MANITOU API - How to get on board

Description : this document provides information on how to use the MANITOU webservices platform for connected machines data. The following key steps are for customer IT teams to go live with their MANITOU API solution upon agreement signature and terms & conditions acceptance.

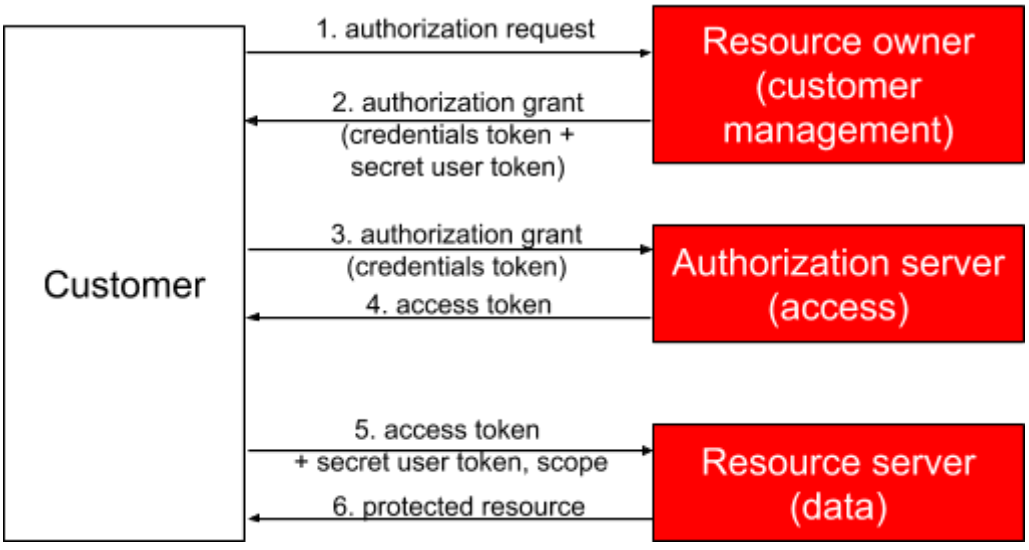
Preamble

MANITOU API is a data service in the form of APIs (Application Programming Interface) that provide the Customer access to protected resources, in coherence with the Customer's service level of subscription.

The access to the protected resources provided through the API system is regulated through a 2-step authentication process, complying with the OAuth2 authorization framework, a recognized Internet standard (see IETF RFC 6749 and IETF RFC 6750 for detailed information on the OAuth2 framework).

Overview of the authorization process

The following schema describes every step needed to interact successfully with MANITOU API :



Steps 1 & 2 : exchange with the resource owner

1. **Authorization request**
   The first step is for the customer to agree to the terms & conditions of our service, and

sign up for it.

2. **Authorization grant**
   As a result of the customer's subscription, we create an account for the Customer in our platform, and provide the Customer with 2 informations :
   a. His credentials token
   b. His secret user token

Steps 3 & 4 : exchange with the authorization server

3. **Authorization grant**
   The Customer places an API call to our authorization server, providing his client credentials (see step 2).

4. **Access token**
   The authorization server provides time-limited, temporary access tokens. These tokens are necessary to give access to protected resources to the Customer.
   Note : if an access token expires, it has to be renewed using the same mechanism.

Steps 5 & 6 : exchange with the resource server

5. **Access token**
   The Customer places an API call to our resource server, providing his valid access token (see step 4) and his secret user token (see step 2).
   The access token provides the Customer with the right to call our resource APIs.
   The secret user token provides the Customer with the right to obtain protected resources that belong to him.
   Optional : the scope provides our system with the type of access the Customer wants, which lets our API system filter calls considering the subscription level of the customer.

6. **Protected resource**
   The resource server give the protected resource in response to the customer's call.

In details : getting an access token with your credentials

The MANITOU information system provides its API subscribers with a dedicated authentication endpoint (see chart below).
The Customer identifies himself towards that endpoint by providing a credential token.
In response, the endpoint returns an *access* token that is valid for a limited time period.

The following chart demonstrates example values that are used when placing a call to the authentication endpoint.

Information	Example value
Authentication endpoint URL	*https://ws.manitou-group.com/token*
Query parameter : `grant_type` Value : `client_credentials`	*grant_type=client_credentials*
Credential token (to be used in Authorization header)	*THISisAcredentialTOKENthisISaCREDENTIALtokenTHISisAcredentialTOKENthisISaCRE*
Example request	*https://ws.manitou-group.com/token?grant_type=client_credentials*
Example header	*Authorization: Bearer THISisAcredentialTOKENthisISaCREDENTIALtokenTHISisAcredentialTOKENthisISaCRE*
Example response	*{ "scope" : "am_application_scope default", "token_type" : "Bearer", "expires_in" : 3600, "access_token" : "abec7405-eade-3195-9d0d-0c06f9d98f45" }*
Access token extracted from the response :	*abec7405-eade-3195-9d0d-0c06f9d98f45*

In details : getting a protected resource from your access token and your secret user token

The MANITOU information system provides its API subscribers with dedicated protected resource endpoints.
The Customer identifies himself as an authorized subscriber towards that endpoint by providing a valid access token (see previous section) in the proper request header.
The Customer also provides his secret user token in an additional request header, so that the protected resource endpoint only delivers the Customer's private protected resource(s).
In response, the endpoint returns the protected resource.

The following chart demonstrates example values that are used when placing a call to the authentication endpoint.

Information	Example value
Resource endpoint URL	*https://ws.manitou-group.com/machine/connected-machine*
Query parameter (optional) : `page[size]` Value : *<number of resource records per response page>*	*page[size]=10*
Query parameter (optional) : `page[number]` Value : *<number of the resource records' requested page>*	*page[number]=2*
Query parameter (optional) : `filter[<attribute>]` Value : *attribute value to filter on*	*filter[machine.id]=123456*
Access token (to be used in Authorization header)	*abec7405-eade-3195-9d0d-0c06f9d98f45*
Secret user token (to be used in X-token header)	*AAAAAAA-AAAA-AAAA-AAAA-AAAAAAAAAAAA*
Example request	*https://ws.manitou-group.com/machine/connected-machine?page[size]=10&filter[machine.id]=123456*
Example Authorization header	*Authorization: Bearer abec7405-eade-3195-9d0d-0c06f9d98f45*
Example X-token header	*X-token: AAAAAAA-AAAA-AAAA-AAAA-AAAAAAAAAAAA*

Confidentiality reminder

Take care of your credentials token & secret user token confidentiality : **these are the keys to your API data !**

- → don’t share them by email
- → don’t write them down
- → keep it unknown from every people that don’t specifically need it

If you think the confidentiality of these informations have been compromised, remember to notify MANITOU as soon as possible.

Technicalities

All the necessary information describing endpoints, data structure, etc, is contained in the OpenAPI / Swaggerhub file joined with this documentation.