



One Identity Manager 9.1.3

API Development Guide

**Copyright 2024 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

**Patents**

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal/trademark-information.aspx](http://www.OneIdentity.com/legal/trademark-information.aspx). All other trademarks are the property of their respective owners.

**Legend**

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager API Development Guide  
Updated - 29 April 2024, 11:43

For the most recent documents and product information, see [Online product documentation](#).

# Contents

<b>About this guide</b>	<b>5</b>
<b>Basic principles of API development</b>	<b>6</b>
API Server basics	6
General information about the API Server	7
Calling the API Server web interface	7
Encryption	7
General notes on programming your own API methods	7
Guidelines and conventions	8
Handling of API Server queries	8
Authentication	10
Configuring authentication	10
Authentication (primary)	11
Logging out	11
Session status and security tokens	12
Querying session status	12
API methods	12
Entity methods	12
User-defined methods	18
SQL methods	18
HTTP methods	19
Date formats	19
Parameter formats	19
Path parameters	19
Query parameters	20
Response formats	20
Response codes	21
Avoiding deadlocks	21
<b>Examples and help – Software Development Kit</b>	<b>22</b>
<b>Implementing your own APIs</b>	<b>23</b>
Managing API plug-ins	23

Creating API plug-ins .....	24
Editing API plug-ins .....	25
Compiling TypeScript API clients .....	25
Adding APIs to One Identity API projects .....	26
Creating API projects .....	28
Adding APIs to your own API projects .....	28
<b>ImxClient command line program .....</b>	<b>29</b>
Starting the ImxClient command line program .....	29
ImxClient command overview .....	29
check-translations .....	30
compile-api .....	31
compile-app .....	32
connect .....	33
edit-config .....	33
fetch-files .....	34
get-apistate .....	35
get-filestate .....	36
help .....	37
inject-package .....	37
install-apiserver .....	38
push-files .....	39
repl .....	40
run-apiserver .....	40
start-update .....	42
workspace-info .....	42
<b>About us .....</b>	<b>44</b>
Contacting us .....	44
Technical support resources .....	44
<b>Index .....</b>	<b>45</b>

# About this guide

This guide explains the API Server's functionality, how you program API calls, and add your own API methods to One Identity Manager.

## Available documentation

The online version of One Identity Manager documentation is available in the Support portal under [Technical Documentation](#). You will find videos with additional information at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity).

# Basic principles of API development

HTML applications use the API Client to communicate with the One Identity Manager API. The API Client controls all network access on the API Server.

The most important components for developing your own APIs are:

- **API projects:** An API project represents the actual application and provides API methods. Various API projects are supplied with One Identity Manager, for example the Web Portal (**portal**).
- **API plug-ins:** An API plug-in serves as a container for custom extensions. With an API plug-in, you can deploy your own API projects and/or add more API methods to existing API projects.
- **API Provider:** An API provider is a single class in a DLL file that declares API methods.

## Detailed information about this topic

- [API Server basics](#) on page 6
- [Guidelines and conventions](#) on page 8

## API Server basics

In this chapter you will find basic information about the API Servers architecture, which is important for custom programming with your own API methods.

## Detailed information about this topic

- [General information about the API Server](#) on page 7
- [Calling the API Server web interface](#) on page 7
- [Encryption](#) on page 7
- [General notes on programming your own API methods](#) on page 7

# General information about the API Server

- The API Server deploys the API.
- The API Server is implemented using the Owin Platform (see <http://owin.org/>).
- URLs are case sensitive.

## Calling the API Server web interface

From the API Server's web interface you can:

- Configure the API Server.
- Call the swagger documentation for your API.
- Open the Operations Support Web Portal.
- Call all installed web applications.

### **To call the API Server web interface**

- In a web browser, open the webpage (URL) of your API Server.

## Encryption

The API Server stores data securely encrypted on the client.

The certificate is configured when the API server is installed on the IIS. For more information on installing the API Servers, see the *One Identity Manager Installation Guide*.

For more information about configuring encryption, see the *One Identity Manager Web Application Configuration Guide*.

## General notes on programming your own API methods

- Because the API Server is stateless, save the API methods without a client specific state.  
For example, you cannot, therefore, define global variables or store session object status data. When the API Server processes are restarted, these values are not restored.
- After enabling routes, you cannot change the definition objects anymore.

- Use asynchronous code for defining API methods. This supports more efficient usage of server resources and improves performance of the system under load. The methods of the API and the underlying object model convert this asynchronicity using the Task-based Asynchronous Pattern (TAP). For more information about TAP, see <https://docs.microsoft.com/de-de/dotnet/standard/asynchronous-programming-patterns/task-based-asynchronous-pattern-tap>.
- Do not use the **HttpContext.Current** method when you define API methods. You can query the current HTTP requirements with the **QBM.CompositionApi.OwinRequestScopeContext.Context.Current** static method.
- If you define API methods that modify data, do NOT use the **GET** method.

## Guidelines and conventions

In this chapter, you will find general policies and conventions, which you must take into account when you create an API.

### Detailed information about this topic

- [Handling of API Server queries](#) on page 8
- [Authentication](#) on page 10
- [Session status and security tokens](#) on page 12
- [API methods](#) on page 12
- [HTTP methods](#) on page 19
- [Date formats](#) on page 19
- [Parameter formats](#) on page 19
- [Response formats](#) on page 20
- [Response codes](#) on page 21
- [Entity methods](#) on page 12
- [Avoiding deadlocks](#) on page 21

## Handling of API Server queries

In this section, you will find information about handling queries that are sent to the API Server.



## Authentication

When a query is sent to the API Server, there is a test to ascertain the success of the primary and, possibly, secondary login in the session for the current project (see [Authentication](#) on page 10).

**NOTE:** This test is not done if the API method used by the query is marked as **AllowUnauthenticated**.

The **imx-session-`<API project name>`** cookie is evaluated to allocate the current session.

If a cookie is passed that cannot be associated with an active session in the current process, the security token in the cookie is used to set up a new session (see [Session status and security tokens](#) on page 12).

If there is no primary login, the API Server tries to establish a database connection through one of the enabled single sign-on authentication modules.

If login cannot be carried out, the process is canceled and the HTTP error code **500** is passed to the client (see [Response codes](#) on page 21).

## Authorizing method access

The API Server checks whether the currently logged in user is authorized to run the method. If the user does not have the required permissions, the process is canceled and the HTTP error code **500** is passed to the client (see [Response codes](#) on page 21).

## Validating the query

The API Server calls the validators stored with the API method one by one. If one fails, the process is canceled and the HTTP error code **400** is passed to the client (see [Response codes](#) on page 21).

## Processing queries (for entity methods)

- GET (loads an entity)
  - Determines the WHERE clause with internal and external filters
  - Loads data from the database
  - Augments an entity with calculated columns
- An entity in delayed-logic mode can be changed with a POST query or deleted with a DELETE query. An entity in this mode is stateless and does not take up any resources on the server after it has been processed.  
Supported HTTP methods:
  - GET (reads an entity)
  - POST (changes an entity)
  - DELETE (deletes an entity)
- An interactive entity must be created once with a PUT query and after that they obtain their own ID. Use the ID in subsequent queries (POST or DELETE).

Supported HTTP methods:

- GET (loads an entity)
- PUT (creates an interactive entity)
- POST (changes an interactive entity)
- DELETE (deletes an interactive entity)

## Authentication

User authentication is carried out on the API Server for each API project.

Running an API method requires prior authentication on an API project. If the API method is marked as `AllowAnonymous`, authentication is not required (you can find an example in the [SDK](#))

Authentication has two steps:

1. Required primary authentication: Default authentication through an authentication module
2. Optional secondary authentication: Multi-factor authentication (by OneLogin)

For more information about configuring authentication, see the *One Identity Manager Web Application Configuration Guide*.

### Detailed information about this topic

- [Authentication \(primary\)](#) on page 11
- [Logging out](#) on page 11

### Related topics

- [Handling of API Server queries](#) on page 8

## Configuring authentication

You can specify how users authenticate themselves on your API. You configure authentication in the API project.

### *To configure authentication*

1. Edit your API project.
2. Create the **SessionAuthDbConfig** class and populate the following properties:
  - a. **Product**: Specify the application with the authentication module that you want to use (for example the **WebDesigner** or the **Manager**),

- b. **SsoAuthenticifiers**: Specify the single sign-on authentication modules to use.
- c. **ExcludedAuthenticifiers**: Specify the authentication modules not to use.

## Authentication (primary)

You can use the **imx/login/<API project name>** API method for primary authentication on the API project.

To do this, use the **POST** HTTP method to send a query containing the following:

```
{ "Module": "RoleBasedPerson", "User": "<user name>", "Password": "<password>" }
```

**TIP:** See the [SDK](#) for examples.

### Security mechanisms

The API Server uses a security mechanism to prevent cross-site request forgery (XSRF) attacks. This randomly generates a token (**XSRF-TOKEN**) and sends it to the client in a cookie at login. The client must then transmit the value of this token in an HTTP header (**X-XSRF-TOKEN**) in each request sent to the server. If this header is missing, the request closes with error code **400**.

**NOTE:** If an API request breaks off with an error and indicates an incorrect CSRF protection cookie, check if your browser accepts the cookies sent by the browser.

**TIP:** You can change the name and path of the cookie and the name of the HTTP header in the Administration Portal. To do this, use the **Name of the cookie containing the CSRF protection token issued by the server** (**XsrfProtectionCookieName**) and **Path for the CSRF protection cookie** (**XsrfProtectionCookiePath**) configuration keys.

You can also disable CSRF protection in the administration portal (**Globally disable CSRF protection tokens** (**XsrfProtectionDisabled**) configuration key). One Identity does not recommend doing this.

For more information about editing configuration keys, see the *One Identity Manager Web Application Configuration Guide*.

## Logging out

You can use the **imx/logout/<API project name>** API method to log out of the API project.

To do this, use the **POST** HTTP method to send a query without content.

# Session status and security tokens

The status a session is saved in a cookie. This cookie contains an encrypted security token which is used to restore a login to the API Server if the API Server was restarted in the mean time. The security token is cryptographically signed by the certificate selected on installation.

**NOTE:** If the API Server's current user restarts the browser, the cookie and its session information are reset.

## Related topics

- [Querying session status](#) on page 12

## Querying session status

You can use the **imx/sessions/<API project name>** API method to query the status of the session. The response contains the following information:

- Permitted authentication module and associated parameters of the respective API project.
- Type of secondary login

## API methods

You can define the following types of API methods.

- Entity methods
- User-defined methods
- SQL methods

## Detailed information about this topic

- [Entity methods](#) on page 12
- [User-defined methods](#) on page 18
- [SQL methods](#) on page 18

## Entity methods

Entity methods work with small parts of the object model in order to read data from the database or write data to the database. When you create an entity method, you only need to enter the table and column name and, if required, a filter condition (WHERE clause).

Internal processing is handled by the API Server. The data schema for the input and output also has a specific format.

For examples for the definition of entity methods, see the [SDK](#) under `Sdk01_Basics\01-BasicQueryMethod.cs`.

## Detailed information about this topic

- [Limiting results](#) on page 13
- [Sort order](#) on page 14
- [Filtering](#) on page 14
- [Grouping](#) on page 15
- [Hierarchical data structure](#) on page 16
- [Additional query parameters](#) on page 17
- [Type-safe classes](#)

## Limiting results

**NOTE:** Entity-based methods normally work with a limit to avoid unintentionally loading extremely large amounts of data.

The following query parameters help you to limit the amount of data that is returned by obtaining multiple data sets from sequential responses:

Query parameter	Default value	Description
PageSize	20	Specifies the maximum number of data sets that can be contained in the response.  If you only determine the total number and do not want to obtains single data sets, use the value <b>-1</b> .
StartIndex	0	Specifies as from which data sets the results are returned in the response.  This parameter is null-based (the first element is addressed with the value <b>0</b> ).

### Example

The following query returns 50 identities and starts with the 101st identity:

`https://<Host-Name>/ApiServer/portal/person?PageSize=50&StartIndex=100`

## Sort order

Use the **OrderBy** query parameter to sort the results returned in an response. This parameter allows you to sort the column names of the underlying database table.

### Examples

The following query returns identities sorted by first name in ascending order:

```
https://<Host-Name>/ApiServer/portal/person?OrderBy=FirstName
```

The following query returns identities sorted by first name in descending order:

```
:https://<host name>/ApiServer/portal/person?OrderBy=FirstName%20DESC
```

## Filtering

Use the **filter** query parameter to filter the results returned in an response. A filter like this consists of a JSON formatted string that must contain the following:

- **ColumnName:** Name of the column used to filter
- **CompareOp:** The operator for comparing the contents of the selected column with the expected value

The following comparison operators are permitted:

- **Equal:** The results only include data sets with column data that matches the comparison value.
- **NotEqual:** The results only include data sets with column data that does NOT match the comparison value.
- **LowerThan:** The results only include data sets with column data less than the comparison value.
- **LowerOrEqual:** The results only include data sets with column data less than or equal to the comparison value.
- **GreaterOrEqual:** The results only include data sets with column data greater than or equal to the comparison value.
- **Like:** Requires the use of a percent sign (%) as a placeholder. You can enter up to two percent signs in this value. The results only include data sets with column data that matches the comparison value pattern.
- **NotLike:** Requires the use of a percent sign (%) as a placeholder. You can enter up to two percent signs in this value. The results only include data sets with column data that does NOT match the comparison value pattern.
- **BitsSet:** The value is compared to the comparison value using the AND (&) logical operator. The result must not be equal to 0.
- **BitsNotSet:** The value is compared to the comparison value using the AND (&) logical operator. The result must be equal to 0.

- **Value1**: Comparison value for comparing the contents of the column
- **Value 2**: If this second comparison value is passed down, the value of **CompareOp** is ignored and all the values that are greater or equal to **Value1** and less or equal to **Value2** are determined.

### Example

The following query returns all identities with the last name "User1":

```
https://<Host-Name>/ApiServer/portal/person/all?filter=[{ColumnName:
'LastName', CompareOp: 'Equal', Value1: 'User1'}]
```

## Grouping

You can use the **group** path parameter to group the results returned in a response. You can use the **by** query parameter to specify which attribute to use for grouping. Furthermore, you can use the **withcount** query parameter to specify (values: **true** or **false**) whether to calculate the number of objects for each group. This may increase the runtime.

**NOTE:** The API method must support grouping (by using the **EnableGrouping** parameter).

The result of the query contains a filter condition that you can pass to the URL parameter as filter.

### Example

The following queries determine the number of identities grouped by primary location:

```
https://<host name>/ApiServer/portal/person/all/group?by=UID_
Locality&withcount=true
```

Response:

```
{
  {
    "Display": "(No value: Primary location)",
    "Filters": [
      {
        "ColumnName": "UID_Locality",
        "CompareOp": 0
      }
    ],
    "Count": 42
  },
  {
    "Display": "Berlin",
```

```

    "Filters": [
      {
        "ColumnName": "UID_Locality",
        "CompareOp": 0,
        "Value1": "c644f672-566b-4ab0-bac0-2ad07b6cf457"
      }
    ],
    "Count": 12
  }
}

```

## Hierarchical data structure

Some data model tables are defined as hierarchical structures (**Department** for example). Data from such tables is loaded from a specific hierarchy level.

You can use the **parentKey** query parameter of the parent object to specify the hierarchy level.

### Example

The following query determines the service categories directly below the **Access Lifecycle** service category:

```
https://<host name>/ApiServer/portal/servicecategories?parentKey=QER-f33d9f6ec3e744a3ab69a474c10f6ff4
```

The following query determines the service categories that do not have a parent service category:

```
https://<Host-Name>/ApiServer/portal/servicecategories?parentKey=
```

The following query determines all service categories regardless of their hierarchy:

```
https://<Host-Name>/ApiServer/portal/servicecategories
```

You can use the **noRecursive** path parameter to specify whether the data is queried as a flat list (values: **true** or **false**).

### Example

```
https://<Host-Name>/ApiServer/portal/servicecategories?noRecursive=true
```



## Additional query parameters

You can use the **withProperties** query parameter to specify whether additional information from specific tables columns are returned in the response.

**NOTE:** To enable table columns for these queries, set the **Show in wizards** option in the column properties of the relevant columns in the Designer.

**TIP:** You can delimit the names of multiple columns with commas.

### Example

The following query determines the number of all identities and also returns their preferred name and title:

https://<host name>/ApiServer/portal/person/all?withProperties=PreferredName,Title

Response:

```
{
  "TotalCount": 105950,
  "TableName": "Person",
  "Entities": [
    {
      "Display": "100, User (USER1)",
      "LongDisplay": "100, User (USER1)",
      "Keys": [
        "bbf3f8e6-b719-4ec7-be35-cbd6383ef370"
      ],
      "Columns": {
        "DefaultEmailAddress": {
          "Value": "USER1@qs.ber",
          "IsReadOnly": true
        },
        "IdentityType": {
          "Value": "Primary",
          "IsReadOnly": true,
          "DisplayValue": "Primary identity"
        },
        "PreferredName": {
          "Value": "Johnny",
          "IsReadOnly": true
        },
        "Title": {
          "Value": "Dr.",
          "IsReadOnly": true
        },
        "XObjectKey": {
          "Value": "<Key><T>Person</T><P>bbf3f8e6-b719-4ec7-be35-cbd6383ef370</P></Key>",
          "IsReadOnly": true
        }
      }
    }
  ]
}
```

```
}  
    }  
}
```

## Type-safe classes

Type-safe classes allow you to use the database model in a type-safe way. This gives you the following advantages:

- Compiling scripts checks whether the classes used are correct. This allows you to detect spelling mistakes in table and column names early on.
- The development environment can offer auto-completion.
- The column's data type is detected, which prevents type conversion errors.

### To use type-safe classes

1. Edit the corresponding API plug-in (see [Editing API plug-ins](#) on page 25) and proceed as follows:

- Add a reference to the type-safe class library of the corresponding database module (A0B.TypedWrappers.dll for example).

This makes the classes for this module available in the <module name>.TypedWrappers namespace (A0B.TypedWrappers for example).

## User-defined methods

User-defined methods are methods for which you fully define the processing, input, and output data in code. This type therefore offers the greatest flexibility.

For examples for the user-defined methods, see the [SDK](#) under Sdk01\_Basics\03-CustomMethod.cs.

## SQL methods

SQL methods are methods that provide data from a predefined SQL query through the API. Create the parameters of a query as SQL parameters.

For examples for the definition of SQL methods, see the [SDK](#) under Sdk01\_Basics\02-BasicSqlMethod.cs.

### Detailed information about this topic

- [Entity methods](#) on page 12

# HTTP methods

HTTP requests can apply the following HTTP methods:

- **GET**: This method requests data from the application server.
- **PUT**: This method changes data on the application server.
- **POST**: This method creates data on the application server.
- **DELETE**: This method deletes data on the application server.

## Date formats

Date values in requests to change or add objects must be specified in ISO 8601 format in the client's local time zone.

### Example

```
2016-03-19T13:09:08.123Z
```

### Related topics

- [Parameter formats](#) on page 19

## Parameter formats

HTTP requests use the following types of parameters:

- [Path parameters](#)
- [Query parameters](#)

### Related topics

- [Date formats](#) on page 19

## Path parameters

Path parameters extend the URL path. A forward slash is used as the delimiter.

If a query uses a path parameters, they are given in URI format.

### Example

```
https://<host name>/ApiServer/imx/sessions/exampleparameter
```

## Query parameters

Query parameter are appended to the URL with a question mark (?) or an ampersand (&). The first query parameter must be prefixed by a question mark. In this case, you must use the following format:

```
?parameter name=parameter value (for example, ?orderBy=LastName)
```

Subsequent query parameters must be prefixed by an ampersand. In this case, you must use the following format:

```
&parameter name=parameter value (for example, ?sortOrder=ascending)
```

**NOTE:** Unknown query parameters are rejected by the server with error code **400**. This also affects query parameters with incorrect upper and lower case spelling.

### Example

```
https://<host name>/AppServer/portal/person?orderBy=LastName
```

## Response formats

Most API methods return results in JSON format (application/json). Furthermore, there is support for results in CSV and PDF format as long as the result of the respective API method is declared as exportable (with the **AllowExport** flag). Basically, an API method can return results in any format compatible with HTTP.

### *To obtain results in CSV format*

- In the query, set **Accept header** to **text/csv**.

### *To obtain results in PDF format*

- In the query, set **Accept header** to **application/pdf**.

**NOTE:** To obtain results in PDF format, the **RPS** module must be installed on your system.

### Related topics

- [Response codes](#) on page 21

# Response codes

Responses that are sent from the REST API use the following codes. If queries fail, an explanatory error message is displayed.

Response codes	Description
200	Query successful.
204	Query successful. Response has no content.
401	Access not authorized. The session must be authorized first.
404	The given resource could not be found.
405	The HTTP method used is not allowed for this query.
500	A server error occurred. The error message is sent with the response. On the ground of security, a detailed error message is not included in the response. For more information, see the application log file on the server.

## Related topics

- [Response formats](#) on page 20

# Avoiding deadlocks

API development includes a lot of asynchronous code with `async/await` constructs. To avoid deadlocks, use the **`ConfigureAwait(false)`** method for every **`await`** keyword.

For more information, see <https://blog.stephencleary.com/2012/07/dont-block-on-async-code.html> and <https://devblogs.microsoft.com/dotnet/configureawait-faq/>.

## Examples and help – Software Development Kit

To make it easier for you to start developing your API, One Identity provides a Software Development Kit (SDK) with lots of commented code example.

The SDK can be found on the installation medium in the directory QBM\dvd\AddOn\ApiSamples.

## Implementing your own APIs

To implement your own APIs, you can create API plugins.

The API Server loads all DLLs matching the `*.CompositionApi.Server.PlugIn.dll` naming scheme and deploys the API definitions contained therein.

To implement your own APIs, the following options are available:

- You can add an API to a One Identity API project (see [Adding APIs to One Identity API projects](#)).
- You can create your own API project ([Creating API projects](#) on page 28).
- You can add an API to your own existing API projects (see [Adding APIs to your own API projects](#) on page 28).

### Detailed information about this topic

- [Managing API plug-ins](#) on page 23
- [Adding APIs to One Identity API projects](#) on page 26
- [Creating API projects](#) on page 28
- [Adding APIs to your own API projects](#) on page 28

## Managing API plug-ins

With the help of API plug-ins, you can implement and use your own customized APIs and API projects.

Prerequisites:

- You use a version management system (for example, Git).
- You use an Integrated Development Environment (IDE).

## Detailed information about this topic

- [Creating API plug-ins](#)
- [Editing API plug-ins](#)
- [Compiling TypeScript API clients](#) on page 25

# Creating API plug-ins

To implement your own customized APIs and API projects, you can create API plug-ins.

### To create an API plug-in

1. Start your IDE (such as Visual Studio).
2. Create a new .NET Framework 4.8 project with a name that complies with the format: `<project name>.CompositionApi.Server.Plugin`.
3. Add references to the following DLL files from the One Identity Manager installation directory:
  - QBM.CompositionApi.Server.dll
  - VI.Base.dll
  - VI.DB.dll
4. Create the API code.
5. Compile the DLL file in your IDE.
6. Copy the DLL file to the bin subdirectory of your IIS installation.
7. Import the DLL file into your One Identity Manager database using the Software Loader and assign it to the **Business API Server** machine role. For more information on importing files using the Software Loader, see the *One Identity Manager Operational Guide*.
8. Copy the DLL file to the One Identity Manager install directory.
9. Import the DLL file into your One Identity Manager database using the Software Loader and assign it to the **Development and Testing** machine role. For more information on importing files using the Software Loader, see the *One Identity Manager Operational Guide*.
10. Restart the API Server and ensure that the `<project name>.CompositionApi.Server.Plugin` file exists in the bin folder of the API Server install directory.
11. Compile the appropriate TypeScript API client (see [Compiling TypeScript API clients](#) on page 25).



# Editing API plug-ins

You can edit existing API plug-ins.

## **To edit an existing API plug-in**

1. Start your IDE (such as Visual Studio).
2. Open an existing .NET Framework 4.8 project.
3. Edit the API code.
4. Compile the DLL file in your IDE.
5. Copy the DLL file to the bin subdirectory of your IIS installation.
6. Import the DLL file into your One Identity Manager database using the Software Loader. For more information on importing files using the Software Loader, see the *One Identity Manager Operational Guide*.
7. Copy the DLL file to the One Identity Manager install directory.
8. Import the DLL file into your One Identity Manager database using the Software Loader. For more information on importing files using the Software Loader, see the *One Identity Manager Operational Guide*.
9. Restart the API Server and ensure that the <project name>.CompositionApi.Server.Plugin file exists in the bin folder of the API Server install directory.
10. Compile the appropriate TypeScript API client (see [Compiling TypeScript API clients](#) on page 25).

# Compiling TypeScript API clients

After you create an API plugin, you need to compile a corresponding TypeScript API client.

## **To compile a TypeScript API client**

1. Open a command line interface (for example, Windows Powershell).
2. In the command line program, go to the One Identity Manager installation directory.
3. Run the ImxClient's **start-update** command (see [start-update](#) on page 42).

### **Example**

```
imxclient start-update
```

4. Run the ImxClient's **compile-api** command (see [compile-api](#) on page 31).

### Example

```
imxclient compile-api /copyapi imx-api-ccc.tgz /packagename imx-api-ccc
```

The dialog to select the database connection is opened.

5. In the dialog, perform one of the following actions:
  - to use an existing connection to the One Identity Manager database, select it in the **Select a database connection** menu.
  - OR -
  - to create a new connection to the One Identity Manager database, click **Add new connection** and enter a new connection.
6. Select the authentication method and, under **Authentication method**, enter the login data for the database.
7. Click **Log in**.
8. Import the `imx-api-ccc` npm package into your TypeScript application.

**TIP:** (Optional) If you want to use another name for the `imx-api-ccc` packet, extend the `remove-local-packages.js` by adding a line for the packet in the list. This ensures that your package is not included in package locking and is always updated from the local source.

### Related topics

- [compile-api](#) on page 31

## Adding APIs to One Identity API projects

You can add your own APIs to One Identity API projects to add customized functionality to One Identity HTML applications. To do this, create an API plug-in, define the API in it and assign the corresponding One Identity API project to the API plug-in.

### *To add an API to a One Identity API project*

1. Create or edit an API plug-in (see [Creating API plug-ins](#) on page 24 or [Editing API plug-ins](#) on page 25) and proceed as follows:
  - a. Create a new class in the API plug-in project. This class represents the so-called API provider.

- b. Declare the class with the interface that belongs to the API project you want to add your API to.

The following One Identity API projects can be added:

**Table 1: Supplied API project**

HTML application name	API project name	Interface to implement
Web Portal	portal	<code>IApiProviderFor&lt;QER.CompositionApi.Portal.PortalApiProject&gt;</code>
Operations Support Web Portal	opsupport	<code>IApiProviderFor&lt;QBM.CompositionApi.Operations.OperationsApiProject&gt;</code>
Administration portal	admin	<code>IApiProviderFor&lt;QBM.CompositionApi.AdminApi.AdminApiProject&gt;</code>
Password Reset Portal	passwordreset	<code>IApiProviderFor&lt;QER.CompositionApi.Password.PasswordPortalApiProject&gt;</code>

- c. Implement the **Build** method of the **IApiProviderFor** interface with the desired API functionality.

**Example**

```
1 public class ExampleApi : IApiProviderFor<QER.CompositionApi.Portal.PortalApiProject>
2
3 {
4     public void Build(IApiBuilder builder)
5     {
6         builder.AddMethod(Method.Define("example")
7             .AllowUnauthenticated()
8             .HandleGet(qr => new DataObject { Message = "Hello world!" }));
9     }
10 }
```

# Creating API projects

You can create your own API projects to add customized functionality to One Identity HTML applications. To do this, copy the **CustomApiProject** sample API project (see [Examples and help – Software Development Kit](#) on page 22), customize it as required, and assign it to an API plug-in.

## *To create your own API project*

1. Copy the **CustomApiProject** sample API project.
2. Make changes to the copied API project as required.
3. Create an API plug-in (see [Creating API plug-ins](#) on page 24) and proceed as follows:
  - In the API plug-in project, create a new class that implements the **IApiProviderFor<name of your API project>** interface. This class represents the so-called API provider.

# Adding APIs to your own API projects

You can add more APIs to your own API projects.

## *To add an API to your API project*

1. Edit the API plug-in (see [Editing API plug-ins](#) on page 25) associated with the API project and proceed as follows:
  - In the API plug-in project, create a new class that implements the **IApiProviderFor<name of your API project>** interface. This class represents the so-called API provider.

# ImxClient command line program

You can use the ImxClient command line tool to run different functions for managing the API Server and files on the command line.

## Detailed information about this topic

- [Starting the ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

## Starting the ImxClient command line program

You can start the ImxClient command line tool at any time using any command line interface.

### *To start the ImxClient command line program*

1. Open a command line interface (for example, Windows Powershell).
2. In the command line program, go to the One Identity Manager installation directory.
3. Run the ImxClient.exe application.

## ImxClient command overview

The following chapters contain a list of all ImxClient commands that you can run.

## Detailed information about this topic

- [check-translations](#) on page 30
- [compile-api](#) on page 31
- [compile-app](#) on page 32
- [connect](#) on page 33
- [edit-config](#) on page 33
- [fetch-files](#) on page 34
- [get-apistate](#) on page 35
- [get-filestate](#) on page 36

- [help](#) on page 37
- [inject-package](#) on page 37
- [install-apiserver](#) on page 38
- [push-files](#) on page 39
- [repl](#) on page 40
- [run-apiserver](#) on page 40
- [start-update](#) on page 42
- [workspace-info](#) on page 42

## check-translations

Searches for captions (multilingual text) with missing translations in a particular folder and its subfolders.

### Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/path <path to folder>`: Specifies the path to the folder you want to check.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`

### Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# compile-api

Compiles the API and saves the result to the database.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`
- `N`: Prevents saving to the database.
- `/modules <module1, module2>`: Specifies which modules are included. If you do not enter anything here, all modules are included. Enter the modules' names, delimited by commas.
- `/clientmodules <module1,module2,...>`: Specifies the modules for which API code is generated. If you do not enter anything here, API code is generated every module. Enter the packages' names, delimited by commas.
- `/packagename <name>`: Specifies the API client package name. The default value is `imx-api`.
- `/copyapi <folder path>`: Specifies where to copy the `imx-api.tgz` to.
- `/nowarn <error1,error2,...>`: Specifies which errors are ignored during compilation. Enter the codes for the warnings, separated by commas.
- `/warnaserror <error1,error2,...>`: Specifies which warnings are displayed as errors during compilation. Enter the codes for the warnings, separated by commas.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# compile-app

Runs HTML5 package compilation.

This command performs the following steps:

1. Runs the **npm install** command in the application folder.
2. Runs the **npm run build** command in the package folder.
3. Creates the output in subdirectory dist  
.The output is stored as a zip file in the database.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`
- `/workspace <path to working directory>`: Specifies the working directory. This folder contains the application to be compiled. This folder normally contains the `package.json` file of the application. If you do not enter anything here, the current directory is used.
- `/app <application project name>`: Specifies which application project to compile. If you do not specify anything here, all application projects are compiled.
- `-D`: Runs debug compilation.
- `-S`: Skips running the **npm install** command in the application folder.
- `-P`: Prevents libraries being built in the application folder.
- `/copyto <file path>`: Saves the result of the compilation as ZIP files in a folder.
- `/exclude <module name>`: Omits packages of a module at compile time (for example, **AOB**).



## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# connect

Establishes a database connection.

If a connection to a database has already been established, this is closed and a new connection is then established.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# edit-config

Configures a trusted source key for an application.

## Parameter

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/path <path to folder>`: Specifies which configuration file to load (for example, the `web.config` file of a web application). The **BaseURL** setting of this configuration file is used to determine the application to create the trusted source key for.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `-T`: Configures a random generated trusted source key for the application.
- `/trustedsourcekey <Trusted Source Key>`: Configures the given trusted source key for the application.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# fetch-files

Loads a specific machine role from the database and saves it in a local folder.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/targets <target1;target2;...>`: Specifies which machine roles you want to use.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even is a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`
- `/workspace <working directory path>`: Specifies the working directory where the files should be placed. If you do not enter anything here, the current directory is used.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# get-apistate

Queries the compilation status of the API in the database.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even is a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.

Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`

- `/branch <compilation branch ID>`: Queries the compilation status of the API saved under this compilation branch.
- `/htmlapp <name of the HTML package>`: Returns data for the specified HTML package.
- `-D`: Returns data for debug assemblies.
- `-R`: Returns data for release assemblies.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# get-filestate

Compares the local file structure with the file structure in the database.

Using the **QBM | ImxClient | get-filestate | NewFilesExcludePatterns** configuration parameter, you can define which files are excluded from the synchronization. This prevents excessive load during synchronization. The `node_modules` and `imx-modules` folders are excluded from the synchronization by default.

You can adjust the configuration parameters in the Designer. Use the following formats when defining the rules:

<https://docs.microsoft.com/en-us/dotnet/api/microsoft.extensions.filesystemglobbing.matcher>

Use the `|` character to delimit multiple entries.

**NOTE:** This configuration parameter is generally only used to exclude new files from the synchronization. Files that already exist in the database are not taken into account.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/targets <target1;target2;...>`: Specifies which machine roles you want to use.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.

- **show**: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
- **fallback** (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- **/factory <target system>**: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`
- **/workspace <directory path>**: Specifies the working directory where the files you want to match are located. If you do not enter anything here, the current directory is used.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# help

Displays a list of available commands.

## Parameters

To view help for a specific command, add the command as a parameter.

Example: `help fetch-files`

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# inject-package

Installs packages from a tgz file into the `node_modules` directory of the working directory.

This is intended to be used only with local, dependency-free packages that do not require a full NPM installation.

## Parameter

Required parameters:

- `/inject <package1>,<package2>,...`: Specifies which packages to install. Enter the packages' names, separated by commas.

Optional parameter:

- `/workspace <working directory path>`: Specifies the working directory where the packages will be installed in the `node_modules` subdirectory. If you do not enter anything here, the current directory is used.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# install-apiserver

Installs an API Server on the local Internet Information Services (IIS).

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/app <application name>`: Specifies which name is used for the application (for example, in the browser's titlebar).
- `/sessioncert <certificate thumbprint>`: Specifies which (installed) certificate is used for creating and verifying session tokens.

**TIP:** For example, to obtain a certificate thumbprint, you can use the **Manage computer certificates** Windows function and find the thumbprint through the certificate's detailed information.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.

- `-u`: Allows insecure HTTP connections to the API Server website. By default, the API Server website can only be opened over an encrypted connection.
- `/site <site name>`: Specifies the website on the IIS under which the web application will be installed. If you do not enter anything, the website is found automatically (normally **Default website**).
- `/searchservice <URL>`: Specifies the application server's URL that the search service you want to use is hosted on.

**NOTE:** If you would like to use the full text search, then you must specify an application server. You can enter the application server in the configuration file at a later date.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# push-files

Saves files that you have changed locally back to the database.

## Parameters

Login parameter:

- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Required parameters:

- `/targets <target1;target2;...>`: Specifies which machine roles you want to use.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`

- `/workspace <folder path>`: Specifies the working directory where the files are located that have been modified and are now to be stored in the database. If you do not enter anything here, the current directory is used.
- `/tag <uid>`: Specifies the change label to use to book the changes. For more information about change labels, see the *One Identity Manager Operational Guide*.
- `/add <file1;file2;...>`: Specifies which new database files are added. Use relative paths.
- `/del <file1;file2;...>`: Specifies which database files are deleted. Use relative paths.
- `-C`: Prevents the saving of changed files and saves only new files, and deletes files from the database.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# repl

Starts the ImxClient command line tool in REPL mode.

In this mode, the following actions are performed in an infinite loop:

- Read commands from **stdin**.
- Forward commands to the relevant plugin.
- Output the results of processing to **stdout**.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

# run-apiserver

Starts or stops a self-hosted API Server.

This command requires a database connection.

## Parameters

Login parameter:



- `/conn <database connection>`: Specifies the database you want to connect to.
- `/dialog <dialog authentication>`: Specifies the dialog authentication.

Optional parameter:

- `/conndialog <option>`: Specifies whether a login window is displayed for the database connection. The following options are possible:
  - `off`: The login window is not shown. If the database is not connected, an attempt is made to establish a connection.
  - `show`: The login window is shown (even if a database is already connected) and the new connection replaces the old one.
  - `fallback` (default): The current database connection is used. If the database is not connected, an attempt is made to establish a connection.
- `/factory <target system>`: Specifies the target system for the connection. Enter this parameter if you want to establish a connection to the application server.  
Example: `QBM.AppServer.Client.ServiceClientFactory`, `QBM.AppServer.Client`
- `-S`: Stops the API Server.
- `/baseaddress <base URL with port>`: Specifies the base URL and port of the web application where the API Server accepts connections.

#### Example

```
/baseaddress http://localhost:8184
```

- `/baseurl <root URL>`: Specifies the web application's URL.

#### Example

```
/baseaddress http://localhost
```

- `/plugin <file name 1, file name 2>`: Loads additional plug-ins from the given files.
- `/htmlmdir <directory>`: Specifies the directory to use to load additional HTML application files and plug-in. This setting is intended for development scenarios.

#### Example

```
/htmlmdir C:\example\imxweb\cpl
```

The **cpl** plug-in is loaded from the C:\example\imxweb\cpl folder instead of the default source.

- -T: Queries the status of the current API Server.
- -B: Locks the console.

### Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

## start-update

Checks if software updates are available. If software updates are found, the software update starts.

### Parameter

Login parameter:

- /conn <database connection>: Specifies the database you want to connect to.

Optional parameter:

- /target <update directory path>: Specifies the installation directory of the software to update. If you do not enter anything here, the current directory is used.
- -C: Only checks if software updates are available. The software update does not start.
- -G: Hides the software update user interface.

### Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

## workspace-info

Queries the state of the Angular working directory (existing applications and last API client update).

## Parameters

Optional parameter:

- `/workspace`: Specifies which working directory to query. If you do not enter anything here, the current directory is used.

## Related topics

- [ImxClient command line program](#) on page 29
- [ImxClient command overview](#) on page 29

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- API development
  - basics 6
- API files 12
- async 21
- authentication 10
  - primary 10-11
  - secondary 10
- await 21

## B

- basics 6

## C

- CLI 29
- code 21
- command line 29
- commandos 29
- ConfigureAwait 21
- conventions 8
- CSV 20
- custom methods 18

## D

- data structure
  - hierarchical 12
- date format 19
- deadlock 21

## E

- entity methods
  - general 12
- examples 22

## F

- filtering 12
- format
  - date 19
  - parameter 19
  - response 20

## G

- grouping 12

## H

- help 22
- HTTP method 19

## I

- ImxClient 29
  - commandos 29
    - check-translations 30
    - compile api 31
    - compile app 32
    - connect 33
    - edit-config 33
    - fetch-files 34

- get-apistate 35
- get-filestate 36
- help 37
- inject-package 37
- install-apiserver 38
- push-files 39
- repl 40
- run-apiserver 40
- start-update 42
- workspace-info 42

- ImxClient command line program
  - start 29

## L

- limit 12
- log out 11
- login 11

## M

- method type 19

## P

- PageSize 12
- parameter format 19
  - query parameter 20
  - URL parameter 19
- PDF 20
- policies 8

## Q

- query
  - authentication 8
  - authorization 8

- processing 8
- validation 8
- query parameter 20

## R

- response 21
- response code 21
- response format 20
- run
  - command line program 29

## S

- SDK 22
- security token 12
- session
  - status 12
- session status
  - inquiry 12
- software development kit 22
- sort by 12
- SQL files 18
- StartIndex 12

## T

- token 12

## U

- URL parameter 19