MyID MFA and PSM

Active Directory Password Audit Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: IMP2056-02

January 2025

Copyright

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

The MyID Password Audit Tool is a command-line program that retrieves user accounts from an Active Directory Domain and analyses passwords to identify potential security and compliance issues. The tool is designed specifically so that no sensitive data leaves the corporate network, with all processing done locally on the machine running the audit tool. For more information, contact Intercede support.

All extracted data is encrypted by default; data files generated from the audit process contain sensitive user information and you must handle them accordingly. The tool generates a set of text and CSV report files that contain no sensitive password information.

The MyID Password Audit Tool includes offline password breach analysis, which does not require access to the cloud-hosted MyID Password Breach Database and is designed to work fully on-premise.

Note: When running the Password Audit Tool against the on-premise Password Breach Database, no email address analysis is performed.

1.1 Change history

Version	Description
`IMP2056-01`	Reformatted and released with MyID MFA and PSM version 5.0.7.
`IMP2056-02`	Released with the latest version of the Active Directory Password Audit tool. Added new `Group` and `CustomADField` options to the `passtool.exe` command line.

1.2 Prerequisites

The following requirements need to be met for a successful audit.

Note: The MyID Password Audit Tool attempts to determine whether the prerequisite requirements are met before the extract process begins.

1.2.1 Requirements

General requirements:

- A domain-joined machine with access to a domain controller.
- Domain Administrator user account permissions for the user running the MyID Password Audit Tool.
- The ability to run a command prompt with administrator privileges.
- .Net Framework version 4.8 or later on the machine running the Password Audit Tool.

For domain controller only extraction mode:

- The Volume Shadow Copy service must be running (on by default).
- The Active Directory Management tools must be installed (installed by default).

For extract processing:

- A valid MyID Password Cloud Database or offline API key (provided by Intercede).
- An Internet connection with HTTPS access to MyID Password Breach database for online processing:

  `https://passwordsecurityapi.authlogics.com/api/*`
- Access to Offline Breach database for offline processing.
- .Net Framework version 4.8 or later.

The audit tool attempts to connect to the internet to process the extract data and uses the system proxy settings if available. If an Internet connection is not available, you can extract the data from the server and complete the analysis process on a separate machine. If .Net framework 4.8 or later is not available, you can manually extract and process the required Active Directory files separately. See section *2.4.1*, *Manual extract process*, for details.

2 Running the MyID Password Audit Tool

The MyID Password Audit Tool is a command-line tool that accepts various parameters. By default, the tool performs the following tasks in sequence:

1. Verifies that the requirements listed above are met.
2. Performs a full Active Directory backup.
3. Extracts the relevant user and password information and creates an encrypted export file.
4. Cleans up any data generated by the backup process.
5. Connects to the MyID Cloud Password Database and perform user and password analysis.
6. Generates text reports and output `.csv` files.

This chapter contains information on:

- How to use the MyID Password Audit Tool.

  See section *2.1*, *Usage*.
- The details you get from the MyID Password Audit Tool.

  See section *2.2*, *Details*.
- The extraction modes you can use and how to extract and process the returned data.

  See section *2.3*, *Extraction modes and steps*.
- How to extract and locally process the users' Active Directory password information.

  section *2.4*, *Offline password breach extract*

2.1 Usage

```
passtool.exe APIKEY [?] [/O <Outputfile>] [/I <Inputfile>] [/D] [/N
<DomainName>] [/P <Password>] [/F] [/V] [/DC] [/Offline] [/OU] [/Group <AD
Security Group name>] [/Active] [/Admin] [/B] [/DCServerName <DC server
name>] [/ADPermissions] [/DormantDays <Days>] [/ExcludeBreachedEmails]
[/OfflineBreachedDBPath <offline breached database path>] [/CustomADField]
```

2.1.1 Parameters

Parameter	Name	Description
APIKEY		Provide the Intercede-supplied API Key. An API Key is always required unless running the tool using the Validate option.
?	Help	Provides help on the parameters available.
O	Output File	Save the extraction data to a hashes data file. Use this option when the machine extracting Active Directory data does not have access to the internet, directly or through a proxy. Analysis and reporting can take place on a separate machine, providing you use the same API keys. If no filename is specified with the /O parameter, a file called extract.dat is created.
I	Input File	Specify the name of the extraction output file, or system files to be processed. Use this option when the /O option has been performed and the contents are available for analysis on a machine with an internet connection, or when data has been manually extracted. If no filename is specified with the /I parameter, the tool tries to import a file called extract.dat.
D	Debug	Enable enhanced diagnostic mode for debugging purposes.
N	Domain Name	Specify the domain name from Active Directory used to report domain breaches. This option is typically used when the AD domain name does not match the organization's email address notation; that is, acme.local compared to acme.com. This parameter reports the email addresses for the specified domain found in the MyID Password Breach Database.
P	Password	Specify the password used in encryption/decryption of input and output files instead of using the API key.
F	Full hashes	Send full password hashes to MyID online servers; turning off partial K-Anonymity.

Parameter	Name	Description
`V`	Validate	Validate only. Use this option to run the verification step only. This can be useful to ensure the environment is configured correctly before a full audit is run.
`DC`	Domain Controller Only Extraction	Execute MyID Password Audit data using a domain-controller based alternate extract method (default method for version 1.x). This can only be performed by a Domain Administrator on a Domain Controller. When executing the solution in domain controller mode, the Windows Volume Shadow Copy service must be running, and the Active Directory Management tools must be installed locally.
`Offline`	Offline Mode	Prevent the MyID Password Audit Tool from accessing the internet and processing any data online. Running in Offline mode limits what is reported on as certain sections, such as password breaches and identifiable email analyses, require Internet access for processing. **Note:** A special offline API key is required to run Password Audit Tool in Offline mode. Contact Intercede for an Offline API key.
`OU`	Organizational Unit	Limit the audit to report on users that are members of the specified Active Directory Organizational Unit only. Accounts that are not members of the specified Organizational Unit are ignored.
`Group`	Active Directory Security Group	Limit the audit to report on users who are members of the specified Active Directory Security Group only. Accounts that are not members of the specified Active Directory Security Group are ignored. Nested group membership is not supported.
`Active`	Active Users Only	Limit the audit to report on Active accounts only. Disabled and Expired accounts are ignored.

Parameter	Name	Description
`Admin`	Administrator Accounts Only	Limit the audit to report on Administrator and elevated privileged accounts only. Non-administrator Active Directory accounts are ignored.
`B`	Blacklist	Enable the Blacklist file mode, which allows an administrator to specify a custom set of passwords to report against. When enabled, create a `Blacklist.txt` file in the same directory as the Audit tool executable and then enter the passwords (in clear text) to report against.
`DCServerName`	Domain Controller Server Name	Override the auto-detection of a Domain Controller and specify the Domain Controller to run the tool against.
`ADPermissions`	Active Directory Domain Permissions	Extract and report on Advanced Security Settings for the root domain.
`DormantDays`	Number of days since last-logon	Set the number of days elapsed for an account not to have logged in to be deemed to be a dormant account. If no number is specified, any account not logged in within the last 90 days is deemed to be a dormant account. Setting this value to `0` turns off this analysis.
`ExcludeBreachedEmails`	Exclude breached email analysis	Limit the analysis to exclude the analysis of matched breached email addresses.
`OfflineBreachedDBPath`	Perform on-premise password breach analysis	Specify the location of the offline password breach database. When not specified, the current folder is applied. You must specify the Offline parameter for this option to be enabled.
`CustomADField`	Extract contents of custom AD field	Extracts the contents of the specified Active Directory field and displays the value in the CSV files when audit is running in verbose user data extraction mode.
`VerboseUserDetails` (Deprecated)	Extract and report on extended user details	Enable detailed user extraction and reporting. **Note:** This option is no longer required to be specified, as this information is extracted by default.

2.2 Details

When running the MyID Password Audit Tool, as well as basic user and password information, the following details are extracted and listed in the CSV files.

Note: This information was previously extracted only when the MyID Password Audit Tool was run using the `VerboseUserDetails` parameter.

- `fullName`
- `username`
- `isAdministrator`
- `isDomainAdmin`
- `isEnterpriseAdmin`
- `isDisabled`
- `isExpired`
- `isBreached`
- `passwordNeverExpires`
- `passwordNotRequired`
- `lastLogon`
- `passwordLastChanged`
- `samaccountname`
- `displayName`
- `distinguishedName` (CNs are ";" delimited)
- `enabled`
- `name`
- `canonicalName`
- `LMHashPasswordExists`
- `DefaultPassword`
- `PreAuthNotRequired`
- `AESKeyMissing`
- `UseDESKeyOnly`
- `AdminDelegated`
- `KerberosRoasting`
- `emails`
- `CustomADField` (when specified using `/CustomADField <AD field name>` parameter)

2.3 Extraction modes and steps

You can run the MyID Password Audit Tool using two different data extraction modes, either on any machine joined to the domain, or directly on a Domain Controller if required.

If the machine has an active Internet connection, the extract and analysis is performed in a single step. If the machine does not have an Internet connection, you must carry out the processing of the data on a machine with an internet connection that provides access to the MyID Password Breach Database. You can use both extraction modes to create output files, although this option is usually only required when data extraction occurs using the Domain Controller extraction mode.

2.3.1 Default extraction mode

The MyID Password Audit Tool uses the context of the user running the command prompt. If you are logged onto a domain-joined machine using a non-Domain Admin account, you are recommended to log off and log on again with a Domain Admin/Enterprise Admin account, or to open a command prompt using we recommend you either log off and then log on with a Domain Admin/Enterprise Admin account or open a command prompt using **Run as different user** and specifying a domain account.

The tool then auto-detects the domain name and closest Domain Controller, both of which are needed for the extract process.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY
```

Wherever possible, the MyID Password Audit Tool tries to remove temporary files and folders on completion; however, this may not always be the case. In these cases, you are recommended to remove the temporary files left behind manually.

2.3.2 Domain Controller mode

If a domain-joined machine cannot remotely access the data on a Domain Controller, you may have to extract, and optionally process, the information directly on a Domain Controller, using a different underlying method for extracting account information from Active Directory.

As with the default extraction method, you are recommended to log off and then log on with a Domain Admin/Enterprise Admin account, or open a command prompt using **Run as different user** and specifying a domain account. You can then run the executable using the `/DC` command-line switch.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /DC
```

2.3.3 Using multiple steps to extract and process data

When the machine used to extract account information from Active Directory does not have Internet access, you can copy the required extract file onto any Windows computer with Internet access and then process it separately.

To do this, first execute the MyID Password Audit Tool as normal using either the default or domain controller extraction method, additionally adding the `/O` (Output mode) command-line parameter. Copy the encrypted output file to a machine with internet access and then use the `/I` (Input) parameter using the same API key in both processes.

If you do not specify a file name, the filename is called `extract.dat`. If you provide a name, the file name can be any name you want except `ntds.dit`, which is reserved for manual extracts.

The example below creates a file called `MyDomain1.dat` in the same folder as the executable:

```
C:\Authlogics\PasswordAudit\Server\>passtool.exe APIKEY /O MyDomain1.dat
```

In this example, you must then copy this file to a machine with Internet access for processing.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /I MyDomain1.dat
```

2.4 Offline password breach extract

The following commands extract the users' Active Directory password information locally and process the breach password database from a local on-premise password breach database; the tool does not connect to the cloud for analysis.

By default, the tool attempts to locate the on-premise password Breach database in the `Breach Database` sub-folder of the current executing folder. You can override this folder structure using the `/OfflineBreachDBPath` parameter.

Execute `passtool.exe` using the `/Offline` and `/OfflineBreachDBPath` parameters.

The example below extracts the Password Audit Tool where the breach database folder resides in:

```
C:\Authlogics\Breach Database
```

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /Offline
/OfflineBreachDBPath "C:\Authlogics"
```

2.4.1 Manual extract process

The following commands extract the users' Active Directory password information locally for offline/remote processing purposes. You are recommended to use the manual extraction only when no other option is available. This performs a full Active Directory database backup and provides the raw data files which you can process on a separate machine. The files contain sensitive user information, and you must handle them accordingly.

Note: This is not the recommended method, and you must use it only when no other methods are available.

You can carry out these steps only using a Domain Administrator account on a Domain Controller with:

- The Volume Shadow Copy service running (on by default).
- The Active Directory Management tools installed on the DC (installed by default).

The Manual Process uses the inbuilt Microsoft Active Directory command-line tool:

```
NTDSUtil.exe
```

To run a manual extract process:

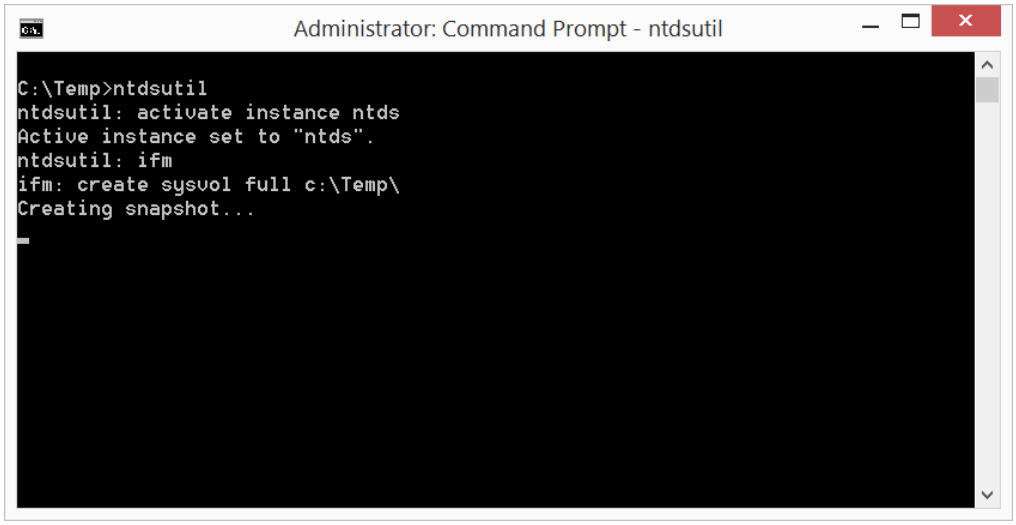
1. Open an administrative command prompt on a Domain Controller within the targeted domain using a Domain Administrator account.
2. Create a temporary folder on the server.

   For example:

   ```
   C:\Temp
   ```

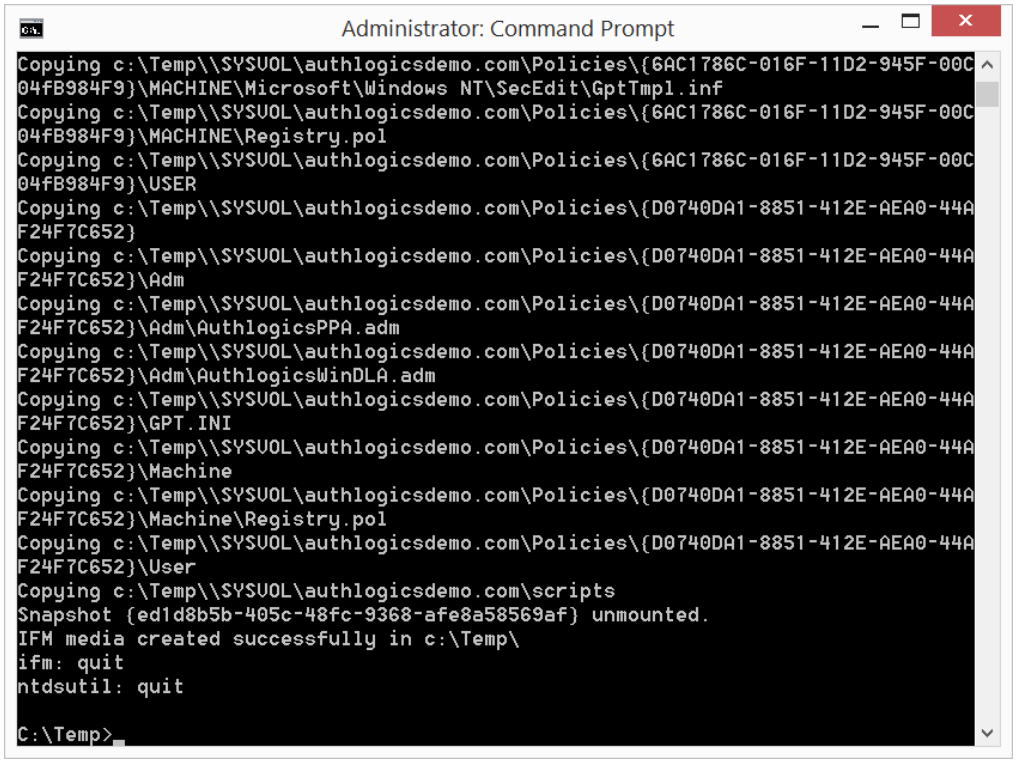
   Note: Ensure that the folder is empty.
3. Change directory to the temporary folder.
4. Type the following commands:

   ```
   ntdsutil

   activate instance ntds

   ifm

   create sysvol full C:\Temp\
   ```



5. Wait for the process to complete, then quit the ntdsutil operation:

   ```
   quit
   quit
   ```



On completion, the following folders remain in the extract folder:

- `Active Directory`
- `Registry`
- `SYSVOL`

To process and analyze the contents, copy the following files:

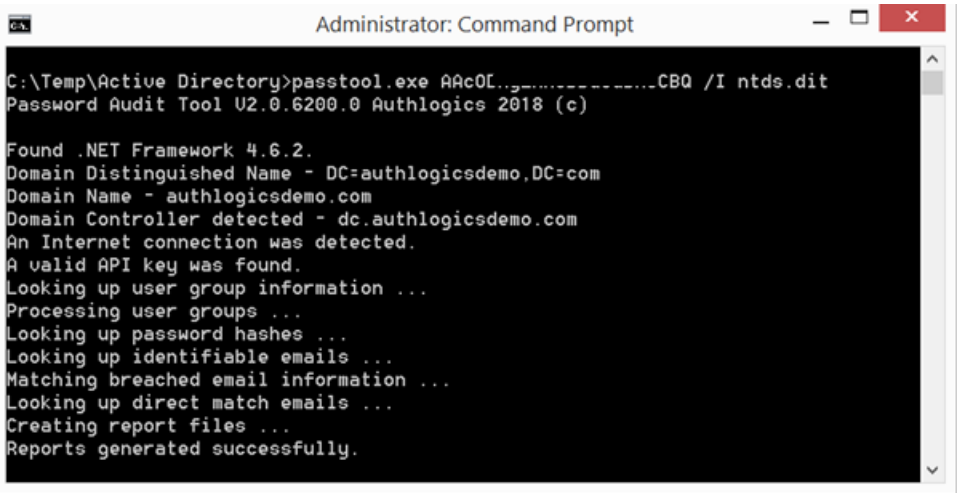
- `\Active Directory\NTDS.dit`
- `\Registry\SYSTEM`

to a temporary folder on a machine with the pre-requisites noted above. Copy the `passtool.exe` file to the same folder.

Note: As the process is manual, the residual files do not auto-clean and therefore you must delete them manually once the analysis has been processed.

Execute `passtool.exe` using the `/I` option specifying the `ntds.dit` file.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /I ntds.dit
```



3 Audit report result

When the analysis has been completed, the audit report results are created in a folder dated with the processing date.

The audit report contains the following text and comma-separated files:

Filename	Extension	Reported Offline	Description
`Summary-report`	`txt`	No	Consolidates analysis in a summary.
`Detail-report`	`txt`	Yes	Lists in detail accounts matching criteria of analysis control.
`Ad-principal-permissions`	`txt`	Yes	Lists the advanced security permissions for the root domain. Extracted using `ADPermissions` parameter.
`Aeskeymissing-accounts`	`csv`	Yes	Lists all Active Directory accounts where weak encryption algorithms like DES or RC4 can be used during authentication of accounts as these accounts are missing Kerberos AES Keys.
`Aeskeymissing-admin-accounts`	`csv`	Yes	Lists all Administrator Active Directory accounts where weak encryption algorithms like DES or RC4 can be used during authentication of accounts as these accounts are missing Kerberos AES Keys.
`Blankpwd-accounts`	`csv`	Yes	Lists all accounts that have a blank password .
`Blankpwd-admin-accounts`	`csv`	Yes	Lists all Administrator accounts that have a blank password.
`Breached`	`csv`	No	Lists all the Active Directory accounts with breached passwords.
`Breached-administrators`	`csv`	No	Lists all the administrator Active Directory accounts with breached passwords.
`Breached-common`	`csv`	No	Lists all the Active Directory accounts with commonly breached passwords; that is, these passwords have been breached thousands of times and therefore are deemed to be common.
`Breached-identifiable`	`csv`	No	Lists all the Active Directory accounts with breached passwords which can be traced to social media and other breaches based on breached password in use.

Filename	Extension	Reported Offline	Description
Breached-matching	csv	No	Lists all the Active Directory accounts with breached passwords which match the local domain name; that is, the username/email address and password are breached and can be used to authenticate to the domain.
Defaultpwds-accounts	csv	Yes	Lists all the Active Directory accounts where the password is set to the default password (logon username).
Defaultpwds-admin-accounts	csv	Yes	Lists all the administrator Active Directory accounts where the password is set to the default password (logon username).
Deskeyonly-accounts	csv	Yes	Lists all the Active Directory accounts using DES as the block cipher for encryption and susceptible for brute force attacks.
Deskeyonly-admin-accounts	csv	Yes	Lists all the administrator Active Directory accounts using DES as the block cipher for encryption and susceptible for brute force attacks.
Domain-breaches	csv	No	Lists all the email address in the MyID Password Breach Database matching the domain name.
Dormant-accounts	csv	Yes	Lists all accounts that have not logged on for the period of days specified by the /DormantDays parameter. The default is 90 days.
Dormant-admin-accounts	csv	Yes	Lists all administrator accounts that have not logged on for the period of days specified by the /DormantDays parameter. The default is 90 days.
Lmhashpwdexists-accounts	csv	Yes	Lists all the Active Directory accounts with passwords stored in LM Hash form. Extracted using the VerboseUserDetails parameter.
Lmhashpwdexists-admin-accounts	csv	Yes	Lists all the administrator Active Directory accounts with passwords stored in LM Hash form.

Filename	Extension	Reported Offline	Description
Never-logged-on-accounts	csv	Yes	Lists all accounts that have never logged on.
Preauthnotreqd-accounts	csv	Yes	Lists all the Active Directory accounts with where pre-authentication has been disabled.
Preauthnotreqd-admin-accounts	csv	Yes	Lists all the administrator Active Directory accounts with where pre-authentication has been disabled.
Servicedelegatable-admin-accounts	csv	Yes	Lists all the administrator Active Directory accounts which can be delegated as a service.
Shared-passwords	csv	Yes	Lists the partial hash of the shared passwords and accounts that share those passwords.
Shared-passwords-administrators	csv	Yes	Lists the partial hash of the shared passwords and accounts that share those passwords with administrator accounts.
Blacklist-passwords	csv	Yes	Lists the partial hash of the passwords and administrator accounts that match the passwords specified in the custom Blacklist.txt file.
Blacklist-passwords-administrators	csv	Yes	Lists the partial hash of the passwords and accounts that match the passwords specified in the custom Blacklist.txt file.
Summary	csv	No	As with Summary-report, only in CSV format.

3.1 Audit controls

Name	Administrator accounts with passwords that have been breached
Risk Severity	Critical
Description	The Administrator accounts that have a password that appears in at least one public breach and also are members of one or more of the following Active Directory Groups: Administrators, Domain Admins, Enterprise Admins. Because these accounts have elevated privileges, the passwords should be changed to one that does not appear in a breach.
Remediation	Force the users to change their passwords to a NIST compliant password.

Name	Accounts with passwords that have been found in previous breaches
Risk Severity	High
Description	User accounts with passwords that have been found in any breach. The password does not need to be related to the user in any way, just that this password was found in a breach somewhere at least once. This is a key part of the NIST 800-63 password guidelines, meaning this password should be changed to one that has not appeared in a breach to comply with these guidelines.
Remediation	Force the users to change their passwords to a NIST compliant password.

Name	Accounts with passwords that are commonly breached
Risk Severity	Critical
Description	User accounts with passwords that appear often in breaches (usually more than 100 times). This means that the password is often found in breaches and would mean it could appear in a list of common passwords bad actors would use to try gain access to an account. Because these passwords are commonly breached, these passwords should be reset and users should choose a password that has not been breached.
Remediation	Force the users to change their passwords to a NIST compliant password.

Name	Breached account passwords with identifiable information
Risk Severity	High
Description	These users have passwords that have been breached and list those with identifiable information, such as email addresses, that could allow bad actors to tie information in this password breach back to the user, allowing them to gain access to their account. The email address does not have to belong to a specific domain, the account details are used to look at full or partial matches for any email address information that could be used to identify the user. Each user password in the list should be immediately changed to a non-breached password if there is a suspicion that the email information supplied could identify the user account and allow a bad actor to gain access.
Remediation	Force the users to change their passwords to a NIST compliant password.

Name	Breached accounts with matching emails and passwords
Risk Severity	Critical
Description	Lists users with breached passwords and email addresses that are tied directly to the active directory domain or to the domain supplied to the tool. Because both the identifying information as well as the passwords in the list match a known breach these accounts are highly likely to be compromised. These passwords for these accounts should be changed immediately to a secure, compliant password.
Remediation	Force the user to change their passwords and apply multi-factor authentication to their account as they have been compromised and that their details are known.

Name	Accounts with shared passwords
Risk Severity	High
Description	List of users by password hash that share the same password. Shared passwords can be used to compromise multiple accounts and may be against local password policies or indicate that default passwords have not been changed.
Remediation	Force the user to change their passwords and ensure that users with multiple accounts (Administrative, standard, system, and test accounts) do not re-use this password across accounts.

Name	Emails for this domain with breached passwords
Risk Severity	High
Description	List of all emails found in password breaches for the active directory domain or to the domain supplied to the tool. This list provides a good indication of the amount of user account information available for use by bad actors. It does not indicate that any of these accounts have passwords that have been breached; however, these accounts are at higher risk of being involved in a breach as they are publicly associated with this domain.
Remediation	Apply multi-factor authentication to these accounts as their credentials have been compromised and the account may already have been hacked or is currently subject to attacks.

Name	Administrator Accounts with a Blank Password
Risk Severity	Critical
Description	Lists all the Active Directory administrator accounts which have a blank password assigned to them. Should these accounts be active, then bad actors will have the ability to log in as an administrator without needing to provide a password.
Remediation	Force these administrators to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the administrator's account as their account details are known and therefore it is safe to assume that the account has been hacked or is currently subject to multiple attacks.

Name	Accounts with a Blank Passwords
Risk Severity	High
Description	Lists all the Active Directory accounts which have a blank password assigned to them. Should these accounts be active, then bad actors will have the ability to log in with this user account without needing to provide a password.
Remediation	Force the users to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the user's accounts as their account details are known and therefore it is safe to assume that the account has been hacked or is currently subject to multiple attacks.

Name	Administrator Accounts with Default Password
Risk Severity	Critical
Description	Lists all the Active Directory administrator accounts which have the default Active Directory password assigned to them. Should these accounts be active, then bad actors will have the ability to log in with this administrator account with a known and highly compromised password.
Remediation	Force these administrators to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the administrator's account as their account details are known and therefore it is safe to assume that the account has been hacked or is currently subject to multiple attacks.

Name	Accounts with Default Password
Risk Severity	High
Description	Lists all the Active Directory accounts which have the default Active Directory password assigned to them. Should these accounts be active, then bad actors will have the ability to log in with this user account with a known and highly compromised password.
Remediation	Force the users to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the user's accounts as their account details are known and therefore it is safe to assume that the account has been hacked or is currently subject to multiple attacks.

Name	Administrator Accounts with AES Key Missing
Risk Severity	High
Description	When AES encryption keys are not present, only weak encryption algorithms (DES and RC4) can be used and are susceptible to brute-force attacks.
Remediation	Raise the domain-functional level to 2008 or above. Force the administrators to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the users.

Name	Accounts with AES Key Missing
Risk Severity	Moderate
Description	When AES encryption keys are not present, only weak encryption algorithms (DES and RC4) can be used and are susceptible to brute-force attacks.
Remediation	Raise the domain-functional level to 2008 or above. Force the users to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the users.

Name	Administrator Accounts with DES Key Only
Risk Severity	High
Description	Administrator accounts with a DES key only assigned to them are using weak encryption algorithms and are highly susceptible to brute-force attacks.
Remediation	Apply DES encryption keys to these accounts. Force the administrators to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the user's accounts.

Name	Accounts with DES Key Only
Risk Severity	Moderate
Description	Accounts with a DES key only assigned to them are using weak encryption algorithms and are highly susceptible to brute-force attacks.
Remediation	Apply DES encryption keys to the accounts. Force the users to change their passwords to a NIST-compliant password. Apply multi-factor authentication to the user's accounts.

Name	Administrator Accounts with LAN Manager HASHed Passwords
Risk Severity	High
Description	LAN Manager Hash is a very weak hashing algorithm and is very susceptible to brute-force attacks.
Remediation	Set the Active Directory to prevent passwords from being stored with LAN Manager Hash. Reset the password on the administrator and apply multi-factor authentication to the account.

Name	Accounts with LAN Manager HASHed Passwords
Risk Severity	Moderate
Description	LAN Manager Hash is a very weak hashing algorithm and is very susceptible to brute-force attacks.
Remediation	Set AD to prevent passwords from being stored with LAN Manager Hash. Reset the password on the account and apply multi-factor authentication to the account.

Name	Dormant Administrator Accounts
Risk Severity	Moderate
Description	Lists all Active Directory administrator accounts that have not logged on for an extended period of time.
Remediation	Determine whether or not these administrator accounts are still required and, if not, consider disabling or removing these accounts from the environment.

Name	Dormant Accounts
Risk Severity	Low
Description	Lists all AD Accounts that have not logged on for an extended period of time.
Remediation	Determine whether or not these accounts are still required and, if not, consider disabling or removing these accounts from the environment.

Name	Accounts Never Logged-On
Risk Severity	Low
Description	Lists all AD Accounts that have never been used to login with.
Remediation	Determine whether these accounts are required and if not, consider disabling or removing these accounts from the environment.

Name	Administrator accounts where Kerberos pre-authentication is not required
Risk Severity	Moderate
Description	Kerberos pre-authentication is enabled to prevent offline password-guessing attacks and is implemented by default.
Remediation	Enable Kerberos pre-authentication on the accounts. Force the users to change their passwords to a NIST-compliant password.

Name	Accounts where Kerberos pre-authentication is not required
Risk Severity	Low
Description	Kerberos pre-authentication is enabled to prevent offline password-guessing attacks and is implemented by default.
Remediation	Enable Kerberos pre-authentication on the account. Force the users to change their passwords to a NIST-compliant password.

Name	Administrator account allowed to be delegated as a service
Risk Severity	Moderate
Description	Least-privilege access models dictate that administrator accounts should never be delegated to a service. Service accounts should be left as dedicated service accounts.
Remediation	Disable the Active Directory account option allowing Administrator accounts from being delegated as a service.