

New Install:

1. Install PostgreSQL Database Server

- Download the database server rpm from postgres.org
- Switch to root user and install postgresql to /usr/local/pgsql
- Create a user named postgres
- Create data directory and define owner.

```
mkdir /usr/local/pgsql/data  
chown postgres /usr/local/pgsql/data
```

- Create environment variable PGDATA.

```
PGDATA=/usr/local/pgsql/data  
export PGDATA
```

Add the above lines to the end of the file /etc/profile.

- Initialize the database cluster and start postgres

```
su postgres  
  
/usr/local/pgsql/bin/initdb -D  
/usr/local/pgsql/data
```

- Adjust SHMMAX, and edit postgres.conf and pg_hba.conf files. Start postgresql:

```
pg_ctl start
```

2. Install Stonylake Firewall Reporter

Download sfr400lnxsetup.tar. Decompress the archive to /opt:

```
tar -zxvf sfr400lnxsetup.tar
```

3. Open SFR Control Center

Run /opt/sfr/jakarta-tomcat-5.5.4/bin/startup.sh

Launch URL <http://localhost:8080/sfr/admin.html> to configure SFR (refer to the chapter titled Configuration in the Stonylake Firewall Reporter User Guide for details). This URL will launch the SFR Control Center. Choose an edition to activate. A 30-day trial license will be created on activation. It can be viewed in the Licensing section of the Control Center.

Note: You can substitute the machine's IP address for *localhost* if you're using a browser on another machine.

4. Database Settings

Choose the database type; provide database user id (postgres) and the password. Click Apply.

5. Reload SFR Control Center

Refresh the browser to reload the SFR Control Center. The default password to access the SFR Control Center is **stonylake**. The SFR Control Center will now show the

default Stonylake Logging Engine (SLE) and Processor (data processor).

6. Processor Settings

Expand the SFR Control Center tree to display the default Stonylake Logging Engine and default Processor. Review Processor settings and change as necessary. Origin IP will be the IP address of the firewall. Click Apply.

7. Assign License

In Processor Settings, click the Assign License button and assign an available license.

8. Start Stonylake Logging Engine

Run /opt/sfr/sle/bin/startup.sh

9. Configure Firewall

Configure your firewall to send its logs via Syslog to the Processor defined in Step 6. The Syslog port (default is UDP 514) will be the same as what the Processor is listening on. For Check Point, refer to the section on configuring Check Point in the Stonylake Firewall Reporter User Guide or the *checkpointconfig.pdf* file.

10. Check Point Users only: start Check Point LEA

Edit the lea.conf file located in the /opt/sfr/lea (default location) folder to suit your environment. Detailed editing instructions are given in the lea.conf file as well as in *checkpoint config.pdf* file.

12. View Reports

Open URL <http://localhost:8080/sfr> or <http://server-ip:8080/sfr> if using a browser on another machine. The default userid to access the reports is **admin** and the password is **stonylake**.

13. Configure Anomaly Detection System (ADS)

Open URL <http://localhost:8080/ads> or <http://server-ip:8080/ads> if using a browser on another machine. Enter the email address to send alerts to, and set up the rules.

14. Start the ADS service

Run /opt/sfr/ads/bin/startup.sh for the monitoring to commence.

Upgrade:

Stop the version 3.x processes including Tomcat. Install the ver 4 software and complete the configuration steps given above. The database will automatically be updated in the background when the version 4 processes start. Uninstall version 3.x once ver 4 is up and running.

Version 4 will require a [new license key](#); contact licensing@stonylakesolutions.com for your key.

System Checks

General

1. Is the database server running?
2. Is the correct database userid and password specified in the SFR Control Center?
4. Is the Stonylake Firewall Reporter database installed?
5. Browser — is either Microsoft VM or Java (Sun) VM installed and enabled.

SFR Control Center (ICC)

1. On Windows, is Tomcat running as a service as well as via startup.bat? Only one instance must run — either as a service or via startup.bat
2. Has an edition been activated —
`http://server_ip:8080/sfr/admin.html`
3. Is the Processor assigned a valid license?
4. Has an Origin IP address been specified?
5. Is the SLE running? On Windows, start it from Windows Services | Stonylake Firewall Reporter (SLE Service) or
`c:\program files\sfr\sle\bin\startup.bat`

Stonylake Logging Engine (SLE)

1. Is the IP address defined for the SFR Control Center in the sle.ini file correct?
2. Has the Stonylake Firewall Reporter (SLE Service) already started in the background and you are trying to start another instance via startup.bat?
3. Is the Stonylake Logging Engine defined in the SFR Control Center?
4. Is another vendor's syslog server running on the machine? Shut it down.

Firewall

1. Stonegate — is the Origin ID defined correctly in the Processor? This is the IP address of the firewall node.
2. Check Point error —“unable to contact the Certificate Authority on the management station, please make sure the certificate authority daemon is running”. To resolve this problem add the following line to fwopsec.conf:

```
lea_server auth_port 0
```

Error Log Files

If you encounter any issues with getting the Stonylake Firewall Reporter to run, there are a few log files you can look at that may provide some information. On Windows these files are located at `c:\program files\sfr\shared\logs`. On Linux these are located at `/opt/sfr/shared/logs`

Common Problems and Solutions

1. On Windows, Tomcat does not start when you run startup.bat
 - Tomcat may have already started as a service. Stop the service and then try running startup.bat
2. SLE does not run — starts and quits because no configuration is available.
 - Verify that the SCC address is correctly specified in the sle.ini. Ensure that Tomcat is running.
3. Check Point LEA is consuming 99% processor power.
 - Probably the LEA service is running in the background and in addition the LEA client is run as a foreground process. Run only one instance.