



One Identity Starling Two-Factor HTTP  
Module 3.0

Administration Guide

## 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.

# Contents

<b>Overview</b> .....	<b>4</b>
Starling Two-Factor HTTP Module Network diagram .....	4
<b>Installing Starling Two-Factor HTTP Module</b> .....	<b>6</b>
Prerequisites for installation .....	6
Downloading and running the installer .....	6
<b>Starling Two-Factor HTTP Module Configuration</b> .....	<b>8</b>
Connecting Starling for authentication .....	8
Prerequisites to connect Starling .....	9
Connecting HTTP Module to Starling .....	9
Configuring Push notification settings .....	10
Configuring user repository for Active Directory .....	10
Prerequisites to configure user repository .....	10
Configuring protected server sites .....	11
<b>Logging into the client application</b> .....	<b>13</b>
OTP through SMS .....	13
OTP through phone call .....	14
OTP through Starling 2FA app .....	14
Push Notifications in Starling 2FA app .....	14
<b>Diagnostic logging</b> .....	<b>16</b>
Enabling diagnostic logging for Configuration tool .....	16
Enabling diagnostic logging for web interface .....	17
Disabling diagnostic logging for configuration tool .....	17
Disabling diagnostic logging for web interface .....	18
<b>Uninstalling Starling Two-Factor HTTP Module</b> .....	<b>19</b>
<b>About us</b> .....	<b>20</b>
Contacting us .....	20
Technical support resources .....	20

## Overview

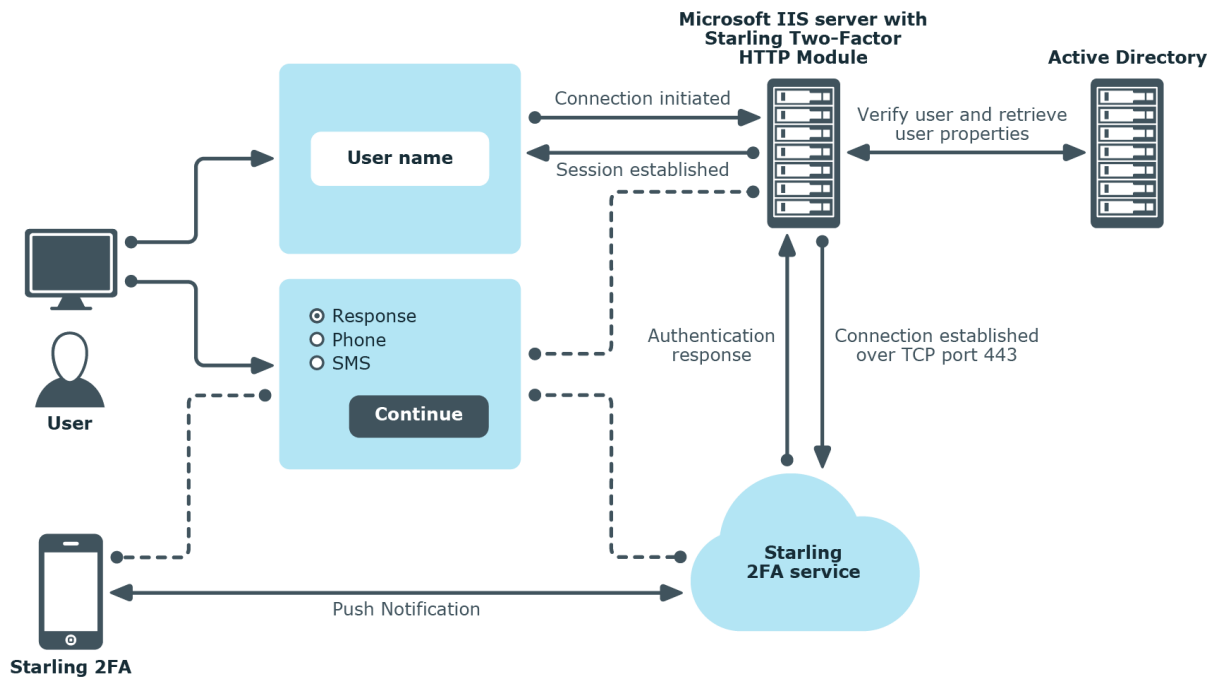
One Identity Starling Two-Factor HTTP Module protects on-premise websites with Starling Two-Factor Authentication. You can use One Identity Starling Two-Factor HTTP Module to secure access to websites hosted on Microsoft Web Server (IIS). For that you must deploy One Identity Starling Two-Factor HTTP Module on the web server that hosts the websites. 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.

**Figure 1: Starling Two-Factor HTTP Module deployment overview**



## Starling Two-Factor HTTP Module Network diagram

The following diagram provides an overview of the authentication flow.



If you have an application that uses HTTP Module, you can use the Starling Two-Factor HTTP Module as a Software as a Service for two-factor authentication. The Starling Two-Factor HTTP Module forwards the authentication requests from the customer application to Starling Two-Factor Authentication. Starling Two-Factor Authentication validates the requests and responds to the applications with an appropriate authentication response (Access-Accept, Access-Reject, or Access-Challenge).

# Installing Starling Two-Factor HTTP Module

The following sections brief about the prerequisites and the steps to download and install the latest version of the Starling Two-Factor HTTP Module.

- [Prerequisites for installation](#)
- [Downloading and running the installer](#)

## Prerequisites for installation

The following are the prerequisites for installing Starling Two-Factor HTTP Module

- Microsoft .NET Framework 4.5.2 or later
- Microsoft IIS (7.0 or later)
- Windows firewall port 443
- Starling Two-Factor Authentication subscription
- A valid mobile number and email address configured for the user

## Downloading and running the installer

The following sections brief about the steps to download and install the latest version of the **Starling Two-Factor HTTP Module**.

### ***To download the installer***

1. On the [support.oneidentity.com](https://support.oneidentity.com) site, sign in to the One Identity account by entering credentials. If you do not have an account, click **Sign up for a new account**. You also have the option of signing in through the Microsoft account.

The **One Identity Support page** is displayed.

2. In the **Identity as a Service** section, click **Starling Two-Factor Authentication**.
3. In the **Download Software** section, click **See All Downloads** link.

The **Starling Two-Factor Authentication - Download Software** page is displayed.

4. Click **Starling Two-Factor HTTP Module 3.0**.

The **Download Starling Two-Factor HTTP Module 3.0** page is displayed.

5. Click **Add to Downloads**.

6. Review the terms and conditions and click **Continue**.

The **Add to My Downloads** page is displayed.

7. Click **Download Now** to download the .exe file.

8. Alternatively, click **Add to My Downloads** to save the application in the **My Downloads** cart. It is recommended to use this option when you are downloading multiple products.

The Starling.2FA.HttpModule.exe file is downloaded.

### **To run the installer**

1. Right-click on the installer and click **Run as Administrator**.
2. Follow the instructions on the installer to complete the installation.

**NOTE:** Elevated privileges are required to run the Starling Two-Factor HTTP Module configuration tool. Once the installation is complete, configure Starling Two-Factor HTTP Module settings. For details, see [Starling Two-Factor HTTP Module configuration](#).

#### **NOTE:**

- The default application pool in IIS requires .NET Framework version 4.0 or later.
- **The account under which you will be running the Setup must be a member of the local administrators group.**

#### **IMPORTANT:**

- *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. Connect to Starling using the credentials that were used earlier to create the Starling account.*
- All configurations that were part of the earlier version of HTTP Module will be retained after the upgrade. For more information on connecting to Starling, see [Connecting Starling for authentication](#).

# Starling Two-Factor HTTP Module Configuration

You can configure the Starling Two-Factor HTTP Module for two factor authentication by setting the required parameters in the Starling Two-Factor HTTP Module Configuration window.

You can set the parameters using the following options that are displayed on the **Starling Two-Factor HTTP Module configuration** window:

- **Home:** Displays the various configuration options in a tree view and as tiles.
- **Connect Starling:** Allows you to connect to the Two-Factor Authentication subscription by logging in to your One Identity Starling account.
- **Push Notification:** Allows you to configure the push notifications messages and timeout settings.
- **Active Directory:** Configures the repository for data stored in Active Directory.
- **Protected Server Sites :** Allows you to protect the websites hosted on your IIS.

## Connecting Starling for authentication

To use the Starling Two-Factor authentication for HTTP Module, you must first connect to Starling using the Starling Join option available for One Identity on-premises products.

To obtain a Starling Two-Factor Authentication subscription and register with Starling, click <https://www.cloud.oneidentity.com/>.

**NOTE:** If you do not have a Starling account, you can create a new account. For more information on creating a Starling account, see the *One Identity Starling User Guide*.

To connect to Starling for authentication, see

- [Prerequisites to connect Starling](#)
- [Connecting HTTP Module to Starling](#)



# Prerequisites to connect Starling

Following are the prerequisites to connect to Starling

- User must have One Identity Starling account. For more information on creating a One Identity Starling account, see the *Starling Two-Factor Authentication Administration Guide*.
- The Starling Account must be activated with a valid Two-Factor Authentication subscription.

## Connecting HTTP Module to Starling

After the pre-requisites to connect to Starling are met, connect HTTP Module to Starling using the Starling Join option available for One Identity on-premises products.

### **To connect and configure One Identity Starling for authentication**

1. On the Starling Two-Factor HTTP Module configuration window, click **Connect Starling**.

The **Connect Starling** window is displayed.

2. Click **Connect my account**.

You are redirected to the **One Identity Starling** authentication window.

3. Provide your Starling credentials and click **SIGN IN**.
4. In the **Join to Starling** window, click **Allow**.

**NOTE:** If you are a member of more than one Starling organization, use the drop-down to select the organization to which you want to connect.

5. Click **Join**.

After successful authentication, you are redirected to the One Identity Starling Two-Factor HTTP Module Configuration **Connect Starling** window.

**NOTE:** To connect to a different organization in your One Identity Starling account, click **Change Account**.

If the connection is unsuccessful, a message is displayed providing the details of the error and the previously connected account is continued to be used. In such a case, it is recommended to contact support for any help.

**NOTE:** If there are any network issues or if the Starling is down, your account may get disconnected. In such cases, click **Reconnect**. To test the validity of your account connection, click **Test connection**.

# Configuring Push notification settings

Push notification enables you to Approve or Deny login requests. These requests facilitate an end-to-end encrypted communication between the application and a secured authentication service. Accurate configuration of the push notification allows you to Approve or Deny a login attempt.

## *To configure the push notification settings*

1. On the Starling Two-Factor HTTP Module Configuration page, click **Push Notifications**.

Push Notifications page is displayed.

2. On the **Message** field, enter a message to be displayed in the Starling Two-Factor application.

The message entered must be in the range of 10 to 50 characters.

3. On the **Timeout (seconds)** field, select the timeout duration or the validity of the notification from the drop-down menu. If you select **Other**, you can specify the customized timeout duration in seconds. By default, 60 seconds is set as a timeout duration for notifications.
4. Click **Save Settings** after completing the configuration.

# Configuring user repository for Active Directory

Use the **Active Directory** tab to configure the user repository details.

## Prerequisites to configure user repository

The following are the pre requisites to configure user repository

- A domain controller must exist.
- User must have the minimum read permission to query the Active Directory and read user data.

### ***To configure the repository for data stored in Active Directory***

1. In the **Starling Two-Factor HTTP Module Configuration** window, click the **Active Directory** tab and configure the following parameters:
  - **Domain name:** Enter the name of the Active Directory domain.
  - **User name:** Allows you to enter the name of the user used for querying the Active Directory.
  - **Password:** Allows you to enter the account password used to access the Active Directory.
  - **Base DN:** This is the path from where user search is performed. You must specify the root container to search the users in the format **cn=users,dc=domain,dc=com**, where **cn** is Common Name and **dc** is Domain Component. If Base DN is not specified, the entire directory is searched to locate the users.
  - **Use SSL:** Select this check box to enable LDAP over SSL for communicating with the Active Directory server.
  - **Test Connection** : Clicking this button will validate whether the entered domain credentials are valid or not.
  - **Advanced Settings:** Allows to modify the Active Directory attribute mapping. These attribute values are used during authentication. You can update the Active Directory attribute fields in the **Active Directory Advanced Settings** window as per the requirement. In the window, you can map Name, Email, and Phone Number to the attributes in Active Directory. The username entered in the client application will be validated against the Name attribute during two-factor authentication. By default, Name attribute is mapped to the samAccountName attribute in Active Directory.

## **Configuring protected server sites**

The Starling Two-Factor HTTP Module allows you to protect your websites. You can add the websites that you want to protect in the **Protected Server Sites** tab. The tab lists the websites in the Microsoft Web Server (IIS). You can select the required websites that have to be protected. You can enable protection for one or more websites both at server level and at the application level by selecting the appropriate check boxes.

### ***To configure the protected server sites***

1. In the Starling Two-Factor HTTP Module Configuration window, click the **Protected Server Sites** tab and select one or more websites that you want to secure with the Starling Two-Factor Authentication.
2. Click **Save Settings**.

To reflect the changes made during configuration after clicking **Save Settings**, Starling Two-Factor HTTP Module prompts you to restart IIS. You can click **Yes** to reflect the changes.

**NOTE:** Web applications having dependent sites will also show Starling Two-Factor authentication page, since they internally access the same URL.

For example, if the user protects OWA web application using Starling Two-Factor authentication, ECP or all dependent websites that also access OWA internally will also see the Starling Two-Factor authentication page. Access control is determined by the most specific path match found.

**NOTE:** Certain web applications does not allow you to edit the web.config file. It is recommended to avoid protecting these applications from the Two-Factor authentication.

## Logging into the client application

When you log in to the protected web site locally or remotely with a valid Active Directory username, Starling Two-Factor HTTP Module sends a push notification to Starling 2FA app automatically. Alternatively, you can click **Sign-in with other options** link from the Starling Two-Factor Authentication Log-in page. After clicking the link, the Token Response page is displayed. Based on the option selected, the token response is provided through SMS, Phone Call, or the Starling 2FA app.

When you log in to the application for the first time, during two-factor authentication, you will receive an SMS to install the Starling 2FA app if:

- You have not installed the Starling 2FA app.
- The **Installation Instructions** option in the Starling Two-Factor Authentication Dashboard is enabled.

Use one of the following methods for Two-Factor Authentication.

- [OTP through SMS](#)
- [OTP through phone call](#)
- [OTP through Starling 2FA app](#)
- [Push Notifications in Starling 2FA app](#)

## OTP through SMS

### **To generate OTP through SMS**

1. On the Starling Two-Factor Authentication Token response page, click **Send SMS**. You will receive an OTP through SMS on the registered phone number
2. Enter the received OTP in the token response field of the Starling Two-Factor Authentication **Token Response** page, and click **Continue** to log in.

# OTP through phone call

## *To generate OTP through phone call*

1. On the Starling Two-Factor Authentication Token response page, click **Phone Call**. You will receive a phone call on the registered mobile number.
2. Enter the received OTP in the token response field of the Starling Two-Factor Authentication **Token Response** page, and click **Continue** to log in.

# OTP through Starling 2FA app

## *To generate OTP through Starling 2FA app*

1. If you have installed Starling 2FA app, your account is added to Starling 2FA app. If you have not installed the Starling 2FA app, install the app and register your phone number. Your account will be added to the Starling 2FA app.

**NOTE:** Install the Starling 2FA app either by clicking the link in the SMS you have received or from the app store.

2. Enter the received OTP from the Starling 2FA App in the token response field of the Starling Two-Factor Authentication **Token Response** page, and click **Continue** to log in.

### **NOTE:**

- The Starling 2FA app is available on Android and iOS for Mobile versions, and Windows and Macintosh for Desktop versions.
- You can download the Starling 2FA app using **Get the app** link (<https://2fa.cloud.oneidentity.com/install>) to automatically detect which version to install.

# Push Notifications in Starling 2FA app

To use push notifications, you must install Starling 2FA app and register your phone number.

**NOTE:** The Starling 2FA app can be used for two-factor authentication on Android or iOS devices, for Mobile versions, and the Windows or Macintosh for Desktop versions.

## *To use push notifications*

1. If you have not installed the Starling 2FA app on your mobile device, install the app from the app store or using **Get the app** link

(<https://2fa.cloud.oneidentity.com/install>).

2. Open the Starling 2FA app and navigate to the **Requests** menu.
3. In the **Pending** tab, approve the request to log in to the application.

## Diagnostic logging

To troubleshoot issues that may occur during authentication with Starling Two-Factor HTTP Module, you need to enable diagnostic logging. You can enable or disable diagnostic logging for the configuration tool and the web UI.

By default, diagnostic logging is disabled. After enabling or disabling diagnostic logging, you must restart the configuration tool and client application.

### Enabling diagnostic logging for Configuration tool

#### ***To enable diagnostic logging for Starling Two-Factor HTTP Module Configuration tool:***

1. On a computer where Starling Two-Factor HTTP Module is installed, go to the **bin** folder in the installation directory. Normally, the path to the folder is **%ProgramFiles%\One Identity\Starling Two-Factor HTTP Module\bin**.
2. Make the following changes to **Starling.TwoFactor.HttpModule.Settings.exe.config** file in the **bin** folder:
  - In the **<log4net debug="false">** entry, set the value to **true**. For example, **<log4net debug="true">**
  - In the **<level value="ERROR" />** entry, set the value to **DEBUG**. For example, **<level value="DEBUG"/>**

You can find the log file, **Configuration.log**, in **%ProgramData%\One Identity\Starling Two-Factor HTTP Module**.



# Enabling diagnostic logging for web interface

**To enable diagnostic logging for Starling Two-Factor HTTP Module web interface:**

1. On a computer where Starling Two-Factor HTTP Module is installed, go to **Starling Two-Factor HTTP Module** folder in the installation directory. Normally, the folder path is **%ProgramFiles%\One Identity\Starling Two-Factor HTTP Module**.
2. Make the following changes to the **web.config** and **log4net.config** files in the **Starling Two-Factor HTTP Module** folder:
  - In the **<log4net debug="false">** entry, set the value to **true**. For example, `<log4net debug="true">`
  - In the **<level value="ERROR" />** entry, set the value to **DEBUG**. For example, `<level value="DEBUG"/>`

You can find the log file **HttpModuleWeb.log** in **%ProgramData%\One Identity\Starling Two-Factor HTTP Module**.

# Disabling diagnostic logging for configuration tool

**To disable diagnostic logging for Starling Two-Factor HTTP Module configuration tool:**

1. On a computer where Starling Two-Factor HTTP Module is installed, go to the **bin** folder in the installation directory. Normally, the path to the folder is **%ProgramFiles%\One Identity\Starling Two-Factor HTTP Module\bin**.
2. Make the following changes in **Starling.TwoFactor.HttpModule.Settings.exe.config** file in the **bin** folder:
  - In the **<log4net debug="true">** entry, set the value to **false**. For example, `<log4net debug="false">`
  - In the **<level value="DEBUG" />** entry, set the value to **ERROR**. For example, `<level value="ERROR"/>`

# Disabling diagnostic logging for web interface

**To disable diagnostic logging for Starling Two-Factor HTTP Module web interface:**

1. On a computer where Starling Two-Factor HTTP Module is installed, go to **Starling Two-Factor HTTP Module** folder in the installation directory. Normally, the path to the folder is **%ProgramFiles%\One Identity\Starling Two-Factor HTTP Module**.
2. Make the following changes to the **web.config** and **log4net.config** files in the **Starling Two-Factor HTTP Module** folder:
  - In the **<log4net debug="true">** entry, set the value to **false**. For example, `<log4net debug="false">`
  - In the **<level value="DEBUG" />** entry, set the value to **ERROR**. For example, `<level value="ERROR"/>`

## Uninstalling Starling Two-Factor HTTP Module

The following section briefs about the steps to uninstall the **Starling Two-Factor HTTP Module**.

### ***To uninstall the Starling Two-Factor HTTP Module***

1. Navigate to **Programs and Features** in Control Panel.
2. Click **One Identity Starling Two-Factor HTTP Module**, and then click **Uninstall**.

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