

How to Journal to the Cloud Archiving Service from G Suite

<https://campus.barracuda.com/doc/46892517/>

Use this article to deploy the Barracuda Cloud Archiving Service component of Advanced Email Security and Compliance for G Suite in your environment.

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.

To deploy the Barracuda Archiving Service with G Suite, you must have a G Suite Basic, Business, or Enterprise account. The legacy free edition of G Suite is missing key features required for this deployment. For details on upgrading your G Suite subscription, refer to the Google Support article [G Suite legacy free edition](#).

You must configure G Suite to send archived mail directly to the Barracuda Cloud Archiving Service.

Google IP address ranges and user interface can change; refer to the G Apps Administrator Help articles [Google IP address ranges](#) and [Add mail routes with the Hosts tab](#).

G Suite Enterprise and G Suite Enterprise for Education include some built-in archiving capability. For additional information, see the G Suite Administrator Help solution [Integrate Gmail with a third-party archiving solution](#).

Step 1. Activate the Service

1. Log in to 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 LDAP authentication and associate a role and whose mail can be viewed with an

LDAP 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

Add LDAP Active Directory

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

1. Log in to <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:

Create Directory ✕

INFO HOST DOMAINS

Directory Name

User / Group Sync

Authentication

Contact Email (Optional)

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 LDAP User or Group name to which the permissions apply.
3. Select the **Role** for the specified LDAP user or group account:
 1. **User Role** - Specify mailbox addresses to include or exclude from the LDAP account:
 - **Include these Addresses** - Enter a mailbox address that you wish to make available to the specified LDAP account, and then click **Add**.
 - **Exclude these Addresses** - Enter a mailbox address that you wish to hide from the specified LDAP 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 LDAP account, and then click **Add**.
 3. **Admin Role** - Specify mailbox addresses that you want to hide from the specified LDAP account, and then click **Add**.
4. Click **Save**.

For end-user authentication, refer to [How to Set Up LDAP Groups for End-User Authentication](#).

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. Obtain Your Journaling Address

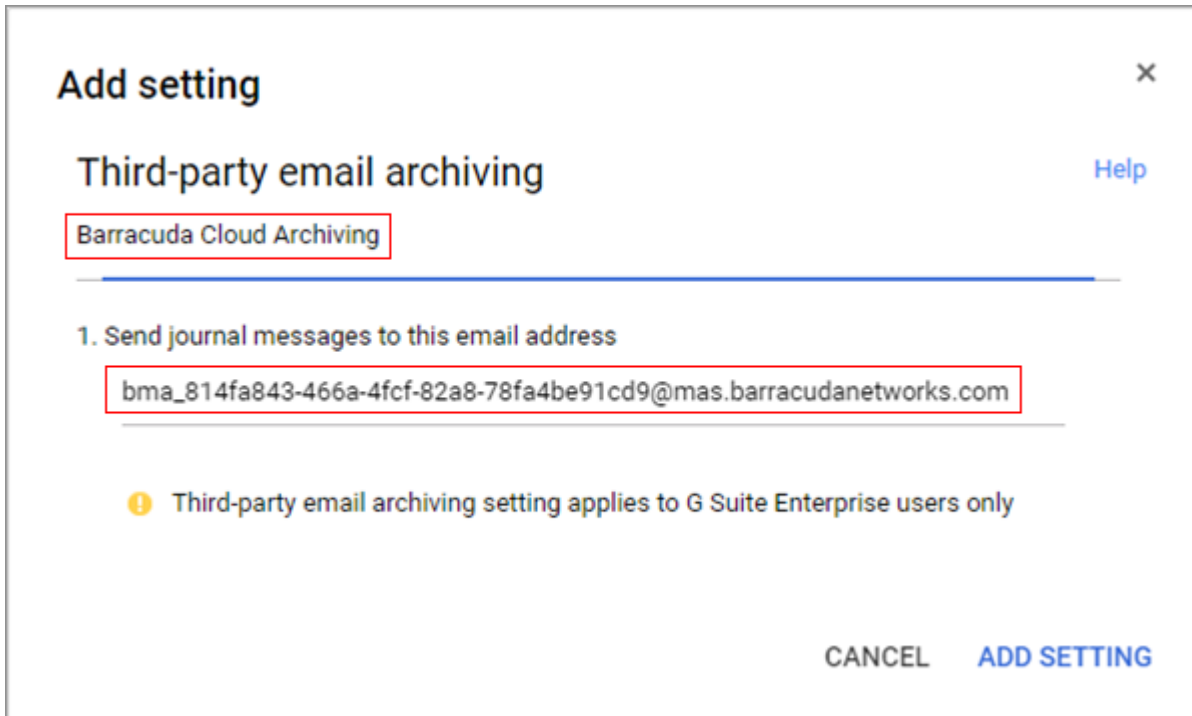
1. Log in to the Barracuda Cloud Archiving Service, and go to the **Mail Sources > SMTP Journaling** page.
2. Verify your journaling address.

Step 4. Configure G Suite

- G Suite Enterprise - If you are using G Suite Enterprise, use the steps in the section *G Suite Enterprise Configuration* below
- G Suite; non-Enterprise version - If you are using a version of G Suite that is not G Suite Enterprise, use the steps in the section *G Suite Configuration* below

G Suite Enterprise Configuration

1. Log in to your Google Admin console at <https://admin.google.com>.
2. From the **Home** page, go to **Apps > G Suite > Gmail > Advanced settings**.
3. Scroll to **Advanced settings** at the bottom of the page.
4. In the **Third-party email archiving** section, enter a unique name to identify the setting.
5. In the **Send journal messages to this email address** field, enter your journaling address from the Barracuda Cloud Archiving Service **Mail Sources > SMTP Journaling** page:



Add setting ×

Third-party email archiving Help

Barracuda Cloud Archiving

1. Send journal messages to this email address

bma_814fa843-466a-4fcf-82a8-78fa4be91cd9@mas.barracudanetworks.com

! Third-party email archiving setting applies to G Suite Enterprise users only

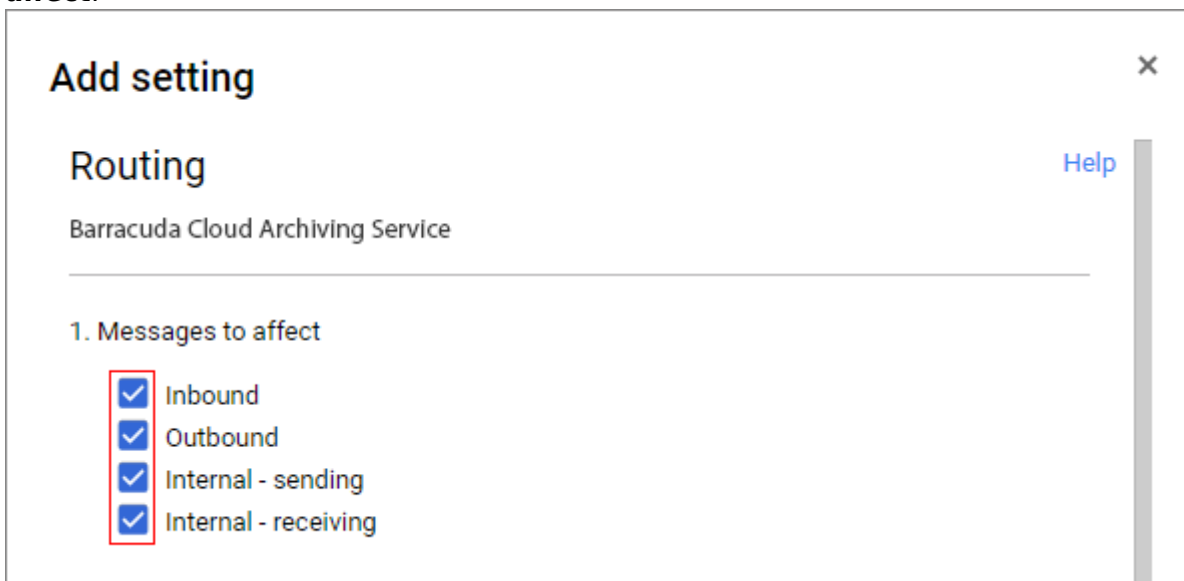
CANCEL ADD SETTING

6. Click **Add setting**, and click **Save**.

G Suite Configuration

Use the following steps to configure G Suite. If you are using G Suite Enterprise, use the steps in the previous section, *G Suite Enterprise Configuration*.

1. Log in to your Google Admin console at <https://admin.google.com>.
2. From the **Home** page, go to **Apps > G Suite > Gmail > Advanced settings**.
3. Scroll to **Routing**, and click **Configure**.
4. Enter a unique name to identify the setting, and select all check boxes under **Messages to affect**:



Add setting ×

Routing Help

Barracuda Cloud Archiving Service

1. Messages to affect

- Inbound
- Outbound
- Internal - sending
- Internal - receiving

5. In the **Also deliver to** section, click **Add more recipients**, and click **Add**.
6. Under **Recipients**, select **Advanced** from the drop-down menu.
7. In the **Envelope recipient** section, select **Change envelope recipient**.
8. In the **Replace recipient** field, enter the journaling address from the Barracuda Cloud Archiving Service **Mail Sources > SMTP Journaling** page.
9. Clear **Do not deliver spam to this recipient** and select **Suppress bounces from this recipient**:

Also deliver to
 Add more recipients

Recipients ADD

Advanced ▾

Apply the above modifications, plus the following:

Route
 Change route

Envelope recipient

Change envelope recipient

Replace recipient: bma_814fa843-466a-4fcd

Enter new username @ existing-domain

Existing-username @ Enter new domain

Spam and delivery options

Do not deliver spam to this recipient

Suppress bounces from this recipient

Headers

Add X-Gm-Original-To header

Add X-Gm-Spam and X-Gm-Phishy headers

Add custom headers

Subject

Prepend custom subject

Attachments

Remove attachments from message

CANCEL SAVE

10. Click **Save**. Select **Require secure transport (TLS)**:

Also deliver to
 Add more recipients

Recipients	ADD
Deliver to: bma_814fa843-466a-4fcf-82a8-78fa4be91cd9@mas.barracudanetworks.com Suppress bounces from this recipient	

Encryption (onward delivery only)
 Require secure transport (TLS)

11. Click **Add Setting**, and click **Save**.

Figures

1. BCASSetup.png
2. CreateDirectory.png
3. VerifyDomain.png
4. GSuite_Enterprise.png
5. bcas_messages_to_affect.png
6. AlsoDeliverTo.png
7. RequireTLS.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.