TOP 10 SECURITY EVENTS TO MONITOR IN AZURE AD AND OFFICE 365

Discover how native auditing tools can help — and how to overcome their shortcomings.

Quest®

Introduction

Is your organization really more secure now that you're running applications in the cloud?

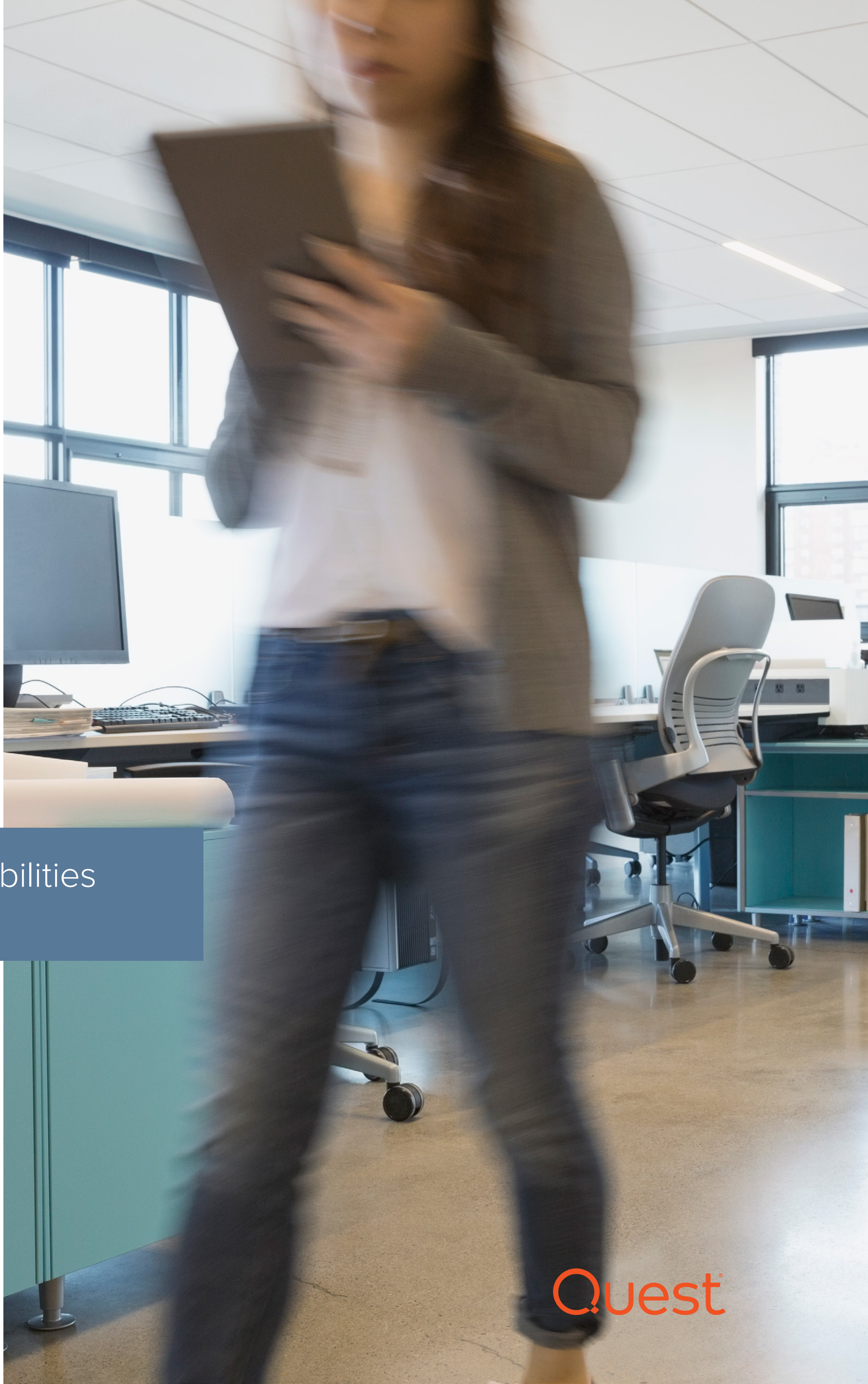
More efficient, probably. But more secure?

Users can still perform high-risk actions in the cloud, and their account credentials can still be compromised and misused by others. According to Verizon's 2020 Data Breach Investigations Report, nearly a third (30 percent) of data breaches involve someone already inside the network. And Microsoft reports that 95 million AD accounts are the target of cyberattack each day and 1.2 million Azure AD accounts are compromised each month.

To avoid becoming the next breach headline, you need to keep a close eye on all changes to your roles, groups, applications, sharing and mailboxes. Unfortunately, native Office 365 and Azure AD tools leave a lot to be desired when it comes to auditing these critical modifications; among other things, their search capabilities are limited and the logs retain audit events for only a short time.

Office 365 and Azure AD offer limited search capabilities and retain audit events for only a limited time.

This ebook highlights ten security events that administrators track closely to keep their Azure AD and Office 365 environment secure. It explores the audit information they can find using native tools and consoles, and identifies the pitfalls they are most likely to encounter when pulling audit reports natively. Finally, it offers a look at a solution that can help them overcome some of these native auditing limitations.



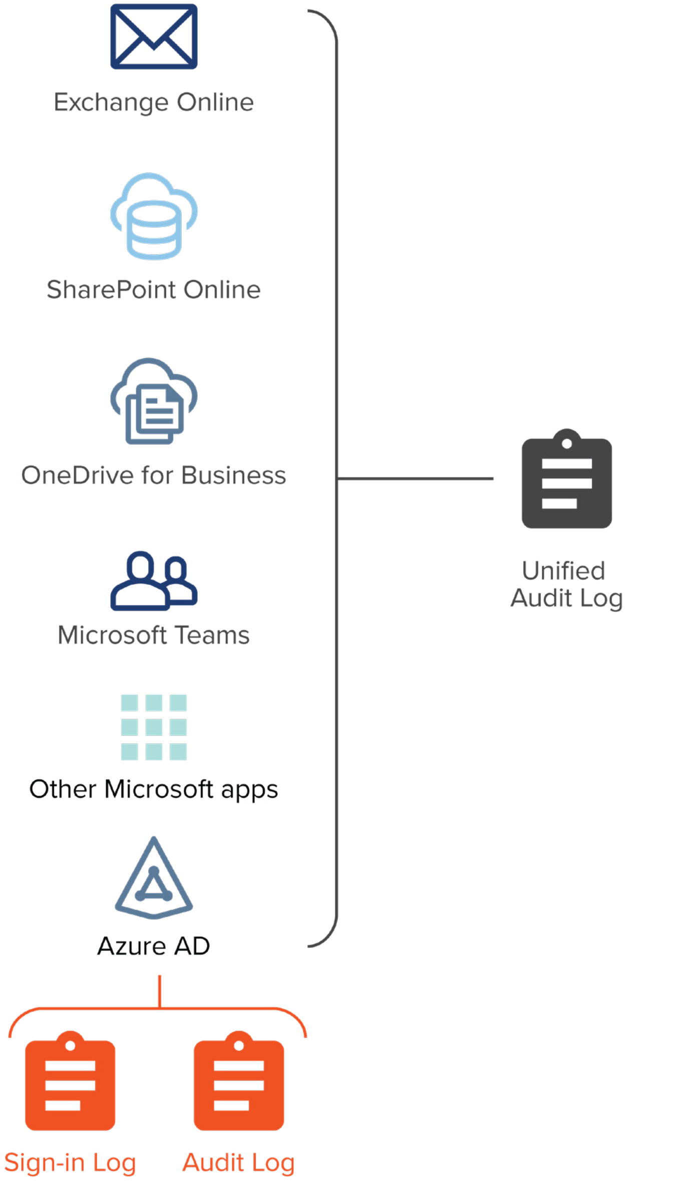


Figure 1. Unified Audit Log (for Office 365 audit log search)

How does auditing work in Azure and Office 365?

Managing and securing a cloud environment starts with being able to follow a user's login and logout events.

To obtain this information on premises, system administrators trying to track users must examine multiple logs on every Windows domain controller and correlate audit events across the logs of multiple servers.

In the cloud, administrators must correlate in a similar manner across two logs in Azure AD: the Audit Log, containing all change events, and the Sign-in Log, containing all authentication events. They access the logs through either the Azure Portal or PowerShell.

As for Office 365, each application — Exchange Online, SharePoint Online, OneDrive for Business, etc. — writes to what will become the Office 365 Unified Audit Log, containing all administrator- and user-level events. The Unified Audit Log also includes events from the Azure Audit Log and Sign-in Log (see Figure 1).

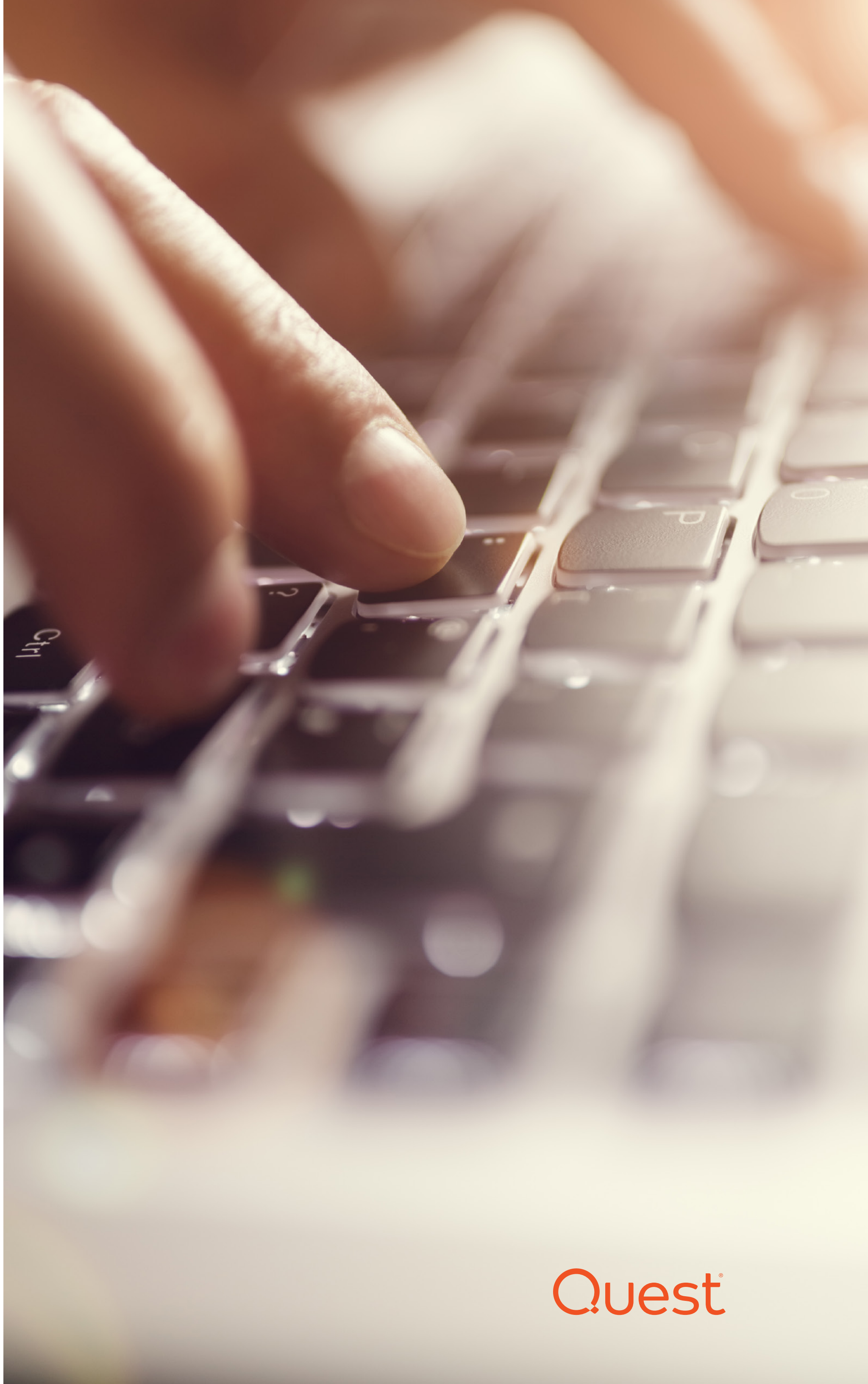
> To track a user's activity using native tools, administrators have to pull and correlate data from multiple logs.

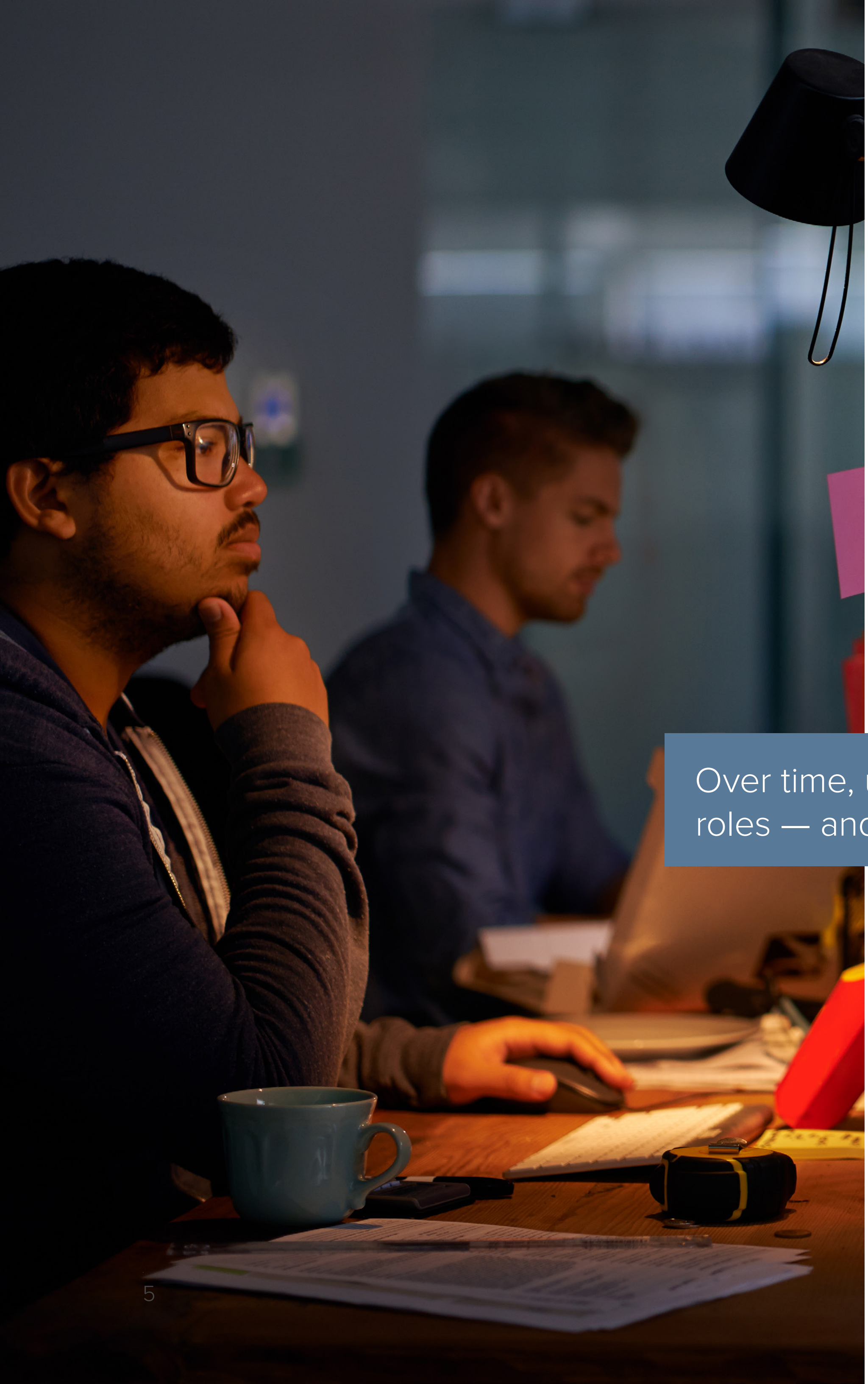
Administrators know where the logs are, and they know what kinds of data are stored in those logs. But pulling out that data and using it to manage and secure their environment is another matter.

THE AUDITING GAPS OF NATIVE TOOLS

Auditing in Azure and Office 365 has a number of limitations, including the following:

- For organizations with hybrid environments, it is not possible to search audit activity across on-premises and cloud workloads in a single view.
- Similarly, the audit policies for on-premises workloads must be configured separately from those for cloud workloads. Also, there is no way to monitor audit policies in case they are changed or disabled by other administrators.
- There can be a delay of 24 hours or more in processing some of the entries to the audit logs and adding them to the Unified Audit Log.
- The retention period for logs in Azure varies based on workload and subscription type, but even the longest ones are usually too short to enable proper incident investigations and regulatory compliance.
- Events are formatted differently depending on the type of event and whether it occurred on premises or in the cloud. With no normalized format, the logs visible through native consoles are difficult to interpret and correlate.
- It is possible to access the audit events for Azure and Office 365 through PowerShell, and both Azure and Office 365 provide a web portal for accessing audit events. However, the portal displays only 15 events at a time, and the processing delay means that not all relevant audit events are necessarily there when you need them.





1. Changes to important roles

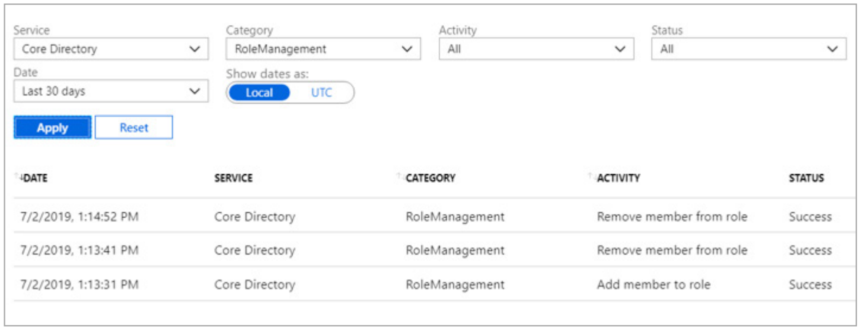
In an on-premises Active Directory, permissions are usually assigned through membership in security groups. It's particularly important to monitor changes to groups like Domain Administrators, Account Operators and Server Administrators, because of the powerful rights they bestow.

In the cloud, users gain additional permissions through their Azure roles, which include various types of administrators, operators, managers and helpdesk technicians. Over time, however, users often gradually acquire many more roles, and therefore rights, than they should have. Moreover, malicious actors try to escalate their permissions by gaining membership in critical roles. Therefore, security in the cloud requires being able to report and alert on changes to important roles.

> Over time, users often gradually acquire many more roles — and therefore rights — than they should have.

FINDING ROLES IN THE AZURE AUDIT LOG

The first step is to identify changes to critical roles. In the Azure portal, in the **Audit logs** section under Azure Active Directory, a search on the **Core Directory** service and **RoleManagement** category returns all of the changes to roles in the tenant, as shown in Figure 2. Unfortunately, that does not allow direct searches for only the roles deemed important; administrators must examine each audit event individually to know which role was modified.



Service: Core Directory
Category: RoleManagement
Activity: All
Status: All
Date: Last 30 days
Show dates as: Local | UTC

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
7/2/2019, 1:14:52 PM	Core Directory	RoleManagement	Remove member from role	Success
7/2/2019, 1:13:41 PM	Core Directory	RoleManagement	Remove member from role	Success
7/2/2019, 1:13:31 PM	Core Directory	RoleManagement	Add member to role	Success

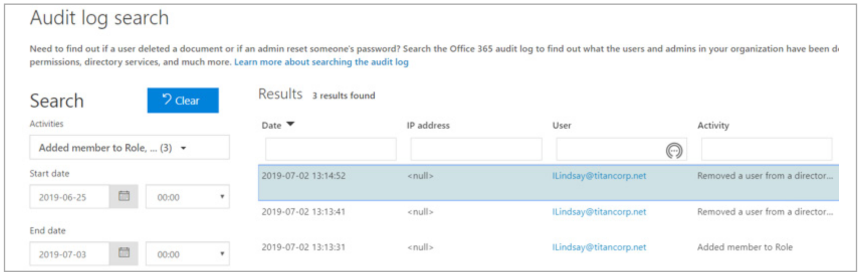
Figure 2. Searching on roles in Azure portal

Exporting data to Excel requires subscriptions to both Office 365 and Azure.

Another option is to export and analyze the results as a Microsoft Excel spreadsheet. That requires a subscription not only to Office 365 but also to Azure.

FINDING ROLE CHANGES IN THE UNIFIED AUDIT LOG

Information about role changes can also be gathered from a search of the Unified Audit Log through the Office 365 Security & Compliance Center. (These searches run against the logs of Azure AD, plus the logs of all Office 365 tools, as described above. They may take longer than searches against the Azure Audit Log alone.)



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been d
permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: Added member to Role, ... (3)
Start date: 2019-06-25 00:00
End date: 2019-07-03 00:00

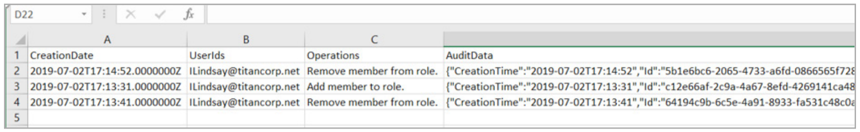
Results 3 results found

Date	IP address	User	Activity
2019-07-02 13:14:52	<null>	ILindsay@titancorp.net	Removed a user from a director...
2019-07-02 13:13:41	<null>	ILindsay@titancorp.net	Removed a user from a director...
2019-07-02 13:13:31	<null>	ILindsay@titancorp.net	Added member to Role

Figure 3. Unified Audit Log search

You can limit the search to all actions related to role administration within a given date range (see Figure 3), which is an advantage over searching the Azure Audit Log.

However, the entire audit detail is in one embedded JSON, so identifying the modified role means looking through all of the details. It is possible to export the data to a tool like Excel, but the entire JSON is put into the **AuditData** column (see Figure 4), so it is difficult to filter for modified roles.



D22

	A	B	C	
1	CreationDate	UserIds	Operations	AuditData
2	2019-07-02T17:14:52.0000000Z	ILindsay@titancorp.net	Remove member from role.	{"CreationTime":"2019-07-02T17:14:52","Id":"5b1e6bc6-2065-4733-a6fd-0866565f728
3	2019-07-02T17:13:31.0000000Z	ILindsay@titancorp.net	Add member to role.	{"CreationTime":"2019-07-02T17:13:31","Id":"c12e66af-2c9a-4a67-8efd-4269141ca48
4	2019-07-02T17:13:41.0000000Z	ILindsay@titancorp.net	Remove member from role.	{"CreationTime":"2019-07-02T17:13:41","Id":"64194c9b-6c5e-4a91-8933-fa531c48c0a
5				

Figure 4. Unified Audit Log search results viewed in Microsoft Excel

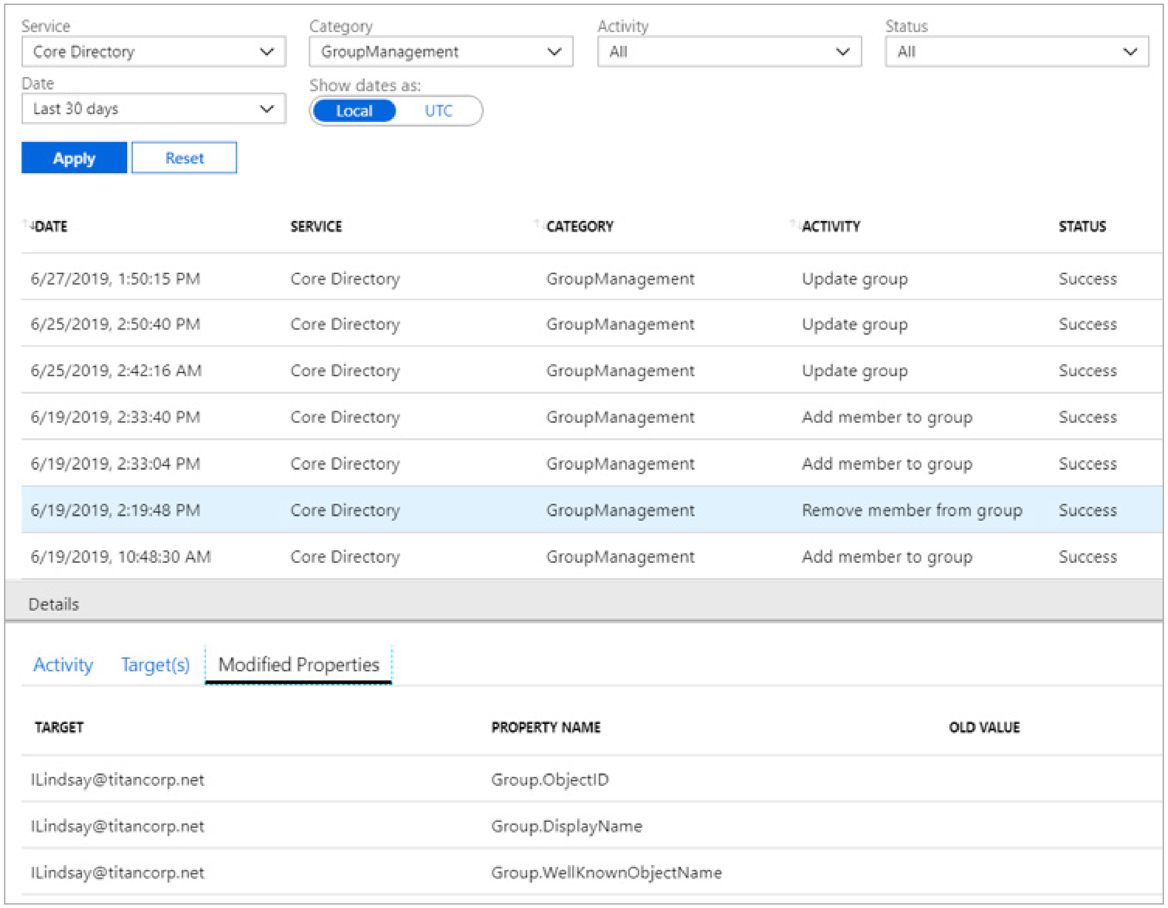
2. Changes to groups

As noted earlier, groups are the primary means for granting access to resources in AD. That remains true in the cloud, with some complications:

- Azure allows more types of groups. For example, users can create groups through apps like Outlook and Teams.
- Microsoft 365 groups, such as those created through Teams, generate other Azure resources to support the application.[1]
- Azure AD makes it easy to create B2B groups for collaboration with customers and vendors, which increases the risk of a user granting improper access to a third party.

Controlling group membership is even more complicated in the cloud than in your on-prem AD.

[1] For more information, see the ebook, "Frequently Asked Questions: Office 365 Groups," https://www.quest.com/whitepaper/frequently-asked-questions-office-365-groups8134485/.



Service: Core Directory

Category: GroupManagement

Activity: All

Status: All

Date: Last 30 days

Show dates as: Local

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
6/27/2019, 1:50:15 PM	Core Directory	GroupManagement	Update group	Success
6/25/2019, 2:50:40 PM	Core Directory	GroupManagement	Update group	Success
6/25/2019, 2:42:16 AM	Core Directory	GroupManagement	Update group	Success
6/19/2019, 2:33:40 PM	Core Directory	GroupManagement	Add member to group	Success
6/19/2019, 2:33:04 PM	Core Directory	GroupManagement	Add member to group	Success
6/19/2019, 2:19:48 PM	Core Directory	GroupManagement	Remove member from group	Success
6/19/2019, 10:48:30 AM	Core Directory	GroupManagement	Add member to group	Success

TARGET	PROPERTY NAME	OLD VALUE
lLindsay@titancorp.net	Group.ObjectID	
lLindsay@titancorp.net	Group.DisplayName	
lLindsay@titancorp.net	Group.WellKnownObjectName	

Figure 5. Searching on groups in the Azure portal

FINDING GROUP CHANGES IN THE AZURE AUDIT LOG

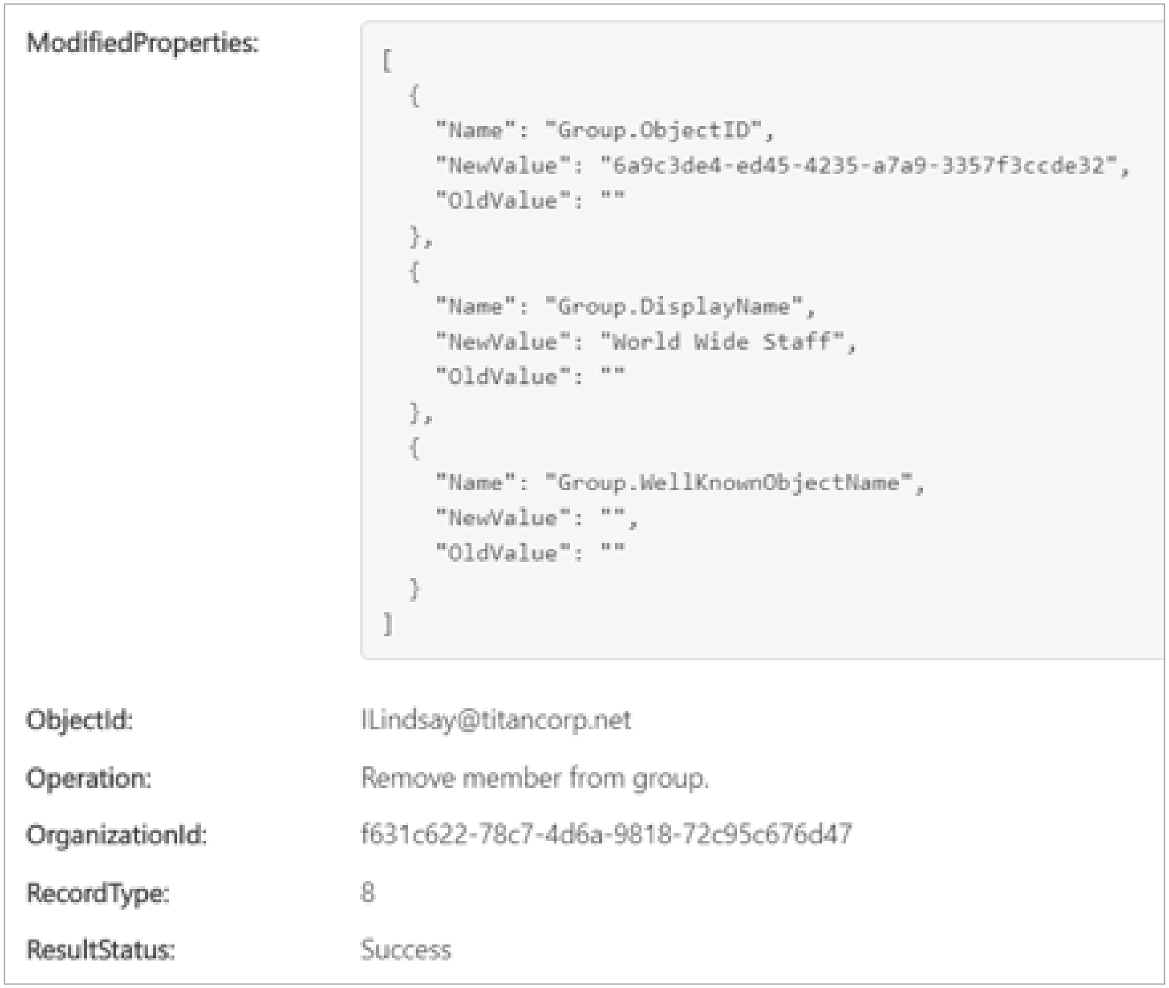
As with role changes, the Azure portal is the logical first stop for keeping track of changes to groups. In the **Audit logs** section under Azure Active Directory, a search on the **Core Directory** service and **GroupManagement** category returns all of the changes to groups in the tenant (see the top of Figure 5). Again, however, the interface does not allow direct searches for only the groups deemed important. Furthermore, to find modified groups, administrators must examine the details of the audit event on the Modified Properties tab (see the bottom of Figure 5).

Another option is to export and analyze the results as a Microsoft Excel spreadsheet; again, that requires subscriptions to both Office 365 and Azure.

FINDING GROUP CHANGES IN THE UNIFIED AUDIT LOG

As with role changes, information on group changes can also be gathered in the Office 365 Security & Compliance Center using an audit log search on all **Azure AD group administration activities**. A search on **Added member to group** and **Removed member from group** yields the changes in membership (see Figure 6).

But that procedure still does not allow direct searches on only the desired groups; it is necessary to search for changes to all groups and then examine the data. And, again, the entire audit detail is in one embedded JSON, so identifying the modified group means looking through all of the details. It is possible to export the data to a tool like Excel, but the JSON makes it difficult to filter for the modified groups.



```
ModifiedProperties:    [
                         {
                           "Name": "Group.ObjectID",
                           "NewValue": "6a9c3de4-ed45-4235-a7a9-3357f3ccde32",
                           "OldValue": ""
                         },
                         {
                           "Name": "Group.DisplayName",
                           "NewValue": "World Wide Staff",
                           "OldValue": ""
                         },
                         {
                           "Name": "Group.WellKnownObjectName",
                           "NewValue": "",
                           "OldValue": ""
                         }
                       ]

ObjectId:              lLindsay@titancorp.net
Operation:             Remove member from group.
OrganizationId:        f631c622-78c7-4d6a-9818-72c95c676d47
RecordType:            8
ResultStatus:          Success
```

Figure 6. Modified properties in Unified Audit Log

3. Changes to applications

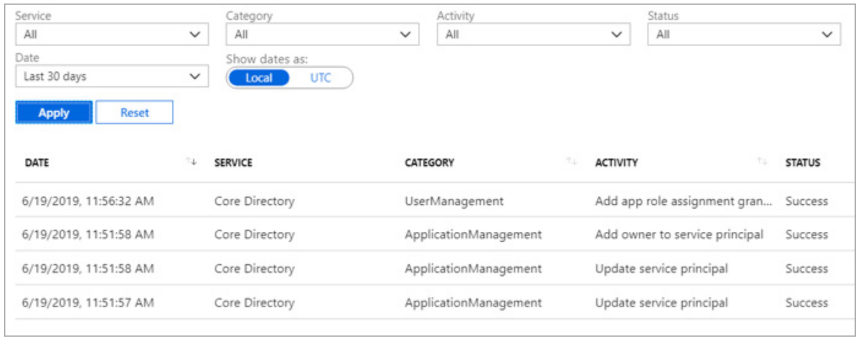
Azure AD streamlines setup of many SaaS applications and access to on-premises applications.

These applications can be easily broken if changes are not made correctly. While applications are unavailable, the business will suffer, as IT teams get pulled off of other key tasks to investigate, user productivity plummets and key business processes come to a halt. Thus, being able to track changes to applications is a business imperative.

> Finding all changes to a particular application using the Azure portal requires a lot of manual effort.

FINDING APPLICATION CHANGES IN THE AZURE AUDIT LOG

In the Azure portal, the first step to finding changes to an individual application is under **Azure Active Directory** in the **Audit logs** section for the individual application. The problem is that it takes a lot of repetitive manual drilling to find changes.



Service: All
Category: All
Activity: All
Status: All
Date: Last 30 days
Show dates as: Local UTC

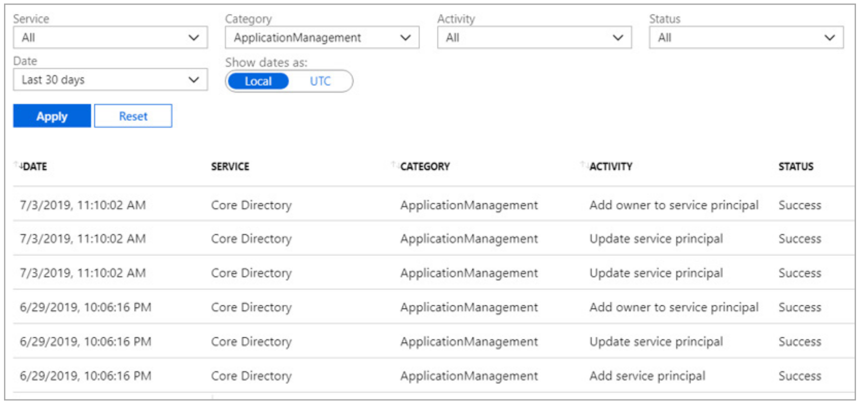
Apply Reset

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
6/19/2019, 11:56:32 AM	Core Directory	UserManagement	Add app role assignment gran...	Success
6/19/2019, 11:51:58 AM	Core Directory	ApplicationManagement	Add owner to service principal	Success
6/19/2019, 11:51:58 AM	Core Directory	ApplicationManagement	Update service principal	Success
6/19/2019, 11:51:57 AM	Core Directory	ApplicationManagement	Update service principal	Success

Figure 7. Application changes listed in Azure Audit Log

As shown in the **Category** column of Figure 7, the audit events come from **ApplicationManagement** and **UserManagement**.

Drilling into the **ApplicationManagement** category yields the list shown in Figure 8.

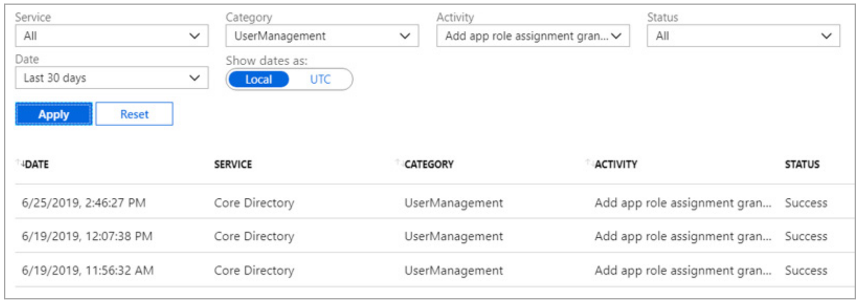


Service: All
Category: ApplicationManagement
Activity: All
Status: All
Date: Last 30 days
Show dates as: Local UTC

Apply Reset

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
7/3/2019, 11:10:02 AM	Core Directory	ApplicationManagement	Add owner to service principal	Success
7/3/2019, 11:10:02 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/3/2019, 11:10:02 AM	Core Directory	ApplicationManagement	Update service principal	Success
6/29/2019, 10:06:16 PM	Core Directory	ApplicationManagement	Add owner to service principal	Success
6/29/2019, 10:06:16 PM	Core Directory	ApplicationManagement	Update service principal	Success
6/29/2019, 10:06:16 PM	Core Directory	ApplicationManagement	Add service principal	Success

Figure 8. Searching for ApplicationManagement events



Service: All
Category: UserManagement
Activity: Add app role assignment gran...
Status: All
Date: Last 30 days
Show dates as: Local UTC

Apply Reset

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
6/25/2019, 2:46:27 PM	Core Directory	UserManagement	Add app role assignment gran...	Success
6/19/2019, 12:07:38 PM	Core Directory	UserManagement	Add app role assignment gran...	Success
6/19/2019, 11:56:32 AM	Core Directory	UserManagement	Add app role assignment gran...	Success

Figure 9. Searching for UserManagement events

To drill into the application changes related to **UserManagement**, it is necessary to switch to that category and then select the following five activities from the **Activity** drop-down:

- Add app role assignment to user (see Figure 9)
- Create application password for user
- Delete application password for user
- Remove app role assignment from user
- Review app assignment

Thus, there is no easy way to search on all application changes or generate a list containing only the desired ones.

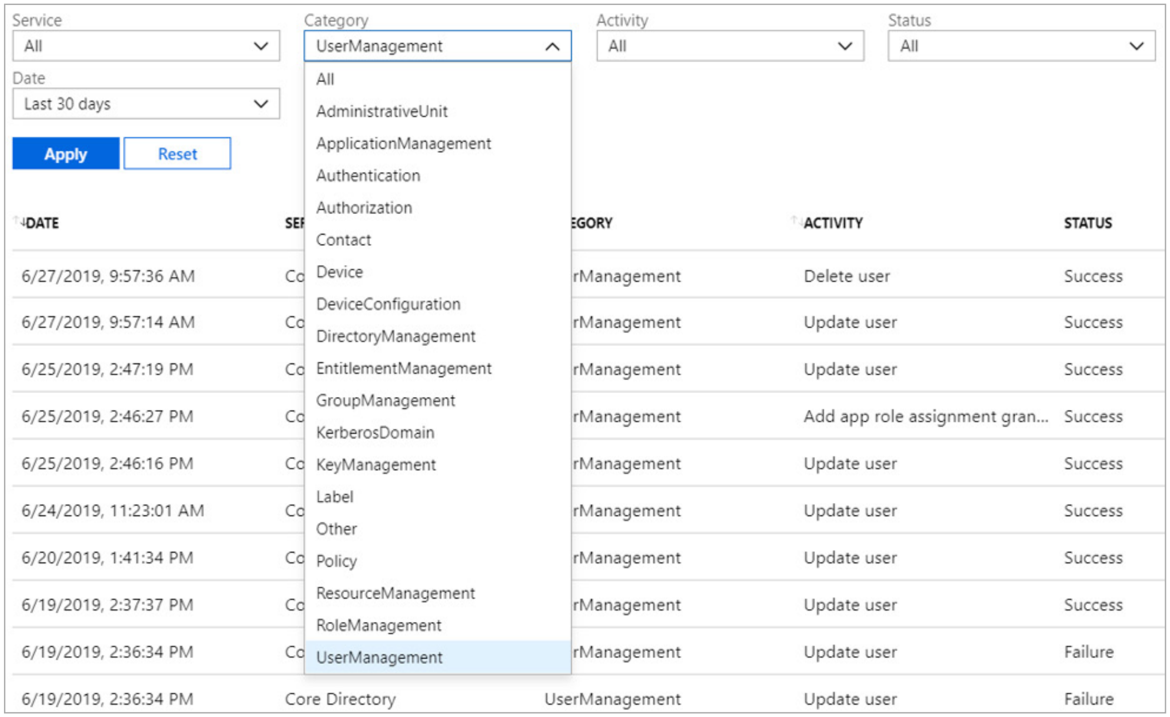
4. Resource creation

In the Microsoft cloud, resources are created not only explicitly, but also under the covers, by applications. For example, when a user creates a Microsoft Teams site, multiple resources are created automatically, including a group inbox and calendar in Outlook, a SharePoint site, and a OneNote notebook. Being able to track the kind and number of resources being created will help administrators reduce the costly and time-consuming burden of managing them.

FINDING CREATED RESOURCES IN THE AZURE AUDIT LOG

The best place to discover the resources that have been created is in the Azure portal, in the **Audit logs** section under Azure Active Directory.

Unfortunately, it is possible to search on only one category at a time, so administrators must execute multiple queries to gather the information. Search first on **UserManagement** (see Figure 10), and then on **GroupManagement**.

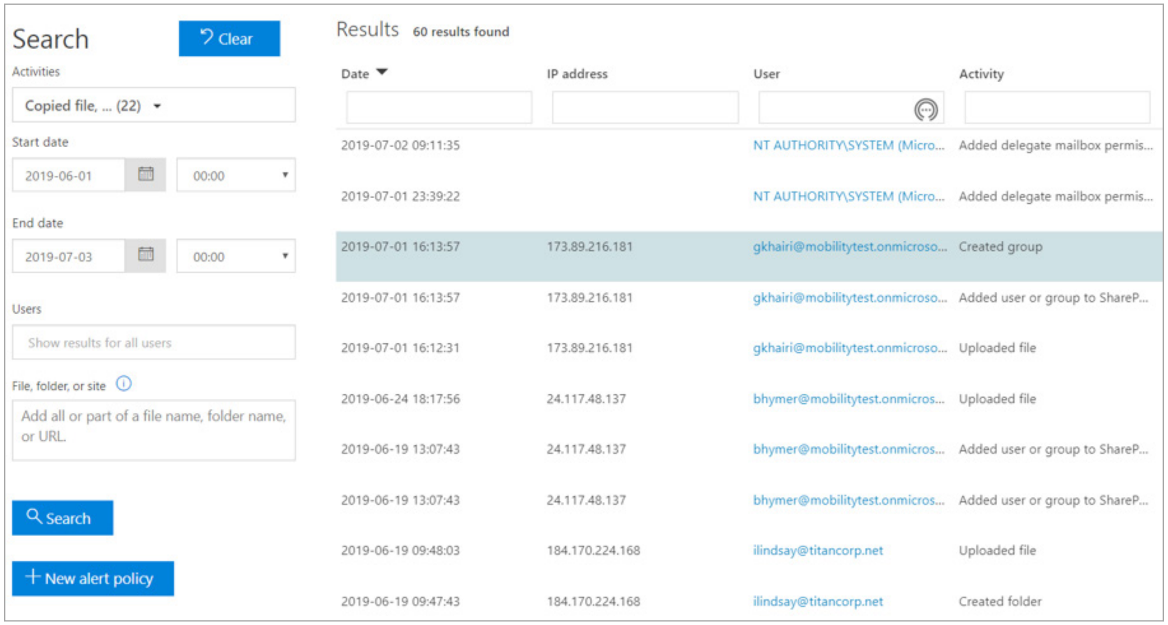


Service: All
Category: UserManagement
Activity: All
Status: All
Date: Last 30 days

DATE	SER	EGORY	ACTIVITY	STATUS
6/27/2019, 9:57:36 AM	Co	rManagement	Delete user	Success
6/27/2019, 9:57:14 AM	Co	rManagement	Update user	Success
6/25/2019, 2:47:19 PM	Co	rManagement	Update user	Success
6/25/2019, 2:46:27 PM	Co	rManagement	Add app role assignment gran...	Success
6/25/2019, 2:46:16 PM	Co	rManagement	Update user	Success
6/24/2019, 11:23:01 AM	Co	rManagement	Update user	Success
6/20/2019, 1:41:34 PM	Co	rManagement	Update user	Success
6/19/2019, 2:37:37 PM	Co	rManagement	Update user	Success
6/19/2019, 2:36:34 PM	Co	rManagement	Update user	Failure
6/19/2019, 2:36:34 PM	Core Directory	UserManagement	Update user	Failure

Figure 10. Created resources listed in the Azure portal

In the cloud, resources are created not only explicitly, but also under the covers, by applications like Teams.



Search

Activities: Copied file, ... (22)

Start date: 2019-06-01 00:00

End date: 2019-07-03 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Results 60 results found

Date	IP address	User	Activity
2019-07-02 09:11:35		NT AUTHORITY\SYSTEM (Micro...	Added delegate mailbox permis...
2019-07-01 23:39:22		NT AUTHORITY\SYSTEM (Micro...	Added delegate mailbox permis...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created group
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Added user or group to ShareP...
2019-07-01 16:12:31	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Uploaded file
2019-06-24 18:17:56	24.117.48.137	bhymer@mobilitytest.onmicros...	Uploaded file
2019-06-19 13:07:43	24.117.48.137	bhymer@mobilitytest.onmicros...	Added user or group to ShareP...
2019-06-19 13:07:43	24.117.48.137	bhymer@mobilitytest.onmicros...	Added user or group to ShareP...
2019-06-19 09:48:03	184.170.224.168	ilindsay@titancorp.net	Uploaded file
2019-06-19 09:47:43	184.170.224.168	ilindsay@titancorp.net	Created folder

Figure 11. Created resources listed in Unified Audit Log

FINDING CREATED RESOURCES IN THE UNIFIED AUDIT LOG

The audit log search in the Office 365 Security & Compliance portal (see Figure 11) offers a view of multiple resources:

- **Files —** Copied, moved, uploaded, renamed, restored files
- **Folders —** Created, renamed, moved, restored folders
- **SharePoint sites —** Created list, created list item
- **Site permissions —** Added site collection admin, added user or group to SharePoint group, created group
- **Exchange —** Created mailbox item, added mailbox permissions
- **Teams —** Created team, added tab, added connector, added channel, added member, added bot

Getting a full picture of all of these resources requires multiple queries. And, as with any other search of Office 365 audit events, the details will be in the embedded JSON, which makes them less accessible than a simple query result.

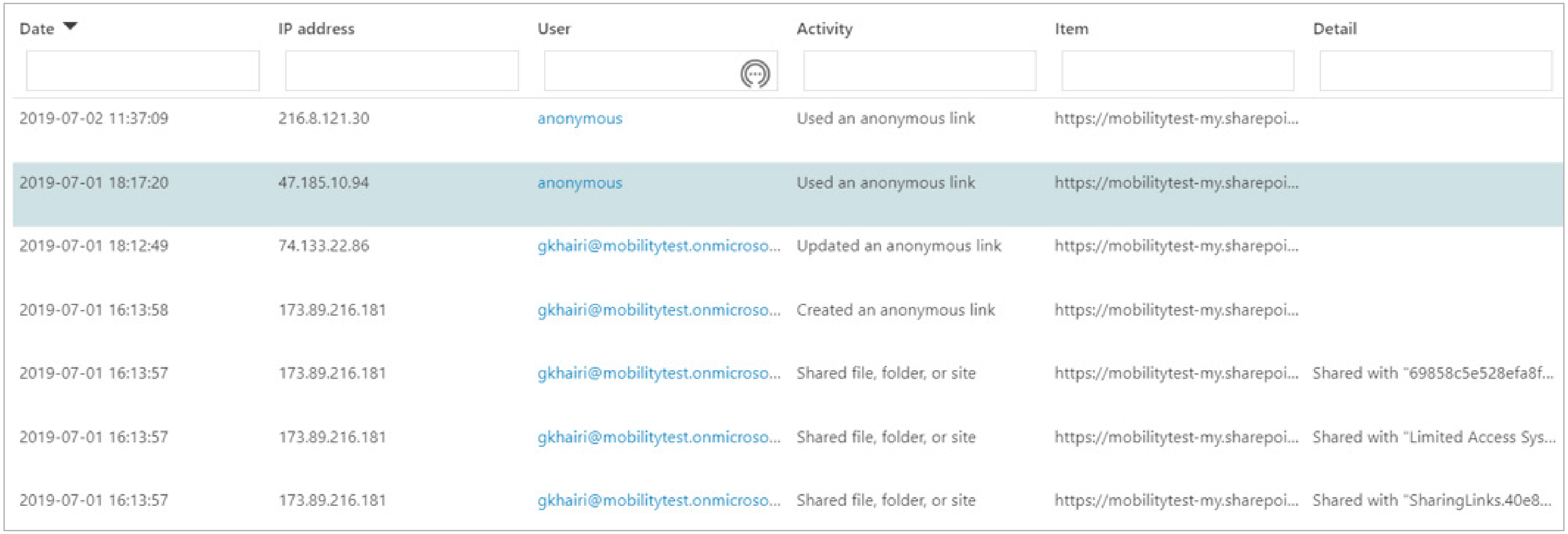
5. Sharing of important files and anonymous links

Moving to SharePoint Online and OneDrive for Business introduces new kinds of risk, especially around data sharing. As mentioned above, users can unintentionally share sensitive data by including a B2B user from another company without realizing it. Moreover, users can easily create links that enable anyone who obtains them to access data on the corporate OneDrive anonymously. Therefore, organizations have strong reasons to block or tightly control the sharing of specific content.

> Users can easily create links that enable anyone who receives them to access your OneDrive data anonymously.

FINDING SHARES AND ACCESS REQUESTS IN THE UNIFIED AUDIT LOG

The audit log search in the Office 365 Security & Compliance portal returns information on shared files, folders and sites. Figure 12 depicts the results of a search on **Sharing and access request activities**.



Date ▼	IP address	User	Activity	Item	Detail
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "69858c5e528efa8f...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "Limited Access Sys...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "SharingLinks.40e8...

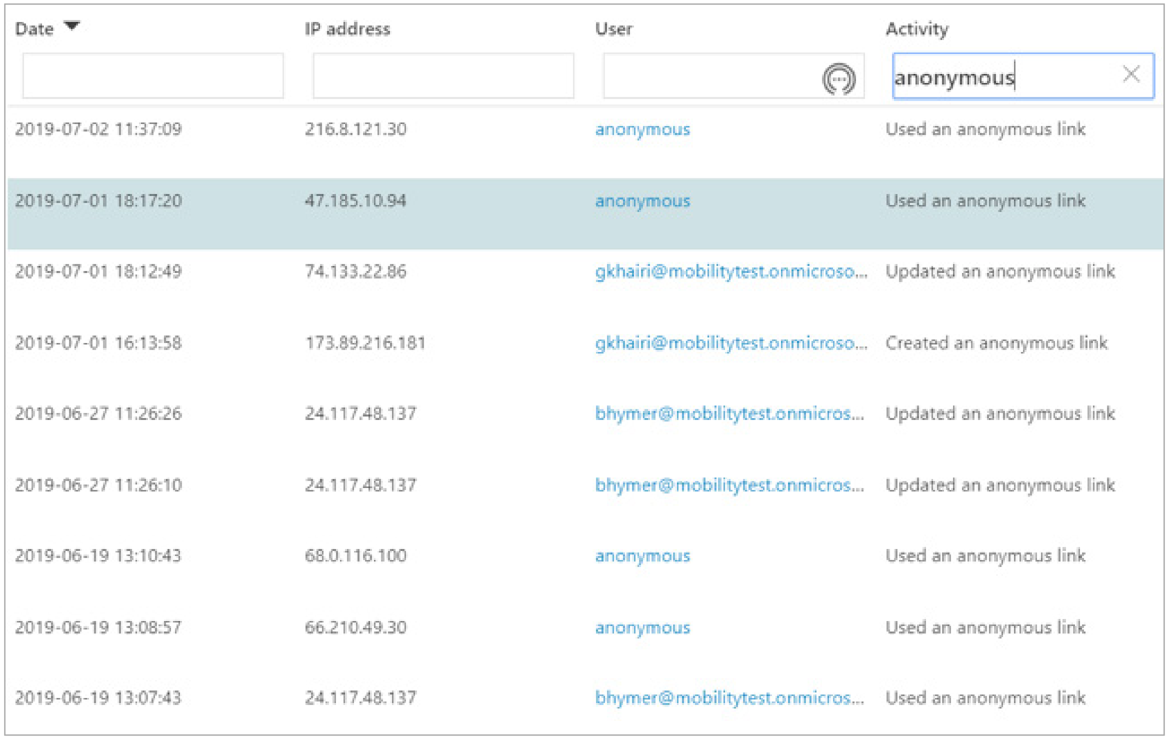
Figure 12. Sharing activity listed in the Office 365 Security & Compliance portal

The problem is that the query returns all the data for those activities. A more effective and more useful query would limit results by file extension, such as CER, DER, CRT, PEM, PFX, P7B, P7C, P12, PPK, PUB, SPC, STL, CRL, SSH, EVT, EXE, BAT, PIF. Or it would pare the results down to Microsoft Office file extensions, such as PPT, PPTX, XLS, XLSX, DOC and DOCX. The audit log search does not allow for that.

Another option is to export the superset of data from the **AuditData** field in the Unified Audit Log to a spreadsheet. Still, some data manipulation is necessary to narrow the results to the questionable sharing activity.

Anonymous access events, which are of particular interest, are easier to query by entering the word **anonymous** in the Activity filter, as shown in Figure 13.

Changing the User filter to **anonymous** returns any file that was accessed anonymously. Similar results come from filtering on the **UserIds** or **Operations** columns in the exported audit events.



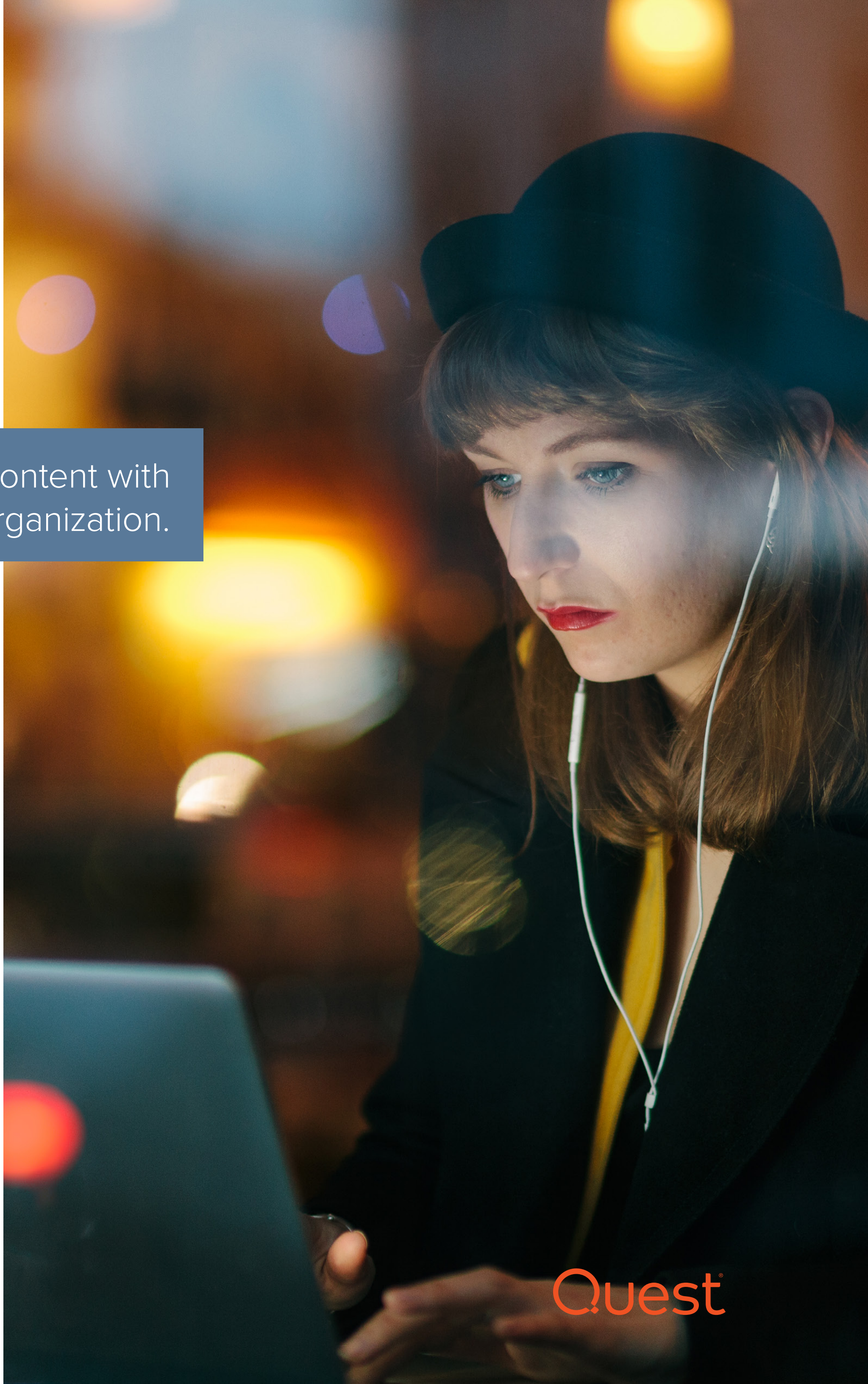
Date ▼	IP address	User	Activity
			anonymous
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link
2019-06-27 11:26:26	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-27 11:26:10	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-19 13:10:43	68.0.116.100	anonymous	Used an anonymous link
2019-06-19 13:08:57	66.210.49.30	anonymous	Used an anonymous link
2019-06-19 13:07:43	24.117.48.137	bhymer@mobilitytest.onmicros...	Used an anonymous link

Figure 13. Limiting the search results to anonymous sharing activity

6. Guest access in Teams

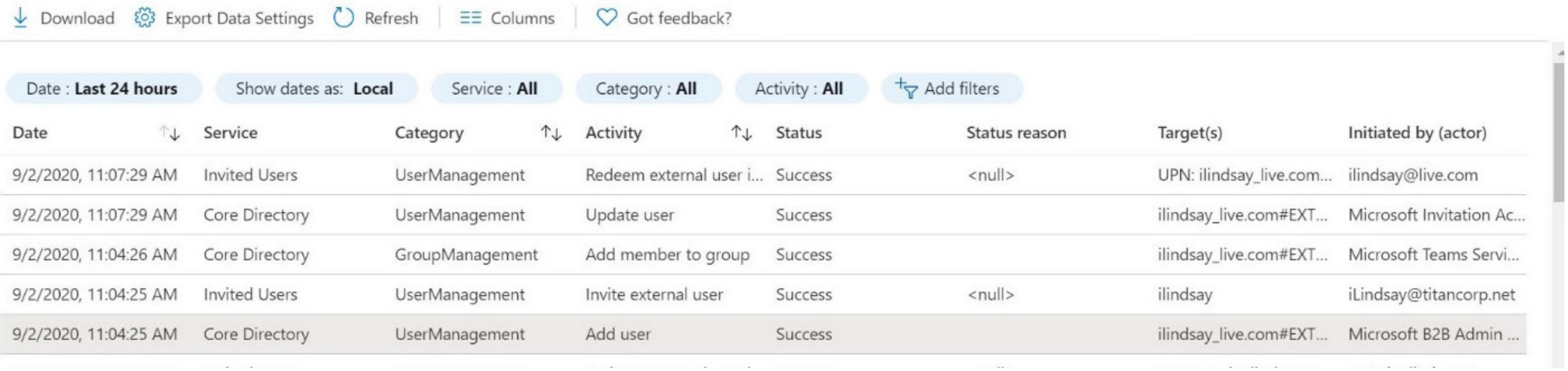
Adoption of Microsoft Team exploded when organizations needed to quickly enable employees to work from home as the Covid-19 pandemic began to spread. In the rush to deploy the application, some organizations did not take the time to consider and mitigate the security risks.

Microsoft Teams makes it easy for users to share content with each other — and with guests from outside your organization.



The power of Microsoft Teams is that it makes collaboration and communication easy, both within an organization and with external users, such as customers or partners. A team is made up of a set of user accounts in Azure AD, an Microsoft 365 group in Azure AD, a distribution list in Office 365 and a SharePoint site that stores the data. By default, team owners can easily add anyone they like to their team, including external users (called guests), and those people will have full access to the team's chats, meetings and files. Clearly, this is a security risk that must be well controlled by IT.

In addition, adding an external user to a team will create a new user account in your Azure AD. This could have implications for your software licensing, since some vendors require a license for all active users in AD and Azure AD, including external ones.



Date : **Last 24 hours** | Show dates as: **Local** | Service : **All** | Category : **All** | Activity : **All**

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
9/2/2020, 11:07:29 AM	Invited Users	UserManagement	Redeem external user i...	Success	<null>	UPN: ilindsay_live.com...	ilindsay@live.com
9/2/2020, 11:07:29 AM	Core Directory	UserManagement	Update user	Success		ilindsay_live.com#EXT...	Microsoft Invitation Ac...
9/2/2020, 11:04:26 AM	Core Directory	GroupManagement	Add member to group	Success		ilindsay_live.com#EXT...	Microsoft Teams Servi...
9/2/2020, 11:04:25 AM	Invited Users	UserManagement	Invite external user	Success	<null>	ilindsay	iLindsay@titancorp.net
9/2/2020, 11:04:25 AM	Core Directory	UserManagement	Add user	Success		ilindsay_live.com#EXT...	Microsoft B2B Admin ...

Figure 14. Events for an invited user as shown in the Azure portal

FINDING GUEST USERS IN THE AZURE AUDIT LOG

When an external user is invited to join a team, three things will happen in Azure AD: A new user account will be created, an invitation will be emailed to the user and the new account will be added to the Microsoft 365 group that controls the team (see the highlighted row in Figure 14). When the user accepts the invitation, two additional events will be generated (see the top two rows in Figure 14).

To show just the user creation events, set up the following filters:

- **Service —** Core Directory
- **Category —** UserManagement
- **Activity —** Add user

Unfortunately, there is no way to filter to just external users. You need to find them manually by looking for **#EXT** in the user name.

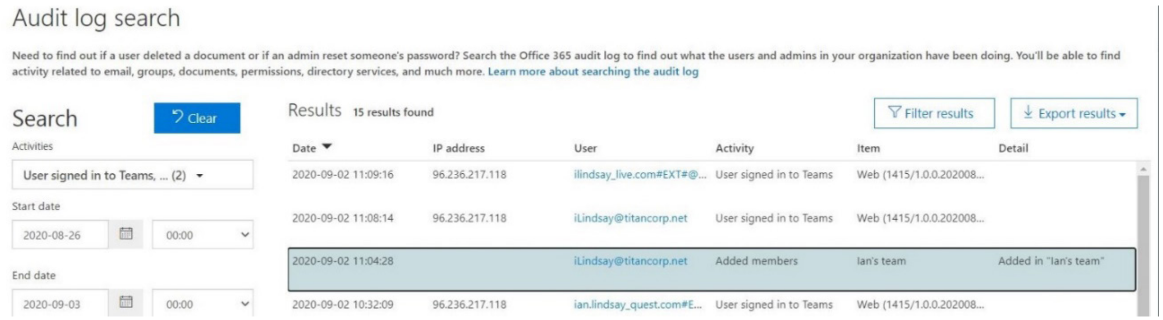
FINDING GUEST USERS IN THE UNIFIED AUDIT LOG

Information about user creation and other activity in Teams can also be gathered from a search of the Unified Audit Log through the Office 365 Security & Compliance Center. These searches run against the logs of Azure AD, plus the logs of all Office 365 tools, as described above, so they can take longer than searches against the Azure Audit Log alone. There can also be a delay of 15 minutes or more until new entries appear in the log.

> Not all relevant audit events might be in the log when you need them, due to processing delays.

You can limit the search by date range (see Figure 15), which is an advantage over searching the Azure Audit Log. Click on the audit record to display the details (see Figure 16); you can find the added users in the **Members** section. However, all of the audit details are in one embedded JSON, so identifying added users means looking through each record individually, which can be quite a cumbersome and error-prone process, especially if you have a lot of records to examine.

To identify new guest users in Teams using the native logs, you have to painstakingly review each event record.



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: User signed in to Teams, ... (2)

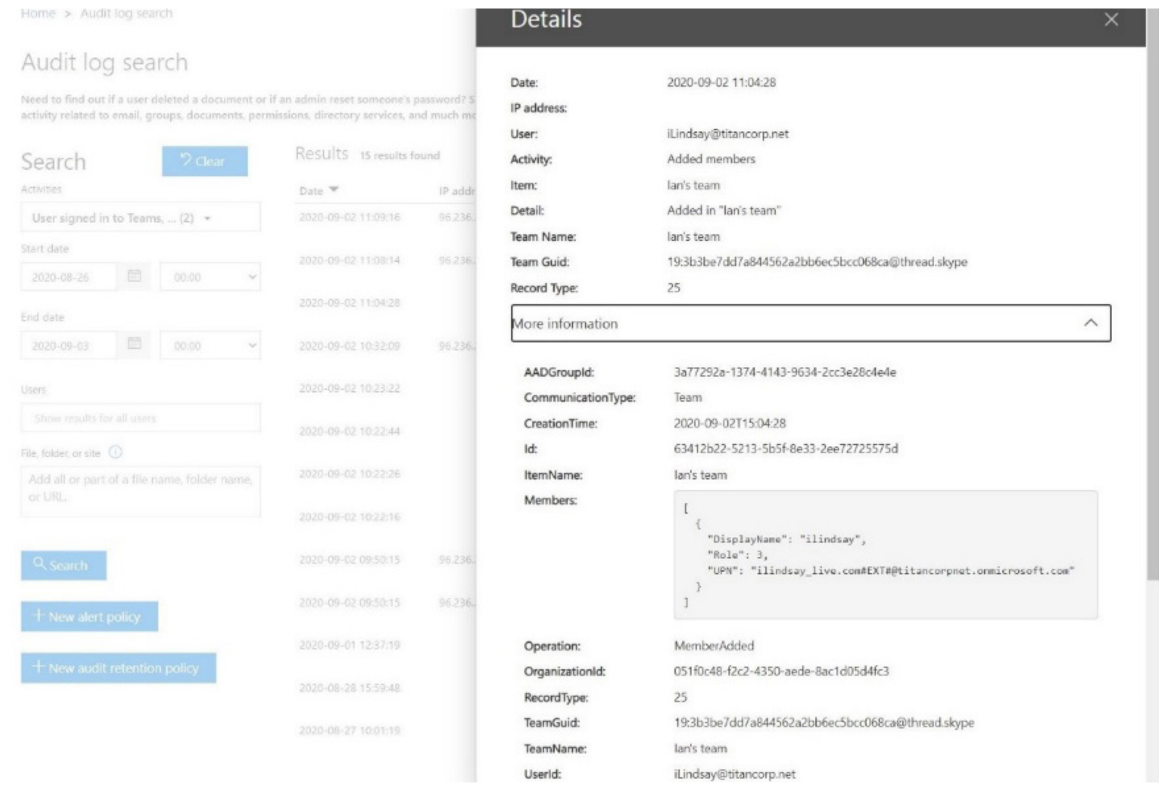
Start date: 2020-08-26 00:00

End date: 2020-09-03 00:00

Results 15 results found

Date	IP address	User	Activity	Item	Detail
2020-09-02 11:09:16	96.236.217.118	ilindsay_live.com#EXT#@...	User signed in to Teams	Web (1415/1.0.0.202008...	
2020-09-02 11:08:14	96.236.217.118	iLindsay@titancorp.net	User signed in to Teams	Web (1415/1.0.0.202008...	
2020-09-02 11:04:28		iLindsay@titancorp.net	Added members	Ian's team	Added in "Ian's team"
2020-09-02 10:32:09	96.236.217.118	ian.lindsay_quest.com#E...	User signed in to Teams	Web (1415/1.0.0.202008...	

Figure 15. Searching for user creation in the Office 365 Security & Compliance Center



Details

Date:	2020-09-02 11:04:28
IP address:	
User:	iLindsay@titancorp.net
Activity:	Added members
Item:	Ian's team
Detail:	Added in "Ian's team"
Team Name:	Ian's team
Team Guid:	19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype
Record Type:	25

More information

AADGroupId:	3a77292a-1374-4143-9634-2cc3e28c4e4e
CommunicationType:	Team
CreationTime:	2020-09-02T15:04:28
Id:	63412b22-5213-5b5f-8e33-2ee72725575d
ItemName:	Ian's team
Members:	

```
[
  {
    "DisplayName": "ilindsay",
    "Role": 3,
    "UPN": "ilindsay_live.com#EXT#@titancorpnet.onmicrosoft.com"
  }
]
```

Operation:	MemberAdded
OrganizationId:	051f0c48-f2c2-4350-aede-8ac1d05d4fc3
RecordType:	25
TeamGuid:	19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype
TeamName:	Ian's team
UserId:	iLindsay@titancorp.net

Figure 16. Viewing the details of a user creation event

You have two options for exporting the data to a tool like Excel: **Save loaded results** and **Download all results** (see Figure 17). If you choose the former option, the JSON information is not included in the downloaded file, as shown in Figure 18. You can see which team had a user account added, but not what user account it was; you still need to look at the Audit Log in the Office Portal to find that information.

To get more information, choose the **Download all results** option. However, the entire audit detail will be in one embedded JSON in the **AuditData** column (see Figure 19), so identifying the created user means looking through all of the details.

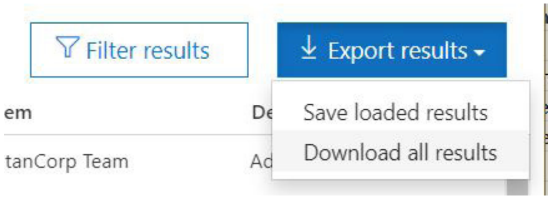
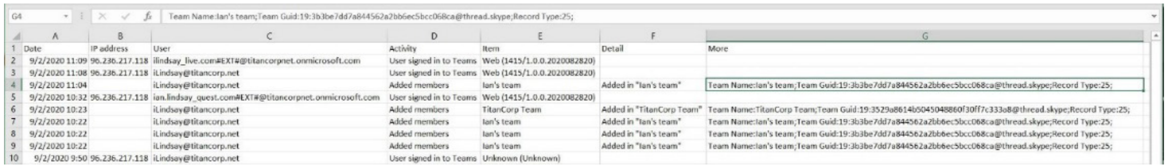


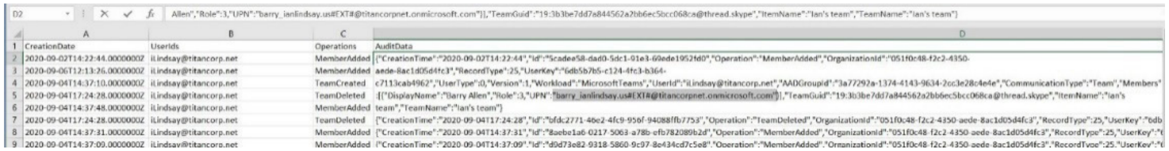
Figure 17. Options for exporting results to Microsoft Excel



G4 — Team Name:Ian's team;Team Guid:19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype;Record Type:25;

	A	B	C	D	E	F	G
1	Date	IP address	User	Activity	Item	Detail	More
2	9/2/2020 11:09	96.236.217.118	ilindsay_live.com#EXT#@titancorpnet.onmicrosoft.com	User signed in to Teams	Web (1415/1.0.0.2020082820)		
3	9/2/2020 11:08	96.236.217.118	iLindsay@titancorp.net	User signed in to Teams	Web (1415/1.0.0.2020082820)		
4	9/2/2020 11:04		iLindsay@titancorp.net	Added members	Ian's team	Added in "Ian's team"	Team Name:Ian's team;Team Guid:19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype;Record Type:25;
5	9/2/2020 10:32	96.236.217.118	ian.lindsay_quest.com#EXT#@titancorpnet.onmicrosoft.com	User signed in to Teams	Web (1415/1.0.0.2020082820)		
6	9/2/2020 10:23		iLindsay@titancorp.net	Added members	TitanCorp Team	Added in "TitanCorp Team"	Team Name:TitanCorp Team;Team Guid:19:3529a8614b5045048860f30ff7c333a8@thread.skype;Record Type:25;
7	9/2/2020 10:22		iLindsay@titancorp.net	Added members	Ian's team	Added in "Ian's team"	Team Name:Ian's team;Team Guid:19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype;Record Type:25;
8	9/2/2020 10:22		iLindsay@titancorp.net	Added members	Ian's team	Added in "Ian's team"	Team Name:Ian's team;Team Guid:19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype;Record Type:25;
9	9/2/2020 10:22		iLindsay@titancorp.net	Added members	Ian's team	Added in "Ian's team"	Team Name:Ian's team;Team Guid:19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype;Record Type:25;
10	9/2/2020 9:50	96.236.217.118	iLindsay@titancorp.net	User signed in to Teams	Unknown (Unknown)		

Figure 18. User creation search results viewed in Microsoft Excel



D2 — Allen","Role":3,"UPN":"barry_ianlindsay.us#EXT#@titancorpnet.onmicrosoft.com"}],"TeamGuid":"19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype","ItemName":"Ian's team","TeamName":"Ian's team"}

	A	B	C	D
1	CreationDate	UserIds	Operations	AuditData
2	2020-09-02T14:22:44.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-02T14:22:44","Id":"5cadee58-dad0-5dc1-91e3-69ede1952fd0","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-
3	2020-09-06T12:13:26.0000000Z	iLindsay@titancorp.net	MemberAdded	aede-8ac1d05d4fc3","RecordType":25,"UserKey":"6db5b7b5-c124-4fc3-b364-
4	2020-09-04T14:37:10.0000000Z	iLindsay@titancorp.net	TeamCreated	c7113cab4962","UserType":0,"Version":1,"Workload":"MicrosoftTeams","UserId":"iLindsay@titancorp.net","AADGroupId":"3a77292a-1374-4143-9634-2cc3e28c4e4e","CommunicationType":"Team","Members"
5	2020-09-04T17:24:28.0000000Z	iLindsay@titancorp.net	TeamDeleted	:[{"DisplayName":"Barry Allen","Role":3,"UPN":"barry_ianlindsay.us#EXT#@titancorpnet.onmicrosoft.com"}],"TeamGuid":"19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype","ItemName":"Ian's
6	2020-09-04T14:37:48.0000000Z	iLindsay@titancorp.net	MemberAdded	team","TeamName":"Ian's team"}
7	2020-09-04T17:24:28.0000000Z	iLindsay@titancorp.net	TeamDeleted	{"CreationTime":"2020-09-04T17:24:28","Id":"bfdc2771-46e2-4fc9-956f-94088ffb7753","Operation":"TeamDeleted","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"6db
8	2020-09-04T14:37:31.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-04T14:37:31","Id":"8aebe1a6-0217-5063-a78b-efb782089b2d","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"
9	2020-09-04T14:37:09.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-04T14:37:09","Id":"d9d73e82-9318-5860-9c97-8e434cd7c5e8","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"

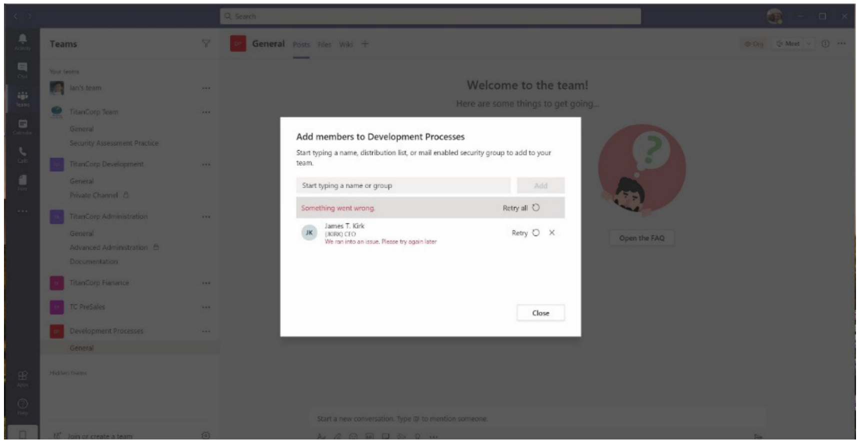
Figure 19. User creation search results with JSON viewed in Microsoft Excel

7. Teams being created or deleted

Teams facilitates collaboration by making it easy for users to create and delete teams. But native tools don't make it easy for admins to keep it all under control.

In addition to keeping a close eye on external users in Teams, you also need to keep track of what teams are being created and deleted. By default, users can create and delete teams at will to facilitate communication and collaboration. As an administrator, you can turn off that feature, but then users will have to go through IT every time they need a group created or removed. If you leave it enabled, you need to know exactly how it is being used — but if all you have is native tools, that's a tough challenge.

Plus, business users are not the only ones who can make unwanted changes to your teams; you also need to monitor the actions of administrators. For example, if an admin accidently deletes the Microsoft 365 group in Azure AD that corresponds to a team, a user who tries to add a user to the team will get the confusing error shown in Figure 20. The reason for the error is that the Microsoft 365 group for the team no longer exists, but there is no way for the user to know that.



Add members to Development Processes

Start typing a name, distribution list, or mail enabled security group to add to your team.

Start typing a name or group

Something went wrong.

James T. Kirk
(JKIRK) CFO
We ran into an issue. Please try again later

Welcome to the team!

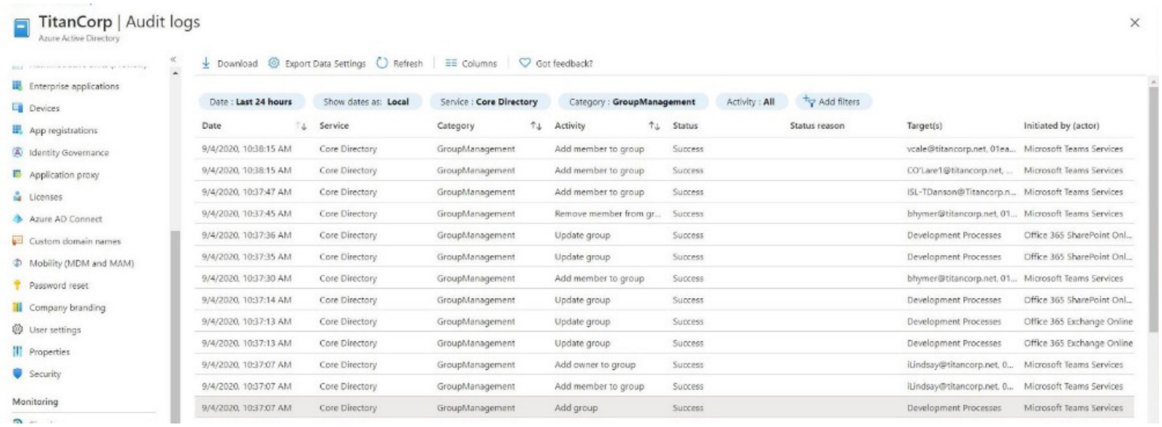
Here are some things to get going...

Start a new conversation. Type @ to mention someone.

Figure 20. If an admin deletes the M365 group for a team, a user who tries to add a user to the team will get a cryptic error.

FINDING TEAMS IN THE AZURE AUDIT LOG

Information about the creation or deletion of a team will not be in the Azure Audit Log directly, but there will be information about the creation or deletion of the associated Microsoft 365 group. However, there is no distinction between Microsoft 365 groups associated with teams and any other group in Azure AD, and the list will include all changes to the groups as well as creation and deletion events (see Figure 21). To narrow down the view to the records of most interest, set the filters as follows: Service to **Core Directory** and Category to **GroupManagement**. The events specific to Teams will have **Microsoft Teams Service** in the **Initiated by** field. Unfortunately, this field cannot be filtered upon.

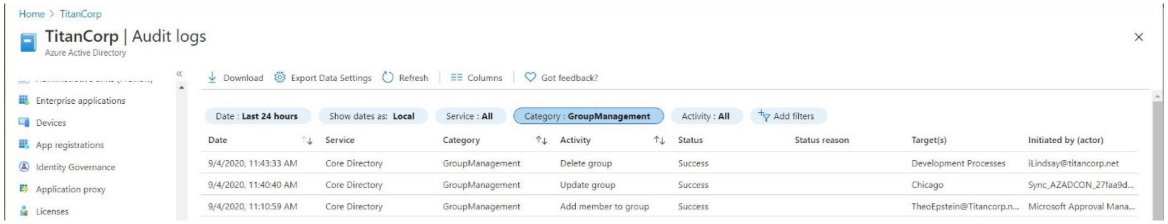


TitanCorp | Audit logs
Azure Active Directory

Date : **Last 24 hours** | Show dates as: **Local** | Service : **Core Directory** | Category : **GroupManagement** | Activity : **All**

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
9/4/2020, 10:38:15 AM	Core Directory	GroupManagement	Add member to group	Success		vcale@titancorp.net, 01ea...	Microsoft Teams Services
9/4/2020, 10:38:15 AM	Core Directory	GroupManagement	Add member to group	Success		CO'Lare1@titancorp.net, ...	Microsoft Teams Services
9/4/2020, 10:37:47 AM	Core Directory	GroupManagement	Add member to group	Success		ISL-TDanson@Titancorp.n...	Microsoft Teams Services
9/4/2020, 10:37:45 AM	Core Directory	GroupManagement	Remove member from gr...	Success		bhymer@titancorp.net, 01...	Microsoft Teams Services
9/4/2020, 10:37:36 AM	Core Directory	GroupManagement	Update group	Success		Development Processes	Office 365 SharePoint Onl...
9/4/2020, 10:37:35 AM	Core Directory	GroupManagement	Update group	Success		Development Processes	Office 365 SharePoint Onl...
9/4/2020, 10:37:30 AM	Core Directory	GroupManagement	Add member to group	Success		bhymer@titancorp.net, 01...	Microsoft Teams Services
9/4/2020, 10:37:14 AM	Core Directory	GroupManagement	Update group	Success		Development Processes	Office 365 SharePoint Onl...
9/4/2020, 10:37:13 AM	Core Directory	GroupManagement	Update group	Success		Development Processes	Office 365 Exchange Online
9/4/2020, 10:37:13 AM	Core Directory	GroupManagement	Update group	Success		Development Processes	Office 365 Exchange Online
9/4/2020, 10:37:07 AM	Core Directory	GroupManagement	Add owner to group	Success		iLindsay@titancorp.net, 0...	Microsoft Teams Services
9/4/2020, 10:37:07 AM	Core Directory	GroupManagement	Add member to group	Success		iLindsay@titancorp.net, 0...	Microsoft Teams Services
9/4/2020, 10:37:07 AM	Core Directory	GroupManagement	Add group	Success		Development Processes	Microsoft Teams Services

Figure 21. Group creation, deletion and change events in the Azure Audit Log



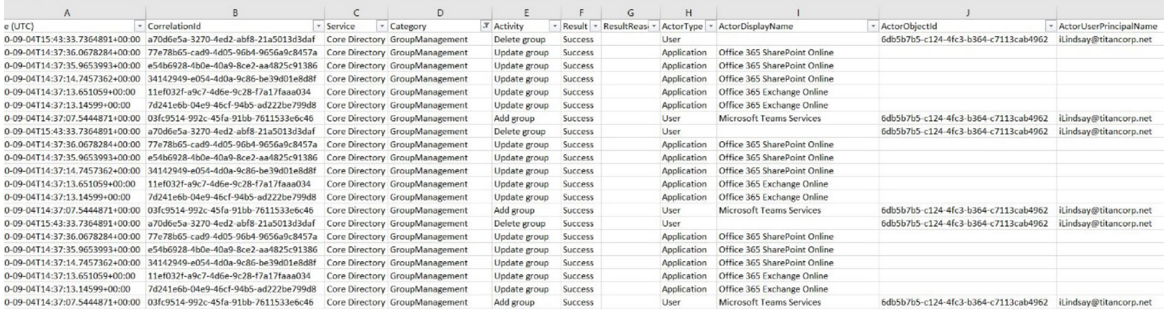
Home > TitanCorp

TitanCorp | Audit logs
Azure Active Directory

Date : **Last 24 hours** | Show dates as: **Local** | Service : **All** | Category : **GroupManagement** | Activity : **All**

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
9/4/2020, 11:43:33 AM	Core Directory	GroupManagement	Delete group	Success		Development Processes	iLindsay@titancorp.net
9/4/2020, 11:40:40 AM	Core Directory	GroupManagement	Update group	Success		Chicago	Sync_AZADCON_27faa9d...
9/4/2020, 11:10:59 AM	Core Directory	GroupManagement	Add member to group	Success		TheoEpstein@Titancorp.n...	Microsoft Approval Mana...

Figure 22. Determining who deleted a group using the Azure Audit Log



A	B	C	D	E	F	G	H	I	J	
e (UTC)	CorrelationId	Service	Category	Activity	Result	ResultReas	ActorType	ActorDisplayName	ActorObjectId	ActorUserPrincipalName
0-09-04T15:43:33.7364891+00:00	a70d6e5a-3270-4ed2-abf8-21a5013d3daf	Core Directory	GroupManagement	Delete group	Success		User		6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net
0-09-04T14:37:36.0678284+00:00	77e78b65-cad9-4d05-96b4-9656a9c8457a	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:35.9653993+00:00	e54b6928-4b0e-40a9-8ce2-aa4825c91386	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:14.7457362+00:00	34142949-e054-4d0a-9c86-be39d01e8d8f	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:13.651059+00:00	11ef032f-a9c7-4d6e-9c28-f7a17faaa034	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:13.14599+00:00	7d241e6b-04e9-46cf-94b5-ad222be799d8	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:07.5444871+00:00	03fc9514-992c-45fa-91bb-7611533e6c46	Core Directory	GroupManagement	Add group	Success		User	Microsoft Teams Services	6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net
0-09-04T15:43:33.7364891+00:00	a70d6e5a-3270-4ed2-abf8-21a5013d3daf	Core Directory	GroupManagement	Delete group	Success		User		6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net
0-09-04T14:37:36.0678284+00:00	77e78b65-cad9-4d05-96b4-9656a9c8457a	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:35.9653993+00:00	e54b6928-4b0e-40a9-8ce2-aa4825c91386	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:14.7457362+00:00	34142949-e054-4d0a-9c86-be39d01e8d8f	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:13.651059+00:00	11ef032f-a9c7-4d6e-9c28-f7a17faaa034	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:13.14599+00:00	7d241e6b-04e9-46cf-94b5-ad222be799d8	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:07.5444871+00:00	03fc9514-992c-45fa-91bb-7611533e6c46	Core Directory	GroupManagement	Add group	Success		User	Microsoft Teams Services	6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net
0-09-04T15:43:33.7364891+00:00	a70d6e5a-3270-4ed2-abf8-21a5013d3daf	Core Directory	GroupManagement	Delete group	Success		User		6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net
0-09-04T14:37:36.0678284+00:00	77e78b65-cad9-4d05-96b4-9656a9c8457a	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:35.9653993+00:00	e54b6928-4b0e-40a9-8ce2-aa4825c91386	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:14.7457362+00:00	34142949-e054-4d0a-9c86-be39d01e8d8f	Core Directory	GroupManagement	Update group	Success		Application	Office 365 SharePoint Online		
0-09-04T14:37:13.651059+00:00	11ef032f-a9c7-4d6e-9c28-f7a17faaa034	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:13.14599+00:00	7d241e6b-04e9-46cf-94b5-ad222be799d8	Core Directory	GroupManagement	Update group	Success		Application	Office 365 Exchange Online		
0-09-04T14:37:07.5444871+00:00	03fc9514-992c-45fa-91bb-7611533e6c46	Core Directory	GroupManagement	Add group	Success		User	Microsoft Teams Services	6db5b7b5-c124-4fc3-b364-c7113cab4962	iLindsay@titancorp.net

Figure 23. Azure Audit Log events in Excel

> If an admin deletes the Microsoft 365 group for a team, a user who tries to add a user to the team will get a cryptic error.

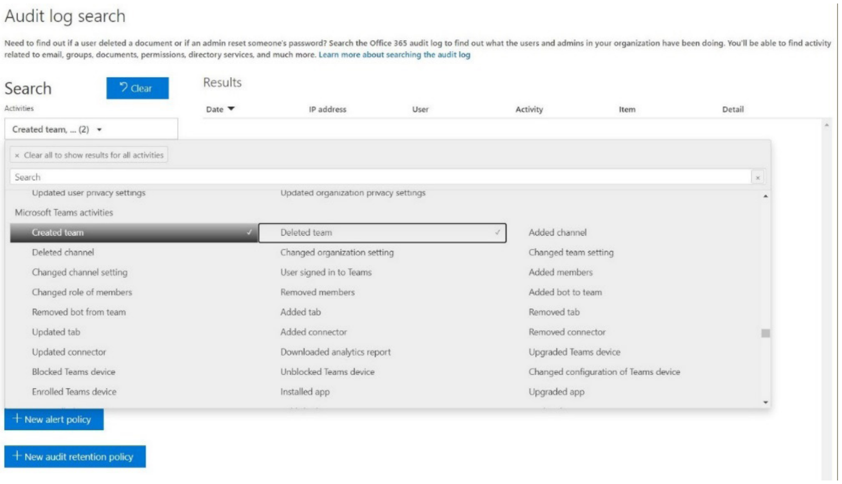
To find changes that were not made through the Teams interface, you will need to look for the group directly. For instance, if an Microsoft 365 group was deleted outside of Teams, you would need to look for the group name in the **Targets** field to determine who deleted the group (see Figure 22).

You can download the data in either CSV or JSON format. (Unless you are a programmer with experience working with JSON files, CSV download is recommended.) For example, Figure 23 shows a log that was downloaded in CSV format, opened in Excel, and filtered to **Category** = **GroupManagement** and **ActorDisplayName** = **Microsoft Teams Service**. The column **Target1DisplayName** shows the names of the groups that were added, deleted or modified.

FINDING TEAMS IN THE UNIFIED AUDIT LOG

Information about the addition and deletion of teams can be gathered from a search of the Unified Audit Log through the Office 365 Security & Compliance Center. These searches run against the logs of Azure AD, plus the logs of all Office 365 tools, as described above, so they may take longer than searches against the Azure Audit Log alone. There can also be a delay of 15 minutes or more until the entries appear in the log. When a team is deleted, It could take over a day for the deletion of the associated Microsoft 365 group to show up in the log.

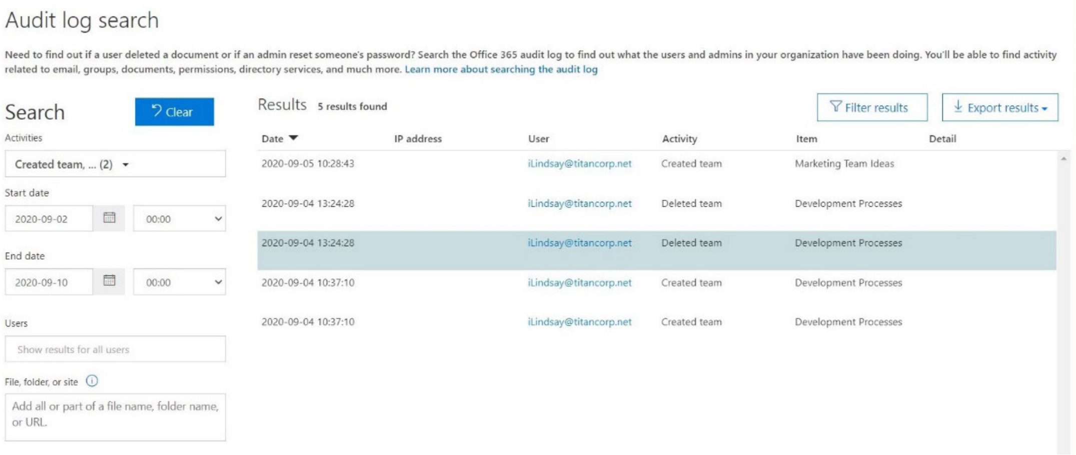
Filters can be set to look for new users added in a given date range, which is an advantage over searching the Azure Audit Log. You can also filter for created teams, deleted teams or various changes in group membership (see Figure 24). Figure 25 shows the log filtered to show just the teams that were added or deleted during a particular date range. Note that there is no way to distinguish a team that was deleted by the Microsoft 365 group being deleted from a team that was deleted by an owner in the Teams interface.



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Figure 24. Unified Audit Log search filters



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Created team, ... (2)

Start date: 2020-09-02 00:00

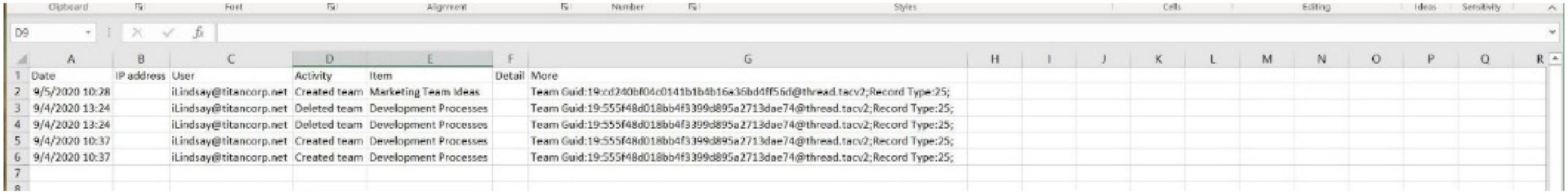
End date: 2020-09-10 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Date	IP address	User	Activity	Item	Detail
2020-09-05 10:28:43		iLindsay@titancorp.net	Created team	Marketing Team Ideas	
2020-09-04 13:24:28		iLindsay@titancorp.net	Deleted team	Development Processes	
2020-09-04 13:24:28		iLindsay@titancorp.net	Deleted team	Development Processes	
2020-09-04 10:37:10		iLindsay@titancorp.net	Created team	Development Processes	
2020-09-04 10:37:10		iLindsay@titancorp.net	Created team	Development Processes	

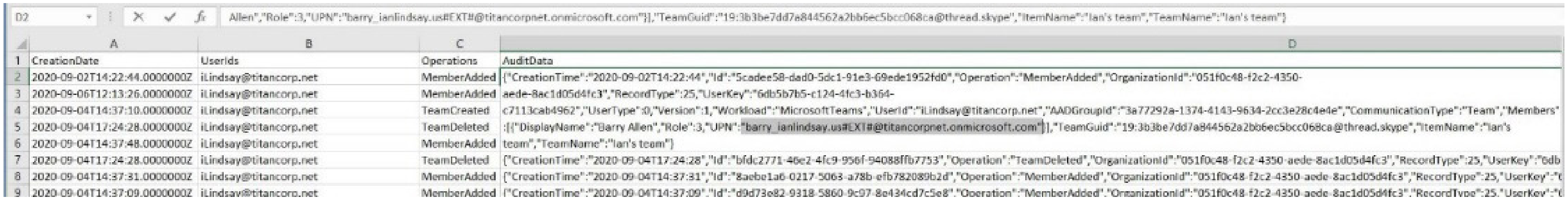
Figure 25. Unified Audit Log filtered



	A	B	C	D	E	F	G
1	Date	IP address	User	Activity	Item	Detail	More
2	9/5/2020 10:28		iLindsay@titancorp.net	Created team	Marketing Team Ideas		Team Guid:19:cd240bf04c0141b1b4b16a36bd4ff56d@thread.tacv2;Record Type:25;
3	9/4/2020 13:24		iLindsay@titancorp.net	Deleted team	Development Processes		Team Guid:19:555f48d018bb4f3399d895a2713dae74@thread.tacv2;Record Type:25;
4	9/4/2020 13:24		iLindsay@titancorp.net	Deleted team	Development Processes		Team Guid:19:555f48d018bb4f3399d895a2713dae74@thread.tacv2;Record Type:25;
5	9/4/2020 10:37		iLindsay@titancorp.net	Created team	Development Processes		Team Guid:19:555f48d018bb4f3399d895a2713dae74@thread.tacv2;Record Type:25;
6	9/4/2020 10:37		iLindsay@titancorp.net	Created team	Development Processes		Team Guid:19:555f48d018bb4f3399d895a2713dae74@thread.tacv2;Record Type:25;
7							
8							

Figure 26. Search results viewed in Microsoft Excel

Again, you have two options for exporting the data to a tool like Excel: **Save loaded results** and **Download all results**. If you choose the former, the JSON information is not included (see Figure 26). If you just need to see data on teams being added and deleted, this export option will give you all the information you need.

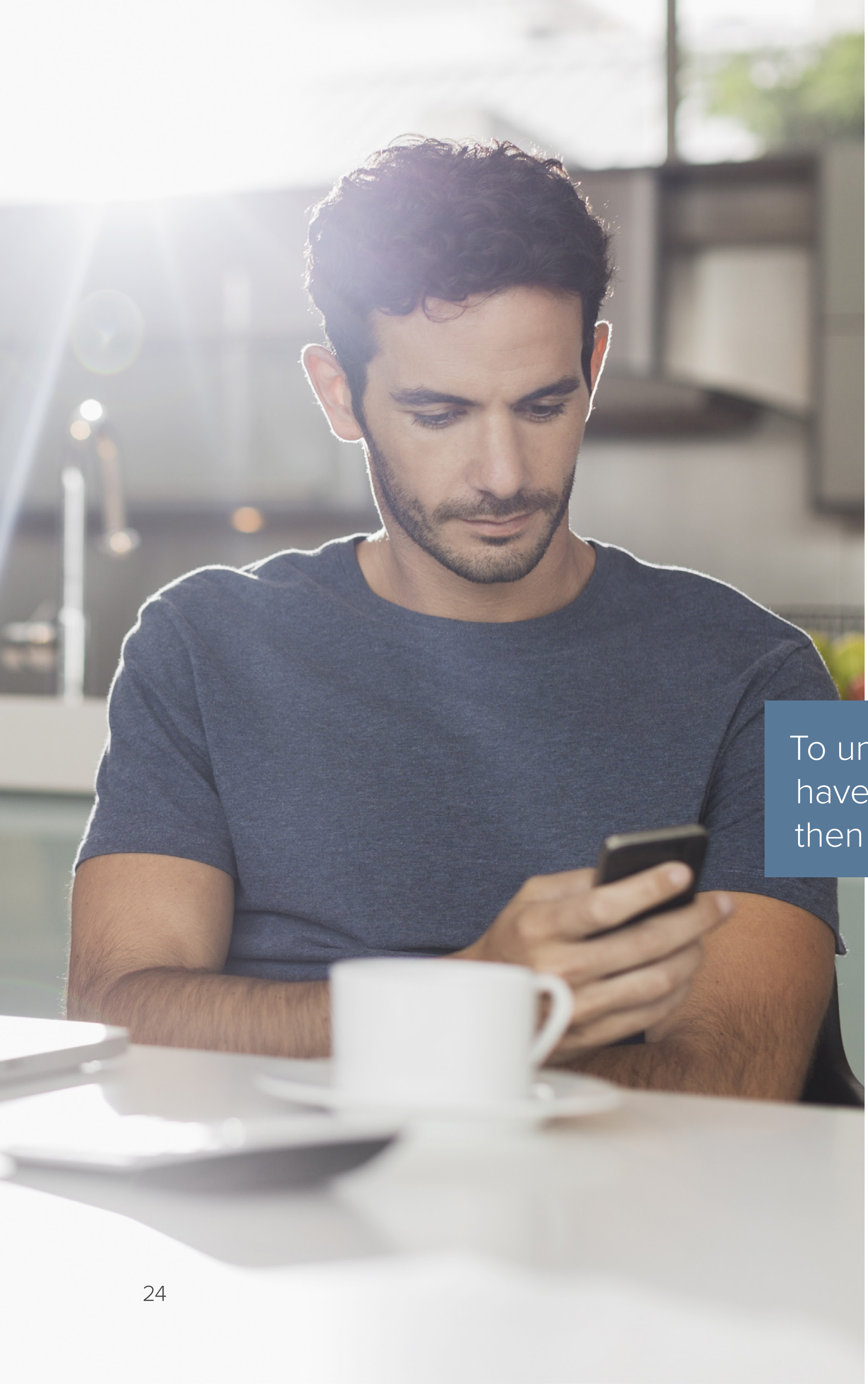


Allen","Role":3,"UPN":"barry_ianlindsay.us#EXT#@titancorpnet.onmicrosoft.com"}],"TeamGuid":"19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype","ItemName":"Ian's team","TeamName":"Ian's team"}

	A	B	C	D
1	CreationDate	UserIds	Operations	AuditData
2	2020-09-02T14:22:44.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-02T14:22:44","Id":"5cadee58-dad0-5dc1-91e3-69ede1952fd0","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-
3	2020-09-06T12:13:26.0000000Z	iLindsay@titancorp.net	MemberAdded	aede-8ac1d05d4fc3","RecordType":25,"UserKey":"6db5b7b5-c124-4fc3-b364-
4	2020-09-04T14:37:10.0000000Z	iLindsay@titancorp.net	TeamCreated	c7113cab4962","UserType":0,"Version":1,"Workload":"MicrosoftTeams","UserId":"iLindsay@titancorp.net","AADGroupId":"3a77292a-1374-4143-9634-2cc3e28c4e4e","CommunicationType":"Team","Members"
5	2020-09-04T17:24:28.0000000Z	iLindsay@titancorp.net	TeamDeleted	:[{"DisplayName":"Barry Allen","Role":3,"UPN":"barry_ianlindsay.us#EXT#@titancorpnet.onmicrosoft.com"}],"TeamGuid":"19:3b3be7dd7a844562a2bb6ec5bcc068ca@thread.skype","ItemName":"Ian's
6	2020-09-04T14:37:48.0000000Z	iLindsay@titancorp.net	MemberAdded	team","TeamName":"Ian's team"}
7	2020-09-04T17:24:28.0000000Z	iLindsay@titancorp.net	TeamDeleted	{"CreationTime":"2020-09-04T17:24:28","Id":"bfdc2771-46e2-4fc9-956f-94088ffb7753","Operation":"TeamDeleted","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"6db
8	2020-09-04T14:37:31.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-04T14:37:31","Id":"8aebe1a6-0217-5063-a78b-efb782089b2d","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"(
9	2020-09-04T14:37:09.0000000Z	iLindsay@titancorp.net	MemberAdded	{"CreationTime":"2020-09-04T14:37:09","Id":"d9d73e82-9318-5860-9c07-8e434cd7c5e8","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"(

Figure 27. Search results viewed in Microsoft Excel

If you also want information on changes to the groups, select the **Download all results** option. The entire audit detail is in one embedded JSON in the **AuditData** column (see Figure 27), so it is difficult to filter for the modified groups.



8. Forwarding of inbound email messages

By itself, forwarding inbound email to other addressees is neither good nor bad. Recipients may need to share information in a message with outside vendors or customers. On-site consultants and contractors may prefer to forward messages and consolidate all their email in a single account. Users can manually forward email, and automatic forwarding can be set up on a mailbox by a user (through ForwardSMTP) or an administrator (through ForwardAlias).

Automatic forwarding could be perfectly innocuous, but smart administrators keep an eye on changes that involve email forwarding to thwart changes that suggest malicious activity.

> To uncover changes to email forwarding, you have to first export the native audit log and then search for the desired events.

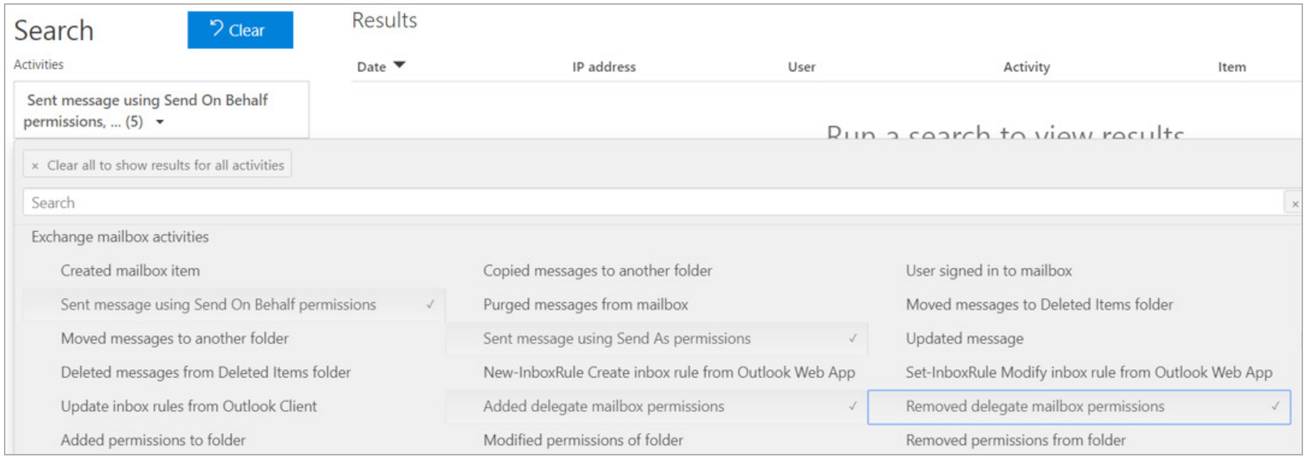
Unfortunately, the audit logs in Azure Active Directory and Office 365 do not allow for direct searches on those changes. Instead, it is necessary to export the entire log of changes in Exchange Online to a CSV file, and then search the exported audit events with {**"name":"DeliverToMailboxAndForward","value":"True"**} in the **Parameters** field of the audit detail to return the desired events.

9. Non-owner email activity

Non-owner email activity is common in large organizations, since administrative assistants often need access to the email accounts of the executives they support, or multiple employees monitor shared mailboxes, such as customer support mailboxes. However, a non-owner can misuse their privileges, and if their account is compromised, an attacker can obtain access to sensitive information.

In addition, Exchange Online administrators can perform almost any action — including granting themselves access to look in executives' mailboxes. While every organization trusts its administrators to manage and maintain systems, it must also keep an eye out for rogue activity.

> If an executive assistant's account is compromised, an attacker could gain access to your CEO's mailbox.



Sent message using Send On Behalf permissions, ... (5)

Run a search to view results

× Clear all to show results for all activities

Search

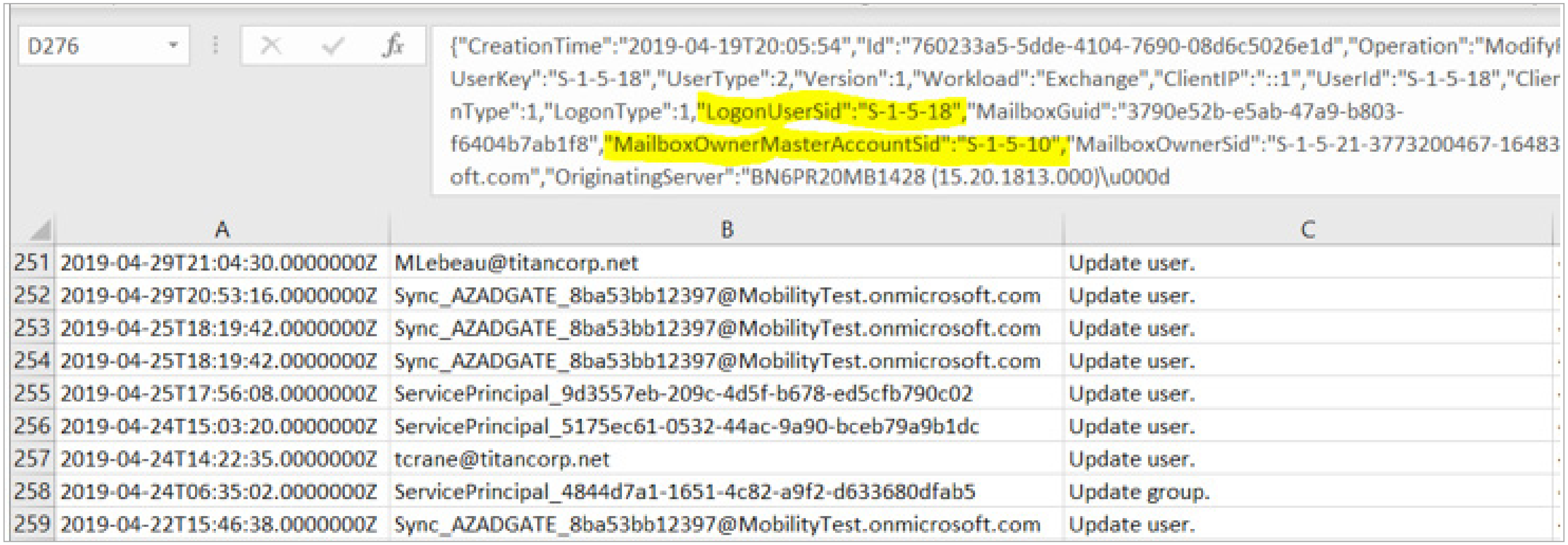
Exchange mailbox activities

Created mailbox item
Sent message using Send On Behalf permissions ✓
Moved messages to another folder
Deleted messages from Deleted Items folder
Update inbox rules from Outlook Client
Added permissions to folder

Copied messages to another folder
Purged messages from mailbox
Sent message using Send As permissions ✓
New-InboxRule Create inbox rule from Outlook Web App
Added delegate mailbox permissions ✓
Modified permissions of folder

User signed in to mailbox
Moved messages to Deleted Items folder
Updated message
Set-InboxRule Modify inbox rule from Outlook Web App
Removed delegate mailbox permissions ✓
Removed permissions from folder

Figure 28: Non-owner email activity listed in Unified Audit Log



```
{"CreationTime":"2019-04-19T20:05:54","Id":"760233a5-5dde-4104-7690-08d6c5026e1d","Operation":"Modifyl
UserKey":"S-1-5-18","UserType":2,"Version":1,"Workload":"Exchange","ClientIP":"::1","UserId":"S-1-5-18","Clier
nType":1,"LogonType":1,"LogonUserSid":"S-1-5-18","MailboxGuid":"3790e52b-e5ab-47a9-b803-
f6404b7ab1f8","MailboxOwnerMasterAccountSid":"S-1-5-10","MailboxOwnerSid":"S-1-5-21-3773200467-16483
oft.com","OriginatingServer":"BN6PR20MB1428 (15.20.1813.000)\u000d
```

	A	B	C
251	2019-04-29T21:04:30.0000000Z	MLebeau@titancorp.net	Update user.
252	2019-04-29T20:53:16.0000000Z	Sync_AZADGATE_8ba53bb12397@MobilityTest.onmicrosoft.com	Update user.
253	2019-04-25T18:19:42.0000000Z	Sync_AZADGATE_8ba53bb12397@MobilityTest.onmicrosoft.com	Update user.
254	2019-04-25T18:19:42.0000000Z	Sync_AZADGATE_8ba53bb12397@MobilityTest.onmicrosoft.com	Update user.
255	2019-04-25T17:56:08.0000000Z	ServicePrincipal_9d3557eb-209c-4d5f-b678-ed5cfb790c02	Update user.
256	2019-04-24T15:03:20.0000000Z	ServicePrincipal_5175ec61-0532-44ac-9a90-bceb79a9b1dc	Update user.
257	2019-04-24T14:22:35.0000000Z	tcrane@titancorp.net	Update user.
258	2019-04-24T06:35:02.0000000Z	ServicePrincipal_4844d7a1-1651-4c82-a9f2-d633680dfab5	Update group.
259	2019-04-22T15:46:38.0000000Z	Sync_AZADGATE_8ba53bb12397@MobilityTest.onmicrosoft.com	Update user.

Figure 29: Detail of AuditData column

FINDING NON-OWNER EMAIL ACTIVITY IN THE UNIFIED AUDIT LOG

Information on non-owner activity is available only in the Unified Audit Log, as shown in Figure 28. You can review the most common types of non-owner events by including the following options:

- Sent message using Send On Behalf permission
- Added or removed user with delegate access to calendar/folder
- Sent message using Send As permission
- Added delegate mailbox permission
- Removed delegate mailbox permission

Note, however, that this will not include many important actions, such as adding, deleting or moving folders or messages, and changing some permissions, to name a few.

To perform an exhaustive search, you need to query all mailbox activities and export the results as a spreadsheet. But the next step — finding audit events where **LogonUserSid** does not match **MailboxOwnerMasterSid** — is labor-intensive because the information is embedded in the **AuditData** column with the rest of the information from the event (see Figure 29).[2]

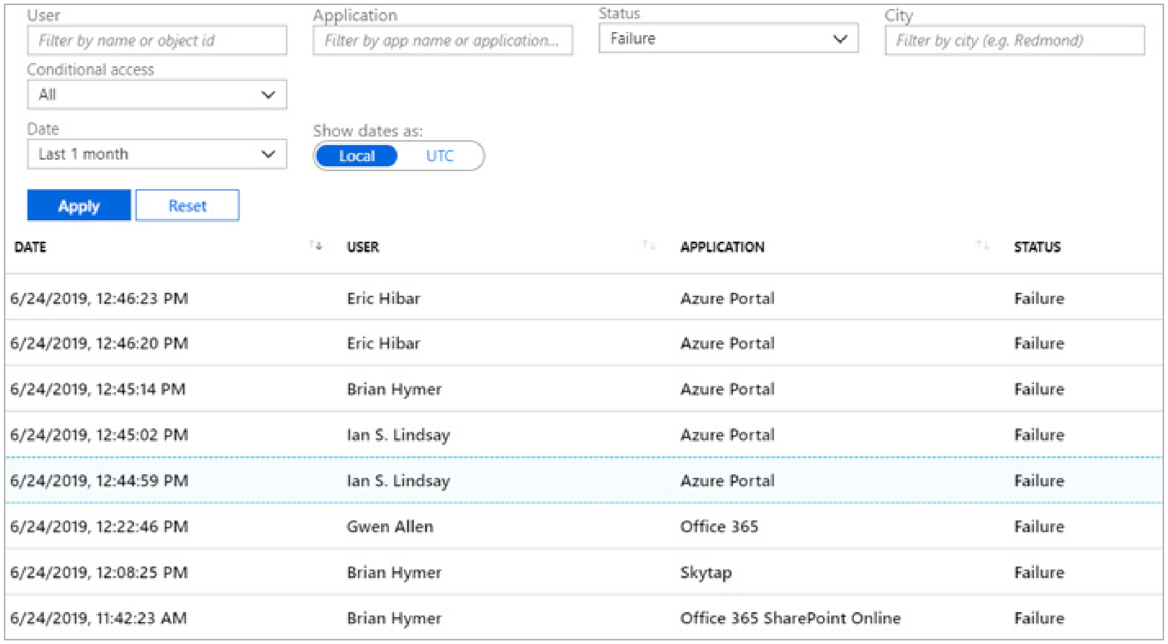
[2] See also "Auditing Privileged Operations and Mailbox Access in Office 365 Exchange Online," https://www.quest.com/whitepaper/auditing-privileged-operations-and-mailbox-access-in-office-3658121801/.

10. Failed sign-in attempts

Tracking failed sign-in attempts is a crucial part of an administrator's job. Lockouts frustrate users, who rarely know why they have been locked out; hybrid environments exacerbate the problem by adding another potential source of lockouts. And repeated failed sign-in attempts can indicate an attacker attempting to discover user passwords by brute force.

On premises, information about failed login events is stored in the security logs on all domain controllers. In the cloud, the information is in the audit events of each Azure tenants. To see the failed sign-in events for a tenant, go to the Sign-ins screen under **Monitoring** and search on **Failure**, as shown in Figure 30.

Of course, simply gathering all the failed sign-in events is only the start. The next task is to analyze all the information for patterns that indicate malicious activity. This task is not easy, due to the lack of detail in the search results.


User
Filter by name or object id
Application
Filter by app name or application...
City
Filter by city (e.g. Redmond)
Show dates as:
Local
UTC
Apply
Reset

Status: Failure

Conditional access: All

Date: Last 1 month

DATE	USER	APPLICATION	STATUS
6/24/2019, 12:46:23 PM	Eric Hibar	Azure Portal	Failure
6/24/2019, 12:46:20 PM	Eric Hibar	Azure Portal	Failure
6/24/2019, 12:45:14 PM	Brian Hymer	Azure Portal	Failure
6/24/2019, 12:45:02 PM	Ian S. Lindsay	Azure Portal	Failure
6/24/2019, 12:44:59 PM	Ian S. Lindsay	Azure Portal	Failure
6/24/2019, 12:22:46 PM	Gwen Allen	Office 365	Failure
6/24/2019, 12:08:25 PM	Brian Hymer	Skytap	Failure
6/24/2019, 11:42:23 AM	Brian Hymer	Office 365 SharePoint Online	Failure

Figure 30. Search on failed sign-ins in Azure AD

Repeated failed sign-in attempts can indicate malicious actors attempting to discover user passwords by brute force.

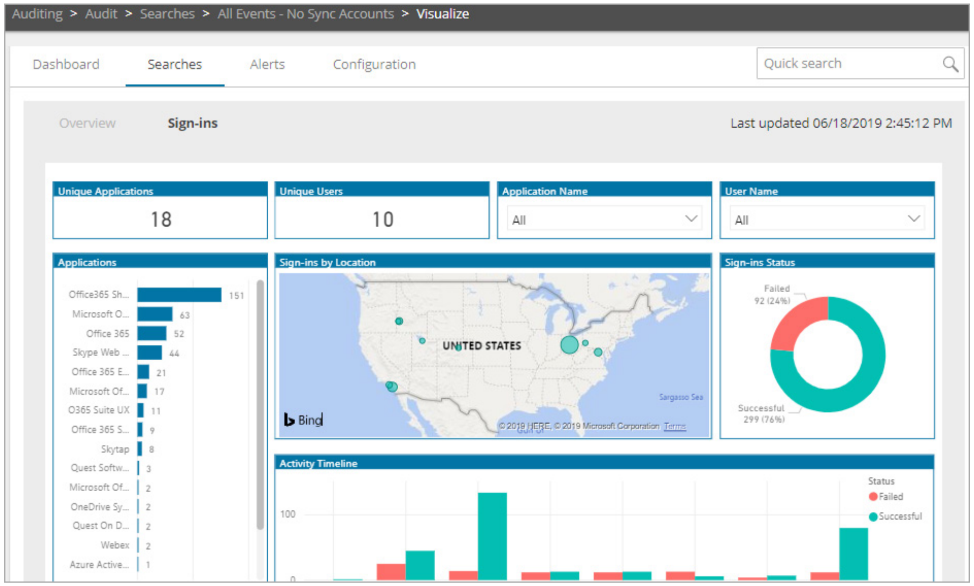
On Demand Audit from Quest

What if you didn't have to fly blind, struggling with all the shortcomings of the native auditing tools for Office 365 and Azure?

On Demand Audit Hybrid Suite for Office 365 by Quest provides a single hosted view of user activity across hybrid Microsoft environments. It exposes all changes taking place, whether in on-premises AD, Azure AD, or Office 365 workloads such as Exchange Online, SharePoint Online, OneDrive for Business and Teams. Instead of combing through partial peeks at cryptic audit logs, you can use responsive search across years of data to investigate and report on events, all from a single window. You can generate reports through interactive data visualizations, as shown in Figure 31.

Moreover, On Demand Audit Hybrid Suite provides granular delegated access, so you can safely empower users to get the insights they need without making any configuration changes or setting up additional infrastructure. In just a few clicks, you can give your security and compliance teams, helpdesk staff, IT managers and even external auditors and partners exactly the reports they need and nothing more.

For more information, visit quest.com/on-demand.



Last updated 06/18/2019 2:45:12 PM

Unique Applications: 18

Unique Users: 10

Application Name: All

User Name: All

Applications	
Office365 Sh...	151
Microsoft O...	63
Office 365	52
Skype Web ...	44
Office 365 E...	21
Microsoft Of...	17
O365 Suite UX	11
Office 365 S...	9
Skytap	8
Quest Softw...	3
Microsoft Of...	2
OneDrive Sy...	2
Quest On D...	2
Webex	2
Azure Active...	1

Figure 31: Audit and investigate changes across your on-prem and cloud environments with On Demand Audit Hybrid Suite for Office 365.

> Get clear, actionable insight into changes across your on-prem AD, Azure AD and Office 365 workloads from a single console with On Demand Audit Hybrid Suite.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks