Microsoft Office 365
with ADFS
Implementation Guide
(Version 5.4)
Trademarks
Deepnet Unified Authentication, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights
Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions
Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer
This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact
If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Northway House
1379 High Road
London N20 9LP
United Kingdom

Tel:   +44(0)20 8343 9663
Fax:  +44(0)20 8446 3182
Web:  www.deepnetsecurity.com
Email: support@deepnetsecurity.com
Table of Contents

Overview ......................................................................................................................... 4
Prerequisites .................................................................................................................... 4
Installation of DualShield IIS Agent .............................................................................. 6
Configure IIS on ADFS ................................................................................................. 7
  Enable Form-Based Authentication ......................................................................... 7
  Enable DualShield Authentication ...................................................................... 8
  Enable Reverse Proxy ....................................................................................... 10
Test Logon .................................................................................................................. 11
Overview

This document describes how to implement multifactor authentication for Microsoft Office 365 configured for SSO to a local ADFS 2.0 service with the DualShield SSO service provided by the DualShield Unified Authentication Platform.

Microsoft Office 365 is a cloud based service that can be configured to use a local Active Directory Federation Service (ADFS) to enable local users to sign on with their existing AD credential to gain access to various Microsoft online services such as Office, Outlook, SharePoint and Lync.

Prerequisites

It is expected that Office365 has already been setup for SSO to an on-premises ADFS server with working SSO based on users AD passwords.

You must have the DualShield Authentication Server and DualShield SSO Server installed and operating (both are installed by default in the installation of the platform). For the installation, configuration and administration of DualShield Authentication and SSO servers please refer to the following documents:

- DualShield Authentication Platform – Installation Guide
- DualShield Authentication Platform – Quick Start Guide
- DualShield Authentication Platform – Administration Guide

You should also have created an application in DualShield for your Office 365 service, and published the application on the DualShield SSO server.
For Office 36 service, the logon procedure would typically contain 2 steps with the AD Static Password and a second-factor token:
Use the Self-Test function to verify that the application is ready:

![Self-Test](image1)

**Installation of DualShield IIS Agent**

To implement two-factor authentication for Office 365, you will need to install the DualShield IIS Agent on the ADFS server. For the general instruction of the installation and configuration of the DualShield IIS Agent, please refer to the following document:

- IIS 7.0 - Implementation Guide
Configure IIS on ADFS

The first step is to configure the IIS on ADFS to work on Form Based authentication.

Enable Form-Based Authentication

1. Open IIS and Windows Explore under Default Website\adfs\ls

2. Open the web.config file with Notepad, look for the localAuthenticationTypes section.

3. Move the line for Forms above the line for Integrated and save the web.config file. This will force the ADFS application to use the Form Based authentication before trying to use Windows Authentication.
4. Restart the IIS server and test your Office 365 logon to ensure that Form-based authentication is functional. Below is the screen shot of the default logon page when ADFS works in form-based authentication:

Enable DualShield Authentication
The next step is to enable DualShield two-factor authentication

1. In the IIS Manager, select “Default Web Site | adfs | ls”
2. Double click the “DualShield Authentication” icon

Enable “Enable Two-Factor Authentication on the Current Node”

Enable “Apply Settings to Child Nodes”

Select “Service Type” to “ADFS 2.0”

Click “Change” in the “SSO Server” section, enter the connection details of your DualShield SSO server

Only to enable the “SSL” option if your DualShield platform is operating on the SSL mode.
Select your DualShield application for the Office 365 service

Click “Apply” to save changes.

Enable Reverse Proxy

If you chose to enable the proxy feature in the DualShield SSO server settings, you will also need to enable the reverse proxy engine in the IIS server.

1. Select the web server (not a web site or virtual directory) node from the list on the left pane in the IIS manager window

2. In the "features view" window (the window in the middle), find "Application Request Routing" and double click it
3. On the right pane, find the "Server Proxy Settings..." link and click it

4. Back to the middle pane, tick (enable) the first check box, "Enable Proxy"

5. Click "Apply" on the left hand side window to save the change

Test Logon

1. Open a browser and navigate to https://login.microsoftonline.com
2. Enter a valid User ID
3. You will be then redirected to your ADFS server, and see the logon page presented by the DualShield SSO server:

![ADFS Logon Page]

4. Once you have been successfully authenticated by the DualShield SSO server, you’ll be redirected back to the Office 365 online portal:

![Office 365 Portal]

- END -