OSIRIUM AUTOMATION

Solving the Active Directory Management Challenge

OSIRIUM

Contents

Introduction

Microsoft Active Directory (AD) is the de facto standard for user and device directory management in medium to large enterprises. It is estimated that 90% of the Global Fortune 1000 depend on AD as their primary authentication and authorisation system.

AD is a critical part of the IT infrastructure. As it's the central point of authentication across all IT services and devices, it needs careful management. Admins must make accurate updates to accounts to ensure continuity of business operations and reduce the risk of attack. The right users must be members of the right groups to access the right systems to do their work. It is also vital that AD account updates are managed carefully to ensure attackers can't grant themselves permissions or remove permissions from users.

The management tools supplied with AD are powerful but complex. The result is that any updates, and there are many every day, are performed by trained experts. That makes the changes expensive. The experts are always busy, and any delays can prevent users from getting on with their work. Over-stretched experts ("administrators") end up spending too much time on trivial tasks such as resetting passwords rather than projects that deliver on corporate strategy.

This book looks at the most common AD management tasks and how to automate those jobs. With secure automation, organisations delegate everyday AD tasks to the IT Help Desk Engineers (or even to line-of-business users). That frees valuable expert resources, improves service, and reduces the risk of cyber attack.

Microsoft
Active Directory

Meet ADA

Introducing the automated assistant for AD management

In this book, we'll introduce you to the Osirium Active Directory Assistant, also known as ADA. In reality, ADA will be a set of automated playbooks or tasks for AD. These playbooks capture your AD expert's experience so that AD operations are performed according to best practice and in compliance with corporate policies.

With that experience, ADA is the specialist assistant for your AD administrators that can take care of the routine tasks they perform every day. A rich set of pre-built AD playbooks are available for free in the Osirium Automation Resource Hub to get you started as quickly as possible. You can extend or build news skills for ADA to match your needs.

ADA is just one example of the assistants that could be built with Osirium Automation. Visit www.osirium.com/automation for more examples.

Typical challenges with Active Directory

AD – the gateway to the business

When a user logs in to their workstation, accesses a database, connects to VPN, or performs any one of a hundred other regular business operations, they will be interacting with AD.

At its simplest, AD will be validating that the user is the person they claim to be. Typically, that will be by providing a username and password that are set for that account. Often this is augmented with add-on systems to improve security, such as multi-factor authentication.

The next job for AD is to determine what that user can do. Permissions are defined by the user being allocated to AD “groups” – essentially a way to group user accounts that have similar requirements for access to applications or devices. These groups allow policies to apply to the whole group rather than applying to each user. For example, all marketing team users may have access to a customer database or all users on floor 2 of the Munich office share the same printer.

That’s certainly a time-saver for the AD admin, but it introduces a new set of challenges. To align with the flexible nature of the business, AD groups proliferate. Often, groups need to be sub-divided to have more granular control, leading to inherited permissions, which are particularly hard to track and manage.

With constant changes as a result of starters, staff departures and moving between teams, the AD accounts and groups are rarely an accurate reflection of the business. That means accounts are left open when they should be deleted, or users can access systems they no longer need. Any effort to validate and cleanse AD becomes extremely expensive.

Typical challenges with Active Directory Continued

Who owns AD security?

Suppose an attacker can access AD and the credentials of the users. In that case, they could impersonate those users to access corporate data or systems. Alternatively, they could create new users or elevate permissions on existing, compromised accounts to access the business's most valuable data and systems.

Because AD is central to everything in the IT estate, AD's security should be a high priority. Without protection on AD, then all systems are vulnerable. But AD administrators are not security experts. There's a risk that AD security falls through a crack between the AD team and IT security. According to one report, 27% of UK businesses thought the IT team have responsibility for AD security, and 19% thought responsibility was with the security team. 24% said they didn't know who was responsible for AD security (https://www.helpnetsecurity.com/2019/11/06/active-directory-security/).

AD security is a prime use case for Privileged Access Management (PAM). PAM can separate the AD admins from the credentials for AD preventing incorrect access and recording any sessions to investigate potential security incidents.

Automation takes security and protection of AD to another level. It ensures only valid changes are made to AD, by the right people and keeps a full end-to-end audit trail. As the user can't access ADUC, they can't do anything they shouldn't.

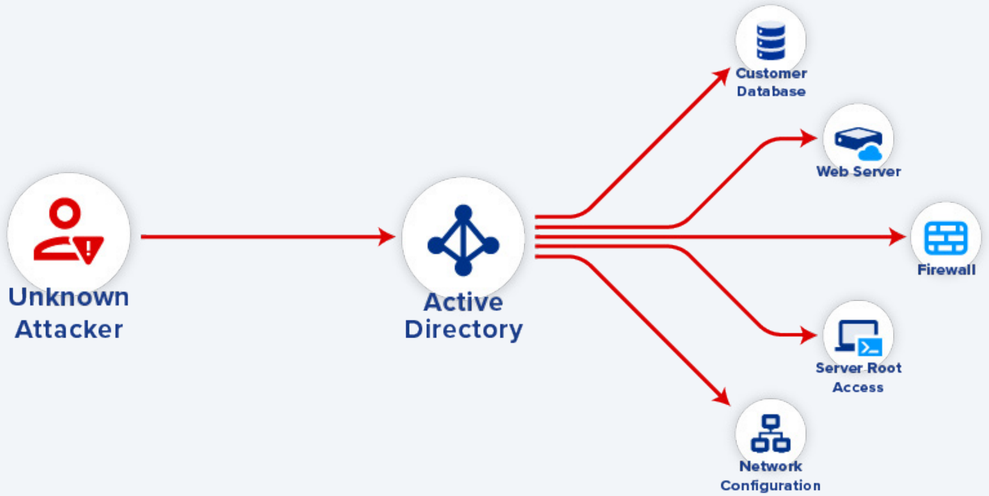


Figure: *Active Directory: The keys to the IT kingdom*

Typical challenges with Active Directory Continued

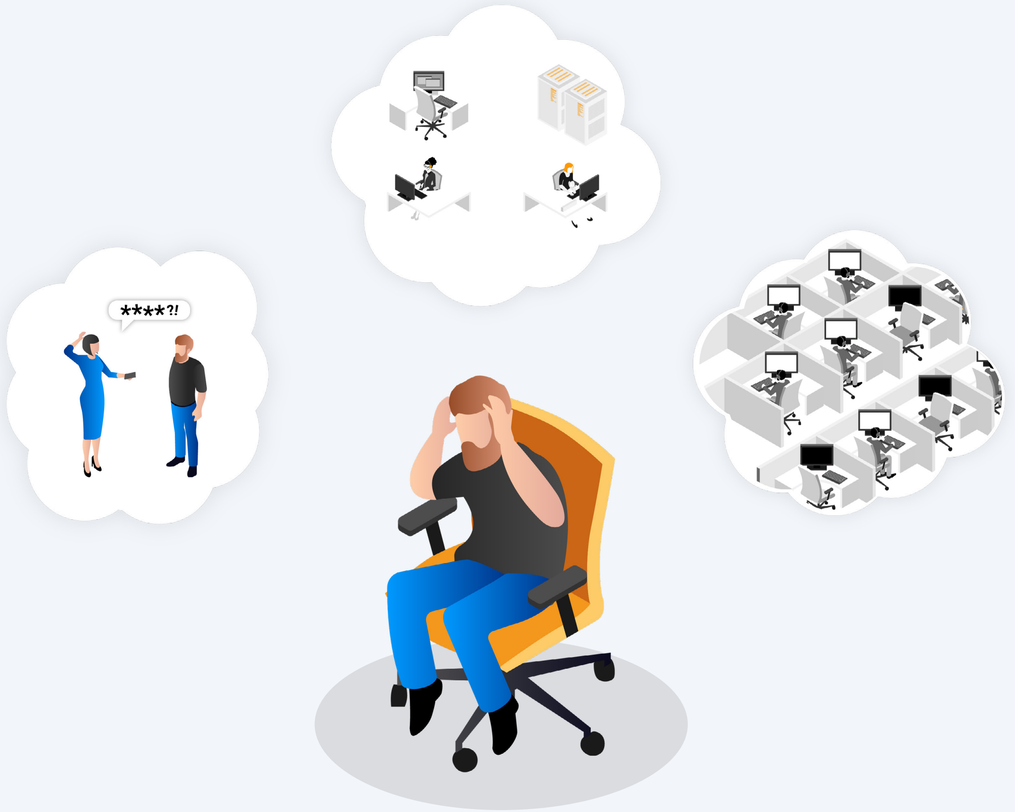
AD Experts are Busy

Changes needed in AD are often the most common request to IT Help Desks. The majority are to reset account passwords. For example, if the user has tried to remember their password and failed too many times.

Although resetting a password seems like a trivial task, it's a complex process. The AD admin uses the AD Users and Computers (ADUC) management console, navigates through the console's interface to find the right account, updates the password, and marks the account as needing to reset the password on the next login. Finally, they communicate the new password to the affected user.

That could take anywhere between 10 and 30 minutes for every request, and there could be hundreds every day.

Another common set of jobs for the AD team are account management tasks. There is often a constant flow of requests to create accounts for new users. To remove accounts for staff that are leaving. To remove users from one set of groups and add to another as they transfer between locations, teams or projects. Again, each change needs an expert to work through ADUC to make the changes. Especially with group changes, it's easy to make mistakes that prevent the user from working and causes more work for the admin.



Typical challenges with Active Directory Continued

Compliance: The Recurring Challenge

A common requirement of most regulatory standards is active account management. ISO27001, NIST-800, PCI DSS, Cyber Essentials, and many more include requirements for account management and hygiene. They have particular specifications for privileged accounts, but user accounts are also included. Typical requirements include:

- Users should only be able to access the systems they need.
- User access levels should be reviewed at regular intervals.
- Allocation and use of privileged user accounts should be restricted and controlled.
- Access rights of all employees and external party users should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Compliance audits are a regular part of the calendar. In some cases, that might be an annual review, but it could be twice per year or even quarterly.

Audits can be very expensive. A typical review, or “re-certification,” is to review lists of users and the group to which they belong. Group membership review is critical as that is what grants access rights to the users. It’s also difficult to review accurately. As noted previously, users can be in many groups. Those groups can be nested so inherit permissions are hard to trace.

Typical re-certification processes require generating reports of users and their groups, having the users and the group owners review those lists and mark-up any changes. The AD admin must collate these manual lists and update AD as needed. It’s a slow, tedious and highly error-prone process.

Ideally, accounts and memberships would be under constant review and preparing for the audit should be an automated process. An example is shown later in this document.

Automating AD Management

As we've seen, accurate, secure management of Active Directory is a critical capability.

Osirium Automation has been built to automate IT Operations, including AD Management. With secure automation, tasks that currently need expert admins can be safely delegated to Help Desk or 2nd level IT engineers.

http://www.osirium.com/videos/introducing-osirium-automation

Here are some examples of typical AD management tasks and how they are automated.

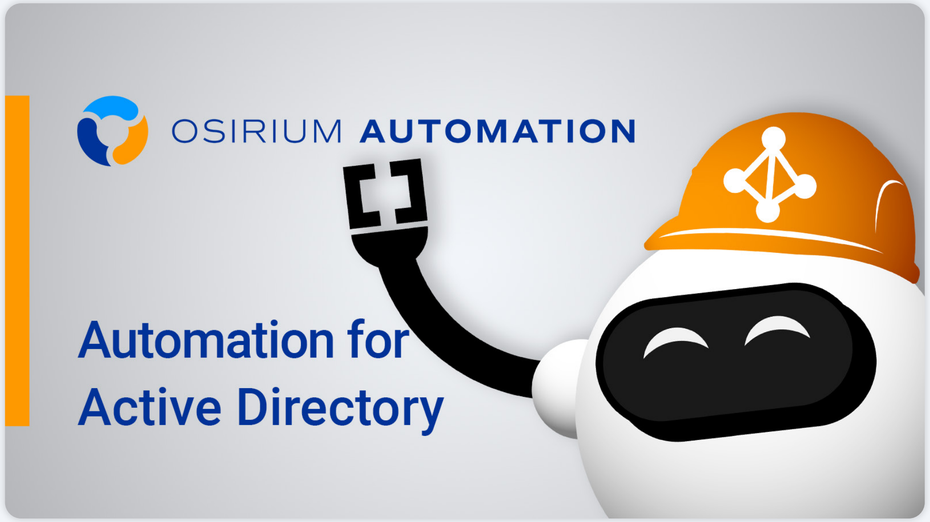
Automating AD Management Continued

Account Reset

The most common request to the IT Help Desk is to reset a user's account or password. Although it's seen as a relatively low-value operation, the longer the user can't access IT systems, then longer it is before they can get back to work.

With Osirium Automation, the account reset operation can be fully automated. AD credentials are always protected, and a full audit trail tracks all changes.

You can see the process in this demonstration:



https://www.osirium.com/videos/osirium-automation-for-active-directory

A task that might have taken 10 to 30 minutes for every reset, can now be completed in just a few minutes. Users can get back to work faster, IT can focus on higher-value projects.

Automating AD Management Continued

Account Re-certification

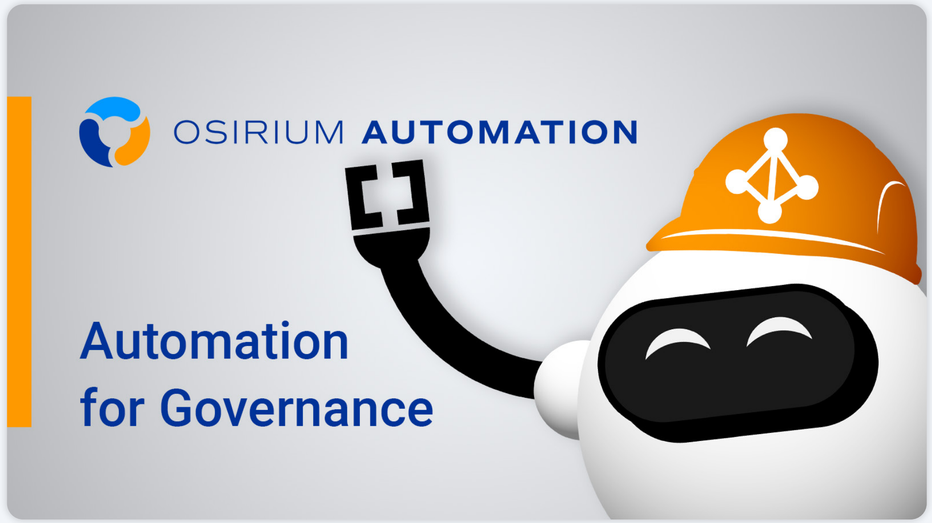
Another common request is to validate who has access to which systems. Often called a “re-certification,” it’s a critical task to show compliance with standards such as ISO27001 or Cyber Essentials.

The traditional method was to generate reports of AD users and groups and review with each group owner or team leads. As AD Groups can be nested and individual users can be members or many groups, it’s hard to work out who needs to do the reviews, let alone make any changes as a result.

With Osirium Automation, the process is simplified and delegated to the owners of the AD groups. Each group owner is sent a link to access an automated playbook in Osirium Automation. They are presented with a list of their groups, which they can review and update as needed. Because AD credentials are always protected and there’s a full audit trail, it’s a safe operation. If extra checks were needed, Automation playbooks can request approvals from a senior leader before any changes are made.

With this level of automation, the re-certification task has low impact on IT, and can be performed more often and compliance audits are easy.

You can see the process in action in this video:



https://www.osirium.com/videos/osirium-automation-for-governance

Automating AD Management Continued

Auditing Domain Administrators

One of the most powerful roles any user in the Active Directory database is Domain Administrator. Users within this group automatically inherit admin permissions on every computer in that domain and can control membership of the Administrator groups.

Managing the members of this group can be complicated because, as with all AD groups, memberships can be nested and hard to understand.

One of the AD Automation playbooks is to audit the Domain Admin group as you can see in this demo:

https://www.osirium.com/videos/ppa-bitesized-demo-audit-domain-admins

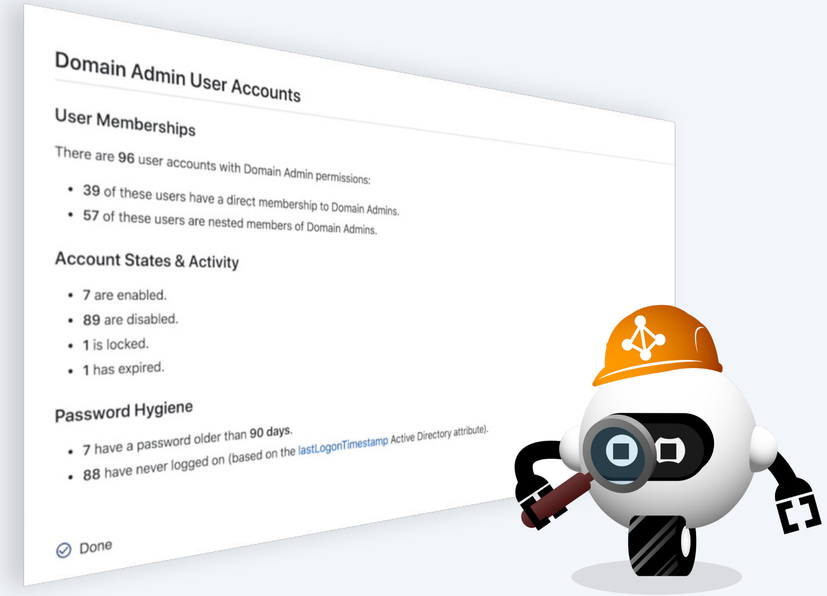


Figure: *Domain Admin report*

The report generated by Automation includes valuable information such as the nesting of groups, how long since an account was used (likely candidates for being cleaned out), and how stale the passwords are.

Automating AD Management Continued

Creating Accounts for New Users

Provisioning accounts for new hires is a frequent task for IT Operations. One of the first accounts that will be needed will be in Active Directory. It enables access to many core systems like logging into the user's laptop, network access, file shares, Office 365, and much more. Crucially, the user has to be added to the right groups for their role so they can access the services for their role or their local printer. If the account is not created or the user not added to the correct groups, they won't be able to start working.

Of course, a very similar process has to be performed each time a staff member moves between groups or leaves the business.

With Automation, the Help Desk engineer or someone in the HR team can run the process and ensure the right accounts are created and added to the right groups. The same task can also create accounts in all the applications the user needs.

You can see how in this demonstration:

https://www.osirium.com/videos/osirium-automation-for-it-operations

Automating AD Management Continued

Day-to-day AD Queries

Every day, there will be questions to the Help Desk like “Is my account OK?” “Who is a member of the Marketing group?” “What group does user01234 belong to?”

They’re all important questions, but each one requires the AD expert to login to AD Users and Computers, search for the user or group collect the information, export a report or capture a screenshot, and send it to whoever asked for the information. Invariably, that will spark follow-up requests like, “Please reset the account” or “Remove this person from that Group.”

These are perfect scenarios for automation. As you’ll see in this short demo, the automated playbook takes care of securely connecting to AD and collect all the information. The reports can be filtered online or exported in spreadsheet format. Automation can also be used to distribute the results via email or other communications such as Slack or Microsoft Teams.

You can see how in this demonstration:

https://www.osirium.com/videos/ppa-bitesized-demo-view-group-members

About Osirium Automation

Day-to-day AD Queries

Osirium Automation is a unique solution for automating IT and business processes that traditionally require expert skills.

Its flexibility comes from the open, secure Privileged Process Automation (PPA) framework to automate workflows across systems via API, REST, SSH, or command lines.

By hiding the complexity and need for specialist technical knowledge, processes can now be securely delegated and accelerated.

Credentials stored in secure vaults such as Osirium PAM or HashiCorp and always protected when interacting with the back-end IT systems, such as Active Directory. Those credentials are never passed back to the user's workstation so can't be intercepted on the network or misused by the user.

AD administration tasks are automated using "playbooks" – simple, low-code automation built using the built-in development and test environment. Those playbooks have a simple, conversational interface so any user can complete tasks with little knowledge of the underlying systems.

The playbooks can include workflow and approval mechanisms via email, Microsoft Teams or Slack to ensure that particularly sensitive changes are reviewed before being completed. A complete audit trail is maintained of all the changes and approvals. A rich set of pre-built playbooks is available from the PPA Resource Hub, including the AD management tools. Automation integrates with existing service desk management tools such as ServiceNow or corporate intranet portal so that existing processes and tools can be used with the final changes implemented by Osirium Automation.

Regular operations, such as generating lists of group memberships, can be scheduled to run weekly or monthly.

Full audit logs are maintained within PPA and your preferred SIEM logging systems such as Splunk.

If you'd like a demo of Osirium Automation, please get in touch. You can also download Osirium Automation for free and start automating your own AD tasks.

About Osirium

Osirium is the leading UK-based vendor of Privileged Access Security (PAS) solutions. Osirium's cloud and on-premises products protect critical shared IT infrastructure and endpoints, and securely streamline IT operations to deliver digital transformation fast.

Besides, Osirium Automation, Osirium's PAS solution includes modern **Privileged Access Management (PAM)** to protect valuable services and enables managed access by third-party vendors and partners. It includes high-availability clustered servers, session recording, just-in-time approvals, and simple deployment.

It also includes **Privileged Endpoint Management (PEM)** to remove local administrator accounts and manage applications approved to run with elevated privileges. Removing local admin rights is a critical part of any "least privilege" strategy.

For more information, please visit **https://www.osirium.com/automation**.

"Osirium's automation allows vital processes to be automated and delegated without compromising security."

SAUNDERSON HOUSE