FAQ (FREQUENTLY ASKED QUESTIONS)

Version: Release_v1.0

PRAMOSA

CONCEPT

Basic questions and answers of the features and functionality supported by IDKi.

AUDIENCE

Administrators and Users

Table of Contents

Definitions and Acronyms

Acronym	Definition
API	Application Program Interface
URL	Uniform Resource Locator
GUI	Graphic User Interface
U2F	Universal 2nd Factor
FIDO	Fast IDentity Online
HTTPS	Secure Hypertext Transfer Protocol
OTP	One Time Password
TOTP	Time-based One Time Password
SSL	Secure Sockets Layer
SMS	Short Message Service
OS	Operating System

1. WHAT IS A YUBIKEY?

A YubiKey is a small hardware device that offers two-factor authentication with a simple touch of a button. YubiKeys are built strong enough for the largest enterprises, while remaining simple enough for anyone to use. The YubiKey can support an unlimited number of applications without the need for drivers, client software, or batteries.

2. IS IT POSSIBLE TO UPGRADE THE YUBIKEY FIRMWARE?

No, it's currently not possible to upgrade YubiKey firmware. To prevent attacks on the YubiKey which might compromise its security, the YubiKey does not permit its firmware to be accessed or altered.

3. IS THE YUBIKEY A BIOMETRIC DEVICE?

No. The touch of a finger provides a small electrical charge that activates the YubiKey.

4. CAN A YUBIKEY BE COPIED?

No, a YubiKey cannot be copied as the computer recognizes the YubiKey as a keyboard.

5. WHAT IS FIDO U2F?

FIDO U2F is an emerging open authentication standard, with native support in platforms and browsers. U2F breaks the mold for high security public key authentication, removing the complexity of drivers and the traditional costly CA model.

The FIDO U2F (Universal 2nd Factor) protocol enables a strong cryptographic 2nd factor option for end user security.

The primary objective is to enable online services, websites and applications, whether on the open Internet or within enterprises, to leverage U2F security features for strong user authentication and to reduce the problems associated with creating and remembering many user credentials.

As one of the founders of the U2F working group in FIDO, Google build U2F support into their Chrome browser and offers U2F as a 2nd factor option on Google accounts to help the start-up of the open ecosystem, other services supporting U2F 2nd factor is GitHub, Dropbox and IDKi.

The core ideas driving the FIDO U2F Alliances are:

1) Ease of use
2) Privacy and security
3) Standardization

More information and specifications about FIDO-U2F can be found under the FIDO Alliance Web site at https://fidoalliance.org/specifications

6. WHAT IS THE PRIVACY CONSIDERATIONS OF U2F?

User privacy is a fundamental design consideration for the U2F protocol. The various privacy related design points are reiterated here:

6.1 A U2F device does not have a global identifier visible across online services, websites or applications.

6.2 A U2F device does not have a global identifier within a particular online service, website or application

- Example 1: If a person loses their U2F device, the finder cannot 'point it at a website' to see if some accounts get listed. The device simply does not know.
- Example 2: If person A and B share a U2F device and they have each registered their accounts on site X with this device, there isn't any way for the site X to guess that the two accounts share a device based on the U2F protocol alone.

6.3 A key issued to a particular online service, website or application can only be exercised by that online service, website or application.

- Since a key is essentially a strong identifier this means U2F does not give any signal which allows online services, websites or applications to strongly cross-identify shared users.

6.4 A user has to activate the U2F device (i.e., 'press the button') before it will issue a key pair (for registration) or sign a challenge for authentication.

7. WHICH BROWSERS SUPPORT U2F?

Google Chrome.

You must be running Google Chrome version 38 or later, which includes support for the U2F protocol. To check the version number, in the Chrome toolbar, click the Chrome menu, then select About Google Chrome.

8. IS USER INTERACTION REQUIRED?

The U2F device has a physical 'test of user presence'. The user touches a button to 'activate' the U2F device and this feeds into the device's operation as follows:

- ***Registration***: The U2F device responds to a request to generate a key pair only if it has been 'activated', the user will have to touch a button to register.
- ***Authentication***: During authentication, the provider (in this case, IDKi) sends information to the U2F device that it needs to sign by the U2F device. The U2F device needs to see a 'test of user presence' before it will sign - i.e., the user has to press a button on the device. This ensures that a signature happens only with the user's permission. It also ensures that that malware cannot exercise the signature when the user is not present.

9. DOES IDKi AUTHENTICATION SERVER REQUIRES A SSL CERTIFICATE?

Yes, a trusted SSL certificate linked to the IDKi Authentication Server Url is required as all communication is done over the HTTPS protocol.

NOTE: This must be a trusted cert and not a self-signed cert. Wildcard org cert linked to subdomain will also be sufficient eg: IDKi.org.com

10. WHAT IDKi LICENSE FEATURES ARE AVAILABLE?

- Full – includes all the below listed functionalities.
- Online OTP
- Offline OTP
- Password Reset
- LDAP Integration
- SMS Integration

11. WHAT IS OTP?

OTPs are one-time-passwords. These passwords are randomly generated on demand, once used to login it will then expire or after x minutes.

12. WHAT IS TOTP?

TOTPs are time based one-time-passwords. These passwords are randomly generated on demand and only valid for x minutes.

NOTE: Client- / User machines, Domain Controller and IDKi Authentication Servers time must be synced at all times for a consistent TOTP experience.

13. WHY USE OTPs?

One-time-passwords are significantly more secure and convenient than common static passwords. Static passwords are often not complex enough to be secure. In order to make them easy to remember, users tend to use the same password repeatedly or even write them down if forced to make use of complex passwords. This reduces their security and opens up the possibility of the password being cracked.

Static passwords can also be captured by 'shoulder surfing' or Trojan key logger applications. One-time-passwords are randomly generated on demand by the user, which immediately offers unique authentication in every instance. The OTP then expires immediately.

14. WHAT IS IDKi ONLINE OTP?

Allows a user to log into windows without a YubiKey being present, an OTP will get generated by the IDKi Authentication Server and sent to the user via a SMS and / or Email. The user can then unlock their machine using his / her windows password and the generated OTP.

The online OTP is only valid for a specific time period and can only be used once.

15. WHAT IS IDKi OFFLINE OTP?

Allows a user to log into windows without a YubiKey being present nor being online, a TOTP will be generated by a system administrator / helpdesk user via the IDKi Web Admin and sent to the user via

configured communication channels. The user can then unlock their machine using his / her windows password and the generated TOTP.

The offline OTP is only valid for a specific time period.

NOTE: Client- / User machines, Domain Controller and IDKi Authentication Servers time must be synced at all times for a consistent Offline OTP experience.

16. WHAT HAPPENS IF I GENERATE OTPs AND DON'T USE THEM?

OTPs and TOTPs are only valid for a specific set time period, after the time period elapsed the OTP / TOTP is no longer valid and a new one needs to be generated if required.

OTPs can only be used once.

17. HOW DOES THE OTP GET VALIDATED?

After you have entered the OTP on the client, the IDKi Authentication Server will be contacted to verify and validate the OTP, the IDKi Authentication Server will then send a response back to the client indicating if the OTP was valid or not.

18. HOW LONG IS A IDKi ONLINE OTP VALID FOR?

By default a IDKi Online OTP is valid for 5 minutes. This can be changed by updating the configuration setting "*OTPValidPeriodInMinutes*" in the IDKi Web Admin.

19. HOW LONG IS A IDKi OFFLINE OTP VALID FOR?

By default a IDKi Online OTP is valid for 5 minutes. This can be changed by updating the configuration setting "*OTPOfflineValidForMinutes_CP*" in the IDKi Web Admin.

20. CAN A IDKi ONLINE OTP BE USED ON ANOTHER MACHINE \ USER IT WAS GENERATED FOR?

No, the IDKi online OTP is bound to the user and machine from where the OTP was requested.

21. CAN A IDKi OFFLINE OTP BE USED ON ANOTHER MACHINE \ USER IT WAS GENERATED FOR?

No, the IDKi online OTP is bound to the user and machine it was generated for.

22. WHAT HAPPENS IF I DON'T HAVE MY YUBIKEY WITH ME?

In an **online scenario** (IDKi authentication server can be accessed) an online OTP can be requested, if the request was successful the user will receive a notification via SMS and / or Email containing the OTP. The OTP can then be used to login to windows without a YubiKey being present.

In an **offline scenario** (IDKi authentication server cannot be accessed) an offline OTP needs to be requested via the IDKi Web Admin (typically through a helpdesk call), if the request was successful the user will receive a notification via SMS and / or Email containing the OTP. The OTP can then be used to login to windows without a YubiKey being present.

23. WHAT HAPPENS IF I HAVE MY YUBIKEY BUT CANNOT ACCESS THE IDKi AUTHENTICATION SERVER?

IDKi caters for various offline scenarios.

If you previously successfully enrolled through the self-enroll application, you will be able to login to windows when you are in an offline scenario (cannot access the IDKi Authentication Server).

24. WHAT HAPPENS IF I LOSE MY YUBIKEY?

Configurable and selectable fallback features include: SMS, Email that will allow you to access your machine data in case of a lost key. A new key can then be enrolled to replace the lost key.

You will need to contact your help desk / administrator to de-active the old key by selecting the "*Must Re-enrol*" option on the user properties through the IDKi Web Admin, this will allow you to enroll a new YubiKey.

Note: You need to be online (must be able to access the IDKi Authentication Server) to complete the re-enrollment process.

25. CAN I USE MY YUBIKEY TO LOCK MULTIPLE WINDOWS MACHINES?

Yes, as part of the U2F standard, as single key can be used for numerous applications, including IDKi, with no loss of security between applications. It is recommended though that each person has his/her own Yubikey to ensure security to personal data.

26. HOW MANY ACTIVE KEYS CAN I HAVE?

Only 1 active key per user is allowed.

27. DOES IDKi WORK ONLY IN DOMAIN ENVIRONMENTS?

No, IDKi works in domain as well as workgroup environments.

28. WHERE ELSE CAN I USE MY YUBIKEY?

The U2F Yubikey for your IDKi can also be used to enable strong authentication on your Gmail, Dropbox, GitHub account, as well as various enterprise applications. A single key can therefore be used to protect your personal as well as corporate data.

29. DO I NEED TO INSTALL ANYTHING TO USE IDKi?

Yes, you need a server with the IDKi Authentication Server and Web Admin installed as well as the IDKi client software must be installed on all the clients and servers that require the 2 factor security.

30. DOES THE CLIENT INSTALLER SUPPORT SILENT PARAMETERS?

Yes, the client installer does support silent installation parameters (no user interaction) installations for deployment through Group Policies for instance.

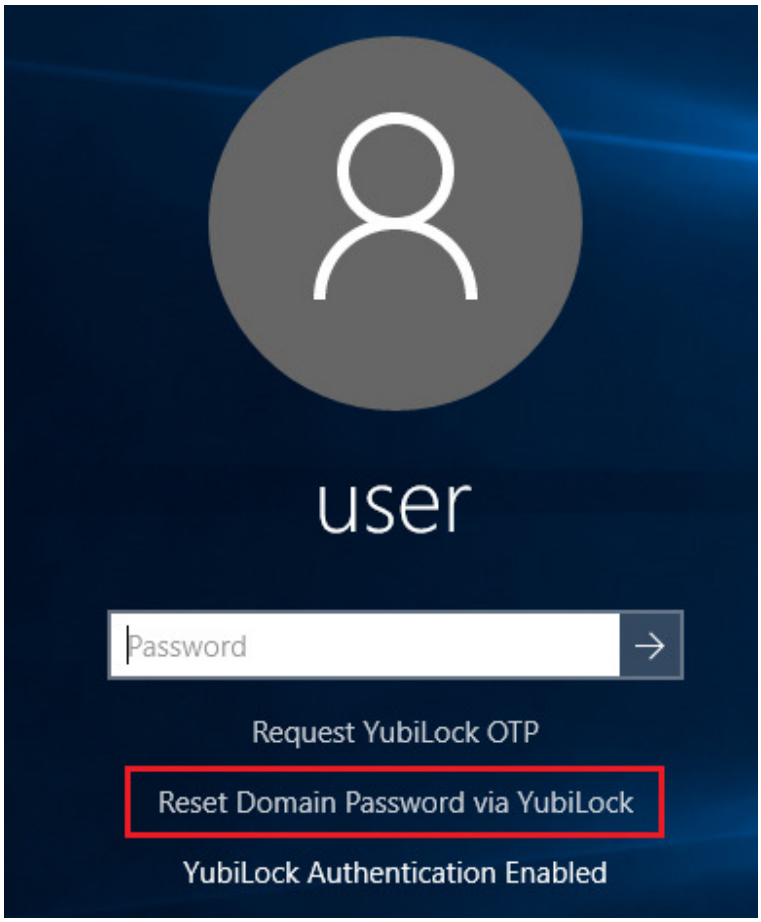
31. WHO CAN USE PASSWORD RESET FUNCTIONALITY?

Only users joined to a domain would be able to reset their domain passwords.

NOTE: This functionality will only be available if system administrators enabled the password reset functionality through the IDKi Web Admin Settings.

32. HOW TO RESET YOUR DOMAIN PASSWORD?

To reset the domain password click on "*Reset Domain Password via IDKi*", an overlay will appear with various steps that must be completed to reset your domain password.



NOTE:

- For a user to reset his / her domain password the machine must be able to contact the IDKi Authentication Server.
- The user YubiKey must be plugged into the machine, if no YubiKey is present when the user wants to reset his / her domain password a notification message will be display on the password reset overlay and you will not be able to reset your password.

33. ARE SMS MESSAGES RELIABLE?

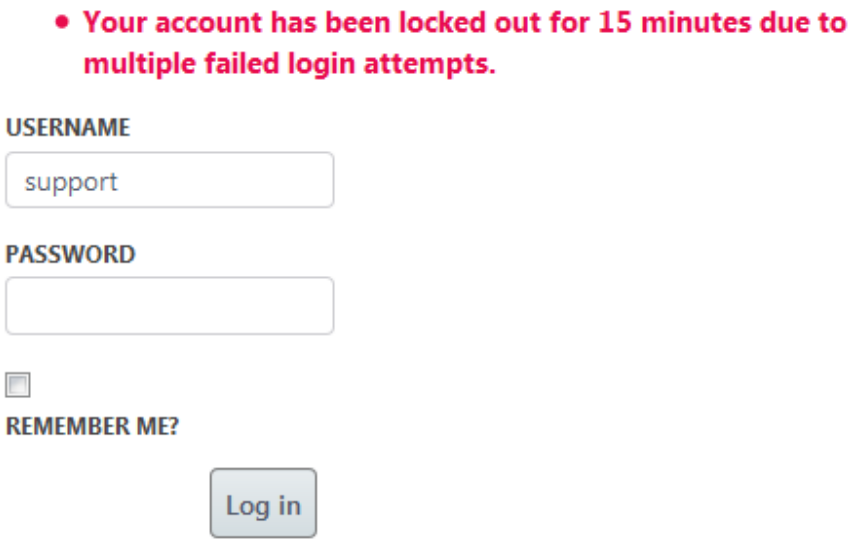
Yes. Nowdays, SMS messages are very reliable. Currently IDKi supports mymobileapi (http://www.mymobileapi.com/fe/v1/index.html).

Most bulk SMS gateways support the MyMobileAPI.

34. DOES THE WEB ADMIN SUPPORT "LOCK OUT" FUNCTIONALITY?

Yes, "Lock Out" feature is supported for Web Admin users. The feature can be enabled/disabled by selecting the *"Lockout Enabled"* option on a Web Admin user properties.

When a Web Admin user enters his/her password incorrectly 3 times they will be logged out of the Web Admin for 15 minutes before they can retry to login.

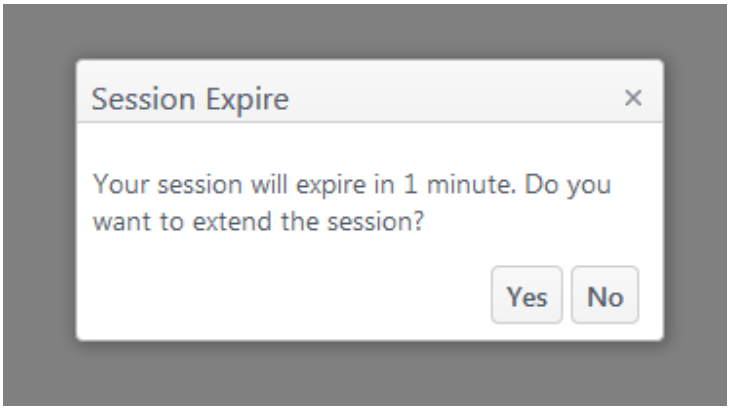


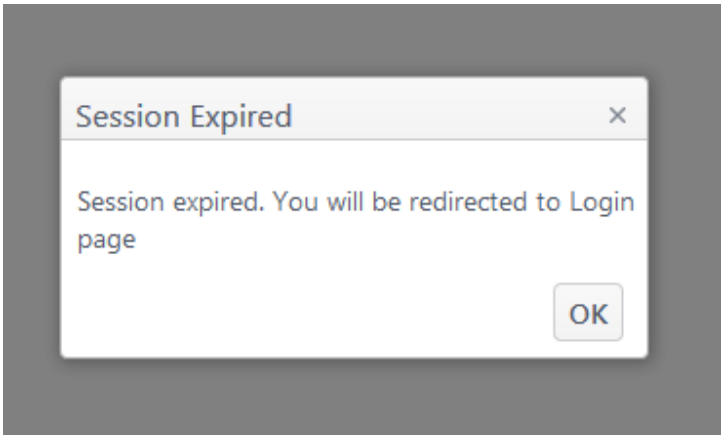
35. WHAT IS THE DEFAULT WEB ADMIN "SESSION TIME OUT"?

The default session time out is 2 minutes.

36. DOES WEB UI SUPPORT "SESSION TIME OUT"?

Yes, "Session Time Out" feature is supported by the Web Admin. After a minute of no activity a notification message will be displayed indicating that the session will expire in 1 minute, the user has the option to extend the session. The default session timeout is 2 minutes.





37. CAN YOU VIEW AUDIT EVENTS IN THE WEB ADMIN?

Yes, under the "*Audit*" section the Web Admin you can view / filter various audit events. Audit events, by default, are stored for a period of 12 months.

38. WHAT IS THE MINIMUM SERVER REQUIREMENTS (LOCAL SQL EXPRESS DB SERVER) (50 USERS)?

- **Operating System:** Server 2008 R2 with IIS 7+, .net 4.5.1, MS-SQL Express 2014 SP1 installed and updated.
- **CPU:** minimum 4 cores.
- **MEMORY:** minimum 8GB.

39. WHAT IS THE MINIMUM SERVER REQUIREMENTS (STANDALONE DB SERVER) (50 USERS)?

- **Operating System:** Server 2008 R2 with IIS 7+, .net 4.5.1 installed and updated.
- **CPU:** minimum 2 cores.
- **MEMORY:** minimum 4GB.
- **MS-SQL:** minimum SQL SERVER 2008 R2.

40. DOES IDKi HAVE AN API?

Yes, we have an extended REST API functionality for integration in any 3rd party application(s) to extend secure 2 factor authentication abilities.