

ManageEngine  
M365 Security Plus

# M365 Security Plus

Product overview



# Solutions Offered



Microsoft 365 Auditing



Microsoft 365 Monitoring



Microsoft 365 Alerting



Microsoft 365 Content Search



Microsoft 365 Delegation

# Supported Services



Yammer



# Highlights of M365 Security Plus

- Custom profile-based auditing and alerting
- Access to historical audit data with indefinite storage
- Schedule audit reports to be generated at periodical time intervals
- Instant alerts for critical events and service health decline
- Instant notifications for service health decline
- 24x7 monitoring of Microsoft 365 features and endpoints
- Advanced content search to identify spear-phishing attacks
- Custom help desk roles without escalating user privileges in Microsoft 365
- Cross tenant and virtual tenant delegation
- Dashboard with embeddable widgets
- In-depth analysis with SIEM integration



# Microsoft 365

## auditing & alerting

# M365 Security Plus vs Microsoft 365 admin center

Auditing features	M365 Security Plus	Microsoft 365
Geolocation-enabled audit reports	✓	✗
Custom views and advanced filtering options	✓	✗
Auditing based on business and non-business hours	✓	✗
Custom alerts to keep you informed about real-time changes	✓	✗
User-based and group-based auditing	✓	✗
Long term historical data/audit log storage	✓	✗
Individual audit profiles for each activity	✓	✗

# Custom audit and alert profiles

Dashboard Audit Alerts Monitoring Delegation Settings Support Tenant Settings

Configuration Admin

**Audit Profiles** ?

Office 365 Tenant:  Enable Audit:  Data Fetch Interval: Every 1 hours and 0 minutes Last Data Read Time: 31 Aug 2020 07:04 PM [Run Now] Status: Success

[+ Add Profile](#)

Showing All 1-25 of 87 25

<input type="checkbox"/>	Actions	Profile Name	Office 365 Service	Category	Last Modified On	Reports
<input type="checkbox"/>		Activities by Mailbox Owners	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Send As Activities	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Activities by Mailbox Non-Owners	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Activities by Exchange Admins	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Activities by Mailbox Delegates	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Mail Move and Delete Activities	Exchange Online	Exchange Online Activities	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Mailbox Permission Changes	Exchange Online	Mailbox permission	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Mailbox Storage Quota Changes	Exchange Online	Mailbox	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Mailbox Move Activities	Exchange Online	Mailbox move	17 Jul 2020 06:11 PM	<a href="#">View Report</a>
<input type="checkbox"/>		Mailbox Create and Delete Activities	Exchange Online	Mailbox	17 Jul 2020 06:11 PM	<a href="#">View Report</a>

# Geolocation feature

Search Report (Ctrl+Space)

zohocorpadmgrplus.onmicroso...

Exchange Online

- Exchange Activity
- Activities by Mailbox Owners
- Send As Activities
- Activities by Mailbox Non-Owners
- Activities by Exchange Admins
- Activities by Mailbox Delegates
- Mail Move and Delete Activities
- Mail Contact
- Connector
- Mailflow
- Management Roles
- Public Folder
- Mailbox Move
- Mail Trace

Period: 13/01/2020 12:00 AM - 12/02/2020 11

Domains: All Domains

Export As Schedule Profiles more

Operations

When	Who	Mailbox UserPrincipalName	Operation	Result Status	Target Details	Modified Properties	Logon Type	Country
11 Feb 2020 05:33 AM	admin@zohocorpadmgrplus.onmicrosoft.com	admin@zohocorpadmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	-	Owner	India
11 Feb 2020 03:27 AM	janakar.m@zohocorpadmgrplus.onmicroso...	janakar.m@zohocorpadmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	-	Owner	India

1-25 of 47 25 Add/Remove Columns Create New View

+ New Audit Profile

# Audit profile configuration and advanced filters

The screenshot displays the 'Audit Profile Configuration' page in the ManageEngine M365 Security Plus interface. The top navigation bar includes 'Dashboard', 'Audit', 'Alerts', 'Monitoring', 'Delegation', 'Settings', and 'Support', with 'Tenant Settings' available in the top right. The left sidebar shows a navigation menu with 'Configuration' and 'Admin' sections. Under 'Configuration', there are sub-menus for 'Audit Configuration', 'Alert Profiles', 'Monitoring Configuration', 'Content Search Configuration', and 'Other Configuration'. The main content area is titled 'Audit Profile Configuration' and contains the following fields:

- \* Profile Name:** Text input field containing 'Test'.
- Description:** Text input field.
- \* Office 365 Service:** Dropdown menu with 'Azure Active Directory' selected.
- \* Category:** Dropdown menu with 'Azure AD user' selected.
- \* Actions:** Dropdown menu with '- Select -' selected.

Below these fields is an 'Advanced Configuration' section with a 'Filter Settings' sub-section containing two checkboxes:

- Business Hours Filter
- Filter By Column

At the bottom of the configuration area, there are two buttons: a green 'Add' button and a grey 'Cancel' button. A user profile icon is visible in the bottom right corner of the interface.

# Alert profile configuration

Dashboard Audit Alerts Monitoring Delegation Settings Support Tenant Settings

Configuration Admin

### Alert Profile Configuration

\* Profile Name

Description

\* Office 365 Service

\* Category

\* Actions

\* Severity  Attention  Trouble  Critical

\* Alert Message  [Macros](#)

Advanced Configuration ▾

Notification Filter Settings

Email every alert corresponding to this profile

Select Notification Template  +

Include event details. ?

Add Cancel

# Custom alerts threshold configuration

**Alert Profile Configuration**

**Configuration** | **Admin**

**Audit Configuration** ▾  
Audit Profiles  
Alert Profiles

**Monitoring Configuration** ▶  
Content Search Configuration ▶  
Other Configuration ▶

\* Profile Name:

Description:

\* Microsoft 365 Service:

\* Category:

\* Actions:

\* Severity:  Attention  Trouble  Critical

\* Alert Message:  [Macros](#)

**Advanced Configuration** ▾

**Notification** | **Filter Settings**

Alerts Threshold

At least  events occurring within  minutes grouped by  ?

Business Hours Filter

Filter By Column



# Microsoft 365 monitoring

# M365 Security Plus vs Microsoft 365 admin center

Monitoring Features	M365 Security Plus	Microsoft 365
Single dashboard for all Microsoft 365 services	✓	✗
Graphical representation of service health	✓	✗
Endpoint monitoring	✓	✗
Real-time email alerts	✓	✗
Access to monitoring data older than 30 days	✓	✗

# Service health overview

Search Report (Ctrl+Space) | All Services Health ? | Export As | Schedule Profiles | More

ompga.onmicrosoft.com

All Services Health

Overview

Exchange Online

Azure Active Directory

Microsoft 365

Skype for Business

SharePoint Online

OneDrive for Business

Others

Incident 0

Advisory 5

Healthy 10

Last updated on: 15 Dec 2021 10:45 PM

Service Name	Health Status	
Microsoft 365 suite	Advisory - 2	<a href="#">View Report</a>
Exchange Online	Advisory - 2	<a href="#">View Report</a>
Microsoft Teams	Advisory - 1	<a href="#">View Report</a>
Azure Information Protection	Healthy	
Skype for Business	Healthy	
SharePoint Online	Healthy	
OneDrive for Business	Healthy	
Identity Service	Healthy	
Mobile Device Management for Office 365	Healthy	
Sway	Healthy	
Planner	Healthy	
Power BI	Healthy	
Microsoft StaffHub	Healthy	

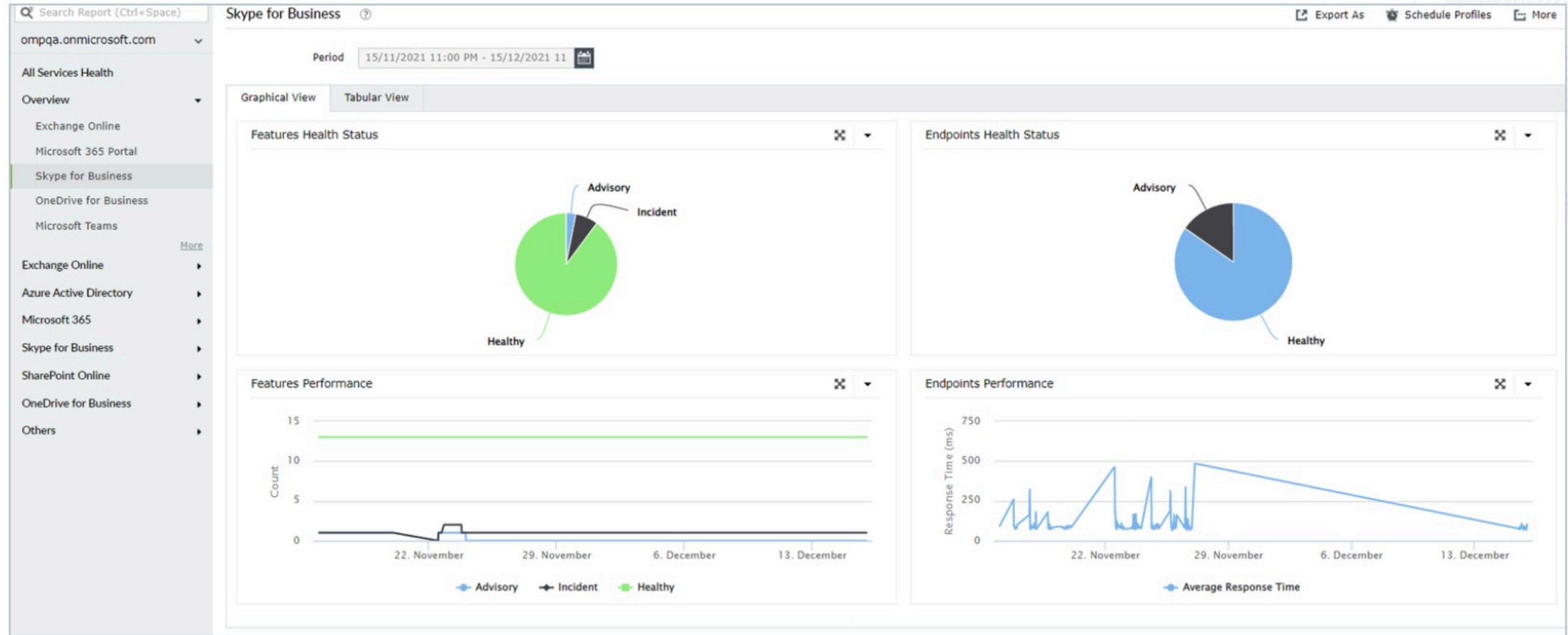
+ New Monitoring Profile

# Detailed summary of service incidents

The screenshot displays the Microsoft 365 Services Health dashboard. At the top, there is a search bar and navigation options like 'Export As', 'Schedule Profiles', and 'More'. A summary bar shows the status of services: 0 Incidents (red), 5 Advisories (orange), and 10 Healthy services (green). The 'Last updated on' timestamp is 15 Dec 2021 10:45 PM. A table lists various services, with 'Exchange Online' selected. A detailed view for Exchange Online shows two advisories under the 'Email and Calendar' category. The first advisory (EX303756) is titled 'Users may not receive click alerts for potentially malicious URLs in Exchange Online' and has a status of 'Restoring service', updated on 2021-12-15 05:54:15 (UTC). The second advisory (EX302429) is titled 'Some users may be unable to utilize some Exchange Online features via all connection methods' and has a status of 'Extended recovery', updated on 2021-12-13 19:34:11 (UTC). Both advisories include a 'Show Details' link.

Service Name	Exchange Online
Microsoft 365 suite	Advisory - 2
Exchange Online	<b>Email and Calendar</b>
Microsoft Teams	Event Title :  Users may not receive click alerts for potentially malicious URLs in Exchange Online Status : Restoring service
Azure Information Protection	Event ID : EX303756 Updated : 2021-12-15 05:54:15 (UTC)
Skype for Business	User Impact : Users may not receive click alerts for potentially malicious URLs in Exchange Online. <a href="#">Show Details</a>
SharePoint Online	<b>Email and Calendar</b>
OneDrive for Business	Event Title :  Some users may be unable to utilize some Exchange Online features via all connection methods Status : Extended recovery
Identity Service	Event ID : EX302429 Updated : 2021-12-13 19:34:11 (UTC)
Mobile Device Management for Office 365	User Impact : Users may be unable to utilize some Exchange Online features via all connection methods. <a href="#">Show Details</a>
Sway	
Planner	
Power BI	
Microsoft StaffHub	

# Graphs for quick understanding



# Trove of monitoring data for reference

Monitoring Profiles ?

Microsoft 365 Tenant: ompqa.onmicrosoft.com | Enable Monitoring:  | Polling Frequency: Every 30 minutes | Last Data Read Time: 16 Dec 2021 12:15 AM [Run Now] | Status: Success

Monitoring Settings | + Add New Profile

Actions	Profile Name	Microsoft 365 Service	Feature/Endpoint	Last Modified On	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Access Services	SharePoint Online	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Admin and Sharing	OneDrive for Business	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Administration	Microsoft 365 Portal	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	All Features	Skype for Business	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	All Services Health	All Services Health	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Audio and Video	Skype for Business	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure AD Connect	Azure Information Protection	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure Device Registration	Azure Information Protection	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure Information Protection	Azure Information Protection	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure Portal	Azure Information Protection	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure Remote App	Azure Information Protection	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Azure Rights Management	Azure Information Protection	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	CDNs for SharePoint Online and associated applications	SharePoint Online	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Cloud App Security	Microsoft 365 Portal	Endpoint	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Cloud PBX	Skype for Business	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Custom Solutions and Workflows	SharePoint Online	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Dial-In Conferencing	Skype for Business	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Email and Calendar	Exchange Online	Feature	02 Jun 2021 12:55 AM	<a href="#">View Report</a>



# Microsoft 365 content search

# M365 Security Plus vs Microsoft 365 admin center

Content search features	M365 Security Plus	Microsoft 365
Instant search option for mailboxes	✓	✗
Search options for all email attributes, e.g. subject, body, internet message headers	✓	✗
Pattern-based content search—choose your own options	✓	✗
Keyword-based mail search	✓	✗
Customized content search profiles that suit your need	✓	✗
Real-time alerts for particular profiles	✓	✗
Bulk mailbox content monitoring	✓	✗

# Instant search option

Search Report (Ctrl+Space)

zohocorpadmgrplus.onmicroso... ▾

Content Search Profiles ▾

- Mail Content Profiles
- Instant Search**

Instant Search ?

Select Mailbox  +

Search Criteria

1	<input type="text" value="From"/> ▾	<input type="text" value="Contains"/> ▾	<input type="text" value="harry@mydomain.com"/>	<input type="button" value="+"/>	<input type="button" value="x"/>
2	<input type="text" value="AND"/> ▾	<input type="text" value="Cc Recipients"/> ▾	<input type="text" value=""/>	<input type="button" value="+"/>	<input type="button" value="x"/>

Criteria : ( 1 AND 2 )

# Mail attributes and keyword-based search

The screenshot displays the 'Instant Search' interface. On the left, a sidebar contains a search bar with the text 'Search Report (Ctrl+Space)', a mailbox selection dropdown showing 'zohocorpadmgrplus.onmicroso...', and a 'Content Search Profiles' section with 'Mail Content Profiles' expanded. Under 'Mail Content Profiles', 'Instant Search' is selected, with sub-options for 'All Mails - Last 30 days' and 'Mails with Attachments'. The main area is titled 'Instant Search' and includes a 'Select Mailbox' dropdown set to '-Select-' and a 'Search Criteria' field. The 'Search Criteria' field contains a dropdown menu with 'Body' selected, followed by a 'Contains' dropdown and a text input field containing 'confidential'. A green 'Search' button is visible below the criteria field.

# Pattern-based search

The screenshot displays the 'Instant Search' configuration window. On the left, a sidebar shows the navigation menu with 'Instant Search' selected. The main window has a title bar 'Instant Search' with a help icon. Below the title bar, there are two main sections: 'Select Mailbox' and 'Search Criteria'. The 'Select Mailbox' section features a dropdown menu currently set to '-Select-' and a '+' button to the right. The 'Search Criteria' section contains a large text input field with the text 'Body', 'Contains', and 'Confidential' entered. Each of these terms is followed by a small dropdown arrow. To the right of the input field is a green '+' button. At the bottom of the window, there are two buttons: a green 'Search' button and a grey 'Cancel' button.



# Help desk delegation

# M365 Security Plus vs Microsoft 365 admin center

Delegation features	M365 Security Plus	Microsoft 365
Custom roles for technician delegation	✓	✗
Customized tenants and virtual tenants delegation	✓	✗
Role delegation to technicians without providing admin rights	✓	✗
Help desk technician activity auditing	✓	✗

# Creating custom help desk technician roles

The screenshot shows the 'Create New Role' page in the ManageEngine M365 Security Plus interface. The top navigation bar includes 'Dashboard', 'Audit', 'Alerts', 'Monitoring', 'Delegation', 'Settings', and 'Support', with 'Tenant Settings' in the top right. The page title is 'Create New Role' with a 'Back' button. Below the title are two input fields: '\*Role Name' and 'Description'. A horizontal bar contains four categories: 'Audit', 'Monitoring', 'Content Search', and 'Others'. The main content area is divided into two columns. The left column lists various services with checkboxes: Azure Active Directory, Exchange Online, OneDrive for Business, Compliance Management, Microsoft Streams, Sway Services, Microsoft Teams, Power BI, Yammer, and SharePoint Online. The right column contains six role categories, each with a list of permissions: 'Azure AD User' (Added, Updated, Deleted user), 'Azure AD Password' (Reset, Changed user password, Set property that forces user to change password, Updated user credentials), 'Azure AD License' (Set license properties, Changed user license), 'Azure AD Group' (Added, Updated, Deleted group, Add member to group), 'Azure AD Role Administration' (Added users to admin role, Deleted users from member role, Updated company contact information), and 'Azure AD App Administration' (Added delegation entries, Added service principals, Added credentials to service principals, Removed delegation entry). A user profile icon is visible in the bottom right corner.

# Adding a help desk technician

Help Desk Delegation ▾

Help Desk Technicians

Help Desk Roles

HDT Detailed View

HDT Audit Reports ▶

### Add New Technician

Authentication Type  ▾

Microsoft 365 Tenant  ▾

Select M365 Users  +

Help Desk Roles  ▾

Delegate Microsoft 365 Tenants  ▾

# Detailed help desk technician view

Dashboard Audit Alerts Monitoring Delegation Settings Support Tenant Settings

Help Desk Delegation ▾ HDT Detailed View ? Export As More

Help Desk Technicians

Help Desk Roles

HDT Detailed View

HDT Audit Reports ▶

Delegated Roles Delegated O365 Tenants Delegated Virtual Tenants Delegated Profile Actions Delegated Monitoring Profiles

admin [Product Authentication]

Delegated Roles	Delegated O365 Tenants	Delegated Virtual Tenants	Delegated Profile Actions	Delegated Monitoring Profiles
Super Admin	All Tenants.	Default Virtual Tenant.	<a href="#">Azure AD User:</a> Added user, Updated user, Deleted user. <a href="#">Azure AD Password:</a> Reset user password, Changed user password	<a href="#">Features:</a> Sign In, Email and Calendar, Email Timely Delivery, Management and Provisioning, Voice Mail.
securityAnalyst [Product Authentication]				
Security Analyst	All Tenants.	Default Virtual Tenant.	<a href="#">Azure AD User:</a> Added user, Updated user, Deleted user. <a href="#">Azure AD Password:</a> Reset user password, Changed user password	--
securityAdministrator [Product Authentication]				
Security Administrator	All Tenants.	Default Virtual Tenant.	<a href="#">Azure AD User:</a> Added user, Updated user, Deleted user. <a href="#">Azure AD Password:</a> Reset user password, Changed user password	<a href="#">Health Overview:</a> Exchange Online, Office 365 Portal, Office Subscription, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, Yam

# Help desk technician audit report

Help Desk Delegation ▸  
HDT Audit Reports ▾  
Audit Reports  
Admin Activity

## HDT Audit Report ?

Export As More

Select Help Desk Technicians: All Technicians

Period: 16/11/2021 12:00 AM - 15/12/2021 01:00 AM

[Generate Now](#)

Q 1-25 of 108 25 Add/Remove Columns

Technician Name	Category	Activity	Target	Audit Time	Client IP
admin	Login	Logged in	M365 Security Plus Authentication	15 Dec 2021 05:57 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	15 Dec 2021 05:02 PM	192.168.75.104
admin	Login	Logged in	M365 Security Plus Authentication	15 Dec 2021 04:17 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	15 Dec 2021 02:09 PM	192.168.75.104
admin	Login	Logged in	M365 Security Plus Authentication	15 Dec 2021 02:07 PM	192.168.75.104
admin	Login	Logged in	M365 Security Plus Authentication	14 Dec 2021 10:21 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	14 Dec 2021 06:38 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	14 Dec 2021 02:34 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	14 Dec 2021 01:22 PM	192.168.75.82
admin	Login	Logged in	M365 Security Plus Authentication	14 Dec 2021 01:21 PM	192.168.75.82



# SIEM integration



# Configuring syslog server/Splunk server

The screenshot shows the 'Log Forwarder' configuration page in the ManageEngine M365 Security Plus interface. The left sidebar contains navigation options: Configuration, Admin, Administration (with sub-items: Notification Templates, Product Schedulers, Disk Space Alerts, Integration Settings, Logon Settings), and General Settings. The main content area is titled 'Log Forwarder' and includes a 'Back' button. A checkbox for 'Enable Log Forwarding' is checked. Below this, there are two radio buttons for 'Syslog' (selected) and 'Splunk'. The Syslog configuration section includes: a required 'Server Name or IP' field with the value 'Test'; a 'Protocol' dropdown menu set to 'UDP'; a required 'Port' field with the value '514'; and a 'Syslog Type' dropdown menu set to 'Raw Log' with a help icon. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Configuration Admin

Administration

- Notification Templates
- Product Schedulers
- Disk Space Alerts
- Integration Settings
- Logon Settings

General Settings

Log Forwarder ?

Back

Enable Log Forwarding

Syslog  Splunk

\* Server Name or IP

Protocol

\* Port

Syslog Type  ?

Save Cancel



**THANK YOU**