

NAS Installation - Synology DSM 7.4

Upgrade from DSM 6.4

- First upgrade to DSM 7.0 through *Control Panel*
- Go to the [Synology Download Center](#), *Select product type* and *Select your Synology Product*, then *Select DSM version* currently installed and the latest DSM version offered for this product as a target DSM version
- Upload the downloaded update file in *Control Panel* -> *Update & Restore* -> *Manual DSM Update* and start the update
- The update should run without issues, after which there are a few extensions which are obsolete and which you can uninstall

KMIP for key management

- Follow the guide to install [KMIP](#) on a Synology NAS server and client
- Further guidance for [KMIP for key management](#)
- How to setup a [KMIP Server \(PyKMIP\)](#) on Debian 13

Encrypted shared folders

- On a NAS where encrypting the entire /volume1 is not necessary or not advisable (no sensitive data, or performance concerns) you can encrypt single shared folders.
- To avoid data in encrypted shared folders get into the wrong hands follow my guide [Encrypted partitions/folders with auto-mount](#). This guide is outdated, but principles still apply. I will update the guide in due time.

Setup rescue login

- Since DSM 7.2 and DS220+ and younger models Synology offers full volume encryption. This is finally the protection you need to fully protect all your data, including mail directories and user directories.
- You need to setup the volume with encryption when you first create the volume, a non-encrypted volume cannot be encrypted in place.
- The encryption keys will be stored in the Encryption Key Vault of the NAS, the keys will be automatically applied on boot of the system. This protects against theft or change of hard disks, but not against theft of the entire NAS. To protect against theft of the NAS you need to move the Encryption Key Vault to an external device running a KMIP server, which is supported by Synology. How to setup the KMIP server on a Synology NAS is described in [KMIP for key management](#).
- If you do not have another Synology NAS on another location, or you do not want to use your other NAS on another location as the KMIP server, you can install a working KMIP server on a linux machine. How this is done is described in [KMIP Server \(PyKMIP\)](#).

- You need to take precautions in case you get locked out from your DSM because the Encrypted Key Vault is not accessible. Synology let's you login with SSH when password login is enabled even if the homes directory is not accessible (e.g. if it resides on the non-accessible encrypted volume). However, enabling password login is a security risk which I want to avoid, so I developed a method to handle this case in [Rescue an encrypted volume](#) .

Migrate MailPlus Server to new NAS

1. Backup full system configuration on your source NAS in **Control Panel -> Backup & Restore -> Configuration Backup -> Export** and save it to your local drive
2. Restore the configuration backup on your target NAS in **Control Panel -> Backup & Restore -> Configuration Backup -> Restore**, select only *Users* and *Groups* from *Users, Groups, Shared Folders, Application Privileges*, leave everything else unchecked
3. Install *Hyper Backup* on your source NAS
4. Install *Hyper Backup* and *Hyper Backup Vault* on your target NAS
5. Run a *Hyper Backup* task for application *Synology MailPlus Server* with your target NAS as destination
6. Enable *rsync* service on your target NAS in **Control Panel -> File Services -> rsync** on default port 22
7. Go to **Control Panel -> File Services -> Advanced -> Shared Folder Sync** on your source NAS, click *Task List* and create a manual full sync task with the (internal) IP address of your target NAS as destination
8. Do the sync before you intend to switch to the target NAS. Once everything else is setup, come back to **Shared Folder Sync** and do another full sync. The initial sync takes a while, but the follow up sync executes fast as *rsync* only copies files which were added or changed in the meantime.
9. Update all port forwards in your firewall to your target NAS
10. If you have a web server running on a different machine you probably keep your target NAS behind a reverse proxy. In this case you need to update the reverse proxy settings to reach your target NAS.
11. Check your mail server by sending mail and receiving mail
12. Remove the sync task you created from your source NAS (see above) in **Control Panel -> File Services -> Advanced -> Shared Folder Sync** click *Task List*
13. Set the login portal for the mail client in **Control Panel -> Login Portal -> Applications**
14. Use *traceroute* to find connectivity issues to your mail server from another computer:

```
sudo traceroute -T -p 5001 your.mailserver.tld
```

15. Set up regular backups to safeguard your MailPlus data on the new NAS using *Shared Folder Sync* and *Hyper Backup*.
16. Create a scheduled task on your target NAS to copy renewed certificates (e.g. using Let's encrypt) if your NAS is behind a reverse proxy:

```
#!/bin/sh
#
# Copy certificates from web server to NAS, must be run as root
# (c) Bernard Condrau, 2026-08-25: adapted to DSM 7.4
#
SERVER="your_webserver_generating_certificates"
PORT=22
```

```
IDENTITY="/volume1/homes/user/.ssh/id_rsa"
# make sure your user can run rsync and cksum as root without password
(check visudo)
SERVER_RSYNC="sudo rsync"
SERVER_CKSUM="sudo cksum"
SERVER_CERTDIR="/etc/letsencrypt/live/cloud.condrau.com"
# CERTDIR must be hardcoded and is different in every server instance
CERTDIR="_archive/"$(sudo cat
/usr/syno/etc/certificate/_archive/DEFAULT)
CERTROOTDIR="/usr/syno/etc/certificate"
PACKAGECERTROOTDIR="/usr/local/etc/certificate"

# compare cksums first to decide whether certificates need to be copied
REM_PRIV=$(ssh -i $IDENTITY -p $PORT user@$SERVER $SERVER_CKSUM
$SERVER_CERTDIR/privkey.pem | cut -d' ' -f 1)
LOC_PRIV=$(cksum $CERTROOTDIR/$CERTDIR/privkey.pem | cut -d' ' -f 1)

if [[ $LOC_PRIV -ne $REM_PRIV ]]; then

    # copy certificates from web server
    sudo rsync -aPle "ssh -i $IDENTITY -p $PORT" --rsync-
path="$SERVER_RSYNC" user@$SERVER:$SERVER_CERTDIR/cert.pem
$CERTROOTDIR/$CERTDIR/cert.pem
    sudo rsync -aPle "ssh -i $IDENTITY -p $PORT" --rsync-
path="$SERVER_RSYNC" user@$SERVER:$SERVER_CERTDIR/fullchain.pem
$CERTROOTDIR/$CERTDIR/fullchain.pem
    sudo rsync -aPle "ssh -i $IDENTITY -p $PORT" --rsync-
path="$SERVER_RSYNC" user@$SERVER:$SERVER_CERTDIR/privkey.pem
$CERTROOTDIR/$CERTDIR/privkey.pem
    sudo rsync -aPle "ssh -i $IDENTITY -p $PORT" --rsync-
path="$SERVER_RSYNC" user@$SERVER:$SERVER_CERTDIR/chain.pem
$CERTROOTDIR/$CERTDIR/chain.pem

    # push the updated archive certificates to the system and restart
web services
    sudo /usr/syno/bin/synow3tool --gen-all
    sudo /usr/syno/bin/synosystemctl restart nginx

    echo "certificates updated"
else
    echo "nothing to update"
fi

exit 0
```

17. Check basic TCP connectivity:

```
telnet [smtp_host] [port] (e.g., telnet smtp.gmail.com 587)
```

18. Check certificate assignment in Synology DSM

```
openssl s_client -connect mail.yourdomain.tld:465 -showcerts
```

```
openssl s_client -connect mail.yourdomain.tld:993 -showcerts
openssl s_client -connect mail.yourdomain.tld:587 -starttls smtp -
showcerts
```

19. If the *verify return code: 0* is not 0 but 1 or another number, your DSM most likely does not serve the intermediate certificate. In this case you need to do the following:
 1. Go to **Control Panel -> Security -> Certificate -> Settings** and assign Synology's default certificate to *MailPlus-Server-dovcot* and *MailPlus-Server-postfix*. Click **OK** and wait 30 seconds, then set the certificates back to your Letsencrypt certificate and hit **OK**.
 2. Go to **Control Panel -> Security -> Advanced -> Custom Settings** and set *MailPlus-Server-dovcot* and *MailPlus-Server-postfix* to *Intermediate compatibility*.
 3. Stop and restart *Synology MailPlus Server* and *Synology MailPlus (Client)*.
20. You can also enter `cat /var/packages/MailPlus-Server/target/etc/main.cf | grep .pem` and check whether `fullchain.pem` is referenced.
21. Re-check the certificate assignment.
22. Open **MailPlus Server** and go to **Mail Delivery -> General**. *Enable SMTP authentication* and *disable external postmaster* in *External Postmaster*.
23. Disable *SMTP-SSL/TLS (port 465)* in **Synology MailPlus Server -> Service**

Check MailPlus Server connectivity

- Use the following command from an external source and from within your LAN:

```
openssl s_client -starttls smtp -connect smtp.example.com:587
```

- If external access works, but LAN access does not, then you have likely run into DNS/hairpin NAT issues. You best solve this by adding your mail host to the host overrides table. In [pfSense firewall](#) this is at *Services -> DNS Resolver -> General Settings*, scroll down to the bottom of the page.
- You can check this by accessing your SMTP Server from within your LAN by IP address instead of the mail domain name.
- Another good tool to check SMTP accessibility is [swaks](#):

```
sudo apt update
sudo apt install swaks
swaks --to recipient@example.com \
      --from sender@example.com \
      --server smtp.example.com \
      --port 587 \
      --tls \
      --auth LOGIN \
      --auth-user your_username \
      --auth-password your_password
```

- Make sure your web server who uses your SMTP Server will not get blocked by DSM or MailPlus Server. Go to *MailPlus Server -> Mail Delivery -> Security -> Block/Allow List* and *Control Panel -> Security -> Protection*, check *Block List* and add the web server's IP address to the *Allow List*.

Links

- [How do I migrate MailPlus to another Synology NAS?](#)
- [What network ports are used by services on my Synology system?](#)
- [Configuration Backup](#)
- [Shared Folder Sync](#)

From:

<https://wiki.condrau.com/> - **Bernard's Wiki**

Permanent link:

<https://wiki.condrau.com/syno:dsm7inst?rev=1790622518>

Last update: **2026/09/29 02:08**

