

Stopping hackers with better Active Directory password policies

White Paper

wanstor

Contents

- + Thwarting hackers with better Active Directory password policies
- + Types of attack to look out for
- + Password policies
- + Microsoft password policy
- + Password policy implemented via Group Policy
- + Password policy implemented via FGPP
- + Password policy implemented via ADSelfService Plus

Introduction

Most IT professionals would agree that hacking passwords is the easiest way to gain access to a user account in Active Directory.

Hackers have been able to easily compromise the passwords of Microsoft Active Directory users for years. This is no surprise, considering the password policy and password controls in Active Directory have not been changed since early 2000's.

IT security was very different 15+ years ago. At Wanstor we believe now is the time for IT administrators to consider improving their Active Directory password policy controls and environment to keep the hackers out of their business or not for profit organisation.

Stopping hackers with better Active Directory password policies

The logo for Wanstor, featuring the word "wanstor" in a white, lowercase, sans-serif font. The logo is positioned in the bottom right corner of the page, overlaid on a blue triangular graphic that points towards the top right. The background of the entire page is a low-angle photograph of modern glass skyscrapers against a cloudy sky.

Password hacking strategies

Generally, password hacking technologies have not changed much over the past 15 years. This is mainly due to the fact that the controls over passwords have not changed. Microsoft has not provided any additional password controls in Active Directory since its inception in the year 2000. This means existing hacker strategies and technologies still work on a Windows Server 2012 R2 Active Directory user, just as they did on a Windows 2000 Mixed Mode Active Directory domain.

Most password hacking tools use the same logic as the foundation for obtaining the password. First, the attacker must obtain the password hash. The password hash is a mathematical algorithm that converts the password to an alphanumeric string, which is not reversible back to the password. This hash is generated by the operating system, in this case Active Directory.

The hash is stored in the Active Directory database and is also stored in the security database on the client computer when the user logs in. The hash is used to authenticate the user as they gain access to resources throughout the network. The attacker can obtain the hash from the Active Directory database, the local client computer, or from authentication packets.

Secondly, a set of characters is chosen from which a hash is calculated. This set of characters can be chosen from a dictionary, or chosen by specifying parameters such as characters, minimum password length, and maximum password length.

Finally, the hash obtained by the first step is compared to the hash generated by the second step. If the hashes match, the password is known as the set of characters that generated the matching hash.

The management of user accounts must coincide with the management of groups, computers, domain controllers, services, security, applications, files, and everything else that must be managed on a typical corporate network.

However, some Active Directory solutions actually help IT teams as they can manage users from creation, through changes over their employment, to removal when the user account is no longer needed.

Such systems help comfort IT administrators that all user accounts will be correctly managed and the daily tasks of user life cycle management will be addressed.

Types of attack

Dictionary attacks

A dictionary attack takes a set list of words from a dictionary file as the foundation for the hack. In most cases, there are many dictionaries used in an attack against password hashes.

These dictionaries might be normal language dictionaries or hacker dictionaries. Hacker dictionaries usually take normal language dictionaries and add words that use character replacements (See Figure 1 for examples). Since the parameters of these words follows those of words that already exist, dictionary attacks are faster than other types of attacks.

Language Dictionary Word	Hacker Dictionary Words
password	Pa\$\$word P@55w0rd
admin	@dmin @Dm1n
american	Am3R!c@n amEr1c@n

figure 1: Examples of words that might be in hacker dictionaries

Brute force attacks

A brute force attack uses a logical sequence of characters to develop hashes which are then compared to the password hashes that are obtained. Instead of using a list of words, like a dictionary attack, brute force attacks use every a combination of characters, with specified lengths of characters.

The possible characters used in a brute force attack include lowercase alpha, uppercase alpha, numeric, and special (a, A, 1, \$). Just like any password attack, the resulting hashes from the character combinations will be compared to the hashes that are acquired. If there is a match, the password is known.

Rainbow table attacks

Rainbow table attacks are the next generation of brute force attacks. Brute force attacks require the attacker to define a character space (a, A, 1, and/or \$) along with password lengths. Each time a brute force attack is attempted, the same character combinations and resulting hashes are produced. Instead of taking the time to produce the same hashes each time, a rainbow table caches the hashes.

Now, instead of taking the time to develop the hash, a simple comparison can be done with the hash table to the captured hashes. This can take much less time, some estimate about one tenth the time of brute force attacks.

Pattern attacks

Pattern attacks exploit characteristics that are commonly found in the typical user's password. For instance, that users like to use consecutive passwords when they change their password. This makes it easier for them to remember. Consecutive passwords would be Password1, Password2, Password3, etc.

Another pattern is that users will typically start their password with an uppercase alpha character. This again makes it easier for them to remember, as we start sentences with an uppercase letter.

Finally, another pattern is that when users are forced to use three of the four types of characters (a, A, 1, \$), they will usually use all but the special characters. Knowing these patterns lets the attacker develop attacks that will take advantage of the patterns, in turn reducing the time needed to hack the password.



Password policies

The password policy for an operating system contains controls a user must adhere to when creating their password. E.g. the password will be required to have a minimum number and maximum number of characters. The makeup of the password policy should help defend against the known password attacks and vulnerabilities for the password and its hash.

Unfortunately this is not the case in most situations. The reason most password policy solutions and implementations have insufficient controls to protect against known password attacks is usually due to end user limitations. A long, strong, complex password is not what most users are willing and able to deal with on a daily basis.

As a compromise, corporations allow users to input short, weak, and somewhat complex passwords. These passwords are often easy to hack. Ideally, the password policy should have controls that fight known password attacks, whilst still giving the user the flexibility to have a password they can remember. In the next section of this document we will explore ManageEngine's AD Manager role in helping organisations have more secure passwords and less inherent risk in their Active Directory environments

Microsoft password policy

For people who understand Active Directory and Microsoft technologies well they will know that Microsoft provides two ways to implement the password policy to Active Directory domain users.

One is through Group Policy and the other is through fine-grained password policies (FGPPs). Regardless of the implementation technology IT administrators use, the same controls are available.

The controls for the Microsoft password policy solutions include the following:

- + Enforce password history
- + Maximum password age
- + Minimum password age
- + Minimum password length
- + Password must meet complexity requirements
- + Store passwords using reversible encryption

These controls have been in place since the beginning of Windows Active Directory back in 2000. These settings have proven to be inferior in an attempt to secure passwords against hacking technologies.

The default of a seven character minimum length password is weak and does not provide the level of control needed to combat password-cracking technologies. The setting for complexity requirements is also limited in breadth and effectiveness. The complexity requirements by Microsoft are defined as the following:

- + The password must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- + The password must be at least six characters in length
- + The password must contain characters from three of the following four categories:
 - ++ Uppercase characters (A through Z)
 - ++ English lowercase characters (a through z)
 - ++ Base 10 digits (0 through 9)
 - ++ Non-alphabetic characters (for example !, \$, #, %)

Defending against dictionary, brute force, rainbow table, and pattern attacks is not addressed by Microsoft in their password policy controls.

Password policy implemented via Group Policy

At the heart of Active Directory is a password policy that controls all domain user account passwords. This password policy, by default, is configured in the Default Domain Policy Group Policy Object (GPO). This GPO is linked to the Active Directory domain node. There are some minor details that need to be explained regarding the password policy for domain users that is implemented using Group Policy:

- + The password policy does not need to be configured in the Default Domain Policy
- + The password policy must be configured in a GPO that is linked to the domain
- + The password policy controls will be implemented from the GPO(s) linked at the domain with the highest precedence for each control
- + GPOs containing password policy control settings linked to organizational units (OUs) do not affect domain users

The result of these details regarding the GPO-based password policy is that there can only be a single password policy for all domain users. There is no way to use Group Policy to have multiple password policies in a single Active Directory domain.



Password policy implemented via FGPP

Starting with Windows Server 2008, Microsoft added another password policy technology called finegrained password policies (FGPPs). Instead of using Group Policy to implement the password policy, Microsoft instead decided to use an Active Directory object approach. The controls for the password policy are nearly the same, but FGPPs do provide these additional aspects:

- + Precedence of each FGPP in relation to one another (so that only one FGPP can apply to each user)
- + Application of each FGPP to one or more security groups

The outcome of this approach to password policies is that there can be more than one password policy in the same Active Directory domain. Any user having membership in a group which is associated with an FGPP will receive the highest precedence FGPP applying to each user.

If a user is not a member of a group that is associated with a FGPP, the user will receive the password policy which is implemented through Group Policy.



Password policy implemented via ADSelfService Plus

Since Microsoft password policy solutions fail to secure passwords, there needs to be a solution that works with Active Directory and the Group Policy/FGPP based password policies that does protect an organisations Active Directory passwords.

Wanstor recommends ManageEngine's ADSelfService Plus. It is designed to protect against the most recent passwords attacks and is implemented using your current Active Directory OU design.

ADSelfService Plus provides enhancements to the Microsoft password policy solutions, allowing for different password policy enhancements in a single Active Directory domain.

The password policy enhancements work with the Windows password policy settings to improve the portions of the password essential for an organisations needs.

The following are features of ADSelfService Plus with regarding Active Directory user passwords:

- + Different password policy enhancements in a single domain
- + Provides implementation over group membership or user locations in OU
- + Dictionaries can be imported to negate the use of these words as passwords
- + Password pattern controls (incremental, omitting of special characters, palindromes, etc.)
- + The password policy is enforced through ADSelfService Plus's web portal and mobile application
- + The password policy is enforced through the Ctrl+Alt+Del Change Password screen. The password policy is enforced when the administrator resets the end user password from within Active Directory users and computers

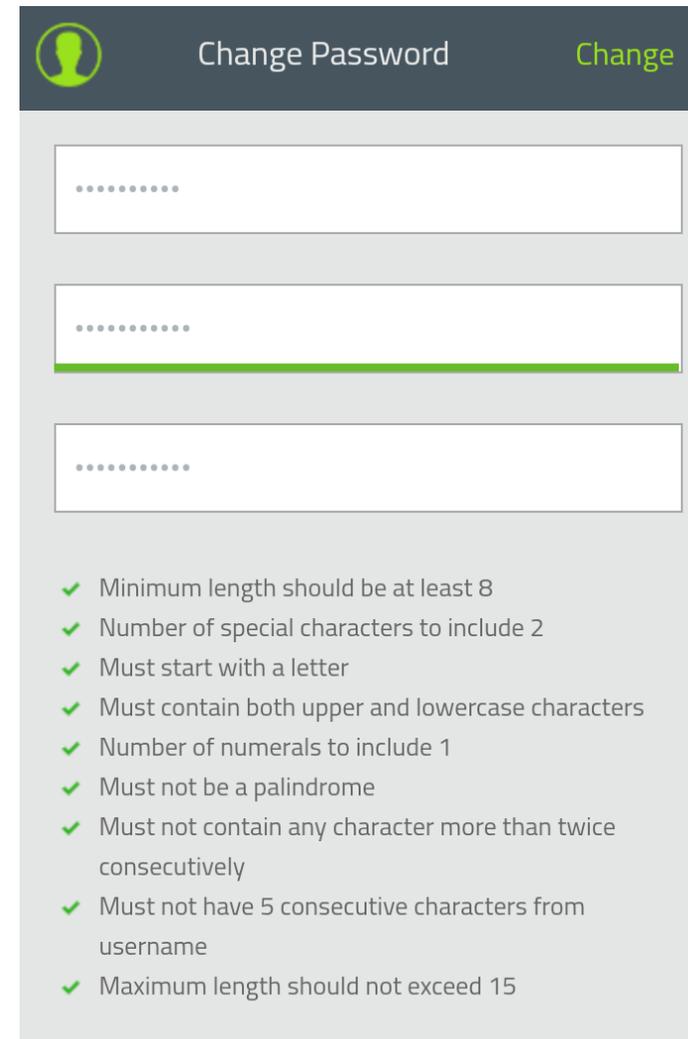
ADSelfService Plus provides an easy to configure and manage environment for your Active Directory password policies, as shown in Figure 2 on the right. The ADSelfService Plus password policy architecture is an enhancement to the existing Microsoft Group Policy and/or FGPP password policy.

If a user does not have a ADSelfService Plus password policy associated with them (*via group membership or OU*), only the password policy, either FGPP or Group Policy-based, will apply to the user. This provides a simple and effective way to implement additional controls over an organisations passwords, without needing to re-architect current Active Directory environments.

With the ability to import one or more dictionaries into your password policy controls, IT administrators are able to defend against dictionary attacks.

The password pattern controls in ADSelfService Plus provide security for users, preventing them from using common password pattern mistakes. These controls provide additional security to enhance Active Directory users' passwords against common password attacks.

figure 2 (right) : ADSelfService plus password policy enhancement controls



Change Password Change

.....

.....

.....

- ✓ Minimum length should be at least 8
- ✓ Number of special characters to include 2
- ✓ Must start with a letter
- ✓ Must contain both upper and lowercase characters
- ✓ Number of numerals to include 1
- ✓ Must not be a palindrome
- ✓ Must not contain any character more than twice consecutively
- ✓ Must not have 5 consecutive characters from username
- ✓ Maximum length should not exceed 15

There is no doubt that the modern medium sized business is under attack from hackers. It's not "if" it has happened it is "when" it has happened. Do the IT team know how the attackers got into the organisation? Unfortunately, Microsoft has not provided any additional password policy controls to help protect Active Directory users' passwords. Without some additional help and technologies in place, there simply will not be enough to protect your passwords.

Group Policy and FGPP-implemented password policies do not provide the needed password controls. Only FGPP provides more than one password policy for a single domain, but the controls are distributed via group membership, not even the OU location. These are significant limitations, and prevent IT teams from protecting their users passwords.

Wanstor recommends ADSelfService Plus as it provides a sophisticated solution that gives Active Directory domain users' passwords the protection needed. The ability to have multiple password policies in a single domain distributed through user group membership or OU is essential for most Active Directory installations.

The ability to have controls to protect against dictionary and password pattern attacks is also required to help reduce attacks against these password weaknesses. ADSelfService Plus is an easy to implement, configure, manage, and secure solution to any Active Directory domain.



Active Directory

Practical Management Solutions

What is ADManager Plus?

What is ADManager Plus?

ADManager Plus is a simple, easy-to-use Windows Active Directory Management and Reporting Solution that helps IT administrators and Help Desk Technicians with their day-to-day activities. With a centralized and intuitive web-based user interface, the software handles a variety of complex tasks like Bulk Management of User accounts and other AD objects, delegates Role-based access to Help Desk Technicians, and generates various AD Reports as an essential requirement in satisfying Compliance Audits. This tool also offers mobile AD apps empowering performance of important user management tasks right from mobile devices at any location with an internet connection.

What problems does ADManager Plus address?

- + Eliminates repetitive, mundane and complex tasks associated with AD Management
- + Automates routine AD Management and Reporting activities for AD Administrators
- + Facilitates Creation, Management and Deletion of AD objects in Bulk
- + Provides 'on the move' AD user management capability through its mobile apps
- + Acts as an essential resource during Compliance Audits like PCI, GDPR and ISO

What features does it offer?

+ Single and bulk user management	+ Group Computer Management	+ Help Desk Delegation
+ O365 Management & Reporting	+ Active Directory Automation	+ Active Directory Cleanup
+ Active Directory Reports	+ Real Last Logon Reports	+ Exchange Management

Key Features of AD Manager Plus

Every IT administrator faces the challenge of managing Active Directory objects including users, groups, computers, OUs and more daily. Manually performing complex tasks such as configuring user properties is extremely time consuming, tiresome and prone to error. AD Manager Plus enables automation and simplification of many of these tasks, with key features including:



MANAGEMENT

- + Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step
- + Create or modify AD objects (users, groups, contacts, OUs, computers) in bulk via CSV import
- + Perform tasks like password reset, account unlock, clean up and more
- + Streamline management of AD objects such as users and OUs with customizable templates
- + Assign, replace, or revoke Office 365 licenses in bulk
- + Manage shared, remote, room, equipment mailboxes



OU & ROLE-BASED HELP DESK DELEGATION

- + Delegate AD tasks to help desk technicians granularly within specific OUs
- + Delegate tasks like password reset and user creation
- + Delegate without elevating technicians' AD privileges



AD AUTOMATION & WORKFLOW

- + Automate routine tasks such as AD clean up
- + Manipulate automated tasks via workflow with automation
- + Configure review-approval workflows to execute AD tasks with a structured flow



REPORTING

- + Generate and schedule more than 150 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps
- + View inactive users, locked out users, disabled computers, and more in just few clicks
- + Perform management tasks for specific users within reports
- + Export to various formats: HTML, PDF, XLS, XLSX, CSV, CSVDE
- + Mention specific users or computers in a CSV file for generating their important details
- + Generate compliance reports to meet regulatory standards such as PCI, GDPR, ISO and more



iOS & ANDROID APPS

- + Manage users from anywhere - reset passwords; unlock, enable, disable and delete accounts
- + Report on locked out, disabled, password, expired, inactive users
- + View, manage, and execute AD workflow requests

Other Active Directory Tools by Wanstor & ManageEngine

		Features & Benefits
<p>ManageEngine ADSelfService Plus</p>	<p>ADSelfService Plus is an IT self-service solution designed for Windows environments. It is a feature rich IT self service solution which can be implemented independently or integrated seamlessly with company websites.</p>	<ul style="list-style-type: none"> + Self-service password management for on-premises Active Directory and cloud applications + Notify users (email & SMS) on impending password & account expiration + Enforces granular password policies across AD and connected on-premises and cloud applications + Automatically syncs Active Directory password in real-time across multiple applications + Offers Active Directory-based single sign-on (SSO) for cloud applications
<p>ManageEngine ADAudit Plus</p>	<p>In real-time, IT administrators can ensure critical resources in the network like Domain Controllers are audited, monitored and reported on with information on Users, Groups, GPO, Computer and OU changes, with 200+ detailed event specific reports and instant email alerts.</p>	<ul style="list-style-type: none"> + Web-based, Active Directory tool to track all domain events, including user, group, computer, GPO, and OU changes + Audits Windows files servers, failover clusters, NetApp for doc changes to files and folders, audit access + Monitors every user logon and logoff, including every successful and failed logon event across network workstations + Tracks Windows member servers, FIM, printers, and USB changes with events summary; tracks application, policy, and system events + Brings 150+ ready-to use audit reports with instant email alerts to ensure security and meet IT Compliance requirements
<p>ManageEngine Exchange Reporter Plus</p>	<p>ManageEngine Exchange Reporter Plus is a comprehensive web-based analysis & reporting solution for Microsoft Exchange, providing over 100 different reports on every aspect of the Microsoft Exchange Server environment.</p>	<ul style="list-style-type: none"> + Web-based change auditing / reporting solution for MS Exchange environments + Track / monitor enterprise ActiveSync infrastructure & inventory of related smart devices + Report on Outlook Web Access usage, mailbox traffic, mailbox growth + Supports customized reports that use data filters, automatic scheduling, and multi-format report generation + Provides audit feature to enable investigation of unauthorized mailbox logons and other critical changes
<p>ManageEngine RecoveryManager Plus</p>	<p>Empowers IT teams to back up changes made to AD objects as separate versions, providing an Exchange Online backup solution for numerous Exchange functions & data</p>	<ul style="list-style-type: none"> + Automated incremental backup of Active Directory objects + Simple and granular restoration down to the attribute level + Change tracking to undo changes + Detailed version management of each attribute change + Provision to roll back Active Directory to an earlier state

Features & Benefits

ManageEngine SharePoint Manager Plus

ManageEngine SharePoint Manager Plus is a tool that helps IT administrators to manage, audit and report on both on-premises and Office 365 SharePoint environments. It also allows monitoring, tracking and analysis of all activities in a SharePoint infrastructure, which facilitates informed, timely and accurate decision-making and management.

- + Web-based tool to manage and audit SharePoint on-premise servers and Office 365 configurations
- + Provides complete infrastructure visibility into both on-premise and online SharePoint server components
- + Includes out-of-the-box reports for monitoring SharePoint components such as farms, content databases, web applications, site collections, sites, lists and document libraries
- + Performs component level and security level auditing. Tracks permission changes, group changes and new role changes instantly with alerts
- + Meet compliance requirements by archiving audit log data for flexible time period

ManageEngine DataSecurity Plus

ManageEngine DataSecurity Plus is agent-based, real-time file auditing & reporting software that delivers complete visibility into Windows file server environments, showing IT administrators the 'who, what, where and when' behind every access event while also perform storage analysis. This helps to improve organisational Windows file server data security and information management, in a simple yet efficient and cost-effective way.

- + Web-based, real-time Windows file server access auditing & storage analysis tool helping meet data security, information management & compliance needs
- + Track & analyze access to files & folders by inspecting anomalies, recording access patterns & examining share & NTFS permissions
- + Optimize storage space by isolating old, stale & non-business files, gain insight into disk space usage & viewing file and folder properties
- + Actively respond to security breaches with instant email alerts. Detect & counter ransomware with mass access alerts & response automation
- + Stay compliant with SOX, HIPAA, FISMA, PCI, GLBA, GDPR, and other regulatory mandates

ManageEngine O365 Manager Plus

Providing exhaustive preconfigured reports on Office 365 & helping IT administrators perform complex tasks including bulk user & mailbox management, secure delegation and more. Monitor Office 365 services 24/7 and receive instant email notifications about service outages. O365 Manager Plus eases compliance management with built-in reports, offering advanced auditing & alert features to keep Office 365 setups secure.

- + An Office 365 reporting, monitoring, management and auditing tool
- + Utilize out-of-the-box reports Exchange Online, Azure Active Directory, OneDrive for Business and Skype for Business, as well as reports on security, compliance management and licences for Office 365
- + Monitor Office 365 service health around the clock, and receive instant email notifications on service outages
- + Effortlessly oversee your Office 365 setup with a wide range of Exchange Online and Azure Active Directory management features
- + Track even the most granular user activities in Exchange Online, Azure Active Directory, OneDrive for Business, Sway, and other services
- + Audit critical activities and changes in your Office 365 environment with custom alerts for each Office 365 service
- + Delegate Office 365 administration tasks granularly to help desk staff and other non-IT users through role-based delegation

Wanstor's ManageEngine Customers



Final Thoughts

Every IT Administrator faces a number of Active Directory management challenges, which include managing user accounts in Active Directory almost every day.

Configuring user properties manually is extremely time consuming, tiresome, and error-prone, especially in a large, complex Windows network.

A solution that can automate cumbersome, boring, repetitive tasks, simplify AD management and provide exhaustive reports on tasks completed is now a must-have for all proactive IT departments, no matter what the size of their organisation.

Wanstor is ManageEngine's largest European partner. We work with ManageEngine to plan, deploy and manage Active Directory tools such as ADManager Plus in helping IT administrators overcome their Active Directory management challenges.

Our Active Directory management tools are designed to offer IT professionals absolute control over their Active Directory environment, with the main toolset that we recommend being ADManager Plus.

ADManager Plus is comprehensive web-based Microsoft Windows Active Directory management software that simplifies user provisioning and Active Directory administration with complete security and authentication, allowing only authorized users to perform management actions.

It also provides a complete set of management tools to IT administrators for efficient management of Active Directory.

For more information about Wanstor and ManageEngine's Active Directory management solutions, call us on **0333 123 0360**, email us at **info@wanstor.com** or visit our website at **www.wanstor.com** and one of our Active Directory experts will be in touch.