WHITEPAPER

16 Microsoft 365 Tasks Easily Automated with Workflow

CoreView

Now It's Under Control

Contents

Introduction

How many tedious manual tasks must a Microsoft 365 administrator complete, leading to tears of frustration and errors they may be held accountable for, before they are forced to concede?

This pain stops by figuring out how to do a task perfectly, then automating it through a repeatable, reliable workflow. Then do the same for all your repetitive tasks. By automating admin tasks through workflow, which includes on-premises Active Directory tasks, IT administrators save hours of manual effort each week – time better spent for more productive and satisfying endeavours.

Even better, everyone can use the same workflow and do the task perfectly. No more going to the onboarding expert or scratching your head when that person leaves the company! Now common Microsoft 365 admin tasks can be easily delegated – even to non-IT pros. This is the beauty of delegated administration.

Get to Work on Workflow

Microsoft 365 doesn't come with administrative workflows built in. Fortunately, CoreView provides a workflow solution that allows for easy creation and customization of workflows to automate and run IT administration processes – often in one click. These automations can reach towering levels of complexity, as many different steps are chained together and performed in the appropriate and exact sequence.

All M365 management actions can be accomplished through a workflow, including custom PowerShell scripts, opening the door to unlimited automation scenarios. CoreView's workflow capabilities allow for the automation of myriad actions across a variety of M365 workloads – account management, license administration, security and compliance processes ... there are even options for extending the out-of-the-box options with Custom Actions.

Workflow is critical for one CoreView customer. "We view CoreView as experts in the field that can guide us to the most pertinent parts of the M365 ecosystem and integrate best practices into workflows," said Tobin M. Cataldo, Executive Director – Jefferson County Library Cooperative.

TOBIN M. CATALDO
Executive Director
Jefferson County Library Cooperative

Automating the Automation

Workflows can be automated in two different ways: Report-Based Workflows and Event-Based Workflows.

Report-Based Workflows are initiated by reports, and automatically perform predetermined actions to address the situation.

Event-Based Workflows on the other hand, are triggered by risk events such as an attack on a user, and then take the appropriate action.

By automating the automation, organizations can ensure that the right action is taken as soon as a risk is detected. **CoreView Playbooks** are a set of automation tools that can be used to implement both Report-Based and Event-Based Workflows. They allow organizations to quickly and easily define the appropriate actions to take when a risk is identified and automate the entire process to ensure that the right action is taken as soon as a risk is detected.

SECTION ONE

Security

1. Simple and Superior Security

Dealing with security alerts, as well as creating security policies, and ensuring compliance requires the creation and performance of complex repetitive tasks. Workflows make protecting the environment orders of magnitude easier. For instance, CoreView may detect that a file was downloaded from OneDrive that shouldn't have been. With a workflow, an automated remediation task could be tied to that event trigger, such as disabling that account or alerting an administrator.

2. Dealing with Risky Users – Security Orchestration, Automation and Response (SOAR)

Microsoft 365 includes risk reports showing what events IT should look into, and in many cases, which users may have been compromised. Here is an example of a four-step workflow to use in such a case:

- Wipe user session
- Disable user
- Quarantine device
- Notify IT Security

3. Event-Based Password Management

The new way to handle passwords is to not require regular expiration and resets – but only change passwords when there is a risk alert. While risk or event-based password changes are a great idea, execution isn't so easy. "What CoreView has, which is completely unique in the industry, is we know that you're on that risk report, and we can schedule the changes: Since you're on it, I'm going to wipe your user session. In other words, log you out of all your applications. I'll reset your password, notify the help desk, and notify IT security that Joe User was on a high-risk report for impossible travel, and please check A, B, and C before you re-initialize his account," explained CoreView Solution Architect Matt Smith.

4. Event-Based Password MFA Management

Like passwords, MFA can be dealt with based on risk events. “IT should enable risk-based multi-factor authentication activation. If you’re at risk, IT will make you authenticate. CoreView takes this a step further, which is part of our workflow. IT can wipe user sessions. Because a user token is good for eight hours by default, should IT allow the user to keep pounding on it for eight hours? No, IT should log them out right now, because they showed up on a high-risk report. An admin can block the account and notify IT security and the help desk because you showed up on an impossible travel report or malware on a device report, something like that,” Smith explained.

MATT SMITH
Senior Solutions Architect
CoreView

5. Keeping M365 Safe from Sketchy Mobile Devices with Workflow

Mobile devices are a prevalent M365 endpoint, so security here is paramount. Managing, tracking, and acting on mobile device issues can be automated through CoreView workflows.

Case in point is a recent iOS vulnerability. To handle this, CoreView admins were given a workflow to identify iPhones with an older OS, or still using the IOS Mail App, and update iOS or move users off the iOS Mail App.

Knowing that these iOS MailDemon attacks are in the wild with millions of non-updated iPhones and countless folks using the iOS Mail App, CoreView co-founder David Mascarella rushed out a KPI to identify and delineate the issue, and an automated workflow that solves the problem tout de suite.

“I created a policy that identifies the devices affected by this vulnerability. If we select the policy that dives into the data, the system will automatically target the users that are affected. We do that by targeting all users with mobile devices, with the operating system equal to iOS, with the versions that do not include 13.5,” Mascarella explained.

The KPI and workflow then suggest management actions an operator can perform in order to disassociate these mobile devices from the tenant, and also run a workflow.

“When you run the workflow, the system automatically targets all of the affected users, and sends an email — there is a description of the problem CoreView detected, that you are accessing your email with an unsafe client. You have to update your mobile device. To learn how to update your mobile device operating system, please look at this video. There is a link to a helpful video that shows how to update the device,” Mascarella said.

The workflow offers several ways to remediate the iOS problem. We mentioned sending an email advising an end-user to update iOS or switch off the iOS Mail App. It can also remove the device.

Finally, the workflow can automatically enforce an iOS security policy. IT can have a report showing which devices are still not secure, and run the report, say, every Friday. If the report is empty, there is no problem. “Every Friday the system will check if we still have a user who has not updated their device. Then the system will engage the user and alert them to update their system. You can also make these workflows more active and run these workflows every day. You can also deactivate the mobile device, and remove the mobile devices and the email client,” Mascarella said.

DAVID MASCARELLA
Co-founder & Chief Global Strategist
CoreView

6. Safe, Secure, Proper, and Always Perfect Provisioning

User provisioning and deprovisioning are prone to error, allowing successful cloud attacks. Workflows allow for easy creation and automation of complex provisioning and deprovisioning processes, eliminating these mistakes. This ensures users have the right licenses and access to the right applications and infrastructure. You can also “clone” users to reduce errors and speed provisioning.

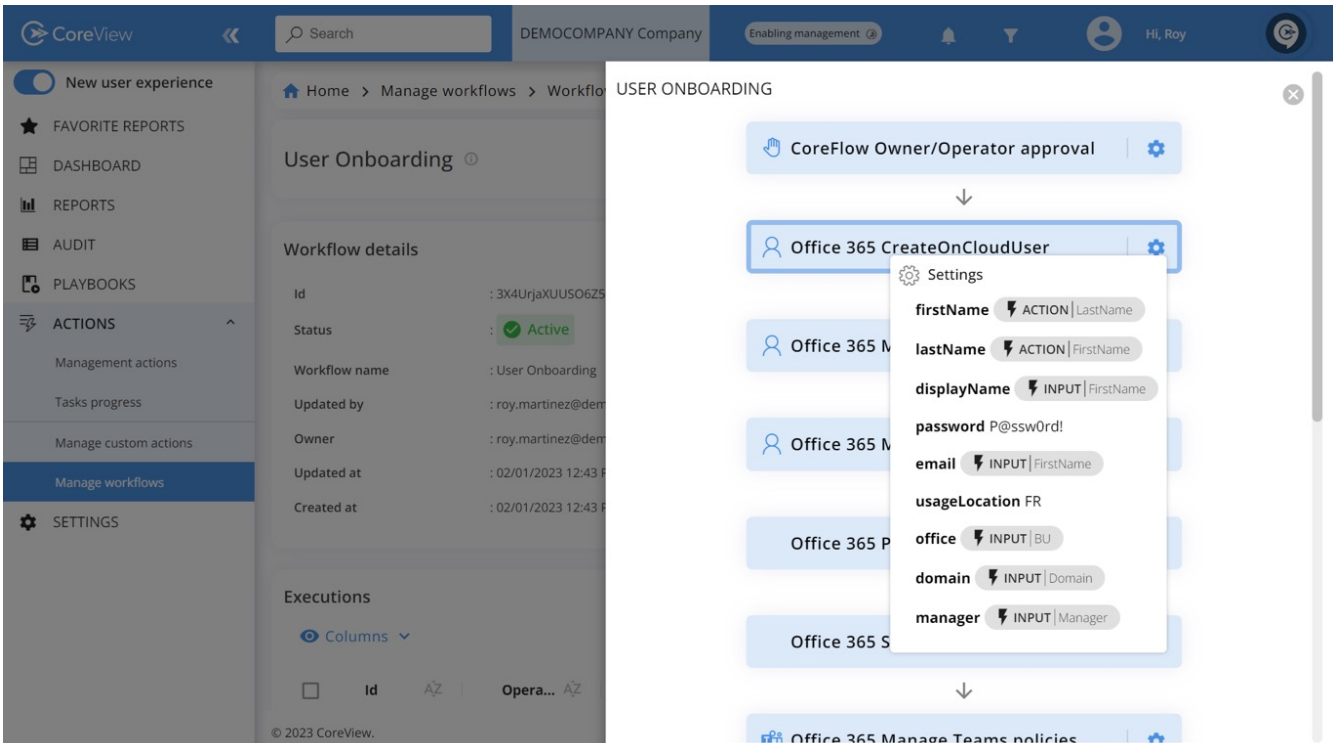
Incorrect user provisioning can have a direct impact on user productivity, while mismanaged deprovisioning can open the doors to potential data breaches.

7. Efficient and Secure Onboarding

Onboarding and provisioning are related and complementary processes. Onboarding is much the same as provisioning. It is just more extensive. Technically, provisioning refers to the creation of the user object. Onboarding is all the stuff that takes place outside of that user creation.

Onboarding speaks to the authorizations and permissions that are then bound to the object. We might say that a provisioning action is creating the user, giving that person a license, and setting the password. The onboarding is everything else. That person now needs to be inserted into 10 distribution lists, needs to be given a pre-provisioned OneDrive share, or has a script run against them to turn on their access.

"If we have to onboard a user, we can create a fully automated workflow. Inside our own company, we have a 50 – step workflow to onboard a user – and it's one click," said Ivan Fioravanti, CoreView Chief Technical Officer. "I create a user, assign the Teams membership, group membership, create the mailbox, and so on – it is super easy."



Inside the Onboarding Workflow

8. Fool and Hacker-Proof Configuration

According to Gartner analyst Neil MacDonald, "Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities."

In fact, a large number of data breaches are because admins did not complete all required configuration steps, and misconfiguration arises. With a workflow based on a proven and perfected configuration process, regardless of what is being configured, mistakes are never made again.

CoreView workflow eliminates that human error and ensures that all the dependencies are met. Moreover, it guarantees that desired configuration management practices are met which is critical for setting up user accounts and other data assets like mailboxes, shared mailboxes, and Teams channels.

Gartner finds that most successful cloud attacks exploit misconfiguration. Once you have a secure approach to configuration, map it to a workflow so it is done properly each time.

Customizable IT admin processes can be run from the workflow engine. Steps can be chained together so they are performed in the proper sequence. Management actions can be part of a workflow, including custom PowerShell scripts, leading to unlimited scenarios.

9. Safety Proof External Users – Govern the Lifecycle

From CoreView usage stats, we have found that 90% of external users become inactive after 90 days. With automation, you can automatically block access and remove the user, or ask consent of the person or the manager who invited them. Any active account is an additional endpoint opened on your tenant.

As an example, a workflow automation might identify external users inactive in the last 60 days and automatically start a process of clean-up with approval. Another workflow could force employees to add detailed information when an external user is invited (such as department, company, manager, country, or validity). The workflow would then take care of removing the invited user or renewing them based on a customizable approval process. Putting several workflow policies together into custom Playbooks allows for precise optimization of compliance strategies. The possibilities and use cases are virtually limitless!

Adding Workflow automation to the external user equation makes it faster, easier and safer to perform external user processes. Chief Technology Officer Ivan Fioravanti detailed how CoreView does this work. “Maybe you do not want the M365 operator to go manually through all the external users. A second way is to run a workflow. Built into the platform we have Workflow, which does business process automation,” Fioravanti said.

Meanwhile, workflow scheduling is flexible and easy. “Maybe we want a Monday morning habit of dealing with external users. You can schedule the ‘Inactive External User’ report, and have IT alerted if it is not empty. So, you choose every week. The action is that the workflow will automatically execute and send an email to the manager asking to remove the external user. You can always re-invite an external user that has been removed,” Fioravanti said.

Workflow adds to external user security. “Everything is extremely secure. You can create a workflow that will only be visible to specific users, and specific operators of the platform. Using RBAC and virtual tenants, only that operator can see and use that workflow,” Fioravanti said.

IVAN FIORAVANTI
Co-founder & Chief Technology Officer
CoreView

SECTION TWO

Administration

10. Protect and Update Active Directory Automatically

Managing Active Directory and Azure Active Directory (AAD) is a constant and complex effort. Fortunately, common tasks, whether Azure AD or on-premises Active Directory, can be automated, ensuring they are done correctly and on time.

By automating admin tasks through workflow, which includes updates to the on-premises Active Directory environment, IT administrators will save hours of manual effort each week. One customer automates an array of directory-related tasks, including:

- ✓ Adding a remote user from an Organizational Unit (OU)
- ✓ Creating an M365 user from Azure AD
- ✓ Moving group to a different Organizational Unit
- ✓ Moving user to different OU

11. Create, Enforce, and Manage Policies

Policies are key to M365 administration efficiency and security. Wouldn't it be great to create, automate and apply unique automation policies that handle various aspects of Microsoft 365 administration?

You can. The same large CoreView customer referenced above uses myriad workflows for policies, including:

- ✓ Setting conditional access policies for users outside the country
- ✓ Forcing changed password on next login
- ✓ Reactivating compromised account
- ✓ Managing SharePoint external sharing policies

Now, with the advent of CoreView Playbooks, setting up and managing these policies is even easier!

12. Workflow Gets Dependencies Right Every Time

It is not reasonable to expect a non-expert in Microsoft 365 administration to understand the dependencies involved in a task. Take mailbox administration. You have to create a user before you can create a mailbox, which seems obvious. However, there are many layers of subtleties beneath that. You need to wait until the mailbox is fully created before setting a litigation hold or retention policies on it, and so forth.

Workflow helps to get all these dependencies right and can even put in the requisite waits and retries, which are important because M365 is a shared environment of well over 300 million users. Things do not often happen instantaneously within a system as large as Microsoft 365. To set up mailboxes right, you must know the exact commands to operate, and the order that they needed to be operated in. In practice, people sometimes start the task and then must wait – 15, 30 minutes, an hour – for, say, step three of seven to complete. So, they switch to another task, and critical step number four never gets finished due to human error.

A workflow can be designed to know all the intricacies and dependencies – and get the job done right.

13. Taking the Trickiness Out of Teams

Workflow is also key to solving the Teams configuration problem. To set up Teams properly, certain tasks must be performed in order. In the case of Teams, a higher-level admin can create workflows to set up Teams-oriented voice functions such as routing and provide that to local employees that simply apply those workflows and those processes to their own environments.

With CoreView workflow, these local workers or admins get a form to fill out instead of waiting on a person to execute that form. CoreView workflow automates the process, so it is much timelier and more straightforward. IT defines exactly what data is needed to process the request and CoreView workflow processes that request efficiently and precisely.

A person needing to set up Teams' voice features in Spain, for instance, could use a form provided by higher-level admin, and apply that to setting up call features such as auto attendant for their organization, department, or group of users. Even better, this workflow is available on-demand, 24 hours a day, seven days a week in their language. There is no need to pick up the phone or translate user requests.

14. Automate License Management

License management is a complex, but necessary task. A great approach is to create and automate a process to reclaim licenses when a user becomes inactive, or ask approval from the manager or IT, or start the process to buy additional licenses, OR automate the request to your LSP through a workflow when a usage threshold is reached.

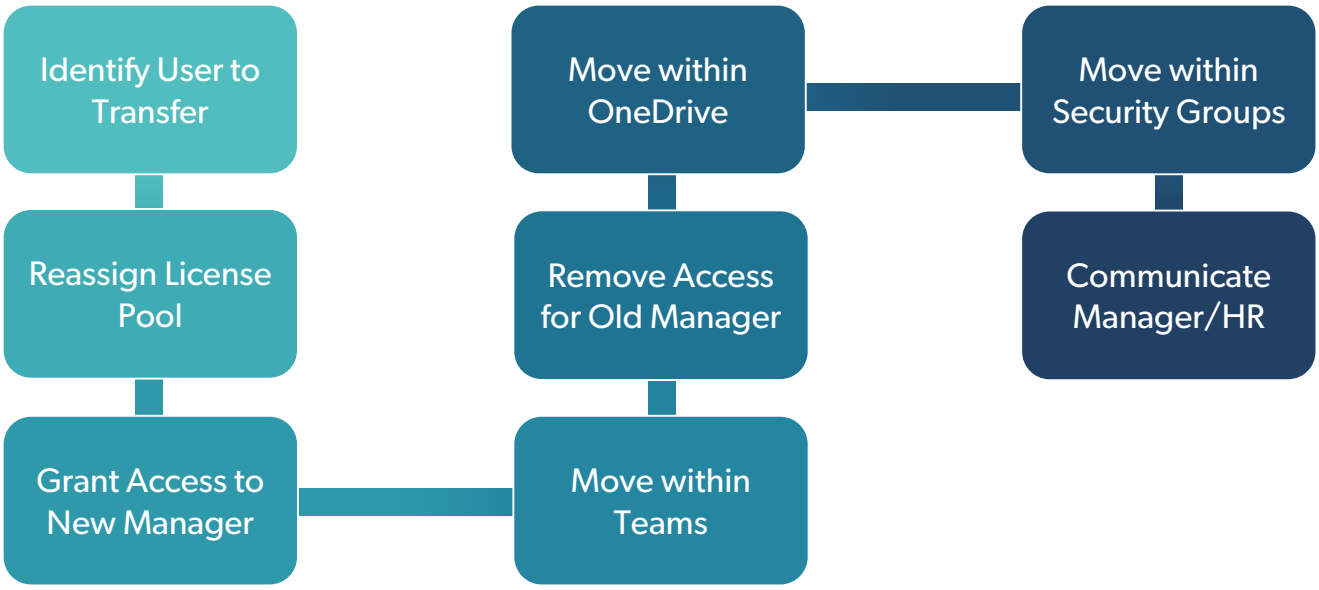
Here is an example of such as scheduled workflow. Every month it targets users with inactive licenses in the last 90 days then:

- Send an email to the manager asking if IT should remove the license
- If the manager is not the right person, send the request to HR or other target
- If the answer is yes, remove the license

Usually, IT does not have enough information to decide if a license must be removed or not. Managing this process manually can be very time-consuming – often IT simply decides to do nothing. The workflow, on the other hand, speeds up inactive license deprovisioning by the actual manager who should know if the license must be removed or not.

15. Transferring a User in 7 Easy Automated Steps

Transferring a user is tricky – doing so for an admin or manager is even more thorny. The graphic below shows how easily a CoreView workflow gets the job done



Transferring user, as Microsoft admin

SECTION THREE

One CoreView Customer's Workflow Story

One CoreView customer has 51 different automations (and counting) leveraging a variety of management actions incorporated into workflows. Here are some of the best

- Creating O365 user
- Display or hide a user in the global address list
- Conditional access for users outside of the country
- Add or remove a user (with a specific title) from an Organizational Unit (OU)
- Changing the main email address and UPN
- Change password
- Change state ID
- Change immigrant ID
- Change language for a mailbox
- Create an M365 user from Azure AD
- Create a meeting room
- Create an external mailbox
- Create a contact
- Create/Manage groups (distribution, security, M365)
- Move group to a different Organizational Unit
- Move user to a different Organizational Unit
- Disable cloud/sync/on-prem account
- Disable user
- Deactivate MFA
- Unassign licenses
- Merge 2 mailboxes
- Manage Teams Voice
- Change licenses
- Update user (custom attributes)
- Force change password at next login
- Change custom attributes
- Reactivate compromised account
- SharePoint – Manage admins
- SharePoint – Site provisioning
- SharePoint – External sharing management
- Restore deleted SharePoint site
- Delete SharePoint site
- Delete User
- Delete user but keep a shared mailbox

WorkFlows with CoreView

Challenges

- Common tasks like provisioning and de-provisioning users are time-consuming, tedious, and prone to errors, angering users, and increasing support desk calls
- Incomplete or late de-provisioning of departed users creates security risks and wasted spend
- You want to automate everything you can, but the tools available are too expensive or just too cumbersome

Results with CoreView

- ✓ Automate common business processes like user provisioning, de-provisioning, and cloning; workflows that alert and allow actions from reports
- ✓ Automatically scan configurations and activities to identify problems and enforce policies
- ✓ Easily automate tasks using the visual workflow builder that incorporates approval management steps, custom scripts, and more

About CoreView

CoreView cuts the chaos and gets Microsoft 365 under control. The CoreView Microsoft 365 Management Platform helps IT teams get full value from their Microsoft 365 investment, gain full oversight of their environment, and move at full speed. More than 25 million users and the world's largest organizations rely on CoreView to craft perfect privileges, eliminate wasted licenses, drive adoption, and automate repetitive tasks. A Microsoft Gold Partner, CoreView is Co-Sell Prioritized and available on the Azure Marketplace. CoreView | Now It's Under Control. Learn more at CoreView.com and follow us on Twitter and LinkedIn.

sales@CoreView.com

+1.800.436.8183 (US)

+39.028.725.9395 (EMEA)

www.CoreView.com