HarePoint Multi-Factor Authentication

For SharePoint Server 2010, 2013, 2016, 2019 and Subscription Edition.

Product version 1.3

March 31, 2022

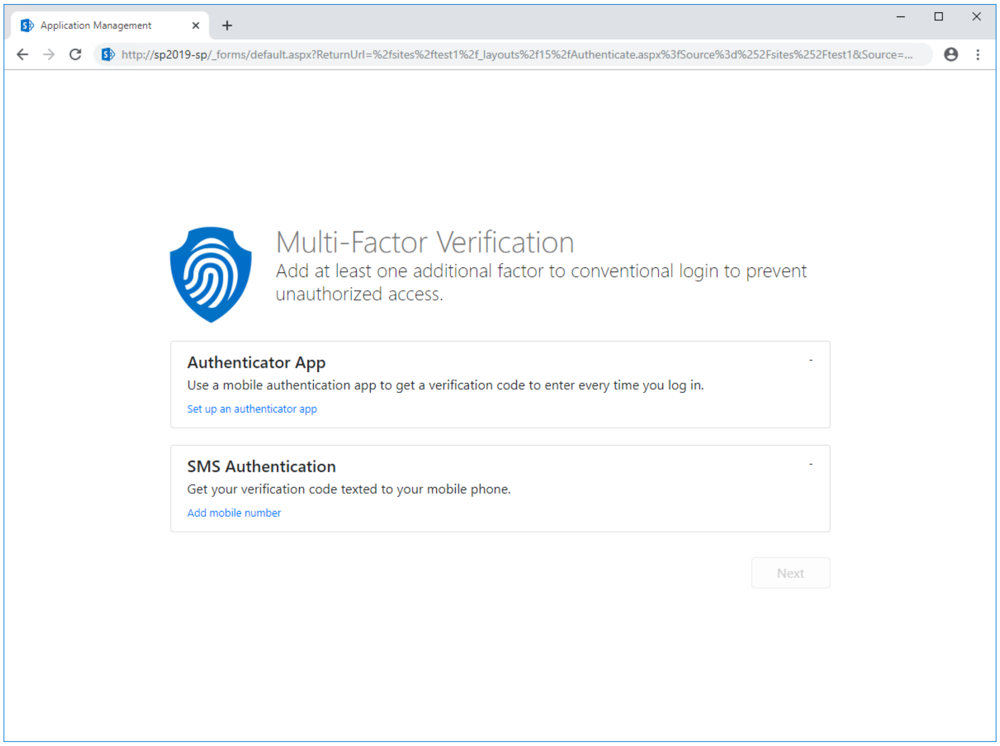
Table of Contents

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.


Application Management
http://sp2019-sp/_forms/default.aspx?ReturnUrl=%2fsites%2ftest1%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252Fsites%252Ftest1&Source=...

Multi-Factor Verification

Add at least one additional factor to conventional login to prevent unauthorized access.

Authenticator App

Use a mobile authentication app to get a verification code to enter every time you log in.

Set up an authenticator app

SMS Authentication

Get your verification code texted to your mobile phone.

Add mobile number

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).

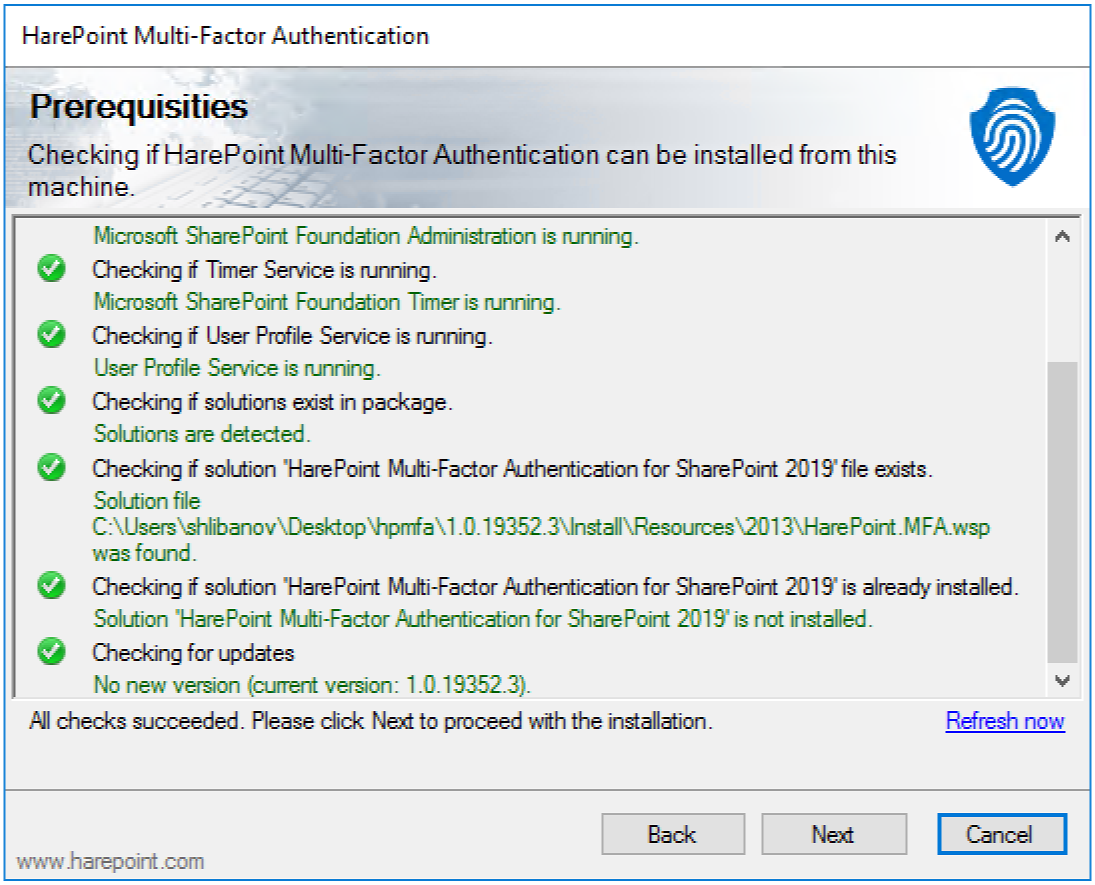
There is no functional difference between the trial and the registered version except that:

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:



HarePoint Multi-Factor Authentication

Prerequisities

Checking if HarePoint Multi-Factor Authentication can be installed from this machine.

Microsoft SharePoint Foundation Administration is running.

✓ Checking if Timer Service is running.

Microsoft SharePoint Foundation Timer is running.

✓ Checking if User Profile Service is running.

User Profile Service is running.

✓ Checking if solutions exist in package.

Solutions are detected.

✓ Checking if solution 'HarePoint Multi-Factor Authentication for SharePoint 2019' file exists.

Solution file C:\Users\shlibanov\Desktop\hpmfa\1.0.19352.3\Install\Resources\2013\HarePoint.MFA.wsp was found.

✓ Checking if solution 'HarePoint Multi-Factor Authentication for SharePoint 2019' is already installed.

Solution 'HarePoint Multi-Factor Authentication for SharePoint 2019' is not installed.

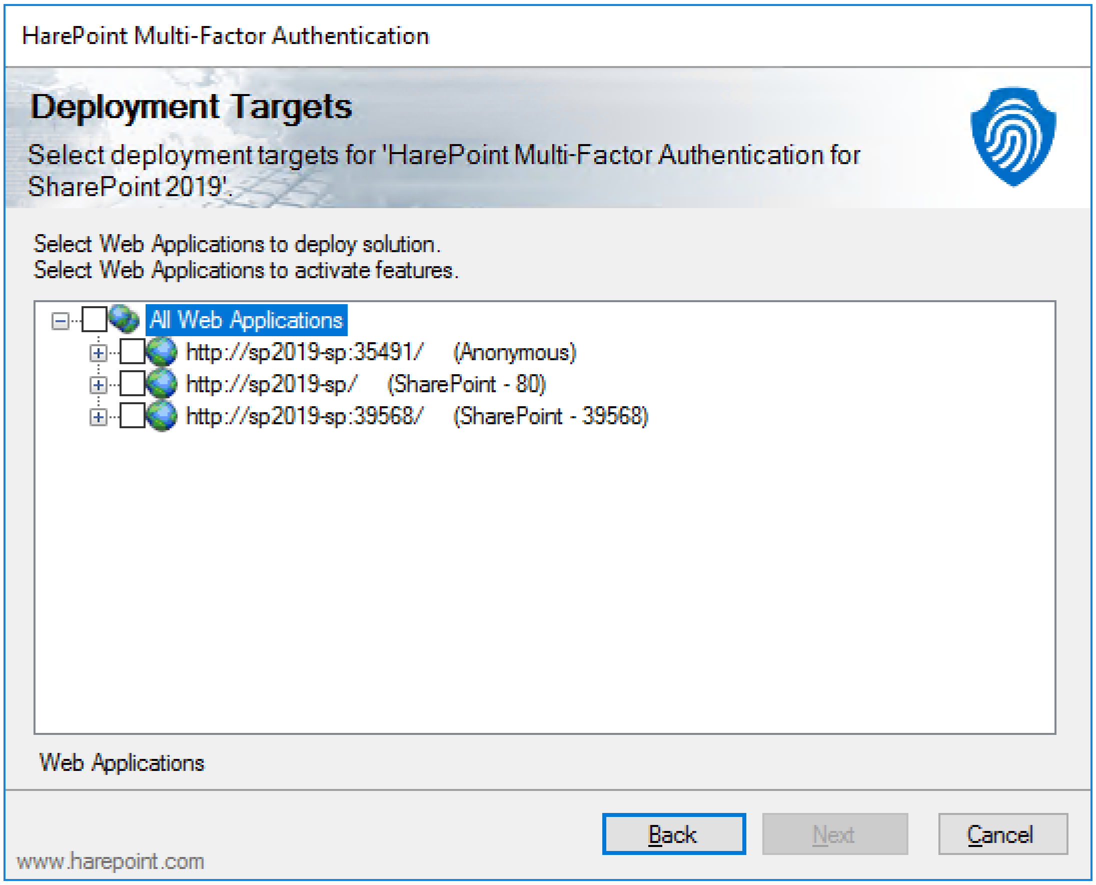
✓ Checking for updates

No new version (current version: 1.0.19352.3).

All checks succeeded. Please click Next to proceed with the installation.

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:



HarePoint Multi-Factor Authentication

Deployment Targets

Select deployment targets for 'HarePoint Multi-Factor Authentication for SharePoint 2019'.

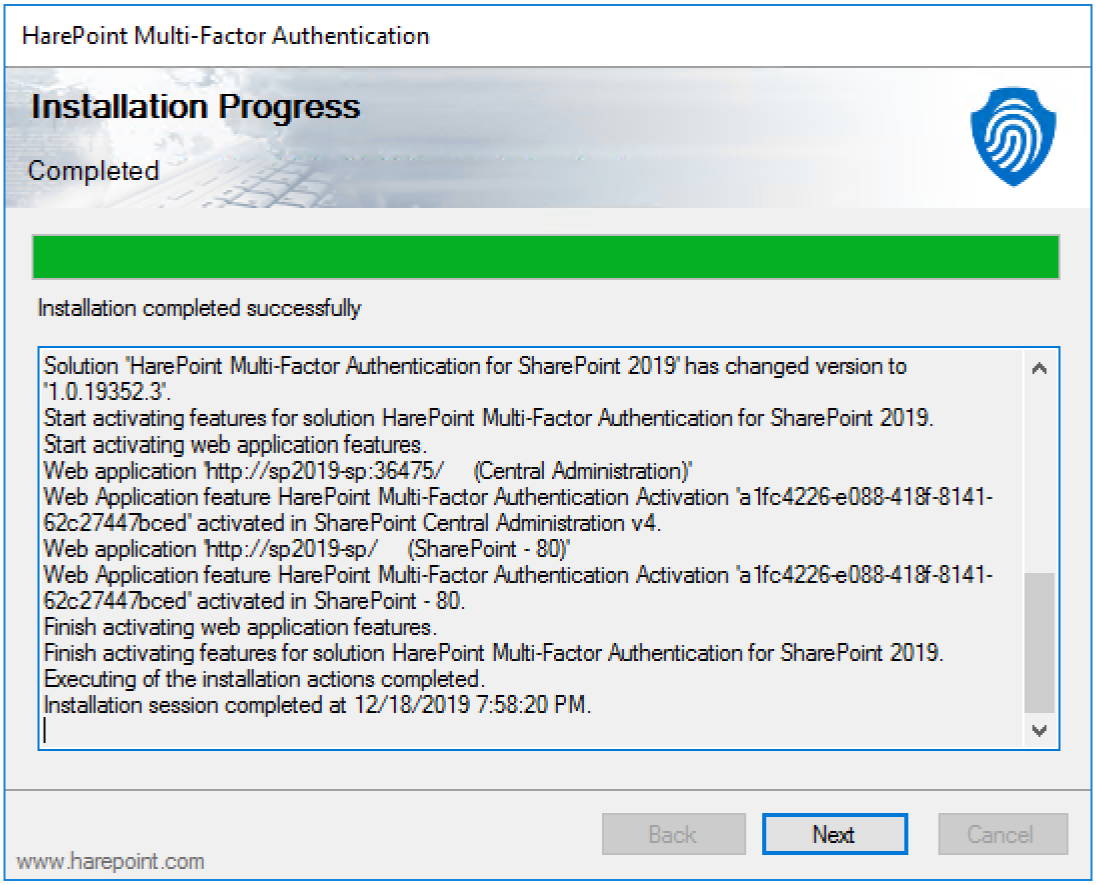
Select Web Applications to deploy solution.
Select Web Applications to activate features.

- □ All Web Applications
  - □ http://sp2019-sp:35491/ (Anonymous)
  - □ http://sp2019-sp/ (SharePoint - 80)
  - □ http://sp2019-sp:39568/ (SharePoint - 39568)

Web Applications

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 completed successfully

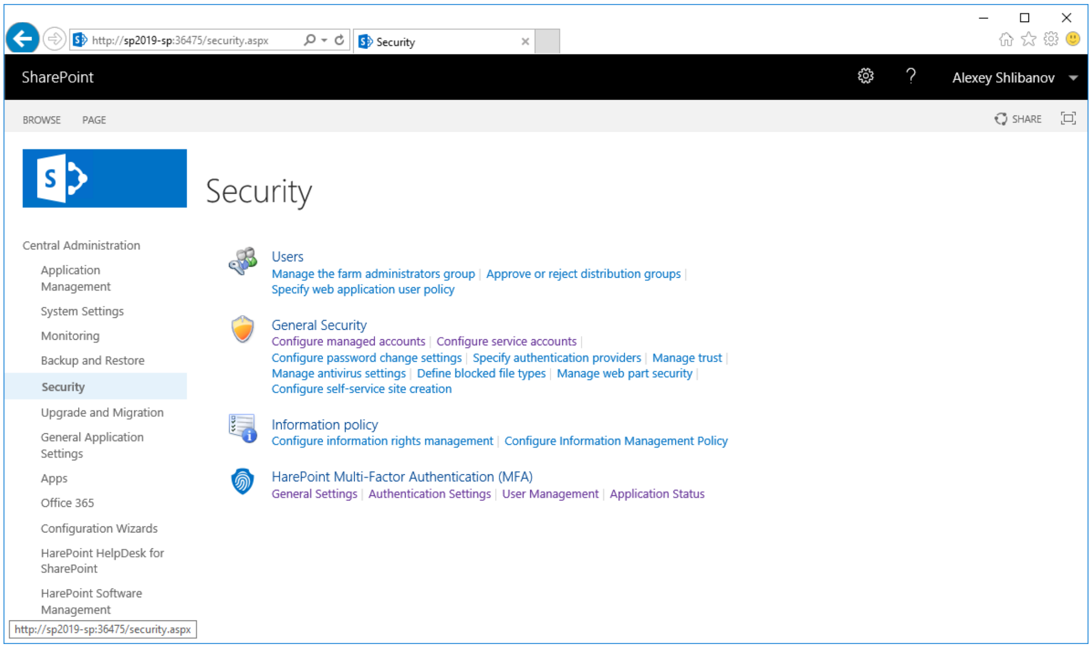
```
Solution 'HarePoint Multi-Factor Authentication for SharePoint 2019' has changed version to
'1.0.19352.3'.
Start activating features for solution HarePoint Multi-Factor Authentication for SharePoint 2019.
Start activating web application features.
Web application 'http://sp2019-sp:36475/     (Central Administration)'
Web Application feature HarePoint Multi-Factor Authentication Activation 'a1fc4226-e088-418f-8141-
62c27447bced' activated in SharePoint Central Administration v4.
Web application 'http://sp2019-sp/     (SharePoint - 80)'
Web Application feature HarePoint Multi-Factor Authentication Activation 'a1fc4226-e088-418f-8141-
62c27447bced' activated in SharePoint - 80.
Finish activating web application features.
Finish activating features for solution HarePoint Multi-Factor Authentication for SharePoint 2019.
Executing of the installation actions completed.
Installation session completed at 12/18/2019 7:58:20 PM.
```

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.



Security

Users
Manage the farm administrators group | Approve or reject distribution groups | Specify web application user policy

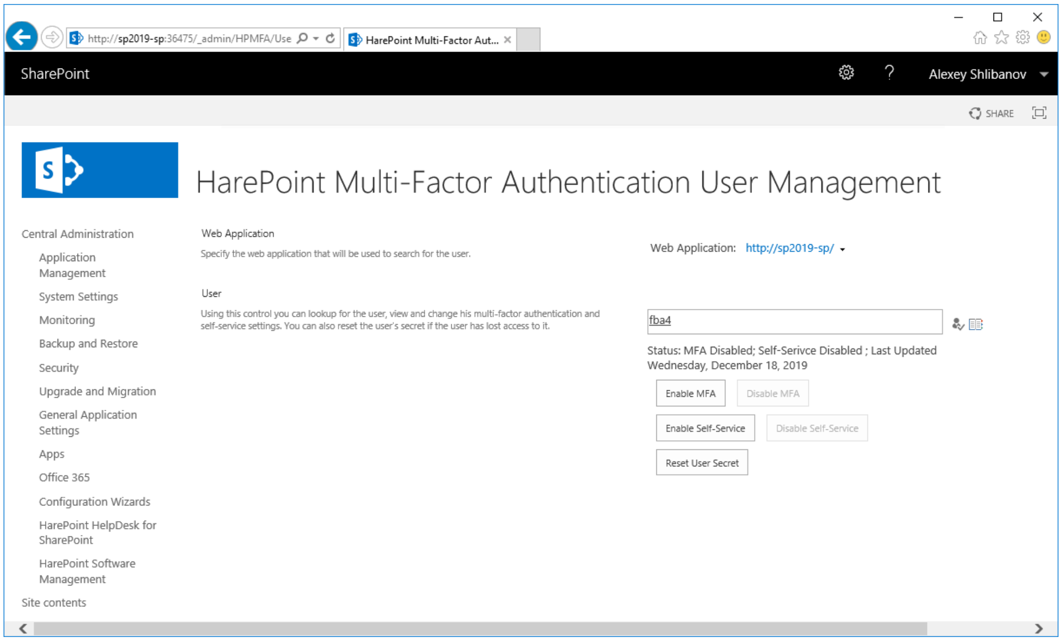
General Security
Configure managed accounts | Configure service accounts | Configure password change settings | Specify authentication providers | Manage trust | Manage antivirus settings | Define blocked file types | Manage web part security | Configure self-service site creation

Information policy
Configure information rights management | Configure Information Management Policy

HarePoint Multi-Factor Authentication (MFA)
General Settings | Authentication Settings | User Management | Application Status

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:



HarePoint Multi-Factor Authentication User Management

Web Application

Specify the web application that will be used to search for the user.

Web Application: http://sp2019-sp/

User

Using this control you can lookup for the user, view and change his multi-factor authentication and self-service settings. You can also reset the user's secret if the user has lost access to it.

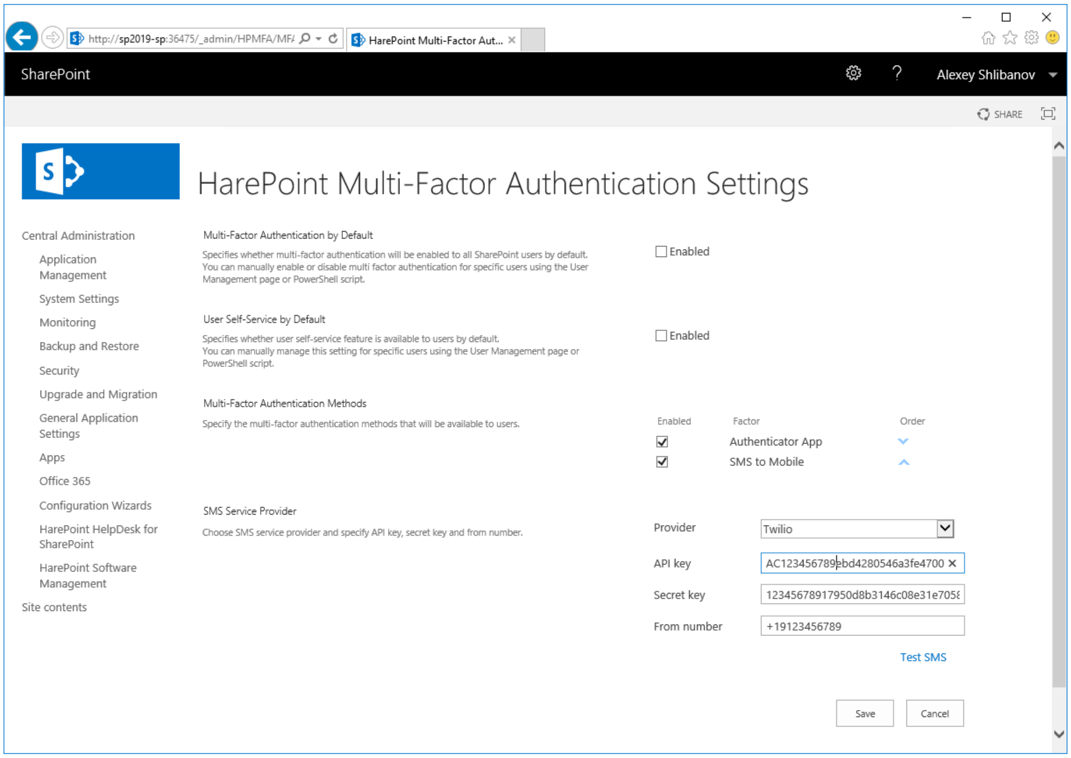
fba4

Status: MFA Disabled; Self-Serivce Disabled ; Last Updated Wednesday, December 18, 2019

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:



HarePoint Multi-Factor Authentication Settings

Multi-Factor Authentication by Default

Specifies whether multi-factor authentication will be enabled to all SharePoint users by default. You can manually enable or disable multi factor authentication for specific users using the User Management page or PowerShell script.

□ Enabled

User Self-Service by Default

Specifies whether user self-service feature is available to users by default. You can manually manage this setting for specific users using the User Management page or PowerShell script.

□ Enabled

Multi-Factor Authentication Methods

Specify the multi-factor authentication methods that will be available to users.

Enabled	Factor	Order
☑	Authenticator App	⌄
☑	SMS to Mobile	⌃

SMS Service Provider

Choose SMS service provider and specify API key, secret key and from number.

Provider	Twilio
API key	AC123456789ebd4280546a3fe4700
Secret key	12345678917950d8b3146c08e31e705
From number	+19123456789

The list of supported SMS service providers:

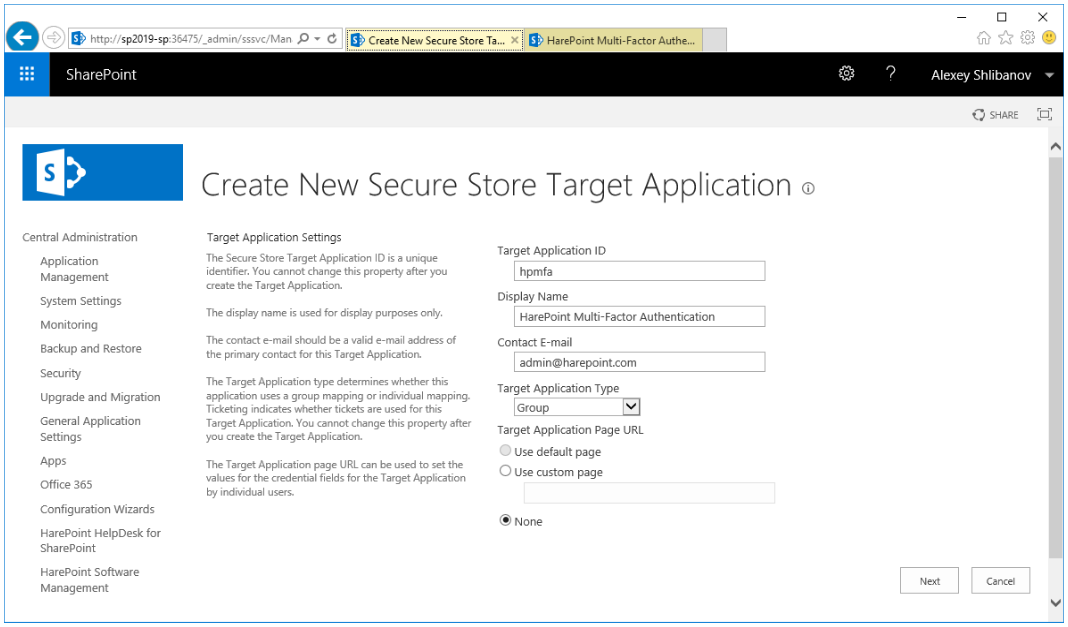
- Twilio (https://www.twilio.com/)
- Sinch (https://www.sinch.com/)
- Nexmo (https://www.nexmo.com/)
- aql (https://www.aql.com/)
- SMSGlobal (https://www.smsglobal.com/)
- SMSMKT (https://smsmkt.com/en/)

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/

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 New Secure Store Target Application

Target Application Settings

The Secure Store Target Application ID is a unique identifier. You cannot change this property after you create the Target Application.

The display name is used for display purposes only.

The contact e-mail should be a valid e-mail address of the primary contact for this Target Application.

The Target Application type determines whether this application uses a group mapping or individual mapping. Ticketing indicates whether tickets are used for this Target Application. You cannot change this property after you create the Target Application.

The Target Application page URL can be used to set the values for the credential fields for the Target Application by individual users.

Target Application ID: hpmfa

Display Name: HarePoint Multi-Factor Authentication

Contact E-mail: admin@harepoint.com

Target Application Type: Group

Target Application Page URL

○ Use default page

○ Use custom page

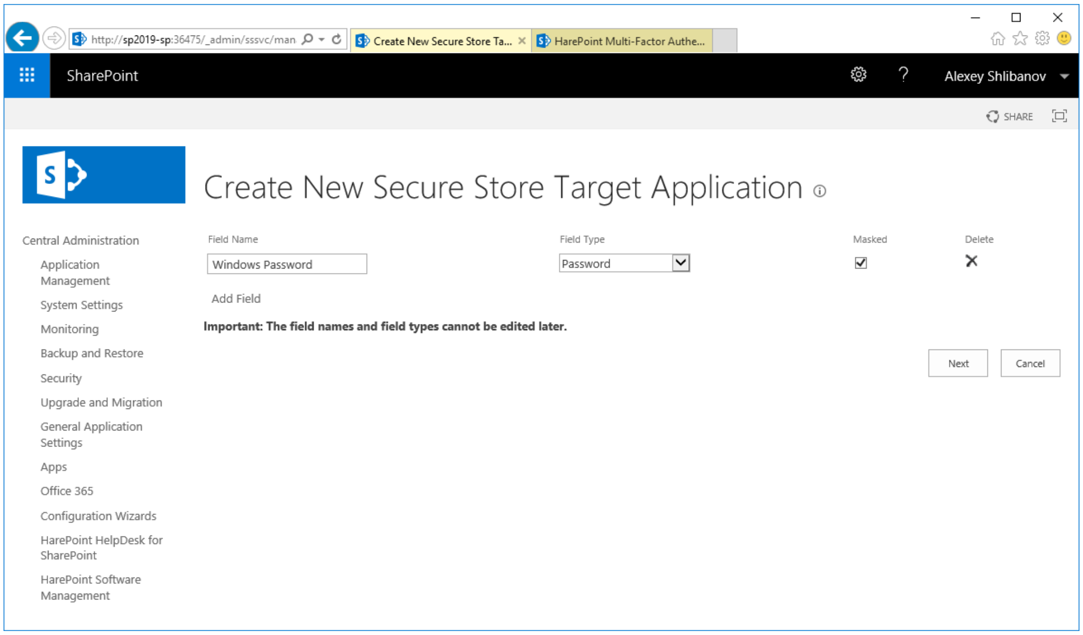
● None

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:



Create New Secure Store Target Application

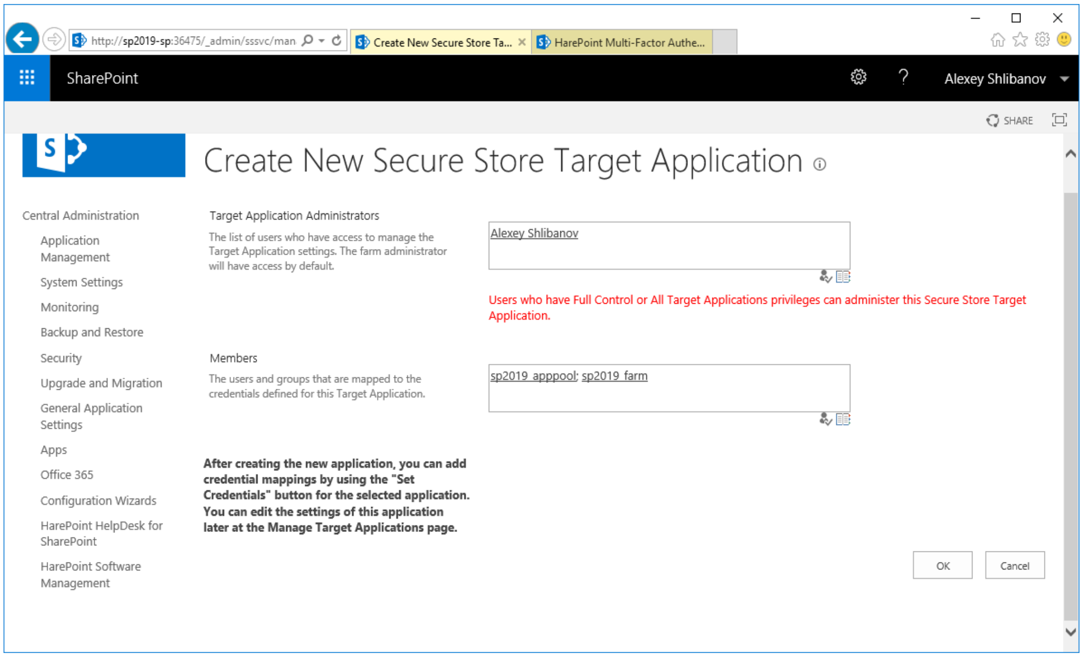
Field Name	Field Type	Masked	Delete
Windows Password	Password	☑	✕

Add Field

Important: The field names and field types cannot be edited later.

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:



Create New Secure Store Target Application

Target Application Administrators

The list of users who have access to manage the Target Application settings. The farm administrator will have access by default.

Alexey Shlibanov

Users who have Full Control or All Target Applications privileges can administer this Secure Store Target Application.

Members

The users and groups that are mapped to the credentials defined for this Target Application.

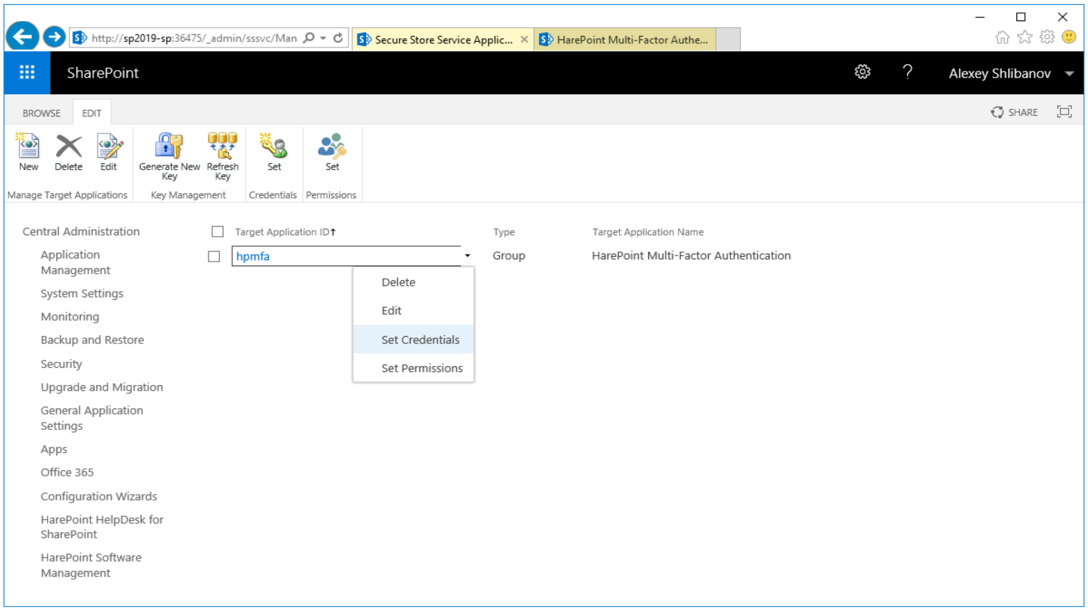
sp2019_apppool; sp2019_farm

After creating the new application, you can add credential mappings by using the "Set Credentials" button for the selected application. You can edit the settings of this application later at the Manage Target Applications page.

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.

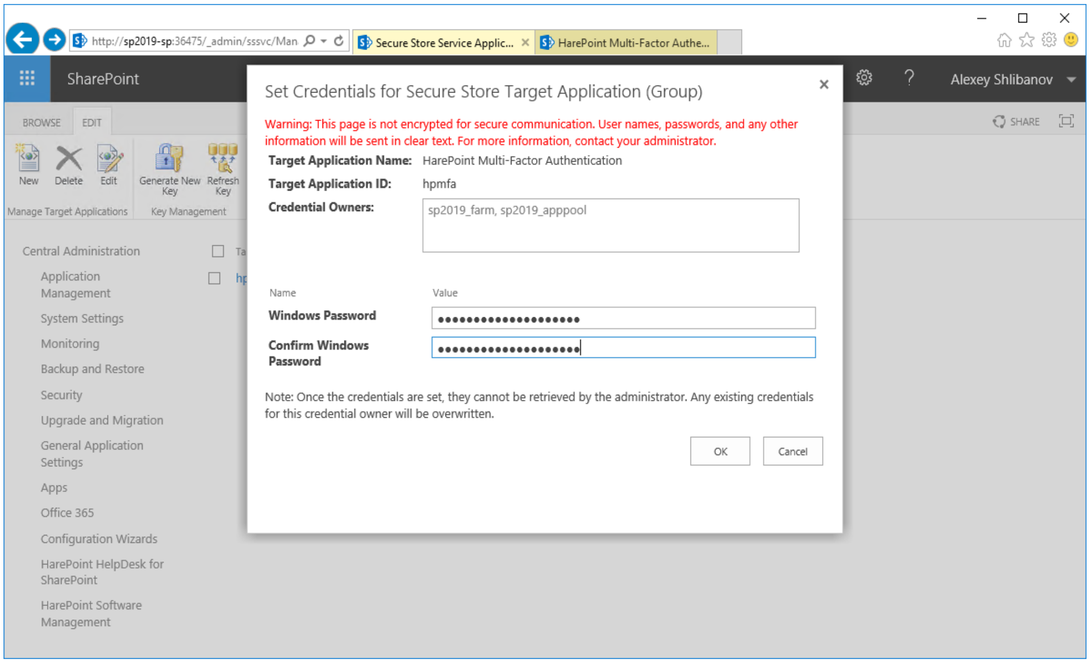
Click *OK* button to create Secure Store target application:

Click on the dropdown menu of the newly created *hpmfa* target application and select Set Credentials:



□	Target Application ID↑	Type	Target Application Name
□	hpmfa	Group	HarePoint Multi-Factor Authentication

You should create a strong password that will be used to encrypt user's secrets in the User Profile service.



Set Credentials for Secure Store Target Application (Group)

Warning: This page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

Target Application Name: HarePoint Multi-Factor Authentication

Target Application ID: hpmfa

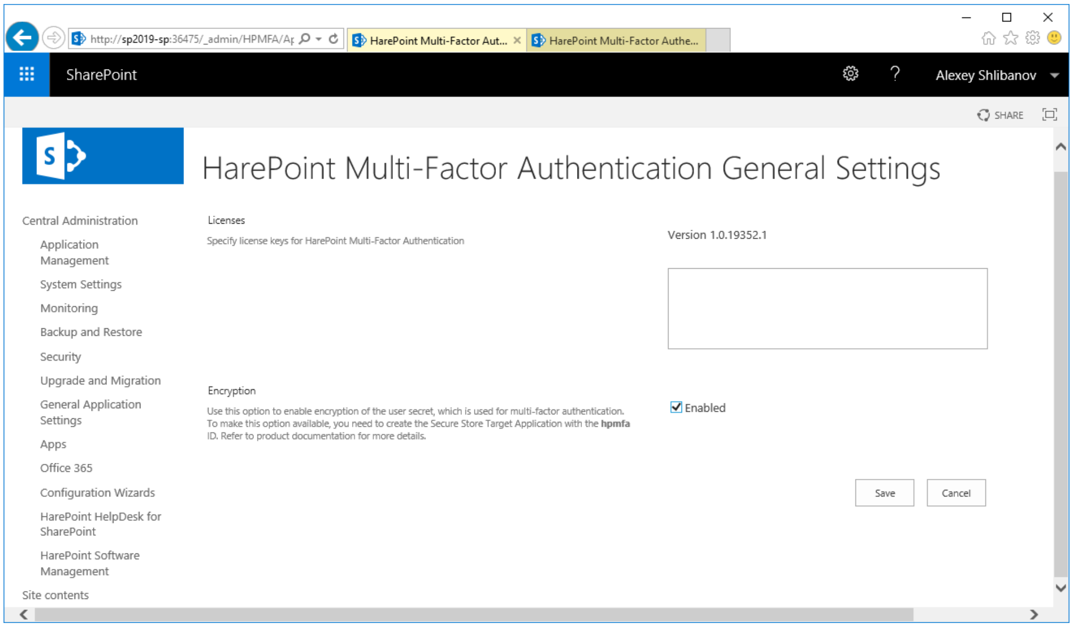
Credential Owners: sp2019_farm, sp2019_apppool

Name	Value
Windows Password	••••••••••••••••••••
Confirm Windows Password	••••••••••••••••••••

Note: Once the credentials are set, they cannot be retrieved by the administrator. Any existing credentials for this credential owner will be overwritten.

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:



HarePoint Multi-Factor Authentication General Settings

Licenses

Specify license keys for HarePoint Multi-Factor Authentication

Version 1.0.19352.1

Encryption

Use this option to enable encryption of the user secret, which is used for multi-factor authentication. To make this option available, you need to create the Secure Store Target Application with the **hpmfa** ID. Refer to product documentation for more details.

☑ Enabled

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:

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

$ServiceContext  = Get-SPServiceContext -site $SiteURL
$UserProfileManager = New-Object Microsoft.Office.Server.UserProfiles.UserProfileManager($ServiceContext)

$UserProfile = $UserProfileManager.GetUserProfile($UserLogin)

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