One Identity Manager 8.0

Web Application Configuration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Web Application Configuration Guide
Updated - November 2017
Version - 8.0

Contents

Configuring Web Applications **1**

Configuring Web Portal **2**

IT Shop Configuration 2

Requesting by Reference User 2

Enable or Disable 'by Reference User' 3

Setting the Number of Reference Users 3

Sending the Shopping Cart 3

Setting the Request Priority 4

Confirming Requests 4

Forcing Reauthentication 5

Handling Required Products 5

Approver Options 6

Setting Validity Periods 6

Asking a Question 7

Require a Reason 7

Approval Decisions about URL Links 8

Starling Two-Factor Authentication **10**

Setting up Starling Two-Factor Authentication 10

Starling Two-Factor Authentication for Specific People 11

Logging in without Starling 2FA Tokens 11

Password Reset Portal **13**

Setting up a Password Reset Portal 13

Installing the Password Reset Portal 13

Authentication 14

Settable Passwords 14

Excluding Passwords from being Reset 15

Central Password 16

Defining Password Dependencies 16

Setting the Central Password 17

Setting up a New Application Token 17

About us **19**
Contacting us 19
Technical support resources 19

Configuring Web Applications

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

You can find out how to configure the IT Shop in the Web Portal or how to set up Starling Two-Factor Authentication. There is also step-by-step instructions for setting up the Password Reset Portal.

Configuring Web Portal

The Web Portal can be configured in the Web Designer. However, only IT Shop configuration will be handled In the next section.

IT Shop Configuration

You can configure the Web Portal's IT Shop in the Web Designer.

Requesting by Reference User

Table 1: Configuration Parameter for Requesting by Reference User

Configuration Parameter	Description
VI_ITShop_ProductSelectionByReferenceUser	Provides the functionality "By reference user" for requests in the Web Portal.
VI_ITShop_Filter_PersonReference	Specifies the number of reference users displayed. This configuration parameter is an SQL filter on the table "Person".

To make requests by reference user in the Web Portal or to determine the number of reference displayed, you must adjust the configuration parameter settings.

Detailed information about this topic

- Enable or Disable 'by Reference User' on page 3
- Setting the Number of Reference Users on page 3

Enable or Disable 'by Reference User'

In the Web Designer, you can specify whether it is possible to make a request using another user's requests. This function means requesting by reference user. To do this you must edit the configuration parameter "VI_ITShop_ProductSelectionByReferenceUser" in the Web Designer.

To enable or disable requesting by reference user

1. Open the Web Designer.
2. Open the module "VI_ITShop_ProduCtSelection" and search for "VI_ITShop_ProductSelectionByReferenceUser" in the definition tree view.
3. Select the configuration parameter "VI_ITShop_ProductSelectionByReferenceUser" in the definition tree view .
4. Switch to the **Configuration (custom)** view with where you can edit the configuration parameter.
5. Perform one of the following tasks.
    a. If you want to deactivate requesting by reference user: set **True** in the `Node editor` view.
    b. If you want to enable requesting by reference user: set **False** in the `Node editor` view.

Setting the Number of Reference Users

To set the number of reference users displayed in the Web Portal when you select a reference user, you must configure the configuration parameter in the Web Designer.

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

To set the number of reference users displayed

1. Open the Web Designer.
2. Open a module an search the definition tree view for "VI_ITShop_Filter_PersonReference".
3. Select the configuration parameter "VI_ITShop_Filter_PersonReference" in the definition tree view.
4. Enter the desired value **Value** in the **Node editor** view.

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 Request Priority on page 4
- Confirming Requests on page 4
- Forcing Reauthentication on page 5
- Handling Required Products on page 5

Setting the Request Priority

Table 2: 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" in the definition tree view.
3. Select the configuration parameter "VI_ITShop_DisablePWOPriorityChange" in the definition tree view.
4. Set the value to **true** in the `Node editor` view.

Confirming Requests

Table 3: 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 the configuration parameter "VI_ITShop_SubmitOrderImmediately".

To demand confirmation for a request

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

Forcing Reauthentication

Table 4: Configuration Parameter for Active Directory Authentication while Requesting

Configuration Parameter	Description	Setting	
		False	**True**
VI_ITShop_ TermsOf UseRe-quireAD Authentic-ation	Forces Active Directory reauthentication during execution of a request.	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 force 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" in the definition tree view.
4. Select the configuration parameter "VI_ITShop_ TermsOfUseRequireADAuthentication" in the definition tree view.
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 the Web Designer.

Table 5: 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.

The configuration parameter "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" in the definition tree view.
3. Mark the configuration parameter "VI_ITShop_ AllowRequestWithMissingDependencies" in the definition tree view.
4. Edit the configuration parameter on the **Configuration** tab by setting the value **true** in the `Node Edit` view. 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 6
- Asking a Question on page 7
- Require a Reason on page 7

Setting Validity Periods

Table 6: Configuration Parameter for Validity

Configuration Parameter	Description
VI_ITShop_ApproverCanSetValidFrom	Allows the approver to set a new start 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 the configuration parameters `VI_ITShop_ApproverCanSetValidFrom` and `VI_ITShop_ApproverCanSetValidUntil` you 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" in the definition tree view.
3. Select the configuration parameter "VI_ITShop_ApproverCanSetValidFrom" in the definition tree view.
4. Set the value to **true** in the `Node editor` view.
5. Search for "VI_ITShop_ApproverCanSetValidUntil" in the definition tree view.
6. Select the configuration parameter "VI_ITShop_ApproverCanSetValidUntil" in the definition tree view.
7. Set the value to **true** in the `Node editor` view.

Asking a Question

Table 7: Configuration Parameters for the Query

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

To ask a question

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

Require a Reason

Table 8: Configuration Parameter for Reason

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

To demand a reason

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

Approval Decisions about URL Links

Table 9: 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 an SQL filter condition on the table "AccProduct".	Product fulfills filter condition	Approval is not done directly. Displays form 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 which 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" in the definition tree view.

3. Select the configuration parameter "VI_ITShop_Approvals_InteractiveApproval" in the definition tree view.
4. Set the value to **true** in the Node editor view.

Starling Two-Factor Authentication

Multi-factor authentication guarantees better security for logging into web applications. One Identity Manager tools user 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 executed.

Setting up Starling Two-Factor Authentication

Table 10: Configuration Parameter for Multi-Factor Authentication

Configuration Parameter	Description
VI_Common_RequiresAccessControl	Requires authentication for web applications.
VI_Common_AccessControl_StarlingEnabled	Enables use of Starling Two-Factor Authentication.

Multi-factor authentication is done in the web project in the Web Designer.

To set up Starling Two-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 configuration parameter "VI_Common_RequiresAccessControl" in the definition tree view and set the value to `true` in the node editor view.
4. Mark the configuration parameter "VI_Common_AccessControl_StarlingEnabled" in the definition tree view and set the value to `true` in the node editor view.

Starling Two-Factor Authentication for Specific People

Table 11: Configuration Parameter for Multi-Factor 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 Starling Two-Factor Authentication only for specific people

1. Open the Web Designer.
2. Open a module and search for "VI_Common_AccessControl_Filter" in the definition tree view.
3. Mark the configuration parameter "VI_Common_AccessControl_Filter" 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 Starling 2FA Tokens

Table 12: Configuration Parameter for Logging in without Multi-Factor Authentication

Configuration parameter	Description	Setting	
		True	false
VI_Common_ AccessControl_ Starling_ AllowUnregistered	Allows users to log in to the web application without multi-factor authentication.	Users without a registered Starling 2FA token can log in to the web application without Starling Two-Factor Authentication.	Users without a registered Starling 2FA token cannot log in to the web application.

You can configure your web project to allow users without multi-factor authentication to log in to the web application.

To log in without Starling 2FA tokens

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`.

4

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 if guaranteed by multi-factor authentication.

Installing the Password Reset Portal

Table 13: 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 the project **QER_PasswordWeb** from **Web Project**.

   After selecting the web project, you will be 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 the configuration parameter "QER\Person\PasswordResetAuthenticator\ApplicationToken" and stored encrypted in the file `web.config`.

Authentication

Authentication on the Password Reset Portal differs from authentication on the Web Portal. The user has three options to choose from.

Table 14: 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.

Settable Passwords

Users can set the following default passwords.

Table 15: 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	AADUser.Password ADSAccount.UserPassword CSMUser.Password EBSUser.Password GAPUser.Password LDAPAccount.UserPassword NDOUser.Password SAPUser.Password UNSAccountB.Password

User	Password	Table / Column
	employee's sponsored identity, service identity or group identity. - OR - d. Assigned to one of the current user's shared user accounts.	UNXAccount.UserPassword
Members of the application role "Base roles\Administrators"	System user's password	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 .

In this case, "QER_PasswordWeb_IsAllowSet" is implemented, 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 16: 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 might be passwords that are calculated from other values or passwords for target systems that are only connected as read-only.

NOTE: In the script "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 the script "QER_PasswordReset_IsAllowSet".
3. Use the template "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's 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 17: Script for Declaring Passwords

Script	Description
QER_PasswordWeb_IsByCentralPwd	By default, the script checks whether the configuration parameter "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

Script	Description
	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 for the script QER_PasswordWeb_IsByCentralPwd.
3. Use the template "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.

   Based on these input parameters, the script must return the information as to whether the password is managed by the central password.
4. Save the setting in the Designer.
5. Compile the Password Reset Portal.

Setting the 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 15.

Setting up a New Application Token

You can set a new application toke using the `WebDesigner.ConfigFileEditor.exe` file.

To set a new application token

1. Open the `WebDesigner.ConfigFileEditor.exe` file.
2. Ensure that **QER_PasswordWeb** is set as the web project.

3. Click next to **Application token exists**.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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