HarePoint Multi-Factor Authentication


Product version 1.3
March 31, 2022
# Table of Contents

Table of Contents ................................................................. 2  
I. Introduction ........................................................................... 3  
II. Deployment ............................................................................. 4  
   1. System requirements ............................................................. 4  
   2. Licensing and trial limitations .............................................. 5  
   3. Installing HarePoint Multi-Factor Authentication for SharePoint ................................................................. 6  
III. Product Overview ................................................................. 9  
   1. Getting started ................................................................. 9  
   2. Enabling encryption of secrets .......................................... 12  
Appendix A. Manage MFA settings via PowerShell ....................... 16
I. Introduction

Multi-factor authentication (MFA) is defined as a security mechanism that requires an individual to provide two or more credentials in order to authenticate their identity. In IT, these credentials take the form of something you know (typically a password), something you have (a trusted device that is not easily duplicated, like a phone) and something you are (biometrics).

Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method.

HarePoint Multi-Factor Authentication allows you to secure user access to SharePoint portals and sites with efficient and reliable multi-factor authentication (MFA) solution.

The product supports on-premises SharePoint environments and a set of authentication factors that will be constantly expanded.
II. Deployment

1. System requirements

HarePoint Multi-Factor Authentication is designed to operate in:

- Microsoft SharePoint Server Subscription Edition,
- Microsoft SharePoint Server 2019,
- Microsoft SharePoint Server 2016,
- Microsoft SharePoint Server 2013,
- Microsoft SharePoint Server 2010.

(hereinafter referred to as SharePoint) environments.

HarePoint Multi-Factor Authentication requires the following SharePoint service applications to be installed and configured:

- User Profile Service Application,
- Secure Store Service (optional).

The Product supports following types of authentication:

- Forms Based Authentication (FBA),
- Trusted Identity Provider (e.g. ADFS).

Windows Authentication is not supported.

The Product has no special requirements to the operating system and its components, RAM memory space and CPU type. The Product can operate on any of the above-mentioned SharePoint deployments.

No internet connection is required to use the authentication app as a second factor authentication method.

The internet connection is required if the SMS notification is selected as the second authentication method.
2. Licensing and trial limitations

HarePoint MFA for SharePoint is licensed by purchasing the required number of user licenses.

**SharePoint user** - a user authorized in any way on a SharePoint server; including users interacting with a SharePoint server through Microsoft Word, Microsoft Excel or other applications.

The number of user licenses for HarePoint MFA for SharePoint must be equal to the number of users having access to the SharePoint web-site(s).

There is no functional difference between the trial and the registered version except that:

1. There will be small box with trial warning on a login page.
2. The evaluation time for the trial version is 30 days.
3. Installing HarePoint Multi-Factor Authentication for SharePoint

To install the product, you'll need Farm Administrator rights.

Log into any WFE server of the SharePoint farm, unpack the product archive into a folder on the local disk. Run SETUP.EXE in the selected folder. Installation Wizard will start:

Should any problems be detected, please rectify them and restart the installation wizard.
Press Next button twice, accept End-User license agreement, and proceed to Deployment Targets step:

Select the web applications in which you plan to enable multi-factor authentication and click Next. The product deployment will start and you will see the window with the progress bar and deployment logs.
When the deployment is finished you will see message Installation completed successfully below the status bar:

![Installation Progress]

Click Next and Finish to exit the installation tool. The product is now installed and deployed.
III. Product Overview

1. Getting started

Open the Central Administration site and select “Security” section. Main settings of the Product located here in the “HarePoint Multi-Factor Authentication (MFA)” section.

When you first install the product, multi-factor authentication will not be enabled by default for users in your organization. We recommend that you first test it on specific users and only then enable it for all or a group of users.
To enable multi-factor authentication for a specific user, you can use the User Management page in the Product settings:

If you need to change settings of multiple user you can use PowerShell scripts located in Appendix A.

Then you need to configure additional authentication methods that will be available to users in your organization.
When you first time install the Product only Authenticator App method is enabled. You can enable additional authentication factors on the Authentication Settings page in the Product Settings:

The list of supported SMS service providers:

- Twilio ([https://www.twilio.com/](https://www.twilio.com/))
- Sinch ([https://www.sinch.com/](https://www.sinch.com/))
- Nexmo ([https://www.nexmo.com/](https://www.nexmo.com/))
- aql ([https://www.aql.com/](https://www.aql.com/))
- SMSGlobal ([https://www.smsglobal.com/](https://www.smsglobal.com/))

If you want to use a provider that is not in the list, then let us know via our support portal at [http://support.harepoint.com/](http://support.harepoint.com/)
2. Enabling encryption of secrets

Open Central Administration and go to Application Management -> Manage service applications.

Click on the Secure Store Service application and click New button on the ribbon to create a new target application.

Create a new secure storage target application with the following values:

- **Target Application ID**: `hpmfa`
- **Display Name**: `HarePoint Multi-Factor Authentication`
- **Contact E-mail**: `admin@yourcompany.com`
- **Target Application Type**: `Group`
- **Target Application Page URL**: `None`

Click Next button.
On the field list page, you need to remove *Windows Username* field (first) and change type of *Windows Password* field (second one) to Password:

![Image of field list page with modified fields](image)

Click *Next* Button.

On the membership settings page, you need to specify administrators who have access to manage this target application settings, as well as managed accounts who have access to read credentials stored in this target application:

![Image of membership settings page with administrators](image)
**Note:** each application pool account where you use HarePoint Multi-Factor Authentication must be listed as a member of the *hmpfa* Secure Store target application. In addition, the farm account must be a member of the *hmpfa* Secure Store target application.

Click OK button to create Secure Store target application:

Click on the dropdown menu of the newly created *hmpfa* target application and select Set Credentials:
You should create a strong password that will be used to encrypt user’s secrets in the User Profile service.

Click **OK** to complete the configuration of the *hpmfa* Secure Store target application.

Now you can enable encryption in HarePoint Multi-Factor Authentication General Settings:

**Note:** user secrets created before encryption is turned on will remain unencrypted and will work until the administrator or user himself reset a specific secret.
Appendix A. Manage MFA settings via PowerShell

You can use the following PowerShell script to enable multi-factor authentication for specific user:

```powershell
$SiteURL = "http://company.local/
$UserLogin="i:0#.f|fbamembershipprovider\sampleuser"

$ServiceContext = Get-SPServiceContext -site $SiteURL

$UserProfile = $UserProfileManager.GetUserProfile($UserLogin)

$userProfile["HPMFAForce"].Value = $true
$userProfile.Commit()
```