COMODO
Creating Trust Online®

cWatch

cWatch Web Security

WHM Plugin Installation

Software Version 1.0
Guide Version 1.0.041216

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013
United States

cWatch - WHM Plugin Installation

Installing the Web Hosting Control Panel Plugin

To set up cWatch Web Security, you first need to install the cWatch plugin for WHM on your webserver. This plugin is the component responsible for forwarding logs to your cWatch account. You need a valid cWatch license key to use this product. If you have not done so already, please purchase a cWatch license from https://accounts.comodo.com/capt/management/signup

System Requirements:

1. Supported operating systems:

- Red Hat Enterprise Linux versions 5, 6, and 7
- CentOS versions 6.5 or later
- Cloud Linux versions 5, 6, and 7
- Amazon Linux

2. Web management panels:

- cPanel

3. Web Server

- Apache web server v.2.2, 2.4.2 and upwards

4. ModSecurity version 2.7.5 - 2.9.0 *(will be installed during setup if required)*

- Versions 2.75 – 2.90

5. Rsyslog *(will be installed during setup if required)*

- Version 8.15.0 and above
- TLS support for Rsyslog (package rsyslog-gnutls)
- RELP protocol support for Rsyslog (package rsyslog-relp)

5. Perl, CPAN

To install the cWatch agent

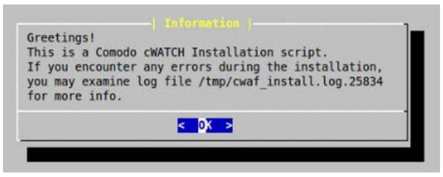
- If you have not yet done so, please purchase a cWatch Web Security license from https://accounts.comodo.com/capt/management/signup
- Make sure you receive your license acknowledgment mail containing your activation key
- Download/get the latest cWatch Agent:

  wget -O cwatch_client_install.sh https://portal.cwatch.comodo.com/cwatch/agent/cwatch_client_install.sh

- Copy the cWatch agent to your hard drive (e.g., to /root/)
- Run the installation script with root privileges:

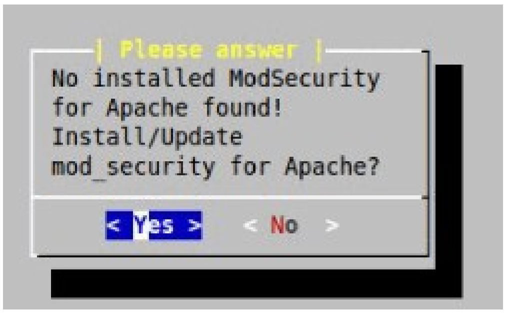
# bash ./cwatch_client_install.sh

First, read the note regarding log file location warning and click 'OK' to proceed.



```
Greetings!
This is a Comodo cWATCH Installation script.
If you encounter any errors during the installation,
you may examine log file /tmp/cwaf_install.log.25834
for more info.
```

The installer will next check whether the latest version of mod_security is installed. If not, you will be prompted to install or update it.

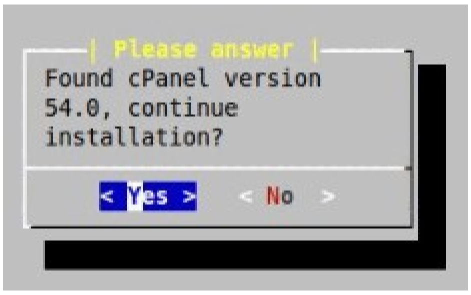


```
No installed ModSecurity
for Apache found!
Install/Update
mod_security for Apache?
```

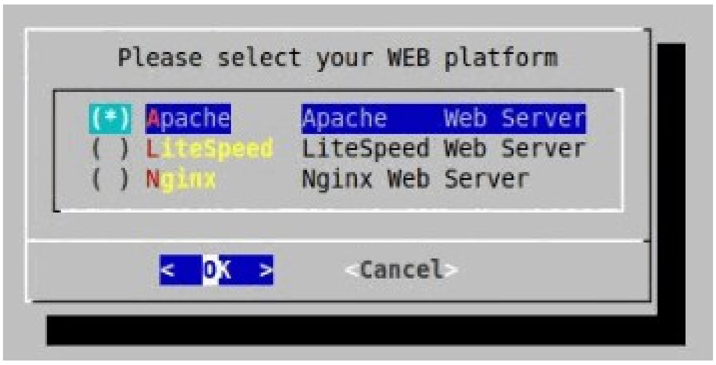
Click 'Yes' to install mod_security. Accept the license terms on the next screen to begin package installation.

The setup wizard will next check for the presence of supported web server types (Apache, Lightspeed or Nginx) and supported control panels (cPanel, DirectAdmin, Webmin, Plesk).

- If no supported control panels are detected then you will be offered the opportunity to install in standalone mode.
- If a supported control panel is detected you will be offered the opportunity to install a cWatch plug-in for that panel. For example, "Found Cpanel version CPANEL_VERSION, continue installation?”
- If more than one web server is detected, you will be asked to choose which one you want to protect.



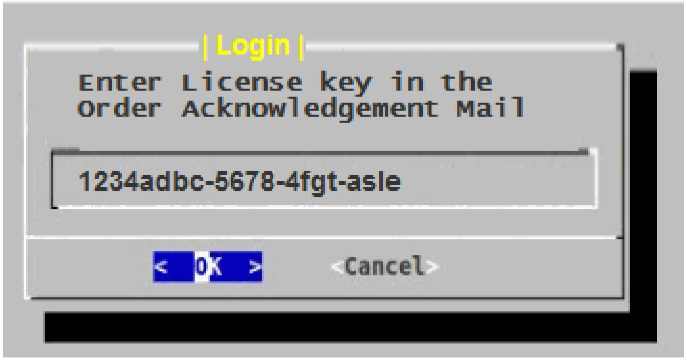
```
Found cPanel version
54.0, continue
installation?
```



```
Please select your WEB platform

(*) Apache       Apache     Web Server
( ) LiteSpeed    LiteSpeed Web Server
( ) Nginx        Nginx Web Server
```

Select 'OK' to continue. Next, enter your cWatch license key as provided in your order confirmation email and select 'OK':

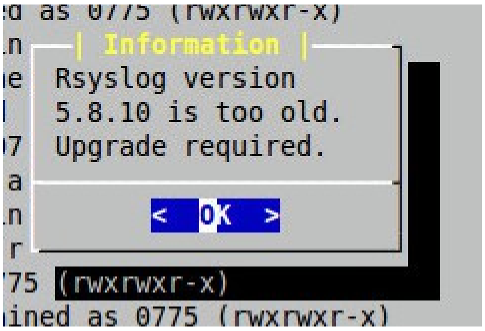


```
Enter License key in the
Order Acknowledgement Mail

1234adbc-5678-4fgt-asle
```

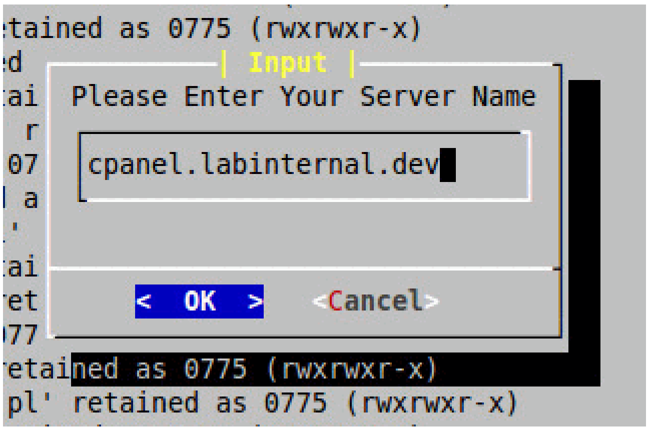
The installer will next check for the presence of Rsyslog.

- If Rsyslog 8.16 is not found then you will be offered the chance to install it.
- Click 'OK' to continue:



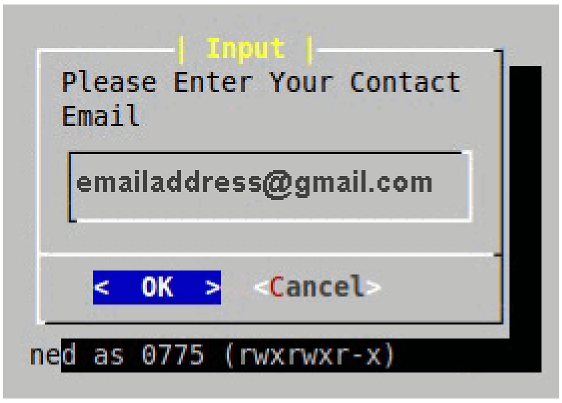
```
ed as 0775 (rwxrwxr-x)
.n ──| Information |──
ie   Rsyslog version
|    5.8.10 is too old.
)7   Upgrade required.
 a
.n         <  OK  >
 r
'75 (rwxrwxr-x)
ined as 0775 (rwxrwxr-x)
```

Enter your server name. The name of the host on which you are installing will be presented by default in this field:



```
tained as 0775 (rwxrwxr-x)
ed ──────────| Input |──────────
ai  Please Enter Your Server Name
 r
07   cpanel.labinternal.dev
| a
'
ai
et       <  OK  >    <Cancel>
)77
etained as 0775 (rwxrwxr-x)
pl' retained as 0775 (rwxrwxr-x)
```

Click 'OK' to continue. Next, enter your contact email address. Comodo will use this email address in future communications with you:



```
 ──────────| Input |──────────
  Please Enter Your Contact
  Email

   emailaddress@gmail.com

      <  OK  >   <Cancel>

ned as 0775 (rwxrwxr-x)
```

Click 'OK' to continue.

The next few screens will ask you to specify the location where the agent should collect logs from. In most cases these will be auto-populated with default locations. If you have different log file locations please configure them accordingly. You will be asked to provide the location of the following logs:

- Linux Audit Logs. Default = */var/log/audit/audit.log*
- Mod Security Audit Logs. Default = */usr/local/apache/logs/modsec_audit.log*
- cPanel Access Logs. Default = */usr/local/cpanel/logs/access_log*

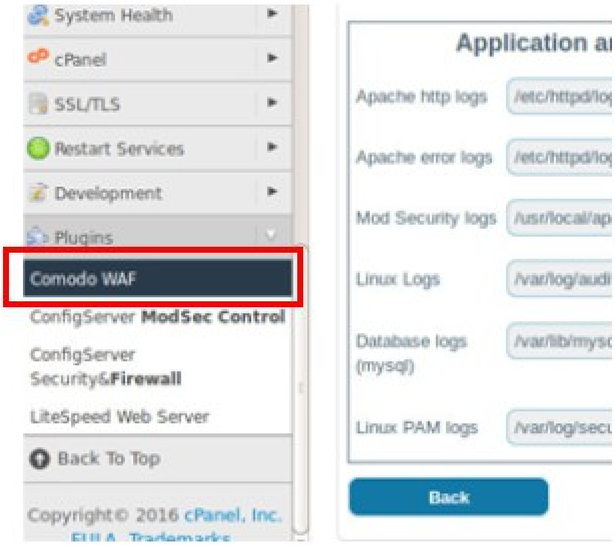
- cPanel Login Logs. Default = */usr/local/cpanel/logs/login_log*

After confirming your log locations, installation will be complete.

To verify agent installation, navigate to the WHM control panel interface. Refer to Configuring CWatch Web Security for more information.

Accessing the cWatch WHM Plugin

- Login to WHM on your server
- Click 'Plugins' > ‘Comodo WAF’:



Apache http logs /etc/httpd/lo

Apache error logs /etc/httpd/lo

Mod Security logs /usr/local/ap

Linux Logs /var/log/audi

Database logs (mysql) /var/lib/mysq

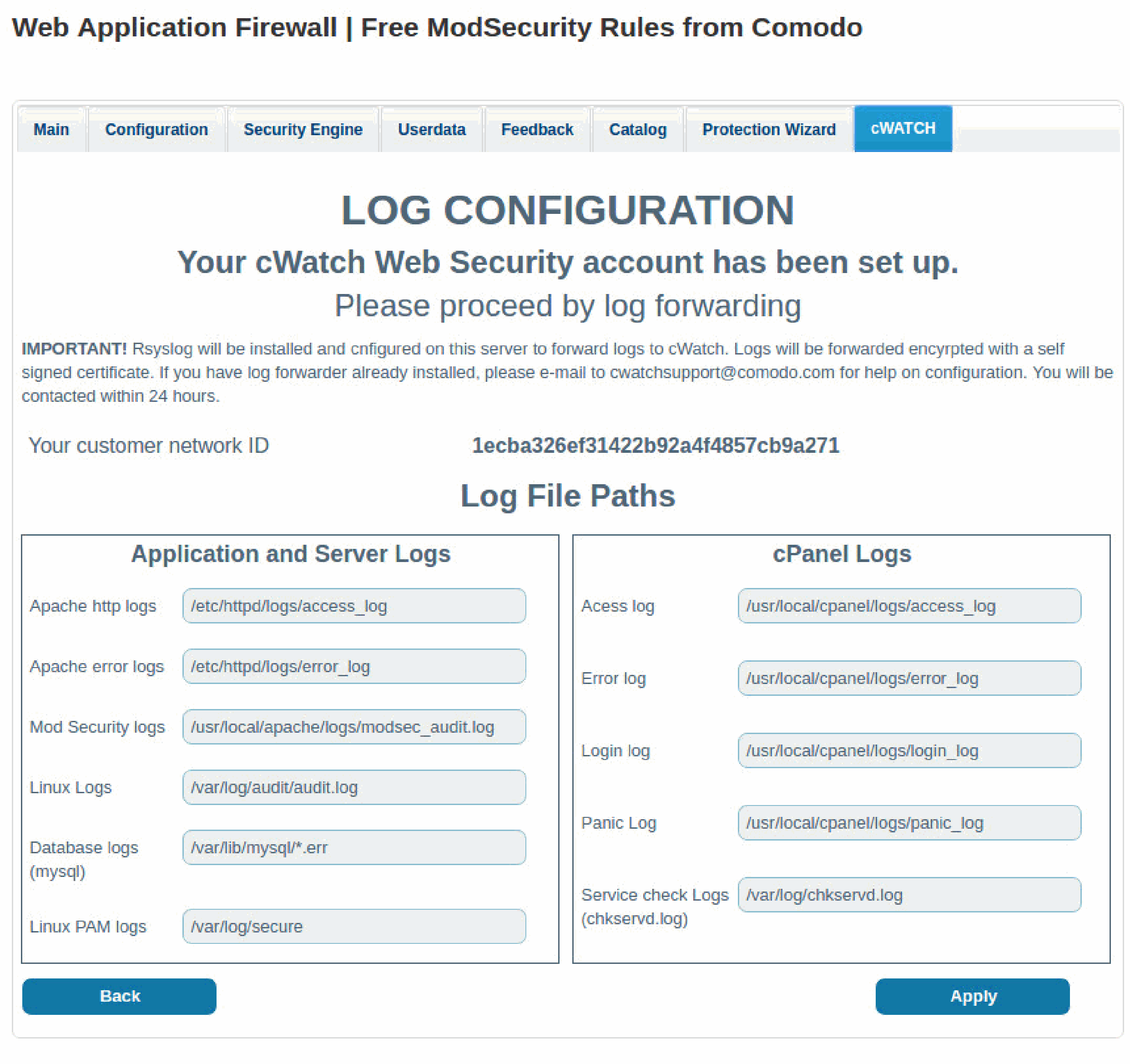
Linux PAM logs /var/log/secu

The interface has eight tabs:

- Main - Displays the versions of the currently loaded rule set, Apache server, Mod-Security status and number of websites protected.
- Configuration – Enables the administrator to manually download the ruleset updates or restore to previous version of rule set.
- Security Engine - Enables the administrator to set up Mod Security rules.
- Userdata - Allows administrators to manage custom user settings such as user rules, Mod_security options, and the parameters of currently loaded rule-sets.
- Feedback – Enables the administrator to submit their feedback such as false positives reported by the currently loaded version of the ruleset.
- Catalog - Allows administrators to specify rules that should be excluded from implementation.
- Protection Wizard – Allows administrators to enable/disable rules depending on the web applications installed on the server, thus helping to reduce server load.
- Cwatch – Allows administrators to purchase, activate and configure cWatch Web Security.

Configuring cWatch Web Security

Click the ‘cWatch’ tab to begin configuration:



Web Application Firewall | Free ModSecurity Rules from Comodo

LOG CONFIGURATION

Your cWatch Web Security account has been set up.

Please proceed by log forwarding

IMPORTANT! Rsyslog will be installed and cnfigured on this server to forward logs to cWatch. Logs will be forwarded encyrpted with a self signed certificate. If you have log forwarder already installed, please e-mail to cwatchsupport@comodo.com for help on configuration. You will be contacted within 24 hours.

Your customer network ID **1ecba326ef31422b92a4f4857cb9a271**

Log File Paths

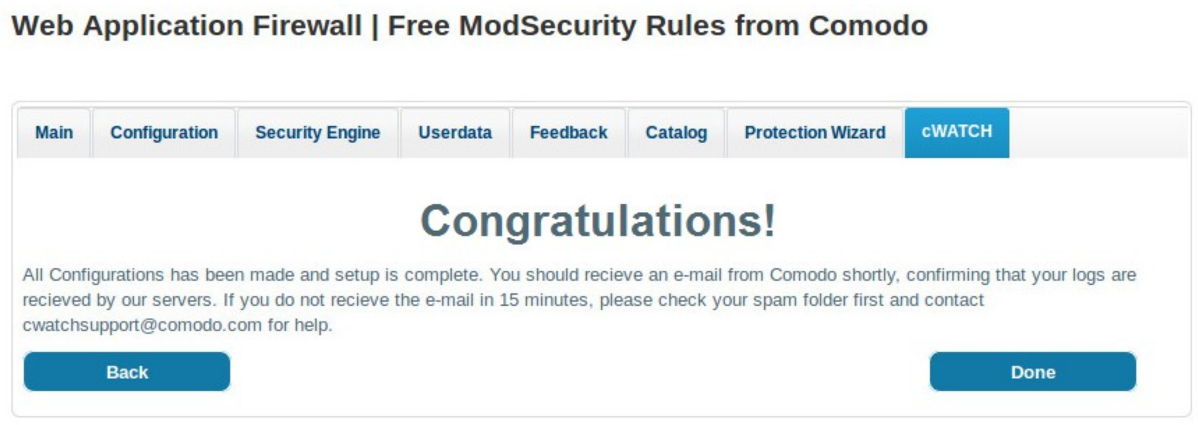
Application and Server Logs

Apache http logs	/etc/httpd/logs/access_log
Apache error logs	/etc/httpd/logs/error_log
Mod Security logs	/usr/local/apache/logs/modsec_audit.log
Linux Logs	/var/log/audit/audit.log
Database logs (mysql)	/var/lib/mysql/*.err
Linux PAM logs	/var/log/secure

cPanel Logs

Acess log	/usr/local/cpanel/logs/access_log
Error log	/usr/local/cpanel/logs/error_log
Login log	/usr/local/cpanel/logs/login_log
Panic Log	/usr/local/cpanel/logs/panic_log
Service check Logs (chkservd.log)	/var/log/chkservd.log

Log locations will be auto-populated from the information entered during installation. If you have different log file locations please configure them accordingly. After configuration is complete, click ‘Finish’. cWatch is now ready to use:



Web Application Firewall | Free ModSecurity Rules from Comodo

Congratulations!

All Configurations has been made and setup is complete. You should recieve an e-mail from Comodo shortly, confirming that your logs are recieved by our servers. If you do not recieve the e-mail in 15 minutes, please check your spam folder first and contact cwatchsupport@comodo.com for help.

Your logs will be forwarded to cWatch Cloud for monitoring, analysis and real time alerts. You should receive a ‘service started’ mail from cWatch support shortly. Please contact support if you do not get this e-mail in 15 minutes.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,
Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit http://www.comodo.com.