One Identity Manager 8.2.1

Web Designer Web Applications Configuration Guide

One Identity Manager Web Designer Web Applications Configuration Guide
Updated - 27 April 2022, 01:20
Version - 8.2.1

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

Configuring the Web Portal

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

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

Detailed information about this topic

Configuring request functions

You can configure Web Portal request functions in the Web Designer.

Configuring requesting by reference users

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

Required configuration key:

- (**VI_ITShop_ProductSelectionByReferenceUser** : Enables or disables the "By reference user" function in the Web Portal.
- **VI_ITShop_Filter_PersonReference**: Sets the number of reference users displayed. This configuration parameter is a SQL filter on the **Person** table.

To configure requesting by reference user

1. Open the Web Designer.
2. Open the **VI_ITShop_ProduCtSelection** module and search through the definition tree view for **VI_ITShop_ProductSelectionByReferenceUser**.
3. In the definition tree view, select the **VI_ITShop_ ProductSelectionByReferenceUser** configuration parameter.
4. In the definition tree view, choose to switch to the **Configuration (custom)** view. where you can edit the configuration parameter.
5. Perform one of the following actions:
   - To enable requesting by reference users: in the **Node editor** window set the value to `True`.
   - To disable requesting by reference users: in the **Node editing** window set the value to `false`.

To set the number of reference users displayed

1. Open the Web Designer.
2. Open a module and search through the definition tree view for **VI_ITShop_Filter_ PersonReference**.
3. In the definition tree view, mark the **VI_ITShop_Filter_PersonReference** configuration parameter.
4. In the **Node editing** window, enter the desired value in the **Value** field.

   NOTE: If you can include the variable `%useruid%` if want to reference the current user.

Sending the shopping cart

There are difference ways you can configure the shopping cart in the Web Portal.

Detailed information about this topic

- Setting the priority on page 8
- Confirming requests on page 8
- Forcing reauthentication on page 9
- Handling required products on page 9

Setting the priority

Table 1: Configuration parameters for the request priority

Configuration parameter	Description
VI_ITShop_DisablePWOPriorityChange	Disables the priority's setting for a request made by a user in the Web Portal.

By default, users can set the priority of their own request.

To disable a priority setting

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_DisablePWOPriorityChange".
3. Select "VI_ITShop_DisablePWOPriorityChange".
4. Set the value to **true** in the `Node editor` view.

Confirming requests

Table 2: Configuration parameter for confirming requests

Configuration parameter	Description
VI_ITShop_SubmitOrderImmediately	Forces confirmation of a request in the Web Portal.

The user can send a request in the Web Portal without confirmation, by default. However, confirmation is required if at least one warning is issued while checking the request.

If you want to have confirmation for requests without requiring a warning, you can configure "VI_ITShop_SubmitOrderImmediately".

To demand confirmation for a request

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_SubmitOrderImmediately".
3. Select the configuration parameter "VI_ITShop_SubmitOrderImmediately".
4. Set the value to **false** in the `Node editor` view.

Forcing reauthentication

Table 3: Configuration parameter for Active Directory request authentication

Configuration Parameter	Description	Setting	
		False	True
VI_ITShop_TermsOfUseRe-quireADAuthentication	Ensures Active Directory reauthentication when a request is carried out.	Denied and unsubscribed requests cannot be directly reinstated as new requests.	Denied and unsubscribed requests can be reinstated by recipients or requesters of the request.

To ensure reauthentication during a request

1. Assign the terms of use to the service item.

   For more detailed information about assigning service items, see the One Identity Manager IT Shop Administration Guide.
2. Open the Web Designer.
3. Open a module and search for "VI_ITShop_TermsOfUseRequireADAuthentication".
4. Select the configuration parameter "VI_ITShop_ TermsOfUseRequireADAuthentication".
5. Set the value to **true** in the `Node editor` view.

Handling required products

There are different ways of handling required products in the Web Portal. Configuration parameter settings are carried out in Web Designer.

Table 4: Configuration parameter for required products

Configuration parameter	Description
VI_ITShop_AllowRequestWithMissingDependencies	If the configuration parameter is set, a request can be sent even though the required product cannot be requested due to an existing assignment.

"VI_ITShop_AllowRequestWithMissingDependencies" is not set by default. This means a request cannot be sent if the required product cannot be requested.

To configure required product handling

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_AllowRequestWithMissingDependencies".
3. Mark "VI_ITShop_AllowRequestWithMissingDependencies".
4. Edit the configuration parameter on **Configuration** by setting the value **true** in the `Node Edit`. This overwrites the default setting.

Approver options

There are various configuration options available for request approvers in the Web Portal.

Detailed information about this topic

- Setting validity periods on page 10
- Submitting inquiries on page 11
- Require a reason on page 11

Setting validity periods

Table 5: Configuration parameter for validity

Configuration parameter	Description
VI_ITShop_ApproverCanSetValidFrom	Allows the approver to set a new activation time for a request's validity period.
VI_ITShop_ApproverCanSetValidUntil	Allows the approver to set a end time for a request's validity period.

The settings for `VI_ITShop_ApproverCanSetValidFrom` and `VI_ITShop_ApproverCanSetValidUntil` allow the request's approver to set a new validity period.

To set the validity period

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_ApproverCanSetValidFrom".
3. Select "VI_ITShop_ApproverCanSetValidFrom".
4. Set the value to **true** in the `Node editor` view.
5. Search for "VI_ITShop_ApproverCanSetValidUntil".
6. Select the configuration parameter "VI_ITShop_ApproverCanSetValidUntil"
7. Set the value to **true** in the `Node editor` view.

Submitting inquiries

Table 6: Configuration parameters for the inquiry

Configuration parameter	Description
VI_ITShop_WantSeeQueryToPerson	Allows the approver to ask another employee a question in the context of the approval workflow.

To submit inquiries

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_WantSeeQueryToPerson".
3. Select "VI_ITShop_WantSeeQueryToPerson".
4. Set the value to **true** in the `Node editor` view.

Require a reason

Table 7: Configuration parameter for reason

Configuration parameter	Description
VI_ITShop_ApproverReasonMandatoryOnDeny	Requires a reason from the approver for denying a request.

To ask a question

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_ApproverReasonMandatoryOnDeny".
3. Select the configuration parameter "VI_ITShop_ApproverReasonMandatoryOnDeny".
4. Set the value to **true** in the `Node editor` view.

Approval decisions about URL links

Table 8: Configuration parameter for approval decisions about URL links

Configuration parameter	Description	Meaning	
VI_ITShop_Approvals_InteractiveApproval	Requires consultation with the user before approval. This key is a SQL filter	Product fulfills filter condition	Approval is not done directly. Displays form

Configuration parameter	Description	Meaning	
	condition on the "AccProduct" table.		for confirming the approval decision.
		Product does not fulfill filter condition	Approval decision is made when the page is called. Approvers receive a message that the approval decision has been entered into the system.

An approval decision about a request can be made by opening a URL that is sent in an email, for example.

Cases that use this type of messaging for request approvals are special service items, which are required for informing the user about the approval decision. Approvals through these service items are not permitted without prior consultation.

To prevent a approval by URL link

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_Approvals_InteractiveApproval".
3. Select the configuration parameter "VI_ITShop_Approvals_InteractiveApproval".
4. In the Node editor, set the value to **true**.

Displaying user-specific processes in the Web Portal

A user-specific process is a process that is specifically configured for tracing by the user. It enables status tracking and confirmation of a processing result to the Web Portal.

A user who is logged on to the Web Portal can see all processes that they have initiated. The value in the `XUserInserted` column corresponds to the user who is currently logged on. A process can only be generated from within a session of the current logged on user if it is to be identified as a user-specific process.

The user-specific processes are displayed in the Web Portal in the **My Processes** view. For more detailed information, see the *One Identity Manager Web Designer Web Portal User Guide*.

This section only covers the configuration for displaying the process information in the Web Portal. For more detailed information about process monitoring, recording process information, and the configuration of processes and process steps, see the *One Identity Manager Configuration Guide*.

Configuration recommendations for the recording of user-specific processes

- In the Designer, check the **Common | ProcessState** configuration parameter. The configuration parameter must be set.
- In the Designer, check the **Common | ProcessState | JobHistory** configuration parameter. The configuration parameter must be set. As a value for the configuration parameter, select **ERRORorSELECTED** or **SELECTED**.

  NOTE: The value **ALL** also takes into account the notifications from the process history. However, this setting can lead to an extremely large data volume.
- In the Designer, check the **Common | ProcessState | ProgressView** configuration parameter. The configuration parameter must be set and should have the value **2**.
- In the Designer, check the **Common | ProcessState | ProgressView | LifeTime** and **Common | ProcessState | JobHistory | LifeTime** configuration parameters. These configuration parameters define the retention time of the process information and notifications in the process history. The configuration parameters must be set. Adjust the retention times if necessary. By default, the information is stored for 30 days before it is removed from the One Identity Manager database.
- In the Designer, configure the processes and process steps for recording process information.
  - In the **Process information** property for a process, select the value **Web Portal tracking**.
  - In the **Process information** property for the process steps, select the value **Web Portal tracking**. Enable the **Process history** option.
  - Use user-friendly informative display values for the processes and process steps. To do this, enter the formatting rules for the process information of processes and process steps.

Configuring self-registration of new users

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

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

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

To configure self-registration

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

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

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

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

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

     TIP: In the Designer, you can configure the current mail template in the **Mail templates** > **Person** category. For more information about mail templates, see the *One Identity Manager Operational Guide*.
   - **QER** | **Attestation** | **ApproveNewExternalUsers**: Specify whether self-registered users must be attested before they are activated. A manager then decides whether to approve the new user's registration.
   - **QER** | **Attestation** | **NewExternalUserTimeoutInHours**: For new self-registered users, specify the duration of the verification link in hours.
   - **QER** | **Attestation** | **NewExternalUserFinalTimeoutInHours**: Specify the duration in hours, within which self-registration must be successfully completed.
4. Assign at least one employee to the **Identity & Access Governance | Attestation | Attestor for external users** application role.

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

employee's manager. The employee 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.

   NOTE: For more information about editing configuration parameters in the 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 **Employee - manager half of passcode for password reset** 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 password questions

If Web Portal users forget their password, they can set a new one with the help of the password questions.

To configure the use of password questions.

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

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

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

     NOTE: The value must not be less than the value in the **QueryAnswerRequests** configuration parameter.
   - **QER** | **Person** | **PasswordResetAuthenticator** | **QueryAnswerRequests**: Specify how many password questions users have to answer before they can reset their password.

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

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

Configuring the search

Many of the Web Portal's pages provide a search option for objects in context of the page.

To configure the search

1. Start the Web Designer program.
2. Connect to the relevant database.
3. Configure the **VI_Common_SqlSearch_PrefixLike** configuration key: To show the user matching search results as fast as possible, search suggestions are already shown while you are entering the word. If you set the parameter, the last word of the input will also be taken into account.
4. Start the Designer.
5. Configure the following configuration parameters:

   Common | **Indexing** | **IndexNonTokenChars**: Specify which delimiters can be used in the search.

   Common | **Indexing** | **IndexUseLegacyAnalyzer**: Specify whether an alternative tokenizing is also be performed. The alternative method of tokenizing is preferable for long tokens. For example, if the string `Department_01` is a token, the partial string `Department` is not considered to be a token.

   The following tokens are named.

Table 9: Tokens for alternative tokenizing

Token	Description with example
Words	Sequence of letters and/or numbers
Enumeration	Words linked by punctuation marks (**_-/.,**) of which at least every second one contains a number. An example is **Department_01**. Sequences are also decimal numbers and IP addresses.
Email addresses	An email address is often made up of first name, last name, company name and generic top-level domain (for example **.com**). The order or spelling of the first and last names may vary (for

Token	Description with example
	example, use of initials). The special character @ and the punctuation mark (.) not only separate each part of the email address but also links them so that Examples of email addresses are **Ben.King@example.com** and **C.Harris@example.com**.
Host names	For example **website.example.com**.
Acronym	For example **U. S. A.**
Apostrophe	For example **O'Reilly**.
@, & surrounded by letters	For example **Me&you**.
Umlauts such as ä, ö, ü	For example **Max Müller**.

NOTE: If you change these configuration parameters, the search indexes will be rebuilt, which may take some time.

3

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

- You can run Starling Two-Factor Authentication and WebAuthn in parallel for a web application. Users that have at least one valid security key, do not have to go through the Starling 2FA process as well. Users that do not have a security key must still use Starling 2FA.
- In the Manager, employee administrators have the option to view all of an employee'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.

Related topics

- WebAuthn configuration on page 18

WebAuthn configuration

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

- WebAuthn security keys on page 18
- Step 1: Configuring an OAuth certificate on page 19
- Step 2: Configuring the RSTS on page 19
- Step 3: Configuring the application server on page 21
- Step 4: Configuring the web application on page 22

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

- WebAuthn security keys on page 18
- Step 2: Configuring the RSTS on page 19
- Step 3: Configuring the application server on page 21
- Step 4: Configuring the web application on page 22

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

19.

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 RSTS already exists: Quit the relevant service, replace the file `RSTS.exe` with the current version and restart the RSTS.

     You will find the current version of the `RSTS.exe` file on the installation medium in the `Modules\QBM\dvd\AddOn\Redistributable STS` directory.
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

- WebAuthn security keys on page 18
- Step 1: Configuring an OAuth certificate on page 19
- Step 3: Configuring the application server on page 21
- Step 4: Configuring the web application on page 22

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

- WebAuthn security keys on page 18
- Step 1: Configuring an OAuth certificate on page 19
- Step 2: Configuring the RSTS on page 19
- Step 4: Configuring the web application on page 22

Step 4: Configuring the web application

NOTE: The web application to be used by WebAuthn, must apply the HTTPS secure communications protocol (see Using HTTPS on page 37).

To configure WebAuthn in web applications

1. Start the Web Designer program.
2. Connect to the relevant database.
3. In the menu bar, click **View** > **Start page**.
4. In the toolbar, click **Select web application** and select the web application you want to use.
5. Click **Edit web application settings**.
6. In the **Edit web application settings** dialog, in the **Authentication module** menu, click **OAuth 2.0/OpenID Connect**.
7. In the **OAuth** pane, in the **OAuth 2.0/OpenID Connect configuration** menu, click the appropriate identity provider.
8. Click **OK**.
9. In the menu bar, click **Edit** > **Configure project** > **Web project**.
10. In the **Configure project** view, configure the following configuration keys:
    - **VI_Common_RequiresAccessControl**: Set this parameter to enable two-factor authentication.

- **VI_Common_AccessControl_WebAuthn_2FA**: Specify whether you want to enable WebAuthn two-factor authentication for the web application.

  You can configure WebAuthn two-factor authentication and security key management separately. If, for example, you want to only enable management of security keys but not of two-factor authentication with the help of security keys in the web application, do not set this configuration key and set the **VI_Common_AccessControl_WebAuthn_2FA_VisibleControls** configuration key described below.
- **VI_Common_AccessControl_WebAuthn_2FA_VisibleControls**: Specify whether users can manage security keys in the web application.
- **VI_Employee_QERWebAuthnKey_Filter**: Specify, which employees can manage security keys in the web application. If you do not enter anything here, all web application users manage the security keys (assuming the **VI_Common_AccessControl_WebAuthn_2FA_VisibleControls** configuration key is set).
- **VI_Common_AccessControl_WebAuthn_2FAID**: Enter a unique identifier for the secondary authentication provider for WebAuthn two-factor authentication. You will find this identifier in your RSTS configuration.
  1. In your Internet browser, call the URL of the RSTS administration interface: https://<Webanwendung>/RSTS/admin.
  2. On the main page, click **Authentication Providers**.
  3. On the **Authentication Providers** page, click the appropriate entry.
  4. On the **Edit** page, switch to the **Two Factor Authentication** tab.
  5. Take the ID from the **Provider ID** field.

Related topics

- WebAuthn security keys on page 18
- Step 1: Configuring an OAuth certificate on page 19
- Step 2: Configuring the RSTS on page 19
- Step 3: Configuring the application server on page 21

Multi-factor authentication

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

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

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

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

Configuring multi-factor authentication

You can configure multi-factor authentication for web applications.

Required configuration key:

- **VI_Common_RequiresAccessControl**: Requests web application authentication.
- **VI_Common_AccessControl_StarlingEnabled**: Enables the use of the Starling Two-Factor Authentication.

To set up multi-factor authentication

1. Open the Web Designer.
2. Open a module and search for **VI_Common_RequiresAccessControl** in the definition tree view.
3. Mark the `VI_Common_RequiresAccessControl` configuration parameter and set the value to **true**.
4. Mark the `VI_Common_AccessControl_StarlingEnabled` configuration parameter and set the value to **true**.

Multi-factor authentication for specific people

Table 10: Configuration parameters for multifactor authentication for specific people

Configuration parameter	Description
VI_Common_AccessControl_Filter	Sets up multi-factor authentication for specific people.

You need to specify, which people can use multi-factor authentication in your web project.

To set up multifactor authentication for specific people only

1. Open the Web Designer.
2. Open a module and search for **VI_Common_AccessControl_Filter** in the definition tree view.
3. Mark the **VI_Common_AccessControl_Starling_AllowUnregistered** configuration parameter in the definition tree view.
4. Enter a filter condition in the node editor view that only matches people who require multi-factor authentication.

Logging in without multi-factor authentication

You can specify that all users can log in to the web application without multi-factor authentication.

Required configuration key:

- **VI_Common_AccessControl_Starling_AllowUnregistered**: Specifies whether users that are not registered for multi-factor authentication are allowed to access the web application.

To allow login without multi-factor authentication for all users

1. Open the Web Designer.
2. Open a module and search for **VI_Common_AccessControl_Starling_ AllowUnregistered** in the definition tree view.
3. Mark the configuration parameter **VI_Common_AccessControl_Starling_ AllowUnregistered** in the definition tree view.
4. Set the value in the node editor view to `true`.

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

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

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

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

Configuring the Application Governance Module

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

Related topics

- Configuring entitlements on page 27
- Filling application hyperviews on page 28

Configuring entitlements

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

NOTE: Managing an application involves the following:

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

To assign an application role for application governance to employees

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

4. In the upper navigation pane, click the application role you want to assign to employees:
    - **Application Governance** | **Administrators**: Members of this application role create new applications and manage all applications in the Web Portal.
    - **Application Governance** | **Owners**: If this application role is assigned to an application as an owner application role, the members manage the application in the Web Portal.
    - **Application Governance** | **Approvers**: If this application role is assigned to an application as an approver application role, the members can approve requests for products of this application (if the **BE - Approver of an application** approval procedure is used).
5. In the **Tasks** pane, select the **Assign employees** task.
6. In the **Add Assignments** area, double-click the employees to whom you want to assign the application role.
7. Click (**Save**).

Filling application hyperviews

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

To start the schedule to populate the hyperview

1. Start the Designer program.
2. Connect to the relevant database.
3. In the Designer, select the **Base data** > **General** > **Schedules** category.
4. In the list, select the **Fill application overview** schedule.
5. In the schedule's details pane, click **Start**.
6. Confirm the security prompt with **Yes**.

To edit the schedule for filling the application's hyperview

1. Start the Designer program.
2. Connect to the relevant database.
3. In the Designer, select the **Base data** > **General** > **Schedules** category.
4. In the list, select the **Fill application overview** schedule.
5. In the schedule's details pane, edit the schedule's main data.

    For more information about schedule and their properties, see *One Identity Manager Operational Guide*.
6. Select the **Database** > **Commit to database** menu item and click **Save**.

6

Configuring the Password Reset Portal

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

Setting up a Password Reset Portal

To utilize the Password Reset Portal, it must be installed as a dedicated web application. The necessary security is guaranteed by multi-factor authentication.

Installing the Password Reset Portal

Table 11: Configuration parameters for application tokens

Configuration parameter	Description
QER | Person | PasswordResetAuthenticator | ApplicationToken	Sets a application token for the Password Reset Portal.

During installation, you will be prompted to enter an application token. This application token functions like a password, which the web application uses to authenticate itself on the database. This ensures that the password can only be reset by the web application assigned for the purpose.

To install the Password Reset Portal

1. Follow the step-by-step "To install the Web Portal" from "Installing the Web Portal" in the One Identity Manager Installation Guide.
2. Select **QER_PasswordWeb** from **Web Project**.

   After selecting the web project, you are prompted to enter an application token.
3. Select a sufficiently secure token and enter it in the box provided.

The application token is saved as a hash value in the database in "QER | Person | PasswordResetAuthenticator | ApplicationToken" and stored encrypted in the file `web.config`.

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:

Table 12: Authentication options

Login Type	Authentication Module Used	Application (QBMProduct)
Login with passcode.	Password reset (role-based), read-only.	Password reset, read-only.
Login using a secret password question.	Password reset (role-based), read-only.	Password reset, read-only.
Login with user name and password.	Specified in the web application configuration.	Specified in the web application configuration.

Configuring Password Reset Portal login with password questions

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

To configure the use of password questions.

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

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

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

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

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

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

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

Settable passwords

Users can set the following default passwords.

Table 13: Password overview

User	Password	Table / Column
Everyone	Own password	Person.DialogUserPassword
Everyone	User account password, which is a. Directly assigned to the current employee. - OR - b. Assigned to the current employee's sub identity. - OR - c. Assigned to the current employee's sponsored identity, service identity or group identity. - OR - d. Assigned to one of the current user's shared user accounts.	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.

Excluding passwords from being reset

Table 14: Script for resetting passwords

Script	Description
QER_PasswordReset_IsAllowSet	Specifies whether resetting a password in the Password Reset Portal is allowed.

To prevent users from setting passwords by mistake, you can exclude certain password 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.

NOTE: In "QER_PasswordWeb_IsAllowSet", the system user is prevented, by default, from resetting the password 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 automatic software updating of One Identity Manager web applications.

To exclude passwords from being reset

1. Open the Designer.
2. Find "QER_PasswordReset_IsAllowSet".
3. Use "QER_PasswordReset_IsAllowSet" as the basis for an overrideable script with the following parameters.
    a. Current user's UID_Person.
    b. Object's key (ObjectKey) offered for password reset.
    c. Password column name.
4. Save the setting in the Designer.
5. Compile the Password Reset Portal.

Central password

Apart from setting individual passwords in the Password Reset Portal, you 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

By defining password dependencies, you specify which passwords are managed through the central password.

Table 15: Script for declaring passwords

Script	Description
QER_PasswordWeb_IsByCentralPwd	By default, the script checks whether "QER | Person | UseCentralPassword" is set. If the configuration parameter is set, the employee's central password is mapped to the password column of the employee's user account. A user account must be linked to the current user, it cannot be a privileged account. The script can be overwritten.

To define password dependencies

1. Open the Designer.
2. Search QER_PasswordWeb_IsByCentralPwd.
3. Use "QER_PasswordWeb_IsByCentralPwd" as the basis for an overrideable script with the following parameters.
   a. Current user's UID_Person.
   b. Object's key (ObjectKey) offered for password reset.
   c. Password's column name.

   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 setting in the Designer.
5. Compile the Password Reset Portal.

Setting a central password

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

Once at least one of the logged in user's passwords is managed by the central password, two options are provided after authentication.

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 33.

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.

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

Setting up a new application token

You can set a new application token using `WebDesigner.ConfigFileEditor.exe`.

To set a new application token

1. Open `WebDesigner.ConfigFileEditor.exe`.
2. Ensure that **QER_PasswordWeb** is set as the web project.
3. Click next to **Application token exists**.

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:

   NOTE: For more information about editing configuration parameters in the 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`

Recommendations for secure operation of web applications

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

Detailed information about this topic

Using HTTPS

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

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

Disable automatic password storage

Use this setting to prevent auto-filling of your user data on the login page. This setting is made in the Web Designer and can help running of web applications more securely.

Table 16: Configuration parameter for disabling automatic password storage

Configuration parameter	Description
VI_Common_Login_PrefillLoginData	Prevents auto-filling user data on the login page.

To disable automatic password storage

1. Open the Web Designer.
2. In the menu bar, select the **Edit > Configure project > Web project** menu item.
3. On the **Configure Project** tab, search for "VI_Common_Login_PrefillLoginData".
4. In the **Allow prefill of login data** key, in the **Value (custom)** column, click +.

   This sets the default value to "false". This disables automatic password storage.

Disabling the HTTP request method TRACE

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

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

To disable the HTTP request method TRACE using Internet Information Services

- You will find instructions by following this link:

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

Using HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is a security mechanism for HTTPS connections. is a web security policy mechanism which helps to protect websites against protocol downgrade

attacks and cookie hijacking. For example, a server could send a header "Strict-Transport-Security" to the user's browser such that in future, at a defined time (max-age), this domain should exclusively use encrypted connections. This setting can be optionally extended by the parameter `includeSubDomains` to all subdomains. This means that not only `https://example.org` is taken into account but also `https://subdomains.example.org`.

To enable HSTS

1. Open the configuration file `web.config` for the chosen web application.
2. Set the HTTP Response Header to `Strict-Transport-Security` and the value `maxage = expireTime`.

   For more detailed information about setting the HTTP Response Header, see https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts.

Disabling insecure encryption mechanisms

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

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

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

Detailed information about this topic

- https://blogs.technet.microsoft.com/exchange/2015/07/27/exchange-tls-ssl-best-practices/
- https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc

Setting the "HttpOnly" attribute for ASP.NET session cookies

To prevent cookies being manipulated by JavaScript and to reduce the risk of cross-site scripting attacks and cookie theft, you can set the so called "HttpOnly" attribute for your

ASP.NET session cookies. This means that cookies can no longer be used by client-side scripts.

To set the "HttpOnly" attribute for ASP.NET session cookies

1. Open the configuration file `web.config` for the chosen web application.
2. In the `<configuration>` section, enter the following code snippet:

```
<system.web>
    <httpCookies httpOnlyCookies="true"/>
</system.web>
```

3. Save the file.

Related topics

- Setting the "secure" attribute for ASP.NET session cookies on page 41
- Setting the "same-site" attribute for ASP.NET session cookies on page 40

Setting the "same-site" attribute for ASP.NET session cookies

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

To set the same site attribute for all .NET versions from 4.7.2.

1. Open the configuration file `web.config` for the chosen web application.
2. Enter the following code snippet in the `<configuration>` section:

```
<system.web>
    <httpCookies sameSite="Strict" />
</system.web>
```

3. Save the file.

Related topics

- Setting the "HttpOnly" attribute for ASP.NET session cookies on page 39
- Setting the "secure" attribute for ASP.NET session cookies on page 41

Setting the "secure" attribute for ASP.NET session cookies

To prevent cookies being read by unauthorized persons, you can set the so called "secure" attribute for your ASP.NET session cookies. This means that cookies are only transferred over secure SSL connections.

To set the "secure" attribute for ASP.NET session cookies

1. Open the configuration file `web.config` for the chosen web application.
2. In the `<configuration>` section, enter the following code snippet:

```
<system.web>
    <httpCookies requireSSL="true"/>
</system.web>
```

3. Save the file.

Related topics

- Setting the "same-site" attribute for ASP.NET session cookies on page 40
- Setting the "HttpOnly" attribute for ASP.NET session cookies on page 39

Disabling Windows IIS 8.3 short names

The URL parser in Microsoft Internet Information Services (IIS) makes it possible for remote attackers to reveal file and folder names of web applications (that should not be accessible) by using IIS 8.3 short names.

Use of this weak point can lead to files with sensitive data, such as login data, configuration files, maintenance scripts and other data, being passed on.

To prevent this, you can stop short names in Windows IIS 8.3 from being created.

To disable creation of Windows IIS 8.3 short names

1. On the system the web application is installed on, create the following registry entry:
    - Path: `HKLM\SYSTEM\CurrentControlSet\Control\FileSystem`
    - Name: `NtfsDisable8dot3NameCreation`
    - Value: `1`
2. Reinstall the web application.

Detailed information about this topic

- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959352(v=technet.10)

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/

Creating X-Frame-Options HTTP response header

Attackers can create their own website and use it to load the contents of your website within an iframe. This can result in a clickjacking attack, whereby the attacker targets user input or tricks the user into performing undesired actions within the fake application.

To prevent this, you can create an X-Frame-Option HTTP response header. This stops site content from being embedded into other websites.

To create an X-Frame-Option HTTP response header

1. Open the configuration file `web.config` for the chosen web application.
2. In the `<configuration>` section, enter the following code snippet:

```
<httpProtocol>
    <customHeaders>
        <add name="X-Frame-Options" value="SAMEORIGIN" />
    </customHeaders>
</httpProtocol>
```

3. Save the file.

Running web applications in release mode

To prevent user session from being stolen, run your web applications in release mode. This stops the session ID being given in the HTML code.

To run web applications in release mode

1. Start the Web Designer program.
2. In the menu bar, click **View** > **Start page**.
3. In the toolbar, click **Select web application** and select the web application you want to use.
4. Click **Edit web application settings**.
5. Deselect the **Debugging** check box.

   TIP: If the check box is not set anyway, you do not have to do anything. You web application is now running in release mode.
6. Click **OK**.
7. Restart the Web Designer.
8. On the start page, select a web application and click **Release** (**Compile for release**).

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