One Identity Manager

Web Application Configuration Guide

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 Web Application Configuration Guide
Updated - 26 August 2022, 10:45

Contents

1

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**.

Configuring displaying and editing of API projects

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

In addition, you can display all customizations and undo them if necessary.

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 5).
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 5).
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 5).
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**.

General web application configuration

You can make certain settings that affect all web applications.

Detailed information about this topic

- Customize logo on page 8

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 5).
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**.

4

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

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 5).
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 user 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. Connect to the relevant API Server.
6. In the API Server's installation directory, open the `web.config` file.
7. (Optional) If the file is encrypted, decrypt the file.
8. 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.
9. 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.
10. Save your changes to the file.
11. (Optional) Encrypt the file.

Multi-factor authentication

Multi-factor authentication guarantees better security for logging into web applications. One Identity Manager tools use Starling Two-Factor Authentication for multi-factor authentication.

The following prerequisites must be fulfilled to use Starling Two-Factor Authentication:

- Users must have a registered Starling 2FA token.
- Use of an employee-related authentication module, for example "Person (role-based)"

Starling Two-Factor Authentication takes place after initial database login and is independent of it. At web application level, every access attempt is prevented until Starling Two-Factor Authentication has been completed.

Configuring multi-factor authentication

You can configure multi-factor authentication for web applications.

Required configuration key:

- **Multi-factor authentication(MfaAuthenticationProvider)**: Defines which multi-factor authentication is used.

To set up multi-factor authentication

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 5).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** menu list, select the API project for which you want to set up multi-factor authentication.
4. Expand the **Multi-factor Authentication** configuration key.
5. In the menu, select the authentication module you want to use.
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**.

Logging in without multi-factor authentication

You can specify which users can log in to the web application without multi-factor authentication:

- All users can log in to the web application without multi-factor authentication.
- User with IP addresses from a specific IP address range can log in to the web application without multi-factor authentication.

Required configuration key:

- **Allow access for users who are not registered for multi-factor authentication** (**VI_Common_AccessControl_AllowUnregistered**): Specifies whether users that are not registered for multi-factor authentication are allowed to access the web application.
- **MFA bypass IP address range(MfaAllowListIpAddressRange**): Users with the IP addresses specified here can log in to the web application without multi-factor authentication.

To allow login without multi-factor authentication for all users

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 5).
2. In the navigation, click **Configuration**.
3. In the navigation, click **Configuration**.
4. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the API project that you want configure without multi-factor authentication.
5. Expand the **Allow access for users who are not registered for multi-factor authentication** configuration key.
6. Select the **Allow access for users who are not registered for multi-factor authentication** check box.
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 allow login without multi-factor authentication for specific IP addresses

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 5).
2. In the navigation, click **Configuration**.
3. In the navigation, click **Configuration**.
4. On the **Configuration** page, in the **Show configuration for the following API project** menu, select the **imx** API project.
5. Expand the **MFA bypass IP address range** configuration key.
6. In the **Value** field, enter the corresponding IP addresses/address ranges.

   Example:

   ```
   192.168.0.10 -
   192.168.10.20,192.168.0.*,192.168.0.0/255.255.255.0,192.168.0.0/16,fe
   80::/10,192.168.0.0
   ```

   TIP: You can also give IP addresses in Classless Inter-Domain Routing (CIDR) notation.

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**.

Activating Starling Two-Factor Authentication for the Operations Support Web Portal

On the API Server, you can enable Starling 2FA for the Operations Support Web Portal.

To enable Starling Two-Factor Authentication for the Operations Support Web Portal

1. Start the API Designer program.
2. In the menu bar, click **View** > **Navigation**.
3. In the navigation, click  **API projects**.
4. In the tree view, double-click on the **QBM_OperationsSupport** project.
5. In the definition tree view, right-click (**Authentication**) node.
6. In the context menu, click **Object in extension** > **Add to extension <extension name>** > **Authentication module**.
7. In the menu bar, click **View** > **Node editor**.
8. In the definition tree view, click the newly created **Second authentication factor**.
9. In the Node editor pane, tick the **Second authentication factor** box.
10. In the menu, click **Starling 2FA**.

6

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 on page 17
- Filling application hyperviews on page 18

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. Connect to your API Server
2. Open the `imxclient.exe.config` file with a text editor.
3. Add the following entry:

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

4. Save your changes to the file.
5. (Optional) Encrypt the file.

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/

About us

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