One Identity Manager 9.2

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 - 29 September 2023, 03:26

For the most recent documents and product information, see Online product documentation.

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.

Managing the API Server

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

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**.

Displaying information about the API Server

You can display different information about the API Server. You can display an overview of the API Server that contains any general information and an overview of the plug-ins. In addition, you can display all the packages included in the API Server.

To display an overview of the API Server

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).
2. In the navigation, click **Overview**.

To display all the API Server packages

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 6).
2. In the navigation, click **Packages**.

Viewing and editing API project configurations

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

Detailed information about this topic

- Editing configuration keys on page 7
- Displaying API project custom settings on page 8
- Discarding API project custom settings on page 8
- Converting local changes into global changes on page 9

Related topics

- Configuring API projects and web applications on page 11

Editing configuration keys

You can edit API project configurations with configuration keys.

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 search for a configuration key, 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**.

Displaying API project custom settings

To obtain an overview of customizations that have already been made, you can display all the custom settings of an API project.

To display all API project custom settings

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.

Discarding API project custom settings

You can undo all the custom settings of an API project.

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**.

Converting local changes into global changes

To distribute changes to all API servers that were previously applied only locally to one API Server, you can convert local changes to global changes. This saves the changes in the global configuration file.

To convert local changes into global changes

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 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**.

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.

3

Configuring API projects and web applications

You can make changes to the settings of different API projects (or web applications).

Detailed information about this topic

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 (using 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 on page 12
- Configuring multi-factor authentication on page 12
- Configuring authentication tokens on page 13

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*. For more information about setting up initial synchronization with a OneLogin domain, see the *One Identity Manager Administration Guide for Integration with OneLogin Cloud Directory*.

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**.
    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. Ensure that the authentication data for logging in to the OneLogin domain is available. You can set up the authentication data when the API Server is installed using with the Web Installer or adjust it later. For more information, see the *One Identity Manager Installation Guide*.

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 **API Server** 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**.

Configuring self-registration of new users

In the Password Reset Portal, users who are not yet registered have the option to register themselves and create new user 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 and associated attestation process, see the *One Identity Manager Attestation Administration Guide*.

NOTE: For more information about how users register themselves or create a new user account, see the *One Identity Manager Web Portal User Guide*.

To configure self-registration

1. Start the Designer program.
2. Connect to the relevant database.

3. Configure the following configuration parameters:

   TIP: To find out how to edit configuration parameters in 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. Ensure that an application token exists. You set the application token when installing the API server with the Web Installer. For more information, see the *One Identity Manager Installation Guide*.

   The application token is saved as a hash value in the database in the **QER | Person | PasswordResetAuthenticator | ApplicationToken** configuration parameter and stored encrypted in the `web.config` file of the API Server.
6. Ensure that a user is configured with which the new user accounts can be created. You can set up the user and authentication data when the API Server is installed using with the Web Installer or adjust them later. For more information, see the *One Identity Manager Installation Guide*.

   NOTE: It is recommended to use the **IdentityRegistration** system user. The **IdentityRegistration** system user has the specified permissions required for self-registration of new users in the Password Reset Portal. If you require a custom system user, ensure that it has the necessary permissions. For more information about system users and permissions, see the *One Identity Manager Authorization and Authentication Guide*.

Configuring the 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 configure 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 **API Server** 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 user interface language

You can specify which language setting web applications use for the user interface.

Required configuration key:

- **Use language from profile settings as interface language** (**UseProfileCulture**): Specifies whether the interface language uses the language

selected in the user's profile setting or the browser's language.

To configure the user interface language

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 whose interface language you want to configure.
4. Expand the **Show configuration for the following API project** configuration key.
5. Perform one of the following tasks:
   - To use the language set in the user's profile as the interface language, select the check box.
   - To use the user's browser language as the user interface language, clear the 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**.

Using web applications without menu bar

The so-called "headless" mode allows you to embed web applications or parts of them without a menu bar in your own applications (for example, in an iFrame), provided that they already provide a navigation.

To use a web application in headless mode

Use the format https://<server name>/<application name>/#/headless/ for the URLs that you want to embed into the application.

Example

```
https://ExampleServer/ApiServer/html/qer-app-portal/#/headless/dashboard
```

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**.

Detailed information about this topic

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 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 19
- Filling application hyperviews on page 20

Configuring entitlements

To enable identities to view, create, and manage applications in the Web Portal, and also approve requests for application products, assign the following application roles to the appropriate identities:

- **Application Governance** | **Administrators**
- **Application Governance** | **Owners**
- **Application Governance** | **Approvers**

For more information about application roles and how to assign identities to them, see the *One Identity Manager Authorization and Authentication Guide*.

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

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. You can start the schedule and edit it.

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

Configuring the help desk module/tickets

You can configure the help desk module/tickets via the **Administration Portal**.

For more information about the help desk module/tickets, see the *One Identity Manager Web Portal User Guide* and the *One Identity Manager Help Desk Module User Guide*.

Detailed information about this topic

- Configuring the editable properties for creating tickets on page 20
- Configuring the editable properties of tickets on page 21
- Configuring file types for ticket attachments on page 22

Configuring the editable properties for creating tickets

You can specify which properties users can give when they create tickets.

Required configuration key:

- **Property editors/Primary editable properties/TroubleTicket** (**Server-Config/OwnershipConfig/PrimaryFields/TroubleTicket**): Specifies which properties users can give when creating tickets.

To configure editable properties for creating tickets

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 **Web Portal** API project.
4. Expand the **Properties editors/Primary editable properties/TroubleTicket** configuration keys.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the menu.
    - To change an existing property, select the property in the corresponding menu.
    - To remove a property, Next to the corresponding property, click (**Delete**).
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 editable properties of tickets

You can specify which properties users can change when they edit tickets.

Required configuration keys:

- **Property editors/Editable properties/TroubleTicket** (**Server-Config/OwnershipConfig/EditableFields/TroubleTicket**): Specifies which properties users can modify when editing tickets.

To configure the editable properties of tickets

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 **Web Portal** API project.
4. Expand the **Properties editors/Editable properties/TroubleTicket** configuration keys.
5. You can perform the following actions:

- To add a property, click **New** and select the corresponding property from the menu.
- To change an existing property, select the property in the corresponding menu.
- To remove a property, Next to the corresponding property, click (**Delete**).

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 file types for ticket attachments

You can specify which file types are allowed for ticket attachments. Then users can only attach files of these types to the tickets.

Required configuration key:

- **File types for ticket attachments** (**AttachmentFileTypes**): Specifies which file type are permitted for ticket attachments.

To configure file types for ticket attachments

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 **Web Portal** API project.
4. Expand the **File types for ticket attachments** configuration key.
5. You can perform the following actions:
   - To add a file type, click **New** and enter the file type in the format **.<file extension>** (such as **.png**).
   - To change an existing file type, click in the corresponding input field and change the value.
   - To remove an existing file type, next to the relevant file type, click (**Delete**).
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 software

You can configure software via the **Administration Portal**.

Detailed information about this topic

- Configuring the editable properties of software on page 23

Configuring the editable properties of software

You can specify which properties users can change when they edit software.

Required configuration key:

- **Properties editors/Editable properties/Application** (**Server-Config/OwnershipConfig/EditableFields/Application**): Specify which of the software properties users can edit.

To configure the editable properties of software

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 **Web Portal** API project.
4. Expand the **Properties editors/Editable properties/Application** configuration keys.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the menu.
    - To change an existing property, select the property in the corresponding menu.
    - To remove a property, Next to the corresponding property, click 🗑 (**Delete**).
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 service items

You can configure service items via the **Administration Portal**.

Detailed information about this topic

- Configuring the editable properties of service items on page 24

Configuring the editable properties of service items

You can specify which properties users can change when they edit service items.

Required configuration key:

- **Properties editors/Editable properties/AccProduct** (**Server-Config/OwnershipConfig/EditableFields/AccProduct**): Specify which of the service item properties users can edit.

To configure the editable properties of service items

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 **Web Portal** API project.
4. Expand the **Properties editors/Editable properties/AccProduct** configuration keys.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the menu.
    - To change an existing property, select the property in the corresponding menu.
    - To remove a property, Next to the corresponding property, click (**Delete**).
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 devices

You can configure devices via the **Administration Portal**.

Detailed information about this topic

- Configuring the editable properties of devices on page 25

Configuring the editable properties of devices

You can specify which properties users can change when they edit devices.

Required configuration keys:

- **Editable properties for devices (Computer)** (**VI_Hardware_Fields_PC**): Specifies which properties of computers users can edit.
- **Editable properties for devices (Server)** (**VI_Hardware_Fields_SRV**): Specifies which properties of servers users can edit.
- **Editable properties for devices (Mobilephone)** (**VI_Hardware_Fields_MP**): Specifies which properties of mobile phones users can edit.
- **Editable properties for devices (Tablet)** (**VI_Hardware_Fields_TAB**): Specifies which properties of tablets users can edit.
- **Editable properties for devices (Printer)** (**VI_Hardware_Fields_PR**): Specifies which properties of printers users can edit.
- **Editable properties for devices (Display)** (**VI_Hardware_Fields_MO**): Specifies which properties of monitors users can edit.
- **Editable properties for devices (Default)** (**VI_Hardware_Fields_SRV**): Specifies which properties of default devices users can edit.

To configure the editable properties of service items

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 **Web Portal** API project.
4. Expand the following keys:
    - **Editable properties for devices (Computer)**
    - **Editable properties for devices (Server)**
    - **Editable properties for devices (Mobile phone)**
    - **Editable properties for devices (Tablet)**
    - **Editable properties for devices (Printer)**
    - **Editable properties for devices (Display)**
    - **Editable properties for devices (Default)**
5. You can perform the following actions:

- To add a property, click **New** and select the corresponding property from the menu.
- To change an existing property, select the property in the corresponding menu.
- To remove a property, Next to the corresponding property, click (**Delete**).

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 Password Reset Portal

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

Detailed information about this topic

- Configuring Password Reset Portal authentication on page 26

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 27).
- Users answer their personal password questions (see Configuring Password Reset Portal login with password questions on page 27).
- Users use your user name and personal password.

Detailed information about this topic

- Configuring Password Reset Portal login with a passcode on page 27
- Configuring Password Reset Portal login with password questions on page 27

Configuring Password Reset Portal login with a passcode

NOTE: This step is only required if you are using the ImxClient command line tool to host an API Server locally. For more information about the ImxClient command line tool, see the *One Identity Manager API Development Guide*.

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:

   TIP: To find out how to edit configuration parameters in 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 log in to the Password Reset Portal using their password questions.

     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 log in to the Password Reset Portal.

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

- **QER** | **Person** | **PasswordResetAuthenticator** | **InvalidateUsedQuery**: Specify how many new password questions and answers users must enter after they have successfully logged in to the Password Reset Portal. If this option is enabled, correctly answered password questions are deleted after logging in to Password Reset Portal.

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/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, see here.

Detailed information about this topic

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