StartEncrypt Guide

<table>
<thead>
<tr>
<th>File No.</th>
<th>Control No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3.0</td>
</tr>
<tr>
<td>Security Classification</td>
<td>Interior Publication</td>
</tr>
<tr>
<td>Total Page</td>
<td>Appendix</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Author: __________  Date: 2016-6-2

Approve: __________  Date: __________

Audit: __________  Date: __________

（All reserved, copy reserved!）
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
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)

   ![Command Prompt](image)

   ```bash
   [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)
4) Enter your domain, if it’s in the list above, you can enter the corresponding number instead. Use 
";" to separate multiple domains.

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

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.
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.