

Office 365 and Azure AD roles with access to Cloud App Security

By default, the following Office 365 and [Azure Active Directory \(Azure AD\)](#) admin roles have access to Cloud App Security:

- **Global administrator and Security administrator:** Admins with **Full access** have full permissions in Cloud App Security. They can add admins, add policies and settings, upload logs and perform governance actions.
- **Compliance administrator:** Has read-only permissions and can manage alerts. Can create and modify file policies, allow file governance actions, and view all the built-in reports under Data Management.
- **Compliance data administrator:** Has read-only permissions, can create and modify file policies, allow file governance actions, and view all discovery reports.
- **Security operator:** Has read-only permissions and can manage alerts.
- **Security reader:** Has read-only permissions and can manage alerts. The Security reader is restricted from doing the following actions:
 - Create policies or edit and change existing ones
 - Performing any governance actions
 - Uploading discovery logs
 - Banning or approving third-party apps
 - Accessing and viewing the IP address range settings page
 - Accessing and viewing any settings pages
 - Accessing and viewing the Discovery settings
 - Accessing and viewing the App connectors page
 - Accessing and viewing the Governance log
 - Accessing and viewing the Manage snapshot reports page
 - Accessing and editing the SIEM agent
- **Global reader:** Has full read-only access to all aspects of Microsoft Cloud App Security. Cannot change any settings or take any actions.

Additionally, the following Cloud App Security specific admin roles can be configured in the Cloud App Security portal:

- **App/instance admin:** Has full or read-only permissions to all of the data in Microsoft Cloud App Security that deals exclusively with the specific app or instance of an app selected. For example, you give a user admin permission to your Box European instance. The admin will see only data that relates to the Box European instance, whether it's files, activities, policies, or alerts:
 - Activities page - Only activities about the specific app
 - Alerts - Only alerts relating to the specific app
 - Policies - Can view all policies and if assigned full permissions can edit or create only policies that deal exclusively with the app/instance
 - Accounts page - Only accounts for the specific app/instance
 - App permissions - Only permissions for the specific app/instance

- Files page - Only files from the specific app/instance
- Conditional Access App Control - No permissions
- Cloud Discovery activity - No permissions
- Security extensions - Permissions only for API token with user permissions
- Governance actions - Only for the specific app/instance
- **User group admin:** Has full or read-only permissions to all of the data in Microsoft Cloud App Security that deals exclusively with the specific group selected here. For example, if you give a user admin permission to the group "Germany - all users", the admin can view and modify information in Microsoft Cloud App Security only for that user group:
 - Activities page - Only activities about the users in the group
 - Alerts - Only alerts relating to the users in the group
 - Policies - Can view all policies and if assigned full permissions can edit or create only policies that deal exclusively with users in the group
 - Accounts page - Only accounts for the specific users in the group
 - App permissions – No permissions
 - Files page – No permissions
 - Conditional Access App Control - No permissions
 - Cloud Discovery activity - No permissions
 - Security extensions - Permissions only for API token with users in the group
 - Governance actions - Only for the specific users in the group
- **Cloud Discovery global admin:** Has permission to view and edit all Cloud Discovery settings and data. The Global Discovery admin has access as follows:
 - Settings
 - System settings - View only
 - Cloud Discovery settings - View and edit all (anonymization permissions depend on whether it was allowed during role assignment)
 - Cloud Discovery activity - full permissions
 - Alerts - only alerts related to Cloud Discovery data
 - Policies - Can view all policies and can edit or create only Cloud Discovery policies
 - Activities page - No permissions
 - Accounts page - No permissions
 - App permissions – No permissions
 - Files page – No permissions
 - Conditional Access App Control - No permissions
 - Security extensions - No permissions
 - Governance actions - Only Cloud Discovery related actions
- **Cloud Discovery report admin:** Has permissions to view all the data in Microsoft Cloud App Security that deals exclusively with the specific Cloud Discovery reports selected. For example, you can give someone admin permission to the continuous report from Microsoft Defender ATP. The Discovery admin will see only the Cloud Discovery data that relates to that data source and to the app catalog. This admin will not have access to the **Activities** or **Files** pages and limited access to policies.

Override admin permissions

If you want to override an administrator's permission from Azure Active Directory or Office 365, you can do so by manually adding the user to Cloud App Security and assigning the user permissions. For example, if you want to assign Stephanie, who is a Security reader in Azure Active Directory to have **Full access** in Cloud App Security, you can add her manually to Cloud App Security and assign her **Full access** to override her role and allow her the necessary permissions in Cloud App Security.


Add additional admins

You can add additional admins to Cloud App Security without adding users to Azure Active Directory administrative roles. To add additional admins, perform the following steps:

Important

Only Global administrators or Security administrators can grant access to other users to Cloud App Security.



1. Click the settings cog  and then **Manage admin access**.
2. Click the plus to add the admins who should have access to Cloud App Security. You can type an internal or external email address to enable administrators from inside your organization or external Managed Security Service Providers (MSSPs) to administer your security alerts.

Add admin access

Type the admin username you want to provide access to:

Type admin UPN/email...

Select the type of role for this admin:

App/instance admin

Select apps for this admin:

Box

Select instances (default is all instances for selected apps):

Select instances...

Q |

- Box for Microsoft
- Test2
- test3

Add admin Cancel

- Next, click the drop-down to set what type of role the admin has, **Global admin**, **Security reader**, **Compliance admin**, or **App/Instance admin**. If you select **App/Instance admin**, select the app and instance for the admin to have permissions for.

Note

Any admin, whose access is limited, that attempts to access a restricted page or perform a restricted action will receive an error that they don't have permission to access the page or perform the action.

- Click **Add admin**.

Admin activity auditing

Cloud App Security lets you export a log of all admin activities including auditing of an admin investigating a specific user or viewing specific alerts.

To export a log, perform the following steps:

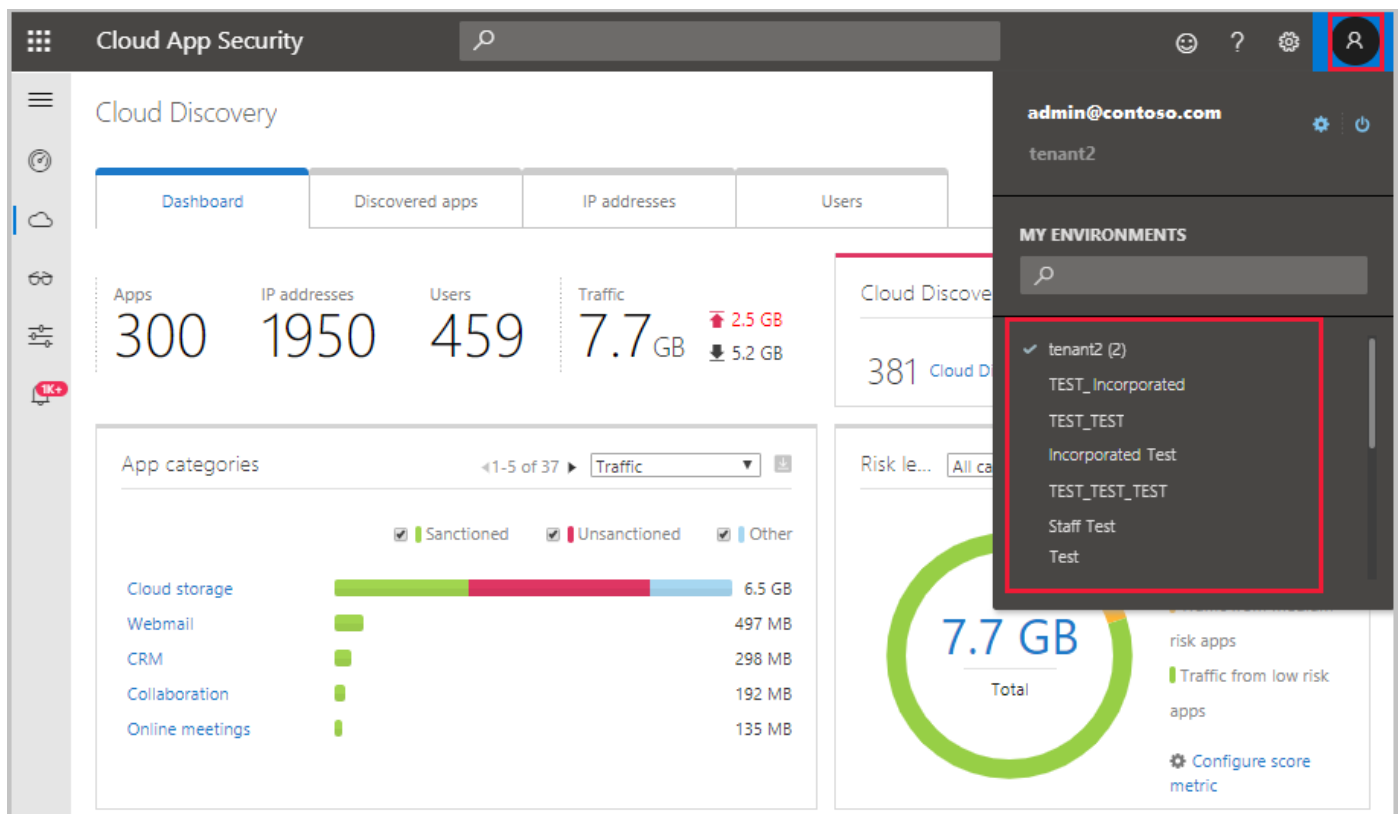
- In the **Manage admins access** page, select **Export admin activities**.

2. Specify the required time range.
3. Click **Export**.

Invite external admins

Cloud App Security enables you to invite external Managed Security Service Providers (MSSPs) as administrators of your Cloud App Security portal. External users can now be configured as administrators and assigned any of the roles available in Cloud App Security. Additionally, to enable MSSPs to provide services across multiple customer tenants, Administrators who have access rights to more than one tenant can now easily switch tenants within the portal.

To switch between tenants, after you have permissions to multiple tenants, click the user icon. You will see a list of the tenants for which you have permissions. Select the tenant you want to manage.



The screenshot displays the Cloud App Security dashboard. The main content area shows 'Cloud Discovery' with a 'Dashboard' tab selected. Key metrics include 300 Apps, 1950 IP addresses, 459 Users, and 7.7 GB of traffic (with a 2.5 GB increase and 5.2 GB decrease). Below this, 'App categories' are listed with a bar chart: Cloud storage (6.5 GB), Webmail (497 MB), CRM (298 MB), Collaboration (192 MB), and Online meetings (135 MB). A 'MY ENVIRONMENTS' sidebar is open, showing a dropdown menu for tenant selection. The dropdown is currently set to 'tenant2 (2)' and lists several test tenants: TEST_Incorporated, TEST_TEST, Incorporated Test, TEST_TEST_TEST, Staff Test, and Test. The user's profile information at the top right shows 'admin@contoso.com' and 'tenant2'.

Category	Value
Apps	300
IP addresses	1950
Users	459
Traffic	7.7 GB

Category	Value
Cloud storage	6.5 GB
Webmail	497 MB
CRM	298 MB
Collaboration	192 MB
Online meetings	135 MB