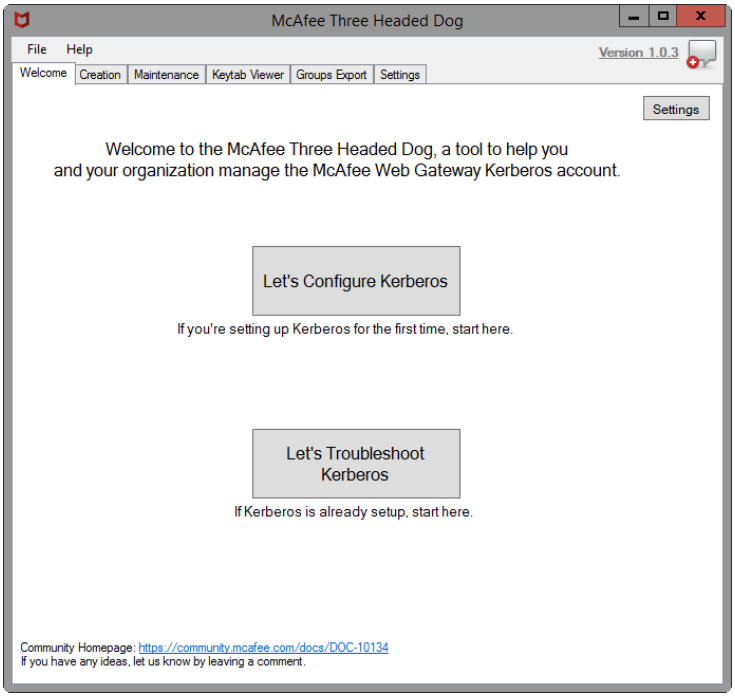
Introduction

Setting up Kerberos can be tough -- from an organizational standpoint as well as a technical standpoint. The McAfee Three Headed Dog (THD) is here to simplify the process by taking the guess work out of the syntax. THD will use smart defaults and validate the inputs to make sure you're on the right track.



Video Walkthrough

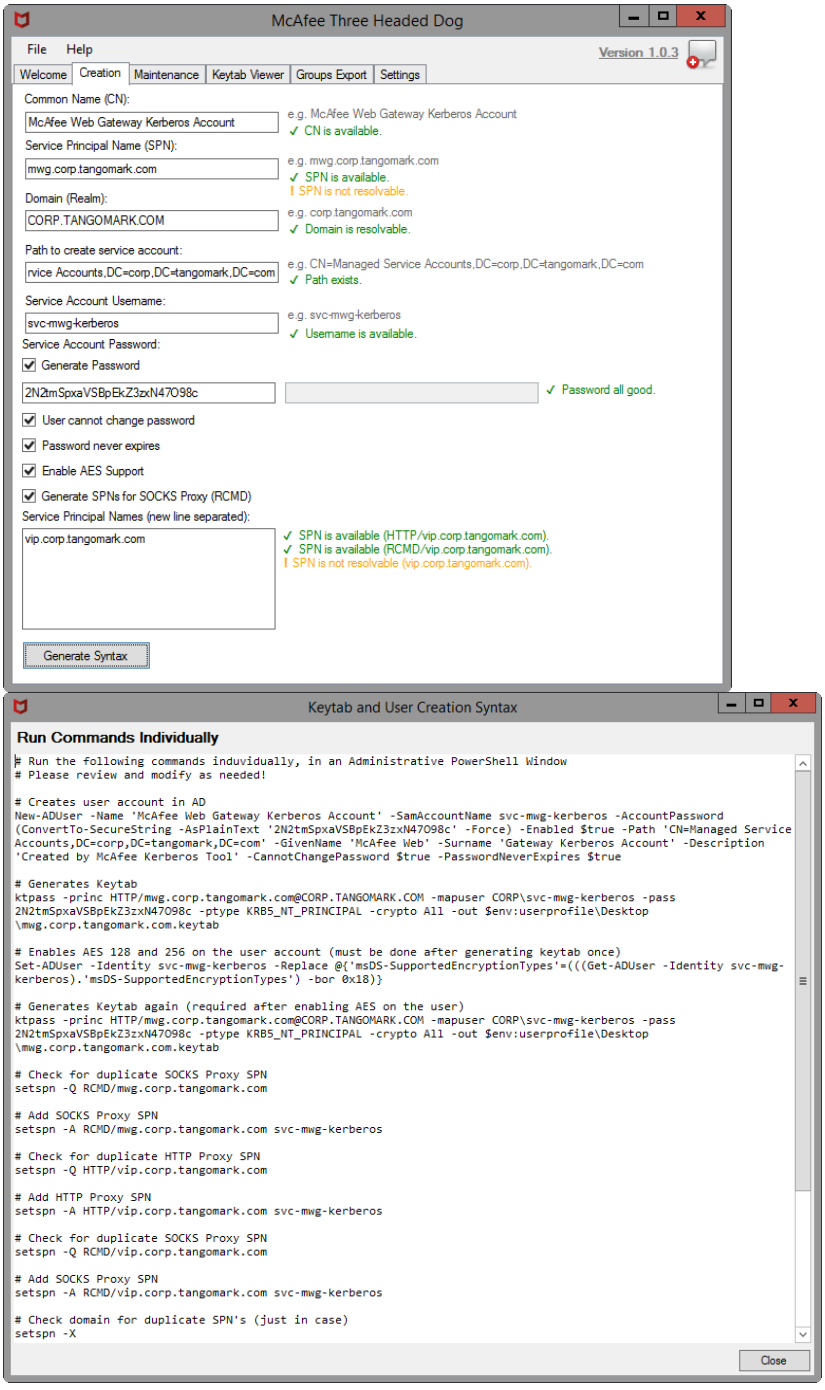
Web Gateway: Three Headed Dog (A Kerberos Setup Tool)

Uses

For version 1.0, the there are two use cases 1) Creation and 2) Maintenance.

Creation

For those setting up Kerberos for the first time, we help you get the syntax right on the first try. Once you have the Syntax, you can pass the commands to your Active Directory Administrator for them to modify as needed.

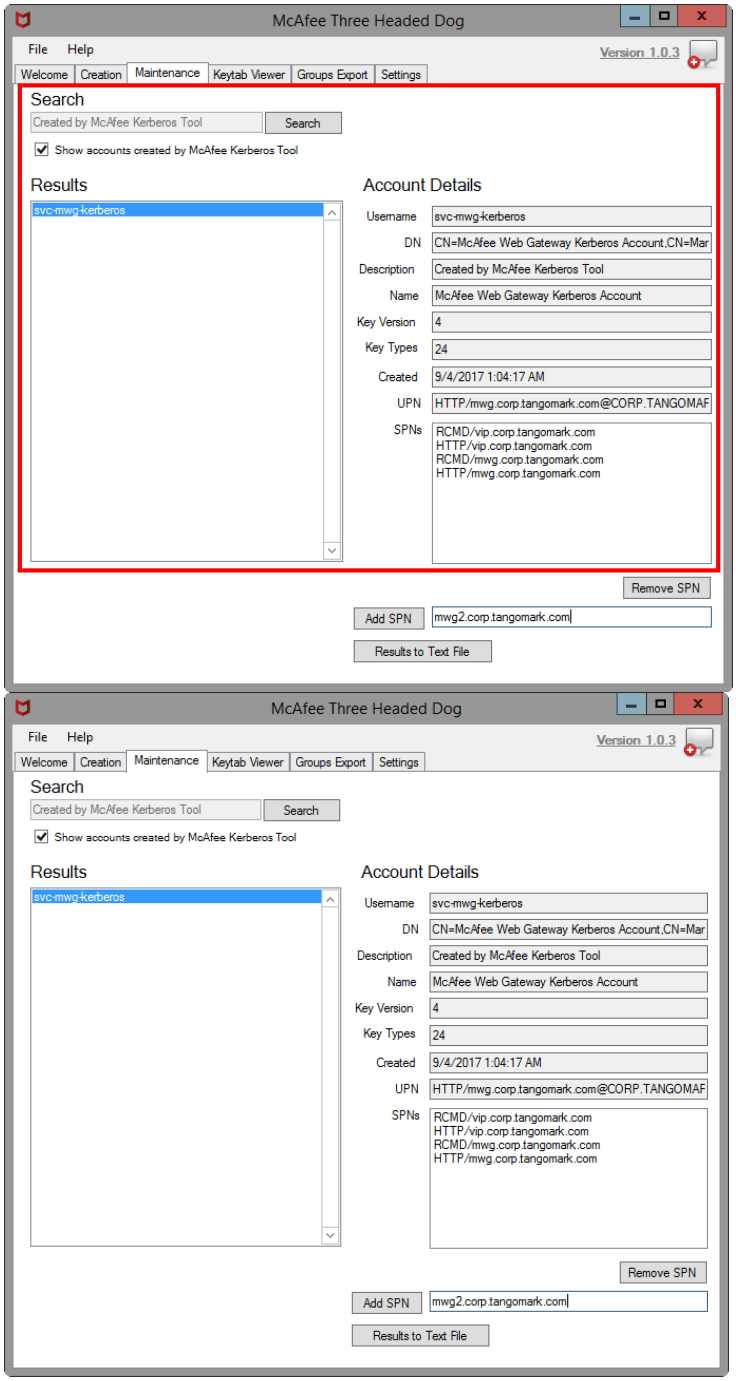


Maintenance

For those who've already got Kerberos setup and working, you may need to maintain your AD user account by adding or removing SPNs. Additionally, quickly reviewing the user account information is important (like getting the Key Version info).

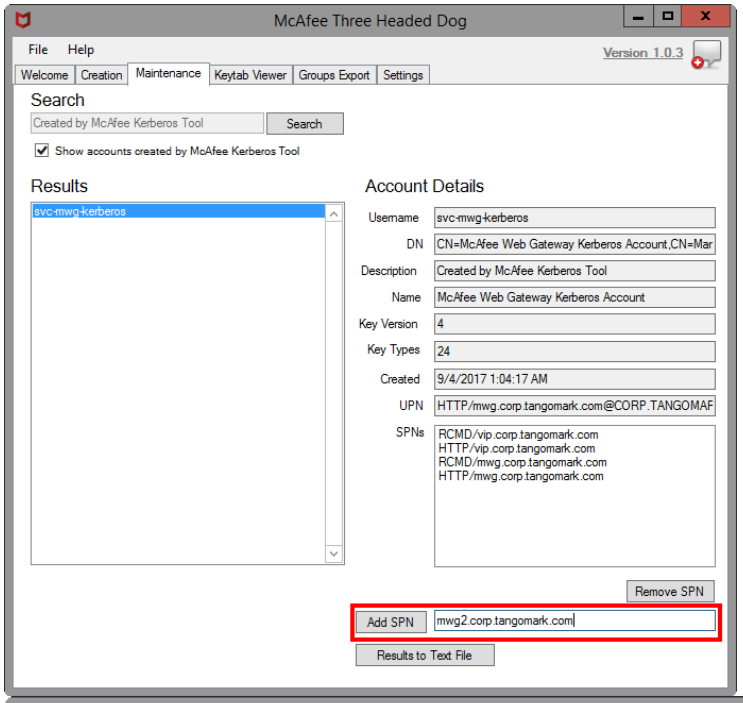
Search for Existing Accounts

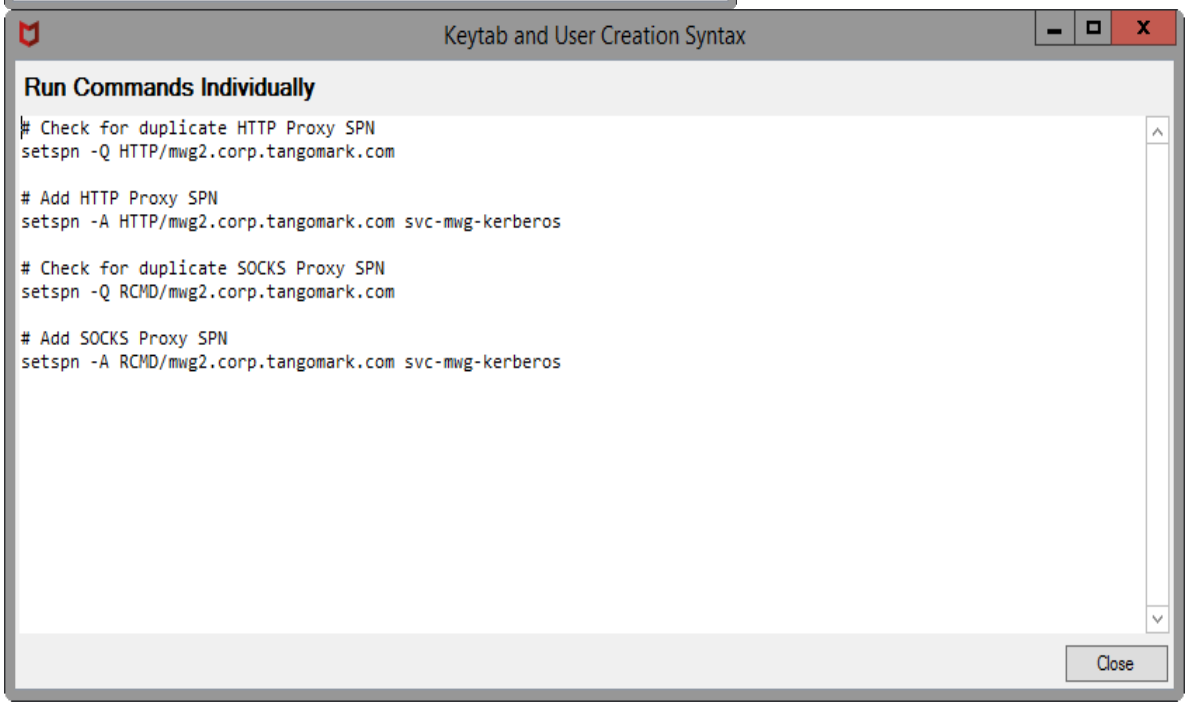
The search option allows you to lookup accounts in Active Directory and review their Kerberos attributes.



Adding an SPN

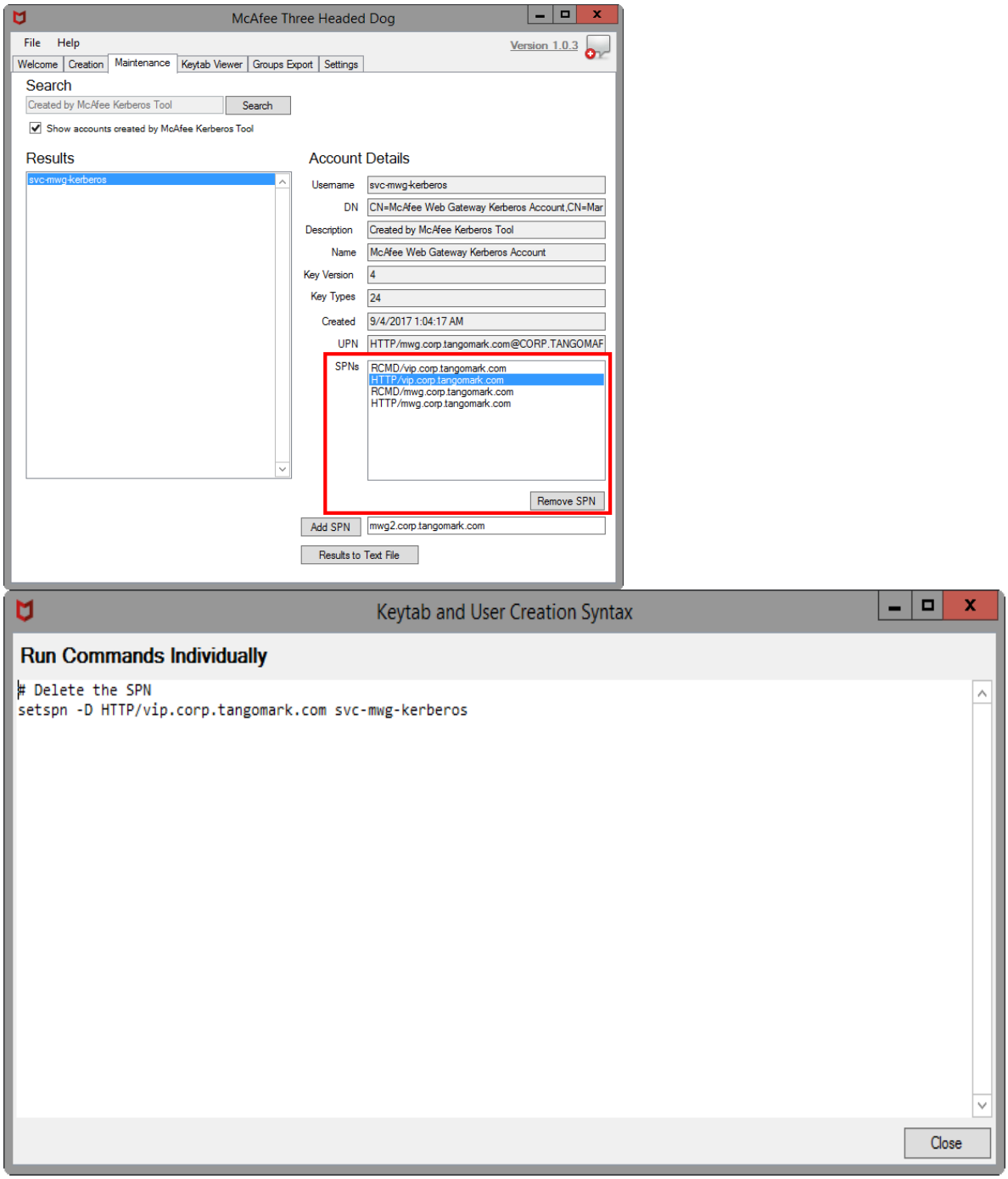
To add an SPN, type the FQDN into the text box next to the "Add SPN" button. Click the "Add SPN" button and syntax will be generated to add the SPN to the given user account.





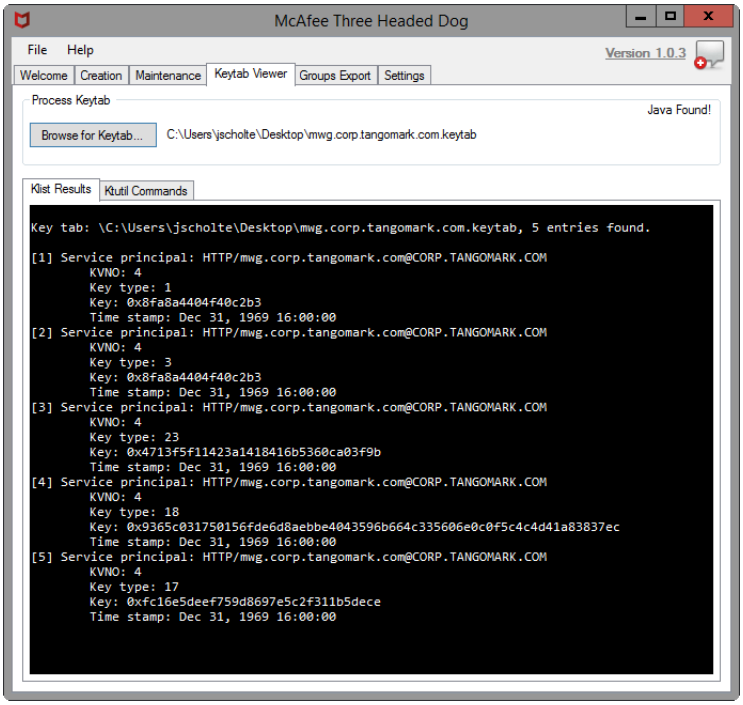
Delete an SPN

To delete an SPN, select a SPN from the list generated above, and click the button for "Remove SPN". This will generate syntax for removing the given SPN from the given user account.



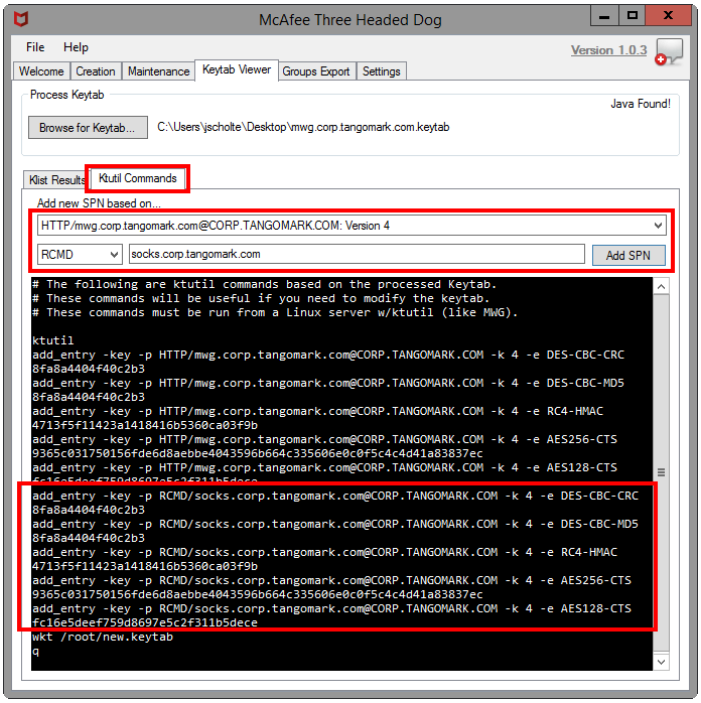
Keytab Viewer

If Java is installed on the workstation, THD will use the build in Keytab viewer tool (klist.exe) to display information about a given keytab. If Java is not installed, this option will not be available (sorry!).



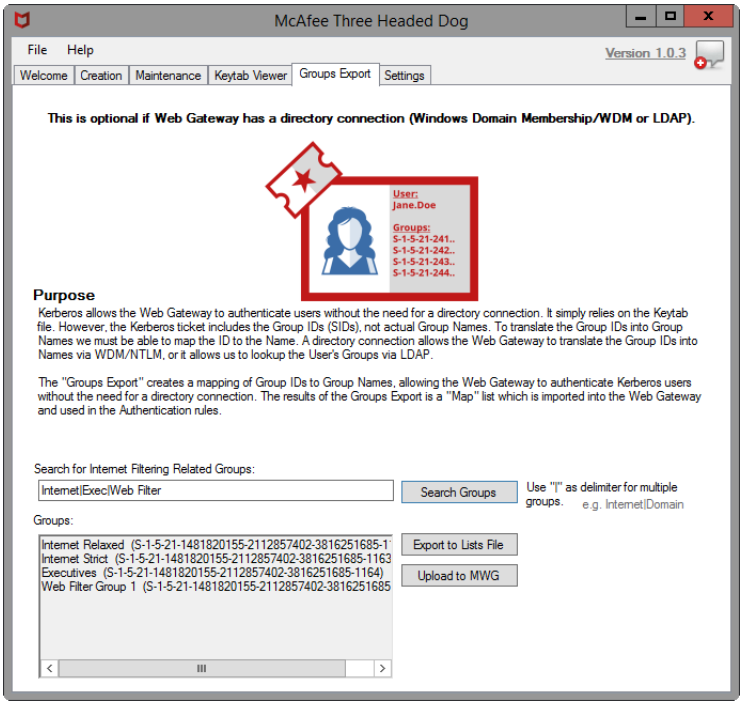
Ktutil Commands

Ktutil is a Linux package (installed on MWG by running -- `yum install krb5-workstation`) that allows you to create and modify keytab files. The Ktutil Commands tab will output the necessary commands to regenerate a given keytab from scratch. It reads the processed keytab and also allows you to add any SPNs to the keytab, should you need to (like for RCMD additions).



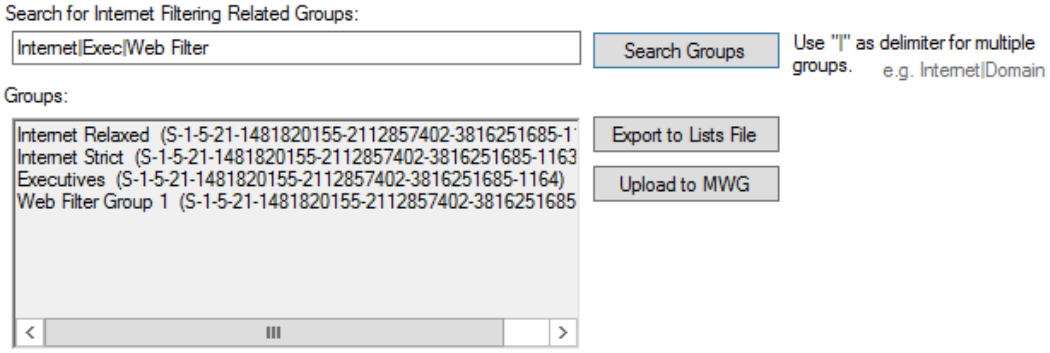
Groups Export

(Optional) Groups Export is a feature intended for deployments where the Web Gateway does not have a connection to directory resources. With Kerberos, the ticket presented by the workstation includes the Group IDs (not Group Names), so a directory connection is required to map or lookup the actual Group Names. With the Groups Export feature in THD, it can export a "Map" list of Group IDs to Group Names. This Map list can be used in the Web Gateway to substitute for a directory connection.



Searching for Groups

When searching for groups, you should search for groups which are used for Internet Filtering as some domains may include tens of thousands of groups. The search option in the Groups Export allows for pipe delimited searches (e.g. Internet|WebFilter|Executives).

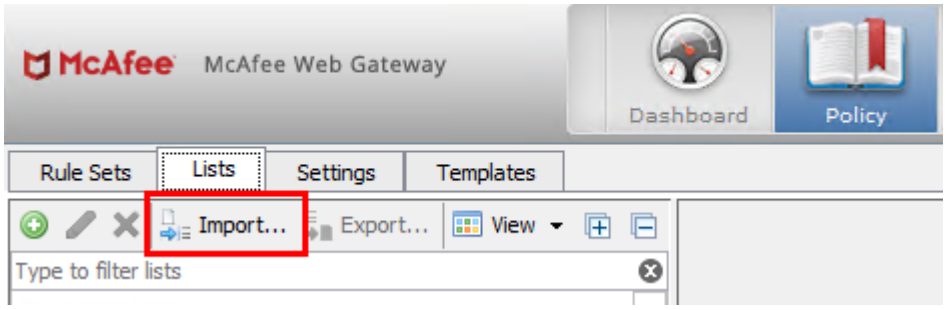


Exporting or Uploading to Web Gateway

To Export the Groups, there is two options 1) Export to .lists File, or 2) Upload directly to Web Gateway via the REST API.

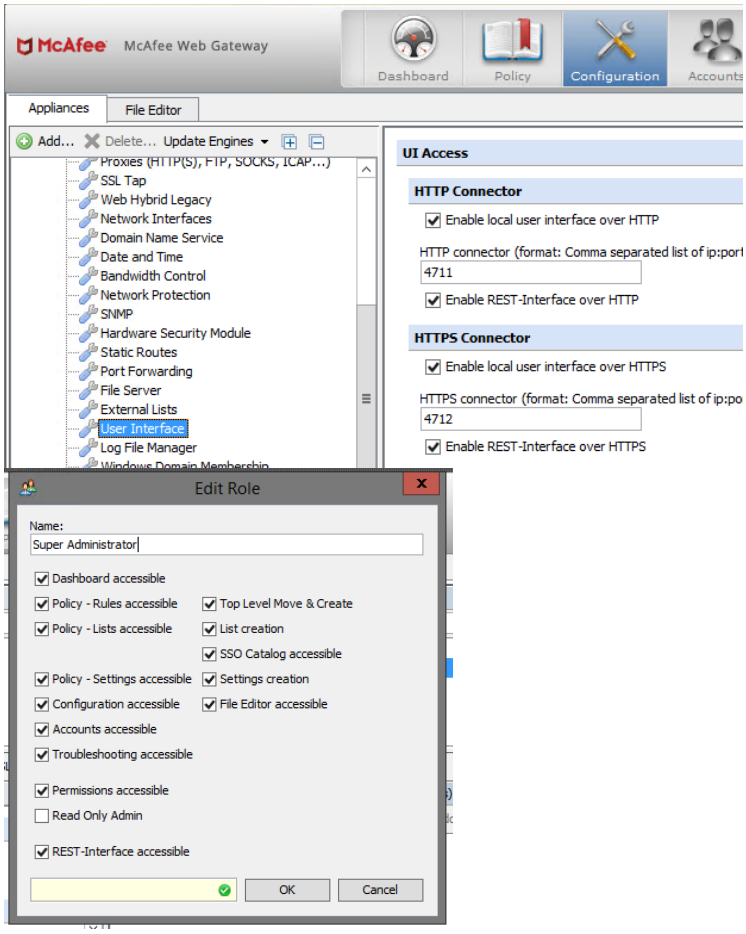
Importing the to .lists File

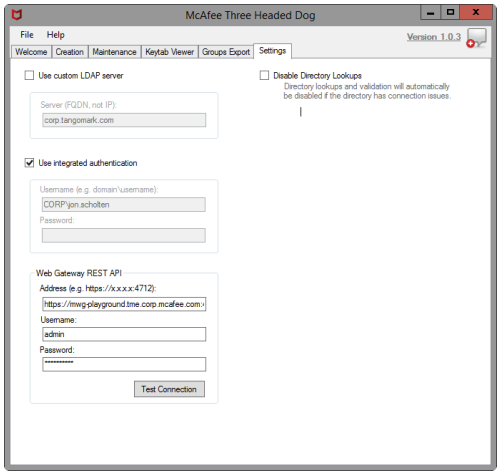
To Import the .lists file into Web Gateway, go to Policy > Lists, then click the Import... button.



Uploading via REST API

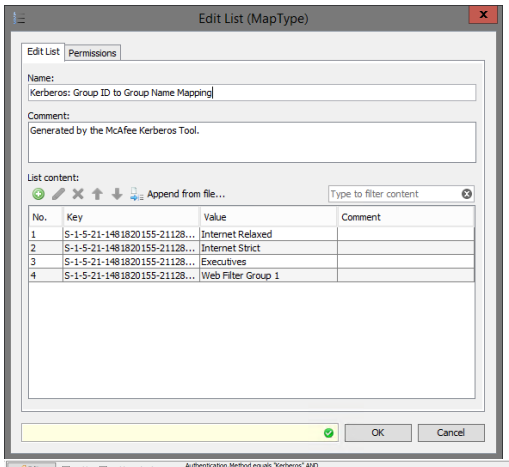
To Upload using the REST API, you must make sure that the REST interface is enabled on the Web Gateway and you must fill in your credentials in THD under Settings > Web Gateway REST API.

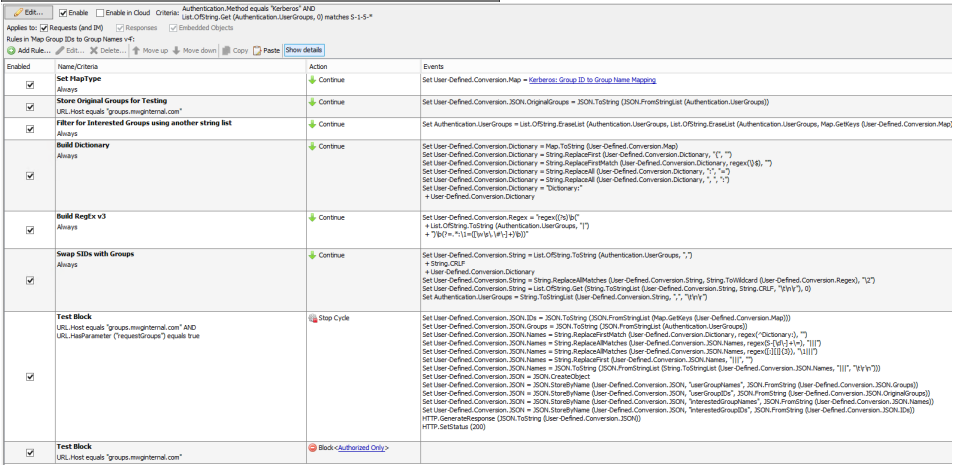


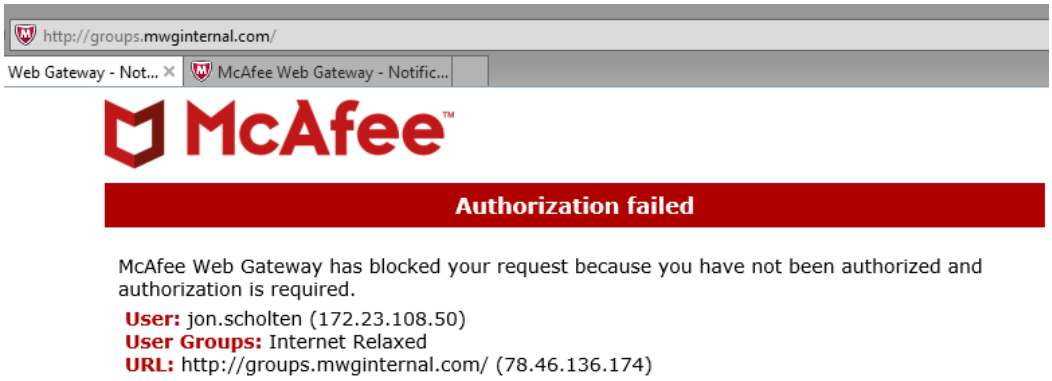


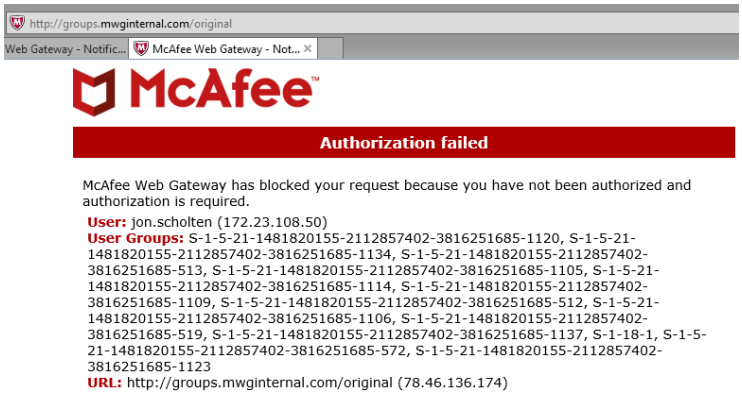
Using the Groups Export in the Rules

Once you have imported the Groups Export into the Web Gateway, we need rules that will actually use it. Attached are rules [Translate Group IDs to Name] which will accomplish this need. The rules will first filter out any Group IDs not in the Mapping list, then build a dictionary and regex based on the Group IDs and Group Names in the mapping list, and finally the Group IDs will be converted to Group Names. In the examples below, I (jon.scholten) am apart of the "Internet Relaxed" group. As such all Group IDs are filtered away and only the Group Name "Internet Relaxed" remains.







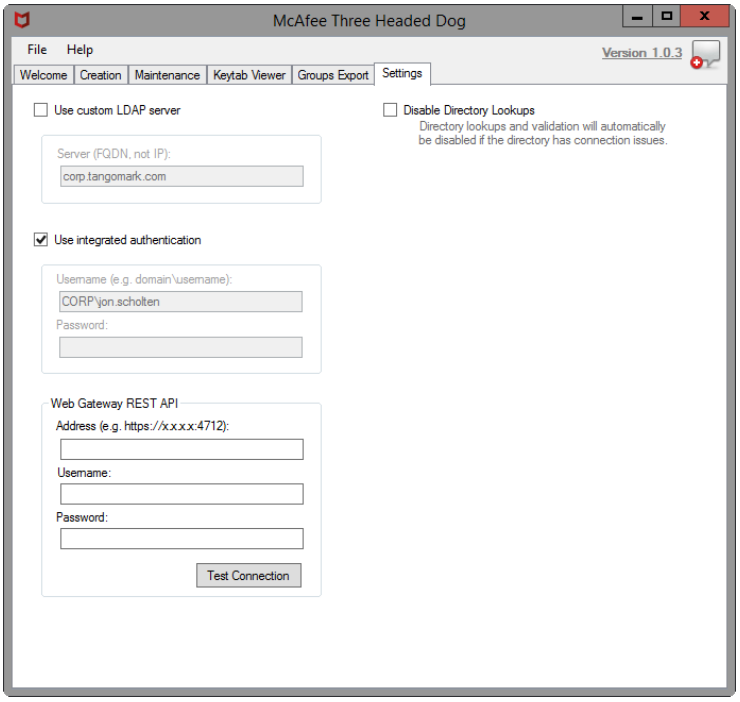


Settings

The settings in THD allow you to target a new domain and use different domain credentials. This is useful if you aren't logged into the domain you're generating the keytab for.

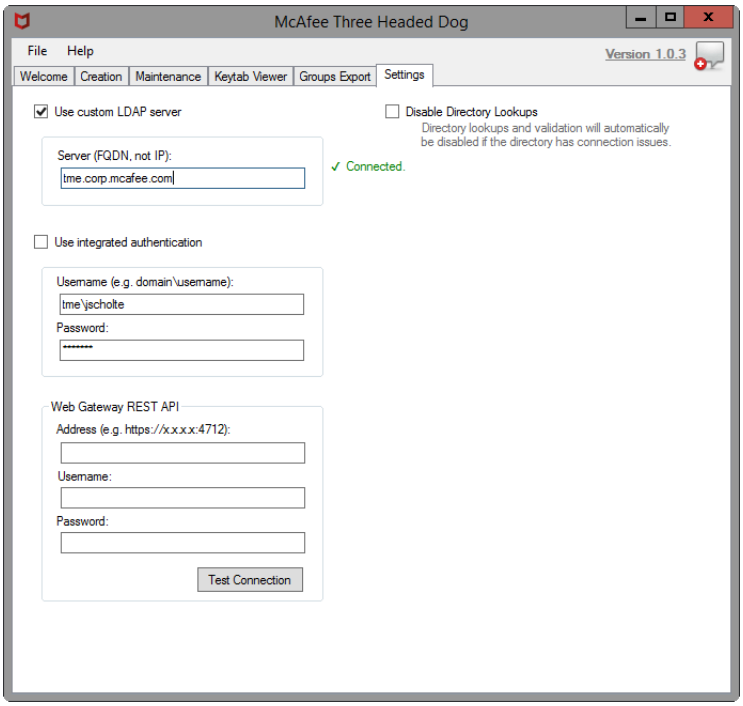
Default Settings

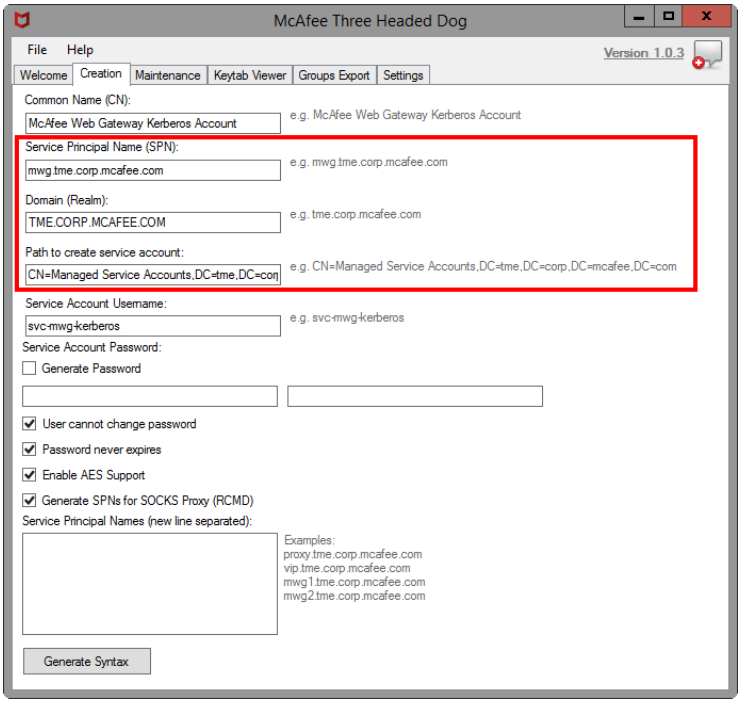
The directory settings will default to using the logged in workstation's domain and user.



Custom Settings

Custom settings can be used if you are attempting to setup Kerberos for a domain different from what your workstation is attached to. When a custom domain is specified, the "Creation" tab's inputs are updated to reflect the domain change.





Known Issues

This is my first C# project from scratch so there might be some exceptions here and there. If you find any that are show stoppers, please let me know. Overall most of the functionality should be pretty solid.

I'm interested in feedback for the Groups Export if this might be a useful feature or not.

Changelog

- 2017-12-11 - Rebranded some images
- 2017-09-12 - Fixed duplicate translation issue for HTTPS with Group IDs to Group Names Ruleset (new version v4)

Version History

Version 1.0.3: 09/05/2017

-First external release!

-Added Groups Export, for mapping Group IDs to Group Names

-Added support for upload of Groups Export to MWG via REST

Requires .NET Framework 4.5

NOTE: This tool is NOT supported by McAfee Technical Support in any way. Do not contact them for help with problems.

NOTE: This tool makes a call to "mcafee.tangomark.com", this domain is owned by the Technical Marketing Team and is used for version checks.

For assistance, questions, comments, improvements and problems with this program, please contact:

Labels : Web Gateway

authentication Add tags

kerberos mwgtools thd three headed dog web gateway

Attachments

ThreeHeadedDog.1.0.3-signed.zip

Map Group IDs to Group Names v4.zip

4 Kudos

Comment

Share

Comments

jebeling 01-08-2020 01:20 PM

With regard to using Kerberos IDs in rules matching against group names in a list, there is another way to accomplish the task without a complex ruleset that maps Authentication.UserGroups and has to apply against every transaction.

You can take an export of an existing group name list and use it as an input to a Powershell script running on a domain joined system with access to the Get-ADGroups cmdlet. The Powershell script will output a new list with the original groupname entries as well as entries for any matching SIDS.

The powershell uses the Get-ADGroups cmdlet of this form:

Get-ADGroup -Filter {Name -like "<group name>"} | Select SID

The Powershell script can be found here

The output can be either appended to, or replace the original list and then the list can be effectively used when using "none in list" or "at least one in list" with Authentication.UserGroups. These are the most commonly used operators with the Authentication.UserGroups property. If other operators will be used then likely you will need to use the maplist method described in the base article and actually convert the group ids to group names on each transaction. Note that when using this alternative method the Authentication.UserGroups property will always have the SIDs and they are never translated.

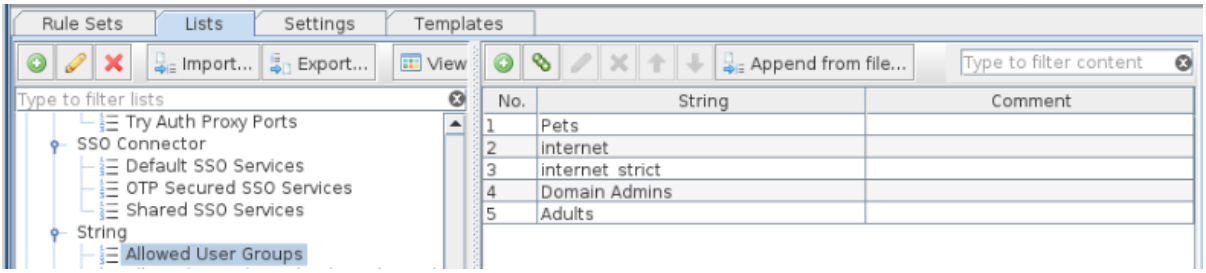
A bit about the sparsely commented script:

If SID lookup fails, no entry is added, but the original entry remains intact.

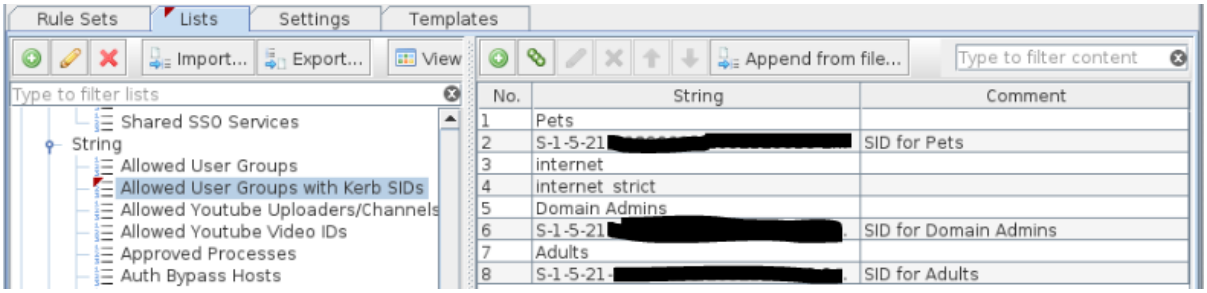
Existing SID entries will be removed and will only be restored if the common group name is still in the sourcelist.

Syntax: KerbGroupListAppend.ps1 -inputFile <inputfile> -outputFile <outputfile>

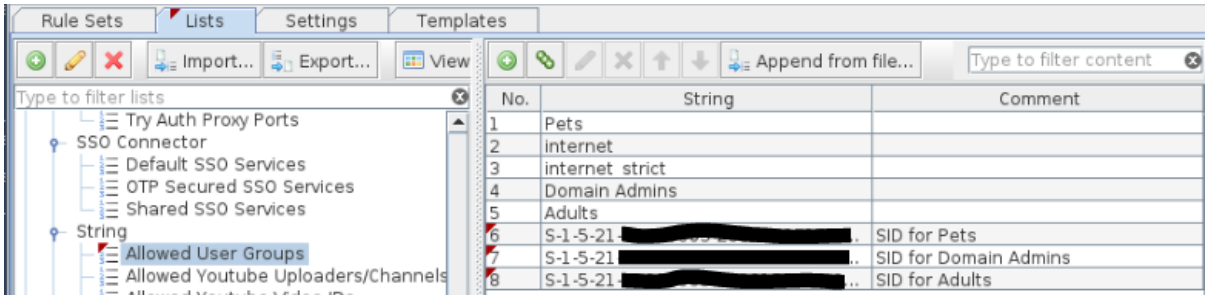
This list:



Gets converted to this list, if you import:



Gets converted to this list, if you append



Suggestions and modifications welcome as always.
