

Installation of the target web-server

The *target web-server* is based on Ubuntu 14.04.5 LTS, has a public IP address and runs both a SSH and HTTP service. Both services are protected by a local IP firewall and an application firewall. As looking at a static html page may not be that sexy we have installed an *emby media server* capable of serving 4 different movies: two analog clocks (with sound), *Seven red lines* from Youtube and a seven second movie of a cartoon rabbit coming out of a hole.

The pre-requisite is Ubuntu 14.04.5 LTS with an ssh server installed.

1. How to Install the media server emby on top of NGINX

This is a documented procedure for the installation of **emby** a media streaming server used as a target for the DEiC Distributed Denial of Service Project. The media server hosts a number of interesting videos, among one 12 hour long video of a analog clock with hands. The purpose of the installation is to demonstrate a service under attack.

Notice that the following commands require root privileges.

Start by installing an Ubuntu 14.04 LTS server with an SSH daemon. Reboot and install patches:

```
apt-get -y update  
apt-get -y dist-upgrade
```

Reboot if required.

Install the local developed packages from SSI:

- `cmod_1.1-2.deb` : modules (not essential)
- `dailybuandupdate_1.6-1.deb` : automated patch and backup. Patches are installed on a daily basis, the host reboots if required.
- `grouproot_1.2-1.deb` : shared administrator environment (not essential)

Next install [NGINX](#):

```
apt-get -y install nginx
```

Then install the [emby](#) media server:

```
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 0A506F712A7D8A28  
echo 'deb http://download.opensuse.org/repositories/home:/emby/xUbuntu_14.04/' > /etc/apt/sources.list.d/emby-server.list  
apt-get -y update  
apt-get -y install emby-server
```

You may have to start it manually:

```
service emby-server start
```

The emby server is now running on TCP port 8096.

Next configure NGINX to proxy port 80 to port 8096:

```

test -f /etc/nginx/sites-available/default.org || {
    /bin/cp -v /etc/nginx/sites-available/default \
        /etc/nginx/sites-available/default.org
}

cat << 'EOF' > /etc/nginx/sites-available/default
#
# emby as default server
#
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /usr/share/nginx/html;
    index index.html index.htm;

    # Make site accessible from http://localhost/
    server_name localhost;

    location / {
        proxy_pass http://127.0.0.1:8096;
    }
}
# HTTPS server
#
#server {
#    listen 443;
#    server_name localhost;
#
#    root html;
#    index index.html index.htm;
#
#    ssl on;
#    ssl_certificate cert.pem;
#    ssl_certificate_key cert.key;
#
#    ssl_session_timeout 5m;
#
#    ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;
#    ssl_ciphers "HIGH:!aNULL:!MD5 or HIGH:!aNULL:!MD5:!3DES";
#    ssl_prefer_server_ciphers on;
#
#    location / {
#        proxy_pass http://127.0.0.1:8096;
#    }
#}
EOF

```

Then reload the nginx configuration:

```
nginx -s reload
```

The emby server is now running on TCP port 80.

2. Local host security

The server has to be secured. As everything has been installed as packages and all patches will be applied on a daily basis we just need to apply general IP address filtering and brute force login mitigation. The installation and configuration of a host-based intrusion detection system is outside the scope of this document. See e.g. [OSSEC](#).

2.1. IP filtering

Enable the build in [ufw](#) IP firewall - the commands may block your access:

```
ufw enable
ufw default deny incoming
ufw default allow outgoing
```

Then open for *forskningsnet* addresses:

```
for CIDR in 95.128.24.0/21 130.225.0.0/16 130.226.0.0/16 192.38.0.0/17 185.1.5
7.0/24
do
    ufw allow from ${CIDR} to any port 22
    ufw allow from ${CIDR} to any port 80
    ufw allow from ${CIDR} to any port 443
done
```

And check the rules has been enabled:

```
ufw status numbered
```

A comprehensive introduction to *ufw rules* on Ubuntu 14 is available at [digitalocean](#).

2.2. Application firewall

While the *ufw* rules limits access to *forskningsnet* addresses, it doesn't prevent brute force attacks.

[fail2ban](#) is an intrusion prevention software framework that protects computer servers from brute-force attacks. Written in the Python programming language, it is able to run on POSIX systems that have an interface to a packet-control system or firewall installed locally, for example, iptables or TCP Wrapper. It may be installed with:

```
apt-get -y install fail2ban
```

And an configuration for the emby media server added with:

```

cat << EOF > /etc/fail2ban/filter.d/emby.conf
# Fail2Ban filter for emby

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]

_daemon = emby-server

failregex = Info HttpSession: HTTP Response 401 to <HOST>.*authenticatebyname
           Info HttpSession: HTTP Response 500 to <HOST>.*mediabrowser/Users/None
one

ignoreregex =

# Invalid username or password entered
# DEV Notes:
#
# Matching on http 401 with a trailing url including 'authenticatebyname' to
# catch incorrect passwords
# Matching on http 500 with a trailing url including 'mediabrowser/Users/None'
# to catch incorrect usernames
#
# From: https://emby.media/community/index.php?/topic/31362-fail2ban-custom-em
# by-filter/
EOF

```

The configuration is enabled by adding a section to `/etc/fail2ban/jail.local` which may or may not exist already.

```

test -f /etc/fail2ban/jail.local.org || {
    /bin/cp /etc/fail2ban/jail.local /etc/fail2ban/jail.local.org
}
touch /etc/fail2ban/jail.local.org

(
    cat /etc/fail2ban/jail.local.org > /etc/fail2ban/jail.local
    cat << EOF >> /etc/fail2ban/jail.local
    [emby]
    enabled = true
    port = 8096
    filter = emby
    logpath = /var/lib/emby-server/logs/server-*.txt
    maxretry = 2
    EOF
)

```

Finally the service has to be reloaded:

```
service fail2ban reload
```

3. Emby configuration

The configuration is done through the Web-UI, but requires data to be added in advance.

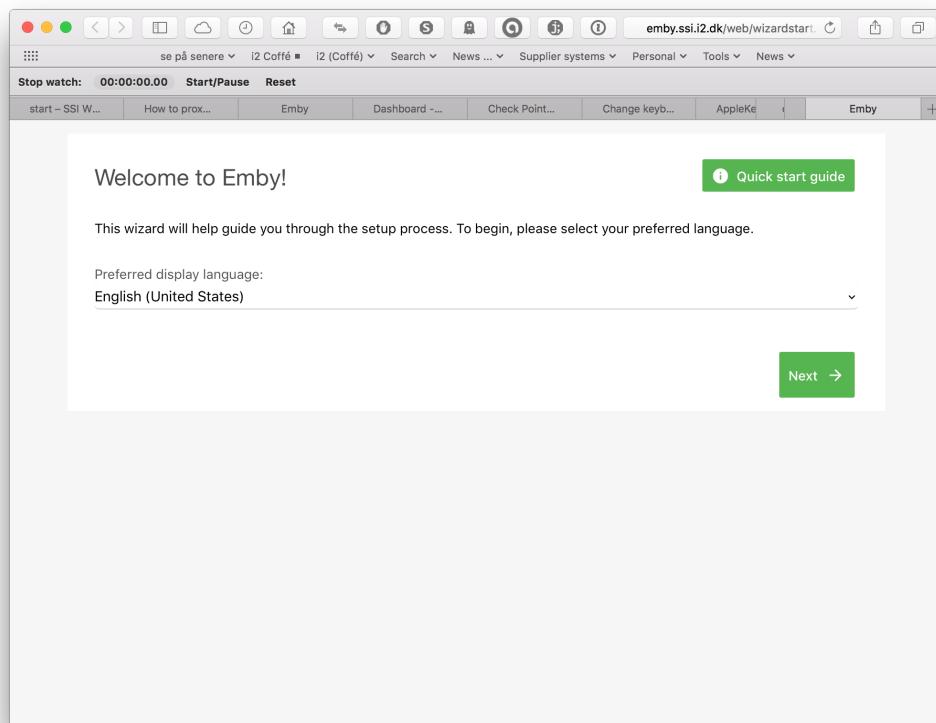
3.1. Data - lots of clocks but no cats

```
mkdir -p /home/media/Movies
```

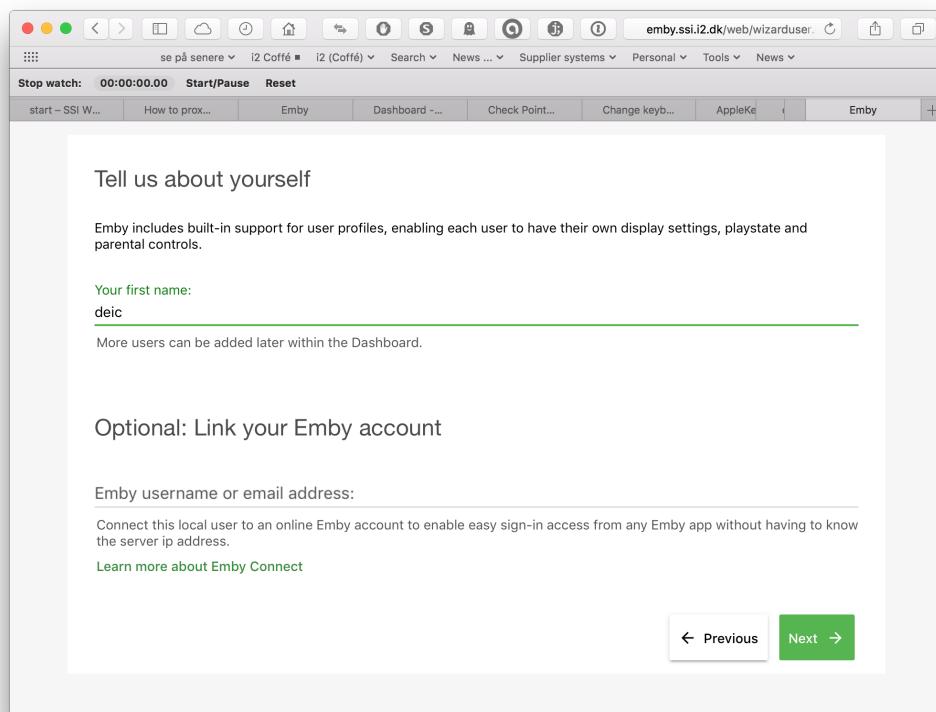
Upload relevant information from `/lan/ssi/shared/docs/emby-test-data`

3.2. Configuration

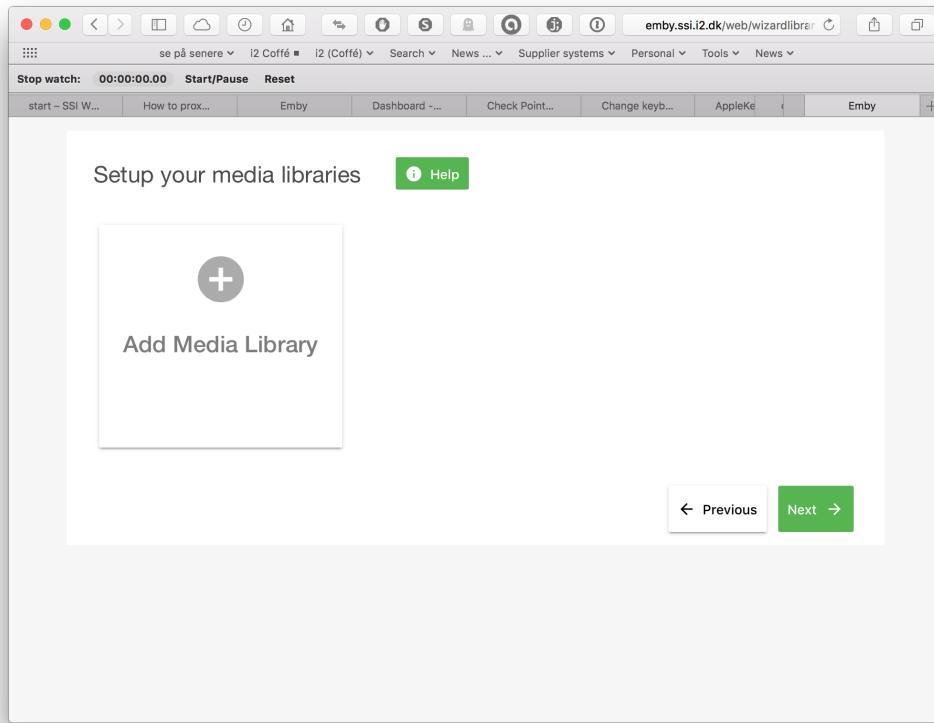
The goal is to have one user - deic - and manual login with username and password on the main web page and no anonymous data collection. The Web-UI configuration is done this way; select language



well come



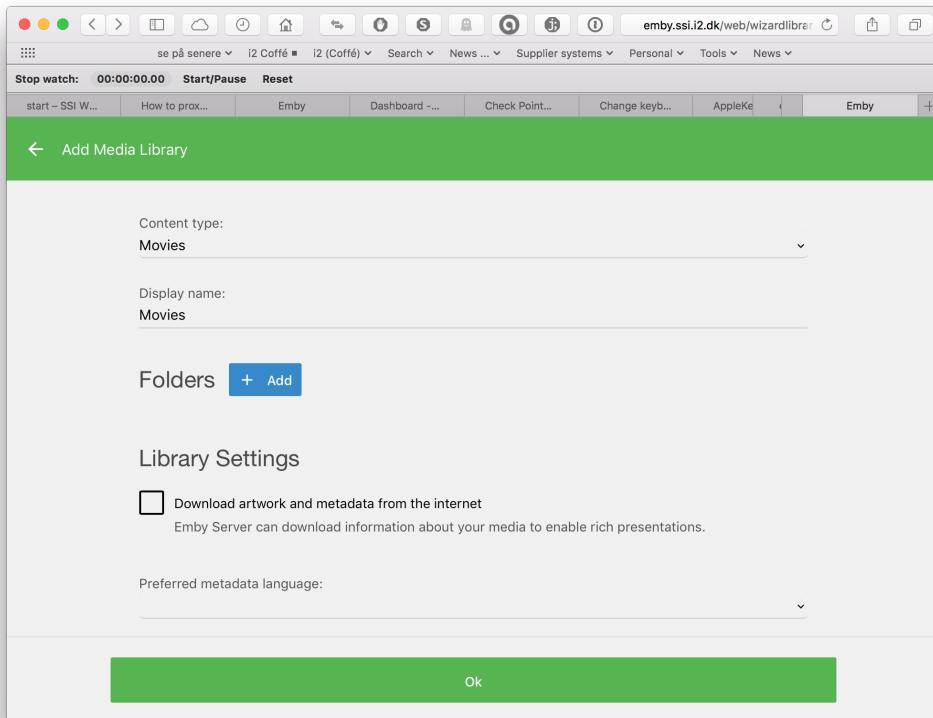
create a user



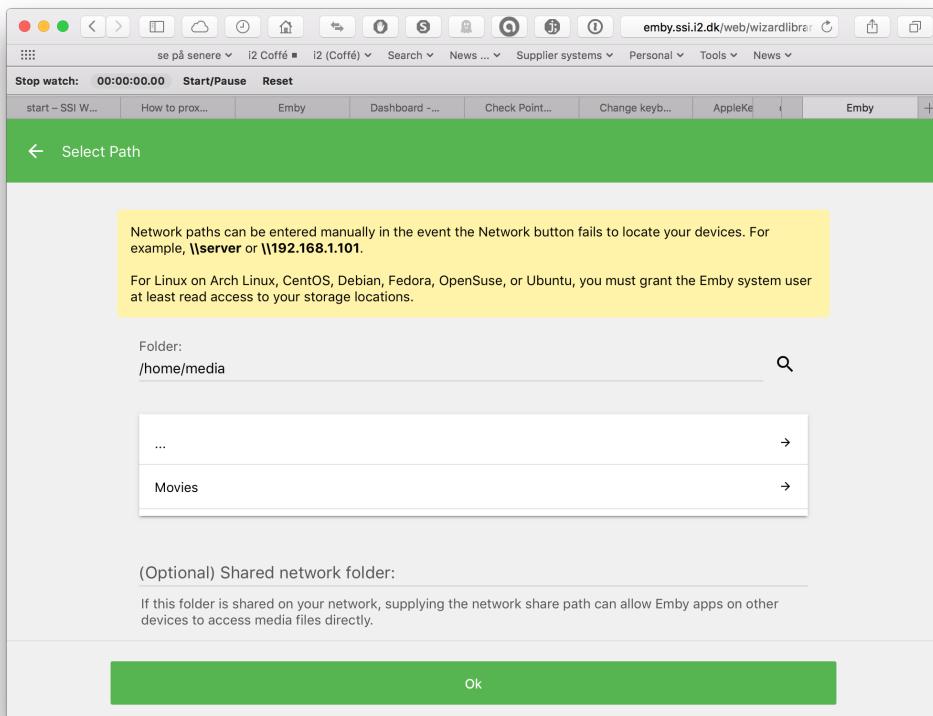
add media libraries - Movies

A screenshot of the 'Add Media Library' configuration page. The title bar says 'Add Media Library'. The content area has a green header bar with the text '← Add Media Library'. Below this, there are two input fields: 'Content type:' with 'Movies' selected and 'Display name:' also with 'Movies'. Underneath these is a 'Folders' section with a blue '+ Add' button. Below this is a 'Library Settings' section. It contains a checked checkbox for 'Download artwork and metadata from the internet' with the note 'Emby Server can download information about your media to enable rich presentations.' At the bottom is a large green 'Ok' button.

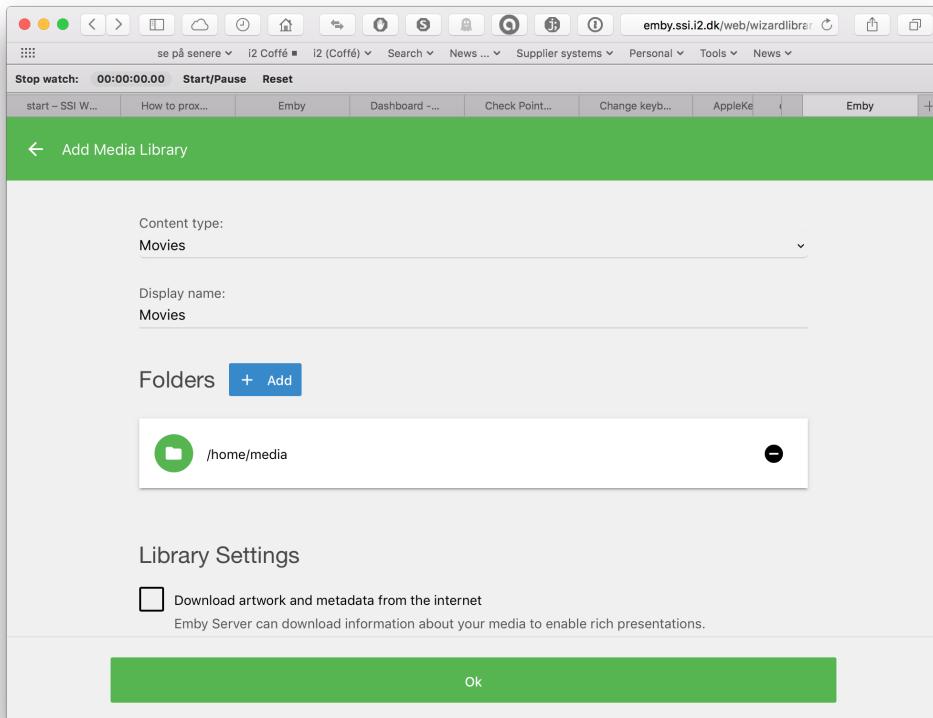
select folders



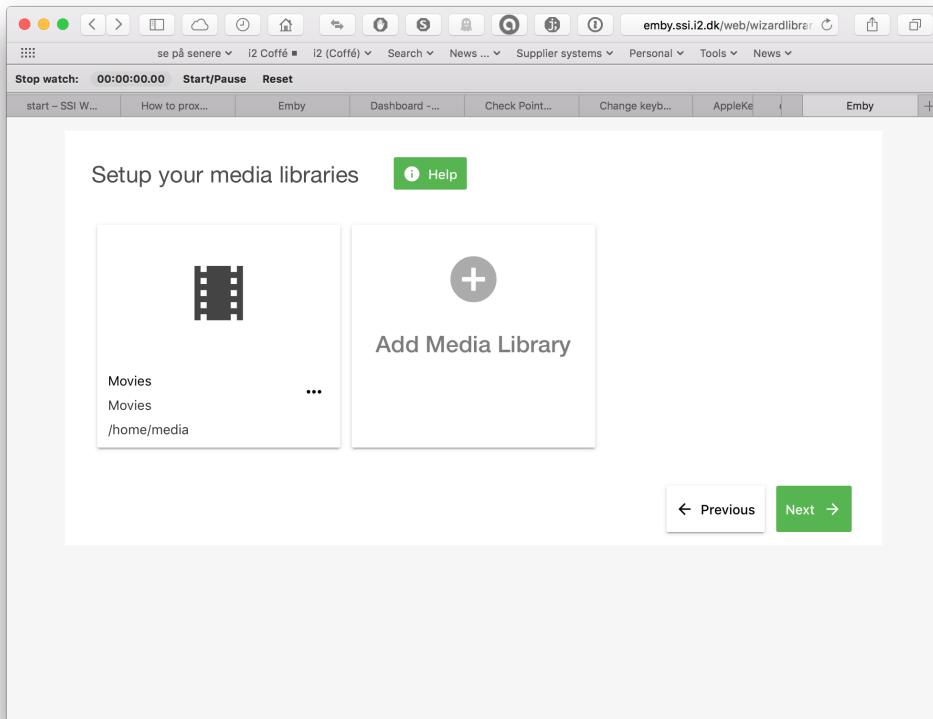
Add - and don't download information from the Internet



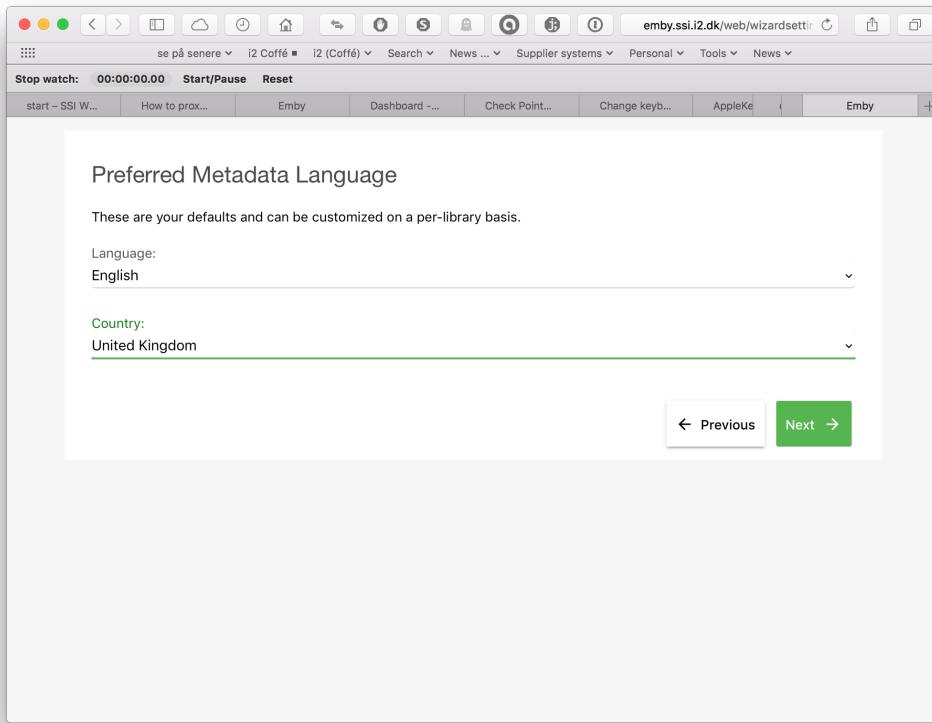
Local filesystem navigation



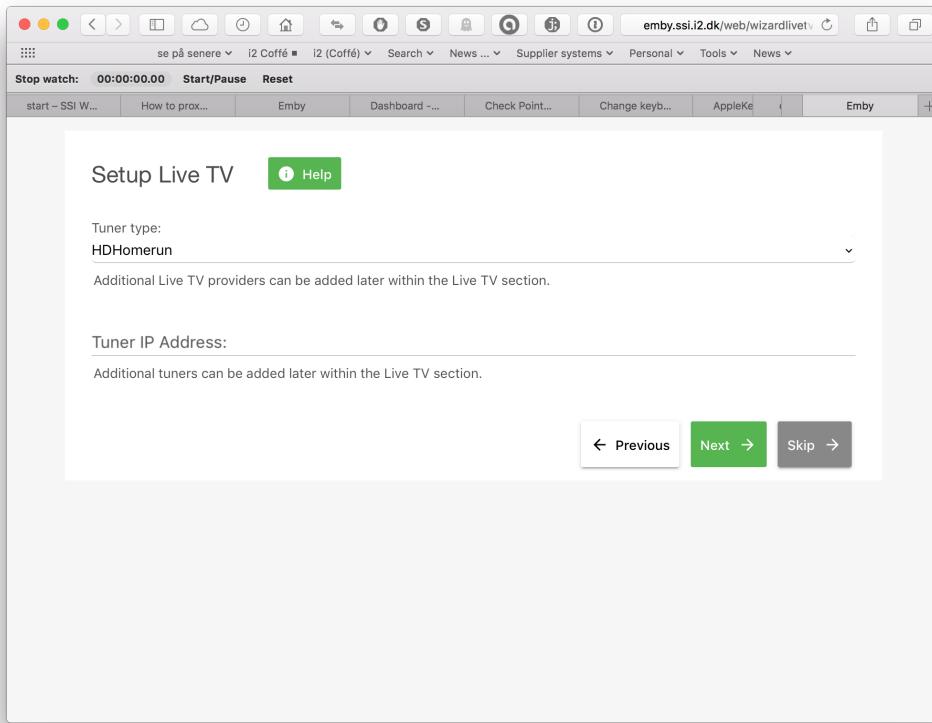
click ok



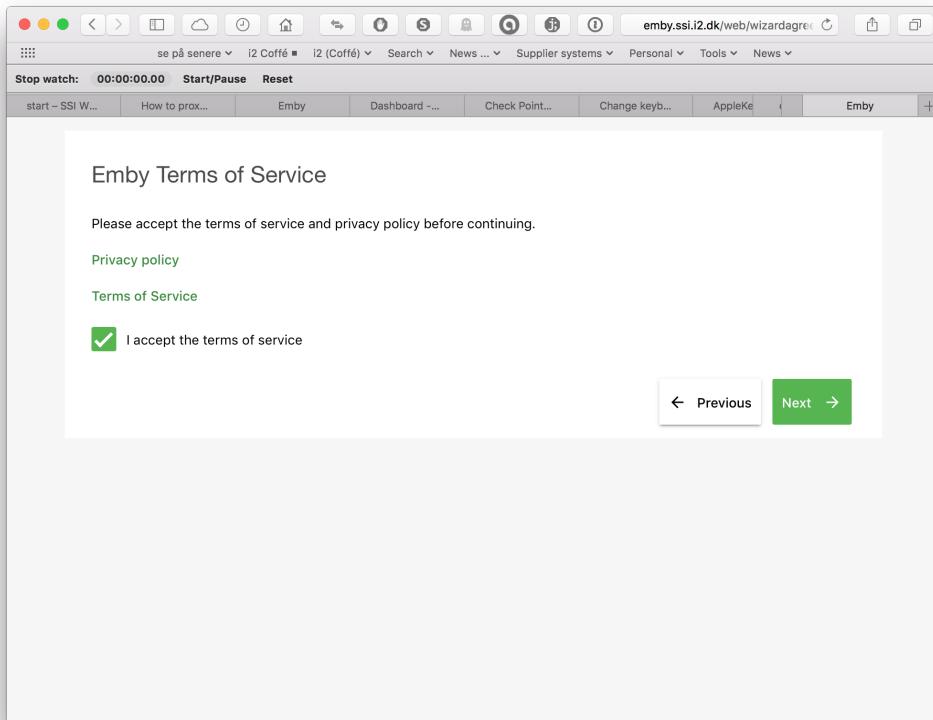
Next



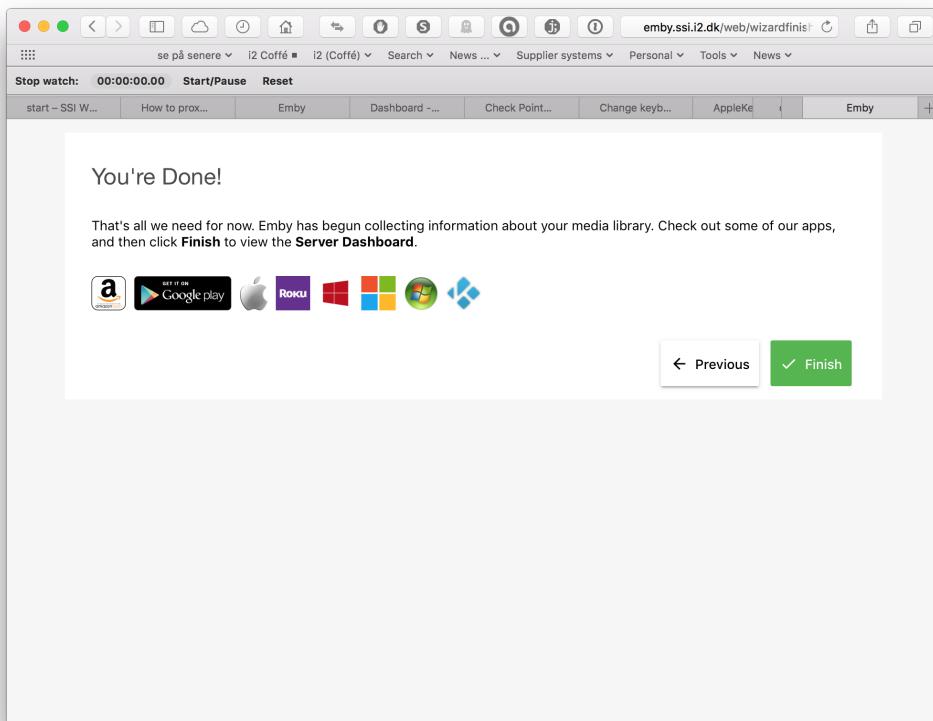
Select Language



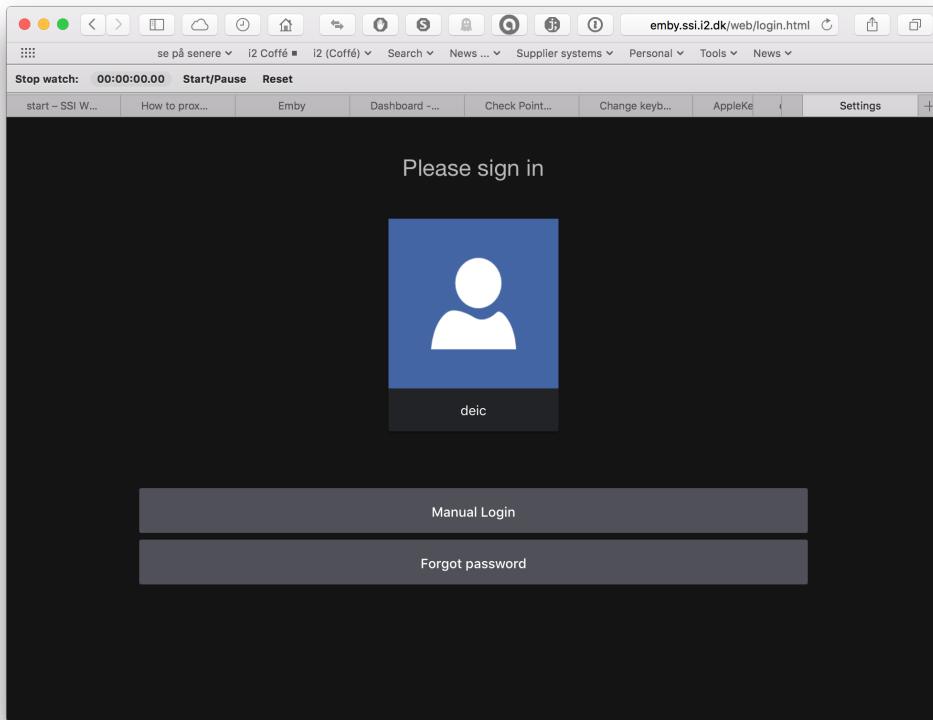
Disable Live TV



Accept Terms of Service



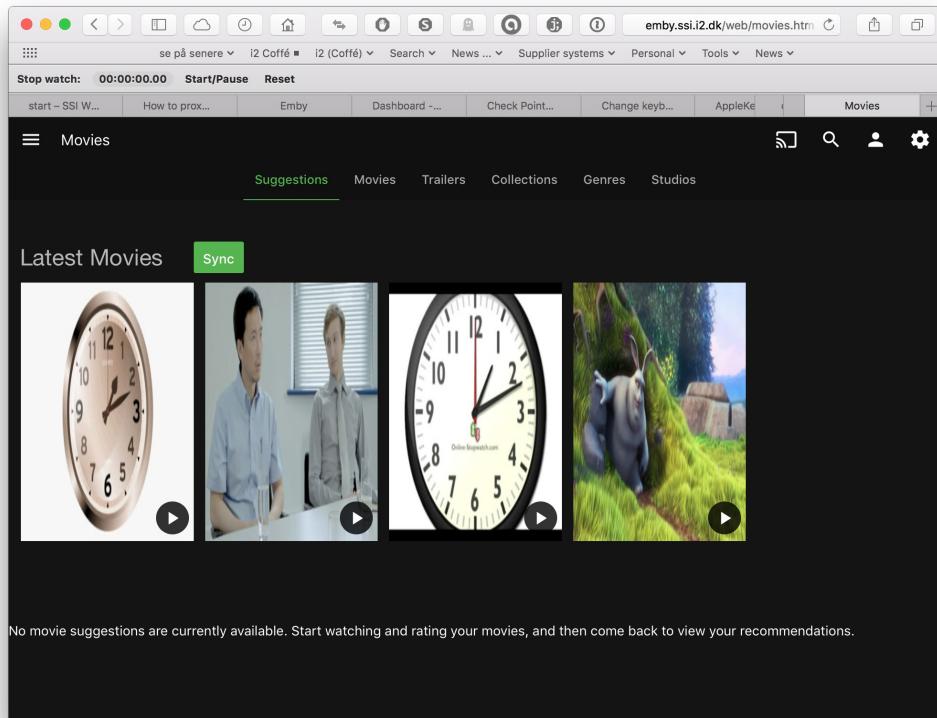
Finish



Sign in

A screenshot of the Emby home page. The URL in the address bar is "emby.ssi.i2.dk/web/home.html". The page has a dark background. At the top, there's a navigation bar with links like "se på senere", "i2 Coffé", "Search", "News", "Supplier systems", "Personal", "Tools", and "News". Below the navigation bar, there's a "Stop watch" section with "00:00:00.00", "Start/Pause", and "Reset" buttons. A logo for "emby" is on the left, followed by a search bar and user account icons. The main content area starts with a "Welcome to Emby" message and a "Take the tour" button. Below that is a section titled "My Media" featuring two red rectangular buttons labeled "Folders" and "Movies". At the very bottom of the page, there's a small "Install Emby" link.

Check movies



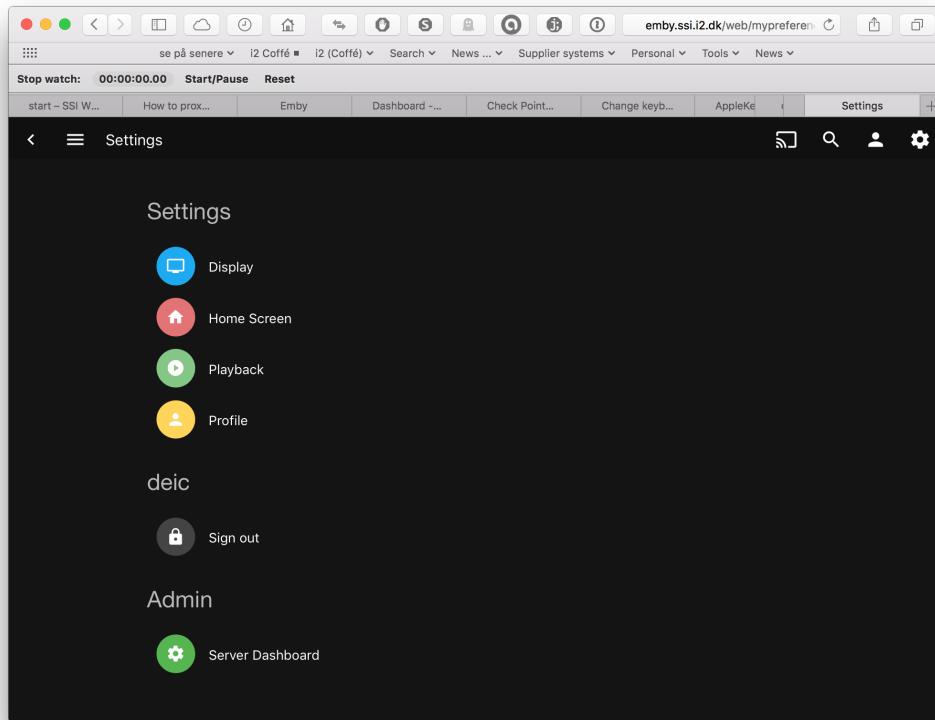
Select movie

A screenshot of the Emby item details page for a video file named 'big_buck_bunny'. The page has a dark theme. At the top, there's a navigation bar with 'Stop watch', 'Search', 'News', 'Supplier systems', 'Personal', 'Tools', and 'Movies'. Below the navigation bar, there's a sub-navigation bar with 'Emby', 'Dashboard', 'Check Point...', 'Change keyb...', 'AppleKe', 'Emby', and a '+' button. The main content area shows a thumbnail of a cartoon rabbit in a grassy field. The title 'big_buck_bunny' is displayed, along with '0 mins' and 'Ends at 3:36 PM'. Below the title are several control buttons: 'Play', a three-dot menu, a trash can, a checkmark, and a heart. At the bottom of the video card, there are technical details: '720P', 'H264', '5.1', 'AAC', and 'Added 3/6/2017 3:32 PM'.

Media Info

Video	Audio
Codec H264	Language und
Codec tag avc1	Codec AAC
AVC Yes	Codec tag mp4a
Profile Main	Profile LC
Level 31	Layout 5.1
Resolution 1280x720	Channels 6 ch
Aspect ratio 16:9	Bitrate 384 kbps
Anamorphic No	Sample rate 48000 Hz

Play shortest movie



Select settings (top right corner)

A screenshot of the "Settings" page in the Emby web interface. The URL bar shows "emby.ssi.i2.dk/web/dashboardgeneral.htm". The top navigation bar is identical to the previous screenshot. The left sidebar has a "Settings" section highlighted in green, containing options like "Dashboard", "Devices", "Users", "Emby Premiere", "Library", "Subtitles", "Playback", "Sync", and "Transcoding". Other sections include "Extras" (Auto-Organize, DLNA, Live TV, Notifications, Plugins) and "Expert" (Advanced). The main content area shows "Preferred display language: English (United Kingdom)" with a dropdown menu. It also features a "Support the Emby Team" button with "Enjoy Bonus Features". Under "Advanced", there is a checkbox for "Enable anonymous usage reporting" with a descriptive text and a "Learn more" link. A large green "Save" button is at the bottom.

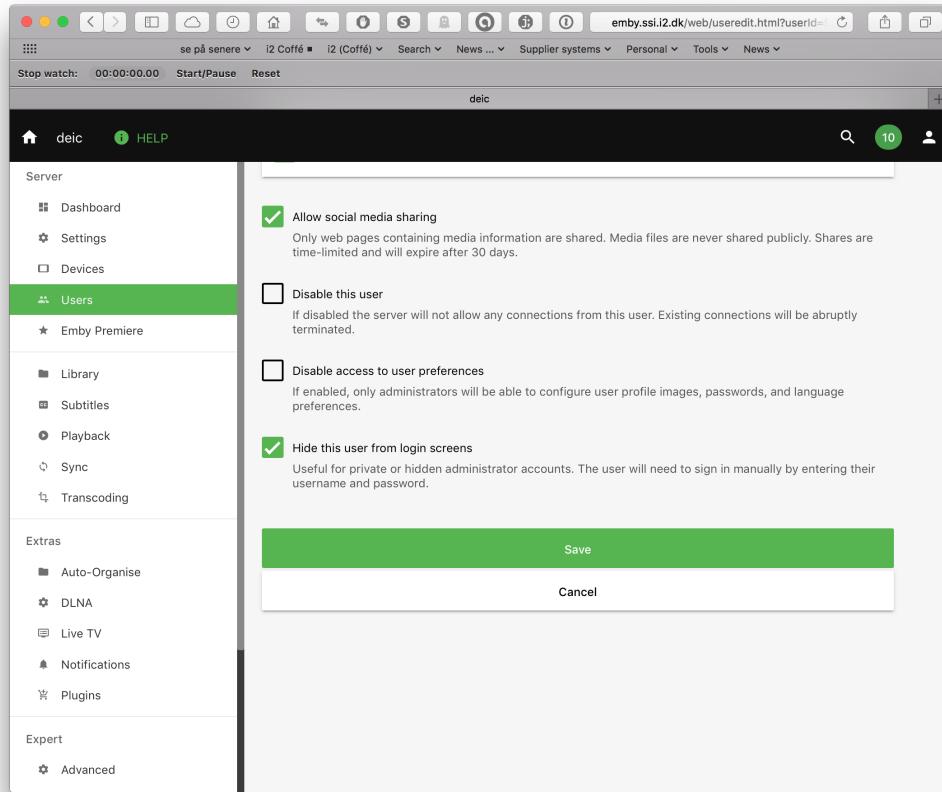
Disable anonymous usage reporting

The screenshot shows the Emby web interface with the URL `emby.ssi.i2.dk/web/useredit.html?userId=...`. The top navigation bar includes links for 'se på senere', 'I2 Coffé', 'Search', 'Supplier systems', 'Personal', 'Tools', and 'News'. A 'Stop watch' timer is at 00:00:00.00. The main menu on the left has sections for 'Server' (Dashboard, Settings, Devices), 'Users' (Emby Premiere, Library, Subtitles, Playback, Sync, Transcoding), 'Extras' (Auto-Organise, DLNA, Live TV, Notifications, Plugins), and 'Expert' (Advanced). The 'Users' section is currently selected. The right panel shows the 'Profile' tab selected, with tabs for Profile, Access, Parental Control, and Password. The Profile section contains fields for 'Name' (set to 'deic') and 'Emby username or email address' (empty). It also includes a note about connecting to an online Emby account for easy sign-in. A checkbox 'Allow this user to manage the server' is checked. The 'Access' section contains four checkboxes: 'Allow media deletion', 'Allow media downloading', 'Allow Live TV access', and 'Allow Live TV recording management', all of which are checked.

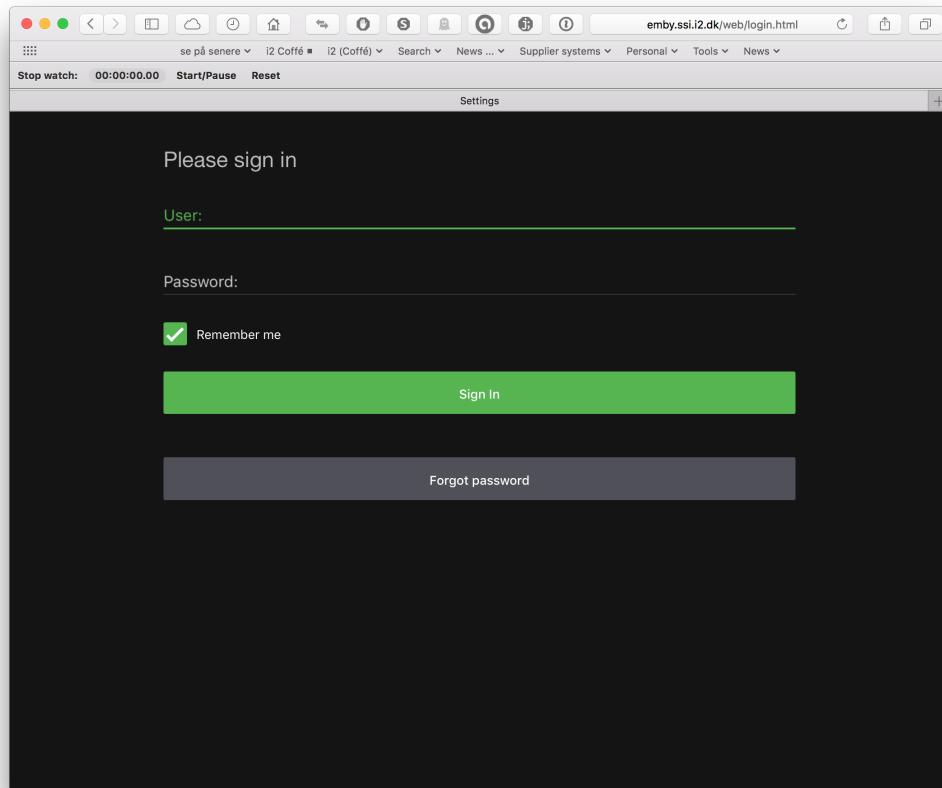
Users->deic

The screenshot shows the Emby web interface with the URL `emby.ssi.i2.dk/web/userpassword.html?userId=...`. The top navigation bar and 'Stop watch' are identical to the previous screenshot. The main menu and 'Users' selection are also the same. The right panel shows the 'Password' tab selected, with tabs for Profile, Access, Parental Control, and Password. It contains fields for 'New password' and 'New password confirm', both of which are empty. A large green 'Save' button is at the bottom of the form.

Set password (1qazxsw2)



scroll down and disable from login screen then sign out



check login screen

That should be it, we now have a media server suitable for target testing.

--- [cover page generator](#)

