SafeNet Authentication Service

Integration Guide

Using SAS as an Identity Provider for Office 365

THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012543-001, Rev. B
Release Date	June 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Office 365.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Office 365 is the brand name used by Microsoft for a group of software plus services subscriptions that provides productivity software and related services to its subscribers.

For consumers, the service allows the use of Microsoft Office apps on Windows and OS X, provides storage space on Microsoft's cloud storage service OneDrive, and grants 60 Skype minutes per month.

For business and enterprise users, Office 365 offers plans including e-mail and social networking services through hosted versions of Exchange Server, Lync, SharePoint and Office Online, integration with Yammer, as well as access to the Office software.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Office 365 using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in Office 365 using SafeNet Authentication Service as an identity provider.

It is assumed that the Office 365 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Office 365 can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** — SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** — A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — A server version that is used to deploy the solution on-premises in the organization.

Environment

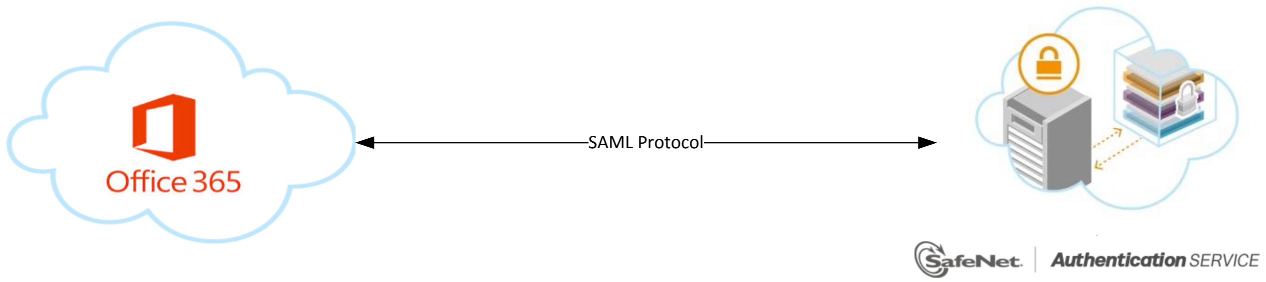
The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service –** 3.3
- **Office 365** - web account
- **AD FS 2012 R2**

This document is targeted to system administrators who are familiar with Office 365 and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SAS Cloud

SAS Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.



SAML Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

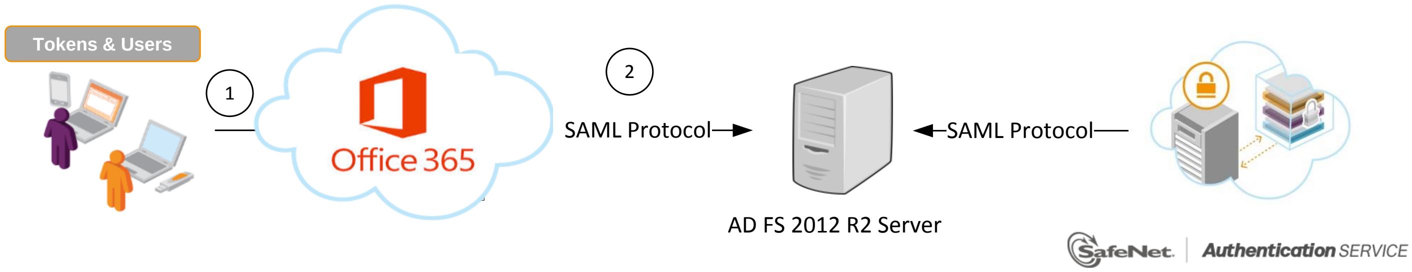
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.

SAML Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of Service Providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Office 365.



1. A user attempts to log on to Office 365. The user is redirected to AD FS 2012 R2 for AD authetnication.
2. After successful authentication the user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user's credentials.
3. SAS returns a response to Office 365, accepting or rejecting the user`s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service to receive SAML authentication requests from Office 365, ensure that the end users can authenticate through from the Office 365 environment with a static password.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Office 365 using SAML authentication requires:

- Synchronizing User Stores to SAS
- Authenticators assignment in SAS
- Adding Office 365 as a Service Provider (SP) in SAS
- Configure SAML Services in SAS

Synchronizing Users Stores to SafeNet Authentication Service

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to creating users in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through Office 365.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manually provision** – Assign an authenticator to users one by one.

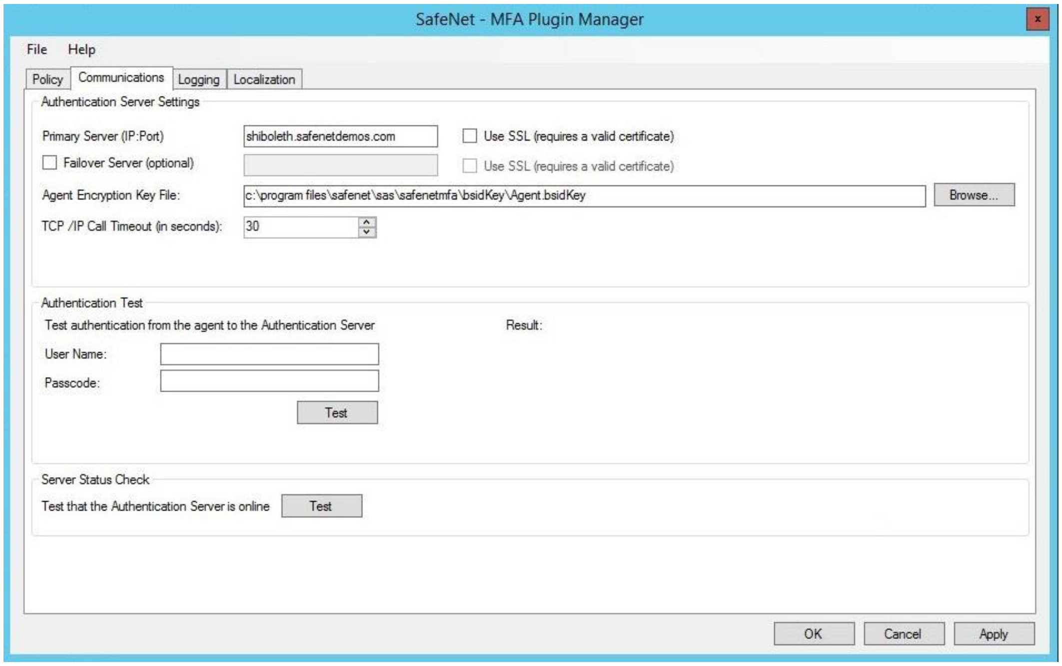
- **Provisioning rules** – The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change; an authenticator will be assigned automatically to the user.

Refer to “provisioning rules” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service User Store.

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Configuring the MFA Agent

1. Run the MFA agent.
2. On the **Policy** tab, verify that the **Enable/Disable Agent** and **Pre Generate Challenge** check boxes are selected.
3. On the **Communications** tab, in the **Primary Server (IP:Port)** box, type the SAS server IP address or name (and port if non-causal is used).
4. In case your SAS server is not installed on same machine as the AD and AD FS, key encryption file needs to be loaded (was downloaded as explained in page 5).



5. Click **Apply**. Enabling the agent registers the SafeNet MFA (multi-factor authentication) adapter with AD FS and enables it at a global policy level.
6. You can verify your settings by testing authentication from the agent to the authentication server. To do so, under **Authentication Test**, enter your user name and passcode, and then click the **Test** button. The result of the test will be displayed on the right side of the box.
7. Click **OK** when finished.

Configuring Office 365

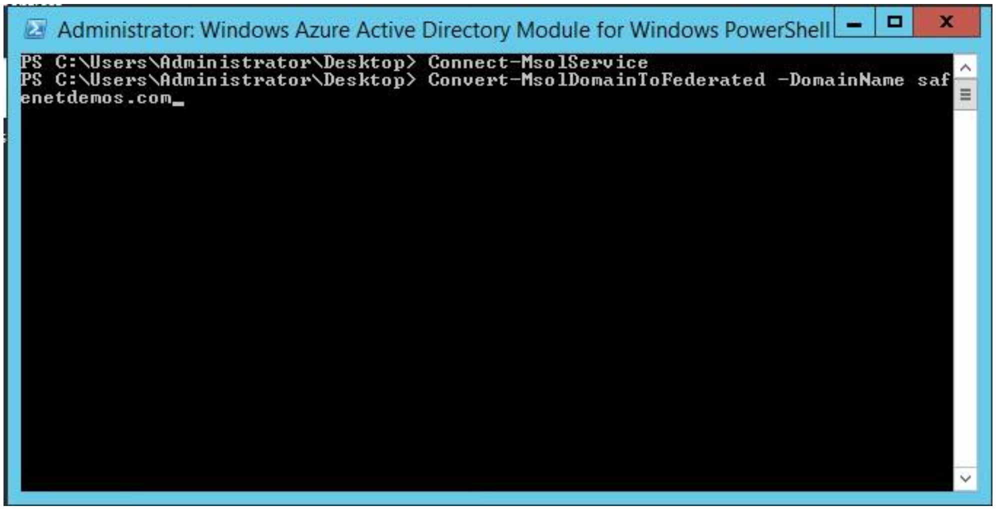
To add SafeNet Authentication Service as an Identity Provider in Office 365:

Enabling Office 365 Federated Domains

The SAS Administrator Console settings are used to establish SafeNet Authentication Service (SAS) as the identity provider for Office 365.

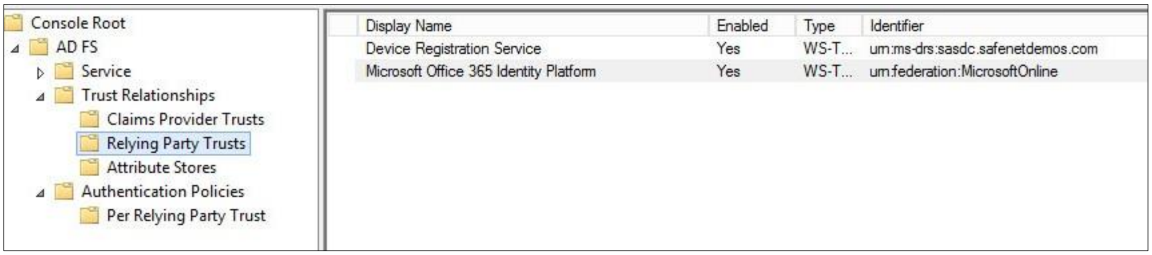
1. Log in to the AD FS server machine as Domain Admin.
2. Open **Windows Azure AD Module for Windows PowerShell**.
3. At the command prompt, type **Connect-MsolService**, and then press **Enter**.
4. On the **Enter Credentials** dialog box, type your Office 365 user name and password, and then click **OK**.

5. At the command prompt, type **Convert-MsolDomainToFederated –DomainName <*your domain name*>**, and then press **Enter**.



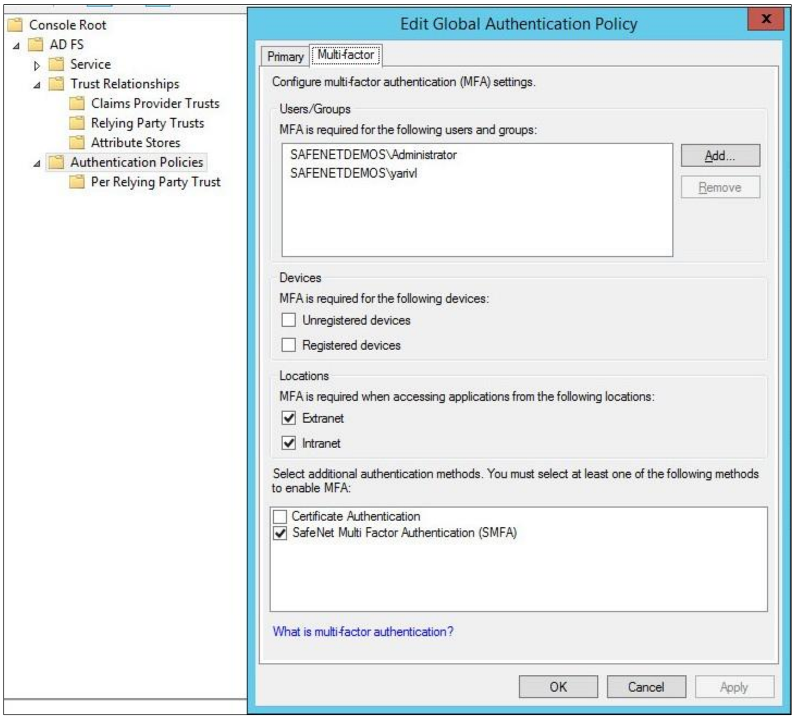
6. Open the **AD FS Management Console**.

7. In the left pane, under Console Root, click **AD FS > Trust Relationships > Relying Party Trusts**. In the right pane, Microsoft **Office 365 Identity Platform** should be listed as a trust.



Configuring the AD FS Authentication Policy

1. In the AD FS Management Console, in the left pane, under **AD FS**, right-click **Authentication Policies** and select **Edit Global Primary Authentication**.
2. On the **Primary** tab, verify that **Form Authentication** is selected for both **Extranet** and **Intranet**.
3. Click the **Multi-factor** tab, and then perform the following steps:
    a. Under **Users/Groups**, add the users and/or groups for which MFA will be required.
    b. Choose **Extranet** and/or **Intranet**, according to your preferred configuration.
    c. Verify that **SafeNet Multi Factor Authentication (SMFA)** is selected as an additional authentication method.
    d. Click **OK**.



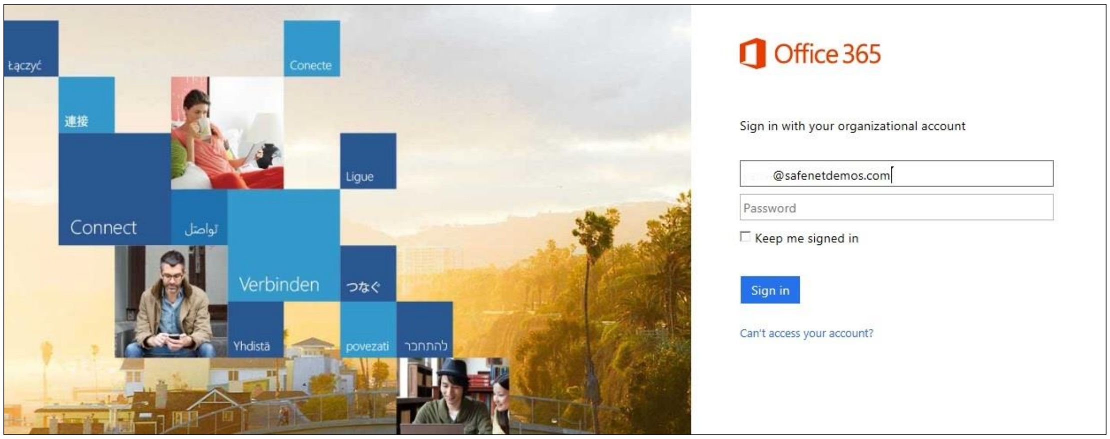
Running the Solution

After Office 365 is configured to use SafeNet Authentication Service as its identity provider, and SafeNet Authentication Service is configured to use Office 365 as a SAML service provider, users can log in to Office 365.

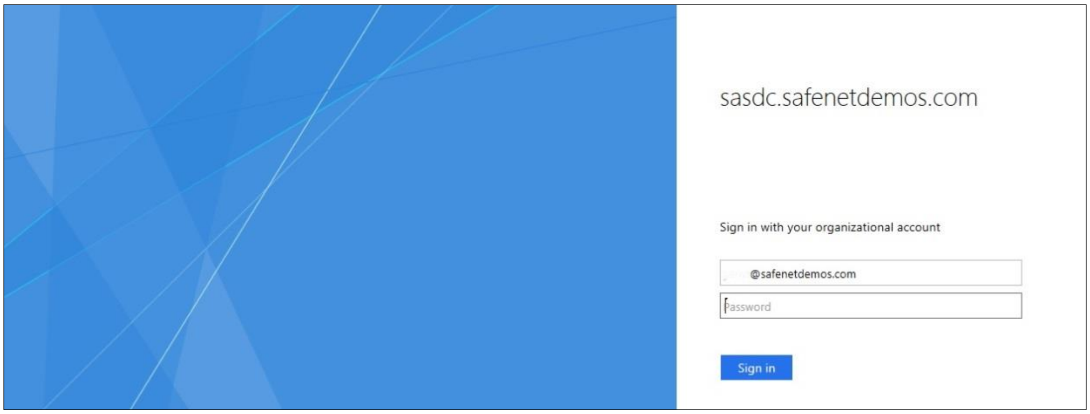
Connecting to Office 365

1. Open a browser and go to https://login.microsoftonline.com.

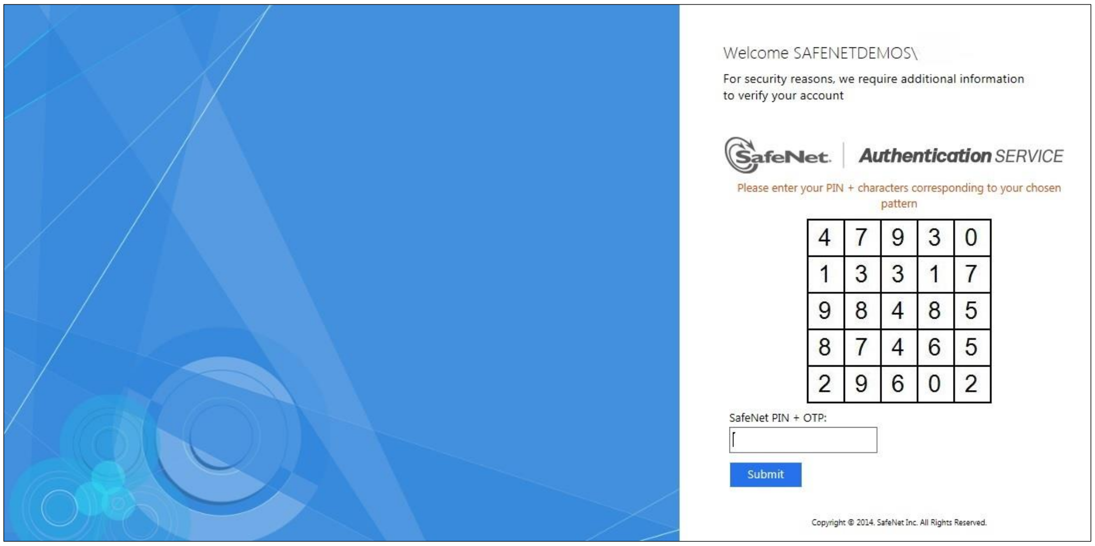
1. At the login prompt, type your user name (including domain; for example, **Bob@SafeNetdemos.com**) and password, and then click **Sign In**.



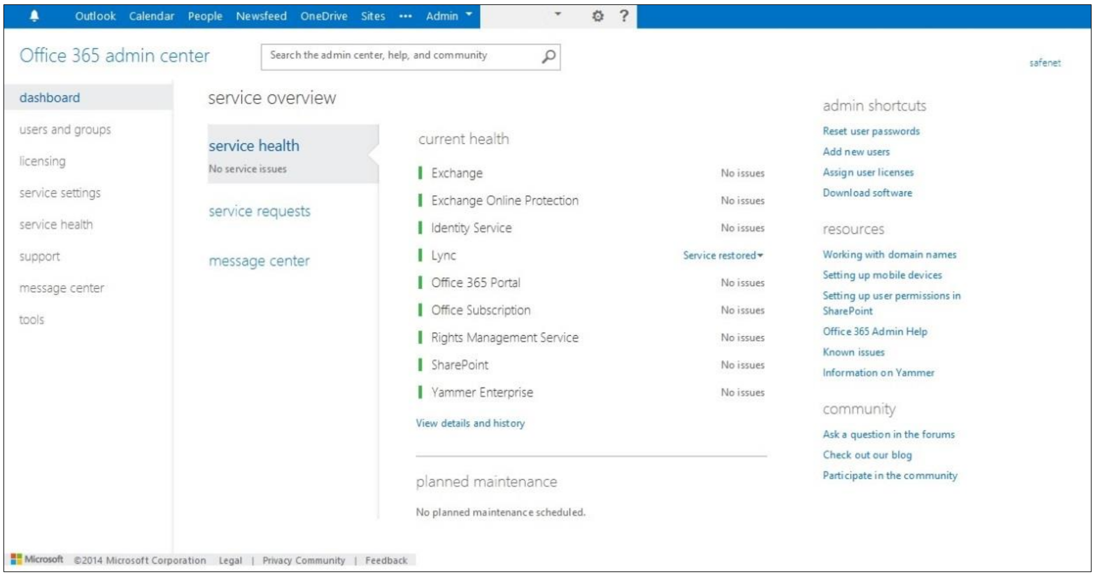
2. You will be redirected to your organization's login page. Type your organizational user name and password, and then click **Sign In**.



3. After successful login, the SafeNet Authentication login page is displayed. Enter your SafeNet Authentication Service credentials (PIN+OTP), and then click **Submit**.

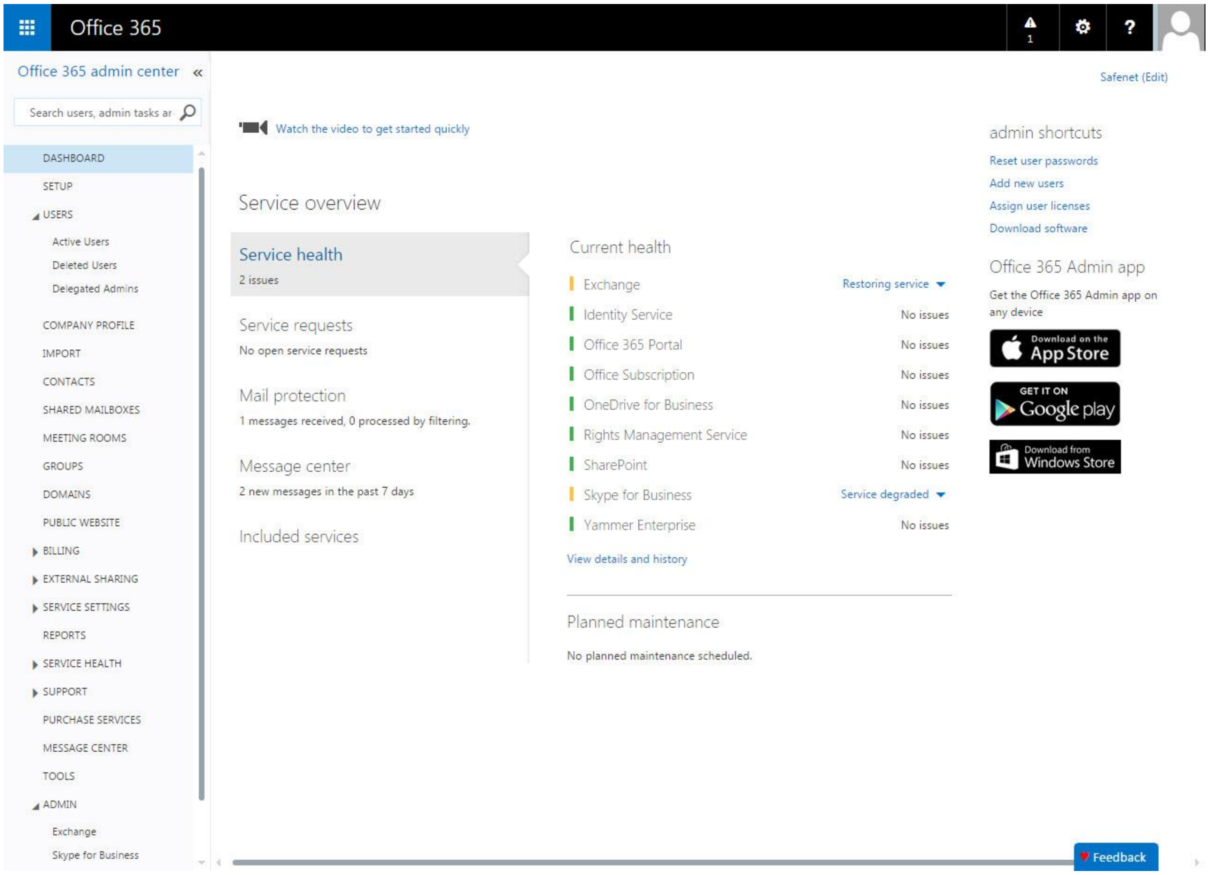


4. After successful authentication, the **Office 365 admin center** page is displayed.

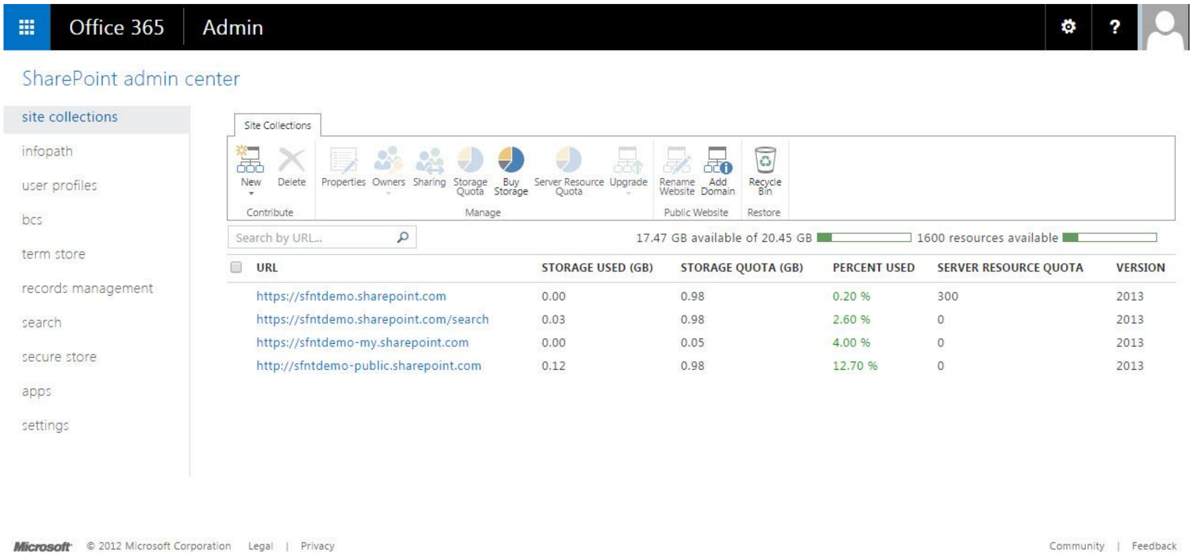


Connecting to Office 365's SharePoint

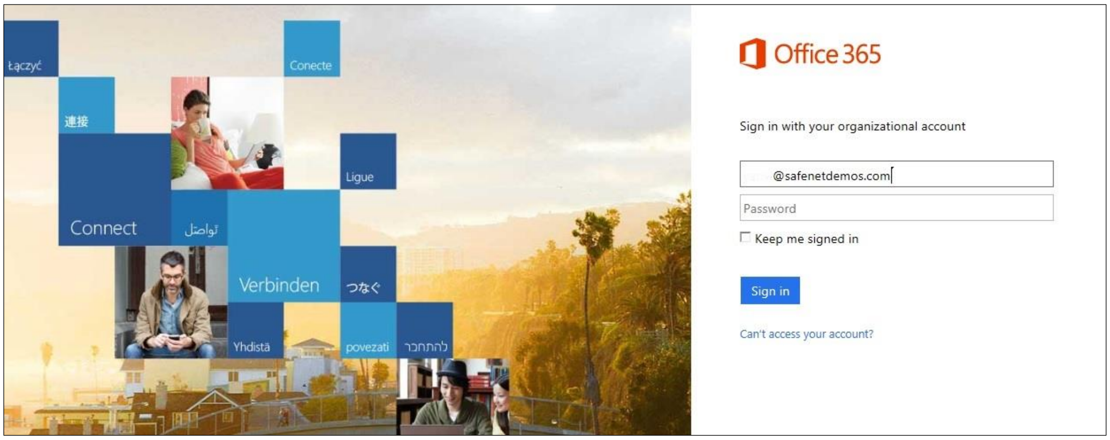
1. In order to get your Office365 SharePoint URL you first need to login to Office365 console as Administrator.



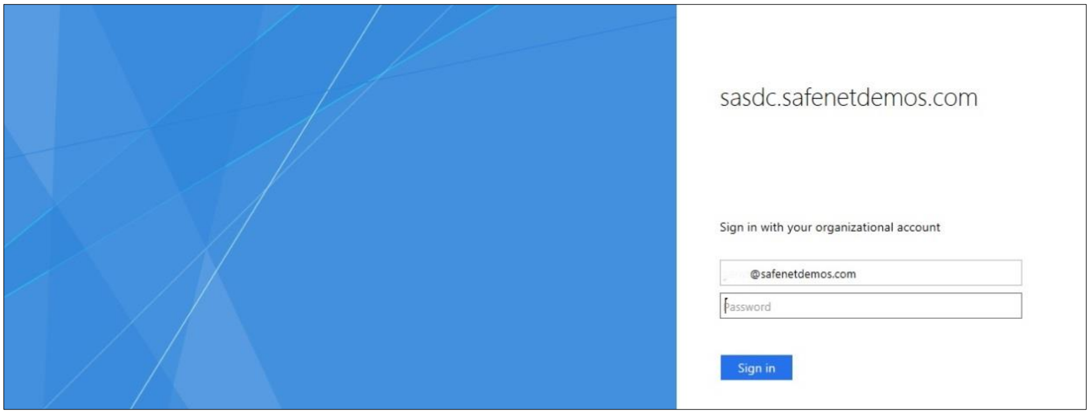
2. Press on **Admin** -> **ShaerPoint** to enter the SharePoint admin center.
3. Here you will find your SharePoint's URLs.



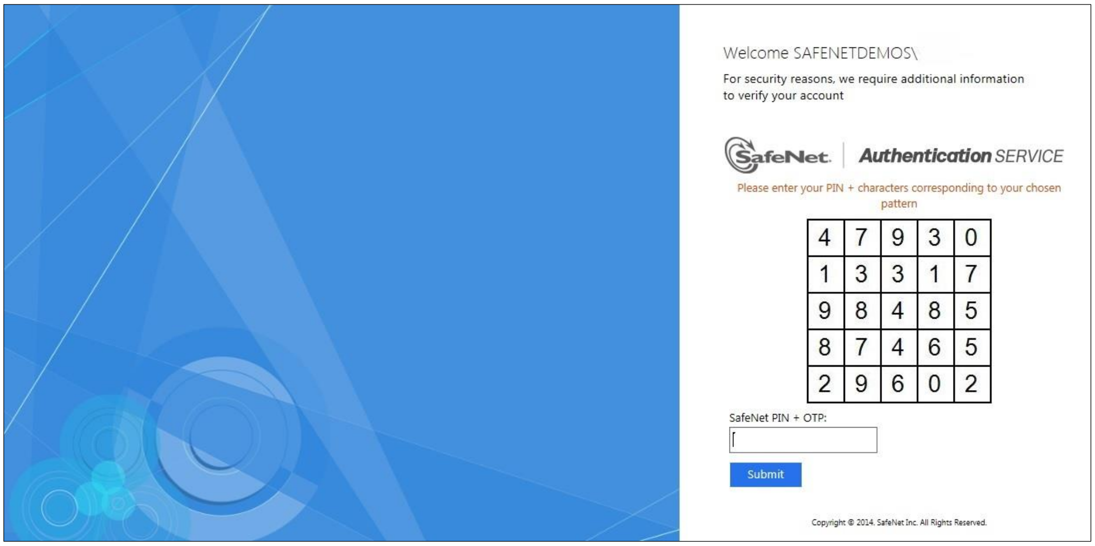
4. Using one of this Office 365 SharePoint's URLs, open a new browser and try to login.
5. At the login prompt, type your user name (including domain; for example, **Bob@SafeNetdemos.com**) and password, and then click **Sign In**.



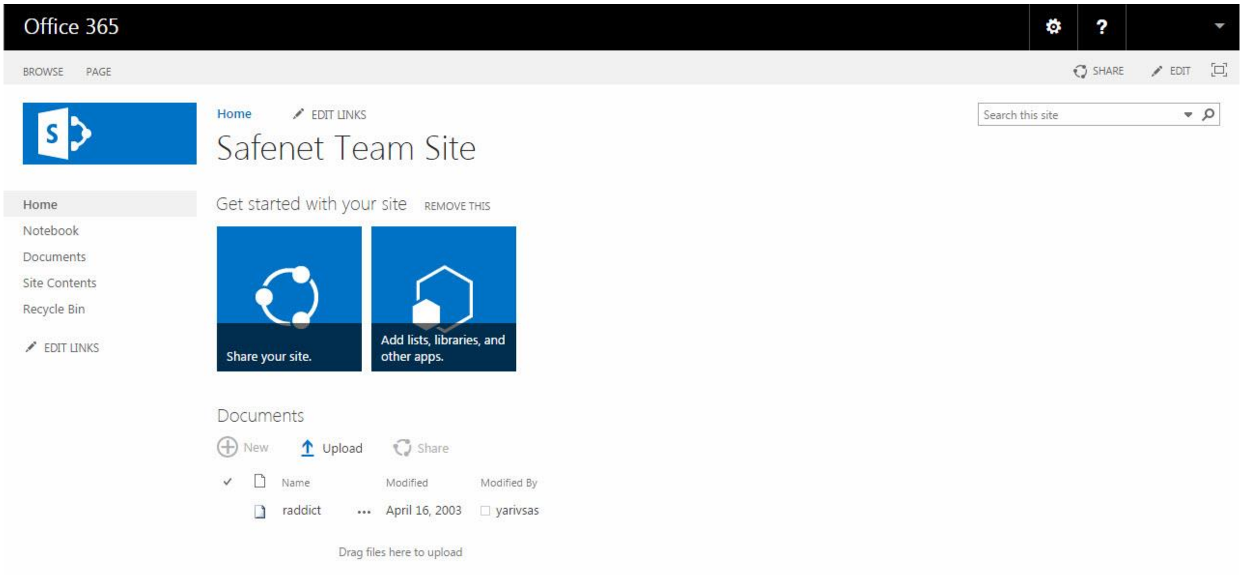
6. You will be redirected to your organization's login page. Type your organizational user name and password, and then click **Sign In**.



7. After successful login, the SafeNet Authentication login page is displayed. Enter your SafeNet Authentication Service credentials (PIN+OTP), and then click **Submit**.



8. After successful authentication, the **Office 365 SharePoint** page is displayed.



Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<tr><th>Contact Method</th><th colspan="2">Contact Information</th></tr>
<tr><td>Address</td><td colspan="2">SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017 USA</td></tr>
<tr><td rowspan="2">Phone</td><td>United States</td><td>1-800-545-6608</td></tr>
<tr><td>International</td><td>1-410-931-7520</td></tr>
<tr><td>Technical Support Customer Portal</td><td colspan="2">https://serviceportal.safenet-inc.com
Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td></tr>
</table>