Dovecot SSL Configuration

Serge Y. Stroobandt

> **This document is still under construction.**

Server account testing

```
$ sudo doveadm log errors

$ tail /var/log/mail.err

$ sudo doveadm user serge
    field    value
    uid      1000
    gid      1000
    home    /home/serge
    mail    maildir:~/Mail
    system_groups_user    serge

$ sudo doveadm auth test serge
```

DH parameters

Diffie-Hellman parameters

```
$ sudo doveadm log errors
    Oct 09 15:00:02 Warning: config: please set ssl_dh=</etc/dovecot/dh.pem
    Oct 09 15:00:02 Warning: config: You can generate it with: dd
if=/var/lib/dovecot/ssl-parameters.dat bs=1 skip=88 | openssl dhparam
-inform der > /etc/dovecot/dh.pem

$ cd /usr/share/dovecot/

$ sudo su
root@c2550:/home/etc/dovecot/dovecot.current# dd if=/var/lib/dovecot/ssl-
parameters.dat bs=1 skip=88 | openssl dhparam -inform der >
/etc/dovecot/dh.pem
    272+0 records in
    272+0 records out
    272 bytes copied, 0.00161711 s, 168 kB/s
root@c2550:/home/etc/dovecot/dovecot.current# exit
    exit
```

SSL certificate creation

```
$ cd /etc/dovecot/ssl/

$ sudo rm *

$ cd /usr/share/dovecot/

$ sudo vim dovecot-openssl.cnf

$ sudo vim mkcert.sh

    $OPENSSL req -new -x509 -nodes -config $OPENSSLCONFIG -out $CERTFILE
-keyout $KEYFILE -days 3650 || exit 2

$ sudo ./mkcert.sh
```

HTTPS certificate publishing

```
$ sudo vim /etc/dovecot/conf.d/10-master.conf
```

```
service imap-login {
  inet_listener imap {
    #port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }
  inet_listener https {
    port = 443
    ssl = yes
  }
```

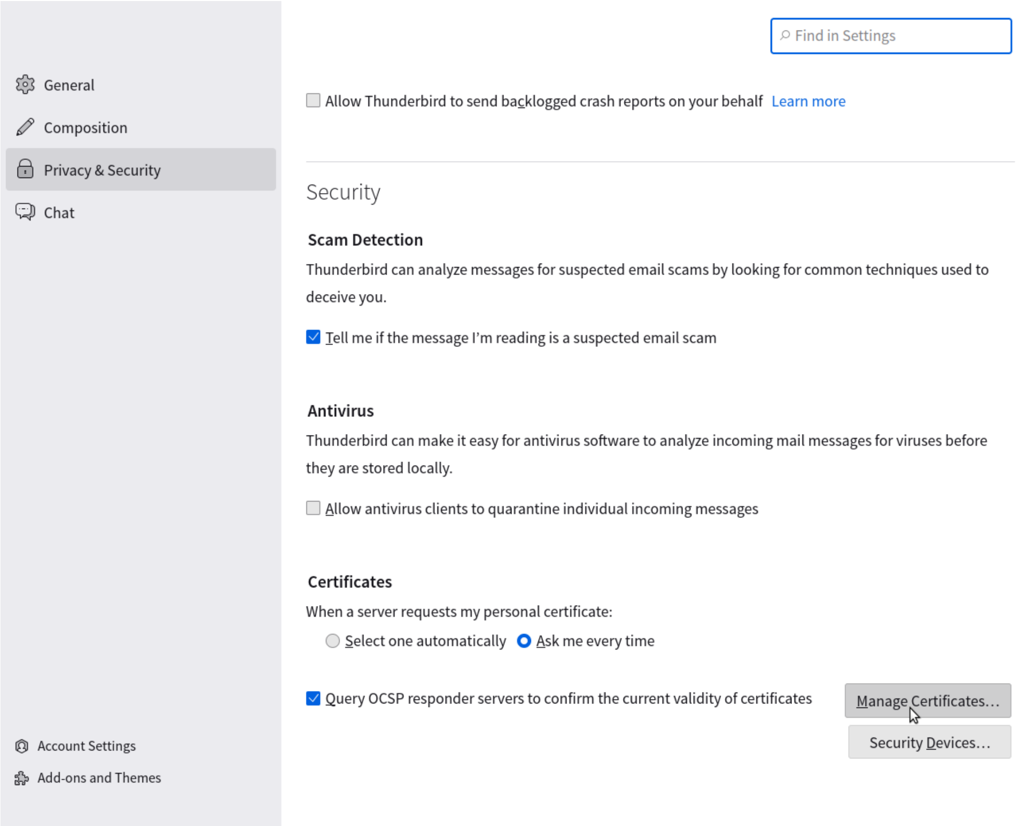
```
$ sudo service dovecot restart
```

Client account testing

```
$ openssl s_client -connect c2550:imaps

$ telnet c2550 imaps
a LOGIN serge <password>
```

Thunderbird



□ Allow Thunderbird to send backlogged crash reports on your behalf

Security

Scam Detection

Thunderbird can analyze messages for suspected email scams by looking for common techniques used to deceive you.

☑ Tell me if the message I'm reading is a suspected email scam

Antivirus

Thunderbird can make it easy for antivirus software to analyze incoming mail messages for viruses before they are stored locally.

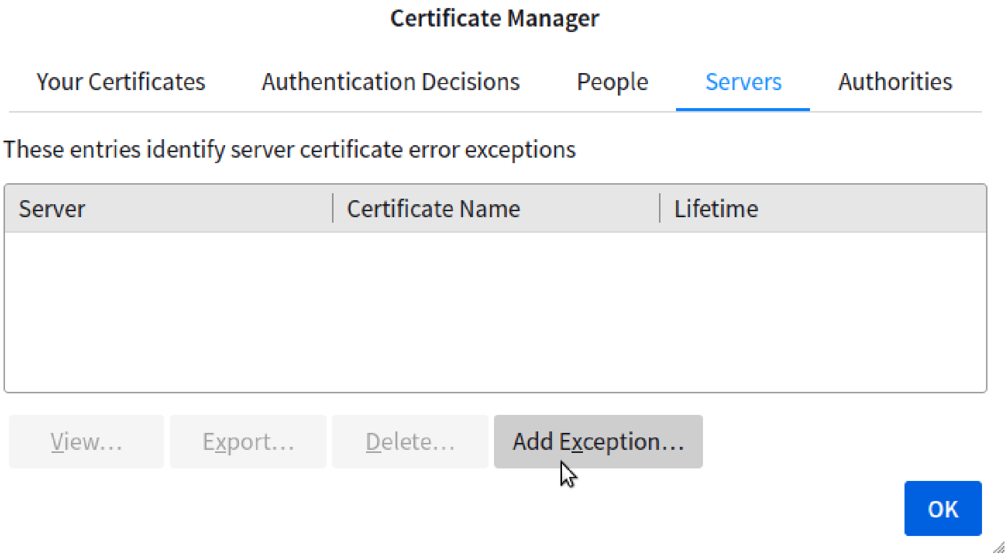
□ Allow antivirus clients to quarantine individual incoming messages

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

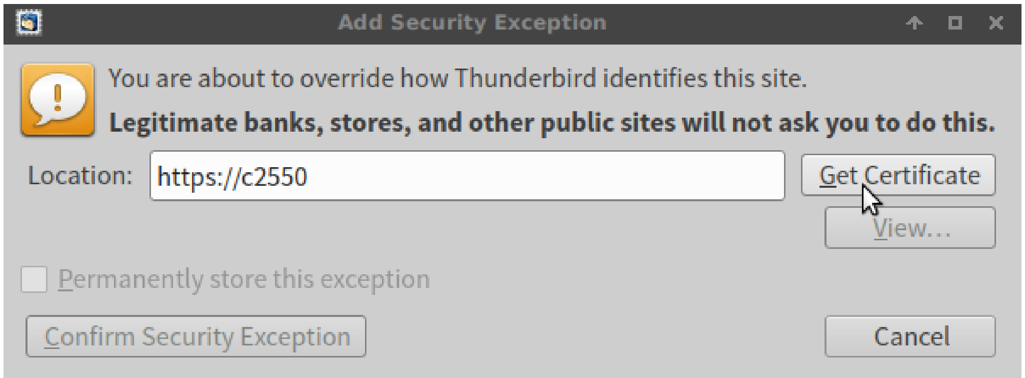
☑ Query OCSP responder servers to confirm the current validity of certificates



Certificate Manager

These entries identify server certificate error exceptions

Server	Certificate Name	Lifetime

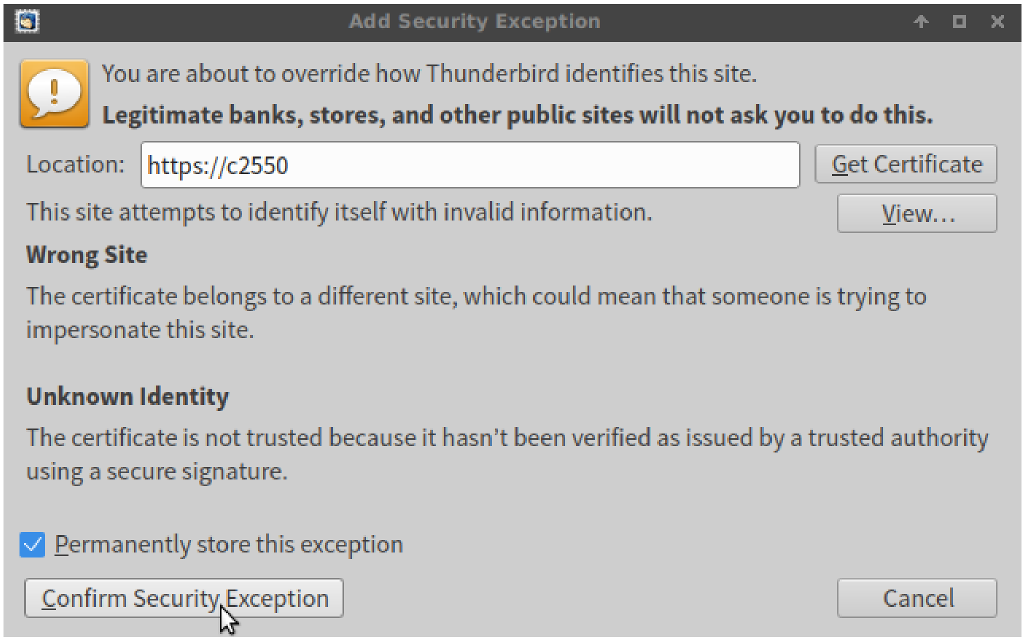


You are about to override how Thunderbird identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://c2550

Get Certificate
View…
□ Permanently store this exception
Confirm Security Exception
Cancel



You are about to override how Thunderbird identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://c2550

This site attempts to identify itself with invalid information.

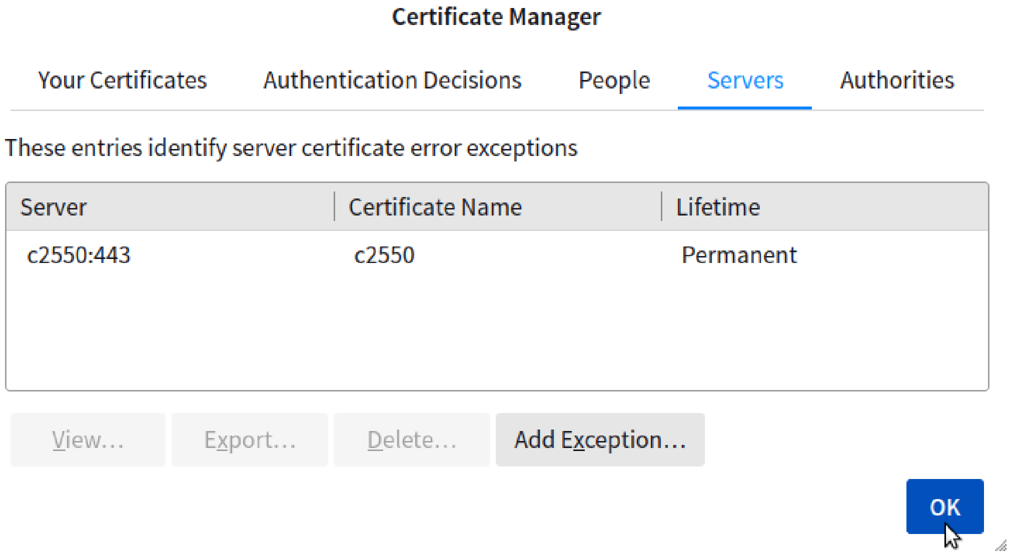
Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

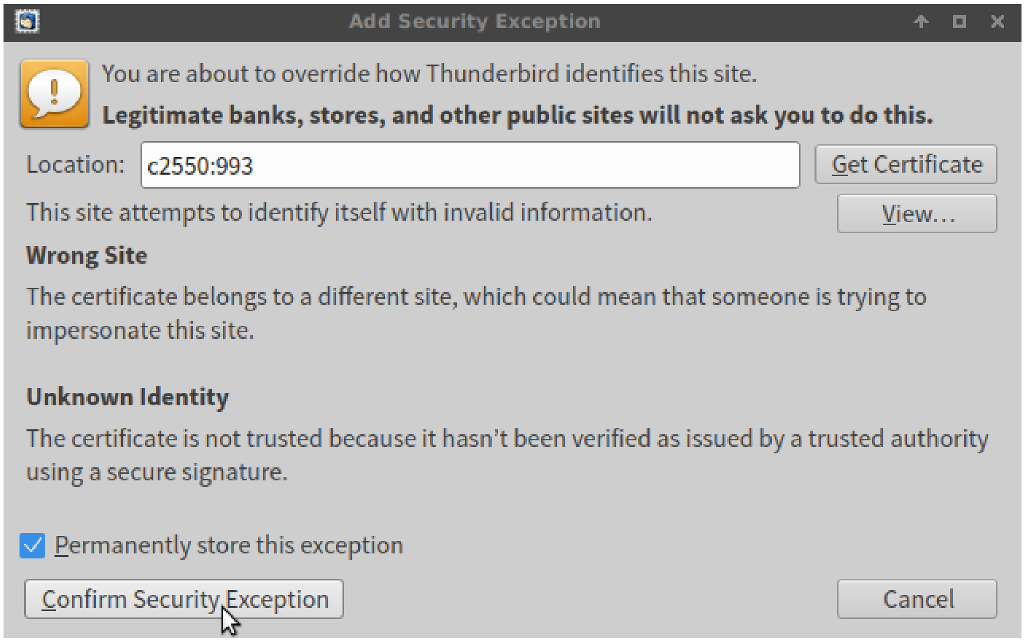
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception



These entries identify server certificate error exceptions

Server	Certificate Name	Lifetime
c2550:443	c2550	Permanent



You are about to override how Thunderbird identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Location: c2550:993

This site attempts to identify itself with invalid information.

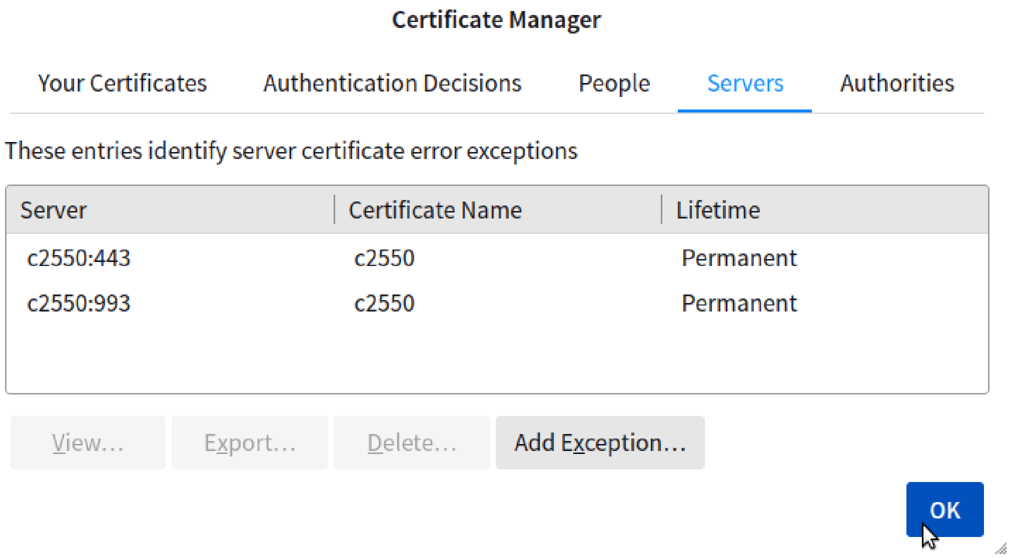
Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception



These entries identify server certificate error exceptions

Server	Certificate Name	Lifetime
c2550:443	c2550	Permanent
c2550:993	c2550	Permanent

```
$ cd ~/.thunderbird/5usajp37.default
$ gvim cert_override.txt
```

Unattended CSS typesetting with Prince.

This work is published at https://hamwaves.com/dovecot.ssl/en/.

Last update: Tuesday, October 11, 2022.