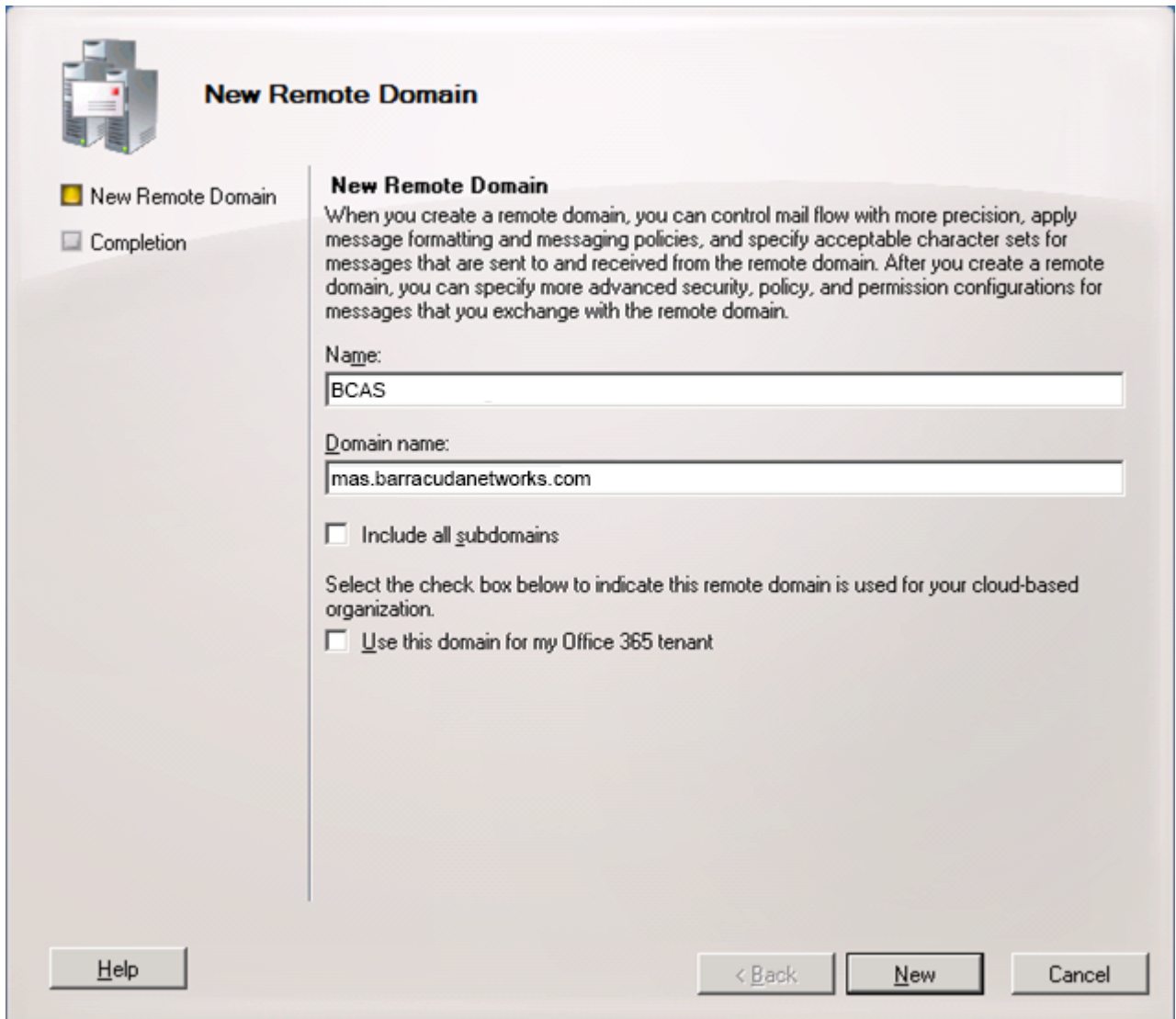
The Remote Domain must match the Mail Contact that is the recipient of journaled messages as it is used by the Exchange Server for routing all SMTP Journal traffic. Use the following steps to create a remote domain:

1. Open the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and click

the **Remote Domains** tab in the center pane.

2. In the **Actions** panel in the right pane, click **New Remote Domain.** The **New Remote Domain** dialog displays.

3. In the **Name** field, type   BCAS, and in the **Domain name** field, type your region-specific MAS hostname, for example: `mas.barracudanetworks.com`

    See [Data Centers by Region](#) for a list of region-specific MAS hostnames.

New Remote Domain

- New Remote Domain
- Completion

New Remote Domain

When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging policies, and specify acceptable character sets for messages that are sent to and received from the remote domain. After you create a remote domain, you can specify more advanced security, policy, and permission configurations for messages that you exchange with the remote domain.

Name:

`BCAS`

Domain name:

`mas.barracudanetworks.com`

☐ Include all subdomains

Select the check box below to indicate this remote domain is used for your cloud-based organization.

☐ Use this domain for my Office 365 tenant

Help   < Back   New   Cancel

4. Click **New** to verify the domain settings, and click **Finish** to save your settings. The newly created domain displays in the **Remote Domains** list.

5. Double-click on the newly created domain to open the **Properties** dialog for the newly created domain, and:
    - In Exchange 2007, select **Format of original message sent as attachment to the journal report**.
    - In Exchange 2010, select the **Message Format** tab in the **Properties** dialog box.

6. Select the following options to ensure journal messages sent to this domain are *MIME Plain Text* format (rather than the unsupported *Exchange Rich Text* format):
    - In the **Message Format Options** section, turn on **Allow automatic forward**.

- In the **Exchange rich-text format** section, select **Never Use**:
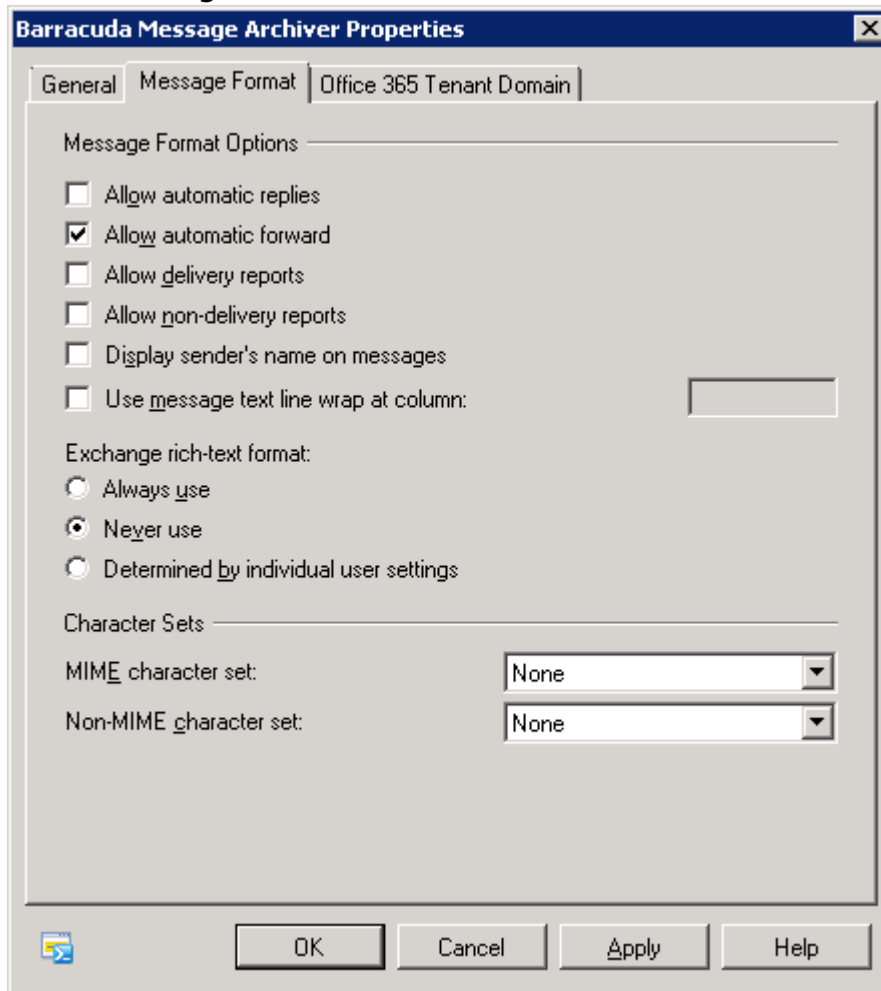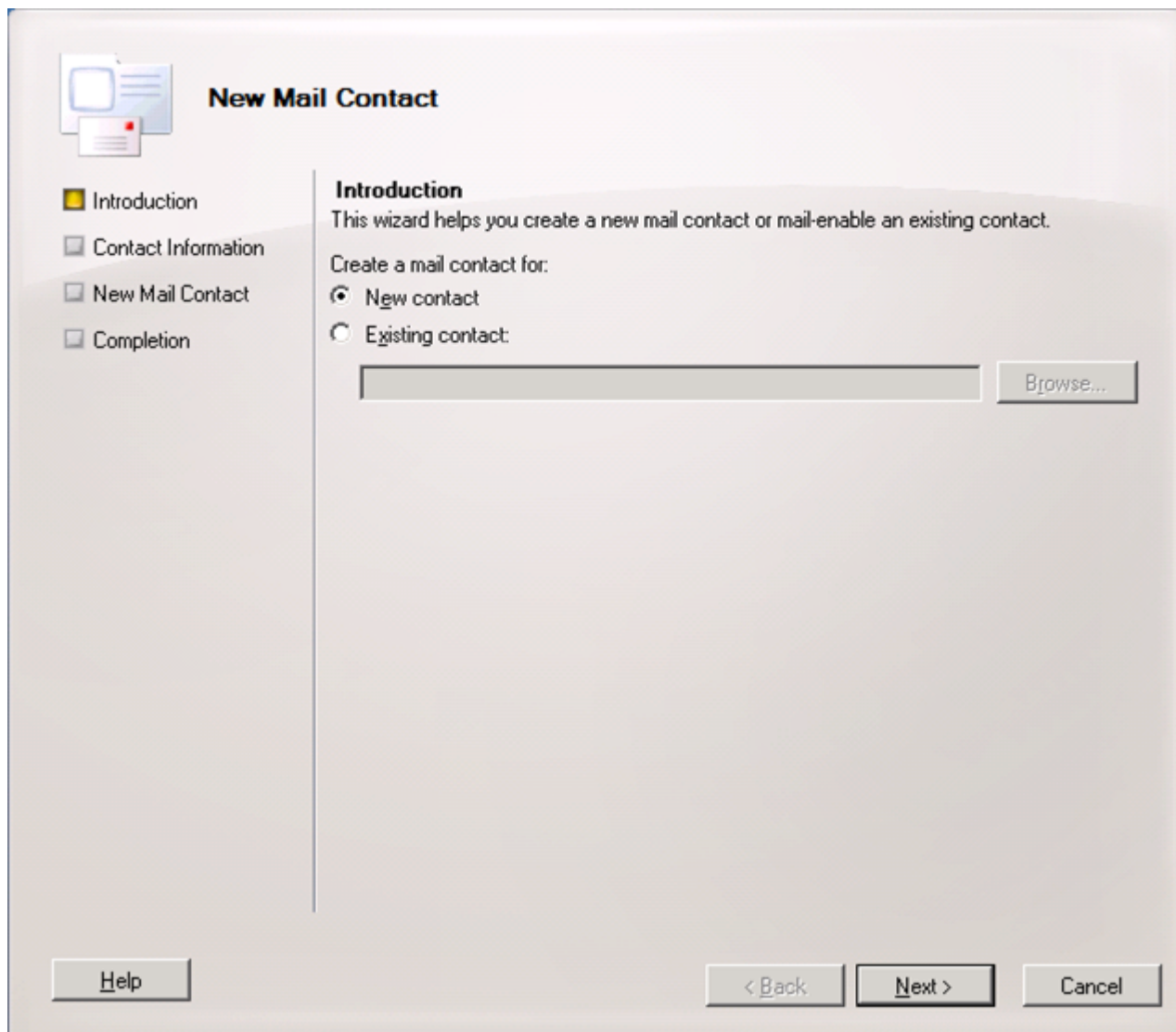
> Verify that only **Never use** and **Allow automatic forward** are selected in the dialog box.

7. Click **Apply** to save your settings, and click **OK** to close the **Properties** dialog.

Step 2. Create Mail Contact
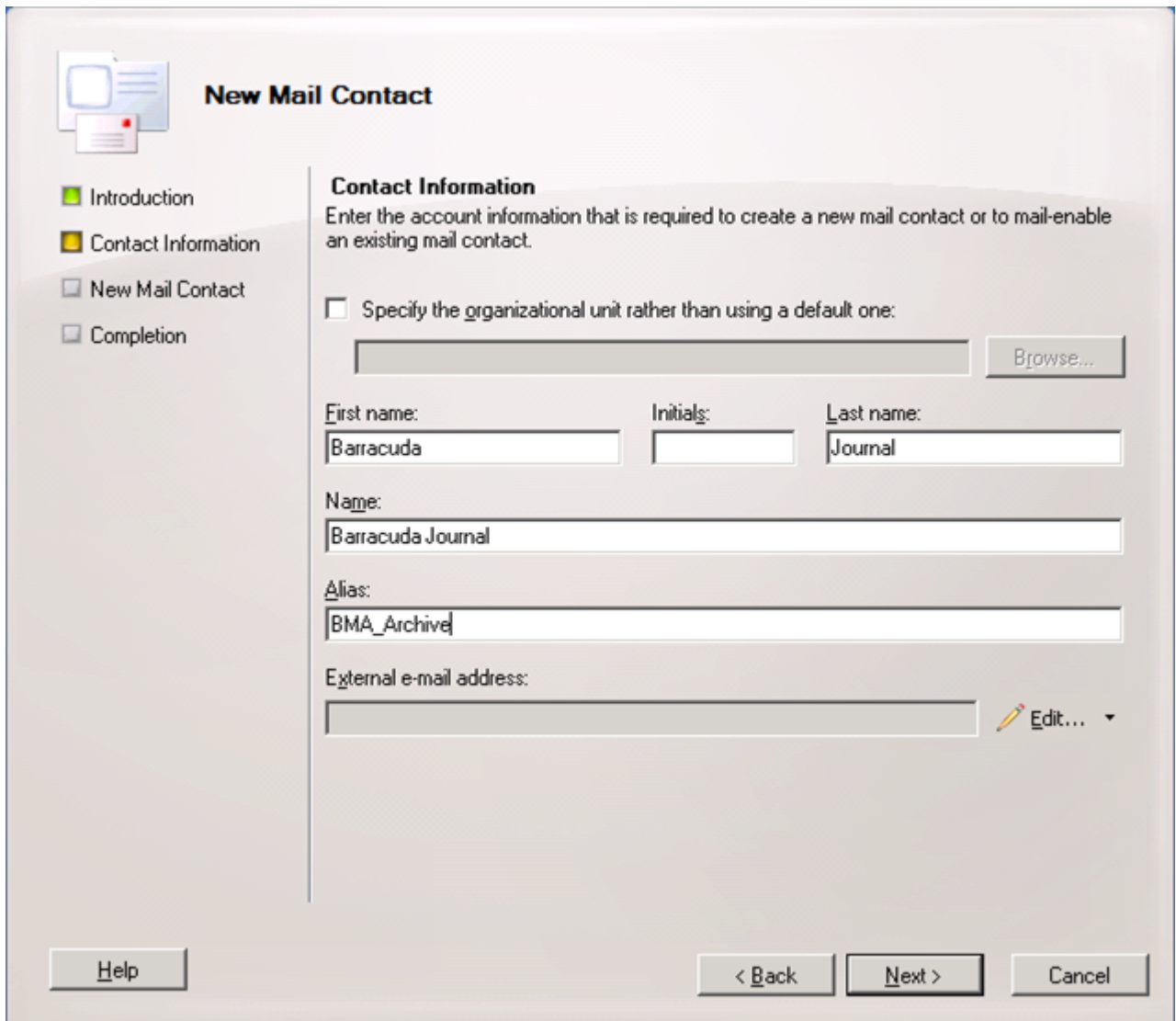
The Mail Contact is the account that is to act as a "holding location" for journaled messages. The email address associated with this account is the designated recipient. Use the following steps to create a Mail Contact:

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

2. In the dialog, select **New Contact**, and click **Next**.
3. Enter a **First name** and **Last name**; the **Name** field automatically populates based on the entered values. Enter an **Alias**:
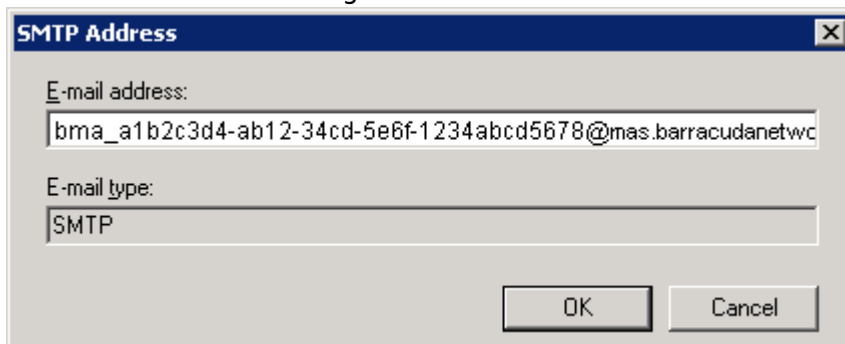
4. Click **Edit** to the right of the **External e-mail address** field, and in the **SMTP Address** dialog, enter the journaling address from the **Mail Sources > SMTP Journaling** page in the Barracuda Cloud Archiving Service web interface:
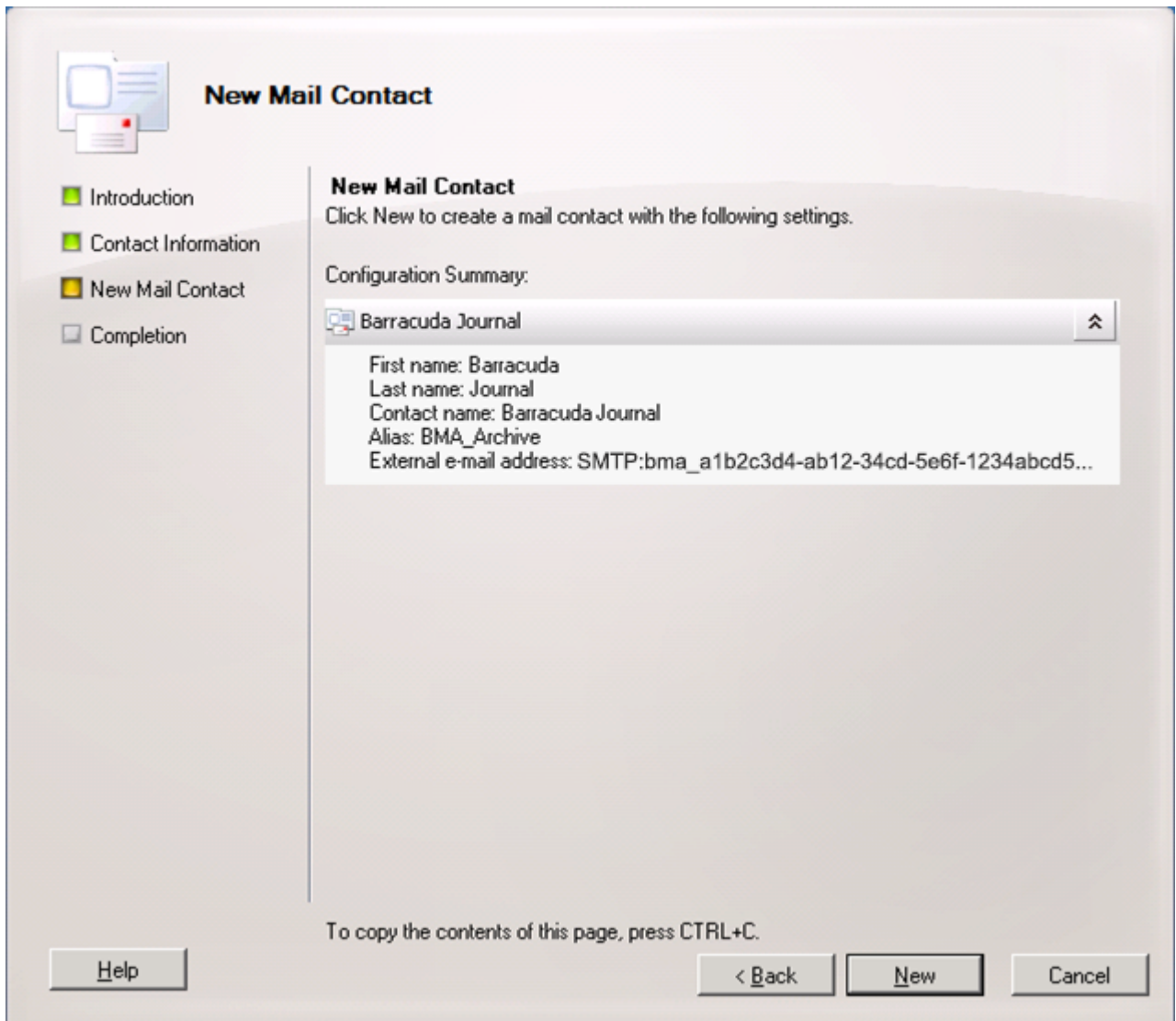
5. Click **OK** to close the dialog box. In the Wizard, click **Next** to verify the information:
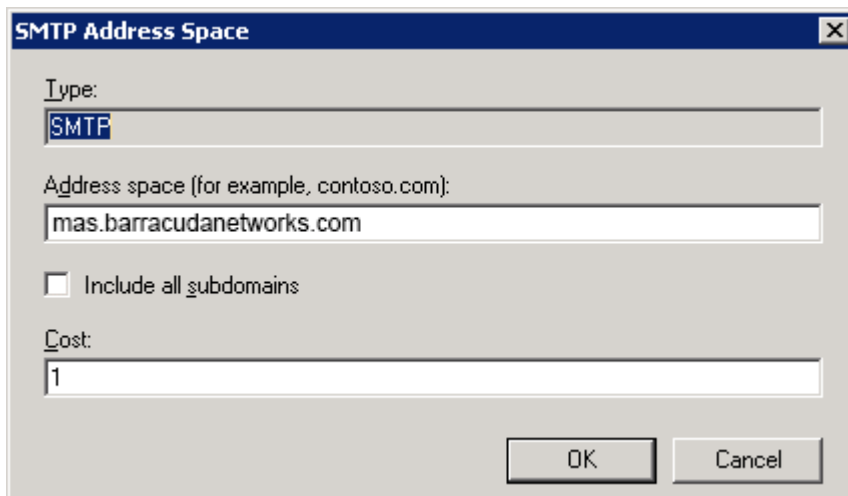
6. Click **New** to create the Mail Contact. The newly-created contact appears in the **Mail Contact** list. Click **Finish** to close the Wizard.

Step 3. Create Send Connector

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

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

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

7. Click **Next**. In the **Source Server** page, if your Exchange server is not already listed, click **Add** to search for and add the server to this list. Click **Next** to verify your configuration, and click **New** to create the Send Connector. Click **Finish** to return to the   **Send Connectors** tab; the newly-created Send Connector displays in the list.

8. Right-click on the new Send Connector, and click **Properties**.

9. In the **Properties** dialog box, clear **Maximum message size (KB)**:
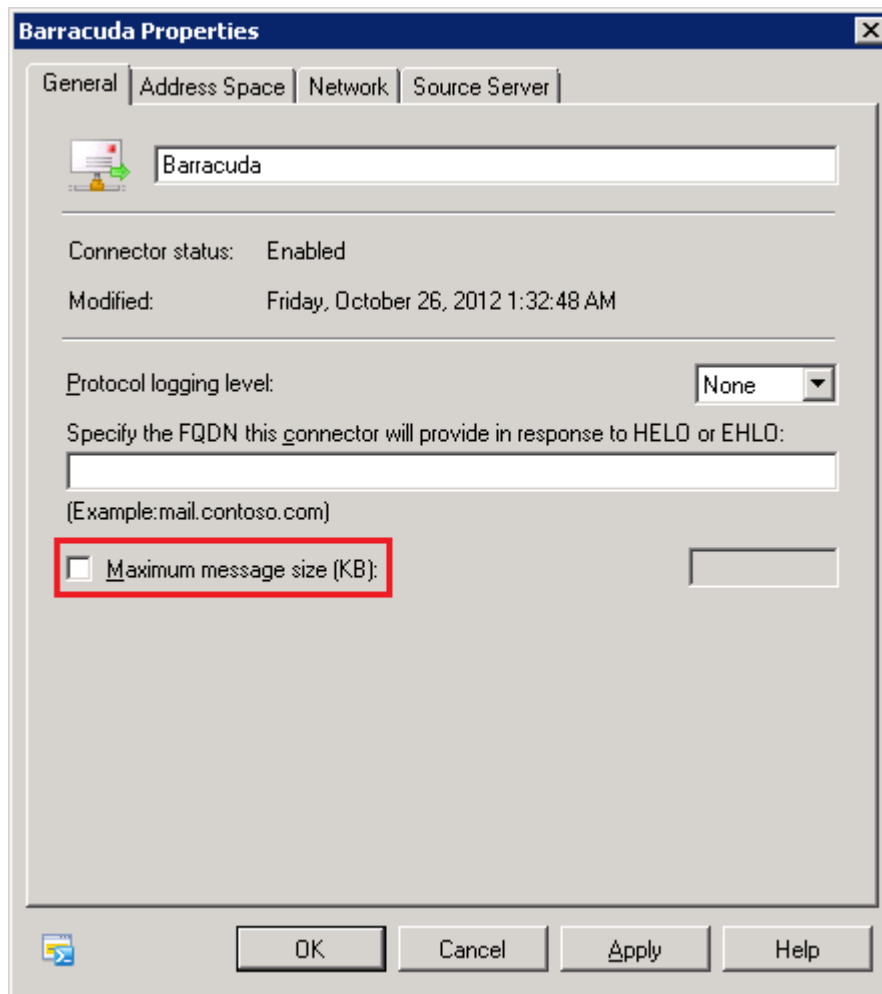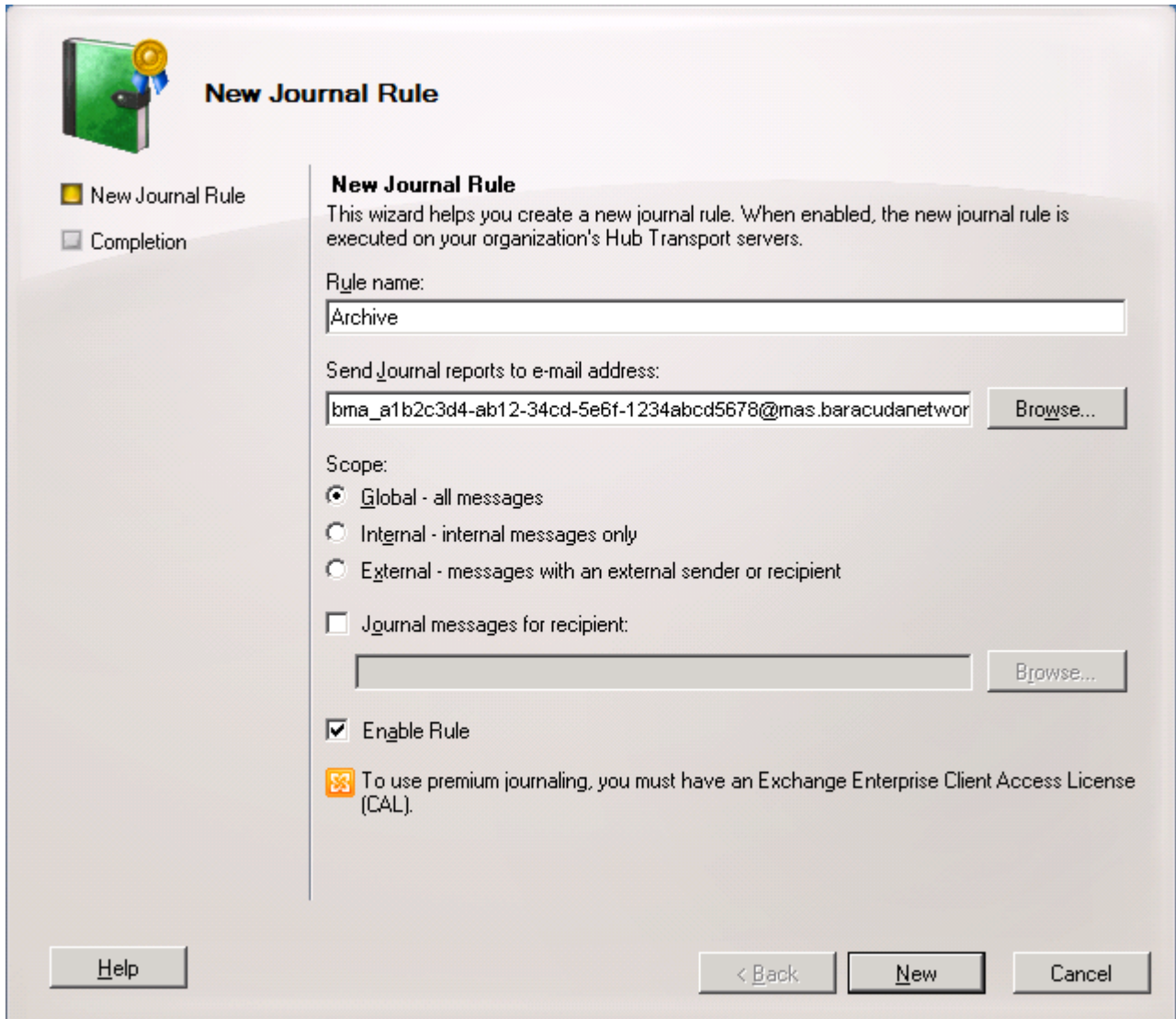
10. Click **Apply**, and then click **OK** to save your changes and close the dialog box.

Step 4. Create Journaling Rule

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

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

4. Select the Scope for archiving; the recommended setting is **Global - all messages** for the most complete coverage.

5. Turn on **Enable Rule**, click **New** to create the Journaling rule, and click **Finish** to return to the **Journal Rules** tab where the newly-created rule displays in the list.

Use Case Examples

This section includes a set of examples you can walk through to further evaluate the Barracuda Cloud Archiving Service.

Example 1. Add a User in the Auditor Role who can View and Search Mail without Domain Limits.
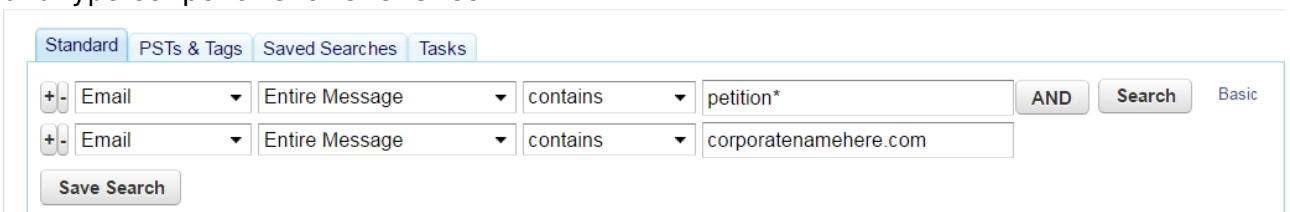
The Barracuda Cloud Archiving Service supports three user roles:

- **User** – The *user* can view and search content associated with their own mailbox and any shared mailboxes.
- **Auditor** – The *auditor* can view all items from any user, and can create and activate policies. Note that the auditor role can be restricted to specific domains and Saved Searches by the Admin role.
- **Admin** – The *admin* can view all items from any user, create and activate policies, and make system and network changes.
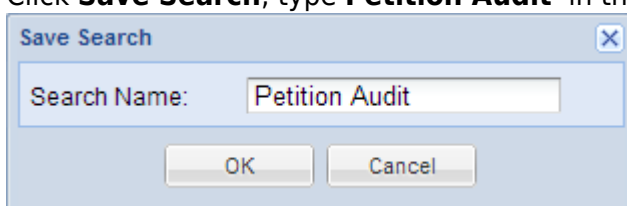
In this example, the administrator adds Ryan in the auditor role without domain limits:

Step 1: Create a Saved Search

1. On the **Basic > Search** page, click **Advanced**. Select **Email > Entire Message > contains**, and type `petition*` as the first set of search criteria.
   Using the asterisk (*) wildcard returns the words petition, petitions, petitioned, petitioner, and petitioning.
2. Click the **+** symbol to the left of the search parameter, select **Email > Domain > contains**, and type `corporatenamehere.com`:

3. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
4. Click **Save Search**, type **Petition Audit** in the **Search Name** field:

5. Click **OK**; the search is added to the **Saved Searches** page.

Step 2: Add User

1. On the **Users > LDAP User Add/Update** page, enter the user's email address, `rdouglas@corporatenamehere.com`, in the **LDAP User/Group** field.
2. Select **Auditor** from the **Role** drop-down menu.
3. Leave the **Domain** field blank to allow Ryan to access all items from all domains.
4. From the **Saved Search** drop-down menu, select **Petition Audit**:

5. Click **Save** at the top of the page to add the new user.

Ryan is added as a user with the auditor role, and the Petition Audit Saved Search criteria is automatically applied to all searches performed by Ryan.

Example 2. Create a Litigation Hold (Auditor Role Only).

Additional Resources

For more information, refer to the article Litigation Holds, or log in to your Barracuda Cloud Archiving Service using the Auditor role, and go to either of the following pages:

- **Policy > Retention** page, and click **Help**
- **Basic > Search > Saved Search** page, and click **Help**

A user with the auditor role can create litigation holds which prevent messages matching the criteria of a specific Saved Search from being removed from the Barracuda Cloud Archiving Service. On the **Basic > Search > Saved Search** page, litigation hold details include:
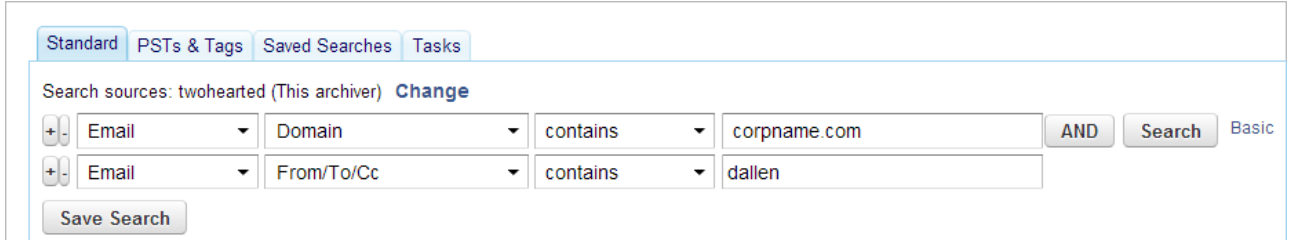
- **Auditor** – The account name of the auditor who created the Litigation Hold
- **Saved Search** – The name of the Saved Search associated with this Litigation Hold
- **Hold End Date** – The date and time when this Litigation Hold expires

Before an auditor can set up a litigation hold, the administrator must first enable litigation holds by completing the following steps:
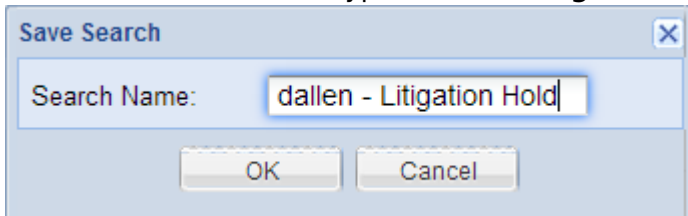
1. Log into the Barracuda Cloud Archiving Service, and go to the **Policy > Retention** page.
2. Set **Enable Litigation Holds** to **Yes**, and click **Save**.

In this example, Sue is a user with the auditor role at a large corporation, and has been asked to set up a litigation hold to retain all emails related to the user '**Dallen**' from their client '**CorpName**'. Sue uses the following steps to set up the litigation hold:
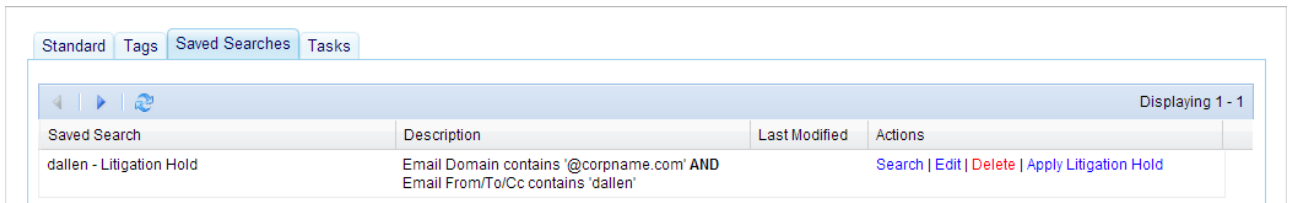
1. Log into the Barracuda Cloud Archiving Service in the auditor role.
2. Go to the **Basic > Search** page, and click **Advanced**.
3. Select **Email > Domain > contains**, and type **@corpname.com** as the domain name. Click the **+** symbol to the left of the search parameter.
4. Select **Email > From/To/Cc > contains**, and type **dallen** as the second set of search criteria:

5. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
6. Click **Save Search**, and type **dallen - Litigation Hold** as the **Saved Search** name:

7. Click **OK**. Click the **Saved Searches** tab:

8. In the **Actions** column, click **Apply Litigation Hold**. In the **Apply Litigation Hold** window, to hold the associated emails indefinitely, click **None**, or you can specify a specific expiry date.
9. For this example, select **Specific Date**, click the **Calendar** icon, and select the date to end the litigation hold.
10. Click **OK** to apply the litigation hold.

Once a litigation hold is added, it displays in the **Litigation Holds** section on the **Policy > Retention** page when a user is *logged in using the admin role*:

Example 3. Create Retention Policies

> **Additional Resources**
>
> For more information, refer to the article Retention Policies, or log in to your Barracuda Cloud Archiving Service, go to the **Policy > Retention** page, and click **Help**.

By default, automated message purging on the Barracuda Cloud Archiving Service is disabled. If you enable this ability, the Global Retention Policy and any Saved-Search retention policies are compared to all archived messages once a week. You can allow these messages to be deleted from the Barracuda Cloud Archiving Service based on the Saved Search retention policies. Note that before you can create a Saved Search retention policy, you must create at least one Saved Search in the **Basic > Search > Advanced Search** page.
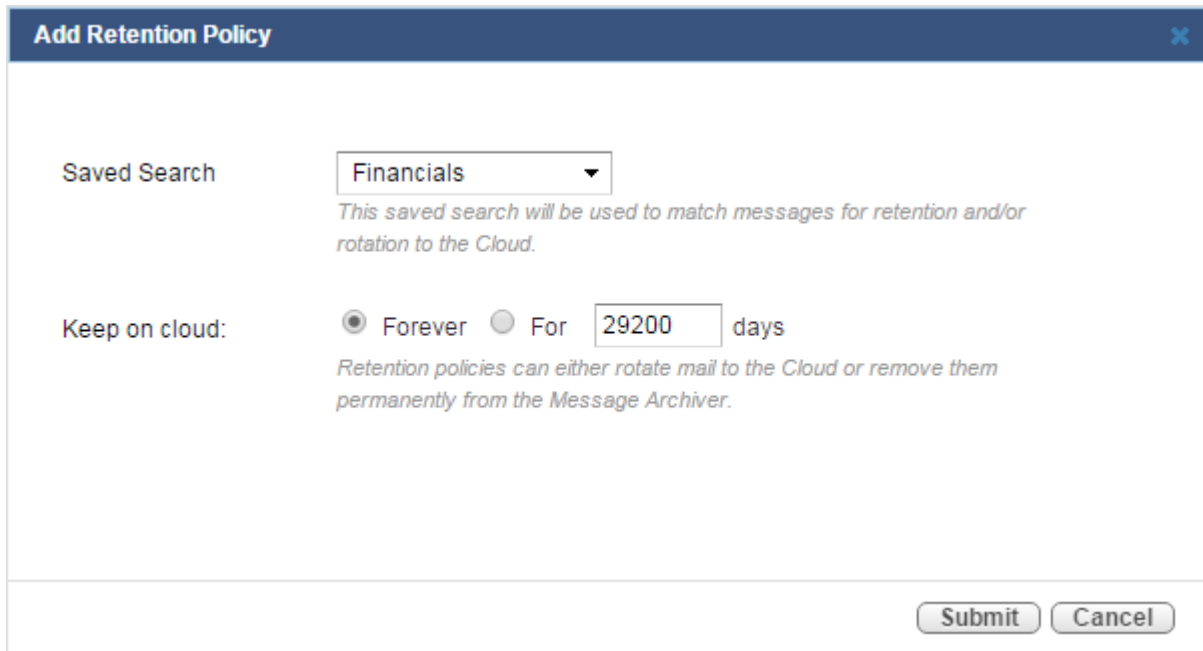
A Saved Search retention policy enables you to automatically expire messages matching a specified saved search. Use this feature to create exceptions to the Global Retention Policy.

Important

- The Global Retention Policy setting does not apply to any messages that match a Saved-Search retention policy. If the age of any message exceeds the maximum age allowed by all Saved-Search retention policies that apply to the message, that message is *permanently deleted from the Barracuda Cloud Archiving Service*.
- Saved searches containing tags, folders, or discovery fields cannot be used in a Saved Search retention policy and do not appear in the list of available Saved Searches.
- If a message matches more than one Saved Search-based policy, then the message is kept according to the longest policy length. If it matches a Saved Search-based policy and the global retention policy, then the Saved Search policy takes precedence.
- Once the Global Retention Policy is set, archived messages are automatically deleted from the Barracuda Cloud Archiving Service.

In this example, Kari is the administrator and wants to set the maximum age of a set of archived messages before they are permanently purged from the archive. Kari uses the following steps to set up a retention policy based on a Saved Search:

1. Go to the **Basic > Search** page, and create a Saved Search with the desired criteria.
2. Go to the **Policy > Retention** page, and set **Allow automatic message deletion** to **Yes**.
3. Note the value of the **Policy Length** that is set for the Global Retention Policy.
4. Click **Add Retention Policy**, and set the retention policy criteria:

5. Click **Submit** to save the Saved Search retention policy, and then click **Save** in the **Policy > Retention** page and add it to the table.

Example 4. Search Mail Using the Web Interface.

> **Additional Resources**
>
> All user roles can view and search content associated with their own mailbox and any shared mailboxes.
>
> For more information, refer to the articles Search Options and Advanced Search Options, or log in to the web interface, go to the **Basic > Search** page, and click **Help**.

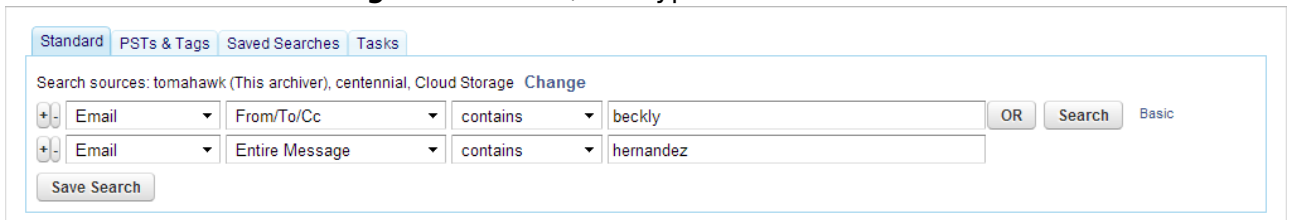There are two search modes on the **Basic > Search** page:

- **Basic** – Run a search based on a word or phrase across all messages accessible by your account.
- **Advanced** – Run a complex search query based on multiple criteria; note that you can save queries for future use.

When you initially go to the **Basic > Search** page, all messages accessible by your account display in the message list in the **Standard** tab.

Use the Basic Search mode to perform a quick search across all of your messages. Use Advanced Search mode to perform complex search queries based on selected attributes.

In this example, Uma works in a real estate office. She recently closed a sale for property on Hernandez Avenue with M. Beckly. The procedure in the office is to burn a CD with all correspondence regarding a sale once the sale is complete. Uma needs to search for all messages related to the sale, and then export the messages to a .**zip** file:

1. Log into the Barracuda Cloud Archiving Service as a user.
2. Go to the **Basic > Search** page, and click **Advanced**.
3. Select **Email > From/To/Cc > contains**, type beckly as the first set of search criteria, and then click the **+** symbol to the left of the search parameter.
4. To the right of the first set of search criteria, click **AND** to toggle to **OR**.
5. Select **All > Entire Message > contains**, and type hernandez:

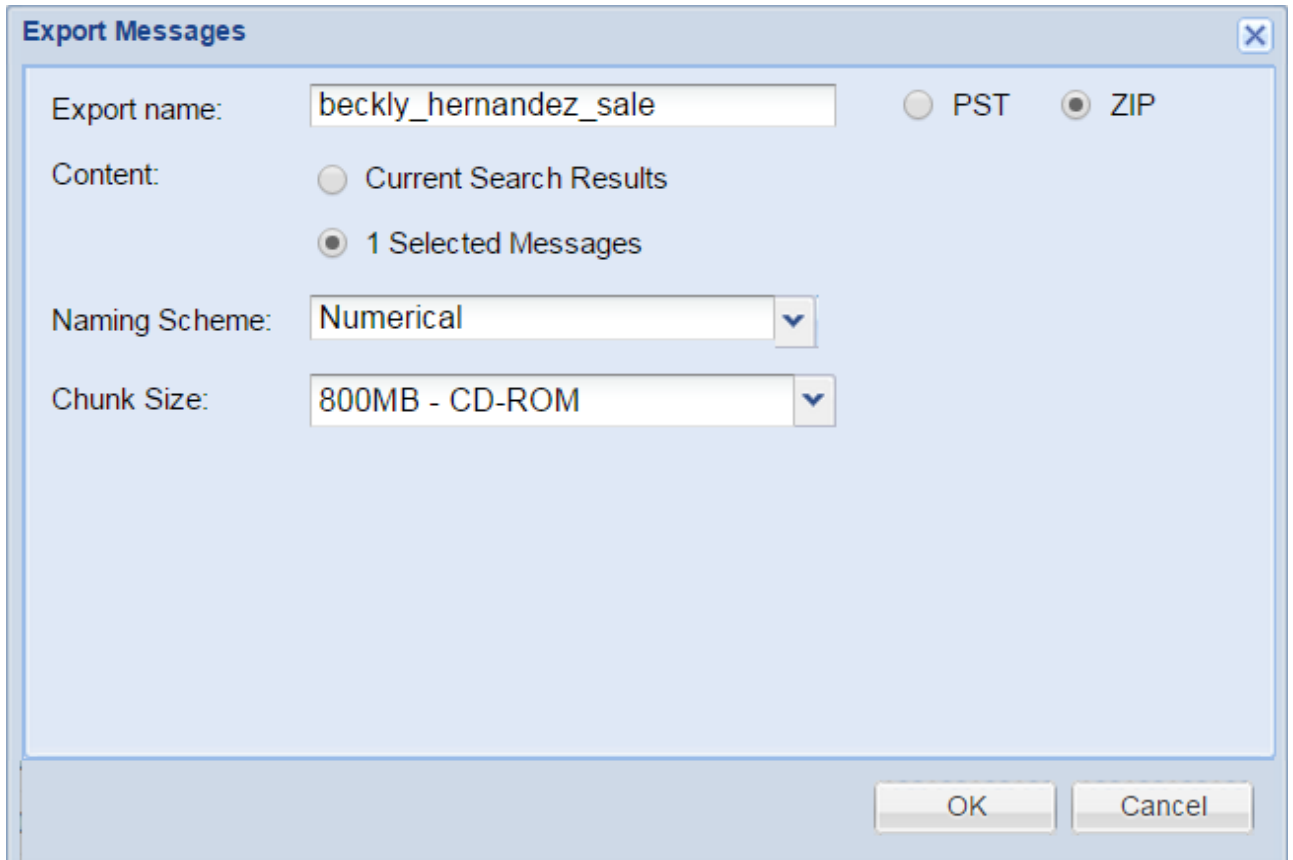6. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
7. In the results window, use **Ctrl-** and **Shift-**click to select all of the messages to include in the .**zip** file.
8. Click the **Tools** menu, and select **Export Messages**; in the **Export Messages** dialog box, specify the export details:

9. Click **OK**. Go to the **Tasks** tab to view the download progress. Once the download is complete, select the export, and click **Download** to save the .**zip** file to your local system.

Uma can now burn the .**zip** file to a CD to place in M. Beckly's customer file.

Example 5. Set Up Authorized Search of Another User's Email.

In this example, Abe is a legal assistant for Dale. Dale often needs Abe to search through his email on his behalf. To avoid sharing Dale's LDAP credentials with Abe, the administrator creates a local user account with entitlements so that Abe can access Dale's email:

Step 1. Administrator Creates a Local User Account

1. Login to the Barracuda Cloud Archiving Service as the account administrator.
2. Go to the **Users > LDAP User Add/Update** page.
3. Type Abe's email address, abe@corporate.com, in the **Email Address** field, and select **User** from the **Role** drop-down menu.
4. In the **Include These Addresses** field, type Dale's email address, dale@corporate.com:

5. Click **Add**, and click **Save**.

Step 2. Abe Searches Dale's Email

Dale asks Abe to search his account for all email correspondence with MarilynCorp during May, 2015.

1. Abe logs in to the Barracuda Cloud Archiving Service.
2. Go to the **Basic > Search** page, and click **Advanced**.
3. Select **Email > Entire Message**, and type **MarilynCorp** as the first set of search criteria.
4. Click the **+** symbol to the left of the search parameter. To the right of the first set of search criteria, leave the value as **AND**.
5. Select **Email > Date > on or after** , click in the associated field, and type or select the date **2015-05-01**.
6. Click the **+** symbol to the left of the search parameter. To the right of the first set of search criteria, leave the value as **AND**.
7. Select **Email > Date > on or before** , click in the associated field, and type or select the date **2015-05-31**:


8. Click **Search** to execute the search.

Step 3. Abe Saves Search Results

Abe now saves the search results as a **.csv** file that his manager, Dale, can download from the **Tasks** tab.

1. Once the search results are returned, from the **Tools** menu, click **Save Results as CSV**.
2. In the **Export Name** field, type **MarilynCorpArchive**:

Save Search Results as CSV

Export name: MarilynCorpArchive

OK   Cancel
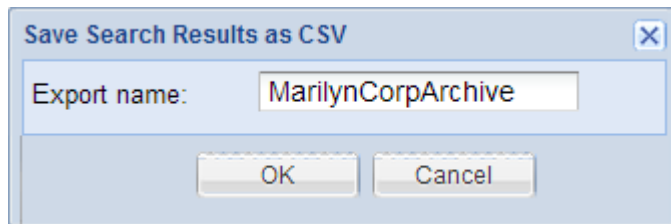
3. Click **OK**. The **.csv** file is now available for download from the **Tasks** tab.
4. Dale selects the item in the table, and clicks **Download** to save the **.csv** file to his local system.

Example 6. View Statistics.

Additional Resources

For more information, refer to the article Viewing Performance Statistics or log in to your Barracuda Cloud Archiving Service, go to the **Basic > Dashboard** page, and click **Help**.

View operating status on the **Basic > Dashboard** page when you log in to the Barracuda Cloud Archiving Service using either the auditor or administrator role as described in the following table. Please note statistics are cached and may take up to thirty minutes to appear.

Status Type	Description
Message Statistics	A snapshot of archived email, appointments, contacts, distribution lists, notes, and tasks.
Performance Statistics [1]	Current operating status and performance of the Barracuda Cloud Archiving Service.
Storage Statistics [1]	Statistics on the amount of data stored on the Barracuda Cloud Archiving Service by hour, day, and total.
Subscription Status [1]	Current status of your Barracuda Cloud Archiving Service subscription.
Email Statistics	Breakdown of message traffic and policy violations for the last 24 hours and last 30 days.
Note: [1]Statistics for this item are not visible when a user is logged in with the auditor role.	

Example 7. Tools and Add-Ins.

Additional Resources

For more information, log in to your Barracuda Cloud Archiving Service, go to the **Users > Client Downloads** page, and click **Help**.

You can download and install Barracuda Cloud Archiving Service tools and add-ins to your local system.

- **Barracuda Cloud Archiving Service Outlook Add-In** – The Barracuda Cloud Archiving Service Outlook Add-in allows users to perform various functions with messages that are stored on your organization's Barracuda Cloud Archiving Service, including:

  These functions are available directly from Outlook, allowing transparent access to your messages and attachments, all with no browser interaction required. All that is needed is a network connection to your organization's mail server and to the Barracuda Cloud Archiving Service.

  - Synchronization of your archived folders with Outlook
  - Search for archived messages and other Microsoft Outlook data, such as Contacts
  - View and interact with (forward, reply to, etc.) all of your archived Outlook items
  - Archive messages

- **Barracuda Cloud Archiving Service Standalone Search Utility** – The Stand-Alone Search Utility provides access to the search features of the Barracuda Cloud Archiving Service for Mac OS X and Microsoft Windows users. This utility allows users to search through their own archived messages directly from their desktop without needing to log in to the Barracuda Cloud Archiving Service web interface, and perform actions such as forwarding or replying to the located messages.

Figures

1. BCASSetup.png
2. VerifyDomain.png
3. CreateRemoteDomain.png
4. bmaproperties.png
5. newmailcontact.png
6. newmailcontact2.png
7. 2007-mail-contact-4-journaling-address.png
8. newmailcontact3.png
9. smtpaddressspace.png
10. SendConnector02.png
11. UseDefault.png
12. send_connector_properties.png
13. 2007-journaling-rule-3.png
14. BCASPetitionEx.png
15. BCAS_eval03.png
16. add_LDAP_user.png
17. BCASDallen.png
18. BCAS_eval05.png
19. LitigationDallen.png
20. litigation08.png
21. BCAS_eval06.png
22. ArchiveSearch.png
23. ExportMsgs.png
24. Example6.png
25. BCAS_eval08.png
26. export_csv.png