HYCU

HYCU R-Cloud for Microsoft 365 and Google Workspace

Quick Start Guide

Table of Contents

Copyright notice

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

> **Important**: Please read Software License and Support Terms before using the accompanying software product(s).

About HYCU R-Cloud Backup and Archiving for Microsoft 365 and Google Workspace

HYCU R-Cloud Backup and Archiving for Microsoft 365 and Google Workspace is an agentless archiving solution for companies that need to comply with regulatory requirements.

Emails are archived using Envelope Journaling thereby ensuring that all emails are properly archived. Available features include advanced eDiscovery (with an option to filter using 16 attributes), legal hold, customizable retention periods, audit trail, audit review capabilities, tags in addition to granular user access control, file/attachment manager, and advanced reporting via insights.

In the event of legal discovery, audits, and business or personnel investigations, business organizations need to be able to retrieve any relevant email message. Our archiving solution assures that evidentiary-quality records are systematically stored in a central repository with security in place to guard against any form of tampering.

Service pricing

Pricing is based on the number of mailboxes subscribed to and includes unlimited storage and retention.

Features include user access control, file/attachment manager, advanced search and reporting via insights. Insights and relationships give a summary of all emails in sent and received. You can restore, download, or migrate mailboxes or separate emails with just a click of a button. Search of emails can be done on 16 attributes.

For more details on pricing contact your HYCU representative.

Subscribing and signing to HYCU R-Cloud for Microsoft 365 and Google Workspace

To subscribe to HYCU R-Cloud for Microsoft 365 and Google Workspace contact the HYCU sales team and follow the instructions.

HYCU creates a login for the subscription owner, who is top level subscription administrator and sends you the email login information.

You can now sign in as an administrator and add your organization and users to be backed up.

Protecting Microsoft 365 or Google Workspace

Backing up

After the login to the subscription, proceed with the following steps to configure backup for Microsoft 365 or Google Workspace.

Preparing for backup of Microsoft 365

Depending on your needs you can configure Microsoft 365 backups in two ways.

- Backup that uses Global Admin user.
- Backup with Service Principal Authentication.
  This approach cannot backup Groups & Teams calendar and group email attachments.

Based on selected backup method follow the appropriate steps below.

Backup with Global Admin

1. Select **Add Backup** and **Sign in with Microsoft 365**. In Add Microsoft 365 Backup window select **Authorize with Global Admin**. Use Global Admin and accept the requested permission that Microsoft 365 prompts you for.

2. A new non-licensed global admin account is created for backup purposes. The username created starts with “backupadmin”. Copy and save the username and credentials to use them in next steps.
3. The next step is device authorization, where you configure Microsoft Exchange Online Remote PowerShell access with OAuth token:
    a) Copy the user code, open the link provided, and use the backup admin account created in previous steps to sign into Exchange Online Remote PowerShell.
    b) You need to provide additional security verification (using a mobile app) and enter the generated verification code. If the procedure takes too long, the user code might expire, and you need to repeat the previous step after regenerating the user code.
    c) Once logged in, an additional MFA verification of the backup admin is requested.
    d) When you see a message that you have signed into Microsoft Online Remote PowerShell application on your device, you can close the window.

    After these steps are performed, verification of authorization is done when you click **Verify & Continue**. If the verification fails, the steps must be repeated.
4. The final step is the re-authentication of the backup admin and granting the Email Backup the Oauth token access.

Backup with Service Principal Authentication

1. Select **Add Backup** and **Sign in with Microsoft 365**. In Add Microsoft 365 Backup window select **Authorize with Service Principal**. Use Global Admin and accept the requested permission that Microsoft 365 prompts you for.
2. A Backup Application will be created.
3. The next step will authorize the Exchange Online Management App using the device authorization flow to create custom role. It can happen that role creation takes a long time, up to 24 hours.
    a) Copy the user code, open the link provided, and use the Global Admin account to sign into Exchange Online Remote PowerShell.
    b) When you see a message that you have signed into Microsoft Online Remote PowerShell application on your device, you can close the window.

4. After these steps are performed, verification of authorization is done when you click **Verify & Continue**. If the verification fails, the steps must be repeated.

Selecting SharePoint sites

5. Users and SharePoint sites from the configured organization can now be selected for backup.
    - You can also enable automatic discovery and backup of all users or SharePoint sites by selecting the option AutoDiscover in Accounts or Sites tabs.
    - If you want to use automatic discovery for mailboxes in a specific Azure AD Group users only, please let us know the group name and we will configure your account to automatically backup all users in that specified AD Group.
    - You can enable AD Sync to synchronize the user details. Any changes on the M365 side (such as UPN or email address) will be reflected in the portal under the account list page.

Preparing for backup of Google Workspace

1. Select **Add Backup** and install the required application. To install the application use the Google Workspace administrator account.
2. Sign in with the Google Workspace administrator account that you used in step 1.
3. The journaling needs to be configured manually. This is done in the Google Admin console by going to Apps, then Google Workspace and then Gmail and opening the Routing.

    There create new routing for all message types, add new delivery (advanced, change envelope recipient, replace recipient) with provided email. Enable spam and delivery options to not deliver spam and suppress bounces and add a custom header `DME-JOURNAL-REPORT` with the value `true`.

    If not all users are under backup, create a user group for users under backup and set the routing to only affect specific envelope recipients (group).
4. Users from the configured organization can now be selected for backup.
    - You can also enable automatic discovery and backup of all users by selecting the option AutoDiscover.

Backup overview

- As soon as users are added, their emails are backed up. This also includes OneDrive, G Drive, Contacts, Calendar, and Tasks.
- Microsoft 365 Groups & Teams backups are started automatically for the whole organization.
- Google Workspace Shared Drive backup is started automatically.
- The storage is configured and provisioned automatically.
- Backup frequency is set and cannot be changed:

Item	Backup frequency
Emails	Via journaling
Contacts, Calendar, Tasks	1x/day
Teams Private Chat	1x/day
OneDrive, G Drive	1x/day
SharePoint, Groups & Teams	3x/day
Shared Drive	3x/day

- Retention is unlimited. You can reduce it to best fit your business requirements.
- An existing user cannot be removed from backup, backups can only be suspended (using the De-Activate option).

Configuring user access

User management allows the creation of departments and assignment of users to the departments. Users can be configured to have access to the backups and can be assigned departmental roles.

You can add external users, whose emails are not backed up – a useful feature for reviewers.

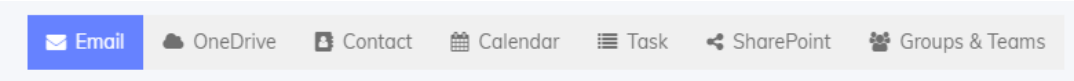
You can select several access levels - such as admins (Full Admin, Group Supervisor, IT Admins, Restricted IT Admins), users, reviewers, and so on.

For a complete list of access levels and details on user roles, see Access levels. For details on how to manage users, see Managing users.

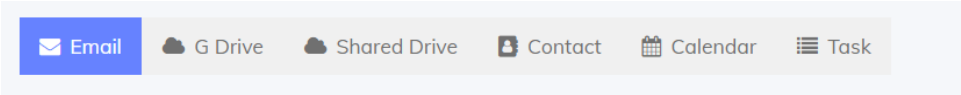
Restoring, downloading, and migrating

The dashboard shows tabs for different items protected.

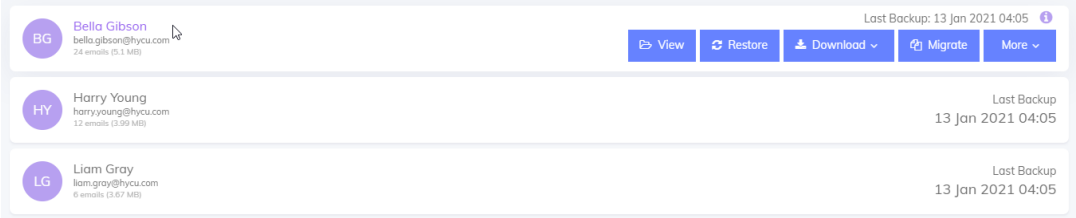
Tabs for Microsoft 365:



Tabs for Google Workspace:



Items backed up are displayed underneath the tabs. Available actions such as restore or download are displayed when you pause the cursor over the items:



Migrating, restoring, and downloading emails

Restoring an email backup or archive

1. Log in to your account and go to the dashboard.
2. Pause the pointer over the mailbox you want to restore and click **Restore**. The restore page opens.
3. Select the date range and the destination.

   To restore all emails in the account, select **All** in Select Date. To selectively restore emails, select the start and end date.

   You can select the following destinations:

- Restore to default folder (M365) / Restore to default labels (GWS)

  All messages selected are restored to the default folder for M365 and to default labels for Google Workspace.

  This option is available for all pages with the Restore button.

- Select existing folder to restore (M365) / Select existing label to restore (GWS)

  All messages selected are restored to an existing folder for M365 and to an existing label for Google Workspace.

  Available only for restore from the dashboard page, view list message mail account page, and preview message email account page.

  The Restore can go to the main folder or to a sub folder.

  Folders are listed in alphanumeric ascending order.

- Create new folder as restore destination (M365) / Create new label as restore destination (GWS)

  All messages selected are restored to the new folder created for M365 and the new label for Google Workspace.

  This option is available for all email pages with the Restore button.

  When specifying a new folder name, consider the following:

  - The maximum length for the name of the folder is 60 characters.
  - To create a sub-folder, use the ”/" separator.
  - Special characters (`!@#$%^&*()_+-=[]{};':\”`) are not allowed.
  - The used text encoding is UTF-8.
  - If a folder already exists, the restore process does not create a new folder but restores directly to the existing folder.
  - All whitespace before and after text is trimmed.

4. Click **Start Restore**.
5. You can check the status of your restore by clicking on **System Status** and then **Restores** in your dashboard.

Restoring a folder

The folder structure is replicated in the backups and you can restore emails to folders directly. If a folder is deleted, HYCU creates the folder and adds emails there.

1. Log in to your account and go to your dashboard.
2. Select the Email tab and the mailbox to restore.
3. Select the email folder instead of default **All** below the tab.
4. Select the message(s) or click **Select All** to select all messages.
5. Click **Restore**.

Migrating an archive or backed up mailbox to a new or another account

1. Log in to your account and go to your dashboard.
2. Pause the pointer over the mailbox you wish to migrate *from* and click **Migrate**.
3. Select the date range and the email destination. You can migrate emails to:
   - An existing email account.
     Select the account and the emails are restored to that mailbox.
   - A new email account.

     Select the type of email you want to migrate to:
     - M365 - Single Email Account
     - Other Email (includes Microsoft Exchange)

       If you email provider is not Google or Microsoft 365, select **Other Email**:

       a) Enter the email address and password of the new account to which you want to migrate the emails to.

       b) Enter the IMAP details for your destination mail server in the Advanced settings.
       If you do not know the required IMAP settings, contact your email service provider.
4. Click **Start Migrate**.
5. Your email is scheduled for migration. You can check the migration status from the dashboard by selecting **System Status** and then **Migrate**.

Migration notes

- You can migrate multiple email archives to a single email account.
- The original date and time of the emails are preserved in the target email account.
- Emails in sub-folders such as trash, sent, and similar:
  When migrating an account from IMAP to IMAP, the migrated emails are sorted out into sub-folders.

Downloading emails

1. Log in to your account and go to the dashboard.
2. Pause the pointer over the mailbox you wish to download.
3. Click **Download** and select **Email as PST** or **Email as EML** from the drop-down menu.
   Downloads are generated as ZIP files. If you select Email as EML, the zip file contains emails as EML files in folder(s). If you select Email as PST, the PST file is generated and compressed.
4. Select the folders you want to download and click **Generate Download**.
   The download link generation process starts, and an email is sent to you once the download is generated.
5. Once you receive this email, log in back to the dashboard, select **System Status** and then **Download**.
6. You can see the download link there. Click on the link to download the ZIP file.

Restoring and downloading Contacts, Calendars, and Tasks

1. Log in to your account and go to your dashboard.
2. Select the **Contacts**, **Calendars**, or **Tasks** tab.
3. Pause the pointer over the user you want to restore or download:
   - If you want to restore or download all the contact, calendar, or task data for the user:
     1. Click **Restore** or **Download**.
        For contacts download you can select **Download Latest Version** or **Download Latest and previous versions**.
     2. Click **Yes, Continue** to confirm.

- If you want to restore or download selected contacts, calendar items, or task data for a user:
  1. Click on the user.
  2. Select the data you want to restore.
  3. Click **Restore** or **Download**.
     For contacts download you can select **Download Latest Version** or **Download Latest and previous versions**.
  4. Click Yes, **Continue** to confirm.

4. You can check the status of your restores or downloads by clicking on **System Status** and then **Restores** or **Downloads** on your dashboard.

Restoring Contacts, Calendars, and Tasks to a different user

To restore to another user, download the data and then upload to the other user's accounts.

Restoring OneDrive or G Drive

HYCU R-Cloud for Microsoft 365 and Google Workspace supports the restore of the following OneDrive For Business or Google Workspace G Drive items:

- Restore of the entire User OneDrive, G Drive, Single Folder or Single File.
- Point in time restore - you can restore a file or folder or the entire drive from a specific backup date.
- Restore of data to the same user's drive or any other user's drive in the same tenant.

To restore OneDrive or G Drive items, perform the following steps:

1. Log in to your account and go to your dashboard.
2. Select the **OneDrive** (M365) or **G Drive** (Google Workspace) tab.
3. Hover the pointer over the user you want to restore.
4. Restore can be done of the whole drive or only selected files.

   To restore the entire user's drive data, click **Restore**.

   On the next page, select the:

   - Backup date – restores the files and folders as on that date

- Destination – you can choose to restore the same user's drive or another users drive in the same tenant.
- Restore method:
    - Keep Folder Structure – available for restore to the same account, restores everything to the same folder as in backup.
    - Create a new folder in the user's drive and restore the data there. The Folder Structure option allows you to keep the folder structure or remove it.

To restore selected files and folders, click on the user whose data you want to restore.

1. Select the backup and the data to restore.

   Click **Restore**.

2. Select **Restore Latest Version** to restore the latest version of the backup or **Latest & Previous Versions** to restore all backed up versions.
3. Select one of the following options:
    - Destination – you can choose to restore to the same user's or another user's OneDrive or G Drive in the same tenant.
    - Keep Folder Structure (Default) to restore and maintain the folder structure of the last backup.
    - Create New Folder to create a new folder in the root of user's drive and restore the data there.

5. Click **Start Restore**

   Click **Yes, Continue** to confirm the restore.

6. You can check the status of your restores or downloads by clicking on **System Status** and then **Restores** on your dashboard.

Downloading OneDrive or G Drive

1. Log in to your account and go to the dashboard.
2. Select the OneDrive or G Drive tab.
3. Pause the pointer over the user whose OneDrive or G Drive data you wish to download.
   Download can be done for the entire OneDrive or G Drive or only selected

files.
To download the entire user's drive data, click **Download**.

- On the download page, select the backup date – this downloads the files and folders as on that date.
- Click **Generate Download**.

To download selected files and folders, click on the user whose data you want to download.

- Select the backup and the data to download.
- Click **Download**. From the drop-down menu, select one of the options
    - Download Latest Version
    - Download Latest & Previous Version

1. Select the backup and the data to download.
2. Click **Download**.
3. From the drop-down menu, select one of the options:
    - Download Latest Version
    - Download Latest & Previous Version

5. Click **Yes, Continue** to confirm.
6. You can check the status of your restores or downloads by clicking on **System Status** and then **Downloads** on your dashboard.

Restoring Shared Drive

HYCU R-Cloud for Microsoft 365 and Google Workspace supports the restore of the following Google Workspace Shared Drive items:

- Restore of the entire Shared Drive.
- Point in time restore - you can restore a file or folder or the entire drive from a specific backup date.

To restore Shared Drive items, perform the following steps:

1. Log in to your account and go to your dashboard.
2. Select the **Shared Drive** tab.
3. Hover the pointer over the Shared Drive name you want to restore.
4. Restore can be done of the whole drive or only selected files.

To restore the drive data, click **Restore**.

To restore selected files and folders, you can

- Select **Restore** on the top level folder to restore last version of that folder
- Select top level folder to browse for specific files or folders on the drive.

  After selecting the files and folders, click **Restore** and select **Selected (latest version only)** to restore the latest version of the backup or **Selected and previous versions** to restore all backed up versions.

  Select one of the following options:

  - Select Destination – you can choose to restore to the original Shared Drive or to other Shared Drive.
  - Keep Folder Structure (Default) to restore and maintain the folder structure of the last backup.
  - Restore to New Folder to create a new folder in the root level of the destination and restore the data there.

5. Click **Start Restore**

   Click **Yes, Continue** to confirm the restore.

6. You can check the status of your restores or downloads by clicking on **System Status** and then **Restores** on your dashboard.

Downloading Shared Drive

1. Log in and go to the dashboard.
2. Go to the **Shared Drive** tab.
3. You can download the whole drive or only selected folders or files.

   To download the whole drive data, you can

   1. Pause the pointer over the Shared Drive name you want to download.
   2. Click **Download**.
   3. Select the data & time of the data you want to download.
   4. Select the data.
   5. Click **Generate Download**.

To download selected top level folders, you can

1. Hover the pointer over the Shared Drive top folder name you want to download.
2. Click **Download**.
3. Select the data & time of the data you want to download.
4. Click **Generate Download**.

To download selected folders or files, you can

1. Click the Shared Drive top folder name.
2. Select folders and files.
3. Click **Download**.
4. From the drop-down menu, select one of the options:
    - Selected (latest version only)
    - Selected and previous versions

4. Click **Yes, Continue** to confirm.
5. You can check the status of your restores or downloads by clicking on **System Status** and then **Downloads** on your dashboard.

Restoring SharePoint

For SharePoint Online you can:

- Restore a SharePoint Site, subsite, or single file folder in SharePoint.
- Perform a point in time restore: You can restore data from any previous backup.
- Restore data to the same site or any other site in the same tenant.

To restore SharePoint items, perform the following steps:

1. Log in and go to the dashboard.
2. Go to the **SharePoint** tab.
3. Pause the pointer over the site you want to restore.
    - To restore the entire site, click **Restore**.

      On the next page, select the:
        - Backup date – restore the site as on that date

    - Backup time – as a backup is preformed three times a day for SharePoint, select one of the backups from that day.

- To restore subsites, expand the main site and click Restore for the sub site.

  On the next page select:

    - Backup date – restore the site as on that date
    - Backup time – as backup is preformed three times a day for SharePoint, select one of the backups from that day.
    - Destination – you can choose to restore to the same main site or any other site in the same tenant.
    - Restore method:
        - **Keep folder structure** – restore everything by following the path and folder structure from the latest backup.
        - **Restore to new folder**: Create new folder in the root of the selected site and restore the data there.

- To restore selected folders and files in a sub-site click on the sub-subsite and open it.

  Select the files and folders and click **Restore**. Choose to restore the selected version or selected and previous versions.

  Select the restore options:

    - **Destination** – you can choose to restore to the same main site or any other site in the same.
    - **Restore method**
        - Keep Folder Structure (Default) – restore everything by maintaining the path and folder structure based on the latest backup.
        - Restore to new folder: Create a new folder on the root level of destination and restore the data there.

4. Click **Start Restore**.
5. Click **Yes, Continue** to confirm.
6. You can check the status of your restores or downloads by selecting **System Status** and then **Restores** on your dashboard.

Downloading SharePoint

1. Log in and go to the dashboard.
2. Select the **SharePoint** tab.
3. Hover the pointer over the site you want to download.
4. Select the items to download.
   - To download the entire site, click **Download**.

     In the Download screen, select the:
     - Date – download the site as on that date.
     - Time – Since we perform three backups per day for SharePoint, select the version that you want to download on the backup date.
     - Subsites to be downloaded.
   - To download only one subsite, expand the main site and click **Download** for the sub-site.

     In the download screen, select the:
     - Backup date – download the site as on that date
     - Backup time – as backup is preformed three times a day for SharePoint, select one of the backups from that day.
     - To download selected folders and files in a sub-site click on the sub-subsite and open it.
5. Select the files and folders and click **Download**. Select the versions to be restored.
6. Click **Generate Download**.

   Click **Yes, Continue** to confirm.
7. You can check the status of your downloads by clicking on **System Status** and then **Downloads** on your dashboard.

Restoring Groups and Teams

1. Log in and go to your dashboard.
2. Select the **Groups and Teams** tab.
3. Pause the pointer over the group that you want to restore and select one of the following items:

- To restore the whole group, select a group and click **Restore**.
    - Select a subproduct and click **Next**.
    - If you selected Chat for restore, the Chat settings are displayed. To modify them, click **Edit Settings**.

      Click **Next**.
    - Select the restore destination:
        - **Original group**

          Restore to the original group.
        - **New group**

          Create a new group and restore to it.
        - **Add to chat group**

          This option is available if you selected Chat for restore. Restore to the new group that is created when restoring Chat.
    - Click Start **Restore**.
- To restore only subproduct items, select the subproduct that you want to restore, and then the items you want to restore. Click **Restore**.
    - File, Site, and Note items only. From the drop-down list, choose to restore the selected (the latest version only) or the selected and previous versions of the item.
    - Site, Note, Calendar, and Task subproducts only. Select the restore destination:
        - **Original group**

          Restore to the original group.
        - **New group**

          Create a new group and restore to it.
    - Click Start Restore.

Downloading Groups and Teams

1. Log in and go to your dashboard.
2. Select the **Groups and Teams** tab. Expand the site and reveal all the groups.

3. Expand the Groups to access the different Teams items.
4. Click **Download**.
5. Select the items to download. The following items have additional options:
   - Team chats can be downloaded as EML, CSV, or PDF files.
   - Mailboxes can be downloaded as EML or PST files.

   Select the appropriate format from the Download drop-down list.
6. Click **Next**.
7. In the download screen, select the:
   - Backup date – download the data as on that date
   - Backup time – as backup is preformed three times a day for Teams, select one of the backups from that day.
8. Click **Generate Download** and then click **Yes, Continue** to confirm.

Performing common tasks

Managing users

Access levels

HYCU R-Cloud Backup and Archiving for Microsoft 365 provides the following access levels:

- **Full Admin**: Has complete access and all capabilities. They can view, download, restore, migrate, and search emails from all email accounts. They can also set user permissions, compliance policies, and view logs, set legal holds, and set up review processes.
- **IT Admin**: They have access to view info, restore, delete, and deactivate email for all accounts. They also can set up all user settings, but can't access compliance tab. They cannot view the content of any email but can see the metadata (header, subject, from, to fields) of an email.
- **Restricted IT Admin**: They have access to view info, restore, delete, and deactivate email for all accounts. They also can set up all user settings. They cannot view the content or metadata (header, subject, from, to fields) of email. They can access compliance tab, see audit logs and edit retention policies.

- **Group Supervisor**: They have complete access for the departments for which they are supervisors. They can view, download, restore, migrate, search emails from all email account within their allotted department. They can set user permissions, but can't access all compliance policies.
- **User**: They can only view, download, restore, migrate, and search their own emails. They have no access to other email accounts and cannot access the compliance tab.
- **User View and Restore**: They can only view, restore and search their emails but cannot download or migrate them. They have no access to other email accounts and cannot access the compliance tab.
- **Compliance and Review Officer**: They only have access to eDiscovery Search, Alerts, View Audit Logs, Retention policy, Legal Hold and Review Process tabs. They also have access to view email for all accounts.
- **Reviewer**: They only have access to Review Process tab where they can review emails. They are able to review all review processes. They are not able to set up a review process. The account owner, full admin, or compliance officer have to set these up for the reviewers.
- **Limited Reviewer**: They have access to the Review Process menu, but they can only review emails within the selected list in the Review Process.
- **Data Protection Officer**: This user has access to the Review Process Tab in Compliance and can delete messages marked for deletion. They also can create their tags to classify messages. They can add notes to messages marked for deletion for the audit log. They also have access to view email for all accounts.

Managing user access

1. Log in to your account.
2. Select **User Management**.
3. Select **Grant Permission**.
4. Select the user and assign the role from the drop-down menu.
5. For Group supervisors, select the department for which they are supervisors.
6. Click **Save Changes**.

Enabling and disabling the user login

1. To enable or disable login of an user whose email is backed up;
2. Log in to your dashboard.
3. Go to **User management**.
4. Select the **Grant Permission**.
5. In the Grant Permission page, enable or disable the login of the user by clicking on the Login Status switch.

Enabling two-factor authentication

Each user can enable two-factor authentication on top of login method used. The two-factor authentication uses time-based OTP, supported by for example Google or Microsoft Authenticator.

1. Log in to your dashboard.
2. Go to **Two-factor Authentication**.
3. Prepare mobile authenticator application. Search links for iOS and Android are provided.
4. Display the QR code by selecting **Setup Two-factor Authentication** and scanning it with authenticator application.
5. Scan the code with the app and select **Next**.
6. Next dialog will ask you to enter the code generated to verify proper setup. Enter the code and select **Verify & Finish**.
7. The two-factor authentication is now enabled and code will be requested on each login.

To disable two-factor authentication, deselect the Two-Factor Authentication option.

Enable Azure Active Directory Single Sign On access to dashboard for users

You can enable Microsoft 365 Azure Active Directory Single Sign On, enabling users to log in to their backup dashboard using their Microsoft 365 credentials. This way they do not have to keep a separate password for the backup portal.

1. Log in to your dashboard.
2. Go to **User management**.
3. Select **Grant Permission**.
4. Enable the **Enforce Azure AD SSO Log In** access for all users. Once enabled for all users, users need to use their Microsoft 365 credentials to log in to their backup dashboard.

You can enable and disable the user login on the same page.

Enable Google Single Sign On access to dashboard for users

You can enable Google Single Sign On, enabling users to log in to their backup dashboard using their Google credentials. This way they do not have to keep a separate password for the backup portal.

1. Log in to your dashboard.
2. Go to **User management**.
3. Select **Grant Permission**.
4. Enable the **Enforce Google SSO Log In** access for all users. Once enabled for all users, users need to use their Google credentials to log in to their backup dashboard.

You can enable and disable the user login on the same page.

Enabling access for external users (Delegated Users)

You can add users who can access your backups without the need to back them up. For example, you can grant access to your backup to an external auditor. Consider the following:

- Only admins who have access to the user management page can enable access to external users tab.
- They create a user on the backup portal and HYCU invites them to log in to the portal.

To enable access for external users:

1. Log in to the dashboard.
2. Click **User management** to open the user management page.
3. Open **Grant Permission**.
4. Click **Add user**.
5. Enter the email of the user you want to invite.
6. Select the role of the user.
7. Check the box **I agree with this Term** and click **Invite**.

   Note that once you click Invite, an email with the link to login and reset the password is sent to the user. *This link expires in 24 hours.*
8. You can check whether the user has accepted it on the **Invitation List** tab:

   If the user did not get the email or if the invitation expired, then you can resend the invitation. Right-click the status and select **Resend** from the drop-down menu. To cancel the invitation, select **Cancel**.

   > **Important** You are granting an external user access to the portal. Depending on the selected role, the user might be able to see your data. Additionally, only the account owner, full admin, and the IT admin can enable and disable this access. Creating this access does not mean HYCU is backing up the user's data. The user has only access to the backups. You can also add the same user in another subscription.
9. Once the user accepts the invitation and logs in, he /she is added to the user list on the grant permissions tab.

   You can send the password reset link again if necessary.

   The user type is marked with colored band on the left of the user card: orange for delegated users and blue for backup users.

> **Note**
>
> - You cannot transfer ownership to a delegated user.
> - Every user's activity regarding delegated users is recorded in the audit log.
> - A revoked permission to review process for a "Limited Reviewer" is handled by displaying an error notification.
> - You cannot delete a delegated user. You can only revoke his access.

Assigning users to departments

1. Log in and go to the dashboard.
2. Click on **User Management** to display a list of users.
3. If you do not have any departments yet or the department is missing, click on **Department Management** to add it.

   Enter the name and click Add More.

   Click Save Changes and go back to the User Management page.
4. On the Grant Permission page, assign one or multiple departments to the user.

The departments can also be assigned to the users based on the department information present in Active Directory. If Azure Active Directory (AD) Department Sync is selected, the departments assigned to users in Active Directory are created if needed and assigned to users.

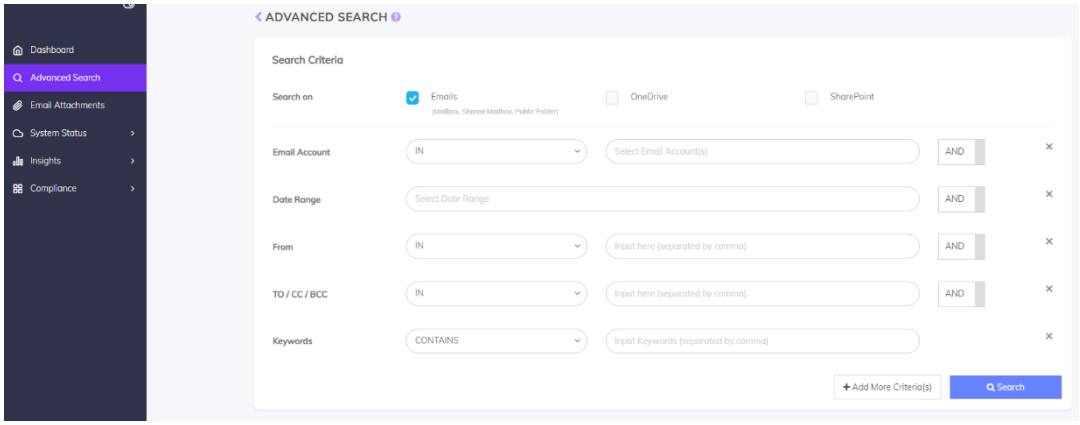
Managing licenses

- Licenses are counted per seat.
- The user *can only be deactivated*:
    - Due to compliancy, data is retained; emails can be removed if retention is shortened, but OneDrive, G Drive, Contacts, Calendars, and Tasks are retained.
    - On top of licensed seats an additional 20% of seats can be deactivated without additional licensing – if you exceed this number you need additional seat licenses.

Advanced search

You can use advanced search to locate emails, OneDrive files, or SharePoint items of interest.

1. To open the Advanced Search page, select Advanced Search in the side menu.



2. Select the search area (emails, OneDrive, G Drive, SharePoint).

   If the default search properties do not cover your search (for example, you want to search the email body and similar), you can add additional search properties as well as remove them.

   Click **+Add More Criteria(s)** and select the additional search criteria.

   Separate multiple keywords by comma. Combine search criteria from top to bottom:

   ```
   ((criteria1 operator1 criteria2) operator2 criteria3)
   ```

   Example:

   ```
   (to “finance” OR to “approvers) AND subject contains “contract, agreement”
   ```

   Emails with To containing “finance” or “approvers” and subject containing either “contract” or “agreement”.

   Some search examples

   - Search Internal Emails - emails that are sent within company only

     ```
     To / CC / BCC Only IN @domain.com AND

     From Only IN @domain.com
     ```

   - Search External Emails - to emails that are distributed outside the company

     ```
     To / CC / BCC Not IN @domain.com OR

     From Not IN @domain.com
     ```

- Inbound Emails - emails that are received by the company

```
Folder Not IN Sent Items
```

- Outbound emails - emails that are sent by the company employees

```
Folder IN Sent Items
```

3. Click Search to start the search.

Insights

The **Insights** section shows insights based on backed up emails. You can view:

- email volume and storage, most frequently contacted account, and attachment types
- how often during work emails are sent, how fast they are responded to, and the most active email users

> **Note** On request, insights can be disabled.

Statistics displays email volume and used storage. Top contacts and attachment types are also listed.

Productivity displays productivity information as seen from emails, from sending emails, response times, to top email users.

Compliance

The Compliance section offers the following compliancy related tools:

- Auditing
- Selectable retention settings
- Legal hold
- Discovery, alerts, tags based on search
- Review process

eDiscovery

eDiscovery is based on email advanced search. For details on advanced search, see Advanced search.

eDiscovery expands the advanced search with alerts, tags, and a review process on the results. You can do the following::

- Apply tags to search results, including saved ones
- Mark the results for review
- Run the search daily and the results are sent by email as alerts

Creating an eDiscovery

1. Log in to your dashboard.
2. Select **Compliance** and then **eDiscovery**.
3. If the default search properties do not cover your search (for example, you want to search the email body and similar), you can add additional search properties as well as remove them.

   Click **+Add More Criteria(s)** and select the additional search criteria.

   For an example, see Advanced search.
4. After setting the criteria, enter a name for the search. Consider the following limitations:
   - A maximum 35 characters are allowed.
   - The name can contain only letters (a-z or A-Z) and/or numbers (0-9). No other special characters are allowed, except the currency symbols and the underscore ("_").
5. Click **Save**. Any criteria and the search are saved and accessible under the Saved Search tab.

Viewing, tagging, and marking the search results for review

1. Once you saved an eDiscovery Search, select the **Saved Search** tab.
2. A list of saved searches is displayed. The most recent search that you created in an eDiscovery search is at the top of the list.

3. Select the search and select an action for it:
   - **View**
     Select the item for viewing:
     - **View Emails**

       The View Emails page opens and allows you to preview emails one by one.

       You can also download, restore, or migrate emails and add or remove tags to search results.
     - **View & Edit Criteria**

       The View & Edit Criteria page opens, which allows you to view or edit the search criteria.

       After editing the criteria, click **Update**.
   - **Tag**

     Select **Add tag** from the drop-down list to apply the tag to all search results.
   - **Mark for review**

     All the search results emails will be marked for review. See Creating a Review Process for details.

Retention policy

Consider the following when defining your retention policy:

- By default, backups are kept forever.
- The retention policy can be set to one of the predefined periods.
- The Retention time is calculated from the email date, not the backup date.
- Retention policy can be defined for email account(s), department(s) or all email accounts. For SharePoint the retention policy can be defined for site(s) or whole SharePoint.
- Retention period can be selected for the policy.
- Retention can be defined on the Message level.
- On the Message level the saved eDiscovery Search can be selected and the desired retention period set for matching messages.

- If email or site is part of more than one retention policy, the longest retention will be used.

Creating a retention policy

1. Select **Compliance** and then **Retention Policy**.
2. Select **Create New** on
   - Account Level tab for emails retention policies.
   - Site Level tab for SharePoint retention policies.
3. Enter the policy name. Consider the following limitations for the policy names:
   - A maximum 35 characters are allowed.
   - The name can contain only letters (a-z or A-Z) and/or numbers (0-9). No other special characters are allowed, except the currency symbols and the underscore ("_").

   For email retention select the scope of the policy:

   - **Email Account**

     Enter one or more email accounts.

   - **Department**

     Enter one or more department names.

   - **All**

     Policy will apply to all email accounts.

   For SharePoint retention select the scope of the policy:

   - **SharePoint Site**

     Select one or more SharePoint sites.

   - **All**

     Policy will apply to all SharePoint sites.

   Select the retention period for the retention policy. The retention period options are from 30 days to 11 years plus Unlimited. Unlimited prevents automatic deletion of emails.
4. Click Save. The saved policy is listed in the Retention Policy List.

Legal hold

The legal hold functionality allows emails to be marked for legal hold, preventing their deletion until legal hold is removed.

> Note Emails are retained indefinitely once placed on legal hold, superseding any previously set retention policies**. Emails under legal hold cannot be deleted by any retention policy until the legal hold is removed.**

You can define legal hold for:

- email accounts
- departments (applied to all accounts of the department)
- all email accounts

The legal hold can be defined at the Message level and saved eDiscovery Search can be selected to apply legal hold to results.

Creating a legal hold

To create a legal hold:

1. Select **Compliance** and then **Legal Hold**.
2. Select **Create New** to open the Create New page.
3. Enter a name for the legal hold. Consider the following limitations:
   - A maximum 35 characters are allowed.
   - The name can contain only letters (a-z or A-Z) and/or numbers (0-9). No other special characters are allowed, except the currency symbols and the underscore (“_”).
4. Select the scope of the legal hold:
   - **Email Account**

     Enter one or more email accounts.
   - **Department**

     Enter one or more department names.
   - **All**

     All email accounts are selected.

5. Click **Enable Hold**. The legal hold is saved and you can view it under the Legal Hold List.

Access to legal hold

The following admins and users have access to legal hold:

- All Admins (Full Admin, Group Supervisor, and IT Admin)
- Compliance Reviewer(s).

Audit log

Audit log can be used to audit operations:

- Email view, restore, download, or review actions
- User configuration, compliancy options
- System notifications
- List options can be used to perform a more granular search of logs

Creating an audit log

1. Select **Compliance** and then **Audit Log**.
2. Select the activity:
   - **Messages & File Audit Log**

     Select a date dange, a specific user for whom you want to see logs, or enter the Archive Message ID of the email if you want to just see the logs for a message.
   - **User Activity Log**

     Select a date range, a specific user for whose logs you want to see, or enter the Object Name (email account) if you want to just see the logs for that object.
   - **System Activity Log**

     Select a Date Range or a specific user for whose logs you want to see.
3. Click **Search**.
4. The audit log is displayed below.

Downloading an audit log

1. Click on **Download** to download the logs
2. You can download the audit log file in the CSV or PDF format.
3. The selected file is generated and added into your Download List.
4. Once the file is ready, a download link is provided. The link expires within 24 (twenty-four) hours.

Access to audit logs

The following admins and users have access to audit logs:

- Full Admin and Group Supervisor
- Restricted IT Admin
- All Reviewers.

Review process

A review process uses saved eDiscovery Search to mark emails for review or review and deletion.

A reviewer can see the emails for review and perform the following actions:

- Remove the review status
- Add retention policy
- Add legal hold

Creating a Review Process

Prerequisite

Before you create the review process, you must create an eDiscovery search and save it.

> Tip Use filters to reduce the number of emails in the saved search. A huge number of emails (for example above 100000) significantly slows down the creation process.

Procedure

1. Select **Compliance**, then **eDiscovery** and then **Saved Search**.
2. Select the saved search and select Mark for Review. Select the review option:

- **Mark for review**

  The emails are marked for review.

- **Mark for Review & Deletion (DPO)**

  The emails are marked for deletion by the Data Protection Officer (DPO).

  The DPO can later on review and delete emails, but must provide the deletion reason that is added to the audit logs for compliance reasons.

  Once emails are deleted, they cannot be recovered.

  > Note Emails on legal hold cannot be deleted by the DPO.

3. Select **Create**.
4. Once you create the review process, you are directed to the Review process page. The most recent Review Process is added to the top of the list, with a same name as that of the eDiscovery Saved Search. Note that review process preparation may take some time.

Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

info@hycu.com

We will be glad to hear from you!

www.hycu.com

HYCU®