
Guide to AEMO's e-Hub APIs

1.03 Final
October 2020

Provides details for the e-Hub API interface to communicate with AEMO.

Important Notice

PURPOSE

This Guide to AEMO's e-Hub APIs (Guide), prepared by AEMO, provides guidance for e-Hub APIs under the National National Electricity Rules (Rules).

NO RELIANCE OR WARRANTY

This document does not constitute legal or business advice, and should not be relied on as a substitute for obtaining detailed advice about the National Gas or Electricity Law, the Rules or any other applicable laws, procedures or policies. While AEMO has made every effort to ensure the quality of the information in this Guide, neither AEMO, nor any of its employees, agents and consultants make any representation or warranty as to the accuracy, reliability, completeness, currency or suitability for particular purposes of that information.

LIMITATION OF LIABILITY

To the maximum extent permitted by law, AEMO and its advisers, consultants and other contributors to this Guide (or their respective associated companies, businesses, partners, directors, officers or employees) are not liable (whether by reason of negligence or otherwise) for any errors, omissions, defects or misrepresentations in this document, or for any loss or damage suffered by persons who use or rely on the information in it.

TRADEMARK NOTICES

Microsoft is a trademark of Microsoft Corporation in the United States and/or other countries.
Oracle and Java are registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

DISTRIBUTION

Available to the public.

DOCUMENT IDENTIFICATION

Business custodian: Manager, Prudentials
IT custodian: Manager, Settlements and Prudential Systems
Prepared by: Technical Writers, Digital and Technology

VERSION HISTORY

Version 1.03. Updated CSR and API access information.
Last update: Monday, 19 October 2020 4:35 PM

DOCUMENTS MADE OBSOLETE

The release of this document changes any previous versions of Guide to AEMO's e-Hub APIs.

FEEDBACK

Your feedback is important and helps us improve our services and products. To suggest improvements, please contact AEMO's Support Hub.

Contents

Introduction	1
Purpose	1
Audience	1
How to use this guide	1
What's in this guide	2
About AEMO's e-Hub	3
Architecture	4
API Standard	4
Design principles	5
URL format	5
Network connectivity requirements	7
HTTP request	8
HTTP response	10
Traffic Management	12
Connection and read timeout settings	12
Security	13
System requirements	14
Swagger files	15
Participant e-Hub Gateway	15
Using the API Portal	16
Steps to use APIs	16
Access the API Portal	16
Register	17
View the API catalogue	18
Manage Certificates	21
Decide how to use certificates	21
Use an existing certificate	22
Obtain a new certificate	22
Information required for your CSR	23
Send the certificate to AEMO	24
AEMO validates, generates, and issues the certificate	25
AEMO and participants install the digital certificate	25

Needing Help?	27
Developer Portal FAQs	28
AEMO's Support Hub	28
Information to provide	28
Feedback	29
Related resources	29
Glossary	30
Index	37

Introduction

In this chapter:

Purpose	1
Audience	1
How to use this guide	1
What's in this guide	2

Purpose

This guide provides details about using AEMO's e-Hub as an interface to communicate information with AEMO.

It assists wholesale electricity and gas participants developing their own APIs.

For details about MSATS B2B e-Hub communications, see B2B SMP Technical Guide.

Audience

The primary audience is participants' technical staff responsible for developing APIs.

The secondary audience is anyone who has an interest in understanding how AEMO APIs work.

How to use this guide

- This document is written in plain language for easy reading. Where there is a discrepancy between the Rules and information or a term in this document, the Rules take precedence.
- The references listed throughout this document are primary resources and take precedence over this document.
- **Text in this format** indicates a resource on AEMO's website.
- Glossary terms are capitalised and have the meanings listed against them in the Glossary section.
- Italicised terms are defined in the Rules. Any rules terms not in this format still have the same meaning.
- This guide assumes you have knowledge of the RESTful programming architecture.
- Actions to complete in the API Web Portal interface are bold and dark grey.

What's in this guide

- **About AEMO's e-Hub** provides an overview of the e-Hub environment, basic requirements, security, and system requirements. It also explains the HTTP request methods and responses, what goes in the header, and provides POST and GET examples.
- **Using the API Portal** provides the steps to access the e-Hub, including URLs, and how to register and view the APIs.
- **Manage Certificates** provides guidance about managing certificates and how to set them up.
- **Needing Help? 27** provides some FAQs, related resources, and a glossary.

About AEMO's e-Hub

The e-Hub is AEMO's communication platform supporting exchange of information between participants and AEMO. The e-Hub is accessible over MarketNet and internet and includes:

- An **API Web Portal** for registration and as a resource for downloading Swagger files, see [About AEMO's e-Hub](#).
- An **API Gateway**, see [About AEMO's e-Hub above](#).

Figure 1 AEMO's e-Hub and Participant API Gateway

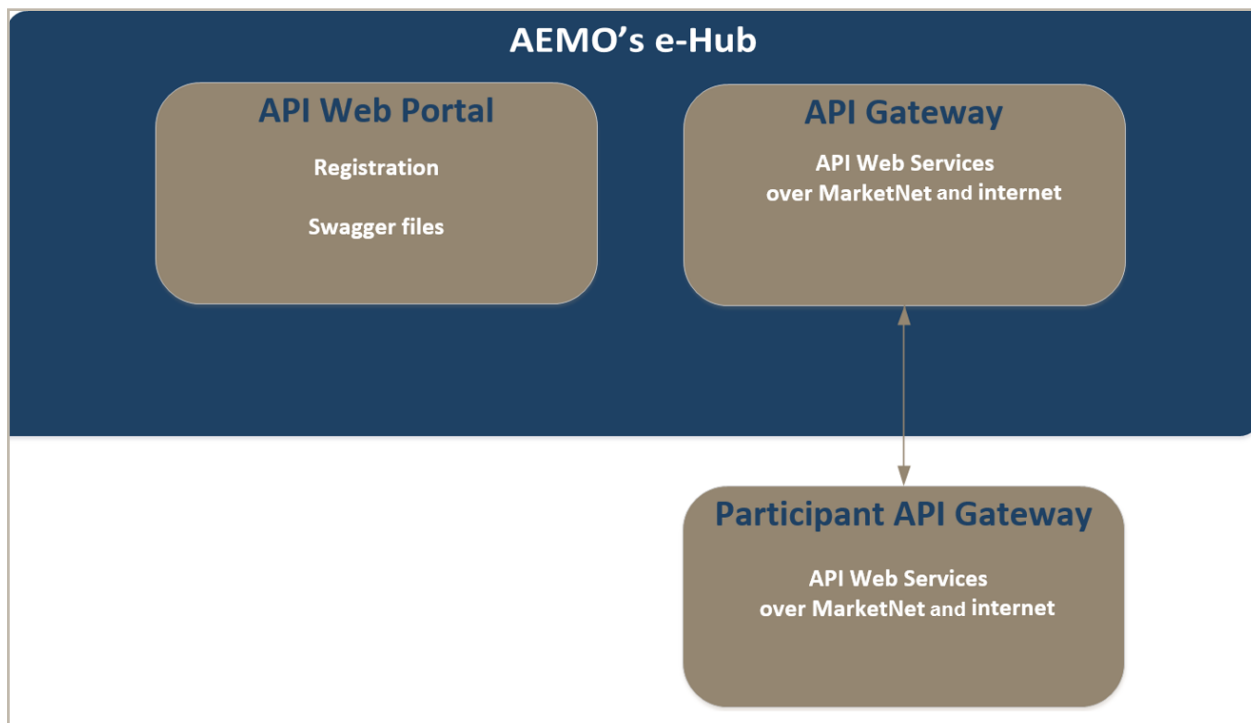
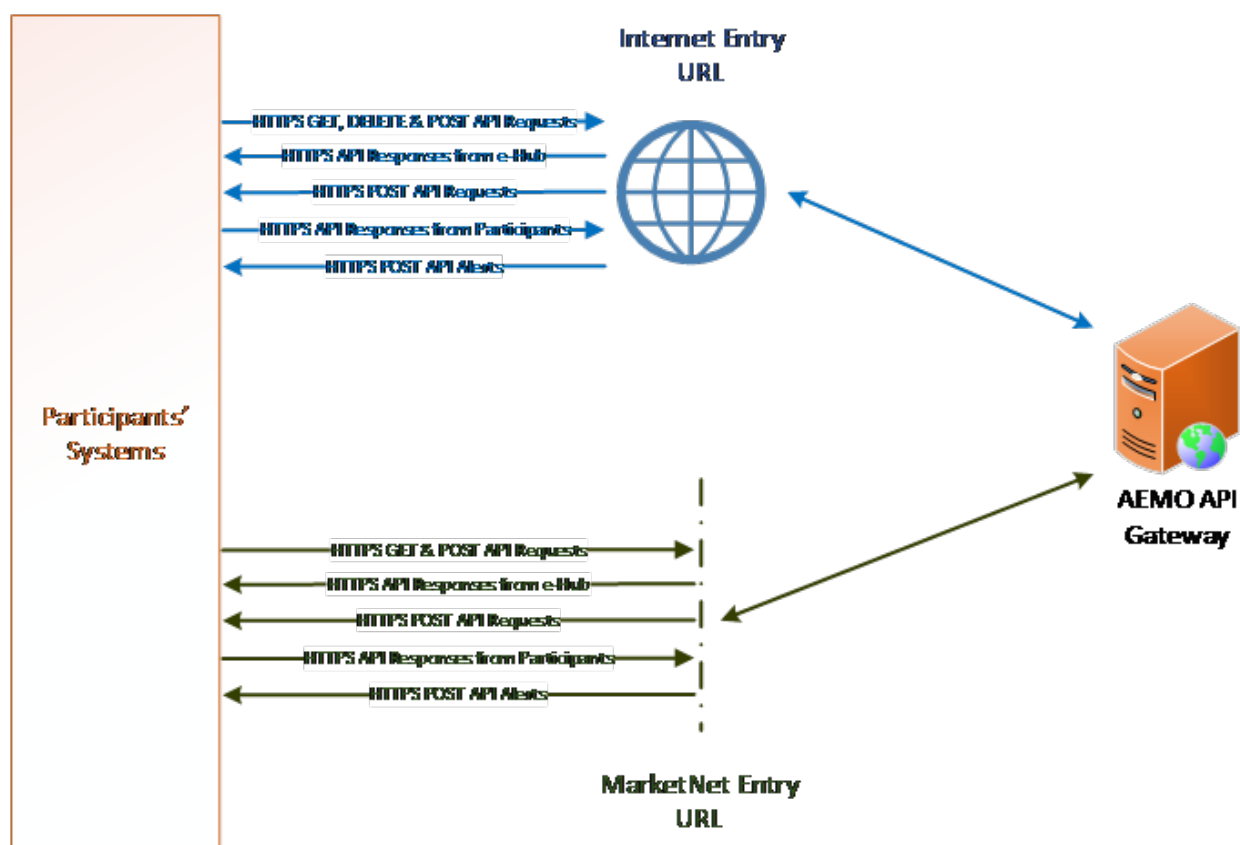


Figure 2 API Gateway



Architecture

AEMO chose RESTful (REST) for its web services architecture because of its lightweight nature and ability to transmit data using HTTPS and JSON. REST is an alternative to SOAP and WSDL and is cheaper, simpler, and faster. The REST architecture makes it possible to start small; developing what is required with available resources, scaling up as the number of services increase.

AEMO's goal with this approach is:

- Performance: quality of responsiveness.
- Scalability: many users can simultaneously use the systems.
- Generality: solve a wide variety of problems.
- Simplicity: no complex interactions, easy to prove the system is doing as it should.
- Modifiability: extensible in the face of new requirements and technologies.

MarketNet is AEMO's private data network connection. For details about the options available to connect to MarketNet, see [Guide to Information Systems on AEMO's website](#).

API Standard

The standard AEMO uses for APIs is the OpenAPI Specification (OAS). For more details, see [OpenAPI-Specification](https://github.com/OAI/OpenAPI-Specification): <https://github.com/OAI/OpenAPI-Specification>.

Design principles

The REST approach uses the features of HTTP to make requests using these design principles:

- HTTPS protocol provides services over MarketNet or the internet.

While APIs are defined in either YAML or JSON format, the API request body and other content are not required to be JSON or YAML.

For technical details about individual API specifications, see the generated Swagger files in the API Web Portal. For help, see [View the API catalogue](#).

- Resources are mapped to a location within a hierarchy of URIs, for example: `service host>/<system>/<business_function>`.
- Accommodates a variety of payloads such as XML, JSON, or a custom schema.

The root of the hierarchy represents the web service or API application and provides the resources available.

The next level provides specific information about the resource,

The final level provides data from the specific resource records. For more details, see [URL format](#).

URL format

API URLs are in the following format:

`<protocol>://<webservice_host>/<routing_gateway>/<business_name>/<business_function>/<API_version>/<resource>?querystring parameters`

Parameter	Description										
<protocol>	HTTP or HTTPS Note: Participant facing protocol must be HTTPS.										
<webservice_host>	Name of the server hosting the service or an external proxy. Example: Market Facing Internet web service host: apis.prod.aemo.com.au:9319 Market Facing MarketNet web service host: apis.prod.marketnet.net.au:9319										
<routing_gateway>	Identifies the AEMO API gateway to which the request must be routed to Domain Values: ehub: APIs mediated via webMethods platform (Mediator) public: APIs mediated via the cloud gateway (e.g. AWS gateway for the GBB project)										
<business_name>	Identifies the business name. Note: The enumerations documented below are not complete. The enumerations will be amended as and when the standards are adopted by other applications: Enumerations:										
	<table border="1"> <thead> <tr> <th><business_name></th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>NEMRetail</td> <td>NEM Retail B2B & B2M</td> </tr> <tr> <td>NEMWholesale</td> <td>NEM Wholesale</td> </tr> <tr> <td>gbb</td> <td>Gas Bulletin Board</td> </tr> <tr> <td>common</td> <td>APIs that are common to various markets/applications e.g. eHub Identity Service, eHub Throttling API</td> </tr> </tbody> </table>	<business_name>	Description	NEMRetail	NEM Retail B2B & B2M	NEMWholesale	NEM Wholesale	gbb	Gas Bulletin Board	common	APIs that are common to various markets/applications e.g. eHub Identity Service, eHub Throttling API
<business_name>	Description										
NEMRetail	NEM Retail B2B & B2M										
NEMWholesale	NEM Wholesale										
gbb	Gas Bulletin Board										
common	APIs that are common to various markets/applications e.g. eHub Identity Service, eHub Throttling API										
<business_function>	API Name - The AEMO system providing the services, e.g. generatorRecall										
<API_version>	Version of the API. Starts with <v1>. This is utilised when multiple versions of the API are supported; enables Participants to gradually transition from one version of the API to another. Note: No dot releases/versions are allowed such as v1.1										
<Resource>	Entities of the business function e.g. /listRecallPlans										
?querystring parameters	Case-sensitive query string parameters for GET & DELETE methods.										

Format example

```
https://<webservice_host>/<routing_gateway>/<business_name >/<business_
function>/<API_version>/<resource>?querystring parameters
```

Internet URL example

```
https://apis.prod.aemo.com.au:9319/ehub/NEMRetail/generatorRecall/v1/listReca
llPlans
```

MarketNet URL example

```
https://apis.prod.marketnet.com.au:9319/ehub/NEMRetail/generatorRecall/v1/list
RecallPlans
```

Network connectivity requirements

This section describes the connectivity requirements between AEMO IP addresses, the public IP addresses that AEMO will whitelist and the IP addresses of the API gateway(s).

Participants can use this information to provide the relevant IP address, URLs and ports to AEMO for whitelisting.

Table 1 Participant systems to AEMO

Source (provide to AEMO)	Destination	Protocol and Port
Public IP address(s) that will access AEMO's network	apis.preprod.aemo.com.au – 202.44.77.88	TCP, 9319
	apis.prod.aemo.com.au – 202.44.77.87	TCP, 9319

Table 2 AEMO to Participant systems

Source	Destination (provide to AEMO)	Protocol and Port (participants specify the port from the range below)
202.44.78.204	Participant to provide URL	TCP, 9318-9330
202.44.76.204	Example: https://<url>:93xx/destinationURI Note: This must translate to a publicly routable IP address.	

HTTP request

HTTP header attributes are case sensitive.

Header

Header parameter	Description	Allowed values / Example
Content-type	HTTPS request format.	Content-type: application/json
Accept	HTTPS response format.	Accept: application/json
Content-length	Content length of file. The value is populated when the request is sent.	Content-length: nnn

Header parameter	Description	Allowed values / Example
X-initiatingParticipantID	The participant ID	X-initiatingParticipantID: 123456
X-market	The market type that the request applies.	X-market: GAS
Authorisation	Specifies basic HTTP authentication containing the Base64[1] encoded username and password. The participant's URM username and password are concatenated with a colon separator and then Base64 encoded.	Authorisation: Basic QFhQVC0wMDAwMzoyZWRmOGJhYS0wY2I0LTQwZjctOTlyMS0yODUxNmM4N2MxNjQ= (For URM username "@XPT-00003" and password "2edf8baa-0cb4-40f7-9221-28516c87c164")

Note: There may be other HTTP request header parameters that are specific to the individual APIs.

Methods

HTTPS method	Operation	Details
GET	Retrieve Data	<p>The GET method has the query string parameters in the URL.</p> <p>The GET method does not have the Content-Type passed in the HTTP request.</p> <p>Not all AEMO's APIs use the GET method.</p>
POST	Post Data	<p>The POST method has:</p> <ul style="list-style-type: none"> • No query string parameters in the URL. • HTTP request header parameters specific to the API (if any). • Payload <p>Example:</p> <pre>{ "ParticipantId": "PID", "StartDate": "2017-11-01T00:00:00+10:00", "EndDate": "2017-11-02T00:00:00+10:00", "StationId": "PID6", "DUID": "AEMO1", "OutagePlanId": "MMS_GEN_OUT1" }</pre>
DELETE	Delete Data	<p>The DELETE method has the query string parameters in the URL.</p>
PUT	Update Data	<p>PUT method has:</p> <ul style="list-style-type: none"> • No query string parameters in the URL • HTTP request header parameters specific to the API (if any) • Payload

Note: BASIC Authentication details, username and password encoded and passed in the request header for all these 4 methods above.

HTTP response

The HTTP Response has:

- A response code and description, with
 - A successful request indicated by 200 OK.
 - Other response codes for technical and Payload validation failures. For details, see [Codes](#).
- Optional Payload.

Codes

The e-Hub sends an appropriate HTTP response code and response Payload when any of the technical validations fail.

Some APIs may have specific response codes, for details check the individual Swagger file.

Code	Condition	Description
200	Indicates a successful request.	OK (Response example - 200 OK with response Payload).
400	Invalid API URI	The service cannot be found for the endpoint reference (EPR) <URI> "Fault": "<SystemMessageExceptionDump>"
401	Invalid credentials No BASICAuth information in HTTP Request Header	Unauthorized "Exception": "Unauthorized:Invalid UserName or Password" "Exception": "Unauthorized:Invalid UserName or Password"
404	Resource not Found	"Exception": "Resources for the endpoint URI not found. Endpoint URI: <Resource>"
405	Invalid Method used (e.g. GET used instead of POST)	"Exception": "Input request HTTP method is <Invalid Method passed> but operation <Resource Name> accepts only: [<Valid Method>]" (see Response example - HTTP response code 405)
422	Business validation failure	Unprocessable entity
500	e-Hub is operational but downstream systems are not available or malformed payload (JSON)	"Exception": "Application Unavailable"
503	Exceeds Throttling Limits	Service invocation for API was rejected based on policy violation

Response example - 200 OK with response Payload

```

HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: nnn
Date: Mon, 01 May 2017 18:00:00 GMT
Connection: close
{
  "data": {
    "MaxRecallTime": 506200,
    "SuccessFlag": true,
    "ResponseMessage": "Get Recall Plan action succeeded",
    "RecallPlanList": [
      {
        "StationId": "TEST",
        "OutagePlanId": "TEST_OUT1",
        "Stage1Description": null,
        "Stage2Description": null,
        "DUID": "TEST1",
        "MinimumStartDate": "2017-11-10T00:00:00",
        "MaximumEndDate": "2017-11-11T00:00:00",
        "VersionDateTime": "2017-11-16T18:20:12",
        "Entries": []
      }
    ]
  }
}

```

Response example - HTTP response code 405

```

HTTP/1.1 405 Method Not Allowed
Content-Length: nnn
Date: Mon, 01 May 2017 18:00:00 GMT
Connection: close
{
  "Exception": "Input request HTTP method is GET but operation /listRecallPlans
accepts only: [POST]"
}

```

Traffic Management

To protect the backend service from overload, the e-Hub enforces traffic limits. For details about the traffic limits for each individual API, see the individual API policy. For help, see [View the API catalogue](#).

Connection and read timeout settings

We recommend participants use the following settings when calling AEMO's APIs.

Type	Problem	Recommended Settings
Connection timeout	Cannot connect to the e-Hub's endpoint (e.g. e-Hub infrastructure is not available).	10 seconds
Read timeout	Connected to the endpoint but the e-Hub does not respond within the configured time.	30 seconds

Security

Custom Ports

The API Gateway uses custom ports as a defence against Denial of Service (DoS) attacks.

- For HTTPS the port is 9319.
- Participants may nominate a port between 9318 and 9330 in the URLs they supply to the SMP (Shared Market Protocol) administration. These URLs apply to the participant gateways.

SSL certificates

The e-Hub uses SSL certificates to secure encrypted communication and secure interactions between participants' and AEMO's systems. All communications between the e-Hub and participants' gateways use HTTPS. The e-Hub does not support HTTP.

Each participant must create / obtain a private key and a Certificate Signing Request (CSR).

A private key and CSR is usually created at the same time, making a key pair. A CSR is usually generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organisation name, common name (CN), locality and country. It also contains the public key that will be included in the certificate. For more information, refer to the **SMP Technical Guide**.

Access to production and pre-production APIs require different SSL certificates.

Authentication and authorisation

When calling APIs, participants authenticate their identity using Basic Authentication – passing a username and password.

The username and password are provided by your company's participant administrator (PA) and is encoded into a Base64 authorisation token.

SSL connectivity for the e-Hub complies with the TLS v1.1 and v1.2 protocols.

To do this you need an application such as Postman (for help, see <https://www.getpostman.com/>).

The HTTP Basic authentication header takes the following format:

Authorization: Basic {Base64 hash of user:password}, for example:

```
Authorization: Basic QWxhZGRpbjpvYVUyIHh1c2FtZQ==
```

System requirements

API Portal

To connect to the API Portal, participants need:

- Access to the internet. For details about MarketNet, see [Guide to Information Systems](#). If you are an existing participant your company probably already has access to MarketNet.
- API Portal registration, see [Register 17](#).
- A valid SSL certificate, see [Manage Certificates 21](#).

API Gateway

To connect to the API Gateway, participants need:

- Access to MarketNet or the internet. For details about MarketNet, see [Guide to Information Systems](#).
- Their IP address range white listed by AEMO.
- SSL authentication using digital certificates.

A user ID and password with access rights for the API provided by your company's Participant Administrator (PA). For help, see [Participant usernames and passwords expire every 60 days](#). This is the username and password that goes in the authorisation header. For help, see [Authentication and authorisation](#).

Participant usernames and passwords expire every 60 days. This is the username and password that goes in the authorisation header. For help, see [Authentication and authorisation](#).

User access rights

For access to APIs, participant administrators select the relevant entity in the MSATS “Maintain Rights” menu and assign the right to their participant users. For help, see **Guide to User Rights Management**.

For help with passwords, see **Guide to Information Systems**.

For example, the entity required for the Generator Recall APIs is:

- EMMS - Offers and Submissions - Generator Recall

Swagger files

What are they?

Swagger files are one of the tools of the OpenAPI Specification (OAS). It is the specification of the API detailing its resources and operations in a human and machine readable format for easy development, discovery, and integration. AEMO uses Swagger files in its API Portal.

How to use

You can use the Swagger tools to view, inspect, and test the Swagger file before integrating it into your systems.

To download an AEMO API, see **3.5 Obtain a Swagger file 1**.

For more details and examples, see **OpenAPI Specification**:
<https://swagger.io/specification/>

Participant e-Hub Gateway

Participants can implement their own API Gateway to interact with AEMO’s API Gateway.

To set up your own gateway define your URL and API names. The e-Hub uses the resources and methods to push the messages to your gateway.

Using the API Portal

In this chapter:

Steps to use APIs	16
Access the API Portal	16
Register	17
View the API catalogue	18

Steps to use APIs

Follow these steps to begin using AEMO's APIs:

1. Register
2. Access the API Portal
3. View the API catalogue
4. Send the certificate to AEMO
5. AEMO validates, generates, and issues the certificate
6. AEMO and participants install the digital certificate
7. (If required), set up your Participant e-Hub Gateway (see page 15).

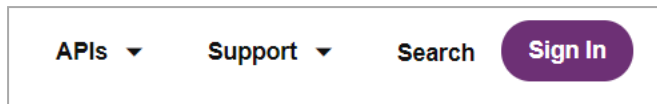
You will need a different Certificate to connect to each environment – pre-production and production.

Access the API Portal

1. Access the API Portal using one of the following URLs:

Pre-production	Production
https://dev.preprod.aemo.com.au	https://dev.aemo.com.au

2. In the top-right corner, click **Sign in**.



Register

The first step to complete before you use the API Portal is to complete the [registration process](#).

Existing participants

Step	Who	What	Requirements/Comments
1	Participant	Contacts Support Hub for access to eHub.	Must be a Registered Participant. For more information on registration, see registration process .
2	Participant	Provides Participant ID	Participant must exist in the NEM.
3	Participant	Request to use an existing certificate for multiple participant IDs. For new certificates, see Obtain a new certificate .	
4	Participant Administrator	Creates a URM user account for the API and grants it access to the API role, by assigning the corresponding entities to Rights and Rights to the user account.	Entity exists in MSATS.
5	Support Hub	Lodges a Support Call for the participant.	Support Hub provides the following information as part of the Support call: <ul style="list-style-type: none"> • IT contact name • IT contact email address • IT contact phone number
6	Integration team	Signs the certificate request.	
7	Integration team	Creates Participant Portal users and API keys (if required)	

New participants

Step	Who	What	Requirements/Comments
1	Participant	Completes the relevant registration forms.	Need Participant id for this process
2	Participant	Provides Participant ID.	
3	Support Hub	Lodges a Support Call for the participant.	Support Hub provides the following information as part of the Support call: <ul style="list-style-type: none"> • IT contact name • IT contact email address • IT contact phone number
4	Integration team	Signs the certificate request.	
5	Integration team	Creates Portal users and API keys (if required)	
6	Integration team	Adds and provides certificate to participant for installation.	Certificate is linked to the ParticipantID.
7	Participant	Tests end-to-end connectivity and troubleshoots as required.	
	Network	Assists participants with testing.	

View the API catalogue

The API catalogue provides a full list of AEMO APIs that you have access to. To view the API Gallery:


1. Access the API Portal. For help, see page [16](#).
2. From the top of the portal, navigate to **APIs > API Docs**.
3. Find the API you want to view and click to view details, for example SelfForecast.

APIs

Explore AEMOs API catalogue below.

[All](#)
[Electricity](#)
[Gas](#)
[Retail](#)
[Wholesale](#)
[Authentication](#)
[Gas Bulletin Board \(GBB\)](#)


[Gas Supply Hub \(GSH\)](#)
[Distributed Energy Resource \(DER\)](#)
[Consumer Data Right \(CDR\)](#)



SelfForecast

Submit Solar or Wind Forecasts to AEMO


[Electricity](#)
[Wholesale](#)



IdentityService

Change a password for a URM account


[Electricity](#)
[Gas](#)
[Authentication](#)



B2BMessagingAsync

Send and receive B2B messages between participants in an asynchronous fashion.


[Electricity](#)
[Retail](#)



B2BMessagingSync

Send and receive B2B messages between participants in a synchronous fashion.


[Electricity](#)
[Retail](#)



B2BMessagingPull

Send and receive B2B messages between participants in a pull messaging pattern.

[Electricity](#)
[Retail](#)



P2PMessagingSync

Exchange Peer-to-peer information via the e-Hub.

[Electricity](#)
[Retail](#)

The following details about the SelfForecast API.

SelfForecast

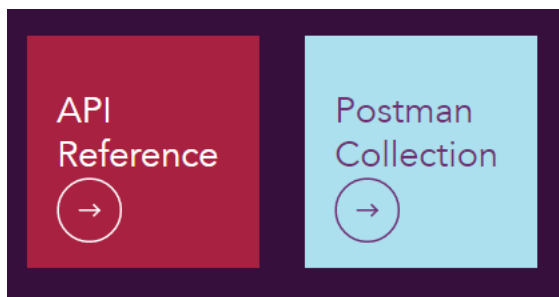
[API Reference](#)
→

[Postman Collection](#)
→

Getting Started >	<h3>Getting Started</h3>
About the API	<h4>About the API</h4> <p>The Self forecasting API is used by participants who wish to submit their Solar or Wind Forecasts for a DUID to AEMO.</p> <p>Market participants can optionally provide dispatch self-forecasts of the unconstrained intermittent generation from their semi-scheduled generating units for use in dispatch. These forecasts are only subject to technical factors, and do not reflect market intentions. Market participants must register with AEMO to submit dispatch self-forecasts.</p>
Getting Access	<h4>Getting Access</h4> <p>All requests to register to submit SFs for one or more semi-scheduled generating units belonging to a Participant ID must be made to AEMO using this application form, and sent from the relevant trading manager for that Participant ID via email to: op.forecasting@aemo.com.au.</p> <p>Subsequent changes to the registration details (including changes to self-forecast providers, forecasting models, participant contact</p>
External Docs	
API Details >	
Authentication Methods	
Base URLs	
Parameters	
API Ref >	

API reference

Click **API Reference** to see the OpenAPI specification and details about the API's resources, paths, and sample code.



You can also this option to download the OpenAPI specification file.

selfForecast
DOWNLOAD SPEC

SELFFORECAST

Overview

PATHS

/SubmitDispatchForecast POST

COMPONENTS

Schemas

- Forecast
- IntervalForecast
- SubmitDispatchForecastPost

selfForecast

Introduction

The Self forecasting API is used by participants who wish to submit their Solar or Wind Forecasts for a DUID to AEMO.

For details on how to get access and business rules for this API:

[View API Docs →](#)

Resource Types

URIs are relative to <https://apis.preprod.aemo.com.au/9319/ws/NEMWholesale/selfForecast/v1>, unless otherwise noted.

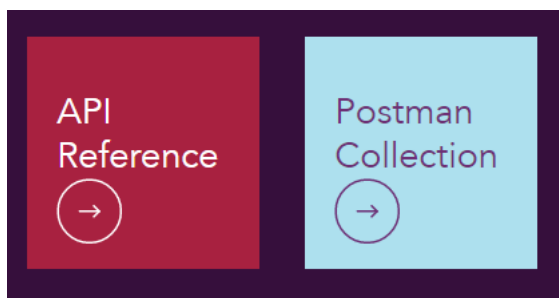
Forecast

For more information, see Forecast.

Method	Endpoint	Description
POST	/SubmitDispatchForecast	Use to submit a dispatch self-forecast. AEMO will use the latest of the highest priority number, unsuppressed submissions as an input to dispatch.

Download Postman Collection

Click **Postman Collection** to download the API Postman collection.



A Postman collection is a group of pre-built API requests that can be organised into folders, and exported and shared with others.

Manage Certificates

In this chapter:

Decide how to use certificates	21
Use an existing certificate	22
Obtain a new certificate	22
Information required for your CSR	23
Send the certificate to AEMO	24
AEMO validates, generates, and issues the certificate	25
AEMO and participants install the digital certificate	25

You will need a different Certificate to connect to each environment – pre-production and production.

Decide how to use certificates

Before obtaining an SSL certificate, determine if you need a new certificate or you can use an existing one.

New e-HUB participants

If you are a new e-HUB participant, you can do one of the following:

- Have one certificate **for multiple** participant IDs.
- Have one certificate **for each** participant ID.

Existing e-HUB participants

If you are an existing e-Hub participant (already having a Certificate), you can do one of the following:

- Request to use an existing certificate **for multiple** participant IDs.
- Have one new certificate **for multiple** participant IDs.
- Have one new certificate **for each** additional participant ID.

For help generating a CSR for your server/operating system, consult your vendor's guide.

Use an existing certificate

To use an existing certificate, send an email to AEMO's [Support Hub](#) with the following information.

Field	Description
To	supporthub@aemo.com.au
From	Participant email
Subject	AEMO e-Hub SSL certificate update
Body	<p>AEMO Support Hub</p> <p>We have an existing SSL certificate with the following Thumbprint: <Thumbprint>.</p> <p>Please update the participant IDs below to use this certificate:</p> <ul style="list-style-type: none"> • <Participant ID 1> • <Participant ID 2> • <Participant ID 3>

Obtain a new certificate

To obtain an SSL certificate, you must generate a Certificate Signing Request (CSR) that identifies your server.

Instructions for generating the CSR depend on your server and operating system.

Information required for your CSR

Before you begin, ensure that you **do not** set the Challenge password. To create a new Certificate-Signing-Request (CSR), you will need to provide the following information.

Requirement	Details
CN (common name)	<p>Preferred Format</p> <p>Using the Organisation ID or Participant ID: <ID>-<PreProd Prod> For example, 30187-PreProd, or REMCO-PreProd</p> <p>If you need to use the same certificate for more than one ID, the name is: <ID1>-<ID2>...<PreProd Prod> For example, NAGMO-REMCO-PreProd, or 30187-30188-PreProd 2.</p> <p>Optional Format</p> <p>A Fully Qualified Domain Name (FQDN) that uniquely identifies the intended environment (PreProd or Prod) and your organisation For example, a1.nonprod-api.yourdomain.com.au</p> <p>The length of the CN field is limited to 64 characters. AEMO can only issue a certificate CN using:</p> <ul style="list-style-type: none"> • Lowercase letters a–z • Uppercase letters A–Z • Digits 0–9 • Special characters: period (.) and hyphen (-)
OU	AEMO will overwrite the OU and remaining fields in the subject attribute.
Public key algorithm	2048 bits RSA
Signature algorithm	SHA-2

Client certificates are issued with 3 years validity, 2048 bits RSA public key and SHA-2 algorithm.

AEMO supports these key usages in a single X.509v3 certificate:

- Digital Signature
- Key Encipherment (a0)

- Server Authentication (1.3.6.1.5.5.7.3.1), and
- Client Authentication (1.3.6.1.5.5.7.3.2)

CSR File

The CSR file contains text that looks similar to the following example. The BEGIN and END lines must be present.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxDTALBgNVBAGMBoMBFV0YWgxDzANBgNV
BACMBkxpbmRvbjEwMBQGA1UECgwNRGlnaUNlcnQgSW5jLjJERMA8GA1UECwwIRGln
aUNlcnQxHTAbBgNVBAMMFV4YW1wbGUuZGlnaWNlcnQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8+To7d+2kPWeBv/orU3LVbJwDrSQbeKamCmo
wp5bqDxIwV20zqRb7APUOKYoVEFFOEqs6T6gImnIo1hbiH6m4zgZ/CPvWB0kZc+c
1Po2EmvBz+AD5sBdT5kzGQA6NbWyZG1dxRthNLOs1ef0hdnWFuhI162qmcflgpiI
WDuwq4C9f+YkeJhNn9dF5+owm8cOQmDrV8NNdiTqin8q3qYAHHJRW28g1JUCZkTZ
wIaSR6crBQ8TbYNE0dc+Caa3DOIkz1EOsHWzTx+n0zKfqcBgXi4DJx+C1bjptYPR
BPZL8DAeWuA8ebudVT44yEp82G96/GgcF7F33xMxe0yc+Xa6owIDAQABoAAwDQYJ
KoZIHvcNAQEFBQADggEBAB0kcrFccSmFDmxox0Ne01UIqSsDqHgL+XmHTXJwre6D
hJSZwbvEt0K0G3+dr4Fs11WuUNT5qcLsx5a8uk4G6AKHMzuhLsJ7XZjgmXGECpY
Q4mC3yT3ZoCGpIXbw+iP3lmEEXgaQL0Tx5LF1/okKbKYwIqNiyKWOMj7ZR/wxWg/
ZDGRs55xuoELDj/ZRFf9bI+IaCUd1YrFYcHI13G87Av+r49YVwqRDT0VDV7uLgqn
29XI1PpVUNCPQgn9p/eX6Qo7vpDaPybRtA2R7XlKjQaF9oXWeCUqy1hvJac9QF02
970b1a1pHPoZ7mWiEuJwjBPii6a9M9G30nUo391Bi1w=
-----END CERTIFICATE REQUEST-----
```

For more information on how to generate a CSR, refer to this DigiCert resource:
<https://www.digicert.com/csr-creation.htm>

Send the certificate to AEMO

Email the CSR file to AEMO's [Support Hub](#) with the following information.

Field	Description
To	suppothub@aemo.com.au
From	Participant email
Subject	CSR request

Field	Description
Attachment	CSR file
Body	<p>AEMO Support Hub</p> <p>Please find attached a Certificate Signing Request (CSR) for signing by the AEMO Certificate Authority.</p> <p>The following Participant ID's will use this certificate:</p> <ul style="list-style-type: none"> • <Participant ID 1> • <Participant ID 2> • <Participant ID 3>

AEMO validates, generates, and issues the certificate

Once received, AEMO:

1. Validates your CSR.
2. Generates the SSL certificate from the CSR.
3. Emails the following SSL certificate details to all involved Participant IDs:
 - a. Participants' public certificate
 - b. e-Hub (production and pre-production) public certificate
 - c. CA certificate

AEMO and participants install the digital certificate

API Gateway

To connect to the API Gateway, participants need:

- Access to MarketNet or the internet. For details about MarketNet, see [Guide to Information Systems](#).
- Their IP address range white listed by AEMO.
- SSL authentication using digital certificates.

Participant API Gateway or system

Participants apply the SSL certificate to their own API Gateway or system.

Participant usernames and passwords expire every 60 days.

This is the username and password that goes in the authorisation header. For help, see [Authentication and authorisation](#).

For help with passwords, see [Guide to Information Systems](#).

Needing Help?

In this chapter:



Developer Portal FAQs

For more information, refer to [API Developer Portal FAQs](#).

AEMO's Support Hub

IT assistance is requested through one of the following methods:

- Phone: 1300 AEMO 00 (1300 236 600)

For non-urgent issues, normal coverage is 8:00 AM to 6:00 PM on weekdays, Australian Eastern Standard Time (AEST).

- Email: supporthub@aemo.com.au

AEMO recommends participants call AEMO's Support Hub for all urgent issues, if you have logged a call in the Customer Portal.

Information to provide

Please provide the following information when requesting assistance from AEMO:

- Your contact details
- Company name
- Company ID
- System or application name
- Environment: production or pre-production
- Problem description
- Screenshots

For AEMO software-related issues please also provide:

- Participant ID (if Data Interchange (DI) problem)
- Version of software
- Properties or log files
- PDR Monitor support dump and DI instance name (if DI problem)

Feedback

To suggest improvements to this document, please contact the [AEMO's Support Hub](#).

Related resources

API Portal: API resources and documents, including OAS (Swagger) files.

B2B SMP Technical Guide: Details about using the MSATS B2B e-Hub.

Connecting to AEMO's IT Systems: Details and URLs for connecting to AEMO's IT Systems.

Guide to Information Systems: Information about AEMO's participant IT systems.

Guide to User Rights Management: Assisting participant administrators (PAs) to use the user rights management functions available in AEMO's web portals.

OpenAPI-Specification: <https://github.com/OAI/OpenAPI-Specification>: Guidelines and examples of the OpenAPI Specification.

Glossary

AEMC

Australian Energy Market Commission

AEMO

Australian Energy Market Operator

AEMO API Gateway

The gateway on AEMO's side providing participant communication options, accessible over the internet or MarketNet. It uses resources and methods to push messages to Participants' API Gateways .

AES

Advanced Encryption Standard

AEST

Australian Eastern Standard Time

API

Application Programming Interface. A set of clearly defined methods of communication between various software components.

API Portal

Where you can view available APIs, manage your API Keys, and obtain OAS files.

API Protocol

An e-Hub delivery method.

aseXML

A standard developed by Australian energy industries to facilitate the exchange of information between energy industry participants using XML.

BB

Bulletin Board

CSR

Certificate Signing Request is a block of encoded text given to a Certificate Authority when applying for an SSL Certificate. It also contains the Public Key to include in the certificate. Usually, a Private Key is created at the same time, making a Key Pair.

csv

Comma-separated values; a file format for exchanging data.

CSV

Comma-separated values; a file format for exchanging data.

Curl

A command line utility used to interact with REST API endpoints.

DWGM

Declared Wholesale Gas Market (Victoria)

e-Hub

Consists of the API Portal and the API Gateway for both electricity and gas.

EMMS

Wholesale Electricity Market Management System; software, hardware, network and related processes to implement the energy market.

Endpoint

Where the API request is sent and where the response comes from.

energy market systems web portal

Single web portal interface to access AEMO's IT systems.

FCAS

frequency control ancillary services

FTP

File transfer protocol; a standard network protocol used for the transfer of computer files between a client and server on a computer network.

Header Parameters

Parameters included in the request header.

Implementation date

Usually one business day before the effective registration date of a registration change. Upon special request, AEMO may agree to implementation two business days before the effective registration date, given sufficient notice time to comply with the Rules and Change Management Procedures.

Interactive entity

Web-based

IPWAN

Internet protocol wide area network

Key Pair

SSL uses a technique called public-key cryptography, based on the concept of a Key Pair. The Key Pair consists of encrypted Public and Private Key data. It is only possible to decrypt the Public Key with the corresponding Private Key.

LAN

Local area network

MACK

Message Acknowledgement

MarketNet

AEMO's private network available to participants having a participant ID

Markets Portal

Web portal for access to AEMO's wholesale web-based applications.

Method

The allowed operation for a resource, e.g. GET, POST, PUT, DELETE, and so on. These operations determine whether you're reading information, creating new information, updating existing information, or deleting information.

MNSP

Market Network Service Provider

MSATS

Retail Market Settlement and Transfer Solution

MSATS Web Portal

MSATS web-based interactive interface

MW

Megawatt

NACK

Negative Acknowledgement (Rejection)

NEM

National Electricity Market

NER

National Electricity Rules

NGERAC

National Gas Emergency Response Advisory Committee

NGR

National Gas Rules

NMI

[electricity] National Metering Identifier

OAS

OpenAPI specification

OpenAPI specification document

The file, either in YAML or JSON, describing your REST API. Follows the OpenAPI specification format.

PA

Participant Administrator who manages participant company's user access and security. The initial PA is set up by the AEMO system administrator as part of the registration process.

Parameters

Parameters are options you pass with the endpoint (such as specifying the response format or the amount returned). There are four types of parameters: header parameters, path parameters, query string parameters, and request body parameters. The different types of parameters are often documented in separate groups on the same page. Not all endpoints contain each type of parameter. See Parameters for more details.

Participant API Gateway

The interface implemented by participants where AEMO pushes messages.

Participant File Server

The publishing point from AEMO systems to participant systems. Each participant is allocated an account and access to private and public areas. Participants are responsible for interfacing with the Participant File Server. If uncollected, files are moved to the archive folder after a couple of days. If your Data Interchange environment is configured properly it automatically retrieves the missing files from the archive. Files are kept in the archive for approximately six months. AEMO's production and pre-production environments are independently operated, so each environment has its own IP address for its Participant File Server. For help, see Connection to AEMO's IT Systems.

Participant ID

Registered participant identifier

Participant User ID

The user ID you used to login to the system.

Participant Users

Set up by the company's Participant Administrator.

PASA

Projected Assessment of System Adequacy

Path parameters

Parameters in the path of the endpoint, before the query string (?). Path parameters are usually set off within curly braces.

Payload

The data sent by a POST request. The Payload section sits after the header.

PID

Participant ID

POP

Point of presence (in network)

Pre-production

AEMO's test system available to participants

Private Key

The secret Private Key is a text file used initially to generate a Certificate Signing Request (CSR), and later to secure and verify connections.

Production

AEMO's live system

Public Key

The Public Key is included as part of your SSL certificate, and works together with your Private Key to make sure your data is encrypted. The Public Key (i.e. the certificate) can verify the digital signature is authentic without having to know the secret Private Key.

Query String Parameters

Parameters in the query string of the endpoint, after the ?.

RDBMS

Relational database management system

Request

The way information is returned from an API. In a request, the client provides a resource URL with the proper authorization to an API server. The API returns a response with the information requested.

Request Body Parameters

Parameters in the request body. Usually submitted as JSON.

Response

The information returned by an API after a request is made. Responses are usually in JSON or XML format.

Response Example

The response example shows a sample response from the request example; the response schema defines all possible elements in the response. The response example is not comprehensive of all parameter configurations or operations, but it should correspond with the parameters passed in the request example. The response lets developers know if the resource contains the information they want, the format, and how that information is structured and labeled. The description of the response is known as the response schema. The response schema documents the response in a more comprehensive, general way, listing each property that could possibly be returned, what each property contains, the data format of the values, the structure, and other details.

REST

The Representational State Transfer API architecture

Rules

The National Electricity or Gas Rules.

SCADA

Supervisory Control and Data Acquisition

SRA

Settlements Residue Auction

SSL

Secure Sockets Layer, cryptographic protocol providing API communication security

STTM

Gas short term trading market

Swagger

Refers to the OpenAPI specification

Swagger File

The OpenAPI Specification (OAS) definition of the API.

TACK

Transaction Acknowledgement

TLS

Transport Layer Security, cryptographic protocol providing API communication security

URM

User Rights Management; see the Guide to URM on AEMO's website

VPN

Virtual Private Network

zip

The file compression format used for exchanging data with AEMO.

ZIP

The file compression format used for exchanging data with AEMO.

Index

2

200 11

4

400 11

401 11

404 11

405 11

5

500 11

503 11

A

API Gateway 3

API Web Portal 3

B

Basic Authentication 13

C

Certificate Signing Request (CSR) 22

CN (common name) 23

Connection timeout 13

CSR file 24

D

DELETE 10

G

GET 10

Glossary 30

H

HTTP 13

HTTP response code 11

HTTPS protocol 5

I

Invalid credentials 11

O

one certificate for each participant ID 21

one certificate for multiple participant IDs 21

one new certificate for each additional
participant ID 22

OU 23

P

POST 10

Public key algorithm 23

R

Read timeout 13

response Payload 11

RESTful 4

S

Signature algorithm 23