



Solution Brief

Exporting Archived Data

Archiving solutions often focus on the process of capturing data accurately and keeping it securely, but it's equally important that archived data can be exported out again when required. Organizations may need to meet compliance regulations or respond to e-discovery requests, both of which require archived data to be produced when requested. They should also ensure they are not "locked in" to their archive solution and are able to retrieve data easily if they need to move some or all of it to an alternate location.

Reasons for Exporting Archived Data

The business reasons which drive the need to export data from the **Barracuda Message Archiver** and the **Barracuda Cloud Archiving Service** fall into four broad categories:

1. Compliance

This is now a key requirement for most organizations, who must comply with strict business or industry regulations that specify the rules for retention, access to, and deletion of email. Many organizations choose Barracuda archiving solutions to help them meet these requirements.

Compliance regulations typically specify that organizations must be able to access and export selected data when needed by third parties and auditors. They also require detailed audit logs of system activities to be produced to enable the organization's compliance activities to be audited.

2. Discovery

An increasing number of organizations are needing to perform discovery and review exercises on historical email data on a regular basis. This may be in response to external litigation, a freedom of information request, or an internal workplace dispute.

Once the subset of data relevant to each specific exercise has been identified, it must be exported out for subsequent disclosure or for further detailed analysis.

3. System Administration

In order to limit the volume of data stored in their operational email archive, administrators may choose to extract older data from Barracuda (e.g., everything more than two years old) and transfer this to second tier or offline storage for long term retention.

If an organization decides to switch to an alternative archiving solution, for instance due to a merger or acquisition, then it will probably be necessary to extract some if not all data currently archived in Barracuda and make this available for transfer into the replacement system.

4. User Data Recovery

In the event that a user inadvertently deletes or loses some or all of their current email from their mailbox, this can be recovered by selecting and exporting the relevant data from the Barracuda archive back to the production mail server.

What Can Be Exported

Barracuda customers have unrestricted access at all times to their archived data (including notes, tasks and calendar entries as well as email), subject to any security restrictions their administrator has implemented. This means they can select and export any or all of their archived data items whenever needed.

Barracuda archiving solutions store archived data in an industry standard format. This avoids the “data lock in” situation found with products from most other vendors which store archived data in a range of proprietary data formats. Extracting data from these other solutions can prove to be a very costly exercise.

Email data can be exported either as a PST file or as a ZIP file containing individual EML format messages. For email messages archived using journaling from Microsoft Exchange it is possible to include the original journal envelope in the export, this contains additional header information such as BCC addressees and can be used to verify exported data as original and unmodified.

All data export operations are of course fully detailed in the audit log alongside other archive activities. The audit log itself can also be searched and exported as a CSV file to provide supporting information as needed.

Who Can Export Data

The ability for each user to export archived data is governed by Barracuda’s role-based security controls, which operate at both a global and an individual data item or user level to restrict access to authorized individuals only.

Each user will be assigned one of the following roles by an administrator using the **USERS** pages in the web interface.

1. Administrators

Two administrator roles are provided within Barracuda archiving solutions:

- **Admin** - Users assigned the Admin role have unrestricted access to search and export archived items from all users, and can also search and export all data from the system audit log. Therefore, this role should be used with extreme caution.
- **IT Admin** – This role is only available in the Barracuda Message Archiver, and is used to manage system and network configuration settings. Users with the IT Admin role do not have access to any archived data or the system audit log.

2. Auditors

The **Auditor** role can by default export items from any user; however, this access can be restricted in three ways:

- Global admin settings control whether end users assigned the Auditor role can export archived data.
- An individual list of domains can be specified for each user account assigned the Auditor role. Access for this auditor will then be restricted to data relating to users within those domains.
- A “Saved Search” previously created by an administrator can be specified for each user account assigned the Auditor role. This will then be automatically applied to all searches performed by this auditor, thereby limiting access to just the subset of data defined by the saved search.

If an organization is using an external resource to access or audit archived data, the Auditor role can be set up for them against a local account. This will provide complete access to all necessary data without adding them to the company directory structure or granting them administrator level privileges.

The Auditor role does not have access to the system audit log.

3. End Users

Global admin settings control whether end users assigned the **User** role are able to export archived data.

Each end user assigned the User role can only access items that are directly associated with their own account (as either a sender or a recipient), or with any accounts they are linked to as an alias.

The User role does not have access to the system audit log.

How to Export Data

There are three ways in which users can export data from Barracuda archiving solutions.

1. Scheduled Exports

If an organization needs to export recently archived data from the Barracuda Message Archiver on an ongoing basis, they can set up

Scheduled Exports. These are useful to support long running activities such as e-discovery investigations, which may require that all new email meeting specified criteria is identified and exported regularly for subsequent review or analysis.

The Scheduled Exports capability is available to administrators assigned the admin role and to users assigned the auditor role. Note that it's not currently included in the Barracuda Cloud Archiving Service.

Each Scheduled Export runs on a regular basis (either every week, or up to once every four weeks) as defined on the **POLICY > Scheduled Exports** page in the Barracuda administration web interface, and will export all new data that has been archived since the previous run. Both administrators and auditors are able to set up Scheduled Exports, and there is no limit to the number that can be set up at one time.

The data to be exported by each Scheduled Export is defined in a Saved Search, which will have been set up previously using the **BASIC > Search** page. The full power of Barracuda's granular search capabilities enables the scope of each scheduled export to be defined as broadly or as precisely as needed. It's based on a wide range of granular search criteria covering message header data, message contents, attachments, and metadata fields.

When each scheduled export run completes, the run will be listed on the **POLICY > Scheduled Exports** page, and the results from that run can be download from there as an individual PST file. It's also possible to set up an SMB share on the Message Archiver where the PST files created by each Scheduled Export run will be stored for a specified period of time.

2. On-Demand Exports

When it's required to export a set of archived data on an ad hoc basis (i.e., to respond to a freedom of information request) or to recover data that a user has inadvertently deleted from the email server, this can be actioned from the **BASIC > Search** page.

The data to be exported must first be identified by running an archive search. Barracuda's granular search capabilities enable the scope of data to be exported to be defined as broadly or as precisely as needed, based on a wide range of granular search criteria covering message header data, message contents, attachments and metadata fields. It's possible to save the criteria for each search so it can be ran again at a later data.

Once the search has completed and the data to be exported is listed, it can be exported using the **Tools > Export Messages** option on the **Search** page. Data can be exported as a PST file, or as a ZIP file containing individual EML files for each mail item.

Exports run as background tasks, with the progress of each export detailed on the **Tasks** tab of the **BASIC > Search page**. Once an export has been completed, a download link will allow the exported data to be downloaded.

The ability of each user role to export data is controlled by global settings on the **BASIC > Administration** page in the Barracuda web interface, under the **Search Page Settings** section:

- **Export Allowed** – Designates which user roles are able to use the export functionality described above. This setting also designates which user roles are able to download individual messages from the Message Preview pane on the Search page.
- **Export All Search Results Allowed** – Designates which user roles are able to export all messages returned by a search. If this setting is disabled, those user roles are only able to export specific messages that have been selected from the search results listed.

3. Audit Log Exports

The Audit Log is accessed from the **ADVANCED > Audit Log** page, and details all activities initiated by every user, including search-related activities. The data displayed on this page can be filtered by date, user, or type of activity in order to focus in on a specific set of activities.

Once the data to be exported has been identified and listed, it can be exported using the **Export** option on the **Audit Log** page. A CSV file containing the selected audit records will be sent to a specified email address.

Conclusion

The **Barracuda Message Archiver** and the **Barracuda Cloud Archiving Service** both store archived data in an industry standard format so it can be easily exported when required. Whether responding to a compliance or e-discovery request, or retiring older data to long-term storage, organizations will find that Barracuda's granular search capabilities make it easy to locate and export the subset of data they need. Scheduled Exports enable the process to be automated, while role-based security controls operate at an individual item level to ensure that data access is restricted to authorized individuals.