

Machine Key Tool

Introduction

Use this guide to install and use the Machine Key Tool.

Applies to

SecureAuth IdP

Discussion

What is the Machine Key Tool?

The Machine Key Tool enables an administrator to backup, restore, and grant / revoke privileges for a SecureAuth IdP Appliance machine key (NetFrameworkConfigurationKey). A machine key is used for encrypting / decrypting the SecureAuth IdP web.config files.

Disclaimer

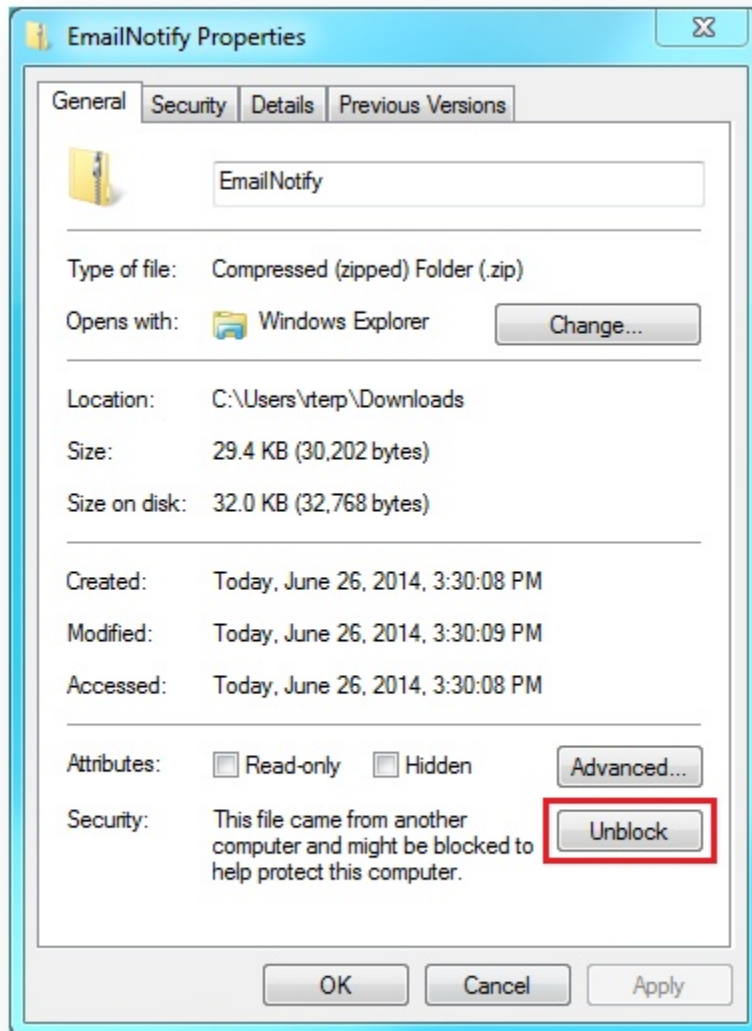
THIS SOFTWARE IS PROVIDED "AS IS" AND SECUREAUTH CORPORATION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL SECUREAUTH CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

System Requirements

The Machine Key Tool requires a SecureAuth IdP Appliance on Microsoft Windows Server 2008 R2, 2012, or 2012 R2.

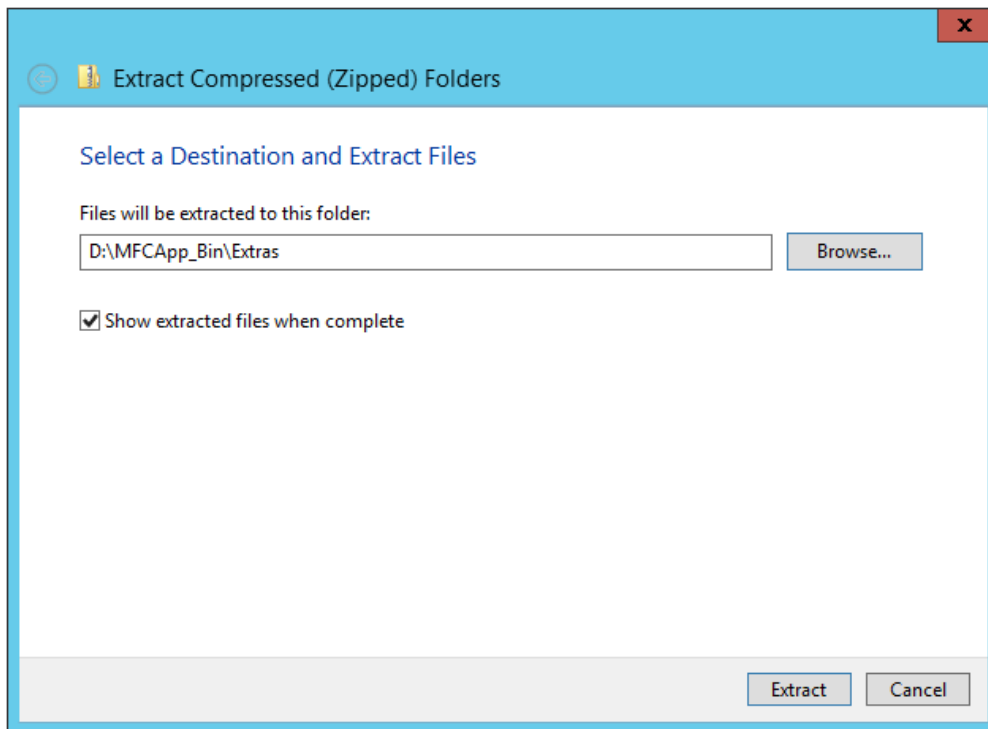
Installation

- 1) [Download the tool](#)
- 2) Navigate to the download, right-click on the archive, select **Properties**, and switch to the **General tab**
- 3) If there is a button titled **Unblock** present in the tab, then click it, and press **OK** to dismiss the Properties window



4) Navigate to the download, right-click on the archive, and select **Extract All...**

5) [Extract the archive](#) to **D:\MFCApp_Bin\Extras**

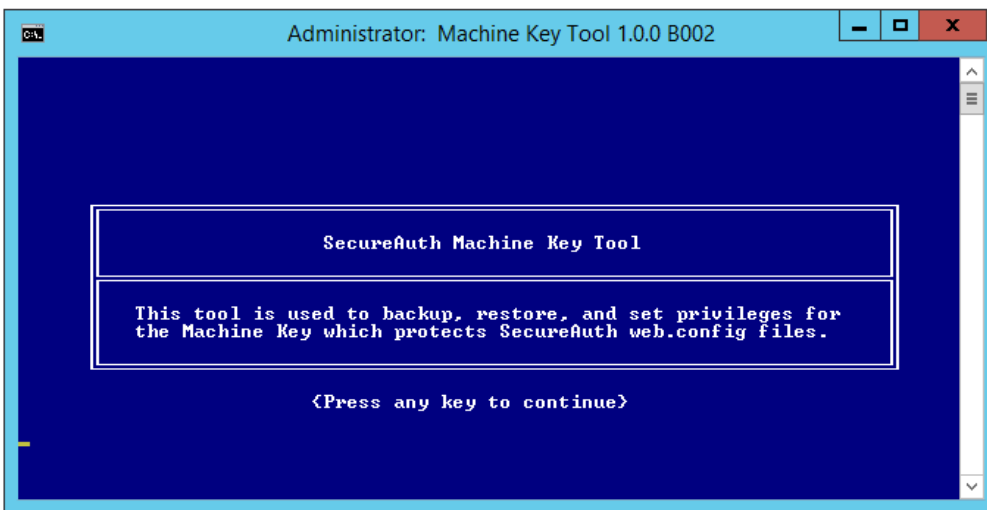


Usage

Backup


1) To backup the Machine Key, navigate to `D:\MFCApp_bin\Extras\MachineKeyTool` and run `Machine Key Tool.bat`

The *Splash* page displays



The *Legal disclaimer* displays

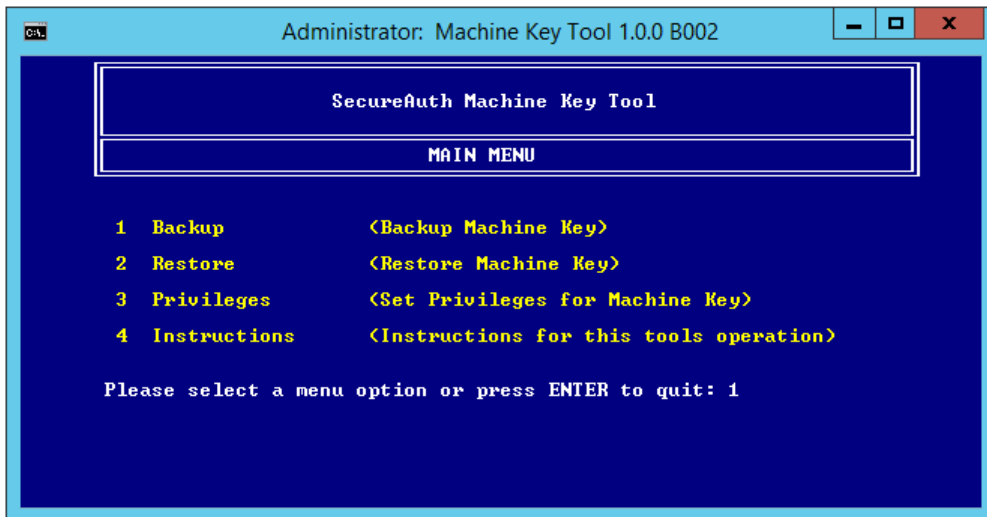
2) Type **AGREE** at the prompt to accept the terms, and press **Enter** and continue to step 3

 If the terms are not agreeable, then press **Enter** and the script exits automatically



The **Main Menu** displays

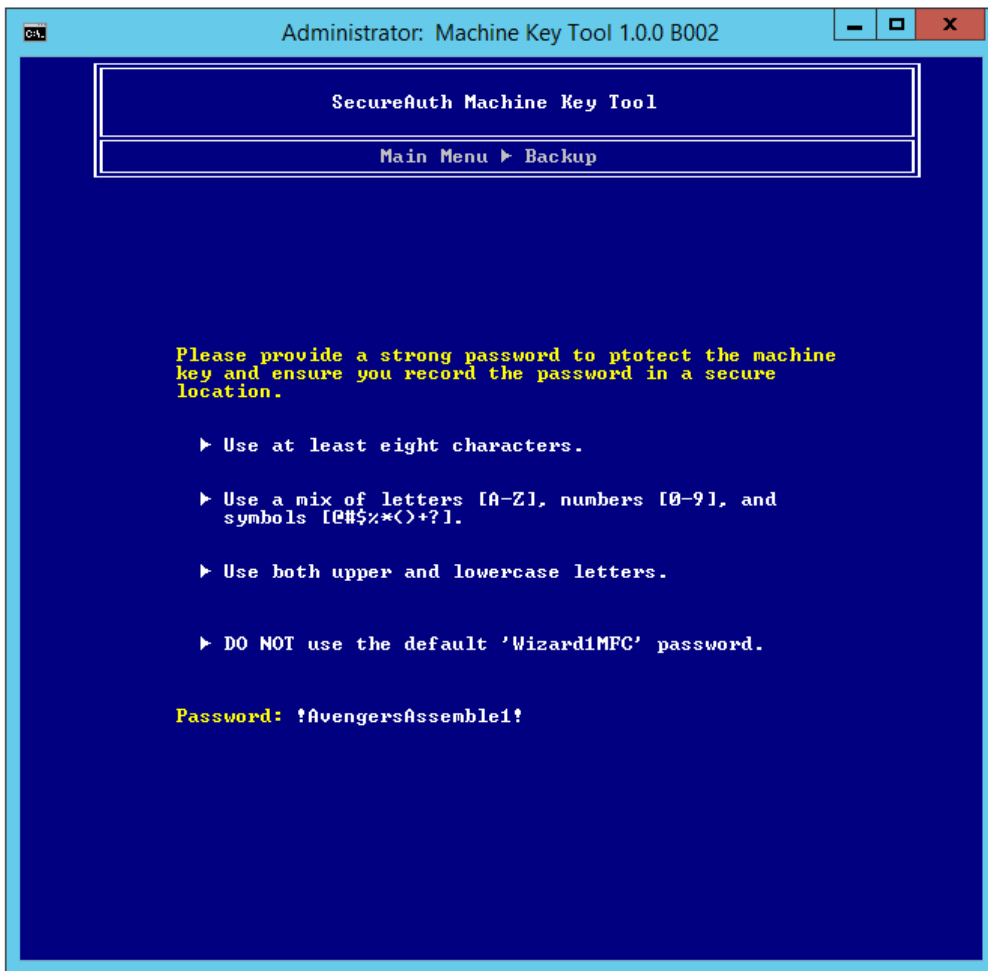
3) Type **1** and press **Enter** to start the backup



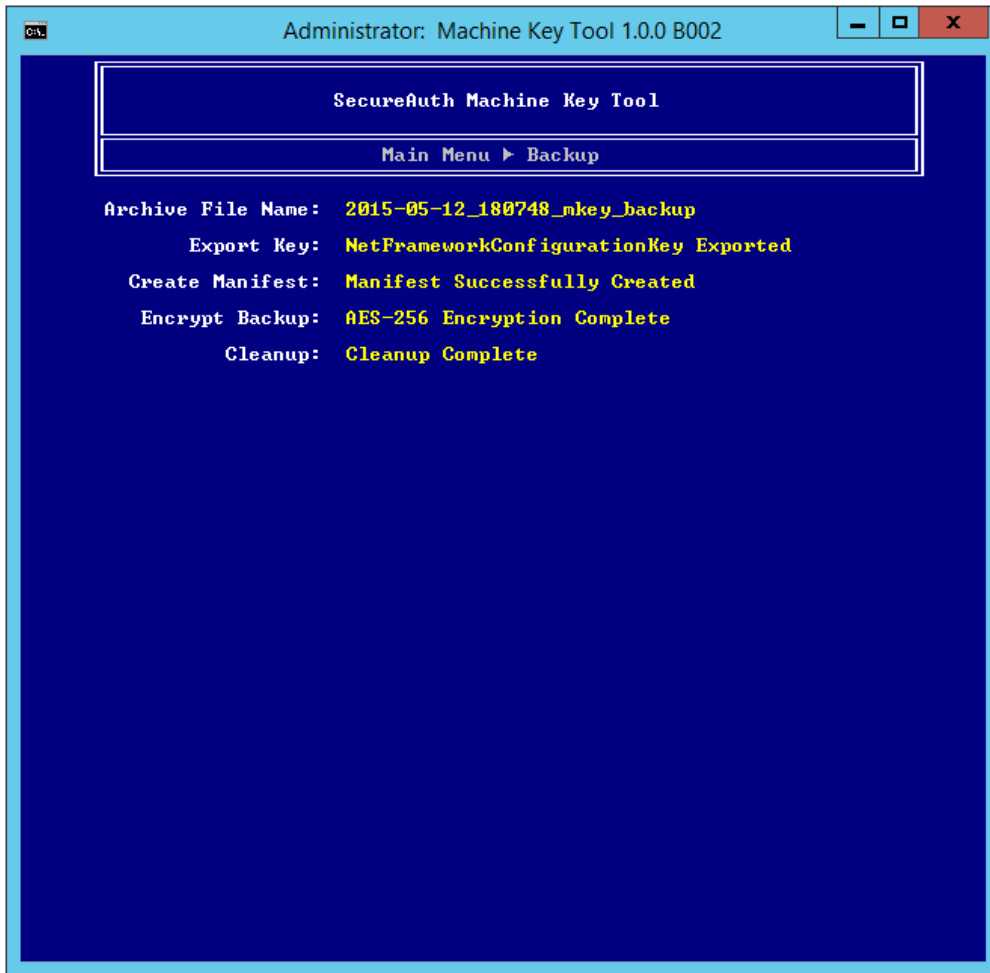
4) Provide a [strong password](#) to protect the backup and press **Enter** to continue



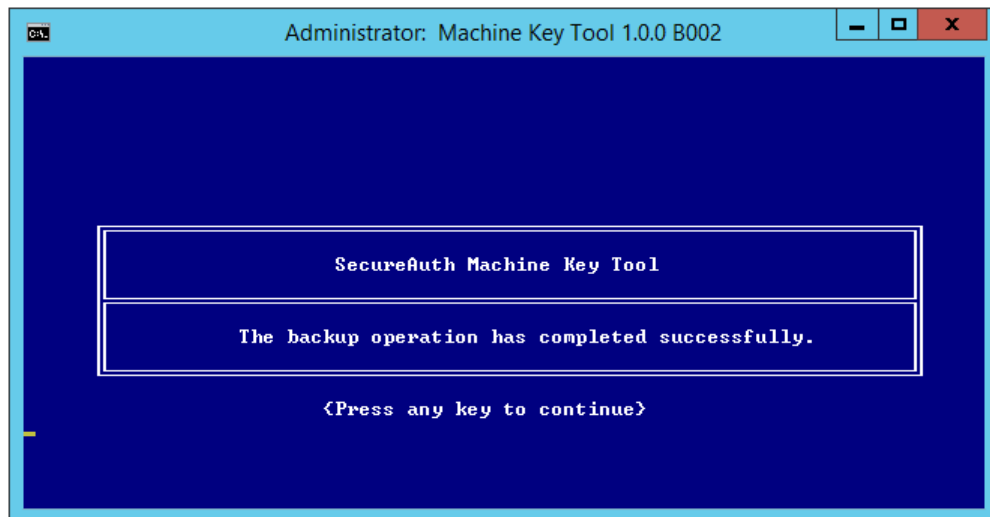
Passwords may only contain the following special characters @ # \$ % * () + ? ; and if an unsupported character is used, the backup may fail



The backup will now begin running



The backup process is complete



Restore

Decrypt the web.config Files

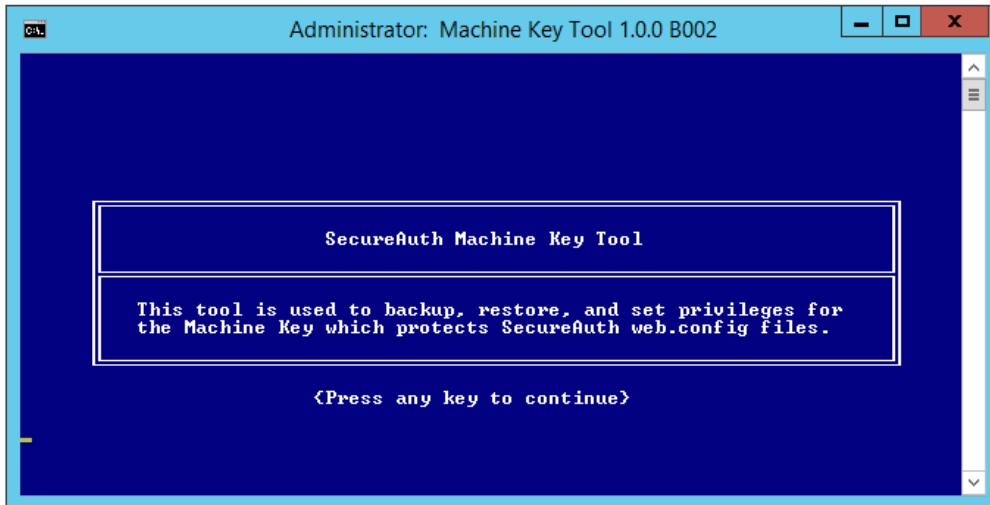
Before performing a restore, it is necessary to decrypt the web.config files through the SecureAuth administrative interface

See the support document [SecureAuth IdP Realm Guide](#); section Decrypting / Encrypting Realms

1. Launch the SecureAuth administrative interface
2. Click the **Decrypt WebConfig** link/button
3. Click the **Select/Unselect All** link and the **Decrypt** button
1. Launch the SecureAuth administrative interface
2. Click the **Decrypt WebConfig** button
3. Click the **Select/Unselect All** link and the **Decrypt** button

1) To restore a Machine Key from backup, navigate to **D:\MFCApp_bin\Extras\MachineKeyTool** and run **Machine Key Tool.bat**

The **Splash** page displays



The **Legal disclaimer** displays

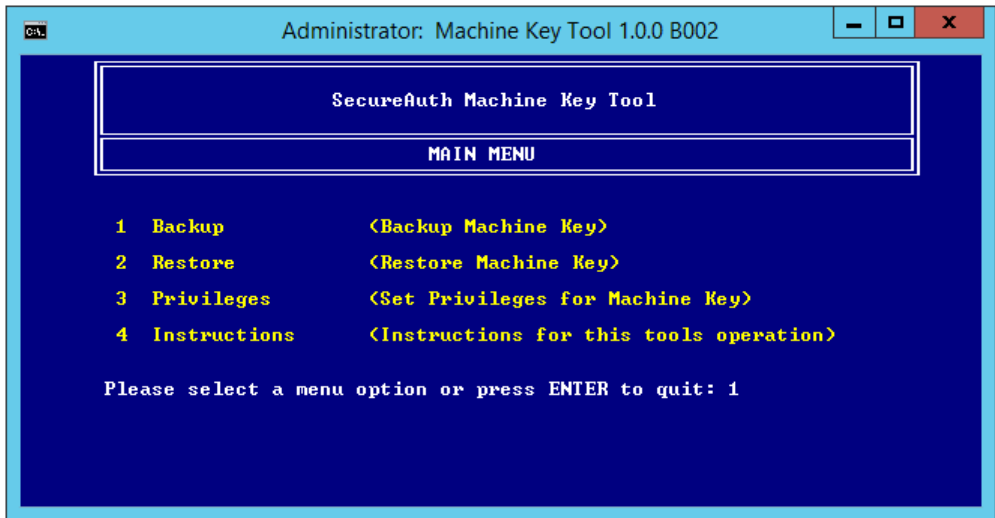
2) Type **AGREE** at the prompt to accept the terms, and press **Enter** and continue to step 3

i If the terms are not agreeable, then press **Enter** and the script exits automatically



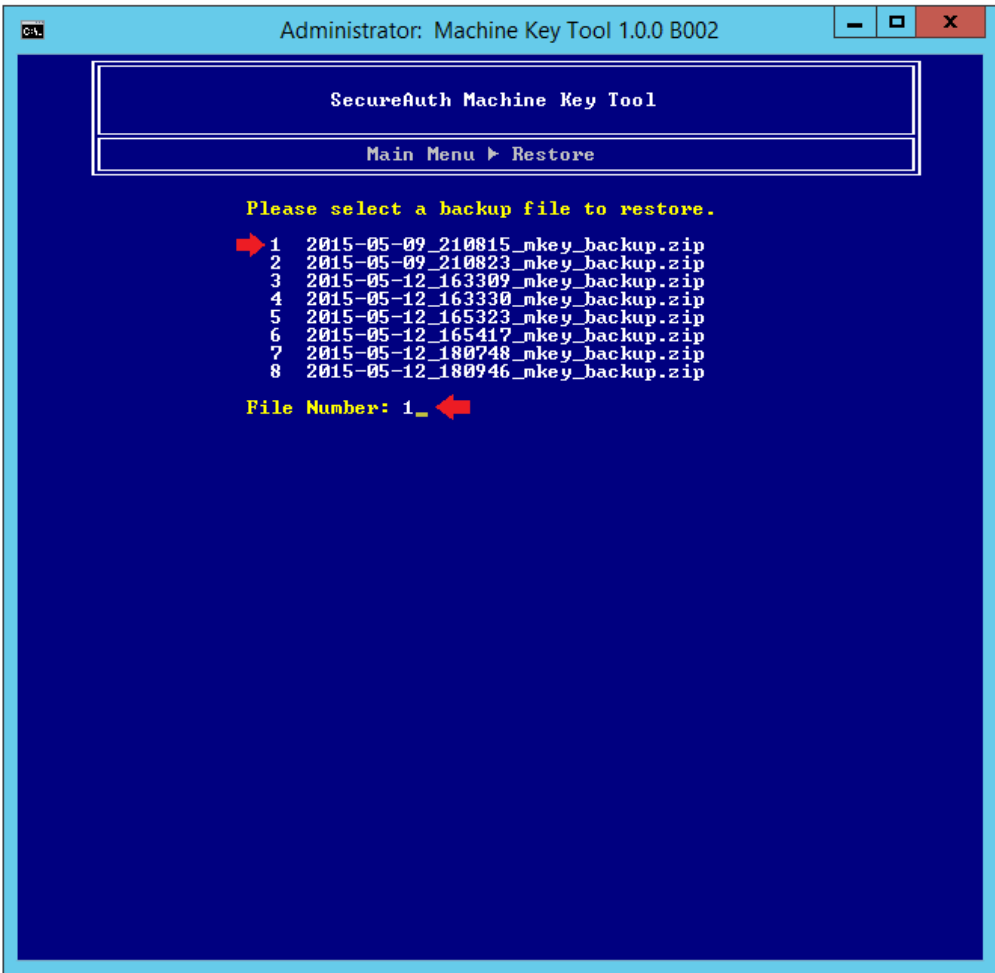
The **Main Menu** displays

3) Type **2** and press **Enter** to start the restore

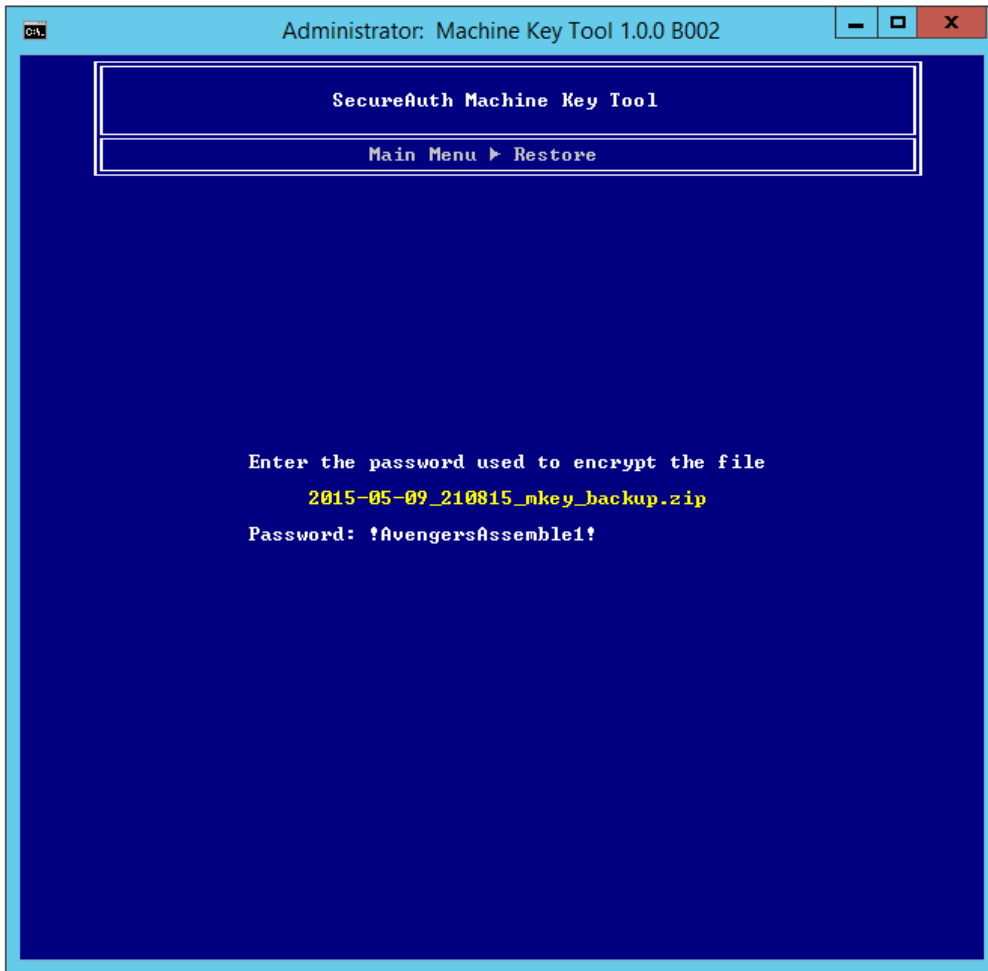


4) Select the backup file to restore by entering its number, and press enter

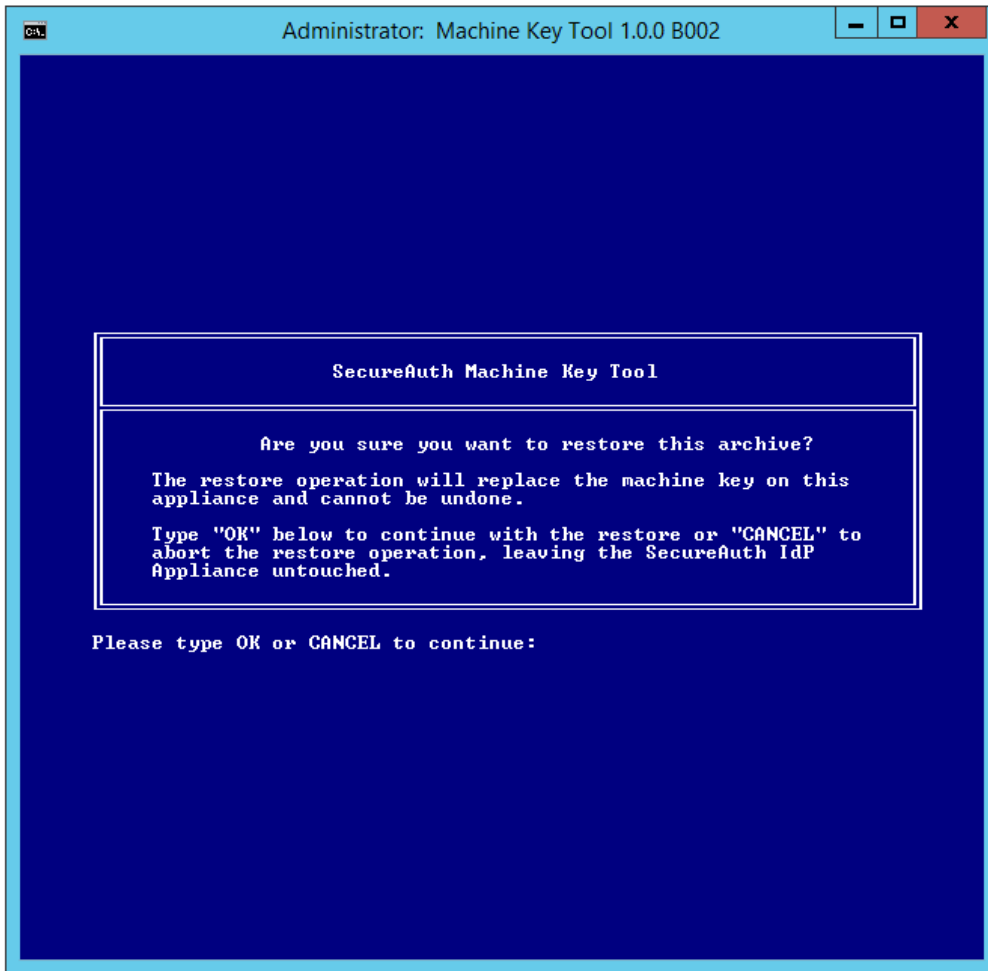
 The backup files are located at D:\MFCApp_Bin\SecureAuth_Archive



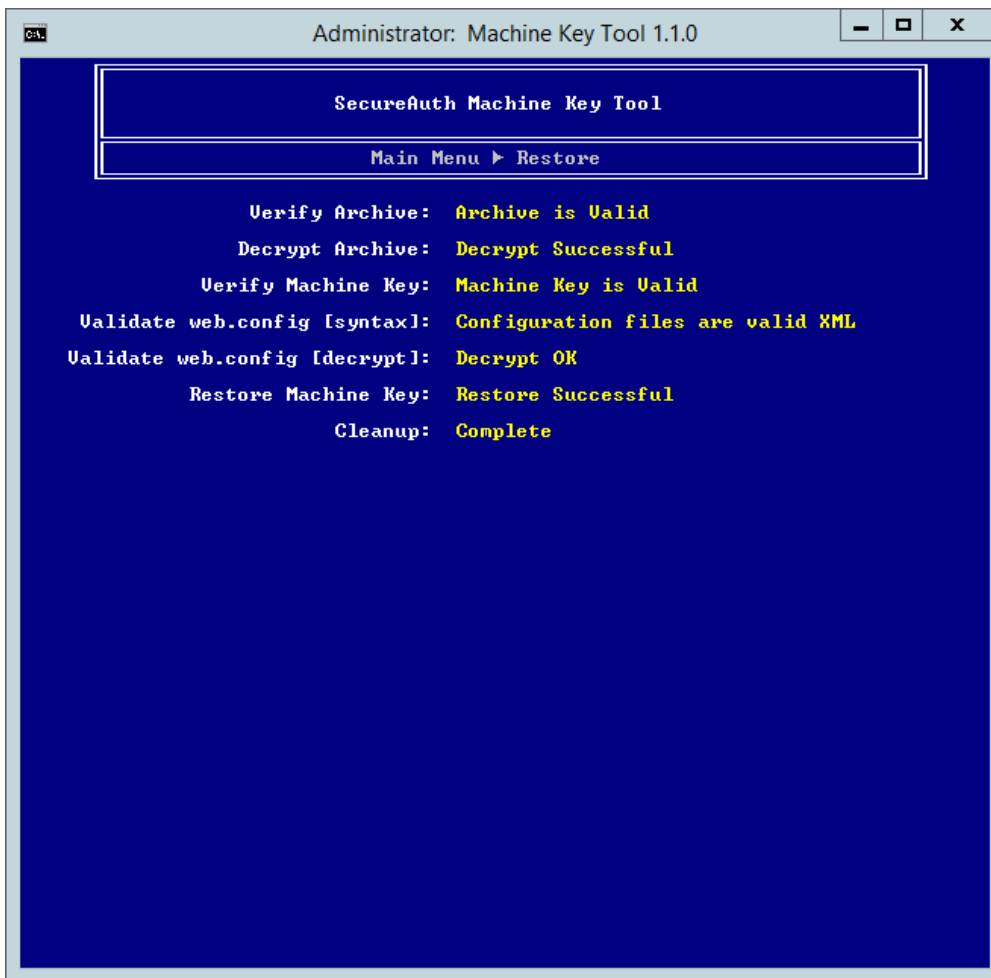
5) Enter the password used to encrypt the backup file



6) Type **OK** to continue with the restore or **CANCEL** to abort the restore process



The **Restore** process will now run

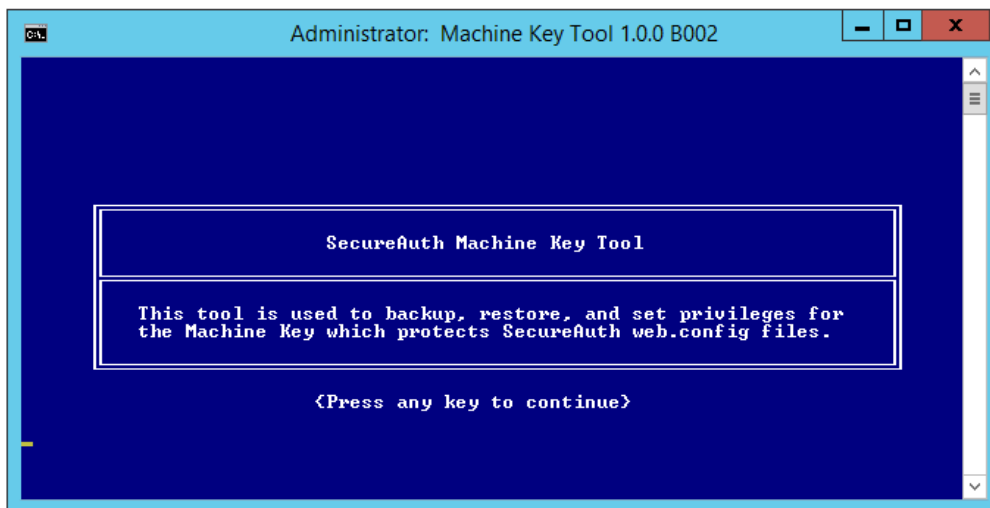


The restore process is now complete

Privileges


1) To allocate access control via privileges, navigate to **D:\MFCApp_bin\Extras\MachineKeyTool** and run **Machine Key Tool.bat**

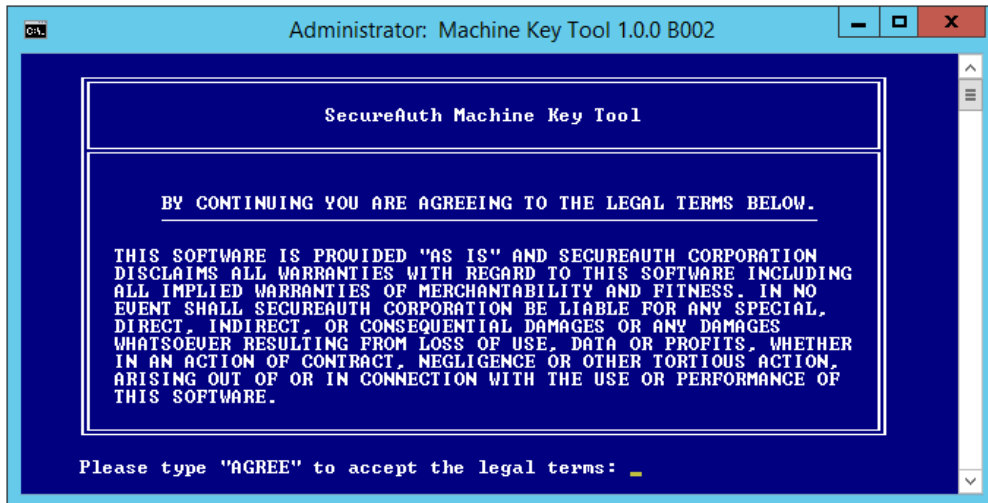
The **Splash** page displays



The **Legal disclaimer** displays

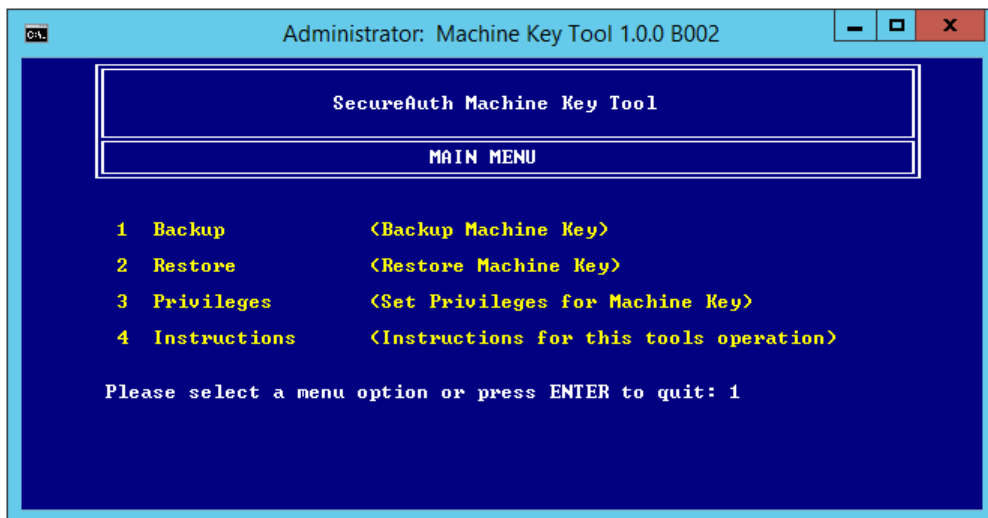
2) Type **AGREE** at the prompt to accept the terms, and press **Enter** and continue to step 3

 If the terms are not agreeable, then press **Enter** and the script exits automatically



The **Main Menu** displays

3) Type 3 and press **Enter** to start the restore



The **Privileges Menu** displays

3) Select the type of right to control

CA

Administrator: Machine Key Tool 1.0.0 B002



SecureAuth Machine Key Tool

Main Menu ▶ Privileges

Please select an option below:

▶ Press 'A' to set the Authenticated Users rights.

Select this option to grant Authenticated Users access to the machine key. This is normally used when the SecureAuth IdP Appliance hosts a realm utilizing the Windows IWA\SSO functionality.

▶ Press 'D' to set the Domain Users rights.

Select this option to grant the Domain Users group access to the machine key. This option should only be used under the supervision of SecureAuth support staff.

▶ Press 'E' to set the Everyone rights.

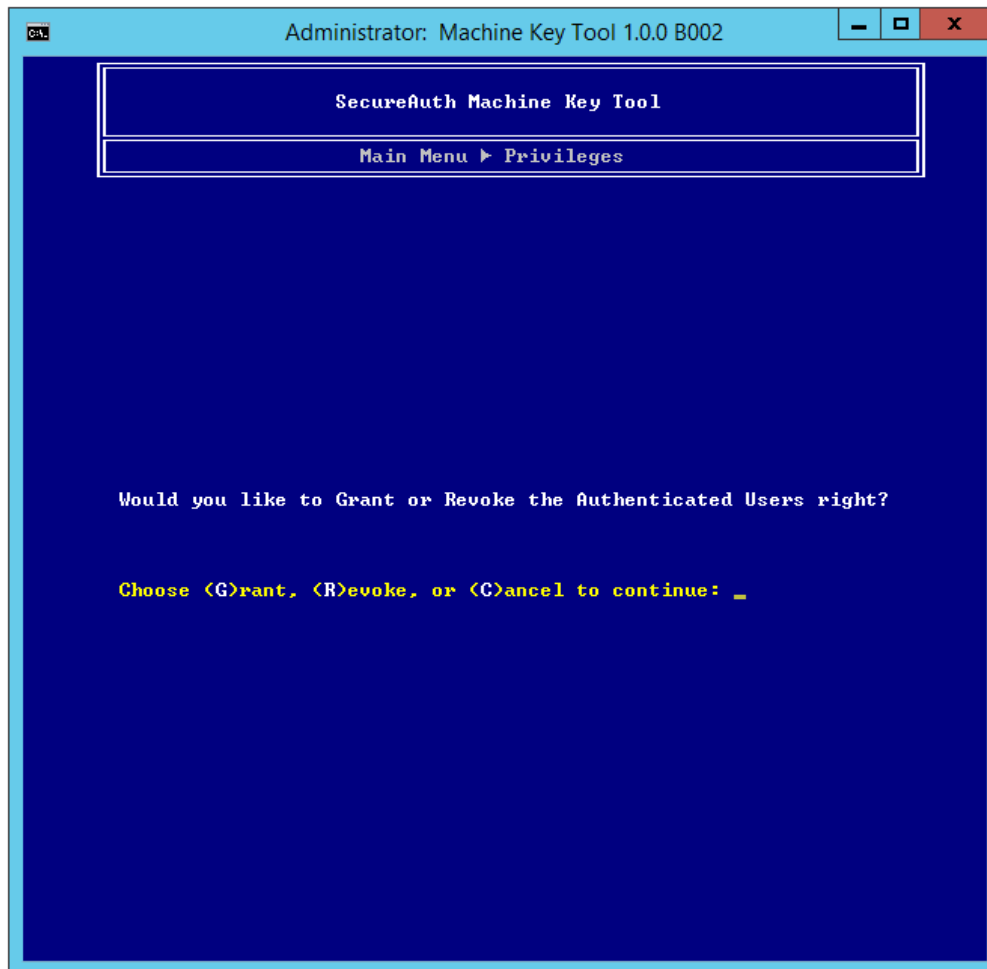
Select this option to grant the Everyone group access to the machine key. This option should only be used under the supervision of SecureAuth support staff.

Choose <A>uth, <D>omain, or <E>veryone to continue:



Select this option to grant Authenticated Users access to the machine key. This is normally used when the SecureAuth IdP Appliance hosts a realm utilizing the Windows IWA / SSO functionality.

- 1) Press **A** to manage the Authenticated Users group rights
- 2) Press **G** to Grant the Authenticated Users group access to the machine key, or **R** to revoke its access to the Machine Key

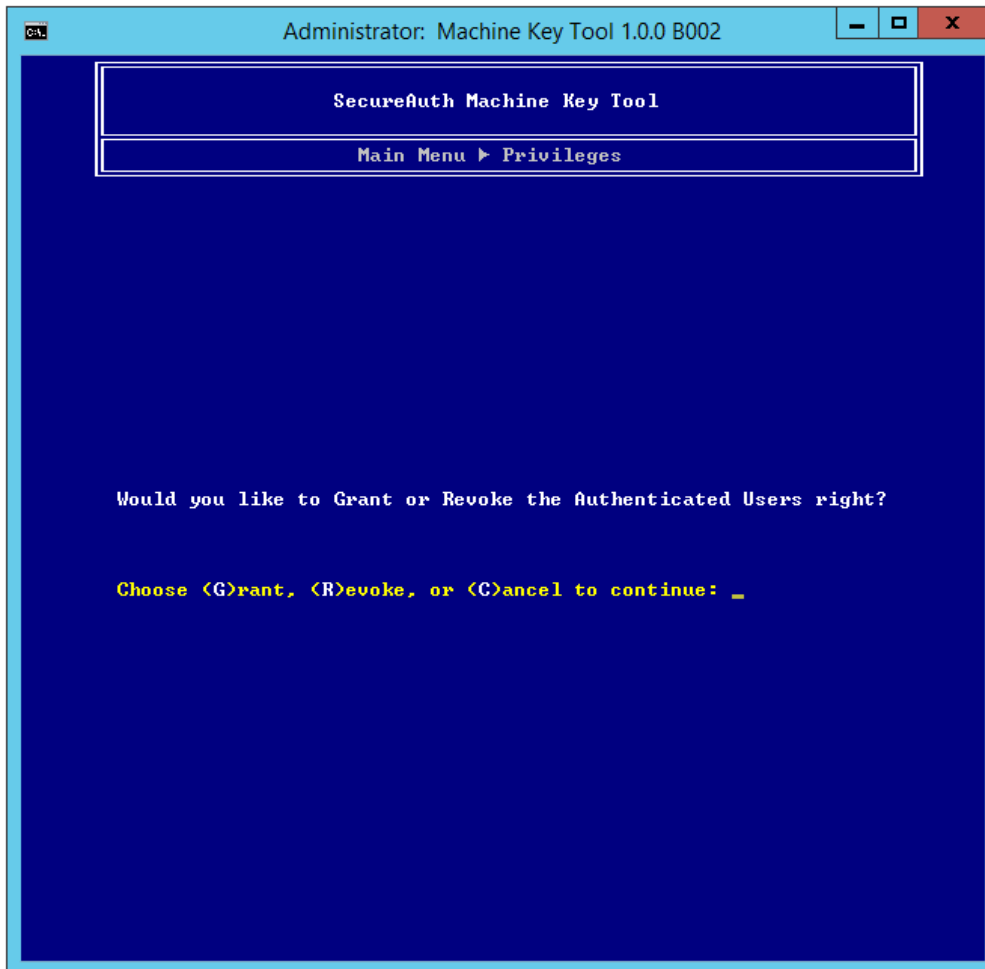


The tool now grants the appropriate access rights to both the Machine Key and the log files in the SecureAuth realms



This option should only be used under the supervision of SecureAuth support staff

- 1) Press **D** to manage the Domain Users group rights
- 2) Press **G** to Grant the Domain Users group access to the machine key, or **R** to revoke its access to the Machine Key

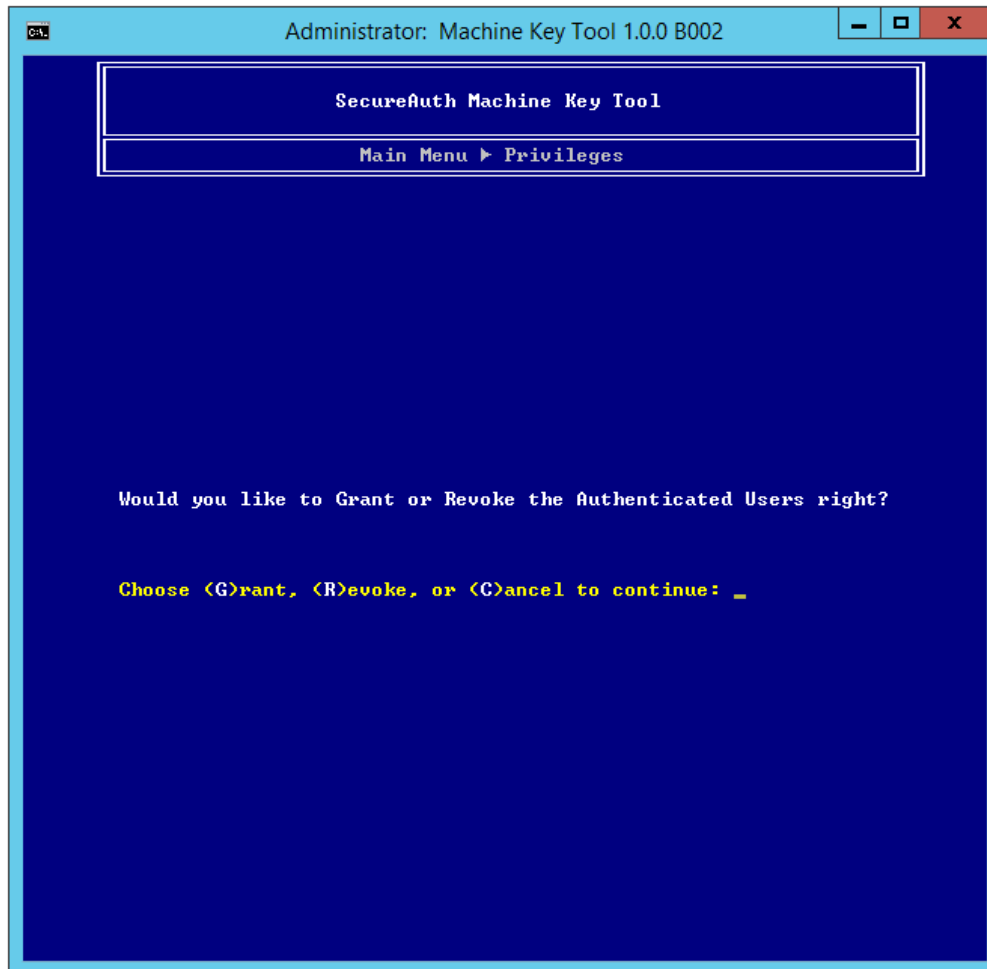


The tool now grants the appropriate access rights to both the Machine Key and the log files in the SecureAuth realms



This option should only be used under the supervision of SecureAuth support staff

- 1) Press **E** to manage the Everyone group rights
- 2) Press **G** to Grant the Everyone group access to the machine key, or **R** to revoke its access to the Machine Key



Release History

Machine Key Tool Release History

1.0.0 2015-05-15

- Initial release of tool

1.1.0 2016-05-17

- Deprecated WebConfigManager
- Updated 7Zip library to v16.0.0.0 to address reported security vulnerabilities