One Identity Starling Two-Factor HTTP Module 2.0

Administration 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.

Starling Two-Factor HTTP Module Administration Guide
Updated - May 2018
Version - 2.0

Contents

1

Overview

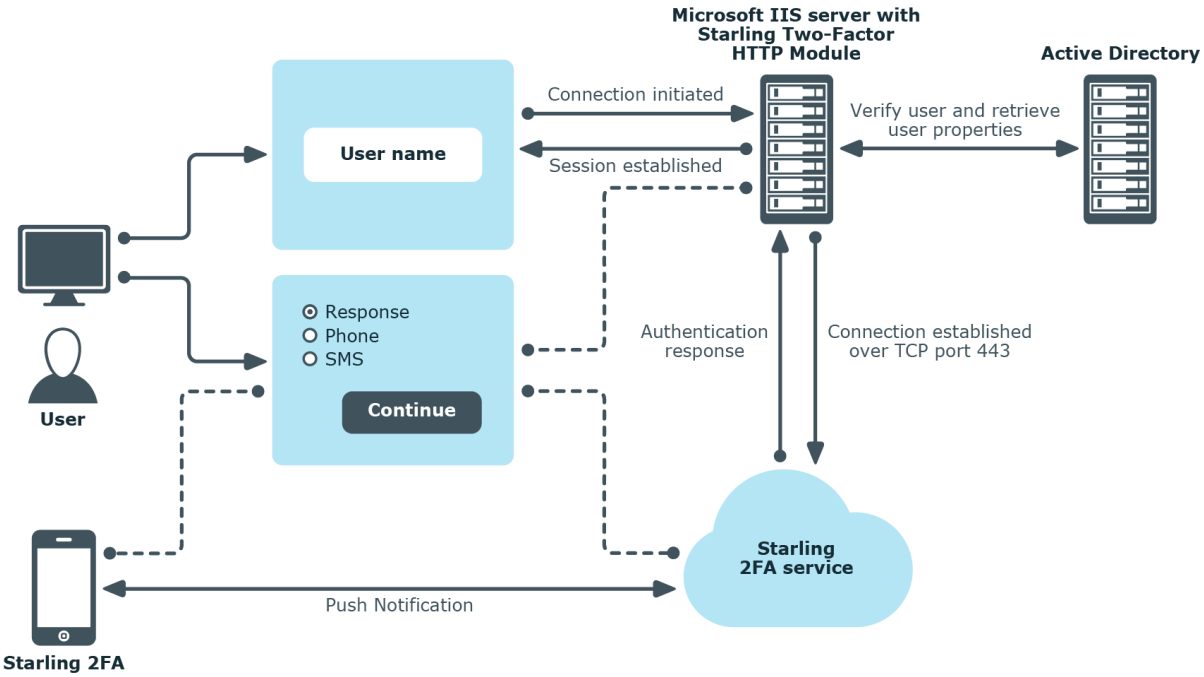
One Identity Starling Two-Factor HTTP Module protects on-premise websites with Starling Two-Factor Authentication. You can use One Identity Starling Two-Factor HTTP Module to secure access to websites hosted on Microsoft Web Server (IIS). For that you must deploy One Identity Starling Two-Factor HTTP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

Prerequisites

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) role is installed
- Windows firewall port 443 must be available
- Starling Two-Factor Authentication subscription
- A valid phone number and email id is configured for the user

Network diagram



Running the installer

To run the installer:

- Double-click the installer and follow the instructions on the installer screens and complete the installation.

NOTE: Elevated privileges are required to run the HTTP Module configuration tool. After 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.

2

Starling Two-Factor HTTP Module configuration

You can configure Starling Two-Factor HTTP Module for two-factor authentication by setting the required parameters in **Starling Two-Factor HTTP Module Configuration** window. In the configuration window, you can configure your Starling Two-Factor Authentication subscription and push notification details, user repository details and protected server site details. These details are required to carry out two-factor authentication.

Configuring Starling Two-Factor Authentication

To configure Starling Two-Factor Authentication:

1. Click the **Configuration** tab, provide the following details:
    - **Subscription key**: The subscription key obtained from Starling Two-Factor Authentication Dashboard.
    - **Message**: The push notification message that has to be displayed on Starling 2FA app.
    - **Timeout (seconds)**: The duration for which the push notification message received on Starling 2FA app is valid.

Configuring user repository for Active Directory

To configure the repository for data stored in Active Directory:

1. Click **Active Directory** tab and provide the following parameters:
    - **Domain name**: Domain name of the Active Directory.
    - **User name**: Name of the account used for querying the Active Directory.

        NOTE: The user account must have read-only permission to query the Active Directory.

    - **Password**: Password of the account used for querying the Active Directory.
    - **Base DN**: Point from where the server searches for users. 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**: Option to enable LDAP over SSL for communicating with Active Directory server.
    - **Advanced**: Option to modify the Active Directory attribute mapping. You can update the **AD attribute** fields in the **Active Directory Advanced Settings** window as per the requirement. In the window, you can map **Name**, **E-mail** and **Phone Number** to the attributes in Active Directory.

        NOTE: The username is verified with **Name** attribute during Two-Factor authentication. By default, **Name** is verified with **sAMAccountName**, **userPrincipalName**, or **name** attribute in Active Directory.

Configuring protected sites

Starling Two-Factor HTTP Module allows you to protect your websites. You can add the websites that you want to protect using Starling Two-Factor HTTP Module in the **Protected server sites** tab. The tab lists the websites in the domain. You can select the required websites that has to be protected. Protection can be enabled at server sites and application level selectively.

To configure the protected sites:

- On **Protected server sites** tab, select the websites that you want to secure with Starling Two-Factor HTTP Module from the tree view and click **Apply** or **OK**.

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 with Starling Two-Factor authentication, ECP or all dependent websites which also access OWA internally will see Starling Two-Factor authentication page. Access control is determined by the most specific path match found.

NOTE: Certain web applications do not allow editing the 'web.config' file. The user must not select these web applications for 2FA protection, as “Error while adding the module in web config for selected sites” message may be displayed.

Accessing Protected Website

To access protected website

1. Using any supported browser, access the protected website. On the Starling Two-Factor Authentication Log-in page, enter your user name and click **Sign in**.

   NOTE: When you are logging into the client application for the first time, you will receive an SMS to install Starling 2FA app during two-factor authentication, if:

   - you have not installed Starling 2FA app **and**
   - the **Installation instructions** option under settings of Starling Two-Factor Authentication Dashboard is enabled.

2. In the next page, if the user account exists in Active Directory then a push notification approval request will be sent automatically to the mobile device. If the user clicks on **Sign in with other options** link, token response page is displayed. Use one of the following methods for authentication. If user account is valid and active, they will be authenticated and permitted to access the protected website.

   a. ***Use push notifications:***

      NOTE: To use push notifications you must install Starling Two-Factor Authentication application and register your phone number.

      i. Open Starling Two-Factor Authentication application and go to **OneTouch** menu.

      ii. Approve the request in the **Pending** tab to log in to the client application.

   b. ***Use OTP:***

      OTP can be obtained through one of the following methods.

      - OTP through SMS
      - OTP through phone call
      - OTP through Starling 2FA app

OTP through SMS

To generate OTP through SMS:

1. On Starling 2FA authentication token response page, click **Send SMS**. You will receive an SMS.
2. Enter the OTP received through SMS, in the token response field of the Starling 2FA authentication token response page, and click **Continue** to log in.

OTP through phone call

To generate OTP through phone call:

1. On the Starling 2FA authentication token response page, click **Phone Call**. You will receive a phone call.
2. Enter the OTP received from the phone call, in the token response field of the Starling 2FA 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, then your token will be added to Starling 2FA app. If you have not installed Starling 2FA app, install the app and register your phone number (Install the app either from the SMS you have received or from the app store). Your token will be added to Starling 2FA app.
2. Enter the OTP received from the Starling 2FA application, in the token response field of the Starling 2FA authentication token response page, and click **Continue** to log in.

NOTE: Starling 2FA app can be used for two-factor authentication on Android, iOS and Chrome.

3

Diagnostic logging

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

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

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product