Connexió al servidor de l'EUSS

```
mercuri.euss.es al port 25
IP 172.20.0.21
```

Via TELNET

```
usr@host:~$ telnet mercuri.euss.es 25
Trying 172.20.0.21...
Connected to mercuri.euss.es.
Escape character is '^]'.
220 mercuri.euss.es ESMTP Servei correu-e EUSS
```

Comunicació utilitzant SMTP i la IP

```
      usr@host:~$ telnet 172.20.0.21 25
      Trying 172.20.0.21...
      Connected to 172.20.0.21.
      Escape character is '^]'.
Serv: 220 mercuri.euss.es ESMTP Servei correu-e EUSS
Cl:   HELO host
Serv: 250 mercuri.euss.es
Cl:   MAIL FROM: user@gmail.com
Serv: 250 Ok
Cl:   RCPT TO: user1@euss.es
Serv: 250 Ok
Cl:   RCPT TO: user2@euss.cat
Serv: 250 Ok
Cl:   DATA
Serv: 354 End data with <CR><LF>.<CR><LF>
Cl:   Subject: mail d'exemple
      From: user@gmail.com
      To: user2@euss.cat
      Cco: user1@euss.es
      Bon dia,
      Aquest mail d'exemple permet definir dos destinataris.
      Un d'ells estarà ocult amb cco.

      Salutacions
      .
Serv: 250 Ok: queued as 78DF863D5
Cl:   QUIT
Serv: 221 Bye
      Connection closed by foreign host.
```

Si es necessita encriptar les dades d'accés es fa amb base 64.

```
usr@host:~$ echo usuari@gmail.com |base64
dXN1YXJpQGdtYWlsLmNvbQo=
usr@host:~$ echo Password03gmail |base64
UGFzc3dvcmQwM2dtYWlsCg==
```

Per decodificar

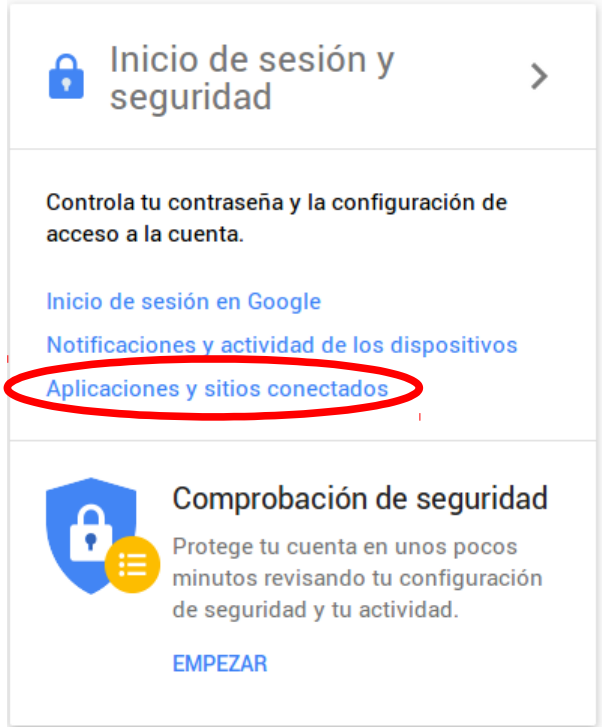
```
usr@host:~$ echo dXN1YXJpQGdtYWlsLmNvbQo= |base64 -d
usuari@gmail.com
```

ACCÉS AL SERVIDOR DE GMAIL
Per pode accedir al servidor de google necessitem les següents condicions:

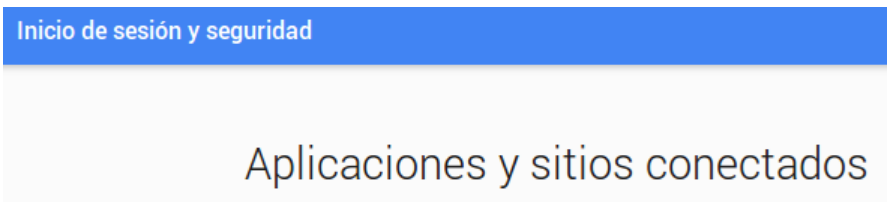
1. Un usuari de google
2. Permetre les comunicacions amb servidors que no són d'alta seguretat.
3. Utilitzar comunicacions encriptades amb un certificat
4. Codificar les dades d'accés en base64.

Permetre les comunicacions amb servidors que no són l'alta seguretat.
Un cop teniu un compte de google cal permetre les comunicacions amb entorns no tan segurs, per fer-ho cal anar a EL MEU COMPTE.

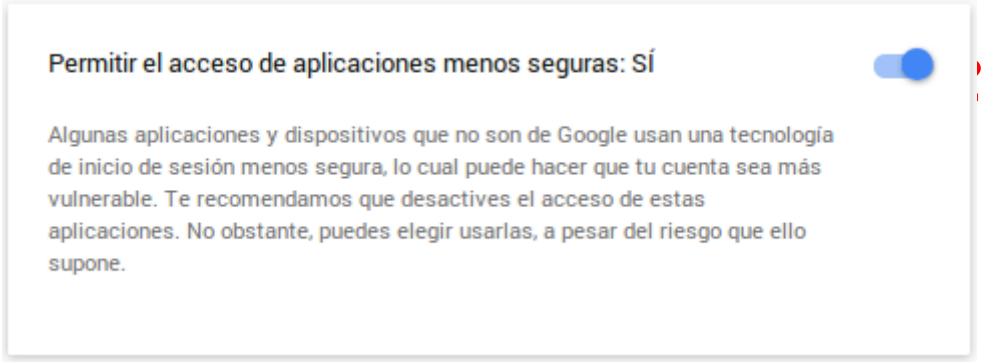
Un cop oberta la plana dels ajustaments del compte cal anar a: INICI DE SESSIÓ i de SEGURETAT i escollir APLICACIONS I LLOCS CONNECTATS



Ens obrirà una plana en que es poden fer diferents controls de les aplicacions connectades.



Una de les opcions és permetre l'accés de les aplicacions menys segures, cal activar l'accés.
Alguns clients de correu (ios d'apple, windows phone o Thunderbird) també ho necessiten.



Utilitzar comunicacions encriptades amb un certificat

Per tal de fer la comunicació de forma encriptada utilitzarem un servei, l'`stunnel4`.

Instal·lació de l'`stunnel4`
És necessari fer la instal·lació com a super-usuari amb `sudo`

```
usr@host:~$ sudo apt-get install stunnel4 -y
[sudo] password for usr:
```

Ara cal crear el fitxer de configuració `/etc/stunnel/stunnel.conf`

```
; Sample stunnel configuration file for Unix by Michal Trojnara 2002-2011
; Some options used here may not be adequate for your particular configuration
; Please read the manual and make sure you understand them

; **************************************************************************
; * Global Options                                                         *
; **************************************************************************

; A copy of some devices and system files is needed within the chroot jail
; Chroot conflicts with configuration file reload and many other features
chroot = /var/lib/stunnel4/
; Chroot jail can be escaped if setuid option is not used
setuid = stunnel4
setgid = stunnel4

; PID is created inside the chroot jail
pid = /stunnel4.pid

; Debugging stuff (may useful for troubleshooting)
;debug = 7
;output = /var/log/stunnel4/stunnel.log

; **************************************************************************
; * Service Defaults (may also be specified in individual service sections)   *
; **************************************************************************

; Certificate/key is needed in server mode and optional in client mode
cert = /etc/stunnel/mail.pem
;key = /etc/stunnel/mail.pem

; Authentication stuff needs to be configured to prevent MITM attacks
; It is not enabled by default!
;verify = 2
; Don't forget to c_rehash CApath
; CApath is located inside chroot jail
```

```
;CApath = /certs
; It's often easier to use CAfile
;CAfile = /etc/stunnel/certs.pem
; Don't forget to c_rehash CRLpath
; CRLpath is located inside chroot jail
;CRLpath = /crls
; Alternatively CRLfile can be used
;CRLfile = /etc/stunnel/crls.pem

; Disable support for insecure SSLv2 protocol
options = NO_SSLv2
; Workaround for Eudora bug
;options = DONT_INSERT_EMPTY_FRAGMENTS

; The following options provide additional security at some performance penalty
; Default ECDH/DH parameters are strong/conservative, so it is quite safe to
; comment out these lines in order to get a performance boost
options = SINGLE_ECDH_USE
options = SINGLE_DH_USE

; ******************************************************************************
; * Service Definitions (remove all services for inetd mode)                   *
; ******************************************************************************

; Example SSL server mode services

;[pop3s]
;accept  = 995
;connect = 110

;[imaps]
;accept  = 993
;connect = 143

;[ssmtp]
;accept  = 465
;connect = 25

; Example SSL client mode services

;[gmail-pop3]
;client = yes
;accept = 127.0.0.1:110
;connect = pop.gmail.com:995

;[gmail-imap]
;client = yes
;accept = 127.0.0.1:143
;connect = imap.gmail.com:993

[gmail-smtp]
client = yes
accept = 127.0.0.1:25
connect = smtp.gmail.com:465

; Example SSL front-end to a web server

;[https]
;accept  = 443
;connect = 80
; "TIMEOUTclose = 0" is a workaround for a design flaw in Microsoft SSL
; It does not use SSL close-notify alert designed to prevent truncation attacks
;TIMEOUTclose = 0

; vim:ft=dosini
```

Hi ha un fitxer de mostra a `/usr/share/doc/stunnel4/examples/stunnel.conf-sample`
El podem copiar a `/etc/stunnel/stunnel.conf` i després editar-lo amb les següents instruccions. Es necessiten permisos de super-usuari per a poder escriure al directori `/etc`

```
usr@host:~$ sudo cp /usr/share/doc/stunnel4/examples/stunnel.conf-
sample /etc/stunnel/stunnel.conf

usr@host:~$ sudo nano /etc/stunnel/stunnel.conf
```

Es pot utilitzar l' editor que es vulgui. Nano, VI ...
Les línies marcades en negreta són les que utilitzarem per definir:

- El nom i la ubicació del certificat SSL: cert = /etc/stunnel/mail.pem
- L'adreça del servidor smtp (localhost) i el port on ens connectarem: accept = 127.0.0.1:25

S'ha definit que ens comunicarem a través del port `25`, però es podria utilitzar algun altre si aquest ja està ocupat, per exemple el `465`, que és el que utilitza el servidor `smtp.gmail.com` de google.

Ara hem de crear el certificat SSL.
Crearem un fitxer amb la clau, un segon amb el certificat i els unirem en el fitxer que s'ha definit en la configuració anterior.
Per fer-ho utilitzarem `openssl`

Creació de la clau privada `key.pem`

```
usr@host:~$ openssl genrsa -out key.pem 2048

Generating RSA private key, 2048 bit long modulus
...
```

Creació del certificat `certificat.pem`, a partir de la clau privada. Caldrà omplir informació per generar el certificat.

```
usr@host:~$ openssl req -new -x509 -key key.pem -out certificat.pem
-days 1095

You are about to be asked to enter information ...
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:BCN
Locality Name (eg, city) []:BCN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EUSS
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:EUSS.ES
Email Address []:
```

Creació del certificat SSL `mail.pem`, concatenant els dos fitxers de clau privada i del certificat generat. I després posant-lo a la ubicació correcta.

```
usr@host:~$ cat key.pem certificat.pem > mail.pem
usr@host:~$ sudo cp mail.pem /etc/stunnel/
```

Ara cal arrancar el procés amb aquestes dues passes:

- modificar el fitxer `/etc/default/stunnel4` per tal que `ENABLED=1`

```
usr@host:~$ sudo nano /etc/default/stunnel4
```

- Arrancar Stunnel

```
usr@host:~$ sudo /etc/init.d/stunnel4 start
Starting SSL tunnels: [Started: /etc/stunnel/stunnel.conf]
stunnel.
```

O rearrancar Stunnel

```
usr@host:~$ sudo /etc/init.d/stunnel4 restart
```

Es pot verificar l'estat de les comunicacions amb `netstat`

```
usr@host:~$ netstat -apn |less
```

Codificar les dades d'accés en base64.

Ara ens podrem comunicar a través d'`Stunnel` de forma segura, però el servidor ens demanarà l'usuari i el password encriptats en base 64.

Els podem generar amb les següents instruccions. (és un exemple no real)

```
usr@host:~$ echo usuari@gmail.com |base64
dXN1YXJpQGdtYWlsLmNvbQo=
usr@host:~$ echo Password03gmail |base64
UGFzc3dvcmQwM2dtYWlsCg==
```

Procés complert per a poder enviar el mail a través de gmail via TELNET.

Ho farem de la mateixa manera que en el primer exemple del correu de l'EUSS, però amb unes petites diferències que hem marcat en negreta.

La connexió es fa a `localhost` al port que hem indicat al fitxer de configuració `/etc/stunnel/ stunnel.conf`, no directament a `gmail`.

Observeu com el servidor que contesta és `smtp.gmail.com`, aquest cas ho fa al port `465`, tal com està establert en el fitxer de configuració de l'`Stunnel`. `/etc/stunnel/stunnel.conf`

En lloc del `HELO` s'utilitza `EHLO` que ens dóna la informació de les característiques del servidor.

`AUTH LOGIN`, és l'ordre per a fer la identificació de l'usuari, el servidor ens contesta `334 VXNlcm5hbWU6` que vol dir `User:` codificat en base 64, just després s'ha de posar el e-mail de `gmail` codificat en base 64.

Si és correcte el servidor ens demanarà el password en base 64 amb el missatge: `334 UGFzc3dvcmQ6` també en base 64, `Password:`

```
usr@host:~$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Serv: 220 smtp.gmail.com ESMTP an7sm14045712wjc.44 - gsmtp
Cl:   ehlo localhost
Serv: 250-smtp.gmail.com at your service, [84.88.55.80]
Serv: 250-SIZE 35882577
Serv: 250-8BITMIME
Serv: 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
Serv: 250-ENHANCEDSTATUSCODES
Serv: 250-PIPELINING
Serv: 250-CHUNKING
Serv: 250 SMTPUTF8
```

```
Cl:   auth login
Serv: 334 VXNlcm5hbWU6
Cl:   dXN1YXJpQGdtYWlsLmNvbQo=
Serv: 334 UGFzc3dvcmQ6
Cl:   UGFzc3dvcmQwM2dtYWlsCg==
Serv: 235 2.7.0 Accepted
Cl:   mail from: <user@euss.es>
Serv: 250 2.1.0 OK an7sm14045712wjc.44 - gsmtp
Cl:   rcpt to: <user@gmail.com>
Serv: 250 2.1.5 OK an7sm14045712wjc.44 - gsmtp
Cl:   data
Serv: 354  Go ahead an7sm14045712wjc.44 - gsmtp
Cl:   Subject: exemple de comunicació a través de gmail
      Cco: user@euss.es
      Hola de nou,
      Aquest missatge funciona a través del servidor de google.

      adeu
      Salva
      .
Serv: 250 2.0.0 OK 1447329502 an7sm14045712wjc.44 - gsmtp
Cl:   Quit
```

Finalment, les adreces del correu han d'anar entre els símbols: <>