One Identity Manager

Web Application Configuration Guide

Contents

About this guide

This guide book provides administrators and web developers with information about configuration and operation of One Identity Manager web applications.

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.

Configuring the API Server

You can configure the API Server and its API projects using the Administration Portal.

Detailed information about this topic

Logging in to the Administration Portal

To configure API Server and its API projects, you must log in to the Administration Portal.

To log in to the Administration Portal

1. In the address line of your web browser, enter the web address (URL) of the Administration Portal.

2. On the Administration Portal login page, in the **Authentication** menu, select the authentication type you want to use to log in.

3. In the **User** input field, enter your full user name.

4. In the **Password** field, enter your personal password.

5. Click **Log in**.

Viewing and editing API project configurations

Once you log in to the Administration Portal, you can view the configuration of each API project and edit it using configuration keys.

You can also display all custom changes and undo them if necessary as well as convert local changes into global changes.

TIP: If you want to try out changes on a server, you can apply the changes locally. If you want to apply changes to all API Server, you can make the changes globally.

To edit an API project configuration key

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project that you want to configure.

4. (Optional) To further limit the displayed configuration keys, enter the name of the configuration key in the search field.

5. Click on the name of the configuration key to expand it.

6. Edit the value in the configuration key.

7. Click **Apply**.

8. Perform one of the following actions:

   - If you want to apply the changes locally only, click **Apply locally**.
   - If you want to apply the changes globally, click **Apply globally**.

9. Click **Apply**.

To display all API project customizations

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project to display the changes.

4. Click ▼ (**Filter**).

5. In the context menu, select the **Customized settings** check box.

To discard all changes to an API project

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project with changes you want to discard.

4. Click ⋮ **Actions**.

5. Perform one of the following actions:

   - To discard all globally customized settings, click **Revert all globally customized settings**.

- To discard all locally customized settings, click **Revert all locally customized settings**.

6. In the **Reset Configuration** dialog, confirm the query with **OK**.

To convert local changes into global changes

1. Log in to the Administration Portal (see).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project that has the local changes you want to convert to global changes.

4. Click ⋮ **Actions** > **Convert locally customized settings to global settings**.

5. In the **Convert Locally Customized Settings to Global Settings** pane, click **Convert**.

Configuring authentication

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

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 authentication, see the *One Identity Manager API Development Guide* and the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

Configuring primary authentication with single sign-on

You can configure single sign-on authentication for API projects with the Administration Portal. In this case, a separate request to the **imx/login** method is not required.

Required configuration key:

- **Single sign-on authentication modules** (**SsoAuthentifiers**): Specifies which authentication modules are used for single sign-on.

TO configure primary authentication with single sign-on

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project that you want configure with single sign-on authentication.

4. Expand the **Single sign-on authentication modules** configuration key.

5. Click **New**.

6. In the menu, select the authentication module you want to use.

   TIP: You can specify additional authentication modules. To do this, click **New**.

7. Click **Apply**.

8. Perform one of the following actions:
   - If you want to apply the changes locally only, click **Apply locally**.
   - If you want to apply the changes globally, click **Apply globally**.

9. Click **Apply**.

Configuring multi-factor authentication

You can set up multi-factor authentication with OneLogin for attestations and request approvals.

Prerequisite

- The OneLogin Module is installed and synchronization is set up.

For more information about setting up multi-factor authentication, see the *One Identity Manager Authorization and Authentication Guide*.

To configure multi-factor authentication with OneLogin

1. In the administration portal, set the ServerConfig/ITShopConfig/StepUpAuthenticationProvider configuration key to **OneLogin MFA**.

   a. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

   b. In the navigation, click **Configuration**.

ONE IDENTITY
by Quest

c. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project for which you want to configure multi-factor authentication.

d. Expand the **Request configuration / Step-up authentication provider for terms of use agreement and workflow approval** configuration key.

e. In the menu, select **OneLogin MFA**.

f. Click **Apply**.

g. Perform one of the following actions:

- If you want to apply the changes locally only, click **Apply locally**.

- If you want to apply the changes globally, click **Apply globally**.

h. Click **Apply**.

2. In the API Server's configuration file, add the connection parameters to your OneLogin domain.

a. In the API Server's installation directory, open the `web.config` file.

> NOTE: If the file is encrypted, decrypt it first.

b. In the `<connectionStrings>` section, add the following entry:

```
<add name="OneLogin"
connectionString="Domain=<domain>;ClientId=<clientid>;ClientSecret=<clientSecret>" />
```

- `<domain>` stands for the DNS name of the synchronized OneLogin domain (`OLGAPIDomain.DNSName`).

- `<clientid>` stands for the client ID of the OneLogin application.

- `<clientSecret>` stands for the OneLogin application's security token.

c. Save your changes to the file.

> NOTE: If the file was encrypted beforehand, encrypt it again.

Configuring authentication tokens

Users receive an authentication token after they have been successfully authenticated on a web application. User do not have to repeat the authentication as long as this token is valid.

Required configuration key:

- **Persistent authentication tokens** (**AuthTokensEnabled**): Specifies whether to use persistent authentication tokens that are stored between sessions.

- **Persistent authentication token lifetime (in minutes)** (**AuthTokensLifetimeMinutes**): Specifies how long persistent authentication tokens are valid.

To configure the use of authentication tokens.

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the **imx** API project.

4. Configure the following configuration keys:

   - **Persistent authentication tokens**: Specify whether to use persistent authentication tokens. To do this, activate or deactivate the corresponding check box.

   - **Persistent authentication token lifetime (in minutes)**: Specify how long persistent authentication tokens are valid. Once the token lifetime has expired, the user must authenticate again.

5. Click **Apply**.

6. Perform one of the following actions:

   - If you want to apply the changes locally only, click **Apply locally**.

   - If you want to apply the changes globally, click **Apply globally**.

7. Click **Apply**.

Changing encryption

You can change the encryption used for data by choosing another encryption certificate.

To change the encryption certificate

1. In the API Server's installation directory, open the `web.config` file.

   | NOTE: If the file is encrypted, decrypt it first.

2. Change the value of the `certificatethumbprint` property to the thumbprint of the certificate you want to use.

3. Save your changes to the file.

   | NOTE: If the file was encrypted beforehand, encrypt it again.

General web application configuration

You can make certain settings that affect all web applications.

Detailed information about this topic

- Customize logo on page 12

Customize logo

You can define which logo to use in the web application. The logo is displayed on the login page and in the web application's header. If you do not define a logo the One Identity company logo is used.

Required configuration key:

- **Company logo** (**CompanyLogoUrl**): URL where you will find the image file for the company logo.

To customize the logo

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the **imx** API project.

4. Expand the **Company logo** configuration key.

5. In the **Value** field, enter the logo's URL. Enter the URL in one of the following formats:

    - **https://www.example.com/logos/company-logo.png**

    - **http://www.example.com/logos/company-logo.png**

- **/logos/company-logo.png** (relative to the API Servers base directory)

> TIP: If the logo does not appear, check the configuration of the Content Security Policy using the **Content security policy for HTML applications** configuration key in the **imx** API project.

6. Click **Apply**.

7. Perform one of the following actions:

   - If you want to apply the changes locally only, click **Apply locally**.

   - If you want to apply the changes globally, click **Apply globally**.

8. Click **Apply**.

Configuring the Web Portal

This section describes the configuration steps and parameters that you will require to configure some of the features of the Web Portal.

For more information about the Web Designer, see the *One Identity Manager Web Designer Reference Guide*.

Detailed information about this topic

- Configuring request functions on page 14
- Configuring self-registration of new users on page 15

Configuring request functions

You can configure Web Portal request functions using the **Administration Portal**.

Configuring requesting by reference users

Web Portal users can request products that have a specific identity. This is called requesting by reference user.

Required configuration key:

- **Products can be requested through reference user**(**VI_ITShop_ ProductSelectionByReferenceUser**): Enables or disables the "By reference user" function in the Web Portal.

To configure requesting by reference user

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).

2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project for which you want to set up requesting by reference users.

4. Expand the **Products can be requested through reference user** configuration key.

5. Perform one of the following actions:

   - To enable the "By reference user" function, select the **Products can be requested through reference user** check box.

   - To disable the "By reference user" function, clear the **Products can be requested through reference user** check box.

6. Click **Apply**.

7. Perform one of the following actions:

   - If you want to apply the changes locally only, click **Apply locally**.

   - If you want to apply the changes globally, click **Apply globally**.

8. Click **Apply**.

Configuring self-registration of new users

In the Password Reset Portal, users who are not yet registered have the option to register themselves to use the Web Portal and to create new accounts. Users who self-register, receive a verification email with a link to a verification page. On this page, users can complete registration themselves and then set their initial login password.

NOTE: To use this functionality, new users must supply an email address, otherwise the verification email cannot be sent.

NOTE: For more information about self-registration of new users in the Web Portal and associated attestation process, see the *One Identity Manager Attestation Administration Guide*.

To configure self-registration

1. Start the Designer program.

2. Connect to the relevant database.

3. Configure the following configuration parameters:

   NOTE: For more information about editing configuration parameters in the Designer, see the *One Identity Manager Configuration Guide*.

   - **QER** | **WebPortal** | **PasswordResetURL**: Specify the Password Reset Portal's web address. This URL is used, for example, in the email notification to new users.

- **QER | Attestation | MailTemplateIdents | NewExternalUserVerification**:

  By default, the verification message and link is sent with the **Attestation - new external user verification link** mail template.

  To use another template for this notification, change the value in the configuration parameter.

  > TIP: In the Designer, you can configure the current mail template in the **Mail templates** > **Person** category. For more information about mail templates, see the *One Identity Manager Operational Guide*.

- **QER | Attestation | ApproveNewExternalUsers**: Specify whether self-registered users must be attested before they are activated. A manager then decides whether to approve the new user's registration.

- **QER | Attestation | NewExternalUserTimeoutInHours**: For new self-registered users, specify the duration of the verification link in hours.

- **QER | Attestation | NewExternalUserFinalTimeoutInHours**: Specify the duration in hours, within which self-registration must be successfully completed.

4. Assign at least one identity to the **Identity & Access Governance | Attestation | Attestor for external users** application role.

5. In the API Server's installation directory, open the `web.config` file.

   > NOTE: If the file is encrypted, decrypt it first.

6. In the `<connectionStrings>` section, add the following entry:

   ```
   <add name="QER\Person\PasswordResetAuthenticator\ApplicationToken"
   connectionString="<application token>" />
   ```

   `<Application token>` is the application token that was set when the API Server was installed.

7. In the `<connectionStrings>` section, add the following entry:

   ```
   <add name="sub:register" connectionString="Module=DialogUser;User=<USER>;
   (Password)Password=<PASSWORD>" />
   ```

   - `<USER>` is the user's login name for creating new user accounts.
   - `<PASSWORD>` stands for the user's password.

8. Save your changes to the file.

   > NOTE: If the file was encrypted beforehand, encrypt it again.

Configuring the Application Governance Module

The Application Governance Module allows you to quickly and simply run the onboarding process for new applications from one place using one tool. An application created with the Application Governance Module combines all the permissions application users require for their regular work. You can assign entitlements and roles to your application and plan when they become available as service items (for example, in the Web Portal).

Related topics

Configuring entitlements

To enable employees to view, create, and manage applications as well as approve requests for application products in the Web Portal, you must assign specific application roles to employees.

NOTE: Managing an application involves the following:

- Editing the application's main data and the assigned entitlements and roles
- Assigning entitlements and roles to the application
- Unassigning entitlements and roles from the application
- Deploying the application and associated entitlements and roles
- Undeploying the application and its associated permissions and roles

To assign an application role for application governance to employees

1. Start the Manager program.
2. Connect to the relevant database.
3. Select the **One Identity Manager Administration** category.

4. In the upper navigation pane, click the application role you want to assign to employees:

- **Application Governance | Administrators**: Members of this application role create new applications and manage all applications in the Web Portal.

- **Application Governance | Owners**: If this application role is assigned to an application as an owner application role, the members manage the application in the Web Portal.

- **Application Governance | Approvers**: If this application role is assigned to an application as an approver application role, the members can approve requests for products of this application (if the **BE - Approver of an application** approval procedure is used).

5. In the **Tasks** pane, select the **Assign employees** task.

6. In the **Add Assignments** area, double-click the employees to whom you want to assign the application role.

7. Click 🖫 (**Save**).

Filling application hyperviews

In the Web Portal, an overview is available to users for each application in the form of a hyperview. The **Fill application overview** schedule collects all the data for this hyperview and fills it.

To start the schedule to populate the hyperview

1. Start the Designer program.

2. Connect to the relevant database.

3. In the Designer, select the **Base data** > **General** > **Schedules** category.

4. In the list, select the **Fill application overview** schedule.

5. In the schedule's details pane, click **Start**.

6. Confirm the security prompt with **Yes**.

To edit the schedule for filling the application's hyperview

1. Start the Designer program.

2. Connect to the relevant database.

3. In the Designer, select the **Base data** > **General** > **Schedules** category.

4. In the list, select the **Fill application overview** schedule.

5. In the schedule's details pane, edit the schedule's main data.

   For more information about schedule and their properties, see *One Identity Manager Operational Guide*.

6. Select the **Database** > **Commit to database** menu item and click **Save**.

Configuring the Password Reset Portal

The Password Reset Portal allows users to reset passwords of the user accounts they manage securely.

Configuring Password Reset Portal authentication

Authentication on the Password Reset Portal differs from authentication on the Web Portal. Users can log in to Password Reset Portal using the following options:

- Users use a passcode that they have received from their manager (see Configuring Password Reset Portal login with a passcode on page 19).

- Users answer their personal password questions (see Configuring Password Reset Portal login with password questions on page 20).

- Users use your user name and personal password.

Configuring Password Reset Portal login with a passcode

Users can use the passcode they received from their manager to log in to the Password Reset Portal.

To configure login with a passcode

1. In the API Server's installation directory, open the `imxclient.exe.config` file.

   | NOTE: If the file is encrypted, decrypt it first.

2. Add the following entry:

```
<add name="QER\Person\PasswordResetAuthenticator\ApplicationToken"
connectionString="<API Server application token>"/>
```

3. Save your changes to the file.

   | NOTE: If the file was encrypted beforehand, encrypt it again.

Configuring Password Reset Portal login with password questions

If Web Portal users forget their password, they can login in to the Password Reset Portal with the help of the password questions and set a new password.

To configure the use of password questions.

1. Start the Designer program.
2. Connect to the relevant database.
3. Configure the following configuration parameters:

   | NOTE: For more information about editing configuration parameters in the Designer, see the *One Identity Manager Configuration Guide*.

   - **QER** | **Person** | **PasswordResetAuthenticator** | **QueryAnswerDefinitions**: Specify how many password questions and answers users must enter. Users who do not enter enough or any questions and answers, cannot reset their password.

     | NOTE: The value must not be less than the value in the **QueryAnswerRequests** configuration parameter.

   - **QER** | **Person** | **PasswordResetAuthenticator** | **QueryAnswerRequests**: Specify how many password questions users have to answer before they can reset their password.

     | NOTE: The value must not be higher than the value in the **QueryAnswerDefinitions** configuration parameter.

   - **QER** | **Person** | **PasswordResetAuthenticator** | **InvalidateUsedQuery**: Specify whether users must enter new password questions and answers after successfully resetting their password. In this case, correctly answered questions are deleted.

Recommendations for secure operation of web applications

Here are some solutions that have been tried and tested in conjunction with One Identity Manager tools to guarantee secure operation of One Identity web applications. You decide which security measures are appropriate for your individually customized web applications.

Detailed information about this topic

Using HTTPS

Always run the One Identity Manager's web application over the secure communications protocol "Hypertext Transfer Protocol Secure" (HTTPS).

In order for the web application to use the secure communications protocol, you can force the use of the "Secure Sockets Layer" (SSL) when you install the application. For more information for using HTTPS/SSL, see the *One Identity Manager Installation Guide*.

Disabling the HTTP request method TRACE

The TRACE request allows the path to the web server to be traced and to check that data is transferred there correctly. This allows a trace route to be determined at application level, meaning the path to the web server over various proxies. This method is particularly useful for debugging connections.

> IMPORTANT: TRACE should not be enable in a productive environment because it can reduce performance.

To disable the HTTP request method TRACE using Internet Information Services

- You will find instructions by following this link:

  https://docs.microsoft.com/en-us/iis/configuration/system.webserver/tracing/

Disabling insecure encryption mechanisms

It is recommended that you disable all unnecessary encryption methods and protocols on the grounds of security. If you disable redundant protocols and methods, older platforms and systems may not be able to establish connections with web applications anymore. Therefore, you must decide which protocols and methods are necessary, based on the platforms required.

> NOTE: The software "IIS Crypto" from Nartac Software is recommended for disabling encryption methods and protocols.

> For more information about disabling encryption, see https://www.n-artac.com/Products/IISCrypto.

Detailed information about this topic

- https://blogs.technet.microsoft.com/exchange/2015/07/27/exchange-tls-ssl-best-practices/

- https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc

Removing the HTTP response header in Windows IIS

Attackers can obtain a lot of information about your servers and network by looking at the response header your server returns.

To give attackers a little information as possible, you can remove the HTTP response header in Windows IIS.

To remove the HTTP response header in Windows IIS

- Read the instructions in the following links:

  - https://github.com/dionach/stripheaders
  - https://www.saotn.org/remove-iis-server-version-http-response-header/

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product