Quest Platform Management Virtual Summit 2020

Office 365 and Azure AD Security Events to Monitor During the COVID-19 Crisis

Speaker: Geir Aasen

Strategic SC, Microsoft Platform Management

Quest

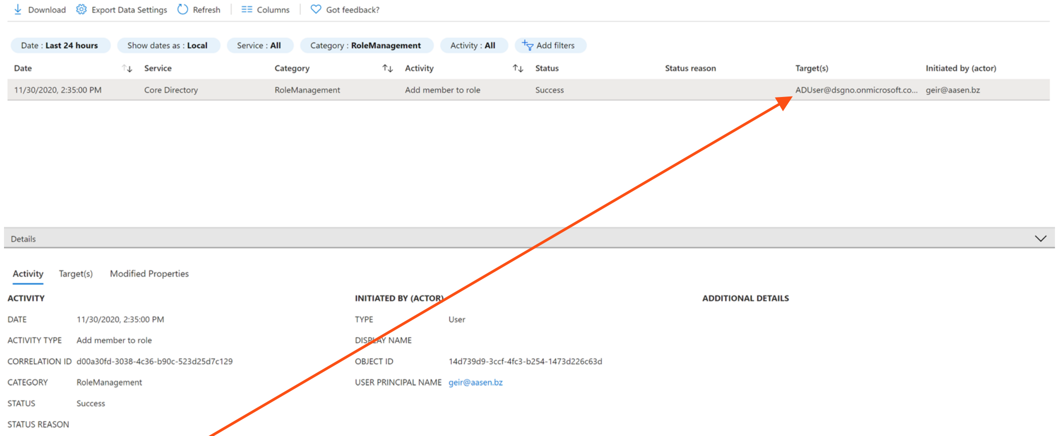
Where Next Meets Now.

1. Changes to important roles

- Make sure all important/privileged role changes are monitored.
- Track changes to Azure AD groups that are linked to Azure AD Roles (public preview per Nov 2020).
- And make sure to include monitoring of the OnPrem AD groups to control role membership when Microsoft make this feature available
- OnPrem AD Privileged groups such as Domain Admins, Account Operators etc

1. Changes to important roles

Azure AD audit log



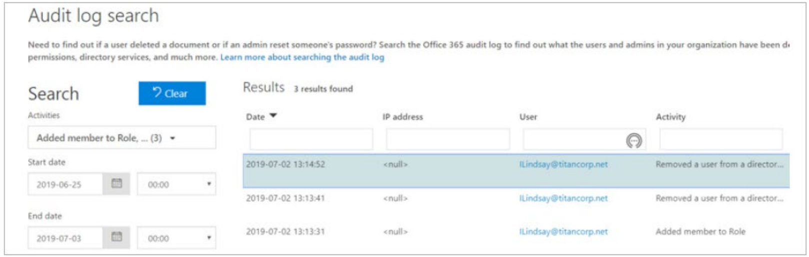
Date : **Last 24 hours** | Show dates as : **Local** | Service : **All** | Category : **RoleManagement** | Activity : **All** | Add filters

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
11/30/2020, 2:35:00 PM	Core Directory	RoleManagement	Add member to role	Success		ADUser@dsgno.onmicrosoft.co...	geir@aasen.bz

Details

ACTIVITY		INITIATED BY (ACTOR)		ADDITIONAL DETAILS
DATE	11/30/2020, 2:35:00 PM	TYPE	User	
ACTIVITY TYPE	Add member to role	DISPLAY NAME		
CORRELATION ID	d00a30fd-3038-4c36-b90c-523d25d7c129	OBJECT ID	14d739d9-3ccf-4fc3-b254-1473d226c63d	
CATEGORY	RoleManagement	USER PRINCIPAL NAME	geir@aasen.bz	
STATUS	Success			
STATUS REASON				

Unified Audit log



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)

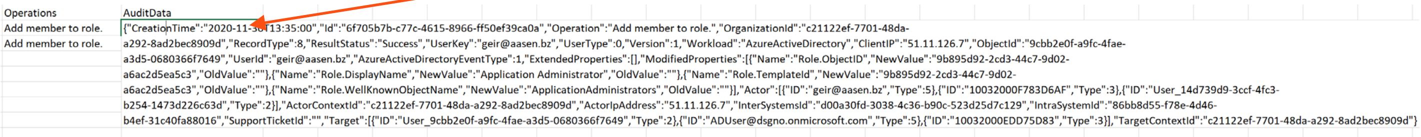
Start date: 2019-06-25 00:00

End date: 2019-07-03 00:00

Results 3 results found

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

Export to CSV or JSON



Operations
Add member to role.
Add member to role.

AuditData

```
{"CreationTime":"2020-11-30T13:35:00","Id":"6f705b7b-c77c-4615-8966-ff50ef39ca0a","Operation":"Add member to role.","OrganizationId":"c21122ef-7701-48da-
a292-8ad2bec8909d","RecordType":8,"ResultStatus":"Success","UserKey":"geir@aasen.bz","UserType":0,"Version":1,"Workload":"AzureActiveDirectory","ClientIP":"51.11.126.7","ObjectId":"9cbb2e0f-a9fc-4fae-
a3d5-0680366f7649","UserId":"geir@aasen.bz","AzureActiveDirectoryEventType":1,"ExtendedProperties":[],"ModifiedProperties":[{"Name":"Role.ObjectID","NewValue":"9b895d92-2cd3-44c7-9d02-
a6ac2d5ea5c3","OldValue":""},{"Name":"Role.DisplayName","NewValue":"Application Administrator","OldValue":""},{"Name":"Role.TemplateId","NewValue":"9b895d92-2cd3-44c7-9d02-
a6ac2d5ea5c3","OldValue":""},{"Name":"Role.WellKnownObjectName","NewValue":"ApplicationAdministrators","OldValue":""}],"Actor":[{"ID":"geir@aasen.bz","Type":5},{"ID":"10032000F783D6AF","Type":3},{"ID":"User_14d739d9-3ccf-4fc3-
b254-1473d226c63d","Type":2}],"ActorContextId":"c21122ef-7701-48da-a292-8ad2bec8909d","ActorIpAddress":"51.11.126.7","InterSystemsId":"d00a30fd-3038-4c36-b90c-523d25d7c129","IntraSystemId":"86bb8d55-f78e-4d46-
b4ef-31c40fa88016","SupportTicketId":"","Target":[{"ID":"User_9cbb2e0f-a9fc-4fae-a3d5-0680366f7649","Type":2},{"ID":"ADUser@dsgno.onmicrosoft.com","Type":5},{"ID":"10032000EDD75D83","Type":3}],"TargetContextId":"c21122ef-7701-48da-a292-8ad2bec8909d"}
```

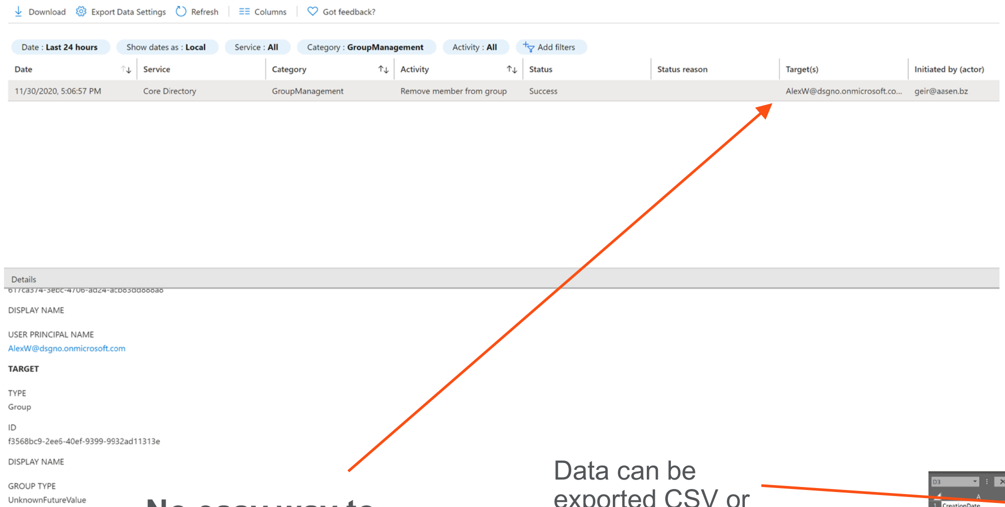
No easy way to filter out and focus on only the roles you want to audit

2. Changes to groups

- Groups are a familiar concept for granting access in the OnPrem world
- New group types were introduced, such as Microsoft 365 groups which can control access to valuable data
- Azure B2B makes it possible to include external parties in groups, such as customers and vendors
- Dont forget to monitor your Hybrid AD Security groups, since access to sensitive data in the cloud can be initiated from OnPrem AD

2. Changes to groups

Azure AD audit log



Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
11/30/2020, 5:06:57 PM	Core Directory	GroupManagement	Remove member from group	Success		AlexW@dsgno.onmicrosoft.co...	geir@aasen.bz

Details

617ca374-3ebc-4706-ad24-acb83dd888a8

DISPLAY NAME

USER PRINCIPAL NAME
AlexW@dsgno.onmicrosoft.com

TARGET

TYPE
Group

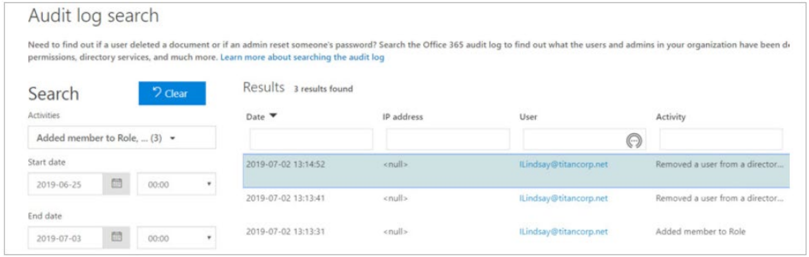
ID
f3568bc9-2ee6-40ef-9399-9932ad11313e

DISPLAY NAME

GROUP TYPE
UnknownFutureValue

No easy way to filter out and focus on only the group you want to audit

Unified Audit log



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

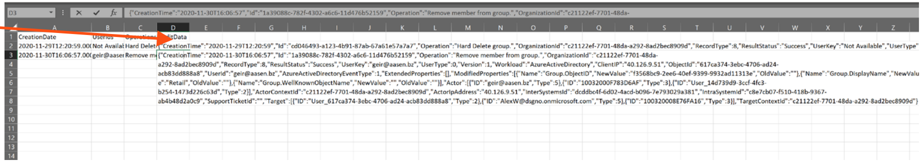
End date: 2019-07-03 00:00

Results 3 results found

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

Data can be exported CSV or JSON but difficult to filter

Export to CSV or JSON



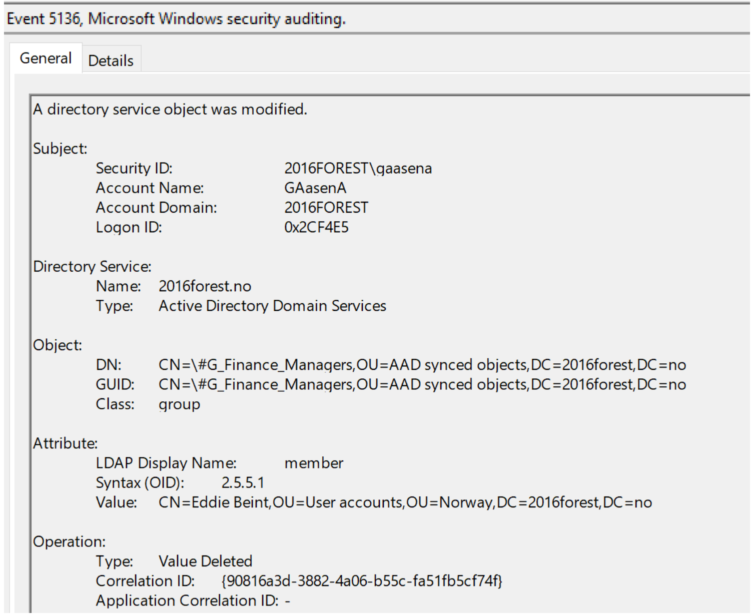
```
D3   {"CreationTime":"2020-11-30T16:06:57","Id":"1a39088c-782f-4302-a6c6-11d476b52159","Operation":"Remove member from group.","OrganizationId":"c21122ef-7701-48da-

1  CreationDate              UserIds     Operations  AuditData
2  2020-11-29T12:20:59.00(  Not Availal Hard Delet  {"CreationTime":"2020-11-29T12:20:59","Id":"cd046493-a123-4b91-87ab-67a61e57a7a7","Operation":"Hard Delete group.","OrganizationId":"c21122ef-7701-48da-a292-8ad2bec8909d","RecordType":8,"ResultStatus":"Success","UserKey":"Not Available","UserType"
3  2020-11-30T16:06:57.00(  geir@aaser  Remove m    {"CreationTime":"2020-11-30T16:06:57","Id":"1a39088c-782f-4302-a6c6-11d476b52159","Operation":"Remove member from group.","OrganizationId":"c21122ef-7701-48da-
                                                    a292-8ad2bec8909d","RecordType":8,"ResultStatus":"Success","UserKey":"geir@aasen.bz","UserType":0,"Version":1,"Workload":"AzureActiveDirectory","ClientIP":"40.126.9.51","ObjectId":"617ca374-3ebc-4706-ad24-
                                                    acb83dd888a8","UserId":"geir@aasen.bz","AzureActiveDirectoryEventType":1,"ExtendedProperties":[],"ModifiedProperties":[{"Name":"Group.ObjectID","NewValue":"f3568bc9-2ee6-40ef-9399-9932ad11313e","OldValue":""},{"Name":"Group.DisplayName","NewValu
                                                    e":"Retail","OldValue":""},{"Name":"Group.WellKnownObjectName","NewValue":"","OldValue":""}],"Actor":[{"ID":"geir@aasen.bz","Type":5},{"ID":"10032000F783D6AF","Type":3},{"ID":"User_14d739d9-3ccf-4fc3-
                                                    b254-1473d226c63d","Type":2}],"ActorContextId":"c21122ef-7701-48da-a292-8ad2bec8909d","ActorIpAddress":"40.126.9.51","InterSystemsId":"dcddbc4f-6d02-4acd-b096-7e793029a381","IntraSystemId":"c8e7cb07-f510-418b-9367-
                                                    ab4b48d2a0c9","SupportTicketId":"","Target":[{"ID":"User_617ca374-3ebc-4706-ad24-acb83dd888a8","Type":2},{"ID":"AlexW@dsgno.onmicrosoft.com","Type":5},{"ID":"100320008E76FA16","Type":3}],"TargetContextId":"c21122ef-7701-48da-a292-8ad2bec8909d"}
```

Quest

Where Next Meets Now.

2. Changes to groups

OnPrem synced group from domain controller security log



```
A directory service object was modified.

Subject:
        Security ID:            2016FOREST\gaasena
        Account Name:           GAasenA
        Account Domain:         2016FOREST
        Logon ID:               0x2CF4E5

Directory Service:
        Name:   2016forest.no
        Type:   Active Directory Domain Services

Object:
        DN:     CN=\#G_Finance_Managers,OU=AAD synced objects,DC=2016forest,DC=no
        GUID:   CN=\#G_Finance_Managers,OU=AAD synced objects,DC=2016forest,DC=no
        Class:  group

Attribute:
        LDAP Display Name:      member
        Syntax (OID):   2.5.5.1
        Value:  CN=Eddie Beint,OU=User accounts,OU=Norway,DC=2016forest,DC=no

Operation:
        Type:   Value Deleted
        Correlation ID:     {90816a3d-3882-4a06-b55c-fa51fb5cf74f}
        Application Correlation ID: -
```

Make sure you get audit events from all DCs and understand who changed what from where and when

3. Changes to applications

- **Azure AD Enterprise Applications are critical resources, changes can break the apps and have negative impact on the organisation**
- **Track and analyse changes to these critical Azure AD objects both the Application and the Service Principal**
- **This requires multiple searches in the Azure AD Audit log, both in ApplicationManagement and UserManagement categories, under UserManagement you need to include these activities :**
  - Add app role assignment to user
  - Create application password for user
  - Delete application password for user
  - Remove app role assignment from user
  - Review app assignment

4. Resource creation

- Monitor the creation of resources. Resources are also created non-explicitly such as when creating a Team, many other resources are created such as mailbox, Sharepoint site and a Onenote notebook
- Track type and number of resources that get created in Azure, to maintain control and ensure they are created according to policy
- The Unified Audit log can be used here, however it requires multiple queries and exports to get a complete view across all workloads

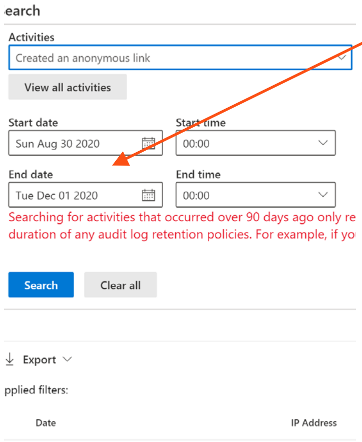
5. Sharing of important files and anonymous links

- Sharepoint Online and Onedrive introduced new risk around data sharing
- Anonymous sharing
- B2B Guest external access unawareness

5. Sharing of important files and anonymous links

Unified Audit log

These events can be very interesting to look at more than 90 days back



earch

Activities

Created an anonymous link

View all activities

Start date: Sun Aug 30 2020

Start time: 00:00

End date: Tue Dec 01 2020

End time: 00:00

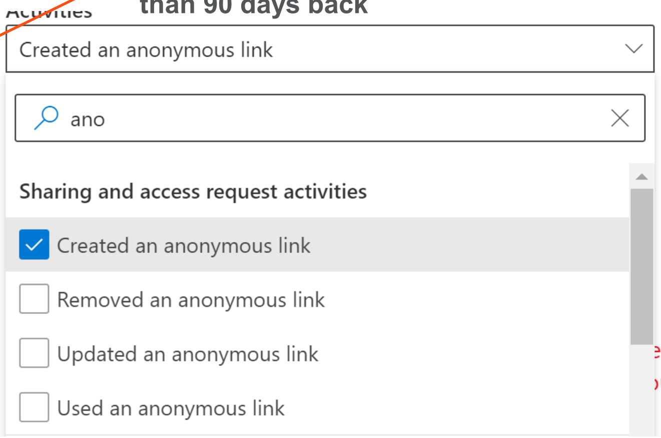
Searching for activities that occurred over 90 days ago only re
duration of any audit log retention policies. For example, if yo

Search | Clear all

Export

pplied filters:

Date	IP Address



Activities

Created an anonymous link

ano

Sharing and access request activities

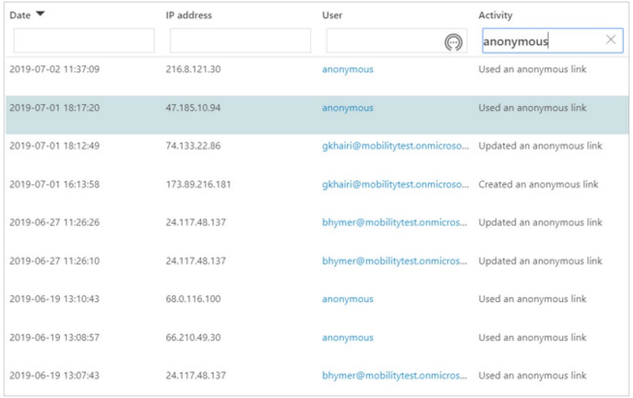
☑ Created an anonymous link

□ Removed an anonymous link

□ Updated an anonymous link

□ Used an anonymous link

Unified Audit log



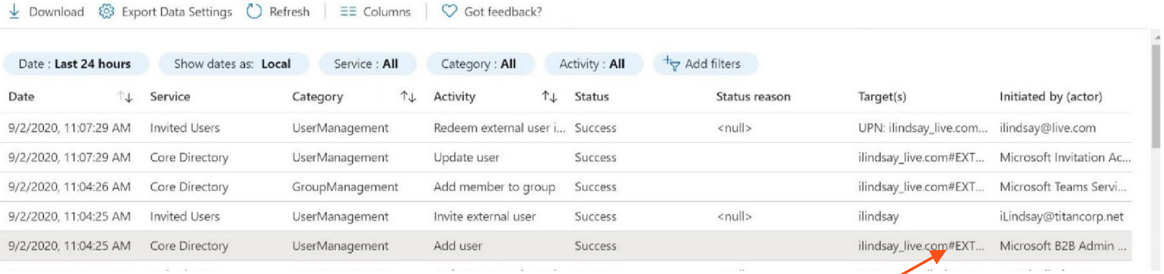
Date	IP address	User	Activity
			anonymous
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link
2019-07-01 16:13:58	173.89.216.181	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

6. Guest access in Teams

- Teams usage have exploded as the Pandemic began to spread
- Teams makes it very easy to share content with each other – also for guests from outside the organisation
- 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, a mailbox and a SharePoint site that stores the data
- Adding an external user to a Team creates a new user account in your Azure AD tenant (B2B)

6. Guest access in Teams

Azure AD Audit log



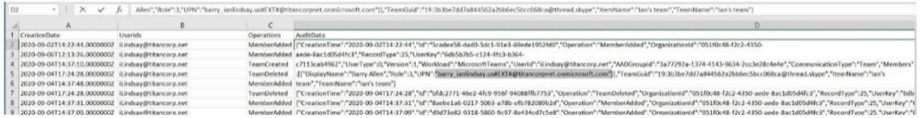
Download | Export Data Settings | Refresh | Columns | Got feedback?

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

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 ...

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

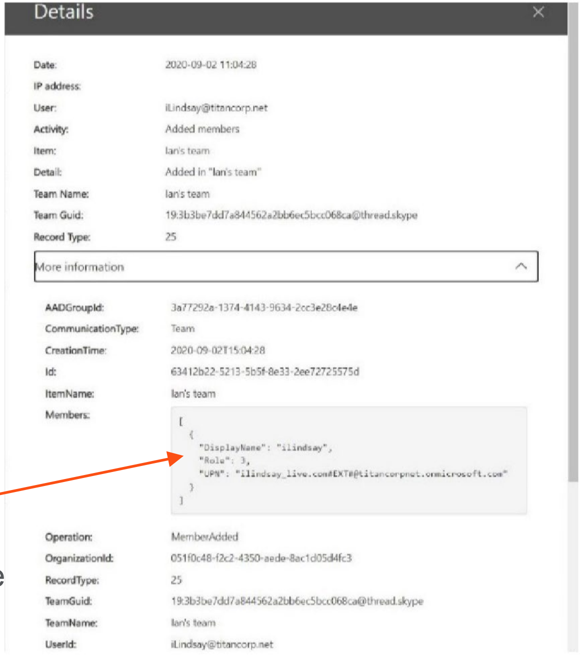
External guests can be identified by looking for #EXT in the username



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":"5cadea58-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":"d0d73e82-9318-5860-9c97-8e434cd7c5e8","Operation":"MemberAdded","OrganizationId":"051f0c48-f2c2-4350-aede-8ac1d05d4fc3","RecordType":25,"UserKey":"(

Unified Audit log



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

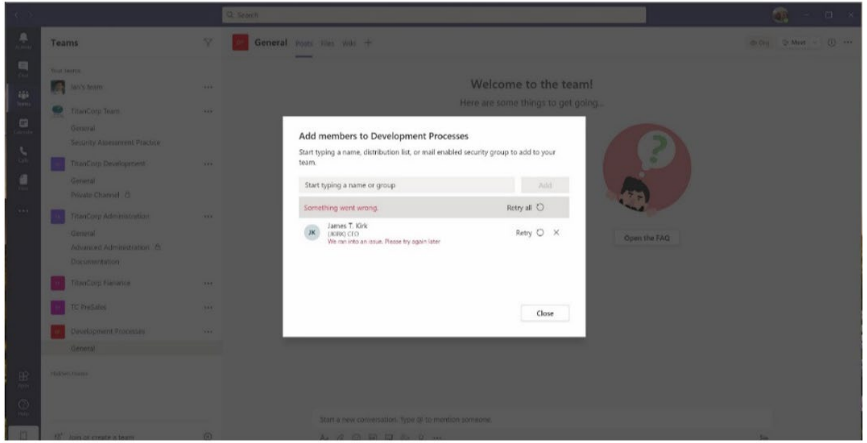
More information

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

You need to review multiple events, to identify the guests added

7. Teams being created or deleted

- Teams facilitates collaboration by making it easy for users to create and delete teams. But native tools dont make it easy for admins to keep it all under control
- Rights for users to create new Teams can be removed, but requiring all users to go through IT for new group creation
- Admins can also delete 365 groups belonging to Teams mistakenly ending with a confusing error as below for the business user



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 | Add

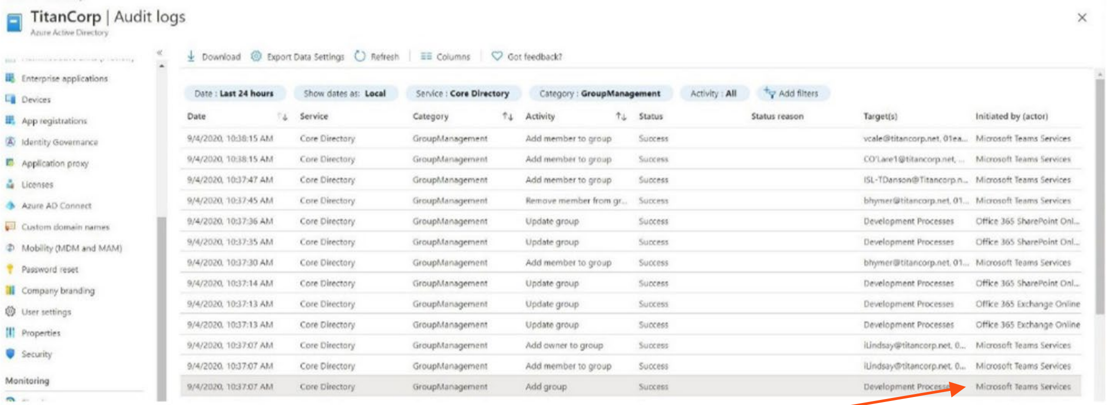
Something went wrong. Retry all

JK James T. Kirk
(KIRK) CEO
We ran into an issue. Please try again later
Retry ×

Close

7. Teams being created or deleted

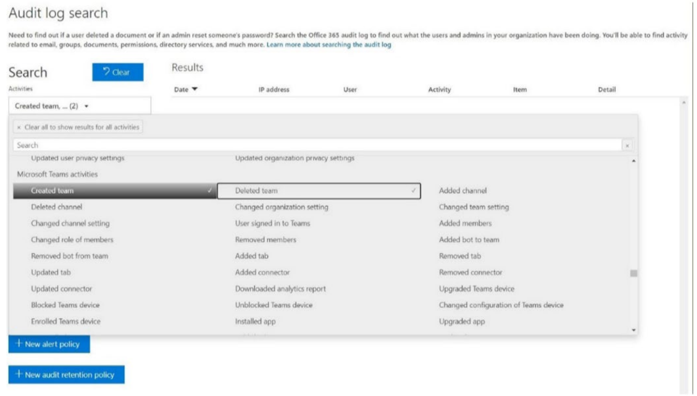
Azure AD Audit log



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

Unified Audit log

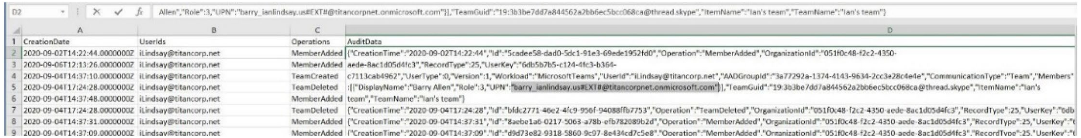


Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and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

Service:Core Directory
Category:Group Management
«Microsoft Teams Service» in **initated by(actor)**

To find changes not made through the Teams interface, search for the group directly, look for the groupname in «Targets» field

Export and view in 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":"6
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":"6

8. Forwarding of inbound email messages

- **Users and admins can set forwarding on Exchange mailboxes**
- **Forwarding inbound mail while leaving mail in the mailbox**
- **Forwarding can be perfectly harmless but many admins really want to pay attention to this to catch changes that suggest malicious activities**

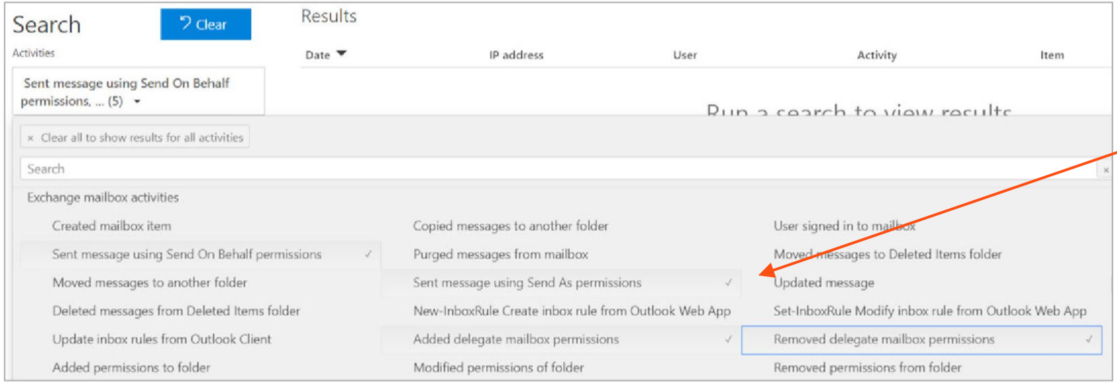
Unfortunately, the audit logs in AAD and Office 365 do not allow for direct searches on those changes. You need to export the entire changelog from ExO to a CSV, then search for exported events containing **{“name”:”DeliverToMailboxAndForward”,”value”:”True”}** in parameters field, to return the desired events.

9. Non-owner mailbox 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
- But, it can also be seriously misused to read data in sensitive mailboxes, while organisations trust their mail admins they must also look out for rogue activity
- If an executive assistants account is compromised, an attacker could get access to your CEOs mailbox

9. Non-owner mailbox activity

Unified Audit log



Search ↻ Clear

Activities

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

× Clear all to show results for all activities

Search

Results

Date ▾	IP address	User	Activity	Item

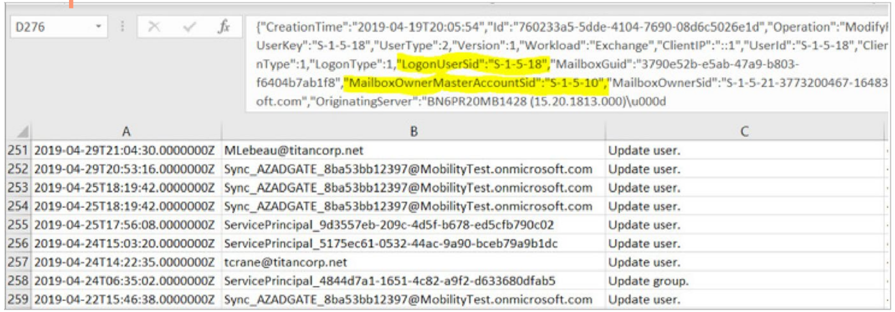
Run a search to view results

Exchange mailbox activities

Created mailbox item	Copied messages to another folder	User signed in to mailbox
Sent message using Send On Behalf permissions ✓	Purged messages from mailbox	Moved messages to Deleted Items folder
Moved messages to another folder	Sent message using Send As permissions ✓	Updated message
Deleted messages from Deleted Items folder	New-InboxRule Create inbox rule from Outlook Web App	Set-InboxRule Modify inbox rule from Outlook Web App
Update inbox rules from Outlook Client	Added delegate mailbox permissions ✓	Removed delegate mailbox permissions ✓
Added permissions to folder	Modified permissions of folder	Removed permissions from folder

You can review the most common types of non-owner events by including the following options

Export and view in Excel



D276

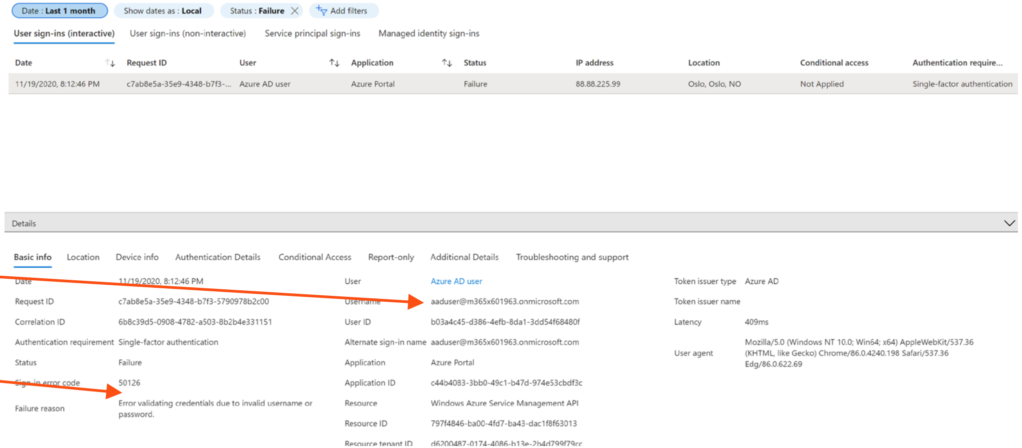
```
{"CreationTime":"2019-04-19T20:05:54","Id":"760233a5-5dde-4104-7690-08d6c5026e1d","Operation":"Modifyf
UserKey":"S-1-5-18","UserType":2,"Version":1,"Workload":"Exchange","ClientIP":"::1","UserId":"S-1-5-18","Clier
nType":1,"LogonType":1,"LogonUserSid":"S-1-5-18","MailboxGuid":"3790e52b-e5ab-47a9-b803-
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.

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]

10. Failed sign-in attempts

- Tracking failed logins is key. Lockouts frustrates users, but failed logins can indicate malicious activity, such as brute force password activity.
- On Premises failed logins is stored in the security logs on all DCs, in Azure these are found in the Azure audit logs. They can be searched, but it can be hard to get an overview and determine the patterns.


Date : Last 1 month
Show dates as : Local
Status : Failure
Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

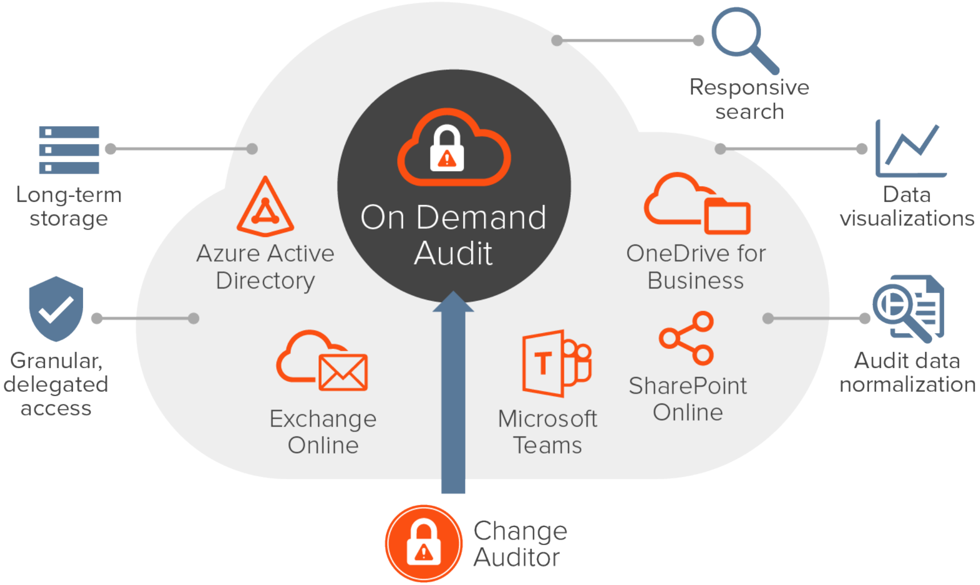
Date	Request ID	User	Application	Status	IP address	Location	Conditional access	Authentication require...
11/19/2020, 8:12:46 PM	c7ab8e5a-35e9-4348-b7f3-...	Azure AD user	Azure Portal	Failure	88.88.225.99	Oslo, Oslo, NO	Not Applied	Single-factor authentication

Date	11/19/2020, 8:12:46 PM	User	Azure AD user	Token issuer type	Azure AD
Request ID	c7ab8e5a-35e9-4348-b7f3-5790978b2c00	Username	aaduser@m365x601963.onmicrosoft.com	Token issuer name	
Correlation ID	6b8c39d5-0908-4782-a503-8b2b4e331151	User ID	b03a4c45-d386-4efb-8da1-3dd54f68480f	Latency	409ms
Authentication requirement	Single-factor authentication	Alternate sign-in name	aaduser@m365x601963.onmicrosoft.com	User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36 Edg/86.0.622.69
Status	Failure	Application	Azure Portal		
Sign-in error code	50126	Application ID	c44b4083-3bb0-49c1-b47d-974e53cbdf3c		
Failure reason	Error validating credentials due to invalid username or password.	Resource	Windows Azure Service Management API		
		Resource ID	797f4846-ba00-4fd7-ba43-dac1f8f63013		
		Resource tenant ID	d6200487-0174-4086-b13e-2b4d799f79cc		

What if you didn’t have to struggle with all the shortcomings of the native auditing tools for Office 365 and Azure?

On Demand Audit Hybrid Suite

- **Full hybrid/cloud auditing – ONE view**
- **Track OnPrem logon activity for complete Hybrid overview**
- **Modern Search UI with interactive data visualizations**
- **Stores your data for up to 10 years**



On Demand Audit

Azure Active Directory

OneDrive for Business

Exchange Online

Microsoft Teams

SharePoint Online

Long-term storage

Granular, delegated access

Responsive search

Data visualizations

Audit data normalization

Change Auditor

On-premises agents

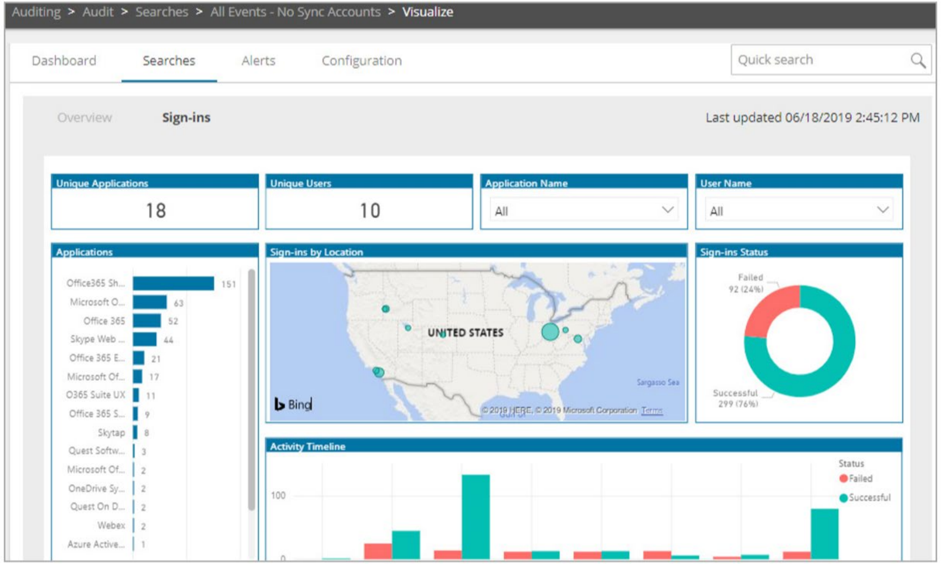
- Active Directory
- Logon activity
- Windows Server / NAS

■ Coming soon to On Demand Audit

Quest

Where Next Meets Now.

On Demand Audit Hybrid Suite



Auditing > Audit > Searches > All Events - No Sync Accounts > Visualize

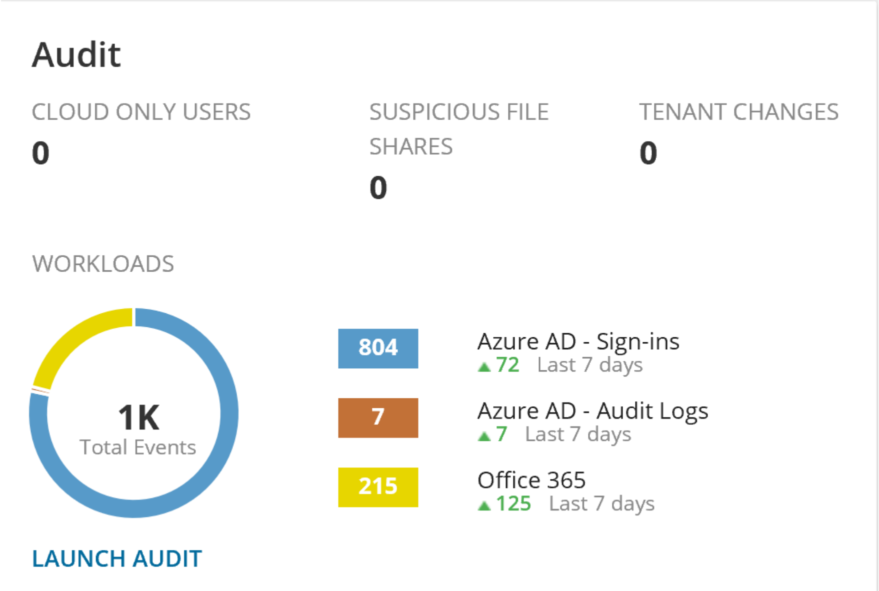
Last updated 06/18/2019 2:45:12 PM

Unique Applications: 18

Unique Users: 10

Application Name: All

User Name: All



Audit

CLOUD ONLY USERS
0

SUSPICIOUS FILE SHARES
0

TENANT CHANGES
0

WORKLOADS

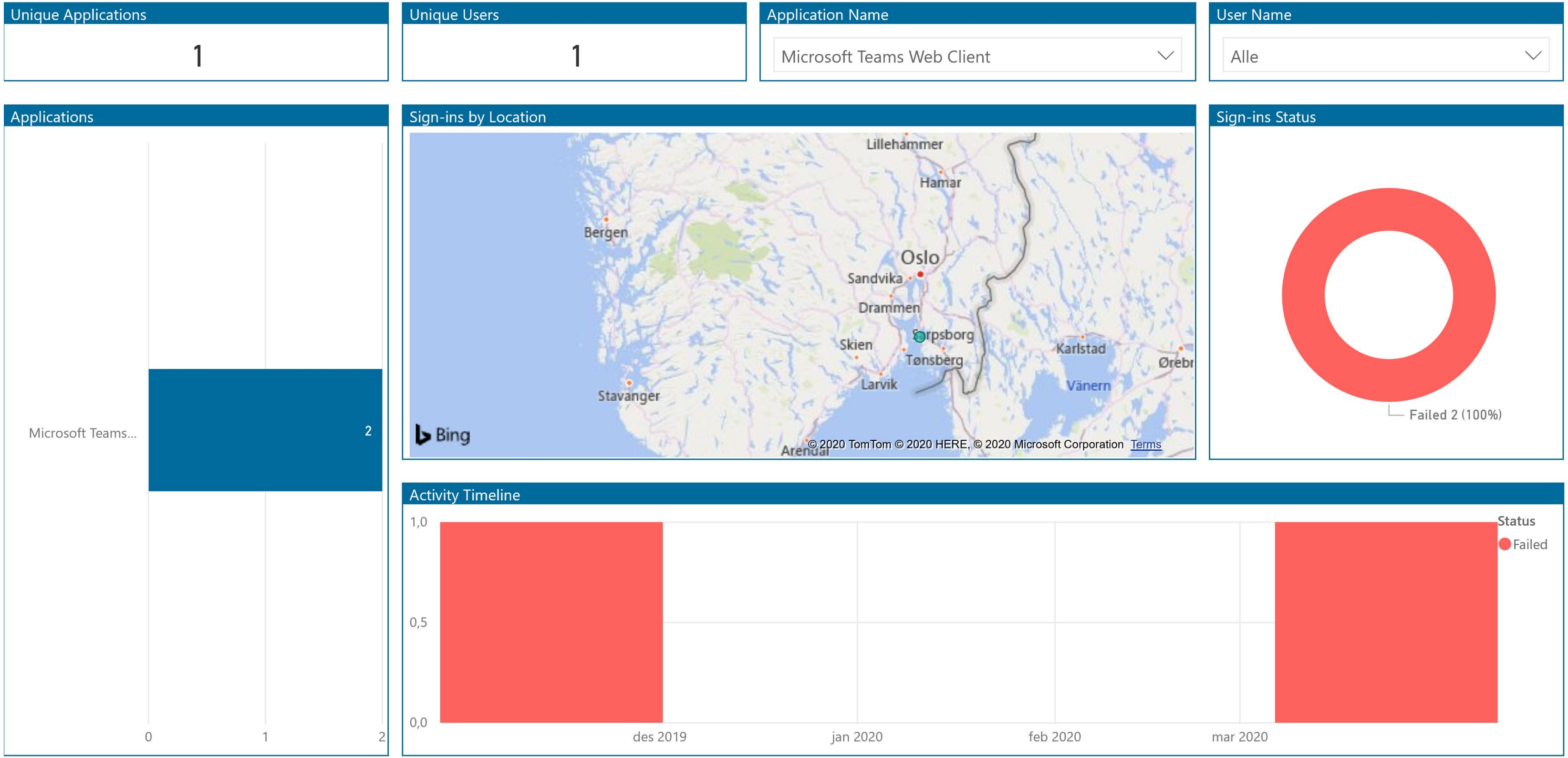
804	Azure AD - Sign-ins ▲ 72 Last 7 days
7	Azure AD - Audit Logs ▲ 7 Last 7 days
215	Office 365 ▲ 125 Last 7 days

LAUNCH AUDIT

Quest

Where Next Meets Now.

On Demand Audit – Azure failed sign-ins



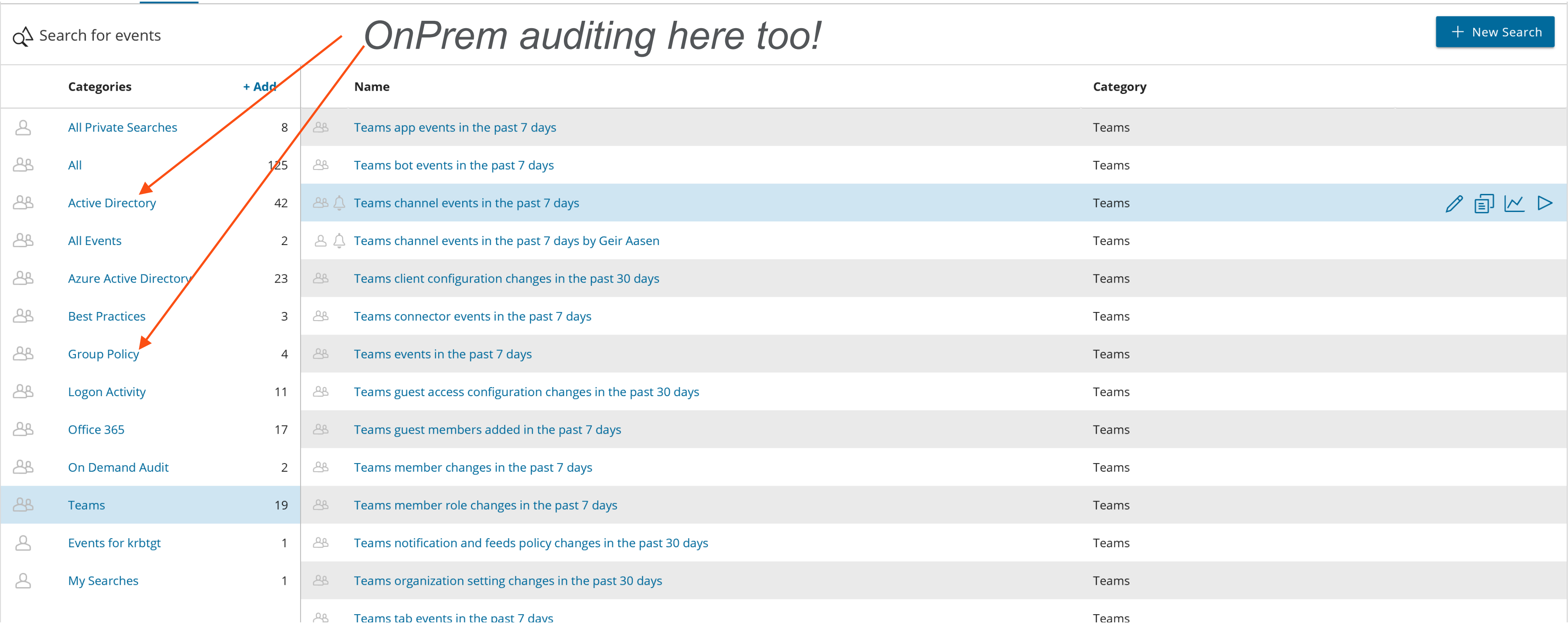
Unique Applications
1

Unique Users
1

Application Name
Microsoft Teams Web Client

User Name
Alle

Get control and insight into Teams



OnPrem auditing here too!

	Categories	
	All Private Searches	8
	All	125
	Active Directory	42
	All Events	2
	Azure Active Directory	23
	Best Practices	3
	Group Policy	4
	Logon Activity	11
	Office 365	17
	On Demand Audit	2
	Teams	19
	Events for krbtgt	1
	My Searches	1

Name	Category
Teams app events in the past 7 days	Teams
Teams bot events in the past 7 days	Teams
Teams channel events in the past 7 days	Teams
Teams channel events in the past 7 days by Geir Aasen	Teams
Teams client configuration changes in the past 30 days	Teams
Teams connector events in the past 7 days	Teams
Teams events in the past 7 days	Teams
Teams guest access configuration changes in the past 30 days	Teams
Teams guest members added in the past 7 days	Teams
Teams member changes in the past 7 days	Teams
Teams member role changes in the past 7 days	Teams
Teams notification and feeds policy changes in the past 30 days	Teams
Teams organization setting changes in the past 30 days	Teams
Teams tab events in the past 7 days	Teams

Comparing Quest with native auditing

Critical auditing requirement	Native	Quest
Alert on suspicious events regardless of whether they occur on prem or cloud	X	✓
Cut through raw data and see only what is important for the change/activity	X	✓
Flexible search on any event or any field, including by actor, changed attributes, activity details or cloud-only objects	X	✓
Normalize view of all user activity, on prem and in the cloud	X	✓
Keep audit data for up to 10 years to satisfy internal policies and external compliance regulations	X	✓

QUESTions?

Active Directory & Office 365 management End-to-end support for your next Microsoft challenge

For more information on O365, Hybrid O365 check out our solutions pages:

https://www.quest.com/solutions/microsoft-platform-management/

Feel free to reach out to me with any questions.

Geir.Aasen@quest.com

Quest

Where Next Meets Now.