


# Custom rules and decoders

It is possible to modify the default rules and decoders from the Wazuh Ruleset and also to add new ones in order to increase Wazuh's detection capabilities.

## Adding new decoders and rules

 **Note**

We will use `local_decoder.xml` and `local_rules.xml` to implement small changes. For larger scale changes/additions to the stock decoders and rules, we recommend you create a new decoder and/or rule file.

We are going to describe these procedures using an easy example. Here is a log from a program called `example`:

```
Dec 25 20:45:02 MyHost example[12345]: User 'admin' logged from '192.168.1.100'
```

First, we need to decode this information, so we add the new decoder to `/var/ossec/etc/decoders/local_decoder.xml`:

```
<decoder name="example">
  <program_name>^example</program_name>
</decoder>

<decoder name="example">
  <parent>example</parent>
  <regex>User '(\w+)' logged from '(\d+\.\d+\.\d+\.\d+)'</regex>
  <order>user, srcip</order>
</decoder>
```

Now, we will add the following rule to `/var/ossec/etc/rules/local_rules.xml`:

```
<rule id="100010" level="0">
  <program_name>example</program_name>
  <description>User logged</description>
</rule>
```

We can check if it works by using `/var/ossec/bin/ossec-logtest`:

```
**Phase 1: Completed pre-decoding.
  full event: 'Dec 25 20:45:02 MyHost example[12345]: User 'admin' logged from '192.168.1.100''
  hostname: 'MyHost'
  program_name: 'example'
  log: 'User 'admin' logged from '192.168.1.100''

**Phase 2: Completed decoding.
  decoder: 'example'
  dstuser: 'admin'
  srcip: '192.168.1.100'

**Phase 3: Completed filtering (rules).
  Rule id: '100010'
  Level: '0'
  Description: 'User logged'
```

## Changing an existing rule

You can modify the standard rules.

## ⚠ Warning

Changes to any rule file inside the `/var/ossec/ruleset/rules` folder will be lost in the update process. Use the following procedure to preserve your changes.

If we want to change the level value of the SSH rule `5710` from 5 to 10, we will do the following:

1. Open the rule file `/var/ossec/ruleset/rules/0095-sshd_rules.xml`.
2. Find and copy the following code from the rule file:

```
<rule id="5710" level="5">
  <if_sid>5700</if_sid>
  <match>illegal user|invalid user</match>
  <description>sshd: Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_10.6.1,</group>
</rule>
```

3. Paste the code into `/var/ossec/etc/rules/local_rules.xml`, modify the level value, and add `overwrite="yes"` to indicate that this rule is overwriting an already defined rule:

```
<rule id="5710" level="10" overwrite="yes">
  <if_sid>5700</if_sid>
  <match>illegal user|invalid user</match>
  <description>sshd: Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_10.6.1,</group>
</rule>
```

## Changing an existing decoder

You can also modify the standard decoders.

## ⚠ Warning

Changes in any decoder file in the `/var/ossec/ruleset/decoders` folder will be lost in the update process. Use the following procedure to preserve your changes.

Unfortunately, there is no facility for overwriting decoders in the way described for rules above. However, we can perform changes in any decoder file as follows:

If we want to change something in the decoder file `0310-ssh_decoders.xml`, we will do the following:

1. Copy the decoder file `/var/ossec/ruleset/decoders/0310-ssh_decoders.xml` from the default folder to the user folder `/var/ossec/etc/decoders` in order to keep the changes.
2. Exclude the original decoder file `ruleset/decoders/0310-ssh_decoders.xml` from the OSSEC loading list. To do this, use the tag `<decoder_exclude>` in the `ossec.conf` file. Thus, the specified decoder will not be loaded from the default decoder folder, and the decoder file saved in the user folder will be loaded instead.

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>

  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>
  <decoder_exclude>ruleset/decoders/0310-ssh_decoders.xml</decoder_exclude>
</ruleset>
```

3. Perform the changes in the file `/var/ossec/etc/decoders/0310-ssh_decoders.xml`.

### Warning

Note that at this point, if updates to the public Wazuh Ruleset include changes to 0310-ssh\_decoders.xml, they will not apply to you since you are no longer loading that decoder file from the standard location that gets updates. At some point you may have to manually migrate your customized material from 0310-ssh\_decoders.xml to a newer copy of that file. Consider internally documenting your changes in 0310-ssh\_decoders.xml so that they are easy to find if they have to be migrated later.