# StartEncrypt Guide

| | | | |
|---|---|---|---|
| **File No.** | | **Control No.** | |
| **Version** | 3.0 | **Security**<br>**Classification** | Interior<br>Publication |
| **Total Page** | | **Appendix** | 0 |

**Author**: ___________ **Date**: 2016-6-2

**Approve**: ___________ **Date**: ____________

**Audit**: ___________ **Date**: ____________

# Linux StartEncrypt

## 1. Introduction

Linux startEncrypt is a Linux application that can automatically manage the process of SSL applying and SSL installation. It supports APACHE, NGINX, TOMCAT webserver. There are two modes of UI for you to run it. Under the Lite mode, the app will automatically read configuration files to obtain the domain of the website, call the background program to carry out the WebSite Domain Validation and apply for a SSL certificate, and install the certificate. While under the Pro mode, users will need to register from our website and obtain a login certificate and a token value. After you finish some configurations, you can start domain validation and automatically apply and install a certificate. Lite mode only works for DV SSL but Pro mode supports DV/OV/IV/EV. Pro version supports two ways to validate a domain. One is to validate the domain in user’s account, the other is to use the app to do the automatic domain validation.

## 2. Installation

1. Copy the tar file to your work catalog

   Reference Command: tar –zxvf filename
2. Perform the install script ./install
3. Get into the /usr/local/StartEncrypt/conf to configure files
4. Get into the /usr/local/StartEncrypt/bin and execute the order ./StartEncrypt under the root permission
5. Back up the runlog into /usr/local/StartEncrypt/log

## 3. Introduction of the configuration files

There are altogether two configuration files stored in the /usr/local/StartEncrypt/conf, which are SERunInfo.xml and StartEncrypt.xml. Under lite mode, it only requires to configure the port that the certificate is listened.

In Pro mode, you need to configure the path and password for the token_ID and the clientCertificate from our website.

**StartEncrypt.xml:**

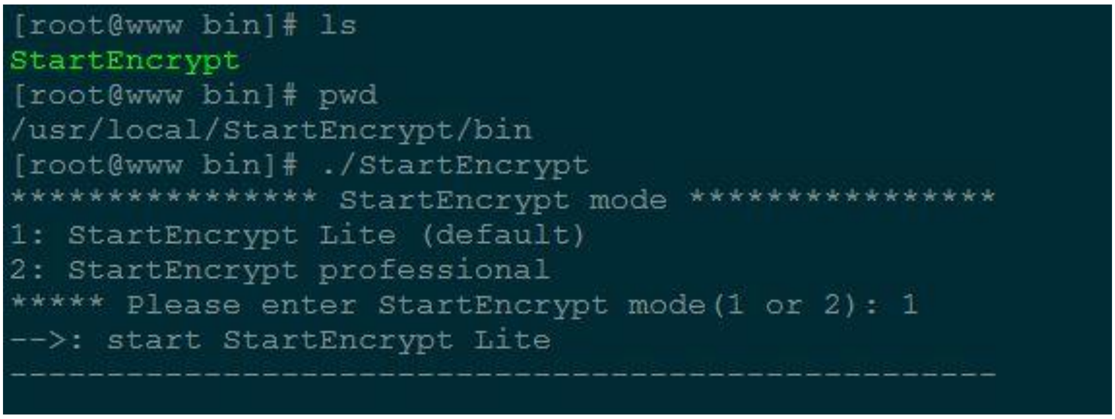
```
<?xml version="1.4" encoding="utf-8"?>
<config>
<professional_config> --Configuration required under Pro mode
        <token_ID ID = "tk_bca7eaf7743941a1a0e5e538e530f445"/> ----User’s token
        <clientCertificate path = "/home/app/app/StartEncrypt/test..p12" password = "password123"/> ----The path to store
the certificate
 </professional_config>
 <customization>
        <!-- 0:auto conf, 1:conf --> --Whether or not to obtain the path automatically，0 is automatically，1 is manually. The
default value is 0
        <confPath conf = "0"/>
        <apacheConfPath path = "/usr/local/apache2"/> --Configure the path for apache manually
        <nginxConPath path = "/usr/local/nginx"/>-- Configure the path for Nginx manually
        <tomcatConPath path = "/usr/local/tomcat"/>-- Configure the path for Tomcat manually
 </customization>
</config>
```

## 4. Detailed instructions and examples

### I. Operation process under Lite mode:

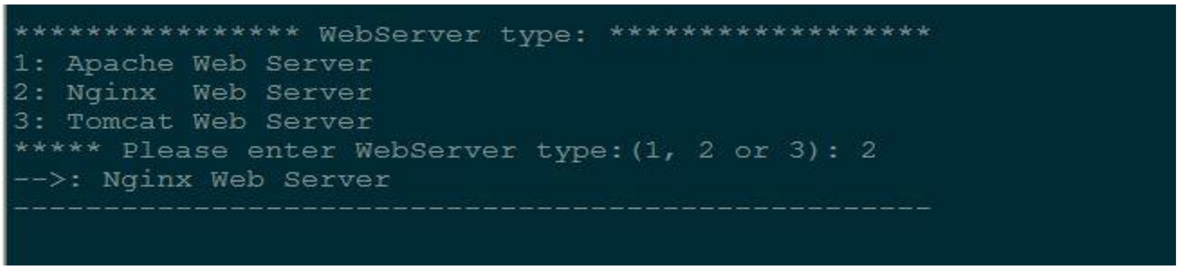
1) **Get into the running catalog，open StartEncrypt**

2) **Select the lite mode（Enter the correspondent number:1）**



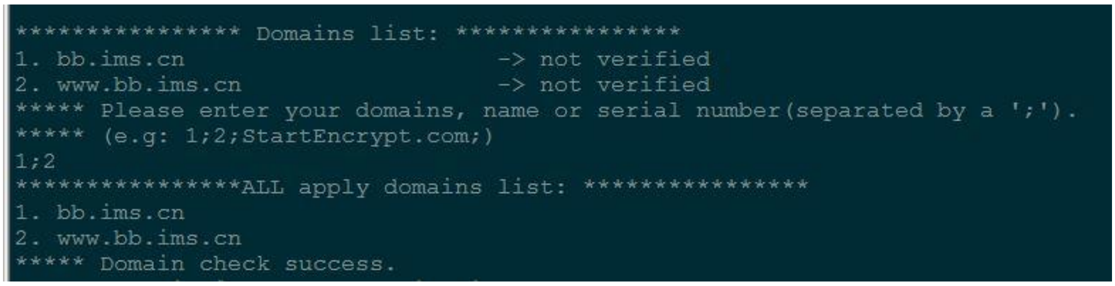
```
[root@www bin]# ls
StartEncrypt
[root@www bin]# pwd
/usr/local/StartEncrypt/bin
[root@www bin]# ./StartEncrypt
**************** StartEncrypt mode ****************
1: StartEncrypt Lite (default)
2: StartEncrypt professional
***** Please enter StartEncrypt mode(1 or 2): 1
-->: start StartEncrypt Lite
---------------------------------------------------
```

3) **Select the web server type（Enter a correspondent number）**



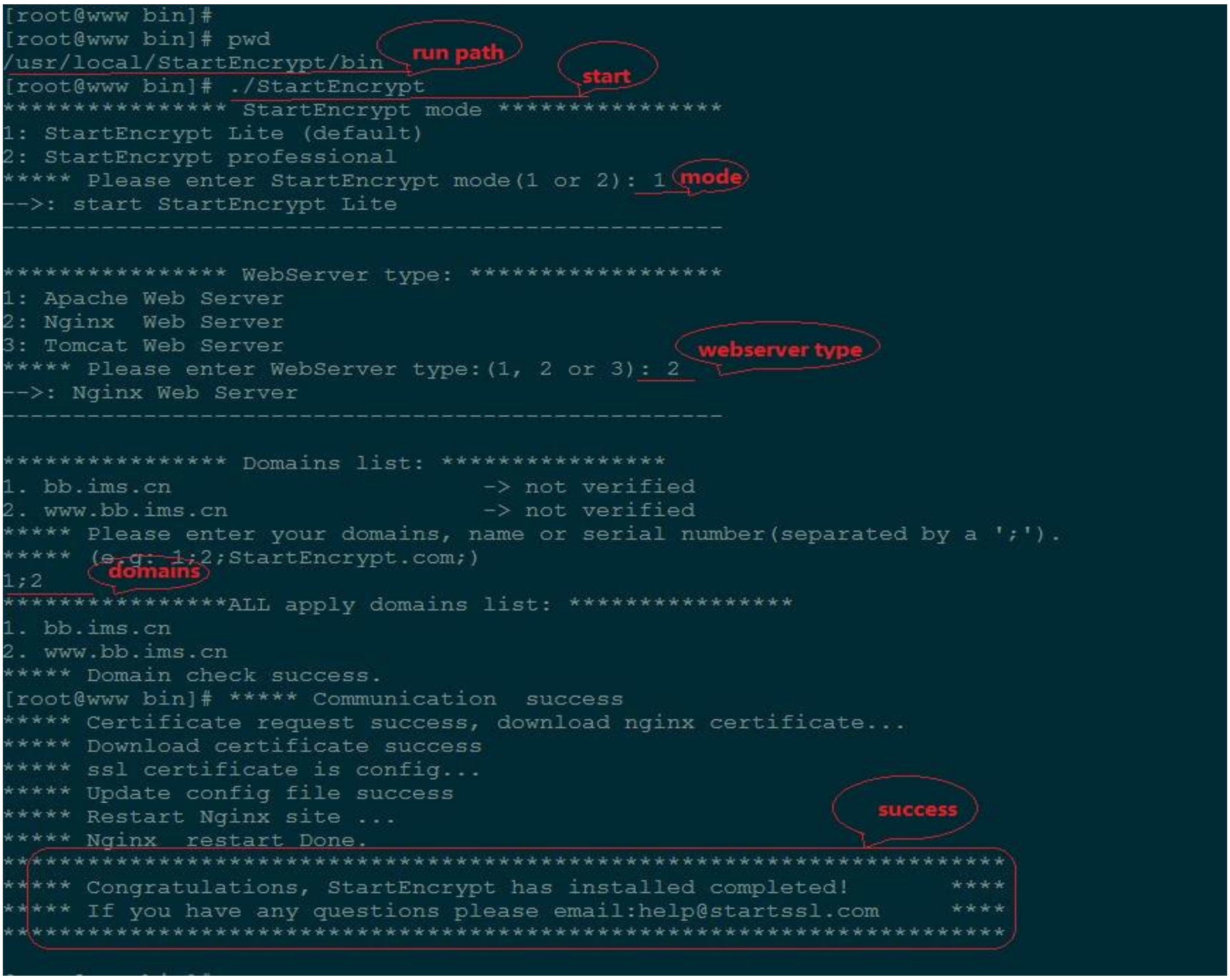
```
**************** WebServer type: ******************
1: Apache Web Server
2: Nginx  Web Server
3: Tomcat Web Server
***** Please enter WebServer type:(1, 2 or 3): 2
-->: Nginx Web Server
---------------------------------------------------
```

4) **Enter your domain, if it’s in the list above, you can enter the corresponding number instead. Use “;”to separate multiple domains.**



```
**************** Domains list: ****************
1. bb.ims.cn                      -> not verified
2. www.bb.ims.cn                  -> not verified
***** Please enter your domains, name or serial number(separated by a ';').
***** (e.g: 1;2;StartEncrypt.com;)
1;2
****************ALL apply domains list: ****************
1. bb.ims.cn
2. www.bb.ims.cn
***** Domain check success.
```

**5）Then StartEncrypt will complete the applying and installation process of a certificate. Screenshots for the complete process are shown below：**



```
[root@www bin]#
[root@www bin]# pwd
/usr/local/StartEncrypt/bin
[root@www bin]# ./StartEncrypt
**************** StartEncrypt mode ****************
1: StartEncrypt Lite (default)
2: StartEncrypt professional
***** Please enter StartEncrypt mode(1 or 2): 1
-->: start StartEncrypt Lite
---------------------------------------------------

**************** WebServer type: ******************
1: Apache Web Server
2: Nginx  Web Server
3: Tomcat Web Server
***** Please enter WebServer type:(1, 2 or 3): 2
-->: Nginx Web Server
---------------------------------------------------

**************** Domains list: ****************
1. bb.ims.cn                      -> not verified
2. www.bb.ims.cn                  -> not verified
***** Please enter your domains, name or serial number(separated by a ';').
***** (e.g: 1;2;StartEncrypt.com;)
1;2
****************ALL apply domains list: ****************
1. bb.ims.cn
2. www.bb.ims.cn
***** Domain check success.
[root@www bin]# ***** Communication  success
***** Certificate request success, download nginx certificate...
***** Download certificate success
***** ssl certificate is config...
***** Update config file success
***** Restart Nginx site ...
***** Nginx  restart Done.
**********************************************************************
***** Congratulations, StartEncrypt has installed completed!      ****
***** If you have any questions please email:help@startssl.com    ****
**********************************************************************
```

6）**Successfully deployed, you can have a test on your website.**

## II. Operation process under Pro mode：

1）**Complete the information needed for the configuration files**

2）**StartEncrypt Get into the running catalog, open StartEncrypt**

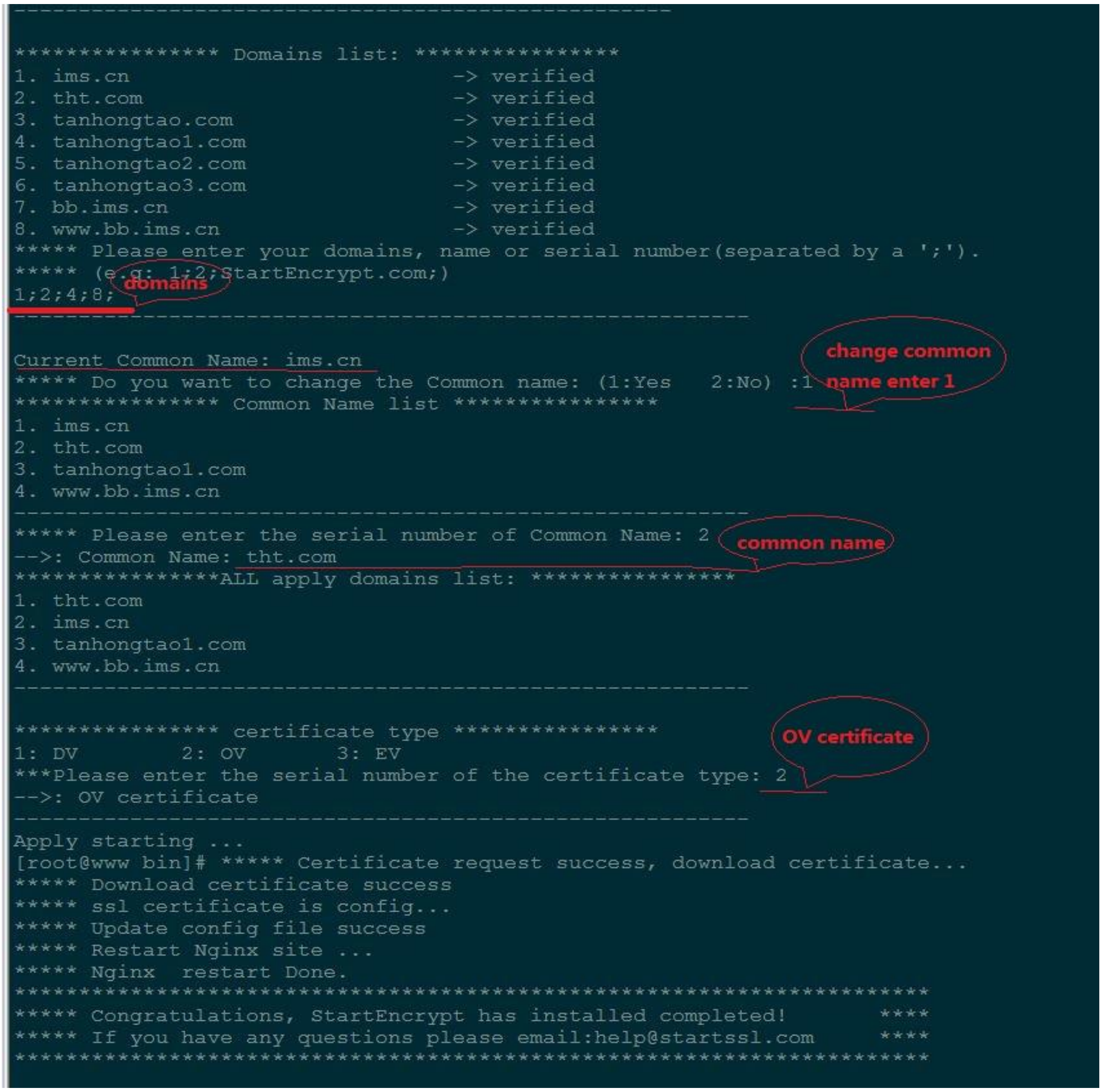
3）**Select the Pro mode (Enter a correspondent number)**

4）**Select a web server type (Enter a correspondent number)**

5) **Enter your domain, if it's in the list above, you can enter the corresponding number instead. Use ";"to separate multiple domains.**

6) **Select whether to change the common name （1: Yes， 2：No）**

7) **Select a corresponding level of certificates that is available to obtain in your account.**



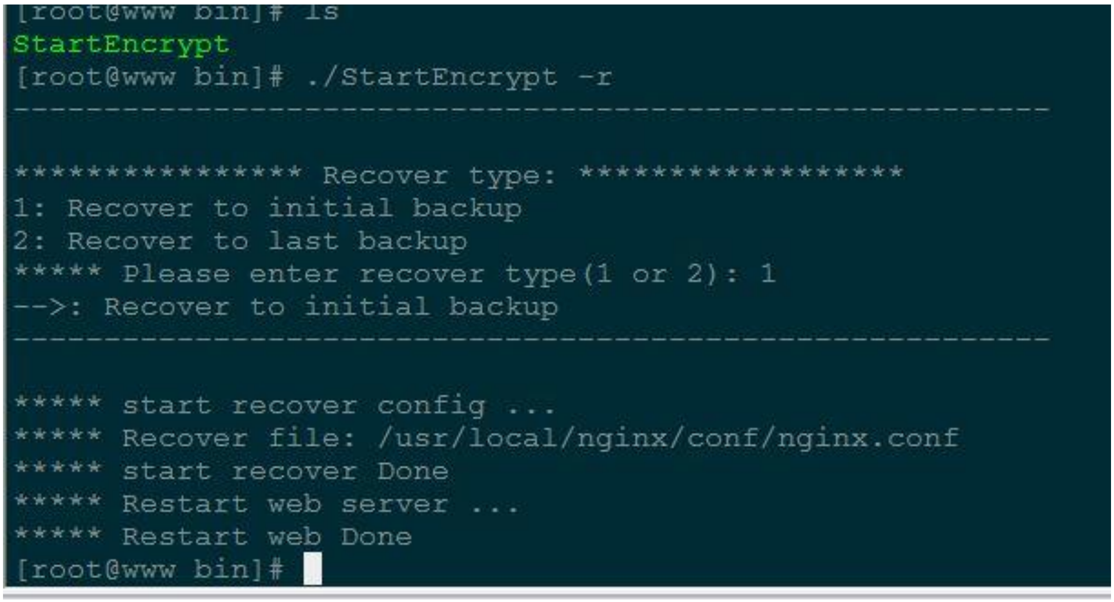
```
---------------------------------------------------

**************** Domains list: ****************
1. ims.cn                        -> verified
2. tht.com                       -> verified
3. tanhongtao.com                -> verified
4. tanhongtao1.com               -> verified
5. tanhongtao2.com               -> verified
6. tanhongtao3.com               -> verified
7. bb.ims.cn                     -> verified
8. www.bb.ims.cn                 -> verified
***** Please enter your domains, name or serial number(separated by a ';').
***** (e.g: 1;2;StartEncrypt.com;)
1;2;4;8;
---------------------------------------------------------

Current Common Name: ims.cn
***** Do you want to change the Common name: (1:Yes   2:No) :1
**************** Common Name list ****************
1. ims.cn
2. tht.com
3. tanhongtao1.com
4. www.bb.ims.cn
---------------------------------------------------------
***** Please enter the serial number of Common Name: 2
-->: Common Name: tht.com
****************ALL apply domains list: ****************
1. tht.com
2. ims.cn
3. tanhongtao1.com
4. www.bb.ims.cn
---------------------------------------------------------

**************** certificate type ****************
1: DV        2: OV        3: EV
***Please enter the serial number of the certificate type: 2
-->: OV certificate
---------------------------------------------------------
Apply starting ...
[root@www bin]# ***** Certificate request success, download certificate...
***** Download certificate success
***** ssl certificate is config...
***** Update config file success
***** Restart Nginx site ...
***** Nginx  restart Done.
***********************************************************************
***** Congratulations, StartEncrypt has installed completed!       ****
***** If you have any questions please email:help@startssl.com     ****
***********************************************************************
```

# File recovering process:

1) **If it turns out that the website cannot be activated, you can follow this to recover the configured files. Open the StartEncrypt with parameter: ./StartEncrypt –r**

2) **Follow the instruction to choose a point to recover the files（1：the original backup， 2.the recent backup）.**

3) **Automatically recover the files and restart.**



```
[root@www bin]# ls
StartEncrypt
[root@www bin]# ./StartEncrypt -r
-----------------------------------------------------------

**************** Recover type: ******************
1: Recover to initial backup
2: Recover to last backup
***** Please enter recover type(1 or 2): 1
-->: Recover to initial backup
-----------------------------------------------------------

***** start recover config ...
***** Recover file: /usr/local/nginx/conf/nginx.conf
***** start recover Done
***** Restart web server ...
***** Restart web Done
[root@www bin]#
```

## 5. Additional instructions

1. Preconditions to utilize the StartEncrypt are： Web server supports SSL, and it was working under http；

2. Configuration files are using a standard path. It can be changed if you want to.

3. StartEncrypt can only work under root permission.