# How to install an LDS for use with GnuPG VS-Desktop®

Guide for Administrators

| | |
|---|---|
| Version | 3.x |
| Stand | 2021-09-17 |
| Revision | 001 |

# Content



## Introduction

This is a guide on how to install a Windows LDS system for use as keyserver by GnuPG. LDS is the Lightweight Directory Service of Windows formerly known as ADAM. Instead of using the Active Directory (AD) directly for storing GnuPG keys it is often more appropriate to have a separate server running for this. The major benefit is that there is no need to touch the AD to extend its schema. However, for authentication purposes the AD can still be used with an LDS and replication of LDS instances is also possible.

## Prerequisites

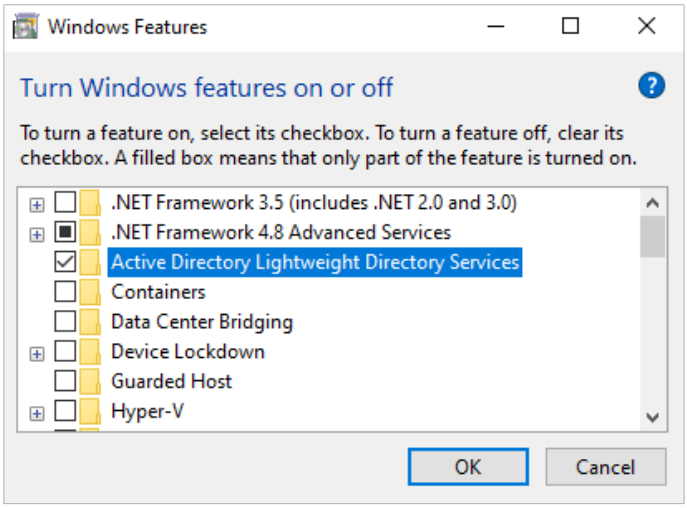
Assign a separate Windows instance for use with LDS or use an instances which does not run a domain controller but, for example, a machine which runs other internal services. In our example we use the domain `w32demo.g10code.de` and the LDS service runs on a machine named `key-server`. The screenshots have been acquired from an English version of Windows-10. The AD in this example has been configured for German; thus some accounts have localized names.

## Manufacturer / Distributor

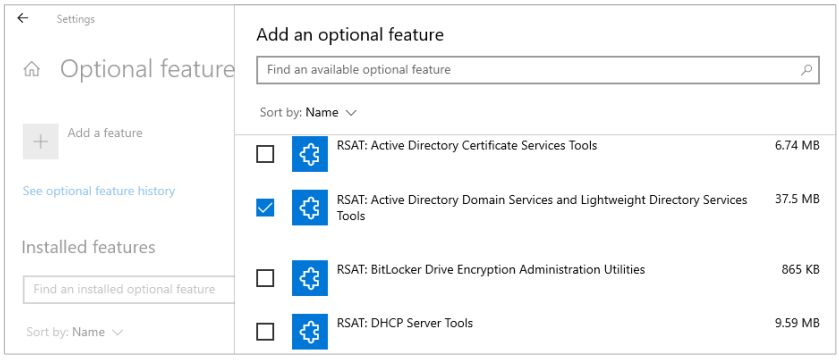
g10 Code GmbH
Gutenbergweg 4
40699 Erkrath / Germany
+49 2104 493 879 0
info@gnupg.com
www.gnupg.com

# 1 Installing the LDS Service

- Create a user in your AD to maintain the LDS installation.
  In our example this is `w32demo\ldsadmin`.
- Login as Administrator to the LDS machine. The LDS service comes with all rent Windows version and can be easily enabled. Open the Windows Features dialog and enable LDS:



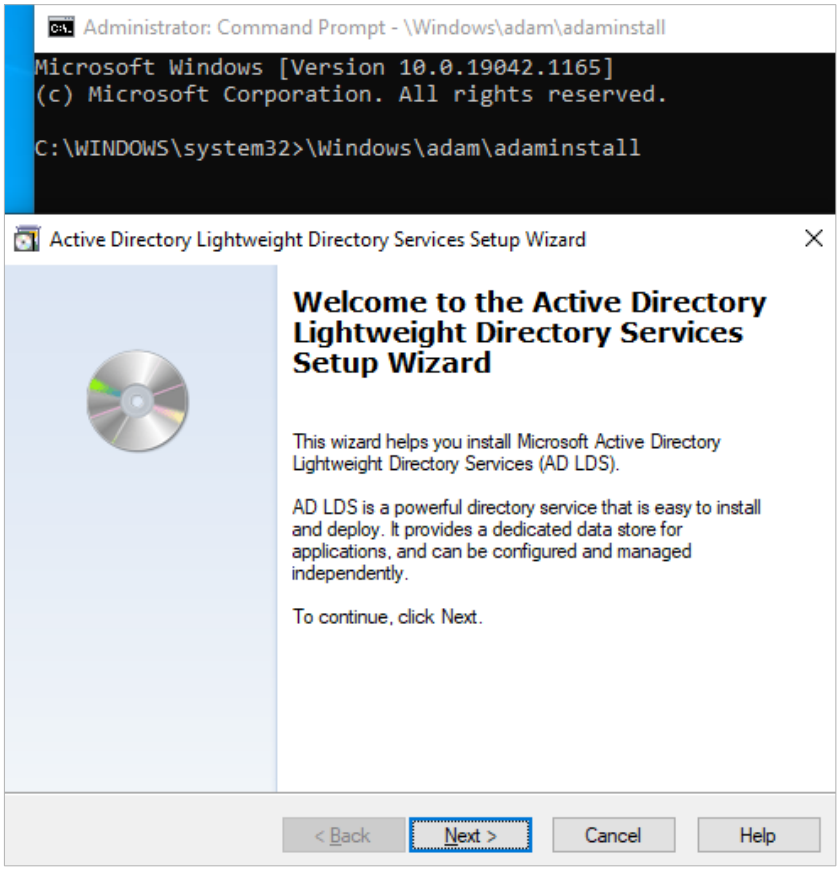

- Click [OK] and the feature will be installed. LDS might already be enabled and running an partition (i.e. an LDAP service). Note that several partitions can be used on one LDS instance; we will later get back to this.
- You also need some extra tools on that machine. Open the dialog to `\emph{Add an Optional Feature}` and scroll down to `\emph{RSAT: Active Directory DomainSerives and Lightweight Directory Services Tool}`and enable this:



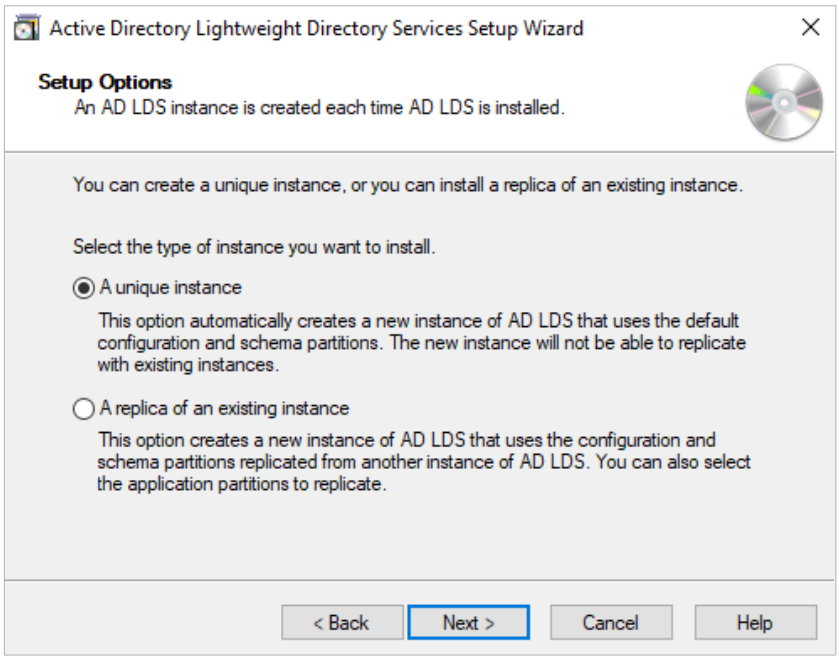

- Click on [Install] to download and install this feature. You may then need to reboot.
- Open a command prompt in Admin mode and enter:

```
\Windows\adam\adaminstall
```

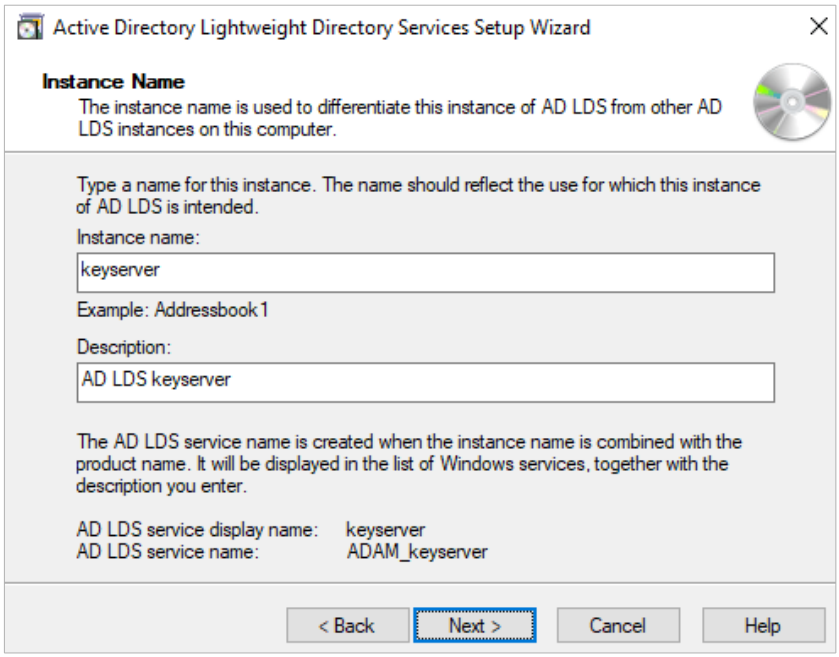
- A wizard dialog pops up:



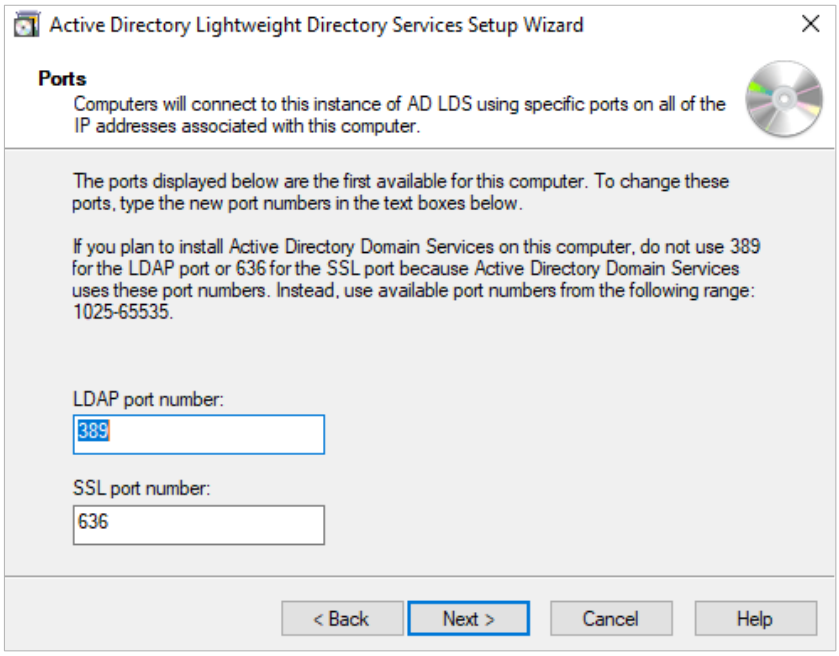

- Click [Next] and select *“A unique instance”*:



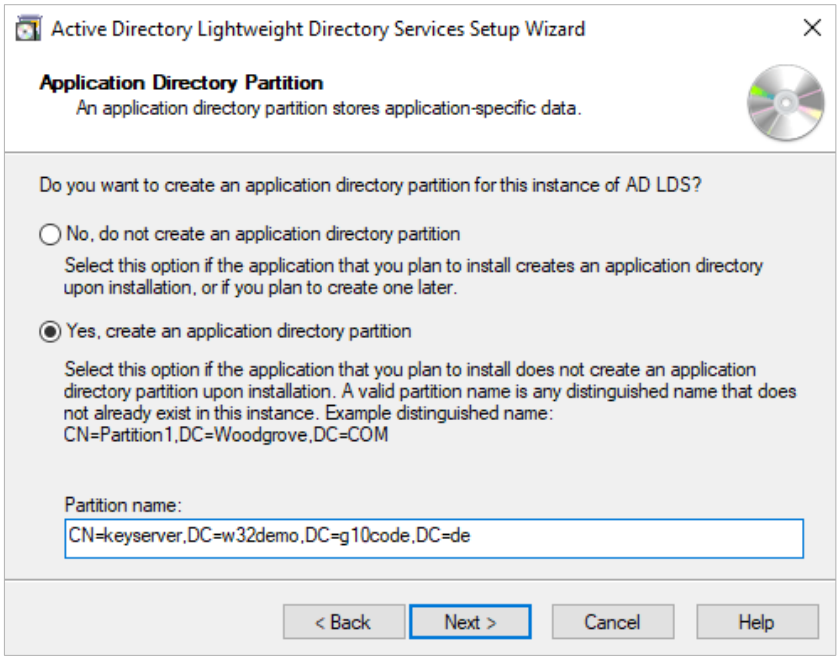
- Click [Next]. On the next dialog enter the name used for the keyserver; it is best to use the name of the machine or an alias for it:



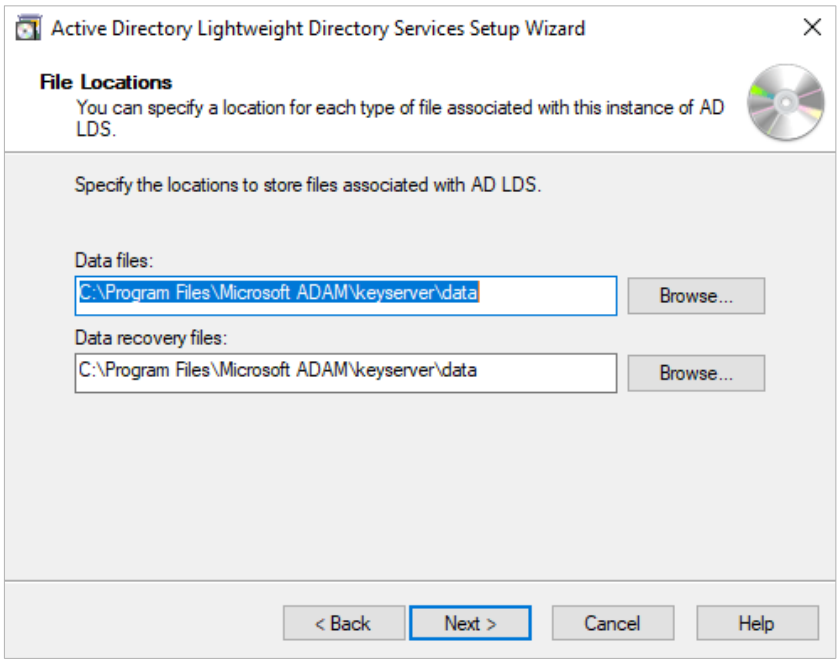

- Click [Next]. The next dialog requests the port numbers to connect to the service. If this is the first instance, use the suggested standard ports. However, if other partitions are already running on that LDS instance you need to choose other ports which will later be part of the GnuPG configuration. Here is the standard case:



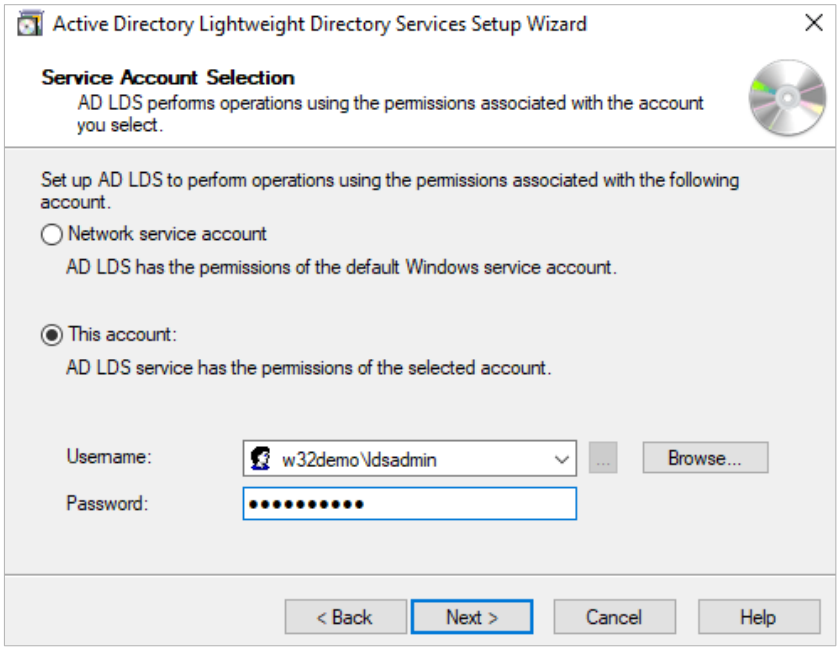

- Click [Next]. In the next dialog you need to create a partition. Enter the DN of the service:



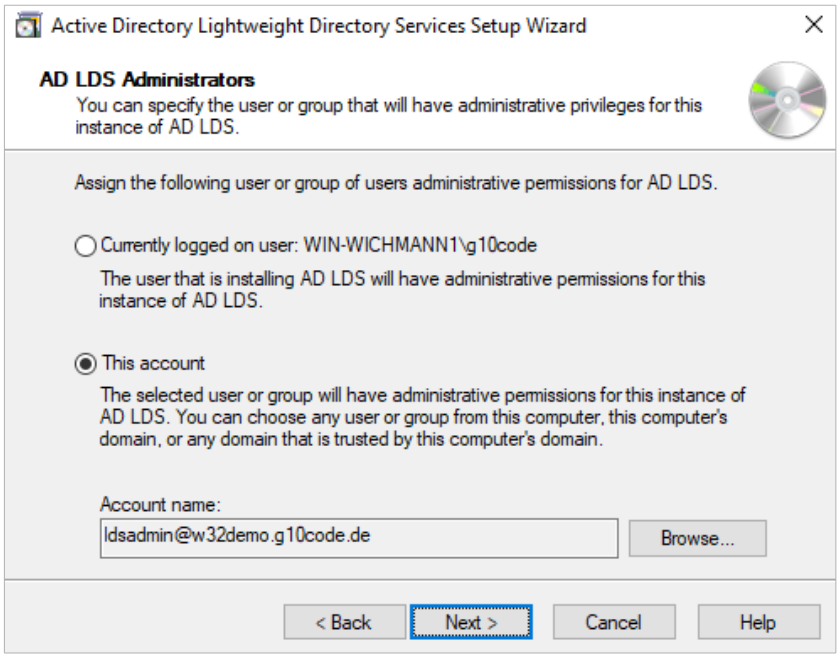

- Click [Next]. The next dialog allows to change the location of the LDS files; in general you will use the defaults:



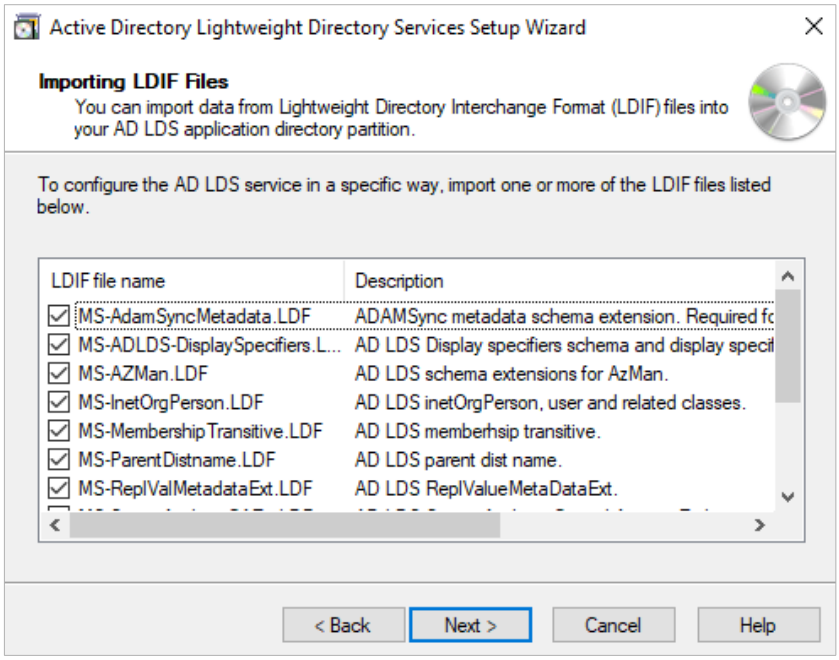

- Click [Next]. In the next dialog select the account under which the the service will run. Use the [Browse]-button to select the *“ldsadmin”* account:



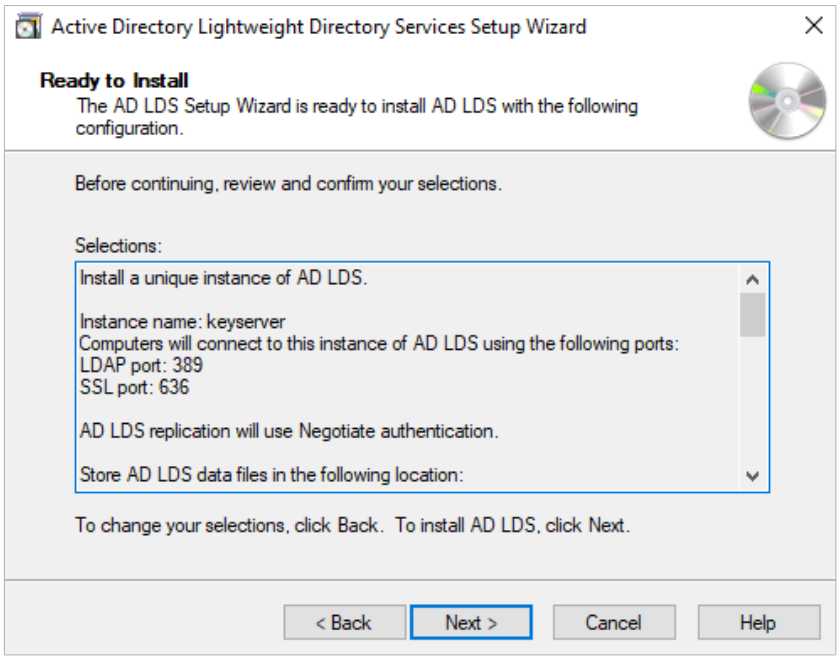

- Click [Next]. You now need to specify an account to administer the LDS instance; obviously we use the *"ldsadmin"* account:



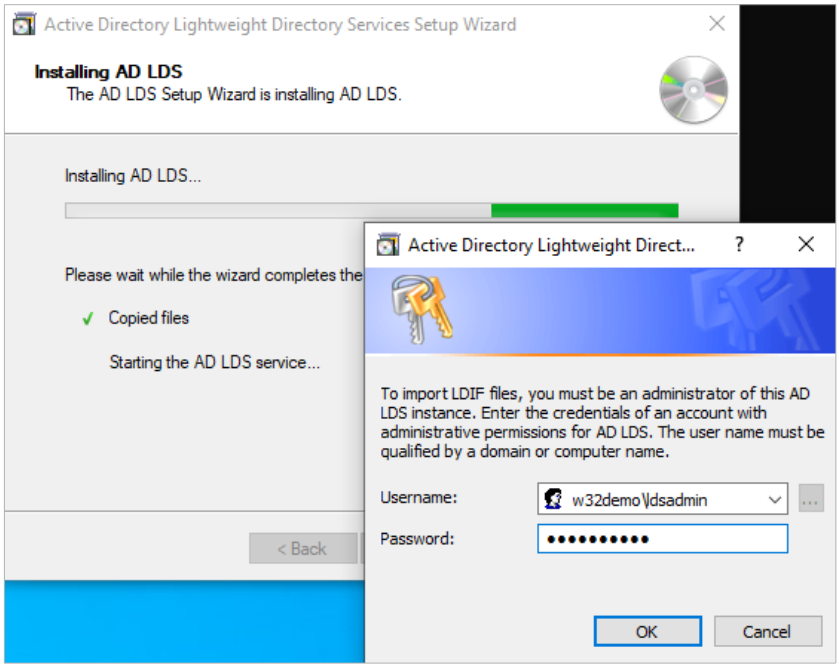

- Click [Next]. Check all boxes to import the usual schemes:




- Click [Next] to view a summary of the configuration options:




- Click [Next] to start the installation. You will be asked to enter the credentials for the administrative account for this LDS. For us this is the *“ldsadmin”*:




- That's it. You now have a running LDS instance which we extend in the next step to host keys for GnuPG.

## 1.1 Setting the LDS up as Keyserver

- Logout as Administrator of the local machine and login as *"ldsadmin"*.
- Download these files:

  https://gnupg.org/misc/gnupg-ldap-ad-schema-v1.ldif

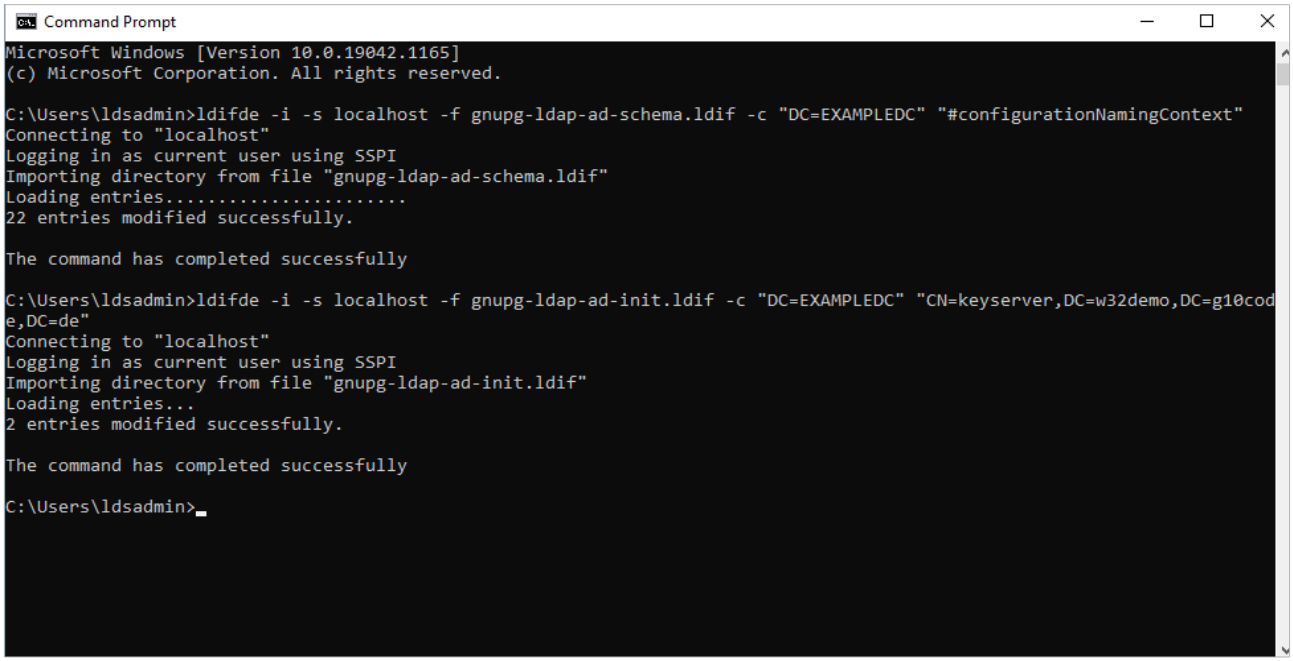
  https://gnupg.org/misc/gnupg-ldap-ad-init-v1.ldif
- Open a command prompt and enter as one line:

```
ldifde -i -s localhost -f gnupg-ldap-ad-schema-v1.ldif
-c "DC=EXAMPLEDC" "#configurationNamingContext"
```

  Then enter as one line:

```
ldifde -i -s localhost -f gnupg-ldap-ad-init-v1.ldif
-c "DC=EXAMPLEDC" "CN=keyserver,DC=w32demo,DC=g10code,DC=de"
```

- Here you need to replace the last part with the keyserver DN you specified during installation. If you do not use the default port (ie. 389) for your LDS installation, but, say 11371, you need to use `localhost:11371` for the `-s` option. If everything works you should see this on your command window:




- That's all. If you want to test this and GnuPG is also installed on this machine you may run this (as always on a single line):

```
gpg --keyserver ldap://localhost/????gpgNtds=1 --batch
--locate-key info@gnupg.com
```

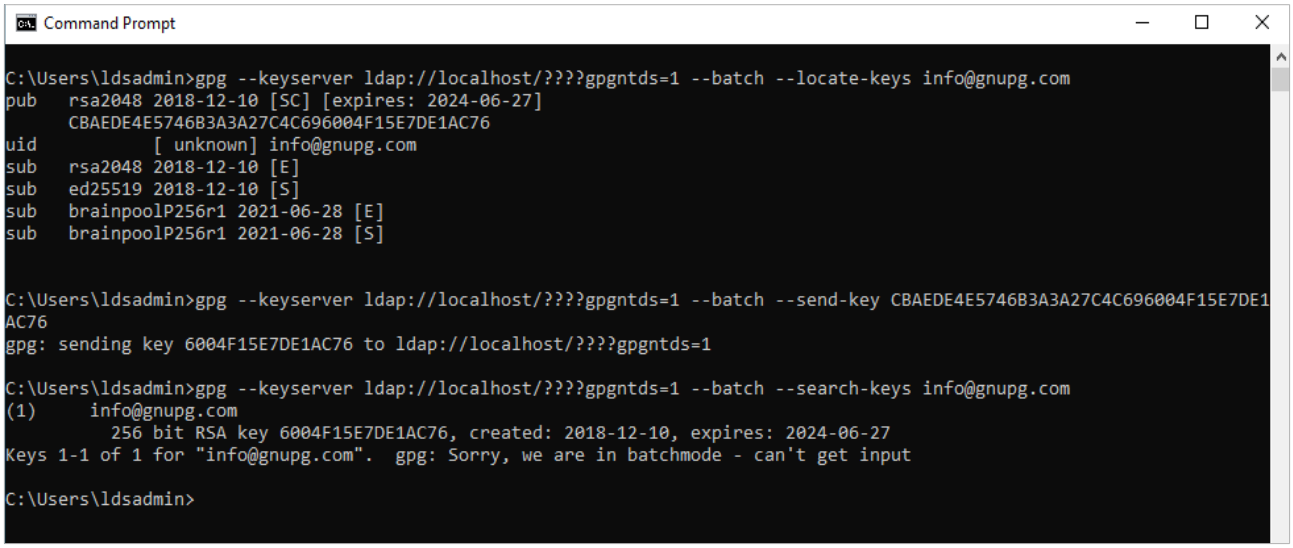
  which imports a public key. Take the fingerprint of that key and run:

```
gpg --keyserver ldap://localhost/????gpgNtds=1 --batch
--send CBAEDE4E5746B3A3A27C4C696004F15E7DE1AC76
```

  to send this key to your new keyserver.

- To test whether you can retrieve this key use:

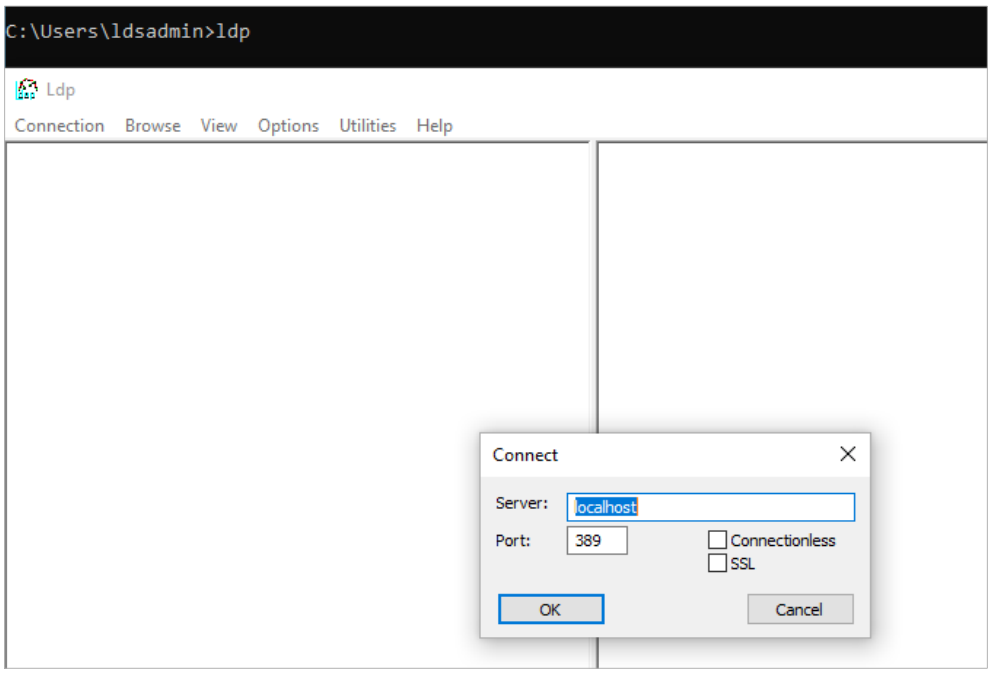
```
gpg --keyserver ldap://localhost/????gpgNtds=1 --batch
--search-keys info@gnupg.com
```



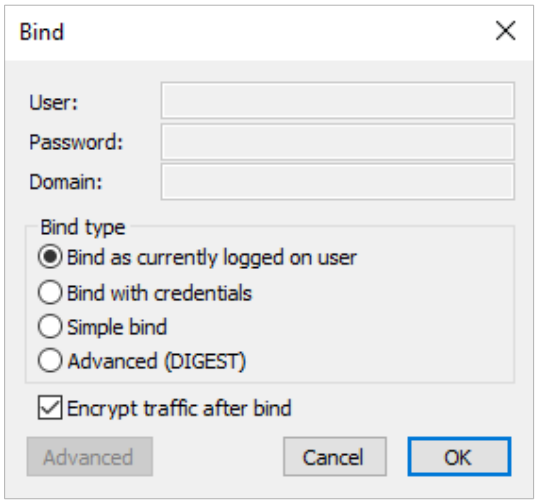

- If you see information about the key everything is fine (the warning about *“batchmode”* can be ignored). The final step will assigning of permissions to the LDS so that other users in the domain can access retrieve and send keys. See the next section.

## 1.2 Assigning Permissions

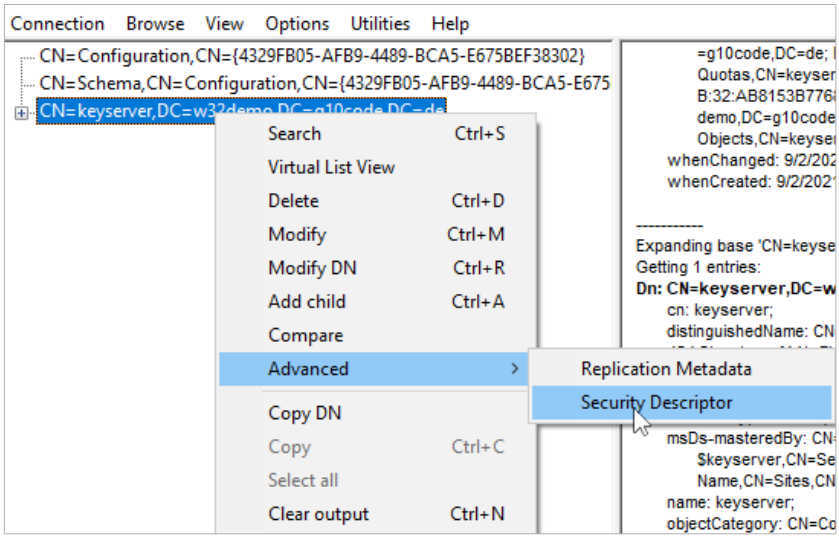
- We want to allow all domain users to retrieve keys and users from an assigned group to send keys. Surely, this depends on your exact needs but here we describe our standard method.
- Login as *“ldsadmin”*, start `ldp`, and connect to the localhost:



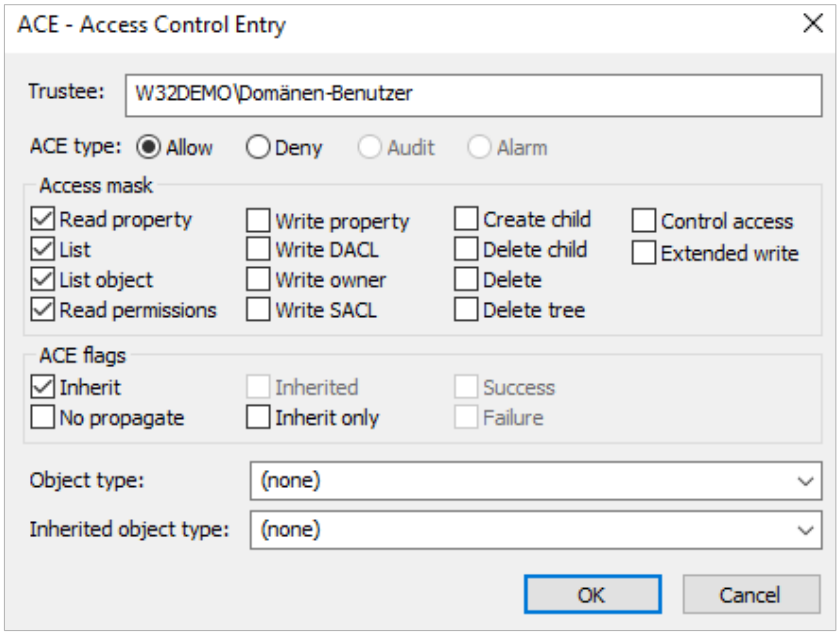
- After you have connected estabish a binding using your current user. Use [Connection] > [Bind] from the menu or hit [Ctrl] + [B]:



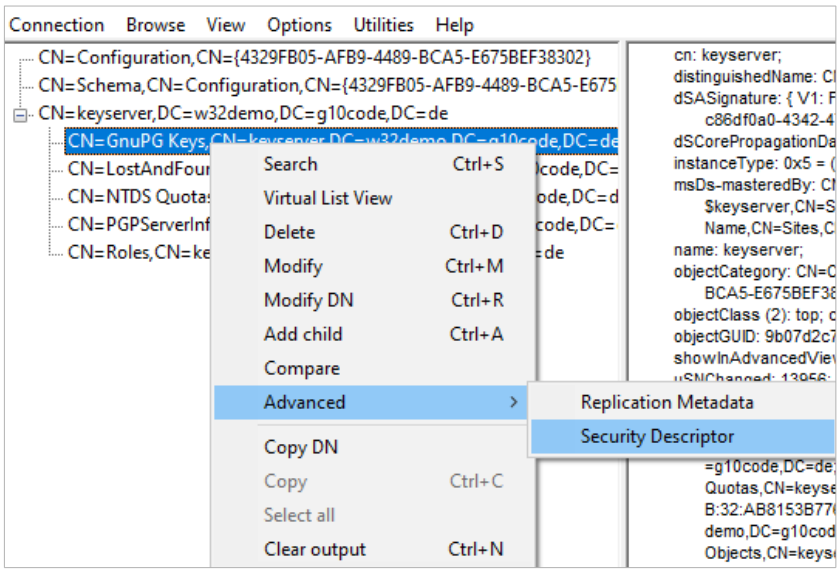

- To browse the DIT use [View] > [Tree] or hit [Ctrl] + [T]. Just hit hinter on the dialog asking for the Base-DN. Then select the DN for your service and use the context menu to open the dialog for the *"Security Descriptor"*:




- The Access Control Entry opens and add as *"Trustee"* the value "*Authenticated Users"* prefixed with your domain name (you may also use the entire DN of that group). Note that in the screenshot below you see *"Domänen-Benutzer"*, which is what you need to use on an German installation of the Active Directory instead of *"Authenticated Users"*. This group has all users (and otehr objects) which are allowed to login to the domain with the exception of the *"Guest"* and *"Anonymous accounts"*. Give the DN full read access and make it inheritable:




- Next is to expand the DN and open the security descriptor dialog for the DN starting with *"CN=GnuPG Keys"*:




- Give the same permissions as above and add *"Write property"* and *"Create Child"*. Now all authenticated users may read from the keuyserver and also update or insert keys. If you want to restrict update and insert capabilities to a dedicated group of users, you can use the permission system to do this.

# 2 Using GnuPG with an LDS Keyserver

- Since GnuPG version 2.2.26 you can put:

```
keyserver ldap://mykeyserver.example.org/????gpgNtds=1
```

  into `dirmngr.conf` and `gpg.conf` and Windows takes care of authentication.

- GnuPG can also be advised to consult this configured LDS similar to a Web Key Directory. For this put:

```
auto-key-locate local,ntds,wkd
```

  into `gpg.conf` so that a missing key is first looked up on the LDS keyserver before a WKD query is done.