This guide will show you how to easily secure your Zimbra Mail Server with Let’s Encrypt SSL certificate. The default installation of Zimbra generates self-signed SSL certificate for Mails services – POP3/IMAP/SMTP over TLS and for HTTPS access to Zimbra console services.

A self-signed certificate can be used for test deployments but for Production setups I recommend you get a commercial certificate to give your business credibility and better security. If you don’t have a budget for established CA certificate you can use free Let’s Encrypt Certificate to secure your Zimbra server.

Let’s Encrypt is a free, automated, and open certificate authority brought to you by the nonprofit Internet Security Research Group (ISRG). The process of certificate generation is automated and fit for Developers. Before you follow this guide along ensure you have a running Zimbra server. Below guides can help you.

* [Install Zimbra Server on CentOS 8|RHEL 8|Rocky Linux 8](https://computingforgeeks.com/install-zimbra-mail-server-on-centos-rhel/)
* [Install Zimbra Server on Ubuntu](https://computingforgeeks.com/how-to-install-zimbra-collaboration-on-ubuntu/)

Step 1: Install certbot tool

We’ll use the *certbot*tool to request for Let’s Encrypt SSL Certificates. The tools is not installed by default on your system but can easily be downloaded and installed.

*# Ubuntu*

sudo apt update

sudo apt install install snapd

sudo snap install --classic certbot

*# CentOS 8*

sudo yum -y install epel-release

sudo yum -y install certbot

*# CentOS 7*

sudo yum -y install epel-release

sudo yum -y install certbot

Confirm it working.

$ certbot --version

certbot 1.22.0

If you get prompt to install dependencies accept it.

Step 2: Stop Zimbra Proxy Service

We need to stop the *jetty* or *nginx* service services before we can configure it to use Let’s Encrypt SSL certificate.

$ sudo su - zimbra -c "zmproxyctl stop"

Stopping proxy...done.

$ sudo su - zimbra -c "zmmailboxdctl stop"

Stopping mailboxd...done.

Step 3: Obtain Let’s Encrypt SSL Certificate

First confirm if Zimbra zmhostname value is same as hostname --fqdn value.

sudo su - zimbra -c 'source ~/bin/zmshutil; zmsetvars'

sudo su - zimbra -c 'zmhostname'

sudo su - zimbra -c 'hostname --fqdn'

Add CAA record

A Certificate Authority Authorization (CAA) DNS record specifies which certificate authorities (CAs) are allowed to issue certificates for a domain. This record reduces the chance of unauthorized certificate issuance and promotes standardization across your organization.

We should add a record on your root domain with the value “***0 issue “letsencrypt.org***“. In Cloudflare it looks like below.

* Record Type: ***CAA***
* Name: ***your domain***
* Tag: ***Specific domain or wildcard***
* For CA domain name: enter the CA name e.g***letsencrypt.org***

Common values:

*# CAA records added by DigiCert*

0 issue "digicert.com; cansignhttpexchanges=yes"

0 issuewild "digicert.com; cansignhttpexchanges=yes"

*# CAA records added by Sectigo*

0 issue "sectigo.com"

0 issuewild "sectigo.com"

*# CAA records added by Let's Encrypt*

0 issue "letsencrypt.org"

0 issuewild "letsencrypt.org"

*# CAA records added by Google Trust Services*

0 issue "pki.goog; cansignhttpexchanges=yes"

0 issuewild "pki.goog; cansignhttpexchanges=yes"

Validate CAA records using dig command.

*### Debian based systems ###*

sudo apt install -y net-tools dnsutils

dig $(hostname -d) caa +short

*### RHEL based systems ###*

sudo yum -y install bind-utils

dig $(hostname -d) caa +short

Obtain Let’s Encrypt SSL certificates

Once the Zimbra proxy and *mailboxd* services are stopped we can proceed to request for Let’s Encrypt in auto mode. Make sure you pass all the hostnames used by your Mail Server.

export *EMAIL*="admin@computingforgeeks.com"

export ZIMBRA\_FQDN=$(hostname -f)

#export ZIMBRA\_FQDN="**mail.computingforgeeks.com**"

sudo certbot certonly --standalone \

-d $ZIMBRA\_FQDN \

--preferred-chain "ISRG Root X1" \

--force-renewal \

--preferred-challenges http \

--agree-tos \

-n \

-m $EMAIL \

--keep-until-expiring \

--key-type rsa

If you don’t want to provide email use option --register-unsafely-without-email

When you run the commands you’ll see output like below.

Saving debug log to /var/log/letsencrypt/letsencrypt.log

Account registered.

Requesting a certificate for mail.computingforgeeks.com

Successfully received certificate.

Certificate is saved at: /etc/letsencrypt/live/mail.computingforgeeks.net/fullchain.pem

Key is saved at: /etc/letsencrypt/live/mail.computingforgeeks.net/privkey.pem

This certificate expires on 2023-12-03.

These files will be updated when the certificate renews.

Certbot has set up a scheduled task to automatically renew this certificate in the background.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

If you like Certbot, please consider supporting our work by:

\* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate

\* Donating to EFF: https://eff.org/donate-le

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

You can find all your files under **/etc/letsencrypt/live/$ZIMBRA\_FQDN**

$ ls -lh /etc/letsencrypt/live/$ZIMBRA\_FQDN

total 4.0K

lrwxrwxrwx. 1 root root 44 Sep 4 11:31 cert.pem -> ../../archive/mail.computingforgeeks.com/cert1.pem

lrwxrwxrwx. 1 root root 45 Sep 4 11:31 chain.pem -> ../../archive/mail.computingforgeeks.com/chain1.pem

lrwxrwxrwx. 1 root root 49 Sep 4 11:31 fullchain.pem -> ../../archive/mail.computingforgeeks.com/fullchain1.pem

lrwxrwxrwx. 1 root root 47 Sep 4 11:31 privkey.pem -> ../../archive/mail.computingforgeeks.com/privkey1.pem

-rw-r--r--. 1 root root 692 Sep 4 11:31 README

You’ll see a number of files.

* **cert.pem**: The actual certificate file
* **chain.pem**: The chain file
* **fullchain.pem**: Concatenation of cert.pem + chain.pem
* **privkey.pem**: Private key

Step 4: Secure Zimbra with Let’s Encrypt SSL

Create directory that will hold Let’s Encrypt certificates for Zimbra Server.

sudo mkdir /opt/zimbra/ssl/letsencrypt

Copy Certificate files.

CERTPATH=/etc/letsencrypt/live/$ZIMBRA\_FQDN

sudo cp $CERTPATH/\* /opt/zimbra/ssl/letsencrypt/

Confirm files are copied successfully.

$ ls /opt/zimbra/ssl/letsencrypt/

cert.pem chain.pem fullchain.pem privkey.pem README

We now need to build a proper Intermediate CA plus Root CA. You must to use the IdenTrust root Certificate and merge it after the chain.pem.

* <https://letsencrypt.org/certs/isrgrootx1.pem.txt>

Place Let’s Encrypt chain in /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem file.

cat $CERTPATH/chain.pem | sudo tee /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

View the file contents:

cat /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

Combine the *chain.pem* with the root CA – Order is chain **before** the root CA.

wget -O /tmp/ISRG-X1.pem https://letsencrypt.org/certs/isrgrootx1.pem.txt

cat /tmp/ISRG-X1.pem | sudo tee -a /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

Confirm the resulting file has the two certificates.

cat /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

Set correct permissions for the directory:

sudo chown -R zimbra:zimbra /opt/zimbra/ssl/letsencrypt/

Confirm the owner is zimbra user.

$ ls -lha /opt/zimbra/ssl/letsencrypt/

total 32K

drwxr-xr-x. 2 zimbra zimbra 4.0K Jul 6 00:18 .

drwxr-xr-x. 8 zimbra zimbra 4.0K Jul 6 00:13 ..

-rw-r--r--. 1 zimbra zimbra 1.9K Jul 6 00:14 cert.pem

-rw-r--r--. 1 zimbra zimbra 1.7K Jul 6 00:14 chain.pem

-rw-r--r--. 1 zimbra zimbra 3.6K Jul 6 00:14 fullchain.pem

-rw-------. 1 zimbra zimbra 1.7K Jul 6 00:14 privkey.pem

-rw-r--r--. 1 zimbra zimbra 692 Jul 6 00:14 README

-rw-r--r--. 1 zimbra zimbra 2.8K Jul 6 00:23 zimbra\_chain.pem

Verify your commercial certificate.

sudo su - zimbra -c '/opt/zimbra/bin/zmcertmgr verifycrt comm /opt/zimbra/ssl/letsencrypt/privkey.pem /opt/zimbra/ssl/letsencrypt/cert.pem /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

Output should not give any errors or mismatch.

\*\* Verifying '/opt/zimbra/ssl/letsencrypt/cert.pem' against '/opt/zimbra/ssl/letsencrypt/privkey.pem'

Certificate '/opt/zimbra/ssl/letsencrypt/cert.pem' and private key '/opt/zimbra/ssl/letsencrypt/privkey.pem' match.

\*\* Verifying '/opt/zimbra/ssl/letsencrypt/cert.pem' against '/opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

Valid certificate chain: /opt/zimbra/ssl/letsencrypt/cert.pem: OK

Backup current certificate files.

sudo cp -a /opt/zimbra/ssl/zimbra /opt/zimbra/ssl/zimbra.$(date "+%Y.%m.%d-%H.%M")

Copy the private key under Zimbra SSL path.

sudo cp /opt/zimbra/ssl/letsencrypt/privkey.pem /opt/zimbra/ssl/zimbra/commercial/commercial.key

sudo chown zimbra:zimbra /opt/zimbra/ssl/zimbra/commercial/commercial.key

Finally deploy the new Let’s Encrypt SSL certificate.

sudo su - zimbra -c '/opt/zimbra/bin/zmcertmgr deploycrt comm /opt/zimbra/ssl/letsencrypt/cert.pem /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

My certificate deployment output is as shown below.

\*\* Verifying '/opt/zimbra/ssl/letsencrypt/cert.pem' against '/opt/zimbra/ssl/zimbra/commercial/commercial.key'

Certificate '/opt/zimbra/ssl/letsencrypt/cert.pem' and private key '/opt/zimbra/ssl/zimbra/commercial/commercial.key' match.

\*\* Verifying '/opt/zimbra/ssl/letsencrypt/cert.pem' against '/opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

Valid certificate chain: /opt/zimbra/ssl/letsencrypt/cert.pem: OK

\*\* Copying '/opt/zimbra/ssl/letsencrypt/cert.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial.crt'

\*\* Copying '/opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial\_ca.crt'

\*\* Appending ca chain '/opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial.crt'

\*\* Importing cert '/opt/zimbra/ssl/zimbra/commercial/commercial\_ca.crt' as 'zcs-user-commercial\_ca' into cacerts '/opt/zimbra/common/lib/jvm/java/lib/security/cacerts'

\*\* NOTE: restart mailboxd to use the imported certificate.

\*\* Saving config key 'zimbraSSLCertificate' via zmprov modifyServer mail.computingforgeeks.com...ok

\*\* Saving config key 'zimbraSSLPrivateKey' via zmprov modifyServer mail.computingforgeeks.com...ok

\*\* Installing imapd certificate '/opt/zimbra/conf/imapd.crt' and key '/opt/zimbra/conf/imapd.key'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/imapd.crt'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/imapd.key'

\*\* Creating file '/opt/zimbra/ssl/zimbra/jetty.pkcs12'

\*\* Creating keystore '/opt/zimbra/conf/imapd.keystore'

\*\* Installing ldap certificate '/opt/zimbra/conf/slapd.crt' and key '/opt/zimbra/conf/slapd.key'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/slapd.crt'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/slapd.key'

\*\* Creating file '/opt/zimbra/ssl/zimbra/jetty.pkcs12'

\*\* Creating keystore '/opt/zimbra/mailboxd/etc/keystore'

\*\* Installing mta certificate '/opt/zimbra/conf/smtpd.crt' and key '/opt/zimbra/conf/smtpd.key'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/smtpd.crt'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/smtpd.key'

\*\* Installing proxy certificate '/opt/zimbra/conf/nginx.crt' and key '/opt/zimbra/conf/nginx.key'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/nginx.crt'

\*\* Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/nginx.key'

\*\* NOTE: restart services to use the new certificates.

\*\* Cleaning up 3 files from '/opt/zimbra/conf/ca'

\*\* Removing /opt/zimbra/conf/ca/ca.key

\*\* Removing /opt/zimbra/conf/ca/ca.pem

\*\* Removing /opt/zimbra/conf/ca/99384721.0

\*\* Copying CA to /opt/zimbra/conf/ca

\*\* Copying '/opt/zimbra/ssl/zimbra/ca/ca.key' to '/opt/zimbra/conf/ca/ca.key'

\*\* Copying '/opt/zimbra/ssl/zimbra/ca/ca.pem' to '/opt/zimbra/conf/ca/ca.pem'

\*\* Creating CA hash symlink '99384721.0' -> 'ca.pem'

\*\* Creating /opt/zimbra/conf/ca/commercial\_ca\_1.crt

\*\* Creating CA hash symlink '8d33f237.0' -> 'commercial\_ca\_1.crt'

\*\* Creating /opt/zimbra/conf/ca/commercial\_ca\_2.crt

\*\* Creating CA hash symlink '4042bcee.0' -> 'commercial\_ca\_2.crt'

Restart Zimbra services

$sudo su - zimbra -c "zmcontrol restart"

Host mail.computingforgeeks.com

Stopping zmconfigd...Done.

Stopping zimlet webapp...Done.

Stopping zimbraAdmin webapp...Done.

Stopping zimbra webapp...Done.

Stopping service webapp...Done.

Stopping stats...Done.

Stopping mta...Done.

Stopping spell...Done.

Stopping snmp...Done.

Stopping cbpolicyd...Done.

Stopping archiving...Done.

Stopping opendkim...Done.

Stopping amavis...Done.

Stopping antivirus...Done.

Stopping antispam...Done.

Stopping proxy...Done.

Stopping memcached...Done.

Stopping mailbox...Done.

Stopping logger...Done.

Stopping dnscache...Done.

Stopping ldap...Done.

Host mail.computingforgeeks.com

Starting ldap...Done.

Starting zmconfigd...Done.

Starting dnscache...Done.

Starting logger...Done.

Starting mailbox...Done.

Starting memcached...Done.

Starting proxy...Done.

Starting amavis...Done.

Starting antispam...Done.

Starting antivirus...Done.

Starting opendkim...Done.

Starting snmp...Done.

Starting spell...Done.

Starting mta...Done.

Starting stats...Done.

Starting service webapp...Done.

Starting zimbra webapp...Done.

Starting zimbraAdmin webapp...Done.

Starting zimlet webapp...Done.

Step 5: Test Let’s Encrypt SSL on Zimbra

Open the Admin or webmail console of Zimbra collaboration server and check certificate details.

You now have Let’s Encrypt SSL certificate working on your Zimbra Server.

Step 6: Renewing Certificates

To simplify renewal let’s create renewal script.

sudo vim /usr/local/sbin/zimbra\_letsencrypt\_renew

Paste below contents into the file.

#!/bin/bash

export ZIMBRA\_FQDN=$(hostname -f)

#export ZIMBRA\_FQDN="mail.example.com"

#export EMAIL="admin@example.com"

# certbot certonly --standalone \

# -d $ZIMBRA\_FQDN \

# --preferred-chain "ISRG Root X1" \

# --force-renewal \

# --preferred-challenges http \

# --agree-tos \

# --register-unsafely-without-email \

# -n \

# -m $EMAIL \

# --keep-until-expiring \

# --key-type rsa

# Let's Encrypt Certificates Path

CERTPATH=/etc/letsencrypt/live/$ZIMBRA\_FQDN

# Copy certs and key files to zimbra directory

cp -f $CERTPATH/\* /opt/zimbra/ssl/letsencrypt/

# Combine the chain.pem with the root CA - Order is chain before the root CA

cat $CERTPATH/chain.pem | tee /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

wget -O /tmp/ISRG-X1.pem https://letsencrypt.org/certs/isrgrootx1.pem.txt

cat /tmp/ISRG-X1.pem | tee -a /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem

# Set permissions to zimbra user

chown -R zimbra:zimbra /opt/zimbra/ssl/letsencrypt/

# Stop Zimbra services

su - zimbra -c 'zmcontrol stop'

# Verify certificates

su - zimbra -c '/opt/zimbra/bin/zmcertmgr verifycrt comm /opt/zimbra/ssl/letsencrypt/privkey.pem /opt/zimbra/ssl/letsencrypt/cert.pem /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

# Backup current used zimbra certificates

cp -a /opt/zimbra/ssl/zimbra /opt/zimbra/ssl/zimbra.$(date "+%Y.%m.%d-%H.%M")

# Copy let's encrypt key to Zimbra commercial key file

cp /opt/zimbra/ssl/letsencrypt/privkey.pem /opt/zimbra/ssl/zimbra/commercial/commercial.key

chown zimbra:zimbra /opt/zimbra/ssl/zimbra/commercial/commercial.key

# Deploy Let's Encrypt SSL certificates

su - zimbra -c '/opt/zimbra/bin/zmcertmgr deploycrt comm /opt/zimbra/ssl/letsencrypt/cert.pem /opt/zimbra/ssl/letsencrypt/zimbra\_chain.pem'

# Restart Zimbra services

su - zimbra -c "zmcontrol restart"

Make the script executable.

sudo chmod +x /usr/local/sbin/zimbra\_letsencrypt\_renew

Create cron job to renew Let’s Encrypt certificates with --renew-hook set to execute our script.

$ sudo crontab -e

15 3 \* \* \* /usr/bin/certbot renew --quiet --renew-hook "/usr/local/sbin/zimbra\_letsencrypt\_renew"

We hope this article was helpful. Enjoy using Zimbra to power your collaboration needs.