

Run this:

```
$ListOWKO = Get-ADObject (Get-ADRootDSE).DefaultNamingContext -Properties  
otherwellKnownObjects
```

```
$ListOWKO.otherwellKnownObjects
```

## MAKE A SNAPSHOT BEFORE TRYING THESE STEPS

If the output looks like below

Example “In-state”

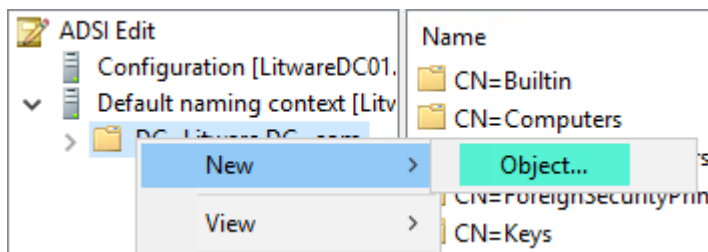
```
objectSid: S-1-5-21-2612367947-598062595-3909775797;  
otherWellKnownObjects (2): B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;  
B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service Accounts  
0ADEL:c5f8d480-7453-414b-97a6-df74d4916253,CN=Deleted Objects,DC=Litware,DC=com;  
pwdHistoryLength: 24;
```

Previous complex steps:

### Step 1: Create the new MSA container

1. Use ADSIEdit to create a new “Managed Service Accounts” container

- R-click on the domain > **New > Object**



- Select the “**Container**” object class and click **Next**

Create Object ✕

Select a class:

- builtinDomain
- classStore
- computer
- contact
- container**
- country
- device
- dfsConfiguration
- domainDNS
- domainPolicy
- friendlyCountry
- group
- groupOfInquireNames

< Back   **Next >**   Cancel   Help

- Enter the Common-Name value = **Managed Service Accounts** and click **Next**

Create Object ✕

Attribute: cn

Syntax: Unicode String

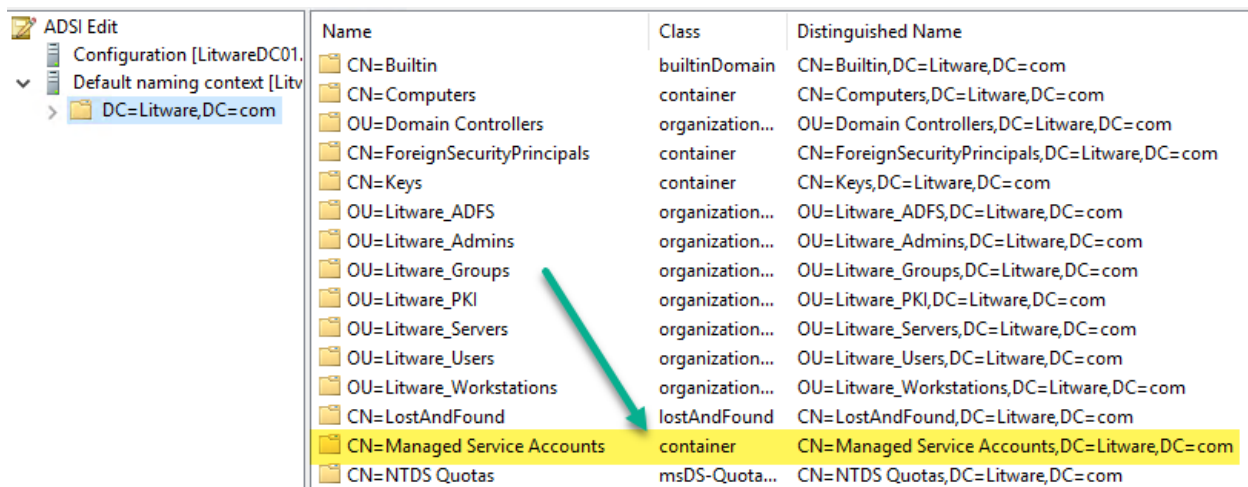
Description: Common-Name

Value: **Managed Service Accounts**

< Back   **Next >**   Cancel   Help

- Click **Finish** on the next pane to complete object creation

Confirm: You should see similar to the following in ADSIEDIT




Name	Class	Distinguished Name
CN=Builtin	builtinDomain	CN=Builtin,DC=Litware,DC=com
CN=Computers	container	CN=Computers,DC=Litware,DC=com
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=Litware,DC=com
CN=ForeignSecurityPrincipals	container	CN=ForeignSecurityPrincipals,DC=Litware,DC=com
CN=Keys	container	CN=Keys,DC=Litware,DC=com
OU=Litware_ADFS	organization...	OU=Litware_ADFS,DC=Litware,DC=com
OU=Litware_Admins	organization...	OU=Litware_Admins,DC=Litware,DC=com
OU=Litware_Groups	organization...	OU=Litware_Groups,DC=Litware,DC=com
OU=Litware_PKI	organization...	OU=Litware_PKI,DC=Litware,DC=com
OU=Litware_Servers	organization...	OU=Litware_Servers,DC=Litware,DC=com
OU=Litware_Users	organization...	OU=Litware_Users,DC=Litware,DC=com
OU=Litware_Workstations	organization...	OU=Litware_Workstations,DC=Litware,DC=com
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=Litware,DC=com
CN=Managed Service Accounts	container	CN=Managed Service Accounts,DC=Litware,DC=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=Litware,DC=com

## Step 2: Modify schemaUpgradeInProgress attribute

**Note:** You must be using an account with Schema Admin rights for these steps

1. On a domain controller, run LDP.exe
  - a. Right click > **Run as Administrator**
2. Click Connection > Connect... > enter the following values and click OK:
  - a. Server: localhost
  - b. Port: 389
  - c. No boxes checked
3. LDP will say “Established connection to localhost” towards the top and output a lot of text
4. Click Connection > Bind... > enter the following values and click OK
  - a. User, Password, Domain: all blank
  - b. Select “Bind as currently logged on user” radio button
  - c. Everything else default
5. The output window will return “Authenticated as: ‘DOMAIN\username’” if successful
6. Click Browse > Modify
7. In the Modify window, perform the following
  - a. Leave the “DN:” field blank
  - b. Attribute: schemaUpgradeInProgress

- c. Values: 1
- d. Operation: Add
- e. Click Enter
- f. The Entry list will populate: “[Add]schemaUpgradeInProgress:1”
- g. Leave everything else default
- h. Click Run
- i. Example:



```
currentTime: 4/6/2018 4:04:08 PM Eastern Daylight Time;
defaultNamingContext: DC=fabrikam,DC=com;
dnsHostName: FABRIKAMD01.fabrikam.com;
domainControllerFunctionality: 6 = ( WIN2012R2 );
domainFunctionality: 6 = ( WIN2012R2 );
dsServiceName: CN=NTDS Settings,CN=FABRIKAMD01,CN=Servers,CN=Default-First
forestFunctionality: 6 = ( WIN2012R2 );
highestCommittedUSN: 1665381;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
ldapServiceName: fabrikam.com:fabrikamdc01$@FABRIKAM.COM;
namingContexts (5): DC=fabrikam,DC=com; CN=Configuration,DC=fabrikam,DC=com; C
DC=ForestDnsZones,DC=fabrikam,DC=com;
rootDomainNamingContext: DC=fabrikam,DC=com;
schemaNamingContext: CN=Schema,CN=Configuration,DC=fabrikam,DC=com;
serverName: CN=FABRIKAMD01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,(
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=fabrikam,DC=
supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.
ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIREC
( ACTIVE_DIRECTORY_WB );
supportedControl (37): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556
NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1
EXTENDED_DN ); 1.2.840.113556.1.4.805 = ( TREE_DELETE ); 1.2.840.113556.1.4.
1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_S
SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.84
1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTRI
); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4
1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_REC
POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX ); 1.2.
1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = ( EXPE
1.2.840.113556.1.4.2256;
supportedLDAPPolicies (19): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDate
MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSe
MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
(NtAuthIdentity: User=NULL; Pwd=<unavailable>; domain = 'NULL')
Authenticated as: 'FABRIKAM\kyleweis'.
-----
***Call Modify...
ldap_modify_s(ld, '(null)',[1] attrs);
Modified "".
```

8. Verify output in the LDP window:

\*\*\*Call Modify...

ldap\_modify\_s(ld, '(null)',[1] attrs);

Modified "".

**Step 3: Collect current value(s) of ‘otherWellKnownObjects’ attribute:**

- Open Notepad

- In the LDP.EXE right-hand pane, copy the contents of the 'otherWellKnownObjects' attribute into Notepad.

o In my example there are two entries:

B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts\0ADEL:c5f8d480-7453-414b-97a6-df74d4916253,CN=Deleted  
Objects,DC=Litware,DC=com;

#### **Step 4: Correct the "Managed Service Accounts" value for Step 5**

- Make the following adjustments to correct the DN of the Managed Service Accounts container

o Remove the \0ADEL:c5f8d480-7453-414b-97a6-df74d4916253,CN=Deleted Objects

- The correct value should look similar to:

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=Litware,DC=com;

- You will need both values below in Step 5

B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=Litware,DC=com;

#### **Step 5: Modify otherWellKnownObjects attribute from LDP.exe**

1. Click View > Tree > Enter DN of domain partition > Click OK

2. Right click the domain partition on the left and click Modify

3. In the Modify window, use the following values

a. DN: <domain partition DN>

b. Attribute: otherWellKnownObjects

c. Values:

B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=Litware,DC=com;

Step 5a: Add Managed Service Accounts object (this is a " Replace " action):

a. Replace domain with DN of your domain

b. Attribute: **otherWellKnownObjects**

c. Values: (below)

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=Litware,DC=com;

a. Operation: Replace

b. Click Enter

c. Verify the Entry List, as shown below

d. Click Run

Example:

Modify

DN: DC=Litware,DC=com

Edit Entry

Attribute: otherWellKnownObjects

Values: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service Accounts,DC=Litware,DC=com;

Operation

☐ Add ☐ Delete ☒ Replace

Entry List

[Replace]otherWellKnownObjects:B:32:1EB93889E40C

☒ Synchronous

☐ Extended

4. Verify output in the LDP window:

-----

\*\*\*Call Modify...

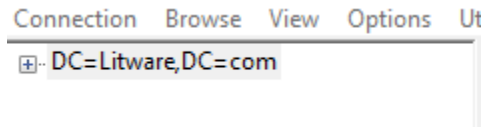
ldap\_modify\_s(ld, 'DC=Litware,DC=com',[2] attrs);

Modified "DC=Litware,DC=com".

-----

5. In ADSIEdit, the otherWellKnownObjects attribute on the domain partition should look similar to:

**NOTE :** You will need to double-click on the domain name in the left-hand pane to refresh the attribute list



Current otherWellKnownObjects attribute value:

```
objectGUID: b41a50fa-2dcd-467a-8d97-53b53e963f32;  
objectSid: S-1-5-21-2612367947-598062595-3909775797;  
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service Accounts,DC=Litware,DC=com;  
pwdHistoryLength: 24;  
pwdProperties: 0x1 = ( COMPLEX );
```

- We now need to add the other value back in as well

o If you had multiple values, please repeat ‘adding’ these values as single operations.

B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;

Step 5b: Add Keys object (this is an “ ADD ” action):

d. Replace domain with DN of your domain

e. Attribute: **otherWellKnownObjects**

f. Values: (below)

B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=Litware,DC=com;

a. Operation: Add

b. Click Enter

c. Verify the Entry List, as shown below

d. Click Run

Example:

Modify

DN: DC=Litware,DC=com

Edit Entry

Attribute: otherWellKnownObjects

Values: C2CF3F981:CN=Keys,DC=Litware,DC=com;

Operation

☒ Add ☐ Delete ☐ Replace

Insert file Enter

Entry List

[Add]otherWellKnownObjects:B:32:683A24E2E8164BD

Edit Remove

☒ Synchronous ☐ Extended

Close Run

5. Verify output in the LDP window:

-----

\*\*\*Call Modify...

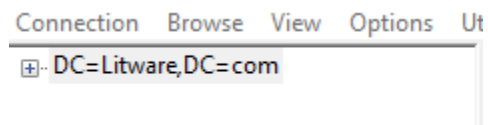
```
ldap_modify_s(ld, 'DC=Litware,DC=com',[1] attrs);
```

Modified "DC=Litware,DC=com".

-----

6. In ADSIEdit, the otherWellKnownObjects attribute on the domain partition should look similar to:

**NOTE** : You will need to double-click on the domain name in the left-hand pane to refresh the attribute list



Current otherWellKnownObjects attribute value:



```
objectGUID: b41a50fa-2dcd-467a-8d97-53b53e963f32;  
objectSid: S-1-5-21-2612367947-598062595-3909775797;  
otherWellKnownObjects (2): B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=Litware,DC=com;  
B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service Accounts,DC=Litware,DC=com;  
pwdHistoryLength: 24;  
pwdProperties: 0x1 = ( COMPLEX );
```

Step 6: Reset schemaUpgradeInProgress attribute and test

1. Re-run “modify schemaUpgradeInProgress attribute” steps above with the following values:

Modify

DN:

Edit Entry

Attribute:

Values:

Operation

☐ Add ☐ Delete ☒ Replace

Entry List

☒ Synchronous

☐ Extended


















2. Test a Managed Service Account creation and verify it goes to the correct container

- From ADMIN PowerShell


- Run: **New-ADServiceAccount -name svc\_test -DNSHostName svc\_test**

```
PS C:\Windows\system32>  
PS C:\Windows\system32> New-ADServiceAccount -name svc_test -DNSHostName svc_test  
PS C:\Windows\system32>
```

1. Confirm that the GMSA is present in the Managed Service Accounts container in ADUC

>  Saved Queries		
▼  Litware.com		
>  Builtin		
>  Computers		
>  Domain Controllers		
>  ForeignSecurityPrincipals		
>  Keys		
>  Litware_ADFS		
>  Litware_Admins		
>  Litware_Groups		
>  Litware_PKI		
>  Litware_Servers		
>  Litware_Users		
>  Litware_Workstations		
>  LostAndFound		
>  Managed Service Accounts		
>  Program Data		

Name	Type
 svc_test	msDS-GroupManagedServiceAccount