

The definitive guide for  
**Office 365 management  
and security**



## Table of contents

1. Introduction .....	3
2. Office 365 management: Five things you can't do using native tools .....	4
3. AD360—Your 360 degree Office 365 manager .....	7
User provisioning .....	8
License management .....	9
Reporting .....	9
Auditing .....	10
Alerting .....	12

## Introduction

Microsoft's SaaS productivity suite, Office 365, offers organizations Exchange Online, Skype for Business, SharePoint Online, Outlook, Word, Excel, and other business applications that can help increase productivity and cut costs. But with these benefits come a few drawbacks, especially in terms of IT management.

As an IT administrator, managing Office 365 by creating new users, assigning appropriate licenses, removing users who leave a department or organization, and revoking licenses can occupy most of your time. Aside from these tasks, you also have to ensure Office 365 is secure by generating various audit reports and monitoring important events.

You might have tried using native Office 365 tools or PowerShell scripting to manage Office 365. You probably found it difficult, especially if you tried performing bulk operations. There are many other shortcomings of these tools that make Office 365 administration difficult, making it nearly impossible to increase productivity in your organization.

In this document, we'll discuss some of the major disadvantages of native Office 365 administration tools. We'll also go over how you can overcome these issues using AD360, a user-friendly, web-based software portfolio, to increase your organization's overall productivity.

# Office 365 administration: Five things you can't do using native tools

Native Office 365 administration tools fail to fulfill some of the essential aspects of administration, such as bulk user provisioning, granular delegation, historical auditing, and more. This not only results in a loss of productivity, but poses serious questions related to the safety of your Office 365 environment. This section covers the five major drawbacks every administrator faces when using Office 365's native tools.

## 1. No simultaneous bulk user provisioning in AD and Office 365.

When you create users in both Active Directory (AD) and Office 365 with the native Office 365 administration tools, you need to toggle between multiple windows.

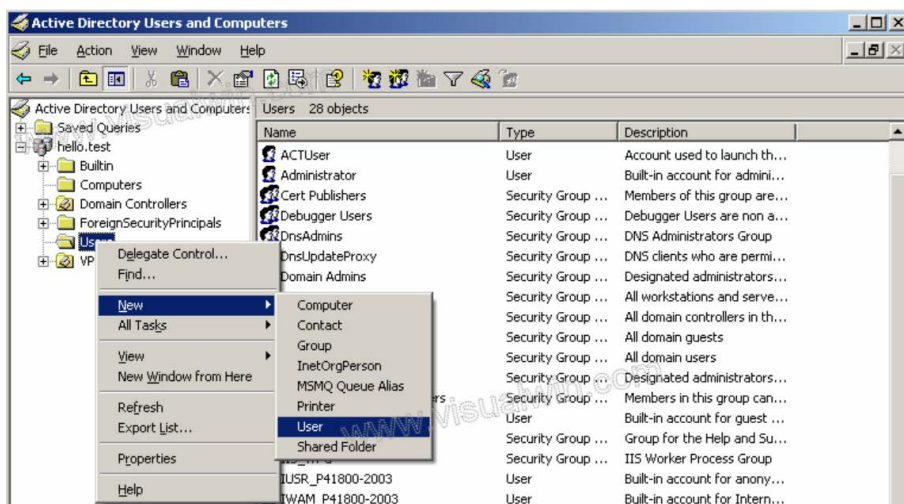
A screenshot of the 'New user' dialog box in Office 365. The dialog has a title bar with 'New user' and a close button. It contains several input fields: 'First name', 'Last name', 'Display name', 'Username', and 'Domain'. The 'Domain' dropdown is set to 'zohocorpadmhybrid.onm'. There is also a 'Location' dropdown set to 'India'. Below these are expandable sections for 'Contact information', 'Password' (set to 'Auto-generated'), 'Roles' (set to 'User (no administrator access)'), and 'Product licenses' (set to 'Decision required'). At the bottom are 'Add' and 'Cancel' buttons.

Figure 1: Using multiple tools to create users in AD and Office 365.

## 2. No provision for granular delegation.

The native Office 365 portal doesn't offer a way to assign individual tasks to specific technicians. As shown in Figure 2, these tools have a set of admin roles with a pre-determined scope of activity.

### Edit user roles

Choose the admin role that you want to assign to this user. [Learn more about administrator roles](#)

- ☐ User (no administrator access)
- ☐ Global administrator
- ☒ Customized administrator
  - ☐ Billing administrator
  - ☐ Dynamics 365 service administrator
  - ☐ Exchange administrator
  - ☐ Password administrator
  - ☐ Skype for Business administrator
  - ☐ Power BI service administrator
  - ☐ Reports reader
  - ☐ Service administrator
  - ☐ SharePoint administrator
  - ☐ User management administrator

Figure 2: Pre-determined admin roles in the native Office 365 portal.

## 3. Difficult to manage multiple tenants.

Working with multiple tenants using native Office 365 administration tools is cumbersome as it involves creating delegated admin permissions.

## 4. Limited Office 365 reporting capabilities.

Native Office 365 administration tools have limited reporting capabilities and lack important features like exporting reports in multiple file formats (only CSV files are supported).

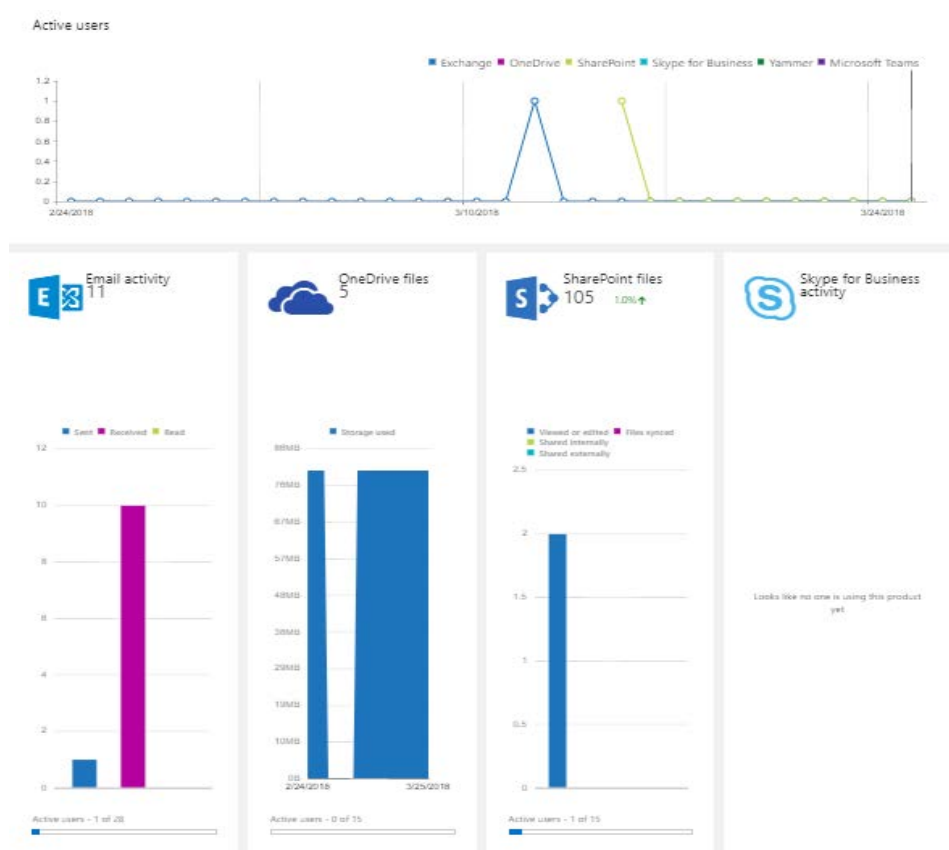


Figure 3: Limited Office 365 reporting capabilities.

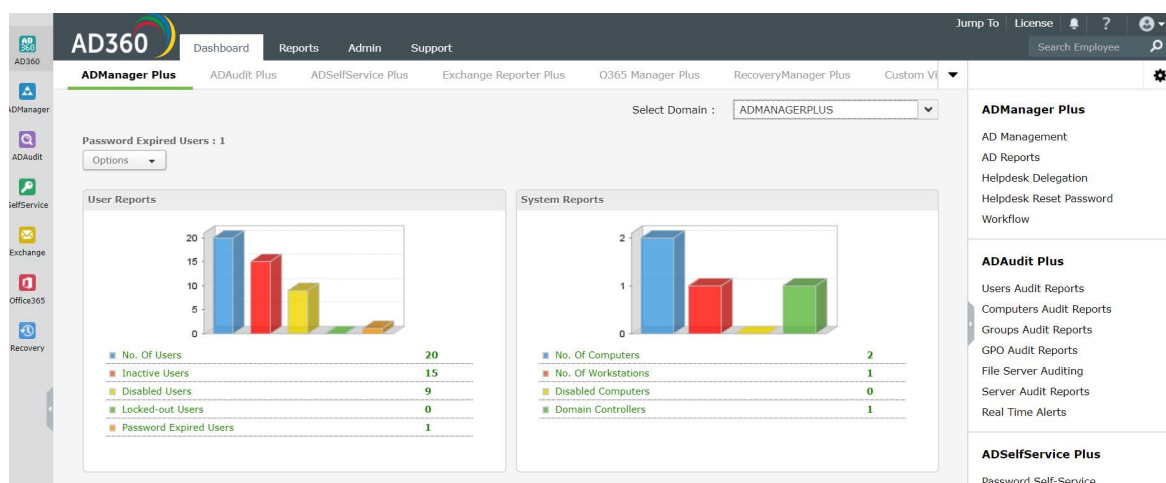
## 5. No provision to generate historical audit data.

Office 365 administration tools store audit log entries in the Unified Audit Log for only 90 days.

To overcome the shortcomings of these native tools, you need an Office 365 tool that supports all the above mentioned tasks and more. AD360 is one such solution that can meet your organization's management, reporting, and auditing needs.

# AD360—Your 360 degree Office 365 manager

AD360 is an integrated solution for any Windows environment's identity and access management (IAM) needs. AD360 automates all routine IAM tasks, including provisioning or de-provisioning bulk user accounts and other AD objects; securely managing account passwords; modifying multiple attributes of user accounts; and managing user mailboxes and their email traffic.



**Figure 4: AD360's console, with all modules and a customizable dashboard.**

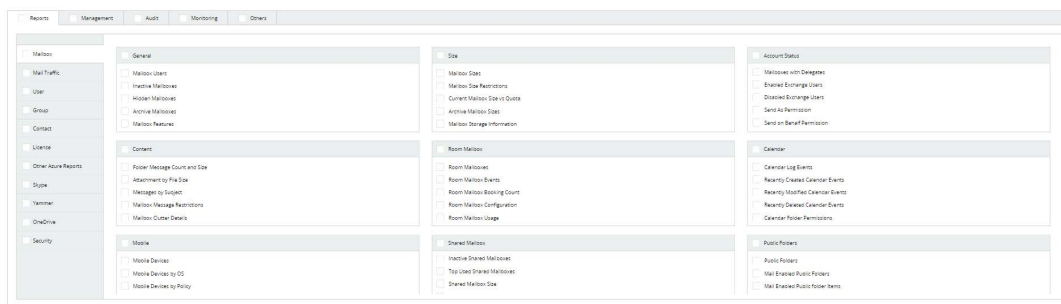
Using AD360, you can configure multiple tenants as shown in the figure below and perform management, auditing, reporting, etc. for any of the tenants from the same console.

Configured Office 365 Tenants

Actions	Office 365 Tenant	Account Name	Domains	Rest API Access	Status
<a href="#">Add New Tenant</a> <a href="#">Manage Licenses</a>	zohocorpadminplus.onmicrosoft.com	o365-demo@zohocorpadminplus.onmicrosoft.com	15 Domains	Enabled	Success

**Figure 5: Configuring multiple tenants in AD360.**

AD360 allows you to create custom role profiles for technicians so you can assign them permissions for carrying out a specific set of activities.



**Figure 6: Granular task delegation using AD360.**

Aside from these features, use AD360 to perform the following activities in your Office 365 environment:

- User provisioning
- License management
- Auditing
- Reporting
- Alerting

## User provisioning

AD360 supports bulk user creation in both AD and Office 365 by simply importing a CSV file with all the users' details. You can also assign Office 365 licenses to these users in the same CSV file. AD360 also lets you:

- Create user accounts by enabling or not enabling DirSync.
- Assign licenses to users and grant them access to certain applications.
- Automate user provisioning using customizable templates.



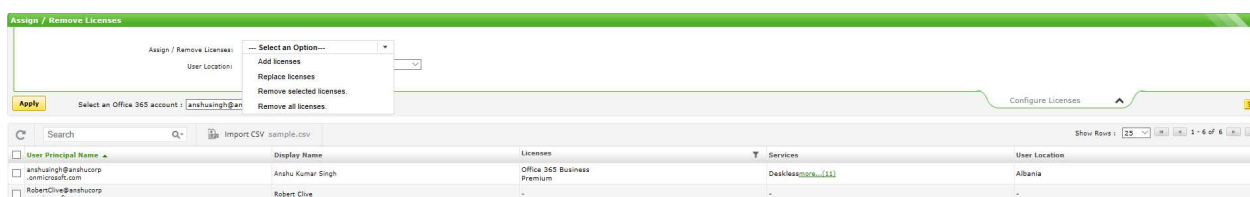
**Figure 7: A single console for simultaneous bulk user creation in AD and Office 365.**

[Learn how to create a CSV file for bulk user creation.](#)

## License management

AD360 helps you easily manage Office 365 licenses. It takes just a few clicks to:

- Add, replace, or revoke selected users' licenses.
- Bulk import a list of users from a CSV file and add, replace, or revoke their licenses.
- Delegate the task of provisioning Office 365 users and managing their licenses to help desk technicians.



**Figure 8: Bulk license management.**

## Reporting

AD360 provides a comprehensive set of reports covering almost all aspects of your Office 365 environment: licenses, admin activity, user security, mailbox security, passwords, and more. Aside from offering reports that can't be generated using native tools, AD360 also allows you to export reports as PDF, XLS, HTML, and CSV files.

### AD360's Office 365 reports can help you:

- Find which user has access to which mailbox and detect unusual mailbox accesses.
- Detect which users have accessed Exchange via Outlook Web Access and from which device.
- Find the top email senders and recipients in your organization, and detect which users have received malware and spam emails.
- View user mailbox usage statistics, including mailbox size and mailbox send and receive quota; compare a mailbox's current size with its maximum allowed size and more.
- View the complete audit trail of user activity in OneDrive for Business, with details on who performed what operation and when.

- Ensure IT compliance with standards such as SOX, PCI DSS, HIPAA, GLBA, and FISMA.
- See a breakdown of active users based on the Skype for Business features they've used.
- Check out Office 365 license assignment.
- Find users whose passwords have expired or are about to expire.

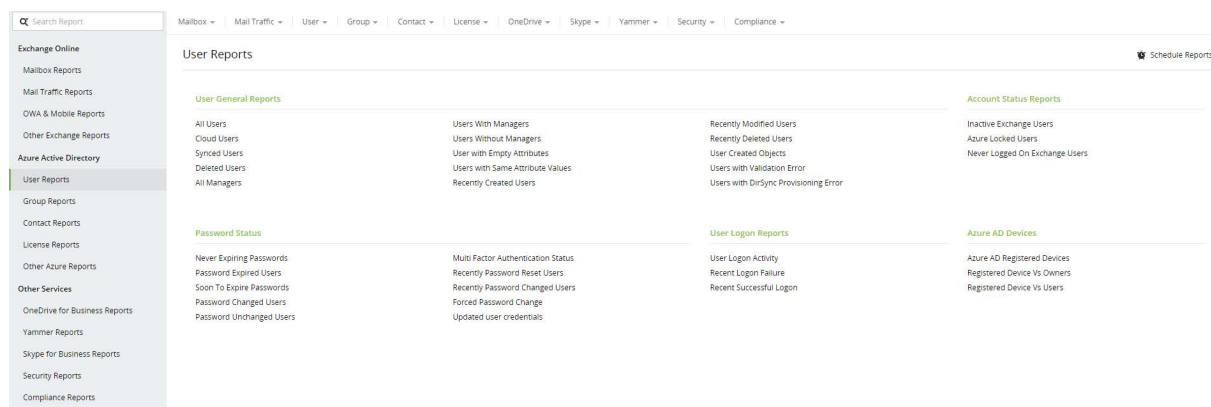


Figure 9: Comprehensive Office 365 reporting in AD360.

## Auditing

AD360 ensures data safety and compliance by letting you keep track of every event happening in Office 365.

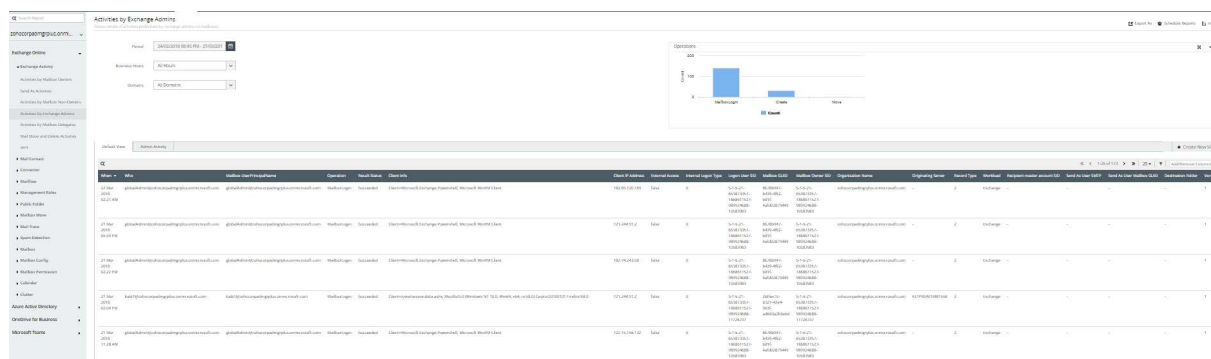


Figure 10: Auditing using AD360.

**It offers the following auditing benefits that aren't available in native tools:**

**Historical data:** Audit data is stored indefinitely in AD360; there's no storage time limit, like in the native Office 365 administration tools. This is crucial to determine if the changes made in your Office 365 environment conform with IT compliance regulations like SOX, HIPAA, and PCI.

**Profile-based auditing:** Create audit profiles that will fetch only those audit details you need instead of having to peruse the entire list of audit reports.

#### Profile Configuration

The screenshot shows the 'Profile Configuration' form. On the left, there are five input fields: '\*Profile Name' (text box), 'Description' (text box), '\*Office 365 Service' (dropdown menu showing 'Azure Active Directory'), '\*Category' (dropdown menu showing 'Azure AD license'), and '\*Actions' (dropdown menu showing 'Select'). On the right, there are two sections: 'Target Callers' and 'Target Objects', each with a green checkmark icon and two buttons: 'All' and 'Custom'. At the bottom center, there are two buttons: a green 'Add' button and a grey 'Cancel' button.

**Figure 11: Creating audit profiles in AD360 to fetch data for a particular event.**

**Group-based auditing:** Generate reports for user activity based on group membership.

**Advanced filtering:** Filter your audit logs based on any attribute and perform multi-valued searches.

**Multi-format audit reports:** Export your audit data to a PDF, XLS, HTML, or CSV file.

The figure below shows how AD360 monitors your Exchange Online, Azure AD, OneDrive for Business, Skype for Business, and other Office 365 services 24x7. AD360 also constantly monitors the health of your cloud setup and notifies you immediately about any service outages.

The screenshot shows the 'All Services Health' dashboard. At the top right, there is a summary bar with three colored boxes: a red box with a warning icon and 'Incident 1', an orange box with an advisory icon and 'Advisory 3', and a green box with a checkmark icon and 'Healthy 12'. Below this is a table with two columns: 'Service Name' and 'Health Status'. The table lists various services and their current health status.

Service Name	Health Status
Skype for Business	Incident - 1, Advisory - 1
Microsoft Teams	Advisory - 1
Yammer Enterprise	Advisory - 1
Exchange Online	Healthy
Office 365 Portal	Healthy
Azure Information Protection	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
Office Subscription	Healthy
Microsoft StaffHub	Healthy

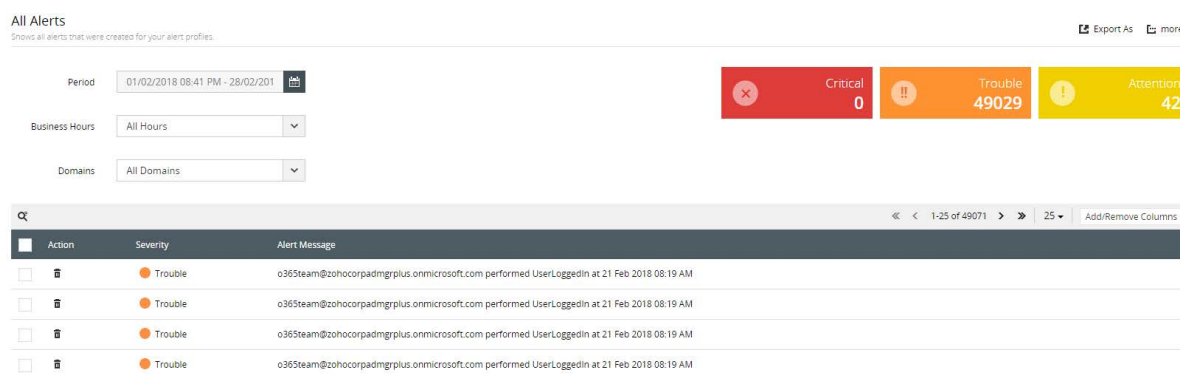
**Figure 12: Continuous monitoring of Office 365 services by AD360.**

## Alerting

Tracking events in Office 365 becomes even more necessary due to its anywhere, any time accessibility. But due to the sheer amount of Office 365 user activity happening every day, auditing alone can't help you keep up with all critical events. You need to configure real-time alerts to save time; AD360 has just what you need with its real-time alerting console.

Keep track of your Office 365 environment by creating alert profiles that send customized messages to administrators when a particular action happens in your Office 365 setup. You can include information on the severity of the activity, who was involved, when the event occurred, and more. For example, you can:

- Create a high-severity alert for when users disable malware filter policies. Email the alert and all relevant details to an admin so they can act immediately.
- Prevent users from deleting important files using a deleted file alert that notifies admins when a file was deleted, who deleted it, and more.
- Set real-time notifications for file sharing to avoid intentional or accidental data leaks.



**Figure 13: Alerting capability in AD360.**

## Summary

As an IT administrator, ask yourself the following questions:

- Can you simultaneously provision bulk users in Active Directory and Office 365 using your Office 365 administration tool?
- Does your tool allow you to create custom role profiles for technicians and delegate a specific activity or set of activities?
- Can you configure and manage multiple tenants from a single console?
- Does your tool store audit data indefinitely to help with IT regulatory compliance standards such as SOX, HIPAA, and PCI DSS?
- Are you able to send customized alerts to administrators when a particular action is performed in your Office 365 setup?

If the answer is no, [Download AD360](#) to experience 360 degree Office 365 administration.

## About AD360

AD360 is an integrated solution that takes care of identity and access management, IT compliance, and security of your AD, Exchange, and cloud applications. It supports user life cycle management; multi-platform user provisioning; single sign-on for cloud applications; password self-service; real-time auditing, monitoring, and alerting; and pre-packaged compliance reports. AD360 also allows you to automate or delegate common administrative tasks to help desk technicians while still retaining control through approval workflows.

[\\$ Get Quote](#)[↓ Download](#)

Toll Free  
+1 844 245 1108

Direct Dialing Number  
+1-408-916-9393



[ad360-support@manageengine.com](mailto:ad360-support@manageengine.com)



[www.manageengine.com/active-directory-360/](http://www.manageengine.com/active-directory-360/)