AllWebID Identity Manager

Online 2-Factor Identity Authentication Solution For Secure Web Access

Integration Manual

Version 4.0

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

Overview

This document describes the activities involved in setting up AllWebID Identity Manager Solution for integrating 2-Factor Authentication (2FA) with web based applications' login workflows.

Introduction

AllWebID currently supports ASP.NET, Node.js and PHP server platform technologies for deploying 2-factor authentication. Using our REST APIs, you can add out-of-band (SMS based) as well as biometrics based 2FA to your existing web application login workflows.

A normal website with insecure single factor (password only) based access, and one enabled with AllWebID 2FA solution are illustrated in figures 1 and 2.

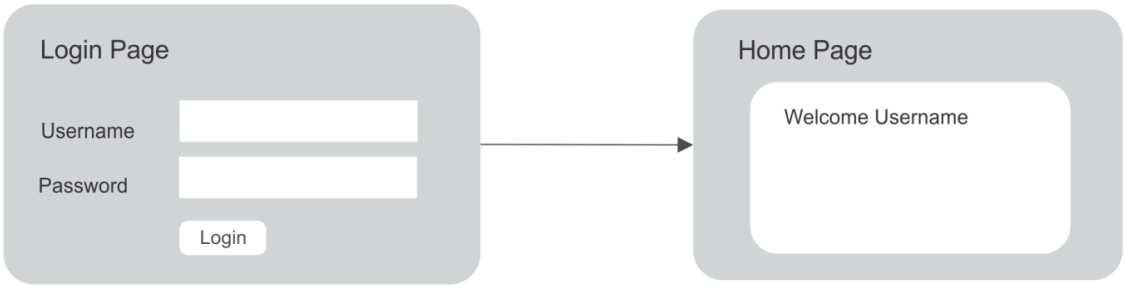

Figure 1: Normal website operation without AllWebID 2FA

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

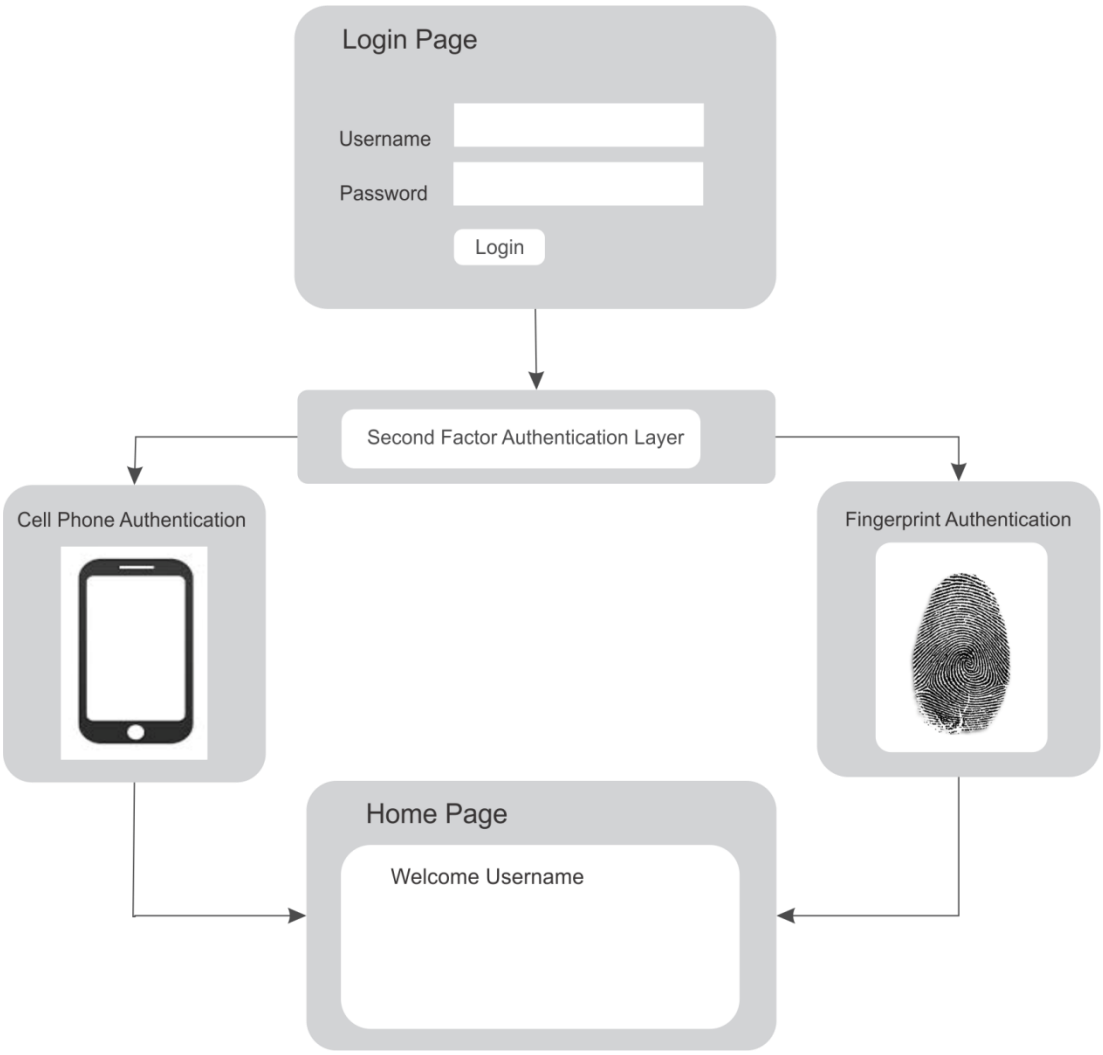

Figure 2: Website login process with AllWebID 2FA

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

How does AllWebID work?

As part of the deployment, your Web Credential Manager (WCM) is integrated with AllWebID Access Layer (AAL), which communicates to AllWebID private cloud equipped with our proprietary identity authentication servers for second factor authentication. The integration does not disturb your existing credential authentication management setup (for example Active Directory, LDAP, Databases etc). You will continue to manage your end users' passwords without exposing them outside your firewall. The whole setup of adding 2FA is done by integrating the AllWebID Identity Manager API SDK, along with some relevant changes to your web user interface. The deployment is illustrated in figure 3.

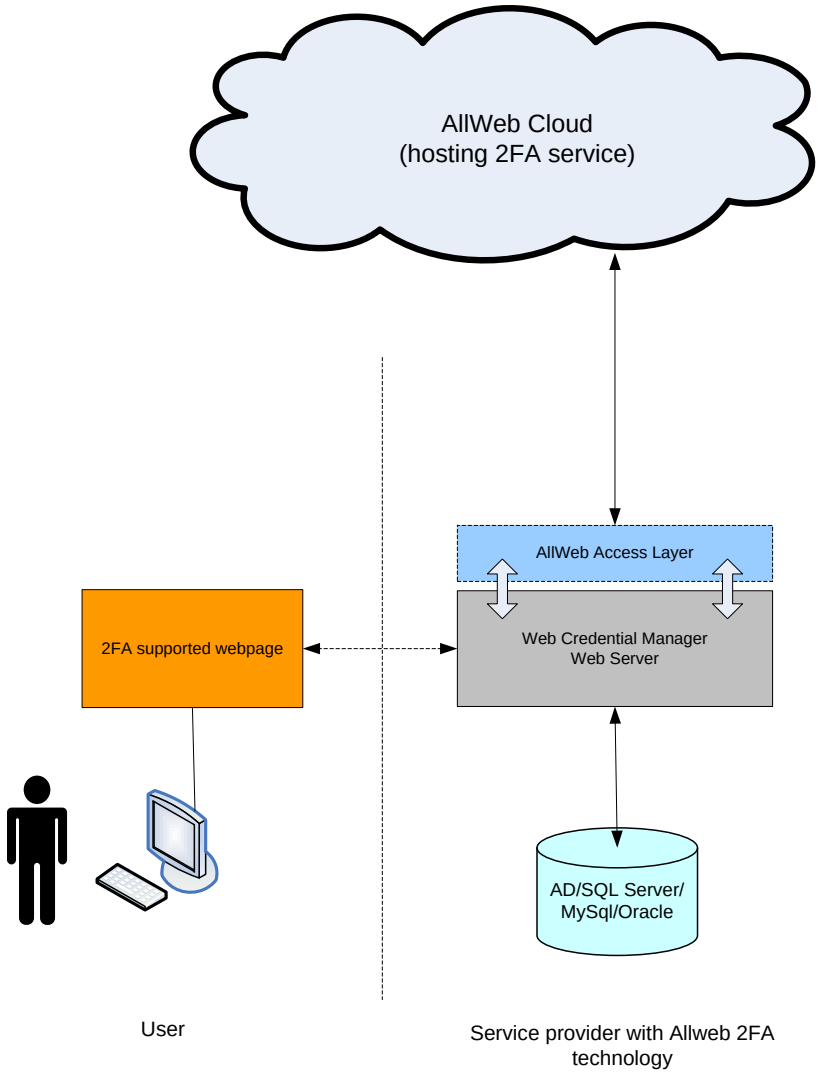

Figure 3: Allweb enabled 2FA eco-system

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

Integrating AllWebID 2FA Solution

Integrating AllWebID 2FA solution is a quick and hassle free process. The offered solution can be easily integrated with any website as it is independent of the client's user database. The main steps of integrating AllWebID 2FA solution with any customer website are given below:

1. Register your web / SaaS application on AllWebID Admin Console for 2FA service.
2. 2FA related additions/ modifications on your website (user enrollment for 2FA, options, account settings, fingerprint acquisition application link). Please refer to the sample scripts included in our SDK package.
3. Integrating AllWebID Access Layer APIs (user enrollment for 2FA and to invoke 2FA)that are available in SDK.

1. Registration of web / SaaS application with AllWebID

Following details are required to register your website with AllWebID:

I. Website Domain Name

This is the URL for your website / SaaS application domain or sub domain name. For example “salesforce.com”, “portal.bankofamerica.com”.

II. Cell Phone Registration Webpage

This is the web address which will be used for the Cell phone registration of the end user. Client can create their own pages or they can use the one being provided by AllWebID.

2. 2FA related additions/ modifications on your website

In order to offer 2FA service to the website users, changes and modifications are required on the website to support enrollment of the user for 2FA and account settings. A link will also be required on the webpage for downloading AllWebID app for fingerprint based authentication. Sample pages in different technologies have been provided in the download SDK package as reference web pages for the integrator.

3. Integration steps to deploy AllWebID 2FA Solution and List of APIs

Following is the list of API calls that the Web Credential Manager needs to make in order to execute the 2FA service. The steps and the APIs used to integrate AllWebID 2FA solution are listed in table 1. The details of the parameters used in these APIs are listed in table 2.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

API Function Name	Parameters	Description	Return Values
Identity Authentication Calls			
CheckUser2FAMethod()	APIKey, Username	To check the user's second factor authentication status (enable/disable), mode (SMS/SMSFP) and user's cell phone registration status.	$ separated values for: 2FA Mode i.e. SMS or SMSFP and 2FA Status i.e. TRUE or FALSE OR CellPhone not Registered OR Website Disabled
If second factor authentication status is "Enable" and second factor and authentication mode is "SMS Authentication" then use these API calls:			
SendPinBySMS()	APIKey, Username	Generate a PIN Code and will be send to the user's registered mobile number.	True or False
VerifySMSPin ()	APIKey, Username, PINCode	Verify the PIN Code enter by the user.	True or False or expired
If second factor authentication Is "Enable" and second factor authentication mode is "Out of Band Authentication (Android/iOS)" then use this API call:			
InitiateAuthenticationProcess ()	APIKey, Username	For initiating fingerprint authentication process via smart devices.	DeviceIsNotRegistered or True or False or Timeout
If second factor authentication Is "Enable" and second factor authentication mode is "On Device Fingerprint Authentication (Windows)" then use this API call:			
GenerateConnection()	APIKey, Username	Initiate a connection for authentication.	Encrypted token for Fingerprint Authentication
If second factor authentication status is "Enable" and second factor authentication mode is "On Device Authentication (Android/iOS)" then use this API call:			

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

InitiateAuthenticationProcess ()	APIKey, Username	For initiating fingerprint authentication process via smart devices.	DeviceIsNotRegistered or True or False or Timeout

API Function Name	Parameters	Description	Return Values
After the initial set of calls according to the specific scenario, two more API calls are required in the case of fingerprint authentication			
AuthenticateConnection()	APIKey, Username	Authenticate channel through supplied parameters of a registered user.	Username of the authenticated user or empty string
ResetConnection()	APIKey, Username	Reset authentication channel.	True or False
Enable End Users To Manage Identity Authentication Options			
SendPinBySMSforRegistration ()	APIKey, Username, Cellphone	Send PIN to user by SMS for user registration.	True or False
VerifyBySMSforRegistration ()	APIKey, Username, Cellphone	Verify user for registration.	True or False
RegistrationWithAllWeb()	APIKey, Username, secFAMode, secFaStatus, Cellphone	Register a user with AllWebID cloud.	True or False or User Limit Reached
GetUserPhoneNumber()	APIKey, Username	Get phone number of registered user.	User's phone number
UpdateUserPhoneNumber()	APIKey, Username, Cellphone	Update phone number of registered user.	True or False
RequestFPPinBySMSRegisteredUser()	APIKey, Username	Request for fingerprint registration PIN by SMS on registered phone number.	True or False
Activate2FA()	APIKey, Username, mode	Activate 2nd factor authentication.	True or False
Deactivate2FA()	APIKey, Username	Deactivate 2nd factor authentication.	True or False
SendDevicePinBySMS()	APIKey, Username	Send PIN by SMS for device registration.	True or False

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

GetUserFingerPrintRegStatus()	APIKey, Username	Get fingerprint registration status for registered user.	Yes / No
CheckDeviceAgainstUser()	APIKey, Username	To check the registered device against user.	True or False
GetOOBPin()	APIKey, Username	To get the registered pass code.	True or False or Pass code
UpdateIdaasOOBPIN()	APIKey, Username, Pass code	To update the registered pass code.	True or False

API Function Name	Parameters	Description	Return Values
Enable IT Admin To Centrally Manage Cell Phone Activation			
SendPinBySMSforCellPhoneRegistration()	APIKey, Username, CellPhone, PhoneActivationCode	Send PIN to user by SMS to verify cell phone number.	True or False
VerifyBySMSforCellPhoneRegistration()	APIKey, Username, PINCode, PhoneActivationCode	Verify PIN to register cell phone number.	True or False
RegisterUserCellPhone()	APIKey, PhoneActivationCode, CellPhone, Username	Register user's cell phone number.	True or False

Table 1: Integration Steps and List of APIs used to integrate AllWebID 2FA solution

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

Parameter	Description	Data Type
APIKey	API key is an Integration key which an integrator can get for creating integration.	String
Username	Username of the user using AllWebID 2FA service.	String
CellPhone	Cell phone number of the user of using AllWebID 2FA service.	String
SecFAMode	Defines 2nd factor authentication mode: - SMS - SMS+ Fingerprint	
secFaStatus	Defines 2nd factor authentication status: - Enable - Disable	String
PINCode	PIN code entered by the user.	String
Token	An identifier to keep track of the authentication process.	String
UserEmail	Email of the user.	String
PhoneActivationCode	PhoneActivationCode to activate phone number.	String
GenerateConnection	Connection string for authentication.	String

Table 2: List of parameters and their description

Data parameters shared between AllWebID Cloud & Client Credential Manager:

Data sharing between Client Credential Manager and AllWebID Cloud is managed through AllWebID Access Layer integrated with Web Credential Manager as shown in figure 3. Below are scenarios and data parameters in which data will be gathered and shared by Client Credential Manager with AllWebID Cloud.

1. User enrollment for 2FA:

When a user enrolls for 2FA, following parameters are gathered and communicated to the AllWebID cloud by Web Credential Manager.

1. User's ID on the website for login
2. User's email address
3. 2FA status
4. 2FA mode
5. Cell number

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

2. Login through 2FA:

When a user logs into a website integrated with AllWebID 2FA solution, a token is generated and shared between Web Credential Manager and AllWebID Cloud to keep track of the authentication process.

Type	Details
User's ID	e.g. smith@aol.com, john@gmail.com, john or any unique identifier.
User's Email address	e.g. smith@aol.com, john@gmail.com
2FA status	Enabled or Disabled.
2FA mode	Type of 2FA selected e.g. SMS only or SMS + FP
Token	An identifier to keep track of the authentication process.
Cell number	Cell phone number of the user where SMS would be sent for authentication.

Table 3:parameters saved and maintained on AllWebID Cloud

Please contact us if you have any questions.
Email: support@allwebid.com
Website: http://allwebid.com/IdentityManagerFAQs.aspx

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com