



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

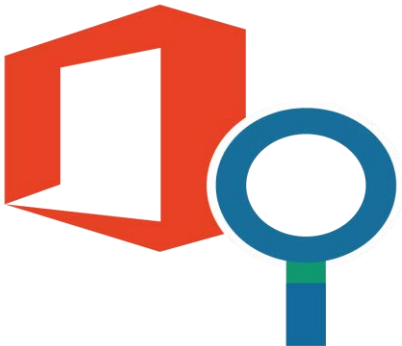
- Exchange Online
- Microsoft Teams
- Azure Active Directory
- SharePoint Online
- OneDrive for Business
- Microsoft Stream
- Skype for Business
- Yammer, Sway, and more.



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 & Alerting 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

The screenshot displays the 'Audit Profiles' configuration interface. At the top, there are controls for 'Office 365 Service' (set to 'Exchange Online'), 'Enable Audit' (checked), 'Daily Audit Interval' (set to 'Every 1 hour and 15 minutes'), and 'Last Audit Run Time' (27 Aug 2020 07:52:00). A 'Refresh' button is also present.

Profile Name	Office 365 Service	Category	Last Modified By	Status
Activities by Mailbox Owners	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Send to Activities	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Activities by Mailbox Mail Owners	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Activities by Exchange Admins	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Activities by Mailbox Administrators	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Mail Flow and Search Activities	Exchange Online	Exchange Online Activities	17 Aug 2020 06:21:46	Active
Mailbox Permission Changes	Exchange Online	Mailbox permissions	17 Aug 2020 06:21:46	Active
Mailbox Storage Quota Changes	Exchange Online	Mailbox	17 Aug 2020 06:21:46	Active

Geolocation feature



Audit profile configuration and advanced filters



Alert profile configuration



Custom alerts threshold configuration

The screenshot displays the 'Alert Profile Configuration' page in the ManageEngine interface. On the left, a navigation sidebar lists various configuration sections: Configuration, Audit Configuration, Audit Profiles, Alert Profiles, Performance Configuration, Control Panel Configuration, and Other Configuration. The main content area is titled 'Alert Profile Configuration' and includes several input fields: 'Profile Name', 'Description', 'Alerts per second' (set to 'Average Interval Summary'), 'Manager' (set to 'Alerts@localhost'), and 'Email' (set to 'admin'). Below these fields are radio buttons for 'Enabled', 'Disabled', and 'Critical', with 'Enabled' selected. A 'Test Message' button is also present. At the bottom, the 'Advanced Configuration' section is expanded to show 'Notification' and 'Alert Settings' tabs. Under 'Alert Settings', there are checkboxes for 'Alert Threshold', 'Business Hours Filter', and 'Alert Acknowledgment'. The 'Alert Threshold' section contains a table with columns for 'Alerts', 'Alerts per second', 'Interval (minutes)', and 'Action', with a 'Save' button to the right.

Microsoft 365 monitoring



M365 Security Plus vs Microsoft 365 admin center

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

Service health overview

The screenshot displays a service health overview dashboard. On the left, there is a navigation sidebar with categories like 'Overview', 'Configuration', 'Monitoring', and 'Reports'. The main content area shows a table of services. At the top right, there are three summary buttons: a red one with a warning icon, an orange one with a refresh icon, and a green one with a checkmark icon. The table lists various services, most of which are in a 'Healthy' state, indicated by green checkmarks.

Service Name	Status	Health
Service 1	Healthy	OK
Service 2	Healthy	OK
Service 3	Healthy	OK
Service 4	Healthy	OK
Service 5	Healthy	OK
Service 6	Healthy	OK
Service 7	Healthy	OK
Service 8	Healthy	OK
Service 9	Healthy	OK
Service 10	Healthy	OK
Service 11	Healthy	OK
Service 12	Healthy	OK
Service 13	Healthy	OK
Service 14	Healthy	OK
Service 15	Healthy	OK
Service 16	Healthy	OK
Service 17	Healthy	OK
Service 18	Healthy	OK
Service 19	Healthy	OK
Service 20	Healthy	OK
Service 21	Healthy	OK
Service 22	Healthy	OK
Service 23	Healthy	OK
Service 24	Healthy	OK
Service 25	Healthy	OK

Detailed summary of service incidents

The screenshot displays the ManageEngine ServiceDesk Plus interface. On the left is a navigation sidebar with categories like 'All Service Incidents', 'Incidents', 'Exchange Online', 'SharePoint Online', 'Office 365', 'Skype for Business', 'Microsoft Exchange', 'Microsoft Office 365', 'Outlook on the Go', 'Office 365 Group', and 'Office 365 Mailbox'. The main area is titled 'All Service Incidents' and contains a list of incidents. A modal window titled 'Skype for Business' is open, showing details for a specific incident. At the top right of the main area, there are three status indicators: a red warning icon with '1' incidents, an orange info icon with '1' incidents, and a green OK icon with '11' incidents.

Skype for Business

Severity: **Warning**

Alerts and Notes

Event ID:	Exchange-incident	Level:	Exchange-incident
Event ID:	Exchange-incident	Level:	Exchange-incident
Log Message:	Users may be unable to use their contacts in the Skype for Business desktop, mobile, and web clients. View Details		

Alerts and Notes

Event ID:	Exchange-incident	Level:	Exchange-incident
Event ID:	Exchange-incident	Level:	Exchange-incident
Log Message:	Users may be unable to use their contacts in the Skype for Business desktop, mobile, and web clients. View Details		

Graphs for quick understanding



Trove of monitoring data for reference

Monitoring Profiles

Office 365 Tenant: Enable Monitoring: Rolling Frequency: Every 30 minutes Last Data Received: 02 Feb 2020 05:13:49 [View Data](#) Status: [Refresh](#)

[Monitoring Settings](#) [Add New Profile](#)

Actions	Profile Name	Office 365 Service	Features/Endpoint	Last Modified To	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Access Services	SharePoint Online	Features	02 Jan 2020 05:20:47 M	View Report A
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Admin and Sharing	Exchange for Business	Endpoint	02 Jan 2020 05:20:47 M	View Report I
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Administration	Office 365 Portal	Features	02 Jan 2020 05:20:47 M	View Report Y
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	All Features	Skype for Business	Features	02 Jan 2020 05:20:47 M	View Report I
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	All Services Health	All Services Health	Features	02 Jan 2020 05:20:47 M	View Report Y

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

The screenshot shows the 'Instant Search' configuration page. On the left is a sidebar with navigation options: 'admin@manageengine.com', 'Content Search Profiles', 'Mail Search Profiles', and 'Instant Search'. The main area is titled 'Instant Search' and contains the following fields:

- Host Name:** A text field containing '192.168.1.100'.
- Search Criteria:** A table with two rows of search filters. Each row includes a dropdown menu, a field type selector, a search field, and status indicators (green and red).

Criteria	Field Type	Search Field	Status
[Dropdown]	Contains	name@mydomain.com	Green, Red
[Dropdown]	Contains	[Empty]	Green, Red

At the bottom of the configuration area are two buttons: a green 'Save' button and a grey 'Cancel' button.

Mail attributes and keyword-based search



Pattern-based search



Help desk delegation



M365 Security Plus vs Microsoft 365 admin center

Help Desk Delegation Features	MMS Security Plus	Microsoft 365
Custom roles for technician delegation	✔	✘
Customized tenants and virtual tenants delegation	✔	✘
Role delegation to technicians without providing admin right	✔	✘

Creating custom help desk technician roles

The screenshot shows the 'Add New Role' configuration page in the ManageEngine Help Desk interface. At the top, there are input fields for 'Role Name' and 'Description'. Below these, a navigation menu on the left lists various system components. The main area is divided into six panels, each representing a different role with a list of permissions:

- Admin All Users:**
 - Add user
 - Update user
 - Delete user
- Admin All Requests:**
 - Add user request
 - Update user request
 - Delete request that have user in change process
 - Update user resolution
- Admin All Groups:**
 - Add group
 - Update group
 - Delete group
 - Add members to group
- Admin All User Administrations:**
 - Add user to admin role
 - Delete users from admin role
 - Update admin user information
- Admin All Request Administrations:**
 - Add request admin role
 - Update admin request
 - Delete admin role to admin request
 - Update request admin role

Adding a help desk technician

The screenshot shows the 'Add New Technician' form in the ManageEngine interface. On the left is a navigation menu with the following items: 'Help Desk Configuration', 'Add New Technician', 'Help Desk Roles', 'Help Desk Users', and 'Help Desk Reports'. The main form area contains the following fields:

- Office 365 Account: [dropdown menu]
- Default Office 365 Name: [text input]
- Help Desk Roles: [dropdown menu]
- Integrated Office 365 Account: [dropdown menu]

Below the fields is a checkbox labeled 'Dependable on MDM (users can access to Office 365 with the account)' and a green 'Add' button.

Detailed help desk technician view

The screenshot displays the 'Help Desk Technician View' interface. On the left is a navigation sidebar with options: 'Help Desk Dashboard', 'Help Desk Rules', 'Help Desk Views', 'Help Desk Reports', and 'Help Desk Settings'. The main area is titled 'Help Desk Views' and contains a table with the following columns: 'Component Name', 'Assigned Help Desk', 'Assigned Group Name', 'Assigned User Name', and 'Assigned Working Status'. The table lists three rows, each representing a different component (e.g., Super Admin, Security Admin, Security Administrator) with associated help desk, group, and user information. A search bar and filter icons are visible at the top right of the table area.

Component Name	Assigned Help Desk	Assigned Group Name	Assigned User Name	Assigned Working Status
Super Admin	All Groups	Default Group Name	Super Admin (Admin user - Not yet set. Contact user)	Assigned (Open to, Start and End times, Fixed Time Interval, No assignment and Processing, No report)
Security Admin	All Groups	Default Group Name	Security Admin (Admin user - Not yet set. Contact user)	Assigned (Open to, Start and End times, Fixed Time Interval, No assignment and Processing, No report)
Security Administrator	All Groups	Default Group Name	Security Administrator (Admin user - Not yet set. Contact user)	Assigned (Open to, Start and End times, Fixed Time Interval, No assignment and Processing, No report)

Help desk technician audit report

Help Desk Delegation

HDT Audit Reports

Audit Reports

Recent Activity

HDT Audit Report

Select Help Desk Technicians: All Technicians

From: 12/10/2023 00:00:00 To: 12/10/2023 23:59:59

Generate Report

Username Name	Category	Activity	Target	Status	Audit Report
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	
johndoe	Login	logged in	CRM Manager Plus Authentication	Success	

SIEM integration



Integrate M365 Security Plus with SIEM solutions



Benefits:

- **Single interface:** The integration offers a central console where users can easily access and analyze security information from a wide range of sources including Microsoft 365 logs.
- **Compliance:** Archive the log data in a central place to meet the requirements of regulatory mandates such as PCI DSS, HIPAA, ISO 27001, SOX, and more.
- **Detect incidents:** With logs presented in easy-to-understand reports, graphs, charts, and other graphical formats, identify security threats in Microsoft 365 easily .

Configuring syslog server/Splunk server





ManageEngine

Thank you!

