One Identity Manager

Web Application Configuration Guide

One Identity Manager Web Application Configuration Guide
Updated - 16 December 2024, 13:07

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.

2

Managing the API Server

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

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** drop-down, 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 API documentation

To obtain additional information about the API and its methods, view the corresponding API documentation.

To display the API documentation in the Administration Portal

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **API documentation**.

To display the API documentation as a JSON file

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. Extend the URL with `/swagger/swagger.json` (example: https://MeinServer/APIServer/swagger/swagger.json).

Related topics

- Configuring display of API documentation on page 42

Managing caches

You can display, empty, and activate/deactivate API Server caches.

Displaying caches

To obtain an overview of the API Server caches, you can display the them.

To display caches

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Caches**.

   TIP: To reload the caches and display the latest information, click **Reload** on the **Caches** page.

Flushing caches

To reset the API Server caches, you can flush them.

To empty the cache

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Caches**.
3. On the **Caches** page, click **Flush all caches**.

Activating and deactivating caches

You can activate and deactivate the use of the API Server's caches.

To deactivate caches

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Caches**.
3. On the **Caches** page, click **Deactivate caches**.
4. In the **Deactivate cashes** dialog, confirm the prompt with **Yes**.

To activate caches

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Caches**.
3. On the **Caches** page, click **Activate caches**.

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.

Related topics

- Configuring API projects and web applications on page 17

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 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 changes to API projects

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 changes to an API project

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the API project to display the changes.
4. Click ▼ (**Filter**).
5. In the **Filter Data** side panel, select the **Customized settings** check box.
6. Click **Apply filter**.

Discarding changes to API projects

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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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**.

Activating or deactivating local changes

You can activate or deactivate applying local changes.

To activate or deactivate applying of local changes

1. In the API Server installation directory, open the `bin\appsettings.json` file.

   NOTE: If the file is encrypted, decrypt it first.
2. Perform one of the following actions:
    - To activate applying local changes, insert the following code:

      ```
      {
         "Settings": {
           "IsStandAlone": "True"
         }
      }
      ```
    - To deactivate applying local changes, insert the following code:

      ```
      {
         "Settings": {
           "IsStandAlone": "False"
         }
      }
      ```

   NOTE: If this code section already exists, change the value of the `IsStandAlone` property accordingly.
3. Save your changes to the file.

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

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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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** side panel, click **Convert**.

Displaying API Server packages

You can display the API Server packages that have been received.

To display all the API Server packages

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Packages**.

Displaying API Server plug-ins

You can display all the API Server plug-ins that are used.

To display all the API Server plug-ins

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Plugins**.

Managing logs

You can display logs, start log monitoring, and download log files.

Related topics

- Configuring logs on page 41

Displaying logs

You can display the API Server's log. This shows you log entries from **Error** level and above.

To display the log

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Logs**.
3. On the new page, click the **Session log** tab.
4. (Optional) To control which log entries are displayed, click ▼ (**Filter**). This allows you to display log entries from a specific time period only.
5. (Optional) To search for specific log entries, enter a search term in the search field.

   TIP: To use regular expression in the search, set the **Use regular expressions** switch to on.
6. (Optional) To display the details of a log entry, click on the corresponding log entry.

Starting log monitoring

To be able to view log entries in real time, you can start log monitoring.

To start log monitoring

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Logs**.
3. On the new page, click the **Live log** tab.
4. (Optional) To control which log entries are displayed, click ▼ (**Filter**). This allows you to display log entries from a specific time period only.
5. (Optional) To search for specific log entries, enter a search term in the search field.

TIP: To use regular expression in the search, set the **Use regular expressions** switch to on.

6. (Optional) To display the details of a log entry, click on the corresponding log entry.

Downloading log files

To keep logs locally on your system, you can download the log files.

To download log files

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Logs**.
3. On the new page, click the **Log files** tab.
4. Click the log file you want to download.

Displaying API Server overview

You can display an overview with general information about 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 9).
2. In the navigation, click **Overview**.

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 installation directory, open the `bin\appsettings.json` file.

   NOTE: If the file is encrypted, decrypt it first.
2. Change the value of the `TokenCertificateThumbprint` 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).

General configuration

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

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*.

Related topics

- Configuring WebAuthn security keys on page 95

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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 drop-down, 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 specify if and how users must authenticate themselves when accepting terms of use, or certifying and approving requests.

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*.

TIP: If you want to use multi-factor authentication with OneLogin, the OneLogin Module must be available and synchronization must be set up.

Required configuration keys:

- **Step-up authentication provider for terms of use agreement and workflow approval** (**StepUpAuthenticationProvider**): Authentication method to be used when accepting terms of use.

To configure multi-factor authentication

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Step-up authentication provider for terms of use agreement and workflow approval** configuration key.
5. In the **Value** drop-down, select the authentication provider you want to use.

   TIP: If you do not want to use authentication, select **No step-up authentication**.
6. (Optional) If you use multifactor authentication with OneLogin (value `OneLoginMFA`), make sure 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*.
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 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 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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, select or clear 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**.

Excluding authentication modules

You can exclude certain authentication modules so that users cannot select them for authentication.

Required configuration keys:

- **Excluded authentication modules** (**ExcludedAuthentifiers**): Specify which authentication modules cannot be used.

To exclude an authentication module

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`Web Portal`** API project.
4. Expand the **Excluded authentication modules** configuration key.
5. You can perform the following actions:
    - To exclude an authentication module, click **Add new** and select the relevant authentication module from the selection list.
    - To include an authentication module again, click (**delete**) next to the corresponding authentication module.
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 CAPTCHAs

To improve the security and reliability of your web applications, configure CAPTCHAs for logging in to these web applications. They allow real users to be distinguished from bots.

Enabling and disabling CAPTCHA login protection

To prevent login attempts by bots or automated requests, you can configure a CAPTCHA test to be required after repeated failed login attempts.

Required configuration keys:

- **CAPTCHA login protection** (**EnableLoginProtection**): Specifies whether CAPTCHA tests are required if repeated login attempts are detected.

To enable or disable the CAPTCHA login protection for all web applications

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **CAPTCHA login protection** configuration key.
5. Perform one of the following actions:
    - To enable CAPTCHA login protection, select the **CAPTCHA login protection** check box.
    - To disable CAPTCHA login protection, clear the **CAPTCHA login protection** 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 CAPTCHA fonts

You can specify which of the fonts stored on the API Server are to be used for generating CAPTCHAs.

Required configuration keys:

- **CAPTCHA fonts** (**CaptchaFonts**): Specifies which fonts are used to generate CAPTCHAs.

To configure the fonts to use for generating CAPTCHAs

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **CAPTCHA fonts** configuration key.
5. In the **Value** field, enter a comma delimited list of the fonts that can be used for generating CAPTCHAs.
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 CAPTCHA characters

You can specify which characters to use for generating CAPTCHAs.

Required configuration keys:

- **Characters used in CAPTCHAs** (**CaptchaAlphabet**): Specifies which characters to use for generating CAPTCHAs.

To configure characters for generating CAPTCHAs

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Characters used in CAPTCHAs** configuration key.
5. In the **Value** field, enter the characters to use for generating CAPTCHAs in sequence.
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 CAPTCHA case sensitivity

To make it easier for users to enter CAPTCHA codes, you can specify whether the codes are case sensitive.

Required configuration keys:

- **CAPTCHA: Do not check upper/lower case** (**CaptchaCaseInsensitive**): Specifies whether to disable case-sensitive checking when CAPTCHA codes are entered.

To enable or disable case checking when entering the CAPTCHA code

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the API project that you want configure with case sensitive checking when entering CAPTCHA codes.
4. Expand the configuration key **CAPTCHA: Do not check upper/lower case**.
5. Perform one of the following actions:
    - To enable case sensitivity checking when entering the CAPTCHA code, clear the **CAPTCHA: Do not check upper/lower case** check box.
    - To disable case sensitivity checking when entering the CAPTCHA code, select the **CAPTCHA: Do not check upper/lower case** 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 fixed CAPTCHA codes

If you are working in test systems, you can avoid having to enter a generated CAPTCHA code each time by defining a fixed CAPTCHA code. If a CAPTCHA code is then required, users can enter this specific code.

NOTE: For security reasons, this setting does not have any effect production environments.

Required configuration keys:

- **CAPTCHA: Fixed CAPTCHA code for testing purposes** (**CaptchaFonts**): Specify which CAPTCHA code to use.

To configure a fixed CAPTCHA code

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the API project that you want to configure with a fixed reCAPTCHA code.
4. Expand the **CAPTCHA: Fixed CAPTCHA code for testing purposes** configuration key.
5. In the **Value** field, enter the fixed CAPTCHA code.
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 reCAPTCHA

By default, web applications use a proprietary CAPTCHA method. To use ReCAPTCHA, you must store the website key and the secret key.

Use the website key (public key) to call the reCAPTCHA service from your web application.

The secret key (private key) authorizes communication between your web application and the reCAPTCHA server to verify the user's response when they solve a reCaptcha in your web application.

Required configuration keys:

- **Website key (public key) for reCAPTCHA integration** (**RecaptchaPublicKey**: Specifies which website key (public key) to use for reCAPTCHA integration.
- **Secret key (private key) for reCAPTCHA integration** (**RecaptchaPrivateKey**): Sepcifies which secret key (private key) to use for the reCAPTCHA integration.

To configure and enable reCAPTCHA

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the API project that you want to configure with reCAPTCHA.

4. Expand the **Website key (public key) for reCAPTCHA integration** configuration key.
5. In the **Value** field, enter the website key (public key).
6. Expand the **Secret key (private key) for reCAPTCHA integration** configuration key.
7. In the **Value** field, enter the secret key (private key).
8. Click **Apply**.
9. 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**.
10. Click **Apply**.

Configuring Content Security Policy

The Content Security Policy enables you to effectively prevent cross-site scripting and other attacks aimed at infiltrating data into your web applications. You can customize the Content Security Policy settings at any time.

Required configuration keys:

- **Content security policy for HTML applications** (**ContentSecurityPolicy**): Specifies which settings are transferred to the content-security-policy header and therefore apply to the Content Security Policy.

To configure Content Security Policy for all web applications

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Content security policy for HTML applications** configuration parameter.
5. In the **Value** field, enter which settings are to be transferred to the content-security-policy header and therefore apply to the Content Security Policy.
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 CORS (Cross-Origin Resource Sharing)

Configure Cross-Origin Resource Sharing (CORS) to enable browsers or web clients to provide API Server content.

Required configuration keys:

- **Allowed sources of requests for CORS(CorsOrigins**): Specifies which sources are allowed to access resources on the API server for Cross-Origin Resource Sharing (CORS).
- **Maximum age of preflight requests for CORS (in seconds)** (**CorsMaxPreflightAgeSeconds**): Specifies how many seconds CORS preflight requests (Cross-Origin Resource Sharing) are valid. The browser sends a preflight request to check whether the server allows a request. After the validity period has expired, the browser sends a new preflight request.

To configure CSP for all web applications

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Allowed request origins for CORS** configuration key.
5. You can perform the following actions:
    - To add a source, click **Add new** and enter the source in the input field.
    - To change an existing source, change the source in the corresponding input field.
    - To remove an existing source, click on (**delete**) next to the corresponding source.
6. Expand the **Maximum age of preflight requests for CORS (in seconds)** configuration key.
7. In the **Value** input field, enter how many seconds CORS preflight requests (Cross-Origin Resource Sharing) are valid.
8. Click **Apply**.
9. 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**.
10. Click **Apply**.

Configuring cross-site request forgery (CSRF)

To protect yourself from cross-site request forgery (CSRF), you can set up different configurations.

Activating and deactivating cross-site request forgery protection

To control cross-site request forgery protection (CSRF) globally, activate or deactivate it.

NOTE: One Identity recommends having CSRF protection activated at all times. To simplify development and testing in their respective environments, you can deactivate CSRF protection, as no special CSRF tokens need to be generated or checked for each request.

Required configuration keys:

- **Globally disable CSRF protection tokens** (**XsrfProtectionDisabled**): Specifies whether CSRF protection is activated or deactivated.

To activate or deactivate CRSF protection

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Globally disable CSRF protection tokens** configuration key.
5. Perform one of the following actions:
    - To activate CSRF protection, clear the **Globally disable CSRF protection tokens** check box.
    - To deactivate CSRF protection, select the **Globally disable CSRF protection tokens** 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 HTTP header with cross-site request forgery protection token

To prevent cross-site request forgery (CSRF) attacks, a token is used that is sent with every request and checked by the server. This ensures that the request comes from a trustworthy source. The token is sent in the HTTP header.

For CSRF protection to work properly, you must define the HTTP header that contains the CSRF protection token.

Required configuration keys:

- **Name of the HTTP header containing the CSRF protection token submitted by the client** (**XsrfProtectionHeaderName**): Defines the HTTP header that contains the CSRF protection token submitted by the client.

To configure HTTP headers with cross-site request forgery protection tokens

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Name of the HTTP header containing the CSRF protection token submitted by the client** configuration key.
5. In the **Value** field, enter the name of the HTTP header that contains the CSRF protection token submitted by the client.
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 HTTP methods without cross-site request forgery protection

Specify which HTTP methods do NOT require cross-site request forgery protection (CSRF).

Typically, actions that trigger data changes or other critical operations should be performed using HTTP methods that provide CSRF protection.

Required configuration keys:

- **HTTP methods which do not require CSRF protection tokens** (**XsrfProtectionDisabledMethods**): Defines which HTTP methods do not require

CSRF protection tokens.

To configure the CSRF protection

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **HTTP methods which do not require CSRF protection tokens** configuration key.
5. In the **Value** field, enter the HTTP methods delimited by commas that do not require CSRF protection tokens.
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 behavior in the event of a cross-site request forgery attack

To configure the behavior in the event of a cross-site request forgery (CSRF) attack, you can specify that user sessions are disconnected as soon as a deviation from the CSRF protection token is detected during a request.

Required configuration keys:

- **End session when a CSRF protection token mismatch is detected** (**XsrfProtectionEndOnMismatch**): Specifies whether the session should end if a mismatch of the CSRF protection token is detected.

To configure the behavior in the event of a CSRF attack

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **End session when a CSRF protection token mismatch is detected** configuration key.
5. Perform one of the following actions:

- To end the session when a deviation from the CSRF protection token is detected, select the **End session when a CSRF protection token mismatch is detected** check box.
- To maintain the session when a deviation from the CSRF protection token is detected, clear the **End session when a CSRF protection token mismatch is detected** 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 cross-site request forgery protection cookie

To ensure that cross-site request forgery (CSRF) protection is implemented effectively, you can configure the CSRF protection cookie.

The CSRF protection cookie is used to store a special token on the client and when required it is sent to the server with requests. This token is then checked by the server to ensure that the request actually comes from the authenticated user and not from a potential attacker attempting to carry out a CSRF attack.

Required configuration keys:

- **Name of the cookie containing the CSRF protection token issued by the server** (**XsrfProtectionCookieName**): Defines the cookie that contains the CSRF protection token issued by the server.
- **Path for the CSRF protection cookie** (**XsrfProtectionCookiePath**): Specifies the URL path that must exist in the requested URL in order to send the cookie header.
- **Domain for the CSRF protection cookie** (**XsrfProtectionCookieDomain**): Specifies the domain whose hosts can receive a cookie.

To configure CSRF protection

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`API Server`** API project.
4. Expand the **Name of the cookie containing the CSRF protection token issued by the server** configuration key.
5. In the **Value** field, enter the name of the cookie that contains the CSRF protection token issued by the server.

6. Expand the **Path for the CSRF protection cookie** configuration key.
7. In the **Value** field, enter the URL path that must exist in the requested URL in order to send the cookie header.
8. Expand the **Domain for the CSRF protection cookie** configuration key.
9. In the **Value** field, enter the name of the domain whose hosts can receive a cookie.
10. Click **Apply**.
11. 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**.
12. Click **Apply**.

Configuring themes

You can configure themes to allow users control over how their web applications are displayed.

Creating and deploying custom themes

To use your corporate design in web applications, create your own custom themes and deploy them for use in web applications. This involves providing a customized version of the default web applications' SCSS file.

To create and deploy a custom theme

1. Set up a working environment for using the GitHub repository. For more information, see the *One Identity Manager HTML5 Development Guide*.
2. In the fork with the source files in the GitHub repository, open the `imxweb\custom-theme\custom-theme.scss` file.
3. Make your changes to the `imxweb\custom-theme\custom-theme.scss` file. Further information on customizing Angular themes can be found here.
4. Change the value of the **$theme-name** variable to the corresponding name of your custom theme (such as `$theme-name: 'company-theme'`).
5. Save the file.
6. In the `imxweb\custom-theme` folder, open a command line prompt.
7. On the command line, run the command **npm run build**.
8. Add the `custom-theme.scss` file to a new ZIP file with the name `Html_<ThemeName>.zip`. Replace `<ThemeName>` with the corresponding name of the theme.
9. Copy the ZIP file to the `bin\imxweb` subfolder of your IIS installation.

10. In the `bin\imxweb` folder, create a new folder with the name `Html_<ThemeName>`. Replace `<ThemeName>` with the corresponding name of the theme.
11. In the newly created folder, create a new JSON file with the name `imx-theme-config.json` and the following parameters:
    - **Name**: Unique identifier of the theme
    - **DisplayName**: Theme name displayed in the web applications
    - **Class**: CSS class ID used for the theme (such as `eui-light-theme` in the default)
    - **Urls**: List of all relevant files for this theme (including images, icons, or other resources that are referenced if required)

    TIP: You can define multiple themes in this file. However, each theme still requires its own ZIP file.

```
{
    "Themes": [
        {
            "Name": "CompanyTheme",
            "DisplayName": "Company Theme",
            "Class": "company-theme",
            "Urls": [
                "../company-theme/custom-theme.css"
            ]
        },
        {
            "Name": "DarkCompanyTheme",
            "DisplayName": "Dark Company Theme",
            "Class": "dark-company-theme",
            "Urls": [
                "../dark-company-theme/custom-theme.css"
            ]
        }
    ]
}
```

12. Use the Software Loader to import the ZIP file and the `imx-theme-config.json` file into your One Identity Manager database.
13. Restart your API Server.

Configuring default themes

To display the web application for users in a certain theme, you can specify a default theme.

Required configuration keys:

- **Default theme** (**DefaultHtmlTheme**): Specifies which theme to use by default.

To configure a default theme

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Default theme** configuration key.
5. In the **Value** drop-down, select which theme to use by default.
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 HTTP response headers

Specify the HTTP headers to add to all responses.

Required configuration keys:

- **HTTP headers** (**HttpHeaders**): Specifies the HTTP headers to add to all the responses.

To configure the HTTP headers

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **HTTP headers** configuration key.
5. In the **Value** field, enter the HTTP headers to add to all responses. Enter each HTTP header on a new line.
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 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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Company logo** configuration key.
5. In the **Value** field, enter the logo 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 API project **API Server** (see Configuring Content Security Policy on page 25).
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 managers

You can specify which identities can be selected as new managers when re-certifying or creating a new user.

Required configuration keys:

- **Identities that can be managers** (**NewManagerWhereClause**): Specify which identities can be selected as new managers.

To configure managers

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Identities that can be managers** configuration key.
5. In the **Value** field, use a WHERE clause to enter which identities can be selected as new managers.
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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 defined in the user profile settings as the interface language, select the **Use language from profile settings as interface language** check box.
    - To use the language defined in the user's browser as the interface language,

clear the **Use language from profile settings as interface language** 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 SameSite cookies

To prevent cross-site request forgery (CSRF), you can configure the SameSite attribute for your ASP.NET session cookies.

Required configuration keys:

- **SameSite cookie setting** (**SameSite**): Specifies which SameSite settings to use for cookies.

To configure SameSite cookies

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`API Server`** API project.
4. Expand the **SameSite cookie setting** configuration key.
5. In the **Value** drop-down, select which type of SameSite setting to use for cookies.
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 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 API Server's web address that deploys the Password Reset Portal. This web address is used for navigation.
   - **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*.

Deleting your own configuration keys

Delete configuration keys that you made yourself.

To delete your own configuration keys

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
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 created the key for.
4. Click ⋮ (**Actions**) > **Delete configuration key**.
5. In the **Delete configuration key** side panel, in the **Configuration key to be deleted** menu, select the configuration key that you want to delete.
6. Click **Delete configuration key**.

Setting the default web application

You can specify which web application to open when users enter the API Server base URL.

Required configuration keys:

- **Name of the default HTML application** (**DefaultHtmlApp**): Specifies which web application starts if the user opens the API Server base URL.

To specify a default web application

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.

4. Expand the **Name of the default HTML application** configuration key.
5. In the **Value** field, enter the name of the web application to open when users enter the API Server base URL (for example, `qer-app-portal` for the Web Portal).
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 support for reverse proxy servers

You can specify whether the API Server supports reverse proxy servers.

Required configuration keys:

- **Run API Server in reverse proxy mode** (**RunReverseProxyMode**): Specify whether the API server is run in a reverse proxy setup.
- **Known reverse proxy servers** (**AllowedReverseProxies**): Specifies which reverse proxy servers accept the X-Forwarded-For HTTP header.

To configure support for reverse proxy servers

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Run API Server in reverse proxy mode** configuration key.
5. Select the **Run API Server in reverse proxy mode** check box.
6. Expand the configuration key **Known reverse proxy servers**.
7. Perform the following actions:
    a. Click **New**.
    b. In the input field, enter the host name of the reverse proxy server (the **X-Forwarded-For** HTTP header value).

    TIP: To add more servers, repeat these steps.

    TIP: To remove a server from the list, click (**delete**) next to the corresponding entry.
8. Click **Apply**.
9. 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**.

10. Click **Apply**.

Configuring URLs for specific APIs

To customize web applications for different systems you can specify a URL to a specific API that web applications use to connect. Only enter a URL here if the clients use a URL other than the base URL of this server to connect to the API.

Required configuration keys:

- **API connection URL** (**ApiConnectionUrl**): Specifies the URL to a specific API that web applications use for connecting.

To specify a default web application

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **API connection URL** configuration key.
5. In the **Value** input field, enter the URL to the API that web applications use for connecting. You can enter the URL as a relative URL (e.g. `/APIConnection`) or a complete URL (e.g. `https://www.example.com/APIConnection`).

   NOTE: Only enter a URL if the clients are to use a URL other than the server's base URL to connect to the API.
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 Administration Portal

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

Configuring logs

You can specify the maximum number of log entries to be saved in the Administration Portal and the maximum age of these log entries.

Required configuration keys:

- **Maximum number of session log entries** (**SessionLogRetentionCount**): Specifies the maximum number of sessions log entries to save.
- **Maximum age of session log entries (in hours)** (**SessionLogRetentionPeriod**): Specifies the maximum length of time to keep the log entries.

To configure logs

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`API Server`** API project.
4. Expand the **Maximum number of session log entries** configuration key.
5. In the **Value** field, enter the maximum number of log entries that can be saved.
6. Expand the **Maximum age of session log entries (in hours)** configuration key.
7. In the **Value** field, enter the maximum length of time to keep the log entries.
8. Click **Apply**.
9. 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**.

10. Click **Apply**.

Configuring display of API documentation

Specify how and whether the API documentation is displayed.

Required configuration keys:

- **Availability of API documentation** (**ApiDocumentation**): Specifies how the API documentation is made available.

To configure the display of API documentation

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Availability of the API documentation** configuration key.
5. From the **Value** drop-down, select how the API documentation is made available:
   - **No API documentation**: API documentation is not shown.
   - **Generate API documentation JSON**: The API documentation is saved as a JSON file and can be accessed via the `/swagger/swagger.json` URL extension (example: https://MeinServer/APIServer/swagger/swagger.json).
   - **Show API documentation in UI**: The API documentation is shown in the Administration Portal (see Displaying API documentation on page 9).
6. In the **Value** drop-down, enter the maximum number of log entries to save.
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**.

Related topics

- Displaying API documentation on page 9

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).

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 Password Reset Portal

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

Configuring Password Reset Portal login using target system user accounts

By default, it is only possible to log in to the Password Reset Portal using password questions or a passcode if you use a central user account. You can configure the Password Reset Portal's authentication module such that log in with the help of password questions or a passcode is also possible using a target system user account (Active Directory user accounts, for example). To do this, enter database tables and columns containing the user names of user accounts that are permitted to log in to the Password Reset Portal. For more information the about Password Reset Portal's authentication module, see the *One Identity Manager Authorization and Authentication Guide*.

To configure login using target system user accounts

1. Start the Designer program.
2. Connect to the relevant database.
3. Set and 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** | **SearchTable**: Enter the name of the database table containing the use names of the user accounts permitted to log in to the Password Reset Portal.
     When a user tries to log in to the Password Reset Portal, this table and the column given under **SearchColumn** are searched for the user names permitted for use.

     Example: `ADSAccount`

     NOTE: This database table must have a foreign key named **UID_Person** that references the **Person** table. This is required to match the user names to the One Identity Manager user accounts.

- **QER** | **Person** | **PasswordResetAuthenticator** | **SearchColumn**: Enter the name of the table column containing the use names of the user accounts permitted to log in to the Password Reset Portal.
  When a user tries to log in to the Password Reset Portal, this column and the table given under **SearchTable** are searched for the user names permitted for use.

  TIP: To enter more than one column, delimit them with the pipe character (|).

  Example: `CN|SamAccountName`
- **QER** | **Person** | **PasswordResetAuthenticator** | **DisabledBy**: (Optional) Enter the name of the Boolean table column that specifies whether a user account is locked. User accounts that are marked as locked (column value: `true`) cannot log in to the Password Reset Portal.

  TIP: To enter more than one column, delimit them with the pipe character (|).

  Example: `Locked|Disabled`
- **QER** | **Person** | **PasswordResetAuthenticator** | **EnabledBy**: (Optional) Enter the name of the Boolean table column that specifies whether a user account is enabled. User accounts that are marked as disabled (column value: `false`) cannot log in to the Password Reset Portal.

  TIP: To enter more than one column, delimit them with the pipe character (|).

  Example: `Active|Enabled`

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 45).
- Users answer their personal password questions (see Configuring Password Reset Portal login with password questions on page 47).
- 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.

Required configuration keys:

- **Login with passcodes** (**EnablePasscodeLogin**): Specifies whether users can log in using passcodes.

To configure login with a passcode

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **Password Reset Portal** API project.
4. Expand the **Login with passcodes** configuration key.
5. Select the **Login with passcodes** 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**.
9. Close the Administration Portal.

   NOTE: The following steps are only necessary if they use the ImxClient command line program to host an API Server locally.
10. Open the API Server installation directory.
11. In the API Server's installation directory, open the `appsettings.json` file.
12. Add the following entry:

```
{
      "ConnectionStrings": {
            "QER\\Person\\PasswordResetAuthenticator\\ApplicationToken":
"<Anwendungstoken>"
      }
}
```

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

13. Save your changes to 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.

Required configuration keys:

- **Login with password questions** (**EnablePasswordProfileLogin**): Specifies whether users can login by answering their password questions.
- **Password questions can be managed** (**VI_MyData_MyPassword_Visibility**): Specifies whether users can manage their password questions and answers.

To configure password questions

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Password Reset Portal` API project.
4. Expand the **Login with password questions** configuration key.
5. Select the **Login with password questions** check box.
6. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
7. Expand the **Password questions can be managed** configuration key.
8. Select the **Password questions can be managed** check box.
9. Click **Apply**.
10. 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**.
11. Click **Apply**.
12. Start the Designer program.
13. Connect to the relevant database.
14. 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.

Excluding passwords from being reset

To prevent users from setting unwanted passwords, you can use the **QER_PasswordWeb_IsAllowSet** script to exclude certain passwords from being reset. User cases for this may be passwords that are calculated from other values or passwords for target systems that are only connected as read-only.

For more information about scripts, see the *One Identity Manager Configuration Guide*.

NOTE: In the **QER_PasswordWeb_IsAllowSet** script, the system user is prevented from resetting the password by default in the following cases:

- If external password management is enabled.
- If the system user is enabled as service account.
- If the system user is used for the automatic software update of One Identity Manager web applications.

To exclude passwords from being reset

1. Start the Designer program.
2. Connect to the relevant database.
3. Copy the **QER_PasswordReset_IsAllowSet** script and customize the copy as required. Use the following parameters for this:
   - UID_Person of the logged in user
   - Key (ObjectKey) of the object to have the password reset option
   - Column names of the password
4. Save the changes.
5. Compile the script.

Settable passwords

Users can set the following default passwords.

Table 1: Password overview

User	Password	Table / Column
Everyone	Own password	Person.DialogUserPassword
Everyone	User account password, which is a. Directly assigned to the logged in identity. - OR - b. Assigned to a sub-identity of the logged in identity. - OR - c. Assigned to a sponsored identity, service identity, or group identity of the logged in identity. - OR - d. Assigned to a shared user account of the logged in identity.	AADUser.Password ADSAccount.UserPassword CSMUser.Password EBSUser.Password GAPUser.Password LDAPAccount.UserPassword NDOUser.Password SAPUser.Password UNSAccountB.Password UNXAccount.UserPassword
Members of the application role **Base roles | Administrators**	Password for individual system users	DialogUser.Password

NOTE: The system user is not suggested for resetting the password in the following cases:

- If external password management is enabled for the system user.
- If the system user is enabled as service account.
- If the system user is used for automatic software updating of One Identity Manager web applications.

These cases are implemented in the `QER_PasswordWeb_IsAllowSet` script, which can be overwritten.

- If the system user is used for role-based login.

In this case, the system user is not accepted by the Password Reset Portal.

Central password

Apart from setting individual passwords in the Password Reset Portal, users can also set the central password. Each user has a central password, with which other passwords can be managed depending on the configuration of the target system.

Defining password dependencies

To specify which password are managed by the central password, use **QER_PasswordWeb_IsByCentralPwd** script to define password dependencies.

For more information about scripts, see the *One Identity Manager Configuration Guide*.

To define password dependencies

1. Start the Designer program.
2. Connect to the relevant database.
3. Copy the **QER_PasswordWeb_IsByCentralPwd** script and customize the copy. Use the following parameters for this:
    - UID_Person of the logged in user
    - Key (ObjectKey) of the object to have the password reset option
    - Column names of the password

    Using this input parameter, the script must return the information regarding whether or not a password is managed by the central password.
4. Save the changes.
5. Compile the script.

Setting a central password

The central password is set separately from other password to prevent problems.

If at least one password of the logged-in user is managed by the central password, the following options are available after logging in to the Password Reset Portal.

a. Setting the central password

b. Setting one or more passwords

If setting one or more passwords, it is possible to set a password managed by the central password. If you want to prevent this, you can exclude the password from being reset.

For more information, see Excluding passwords from being reset on page 48.

Configuring checks for all passwords

Once a user has changed their central password and the user account is linked to other target system accounts, the password can be checked against all the password policies of the connected target systems.

To configure checks for all passwords

1. Start the Designer program.
2. Connect to the relevant database.
3. Set the **QER** | **Person** | **UseCentralPassword** | **CheckAllPolicies** configuration parameter:

   TIP: To find out how to edit configuration parameters in Designer, see the *One Identity Manager Configuration Guide*.

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.

Configuring departments

Use the Administration Portal to configure settings for departments that are managed in the Web Portal.

Enabling or disabling department creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:

- To enable creation, select the check box.
- To disable creation, 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**.

Configuring address books

You can use the Administration Portal to configure Web Portal address book settings.

Showing or hiding organizational charts in the address book

You can specify whether organizational charts are show or hidden in the address book.

Required configuration keys:

- **Show organizational charts in address book** (**ShowOrgChart**): Enables or disables the organizational chart in the address book.

To show or hide organizational charts in the address book

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Show organizational charts in address book** configuration key.
5. Perform one of the following tasks:
    - To show organizational charts in the address book, select the **Show organizational charts in address book** check box.
    - To hide organizational charts in the address book, clear the **Show organizational charts in address book** 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 information in the address book overview

You can specify which information is displayed in the overview of an address book.

Required configuration keys:

- **Fields displayed in the result list in the address book** (**VI_MyData_WhitePages_ResultAttributes**): Specifies which information is shown in the address book overview.

To specify the information in the address book overview

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Fields displayed in the result list in the address book** configuration key.
5. You can perform the following actions:
   - To add a property, click **New** and select the corresponding property from the drop-down.
   - To change an existing property, select the property in the corresponding drop-down.
   - 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 information in the address book entry detail view

You can specify which information is displayed in the detail view of an address book entry. The detail view is displayed as soon as you click on an identity in the address book.

Required configuration keys:

- **Fields displayed in the address book detail view** (**VI_MyData_WhitePages_DetailAttributes**): Specifies which information is displayed in the address book's detail view.

To specify the information in the detail view of an address book entry

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Fields displayed in the address book detail view** configuration key.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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**.

Ansichten konfigurieren

Sie können festlegen, wie Daten auf bestimmten Seiten im Web Portal angezeigt werden sollen.

Configuring default page filters

Define which filters are applied to a page by default.

Required configuration keys (available for various pages):

- **Default filters** (**AdditionalParameters**): Specifies which filters are applied by default.

To configure default page filters

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Default filters** configuration key for the relevant page.
5. In the **Value** input field, enter the internal name of the filter to be used by default and a corresponding value.

   For example, if you want to apply the **Activated attestation policies** filter by default on the **Attestation policies** page so that only activated attestation policies are displayed, use the **View configuration for attestation policies / Default filters** configuration key and, in the **Value** input field, enter the value `OnlyActivePolicies=1`.

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 default grouping of data on pages

You can specify whether and according to which property to group data on a page.

Required configuration keys (available for various pages):

- **Default grouping** (**GroupBy**): Specifies whether and according to which property to group the data.

To configure default grouping of a page

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Default grouping** configuration key for the corresponding page.
5. In the **Value** input field, enter the internal name of the property to use to group the data.

> For example, if you want to group attestation runs on the **Attestation Runs** page according to attestation policies, use the **View configuration for attestation runs / default grouping** configuration key and enter `UID_AttestationPolicy` in the **Value** input field.

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 default sorting of data on pages

You can specify whether and according to which property to sort the data on a page.

Required configuration keys (available for various pages):

- **Standard sorting** (**OrderBy**): Specifies whether and according to which property to sort the data.

To configure the default sorting of a page

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Default sorting** configuration key for the corresponding page.
5. In the **Value** input field, enter the internal name of the property to use for sorting the data. To sort in descending or ascending order, add `ASC` (ascending) or `DESC` (descending) accordingly.

   > For example, if you want to sort the attestations on the **Open attestations** page by descending due date, use the **View configuration for pending attestations / Default sorting** configuration key and enter the `ToSolveTill DESC` in the **Value** input field.

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 optional columns for tables

You can specify which additional columns users can display in the table of a page.

Required configuration keys (available for various pages):

- **Optional columns that can be added to the table** (**OptionalColumns**): Specifies which additional columns users can display in the table.

To configure optional columns for tables

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Optional columns that can be added to the table** configuration key for the corresponding page.
5. Click **Add new** and, in the drop-down, select the relevant column.

   TIP: To change a table column, select a different table column in the corresponding drop-down. To remove a table column, click (**delete**) next to the table column.
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**.

Adding additional information to tables

You can add additional information to individual entries in a table.

Required configuration keys (available for various pages):

- **Additional information per entry** (**AdditionalListColumns**): Specifies which additional information to display for each entry in the table.

To add additional information to a table

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Additional information per entry** configuration key for the corresponding page.
5. Click **Add new** and, from the drop-down, select the property you want to display as additional information.

   TIP: To change a property, in the corresponding drop-down, select another property. To remove a property, click (**delete**) next to the property.
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**.

Adding additional columns to tables

You can add further columns to a table on a page.

Required configuration keys (available for various pages):

- **Additional table columns** (**AdditionalTableColumns**): Specifies which additional columns to display in the table.

To add additional columns to a table

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Additional table columns** configuration key for the corresponding page.
5. Click **Add new** and, in the drop-down, select the relevant column.

   TIP: To change a table column, in the corresponding drop-down, select a different table column. To remove a table column, click (**delete**) next to the table column.
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 application roles

Use the Administration Portal to configure settings for application roles that are managed in the Web Portal.

Enabling or disabling application role creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
   - To enable creation, select the check box.
   - To disable creation, 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**.

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).

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 attestation

Use the Administration Portal to configure settings for attestation.

Configuring recipients of delegated attestation cases

Web Portal users can give an another identity the task of approving an attestation case. This identity is added as approver in the current approval step and approves instead.

Required configuration keys:

- **Recipients of delegated attestation cases** (**AttestationConfig/FilterIdentityApproverInsteadOf**): Specify which identities are given approval of attestation cases through delegation.

To configure recipients of delegated attestation cases

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Recipients of delegated attestation cases** configuration key.
5. In the **Value** field, enter an appropriate WHERE clause.
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 warning threshold of attestation policy objects to attest

You can configure the warning threshold of attestation policy objects to attest. If an attestation policy attests more than the objects specified here, a warning is shown.

Required configuration keys:

- **Warning threshold for affected objects** (**PolicyObjectCountThreshold**): Specifies the warning threshold for objects to be attested in an attestation policy.

To configure the warning threshold for objects to attest

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Warning threshold for affected objects** configuration key.
5. In the **Value** field, enter how many objects can be attested before a warning is shown.
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 authentication by accepting the terms of use

You can specify if and how users must authenticate themselves when accepting terms of use.

Required configuration keys:

- **Step-up authentication provider for terms of use agreement and workflow approval** (**StepUpAuthenticationProvider**): Authentication method to be used when accepting terms of use.

For more information about configuring accepting the terms of use, see Configuring multi-factor authentication on page 18.

You must also enable the **Multi-factor authentication required** property for the corresponding terms of use. For more information about terms of use, see the *One Identity Manager IT Shop Administration Guide* and in *One Identity Manager Attestation Administration Guide*.

Configuring request functions

You can use the Administration Portal to configure Web Portal request function settings.

Limiting products and service categories shown to specific recipients

Specify which service items or service categories are shown to selected request recipients in the Web Portal.

Required configuration keys:

- **Products to be displayed for specific recipients** (**VI_ITShop_Filter_AccProduct**): Specifies which service items are shown to the specific request recipients.
- **Service categories to be displayed for specific recipients** (**VI_ITShop_Filter_AccProductGroup**): Specifies which service categories are shown to the specific request recipients.

To enable or disable navigation in hyperviews

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`Web Portal`** API project.
4. Expand the **Products to be displayed for specific recipients** configuration key.
5. In the **Value** field, use a WHERE clause to enter which products are shown only to specific recipients.

   TIP: Use the **`{0}`** parameter as a wildcard for the list of **UID_Person**.

   Example: `uid_accproduct in ( select uid_accproduct from MyCustomView where uid_person in ( {0} ))`

6. Expand the **Service categories to be displayed for specific recipients** configuration key.
7. In the **Value** field, use a WHERE clause to enter which service categories are shown only to specific recipients.

   TIP: Use the {0} parameter as a wildcard for the list of **`UID_Person`.**

   Example: `uid_accproductgroup in ( select uid_accproductgroup from MyCustomView where uid_person in ( {0} ))`

8. Click **Apply**.
9. 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**.
10. Click **Apply**.

Configuring requests of products recommended from peer group

Web Portal users can request products that have been requested by other identities within your system. Managers can also see products from the peer group of an identity reporting to them.

A peer group contains all the identities that have the same manager or the same primary or secondary department as the request recipient.

Required configuration keys:

- **Products are recommended by peer group analysis** (**ProductSelectionByPeerGroup**): Specifies whether to recommend products when creating a new request by analyzing the recipient's peer group.
- **Product selection for reference user and peer group uses only products and assignments that have been requested** (**ReferenceUserUseRequestedOnly**): Specifies which products and assignments are displayed to users when they make a request using a reference user or the peer group.

To enable or disable requesting of recommended products from the peer group

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Products are recommended by peer group analysis** configuration key.
5. Perform one of the following actions:
    - To enable requesting of recommended products from the peer group, select the **Products are recommended by peer group analysis** check box.
    - To disable requesting of recommended products from the peer group, clear the **Products are recommended by peer group analysis** 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**.

To specify which products and assignments are shown to users

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Product selection for reference user and peer group uses only products and assignments that have been requested** configuration key.
5. Perform one of the following tasks:
    - To show users only products and assignments that have been requested for the reference user or members of the peer group, select the **Product selection for reference user and peer group uses only products and**

assignments that have been requested check box.

- To show users all the products and assignments that are assigned to the reference user or members of the peer group (type is irrelevant), clear the **Product selection for reference user and peer group uses only products and assignments that have been requested** 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 requesting by reference users

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

Required configuration keys:

- **Products can be requested through reference user** (**VI_ITShop_ ProductSelectionByReferenceUser**): Enables or disables the "By reference user" function in the Web Portal.
- **Product selection for reference user and peer group uses only products and assignments that have been requested** (**ReferenceUserUseRequestedOnly**): Specifies which products and assignments are displayed to users when they make a request using a reference user or the peer group.

To enable or disable requesting by reference user

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Products can be requested through reference user** configuration key.
5. Perform one of the following tasks:
   - 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**.

To specify which products and assignments are shown to users

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Product selection for reference user and peer group uses only products and assignments that have been requested** configuration key.
5. Perform one of the following tasks:
   - To show users only products and assignments that have been requested for the reference user or members of the peer group, select the **Product selection for reference user and peer group uses only products and assignments that have been requested** check box.
   - To show users all the products and assignments that are assigned to the reference user or members of the peer group (type is irrelevant), clear the **Product selection for reference user and peer group uses only products and assignments that have been requested** 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 recipients of delegated requests

Web Portal users can give an another identity the task of approving a request. This identity is added as approver in the current approval step and approves instead.

Required configuration keys:

- **Recipients of delegated requests** (**ServerConfig/ITShopConfig/FilterIdentityApproverInsteadOf**): Specify which identities are given approval of requests through delegation.

To configure recipients of delegated requests

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Recipients of delegated requests** configuration key.
5. In the **Value** field, enter an appropriate WHERE clause.
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 missing user account as optional product

Every time you request a system entitlement, you can specify whether the system checks if the recipient has a user account for this target system. If not, you can specify whether a user account is offered with the request.

Required configuration keys:

- **Display missing user accounts as optional products** (**RequestMissingAccounts**): Specifies whether the system checks if the recipient has a user account for the target system every time a system entitlement is requested. If not, whether a user account is offered with the request.

To enable or disable offering missing user accounts as optional products

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Display missing user accounts as optional products** configuration key.
5. Perform one of the following actions:
    - To enable offering missing user accounts as optional products, select the **Display missing user accounts as optional products** check box.
    - To disable offering missing user accounts as optional products, clear the **Display missing user accounts as optional products** 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**.

Linking service categories and products

To direct others to a specific service category or product on the Web Portal request page, you can link to the relevant service category or product using the `/#/newrequest/allProducts?serviceCategory=<UID-of-service-category>` or the `/#/newrequest/allProducts?serviceItem=<UID-of-service-item>` URL parameter.

Configuring delegation

Use the Administration Portal to configure the settings for delegating responsibilities in the Web Portal.

Enabling or disabling global delegation

Specify whether users can delegate multiple responsibilities that are grouped together in sets (global delegations). Users then select responsibilities grouped by topic instead of individual responsibilities in order to delegate them.

Required configuration keys:

- **Sets of responsibilities can be delegated (global delegations)** (**EnableNewDelegationSubstitute**): Specifies whether users can delegate responsibilities grouped by topic.

To enable or disable global delegations

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Sets of responsibilities can be delegated (global delegations)** configuration key.
5. Perform one of the following actions:
    - To enable global delegations, select the **Sets of responsibilities can be delegated (global delegations)** check box.

- To disable global delegations, clear the **Sets of responsibilities can be delegated (global delegations)** 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**.

Enabling or disabling individual delegations

Specify whether users can delegate individual responsibilities (individual delegations).

Required configuration keys:

- **Individual responsibilities can be delegated (individual delegations)** (**EnableNewDelegationIndividual**): Specifies whether users can delegate certain individual responsibilities.

To enable or disable individual delegations

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Individual responsibilities can be delegated (individual delegations)** configuration key.
5. Perform one of the following actions:
   - To enable individual delegations, select the **Individual responsibilities can be delegated (individual delegations)** check box.
   - To disable individual delegations, clear the **Individual responsibilities can be delegated (individual delegations)** 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 your own API filter

To restrict the number of objects returned by a specific API endpoint, you can create, edit, and delete your own filter conditions.

Creating your own API filters

To restrict the number of objects returned by a specific API endpoint, you can create your own filter conditions.

To create your own API filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Click ⋮ (**Actions**) > **Create configuration key**.
5. In the **Create configuration key** side panel, in the drop-down, select the `API method configuration` value.
6. In the **Name of the new configuration key** field, enter the name of the API method whose objects you want to restrict.
7. Click **Create**.
8. Expand the **API method configuration / <API method name> / filter condition** configuration key.
9. Enter the filter condition in the **Value** field.
10. Click **Apply**.
11. 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**.
12. Click **Apply**.

Editing your own API filters

You can edit filter conditions for API methods.

To edit your own API filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **API method configuration / <API method name> / filter condition** configuration key.
5. Change the filter condition in the **Value** field.
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**.

Deleting your own API filters

You can delete your own filter conditions for API methods.

To delete your API filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Click ⋮ (**Actions**) > **Delete configuration key**.
5. In the **Delete configuration key** side panel, in the **Configuration key to be deleted** drop-down, select the API method whose filter condition you want to delete. For example, if you want to delete the filter condition for the **MyAPIMethod** API method, select the `API method configuration / MyAPIMethod` value.
6. Click **Delete configuration key**

Configuring your own filters

To restrict the number of candidate objects on foreign key relations, you can create, edit, and delete your own filter conditions.

Creating your own filters

To restrict the number of candidate objects on foreign key relations, you can create your own filter conditions.

To create your own filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`Web Portal`** API project.
4. Click ⋮ (**Actions**) > **Create configuration key**).
5. In the **Create Configuration Key** side panel, perform one of the following actions:
   - To create a filter that refers to a specific foreign key column of a table, in the drop-down, select the **`Filters for object selection`** value.
   - To create a filter that refers to all foreign key columns of a specific table, in the drop-down, select the value **`Filters for object selection by table`**.
6. Perform one of the following tasks:
   - In the **Name of the new configuration key** field, enter the name of the foreign key column in **`<table name>.<column name>`** format (**`MyTable.FirstColumn`** for example).
   - In the **Name of the new configuration key** field, enter the name of the table (**`MyTable`** for example).
7. Click **Create**.
8. Expand the **Filters for object selection / <foreign key column name/table name>** configuration key.
9. Enter the filter condition in the **Value** field.
10. Click **Apply**.
11. 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**.
12. Click **Apply**.

Editing your own filters

You can edit the filter conditions.

To edit your own filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Filters for object selection / <foreign key column name/table name>** configuration key.
5. Change the filter condition in the **Value** field.
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**.

Deleting your own filters

You can delete your own filter conditions.

To delete a filter

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Click ⋮ (**Actions**) > **Delete configuration key**.
5. In the **Delete configuration key** side panel, in the **Configuration key to be deleted** drop-down, select the API method whose filter condition you want to delete. For example, if you want to delete the filter condition for the **MyAPIMethod** API method, select the `API method configuration / MyAPIMethod` value.
6. Click **Delete configuration key**

Configuring recommendations for adding entitlements to objects

Use the Administration Portal to configure the settings for entitlement recommendations.

The Web Portal can recommend users to assign entitlements to objects that are assigned to members of the object but not the object itself.

Excluding entitlements from recommendations

You can specify which entitlements not to recommend for assignment to objects.

NOTE: System entitlements with read-only memberships are excluded by default.

Required configuration keys:

- **Entitlements that are not recommended** (**RecommendationExclude**): Specify which entitlements not to recommend for assignment to objects.

To exclude entitlements from recommendations

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **`API Server`** API project.
4. Expand the **Entitlements that are not recommended** configuration key.
5. In the **Value** input field, enter a corresponding WHERE clause and use the **objectkey** column as the base column, for example `objectkey not in (...)`.
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 threshold for entitlement recommendations

You can specify how many members of an object must be assigned an entitlement so that the system recommends assigning this entitlement to the object itself.

Required configuration keys:

- **Entitlement recommendation threshold (in percent)** (**RoleAddThreshold**): Specifies how many members of an object must be assigned an entitlement for the system to recommend assigning this entitlement to the object itself.

To configure recommendations for adding entitlements to objects

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Expand the **Recommendation value for entitlements (in percent)** configuration key.
5. In the **Value** field, enter the percentage of how many members of an object must be assigned an entitlement so that the system recommends assigning this entitlement to the object itself.
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

Use the Administration Portal to configure settings for devices that are managed in the Web Portal.

Configuring the editable properties of devices

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

Required configuration key:

- **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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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 business roles

Use the Administration Portal to configure settings for business roles that are managed in the Web Portal.

Enabling or disabling business role creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
    - To enable creation, select the check box.
    - To disable creation, 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**.

Configuring the help desk module/tickets

Use the Administration Portal to configure the help desk module and tickets settings.

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*.

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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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 key:

- **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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Properties editors / Editable properties / TroubleTicket** configuration key.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 hyperviews

Use the Administration Portal to configure the settings for overviews of objects that are displayed as hyperviews in the Web Portal.

Users with the **Portal_HyperView_Navigation** program function can use hyperviews. For more information about program functions, see the *One Identity Manager Authorization and Authentication Guide*.

Enabling and disabling navigation in hyperviews

You can specify whether user are allowed to navigate in hyperviews. That means users can jump from one hyperview to another hyperview by clicking on a linked object.

Required configuration keys:

- **Navigation in hyperviews is possible** (**EnableHyperViewNavigation**): Specifies whether users can navigate in hyperviews.

To enable or disable navigation in hyperviews

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Navigation in hyperviews is possible** configuration key.
5. Perform one of the following actions:
    - To enable navigation in hyperviews, set the **Navigation in hyperviews is possible** check box.
    - To disable navigation in hyperviews, clear the **Navigation in hyperviews is possible** 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 identities

Use the Administration Portal to configure settings for identities that are managed in the Web Portal.

Configuring editable identity properties

Specify which properties of identities can be edited when they are created or edited.

Required configuration keys:

- **Personal properties of identities that can be edited** (**VI_Employee_Master-Data_Attributes**): Specifies which personal properties of identities can be edited.
- **Location-related properties of identities that can be edited** (**VI_Employee_MasterData_LocalityAttributes**): Specifies which location-related properties of identities can be edited.
- **Organizational properties of identities that can be edited** (**VI_Employee_MasterData_OrganizationalAttributes**): Specifies which organizational properties of identities can be edited.

To configure editable properties of identities

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Perform one of the following actions:
    a. To configure personal properties of identities, expand the **Personal properties of identities that can be edited** configuration key.
    b. To configure location-related properties of identities, expand the **Location-related properties of identities that can be edited** configuration key.
    c. To configure organizational properties of identities, expand the configuration key **Organizational properties of identities that can be edited**.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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 properties logged in users can edit in profile settings

Specify which main properties of their own identities logged in users can edit in the profile settings.

Required configuration keys:

- **Properties logged in users can edit in profile settings** (**VI_PersonalData_Fields**): Specifies the main properties of their own identities that logged in users can edit in their profile settings.

To configure editable properties in the identity profile settings

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Properties logged in users can edit in profile settings** configuration key.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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**.

Enabling or disabling identity creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
    - To enable creation, select the check box.
    - To disable creation, 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**.

Configuring maximum size for profile pictures

To prevent users from uploading profile pictures that are too large, you can set the maximum picture size of profile pictures. Images that exceed this maximum size are automatically resized to the maximum size.

Required configuration keys:

- **Maximum profile picture height (in pixels)** (**PersonImageMaxWidth**): Defines the maximum height of a profile picture.
- **Maximum profile picture width (in pixels)** (**PersonImageMaxHeight**): Defines the maximum width of a profile picture.

To skip sorting a table

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Maximum profile picture height (in pixels)** configuration key.
5. In the **Value** input field, enter the maximum height of a profile picture.
6. Expand the **Maximum profile picture width (in pixels)** configuration key.
7. In the **Value** input field, enter the maximum width of a profile picture.
8. Click **Apply**.
9. 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**.
10. Click **Apply**.

Configuring time for actions for responsibilities of identities

You can specify how many days before identities leave the company their responsibilities are marked with "Action needed". The managers of these identities can then take action to prevent objects from remaining without an active responsibility.

Required configuration keys:

- **Time from which actions for responsibilities of leaving identities are needed (in days)** (**ThresholdPersonWarnDaysBeforeLeave**): Specifies how many days before an identity leaves the company, their responsibilities are marked with "Action needed".

To configure time for action

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Time from which actions for responsibilities of leaving identities are needed (in days)** configuration key.
5. In the **Value** input field, enter the number of days before identities leave the company from which their responsibilities should be marked with **Action needed**. For example, if you enter `30` here, the responsibilities of identities that are at least 30 days away from leaving the company will be marked with **Action needed** on the **Responsibilities of My Reports** page in the Web Portal.
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 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.

Required configuration keys:

- **Login with password questions** (**EnablePasswordProfileLogin**): Specifies whether users can login by answering their password questions.
- **Password questions can be managed** (**VI_MyData_MyPassword_Visibility**): Specifies whether users can manage their password questions and answers.

To configure password questions

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Password Reset Portal` API project.

4. Expand the **Login with password questions** configuration key.
5. Select the **Login with password questions** check box.
6. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
7. Expand the **Password questions can be managed** configuration key.
8. Select the **Password questions can be managed** check box.
9. Click **Apply**.
10. 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**.
11. Click **Apply**.
12. Start the Designer program.
13. Connect to the relevant database.
14. 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.

Configuring cost centers

Use the Administration Portal to configure settings for cost centers that are managed in the Web Portal.

Enabling or disabling cost center creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
    - To enable creation, select the check box.
    - To disable creation, 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**.

Configuring service items

Use the Administration Portal to configure settings for service items that are managed in the web portal.

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 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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**.

Program functions for the Web Portal

Program functions are part of the permissions model in One Identity Manager. They allow you to enable and disable features. Certain Web Portal functions are only available if the current user is assigned the corresponding program functions. For more information on controlling permissions through program functions, see the *One Identity Manager Authorization and Authentication Guide*.

Table 2: Program functions for the Web Portal

Program function	Description
Portal_UI_ PersonAdmin	User interface functions for identity administrators
Portal_UI_ PersonManager	User interface functions for identity managers
Portal_UI_ShopAdmin	User interface functions for IT Shop administrators
Portal_UI_StructAdmin	User interface functions for department, cost center, and location administrators
Portal_UI_ ResourceAdmin	User interface functions for resource administrators
Portal_UI_RoleAdmin	User interface functions for business role and application role administrators

Program function	Description
Portal_UI_ ShopStatistics	Statistics for the IT Shop
Portal_UI_ StructStatistics	Statistics for departments, cost centers, and locations
Portal_UI_ RoleStatistics	Statistics for business roles and application roles
QER_CancelPwO	Approval procedures can be canceled in the IT Shop
Portal_UI_ QERPolicyAdmin	User interface functions for company policy administrators
Portal_UI_ QERPolicyStatistics	Statistics for company policies
Portal_UI_ RuleStatistics	Statistics for compliance rules
Portal_UI_PolicyAdmin	User interface functions for attestation policy administrators
Portal_UI_ PolicyStatistics	Statistics for attestation policies
Portal_UI_PolicyOwner	User interface functions for attestation policy owners
Portal_UI_ PAGStatistics	Statistics for privileged accounts
Portal_UI_ TSBStatistics	Statistics for target systems
Portal_UI_ ApplicationAdmin	User interface functions for application administrators
Portal_UI_ ApplicationOwner	User interface functions for application owners
Portal_UI_ PasswordHelpdesk	Functions for help desk password

Configuring software

Use the Administration Portal to configure settings for software that is managed in the Web Portal.

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 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, 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 drop-down.
    - To change an existing property, select the property in the corresponding drop-down.
    - 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 locations

Use the Administration Portal to configure settings for locations that are managed in the Web Portal.

Enabling or disabling location creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.

3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
    - To enable creation, select the check box.
    - To disable creation, 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**.

Configuring statistics

Use the Administration Portal to configure settings for statistics that are displayed in the Web Portal.

Users with corresponding program function can use statistics. For more information about program functions, see the *One Identity Manager Authorization and Authentication Guide*.

Configuring shared statistics

Specify which statistics you want share with all the other Web Portal users.

Required configuration keys:

- **Shared statistics** (**OrganizationStatistics**): Specify which statistics are displayed as shared statistics.

To configure shared statistics

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Shared statistics** configuration key.
5. You can perform the following actions:
    - To add a statistic, click **Add new** and enter the name (**Ident_DialogDashboardDef**) of the relevant statistic.

TIP: You can find a statistic's identifier in the master data of a statistic in the Designer program. For more information about creating and editing statistic definitions, see the *One Identity Manager Configuration Guide*.

- To change an existing statistic, change the identifier in the corresponding input field.
- To remove an existing statistic, click on (**delete**) next to the relevant statistic.

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 system roles

Use the Administration Portal to configure settings for system roles that are managed in the Web Portal.

Enabling or disabling system role creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
   - To enable creation, select the check box.
   - To disable creation, 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**.

Skip table sorting

To improve the performance of the Web Portal, you can minimize data access and sorting processes for certain tables by skipping automatic table sorting.

NOTE: As certain API requests may have specific sorting requirements, this setting can be overridden by individual API methods.

Required configuration keys:

- **Skip table sorting** (**DoNotSortOnApiServer**): Determines whether to skip sorting of table entries.

To skip sorting a table

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the **API Server** API project.
4. Click ⋮ (**Actions**) > **Create configuration key**.
5. In the **Create configuration key** side panel, in the drop-down, select the **Table configuration** value.
6. In the **Name of the new configuration key** field, enter the name of the table whose entries should no longer be sorted.
7. Click **Create**.
8. Expand the **Table configuration/<tablename>/Skip table sorting** configuration parameter.
9. Select the **Skip table sorting** check box.
10. Click **Apply**.
11. 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**.
12. Click **Apply**.

TIP: To delete the newly created configuration key, perform the following actions:

1. Click ⋮ (**Actions**) > **Delete configuration key**.
2. In the **Delete configuration key** side panel, in the **Configuration key to be deleted** drop-down, select the configuration key that you want to delete.
3. Click **Delete configuration key**.

Configuring team roles

Use the Administration Portal to configure settings for team roles that are managed in the Web Portal.

Enabling or disabling team role creation

Required configuration keys:

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the configuration key.
5. Perform one of the following actions:
    - To enable creation, select the check box.
    - To disable creation, 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**.

Configuring the four eyes principle for issuing a passcode.

You can control whether passcodes generated by the help desk are divided into two parts. One half of the passcode is issued to the help desk staff and the other half is sent to the identity's manager. The identity must ask the manager for the second half of the passcode. This procedure increases the security for issuing passcodes.

To configure the four eye principle for issuing passcodes

1. Start the Designer program.
2. Connect to the relevant database.
3. Set the **QER** | **Person** | **PasswordResetAuthenticator** | **PasscodeSplit** configuration parameter.

TIP: To find out how to edit configuration parameters in Designer, see the *One Identity Manager Configuration Guide*.

4. Set the **QER** | **WebPortal** | **MailTemplateIdents** | **InformManagerAboutSecondHalfOfPasscode** configuration parameter.

   By default, the second half of the passcode is sent with the **Identity - part of passcode for password reset (manager)** 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*.

Configuring WebAuthn security keys

One Identity offers users the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. These security keys support the W3C standard **WebAuthn**.

Use of security keys guarantees increased security when logging in.

Advice

- In the Manager, identity administrators have the option to view all of an identity's security keys and to delete them. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
- The WebAuthn standard is NOT support in Internet Explorer. Users must use another browser.

To configure WebAuthn for a web application, carry out these four steps:

1. Configure the OAuth certificate to enable secure communication between RSTS and One Identity Manager.
2. Configure the RSTS.
3. Configure the application server.
4. Configure the web application.

Related topics

- Configuring authentication on page 17

Step 1: Configuring an OAuth certificate

Communication between the RSTS (redistributable security token service) and One Identity Manager uses tokens that are signed with the private key of a certificate. This certificate must be valid and trusted because the RSTS also uses this certificate for client certificate registration on the application server. One Identity recommends that either you use a public key infrastructure (PKI) that already exists or a new certificate chain from the root certificate and the associated OAuth signing certificate.

To configure the OAuth signing certificate

1. Create a new, valid, and trusted, OAuth signing certificate.
2. Ensure the following:
    - The RSTS must have access to the OAuth signing certificate with a private key.
    - The application server from which, the RSTS requests the WebAuthn security keys, must trust the certificate chain of the OAuth signing certificate.
    - The web application that allows login by RSTS, must have access to the OAuth signing certificate with a private key.
    - The web application used to manage the WebAuthn security keys, must have access to the OAuth signing certificate with a private key.

Related topics

- Configuring WebAuthn security keys on page 95
- Step 2: Configuring the RSTS on page 96
- Step 3: Configuring the application server on page 98
- Step 4: Configuring the Web Portal on page 99

Step 2: Configuring the RSTS

NOTE: Before you can configure the RSTS, you must configure the OAuth signing certificate. For more information, see Step 1: Configuring an OAuth certificate on page 95.

To configure WebAuthn on the RSTS

1. Perform one of the following tasks:
    - If you are installing the RSTS: When you install the RSTS, select the previously created OAuth signing certificate so that the corresponding entry in the identity provider in One Identity Manager is set.
    - If the RSTS is already installed: Stop the relevant service, uninstall it and install the new version.
2. In your web browser, call the URL of the RSTS administration interface: https://<Webanwendung>/RSTS/admin.
3. On the start page, click **Applications**.
4. On the **Applications** page, click **Add Application**.
5. On the **Edit** page, complete the data on the various tabs.

    NOTE: The forwarding URLs (**Redirect Url**) on the **General** tab us the following formats:

- For the API Server:

  https://<server name>/<application server path>/html/<web application>/?Module=OAuthRoleBased

- For the Web Portal:

  https://<server name>/<web application>/

6. Switch to the **Two Factor Authentication** tab.
7. On the **Two Factor Authentication** tab, in the list in **Required by** pane, click:
   - **All Users**: All users must log in with two-factor authentication.
   - **Specific Users/Groups**: Specific users must log in using two-factor authentication. You can add these by clicking **Add**.
   - **Note Required**: The application server decided which users must log in using two-factor authentication.
8. In the navigation, click **Home**.
9. On the home page, click **Authentication providers**.
10. On the **Authentication Providers** page, edit the entry in the list.
11. On the **Edit** page, switch to the **Two Factor Authentication** tab.
12. In the **Two Factor Authentication Settings** pane, click **FIDO2/WebAuthn**.
13. Edit the following input fields:
    - **Relying Party Name**: Enter any name.
    - **Domain Suffix**: Enter the suffix of your Active Directory domain that hosts the RSTS.
    - **API URL Format**: Enter the application server's URL. The given URL must contain a place-holder in `{0}` format that supplies a unique identifier for the user.

      The **API URL Format** is used by RSTS to call the list of WebAuthn security keys of a specified user. Enter the URL in the following format:

      https://<server name>/<application server path>/appServer/WebAuthn/<identity provider>/Users/{0}

      - `Server name` – fully qualified host name of the web server hosting the application server
      - `<Application server path>` – path to the web application of the application server (default: `AppServer`)
      - `<Identity provider>` – name of the identity provider

        TIP: You can find the name of the identity provider in the Designer:

        Basic data > **Security settings** > **OAuth 2.0/OpenId Connect configuration**

Example:
https://www.example.com/AppServer/appServer/webauthn/OneIdentity/Users/{0}

14. Click **Finish**.

Related topics

- Configuring WebAuthn security keys on page 95
- Step 1: Configuring an OAuth certificate on page 95
- Step 3: Configuring the application server on page 98
- Step 4: Configuring the Web Portal on page 99

Step 3: Configuring the application server

The RSTS call the WebAuthn security key for Active Directory users over an interface. This information is sensitive and must not be called by unauthorized persons, therefore, access must secured through by client certificate login.

In order for this to work, certificates must be valid and client certificate login on IIS must be enabled.

The application server checks the certifcate's thumbprint the client used to login. Only if the thumbprint matches the stored thumbprint, is the information returned.

If the application server is also used as the backend for web applications, grant access rights to the application pool users for the OAuth signing certificate's private key.

To enable client certificate login on IIS

1. Start the Internet Information Services Manager.
2. Open the **SSL Setting** menu for the relevant application server.
3. In the **Client certificates** option, change the value to **Accept**.

Related topics

- Configuring WebAuthn security keys on page 95
- Step 1: Configuring an OAuth certificate on page 95
- Step 2: Configuring the RSTS on page 96
- Step 4: Configuring the Web Portal on page 99

Step 4: Configuring the Web Portal

NOTE: The web application to be used by WebAuthn, must apply the HTTPS secure communications protocol (see Using HTTPS on page 102).

Required configuration keys:

- **Secondary authentication provider ID for Webauthn two-factor authentication** (**VI_Common_AccessControl_Webauthn_2FAID**): Specifies the unique ID of the secondary authentication provider for Webauthn two-factor authentication.
- **Multi-factor authentication** (**MfaAuthenticationProvider**): Specifies which authentication method to use.
- **WebAuthn security keys can be managed** (**EnableWebauthnKeyManagement**): Specifies whether user can manage their WebAuthn security keys.

To configure WebAuthn in the Web Portal

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Web Portal` API project.
4. Expand the **Secondary authentication provider ID for Webauthn two-factor authentication** configuration key.
5. In the **Value** field, enter the unique identifier of the secondary authentication provider for WebAuthn two-factor authentication. You will find this identifier in your RSTS configuration.
    a. In your Internet browser, call the URL of the RSTS administration interface: `https://<Webanwendung>/RSTS/admin`.
    b. On the main page, click **Authentication Providers**.
    c. On the **Authentication Providers** page, click the appropriate entry.
    d. On the **Edit** page, switch to the **Two Factor Authentication** tab.
    e. Take the ID from the **Provider ID** field.
6. Expand the **Multi-factor Authentication** configuration key.
7. In the **Value** drop-down, select `Webauthn`.
8. Exand the **WebAuthn security keys can be managed** configuration key.
9. Perform one of the following actions:
    a. To enable management of WebAuthn security keys in the Web Portal, select the **WebAuthn security keys can be managed** check box.

b. To disable management of WebAuthn security keys in the Web Portal, clear the **WebAuthn security keys can be managed** check box.

10. Click **Apply**.
11. 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**.
12. Click **Apply**.

Configuring the Operations Support Web Portal

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

Configuring editable properties of Job servers

In the Operations Support Web Portal, you can define which properties of a Job server can be edited in the Job server overview.

Required configuration keys:

- **Properties that can be edited / Job servers** (**QbmOperationsConfig/EditableFields/QBMServer**): Specifies which Job server properties can be edited.

To configure the editable properties of Job servers

1. Log in to the Administration Portal (see Logging in to the Administration Portal on page 9).
2. In the navigation, click **Configuration**.
3. On the **Configuration** page, in the **Show configuration for the following API project** drop-down, select the `Operations Support Web Portal` API project.
4. Expand the **Properties that can be edited / Job servers** configuration key.
5. You can perform the following actions:
    - To add a property, click **New** and select the corresponding property from the drop-down.

- To change an existing property, select the property in the corresponding drop-down.
- 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**.

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.

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 enabled in a production 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