MQTT credentials

# MQTT credentials#

You can use these credentials to authenticate the following nodes:

• MQTT

• MQTT Trigger

## Prerequisites#

Install an MQTT broker.

MQTT provides a list of Servers/Brokers at MQTT Software.

## Supported authentication methods#

• Broker connection

## Related resources#

Refer to MQTT's documentation for more information about the MQTT protocol.

Refer to your broker provider's documentation for more detailed configuration and details.

## Using broker connection#

To configure this credential, you'll need:

• Your MQTT broker's Protocol

• The Host

• The Port

• A Username and Password to authenticate with

• If you're using SSL, the relevant certificates and keys

To set things up:

• Select the broker's Protocol, which determines the URL n8n uses. Options include:  
Mqtt: Begin the URL with the standard mqtt: protocol.  
Mqtts: Begin the URL with the secure mqtts: protocol.  
Ws: Begin the URL with the WebSocket ws: protocol.

• Mqtt: Begin the URL with the standard mqtt: protocol.

mqtt:

• Mqtts: Begin the URL with the secure mqtts: protocol.

mqtts:

• Ws: Begin the URL with the WebSocket ws: protocol.

ws:

• Enter your broker Host.

• Enter the Port number n8n should use to connect to the broker host.

• Enter the Username to log into the broker as.

• Enter that user's Password.

• If you want to receive QoS 1 and 2 messages while offline, turn off the Clean Session toggle.

• Enter a Client ID you'd like the credential to use. If you leave this blank, n8n will generate one for you. You can use a fixed or expression-based Client ID.  
Client IDs can be useful to identify and track connection access. n8n recommends using something with n8n in it for easier auditing.

• Client IDs can be useful to identify and track connection access. n8n recommends using something with n8n in it for easier auditing.

n8n

• If your MQTT broker uses SSL, turn the SSL toggle on. Once you turn it on:  
Select whether to use Passwordless connection with certificates, which is like the SASL mechanism EXTERNAL. If turned on:  
Select whether to Reject Unauthorized Certificate: If turned off, n8n will connect even if the certificate validation fails.  
Add an SSL Client Certificate.  
Add an SSL Client Key for the Client Certificate.  
One or more SSL CA Certificates.

• Select whether to use Passwordless connection with certificates, which is like the SASL mechanism EXTERNAL. If turned on:  
Select whether to Reject Unauthorized Certificate: If turned off, n8n will connect even if the certificate validation fails.  
Add an SSL Client Certificate.  
Add an SSL Client Key for the Client Certificate.

• Select whether to Reject Unauthorized Certificate: If turned off, n8n will connect even if the certificate validation fails.

• Add an SSL Client Certificate.

• Add an SSL Client Key for the Client Certificate.

• One or more SSL CA Certificates.

Refer to your MQTT broker provider's documentation for more detailed configuration instructions.