

# One Identity Starling Two-Factor HTTP Module 3.0

## Release Notes

### August 2020

These release notes provide information about the One Identity Starling Two-Factor HTTP Module release.

## About this release

One Identity Starling Two-Factor HTTP Module protects on-premise websites with Starling Two-Factor Authentication. Starling Two-Factor HTTP Module acts as a filter and requires users to authenticate through Starling Two-Factor Authentication to get access to the websites hosted on the web server.

## New features

New features in the Starling Two-Factor HTTP Module 3.0

- Starling Two-Factor HTTP Module Configuration User Interface (UI) has been simplified and redesigned to streamline configuration of HTTP Module.
- Support for Windows Server 2019

# Enhancements

The following is a list of enhancements implemented in Starling Two-Factor HTTP Module 3.0.

**Table 1: General enhancements**

Enhancement	Issue ID
You can now connect your HTTP Module instance directly to your Starling account.	34679

# Resolved issues

The following is a list of issues addressed in this release.

**Table 2: General resolved issues**

Resolved Issue	Issue ID
While authenticating using HTTP module, multiple push notification requests are sent to the Starling 2FA App.	21934

# Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

**Table 3: General known issues**

Known Issue	Issue ID
When user clicks <b>Change Account</b> in <b>Connect Starling</b> tab and denies joining Starling after entering the credentials, and then tries to rejoin Starling, the <b>Login to Starling</b> window displays previously stored session details. <b>Workaround</b> Close and reopen the configuration tool window to view the login page again so that the user can use any account to connect to Starling.	245048

Known Issue	Issue ID
A warning message is displayed in Starling Two-Factor authentication page if the user has selected 'Use SSL' checkbox in the configuration tool and not configured LDAP over SSL in domain controller.	22226
<b>Workaround</b>	
Configure LDAP over SSL in domain controller.	
Starling Two-Factor authentication does not work if ISAPI agent and Starling 2FA HTTP module both are added for the same site.	21311
<b>Workaround</b>	
Deselect the protected site from ISAPI agent.	
Starling Two-Factor authentication may not be launched if user selects an internal path(s) or a section of a web application are selected.	21450
<b>Workaround</b>	
Select the entire web application.	

## Upgrade and installation instructions

To upgrade to the latest version of One Identity Starling Two-Factor HTTP Module, run the Starling.2FA.HttpModule.exe file and follow the on-screen instructions. After upgrading to the latest version, the configuration settings will be retained.

- *In case of an upgrade from Starling Two-Factor HTTP Module 2.x to 3.0, you must connect to Starling as the Subscription key related provision is removed. You can connect to Starling using the credentials that were used earlier to create the Starling account.*
- Post upgrade, all configurations that were part of the earlier version of the HTTP Module will be retained. For information on connecting to Starling, see *Connecting Starling for authentication* section in the Admin Guide.

## System requirements

Before installing Starling Two-Factor HTTP Module 3.0, ensure that your system meets the following minimum hardware and software requirements.

# Hardware requirements

**Table 4: Hardware requirements**

Requirement	Details
Processor	1.4 GHz or faster, x64 architecture
Memory	4 GB
Hard disk space	50 MB or more
Operating system	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012

# Software requirements

**Table 5: Software requirements**

Requirement	Details
Microsoft .NET Framework	Microsoft .NET Framework 4.5.2 or later
Microsoft IIS	7.0 or later
Windows firewall port	443
.NET Framework for Default application pool in IIS	4.0 or later

# Product licensing

Use of this software is governed by the Software Transaction Agreement found at <https://www.oneidentity.com/legal/sta.aspx>. This software does not require an activation or license key to operate.

# Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section

does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

# 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

# Third-party contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing <https://www.oneidentity.com/legal/license-agreements.aspx>. Source code for components marked with an asterisk (\*) is available at <http://opensource.quest.com>.

**Table 6: List of Third-Party Contributions**

<b>Component</b>	<b>License or Acknowledgement</b>
Log4Net 2.0.8	Copyright © 2004-2017 The Apache Software Foundation This component is governed by <a href="#">Apache 2.0</a>
Microsoft ASP.NET MVC 5.x	Copyright © Microsoft Open Technologies, Inc. All rights reserved This component is governed by <a href="#">Apache 2.0</a>
Newtonsoft.Json.Net 12.0.3	Copyright © 2007 James Newton-King This component is governed by <a href="#">MIT Json.NET N/A</a>

**Copyright 2020 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](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

**Legend**

-  **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**
  
-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**