Surviving Office 365 Management Woes

An IT Pro's Guide

TO UNDERSTANDING THE (UNEXPECTED) CHALLENGES.

Quest

INTRODUCTION

Congratulations on the opportunity to move to Office 365.

In addition to the many benefits to your organization, this also provides an excellent opportunity to grow your skills and broaden your resume. While you may have a number of migrations under your belt, and perhaps a career's worth of experience managing on-premise Microsoft platforms, you may not have any hands-on experience with Office 365. Don't be dismayed – you're not alone. Office 365 deployments are still new, and there are many misconceptions.

What You'll Learn

Office 365 is Microsoft's fastest growing commercial product ever, helping organizations save money, become more agile and drive innovation. It will also bring new and unexpected challenges and risks for everyone in your organization. This eBook will provide insight into the many differences between Microsoft on-premise platforms and the new Office 365 platforms. With a solid understanding of the current gaps and challenges, this eBook will help you more than survive the experience, but to better migrate and successfully manage your new Office 365 and Azure AD environments in a way that serves internal clients and responsibly considers security risks.

BEFORE YOU GET STARTED: UNDERSTANDING THE CHALLENGES WITH OFFICE 365

Office 365 platforms differ greatly from the on-premise applications they're designed to emulate. These are completely new platforms and—in many ways—not what most IT administrators expect.

Simply put, many of the Office 365 platforms and native management tools lack the maturity of their on-premise counterparts. These differences become apparent in multiple areas, such as compliance auditing, recovery, provisioning and policy management. It's an unpleasant surprise for many IT administrators who have long-term experience with the on-premise Microsoft management controls, features and software tools.

> After migration, your job as an IT pro isn't done.

After migration, your job as an IT pro isn't done. In fact, managing Office 365 is where you'll deal with some of the most challenging aspects, and on a daily basis. IT administrators in the on-premise world were primarily a master of a single technology. But now they must learn and manage Azure AD plus multiple Office 365 workloads such as Exchange Online and Skype for Business. This rapid need to develop near-immediate expertise across multiple Microsoft platforms becomes an immediate challenge, and it's a tall order for IT departments already short on time and resources.

The knowledge gaps are compounded by the vast functional gaps in Office 365 and Azure AD security and administration features. Unfortunately, the native management GUIs simply don't scale past approximately 50 users. What should be routine admin tasks are manual, tedious and time-consuming processes that require clicking through seemingly unending screens to complete. Due to the limitations of Microsoft native tools, you'll need a number of work-arounds or third-party tools to effectively manage these new and growing Office 365 platforms.

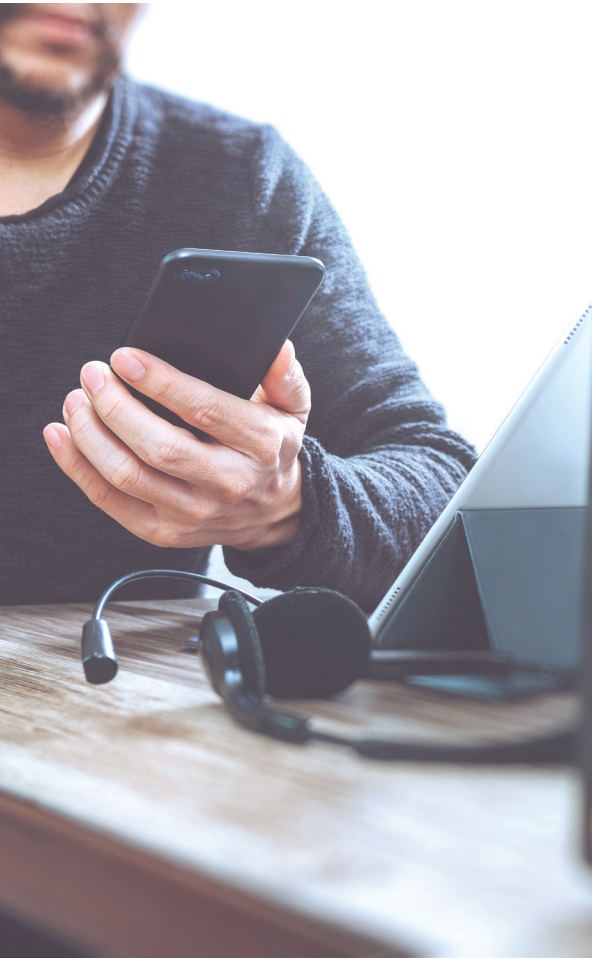
PRE-MIGRATION: THE BEST OPPORTUNITY TO BUILD YOUR ONGOING MANAGEMENT STRUCTURE

Your pre-migration preparation should take a big-picture approach to how your environment will be managed when it's completed. Often, IT teams are so focused on getting the migration completed that they fail to look ahead to how to optimize their future environment. Part of better managing Office 365 begins before the migration occurs. In fact, begin to think of your migration as a way to set up a solid management structure. You're creating a plan not only for the migration, but for the ongoing management of Office 365 and Azure AD.

Standard IT best practices guide you to architect your enterprise to achieve the desired performance levels and the reporting KPIs needed to monitor your success. However with Office 365, you just "sign up, migrate and use," leaving the administrator with limited ability to dictate the architecture. While this simplicity sounds appealing, you'll find the lack of functionality to be more of a curse than a blessing.

Key insights on building a thoughtful migration plan and timeline can be found in an eBook titled **"Surviving Migration to Office 365: An IT Pros Guide to migration, key considerations and critical processes to ease the pain."**

POST-MIGRATION CHALLENGES



Many IT administrators approach an Office 365 migration with the belief that Microsoft will handle many of the management and administration aspects. In reality, ongoing, post-migration management is your responsibility.

The native Microsoft management tools are cumbersome, with some IT pros reporting an extensive amount of time spent fulfilling common tasks. Be prepared for many manual processes, challenges conducting bulk operations and the need to work in multiple screens to accomplish tasks. In some cases for customers with hybrid environments, you'll find yourself hopping between on-premise tools and Office 365 tools – each with a different look and feel.

Navigating the complexities of the Office 365 environment introduces new workloads to manage and a new way of delivering service to end users. Many of your day-to-day responsibilities will be similar, such as help desk tickets and provisioning. However, Office 365 will force you to restructure your methods.

You can also expect an initial wave of helpdesk calls on the new and different look and feel of each Office 365 platform. Your business users will notice these differences and may need some hand-holding – requiring you to rapidly broaden you skill set on the fly. The more you can automate IT tasks, such as provisioning, the more time you'll have to answer helpdesk request and guide end users through the adjustment period.

BACKUP AND RECOVERY FOR OFFICE 365 AND AZURE AD

IT Pro Tip

LIMITATIONS OF THE AZURE AD RECYCLE BIN

The Azure AD Recycle Bin operates differently than you might expect.

Limitations include the inability to execute a bulk modification restore – slogging away at one object at a time. The Recycle Bin also will not allow you to restore Azure or Office 365 Groups or Group Membership, and does not enable backup and restore across Office 365 tenants.

Whether you're in the middle of a migration to Office 365 or have already moved, back-up and disaster recovery strategies should be an important part of your ongoing management plan.

Email backup and recovery is critical, as it's the primary communication and productivity tool for every user, every day. Be prepared to handle email recovery issues such as:

- Access to old mailboxes.
- Internal and external investigations.
- Recovery of accidently deleted messages.

When it comes to Office 365 or Azure AD users, groups and group memberships, this data is equally important. But Microsoft's native restore tools are time-consuming, recovering one object at a time. And the Recycle Bin, if you choose to activate it, empties after 30 days. And don't count on restoring previously "hard-deleted" files. Any Azure AD objects that have been hard-deleted (by-passed the Recycle Bin) cannot be restored – they are lost forever. In fact, when groups are deleted in Azure AD, they don't even go to the recycle bin. It's a hard delete and there's no way to get that back with native Microsoft tools.

REPORTING

Reporting and auditing is a critical function for virtually all IT operations. While Office 365's reporting features are lacking in some areas, Exchange Online offers the most mature capabilities. While full tracking logs aren't available, administrators can view and report in a manner similar to the on-premise version with:

- **MAILBOX OWNERSHIP**
- **LOCATION**
- **CONTENTS**
- **ACCESS DATE/TIME**
- **USAGE DATA**

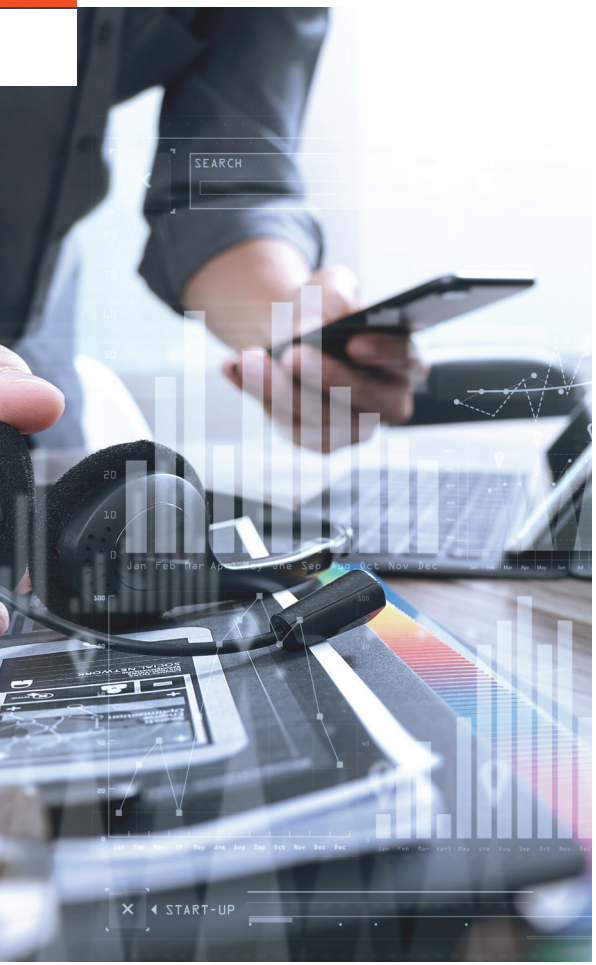
Each platform's reporting capabilities differ greatly in Office 365, and the API maturity on each platform is different, as well. In some cases, you'll receive granular data points allowing you to run intelligent algorithms for exception reporting. In other cases, you'll be limited to dashboard-like information.

Typical usage reports lack important information, such as:

- The user's identity
- Long-term trends – Reporting is limited to just 180 days, you're in the dark beyond that period
- Historic details at the user level: Cannot see what the files, storage, or information was at a given point in time.
- No ability to see permission on aggregate level

Some of the reporting gaps can also have significant effects on compliance, security and your efficiency in managing Office 365 on a daily basis. Some examples of security and administration challenges include:

- **No permission baselines:** Office 365 offers no visibility into who has access to what, how they received the access, who has elevated permissions and which systems are vulnerable to security threats.
- **Limited compliance auditing:** Native Office 365 and Azure AD auditing tools are difficult to configure and interpret, lack real-time alerting of suspicious activities and retain logs only for a limited time before they're lost permanently. This lack of governance and visibility hinders an organization's ability to meet compliance regulations.



AUDITING

Microsoft's native tools also make it difficult to configure auditing. For example, you must configure it one mailbox/object at a time, and there is no way to automatically configure new mailboxes/objects with the desired audit policy. Change reporting and access logging for Azure AD and enterprise applications is time-consuming and, in some cases, not possible using native IT auditing tools. This creates exposure to data breaches and insider threats to Azure AD and other Microsoft platforms, and can go undetected without protections in place.

The limited auditing capabilities present multiple challenges, including:

- No way to monitor audit policies in case they change or are disabled by other administrators
- The audit data is very raw and lacks friendly display names and the format is constantly changing
- There is no normalized 5W format (Who, What, When, Where, Workstation/Origin) so that the event format is the same regardless of what event or workload
- Audit data is spread across multiple platforms and formats
- Need to look at multiple areas for auditing information – no way to pull both on premise and cloud activity into one view

Native tools also only offer limited, non-real time alerting, with only a finite number of alert actions at present. And while storing history of audit data is critical for most internal security policies and external compliance regulations, Office 365 tools only offer a limited history of audit data, held short-term then permanently lost. While the retention period varies based on workload and subscription type, it can be as short as 7 days, and Microsoft can change retention periods at any time.

PROVISIONING AND ACCESS MANAGEMENT

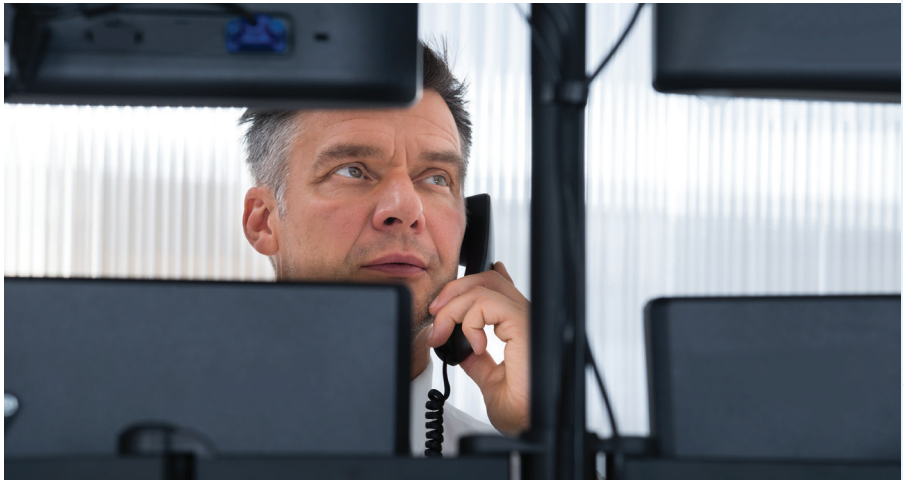
IT Pro Tip

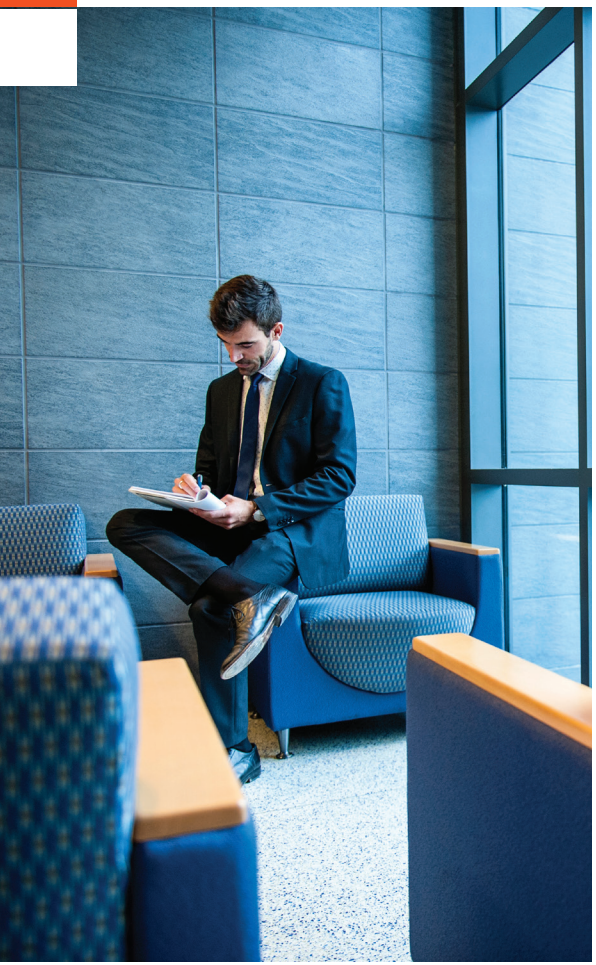
TIME TO SHARPEN YOUR POWERSHELL SCRIPTING SKILLS!

Since Office 365 lacks a proper UI for many operations, you'll may need to fall back on much-dreaded PowerShell scripting for multiple tasks, such as creating new Active Directory users. Windows PowerShell was built to bridge the gap between developers and administrators. However, its cumbersome interface often makes operations even more time-consuming. Administrators who have forgotten PowerShell scripting commands, and those less experienced with PowerShell, should consider third-party tools to automate Office 365 management tasks and drastically increase efficiency.

The functional limitations of Office 365 and Azure AD native tools are noticeably apparent in provisioning and privileged access management. User access requirements are in constant change, and there's no way to dynamically provision access across hybrid directories and applications.

In Office 365, the tedious, error-prone manual provisioning native tools require multiple disparate interfaces. This creates disjointed security policies, leading to data breaches or penalties and fines from being out of compliance.





LICENSE MANAGEMENT

The C-suite always has an eye on the bottom line, and appreciates new efficiencies. IT administrators can play a key role in cost control by actively managing Office 365 subscriptions. Poor license management can increase costs by paying for unused licenses or consuming premium SKUs when users aren't fully utilizing the included features.

In your ongoing management of Office 365, you'll need to track mailbox usage and storage trends, report on which Office 365 subscription and services users are entitled and discover inactive accounts that can be removed. These are new manual processes you'll need to add to your ever-growing list of Office 365 management responsibilities, since there are no native automated reporting on license utilization tools.

When evaluating your license needs and potential cost savings, the ability to run these key reports will help greatly with your decisions:

Office 365 mailboxes

- Usage / trends
- Activity / inactive mailboxes
- File attachments
- Storage

Office 365 user subscriptions

- What subscription does each user have? (Azure AD Premium, E1 vs. E3 licenses)
- What O365 services does each user have? (Exchange Online, SharePoint Online, Skype for Business, etc.)
- Inactive users

SECURITY

IT Pro Tip

BEWARE OF HYBRID AD SECURITY RISKS

Using Office 365 requires an instance of Azure AD, but 75% of organizations with more than 500 users sync AD on-premise with Azure AD, creating a hybrid AD environment. This scenario can lead to dangerous gaps and crippling inefficiencies. If you're running a hybrid environment, you face all the security limitations of native AD plus those of Azure AD, doubling the surface area you must manage to prevent potential data breaches and insider threats.

Detailed insight on negotiating Office 365's security challenges can be found in an eBook titled **"Surviving Migration Surviving Common Office 365 Security Pitfalls: An IT Pro's Guide to Securing Your On-Premise Active Directory in a Hybrid Environment."**

Managing security in Office 365 has similar attributes to managing security on any Microsoft system. Your previous security tasks – establishing and enforcing policies for access to resources, creating and decommissioning end user accounts with appropriate delegation and permissions, making sure Active Directory can be audited – will remain. However, you must be prepared to manage around Office 365's security gaps to mitigate your exposure.

For instance, post-migration many IT administrators will synchronize their on-premise AD with Azure AD, creating a hybrid AD environment. In this scenario, the on-premise AD provides authentication and authorization services. This represents a significant liability: **If AD isn't properly secured, Office 365 will also be at risk**.

Despite common misconceptions – Microsoft will not assist with this scenario. While you may expect that a cloud deployment means less ongoing management, Azure AD management remains your responsibility. Take control of your hybrid AD infrastructure to improve security for both the on-premise and Azure AD. As you build your Office 365 AD security strategy, begin with these four concepts:

1. **Assess:** Understand who has access and permissions to which sensitive data
2. **Detect and Alert:** Monitor for suspicious activities, including insider attacks
3. **Remediate and Mitigate:** Remediate unauthorized actions across AD and Windows immediately
4. **Investigate and Recover:** Understand how these incidents occurred to reduce future response time and further liability

HOW CAN QUEST SOFTWARE HELP?

Tools and assistance are available to better manage the gaps in Office 365. With nearly two decades of Microsoft platform migration experience, Quest enables organizations to overcome gaps in Office 365 and Azure AD. Quest has a world-class network of experts and partners combined with an end-to-end portfolio of solutions to help you efficiently migrate and manage your Office 365, Azure AD and hybrid AD environment into the future.

Award-winning Quest tools have been used to migrate, secure and manage more than 180 million users, and can help with your needs data across on-premises, cloud-based and hybrid platforms.

Quest's sophisticated tools will enable you to overcome Office 365 gaps and bypass PowerShell scripting to better:

- Execute your migration.
- Manage your new environment in a centralized manner.
- Automate administrative tasks and deployment activities.
- Ensure your Office 365 migration is efficient and data is secure.
- Get complete visibility into your environment with enhanced reporting and auditing capabilities.
- Recover, restore and back-up Active Directory (on-premise and Azure) as well as missing files.

With nearly two decades of Microsoft platform migration experience, Quest enables organizations to embrace Office 365 and Azure AD without the burden of crippling costs, risks, fear or uncertainty. Learn more about how Quest can **plan, migrate and manage your Office 365 environment for success.**

Quest

Join the Innovation.