FRSECURE®

KRBTGT RESET

Guidance & Considerations

FRSecure Resource

About FRSecure

> https://frsecure.com/
>
> FRSecure is a mission-driven information security consultancy headquartered in Minneapolis, MN. Our team of experts is constantly developing solutions and training to assist clients in improving the measurable fundamentals of their information security programs.
>
> These fundamentals are lacking in our industry, and while progress is being made, we can't do it alone. Whether you're wondering where to start, or looking for a team of experts to collaborate with you, we are ready to serve.

Introduction

The KRBTGT account is a default account within Active Directory. This covered process of resetting the password is applicable to Windows Server 2008 Domain Functional Level (DFL) and higher. If you are still running Windows Server 2003 DFL or lower, it is very highly recommended raising your DFL to modern and supported levels.

At the most basic level, the KRBTGT account has a random password assigned to it, known only by Active Directory. This account is used to validate Kerberos ticket requests, and an approved request has its authentication ticket sent back encrypted and signed with the KRBTGT account. The encryption is done using the KRBTGT's password, and is signed with a hash of the same password. By acquiring the hash of this account's password, attackers are able to manufacture artificial authentication tickets, bearing proper encryption and signature, without ever having been actually received and approved the Kerberos system. Because this account is trusted, the artificial authentication ticket is accepted as legitimate by any other system within the domain. This is what gets called a Golden Ticket.

The password for the KRBTGT account does not ever change automatically. Resetting the KRBTGT password is not only a vital consideration in response to ongoing malicious or suspicious activity, but also a practice that should be incorporated into a regular maintenance schedule.

Reset KRGTBT Password with Microsoft Powershell Script

> Microsoft has previously provided a powershell script to assist with resetting the KRBTGT account password. That script was updated and previously available from Microsoft TechNet Gallery. With the closure of the TechNet Gallery (information available here) the script has been maintained and updated by its author on his GitHub, and is available here:
>
> Written by: Jorge de Almeida Pinto
>
> Microsoft Powershell Script

Methods

When resetting the KRBTGT account's password, there are two potential methods, each with its place and use.

> 1. **Maintenance:** Changing the KRBTGT account password once, waiting for replication to complete, and then changing the password a second time. This is the only method FRSecure suggests.
>
> 2. **Emergency Breach Recovery:** Changing the KRBTGT account password twice in rapid succession, before AD replication completes. This will invalidate all existing TGTs, forcing clients to re-authenticate. This will require rebooting application servers, or at least re-starting application services to get them talking Kerberos correctly again. This also runs the risk of DirSync issues between multiple DCs.
>
> **FRSecure does NOT recommend this method under any circumstance due to the high risk of additional damage, recovery time, and likelihood of the loss of forensic evidence due to systems needing to be rebooted to get authentication working again.**

FRSecure only recommends the first—Maintenance—method of resetting the KRBTGT account's password.

KRBTGT Password

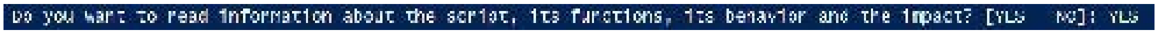
Using the Microsoft KRBTGT Password Reset Script

The KRBTGT reset script sees continued development and updates, it is advised to ensure you have the most up-to-date version prior to execution.

Some notes about running this script:

> 1. To execute this script, the account running the script MUST be a member of the “Domain Admins” or Administrators group in the targeted AD domain.
>
> 2. If the account used is from another AD domain in the same AD forest, then the account running the script MUST be a member of the “Enterprise Admins” group in the AD forest or Administrators group in the targeted AD domain. For all AD domains in the same AD forest, membership of the “Enterprise Admins” group is easier as by default it is a member of the Administrators group in every AD domain in the AD forest
>
> 3. If the account used is from another AD domain in another AD forest, then the account running the script MUST be a member of the “Administrators” group in the targeted AD domain. This also applies to any other target AD domain in that same AD forest
>
> 4. This is due to the reset of the password for the targeted KrbTgt account(s) and forcing (single object) replication between DCs
>
> 5. Testing “Domain Admins” membership is done through “IsInRole” method as the group is domain specific
>
> 6. Testing “Enterprise Admins” membership is done through “IsInRole” method as the group is forest specific
>
> 7. Testing “Administrators” membership cannot be done through “IsInRole” method as the group exist in every AD domain with the same SID. To still test for required permissions in that case, the value of the Description attribute of the KRBTGT account is copied into the Title attribute and cleared afterwards. If both those actions succeed it is proven the required permissions are in place!

The script is very verbose, and it is recommended that you take time and review the information included within the script by responding 'YES' to the first prompt.

> Example of prompt:
>
> 
>
> ```
> Do you want to read information about the script, its functions, its behavior and the impact? [YES   NO]: YES
> ```

This will output detailed blurbs about the script and its numerous execution modes for gathering information, testing, and executing the reset of the KRBTGT account within various domain configurations.

> The color of the mode's description references the impact it will have on your domain:

Color	Domain Implication	Example Actions
Green	None	Informational, creation and removal of test accounts
Yellow	Minimal	Simulated changes
Red	High	Change to production accounts

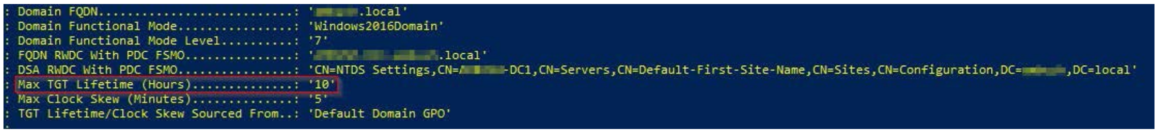
The recommended order of execution is as follows:

> • Mode 1 - Informational Mode (No Changes At All) [Note the Max TGT Lifetime value]
>
> • Mode 8 - Create TEST KrbTgt Accounts
>
> • Mode 2 - Simulation Mode (Temporary Canary Object Created)
>
> • Mode 3 - Simulation Mode - Uses KrbTgt TEST Accounts (No Password Reset)
>
> • Mode 4 - Real Reset Mode - Uses KrbTgt TEST Accounts (Password Will Be Reset Once)
>
> • Mode 5 - Simulation Mode - Uses KrbTgt PRODUCTION Accounts (No Password Reset)

> - Mode 6 - Real Reset Mode - Uses KrbTgt PRODUCTION Accounts (Password Will Be Reset Once)
> - Wait ≥ Max TGT Lifetime. (Value determined in Mode 1, default 10 hours)
>
> - Mode 5 - Simulation Mode - Uses KrbTgt PRODUCTION Accounts (No Password Reset)
>
> - Mode 6 - Real Reset Mode - Uses KrbTgt PRODUCTION Accounts (Password Will Be Reset Once)
>
> - Mode 9 - Cleanup TEST KrbTgt Accounts

When running Mode 1, it will perform a number of checks and gather information about the domain. One piece to pay particular attention to is the Max TGT Lifetime:

Example of Max TGT Lifetime



```
: Domain FQDN..........................: '[redacted].local'
: Domain Functional Mode...............: 'Windows2016Domain'
: Domain Functional Mode Level.........: '7'
: FQDN RWDC With PDC FSMO..............: '[redacted].local'
: DSA RWDC With PDC FSMO...............: 'CN=NTDS Settings,CN=[redacted]-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=[redacted],DC=local'
: Max TGT Lifetime (Hours).............: '10'
: Max Clock Skew (Minutes).............: '5'
: TGT Lifetime/Clock Skew Sourced From..: 'Default Domain GPO'
:
```

The default is 10 hours, but you should reference the time you see in the “Max TGT Lifetime (Hours)” entry that displays for your domain. This is how long you need to wait between KRBTGT password resets.

Learn More

> For more information, check out our blog and resources pages for timely updates and security support.
>
> [Blog]
>
> [Resources]