auth

XML section name

```
<auth>
</auth>
```

This section has options for the registering service.

New in version 2.1.

Options

disabled

Disables the execution of the Auth daemon.

Default value	no
Allowed values	• yes • no

port

TCP port number to listen to connections.

Default value	1515
Allowed values	0 - 65535

use_source_ip

Use client's source IP address instead of "any" to add agent.

Default value	no
Allowed values	• yes • no

force_insert

Force insertion: remove old agent with same name or IP.

Default value	no
Allowed values	• yes • no

force_time

When forcing to remove old agents with same name or IP, this options specifies that the deletion will be performed only if the agent's keepalive has more than a number of seconds.

Default value	0
Allowed values	• Positive number • 0

Value `0` means to force always.

purge

Delete definitely agents when removing.

Default value	no
Allowed values	• yes • no

When set to `no` removed agents will remain in the client keys file, marked as removed. However, when set to `yes`, client keys file will be purged.

use_password

Enable shared password authentication.

Default value	no
Allowed values	• yes • no

When enabled, the shared password will be read from file at `/var/ossec/etc/authd.pass`.

If this file does not exist, a **random password** will be generated.

ssl_agent_ca

Full path to CA certificate used to verify clients.

Allowed values	A full path

ssl_verify_host

When CA certificate is specified, this option enables source host verification. This means that the client source IP will be validated using the *Common Name* field.

Default value	no

Allowed values	• yes • no

ssl_manager_cert

Full path to server SSL certificate.

Default value	/var/ossec/etc/sslmanager.cert
Allowed values	A full path

ssl_manager_key

Full path to server SSL key.

Default value	/var/ossec/etc/sslmanager.key
Allowed values	A full path

ssl_auto_negotiate

Auto select SSL/TLS method.

Default value	no
Allowed values	• yes • no

By default only TLS v1.2 is allowed. When set to `yes` the system will negotiate the most secure common method with the client.

In older systems, where the **manager does not support TLS v1.2**, this option will be enabled automatically.

Default configuration

```
<auth>
  <disabled>no</disabled>
  <port>1515</port>
  <use_source_ip>no</use_source_ip>
  <force_insert>no</force_insert>
  <force_time>0</force_time>
  <purge>no</purge>
  <use_password>no</use_password>
  <!-- <ssl_agent_ca></ssl_agent_ca> -->
  <ssl_verify_host>no</ssl_verify_host>
  <ssl_manager_cert>/var/ossec/etc/sslmanager.cert</ssl_manager_cert>
  <ssl_manager_key>/var/ossec/etc/sslmanager.key</ssl_manager_key>
  <ssl_auto_negotiate>no</ssl_auto_negotiate>
</auth>
```