Active Directory Weak Password Finder Report

Prepared for Contoso, Inc.

Scan Date: 07/10/2020 19:51:15. Scan completed in 14 minutes.

Directory Domain Scanned: contoso.com (Found 5302 accounts of which 4369 are enabled.)

Weaknesses Found: 2368

Most enterprises use Active Directory (AD) as the cornerstone of their IT systems and store domain accounts in the AD database. It’s important to understand how easy it is to crack AD passwords and take the necessary steps to protect them.

The Active Directory Weak Password Finder examines the passwords of your AD accounts to determine if your organization is susceptible to password-related attacks. It connects to your AD to retrieve your password table and analyzes passwords against failure types that increase your risk.

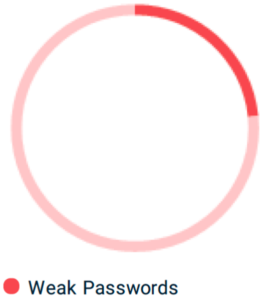
All passwords can be cracked given enough time. Passwords set by humans tend to be the least secure. Unfortunately, the default domain password policy, which admins use to enforce password rules in Active Directory, is usually not configured to force good passwords, and in many cases doesn’t provide necessary controls.

The password policy within AD enforces password length, complexity, and history, but doesn’t control what the password is, just how long it is and what characters are inside. Many people will use easily guessable passwords like Password!@# because they technically meet the standards and are also easy for them to remember.

To prevent cyber criminals from repeatedly guessing the passwords of user accounts, AD supports account lockout policies. But if a criminal were to take a single password and try it against every single account in an organization, lockouts wouldn’t protect you.

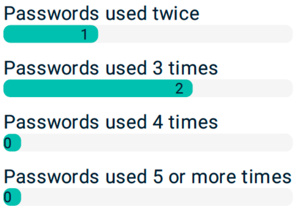
While settings in AD provide flexibility for IT administrators, they also increase risk. Plain text passwords can be exposed within Active Directory, which represents a major vulnerability. Older encryption settings and default passwords can easily be left in place.

Proactive and ongoing management is essential to maintaining the security of Active Directory accounts and passwords. You can use the results of this report to identify areas of highest risk so that you can prioritize your security updates. The associated file shows additional detail for specific user accounts and computers that require immediate attention.



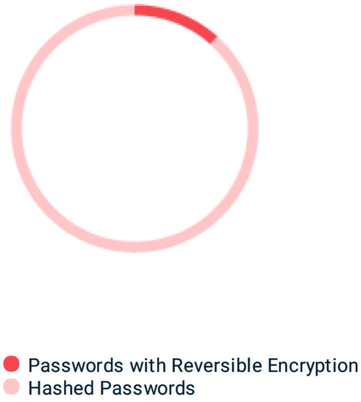
Accounts with Weak Passwords

The ideal password is over 14 characters long with a mixture of upper-case and lower-case letters, numbers, and special characters. Even with these rules in place, users often create weak passwords that are easy to remember. We compared your AD passwords against a list of commonly used weak passwords to flag those that need attention.



Non-Unique Passwords

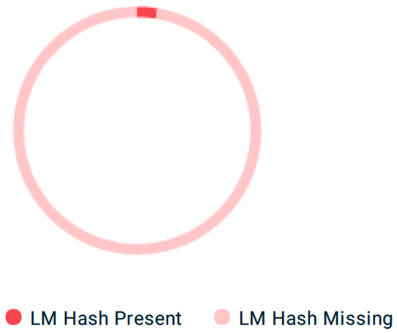
When the same password is used among many different systems, a cyber attack can become a catastrophe. With a single password in hand, a cyber criminal can infiltrate and cause damage to many systems. Make sure all accounts have unique passwords. Ensure members of your IT team with administrative credentials have one password for administrative operations and another for standard use.



Passwords Stored Using Reversible Encryption

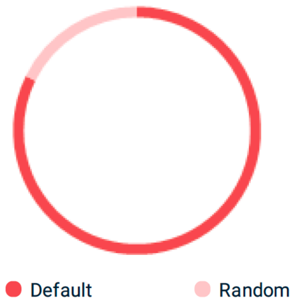
Passwords stored in Active Directory are hashed. Once a user creates a password, an algorithm transforms it into an encrypted output of fixed length. However, Microsoft permits the ability to store passwords using reversible encryption. The “store password using reversible encryption” policy setting provides support for applications that use protocols requiring the user's password for authentication.

This setting is disabled by default and should remain so. Storing encrypted passwords in a way that is reversible means encrypted passwords can be decrypted. If a password is stored using reversible encryption, it's basically the same as storing it in plain text because of the ease with which it can be cracked.



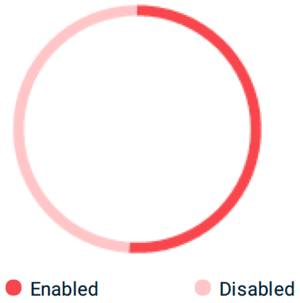
Accounts with LM Hashes

When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generates two hashes: a LAN-manager, or LM , which is based on a simple DES encryption, and an NT, based upon the MD4 hashing function. The LM hash is relatively weak compared to the NT hash, and prone to fast brute force attack. The simplest way to prevent Windows from storing an LM hash of your password is to use a password that is at least 15 characters long.



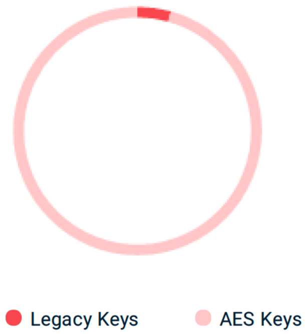
Computer Accounts with Default Passwords

During the process of creating or resetting a computer account, the password is automatically set to its logon name. Default passwords are easier for attackers to guess and thus gain access to a computer and possibly more systems. Ensure these accounts are protected by requiring random passwords.



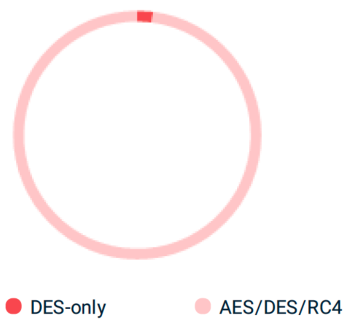
Delegation of Privileged Accounts

All admin accounts in AD have a checkbox called “Account is sensitive and cannot be delegated,” which helps protect them from being used improperly by untrusted systems. Ensure all accounts belonging to administrative groups are marked with this flag to limit the scope of attacks and protect elevation of privileged activities.



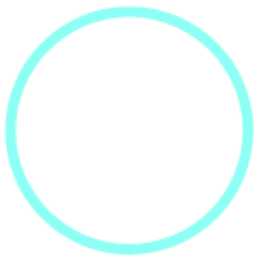
Accounts without Kerberos AES Keys

The Kerberos protocol is built to protect authentication between server and client in an open network where other systems are also connected. Starting in Microsoft Windows Server 2008 R2, an administrator can enforce which Kerberos encryption algorithms are used on participating Microsoft AD domain clients. You should take advantage of the strongest encryption type for Kerberos – Advanced Encryption Standard (AES) – and configure account properties in AD to support AES encryption.



Accounts with Kerberos DES Only

Accounts set up using older functional AD levels have no AES keys. Certain older encryption types are no longer considered secure. The DES and RC4 encryption suites must not be used for Kerberos encryption. In fact, Windows Server 2008 R2, Windows 7, and Windows 10 don’t support the DES cryptographic suites because stronger ones are available. You should change settings to take advantage of the stronger security provided by AES encryption.



Accounts without Kerberos Pre-Authentication

Kerberos Pre-Authentication is a security feature that offers protection against password guessing attacks. If Kerberos Pre-Authentication is enabled, a timestamp will be encrypted using the user's hash (available in AD) as an encryption key. If the Key Distribution Center (KDC) reads a valid time when using the user's password hash to decrypt the timestamp, it knows a request isn't a replay of a previous request. Accounts that don’t encrypt authentication requests give an attacker the ability to perform offline brute force attacks, which are less likely to be detected.

Weak Password Analysis Summary

Administrative accounts whose passwords should be changed	0
Service accounts whose passwords should be changed	0
Accounts with weak passwords	1024
Accounts with non-unique password	0
Passwords stored using reversible encryption	510
Passwords stored in LM hash form	115
Computer accounts with default passwords	255
Delegatable administrative accounts	185
Accounts missing Kerberos AES keys	190
Accounts with Kerberos DES-only encryption	89
Accounts with Kerberos pre-authentication disabled	0

Every account in AD should be properly secured to decrease the likelihood and scope of a cyber attack. All account passwords should be complex, unique, and stored using modern cryptographic algorithms. You should regularly rotate passwords and disable or expire those no longer in use.

Privileged accounts, such as IT administrative accounts and service accounts, are most essential to secure as they provide access to critical IT systems and processes. You should limit all accounts to the minimum privileges required, including membership in privileged groups.

It's difficult and time-consuming to manage privileged security with only with AD and group membership. Integration between AD and enterprise Privileged Access Management (PAM) solutions provide additional security controls for credential management, authentication, access, and monitoring.

Learn more about how Delinea works with Active Directory to protect your privileged accounts

Delinea empowers more than 10,000 organizations around the globe, from small businesses to the Fortune 500, to manage privileged access.

Secret Server

Secret Server is the only fully featured PAM solution available both on premise and in the cloud. Delinea's award-winning software gives security and IT ops teams the agility to secure and manage all types of privileges, protecting administrator, service, application, and root accounts from cyber attack. You can set up a secure vault, discover privileges, manage secrets, delegate access, and control sessions – all from a central hub.

Secret Server's AD integration enables users to sign in with their normal domain account to gain access to privileged accounts, such as their domain administrator credential. By assigning access in Secret Server based on security groups, you won't have to manually grant permissions every time a new admin needs access or users change roles.

Try Secret Server and AD integration for yourself with a free, 30-day trial