

# Instructions for connecting a mod\_security sensor to the Deutsche Telekom AG early warning system

Deutsche Telekom AG

Version 1.2  
Last revised: Apr.04, 2013  
Status Final

Public

Erleben, was verbindet.



## Publication details

---

### Published by

Deutsche Telekom AG  
Data Privacy, Legal Affairs and Compliance Board department  
Germany

---

### Version

### Last revised

### Status

Apr. 04, 2013

Final

---

### Technical contact

Deutsche Telekom AG  
Group Information Security

E-mail: [cert@telekom.de](mailto:cert@telekom.de)

---

### Summary

This document describes the required configuration steps for connecting a mod\_security sensor (web application firewall) to the Deutsche Telekom AG central early warning system (EWS).

The necessary scripts and configuration files for running this can be downloaded via [www.sicherheitstacho.eu](http://www.sicherheitstacho.eu).

---

All rights reserved, including the right to reprint excerpts, the right of photomechanical reproduction (including microcopying) and the right to use in databases and similar configurations.

---

## Table of contents

1.	Introduction .....	4
1.1	An overview of the system .....	4
2	Peer setup.....	6
2.1	mod_security installation overview.....	6
2.2	mod_security configuration .....	6
3	List of links.....	9



One of the Reporting module's main tasks is to inform the abuse<sup>1</sup> units that are connected as partners as soon as the specified criteria for an alert are met. Furthermore, the reporting module allows web-based generation of long-term and real-time statistics regarding the security situation on the Internet.

---

<sup>1</sup> Abuse: The term abuse unit refers to a provider's reporting center, which third parties can contact should suspicions arise relating to the misuse of Internet services and access data/codes.

## 2 Peer setup

### 2.1 mod\_security installation overview

In order to integrate the mod\_security web application firewall as a peer, the mod\_security [Apache](#) module of your respective distribution service must be installed in preparation and the configuration steps described here performed.

Furthermore, you must ensure that an SFTP client is installed on your system for transmitting the log files. Your EWS contact person at Deutsche Telekom AG will provide you with the user name to be used for the transmission (SFTP login). An SSH key pair (RSA2, 2048 Bit key length) then needs to be generated for the SFTP transmission of the mod\_security log files to the EWS. The private key generated must be copied to the `/opt/app/apache2/etc/private/MOD_SEC_KEY` (OpenSuse 7 / SLES environments) directory as it is expected here when establishing a connection in accordance with the configuration proposed here. The public key, on the other hand, is to be submitted to your EWS contact person at Deutsche Telekom AG for setup on the central server.

Note:

All the scripts described here are available under <http://www.sicherheitstacho.eu>.

#### 2.1.1 Preparation

The following sections are based on the example of a Suse Linux SLES11 distribution. The mod\_security module is included in the SLES11-SDK-SP1 pool as a Suse packet. The mod\_security module can be used as of version 2.3. To check whether the module is already installed on your client system, you can use the zypper RPM tool to search for the installed packets, for example.

Furthermore, the unique\_id module is used to provide a unique designation for every request.

Installed packets can be searched for under Suse Linux SLES using the following command:

```
zypper lr
```

The following provides an example of the output of a Suse Linux SLES11 system (SP1):

```
zypper se -s apache2-mod_security2
```

Loading repository data...

Reading installed packages...

S	Name	Type	Version	Arch	Repository
i	apache2-mod_security2	package	2.5.6-2.10.1	x86_64	SLES11-SDK-SP1-Pool

### 2.2 mod\_security configuration

## 2.2.1 Creating directories

```
mkdir /etc/apache2/mod_security
chmod 750 /etc/apache2/mod_security
chown root:root /etc/apache2/mod_security

mkdir /var/log/mod_security
chmod 750 /var/log/mod_security
chown www-data:adm /var/log/mod_security
```

## 2.2.2 Activating modules

```
a2enmod unique_id
a2enmod mod-security
```

Insert the following section in the web server configuration file (/etc/apache2/httpd.conf) (or alternatively in /etc/apache2/conf.d/security):

```
<IfModule security2_module>
  Include mod_security/*.conf
  Include mod_security/base_rules/*.conf
</IfModule>
```

## 2.2.3 Preparing the rule set

Unzip the [mod\\_security\\_conf.tgz](#) rule set specified by Deutsche Telekom AG in the /etc/apache2/mod\_security directory.

```
cd /etc/apache2/mod_security
tar -xzvf mod_security_conf.tgz
```

Once the TAR file is unzipped, the installation is complete and can be activated by restarting the Apache web server.

Restart:

```
apache2ctl restart
```

After sending the restart command, wait for the “done” message.

## 2.2.4 mod\_security log files

In order to record the attacks on the configured system, the relevant log files for the module need to be configured. To do this, open the mod\_security.conf file in a text editor and change the entries in accordance with the following example. Pay attention to the directory structures while doing so.

```
SecDebugLog /var/opt/mod_security/log/debug.log
SecDebugLogLevel 1
SecAuditEngine relevantonly
SecAuditLog /var/opt/mod_security/log/audit.log
SecAuditLogParts ABCFHZ
SecAuditLogType concurrent
SecAuditLogStorageDir /var/opt/mod_security/log
```

## 2.2.5 mod\_security channeling

The mod\_security log data is channeled to the EWS via SFTP (if required, a separate user should be set up for this that is only used for this purpose). A cronjob establishes an SFTP connection from the client at regular intervals to transmit the log files. On the client side, a script needs to be created that automatically prepares for the transmission.

## 2.2.6 Creating the script for rotation (copy truncate) and to transfer the log file (channeling)

Create the start script for the rotation and transmission of the log file in any directory. A suggestion for this would be:

```
/opt/app/apache2/bin/sftp_mod_security_logs.sh
```

The command

```
touch /opt/app/apache2/bin/sftp_mod_security_logs.sh
```

creates the relevant file.

Copy the following script suggestion into the file that was created by the touch command. If other file names and/or directories are to be selected, ensure that the modifications are made in the script suggestion.

```
#####

#!/bin/bash
HOSTNAME=`hostname`
LDIR=/var/opt/mod_security/log
if [ "$1" = "" ] ; then
HDATUM=`date -d 'now -5 min' '+%Y%m%d-%H' `
DATUM=`date -d 'now -5 min' '+%Y%m%d' `
GESTERN=`date -d 'now -1 day' '+%Y%m%d' `
else
DATUM=$1
fi
if [ -d /var/opt/mod_security/log ] ; then
cd /var/opt/mod_security/log
else
exit 1
fi
TGZNAME="${HDATUM}_${HOSTNAME}.tgz"
cp audit.log audit-${HDATUM}.log
> audit.log
cp debug.log debug-${HDATUM}.log
> debug.log
```



```

tar -czf $TGZNAME ${DATUM}/${HDATUM}* audit-${HDATUM}.log debug-
${HDATUM}.log
KEYFILE=/opt/app/apache2/etc/private/MOD_SEC_KEY
ZIEL='Muster-Peer.de@80.153.226.137:incoming'
PORT=37022
echo -e "put $TGZNAME" | sftp -b - -o Port=$PORT -o IdentityFile=${KEYFILE}
${ZIEL} > /dev/null 2>&1
#rm $TGZNAME
rm -rf ${DATUM}/${HDATUM}* audit-${HDATUM}.log debug-${HDATUM}.log
rm -rf ${GESTERN}
#####

```

After creating the channeling script, a corresponding cronjob is required for automated transmission, which controls the channeling script.

## 2.2.7 Channeling cronjob

Create the mod\_security file in the /etc/cron.d/ directory.

```
touch /etc/cron.d/mod_security
```

Then open the file created by the touch command with a text editor and complete it with the following entry.

```
01 * * * * root /opt/app/apache2/bin/sftp_mod_security_logs.sh > /dev/null
2>&1
```

Alternatively, you can create the cronjob using the crontab -e command (as the root user).

The mod\_security cronjob now automatically controls the rotation and channels the log files to the central EWS at every full hour.

In the first few days after activating the module, you should monitor the log file size.

## 3 List of links

<http://www.apache.org>

<http://www.modsecurity.org/>

<http://de.wikipedia.org/wiki/Malware>

<http://www.virustotal.com/>

[http://www.sicherheitstacho.eu/download/sftp\\_mod\\_security\\_logs.sh](http://www.sicherheitstacho.eu/download/sftp_mod_security_logs.sh)

[http://www.sicherheitstacho.eu/download/mod\\_security.cron](http://www.sicherheitstacho.eu/download/mod_security.cron)

[http://www.sicherheitstacho.eu/download/mod\\_security\\_conf.tgz](http://www.sicherheitstacho.eu/download/mod_security_conf.tgz)

