Security Account Manager

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Security_Account_Manager#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Security_Account_Manager#searchInput)

|  |  |  |  |
| --- | --- | --- | --- |
|  | hide**This article has multiple issues.** Please help [**improve it**](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit) or discuss these issues on the [**talk page**](https://en.wikipedia.org/wiki/Talk:Security_Account_Manager). *(*[*Learn how and when to remove these template messages*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)*   |  | | --- | | This article **may be too technical for most readers to understand**. Please [help improve it](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit) to [make it understandable to non-experts](https://en.wikipedia.org/wiki/Wikipedia:Make_technical_articles_understandable), without removing the technical details. *(March 2012)* |  |  | | --- | | This article **needs additional citations for**[**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). *(September 2014)* | |

The **Security Account Manager** (**SAM**) is a database file[[1]](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_note-1) in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory authenticates remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.

The user passwords are stored in a hashed format in a [registry hive](https://en.wikipedia.org/wiki/Windows_Registry#Hives) either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0. When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY"). It can be enabled by running the syskey program.[[2]](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_note-2)



**Contents**

* [1Cryptanalysis](https://en.wikipedia.org/wiki/Security_Account_Manager#Cryptanalysis)
  + [1.1Removing LM hash](https://en.wikipedia.org/wiki/Security_Account_Manager#Removing_LM_hash)
  + [1.2Related attacks](https://en.wikipedia.org/wiki/Security_Account_Manager#Related_attacks)
* [2See also](https://en.wikipedia.org/wiki/Security_Account_Manager#See_also)
* [3References](https://en.wikipedia.org/wiki/Security_Account_Manager#References)

Cryptanalysis[[edit](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit&section=1)]

Since a [hash function](https://en.wikipedia.org/wiki/Hash_function) is one-way, this provides some measure of security for the storage of the passwords.

In the case of online attacks, it is not possible to simply copy the SAM file to another location. The SAM file cannot be moved or copied while Windows is running, since the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file, and will not release that lock until the operating system has shut down or a "[Blue Screen of Death](https://en.wikipedia.org/wiki/Blue_Screen_of_Death)" exception has been thrown. However, the in-memory copy of the contents of the SAM can be dumped using various techniques (including [pwdump](https://en.wikipedia.org/wiki/Pwdump)), making the password hashes available for offline [brute-force attack](https://en.wikipedia.org/wiki/Brute-force_attack).

**Removing LM hash**[[edit](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit&section=2)]

LM hash is a compromised protocol and has been replaced by NTLM hash. Most versions of Windows can be configured to disable the creation and storage of valid LM hashes when the user changes their password. Windows Vista and later versions of Windows disable LM hash by default. Note: enabling this setting does not immediately clear the LM hash values from the SAM, but rather enables an additional check during password change operations that will instead store a "dummy" value in the location in the SAM database where the LM hash is otherwise stored. (This dummy value has no relationship to the user's password - it is the same value used for all user accounts.)

**Related attacks**[[edit](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit&section=3)]

In Windows NT 3.51, NT 4.0 and 2000, an attack was devised to bypass the local authentication system. If the SAM file is deleted from the hard drive (e.g. mounting the Windows OS volume into an alternate operating system), the attacker could log in as any account with no password. This flaw was corrected with Windows XP, which shows an error message and shuts down the computer. However, there exist software utilities[[3]](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_note-3), which, by the aforementioned methodology of using either an emulated virtual drive, or boot disk (usually Unix/Linux, or another copy of Windows like [Windows Preinstallation Environment](https://en.wikipedia.org/wiki/Windows_Preinstallation_Environment)) based environment to mount the local drive housing the active NTFS partition, and using programmed software routines and function calls from within assigned memory stacks to isolate the SAM file from the Windows NT system installation directory structure (default: %SystemRoot%/system32/config/SAM) and, depending on the particular software utility being used, removes the password hashes stored for user accounts in their entirety, or in some cases, modify the user account passwords directly from this environment.

This software has both a highly pragmatic and beneficial use as a password clearing or account recovering utility for individuals who have lost or forgotten their Windows account passwords, as well as a possible use as a malicious software security bypassing utility. Essentially granting a user with enough ability, experience, and familiarity with both the cracking utility software and the security routines of the Windows NT kernel (as well as offline and immediate local access to the target computer) the capability to entirely bypass or remove the Windows account passwords from a potential target computer. Only recently, Microsoft released a utility called LockSmith, which is part of MSDart. MSDart is not freely available to end-users, however.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit&section=4)]

* [chntpw](https://en.wikipedia.org/wiki/Chntpw)
* [Password file](https://en.wikipedia.org/wiki/Passwd#Password_file)

References[[edit](https://en.wikipedia.org/w/index.php?title=Security_Account_Manager&action=edit&section=5)]

* 1. [**^**](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_ref-1) [*"Security Account Manager (SAM)"*](https://technet.microsoft.com/en-us/library/cc756748%28v=ws.10%29.aspx)*. TechNet. Microsoft. Retrieved 11 April 2014.*
  2. [**^**](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_ref-2) [*"How to use the SysKey utility to secure the Windows Security Account Manager database"*](http://support.microsoft.com/kb/310105)*. Support. Microsoft Corporation. Retrieved 12 April 2014.*
  3. [**^**](https://en.wikipedia.org/wiki/Security_Account_Manager#cite_ref-3) An example of offline NT password attack utility: <http://cdslow.org.ru/en/ntpwedit/index.html>

This article is based on material taken from the [*Free On-line Dictionary of Computing*](https://en.wikipedia.org/wiki/Free_On-line_Dictionary_of_Computing) prior to 1 November 2008 and incorporated under the "relicensing" terms of the [GFDL](https://en.wikipedia.org/wiki/GNU_Free_Documentation_License), version 1.3 or later.