

# Installation guide

## Prerequisites for Installing the Federated Data Sharing Appliance

Before you begin the installation process, there are several prerequisites you need to fulfill to ensure a smooth and secure deployment. In this section, we'll walk you through the necessary steps to prepare for the installation, including obtaining a License Key, SSH Key, SSL Certificate, and setting up a Fully Qualified Domain Name (FQDN) and SMTP Server.

### Prerequisite 1: System requirements

- OS: Linux -> Ubuntu 20.04 LTS or higher; Rocky OS version 8+
- CPU: 4 cores or more
- Memory: 8GB or higher
- Storage: 100GB (Min)
- Privileged access (root access)
- Libraries and Tools: Git 1.8+
- Open Port 443 accessible from the internet

### Prerequisite 2: SSL Certificate

An SSL certificate ensures that data transmission between your appliance and users is encrypted and secure. You can obtain an **“FULL CHAIN”** SSL certificate in the following manner:

1. **SSL Purchase:** Purchase a public SSL/TLS v1.2+ CA Certificate (.crt and .key) from a reputable Certificate Authority (CA) like GoDaddy, DigiCert, or Comodo. Avoid using free solutions like 'Let's Encrypt.'
2. **CSR generation:** Follow the CA's instructions to generate a Certificate Signing Request (CSR) and submit it. Once approved, you'll receive the SSL certificate files, including the public key, private key, and intermediate certificates. Keep these secure.
3. **Certificate Note:** When obtaining your SSL certificate, remember to coordinate with your administrator to extract the private key.

### Prerequisite 3: Fully Qualified Domain Name and Public IP Address

A Fully Qualified Domain Name (FQDN) is necessary to access your Federated Data Sharing Appliance over the internet. Here's how to set up an FQDN

1. DNS Selection: Choose a domain name registrar (e.g., GoDaddy, Namecheap) and register a domain name.
2. DNS Configuration: Configure the DNS records for your domain to point to your server's public IP address.
3. DNS Resolution: Ensure that your chosen FQDN resolves correctly to your server.
4. Email the FQDN to [fdsa.support@alzheimersdata.org](mailto:fdsa.support@alzheimersdata.org) for ADWB FAIR Whitelisting. If using a Load Balancer, send the Public facing FQDN.

## Prerequisite 4: SSH Key

To get the project we will need the SSH Key. Here is how to create one:

1. In the server where FDSA is going to be installed, start the root user mode:

```
sudo su
```

2. Generate an SSH Key using your email (you can leave the passphrase empty, but it's optional):

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

3. View the generated SSH Key:

```
cat /root/.ssh/id_rsa.pub
```

4. Copy and send the Public Key to [fdsa.support@alzheimersdata.org](mailto:fdsa.support@alzheimersdata.org). Our support team will add your key to the GitHub FDSA-Release repository and notify you when it's ready.

## Installation Steps

**Note:** If you intend to use an external database instead of the default/local one, refer to the section '[How to use an external PostgreSQL DB for the internal FDSA management](#)' before proceeding.

**Note:** To install behind a load balancer, please first read [How to install behind a load balancer](#).

1. Start the root user mode:

```
sudo su
```

2. Ensure the installation directory exists:

```
mkdir -p /var/www
```

3. Navigate to the installation directory:

```
cd /var/www/
```

4. Clone the release repository from one of the following options:

```
git clone git@github.com:alzheimersdata-org/federated-data-sharing-appliance-releases.git
```

5. Enter the 'federated-data-sharing-appliance-release' directory:

```
cd federated-data-sharing-appliance-releases
```

6. Copy the '.env-template' and rename it to '.env':

```
cp .env-template .env
```

7. Copy your SSL certificates to the 'ssl-certs' folder:

```
cp -f <PATH_TO_YOUR_CERT>/fullchain_certfile.crt ./ssl-certs/fullchain_certfile.crt
```

```
cp -f <PATH_TO_YOUR_PRIVATE_KEY>/private_keyfile.key ./ssl-certs/private_keyfile.key
```

8. Start the appliance and complete the required fields:

```
bash ubuntu-startup.sh host.example.com
```

9. After the installation is completed, you will receive your Super Admin credentials as an output in the console.

10. Reboot the server: `reboot`

# Upgrade guide

To update FDSA, follow the steps below:

## Ubuntu OS

1. Log in as the root user: `sudo su`
2. Go to the installation directory: `cd /var/www/federated-data-sharing-appliance-releases`
3. Run the Ubuntu upgrade script: `bash change-version.sh`

## Rocky OS

1. Log in as the root user: `sudo su`
2. Go to the installation directory: `cd /var/www/federated-data-sharing-appliance-releases`
3. Run the Rocky upgrade script: `bash rocky-update-version.sh`