



One Identity Manager 8.1

Web Application Configuration Guide

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.




Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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.

Contents

About this guide	5
Configuring the Web Portal	6
IT shop configuration	6
Requesting by reference user	6
Enabling or disabling 'by reference user'	7
Setting the reference user display	7
Sending the shopping cart	8
Setting the priority	8
Confirming requests	8
Forcing reauthentication	9
Handling required products	9
Approver options	10
Setting validity periods	10
Asking a question	11
Require a reason	11
Approval decisions about URL links	12
Displaying user-specific processes in the Web Portal	12
Starling Two-Factor Authentication	14
Setting up Starling Two-Factor Authentication	14
Starling Two-Factor Authentication for specific people	15
Logging in without Starling 2FA tokens	15
Password Reset Portal	17
Setting up a Password Reset Portal	17
Installing the Password Reset Portal	17
Authentication	18
Settable passwords	18
Excluding passwords from being reset	19
Central password	20
Defining password dependencies	20
Setting a central password	21

Setting up a new application token	21
Recommendations for secure operation of web applications	23
Disable automatic password storage	23
Disabling the HTTP request method TRACE	24
Using HTTP Strict Transport Security (HSTS)	24
Disabling insecure encryption mechanisms	25
Using Transport Layer Security 1.1 and above with Microsoft .NET Framework	25
Enable same site attribute for ASP.NET session cookies	26
About us	27
Contacting us	27
Technical support resources	27

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 the One Identity Manager documentation is available in the Support-Portal under [Online-Documentation](#). Videos providing further information are available at www.YouTube.com/OneIdentity.

Configuring the Web Portal

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

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

Detailed information about this topic

- [IT shop configuration](#) on page 6
- [Displaying user-specific processes in the Web Portal](#) on page 12

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

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


Detailed information about this topic

- [Enabling or disabling 'by reference user'](#) on page 7
- [Setting the reference user display](#) on page 7

Enabling or disabling '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 "VI_ITShop_ProductSelectionByReferenceUser" in the Web Designer.

To enable or disable requesting by reference user

1. Open the Web Designer.
2. Open "VI_ITShop_ProduCtSelection" and search for "VI_ITShop_ProductSelectionByReferenceUser".
3. Select "VI_ITShop_ProductSelectionByReferenceUser".
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 tasks.
 - a. To disable requesting by reference user: In the **Node editor** view, set the value True.
 - b. To enable requesting by reference user: In the **Node editor** view, set the value false.

Setting the reference user display

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

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

To set the number of reference users displayed

1. Open the Web Designer.
2. Open a module and search for "VI_ITShop_Filter_PersonReference".
3. Select "VI_ITShop_Filter_PersonReference".
4. Enter the desired value **Value** in the **Node editor**.

Sending the shopping cart

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

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

To disable a priority setting

1. Open 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 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 "VI_ITShop_SubmitOrderImmediately".

To demand confirmation for a request

1. Open 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 4: Configuration parameter for Active Directory authentication while requesting

Configuration Parameter	Description	Setting	
		False	True
VI_ITShop_TermsOfUseRequireADAuthentication	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".
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 Web Portal. Configuration parameter settings are carried out in 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.

"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
- [Asking a question](#) on page 11
- [Require a reason](#) on page 11

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 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 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.

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 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 8: 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 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 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 "AccProduct" table.	<table><tbody><tr><td>Product fulfills filter condition</td><td>Approval is not done directly. Displays form for confirming the approval decision.</td></tr><tr><td>Product does not fulfill filter condition</td><td>Approval decision is made when the page is called. Approvers receive a message that the approval decision has been entered into the system.</td></tr></tbody></table>	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.
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 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 Web Designer.
2. Open a module and search for "VI_ITShop_Approvals_InteractiveApproval".
3. Select the configuration parameter "VI_ITShop_Approvals_InteractiveApproval".
4. Set the value to **true** in the Node editor.

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 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 enabled.
- In the Designer, check the **Common | ProcessState | JobHistory** configuration parameter. The configuration parameter must be enabled. As a value for the configuration parameter, select **ERRORorSELECTED** or **SELECTED**.
 - ① **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 enabled and should have the value **2**.
- In Designer, check the configuration parameters **Common | ProcessState | ProgressView | LifeTime** and **Common | ProcessState | JobHistory | LifeTime**. These configuration parameters define the retention time of the process information and notifications in the process history. The configuration parameters must be enabled. 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.

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".

3. Mark the configuration parameter "VI_Common_RequiresAccessControl" and set the value to true.
4. Mark the configuration parameter "VI_Common_AccessControl_StarlingEnabled" and set the value to true.

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 Web Designer.
2. Open a module and search for "VI_Common_AccessControl_Filter".
3. Mark the configuration parameter "VI_Common_AccessControl_Filter".
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 Web Designer.
2. Open a module and search for "VI_Common_AccessControl_Starling_AllowUnregistered".
3. Mark the configuration parameter "VI_Common_AccessControl_Starling_AllowUnregistered".
4. Set the value in the node editor view to true.

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 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 **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.

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 (QBMPProduct)
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	AADUser.Password
	a. Directly assigned to the current employee.	ADSAccount.UserPassword CSMUser.Password
	- OR -	EBSUser.Password
	b. Assigned to the current employee's sub identity.	GAPUser.Password LDAPAccount.UserPassword
	- OR -	NDOUser.Password
	c. Assigned to the current employee's sponsored	SAPUser.Password UNSAccountB.Password

User	Password	Table / Column
	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	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 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 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 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 "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

Script	Description
	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 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 19.

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**.

Recommendations for secure operation of web applications

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

Detailed information about this topic

- [Disable automatic password storage](#) on page 23
- [Disabling the HTTP request method TRACE](#) on page 24
- [Using HTTP Strict Transport Security \(HSTS\)](#) on page 24
- [Disabling insecure encryption mechanisms](#) on page 25
- [Using Transport Layer Security 1.1 and above with Microsoft .NET Framework](#) on page 25
- [Enable same site attribute for ASP.NET session cookies](#) on page 26

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 18: 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. Open **Edit | Configure project | Web project**.

3. Search for "VI_Common_Login_PrefillLoginData" on the **Configure Project** tab.
4. Click **+** on the **Allow prefill of login data** key in the **Value (custom)** column.

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.

- 1 **NOTE:** The software "IIS Crypto" from Nartac.com is recommended for disabling encryption methods and protocols. For more information about disabling encryption, see <https://www.nartac.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>

Using Transport Layer Security 1.1 and above with Microsoft .NET Framework

One Identity tools are currently shipped based on Microsoft .NET Framework 4.7.2. To establish the connection, Microsoft .NET Framework 4.7.2 uses maximum Transport Layer Security (TLS) 1.0 by default. In order to use later versions of TLS, the registry key must be altered in Windows.

Set the following registry subkeys in the Windows Registry Editor.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
```

Detailed information about this topic

- <https://docs.microsoft.com/en-us/officeonlineserver/enable-tls-1-1-and-tls-1-2-support-in-office-online-server>

Enable same site attribute for ASP.NET session cookies

To avoid Cross Site Request Forgery (CSRF), you can set the same site attribute in 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.

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

1. Download the **URL Rewrite** extension: <https://www.iis.net/downloads/microsoft/url-rewrite>
2. Open the configuration file web.config for the chosen web application.
3. Enter the following code snippet in the <system.webServer> section:

```
<rewrite>
  <outboundRules>
    <clear />
    <rule name="Add SameSite" preCondition="No SameSite">
      <match serverVariable="RESPONSE_Set_Cookie" pattern=".*" negate="false" />
      <action type="Rewrite" value="{R:0}; SameSite=lax" />
      <conditions>
      </conditions>
    </rule>
    <preConditions>
      <preCondition name="No SameSite">
        <add input="{RESPONSE_Set_Cookie}" pattern="." />
        <add input="{RESPONSE_Set_Cookie}" pattern="; SameSite=lax" negate="true" />
      </preCondition>
    </preConditions>
  </outboundRules>
</rewrite>
```

4. Save the file.

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 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