One Identity Starling Two-Factor HTTP Module 2.3

Administration Guide

Starling Two-Factor HTTP Module Administration Guide
Updated - April 2020
Version - 2.3

Contents

1

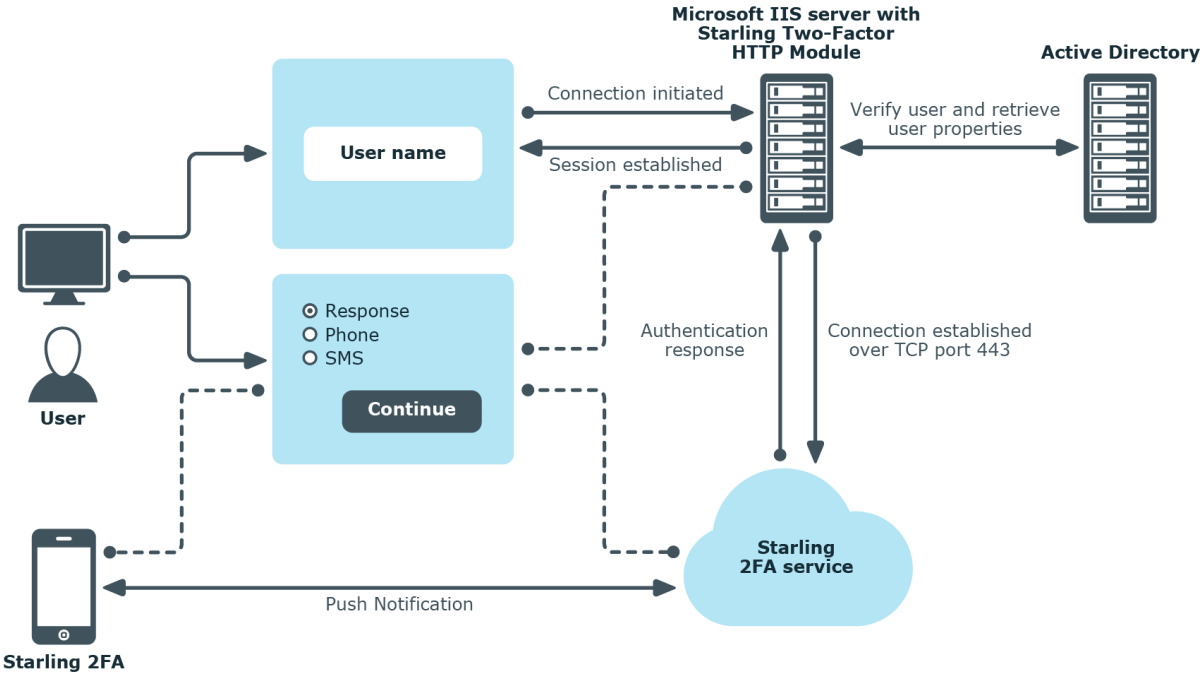
Overview

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).

2

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 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 2.3**.

   The **Download Starling Two-Factor HTTP Module 2.3** 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**.

3

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.

To complete the configuration process, you must configure the following

- Configuring Starling Two-Factor Authentication
- Configuring user repository for Active Directory
- Configuring protected sites

Configuring Starling Two-Factor Authentication

Using the Starling Two-Factor HTTP Module Configuration window, you can complete the Two-Factor Authentication configuration for HTTP Module.

To configure the Configuration tab

1. In the **Starling Two-Factor HTTP Module Configuration** window, click the **Configuration** tab to provide the following details:
    - **Subscription key**: Allows you to enter the subscription key available in the Starling Two-Factor Authentication Dashboard.
    - **Message**: Allows you to enter the message that has to appear in the 2FA app as a push notification for the user.
    - **Timeout (seconds)**: Allows you to enter the duration until which the push notification message received on Starling 2FA app is valid.

Configuring user repository for Active Directory

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

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.

      NOTE: The user account must have read-only permission to query the Active Directory.
    - **Password**: Allows you to enter the 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.
    - **Advanced**: Click this button to open the **Advanced Settings** window to modify the mapping details of the Active Directory attributes.

      NOTE: These attribute values are used during authentication.

Configuring protected 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 sites

1. In the Starling Two-Factor HTTP Module Configuration window, click the **Protected server sites** tab, select one or more websites that you want to secure with the Starling Two-Factor HTTP Module
2. Click **Apply**.

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

NOTE: When you try to log in to the Starling Two-Factor HTTP Module for the first time and if the Starling 2FA app is not installed, you will receive an SMS asking you to install the Starling 2FA app.

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

Using Push Notification

To receive a push notification, your phone number must be registered with your Starling account. You can approve or deny a push notification that is sent to your phone.

NOTE: If your phone does not receive the push notification, perform the following.

1. Open the Starling 2FA app and go to **Requests** menu.
2. Approve the request in the **Pending** tab to log in to the system.

Using OTP

You can perform the two-factor authentication using one of the following methods for authentication. If the user account is valid and active, they will be authenticated and permitted to access the protected website.

- OTP through SMS
- OTP through phone call
- OTP through 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.

5

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="false">*
    - In the **<level value="ERROR" />** entry, set the value to **DEBUG**. For example, *<level value="ERROR"/>*

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"/>*

6

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**.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product