Auth Shield
Multi Factor Authentication

An Authentication Security Organization

Whitepaper

Integration of AuthShield Multi-Factor Authentication with Office 365

By Innefu Labs

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

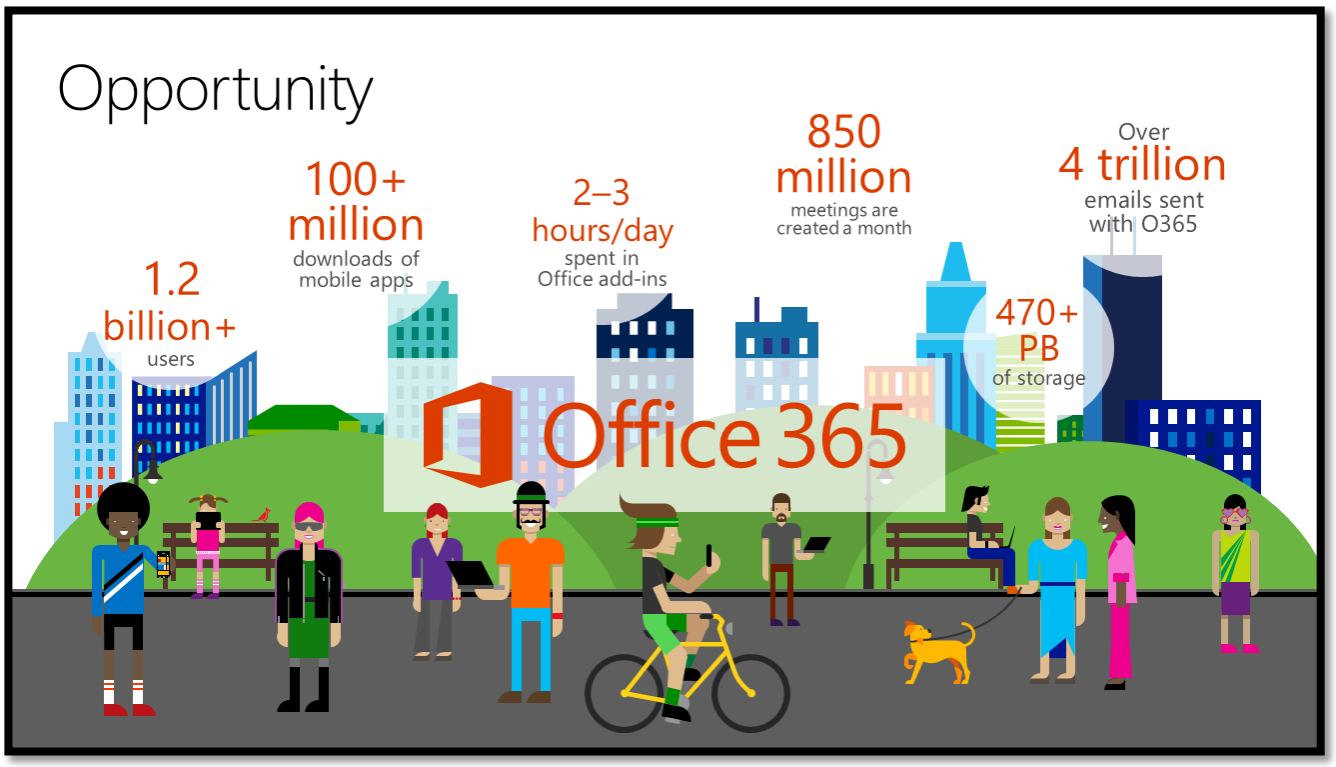
Contents

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

1. Introduction

The rapid growth of internet and digital communications has ensured that most of the organizations today have dispersed workforces across the world.



"A massive security flaw in Microsoft's Office 365 product that would make it possible for an attacker to gain unrestricted access to almost any business account and access company Outlook Online email accounts, Skype for Business, OneNote and OneDrive online storage."

The security threat posed by hackers on the Internet is constantly evolving. As security professionals improve the defensive posture of

systems and networks, hackers have evolved their penetration techniques. Moreover, the nature of the attacks launched against the Cloud is changing. The rise of Web applications and Web services has provided a common foundation for hackers to exploit, independent of the underlying operating system or software stack. In the past hackers would have focused on system level exploits, requiring them to research, develop, and test a malware exploit that was fine-tuned for a particular operating system platform and version.

"A severe vulnerability in the way Microsoft Office 365 handles federated identities via SAML put an attacker in position to have access to any account and data, including email messages and files stored in the cloud-based service."

Cloud attacks are going up simply because that is where the money is. More and more services and the accompanying data are being moved to the cloud because there are a number of advantages to using the cloud over on-premise servers.

"Roughly 57 percent of organizations using Office 365 received at least one copy of the malware into one of their corporate mailboxes during the time of the attack."

In such a scenario, to protect themselves, more and more organizations are using a Multi-Factor Authentication system to protect their accounts on Office 365.

2. Threats to Office 365 Accounts

a. Social Engineering or Password Sharing

Most people end up sharing their passwords with their friends or colleagues. The act may be deliberate or accidental. But the fact remains that a user seldom even remembers the number of people the account details may have been shared with. At the same time, passwords are not changed at frequent interval, giving an outsider unlimited access to an account. Occasionally, users also fall prey to common social engineering techniques and end up revealing answers to their security questions thereby providing intruders a chance to gain unauthorized access to the account.

b. Reuse Logins

A user on the net usually has more than one account. Most users end up using same or similar passwords in multiple accounts leading to a possibility where an inadvertent leak may lead to providing access to multiple accounts

c. Identity thefts – Phishing

"One Phishing attack at a Bank / Online Portal / store/ BPO etc can lead to a loss of thousands of accounts in one step. Acquire details such as credentials to SAP and other critical applications etc by masquerading as a trustworthy entity. Such an information breach by authorized personnel either intentionally or accidentally, can cause irreparable damage to an organization.

d. Virus, worms, Trojans

Keyloggers, remote sniffers, worms and other types of Trojans have been used since the evolution of the internet to steal user's identity. Most data is accessed from stolen computers and laptops or by hackers capturing data on unprotected networks.

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

3. Protecting Office 365 Accounts

When your organization banks on you, what do you bank on?

Prevention is always better than cure. It is truer today than ever before when the theft is conducted on the net with no physical threats and with less cost to the perpetrator of the crime. The only challenge that remains is to cover ones tracks and considering the massive flow of information on the net almost on a daily basis, it is not much difficult either.

Multi-Factor Authentication: why do you need it?

Phishers try to obtain personal information such as your password or PIN-code by pretending to be a legitimate entity.

Using Phishing, static passwords can be easily hacked providing fraudsters easy access your personal accounts, files and confidential information.

AuthShield - Multi Factor Authentication maps the physical identity of the user to the server and increases the security of financial and other critical systems. Integrating Stronger User Authentication system not only helps prevent Online Credit Card fraud, Card Cloning, Identity theft but also helps in the capture of habitual cyber criminals.

AuthShield authenticates and verifies the user based on –

- something only the user has (mobile phone/ land line/ hard token)
- something only the user knows (user id and password)
- something the user is (Biometrics)

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

AuthShield technology uses a dual mode of identification where along with the user id and password, verification is done through a secure randomly generated through One- time password (OTP). This is provided to the user through:

Hard Token

AuthShield's Hard token is a security device given to authorized users who keep them in their possession. To verify a transaction using second factor of authentication, the device displays a changing number that is typed in as a password. The new number is based on a pre-defined unbreakable randomized algorithm. Thereby, the hard token enables the server to authenticate the digital identity of the sender using a hardware device apart from his user name and password.

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

Mobile Token

AuthShield's mobile token is an application installed on smart phones which generates an OTP for the user on the phone itself.

The architecture remains similar to a Hard Token except that the user only has to carry his mobile phone. Thereby, the device enables the server to authenticate the digital identity of the sender using a mobile phone apart from his user name and password.

Auth Shield
Multi Factor Authentication

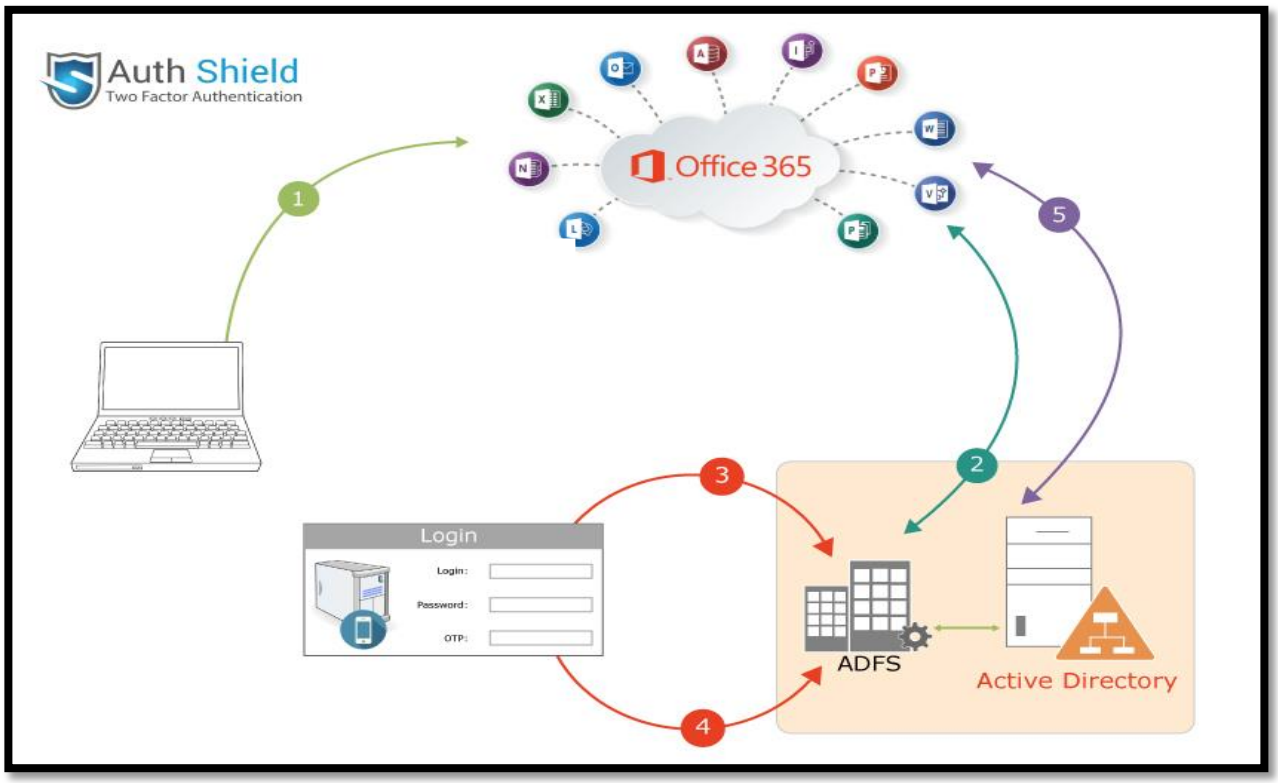
An Authentication Security Organization

Soft Token

AuthShield soft token is a convenient form factor installed on the laptop / desktop itself. The token generates a new password after fixed intervals of time. The user enters the password generated by the soft token as a secondary form of authentication.

4. Integration of AuthShield with Microsoft Office 365

Architecture



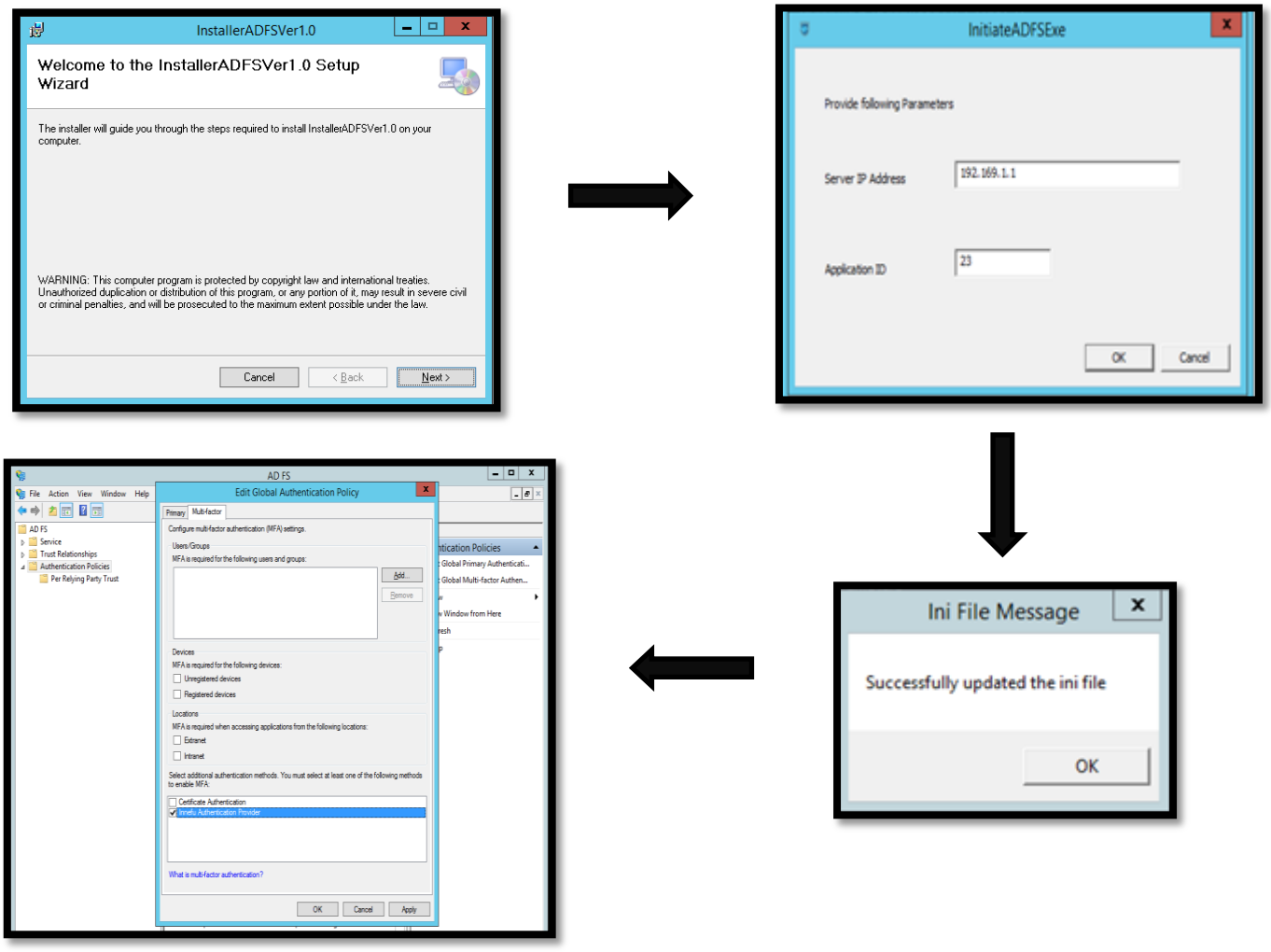
Process to integrate

- AuthShield integrated plugin can be used to authenticate services using –
  - Microsoft's WS-Federation Protocol
  - SAML 2.0 federated logons
  - Plug-in adds a multi-factor authentication provider to ADFS Identity provider and can be used for external as well as internal users
- In ADFS farm, AuthShield Plug-in has to be installed on all identity provider ADFS servers in the farm

Auth Shield
Multi Factor Authentication

An Authentication Security Organization

5. Installation Guide



- Copy AuthShield installer
- Add IP address of AuthShield Authentication Server and Application ID
- Modify Authentication Policies
- Restart ADFS

6. Features

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for Mails
- 99% security from Phishing attacks and identity thefts
- Unbreakable encryption on the lines of those used by US Government
- Logs are maintained to fix responsibility in case of an unlawful event.

7. Advantages of using AuthShield

For Users

Using AuthShield Multi-factor authentication can help in preventing-

- Online credit card fraud Phishing
- Card cloning
- Unauthorized access to data by employees.

For the organization

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for critical applications.

8. About Us

The world today revolves around information. Information today is the energy that plays a critical role in our personal lives and drives our businesses. As we move further into this digital age, it has become imperative to not just protect our information from outsiders but to also draw intelligence from the vast amount information available to us.

Internet is the new playground for unwanted elements of society intent on committing terrorist or espionage activities, financial frauds or identity thefts. Keeping this in mind, it has become imperative to not only prevent these acts but also be in a position to intercept, monitor and block Internet communication to draw intelligence out of them.

AuthShield is an Authentication Security solution with a patented technology on implementing Multifactor Authentication at a protocol level. This makes it an application independent technology and needs no changes at the application. As an advantage of working at protocol rather than application level, an organization can use AuthShield to implement Multifactor Authentication in any and every technology such as **Downloading mails on phones / desktops,** SAP, Database queries, Internet of Things, or any other enterprise or cloud technology in a matter of minutes.

For more information visit - www.auth-shield.com