Office 365 Management Made Easy with AdminDroid

AdminDroid offers 1500+ reports and 15+ dashboards to bring your entire Microsoft 365 infrastructure under your radar. With AdminDroid you can manage and secure your organization with better control and visibility in just a few mouse clicks.

The tool provides advanced reporting features, alerting capabilities, customization options, and report automation abilities, that help the Microsoft 365 administrators monitor everything in the organization and make sure that no event gets unnoticed.

Microsoft 365 Reporting - Stay up to date and make decisions faster

AdminDroid provides reports on all major Microsoft 365 services such as Exchange Online, SharePoint Online, Teams, OneDrive, Power BI (Audit), and more.

Every report is very well analyzed and categorized in a granular way based on each service. The reports will contain in-depth and detailed information on the data available in your Microsoft 365 tenant.

() The	ing for more login details? <u>III User Sign-ins With Detailed Informatio</u> a location (country, state, and city), browse	under Sign-in analytics includes details, such as the logged-in r, and authentication method.		Actor Actor Context ID Actor IP Address	: admin@o365droid.onmicrosoft.com : d4599306-7afd-4795-a127-a4887491b46e : 27.5.112.36
B Tabular View B 10 10	Views • Y ± M 1 Operation •	D Cogon Error Application	17	Application Application ID Client Detailed Login Info	: Office365 Shell WCS5-Client : 89bee177-5e6e-4d8a-9f3d-ecd601259da7 : -
.ogin Time 🗸	† Target	1 Logged In User	Operation	Result Status Detail	: Redirect
2/2/2022 9:58:00 AM	5f09333a-842c-47de-a157-57d	a2. admin@o365droid.onmicrosoft.com	User Logger	User Agent	 Mozilla/5.0 (Windows NT 10.0 ; Win64 ; x64) AppleWebKit/537.3 (KHTML like Gecko) Chrome/97.0.4692.99 Safari/537.36
2/2/2022 9 58 00 AM	00000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logge	Request Type	: OAuth2:Authorize
2/2/2022 9:58:00 AM	00000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logger	Event ID	: 210c815d-005d-4b97-ac67-4e4779914600
2/2/2022 9:57:57 AM	0000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logger	Inter-Systems ID	c3bddaa4-3d94-4e0a-ab13-6a6809ef4ebe
				Intra-Systems ID	: 210c815d-005d-4b97-ac67-4e4779914600
2/2/2022 9:57:57 AM	00000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logge	Is Basic Auth	: No
2/2/2022 9:57:57 AM	5f09333a-842c-47da-a157-57d	a2 admin@o365droid.onmicrosoft.com	User Logger	Logged In Machine IP	: 27.5.112.36
2/2/2022 9:57:55 AM	00000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logger	Logged In User	: admin@o365droid.onmicrosoft.com
2/2/2022 9:57:55 AM	5f09333a-842c-47da-a157-57d	a2. admin@o365droid.onmicrosoft.com	User Logger	Login Status Details	
2/2/2022 9:57:55 AM	.00000003-0000-0000-c000-000	00 admin@o365droid.onmicrosoft.com	User Logger	Login Time Logon Error	: 2/2/2022 9:57:57 AM
2/2/2022 9:57:52 AM	00000003-0000-0000-c000-000	00 admin@io365droid.onmicrosoft.com	User Logger	Modified Properties	
2/2/2022 9:57:52 AM	5f09333a-842c-47da-a157-57d	a2 admin@o365droid.onmicrosoft.com	User Logge:	Operation	: User Logged In
2/2/2022.9:57:51 AM	00000003-0000-0000-c000-000	100 admin@o365droid.onmicrosoft.com	User Logger	Operation Name	: User Logged in
2/2/2022 9 57 46 AM	00000002-0000-0000-c000-000	100 admin@o365droid.onmicrosoft.com	User Logges	Result Status Support Ticket ID	: Succeeded
1/11/2022 5:00:43 AM	5109333a-842c-47da-a157-57d	a2. admin@o365droid.onmicrosoft.com	User Logger	Target	: 00000003-0000-0000-0000-000000000000
1/11/2022 5:00:42 AM	00000003-0000-0000-c000-000	and Barrier and a second second	User Logger	Target Context ID	: d4589306-7afd-4795-a127-a4887491b46e
1/11/2022 5:00:42 AM	00000003-0000-0000-0000-000		User Logger	Target(User/Group/File/ Site/Mailbox/)	: 00000003-0000-c000-c000000000000

Microsoft 365 Auditing - Track Activities, know who did what operation and when

With AdminDroid's dedicated audit reports, Microsoft 365 admins will be able keep an eye on all the users and groups in the organization by **tracking day-to-day activities** such as file sharing/access events, email traffic, non-owner accesses, secure score, password changes, login attempts, and so on. You shall also do this by just having a quick glance at '**User Activities Dashboard**'.

	Activities by All Users - T (Available views : 25)	Event Time Workload	Operation		User Principal Name	Ψ	Target(User/Group/File/Site/Mailb		
es	Activities By Users	12 Active Users	Activities By Use	ers			2015	10	
es	A admin @o365droid.onmicrosoft.com	3k activities 7% failure	5k Activities				2915 ^{Total} User	12 Active User	Licensed
	P pete @o365droid.onmicrosoft.com	1k activities 0% failure	Overall Summary 5k	ali Logo	n Activities		Application Administration Activities	User Administratio	on Activities
	M melanie.allan @o365droid.onmicrosoft.com	41 activities 0% failure	Azure AD 2k	*	Success 1k Failure		Success 180 Failure		Success 142 Failure
	s sophie.lee @o365droid.onmicrosoft.com	38 activities	Exchange 79		3		233		11
	A andrea.kelly	32 activities	SharePoint 1k						
	A @o365droid.onmicrosoft.com	396 failure	OneDrive 1k	Grou	p Administration Activitie	s	Unclassified Activities	Role Administratio	
	B brandon, peters @o365droid.onmicrosoft.com	31 activities 0% failure		1	Success 86 Failure		76 Failure		Success 42 Failure
	A admindroid_mailer @o365droid.onmicrosoft.com	27 activities 0% failure		*	0		0		0
	W Wynonah @o365droid.onmicrosoft.com	26 activities		Licen	ise Management Activities	5	Directory Administration activities	Policy Activities	
	A andrea.dyer @o365droid.onmicrosoft.com	17 activities 0% failure	112	() Licen	Success 21 Failure		Success 5 Failure		Success 5 Failure
	Jane @o365droid.onmicrosoft.com	4 activities 0% failure			0				0
	A adelev @0365droid.onmicrosoft.com	4 activities		Adm	inistrativeUnits Administr	ation			

Microsoft 365 Alerting - Detect anomalies in a smarter way

AdminDroid can assist you in identifying new risks and unusual activities, comparing activity trends, and alert you on **1400+ Microsoft 365 activities**.

This includes 45+ prebuilt policy templates that can be deployed readily. You can visualize the alerts, statuses, and trends quickly in the alert's dashboard, and take immediate action on the triggered alerts. Also, you can mark them as open, closed, and investigating as per your needs.

AdminDroid		Alert Policies Overview of all the		ed aler	n policie									king For Help? will 🎔 our interactive
Deshboerds		2												
Overall		Dashboard		20	Alert	Policie	ke	arch Alert Poli	cien				R Alert Policy Beoprits	Add Alert Policy
Azure AD			100	20	Availabl									
Security		4		All 🗵	0	Create	d by You	11 Crea	ted by Others (B)				Table Info : Policy De	Execution Details
Exchange		Alerts												
Emel			A	ctions		Stat	15	Severity	Alert Policy Name	Triggered Alerts	Description	Labels	Alert Settings	Daily Notificatio
SharePoint Audit		Policies		/ 0	0		Active	• Severe	User Sign-Ins Without any Conditional Ac.				When more than 5 new Policy not applied	
Usage and Adoption		Policies		/ 8	0		Active	• Severe	Copy of MFA(Multi-factor Authentication				Create separate alert for each new Logins	
		۲		1.10	0	•	Active	 Severe 	MFA(Multi-factor Authentication) Disabled				Create a single alert by grouping all the n.	
Reports	- 1	Policy		1.8	0	•	Active	• Severe	Blocked user attempted to login		When sign-in blocked users try to login, c	 Treat Management 	When the number of Failed sign-ins for th.	. 24
Audit	. +	Templates		/ 0	i Đ		Active	• Medium	Group owner changes	1	Creates an alert having a list of users wh	Configuration changes	Create a single alert by grouping all the n.	24
Analytics Protes	+	E.		/ 8	0	•	Active	• High	High level risky sign ins		Creates alerts if a high-level risky sign-in i	Flisky sign-les	Create separate alert for each new High r.	24
ReportBoards		Alert		/ 8	0		Active	. Severe	Unusual volume of file deletion		Creates an alert with a list of users who r	🧧 Information governance	When the number of File deletions for the	24
				1.10	0		Active	• High	MFA Disabled			8	Create separate alert for each new MFA	24
Alerts Now				1.8	0		Active	• Severe	MFA Disabled - Severity Alert				Create a single alert by grouping all the n.	
Schedule Reports				/ 8	0		Active	• Severe	Alert Policy by deino 123			Nisky sign-les	Create a single alert by grouping all the n.	100
Settings	+			/ 8	0	•	Active	• Severe	Alert Policy by demo2				Create a single alert by grouping all the n	24
Support			1.0	18	0	-	Active	• Severe	Email Notification Alert			e Information governance	Create separate alert for each new Mails	24
confistion of				1.8	0	•	Active	• Info	Daily Audit Activities Comparision by Op	20	8	Information governance	A single alert is generated every day by g.	24
			1	/ 8	0	•	Active	• Low	Days with more than 5 activities			AdminDroid Costom Label	When more than 5 new Activities occur w.	24
				/ 8		•	Active	e Info	Notify All Logins	1	This policy is created just for populating	Traffic menitoring	Create a single alert by grouping all the n.	24
			1	/ 8	0		Active	. Low	All failed activities		Creates a single alert by comparing the p	Risky sign-les	A single alert is generated every week by	24
				2.14	16	-		• Info	Teams private channel creations		Creates alerts whenever a private channe	Information governance	Create separate alert for each new Privat	24

Microsoft 365 Usage Analytics - Easy user behavior analysis

Admins can easily audit and evaluate the usage & adoption of the various Microsoft 365 services using the '**Usage and Adoption**' dashboard. You can find the active users across each department, job title, city, state, and so on. This will help you to track the active users based on the operation performed, file shared/accessed, workload, and more.

Also, this assists administrators in **identifying inactive resources** and removing unused licenses, hence lowering the cost that is spent on licenses.

× view	Activities by A	Il Users 👻 🛛 🝸 (Available views : \$)	Event Time WorkL	oad	v Operation	٣	User	Target(U	ser/Group/File/Site/N	v .		
	Activities by Dept		8 Active	Activities by Job Title		8 Active Job Title	Activities by City		6 ^{Active}	Activities by State		5 Activ
	29k Activities	230 Active users 310 Licensed users	540 Total User	29k Activities	230 Active users 324 Licensed users	554 Total User	30k Activities	260 Active users 360 Licensed users	620 Total User	31k Activities	270 Active users 380 Licensed users	650 Total User
	n 2k Activities	200 Active users 150 Licensed users	350 Total User	Developer 1k Activities	205 Active users 200 Licensed users	405 Total User	Chicago 1k Activities	180 Active users 170 Licensed users	350 Total User	Texas 841 Activities	230 Active users 150 Licensed users	380 Total User
	634 Activities	90 Active users 80 Licensed users	170 Total User	Sys Admin 841 Activities	100 Active users 90 Licensed users	190 Total User	Peoria 841 Activities	150 Active users 144 Licensed users	294 Total User	California 634 Activities	100 Active users 94 Licensed users	194 Total User
	QA 592 Activities	78 Active users 74 Licensed users	152 Total User	634 Activities	150 Active users 130 Licensed users	280 Total User	Rockford 634 Activities	187 Active users 166 Licensed users	353 Total User	Dubai 592 Activities	110 Active users 100 Licensed users	210 Total User
	Core 141 Activities	60 Active users 54 Licensed users	114 Total User	Job title 592 Activities	110 Active users 70 Licensed users	180 Total User	Elgin 592 Activities	107 Active users 96 Licensed users	203 Total User	Delhi 400 Activities	100 Active users 75 Licensed users	175 Total User
	IT department 84 Activities	32 Active users 24 Licensed users	56 Total User	IT Job 84 Activities	34 Active users 20 Licensed users	54 Total User	Pekin 340 Activities	100 Active users 94 Licensed users	194 Total User	Bangalore 340 Activities	86 Active users 78 Licensed users	164 Total User
	%Teaching 2 Activities	1 Active users 1 Licensed users	2 Total User	Trainer#Softw 2 Activities	1 Active users 1 Licensed users	2 Total User	Morton 254 Activities	75 Active users 41 Licensed users	116 Total User	Alaska 200 Activities	70 Active users 65 Licensed users	135 Total User
	Digital Market	1 Active users	1 Total User	SEO 1 Activities	1 Active users 0 Licensed users	1 Total User	IT city 84	38 Active users 41 Licensed users	79 Total User	IT state 84	45 Active users 30 Licensed users	75 Total User

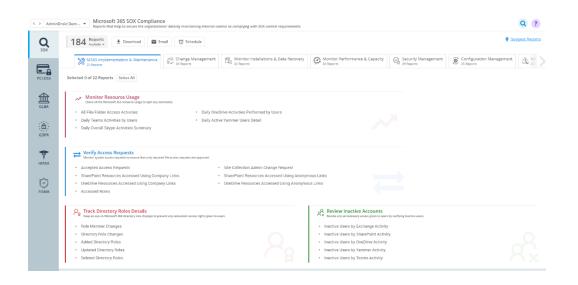
AdminDroid offers up to date analytical reports on detailed internal vs external email statistics, Azure sign-ins, CA Policy based analytics, and so on. These reports will provide with insightful information that are not readily available in Microsoft 365.

Microsoft 365 Compliance Auditing - Manage sensitive organization data in a better way

To simplify your organization's compliance requirements, reports are analyzed and categorized with respect to various compliance requirements.

- SOX
- PCI-DSS
- GLBA
- GDPR
- HIPAA
- FISMA

This will help the Microsoft 365 administrators in **maintaining an internal control over the organization's data securely** by monitoring suspicious activities, alerts, threats, unauthorized accesses, configuration & privilege changes, etc.



Microsoft 365 Insights- Keep an eye on your Office 365 statistics

AdminDroid provides insightful dashboards by allowing admins to get **clear visibility with a bird's eye perspective** of various Microsoft 365 services' statistical data.

Also, every report will contain the respective **visually appealing graphical representation** in the forms of Pie, Donut, and Bar charts. Using this AI-powered graphical view of data, admins can gain insights into any report and better understand the data. Clicking on the available data will quickly drill down into the details.



Multi-factor Authentication Overview

Combo View Ke Views 🔻	T 🛨 🖾 🗘					
n-in Time Signed-in User	Signed-in Application Name City	MFA Authentication S	tatus Device OS with Version	Device Browser	Sign-in Status	
All Time	r 📃 🔍 🗸	Ψ	Ŧ	T	Ŧ	Ŧ
Chart prepared for All Time + Contication	on Status Daily Sign-in summary by I	Device OS with Version 🚺 🔿 by Devi	ce Browser 📊 Daily Sign-in sur	mmary by Sign-in Status $ imes$	Daily Sign-in summary by Sign	ned-in Via
	Sign-in Status 3	200 150 100 50				
	⊘ Failure	Sep 2021 Oct	01 0 2021 Nov:	2021	01 16 Dec 2021 Dec 2021	
ign-in Time v		08	t 2021 Nov	1	01 16	; Device Browser
	✔ Failure	08 Sep.2021 Oct Total Sign-In Status : 3 10 Max	: 2021 Nov : Sign-Ins (856) : Success 🛛 🕲 Min Sign-	1 2021 Ins (23) : Failure	01 16 Dec 2021 Dec 2021	: Device Browser Chrome 96.0.4664
2/16/2021 6:53:42 AM	✓ Failure Signed-in User	08 Sep 2021 Oct 10 Total Sign-In Status : 3 10 Max : ; Signed-in Application Name	2021 Nov: Sign-Ins (856) : Success 30 Min Sign- MFA Authentication Status	1 2021 Ins (23) : Failure ; City	01 16 Dec 2021 Dec 2021	
2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM	G Pallure Signed-in User admin∯o365droid onmicrosoft.com	08 Oct Sep 2021 Oct Total Sign-In Status : 3 To Max 3 : Signed-in Application Name Office365 Shell WCSS-Client	2021 Nov Sign-Ins (856) : Success 0 10 Min Sign- MFA Authentication Status Not Configured	1 2021 Ins (23) : Failure I City Thoraipakkam	01 16 Dec 2021 Dec 2021 2 Device OS with Version Windows 10	Chrome 96.0.4664
2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM	© failure Signed-in User admin@0365droid.com admin@0365droid.com	08 08 Sep 2021 Ora Total Sign-In Status : 3 10 Max Signed-in Application Name Office365 Shell WCSS-Client Office365 Shell WCSS-Client Office365 Shell WCSS-Client	2021 Nov Sgn-Ins (856) : Success 10 Min Sign- MFA Authentication Status Not Configured Not Configured	1 2021 Ins (23) : Failure is City Thoraipakkam Thoraipakkam	01 16 Dec 2021 Dec 2021 Pervice OS with Version Windows 10 Windows 10	Chrome 96.0.4664 Chrome 96.0.4664
2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM 2/16/2021 6:53:42 AM	Graiure Signed in User admin@o365droid.comicresoft.com admin@o365droid.comicresoft.com admin@o365droid.comicresoft.com	08 08 Sep 2021 Ora Total Sign-In Status : 3 Total Sign-In Status : 3 Signed-in Application Name Office365 Shell WCSS-Client Office365 Shell WCSS-Client Office365 Shell WCSS-Client Office365 Shell WCSS-Client Office365 Shell WCSS-Client	2021 Nov. Sgn-Int (B56) : Success 10 Min Fign- i MFA Authentication Status Not Configured Not Configured Not Configured	1 2021 Ins (23) : Failure i City Thoraipakkam Thoraipakkam Thoraipakkam	01 16 Dec 2021 Dec 2021 2 Device OS with Version Windows 10 Windows 10	Chrome 96.0.4664 Chrome 96.0.4664 Chrome 96.0.4664
ign-in Time ♥	Callure Signed-in User admin@03655roid omnicrosoft.com admin@0365droid omnicrosoft.com admin@0365droid omnicrosoft.com	Citeral Segment and C	2221 Nov. Sign-Ins (856) : Success 0 10 Min Sign- MPA Authentication Status Not Configured Not Configured Not Configured	1 2021 in (23) : Failure i City Thoraipakkam Thoraipakkam Thoraipakkam	Dec 2021 10 Dec 2021 Dec 2021 00 Dec 2021 Undows 10 Windows 10 Windows 10 Windows 10	Chrome 96.0.4664 Chrome 96.0.4664 Chrome 96.0.4664 Chrome 96.0.4664

Major feature highlights:

Advanced Reporting Capabilities - Personalize your reports by using the column customization, sorting, and advanced filtering options to limit your report results; Export the report data in your preferred formats such as PDF, HTML, XLS/XLSX, CSV, and RAW format.

Views in Reports - Create reports with customized filters and save them for further use.

Intelligent Scheduling - Send automated reports to the desired email addresses at regular intervals to keep track of the organization's and users' daily/weekly/monthly progress. Also, it is possible to schedule the reports with applied filters, preferred report columns, and more customizations, according to your reporting needs.

Multi-tenant support - Connect multiple Microsoft 365 tenants and generate reports on all the tenants in a single AdminDroid portal itself. This functionality also allows you to delegate separate admins for each tenant as per your wish.

Delegated Access - Limit the reports' and dashboards' access to your AdminDroid admins. Also, it is possible to limit the Microsoft 365 data available in those reports and dashboards; Grant this delegated access to any user irrespective of the assigned Microsoft 365 Roles.

Data Retention - Override the default 90 days limit of native audit log retention and preserve the audit data indefinitely.