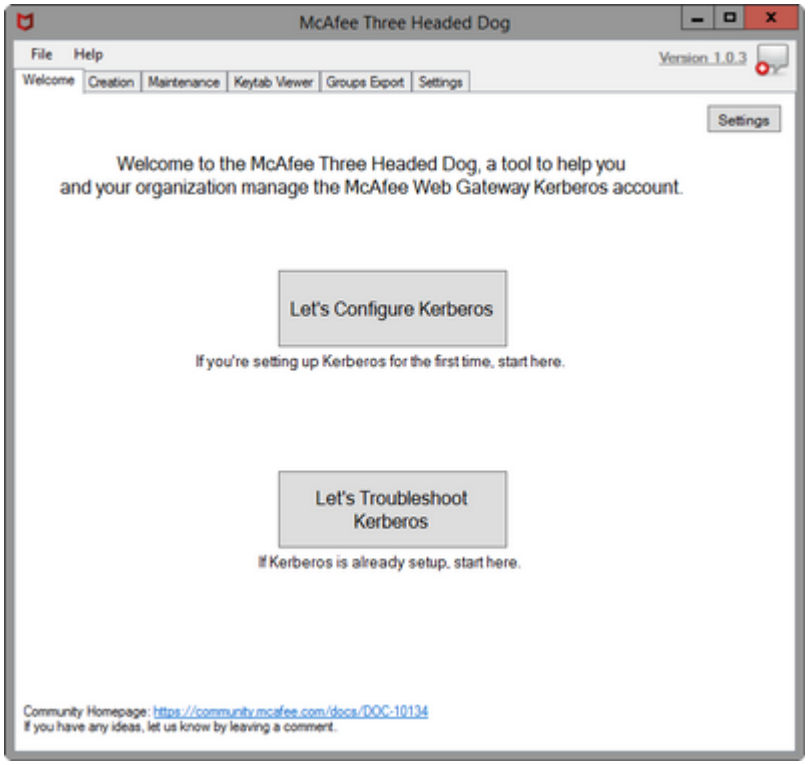
Introduction

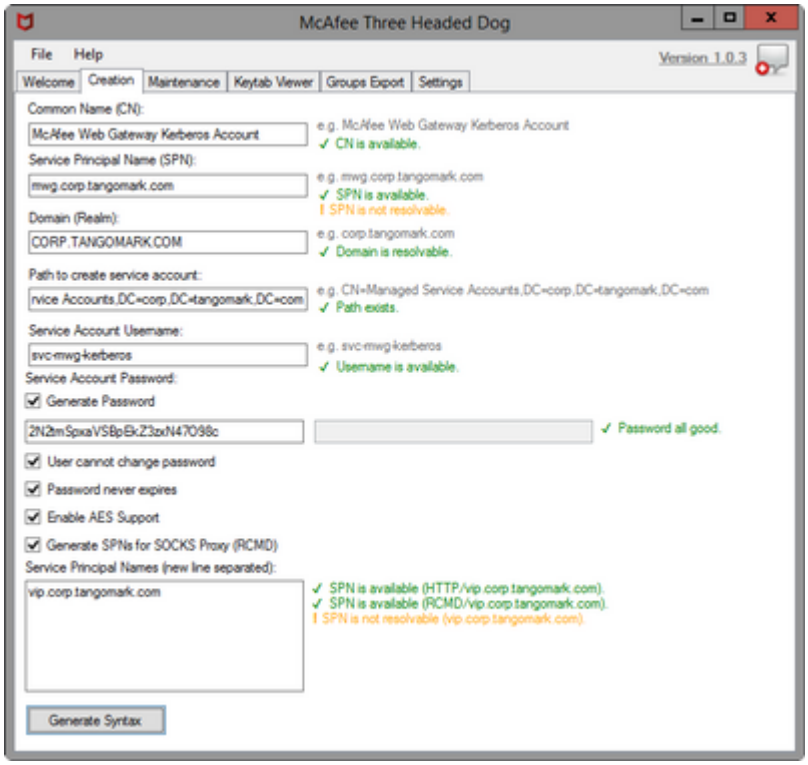
This guide is a trimmed down version of the Ultimate Kerberos Guide, it includes only the basics for setting up Kerberos. No background or historical information will be found here. My comments will also be short and sweet.

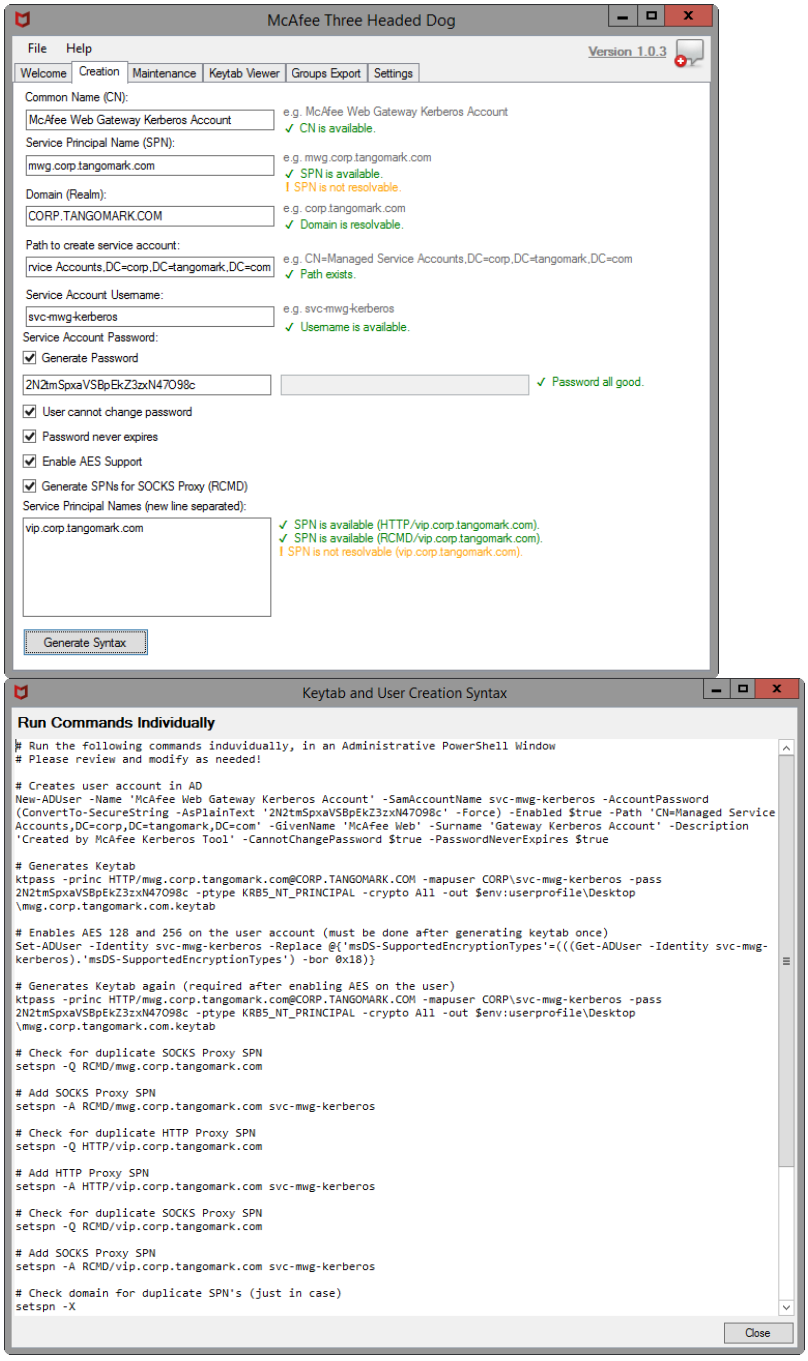
IMPORTANT: By the end of this guide you should only have one user and keytab per domain for all of your MWGs!

Use the Three-Headed Dog

A Kerberos setup tool has been created to make the setup process much easier -- it will provide you with the commands to give to your Active Directory team. You can find the tool here: Web Gateway: Three Headed Dog v1.0.3 (A Kerberos Setup Tool)

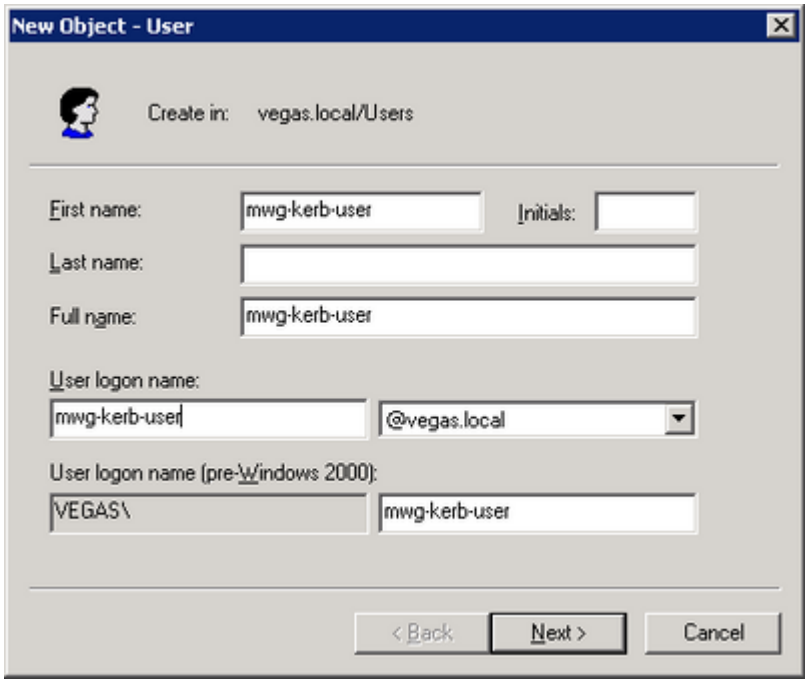

McAfee Three Headed Dog
File
Help
Version 1.0.3
Welcome
Creation
Maintenance
Keytab Viewer
Groups Export
Settings
Settings
Welcome to the McAfee Three Headed Dog, a tool to help you
and your organization manage the McAfee Web Gateway Kerberos account.
Let's Configure Kerberos
If you're setting up Kerberos for the first time, start here.
Let's Troubleshoot Kerberos
If Kerberos is already setup, start here.
Community Homepage: https://community.mcafee.com/docs/DOC-10134
If you have any ideas, let us know by leaving a comment.

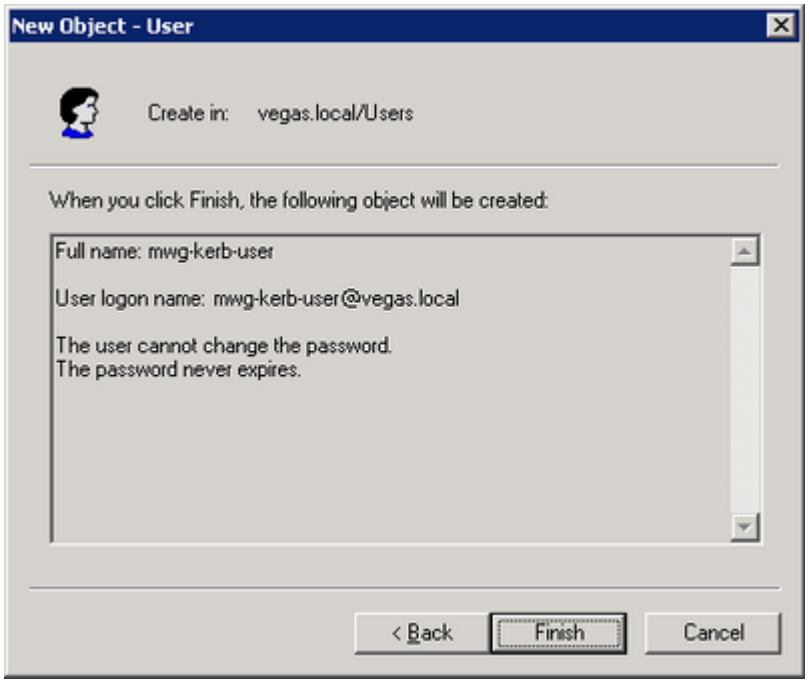

McAfee Three Headed Dog
File
Help
Version 1.0.3
Welcome
Creation
Maintenance
Keytab Viewer
Groups Export
Settings
Common Name (CN):
McAfee Web Gateway Kerberos Account
e.g. McAfee Web Gateway Kerberos Account
✓ CN is available.
Service Principal Name (SPN):
mwg.corp.tangomark.com
e.g. mwg.corp.tangomark.com
✓ SPN is available.
! SPN is not resolvable.
Domain (Realm):
CORP.TANGOMARK.COM
e.g. corp.tangomark.com
✓ Domain is resolvable.
Path to create service account:
rvice Accounts,DC=corp,DC=tangomark,DC=com
e.g. CN=Managed Service Accounts,DC=corp,DC=tangomark,DC=com
✓ Path exists.
Service Account Username:
svc-mwg-kerberos
e.g. svc-mwg-kerberos
✓ Username is available.
Service Account Password:
Generate Password
2N2tmSpxaVSBpEkZ3zxN47O98c
✓ Password all good.
User cannot change password
Password never expires
Enable AES Support
Generate SPNs for SOCKS Proxy (RCMD)
Service Principal Names (new line separated):
vip.corp.tangomark.com
✓ SPN is available (HTTP/vip.corp.tangomark.com).
✓ SPN is available (RCMD/vip.corp.tangomark.com).
! SPN is not resolvable (vip.corp.tangomark.com).
Generate Syntax



Create User in Active Directory

You know how to do this, this account will be treated as a service account so adjust accordingly.





Generate Keytab in Active Directory

When generating the keytab, syntax is essential! The commands are case sensitive. Syntax below is for Windows Server 2008+, start a command prompt as administrator.

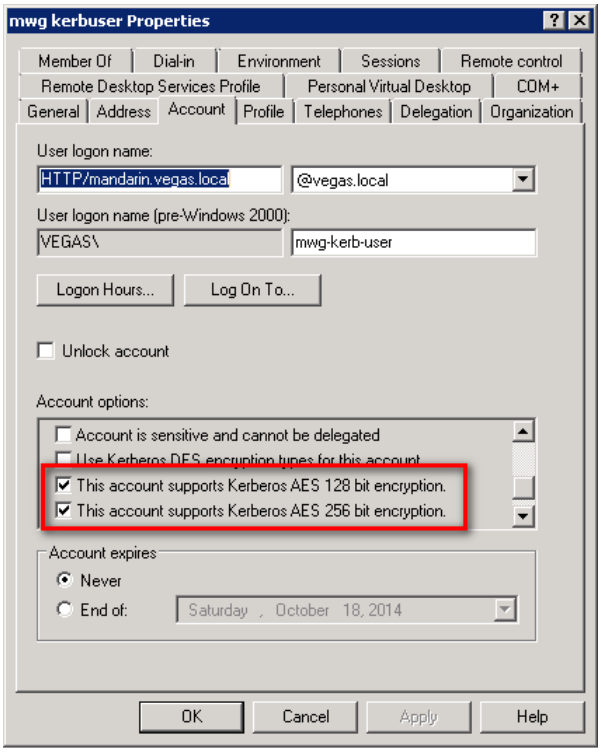
ktpass -princ HTTP/[fqdn-of-appliance_lowercase]@[DOMAIN_UPPERCASE] -mapuser [DOMAIN]\[USERNAME] -pass [PASSWORD] -ptype KRB5_NT_PRINCIPAL -crypto All -out [OUTPUT-FILENAME].keytab

Example:

ktpass -princ HTTP/proxy.domain.local@DOMAIN.LOCAL -mapuser vegas\mwg-kerb-user -pass password -ptype KRB5_NT_PRINCIPAL -crypto All -out proxy.domain.local.keytab

Enable AES support in Active Directory (optional)

If you wish to enable AES support, do it *after* generating a keytab. If you adjust the AES support **generate the keytab again**. In my testing if I enabled AES support before generating a keytab, authentication would fail; only deleting the account and starting again would get it to work.



Set additional SPNs in Active Directory

Additional SPNs are necessary if you have multiple MWGs, they are behind a load balancer, or there are multiple DNS names.

setspn -a HTTP/[fqdn-of-appliance] mwg-kerb-user

Example:

setspn -a HTTP/load-balancer.domain.local mwg-kerb-user

setspn -a HTTP/mwg-alias.domain.local mwg-kerb-user

SOCKS Example:

setspn -a RCMD/proxy.domain.local mwg-kerb-user

setspn -a RCMD/load-balancer.domain.local mwg-kerb-user

setspn -a RCMD/mwg-alias.domain.local mwg-kerb-user

Upload keytab into the Web Gateway

Configuration > [Select your appliance] > Kerberos Administration. Upload the **single** keytab to each appliance.

Import Authentication Rules into Web Gateway

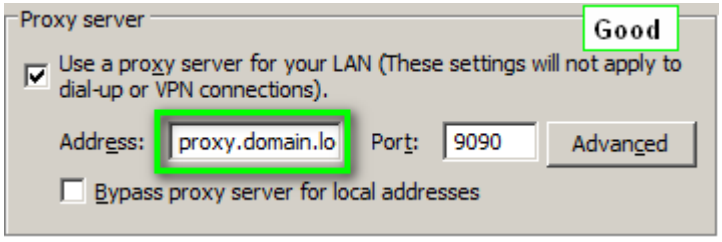
Use the ruleset from the Ultimate Kerberos Guide. Download ruleset here. Screenshot below shows Direct Proxy Authentication rules with NTLM Fallback, rules would be different for Authentication Server. We also assume you have already joined the MWG to the domain () for getting groups.

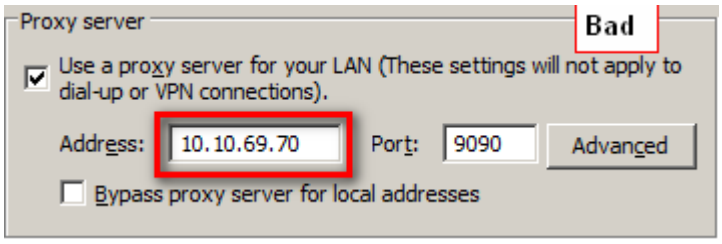
Enabled	Name/Criteria	Action	Events
☑	**Authenticate With NTLM** Authentication.Authenticate<NTLM> equals false	Continue	
☑	**Authenticate With Kerberos (don't evaluate NTLM tokens)** Authentication.RawCredentials does not match Negotiate TlRM* AND Authentication.IsAuthenticated equals false AND Authentication.Authenticate<Kerberos> equals false	Continue	
☑	**Reject All Negotiate with NTLM tokens** Authentication.RawCredentials matches Negotiate TlRM*	Continue	Authentication.ClearMethodList Authentication.AddMethod ("NTLM", "", true)
☑	**Perform Authentication** Authentication.IsAuthenticated equals false	Authenticate<Default>	

Common Issues

Proxy Settings

You must have the proxy settings set to use the FQDN (used in the keytab creation process). Do not use the IP.





Duplicate SPN

You probably created multiple user accounts after generating keytabs and forgot to delete them. To check for it run the command below on the Active Directory server. Replace "**SPN-SEARCH-STRING**" with the actual search string (e.g. **proxy.domain.local**)...

```
ldifde -f c:\dump.txt -l dn,sAMAccountName,msds-keyversionnumber,serviceprincipalname,userprincipalname -p subtree -r "(serviceprincipalname=*SPN-SEARCH-STRING*)"
```

User account / keytab version mismatch

You probably re-created the keytab or updated the account password, and now the versions are off.

Run the ldifde command again:

```
ldifde -f c:\dump.txt -l dn,sAMAccountName,msds-keyversionnumber,serviceprincipalname,userprincipalname -p subtree -r "(serviceprincipalname=*SPN-SEARCH-STRING*)"
```

Example output (showing version 6):

```
> ldifde -f c:\dump.txt -l dn,sAMAccountName,msds-keyversionnumber,serviceprincipalname,userprincipalname -p subtree -r "(serviceprincipalname=*proxy.domain.local*)"
```

c:\dump.txt:

dn: CN=mwg-kerb-user,CN=Users,DC=domain,DC=local

changetype: add

sAMAccountName: mwg-kerb-user

userPrincipalName: HTTP/proxy.domain.local@domain.local

servicePrincipalName: HTTP/proxy.domain.local

servicePrincipalName: HTTP/mwg-alias.domain.local

msDS-KeyVersionNumber: 6

Compare the version listed in the ldifde output with the version in the keytab:

yum install krb5-workstation

klist -tek /etc/krb5.mwg.keytab

Example output (showing version 5):

[root@proxy ~]# klist -tek /etc/krb5.mwg.keytab

Keytab name: FILE:/etc/krb5.mwg.keytab

KVNO Timestamp Principal

---- ----------------- --

5 12/31/69 18:00:00 HTTP/proxy.domain.local@DOMAIN.LOCAL (des-cbc-crc)

5 12/31/69 18:00:00 HTTP/proxy.domain.local@DOMAIN.LOCAL (des-cbc-md5)

5 12/31/69 18:00:00 HTTP/proxy.domain.local@DOMAIN.LOCAL (arcfour-hmac)

5 12/31/69 18:00:00 HTTP/proxy.domain.local@DOMAIN.LOCAL (aes256-cts-hmac-sha1-96)

5 12/31/69 18:00:00 HTTP/proxy.domain.local@DOMAIN.LOCAL (aes128-cts-hmac-sha1-96)

[root@proxy ~]#

Troubleshooting

If you have problems gather the following... (if you don't then we can't pinpoint your issue)

- Flush DNS and purge Kerberos tickets:

ipconfig /flushdns

klist purge

- Screenshot of proxy settings (if applicable)
- **ldifde** output from Active directory server
- **klist** output from MWG
- Client side Wireshark capture while reproducing whatever problem you are having.

Conclusion

By the end of all of this you should have one user and one keytab created (per domain) for all of your MWGs. Authentication rules should be imported into MWG with NTLM Fallback in place.

Labels : Web Gateway

authentication Add tags

kerberos negotiate simplified

3 Kudos

Comment

Share

Comments

jscholte 03-11-2015 10:32 AM

For anyone reading this, if you are planning on enabling AES128|256 encryption on the account, do it after the keytab is generated. In limited testing I can't seem to get the account functioning if encryption was enabled prior to generating the keytab. This means you will need to generate the keytab twice. Will update with more details when I'm able to isolate the problem further.

jscholte 03-20-2015 09:29 AM

I adjusted the order, moving enabling AES support after generating the keytab.

Related note, please make sure your DC is patched up when using Kerberos!

eelsasser 02-12-2016 09:02 AM

Note that when you doing ktpass on the windows command line, Run As administrator. Even if you are a Domain Admin, the command prompt needs elevated.

renata.petrasov 08-29-2016 02:14 AM

Hi, so generate keytabfile without aes support enabled and then enable aes support and generate another keytabfile? did I get this right?

jscholte 08-29-2016 06:50 AM

That is correct.

From my tests, when I enabled AES **before** generating the keytab nothing would work, I was not able to find a reason why.

renata.petrasov 08-29-2016 02:56 PM

worked, thanks!!